COMODO
Creating Trust Online®

Comodo
Internet Security

Software Version 10.0

User Guide

Guide Version 10.0.122117

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

Table of Contents

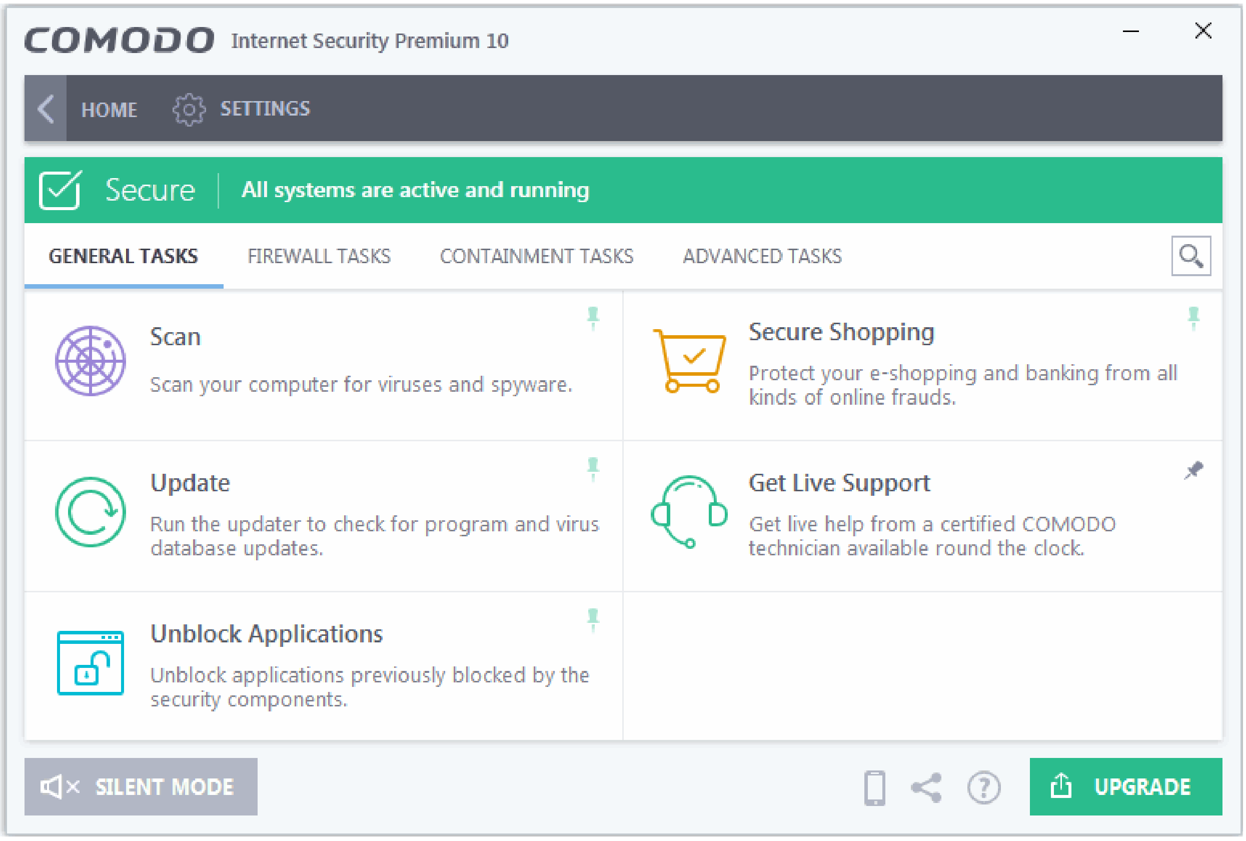
1.Introduction to Comodo Internet Security

Overview

Comodo Internet Security offers 360° protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall, and an advanced host intrusion prevention system (HIPS).

The 'Secure Shopping' feature allows you to perform online banking and shopping without fear that sensitive information like credit card numbers and passwords will be tracked or stolen. The 'Virtual Desktop' allows you open applications and websites that you are unsure of in a secure environment isolated from the rest of your computer. Built in URL filtering blocks malware websites to keep you safe online.

When used individually, each of these components delivers superior protection against their specific threat challenge. When used together as a full suite they provide a complete 'prevention, detection and cure' security system for your computer.



Scan your computer for viruses and spyware.

Protect your e-shopping and banking from all kinds of online frauds.

Run the updater to check for program and virus database updates.

Get live help from a certified COMODO technician available round the clock.

Unblock applications previously blocked by the security components.

CIS is available in free, Pro and Complete editions. While the core CIS software is identical for all three versions, the Pro and Complete packages each offer a range of additional services. The software is designed to be secure 'out of the box' - so even the most inexperienced users need not have to deal with complex configuration issues after installation.

Comodo Internet Security - Key Features:

- **Antivirus -** Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the powerful on-demand, on-access and scheduled scan capabilities, CIS users can now simply drag-and-drop items onto the home screen to run an instant virus scan.
- **Firewall -** Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.

- **Containment** - Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be auto-contained and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data.
- **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **VirusScope** - 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. Using a system of behavior 'recognizers', VirusScope not only detects unauthorized actions but also allows you to completely undo them. Apart from representing another hi-tech layer of protection against malware, this also provides you with the granular power to reverse unwanted actions taken by legitimate software without blocking the software entirely.
- **Virtual Desktop** - The Virtual Desktop is a sandbox operating environment inside of which you can run programs and browse the internet without fear that those activities will damage your real computer. Featuring a virtual keyboard to thwart key-loggers, home users will find the virtual desktop is ideally suited to sensitive tasks like online banking. Advanced users will appreciate the ability to run beta-software in an environment that will not upset the stability or file structure of their production systems.
- **Comodo Internet Security Essentials** - 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. **Click here** to learn more.
- **Secure Shopping** - A security hardened virtual environment which offers complete protection for online banking and shopping. Features include process isolation, remote takeover protection, screenshot blocking, memory-scraping prevention and independent SSL certificate verification.
- **Website Filtering** - Protects you from phishing sites while surfing the 'net and allows you to create rules to prevent specific users from accessing certain websites. CIS ships with several preset lists of malicious websites which form an effective website screening and protection feature for all Internet users. Furthermore, you can easily add or import your own lists of banned URLs and can set up custom access rules for each user on your computer.
- **Rescue Disk** - Built-in wizard that allows you to burn a boot-disk which will run antivirus scans in a pre-Windows / pre-boot environment.
- **Additional Utilities** - Allows you to install other, free, Comodo security products - including 'Comodo Cleaning Essentials' and 'KillSwitch'.
- **Chromodo Browser** - Fast and versatile Internet Browser based on Chromium, infused with Comodo's unparalleled level of Security.
- **GeekBuddy** - 24x7 online support service in which Comodo technicians are ready to deal with any computer issues you may have over an instant messenger style interface.
- **Secure Wireless Internet Connectivity** (*Complete version only*) - TrustConnect makes surfing the web safe from any public Wi-Fi location
- **Comodo Guarantee** (*Pro and Complete versions only*) - If your computer becomes damaged as a result of malware and Comodo support services cannot return it to a working condition then well pay the costs of getting it repaired. Please see the **End User License Agreement** for full details.
- **Cloud Backup** *(Complete version only)* - Back-up your important data to Comodo's highly secure servers. Data is encrypted and can accessed only by the user from any Internet connected computer in the world.

Guide Structure

This introduction is intended to provide an overview of the basics of Comodo Internet Security and should be of interest to all users.

- **Introduction**

        - Special Features
        - Downloading, Installation and Activation
    - Starting Comodo Internet Security
    - The Main Interface
    - Understanding Security Alerts

The remaining sections of the guide cover every aspect of the configuration of Comodo Internet Security.

- General Tasks - Introduction
    - Scan and Clean your Computer
        - Run a Quick Scan
        - Run a Full Computer Scan
        - Run a Rating Scan
        - Run a Custom Scan
    - Secure Shopping
    - Manage Virus Database and Program Updates
    - Get Live Support
    - Manage Blocked Items
    - Instantly Scan Files and Folders
    - Processing Infected Files
- Firewall Tasks - Introduction
    - Allow or Block Internet Access to applications Selectively
    - Manage Network Connections
    - Stop all Network Activities
    - Stealth your Computer Ports
    - View Active Internet Connections
- Containment Tasks - An Introduction
    - Run an Application in the Container
    - Reset the Container
    - Identify and Kill Unsafe Running Processes
    - View Active Process List
    - The Virtual Desktop
        - Starting the Virtual Desktop
        - The Main Interface
        - Running Browsers inside the Virtual Desktop
        - Opening Files and Running Applications inside Virtual Desktop
        - Configuring the Virtual Desktop
        - Closing the Virtual Desktop
- Advanced Tasks - An Introduction
    - Create a Rescue Disk
        - Downloading and Burning Comodo Rescue Disk
    - Remove Deeply Hidden Malware
    - Manage CIS Tasks
    - Manage Quarantined Items
    - View CIS Logs
    - Submit Files for Analysis to Comodo

The final sections contain configuration and technical help for GeekBuddy, TrustConnect, Dragon Browser and Acronis Backup.

1.1. Special Features

Auto-Containment

- Automatically runs unknown files inside a secure container which is isolated from the rest of your computer
- Cloud based behavior analysis helps identify zero-day malware before traditional antivirus

- Alerts you every time an unknown or untrusted application attempts to run or install
- Prevents unauthorized modification of critical operating system files and registry entries

VirusScope

- Monitors the activities of processes running on your computer and alerts you if their actions could potentially threaten your privacy and/or security
- Ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely

Host Intrusion Prevention System

- Virtually bulletproof protection against root-kits, inter-process memory injections, key-loggers and more;
- Monitors the activities of all applications and processes on your computer and allows executables and processes to run if they comply with the prevailing security rules
- Blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- Enables advanced users to enhance their security measures by quickly creating custom policies and rulesets using the powerful rules interface.

Virtual Desktop

An isolated, environment in which to run programs and visit websites that you may not trust 100%. Applications and browsers running inside the virtual desktop leave no history and must write to a virtual file system and registry. This protects you because any activities that take place in the virtual desktop cannot access or cause harm to your real computer.

- Prevents malicious websites from installing viruses malware, rootkits and spyware onto your real computer and provides protection against hacking
- Features a virtual keyboard that allows you to securely enter user-names and passwords without fear of key-logging software recording your physical keystrokes
- Enables advanced users to run beta-software in an environment that will not upset the stability or file structure of their production systems

Secure Shopping

Comodo Secure Shopping provides a security hardened browsing environment for your online banking and shopping activities. Browsers running in the secure environment are isolated from any potentially hostile processes running on your computer.

- Hides sensitive online data from other processes running on your PC
- Prevents key-loggers from recording your keystrokes
- Warns you if there is a remote connection to your computer
- Stops hackers and malware taking screenshots of your session
- Detects fake SSL certificates to stop man-in-the-middle attacks

Advanced Network Firewall Engine

The Firewall component of Comodo Internet Security offers the highest levels of perimeter security against inbound and outbound threats - meaning you get the strongest possible protection against hackers, malware and identity thieves. Now we've improved it again by adding new features like,

- Stealth Mode to make your PC completely invisible to opportunistic port scans;
- Wizard based auto-detection of trusted zones;
- Predefined Firewall policies allow you to quickly implement security rules;
- Diagnostics to analyze your system for potential conflicts with the firewall and much more;

- Website Filtering enables you to set up user based access restriction to specific websites.

Comprehensive Antivirus Protection

- Detects and eliminates viruses from desktops, laptops and network workstations;
- Performs Cloud based Antivirus Scanning;
- Employs heuristic techniques to identify previously unknown viruses and Trojans;
- Scans even Windows Registry and System Files for possible spyware infection and cleans them;
- Constantly protects with real-time, On-Access scanning;
- Comodo AV shows the percentage of the completed scanning;
- Rootkit scanner detects and identifies hidden malicious files and registry keys stored by rootkits;
- Highly configurable On-Demand scanner allows you to run instant checks on any file, folder or drive;
- Comodo AV realtime scanning performance in Stateful mode;
- Seamless integration into the Windows operating system allows scanning specific objects 'on the fly';
- Daily, automatic updates of virus definitions;
- Isolates suspicious files in quarantine preventing further infection;
- Built in scheduler allows you to run scans at a time that suits you;
- Simple to use - install it and forget it - Comodo AV protects you in the background.

Intuitive Graphical User Interface

- Advanced and Basic View summary screens gives an at-a-glance snapshot of your security settings;
- Easy and quick navigation between each modules;
- Simple point and click configuration - no steep learning curves;
- New completely redesigned security rules interface - you can quickly set granular access rights and privileges on a global or per application. The firewall also contains preset policies and wizards that help simplify the rule setting process.

Comodo GeekBuddy (Pro, Complete versions only)

CIS Pro and Complete customers receive Comodo GeekBuddy - Live expert remote support for virtually all personal computer issues. Pro and Complete users benefit from the convenience of having a computer security expert on tap 24/7 to help them fix problems right in front of their eyes.

The services include:

- Virus & Malware Removal
- Internet and Online Identity Security
- Printer or Email Account Setup
- Software Activation
- General PC Troubleshooting
- Computer Power Setting Optimization
- Comodo Software Installation and Set up
- Comodo Account Questions.

Please visit **http://www.geekbuddy.com/** for full product details.

Note: To use the GeekBuddy service on a continuous basis, you have to purchase the product at **http://www.geekbuddy.com/**, **register** and **activate your account**.

Comodo TrustConnect

Included with a Complete subscription, TrustConnect is a fast, secure internet proxy service that makes surfing the web safe from public Wi-Fi, TrustConnect is suitable for:

- Coffee shops, Hotels and Airports
- Any public Wi-Fi location
- At your home
- On the road. Businesses with remote workers that need secure access to internal networks.

Comodo Backup

CIS Complete customers receive Comodo Cloud Backup - powerful and easy to use application that helps home and business users protect their valuable data against damage or loss.

- Quickly create backups of your priceless data to a wide range of storage media
- Backup data from any source and recover to any destination or system
- Granular scheduling options to take automatic backups at a time that suits you.
- Quick recovery of files with a few clicks of the mouse.
- Powerful encryption options to protect your files so that it cannot be accessed by anyone but you.

Dragon Browser

Fast and versatile Internet Browser based on Chromium, infused with Comodo's unparalleled level of Security.

- Improved Security and Privacy over Chromium
- Lightning Fast Page Load Times
- Instantly Scan Web pages for Malware with Web Inspector
- Built-in Media Downloader allows you to quickly save streaming videos
- Greater Stability and Less Memory Bloat
- 'Incognito Mode' stops cookies and improves privacy
- Very easy to switch from your current browser to Dragon

Comodo Internet Security - Extended Features

Highly Configurable Security Rules Interface

Comodo Internet Security offers more control over security settings than ever before. Users can quickly set granular internet access rights and privileges on a global or per application basis using the flexible and easy to understand GUI. This version also sees the introduction of preset security policies which allow you to deploy a sophisticated hierarchy of firewall rules with a couple of mouse clicks.

Application Behavior Analysis

Comodo Internet Security features an advanced protocol driver level protection - essential for the defense of your PC against Trojans that run their own protocol drivers.

Cloud Based Behavior Analysis

Comodo Internet Security features cloud based analysis of unrecognized files, in which any file that is not recognized and not in Comodo's white-list will be sent to 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 behaves in a malicious manner. If yes, the file is then manually analyzed by Comodo technicians to confirm whether it is a malicious file or not. The results will be sent back to your computer in around 15 minutes.

VirusScope

The innovative VirusScope feature monitors the activities of all processes running on your system and generates alerts if any suspicious activities are identified. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the Behavior Blocker by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented in order to run correctly.

Website Filtering

Comodo Internet Security enables you to configure rules to allow or block access to specific websites. Rules can be created for particular users of your computer, which makes this feature very useful for both home and work environments. For example, parents can block juvenile users from visiting inappropriate websites while companies can prevent employees from visiting social networking sites during working hours.

Event logging

Comodo Internet Security features a vastly improved log management module - allowing users to export records of antivirus, firewall, HIPS and container activities according to several user-defined filters. Beginners and advanced users alike will benefit from this essential troubleshooting feature.

Memory Firewall Integration

Comodo Internet Security now includes the buffer-overflow protection original featured in Comodo Memory Firewall. This provides protection against drive-by-downloads, data theft, computer crashes and system damage.

'Training Mode' and 'Paranoid' Mode

These modes enable the firewall and host intrusion prevention systems to automatically create 'allow' rules for new components of applications you have decided to trust, so you won't receive pointless alerts for those programs you trust. The firewall learns how they work and only warn you when it detects truly suspicious behavior.

Application Recognition Database (Extensive and proprietary application safe list)

The Firewall includes an extensive white-list of safe executables called the 'Comodo Safe-List Database'. This database checks the integrity of every executable and the Firewall alerts you of potentially damaging applications before they are installed. This level of protection is new because traditionally firewalls only detect harmful applications from a blacklist of known malware-often-missing new forms of malware as might be launched in day zero attacks.

The Firewall is continually updated and currently over 1,000,000 applications are in Comodo Safe list, representing virtually one of the largest safe lists within the security industry.

Self Protection against Critical Process Termination

Viruses and Trojans often try to disable your computer's security applications so that they can operate without detection. CIS protects its own registry entries, system files and processes so malware can never shut it down or sabotage the installation.

Containment as a security feature

Comodo Internet Security's new 'Virtual Desktop' is an isolated operating environment for unknown and untrusted applications. Because they are virtualized, applications running in the container cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have also integrated auto-containment directly into the security architecture of CIS to complement and strengthen the Firewall, HIPS and Antivirus modules.

Submit Suspicious Files to Comodo

Are you the first victim of a brand new type of spyware? Users can help combat zero-hour threats by using the built in submit feature to send files to Comodo for analysis. Comodo then analyzes the files for any potential threats and update our database for all users.

1.2. Downloading, Installation and Activation

Comodo Internet Security is available in three versions, 'Premium', 'Pro' and 'Complete'. While Comodo Internet Security Premium is free, the other two are paid versions. The core security features for all three are the same but 'Pro' and 'Complete' contains additional services such as 'GeekBuddy', 'TrustConnect', 'Cloud Backup' and the 'Comodo Guarantee'.

Download Location

- Free - **https://www.comodo.com/home/download/download.php?prod=cis**
- Pro - **https://www.comodo.com/home/internet-security/internet-security-pro.php**

- Complete - **https://www.comodo.com/home/internet-security/internet-security-complete.php**

Installation

Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. **Click here** to read the full note. See the online guide at **https://help.comodo.com/topic-72-1-772-9444-CIS - Installation.html** for a complete outline of the installation process.

Activation

Comodo Internet Security Premium is a free application that does not require activation. The licenses for the paid versions, CIS 'Pro' and 'Complete', should be activated after the installation. In order to activate the Comodo guarantee, a full antivirus scan should be run on the system. See the online guide at **https://help.comodo.com/topic-72-1-772-9447-Activating-CIS-Pro-Complete-Services-after-Installation.html** and **https://help.comodo.com/topic-72-1-772-9449-Activating-Your-Guarantee-Coverage.html** for more details on how to activate the license and guarantee.

1.3. Starting Comodo Internet Security

After installation, Comodo Internet Security will start automatically whenever you start Windows. In order to configure and view settings within Comodo Internet Security, you need to access the main interface.

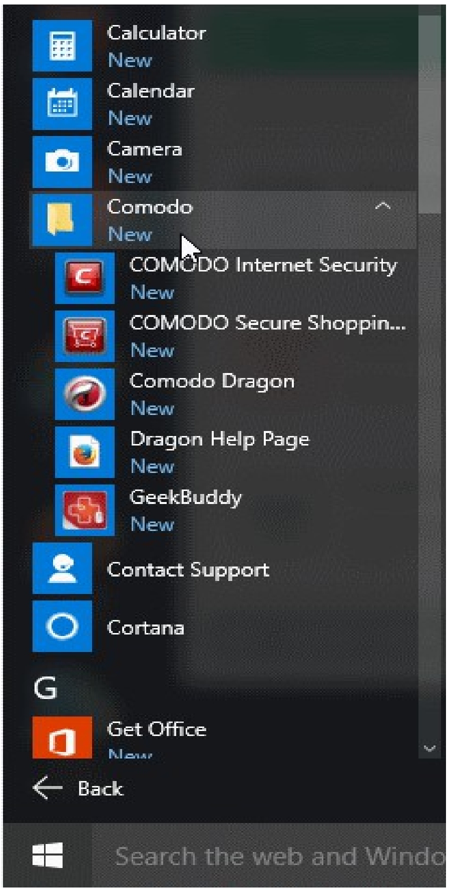
There are four different ways to open Comodo Internet Security:

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

Start Menu

You can access Comodo Internet Security via the Windows Start Menu.

- Click **Start/Windows Home** Button and Select **All Programs/All Apps** > **Comodo** > **COMODO Internet Security** > **COMODO Internet Security.**

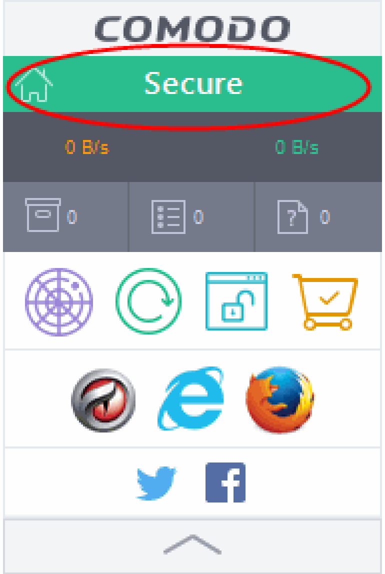


Windows Desktop

- Just double click the shield icon in the desktop to start Comodo Internet Security.

Widget

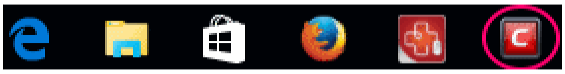
- Just click the information bar in the widget to start CIS.



You can also view other details in the widget such as inbound and outbound traffic, number of tasks running, shortcuts to common CIS tasks and browsers and links to social media sites Twitter and Facebook. See '**The Widget**' for more details.

CIS Tray Icon

- Just double click the CIS 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, Firewall, Auto-Containment, HIPS, VirusScope, Silent Mode options and more. See '**The System Tray Icon**' for more details.

Silent Mode - Switches CIS to Silent Mode if you do want to have any interruptions from various CIS alerts in your computer. The operations that normally interfere while using the system are either suppressed or postponed.

In silent mode:

- HIPS/Firewall alerts are suppressed as if they are in training mode;
- AV database updates and scheduled scans are postponed until the silent mode is switched off;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Silent Mode to resume alerts and scheduled scans.

Widget - **Click here** for more details on CIS Widget.

1.4. The Main Interface

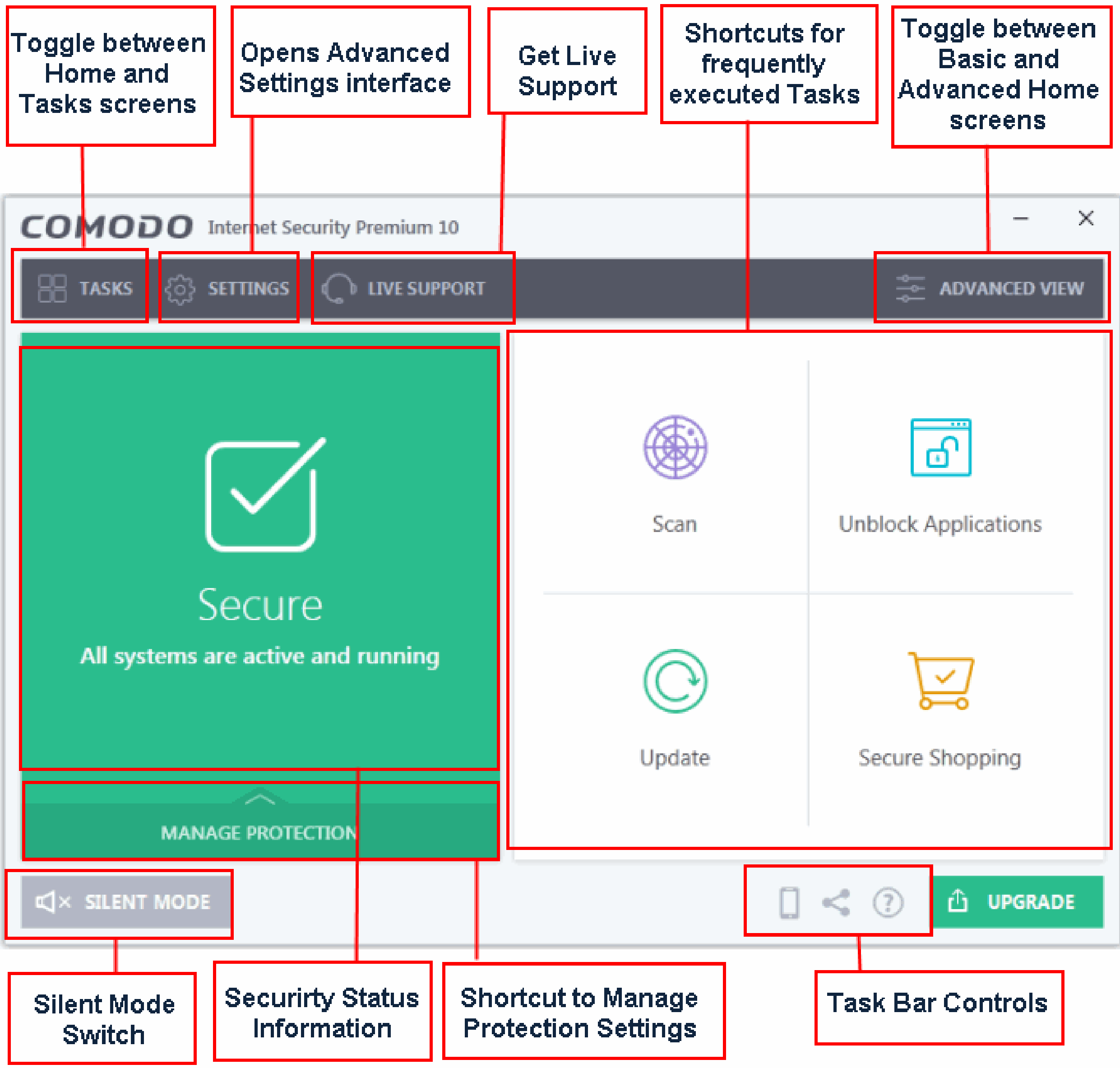
The CIS interface is designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.

The look of the user interface depends on the theme selected. There are four different themes you can choose from. See '**Customize User Interface**' for more details.

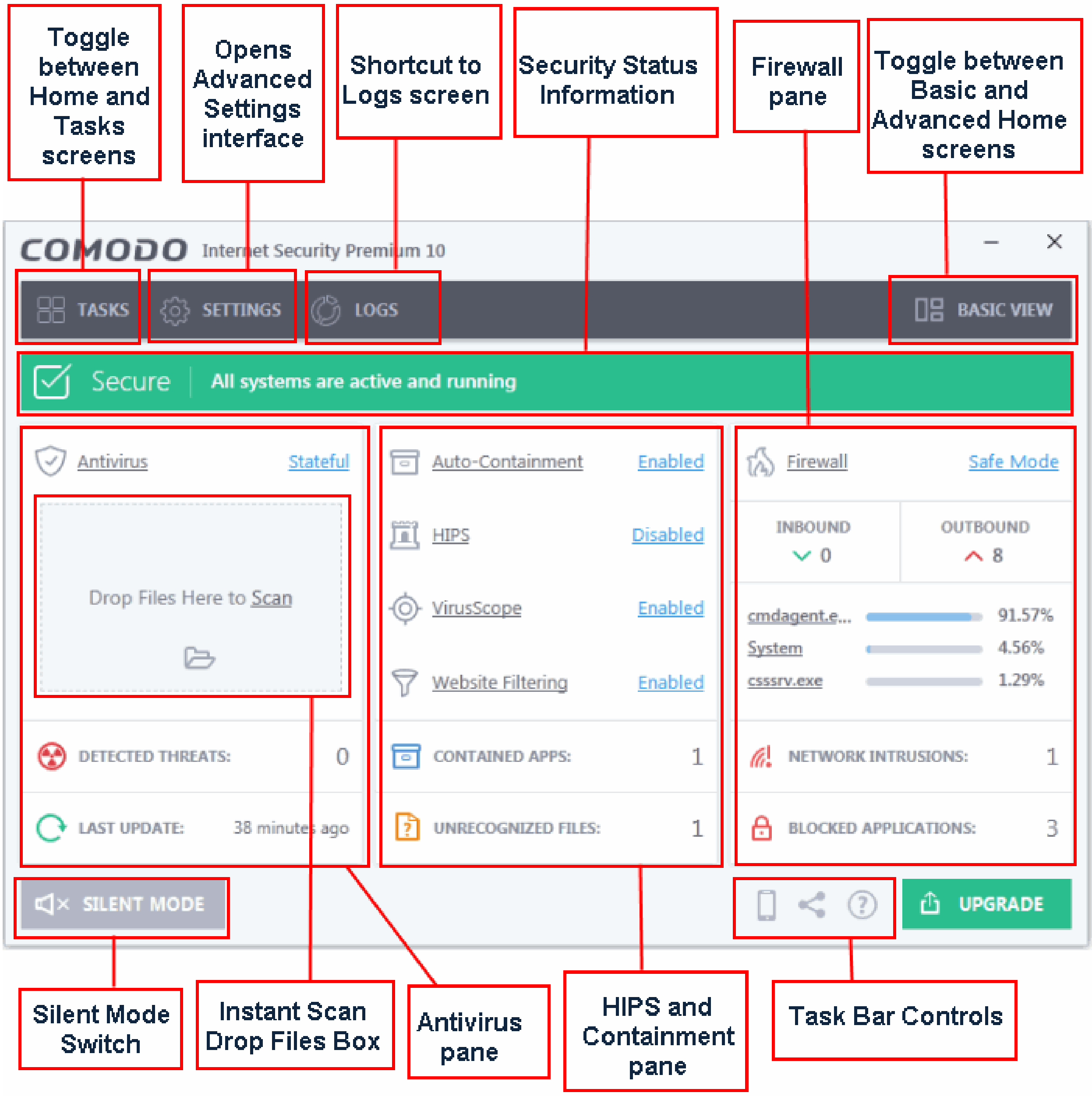
- Click 'Home/Tasks' button at the upper left to switch between the '**home screen**' and the '**tasks interface**'
- Flip between 'Basic View' and 'Advanced View' by using the 'Basic View/Advanced View' button at the upper right of the home screen.

- Instantly run a virus scan on a file or folder by dragging it into the scan box (advanced view)
- Switch on 'Silent Mode' to make sure nothing interrupts you while you are on an important task.
- The tiles in the home screen allow one-click access to important features such as the antivirus scanner, the update checker, Secure Shopping and more.
- The 'Upgrade' button allows Comodo Internet Security users to upgrade to CIS 'Pro' or 'Complete'.

Basic View


Toggle between Home and Tasks screens
Opens Advanced Settings interface
Get Live Support
Shortcuts for frequently executed Tasks
Toggle between Basic and Advanced Home screens
COMODO Internet Security Premium 10
TASKS
SETTINGS
LIVE SUPPORT
ADVANCED VIEW
Secure
All systems are active and running
Scan
Unblock Applications
Update
Secure Shopping
MANAGE PROTECTION
SILENT MODE
UPGRADE
Silent Mode Switch
Securirty Status Information
Shortcut to Manage Protection Settings
Task Bar Controls

Advanced View



The advanced view shows antivirus, containment, and firewall activity in greater detail. This includes the number of detected threats, last virus database update time, contained apps, unrecognized files, the number of inbound and outbound connections and more.

This view also allows you to quickly change security settings for each component.

The following areas are common to both the 'Tasks' and 'Home' screens:

- Task bar controls
- Advanced Settings

Task bar controls

The Task bar (bottom-right) contains shortcuts for:

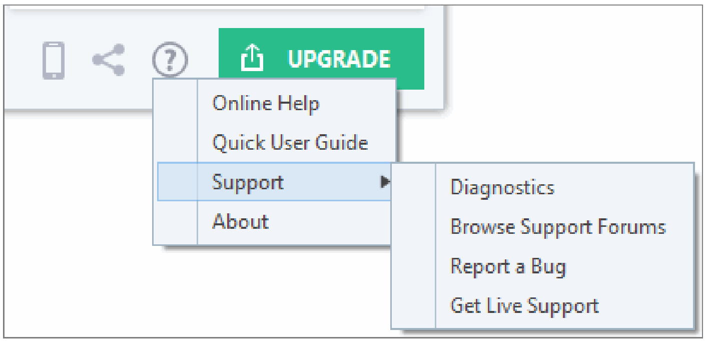
📱	**Go Mobile**	Comodo mobile security apps for Android phones and Tablets. - Available mobile apps include 'Mobile Security', 'Anti-Theft', 'Back Up' and 'App Lock'. You can also get the apps from our website, https://m.comodo.com/ or from the 'Google Play' app store.

Refer Your Friends

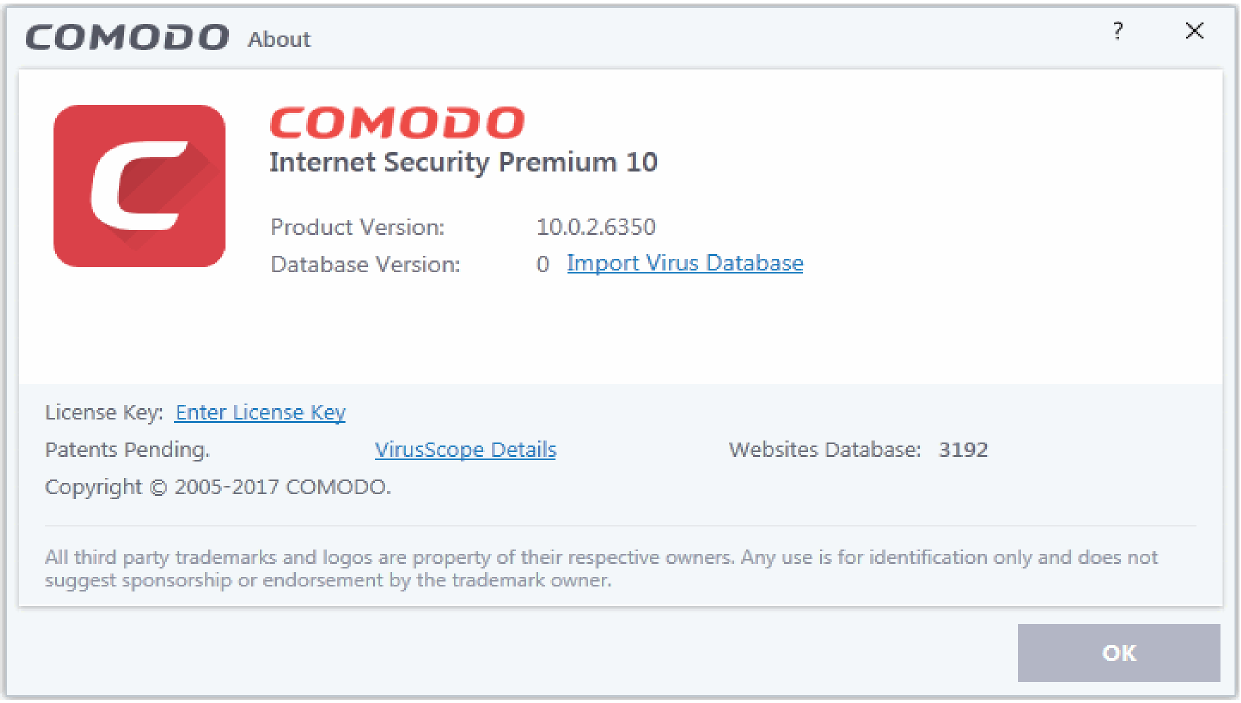
Refer your Friends - Click 'Share' to open the 'Comodo Friends' website. Register an account for free, recommend CIS to your friends and get attractive rewards. Visit http://friends.comodo.com/ for more details

Help Window

Get Help Window - Click '?' for the following options:



- **Online Help** - Opens Comodo Internet Security's online help guide at https://help.comodo.com
- **Quick User Guide** - Open the Comodo Internet Security's quick start guide at https://help.comodo.com
- **Support** - Click this link for the following options:
    - **Diagnostics** - Helps to identify any problems with your installation.
    - **Browse Support Forum** - Links to Comodo User Forums.
    - **Report a Bug** - Opens the bug reports page at Comodo User Forums for reporting problems faced while using the application.
    - **Get Live Support** - Launches the GeekBuddy support client.
- **About** - Displays the product version, virus signature database version, website database version (website filtering URLs), details of active VirusScope Recognizers and copyright information. The 'About' dialog also allows you to import a locally stored virus database and to enter a license key for CIS Pro.



Product Version: 10.0.2.6350

Database Version: 0 Import Virus Database

License Key: Enter License Key

Patents Pending. VirusScope Details Websites Database: 3192

Copyright © 2005-2017 COMODO.

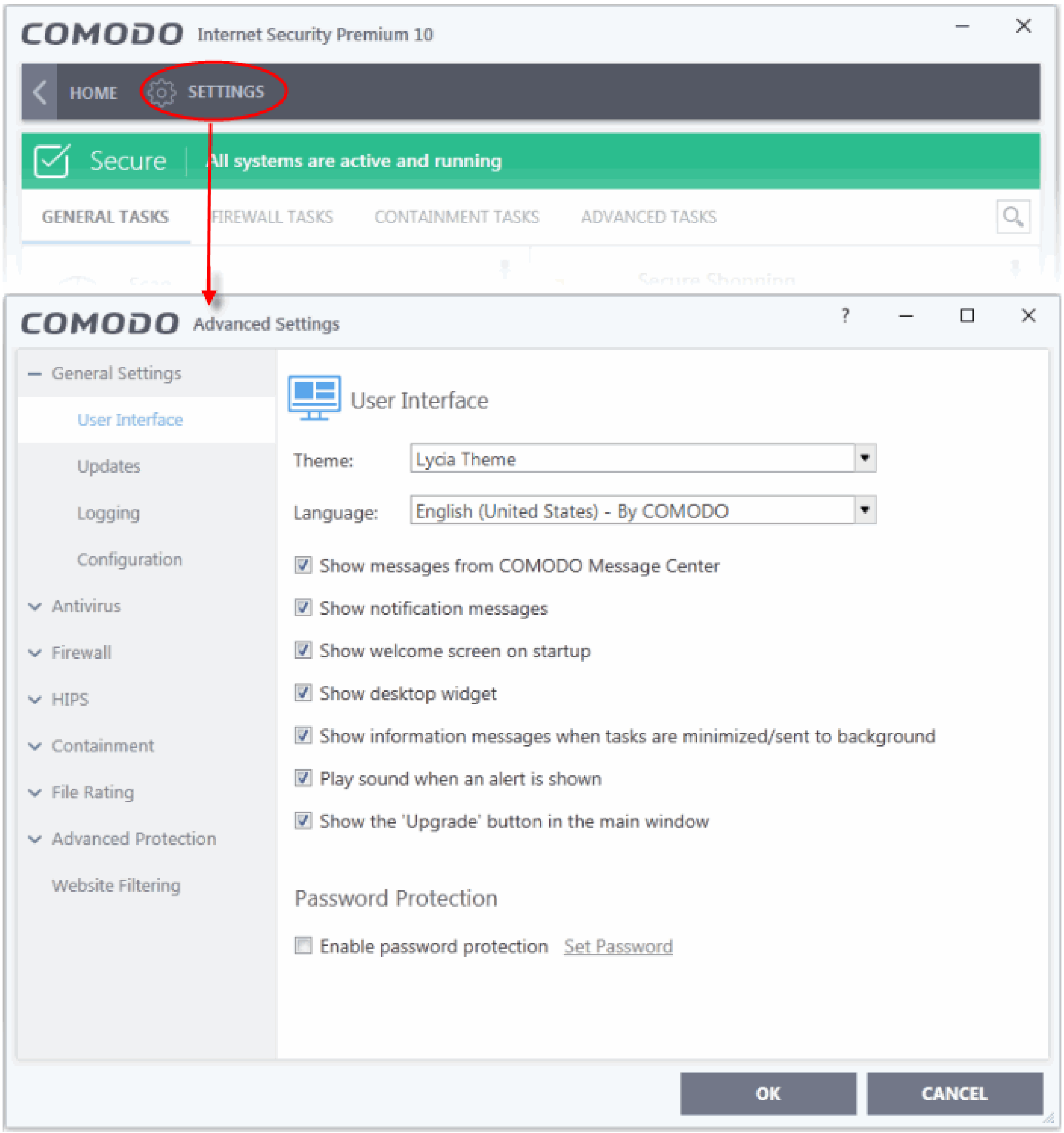
All third party trademarks and logos are property of their respective owners. Any use is for identification only and does not suggest sponsorship or endorsement by the trademark owner.

- Click 'Import Virus Database' link to import a locally stored virus signature database into CIS.
- Click 'Enter License Key' to upgrade to CIS 'Pro' or 'Complete'. See '**Activating CIS Pro/Complete Services**' for more details.
- Click 'VirusScope Details' to open a dialog which shows the VirusScope Recognizers that are active on your system. See '**VirusScope**' for more details.

Advanced Settings

The CIS is shipped with a user-friendly default settings that is sufficient for regular users. However, if you want to customize the settings according to your requirements, then you can do the same in the 'Advanced Settings' interface. This interface allows you to configure the overall behavior and every aspect of the CIS functionality such as 'Antivirus', 'Firewall', 'HIPS' and more.

- To open 'Advanced Settings', click 'Settings' at the top left.



User Interface

Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show welcome screen on startup

☑ Show desktop widget

☑ Show information messages when tasks are minimized/sent to background

☑ Play sound when an alert is shown

☑ Show the 'Upgrade' button in the main window

Password Protection

□ Enable password protection Set Password

See '**CIS Settings**' for more details about configuring each of the components.

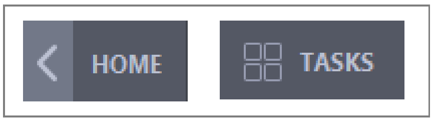
Click the following links for more information:

- **The Home Screen**
- **The Tasks Interface**
- **The Widget**

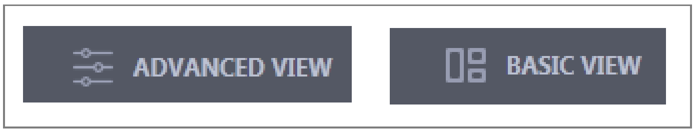
- **The System Tray Icon**

1.4.1. The Home Screen

You can switch between the 'Home' screen and the 'Tasks' interface by clicking the 'Home/Tasks' button at the top left of the interface:



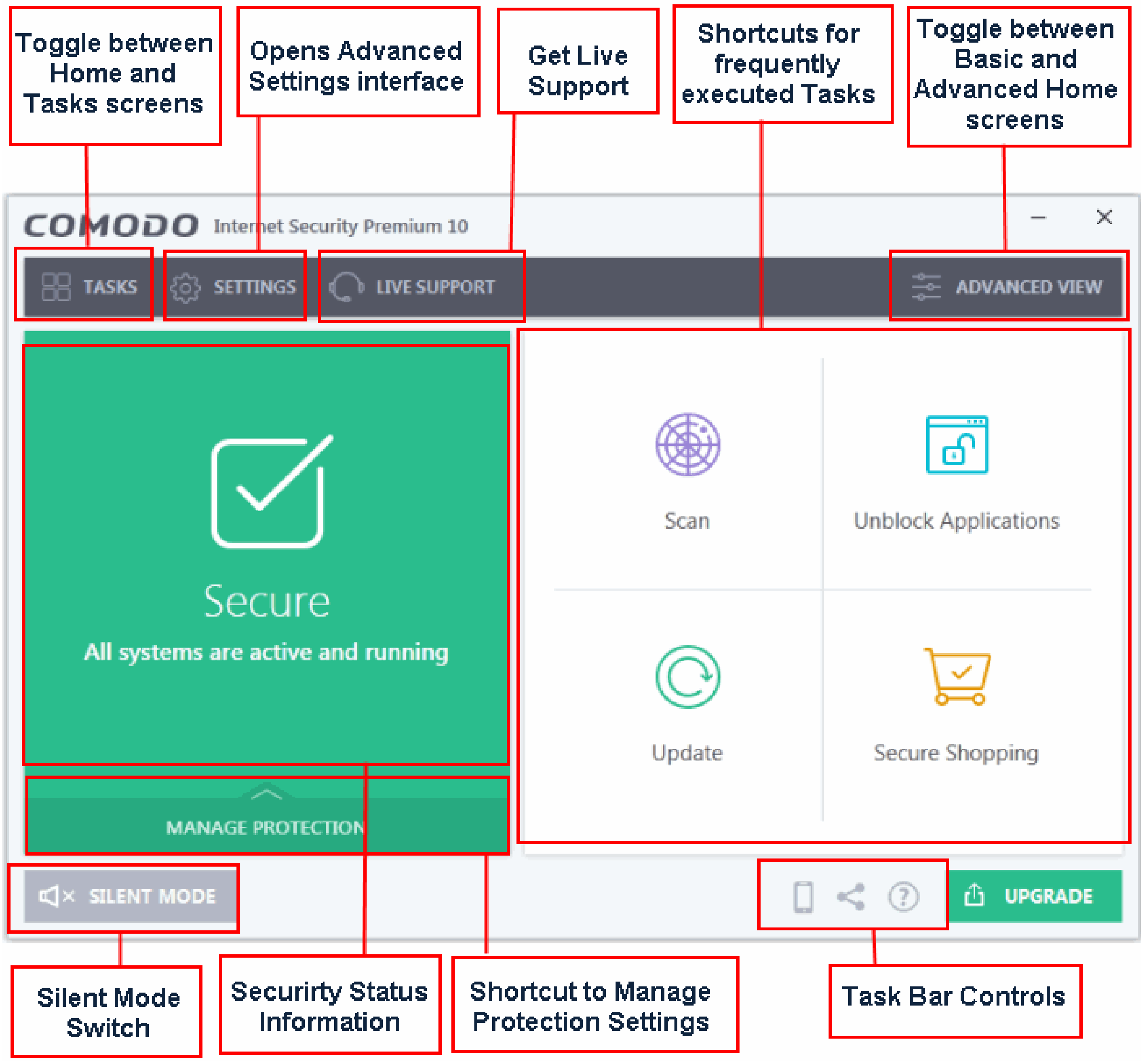
The home screen itself is available in two formats, '**Basic**' view and '**Advanced**' view. Use the button at the top-right of the home screen to switch between them.



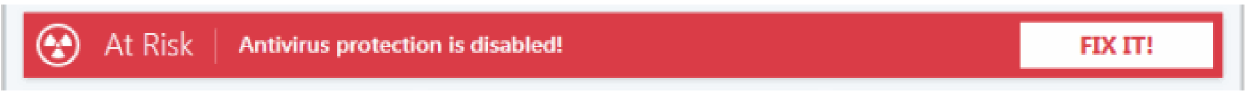
'**Title bar controls**', '**Advanced Settings**' and '**Silent Mode**' are common to both basic and advanced views.

Basic View

- Basic View presents a simple, easy to understand interface that allows users to quickly launch key tasks and gain an immediate overview of the security of their computer.
- The large 'security information' tile on the left provides an at-a-glance view of overall system security and allows you to run an appropriate CIS task if threats are found.
- The 'Manage Protection' button below the 'security information' tile allows you to turn security components on or off as well as open the component's advanced settings interface.


Toggle between Home and Tasks screens
Opens Advanced Settings interface
Get Live Support
Shortcuts for frequently executed Tasks
Toggle between Basic and Advanced Home screens
COMODO Internet Security Premium 10
TASKS
SETTINGS
LIVE SUPPORT
ADVANCED VIEW
Secure
All systems are active and running
Scan
Unblock Applications
Update
Secure Shopping
MANAGE PROTECTION
SILENT MODE
UPGRADE
Silent Mode Switch
Securirty Status Information
Shortcut to Manage Protection Settings
Task Bar Controls

The security information tile on the left will inform you if any component is disabled or any if other problems are found:


At Risk | Antivirus protection is disabled!

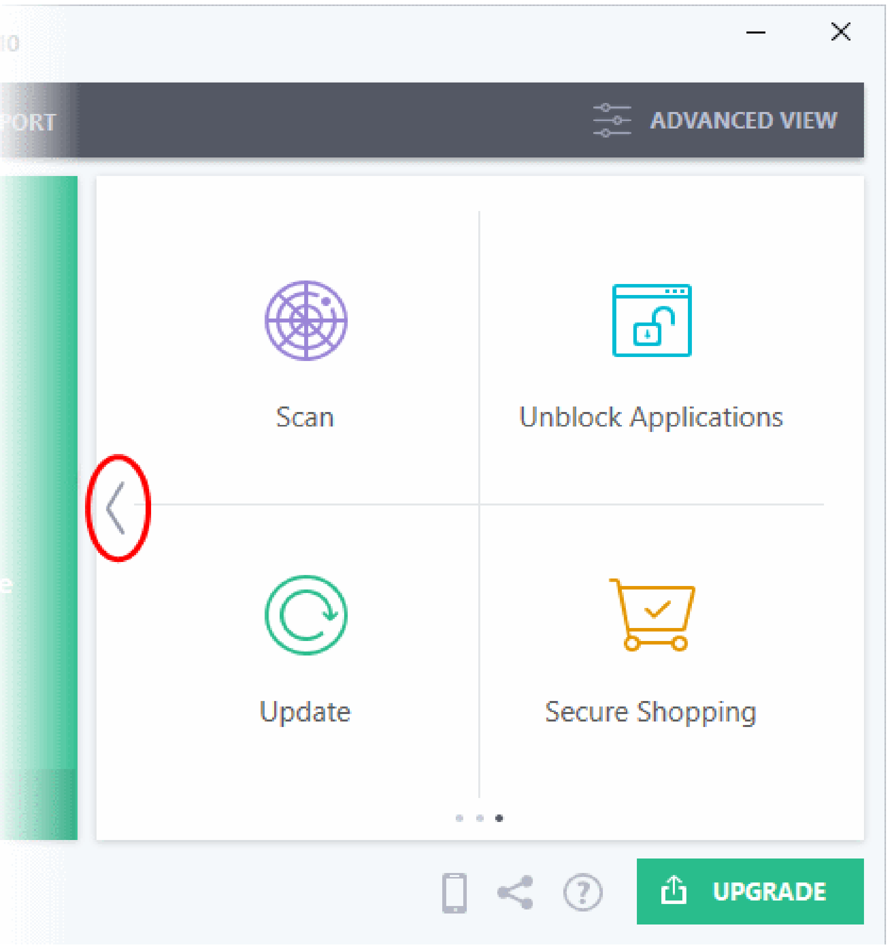
You can easily rectify the issue by clicking the 'FIX IT' button. CIS will automatically take necessary actions to resolve the problem. '**Silent Mode**' and '**Help Window**' are common to both home and tasks screen.

From the 'Basic View' of the home screen you can:

- **Add shortcuts tasks**
- **Manage protection settings**
- **Get live support**

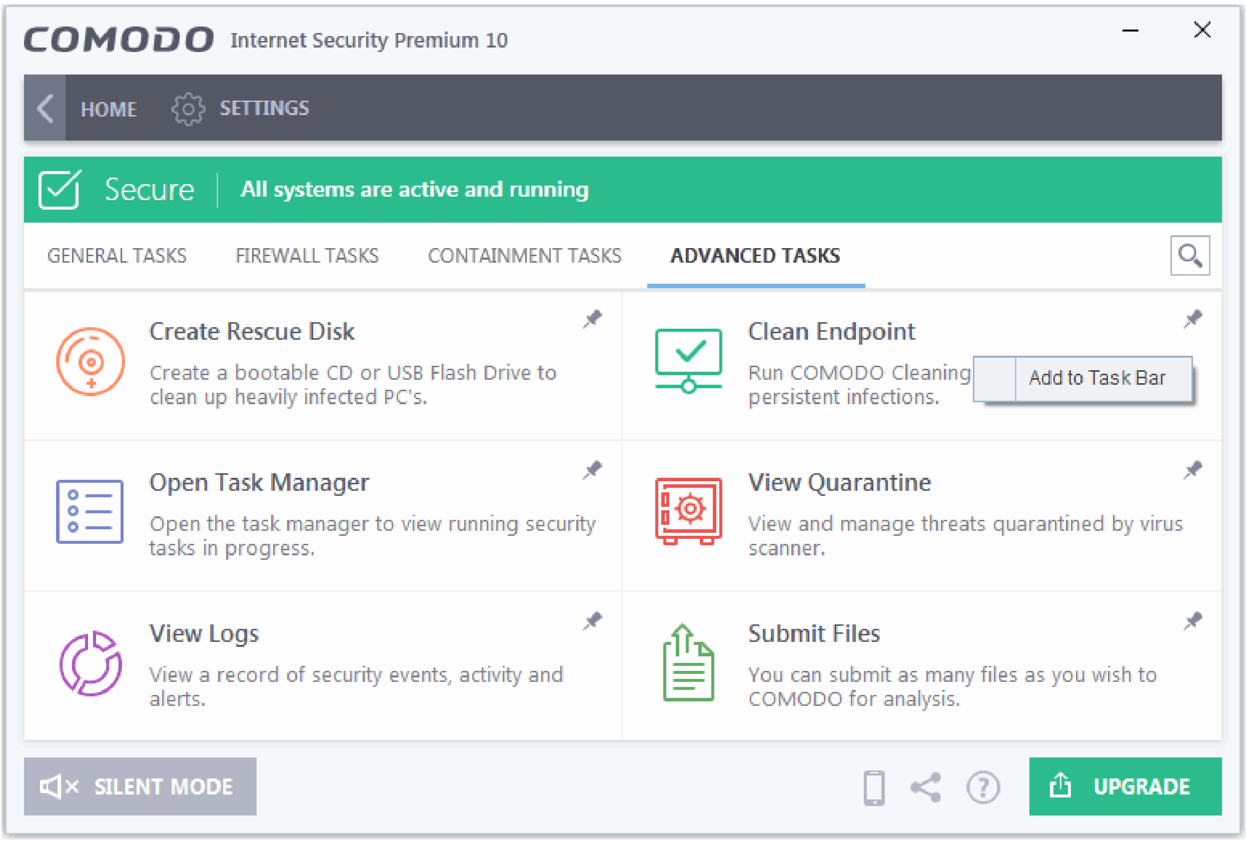
Adding tasks to the home screen

The tasks pane on the right contains a set of shortcuts which will launch common tasks with a single click. The handles at the right and left allow you to scroll through the tasks pane.



You can add tasks to this pane as follows:

- Open the 'Tasks' interface (click the button at top left to switch between the tasks and home screens).
- Click any of the 'General', 'Firewall', 'Containment' or 'Advanced' tabs
- Right-click on the task you wish to add then click 'Add to Task Bar':



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning persistent infections.

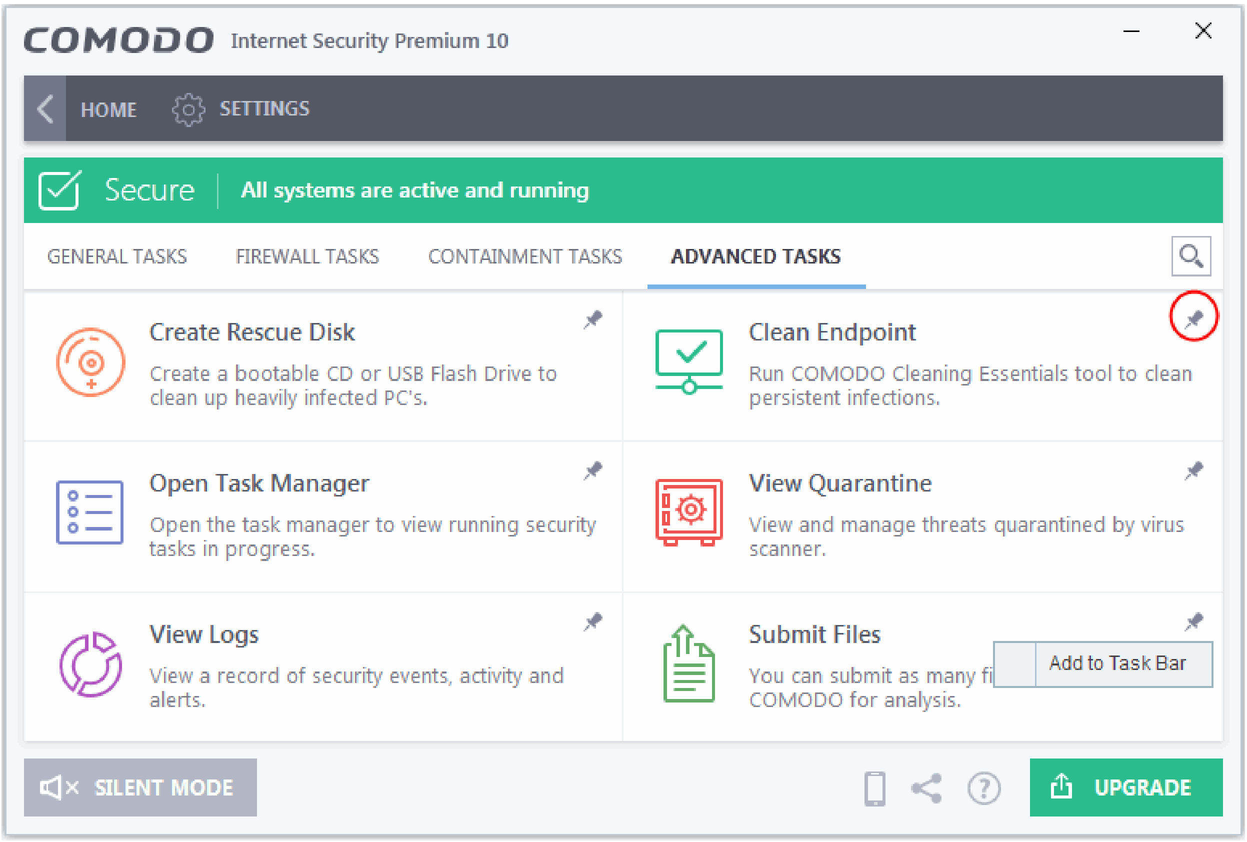
Open Task Manager
Open the task manager to view running security tasks in progress.

View Quarantine
View and manage threats quarantined by virus scanner.

View Logs
View a record of security events, activity and alerts.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

- Alternatively, you can add task shortcuts to the home screen by clicking the 'pin' 📌 button at the top-right of any tile:



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

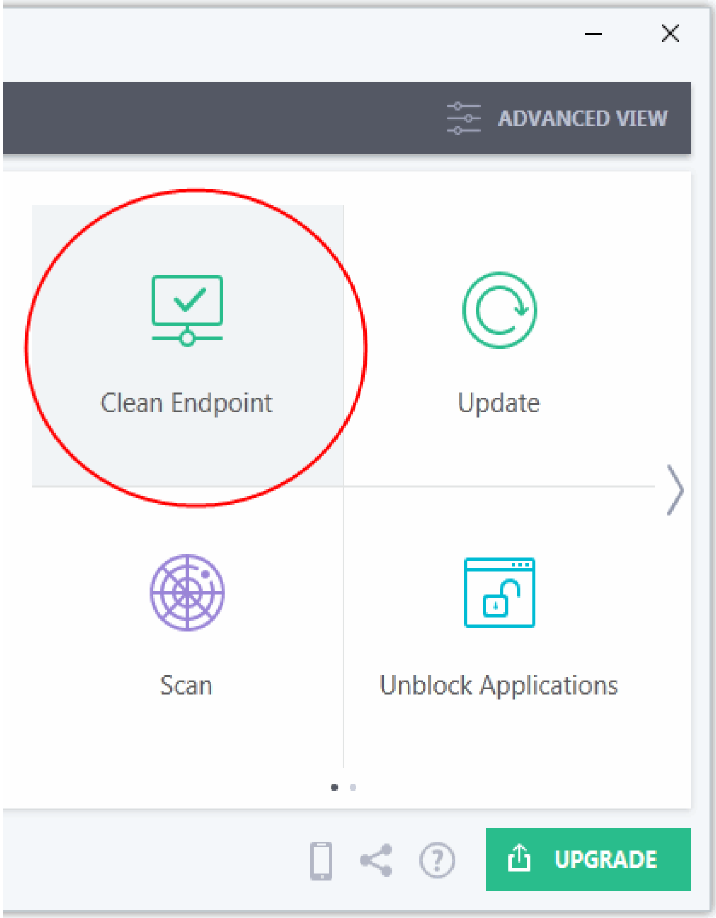
Open Task Manager
Open the task manager to view running security tasks in progress.

View Quarantine
View and manage threats quarantined by virus scanner.

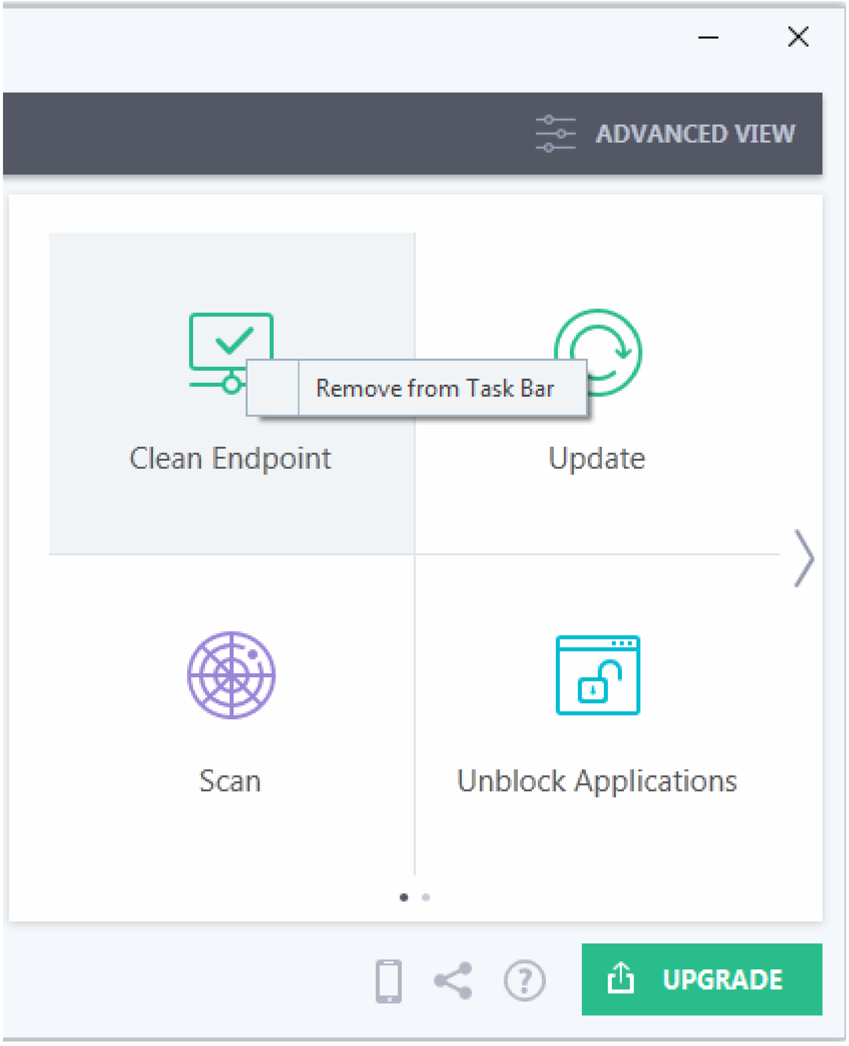
View Logs
View a record of security events, activity and alerts.

Submit Files
You can submit as many fi COMODO for analysis.

- The selected task will be added to the tasks pane.

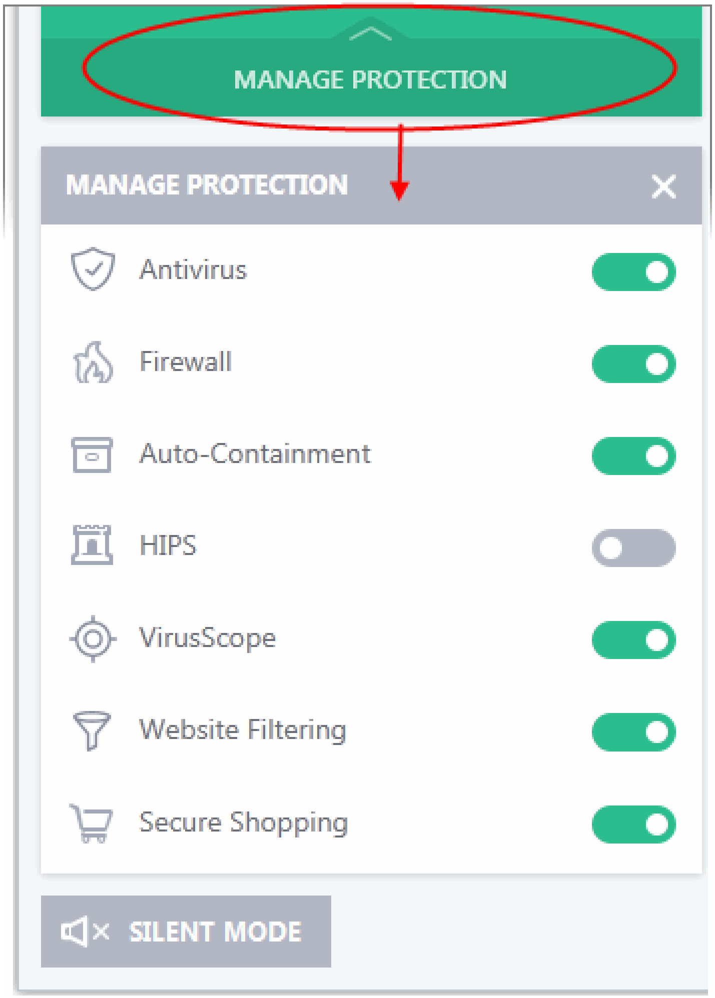


- To remove a task shortcut from the pane, right click on it and choose 'Remove from Task Bar'.



Managing Protection Settings

- Click the 'Manage Protection' button on the home screen to enable or disable various security components.
- Click on any component name to open its dedicated settings screen.



- Use the switch on the right to turn the protection on or off
- Click a component name on the left to open its 'Advanced Settings' screen

See the following sections for more details about each of the protection settings:

- **Antivirus Configuration**
- **Firewall Configuration**
- **Auto-Containment**
- **HIPS Configuration**
- **VirusScope Configuration**
- **Website Filtering**
- **Secure Shopping**

Get Live Support

You can seek the help of GeekBuddy technicians anytime if you require support related to CIS or your computer in general. CIS 'Premium' and 'Pro' users get a free trial of the service.

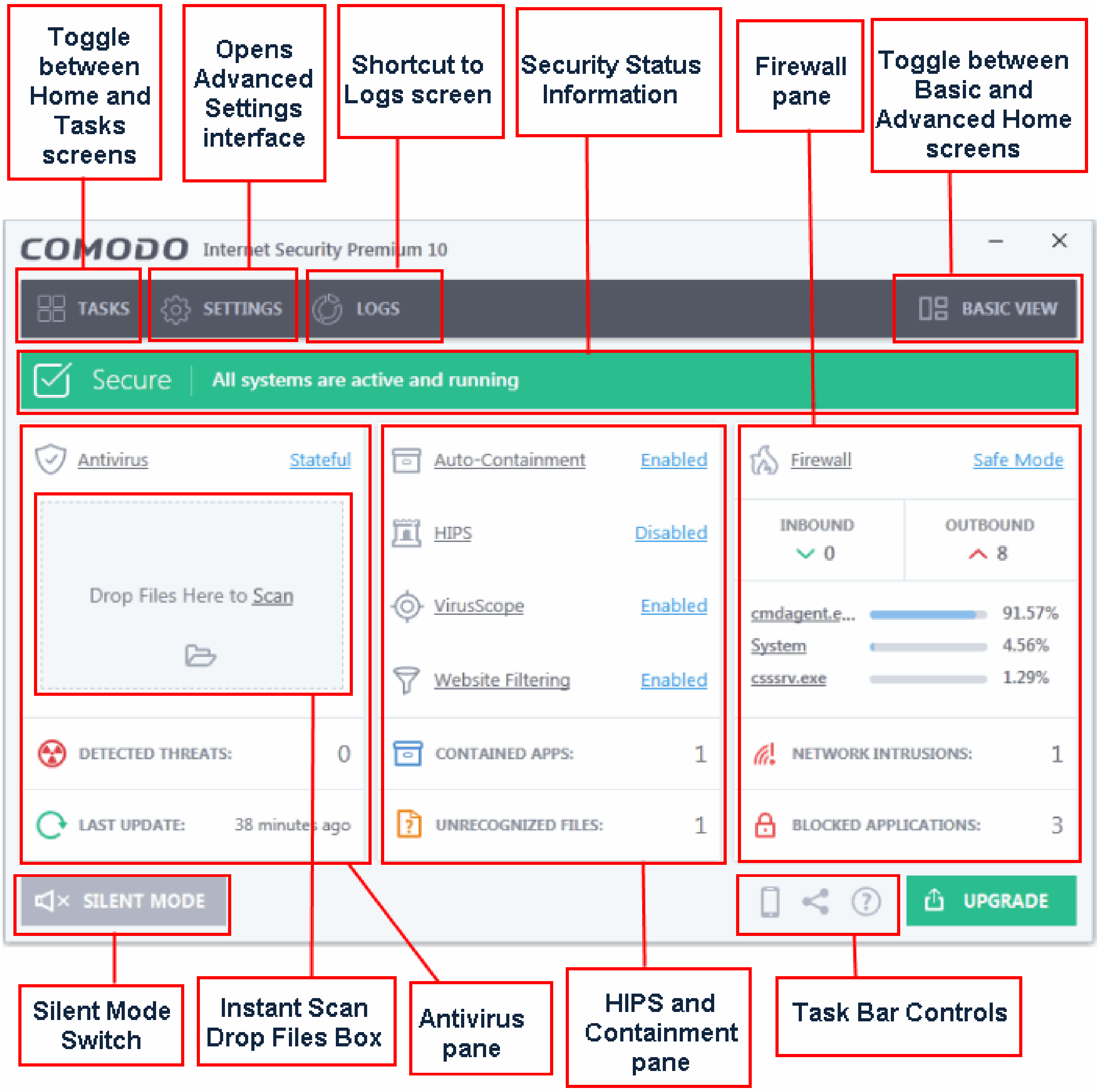
- Click the 'Live Support' link to open the 'Comodo GeekBuddy' chat interface.
- Begin typing your problem. Our technician will attempt to answer any questions you have.

See '**Comodo GeekBuddy**', for more details about live help

Advanced View

The 'Advanced View' of the home screen provides a more finely-detailed view of the security status of each major security component.

Switch to advanced view by clicking the view button at the top-right of the home screen:

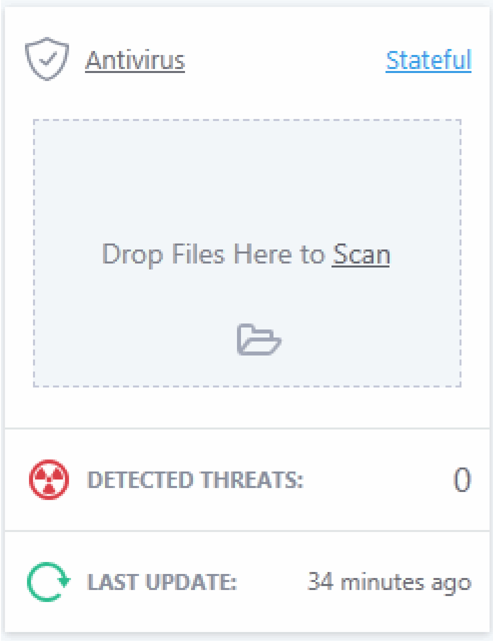


Click on the following links to find out more about each section:

- Antivirus Pane
- HIPS and Containment Pane
- Firewall Pane
- Logs

Antivirus Pane

The Antivirus pane allows you to configure antivirus mode, see when the virus database was last updated, view antivirus logs and instantly scan files and folders.


Antivirus Stateful

Drop Files Here to Scan

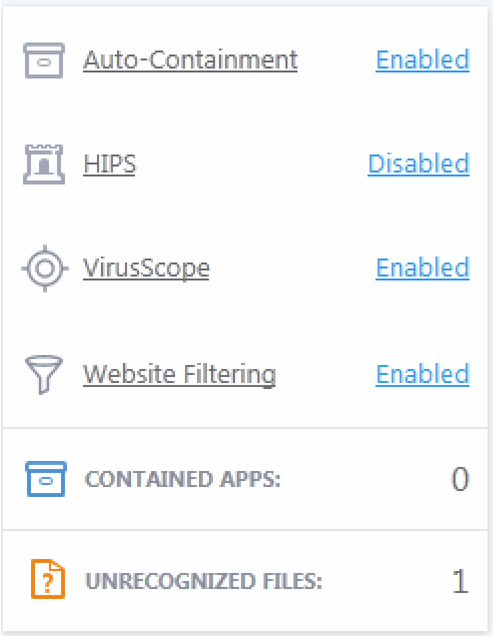
DETECTED THREATS: 0

LAST UPDATE: 34 minutes ago

- **Antivirus -** Displays the current security level of the real-time antivirus scanner. Click on the security mode text to quickly switch between modes. Click 'Antivirus' to open the Realtime Scanner Settings interface. See '**Real-time Scan Settings**' for more details.
- **Last Update -** Displays when the virus database was updated. Click the text link to start the updates again.
- **Detected Threats -** Displays the number of malware threats discovered so far from the start of current session as a link. Clicking this number will open the **Antivirus Logs** panel.
- **Drop Files to Scan -** Drag-and-drop files, folders or even entire drives into this box to instantly scan them. See '**Instantly Scan Files and Folders**' for more details.

HIPS and Containment Pane

The HIPS and Containment pane allows you to quickly configure containment, HIPS, VirusScope and website filtering settings. The bottom of the panel shows the number of unrecognized files and contained applications.


Auto-Containment Enabled

HIPS Disabled

VirusScope Enabled

Website Filtering Enabled

CONTAINED APPS: 0

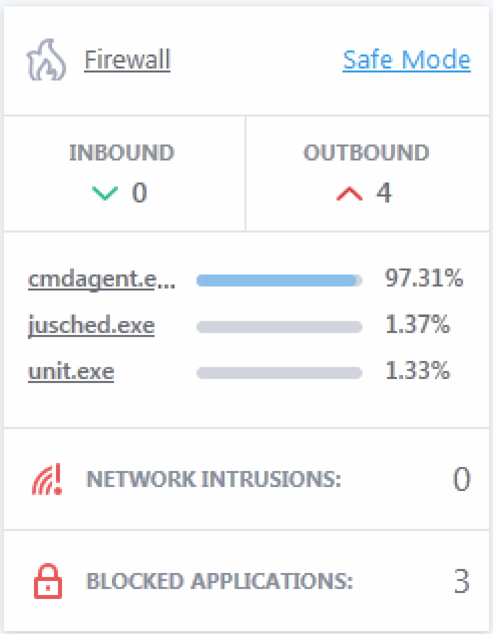
UNRECOGNIZED FILES: 1

- **Auto-Containment -** If enabled, any files with an 'Unknown' trust rating will be automatically run in the container to prevent them from accessing other processes or your personal data. Unknown files are those that are neither 'known-malicious' nor 'known-safe'. Such files are run in the container until their true trust status can be established. Click on the security level itself to change it. Click 'Auto-Containment' to open the 'Auto-Containment Settings' interface. See '**Auto-Containment Rules**' for more details.

- **HIPS -** Click the text of the current HIPS mode to view or modify the mode. Click the word 'HIPS' to open the 'HIPS Settings' interface. See '**HIPS Configuration**' for more details.
- **VirusScope -** Displays whether VirusScope is enabled or not. Click on the security level to change it. Click the work 'VirusScope' to open the 'VirusScope' interface. See '**VirusScope Configuration**' for more details.
- **Contained Apps -** Displays the number of applications that are currently running inside the container. Clicking the number opens the 'Active Processes List (Contained Only)', which provides details of currently contained applications. See '**View Active Process List**' for more details.
- **Unrecognized Files -** Displays the number of unrecognized applications by HIPS that are currently running in the system. Clicking the numbered link beside it will open the 'File List' interface. See '**File List**' for more details.

Firewall Pane

The Firewall pane allows you to configure firewall settings, view the number of inbound and outbound connections and the number of network intrusion attempts blocked by Firewall since the start of current session of CIS.



- **Firewall -** Displays the firewall's current security mode. Click on the level itself to quickly view and modify it. Click on 'Firewall' to open the Firewall Settings interface. See '**Firewall Configuration**' for more details.
- **Inbound / Outbound Connections -** A summary of currently active inbound and outbound connections to and from the system. Clicking on the numbered link will open the View Connections screen. See '**View Active Internet Connections**' for more details.
- **Traffic -** The Traffic area of the pane displays a bar graph showing applications that are currently connected to the internet and are sending or receiving data. The summary also displays the % of total traffic each application is responsible for and the file name of the executable. Clicking on any application name will open the **View Connections** screen.
- **Network Intrusions -** Displays the total number of intrusion attempts blocked by firewall since the start of the current session. Clicking on the numbered link will open the Firewall Logs screen. See '**Firewall Logs**' for more details.
- **Blocked Applications -** Displays the number of applications blocked by Firewall. Clicking on the numbered

link will open the 'Unblock Applications' screen. See **'Allow or Block Internet Access to Applications Selectively'** for more details.

Logs

Clicking the 'Logs' link at the top of the home screen will open the 'View Logs' interface. This is a shortcut link for the 'View Logs' menu available in the 'Tasks' screen > Advanced Tasks interface. See '**View CIS Logs**' for more details.

Silent Mode

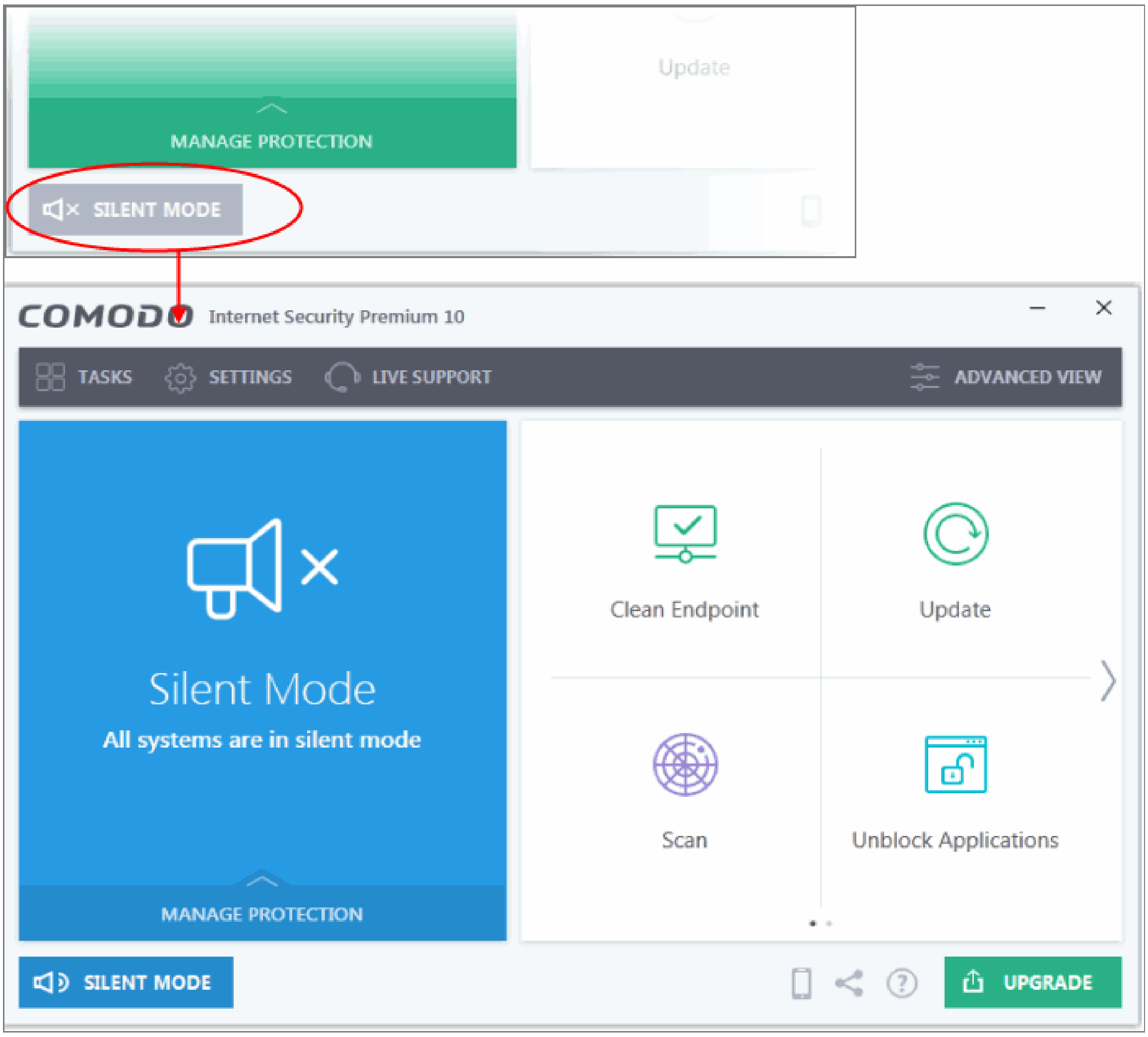
Silent Mode enables you to user your system without interruptions or alerts. Operations that could interfere with your work are either suppressed or postponed.

In silent mode:

- HIPS/Firewall alerts are suppressed.
- AV database updates and scheduled scans are postponed until the silent mode is switched off;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

To switch to Silent mode

- Click the 'Silent Mode' switch at the bottom left of the 'Home' screen



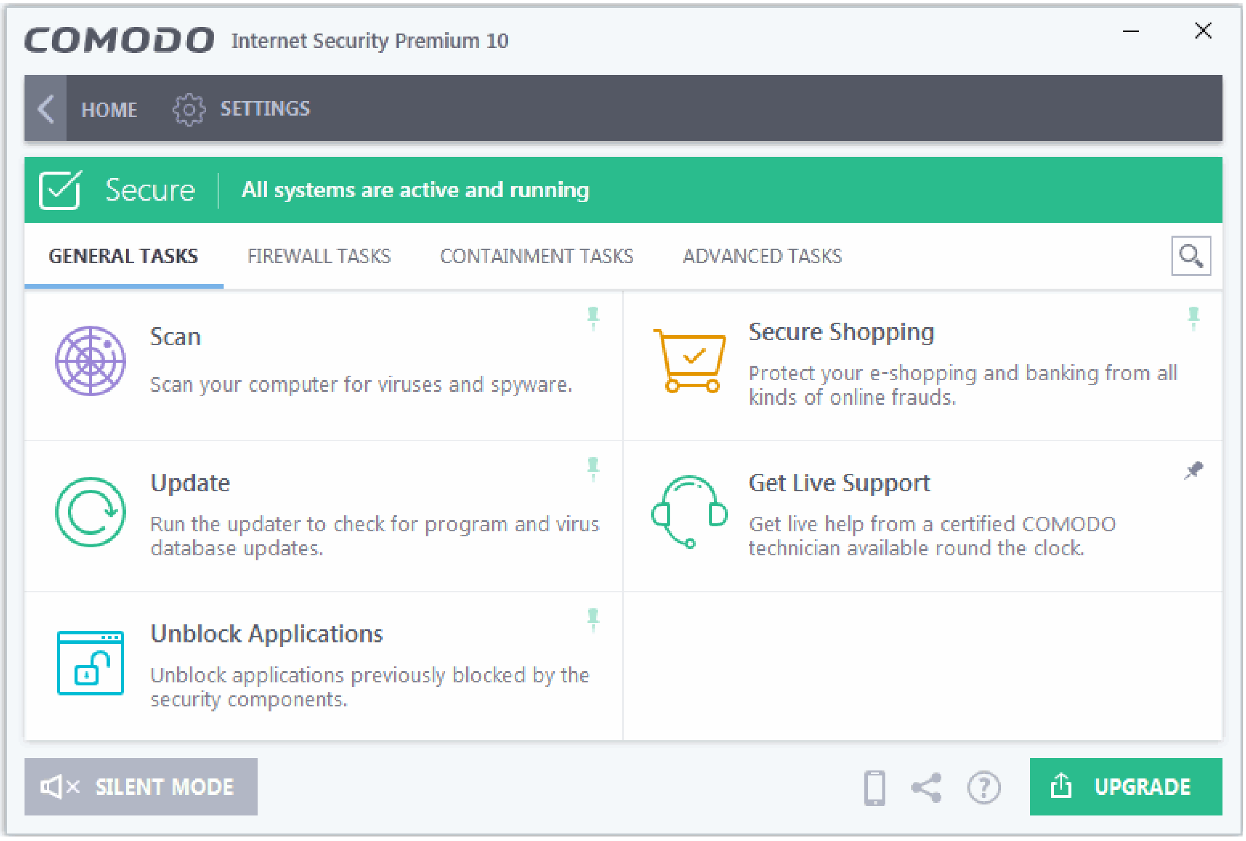
- Deactivate 'Silent Mode' to resume alerts and notifications.

Upgrade

Clicking the 'Upgrade' button leads to the purchase page of CIS Pro and Complete, which in addition to the features available in Comodo Internet Security has more features such as cloud backup, TrustConnect, product warranty and more.

1.4.2. The Tasks Interface

The items in the 'Tasks' area allow you to configure every aspect of Comodo Internet security.

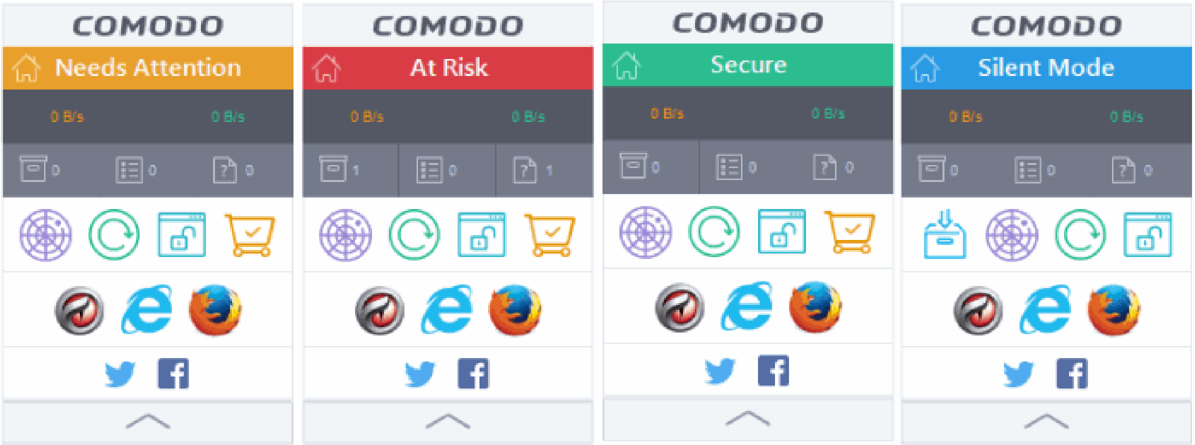

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
SILENT MODE
UPGRADE

Tasks are broken down into four main categories. Click the following links for more details on each:

- **General Tasks** - Run antivirus scans, update the virus database, unblock Applications, Secure Shopping and Get Live support. See '**General Tasks**' for more details.
- **Firewall Tasks** - Allow or Block applications, Manage ports, Manage networks , Restore Network Activity, View Connections, Stealth Ports and configure advanced firewall settings. See '**Firewall Tasks**' for more details.
- **Containment Tasks** - Run applications in a secure virtual environment and configure containment settings. See '**Containment Tasks**' for more details.
- **Advanced Tasks** - Create a boot disk to clean up highly infected systems; install other Comodo software like KillSwitch and Cleaning Essentials; submit files to Comodo for analysis and gain access to the 'Advanced Settings' interface. See '**Advanced Tasks**' for more details.

1.4.3. The Widget

- The Widget is a handy control that provides at-a-glance information about your security status, speed of outgoing and incoming traffic and the number of active processes.
- The Widget starts automatically with CIS unless it is disabled from the **System Tray Icon** or in the '**User Interface**' of **General Settings**.
- Right-clicking on the widget allows you to enable or disable CIS components and configure various settings. The menu is similar to the one available if you right-click on the system tray icon. See '**The System Tray Icon**' for more details.

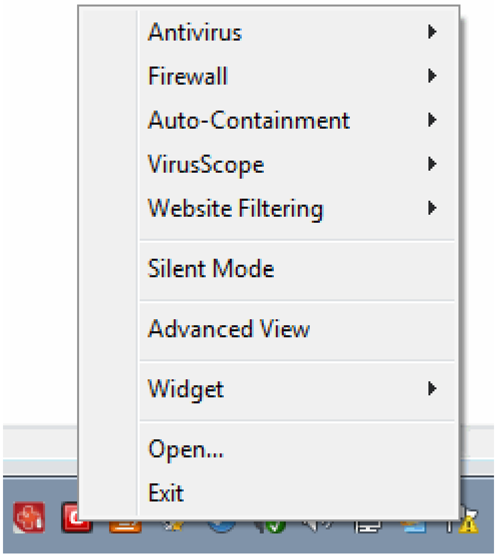


- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' will open the appropriate interface for you to take action.
- The second row displays information about incoming and outgoing network traffic. The network traffic row is displayed only if 'Show Traffic pane' under 'Widget options of CIS tray icon or Widget right click menu is enabled. See **The System Tray Icon** for more details. (***Default = Enabled***)
- The third row tells you about various CIS processes:
  - The first button displays the number of programs/processes that are currently running in the container. Clicking the button opens the Active Process List (Contained Only)' interface, which allows you to identify and terminate unnecessary processes. Clicking the 'More' button in this interface will open the KillSwitch application. If KillSwitch is not yet installed, clicking this button will prompt you to download the application. See **View Active Process List** and **Identify and Kill Unsafe Processes** for more details.
  - The second button tells you how many CIS tasks are currently running. Click the button to open the '**Task Manager**' interface.
  - The third button displays how many 'Unrecognized' files have been added to the **File List** and are pending submission to Comodo for analysis. Click the button to open the '**File List**' interface.

  The status row is displayed only if 'Show Status Pane' is enabled under 'Widget options'. Right-click on the widget or the CIS tray icon to view this setting. See '**The System Tray Icon**' for more details. ***(Default = Enabled)***
- The fourth row contains shortcuts for the common tasks shown on the right of the CIS home screen. Click a shortcut on the widget to run the task. The 'Common Tasks' row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of the CIS tray icon. See '**The System Tray Icon**' for more details. (***Default = Enabled***)
- The fifth row shows the browsers installed on your computer. Click a browser icon to open the browser inside the container for a secure browsing session. You can tell the browser is running in the container because it will have a green border around it. See '**Running an application inside the container**' for more details. The browsers row is only displayed if 'Show Browsers Pane' is enabled under 'Widget' options. Right-click on the widget or the CIS tray icon to view this setting. See '**The System Tray Icon**' for more details. (***Default = Enabled***)
- The last row on the widget provides links to social networking sites. This row is only displayed if 'Show Connect Pane' is enabled under 'Widget' options. Right-click on the CIS tray icon to view this setting. Alternatively, right-click the widget to view the options. See '**The System Tray Icon'** for more details. (***Default = Enabled***)
- You can expand or collapse the 'Widget' by clicking the arrow at the bottom.

1.4.4. The System Tray Icon

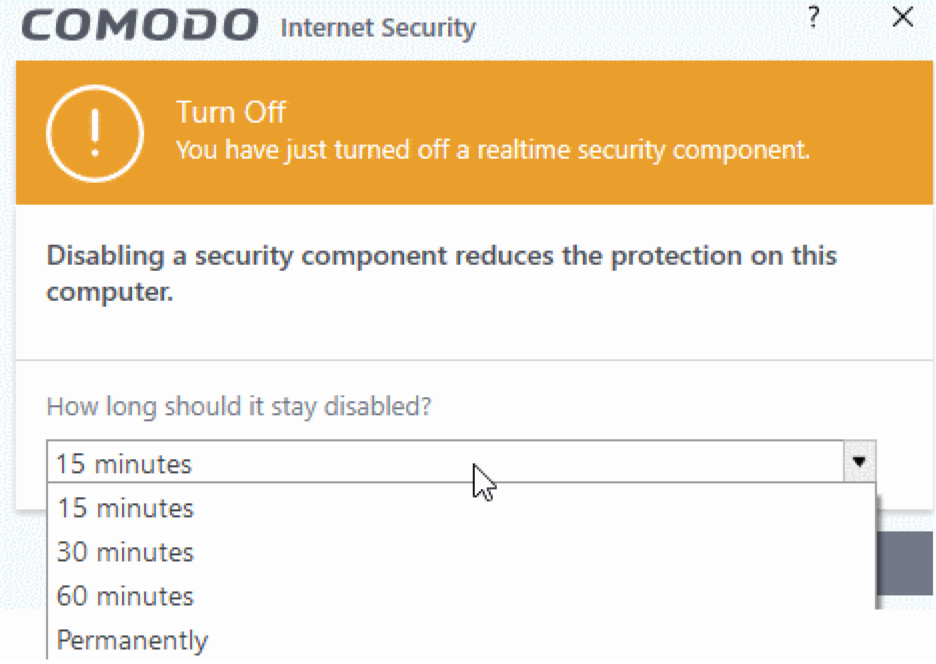
- Double-click the tray icon C to quickly open the CIS interface.
- Right-click on the tray icon to enable or disable various security settings:



The options available for the Antivirus, Firewall, VirusScope, Auto-Containment, HIPS and Website Filtering menu-items depend on whether you are using **Basic View** or **Advanced View**.

Basic View	Advanced View
Antivirus - You can enable or disable Real-time antivirus scan. **Firewall -** You can enable or disable Firewall. **Auto-Containment -** You can enable or disable Auto-Containment. See '**Auto-Containment Rules**' for more details. **VirusScope -** You can enable or disable VirusScope. **Website Filtering -** You can enable or disable Website Filtering.	**Antivirus -** Options available are On Access, Stateful and Disabled. Refer to **Antivirus Pane** for more details. Clicking 'Settings' from the options will open the Realtime Scanner Settings interface. See '**Real-time Scan Settings**' for more details. **Firewall -** Options available are Block All, Custom Ruleset, Safe Mode, Training Mode and Disabled. Clicking 'Settings' from the options will open the Firewall Settings interface. See **Firewall Settings** for more details. **Auto-Containment -** Clicking 'Settings' from the options will open the Auto-Containment settings interface. See **Auto-Containment Rules** for more details. **HIPS -** Options available are Paranoid Mode, Safe Mode, Training Mode and Disabled. Clicking 'Settings' from the options will open the HIPS Settings interface. See **HIPS Settings** for more details. **VirusScope -** Options available are Enabled, Disabled. Clicking 'Settings' from the options will open the VirusScope interface. See **VirusScope Configuration** for more details. **Website Filtering -** You can enable or disable website filtering. Clicking 'Settings' from the options will open the website filtering settings interface. See **Website Filtering Rules** for more details

If you disable any of the antivirus, the firewall or the auto-containment from the right-click menu, then the security info bars on the main interface and the 'Widget' will turn red. You will also see a pop-up warning which allows you to specify how long the feature should remain disabled:



COMODO Internet Security

Turn Off

You have just turned off a realtime security component.

Disabling a security component reduces the protection on this computer.

How long should it stay disabled?

15 minutes

15 minutes
30 minutes
60 minutes
Permanently

- Select the period and click 'OK'.

Unless you have selected 'Permanently', the security component will be automatically re-enabled after the set time period. You can, of course, manually re-enable the component at any time by right-clicking the tray icon and selecting 'Enable' for the component in question.

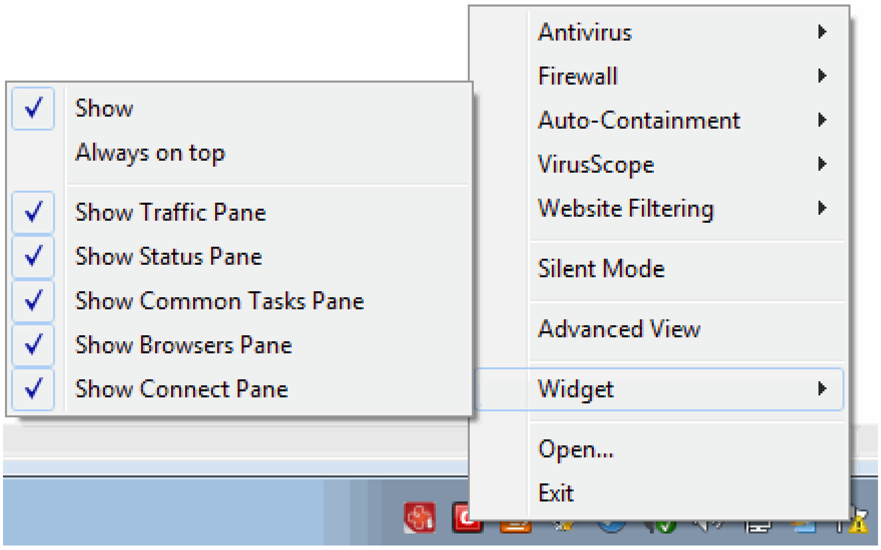
- **Silent Mode** - Switch CIS to Silent Mode if you do not want to have any interruptions from various CIS alerts. Operations that could potentially interrupt your work are suppressed or postponed.

  In silent mode:

  - HIPS/Firewall alerts are suppressed as if they are in training mode;
  - AV database updates and scheduled scans are postponed until the silent mode is switched off;
  - Automatic isolation of unknown applications and real-time virus detection are still functional.

  Deactivate Silent Mode to resume alerts and scheduled scans.

- **Advanced View** - Switches the Home Screen between '**Basic View**' and '**Advanced View**'.
- **Widget** - Select whether the '**Widget**' is to be displayed and which widget components are to be included:



- **Show**: Toggles the widget between on and off (***Default = Enabled***)
- **Always on top**: Displays the widget on top of all windows currently running on your computer. (***Default = Enabled***)
- **Show Traffic Pane**: Displays the network traffic row on the widget. (***Default = Enabled***)
- **Show Status Pane**: Displays the security status tab at the top of the widget. (***Default = Enabled***)
- **Show Common Tasks Pane**: Displays the row containing shortcuts to common CIS tasks. (***Default = Enabled***)
- **Show Browsers Pane**: Displays the row containing shortcuts to your installed browsers. (***Default = Enabled***)
- **Show Connect Pane**: Displays the row containing the shortcuts to social networking sites. (***Default = Enabled***)

- **Open -** Opens the CIS interface.
- **Exit** - Closes the CIS application.

1.5. Understanding Security Alerts

- **Alerts Overview**
  - **Alert Types**
  - **Severity Levels**
  - **Descriptions**
- **Antivirus Alerts**
- **Firewall Alerts**
- **HIPS Alerts**
  - **Device Driver Installation and Physical Memory Access Alerts**
  - **Protected Registry Key Alerts**
  - **Protected File Alerts**
- **Containment Alerts**
  - **Containment Notification**
  - **Elevated Privilege Alerts**
- **VirusScope Alerts**
- **Secure Shopping Alert**

Alerts Overview

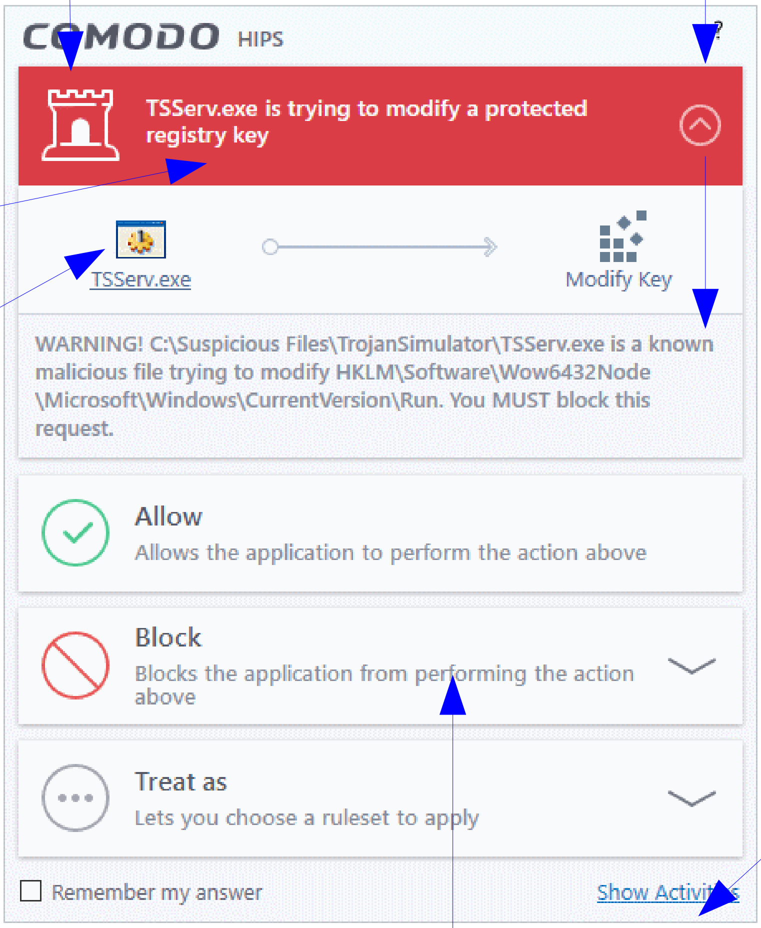
CIS alerts warn you about security related activities at the moment they occur. Each alert contains information about a particular issue so you can make an informed decision about whether to allow or block it. Alerts also let you specify how CIS should behave in future when it encounters activities of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

Type of Alert

Can be Antivirus, Firewall, HIPS, Containment, VirusScope or Secure Shopping

Description of activity or connection attempt

Clicking the handle opens the **alert description** which contains advice about how to react to the alert



COMODO HIPS

TSServ.exe is trying to modify a protected registry key

WARNING! C:\Suspicious Files\TrojanSimulator\TSServ.exe is a known malicious file trying to modify HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run. You MUST block this request.

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

☐ Remember my answer

Color indicates severity of the Alert

Firewall, HIPS and Containment alerts are color coded to indicate risk level

High visibility icons quickly inform you which applications and techniques are involved in an alert. Clicking the name of the executables here opens a window containing more information about the application in question

Click 'Show Activities' to open a list of activities performed by the process

Click these options to allow, block or otherwise handle the request

Alert Types

Comodo Internet Security alerts come in six 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 **Antivirus is enabled** and the option '**Do not show antivirus alerts**' is disabled in **Real-time Scanner Settings**.
- **Firewall Alerts** - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the **Firewall is enabled** and the option '**Do not show popup alerts**' is disabled in **Firewall Settings**.
- **HIPS Alerts** - Shown whenever an application attempts an unauthorized action or tries to access

protected areas. HIPS alerts will only be generated if **HIPS is** enabled and **Do NOT show popup** alerts is disabled.

- **Containment Alerts** (including **Elevated Privilege Alerts**) - Shown whenever an application tries to modify operating system or related files and when CIS automatically contains an unrecognized file. Containment alerts will be shown only if privilege elevation alerts are enabled in **Containment Settings**.
- **VirusScope Alerts** - Shown whenever a currently running process attempts to take suspicious actions. VirusScope alerts allow you to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a VirusScope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. VirusScope Alerts will be displayed only when **VirusScope is enabled** under Advanced Settings.
- **Secure Shopping Alerts** - Shown whenever a user opens a website that is configured to invoke an alert in the rules. Secure Shopping Alerts will be shown only when the **protection setting** is enabled.

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.

Note: This section is concerned only with the security alerts and notifications generated by the Antivirus, Firewall, HIPS, VirusScope, Auto-Containment and Secure Shopping components of CIS. See **Comodo Message Center notifications**, **Notification Messages** and **Information Messages**, for other types of alerts.

Severity Level

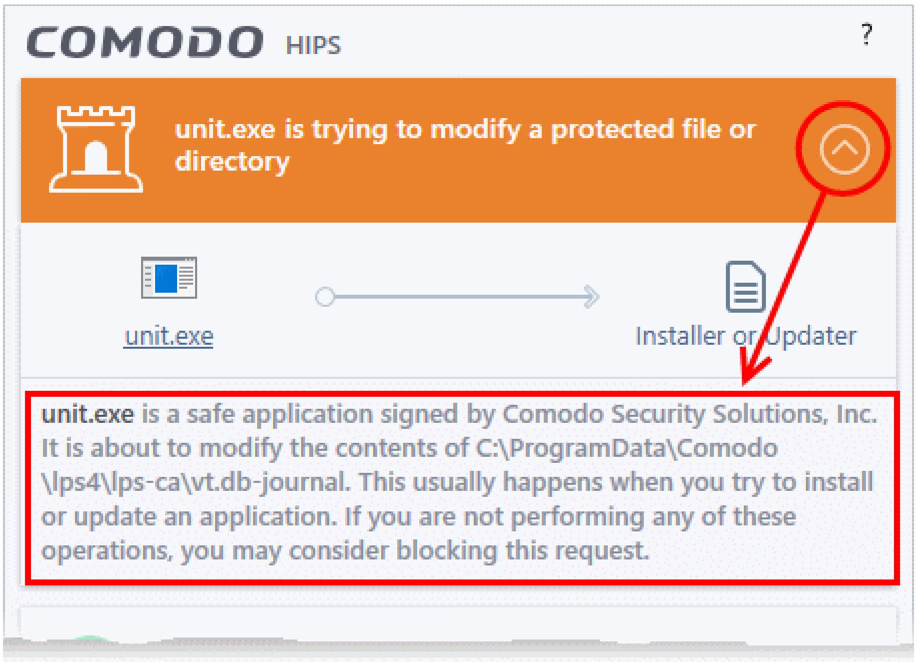
The title bar at the top of each alert is color coded according to the risk level presented by the activity or request.

- **Yellow bar** - Low Severity - In most cases, you can safely approve these requests. The 'Remember my answer' option is automatically pre-selected for safe requests
- **Orange bar** - Medium Severity - Carefully read the information in the alert description area before making a decision. These alerts could be the result of a harmless process by a trusted program or indicative of a malware attack. If you know the application to be safe, then it is usually okay to allow the request. If you do not recognize the application performing the activity or connection request then you should block it.
- **Red bar** - High Severity - These alerts indicate highly suspicious behavior that is consistent with the activity of a Trojan horse, virus or other malware program. Carefully read the information provided when deciding whether to allow it to proceed.

Note: Antivirus alerts are not ranked in this way. They always appear with a red bar.

Alert Description

The description is a summary of the nature of the alert and can be revealed by clicking the handle as shown:



unit.exe is a safe application signed by Comodo Security Solutions, Inc. It is about to modify the contents of C:\ProgramData\Comodo\lps4\lps-ca\vt.db-journal. This usually happens when you try to install or update an application. If you are not performing any of these operations, you may consider blocking this request.

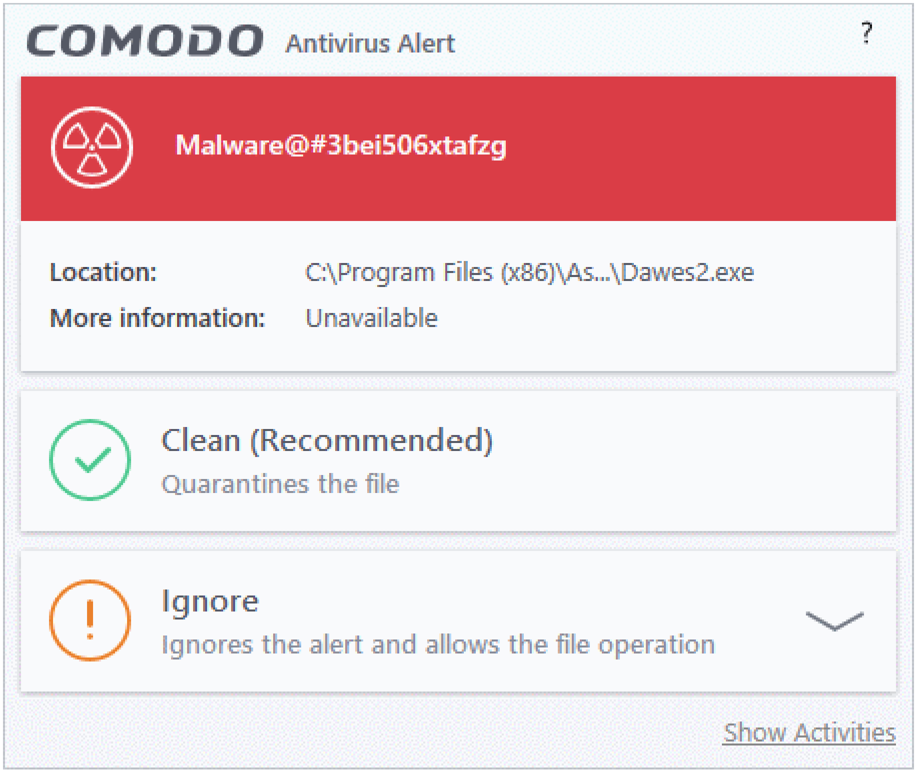
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

Now that we've outlined the basic construction of an alert, let's look at how you should react to them.

Answering an Antivirus Alert

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

Note: Antivirus alerts will be displayed only if the option 'Do not show antivirus alerts' is disabled. If this setting is enabled, **antivirus notifications** will be displayed. This option is found under 'Settings > Antivirus > Realtime Scan'. See **Real-time Scan Settings** for more details.



COMODO Antivirus Alert

Malware@#3bei506xtafzg

Location: C:\Program Files (x86)\As...\Dawes2.exe

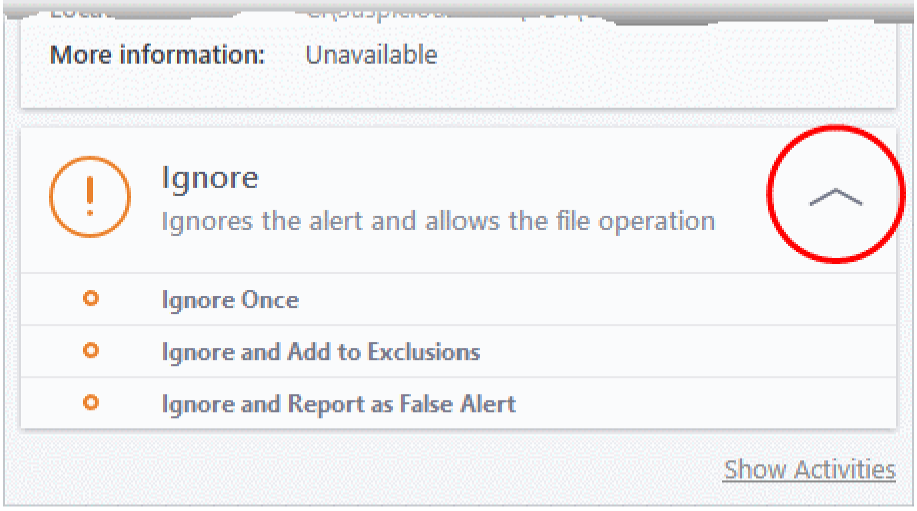
More information: Unavailable

Tip: Clicking the 'Show Activities' link at the bottom right will open the **Process Activities List dialog**. The 'Process Activities' dialog will display the list activities of the processes run by the application.

The 'Show Activities' link is available only if VirusScope is enabled under **Settings> VirusScope**. If none of the processes associated with the infected application has started before the alert is generated, the 'Show Activities' link is disabled and will not open the Process Activities List dialog.

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. See **Manage Quarantined Items** for more details on quarantined files.
- **Ignore -** Allows the process to run and does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:



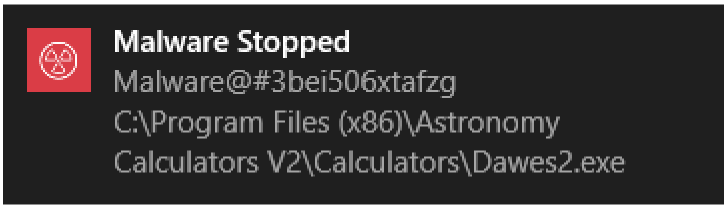
More information: Unavailable

Ignore
Ignores the alert and allows the file operation
Ignore Once
Ignore and Add to Exclusions
Ignore and Report as False Alert
Show Activities

- **Ignore Once** -The file is allowed to run this time only. If the file attempts to execute on future occasions, another antivirus alert is displayed.
- **Ignore and Add to Exclusions** - The file is allowed to run and is moved to the '**Exclusions**' list - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- **Ignore and Report as a False Alert** - If you are sure that the file is safe, select 'Ignore and Report as a False Alert'. CIS will then submit this file to Comodo for analysis. If the false-positive is verified (and the file is trustworthy), it will be added to the Comodo safe list.

Antivirus Notification

If you have chosen to not to show Antivirus Alerts through '**Settings**' **>** '**Realtime Scanner Settings**' by leaving the option 'Do not show antivirus alerts' enabled (***default=enabled***) and if CIS identifies a virus or other malware in real time, it will immediately block malware and provide you with instant on-screen notification:

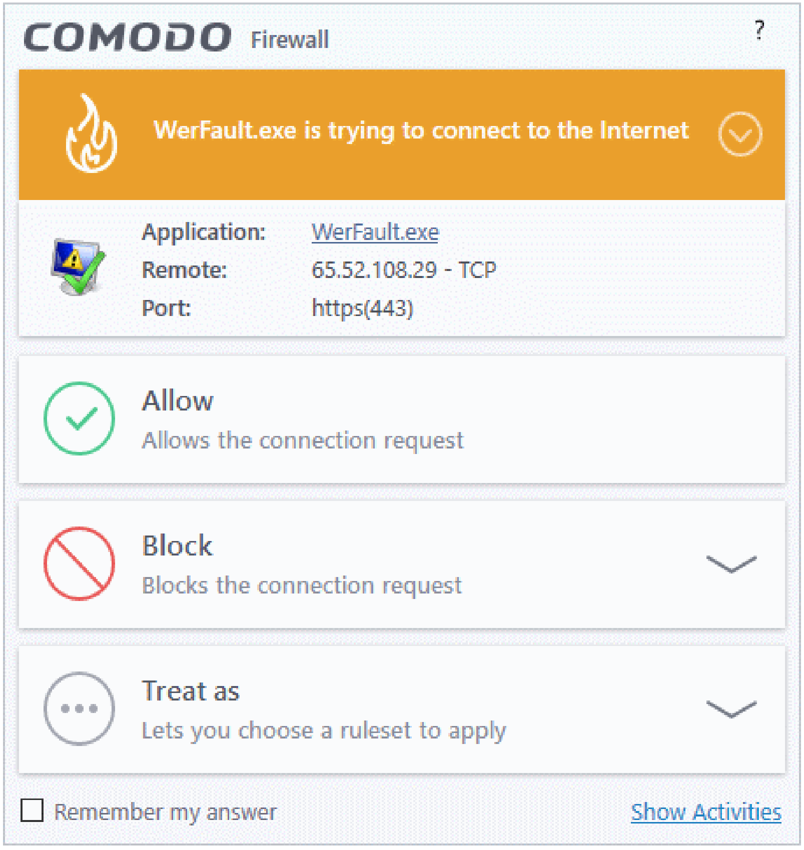


Malware Stopped
Malware@#3bei506xtafzg
C:\Program Files (x86)\Astronomy Calculators V2\Calculators\Dawes2.exe

Please note that these antivirus notifications will be displayed only when 'Do not show antivirus alerts' check box in '**Antivirus**' > '**Real-time Scan settings**' screen is selected *and* 'Show notification messages' check box is enabled in '**Settings**' **>** '**User Interface**' screen.

Answering Firewall Alerts

CIS generates a firewall alert when it detects unauthorized network connection attempts or when traffic runs contrary to one of your application or global rules. Each firewall alert allows you to set a default response that CIS should automatically implement if the same activity is detected in future. The followings steps will help you answer a Firewall alert:



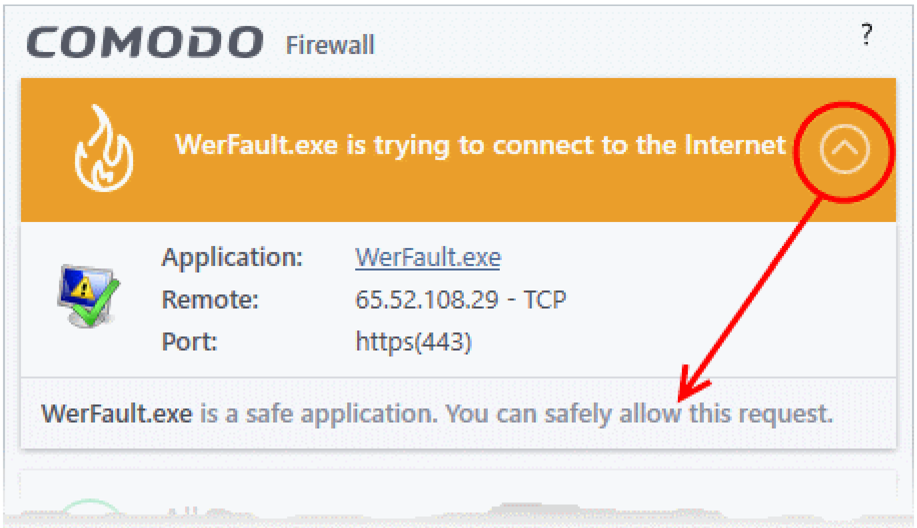
WerFault.exe is trying to connect to the Internet

Application: WerFault.exe
Remote: 65.52.108.29 - TCP
Port: https(443)

Allow
Allows the connection request
Block
Blocks the connection request
Treat as
Lets you choose a ruleset to apply
□ Remember my answer
Show Activities

Tip: Clicking the 'Show Activities' link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

The 'Show Activities' link is available only if VirusScope is enabled under '**Settings**' **>** '**VirusScope**'. If none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the 'Show Activities' link is disabled and will not open the Process Activities List dialog.



WerFault.exe is trying to connect to the Internet

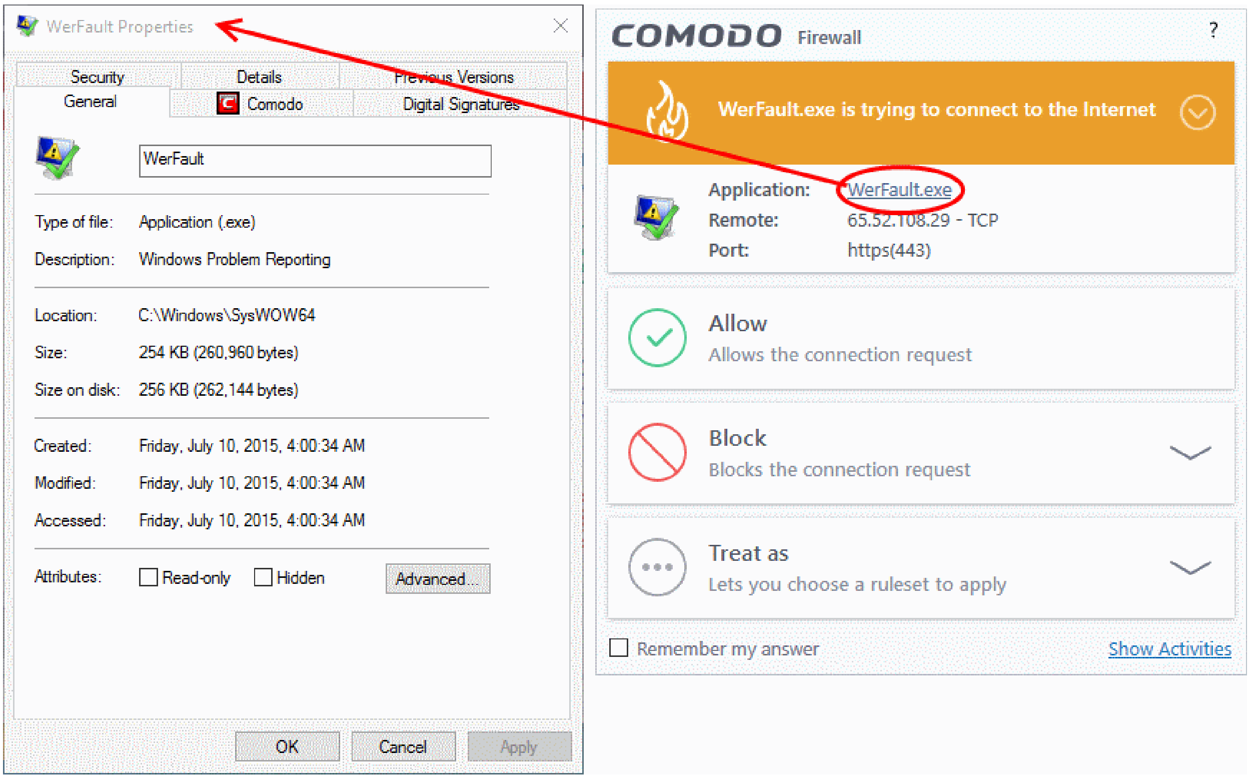
Application: WerFault.exe
Remote: 65.52.108.29 - TCP
Port: https(443)

WerFault.exe is a safe application. You can safely allow this request.

1. Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized you are informed of this.

   If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.

   In all cases, clicking on the name of the application opens a properties window that can help you determine whether or not to proceed:



WerFault

Type of file: Application (.exe)

Description: Windows Problem Reporting

Location: C:\Windows\SysWOW64

Size: 254 KB (260,960 bytes)

Size on disk: 256 KB (262,144 bytes)

Created: Friday, July 10, 2015, 4:00:34 AM

Modified: Friday, July 10, 2015, 4:00:34 AM

Accessed: Friday, July 10, 2015, 4:00:34 AM

Attributes: □ Read-only □ Hidden

WerFault.exe is trying to connect to the Internet

Application: WerFault.exe

Remote: 65.52.108.29 - TCP

Port: https(443)

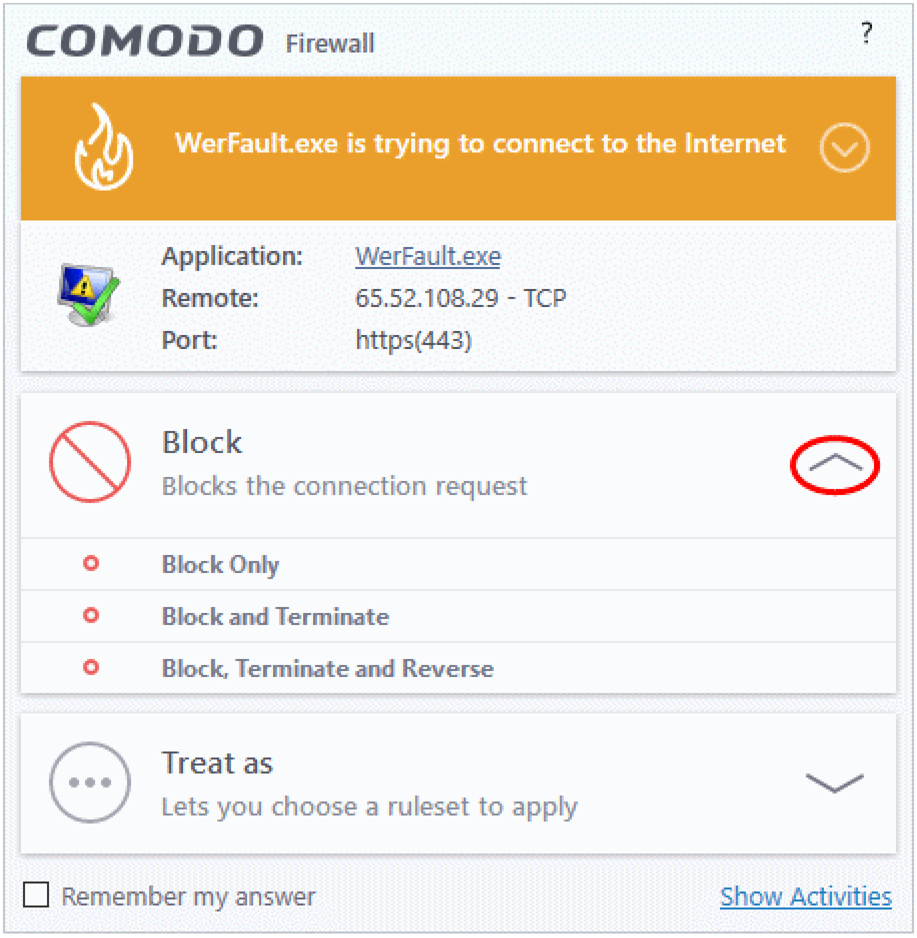
Allow
Allows the connection request

Block
Blocks the connection request

Treat as
Lets you choose a ruleset to apply

□ Remember my answer

If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand the alert, you can choose to 'Block' the connection (connection is not allowed to proceed), 'Block and Terminate' (connection is not allowed to proceed and the process/application that made the request is shut down) or 'Block, Terminate and Reverse' (connection is not allowed to proceed, the process/application that made the request is shut down and the changes made by the process/application to other files/processes in the system will be rolled back).



COMODO Firewall

WerFault.exe is trying to connect to the Internet

Application: WerFault.exe
Remote: 65.52.108.29 - TCP
Port: https(443)

Block
Blocks the connection request

- Block Only
- Block and Terminate
- Block, Terminate and Reverse

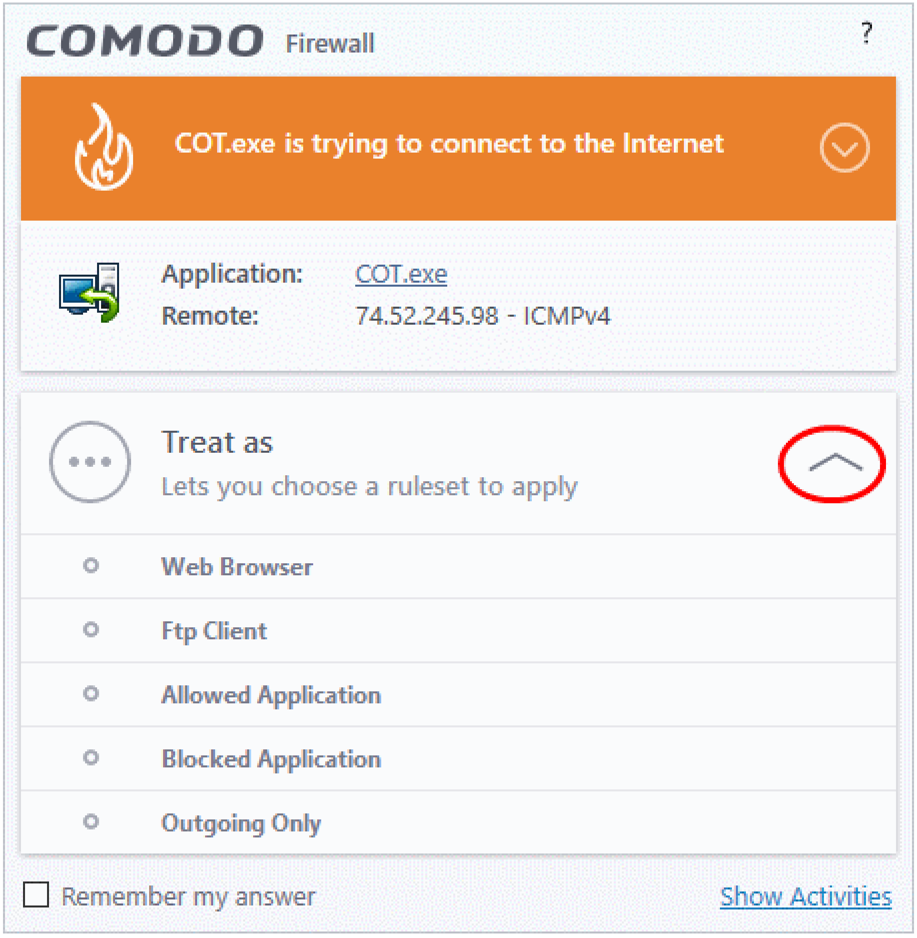
Treat as
Lets you choose a ruleset to apply

□ Remember my answer

Show Activities

Note: 'Block, Terminate and Reverse' option will be available only if VirusScope is enabled under '**Settings**' **>** '**VirusScope**'. Also, if none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the 'Block, Terminate and Reverse' option will not be available.

2. If you are sure that it is one of your everyday application, try to use the '**Treat As**' option as much as possible. This allows you to deploy a **predefined firewall ruleset** on the target application. For example, you may choose to apply the policy **Web Browser** to the known and trusted applications like 'Comodo Dragon', 'Firefox' and 'Google Chrome'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application.



COMODO Firewall ?

COT.exe is trying to connect to the Internet

Application: COT.exe

Remote: 74.52.245.98 - ICMPv4

Treat as

Lets you choose a ruleset to apply

○ Web Browser

○ Ftp Client

○ Allowed Application

○ Blocked Application

○ Outgoing Only

□ Remember my answer

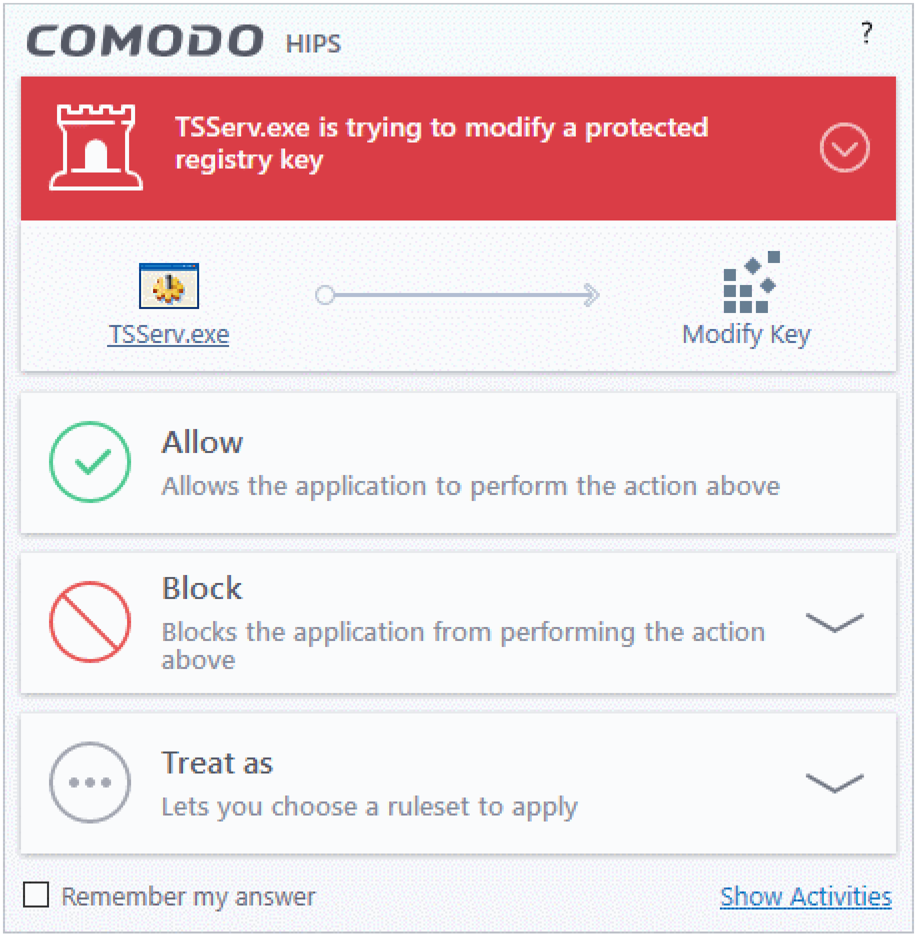
Show Activities

Remember to select '**Remember My Answer**' for ruleset to be created for the application and applied in future.

3. If the Firewall alert reports a behavior, consistent with that of a malware in the security considerations section, then you should block the request AND select '**Remember My Answer**' to make the setting permanent.

Answering HIPS Alerts

Comodo Internet Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:



COMODO HIPS ?

TSServ.exe is trying to modify a protected registry key

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

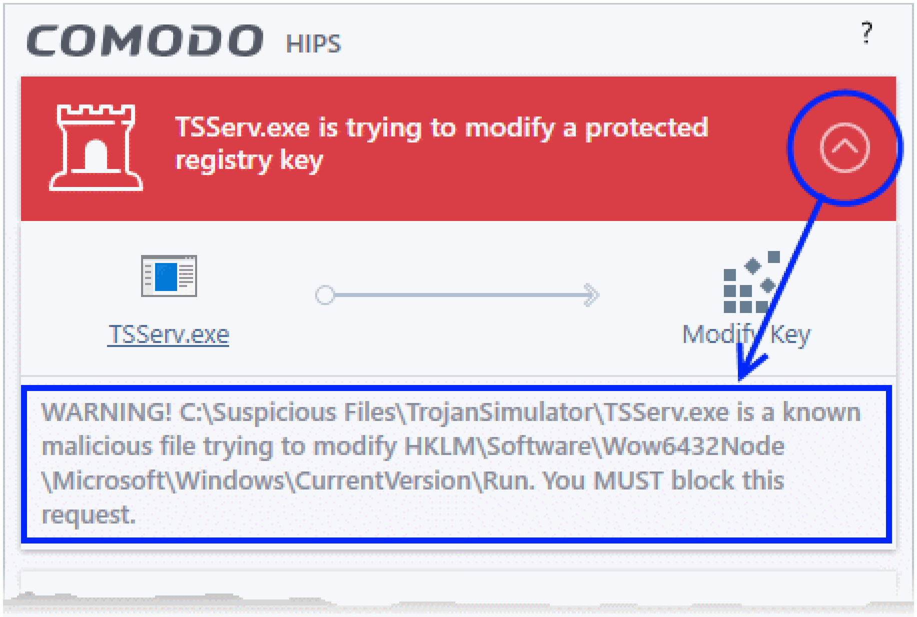
□ Remember my answer

Show Activities

Tip: Clicking the 'Show Activities' link at the bottom right will open the '**Process Activities List dialog**'. The Process Activities dialog will display the list activities of the processes run by the application.

The 'Show Activities' link is available only if VirusScope is enabled under '**Settings> VirusScope**'. If none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the 'Show Activities' link is disabled and will not open the Process Activities List dialog.

1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Internet Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.

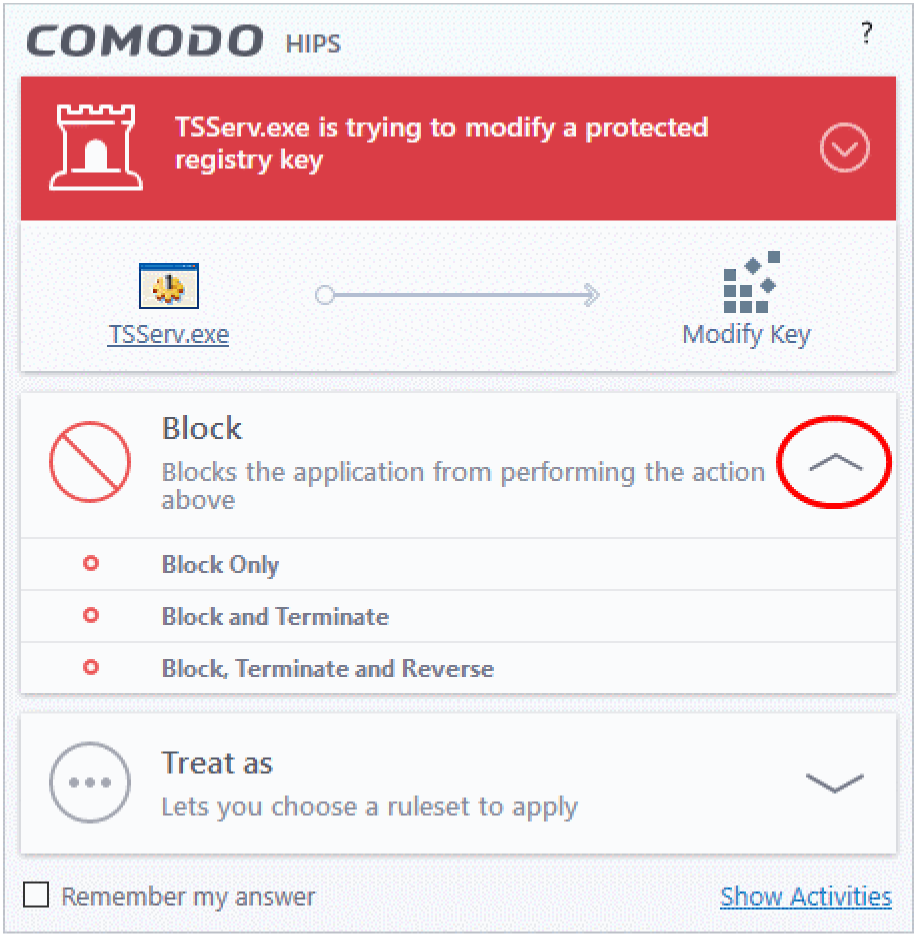


WARNING! C:\Suspicious Files\TrojanSimulator\TSServ.exe is a known malicious file trying to modify HKLM\Software\Wow6432Node \Microsoft\Windows\CurrentVersion\Run. You MUST block this request.

If it is one of your everyday applications and you simply want it to be allowed to continue then you should select **Allow**.

If you don't recognize the application then we recommend you select **Block** the application. By clicking the handle to expand the alert, you can choose to

- 'Block' - The application is not allowed to run
- 'Block and Terminate' - The application is not allowed to run and the processes generated by it are terminated thereby shutting down the application
- 'Block, Terminate and Reverse' - The application is not allowed to run, the processes generated by it are terminated and the changes made by the processes/application to other files/processes in the system will be rolled back.



COMODO HIPS ?

TSServ.exe is trying to modify a protected registry key

TSServ.exe → Modify Key

Block

Blocks the application from performing the action above

- ○ Block Only
- ○ Block and Terminate
- ○ Block, Terminate and Reverse

Treat as

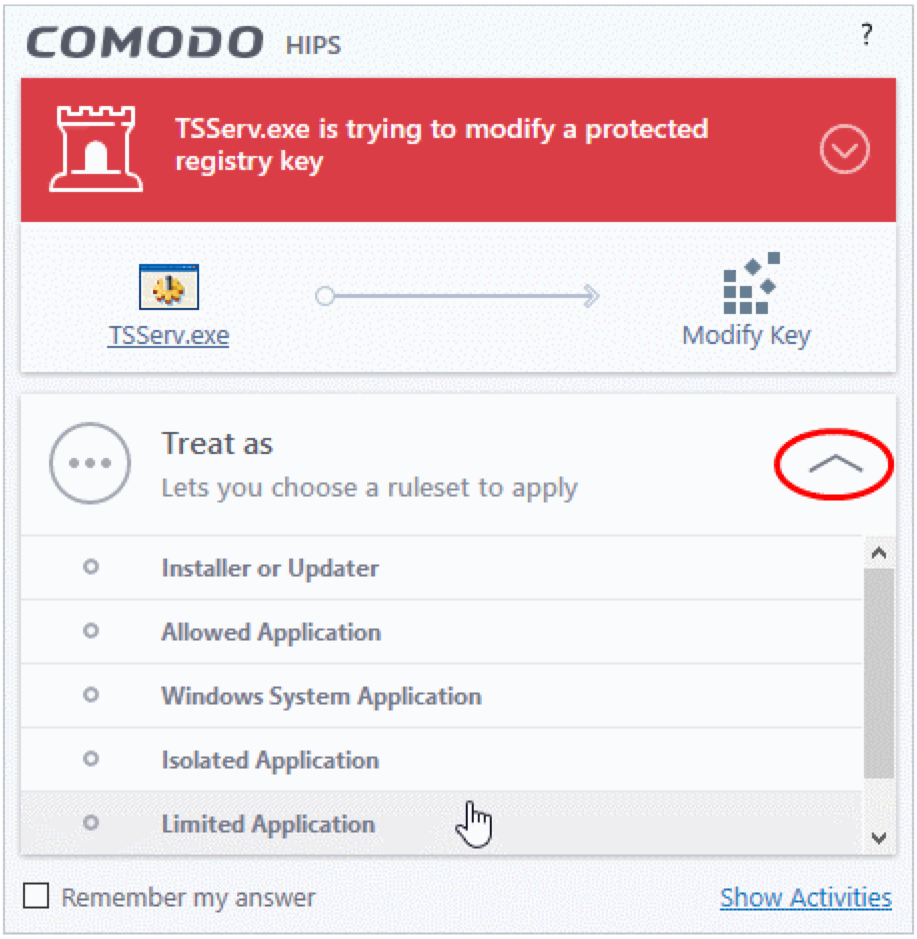
Lets you choose a ruleset to apply

□ Remember my answer

Show Activities

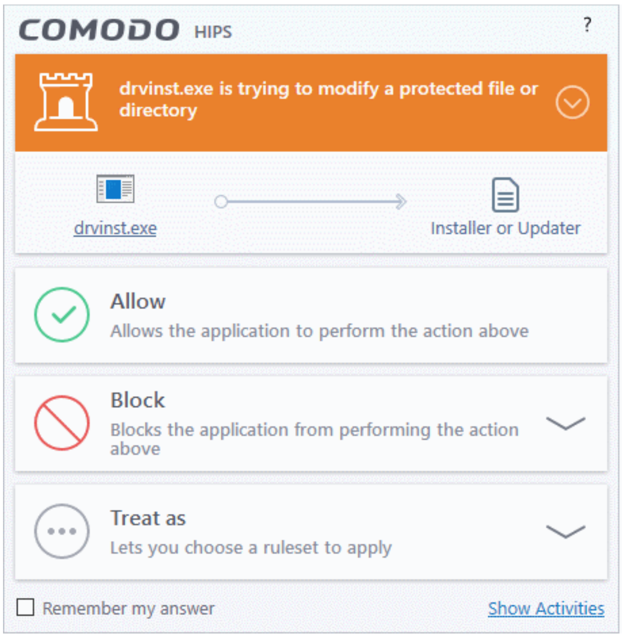
Note: 'Block, Terminate and Reverse' option will be available only if VirusScope is enabled under '**Settings**' > '**VirusScope**'.

2. If you are sure that it is one of your everyday applications and want to enforce a security policy (ruleset) to it, please use the 'Treat As' option. This applies a **predefined HIPS ruleset** to the target application and allows the application to run with access rights and protection settings as dictated by the chosen ruleset.



Avoid using the '**Installer or Updater'** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select 'Installer or Updater', you may consider using it temporarily with '**Remember My Answer'** left unchecked.

3. Pay special attention to '**Device Driver Installation**' and '**Physical Memory Access**' alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity is legitimate, then Comodo recommends blocking these requests.



COMODO HIPS ?

drvinst.exe is trying to modify a protected file or directory

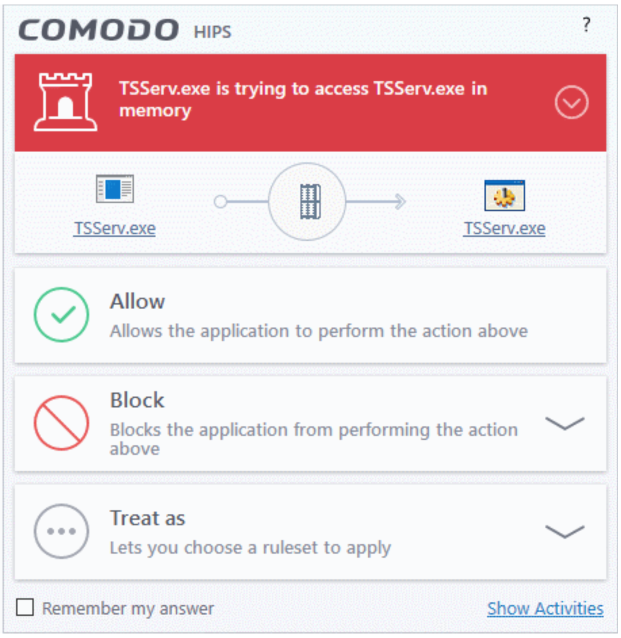
drvinst.exe → Installer or Updater

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer Show Activities



COMODO HIPS ?

TSServ.exe is trying to access TSServ.exe in memory

TSServ.exe → TSServ.exe

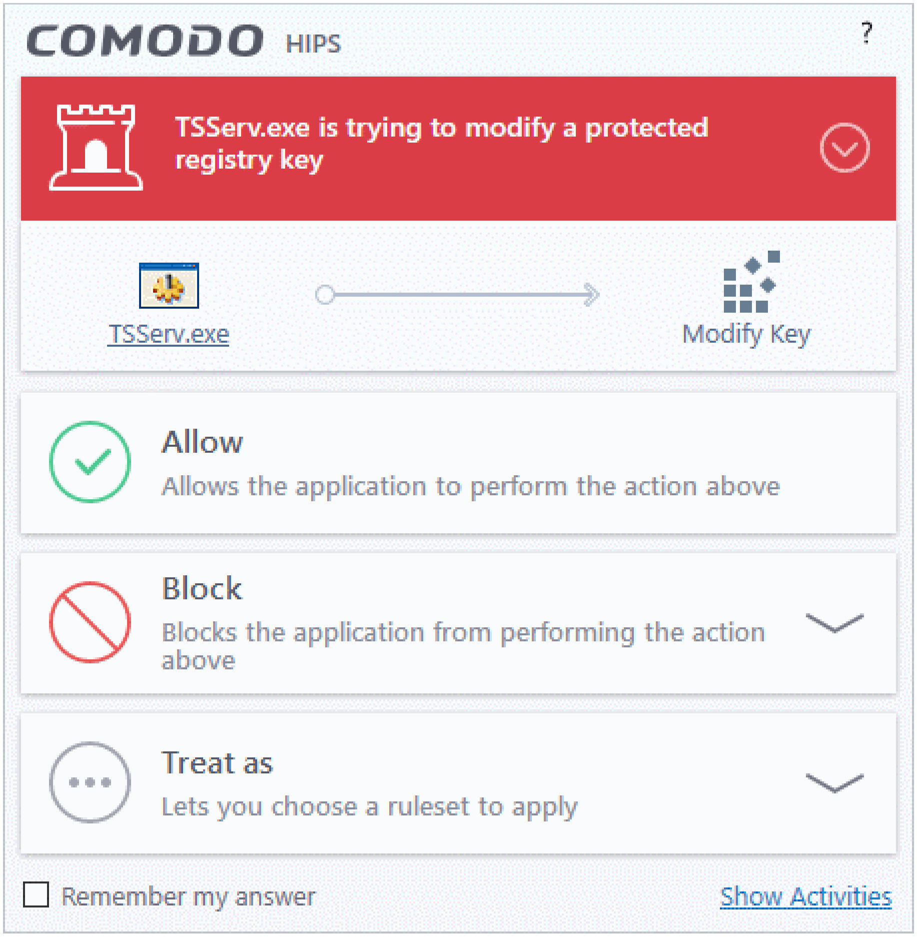
Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer Show Activities

4. '**Protected Registry Key**' Alerts usually occur when you install a new application. If you haven't been installing a new program and do not recognize the application requesting the access , then a 'Protected Registry Key Alert' should be a cause for concern.



COMODO HIPS ?

TSServ.exe is trying to modify a protected registry key

TSServ.exe → Modify Key

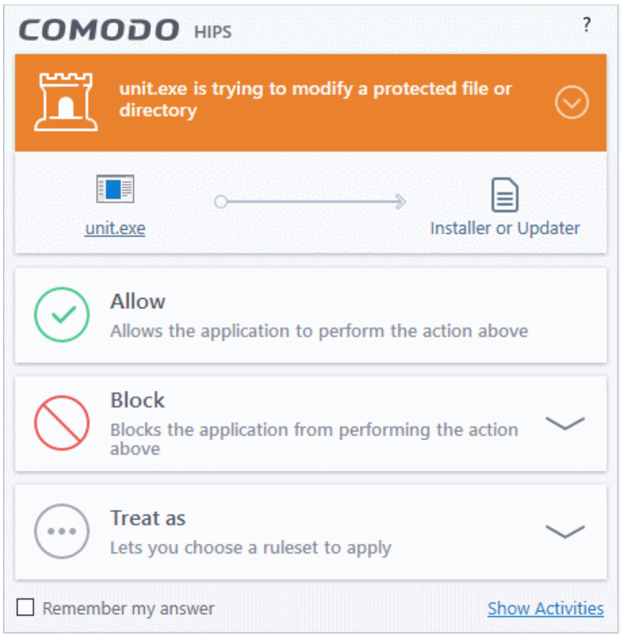
Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer Show Activities

5. '**Protected File Alerts**' usually occur when you try to download or copy files or when you update an already installed application.



COMODO HIPS ?

unit.exe is trying to modify a protected file or directory

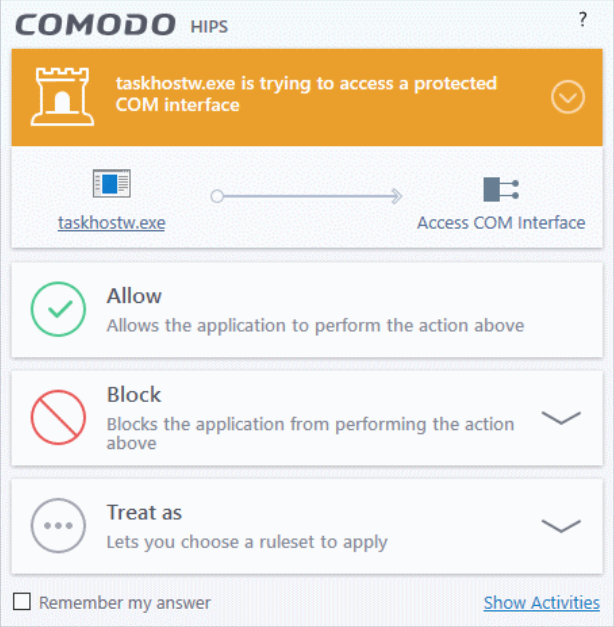
unit.exe → Installer or Updater

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer   Show Activities



COMODO HIPS ?

taskhostw.exe is trying to access a protected COM interface

taskhostw.exe → Access COM Interface

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer   Show Activities

Were you installing new software or trying to download an application from the Internet? If you are downloading a file from the 'net, select '**Allow**', without selecting '**Remember my answer**' option to cut down on the creation of unnecessary rules within the firewall.

If an application is trying to create an executable file in the Windows directory (or any of its sub-directories) then pay special attention. The Windows directory is a favorite target of malware applications. If you are not installing any new applications or updating Windows then make sure you recognize the application in question. If you don't, then click '**Block**' and choose '**Block Only**' from the options, without selecting **Remember My answer** option.

If an application is trying to create a new file with a random file name e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by clicking '**Treat As**' and choosing **'Isolated Application'** from the options.

6. If a HIPS alert reports a malware behavior in the security considerations area then you should '**Block the request**' permanently by selecting the '**Remember My Answer**' option. As this is probably a virus, you should also submit the application in question, to Comodo for analysis.

7. Unrecognized applications are not always bad. Your best loved applications may very well be safe but not yet included in the Comodo certified application database. If the security considerations section says "If xxx is one of your everyday applications, you can allow this request", you may allow the request permanently if you are sure it is not a virus. You may report it to Comodo for further analysis and inclusion in the certified application database.

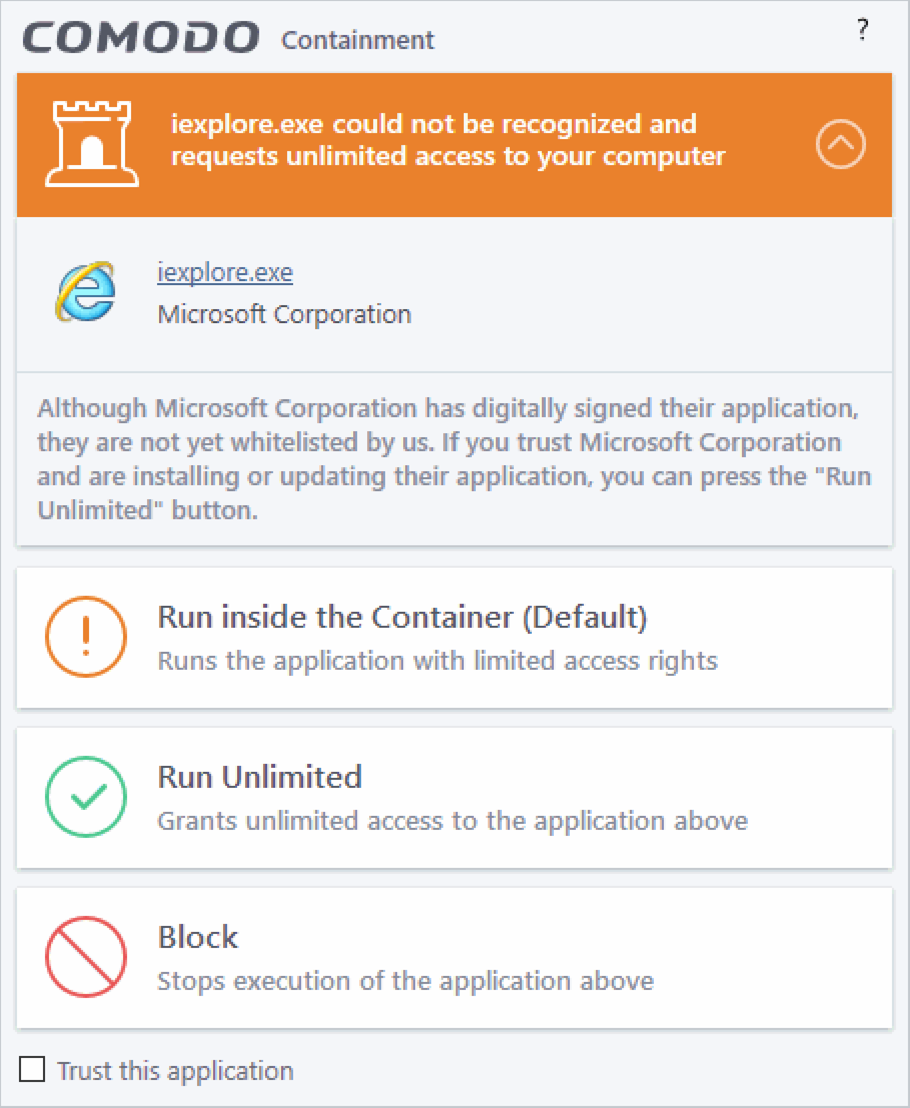
8. If HIPS is in 'Paranoid' mode, you probably are seeing the alerts for any new applications introduced to the system - but not for the ones you have already installed. If required, you may review files with 'Unrecognized' rating in the '**File List**' interface and remove them from the list.

9. Avoid using Trusted Application or Windows System Application policies for you email clients, web browsers, IM or P2P applications. These applications do not need such powerful access rights.

Answering a Containment Alert

Comodo Internet Security generates a containment alert if an application or a process tries to perform certain modifications to the operating system, its related files or critical areas like Windows Registry and when it automatically contained an unknown application.

Please read the following advice before answering a Containment alert:



COMODO Containment ?

iexplore.exe could not be recognized and requests unlimited access to your computer

iexplore.exe
Microsoft Corporation

Although Microsoft Corporation has digitally signed their application, they are not yet whitelisted by us. If you trust Microsoft Corporation and are installing or updating their application, you can press the "Run Unlimited" button.

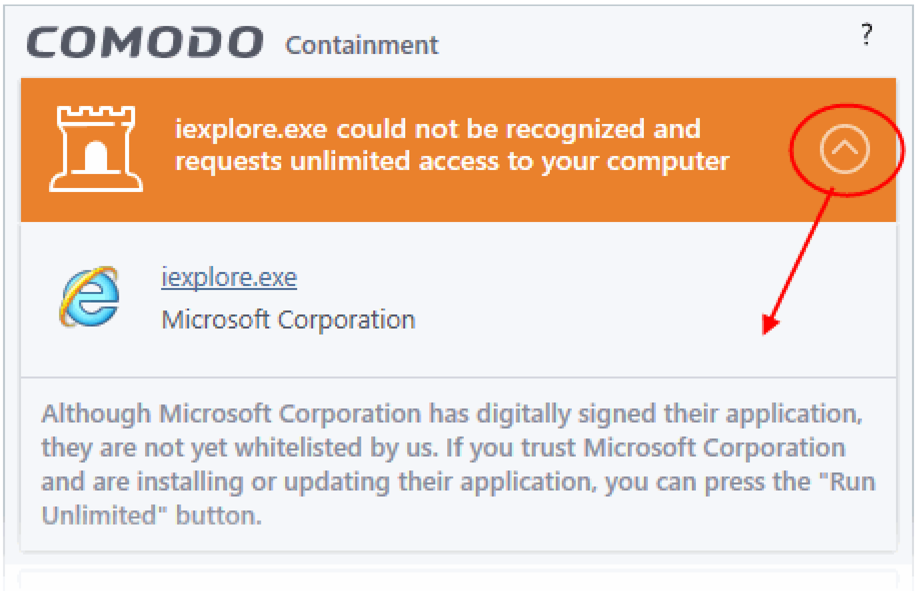
Run inside the Container (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Internet Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.



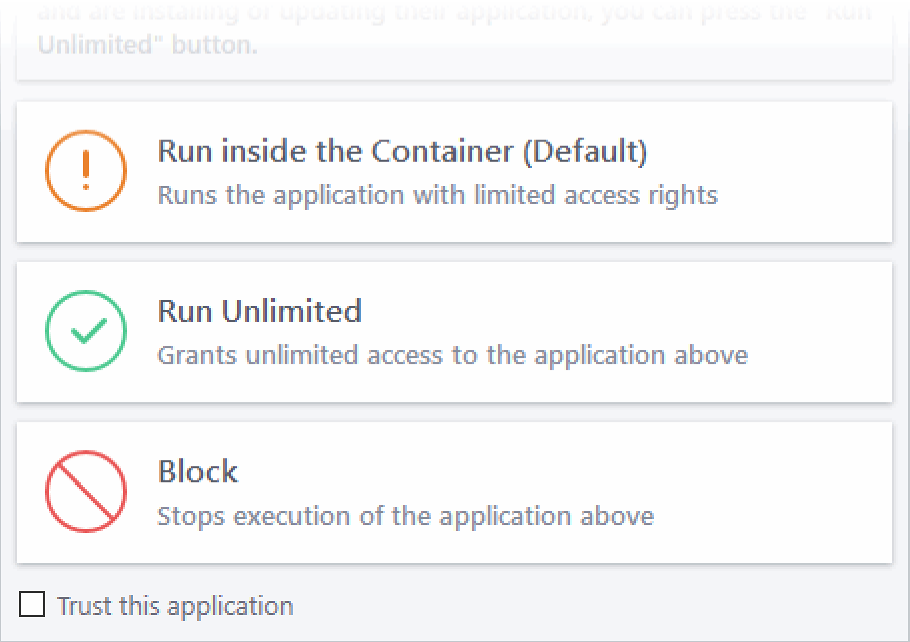
COMODO Containment ?

iexplore.exe could not be recognized and requests unlimited access to your computer

iexplore.exe
Microsoft Corporation

Although Microsoft Corporation has digitally signed their application, they are not yet whitelisted by us. If you trust Microsoft Corporation and are installing or updating their application, you can press the "Run Unlimited" button.

- If you are sure that the application is authentic and safe and you simply want it to be allowed to continue then you should select **Run Unlimited**. If you want the application not to be monitored in future, select 'Trust this application' checkbox. The application will be added to **Trusted Files** list.



and are installing or updating their application, you can press the "Run Unlimited" button.

Run inside the Container (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

- If you are unsure of the safety of the software, then Comodo recommends that you run it with limited privileges and access to your system resources by clicking the 'Run Isolated' button. See '**Unknown Files: The Scanning process**' for more explanations on applications run with limited privileges.
- If you don't recognize the application then we recommend you select to 'Block' the application.

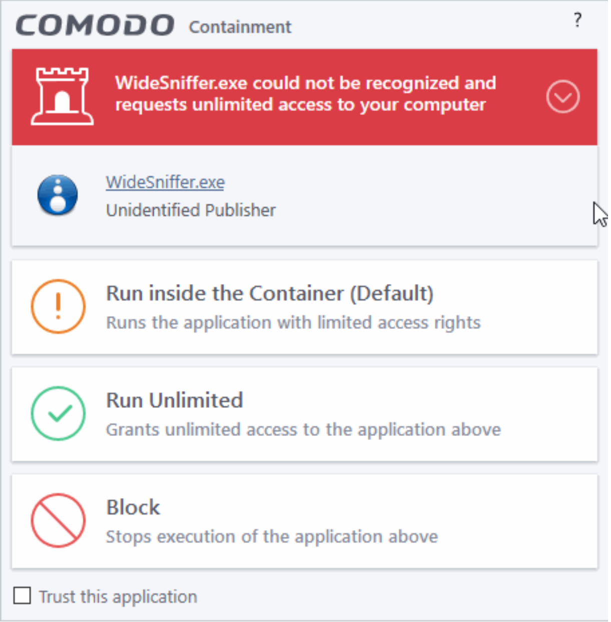
Run with Elevated Privileges Alert

The container will display this kind of alert when the installer of an unknown application requires administrator, or elevated, privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry.

- If you have good reason to trust the publisher of the software then you can click the '**Run Unlimited**' button. This will grant the elevated privilege request and allow the installer to run.
- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted access to your system resources by clicking the 'Run Isolated' button.
- If this alert is unexpected then you should abort the installation by clicking the 'Block' button (for example, you have not proactively started to install an application and the executable does not belong to an updater program that you recognize)
- If you select 'Trust this application' then CIS will include this to Trusted Files list and no future alerts will be generated when you run the same application.

Note: You will see this type of alert only if you have enabled 'Detect programs which require elevated privileges e.g. installers or updaters', and disabled 'Do not show privilege elevation alerts' in containment settings. See '**Containment Settings**' for more details.

There are two versions of this alert - one for unknown installers that are not digitally signed and the second for unknown installers that are digitally signed but the publisher of the software has *not yet* been white-listed (they are not yet a 'Trusted Software Vendor').



COMODO Containment ?

WideSniffer.exe could not be recognized and requests unlimited access to your computer

WideSniffer.exe
Unidentified Publisher

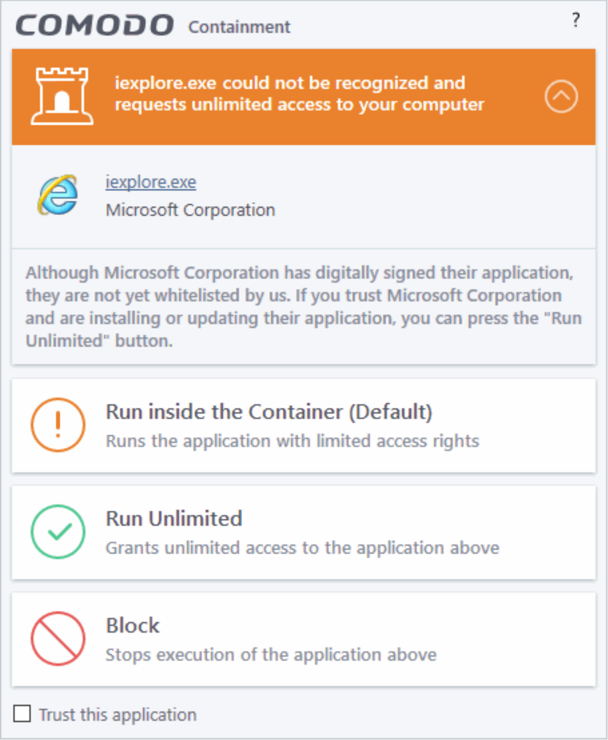
Run inside the Container (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

Unknown and not digitally signed



COMODO Containment ?

iexplore.exe could not be recognized and requests unlimited access to your computer

iexplore.exe
Microsoft Corporation

Although Microsoft Corporation has digitally signed their application, they are not yet whitelisted by us. If you trust Microsoft Corporation and are installing or updating their application, you can press the "Run Unlimited" button.

Run inside the Container (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

Unknown and digitally signed but the publisher not yet whitelisted (Not yet a 'Trusted Vendor')

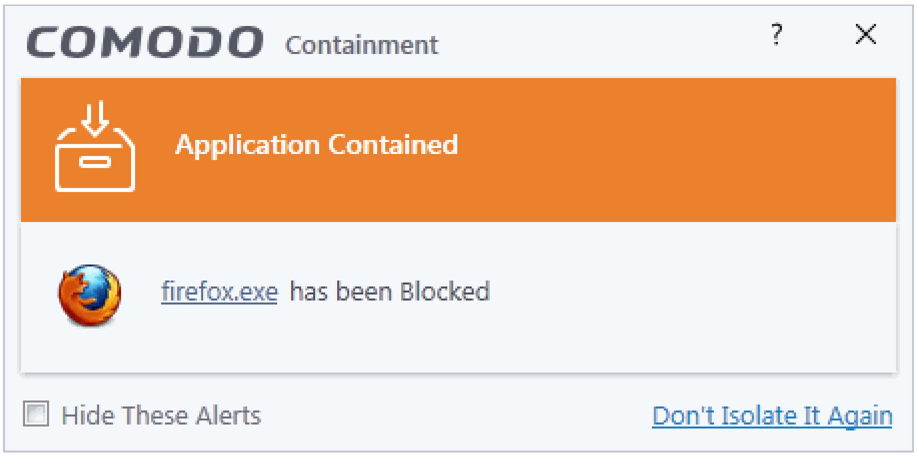
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

- **'Unknown Files: The Scanning Processes'** - to understand process behind how CIS scans files.
- '**Trusted Vendors List**' - for an explanation of digitally signed files and 'Trusted Software Vendors'.

Containment Notification

A notification will be shown when an unknown application is placed in the container:



COMODO Containment ? ×

Application Contained

firefox.exe has been Blocked

□ Hide These Alerts

Don't Isolate It Again

The alert will show the name of the executable that has been auto-contained. The application will be automatically added to '**File List**' with the 'Unrecognized' rating.

- Click the name of the application to open its properties screen.
- Click 'Don't Isolate It Again' to remove the file from the '**blocked items**' list.

Users are also reminded that they should submit such unknown applications to Comodo via the '**File List**' interface. This will allow Comodo to analyze the executable and, if it is found to be safe, to add it to the global safe list. This will ensure that unknown but ultimately safe applications are quickly white-listed for all users.

Also see:

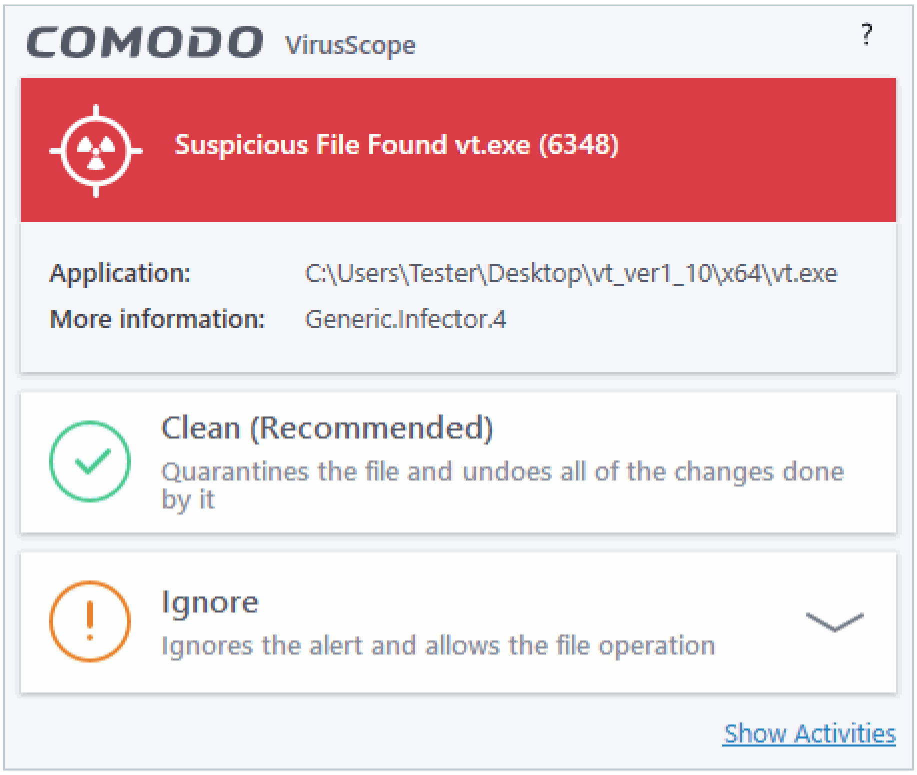
- '**Unknown Files: The Scanning Processes**' - to understand process behind how CIS scans files

Answering a VirusScope Alert

Comodo Internet Security generates a VirusScope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that VirusScope 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 VirusScope alert:

1. Carefully read the information displayed in the alert. The 'More Information' section provides you the nature of the suspicious action.



COMODO VirusScope

Suspicious File Found vt.exe (6348)

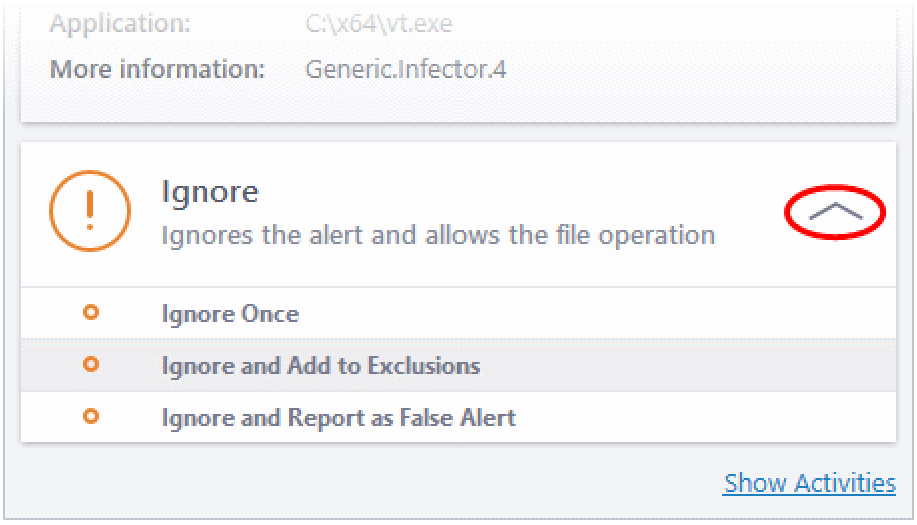
Application: C:\Users\Tester\Desktop\vt_ver1_10\x64\vt.exe

More information: Generic.Infector.4

Clean (Recommended)
Quarantines the file and undoes all of the changes done by it

Ignore
Ignores the alert and allows the file operation

- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking 'Ignore' and selecting the option from the drop-down.



Application: C:\x64\vt.exe

More information: Generic.Infector.4

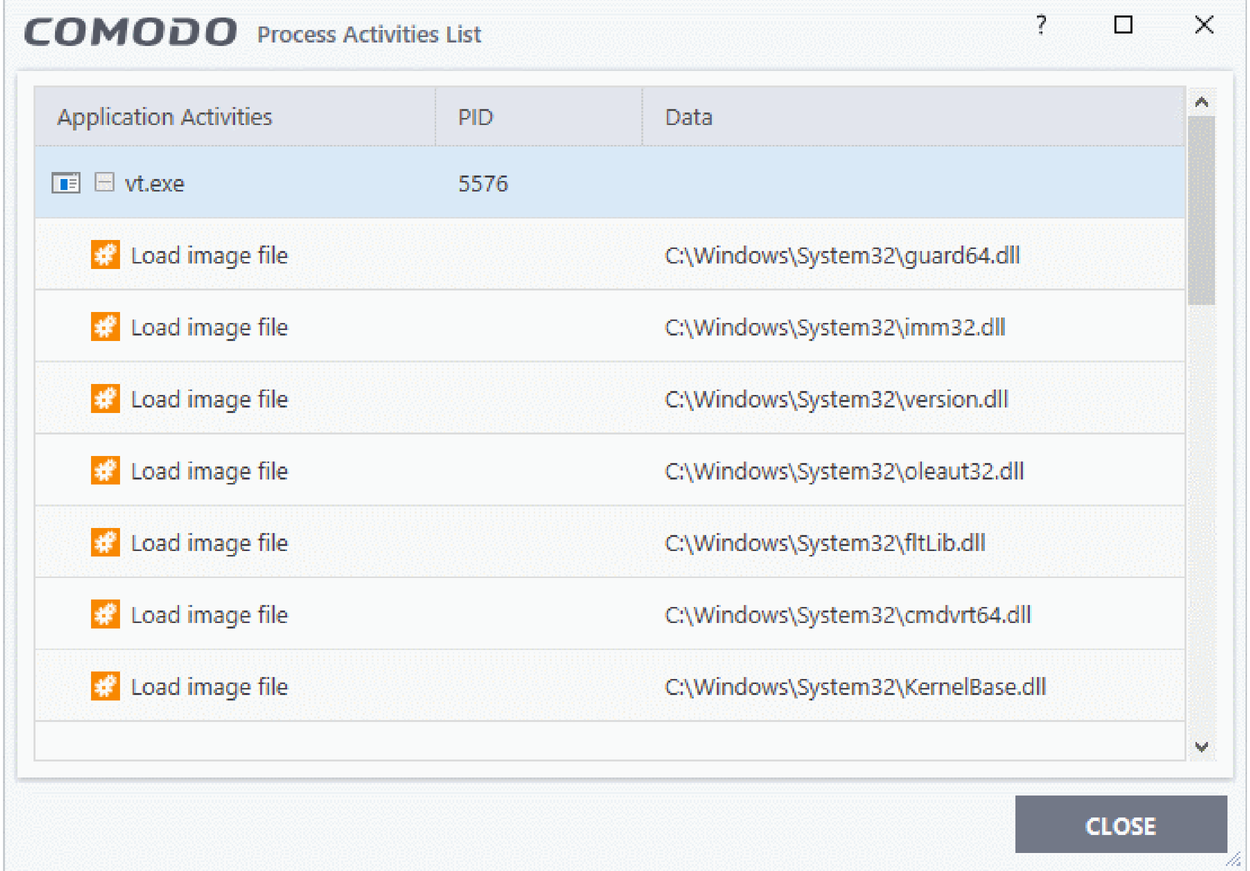
Ignore

Ignores the alert and allows the file operation

- Ignore Once
- Ignore and Add to Exclusions
- Ignore and Report as False Alert

- Ignore Once -The process is allowed to run this time only. If the process attempts to execute on future occasions, another VirusScope alert is displayed.
- Ignore and Add to Exclusions - The file is allowed to run and will not be contained in the future. See '**Auto-Containment Rules**' for help to configure which types of files should be auto-contained.
- Ignore and Report as False Alert - If you are sure that the file is safe, select 'Ignore and Report as a False Alert'. CIS will then submit this file to Comodo for analysis. If the false-positive is verified (and the file is trustworthy), it will be added to the Comodo safe list.

- To view the activities of the processes, 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	PID	Data
vt.exe	5576	
Load image file		C:\Windows\System32\guard64.dll
Load image file		C:\Windows\System32\imm32.dll
Load image file		C:\Windows\System32\version.dll
Load image file		C:\Windows\System32\oleaut32.dll
Load image file		C:\Windows\System32\fltLib.dll
Load image file		C:\Windows\System32\cmdvrt64.dll
Load image file		C:\Windows\System32\KernelBase.dll

Column Descriptions

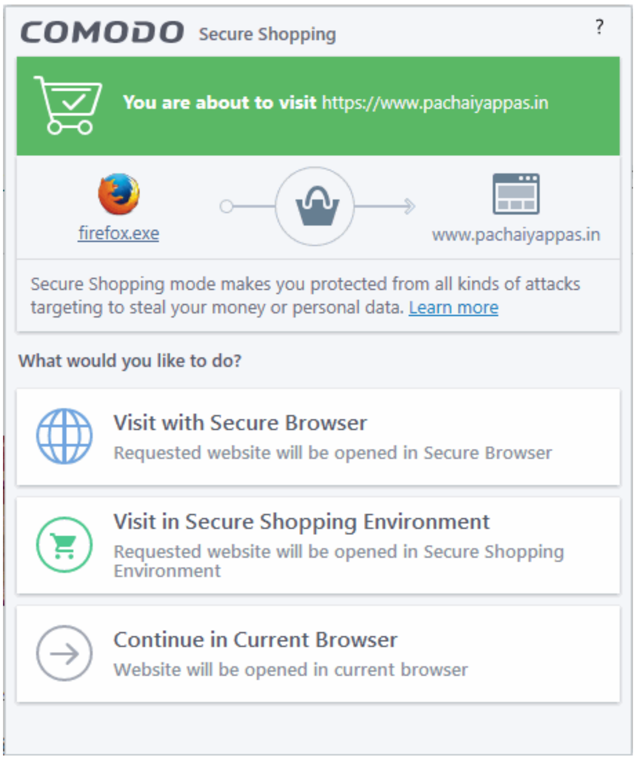
- Application Activities - Displays the activities of each of the processes run by the parent application.

- - File actions: The process performed a file-system operation (create\modify\rename\delete file) which you might not be aware of.
- - Registry: The process performed a registry operation (created/modified a registry key) which might not be authorized.
- - Process: The process created a child process which you may not have authorized or have been aware of.
- - Network: The process attempted to establish a network connection that you may not have been aware of.
- If the process has been terminated, the activities will be indicated with gray text and will appear in the list until you view the 'Process Activities List' interface. If you close the interface and reopen the list within five minutes, the activities will appear in the list. Else, the terminated activities will not be displayed in the list.

- PID - Process Identification Number.
- Data - Displays the file affected by the action.

Secure Shopping Alert

The 'Secure Shopping Alert' will be displayed whenever a user opens a website that is added to the list of websites added for Secure Shopping protection. The user can choose to open the website inside the Secure Shopping environment, with a secure browser window or continue with the current browser. See '**Comodo Secure Shopping**' for more details.



COMODO Secure Shopping ?

You are about to visit https://www.pachaiyappas.in

firefox.exe → www.pachaiyappas.in

Secure Shopping mode makes you protected from all kinds of attacks targeting to steal your money or personal data. Learn more

What would you like to do?

Visit with Secure Browser
Requested website will be opened in Secure Browser

Visit in Secure Shopping Environment
Requested website will be opened in Secure Shopping Environment

Continue in Current Browser
Website will be opened in current browser

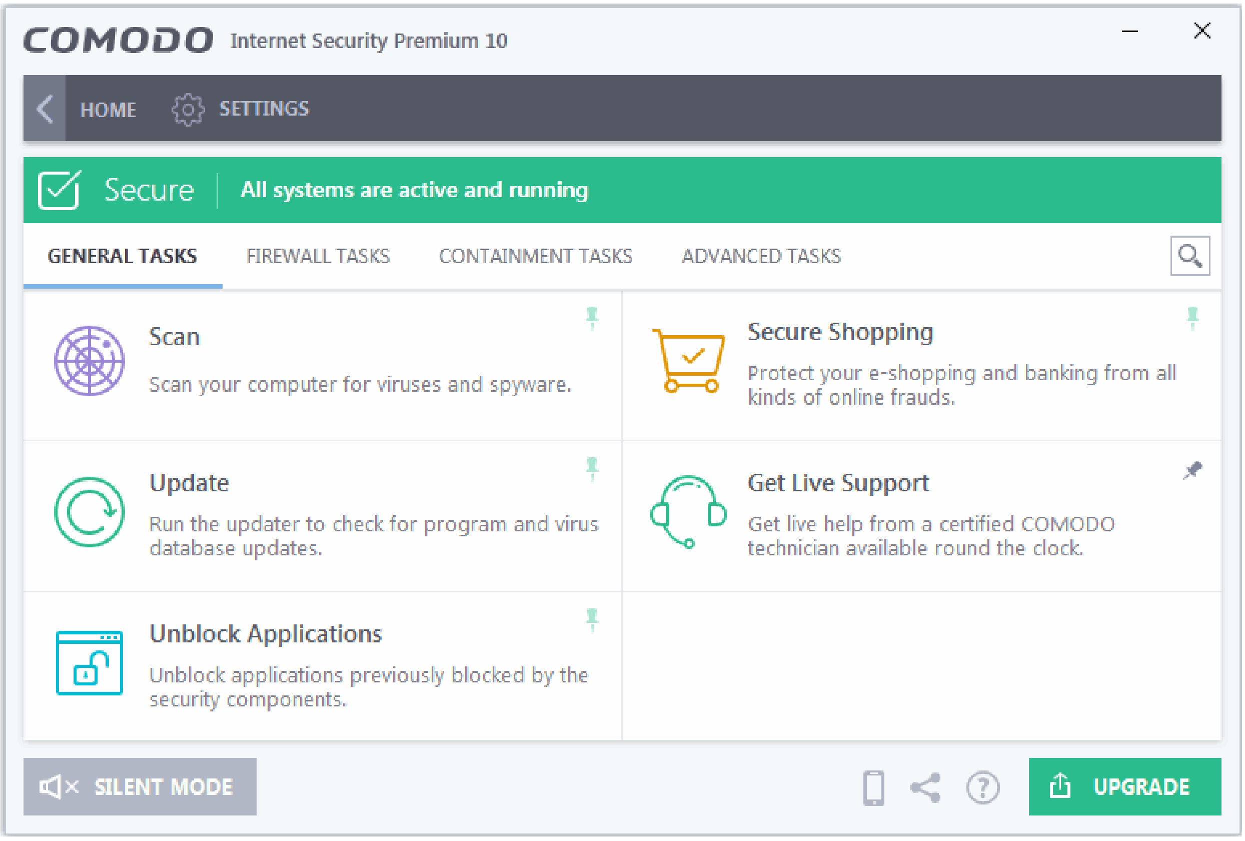
The options available in the alert are:

- Visit with Secure Browser - The website will open in secure mode (incognito mode) /private mode of the default browser.
- Visit in Secure Shopping Environment - The website will open using the web browser that is configured for the secure shopping mode.
- Continue in Current Browser - The website will open in normal mode using the default browser.

2. General Tasks - Introduction

The 'General Tasks' interface allows you to quickly perform antivirus scans, update the virus database, open the Secure Shopping environment, manage blocked files and get live help from Comodo technicians.

The 'General Tasks' area is displayed by default, when switching from the Home screen to the Tasks interface. To return to the 'General Tasks' interface from any other tasks interface, click 'General Tasks' at the top of the 'Tasks' interface.


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
SILENT MODE
UPGRADE

Click the following links to jump to the help page for that topic:

- Scan and Clean your Computer
- Open Secure Shopping
- Manage Virus Database and Program Updates
- Get Live Support
- Manage Blocked Applications
- Instantly Scan Files and Folders
- Processing Infected Files

2.1. Scan and Clean Your Computer

Comodo Antivirus leverages multiple technologies, including real-time and on-demand scanning, to immediately start cleaning suspicious files from your disk drives, emails, downloads and system memory. The application also allows you to create custom scan profiles, configure scheduled scans and features full event logging and file submission facilities.

When you want to run a virus scan on your system, you can launch an **On-Demand Scan** using the **Scan** option.

This executes an instant virus scan on the selected item.

To run an on-demand virus scan:

- Click the 'Scan' tile on the CIS home screen

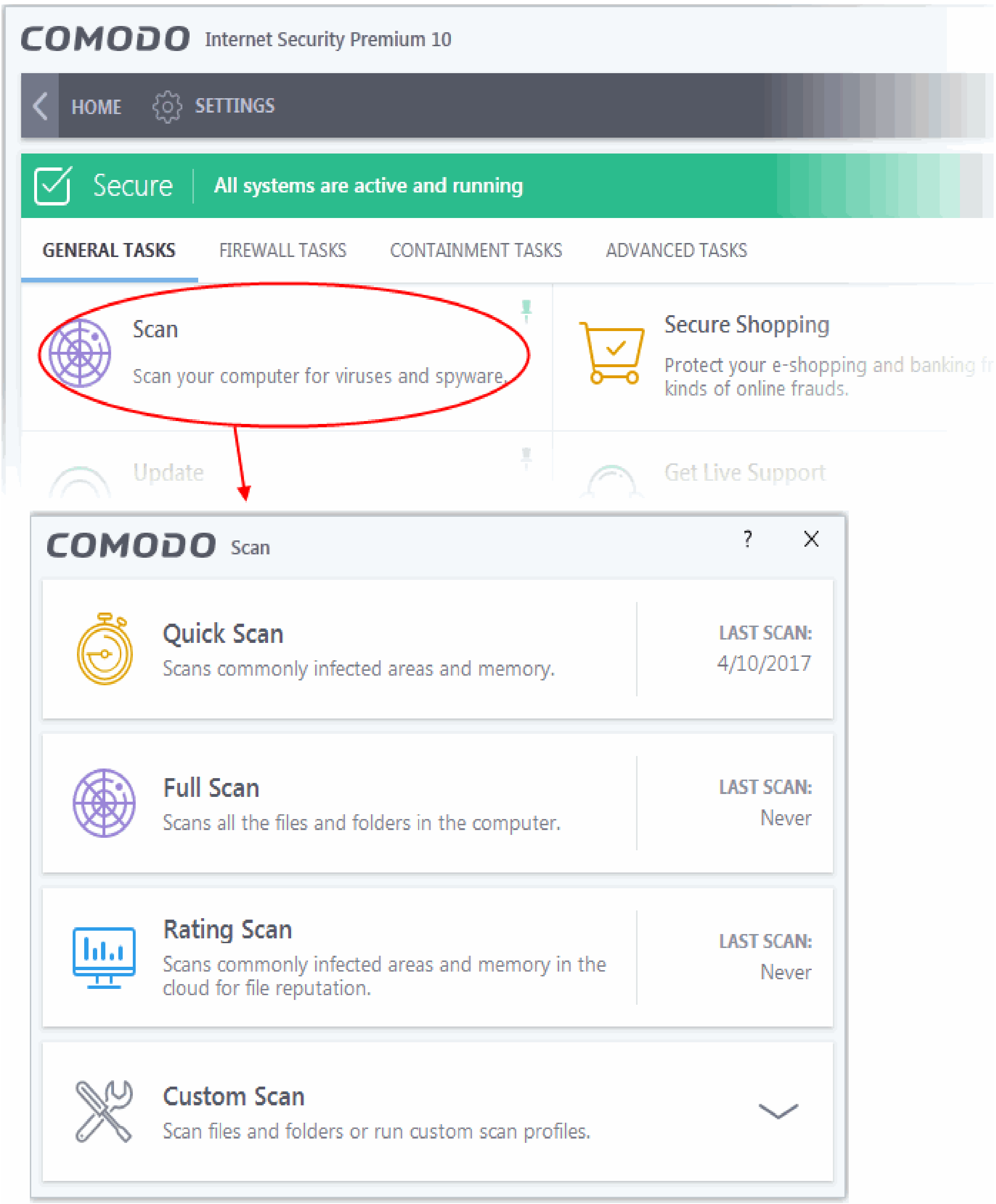
  OR

- Click the scan icon in the widget

  OR

- Click the 'Tasks' button then 'Scan' in the 'General Tasks' section

Any of these methods will open the scan selection screen:



All systems are active and running

Scan
Scan your computer for viruses and spyware.

Secure Shopping
Protect your e-shopping and banking fr
kinds of online frauds.

Quick Scan
Scans commonly infected areas and memory.
LAST SCAN: 4/10/2017

Full Scan
Scans all the files and folders in the computer.
LAST SCAN: Never

Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
LAST SCAN: Never

Custom Scan
Scan files and folders or run custom scan profiles.

A quick scan will scan commonly infected areas while a full scan will scan your entire computer. The rating scan will assign a trust rating to all files on your computer. A custom scan lets you choose specific areas to scan.

The following sections explain more about each scan type:

- **Run a Quick Scan**
- **Run a Full Computer Scan**
- **Run a Rating Scan**

- **Run a Custom Scan**
  - **Scan a Folder**
  - **Scan a File**
  - **Create and Schedule a Custom Scan**
- **Instantly scan individual file/folder**
- **Processing Infected Files**

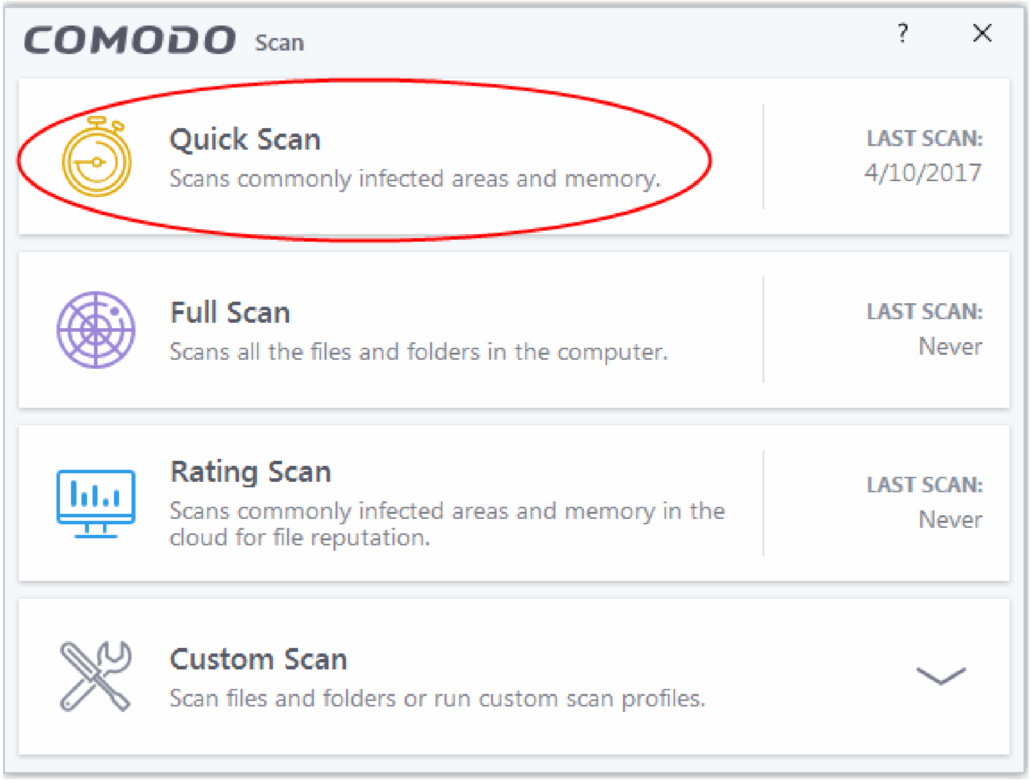
2.1.1. Run a Quick Scan

The 'Quick Scan' profile allows you to scan critical areas of your computer which are most prone to attack from malware. The 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.

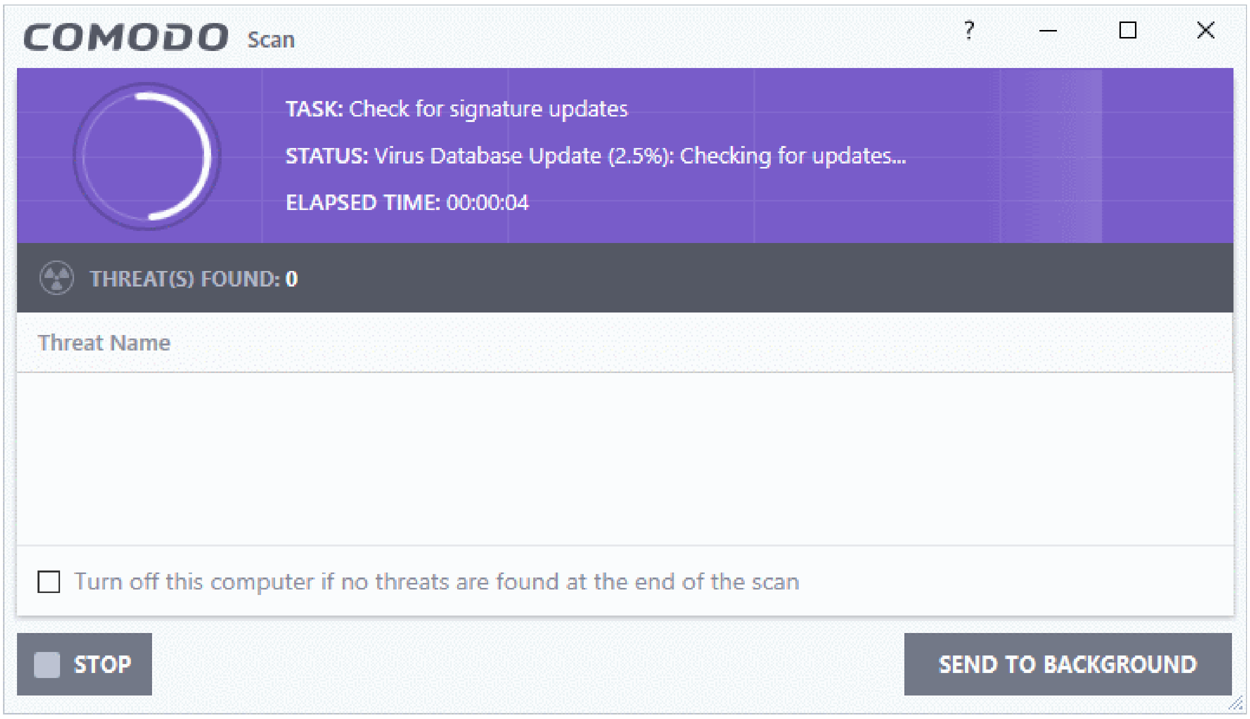
You can customize the scan parameters and create a schedule for 'Quick Scan' from the 'Advanced Settings' interface. See **Antivirus Configuration** > **Scan Profiles** for more details.

To run a Quick Scan

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)
- Select 'Quick Scan' from the 'Scan' interface.


COMODO Scan
?
Quick Scan
Scans commonly infected areas and memory.
LAST SCAN:
4/10/2017
Full Scan
Scans all the files and folders in the computer.
LAST SCAN:
Never
Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
LAST SCAN:
Never
Custom Scan
Scan files and folders or run custom scan profiles.

The scanner will start and first check whether your virus signature database is up-to-date:



COMODO Scan

TASK: Check for signature updates

STATUS: Virus Database Update (2.5%): Checking for updates...

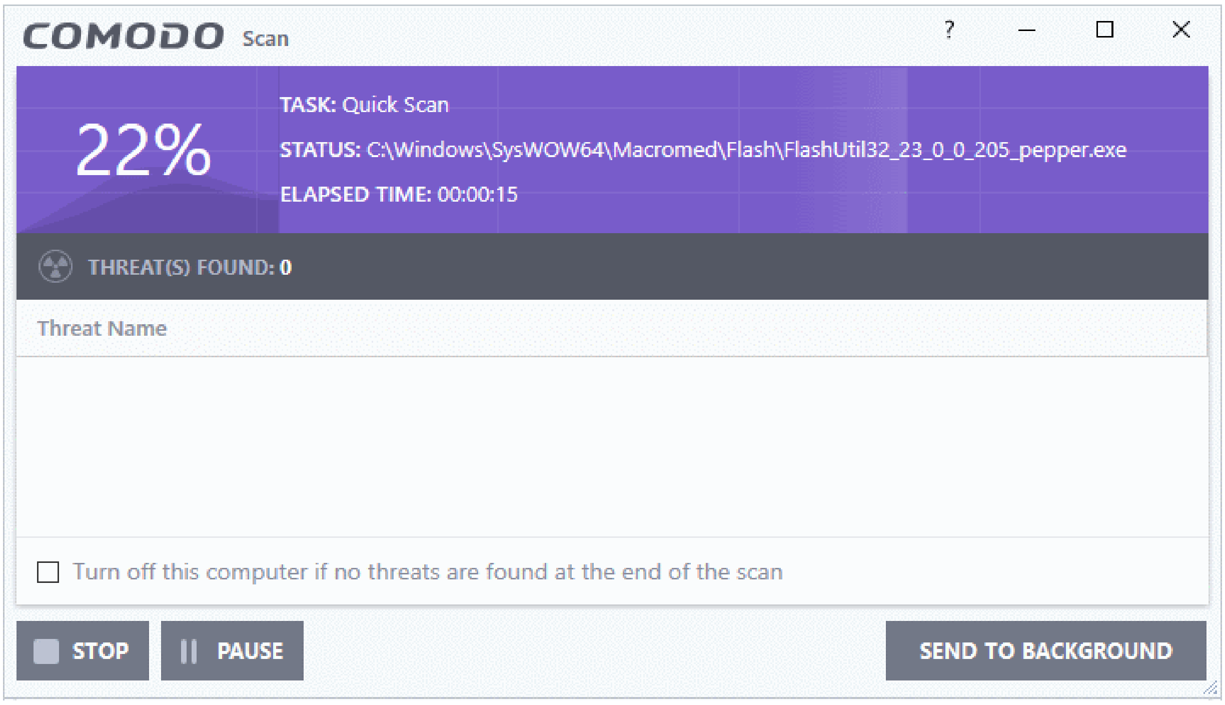
ELAPSED TIME: 00:00:04

THREAT(S) FOUND: 0

Threat Name

☐ Turn off this computer if no threats are found at the end of the scan

If the database is outdated, CIS will download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:



COMODO Scan

22%

TASK: Quick Scan

STATUS: C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_23_0_0_205_pepper.exe

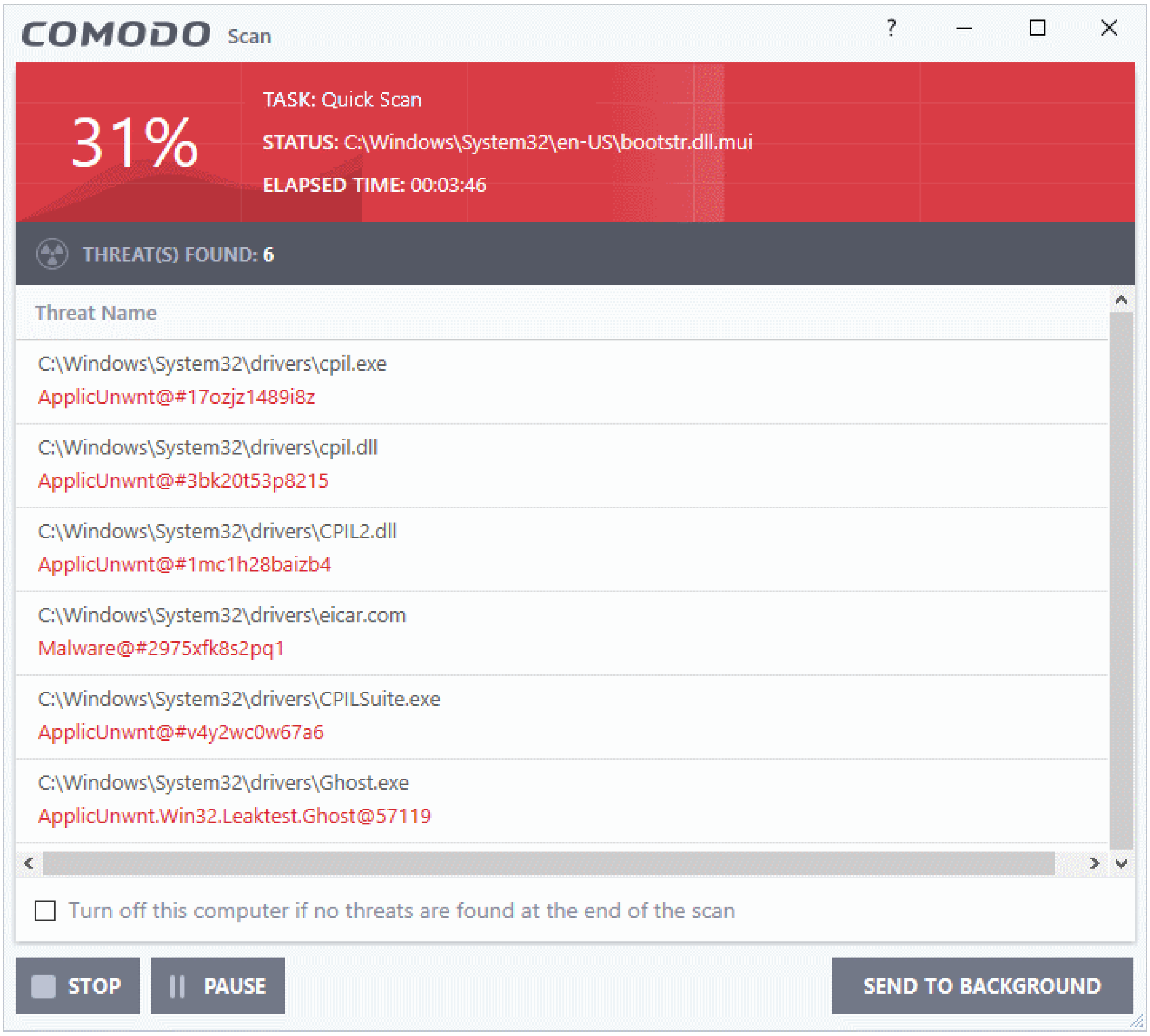
ELAPSED TIME: 00:00:15

THREAT(S) FOUND: 0

Threat Name

☐ Turn off this computer if no threats are found at the end of the scan

- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'. You can still keep track of the scan progress from the 'Task Manager' interface.



31%

TASK: Quick Scan

STATUS: C:\Windows\System32\en-US\bootstr.dll.mui

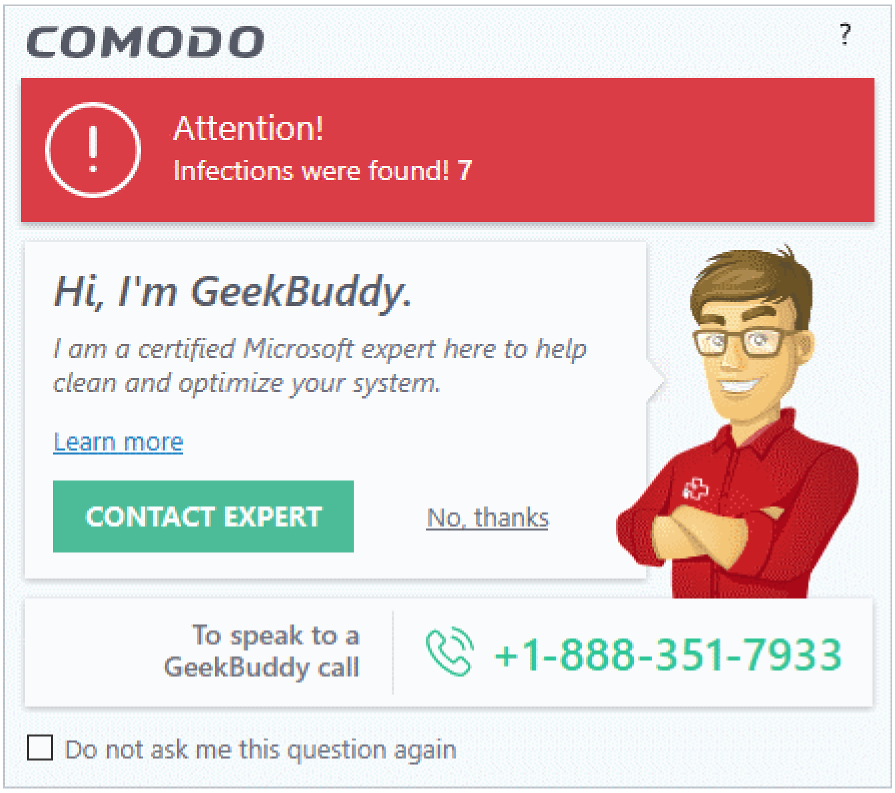
ELAPSED TIME: 00:03:46

THREAT(S) FOUND: 6

Threat Name
C:\Windows\System32\drivers\cpil.exe ApplicUnwnt@#17ozjz1489i8z
C:\Windows\System32\drivers\cpil.dll ApplicUnwnt@#3bk20t53p8215
C:\Windows\System32\drivers\CPIL2.dll ApplicUnwnt@#1mc1h28baizb4
C:\Windows\System32\drivers\eicar.com Malware@#2975xfk8s2pq1
C:\Windows\System32\drivers\CPILSuite.exe ApplicUnwnt@#v4y2wc0w67a6
C:\Windows\System32\drivers\Ghost.exe ApplicUnwnt.Win32.Leaktest.Ghost@57119

☐ Turn off this computer if no threats are found at the end of the scan

- An alert screen will be displayed at the end of the scan if issues were detected. The alert will display the number of threats/infections discovered and present you with cleaning options:



COMODO ?

Attention!
Infections were found! 7

Hi, I'm GeekBuddy.

I am a certified Microsoft expert here to help clean and optimize your system.

Learn more

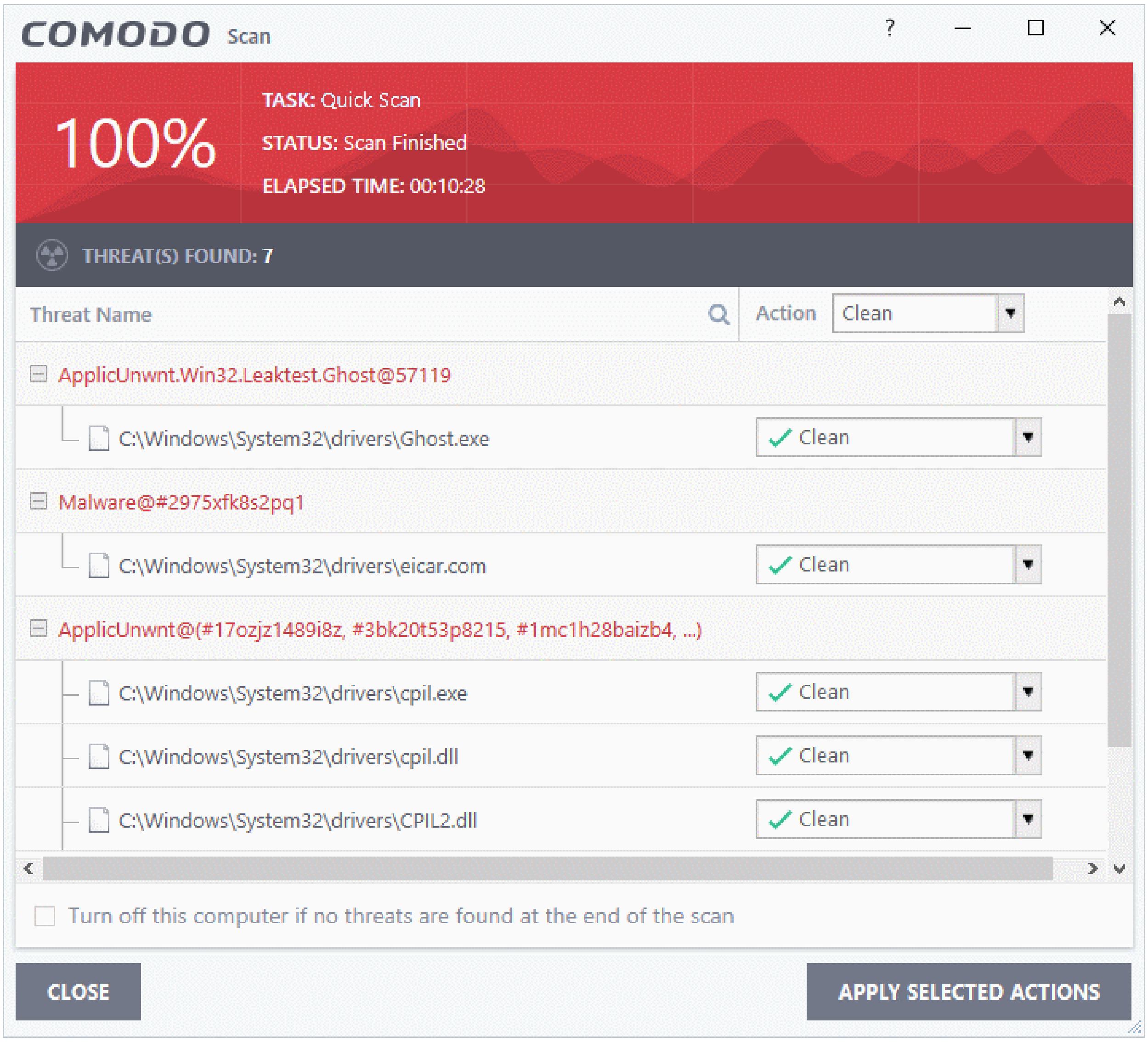
To speak to a GeekBuddy call ☎ +1-888-351-7933

□ Do not ask me this question again

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.

See '**Comodo GeekBuddy**', for more details on 'GeekBuddy' Expert help.

- If you wish to clean the infections yourself, select 'No, Thanks'. The scan results screen will be displayed.



TASK: Quick Scan

STATUS: Scan Finished

ELAPSED TIME: 00:10:28

Threat Name	Action: Clean
ApplicUnwnt.Win32.Leaktest.Ghost@57119	
C:\Windows\System32\drivers\Ghost.exe	✓ Clean
Malware@#2975xfk8s2pq1	
C:\Windows\System32\drivers\eicar.com	✓ Clean
ApplicUnwnt@(#17ozjz1489i8z, #3bk20t53p8215, #1mc1h28baizb4, ...)	
C:\Windows\System32\drivers\cpil.exe	✓ Clean
C:\Windows\System32\drivers\cpil.dll	✓ Clean
C:\Windows\System32\drivers\CPIL2.dll	✓ Clean

□ Turn off this computer if no threats are found at the end of the scan

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

> Note. You will only be presented with the options drop-down if 'Automatically clean threats' is disabled for quick scans.

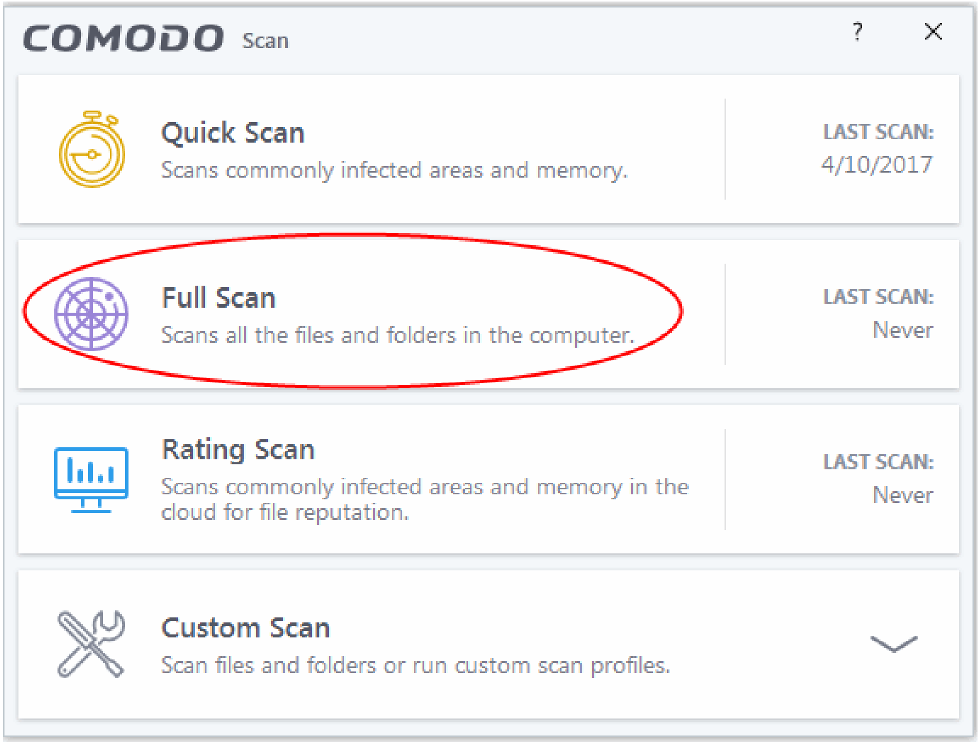
2.1.2. Run a Full Computer Scan

A 'Full System Scan' scans every local drive, folder and file on your system. Any external devices like USB drives and digital camera will also be scanned.

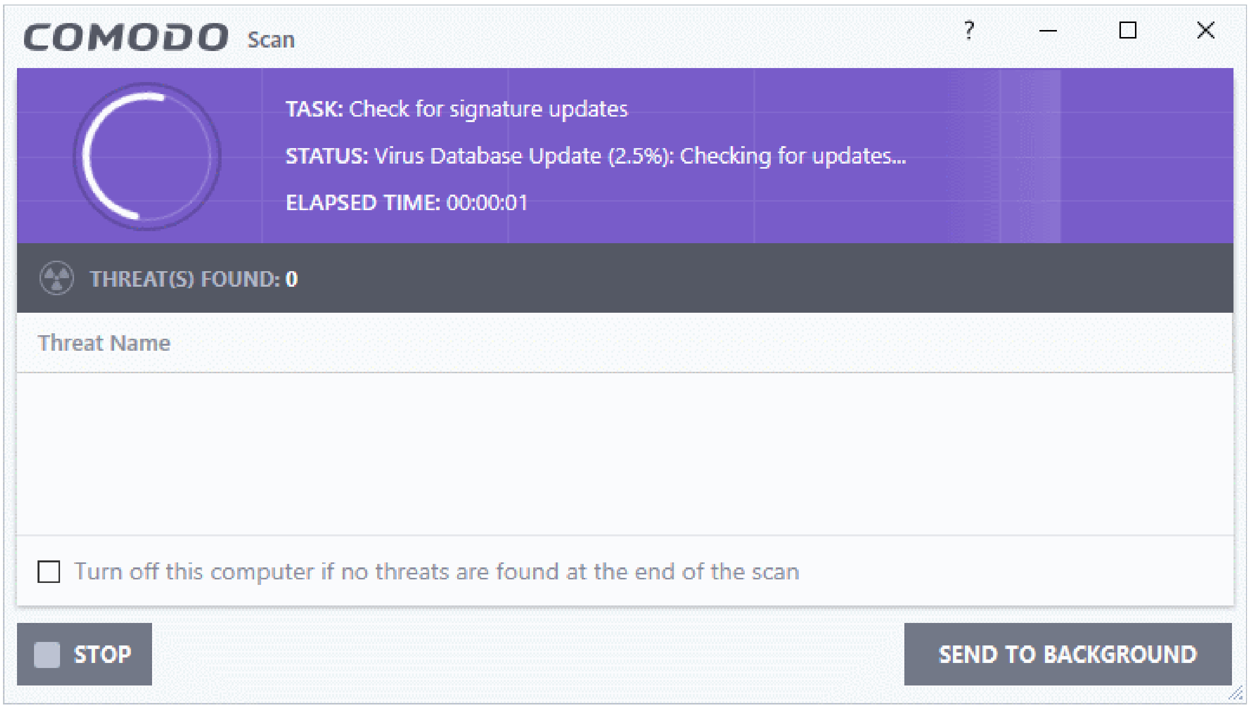
You can customize the scan parameters that define the behavior of the scan and create a schedule for periodically running the Full Scan from the 'Advanced Settings' interface. See **Antivirus Configuration** > **Scan Profiles** for more details.

To run a Full Computer Scan

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)
- Select 'Full Scan' from the 'Scan' interface.


COMODO Scan
?
Quick Scan
Scans commonly infected areas and memory.
LAST SCAN:
4/10/2017
Full Scan
Scans all the files and folders in the computer.
LAST SCAN:
Never
Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
LAST SCAN:
Never
Custom Scan
Scan files and folders or run custom scan profiles.

The scanner will start and first check whether your virus signature database is up-to-date.



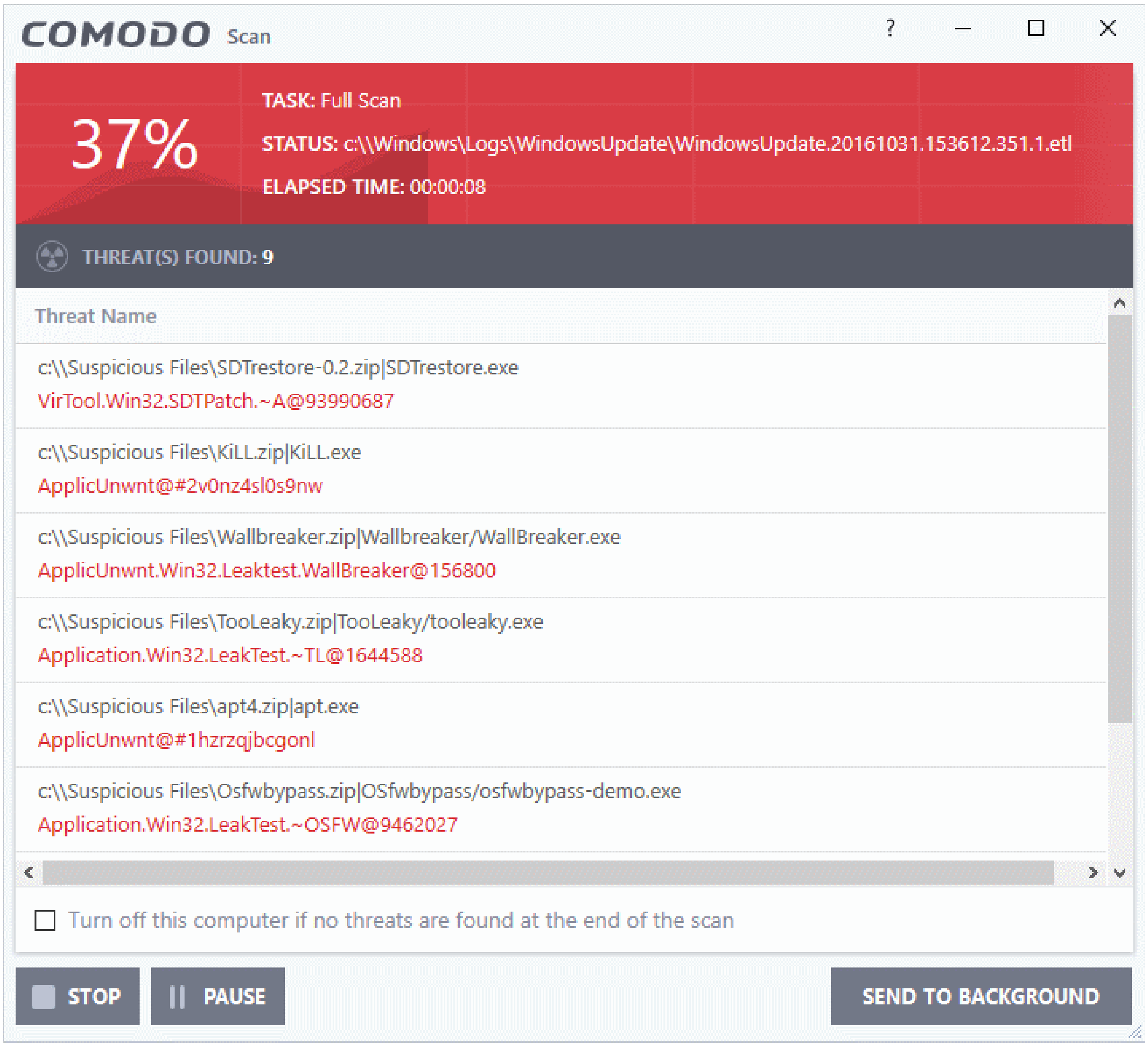
TASK: Check for signature updates

STATUS: Virus Database Update (2.5%): Checking for updates...

ELAPSED TIME: 00:00:01

□ Turn off this computer if no threats are found at the end of the scan

If the database is outdated, CIS will download and install the latest version before commencing the scan.



TASK: Full Scan

STATUS: c:\\Windows\Logs\WindowsUpdate\WindowsUpdate.20161031.153612.351.1.etl

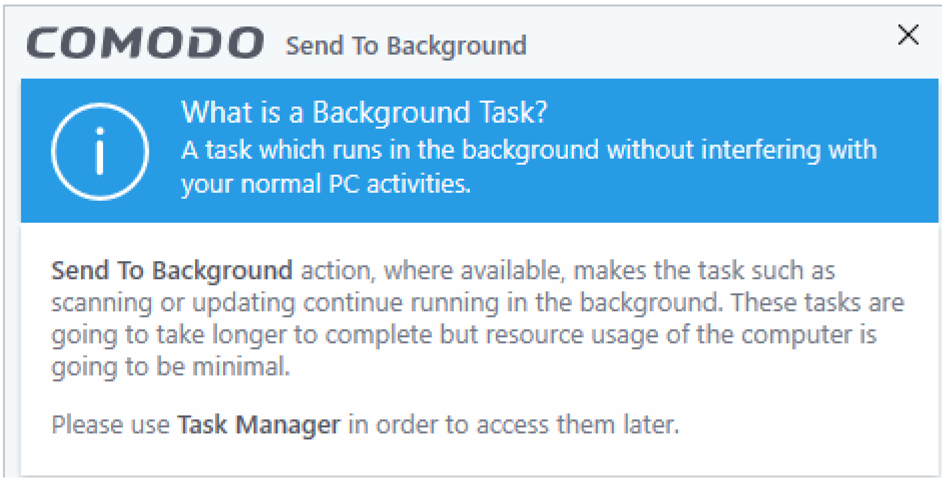
ELAPSED TIME: 00:00:08

THREAT(S) FOUND: 9

Threat Name
c:\\Suspicious Files\SDTrestore-0.2.zip|SDTrestore.exe VirTool.Win32.SDTPatch.~A@93990687
c:\\Suspicious Files\KiLL.zip|KiLL.exe ApplicUnwnt@#2v0nz4sl0s9nw
c:\\Suspicious Files\Wallbreaker.zip|Wallbreaker/WallBreaker.exe ApplicUnwnt.Win32.Leaktest.WallBreaker@156800
c:\\Suspicious Files\TooLeaky.zip|TooLeaky/tooleaky.exe Application.Win32.LeakTest.~TL@1644588
c:\\Suspicious Files\apt4.zip|apt.exe ApplicUnwnt@#1hzrzqjbcgonl
c:\\Suspicious Files\Osfwbypass.zip|OSfwbypass/osfwbypass-demo.exe Application.Win32.LeakTest.~OSFW@9462027

□ Turn off this computer if no threats are found at the end of the scan

- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



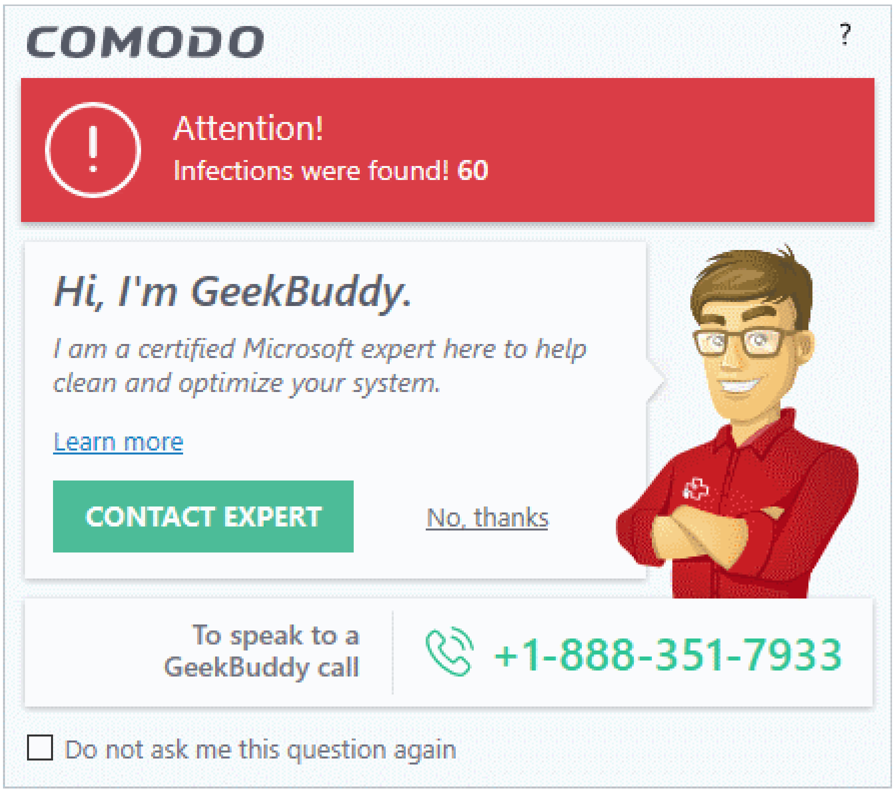
What is a Background Task?
A task which runs in the background without interfering with your normal PC activities.

Send To Background action, where available, makes the task such as scanning or updating continue running in the background. These tasks are going to take longer to complete but resource usage of the computer is going to be minimal.

Please use **Task Manager** in order to access them later.

If you send to the background, you can continue to check scan progress by clicking '**Open Task Manager**' in the 'Advanced Tasks' interface.

- Any detected threats will be displayed in full at the end of the scan. The alert will tell you how many threats were found; the name and location of the threats and will provide you with virus removal options:



COMODO ?

Attention!
Infections were found! 60

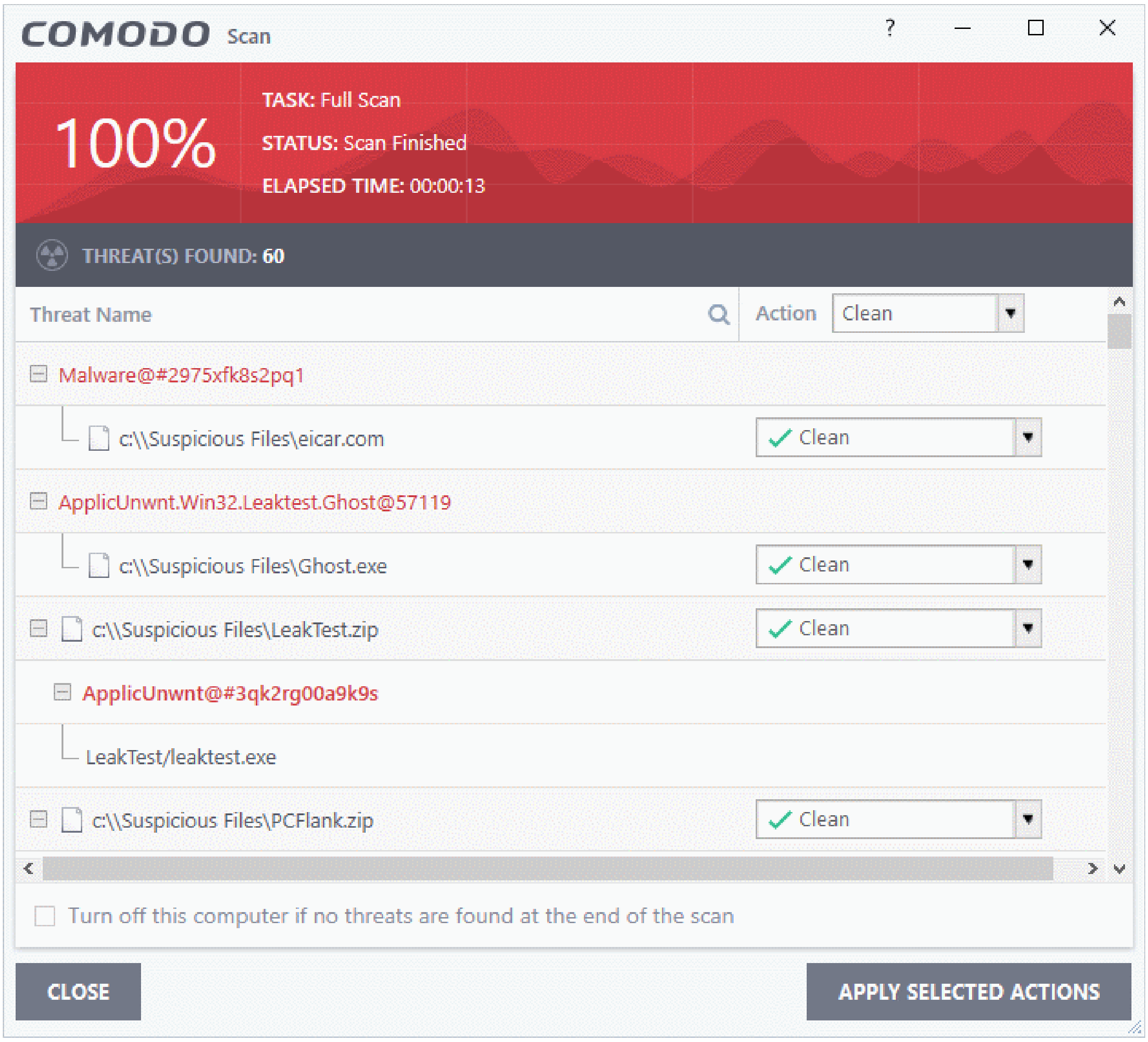
Hi, I'm GeekBuddy.

I am a certified Microsoft expert here to help clean and optimize your system.

To speak to a GeekBuddy call ☎ +1-888-351-7933

□ Do not ask me this question again

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
- See **Comodo GeekBuddy**, for more details on GeekBuddy Expert help.
- If you wish to clean the infections yourself, select 'No, thanks'. The scan results screen will be displayed.


COMODO Scan
100%
TASK: Full Scan
STATUS: Scan Finished
ELAPSED TIME: 00:00:13
THREAT(S) FOUND: 60
Threat Name
Action
Clean
Malware@#2975xfk8s2pq1
c:\\Suspicious Files\eicar.com
✓ Clean
ApplicUnwnt.Win32.Leaktest.Ghost@57119
c:\\Suspicious Files\Ghost.exe
✓ Clean
c:\\Suspicious Files\LeakTest.zip
✓ Clean
ApplicUnwnt@#3qk2rg00a9k9s
LeakTest/leaktest.exe
c:\\Suspicious Files\PCFlank.zip
✓ Clean
□ Turn off this computer if no threats are found at the end of the scan
CLOSE
APPLY SELECTED ACTIONS

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

Note: You will only be presented with the options drop-down if 'Automatically clean threats' is disabled for full scans.

2.1.3. Run a Rating Scan

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

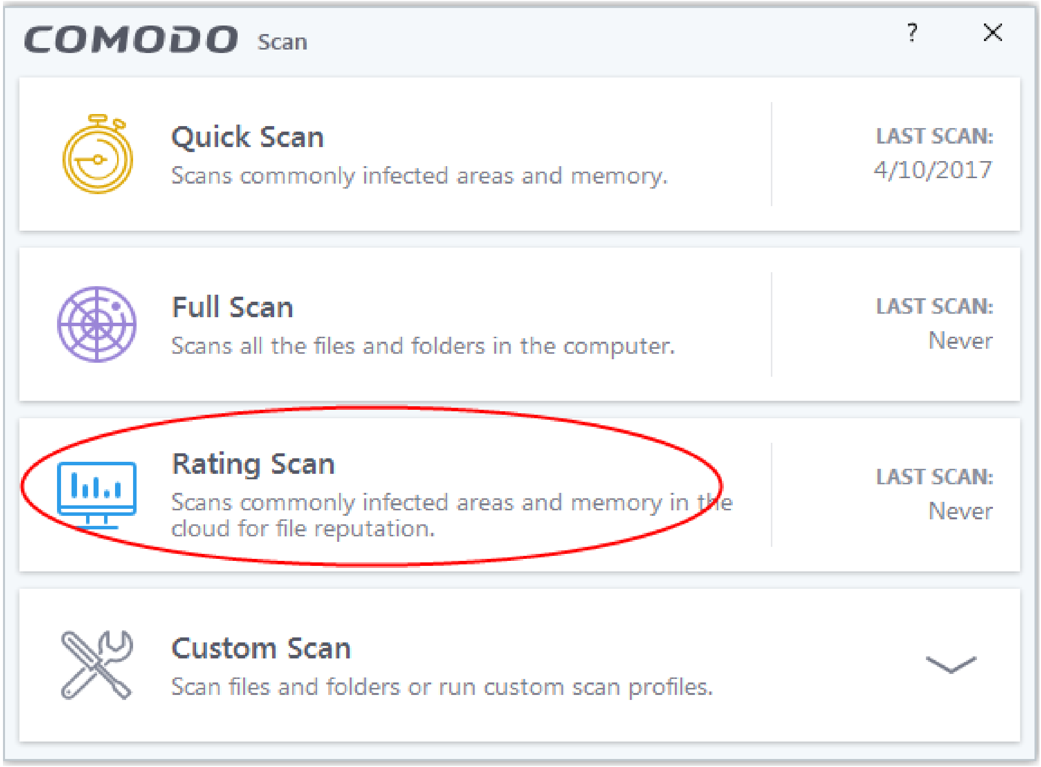
File ratings are as follows:

- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Malicious - the file is unsafe and contains harmful code. You will be presented with disinfection options for such files.

To run a Rating scan

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)

- Select 'Ratings Scan' from the 'Scan' interface.



COMODO Scan

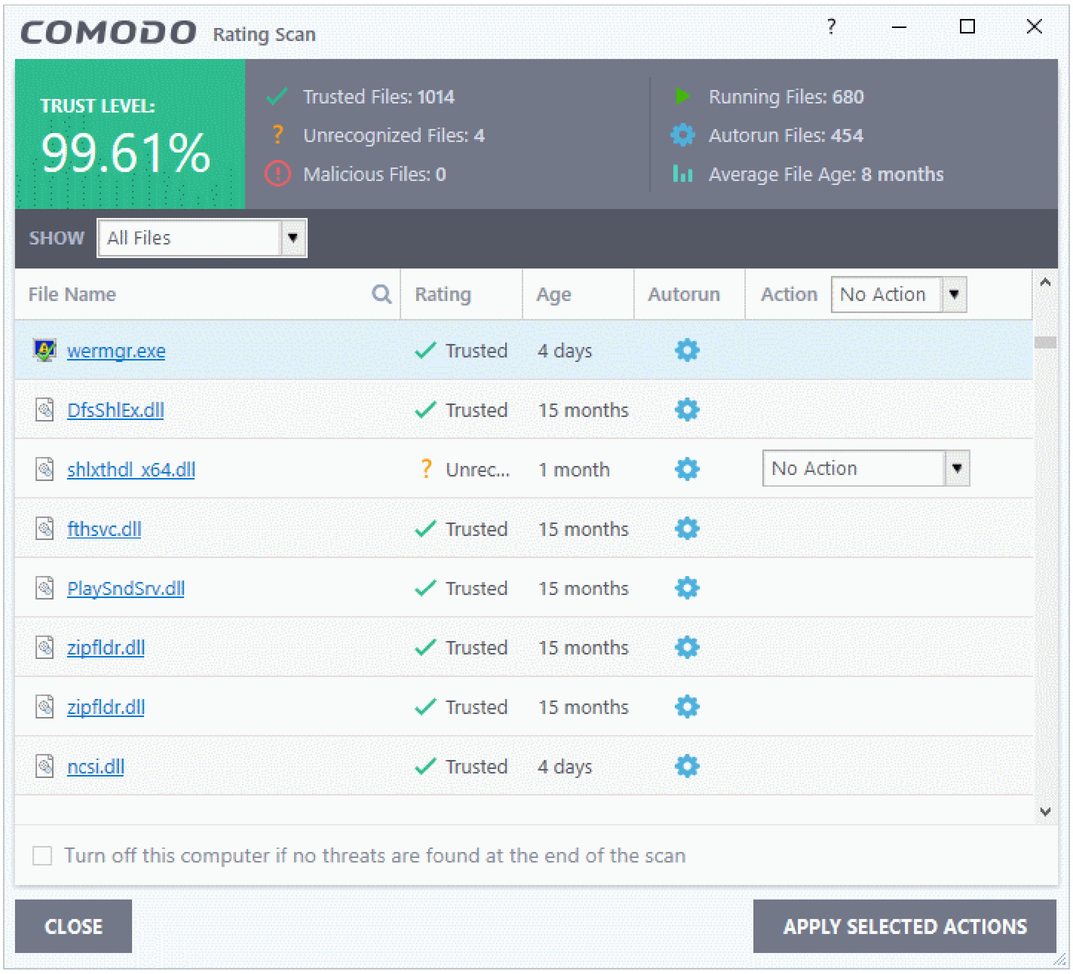
Quick Scan
Scans commonly infected areas and memory.
LAST SCAN: 4/10/2017

Full Scan
Scans all the files and folders in the computer.
LAST SCAN: Never

Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
LAST SCAN: Never

Custom Scan
Scan files and folders or run custom scan profiles.

CIS will analyze all files on your computer then assign them a trust rating. When the analysis has finished, the file ratings will be displayed as follows:



COMODO Rating Scan

TRUST LEVEL: 99.61%

✓ Trusted Files: 1014
? Unrecognized Files: 4
Malicious Files: 0

Running Files: 680
Autorun Files: 454
Average File Age: 8 months

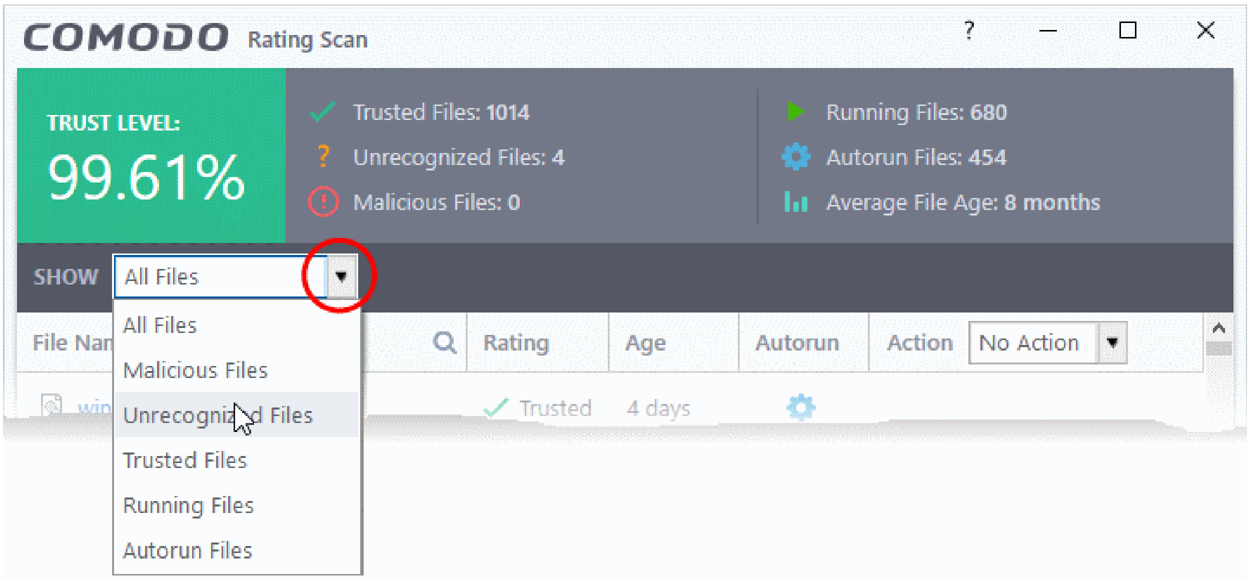
SHOW: All Files

File Name	Rating	Age	Autorun	Action: No Action
wermgr.exe	✓ Trusted	4 days	⚙	
DfsShlEx.dll	✓ Trusted	15 months	⚙	
shlxthdl_x64.dll	? Unrec...	1 month	⚙	No Action
fthsvc.dll	✓ Trusted	15 months	⚙	
PlaySndSrv.dll	✓ Trusted	15 months	⚙	
zipfldr.dll	✓ Trusted	15 months	⚙	
zipfldr.dll	✓ Trusted	15 months	⚙	
ncsi.dll	✓ Trusted	4 days	⚙	

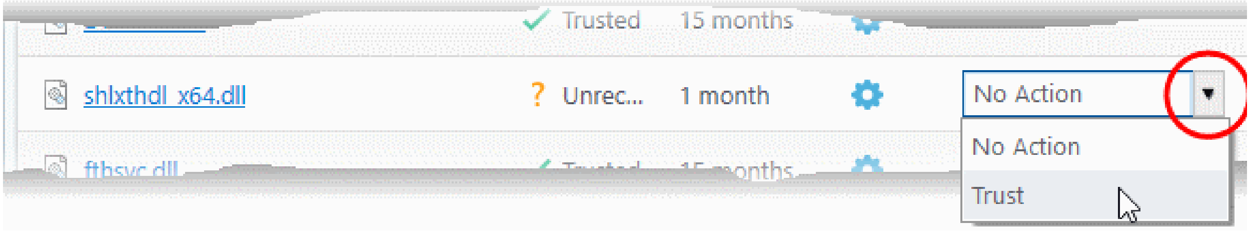
□ Turn off this computer if no threats are found at the end of the scan

Rating Scan Results Table - Column Descriptions	
Column Header	**Description**
File name	The name of the scanned file
Rating	The rating of the file as per the cloud based analysis. The possible values are: • Trusted • Unrecognized • Malicious
Age	The period of time that the file has been stored on your computer
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	Displays a drop-down with actions to be executed on Unrecognized and Malicious files identified.

You can filter the results based on their rating by using the drop-down at top left:



Each file indicated as 'Unrecognized' and 'Malicious' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

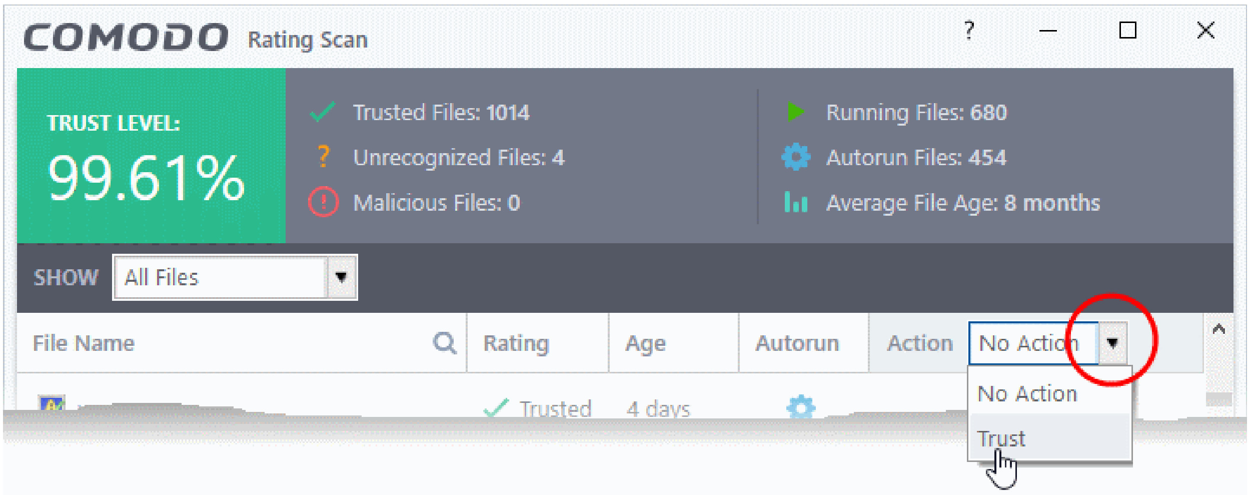


- **Clean -** Available only for malicious files. If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later 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.

- **Trusted** - The file will be moved to '**Trusted Files**' list and will be given 'Trusted' rating from the next scan.

- To apply the same action to all 'Unrecognized' and 'Malicious' files, choose the action from the drop-down menu at the top of the 'Action' column.



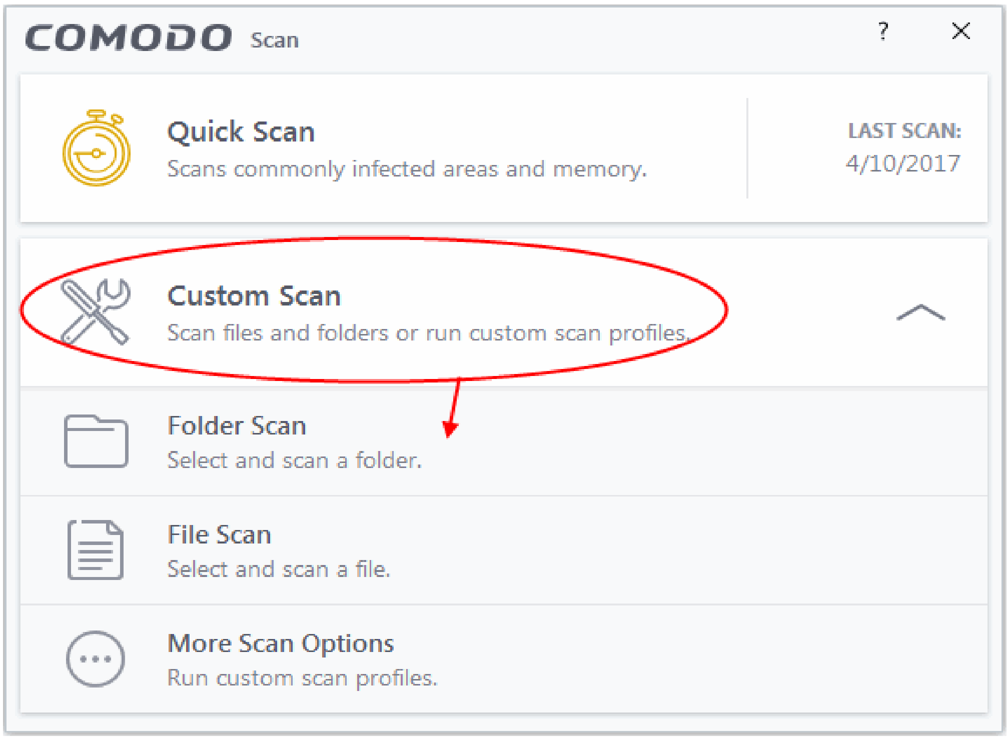
- Click 'Apply Selected Actions' to implement your choice. The selected actions will be applied and a progress bar will be displayed underneath the results.
- Click 'Close' to exit.

2.1.4. Run a Custom Scan

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

To run a custom scan

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)
- Select 'Custom Scan' from the 'Scan' interface:


COMODO Scan
?
Quick Scan
Scans commonly infected areas and memory.
LAST SCAN:
4/10/2017
Custom Scan
Scan files and folders or run custom scan profiles.
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.
More Scan Options
Run custom scan profiles.

The 'Custom Scan' panel contains the following options:

- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file
- **More Scan Options** - create a custom scan profile here

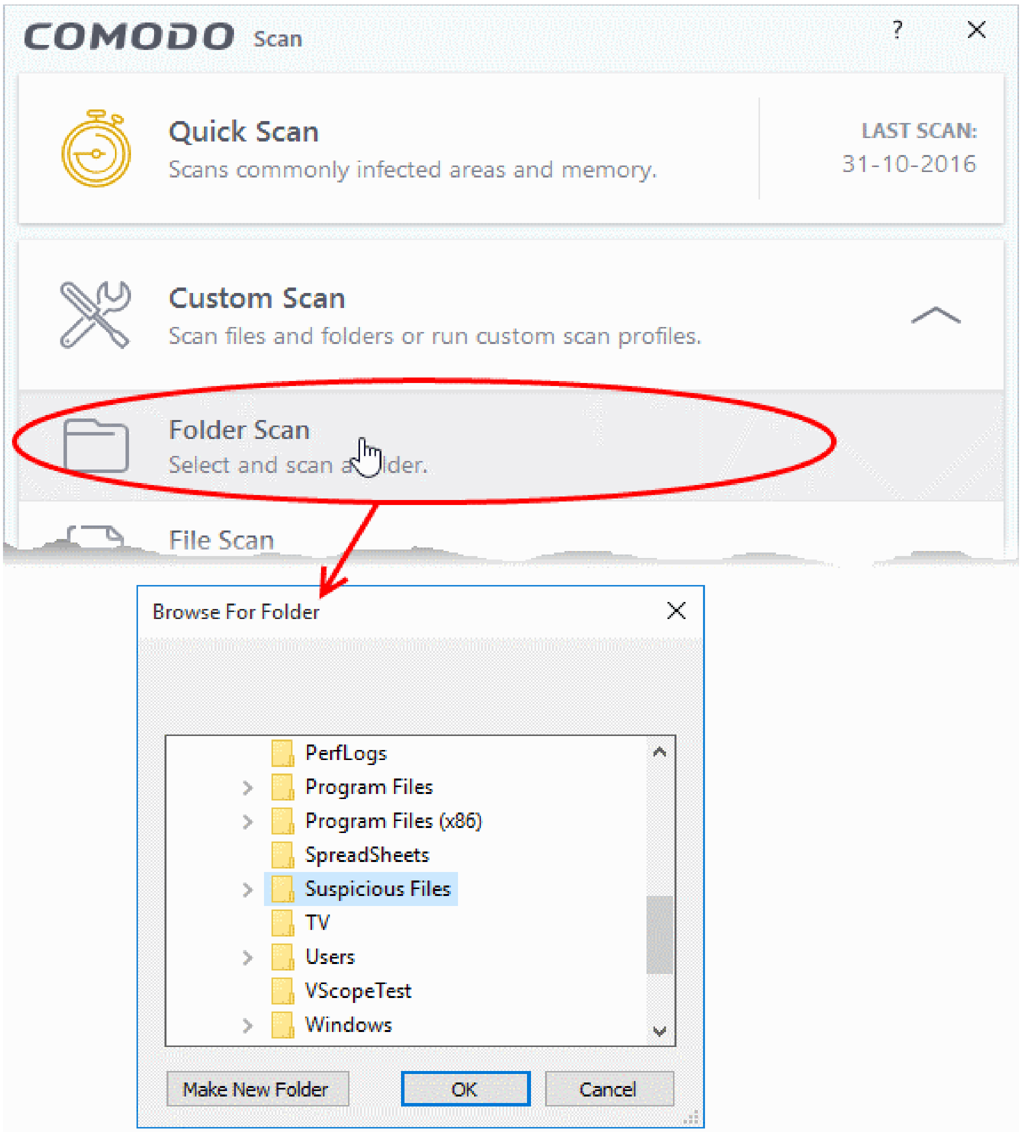
2.1.4.1. Scan a Folder

The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. 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.

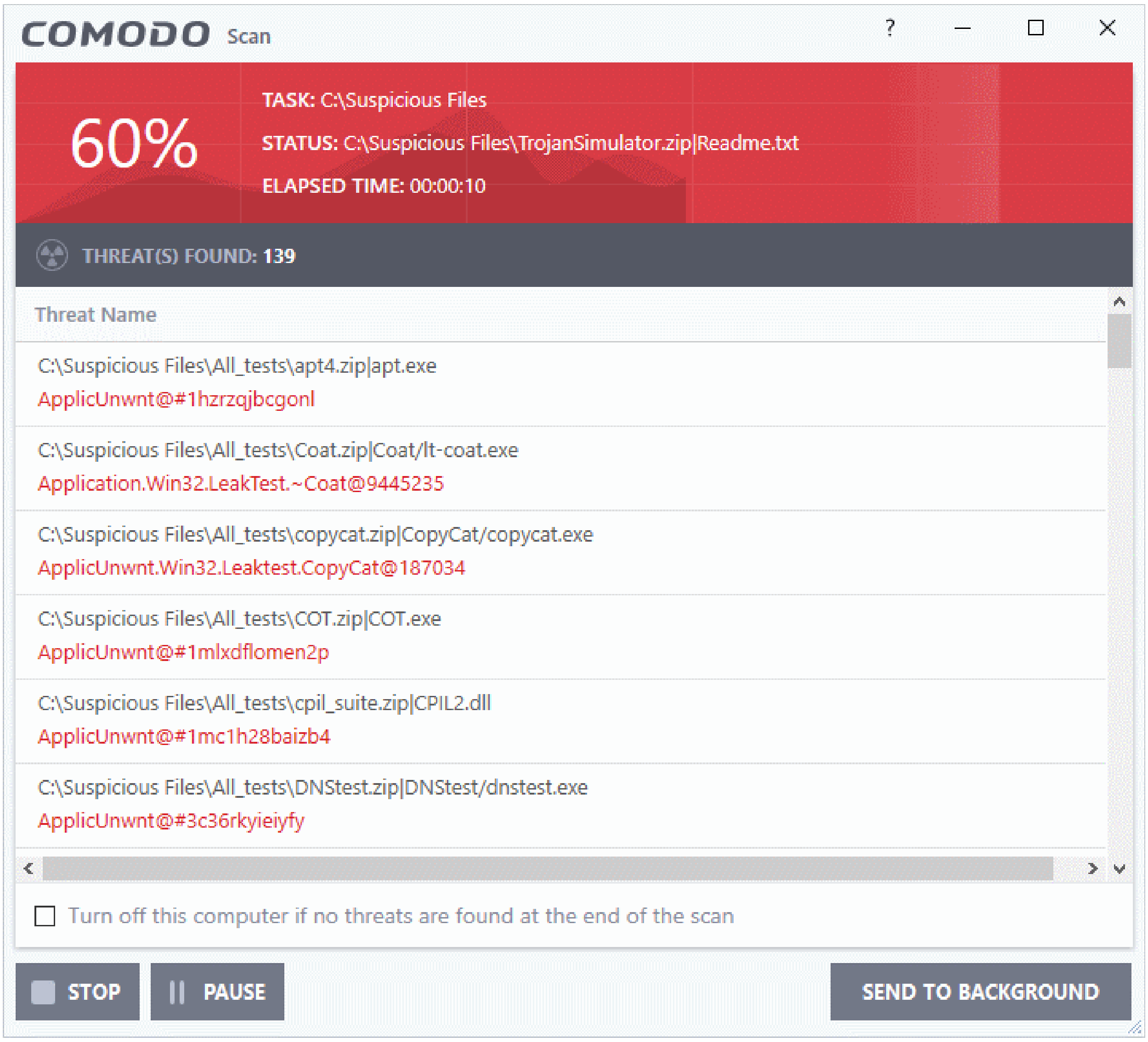
Tip: As an alternative, you can quickly scan a folder by dragging and dropping it onto the CIS interface or by right clicking on it. See '**Scan Individual Files and Folders**' for more details.

To scan a specific folder

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)
- Select 'Custom Scan' from the 'Scan' interface then 'Folder Scan'
- Browse to the folder you want to scan and click 'OK'.



The folder will be scanned instantly and the results will be displayed along with any identified infections:



TASK: C:\Suspicious Files

STATUS: C:\Suspicious Files\TrojanSimulator.zip|Readme.txt

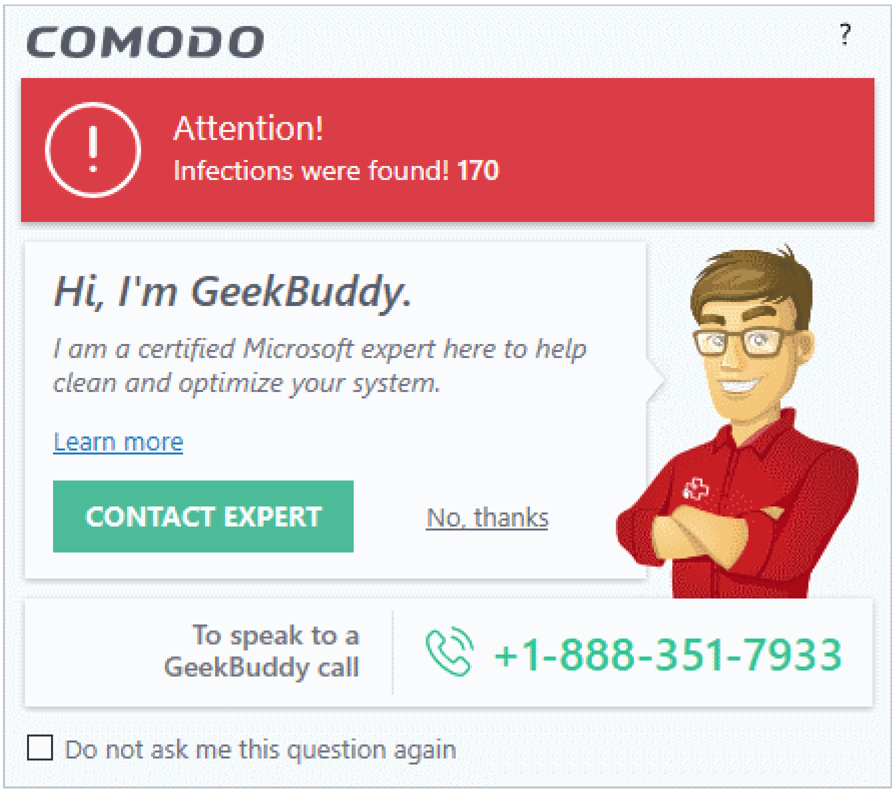
ELAPSED TIME: 00:00:10

THREAT(S) FOUND: 139

Threat Name
C:\Suspicious Files\All_tests\apt4.zip|apt.exe ApplicUnwnt@#1hzrzqjbcgonl
C:\Suspicious Files\All_tests\Coat.zip|Coat/lt-coat.exe Application.Win32.LeakTest.~Coat@9445235
C:\Suspicious Files\All_tests\copycat.zip|CopyCat/copycat.exe ApplicUnwnt.Win32.Leaktest.CopyCat@187034
C:\Suspicious Files\All_tests\COT.zip|COT.exe ApplicUnwnt@#1mlxdflomen2p
C:\Suspicious Files\All_tests\cpil_suite.zip|CPIL2.dll ApplicUnwnt@#1mc1h28baizb4
C:\Suspicious Files\All_tests\DNStest.zip|DNStest/dnstest.exe ApplicUnwnt@#3c36rkyieiyfy

☐ Turn off this computer if no threats are found at the end of the scan

- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



COMODO

Attention!

Infections were found! **170**

Hi, I'm GeekBuddy.

I am a certified Microsoft expert here to help clean and optimize your system.

Learn more

CONTACT EXPERT

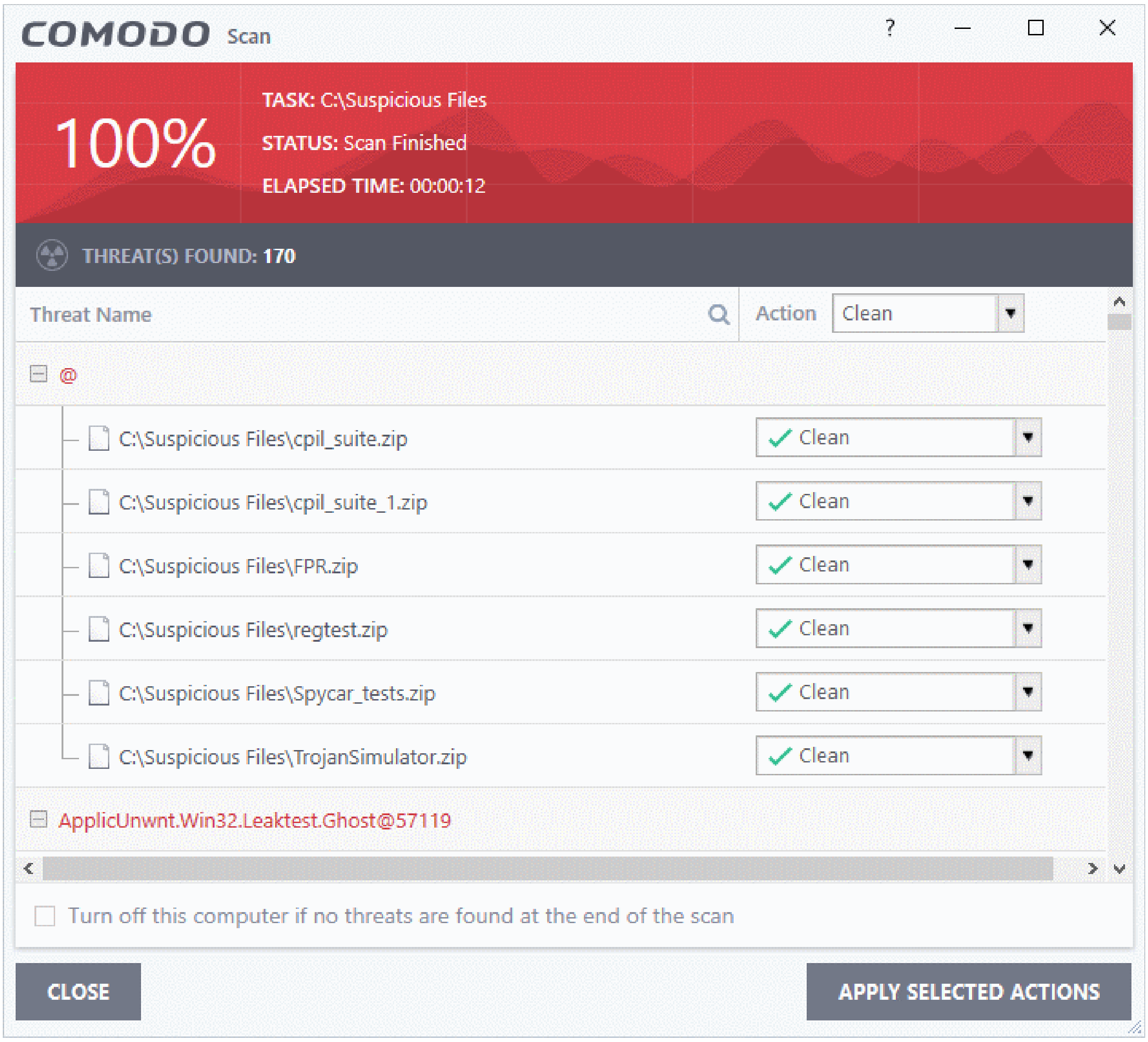
No, thanks

To speak to a GeekBuddy call

☎ +1-888-351-7933

□ Do not ask me this question again

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
- See '**Comodo GeekBuddy**', for more details on GeekBuddy Expert help.
- If you wish to clean the infections yourself, select 'No, thanks'. The scan results screen will be displayed.



COMODO Scan
100%
TASK: C:\Suspicious Files
STATUS: Scan Finished
ELAPSED TIME: 00:00:12
THREAT(S) FOUND: 170
Threat Name
Action
Clean
@
C:\Suspicious Files\cpil_suite.zip
Clean
C:\Suspicious Files\cpil_suite_1.zip
Clean
C:\Suspicious Files\FPR.zip
Clean
C:\Suspicious Files\regtest.zip
Clean
C:\Suspicious Files\Spycar_tests.zip
Clean
C:\Suspicious Files\TrojanSimulator.zip
Clean
ApplicUnwnt.Win32.Leaktest.Ghost@57119
Turn off this computer if no threats are found at the end of the scan
CLOSE
APPLY SELECTED ACTIONS

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 clean, move to quarantine or ignore the threat based in your assessment. See **Processing the infected files** for more details.

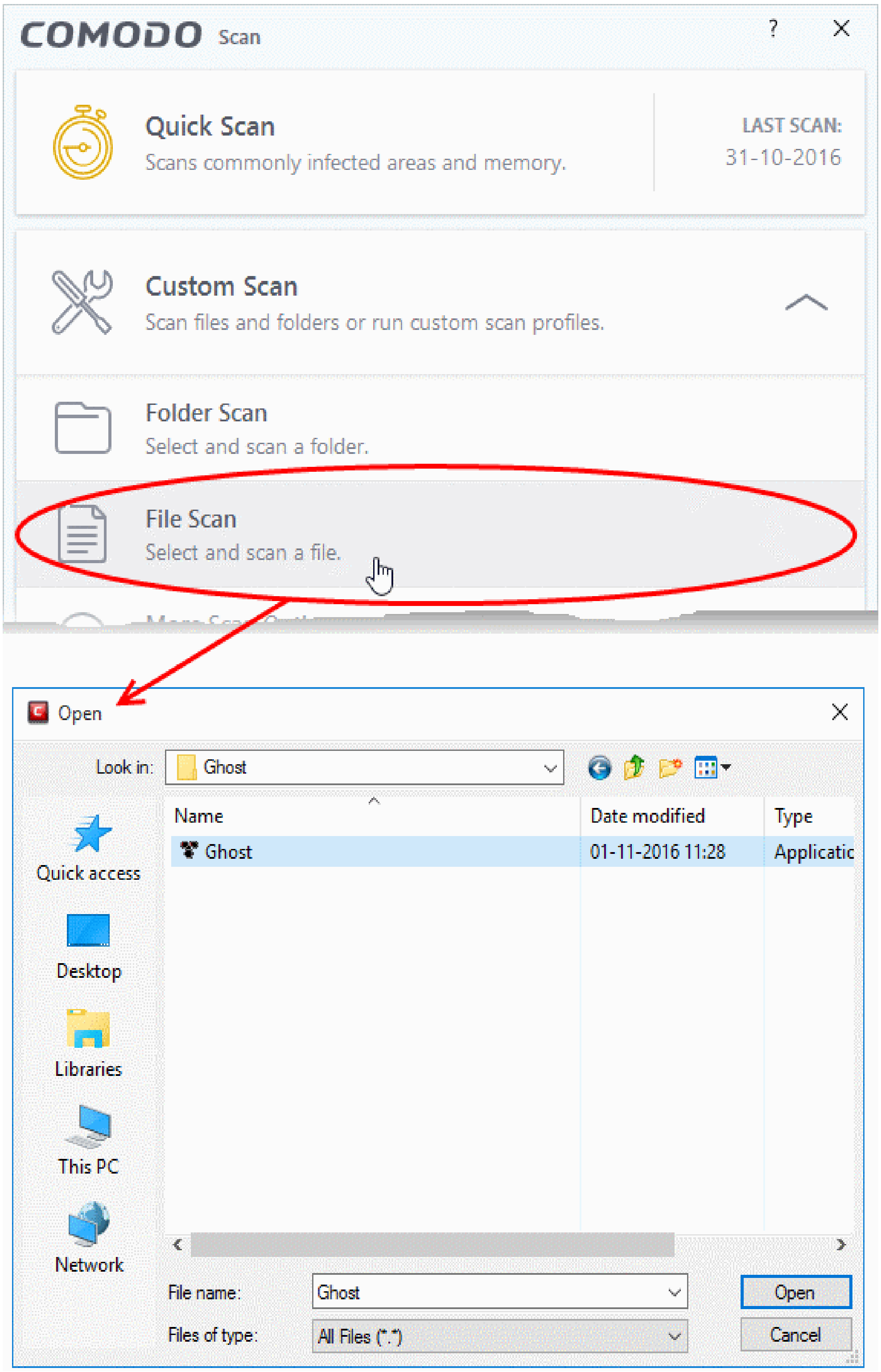
2.1.4.2. Scan a File

The custom scan 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 viruses and other threats before you open it.

> **Tip:** As an alternative, you can quickly scan a file by dragging and dropping it onto the CIS interface or by right clicking on it. See **Instantly Scan Individual Files and Folders** for more details.

To scan a specific file

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)
- Select 'Custom Scan' from the 'Scan' interface then 'File Scan'
- Browse to the file you want to scan and click 'Open'.



Quick Scan
Scans commonly infected areas and memory.
LAST SCAN: 31-10-2016

Custom Scan
Scan files and folders or run custom scan profiles.

Folder Scan
Select and scan a folder.

File Scan
Select and scan a file.

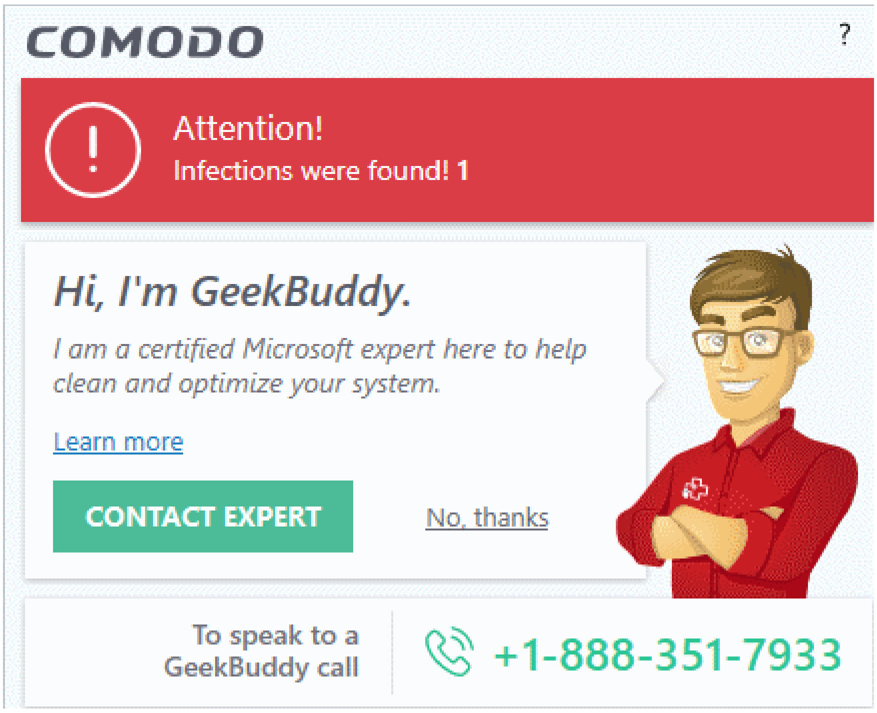
Look in: Ghost

Name	Date modified	Type
Ghost	01-11-2016 11:28	Applicatic

File name: Ghost
Files of type: All Files (*.*)

The file will be scanned instantly.

- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



COMODO

Attention!

Infections were found! 1

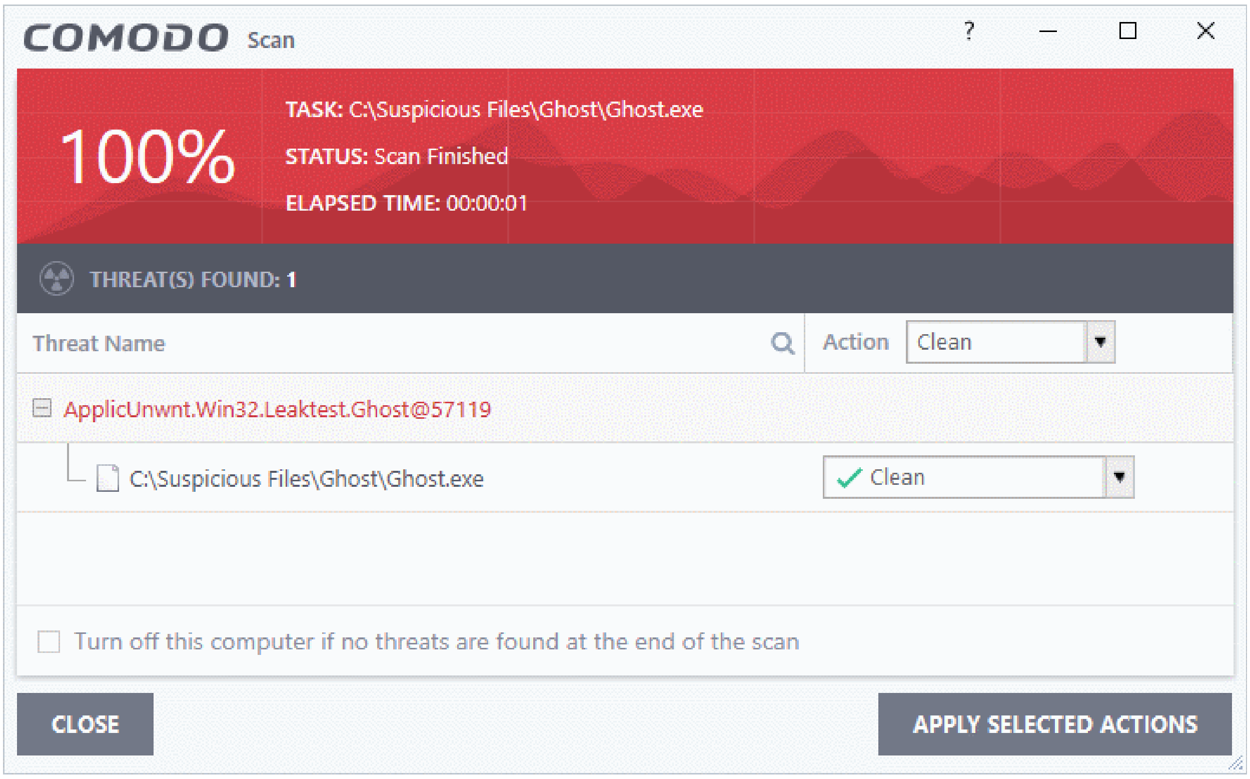
Hi, I'm GeekBuddy.

I am a certified Microsoft expert here to help clean and optimize your system.

Learn more

To speak to a GeekBuddy call ☎ +1-888-351-7933

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - See **Comodo GeekBuddy**, for more details on GeekBuddy Expert help.
- If you wish to clean the infections yourself, select 'No, thanks'. The scan results screen will be displayed.



COMODO Scan

100%

TASK: C:\Suspicious Files\Ghost\Ghost.exe

STATUS: Scan Finished

ELAPSED TIME: 00:00:01

THREAT(S) FOUND: 1

Threat Name	Action: Clean
ApplicUnwnt.Win32.Leaktest.Ghost@57119	
C:\Suspicious Files\Ghost\Ghost.exe	✓ Clean

□ Turn off this computer if no threats are found at the end of the scan

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 clean, move to quarantine or ignore the threat based in your assessment. See **Processing the infected files** for more details.

2.1.4.3. Create, Schedule and Run a Custom Scan

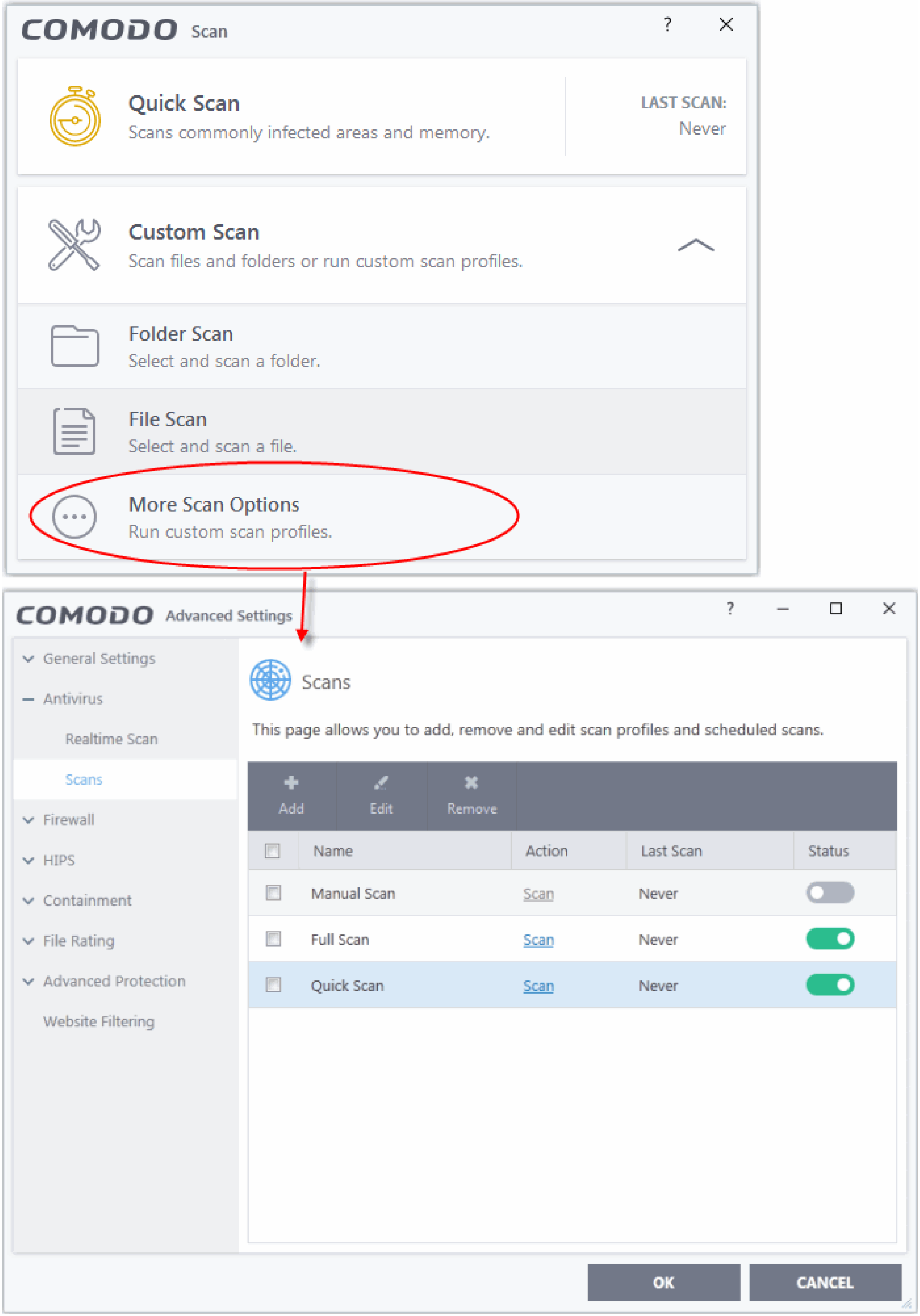
Custom scan profiles allow you configure your own scan with your own scan settings. For each profile, you can define exactly which files and folders to scan, what time they should be scanned and set other scan parameters. Once created and saved, your custom scan profile will appear in the scans interface and can be run on-demand, at any time.

- **Creating a Scan Profile**
- **Running a custom scan**

To create a custom profile

- Click the 'Scan' tile on the CIS home screen (**click here** for alternative ways to open the 'Scan' interface)
- Select 'Custom Scan' from the 'Scan' interface then 'More Scan Options'

The 'Advanced Settings' interface will open at the 'Scans' page. This shows a list of pre-defined and user created scan profiles. You can create and manage new custom scan profiles from this interface:



COMODO Scan

Quick Scan
Scans commonly infected areas and memory.

LAST SCAN: Never

Custom Scan
Scan files and folders or run custom scan profiles.

Folder Scan
Select and scan a folder.

File Scan
Select and scan a file.

More Scan Options
Run custom scan profiles.

COMODO Advanced Settings

Scans

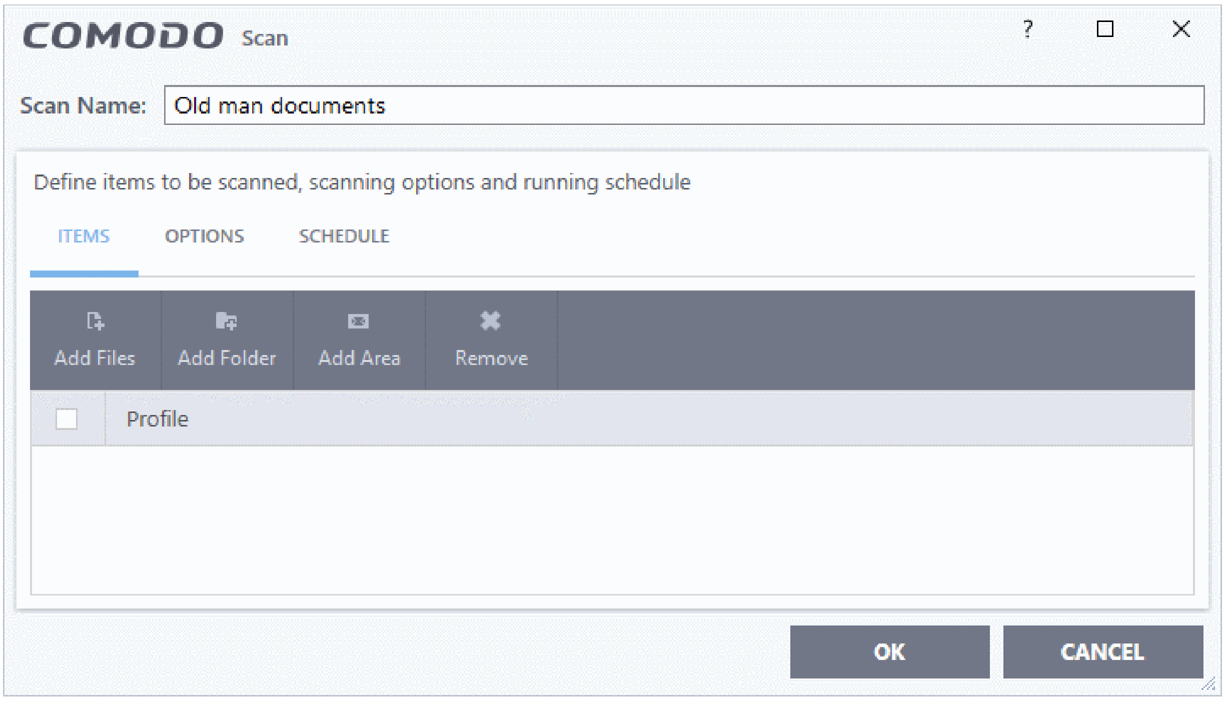
This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	Off
□	Full Scan	Scan	Never	On
□	Quick Scan	Scan	Never	On

Tip: You can also get to this scan configuration screen by clicking 'Settings' on the CIS home screen then 'Antivirus' > 'Scans'

- To add a new custom scan profile, click 'Add' from the options at the top.

The 'Scan' interface for configuring the new custom scan will open.



Scan Name: Old man documents

Define items to be scanned, scanning options and running schedule

- Type a name for the profile in the 'Scan Name' text box.

The next steps are to:

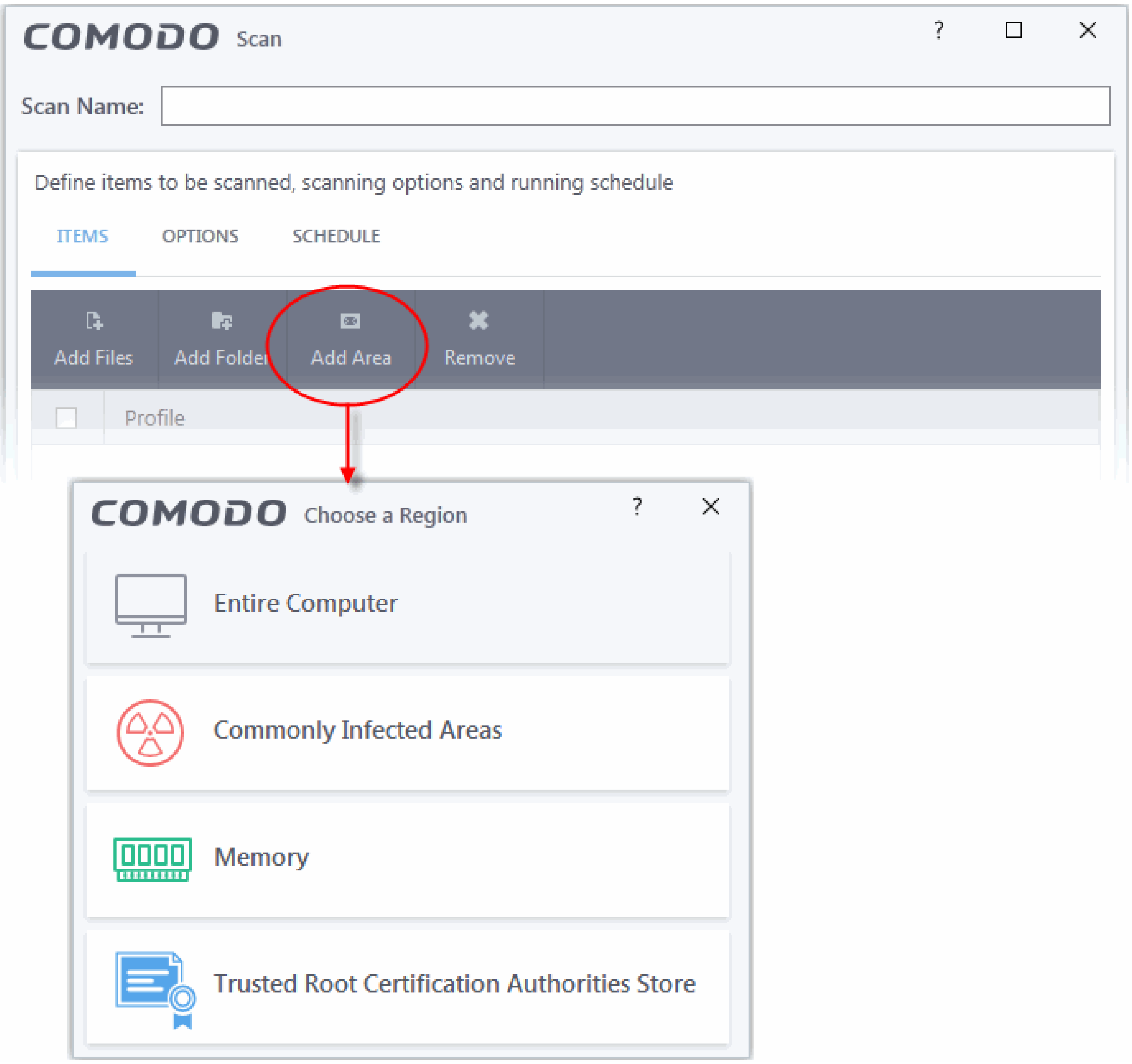
- **Select the items to scan**
- **Configure the scanning options for the profile (Optional)**
- **Configure a schedule for the scan to run periodically (Optional)**

To select the items to scan

- Click Items' at the top of the 'Scan' interface.

The buttons at the top allow you to add scan items in three ways:

- Add File - Add individual files to the profile. Click the 'Add Files' button and navigate to the file to be scanned in the 'Open' dialog and click 'Open'.
- Add Folder – Add entire folders to the profile. Click the 'Add Folder' button and choose the folder from the 'Browse for Folder' dialog.
- Add Area – Include specific regions of your computer in the scan profile (choice of 'Full Computer', 'Commonly Infected Areas', 'System Memory' and 'Trusted Root Certificate Store')

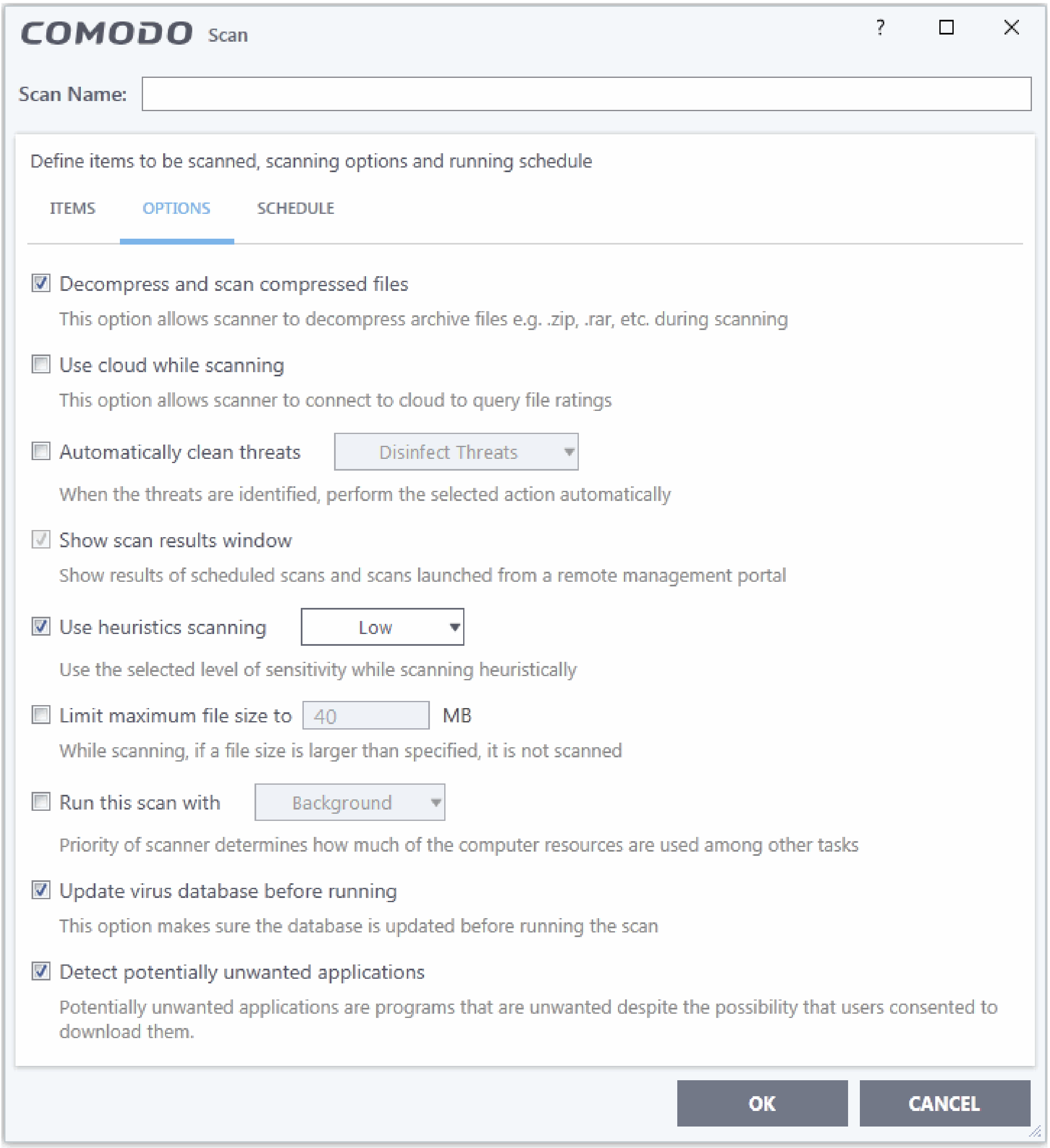


- Repeat the process to add more items to the profile.
- To remove an item, select it and click 'Remove'.

To configure Scanning Options

- Click 'Options' at the top of the 'Scan' interface

The options to customize the scan will be displayed.


COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

☑ Decompress and scan compressed files

This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

□ Use cloud while scanning

This option allows scanner to connect to cloud to query file ratings

□ Automatically clean threats — Disinfect Threats

When the threats are identified, perform the selected action automatically

☑ Show scan results window

Show results of scheduled scans and scans launched from a remote management portal

☑ Use heuristics scanning — Low

Use the selected level of sensitivity while scanning heuristically

□ Limit maximum file size to 40 MB

While scanning, if a file size is larger than specified, it is not scanned

□ Run this scan with — Background

Priority of scanner determines how much of the computer resources are used among other tasks

☑ Update virus database before running

This option makes sure the database is updated before running the scan

☑ Detect potentially unwanted applications

Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download them.

- **Decompress and scan compressed files -** If enabled, the antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
- **Use cloud while scanning -** Enables the scanner to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. ***(Default = Disabled)***.
- **Automatically clean threats -** Allows you to choose which action should be taken against malware detected by the scan. (***Default = Disabled***).

  The available options are:

  - **Quarantine Threats -** Malicious items will be moved to quarantine. You can view the items in the quarantine and choose to remove them or restore them (in case of false positives). Refer to the section **Manage Quarantined Items** for more details.

- **Disinfect Threats** - If a disinfection routine is available for the detected threat, the antivirus will remove the threat from the infected file and retain the application safe. Otherwise the item will be moved to 'Quarantine'.

- **Show scan results window -** If selected, displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on) found during scheduled scan and scan executed from remote management portal.
- **Use heuristics scanning -** Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Enabled).***

  Background Info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' traits or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist.

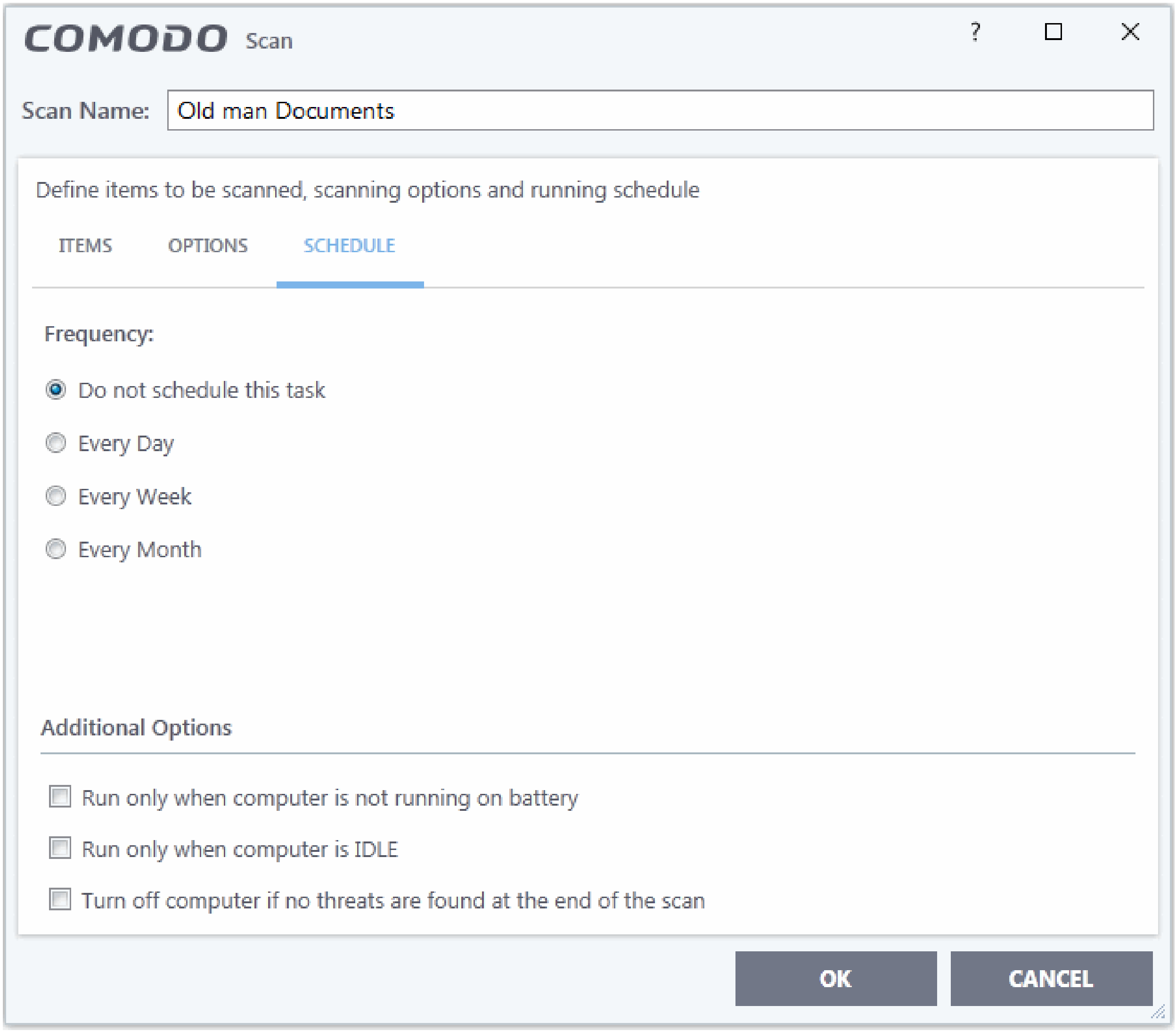
  This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  On selecting this option, you can choose the level for heuristic scanning from the drop-down.

  - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. ***(Default)***
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run this scan with** - Enables you to set the priority of the scan profile. ***(Default = Disabled)***. You can select the priority from the drop-down. The available options are:
  - High
  - Normal
  - Low
  - Background.
- **Update virus database before running** - Instructs Comodo Internet Security to check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning ***(Default = Enabled)***.
- **Detect potentially unwanted applications** - When this option is selected the antivirus will also scan for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional 'utility' when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the internet. ***(Default = Enabled)***.

To schedule the scan to run at specified times

- Click 'Schedule' from the top of the 'Scans' interface.



COMODO Scan

Scan Name: Old man Documents

Define items to be scanned, scanning options and running schedule

Frequency:

● Do not schedule this task

○ Every Day

○ Every Week

○ Every Month

Additional Options

□ Run only when computer is not running on battery

□ Run only when computer is IDLE

□ Turn off computer if no threats are found at the end of the scan

The options to schedule the scans will be displayed.

- **Do not schedule this task -** The scan profile will be created but will not run automatically. The profile will be available for manual, on-demand scans.
- **Every Day -** Scans the areas defined in the profile every day at the time specified in the 'Start Time' field.
- **Every Week -** Scans the areas defined in the profile on the day(s) specified in 'Days of the Week' field at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- **Every Month -** Scans the areas defined in the profile on the date(s) specified in 'Days of the month' field at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery -** The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or any other battery driven portable computer.
- **Run only when computer is IDLE -** The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan -** Selecting this option turns your computer off if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- **Run during Windows Maintenance -** Only available for Windows 8 and later. Select this option if

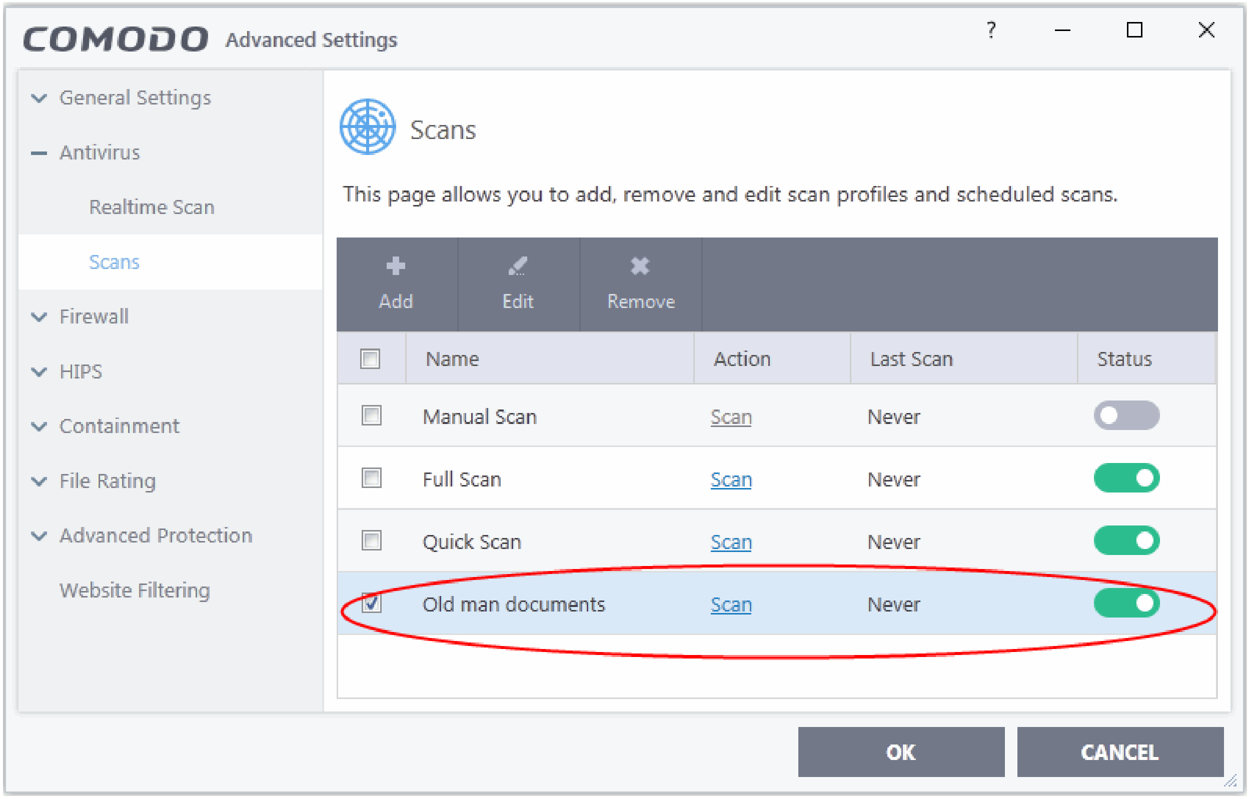
you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.

- The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See the explanation of **Automatically Clean Threats** above.

> **Note**: The scheduled scan will run only if the scan profile is enabled. Use the switch in the 'Status' column to toggle a profile on or off.

- Click 'OK' to save the profile.

The profile will be available for deployment in future.



Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

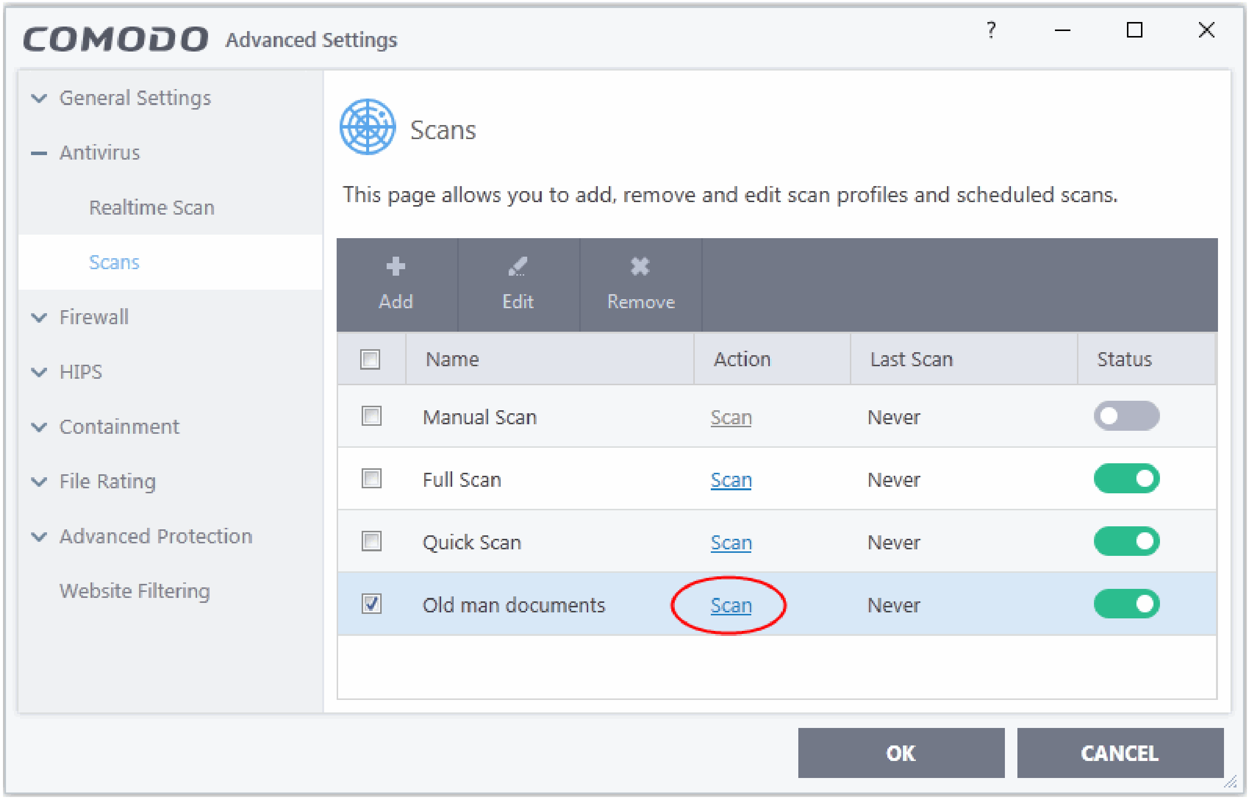
□	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	○
□	Full Scan	Scan	Never	●
□	Quick Scan	Scan	Never	●
☑	Old man documents	Scan	Never	●

To run a custom scan

- Click 'Scan' from the 'General Tasks' interface and click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane

The 'Scans' pane will open with a list of existing scan profiles:

- Click the 'Scan' link in the 'Action' column of profile you wish to run:

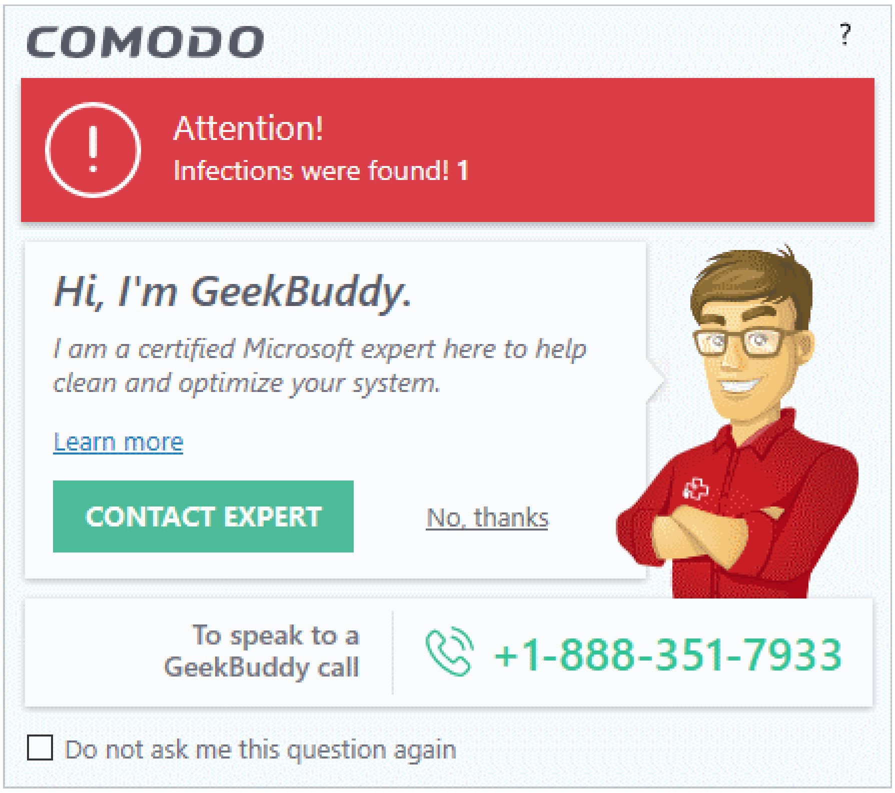


Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

☐	Name	Action	Last Scan	Status
☐	Manual Scan	Scan	Never	○
☐	Full Scan	Scan	Never	●
☐	Quick Scan	Scan	Never	●
☑	Old man documents	Scan	Never	●

The Antivirus will start scanning the locations defined in the profile. On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



Attention!
Infections were found! 1

Hi, I'm GeekBuddy.

I am a certified Microsoft expert here to help clean and optimize your system.

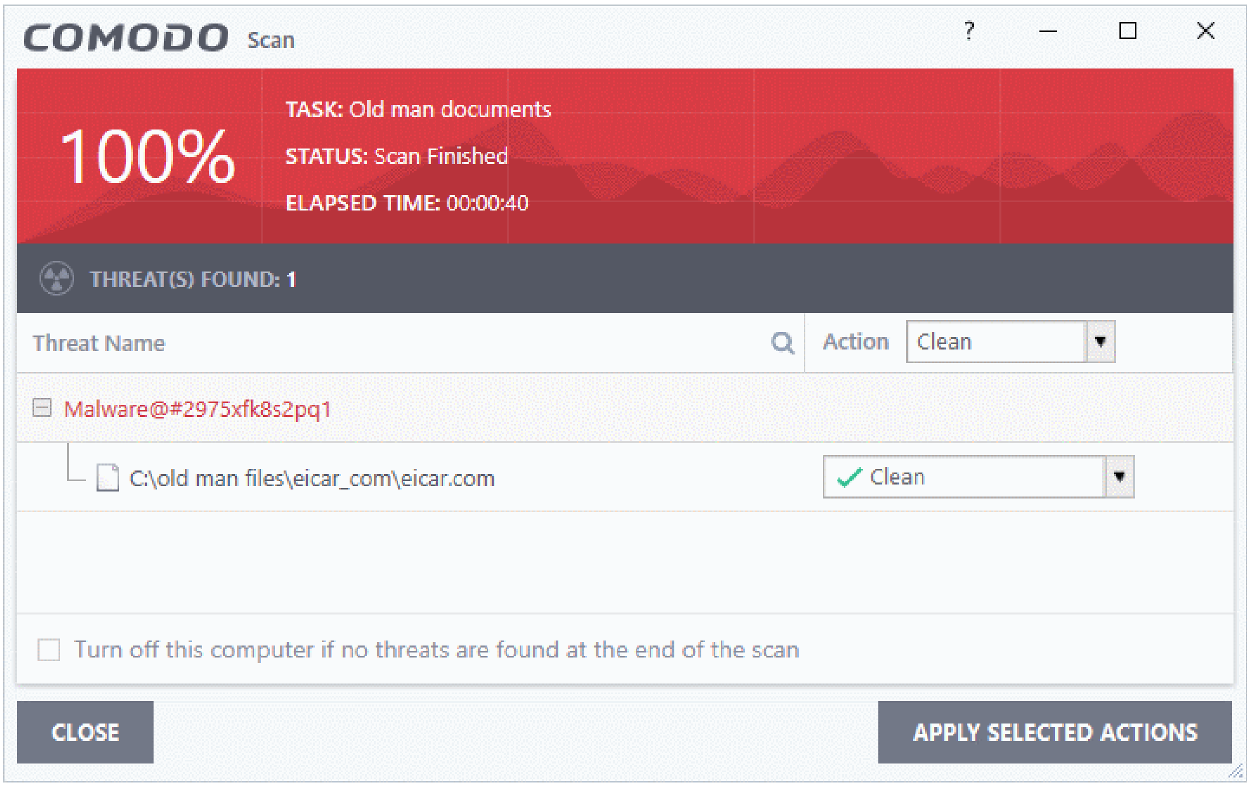
To speak to a GeekBuddy call ☎ +1-888-351-7933

☐ Do not ask me this question again

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.

- See **Comodo GeekBuddy**, for more details on GeekBuddy Expert help,

- If you wish to clean the infections yourself, select 'No, thanks'. The scan results screen will be displayed.



TASK: Old man documents

STATUS: Scan Finished

ELAPSED TIME: 00:00:40

Threat Name	Action: Clean
Malware@#2975xfk8s2pq1	
C:\old man files\eicar_com\eicar.com	✓ Clean

□ Turn off this computer if no threats are found at the end of the scan

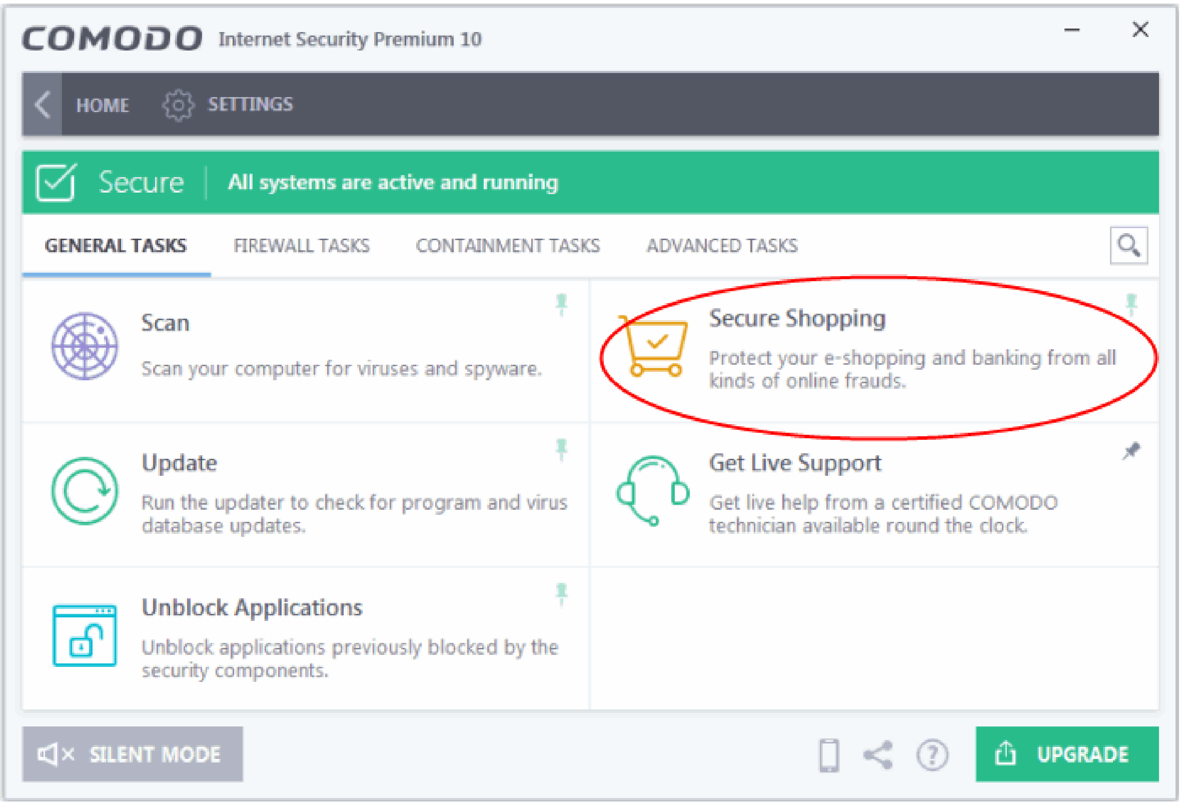
The scan results window displays the number of objects scanned and the number of threats (viruses, rootkits, malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. See **Processing the infected files** for more details.

2.2. Secure Shopping Settings

Comodo Secure Shopping delivers total protection for your online banking and shopping sessions by ensuring you connect to these websites from within an highly secure virtual environment. This creates a dedicated, threat resistant tunnel between you and your target website which cannot be monitored or attacked by any other processes running on your computer. Secure Shopping is covered in more detail in **Comodo Secure Shopping**.

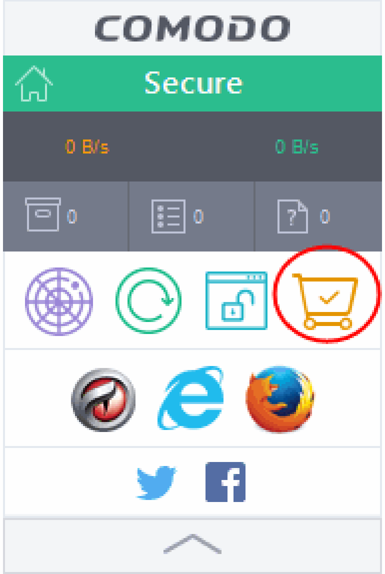
To open Secure Shopping:

- Click 'Tasks' > 'General Tasks' > 'Secure Shopping'

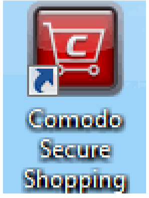

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
SILENT MODE
UPGRADE

OR

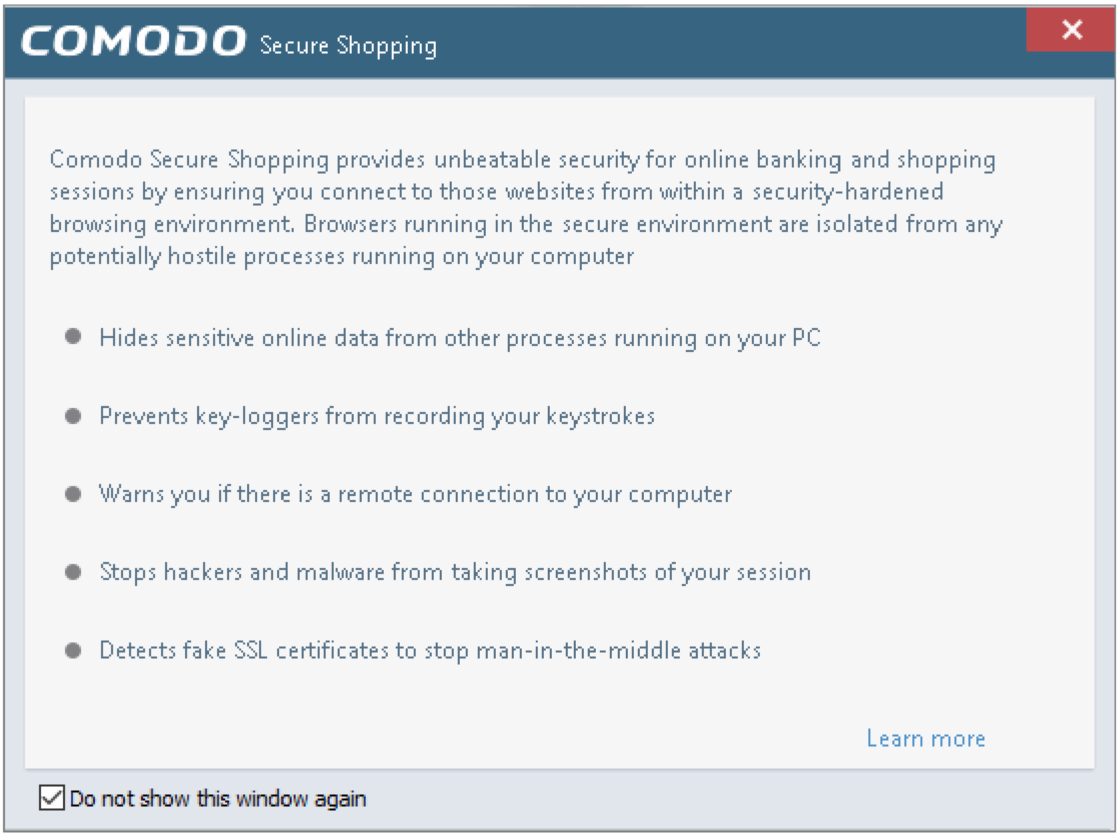
- Click the 'Secure Shopping' icon from the CIS Desktop widget



- Alternatively, double-click the secure shopping desktop shortcut:



When you start the application, a welcome screen will appear which explains the benefits of secure shopping:



Comodo Secure Shopping provides unbeatable security for online banking and shopping sessions by ensuring you connect to those websites from within a security-hardened browsing environment. Browsers running in the secure environment are isolated from any potentially hostile processes running on your computer

- Hides sensitive online data from other processes running on your PC
- Prevents key-loggers from recording your keystrokes
- Warns you if there is a remote connection to your computer
- Stops hackers and malware from taking screenshots of your session
- Detects fake SSL certificates to stop man-in-the-middle attacks

☑ Do not show this window again

- Check 'Do not show this window again' to disable the welcome screen in future.

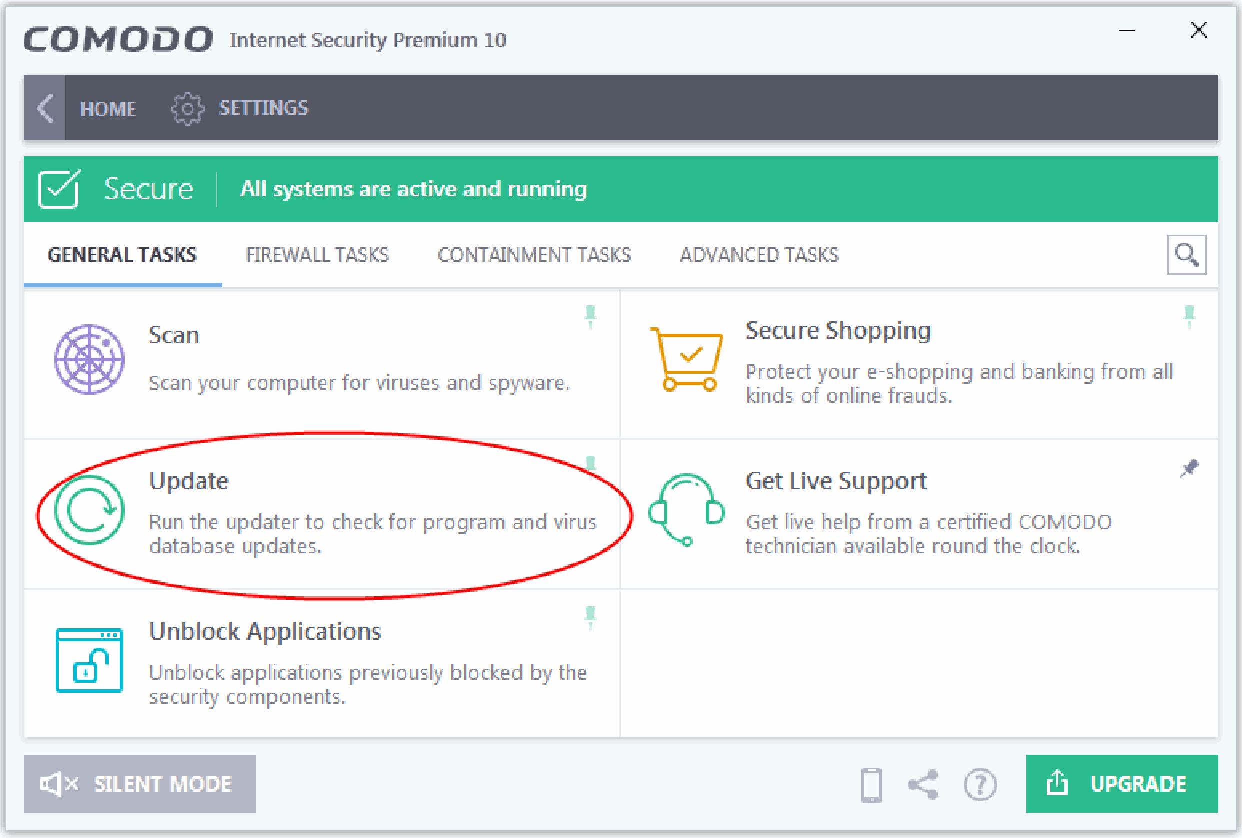
2.3. Manage Virus Database and Program Updates

In order to guarantee continued and effective antivirus protection, it is imperative that your virus databases are updated as regularly as possible. Updates can be downloaded to your system **manually** or **automatically** from Comodo's update servers.

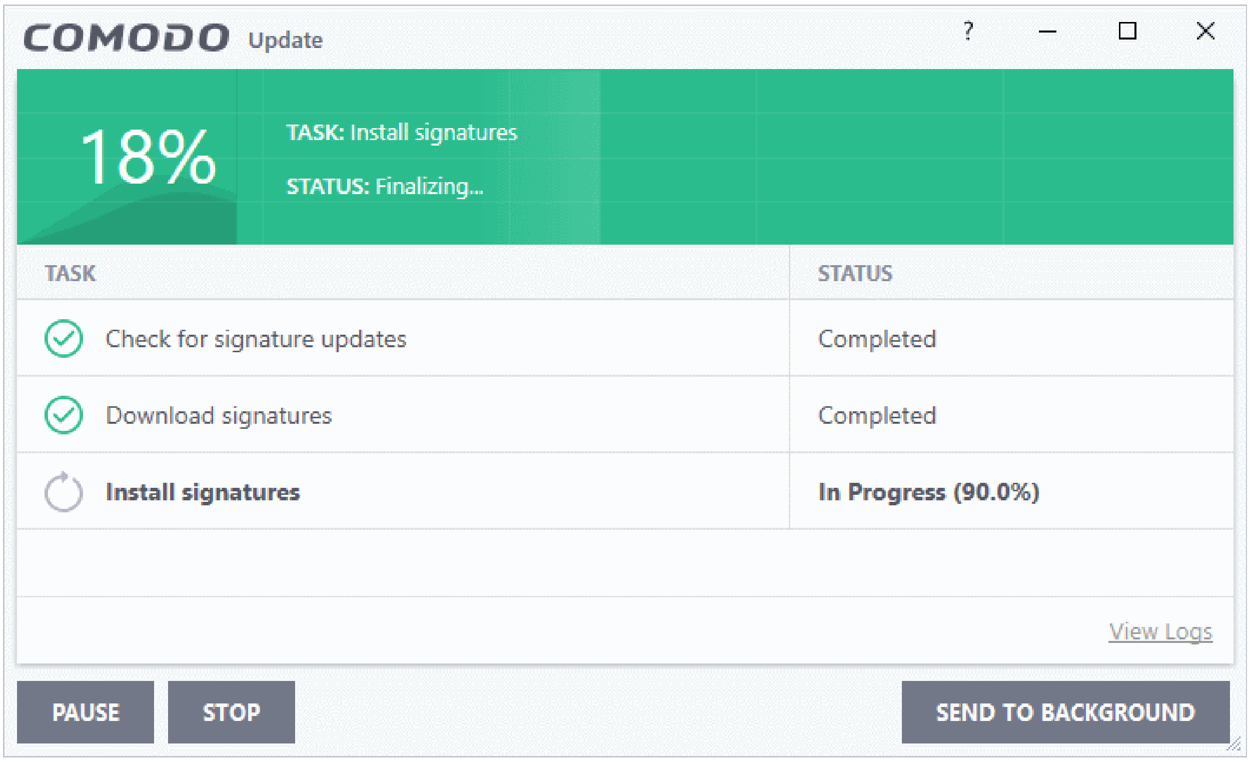
Note: You must be connected to Internet to download updates.

To manually check for the latest virus and program updates

1. Switch to the 'Tasks' screen and click 'General Tasks' to open the 'General Tasks' interface.
2. Click 'Update'. The application will start checking for program and database updates.


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
SILENT MODE
UPGRADE

Signature updates will be downloaded and installed first if they are available:

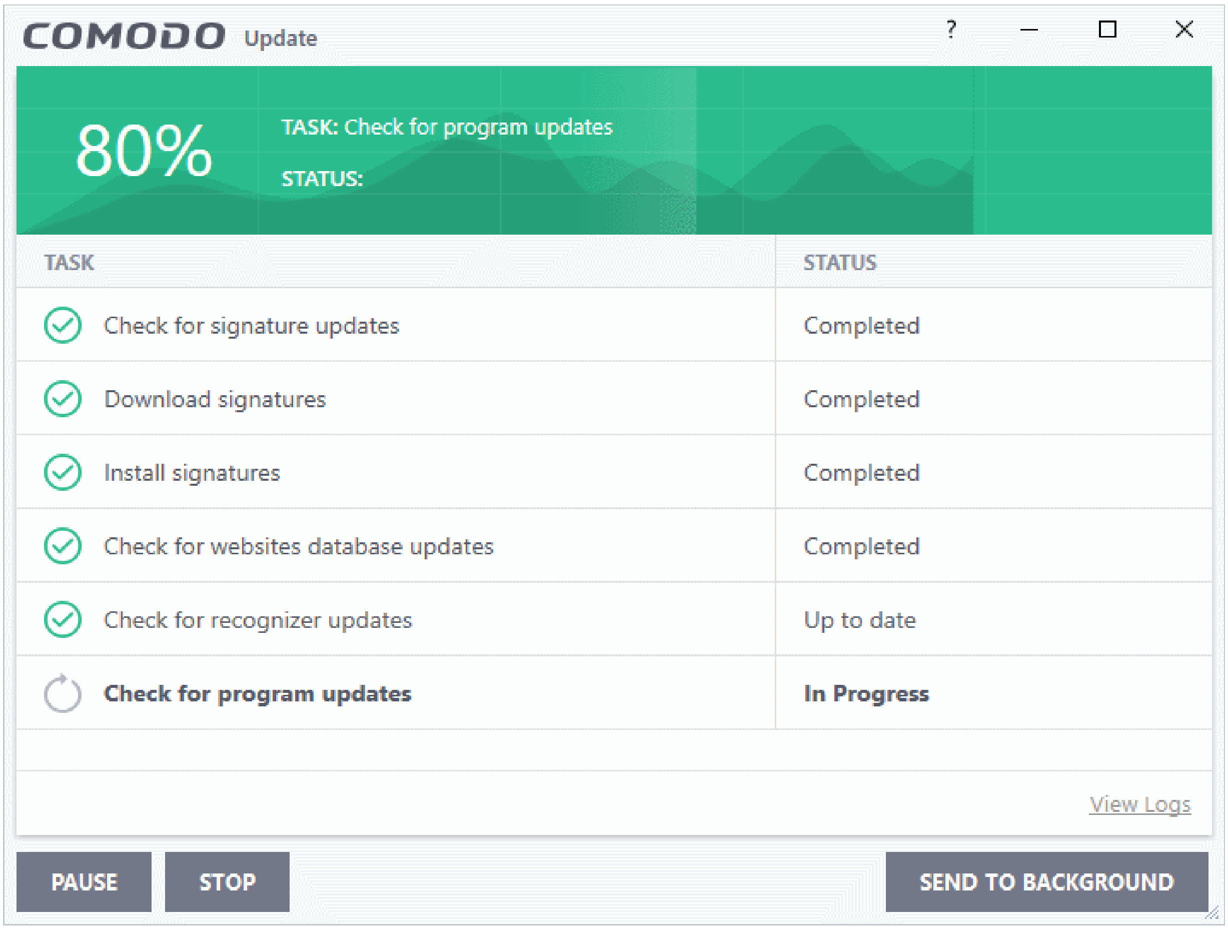


TASK: Install signatures

STATUS: Finalizing...

TASK	STATUS
Check for signature updates	Completed
Download signatures	Completed
Install signatures	**In Progress (90.0%)**

The updater will then check for web filtering, VirusScope (recognizer) and program updates:



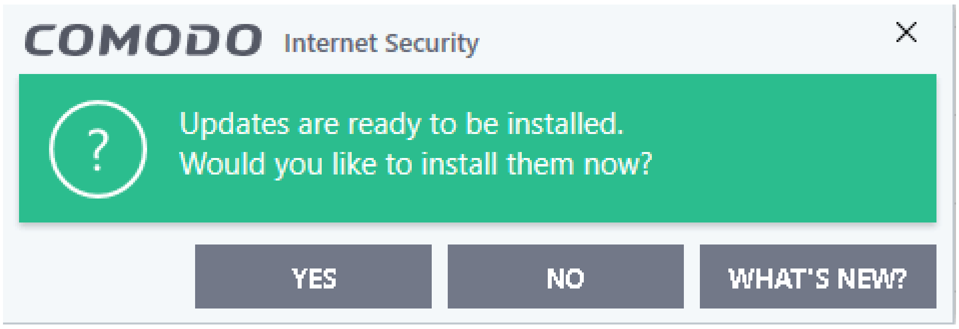
80%

TASK: Check for program updates

STATUS:

TASK	STATUS
✓ Check for signature updates	Completed
✓ Download signatures	Completed
✓ Install signatures	Completed
✓ Check for websites database updates	Completed
✓ Check for recognizer updates	Up to date
Check for program updates	**In Progress**

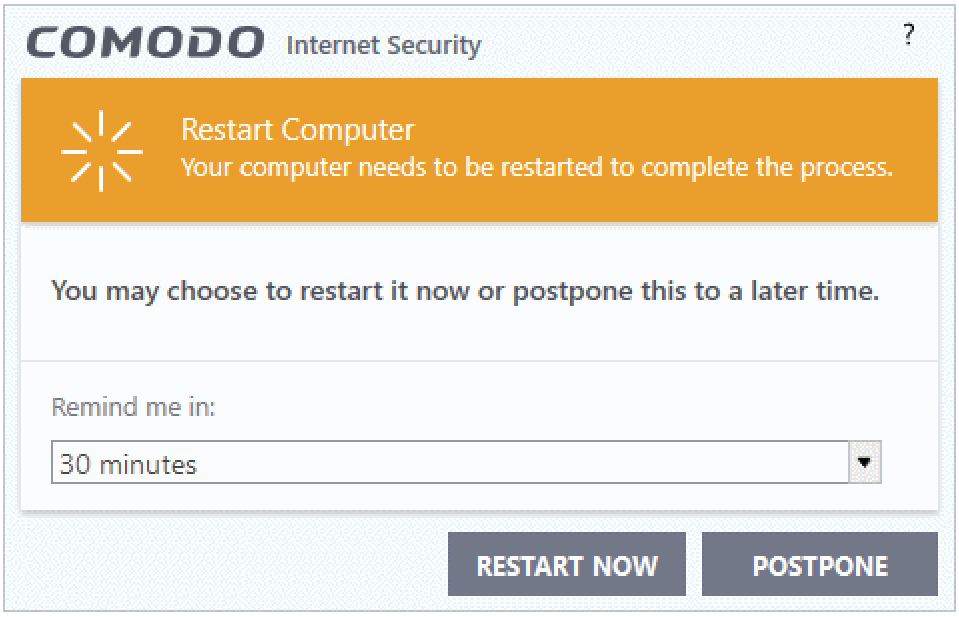
If any updates are available, you will be asked to confirm installation at the following dialog:



Updates are ready to be installed.
Would you like to install them now?

- Click 'Yes' to begin installation:

Your computer will need to be restarted to complete the update process. You can restart immediately or postpone the restart until later:



COMODO Internet Security

Restart Computer

Your computer needs to be restarted to complete the process.

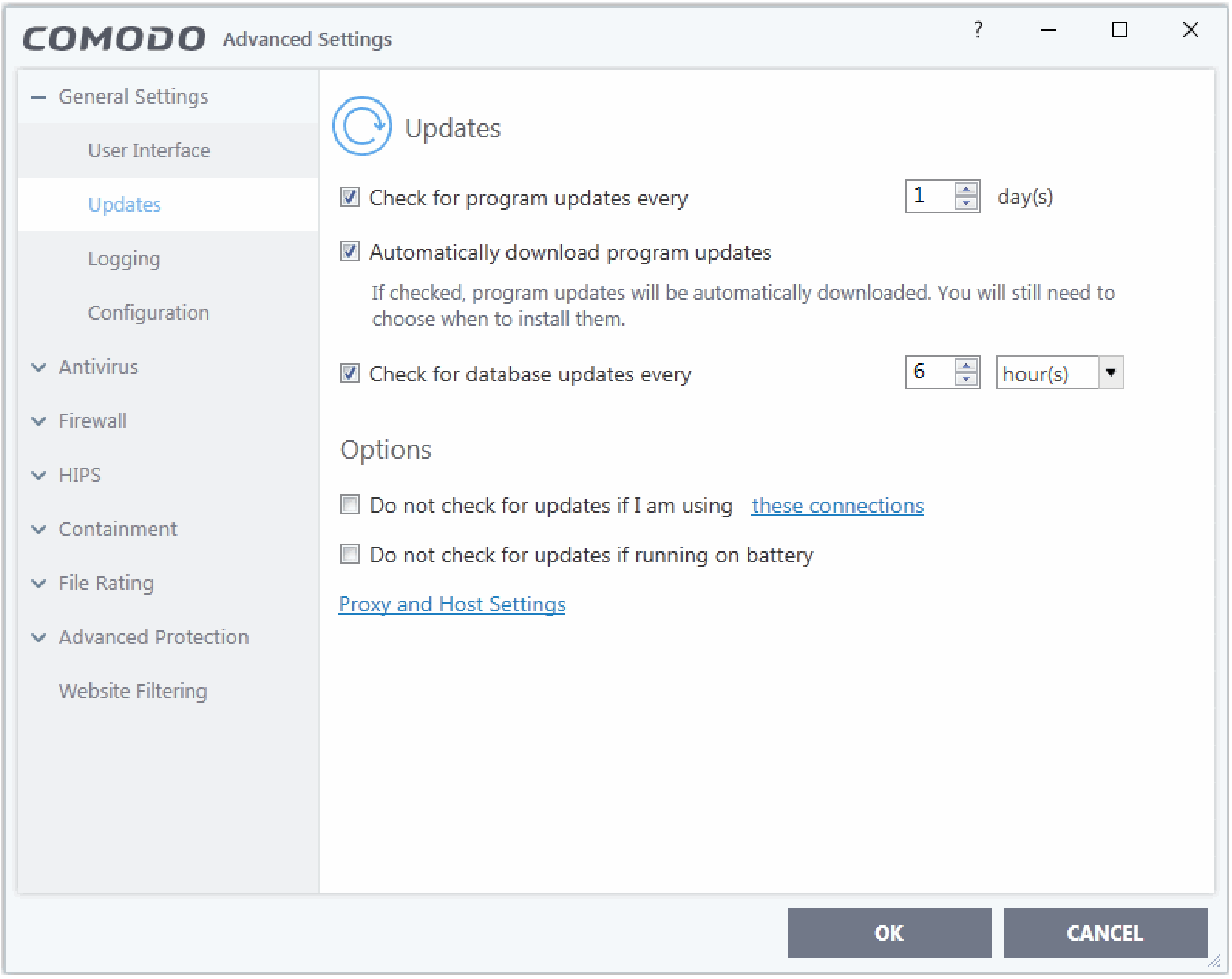
You may choose to restart it now or postpone this to a later time.

Remind me in:

30 minutes

Automatic Updates

By default, Comodo Antivirus automatically checks for and downloads database and program updates. You can modify these settings in '**Settings**' **>** '**General Settings**' **>** '**Updates**'.



Updates

☑ Check for program updates every 1 day(s)

☑ Automatically download program updates

If checked, program updates will be automatically downloaded. You will still need to choose when to install them.

☑ Check for database updates every 6 hour(s)

Options

□ Do not check for updates if I am using these connections

□ Do not check for updates if running on battery

Proxy and Host Settings

You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. See '**Scan Profiles**' for more details.

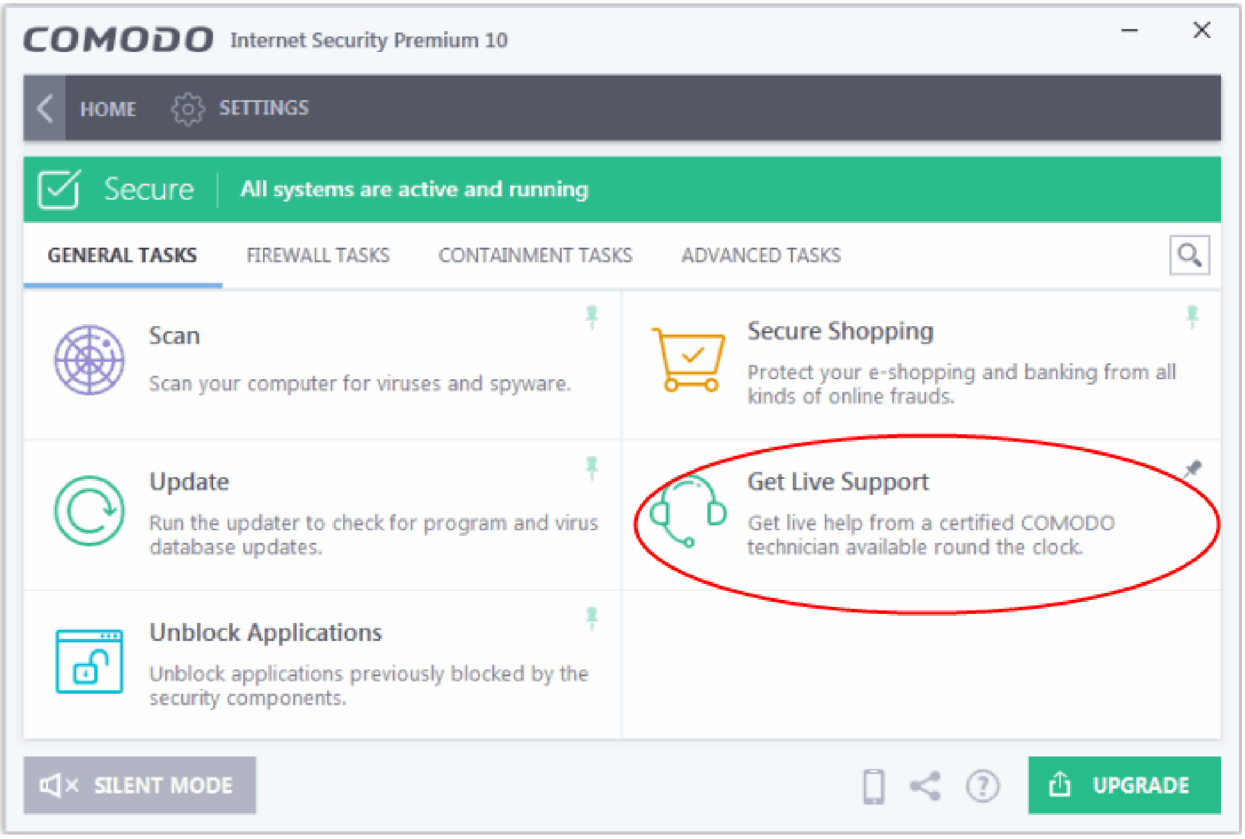
2.4. Get Live Support

Comodo GeekBuddy is a chat based personalized computer support service provided by friendly computer experts at Comodo. If you experience any issues at all with your computer, you can initiate a chat session and ask our technicians to analyze the problem. If requested, they can even establish a remote connection to your PC and fix it right in front of your eyes.

GeekBuddy is included with CIS Pro and Complete. Users of CIS Premium can enjoy a free trial of the service.

To initiate a chat session and get live support

- Switch to 'Tasks' interface by clicking 'Tasks' from the top left of the home screen
- Click 'General' from the top of the 'Tasks' interface and choose 'Get Live Support'



All systems are active and running

Scan
Scan your computer for viruses and spyware.

Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.

Update
Run the updater to check for program and virus database updates.

Get Live Support
Get live help from a certified COMODO technician available round the clock.

Unblock Applications
Unblock applications previously blocked by the security components.

GeekBuddy technicians can help solve most computer issues that you are experiencing. 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. See '**Comodo GeekBuddy**', for more details about this service.

2.5. Manage Blocked Items

The Antivirus, Containment, Firewall and Host Intrusion Prevention System (HIPS) components can be configured to automatically block unknown and suspicious files. CIS retains a list of all blocked applications and allows you to manually release those that you consider legitimate.

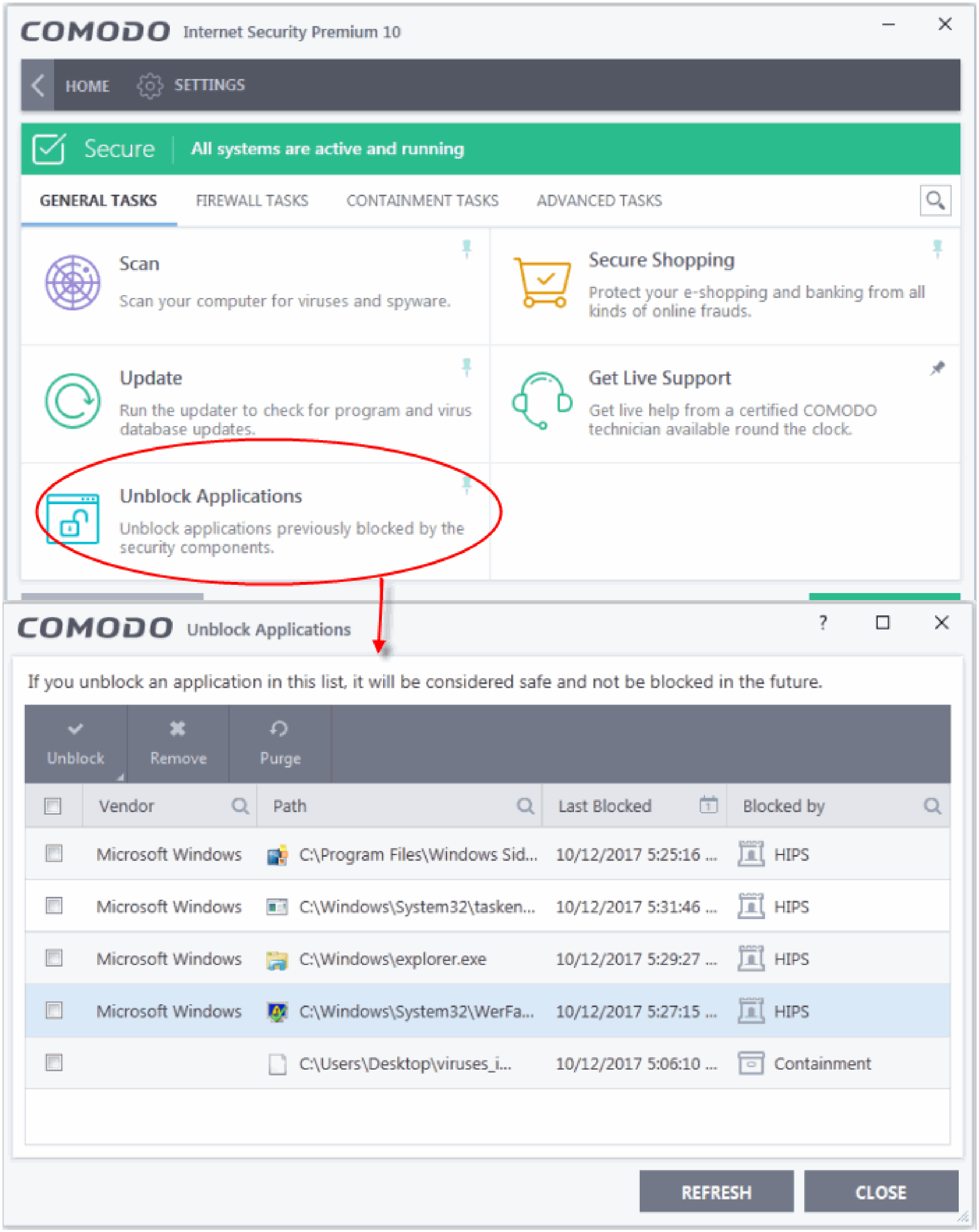
Once you release an item from the blocked files list, a rule will be created so that the same application will not be blocked in future.

- For applications blocked by the Antivirus then unblocked manually, the file will be added to the Exclusion list. See **Scan Exclusions** for more details.

- For applications blocked by the Firewall then unblocked manually, an 'Allow' rule will be added to the Firewall > Application rules. See **Application Rules** for more details
- For applications blocked by the containment system then manually unblocked, an 'Ignore' rule will be added to the Auto-Containment rules. See **Auto-Containment Rules** for more details.
- For applications blocked by HIPS then unblocked manually, an 'Allow' rule will be added to HIPS Rules. See **Active HIPS Rules** for more details.

To view and manage blocked applications

- Click 'Tasks' at the top left of the home screen
- Open the 'General Tasks' tab and choose 'Unblock Applications'



Scan
Scan your computer for viruses and spyware.

Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.

Update
Run the updater to check for program and virus database updates.

Get Live Support
Get live help from a certified COMODO technician available round the clock.

Unblock Applications
Unblock applications previously blocked by the security components.

If you unblock an application in this list, it will be considered safe and not be blocked in the future.

□	Vendor	Path	Last Blocked	Blocked by
□	Microsoft Windows	C:\Program Files\Windows Sid...	10/12/2017 5:25:16 ...	HIPS
□	Microsoft Windows	C:\Windows\System32\tasken...	10/12/2017 5:31:46 ...	HIPS
□	Microsoft Windows	C:\Windows\explorer.exe	10/12/2017 5:29:27 ...	HIPS
□	Microsoft Windows	C:\Windows\System32\WerFa...	10/12/2017 5:27:15 ...	HIPS
□		C:\Users\Desktop\viruses_i...	10/12/2017 5:06:10 ...	Containment

The 'Unblock Applications' interface will open with a list of applications blocked by CIS:

Unblock Applications - Column Descriptions	
Column Header	**Description**
Vendor	The publisher of the blocked application.
Path	The installation path of the blocked application
Last Blocked	The precise date and time at which the application was last run and blocked by CIS
Blocked by	The component of CIS that prevented the application from running

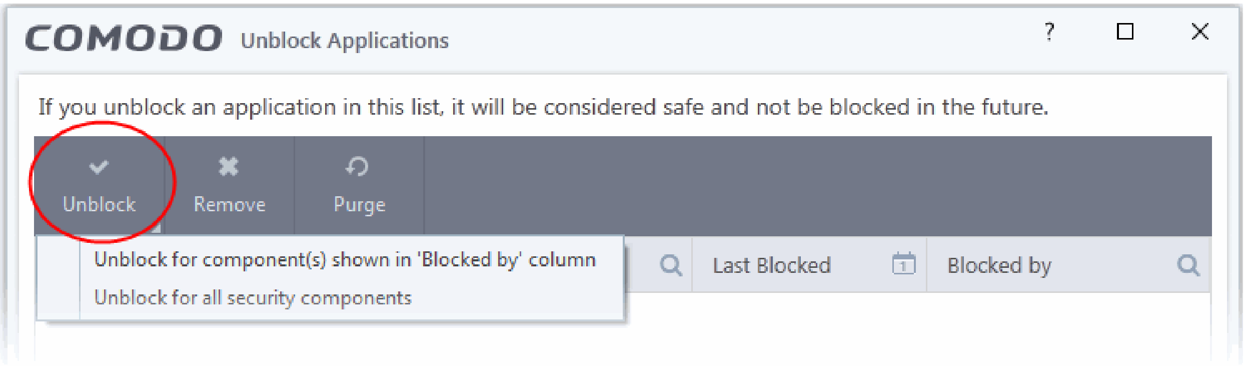
Tip: Clicking a column header sorts items in alphabetical order

From the 'Unblock Applications' interface, you can:

- **Unblock items and allow them to run**
- **View the details of an item in the list**
- **Remove an item from the list**
- **Purge an item in the list**

Unblocking Items

- Select an item or items from the list
- Click 'Unblock' at the top-right
    - Unblock for component(s) shown in 'Blocked by' column' - Item(s) will be released only from the security component(s) that blocked them in the first place.
    - Unblock for all security components - Item(s) will be released by all security components


COMODO Unblock Applications
If you unblock an application in this list, it will be considered safe and not be blocked in the future.
Unblock
Remove
Purge
Unblock for component(s) shown in 'Blocked by' column
Unblock for all security components
Last Blocked
Blocked by

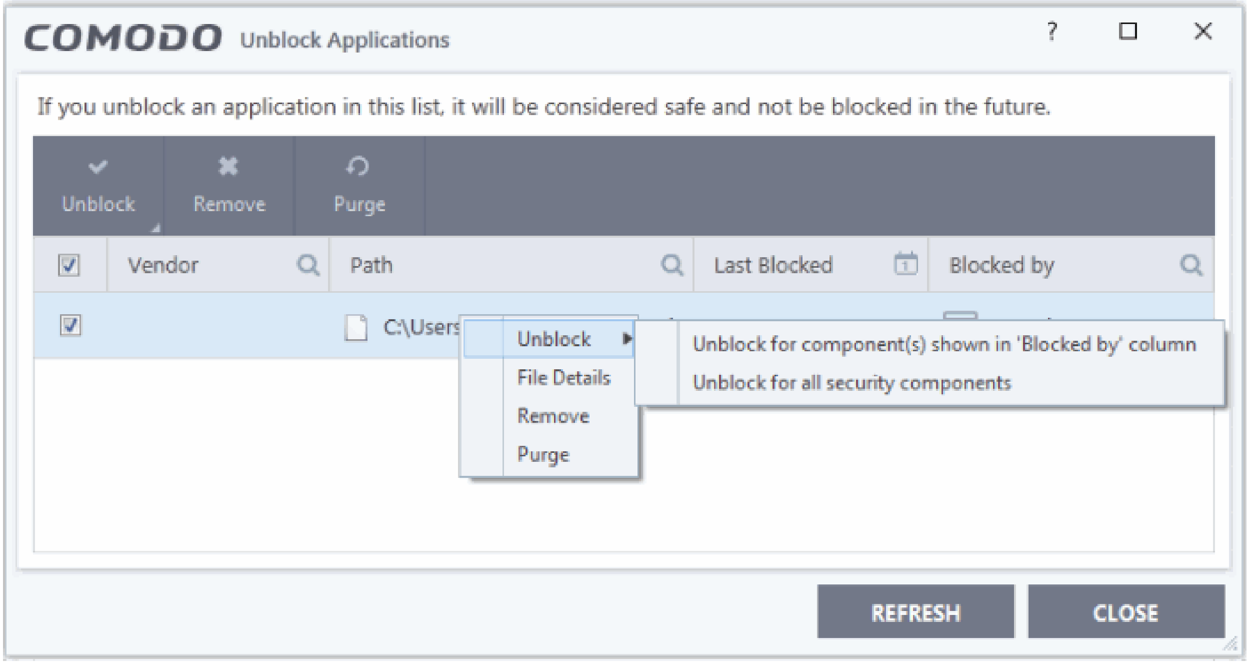
OR

- Right-click on an item and choose 'Unblock' > 'Unblock for component(s) shown in 'Blocked by' column' or 'Unblock for all security components'

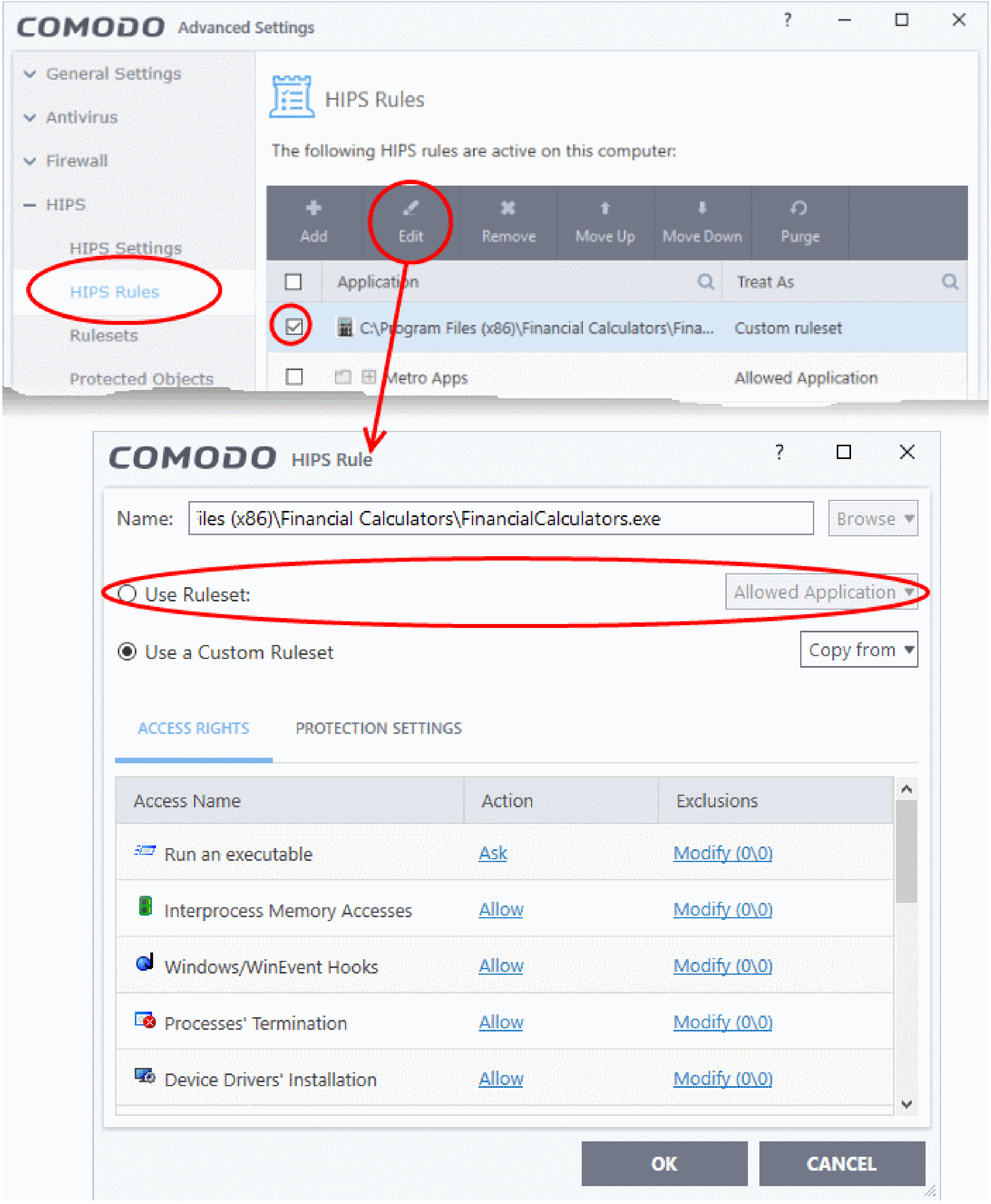
If an item is unblocked, a rule will be added to the component that was responsible for blocking it so the same application will not be blocked in future.

Example:

In the example shown below, the file 'FinancialCalculators.exe' is blocked by HIPS.


COMODO Unblock Applications
If you unblock an application in this list, it will be considered safe and not be blocked in the future.
Unblock
Remove
Purge
Vendor
Path
Last Blocked
Blocked by
C:\Users
Unblock
File Details
Remove
Purge
Unblock for component(s) shown in 'Blocked by' column
Unblock for all security components
REFRESH
CLOSE

If you manually unblock the file, an 'Allowed Application' rule will be automatically created in HIPS:



HIPS Rules

The following HIPS rules are active on this computer:

	Application	Treat As
☑	C:\Program Files (x86)\Financial Calculators\Fina...	Custom ruleset
□	Metro Apps	Allowed Application

Name: iles (x86)\Financial Calculators\FinancialCalculators.exe

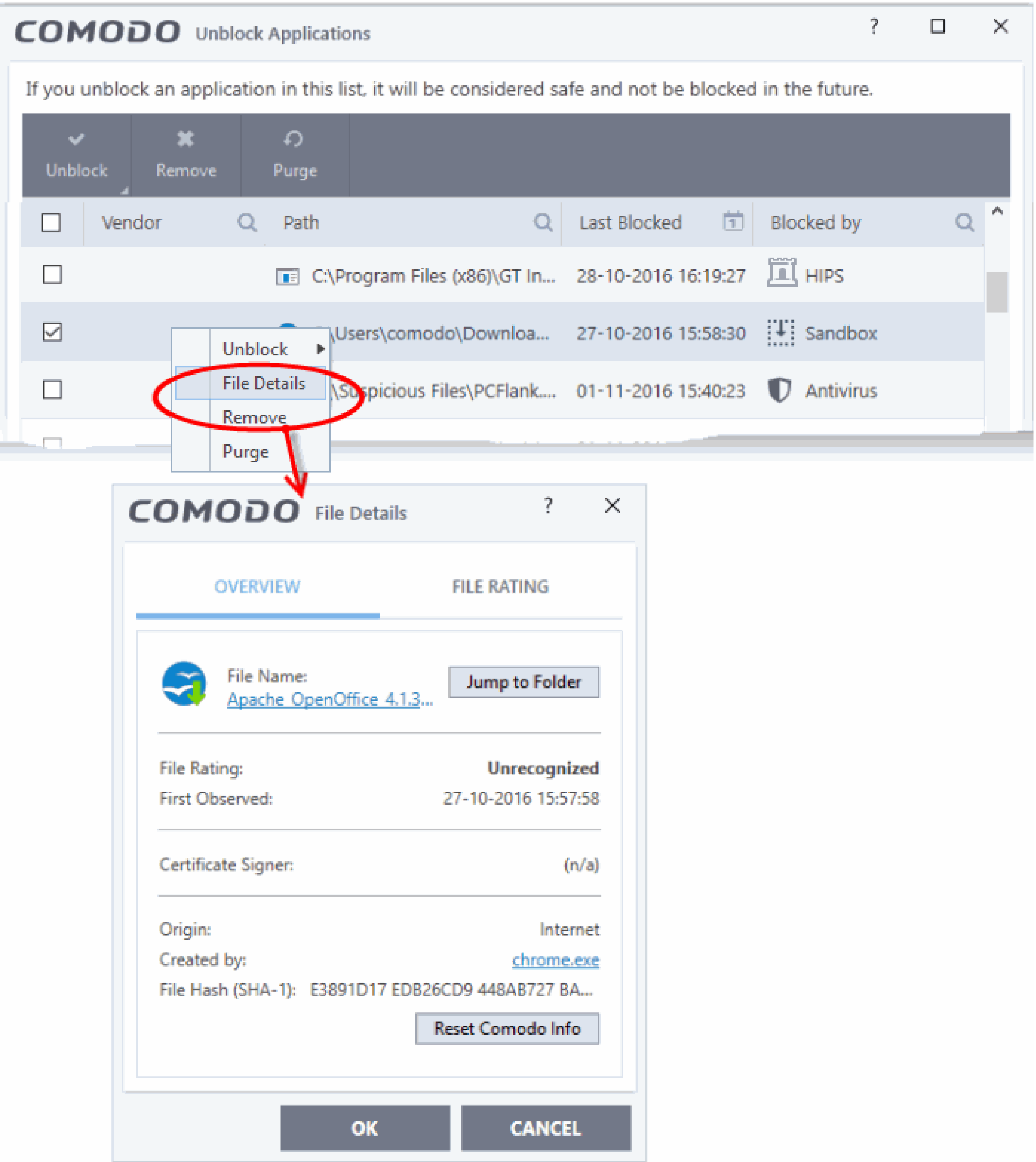
○ Use Ruleset: Allowed Application

● Use a Custom Ruleset

Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Allow	Modify (0\0)
Windows/WinEvent Hooks	Allow	Modify (0\0)
Processes' Termination	Allow	Modify (0\0)
Device Drivers' Installation	Allow	Modify (0\0)

To view the details of an application

- Right-click on an item and choose 'File Details' from the context sensitive menu.



If you unblock an application in this list, it will be considered safe and not be blocked in the future.

	Vendor	Path	Last Blocked	Blocked by
□		C:\Program Files (x86)\GT In...	28-10-2016 16:19:27	HIPS
☑		...\Users\comodo\Downloa...	27-10-2016 15:58:30	Sandbox
□		...\Suspicious Files\PCFlank....	01-11-2016 15:40:23	Antivirus

File Name: Apache OpenOffice 4.1.3...

File Rating: Unrecognized

First Observed: 27-10-2016 15:57:58

Certificate Signer: (n/a)

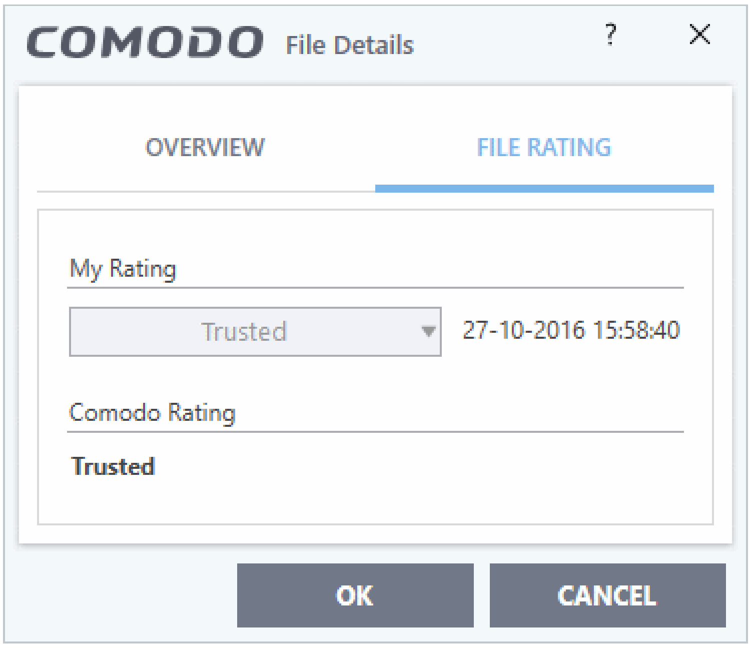
Origin: Internet

Created by: chrome.exe

File Hash (SHA-1): E3891D17 EDB26CD9 448AB727 BA...

The 'Overview' tab displays general information like the name of the file, it's CIS trust rating, application signer and the file hash value.

The file rating tab displays the trust rating assigned to the file by Comodo Internet Security. It also allows you set your own rating for files rated as 'Unrecognized' by Comodo.



My Rating

Trusted 27-10-2016 15:58:40

Comodo Rating

Trusted

To remove an application from the list

- Click the 'Remove' button at top-right to delete an item from the list
- Alternatively, right-click on an item and choose 'Remove' from the context sensitive menu.

To purge rules

Runs a check to verify that all applications mentioned in rules are actually installed at the paths specified. If not, the rule is removed, or 'purged', from the list.

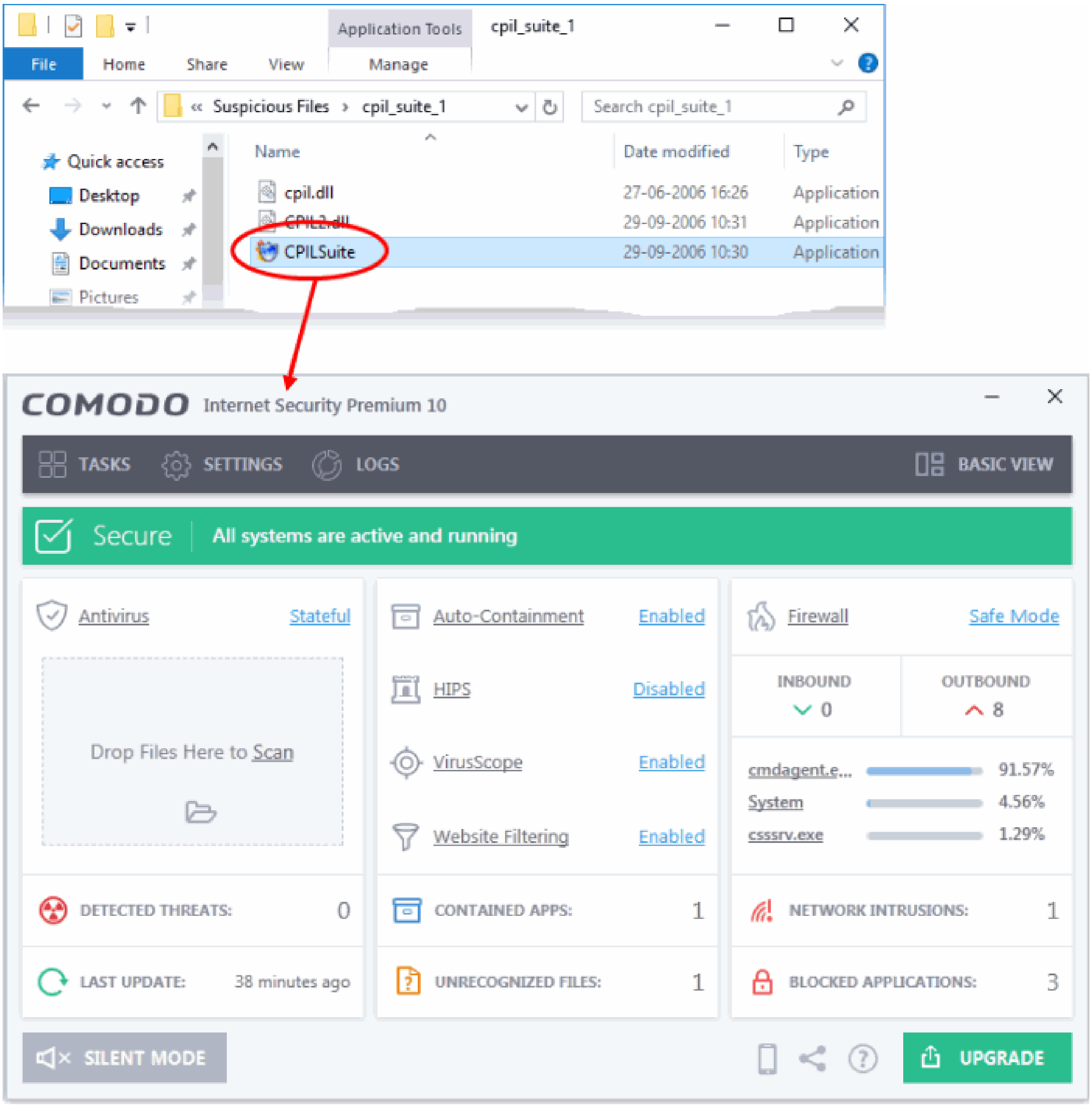
- Click the 'purge' button at the top-right
- Alternatively, right-click on an item and choose 'Purge' from the context sensitive menu.

2.6. Instantly Scan Files and Folders

You can scan individual files or folders instantly to check whether they contain any threats. This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from the internet.

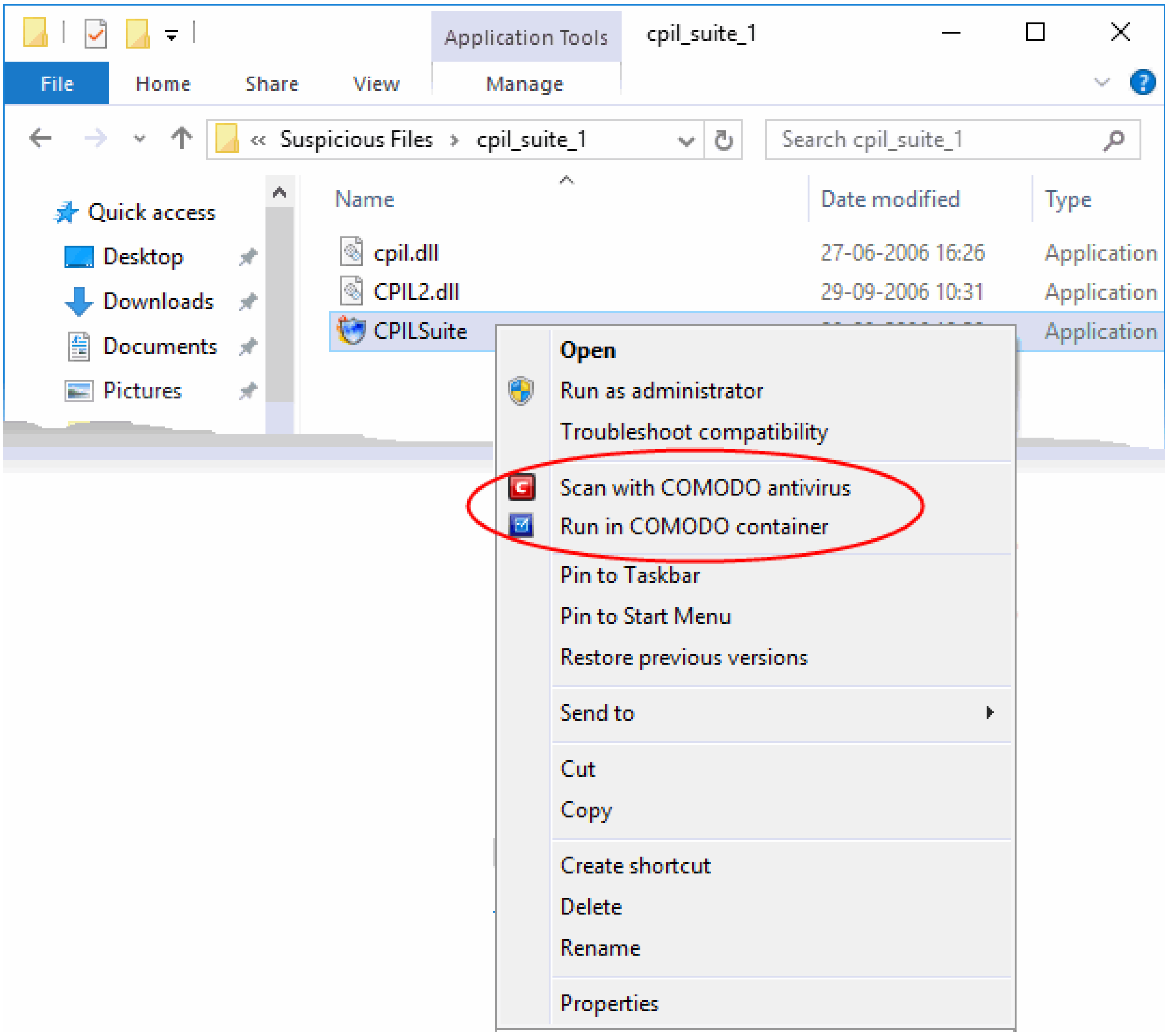
To instantly scan an item

- Click 'Advanced View' at the top right of the home screen.
- Drag and drop the file into the 'Drop Files to Scan' (or click the 'Scan' link inside the box and navigate to the item).

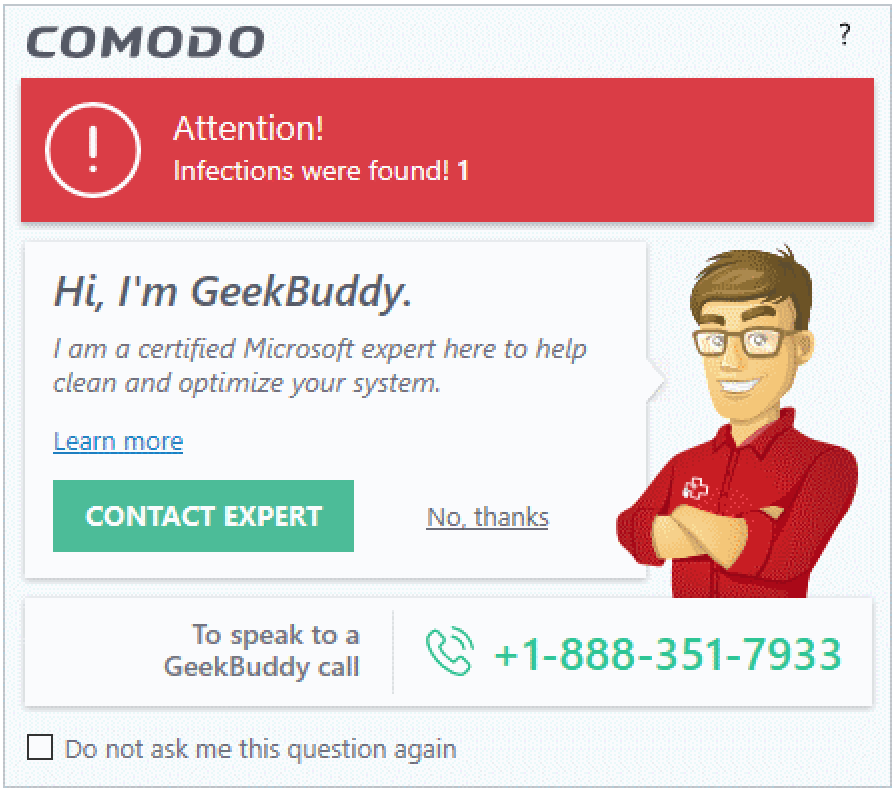


OR

- Right click on a file and select 'Scan with Comodo antivirus' from the context sensitive menu



The item will be scanned immediately. An alert will be displayed if any threats are found:



Attention!

Infections were found! 1

Hi, I'm GeekBuddy.

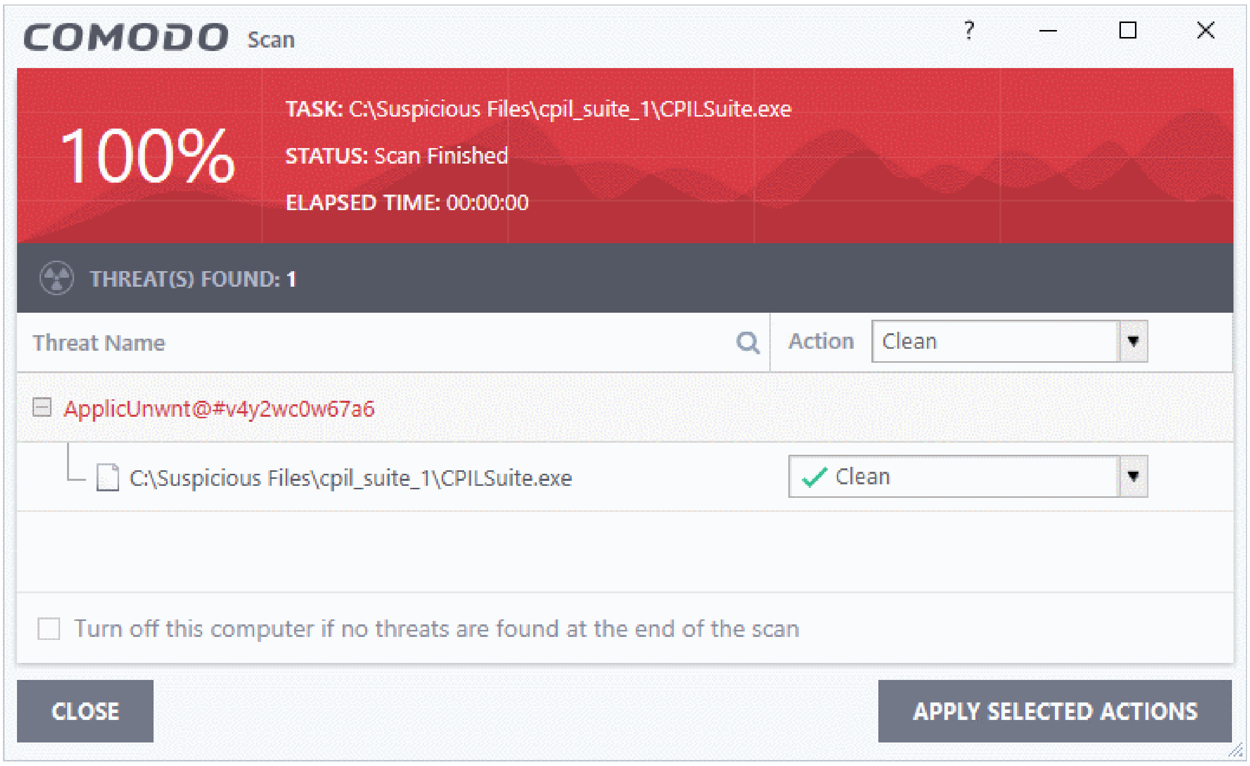
I am a certified Microsoft expert here to help clean and optimize your system.

To speak to a GeekBuddy call ☎ +1-888-351-7933

□ Do not ask me this question again

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.

  See **Comodo GeekBuddy**, for more details on GeekBuddy Expert help.
- If you wish to clean the infections yourself, select 'No, thanks'. The scan results screen will be displayed.



100%

TASK: C:\Suspicious Files\cpil_suite_1\CPILSuite.exe

STATUS: Scan Finished

ELAPSED TIME: 00:00:00

THREAT(S) FOUND: 1

Threat Name	Action: Clean
ApplicUnwnt@#v4y2wc0w67a6	
C:\Suspicious Files\cpil_suite_1\CPILSuite.exe	✓ Clean

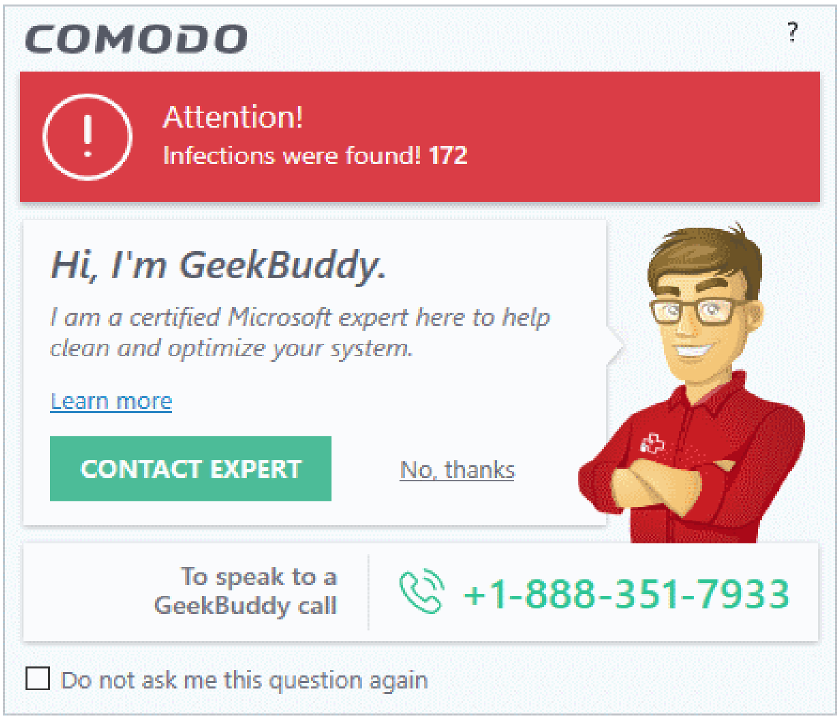
□ Turn off this computer if no threats are found at the end of the scan

You can choose to clean, quarantine or ignore the threat. See **files Processing the infected** for more details.

2.7. Processing Infected Files

Malware found by a virus scan can be processed in two ways:

1. For profile driven scans, malware will be automatically dealt with if 'Automatically Clean Threats' is enabled in a custom scan profile. See **configuring scanning options** for more details.
2. For all other on-demand or scheduled scans, an alert screen will be displayed. The alert will display the number of threats/infections discovered and provide you with cleaning options:



COMODO ?

Attention!

Infections were found! **172**

Hi, I'm GeekBuddy.

I am a certified Microsoft expert here to help clean and optimize your system.

Learn more

CONTACT EXPERT

No, thanks

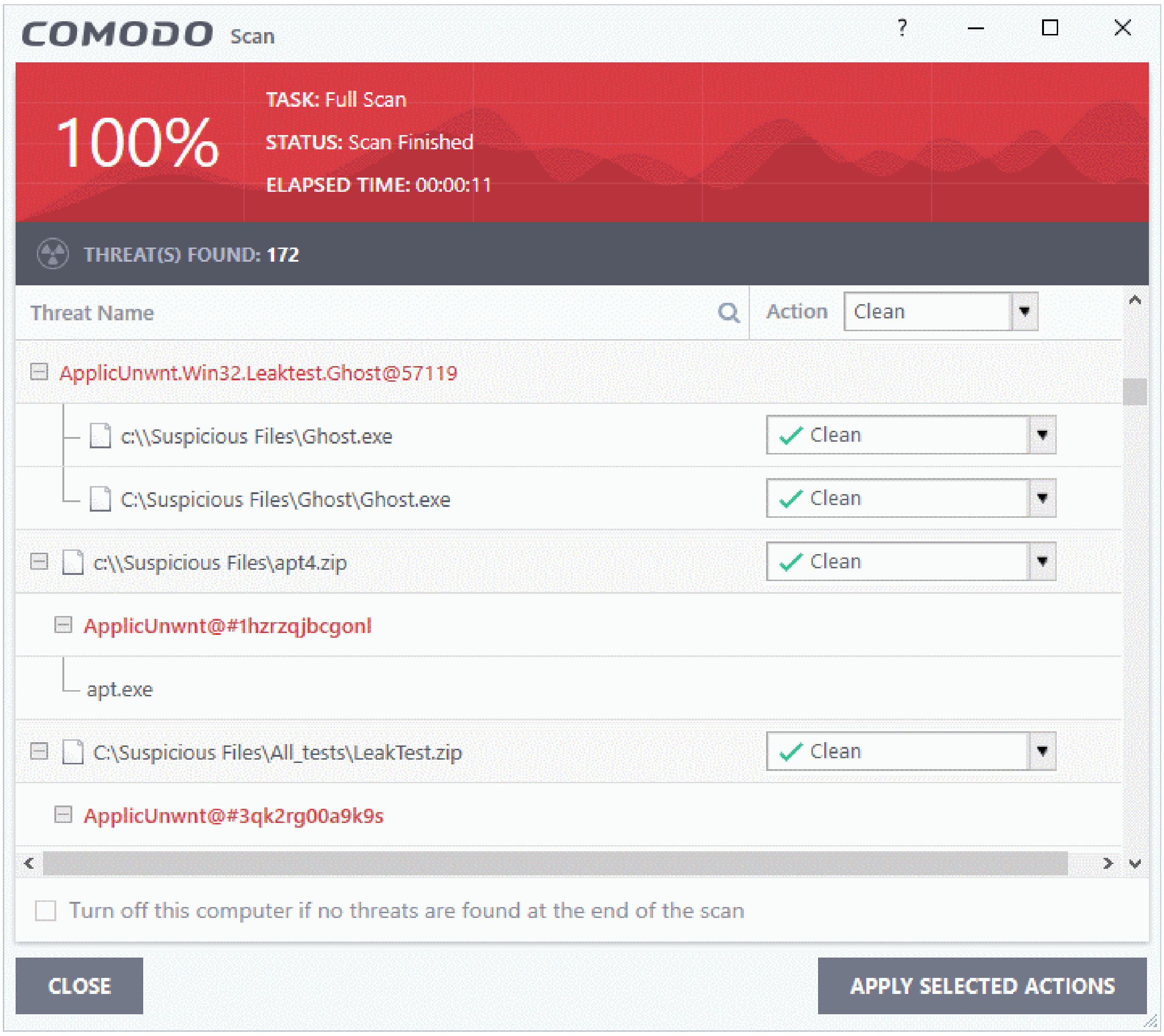
To speak to a GeekBuddy call

+1-888-351-7933

□ Do not ask me this question again

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Contact Expert'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.

  See **Comodo GeekBuddy**, for more details on GeekBuddy Expert help.
- If you wish to clean the infections yourself, select 'No, thanks'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



COMODO Scan

100%

TASK: Full Scan

STATUS: Scan Finished

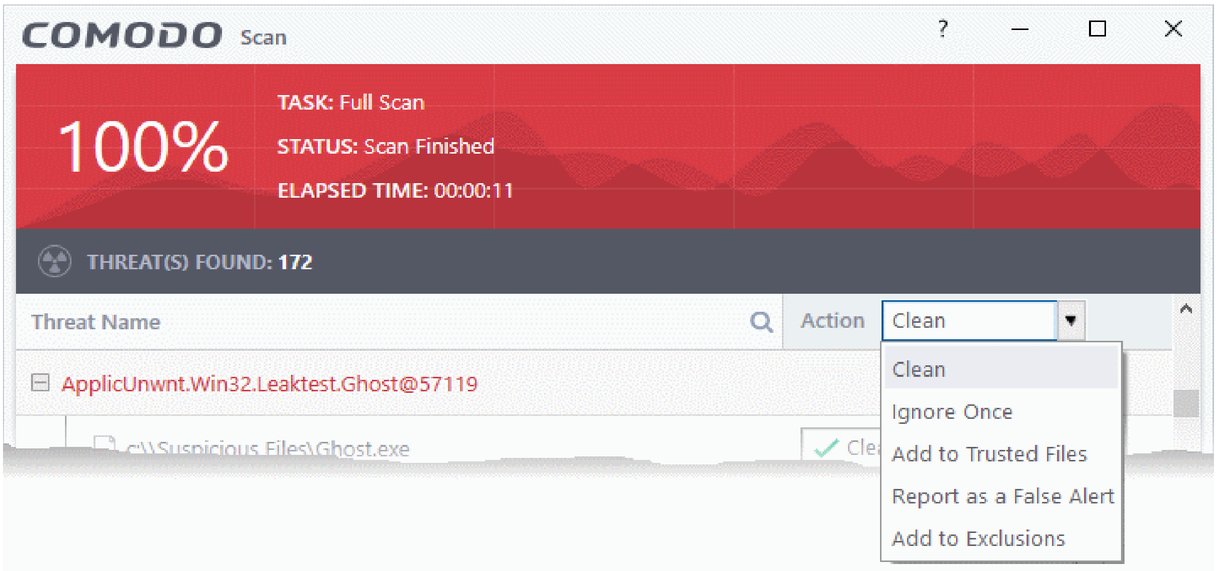
ELAPSED TIME: 00:00:11

THREAT(S) FOUND: 172

Threat Name	Action: Clean
⊟ ApplicUnwnt.Win32.Leaktest.Ghost@57119	
c:\\Suspicious Files\Ghost.exe	✓ Clean
C:\Suspicious Files\Ghost\Ghost.exe	✓ Clean
⊟ c:\\Suspicious Files\apt4.zip	✓ Clean
⊟ ApplicUnwnt@#1hzrzqjbcgonl	
apt.exe	
⊟ C:\Suspicious Files\All_tests\LeakTest.zip	✓ Clean
⊟ ApplicUnwnt@#3qk2rg00a9k9s	

□ Turn off this computer if no threats are found at the end of the scan

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



COMODO Scan

100%

TASK: Full Scan

STATUS: Scan Finished

ELAPSED TIME: 00:00:11

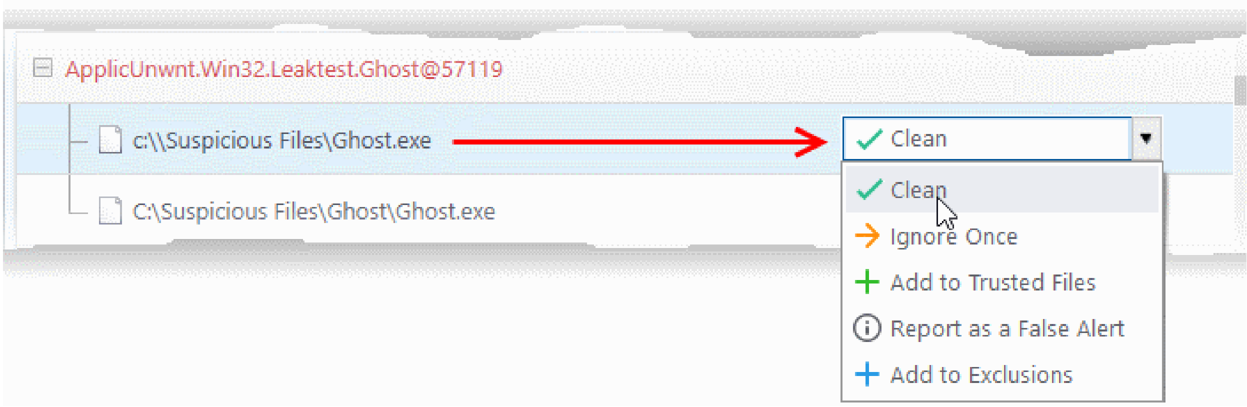
THREAT(S) FOUND: 172

Threat Name | Action: Clean

⊟ ApplicUnwnt.Win32.Leaktest.Ghost@57119

c:\\Suspicious Files\Ghost.exe

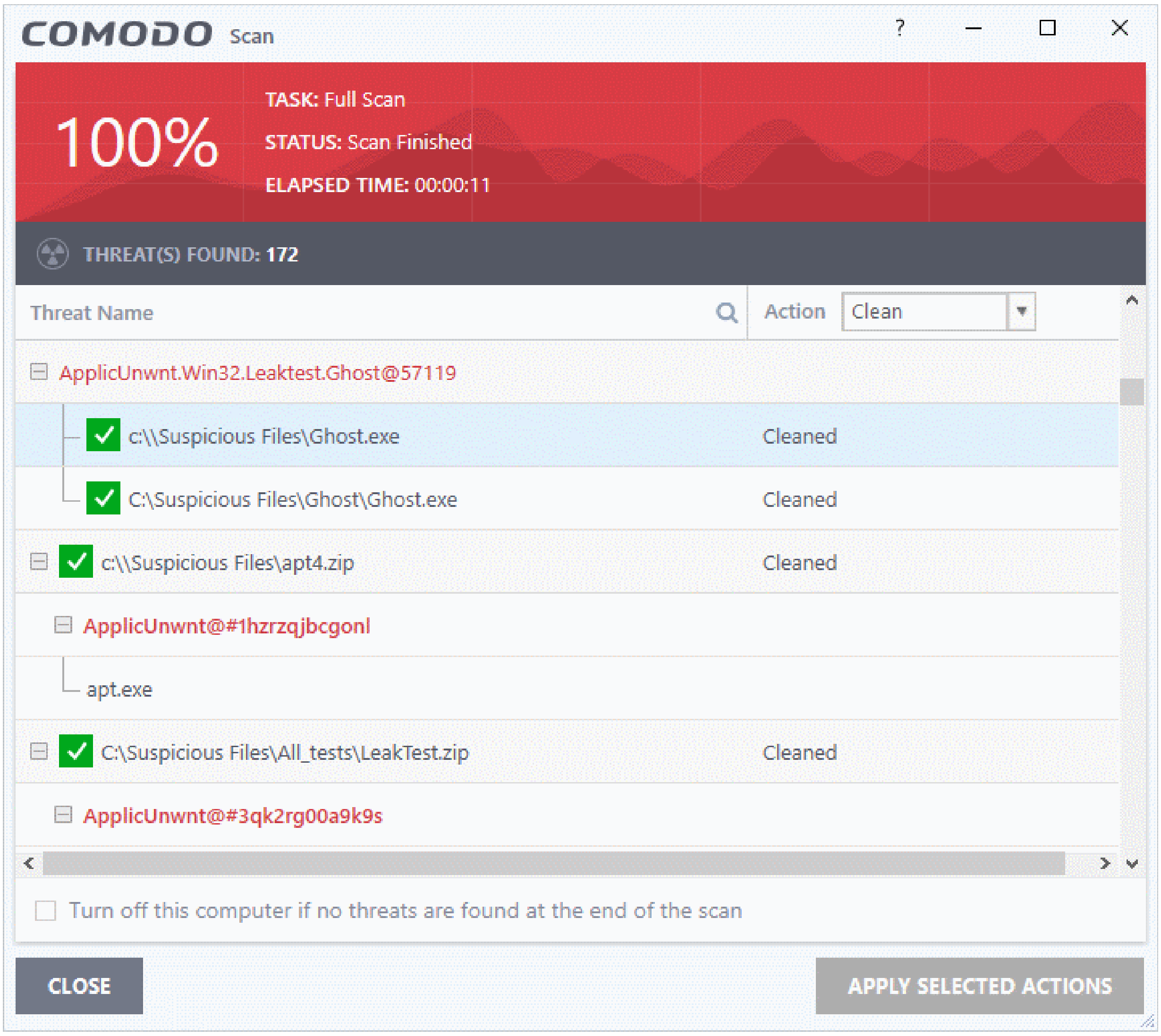
… or the actions to be applied to individual items from the drop-down beside each item.


ApplicUnwnt.Win32.Leaktest.Ghost@57119
c:\\Suspicious Files\Ghost.exe
C:\Suspicious Files\Ghost\Ghost.exe
✓ Clean
✓ Clean
Ignore Once
Add to Trusted Files
Report as a False Alert
Add to Exclusions

Available actions are:

- **Clean** - If a disinfection routine is available, Comodo Antivirus will disinfect the application and the clean application will be retained. If a disinfection routine is not available, Comodo Antivirus will move the files to quarantine for your review. You can choose to restore or permanently delete quarantined files (for more details, see **Manage Quarantined Items**).
- **Ignore Once** - Will allow the file to run this time only. However, the file will be detected as a threat on all subsequent executions.
- **Add to Trusted Files** - The file will be moved to the **Trusted Files** list. An alert will not be generated next time the file runs. Only select this option if you are sure the file is 'OK'.
- **Report as a False Alert** - If you are sure that the file is safe, select 'Report as a False Alert' to send the file to Comodo for analysis. Submitting a false positive will trust the file and omit it from antivirus scans. If Comodo confirm the file to be trustworthy it will be added to the global Comodo safe list.
- **Add to Exclusions** - The file will be moved to the **Exclusions** list and will not be scanned in future.

- After selecting the action(s) to be applied, click 'Apply Selected Actions'. The result of the action will be displayed in the 'Actions' column:



TASK: Full Scan

STATUS: Scan Finished

ELAPSED TIME: 00:00:11

THREAT(S) FOUND: 172

Threat Name	Action: Clean
ApplicUnwnt.Win32.Leaktest.Ghost@57119	
✓ c:\\Suspicious Files\Ghost.exe	Cleaned
✓ C:\Suspicious Files\Ghost\Ghost.exe	Cleaned
✓ c:\\Suspicious Files\apt4.zip	Cleaned
ApplicUnwnt@#1hzrzqjbcgonl	
apt.exe	
✓ C:\Suspicious Files\All_tests\LeakTest.zip	Cleaned
ApplicUnwnt@#3qk2rg00a9k9s	

☐ Turn off this computer if no threats are found at the end of the scan

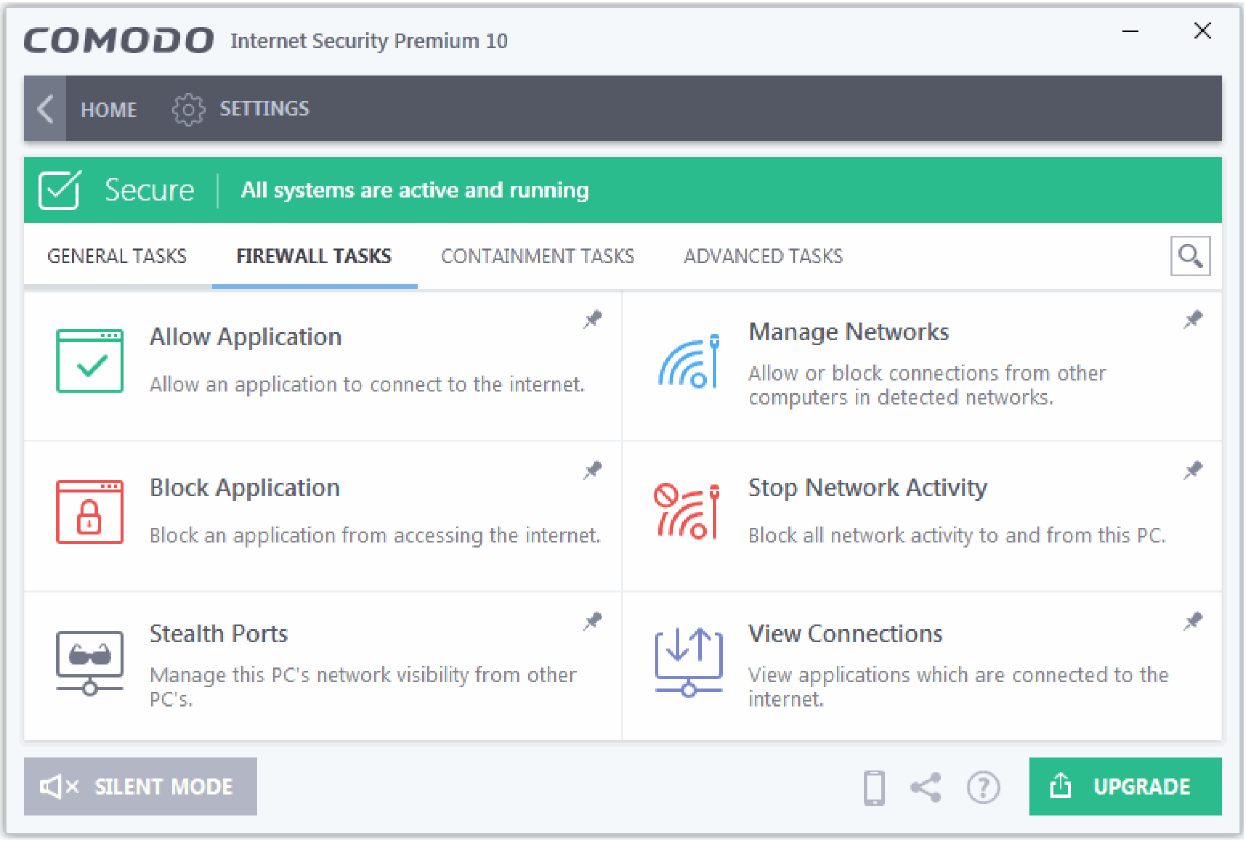
- Click 'Close' to close the results window.

3.Firewall Tasks - Introduction

The Firewall component of Comodo Internet Security offers the highest levels of security against inbound and outbound threats, hides your computer's ports from hackers, and will block malicious software from transmitting your confidential data over the internet. Comodo Firewall makes it easy for you to specify exactly which applications are allowed to connect to the Internet and immediately warns you when there is suspicious activity.

The firewall interface can be accessed by clicking the 'Firewall' link on the tasks screen. From here, you can configure internet access rights per-application, stealth your computer ports, manage available networks, view active Internet connections and even block all network traffic in and out of your computer.

The 'Advanced Settings' interface allows you to choose overall firewall behavior and configure items such as application rules, rulesets, network zones and port sets. See '**Firewall Configuration**' for more details about configuring advanced firewall settings.



COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Allow Application
Allow an application to connect to the internet.
Manage Networks
Allow or block connections from other computers in detected networks.
Block Application
Block an application from accessing the internet.
Stop Network Activity
Block all network activity to and from this PC.
Stealth Ports
Manage this PC's network visibility from other PC's.
View Connections
View applications which are connected to the internet.
SILENT MODE
UPGRADE

Click the links below to see detailed explanations of each area in this section:

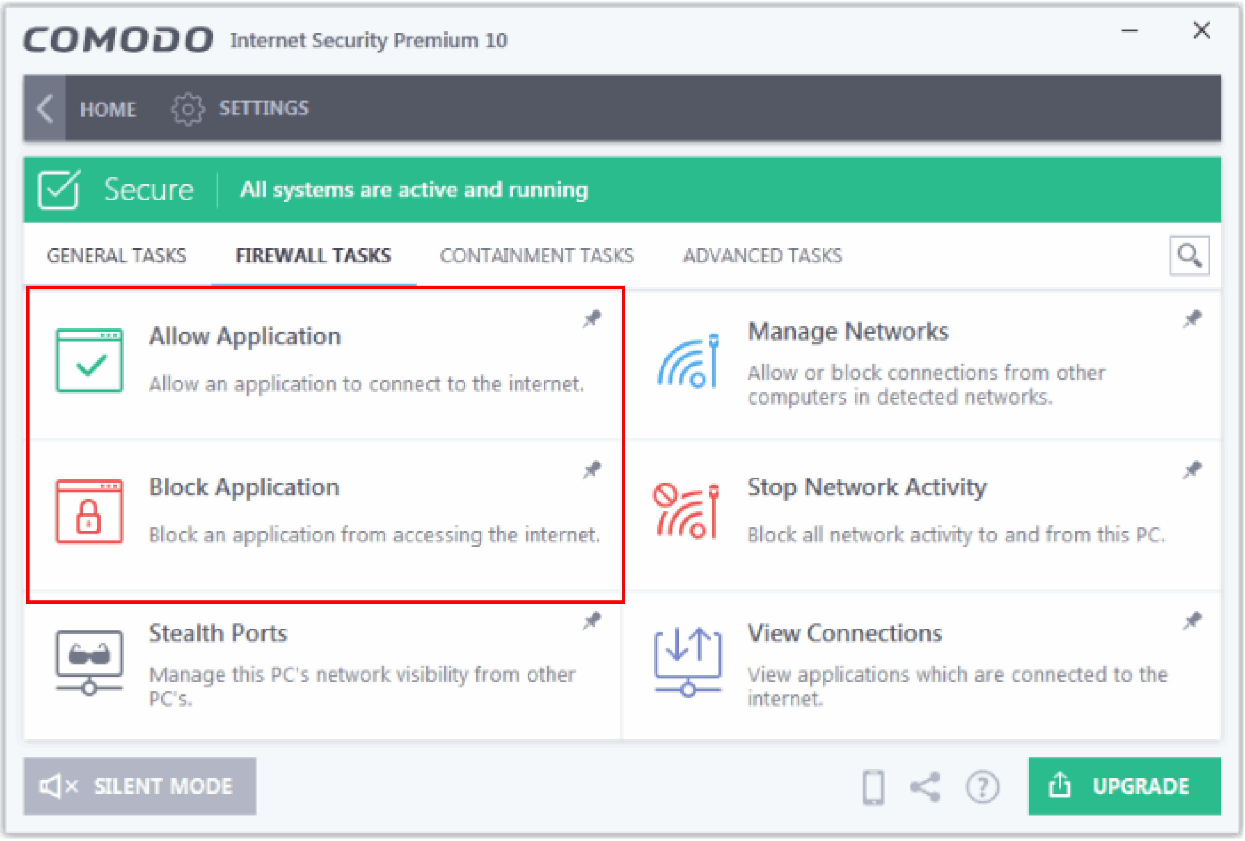
- **Allow or block Internet access to applications selectively**
- **Manage network connections**
- **Stop all network activity**
- **Stealth your computer ports**
- **View active Internet connections**

3.1. Allow or Block Internet Access to Applications Selectively

The 'Firewall' interface allows you to selectively allow or block certain applications from accessing the internet. These shortcuts are a convenient way to create 'Allow Request' or 'Block Request' rules for individual applications - meaning that inbound and outbound connections can be automatically permitted or denied to an app.

To open the 'Firewall Tasks' interface:

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface
- Click 'Firewall Tasks' from the 'Tasks' interface:



All systems are active and running

Allow Application
Allow an application to connect to the internet.

Block Application
Block an application from accessing the internet.

Stealth Ports
Manage this PC's network visibility from other PC's.

Manage Networks
Allow or block connections from other computers in detected networks.

Stop Network Activity
Block all network activity to and from this PC.

View Connections
View applications which are connected to the internet.

To allow an application to access to the Internet:

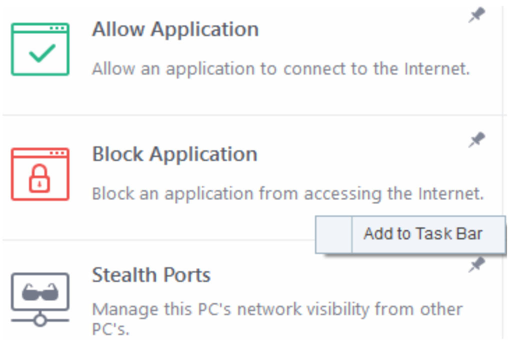
- Click 'Allow Application'
- Navigate to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to allow Internet access to the selected application.

To block an application's Internet access rights

- Click 'Block Application'
- Browse to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to prohibit Internet access to the selected application.

The advanced application rules interface can be accessed by clicking 'Settings' > 'Firewall' > 'Firewall Settings' > Application rules. The application you just allowed or blocked should be listed here. For further information on application rules governing Internet access rights, see '**Application Rules**'.

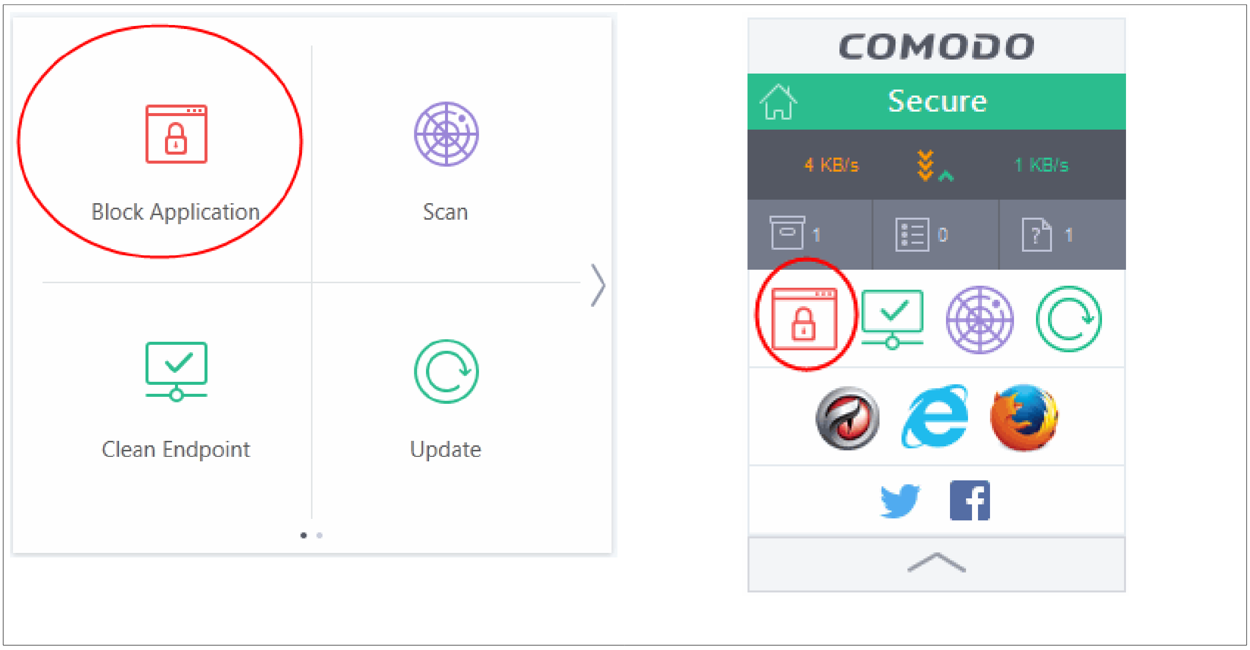
Tip: If you plan to regularly allow/block applications, you can right click on the appropriate feature or the pin button and select 'Add to Task Bar'. It will then be quickly accessible from both the basic view of CIS home screen and the widget:



Allow Application
Allow an application to connect to the Internet.

Block Application
Block an application from accessing the Internet.

Stealth Ports
Manage this PC's network visibility from other PC's.

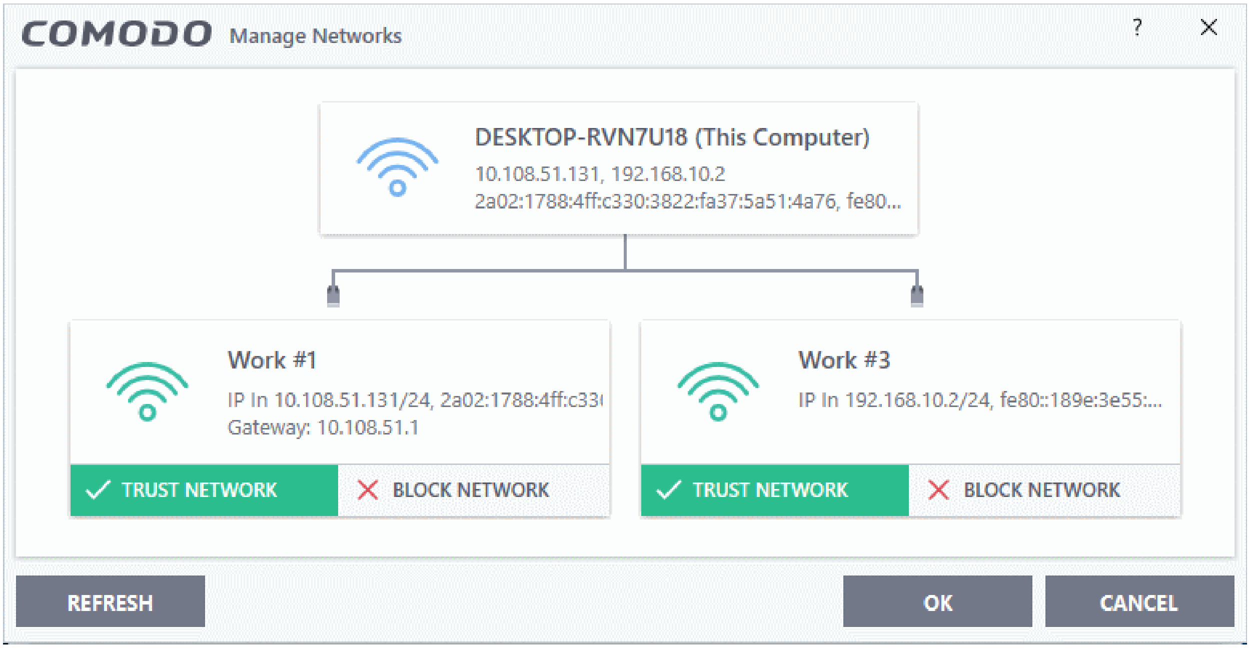


3.2. Manage Network Connections

The 'Manage Network Connections' interface allows you to quickly view all wired and wireless networks to which your computer is connected. The lower half of the panel displays details about each network including its name, IP address and gateway.

To view the network connections of your computer:

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface
- Click 'Firewall Tasks' from the 'Tasks' interface:
- Click 'Manage Networks'



DESKTOP-RVN7U18 (This Computer)
10.108.51.131, 192.168.10.2
2a02:1788:4ff:c330:3822:fa37:5a51:4a76, fe80...

Work #1
IP In 10.108.51.131/24, 2a02:1788:4ff:c33
Gateway: 10.108.51.1

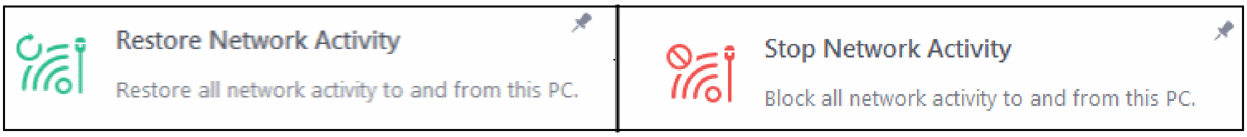
Work #3
IP In 192.168.10.2/24, fe80::189e:3e55:...

- You can choose to trust or block a network by selecting the appropriate radio button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks.
- Use the handles (< >) to scroll through all available networks or computers

- Use the refresh button if you have recently made network changes and these are not yet visible in the interface.
- To view, create or block **Network Zones**, click 'Settings' > 'Firewall' > Network Zones'.

3.3. Stop All Network Activities

As the name suggests, the 'Stop Network Activity' feature instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and outside networks (including the internet). Connections will remained closed until you re-enable them by clicking 'Restore Network Activity'. This allows you to quickly take your computer offline without having to delve into Windows network settings and without having to to unplug any network cables.



Restore Network Activity

Restore all network activity to and from this PC.

Stop Network Activity

Block all network activity to and from this PC.

To manage network activities from your computer:

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface
- Click 'Firewall Tasks' from the 'Tasks' interface
- To disconnect your computer from all networks, click 'Stop Network Activity'
- To re-enable connectivity, click 'Restore Network Activity'
- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have previously blocked in '**Manage Network Connections**' or '**Network Zones**' will remain blocked.
- You can assign networks into network zones in the '**Network Zones**' area
- You can configure rules per network zone in the '**Global Rules**' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the **Manage Network Connections**' area

3.4. Stealth your Computer Ports

Port Stealthing is a security feature whereby ports on an internet connected PC are hidden from sight, providing no response to port scanners.

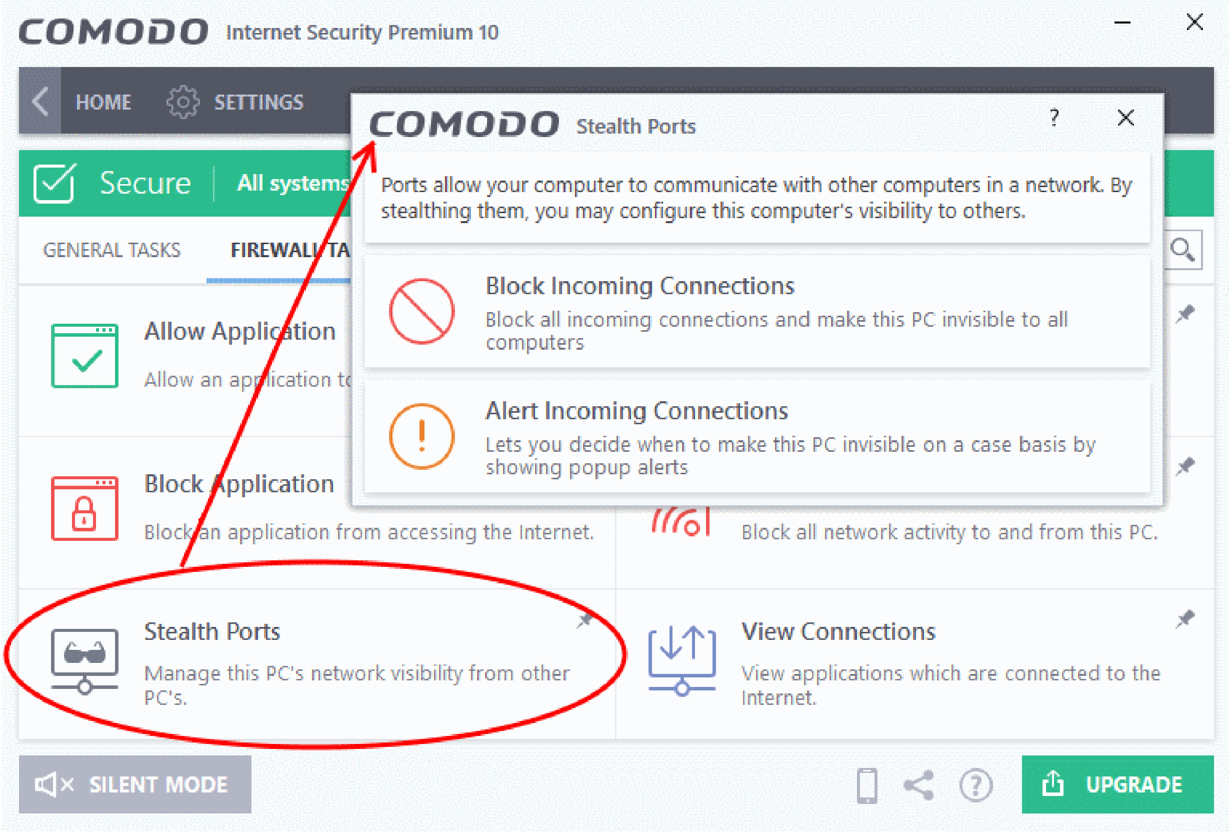
General Note: Your computer sends and receives data to other computers and to the internet through an interface called a 'port'. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to the internet using ports 80 and 443. Your e-mail application connects to your mail server through port 25. A 'port scanning' attack consists of sending a message to each of your computer ports, one at a time. This information gathering technique is used by hackers to find out which ports are open and which ports are being used by services on your machine. With this knowledge, a hacker can determine which attacks are likely to work if used against your machine.

Stealthing a port effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempts ('closed' ports respond with a 'closed' reply- revealing to the hacker that there is actually a PC in existence). If a hacker or automated scanner cannot 'see' your computers ports then they will presume it is offline and move on to other targets. You can still be able to connect to the internet and transfer information as usual but remain invisible to outside threats.

To stealth ports on your computer:

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface

- Click 'Firewall Tasks' from the 'Tasks' interface:
- Click 'Stealth Ports'


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems
GENERAL TASKS
FIREWALL TA
Allow Application
Allow an application to
Block Application
Block an application from accessing the Internet.
Block all network activity to and from this PC.
Stealth Ports
Manage this PC's network visibility from other PC's.
View Connections
View applications which are connected to the Internet.
SILENT MODE
UPGRADE

COMODO Stealth Ports

Ports allow your computer to communicate with other computers in a network. By stealthing them, you may configure this computer's visibility to others.

Block Incoming Connections
Block all incoming connections and make this PC invisible to all computers

Alert Incoming Connections
Lets you decide when to make this PC invisible on a case basis by showing popup alerts

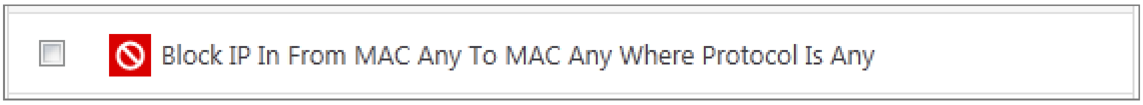
The 'Stealth Ports' dialog will open.

You have two options to choose from:

Block incoming connections

Selecting this option means your computer's ports are invisible to all networks, irrespective of whether you trust them or not. The average home user (using a single computer that is not part of a home LAN) will find this option the more convenient and secure. You are not alerted when the incoming connection is blocked, but the rule adds an entry to the firewall event log file. Specifically, this option adds the following rule in the '**Global Rules**' interface:

Block And Log| IP | In| From Any IP Address| To Any IP Address | Where Protocol is Any



□ Block IP In From MAC Any To MAC Any Where Protocol Is Any

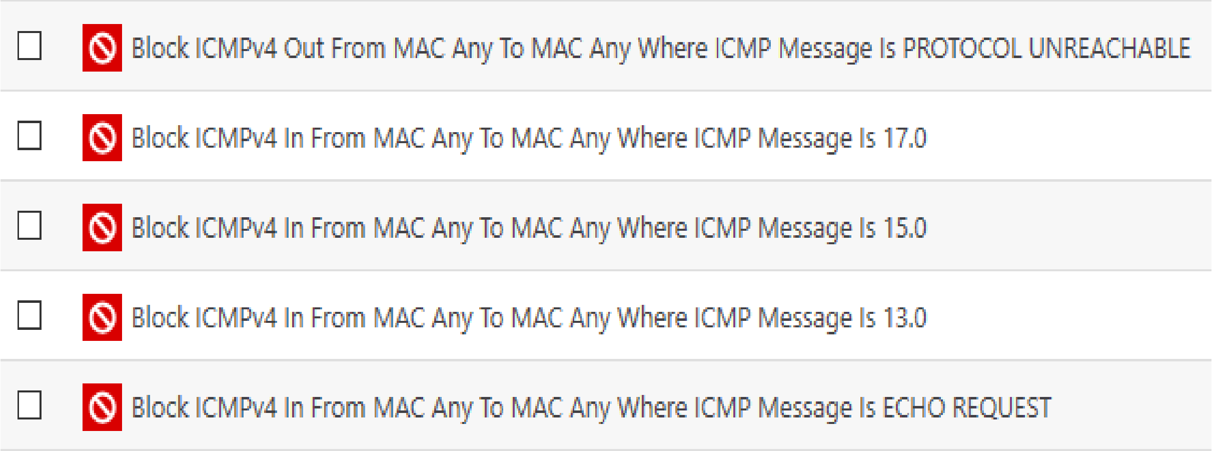
If you would like more information on the meaning and construction of rules, please **click here.**

Alert incoming connections

You see a **firewall alert** every time there is a request for an incoming connection. The alert asks your permission on whether or not you wish the connection to proceed. This can be useful for applications such as Peer to Peer networking and Remote desktop applications that require port visibility in order to connect to your machine.

Specifically, this option adds the following rules in the '**Global Rules**' interface:

Block ICMPv4 In From <Any IP Address> To <Any IP Address> Where Message is <Message>



□ ⊘ Block ICMPv4 Out From MAC Any To MAC Any Where ICMP Message Is PROTOCOL UNREACHABLE

□ ⊘ Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is 17.0

□ ⊘ Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is 15.0

□ ⊘ Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is 13.0

□ ⊘ Block ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is ECHO REQUEST

If you would like more information on the meaning and construction of rules, please **click here**.

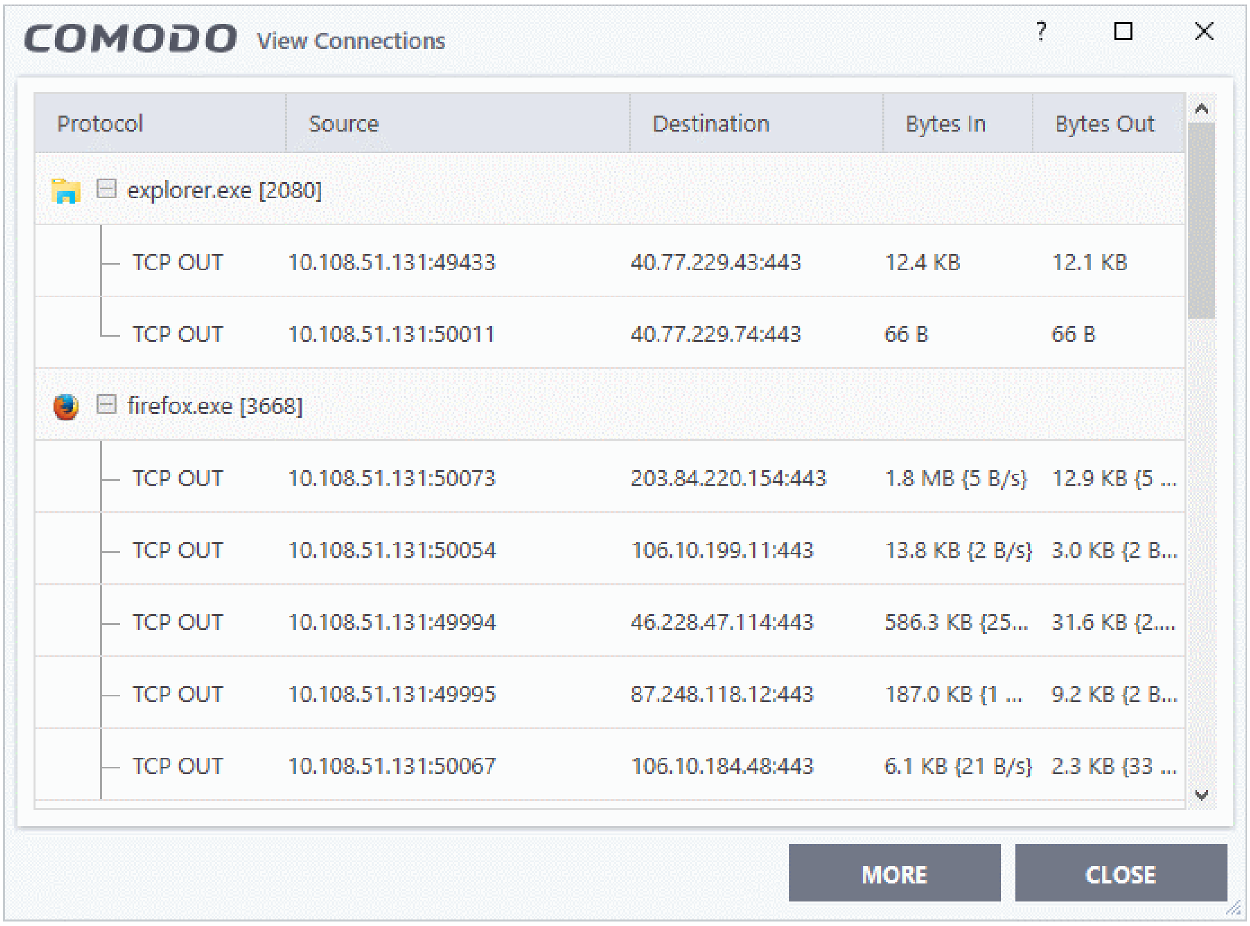
3.5. View Active Internet Connections

- The 'View Connections' interface is an at-a-glance summary of all currently active internet connections on a per-application basis.
- You can view all applications that are connected; all the individual connections that each application is responsible for; the direction of the traffic; the source IP/port and the destination IP/port.
- You can also see the total amount of traffic that has passed in and out of your system over each connection. This list is updated in real time whenever an application creates a new connection or drops an existing connection.
- 'View Connections' is extremely useful when testing firewall configurations or troubleshooting firewall policies and rules. You can also use it to monitor the connection activity of specific applications and your system as a whole, and to terminate unwanted connections.

To view active internet connections on your computer

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface
- Click 'Firewall Tasks' from the 'Tasks' interface
- Click 'View Connections'

Tip: Alternatively, this screen can be accessed by clicking the number below 'Inbound' or 'Outbound' in the Advanced View of the Home screen in the 'Firewall' pane, or by clicking the second row in the widget.



Protocol	Source	Destination	Bytes In	Bytes Out
explorer.exe [2080]				
TCP OUT	10.108.51.131:49433	40.77.229.43:443	12.4 KB	12.1 KB
TCP OUT	10.108.51.131:50011	40.77.229.74:443	66 B	66 B
firefox.exe [3668]				
TCP OUT	10.108.51.131:50073	203.84.220.154:443	1.8 MB {5 B/s}	12.9 KB {5 ...
TCP OUT	10.108.51.131:50054	106.10.199.11:443	13.8 KB {2 B/s}	3.0 KB {2 B...
TCP OUT	10.108.51.131:49994	46.228.47.114:443	586.3 KB {25...	31.6 KB {2....
TCP OUT	10.108.51.131:49995	87.248.118.12:443	187.0 KB {1 ...	9.2 KB {2 B...
TCP OUT	10.108.51.131:50067	106.10.184.48:443	6.1 KB {21 B/s}	2.3 KB {33 ...

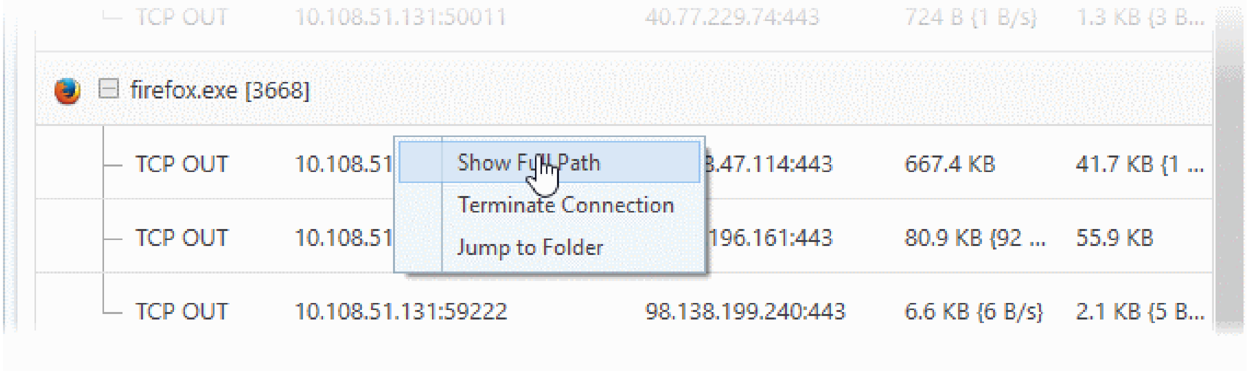
The 'View Connections' interface displays a list of all the currently active connections initiated by various applications as a tree structure.

Column Descriptions

- **Protocol** - Shows the application that is making the connection, the protocol it is using and the direction of the traffic. Each application may have more than one connection at any time. Clicking + at the left of the application name to expand the list of connections.
- **Source (IP : Port)** - The source IP Address and source port that the application is connecting through. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** - The destination IP Address and destination port address that the application is connecting to. This is blank if the 'Source' column is 'Listening'.
- **Bytes In** - Represents the total bytes of incoming data since this connection was first allowed.
- **Bytes Out** - Represents the total bytes of outgoing data since this connection was first allowed.

Context Sensitive Menu

- Right-click on an item in the list to see the context sensitive menu.



TCP OUT	10.108.51.131:50011	40.77.229.74:443	724 B {1 B/s}	1.3 KB {3 B...
firefox.exe [3668]				
TCP OUT	10.108.51	3.47.114:443	667.4 KB	41.7 KB {1 ...
TCP OUT	10.108.51	196.161:443	80.9 KB {92 ...	55.9 KB
TCP OUT	10.108.51.131:59222	98.138.199.240:443	6.6 KB {6 B/s}	2.1 KB {5 B...

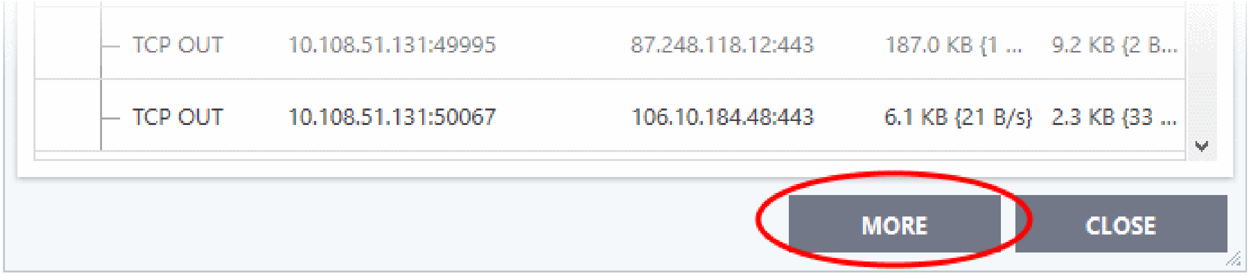
- 'Show Full Path' - view the location of the application
- 'Terminate Connection' – close the application's connection
- Click 'Jump to Folder to open the folder containing the executable file of the application

Identify and Kill Unsafe Network Connections

KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides you with yet another powerful layer of protection for Windows computers.

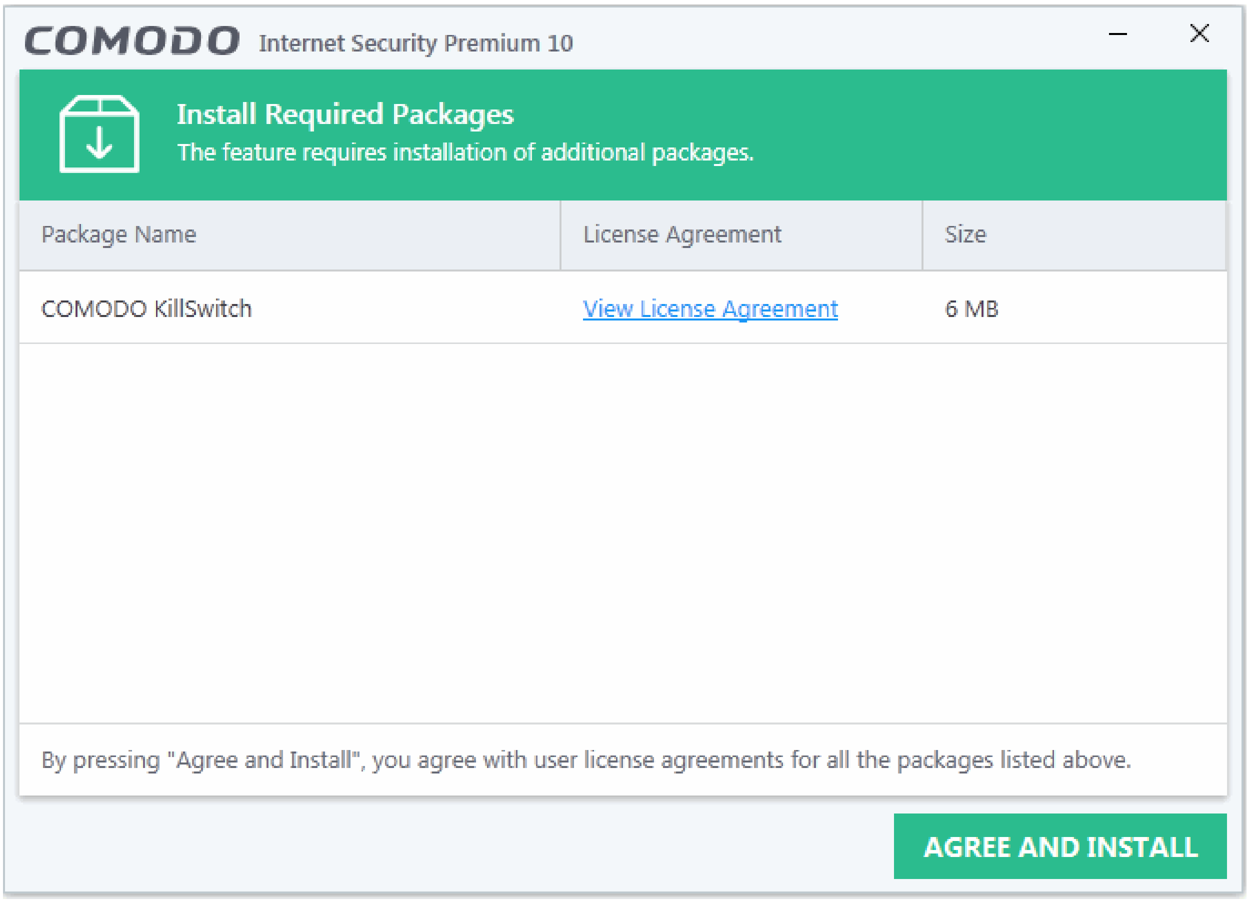
Comodo KillSwitch can show *ALL* running processes in granular detail- exposing even those that were invisible or very deeply hidden. You can simultaneously shut down every unsafe process with a single click and can even trace the process back to the parent malware.

You can directly access Comodo KillSwitch from the 'View Connections' screen by clicking the 'More' button:



TCP OUT	10.108.51.131:49995	87.248.118.12:443	187.0 KB {1 ...	9.2 KB {2 B...
TCP OUT	10.108.51.131:50067	106.10.184.48:443	6.1 KB {21 B/s}	2.3 KB {33 ...

If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



COMODO Internet Security Premium 10

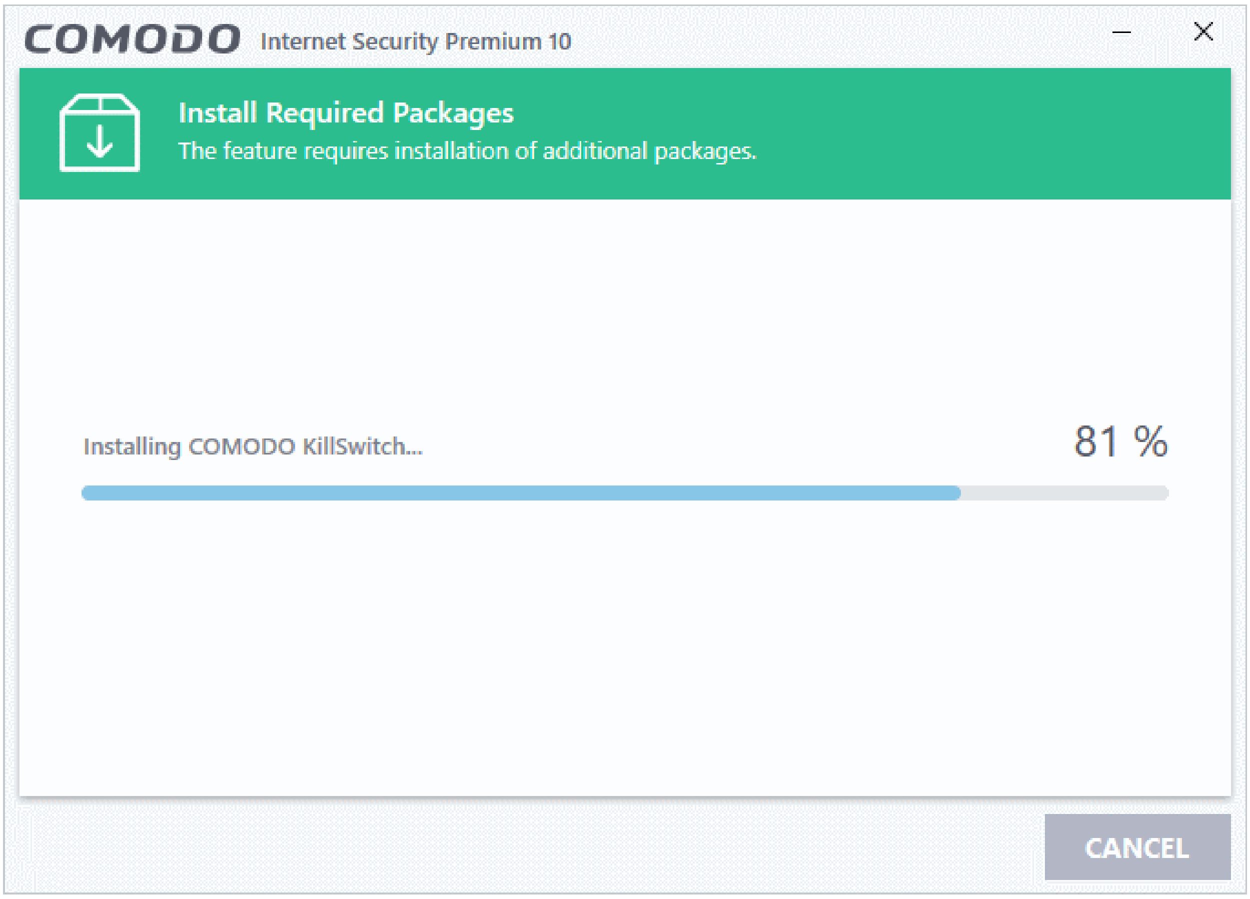
Install Required Packages

The feature requires installation of additional packages.

Package Name	License Agreement	Size
COMODO KillSwitch	View License Agreement	6 MB

By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.



COMODO Internet Security Premium 10

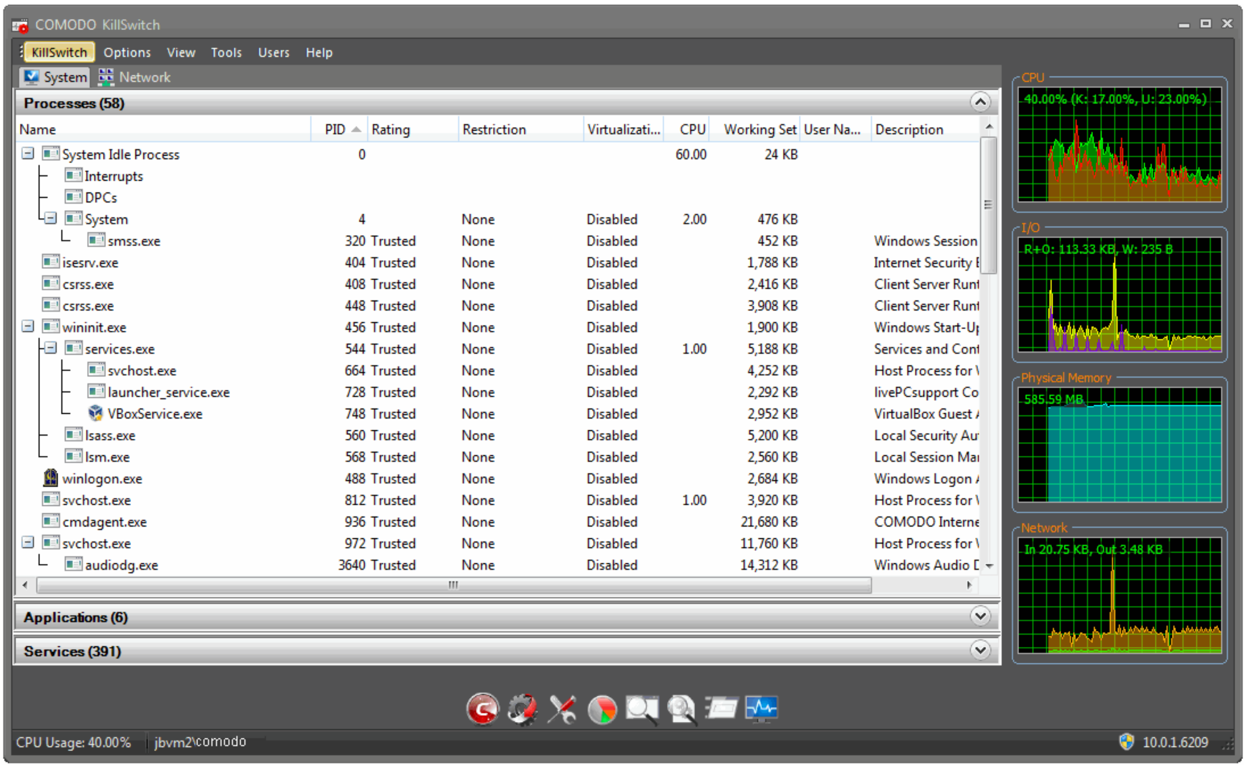
Install Required Packages

The feature requires installation of additional packages.

Installing COMODO KillSwitch...

81 %

On completion of installation, the Comodo KillSwitch main interface will be opened. Clicking the 'Network' tab will display the Network Connections and Network Utilization panes.

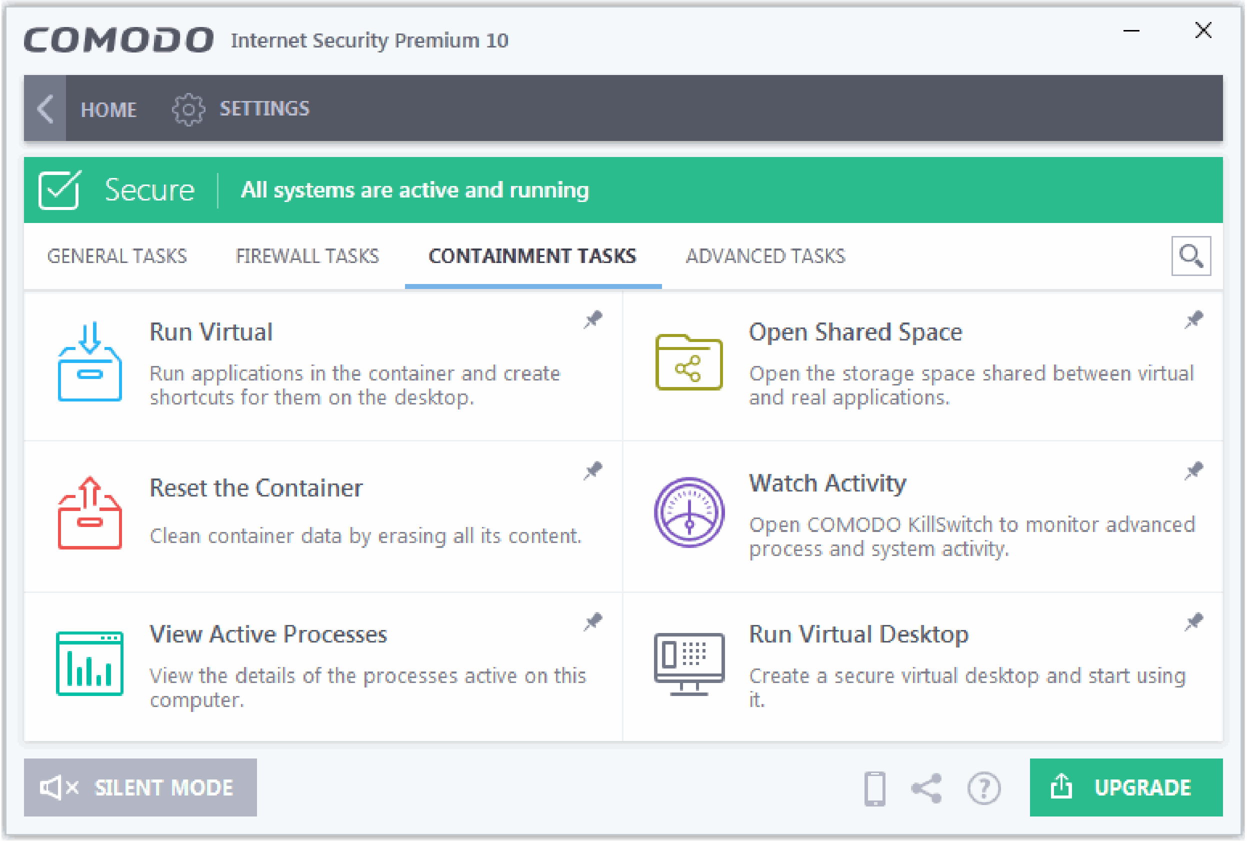


Name	PID	Rating	Restriction	Virtualizati...	CPU	Working Set	User Na...	Description
System Idle Process	0				60.00	24 KB		
Interrupts								
DPCs								
System	4		None	Disabled	2.00	476 KB		
smss.exe	320	Trusted	None	Disabled		452 KB		Windows Session
isesrv.exe	404	Trusted	None	Disabled		1,788 KB		Internet Security I
csrss.exe	408	Trusted	None	Disabled		2,416 KB		Client Server Runt
csrss.exe	448	Trusted	None	Disabled		3,908 KB		Client Server Runt
wininit.exe	456	Trusted	None	Disabled		1,900 KB		Windows Start-Uj
services.exe	544	Trusted	None	Disabled	1.00	5,188 KB		Services and Cont
svchost.exe	664	Trusted	None	Disabled		4,252 KB		Host Process for \
launcher_service.exe	728	Trusted	None	Disabled		2,292 KB		livePCsupport Co
VBoxService.exe	748	Trusted	None	Disabled		2,952 KB		VirtualBox Guest /
lsass.exe	560	Trusted	None	Disabled		5,200 KB		Local Security Au
lsm.exe	568	Trusted	None	Disabled		2,560 KB		Local Session Mai
winlogon.exe	488	Trusted	None	Disabled		2,684 KB		Windows Logon /
svchost.exe	812	Trusted	None	Disabled	1.00	3,920 KB		Host Process for \
cmdagent.exe	936	Trusted	None	Disabled		21,680 KB		COMODO Interne
svchost.exe	972	Trusted	None	Disabled		11,760 KB		Host Process for \
audiodg.exe	3640	Trusted	None	Disabled		14,312 KB		Windows Audio D

- Details of how to use KillSwitch to view granular details on current network connections and terminate unsafe connections can be found at **http://help.comodo.com/topic-119-1-328-3577-Viewing-and-Handling-Network-Connections-and-Usage.html**.
- The complete user guide for Comodo KillSwitch is available at **http://help.comodo.com/topic-119-1-328-3518-Introduction-to-KillSwitch.html**

4. Containment Tasks - Introduction

Comodo Internet Security features a secure, virtual environment called a 'container' in which you can run unknown, untrusted and suspicious applications. Contained applications are denied access to other processes, programs or data on your computer. In addition to running suspicious applications inside the container on an ad-hoc basis, you can create a desktop shortcut of programs that should always run in containment.



COMODO Internet Security Premium 10

Run Virtual

Run applications in the container and create shortcuts for them on the desktop.

Open Shared Space

Open the storage space shared between virtual and real applications.

Reset the Container

Clean container data by erasing all its content.

Watch Activity

Open COMODO KillSwitch to monitor advanced process and system activity.

View Active Processes

View the details of the processes active on this computer.

Run Virtual Desktop

Create a secure virtual desktop and start using it.

Important Note: The Containment feature is not supported on the following platforms:

- Windows XP 64 bit
- Windows Server 2003 64 bit

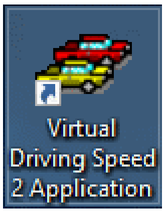
The 'Containment Tasks' interface has shortcuts for the following tasks:

- **Run Virtual** - Allows you to run individual applications in the container depending on the settings configured for it. The 'Advanced Settings' interface allows you to configure the overall 'Containment' behavior. Refer to the section '**Containment Settings**' for more details.
- **Open Shared Space** - Opens the folder 'Shared Space' which is shared by your host operating system and the Virtual Desktop. The folder is created by the Virtual Desktop at the location 'C:\Documents and Settings\All Users\Application Data\Shared Space'. The folder can be opened in both your host operating system and inside the Virtual Desktop, and enables to share files and applications between the OS and the Virtual Desktop.
- **Reset Container** - Allows you to clear all data written by programs inside the container.
- **Watch Activity** - Allows you to open Comodo Killswitch to identify unsafe processes and manage system activity.
- **View Active Process List** - Allows you to view processes which are currently running on your PC. Clicking the 'More' button will open Comodo **KillSwitch**, or present you with the opportunity to install KillSwitch if you do not have it installed.
- **Run Virtual Desktop** - Starts the Virtual Desktop.

4.1. Run an Application in the Container

- Comodo Internet Security allows you to run programs in containment on a 'one-off' basis.

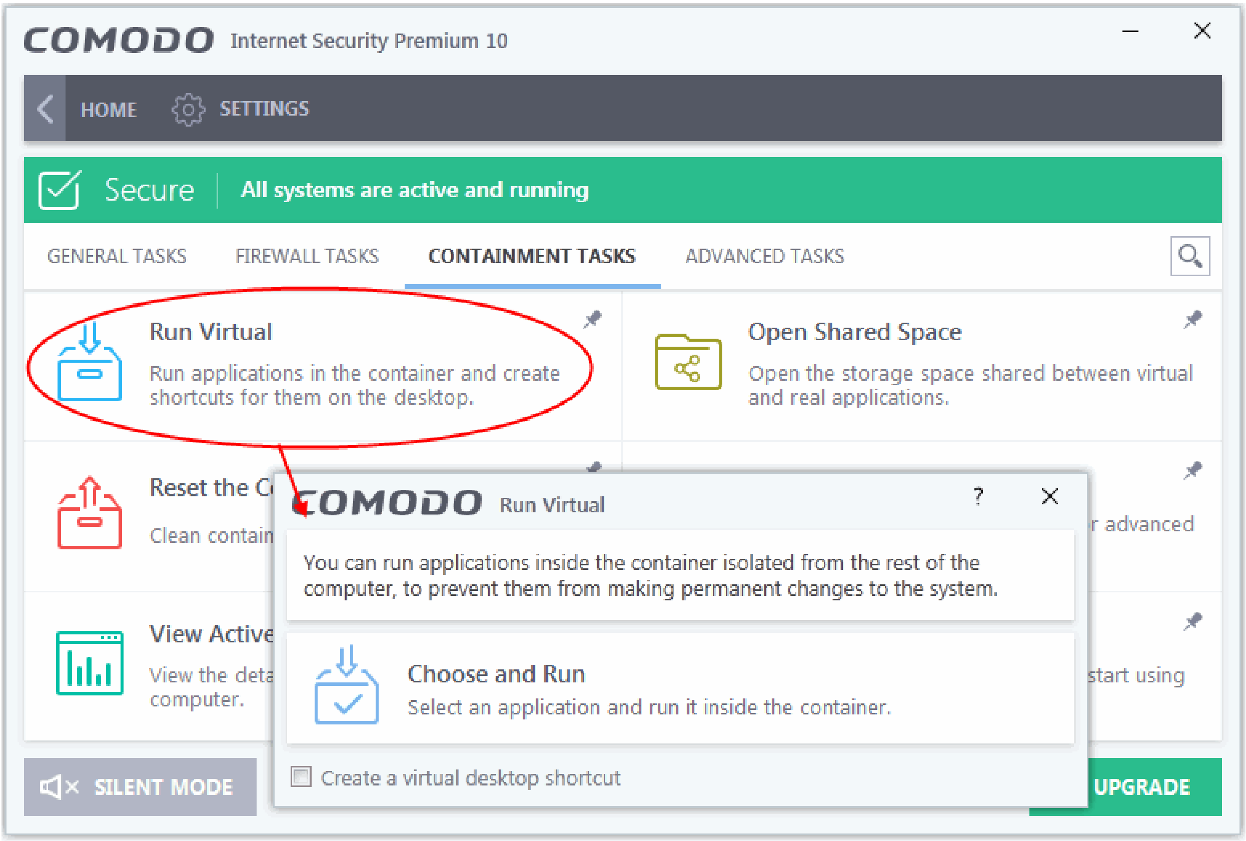
- This is helpful to test the behavior of new programs you have downloaded or for applications that you are not sure about.
- This method will run the application in the container one -time only. On subsequent executions it will not run in the container. You need to create an **auto- containment rule** if you want it to always run in the container.
- Alternatively, you can create desktop shortcuts to launch an application inside the container on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:



Note: If you wish to run an application in the container on a long-term/permanent basis then **add the file to the Container**.

To run an application in the Container

1. Open the 'Tasks' interface by clicking 'Tasks' from the top left of the CIS home screen
2. Click the 'Containment Tasks' tab
3. Click 'Run Virtual':


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Run Virtual
Run applications in the container and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset the C
Clean contain
r advanced
View Active
View the deta
computer.
start using
SILENT MODE
UPGRADE
COMODO Run Virtual
?
Choose and Run
Select an application and run it inside the container.

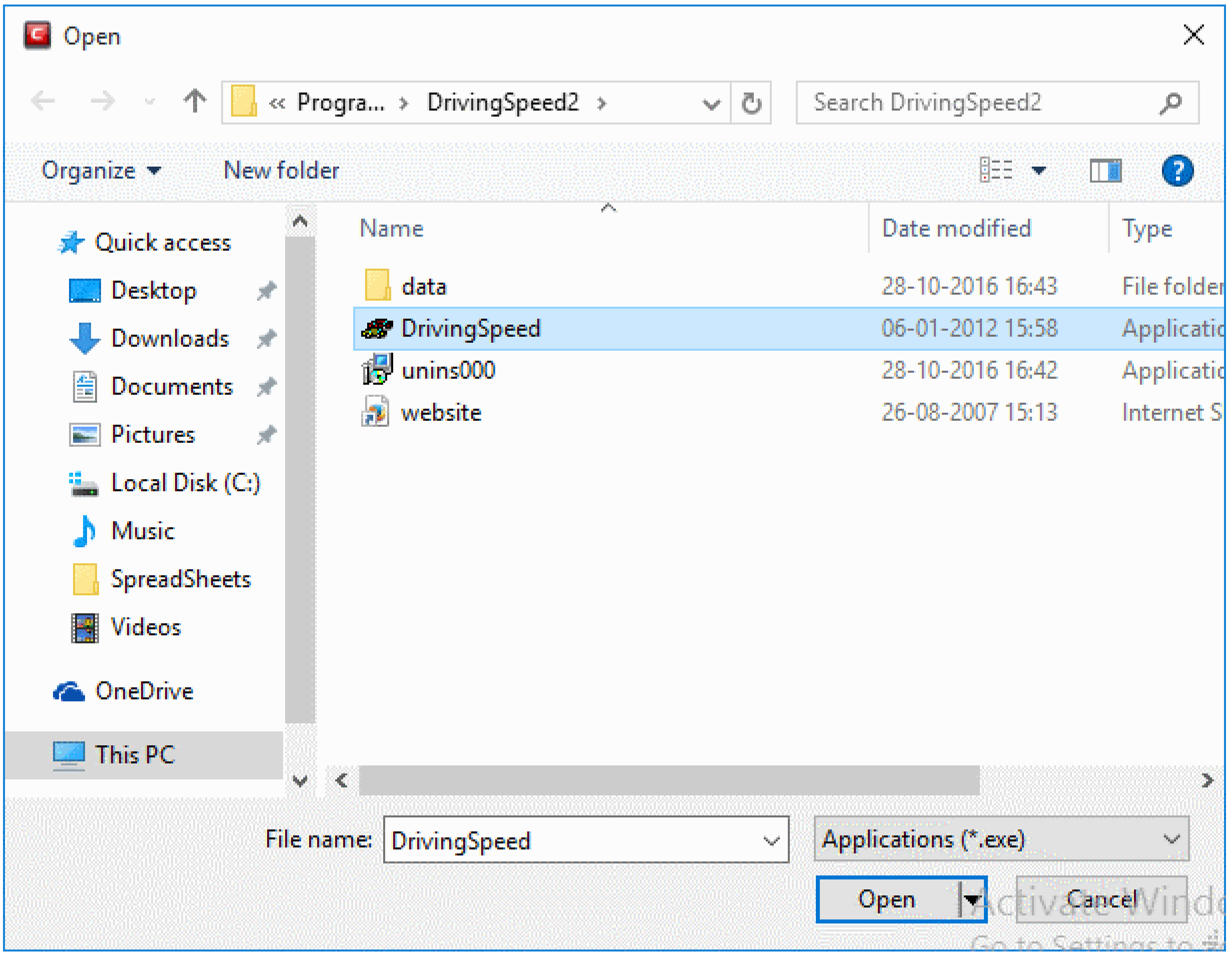
You can run applications inside the container isolated from the rest of the computer, to prevent them from making permanent changes to the system.

☐ Create a virtual desktop shortcut

The 'Run Virtual' dialog will be displayed.

4. Click 'Choose and Run' then browse to your application and click 'Open'.

The contained application will run with a green border around it. If you want to run the application in the container in future then enable 'Create a virtual desktop shortcut'.



Name	Date modified	Type
data	28-10-2016 16:43	File folder
DrivingSpeed	06-01-2012 15:58	Applicatio
unins000	28-10-2016 16:42	Applicatio
website	26-08-2007 15:13	Internet S

File name: DrivingSpeed

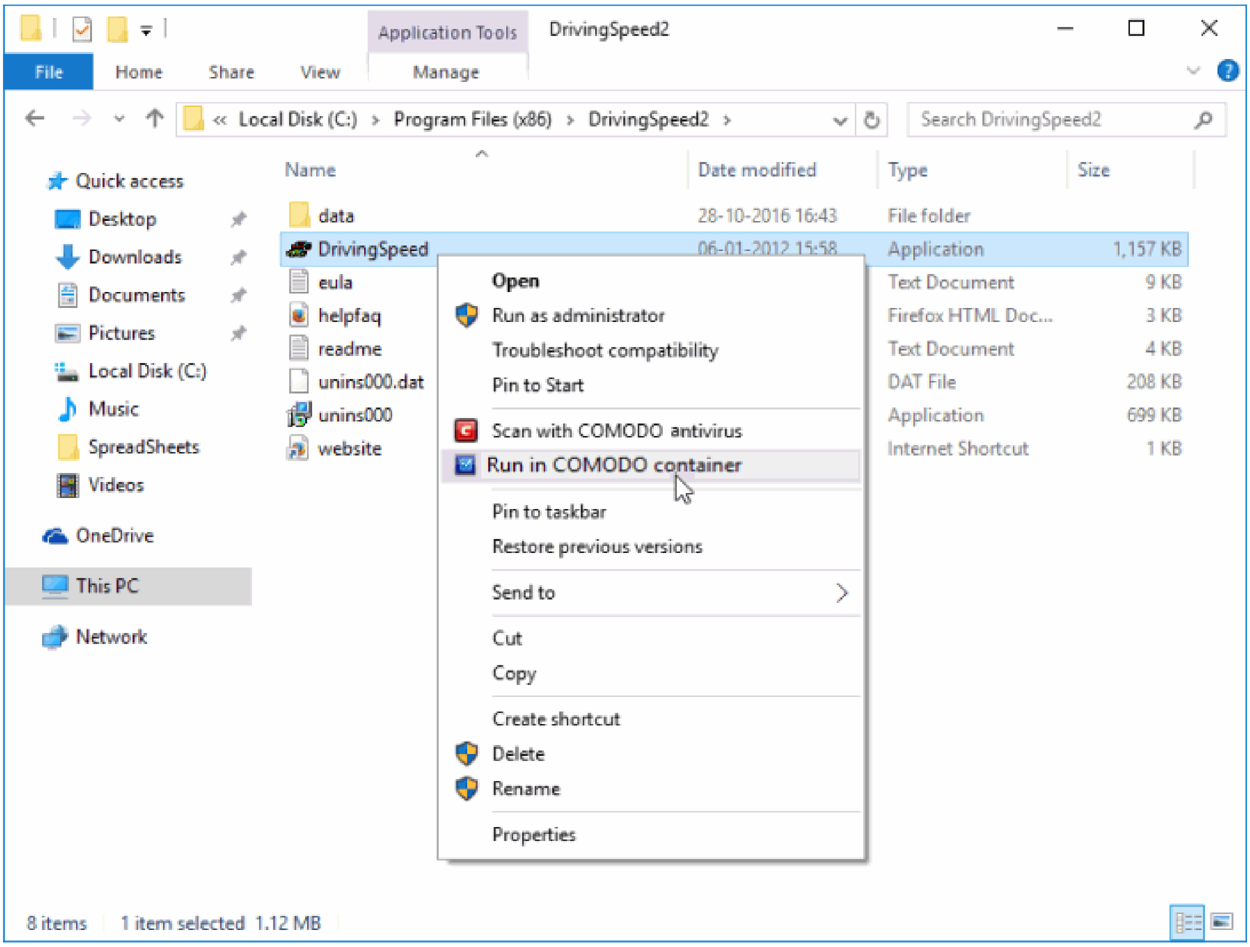
Applications (*.exe)

You can also run applications in the container on a one-off basis using the following methods:

- **From the context sensitive menu**
- **Running browsers inside container**

Running a program from the context sensitive menu

- Navigate to the program in your system that you want to run in the container and right click on it

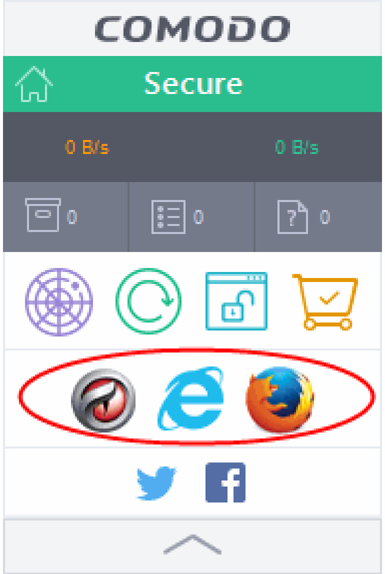


Name	Date modified	Type	Size
data	28-10-2016 16:43	File folder	
DrivingSpeed	06-01-2012 15:58	Application	1,157 KB
eula		Text Document	9 KB
helpfaq		Firefox HTML Doc...	3 KB
readme		Text Document	4 KB
unins000.dat		DAT File	208 KB
unins000		Application	699 KB
website		Internet Shortcut	1 KB

- Choose 'Run in Comodo container' from the context sensitive menu

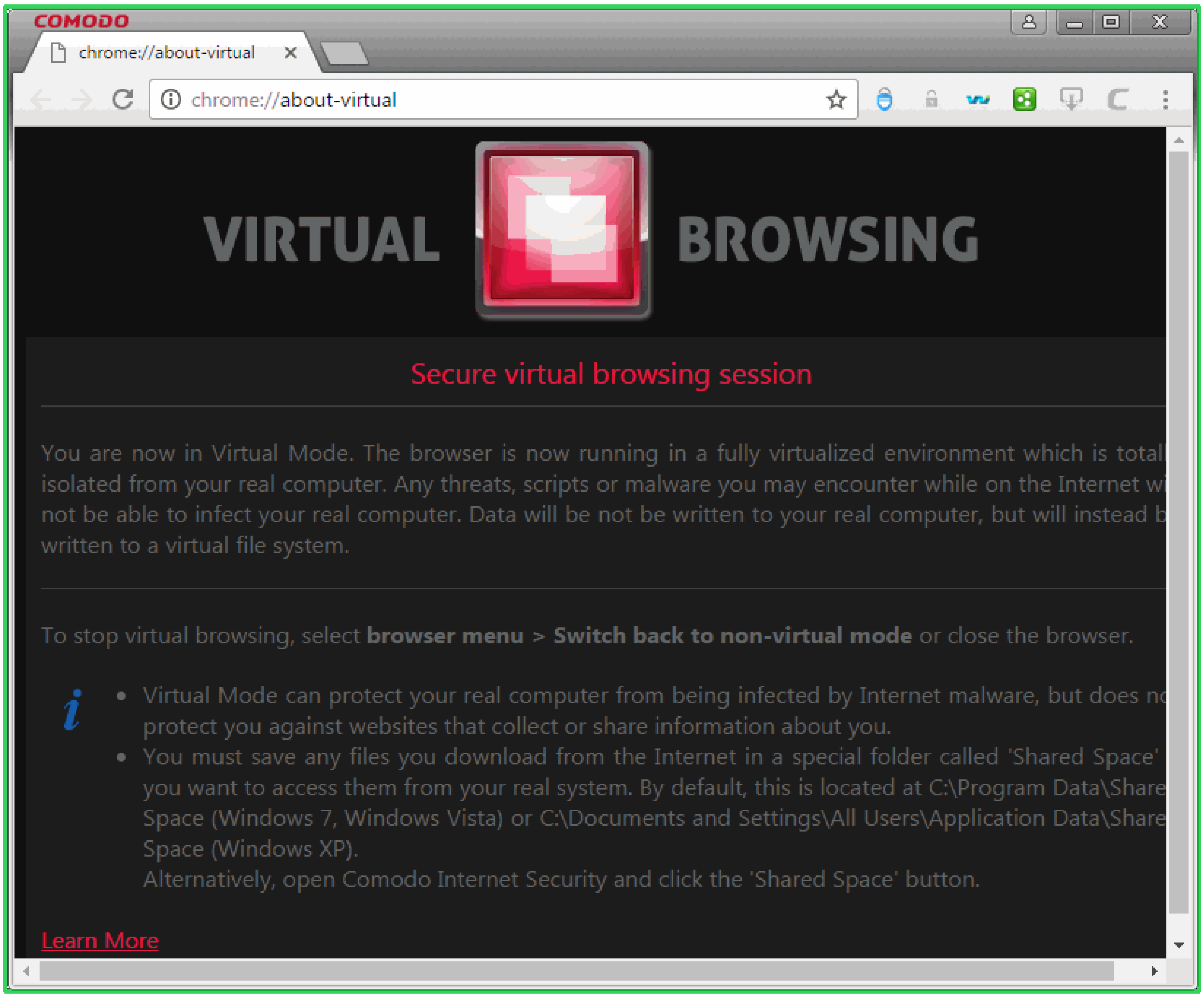
Running Browsers inside the container

The CIS Desktop Widget contains virtual shortcuts to your installed browsers:



- Clicking on a shortcut will start the browser inside the container.

CIS displays a green border around programs running inside the contained environment ('Show highlight frame for contained applications' must be enabled in '**Containment Settings**').



Secure virtual browsing session

You are now in Virtual Mode. The browser is now running in a fully virtualized environment which is total isolated from your real computer. Any threats, scripts or malware you may encounter while on the Internet wi not be able to infect your real computer. Data will be not be written to your real computer, but will instead b written to a virtual file system.

To stop virtual browsing, select **browser menu > Switch back to non-virtual mode** or close the browser.

- Virtual Mode can protect your real computer from being infected by Internet malware, but does no protect you against websites that collect or share information about you.
- You must save any files you download from the Internet in a special folder called 'Shared Space' you want to access them from your real system. By default, this is located at C:\Program Data\Share Space (Windows 7, Windows Vista) or C:\Documents and Settings\All Users\Application Data\Share Space (Windows XP).
  Alternatively, open Comodo Internet Security and click the 'Shared Space' button.

Learn More

Tip: Running a browser inside the container deletes all traces of your browsing activities. This includes your browsing history and cookies and offline data stored by the websites you visit. Virtualization protects your computer from anything malicious that is downloaded. See **The Virtual Desktop** for more details.

However, for visiting important shopping or banking websites, we recommend you use the Secure Shopping environment. Secure Shopping hides your browsing sessions from the rest of your computer and protects your data from any potentially hostile processes running on your computer.

What's the difference between Secure Shopping and the Virtual Desktop/Virtualization?

The two systems are intended for opposite use cases. The virtual desktop/virtualization protects your computer by isolating potentially malicious applications and processes inside a container. Secure Shopping is the reverse of this. It protects the application itself (e.g. browser) from any potentially malicious applications running on your computer. With Secure Shopping, your secure banking sessions are totally sealed off from the rest of your computer.

See **Comodo Secure Shopping** for more details.

4.2. Reset the Container

- Programs running inside the container write all data and system changes inside the container itself. This means the program cannot harm your real computer or sensitive data.
- Files saved in the container could, depending on your usage patterns, contain malware downloaded from

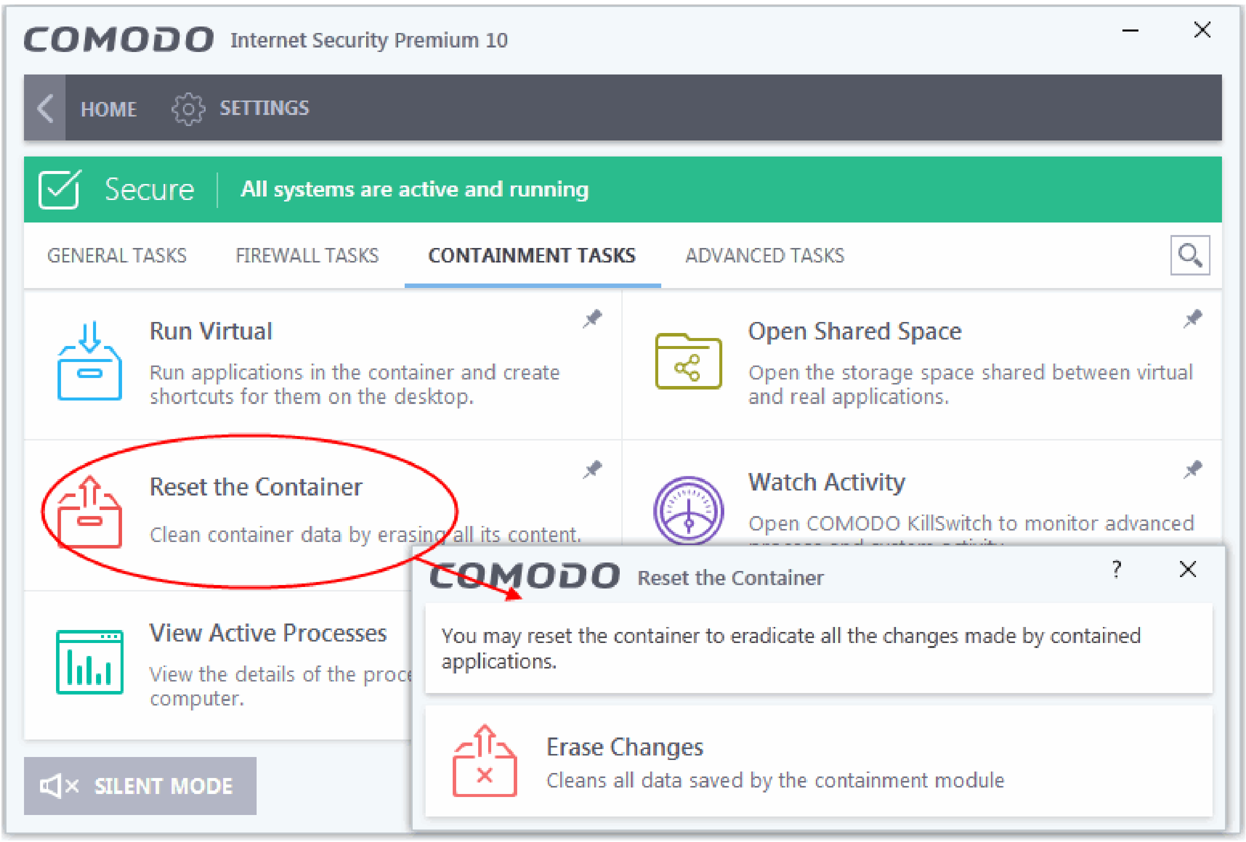
websites or private data in your browsing history.

- Periodically resetting the container will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time, then a reset will also help the container operate more smoothly.

The 'Reset Container' option under the 'Containment' feature allows you to delete all items stored in the container.

To clear the container

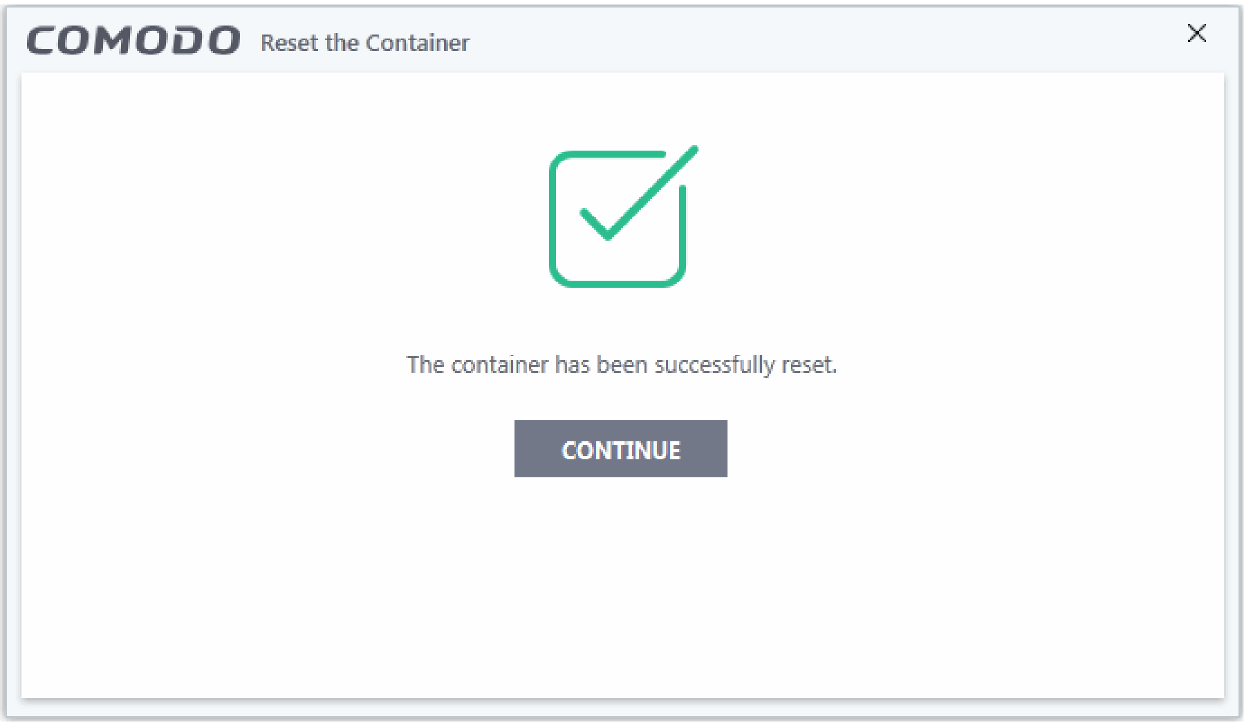
- Click 'Tasks' on the CIS home screen
- Click the 'Containment Tasks' tab
- Click 'Reset the Container':


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Run Virtual
Run applications in the container and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset the Container
Clean container data by erasing all its content.
Watch Activity
Open COMODO KillSwitch to monitor advanced
View Active Processes
View the details of the proce
computer.
SILENT MODE
COMODO Reset the Container
You may reset the container to eradicate all the changes made by contained applications.
Erase Changes
Cleans all data saved by the containment module

The 'Reset the Container' dialog will appear:

- Click 'Erase Changes'.

The contents in the container will be deleted immediately.



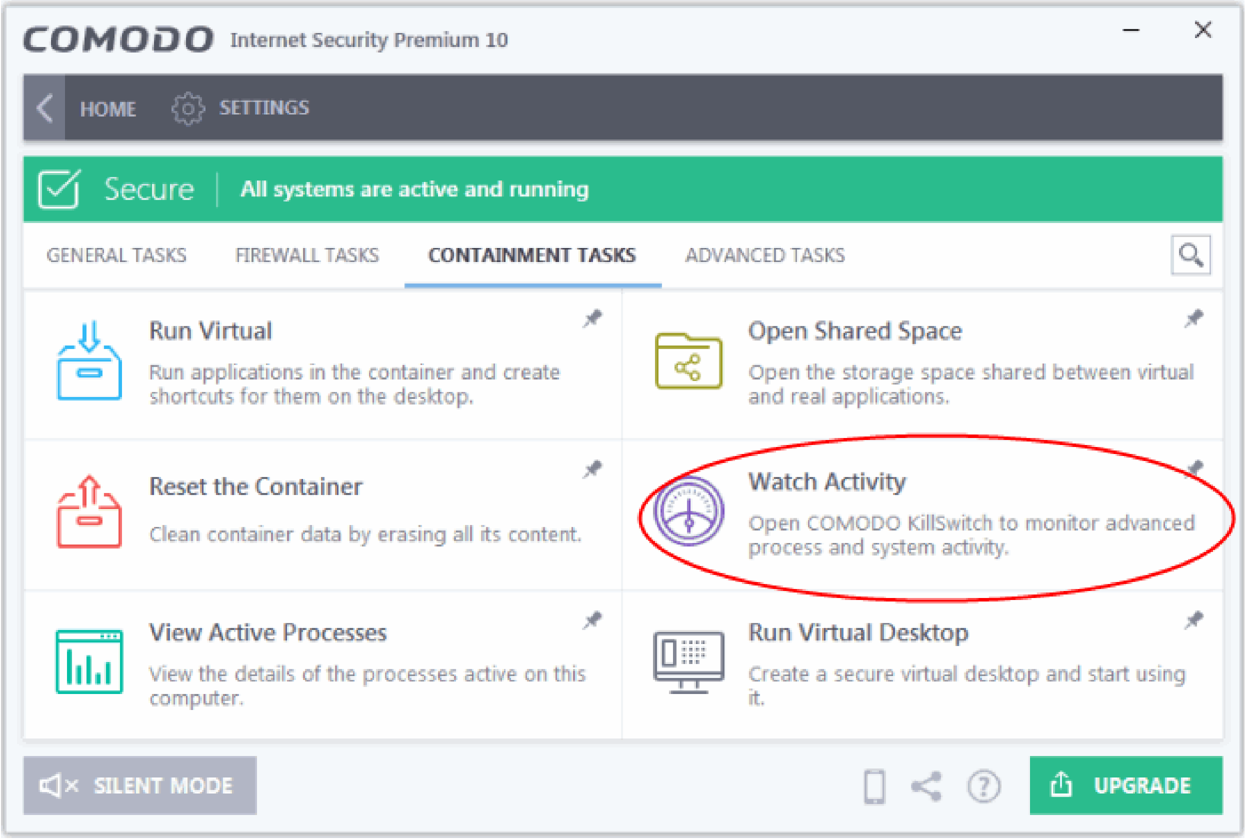
The container has been successfully reset.

4.3. Identify and Kill Unsafe Running Processes

Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer of protection for Windows computers.

KillSwitch can show ALL running processes - exposing even those that were invisible or very deeply hidden. It allows you to identify which of those running processes are unsafe and to shut them all down with a single click. You can also use Killswitch to trace back to the software that generated the unsafe process.

Comodo KillSwitch can be directly accessed from the CIS interface by clicking 'Watch Activity' from the 'Containment Tasks' interface.



Secure | All systems are active and running

Run Virtual
Run applications in the container and create shortcuts for them on the desktop.

Open Shared Space
Open the storage space shared between virtual and real applications.

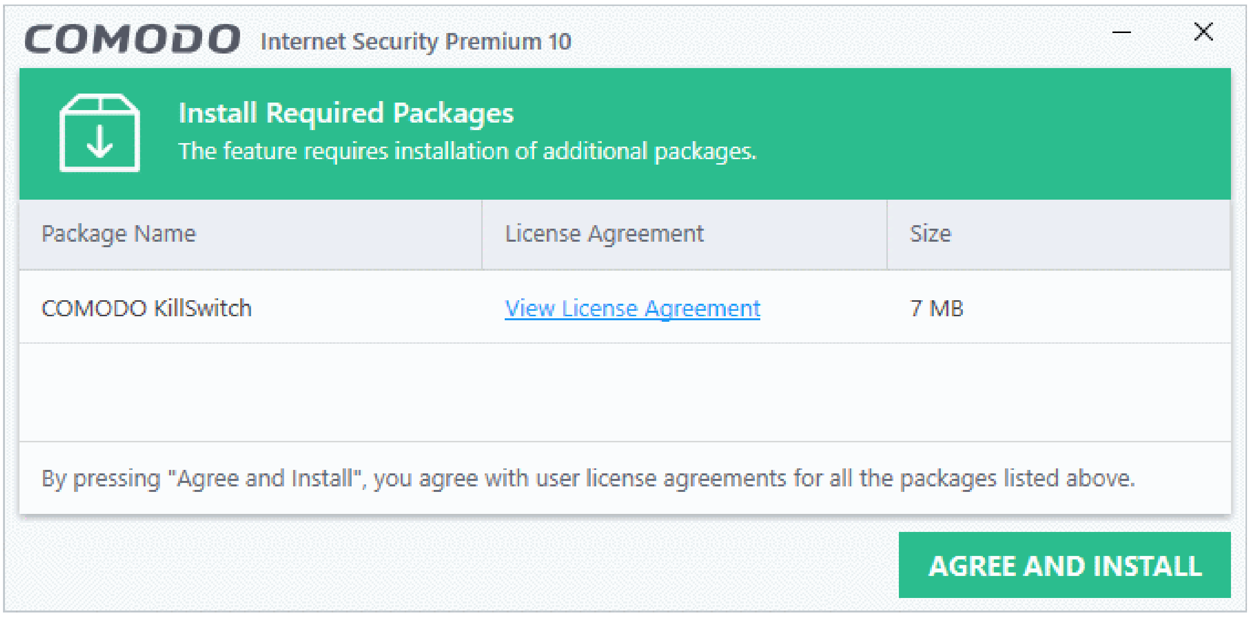
Reset the Container
Clean container data by erasing all its content.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

View Active Processes
View the details of the processes active on this computer.

Run Virtual Desktop
Create a secure virtual desktop and start using it.

- Killswitch is a component of Comodo Cleaning Essentials. If you have already installed Comodo Cleaning Essentials by clicking 'Clean Endpoint' from the 'Advanced' task interface, clicking the 'Watch Activity' will open the KillSwitch interface directly. See **Remove Deeply Hidden Malware** for more details on installing Cleaning Essentials.
- When you click 'Watch Activity' for the first time, CIS will download and install Comodo Killswitch. After it installed, clicking this button in future will open the Killswitch interface.

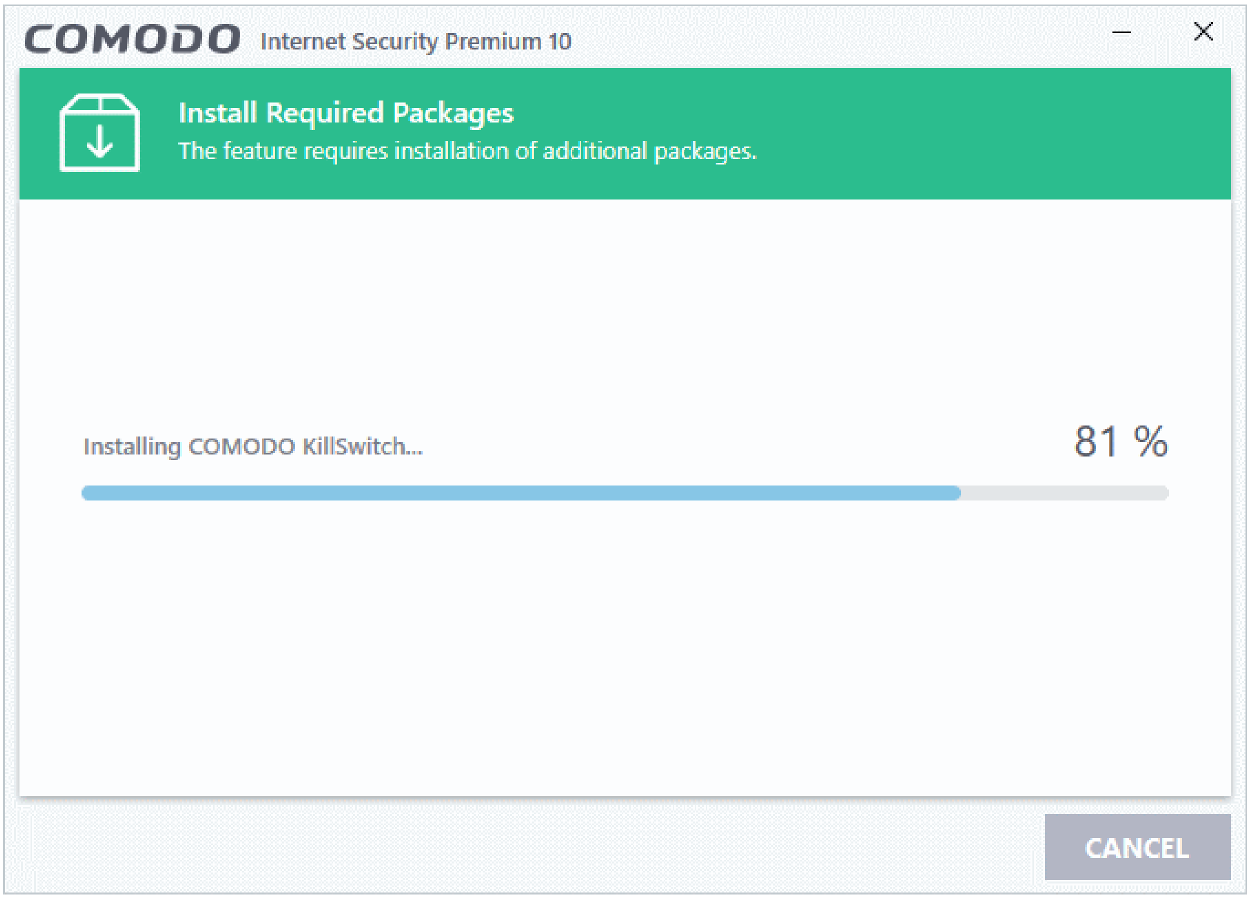


Install Required Packages
The feature requires installation of additional packages.

Package Name	License Agreement	Size
COMODO KillSwitch	View License Agreement	7 MB

By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.



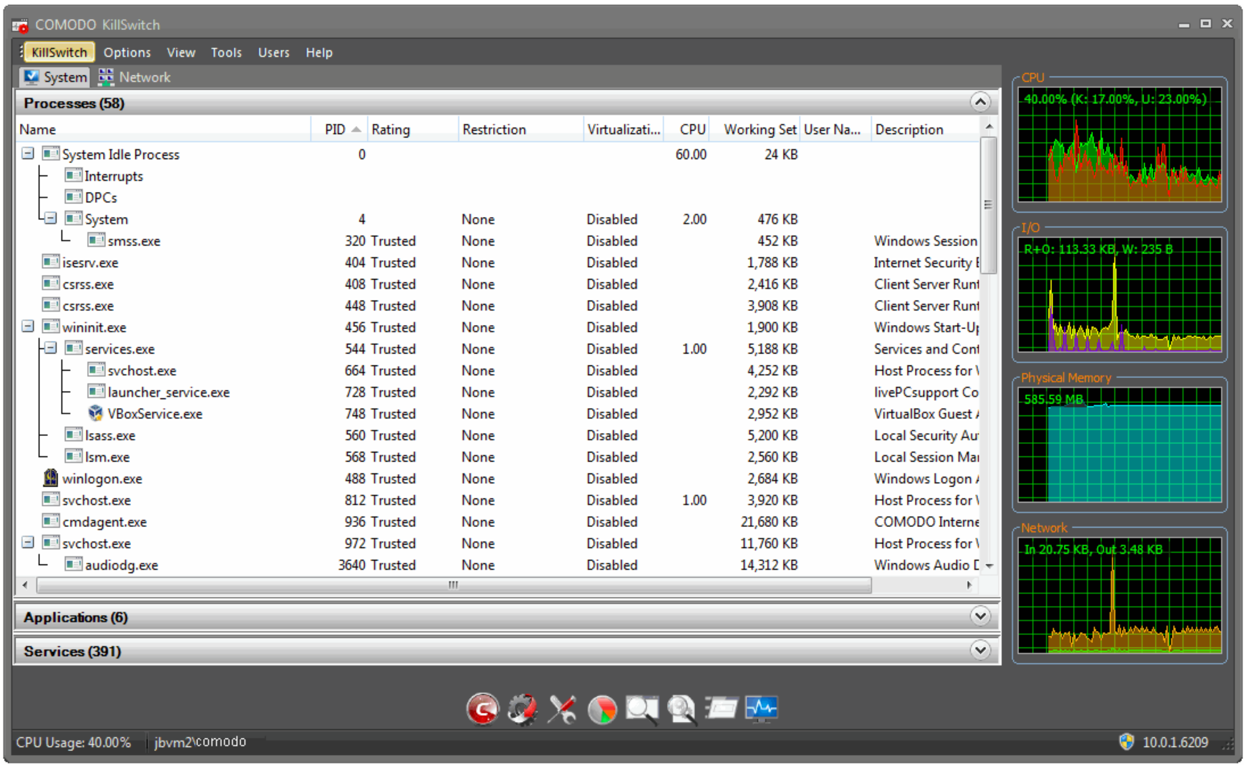
COMODO Internet Security Premium 10

Install Required Packages

The feature requires installation of additional packages.

Installing COMODO KillSwitch... 81 %

On completion of installation, the Comodo KillSwitch main interface will be opened.



Processes (58)

Name	PID	Rating	Restriction	Virtualizati...	CPU	Working Set	User Na...	Description
System Idle Process	0				60.00	24 KB		
Interrupts								
DPCs								
System	4		None	Disabled	2.00	476 KB		
smss.exe	320	Trusted	None	Disabled		452 KB		Windows Session
isesrv.exe	404	Trusted	None	Disabled		1,788 KB		Internet Security E
csrss.exe	408	Trusted	None	Disabled		2,416 KB		Client Server Runt
csrss.exe	448	Trusted	None	Disabled		3,908 KB		Client Server Runt
wininit.exe	456	Trusted	None	Disabled		1,900 KB		Windows Start-Up
services.exe	544	Trusted	None	Disabled	1.00	5,188 KB		Services and Cont
svchost.exe	664	Trusted	None	Disabled		4,252 KB		Host Process for W
launcher_service.exe	728	Trusted	None	Disabled		2,292 KB		livePCsupport Co
VBoxService.exe	748	Trusted	None	Disabled		2,952 KB		VirtualBox Guest A
lsass.exe	560	Trusted	None	Disabled		5,200 KB		Local Security Au
lsm.exe	568	Trusted	None	Disabled		2,560 KB		Local Session Mai
winlogon.exe	488	Trusted	None	Disabled		2,684 KB		Windows Logon A
svchost.exe	812	Trusted	None	Disabled	1.00	3,920 KB		Host Process for W
cmdagent.exe	936	Trusted	None	Disabled		21,680 KB		COMODO Interne
svchost.exe	972	Trusted	None	Disabled		11,760 KB		Host Process for W
audiodg.exe	3640	Trusted	None	Disabled		14,312 KB		Windows Audio D

Applications (6)

Services (391)

CPU Usage: 40.00% | jbvm2\comodo | 10.0.1.6209

On clicking the 'Watch Activity' button from next time onwards, Comodo Killswitch will be opened.

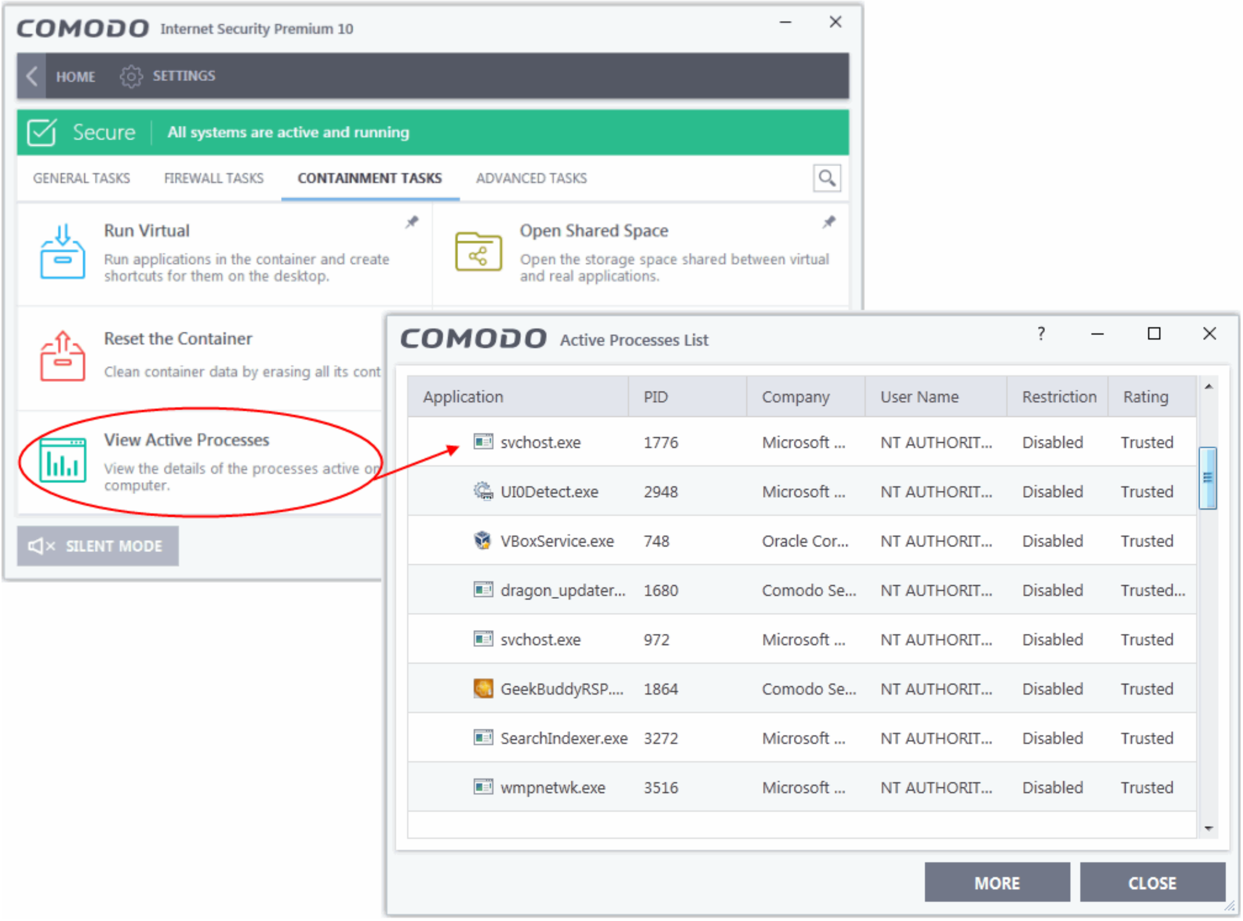
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at **http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html**

4.4. View Active Process List

- The 'Active Process List' shows all currently running processes started by applications currently running on your system.
- CIS can trace an application's parent process to detect whether a non-trusted application is attempting to spawn a trusted application. CIS can then deny access rights to that trusted application.
- This level of inspection provides the very highest protection against malware and rootkits that try to use trusted software to launch an attack.
- The interface also lets you run an online lookup on the parent application, so you can check its trust rating on the latest cloud databases. You can also submit an application to Comodo for analysis, kill unwanted processes and more.

To view the active processes

- Open the 'Tasks' interface by clicking 'Tasks' on the CIS home screen
- Click the 'Containment Tasks' tab
- Click 'View Active Processes':



Run applications in the container and create shortcuts for them on the desktop.

Open the storage space shared between virtual and real applications.

Clean container data by erasing all its cont

View the details of the processes active o computer.

Application	PID	Company	User Name	Restriction	Rating
svchost.exe	1776	Microsoft ...	NT AUTHORIT...	Disabled	Trusted
UI0Detect.exe	2948	Microsoft ...	NT AUTHORIT...	Disabled	Trusted
VBoxService.exe	748	Oracle Cor...	NT AUTHORIT...	Disabled	Trusted
dragon_updater...	1680	Comodo Se...	NT AUTHORIT...	Disabled	Trusted...
svchost.exe	972	Microsoft ...	NT AUTHORIT...	Disabled	Trusted
GeekBuddyRSP....	1864	Comodo Se...	NT AUTHORIT...	Disabled	Trusted
SearchIndexer.exe	3272	Microsoft ...	NT AUTHORIT...	Disabled	Trusted
wmpnetwk.exe	3516	Microsoft ...	NT AUTHORIT...	Disabled	Trusted

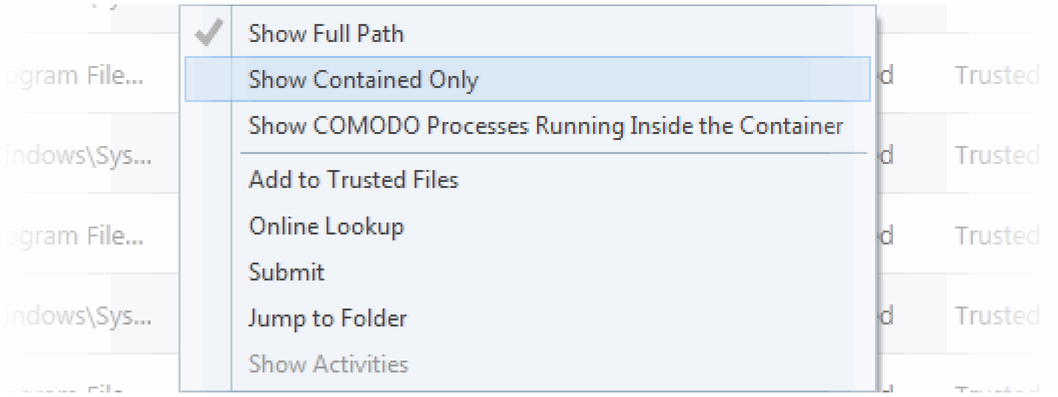
The currently active processes will be displayed.

Column Descriptions

- **Application -** Displays the names of the applications which are currently running on your PC.
- **PID** - Process Identification Number.
- **Company -** Displays the name of the software developer.
- **User Name** - The name of the user that started the process.

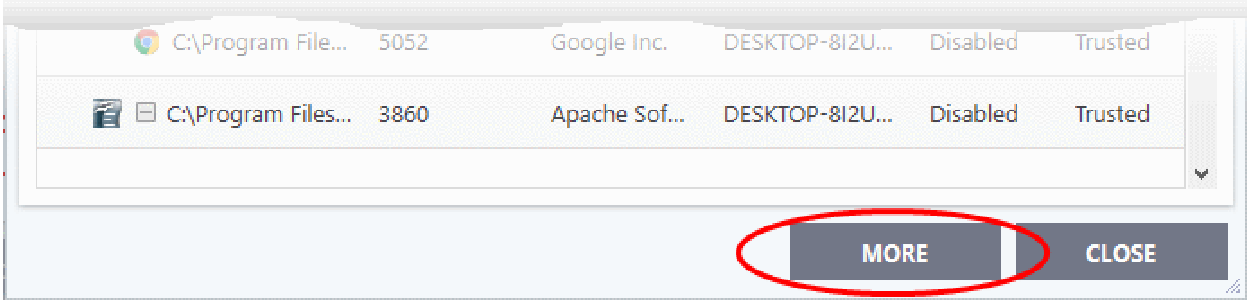
- **Restriction -** Displays the level of containment level of the program.
- **Rating** - Displays the rating of the application whether trusted or unknown.

Right-click on any process to:



- Show Full Path: Displays the location of the executable in addition to it's name.
- Show Contained Only: Will only show programs that are running inside the container.
- Show COMODO Processes Running Inside the Container: Will only show Comodo processes running inside the container.
- Add to Trusted Files: The selected unknown program will be added to CIS '**File List**' with Trusted Status. See '**File List**' for more details.
- Online Lookup: Conducts a look-up of the program in Comodo's global blacklists and whitelists. The results will tell you with the file is clean, malicious or unknown.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: The folder containing the executable file of the application will open.
- Show Activities: Opens the '**Process Activities List dialog**'. The Process Activities dialog will display the list activities of the processes run by the application. The 'Show Activities' option is available only if **VirusScope is enabled** under **VirusScope**.

Clicking the 'More' button at the bottom of the screen will open the Comodo KillSwitch application - an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on your system.

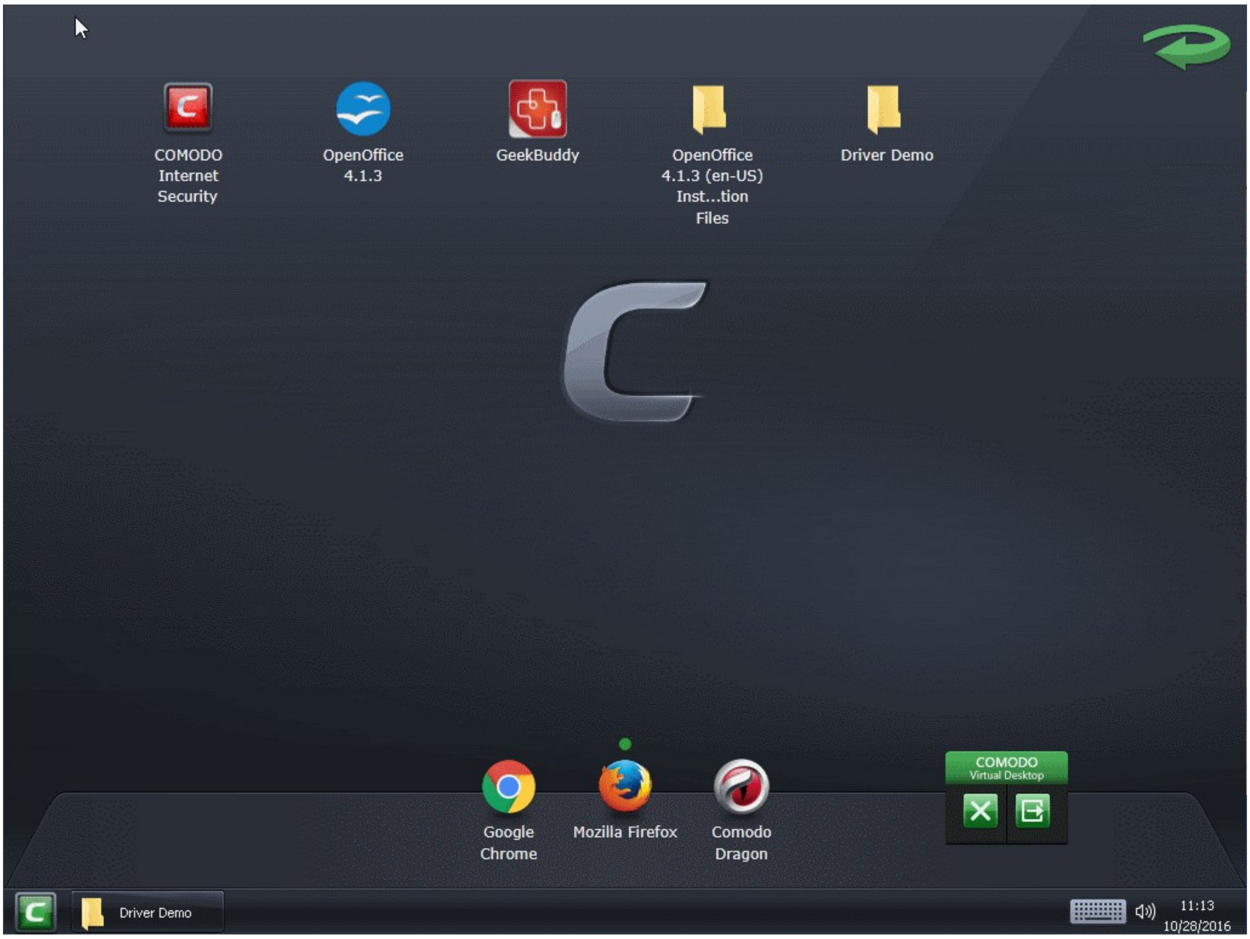


C:\Program File...	5052	Google Inc.	DESKTOP-8I2U...	Disabled	Trusted
C:\Program Files...	3860	Apache Sof...	DESKTOP-8I2U...	Disabled	Trusted

If KillSwitch is not yet installed, clicking this button will prompt you to download the application. See **Identify and Kill Unsafe Running Processes** for more details.

4.5. The Virtual Desktop

The Virtual Desktop is a sandbox operating environment inside of which you can run programs and browse the internet without fear that those activities will damage your computer. Applications running in the Virtual Desktop are isolated from the rest of your computer, write to a virtual file system and cannot access your personal data. This makes it ideal for visiting any risky websites/links and for testing out beta/unstable software.



Virtual Desktop at a glance:

- The Virtual Desktop can run any program that you can run in regular Windows. It is ideal for running untested, unknown and beta software. You can also use it to visit websites that you are not sure about.
- Any changes made to files and settings in the Virtual Desktop will not affect the original versions on your host system. Changes will only be visible in the Virtual System itself.
- Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Any files you wish to keep and access from your host operating system can be saved to 'Shared Space'.
- The Virtual Desktop can be password-protected for added privacy.
- The virtual keyboard allows you to securely enter confidential passwords without fear of key-logging software. Note - we recommend you use the secure shopping environment instead when visiting important shopping or banking websites. See '**Comodo Secure Shopping**' for more details.
- The Virtual Desktop UI can be used in both 'Classic' (Windows style) and 'Tablet' modes by selecting the mode from '**Settings**'.
- You can reset the Virtual Desktop and clear shared space at any time. We recommend that you do this regularly to maximize your privacy and security. Please note that all settings, stored data and any applications you installed in the Virtual Desktop will be deleted.
- Apart from testing software, parents may want to consider the Virtual Desktop as a secure area for children to run programs and surf the web without fear their actions could damage the host computer. The Virtual Desktop can be reset and all changes cleared at the end of every session.

Click the following links to find out more details on:

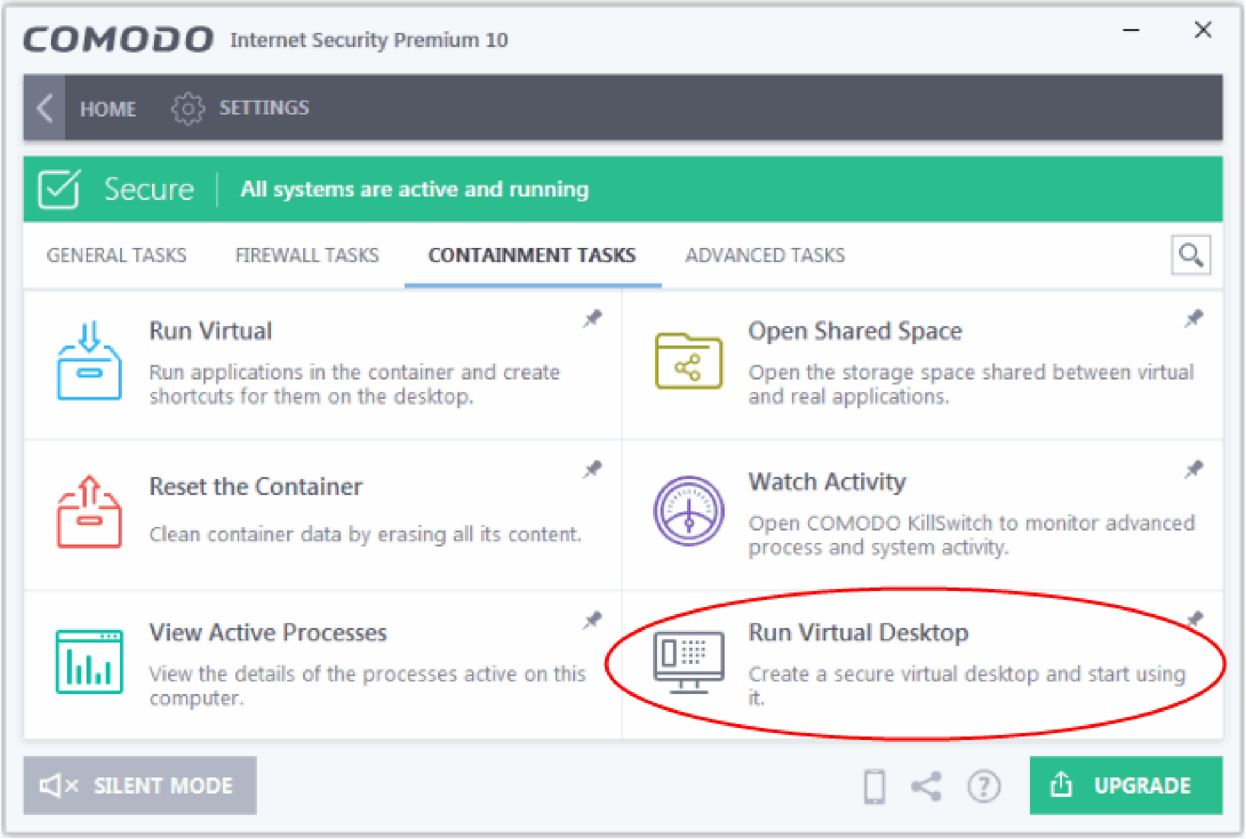
- **Starting the Virtual Desktop**

- The Main Interface
- Run Browsers inside Virtual Desktop
- Open Files and Run Applications inside Virtual Desktop
- Configuring the Virtual Desktop
- Closing the Virtual Desktop

4.5.1. Starting the Virtual Desktop

The Virtual Desktop can be started by:

- Clicking 'Run Virtual Desktop' from the 'Containment Tasks' screen

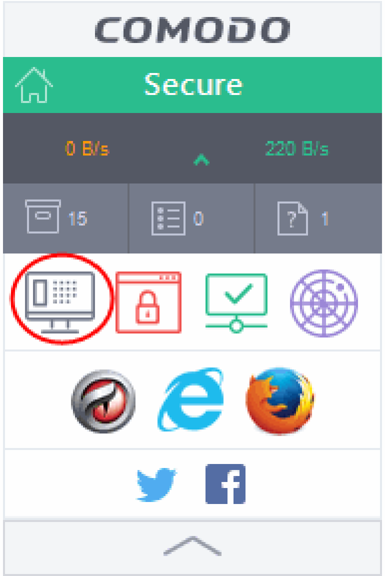

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Run Virtual
Run applications in the container and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset the Container
Clean container data by erasing all its content.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
View Active Processes
View the details of the processes active on this computer.
Run Virtual Desktop
Create a secure virtual desktop and start using it.
SILENT MODE
UPGRADE

OR

- by clicking the 'Run Virtual Desktop' shortcut button Run Virtual Desktop from the basic view of CIS home screen

OR

- by clicking the 'Virtual Desktop' shortcut button from the CIS widget

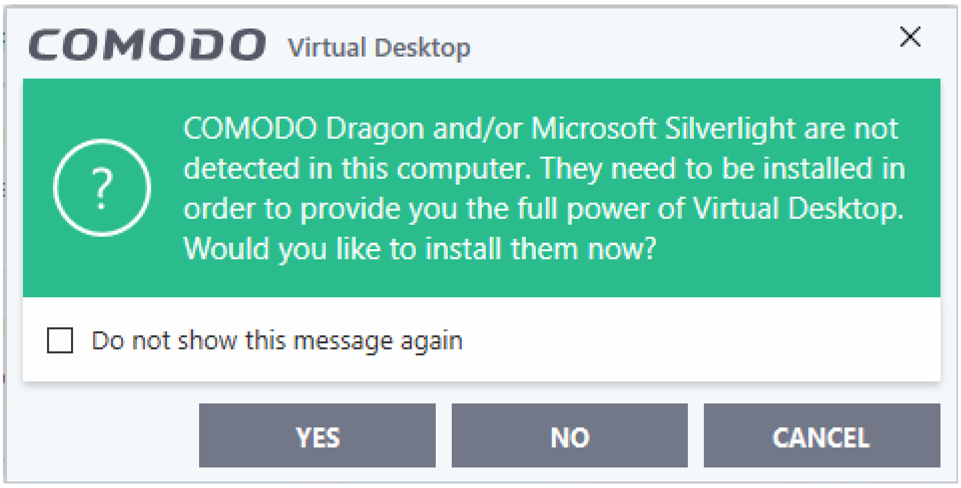


Note: The shortcuts in the home screen and the Widget will be available only if you have added the 'Virtual Desktop' shortcut. See '**Adding tasks to the home screen**' in '**The Home Screen**' for more details.

To run the Virtual Desktop, you must have the following installed:

- Comodo Dragon Browser
- Microsoft Silverlight

Whenever you run the Virtual Desktop, Comodo Internet Security checks whether these components are installed. If they aren't, you will be prompted to install them.


COMODO Virtual Desktop

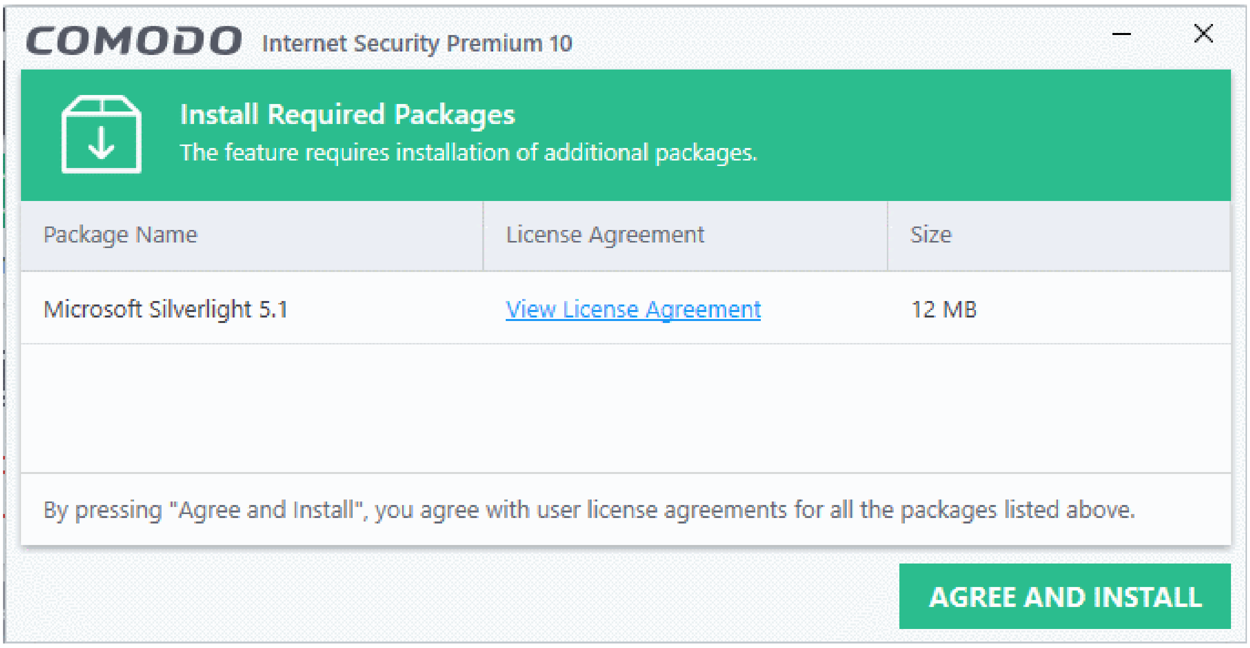
COMODO Dragon and/or Microsoft Silverlight are not detected in this computer. They need to be installed in order to provide you the full power of Virtual Desktop. Would you like to install them now?

□ Do not show this message again

- If you want Comodo Dragon Browser and/or Microsoft Silverlight to be installed this time, click 'Yes'. If not, click 'Cancel'. You will be prompted to install them, next time when you start the Virtual Desktop.
- If you do not want the applications to be installed at all, click 'NO'.

- Click 'Yes' to download and install the software.

The 'Install Required Packages' dialog will be displayed.



COMODO Internet Security Premium 10

Install Required Packages

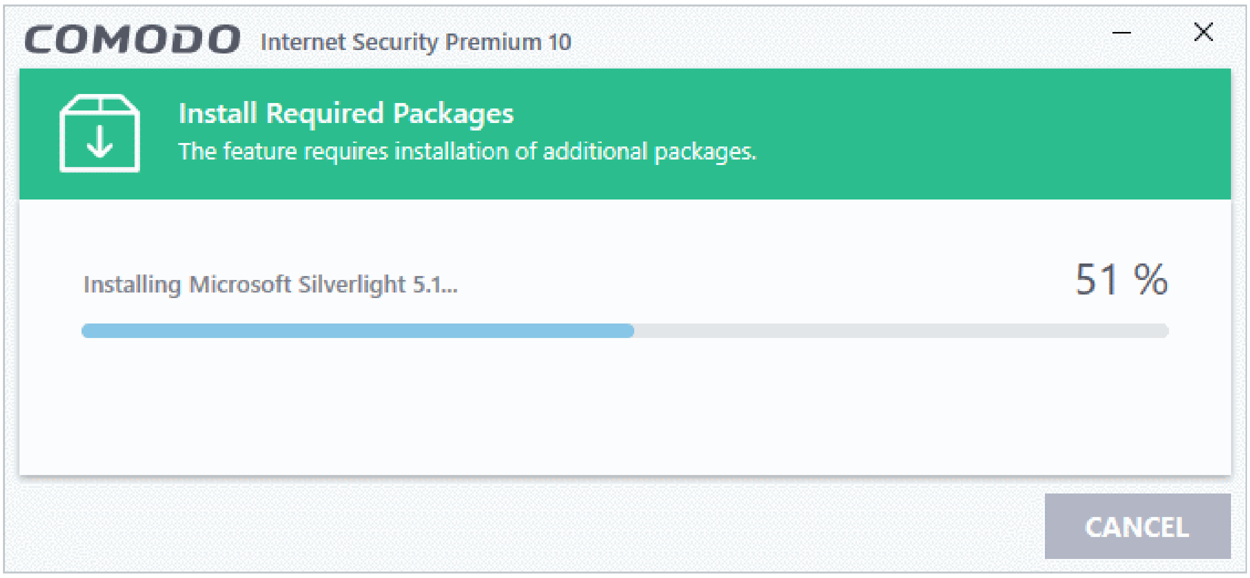
The feature requires installation of additional packages.

Package Name	License Agreement	Size
Microsoft Silverlight 5.1	View License Agreement	12 MB

By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

- Click 'View License Agreement' to read the license agreement of the additional software to be installed
- Click 'Agree and Install' to download and install the required software

The software package(s) will be downloaded and installed automatically.



COMODO Internet Security Premium 10

Install Required Packages

The feature requires installation of additional packages.

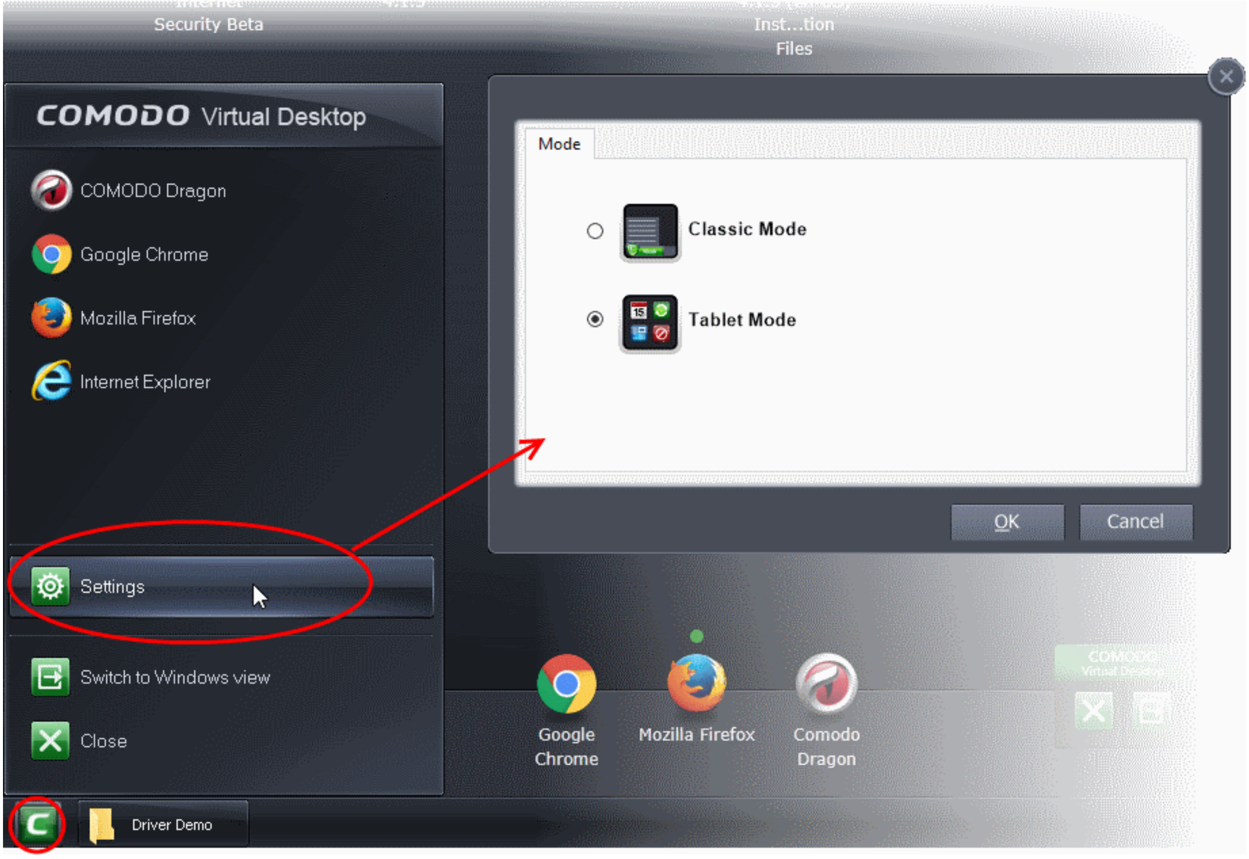
Installing Microsoft Silverlight 5.1... 51 %

4.5.2. The Main Interface

The virtual desktop allows you to switch between two display modes:

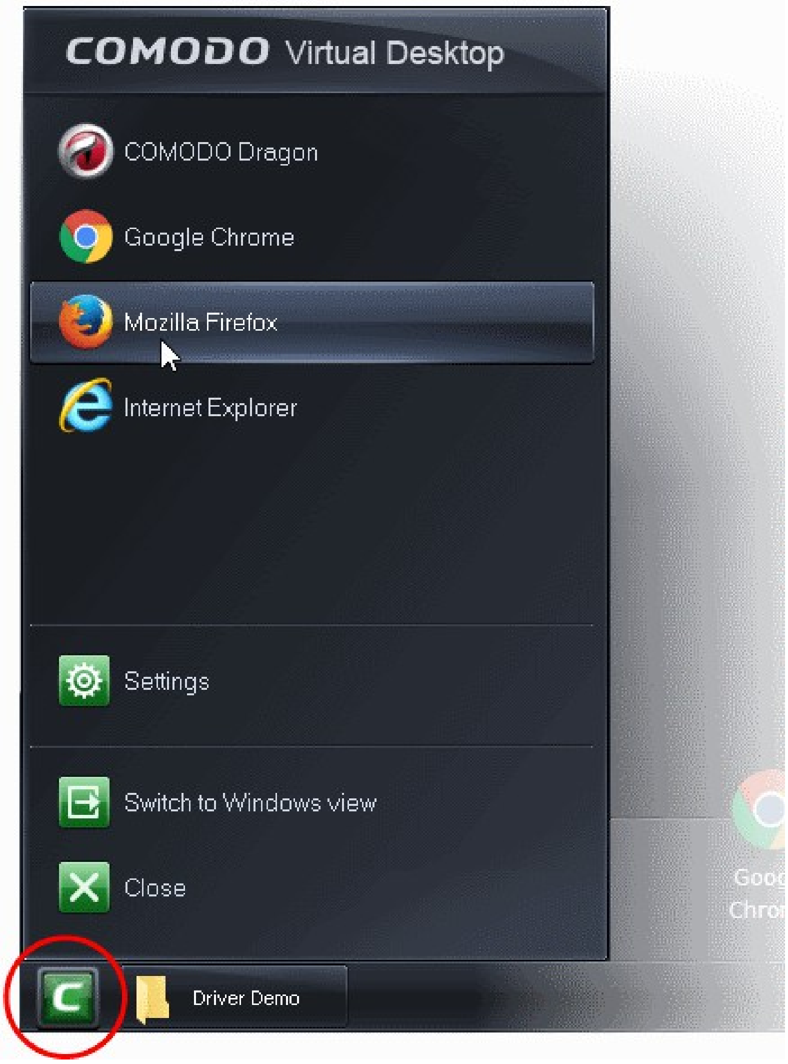
- **Classic Windows style Desktop mode**
- **Tablet mode**

You can switch between these two modes by clicking the 'C' button at bottom-left then 'Settings' (**C Button > Settings > 'Mode' tab**). See **table below** for a comparison of different modes of the Virtual Desktop main interface.



In 'Classic' mode,

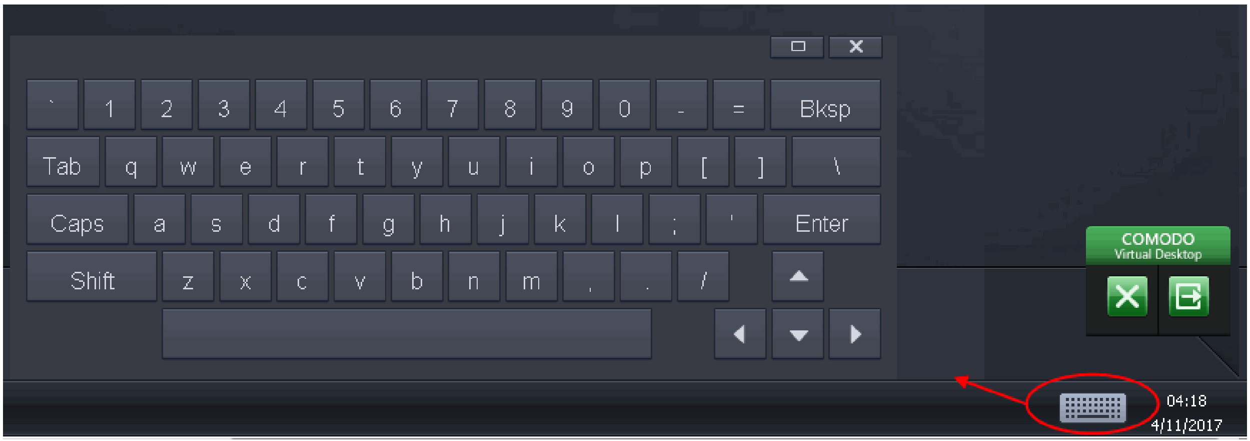
- All items on your real desktop are displayed. Clicking the shortcuts on the Virtual Desktop will run the program or file inside the virtual computer system.
- Clicking the 'C' button at bottom-left will open a Windows-style 'Start Menu'.



The start menu allows you to:

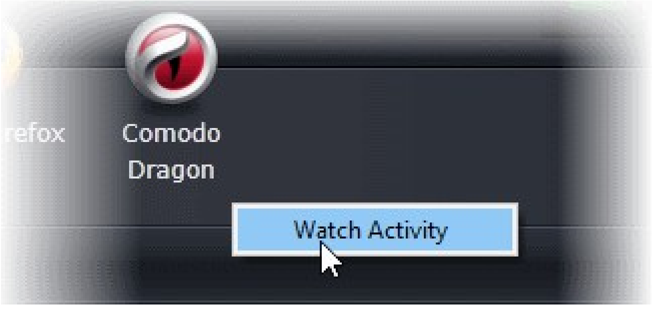
- Run browsers that are installed on your system. See **Running Browsers inside the Virtual Desktop** for more details.
- Configure the Virtual Desktop by clicking 'Settings'. See **Configuring the Virtual Desktop** for more details.

- Clicking the keyboard icon on the system tray opens a virtual keyboard that can be used to input confidential data like website user-names, passwords and credit card numbers. The keyboard can also be used with touch screen displays.


` 1 2 3 4 5 6 7 8 9 0 - = Bksp
Tab q w e r t y u i o p [ ] \
Caps a s d f g h j k l ; ' Enter
Shift z x c v b n m , . /
COMODO Virtual Desktop
04:18
4/11/2017

- Clicking the 'Volume Control' icon at the system tray enables you to control the system volume.
- Right-clicking on the task bar and selecting 'Watch Activity' opens the 'Windows Task Manager' to view your

computer's performance, close unresponsive programs and to troubleshoot problems with Windows.



Tablet Mode

To switch to 'Tablet' mode from 'Classic' mode, click the 'C' button at bottom left followed by Settings > Mode and select 'Tablet Mode'.

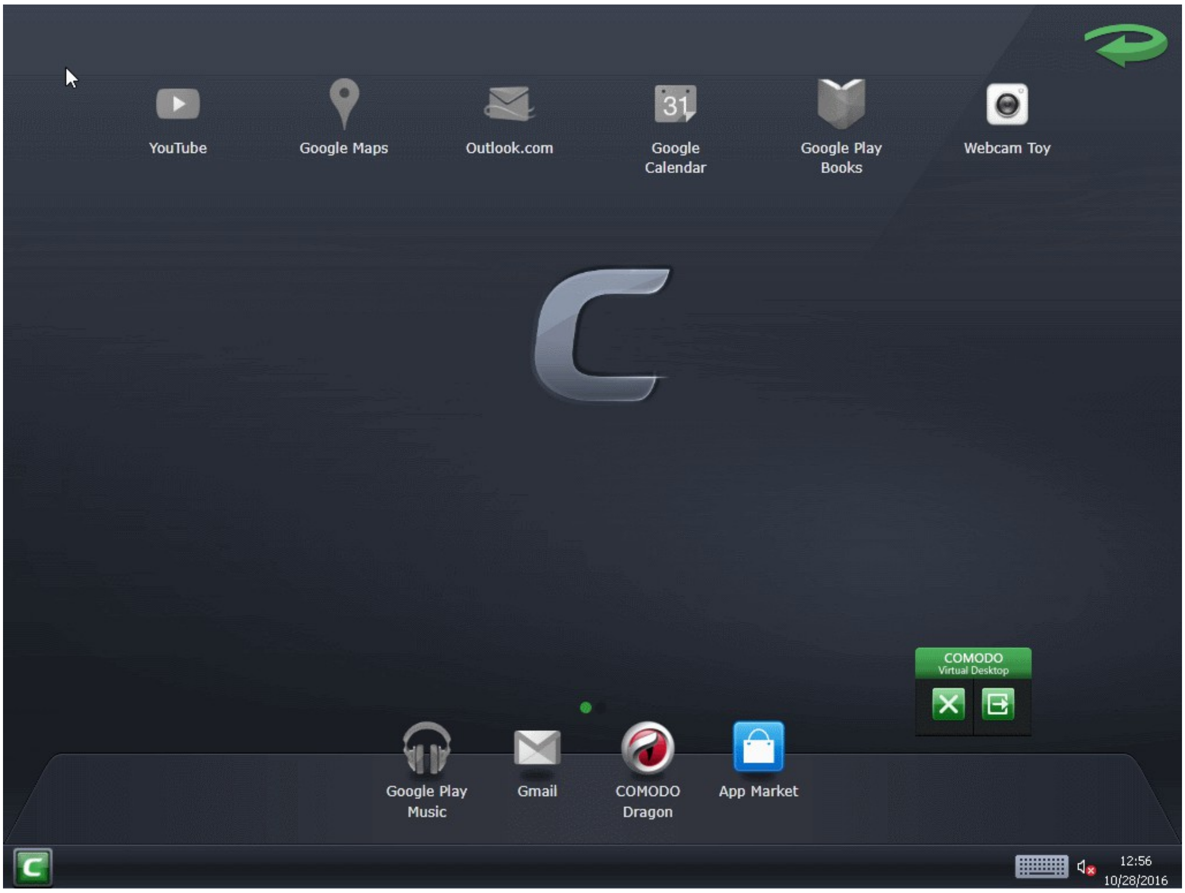
There are two variations of this mode:

1. Mode A - Pure Tablet device - A touch-screen interface that will be familiar to users of modern smart devices. The home page displays a set of popular apps covering games, social media and networking. You can, of course, install your own apps from the app market.
    - To install your own apps, click the App Market icon from the launch bar. You will be taken to **https://chrome.google.com/webstore/category/home?utm_source=COMODO-Kiosk**. Select the apps you want to install from the web-store.
2. Mode B - Tablet device + Windows - The home page displays the desktop items from your real system. The task bar from classic mode is present along with the 'C' button and the virtual keyboard. The launch strip will display all installed browsers.

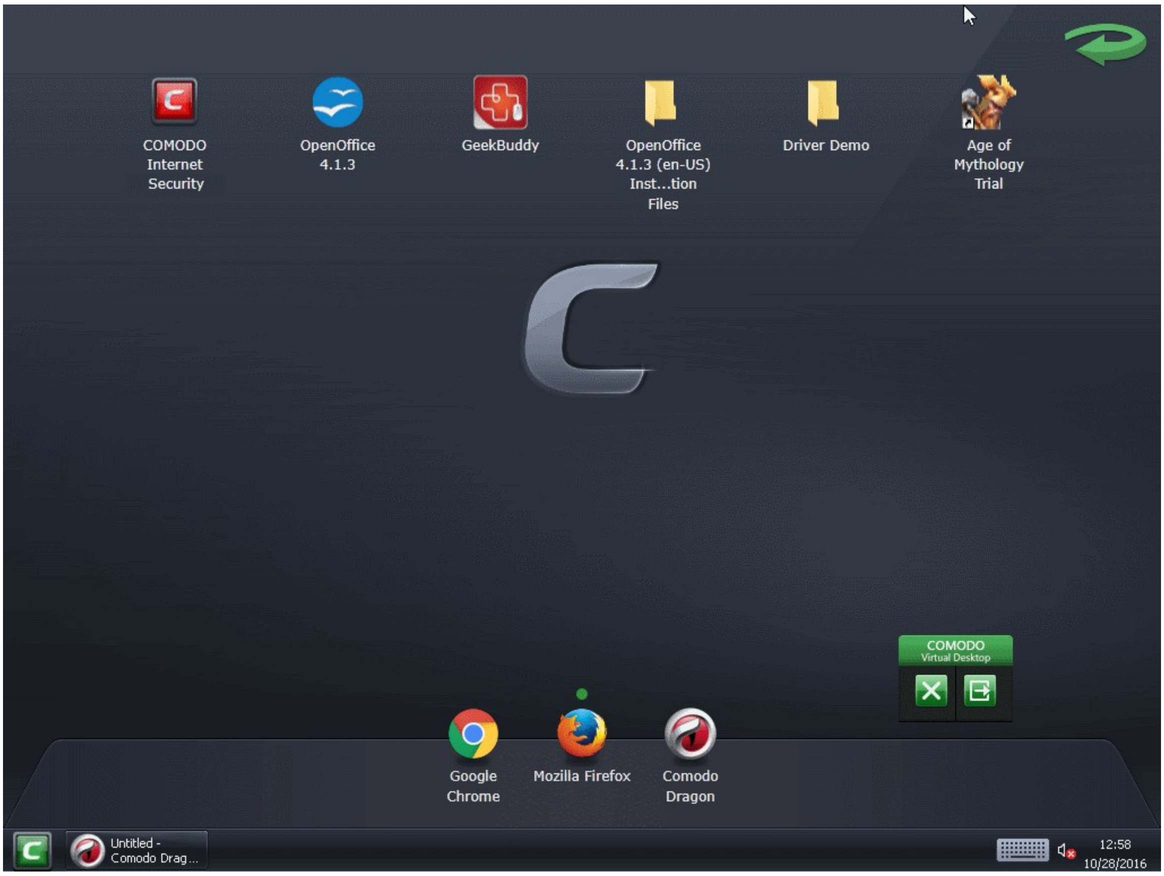
You can swap between the two modes by clicking the curved arrow ↻ at the top right:

You can swipe the home screen in both left and right directions to navigate between successive home pages.

Tablet Mode A - Pure Tablet



Tablet Mode B - Tablet + Windows



The following table gives a comparison of the two modes:

Classic Mode	Mode A - Pure Tablet	Mode B - Tablet + Windows
Windows desktop style interface.	Tablet style interface.	Tablet style interface.
Your real desktop shortcuts and files are displayed	Shortcut icons of the apps installed on the tablet are displayed	Your real desktop shortcuts and files are displayed
Shortcuts and files are laid out vertically as they would be on a Windows desktop	Shortcuts are laid out horizontally	Shortcuts and files are laid out horizontally
No Launch Bar	Browser shortcuts are displayed on the launch bar at the bottom	Browser shortcuts are displayed on the launch bar at the bottom
Cannot have multiple home screens	Can have multiple home screens	Can have multiple home screens if you have many shortcuts and files
Cannot swipe the screen to move between home screens	Can swipe the screen to move between home screens	Can swipe the screen to move between home screens

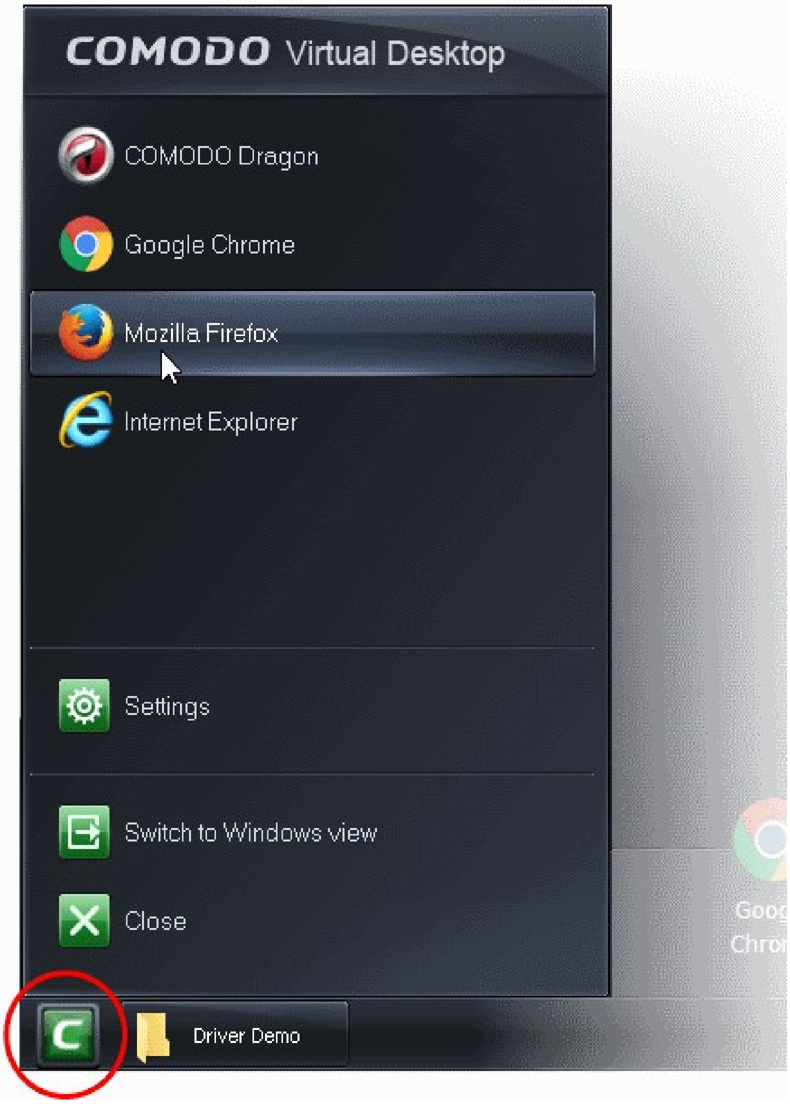
4.5.3. Running Browsers Inside the Virtual Desktop

- The Virtual Desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer.
- Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer.
- Surfing the internet from inside the virtual desktop removes this threat by preventing websites from installing applications on your real computer.
- Further,more the Virtual Keyboard allows you to securely enter your user-names and passwords without fear of key-loggers recording your keystrokes.

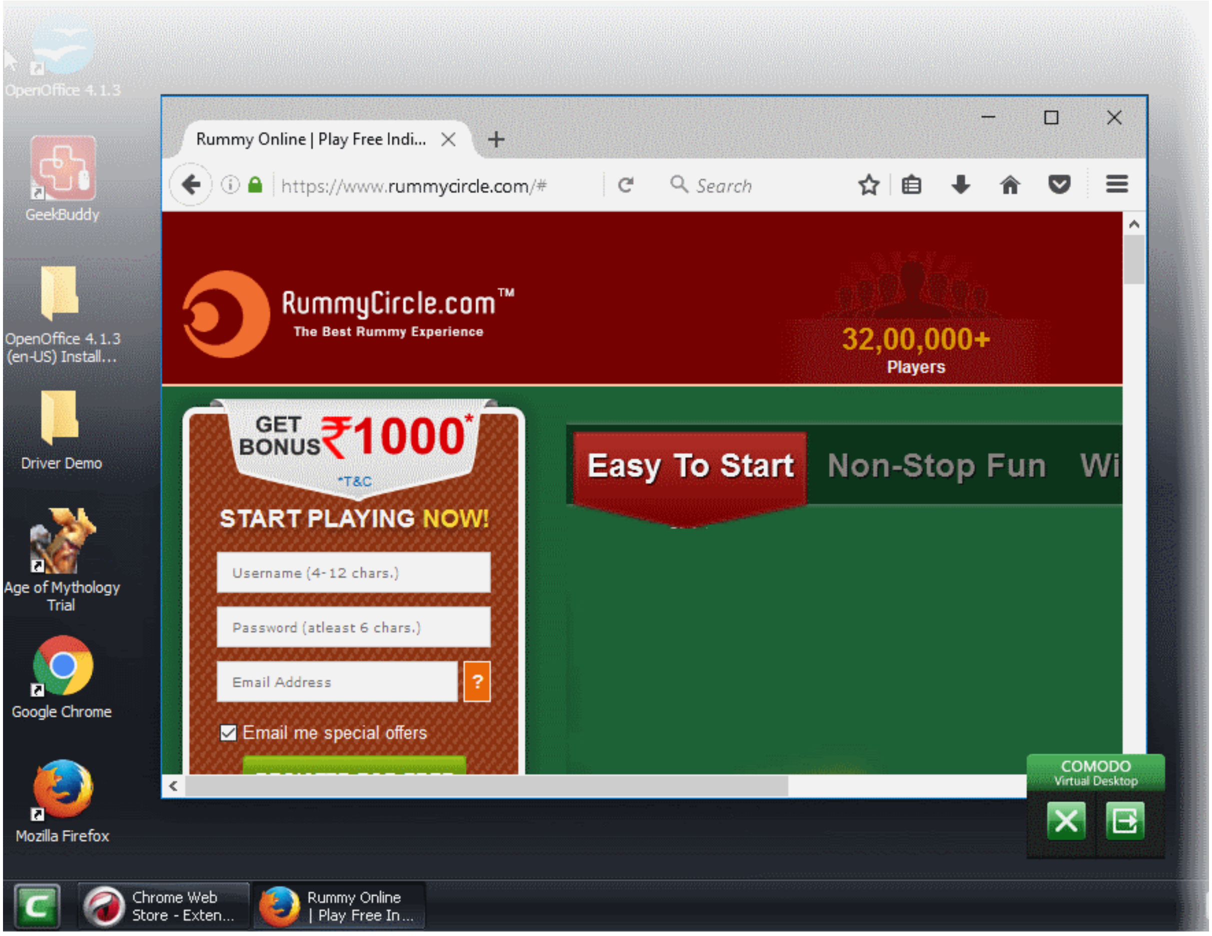
Tip: For visiting important shopping or banking websites, we recommend you use the Secure Shopping environment instead. Whereas the Virtual Desktop protects your computer by stopping threats from getting out of the container, Secure Shopping protects applications inside the container by stopping any threats on your computer from getting in. Secure Shopping hides your browsing sessions from the rest of your computer and provides a range of other online protections. See **Secure Shopping** for more details.

To run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left
2. Select the browser you want to run:



Your choice of browser will open inside the virtual desktop, ready for secure surfing:



Browsing history and other records of your internet activity will not be stored on your computer when your session is closed.

4.5.4. Opening Files and Running Applications inside the Virtual Desktop

Applications installed or the files stored in your system can be opened inside the Virtual Desktop by the following methods:

- **Opening the applications/files from the desktop shortcuts**
- **Sharing the application/files through the Shared Space folder**

Desktop Shortcuts

You can copy the files or create shortcuts for the applications/files to be opened in Virtual Desktop, in the desktop of your real system. The shortcuts of your real desktop will be available in the Virtual Desktop. You can double click on the icon to open the respective application of file inside the Virtual Desktop.

Note: The real computer desktop icons will be available only in the '**Classic Windows Mode**' and '**Tablet + Classic Mode**'.

Shared Space

The Virtual Desktop creates a folder Shared Space in the location "C:\ProgramData\Shared Space". The 'Shared Space' folder can be shared by your host operating system and the Virtual Desktop.

The Shared Space can be accessed in the following ways:

- Click 'Open Shared Space' under 'Containment Task' in the 'Tasks' interface
- Click the 'Shared Space' shortcut icon from the home screen of CIS

- Click the 'Shared Space' shortcut icon from the CIS widget

To open an application or file from your host system in the Virtual Desktop

1. Open the 'Shared Space' as mentioned above
2. Copy/Move the application or the file to be opened into the Shared Space
3. Start 'Virtual Desktop'
4. Open 'Shared Space' inside the 'Virtual Desktop' by clicking the 'Shared Space' icon in the home screen.

> **Note**: The Shared space home screen icon will be available only in the '**Classic Windows Mode**' and '**Tablet + Classic Mode**'.

5. Double click on the application/file in the shared space to open it inside the 'Virtual Desktop'.

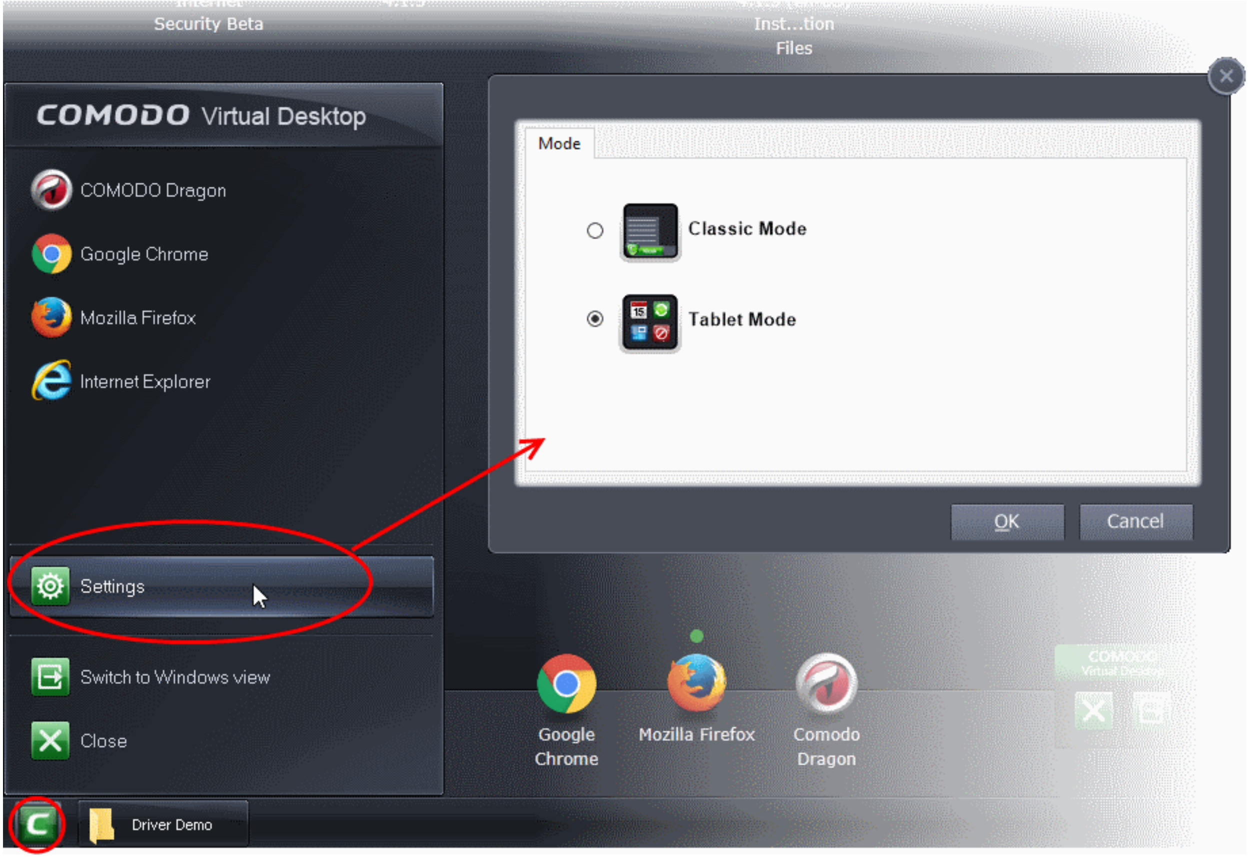
The changes you make to the file will be stored to the file only inside the 'Virtual Desktop' and not in the real computer system.

4.5.5. Configuring the Virtual Desktop

The settings panel allows you to specify the 'Virtual Desktop' operational mode and to modify its look and feel.

To open the settings panel:

1. Click the 'C' button at bottom left.
2. Select 'Settings' from the start menu. The Settings panel will open.



Mode: ○ Classic Mode ● Tablet Mode

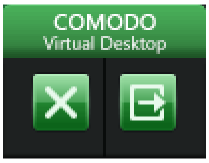
The Settings panel has 'Mode' tab:

- **Mode -** Allows you to select the display mode of the Virtual Desktop between Classic Windows mode and Tablet Mode (Default)

3. Click OK for your settings to take effect

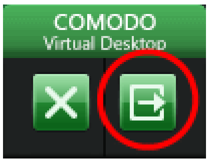
4.5.6. Closing the Virtual Desktop

The shortcuts at the bottom right of the Virtual Desktop, allow you to temporarily switch to your real computer system, if you plan to continue using the virtual desktop at a later time, or to fully exit the Virtual Desktop.



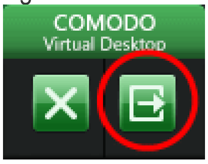
To temporarily switch to your real Windows system

- Click the right button from the shortcuts pane at the bottom right



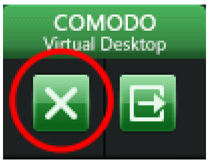
- Alternatively, click the 'C' button at bottom left and choose 'Switch to Windows View' from the Virtual Desktop Start Menu.

The 'Virtual Desktop' will be temporarily closed. You can quickly return to it by clicking the right switch from the 'Virtual Desktop' shortcut buttons displayed at the bottom right of your Windows Desktop or by clicking 'Run Virtual Desktop' from the 'Containment Tasks' interface.



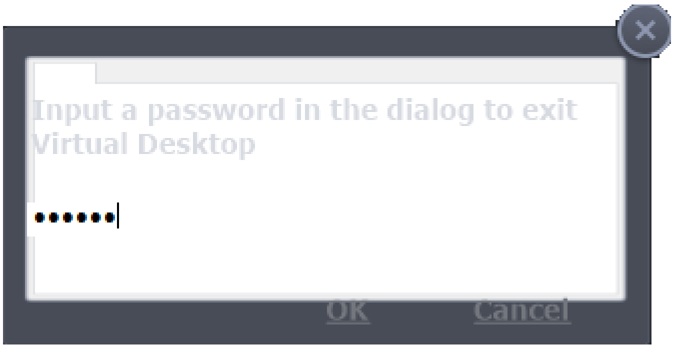
To close the Virtual Desktop

- Click the X button from the Virtual Desktop shortcuts pane at the bottom right



- Alternatively, click the 'C' button at bottom left and choose 'Exit' from the 'Virtual Desktop' Start Menu.

In either case, if password protection is enabled under Settings > Containment > Containment Settings, you will be prompted to enter the password. Else the Virtual Desktop will be closed.



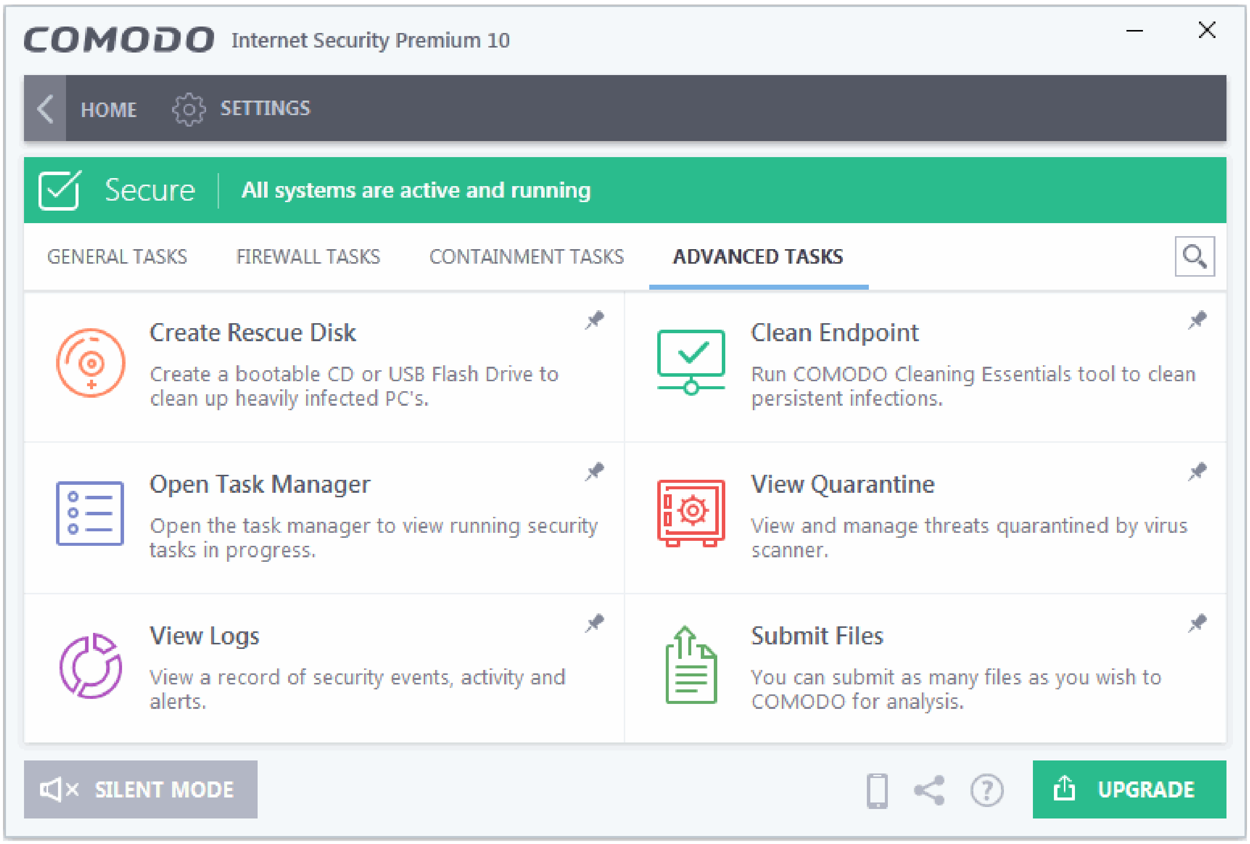
Input a password in the dialog to exit Virtual Desktop

••••••

- Enter the password and click 'OK'.

5. Advanced Tasks - Introduction

The 'Advanced' tasks area allows you to manage quarantined items, view event logs, submit files to Comodo for analysis, manage CIS tasks and to take advantage of several other Comodo utilities.



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Open Task Manager
Open the task manager to view running security tasks in progress.

View Quarantine
View and manage threats quarantined by virus scanner.

View Logs
View a record of security events, activity and alerts.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

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

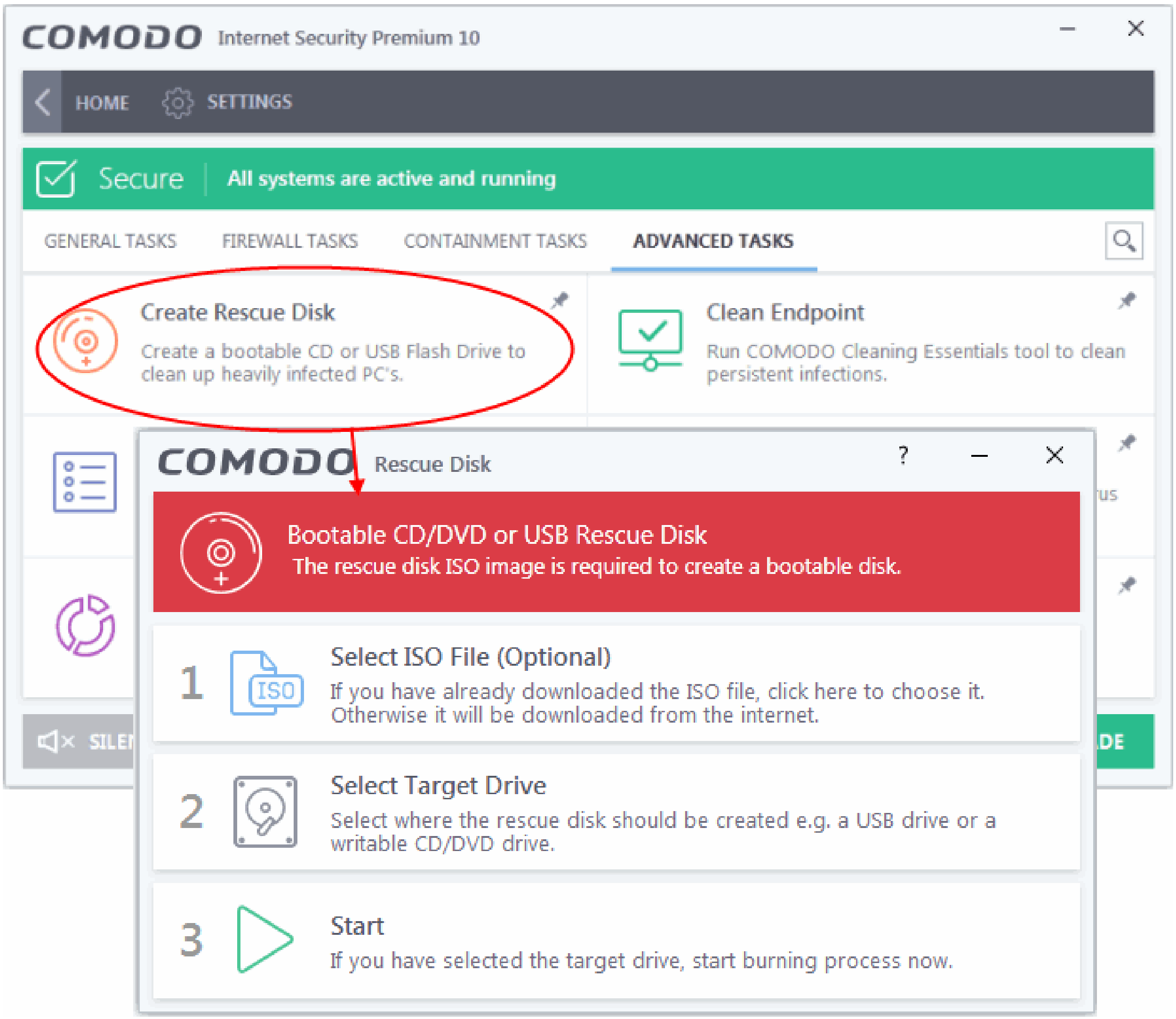
- **Create Rescue Disk - Burn a bootable ISO that lets you run virus scans in pre-boot environments**
- **Clean Endpoint - Deploy Comodo Cleaning Essentials to eradicate persistent infections from your PC**
- **Task Manager - Manage priorities of currently running CIS tasks like Antivirus scans and updates**
- **Quarantined Items - Manage files that are quarantined by the virus scanner or quarantined manually**
- **CIS Logs - View tevent logs of Firewall, Antivirus, Containment and HIPS modules**
- **Submit Files - Submit unknown/suspicious files to Comodo for analysis**

5.1. Create a Rescue Disk

Comodo Rescue Disk (CRD) is a bootable disk image that allows users to run virus scans in a pre-boot environment (before Windows loads). CRD runs Comodo Cleaning Essentials on a lightweight distribution of the Linux operating system. It is a powerful virus, spyware and root-kit cleaner which works in both GUI and text mode.

- CRD can eliminate infections that are preventing Windows from booting in the first place.
- It is useful for removing malware which has embedded itself so deeply that regular AV software cannot remove it.
- CRD contains tools to explore files in your hard drive, take screen-shots and browse web pages.
- Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk' to download and burn the CRD ISO to a CD/DVD,

USB or other drive. See **Downloading and Burning Comodo Rescue Disk** for a walk-through of this process.

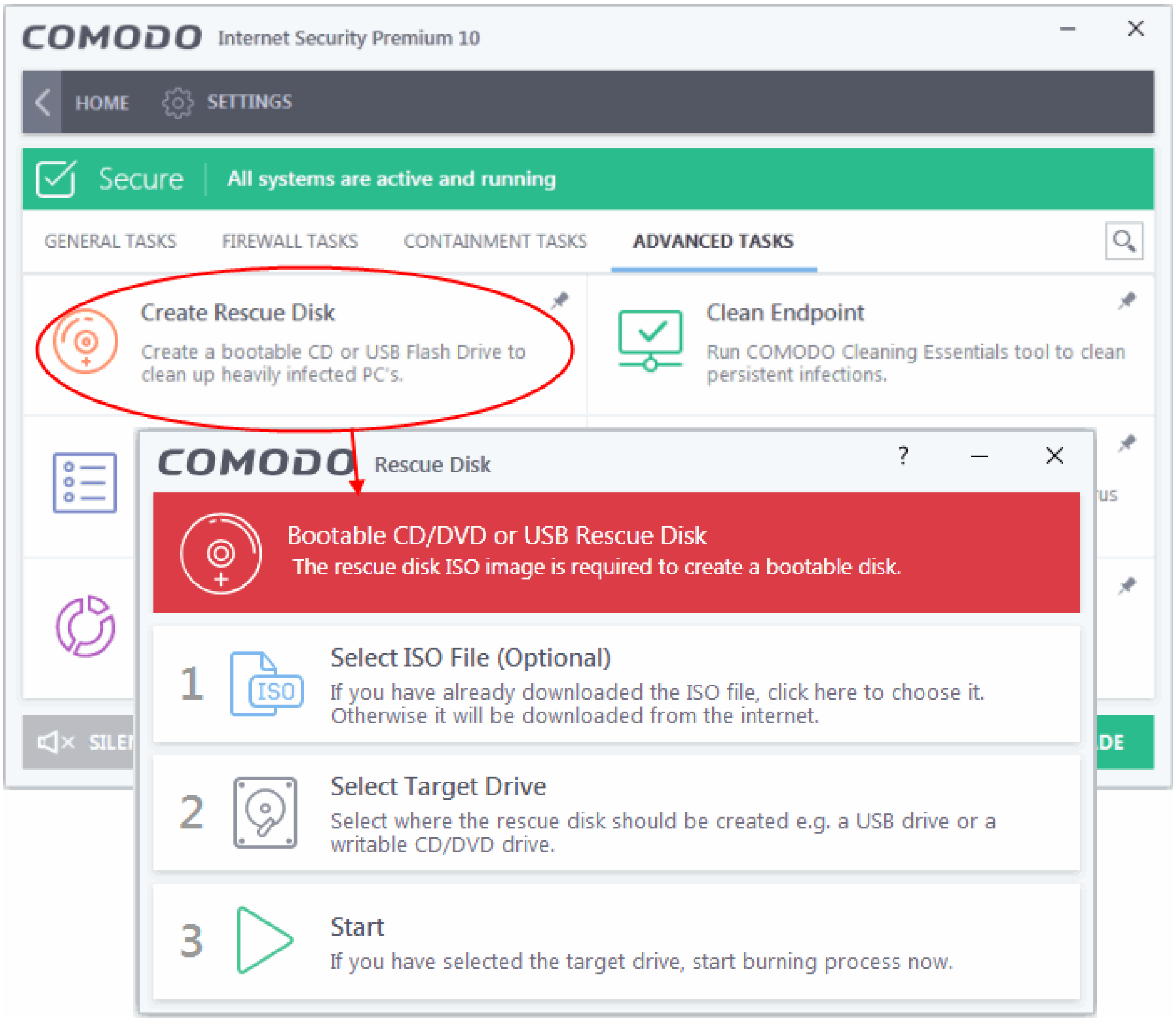

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
COMODO Rescue Disk
Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.
1
Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the internet.
2
Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.
3
Start
If you have selected the target drive, start burning process now.

After you have burned the ISO, you need to boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

- How to change the boot order on your computer - **http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html**
- How to start using CRD - **http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html**
- How to run scans on your pre-boot environment - **http://help.comodo.com/topic-170-1-493-5216-Starting-Comodo-Cleaning-Essentials.html** and **http://help.comodo.com/topic-170-1-493-5217-CCE-Interface.html**

5.1.1. Download and Burn Comodo Rescue Disk

To get started, click 'Create Rescue Disk' in the 'Advanced' tasks interface to open the rescue disk wizard:



COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
SILEI
DE
COMODO Rescue Disk
Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.
1
Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the internet.
2
Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.
3
Start
If you have selected the target drive, start burning process now.

The wizard lists the steps to create a new rescue disk on a CD/DVD or USB drive:

Step 1- Select the ISO file

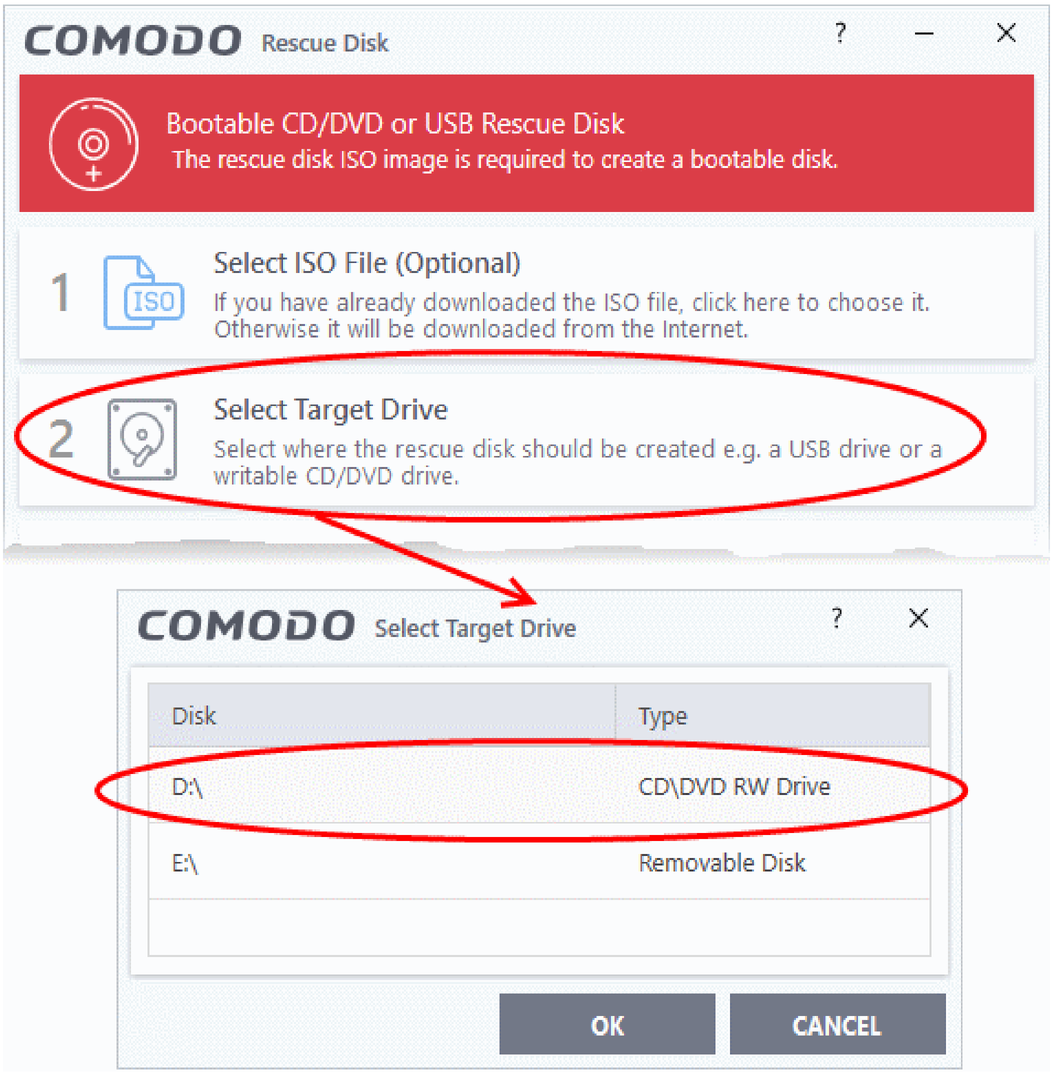
Optional. If you have already downloaded the rescue disk ISO from Comodo then browse to the location on your hard-drive where it is stored and select it. If you haven't downloaded the ISO then ignore this step. It will be downloaded automatically prior to execution of Step 3 - Burning the Rescue Disk.

Step 2 Select target drive

This step allows you to select the CD/DVD or USB on which you want to burn the rescue disk.

To burn the Rescue disk to a CD or a DVD

- Label a blank CD or DVD as "Comodo Rescue Disk - Bootable" and load it to the CD/DVD drive in your system
- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the 'Select Disk' dialog



COMODO Rescue Disk

Bootable CD/DVD or USB Rescue Disk

The rescue disk ISO image is required to create a bootable disk.

1 Select ISO File (Optional)

If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.

2 Select Target Drive

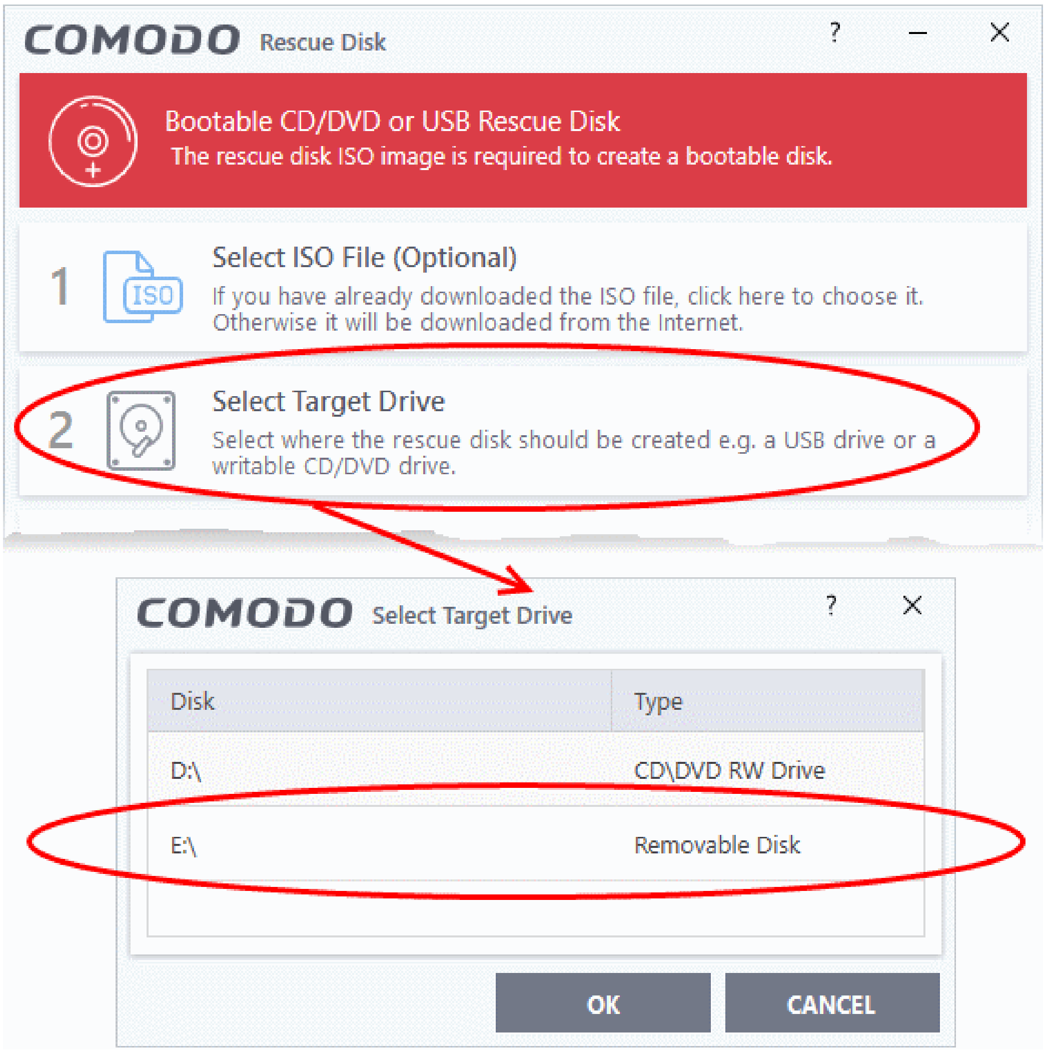
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.

COMODO Select Target Drive

Disk	Type
D:\	CD\DVD RW Drive
E:\	Removable Disk

To burn the Rescue disk on a USB Drive

- Insert a formatted USB memory to a free USB port on your computer
- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the Select Disk dialog



COMODO Rescue Disk

Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.

1 Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.

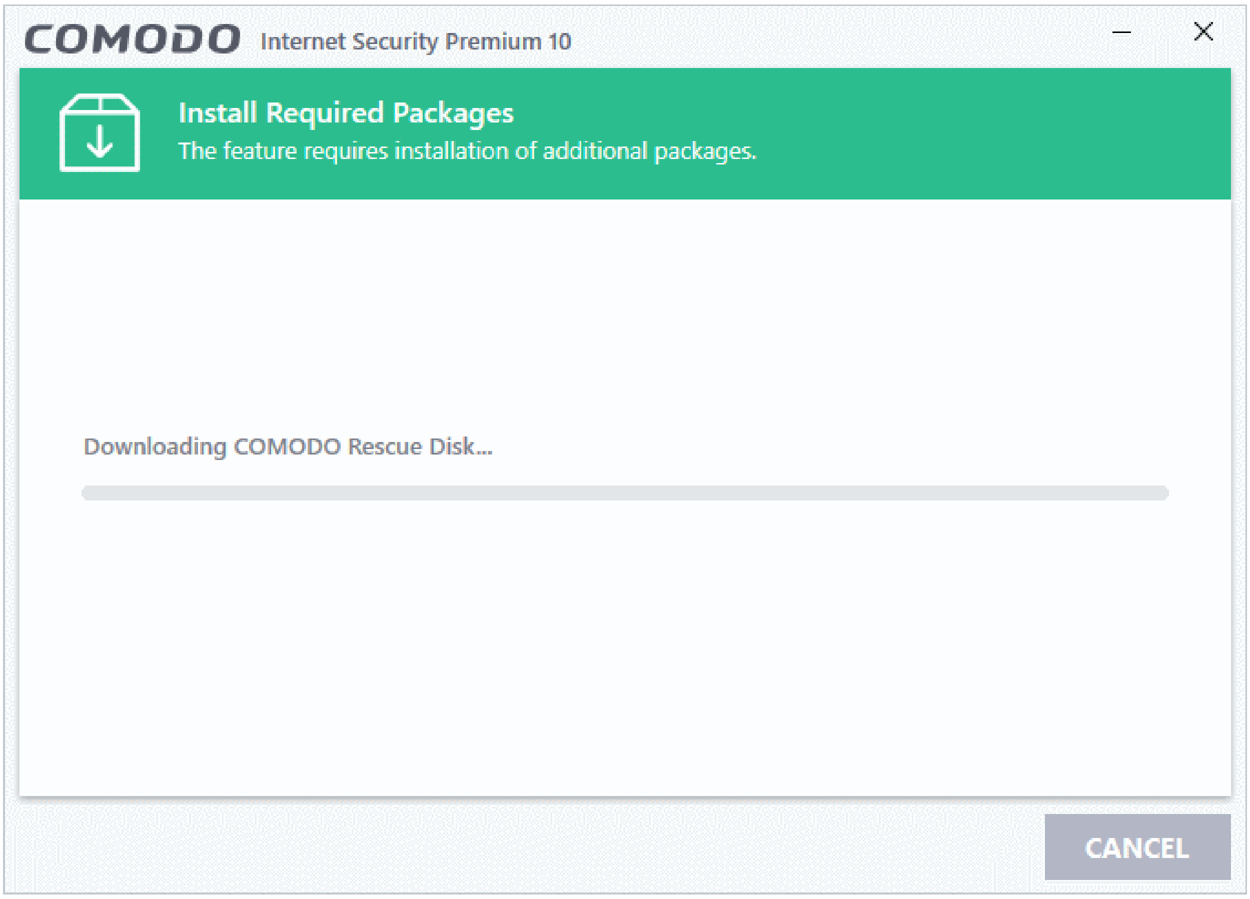
2 Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.

COMODO Select Target Drive

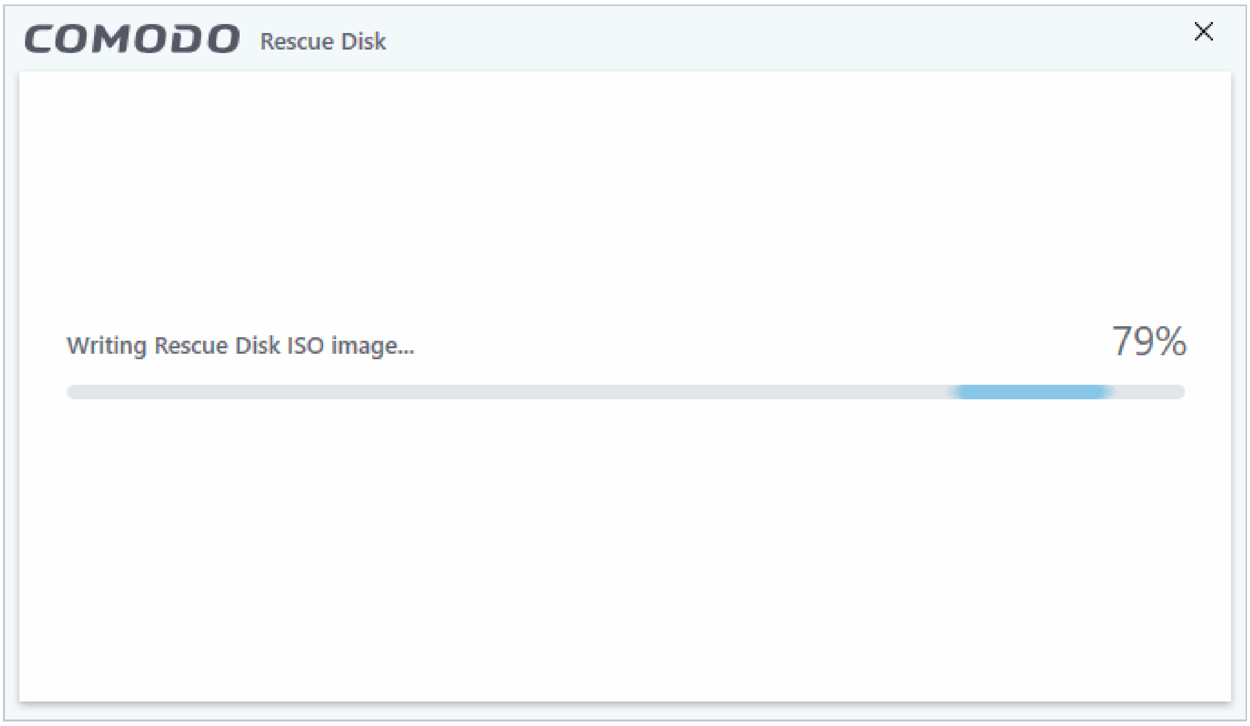
Disk	Type
D:\	CD\DVD RW Drive
E:\	Removable Disk

Step 3 - Burn the Rescue Disk

- After you selected the target drive, click 'Start'. If you have selected an ISO on your hard drive then burning will start immediately. If not, the ISO will be downloaded from Comodo servers.

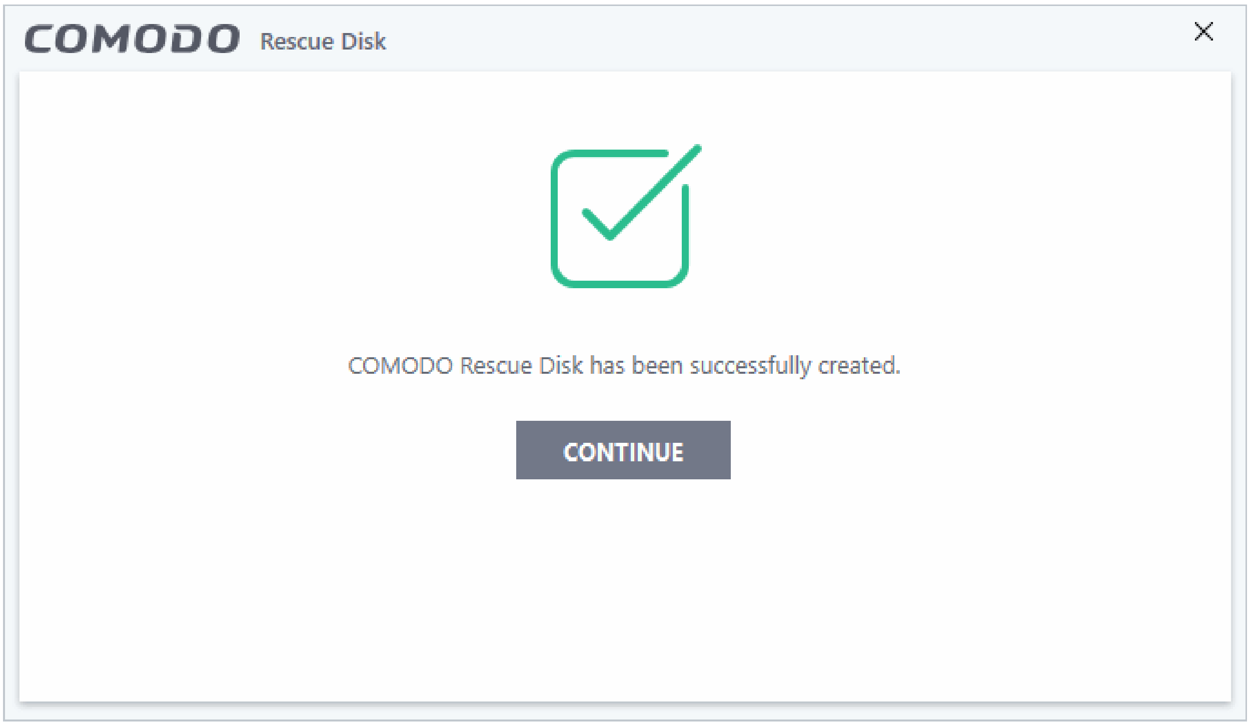

COMODO Internet Security Premium 10
Install Required Packages
The feature requires installation of additional packages.
Downloading COMODO Rescue Disk...
CANCEL

Once downloaded, the creation of rescue disk will start.



On completion, the files will be written on to the CD/DVD or the USB Drive.

- Wait until the write process is complete - do not eject the CD/DVD/USB drive early. The CD/DVD/USB will be ejected automatically once the burning process is finished.



COMODO Rescue Disk has been successfully created.

Your bootable Comodo Rescue Disk is ready.

- Click 'Continue' to go back to CIS interface.

5.2. Remove Deeply Hidden Malware

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

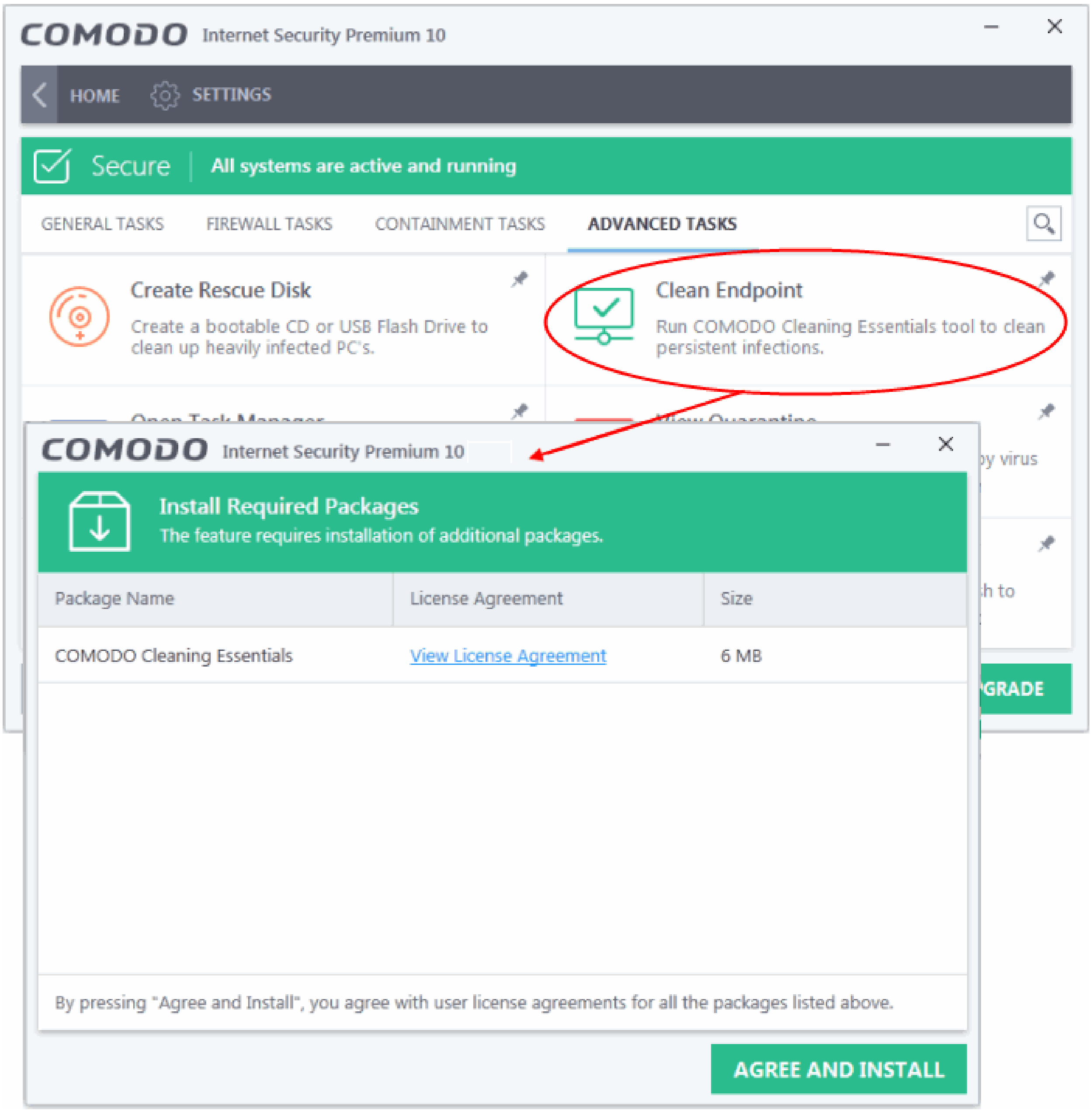
Major features include:

- **KillSwitch -** An advanced system monitoring tool that allows you to identify, monitor and stop unsafe processes that are running on your system.
- **Malware scanner -** Fully customizable scanner capable of unearthing and removing viruses, rootkits and malicious registry keys hidden deep in your system.
- **Autorun Analyzer -** Advanced utility which allows you to view and handle services and programs that are loaded when your system boots-up.

CCE enables home users to quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.

For more details on the features and usage of the application, please refer to the online guide at **http://help.comodo.com/topic-119-1-328-3516-Introduction-to-Comodo-Cleaning-Essentials.html**.

Comodo Cleaning Essentials can be directly accessed from the CIS interface by clicking the 'Clean Endpoint' button from the 'Advanced' tasks interface.


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
GRADE
COMODO Internet Security Premium 10
AGREE AND INSTALL

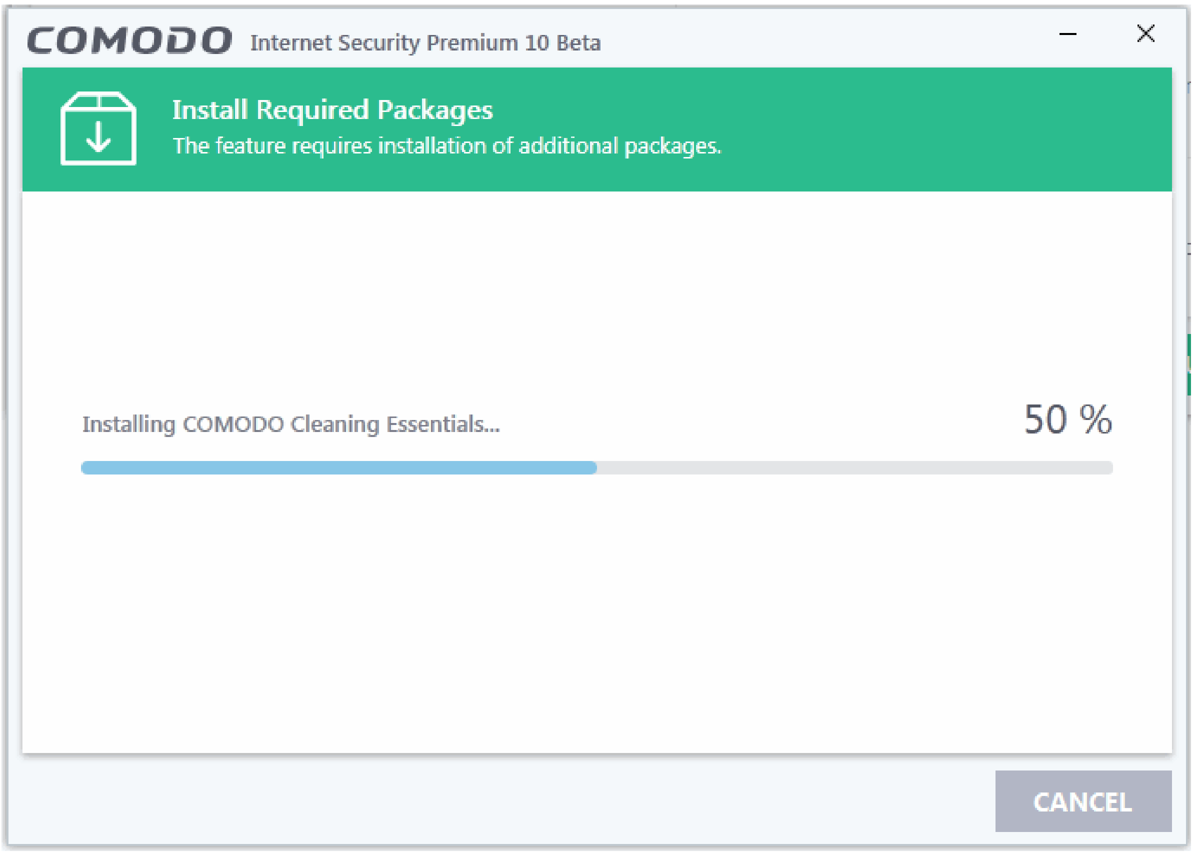
Install Required Packages

The feature requires installation of additional packages.

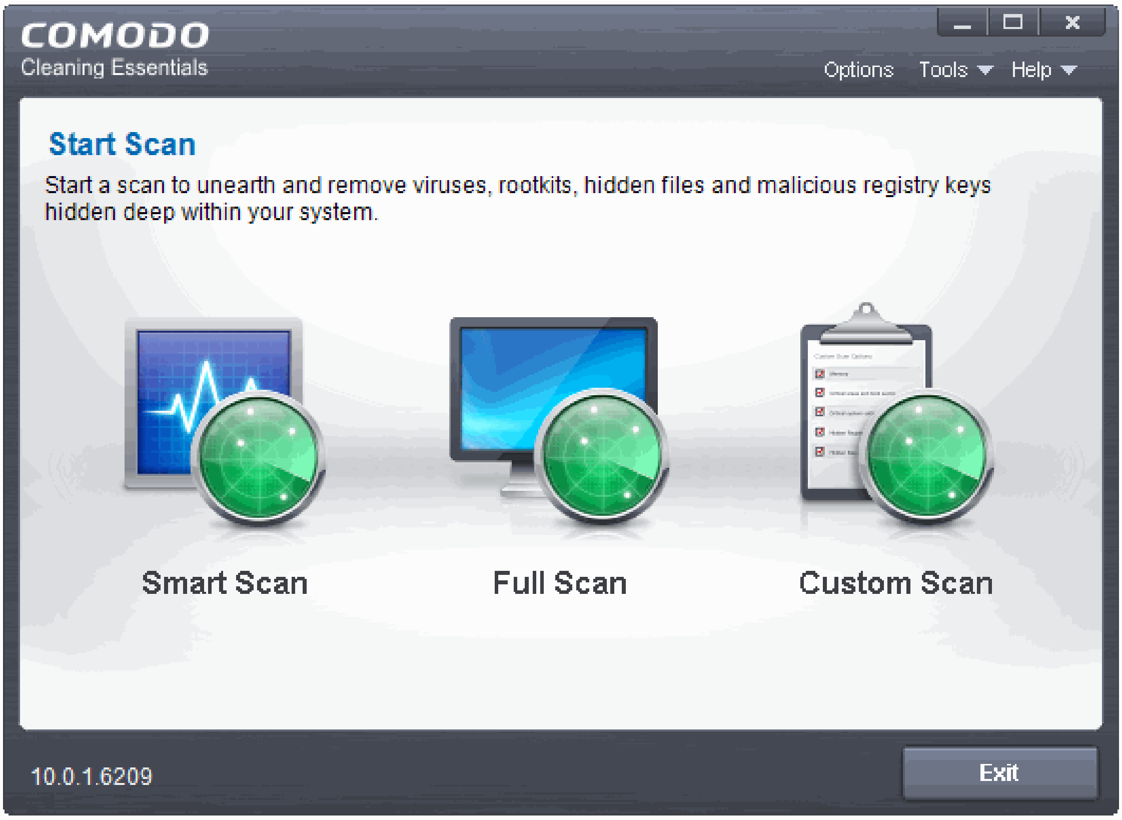
Package Name	License Agreement	Size
COMODO Cleaning Essentials	View License Agreement	6 MB

By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

- Clicking the 'Clean Endpoint' for the first time, CIS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.
- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.


COMODO Internet Security Premium 10 Beta
Install Required Packages
The feature requires installation of additional packages.
Installing COMODO Cleaning Essentials...
50 %
CANCEL

After installation, the Comodo Cleaning Essentials main interface will open:


COMODO
Cleaning Essentials
Options
Tools
Help
Start Scan
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.
Smart Scan
Full Scan
Custom Scan
10.0.1.6209
Exit

See **http://help.comodo.com/topic-119-1-328-3525-The-Main-Interface.html** if you'd like more information on using Comodo Cleaning Essentials.

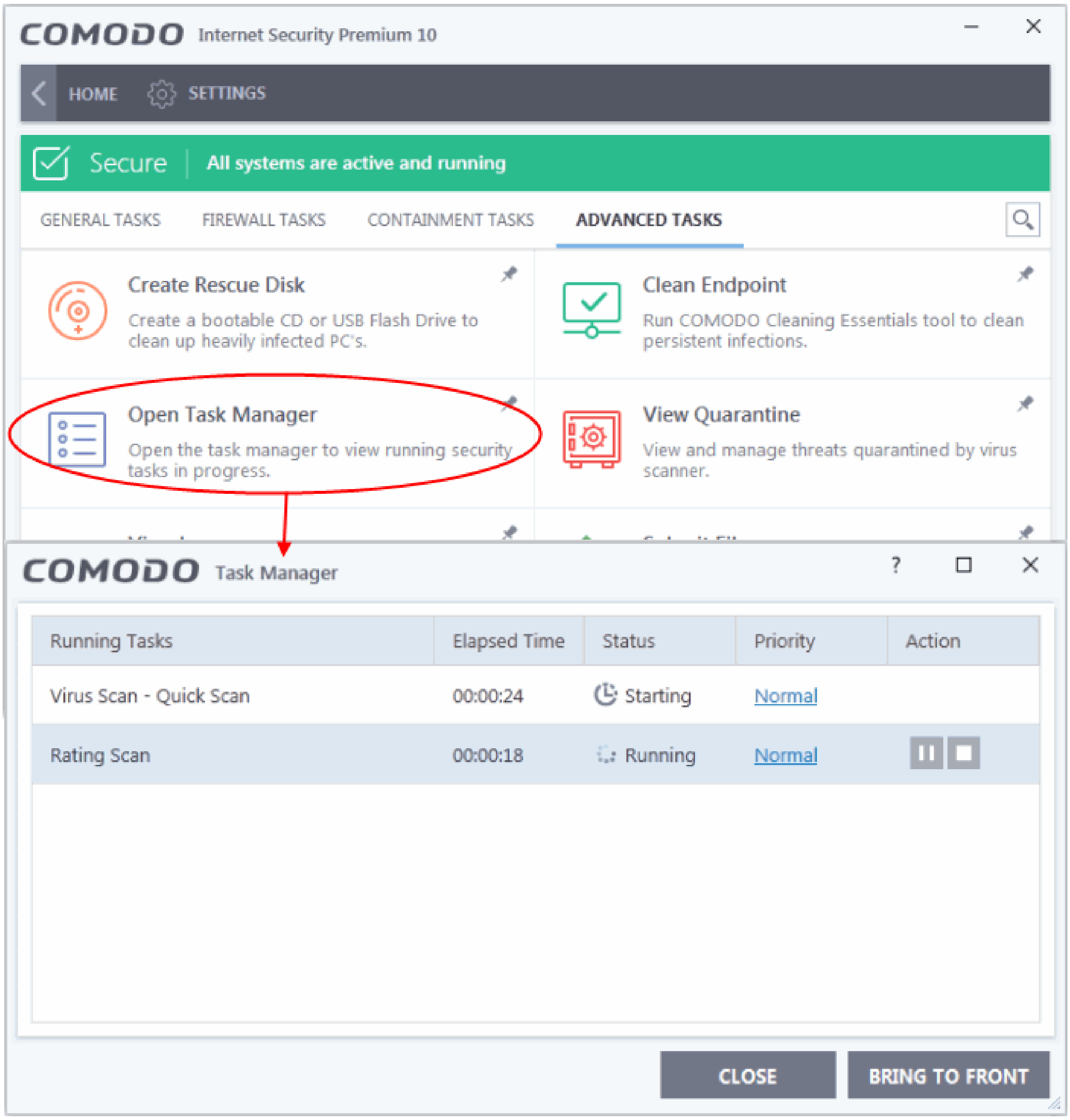
5.3. Manage CIS Tasks

Comodo Internet Security has the ability to run several tasks simultaneously. For example, virus scans and virus signature database updates can run concurrently. The 'Task Manager' interface lets you view all currently running tasks.

To open and manage the task manager

- Click 'Tasks' at the top left of the home screen
- Open the 'Advanced Tasks' tab and choose 'Open Task Manager'

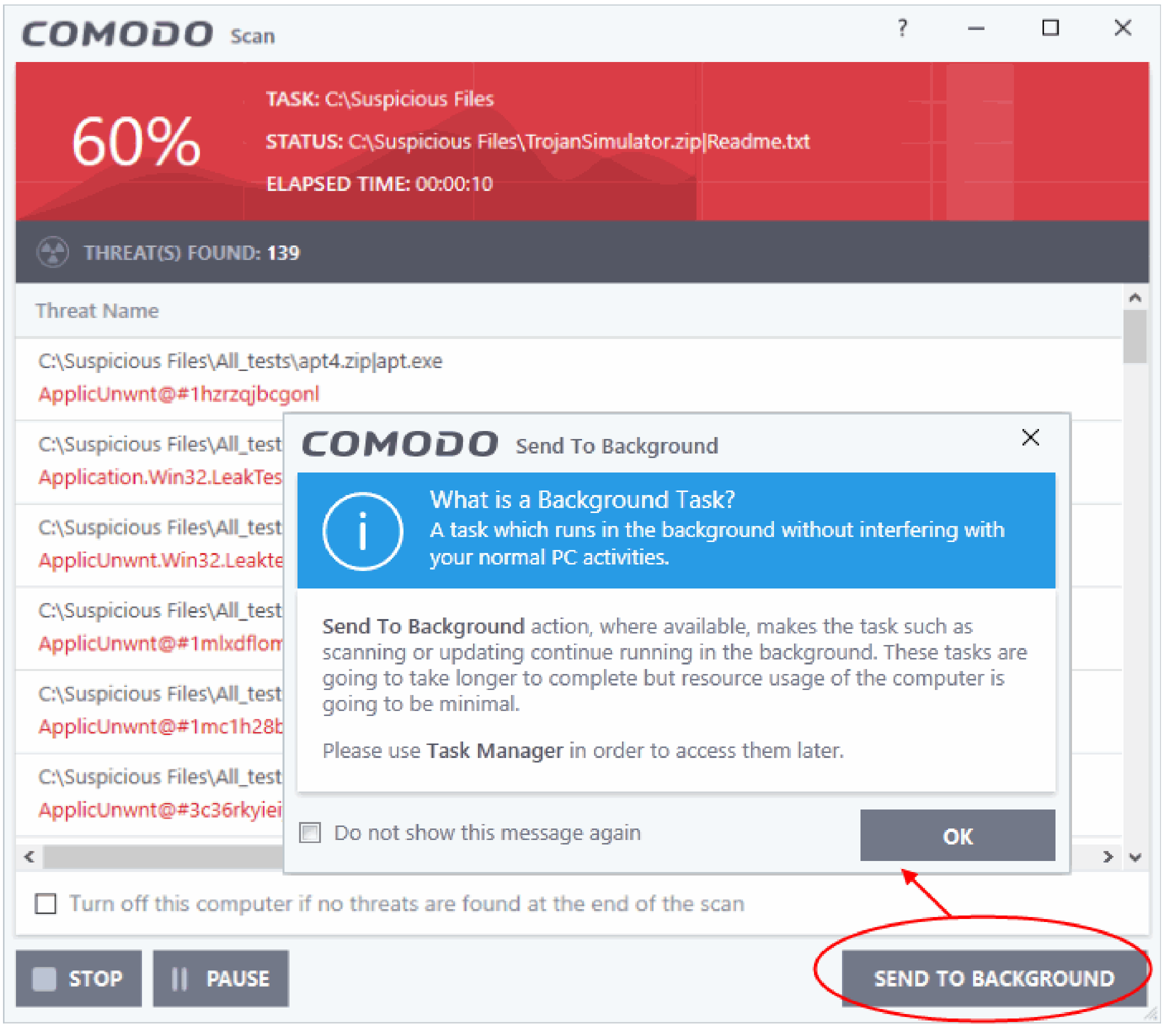
The 'Task Manager' dialog will open:


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Open Task Manager
Open the task manager to view running security tasks in progress.
View Quarantine
View and manage threats quarantined by virus scanner.
COMODO Task Manager
CLOSE
BRING TO FRONT

Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Quick Scan	00:00:24	Starting	Normal	
Rating Scan	00:00:18	Running	Normal	❚❚ ■

You can also open task manager by clicking the center tab in the 'Status' row of the the **widget**

Currently running tasks can be sent to the background by clicking the 'Send to Background' button:



COMODO Scan

60%

TASK: C:\Suspicious Files

STATUS: C:\Suspicious Files\TrojanSimulator.zip|Readme.txt

ELAPSED TIME: 00:00:10

THREAT(S) FOUND: 139

Threat Name
C:\Suspicious Files\All_tests\apt4.zip|apt.exe ApplicUnwnt@#1hzrzqjbcgonl
C:\Suspicious Files\All_test Application.Win32.LeakTes
C:\Suspicious Files\All_test ApplicUnwnt.Win32.Leakte
C:\Suspicious Files\All_test ApplicUnwnt@#1mlxdflom
C:\Suspicious Files\All_test ApplicUnwnt@#1mc1h28b
C:\Suspicious Files\All_test ApplicUnwnt@#3c36rkyiei

COMODO Send To Background

What is a Background Task?
A task which runs in the background without interfering with your normal PC activities.

Send To Background action, where available, makes the task such as scanning or updating continue running in the background. These tasks are going to take longer to complete but resource usage of the computer is going to be minimal.

Please use **Task Manager** in order to access them later.

□ Do not show this message again

OK

□ Turn off this computer if no threats are found at the end of the scan

From the Task Manager interface, you can:

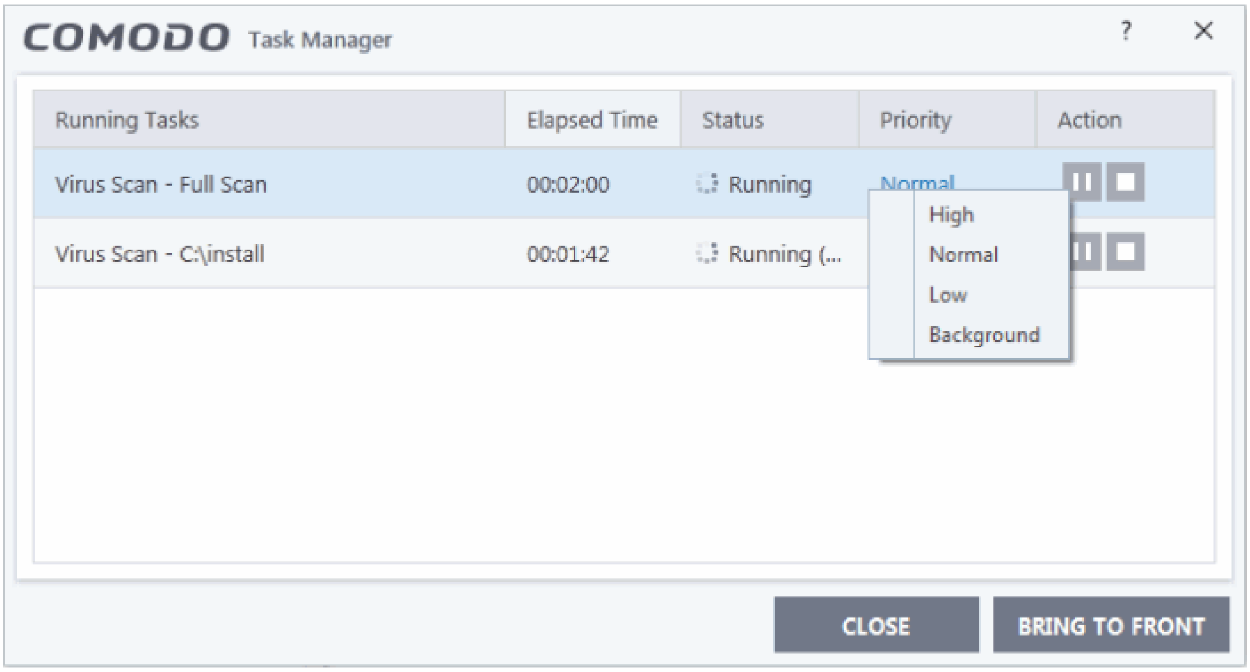
- Reassign priorities to the tasks
- Pause/Resume or Stop a running task
- Bring a selected task to foreground

Reassigning Priorities for a task:

The 'Priority' column in the 'Task Manager' interface displays the current priority assigned for each task.

To change the priority for a task

- Click on the current priority and select the priority you want to assign from the options.

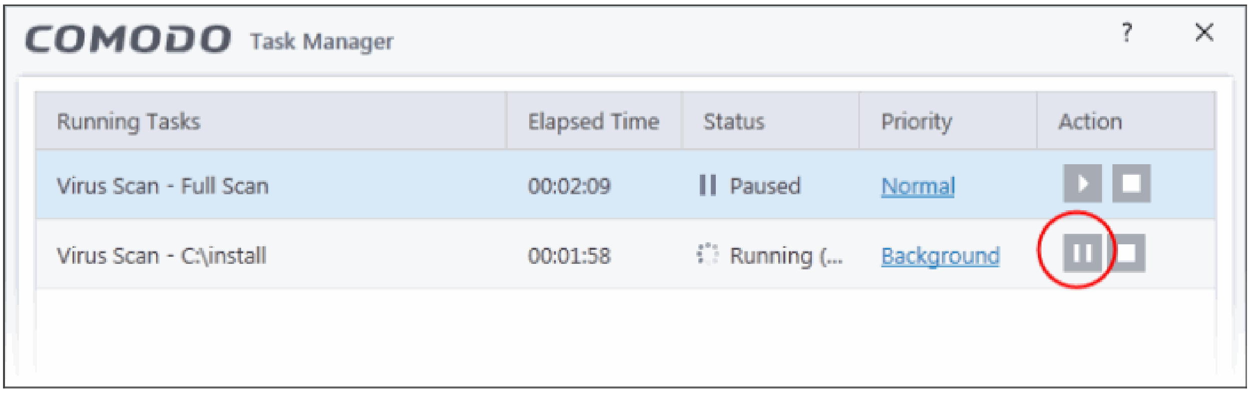


Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:00	Running	Normal	⏸ ⏹
Virus Scan - C:\install	00:01:42	Running (...		⏸ ⏹

Pausing/Resuming or Stopping running tasks

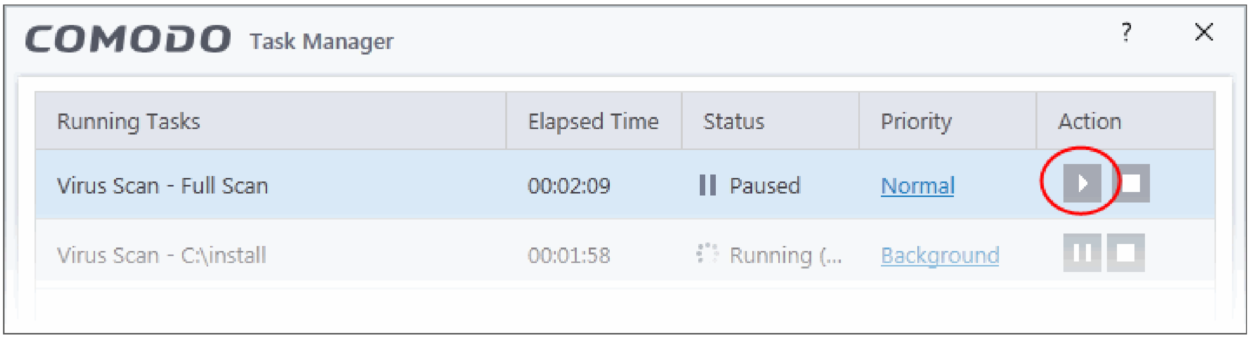
The 'Action' column displays the 'Pause' / 'Resume' and 'Stop' buttons

- To pause a running task, click the 'Pause' button



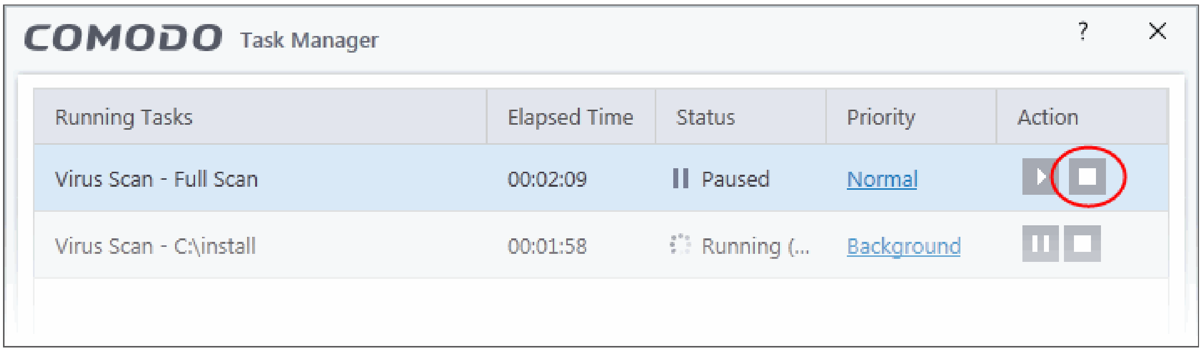
Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:09	Paused	Normal	▶ ⏹
Virus Scan - C:\install	00:01:58	Running (...	Background	⏸ ⏹

- To resume a paused task, click the 'Resume' button



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:09	Paused	Normal	▶ ⏹
Virus Scan - C:\install	00:01:58	Running (...	Background	⏸ ⏹

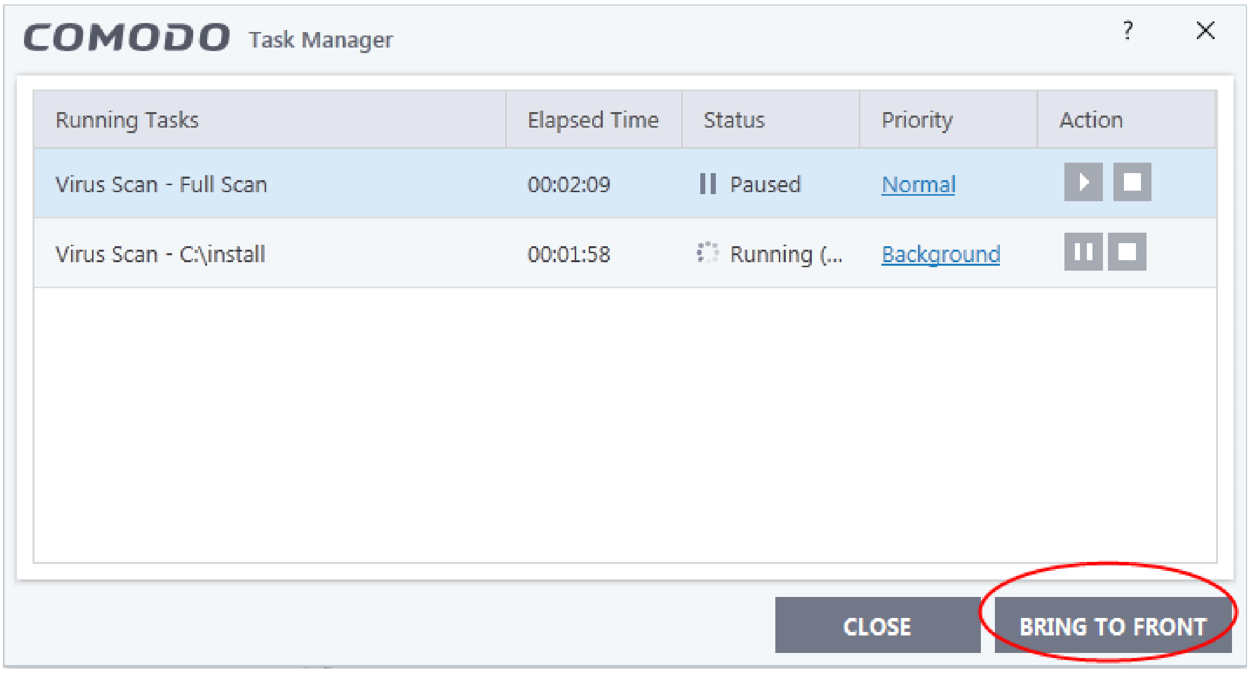
- To stop a running task, click the 'Stop' button



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:09	Paused	Normal	
Virus Scan - C:\install	00:01:58	Running (...	Background	

Bringing a running task to foreground

- To view the progress of a background task, select the task and click 'Bring to Front'



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:02:09	Paused	Normal	
Virus Scan - C:\install	00:01:58	Running (...	Background	

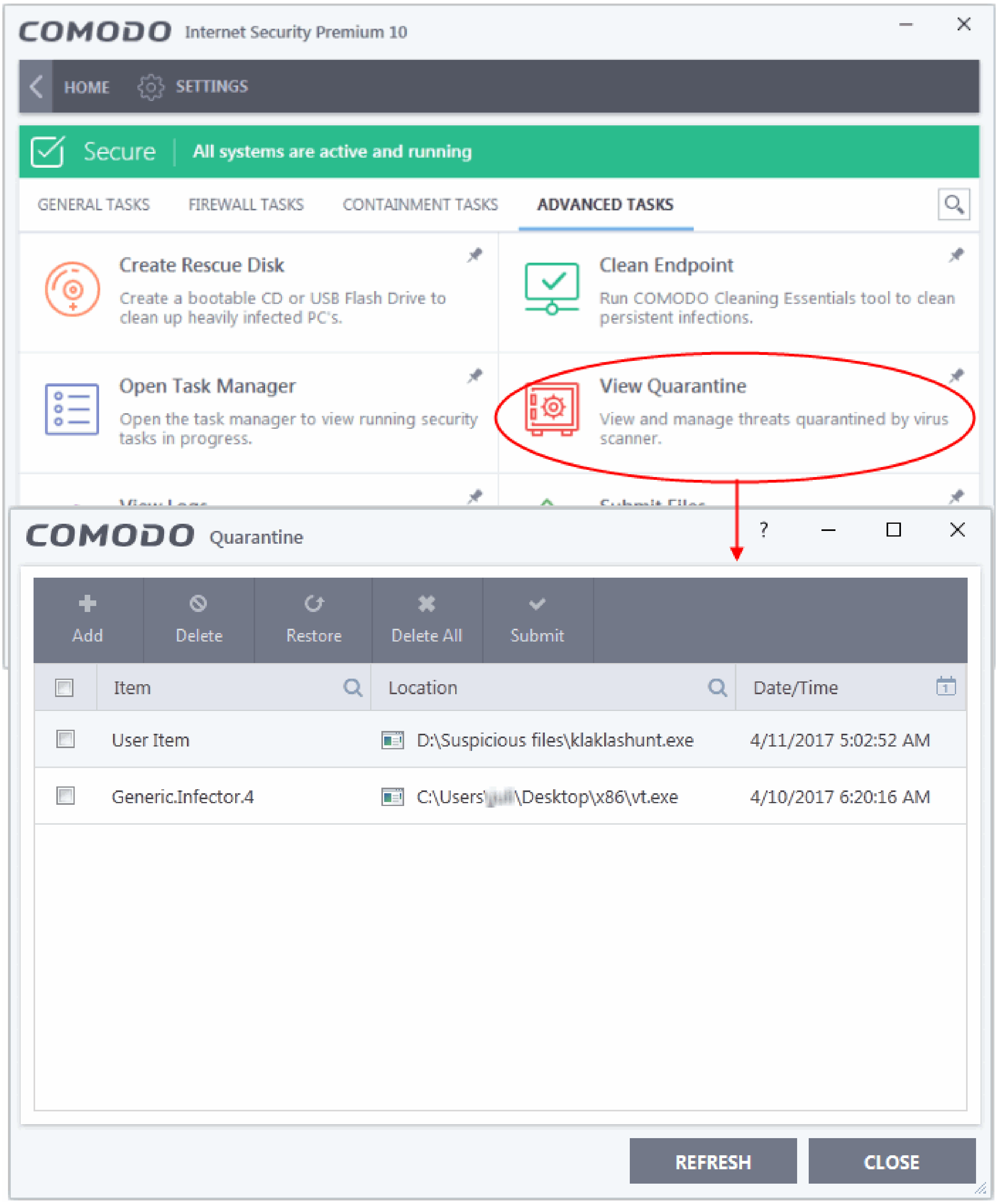
The progress window of the task will be displayed. If the task is completed, the results window will be displayed.

5.4. Manage Quarantined Items

The 'Quarantine' interface displays a list of malicious files which have been isolated by Comodo Internet Security to prevent them from infecting your system. Any files transferred to quarantine are encrypted - meaning they cannot be run or executed.

To access the quarantine interface

- Click 'Tasks' at the top left of the home interface
- Open the 'Advanced Tasks' tab and choose 'View Quarantine'
- This will display a list of items quarantined by the virus scanner or quarantined manually:

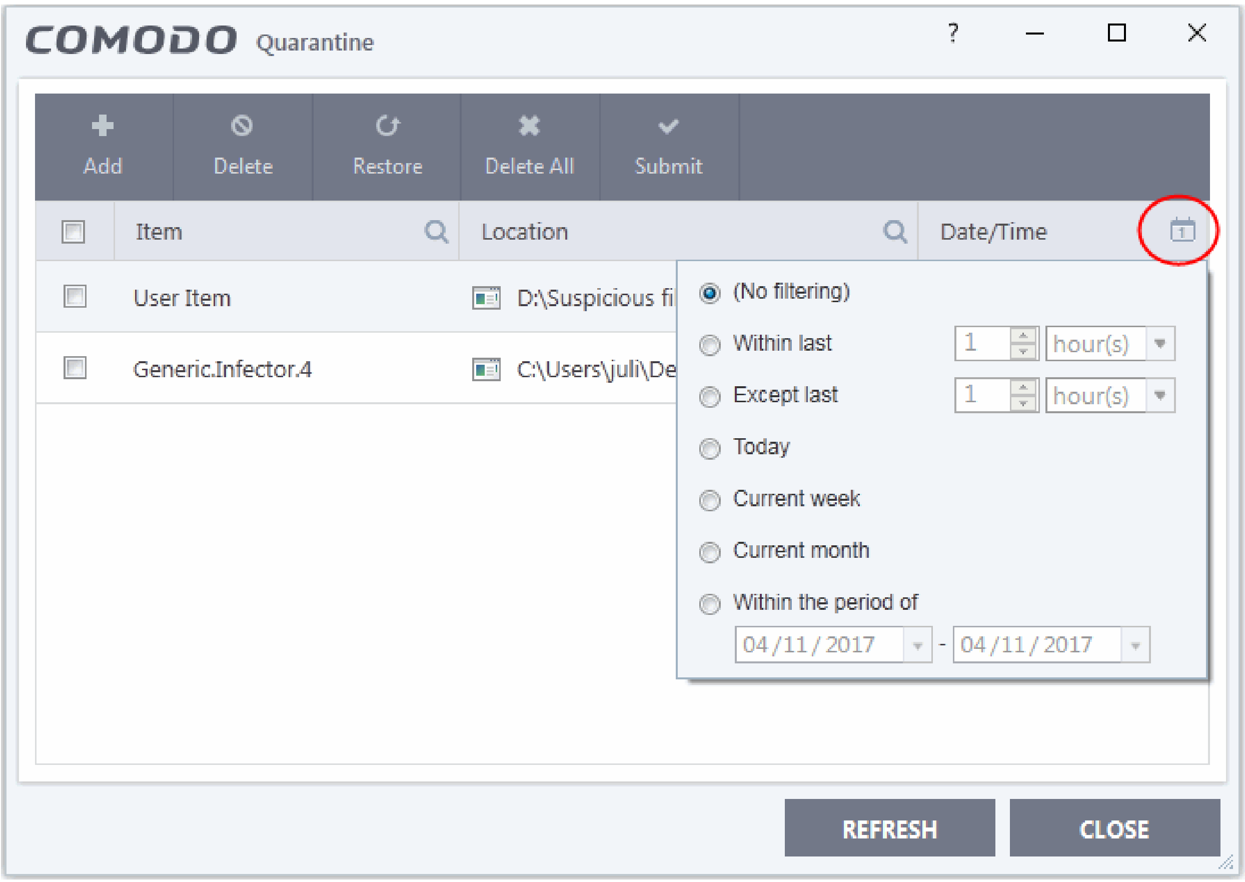

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Open Task Manager
Open the task manager to view running security tasks in progress.
View Quarantine
View and manage threats quarantined by virus scanner.
COMODO Quarantine
Add
Delete
Restore
Delete All
Submit
REFRESH
CLOSE

□	Item	Location	Date/Time
□	User Item	D:\Suspicious files\klaklashunt.exe	4/11/2017 5:02:52 AM
□	Generic.Infector.4	C:\Users\[redacted]\Desktop\x86\vt.exe	4/10/2017 6:20:16 AM

Column Descriptions

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

Items are generally placed in quarantine as a result of an on-demand or real time antivirus scan. See '**General Tasks > Scan and Clean Your Computer**', for more details.



□	Item	Location	Date/Time
□	User Item	D:\Suspicious fi	
□	Generic.Infector.4	C:\Users\juli\De	

● (No filtering)
○ Within last 1 hour(s)
○ Except last 1 hour(s)
○ Today
○ Current week
○ Current month
○ Within the period of
04 / 11 / 2017 - 04 / 11 / 2017

- To use the search option to find a specific quarantined item, click the search icon at top right in the 'Item' column header and enter the item name in full or part. Click the left and right arrows to navigate through the successive results.
- To use the search option to find a specific item based its storage of the file, click the search icon at top right of the 'Location' column header and enter the path.
- To filter the list based on the date of file installation, click the calendar icon at top right of the 'Date/Time' column header and choose the time/date/period.

The Quarantined Items interface also allows you to:

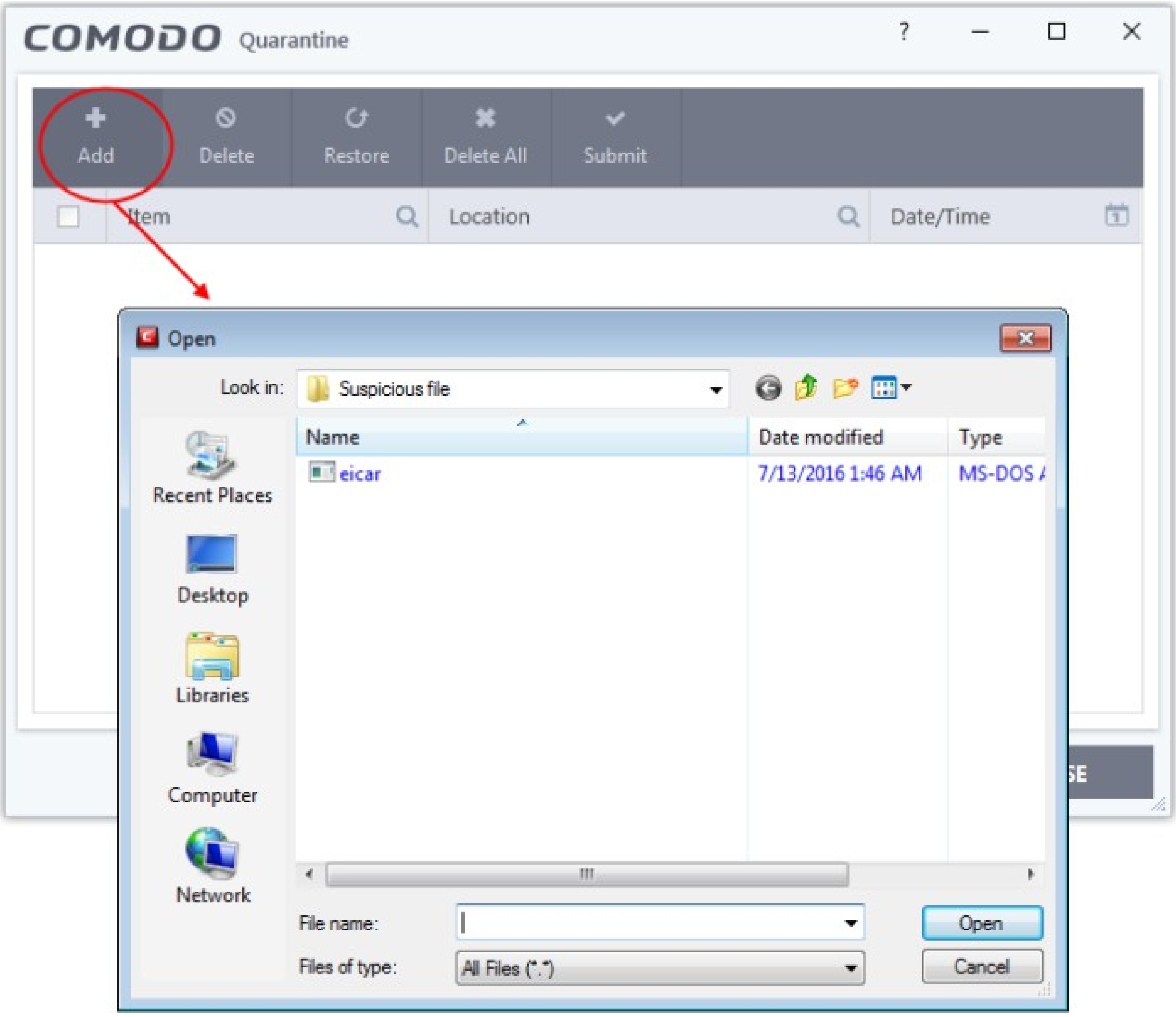
- **Manually add applications, executables or other files as a Quarantined item**
- **Delete a selected quarantined item from the system**
- **Restore a quarantined item to oits original location**
- **Delete all quarantined items**
- **Submit selected quarantined items to Comodo for analysis**

Manually adding files as Quarantined Items

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

To manually add a Quarantined Item

1. Click the 'Add' button at the top of the screen
2. Navigate to the file you want to add to the quarantine and click 'Open'.



The file will be added to 'Quarantine'. You can even send the file for analysis to Comodo, for inclusion in the white list or black list, by clicking the 'Submit' button.

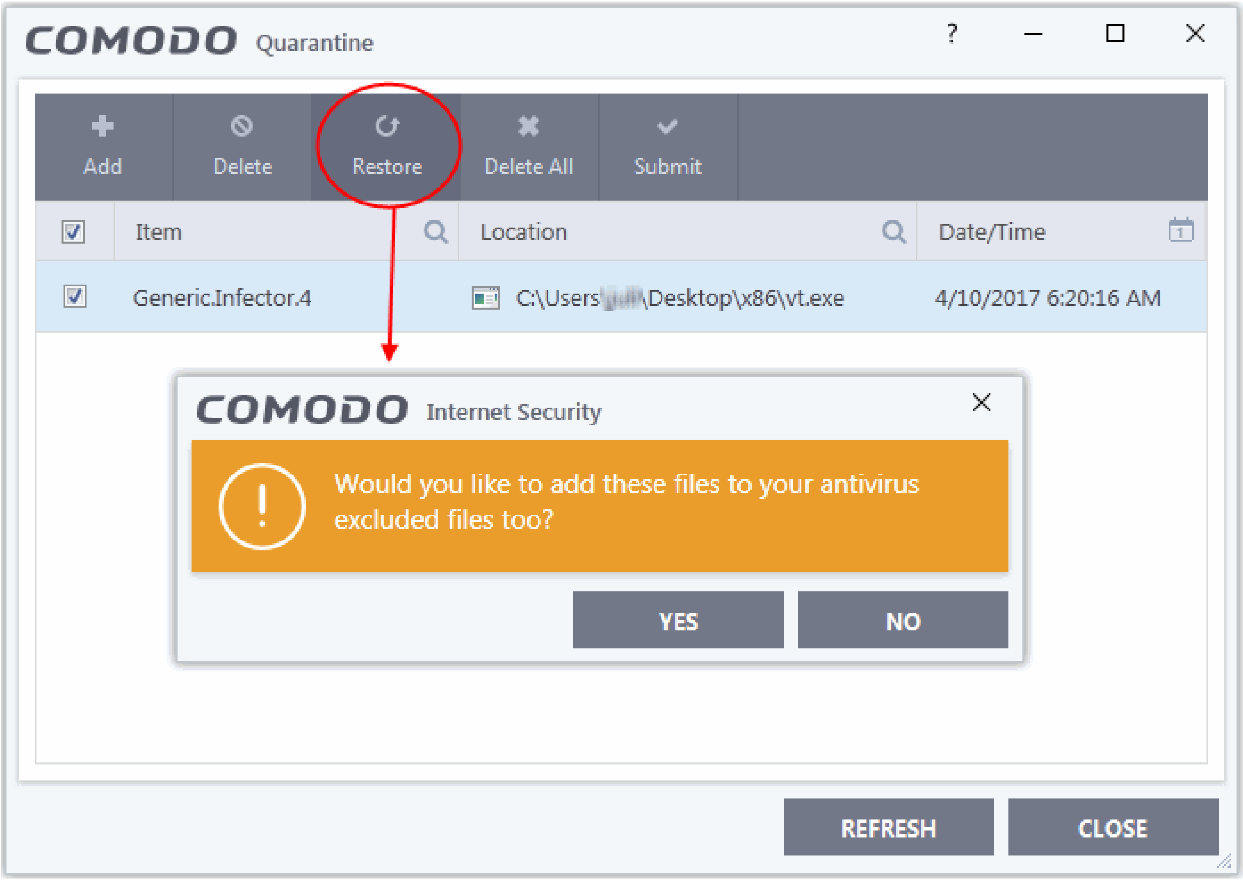
To delete a quarantined item from the system

- Select the item(s) from the 'Quarantine' interface and click the 'Delete' button at the top.

This deletes the file(s) from the system permanently.

To restore a quarantined item to its original location

- Select the item(s) from the 'Quarantine' interface and click the 'Restore' button at the top.



☑ Generic.Infector.4 C:\Users\ \Desktop\x86\vt.exe 4/10/2017 6:20:16 AM

Would you like to add these files to your antivirus excluded files too?

An option will be provided to add the file(s) to **Exclusions** list and if 'Yes' is opted, these files will not be scanned again.

The file will be restored to its original location. If the restored item does not contain malware it will operate as usual. If it contains malware it will be flagged as a threat immediately if real-time scanning is enabled (or during the next scan if real time scanning is disabled). The file will not be flagged if it is on the 'Exclusions' list.

To remove all the quarantined items permanently

- Click the 'Delete All' button at the top.

All the quarantined items will be deleted from your system permanently.

To submit selected quarantined items to Comodo for analysis

- Select the item(s) from the 'Quarantine' interface and click the 'Submit' button at the top.
- 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 CIS (false positives).
- Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (blacklisted).

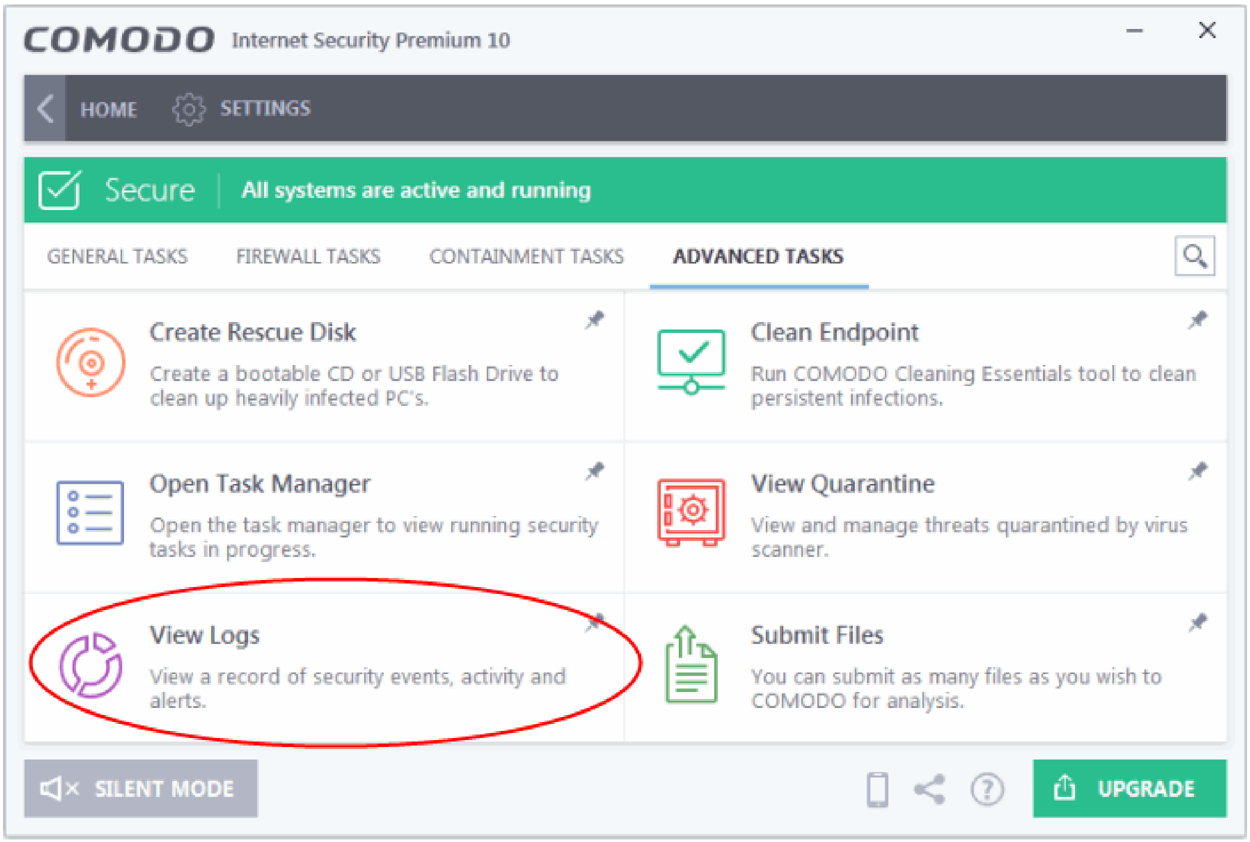
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

5.5. View CIS Logs

CIS keeps logs of antivirus, firewall, HIPS, Containment and other events. These can be viewed at anytime from the 'Log Viewer' module.

To open the 'Log Viewer' module

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface
- Click 'Advanced Tasks' then 'View Logs'



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

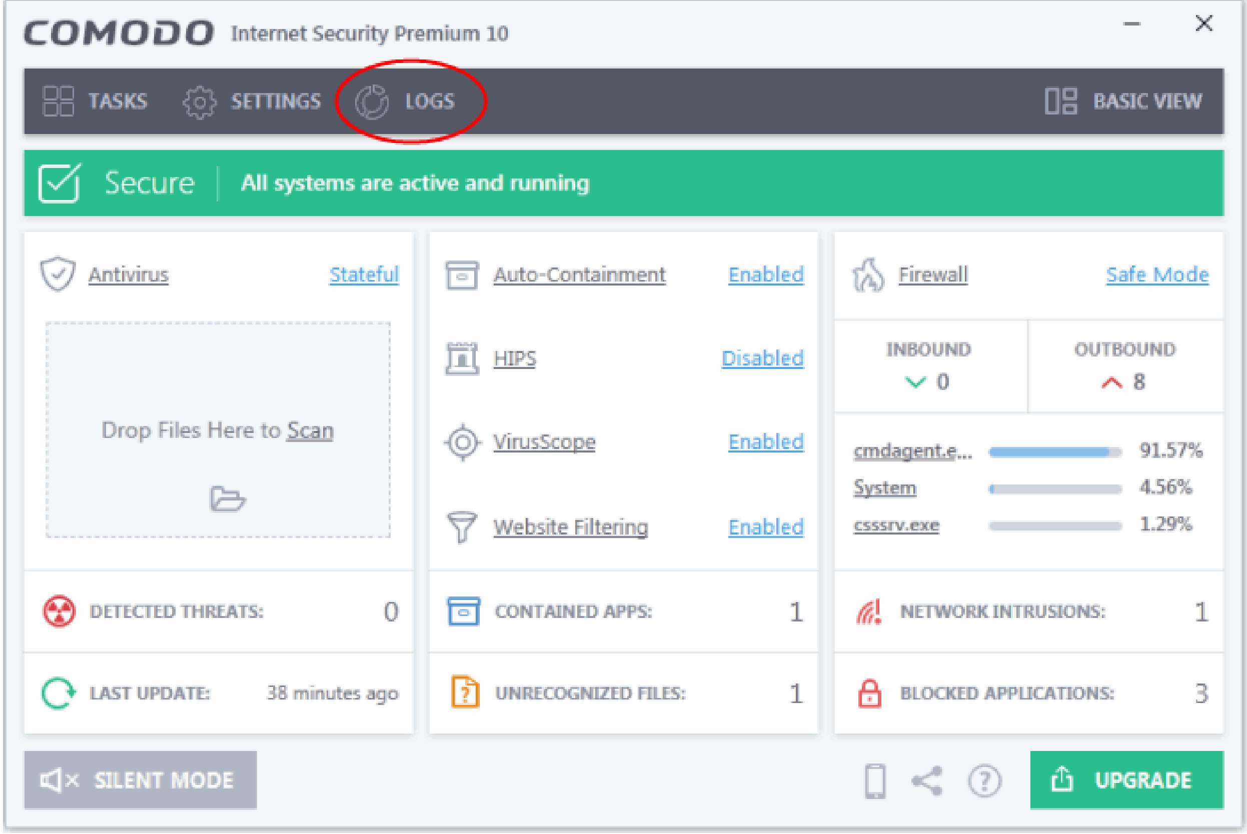
Open Task Manager
Open the task manager to view running security tasks in progress.

View Quarantine
View and manage threats quarantined by virus scanner.

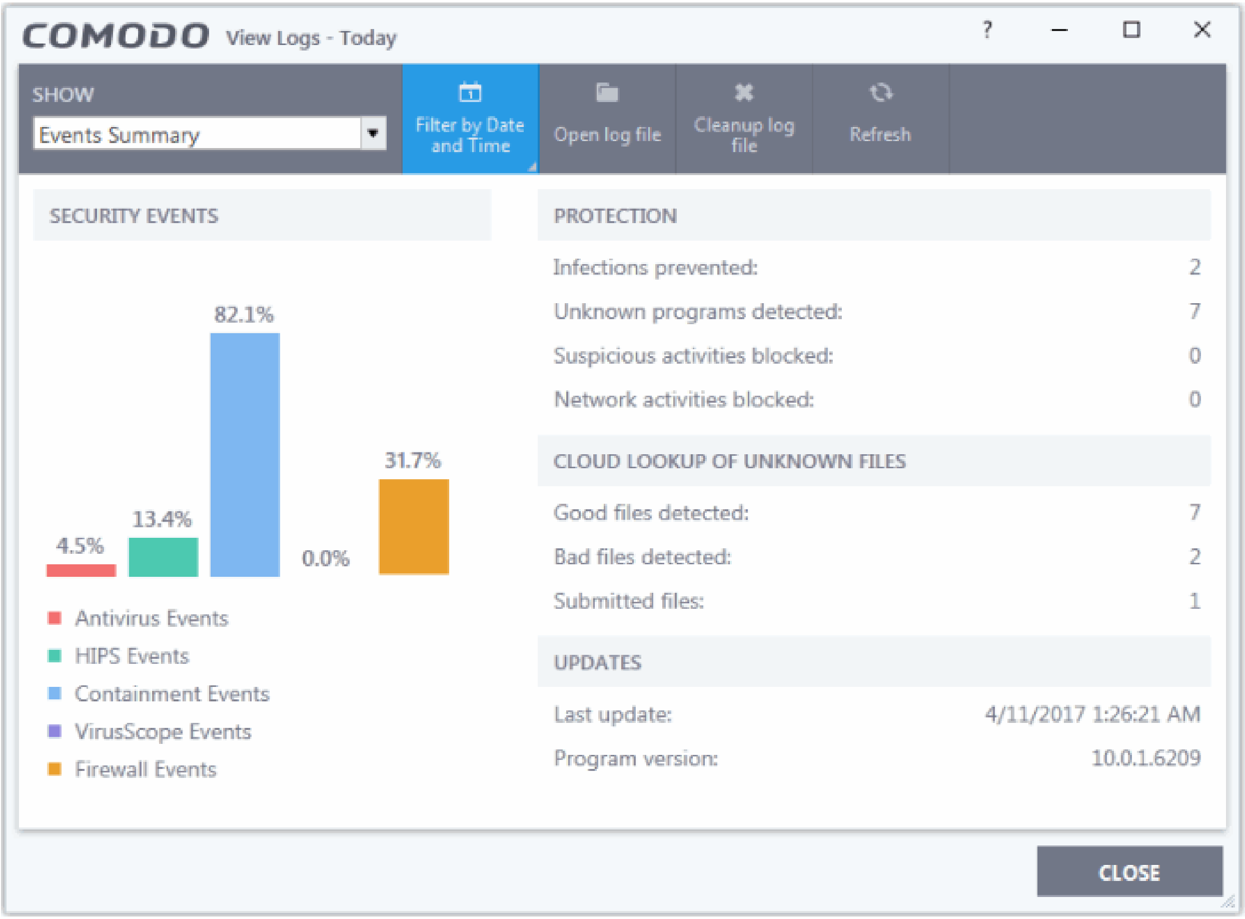
View Logs
View a record of security events, activity and alerts.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

- Alternatively, click 'Logs' in the title bar of the 'Advanced View' of the home screen



The 'View Logs' interface will open, showing a summary of CIS events:



PROTECTION

Infections prevented:	2
Unknown programs detected:	7
Suspicious activities blocked:	0
Network activities blocked:	0

CLOUD LOOKUP OF UNKNOWN FILES

Good files detected:	7
Bad files detected:	2
Submitted files:	1

UPDATES

Last update:	4/11/2017 1:26:21 AM
Program version:	10.0.1.6209

- The bar graph on the left shows a comparison of antivirus, firewall, containment, VirusScope and HIPS events.

- The right side shows a summary of events, the results of cloud based scanning of your system and CIS version and update information.
- The interface contains a full history of logged events from the Firewall, HIPS, Containment, VirusScope, Website Filtering and Antivirus modules. Use the drop-down at top-left to change which events are shown.
- To open a saved log file, click 'Open log file' button beside the drop-down and browse to the location where the CIS log file is stored.
- To clear the logs, click the 'Cleanup log file' button
- To refresh the logs, click the 'Refresh' button

The following sections contain more details about each type of log:

'Logs per Module':

- **Antivirus**
- **VirusScope**
- **Firewall**
- **HIPS**
- **Containment**
- **Website Filtering**

'Other Logs':

- **Alerts Displayed**
- **Tasks Launched**
- **File List Settings Changes**
- **Trusted Vendors List Changes**
- **Configuration Changes**
- **Secure Shopping Activities**

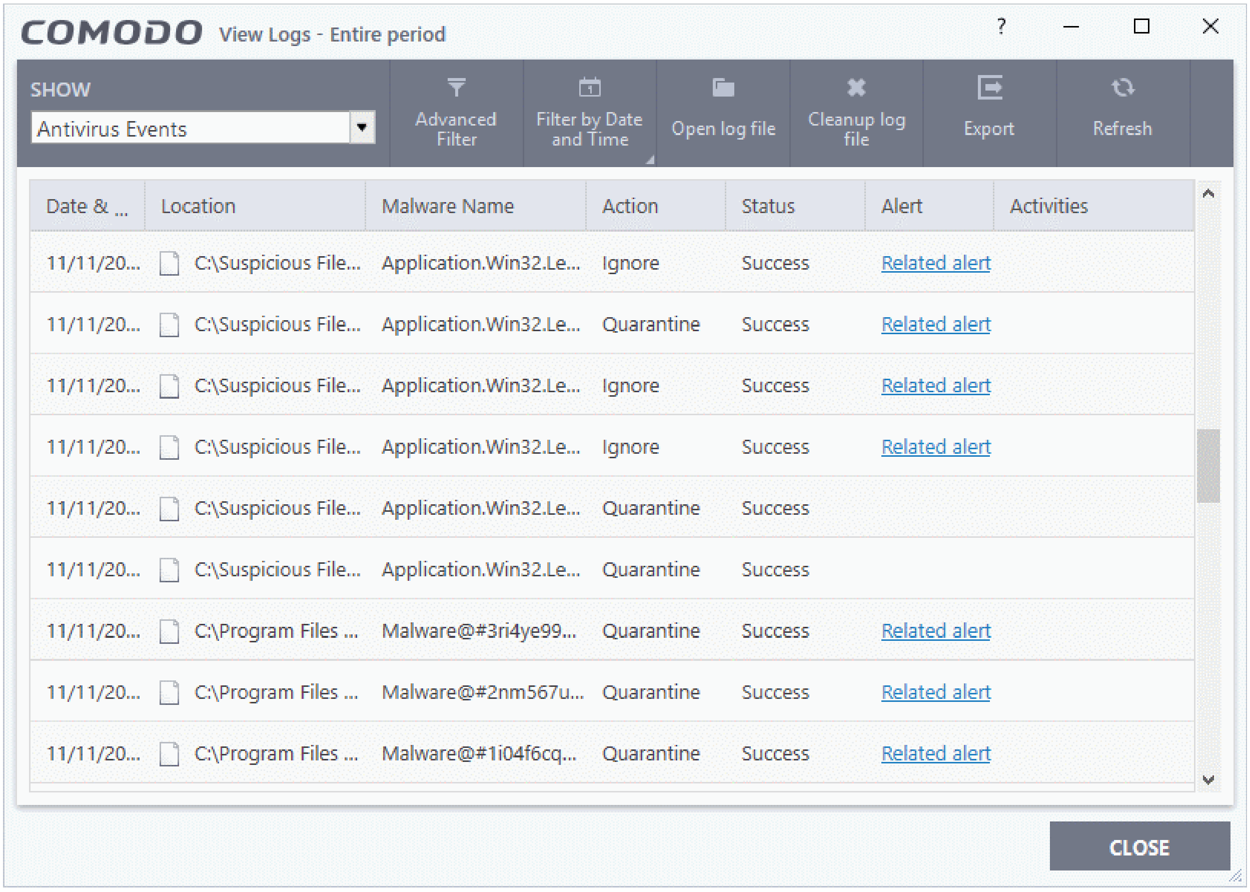
5.5.1. Antivirus Logs

Comodo Antivirus documents the results of all actions it performs in extensive but easy to understand logs. A detailed scan report contains statistics of all scanned objects, settings used for each task and a history of actions performed on individual files. Reports are also generated during real-time protection, and after updating the antivirus database and application modules.

To view the 'Antivirus' Logs

- Click 'Tasks' at the top left of the CIS screen
- Click 'Advanced Tasks' > 'View Logs':
- Select 'Antivirus Events' from the 'Show' drop-down:

Tip: Alternatively, the 'Antivirus' log screen can be accessed by clicking the number beside 'Detected Threats' in the 'Advanced View' of the 'Home' screen in the 'Antivirus' pane.



Date & ...	Location	Malware Name	Action	Status	Alert	Activities
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Ignore	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Quarantine	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Ignore	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Ignore	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Quarantine	Success		
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Quarantine	Success		
11/11/20...	C:\Program Files ...	Malware@#3ri4ye99...	Quarantine	Success	Related alert	
11/11/20...	C:\Program Files ...	Malware@#2nm567u...	Quarantine	Success	Related alert	
11/11/20...	C:\Program Files ...	Malware@#1i04f6cq...	Quarantine	Success	Related alert	

Column Descriptions

1. **Date & Time**- Indicates the precise date and time of the event.
2. **Location -** Indicates the installation location of the application detected as a threat.
3. **Malware Name -** Name of the malware detected at that event.
4. **Action -** Indicates action taken against the malware through Antivirus.
5. **Status -** Gives the status of the action taken. It can be either 'Success' or 'Fail'.
6. **Alert -** Clicking the 'Related Alert' link opens the 'Alerts' interface of the Log Viewer and displays details of the alert displayed during the event.

Note: Antivirus Alerts are displayed to the user only if the option 'Do not Show Antivirus Alerts' is disabled in the Antivirus Settings. See **Real-time Scan Settings** for more details.

7. **Activities -** Clicking the 'Process Activities' link shows details of activities initiated by the infected application.

- To export the 'Antivirus' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu
- To open a stored CIS log file, click the 'Open log file' button
- To refresh the 'Antivirus' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu
- To clear the 'Antivirus' logs, click the 'Cleanup log file' button
- You can sort the entries by ascending \ descending order by clicking on the respective column headers

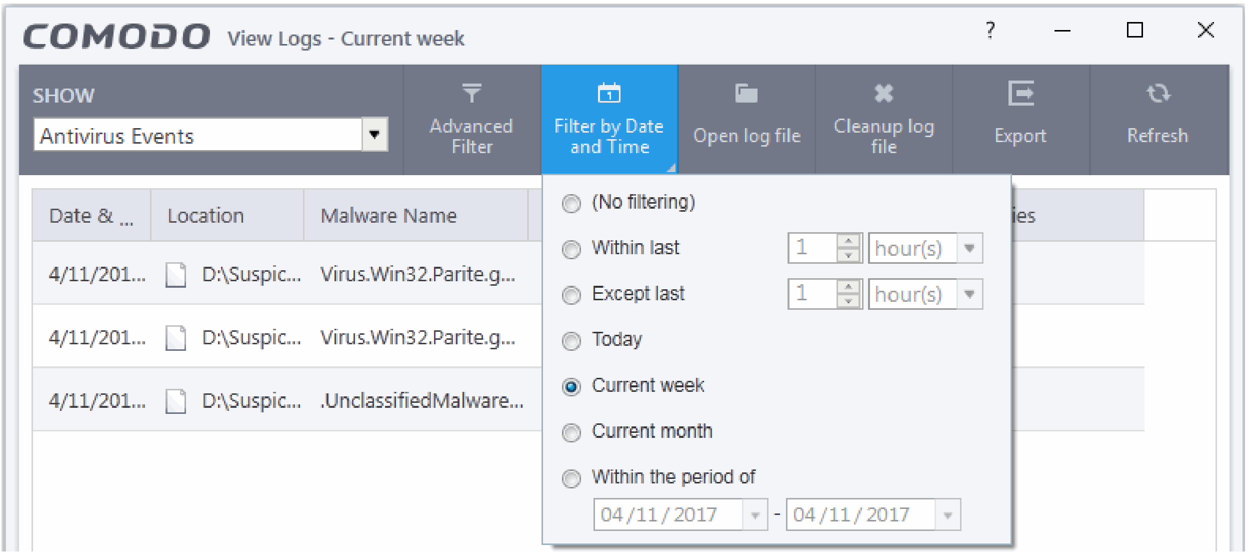
5.5.1.1. Filtering Antivirus Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters:

- Click 'Filter by Date and Time' to filter logs for a selected time period:

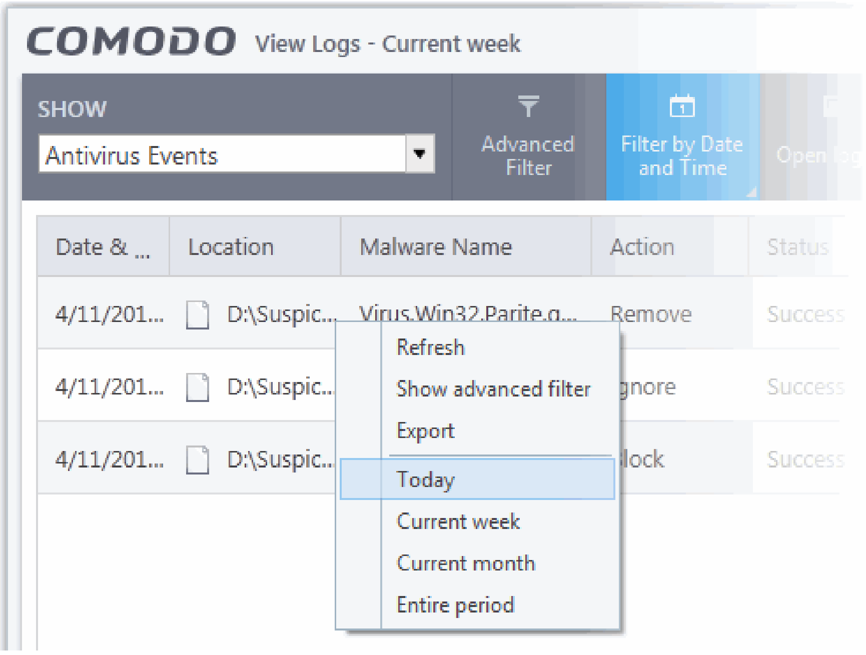


Date & ...	Location	Malware Name
4/11/201...	D:\Suspic...	Virus.Win32.Parite.g...
4/11/201...	D:\Suspic...	Virus.Win32.Parite.g...
4/11/201...	D:\Suspic...	.UnclassifiedMalware...

○ (No filtering)
○ Within last 1 hour(s)
○ Except last 1 hour(s)
○ Today
● Current week
○ Current month
○ Within the period of 04/11/2017 - 04/11/2017

- **No filtering -** Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last -** Show all logs from a certain point in the past until the present time.
- **Except last -** Exclude all logs from a certain point in the past until the present time.
- **Today -** Display all logged events for today.
- **Current Week -** All logged events during the current week. The current week is calculated as the previous Sunday to the next Saturday.
- **Current Month -** All logged events during this month.
- **Custom Filter -** Select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



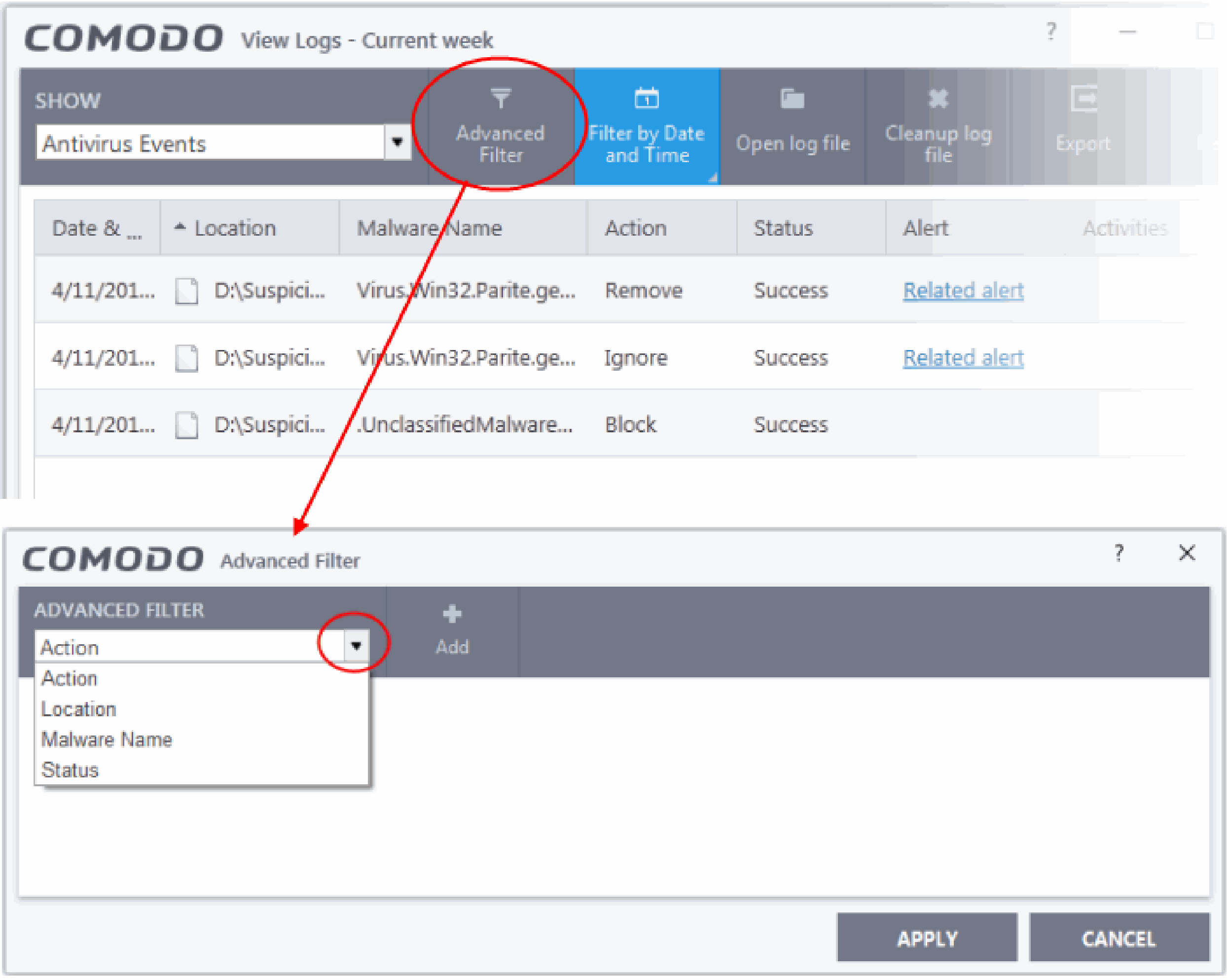
Advanced Filters

Having chosen a **preset time filter**, you can further refine which events are shown by using the following additional parameters:

- **Action -** Events according to the response (or action taken) by the antivirus
- **Location -** Displays only events logged from a specific location
- **Malware Name -** Displays only those events that reference a specific piece of malware
- **Status** – Show events according to whether the logged action was successful or not. Status options are 'Success' or 'Fail'.

To configure Advanced Filters for Antivirus events

- Click the 'Advanced Filter' button from the title bar or right click inside the log viewer module and choose 'Advanced filter' from the context sensitive menu. The 'Advanced Filter' interface for AV events will open.
- Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.

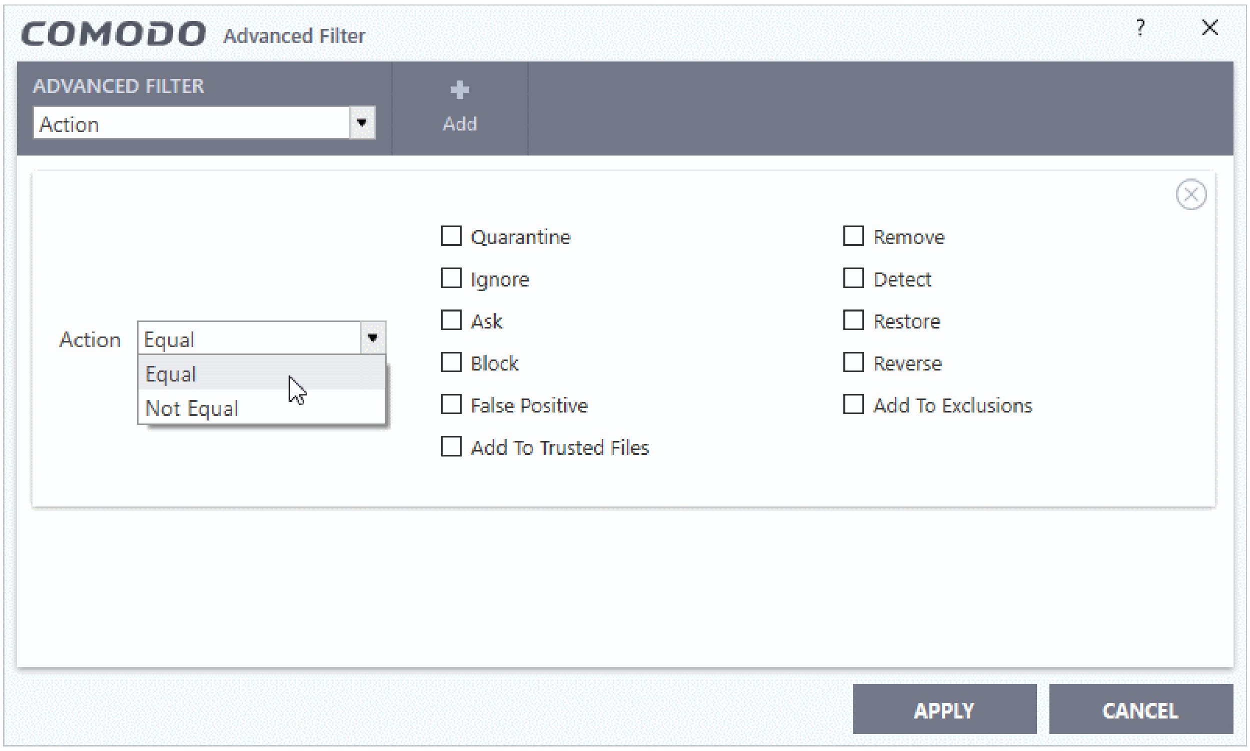


Date & ...	Location	Malware Name	Action	Status	Alert	Activities
4/11/201...	D:\Suspici...	Virus.Win32.Parite.ge...	Remove	Success	Related alert	
4/11/201...	D:\Suspici...	Virus.Win32.Parite.ge...	Ignore	Success	Related alert	
4/11/201...	D:\Suspici...	.UnclassifiedMalware...	Block	Success		

There are 4 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

i. **Action**: The 'Action' option allows you to filter logs based on the action taken by CIS against the detected threat. To filter logs by CIS action, select 'Action' from the drop-down then click 'Add':



You should now choose the actions by which you want to filter the logs:

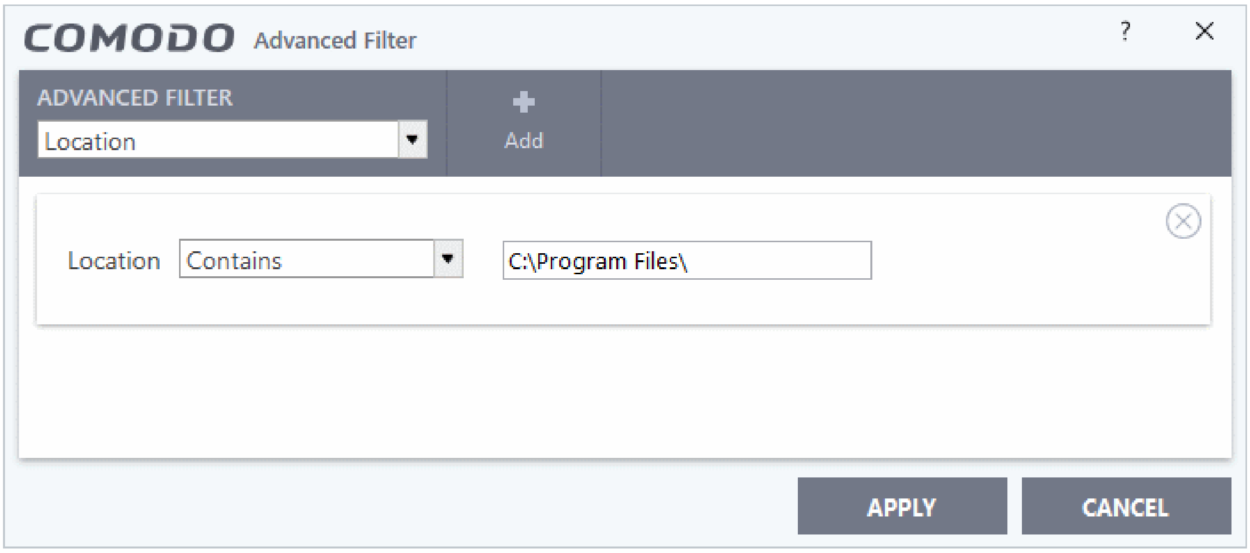
a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

b) Now select the check boxes of the specific filter parameters to refine your search. The parameter available are:

- Quarantine: Displays events at which the user chose to quarantine a file
- Remove: Displays events at which the user chose to delete the detected threat
- Ignore: Displays events at which the user chose to ignore the detected threat
- Detect: Displays events involving only the detection of malware
- Ask: Displays events where an alert was shown to the user so they could choose an action against a piece of detected malware
- Restore: Displays events at which quarantined applications were restored
- Block: Displays event where suspicious applications were blocked
- Reverse: Displays events where VirusScope reversed potentially malicious actions
- False Positive: Displays events where files flagged as threats by CIS were submitted to Comodo by the user as a false positive.
- Add To Exclusions: Displays events in which the user chose to add an item to antivirus exclusions
- Add To Trusted Files: Displays events in which the user changed the file rating to 'Trusted'

For example, if you checked the 'Quarantine' box then selected 'Not Equal', you would see only those events where the 'Quarantine Action' was not selected at the virus notification alert.

ii. **Location**: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



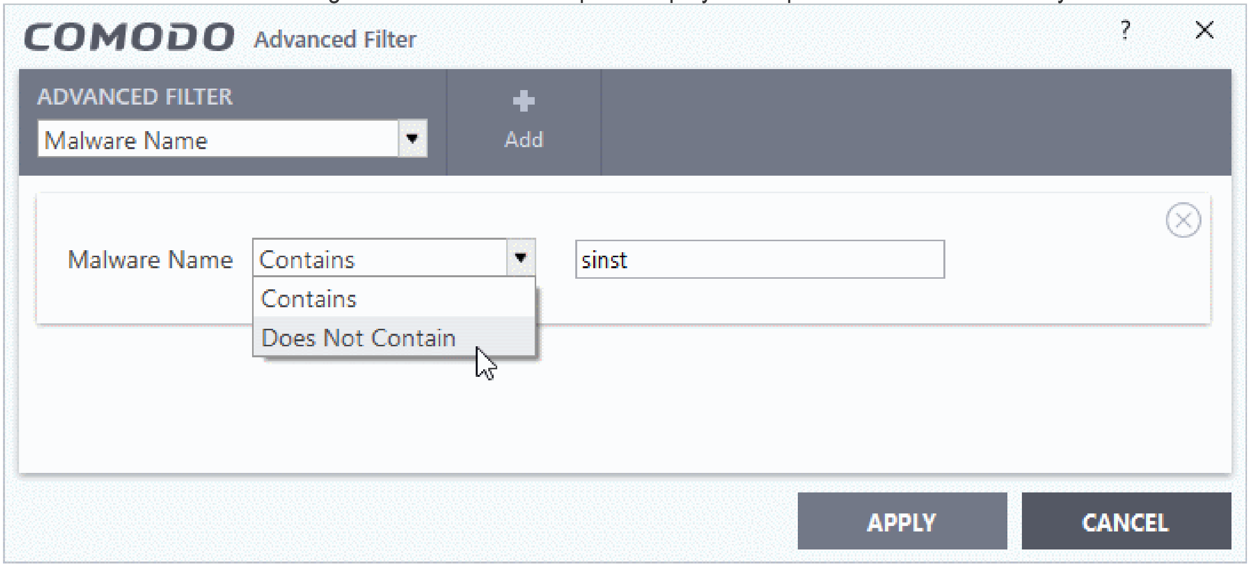
Location: Contains — C:\Program Files\

a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text or word that needs to be filtered.

For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:\Program Files\' in the text field, then all events containing the entry 'C:\Program Files\' in the 'Location' field will be displayed. If you select the 'Does Not Contain' option from the drop-down field and enter the phrase 'C:\Program Files\' in the text field, then all events that do not have the entry 'C:\Program Files\' will be displayed.

iii. **Malware Name**: The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



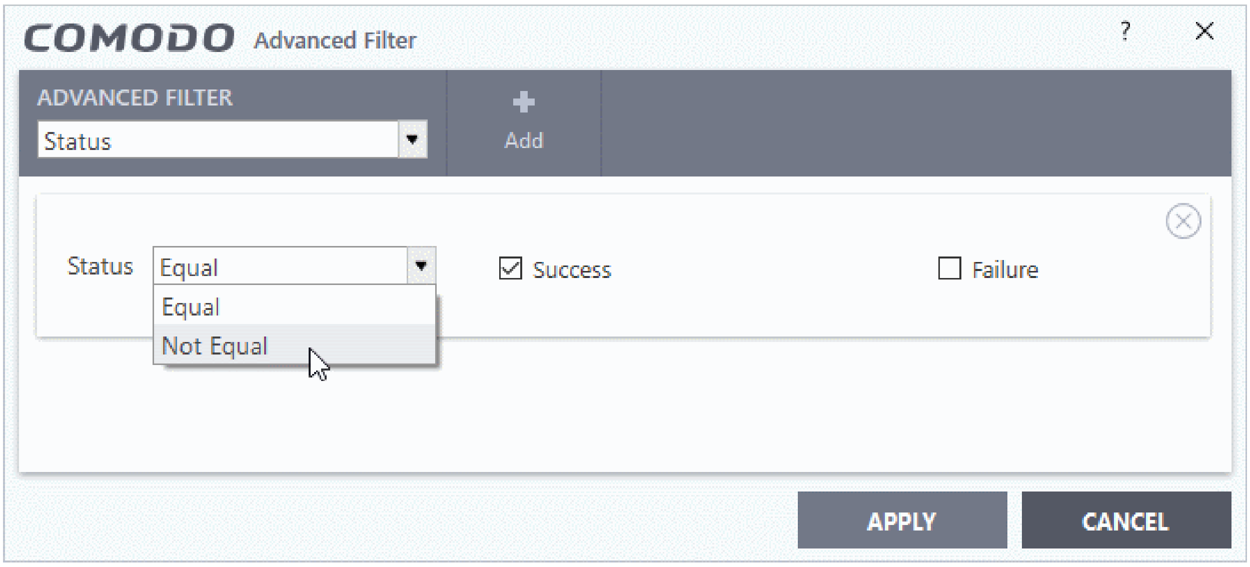
Malware Name: Contains — sinst

a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and type 'siins' in the text field, then all events with 'siins' in the 'Malware Name' field will be shown. If you choose 'Does Not Contain' and type 'siins', then all events that do not have 'siins' in the 'Malware Name' field will be shown.

iv. **Status**: The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CIS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



a) Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- Success: Displays events in which the actions against the detected threat were successfully executed (for example, the malware was successfully quarantined)
- Failure: Displays events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected)

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

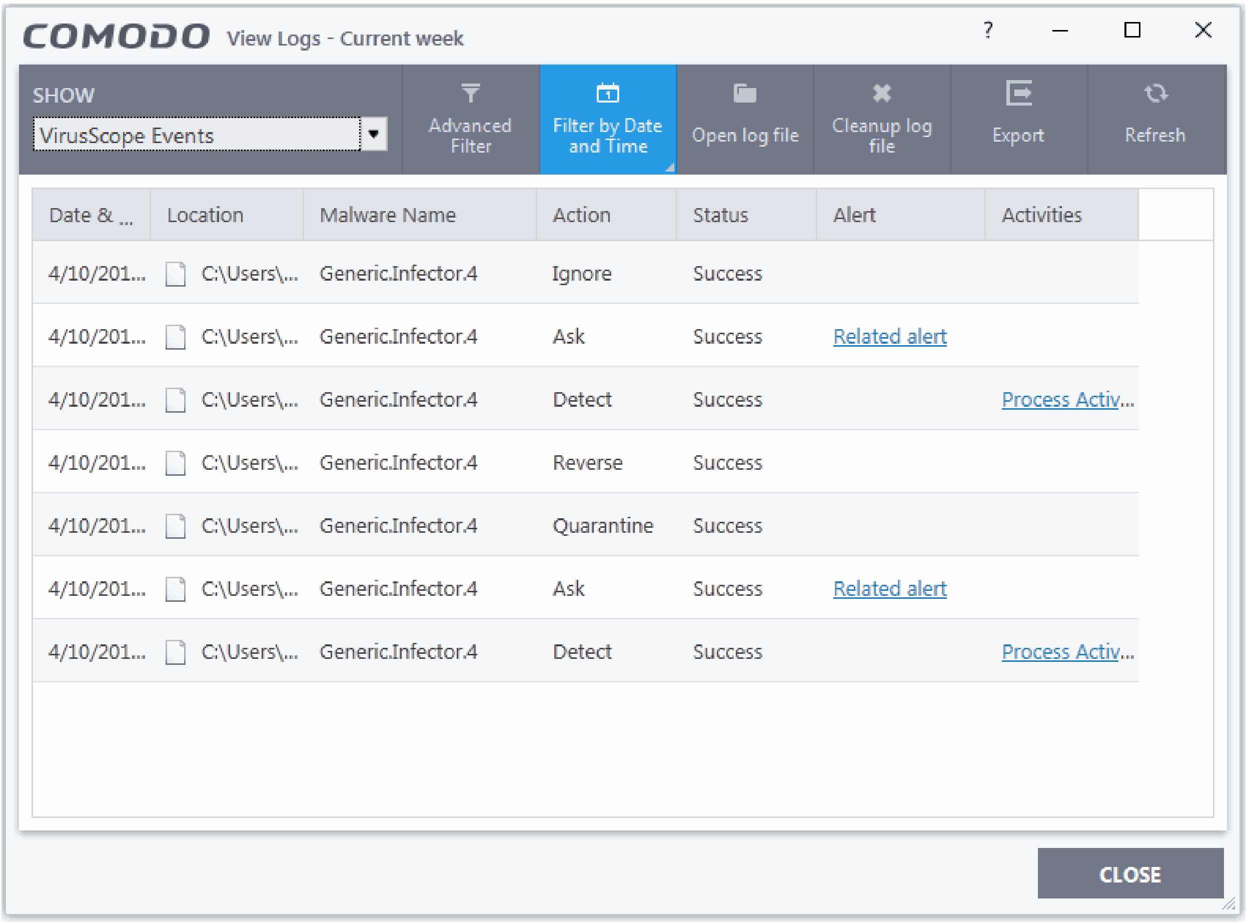
- Click 'Apply' for the filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.5.2. VirusScope Logs

Event logs are created whenever VirusScope blocks or reverses a suspicious activity.

To view the 'VirusScope' Logs

- Open the Log Viewer module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'VirusScope Events' from the 'Show' drop-down



COMODO View Logs - Current week

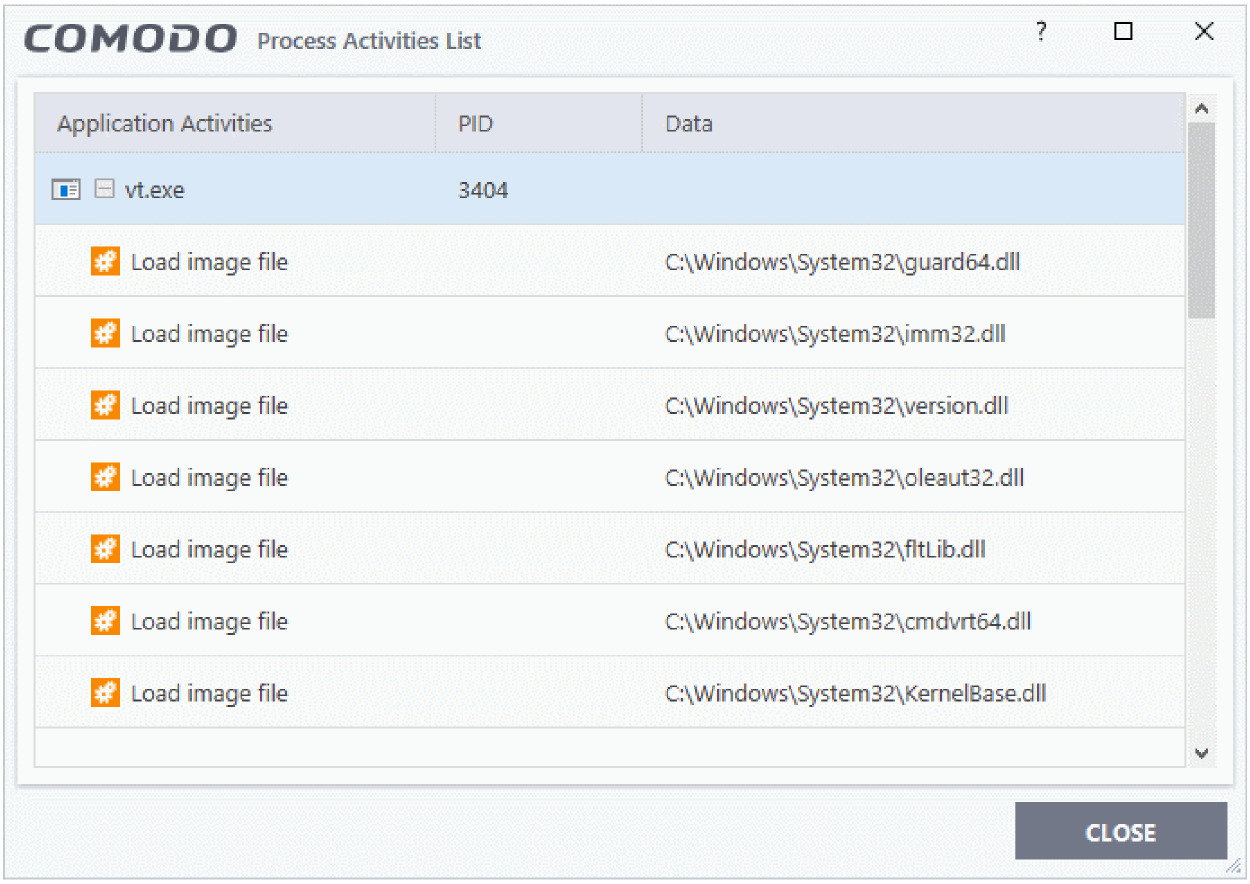
Date & ...	Location	Malware Name	Action	Status	Alert	Activities
4/10/201...	C:\Users\...	Generic.Infector.4	Ignore	Success		
4/10/201...	C:\Users\...	Generic.Infector.4	Ask	Success	Related alert	
4/10/201...	C:\Users\...	Generic.Infector.4	Detect	Success		Process Activ...
4/10/201...	C:\Users\...	Generic.Infector.4	Reverse	Success		
4/10/201...	C:\Users\...	Generic.Infector.4	Quarantine	Success		
4/10/201...	C:\Users\...	Generic.Infector.4	Ask	Success	Related alert	
4/10/201...	C:\Users\...	Generic.Infector.4	Detect	Success		Process Activ...

Column Descriptions

1. **Date & Time** - Indicates the precise date and time of the occurrence of the event.
2. **Location** - Indicates installation location of the suspicious executable.
3. **Malware Name** - Name of the detected malware.
4. **Action** - Indicates the action taken by VirusScope in response to the event.
    - Reverse - VirusScope detected suspicious activity and attempted to reverse any changes made to the file system.
    - Quarantine - VirusScope placed the suspicious file into quarantine
    - Detect - VirusScope detected malicious activity but did not quarantine the executable or reverse its changes
    - Ask - VirusScope detected malicious activity and presented a pop-up asking the user whether it should quarantine the executable or reverse the changes.
5. **Status** - Status of the action taken - 'Success' or 'Fail'.
6. **Alert** - Clicking the 'Related Alert' link shows details of the alert displayed during the event.

Note: VirusScope alerts are displayed only if the option 'Do not pop up alerts' is disabled in VirusScope Settings. See **VirusScope Configuration** for more details.

7. **Activities** - Clicking the 'Process Activities' link displays details of activities executed by the processes that were run by the infected application. An example is shown below.



Application Activities	PID	Data
vt.exe	3404	
Load image file		C:\Windows\System32\guard64.dll
Load image file		C:\Windows\System32\imm32.dll
Load image file		C:\Windows\System32\version.dll
Load image file		C:\Windows\System32\oleaut32.dll
Load image file		C:\Windows\System32\fltLib.dll
Load image file		C:\Windows\System32\cmdvrt64.dll
Load image file		C:\Windows\System32\KernelBase.dll

- To export 'VirusScope' logs as a HTML file, click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a saved CIS log file, click the 'Open log file' button
- To refresh the 'VirusScope' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To delete the 'VirusScope' logs click the 'Cleanup log file' button
- You can sort the entries by ascending \ descending order by clicking on the respective column headers

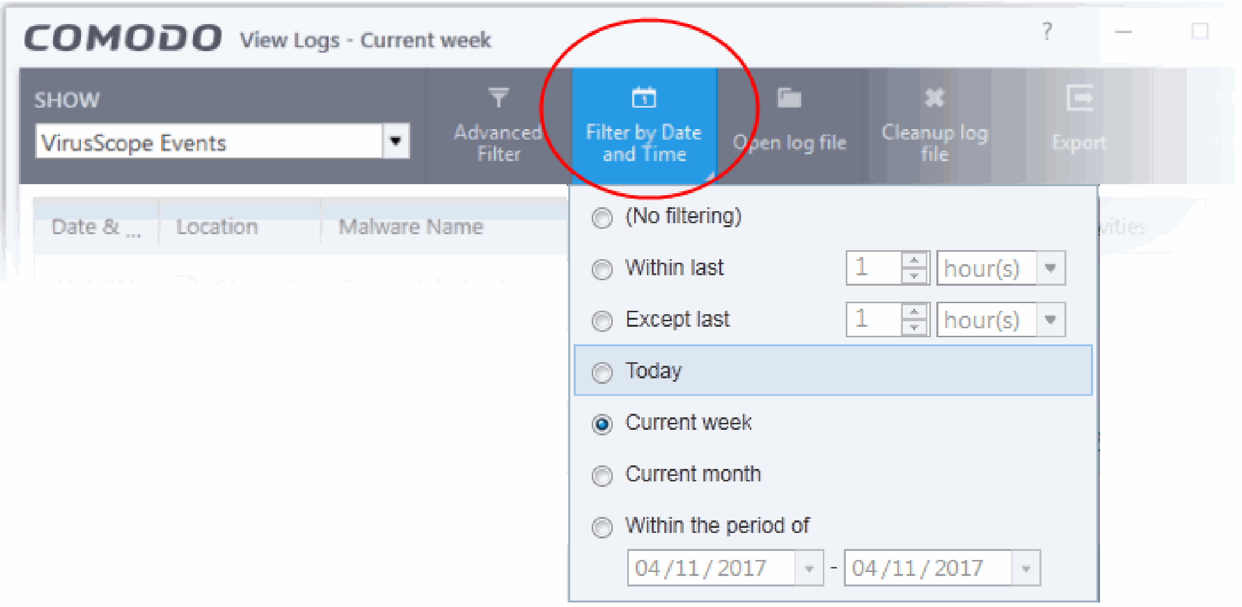
5.5.2.1. Filtering VirusScope Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

- Click 'Filter by Date and Time' to filter logs for a selected time period:



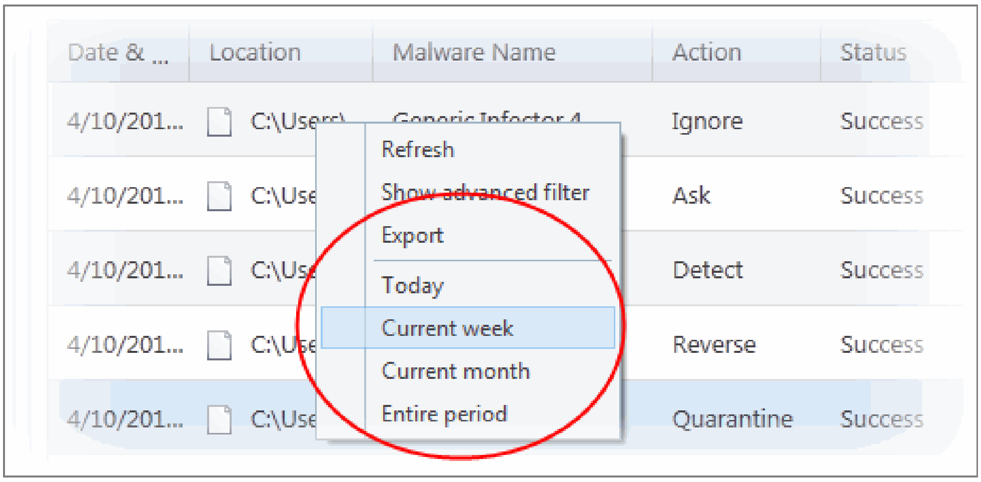
COMODO View Logs - Current week

SHOW: VirusScope Events

- ○ (No filtering)
- ○ Within last 1 hour(s)
- ○ Except last 1 hour(s)
- ○ Today
- ● Current week
- ○ Current month
- ○ Within the period of 04/11/2017 - 04/11/2017

- **No filtering -** Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Display all logged events for today.
- **Current Week -** All logged events during the current week. The current week is calculated as the previous Sunday to the next Saturday.
- **Current Month -** All logged events during this month.
- **Custom Filter** - Select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Date & ...	Location	Malware Name	Action	Status
4/10/201...	C:\Users\	Generic Infector 4	Ignore	Success
4/10/201...	C:\Use		Ask	Success
4/10/201...	C:\Us		Detect	Success
4/10/201...	C:\Use		Reverse	Success
4/10/201...	C:\Use		Quarantine	Success

Advanced Filters

Having chosen a **preset time**, you can further refine which events are shown by using the following additional parameters:

- **Action -** Displays events according to the response (or action taken) by the VirusScope
- **Location -** Displays only the events logged from a specific location
- **Malware Name -** Displays only those events that reference a specific piece of malware

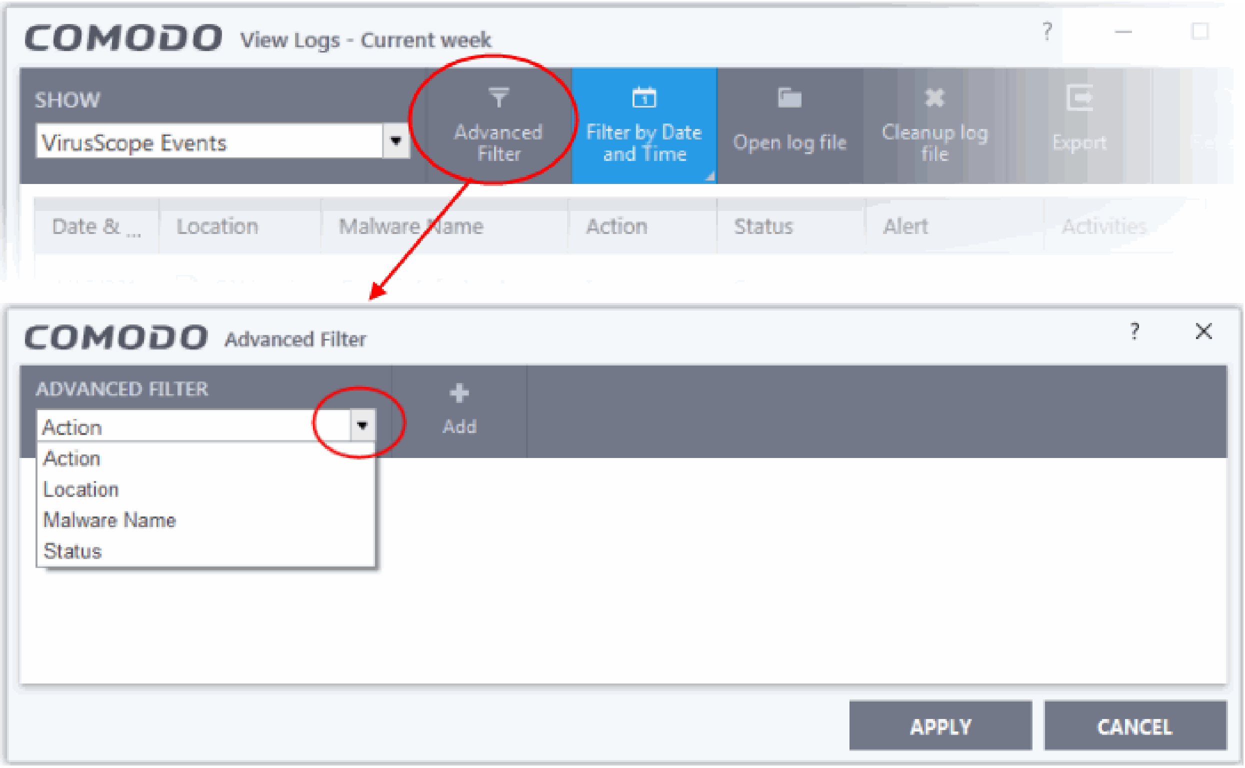
- **Status -** Show events according to whether the logged action was successful or not. Status options are 'Success' or 'Fail'.

To configure Advanced Filters for VirusScope events

1. Click the 'Advanced Filter' button from the title bar or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

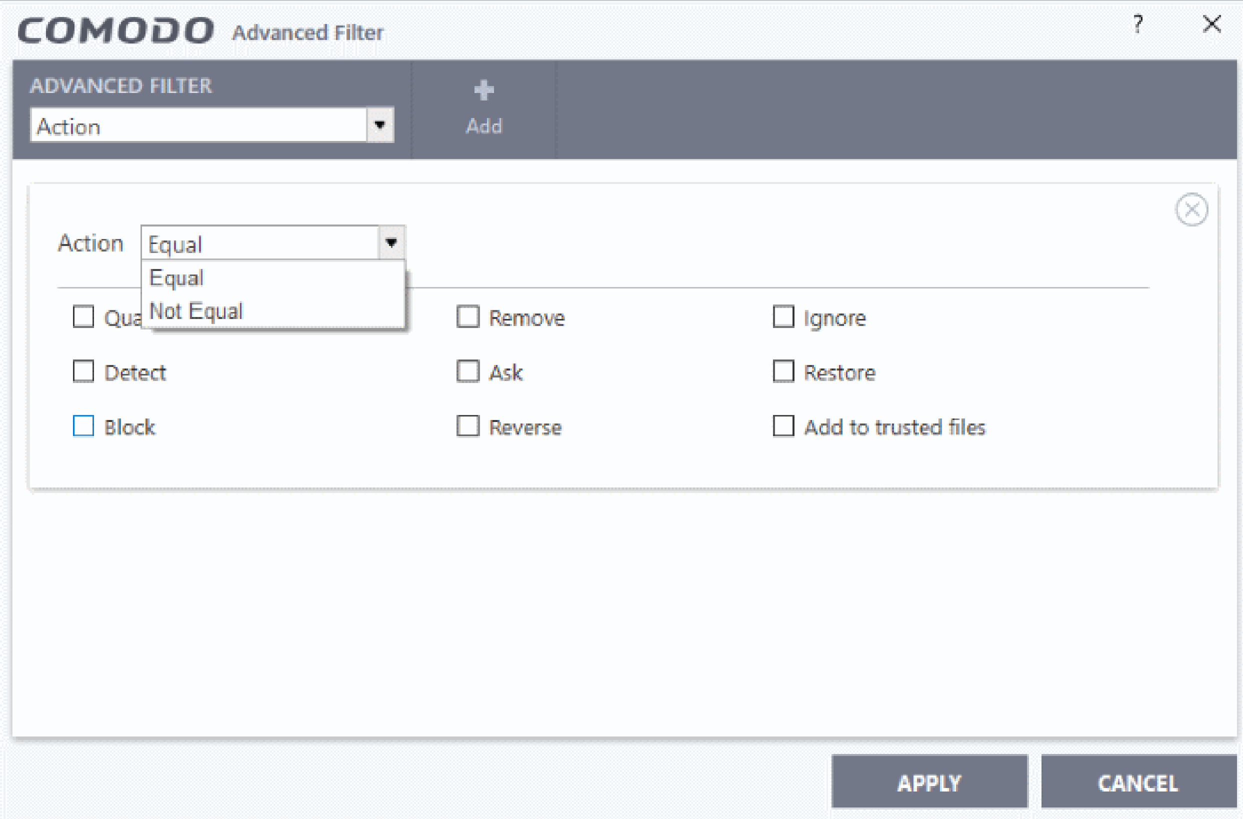
The 'Advanced Filter' interface for VirusScope Logs will open

2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



There are 4 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

i. **Action**: The 'Action' option allows you to filter logs based on the actions taken by CIS against the detected threat. To filter logs by CIS action, select 'Action' from the drop-down then click 'Add':

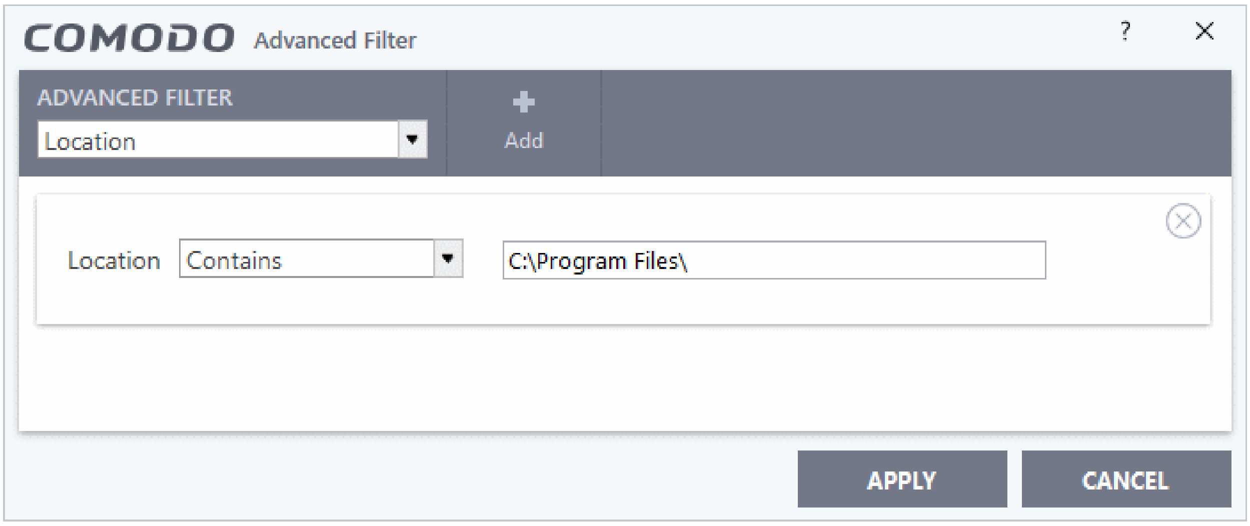


a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

b. Now select the check boxes of the specific filter parameters to refine your search. The parameter available are:

- Quarantine: Displays events at which the user chose to quarantine a file
- Remove: Displays events at which the user chose to delete the detected threat
- Ignore: Displays events at which the user chose to ignore the detected threat
- Detect: Displays events involving only the detection of malware
- Ask: Displays events where an alert was shown to the user so they could choose an action against a piece of detected malware
- Restore: Displays events at which quarantined applications were restored
- Block: Displays event where suspicious applications were blocked
- Reverse: Displays events where VirusScope reversed potentially malicious actions
- Add To Trusted Files: Displays events in which the user changed the file rating to 'Trusted'
- For example, if you checked the 'Quarantine' box then selected 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

ii. **Location**: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



Location: Location

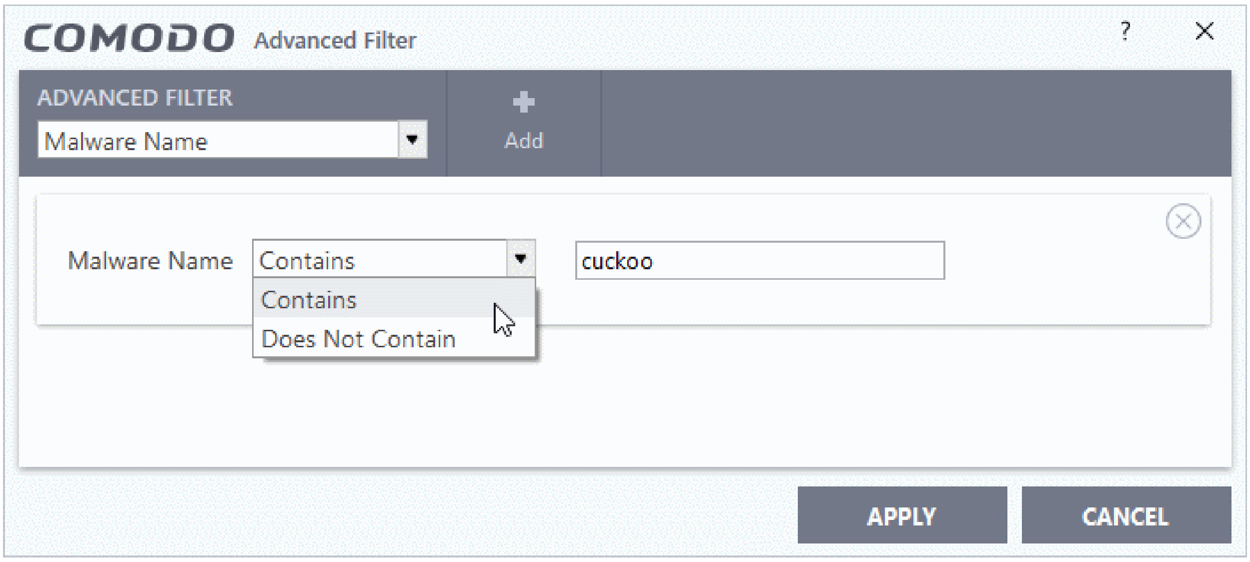
Location Contains C:\Program Files\

a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b. Enter the text or word that needs to be filtered.

For example, if you select 'Contains' from the drop-down and enter the phrase 'C:\Program Files\' in the text field, then all events containing the entry 'C:\Program Files\' in the 'Location' field will be displayed. If you select the 'Does Not Contain' option from the drop-down field and enter the phrase 'C:\Program Files\' in the text field, then all events that do not have the entry 'C:\Program Files\' will be displayed.

iii. **Malware Name**: The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



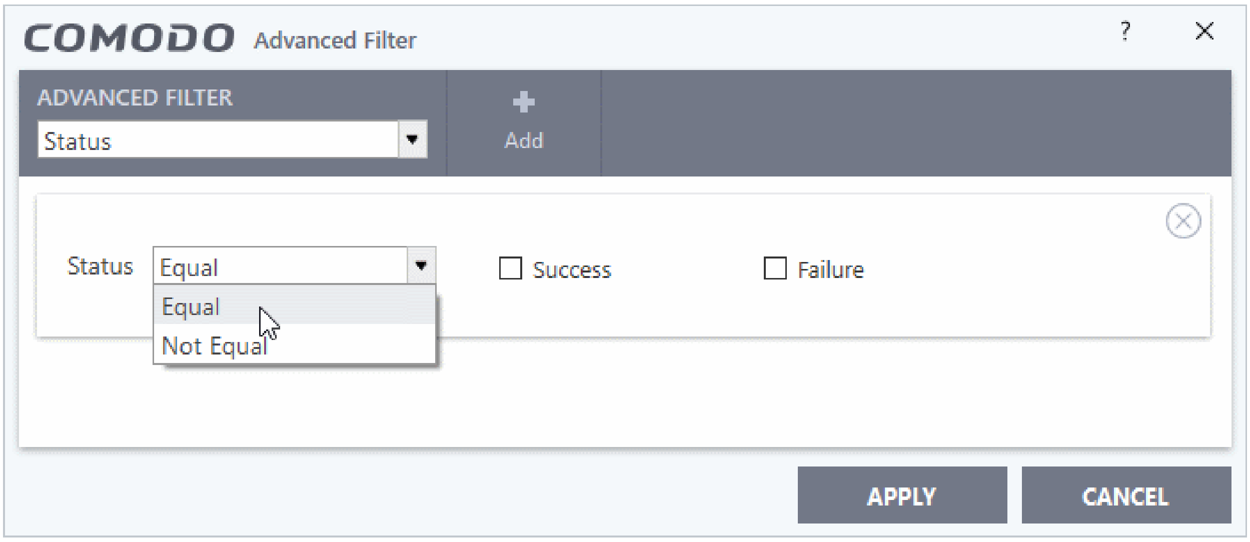
Malware Name

Malware Name Contains cuckoo

a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
b. Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Malware Name' field will be displayed. If you choose the 'Does Not Contain' option from the drop-down and enter the phrase 'cuckoo' in the text field, then all events that do not have the entry 'cuckoo' in the 'Malware Name' field will be displayed.

iv. **Status**: The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CIS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
b. Now select specific filter parameters to refine your search. The parameter available are:
    - Success: Displays events where the actions against the detected threat were successful. For example, the malware was successfully quarantined.
    - Failure: Displays events where the intended actions against the detected threat were not successful .For example, the malware was not disinfected.

Note: Multiple filters can be added in the 'Advanced Filter' pane. After adding a filter, select the next filter type and click 'Add'. You can remove filters by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the VirusScope log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

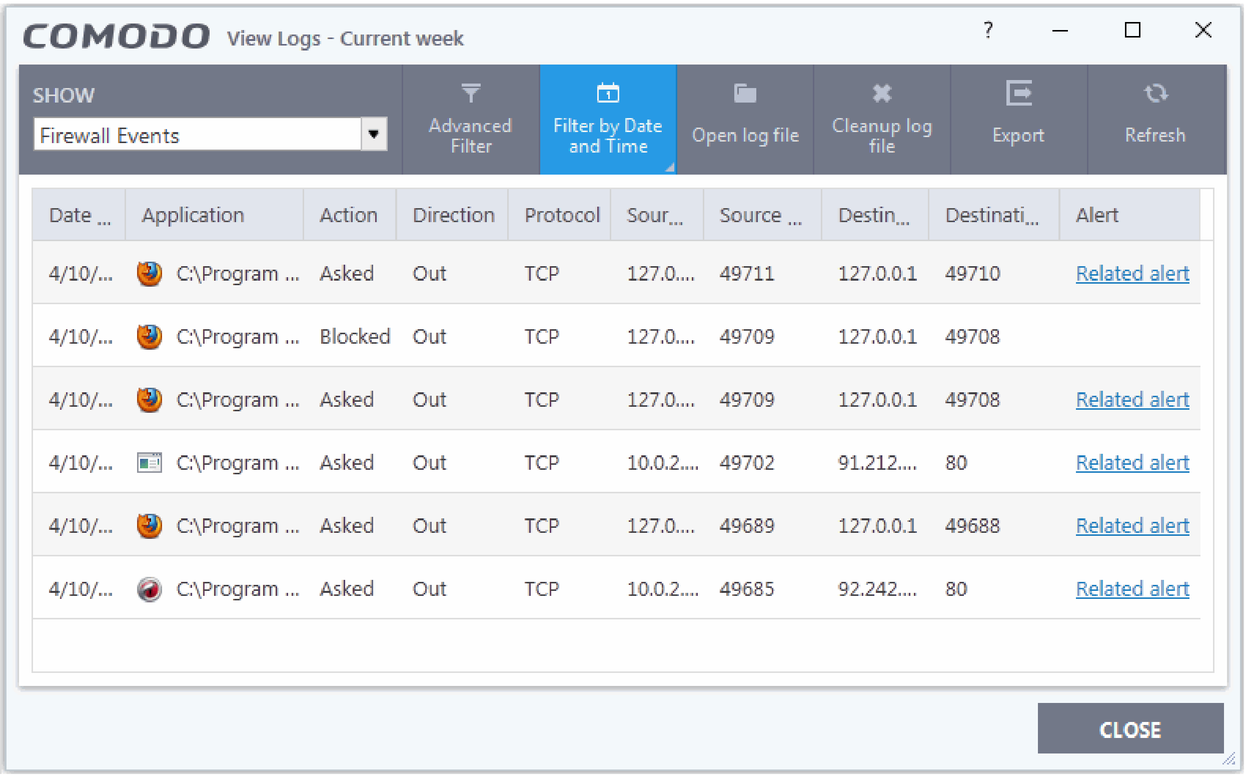
5.5.3. Firewall Logs

Comodo Internet Security records a history of all actions taken by the firewall. Firewall 'Events' are generated and recorded for various reasons - including whenever an application or process makes a connection attempt that contravenes a rule in your **Rule sets** or whenever there is a change in 'Firewall' configuration.

To view the 'Firewall' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Firewall Events' from the 'Show' drop-down

Tip: Alternatively, the 'Firewall' log screen can be accessed by clicking the number beside 'Network Intrusions' in the in the 'Firewall' pane in 'Advanced View' of the 'Home' screen



Date ...	Application	Action	Direction	Protocol	Sour...	Source ...	Destin...	Destinati...	Alert
4/10/...	C:\Program ...	Asked	Out	TCP	127.0....	49711	127.0.0.1	49710	Related alert
4/10/...	C:\Program ...	Blocked	Out	TCP	127.0....	49709	127.0.0.1	49708	
4/10/...	C:\Program ...	Asked	Out	TCP	127.0....	49709	127.0.0.1	49708	Related alert
4/10/...	C:\Program ...	Asked	Out	TCP	10.0.2....	49702	91.212....	80	Related alert
4/10/...	C:\Program ...	Asked	Out	TCP	127.0....	49689	127.0.0.1	49688	Related alert
4/10/...	C:\Program ...	Asked	Out	TCP	10.0.2....	49685	92.242....	80	Related alert

Column Descriptions

1. **Date & Time -** Indicates the precise date and time of the event.
2. **Application -** Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used.
3. **Action -** Indicates how the firewall reacted to the connection attempt. For example, whether the attempt was allowed, blocked or an alert displayed to the user so they could choose an action.
4. **Direction -** Indicates whether the connection attempt is inbound or outbound.
5. **Protocol -** The protocol used by the application that attempted to create the connection. This is usually TCP/IP, UDP or ICMP, which are the most heavily used networking protocols.
6. **Source IP -** Displays the IP address of the host that made the connection attempt. For outbound connections, this is usually the IP address of your computer. For inbound connections, it is usually the IP address of the external server.
7. **Source Port -** The port number on the host at the source IP which was used to make the connection attempt.
8. **Destination IP -** Displays the IP address of the host to which the connection attempt was made. For inbound connections, this is usually the IP address of your computer.
9. **Destination Port -** The port number on the host at the destination IP to which the connection attempt was made.
10. **Alert -** Clicking the 'Related Alert' link shows details of the alert displayed during the event.

Note: Firewall alerts are displayed only if 'Do not show pop up alerts' is disabled in firewall settings. See **General Firewall Settings** for more details.

- To export firewall logs to a HTML file, click the 'Export' button or right click inside the log viewer and choose 'Export'.
- To open a saved CIS log file, click the 'Open log file' button. .

- To refresh the 'Firewall' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the 'Firewall' logs click the 'Cleanup log file' button.
- You can sort the entries by ascending \ descending order by clicking on the respective column headers

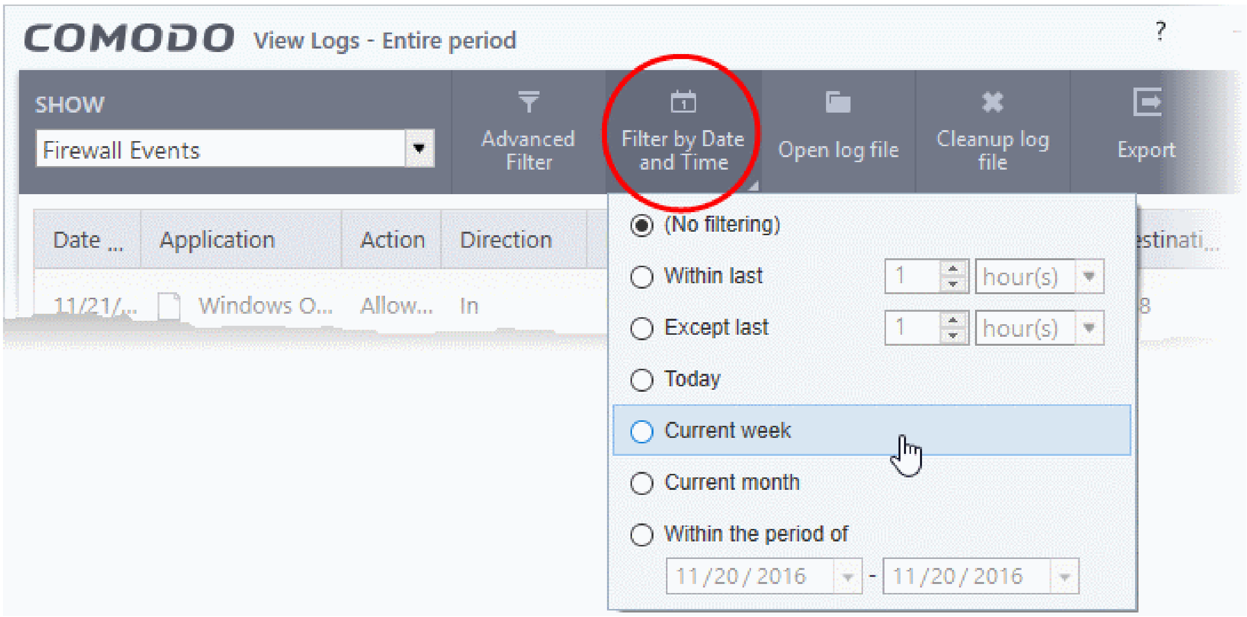
5.5.3.1. Filtering Firewall Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

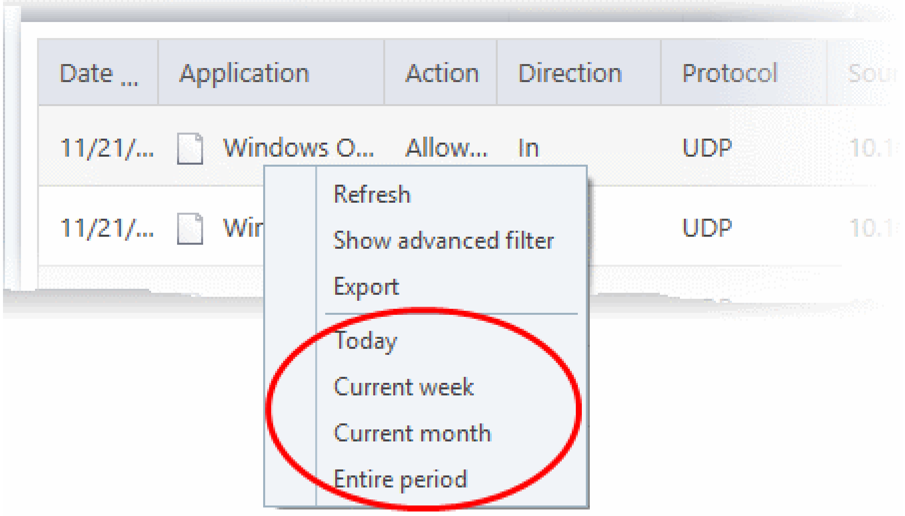
Preset Time Filters:

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



- **No filtering -** Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Display all logged events for today.
- **Current Week -** Display all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month** - Display all events logged during this month.
- **Custom Filter** - Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

Having chosen a **preset time filter**, you can further refine the displayed events according to specific filters. Following are available filters for 'Firewall' logs and their meanings:

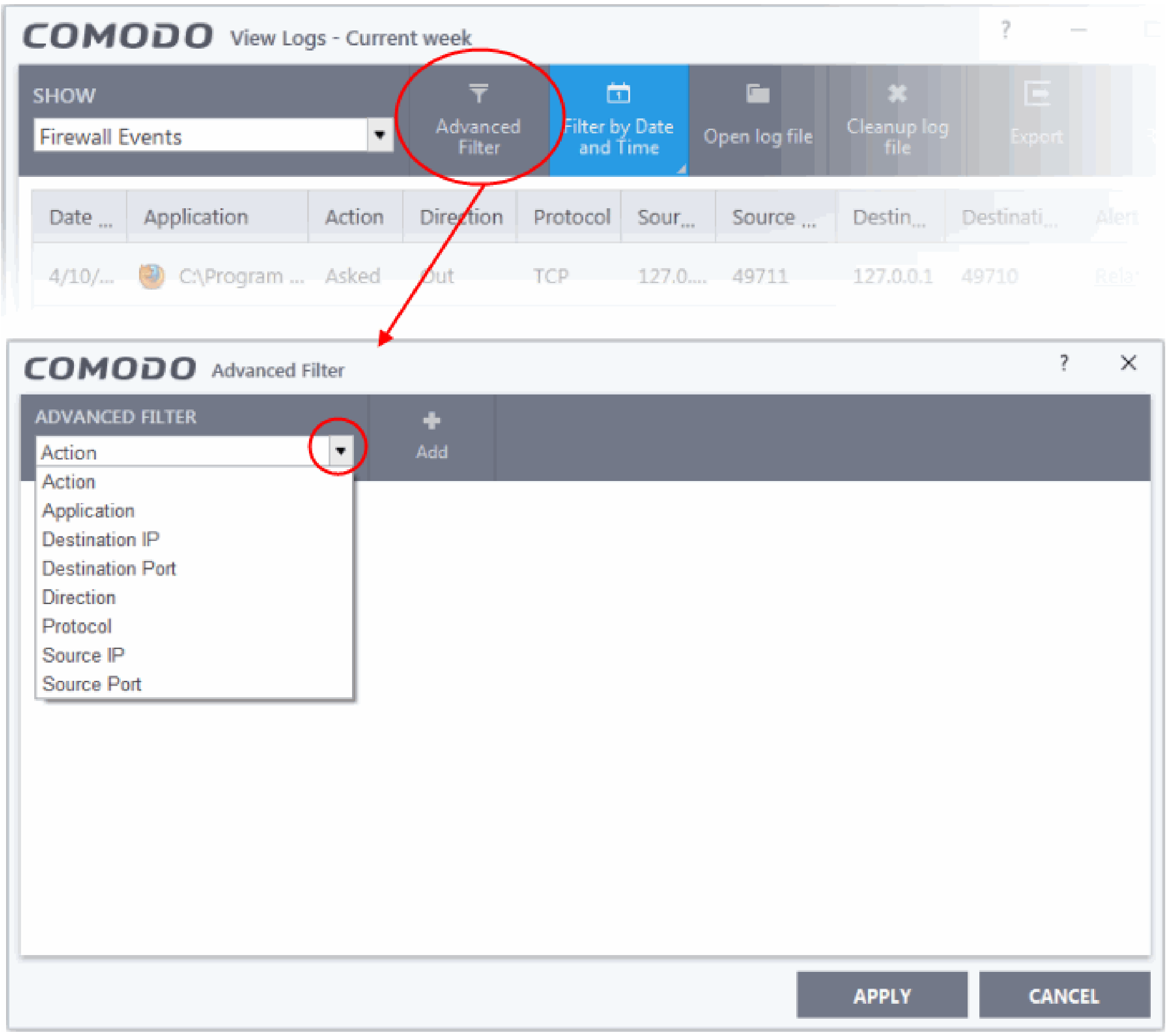
- **Action -** Displays events according to the response (or action taken) by the firewall
- **Application -** Displays only the events propagated by a specific application
- **Destination IP -** Displays only the events with a specific target IP address
- **Destination Port -** Displays only events that involved a specific target port number
- **Direction -** Displays only the events of Inbound or Outbound nature
- **Protocol -** Displays only events that involved a specific protocol
- **Source IP -** Displays only the events that originated from a specific IP address
- **Source Port -** Displays only events that involved a specific source port number

To configure Advanced Filters for Firewall events

1. Click the 'Advanced Filter' button on the title bar or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

The 'Advanced Filter' interface for Firewall Events will open.

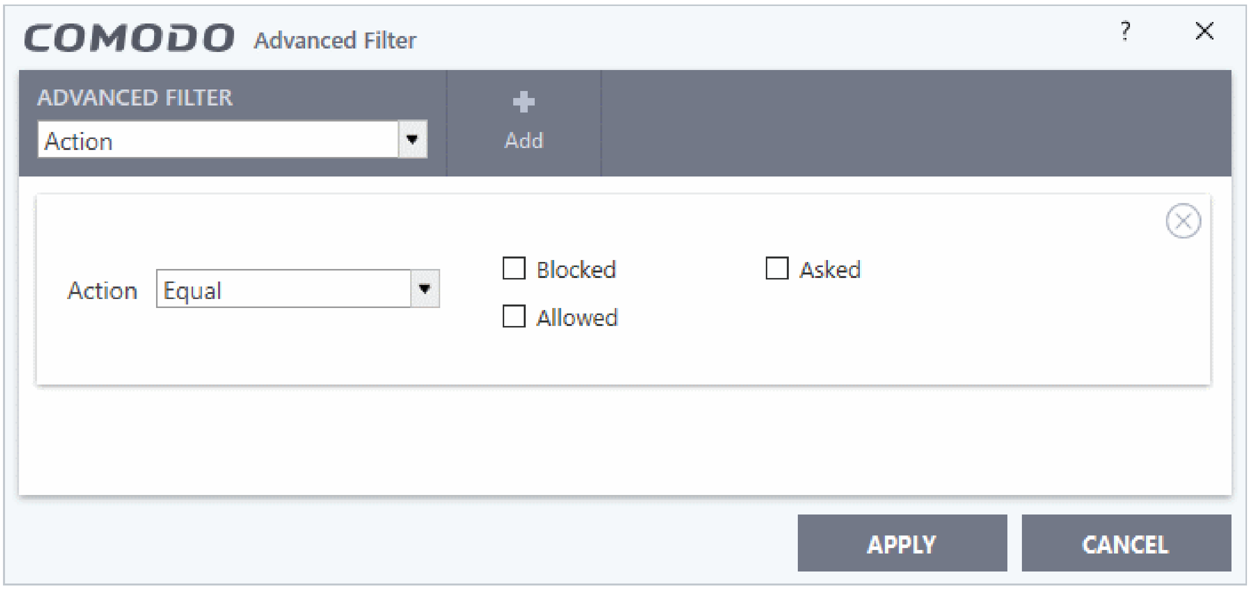
2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.



There are 8 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

i. **Action:** Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



Action: Equal

□ Blocked
□ Asked
□ Allowed

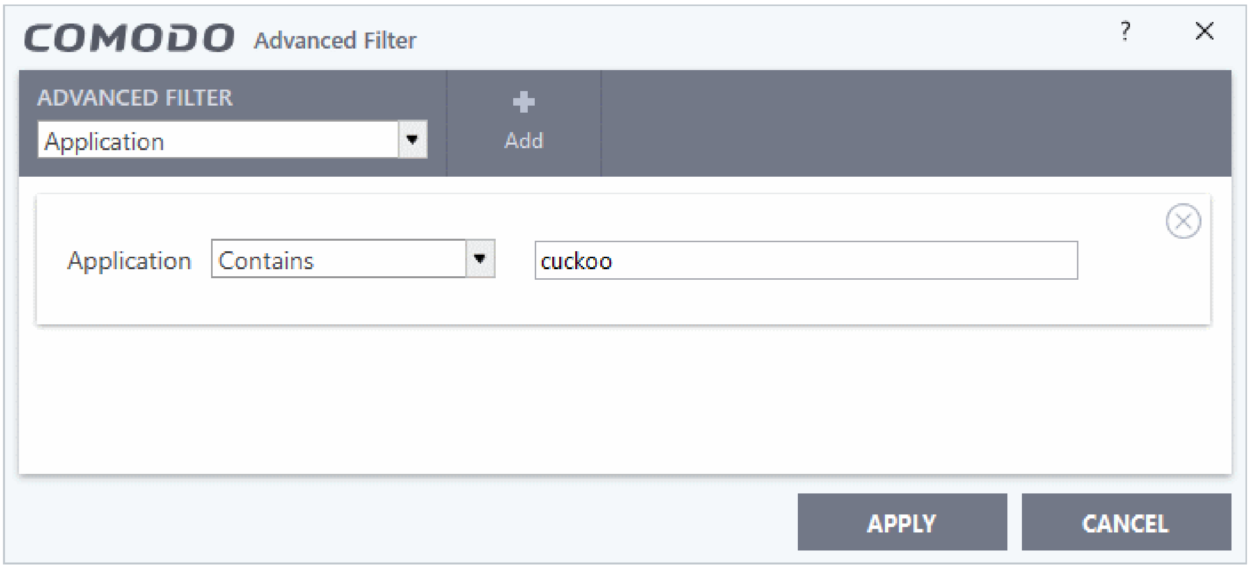
You should now choose the actions by which you want to filter the logs:

a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:

- Blocked: Displays events where CIS prevented the connection
- Allowed: Displays events where the connection was allowed to proceed
- Asked: Displays events where an alert was shown to the user so they could choose whether or not to allow the connection

ii. **Application**: Selecting the 'Application' option displays a drop-down box and text entry field.



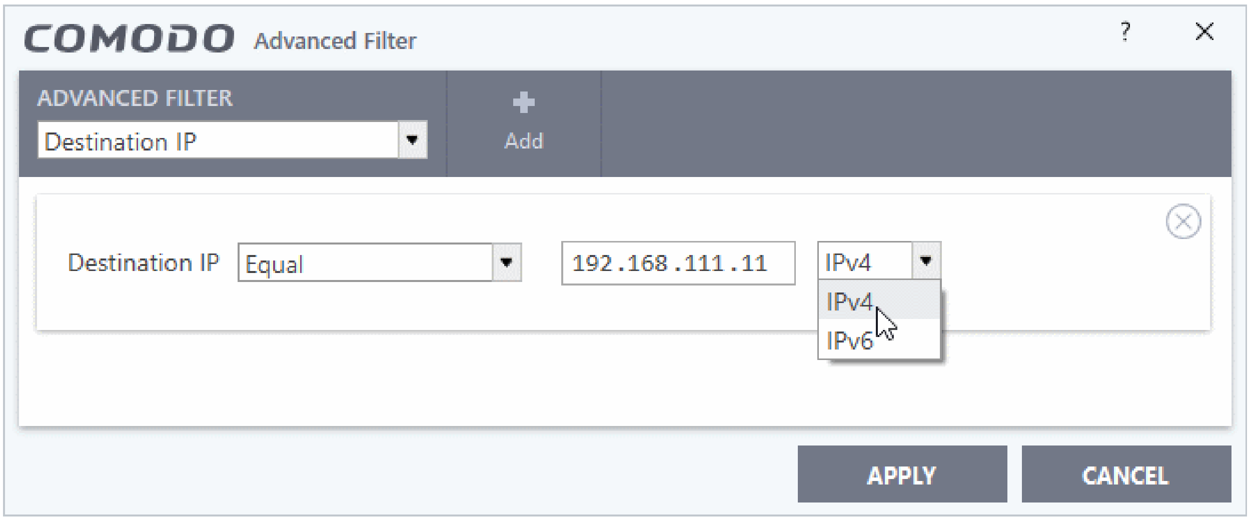
Application: Contains — cuckoo

a) Select 'Contains' or 'Does Not Contain' option from the drop-down box.

b) Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' from and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column will be displayed. If you select 'Does Not Contain' and enter the phrase 'cuckoo' in the text field, then all events that do not have the entry 'cuckoo' in the 'Application' column will be displayed.

iii. **Destination IP:** Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.



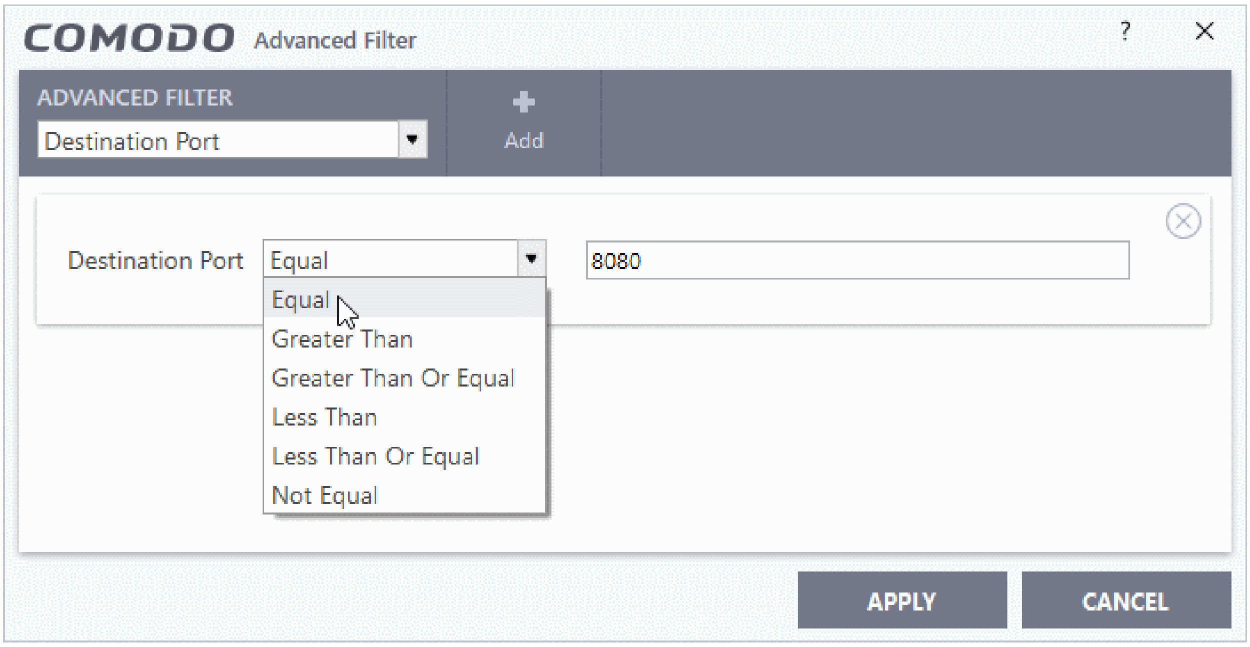
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Select 'IPv4' or 'IPv6' from the drop-down box.

c) Enter the IP address of the destination server or host, to filter the events that involve the connection attempts from/to that destination server or host.

For example, if you choose 'Contains' option from the drop-down, select IPv4 and enter 192.168.111.11 in the text field, then all events containing the entry '192.168.111.11' in the 'Destination IP' column will be displayed.

iv. **Destination Port:** Selecting the 'Destination Port' option displays a drop-down box and text entry field.



a) Select any one of the option the drop-down.

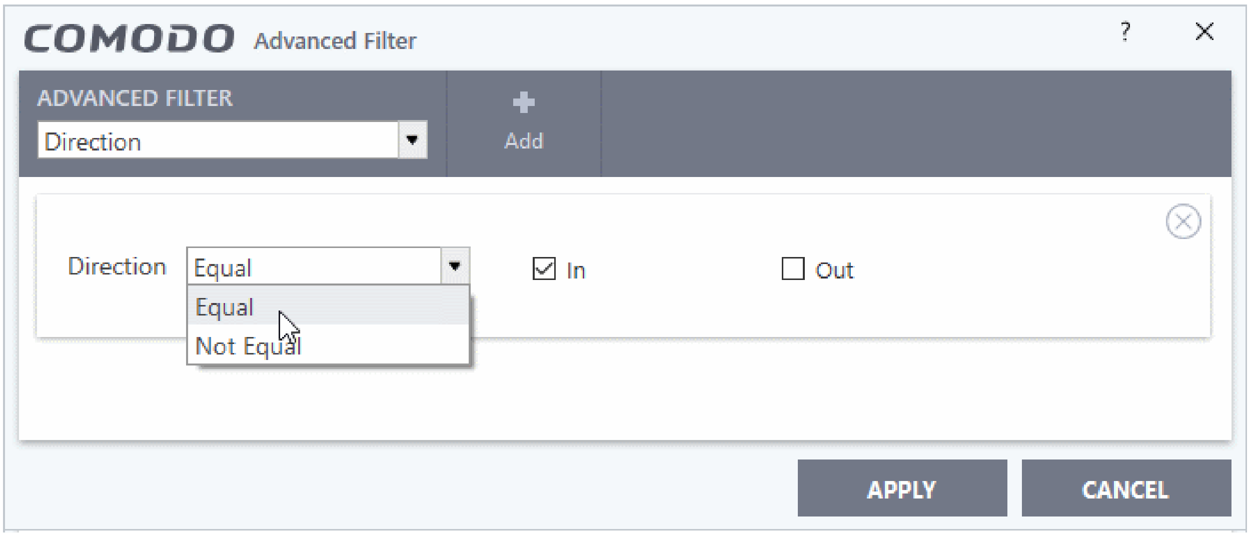
- Equal
- Greater than
- Greater than or Equal
- Less than
- Less than or Equal

- Not Equal

b) Now enter the destination port number in the text entry field.

For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

v. **Direction:** Selecting the 'Direction' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



Direction: Direction
Direction: Equal ☑ In ☐ Out

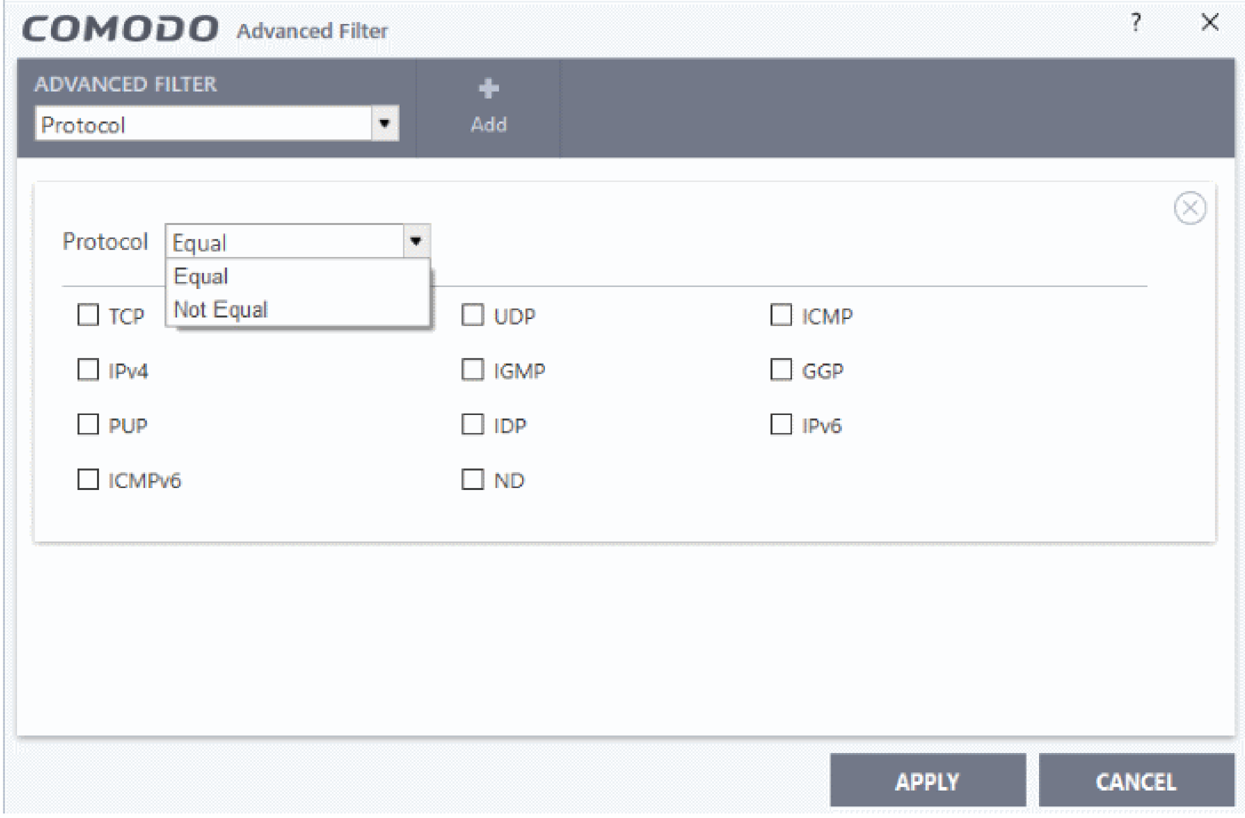
a) Select 'Equal' or 'Not Equal' option from the drop-down. 'Not Equal' will invert your selected choice.

b) Now select the check box of the specific filter parameters to refine your search. The parameters available are:

- In: Displays a list of events involving inbound connection attempts
- Out: Displays a list of events involving outbound connection attempts

For example, if you choose 'Equal' option from the drop-down and select the 'In' checkbox, then all inbound connection attempts will be displayed.

vi. **Protocol**: Selecting the 'Protocol' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



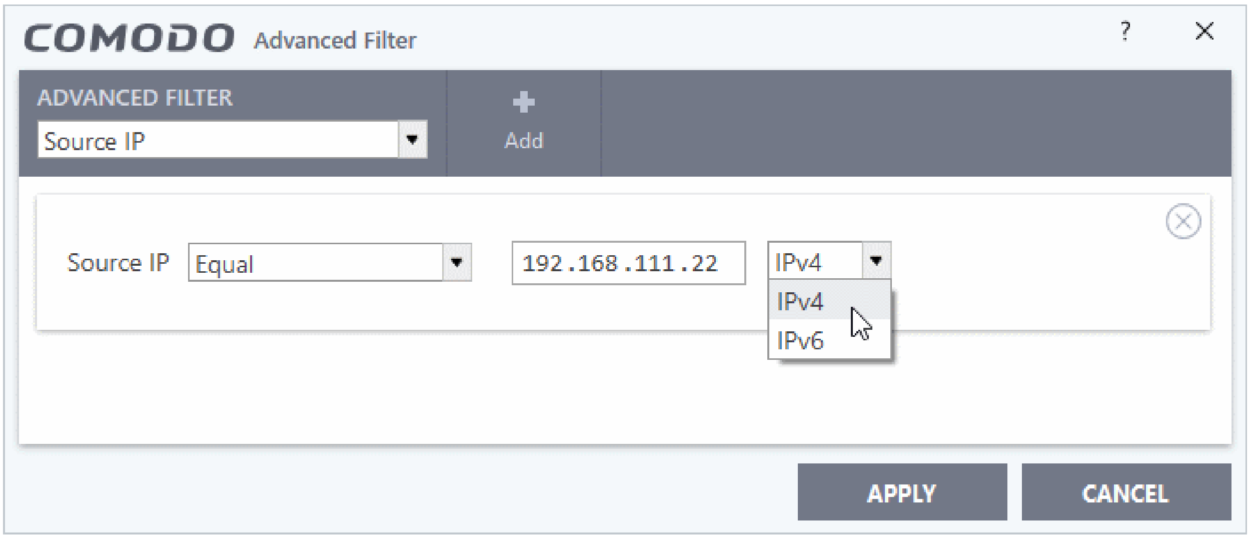
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:

- TCP
- UDP
- ICMP
- IPV4
- IGMP
- GGP
- PUP
- IDP
- IPV6
- ICMPV6
- ND

For example, if you choose 'Equal' option from the drop-down and select the 'TCP' checkbox, then all connection attempts involving TCP protocol will be displayed.

vii. **Source IP:** Selecting the 'Source IP' option displays two drop-down boxes and a set specific filter parameters that can be selected or deselected.



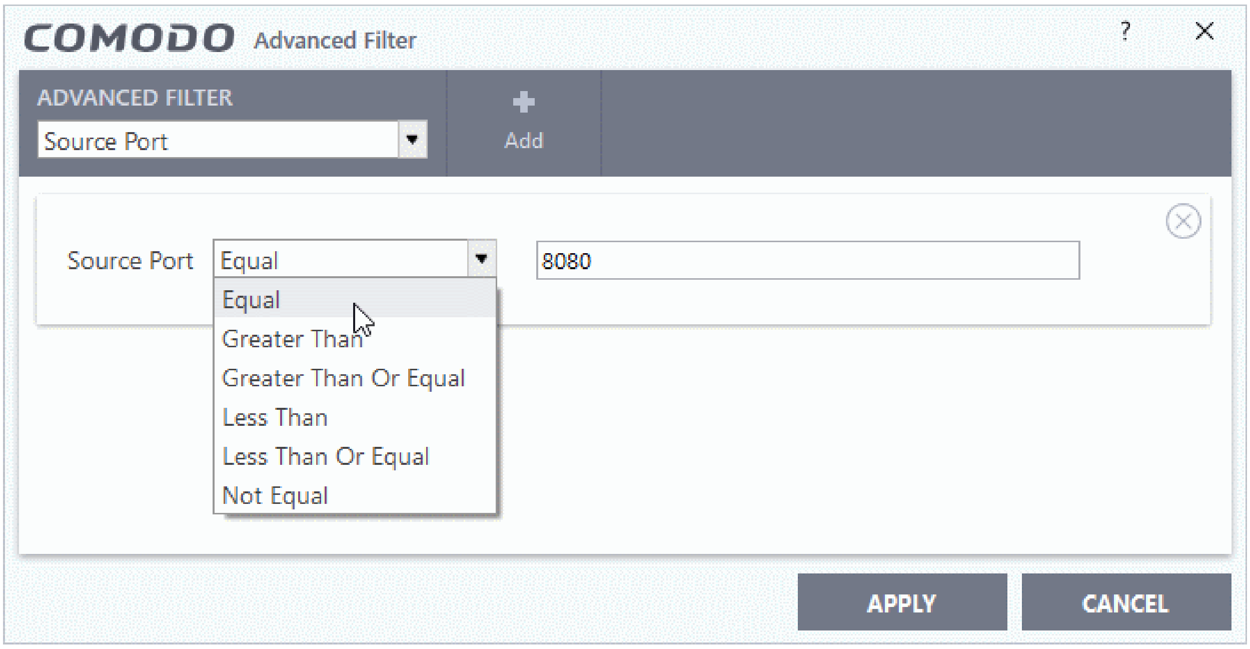
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Select 'IPv4' or 'IPv6' from the drop-down box.

c) Enter the IP address of the source server or host, to filter the events that involve the connection attempts from/to that source server or host system.

For example, if you choose 'Contains' then select IPv4 and enter 192.168.111.22 in the text field, then all events containing the entry '192.168.111.11' in the 'Source IP' column will be displayed.

viii. **Source Port:** Selecting the 'Source Port' option displays a drop-down box and and text entry field.



a) Select any one of the following option the drop-down box:

- Equal
- Greater than
- Greater than or Equal
- Less than
- Less than or Equal
- Not Equal

b) Now enter the destination port number in the text entry field.

For example, if you choose 'Equal' and enter 8080 in the text field, then all events containing the entry '8080' in the 'Source Port' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

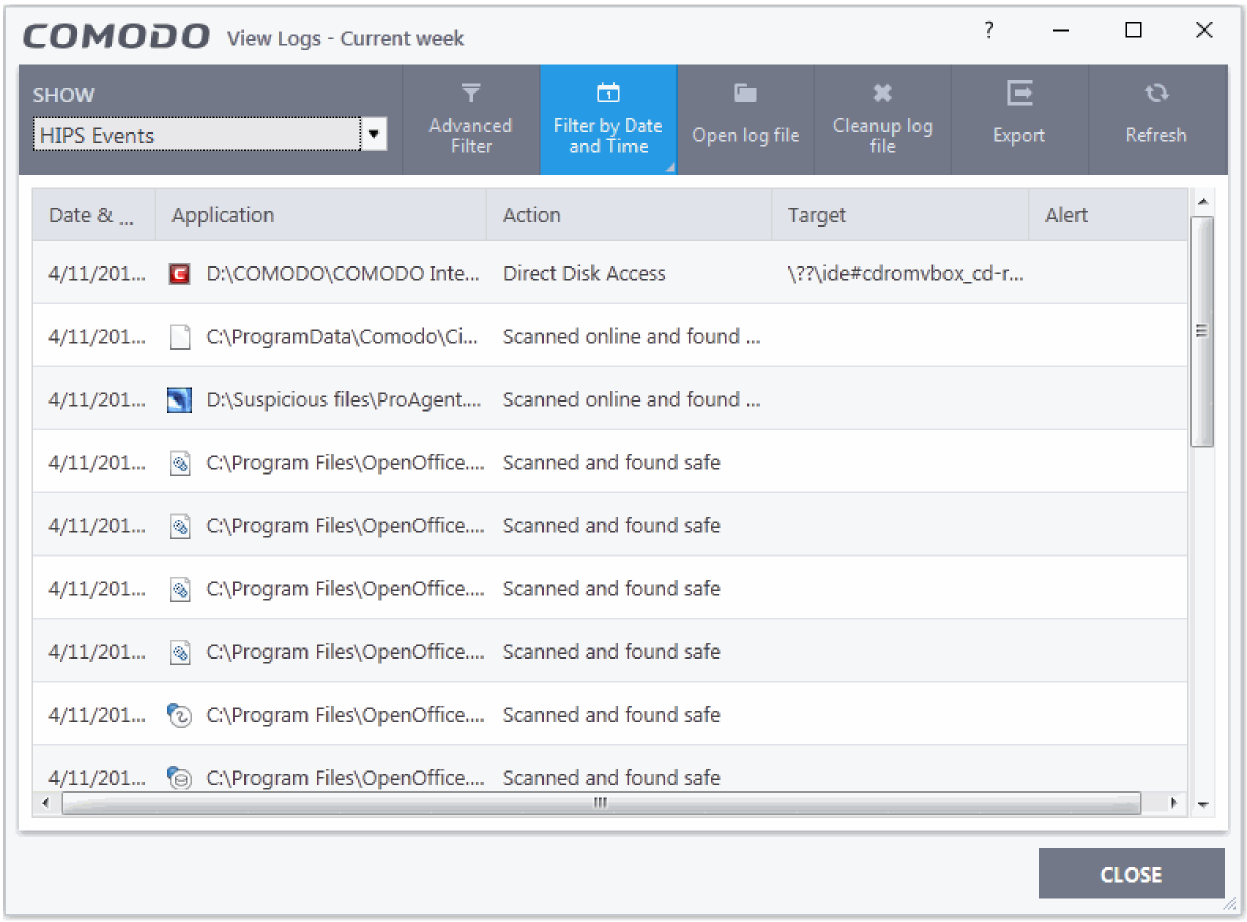
- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.5.4. HIPS Logs

CIS keeps a record of all actions taken by its host intrusion prevention system (HIPS). HIPS events are generated for various reasons. These include changes in 'HIPS' settings, when an application or process attempts to access restricted areas or when an action occurs that contravenes your **HIPS Rulesets**.

To view 'HIPS' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'HIPS Events' from the 'Show' drop-down



Date & ...	Application	Action	Target	Alert
4/11/201...	D:\COMODO\COMODO Inte...	Direct Disk Access	\??\ide#cdromvbox_cd-r...	
4/11/201...	C:\ProgramData\Comodo\Ci...	Scanned online and found ...		
4/11/201...	D:\Suspicious files\ProAgent....	Scanned online and found ...		
4/11/201...	C:\Program Files\OpenOffice....	Scanned and found safe		
4/11/201...	C:\Program Files\OpenOffice....	Scanned and found safe		
4/11/201...	C:\Program Files\OpenOffice....	Scanned and found safe		
4/11/201...	C:\Program Files\OpenOffice....	Scanned and found safe		
4/11/201...	C:\Program Files\OpenOffice....	Scanned and found safe		
4/11/201...	C:\Program Files\OpenOffice....	Scanned and found safe		

Column Descriptions

1. **Date & Time -** Indicates the precise date and time of the event.

2. **Application -** Indicates the application or process that propagated the event. If the application has no icon then the default system icon for executable files are used.
3. **Action -** If the action was allowed to proceed then this column will show the result of that action. Click the 'Related Alert' link to see the alert that was displayed at the time. If the action was not allowed then this column will state 'Block File'.
4. **Target -** Location of the target file, COM interface or registry key accessed by the process.
5. **Alert -** Clicking the 'Related Alert' link shows details of the alert displayed during the event.

Note: HIPS alerts are only displayed if 'Do not show pop up alerts' is disabled in HIPS Settings. See **HIPS Settings** for more details.

- To export the 'HIPS' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open log file' button
- To refresh the 'HIPS' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu
- To clear the 'HIPS' logs click the 'Cleanup log file' button
- You can sort the entries by ascending \ descending order by clicking on the respective column headers

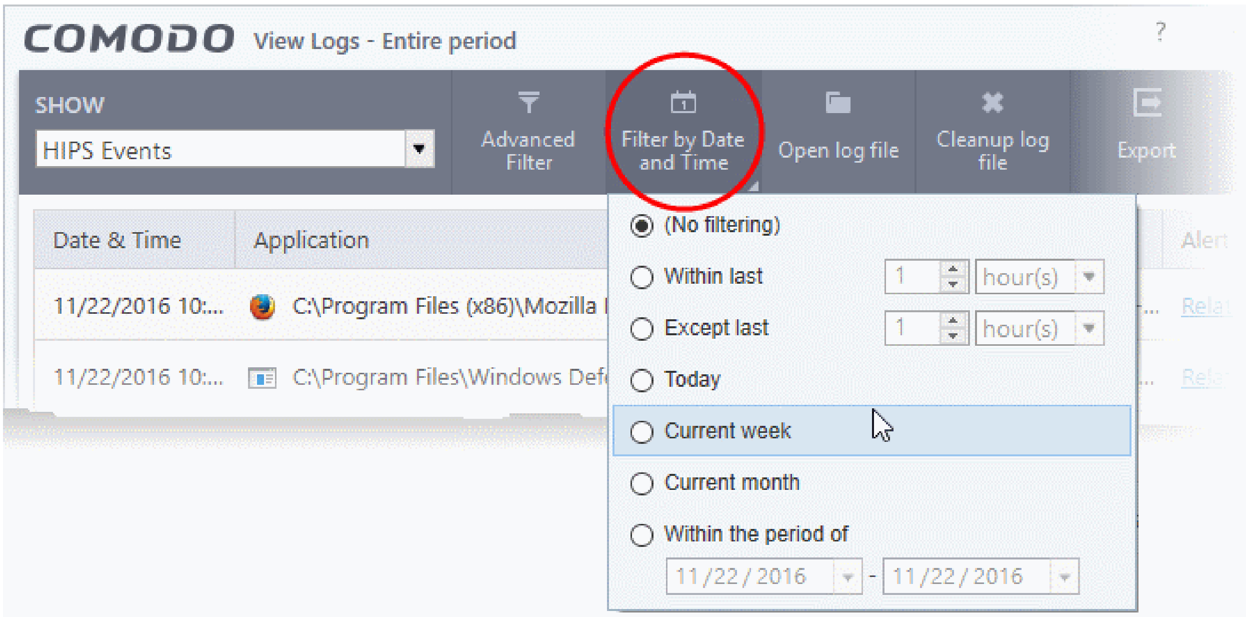
5.5.4.1. Filtering HIPS Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

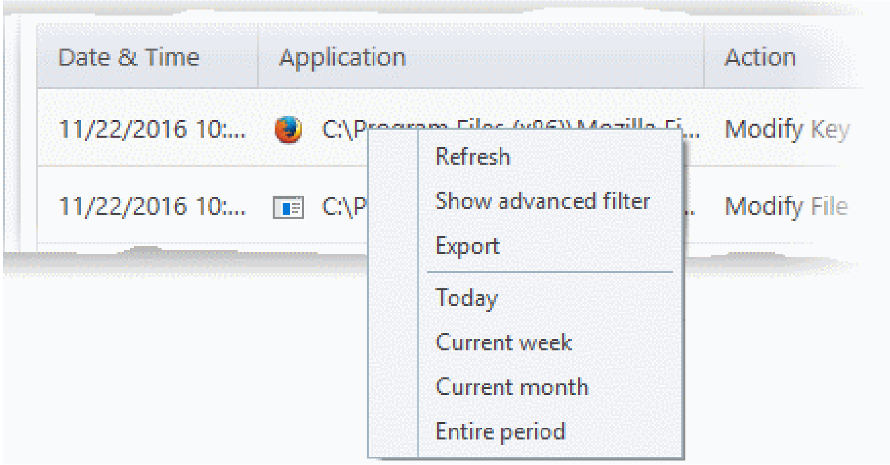
- Click the 'Filter by Date and Time' button at the top to filter the logs for a selected time period:



- **No filtering -** Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.

- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Display all logged events for today.
- **Current Week -** Display all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month** - Display all events logged during this month.
- **Custom Filter** - Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

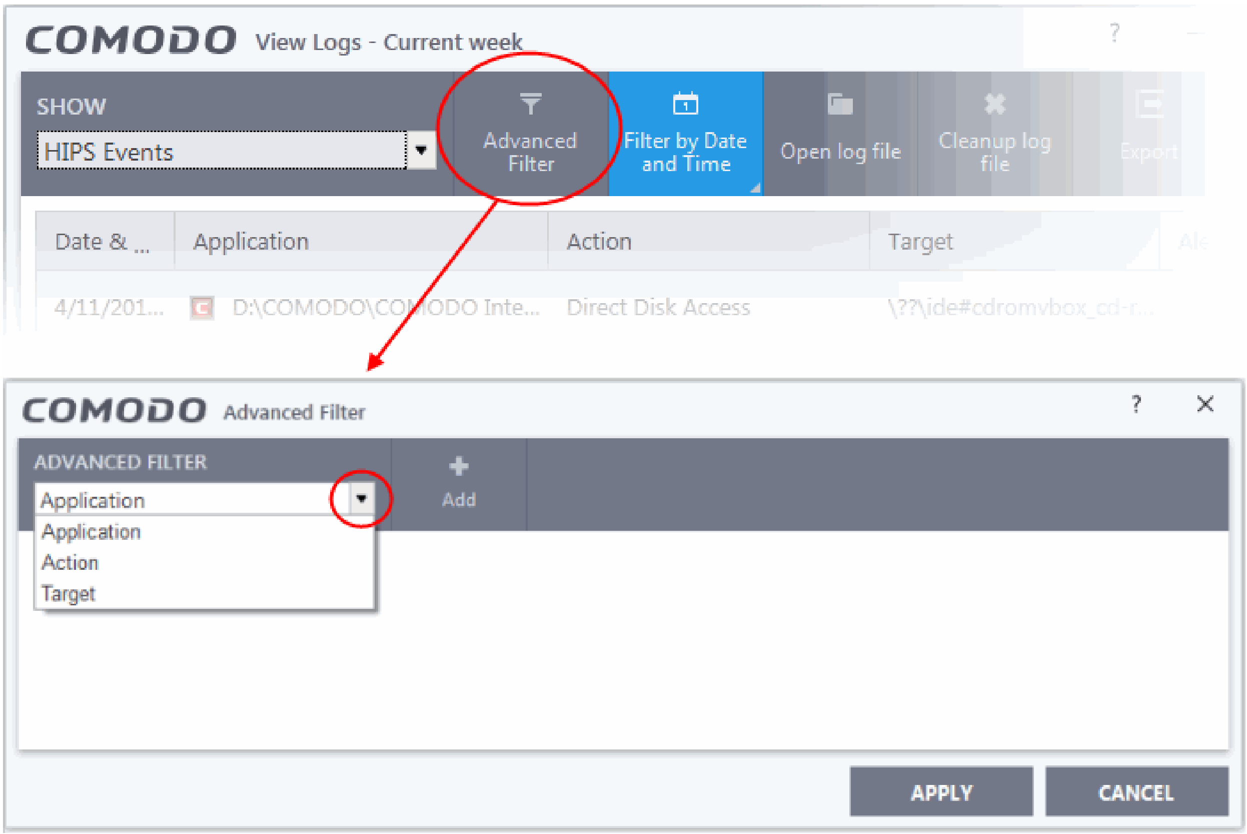
Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. Following are available filters for HIPS logs and their meanings:

- **Application -** Displays only events propagated by a specific application
- **Action -** Displays events according to the response (or action taken) by HIPS
- **Target** - Displays only the events that involved a specified target application

To configure Advanced Filters for HIPS events

1. Click the 'Advanced Filter' button on the title bar or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

The 'Advanced Filter' interface for HIPS Events will open.

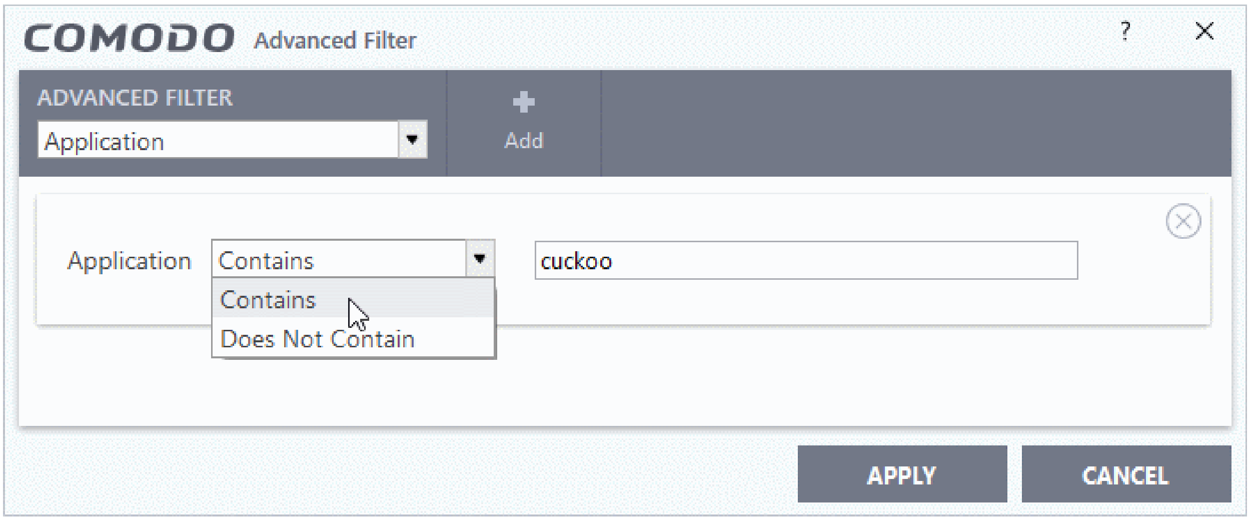


2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.

There are 3 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following options are available in the 'Advanced Filter' drop-down:

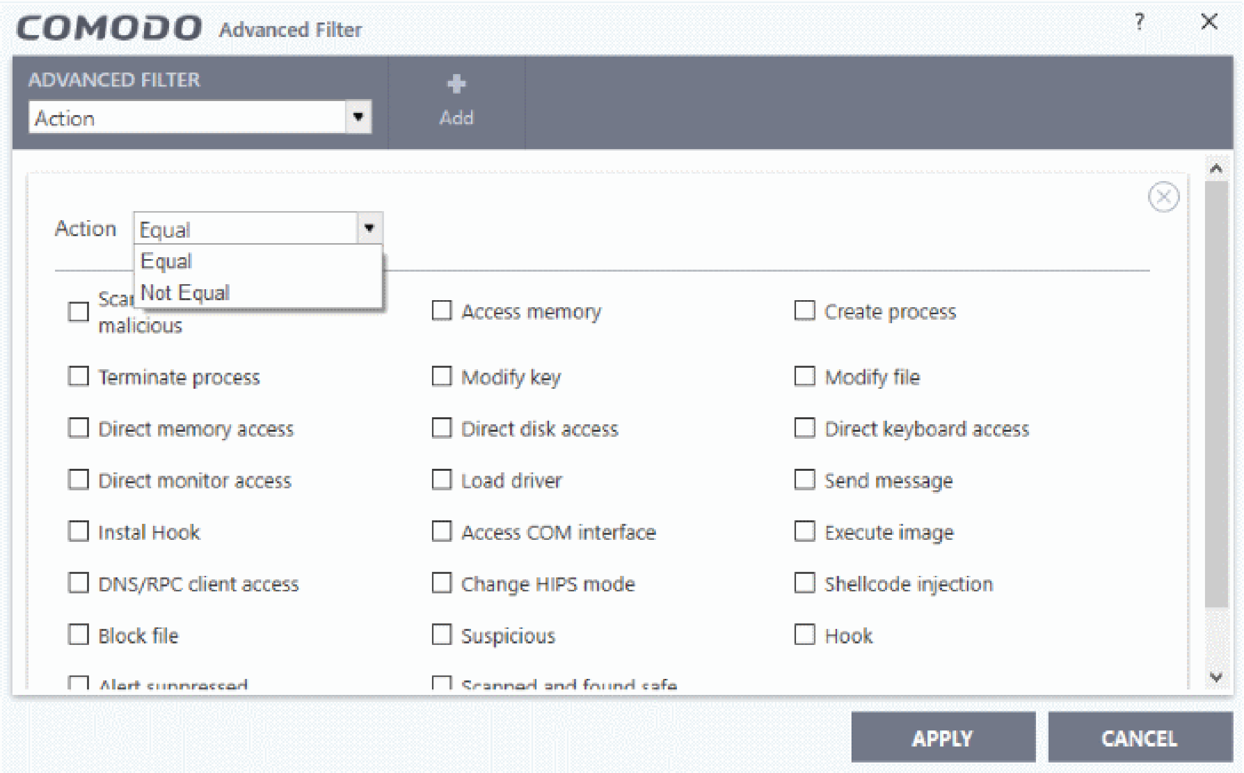
i. **Application**: Adding the 'Application' option displays a drop-down field and text entry field.



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
b) Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column will be displayed. If you choose 'Does Not Contain' from the drop-down and enter the phrase 'cuckoo', then all events that do not have the entry 'cuckoo' in the 'Application' column will be displayed.

ii. **Action**: Selecting the 'Action' option displays a drop down menu and a set of filter parameters that can be selected or deselected.



a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

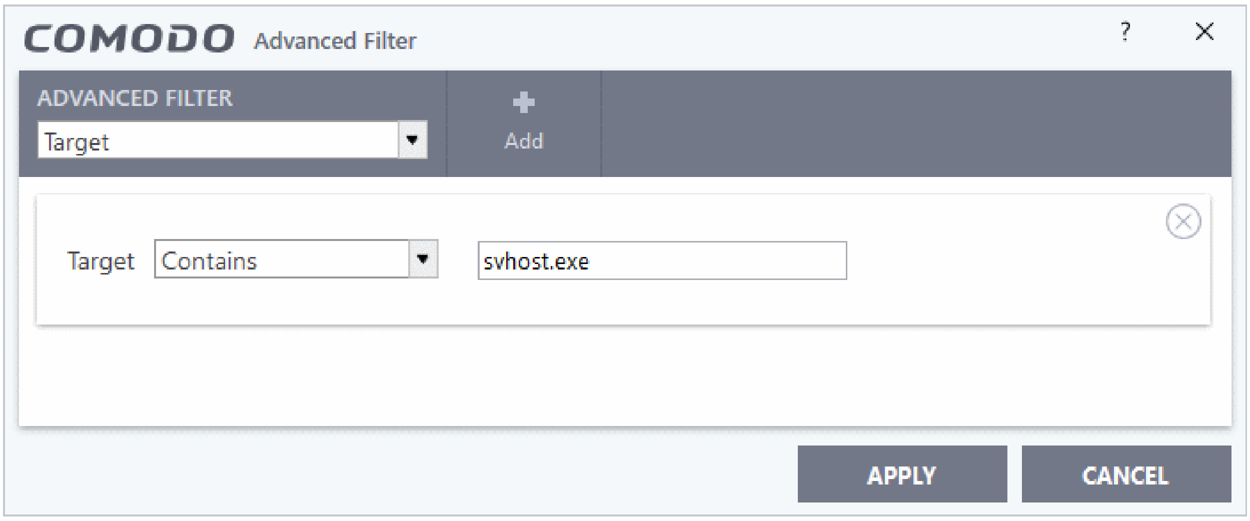
b) Now select the actions to refine your search, so as to display only those events involving the selected actions. The options available are:

- Scanned online and found malicious
  - Access memory
  - Create process
  - Terminate process
  - Modify key
  - Modify file
  - Direct memory access
  - Direct disk access
  - Direct keyboard access
  - Direct monitor access
  - Load driver
  - Send message
  - Install Hook
  - Access COM interface
  - Execute image
  - DNS/RPC client access
  - Change HIPS Mode
  - Shellcode injection
  - Block file
  - Suspicious

- Hook
- Alert Suppressed
- Scanned and found safe

For example, if you choose 'Equal' and select 'Create process', only events involving the creation of a process by applications will be displayed. If you choose 'Not Equal' and select 'Modify key', then all events that do not have the entry 'Modify key' in the 'Actions' column will be displayed. You can select more than one action from this interface, as required.

iii. **Target**: Selecting the 'Target' option displays a drop-down menu and text entry field.



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
b) Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' and enter the phrase 'svchost.exe' in the text field, then all events containing the entry 'svchost.exe' in the 'Target' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'svchost.exe', then all events that do not have the entry 'svchost.exe' in the 'Target' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

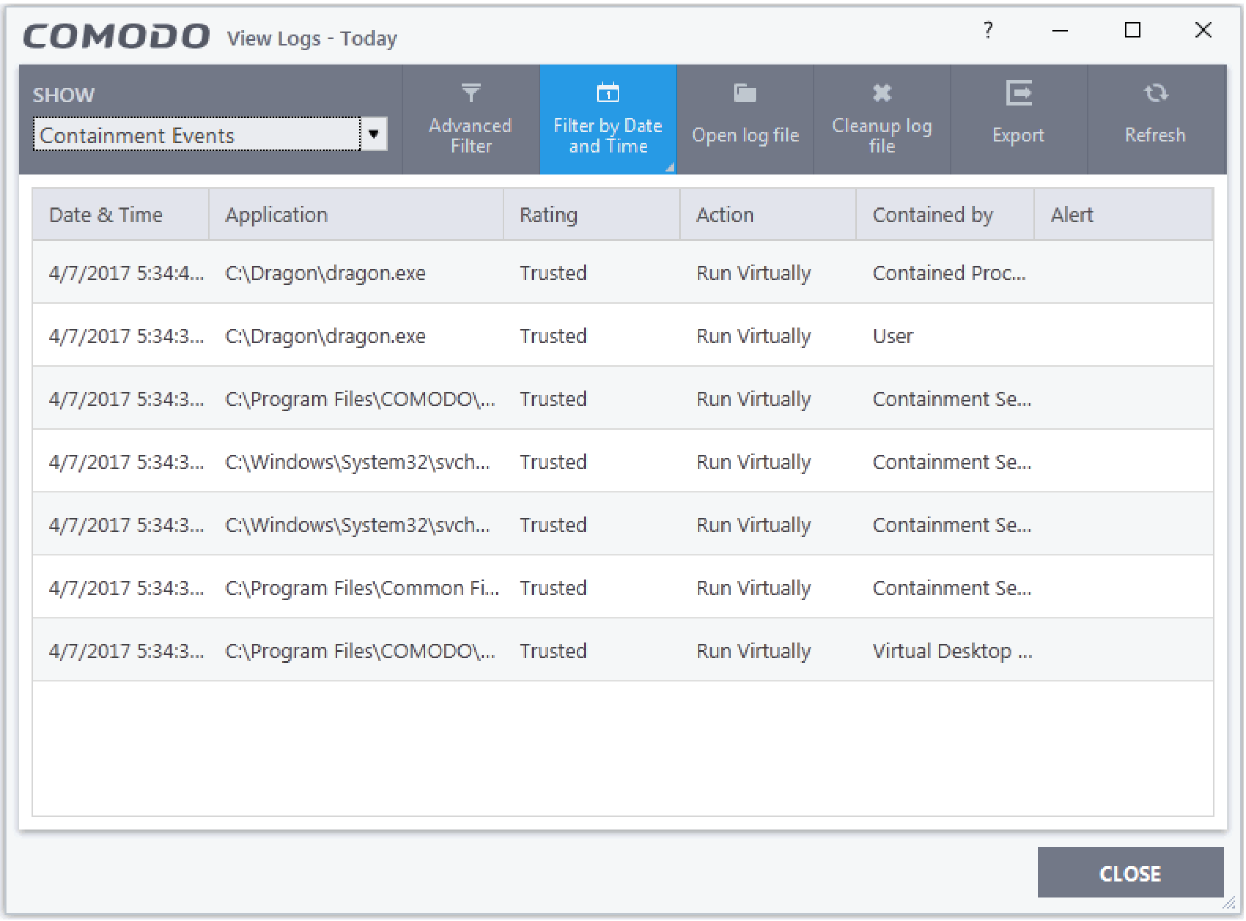
- Click 'Apply' for the filters to be applied to the 'HIPS' log viewer. Only those HIPS entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.5.5. Containment Logs

Comodo Internet Security keeps a record of all actions taken by the 'Containment' feature. Events include when applications are automatically or manually run in the auto-containment and when the Virtual Desktop is used.

To view 'Containment' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Containment Events' from the 'Show' drop-down



Date & Time	Application	Rating	Action	Contained by	Alert
4/7/2017 5:34:4...	C:\Dragon\dragon.exe	Trusted	Run Virtually	Contained Proc...	
4/7/2017 5:34:3...	C:\Dragon\dragon.exe	Trusted	Run Virtually	User	
4/7/2017 5:34:3...	C:\Program Files\COMODO\...	Trusted	Run Virtually	Containment Se...	
4/7/2017 5:34:3...	C:\Windows\System32\svch...	Trusted	Run Virtually	Containment Se...	
4/7/2017 5:34:3...	C:\Windows\System32\svch...	Trusted	Run Virtually	Containment Se...	
4/7/2017 5:34:3...	C:\Program Files\Common Fi...	Trusted	Run Virtually	Containment Se...	
4/7/2017 5:34:3...	C:\Program Files\COMODO\...	Trusted	Run Virtually	Virtual Desktop ...	

Column Descriptions

1. **Date & Time**- Indicates the precise date and time of the event.
2. **Application -** Shows the installation path of the application that was run inside the container.
3. **Rating** - Indicates the file rating of the executable file as per Comodo file rating system, i.e., whether the file is 'Trusted', 'Malicious' or 'Unrecognized'.
4. **Action -** Indicates the restriction level imposed on the application by the container.
5. **Contained by -** Indicates which CIS service or policy was responsible for contained the item.
6. **Alert -** Clicking the 'Related Alert' link shows details of the alert displayed during the event.

Note: The containment will display alerts when the installer of an unknown application requires administrator, or elevated, privileges to run. The alerts are only displayed if 'Do not show privilege elevation alerts' is disabled in containment settings. See **Containment Settings** for more details.

- To export the 'Containment' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open log file' button
- To refresh the 'Containment' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu
- To clear the 'Containment' logs click the 'Cleanup log file' button
- You can sort the entries by ascending \ descending order by clicking on the respective column headers

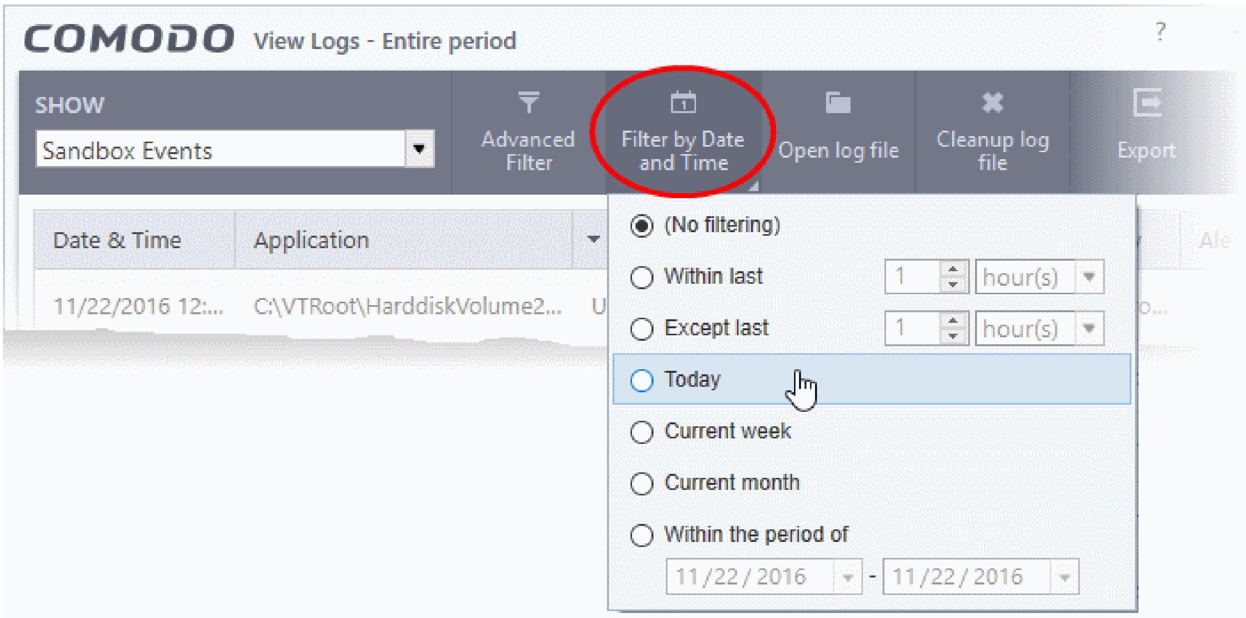
5.5.5.1. Filtering Containment Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

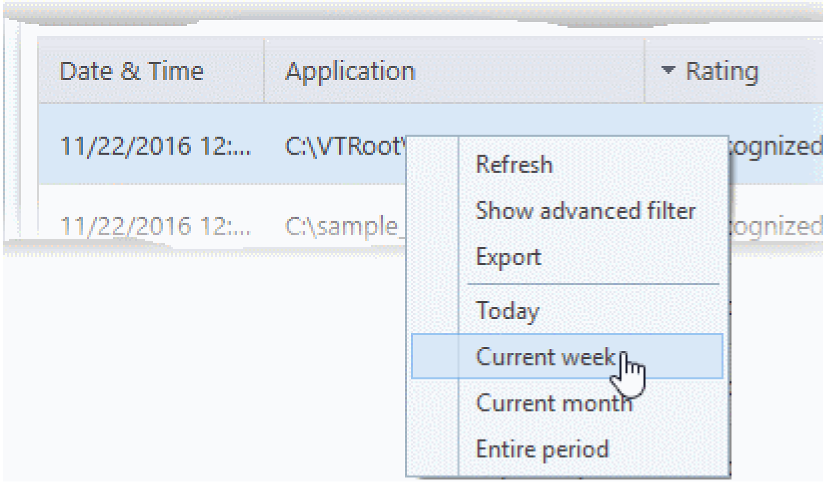
Preset Time Filters:

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



- **No filtering -** Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Display all logged events for today.
- **Current Week -** Display all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month** - Display all events logged during this month.
- **Custom Filter** - Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

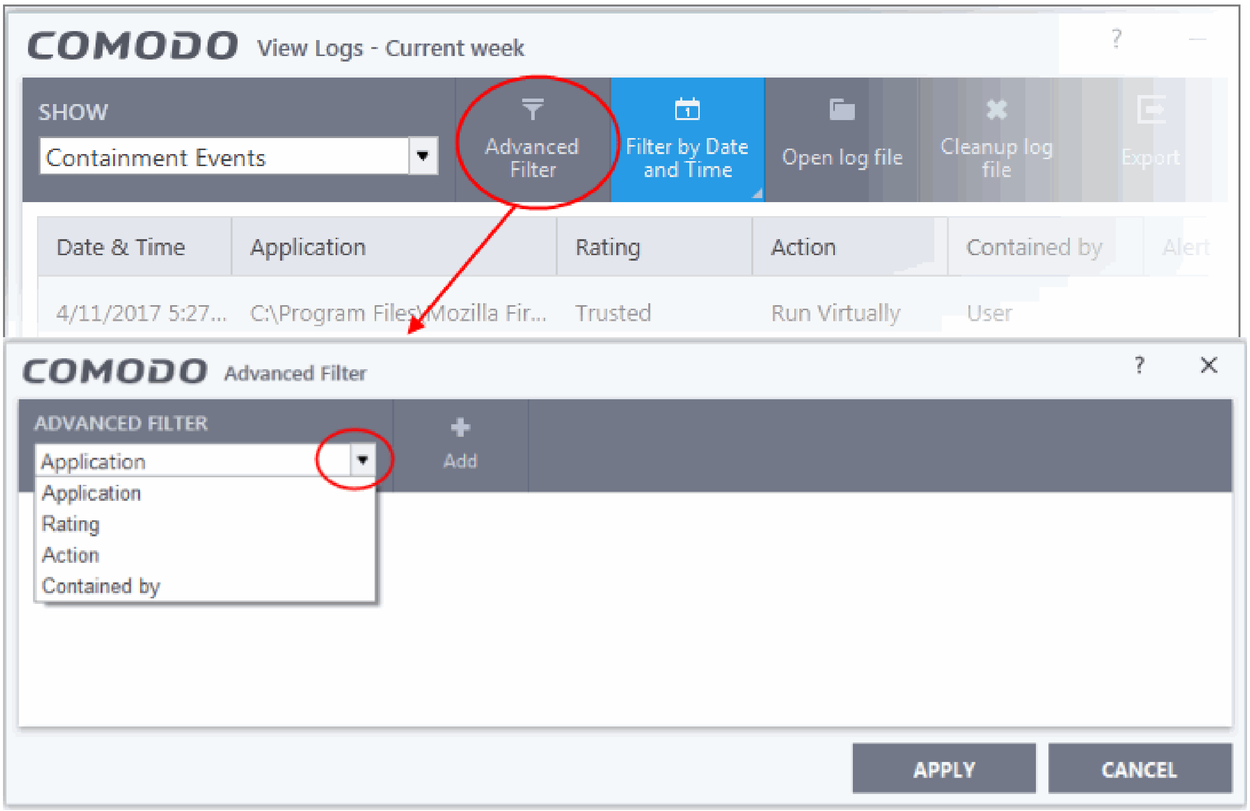
Having chosen a **preset time filter**, you can further refine the displayed events according to specific filters. Following are available filters for 'Containment' logs and their meanings:

- **Application -** Displays only the events propagated by a specific application
- **Rating -** Displays only the events propagated by a specific rated application
- **Action -** Displays events according to the response (or action taken) by the Containment
- **Contained by -** Displays only the events according to the containment method used

To configure filters for Containment Events

1. Click the 'Advanced Filter' button on the title bar (or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu).

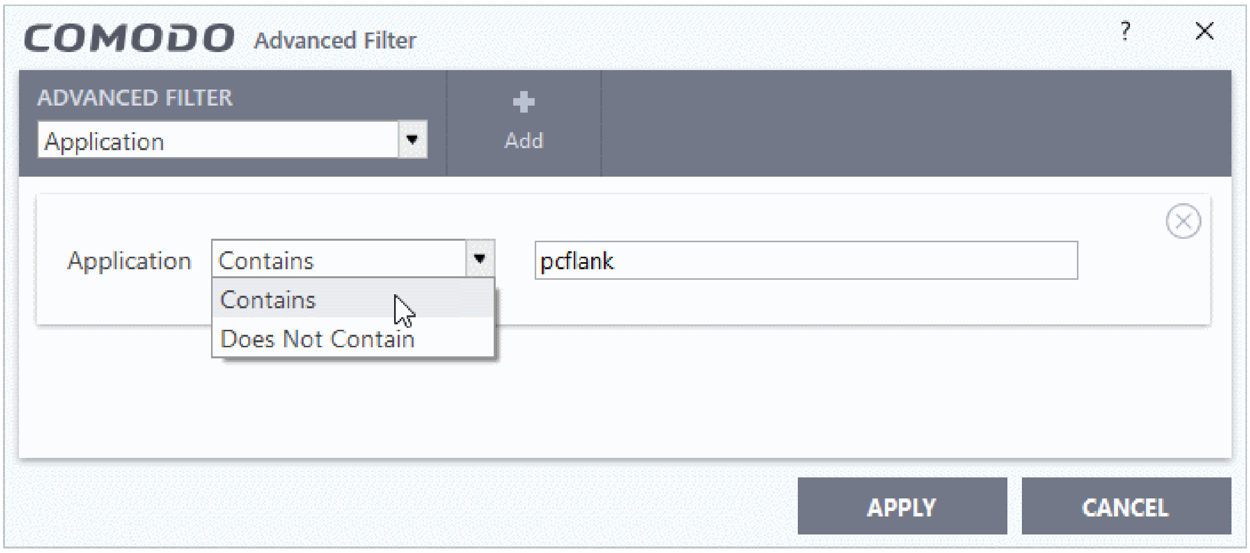
The 'Advanced Filter' interface for containment events will open:



2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.

   There are 4 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

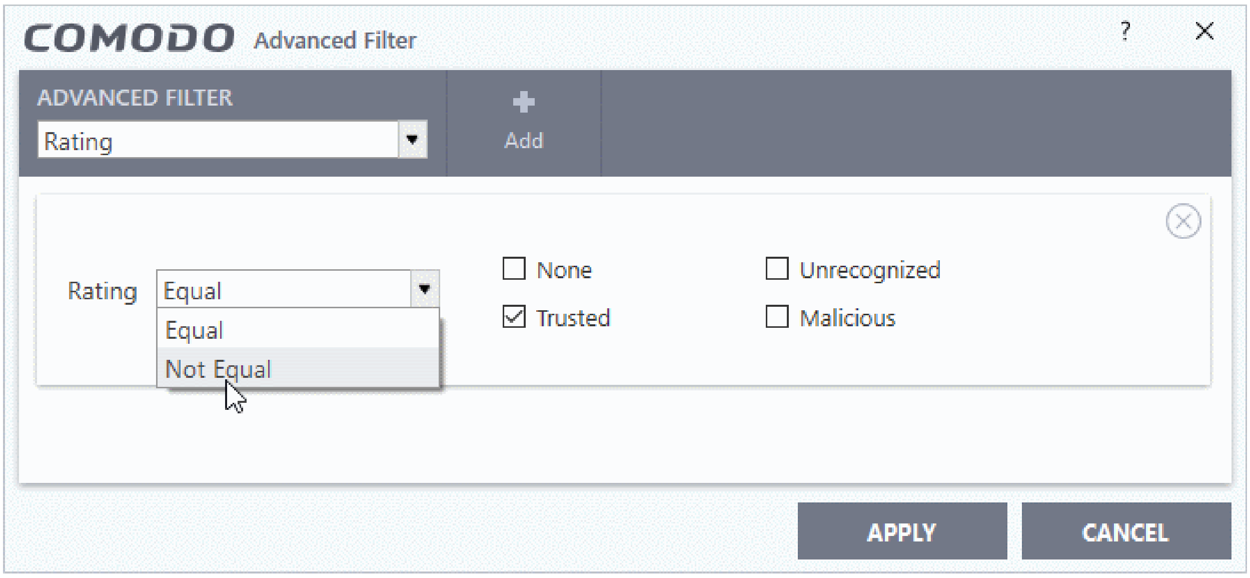
   i. **Application**: Adding the 'Application' option displays a drop-down field and text entry field.



   a) Select 'Contains' or 'Does Not Contain' from the drop-down menu.
   b) Enter the search criteria for filtering the logs in the text field.

   For example, if you choose 'Contains' and enter the phrase 'pcflank' in the text field, then all events containing the entry 'pcflank' in the 'Application' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'pcflank', then all events that do not have the entry 'pcflank' in the 'Application' column will be displayed.

   ii. **Rating**: Selecting the 'Rating' option displays a drop down menu and a set of filter parameters that can be selected or deselected.

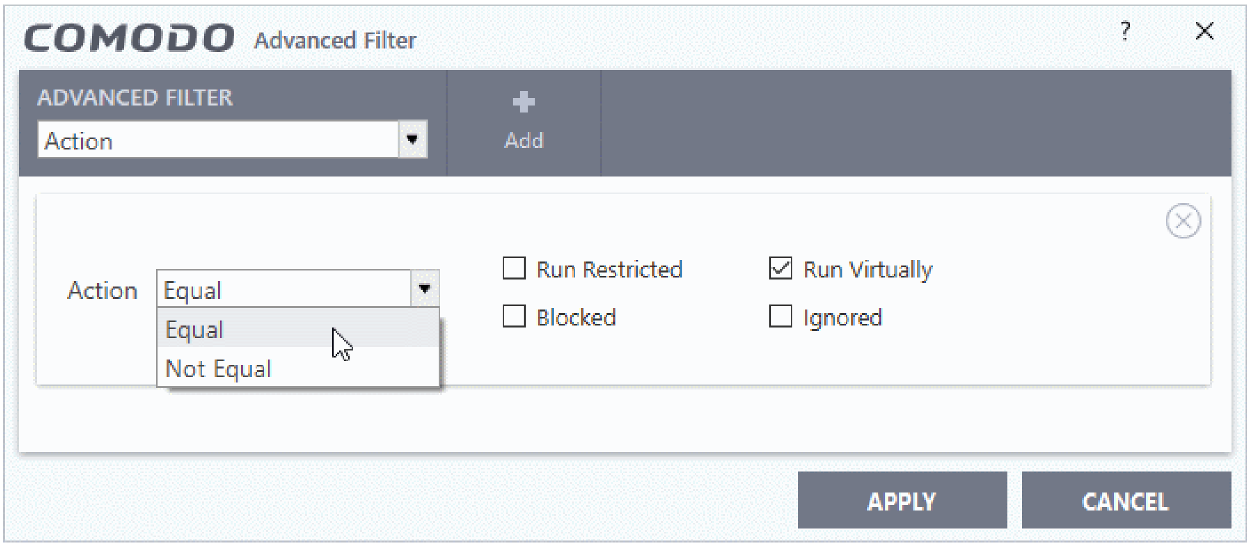


   a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
   b) Now select the file ratings to refine your search. The options available are:

- None
- Unrecognized
- Trusted
- Malicious

For example, if you choose 'Equal' and select the 'Unrecognized' file rating, only the containment events involving applications that are categorized as 'Unrecognized' will be displayed. If you choose 'Not Equal' and choose 'Malicious' file rating, then all events that do not have the entry 'Malicious' in the 'Rating' column will be displayed. You can select more than one file rating from this interface, as required.

iii. **Action**: Selecting the 'Action' option displays a drop down menu and a set of filter parameters that can be selected or deselected.



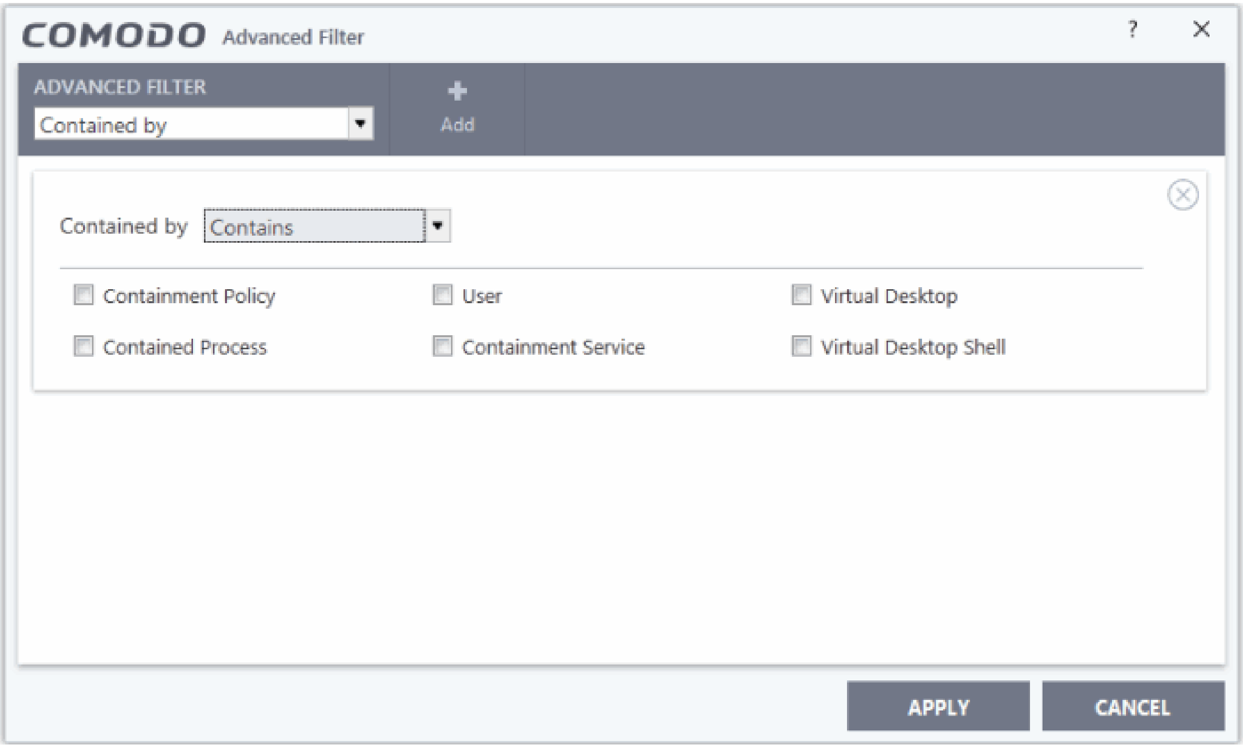
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the restriction level(s) applied by the container to the applications, either automatically of as chosen by the user from the alert. The options available are:

- Run Restricted
- Run Virtually
- Blocked
- Ignored

For example, if you choose 'Equal' from the drop-down and select 'Run Virtually', only the events of applications that are run inside the container will be displayed. If you choose 'Not Equal' and select 'Blocked', then all events that do not have the entry 'Blocked' in the 'Action' column will be displayed. You can select more than one checkbox as required.

iv. **Contained by**: Selecting the 'Contained by' option displays a drop down menu and a set of filter parameters that can be selected or deselected.



Contained by: Contains

□ Containment Policy
□ User
□ Virtual Desktop
□ Contained Process
□ Containment Service
□ Virtual Desktop Shell

a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.

b) To refine your search, select the source(s) by which the applications were contained. The options available are:

- Containment Policy
- User
- Virtual Desktop
- Contained Process
- Containment Service
- Virtual Desktop Shell

For example, if you choose 'Contains' and select the 'User' checkbox, then only events involving applications that were manually run inside the container will be displayed. If you choose 'Does Not Contain' and select the 'Containment Policy' checkbox, then all events that do not have the entry 'Containment Policy' in the 'Contained by' column will be displayed. You can select more than one checkbox options from this interface, as required.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Containment' log viewer. Only those 'Contained' entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.5.6. Website Filtering Logs

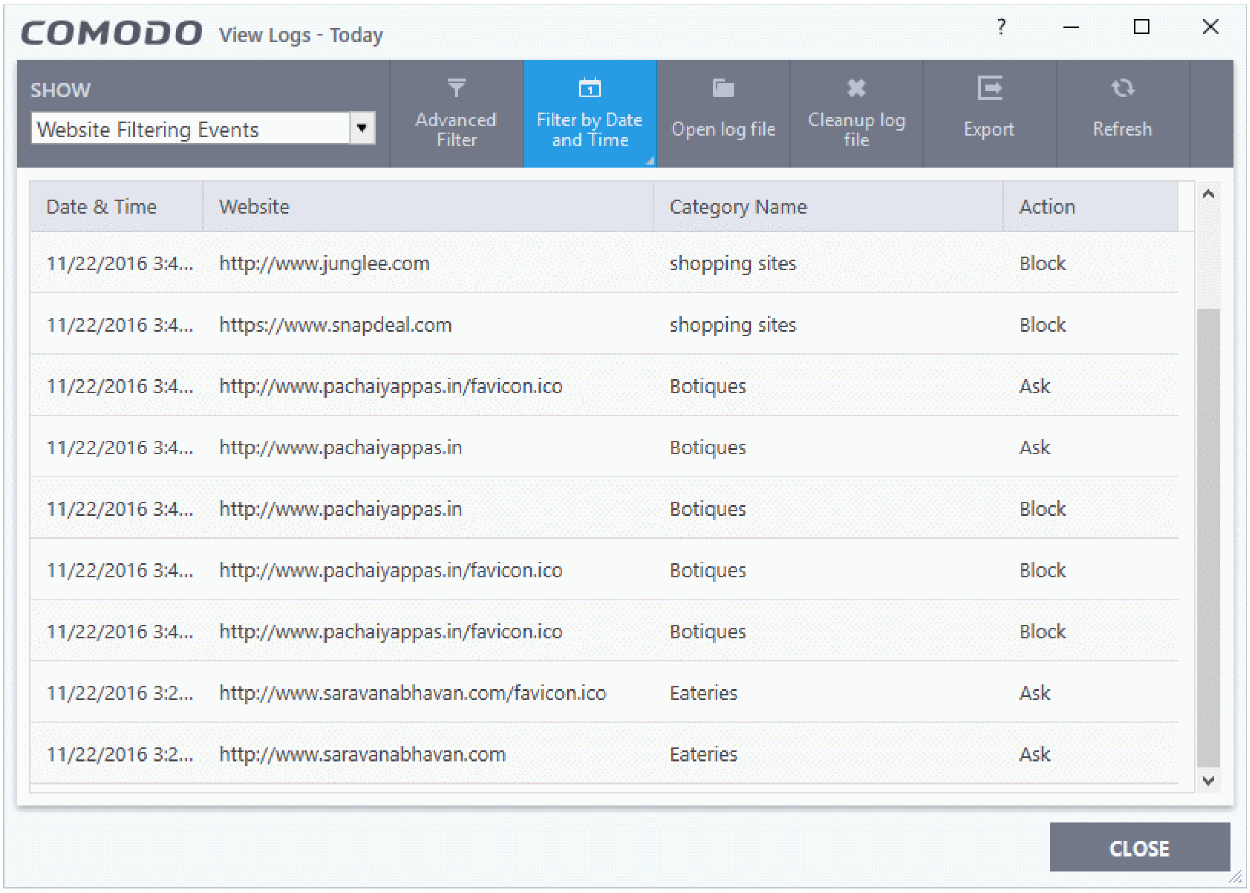
Website filter logs are a record of all websites blocked (or allowed) by the website filtering module.

Background Note: You can create rules to allow or block access to specific websites for particular users under 'Advanced Settings' > 'Website Filtering'. See '**Website Filtering**', for more details on configuring the 'Website Filter'. The 'Website Filtering' log enables you to analyze the attempts made by the other users to access the

blocked or allowed websites.

To view 'Website Filtering' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Website Filtering Events' from the 'Show' drop-down



Date & Time	Website	Category Name	Action
11/22/2016 3:4...	http://www.junglee.com	shopping sites	Block
11/22/2016 3:4...	https://www.snapdeal.com	shopping sites	Block
11/22/2016 3:4...	http://www.pachaiyappas.in/favicon.ico	Botiques	Ask
11/22/2016 3:4...	http://www.pachaiyappas.in	Botiques	Ask
11/22/2016 3:4...	http://www.pachaiyappas.in	Botiques	Block
11/22/2016 3:4...	http://www.pachaiyappas.in/favicon.ico	Botiques	Block
11/22/2016 3:4...	http://www.pachaiyappas.in/favicon.ico	Botiques	Block
11/22/2016 3:2...	http://www.saravanabhavan.com/favicon.ico	Eateries	Ask
11/22/2016 3:2...	http://www.saravanabhavan.com	Eateries	Ask

Column Descriptions

1. **Date & Time -** Indicates the precise date and time of the event.
2. **Website -** Shows the address of the website that was blocked or allowed as per the rules configured in the 'Website Filtering' interface.
3. **Category -** Indicates the category to which the website belongs. As defined in the Website Filtering settings.
4. **Action -** Indicates the action taken by the Website Filtering on the website. For example, whether the website was allowed or blocked to the user, or whether an alert was displayed so they could make a choice.

    - To export the 'Website Filtering' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
    - To open a stored CIS log file, click the 'Open log file' button .
    - To refresh the 'Website Filtering' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
    - To clear the logs, click the 'Clear log file' button
    - You can sort the entries by ascending \ descending order by clicking on the respective column headers

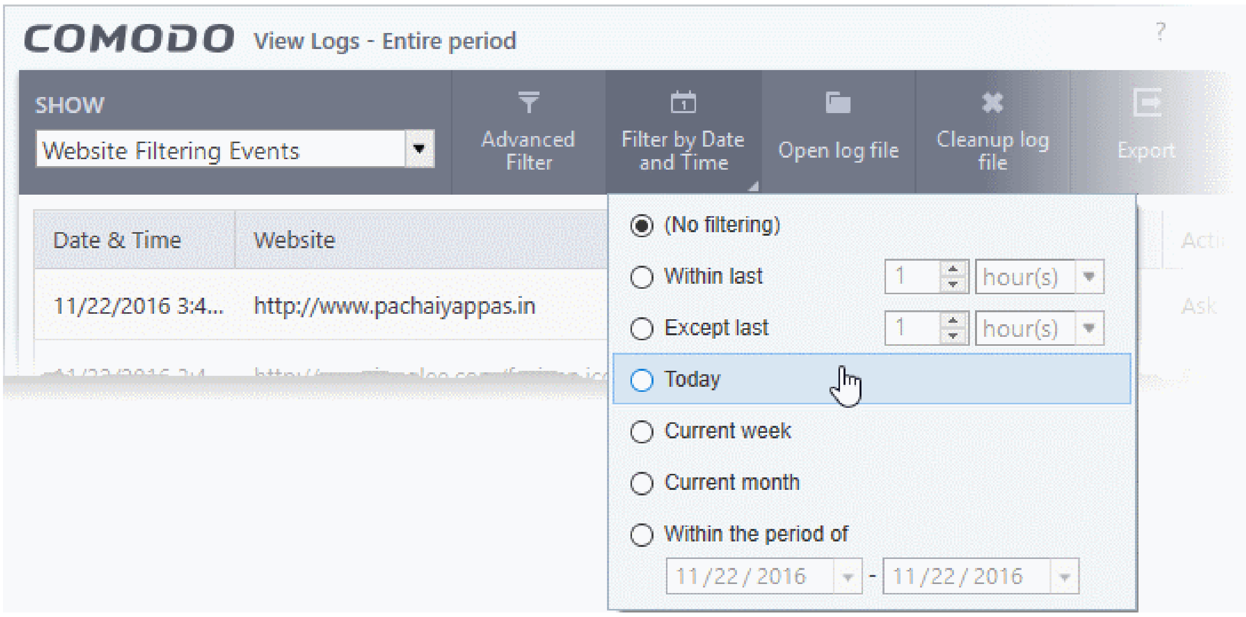
5.5.6.1. Filtering 'Website Filtering' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

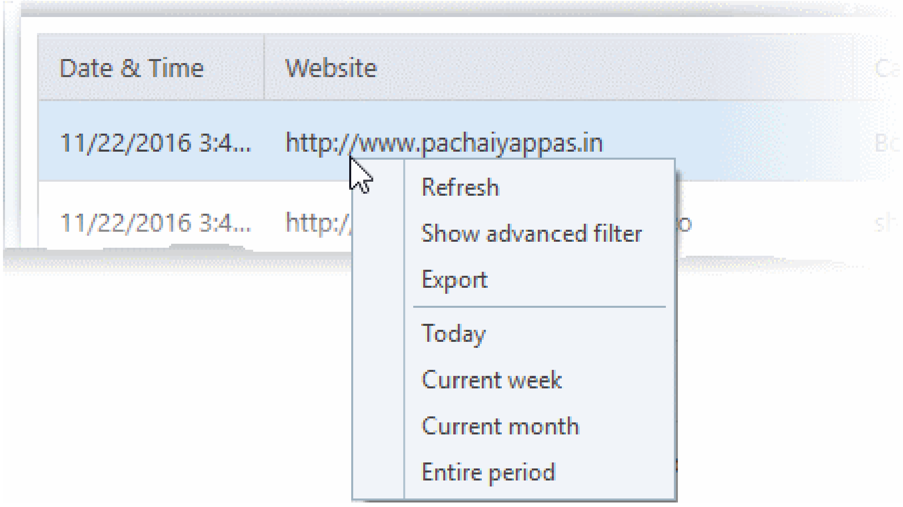
Preset Time Filters

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



- **No filtering** - Display every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Display all logged events for today.
- **Current Week** - All logged events during the current week. The current week is calculated as the previous Sunday to the next Saturday.
- **Current Month** - Display all events logged during this month.
- **Custom Filter** - Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

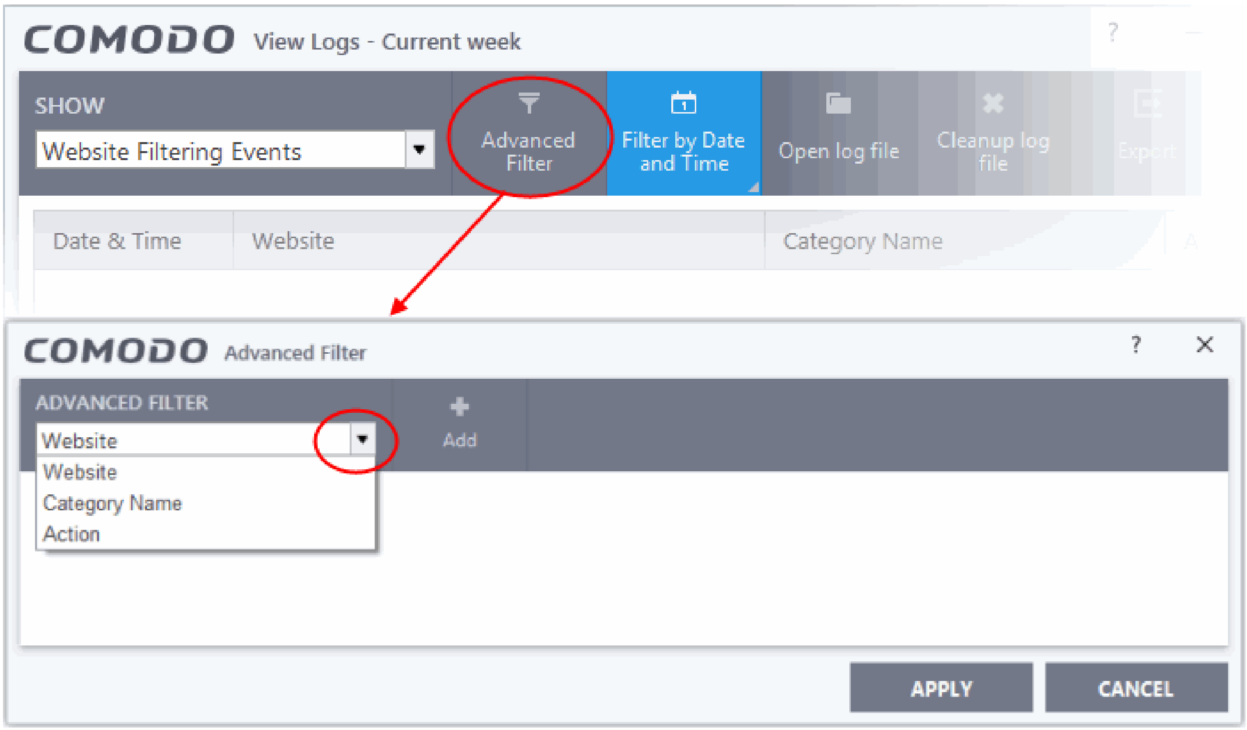
Having chosen a preset time filter from the top panel, you can further refine the displayed events according to certain filtering parameters. The following filters are available for Website Filtering logs:

- **Website -** Displays only events that involved a specific website
- **Category Name -** Displays events that involved websites which are covered by a filtering category.
- **Action -** Displays only events that involved a specific action.

To configure filters for Website Filtering Events

1. Click the 'Advanced Filter' button on the title bar (or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu).

The 'Advanced Filter' interface for Website Filtering Events will open.

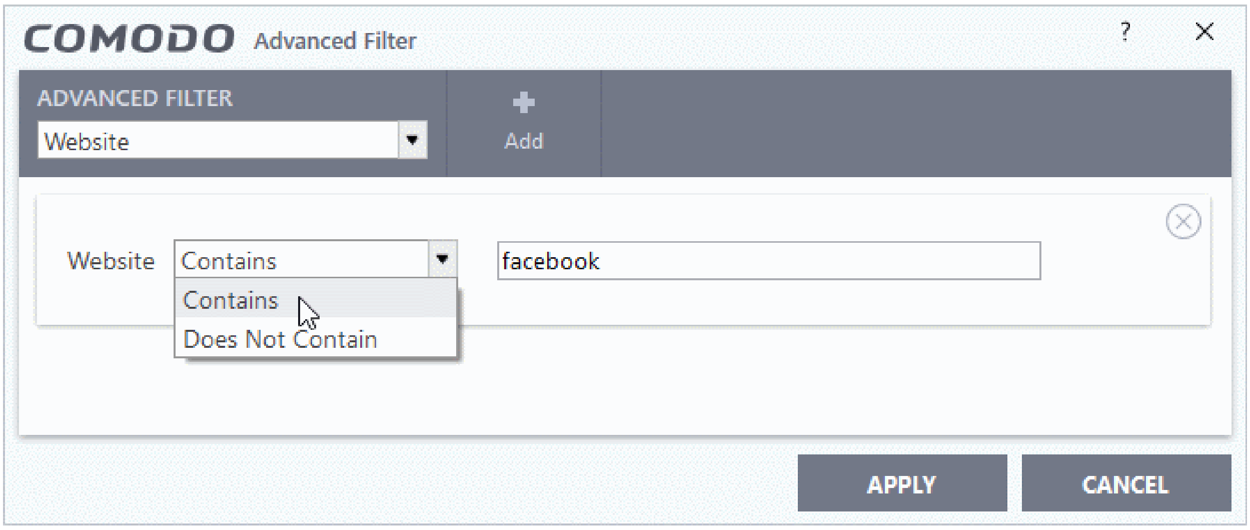


2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.

There are 3 categories of filters that you can add. Each of these categories can be further refined by selecting certain parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

i. **Website**: Adding the 'Website' option displays a drop-down menu and text entry field.



ADVANCED FILTER: Website

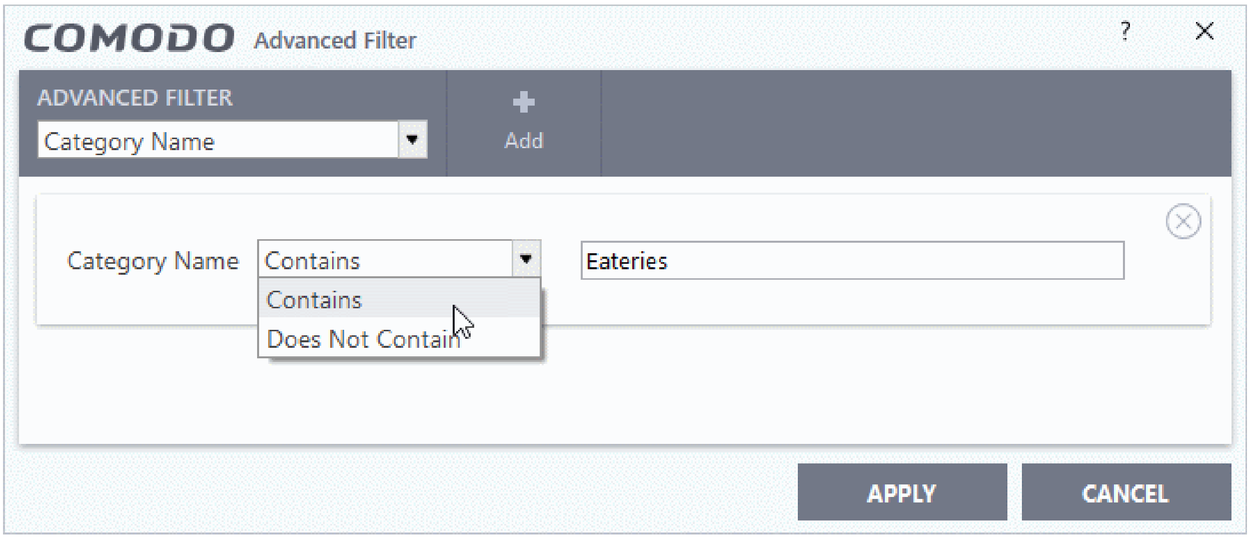
Website: Contains — facebook

a) Select 'Equal' or 'Not Equal' option from the drop-down menu.

b) Enter the website address in part or full, to filter the logs involving the website.

For example, if you choose 'Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that involve the website 'facebook.com' in the 'Website' column will be displayed. If you choose 'Not Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that do not involve 'facebook.com' will be displayed.

ii. **Category**: Selecting the 'Category' option displays a drop down menu and text entry field.



ADVANCED FILTER: Category Name

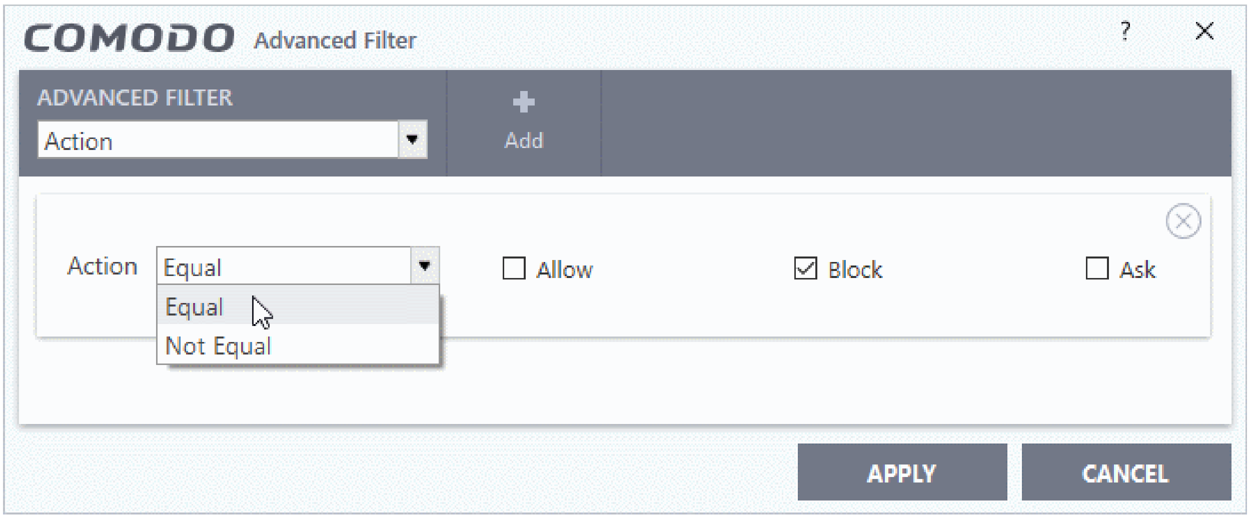
Category Name: Contains — Eateries

a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Pick the filter category. Events related to websites in the category will be shown in the results.

For example, if you choose 'Contains' and enter the phrase 'Malware Sites' in the text field, then all events involving websites in the 'Malware Sites' category will be displayed. If you choose 'Does Not Contain' and enter 'Malware Sites' in the text field, then all events that do not involve sites in the 'Malware Sites' category will be displayed.

iii. **Action**: Selecting the 'Action' option displays a drop-down menu and a set of actions that can be selected or deselected.



□ Allow ☑ Block □ Ask

a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your choice.

b) Now select the action(s) to filter the logs involving those action(s).The available options are:

- Allow
- Block
- Ask

For example, if you choose 'Equal' and 'Block', then only events where a website was blocked will be displayed. If you choose 'Not Equal' and select 'Block' then CIS will show all events except those where a website was blocked. You can select more than one check box options from this interface, as required.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

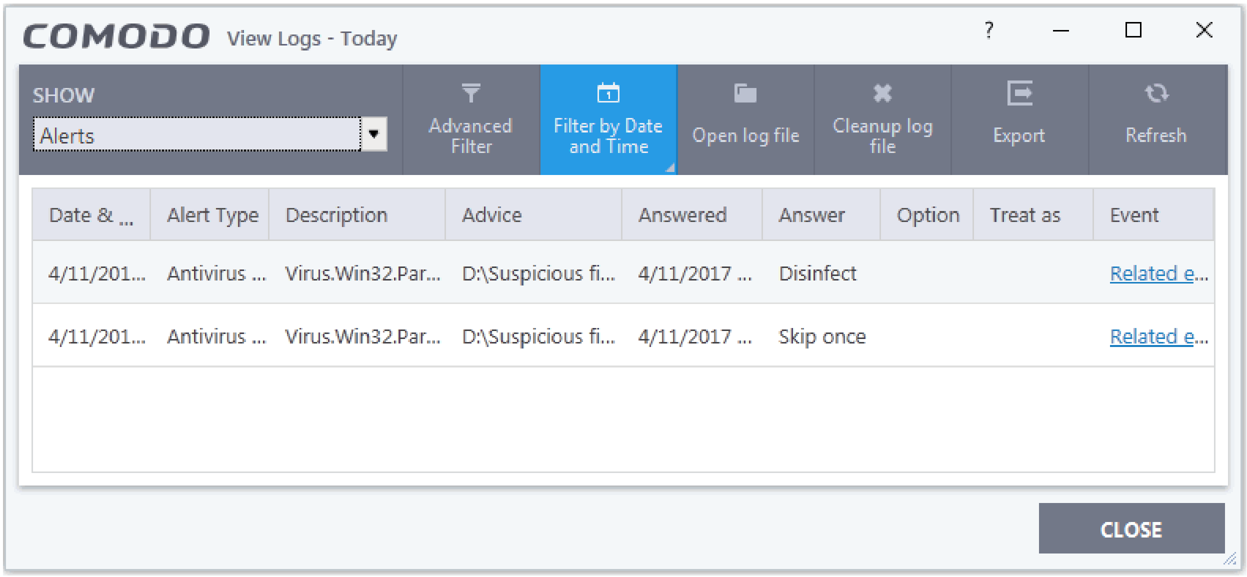
- Click 'Apply' for the filters to be applied to the Website Filtering log viewer. Only those 'Website Filtering' log entries selected based on your filter criteria will be displayed in the log viewer.
- To clear filters, open the 'Advanced Filter' pane and remove filters one-by-one by by clicking the 'X' button on the right. Click 'Apply'.

5.5.7. 'Alerts Displayed' Logs

The 'Alerts Displayed' logs are a record of all alerts generated by CIS and of the actions taken against threats identified by the alerts. The action taken on a threat depends on how the user answered the alert.

To view the 'Alert Displayed' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Alerts Displayed' from the 'Show' drop-down



Date & ...	Alert Type	Description	Advice	Answered	Answer	Option	Treat as	Event
4/11/201...	Antivirus ...	Virus.Win32.Par...	D:\Suspicious fi...	4/11/2017 ...	Disinfect			Related e...
4/11/201...	Antivirus ...	Virus.Win32.Par...	D:\Suspicious fi...	4/11/2017 ...	Skip once			Related e...

Column Descriptions

1. **Date & Time** - Indicates the date and event time that the alert was generated.
2. **Alert Type** - Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope or secure shopping).
3. **Description** - Brief description of the file or the event that triggered the alert.
4. **Advice -** Advice offered by CIS on how to respond to the alert.
5. **Answered** - Indicates whether the alert has been answered by the user. If answered, you will see the date and time of the response.
6. **Answer** - Indicates the response given by the user. For example, allow, block, disinfect, skip.
7. **Options** - Indicates any additional options chosen by the user at the alert. For example, if the user has chosen 'Remember My Answer' at the alert.
8. **Treat As** - Whether the user told CIS to handle the file in accordance with an application category. For example, treat as a safe application, installer etc.
9. **Event** - Clicking 'Related Event' opens the log viewer which provides details of the event that triggered the alert.

   - To export the 'Alerts' logs as a HTML file' click the 'Export' button (or right click inside the log viewer and choose 'Export' from the context sensitive menu).
   - To open a saved CIS log file, click the 'Open log file' button.
   - To refresh the logs, click the 'Refresh' button (or right click inside the log viewer and choose 'Refresh' from the context sensitive menu).
   - To delete all logs, click the 'Clear' button.
   - You can sort the entries in ascending \ descending order by clicking the respective column headers.

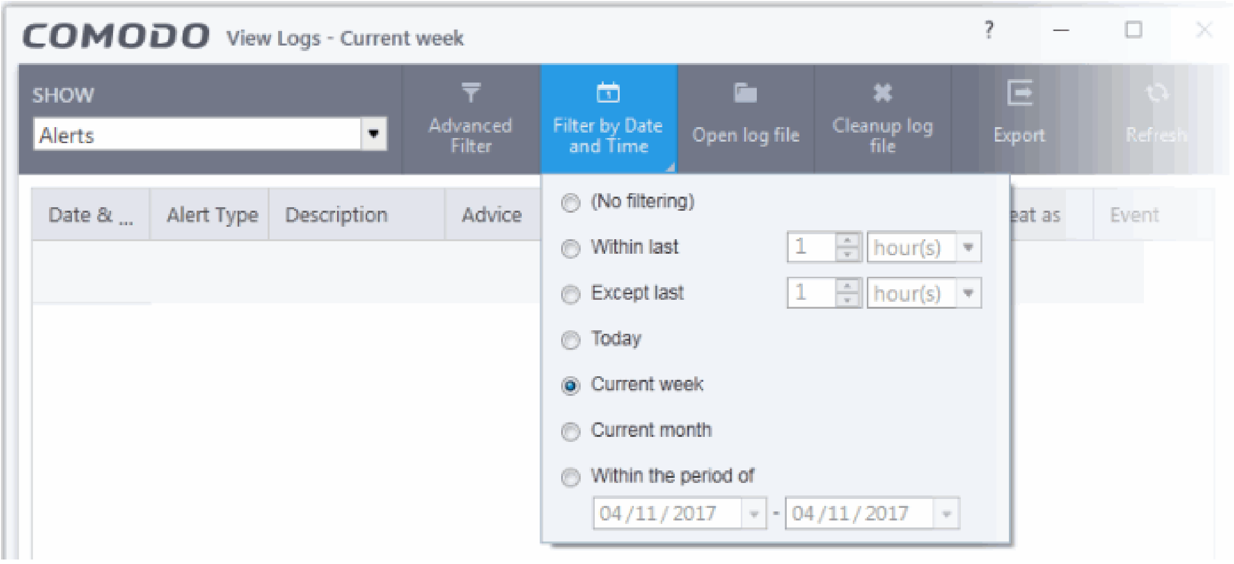
5.5.7.1. Filtering 'Alerts Displayed' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

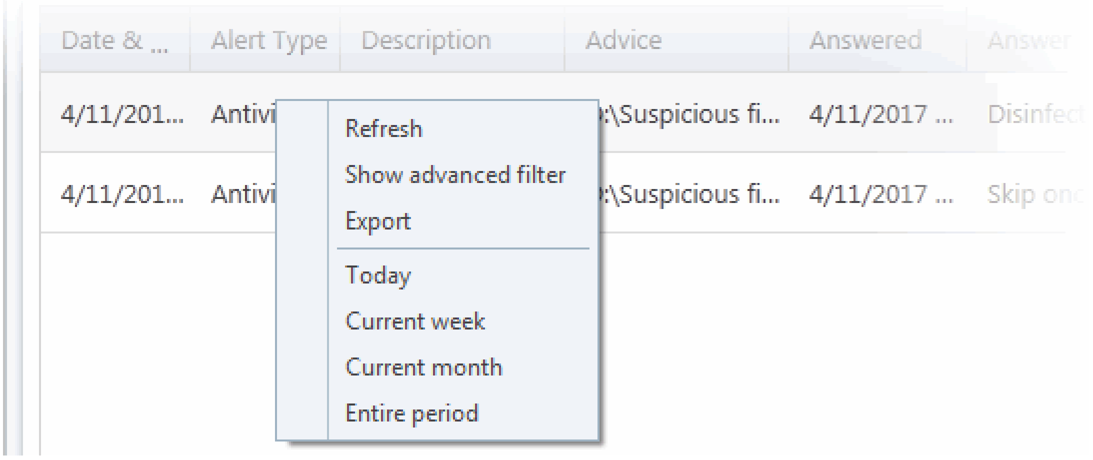
Preset Time Filters

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



- **No filtering -** Displays every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last -** Shows all logs from a certain point in the past until the present time.
- **Except last -** Excludes all logs from a certain point in the past until the present time.
- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month -** Displays all events logged during this month.
- **Within the Period of -** Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

You can further refine which events are displayed according to specific filters. The following filters are available:

- **Advice:** Displays only alerts that match the advice entered.
- **Answer:** Displays only alerts that were answered by the user.
- **Answered:** Displays only alerts that were answered at a specific date and time.

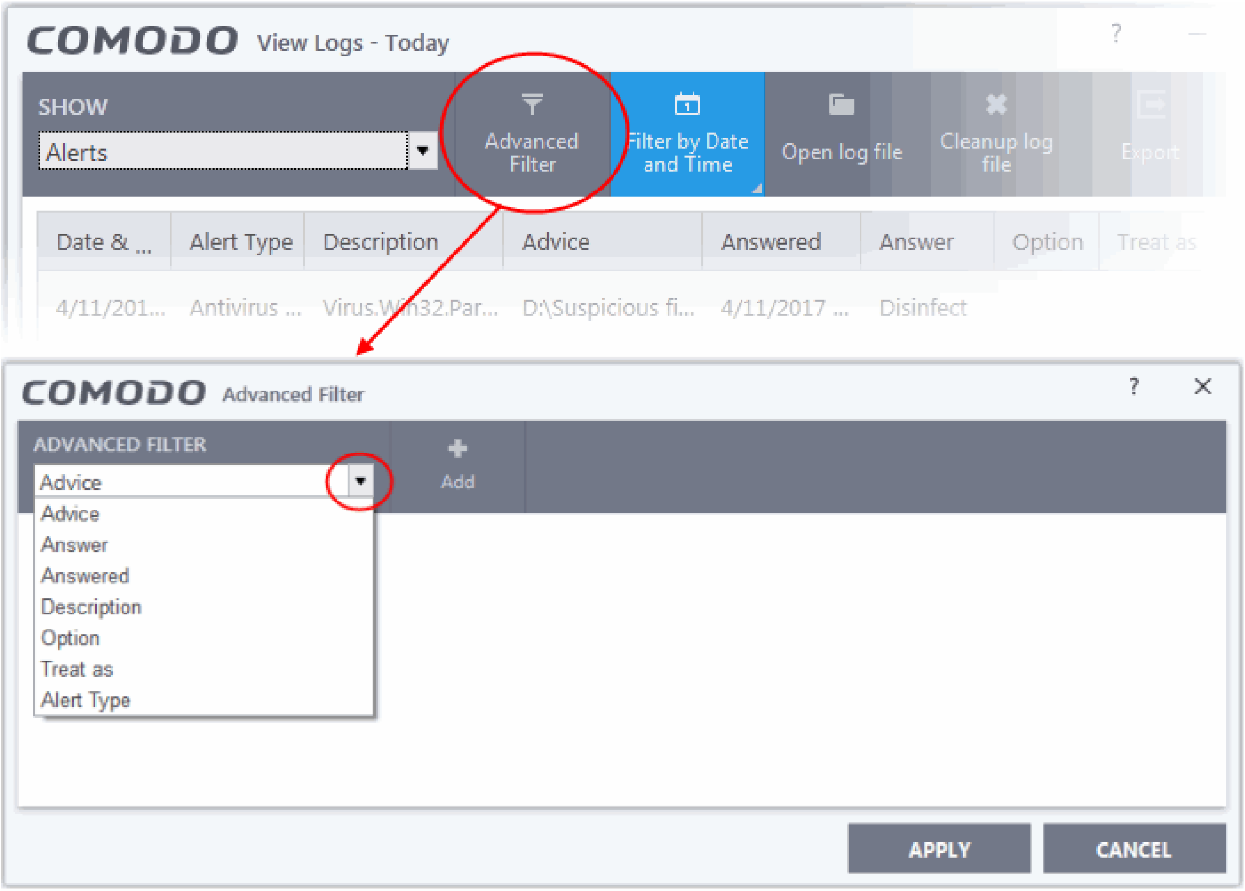
- **Description:** Displays only alerts that match the description entered
- **Option**: Displays only alerts where the user selected an additional option at the alert. Addition options include 'Remember my answer'.
- **Treat As:** Displays only alerts where a 'Treat As' option was chosen by the user. For example, 'treat as a safe application', 'treat as an installer' and so on.
- **Alert Type:** Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope or secure shopping).

To configure Advanced Filters for Alerts Displayed

1. Click the 'Advanced Filter' button on the title bar (or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu).

The 'Advanced Filter' interface for 'Alerts' logs will open:

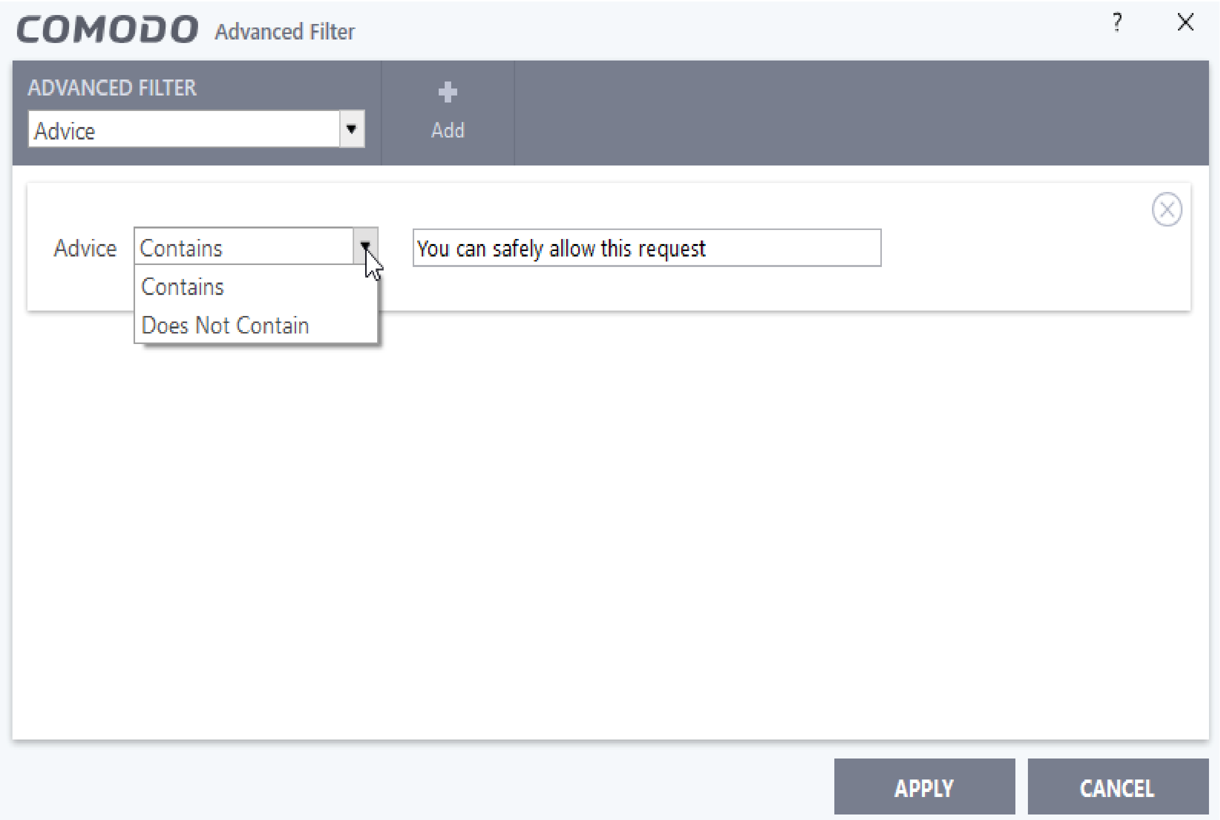
2. Select a filter from the 'Advanced Filter' drop-down and click 'Add':



There are 7 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Add' drop down menu:

i. **Advice**: The 'Advice' option lets you to filter alerts based on the recommendations given by CIS in the alert. Selecting the 'Advice' option will display drop-down and text entry fields.

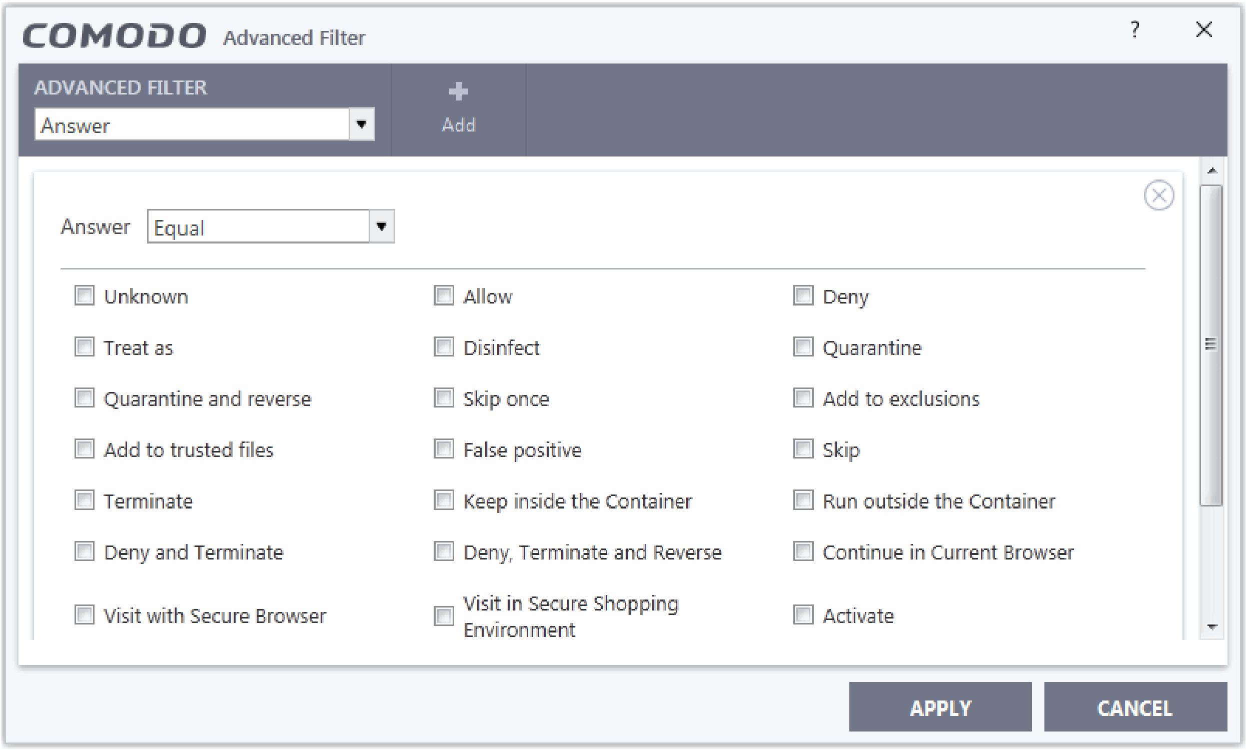


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria.

For example, if you choose 'Contains' and enter the phrase 'you can safely allow this request' in the text field, then only entries containing 'you can safely allow this request' in the 'Advice' column will be displayed.

ii. **Answer**: Allows you to filter alerts based on what action the user selected at the alert. Selecting the 'Answer' option displays a drop-down box and a set of answers that can be selected or deselected.



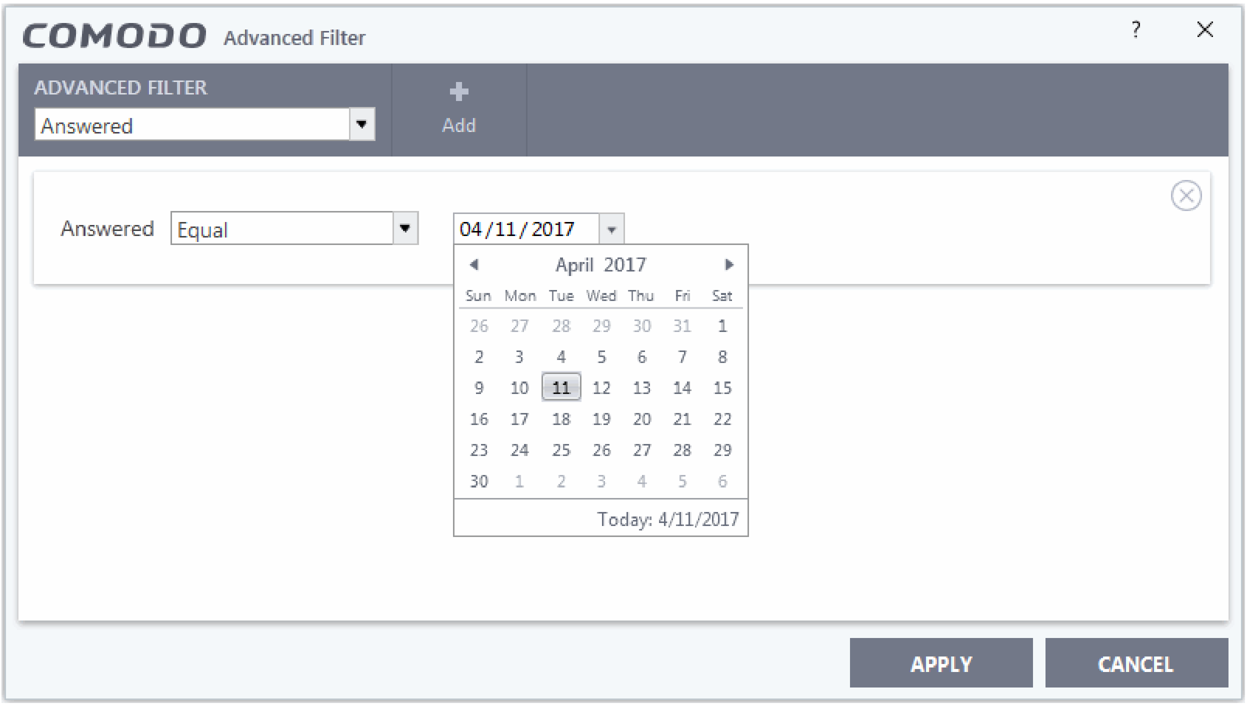
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the responses to refine your search. The options available are:

- Unknown
- Allow
- Deny
- Treat as
- Disinfect
- Quarantine
- Quarantine and reserve
- Skip once
- Add to exclusions
- Add to trusted files
- False positive
- Skip
- Terminate
- Keep inside the Container
- Run outside the Container
- Deny and Terminate
- Deny, Terminate and Reverse
- Continue in Current Browser
- Visit with Secure Browser
- Visit in Secure Shopping Environment
- Activate
- Downgrade
- Postpone
- Containment
- Run Unlimited
- Run inside the Container
- Blocked

For example, if you choose 'Equal' from the drop-down and select the 'Add to exclusions' checkbox, only the alerts where you answered 'Ignore' > 'Ignore and Add to exclusions' will be displayed.

iii. **Answered**: The Answered option enables you to filter logs based on the date you answered the alerts. Selecting the 'Answered' option displays a drop-down box and date field.



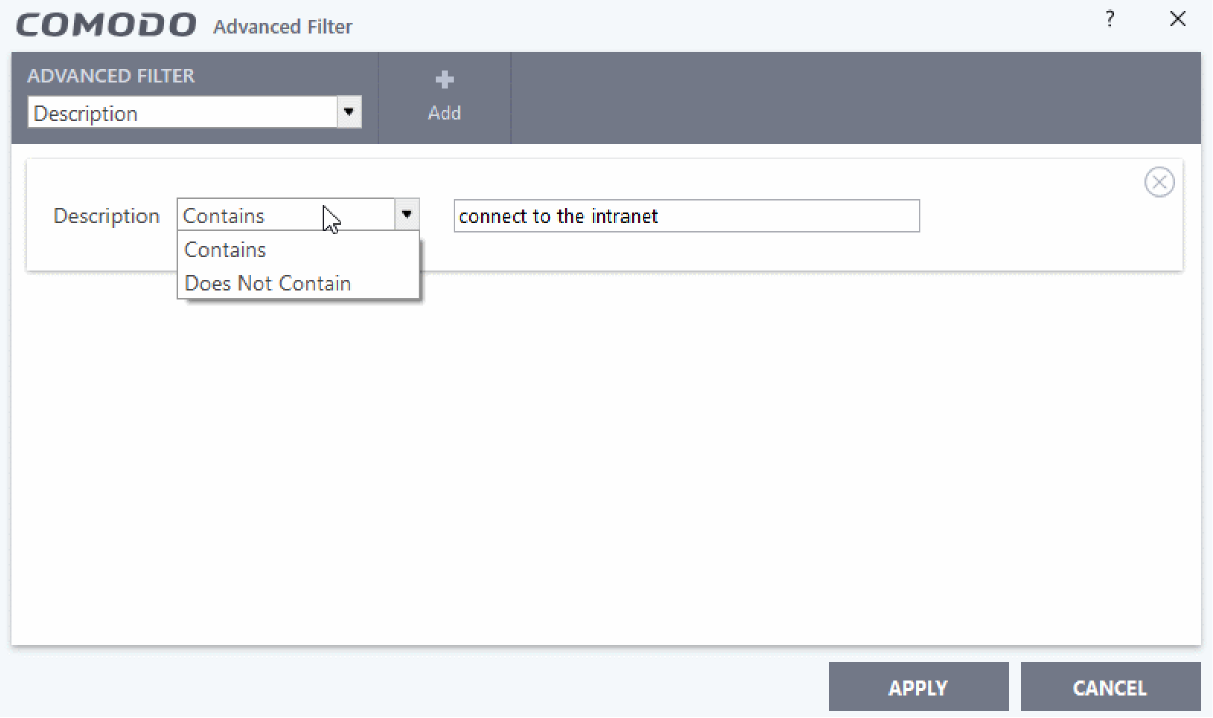
a) Select any one of the following option the drop-down box.

- Equal
- Not Equal

b) Select the required date from the drop-down calendar

For example, if you select 'Equal' and select '04/11/2017', only alerts answered on 04/11/2017 will be displayed.

iv. **Description**: The Description option enables you to filter logs based on the description of the attempt displayed in the alert. Selecting the 'Description' option displays drop-down and text entry fields.

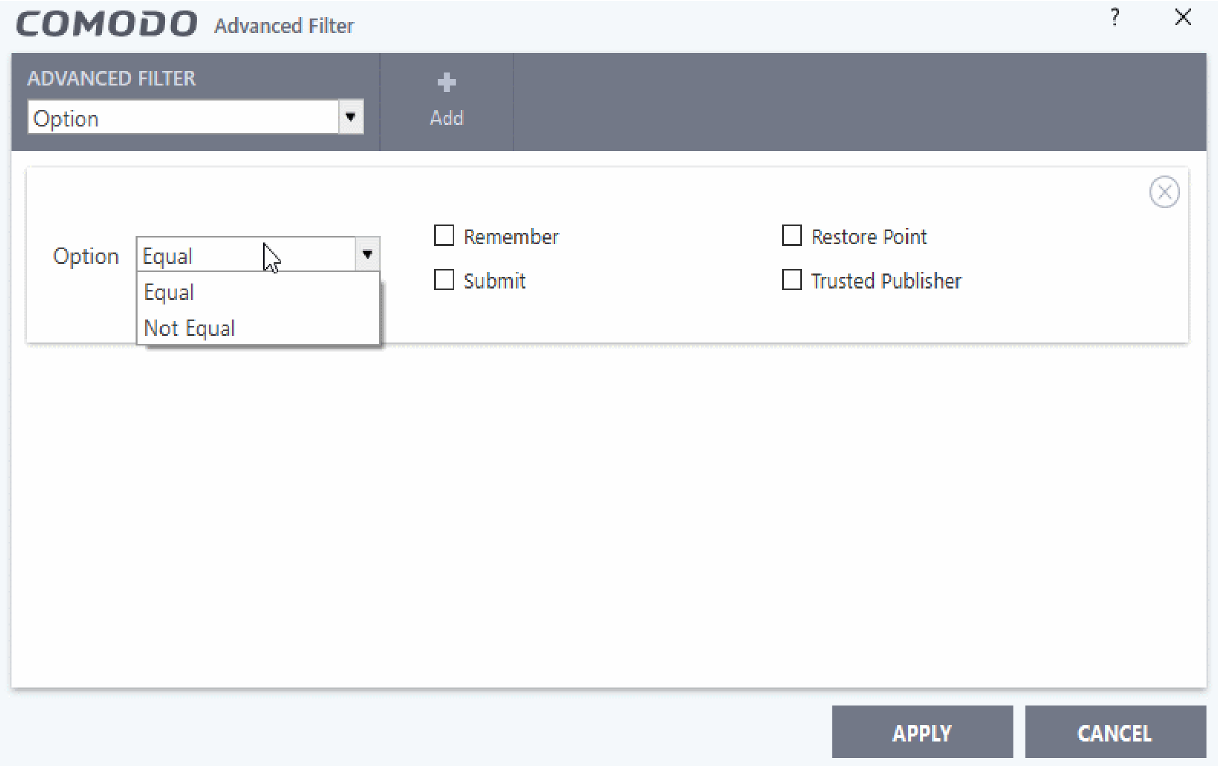


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria.

For example, if you select 'Contains' from the drop-down and enter 'connect to the Internet', only the log entries of Firewall alerts containing the phrase 'connect to the Internet' in the description, will be displayed.

v. **Option**: Displays only alerts where the user selected additional options like 'Remember my answer' or 'Submit as False Positive' at the alert.



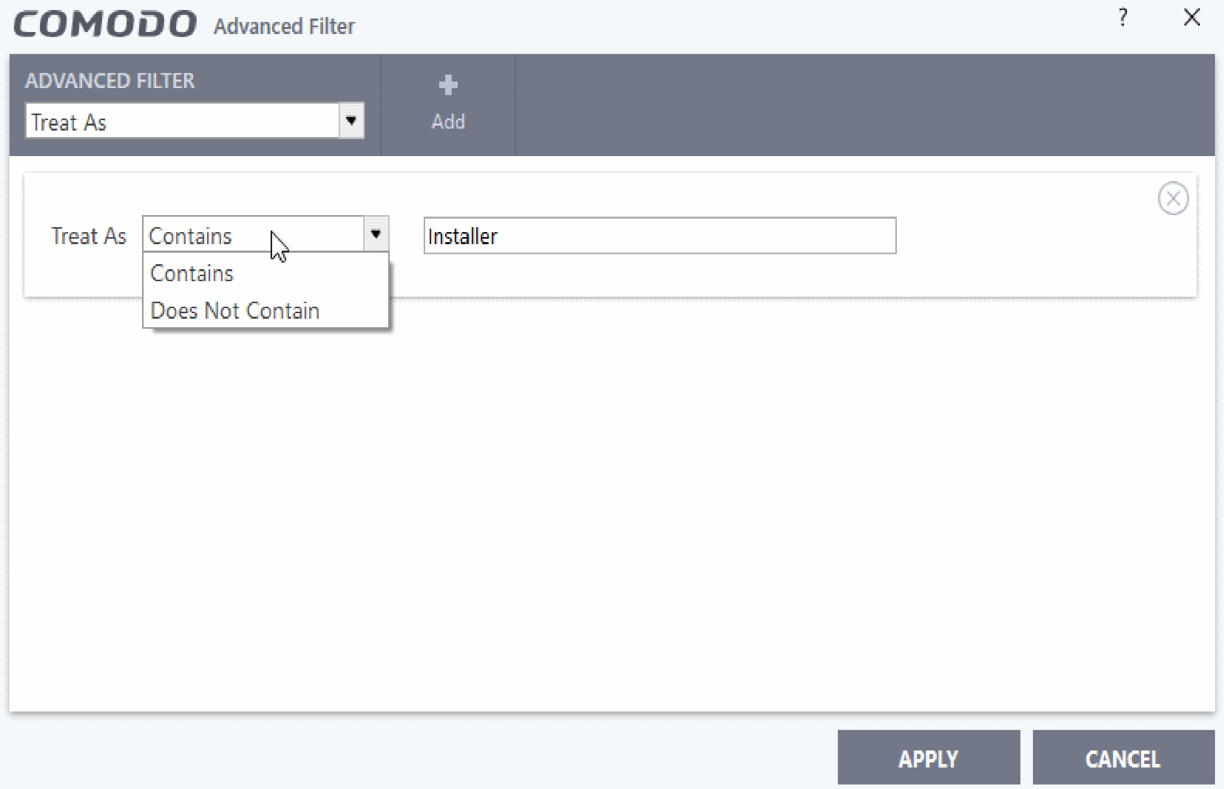
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Remember
- Restore Point
- Submit
- Trusted Publisher

For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected will be displayed.

vi. **Treat As**: Displays only alerts where a 'Treat As' option was chosen by the user. For example, 'treat as a safe application', 'treat as an installer' and so on.



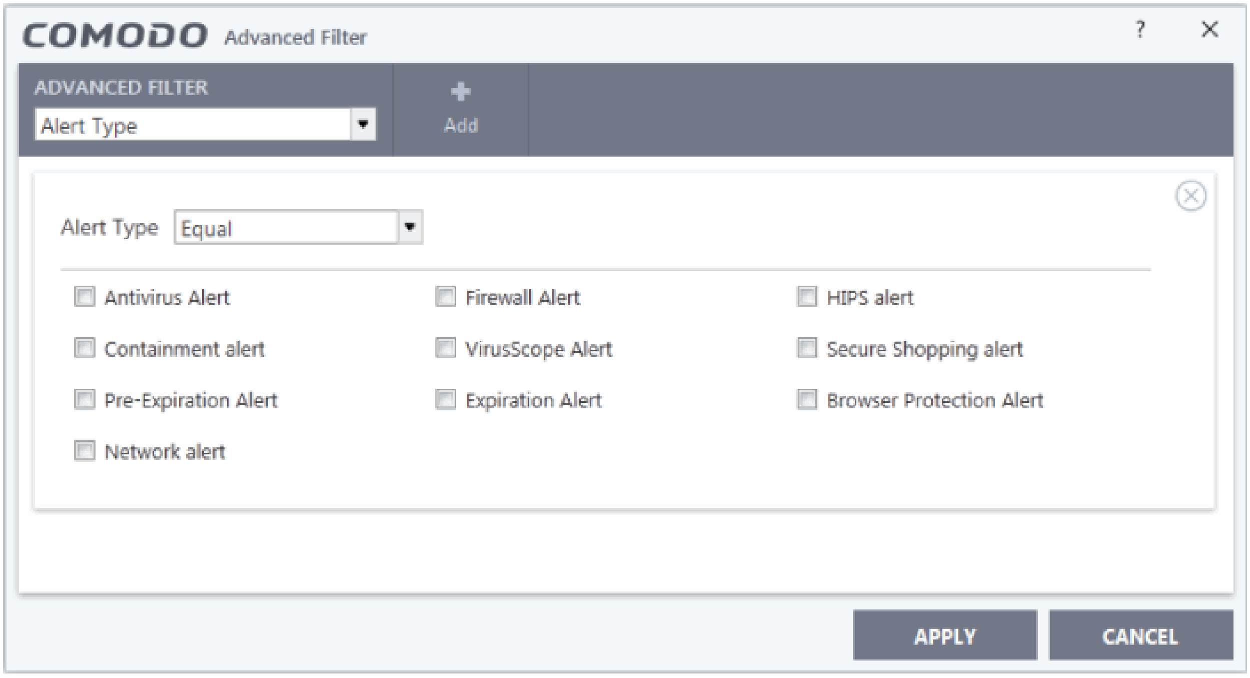
a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria

For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the log entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.

vii. **Alert Type**: The 'Type' option enables you to filter the entries based on the component of CIS that has triggered the alert. Selecting the 'Type' option displays a drop down menu and a set of specific alert types that can be selected or deselected.

Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope or secure shopping).



a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Antivirus Alert
- Firewall Alert
- HIPS Alert
- Containment Alert
- VirusScope Alert
- Secure Shopping Alert
- Pre-Expiration Alert
- Expiration Alert
- Browser Shopping Alert
- Network Alert

For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of Antivirus alerts will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Alerts' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

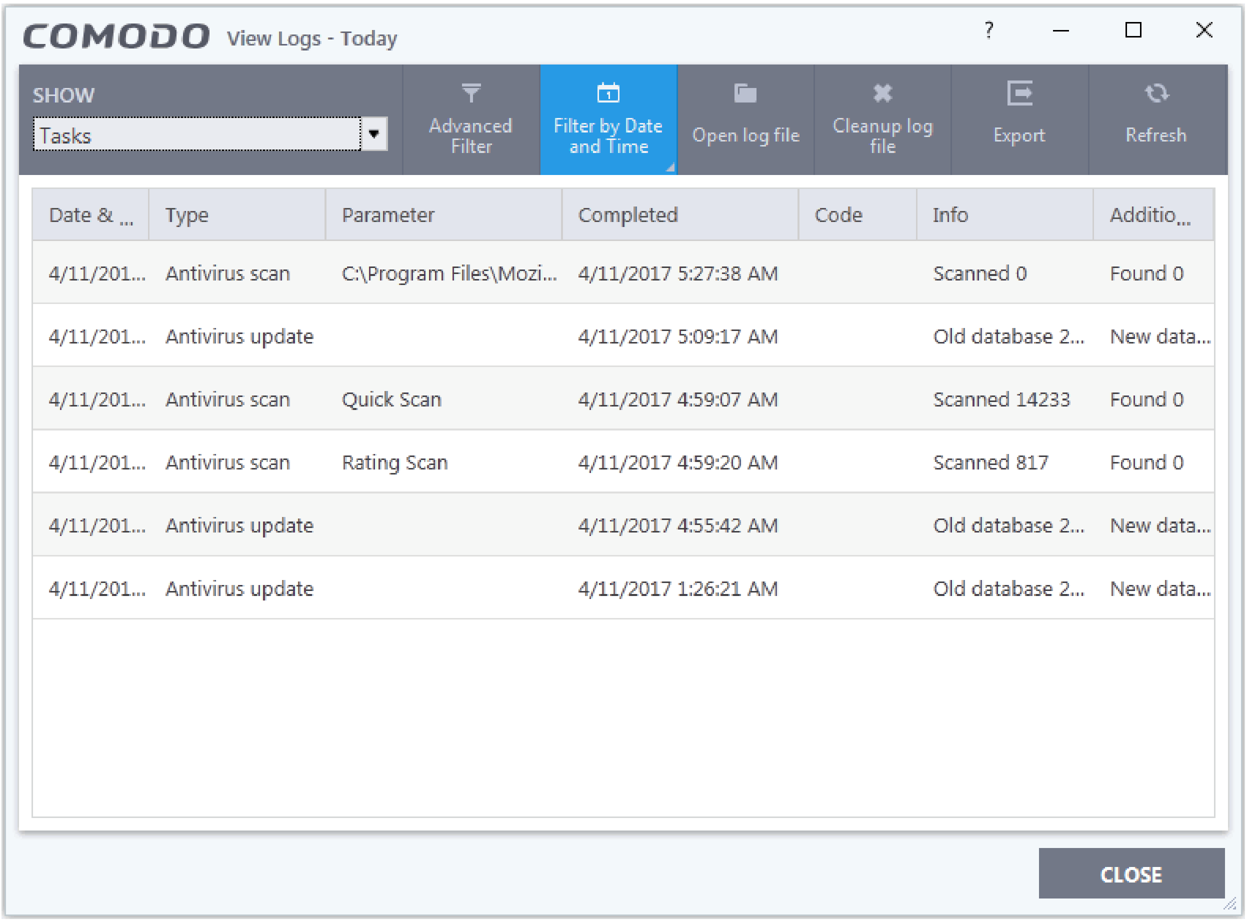
5.5.8. CIS Tasks Logs

Comodo Internet Security keeps a record of all CIS tasks like virus signature database updates, scans run and so on.

The 'Tasks' log window displays a list of all tasks launched along with their completion status and other details.

To view the 'CIS Task' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs' OR click the 'Logs' button at the top-right of the home screen in basic view
- Select 'Tasks' from the 'Show' drop-down



Date & ...	Type	Parameter	Completed	Code	Info	Additio...
4/11/201...	Antivirus scan	C:\Program Files\Mozi...	4/11/2017 5:27:38 AM		Scanned 0	Found 0
4/11/201...	Antivirus update		4/11/2017 5:09:17 AM		Old database 2...	New data...
4/11/201...	Antivirus scan	Quick Scan	4/11/2017 4:59:07 AM		Scanned 14233	Found 0
4/11/201...	Antivirus scan	Rating Scan	4/11/2017 4:59:20 AM		Scanned 817	Found 0
4/11/201...	Antivirus update		4/11/2017 4:55:42 AM		Old database 2...	New data...
4/11/201...	Antivirus update		4/11/2017 1:26:21 AM		Old database 2...	New data...

Column Descriptions

1. **Date & Time** - Indicates the date and time when the alert was generated.
2. **Type** - Indicates the task type.
3. **Parameter** - Indicates the parameter (like scan type) associated with the task.
4. **Completed** - Indicates the date and time that the task finished.
5. **Code** - Indicates the error code generated by Windows operating system for CIS tasks that were not completed successfully. No code will be generated if the tasks that were completed successfully.
6. **Info & Additional Info** - Provides additional information about the task. For example, if the task is to update the version of CIS then these fields will show the old version number and the new version number.

   - To export the Tasks logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
   - To open a stored CIS log file, click the 'Open log file' button.
   - To refresh the 'Tasks' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
   - To clear the 'Tasks' logs click the 'Cleanup log file' button.
   - You can sort the entries by ascending \ descending order by clicking on the respective column headers.

5.5.8.1. Filtering 'CIS Tasks' Logs

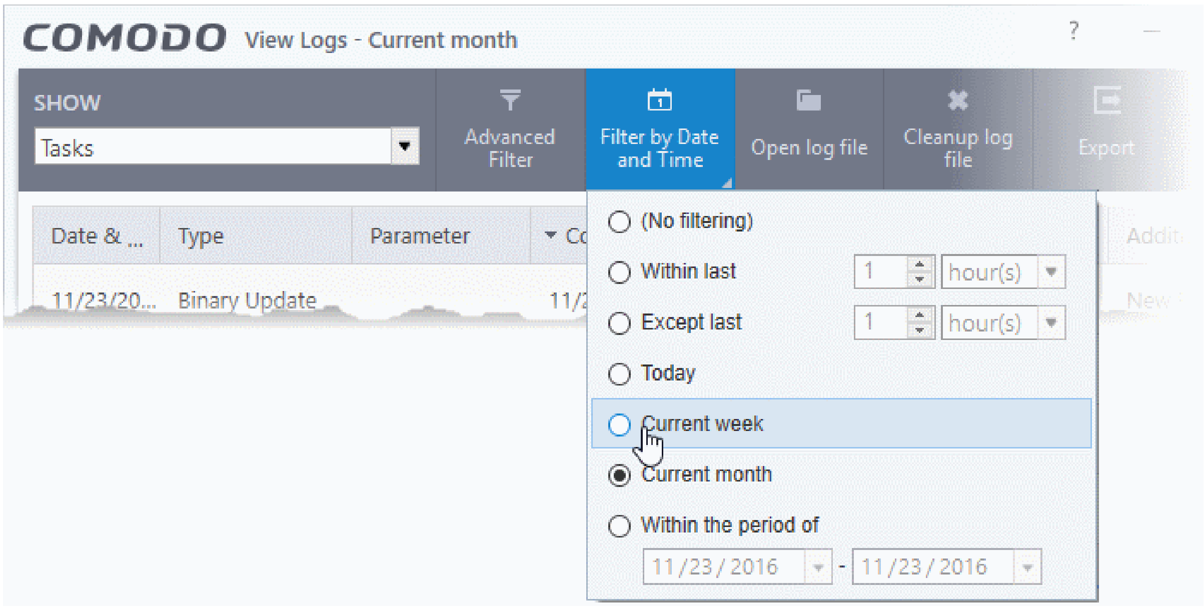
Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters

- Advanced Filters

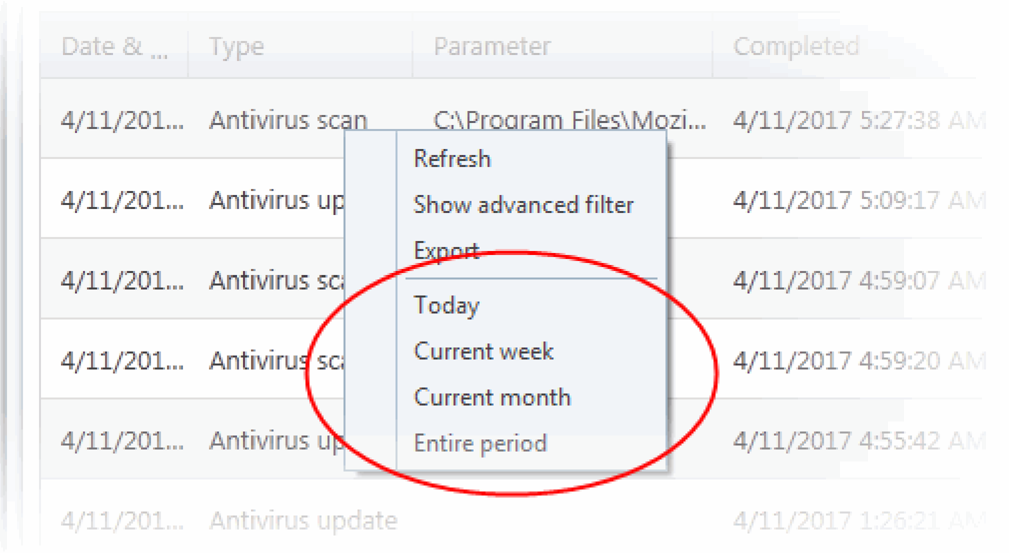
Preset Time Filters

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



- **No filtering -** Displays every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last -** Shows logs from a certain point in the past until the present time.
- **Except last -** Excludes logs from a certain point in the past until the present time.
- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month -** Displays all logged events during the month.
- **Within the Period of -** Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

You can further refine which events are displayed according to specific filters. The following additional filters are available:

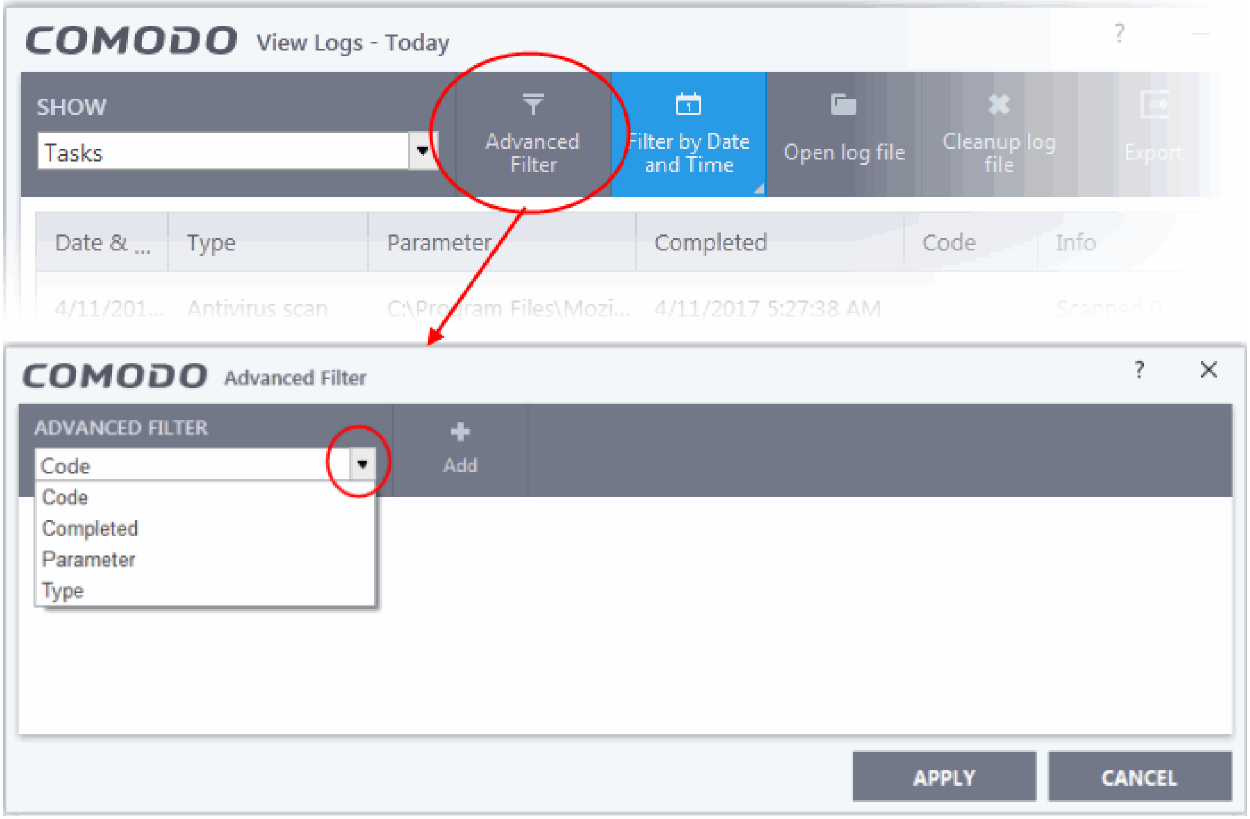
- **Code -** Filter tasks based on specified error code
- **Completed -** Displays only tasks completed on the specified date
- **Parameter -** Displays only tasks that include the selected parameter. A 'parameter' is a sub-type of the main task type. For example, 'Quick Scan' and 'Rating Scan' are both parameters of the main task type 'Antivirus Scan'.
- **Type -** Displays only tasks of a certain type. Tasks that you can filter for include antivirus updates, antivirus scans, log clearing, warranty activation and more.

To configure 'Advanced Filters' for 'Tasks' logs

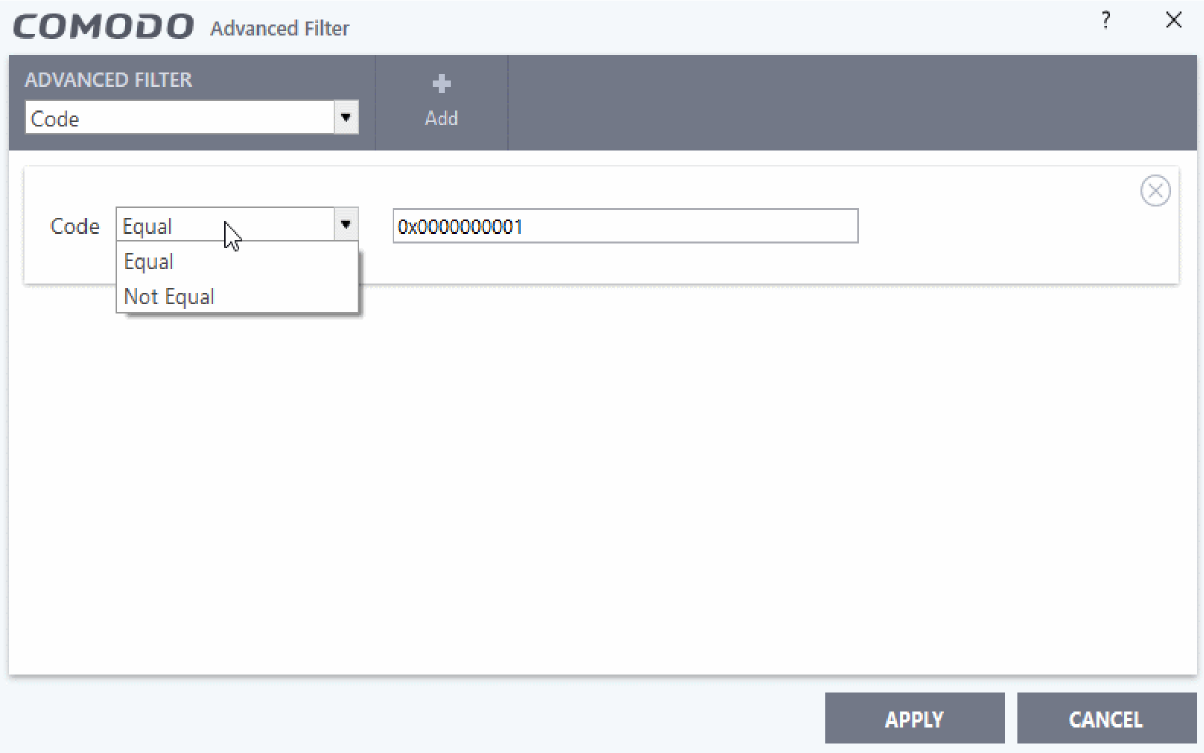
1. Click the 'Advanced Filter' button from the title bar (or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu).

The 'Advanced Filter' interface for 'Tasks' logs will be displayed.

2. Select a filter from the 'Advanced Filter' drop-down and click 'Add':



i. **Code**: Filter incomplete tasks according to their error code generated by Windows. You can view task codes in the 'Code' column of the log viewer. Selecting the 'Code' option will display drop-down and text entry fields.

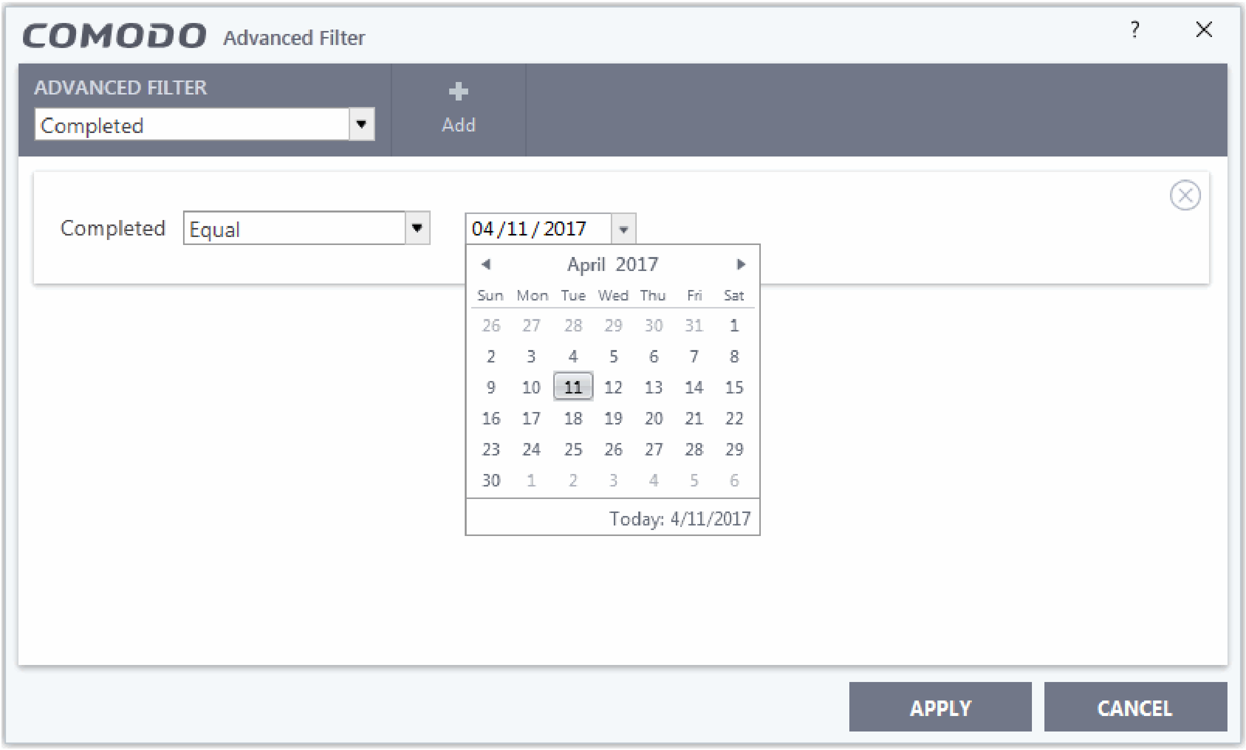


a) Select 'Equal' or 'Not Equal' option from the drop-down. 'Not Equal' will invert your selected choice.

b) Enter the code or a part of it as your filter criteria in the text field.

For example, if you have select 'Equal' and entered '0x80004004' in the text field, then only entries containing the value '0x80004004' in the 'Code' column will be displayed.

ii. **Completed**: Lets you filter logs based on the completion dates of the Tasks. Selecting the 'Completed' option displays drop-down box and date entry field.



a) Select any one of the following option the drop-down box.

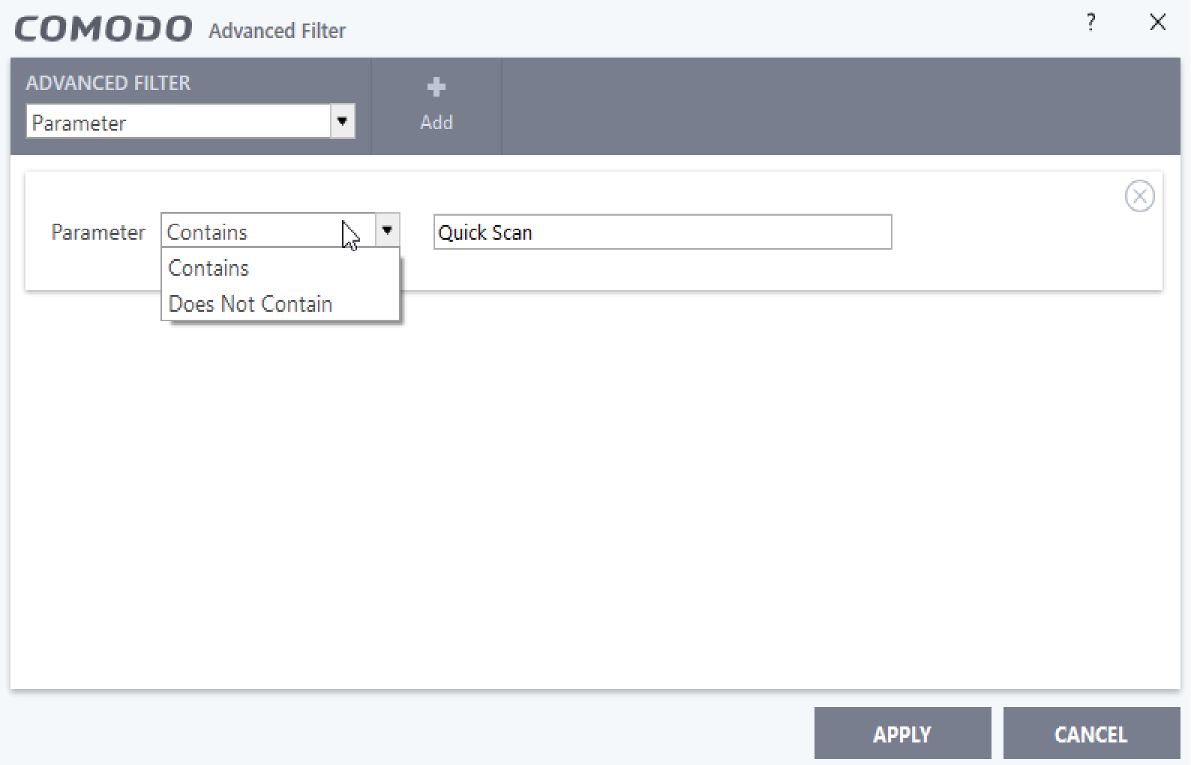
- Equal

- Not Equal

b) Select the required date from the date picker.

For example, if you choose 'Equal' and select '104/11/2017 ', only the logs of tasks completed on '04/11/2017 ' will be displayed.

iii. **Parameter**: The 'Parameter' option lets you filter entries based on the 'Parameter' column of the log viewer. This includes descriptions such as 'Quick Scan' and 'Rating Scan'. Selecting the 'Parameter' option displays drop-down and text entry fields.



ADVANCED FILTER: Parameter

Parameter: Contains — Quick Scan

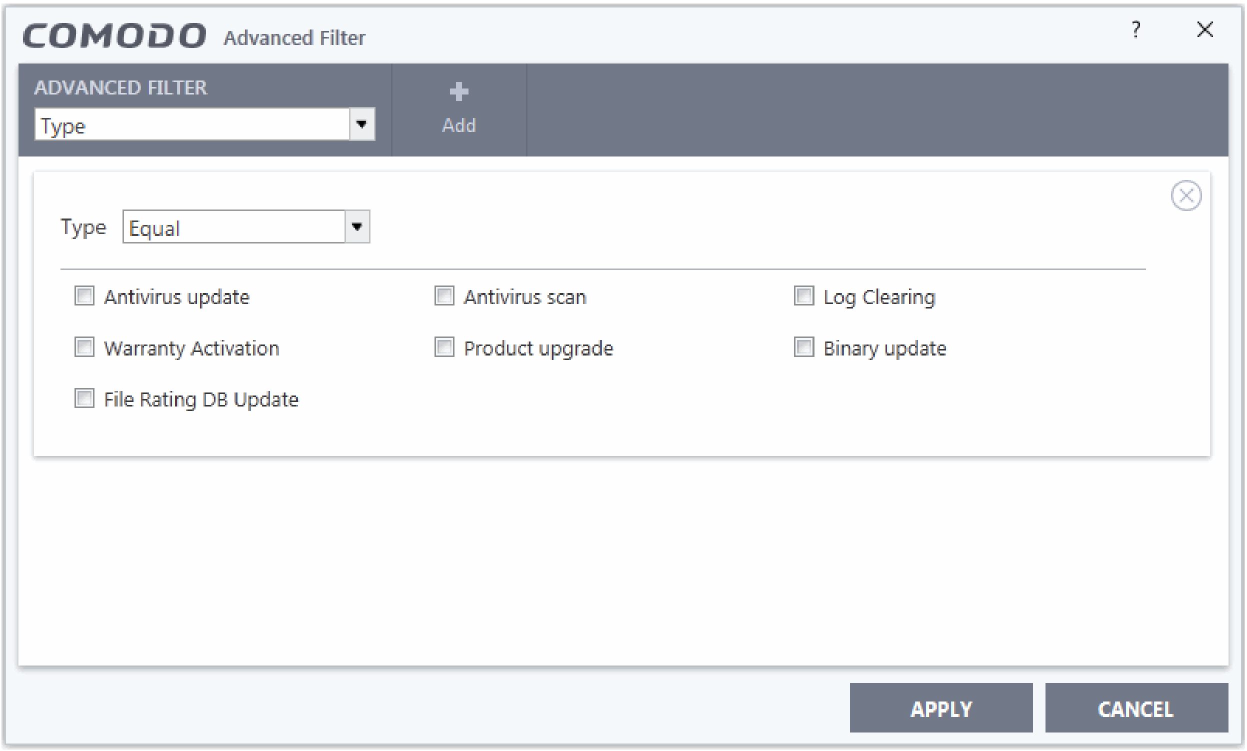
Contains
Does Not Contain

a) Select 'Contains' or 'Does Not Contain' option from the drop-down.

b) Enter the text or word as your filter criteria.

For example, if you choose 'Contains' and enter the phrase 'Quick Scan' in the text field, then only entries of 'Antivirus Scan Tasks' with the scan parameter 'Quick Scan' will be displayed.

iv. **Type**: Allows you to filter entries based on type of 'Tasks' launched. Selecting the 'Type' option displays a drop down box and a set of specific task types that can be selected or deselected.



COMODO Advanced Filter

ADVANCED FILTER

Type

Add

Type Equal

□ Antivirus update
□ Antivirus scan
□ Log Clearing
□ Warranty Activation
□ Product upgrade
□ Binary update
□ File Rating DB Update

a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Antivirus update
- Antivirus scan
- Log clearing
- Warranty activation
- Product upgrade
- Binary update
- File Rating DB Upgrade

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the pane.

- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

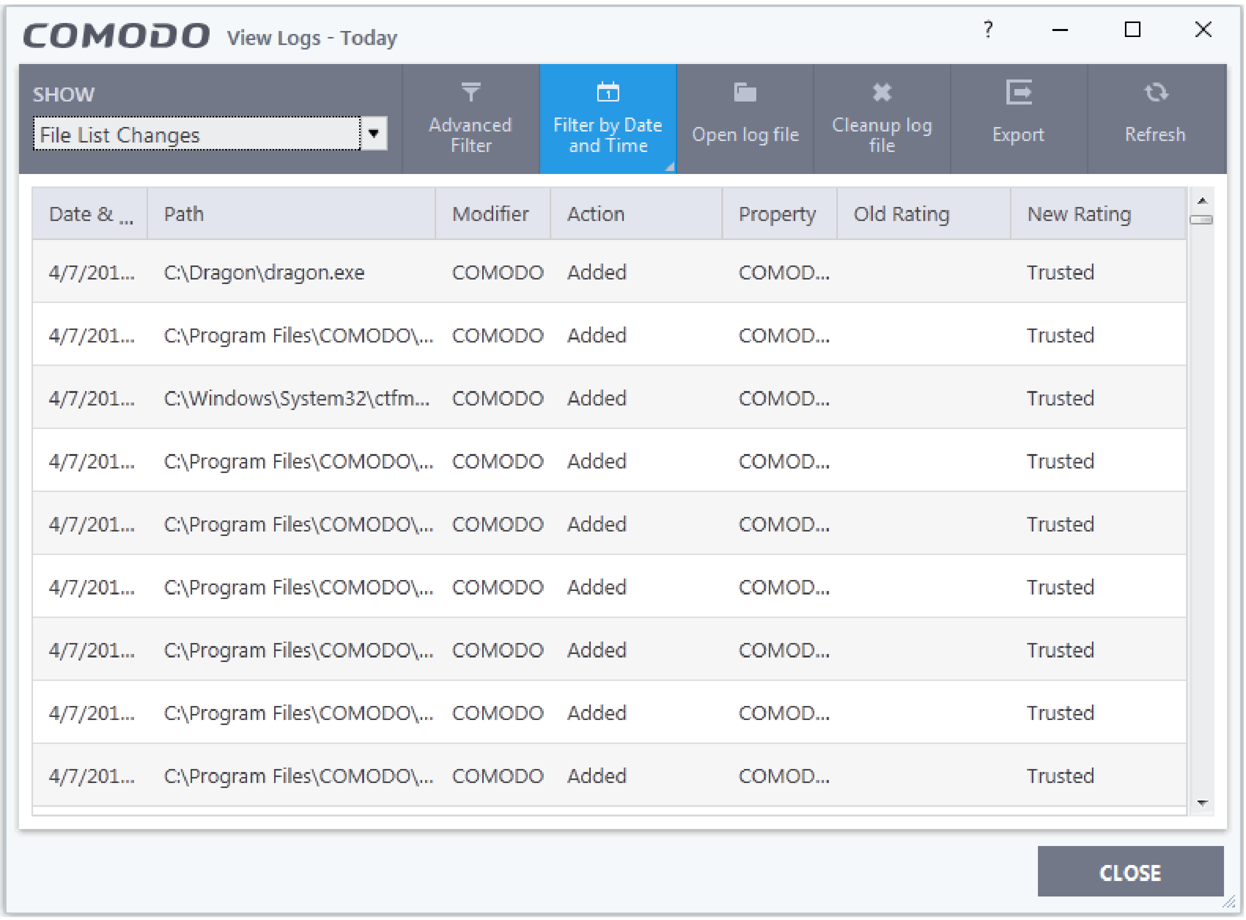
5.5.9. File List Changes Logs

CIS displays executable file on your computer in the '**File List**'. Any changes to the files in the list will be logged. For example, this includes adding a new file, removing a file or changing the rating of a file. See '**File List**' for more details'.

To view the 'File List Changes' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs' OR click the 'Logs' button at the top-right of the home screen in basic view

- Select 'File List Changes' from the 'Show' drop-down



Date & ...	Path	Modifier	Action	Property	Old Rating	New Rating
4/7/201...	C:\Dragon\dragon.exe	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Windows\System32\ctfm...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted
4/7/201...	C:\Program Files\COMODO\...	COMODO	Added	COMOD...		Trusted

Column Descriptions

1. **Date & Time -** Indicates date and time when the file list changes was generated.
2. **Path -** Indicates the file path.
3. **Modifier -** Indicates who made the changes (User, Administrator or Comodo).
4. **Action -** Indicates the action type done for the file.
5. **Property -** Indicates the file rating.
6. **Old Rating -** Indicates the old rating for the file.
7. **New Rating -** Indicates the new rating for the file.

- To export the 'File List Changes' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open log file' button.
- To refresh the 'File List Changes' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the 'File List Changes' logs click the 'Cleanup log file' button.
- You can sort the entries by ascending \ descending order by clicking on the respective column headers.

5.5.9.1. Filtering File List Changes Logs

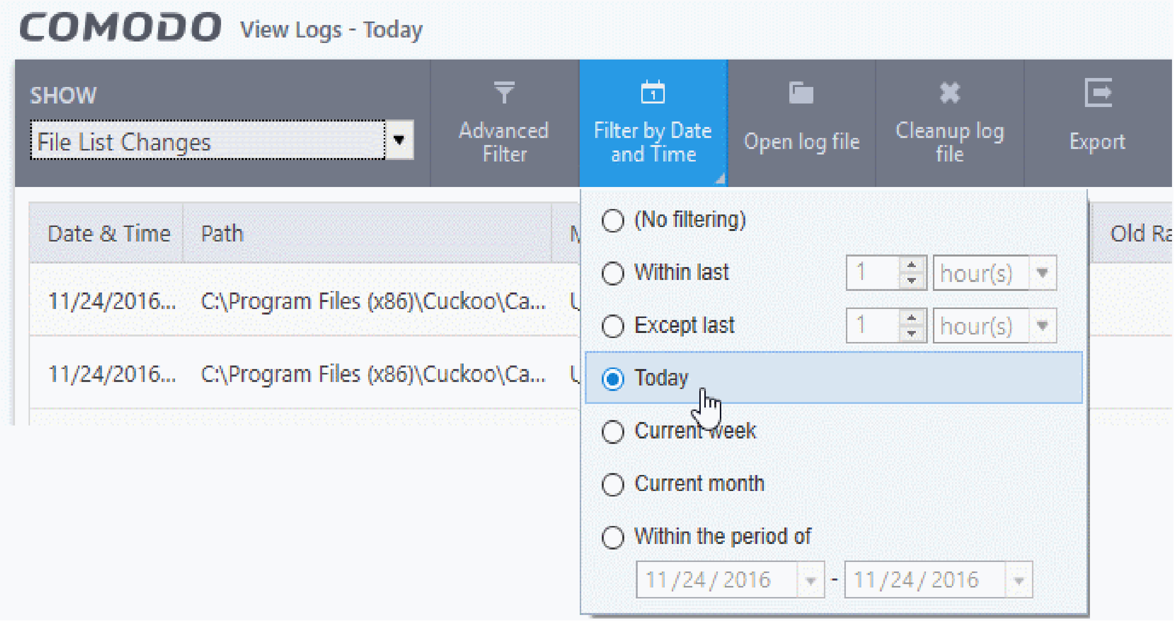
Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria.

You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:

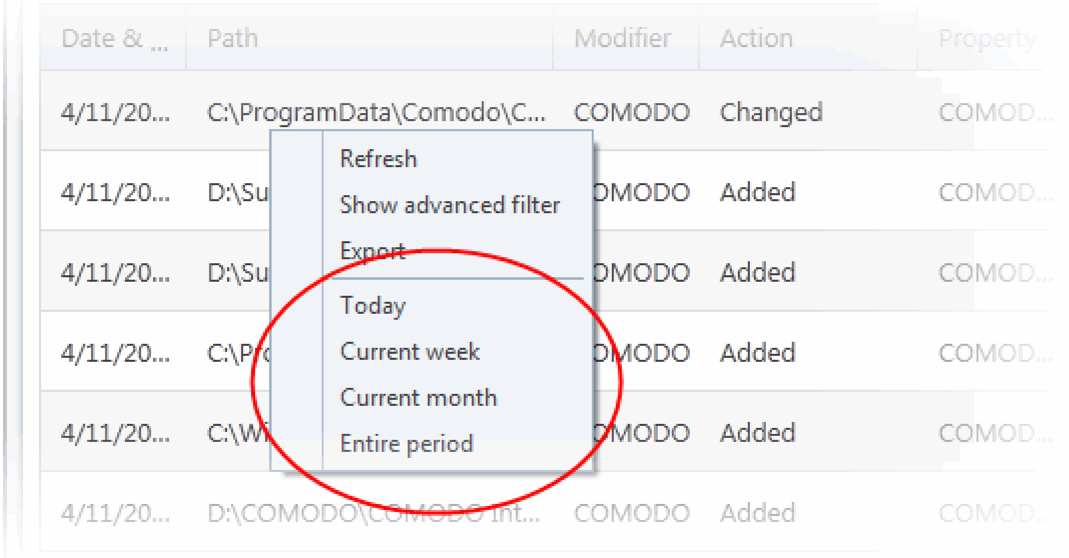


Date & Time	Path
11/24/2016...	C:\Program Files (x86)\Cuckoo\Ca...
11/24/2016...	C:\Program Files (x86)\Cuckoo\Ca...

○ (No filtering)
○ Within last 1 hour(s)
○ Except last 1 hour(s)
● Today
○ Current week
○ Current month
○ Within the period of
11/24/2016 - 11/24/2016

- **No filtering -** Displays every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Within last -** Shows logs from a certain point in the past until the present time.
- **Except last -** Excludes logs from a certain point in the past until the present time.
- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month -** Displays all logged events during the month.
- **Within the period of -** Enables you to select a custom period by choosing 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period:



Date & ...	Path	Modifier	Action	Property
4/11/20...	C:\ProgramData\Comodo\C...	COMODO	Changed	COMOD...
4/11/20...	D:\Su	OMODO	Added	COMOD...
4/11/20...	D:\Su	OMODO	Added	COMOD...
4/11/20...	C:\Pr	OMODO	Added	COMOD...
4/11/20...	C:\W	OMODO	Added	COMOD...
4/11/20...	D:\COMODO\COMODO Int...	COMODO	Added	COMOD...

Advanced Filters

You can further refine which events are displayed according to specific filters. The following additional filters are available:

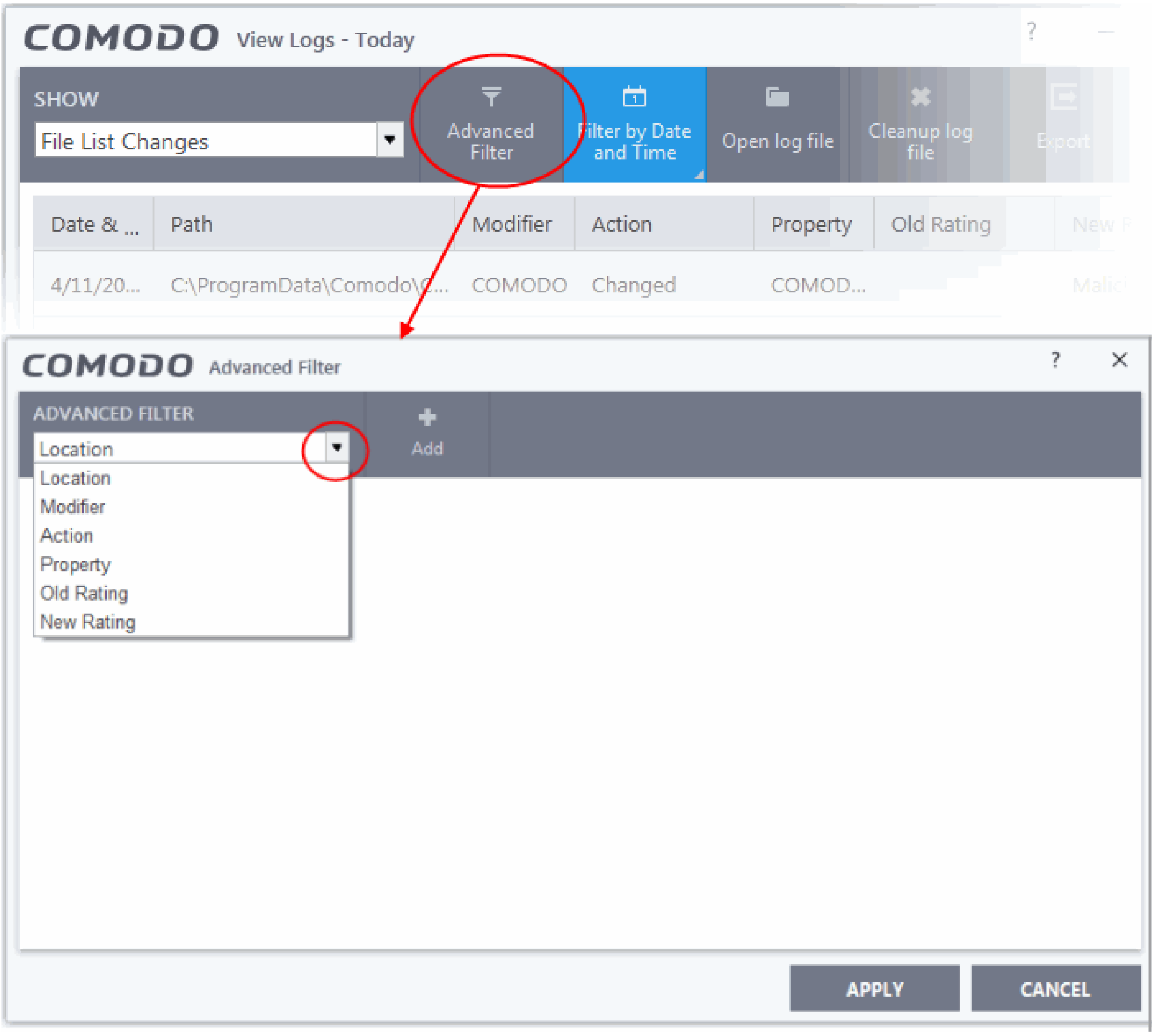
- **Location -** Displays only change logs based on entered file location.
- **Modifier -** Displays only change logs based on change done by such as (User, Administrator, and Comodo).
- **Action -** Displays only change logs for selected actions such as (Added, Removed or Changed).
- **Property** - Displays only change logs based on file rating done by such as (Administrator, User, and Comodo rating).
- **Old Rating -** Displays only change logs based on the old file rating.
- **New Rating -** Displays only change logs based on the new file rating.

To configure filters for 'File List Changes' logs

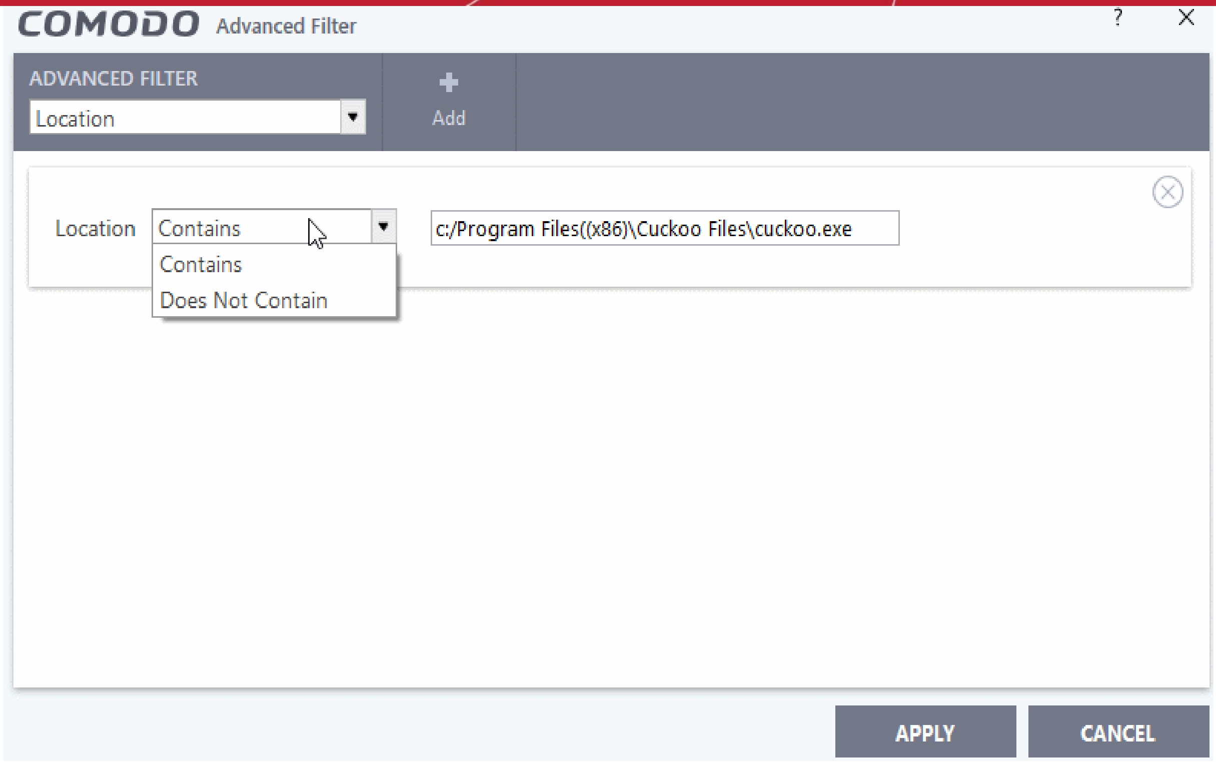
1. Click the 'Advanced Filter' button from the title bar (or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu).

The 'Advanced Filter' interface for 'File List Changes' log viewer will be displayed.

2. Select a filter from the 'Advanced Filter' drop-down and click 'Add':



i. **Location**: Filter file list changes according to their CIS code. You can view file list changes in the 'Location' column of the log viewer. Selecting the 'Location' option will display drop-down and text entry fields.

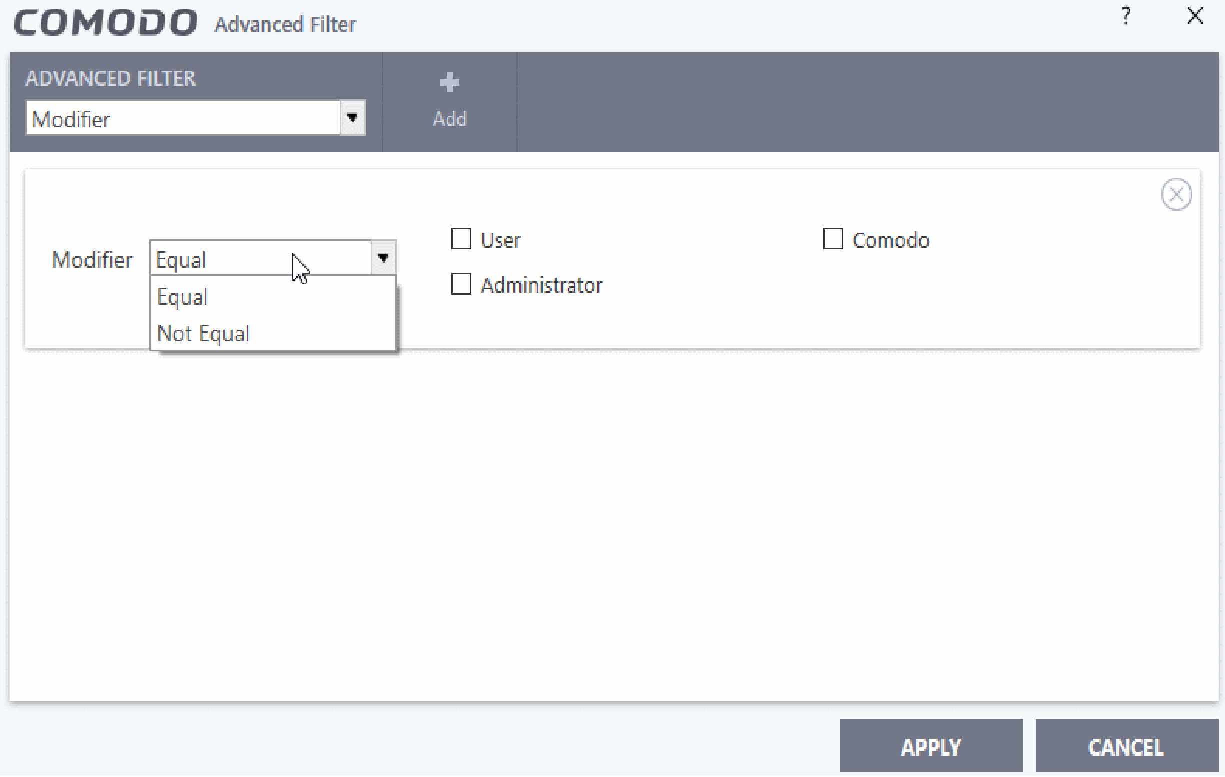


a) Select 'Contains' or 'Does Not Contain' option from the drop-down. 'Does Not Contain' will invert your selected choice.

b) Enter the location or a part of it as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'C:\Program Files (x86)\Cuckoo Files\Cuckoo.exe in the text field, then only log entries with the same value in the 'Path' column will be displayed.

ii. **Modifier**: Allows you to filter logs based on the file list changes. Selecting the 'Modifier' option displays drop-down box and a set of specific filter parameters.



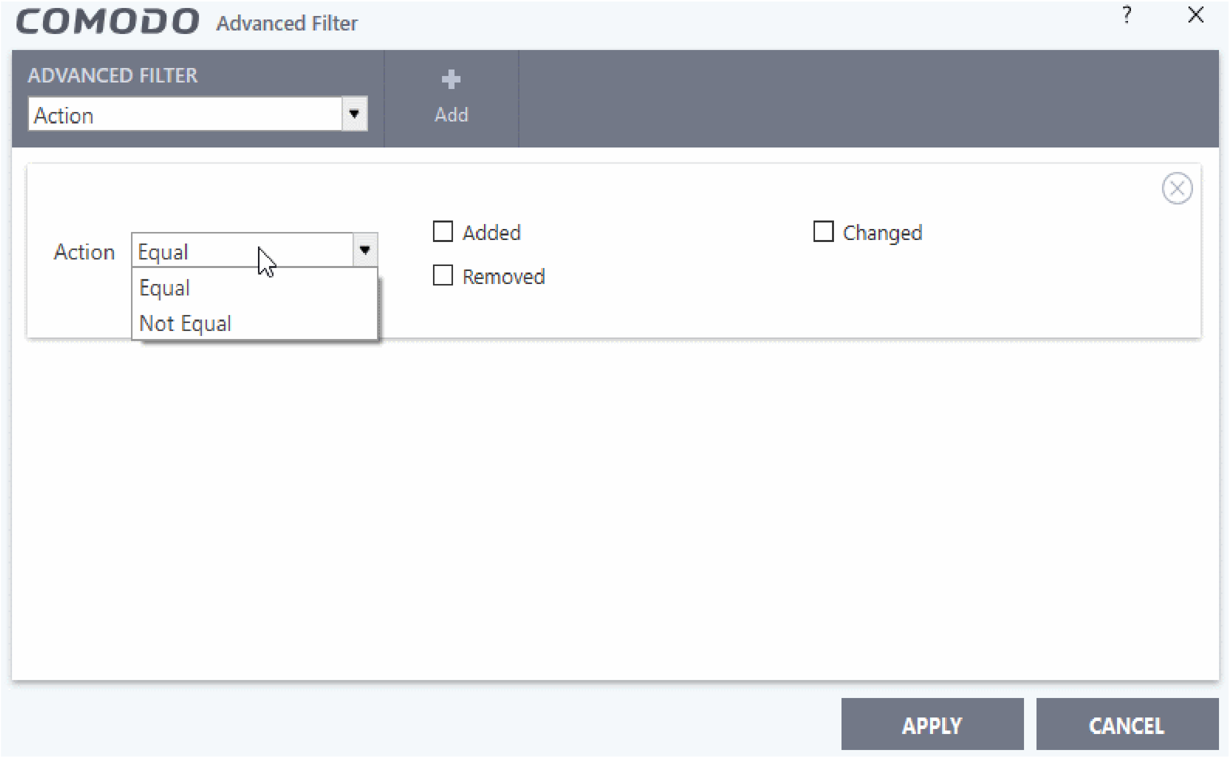
a) Select 'Equal' or 'Not Equal' option from drop down. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- User
- Comodo
- Administrator

For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs changes done by the user will be displayed.

iii. **Action**: The 'Action' option allows you to filter log entries based on the 'Action' column of the log viewer. Selecting the 'Action' option displays drop-down box and a set of specific filter parameters that can be selected or deselected.



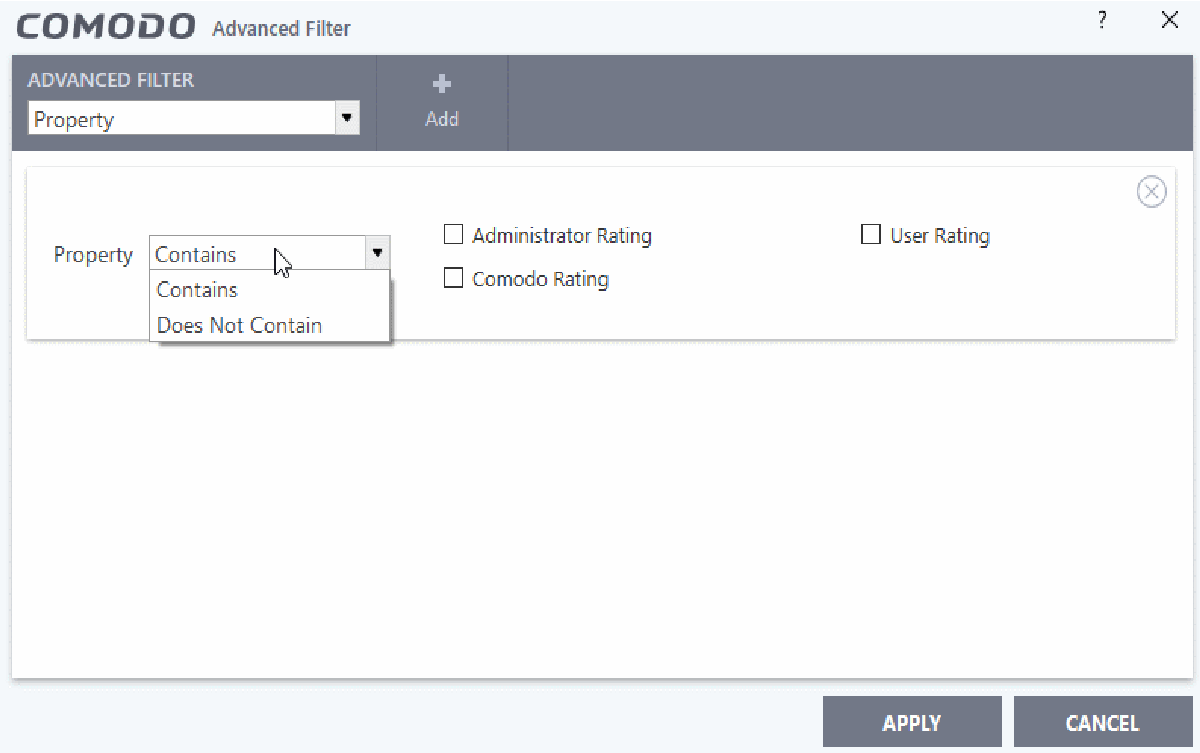
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Added
- Changed
- Removed

For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only logs of files that were removed from the file list will be displayed.

iv. **Property**: Allows you to filter log entries based on the file rating. Selecting the 'Property' option displays a drop-down box and a set of specific filter parameters.



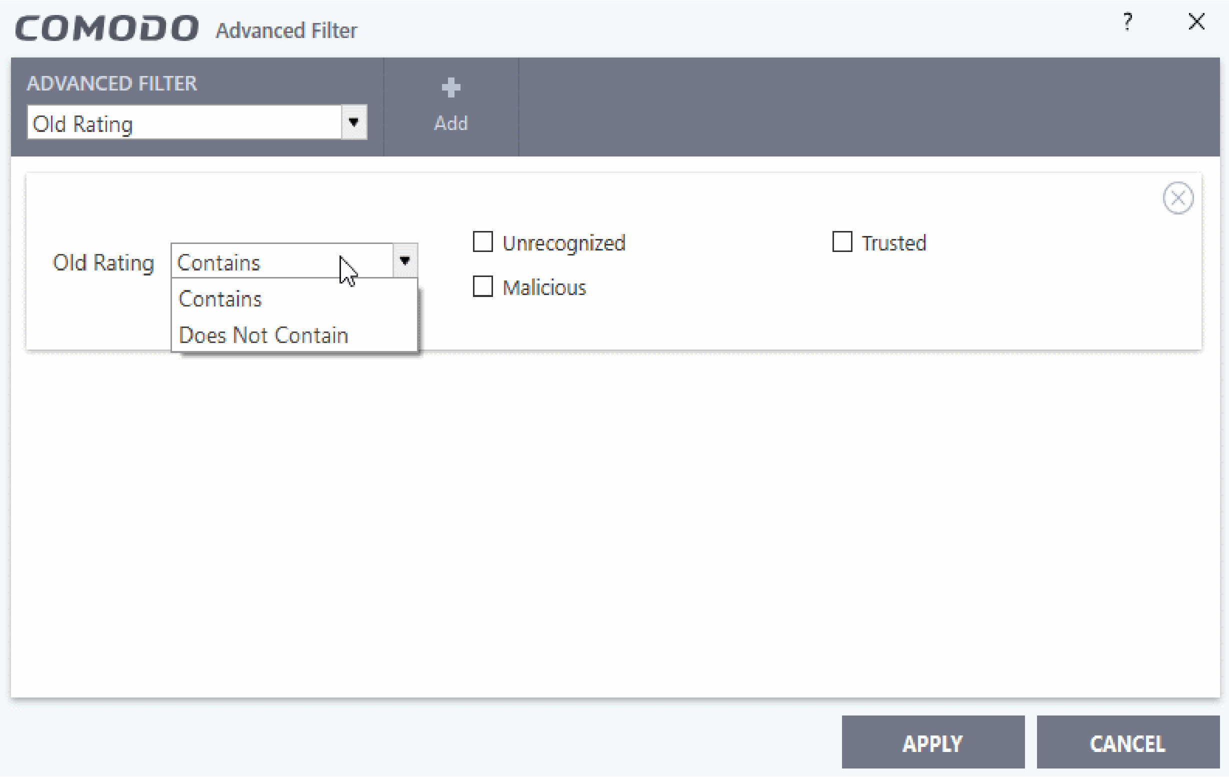
a) Select 'Contains' or 'Does Not Contain' option from the drop down. 'Does Not Contain' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Administrator Rating
- User Rating
- Comodo Rating

For example, if you select 'Equal' from the drop-down and select 'User Rating' checkbox, only the logs of files that were rated by the user will be displayed.

v. **Old Rating**: Allows you to filter log entries based on old file rating before its rating was changed. Selecting the 'Old Value' option displays a drop-down and a set of specific filter parameters.



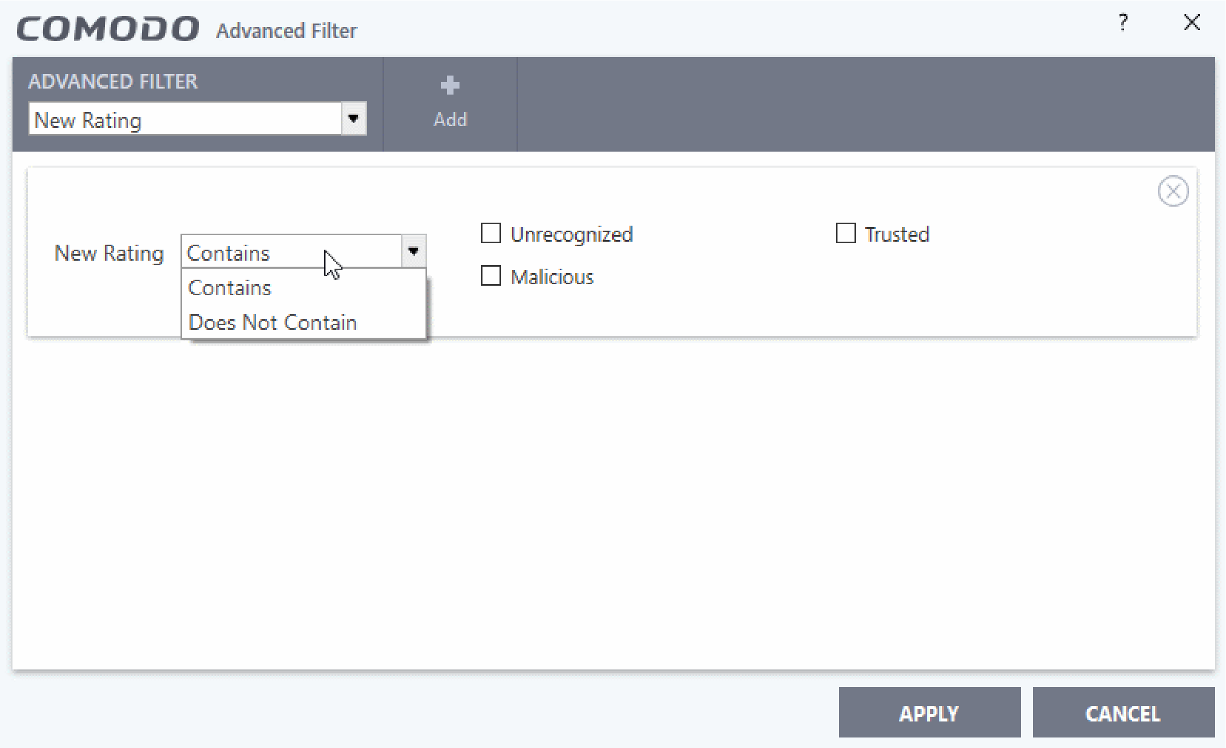
a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Unrecognized
- Trusted
- Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' under the 'Old Value' column will be displayed.

vi. **New Rating**: Allows you to filter log entries based on new file rating before its rating was changed. Selecting the 'Old Value' option displays a drop-down and a set of specific filter parameters.



a) Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Unrecognized
- Trusted
- Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' under the 'New Value' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

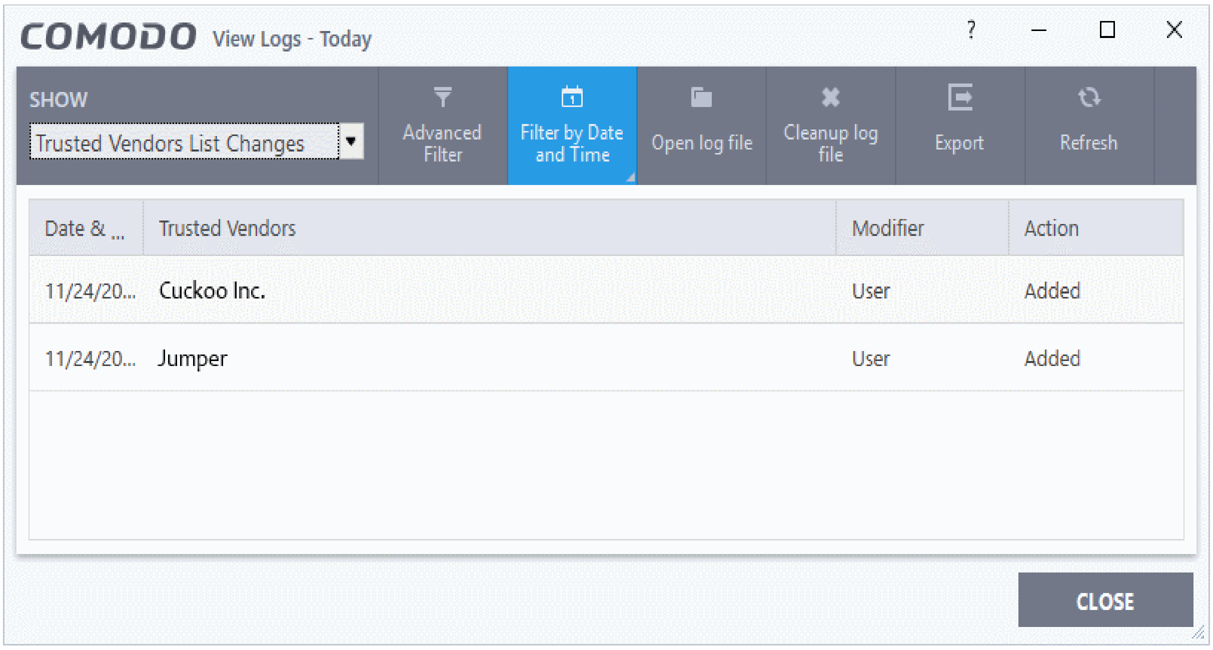
- Click 'Apply' for the filters to be applied to the 'File List Changes' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.5.10. Trusted Vendors List Changes Logs

CIS has a built-in list of trusted software publishers which are shown in the 'Trusted Vendors List'. Files from trusted vendors are excluded from CIS scanning. You can add or remove vendors from the list (see '**Trusted Vendors List**' for more details). Changes to this list are logged under 'Trusted Vendor List Changes'.

To view the 'Trusted Vendors List Changes' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs' OR click the 'Logs' button at the top-right of the home screen in basic view.
- Select 'Trust Vendors List Changes' from the 'Show' drop-down.



Date & ...	Trusted Vendors	Modifier	Action
11/24/20...	Cuckoo Inc.	User	Added
11/24/20...	Jumper	User	Added

Column Descriptions

1. **Date & Time -** Indicates date and time when the log was generated.
2. **Trusted Vendors -** Displays names of the software publisher.
3. **Modifier -** Indicates who the changes were done by (User, Administrator or Comodo).
4. **Action -** Indicates the type of action done for the file. For example, removed or added to the list.

- To export the 'Trusted Vendors List Changes' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open log file' button.
- To refresh the 'Trusted Vendors List Changes' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the 'Trusted Vendors List Changes' logs click the 'Cleanup log file' button.
- You can sort the entries by ascending \ descending order by clicking on the respective column headers.

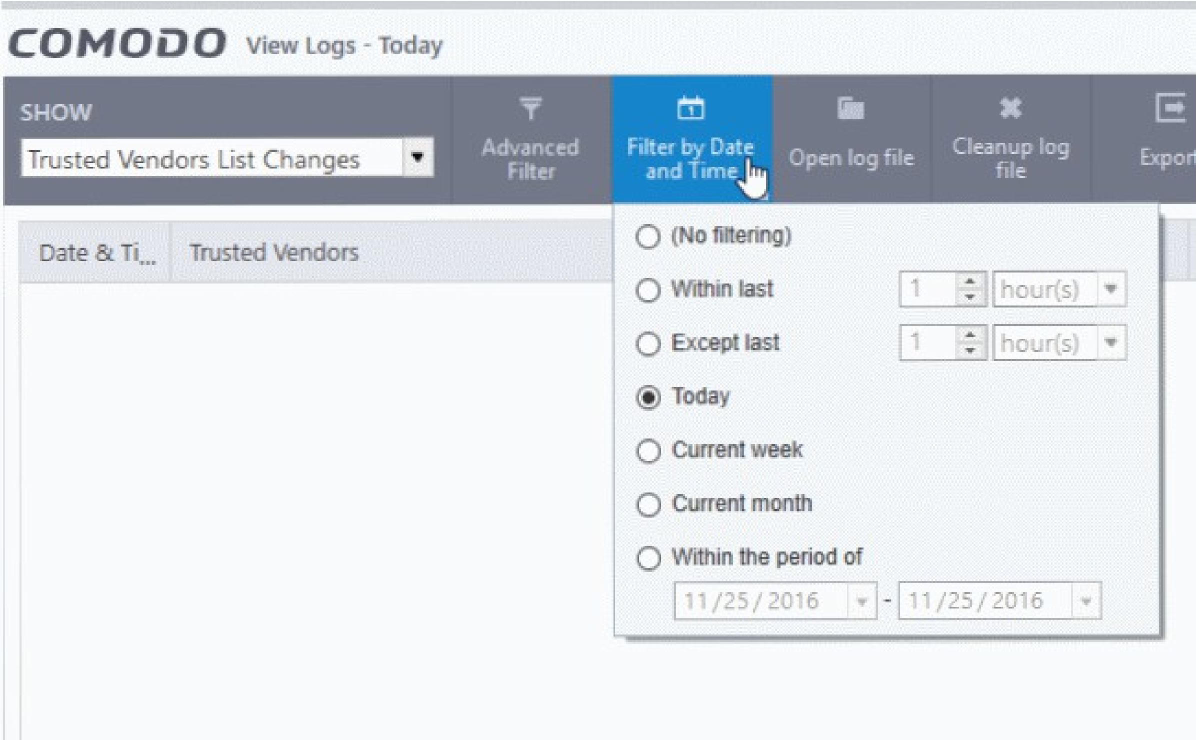
5.5.10.1. Filtering Trusted Vendors List Changes Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

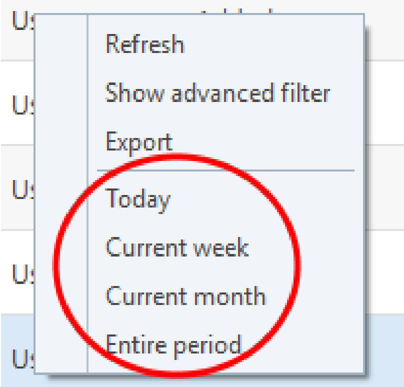
Preset Time Filters

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



- **No filtering -** Displays every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Shows logs from a certain point in the past until the present time.
- **Except last** - Excludes logs from a certain point in the past until the present time.
- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month -** Displays all logged events during the month.
- **Within the period of** - Enables you to select a custom period by choosing 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

You can further refine which events are displayed according to specific filters. The following additional filters are available:

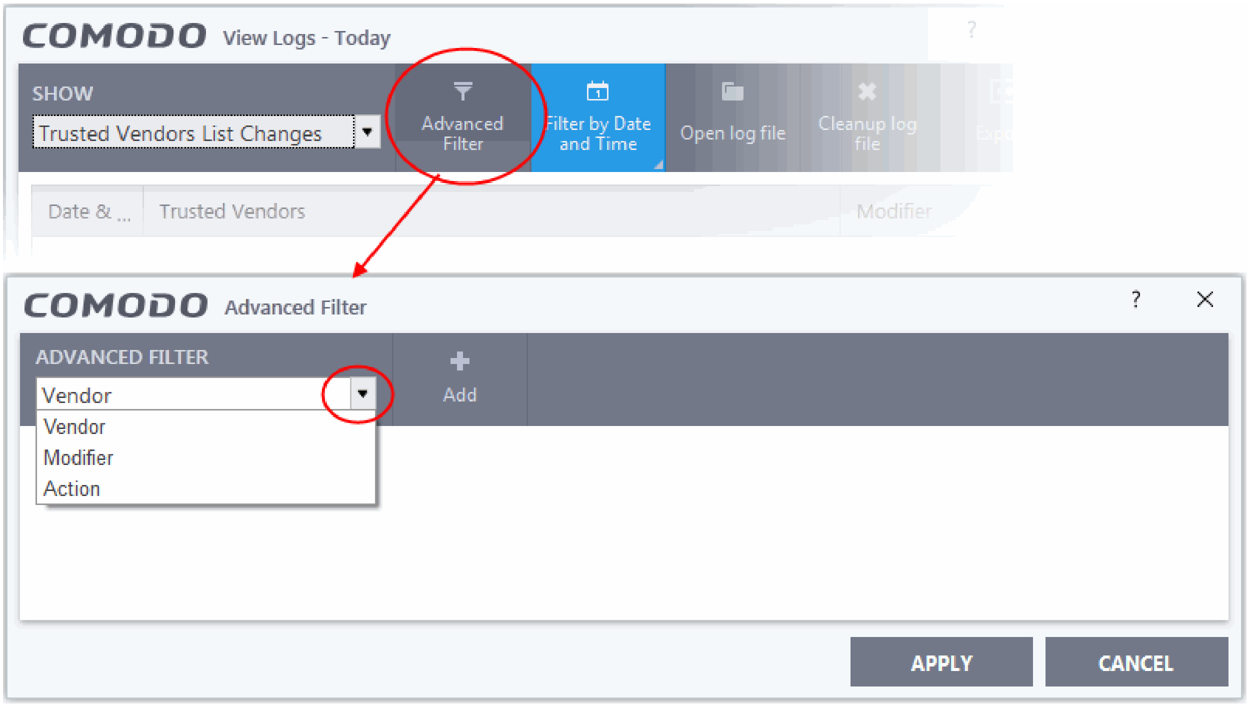
- **Vendors** - Displays logs according to software publisher name.
- **Modifier** - Displays logs according to who made the change (User, Administrator, and Comodo).
- **Action -** Displays logs according to the selected action(s). For example, object added or removed.

To configure Advanced filters Trusted Vendors List Changes logs

1. Click the 'Advanced Filter' button from the title bar (or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu).

The 'Advanced Filter' interface for the 'Trusted Vendors List Changes' log viewer will open.

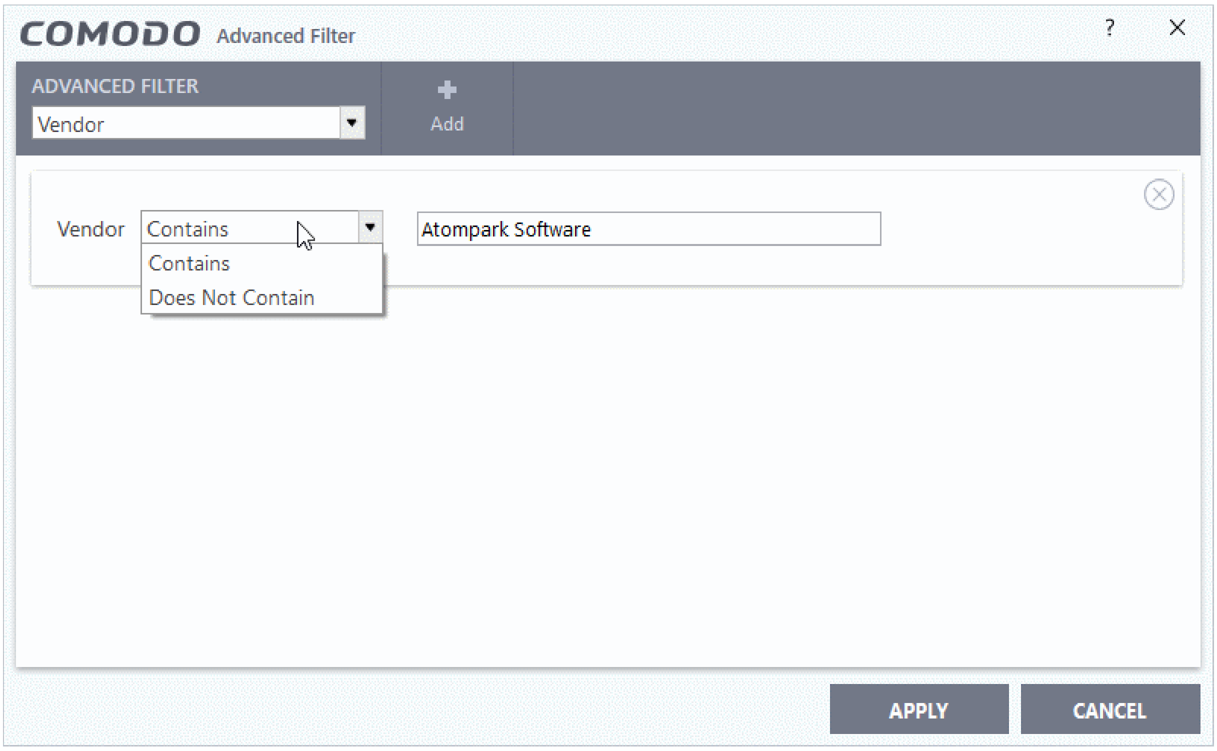
2. Select a filter from the 'Advanced Filter' drop-down and click 'Add':



There are 3 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Add' drop-down menu:

i. **Vendor**: Allows you to filter the change logs based on a software publisher name. Selecting the 'Vendor' option displays a drop-down and text entry fields.

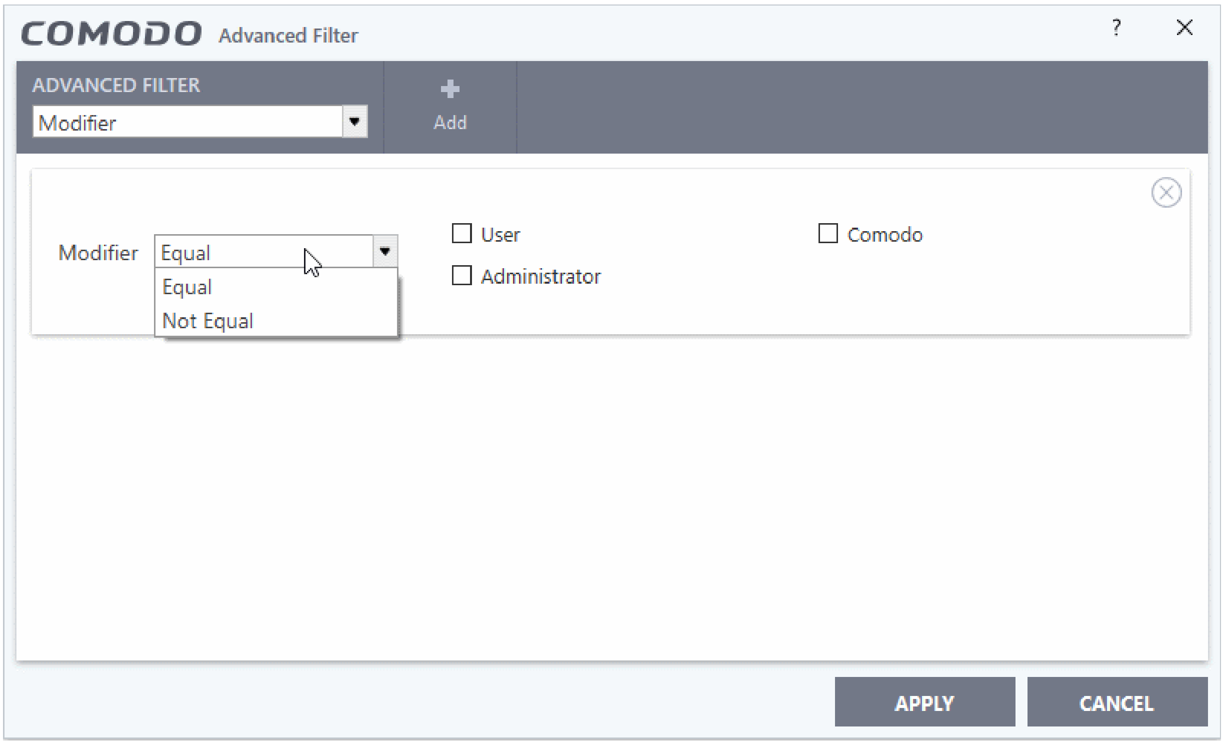


a) Select 'Contains' or 'Does Not Contain' option from the drop-down. 'Does Not Contain' will invert your selected choice.

b) Enter the vendor name in full or a part of it as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'Atompark Software' in the text field, then only log entries with the same name 'Atompark Software' in the 'Trusted Vendors' column will be displayed.

ii. **Modifier**: Allows you to filter logs based on 'Trusted Vendors' list changes done. Selecting the 'Modifier' option displays drop-down box and a set of specific filter parameters.



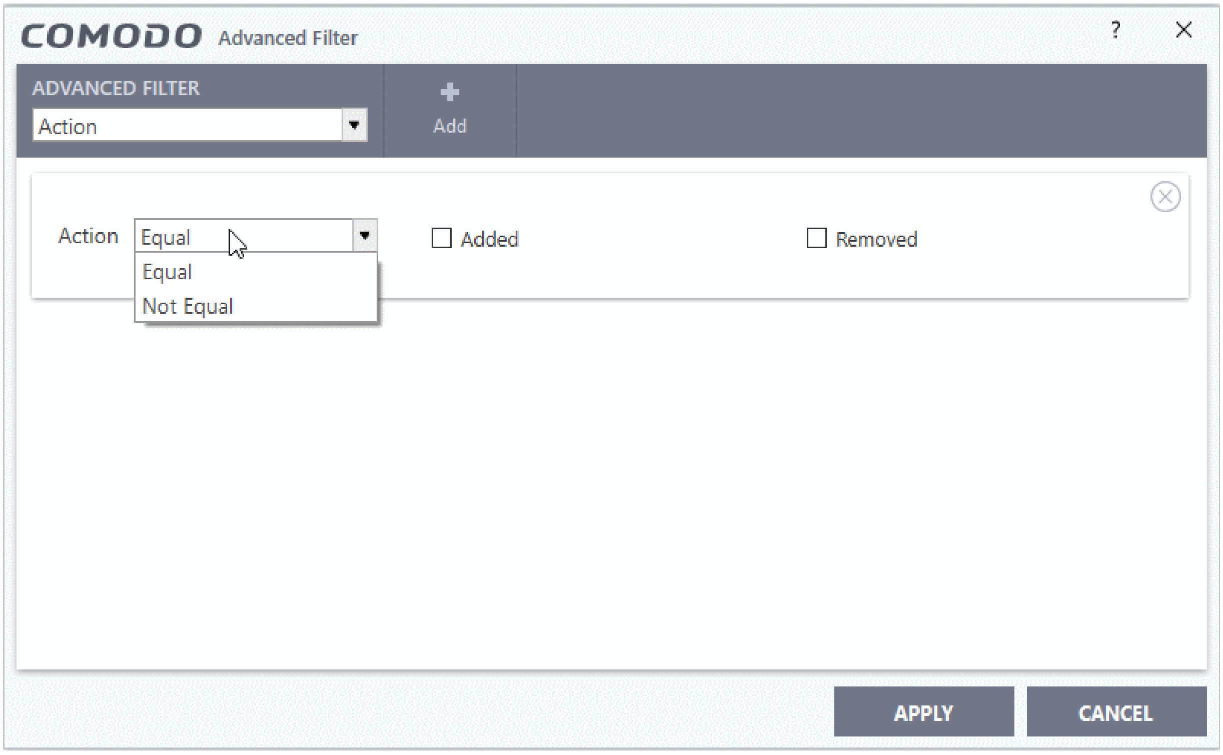
a) Select 'Equal' or 'Not Equal' option from drop down. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- User
- Comodo
- Administrator

For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs changes done by the user under 'Modifier' column will be displayed.

iii. **Action**: Allows you to filter log entries based on 'Trusted Vendors' list changes done. Selecting the 'Action' option displays drop-down box and set of specific filter parameters.



a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Added
- Removed

For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only logs of trusted vendors that were removed from the list will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

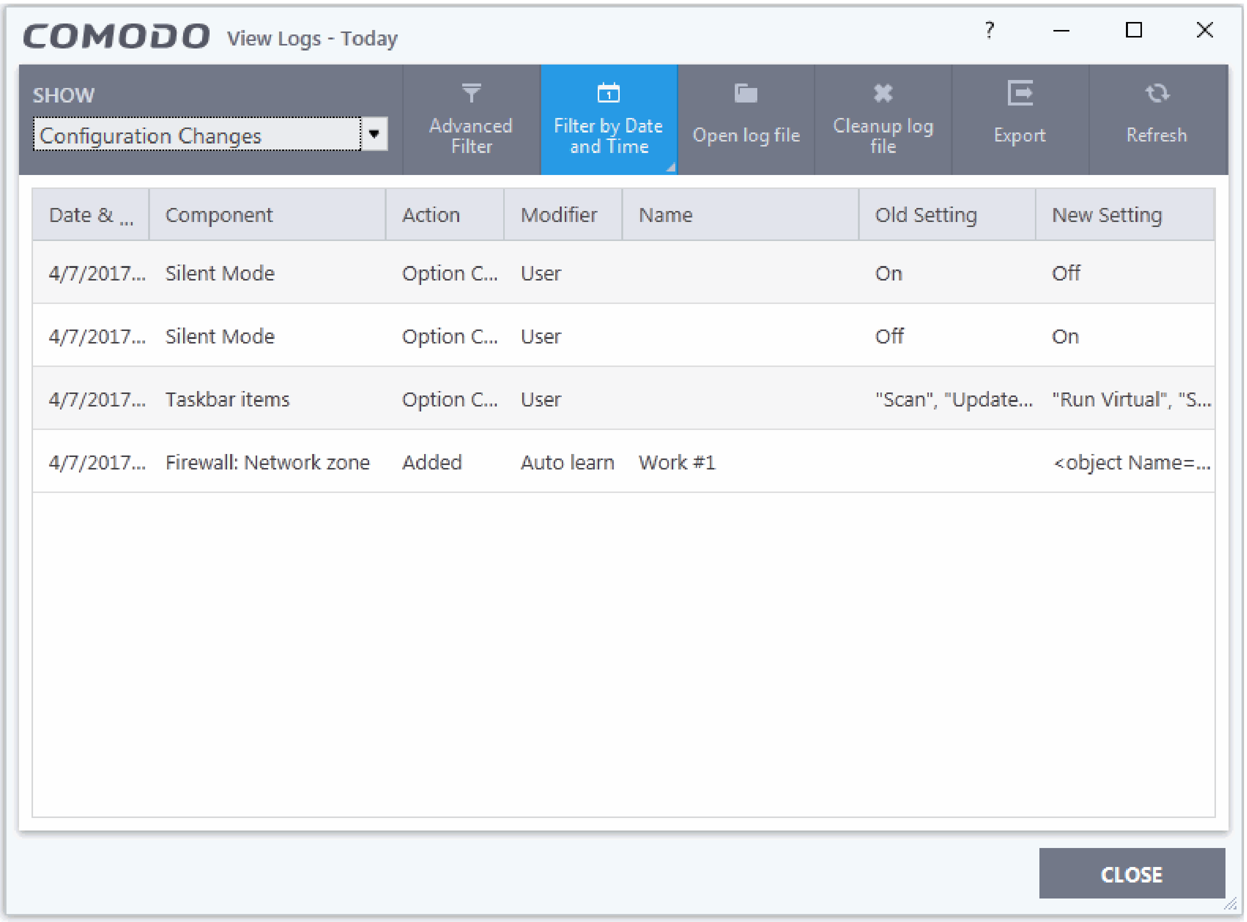
- Click 'Apply' for the filters to be applied to the 'Trusted Vendors List Changes' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.5.11. Configuration Changes Logs

The 'Configuration Changes Log' is where CIS records all changes made to its settings since installation. The log can be viewed by selecting 'Configuration Changes' from the 'Show' drop-down of the log viewer interface.

To view the 'Configuration Changes' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs' OR click the 'Logs' button at the top-right of the home screen in basic view.
- Select 'Configuration Changes' from the 'Show' drop-down.



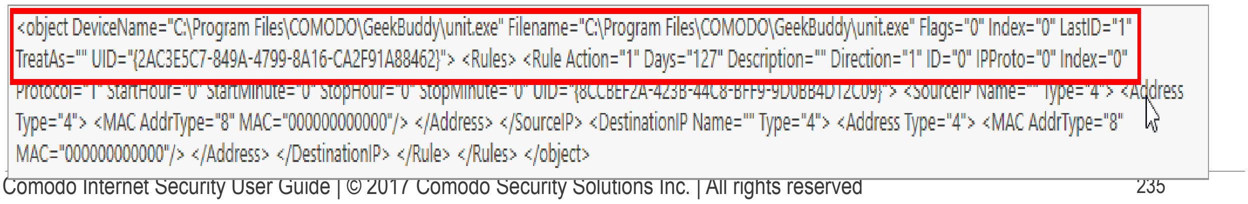
SHOW: Configuration Changes

Date & ...	Component	Action	Modifier	Name	Old Setting	New Setting
4/7/2017...	Silent Mode	Option C...	User		On	Off
4/7/2017...	Silent Mode	Option C...	User		Off	On
4/7/2017...	Taskbar items	Option C...	User		"Scan", "Update...	"Run Virtual", "S...
4/7/2017...	Firewall: Network zone	Added	Auto learn	Work #1		<object Name=...

Column Descriptions

1. **Date & Time -** Indicates date and time when the change occurred.
2. **Action -** Indicates the type of action applied to the component. For example, whether the component was removed, added or changed.
3. **Modifier -** Indicates who the changes were done by (User, Antivirus Alert, Auto Learn, Firewall Alert, HIPS Alert, Containment Alert, Scheduler, Comodo, and Administrator)
4. **Name -** Indicates the name of the rule, program or the file that has been changed.
5. **Old Setting -** Indicates parameter value before configuration change.
6. **New Setting -** Indicates parameter value after configuration change.

- To view full details of a particular configuration change, place your mouse cursor over the entry in the 'Old



```
<object DeviceName="C:\Program Files\COMODO\GeekBuddy\unit.exe" Filename="C:\Program Files\COMODO\GeekBuddy\unit.exe" Flags="0" Index="0" LastID="1"
TreatAs="" UID="{2AC3E5C7-849A-4799-8A16-CA2F91A88462}"> <Rules> <Rule Action="1" Days="127" Description="" Direction="1" ID="0" IPProto="0" Index="0"
Protocol="1" StartHour="0" StartMinute="0" StopHour="0" StopMinute="0" UID="{8CCBEF2A-423B-44C8-BFF9-9D0BB4D12C09}"> <SourceIP Name="" Type="4"> <Address
Type="4"> <MAC AddrType="8" MAC="000000000000"/> </Address> </SourceIP> <DestinationIP Name="" Type="4"> <Address Type="4"> <MAC AddrType="8"
MAC="000000000000"/> </Address> </DestinationIP> </Rule> </Rules> </object>
```

Value' or 'New Value' column

- To export the 'Configuration Changes' logs as a HTML file, click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open log file' button.
- To refresh the 'Configuration Changes' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the 'Configuration Changes' logs click the 'Cleanup log file' button.
- You can sort the entries by ascending \ descending order by clicking on the respective column headers.

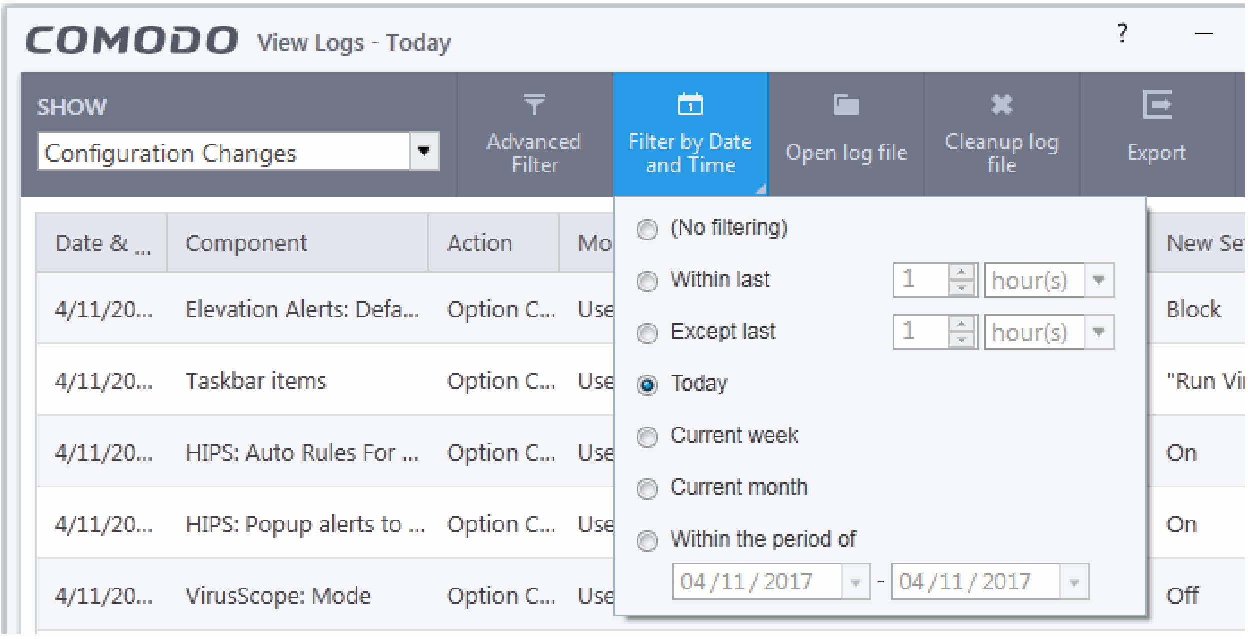
5.5.11.1. Filtering 'Configuration Changes' Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

- Clicking the 'Filter by Date and Time' button at the top enables you to filter the logs for a selected time period:



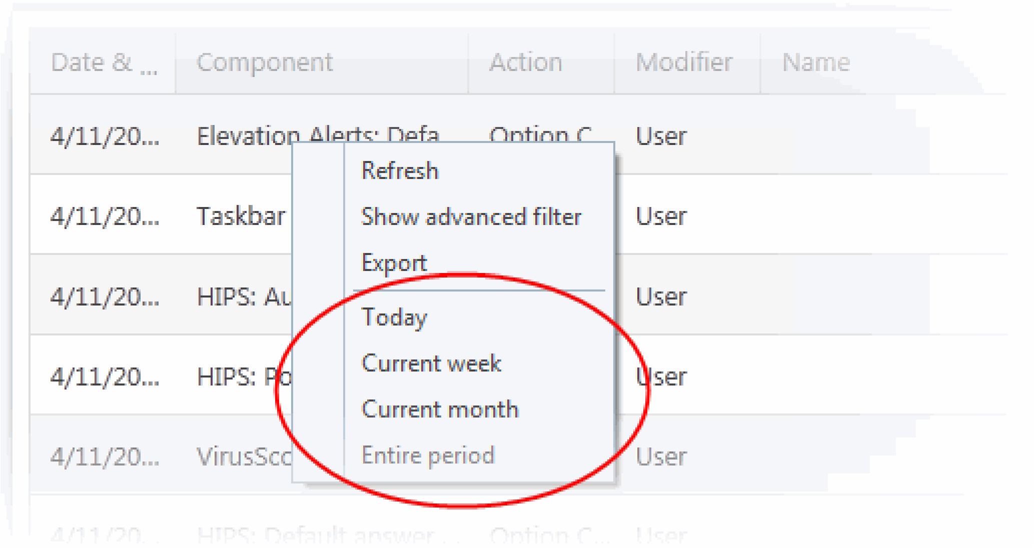
SHOW: Configuration Changes

Date & ...	Component	Action	Mo	New Se
4/11/20...	Elevation Alerts: Defa...	Option C...	Use	Block
4/11/20...	Taskbar items	Option C...	Use	"Run Vi
4/11/20...	HIPS: Auto Rules For ...	Option C...	Use	On
4/11/20...	HIPS: Popup alerts to ...	Option C...	Use	On
4/11/20...	VirusScope: Mode	Option C...	Use	Off

○ (No filtering)
○ Within last 1 hour(s)
○ Except last 1 hour(s)
● Today
○ Current week
○ Current month
○ Within the period of
04 / 11 / 2017 - 04 / 11 / 2017

- **No filtering -** Displays every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Displays logs from a certain point in the past until the present time.
- **Except last** - Excludes logs from a certain point in the past until the present time.
- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month -** Displays all logged events during the month.
- **'Within the period of'** - Enables you to select a custom period by choosing 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Date & ...	Component	Action	Modifier	Name
4/11/20...	Elevation Alerts: Defa	Option C	User	
4/11/20...	Taskbar		User	
4/11/20...	HIPS: Au		User	
4/11/20...	HIPS: Po		User	
4/11/20...	VirusSco		User	
4/11/20...	HIPS: Default answer ...	Option C...	User	

Advanced Filters

You can further refine which events are displayed according to specific filters. The following additional filters are available:

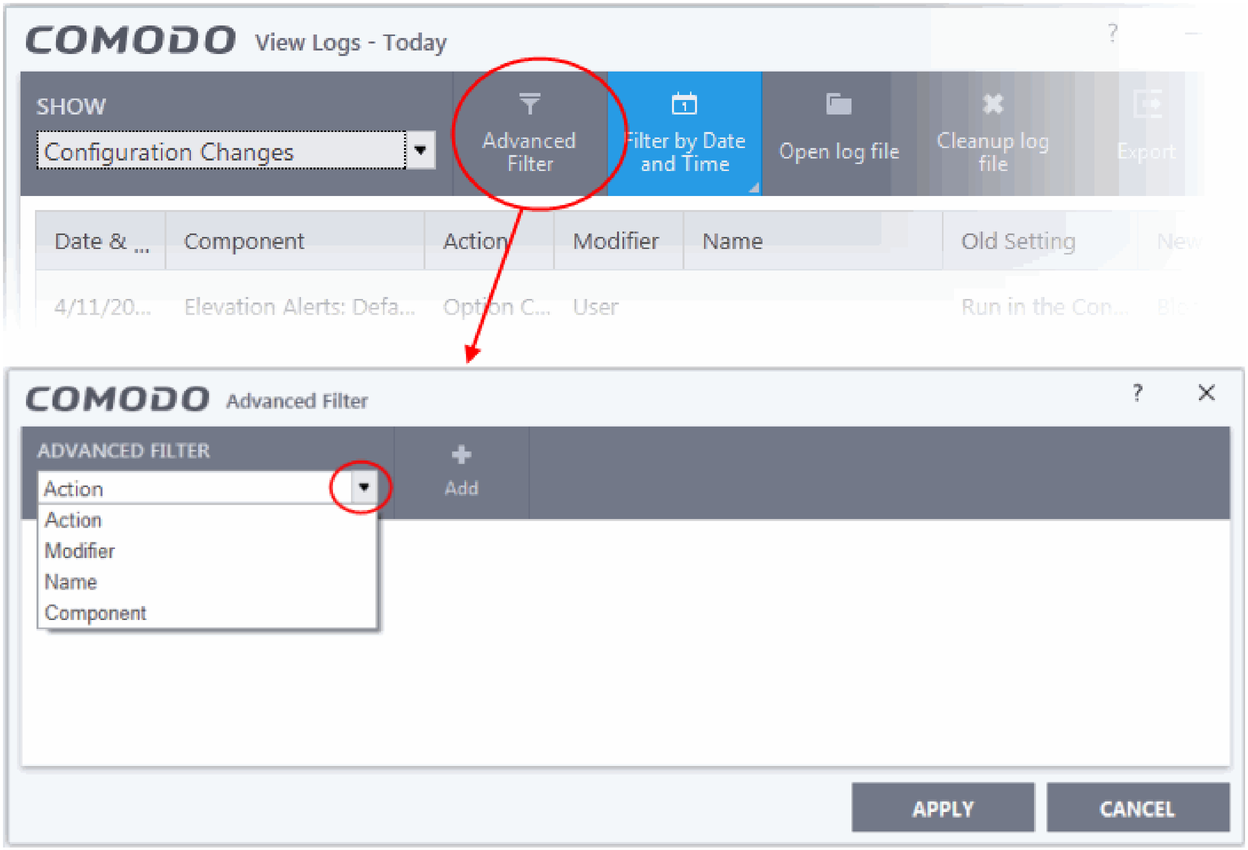
- **Action:** Displays only logs for the selected action(s). Example actions are add, remove and change of rules.
- **Modifier:** Filters logs based on the source of the change. Example sources include the user making a change at an alert, auto-learning, the scheduler, Comodo, Administrator and so on.
- **Name:** Filters logs based on the name of the object.
- **Component:** Filters logs according to changes in selected CIS components and settings

To configure Advanced Filters for 'Configuration Changes' Logs

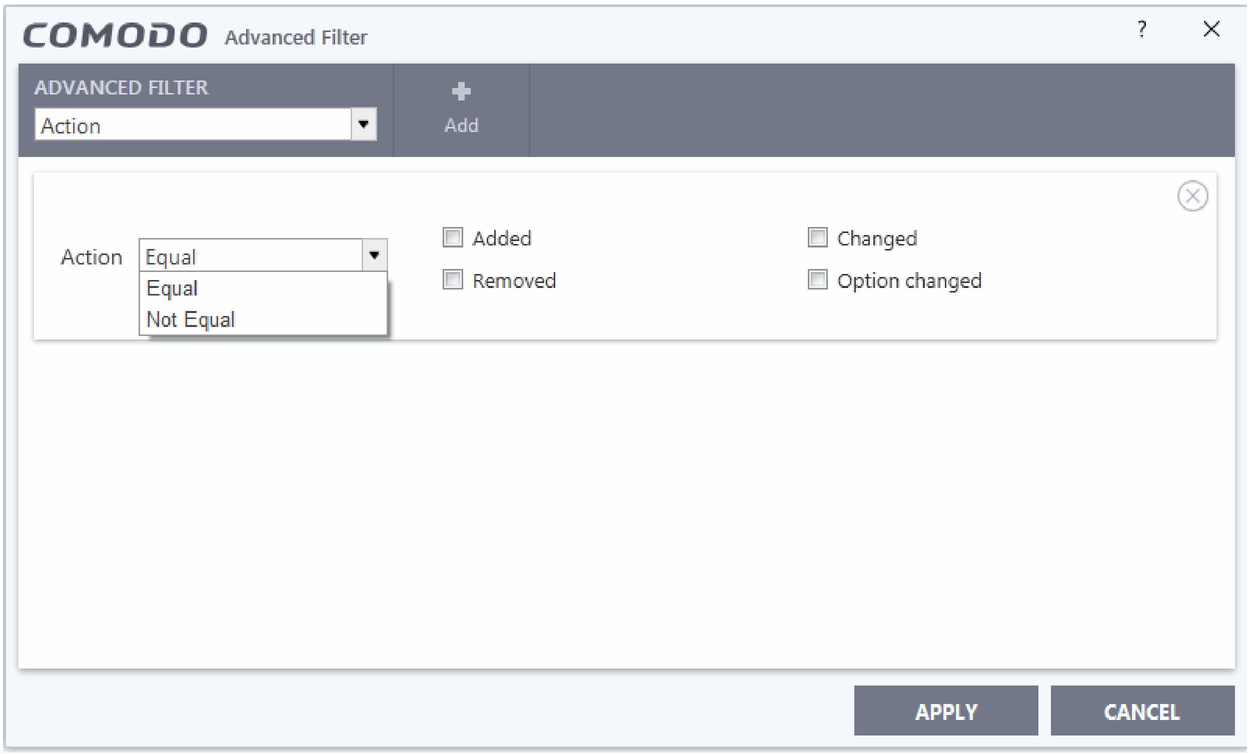
1. Click the 'Advanced Filter' button from the title bar (or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu).

The Advanced Filter interface for 'Configuration Changes' logs will open.

2. Select a filter from the 'Advanced Filter' drop-down and click 'Add':



i. **Action**: Allows you to filter log entries based on the actions executed. These include a change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



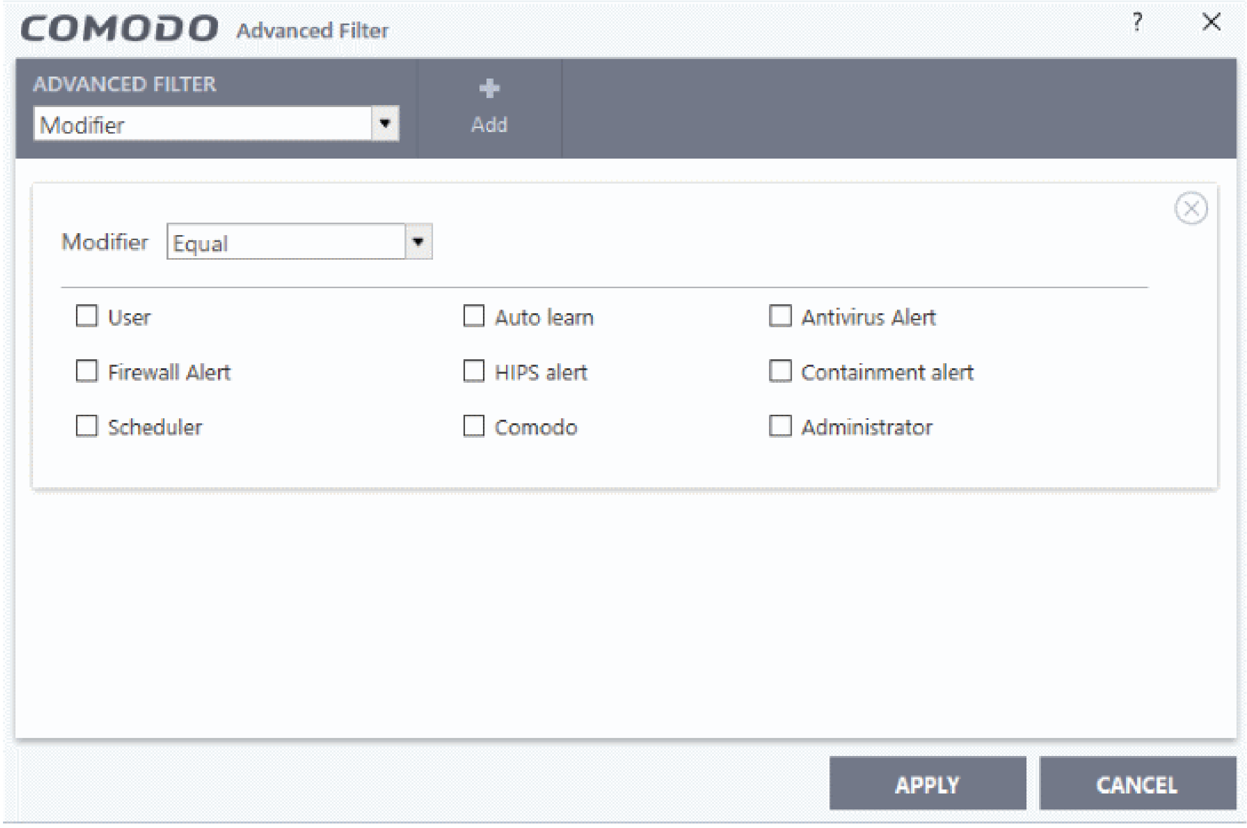
a) Select 'Equal' or 'Not Equal' option from drop-down. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Added
- Changed
- Removed
- Option changed

For example, if you choose 'Equal' from the drop-down and select 'Added' checkbox, only logs entries with the value 'Added' under 'Action' column will be displayed.

ii. **Modifier**: Allows you to filter log entries based on the entity that is responsible for the configuration change. It can be the user or the response given to an alert. Selecting the 'Modifier' option displays drop-down box and a set of specific filter parameters.



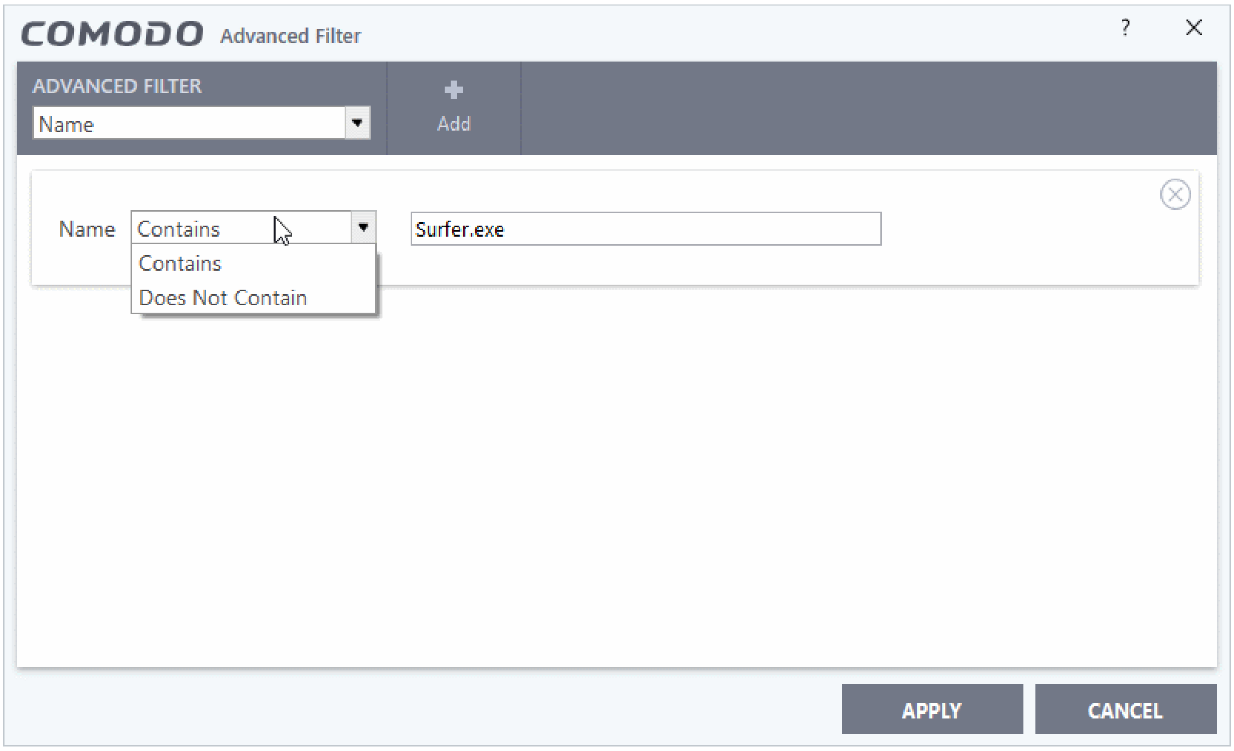
a) Select 'Equal' or 'Not Equal' option from drop-down. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- User
- Auto learn
- Antivirus Alert
- Firewall Alert
- HIPS alert
- Containment Alert
- Scheduler
- Comodo
- Administrator

For example, if you have chosen 'Equal' from the drop-down and selected 'Antivirus Alert ' checkbox, only logs entries related to the configuration changes effected by responses to 'Antivirus Alerts' will be displayed.

iii. **Name**: The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down and text entry field.

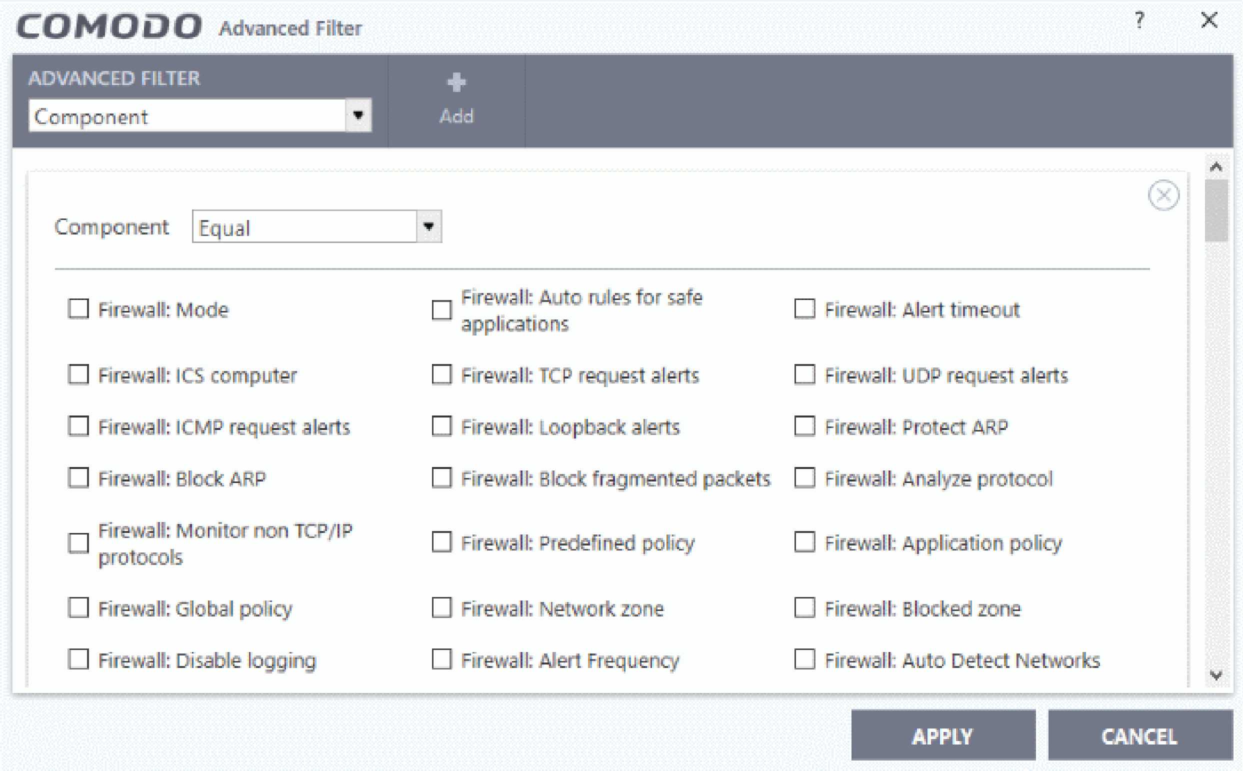


a) Select 'Contains' or 'Does Not Contain' option from drop-down. 'Does Not Contain' will invert your selected choice.

b) Enter the name in full or a part of it as your filter criteria in the text field.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'surfer.exe' in the text field, then only the log entries containing the surfer.exe in the name column will be displayed.

iv. **Component**: Allows you to filter log entries related to the objects modified during the configuration change. Selecting the 'Object' option displays drop down and the objects of CIS configuration.



- □ Firewall: Mode
- □ Firewall: ICS computer
- □ Firewall: ICMP request alerts
- □ Firewall: Block ARP
- □ Firewall: Monitor non TCP/IP protocols
- □ Firewall: Global policy
- □ Firewall: Disable logging
- □ Firewall: Auto rules for safe applications
- □ Firewall: TCP request alerts
- □ Firewall: Loopback alerts
- □ Firewall: Block fragmented packets
- □ Firewall: Predefined policy
- □ Firewall: Network zone
- □ Firewall: Alert Frequency
- □ Firewall: Alert timeout
- □ Firewall: UDP request alerts
- □ Firewall: Protect ARP
- □ Firewall: Analyze protocol
- □ Firewall: Application policy
- □ Firewall: Blocked zone
- □ Firewall: Auto Detect Networks

a) Select 'Equal' or 'Not Equal' option from drop down. 'Not Equal' will invert your selected choice.

b) Now select the check-boxes of the specific filter parameters to refine your search. Scroll down the window to see all the parameters options.

For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode ' checkbox, only log entries related to the change of Firewall mode will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

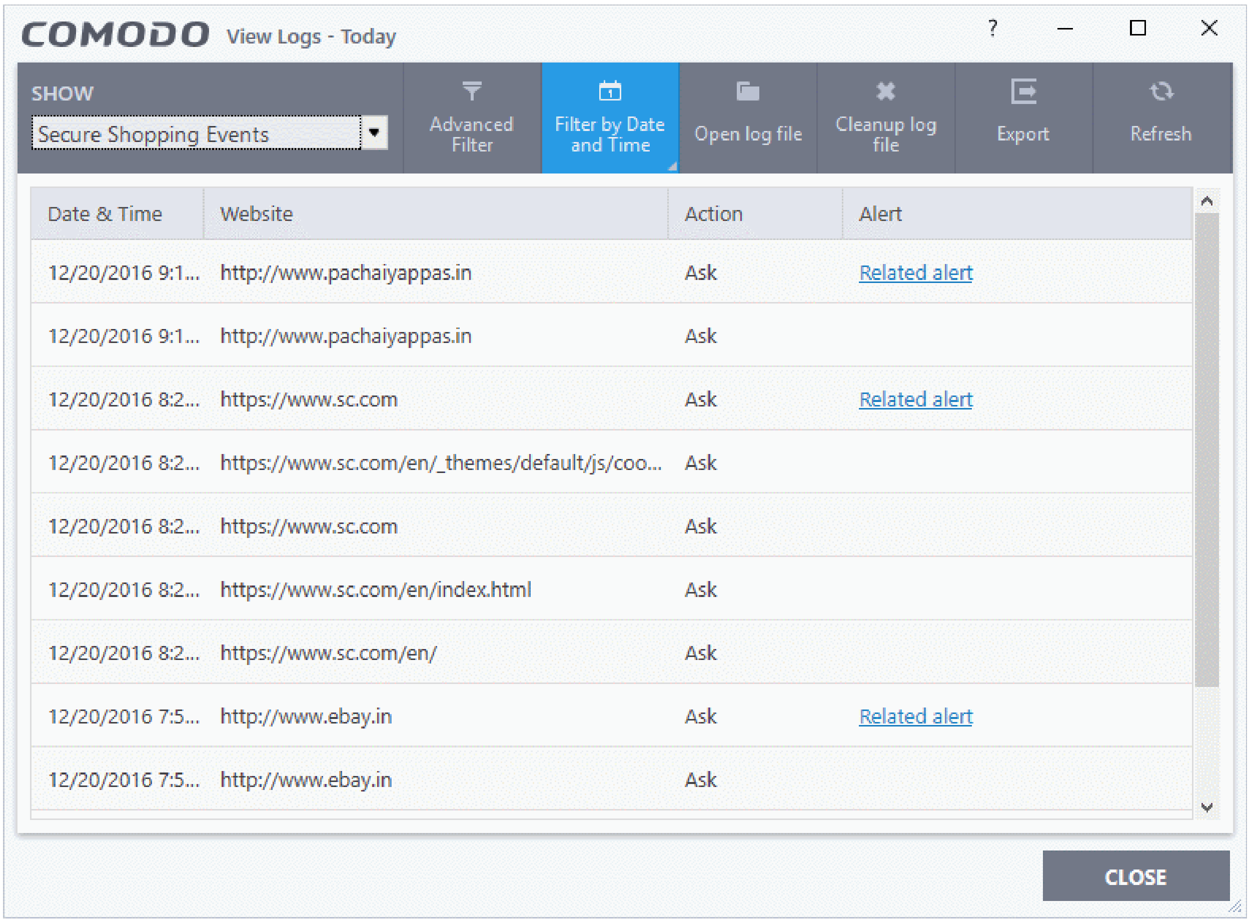
- Click 'Apply' for the filters to be applied to the 'Configuration Changes' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- To clear filters, open the 'Advanced Filter' pane and remove each filter by clicking the 'X' button at the top right of each filter pane then click 'Apply'.

5.5.12. Secure Shopping Activity Logs

The 'Secure Shopping' feature creates a highly secure environment for sensitive online activities such as internet banking and shopping. See **'Comodo Secure Shopping'** for more details. CIS keeps a record of 'Secure Shopping' activities such as name of the website visited and whether secure shopping or a secure browser was used.

To view 'Secure Shopping' Logs

- Open the 'Log Viewer' module by clicking 'Tasks' > 'Advanced Tasks' > 'View Logs'
- Select 'Secure Shopping' from the 'Show' drop-down



Date & Time	Website	Action	Alert
12/20/2016 9:1...	http://www.pachaiyappas.in	Ask	Related alert
12/20/2016 9:1...	http://www.pachaiyappas.in	Ask	
12/20/2016 8:2...	https://www.sc.com	Ask	Related alert
12/20/2016 8:2...	https://www.sc.com/en/_themes/default/js/coo...	Ask	
12/20/2016 8:2...	https://www.sc.com	Ask	
12/20/2016 8:2...	https://www.sc.com/en/index.html	Ask	
12/20/2016 8:2...	https://www.sc.com/en/	Ask	
12/20/2016 7:5...	http://www.ebay.in	Ask	Related alert
12/20/2016 7:5...	http://www.ebay.in	Ask	

Column Descriptions

1. **Date & Time -** Indicates the precise date and time of the event.
2. **Website -** Shows the URL of the webpage visited.
3. **Action -** Indicates whether an alert is displayed on the connection attempt.

- To export the 'Secure Shopping' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open log file' button.
- To refresh the 'Secure Shopping' logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.

- To clear the logs click the 'Cleanup log file' button.
- You can sort the entries by ascending \ descending order by clicking on the respective column headers.

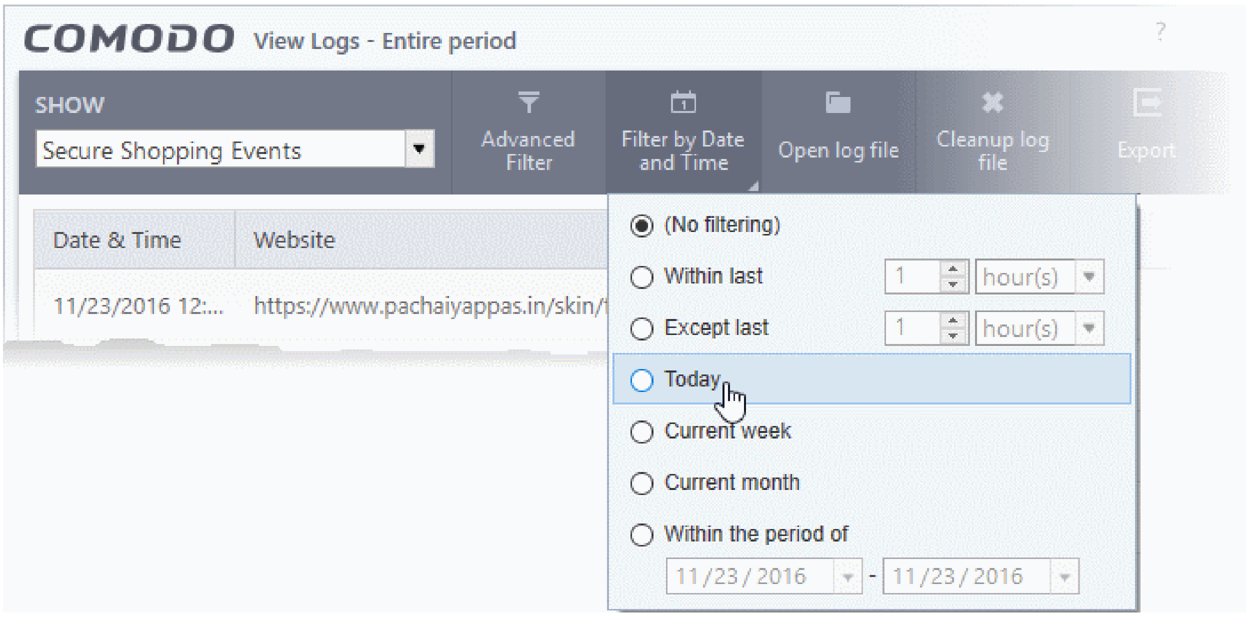
5.5.12.1. Filtering Secure Shopping Activities Logs

Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

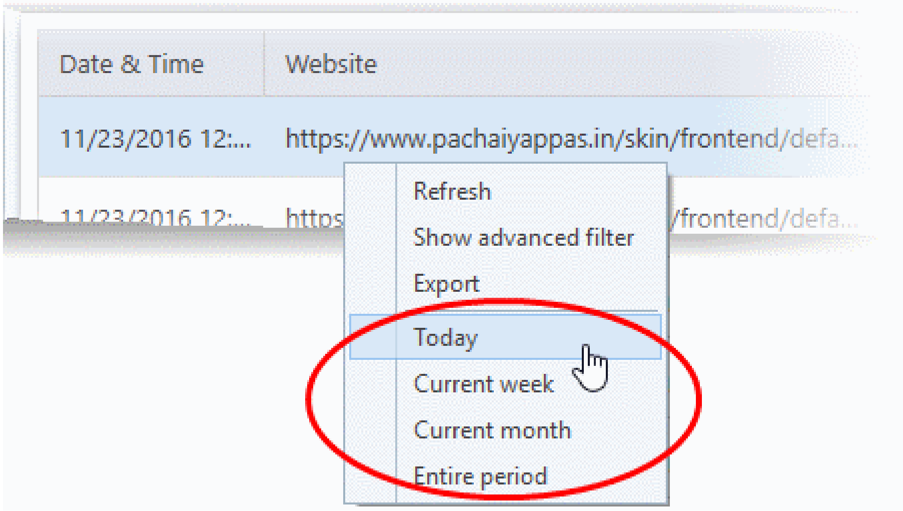
Preset Time Filters

- Click the 'Filter by Date and Time' button at the top to filter the logs for a selected time period:



- **No filtering** - Displays every event logged since Comodo Internet Security was installed. If you have cleared the log history since installation, this option shows all logs created since that clearance.
- **Within last** - Shows all logs from a certain point in the past until the present time.
- **Except last** - Excludes all logs from a certain point in the past until the present time.
- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. The current week is calculated from the Sunday to Saturday that holds the current date.
- **Current Month** - Displays all events logged during this month.
- **Custom Filter** - Enables you to select a custom period by specifying 'From' and 'To' dates.

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

You can further refine log results by using the following filters:

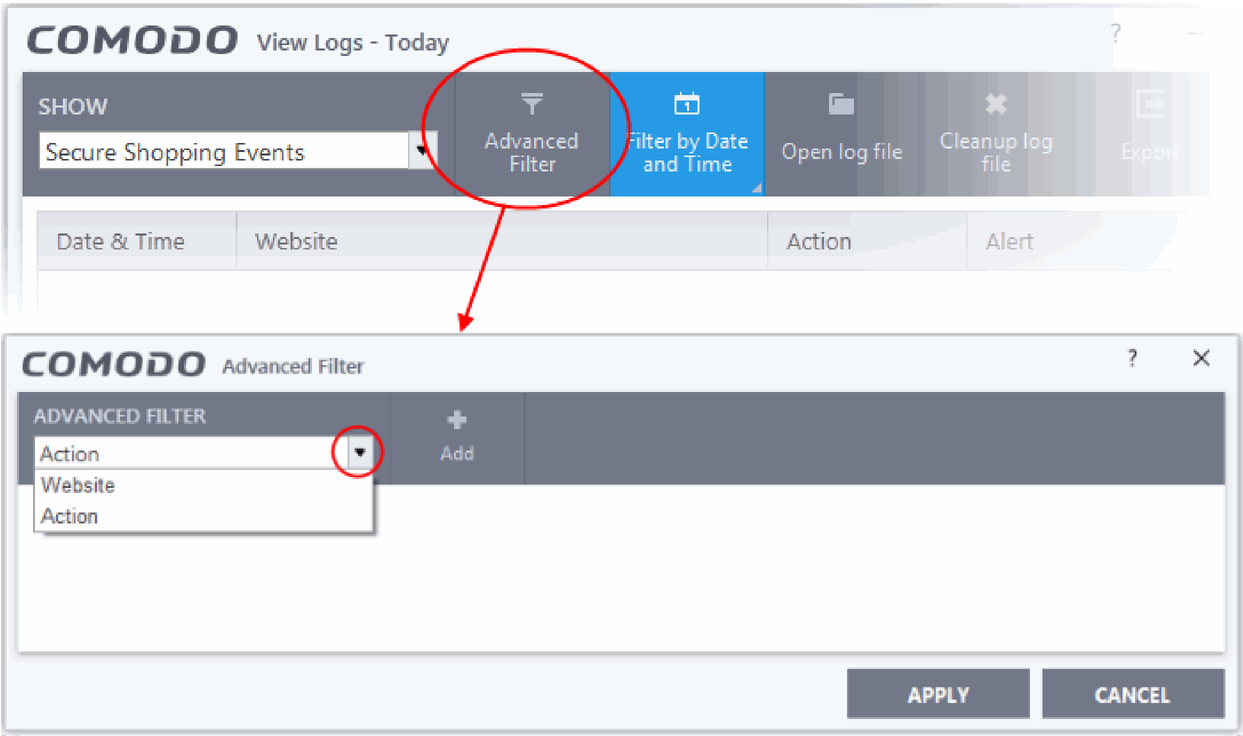
- **Website** - Filters logs based on website name
- **Action** - Displays only logs that contain a selected action(s). These include whether the user was shown an alert so they could choose what to do, or if the website was opened automatically as per the configured settings.

To configure Filters for 'Secure Shopping' Logs

1. Click the 'Advanced Filter' button on the title bar (or right-click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu).

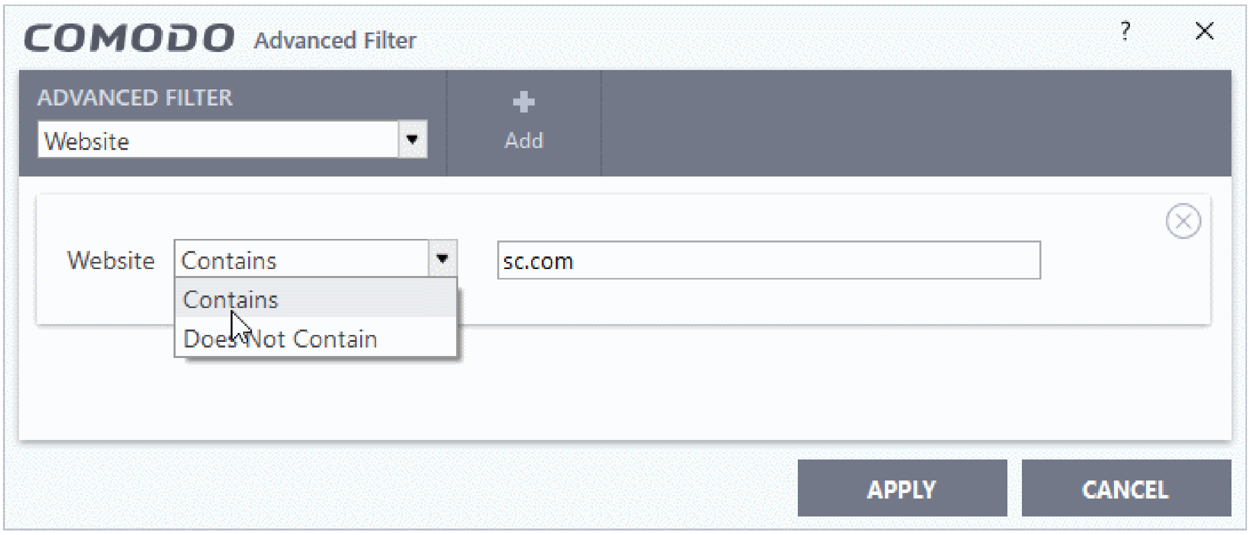
The 'Advanced Filter' interface for 'Secure Shopping' logs will open.

2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.



There are 2 categories of filters that you can add. Each of these categories can be further refined by selecting certain parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

i. **Website**: The 'Website' option allows you to filter the log entries based on the names of websites visited. Selecting the 'Websites' option displays a drop-down and a text entry field.

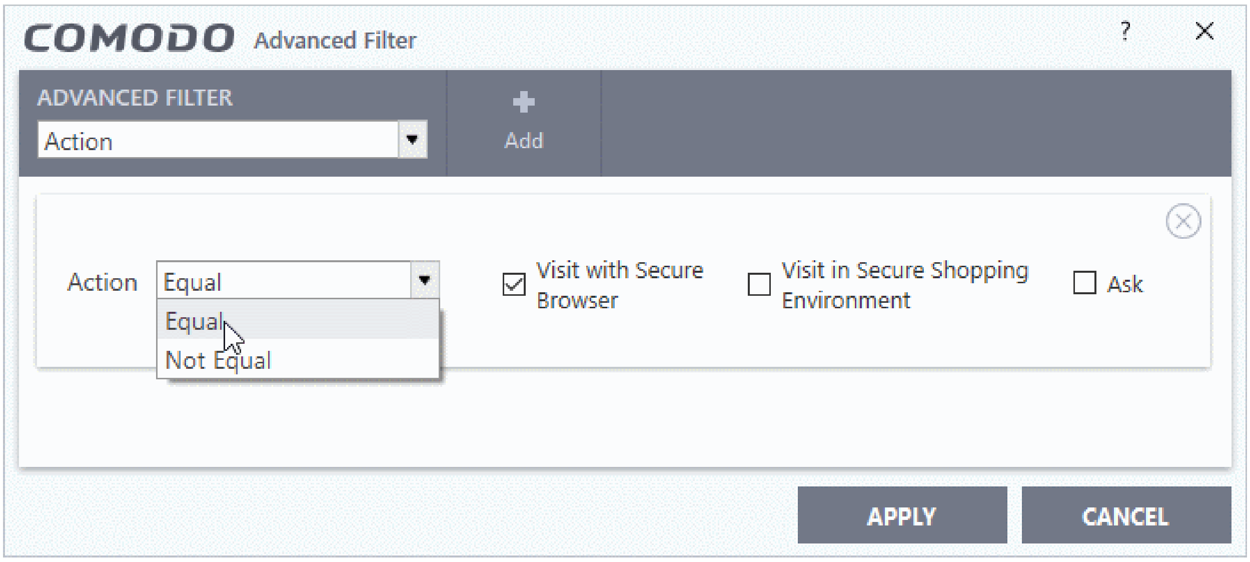


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu. 'Does Not Contain' inverts your selected choice.

b) Enter the name of the website, in part or full as search criteria in the text box.

For example, if you choose 'Contains' and enter the phrase 'sc.com' in the text field, then only logs containing 'sc.com' in the 'Website' column will be displayed.

ii. **Action**: The 'Action' option lets you filter logs based on how the configured websites were opened. Selecting the 'Action' option displays a drop down and actions to select from, as filter criteria.



a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

b) Now select the action as filter parameters to refine your search.

For example, if you chose 'Equal' and select the 'Ask' checkbox, then only logs for sites that were opened after the user made a choice at a secure shopping alert will be shown.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Configuration Changes log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- To clear filters, open the 'Advanced Filter' pane and remove each filter by clicking the 'X' button at the top right of each filter pane then click 'Apply'.

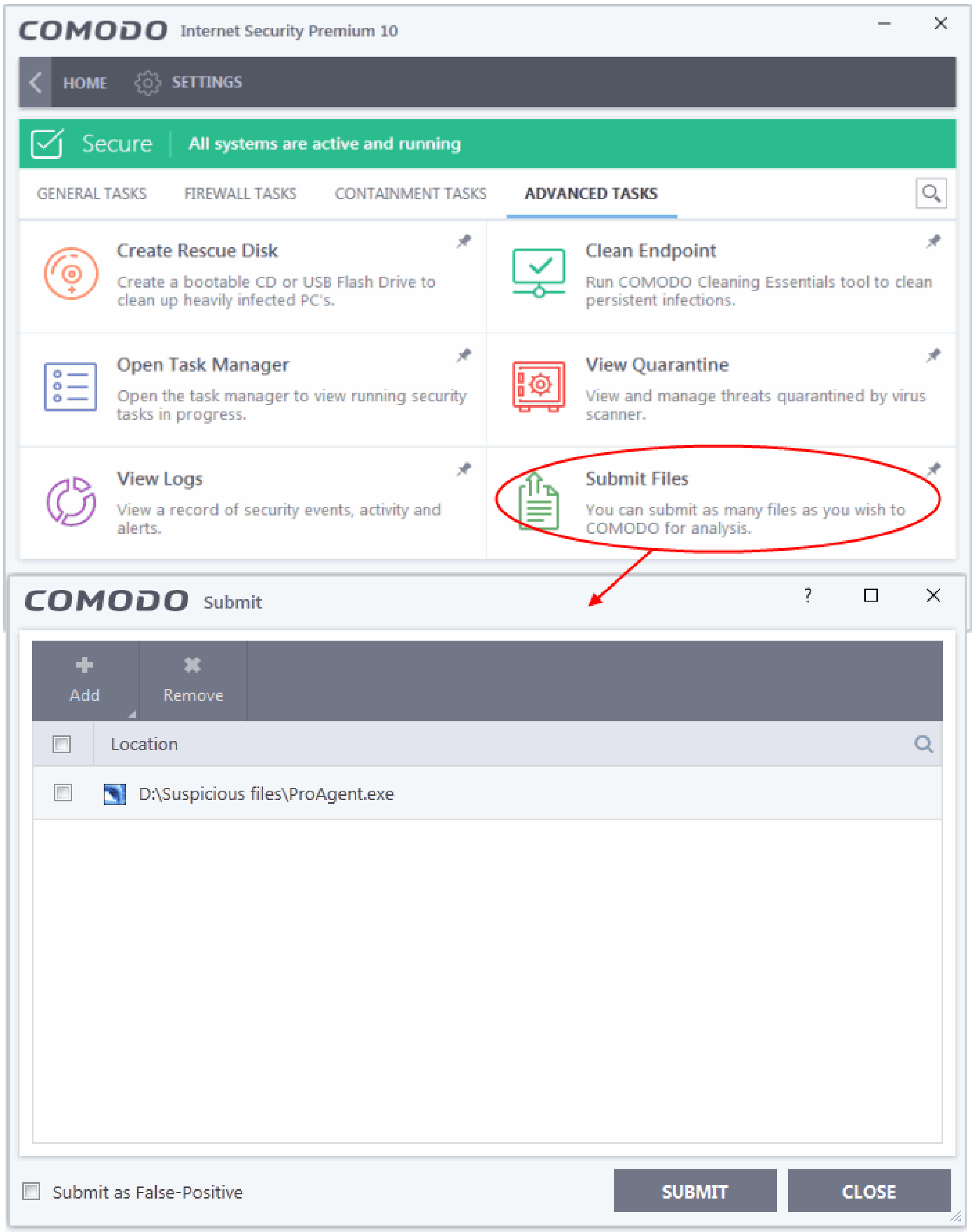
5.6. Submit Files for Analysis to Comodo

- As the name suggests, the 'Submit Files' interface allows you to files to Comodo for analysis.
- Files which CIS classifies as 'Unknown' or 'Unrecognized' are not in the Comodo safe list but have also not been identified as malware. By sending these files to Comodo, you allow our team to analyze them and classify them as either 'Safe' or 'Malicious'.
- You can also submit files you suspect of being 'false positives' (those files that you feel CIS has incorrectly identified as malware). After analysis and classification they will be added to the white or black list accordingly.

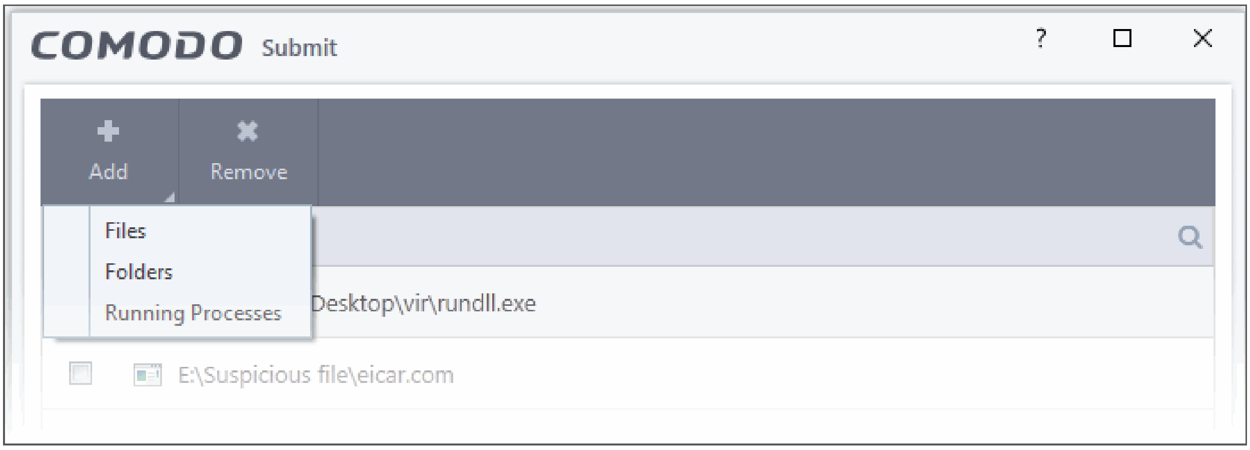
Note: Unrecognized files can also be submitted from the '**File List**' interface should you prefer.

To add new file(s) to 'Submit Files' list

- Click 'Tasks' at the top left of the home screen
- Open the 'Advanced Tasks' tab and choose 'Submit Files'


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Open Task Manager
Open the task manager to view running security tasks in progress.
View Quarantine
View and manage threats quarantined by virus scanner.
View Logs
View a record of security events, activity and alerts.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
COMODO Submit
Add
Remove
Location
D:\Suspicious files\ProAgent.exe
Submit as False-Positive
SUBMIT
CLOSE

- Click 'Add' at top right. You can add files to the 'Submit Files' list in three ways:



- **Files** - Navigate the file or executable of the program you wish to add.
- **Folders** - Navigate the folder you wish to add. All the files in the folder will be added to the 'Trusted Files' list.
- **Running Processes** - Select a process to be run. On selecting a process, the parent application, which invoked the process will be added to the 'Trusted Files' list.

- Repeat the process to add more files and to submit them at-once.

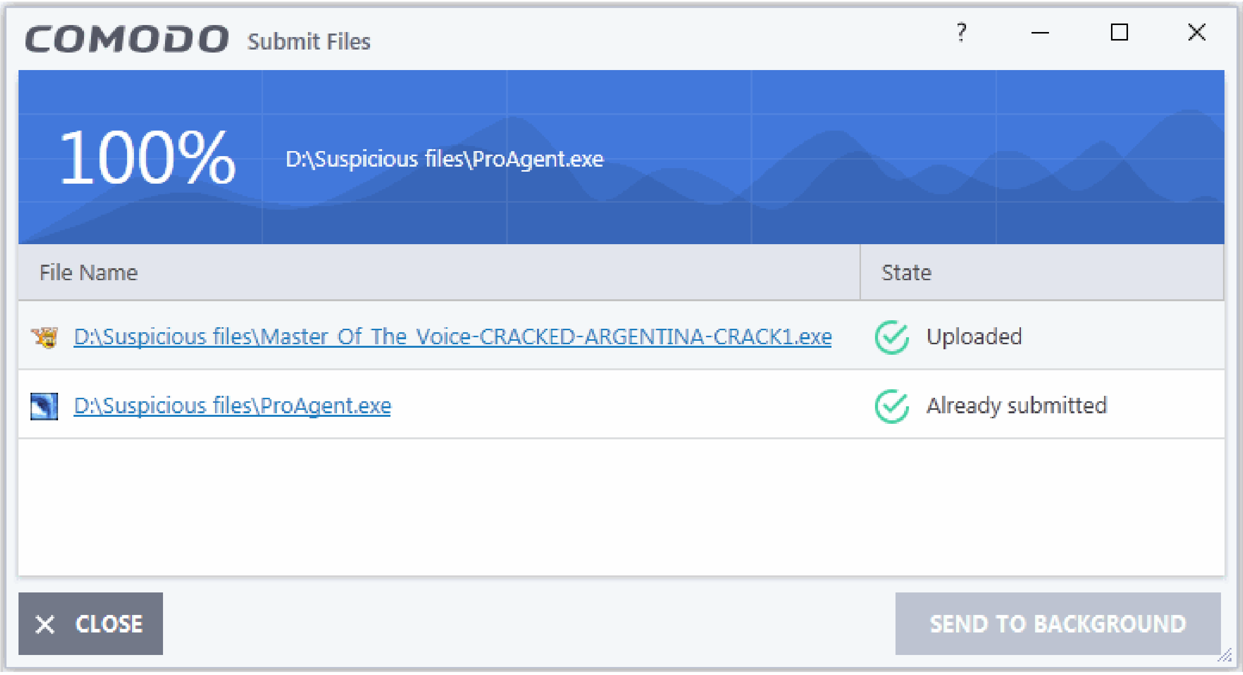
To remove the files from 'Submit Files' list

- Select the file from the list and click 'Remove'

After adding the files you want to submit, click the 'Submit' button. If you want to submit the files as 'False Positives' to Comodo, select the 'Submit as False-Positive check' box. The files will be submitted and the progress will be displayed.

You can stop, pause/resume or send the submission process to background by clicking respective buttons.

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen displays these results on completion.



File Name	State
D:\Suspicious files\Master_Of_The_Voice-CRACKED-ARGENTINA-CRACK1.exe	✓ Uploaded
D:\Suspicious files\ProAgent.exe	✓ Already submitted

- Uploaded - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- Already submitted - The file has *already* been submitted to our labs by another CIS user and was not uploaded from your machine at this time.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

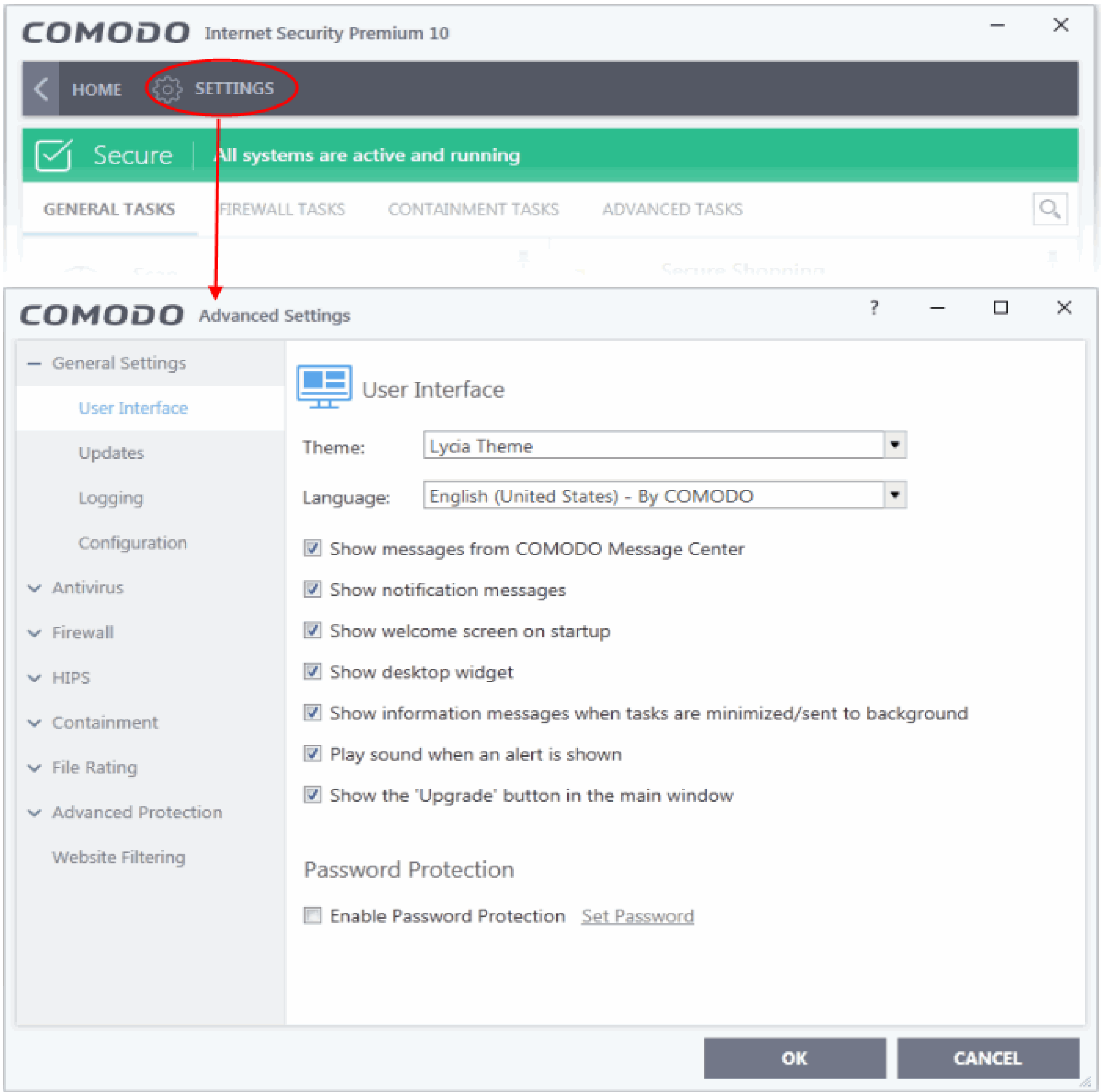
The list of files submitted from your computer can be viewed from the **Submitted Files** interface.

6.CIS Settings

- You can configure every aspect of the operation, behavior and appearance of Comodo Internet Security through the 'Advanced Settings' interface.
- The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and

event logging.

- The 'Security Settings' section lets advanced users delve into the configuration of each CIS security module.
  - For example, the 'Security Settings' area allows you to create custom virus scan schedules, create virus exclusions, create Firewall and HIPS rules, modify containment behavior, define network zones and specify how the file rating system deals with trusted and untrusted files.
- To open 'Advanced Settings', click the 'Settings' link at the top of the home screen.



User Interface

Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show welcome screen on startup

☑ Show desktop widget

☑ Show information messages when tasks are minimized/sent to background

☑ Play sound when an alert is shown

☑ Show the 'Upgrade' button in the main window

Password Protection

☐ Enable Password Protection Set Password

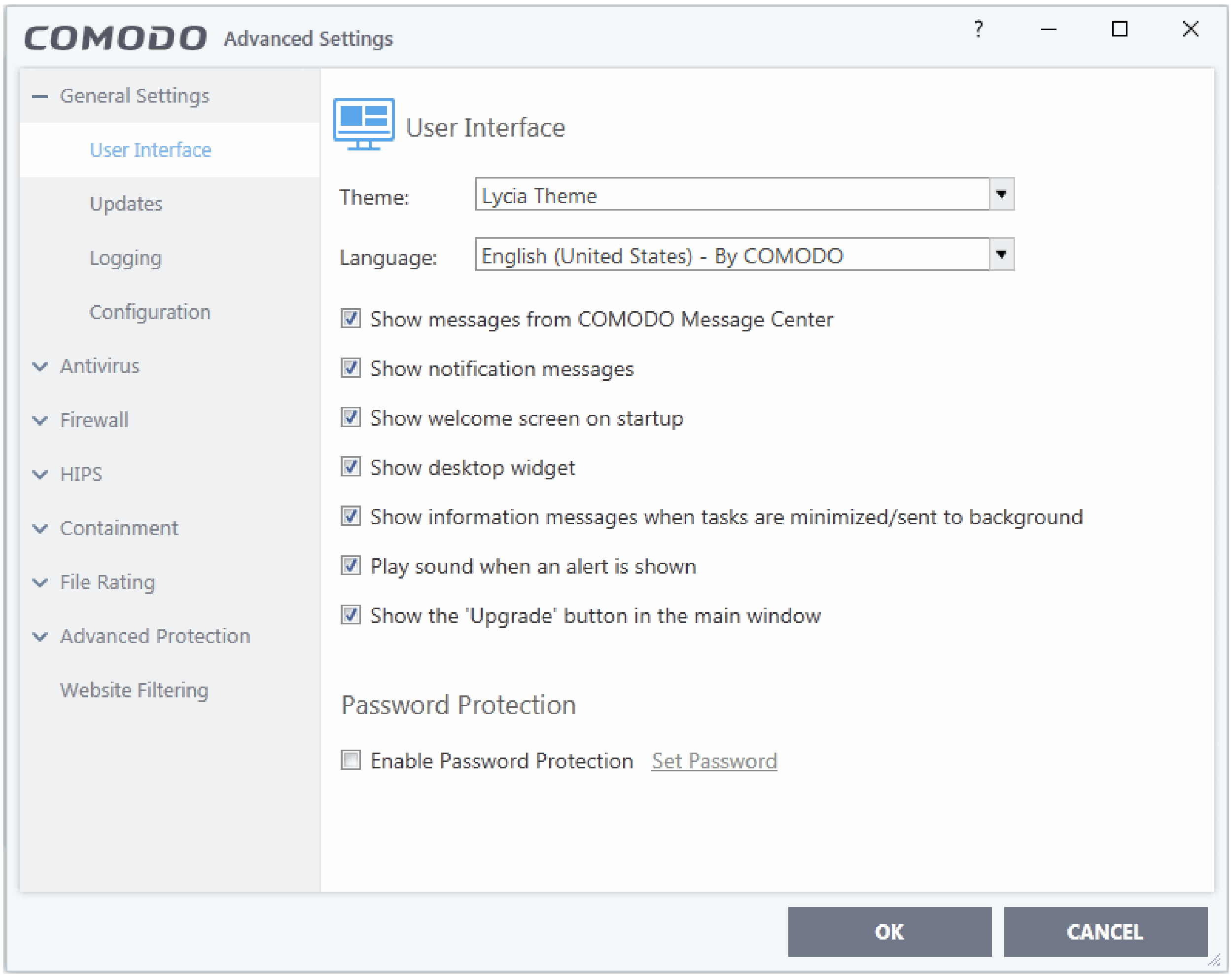
The left hand menu lets you access the following areas:

- **General Settings** - Allows you to configure the appearance and behavior of the application
  - **Customize User Interface**
  - **Configure Program and database Updates**
  - **Log Settings**
  - **Manage CIS Configurations**
- **Antivirus Settings**
  - **Real-time Scanner Settings**
  - **Scan Profiles**

6.1. General Settings

The 'General Settings' area enables you to customize the appearance and overall behavior of Comodo Internet Security. You can configure interface language, notification messages, automatic updates, logging and more.

- Click 'Settings' on the CIS home screen to open the 'Advanced Settings' interface.
- Click 'General Settings' on the left:



User Interface

Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show welcome screen on startup

☑ Show desktop widget

☑ Show information messages when tasks are minimized/sent to background

☑ Play sound when an alert is shown

☑ Show the 'Upgrade' button in the main window

Password Protection

□ Enable Password Protection Set Password

General Settings is broken down into the following areas:

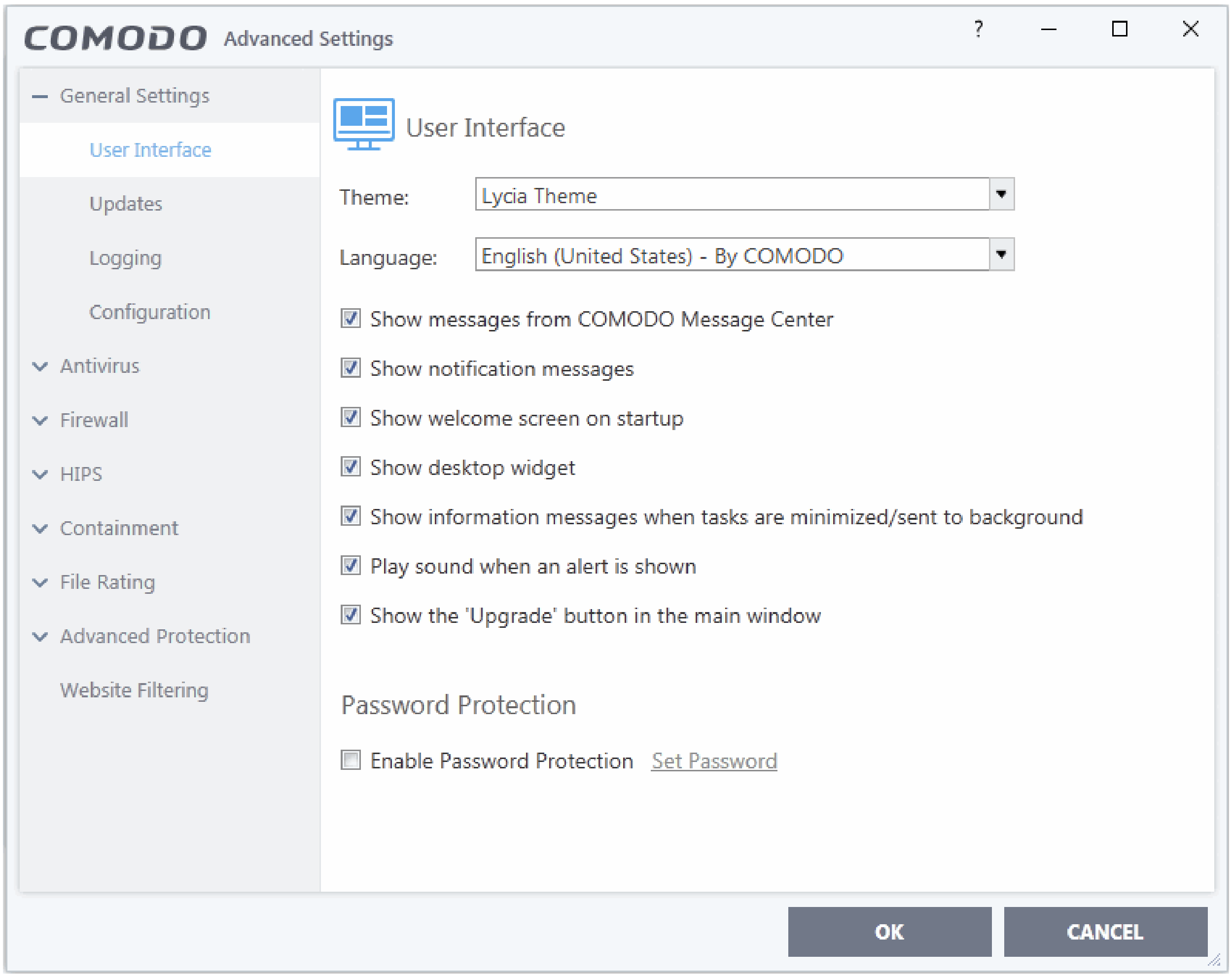
- **User Interface**
- **Updates**
- **Logging**
- **Configuration**

6.1.1. Customize User Interface

The 'User Interface' tab lets you choose your preferred language and customize the look and feel of the application. You can also configure how messages are displayed and enable password protection for your settings.

To open the user interface screen:

- Click 'Settings' on the CIS home screen to open the 'Advanced Settings' interface.
- Click 'General Settings' > 'User Interface' on the left:



User Interface

Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show welcome screen on startup

☑ Show desktop widget

☑ Show information messages when tasks are minimized/sent to background

☑ Play sound when an alert is shown

☑ Show the 'Upgrade' button in the main window

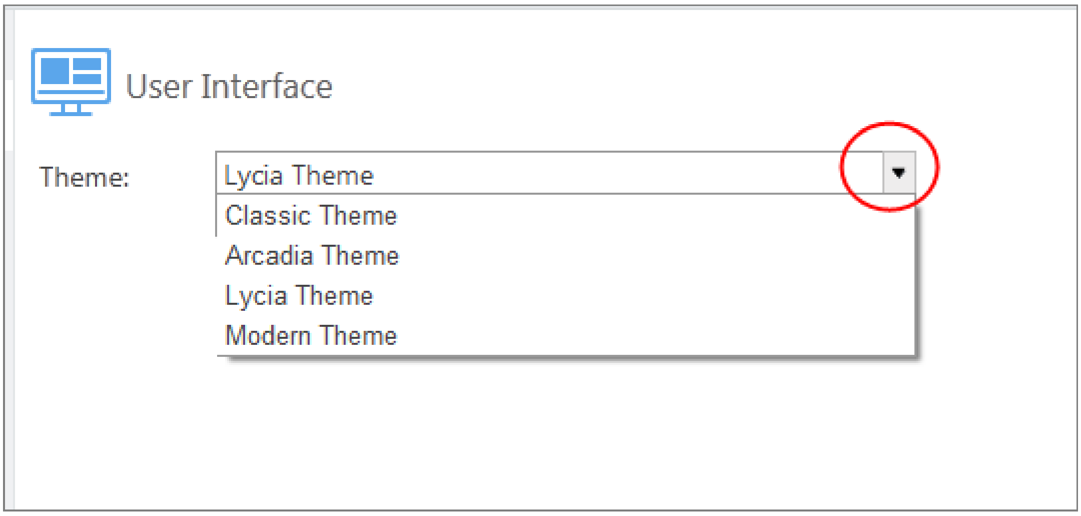
Password Protection

☐ Enable Password Protection Set Password

The 'User Interface' area allows you configure the following:

- **Themes**
- **Language**
- **Show messages from COMODO Message Center**
- **Show notification messages**
- **Show Welcome screen on start up**
- **Show desktop widget**
- **Show information messages when tasks are minimized/sent to background**
- **Play sound when an alert is shown**
- **Show upgrade button in the main window** *(Available only in free version)*
- **Enable Password Protection**

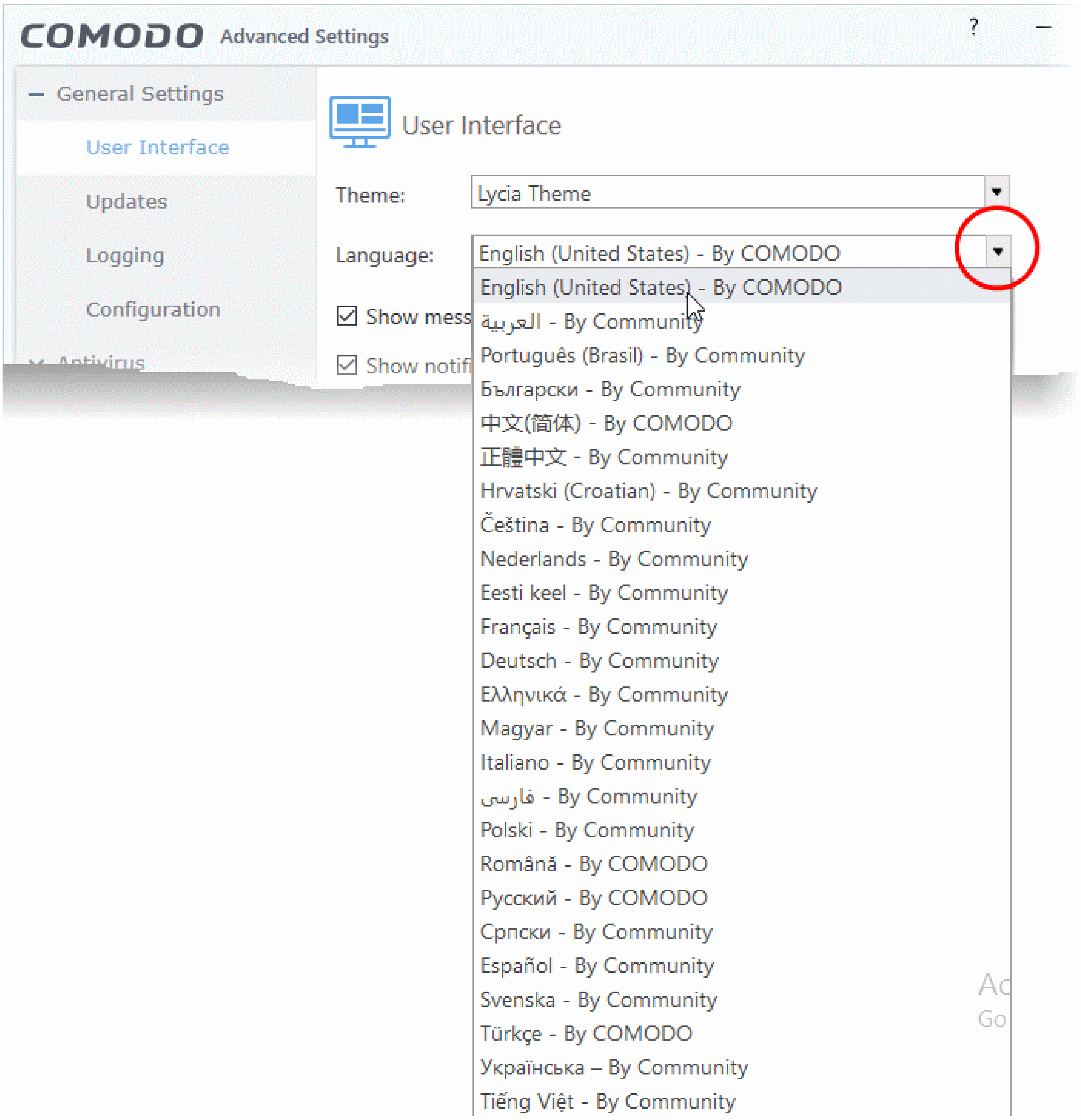
- **Theme -** The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (***Default = Lycia Theme***).



User Interface

Theme: Lycia Theme

- **Language Settings -** Comodo Internet Security is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (***Default = English (United States)***).



User Interface

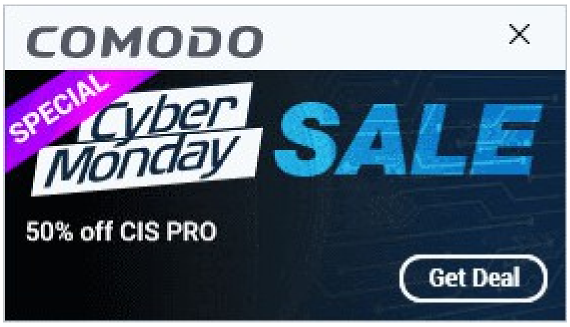
Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show mess

☑ Show notifi

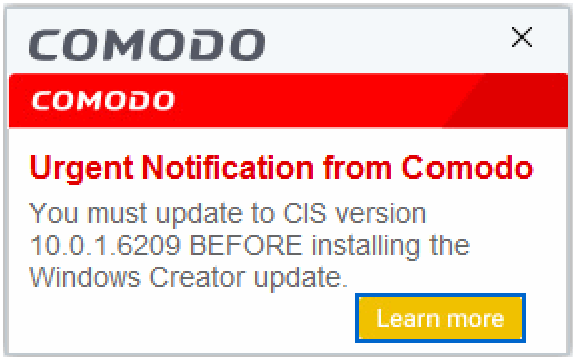
- **Show messages from COMODO Message Center -** If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world. (***Default = Enabled***).



They contain news about product updates, occasional requests for feedback and info about other Comodo products you may want to try. (***Default = Enabled***).

- **Show notification messages -** These are the CIS system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CIS is taking and any

CIS status updates. For example ' Comodo Firewall is learning ' or 'HIPS' is learning ' are generated when these modules are learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in **Antivirus > Real-time Scan settings** screen. Clear this check box if you do not want to see these system messages (***Default = Enabled***).



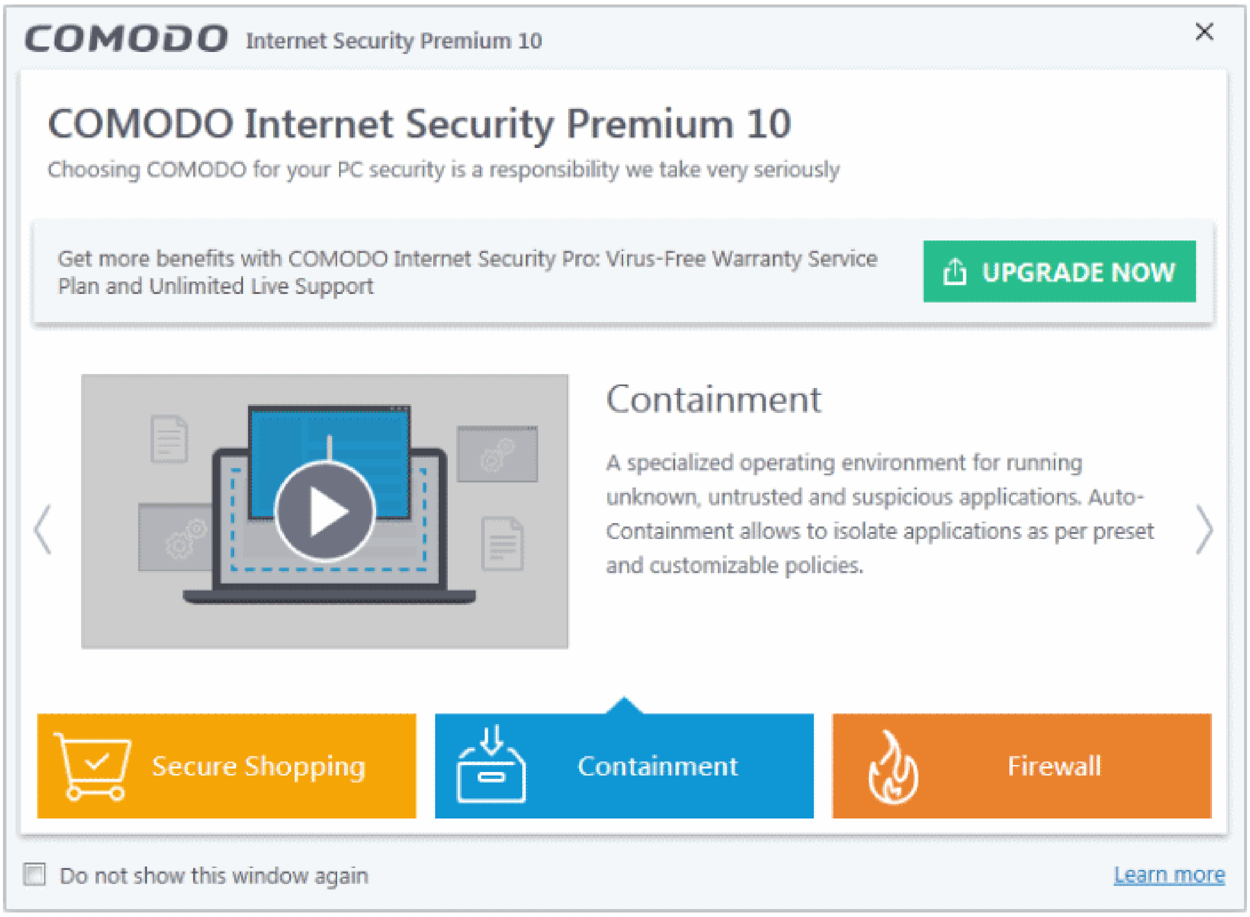
COMODO

COMODO

Urgent Notification from Comodo

You must update to CIS version 10.0.1.6209 BEFORE installing the Windows Creator update.

- **Show welcome screen on start up -** If enabled, CIS will display a welcome screen when the application first starts. ***(Default = Enabled)**:*



COMODO Internet Security Premium 10

COMODO Internet Security Premium 10

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

Get more benefits with COMODO Internet Security Pro: Virus-Free Warranty Service Plan and Unlimited Live Support

Containment

A specialized operating environment for running unknown, untrusted and suspicious applications. Auto-Containment allows to isolate applications as per preset and customizable policies.

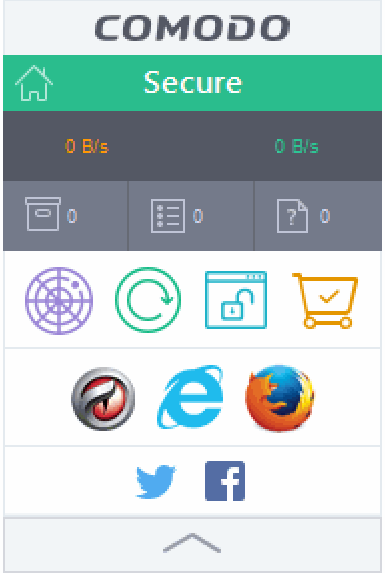
□ Do not show this window again

Tip: You can disable the Welcome Screen by selecting the checkbox 'Do not show this window again' in the window itself.

- **Show desktop widget -** The CIS desktop widget displays information about security status, outgoing and incoming traffic, background tasks.
  - The widget also acts as a shortcut to open the CIS interface, the task manager, your browsers and

social network sites.

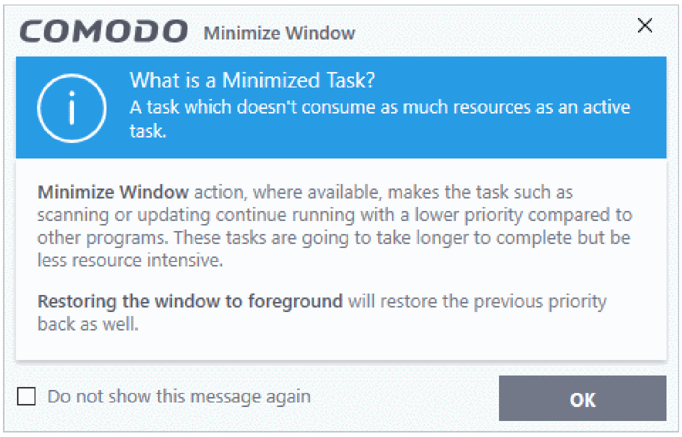
- Clear this checkbox if you do not want the widget to be displayed on your desktop. ***(Default = Enabled).***



See **The Widget**, for more details on the Widget.

Tip: You can also enable or disable the widget from the CIS system tray icon. Right click on the CIS system tray icon and deselect the 'Show' option that appears on hovering your mouse cursor over 'Widget'.

- **Show information messages when tasks are minimized/sent to background** - CIS displays messages explaining the effects of minimizing or moving a running CIS task to the background:



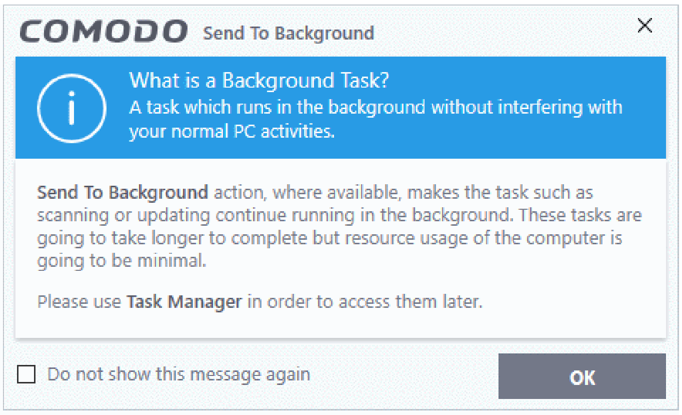
COMODO Minimize Window

What is a Minimized Task?
A task which doesn't consume as much resources as an active task.

Minimize Window action, where available, makes the task such as scanning or updating continue running with a lower priority compared to other programs. These tasks are going to take longer to complete but be less resource intensive.

Restoring the window to foreground will restore the previous priority back as well.

□ Do not show this message again



COMODO Send To Background

What is a Background Task?
A task which runs in the background without interfering with your normal PC activities.

Send To Background action, where available, makes the task such as scanning or updating continue running in the background. These tasks are going to take longer to complete but resource usage of the computer is going to be minimal.

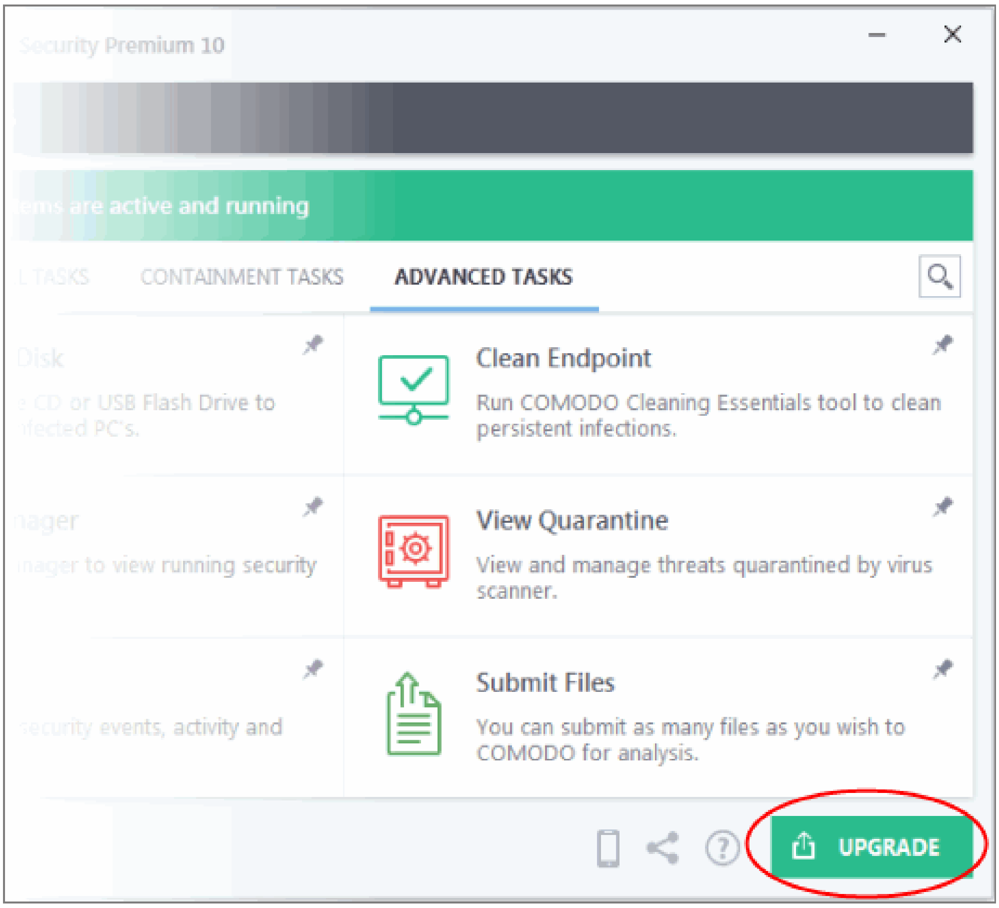
Please use **Task Manager** in order to access them later.

□ Do not show this message again

If you do not want these messages to be displayed, clear this check-box (***Default = Enabled***).

Tip: You can also disable these messages from the message window itself, by selecting 'Do not show this message again'

- **Play sound when an alert is shown -** CIS 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).***
- **Show 'Upgrade' button in the main window - ** This option is available only in the Comodo Internet Security Premium version. If enabled, CIS will display the green upgrade button at the bottom right of the interface. Clicking the button will take you to the product upgrade page enabling you to upgrade to Pro or Complete versions. ***(Default = Enabled)***.


Security Premium 10
ems are active and running
L TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Disk
a CD or USB Flash Drive to
nfected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
nager
nager to view running security
View Quarantine
View and manage threats quarantined by virus scanner.
security events, activity and
Submit Files
You can submit as many files as you wish to COMODO for analysis.
UPGRADE

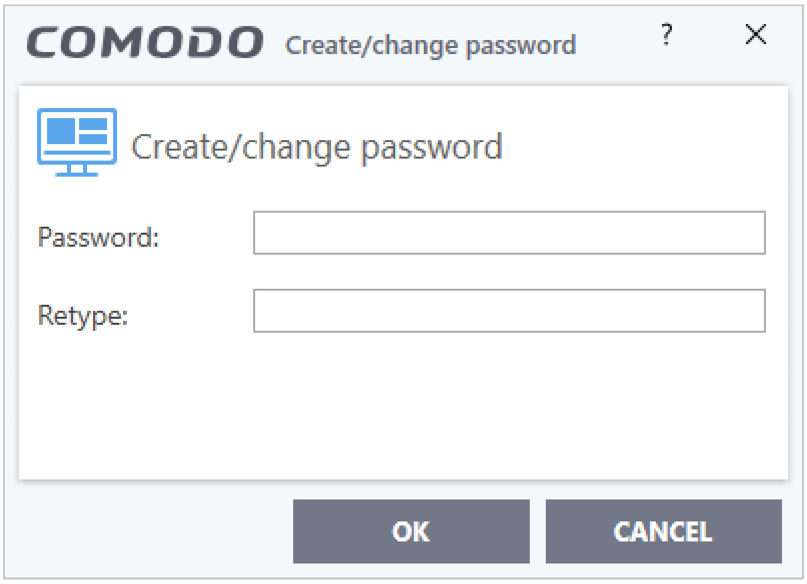
- Deselect this option if you do not want to see the Upgrade button on the main interface.

- **Enable Password Protection** - Enforces password protection for all important configuration sections and wizards within the interface. If you enable this feature, you must first specify and confirm a password by clicking the 'Set Password' link. You will then be asked for this password whenever you try to access important configuration areas. For example, all sections in the **General Tasks**, **Firewall Tasks**, **Containment Tasks** and **Advanced Tasks** will request the password.

  This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and exposing the machine to threats (***Default = Disabled***).

  To enable password protection

  - Select the 'Enable Password Protection' check-box then click 'Set Password'. The Create/change password' dialog will appear:



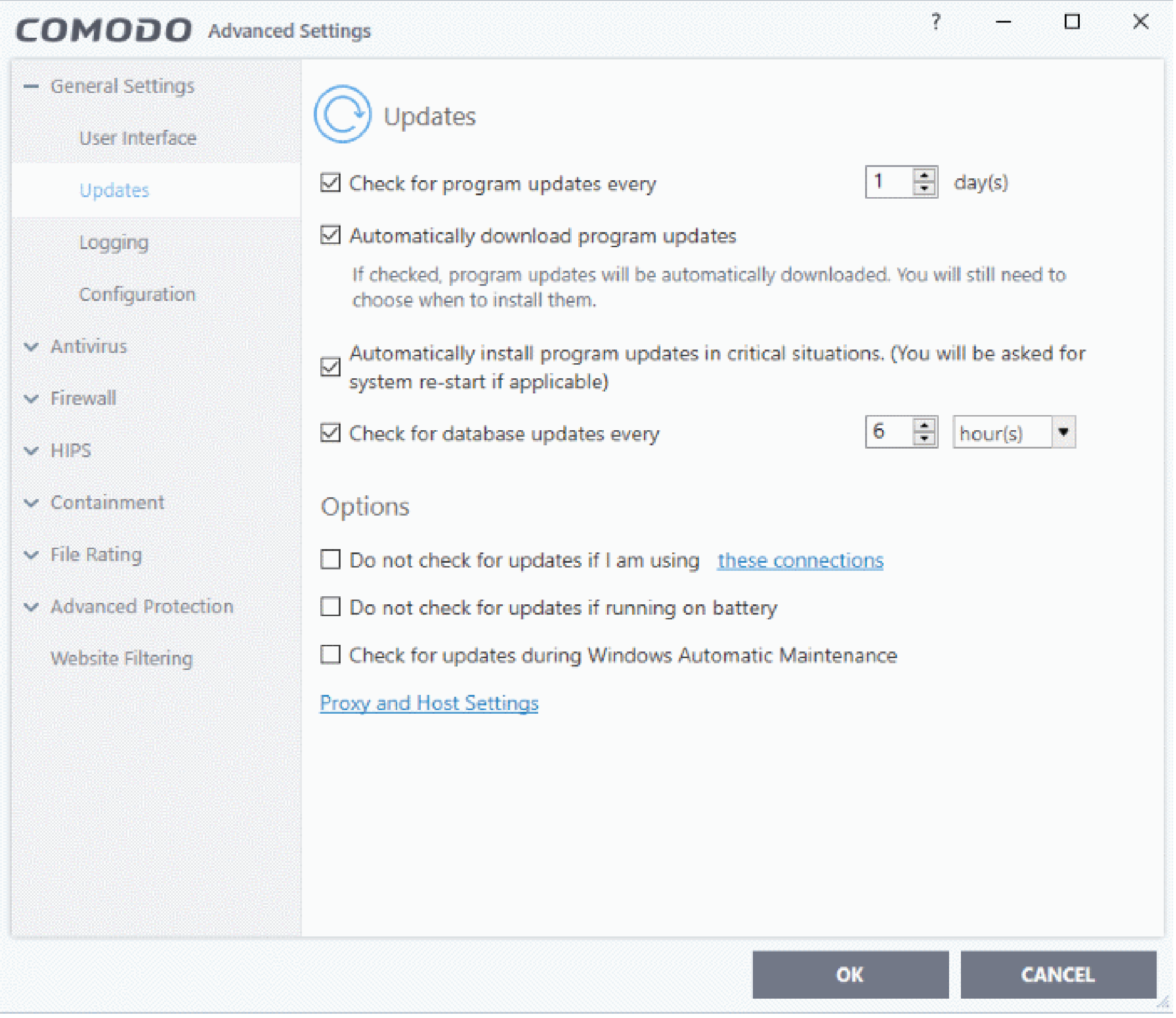
- Enter and confirm your password then click 'OK'. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

6.1.2. Configure Program and Virus Database Updates

The 'Updates' area allows you to configure settings that govern CIS program and virus database updates.

To access update settings:

- Click 'Settings' at the top of the CIS home screen
- Click 'General Settings' > 'Updates' on the left:



☑ Check for program updates every 1 day(s)

☑ Automatically download program updates

If checked, program updates will be automatically downloaded. You will still need to choose when to install them.

☑ Automatically install program updates in critical situations. (You will be asked for system re-start if applicable)

☑ Check for database updates every 6 hour(s)

Options

□ Do not check for updates if I am using these connections

□ Do not check for updates if running on battery

□ Check for updates during Windows Automatic Maintenance

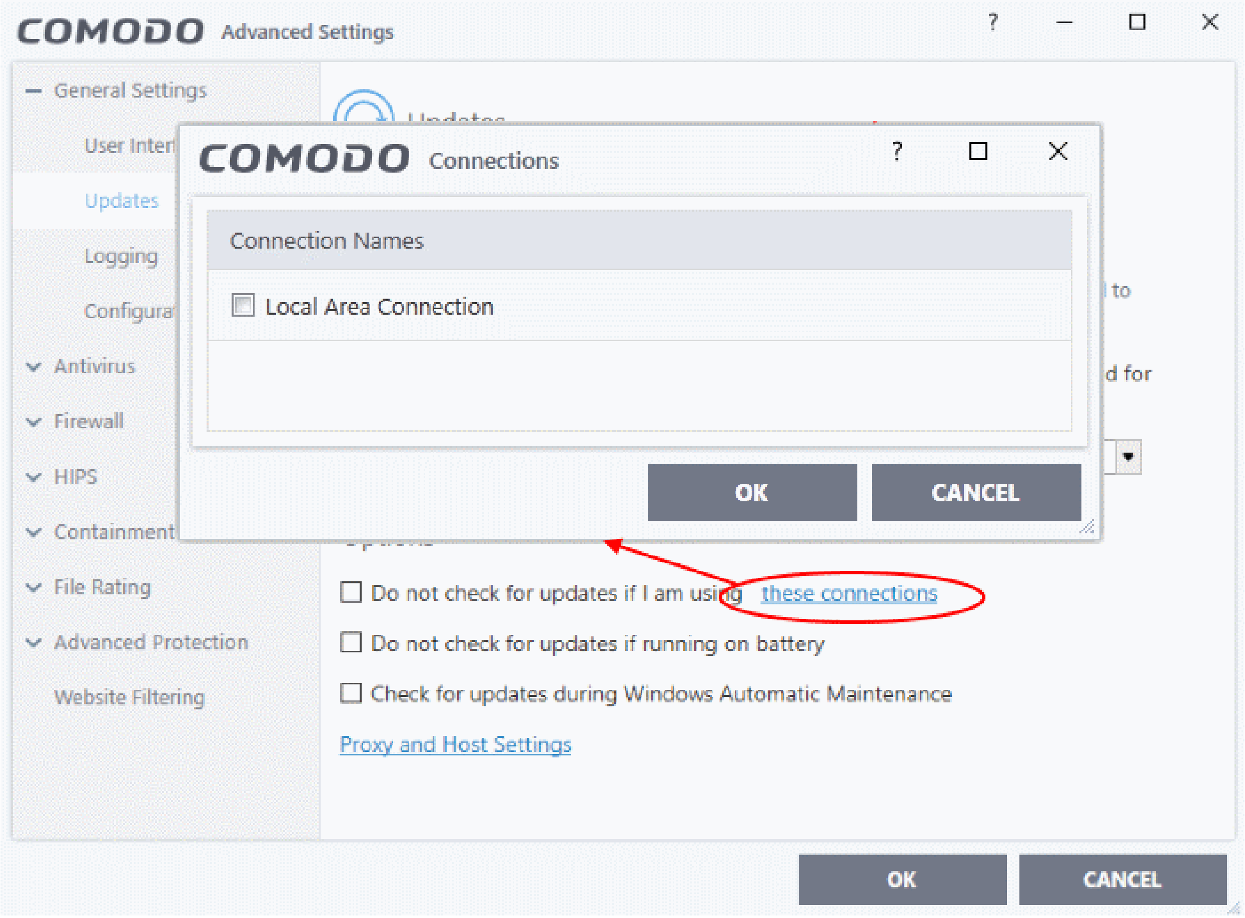
Proxy and Host Settings

The updates area allows you configure the following:

- **Check for program updates every NN day(s)** - Set the interval at which CIS should check for program updates. Select the interval in days from the drop-down menu. ***(Default = 1 day)***
- **Automatically download program updates** - Instructs CIS to automatically download virus database updates as soon as they are available. You will be notified when they are ready for installation. ***(Default=Enabled)***
- **Automatically install program updates in critical situations. (You will be asked for system re-start if applicable)** - Will automatically install updates which fix very serious bugs and incompatibilities. For example, a new release of Windows may introduce a critical incompatibility with Comodo Internet Security which needs to be addressed immediately. We strongly recommend you leave this setting enabled, even if you disable automatic download of updates. ***(Default = Enabled)***
- **Check for database updates every NN hour(s)/day(s)** - Lets you set the interval at which CIS should check for virus database updates. ***(Default and recommended = 6 hours)***
- **Do not check updates if am using these connections** - Allows you to stop CIS checking for updates if you are using specific internet connections. For example, you may not wish to check updates if using a wireless connection you know is slow or not secure. ***(Default = Disabled)***

  To do this:

  - Select the 'Do not check updates if am using these connections' check-box
  - Then click the 'these connections'. The connections dialog will appear with the list of connections you use.

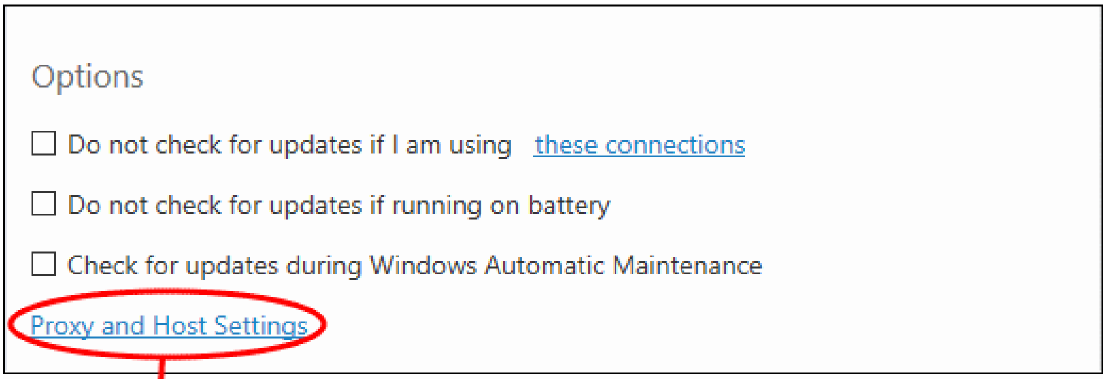


  - Select the connection through which you do not want CIS to check for updates and click 'OK'.
- **Do not check for updates if running on battery** - If enabled, CIS will not download updates if it detects your computer is running on battery power. This is intended to extend battery lifetime on laptops. ***(Default = Disabled)***
- **Check for updates during Windows Automatic Maintenance** - If enabled, CIS will check for and download updates when Windows is updating itself.
- **Proxy and Host Settings** - Allows you to select the host from which updates are downloaded. By default, CIS will download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CIS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CIS at this proxy/staging server. This helps to conserve bandwidth and accelerate the update process when a large number of endpoints are involved.

Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from **http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php**

To configure updates via proxy server

  - Click 'Proxy and Host Settings' at the bottom of the 'Updates' interface. The 'Proxy and Host Settings' dialog will open.



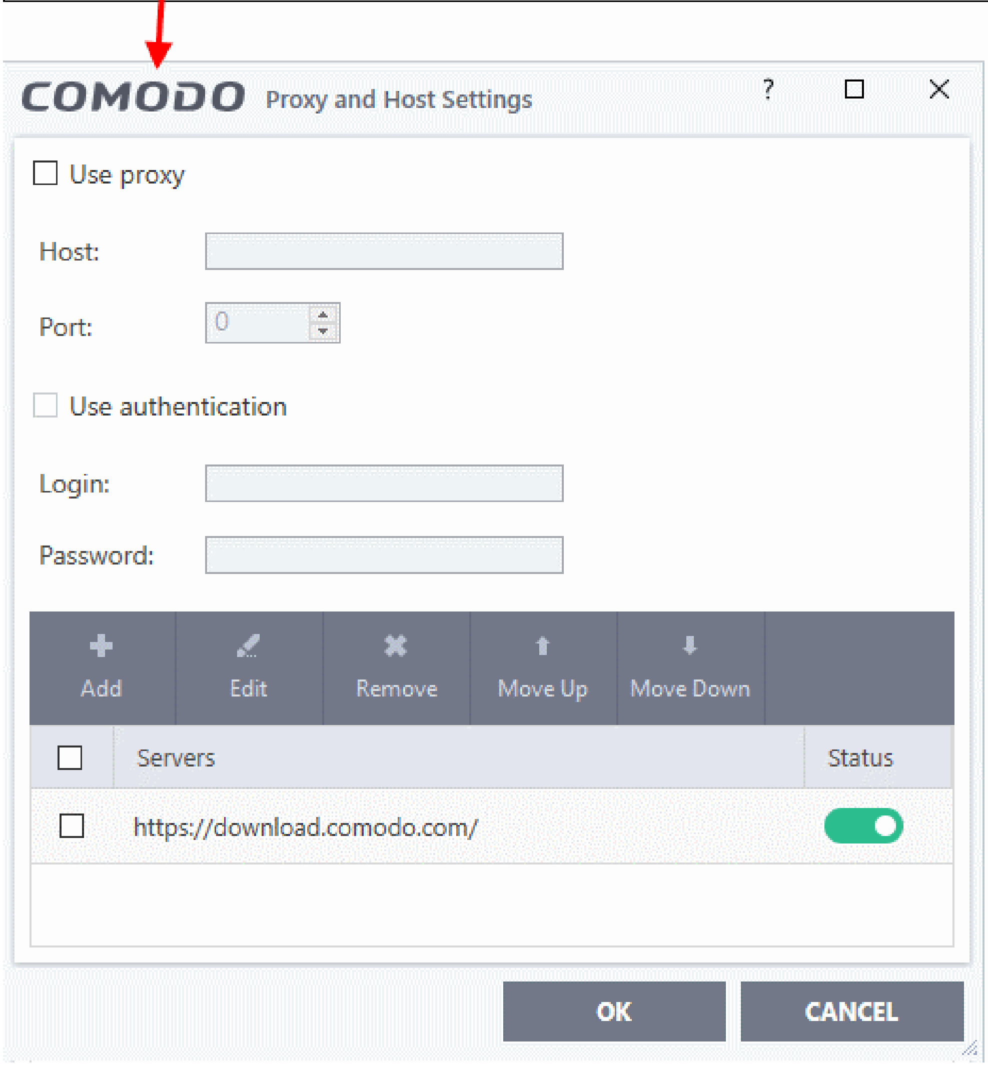
Options

□ Do not check for updates if I am using these connections

□ Do not check for updates if running on battery

□ Check for updates during Windows Automatic Maintenance

Proxy and Host Settings



COMODO Proxy and Host Settings

□ Use proxy

Host:

Port: 0

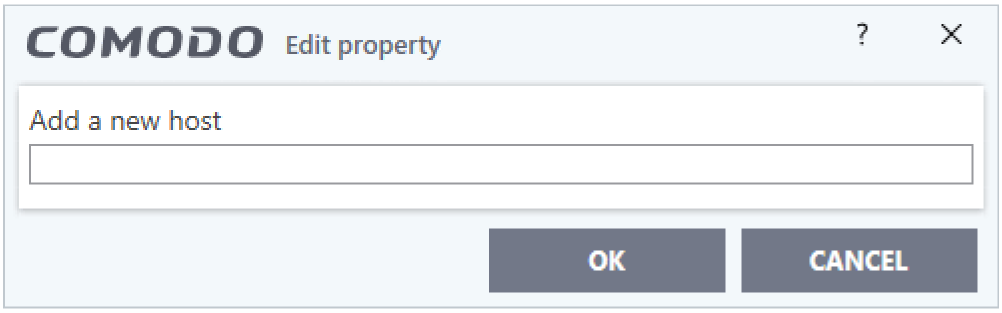
□ Use authentication

Login:

Password:

□	Servers	Status
□	https://download.comodo.com/	●

- Select the 'Use Proxy' check-box.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- You can add multiple servers from which updates are available. To do this, click the 'Add' button then enter the host name in the 'Edit Property' dialog.



- If you specify multiple servers:
  - Activate or deactivate each update server using the 'Status' switch alongside it
  - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CIS will download from the first server that contains new updates.
- Click 'OK' for your settings to take effect.

6.1.3. Log Settings

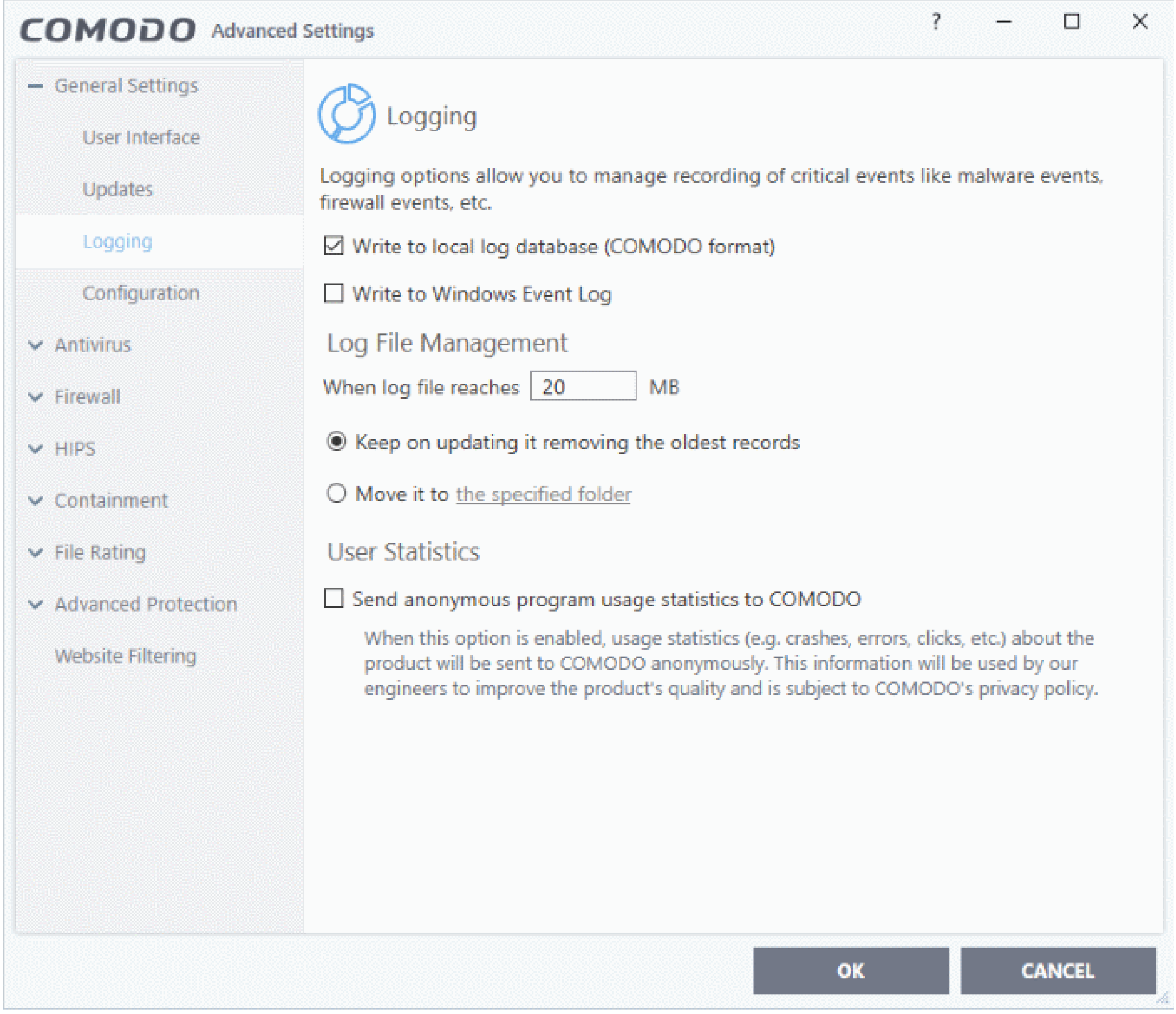
Comodo Internet Security keeps detailed records of all antivirus, firewall, HIPS, containment, website filtering, VirusScope and secure shopping events. Logs are also created for 'Alerts Displayed', 'Tasks Launched', 'File List' changes, 'Trusted Vendors' list changes and 'Configuration Changes'.

The 'Logging' interface lets you to specify the location to store logs, the maximum size of log files, and how CIS should react if the maximum file size is exceeded.

Note: If you wish to actually view, manage and export logs, then you need to open the '**View Logs**' interface under 'Advanced Tasks' interface. ('Tasks' > 'Advanced' > 'View Logs')

To access the 'Logging' settings interface

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Logging' under 'General Settings' on the left:



Logging

Logging options allow you to manage recording of critical events like malware events, firewall events, etc.

☑ Write to local log database (COMODO format)

□ Write to Windows Event Log

Log File Management

When log file reaches 20 MB

● Keep on updating it removing the oldest records

○ Move it to the specified folder

User Statistics

□ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, errors, clicks, etc.) about the product will be sent to COMODO anonymously. This information will be used by our engineers to improve the product's quality and is subject to COMODO's privacy policy.

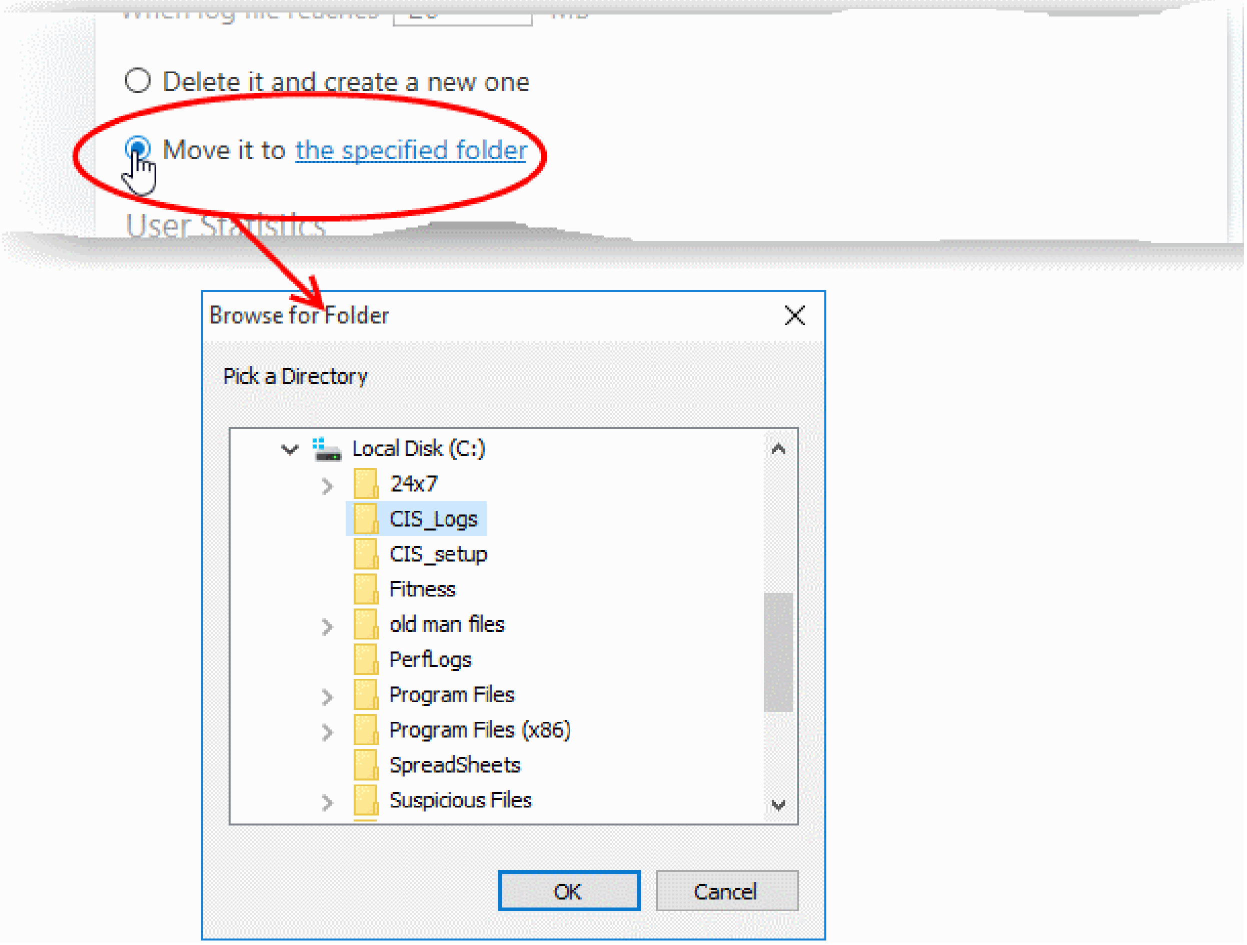
The 'Logging' Settings area allows you configure the following:

Logging Options

- **Write to local log database (COMODO format)** - CIS logs events in Comodo format and the log storage depends on settings done in Log File Management section below. ***(Default = Enabled***)
- **Write to Windows Event Logs** - CIS log events are written to Windows Event Logs. ***(Default = Disabled)***

Log File Management

- **When log file reaches -** Enables you to specify behavior when the log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.
  - Specify the maximum limit for the log file size (in MB) in the text box beside 'When the log file's size reaches' . (***Default = 20MB***)
  - Select 'Delete it and create a new one' to discard the log file if it reaches the maximum size. When the log file reaches maximum size it will be deleted and a new log file will be created. (***Default = Enabled***)
  - Select 'Move it to' and select a folder in which to save the log file when it reaches the maximum size. (***Default = Disabled***)



○ Delete it and create a new one

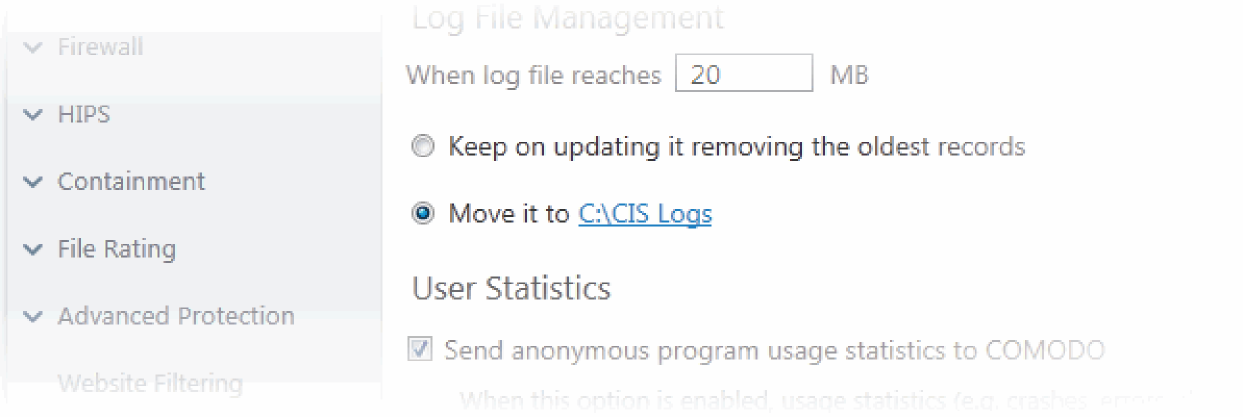
● Move it to the specified folder

User Statistics

Browse for Folder

Pick a Directory

The selected folder path will appear beside 'Move it to'.



Log File Management

When log file reaches 20 MB

○ Keep on updating it removing the oldest records

● Move it to C:\CIS Logs

User Statistics

☑ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, errors

User Statistics

- **Send anonymous program usage statistics to COMODO** - Comodo collects usage details so we can analyze how our users interact with CIS. This 'real-world' data allows us to create product improvements which reflect the needs of our users. If you enable this option, CIS will periodically send usage data to Comodo servers through a secure, encrypted channel. Your privacy is not affected because the data is anonymized. Disable this option if you don't want to send usage details to Comodo. ***(Default = Enabled)***
- Click 'OK' for your changes to take effect

6.1.4. Manage CIS Configurations

- Comodo Internet Security allows you to maintain, save and export your security settings as a profile.

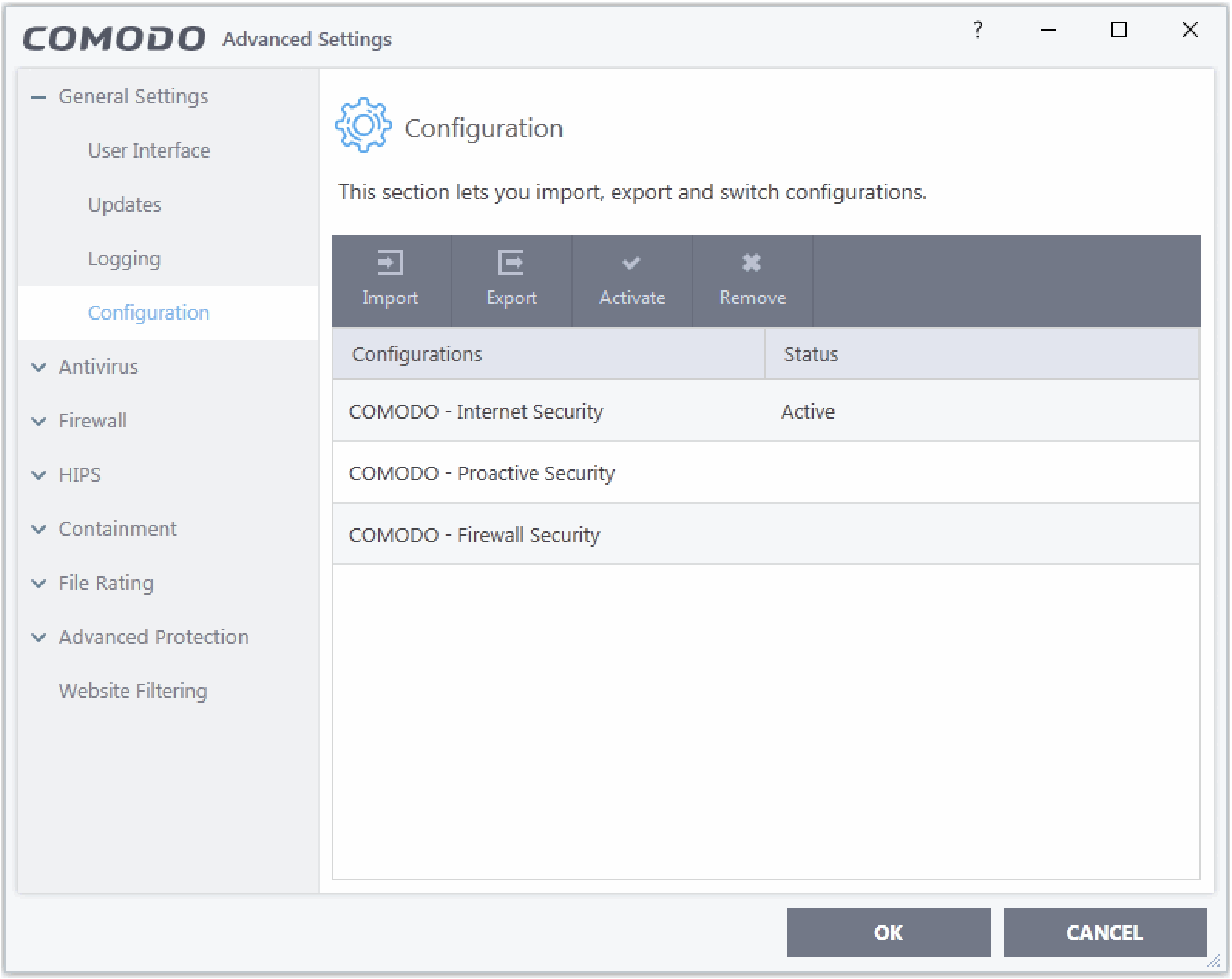
- These settings include your configuration of the antivirus, firewall, HIPS, containment, website filtering, VirusScope and secure shopping modules.
- Exporting your settings can be a great time-saver if:
  - You are a network admin looking to roll out a standard security configuration across multiple computers.
  - You are upgrading your system and need to uninstall and re-install Comodo Internet Security.
- After re-installation, you can import your previous settings and avoid having to configure everything over again.

Note: Any changes you make over time will be automatically stored in the currently active profile. If you want to export your current settings then export the 'Active' profile.

The 'Configuration' tab under 'General Settings' allows you to switch your currently active profile and import/export profiles.

To access the 'Configuration' settings interface

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Configuration' under 'General Settings' on the left:



Configuration

This section lets you import, export and switch configurations.

Configurations	Status
COMODO - Internet Security	Active
COMODO - Proactive Security	
COMODO - Firewall Security	

The 'Configurations' interface displays a list of pre-defined and user-defined configuration profiles. The profile that is currently deployed is shown as 'Active' in the 'Status' column. The following sections explain more about:

- **Comodo Preset Configurations**

- **Importing/Exporting and Managing Personal Configurations**

6.1.4.1. Comodo Preset Configurations

CIS ships with the following preset configurations:

- **COMODO - Internet Security**
- **COMODO - Proactive Security**
- **COMODO - Firewall Security**

By default, CIS is installed with 'COMODO - Internet Security' as the active configuration profile.

- Reminder - the active profile is, in effect, your current CIS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time from the 'Configuration' panel.

COMODO - Internet Security - This configuration is activated by default, when both Antivirus and Firewall components are installed (i.e. the complete installation). The firewall is always set to 'Safe mode' but, according to the results of the 'Quick Scan' performed during the setup process, the HIPS setting may vary. If no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is 'Safe Mode'.

- Auto-Containment is Enabled.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- HIPS is tuned to prevent infection of the system.

If you wish to switch to Internet Security option, you can **select** the option from the 'Configuration' panel.

COMODO - Proactive Security - This configuration turns CIS into the ultimate protection machine. All possible protections are activated and all critical COM interfaces and files are protected. During the setup, if only Comodo Firewall installation option is selected, the next screen allows users to select this configuration as default CIS configuration. If selected, Firewall is always set to Safe mode. But according to the 'Quick Scan' results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

If you wish to switch to Proactive Security option, you can **select** the option from the 'Configuration' panel.

COMODO - Firewall Security - This configuration is activated when the user chooses to install Firewall only and selects optimum protection settings for HIPS. Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

- Auto-Contained is disabled.
- Computer Monitor and Keyboard are NOT monitored.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- HIPS is tuned to prevent infection of the system and detect Internet access request leaks even if it is infected.

If you wish to switch to Firewall Security option, you can **select** the option from the 'Configuration' panel.

6.1.4.2. Importing/Exporting and Managing Personal Configurations

CIS configurations can be imported, exported, activated and managed through the 'Configuration' panel (click the 'Configuration' tab under 'General Settings' in the 'Advanced Settings' interface). Configuration profiles have the file extension .cfgx.

Click the link on which you would like more information:

- **Export a stored configuration to a file**
- **Import a saved configuration from a file**

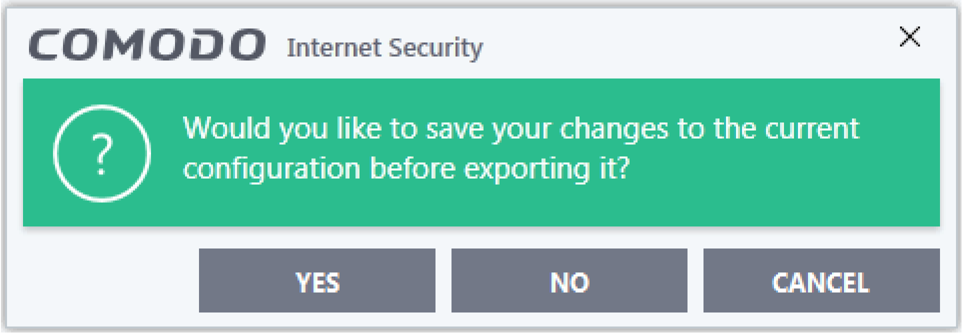
- **Select a different active configuration setting**
- **Remove an inactive configuration profile**

Exporting a stored configuration to a file

1. Open the configuration panel by clicking 'Configuration' under General Settings in the 'Advanced Tasks' interface

2. Select the configuration and click 'Export' at the top.

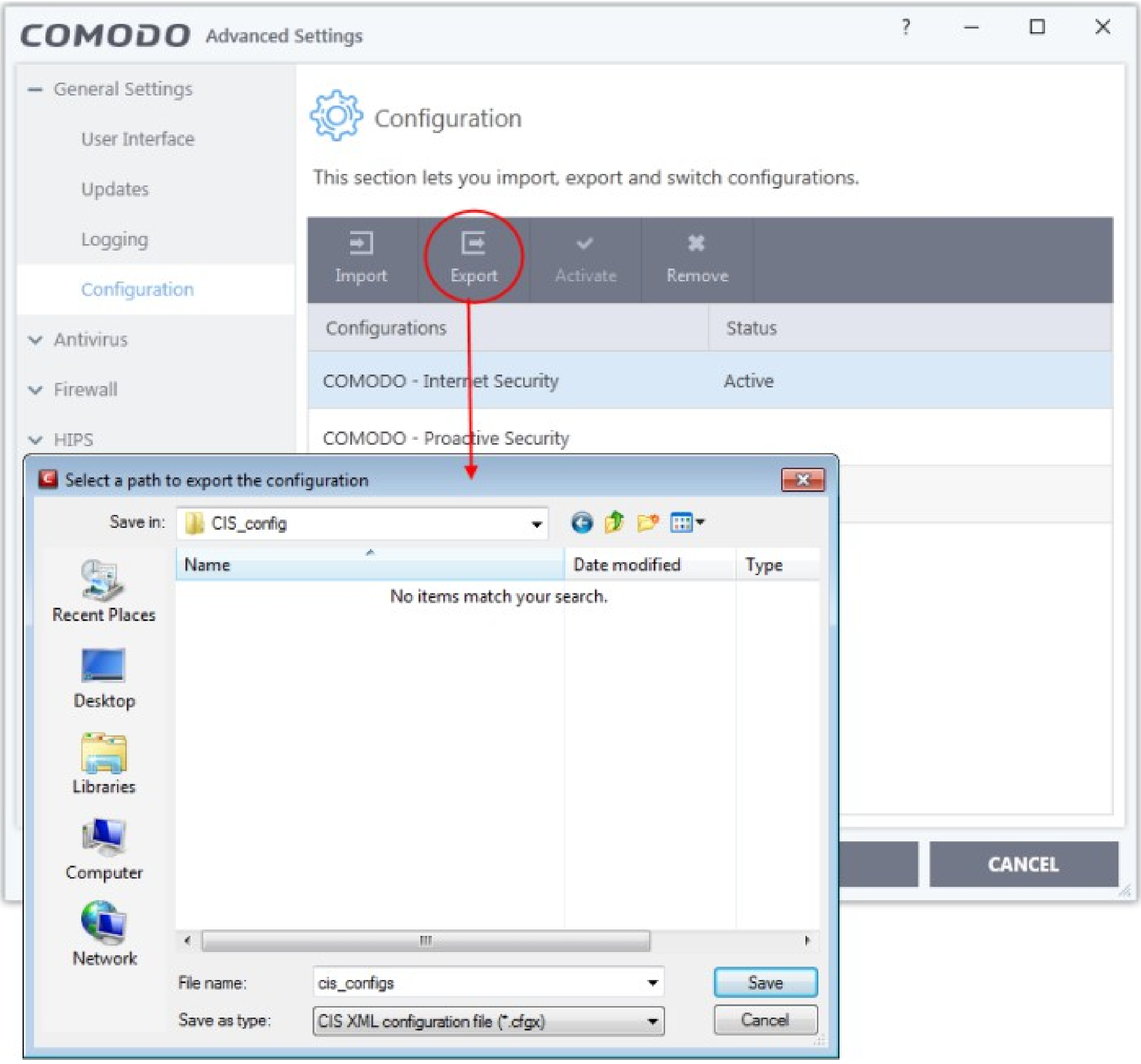
3. If there are any unsaved changes to CIS settings then you can save them before exporting:



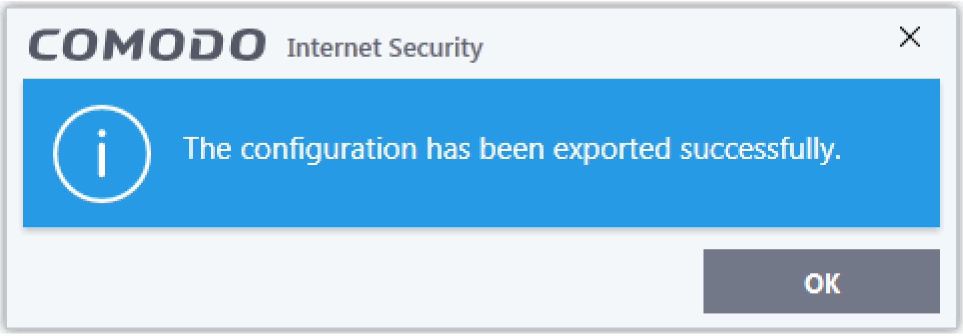
COMODO Internet Security

Would you like to save your changes to the current configuration before exporting it?

4. Navigate to the location where you want to save the configuration file, type a name (e.g., 'My CIS Profile') and click 'Save':



A confirmation dialog will appear if the export is successful:



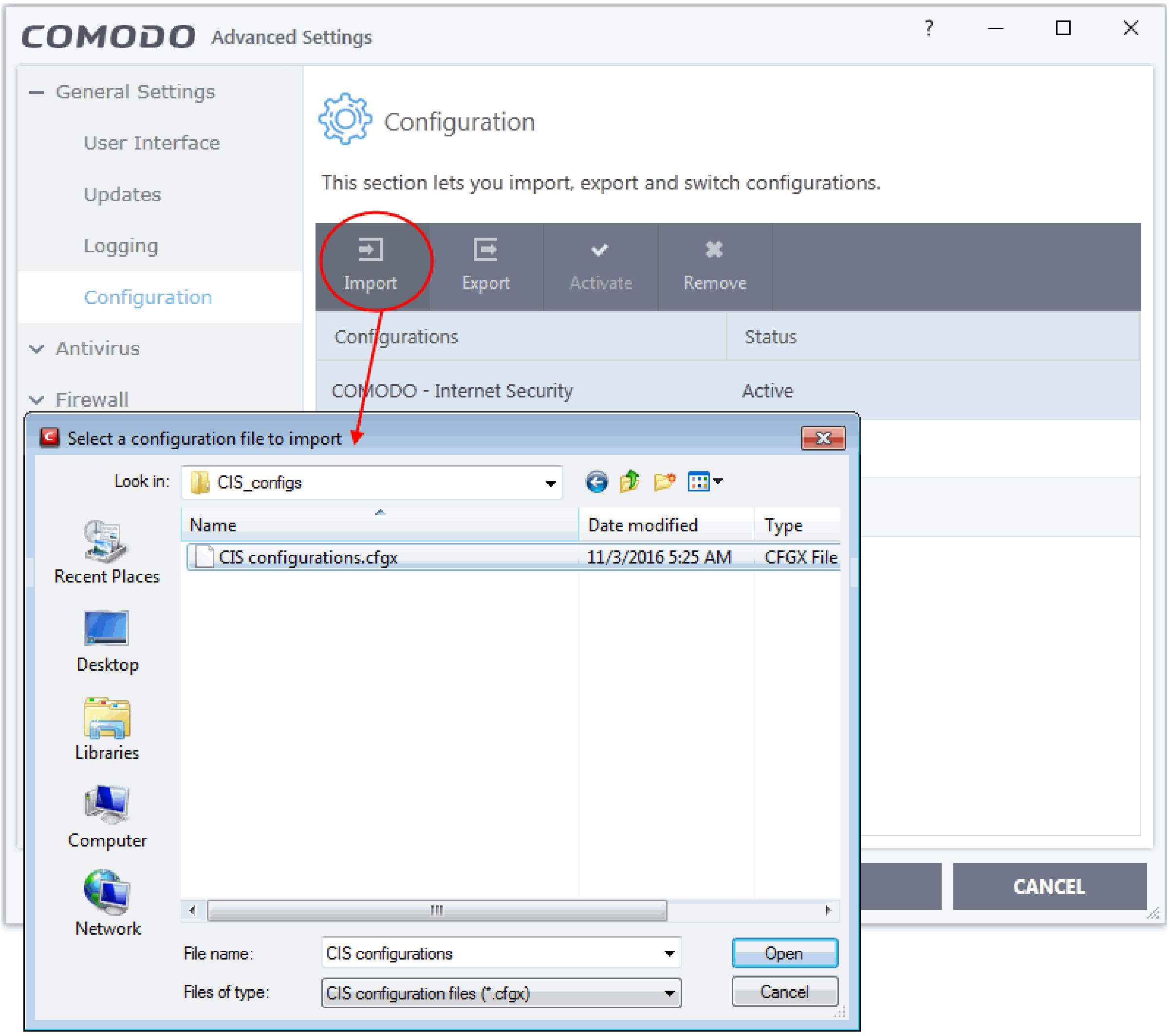
Importing a saved configuration from a file

You can import a CIS configuration file by clicking the 'Import' button. Note - any profile you import will not become active until you **activate it**.

To import a profile

1. Open the configuration panel by clicking 'Configuration' under General Settings in the 'Advanced Tasks' interface

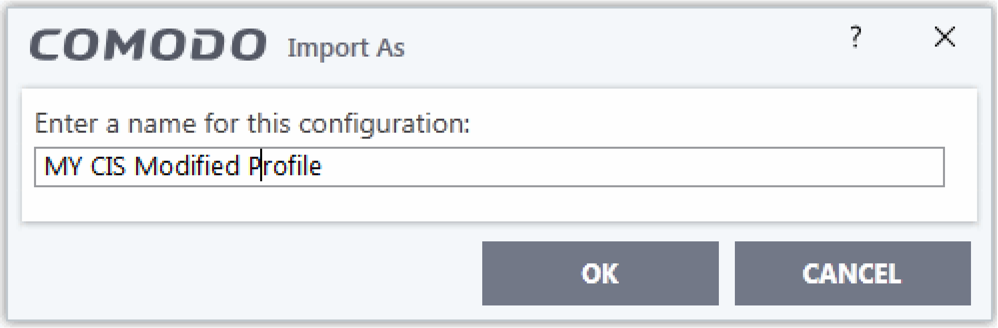
2. Click 'Import' at the top.



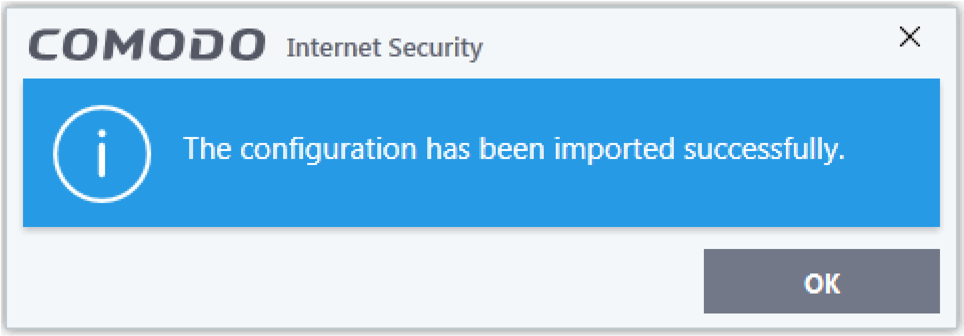
3. Navigate to the location of the saved profile and click 'Open'. Configuration files have a .cfgx extension.

The 'Import As' dialog will appear.

4. Enter a name for the profile you wish to import and click 'OK'.

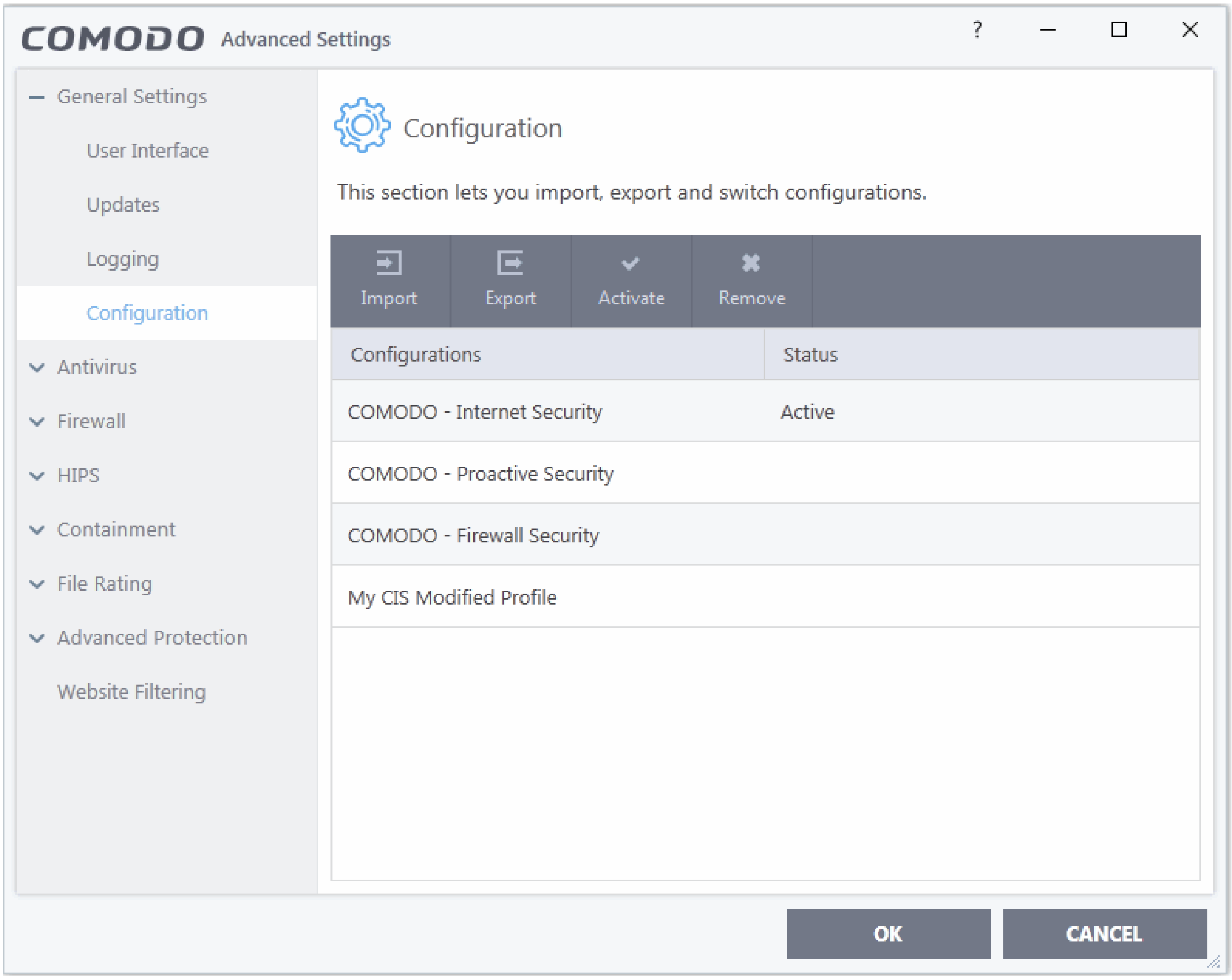


A confirmation dialog will appear indicating the successful import of the profile.



The configuration has been imported successfully.

Once imported, the configuration profile can be re-exported or deployed in the current installation by making it **active**.



Configuration

This section lets you import, export and switch configurations.

Configurations	Status
COMODO - Internet Security	Active
COMODO - Proactive Security	
COMODO - Firewall Security	
My CIS Modified Profile	

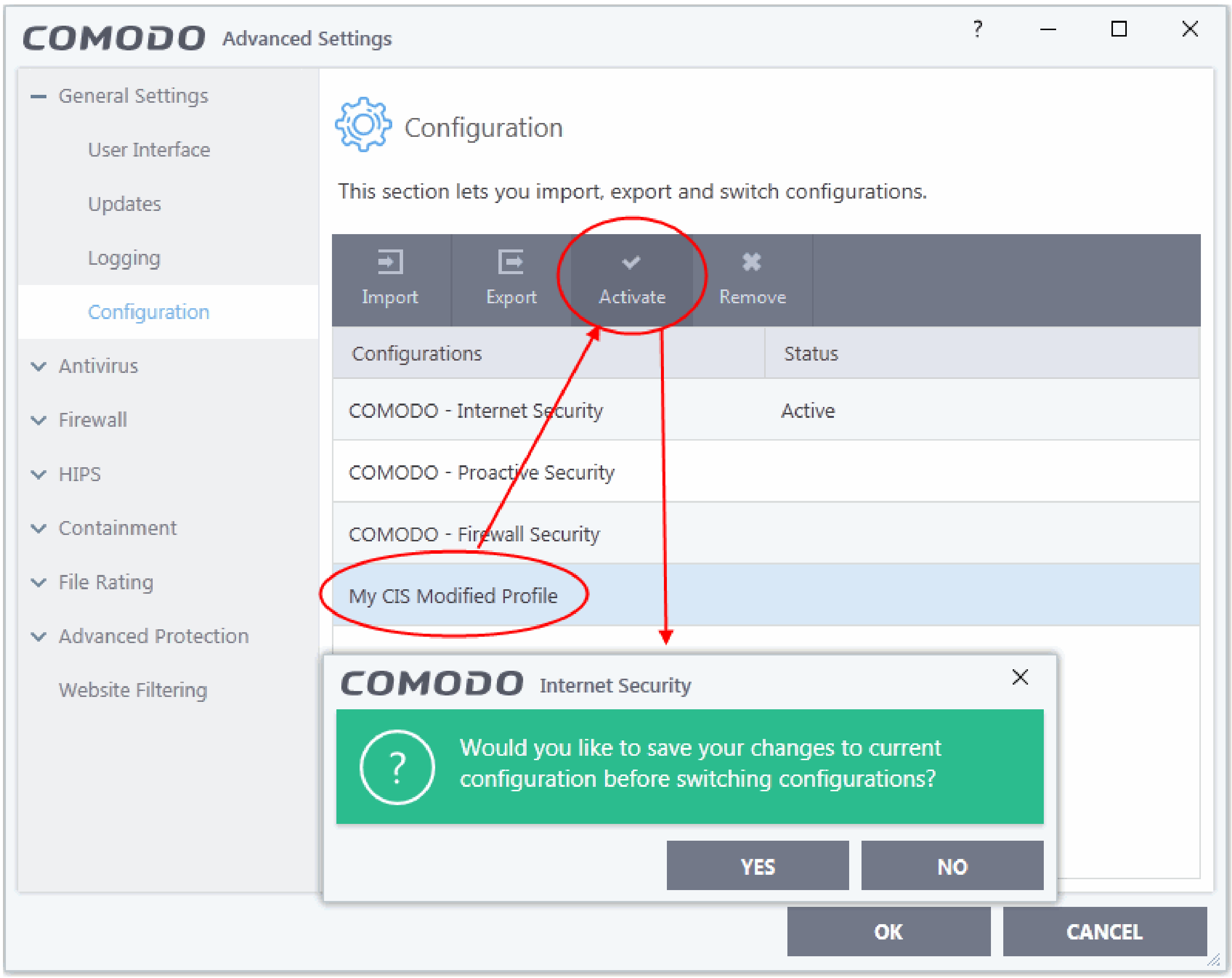
Selecting and Implementing a different configuration profile

You can change the active configuration profile at any time from the 'Configurations' panel

To change the active configuration profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Choose the configuration profile you want to activate and click 'Activate' from the top.

You will be prompted to save the changes in the settings in you current profile before the new profile is deployed.



COMODO Advanced Settings

Configuration

This section lets you import, export and switch configurations.

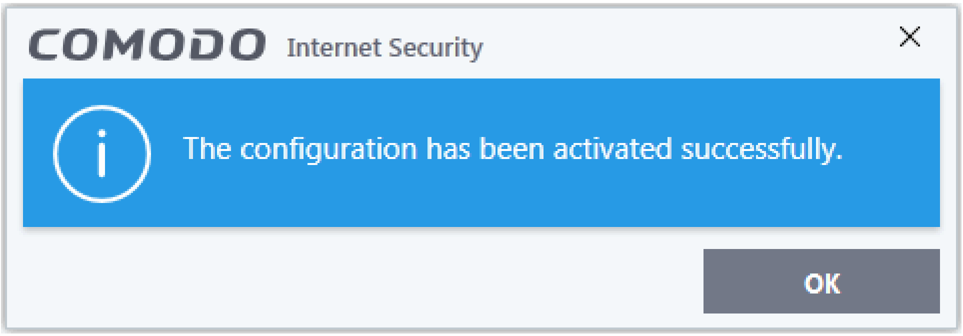
Configurations	Status
COMODO - Internet Security	Active
COMODO - Proactive Security	
COMODO - Firewall Security	
My CIS Modified Profile	

COMODO Internet Security

Would you like to save your changes to current configuration before switching configurations?

3. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

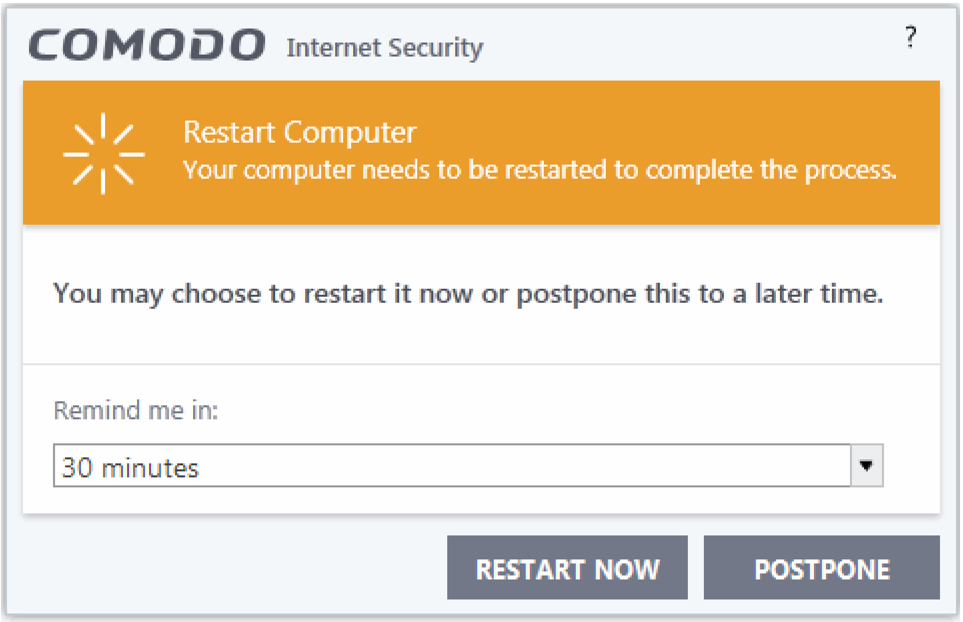
An activation confirmation dialog will be displayed.



COMODO Internet Security

The configuration has been activated successfully.

Your new profile will be set active. If you are switching to 'Comodo Proactive Security' profile from a different profile or switching to any other profile from 'Comodo Proactive Security' profile, your computer needs to be restarted for the new profile to be activated. 'A Restart Computer' dialog will appear at the bottom right of the screen.



Restart Computer

Your computer needs to be restarted to complete the process.

You may choose to restart it now or postpone this to a later time.

Remind me in:

30 minutes

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

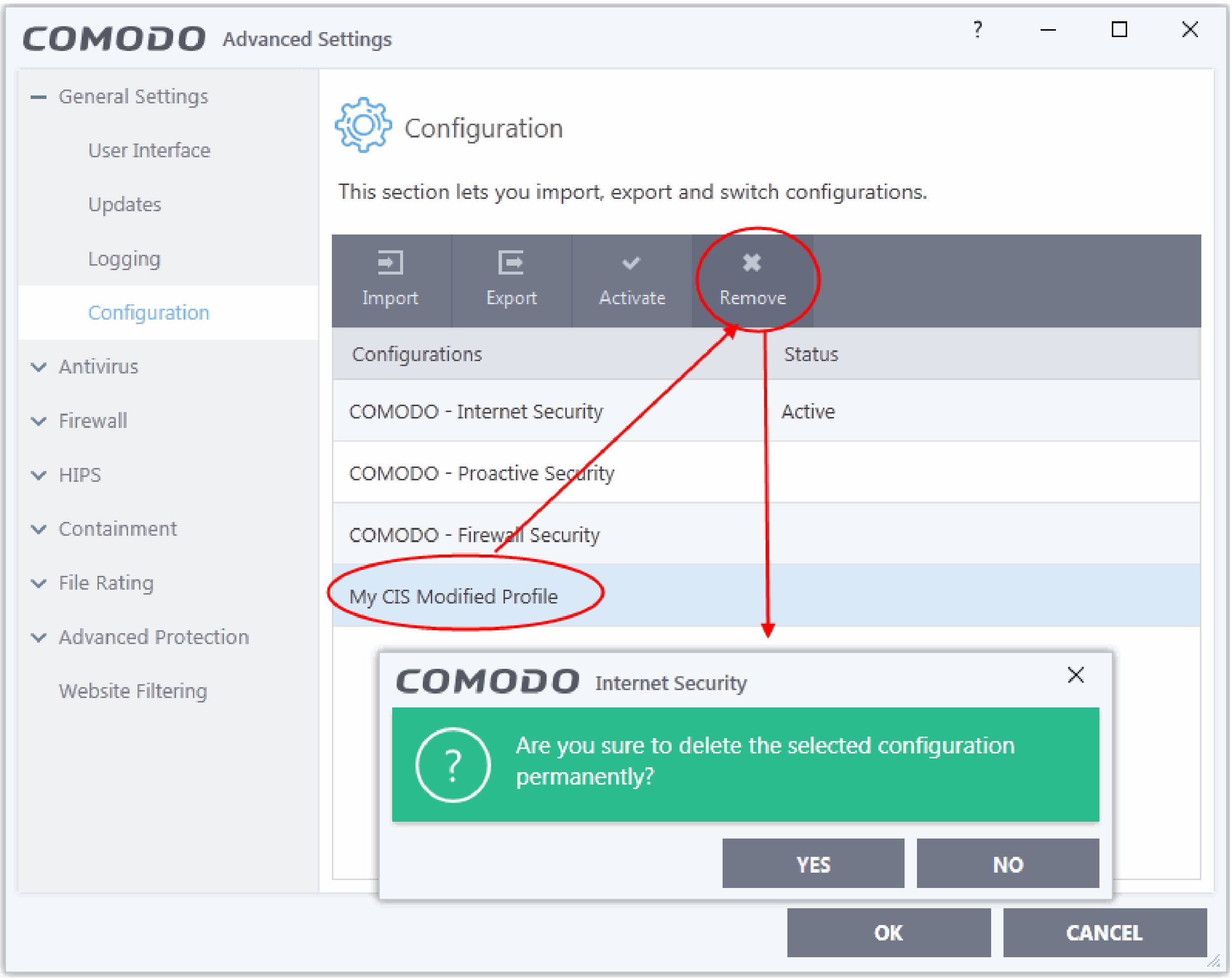
Removing an inactive configuration profile

You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that Comodo Internet Security is currently using - only the inactive ones. For example if the COMODO - Internet Security is the active profile, you can only delete the inactive profiles, 'COMODO - Proactive Security, 'My_CIS_Configuration and so on.

To remove an unwanted profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Choose the configuration profile you want to delete and click the 'Remove' from the top.

A confirmation dialog will be displayed.



Configuration

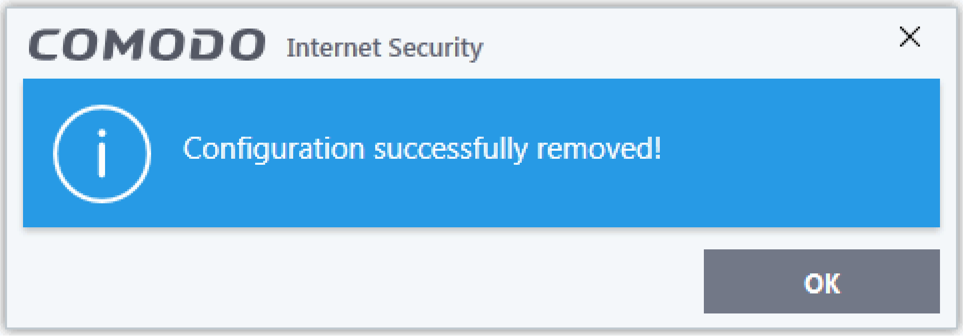
This section lets you import, export and switch configurations.

Configurations	Status
COMODO - Internet Security	Active
COMODO - Proactive Security	
COMODO - Firewall Security	
My CIS Modified Profile	

COMODO Internet Security

Are you sure to delete the selected configuration permanently?

3. Click 'Yes'. The configuration profile will be deleted from your computer.



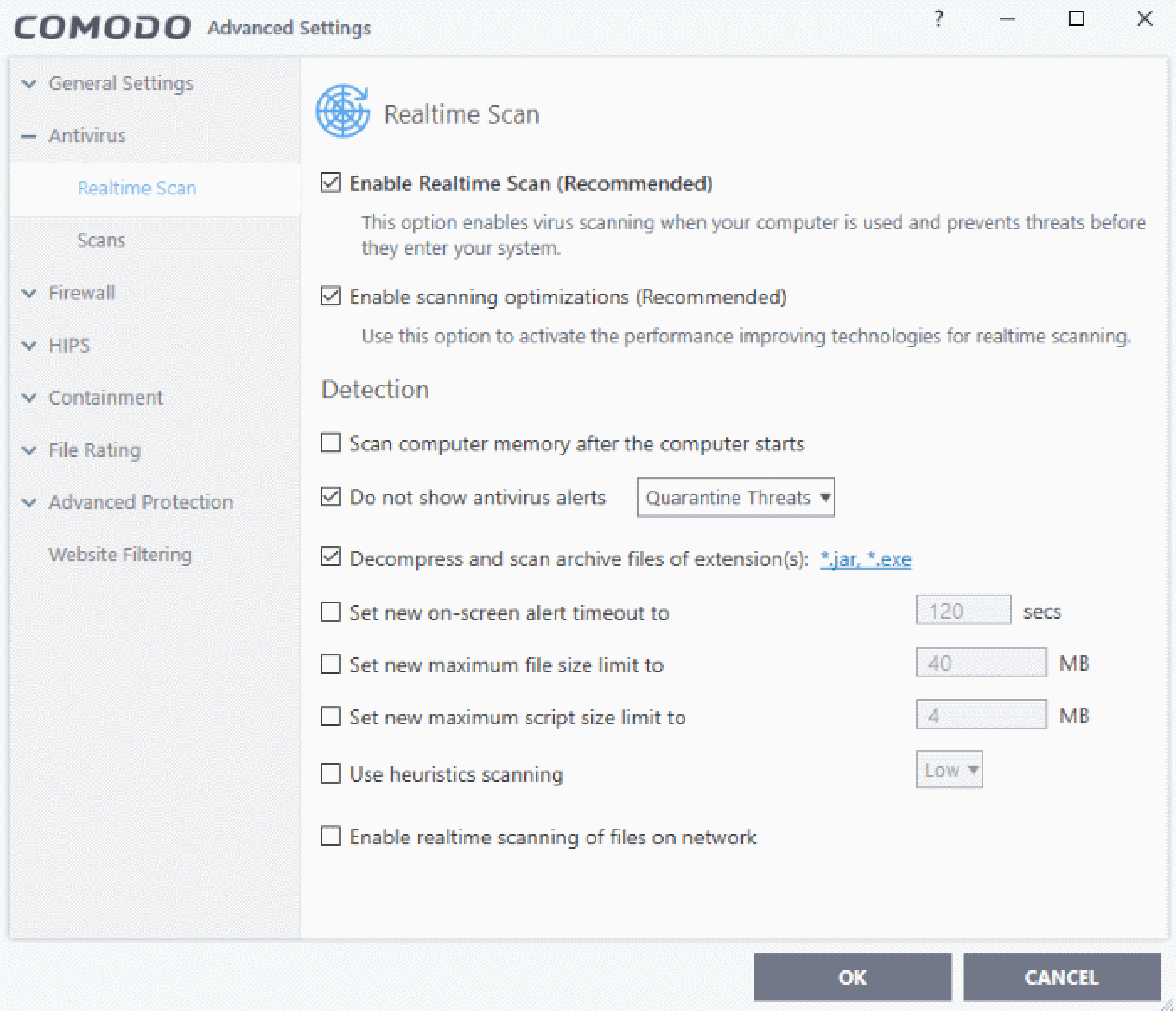
Configuration successfully removed!

6.2. Antivirus Configuration

The 'Antivirus' component of CIS allows you to configure realtime scans and custom scan profiles.

To configure the 'Antivirus' component:

- Click 'Settings' on the CIS home screen to open the 'Advanced Settings' interface.
- Click 'Antivirus' on the left:



Realtime Scan

☑ Enable Realtime Scan (Recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning.

Detection

☐ Scan computer memory after the computer starts

☑ Do not show antivirus alerts: Quarantine Threats

☑ Decompress and scan archive files of extension(s): *.jar, *.exe

☐ Set new on-screen alert timeout to 120 secs

☐ Set new maximum file size limit to 40 MB

☐ Set new maximum script size limit to 4 MB

☐ Use heuristics scanning: Low

☐ Enable realtime scanning of files on network

The following sections explain in detail on:

- **Real-time Scan Settings**
- **Custom Scan Profiles**

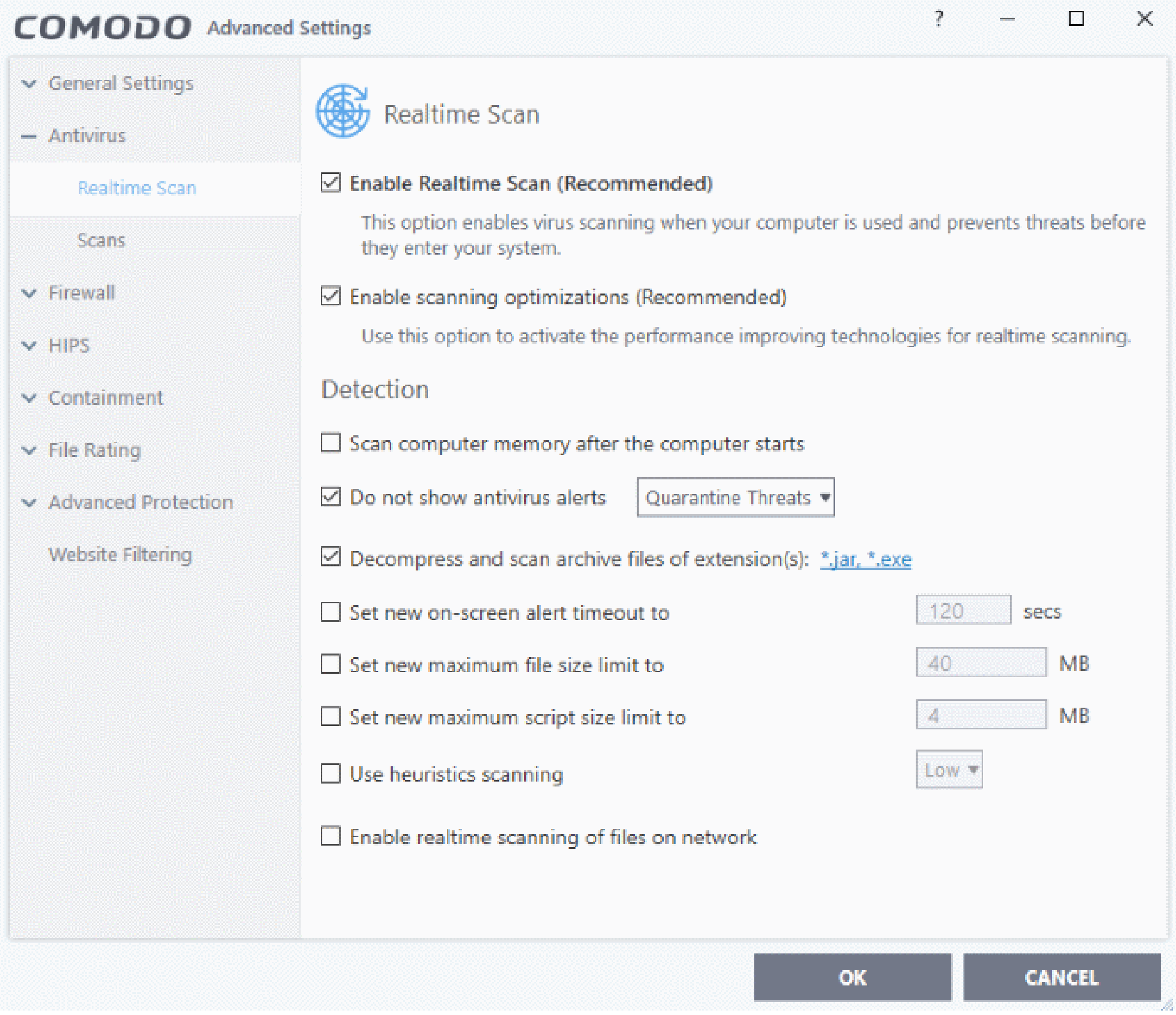
6.2.1. Real-time Scan Settings

The real-time virus scanner (aka 'On-Access Scanner') checks files in real-time when they are created, opened or copied. As soon as you interact with a file, Comodo Antivirus checks it. This ensures your system is constantly monitored for malware and enjoys the highest levels of protection. The real-time scanner also scans system memory on system startup.

The scanner will detect and block any malicious programs and show you an alert. Should you wish, you can specify that CIS does not show you alerts but automatically deals with the threat (choice of auto-quarantine or auto-block/delete). We recommend you leave the real-time scanner enabled at all times.

To open the 'Real-time Scan' settings panel

- Click 'Settings' at the top of the CIS home screen
- Click 'Antivirus' > 'Realtime Scan' on the left



COMODO Advanced Settings

Realtime Scan

☑ Enable Realtime Scan (Recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning.

Detection

☐ Scan computer memory after the computer starts

☑ Do not show antivirus alerts [Quarantine Threats ▾]

☑ Decompress and scan archive files of extension(s): *.jar, *.exe

☐ Set new on-screen alert timeout to [120] secs

☐ Set new maximum file size limit to [40] MB

☐ Set new maximum script size limit to [4] MB

☐ Use heuristics scanning [Low ▾]

☐ Enable realtime scanning of files on network

- **Enable Realtime Scan *(Recommended)*** – Activate or deactivate real-time scanning. The real-time scanner continually monitors your computer for malicious activity and protects you from threats as soon as they occur. Comodo strongly recommends you keep this option enabled. ***(Default=Enabled)***
- **Enable scanning optimizations** - Will enable various optimization techniques during a virus scan to reduce resource usage and speed-up the scanning process. For example, running the scan in the background. ***(Default = Disabled)***

Note: The above two settings can be modified from the 'Advanced View' of the Home screen by clicking the status link beside Antivirus. If you choose Disabled option, both 'Enable Realtime Scan' and 'Enable scanning optimizations' will be disabled. If you choose 'Stateful', both the settings will be enabled and on choosing 'On Access', only 'Enable Realtime Scan' will be enabled.

Detection Settings

- **Scan computer memory after the computer starts** - The antivirus scans system memory immediately after your computer starts up. Disable to remove the scan from the list of Windows startup processes. ***(Default = Disabled)***
- **Do not show antivirus alerts** - Configure whether or not alerts are shown when malware is encountered. (***Default = Enabled***)

  Choosing 'Do not show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CIS should automatically take:

  - **Quarantine Threats** - Blocks the threat and moves it to quarantine for your later assessment and action. (***Default***)

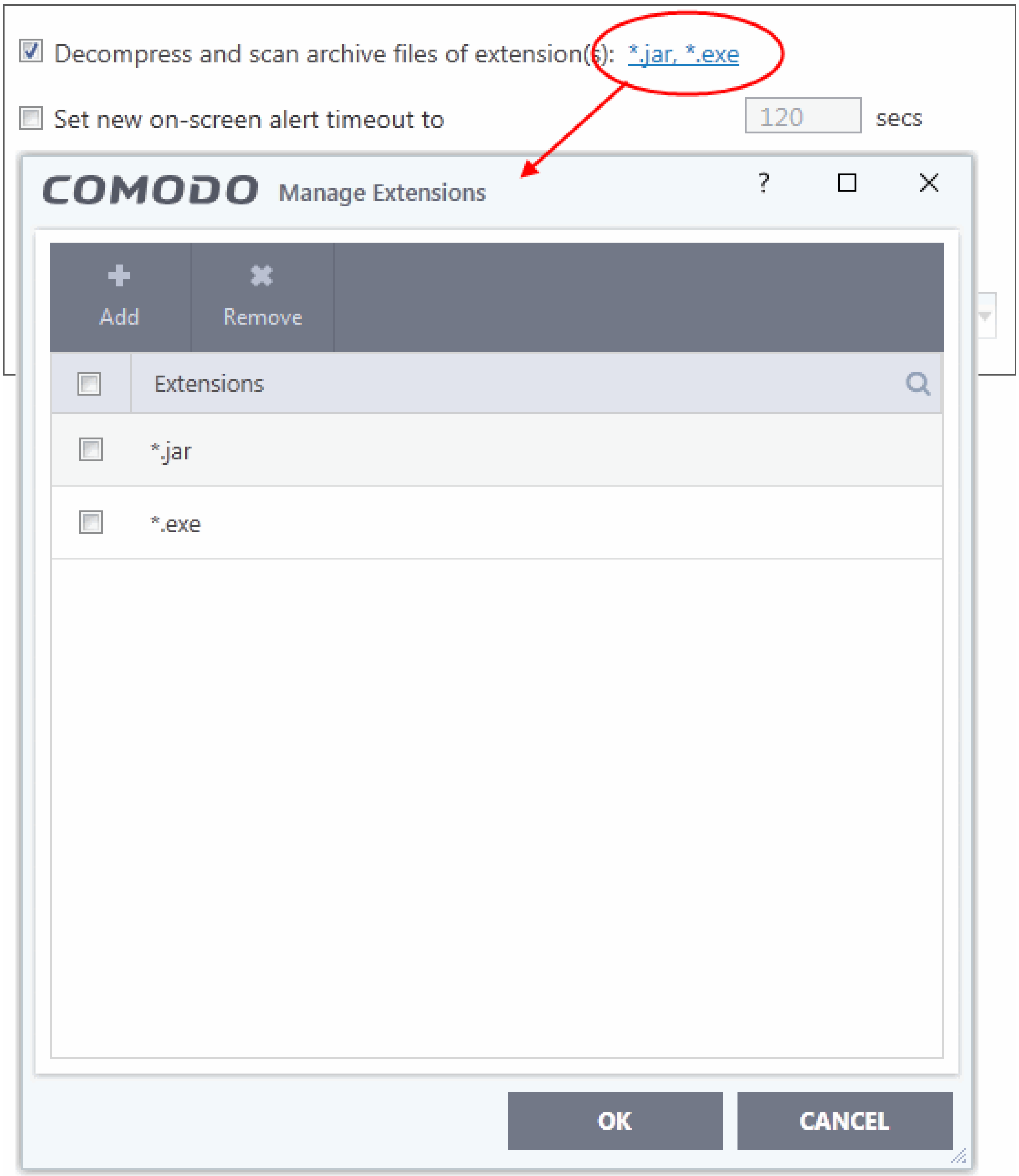
- **Block Threats -** Will automatically block and delete the threat.

Note: If you deselect this option, and thus enable alerts, then your choice of quarantine/block is presented within the alert itself.

- **Decompress and scan archive files of extension(s) -** If enabled, Comodo Antivirus will scan all types of archive files. Archive file types include .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB files. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default = Enabled)***

  You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

  - Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open with a list of archive file types that are decompressed and scanned by real-time scanner.



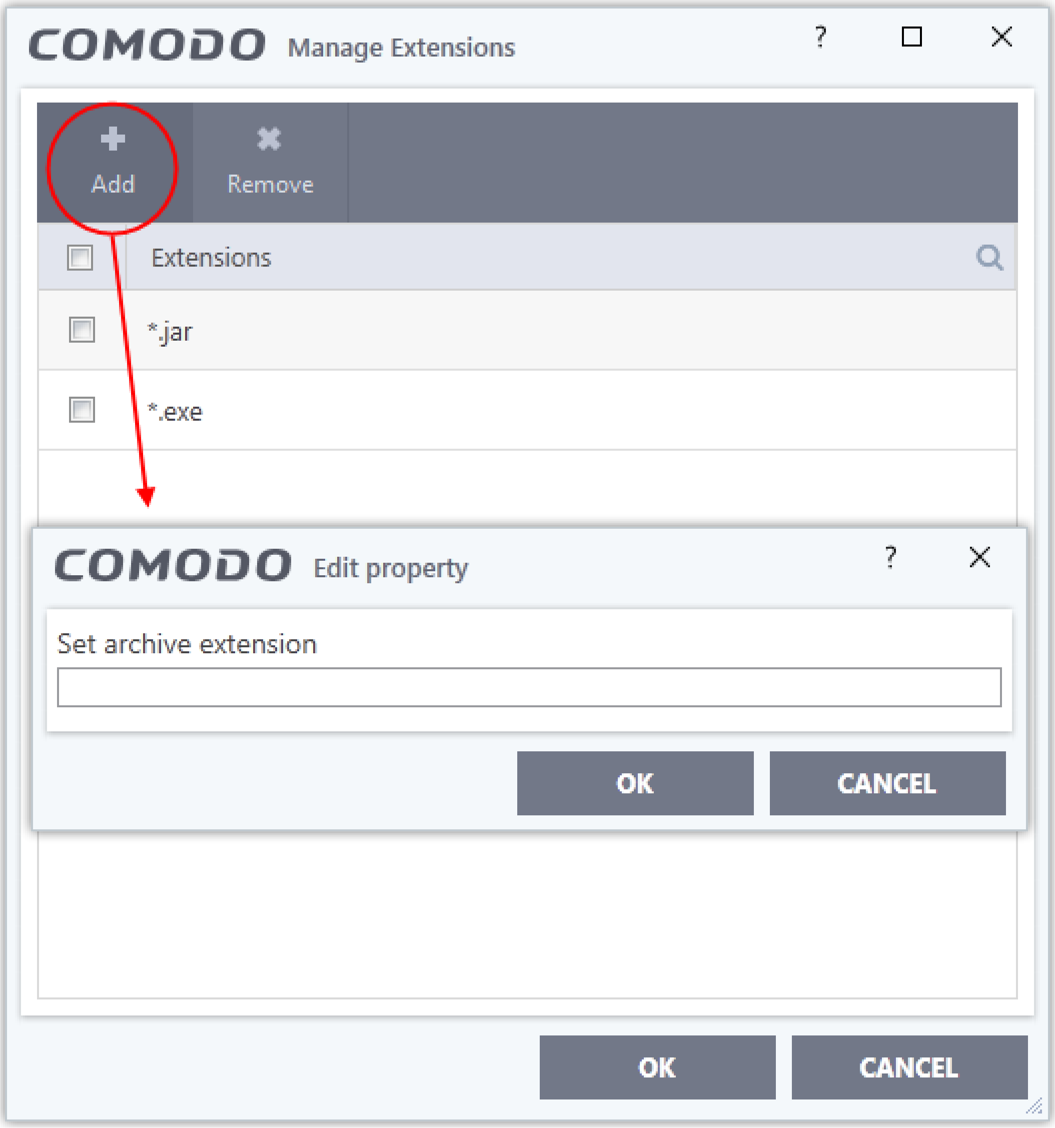
☑ Decompress and scan archive files of extension(s): *.jar, *.exe

□ Set new on-screen alert timeout to 120 secs

COMODO Manage Extensions

□	Extensions
□	*.jar
□	*.exe

  - To add a new archive file type, click 'Add' at the top



   - Enter the extension type you wish to scan and click 'OK'. Example extensions include .zip , .rar, .msi, .7z , .jar and .cab.
   - Repeat the process to add more extensions
   - Click 'OK' in the 'Manage Extensions' dialog
   - To remove an archive file type, choose the file type from the list, click 'Remove' from the top and click 'OK' in the 'Manage Extensions' dialog.

- **Set new on-screen alert timeout to -** Set the time period (in seconds) that virus alerts should stay on the screen. ***(Default = 120 seconds)***
- **Set new maximum file size limit to -** Set the maximum size of files (in MB) that the antivirus should scan. Files larger than the size specified here will not be not scanned. **(*Default = 40 MB*)**
- **Set new maximum script size limit to -** Set the maximum size of scripts (in MB) that the antivirus should scan. Files larger than the size specified here will not be scanned. **(*Default = 4 MB*)**
- **Use heuristics scanning -** Enable or disable heuristics scanning and define scanning level. ***(Default = Enabled)***

  Background. Heuristic techniques identify previously unknown malware by analyzing a file to see if it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' attributes rather than looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current virus database.

If enabled, select the level of heuristic scanning from the drop-down:

- **Low -** 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest alerts. This setting combines a high level of protection with a low rate of false positives. Comodo recommends this setting for most users. ***(Default)***
- **Medium -** Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High -** Highest sensitivity to detecting unknown threats but also raises the possibility of more false positives.

- **Enable Realtime Scanning of files on network –** Activate or deactivate on-access scans of network files. If enabled, any files you interact with on a network drive will be checked by the virus scanner, even if you do not copy them to your local machine. ***(Default=Disabled)***

6.2.2. Scan Profiles

An antivirus scan profile is a collection of scanner settings that tell CIS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)
- How to scan (a profile lets you specify the behavior of the scan engine)

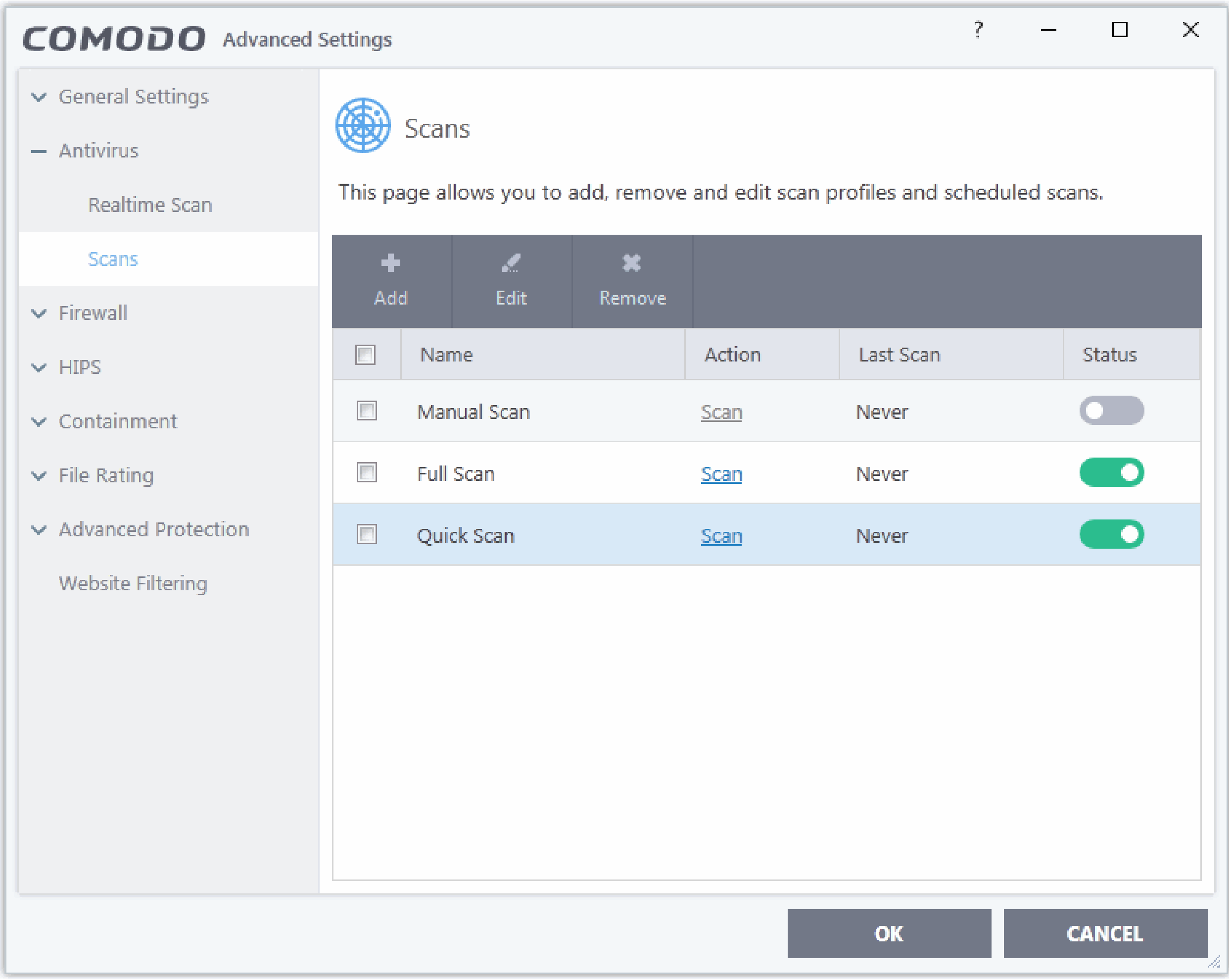
CIS ships with three pre-defined scan profiles and allows you to create custom scan profiles.

- Full Scan - Covers every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.
- Quick Scan - Covers critical areas of your computer which are highly prone to infection from viruses, root-kits and other malware. 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.
- Manual Scan - Choose the settings you wish to use for manual scans. Manual scans are used, for example, when you right-click on a file/folder and choose 'Scan with COMODO antivirus'. Double-click 'Manual scan' to the set items you want to scan. See '**Instantly Scan Files and Folders**' for more details.

You cannot modify the areas scanned in a pre-defined profile, but can edit the parameters that define the behavior of the scan. You can also create custom profiles and scan schedules.

To access the 'Scans' panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Scans' under 'Antivirus' on the left



Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	Off
□	Full Scan	Scan	Never	On
□	Quick Scan	Scan	Never	On

The 'Scans' panel displays a list of pre-defined and user defined scan profiles.

Scan Profiles - Column Descriptions	
Column Header	**Description**
Name	Name of the scan profile.
Action	The activity that the profile is set to perform. Click this link to manually run a scan according to the profile's parameters.
Last Scan	Date and time of the most recent virus scan using this profile.
Status	Enable or disable the profile. 'On' – Any scheduled scans configured in the profile will continue to run. In addition, you can manually run the scan at any time by clicking the 'Scan' link. 'Off' - Any scheduled scans configured in the profile will not run. You can still manually run the scan by clicking the 'Scan' link.

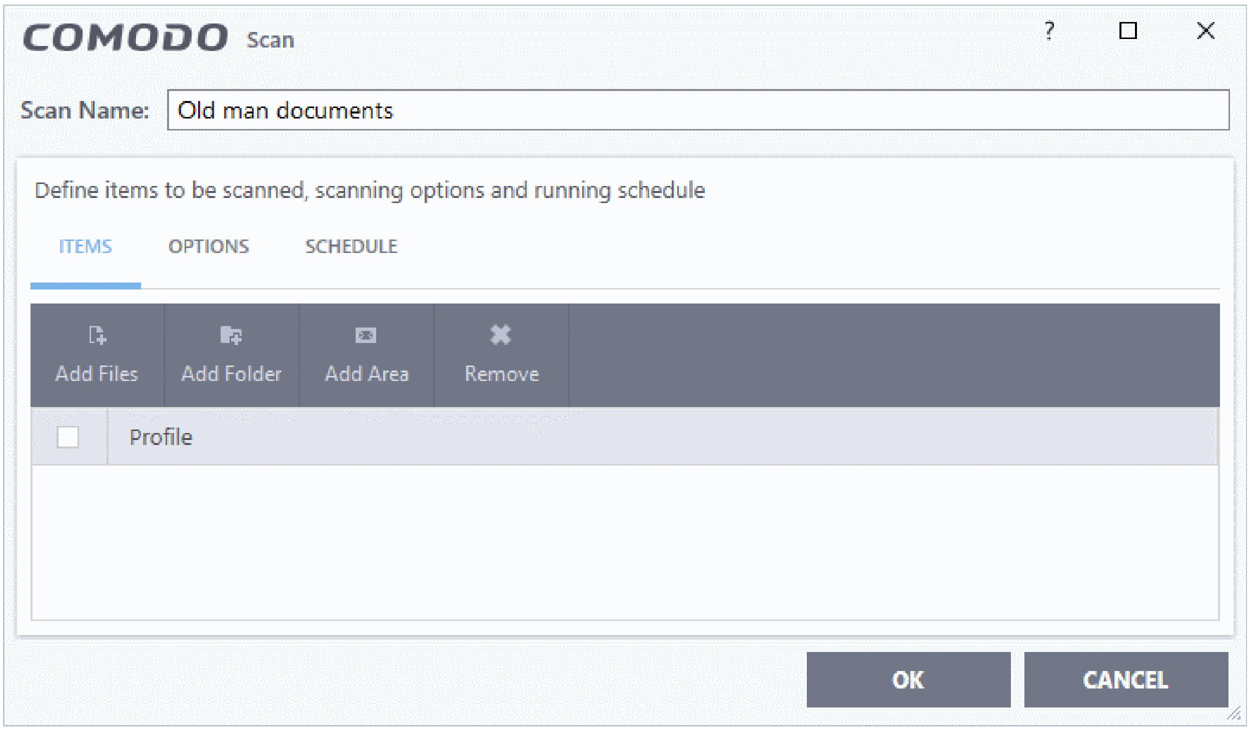
The following sections explain more on:

- Creating a Scan Profile
- Running a custom scan

To create a custom profile

- Click 'Add' from the options at the top.

The profile configuration screen will open:



- Type a name for the profile in the 'Scan Name' text box.

The next steps are to:

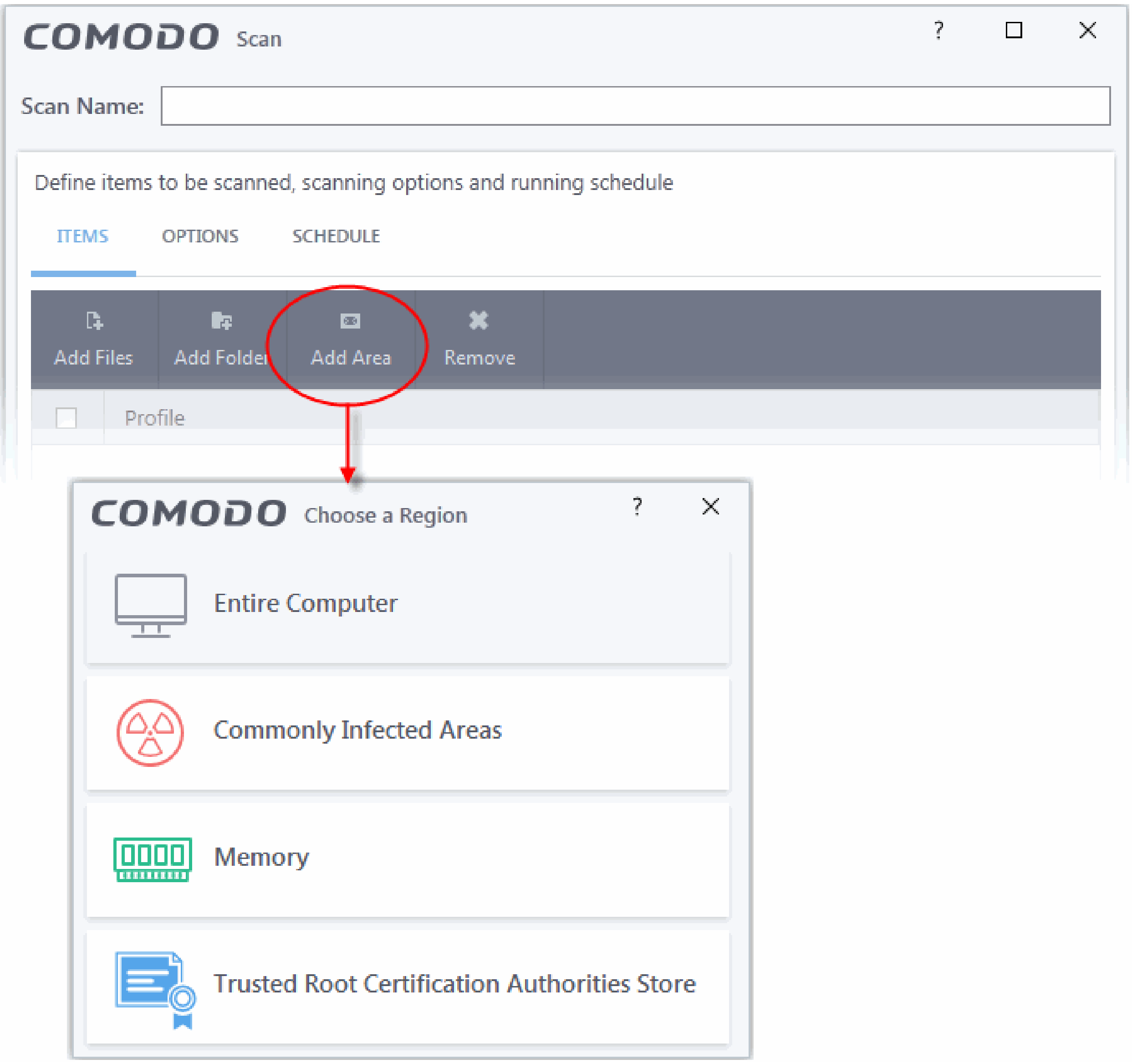
- Select the items to be scanned
- Configure the scanning options for the profile
- Configure a schedule for the scan to run periodically

To select the items to be scanned

- Click 'Items' at the top of the 'Scans' interface.

The buttons at the top allow you to add three item types. You can add any combination of items.

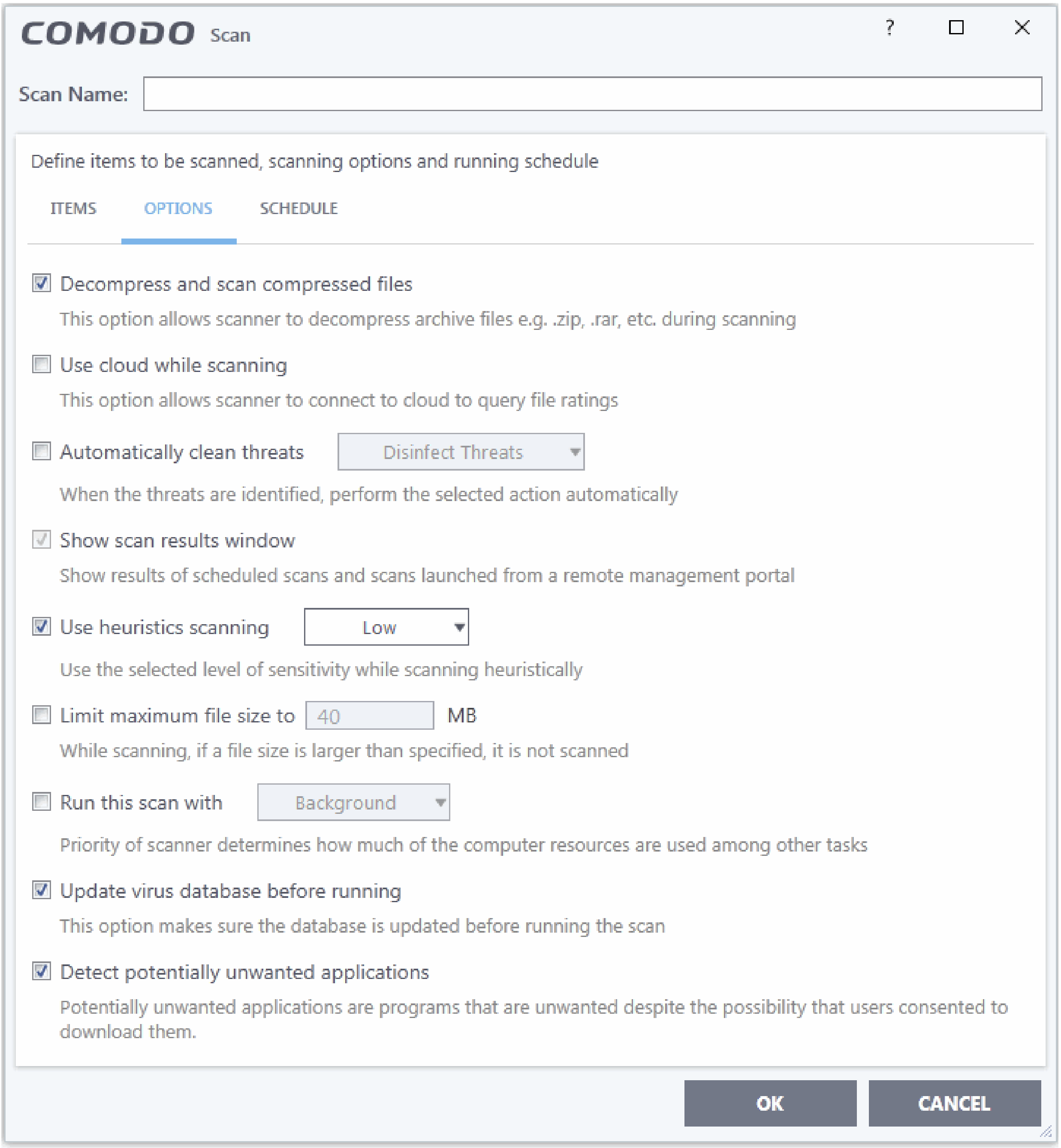
- Add File - Add individual files to the profile. Any files you add will be specifically scanned when the profile runs.
- Add Folder - Add entire folders to the profile. All folder contents will be scanned when the profile runs.
- Add Area - Add a regions of your computer which should be scanned when you run the profile. Regions include 'Full Computer', 'Commonly Infected Areas', 'System Memory' and 'Trusted Root Certificate Store'.



- Repeat the process to add more items to the profile.
- To remove an item, select it and click 'Remove'.

To configure Scanning Options

- Click 'Options' at the top of the 'Scans' interface



Scan Name:

Define items to be scanned, scanning options and running schedule

☑ Decompress and scan compressed files

This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

□ Use cloud while scanning

This option allows scanner to connect to cloud to query file ratings

□ Automatically clean threats: Disinfect Threats

When the threats are identified, perform the selected action automatically

☑ Show scan results window

Show results of scheduled scans and scans launched from a remote management portal

☑ Use heuristics scanning: Low

Use the selected level of sensitivity while scanning heuristically

□ Limit maximum file size to 40 MB

While scanning, if a file size is larger than specified, it is not scanned

□ Run this scan with: Background

Priority of scanner determines how much of the computer resources are used among other tasks

☑ Update virus database before running

This option makes sure the database is updated before running the scan

☑ Detect potentially unwanted applications

Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download them.

- **Decompress and scan compressed files** - The scan will include archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
- **Use cloud while scanning** - Improves scan accuracy by augmenting the local scan with an online look-up of Comodo's latest signature database. Cloud Scanning means CIS can detect the latest malware even if your virus database is out-dated. ***(Default = Disabled)***.
- **Automatically clean threats** - Choose the automatic action to be taken against detected threats. The options are:
  - **Quarantine Threats** - Infected items will be moved to Quarantine. You can review quarantined items later and remove them or restore them (in case of false positives). See **Manage Quarantined Items** for more details on managing quarantined items.
  - **Disinfect Threats** - If a disinfection routine is available, the antivirus will remove the infection and keep the original, safe, file. If not, the item will be moved to 'Quarantine'. (***Default***)
- **Show scan result window** – If selected, you will see a summary of results at the end of the scan.

This includes the number of objects scanned and the number of threats found.

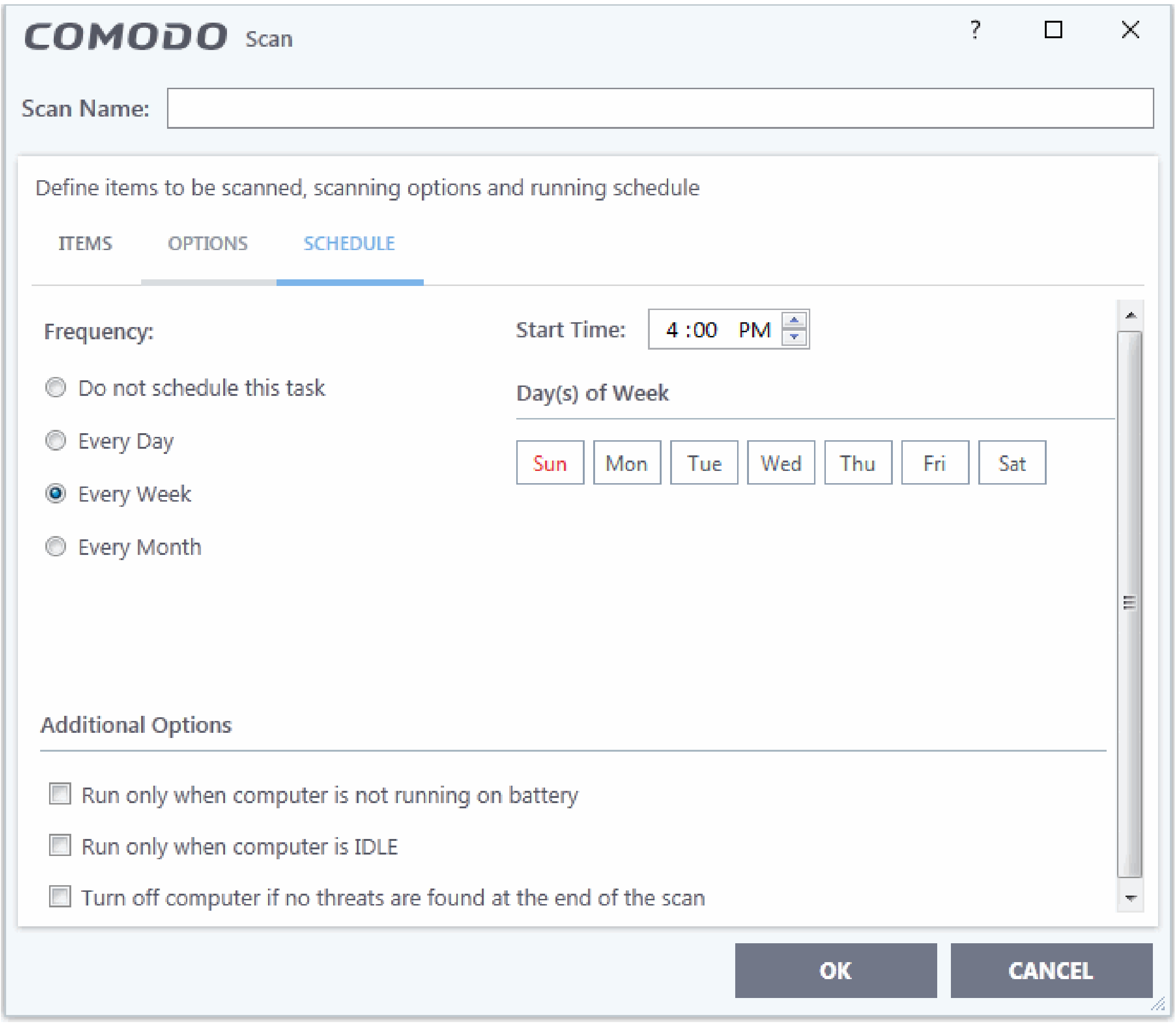
- **Use heuristics scanning -** Select whether or not heuristic techniques should be used during scans in this profile. You are also given the opportunity to define the heuristics scan level. (***Default = Enabled***).

  Background. Heuristic techniques identify previously unknown malware by analyzing a file to see if it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' attributes rather than looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current virus database.
  If enabled, select the level of heuristic scanning from the drop-down:

  - **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest alerts. This setting combines a high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (***Default***)
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High -** Highest sensitivity to detecting unknown threats but also raises the possibility of more false positives.
- **Limit maximum file size to -** Set the maximum size of files (in MB) that the profile should scan. Files larger than the size specified here will not be not scanned. ***(Default = 40 MB)***.
- **Run this scan with -** Set the Windows priority of the scan process. (***Default = Disabled***). The available options are:
  - High
  - Normal
  - Low
  - Background.
- **Update virus database before running -** Instructs Comodo Internet Security to check for and download the latest virus signatures before starting the scan (***Default = Enabled***) .
- **Detect potentially unwanted applications -** If enabled, the scan will also flag applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. Background. PUA's are often bundled as an additional 'utility' when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks your activity on the internet. ***(Default = Enabled).***

To schedule the scan to run at specified time

- Click 'Schedule' at the top of the 'Scan' interface.



COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

Frequency:

○ Do not schedule this task

○ Every Day

● Every Week

○ Every Month

Start Time: 4 :00 PM

Day(s) of Week

Additional Options

□ Run only when computer is not running on battery

□ Run only when computer is IDLE

□ Turn off computer if no threats are found at the end of the scan

Schedule options are:

- **Do not schedule this task -** The scan profile will be created but will not run automatically. The profile will be available for on-demand scans.
- **Every Day -** Run the scan every day at the time specified in the 'Start Time' field.
- **Every Week -** Run the scan on the day(s) specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- **Every Month -** Run the scan on the date(s) specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery -** The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or other mobile device.
- **Run only when computer is IDLE -** The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan -** Will turn off your computer if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.

- **Run during Windows Automatic Maintenance -** Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.

The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See **Automatically Clean Threats**.

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

- Click 'OK' to save the profile.

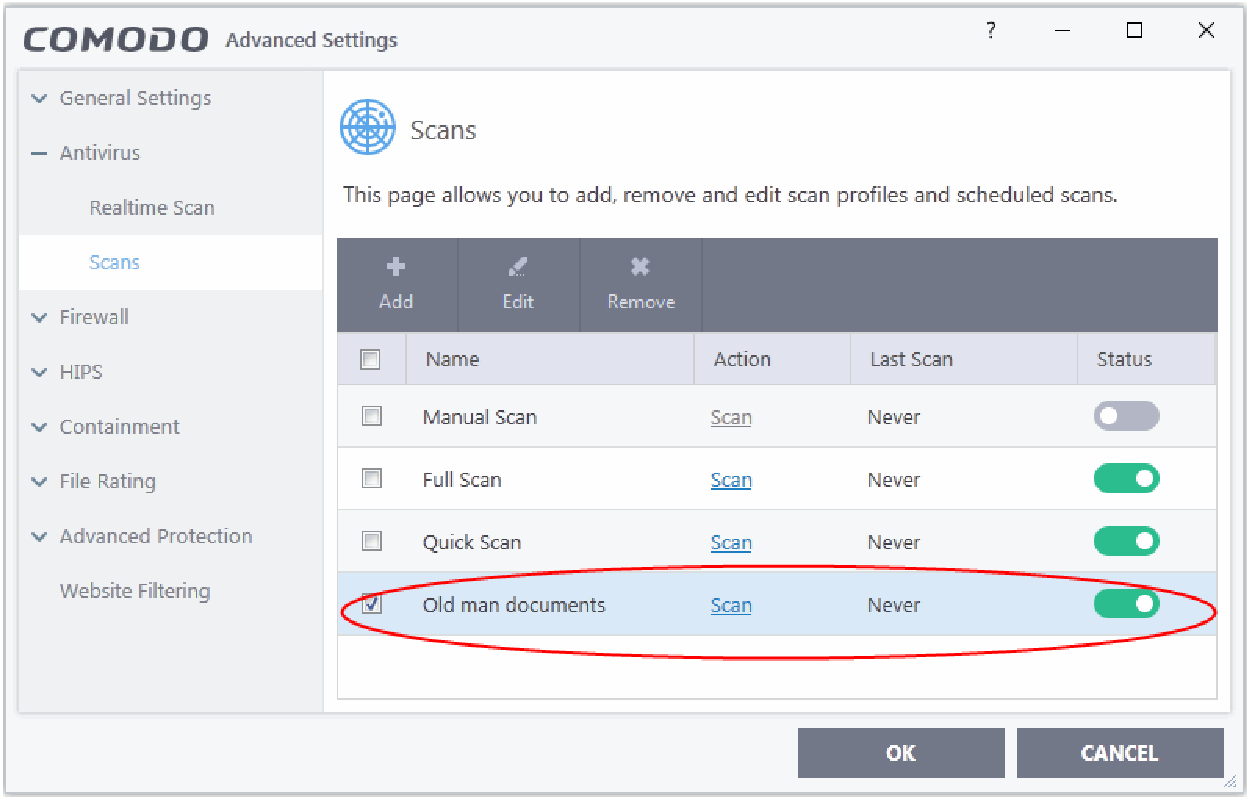
The profile will be available for deployment in future.

To run a custom scan as per scan profile

- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scans' interface
- Click 'More Scan Options' from the 'Custom Scan' pane

The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.

- Click 'Scan' beside the required scan profile.

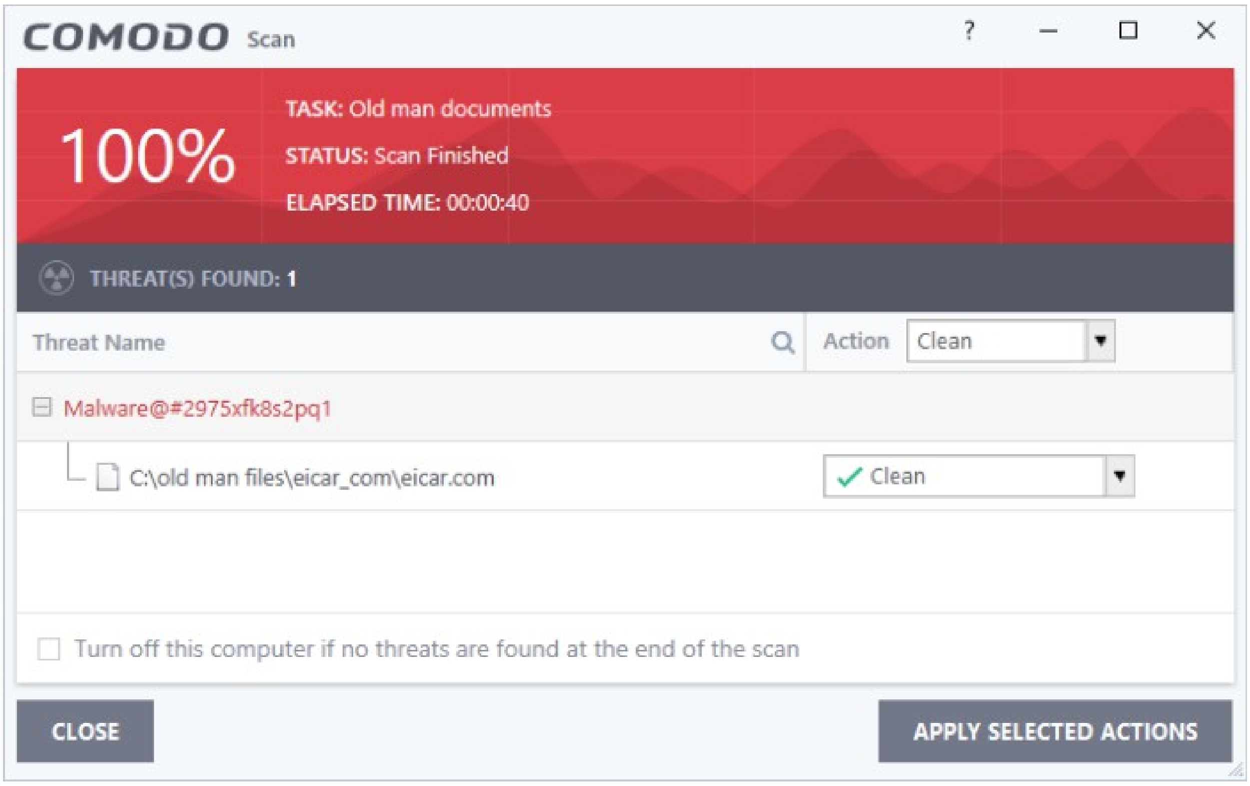


Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	off
□	Full Scan	Scan	Never	on
□	Quick Scan	Scan	Never	on
☑	Old man documents	Scan	Never	on

The scan will start immediately. Results will be displayed afterwards:



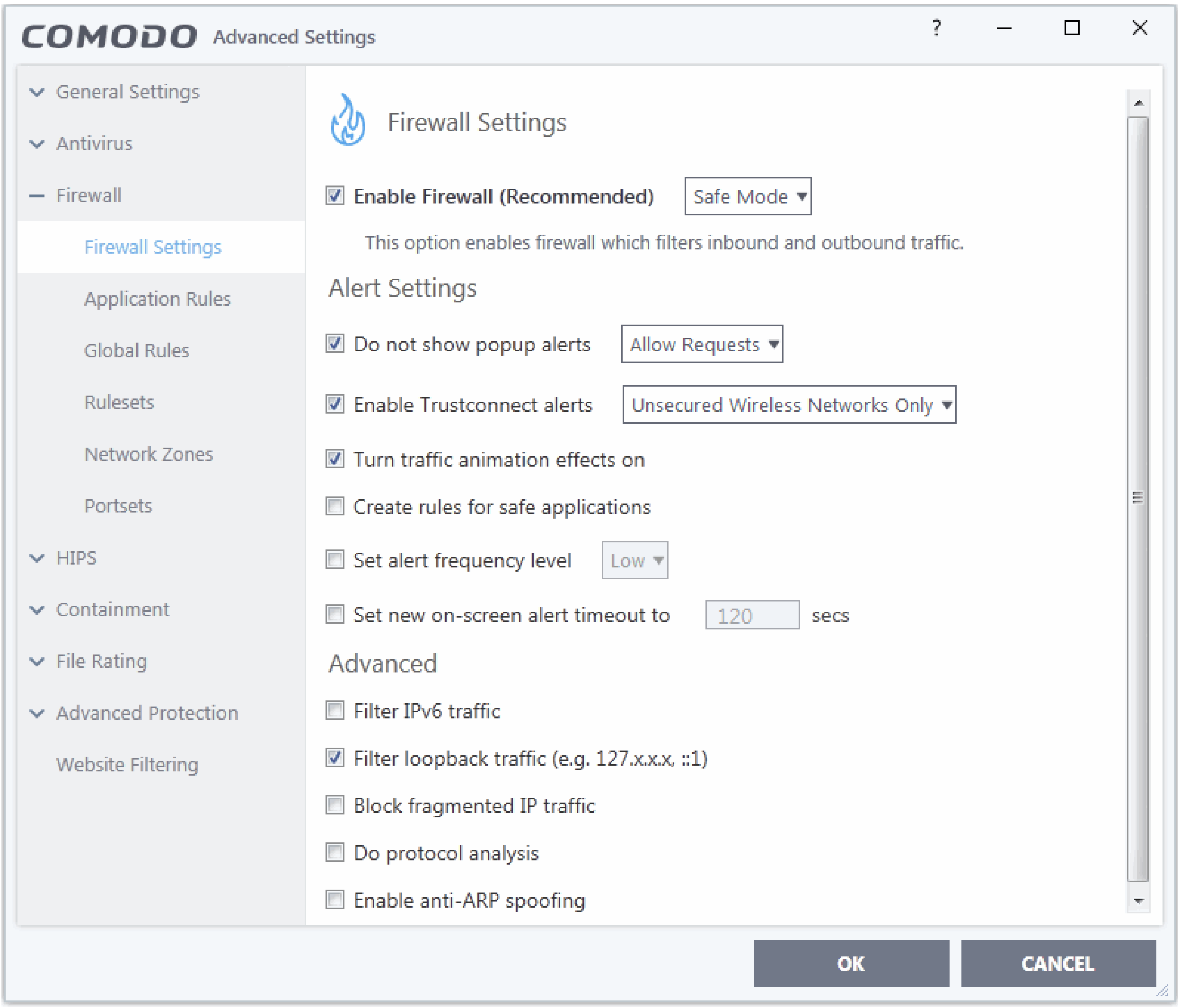
The scan results window displays the number of objects scanned and the number of threats discovered. You can choose to clean, move to quarantine or ignore the threat based on your assessment. See **Processing infected files** for more details.

6.3. Firewall Configuration

The Firewall component of Comodo Internet Security offers the highest levels of security against inbound and outbound threats. It checks that all network traffic in and out of your computer is legitimate, hides your computer ports against hackers and blocks software from transmitting your personal data over the internet. Comodo Firewall also makes it easy for you to specify exactly which applications are allowed to connect to the Internet and immediately warns you when there is suspicious activity.

To configure 'Firewall' components

- Click 'Settings' from the top left of the CIS interface
- Click 'Firewall' on the left:



Firewall Settings

☑ Enable Firewall (Recommended) — Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do not show popup alerts — Allow Requests

☑ Enable Trustconnect alerts — Unsecured Wireless Networks Only

☑ Turn traffic animation effects on

□ Create rules for safe applications

□ Set alert frequency level — Low

□ Set new on-screen alert timeout to 120 secs

Advanced

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

□ Block fragmented IP traffic

□ Do protocol analysis

□ Enable anti-ARP spoofing

Firewall settings has several sub-sections:

- **General Firewall Settings** - Configure settings that govern the overall behavior of the firewall component.
- **Application Rules** - View, create and modify rules that determine the network access privileges of individual applications or specific types of application
- **Global Rules** - View, create and modify rules that apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Predefined collections of firewall rules that can be applied, out-of-the-box, to Internet capable applications such as browsers, email clients and FTP clients.
- **Network Zones** - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Predefined groups of regularly used ports that can be used and reused when creating traffic filtering rules.

Background note on rules:

Both application rules and global rules are consulted when the firewall is determining whether to allow or block a connection attempt.

- For Outgoing connection attempts, the application rules are consulted first then the global rules.

- For Incoming connection attempts, the global rules are consulted first then application specific rules.

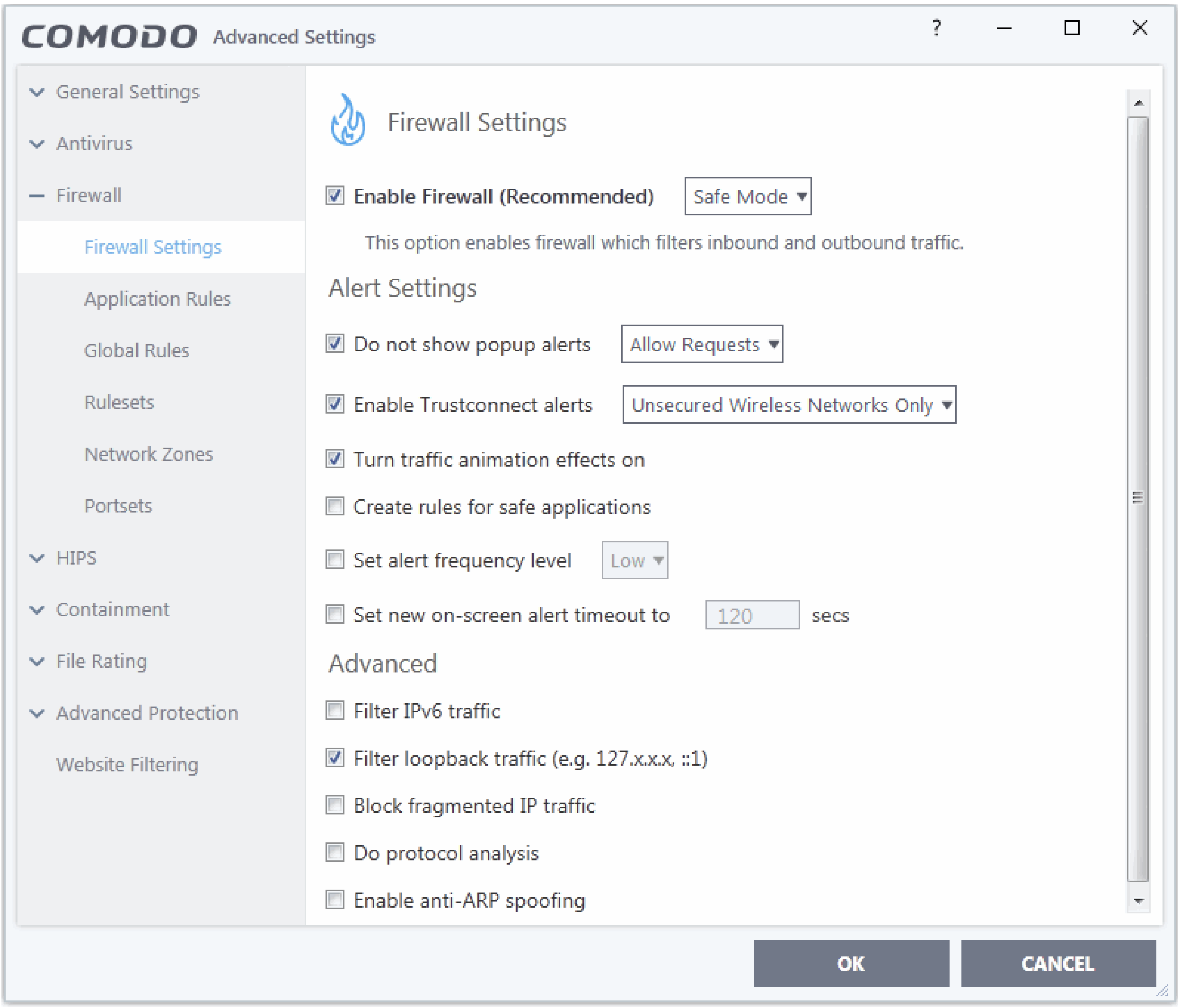
6.3.1. General Firewall Settings

Firewall Settings panel allows you to quickly configure overall Firewall settings and is divided into three main areas:

- **General Settings**
- **Alert Settings**
- **Advanced Settings**

To open the 'Firewall Settings' panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Firewall Settings' under 'Firewall' on the left



Firewall Settings

☑ Enable Firewall (Recommended) — Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do not show popup alerts — Allow Requests

☑ Enable Trustconnect alerts — Unsecured Wireless Networks Only

☑ Turn traffic animation effects on

☐ Create rules for safe applications

☐ Set alert frequency level — Low

☐ Set new on-screen alert timeout to 120 secs

Advanced

☐ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☐ Block fragmented IP traffic

☐ Do protocol analysis

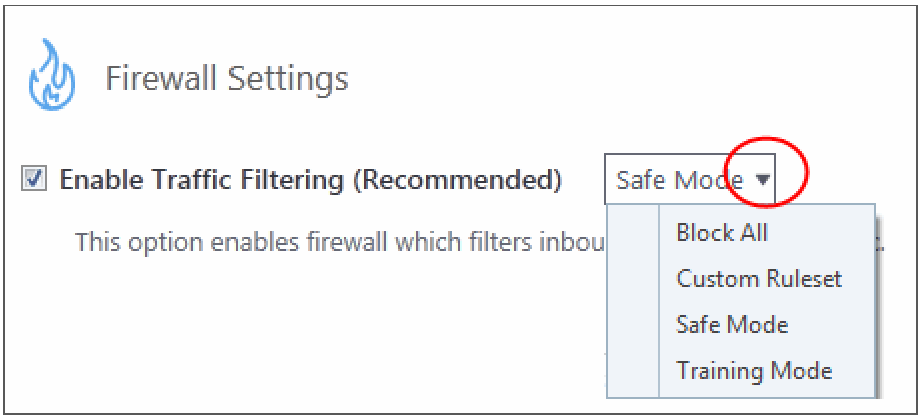
☐ Enable anti-ARP spoofing

General Settings

- **Enable Firewall** - Allows you to enable or disable Firewall protection. ***(Default and recommended =Enabled)***

> **Note**: The Firewall configuration settings can also be modified in the 'Advanced View' of the Home screen by clicking the status link beside Firewall in the Firewall pane.

If enabled, you can also choose the security level from the accompanying drop-down menu:



Firewall Settings

☑ Enable Traffic Filtering (Recommended) Safe Mode

This option enables firewall which filters inbou

The choices available are:

- **Block All:** The firewall blocks all traffic in and out of your computer regardless of any user-defined configuration and rules. The firewall does not attempt to learn the behavior of any application and does not automatically create traffic rules for any applications. Choosing this option effectively prevents your computer from accessing any networks, including the Internet.
- **Custom Ruleset Mode:** The firewall applies ONLY the custom security configurations and **network traffic rules** specified by the user. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. You will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, you have specified rules and policies that instruct the firewall to trust the application's connection attempt).

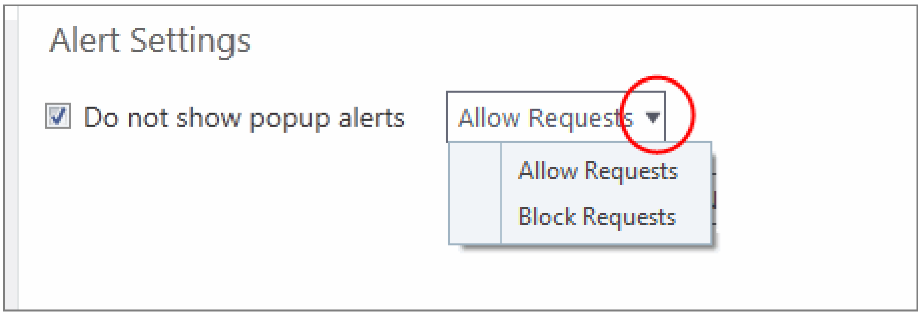
  If any application tries to make a outbound connection, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.
- **Safe Mode *(Default)***: If **Create rules for safe applications** is enabled then the firewall automatically creates rules to allow traffic by applications certified as 'Safe' by Comodo. For new, unknown applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This deploys the **predefined firewall ruleset** 'Trusted Application' onto the application.

  'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.
- **Training Mode** : The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the **correct network access rights**.

Alert Settings

- **Do not show popup alerts** - Configure whether or not you want to be notified when the firewall encounters a request for network access. Choosing 'Do not show pop up alerts' will minimize disturbances but at some loss of user awareness. ***(Default = Enabled)***

  If you choose this option then you have a choice of default responses that CIS should take - either 'Block Requests' or 'Allow Requests'.

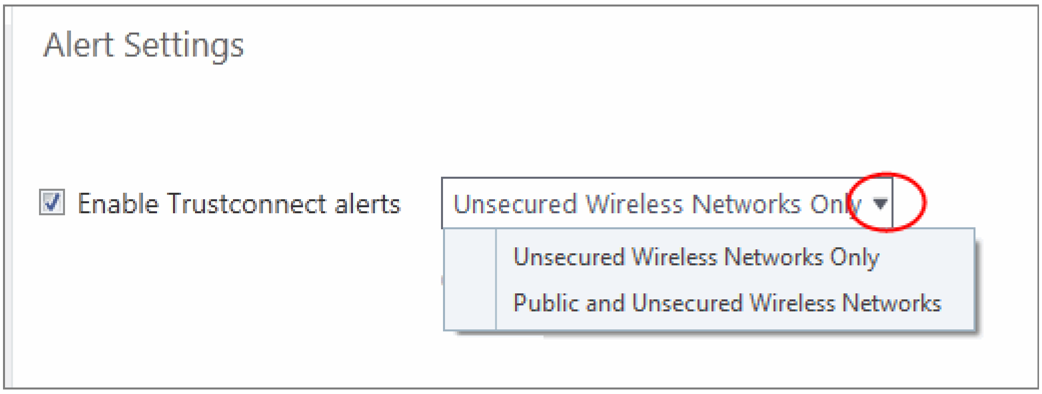


Alert Settings

☑ Do not show popup alerts

- **Enable Trustconnect alerts -** If you are connecting to Internet at a public place like an airport or a coffee shop then you are potentially exposing yourself to danger. Unsecured public networks can allow other people to easily eavesdrop on your communications or even gain access to your computer to steal your confidential information. In order to safeguard against such attempts, Comodo recommends you encrypt your connection in public hotspots using TrustConnect - a secure Internet proxy service.

  If selected, Comodo Firewall will display an alert if it detects you are connected to the Internet through an unsecured network ***(Default=Enabled)***.The drop-down options allow you to select the conditions under which you want alerts to be displayed:



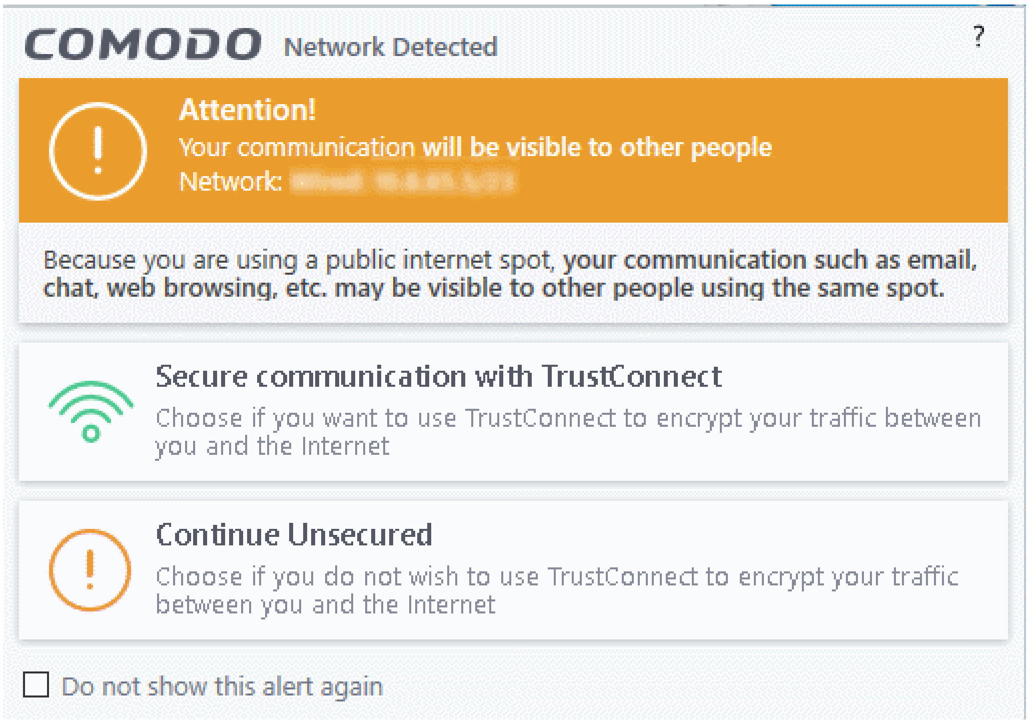
Alert Settings

☑ Enable Trustconnect alerts

Unsecured Wireless Networks Only ▾
Unsecured Wireless Networks Only
Public and Unsecured Wireless Networks

  - **Unsecured Wireless Networks Only -** TrustConnect alerts are displayed only if you are connecting to an unencrypted wireless network. ***(Default)***
  - **Public and Unsecured Wireless Networks only -** TrustConnect alerts are displayed whenever you connect to a public wireless network irrespective of whether the connection is encrypted

You will be alerted and offered the opportunity to secure the connection via the following notification:



COMODO Network Detected ?

Attention!
Your communication will be visible to other people
Network: [redacted]

Because you are using a public internet spot, your communication such as email, chat, web browsing, etc. may be visible to other people using the same spot.

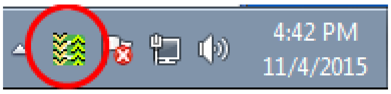
Secure communication with TrustConnect
Choose if you want to use TrustConnect to encrypt your traffic between you and the Internet

Continue Unsecured
Choose if you do not wish to use TrustConnect to encrypt your traffic between you and the Internet

□ Do not show this alert again

Note: TrustConnect is available as a standard feature only with CIS Complete. On clicking 'Secure communication with TrustConnect', the users of Comodo Internet Security and CIS Pro will be taken to the product upgrade page, enabling them to upgrade their product. See **TrustConnect Overview**, for more details.

- **Turn traffic animation effects on** - By default, the Comodo Internet Security's tray icon displays a small animation whenever traffic moves to or from your computer.

  If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the icon. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer. Clear this check box If you would rather not see this animation ***(Default = Enabled)***.

- **Create rules for safe applications** - Comodo Firewall trusts the applications if:

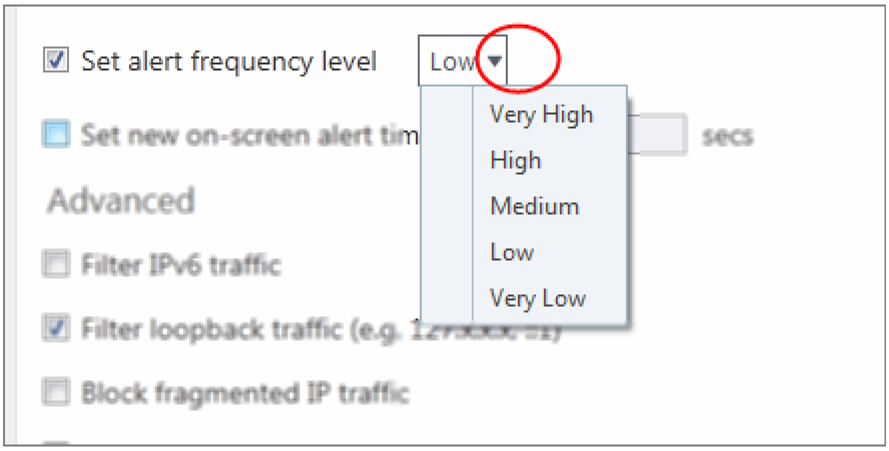
  - The application/file is included in the Trusted Files list under File Rating Settings;
  - The application is from a vendor included in the **Trusted Software Vendors** list under File Rating Settings;
  - The application is included in the extensive and constantly updated Comodo safelist.

  By default, CIS does not automatically create 'allow' rules for safe applications. This helps to lower resource usage and simplifies the rules interface. It also reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

  Enabling this checkbox instructs CIS to begin learning the behavior of safe applications so that it can automatically generate 'Allow' rules. These rules are listed in the **Application Rules** interface. Advanced users can edit/modify the rules as they wish ***(Default = Disabled).***

Background Note: Prior to version 4.x, CIS would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CIS version 3.x).

- **Set alert Frequency level** - Allows you to configure the amount of alerts that Comodo Firewall generates. Please note that this does not affect your security levels, which is determined by the rules you have configured (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages. ***(Default=Disabled)***



☑ Set alert frequency level Low ▾

☐ Set new on-screen alert tim secs

Advanced

☐ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☐ Block fragmented IP traffic

The options available are:

- **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.
- **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.
- **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.
- **Low:** The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.
- **Very Low**: The firewall shows only one alert for an application.

The alert frequency settings refer only to connection attempts by applications or from IP addresses that you do not trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.

- **Set new on-screen alert time out to**: Determines how long the Firewall shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced Settings

Advanced detection settings help protect your computer against common types of denial of service (DoS) attack. When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server.

- **Filter IP v6 traffic** - If enabled, CIS will filter IPv6 network traffic in addition to IPv4 traffic.(***Default = Disabled***).

Background Note: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available. This hard limit has already led to the development of 'work-around' solutions such as Network Address Translation (NAT), which enable multiple hosts on private networks to access the Internet using a single IP address.

IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

- **Filter loopback traffic**: Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately received by it. This involves no connection outside your computer to the internet or a local network. The IP address of the loopback network is 127.0.0.1, which you might have heard referred to by its domain name of '**http://localhost**'. This is the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this option enabled means the firewall will filter traffic sent through this channel. (***Default = Enabled***).
- **Block fragmented IP traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using. When a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, fragmentation can double the amount of time it takes to send a single packet and slow down your download time (***Default = Disabled***).
- **Do protocol analysis** - Protocol Analysis is key to the detection of fake packets used in denial of service attacks. Enabling this option means Comodo Firewall checks that every packet on whether it conforms to its protocols standards. If not, then the packets are blocked (***Default = Disabled***).
- **Enable anti-ARP spoofing** - A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update your machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in a machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update your ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in your home network. Enabling this setting helps to block such requests - protecting the ARP cache from potentially malicious updates ***(Default = Disabled).***
- Click 'OK' for your settings to take effect.

6.3.2. Application Rules

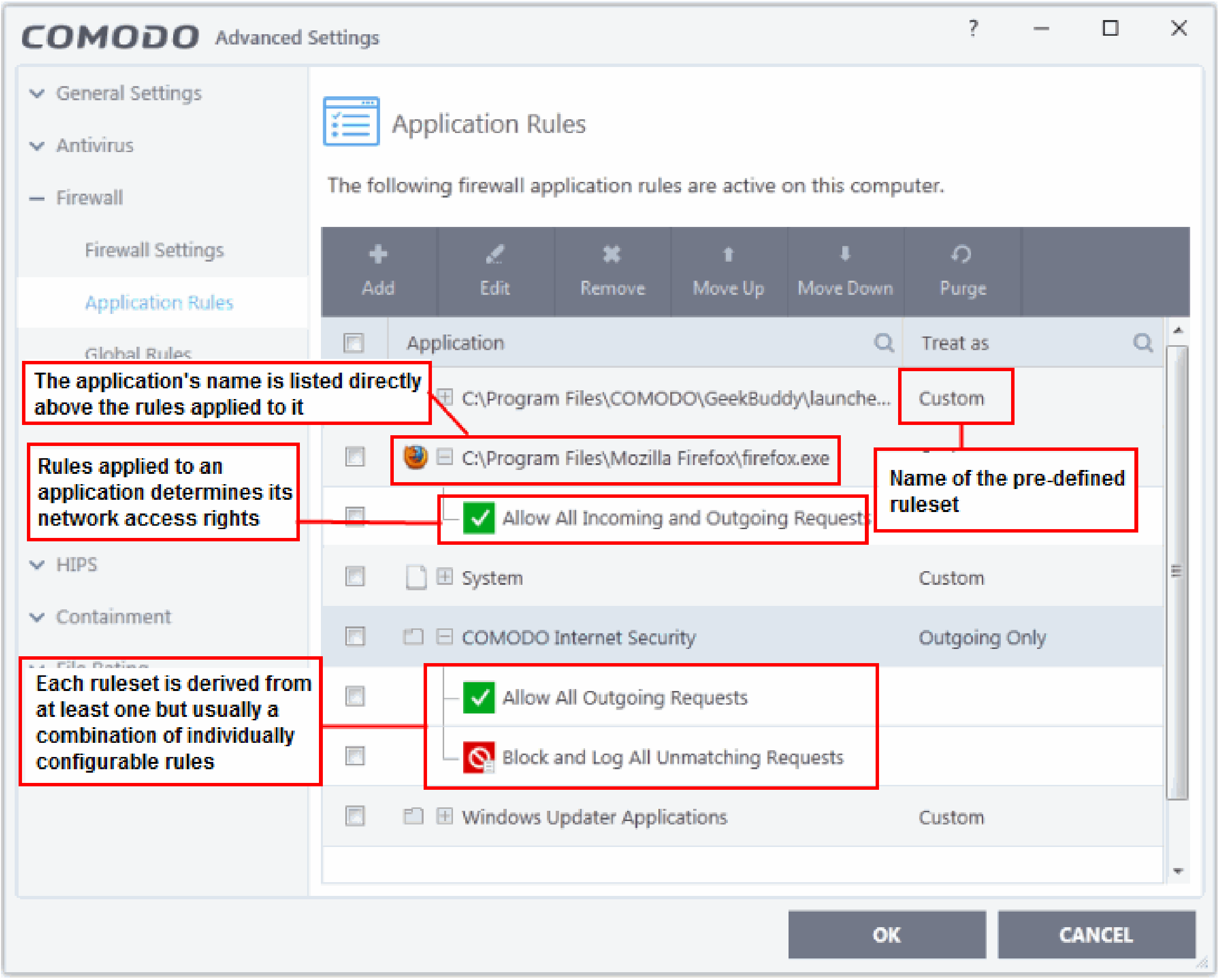
Overview of Rules and Rulesets

- Whenever an application makes a request for internet or network access, CIS will allow or deny this request based upon the 'Firewall Ruleset' that has been specified for that application.
- Firewall rulesets are made up of one or more application rules.
- Each application rule contains instructions that determine whether the application should be allowed or blocked; which protocols or ports it is allowed to use and so on.

Application rules are configured in the application rules panel.

To open the Application Rules panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Application Rules' under 'Firewall' on the left.



The following firewall application rules are active on this computer.

Application	Treat as
C:\Program Files\COMODO\GeekBuddy\launche...	Custom
C:\Program Files\Mozilla Firefox\firefox.exe	
✓ Allow All Incoming and Outgoing Requests	
System	Custom
COMODO Internet Security	Outgoing Only
✓ Allow All Outgoing Requests	
Block and Log All Unmatching Requests	
Windows Updater Applications	Custom

The application's name is listed directly above the rules applied to it

Rules applied to an application determines its network access rights

Each ruleset is derived from at least one but usually a combination of individually configurable rules

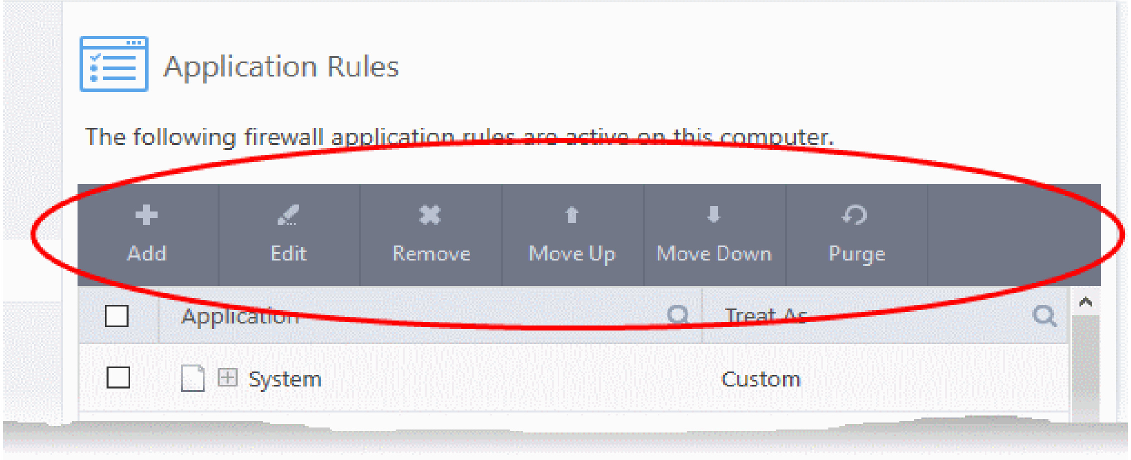
Name of the pre-defined ruleset

- The first column, **Application**, displays a list of applications for which a firewall ruleset has been created. If the application belongs to a file group, then all member applications assume the ruleset of the file group.
- The second column, **Treat as**, displays the name of the ruleset assigned to the application or group
- Click '+' at the left of the application name to view the individual rules contained in a ruleset

You can use the search option to find a specific name in the list by clicking the search icon at the far right of the column header and entering the application name in full or part.

General Navigation:

The control buttons at the top of the list enable you to create and manage application rule sets.



- **Add -** Add a new Application to the list then create a ruleset for it. See '**Creating or Modifying Firewall Rules**' and '**Adding and Editing a Firewall Control Rule**'.
- **Edit -** Allows you to modify the firewall rule or ruleset of the selected application. See '**Creating or Modifying Firewall Rules**' and '**Adding and Editing a Firewall Rule**', for more details.
- **Remove -** Deletes the selected ruleset.
- **Purge -** Runs a check to verify that all applications mentioned in a ruleset are actually installed at the paths specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down -** Rules are prioritized top-to-bottom, with rules at the top of the list having highest priority. The 'Move Up' and 'Move Down' buttons enable you to change the priority of a selected rule.

If you wish to modify the **firewall ruleset** for an application:

- Double click on the application name to begin **'Creating or Modifying Firewall Rules'**

Or

- Select the application name and choose 'Edit' from the options to begin '**Creating or Modifying Firewall Rules'**

If you wish to modify an **individual rule** within the ruleset:

- Double click on the specific rule to begin '**Adding and Editing a Firewall Rule**'

Or

- Select the specific rule and choose 'Edit' at the top to begin 'Adding and Editing a Firewall Rule'

Users can also re-prioritize rulesets by moving them up or down, by selecting them and clicking the 'Move Up' or 'Move Down' buttons.

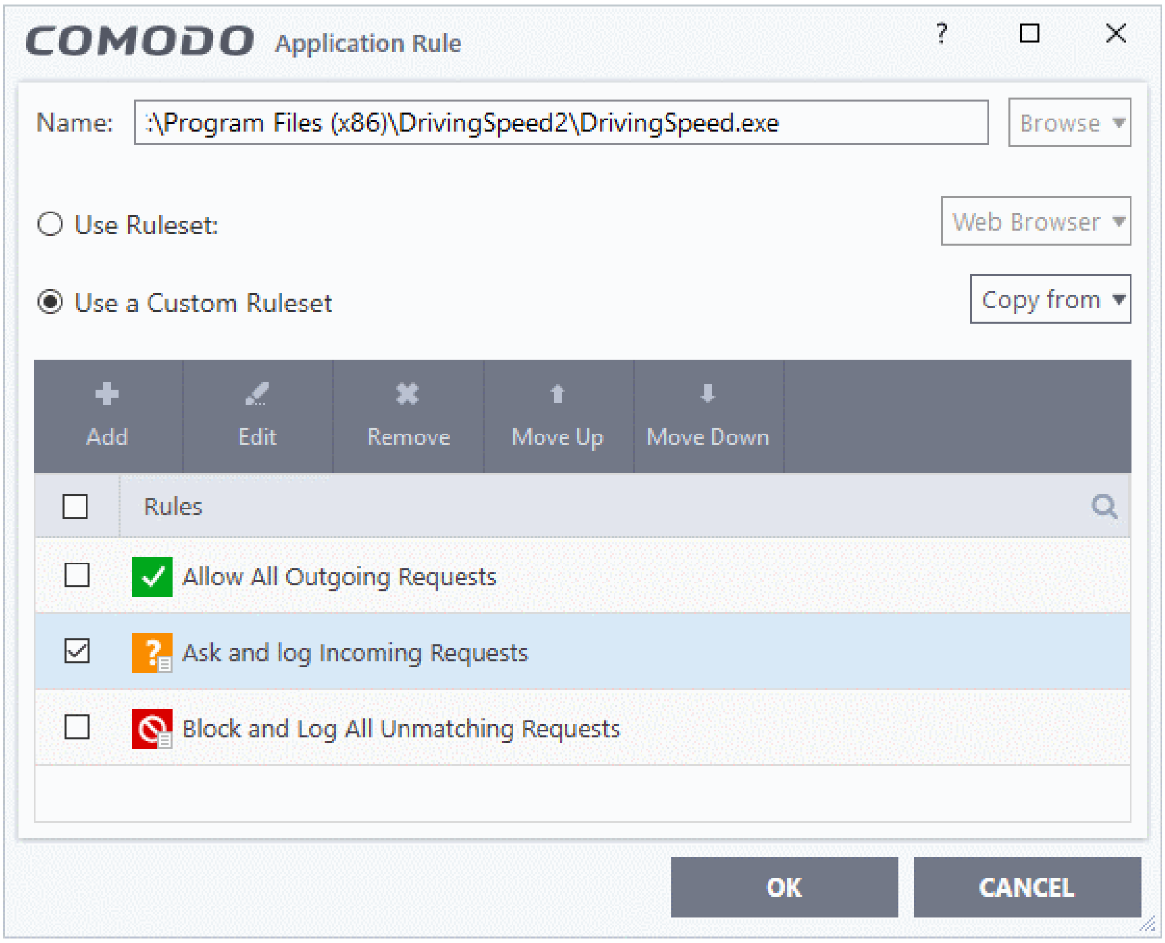
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. See **Predefined Rule Sets,** for more details.

- See **Application Rule interface** for an introduction to the rule setting interface
- See **Creating and Modifying Firewall Rulesets** to learn how to create and edit Firewall rulesets
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration

Application Rule interface

Firewall rules can be added/modified/removed and re-ordered through the Application Rule interface. Any rules created using Adding and Editing a Firewall Rule is displayed in this list.

The Application Rule interface is displayed when you click 'Add' or 'Edit' from the options in 'Application Rules' interface.



COMODO Application Rule

Name: :\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

○ Use Ruleset: Web Browser

● Use a Custom Ruleset Copy from

	Rules
☐	✓ Allow All Outgoing Requests
☑	? Ask and log Incoming Requests
☐	Block and Log All Unmatching Requests

Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see Understanding Firewall Rules for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied.

Users can also re-prioritize rulesets by uisng the 'Move Up' or 'Move Down' buttons. To begin creating Firewall rulesets, first read 'Overview of Rules and Rulesets' then 'Creating and Modifying Firewall Rulesets

You can search for specific rules by clicking the search icon in the 'Rules' column header and entering the name of the item.

Creating and Modifying Firewall Rulesets

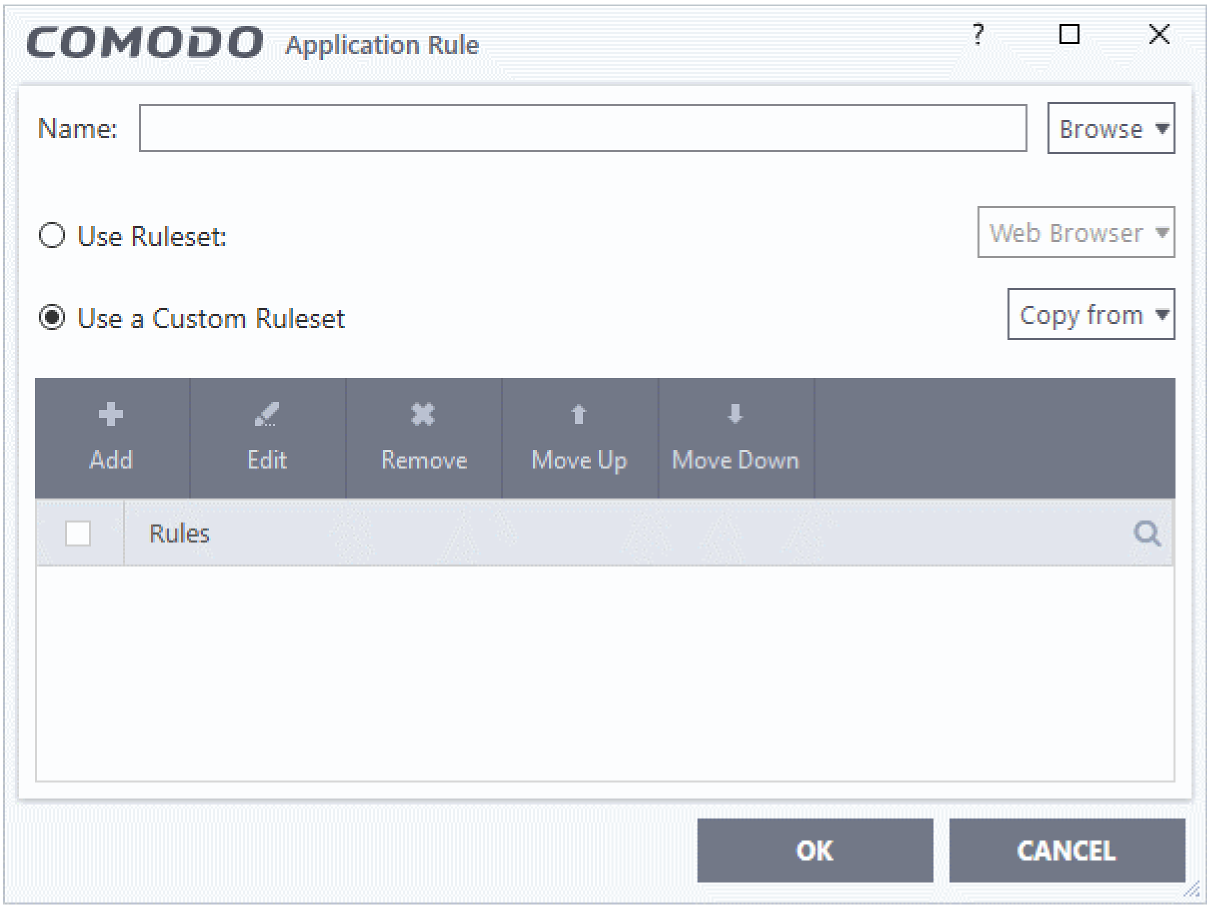
To begin defining an application's Firewall ruleset, you need take two basic steps.

- Step 1 - Select the application that you wish the ruleset is to be applied.
- Step 2 - Configure the rules for this application's ruleset.

Step 1 - Select the application to which you want to apply the ruleset

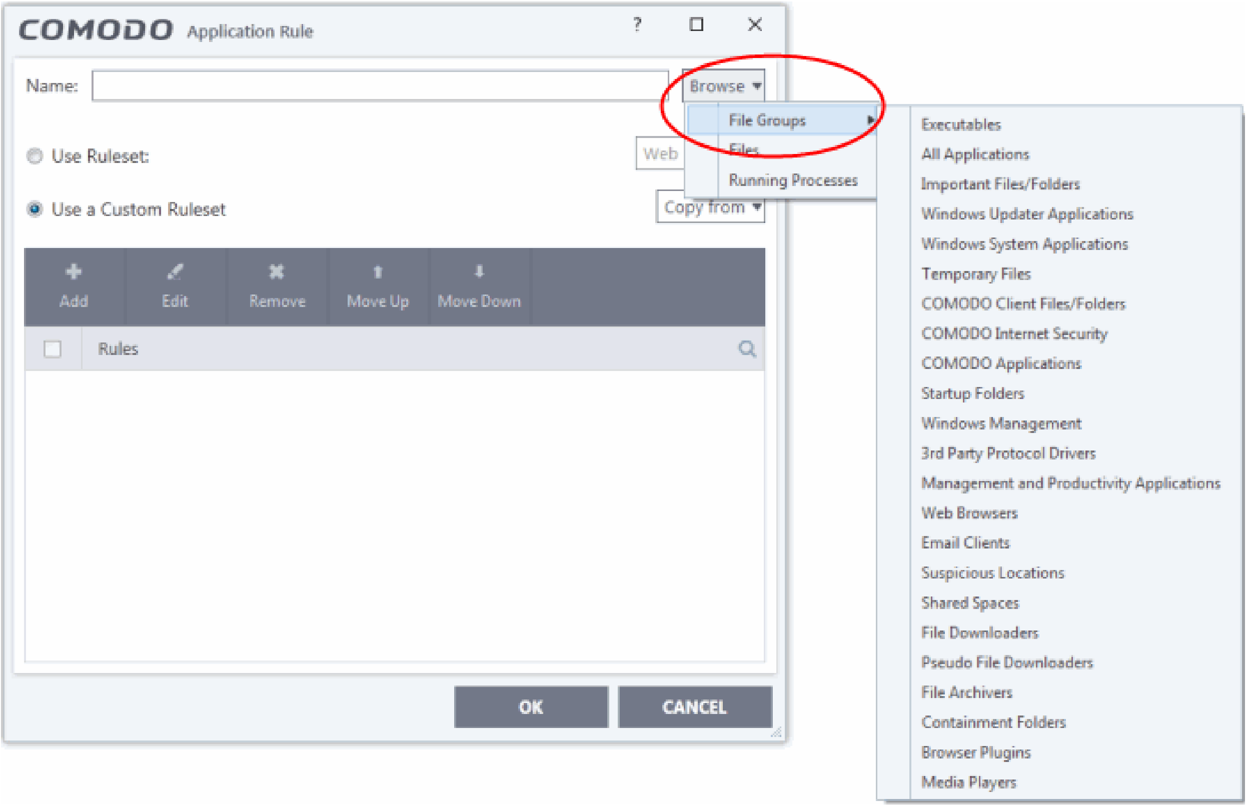
- To define a ruleset for a new application (i.e. one that is not already listed), click the 'Add' button at the top of the list in the Application Rules interface.

The 'Application Rules' interface will open as shown below:



Because this is a new application, the 'Application Path' field is blank. If you are modifying an existing ruleset then the individual rules will be shown.

- Click 'Browse' button beside the 'Name' text box to choose the application file to which this rule set is to be applied.

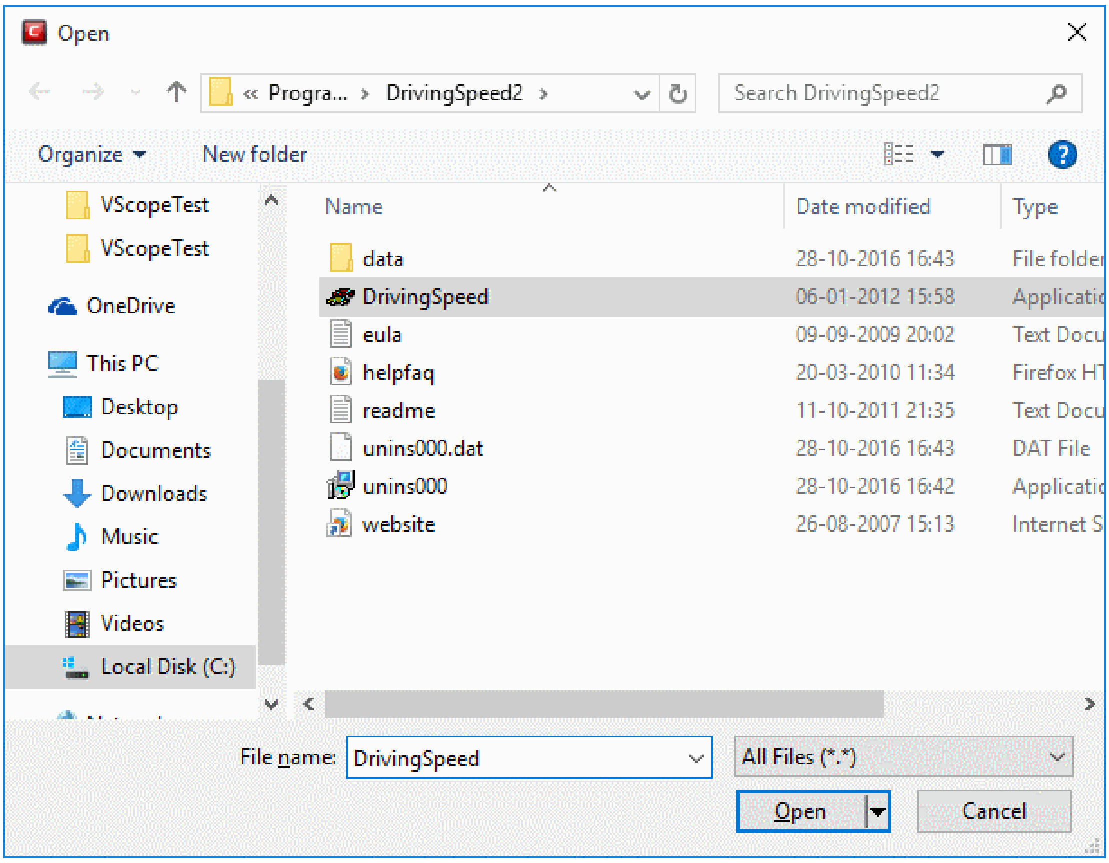


You now have 3 methods available to choose the application for which you wish to create a ruleset - **File Groups**; **Files** and **Running Processes** and

i. **File Groups -** Allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe, *.bat, *.cmd. Other such categories available include 'Windows System Applications' , 'Windows Updater Applications', 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

   CIS ships with a set of pre-defined file groups and also allows you to create your own file groups. You can view and manage the file groups from the 'File Groups' interface accessible from the 'Advanced Settings' interface by clicking 'File Rating' > 'File Groups'. See **File Groups**, for more details on file groups.

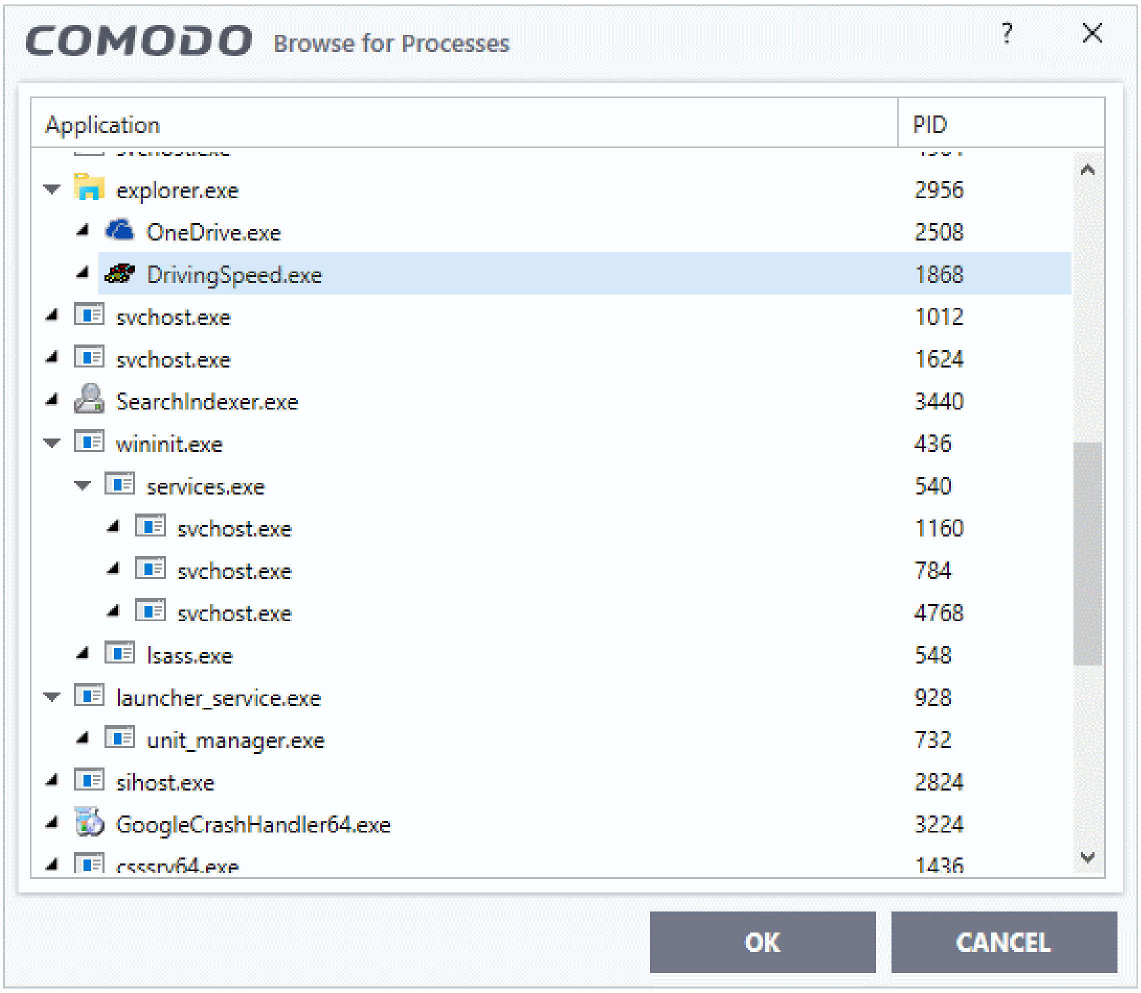
ii. **Files -** this option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the firewall ruleset. In the example shown below, Opera web browser is selected for creating a firewall ruleset.



Name	Date modified	Type
data	28-10-2016 16:43	File folder
DrivingSpeed	06-01-2012 15:58	Applicati
eula	09-09-2009 20:02	Text Docu
helpfaq	20-03-2010 11:34	Firefox HT
readme	11-10-2011 21:35	Text Docu
unins000.dat	28-10-2016 16:43	DAT File
unins000	28-10-2016 16:42	Applicati
website	26-08-2007 15:13	Internet S

File name: DrivingSpeed

iii. **Running Processes -** Displays list of currently running processes in your computer. You can select the process, for whose target application, you wish to deploy a firewall rule.



Application	PID
explorer.exe	2956
OneDrive.exe	2508
DrivingSpeed.exe	1868
svchost.exe	1012
svchost.exe	1624
SearchIndexer.exe	3440
wininit.exe	436
services.exe	540
svchost.exe	1160
svchost.exe	784
svchost.exe	4768
lsass.exe	548
launcher_service.exe	928
unit_manager.exe	732
sihost.exe	2824
GoogleCrashHandler64.exe	3224
csssrv64.exe	1436

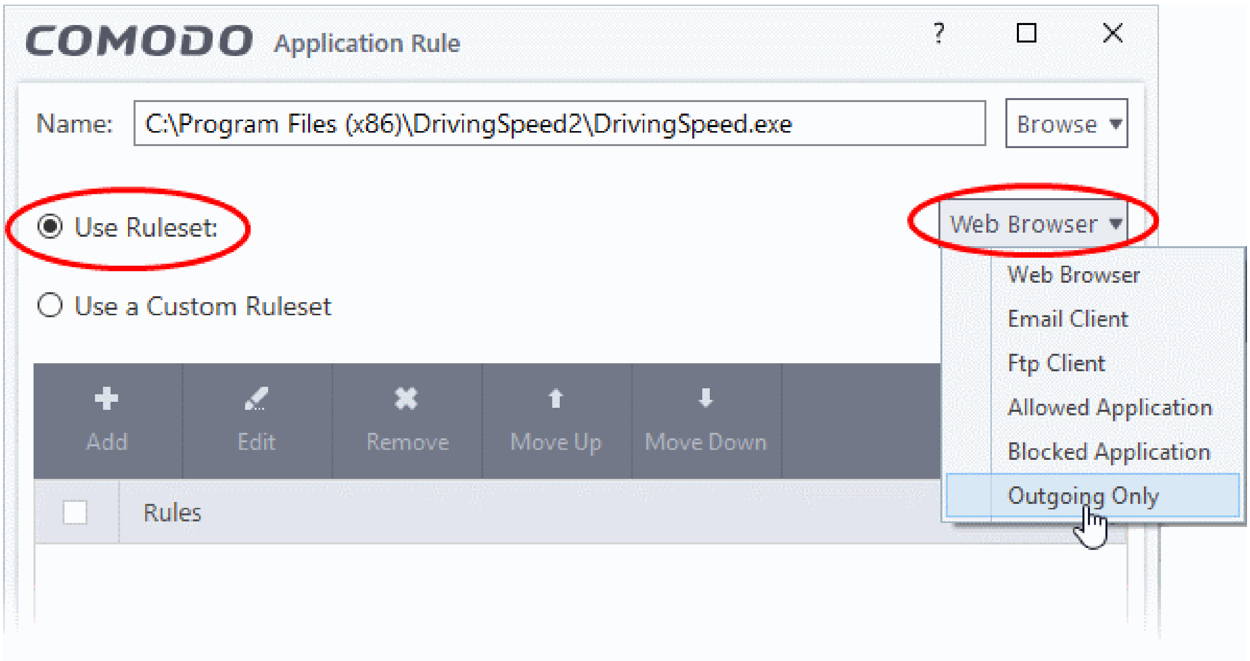
You can choose an individual process or the parent process of a set of running processes. Click 'OK' to confirm your choice.

Having selected the individual application, running process or file group, the next stage is to Configure the rules for this application's Firewall Ruleset.

Step 2 - Configure the rules for this application's ruleset

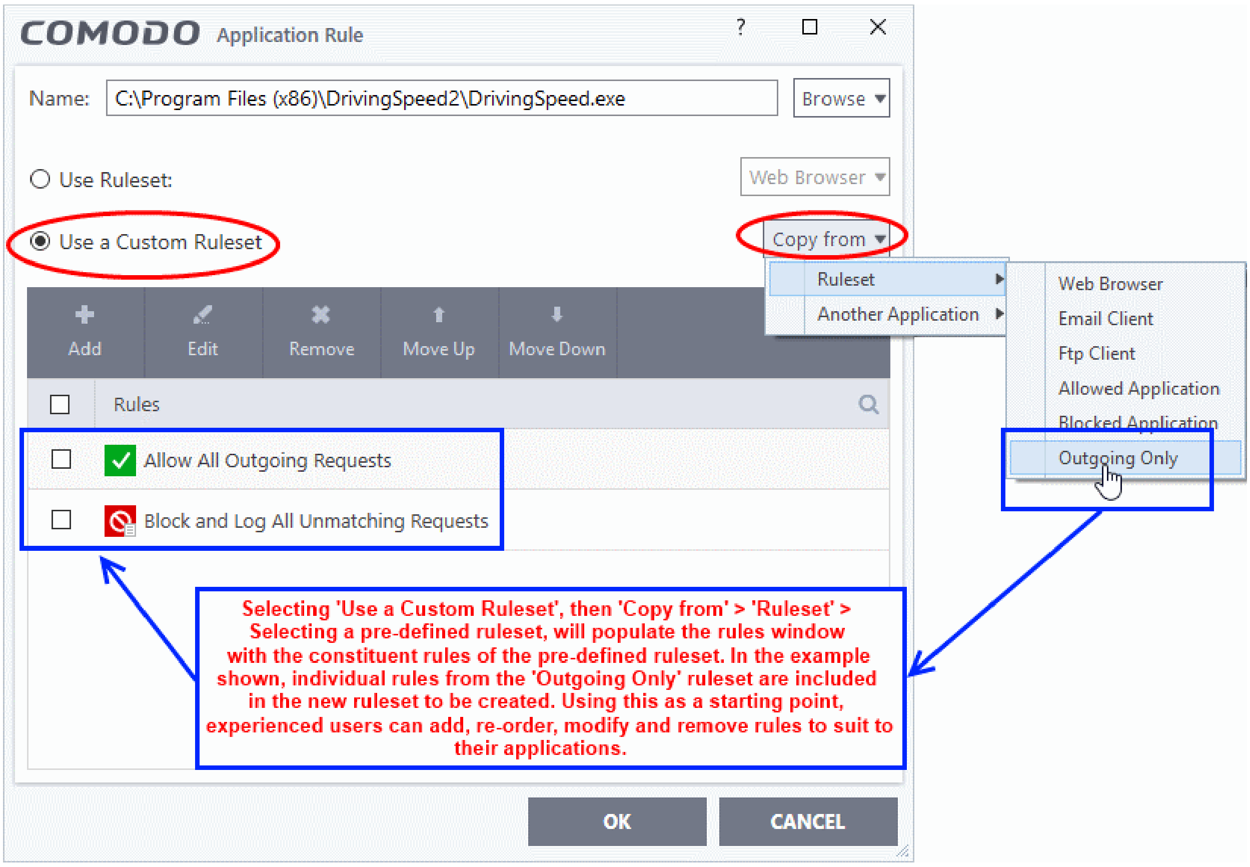
There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset** - Allows you to quickly deploy an existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Opera' browser. The name of the predefined ruleset you choose is displayed in the **Treat As** column for that application in the **interface** ***(Default = Disabled).***



Note: Predefined Rulesets, once chosen, cannot be modified ***directly*** from this interface - they can only be modified and defined using the **Rulesets** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - designed for more experienced users, the **Custom Ruleset** option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset ***(Default = Enabled)***.



Selecting 'Use a Custom Ruleset', then 'Copy from' > 'Ruleset' > Selecting a pre-defined ruleset, will populate the rules window with the constituent rules of the pre-defined ruleset. In the example shown, individual rules from the 'Outgoing Only' ruleset are included in the new ruleset to be created. Using this as a starting point, experienced users can add, re-order, modify and remove rules to suit to their applications.

You can create an entirely new ruleset or use a predefined ruleset as a starting point by:

- Clicking 'Add' from the top to add individual Firewall rules. See '**Adding and Editing a Firewall Rule**' for an overview of the process.
- Use the 'Copy From' button to populate the list with the Firewall rules of a **Predefined Firewall Rule.**
- Use the 'Copy From' button to populate the list with the Firewall rules of another application's ruleset.

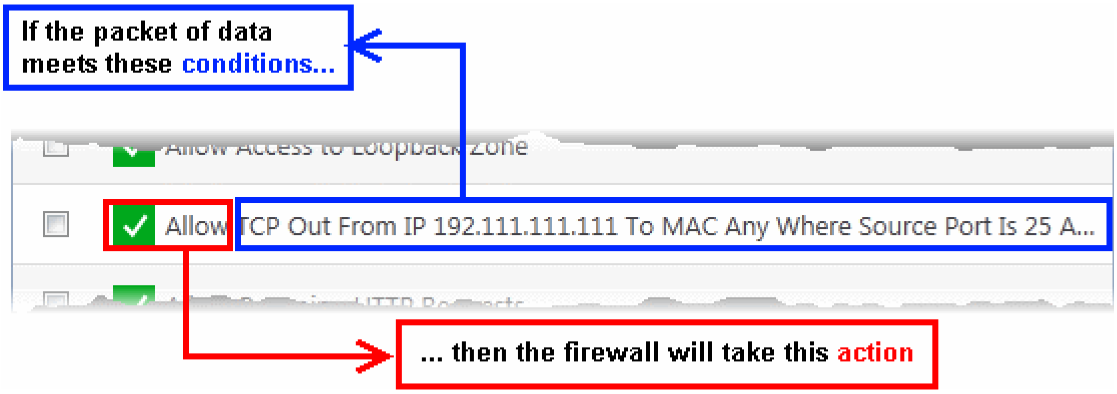
General Tips:

- If you wish to create a reusable ruleset for deployment on multiple applications, we advise you add a new **Predefined Firewall Rules** (or modify one of the existing ones to suit your needs) - then come back to this section and use the '**Ruleset**' option to roll it out.
- If you want to build a bespoke ruleset for maybe one or two specific applications, then we advise you choose the '**Use a Custom Ruleset**' option and create your ruleset either from scratch by adding individual rules or by using one of the built-in rulesets as a starting point.

Understanding Firewall Rules

At their core, each Firewall rule can be thought of as a simple **IF THEN** trigger - a set of **conditions** (or attributes) pertaining to a packet of data from a particular application and an **action** it that is enforced if those conditions are met.

As a packet filtering firewall, Comodo Firewall analyzes the attributes of *every single* packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a Firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding Firewall rule, then the connection is automatically blocked until a rule is created.


If the packet of data meets these conditions...
Allow Access to Loopback Zone
Allow TCP Out From IP 192.111.111.111 To MAC Any Where Source Port Is 25 A...
... then the firewall will take this action

The actual **conditions** (attributes) you see * on a particular Firewall Rule are determined by the protocol chosen in **Adding and Editing a Firewall Rule**

If you chose 'TCP' , 'UDP' or 'TCP and 'UDP', then the rule has the form: **Action** |**Protocol** | **Direction** |**Source Address** | **Destination Address** | **Source Port** | **Destination Port**

If you chose 'ICMP', then the rule has the form: **Action** |**Protocol** | **Direction** | **Source Address** | **Destination Address** | **ICMP Details**

If you chose 'IP', then the rule has the form: **Action** | **Protocol** | **Direction** | **Source Address** | **Destination Address** | **IP Details**

- **Action**: The action the firewall takes when the conditions of the rule are met. The rule shows '**Allow**', '**Block**' or '**Ask**'.**

- **Protocol**: States the protocol that the target application must be attempting to use when sending or receiving packets of data. The rule shows '**TCP**', '**UDP**', '**TCP** or **UDP**', '**ICMP**' or '**IP**'
- **Direction**: States the direction of traffic that the data packet must be attempting to negotiate. The rule shows '**In**', '**Out**' or '**In/Out**'
- **Source Address**: States the source address of the connection attempt. The rule shows '**From**' followed by one of the following: **IP** , **IP range**, **IP Mask** , **Network Zone**, **Host Name** or **Mac Address**
- **Destination Address**: States the address of the connection attempt. The rule shows '**To**' followed by one of the following: **IP**, **IP range**, **IP Mask**, **Network Zone**, **Host Name** or **Mac Address**
- **Source Port**: States the port(s) that the application must be attempting to send packets of data through. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **Destination Port**: States the port(s) on the remote entity that the application must be attempting to send to. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **ICMP Details**: States the ICMP message that must be detected to trigger the action. See **Adding and Editing a Firewall Rule** for details of available messages that can be displayed.
- **IP Details**: States the type of IP protocol that must be detected to trigger the action: See **Adding and Editing a Firewall Rule** to see the list of available IP protocols that can be displayed here.

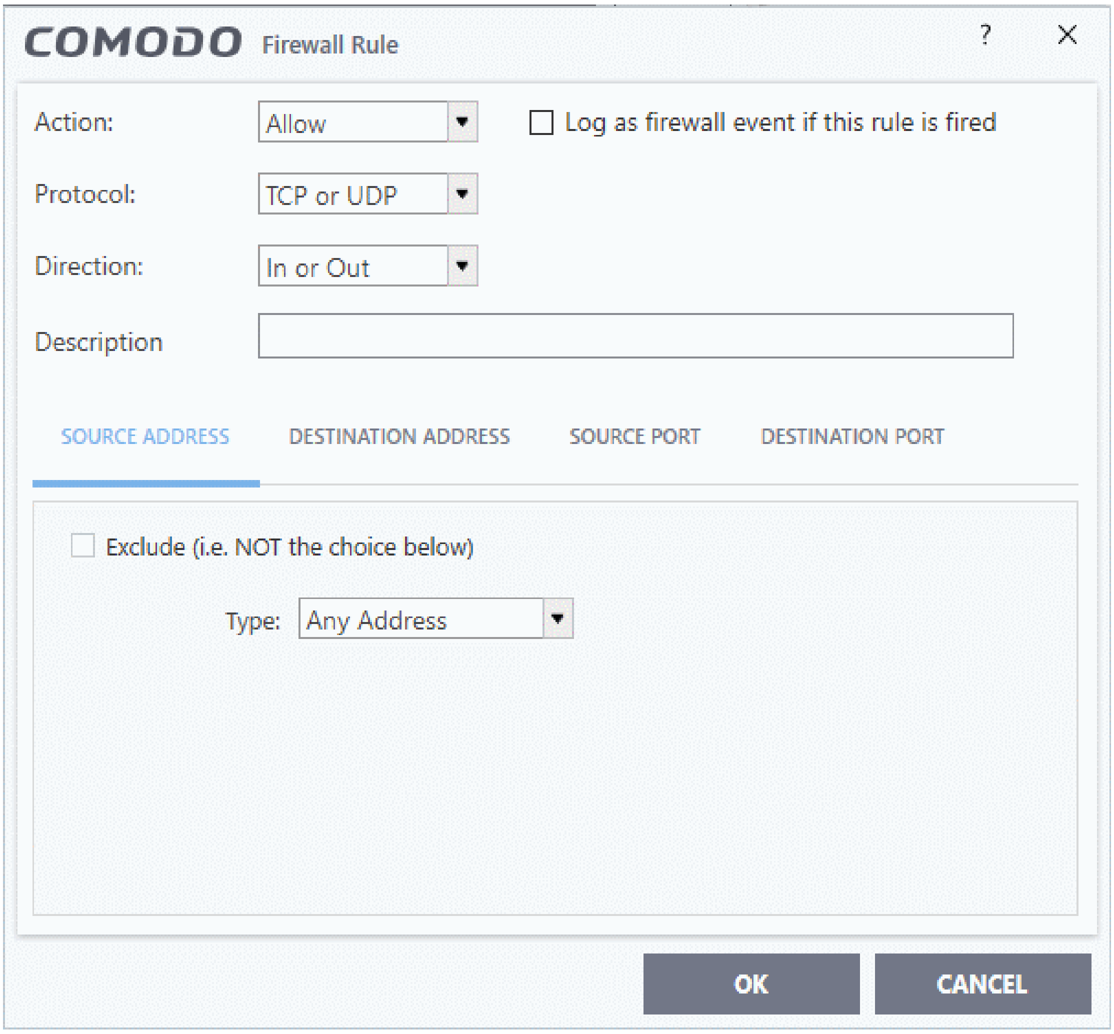
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. See '**Global Rules**' to understand the interaction between Application Rules and Global Rules.

* If you chose to add a descriptive name when creating the rule the*n this name is displayed here rather than it's full parameters. See the next section, '**Adding and Editing a Firewall Rule**', for more details.*

*** If you selected 'Log as a firewall event if this rule is fired' then the action is postfixed with 'Log'. (e.g. Block & Log)*

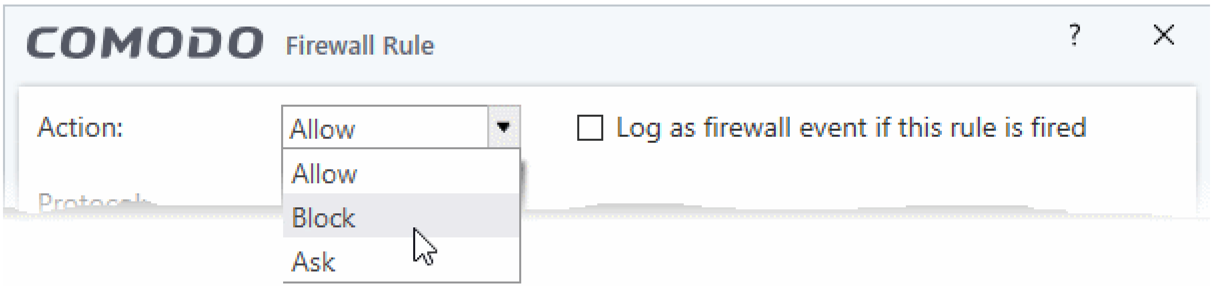
Adding and Editing a Firewall Rule

The Firewall Rule Interface is used to configure the actions and conditions of an individual Firewall rule. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading the sections '**Understanding Firewall Rules**', '**Overview of Rules and Policies**' and '**Creating and Modifying Firewall Rulesets**'.



General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' ***(Default)***, '**Block'** or '**Ask**'.



- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' ***(Default)***, '**ICMP**' or '**IP**' .

Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

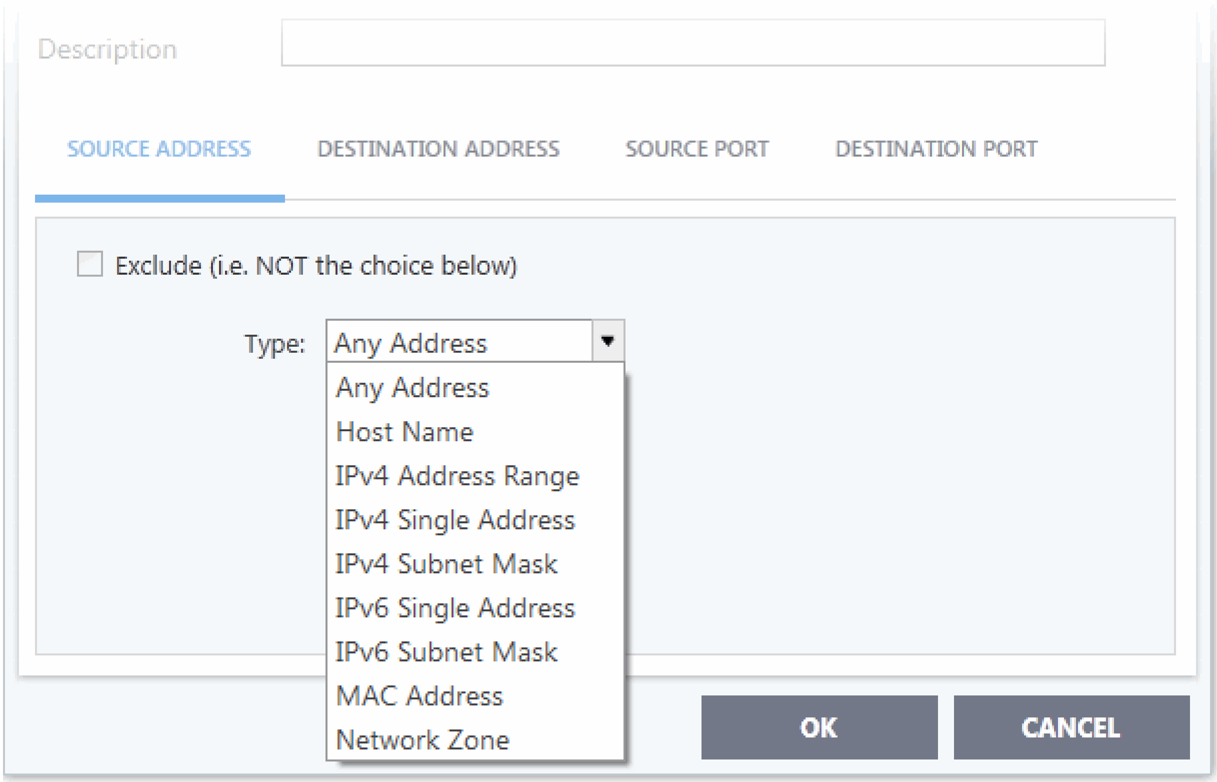
- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the **firewall event log viewer** whenever this rule is called into operation. (i.e. when ALL conditions have been met) ***(Default = Disabled).***

- **Description**: Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is displayed to represent instead of the full actions/conditions in the main **Application Rules interface** and the **Application Rule interface**.

Protocol

i. **TCP**', '**UPD**' or '**TCP or UDP**'

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information.



Source Address and Destination Address:

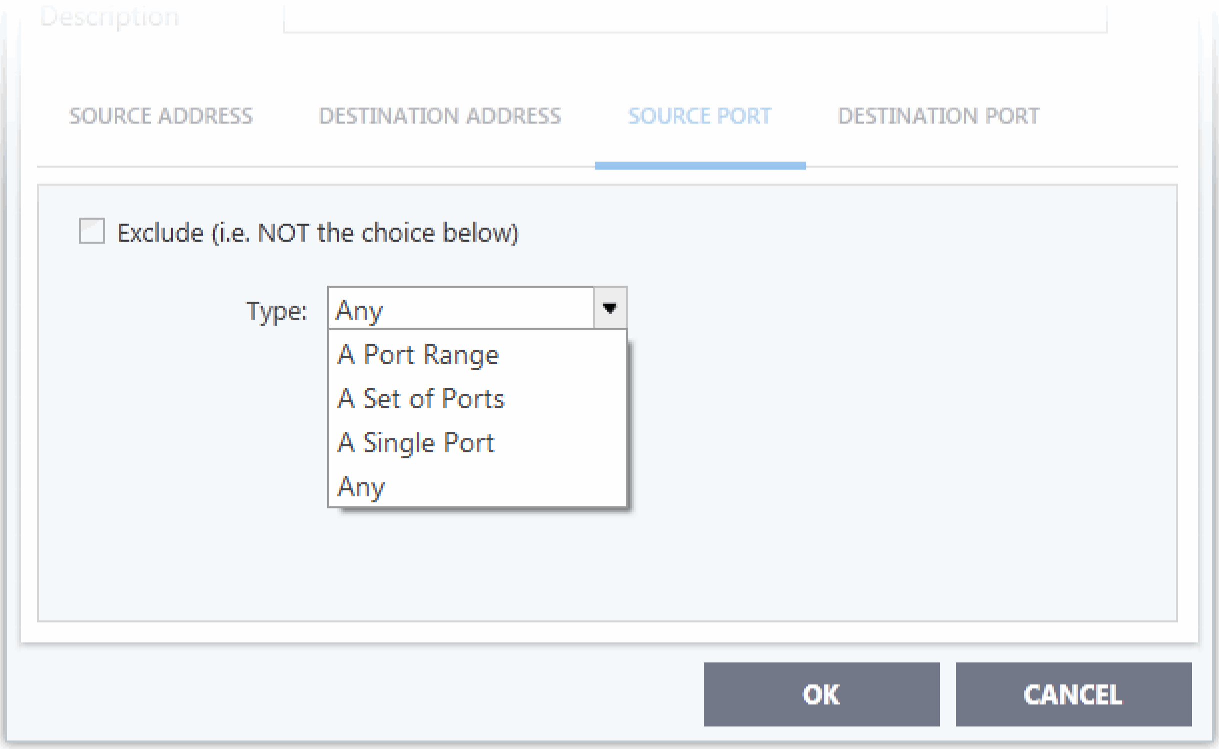
1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.



□ Exclude (i.e. NOT the choice below)

Type: Any

A Port Range
A Set of Ports
A Single Port
Any

1. You can choose any port number by selecting Any - set by default, 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a predefined **Port Set** by choosing A Set of Ports. If you wish to create a custom port set then please see the section '**Port Sets**'.

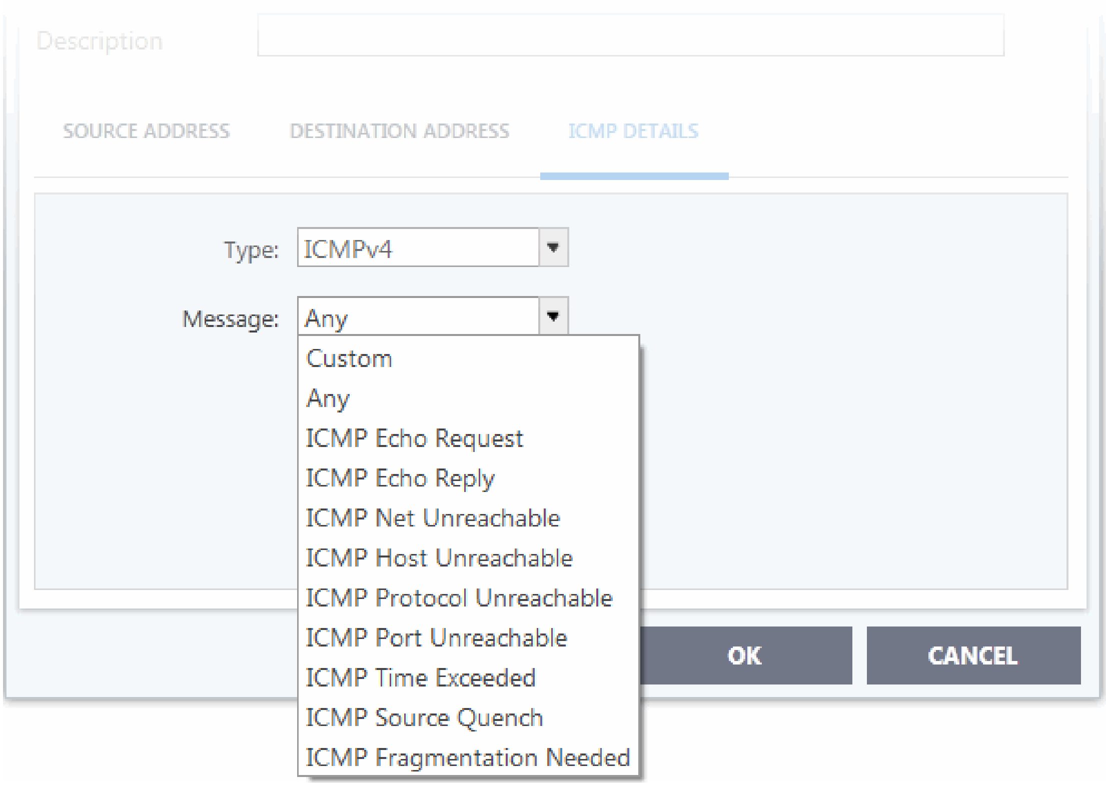
ii. **ICMP**

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

- **ICMP Details**

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.

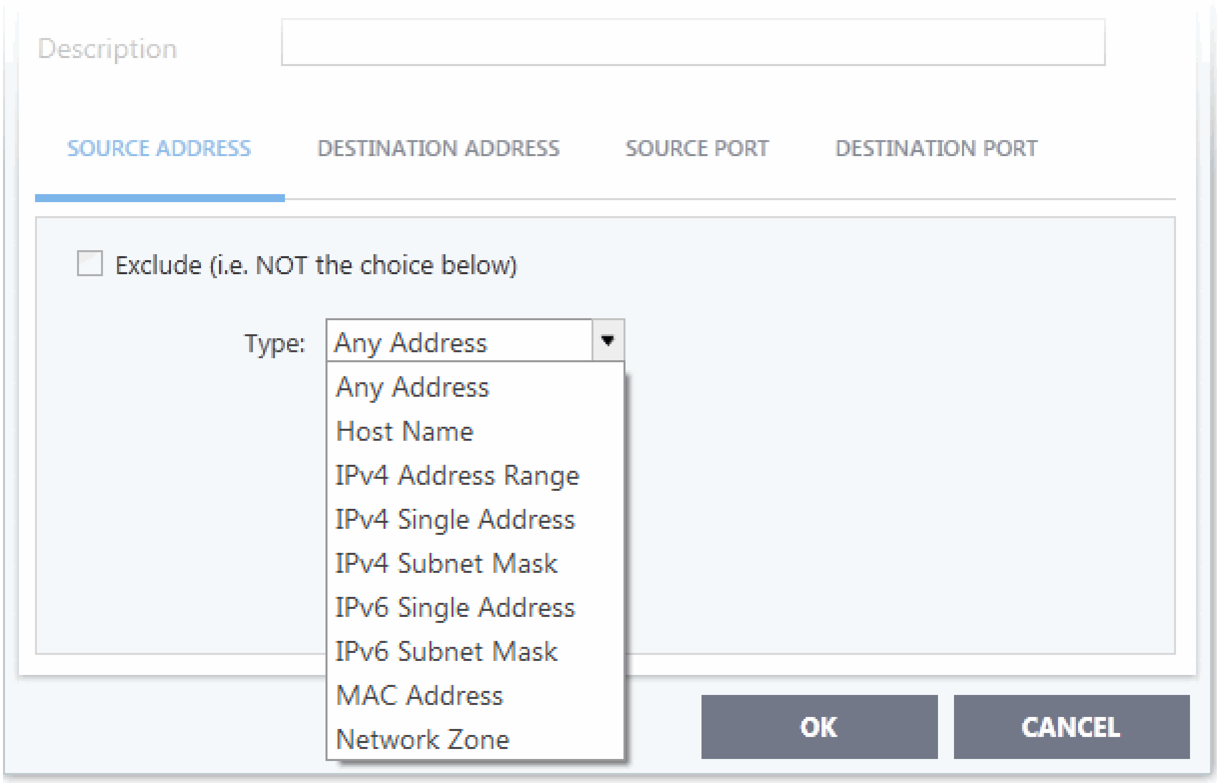


2. Under the 'ICMP Details' tab, choose the ICMP version from the 'Type' drop-down.
3. Specify ICMP Message, Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.

When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

iii. **IP**

When you select IP as the protocol in '**General Settings**', you are shown a list of IP message type in the 'IP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

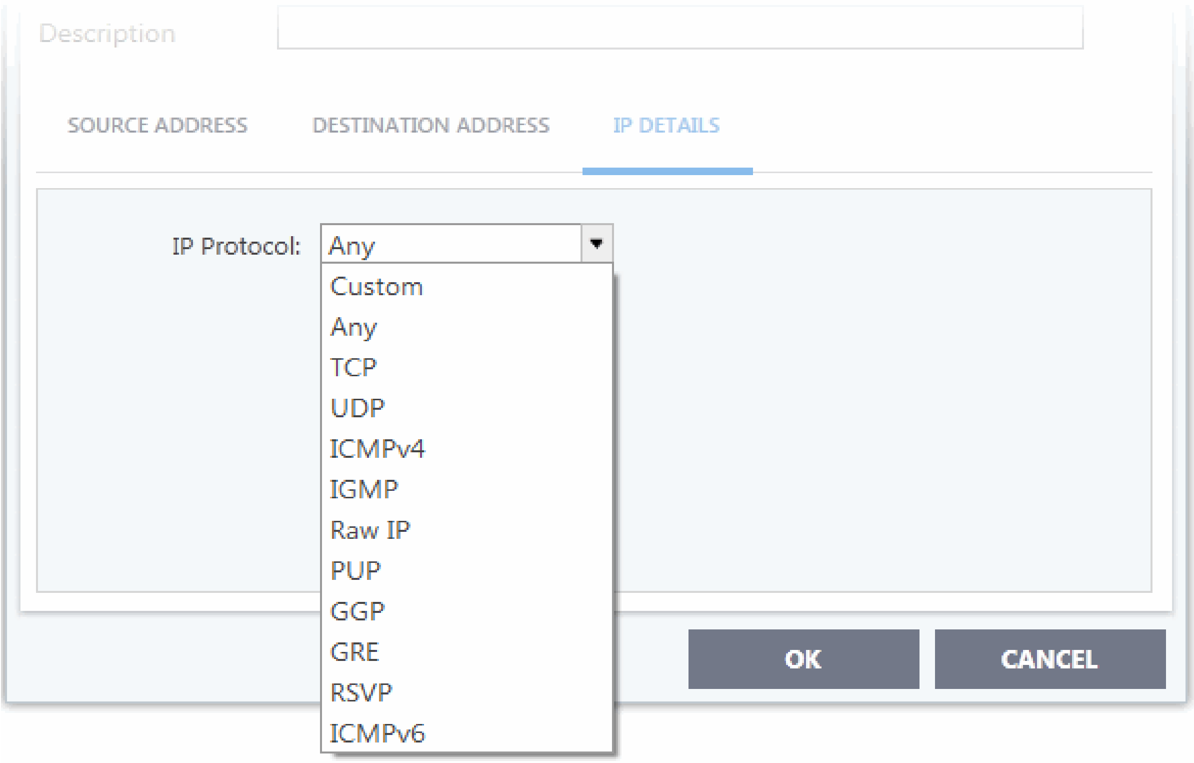


□ Exclude (i.e. NOT the choice below)

Type: Any Address

- **IP Details**

Select the types of IP protocol that you wish to allow, from the ones that are listed.



IP Protocol: Any

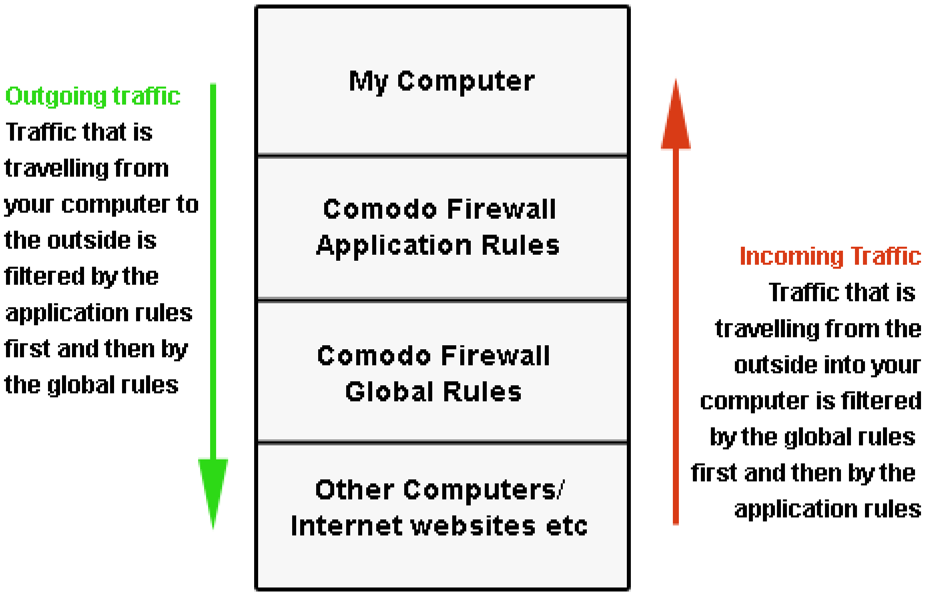
- Click 'OK' to save the firewall rule.

6.3.3. Global Rules

'Global Rules' are applied to *all* traffic traveling in and out of your computer. This makes them different to 'Application Rules', which are applied to and triggered by traffic for a specific application.

Comodo Firewall analyzes every packet of data in and out of your PC using combination of Application and Global Rules.

- Outgoing connection attempts - Application rules are consulted first and the global rules second.
- Incoming connection attempts - Global rules are consulted first and the application rules second.


Outgoing traffic
Traffic that is travelling from your computer to the outside is filtered by the application rules first and then by the global rules
My Computer
Comodo Firewall Application Rules
Comodo Firewall Global Rules
Other Computers/ Internet websites etc
Incoming Traffic
Traffic that is travelling from the outside into your computer is filtered by the global rules first and then by the application rules

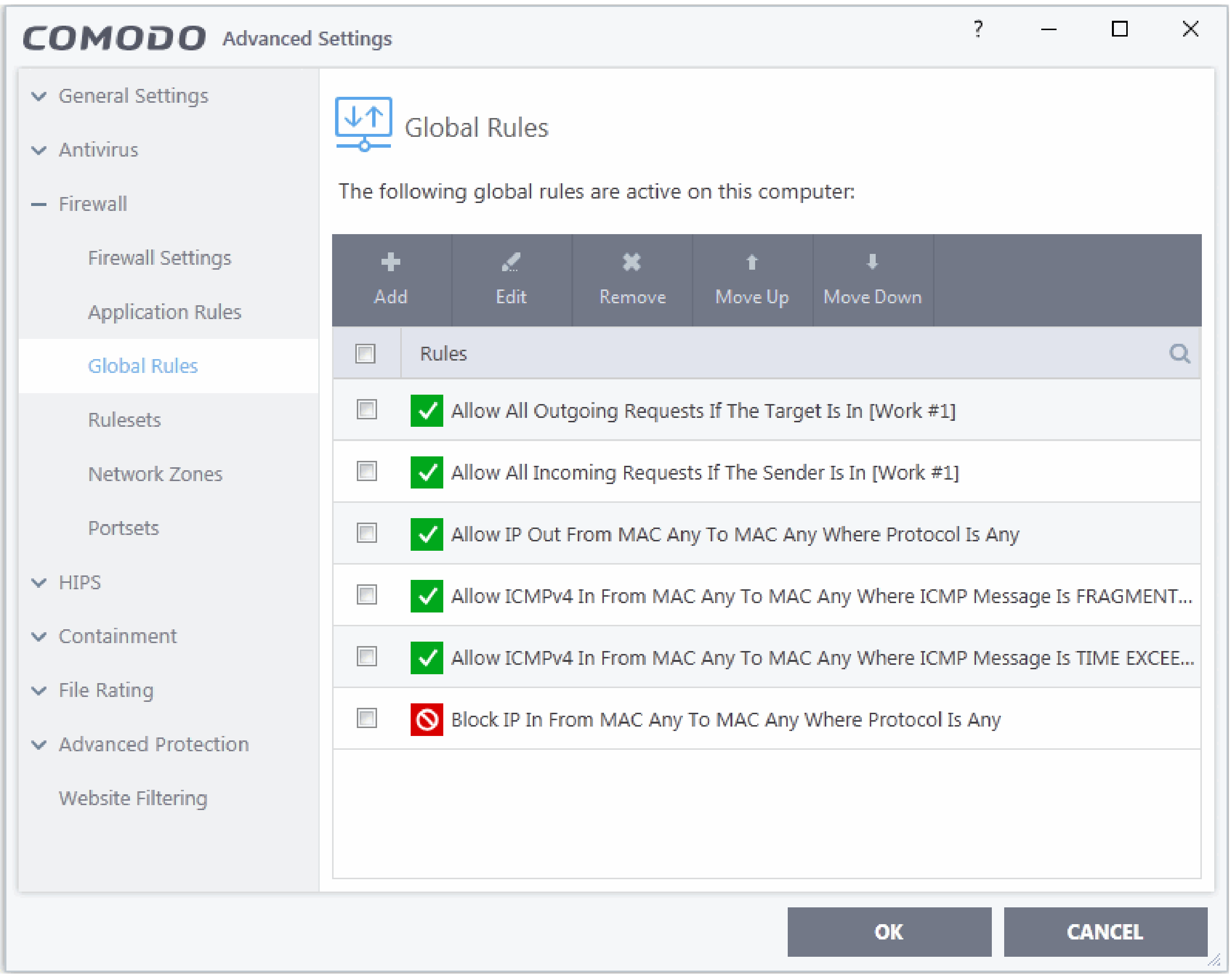
Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.

Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

The 'Global Rules' panel in the 'Advanced Settings' interface allows you to view create and manage the global firewall rules.

To open the Global Rules panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Global Rules' under 'Firewall' on the left.



Global Rules

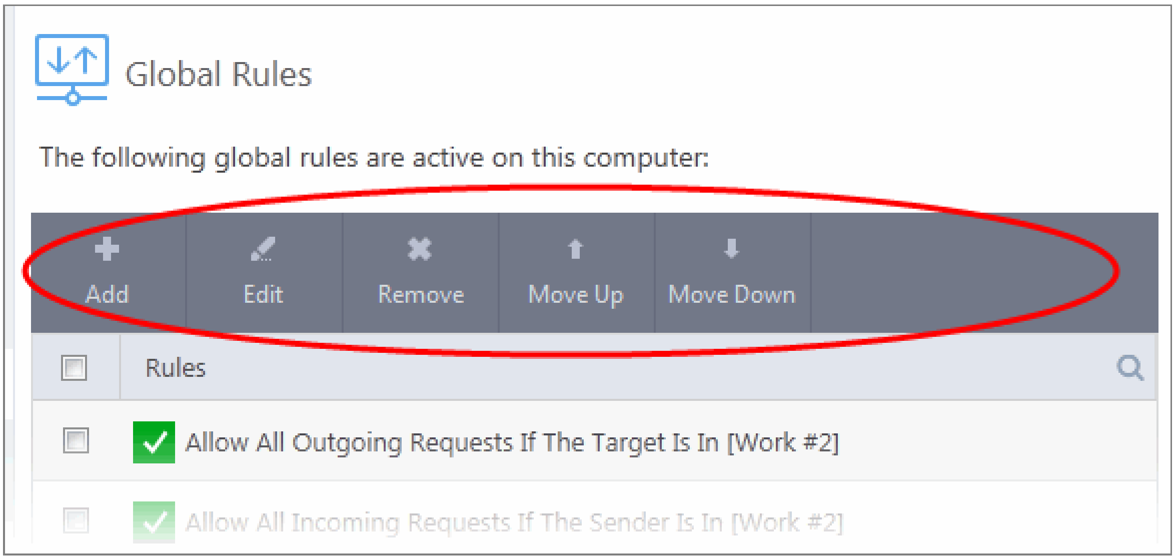
The following global rules are active on this computer:

□	Rules
□	✓ Allow All Outgoing Requests If The Target Is In [Work #1]
□	✓ Allow All Incoming Requests If The Sender Is In [Work #1]
□	✓ Allow IP Out From MAC Any To MAC Any Where Protocol Is Any
□	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is FRAGMENT...
□	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME EXCEE...
□	🚫 Block IP In From MAC Any To MAC Any Where Protocol Is Any

You can search for a specific rule in the list by clicking the search icon on the right and entering the name of the rule in part or full.

General Navigation:

The control buttons at the top of the list enable you to create and manage global rules.



Global Rules

The following global rules are active on this computer:

□	Rules
□	✓ Allow All Outgoing Requests If The Target Is In [Work #2]
□	✓ Allow All Incoming Requests If The Sender Is In [Work #2]

- **Add -** Allows you to add a new global rule. See '**Adding and Editing a Firewall Rule**' in the previous section 'Application Rules' for guidance on creating a new rule.

- **Edit -** Allows you to modify the selected global rule. See **'Adding and Editing a Firewall Rule'** in the previous section 'Application Rules' for guidance on editing a new rule.
- **Remove -** Deletes the selected rule.
- **Purge -** Runs a system check to verify that all the applications for which rules are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down -** The traffic is filtered by referring to the rules in order from the top. The Move Up and Move Down buttons enable you to change the priority of a selected rule.

To add a global rule, click the 'Add' button. To edit an existing global rule, right click and select 'Edit'. The configuration of Global Rules is identical to that of application rules.

- See **Application Rules** for an introduction to the rule setting interface.
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration.

6.3.4. Firewall Rule Sets

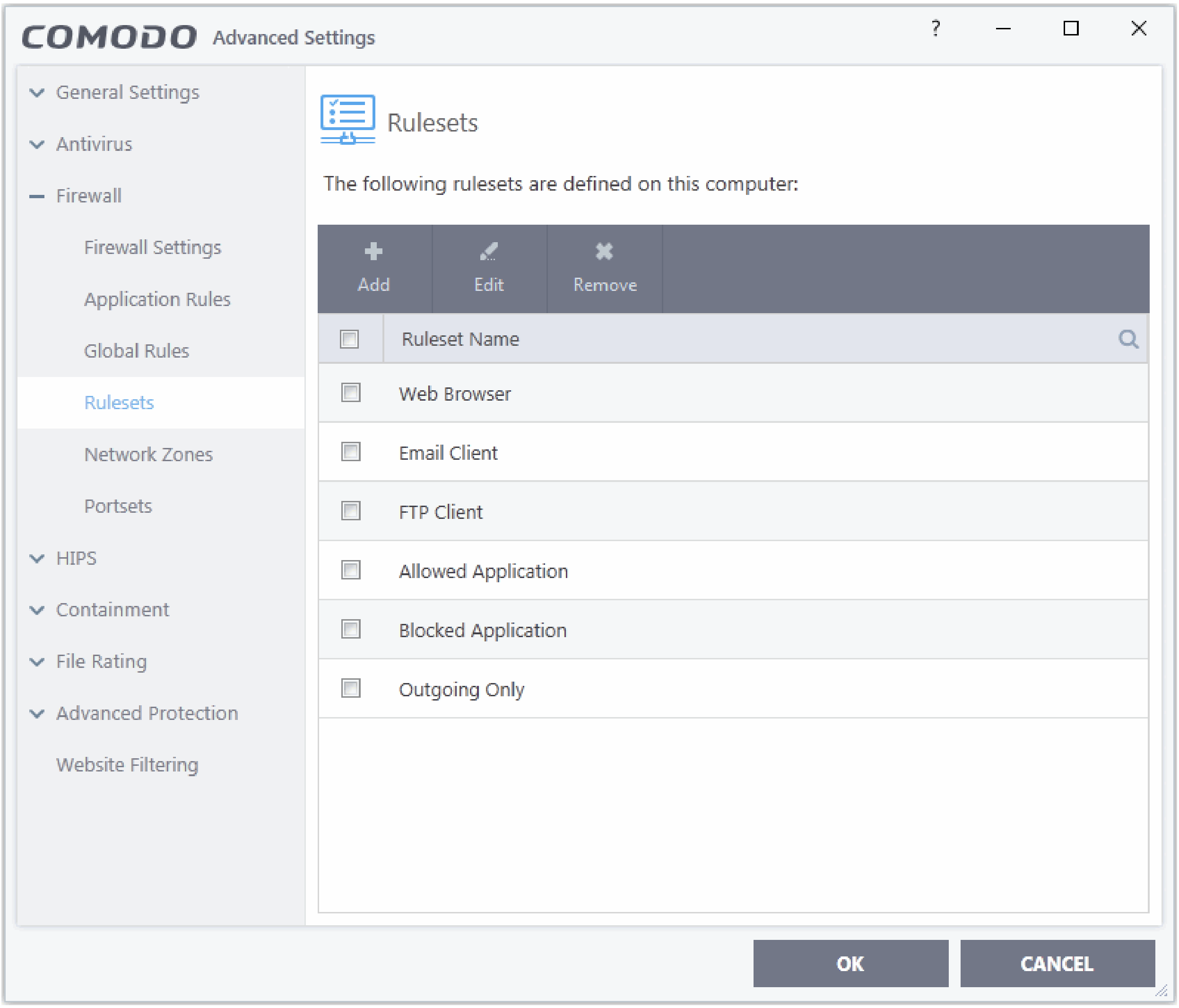
A firewall ruleset is a collection of one or more individual firewall rules that have been saved and which can be deployed on multiple applications. CIS ships with six predefined rulesets and allows you to create custom rulesets.

This section contains advice on the following:

- **Predefined Rulesets**
- **Creating a new ruleset**

To open the Rulesets panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Rulesets' under 'Firewall' on the left.
- The interface displays a list of pre-defined and custom rulesets. You can search for a specific ruleset by clicking the search icon on the right and entering the name of the ruleset in part or full:



The following rulesets are defined on this computer:

□	Ruleset Name
□	Web Browser
□	Email Client
□	FTP Client
□	Allowed Application
□	Blocked Application
□	Outgoing Only

Predefined Rulesets

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring separate rules, this practice would prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Chrome'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can modify pre-defined policies to suit their environment and requirements. For example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of its rules.

CIS ships with six predefined firewall rulesets for different categories of applications:

- Web Browser
- Email Client
- FTP Client
- Allowed Application
- Blocked Application
- Outgoing Only

These rulesets can be edited by adding new rules or re-configuring the existing rules. See **Adding and Editing Firewall Rules** in 'Application Rules'.

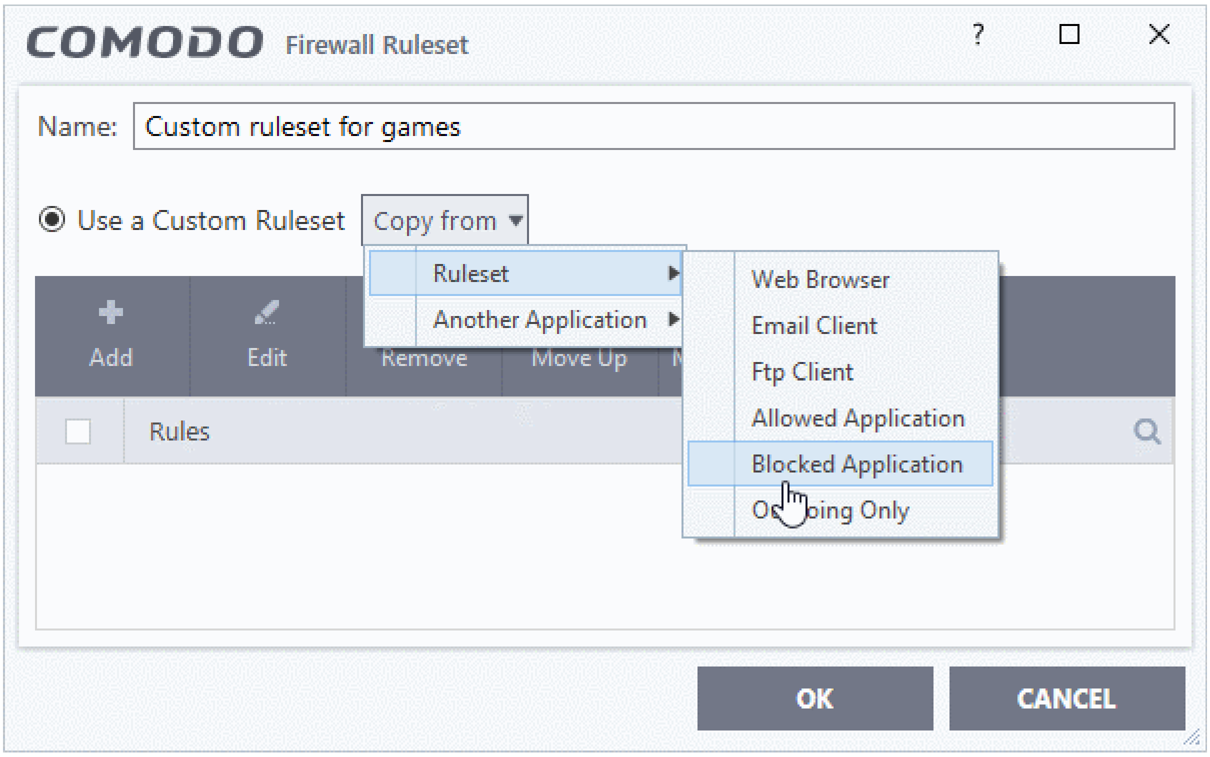
Creating a new ruleset

You can create new rulesets with custom network access control rules as per your requirements. These can then be rolled out to specific applications when **creating Firewall ruleset** for the application.

To add a new Ruleset

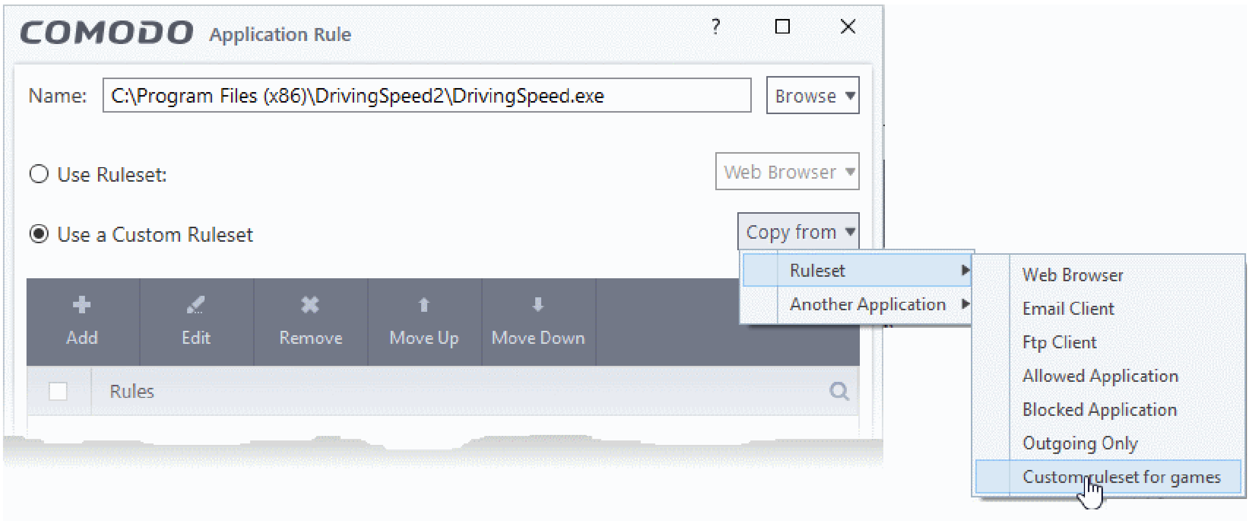
- Click the 'Add' button at the top of the list of rulesets in the 'Rulesets' panel

The 'Firewall Ruleset' interface will open.



- As this is a new ruleset, you need to name it in the text field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for.
- Next you should add and configure the individual rules for this ruleset. You can choose to use an existing ruleset as a starting point and add/edit rules as required. See '**Adding and Editing a Firewall Rule**' for more advice on this.

Once created, this ruleset can be quickly called when **creating or modifying a Firewall ruleset** for an application:



To view or edit an existing predefined Ruleset

- Double click on the ruleset Name in the list

Or

- Select the ruleset name then click the 'Edit' button
- Details of the process from this point on can be found here.

6.3.5. Network Zones

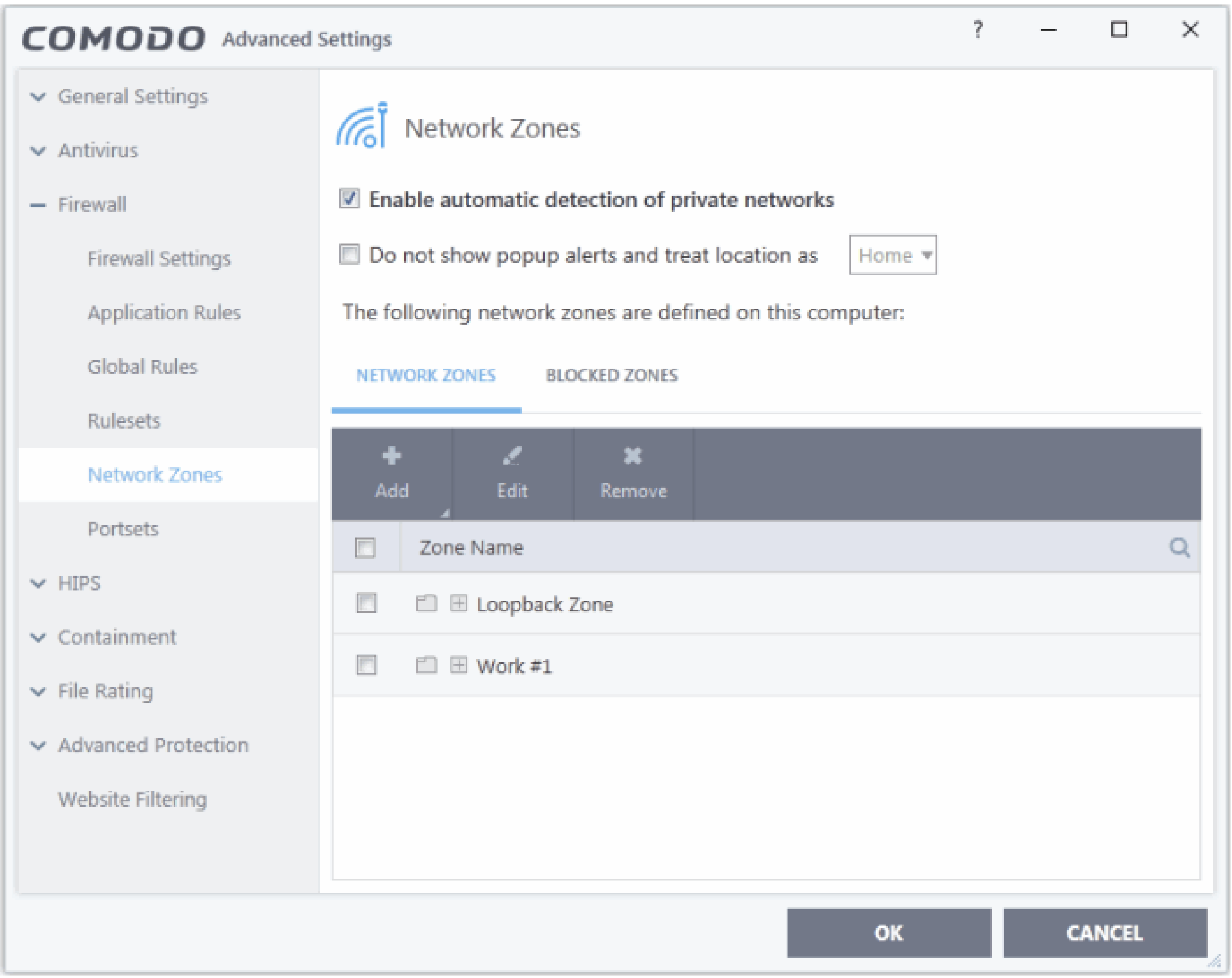
A 'Network Zone' can consist of an individual machine (including a single home computer connected to the internet) or a network of thousands of machines. Access to any network zone can be easily granted or denied in the network zones panel.

The Network Zones panel allows you to:

- Configure automatic detection of new networks (wired or wireless) that your computer can connect to.
- Configure alerts for network connections
- Define network zones that are trusted and specify access privileges to them
- Define network zones that are untrusted and block access to them

To open the Network Zones panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Firewall' then 'Network Zones' on the left.



☑ Enable automatic detection of private networks

☐ Do not show popup alerts and treat location as Home

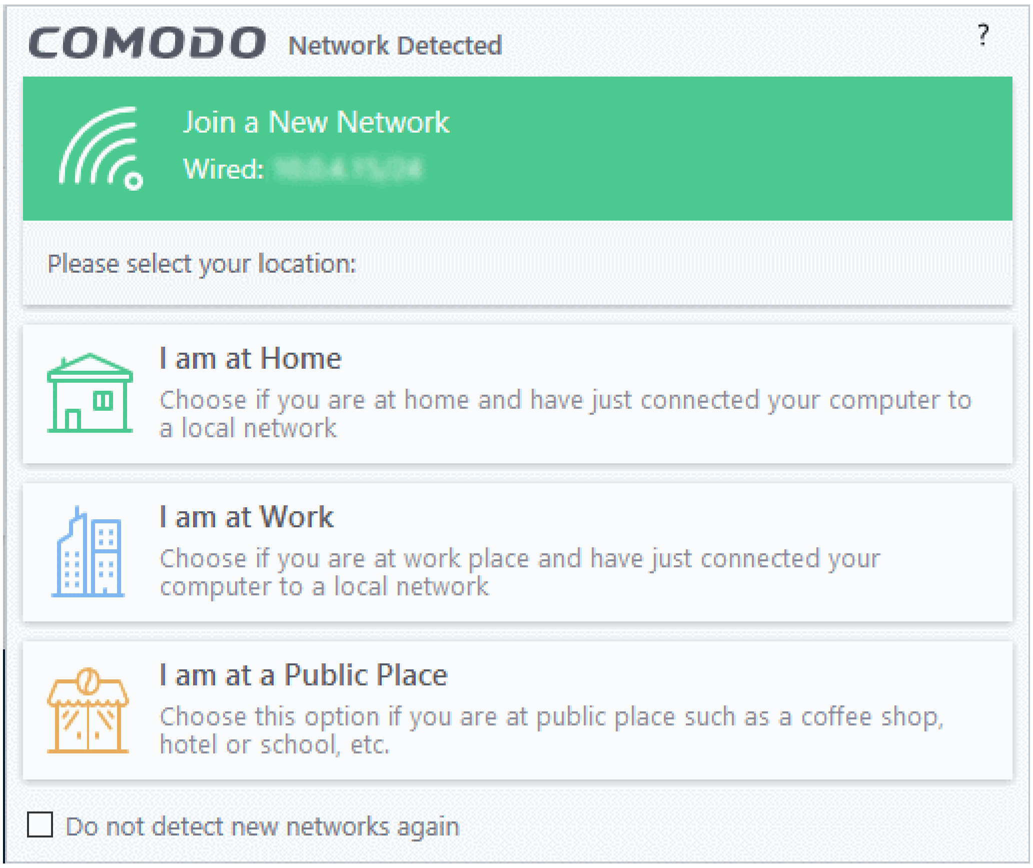
The following network zones are defined on this computer:

☐	Zone Name
☐	Loopback Zone
☐	Work #1

Network Monitoring Settings:

- **Enable automatic detection of private networks -** Instructs Comodo Firewall to monitor for attempted connections to any new wired or wireless network ***(Default = Enabled).*** Deselect this option if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**').
- **Do not show popup alerts and treat location as -** If enabled, the 'new network connection' alert will not appear and the network location will default to the location selected in the drop-down - Home, Work or Public. ***(Default = Disabled)***

If 'automatic detection' is enabled, and 'do not show...' is disabled, then the following alert will be displayed whenever your system tries to connect to a new network:



COMODO Network Detected ?

Join a New Network

Wired: [redacted]

Please select your location:

I am at Home

Choose if you are at home and have just connected your computer to a local network

I am at Work

Choose if you are at work place and have just connected your computer to a local network

I am at a Public Place

Choose this option if you are at public place such as a coffee shop, hotel or school, etc.

□ Do not detect new networks again

Select the appropriate network type for your connection. Your firewall configuration will be optimized for security and usability accordingly.

- Select 'Do not automatically detect new networks again' If you are an experienced user that wishes to manually set-up their own trusted networks. This can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**'.

The panel has two tabs:

- **Network Zones** - Allows you to define network zones with specific access rights. Application access privileges are specified through the **Application Rule** interface. See '**Creating or Modifying Firewall Rules**' for more details.
- **Blocked Zones** - Allows you to define trusted networks that are not trustworthy and to block access to them.

6.3.5.1. Network Zones

A 'Network Zone' can consist of an individual machine (including a single home computer connected to internet) or a network of thousands of machines. You can grant or deny access to a network zone as required.

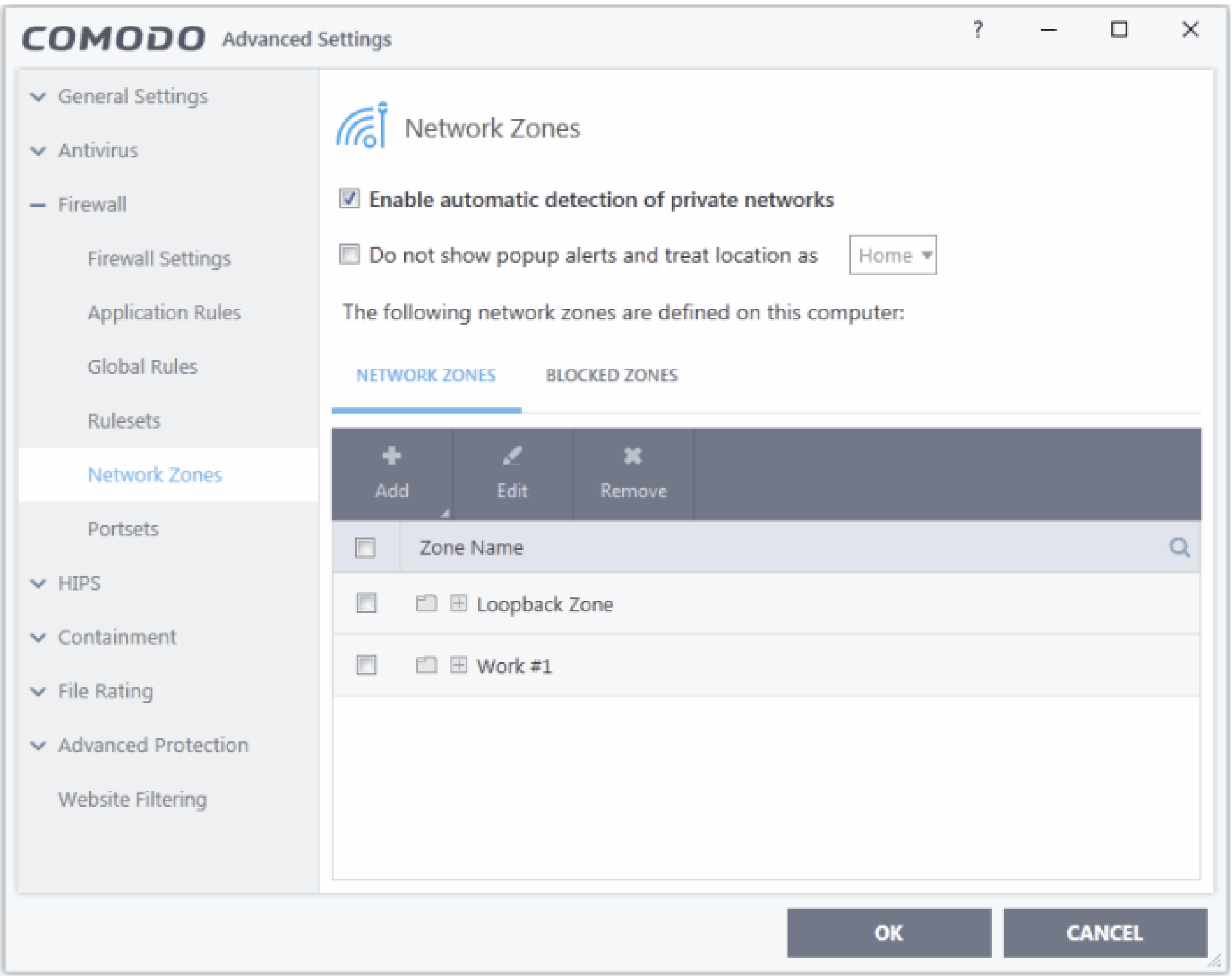
Background Note:

- A computer network is a connection between computers through a cable or some type of wireless connection.
- It enables users to share information and devices between computers and other users within the network.
- Obviously, there are certain computer networks which you need to grant access to, including your home or work network.
- Conversely, there may be other networks with which you want to restrict communication, or even block entirely.

The 'Network Zones' tab in the 'Network Zones' panel allows allows you to define network zones, to which your computer can connect with access rights as defined by the firewall rules or blocked access to.

To add and manage network zones

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Network Zones' under 'Firewall' on the left.
- Click the 'Network Zones' tab



Network Zones

☑ Enable automatic detection of private networks

☐ Do not show popup alerts and treat location as Home

The following network zones are defined on this computer:

☐	Zone Name
☐	Loopback Zone
☐	Work #1

The 'Network Zones' tab displays a list of zones added to CIS. You can add new zones and manage existing zones.

Note 1: Adding a zone to this area does not, by itself, define any permission levels or access rights to the zone. This area lets you define the zones so you can quickly assign such permissions **in other areas of the firewall**.

Note 2: A network zone can be designated as 'Trusted' and allowed access from the '**Manage Network Connections**' interface. An example would be your home computer or network.

Note 3: A network zone can be designated as 'Blocked' and denied access by using the '**Blocked Zones**' interface. An example would be a known spyware site.

Note 4: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rules** assigned to a zone will inspect all traffic to/from a zone.

Note 5: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc) once you connect to them. This can be disabled by deselecting the option 'Enable automatic detection of private networks' in the **Firewall Settings** panel.

You can use search for a specific zone by clicking the search icon and entering the name of the zone in part or full.

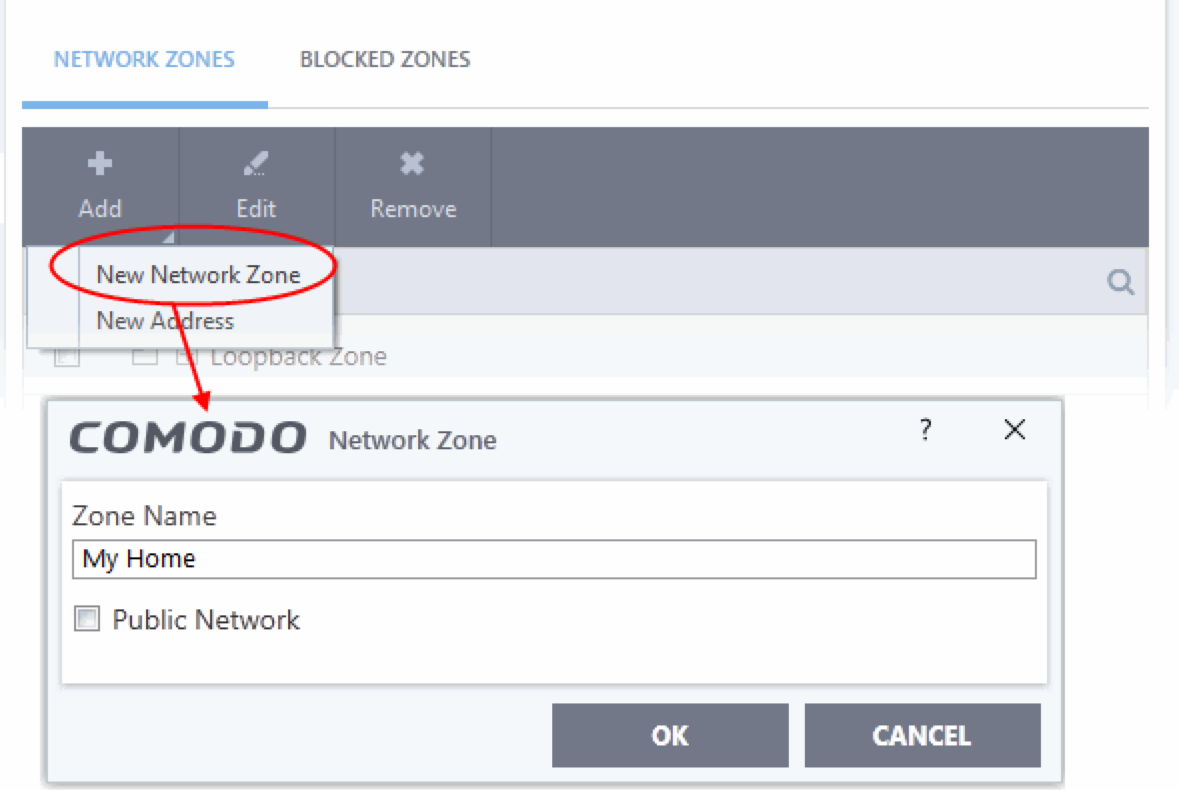
Defining a new Network Zone

To add a new network zone:

- Step 1 - **Define a name for the zone**.
- Step 2 - **Select the addresses to be included in this zone**.

Step 1 - Define a name for the zone

- Click the 'Add' button at the top of the list and choose 'New Network Zone' from the options.

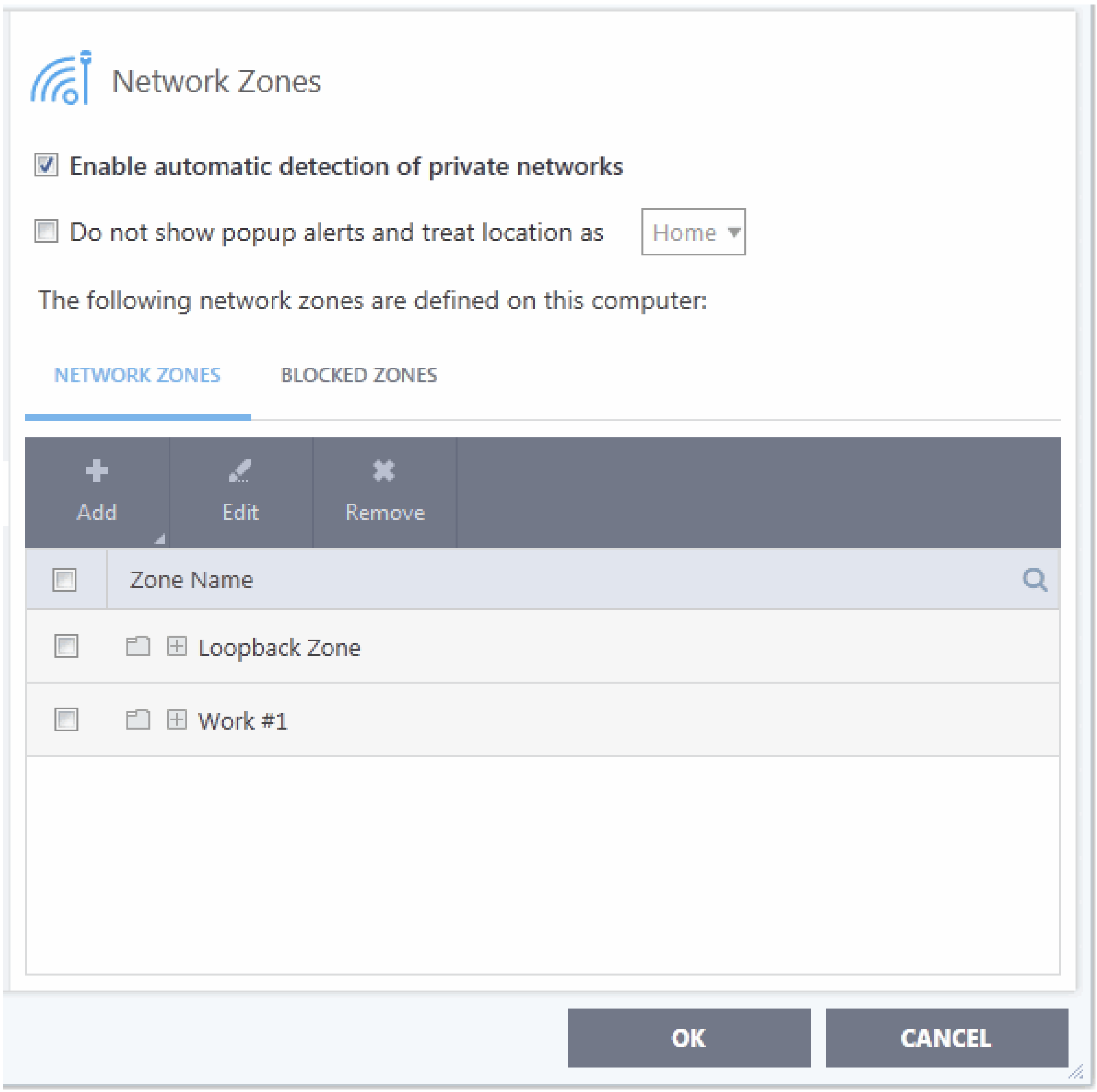


Zone Name: My Home

□ Public Network

- Choose a name that accurately describes the network zone you are creating.
- Select 'Public Network' if you are defining a network zone for a network in a public place. For example, when you are connecting to a Wi-Fi network at an airport, restaurant etc. The firewall will optimize the connection accordingly.
- Click 'OK' to confirm your zone name.

This adds your new zone to the 'Network Zones' list:



Network Zones

☑ Enable automatic detection of private networks

□ Do not show popup alerts and treat location as Home

The following network zones are defined on this computer:

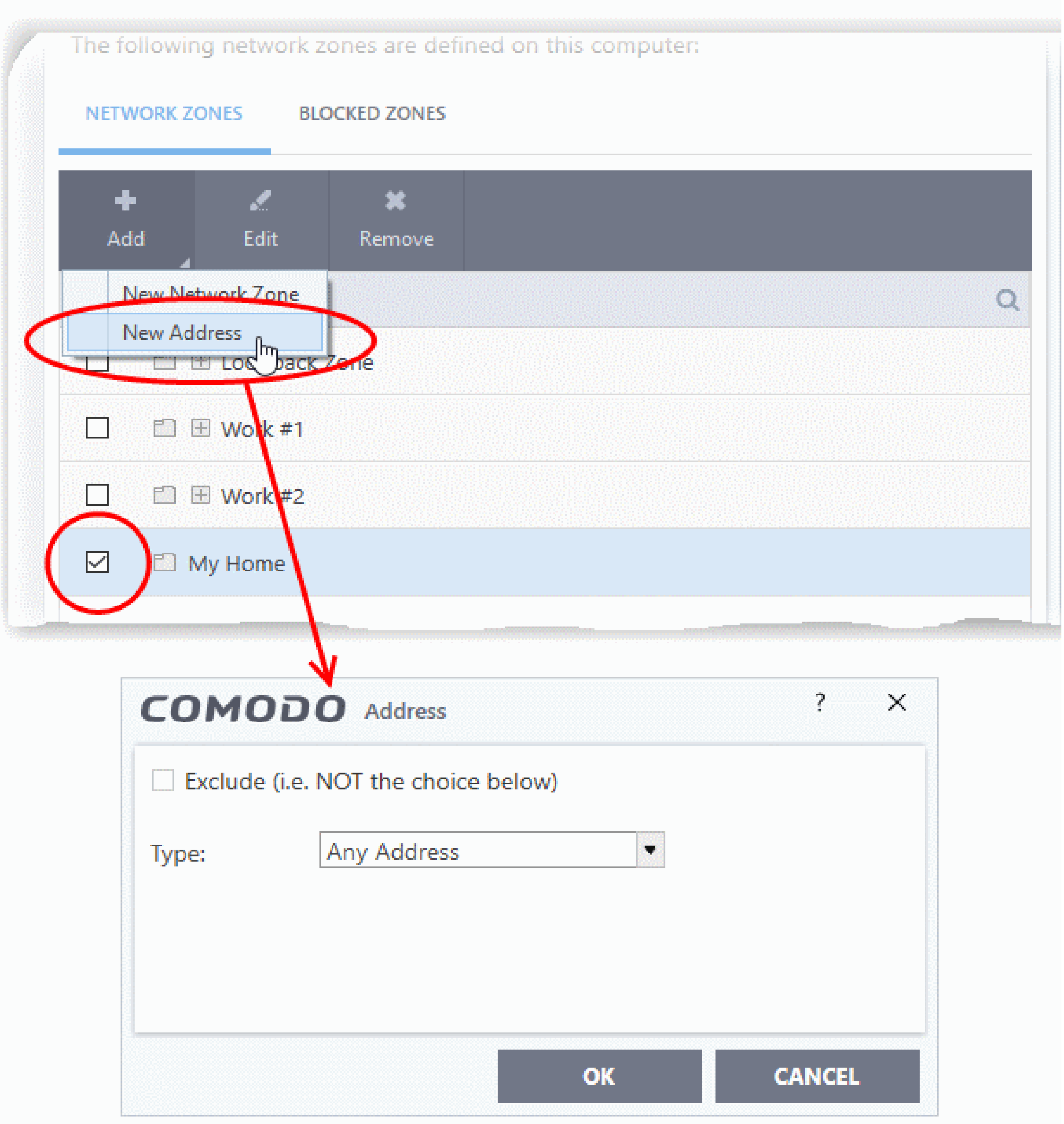
□	Zone Name
□	Loopback Zone
□	Work #1

Step 2 - Select the addresses to be included in this zone

- Select the network zone name then click the 'Add' button at the top
- Choose 'New Address' from the options
- Alternatively, right click on the network zone and choose 'Add' > 'New Address' from the context sensitive menu

The 'Address' dialog allows you to select an address from the 'Type' drop-down box shown below ***(Default = Any Address)***.

The 'Exclude' check box will become active if you select anything other than 'Any Address'



Address Types:

1. Any Address - Adds all the IP addresses (0.0.0.0- 255.255.255.255) to the zone.
2. Host Name - Enter a named host which denotes an address on your network.
3. IPv4 Range - Will include all the IPv4 addresses between the values you specify in the 'Start Range' and 'End Range' text boxes.
4. IPv4 Single Address - Enter a single IP address to be added to the zone - e.g. 10.100.100.11.
5. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to add to the defined zone.
6. IPv6 Single Address - Enter a single address to be added to the zone – e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.

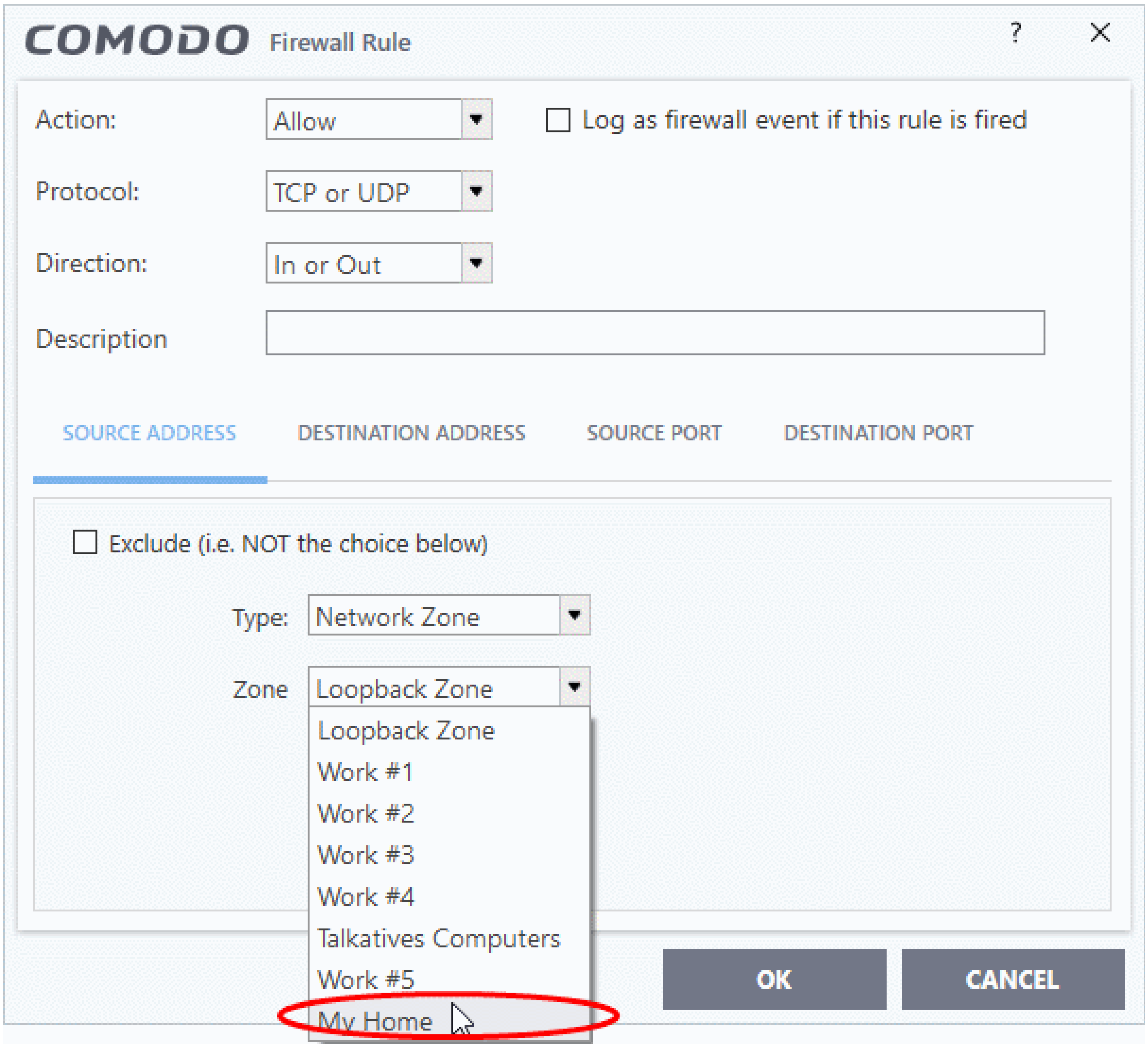
8. MAC Address - Enter a specific MAC address to be added to the zone.

- Click 'OK' to confirm your choice.
- Click 'OK' in the 'Network Zones' interface.

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

- Quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**



COMODO Firewall Rule

Action: Allow

☐ Log as firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description

SOURCE ADDRESS | DESTINATION ADDRESS | SOURCE PORT | DESTINATION PORT

☐ Exclude (i.e. NOT the choice below)

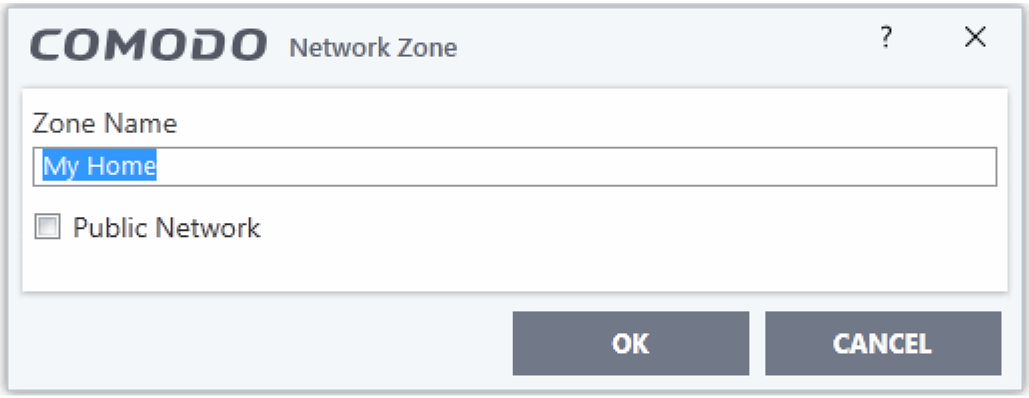
Type: Network Zone

Zone: Loopback Zone

- Quickly called and designated as a blocked zone from the '**Blocked Zones**' interface

To edit the name of an existing Network Zone

1. Select the name of the zone in the list (e.g., My Home) and click the 'Edit' button from the top or double click on the network zone name.



2. Edit the name of the zone.

To add more addresses to an existing Network Zone

- Select the network name, click the 'Add' > 'New Address' from the top.
- Add new address from the **'Address' interface**.

To modify or change the existing address in a zone

- Click the + button beside the network zone name to expand the addresses
- Double click on the address to be edited or select the address, click 'Edit' at the top
- Edit the address from the **'Address' interface**.

To remove an existing address in a zone

- Click the '+' button beside the network zone name to expand the addresses
- Select the address and click 'Remove' from the top

6.3.5.2. Blocked Zones

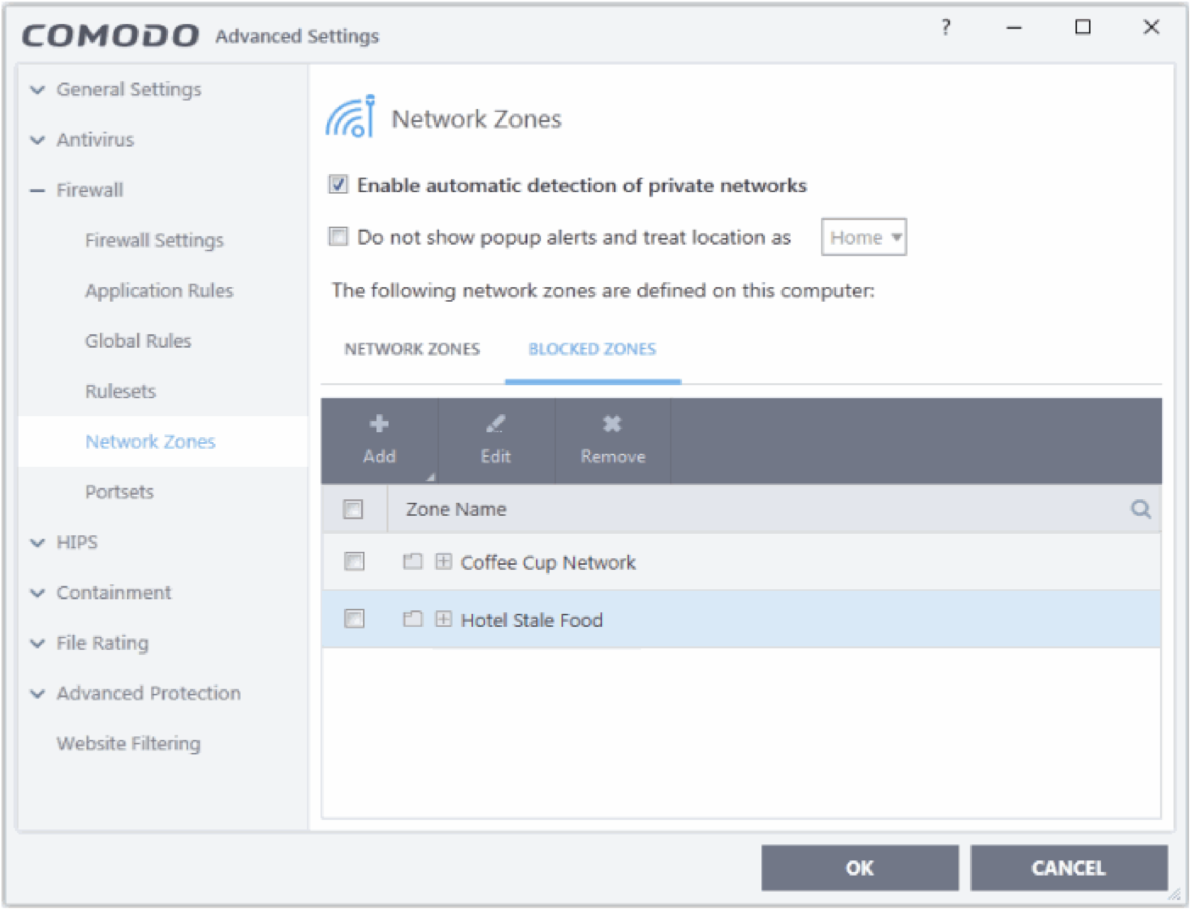
A computer network lets you share information and devices with other users and other computers. There are certain networks that you'll want to 'trust' and grant access to, for example your home or work network. Conversely, there may be other networks that you do not trust and want to restrict communications with or block entirely.

The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not wish to trust.

Note: We advise new or inexperienced users to first read '**Network Zones**', '**Stealth Ports Wizard**' and '**Application Rules**' before blocking zones using this interface.

To add and manage blocked zones

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Network Zones' under 'Firewall' on the left.
- Click the 'Blocked Zones' tab



The 'Blocked Network Zones' tab allows you to:

- Deny access to an existing network zone
- Deny access to a network by manually defining a new blocked zone

Note 1: You must create a zone before you can block it. There are two ways to do this;

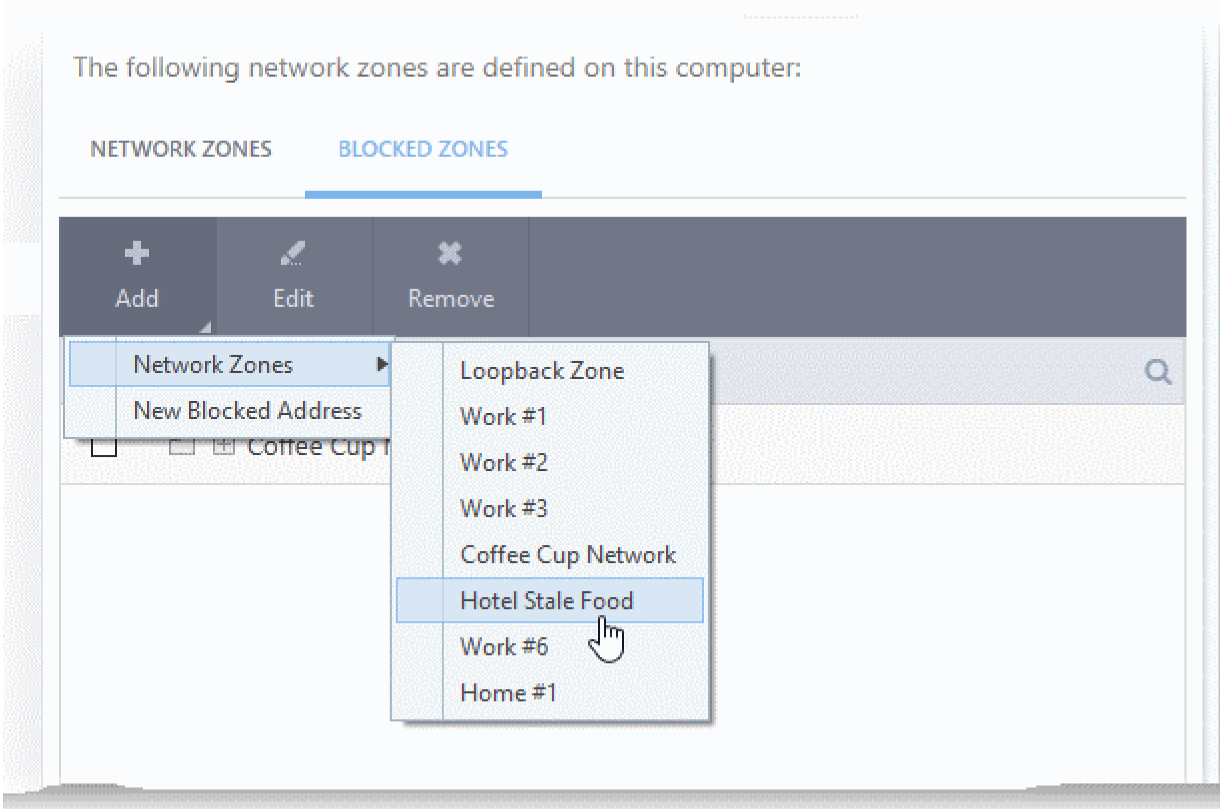
1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

Note 2: You cannot reconfigure *existing* zones from this interface (e.g., to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

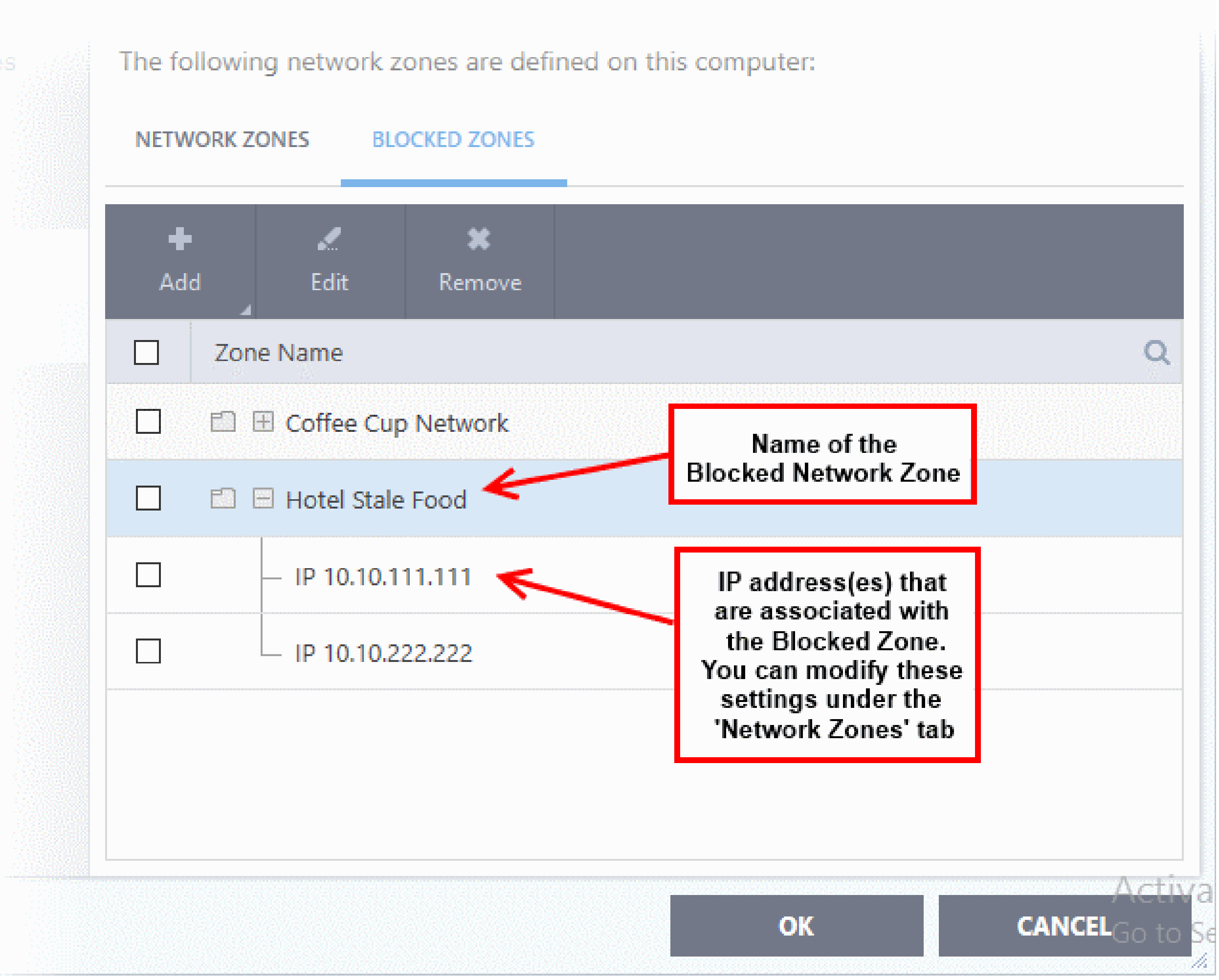
You can search for specific blocked zone by clicking the magnifying glass icon and entering the name of the zone in part or full.

To deny access to an existing network zone

1. Click 'Add' button at the top and choose 'Network Zones' from the options
2. Select the particular zone you wish to block.


The following network zones are defined on this computer:

The selected zone will appear in the 'Blocked Zones' interface.


The following network zones are defined on this computer:

□	Zone Name
□	Coffee Cup Network
□	Hotel Stale Food
□	IP 10.10.111.111
□	IP 10.10.222.222

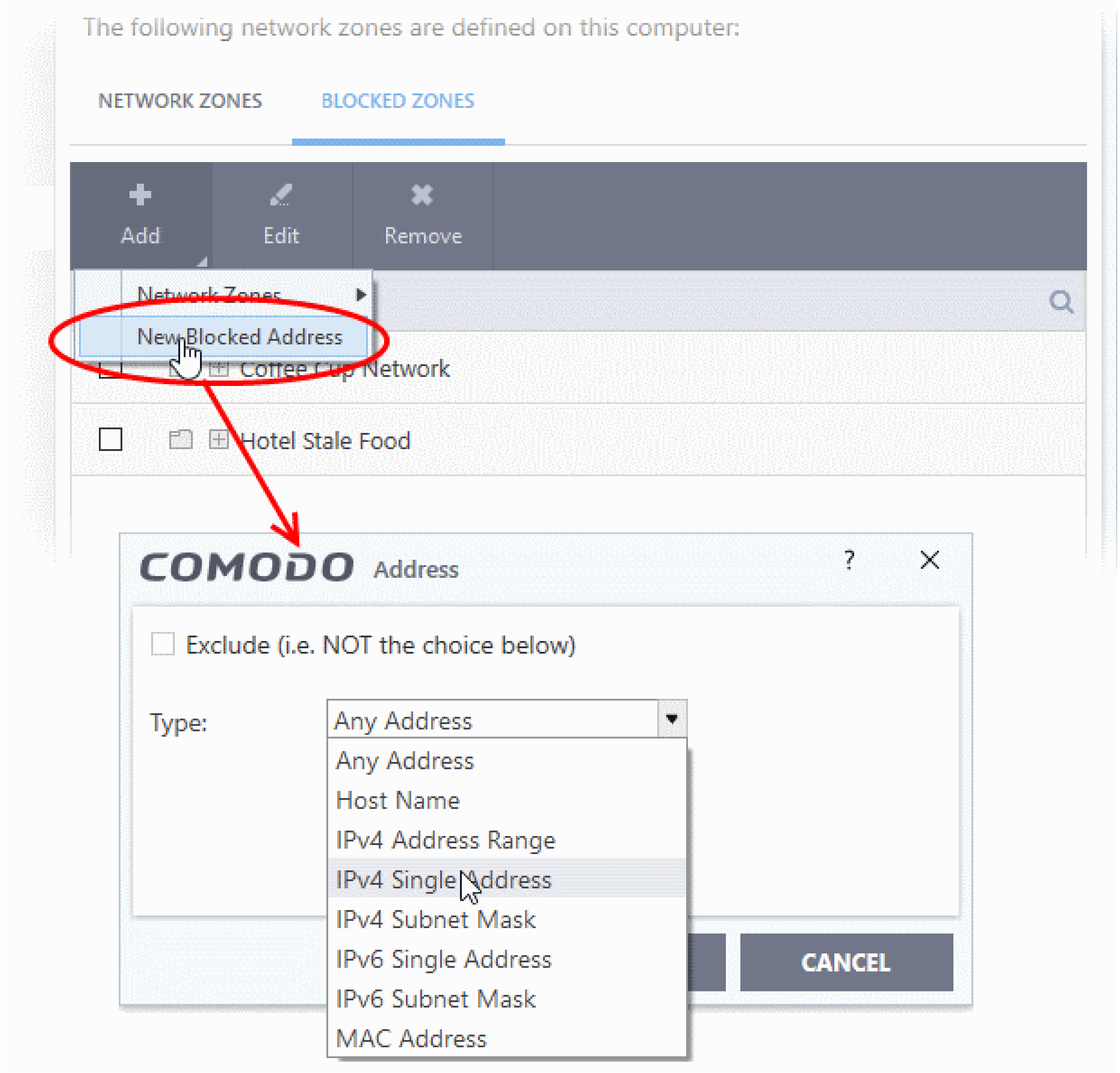
Name of the Blocked Network Zone

IP address(es) that are associated with the Blocked Zone. You can modify these settings under the 'Network Zones' tab

3. Click 'OK' to confirm your choice. All traffic intended for and originating from devices in this zone is now blocked.

To deny access to a network by manually defining a new blocked zone

1. Click the 'Add' button and choose 'New Blocked Address':



Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

Address Types:

- Any Address - Will block connections from all IP addresses (0.0.0.0- 255.255.255.255)
- Host Name- Enter a named host which denotes an address on your network.
- IPv4 Range - Will block access to the IPv4 addresses you specify in the 'Start Range' and 'End Range' text boxes.
- IPv4 Single Address - Block access to a single address - e.g. 192.168.200.113.
- IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to block.

- IPv6 Single Address -Block access to a single address - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
- MAC Address - Block access to a specific MAC address.

2. Select the address to be blocked and click OK

   The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

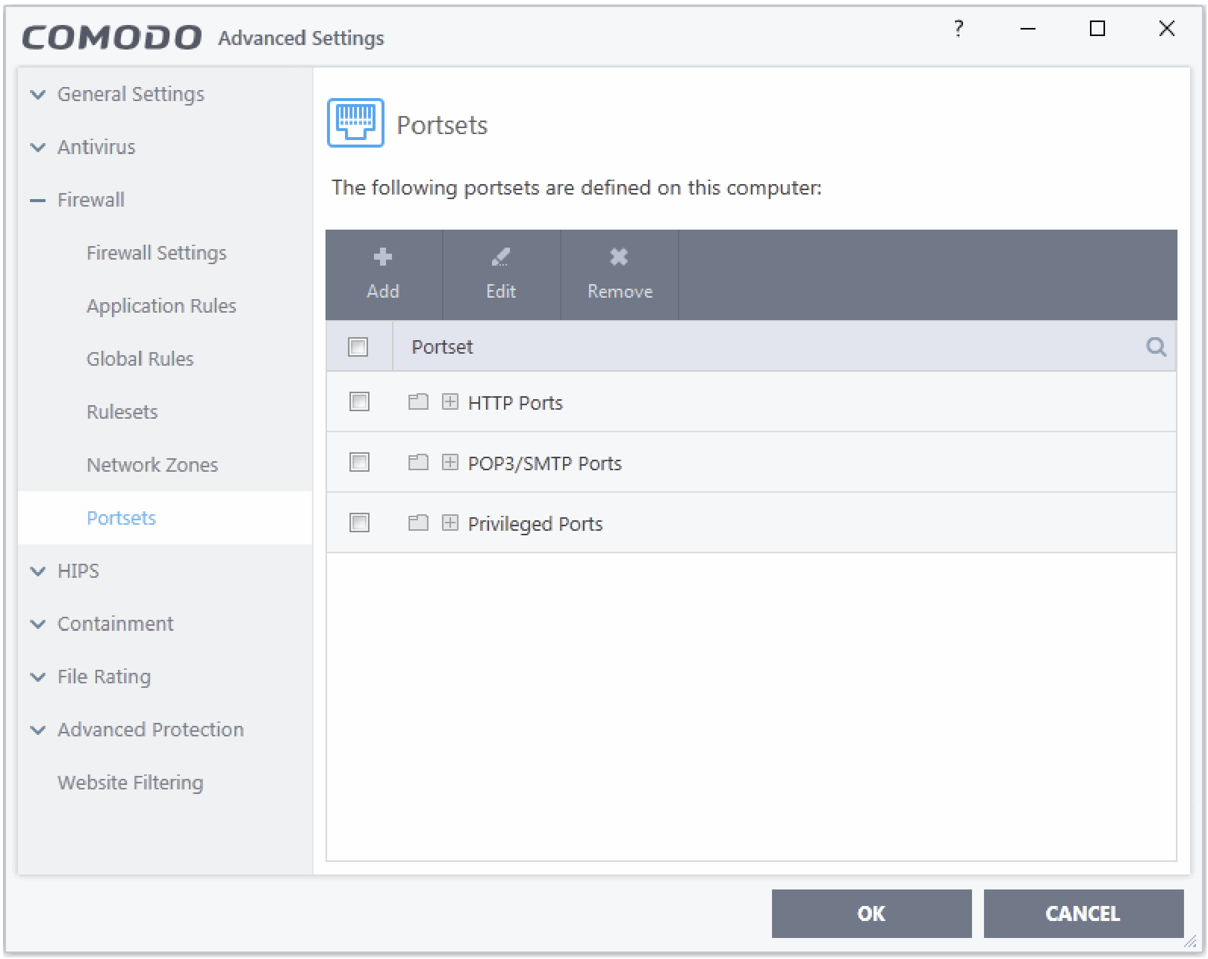
3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from devices in this zone is now blocked.

6.3.6. Port Sets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple **Application Rules** and **Global Rules**. The 'Port Sets' panel allows you to view and manage pre-defined port sets and to add new port sets.

To open the Portsets panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Portsets' under 'Firewall' on the left.



The following portsets are defined on this computer:

□	Portset
□	⊞ HTTP Ports
□	⊞ POP3/SMTP Ports
□	⊞ Privileged Ports

Port Sets are displayed in a tree structure. Click the + button beside a port set name to view ports in the set.

CIS ships with three default portsets:

- **HTTP Ports**: 80, 443 and 8080. These are the default ports for http traffic. Your internet browser uses these ports to connect to the internet and other networks.
- **POP3/SMTP Ports**: 110, 25, 143, 995, 465 and 587. These ports are typically used for email communication by mail clients like Outlook and Thunderbird.
- **Privileged Ports:** 0-1023**.** This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports.

You can search for a specific portset by clicking the search icon and entering the name of the portset in part or full.

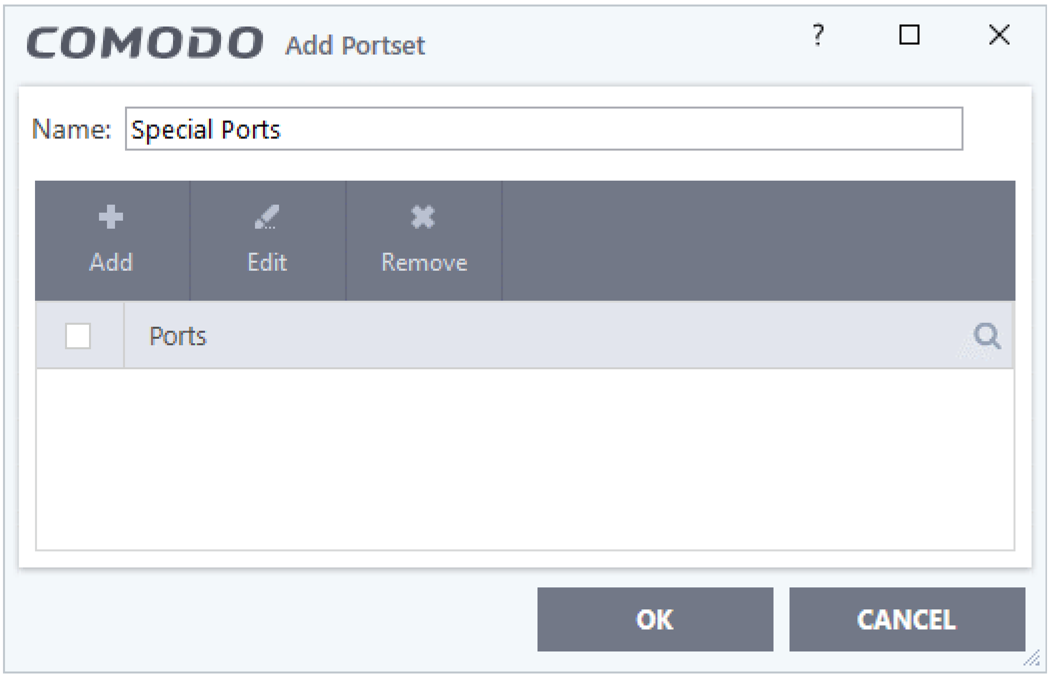
Defining a new Port Set

After defining a new portset you can apply it to applications through the **Application Rule** interface. See '**Creating or Modifying Firewall Rules**' for more details.

To add a new portset

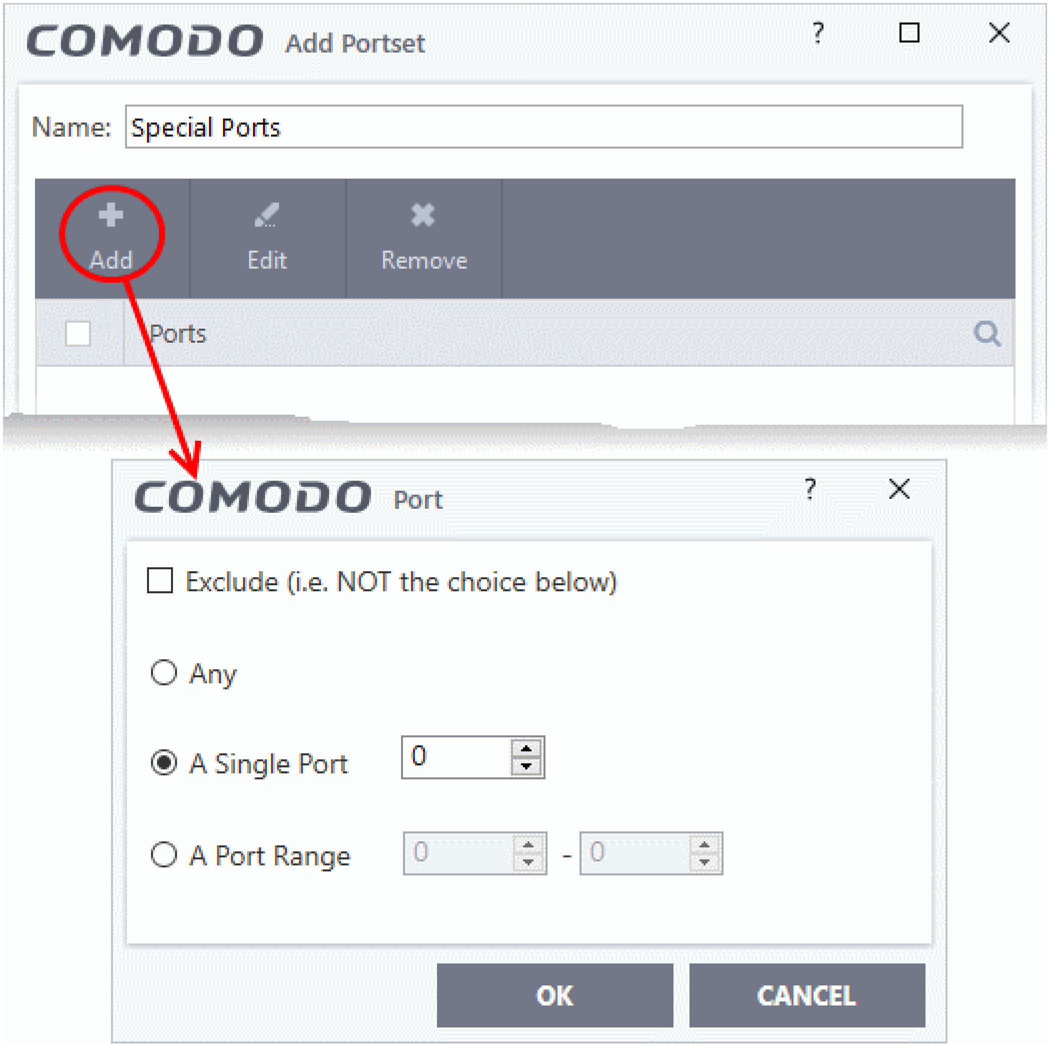
1. Click the 'Add' button at the top.

The 'Add Portset' dialog will open.



Name: Special Ports

2. Enter a name for the portset in the 'Name' field.
3. Click the 'Add' button to add ports/port ranges to the set:



COMODO Add Portset

Name: Special Ports

COMODO Port

☐ Exclude (i.e. NOT the choice below)

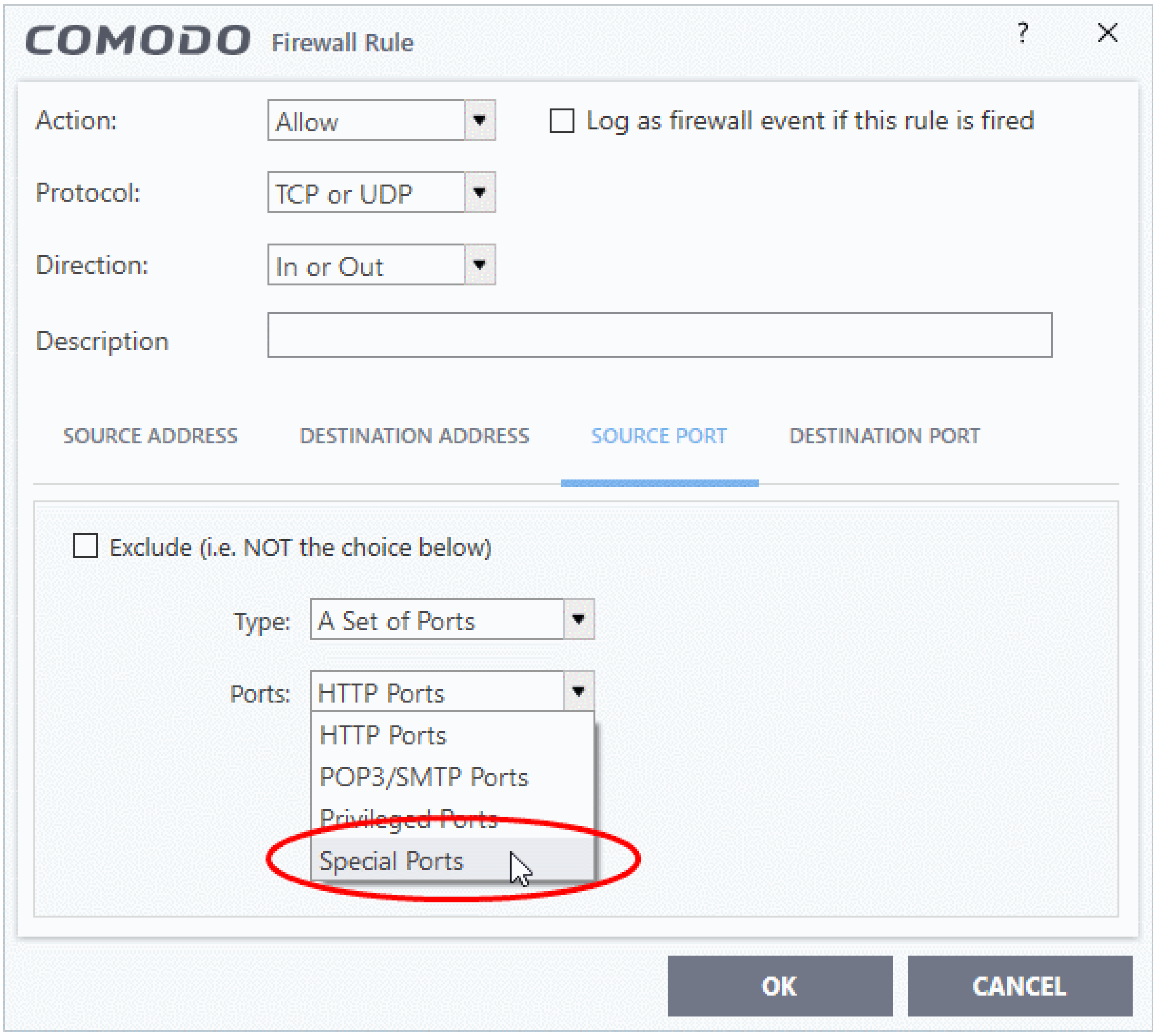
○ Any

● A Single Port 0

○ A Port Range 0 - 0

4. Specify the ports to be included in the new portset:
   - **Any -** to choose all ports
   - **A single port -** Specify the port number
   - **A port range -** Enter the start and end port numbers in the respective combo boxes.
   - Exclude (i.e. NOT the choice below): Means all ports will be included in the portset except the ones you specify here.
5. Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Edit Portset' interface.
6. Click 'OK' in the 'Add Portsets' interface to create the new portset.

   Once created, a Portset can be quickly called as 'A Set of Ports' when **creating or modifying a Firewall Ruleset**



COMODO Firewall Rule

Action: Allow

□ Log as firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description

SOURCE ADDRESS | DESTINATION ADDRESS | SOURCE PORT | DESTINATION PORT

□ Exclude (i.e. NOT the choice below)

Type: A Set of Ports

Ports: HTTP Ports

To edit an existing port set

- Select the portset from the 'Portsets' interface and click the 'Edit' button from the top to bring up the 'Edit Portset' dialog.
- The editing procedure is similar to **adding the portset** explained above.

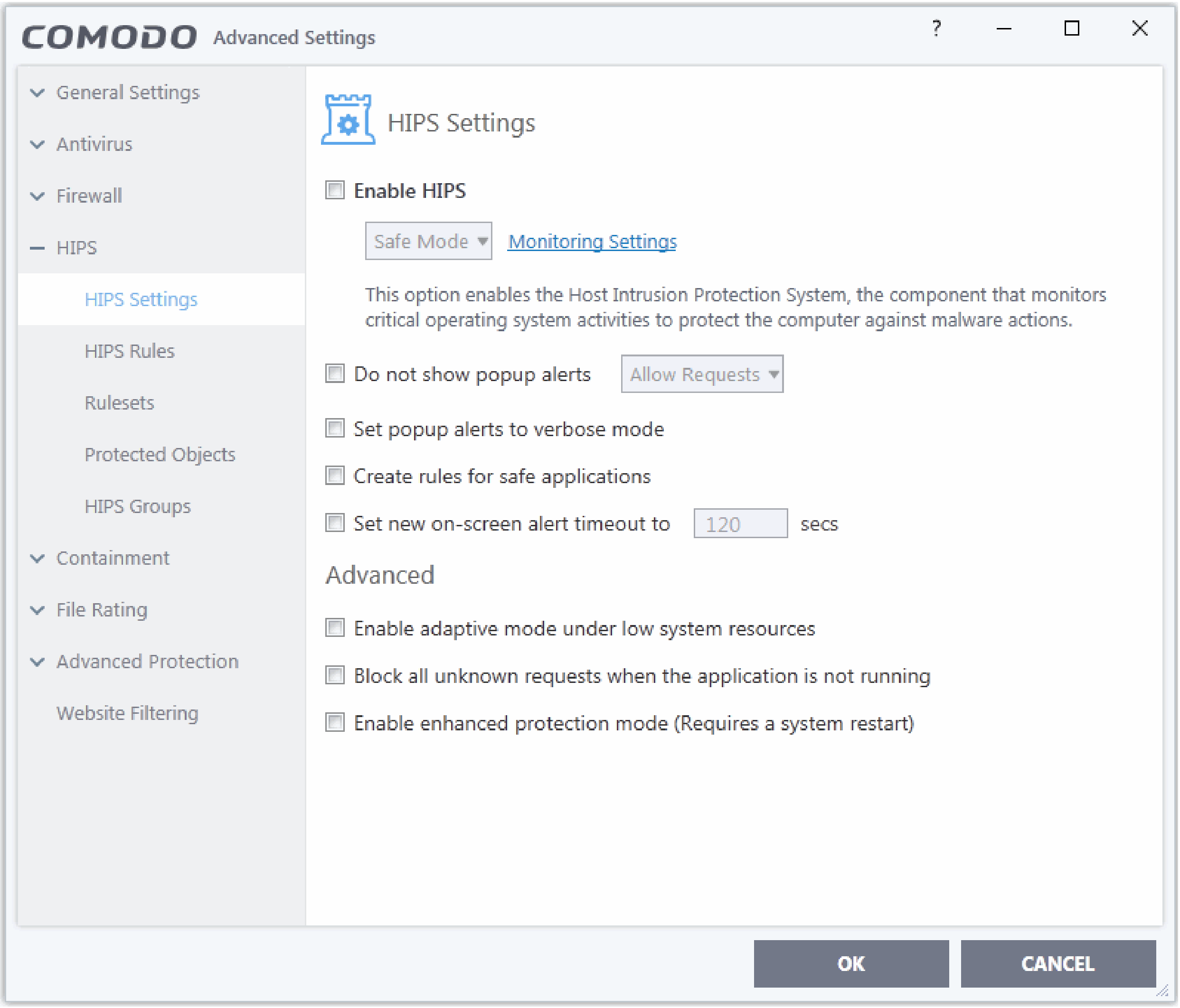
6.4. HIPS Configuration

- The Host Intrusion Protection System (HIPS) constantly monitors system activity and only allows executables and processes to run if they comply with security rules that have been enforced by the user.
- Comodo Internet Security ships with a default HIPS ruleset that work 'out of the box' - providing extremely high levels of protection without any user intervention.
  - For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modification by malicious programs.
- Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.
- The 'HIPS' section of 'Advanced Settings' lets you configure general HIPS behavior and HIPS rules.

To configure 'HIPS' components

- Click 'Settings' on the CIS home screen to open the 'Advanced Settings' interface.

- Click 'HIPS' on the left:



HIPS Settings

□ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

□ Do not show popup alerts Allow Requests ▾

□ Set popup alerts to verbose mode

□ Create rules for safe applications

□ Set new on-screen alert timeout to 120 secs

Advanced

□ Enable adaptive mode under low system resources

□ Block all unknown requests when the application is not running

□ Enable enhanced protection mode (Requires a system restart)

The 'HIPS' area has several sub-sections that allow you to configure overall behavior, define objects and object groups for protection, and define HIPS rules and rulesets.

- **HIPS Settings** - Configure settings that govern the overall behavior of the HIPS component.
- **HIPS Rules** - View, create and modify rules that determine how the applications in your system have to be protected.
- **Rulesets** - View predefined rulesets and create new rulesets that can be applied to your applications in your system.
- **Protected Objects** - Define objects to be protected by HIPS such as specific folders, system critical registry keys and so on.
- **HIPS Groups** - View and edit predefined 'Registry Groups' and 'COM Groups', create new groups so as to add them to Protected Objects.

Note for beginners:

- This section often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your computer to perform a task or function.
- Every program, application and device you run on your computer requires an executable file of some kind to start it.
- The most recognizable type of executable file is the '.exe' file. (e.g., when you start Microsoft Word, the executable file 'winword.exe' instructs your computer to start and run the Word application). Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

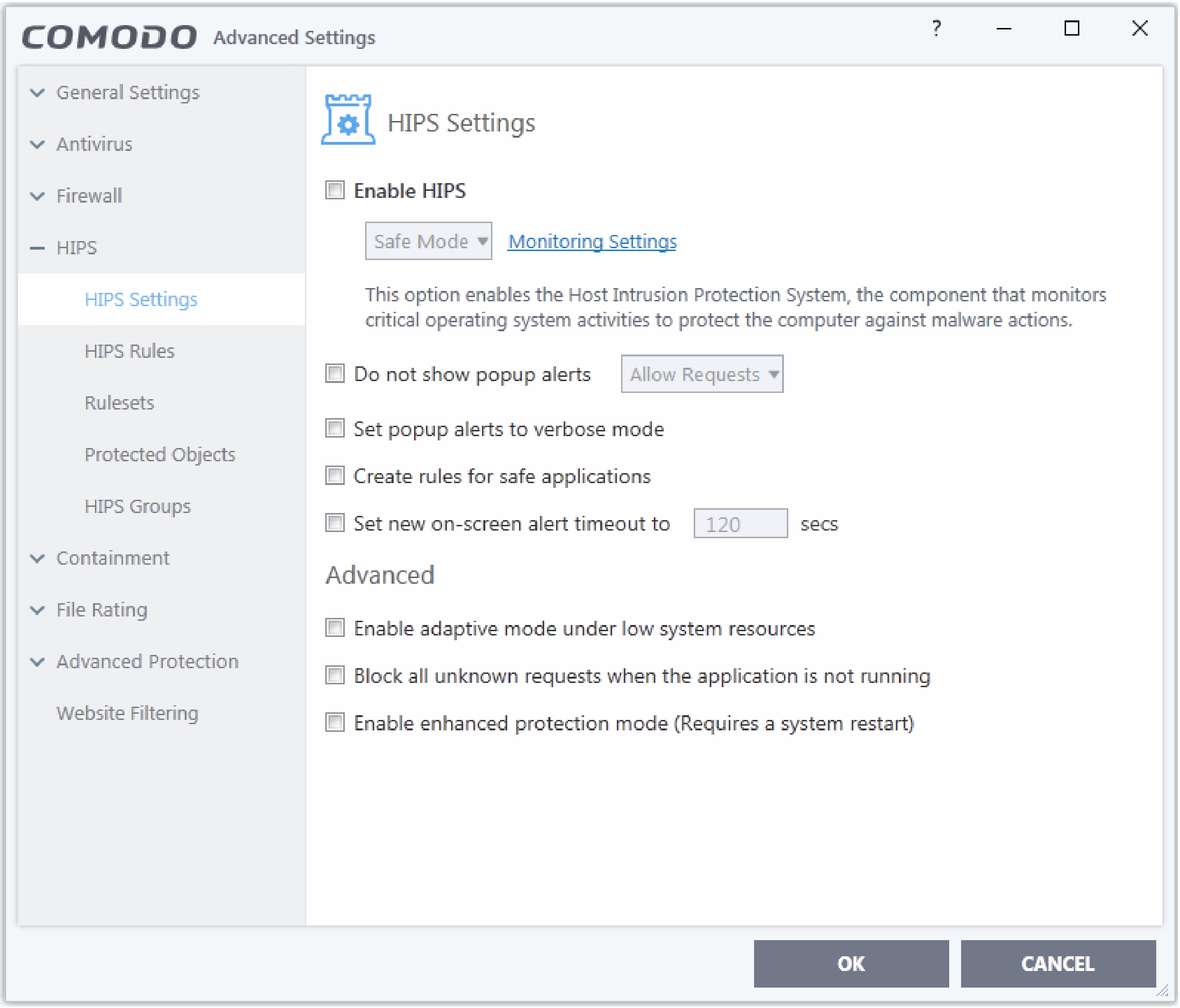
- Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data; steal your identity; corrupt system files; give control of your PC to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms

6.4.1. HIPS Settings

The HIPS settings panel allows you to enable/disable HIPS, set HIPS security level and configure HIPS' general **6.2.2. Scan Profiles**behavior.

To open the HIPS Settings panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Hips' > 'HIPS Settings' on the left.
- Alternatively, click 'HIPS' link in the 'Advanced View' of the CIS 'Home' screen.



HIPS Settings

☐ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☐ Do not show popup alerts   Allow Requests ▾

☐ Set popup alerts to verbose mode

☐ Create rules for safe applications

☐ Set new on-screen alert timeout to 120 secs

Advanced

☐ Enable adaptive mode under low system resources

☐ Block all unknown requests when the application is not running

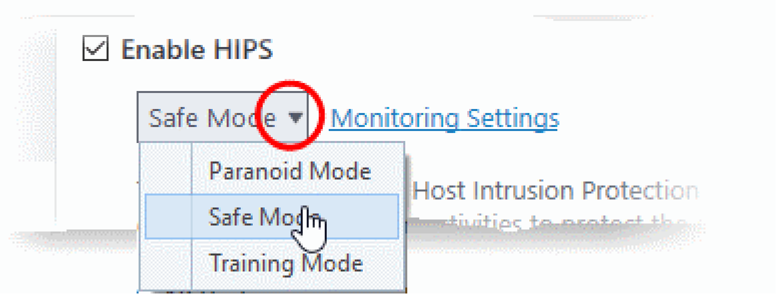
☐ Enable enhanced protection mode (Requires a system restart)

- **Enable HIPS** - Allows you to enable or disable HIPS protection. ***(Default=Disabled)***

If enabled, you can configure the HIPS security level and monitoring settings:

Configuring HIPS Security Level

The security level can be chosen from the drop-down under the 'Enable HIPS' check-box:



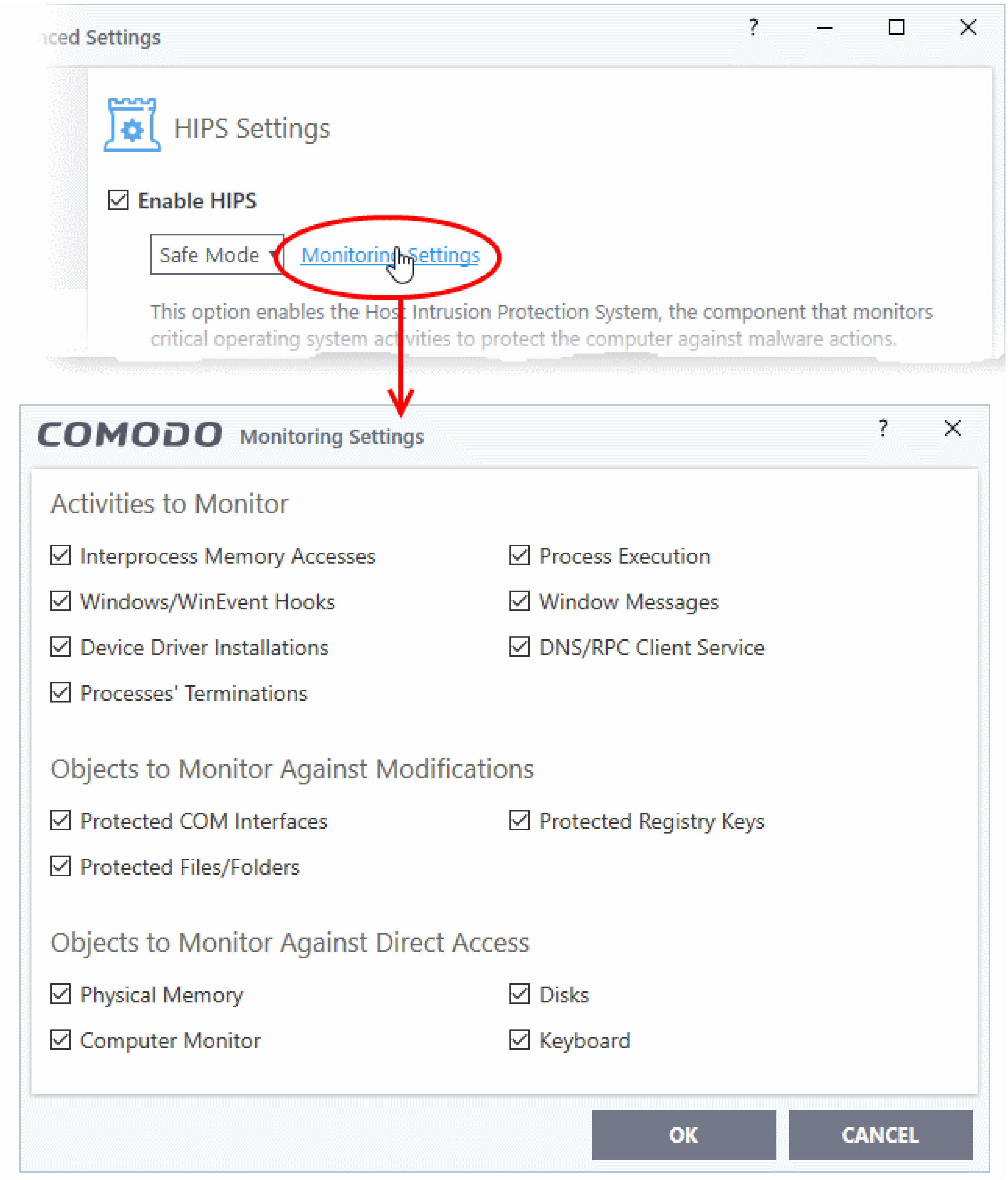
The choices available are:

- **Paranoid Mode**: This is the highest security level setting and means that HIPS monitors and controls all executable files apart from those that you have deemed safe. Comodo Internet Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses *your* configuration settings to filter critical system activity. Similarly, the Comodo Internet Security does not automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their system.
- **Safe Mode**: While monitoring critical system activity, HIPS automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules for these activities, if the checkbox '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the HIPS rules list by choosing 'Treat as' and selecting 'Allowed Application' at the alert with 'Remember my answer' checked. This instructs the HIPS not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Training Mode**: HIPS monitors and learns the activity of any and all executables and creates automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

Configuring Monitoring Settings

The activities, entities and objects that should be monitored by HIPS can be configured by clicking the Monitoring Settings link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a ***global*** basis - effectively creating a universal '**Allow**' rule for that activity . This 'Allow' setting ***over-rules*** any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the '**Access Rights**' and '**Protection Settings**' interface.



nced Settings

HIPS Settings

☑ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

COMODO Monitoring Settings

Activities to Monitor

☑ Interprocess Memory Accesses

☑ Windows/WinEvent Hooks

☑ Device Driver Installations

☑ Processes' Terminations

☑ Process Execution

☑ Window Messages

☑ DNS/RPC Client Service

Objects to Monitor Against Modifications

☑ Protected COM Interfaces

☑ Protected Files/Folders

☑ Protected Registry Keys

Objects to Monitor Against Direct Access

☑ Physical Memory

☑ Computer Monitor

☑ Disks

☑ Keyboard

Activities To Monitor:

- **Interprocess Memory Access -** Malware programs use memory space modification to inject malicious code for numerous types of attacks. These include recording your keyboard strokes; modifying the behavior of applications and stealing data by sending confidential information from one process to another. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of a compromised process to 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application ***(Default = Enabled)***.
- **Windows/WinEvent Hooks -** In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events *before* they reach an application. Example intercepted events include messages, mouse actions and keystrokes. Hooks can react to these events and, in some cases, modify or discard them. Originally developed to allow legitimate software developers to develop more powerful and

useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer and take remote control of your computer. Leaving this box checked means that you are warned every time a hook is executed by an untrusted application ***(Default = Enabled)***.

- **Device Driver Installations -** Device drivers are small programs that allow applications and/or operating systems to interact with hardware devices on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable damage to your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application ***(Default = Enabled)***.
- **Processes' Terminations -** A process is a running instance of a program. (for example, the Comodo Internet Security process is called 'cis.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your system). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, HIPS monitors and alerts you to all attempts by an untrusted application to close down another application ***(Default = Enabled)***.
- **Process Execution** - Malware such as rootkits and key-loggers often execute as background processes. With this setting enabled, HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. ***(Default = Enabled)***.
- **Windows Messages -** This setting means Comodo Internet Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) ***(Default = Enabled)***.
- **DNS/RPC Client Service -** This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby a malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed so that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' PCs which are sending out these requests without their owners' knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack ***(Default = Enabled)***.

Background Note: DNS stands for Domain Name System. It is the part of the internet infrastructure that matches a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the internet routes messages to their destinations using these IP addresses, not the domain name you type into your browser. Whenever you enter a domain name, your internet browser contacts a DNS server and makes a 'DNS Query'. In simple terms, this query is 'What is the IP address of example.com?'. The DNS server replies to your browser, telling it to connect to the IP in question.

Objects To Monitor Against Modifications:

- **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the **COM Protection** pane. ***(Default = Enabled)***
- **Protected Registry Keys** enables monitoring of Registry keys you specified from the **Registry Protection** pane. ***(Default = Enabled)***.
- **Protected Files/Folders** enables monitoring of files and folders you specified from the **File Protection** pane. ***(Default = Enabled)***.

Objects To Monitor Against Direct Access:

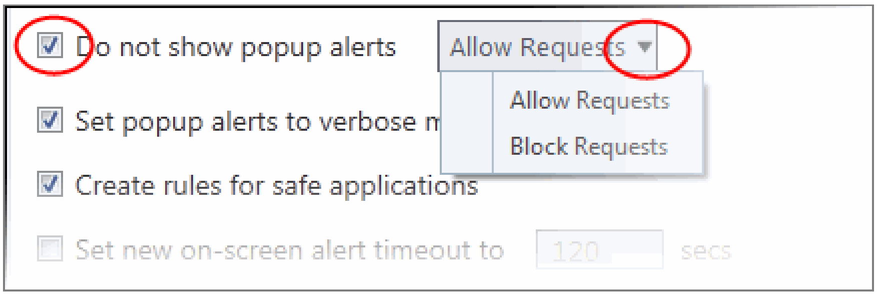
Determines whether or not Comodo Internet Security should monitor access to system critical objects on your computer. Using direct access methods, malicious applications can obtain data from storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:

- **Physical Memory:** Monitors your computer's memory for direct access by applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code ***(Default = Enabled)***.
- **Computer Monitor:** Comodo Internet Security raises an alert every time a process tries to directly access your computer monitor. Although legitimate applications sometimes require this access, spyware can also use such access to take screen shots of your current desktop, record your browsing activities and more. ***(Default = Enabled).***
- **Disks:** Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data ***(Default = Enabled)***.
- **Keyboard:** Monitors your keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Internet Security alerts you every time an application attempts to establish direct access to your keyboard ***(Default = Enabled)***.

Checkbox Options

- **Do not show popup alerts** - Configure whether or not you want to be notified when the HIPS encounters malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness ***(Default = Disabled).***

  If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Requests' or 'Allow Requests'.



☑ Do not show popup alerts   Allow Requests ▾

Allow Requests
Block Requests

☑ Set popup alerts to verbose m

☑ Create rules for safe applications

□ Set new on-screen alert timeout to 120 secs

- **Set popup alerts to verbose mode** - Enabling this option instructs CIS to display HIPS alerts in verbose mode, providing more informative alerts and more options for the user to allow or block the requests ***(Default = Disabled).***
- **Create rules for safe applications -** Automatically creates rules for safe applications in HIPS Ruleset ***(Default = Disabled).***

Note: HIPS trusts the applications if:

- The application/file is rated as 'Trusted' in the **File List**
- 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.

By default, CIS does not automatically create 'allow' rules for safe applications. This helps to reduce resource usage, to simplify the rules interface by reducing the number of 'Allow' rules, and can reduce the number of pop-up alerts. Enabling this check-box instructs CIS to begin learning the behavior of safe applications so that it can automatically generate 'Allow' rules. These rules are listed in the **HIPS Rules** interface. Advanced users can edit / modify the rules as they wish.

Background Note: Prior to version 4.x , CIS would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The automatic addition of 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CIS version 3.x).

- **Set new on-screen alert time out to**: Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced HIPS Settings

Note: These settings are recommended for advanced users only.

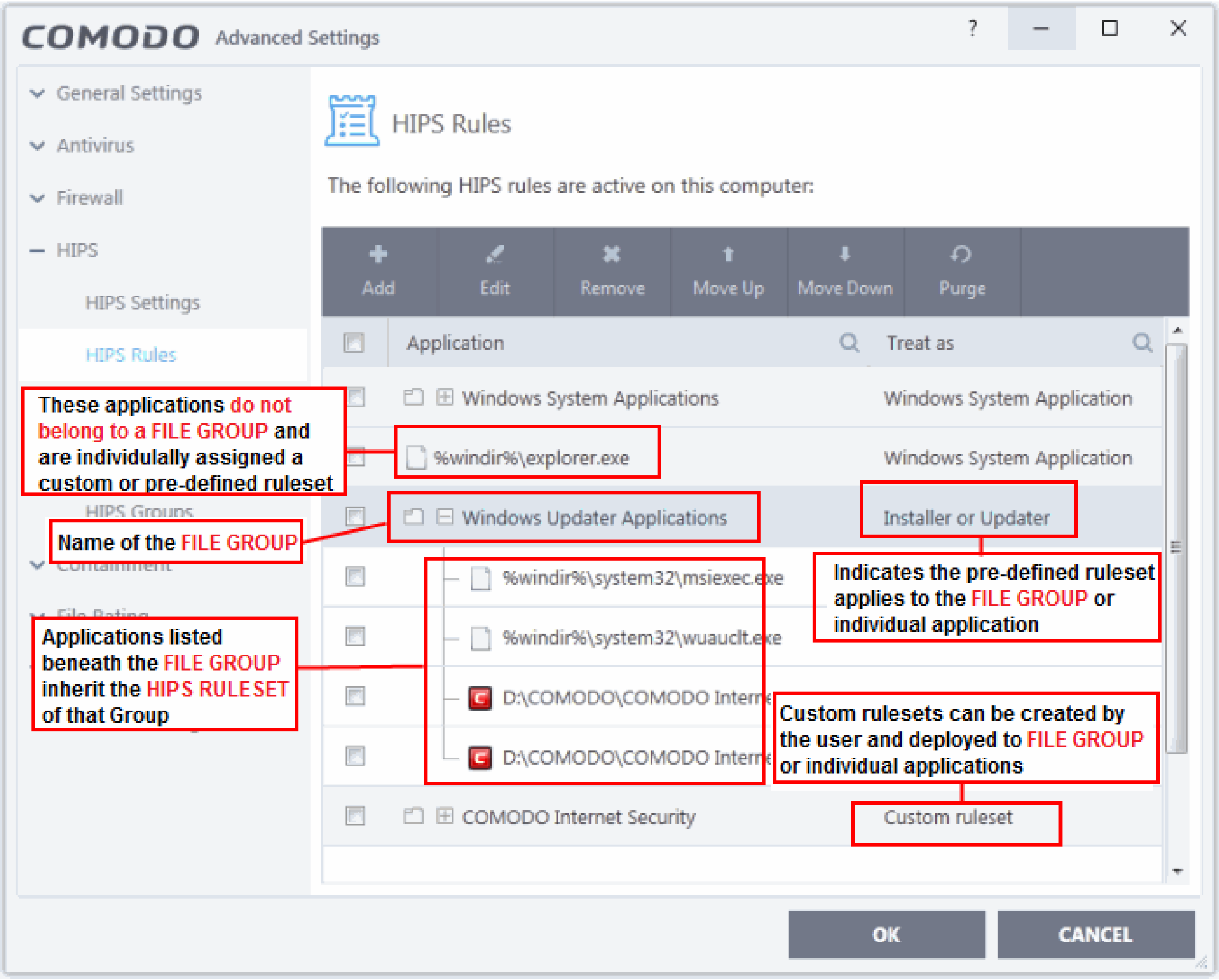
- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. With this option enabled, CIS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems ***(Default = Disabled)***.
- **Block all unknown requests when the application is not running** - Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. ***(Default = Disabled)***
- **Enable enhanced protection mode (Requires a system restart)** - On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to counteract extremely sophisticated malware that tries to bypass regular HIPS protection. Because of limitations in Windows 7/8/10 x64 systems, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. CIS requires a system restart for enabling enhanced protection mode. ***(Default = Disabled)***

6.4.2. Active HIPS Rules

The 'HIPS Rules' screen displays a list of your applications classified into file groups and the HIPS rulesets which are applied to them. This interface allows you to change the ruleset applied to a selected application or group, and create custom rulesets.

To open the HIPS Rules panel

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'HIPS Rules' on the left.



The following HIPS rules are active on this computer:

Application	Treat as
⊞ Windows System Applications	Windows System Application
%windir%\explorer.exe	Windows System Application
⊟ Windows Updater Applications	Installer or Updater
%windir%\system32\msiexec.exe	
%windir%\system32\wuauclt.exe	
D:\COMODO\COMODO Interne	
D:\COMODO\COMODO Interne	
⊞ COMODO Internet Security	Custom ruleset

These applications do not belong to a FILE GROUP and are individually assigned a custom or pre-defined ruleset

Name of the FILE GROUP

Applications listed beneath the FILE GROUP inherit the HIPS RULESET of that Group

Indicates the pre-defined ruleset applies to the FILE GROUP or individual application

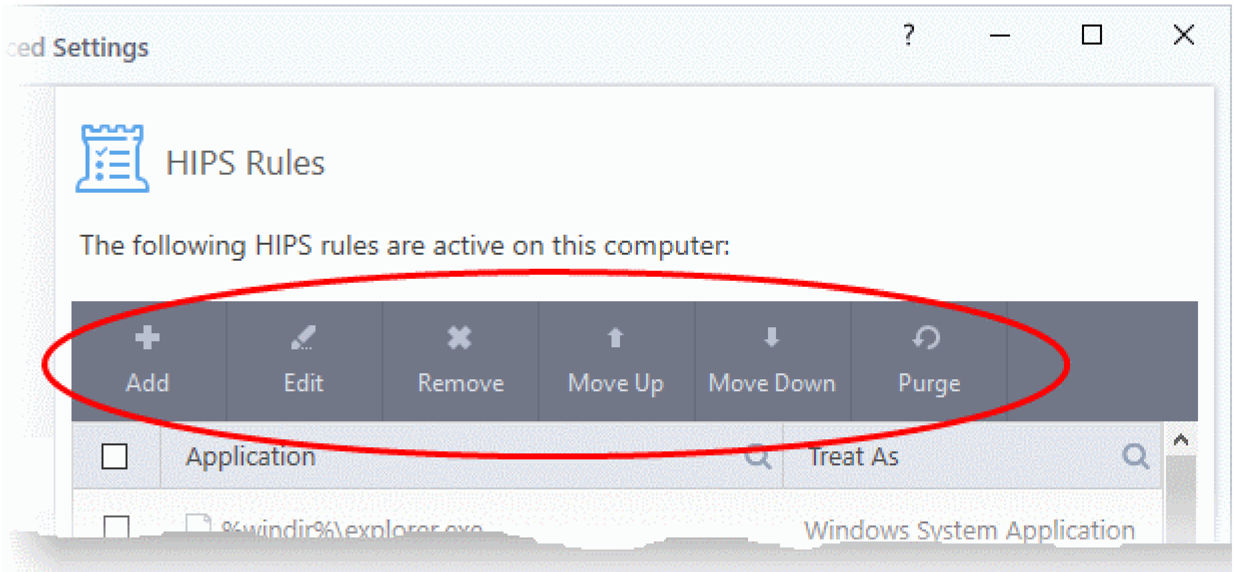
Custom rulesets can be created by the user and deployed to FILE GROUP or individual applications

The first column, **Application**, displays a list of the applications on your system for which a HIPS ruleset has been defined. If the application belongs to a file group, then all member applications assume the ruleset of the group. The second column, **Treat As**, displays the name of the HIPS ruleset assigned to the application or group of applications.

You can use the search option to find a specific file in the list by clicking the search icon at the far right of the column header and entering the name in full or part.

General Navigation:

The control buttons at the top of the list enable you to create and manage application rule sets.



The following HIPS rules are active on this computer:

Application	Treat As
%windir%\explorer.exe	Windows System Application

- **Add** - Allows the user to add a new application to the list and then create its ruleset. See '**Creating or Modifying a HIPS Ruleset**' for more details.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See '**Creating or Modifying a HIPS Ruleset**' for more details.
- **Remove** - Deletes the selected ruleset.

> **Note**: You cannot add or remove individual applications from a file group using this interface - you must use the '**File Groups**' interface to do this.

- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move UP/Move Down** - Users can re-order the priority of rules by simply selecting an application name or file group and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the '**File Groups'** interface.

Creating or Modifying a HIPS Ruleset

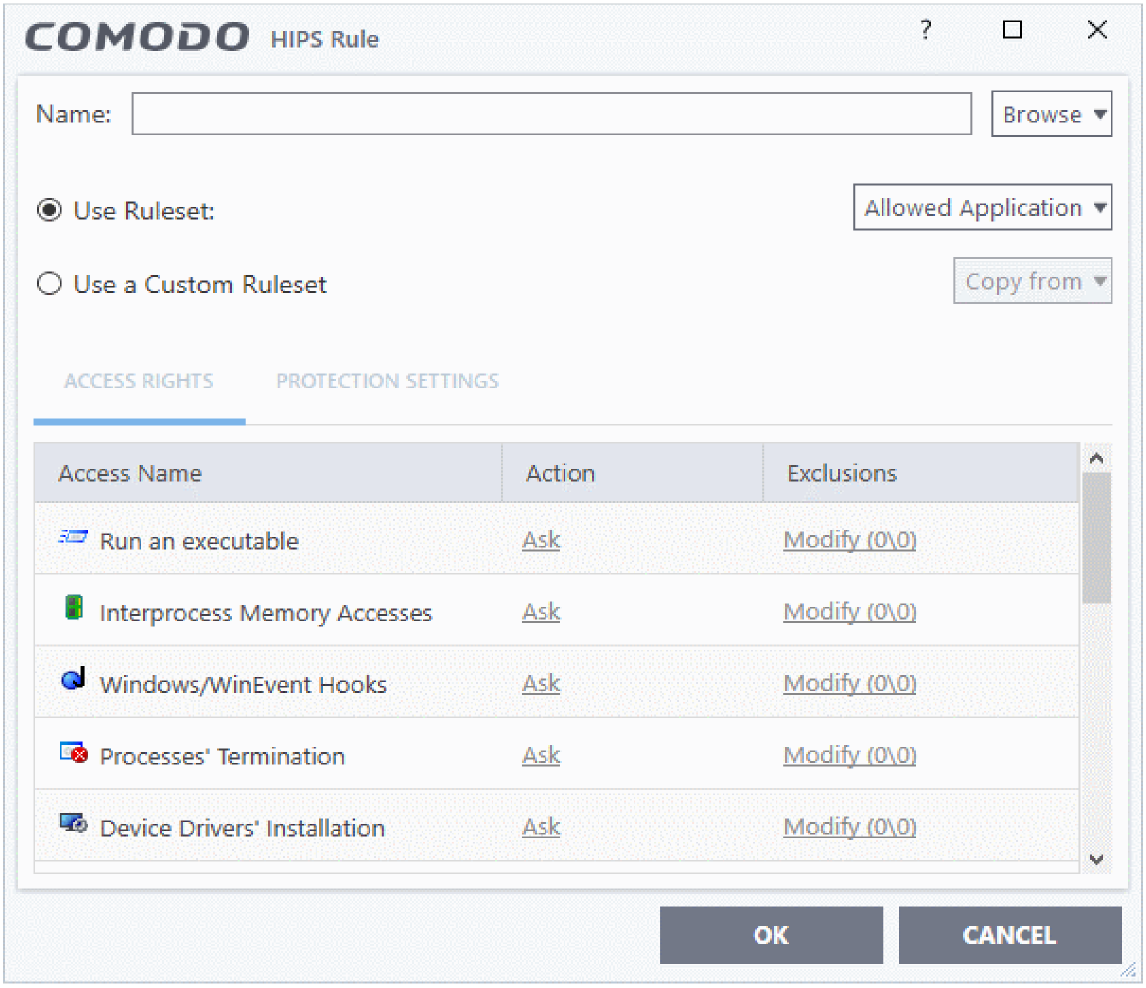
Defining a HIPS Ruleset for an application or File group involves two steps:

1. **Select the application or file group that you wish the ruleset to apply to.**
2. **Configure the ruleset for this application.**

Step 1 - Select the application or file group that you wish the ruleset to apply to

- To define a rule for a new application (i.e. one that is not already listed), click the 'Add' button at the top of the **HIPS Rules pane**.

This brings up the 'HIPS Rule' interface as shown below.



COMODO HIPS Rule

Name: [ ] Browse

● Use Ruleset: Allowed Application

○ Use a Custom Ruleset Copy from

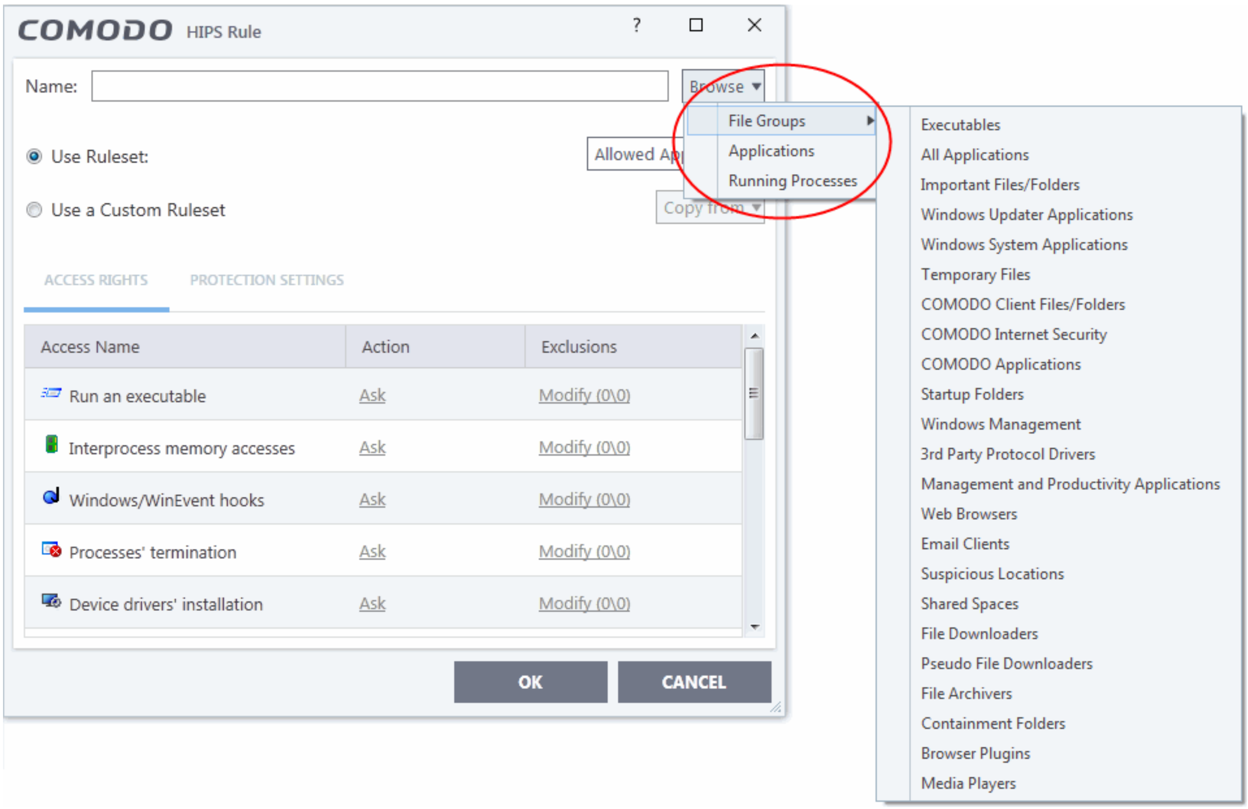
Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)

The 'Name' box is blank because you are defining a HIPS rule settings for a new application. If you were editing an existing rule, this field would show the application name and its installation path, or the application group name.

- Click 'Browse' to begin.

You now have 3 methods available to choose the application for which you wish to create a Ruleset - **File Groups**; **Applications** and **Running Processes**.

1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl *\cmd.exe, *.bat, *.cmd. Other such categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.



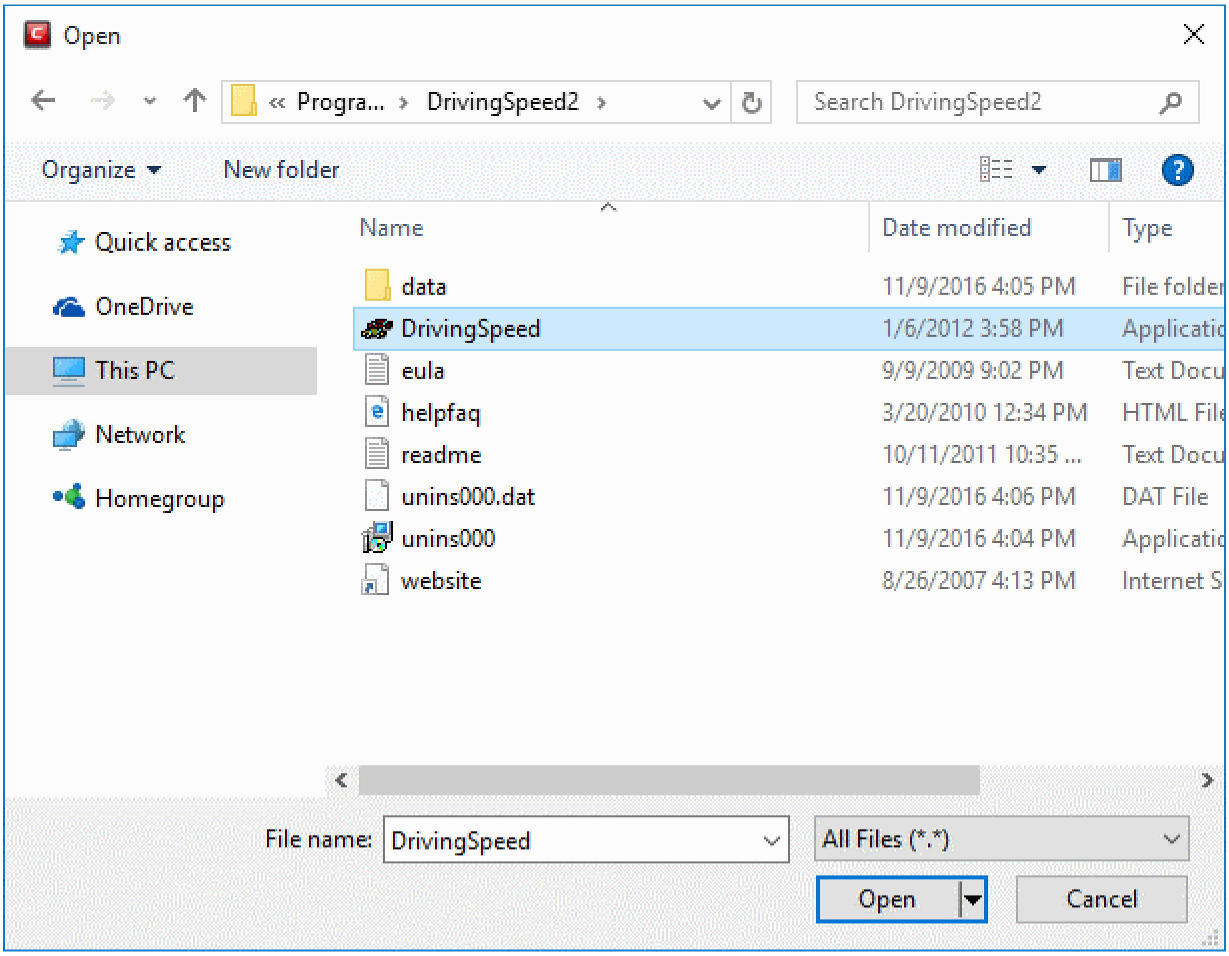
● Use Ruleset: Allowed Ap

○ Use a Custom Ruleset

Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess memory accesses	Ask	Modify (0\0)
Windows/WinEvent hooks	Ask	Modify (0\0)
Processes' termination	Ask	Modify (0\0)
Device drivers' installation	Ask	Modify (0\0)

To view the file types and folders that are affected by choosing one of these options, you need to visit the '**File Groups**' interface.

2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.

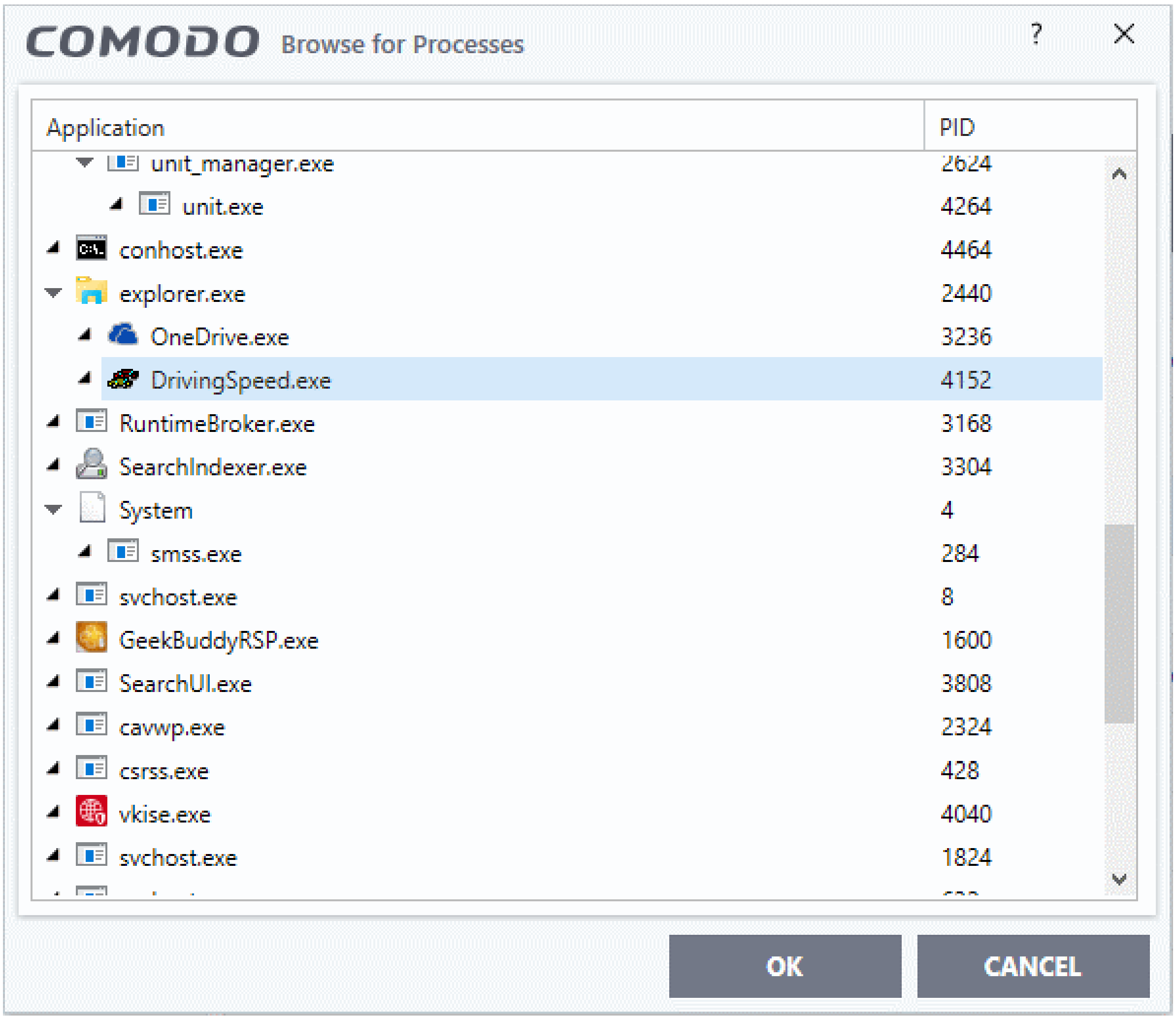


Name	Date modified	Type
data	11/9/2016 4:05 PM	File folder
DrivingSpeed	1/6/2012 3:58 PM	Applicatio
eula	9/9/2009 9:02 PM	Text Docu
helpfaq	3/20/2010 12:34 PM	HTML File
readme	10/11/2011 10:35 ...	Text Docu
unins000.dat	11/9/2016 4:06 PM	DAT File
unins000	11/9/2016 4:04 PM	Applicatio
website	8/26/2007 4:13 PM	Internet S

File name: DrivingSpeed

All Files (*.*)

3. **Running Processes -** as the name suggests, this option allows you choose any process that is currently running on your PC in order to create and deploy a ruleset for its parent application.



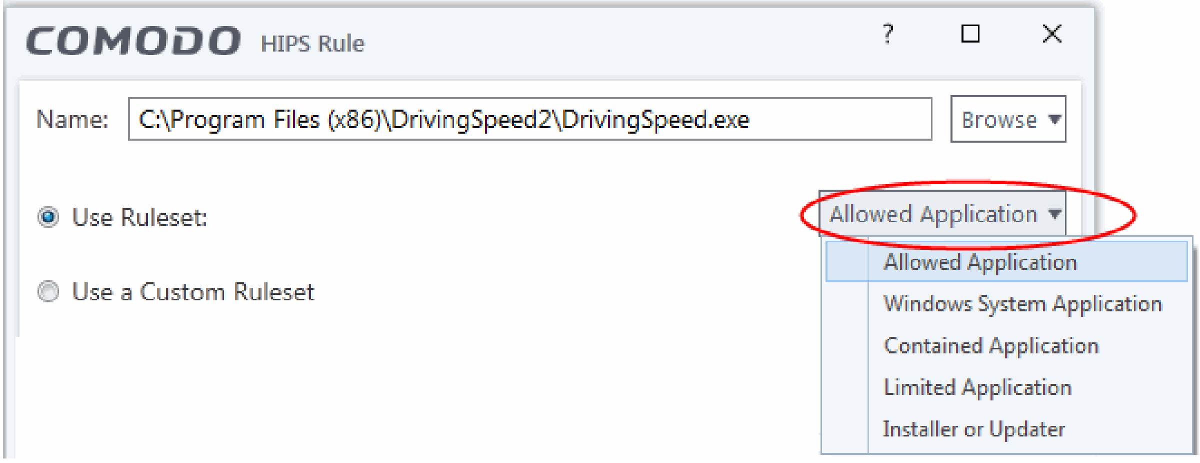
Application	PID
unit_manager.exe	2624
unit.exe	4264
conhost.exe	4464
explorer.exe	2440
OneDrive.exe	3236
DrivingSpeed.exe	4152
RuntimeBroker.exe	3168
SearchIndexer.exe	3304
System	4
smss.exe	284
svchost.exe	8
GeekBuddyRSP.exe	1600
SearchUI.exe	3808
cavwp.exe	2324
csrss.exe	428
vkise.exe	4040
svchost.exe	1824

Having selected the individual application, running process or file group, the next stage is to configure the rules for this ruleset.

Step 2 - Configure the HIPS Ruleset for this application

There are two broad options available for selecting a ruleset that applies to an application - **Use Ruleset** or **Use a Custom Ruleset**.

1. **Use Ruleset** - Selecting this option allows you to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the **HIPS Rules** interface ***(Default = Enabled).***



Name: C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

● Use Ruleset: Allowed Application

○ Use a Custom Ruleset

Note on 'Installer or Updater' Rule : Applying this rule to an application defines it as a trusted installer. All files created by this application will also be trusted. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo advises you to use this 'Predefined Ruleset' - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.

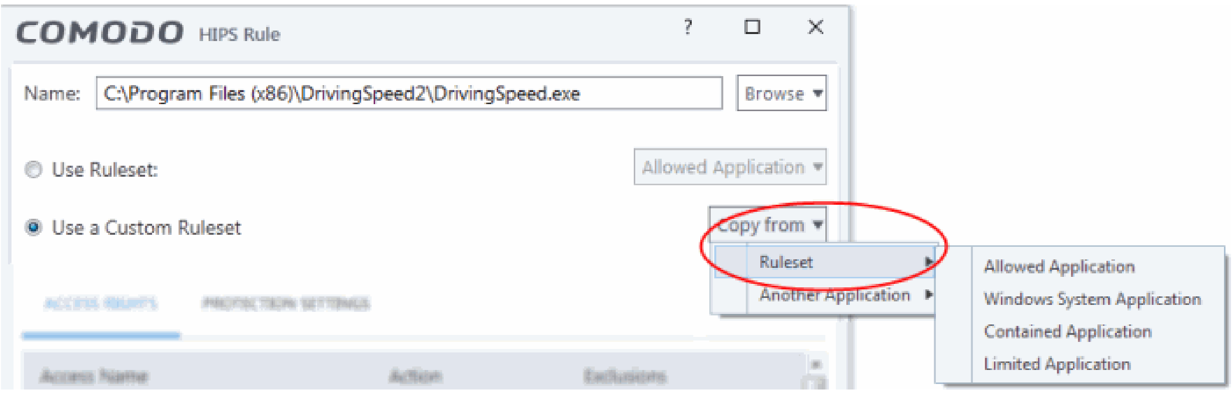
General Note: Predefined Rulesets cannot be modified directly from this interface - they can only be modified and defined using the '**Rulesets**' interface. If you require the ability to add or modify settings for a specific application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use a Custom Ruleset** option instead.

2. **Use a Custom Ruleset** - Designed for more experienced users, the 'Custom Ruleset' option grants full control over the configuration of each rule within that ruleset.

   The custom ruleset has two main configuration areas - **Access Rights** and **Protection Settings**.

   In simplistic terms 'Access Rights' determine what the application *can do to other processes* and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

Tip: You can use the 'Copy from' drop-down to choose an existing rule set for an application or file group. Using that as a starting point, you can customize the 'Access Rights' and 'Protection Settings' for the rules as required.



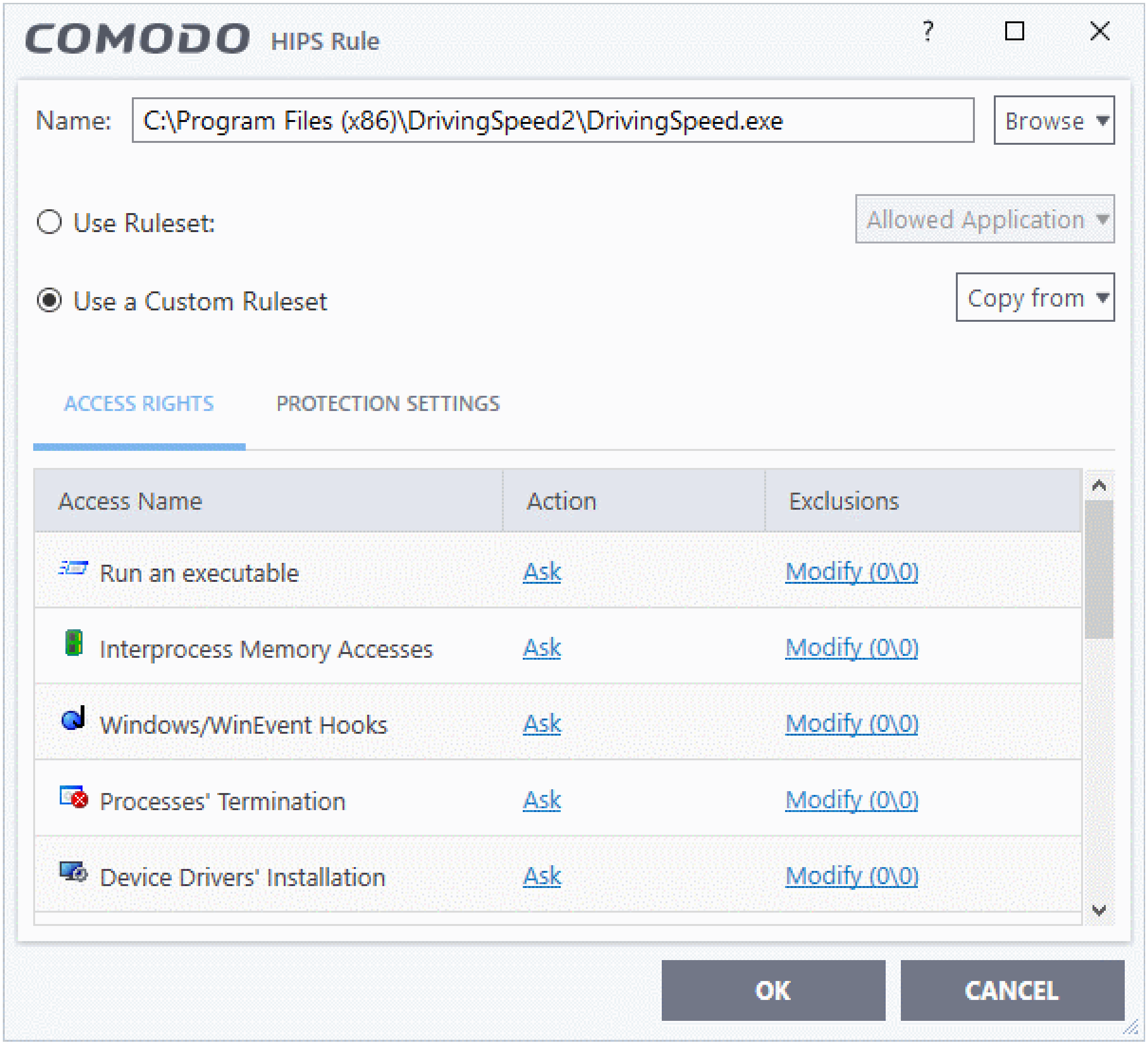
COMODO HIPS Rule

Name: C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

○ Use Ruleset: Allowed Application

● Use a Custom Ruleset

i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset. These activities are called 'Access Names'.



COMODO HIPS Rule

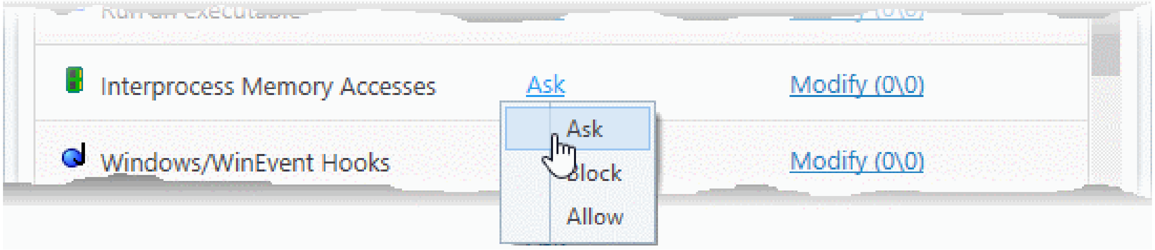
Name: C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

○ Use Ruleset: Allowed Application

● Use a Custom Ruleset

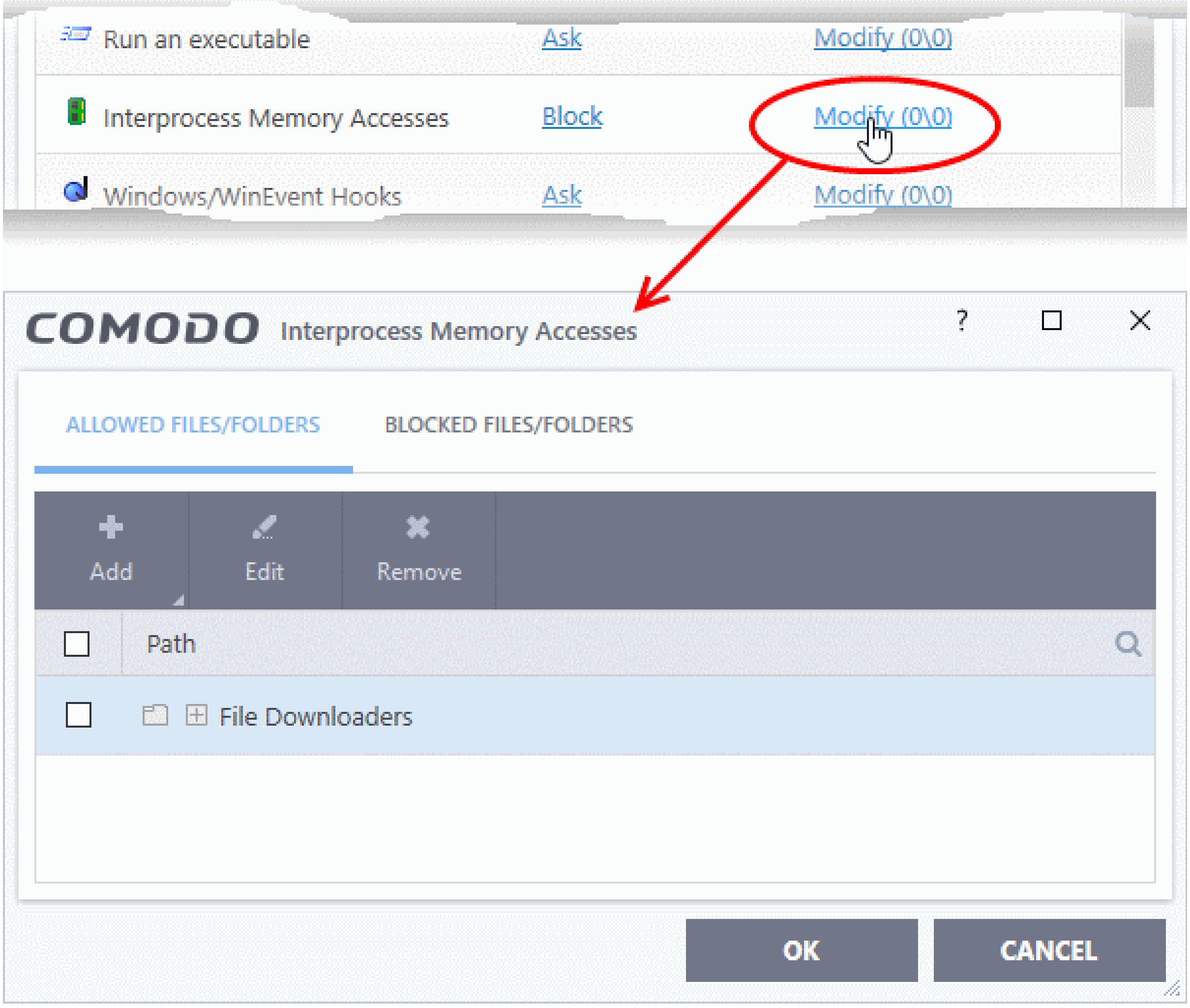
Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)

See **HIPS Settings > Activities to Monitor** to see definitions of the 'Action Names' listed above, and the implications of choosing 'Ask', 'Allow' or 'Block':



Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks		Modify (0\0)

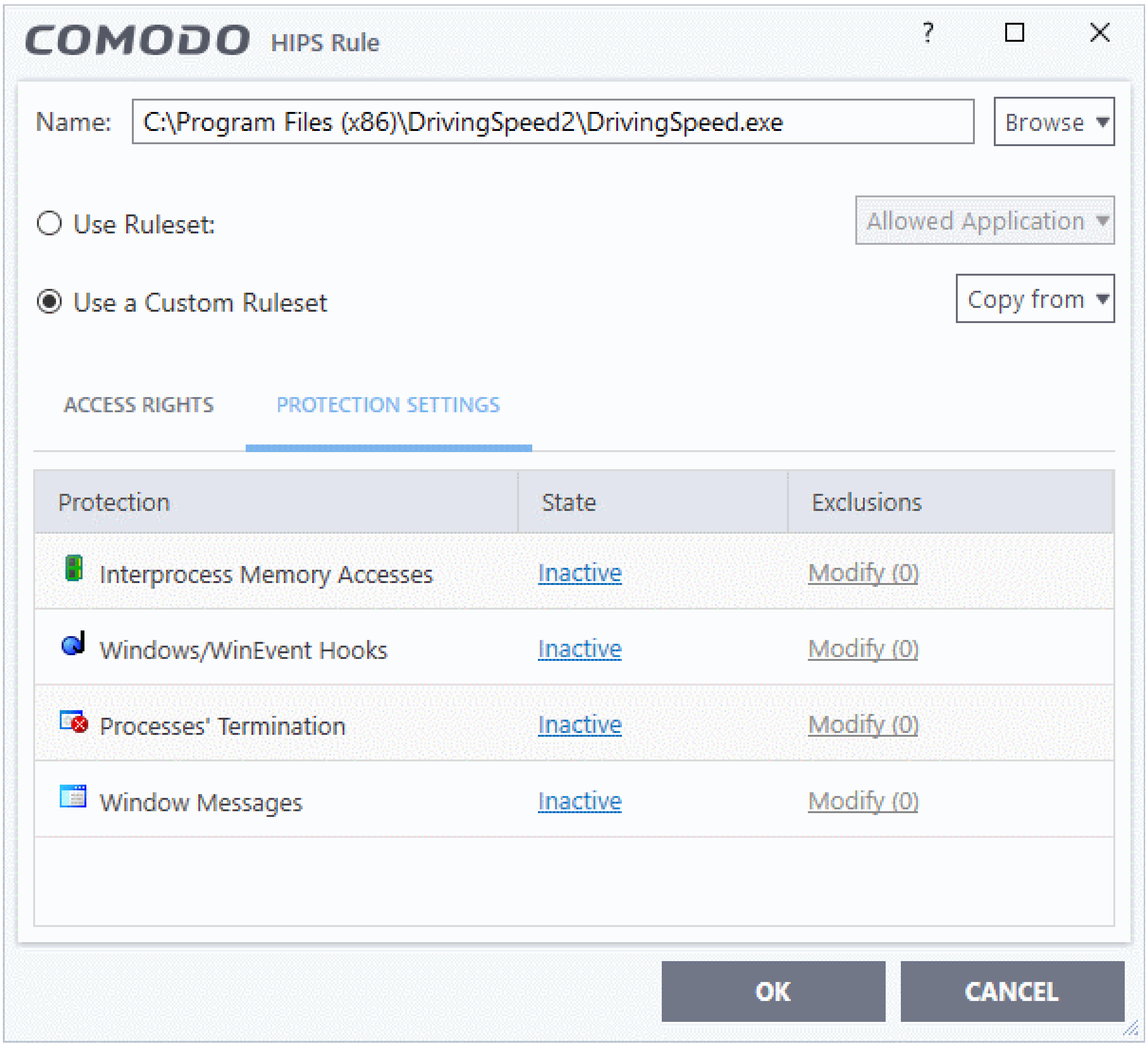
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.



Clicking the 'Add' button at the top allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

In **the example above**, the default action for 'Interprocess Memory Access' is 'Block'. This means HIPS will block the action if 'DrivingSpeed.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'File Downloaders' File Group to the 'Allowed Files\Folders' area creates an exception to this rule. 'DrivingSpeed.exe' can now modify the memory space of files belonging to the 'File Downloaders' File Group.

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



Name: C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

○ Use Ruleset: Allowed Application

● Use a Custom Ruleset

Protection	State	Exclusions
Interprocess Memory Accesses	Inactive	Modify (0)
Windows/WinEvent Hooks	Inactive	Modify (0)
Processes' Termination	Inactive	Modify (0)
Window Messages	Inactive	Modify (0)

- Set the 'State' as 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

6.4.3. HIPS Rule Sets

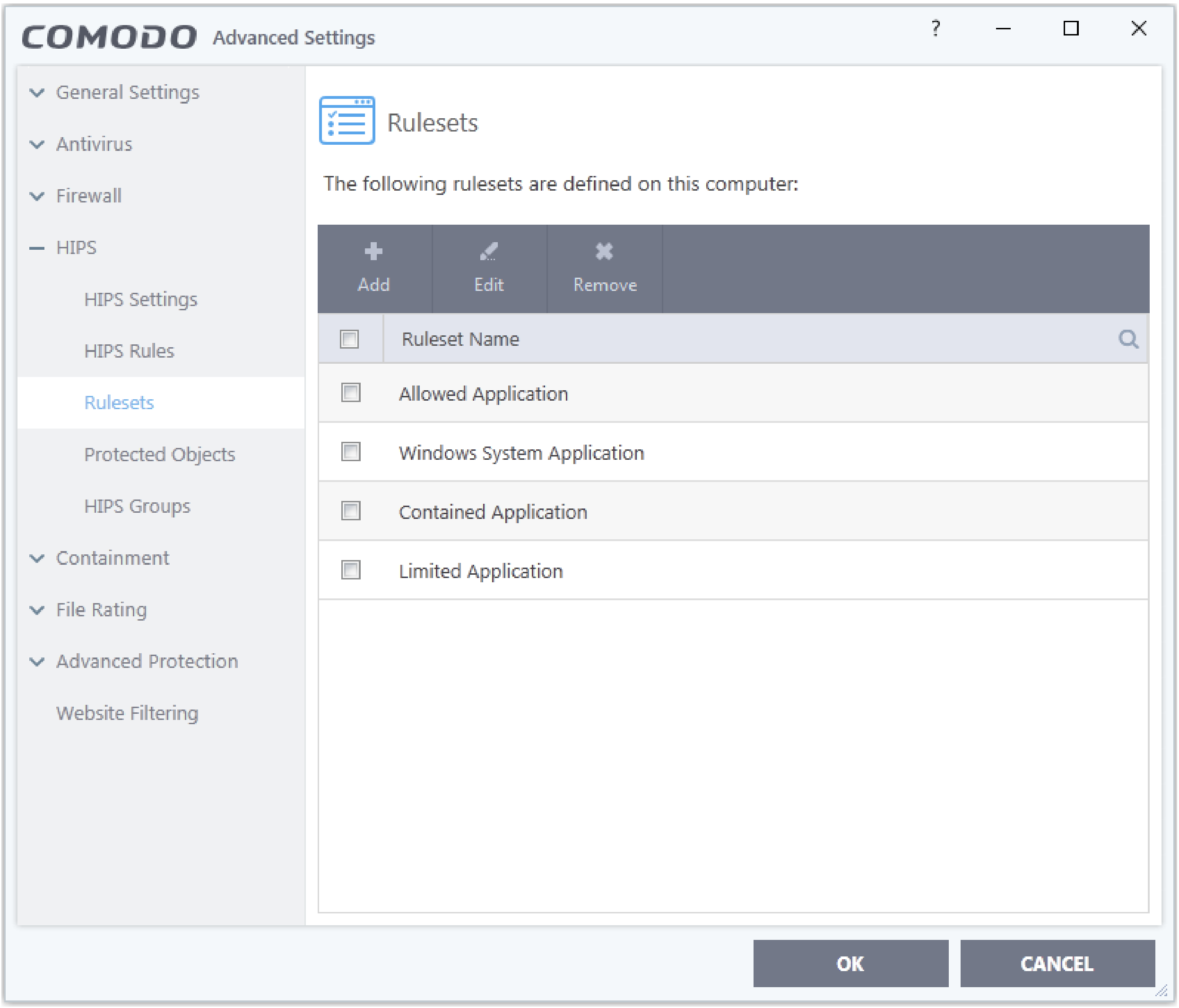
A ruleset is a set of **access rights and protection settings** that can be deployed to control applications or application groups. Each ruleset consists of a number of rules and each of these rules is defined by a set of conditions and parameters. Rulesets govern an application's rights to access memory, other programs, the registry etc.

Note: This section is for advanced users. If you are new CIS user, we advise you first read the **Active HIPS Rules** section in this help guide.

Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Internet Security contains a selection of pre-defined rulesets which implement optimal security settings for a range of application types. Users can, of course, modify these predefined rulesets to suit their requirements.

To view the list of HIPS Rulesets

- Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'Rulesets' on the left.



Rulesets

The following rulesets are defined on this computer:

□	Ruleset Name
□	Allowed Application
□	Windows System Application
□	Contained Application
□	Limited Application

You can search for a specific ruleset by clicking the search icon and typing the rulesets name in full or part.

To view or edit a ruleset

- Double click on the 'Ruleset' in the list

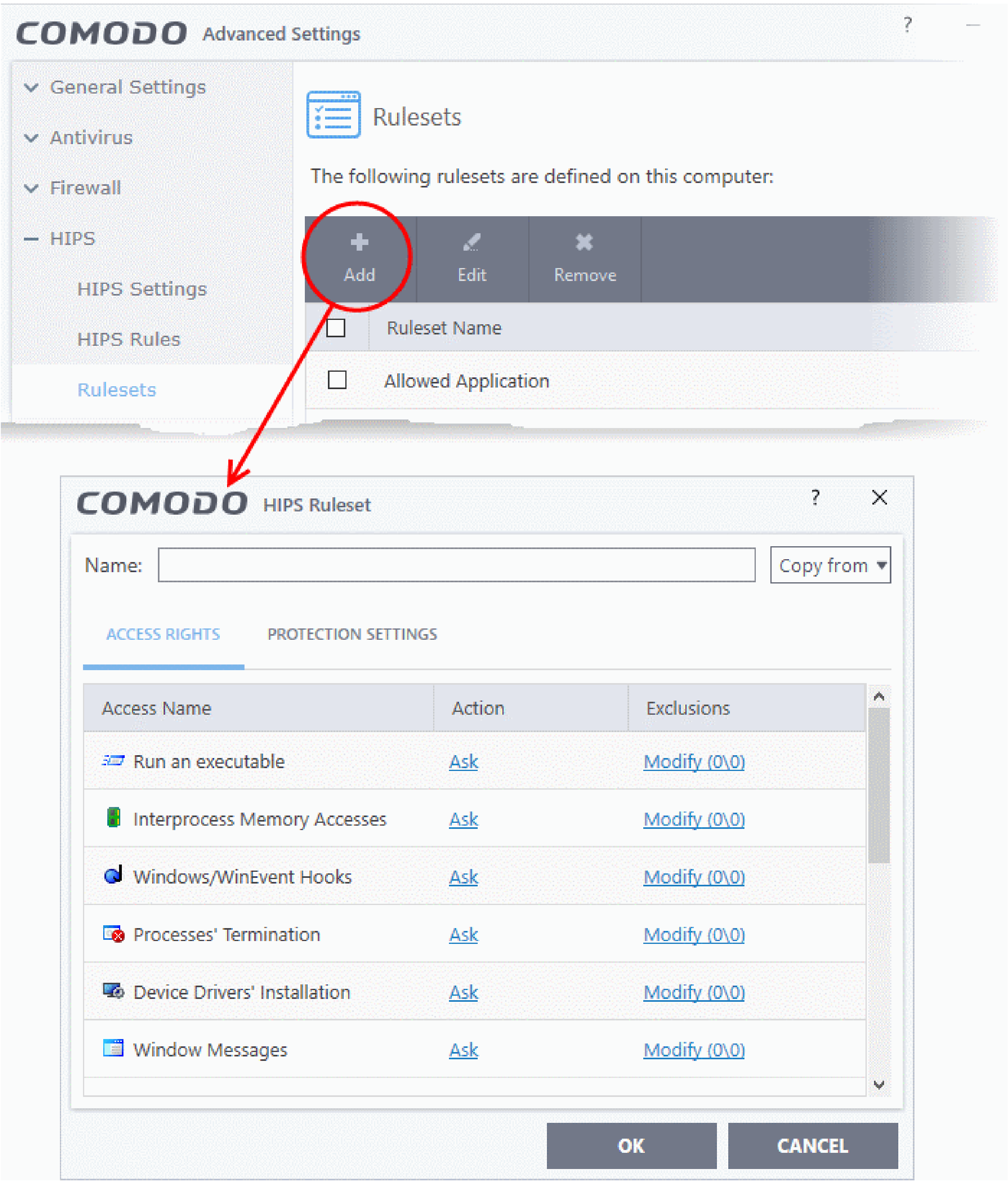
  or

- Select the 'Ruleset' and click the 'Edit' button at the top of the interface

From here, you can make changes to its **'Access Rights' and 'Protection Settings'**. Any changes you make here are automatically rolled out to all applications that are covered by the ruleset.

To create a new ruleset

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



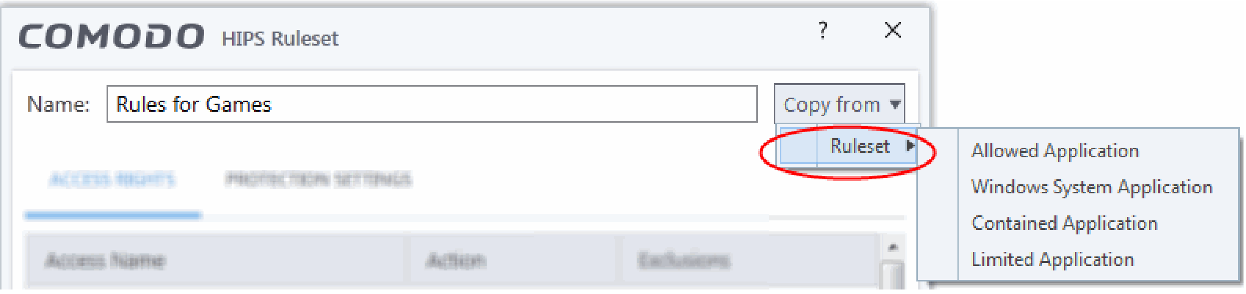
The following rulesets are defined on this computer:

	Ruleset Name
□	Allowed Application

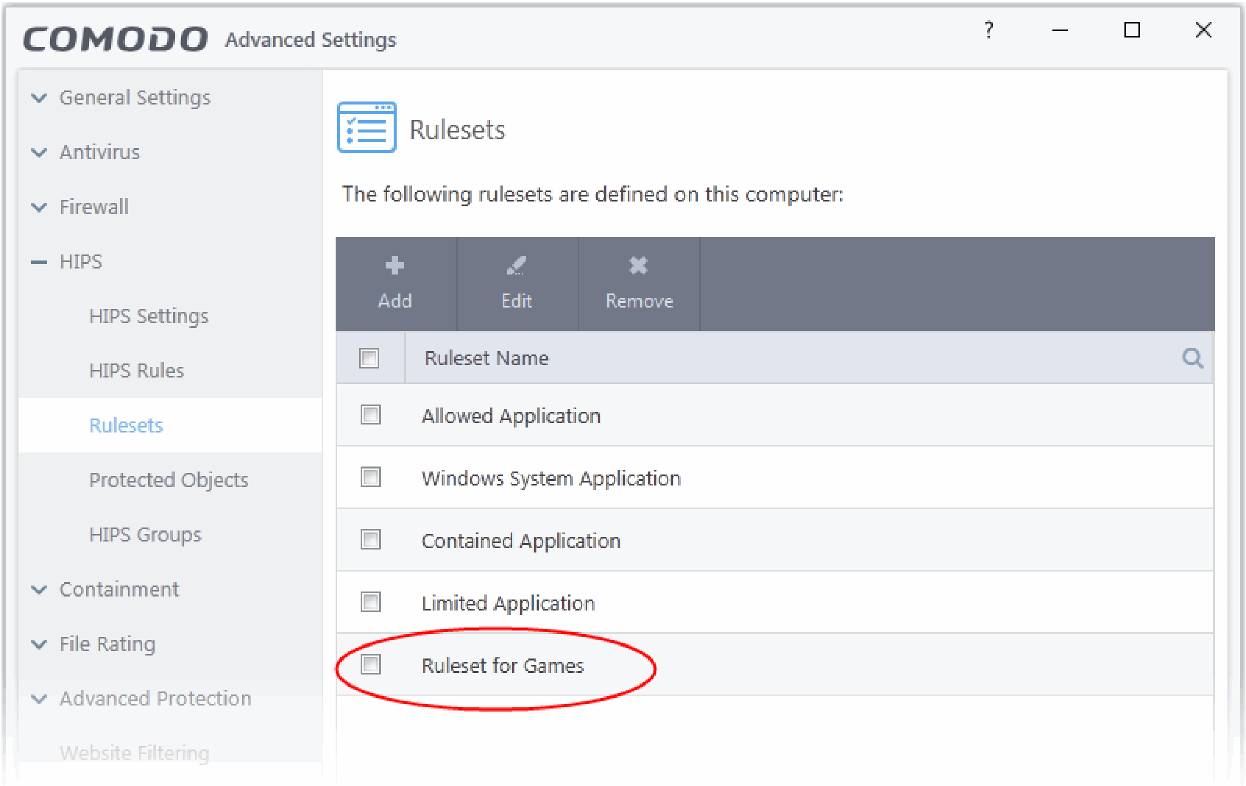
Name:

Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)

- Enter a name for the new ruleset.
- To copy the **Access Rights** and **Protection Settings** from an existing ruleset, click 'Copy From' and choose the ruleset from the drop-down.



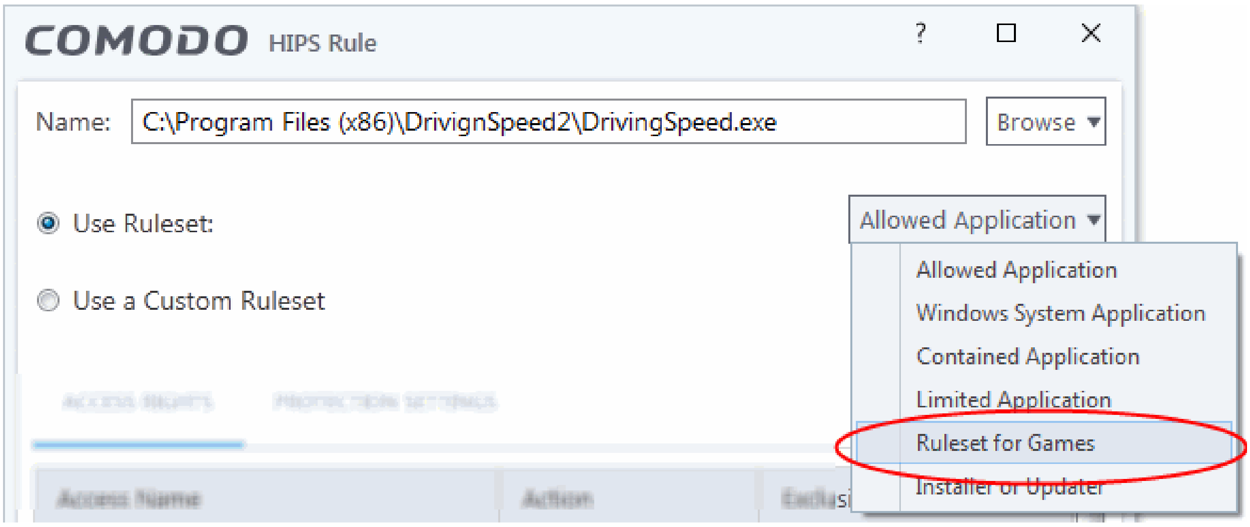
- To customize the **Access Rights** and **Protection Settings** of this new rule set, follow the procedure explained under **Use a Custom Ruleset** in the section **Active HIPS Rules**.
- Click 'OK' to save the new ruleset.



The following rulesets are defined on this computer:

□	Ruleset Name
□	Allowed Application
□	Windows System Application
□	Contained Application
□	Limited Application
□	Ruleset for Games

Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.



Name: C:\Program Files (x86)\DrivignSpeed2\DrivingSpeed.exe

● Use Ruleset: Allowed Application

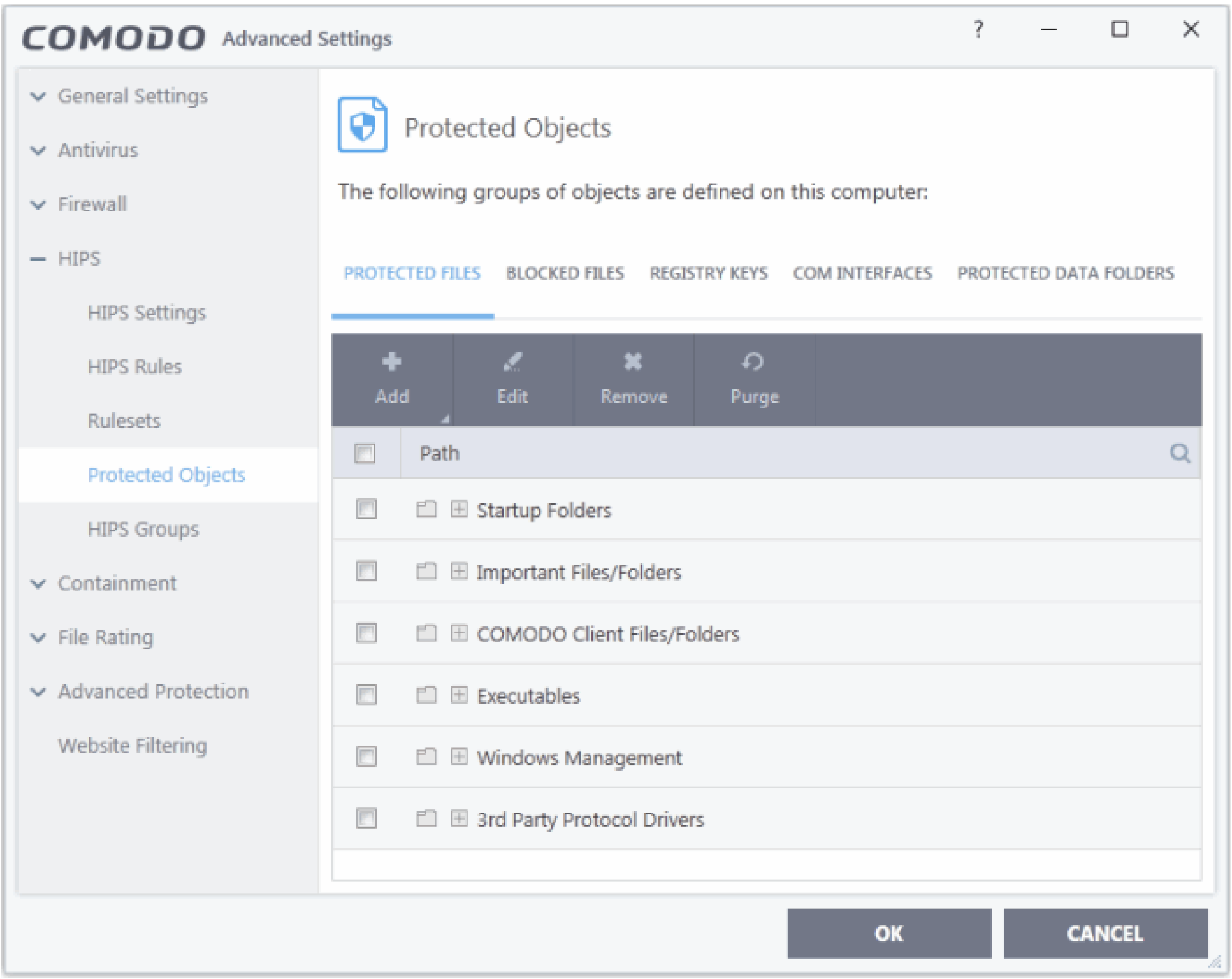
○ Use a Custom Ruleset

6.4.4. Protected Objects

The 'Protected Objects' interface allows you to protect specific files, folders, registry keys and COM interfaces against access or modification by unauthorized processes. You can also specify data folders to be protected so that contained programs cannot access them.

To open the 'Protected Objects' interface

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'Protected Objects' on the left



The following groups of objects are defined on this computer:

	Path
□	Startup Folders
□	Important Files/Folders
□	COMODO Client Files/Folders
□	Executables
□	Windows Management
□	3rd Party Protocol Drivers

The 'Protected Objects' interface has the following sub-sections:

- **Protected Files** - Allows you to specify programs, applications and files that are to be protected from changes
- **Blocked Files** - Allows you to specify programs, applications and files that should be prevented from executing
- **Registry Keys** - Allows you to specify registry keys that should be protected from changes
- **COM Interfaces** - Allows you to specify COM interfaces that are to be protected from changes
- **Protected Data Folders** - Allows you prevent contained programs from accessing files inside specific, protected folders.

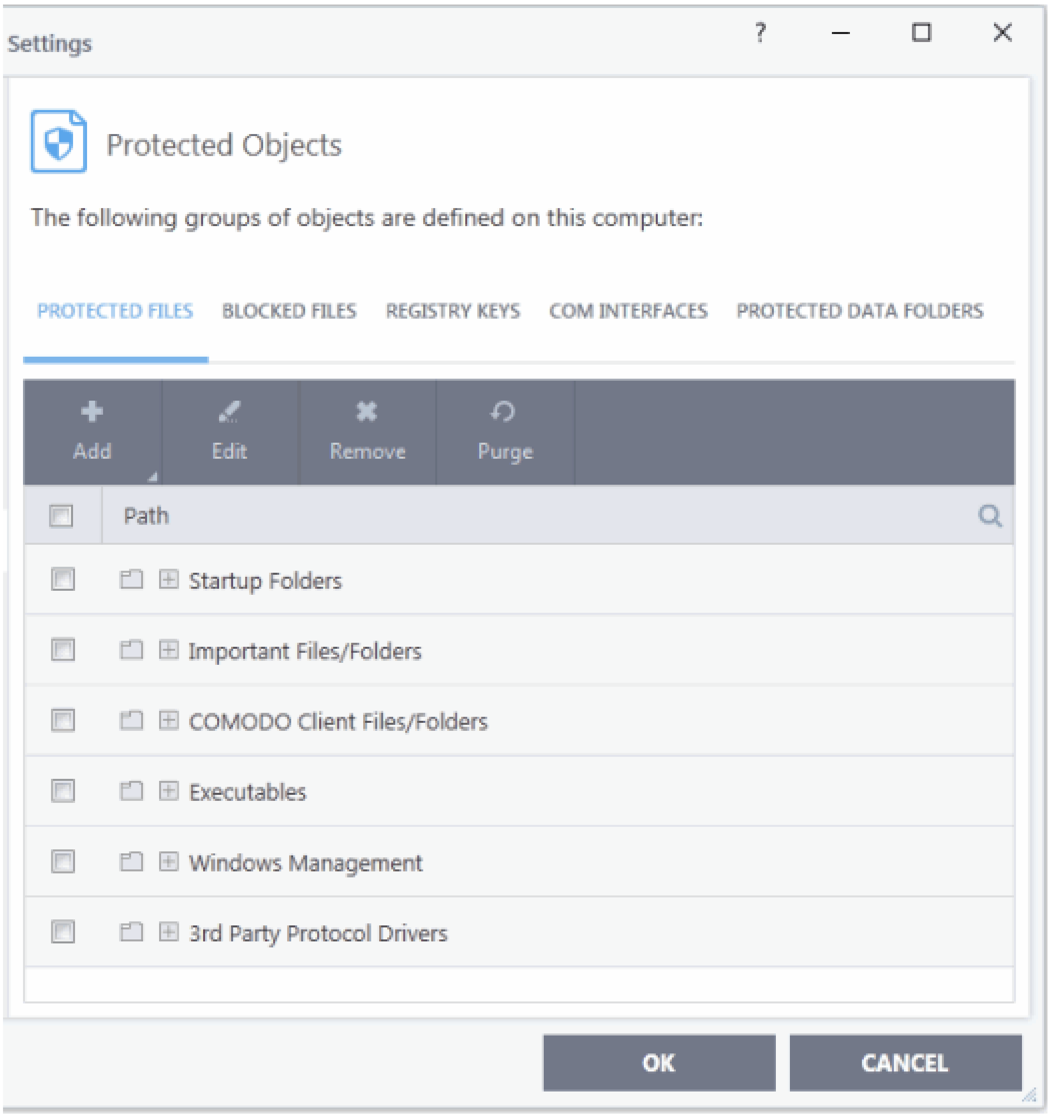
6.4.4.1. Protected Files

- The 'Protected Files' screen displays a list of file groups which are protected from access by other programs.

- This prevents malicious programs from gaining access to important personal or system data. It is also useful for safeguarding valuable files (spreadsheets, databases, documents) against accidental or deliberate sabotage.
- If a file is 'Protected' it can still be accessed and read, but cannot be altered.
- A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Placing your host file in 'Protected Files and Folders' area will allow web browsers to use the file as normal, but any attempt to modify it will be blocked.
- You can create exceptions if you want to allow a trusted application to access a protected file. See **Exceptions** for more details about how to allow access to files placed in 'Protected Files'.

To open the 'Protected Files' section

- Click 'Settings' from the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'Protected Objects' on the left
- Click the 'Protected Files' tab



□	Path
□	⊞ Startup Folders
□	⊞ Important Files/Folders
□	⊞ COMODO Client Files/Folders
□	⊞ Executables
□	⊞ Windows Management
□	⊞ 3rd Party Protocol Drivers

The buttons at the top provide the following options:

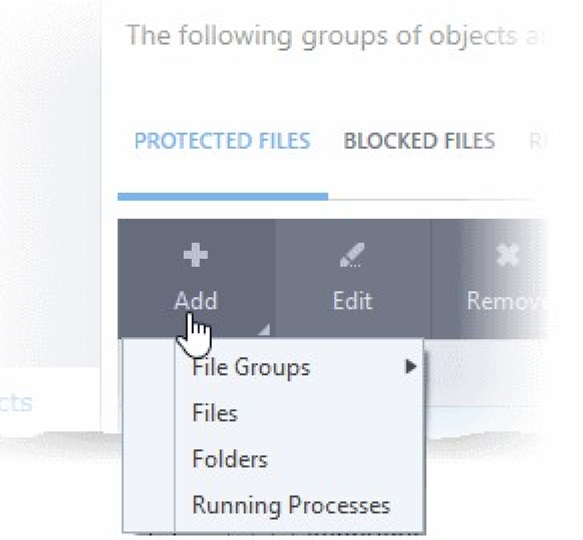
- **Add** - Allows you to add individual files, programs and applications to 'Protected Files'.
- **Edit** - Allows you to edit the path of the file or group of a selected item
- **Remove** - Deletes the currently highlighted file or file group.

- **Purge -** Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

To manually add an individual file, folder, file group or process

- Click the 'Add' button

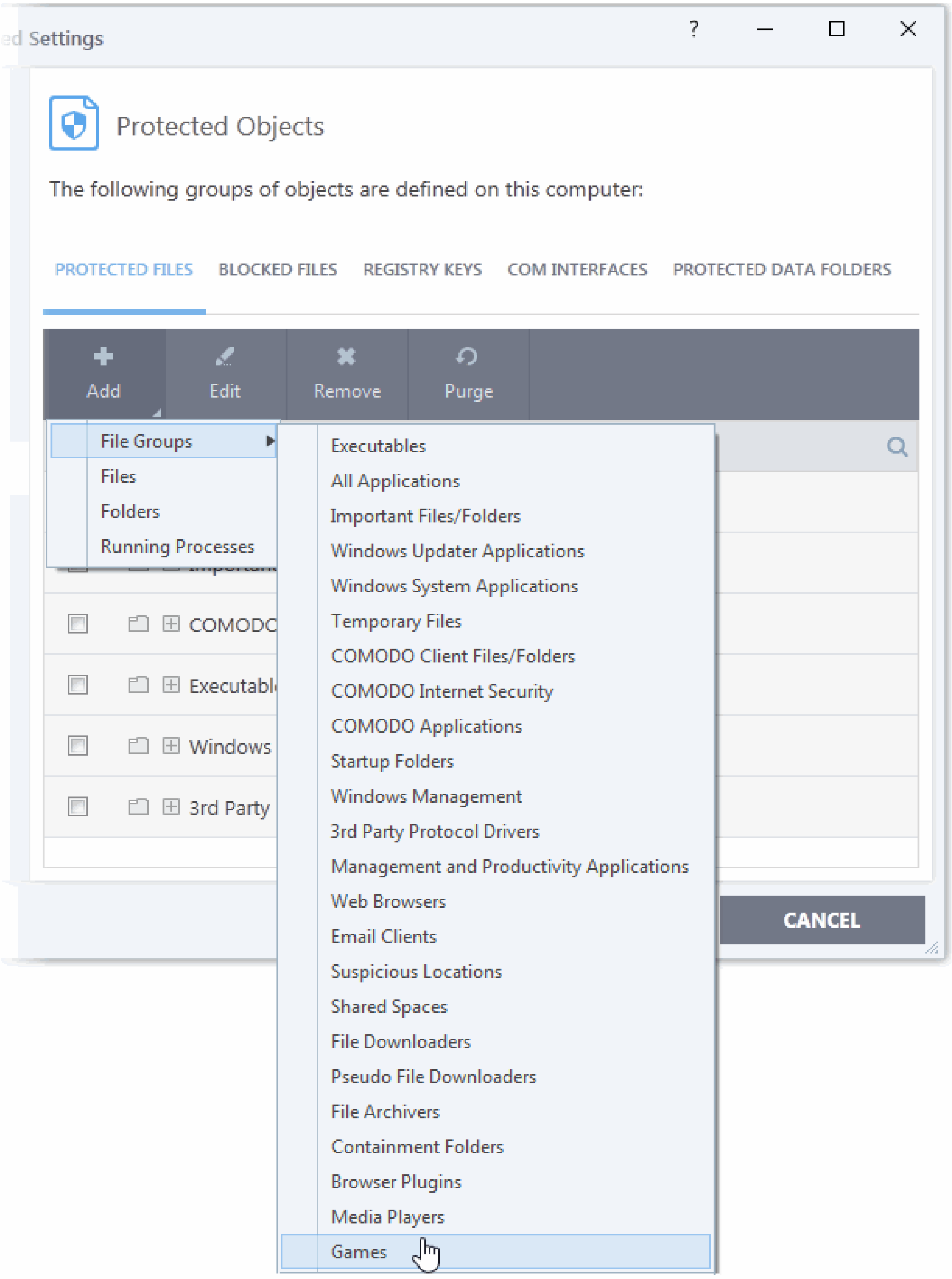


You can add the files by following methods:

- Selecting from File Groups
- Browsing to a File
- Browsing to a Folder
- Selecting from currently running Processes

Adding a File Group

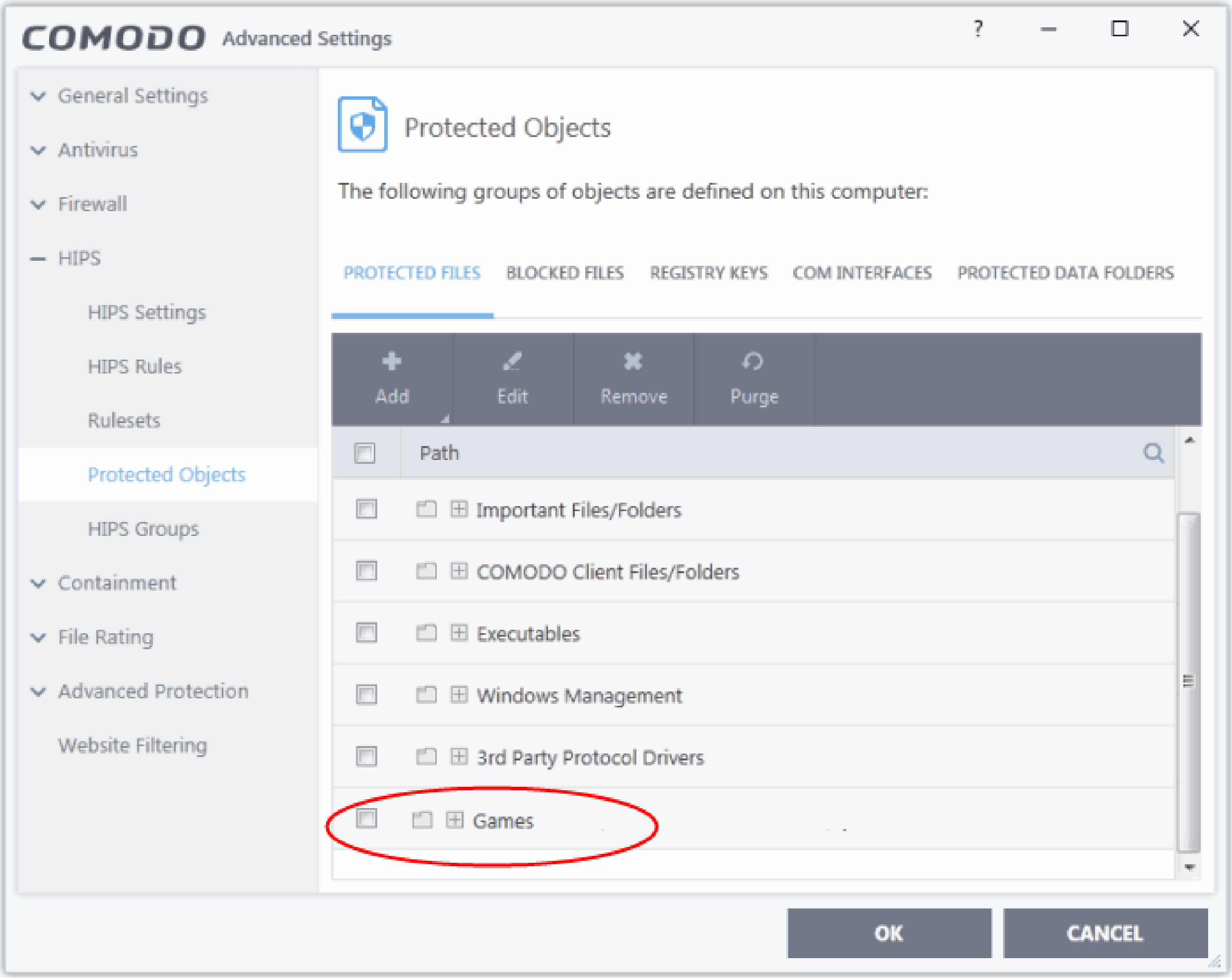
Choosing 'File Groups' allows you to add a category of pre-set files or folders. For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe, *.bat, *.cmd. Other categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.



CIS ships with a set of predefined 'File Groups' and can be viewed in Settings > File Rating > **File Groups**. You can also add new file groups here which will be displayed in the predefined list.

- To add a file group to 'Protected Files', click 'Add' > 'File Groups' and select the type of 'File Group' from the list.

The file group will be added to 'Protected Files' list.

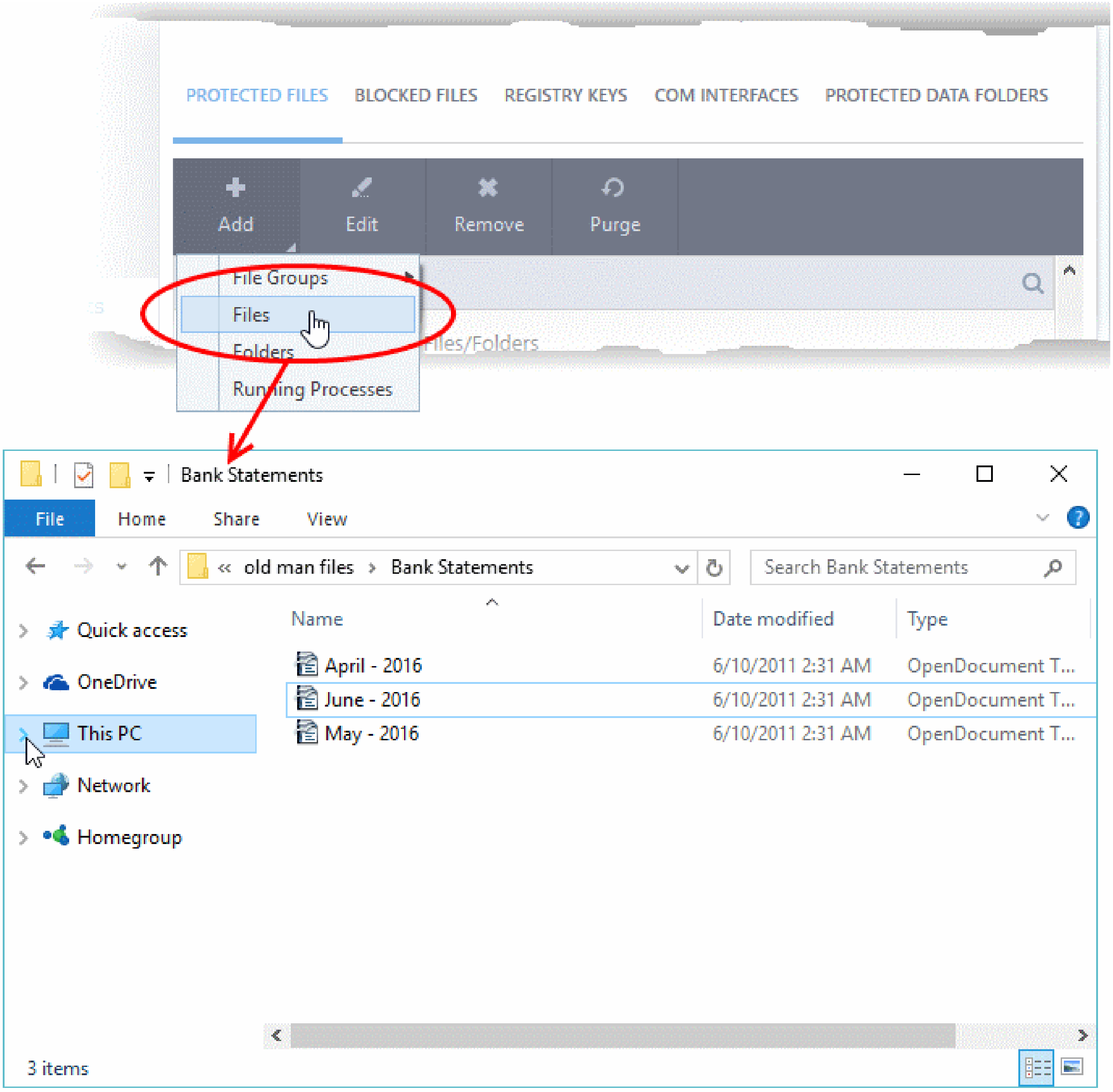


The following groups of objects are defined on this computer:

- □ Important Files/Folders
- □ COMODO Client Files/Folders
- □ Executables
- □ Windows Management
- □ 3rd Party Protocol Drivers
- □ Games

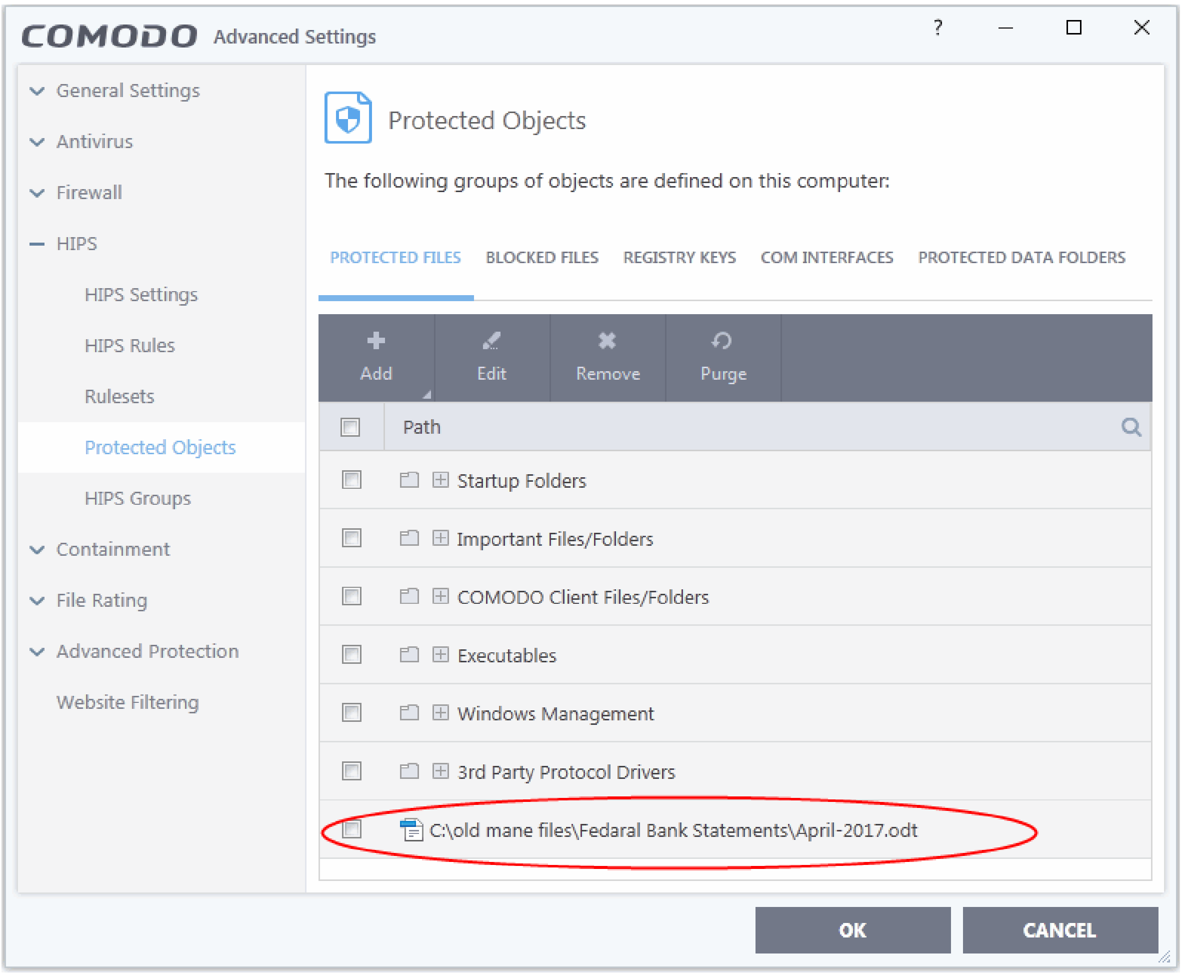
Adding an individual File

- Click 'Add' and choose 'Files' from the options



- Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open'

The file will be added to 'Protected Files'.

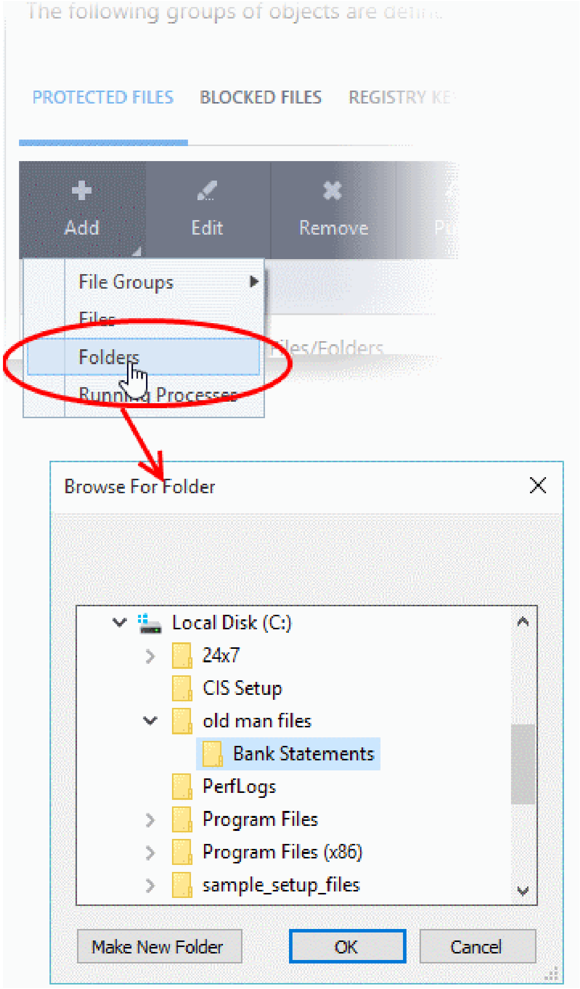


The following groups of objects are defined on this computer:

Path
Startup Folders
Important Files/Folders
COMODO Client Files/Folders
Executables
Windows Management
3rd Party Protocol Drivers
C:\old mane files\Fedaral Bank Statements\April-2017.odt

Adding a Drive Partition/Folder

- To add a folder, choose 'Folders' from the 'Add' drop-down.

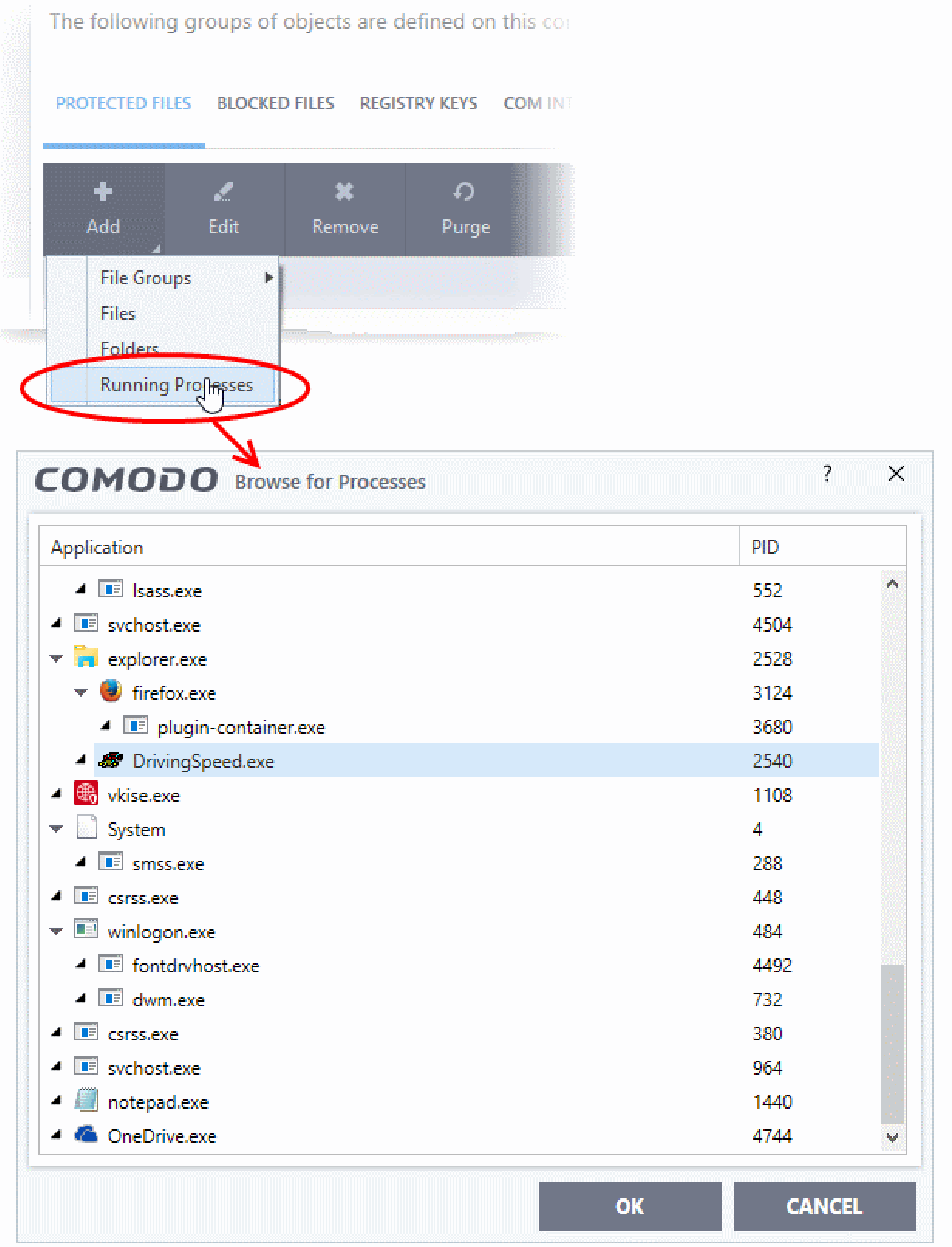


The 'Browse for Folder' dialog will appear.

- Select the folder/drive and click 'OK'. Repeat the process to add more items. The items added to the 'Protected Files' will be protected from access by other programs.

Adding an application from a running processes

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

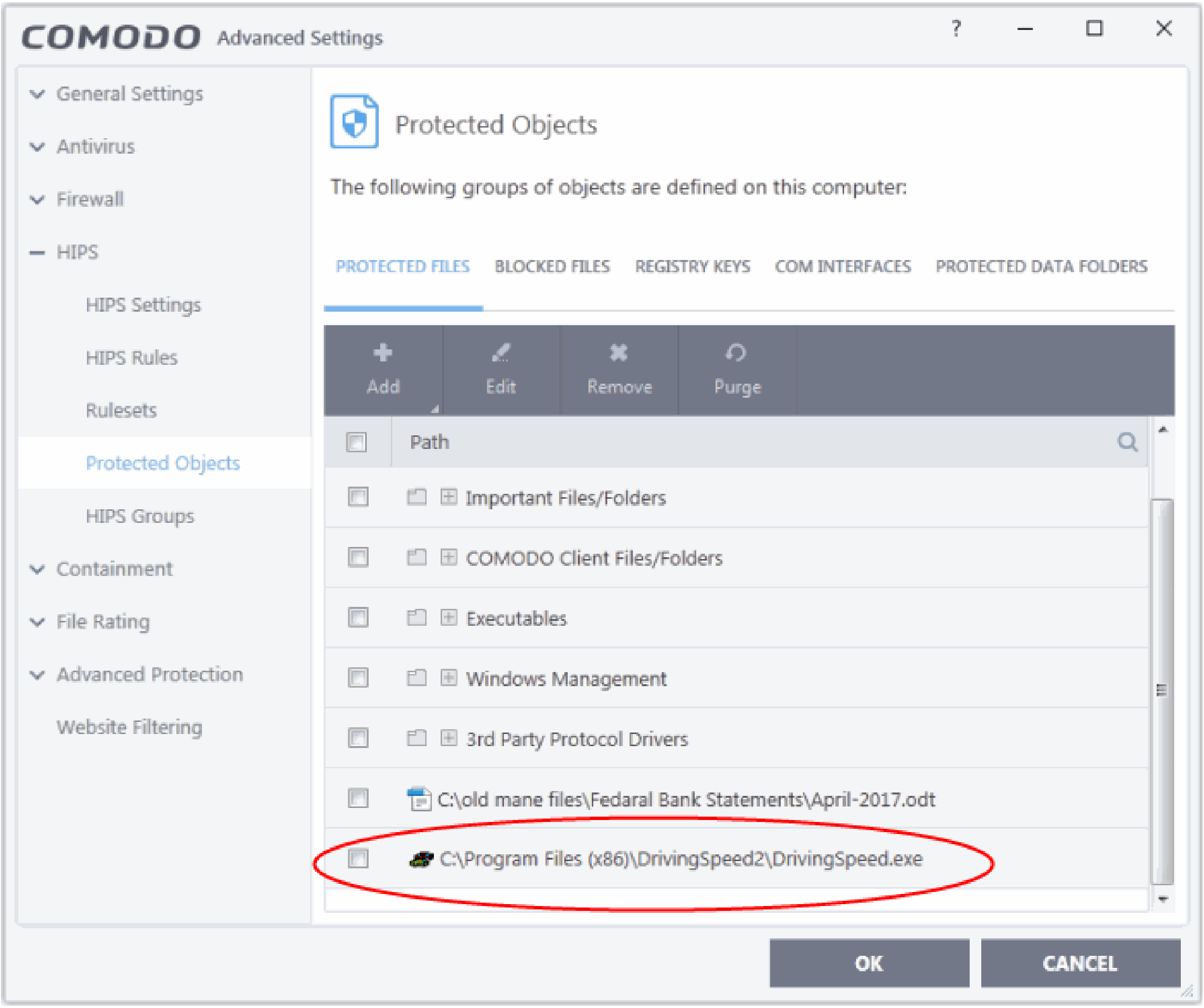


Application	PID
lsass.exe	552
svchost.exe	4504
explorer.exe	2528
firefox.exe	3124
plugin-container.exe	3680
DrivingSpeed.exe	2540
vkise.exe	1108
System	4
smss.exe	288
csrss.exe	448
winlogon.exe	484
fontdrvhost.exe	4492
dwm.exe	732
csrss.exe	380
svchost.exe	964
notepad.exe	1440
OneDrive.exe	4744

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

- Select the process, whose target application is to be added to 'Protected Files' and click 'OK' from the 'Browse for Process' dialog.

The application will be added to the 'Protected Files' list.



Protected Objects

The following groups of objects are defined on this computer:

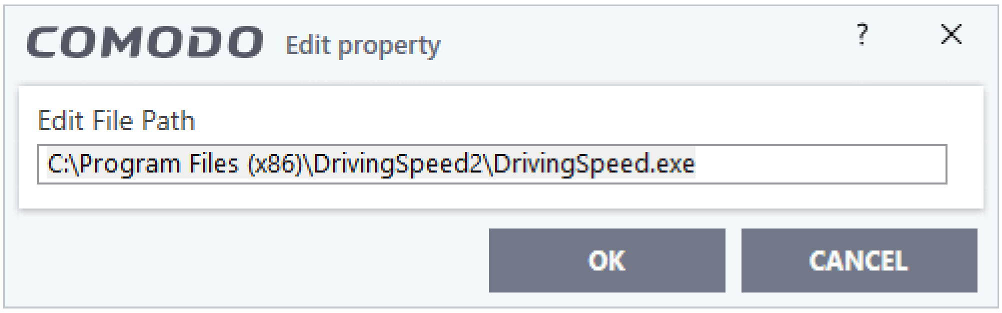
PROTECTED FILES | BLOCKED FILES | REGISTRY KEYS | COM INTERFACES | PROTECTED DATA FOLDERS

	Path
□	⊞ Important Files/Folders
□	⊞ COMODO Client Files/Folders
□	⊞ Executables
□	⊞ Windows Management
□	⊞ 3rd Party Protocol Drivers
□	C:\old mane files\Fedaral Bank Statements\April-2017.odt
□	C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

- Repeat the process to add more files. The items added to the 'Protected Files' will be protected from access by other programs.

To edit an item in the Protected Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



Edit File Path

C:\Program Files (x86)\DrivingSpeed2\DrivingSpeed.exe

- Edit the file path, if you have relocated the file and click 'OK'

To delete an item from Protected Files list

- Select the item from the list and click the 'Remove' button

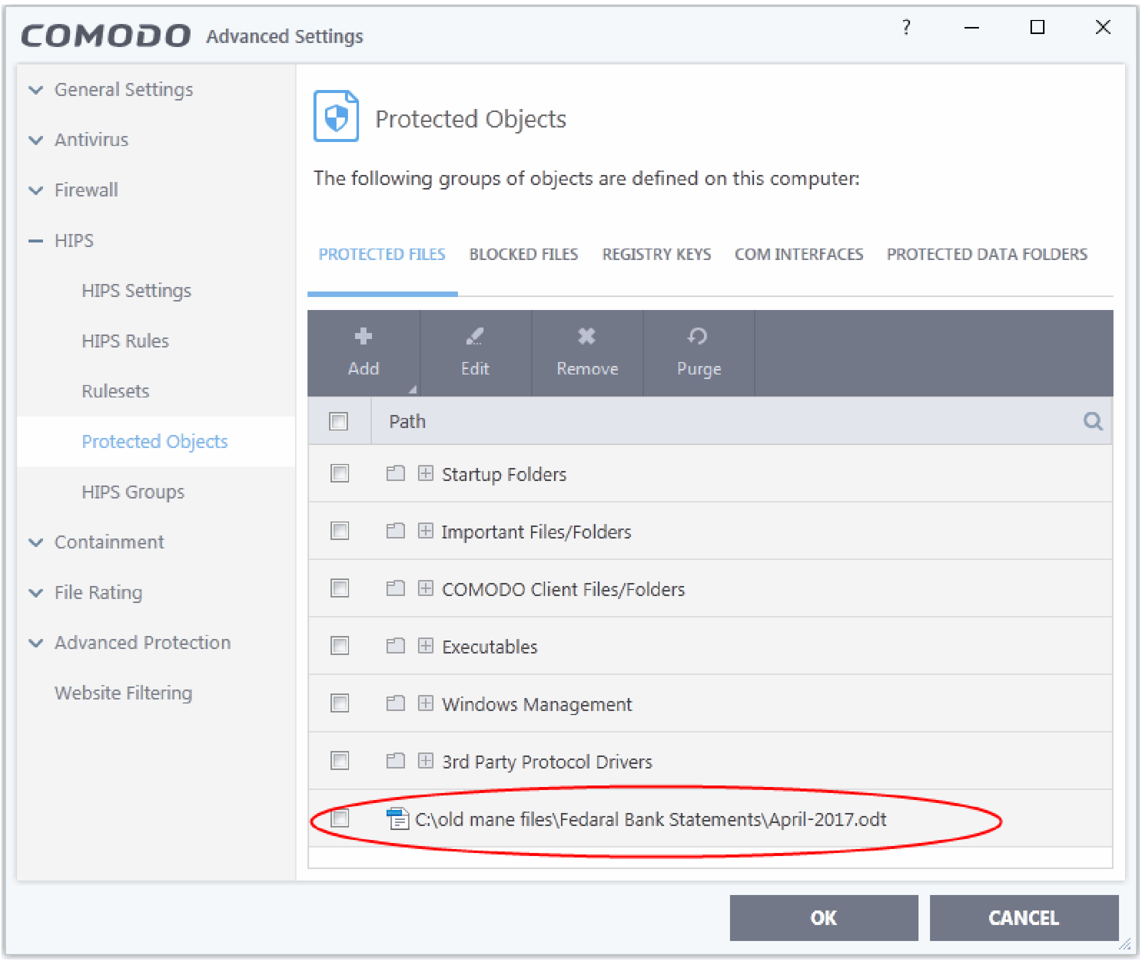
The selected item will be deleted from the protected files list. CIS will not generate alerts, if the file or program is subjected to unauthorized access.

Exceptions

Users can selectively allow another application (or file group) to modify a protected file by affording the appropriate 'Access Right' in '**Active HIPS Rules**' interface.

A simple example would be the imaginary file 'April - 2017.odt'. You would want the 'Open Office Writer' program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potentially malicious program. You would first **add** the document to the 'Protected Files' area. Once added to 'Protected Files', you would go into '**Active HIPS Rules**' and create an exception for 'swriter.exe' so that it alone could modify 'June - 2016.odt'.

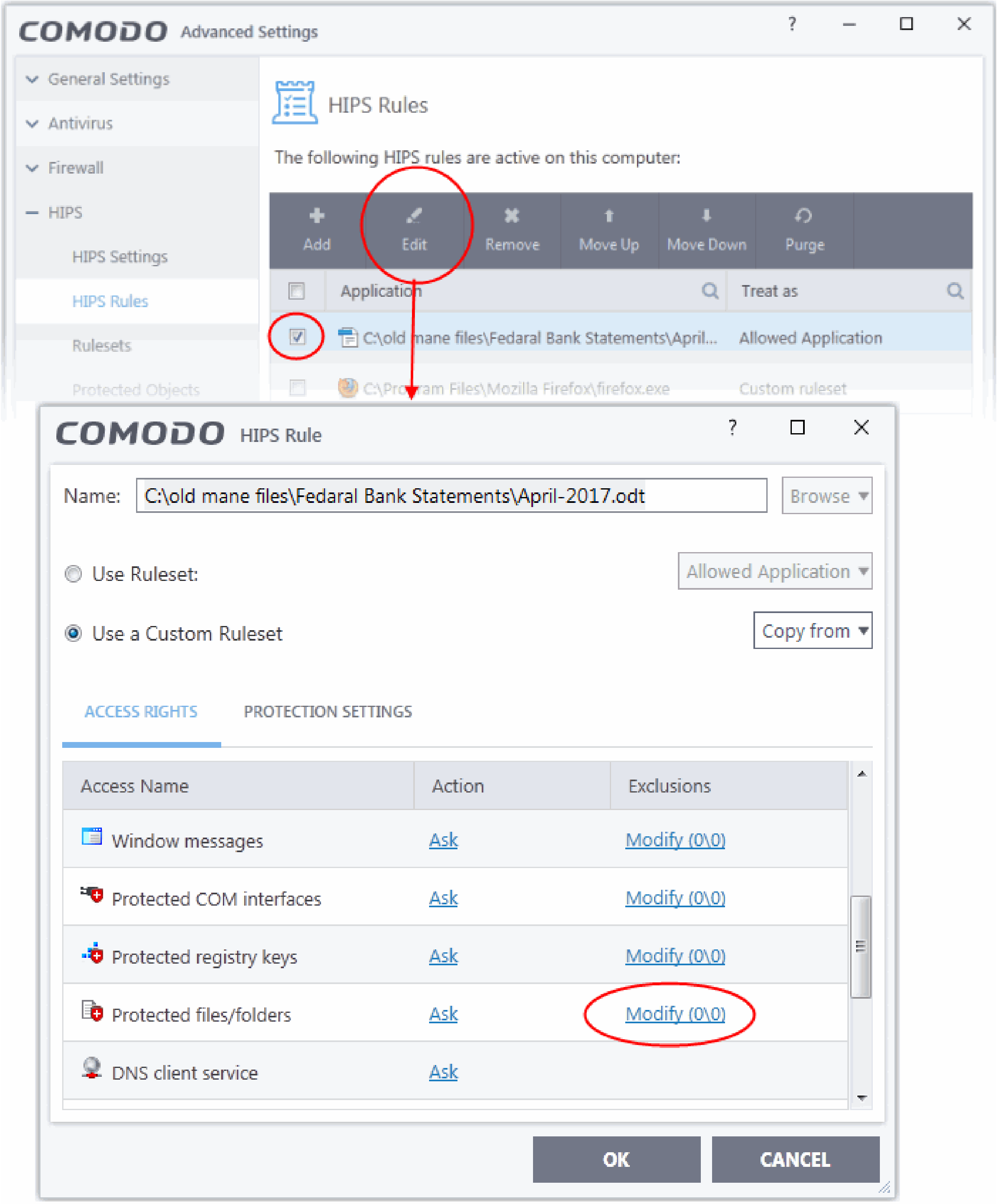
- First add 'April - 2017.odt' to 'Protected Files' area



The following groups of objects are defined on this computer:

- Startup Folders
- Important Files/Folders
- COMODO Client Files/Folders
- Executables
- Windows Management
- 3rd Party Protocol Drivers
- C:\old mane files\Fedaral Bank Statements\April-2017.odt

- Then go to 'HIPS Rules' interface and add it to the list of applications.
- Click the 'Edit' button after selecting the checkbox beside it.
- In the 'HIPS Rule' interface, select 'Use a Custom Ruleset'.



The following HIPS rules are active on this computer:

	Application	Treat as
☑	C:\old mane files\Fedaral Bank Statements\April...	Allowed Application
□	C:\Program Files\Mozilla Firefox\firefox.exe	Custom ruleset

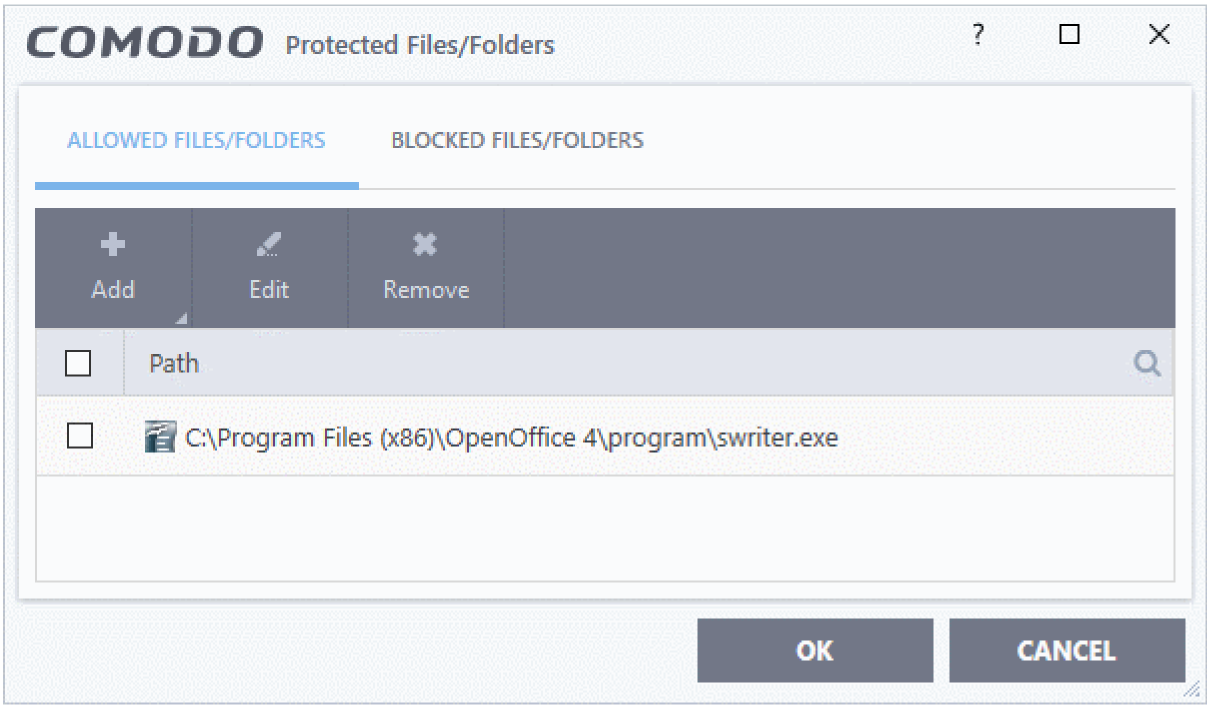
Name: C:\old mane files\Fedaral Bank Statements\April-2017.odt

○ Use Ruleset: Allowed Application

● Use a Custom Ruleset

Access Name	Action	Exclusions
Window messages	Ask	Modify (0\0)
Protected COM interfaces	Ask	Modify (0\0)
Protected registry keys	Ask	Modify (0\0)
Protected files/folders	Ask	Modify (0\0)
DNS client service	Ask	

- Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'. The 'Protected Files/Folders' interface will appear.
- Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add swriter.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



□ C:\Program Files (x86)\OpenOffice 4\program\swriter.exe

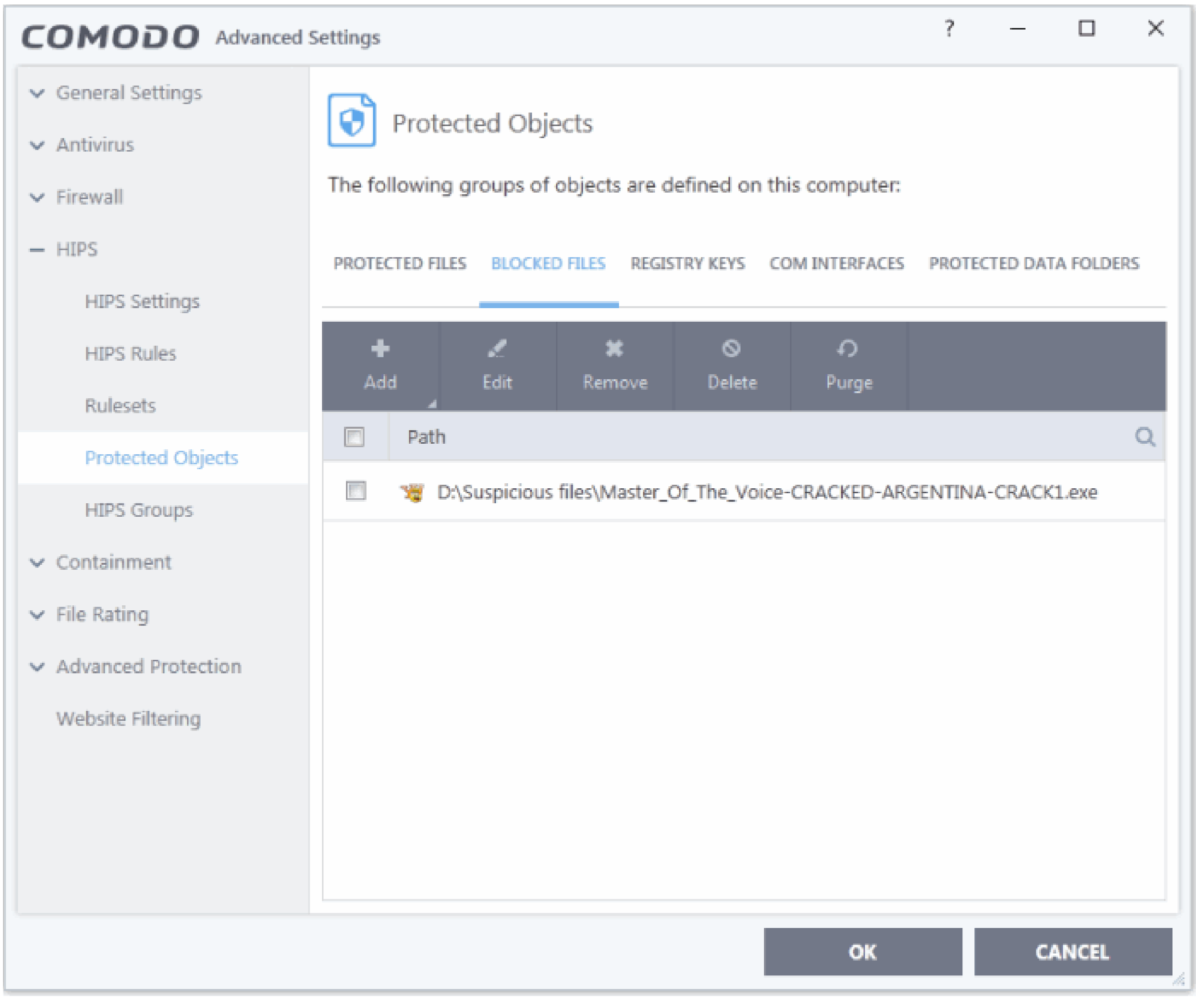
Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32\* to the 'Protected Files area (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

6.4.4.2. Blocked Files

CIS allows you to lock-down files and folders by completely denying all access rights to them from other processes or users - effectively cutting them off from the rest of your system. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files in 'Protected Files', users cannot selectively allow access a blocked file.

To open the 'Blocked Files' section

- Click 'Settings' from the top left of the CIS home screen to open 'Advanced Settings' interface
- Click 'HIPS' > 'Protected Objects' on the left
- Click the 'Blocked Files' tab



The following groups of objects are defined on this computer:

D:\Suspicious files\Master_Of_The_Voice-CRACKED-ARGENTINA-CRACK1.exe

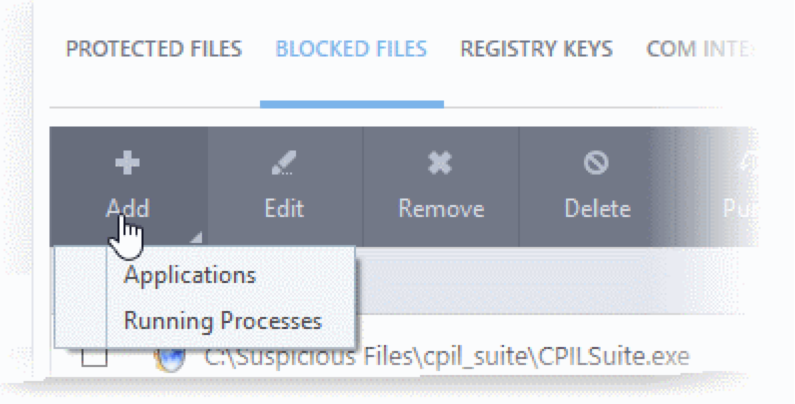
The buttons at the top provide the following options:

- **Add** - Allows you to add individual files, programs, applications to Blocked Files.
- **Edit** - Allows you to edit the path of the file.
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

To manually add an individual file or application

- Click the 'Add' button



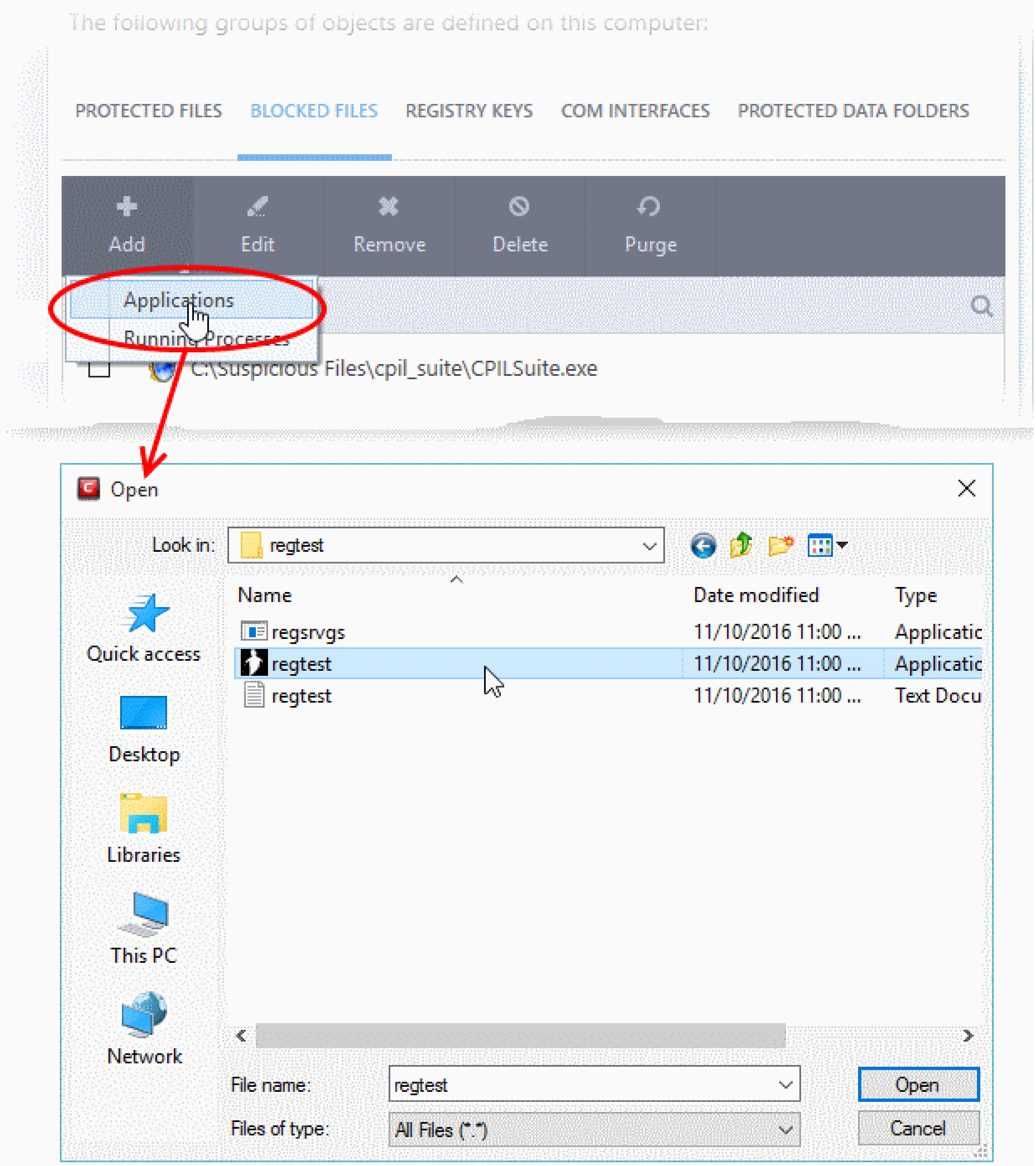
C:\Suspicious Files\cpil_suite\CPILSuite.exe

You can add the files by following methods:

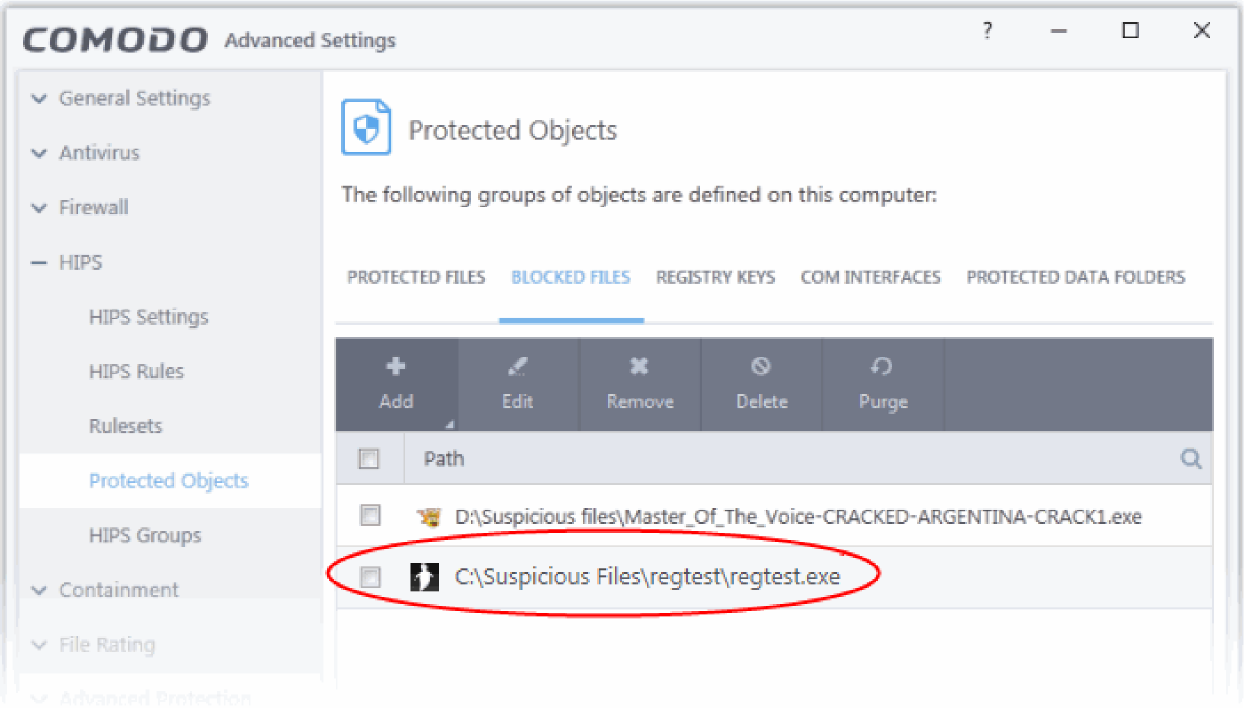
- **Selecting a File**
- **Selecting from currently running Processes**

Adding a File

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



The file will be added to 'Blocked Files' list.



Protected Objects

The following groups of objects are defined on this computer:

□	Path
□	D:\Suspicious files\Master_Of_The_Voice-CRACKED-ARGENTINA-CRACK1.exe
□	C:\Suspicious Files\regtest\regtest.exe

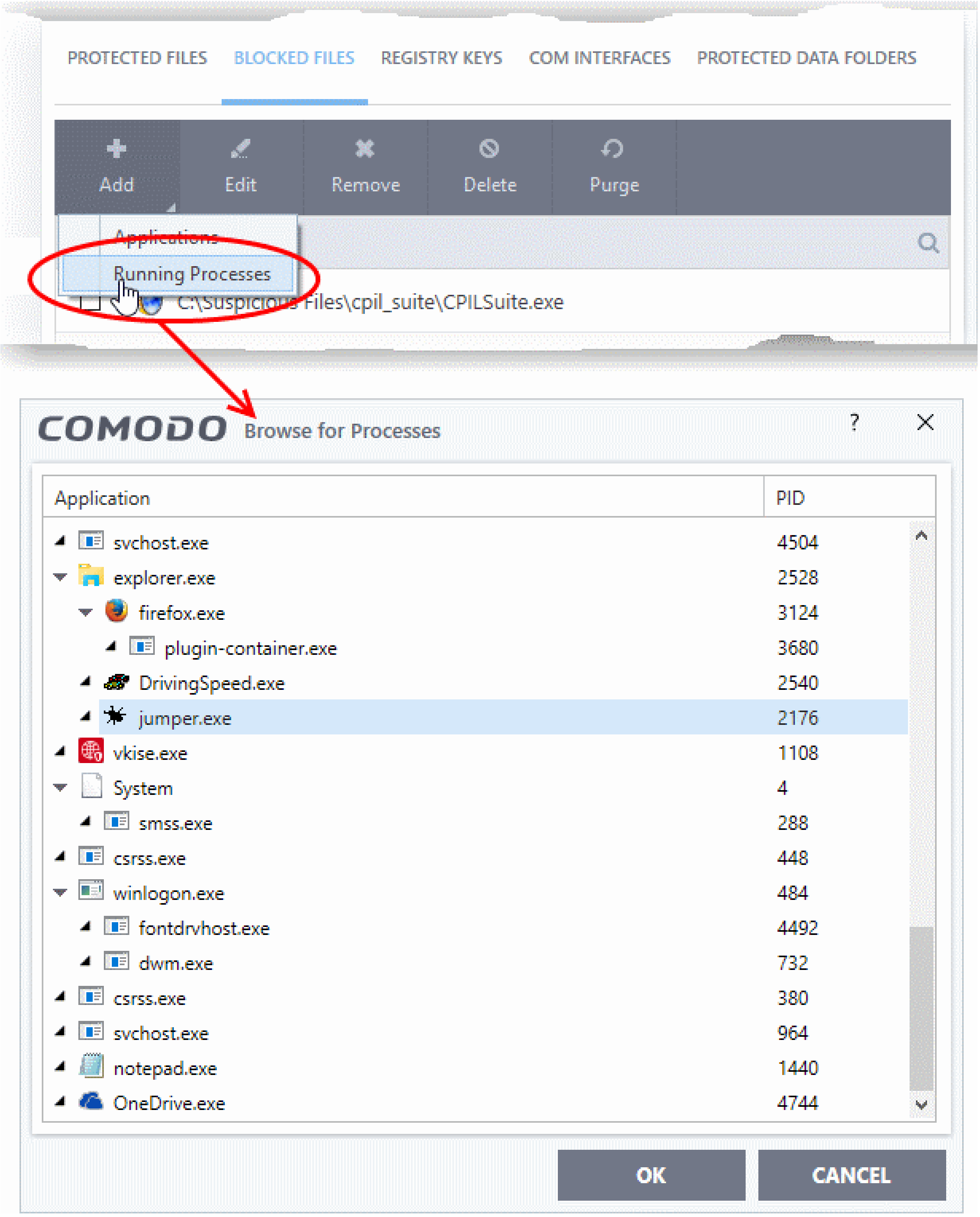
- Repeat the process to add more files.

Adding an application from a running process

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

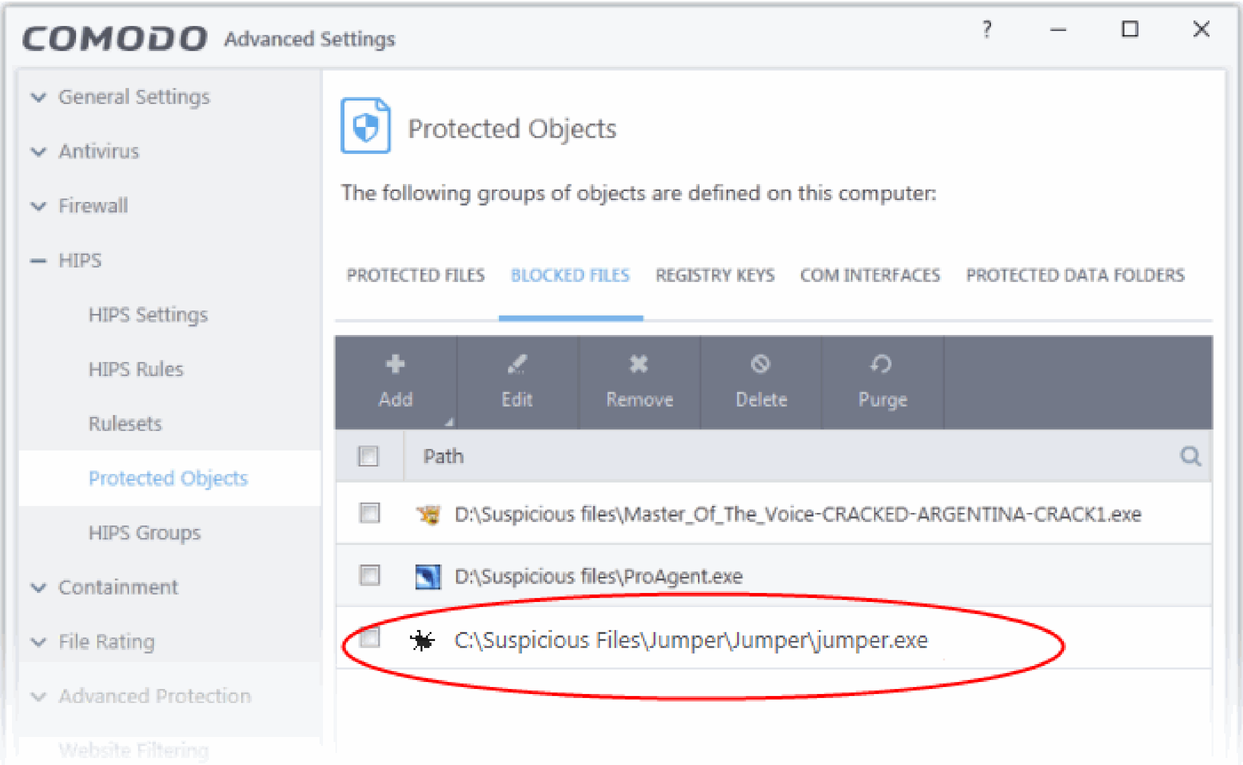
A list of currently running processes in your computer will be displayed.

- Select the process whose parent application you want to add to the 'Blocked Files' list and click 'OK'



Application	PID
svchost.exe	4504
explorer.exe	2528
firefox.exe	3124
plugin-container.exe	3680
DrivingSpeed.exe	2540
jumper.exe	2176
vkise.exe	1108
System	4
smss.exe	288
csrss.exe	448
winlogon.exe	484
fontdrvhost.exe	4492
dwm.exe	732
csrss.exe	380
svchost.exe	964
notepad.exe	1440
OneDrive.exe	4744

The application will be added to the 'Blocked Files' list.



The following groups of objects are defined on this computer:

D:\Suspicious files\Master_Of_The_Voice-CRACKED-ARGENTINA-CRACK1.exe

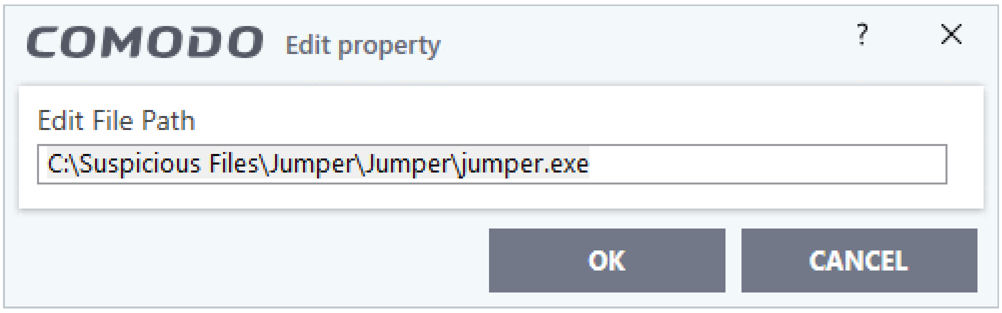
D:\Suspicious files\ProAgent.exe

C:\Suspicious Files\Jumper\Jumper\jumper.exe

- Repeat the process to add more files.

To edit an item in the Blocked Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



Edit File Path: C:\Suspicious Files\Jumper\Jumper\jumper.exe

- Edit the file path, if you have relocated the file and click 'OK'

To release an item from Blocked Files list

- Select the item from the list and click the 'Remove' button

The selected item will be removed from the 'Blocked Files' list. CIS will not block the application or file from execution or opening then onwards.

To permanently delete a blocked file from your system

- Select the item from the list and click the 'Delete' button

The selected item will be deleted from your computer immediately.

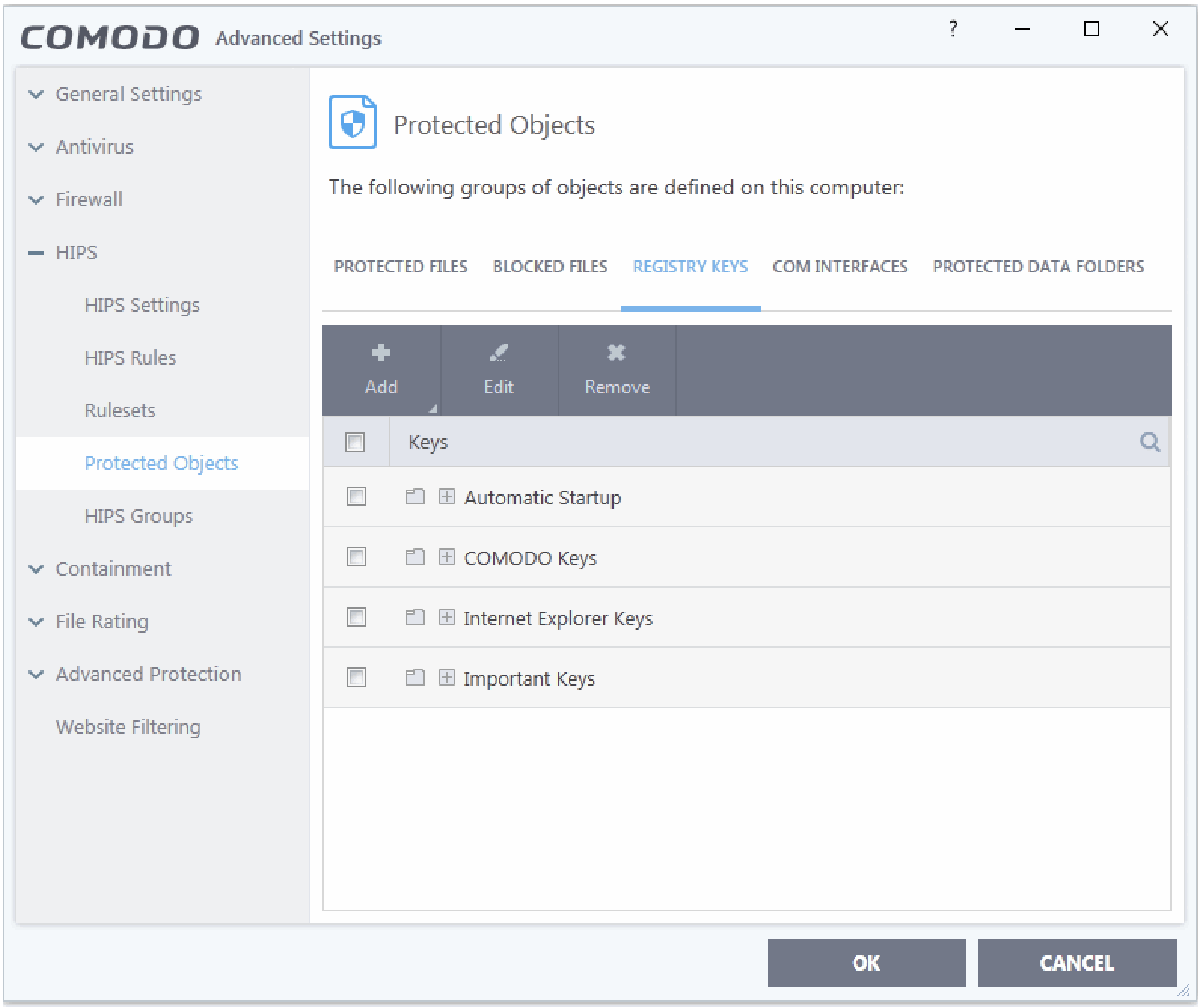
Warning: Deleting a file from from the 'Blocked Files' interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

6.4.4.3. Protected Registry Keys

The 'Registry Keys' panel allows you to define system critical registry keys to be protected against modification. Irreversible damage can be caused to your system if important registry keys are corrupted or modified.

To open the 'Registry Keys' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'Protected Objects' on the left
- Click the 'Registry Keys' tab



The following groups of objects are defined on this computer:

□	Keys
□	⊞ Automatic Startup
□	⊞ COMODO Keys
□	⊞ Internet Explorer Keys
□	⊞ Important Keys

The buttons at the top provide the following options:

- **Add** - Allows you to add 'Registry Groups' or individual registry keys/entries to 'Registry Keys' protection list.
- **Edit** - Allows you to edit the path of the 'Registry Group' or individual registry keys/entries of the selected item.
- **Remove** - Deletes the currently selected 'Registry Group' or individual registry key from the list.
- Click the magnifying glass on the right to search for a specific item.

To manually add an individual Registry key or Registry Group

- Click the 'Add' button

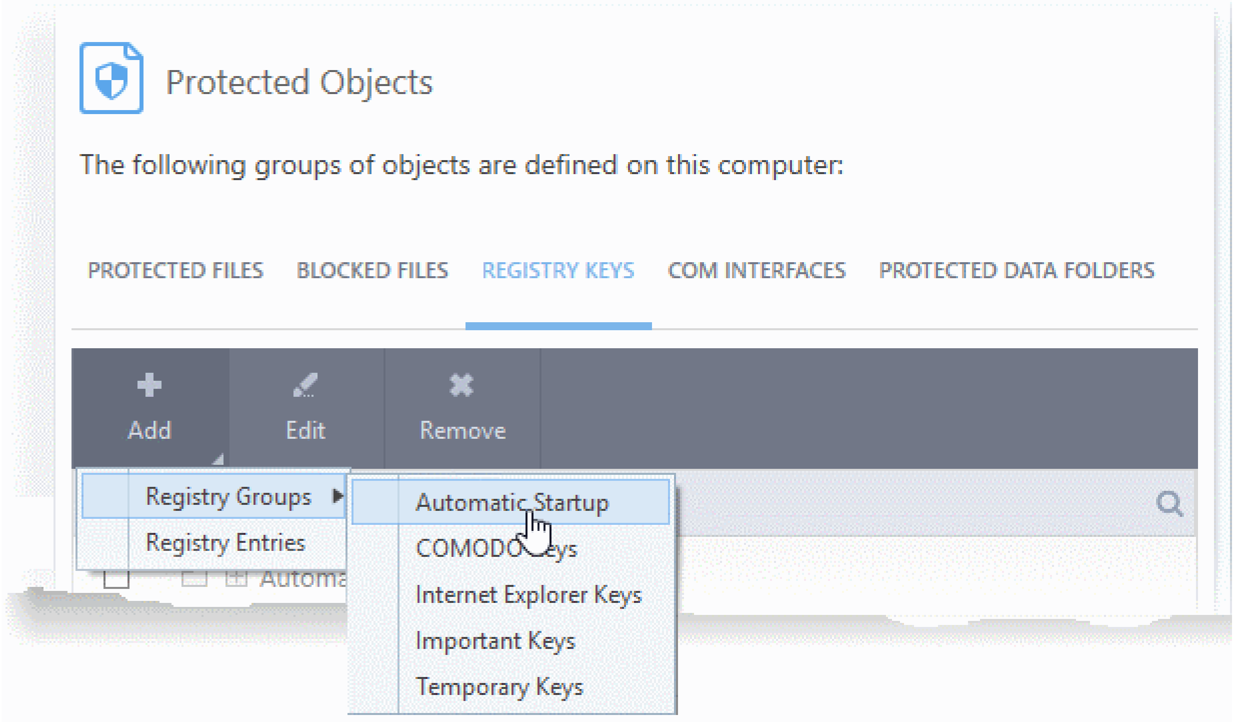
You can add keys individually or by registry group:

- **Adding Registry Groups -** Adding a registry group allows you to batch select and import groups of important registry keys. Comodo Internet Security provides the following, pre-defined groups - 'Automatic

Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.

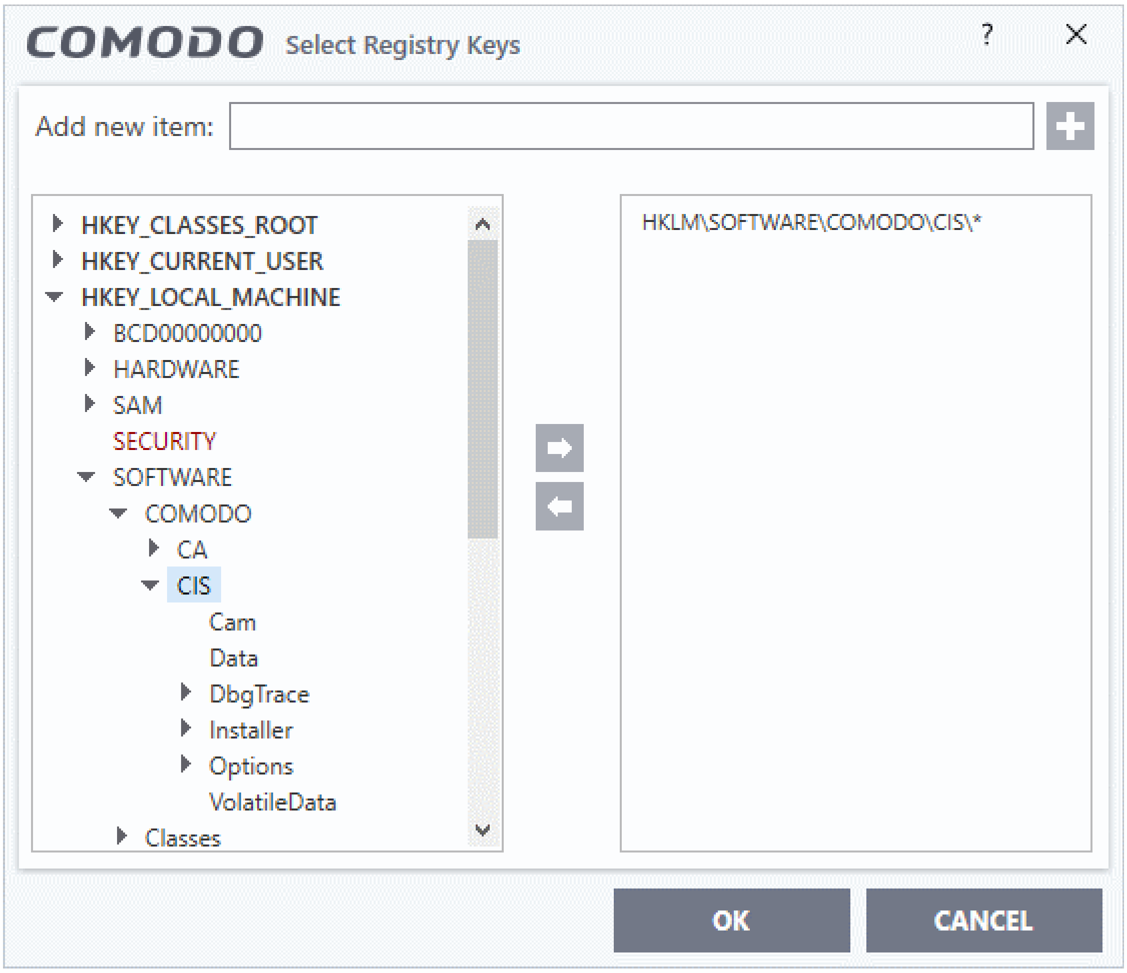
You can also create custom registry groups containing keys you wish to protect.

- To add a new group, click the 'Add' button > 'Registry Groups' and select the predefined group from the list and click 'OK'



See **Registry Groups** in the **HIPS Groups** section, for explanations on editing existing registry groups and creating new groups.

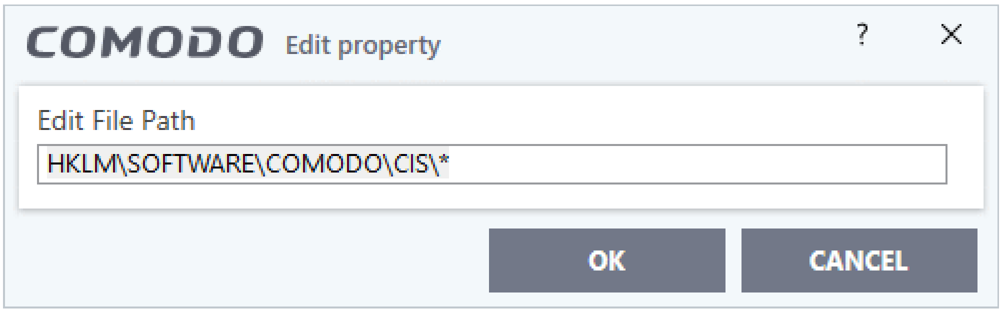
- **Adding individual Registry Keys -** Click the 'Add' button and then 'Registry Entries'. The 'Select Registry Keys' screen will open.



You can add items by selecting a key on the left and moving it to over to the right by clicking the right arrow. To add an item manually, enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the Registry Protection list

- Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



Edit File Path

HKLM\SOFTWARE\COMODO\CIS\*

- Edit the key path, if you have relocated the key and click 'OK'.

Note: The 'Registry Groups' cannot be edited from this interface. You can edit only from **Registry Groups** in **HIPS Groups** section.

To delete an item from Registry Protection list

- Select the item from the list and click the 'Remove' button.

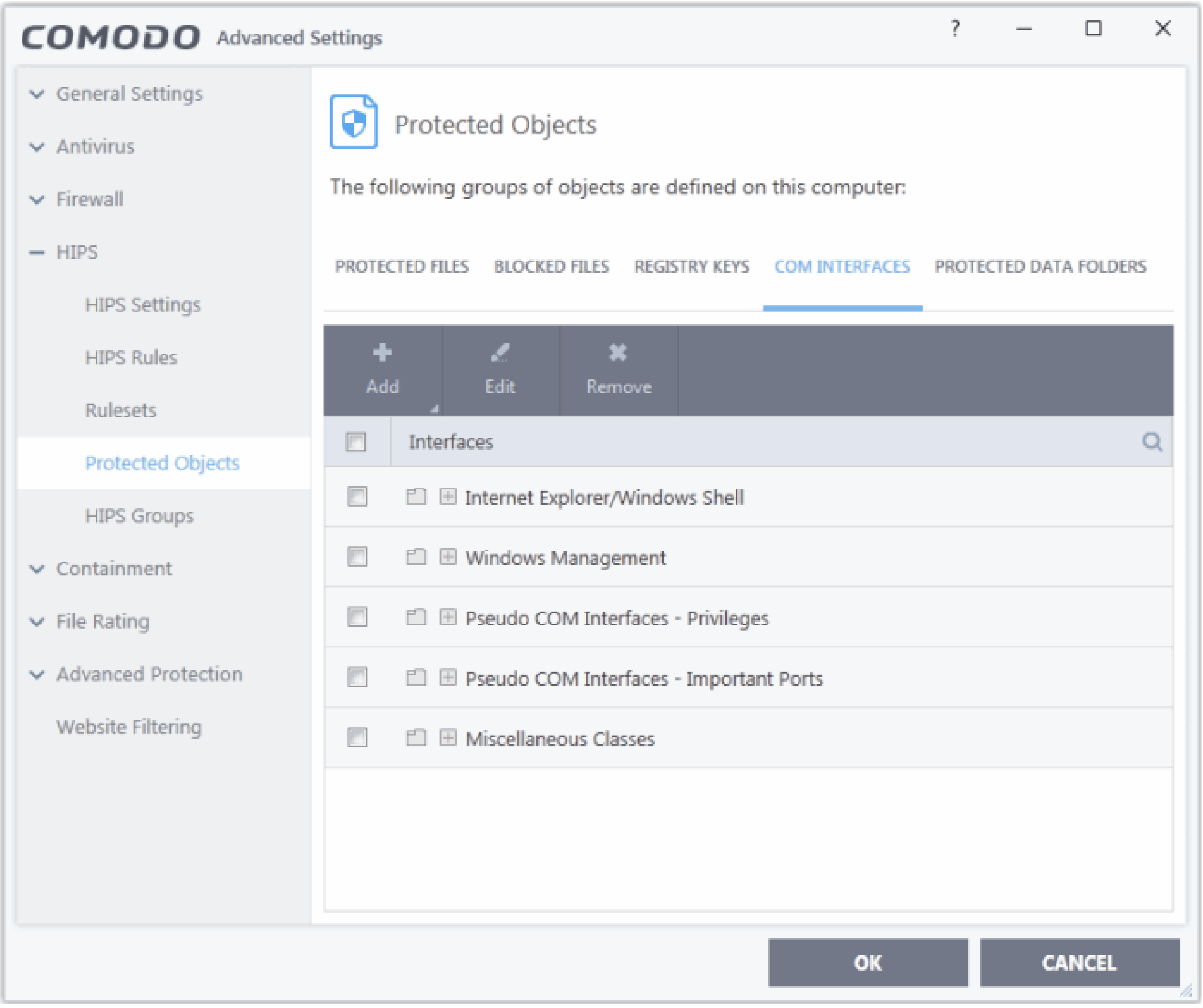
The selected item will be deleted from the 'Registry Keys' protection list. CIS will not generate alerts, if the key or the group is modified by other programs.

6.4.4.4. Protected COM Interfaces

- The Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application, or between applications.
- COM is used as the basis for Active X and OLE - two favorite targets of hackers and malware for launching attacks on your computer.
- Comodo Internet Security automatically protects COM interfaces against modification and manipulation by malicious processes.
- Comodo Internet Security automatically protects COM interfaces against modification and manipulation by malicious processes.
- CIS ships with a set of COM Interface Groups which are category based collections of COM Interface components.
- You can view and manage the COM Groups by clicking 'Settings' > 'HIPS Groups' > 'COM Groups' tab from the 'Advanced Settings' interface. It also allows you to create custom COM Interface groups as required. See **COM Groups** for more details.

To open the protected 'COM Interfaces' section

- Click 'Settings' from the top left of the CIS home screen to open 'Advanced Settings' interface
- Click 'HIPS' > 'Protected Objects' on the left
- Click the 'COM Interfaces' tab



The buttons at the top provide the following options:

- **Add** - Allows you to add COM groups or individual COM components to COM Protection list.
- **Edit** - Allows you to edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.

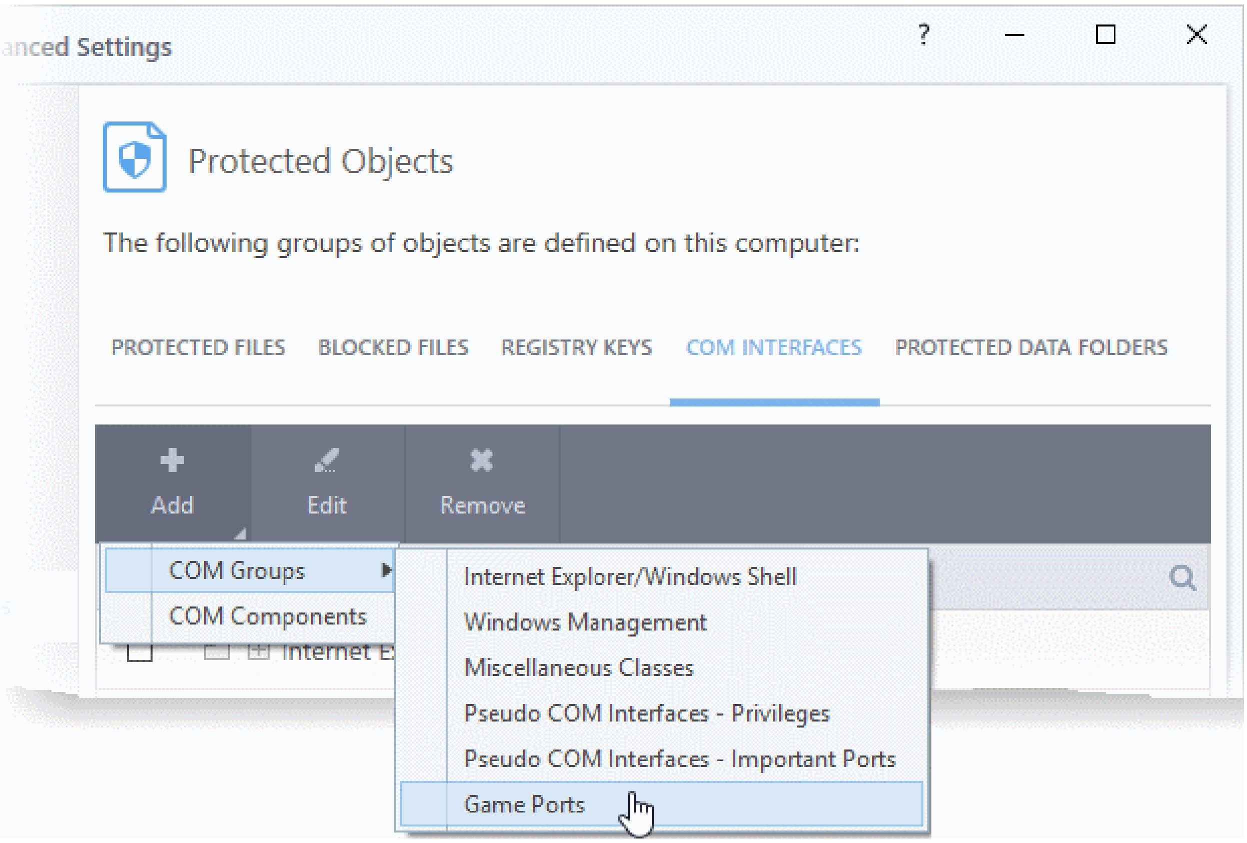
You can search for a specific interface by clicking the magnifying glass icon at the far right of the column header.

To manually add a COM Group or individual COM component

- Click the 'Add' button

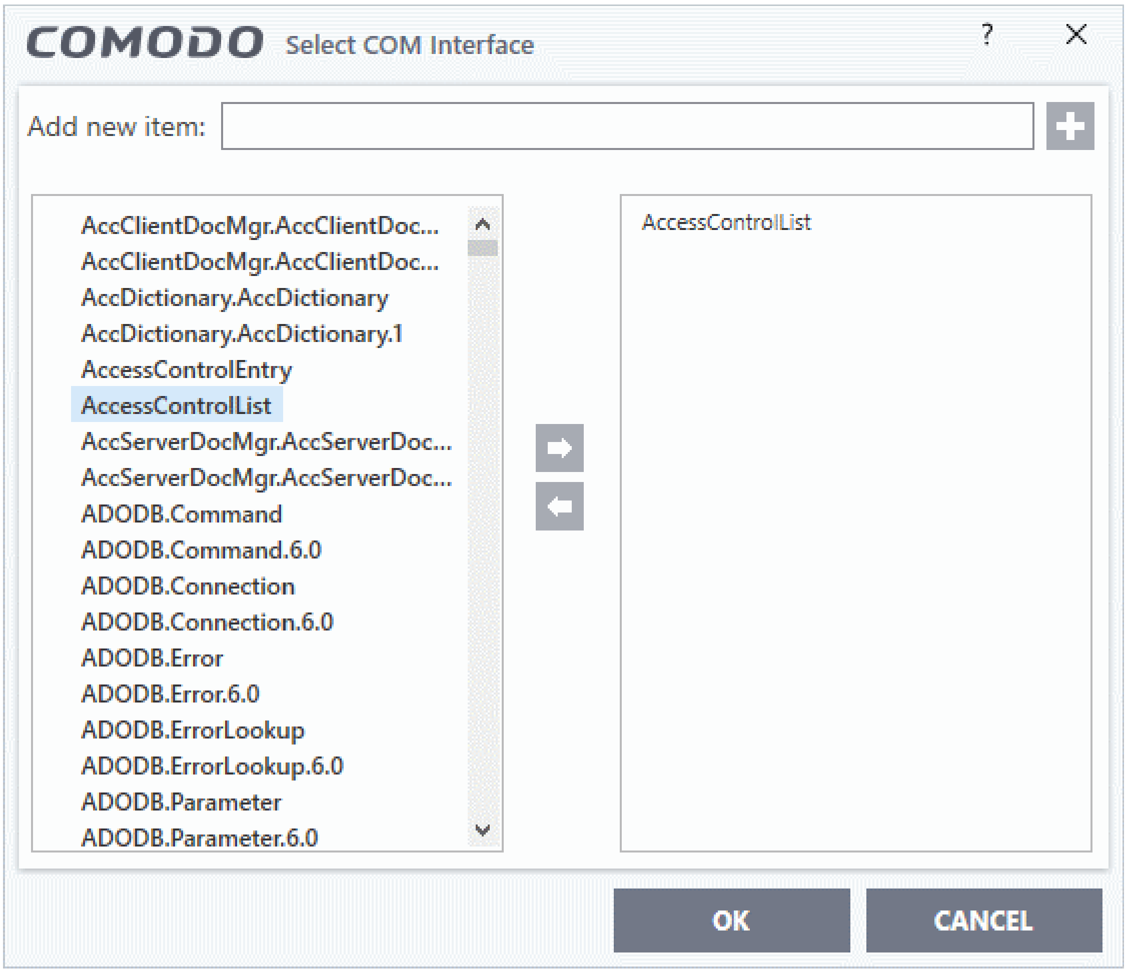
You can add items as follows:

- **Adding COM Groups -** Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components.
- To add a new group, click the 'Add' button > 'COM Groups' and select the predefined or custom COM Interface group from the options and click 'OK'



For explanations on editing existing 'COM Groups' and creating new groups, see **COM Groups**.

- **Adding COM Components -** Click the 'Add' button and then 'COM Components'. The 'Select COM Interface' screen will open.

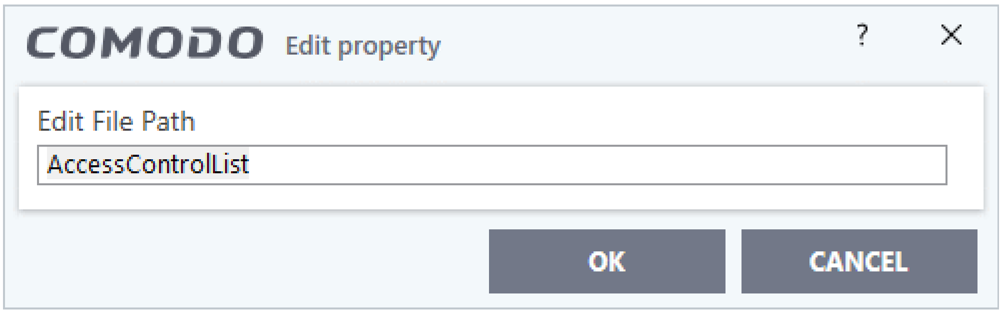


You can add items by selecting from the left side pane and moving it to right side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

- Click 'OK' to add the items to the 'COM Interfaces' list

To edit an item in the COM Interfaces protection list

- Select the COM component from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



Edit File Path
AccessControlList

- Edit the COM Class file path and click 'OK'

Note: The COM Groups cannot be edited from this interface. You can edit only from **COM Groups** in **HIPS Groups** section.

To delete an item from COM Interfaces protection list

- Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the 'COM Interfaces' protection list. CIS will not generate alerts, if the COM component or the group is modified by other programs or processes.

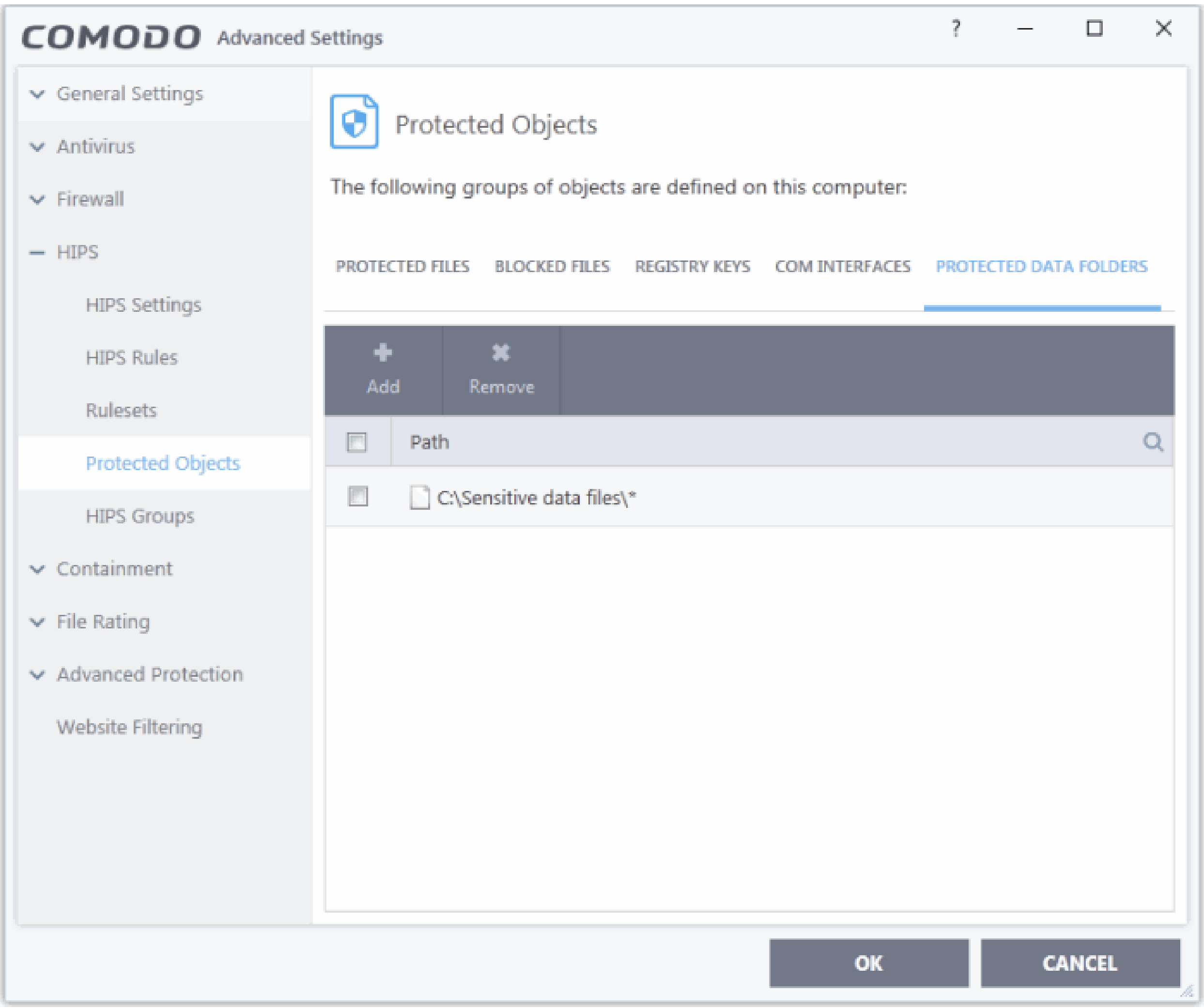
6.4.4.5. Protected Data Folders

The data files in the folders listed under the 'Protected Data Folders' area cannot be seen, accessed or modified by any known or unknown application that is running inside the container.

Tip: Files and folders that are added to '**Protected Files**' interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to contained programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all the contained programs but allow read/write access by other known/trusted programs, then add it to 'Protected Data Folders'.

To open the 'Protected Data Folders' section

- Click 'Settings' from the top left of the CIS home screen to open 'Advanced Settings' interface
- Click 'HIPS' > 'Protected Objects' on the left
- Click the 'Protected Data Folders' tab



The following groups of objects are defined on this computer:

□	Path
□	C:\Sensitive data files*

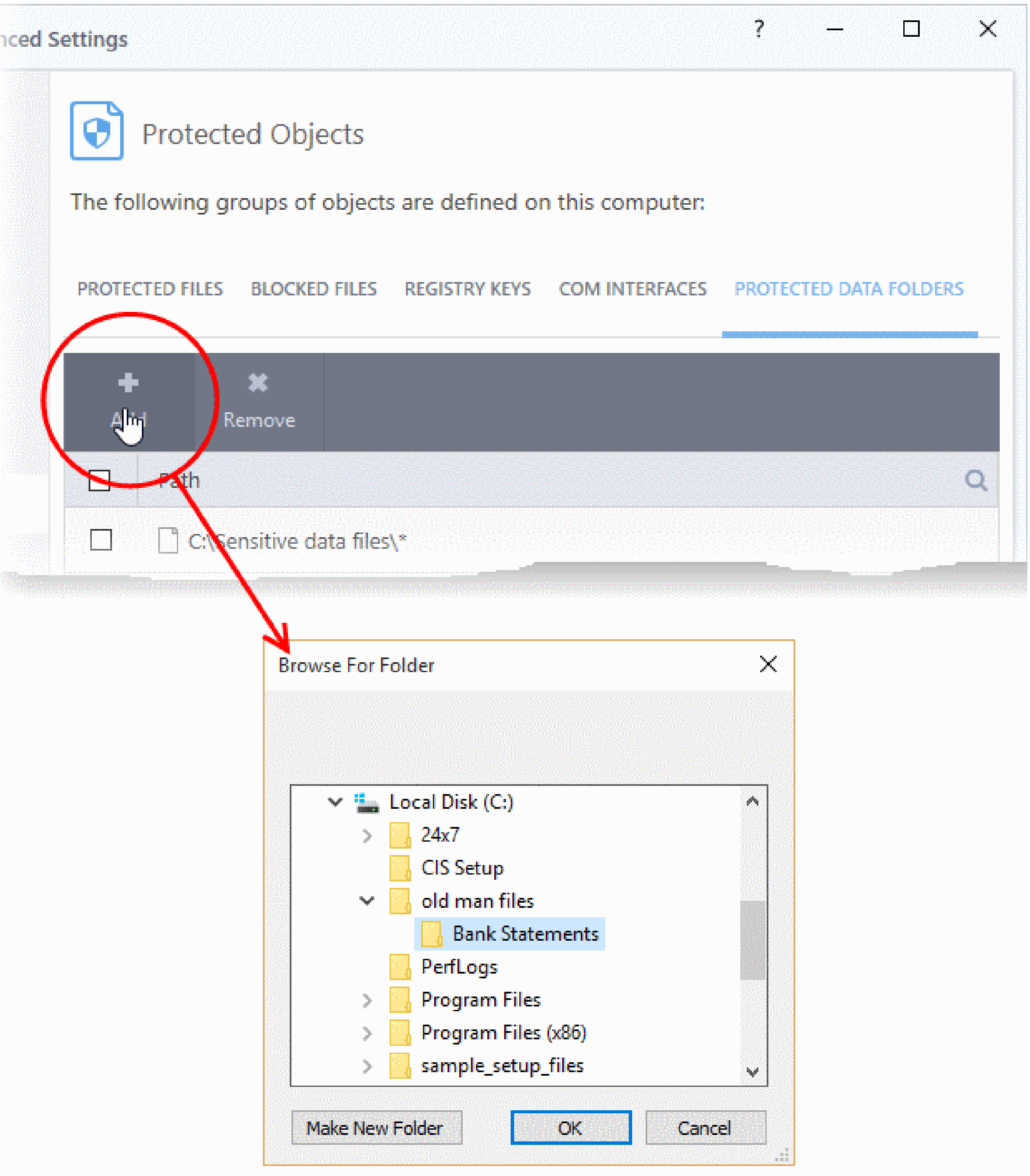
The buttons at the top provide the following options:

- **Add** - Allows you to add folders to 'Protected Data Folders' list.
- **Remove** - Deletes the currently selected folder.

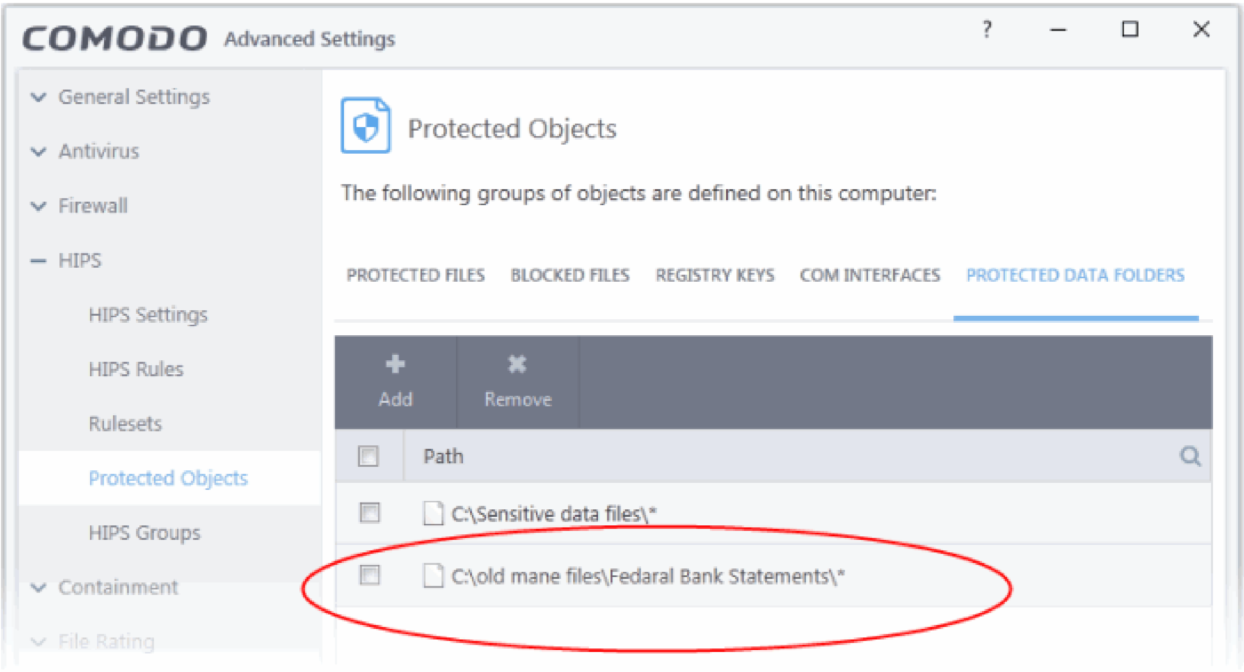
You can use the search option to find a specific name in the list by clicking the search icon at the far right of the column header and entering the name in full or part.

To add a folder to be protected

- Click the 'Add' button



- Navigate to the folder to be added and click 'OK'.



- Click 'OK' to confirm your choice.

To remove an item from Protected Data Folders list

- Select the folder from the list and click the 'Remove' button.

The selected folder will be removed from the protected folders list. CIS will not generate alerts, if the folder is subjected to unauthorized access.

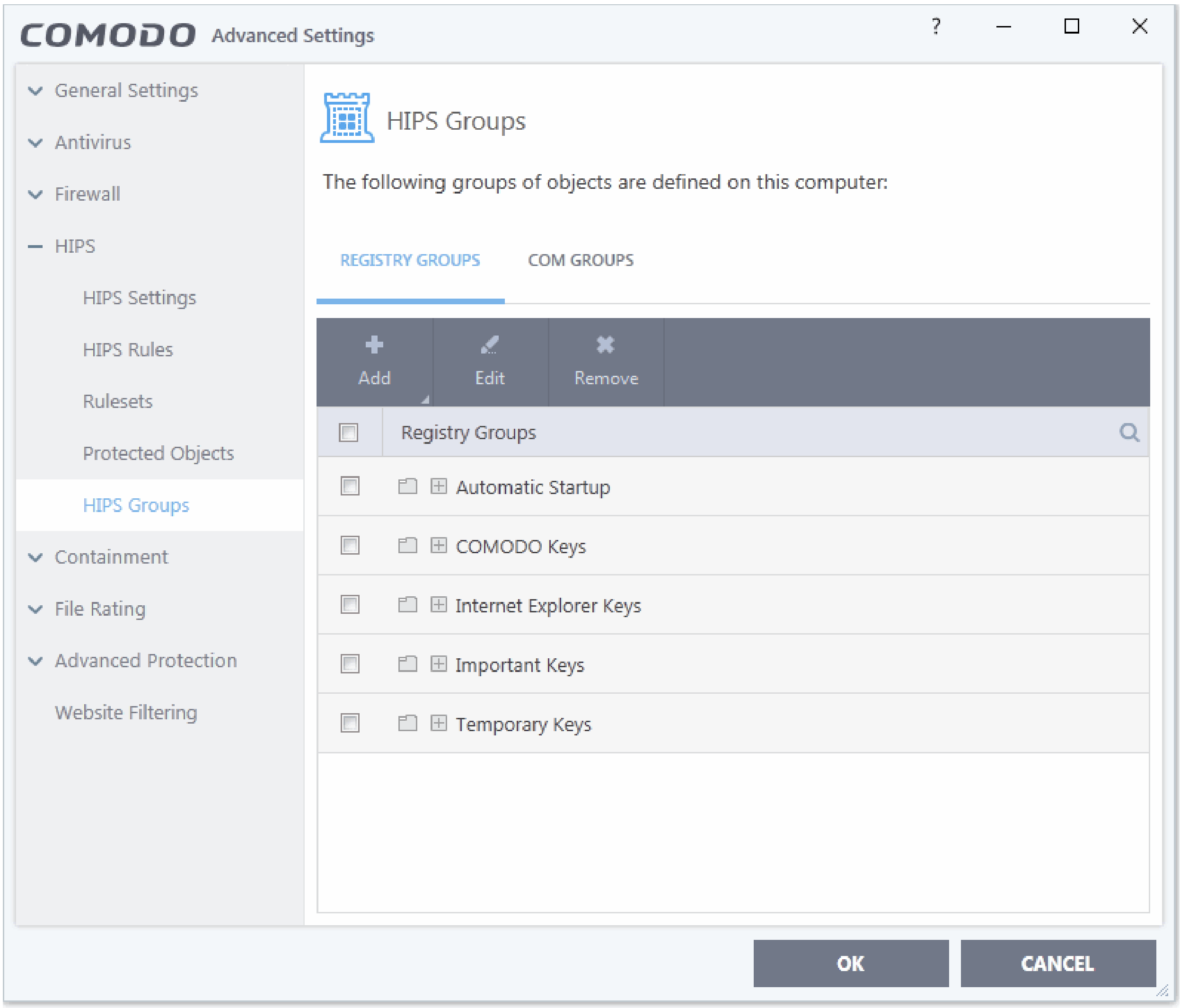
6.4.5. HIPS Groups

HIPS groups are collections of one or more COM interfaces or registry keys which, once defined, will become available for selection and protection in the **Registry Keys** and **COM Interfaces**. CIS ships with important predefined 'Registry' and 'COM' groups and allows you to add new groups.

You can view pre-defined Registry and COM groups and create and manage custom groups through the 'HIPS Groups' interface.

To open the 'HIPS Groups' interface

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'HIPS Groups' on the left



The following groups of objects are defined on this computer:

- Automatic Startup
- COMODO Keys
- Internet Explorer Keys
- Important Keys
- Temporary Keys

Please note, this area is just where you can view and define the groups. To actually apply the protections you need to select the group in the **Protected Objects** interface.

The panel has two sections:

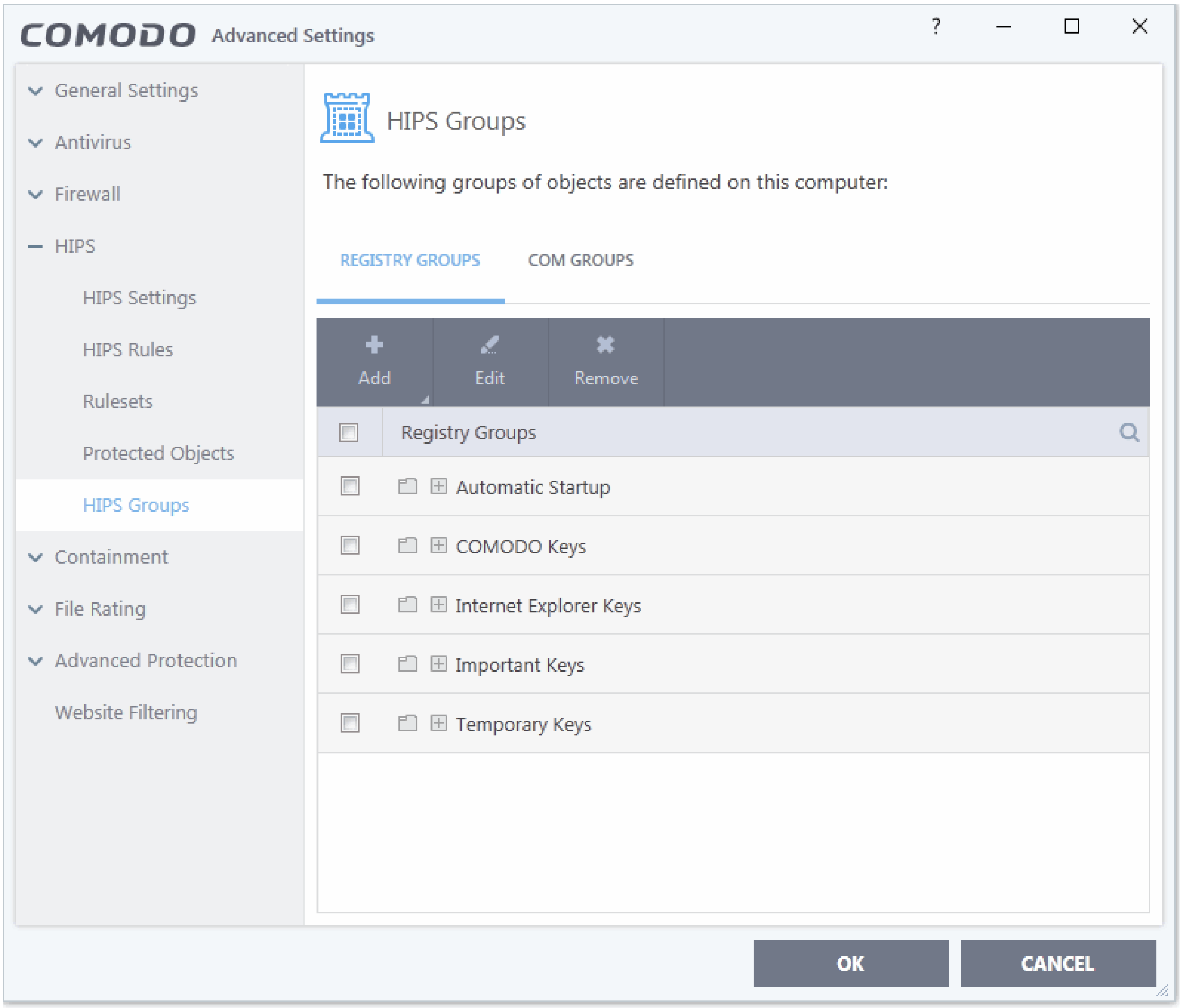
- **Registry Groups** - Allows you to view, edit and create groups of registry keys which you want to protect from changes.
- **COM Groups** - Allows you to view, edit and create groups of COM interfaces which you want to protect from changes.

6.4.5.1. Registry Groups

- Registry groups are predefined batches of one or more registry keys.
- Comodo Internet Security ships with a set of important registry groups: 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.
- Creating a registry group allows you to quickly add it to the list of protected keys. See '**Protected Registry Keys**' for help with this.

To open the 'Registry Groups' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'HIPS Groups' on the left
- Click the 'Registry Groups' tab

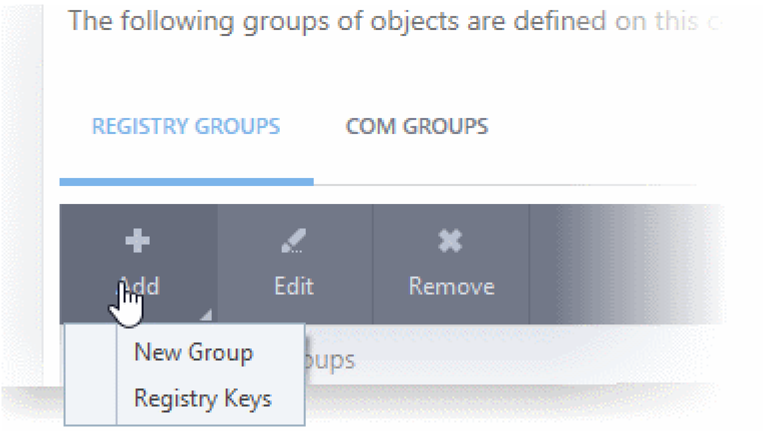


- Click the search icon on the right to find a specific item. You can enter a full or partial name.

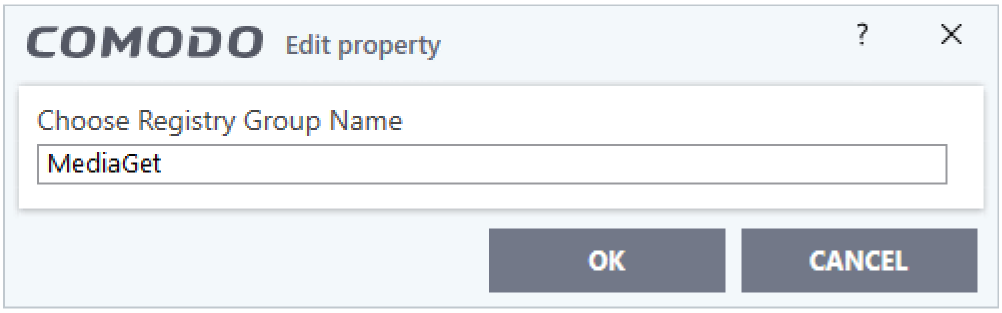
This interface allows you to:

  - **Create a new Registry Group**
  - **Add Registry key(s) to an existing group**
  - **Edit the names of an Existing Registry Group**
  - **Remove existing group(s) or individual key(s) from existing group**

- To add a new group or add key(s) to an existing group, click the 'Add' button



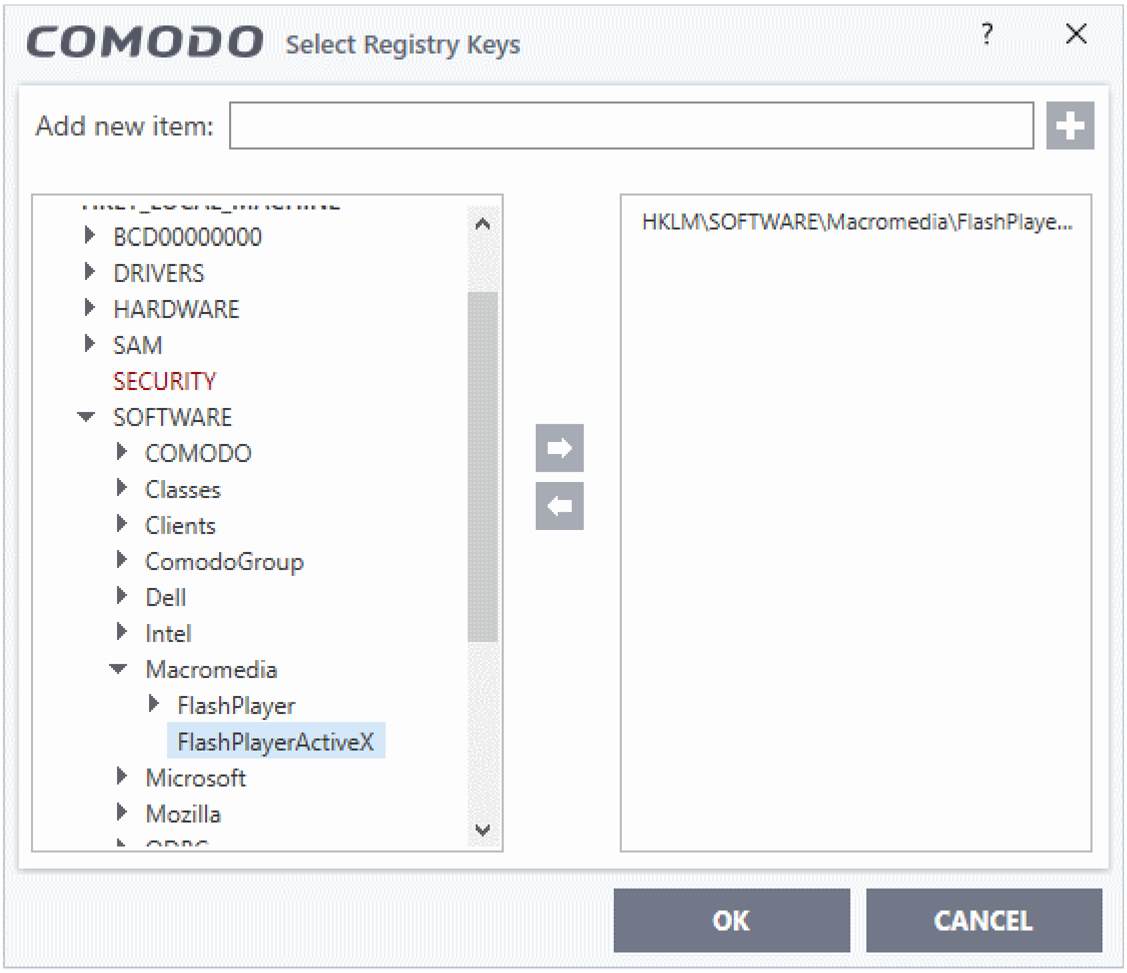
- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.



Choose Registry Group Name
MediaGet

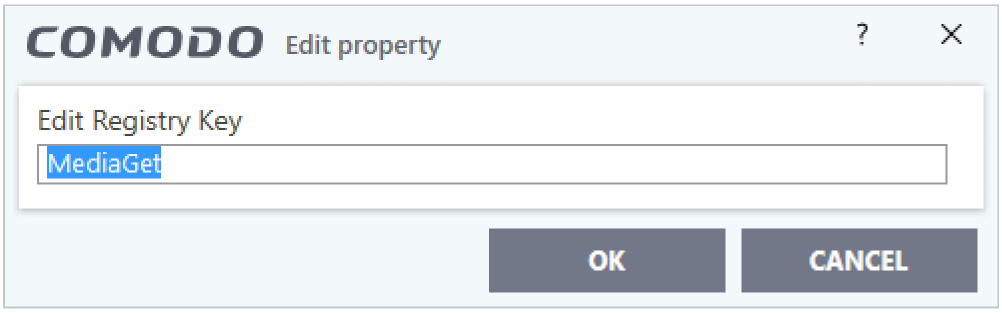
The group will be added to the list.

- **Add keys to a group** - Select the group from the list, click 'the Add' button and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.

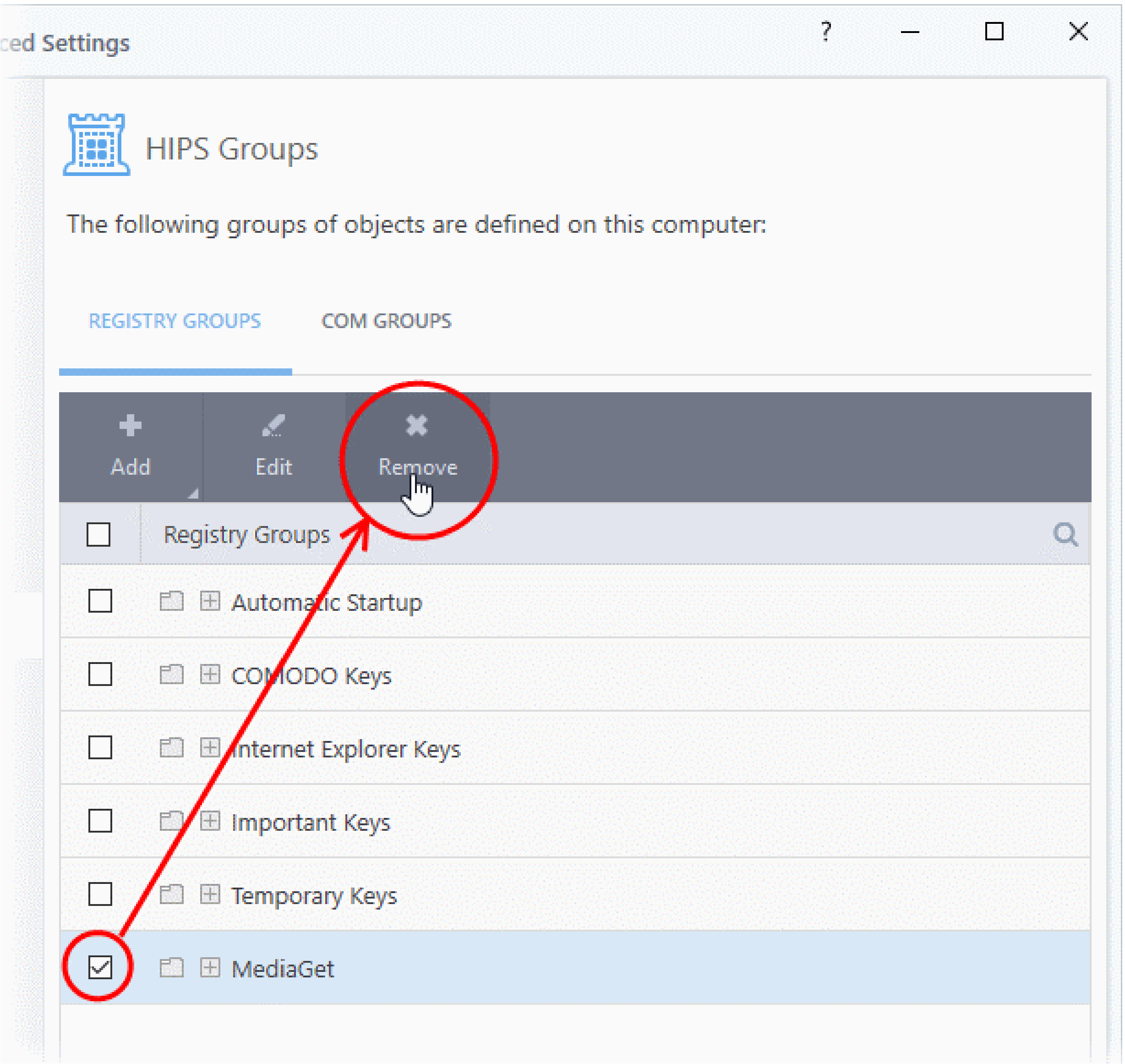


HKLM\SOFTWARE\Macromedia\FlashPlaye...

- Select a key on the left then click the right arrow to add a new key to the group. You can add a key manually by typing its name in the 'Add new item' field then clicking the '+' button.
- To edit an existing group, select the group from the list and click the 'Edit' button.



- Modify the name of the group as required and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.



- To remove a key from a group, first expand the group by clicking its '+' symbol, select the key to be removed and click the 'Remove' button.

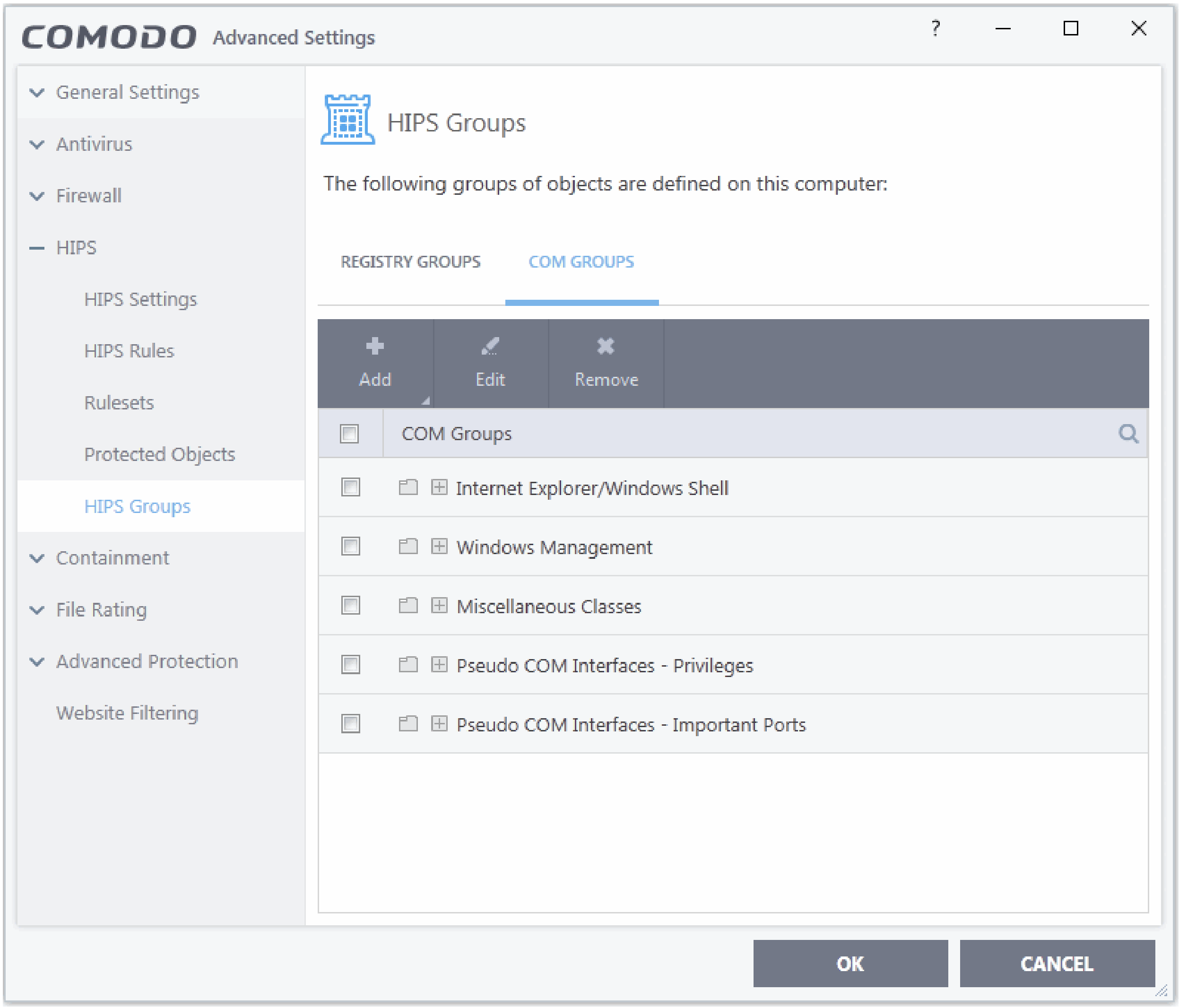
6.4.5.2. COM Groups

- COM groups are predefined groups of COM interfaces. COM interfaces are used by Windows to define how objects interact within a single application or between applications.

- COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks. It is therefore essential that COM interfaces are protected.
- Comodo Internet Security ships with the following, important COM groups: 'Internet Explorer/Windows Shell', 'Windows Management', 'Miscellaneous Classes', 'Pseudo COM Interfaces - Privileges' and 'Pseudo COM Interfaces - Important Ports'.
- Creating a COM group allows you to quickly add it to the 'COM' protection list. See '**Protected COM Interfaces**' for more details.

To open the 'COM Groups' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'HIPS' > 'HIPS Groups' on the left
- Click the 'COM Groups' tab



The following groups of objects are defined on this computer:

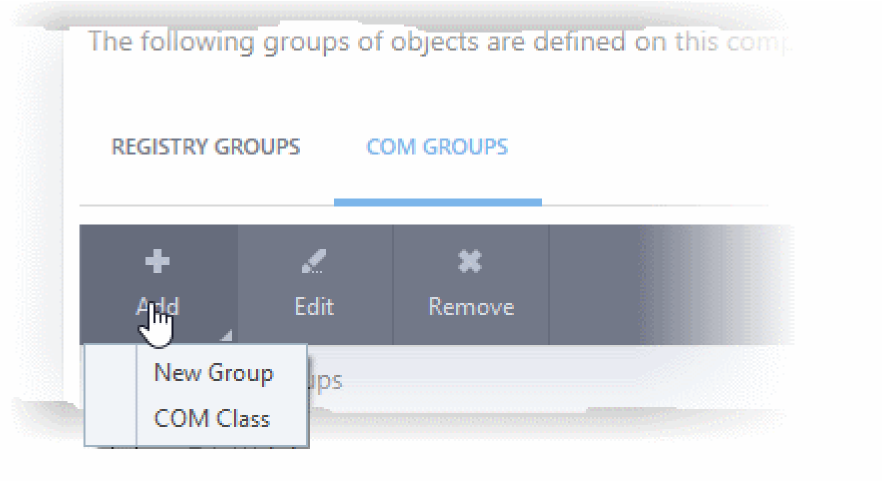
□	COM Groups
□	Internet Explorer/Windows Shell
□	Windows Management
□	Miscellaneous Classes
□	Pseudo COM Interfaces - Privileges
□	Pseudo COM Interfaces - Important Ports

- Click the search icon on the right to find a specific item. You can enter full or partial names.

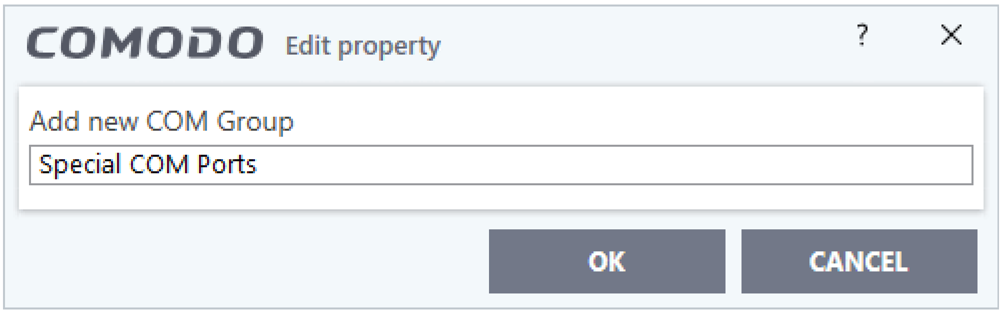
This interface allows you to:

- **Create a new COM Group**
- **Add COM Component(s) to an existing group**
- **Edit the names of an Existing COM Group**
- **Remove existing group(s) or individual COM Component(s) from existing group**

- To add a new group or add new COM Component(s) to an existing group, click the 'Add' button



- **Add a new group -** Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.

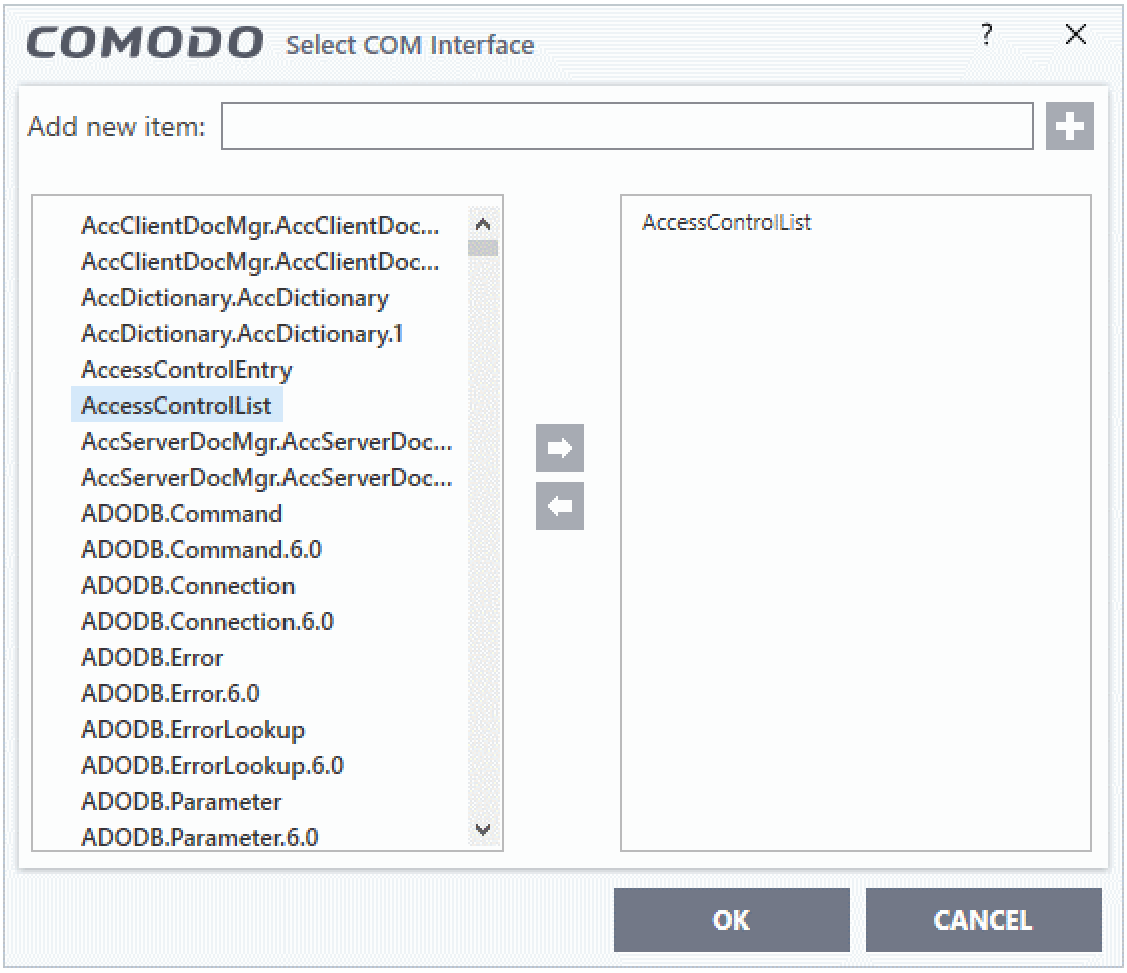


Add new COM Group

Special COM Ports

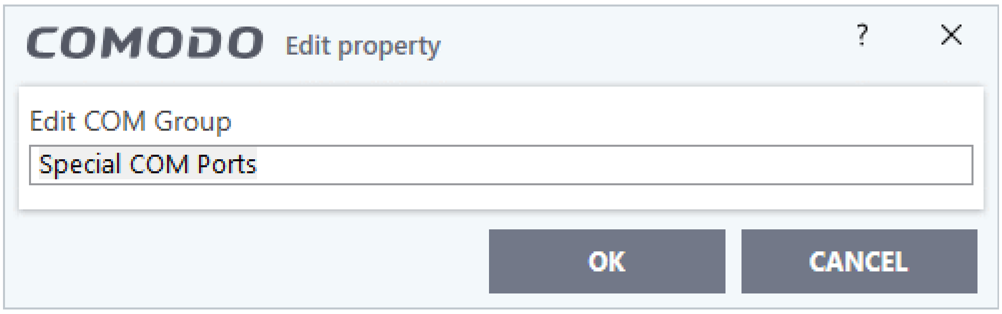
The group will be added to the list.

- **Add COM Components to a group -** Select the group, click the 'Add' button and choose 'COM Class'. The 'Select COM Interface' dialog will be opened.



You can add new items by selecting them on the left and clicking the right arrow button. To add items manually, type their name in the 'Add new item' field and press the '+' button.

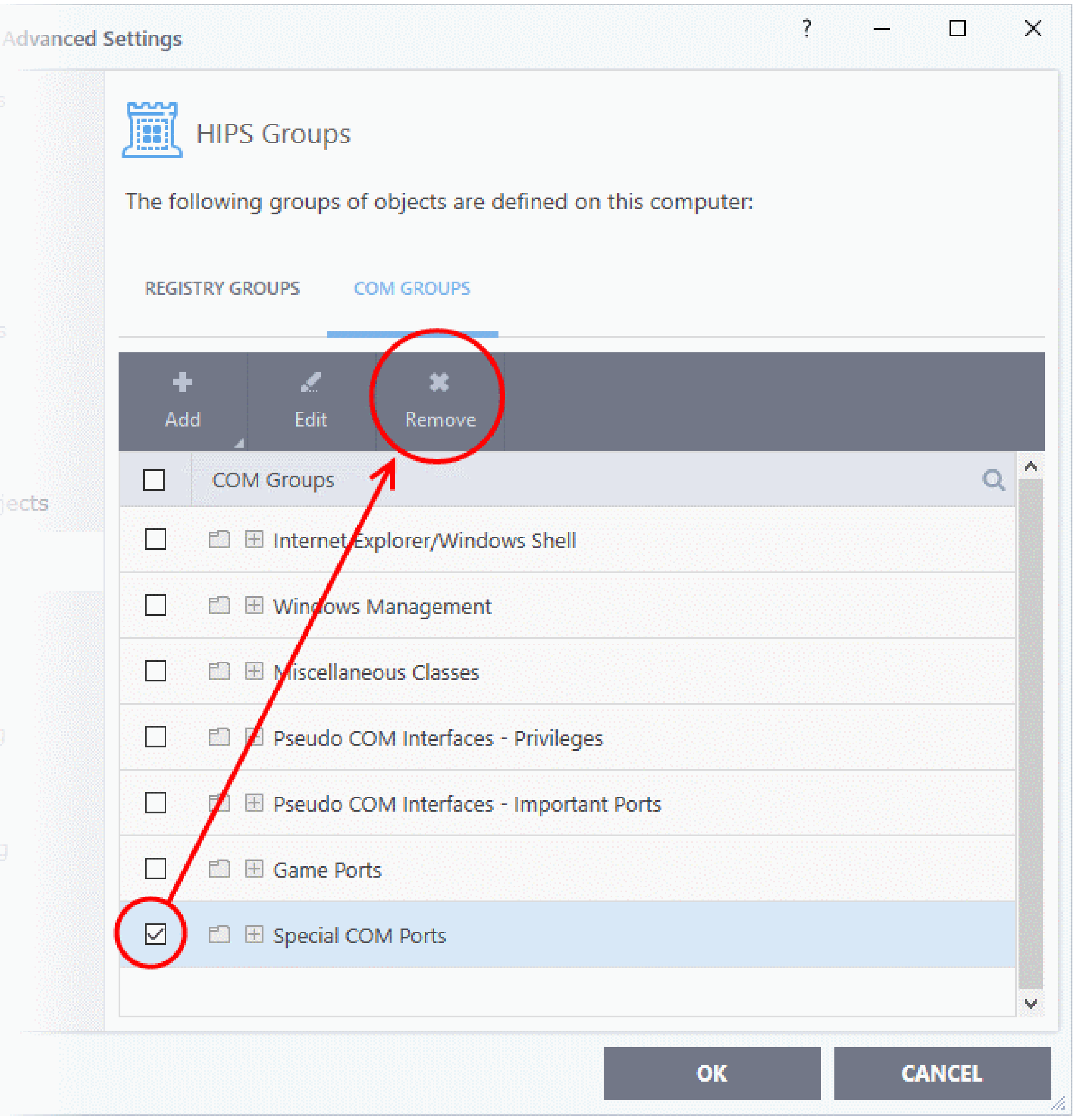
- To edit an existing group, select the group from the list and click the 'Edit' button.



Edit COM Group

Special COM Ports

- Edit the name of the group in the 'Edit Property' dialog and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.



Advanced Settings

HIPS Groups

The following groups of objects are defined on this computer:

- □ COM Groups
- □ Internet Explorer/Windows Shell
- □ Windows Management
- □ Miscellaneous Classes
- □ Pseudo COM Interfaces - Privileges
- □ Pseudo COM Interfaces - Important Ports
- □ Game Ports
- ☑ Special COM Ports

- To remove an individual COM component from a group, click + at the left of the group to expand the group, select the item to be removed and click the 'Remove' button.

6.5. Containment Configuration

If CIS encounters a file that has a trust status of 'Unknown' then you have the option to automatically run that file in the container. Files running in the container are isolated from the rest of your computer and your data to prevent them causing damage. The containment configuration section allows you define what level of restriction is applied to such 'Unknown' files:

- Run with restricted access to operating system resources
- Run completely isolated from your operating system and files on your computer
- Completely prevent it from running
- Allow to run outside the containment environment without restriction

See '**Auto-Containment Rules**' for more information about defining containment rules.

Applications running in the container are not allowed to write or save files to your local system. CIS creates a special folder called 'Shared Space' at 'C:/Program Data/Shared Space' so you can pass files between the container and your real system. This data can also be accessed by non-contained applications.

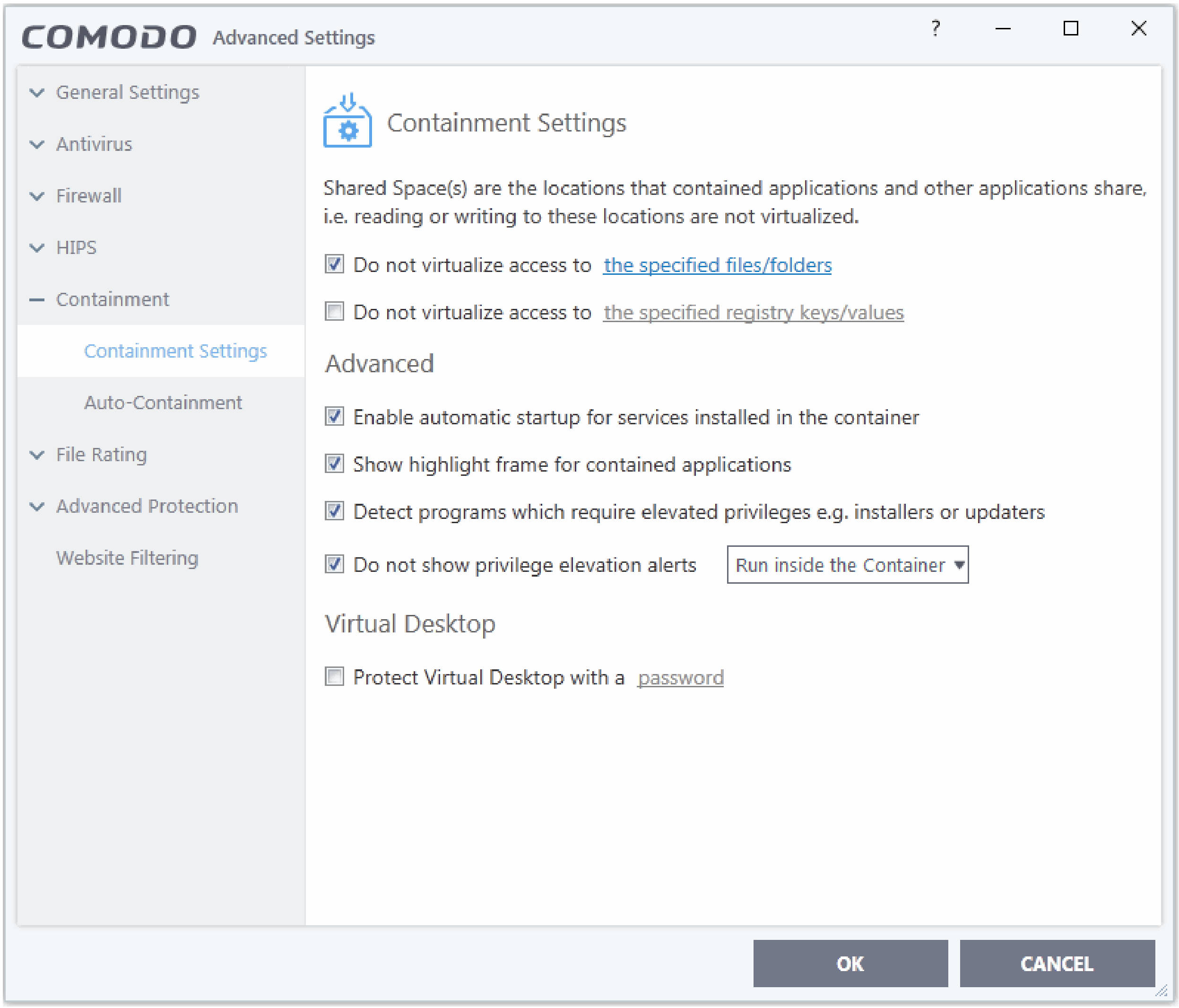
- See '**Containment - An Overview**' for background information about the containment process.
- See '**Unknown Files: The Scanning Processes**' for more information about how CIS determines the reputation of a file.

Important Note: The Containment feature is not supported on the following platforms:

- Windows XP 64 bit
- Windows Server 2003 64 bit

To open the containment interface:

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Containment' > 'Containment Settings' on the left



Containment Settings

Shared Space(s) are the locations that contained applications and other applications share, i.e. reading or writing to these locations are not virtualized.

☑ Do not virtualize access to the specified files/folders

□ Do not virtualize access to the specified registry keys/values

Advanced

☑ Enable automatic startup for services installed in the container

☑ Show highlight frame for contained applications

☑ Detect programs which require elevated privileges e.g. installers or updaters

☑ Do not show privilege elevation alerts — Run inside the Container ▾

Virtual Desktop

□ Protect Virtual Desktop with a password

The 'Containment Settings' and 'Auto-Containment' options allow you to quickly configure overall containment behavior and create rules for auto-contained selected programs.

Refer to the following sections for more details:

- **Containment - An Overview**
- **Unknown Files: The Scanning Processes**

- **Configuring the Containment Settings**
- **Configuring Rules for Auto-Containment**

6.5.1. Containment - An Overview

- Comodo Internet Security's container is an isolated operating environment for unknown and untrusted applications. Comodo has built automatic containment of unknown files into the security architecture of Comodo Internet Security, complementing and strengthening the Firewall, HIPS and Antivirus modules.
- Applications in the container cannot make permanent changes to other processes, programs or data on your 'real' system. They are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of the real system.
- After an unknown application has been placed in the container, CIS also automatically queues it for submission to Comodo Cloud Scanners for automatic behavior analysis.
- Firstly, the files undergo another antivirus scan using the very latest cloud blacklist.
    - If the scan discovers the file to be malicious then it is designated as malware and the result is sent back to your installation of CIS. The local black-list will also be updated.
    - If the scan does not detect that the file is malicious then its run-time behavior will be tested by Comodo's Instant Malware Analysis (CIMA) servers. If CIMA finds it to be malicious then the file is manually analyzed by Comodo technicians to confirm it as malware.
    - If confirmed as malware, the executable is added to the global antivirus black list. The 'malware' verdict is sent back to your installation of CIS and the file will be quarantined.
- This process delivers the perfect balance between usability and security for unknown files. Unknown applications can run 'normally' in the container but are denied any opportunity to damage your computer or access your data.

6.5.2. Unknown Files: The Scanning Processes

- When an executable is first run it passes through the following CIS security inspections:
    - Antivirus scan
    - HIPS Heuristic check
    - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CIS (and therefore not auto-contained or scanned in the cloud) in the following ways:
    - Because it is on the local Comodo White List of known safe applications
    - Because the user has rated the file as 'Trusted' in the '**File List**'
    - By the user granting the installer elevated privileges (CIS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CIS regards the installer and all files generated by the installer as safe)
    - Additionally, a file is not auto-contained or sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS Ruleset (See '**Active HIPS Rules**' for more details)
- **Cloud Scanning**

    Files and processes that pass the security inspections above but are not yet recognized as 'safe' (white-listed) are 'Unrecognized' files and contained automatically. In order to try to establish whether a file is safe or not, CIS will first consult Comodo's File Look-Up Server (FLS) to check the very latest signature databases:

    - A digital hash of the unrecognized process or file is created.
    - These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all

known malware and a white list of the signatures of the 'safe' files.

    - First, our servers check these hashes against the latest available black-list
    - If the hash is discovered on this blacklist then it is malware
    - The result is sent back to the local installation of CIS
  - If the hash is not on the latest black-list, it's signature is checked against the latest white-list
    - If the hash is discovered on this white-list then it is trusted
    - The result is sent back to local installation of CIS
    - The local white-list is updated
  - The FLS checks detailed above are near instantaneous.
  - If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'.
- Unrecognized files are simultaneously uploaded to Comodo's Instant Malware Analysis servers for further checks:
  - Firstly, the files undergo another antivirus scan on our servers.
  - If the scan discovers the file to be malicious (for example, heuristics discover it is a brand new variant) then it is designated as malware. This result is sent back to the local installation of CIS and the local and global black-list is updated.
  - If the scan does not detect that the file is malicious then it passes onto the next stage of inspection - behavior monitoring.
  - The behavior analysis system is a cloud based service that is used to help determine whether a file exhibits malicious behavior. Once submitted to the system, the unknown executable will be automatically run in a virtual environment and all actions that it takes will be monitored. For example, processes spawned, files and registry key modifications, host state changes and network activity will be recorded.
  - If these behaviors are found to be malicious, the file is submitted to our technicians for further manual checks and confirmation. If the manual testing confirms it as a malware, then it will be added to the global blacklist which will benefit all users. The results will be sent back to local installation of CIS, file will be quarantined and the user alerted.

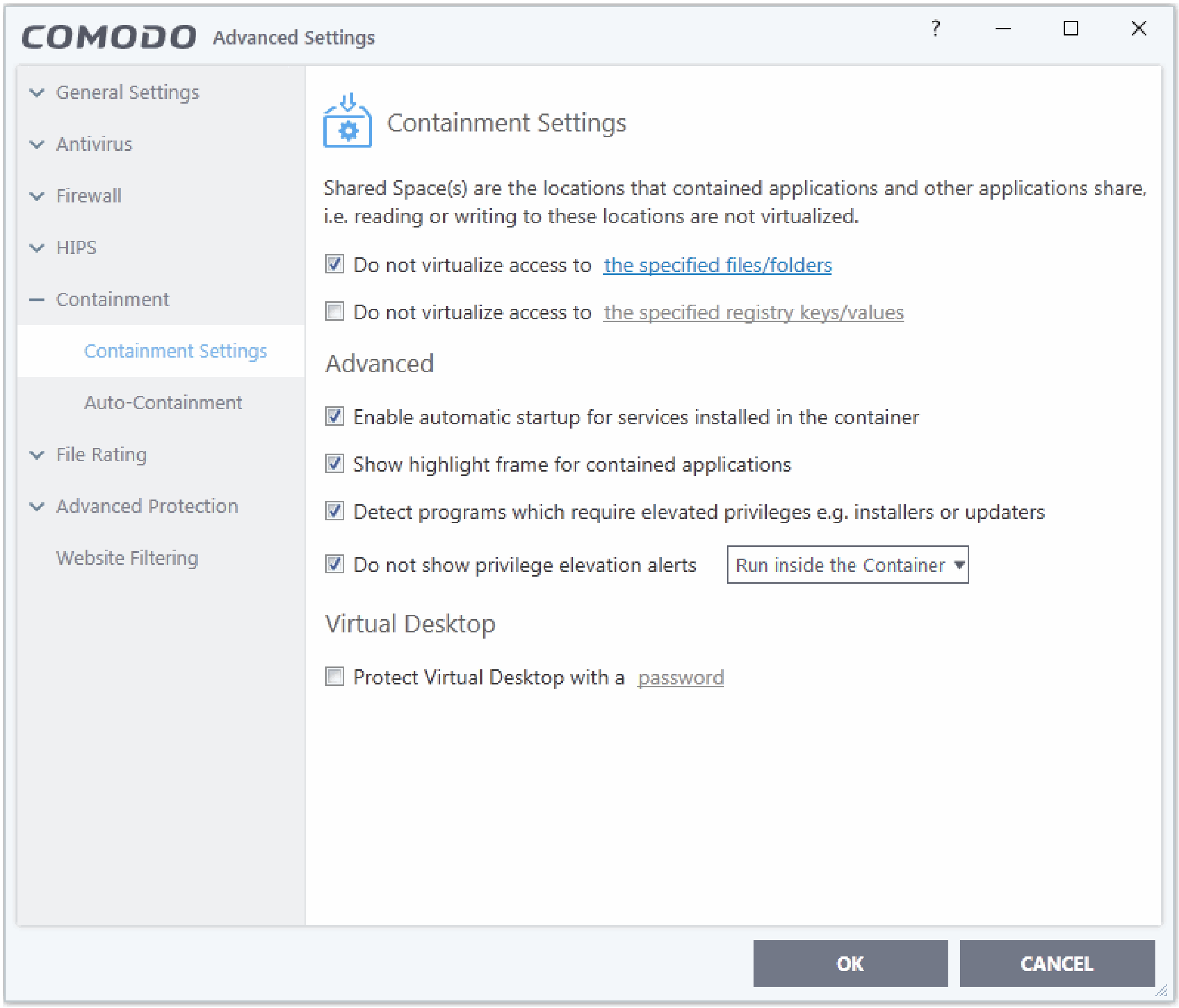
If the manual analysis confirms the file is safe, then it will be added to global whitelist and results sent back to local installation of CIS.

6.5.3. Containment Settings

The 'Containment Settings' panel lets you configure how proactive the auto-containment feature should be, and which types of files it should check.

To open the 'Containment Settings' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Containment' > 'Containment Settings' on the left



Containment Settings

Shared Space(s) are the locations that contained applications and other applications share, i.e. reading or writing to these locations are not virtualized.

☑ Do not virtualize access to the specified files/folders

□ Do not virtualize access to the specified registry keys/values

Advanced

☑ Enable automatic startup for services installed in the container

☑ Show highlight frame for contained applications

☑ Detect programs which require elevated privileges e.g. installers or updaters

☑ Do not show privilege elevation alerts — Run inside the Container

Virtual Desktop

□ Protect Virtual Desktop with a password

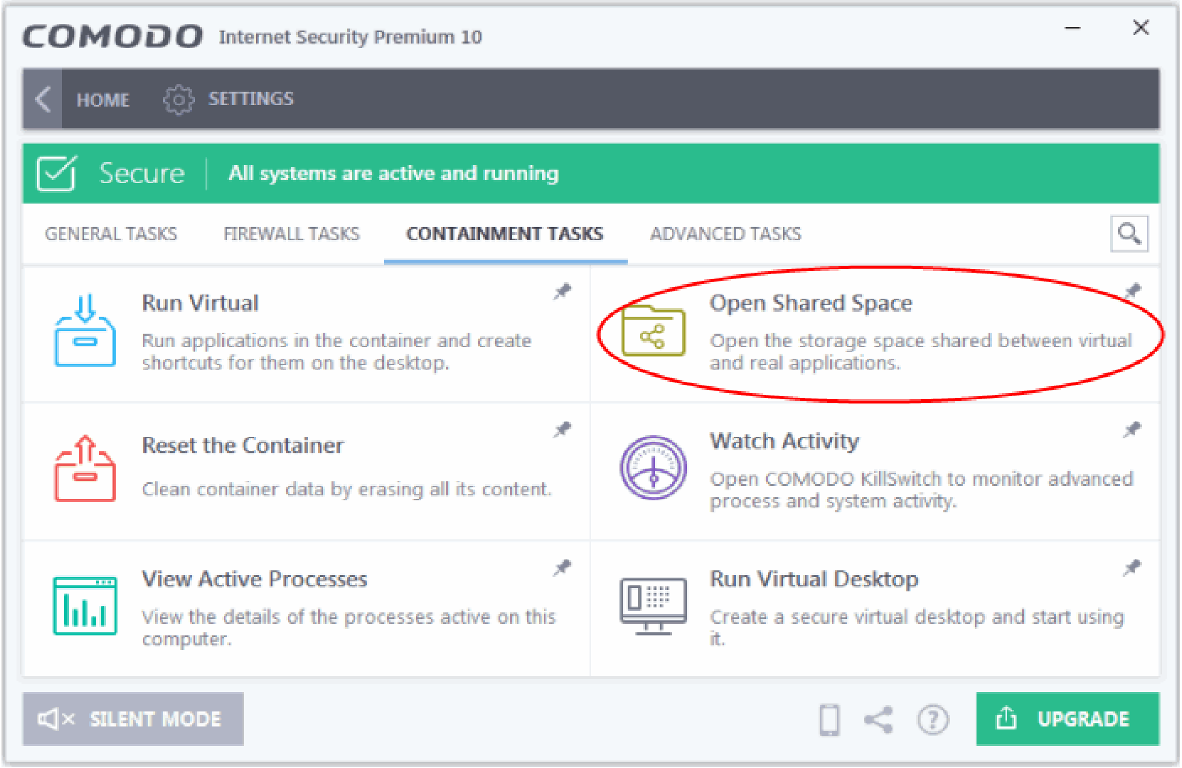
Click the following links to find out more about each section:

- **Shared Space Settings** - Shared space lets you swap files between the sandbox environment and your real computer. Files downloaded or generated by contained applications that you wish to access from your real system should be downloaded to the shared space
- **Advanced Settings** - Allows you to configure containment alert settings as well as to enable automatic startup services for programs installed in the Containment.
- **Virtual Desktop** - Create an 'exit' password for the Virtual Desktop. If set, the Virtual Desktop cannot be closed or minimized until the correct password is entered. This prevents guests, younger users or unauthorized users from exiting the sandbox environment.

Shared Space Settings:

'Shared Space' is a dedicated area on your local drive that contained applications are allowed to write to. Files in shared space can also be accessed by non-contained applications. For example, any files or programs you download via a contained browser that you wish to be able to access from your real system should be downloaded to the shared space. This folder is also used by the Virtual Desktop and is located by default at 'C:/Program Data/Shared Space'.

You can access the shared space folder by opening 'Containment Tasks' from the Tasks interface then clicking 'Open Shared Space'.



Run Virtual
Run applications in the container and create shortcuts for them on the desktop.

Open Shared Space
Open the storage space shared between virtual and real applications.

Reset the Container
Clean container data by erasing all its content.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

View Active Processes
View the details of the processes active on this computer.

Run Virtual Desktop
Create a secure virtual desktop and start using it.

Exclusions

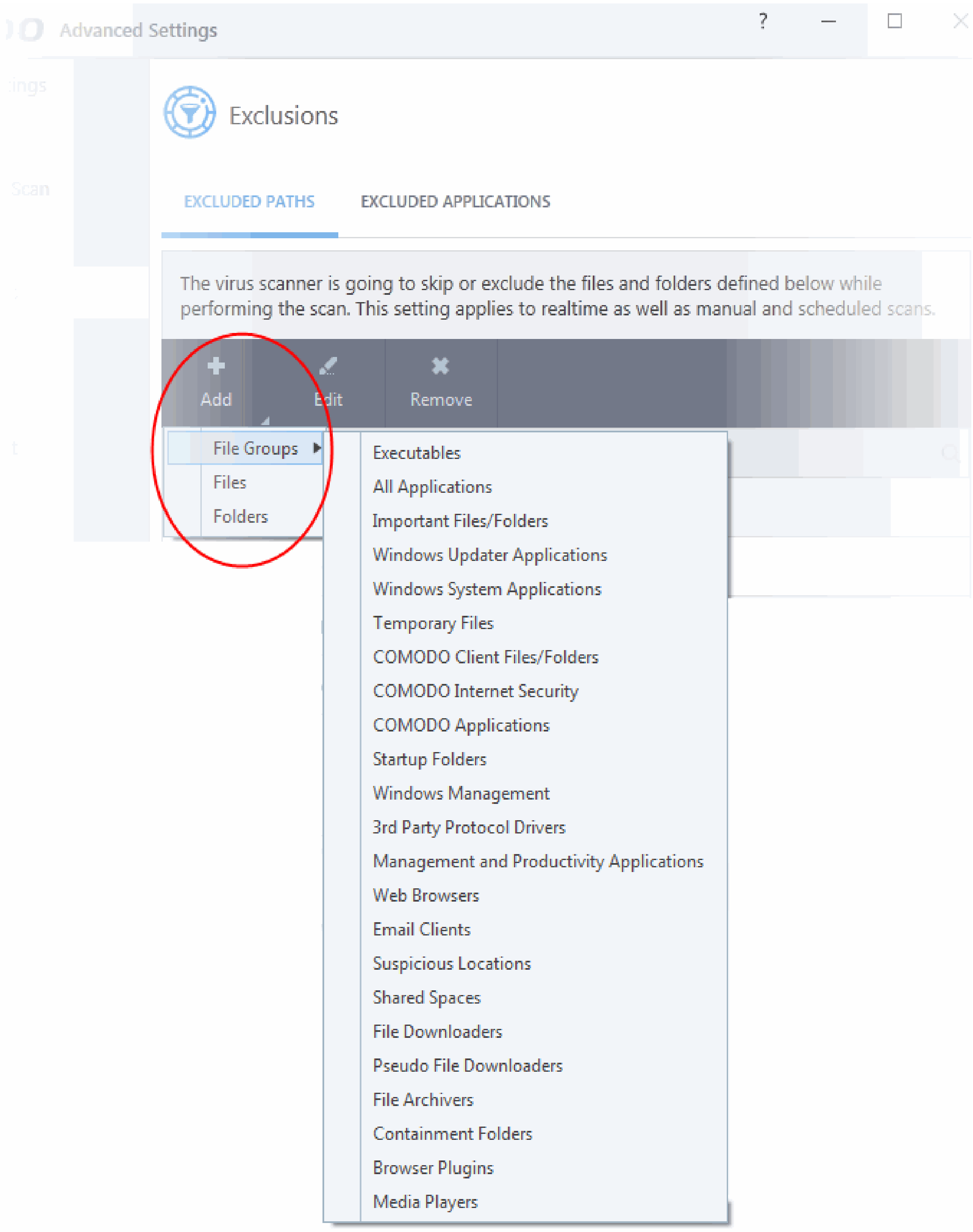
By default, contained applications can access folders and files on your 'real' system but cannot modify them. However, you can define exclusions to this rule by using the 'Do not virtualize access to...' links.

To define exclusions for files and folders

- Enable 'Do not virtualize access to the specified files/folders' then click the link 'the specified files/folders'.

The 'Manage Exclusions' dialog will appear with a list of defined exclusions. You can search for a specific item from the list by clicking the search icon at the far right of the column header and entering the name of the item in part or full.

- Click the 'Add' button in the 'Manage Exclusions' dialog.



Advanced Settings

Exclusions

The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

- **Files** - Allows you to specify files or applications that contained applications are able to access
- **Folders** - Specify a folder that can be accessed by contained applications
- **File Groups** - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd. See '**File Groups**', for more details on file groups.
- **Running Processes** - Allows you to choose a process from the list of currently running processes, so that the parent application of the chosen process will be added to the exclusion.

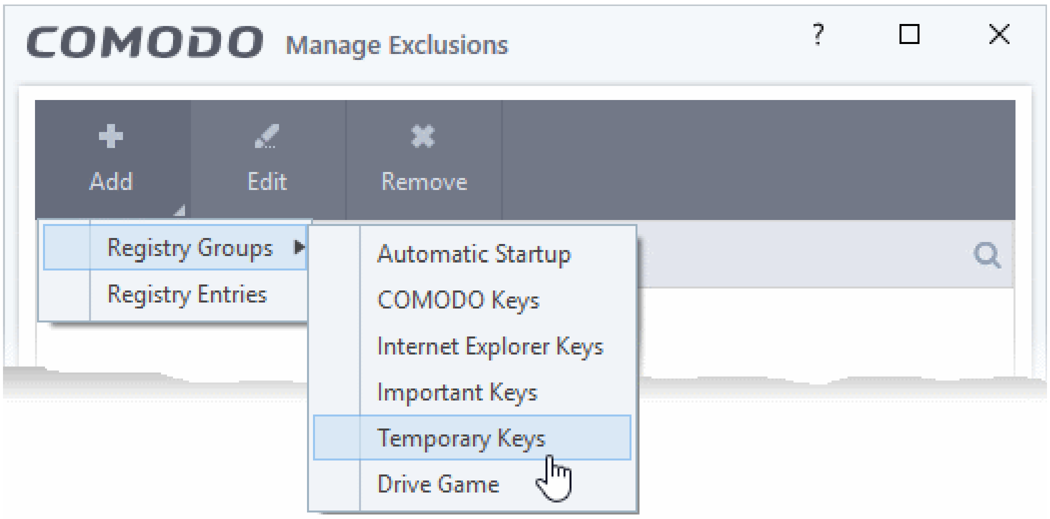
- To edit an exception, select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Change file or folder location path and click 'OK'
- Click 'OK' to implement your settings

To define exclusions for specific Registry keys and values

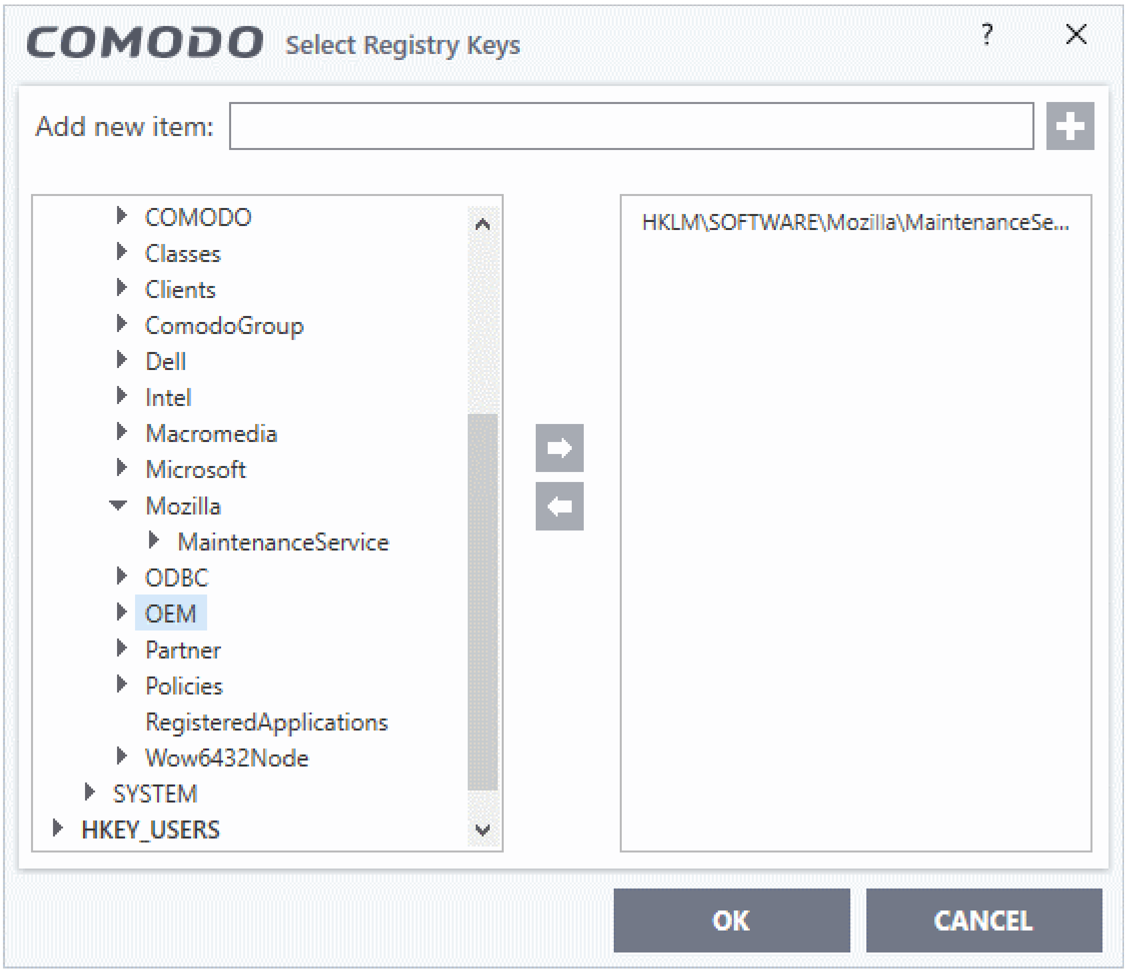
- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the link 'the specified registry keys/values'.

The 'Manage Exclusions' dialog will appear with the list of excluded registry keys and values. You can search for a specific item from the list by clicking the search icon at the far right of the column header and entering the name of the item in part or full.

- Click the 'Add' button in the 'Manage Exclusions' dialog.

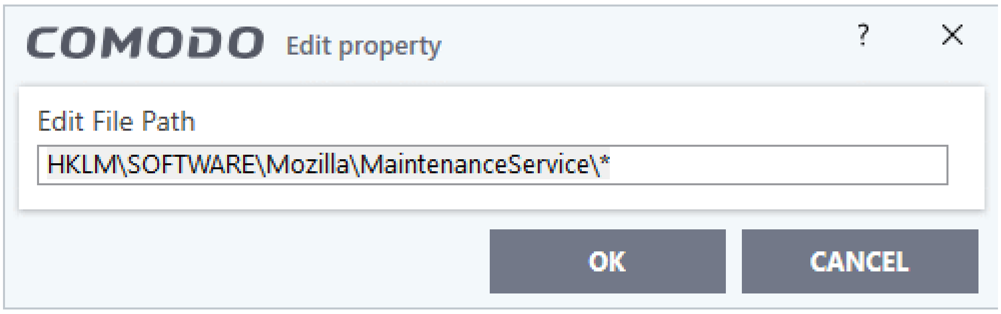


- **Registry Groups -** Allows you to batch select a predefined group of important registry keys as exclusions. See '**Registry Groups**', for an explanation of CIS registry groups.
- **Registry Entries -** Opens an interface that allows you to quickly browse Windows registry keys and add them as exclusions:



- Click 'OK' to implement your settings.

- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Edit the key path and click 'OK'.

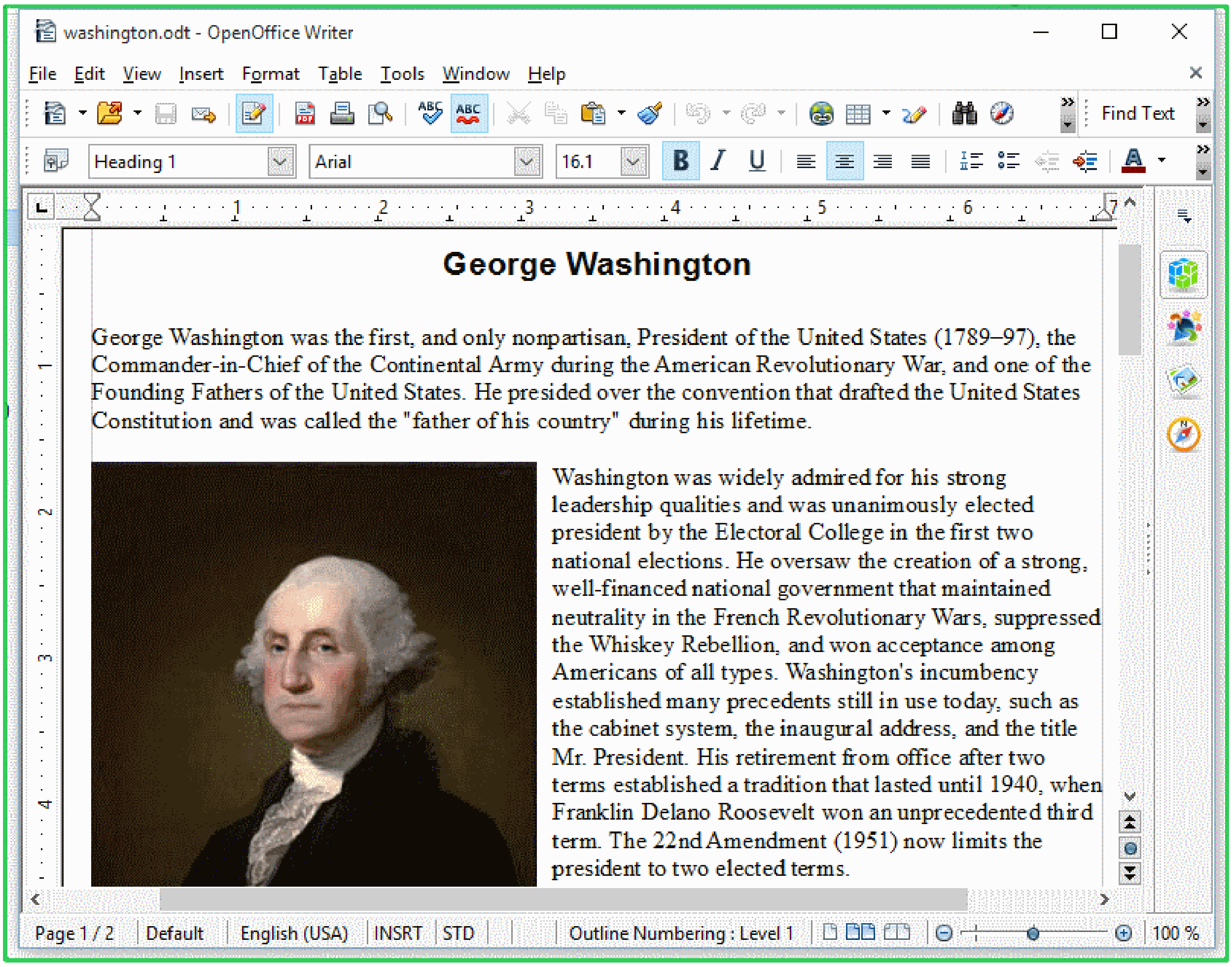


HKLM\SOFTWARE\Mozilla\MaintenanceService\*

Advanced Settings:

- **Enable automatic startup for services installed in the container** - CIS permits contained services to run at Windows startup only if this option is enabled. Clear this check-box if you do not want those services to run at Windows Startup. (***Default = Enabled***)
- **Show highlight frame for contained applications** - If enabled, CIS displays a green border around the windows of programs that are running inside the container. (***Default = Enabled***)

The following example shows an .odt document opened with a contained instance of OpenOffice Writer:

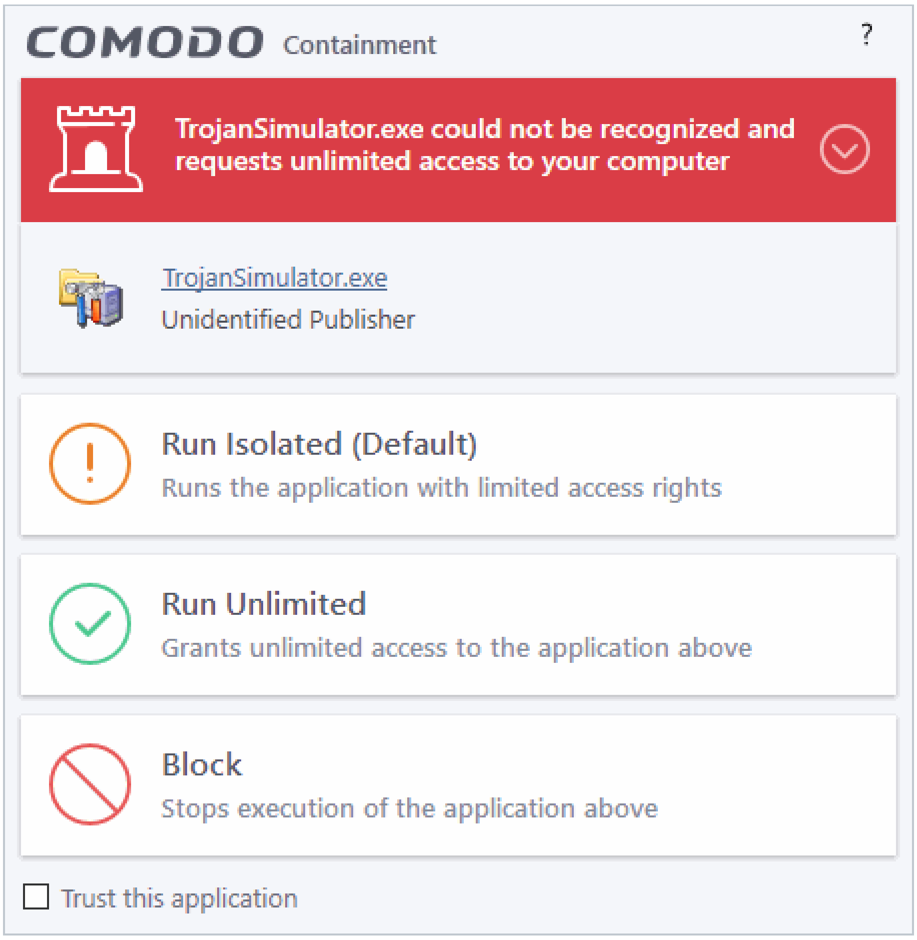

washington.odt - OpenOffice Writer
File Edit View Insert Format Table Tools Window Help
Find Text
Heading 1
Arial
16.1
Page 1 / 2
Default
English (USA)
INSRT
STD
Outline Numbering : Level 1
100 %

George Washington

George Washington was the first, and only nonpartisan, President of the United States (1789–97), the Commander-in-Chief of the Continental Army during the American Revolutionary War, and one of the Founding Fathers of the United States. He presided over the convention that drafted the United States Constitution and was called the "father of his country" during his lifetime.

Washington was widely admired for his strong leadership qualities and was unanimously elected president by the Electoral College in the first two national elections. He oversaw the creation of a strong, well-financed national government that maintained neutrality in the French Revolutionary Wars, suppressed the Whiskey Rebellion, and won acceptance among Americans of all types. Washington's incumbency established many precedents still in use today, such as the cabinet system, the inaugural address, and the title Mr. President. His retirement from office after two terms established a tradition that lasted until 1940, when Franklin Delano Roosevelt won an unprecedented third term. The 22nd Amendment (1951) now limits the president to two elected terms.

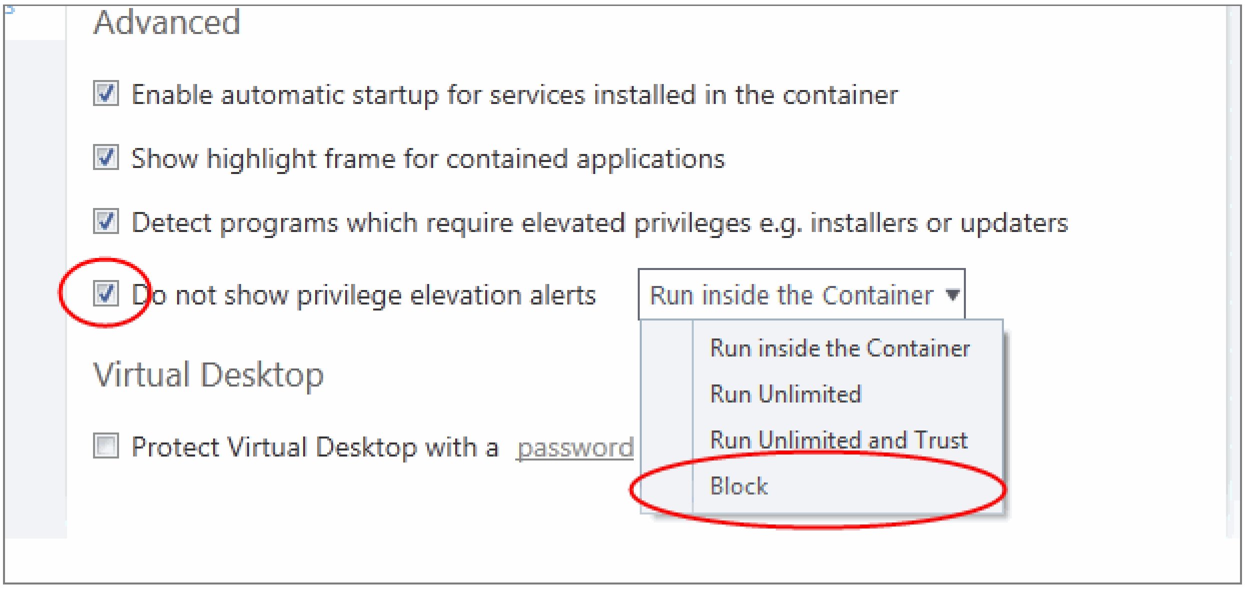
- **Detect programs which require elevated privileges, e.g., installer or updaters:** Allows you to instruct the Container to display alerts when an installer or updater requires administrator or elevated privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry. See '**Understanding Security Alerts**' for more details.


COMODO Containment
?
TrojanSimulator.exe could not be recognized and requests unlimited access to your computer
TrojanSimulator.exe
Unidentified Publisher
Run Isolated (Default)
Runs the application with limited access rights
Run Unlimited
Grants unlimited access to the application above
Block
Stops execution of the application above
□ Trust this application

You can decide whether or not to allow the installer/updater from the options in the alert. ***(Default=Enabled)***

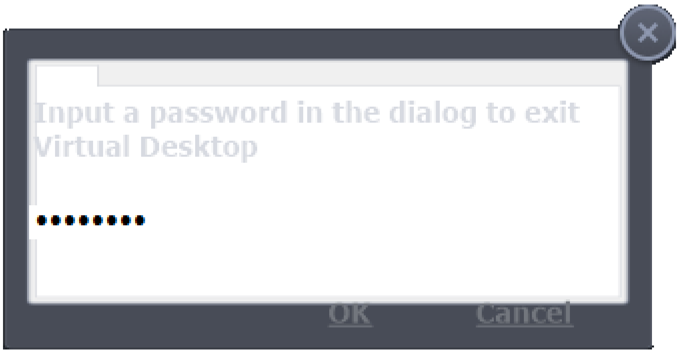
- **Do not show privilege elevation alerts**: Allows you to instruct the Container to not to display alerts (as shown above) when a new or unrecognized application requires administrator or elevated privileges to run.

  On selecting this option, you need to choose the action to be taken by the container from the drop-down. (***Default=Disabled***)


Advanced
☑ Enable automatic startup for services installed in the container
☑ Show highlight frame for contained applications
☑ Detect programs which require elevated privileges e.g. installers or updaters
☑ Do not show privilege elevation alerts
Run inside the Container
Run inside the Container
Run Unlimited
Run Unlimited and Trust
Block
Virtual Desktop
□ Protect Virtual Desktop with a password

Virtual Desktop Settings

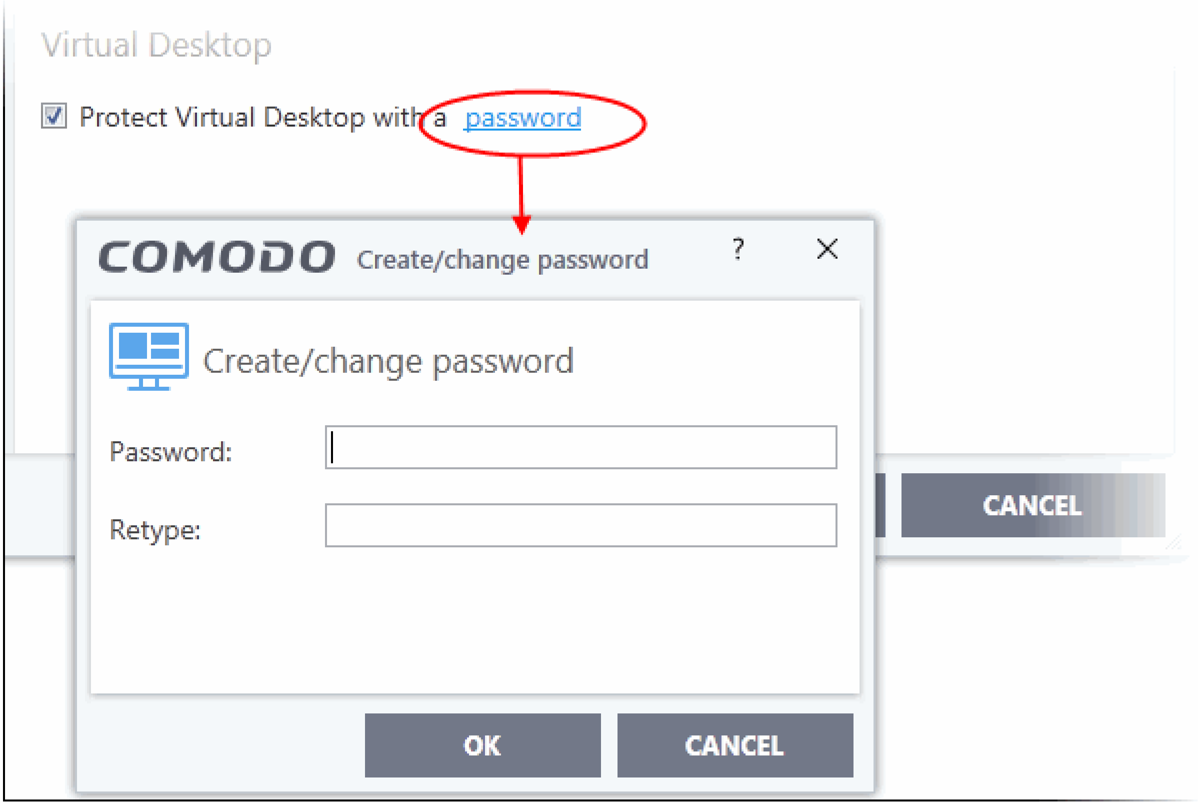
The 'Virtual Desktop' Settings area allows you to password protect your Virtual Desktop. Once set, the password has to be entered every time the Virtual Desktop is closed.



The exit password acts as a security measure to prevent guests or younger users from exiting the secure Virtual Desktop and potentially exposing your computer to danger.

To set an exit password for Virtual Desktop:

- Check the 'Protect Virtual Desktop with a password' box then click the password link. The 'Create/change password' dialog will appear:


Virtual Desktop
☑ Protect Virtual Desktop with a password
COMODO Create/change password
?
Create/change password
Password:
Retype:
OK
CANCEL
CANCEL

- Type a password that cannot easily be guessed. It should be at least 8 characters long and contain a combination of uppercase and lowercase letters, numbers and special characters.
- Re-enter the password in the 'Retype' field then click 'OK'.

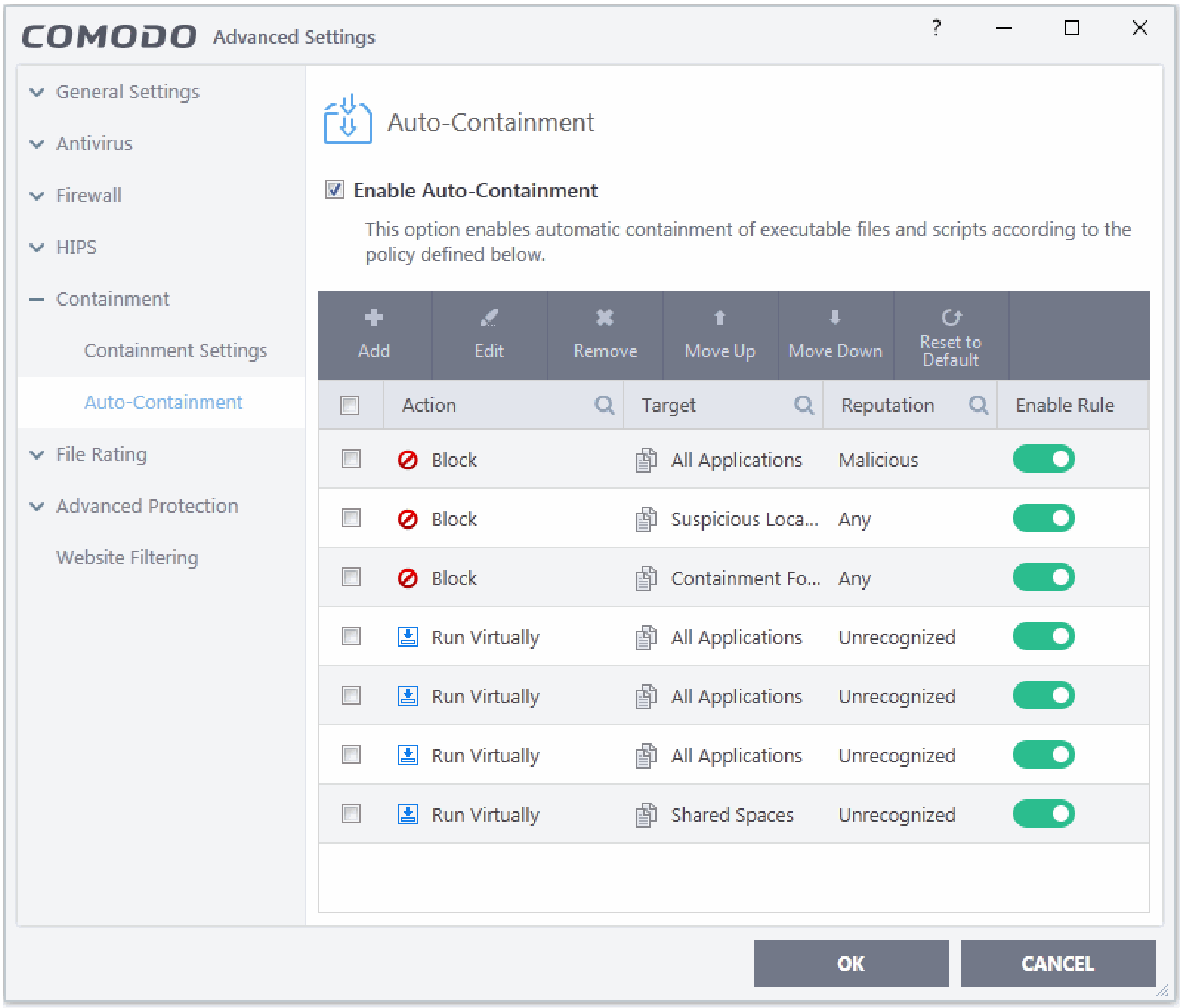
You will now be asked for a password every time you exit the Virtual Desktop.

6.5.4. Auto-Containment Rules

- The 'Auto-Containment' panel allows you to add and define rules for programs that run in the container.
- A contained application has much less opportunity to damage your computer because it is isolated from your operating system, important system files and personal data. This allows you to safely run applications that you are not 100% sure about.
- Auto-containment rules allow you to determine whether programs should be allowed to run with full privileges, ignored, run restricted or run in a fully-virtual environment. For easy identification, Comodo Internet Security will show a green border around programs that are running in the container.
- CIS ships with a set of pre-configured containment rules which provide maximum protection against unknown, potentially malicious applications.

To open the Auto-Containment panel

- Open the 'Advanced Settings' interface by clicking the 'Settings' link from the top left
- Click 'Containment' from the left and choose 'Auto-Containment'



Auto-Containment

☑ Enable Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malicious	●
□	Block	Suspicious Loca...	Any	●
□	Block	Containment Fo...	Any	●
□	Run Virtually	All Applications	Unrecognized	●
□	Run Virtually	All Applications	Unrecognized	●
□	Run Virtually	All Applications	Unrecognized	●
□	Run Virtually	Shared Spaces	Unrecognized	●

The 'Auto-Containment' panel contains configuration options and a list of currently defined auto-contained rules. You can add new rules and manage existing rules from this panel.

General Settings

- **Enable Auto-Containment** - Allows you to enable or disable the Containment. If enabled, the applications are run inside the container as per the rules defined. (***Default = Enabled***)

Containment Rules

Containment Rules - Column Descriptions	
Column Header	**Description**
Action	The operation that the container should perform on the 'Target' if the rule is triggered.
Target	The files, file groups or specified locations on which the rule will be executed.
Reputation	The trust status of the 'Target' files to which the rule will apply. Can be 'Malware', 'Trusted' 'Unrecognized' or 'Any'.
Enable Rule	Allows you to enable/disable the rule.

CIS ships with a set of pre-defined auto-containment rules that are configured to provide maximum protection for your system. The table provides the configuration settings for these pre-defined rules:

Predefined Rule no.			1	2	3	4	5	6	7
Action			Block	Block	Block	Ignore	Run Virtually	Run Virtually	Run Virtually
Target			File Group - All Applications	File Group - Suspicious Locations	File Group - Contained Folders	File Group - Metro Apps	File Group - All Applications	File Group - All Applications	File Group - Shared Spaces
File Reputation			Malicious	Any	Any	Any	Unrecognized	Unrecognized	Unrecognized
File origin	Source of file creation	Process(es)	Any	Any	Any	Any	Any	Web Browsers Email Clients File Downloaders Pseudo File Downloaders File Archivers Management and Productivity Applications Browser Plugins Media Players	Any
		user(s)	Any	Any	Any	Any	Any	Any	Any
	Downloaded from		Any	Any	Any	Any	Intranet	Any	Any

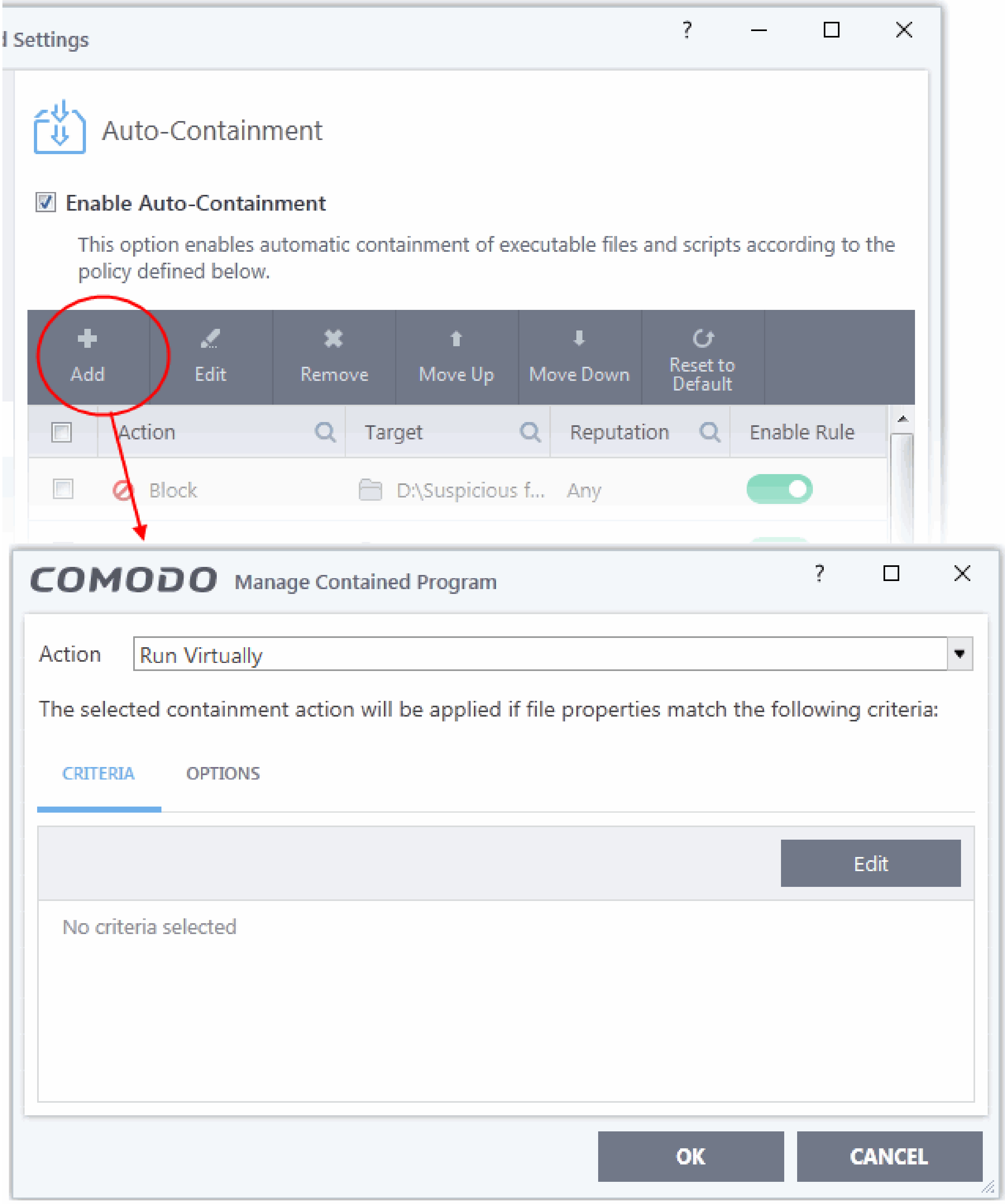
					Removable Media Internet		
Age of file		Any	Any	Any	Any	Any	Any	Any
Log Action		On	On	On	On	On	On	On
Restriction Level		N/A	N/A	N/A	N/A	Partially Limited	Off	Off
Limit Maximum Memory		N/A	N/A	N/A	N/A	Off	Off	Off
Limit Program Execution Time		N/A	N/A	N/A	N/A	Off	Off	Off
Quarantine		On	Off	Off	N/A	N/A	N/A	N/A
Exclude child processes from the action		N/A	N/A	N/A	Off	N/A	N/A	N/A

When you open an application, the auto-containment rules are prioritized by CIS in order from top to bottom. You can re-prioritize rules using the 'Move Up' and 'Move Down' buttons at the top of the list.

Adding an Auto-Containment Rule

Auto-containment rules can be created for a single application, for all applications in a folder or file group, for running processes or for applications based on their file or for process hash. You can add detailed filters by specifying the 'file creation source', 'file origin', 'file rating' and 'file age' and specify the action to be taken on the contained file. You can also create simple rules to run an application in the container just by specifying the action and the target application.

- Click the 'Add' button at the top of the list in the Auto-Containment panel.



☑ Enable Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
□	Block	D:\Suspicious f...	Any	●

Action: Run Virtually

The selected containment action will be applied if file properties match the following criteria:

No criteria selected

The 'Manage Contained Program' dialog will appear. The 'Manage Contained Program' displays the action at the top and contains two tabs:

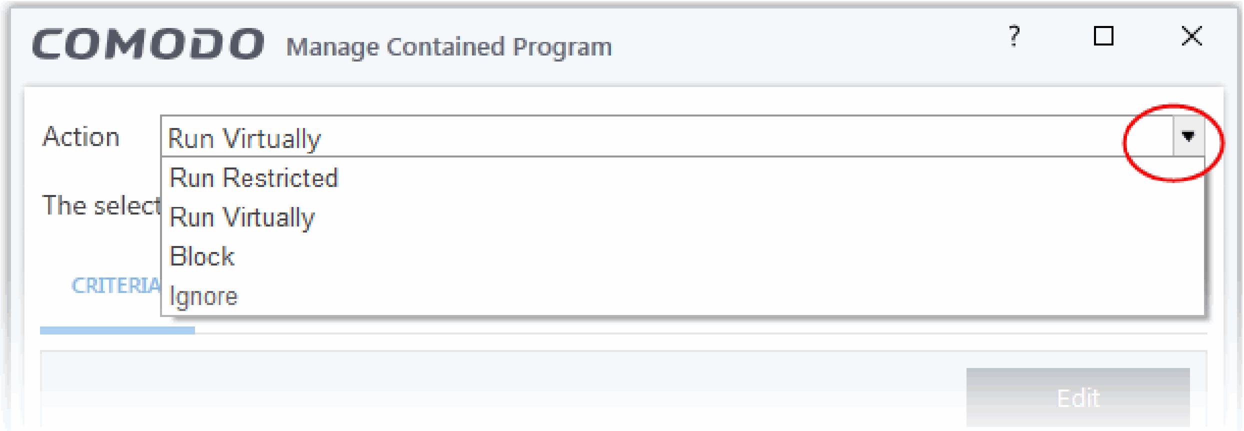
- **Criteria** - Allows you to define conditions upon which the rule should be applied.
- **Options** - Allows you to configure additional actions like logging, setting memory usage and execution time restrictions.

Creating a new containment rule involves the following steps:

- Step 1 - Choose the action
- Step 2 - Select the target file/group and set the filter criteria for the target files
- Step 3 - Select the options

Step 1 - Choose the action

The settings in the 'Action' drop-down combined with the restriction level in the 'Options' tab determine the privileges of an auto-contained application. This determines what right it has to access other processes and hardware resources on your computer.



The options available under the 'Action' drop-down are:

- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Run Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be contained and allowed to run with all privileges.

- Choose the action from the options.

Step 2 - Select the target file/group and set the filter criteria for the target files

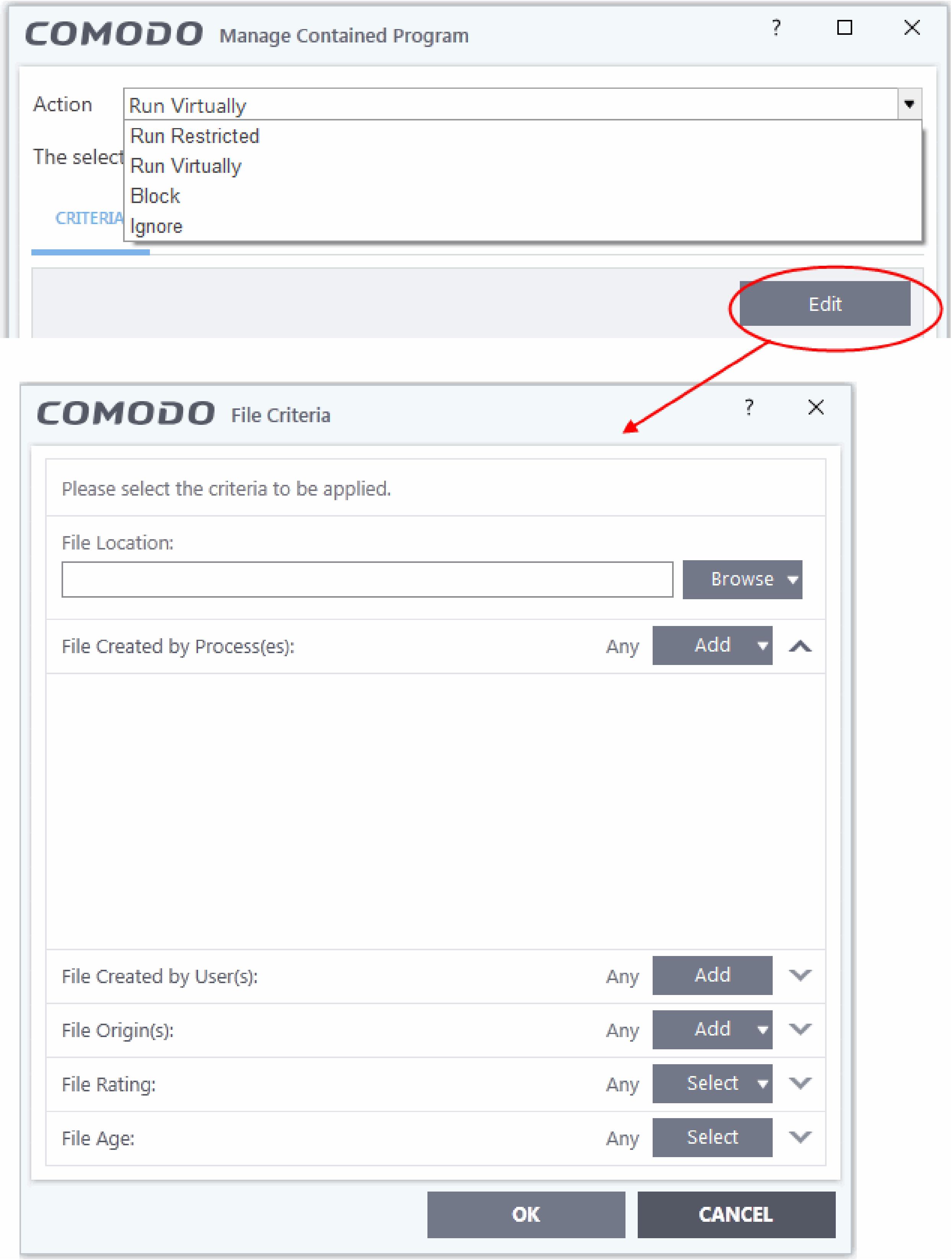
The next step is to select the target application(s)/file(s) and configure the filter parameters. You can filter to a rule so that it applies to specific types of file. For example, you can specify 'All executables' as the target and add a filter so it only affects executables downloaded from the internet. Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target and 'File created by specific user' as the filter criteria.

To select the target and set the filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- To add new target and filter criteria, click the 'Edit' button at the far right



Please select the criteria to be applied.

File Location:

File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

File Rating: Any

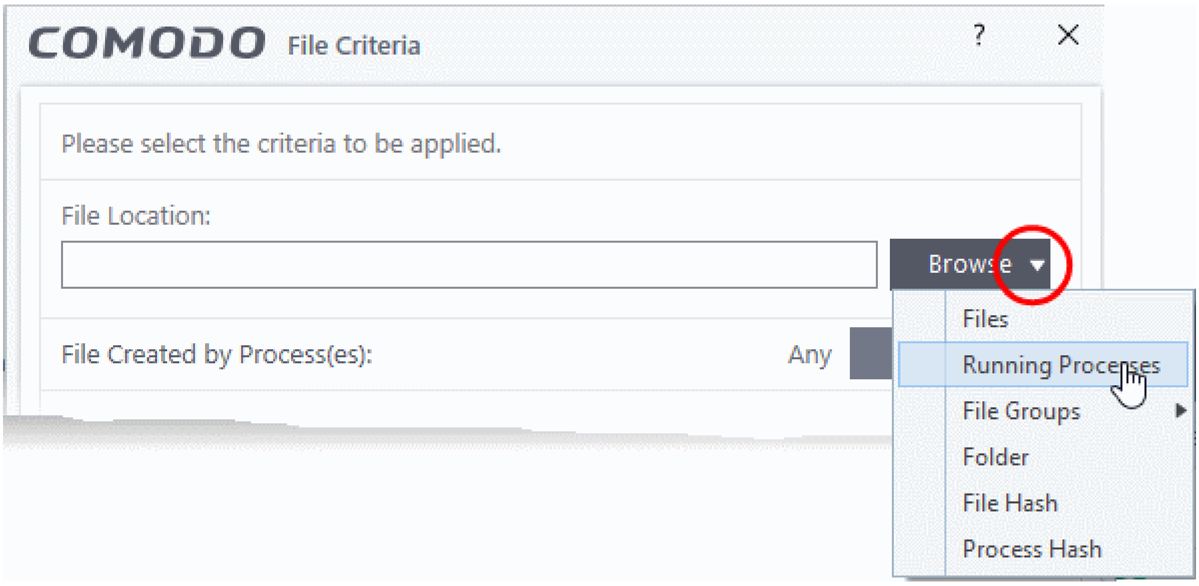
File Age: Any

The 'File Criteria' dialog will open. The file criteria dialog allows you:

- **Select the target**
- **Configure the filter criteria**

Select the target

- To select the target, click the 'Browse' button beside the 'File Location' field



COMODO File Criteria

Please select the criteria to be applied.

File Location:

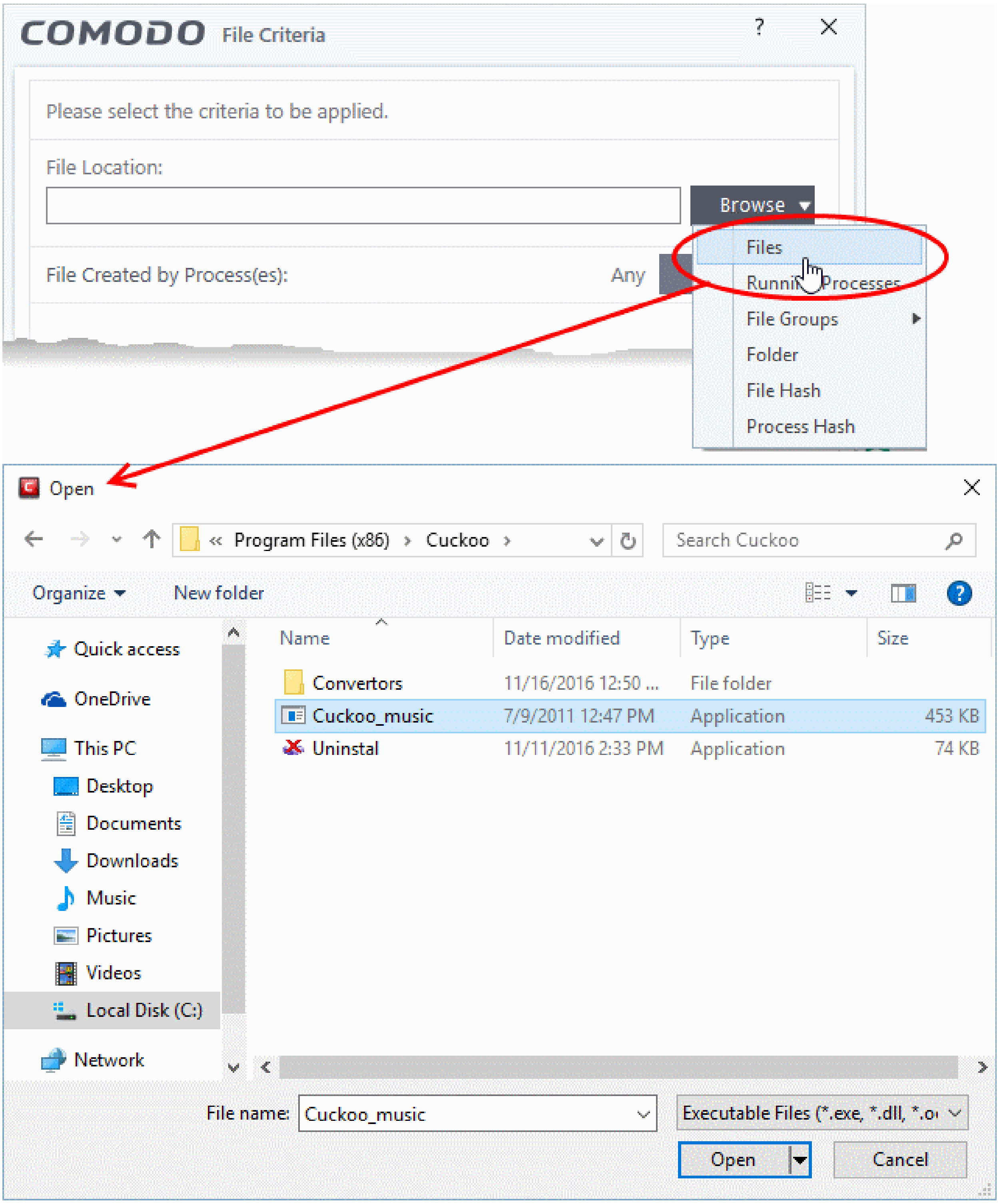
File Created by Process(es): Any

You have six options available for adding a target:

- **Files** - Allows to add individual files as target.
- **Running Processes** - As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** - Allows to add predefined File Groups as target. To add or modify a predefined file group refer to the section **File Groups** for more details.
- **Folder** - Allows you to add a folder or drive as the target
- **File Hash** - Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

Adding an individual File

- Choose 'Files' from the 'Browse' drop-down.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

File Created by Process(es): Any

Open

Program Files (x86) › Cuckoo ›

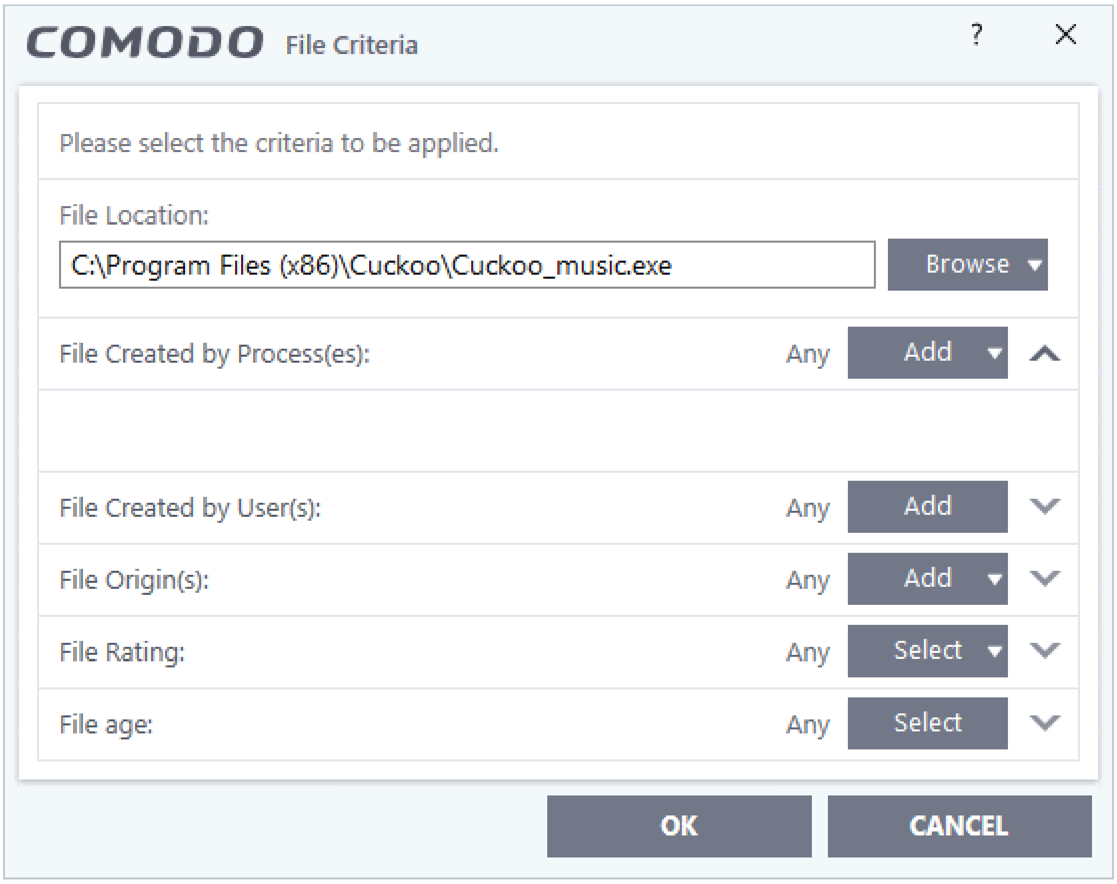
Name	Date modified	Type	Size
Convertors	11/16/2016 12:50 ...	File folder	
Cuckoo_music	7/9/2011 12:47 PM	Application	453 KB
Uninstal	11/11/2016 2:33 PM	Application	74 KB

File name: Cuckoo_music

Executable Files (*.exe, *.dll, *.o

- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'

The file will be added as target and will be run as per the action chosen in **Step 1**.



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es):	Any	Add
File Created by User(s):	Any	Add
File Origin(s):	Any	Add
File Rating:	Any	Select
File age:	Any	Select

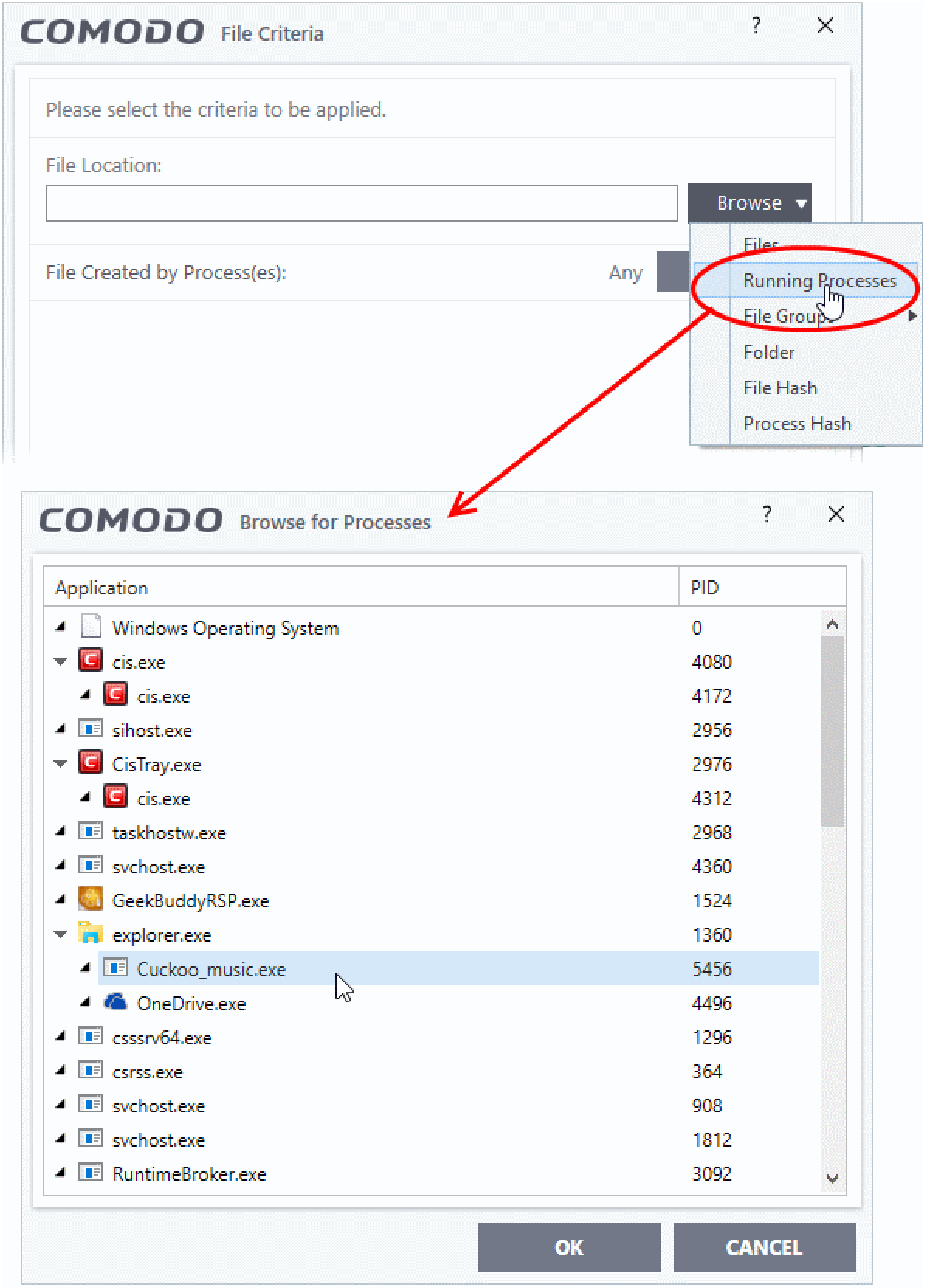
- Click 'OK', if you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a currently running application by choosing its process

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

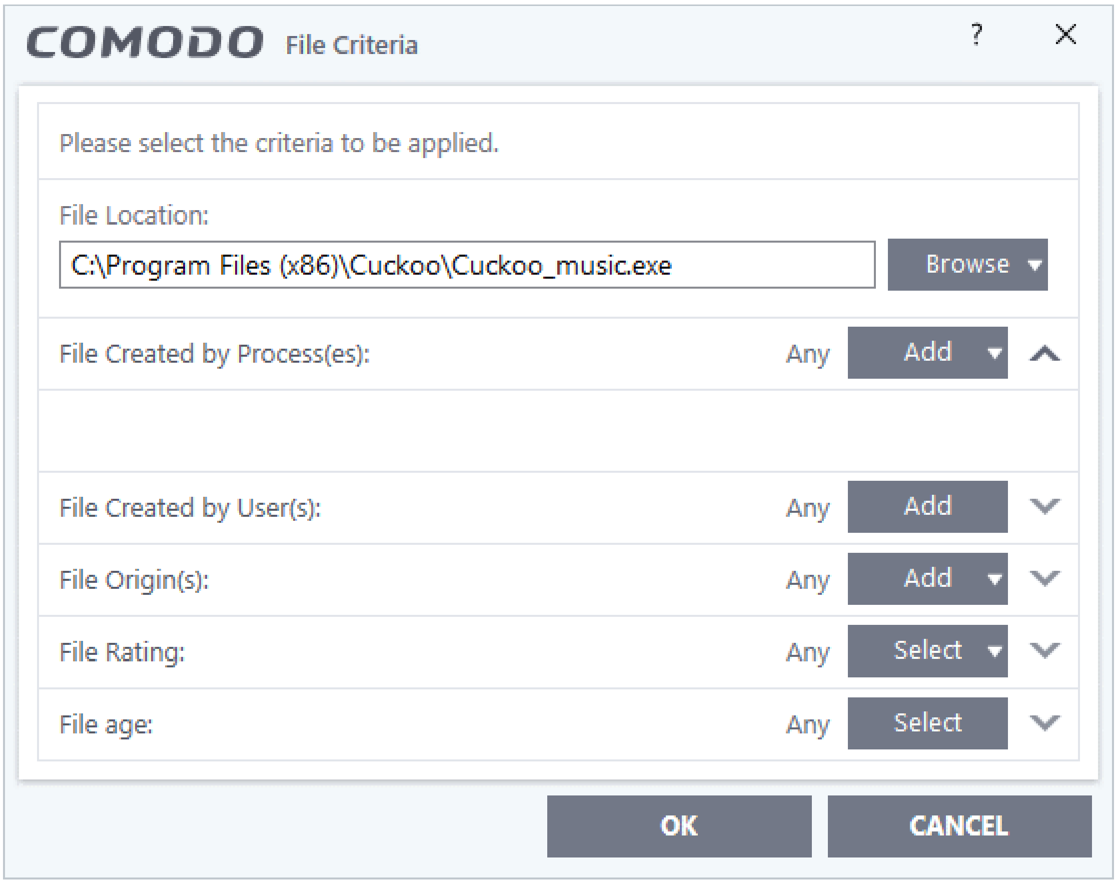


Application	PID
Windows Operating System	0
cis.exe	4080
cis.exe	4172
sihost.exe	2956
CisTray.exe	2976
cis.exe	4312
taskhostw.exe	2968
svchost.exe	4360
GeekBuddyRSP.exe	1524
explorer.exe	1360
Cuckoo_music.exe	5456
OneDrive.exe	4496
csssrv64.exe	1296
csrss.exe	364
svchost.exe	908
svchost.exe	1812
RuntimeBroker.exe	3092

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

- Select the process, whose target application is to be added to target and click 'OK' from the 'Browse for Process' dialog.

The file will be added as target and will be run as per the action chosen in **Step 1**.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

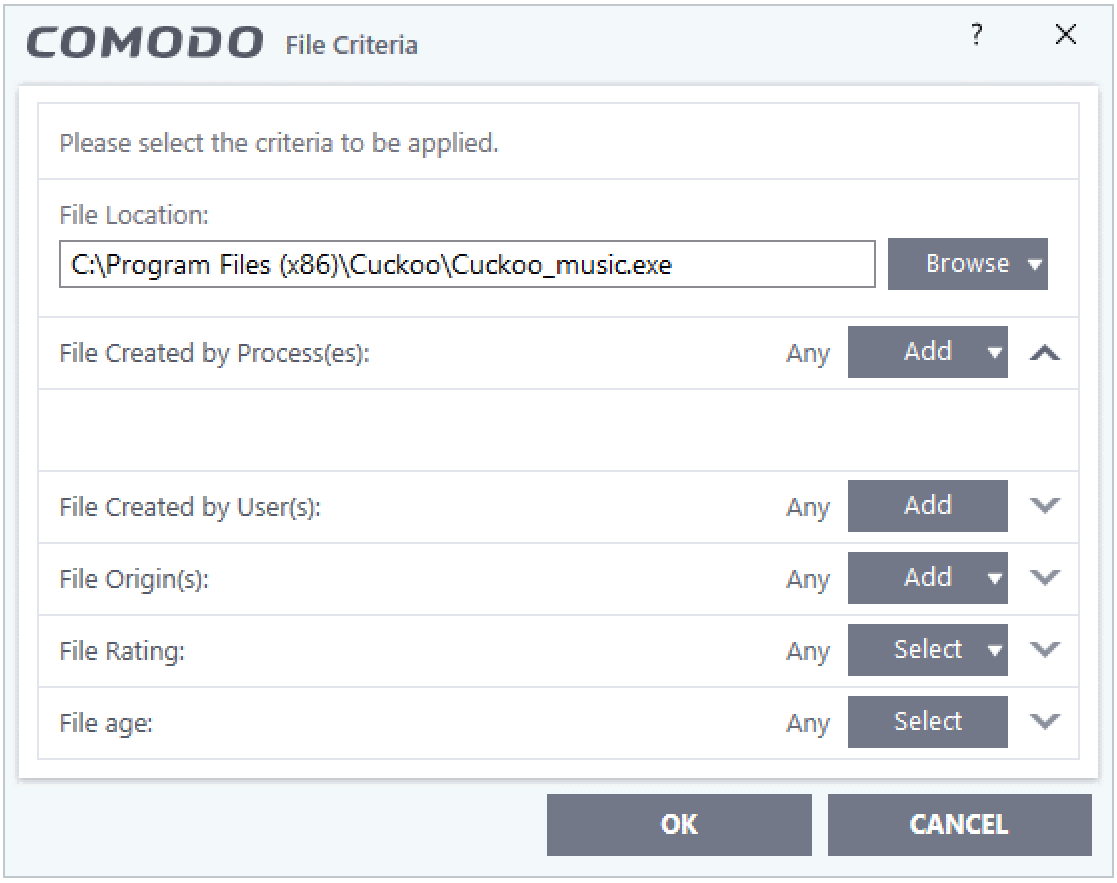
File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

File Rating: Any

File age: Any



COMODO File Criteria

Please select the criteria to be applied.

File Location:

C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

File Rating: Any

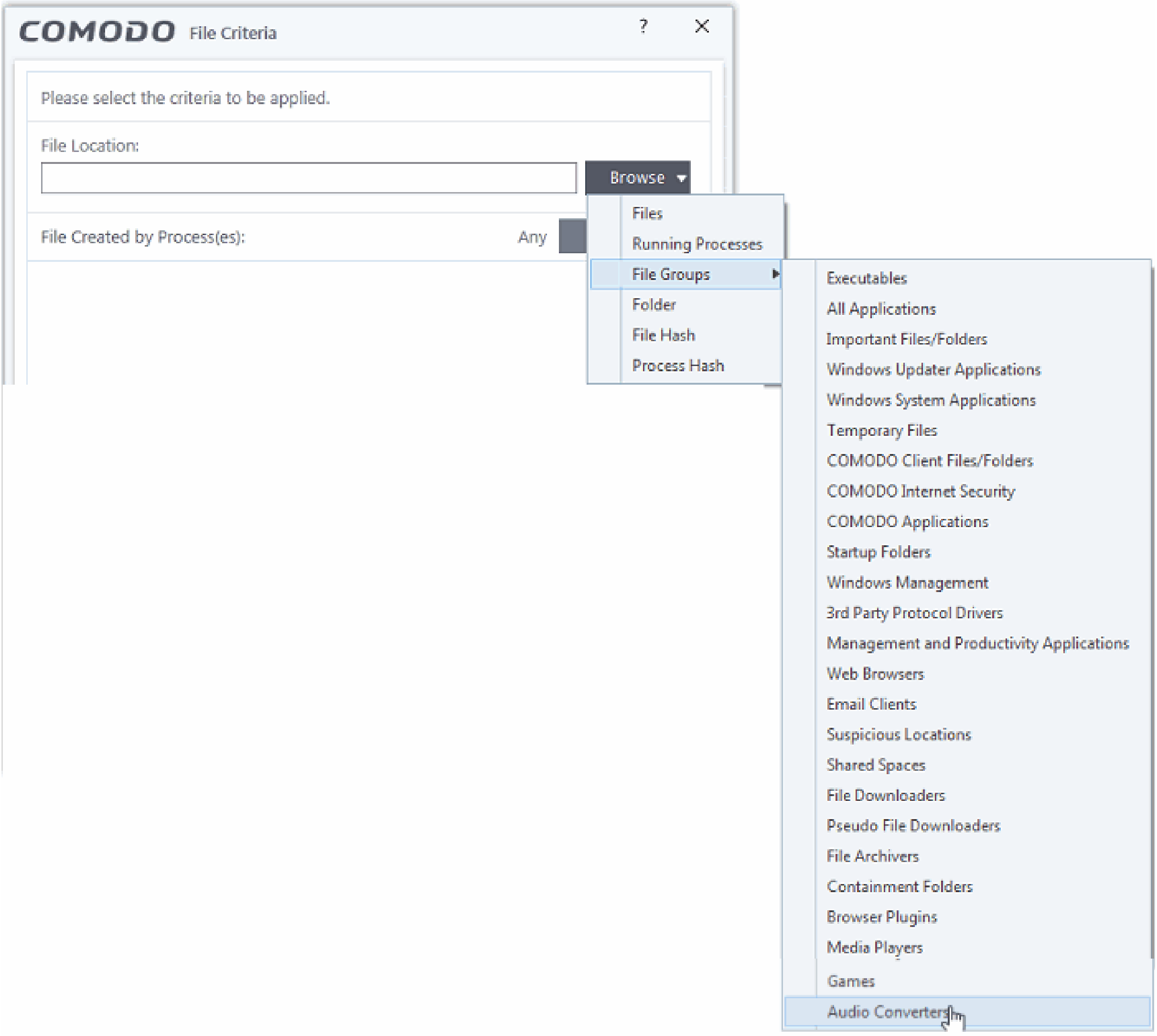
File age: Any

- Click 'OK', if you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options.

- The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.
- If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a File Group

- Choose 'File Groups' from the 'Browse' drop-down. Choosing File Groups allows you to include a category of files or folders configured as a 'File Group'. For more details on viewing and managing pre-defined and user-defined file groups refer to the section **File Groups**.



- Select the file group from the drop-down.

The file group will be added as target and will be run as per the action chosen in **Step 1**.

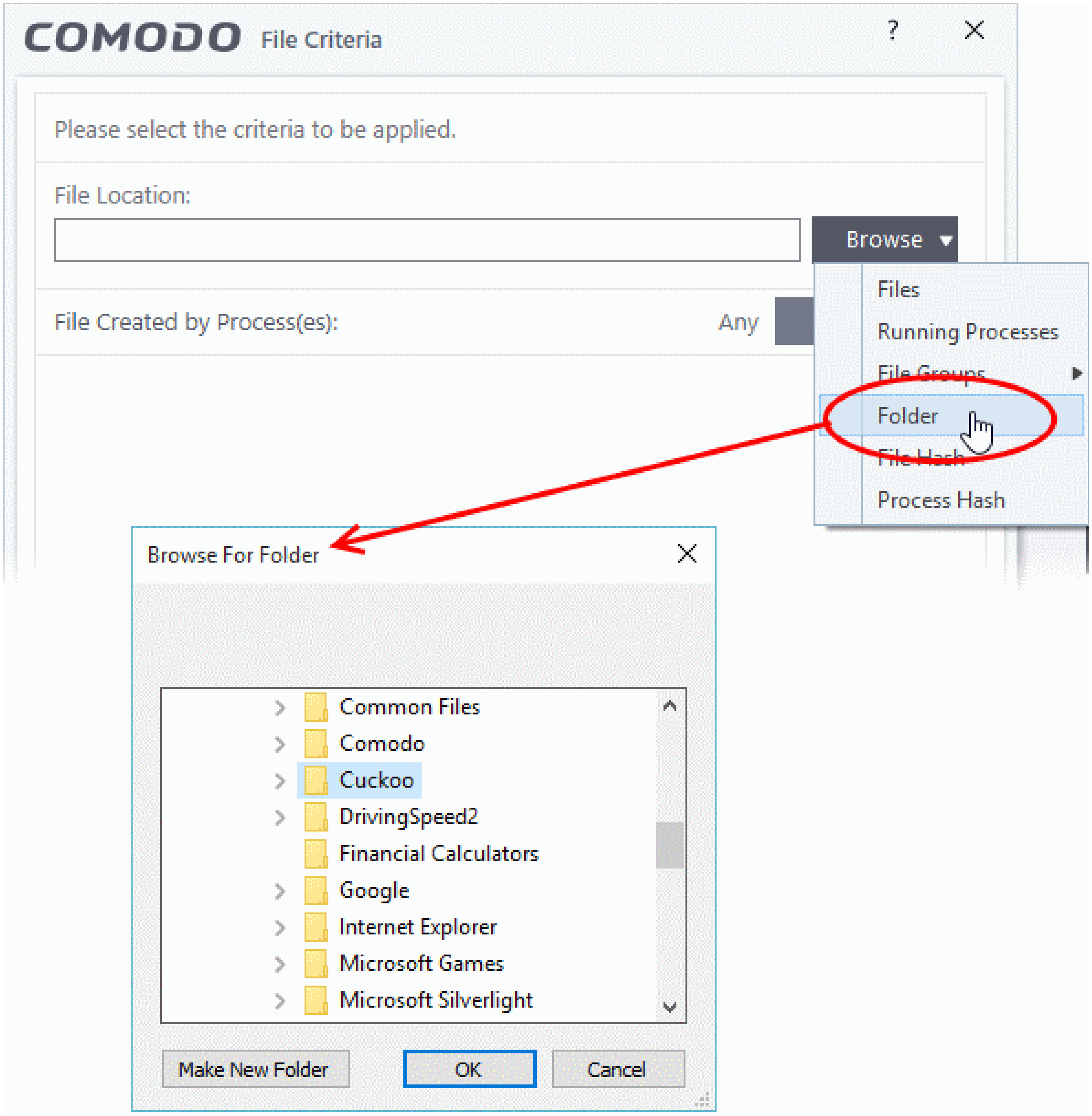
- Click 'OK', if you want to just add the file group for a particular action as selected in Step 1 without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.



The 'Browse for Folder' dialog will appear.

- Navigate to the drive partition or folder you want to add as target and click 'OK'

The drive partition/folder will be added as the target. All executable files in the folder will be run as per the action chosen in **Step 1**.

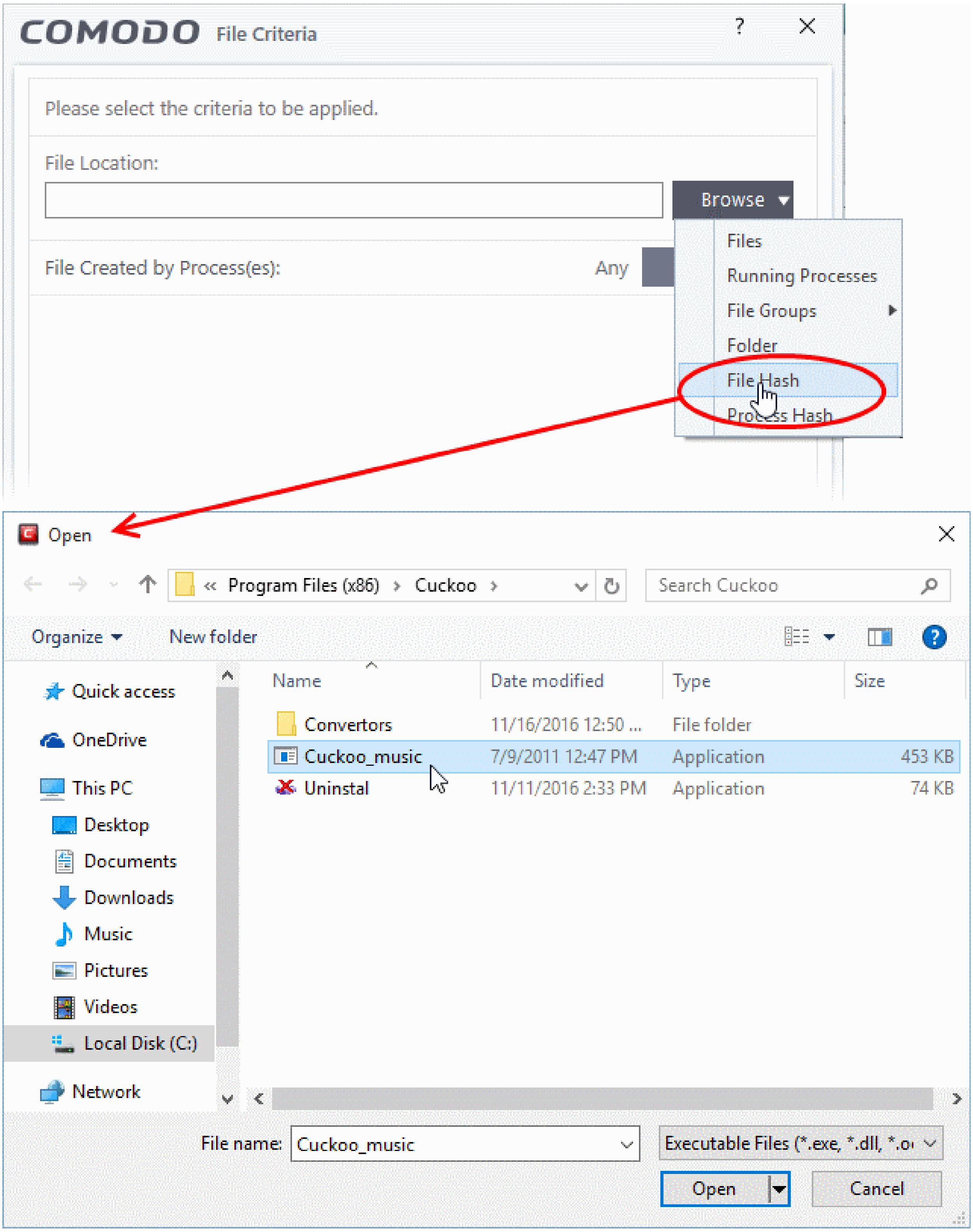
- Click 'OK', if you want to just add the applications for a particular action as selected in **Step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a file based on its hash value

- Choose 'File Hash' from the 'Browse' drop-down.



- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'

The file will be added as target and will be run as per the action chosen in **Step 1**.

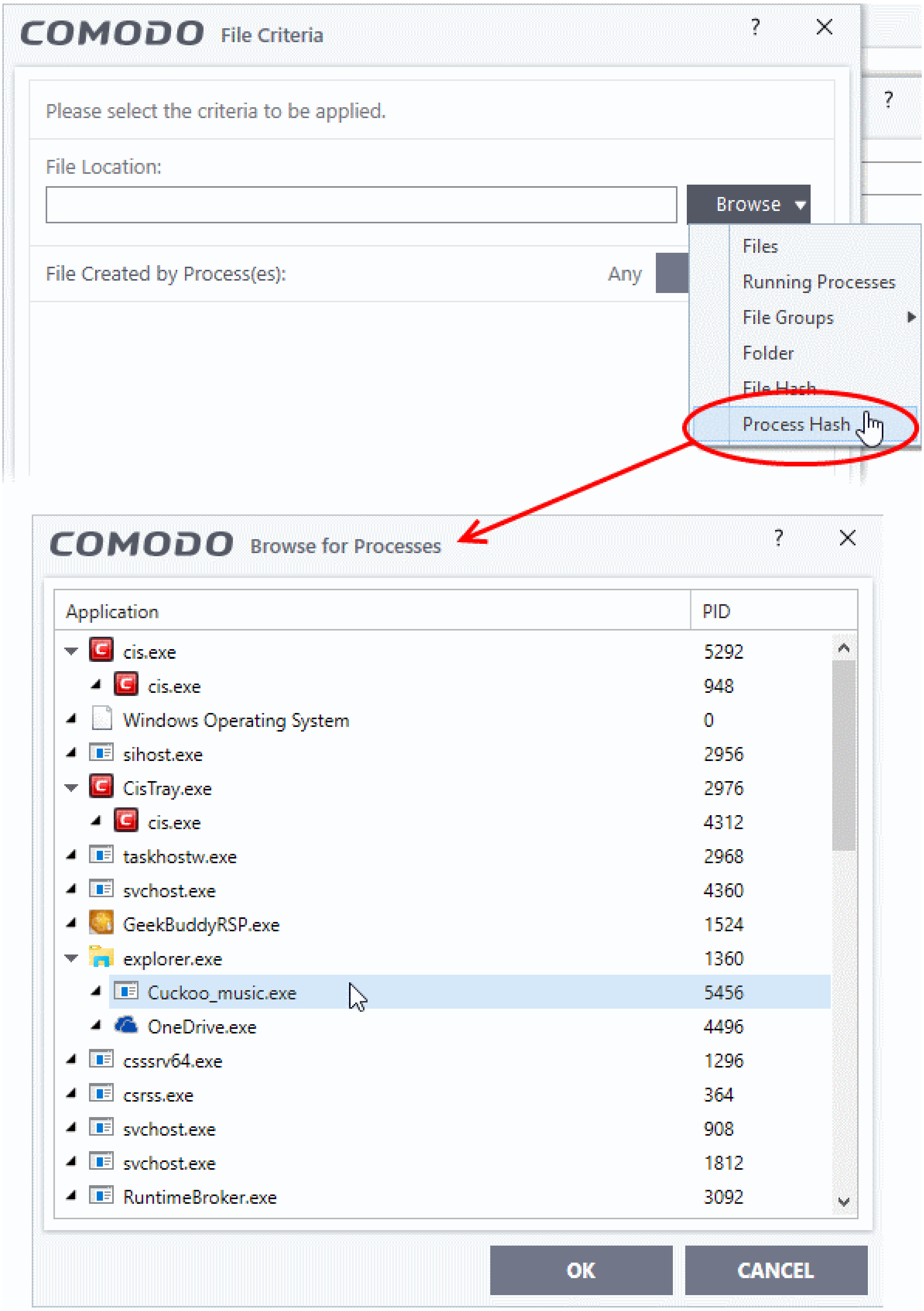
- Click 'OK', if you want to just add the file for a particular action as selected in **Step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

File Created by Process(es): Any

COMODO Browse for Processes

Application	PID
cis.exe	5292
cis.exe	948
Windows Operating System	0
sihost.exe	2956
CisTray.exe	2976
cis.exe	4312
taskhostw.exe	2968
svchost.exe	4360
GeekBuddyRSP.exe	1524
explorer.exe	1360
Cuckoo_music.exe	5456
OneDrive.exe	4496
csssrv64.exe	1296
csrss.exe	364
svchost.exe	908
svchost.exe	1812
RuntimeBroker.exe	3092

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

- Select the process, to add the hash value of its target application to target and click 'OK' from the 'Browse for Process' dialog.

The hash value of the parent executable file will be added as the target and the file will be run as per the action chosen in **Step 1**.

- Click 'OK', if you want to just add the application for a particular action as selected in **Step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria and file rating** and **Options** for the rule.

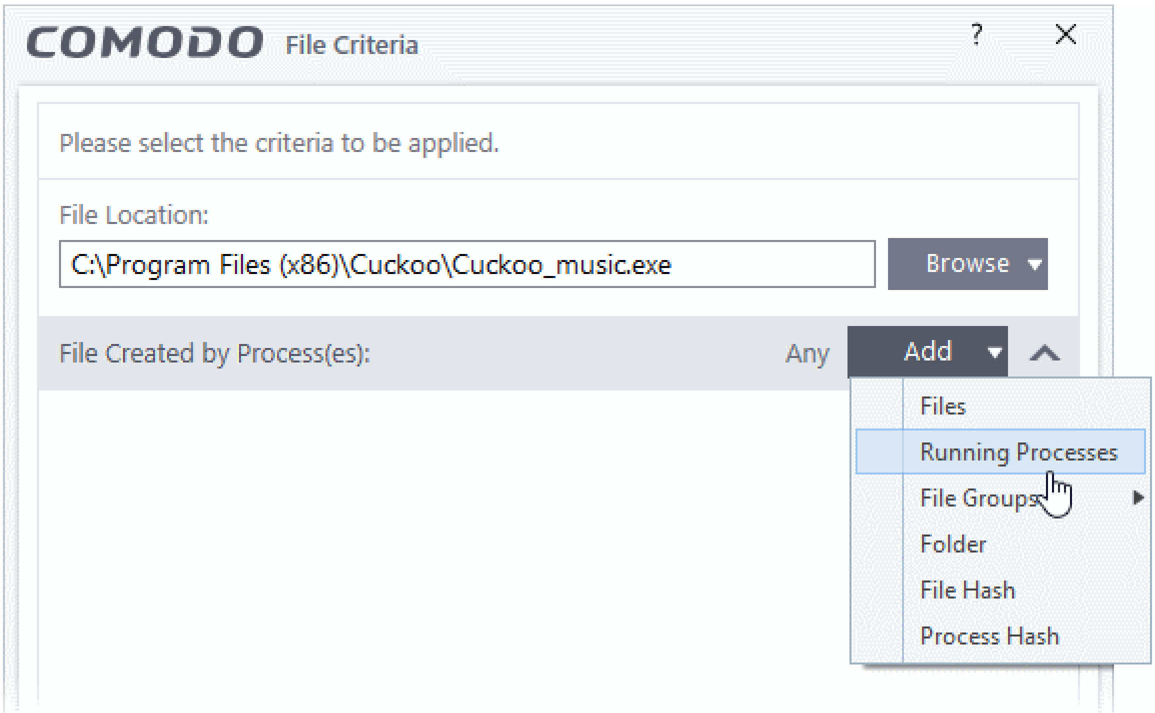
Configure the Filter Criteria and File Rating

You can set the filter criteria, so that the auto-containment action will be applied only to those items that meet the criteria, from the set of items contained in the target. The available filter criteria are:

- **Process(es) that created the file**
- **User(s) that created the file**
- **The origin from which the file was downloaded**
- **The file rating**
- **The age of the file**

To choose the source process(es) to auto-contained the files created by them

- Click the 'Add' button in the 'File Created by Process(es)' stripe.



Please select the criteria to be applied.

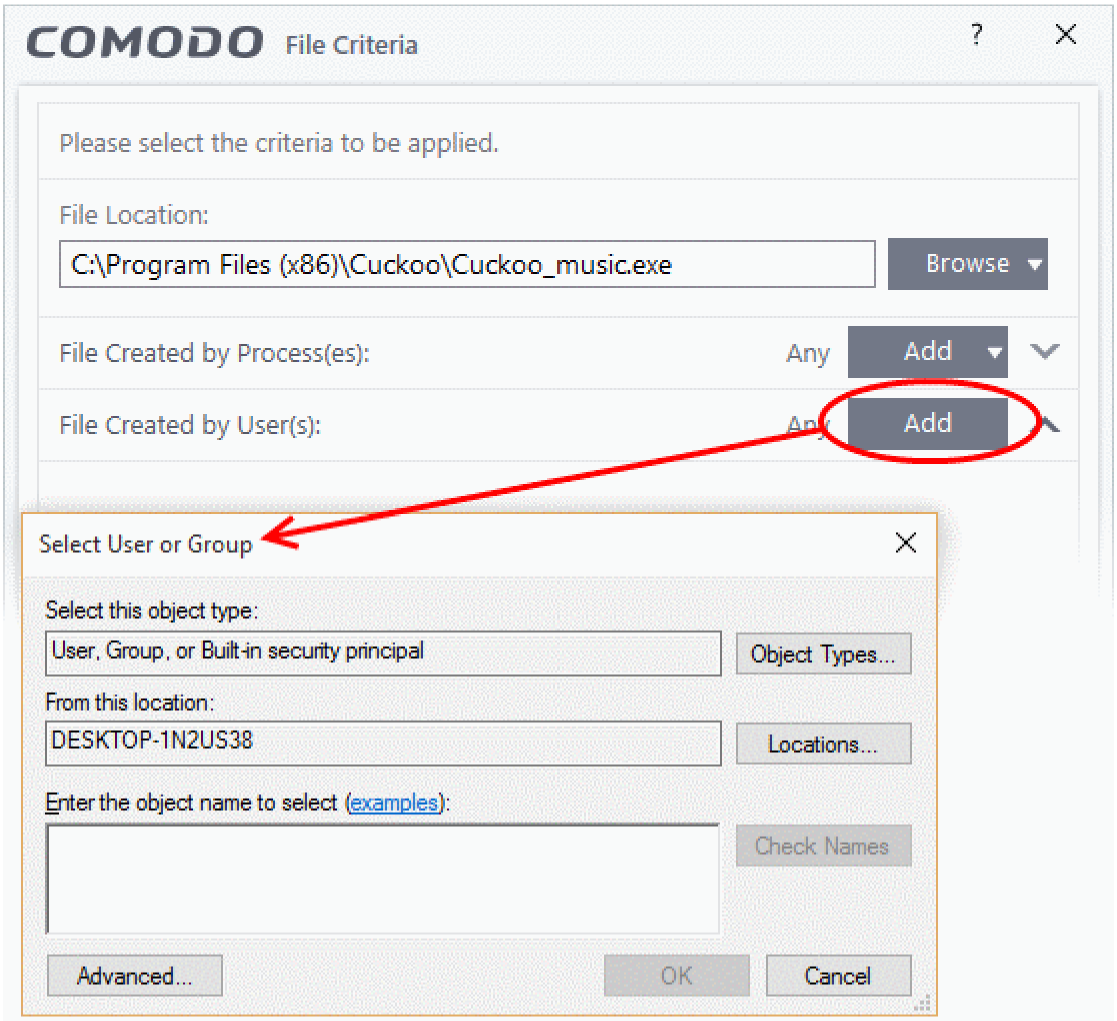
File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe Browse

File Created by Process(es): Any

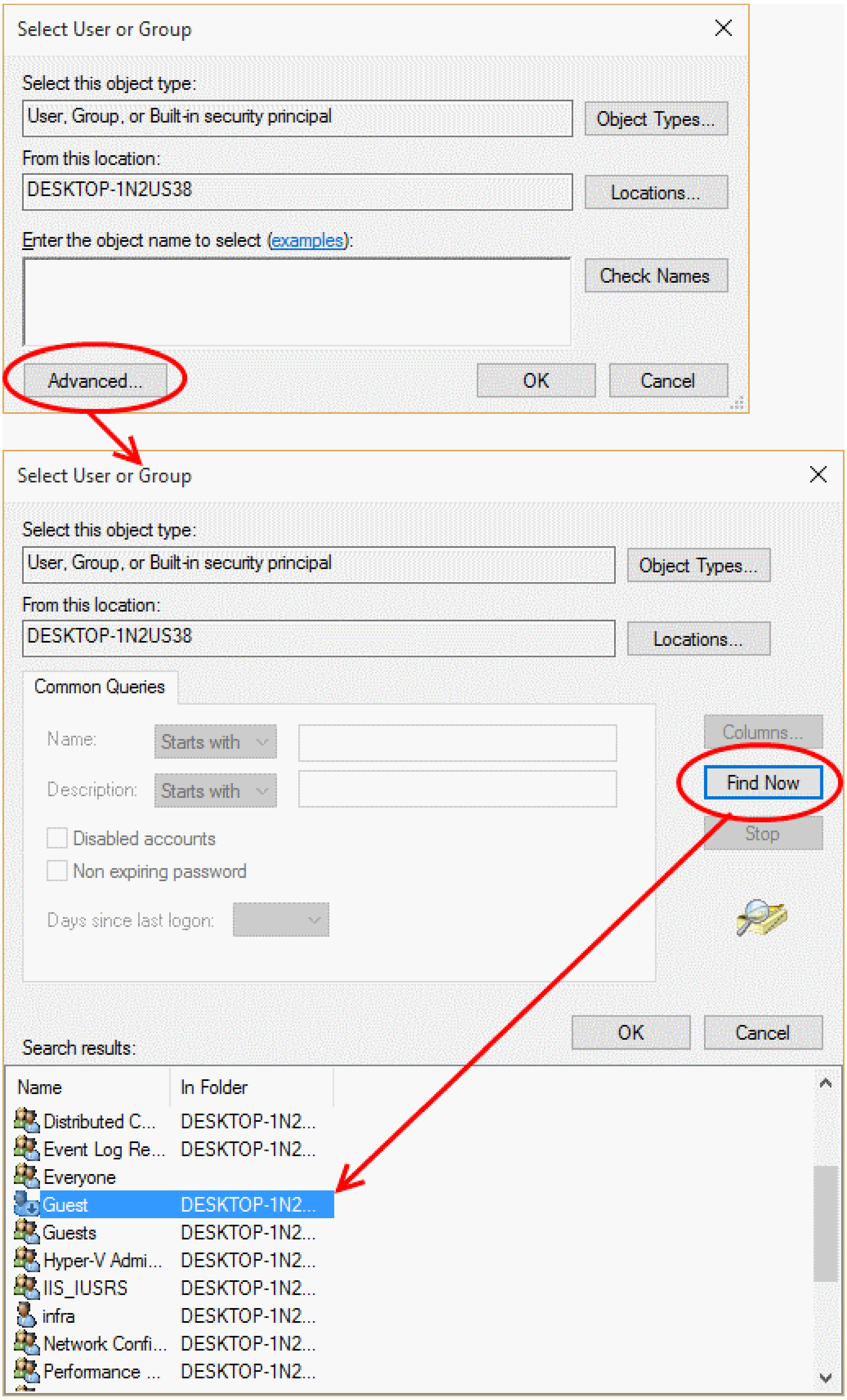
The options available are same as those available under the 'Browse' button beside 'Target', as explained **above**. Refer to previous section for each of options for more details. You can add more than one process for auto-contained all the files created by them and contained in the chosen target group/folder.

To choose the user(s) to auto-contained files created by them

- Click the 'Add' button in the 'File Created by User(s)' stripe.



- The 'Select User or Group' dialog will appear.
  - Enter the names of the users to be added to the rule in the 'Enter the object name to select' text box. Use the format <domain name>\<user/group name> or <user/group name>@<domain name>.
  - Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



Select this object type: User, Group, or Built-in security principal

From this location: DESKTOP-1N2US38

Enter the object name to select (examples):

Select this object type: User, Group, or Built-in security principal

From this location: DESKTOP-1N2US38

Name: Starts with

Description: Starts with

□ Disabled accounts

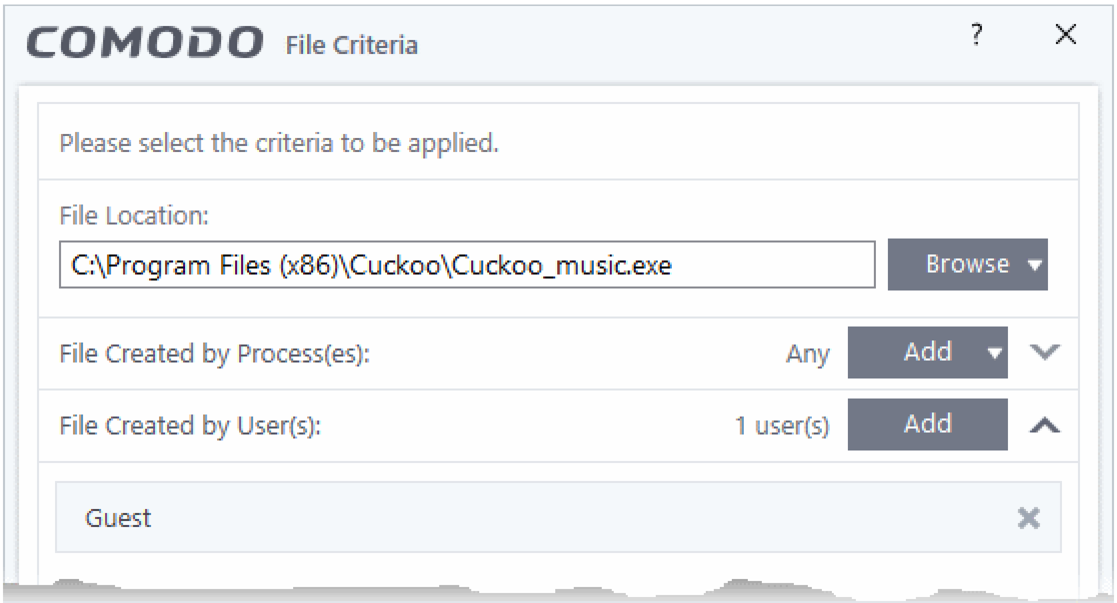
□ Non expiring password

Days since last logon:

Search results:

Name	In Folder
Distributed C...	DESKTOP-1N2...
Event Log Re...	DESKTOP-1N2...
Everyone	
Guest	DESKTOP-1N2...
Guests	DESKTOP-1N2...
Hyper-V Admi...	DESKTOP-1N2...
IIS_IUSRS	DESKTOP-1N2...
infra	DESKTOP-1N2...
Network Confi...	DESKTOP-1N2...
Performance ...	DESKTOP-1N2...

The user will be added to the list.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

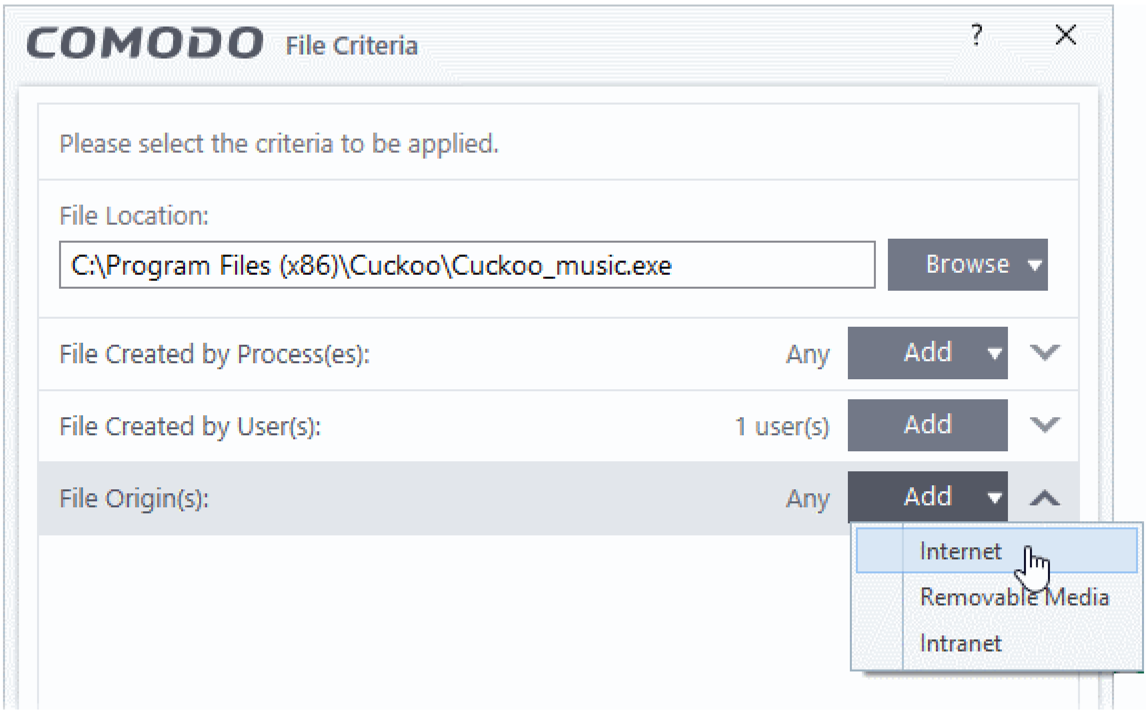
File Created by User(s): 1 user(s)

Guest

- Repeat the process for adding more users.
- To remove the user added by mistake or no longer needed in the list, click the 'X' icon at the right end of the user name.

To select the sources(s) from which the file was downloaded/copied to the computer

- Click the 'Add' button in the 'File Origin(s)' stripe.
- Choose the source from the options:



COMODO File Criteria

Please select the criteria to be applied.

File Location:

C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

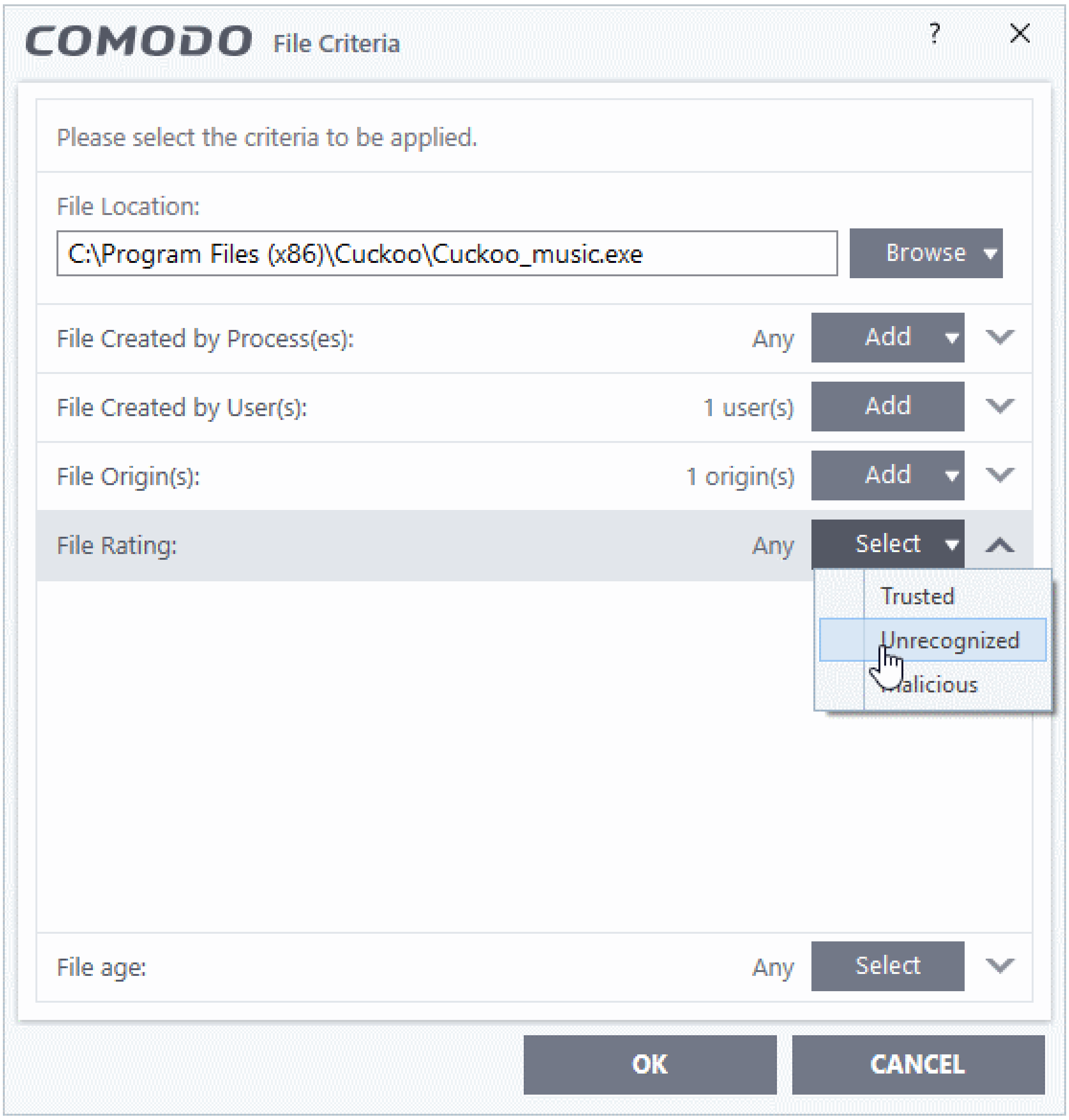
File Created by User(s): 1 user(s)

File Origin(s): Any

  - Internet - The rule will only apply to files that were downloaded from the internet.
  - Removable Media - The rule will apply only to items copied to the computer from removable storage devices like a USB drive, CD/DVD or portable hard disk drive
  - Intranet - The rule will only apply to files that were downloaded from the local intranet.
- Repeat the process to add more sources

To select the file rating as filter criteria

- Click the 'Select' button in the 'File Rating' stripe



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

File Created by User(s): 1 user(s)

File Origin(s): 1 origin(s)

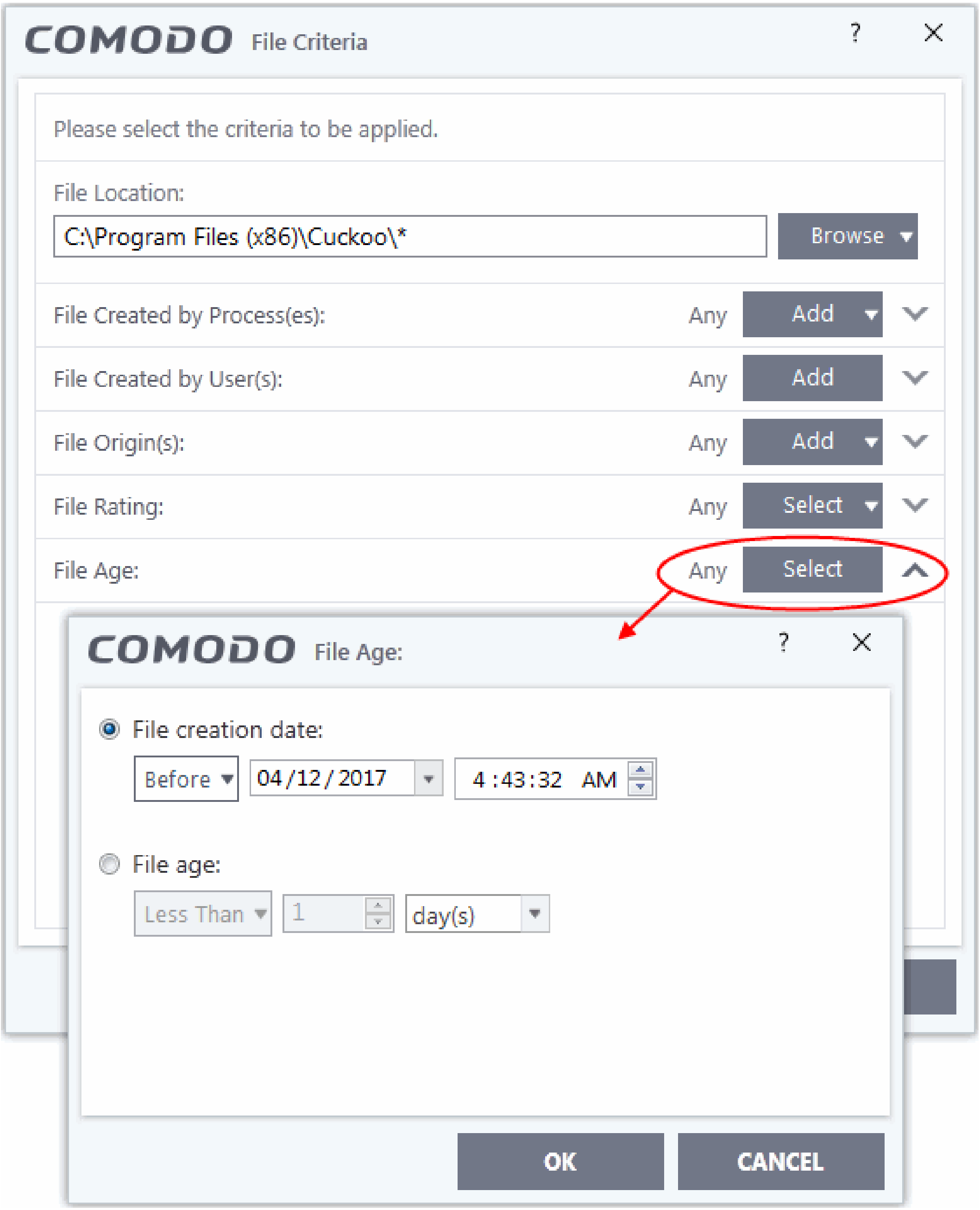
File Rating: Any

File age: Any

- Choose the source from the options:
  - **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by CIS. See **File Rating Settings** for more information.
  - **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. See **File List** for more information.
  - **Malware** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. See **Unknown Files - The Scanning Process** for more information.

To set the file age as filter criteria

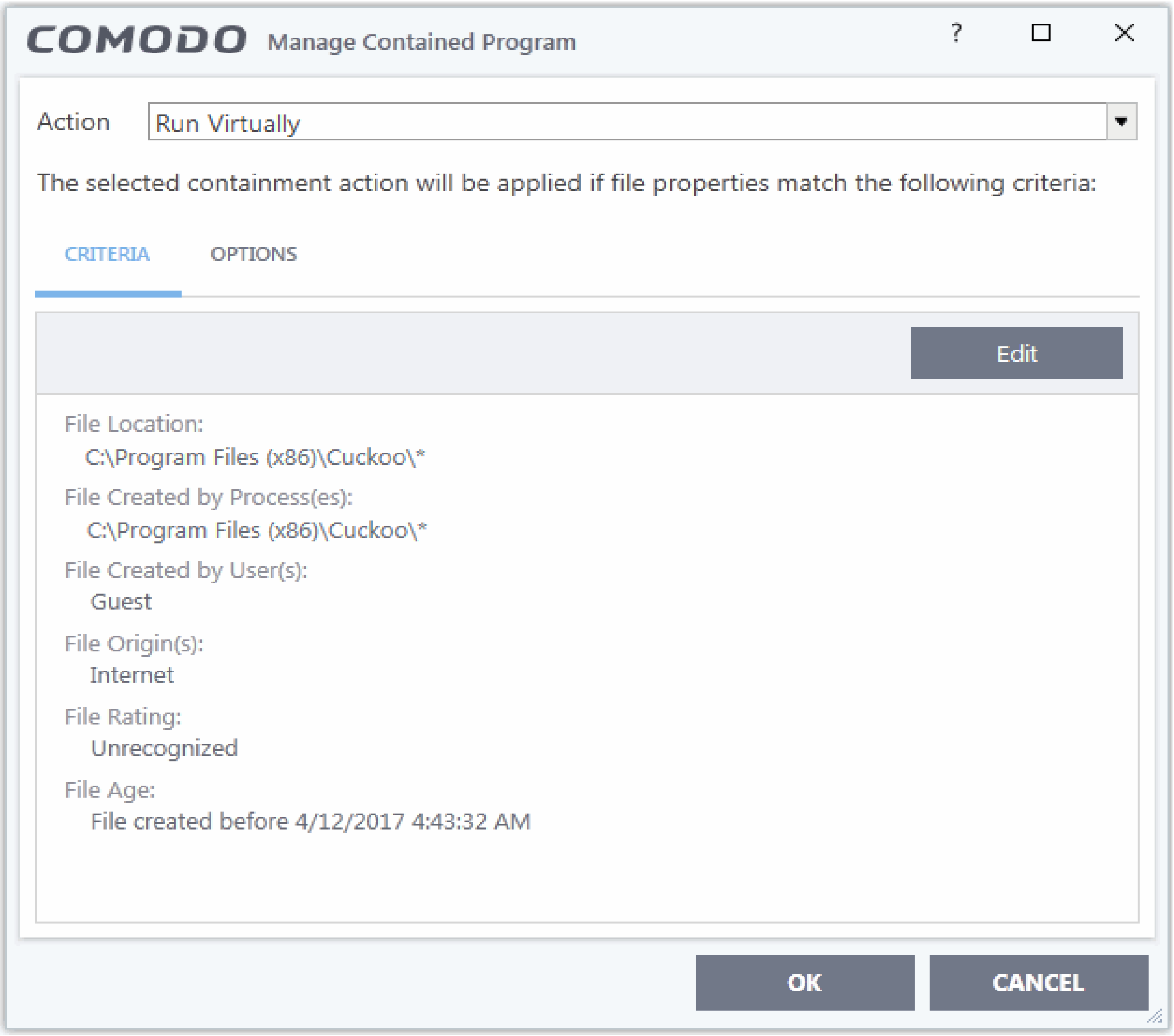
- Click the 'Select' button in the 'File age' stripe.



The 'File Age' dialog will appear. You can set the file age in two ways:

- **File Creation Date -** To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- **File age -** To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - **Less Than -** CIS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)
  - **More Than -** CIS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)

- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.



Action: Run Virtually

The selected containment action will be applied if file properties match the following criteria:

File Location:
C:\Program Files (x86)\Cuckoo\*

File Created by Process(es):
C:\Program Files (x86)\Cuckoo\*

File Created by User(s):
Guest

File Origin(s):
Internet

File Rating:
Unrecognized

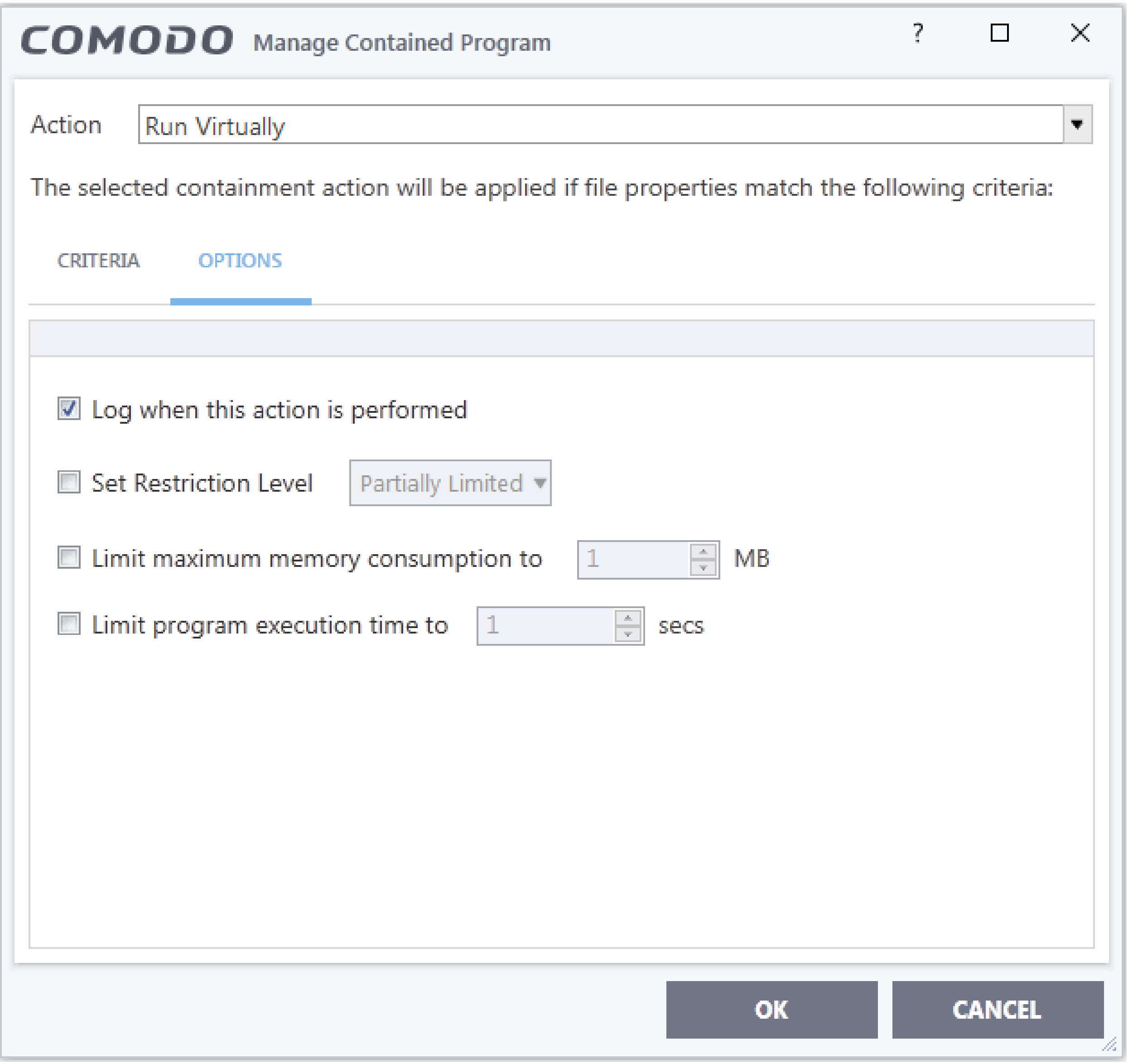
File Age:
File created before 4/12/2017 4:43:32 AM

Step 3 - Select the Options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

To select the options

- Click the 'Options' tab.



Action: Run Virtually

The selected containment action will be applied if file properties match the following criteria:

☑ Log when this action is performed

□ Set Restriction Level: Partially Limited

□ Limit maximum memory consumption to 1 MB

□ Limit program execution time to 1 secs

The options will be displayed, depending on the 'Action' chosen in **Step 1**.

The options available for '**Ignore**' action are:

- **Log when this action is performed -** Whenever this rule is applied for the action, it will be added to CIS Containment logs.
- **Don't apply the selected action to child processes -** Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CIS treats all the child processes as individual processes and forces them to run as per the file rating and the Containment rules.
  - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
  - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Containment rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the 'Ignore' action only.

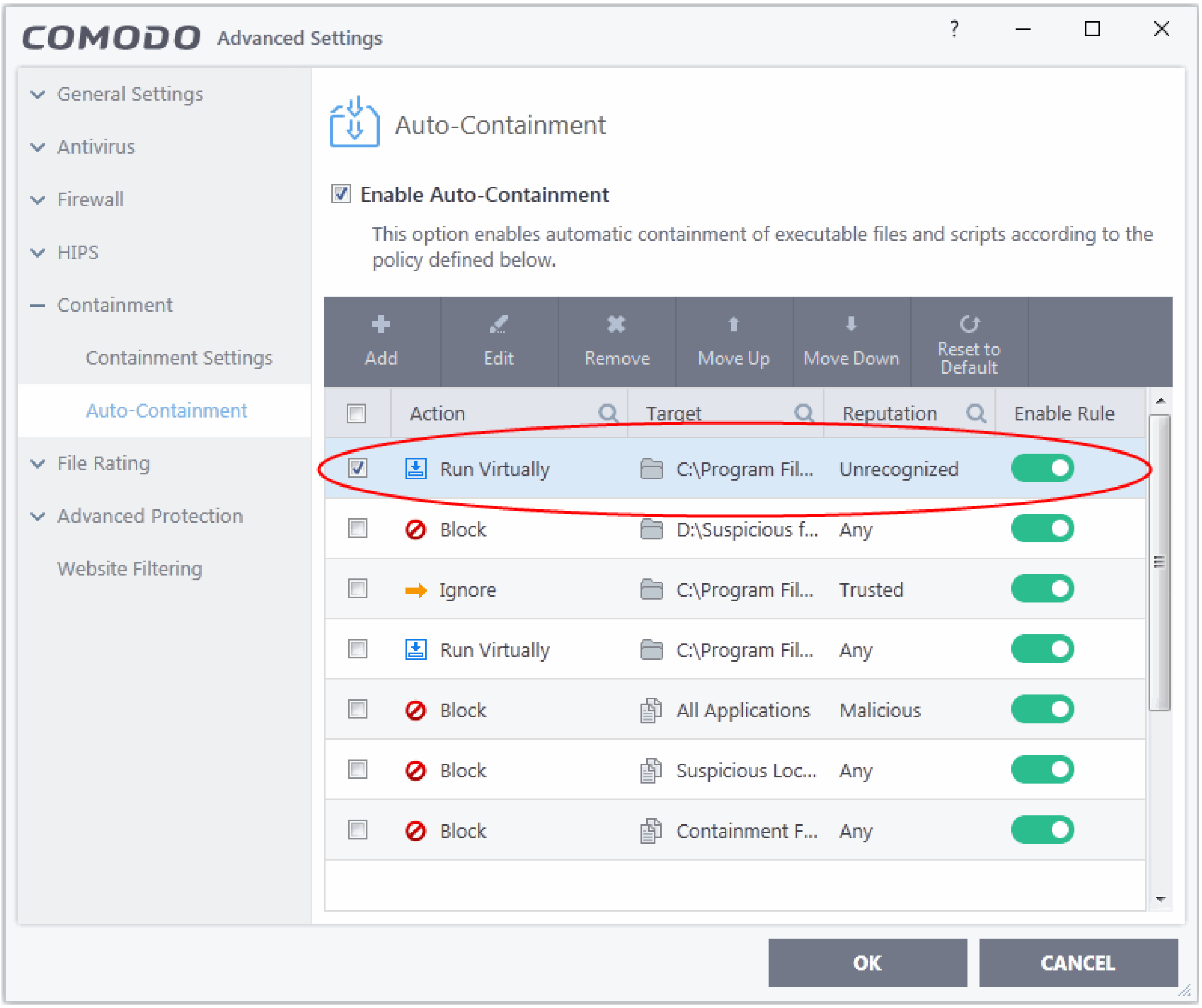
The options available for '**Run Restricted**' and '**Run Virtually**' actions are:

- **Log when this action is performed -** Whenever this rule is applied for the action, it will be added to CIS Containment logs

- **Set Restriction Level -** When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked.
- You can select the 'Restriction Level' from the following options:
    - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.**(*Default*)**
    - **Limited -** Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
    - **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
    - **Untrusted -** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
- **Limit maximum memory consumption to -** Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to -** Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

The options available for '**Blocked**' action are:

- **Log when this action is performed -** Whenever this rule is applied for the action, it will be added to CIS Containment logs.
- Quarantine program - If selected, the applications satisfying the rule will be automatically quarantined. See **Manage Quarantined Items** for more information.
- Choose the options and click 'OK' to save them for the rule. The rule will be added and displayed in the list.



Auto-Containment

☑ Enable Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
☑	Run Virtually	C:\Program Fil...	Unrecognized	On
□	Block	D:\Suspicious f...	Any	On
□	Ignore	C:\Program Fil...	Trusted	On
□	Run Virtually	C:\Program Fil...	Any	On
□	Block	All Applications	Malicious	On
□	Block	Suspicious Loc...	Any	On
□	Block	Containment F...	Any	On

You can move the rule up or down depending on the priority to be given to it, with respect to the other rules.

Editing an Auto-Containment Rule

- To edit an auto-containment rule, select it from the list in the Auto-Containment panel and click 'Edit' from the top.

The 'Manage Contained Program' diaslog will be displayed. The procedure is similar to **Adding an Auto-Containment Rule**.

- Click 'OK' to save the changes to the rule.

Important Note: Please make sure the auto-containment rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail. You can restore the rules to default rules at any time by clicking the 'Reset to Default' button at the top.

6.6. File Rating Configuration

- The CIS 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, CIS will check the file against our master whitelist and blacklists and will award it trusted status if:
  - The application/file has a 'Trusted' status in the CIS **File List**

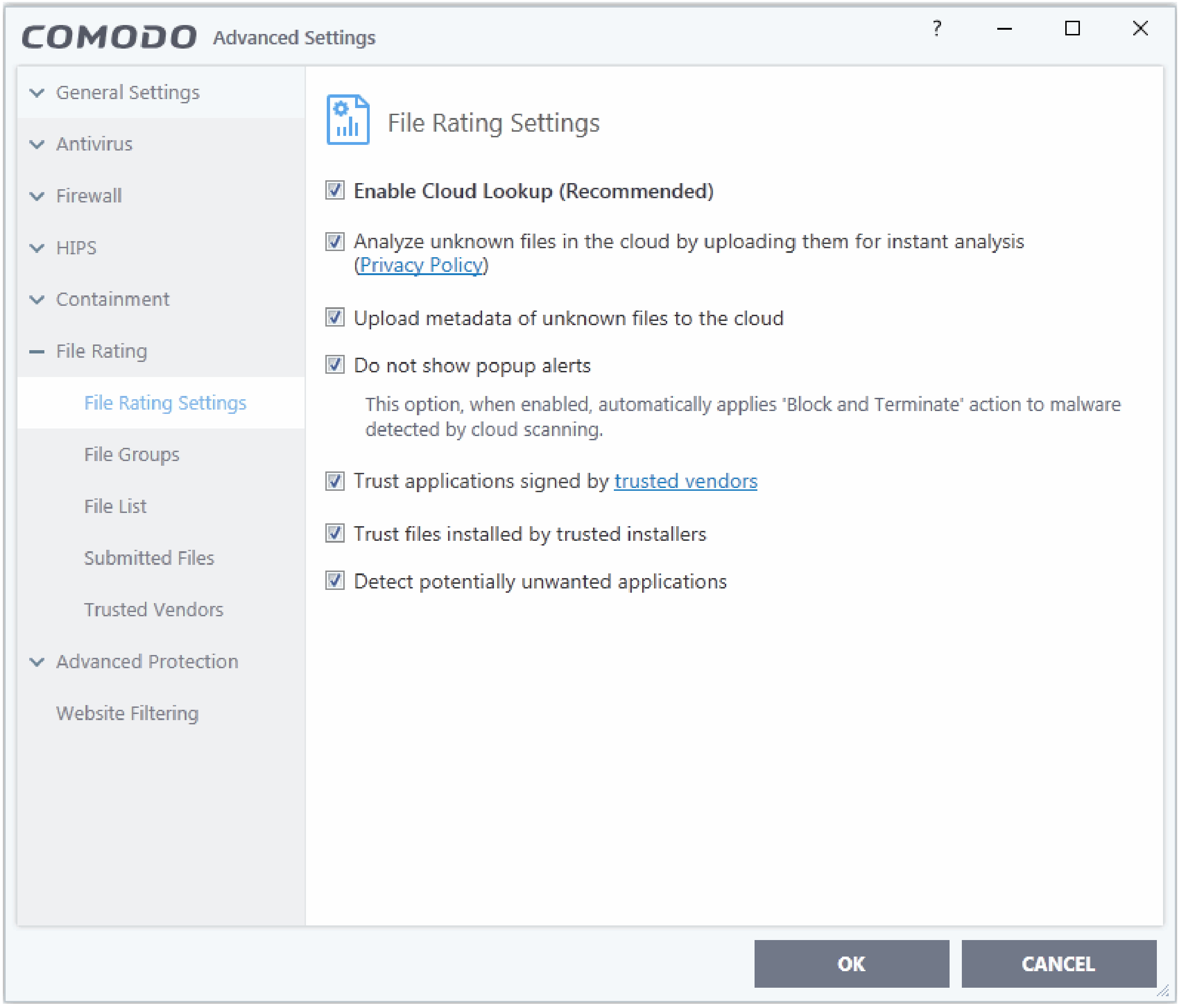
- The application is from a vendor included in the **Trusted Software Vendors**
- The application is included in the extensive and constantly updated Comodo safelist.

- Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource consumption.
- On the other hand, files which are identified as definitely harmful will be given a status of 'Malicious' and quarantined or deleted automatically.
- Files which could not be recognized by the rating system are awarded 'Unrecognized' status.
- You can review unrecognized files in the **File List** interface and manually trust/block/delete them.
- You can also submit them to Comodo for further analysis or to run an on-demand file-lookup.

The 'File Rating' area allows you to view and manage the list of 'Trusted Files', Malicious Files, and 'Unrecognized Files' and also allows you to:

- Manually add files and executable to 'Trusted Files' list.
- Submit 'Unrecognized Files' for look-up and view the list of files you have submitted previously.
- View and manage the 'Trusted Software Vendor' list.

To open the 'File Rating' section, click 'Settings' from the top left of the CIS home screen then select 'File Rating' from 'Advanced Settings'.



File Rating Settings

☑ Enable Cloud Lookup (Recommended)

☑ Analyze unknown files in the cloud by uploading them for instant analysis (Privacy Policy)

☑ Upload metadata of unknown files to the cloud

☑ Do not show popup alerts

This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

☑ Detect potentially unwanted applications

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.

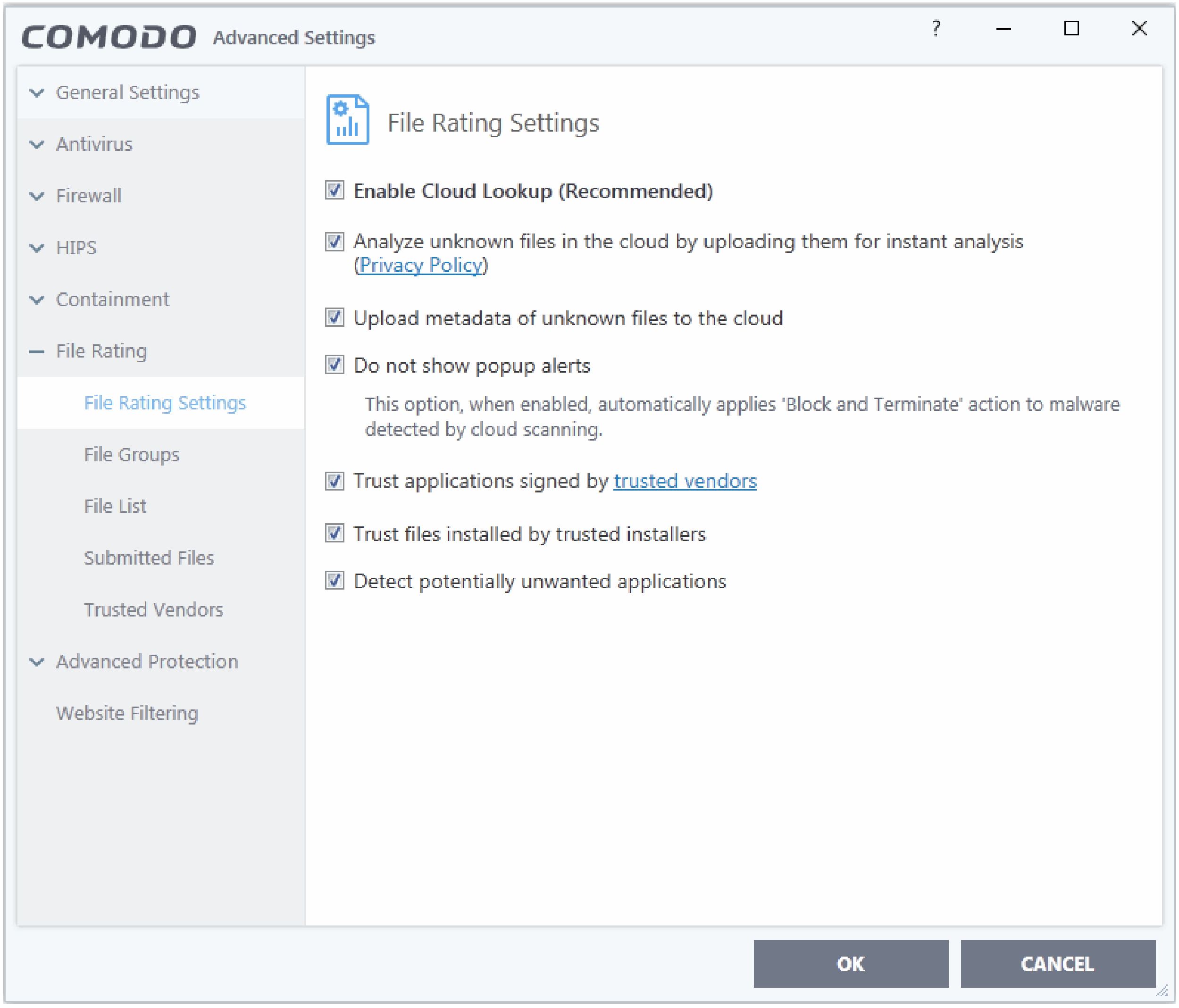
- **File Groups** - Create predefined groups of one or more file types.
- **File List** - View, manage and investigate executable files on your computer and their current trust rating.
- **Submitted Files** - View any files already submitted to Comodo for analysis.
- **Trusted Vendors** - View the list of trusted software vendors and manually add vendors.

6.6.1. File Rating Settings

The 'File Rating Settings' panel allows you to configure the behavior of the file rating feature. File ratings allow Comodo Internet Security to classify files as malicious, safe or unknown.

To open the 'File Rating Settings' interface

- Click 'Settings' from the top left of the CIS home screen
- Click 'File Rating' > 'File Rating Settings':



File Rating Settings

☑ Enable Cloud Lookup (Recommended)

☑ Analyze unknown files in the cloud by uploading them for instant analysis (Privacy Policy)

☑ Upload metadata of unknown files to the cloud

☑ Do not show popup alerts

This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

☑ Detect potentially unwanted applications

- **Enable Cloud Lookup** - If enabled, CIS will check a file's trust rating on our cloud severs as part of the scan process. ***(Default and recommended = Enabled)***
- **Analyze unknown files in the cloud by uploading them for instant analysis** - Instructs CIS to upload to Comodo for further analysis those files whose trustworthiness could not be determined by the cloud lookup. Technicians at Comodo will analyze the file and add it to the global whitelist or blacklist as appropriate. ***(Default = Enabled)***
- **Upload metadata of unknown files to the cloud** - If enabled, information about unknown files will be uploaded to Comodo servers. Metadata is basic file information such as file source, author, date of creation

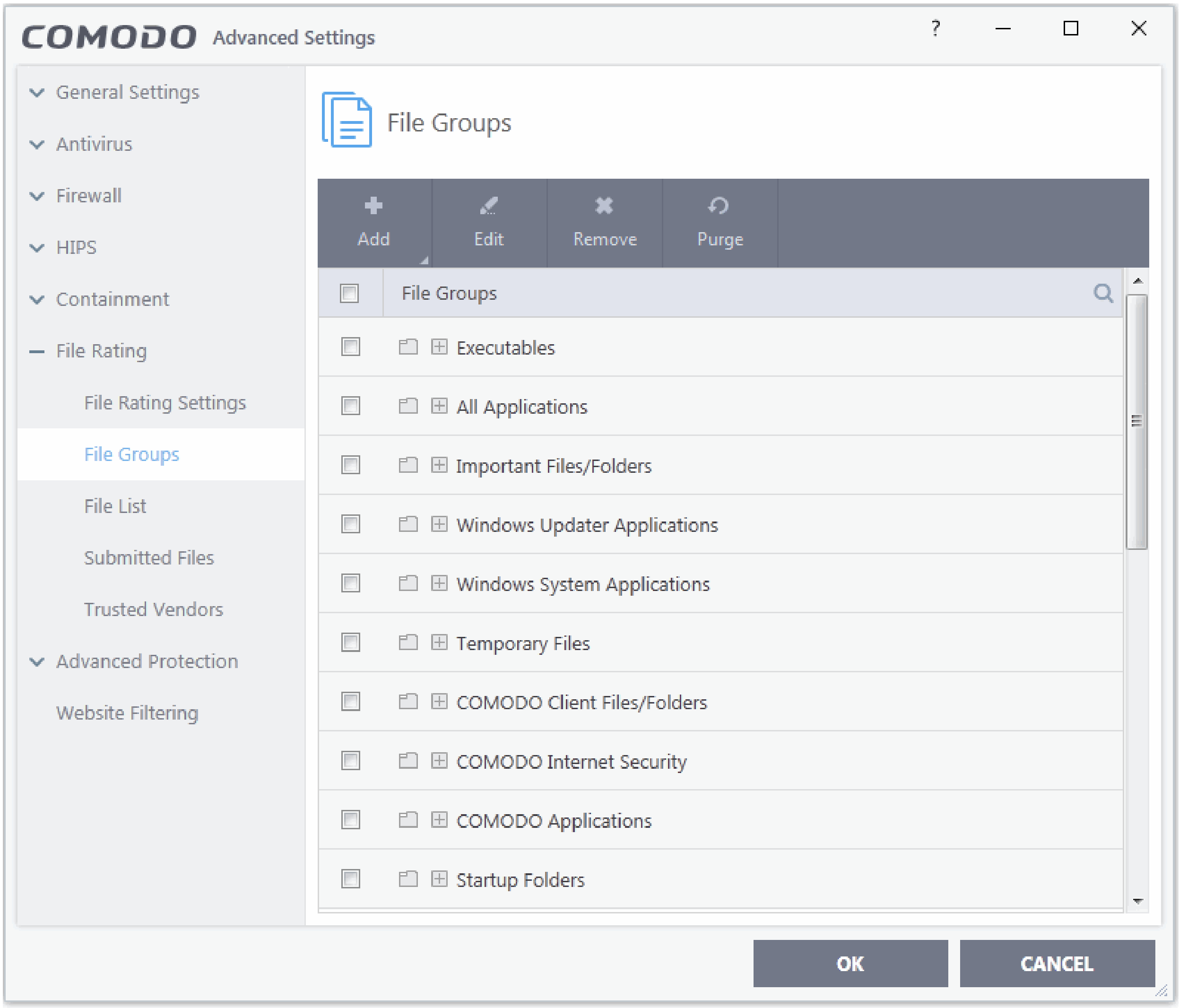
(Default =Enabled)

- **Do not show popup alerts -** This option allows you to configure whether or not to show containment alerts when malware is detected by cloud scanning. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If the option is disabled, a containment alert will be displayed and the file quarantined. ***(Default = Enabled)***
- **Trust applications signed by trusted vendors -** If enabled, CIS will award trusted status to executables and files that are digitally signed by vendors in the Trusted Vendors list. Click the words 'trusted vendors' to open the **Trusted Vendors** panel. (***Default = Enabled***)
- **Trust files installed by trusted installers -** If enabled, CIS will trust executable and files whose parent applications are listed under the 'Installer or Updater' rule in **HIPS Rules**. ***(Default = Enabled)***
- **Detect potentially unwanted applications -** When this check box is selected, antivirus scans will flag applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet ***(Default = Enabled).***

6.6.2. File Groups

- As the name suggests, a file group is a collection of one or more file types.
- Once created, file groups can be referenced from other areas of CIS, making it easy to add an entire class of files to exclusions, HIPS rules, containment rules and more.
- CIS ships with a set of predefined file groups. You can also create your own file groups and edit existing groups as required.

To open the 'File Groups' interface, click 'Settings' from the top left of the CIS home screen then select 'File Rating' > 'File Groups' from 'Advanced Settings'.



□	File Groups
□	Executables
□	All Applications
□	Important Files/Folders
□	Windows Updater Applications
□	Windows System Applications
□	Temporary Files
□	COMODO Client Files/Folders
□	COMODO Internet Security
□	COMODO Applications
□	Startup Folders

You can use the search option to find a specific name in the list by clicking the search icon at the far right of the column header and entering the name in full or part.

The buttons at the top provide the following options:

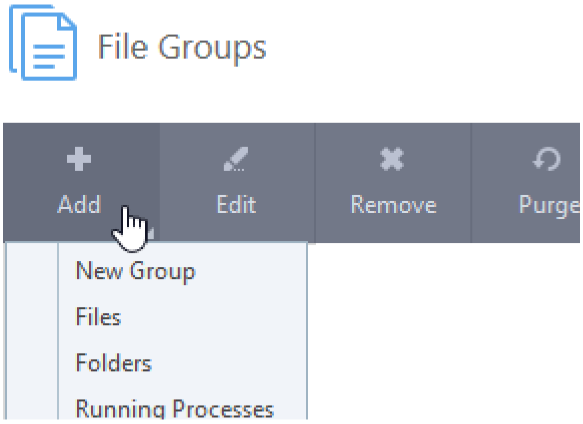
- **Add -** Allows you to add new groups, files, folders or running processes to a file group.
- **Edit -** Allows you to rename file groups and edit the file path of items under a file group.
- **Remove -** Allows you to delete a File Group or item(s) under a file group.
- **Purge -** Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

This interface allows you to:

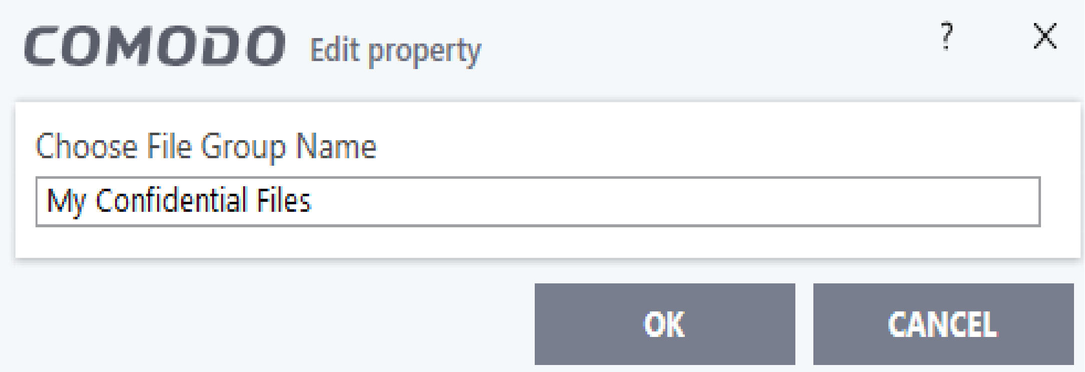
- Create a new File Group
- Edit the names of an Existing File Group
- Add a file to an existing file group
- Remove existing file group(s) or individual file(s) from existing group

Adding a File Group

- To add a new 'File Group', click the 'Add' button from 'File Groups Pane'.



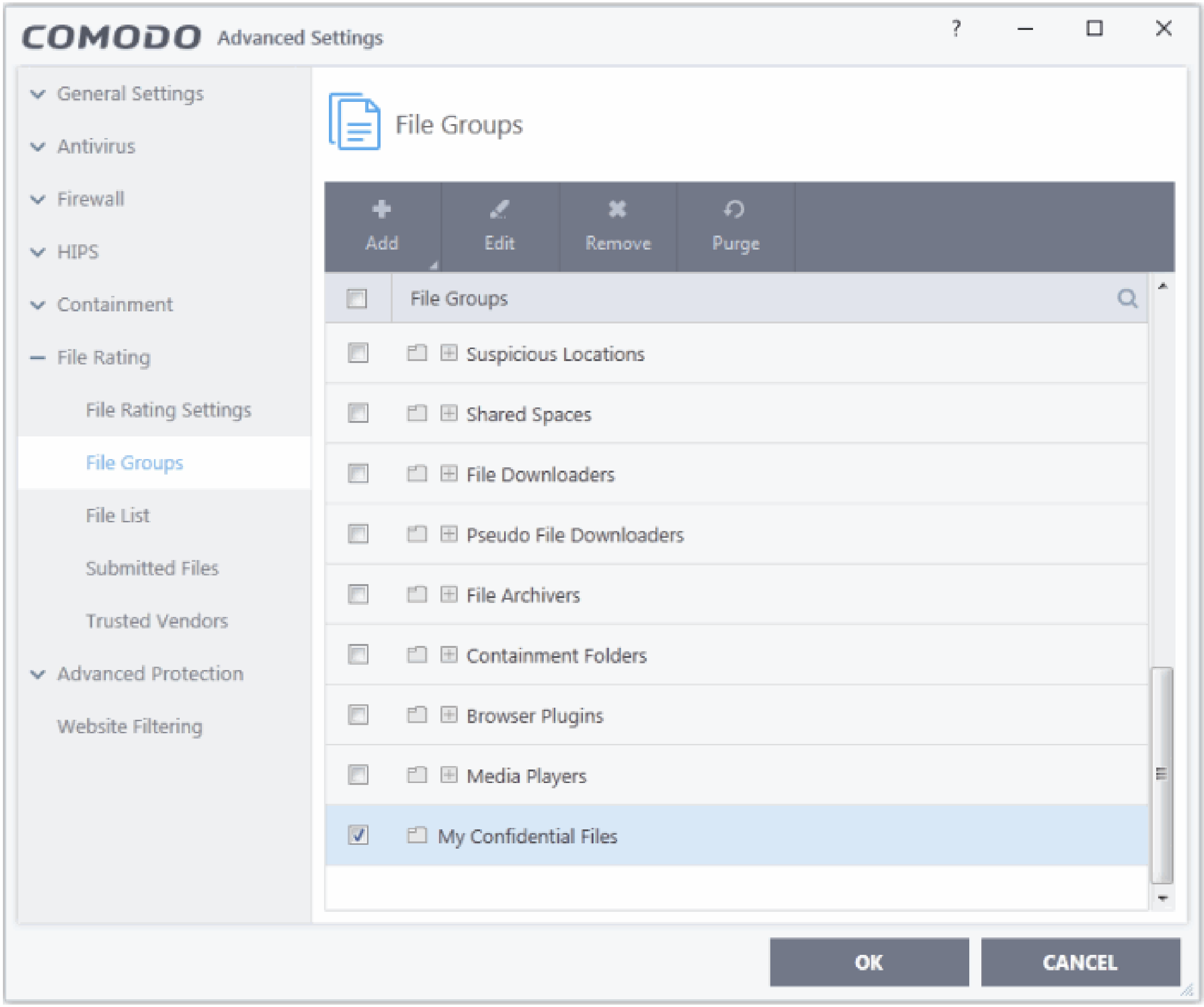
- Select 'New Group' from the 'Add' drop-down menu.
- Enter a 'File Group Name' in the 'Edit property' dialog and click 'OK'.



Choose File Group Name

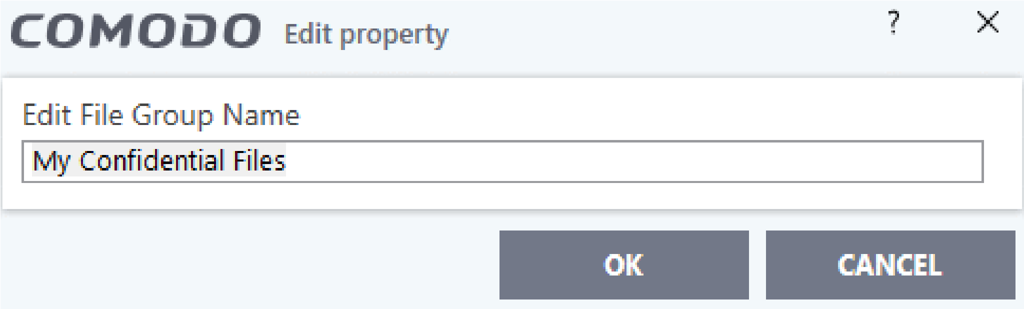
My Confidential Files

The 'File Group' will be added and displayed in the list.



□	File Groups
□	Suspicious Locations
□	Shared Spaces
□	File Downloaders
□	Pseudo File Downloaders
□	File Archivers
□	Containment Folders
□	Browser Plugins
□	Media Players
☑	My Confidential Files

- To edit the name of an existing group, select it from the 'File Groups' list and click the 'Edit' button.

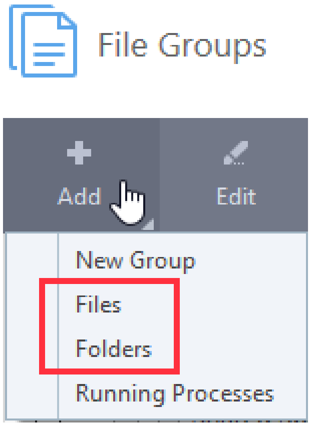


Edit File Group Name: My Confidential Files

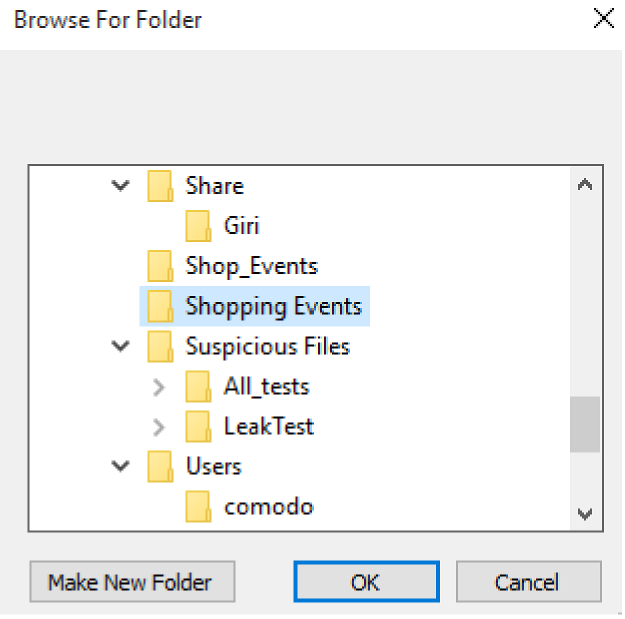
- Edit the 'File Group Name' in the 'Edit property' dialog and click 'OK'.

Add individual files or folder to a group

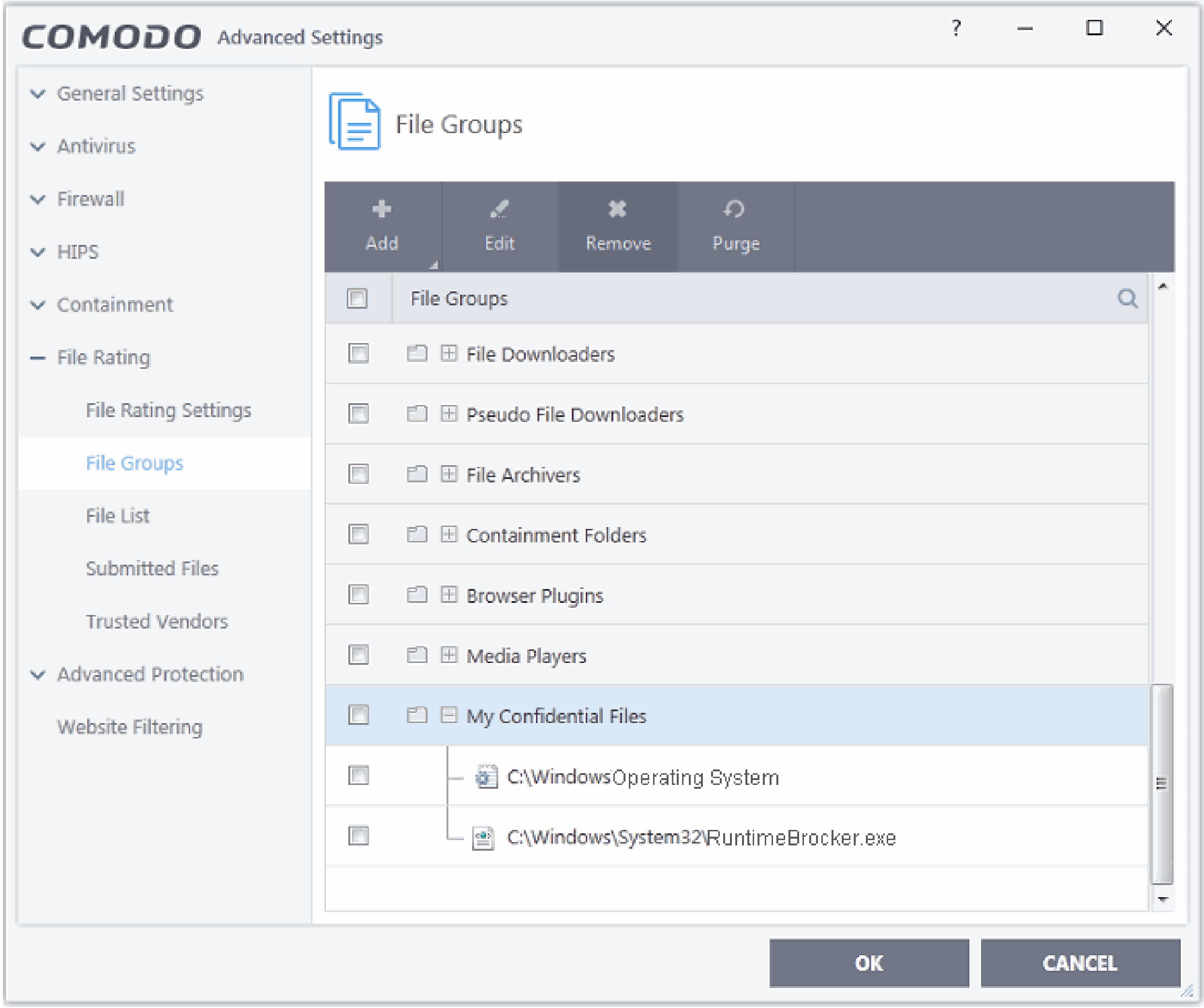
- Select the group from the list and click the 'Add' button. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes.
  - To add a file or folder, choose 'Files' or 'Folders' from the 'Add' drop-down menu.



The 'Browse' dialog will be displayed:



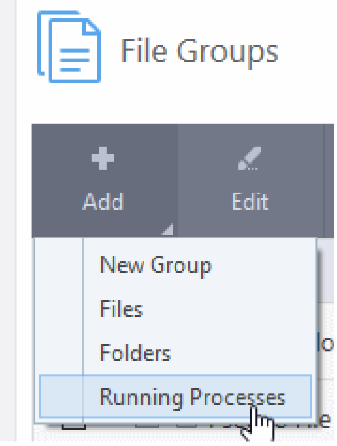
- Navigate to the file or folder you want to add to add to the group and click 'OK'



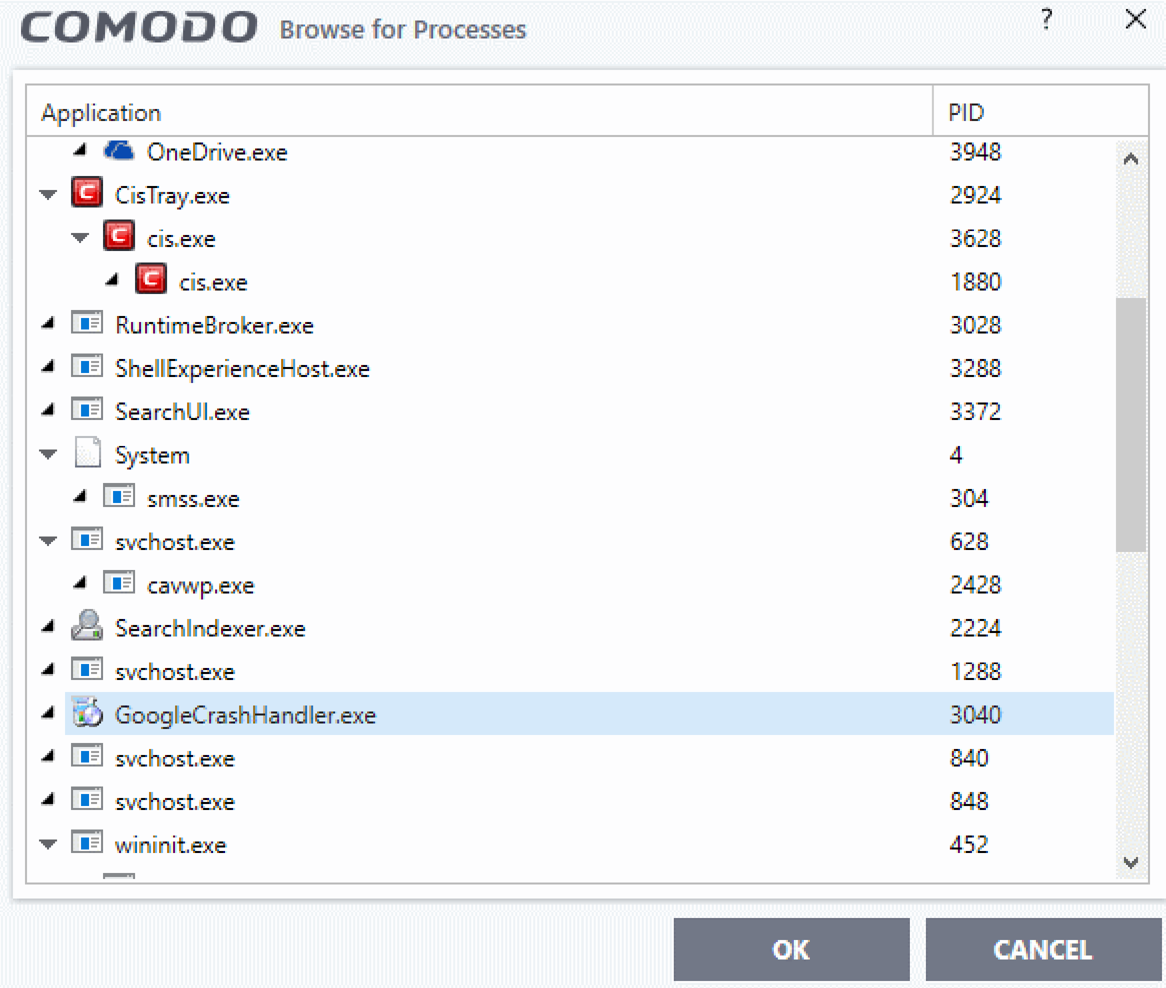
The drive file/folder will be added to 'File Groups'. Repeat the process to add more individual files or folders.

Add an application from a running processes

Click the 'Add' button then select 'Running Processes':



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



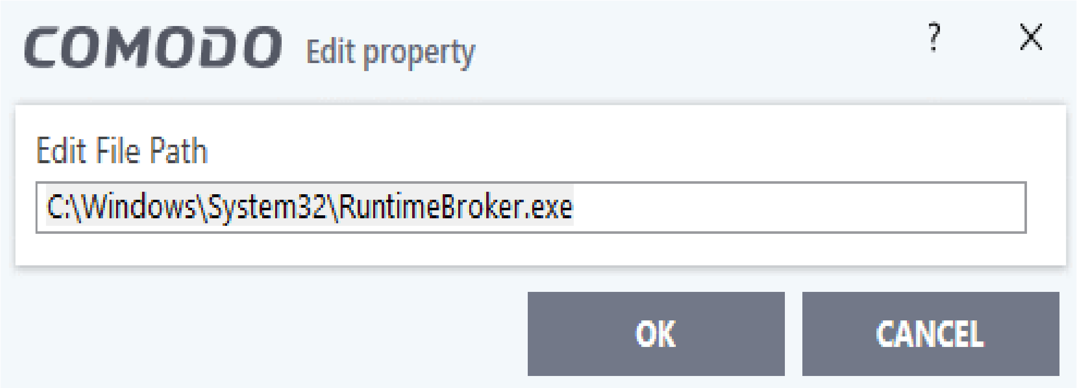
Application	PID
OneDrive.exe	3948
CisTray.exe	2924
cis.exe	3628
cis.exe	1880
RuntimeBroker.exe	3028
ShellExperienceHost.exe	3288
SearchUI.exe	3372
System	4
smss.exe	304
svchost.exe	628
cavwp.exe	2428
SearchIndexer.exe	2224
svchost.exe	1288
GoogleCrashHandler.exe	3040
svchost.exe	840
svchost.exe	848
wininit.exe	452

- Select the process, whose target application is to be added to 'Files Groups' and click 'OK' from the 'Browse for Process' dialog.

The application will be added to the selected group.

To edit an item in the Files Groups list

- Select the item from the list and click the 'Edit' button. The 'Edit property' dialog will be displayed:



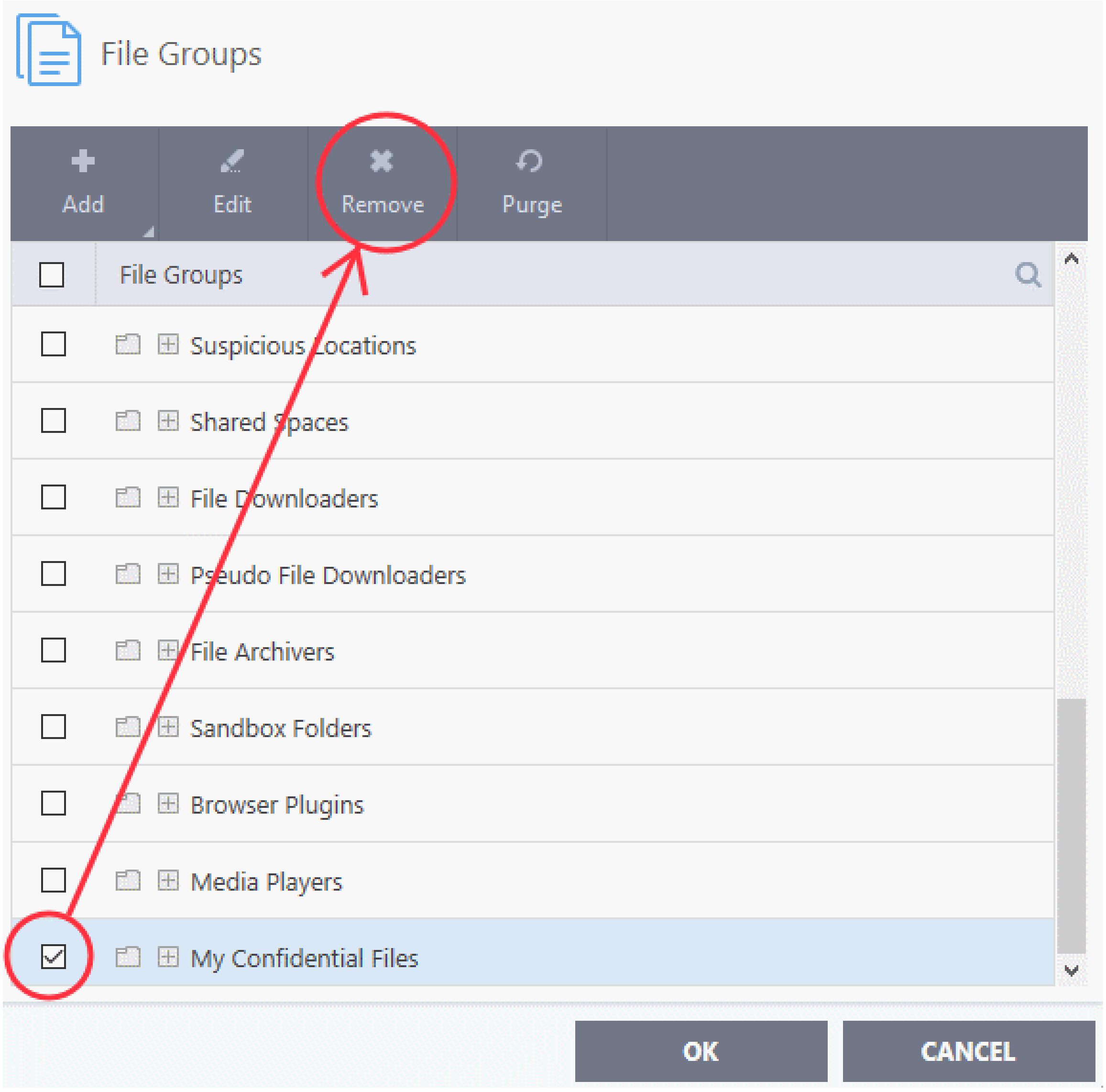
Edit File Path

C:\Windows\System32\RuntimeBroker.exe

- Edit the file path if required and click 'OK'.

To delete existing file group(s) individual file(s) from existing group

- To remove a file group, select it from the list and click the 'Remove' button.



- To remove an individual file from a group - expand the group by clicking '+' at the left of the group, select the file to be removed and click the 'Remove' button.
- Alternatively, right-click on a file and choose remove from drop-down menu.

6.6.3. File List

The 'File List' shows an inventory of executable files and applications discovered on your computer. Details about each file include the vendor, the date it was discovered and the file's trust rating.

- Click 'Settings' > 'File Rating' > 'File List' to open the file list

CIS rates files as:

- **Trusted**
- **Unrecognized**
- **Malicious**

Trusted Files

Files with a 'Trusted' rating are automatically given HIPS trusted status. Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, CIS will check the file against our master whitelist and blacklists and will award it trusted status if:
  - The application is from a vendor included in the **Trusted Software Vendors** list;
  - The application is included in the extensive and constantly updated Comodo safelist.
- User Rating - You can provide 'Trusted' status to your files in two ways:
  - If an executable is unknown to the HIPS safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, you could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted'.
  - You can assign 'Trusted' rating to any desired file from the Files List interface. See **changing the file rating** in **File Details** for more information.

  For the files assigned with 'Trusted' status by the user, CIS 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 (including sub folders containing many components) you can reduce the amount of alerts that HIPS generates whilst maintaining a higher level of HIPS 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.

Unrecognized Files

Once installed, HIPS monitors and verifies all file system activity on your computer. Every new executable file is first scanned against the virus blacklist (known 'bad' files) and the file whitelist (known 'good' files). If the file is on neither list it is given an 'Unrecognized' file rating. Apart from new executables, any executables that are modified are also given the 'Unrecognized' status. This helps safeguard against malware changing the behavior of a previously trusted application.

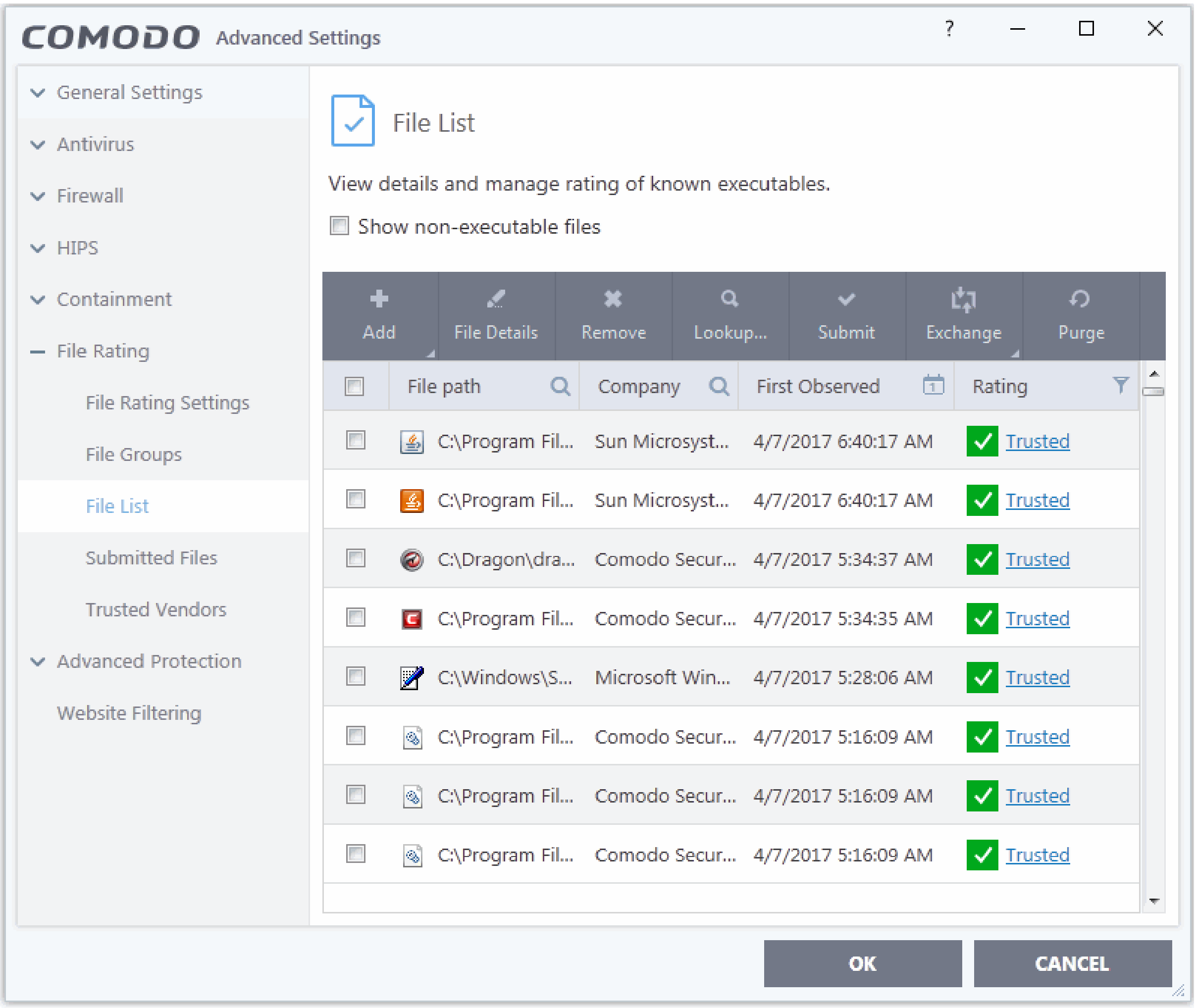
You can review pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be given the 'Trusted' rating. See **changing the file rating** for more details. You can also submit the files to Comodo for analysis. Experts at Comodo will analyze the files and add them to global white-list or black-list accordingly.

Malicious Files

Files that identified as malware will be given a 'Malicious' rating and will not be allowed to run.

To open the 'File List' interface

- Click 'Settings' from the top left of the CIS home screen then 'File Rating' > 'File List' from 'Advanced Settings'.



File List

View details and manage rating of known executables.

□ Show non-executable files

□	File path	Company	First Observed	Rating
□	C:\Program Fil...	Sun Microsyst...	4/7/2017 6:40:17 AM	✓ Trusted
□	C:\Program Fil...	Sun Microsyst...	4/7/2017 6:40:17 AM	✓ Trusted
□	C:\Dragon\dra...	Comodo Secur...	4/7/2017 5:34:37 AM	✓ Trusted
□	C:\Program Fil...	Comodo Secur...	4/7/2017 5:34:35 AM	✓ Trusted
□	C:\Windows\S...	Microsoft Win...	4/7/2017 5:28:06 AM	✓ Trusted
□	C:\Program Fil...	Comodo Secur...	4/7/2017 5:16:09 AM	✓ Trusted
□	C:\Program Fil...	Comodo Secur...	4/7/2017 5:16:09 AM	✓ Trusted
□	C:\Program Fil...	Comodo Secur...	4/7/2017 5:16:09 AM	✓ Trusted

The 'File List' pane displays applications, programs and executable files discovered on your computer.

Column Descriptions:

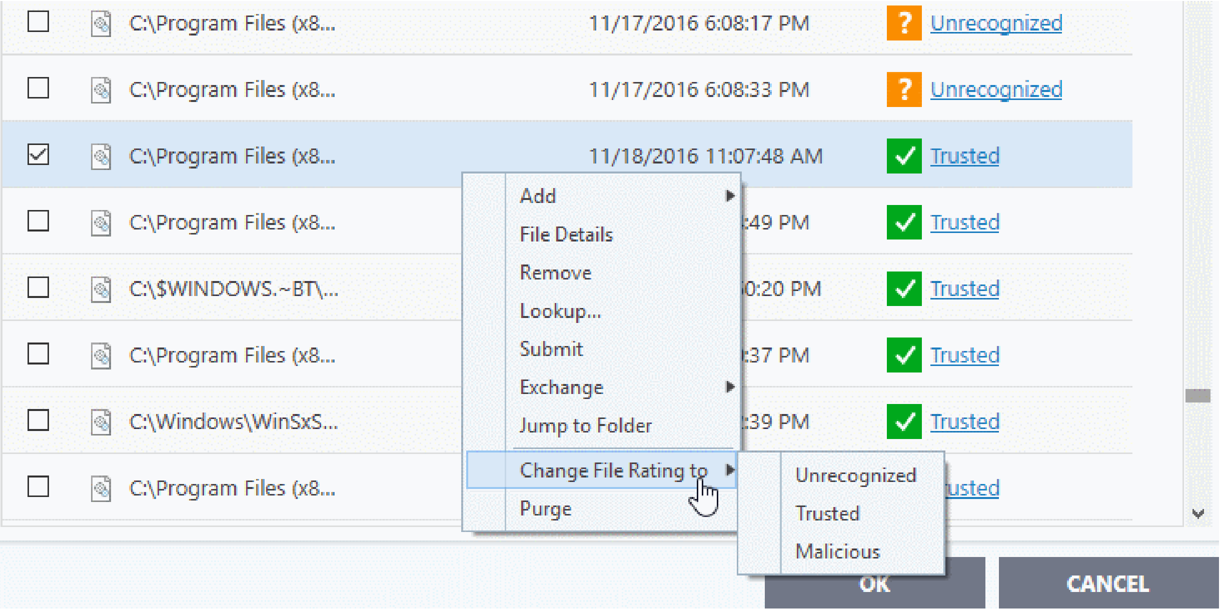
- **File Path-** Indicates the file's location
- **Company -** Shows the publisher of the file
- **First Observed -** Indicates date and time at which the file was first discovered by CIS.
- **File Rating -** Indicates the current CIS rating of the file. The possible values are:
  - **Trusted**
  - **Unrecognized**
  - **Malicious**

Files are rated based on the following, in order of priority:

1. Administrator rating (applicable only if your CIS installation is remotely managed by your CIS administrator).
2. User rating (rating as set by the user, if modified from the default rating)
3. FLS rating

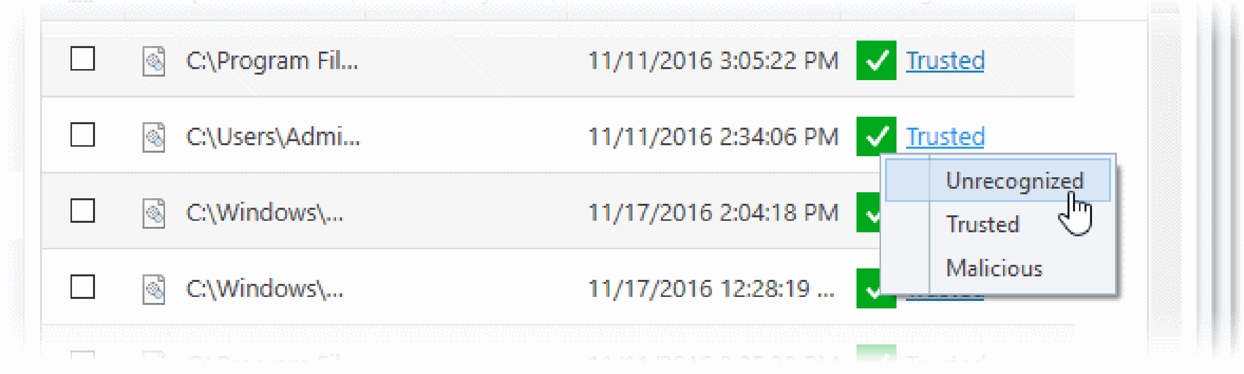
File rating can be modified by the user in three ways:

- Right click on a file, select 'Change File Rating to' from the context sensitive menu then choose a rating.



☐	C:\Program Files (x8...	11/17/2016 6:08:17 PM	? Unrecognized
☐	C:\Program Files (x8...	11/17/2016 6:08:33 PM	? Unrecognized
☑	C:\Program Files (x8...	11/18/2016 11:07:48 AM	✓ Trusted
☐	C:\Program Files (x8...	:49 PM	✓ Trusted
☐	C:\$WINDOWS.~BT\...	0:20 PM	✓ Trusted
☐	C:\Program Files (x8...	:37 PM	✓ Trusted
☐	C:\Windows\WinSxS...	:39 PM	✓ Trusted
☐	C:\Program Files (x8...		usted

- By clicking on the rating of a file in the 'Rating' column and choosing a new rating from the options

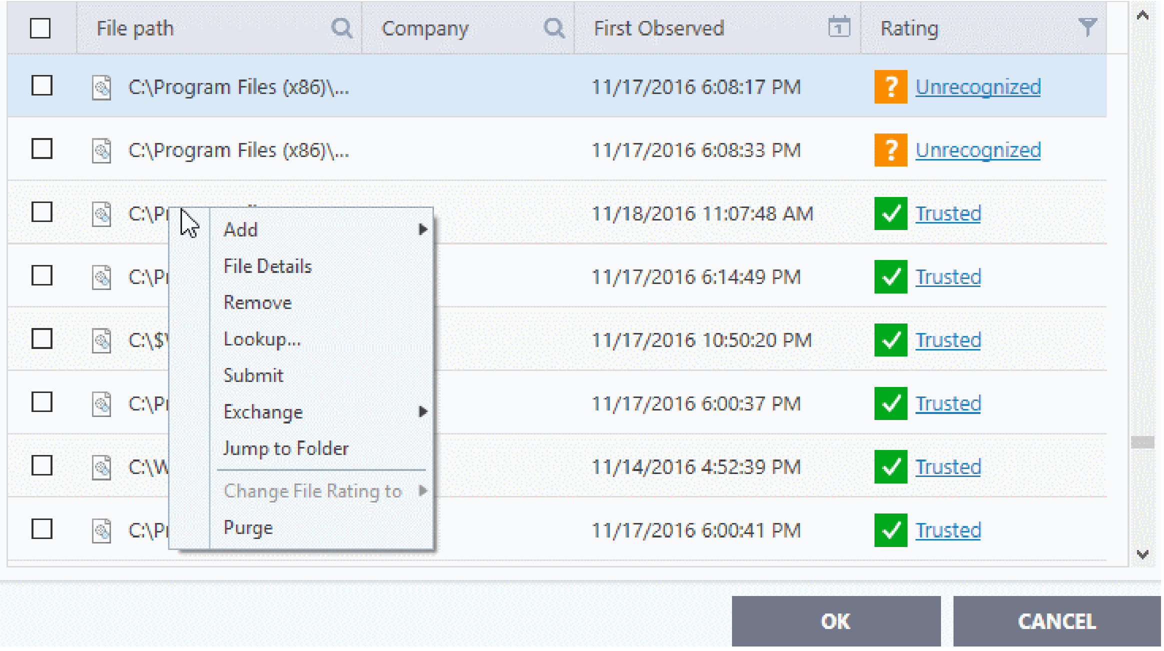


☐	C:\Program Fil...	11/11/2016 3:05:22 PM	✓ Trusted
☐	C:\Users\Admi...	11/11/2016 2:34:06 PM	✓ Trusted
☐	C:\Windows\...	11/17/2016 2:04:18 PM	✓
☐	C:\Windows\...	11/17/2016 12:28:19 ...	✓

- From the 'File Details' dialog. Select a file and click the 'File Details' button at the top. See **changing the file rating** under **File Details** for more details.

Context Sensitive Menu

Right-clicking on a file opens a context sensitive menu that allows you to view the 'File Details' dialog, remove the file from the list, submit the file to Comodo for analysis and more.



□	File path	Company	First Observed	Rating
□	C:\Program Files (x86)\...		11/17/2016 6:08:17 PM	Unrecognized
□	C:\Program Files (x86)\...		11/17/2016 6:08:33 PM	Unrecognized
□	C:\Pr		11/18/2016 11:07:48 AM	Trusted
□	C:\Pr		11/17/2016 6:14:49 PM	Trusted
□	C:\$\		11/17/2016 10:50:20 PM	Trusted
□	C:\Pr		11/17/2016 6:00:37 PM	Trusted
□	C:\W		11/14/2016 4:52:39 PM	Trusted
□	C:\Pr		11/17/2016 6:00:41 PM	Trusted

- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the file submission process.
- **Import** - Enables you import a file list from an XML file
- **Export** - Enables you export the current file list with existing ratings to an XML file
- **Jump to Folder** - Opens the folder containing the file in Windows Explorer.
- **Change File Rating to** - Allows you to change the file rating.
- **Purge** - Runs a system check to verify that all the files for which the ratings are listed are actually installed on the host machine at the path specified. If not, the fie is removed, or 'purged', from the list.

Sorting, searching and filtering options

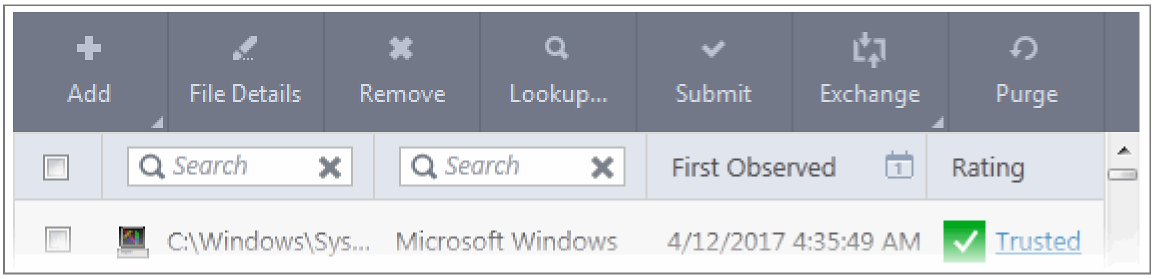
Sorting option

You can sort the items in alphabetical / ascending / descending order by clicking on the respective column headers.

Searching option

You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and 'File rating'.

To use the search option, click the search icon at the far right in the 'File path' and/or 'Company' column header.



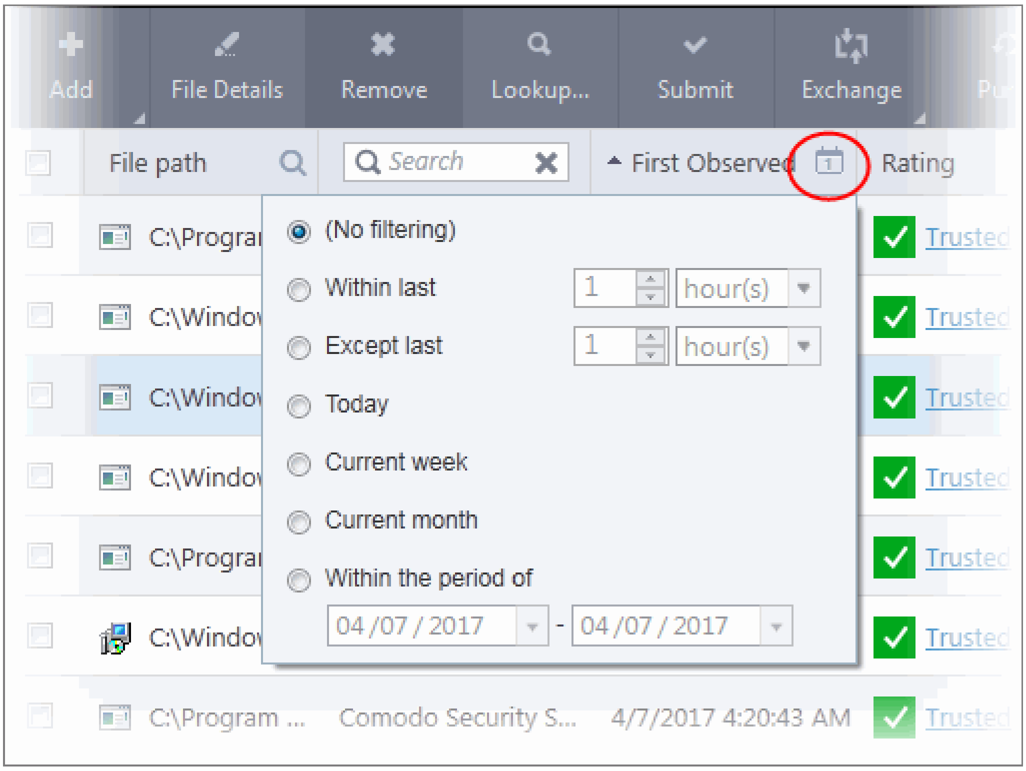
□	Search	Search	First Observed	Rating
□	C:\Windows\Sys...	Microsoft Windows	4/12/2017 4:35:49 AM	Trusted

- Enter the file path and/or the name of company in part or full as per the selected criteria in the search field

The result for the entered criteria will be listed automatically within a few moments. Click the 'X' icon to clear the search criteria and display all the items again in the list.

Filtering option

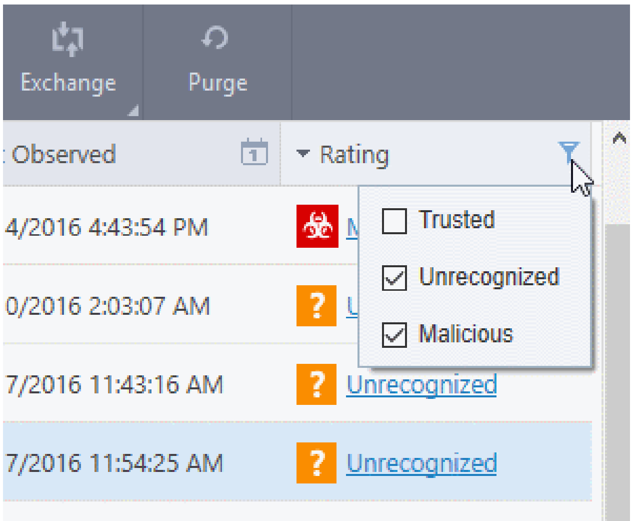
- To filter the list based on the date of installation or storage of the files, click the calendar icon at the right of the 'First Observed' column header and choose the time/date/period.



● (No filtering)
○ Within last 1 hour(s)
○ Except last 1 hour(s)
○ Today
○ Current week
○ Current month
○ Within the period of 04 /07 / 2017 - 04 /07 / 2017

C:\Progra			✓ Trusted
C:\Windo			✓ Trusted
C:\Windo			✓ Trusted
C:\Windo			✓ Trusted
C:\Progra			✓ Trusted
C:\Windo			✓ Trusted
C:\Program ...	Comodo Security S...	4/7/2017 4:20:43 AM	✓ Trusted

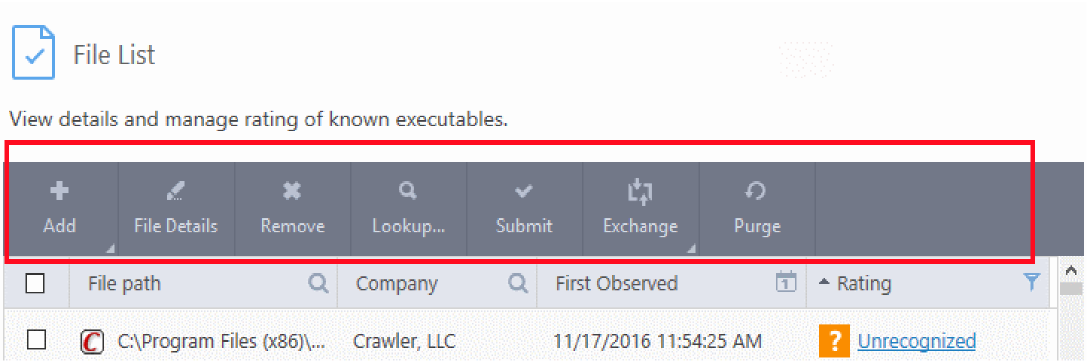
- To filter the list based on the file rating, click the funnel icon at the right of the 'File Rating' column header and select the specific ratings to display the files.



☐ Trusted
☑ Unrecognized
☑ Malicious

4/2016 4:43:54 PM	M
0/2016 2:03:07 AM	U
7/2016 11:43:16 AM	Unrecognized
7/2016 11:54:25 AM	Unrecognized

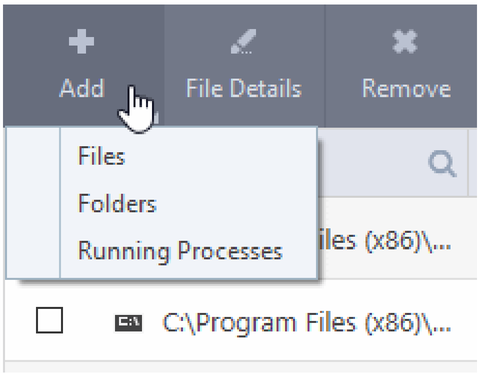
The buttons at the top provide the following options:



- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the file submission process.
- **Exchange** - Consists of two options (**Import** and **Export**).
    - **Import** - Allows you to import a file list from an XML file
    - **Export** - Allows you to export the current file list and ratings to an XML file
- **Purge** - Runs a check to verify the listed applications are still installed on the host machine at the stated location. If not, the rule is removed, or 'purged', from the list.

To manually add files to 'File list'

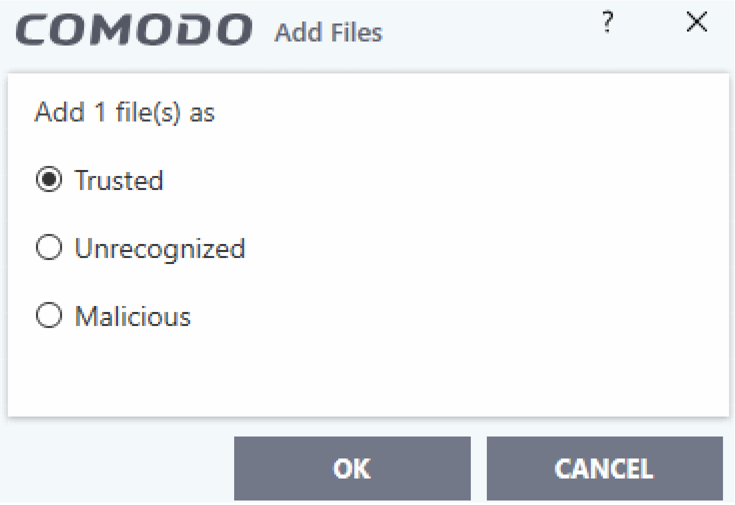
- Click the 'Add' button at the top



Tip: Alternatively, right click inside the 'File List' page and choose 'Add' from the context sensitive menu.

- You can add files to the file list by three ways:
    - **Files** - Allows you to navigate to the file or executable of the program you wish to add and assign a rating.
    - **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'File List' with the rating you assign.
    - **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'File List' with the rating you assign.

Once you have chosen the file(s) or the folder, you can assign the rating for the file(s) to be added.



Add 1 file(s) as

● Trusted

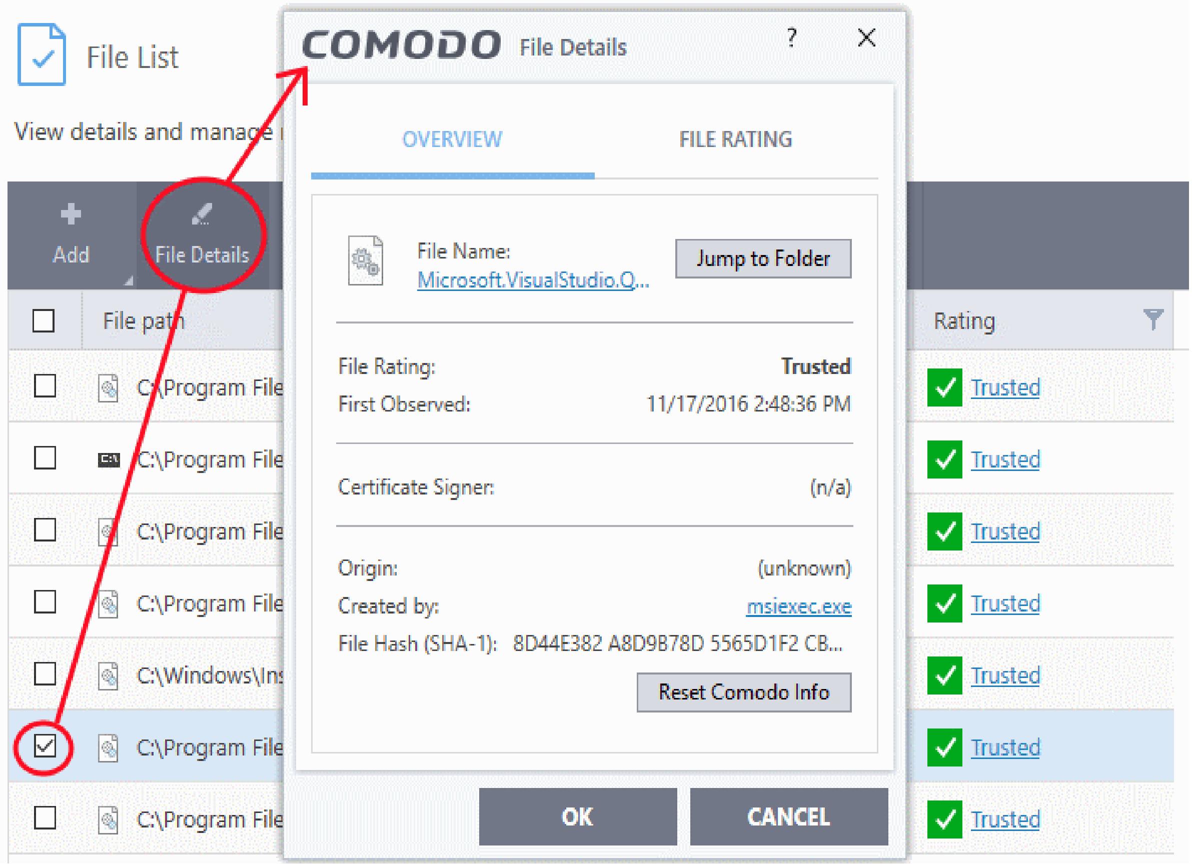
○ Unrecognized

○ Malicious

- Choose the rating to be assigned to the file(s). The available options are:
  - Trusted - The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
  - Unrecognized - The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
  - Malicious - The file will not be allowed to run.
- Click 'OK' in the 'Add Files' dialog.
- Click 'OK' in the 'Advanced Settings' for your changes to take effect.

To view the 'File Details' and change the rating

- Choose the file to view its details and click the 'File Details' button on the 'File List' pane.



	File path	Rating
□	C:\Program File	✓ Trusted
□	C:\Program File	✓ Trusted
□	C:\Program File	✓ Trusted
□	C:\Program File	✓ Trusted
□	C:\Windows\Ins	✓ Trusted
☑	C:\Program File	✓ Trusted
□	C:\Program File	✓ Trusted

File Name: Microsoft.VisualStudio.Q...

File Rating: Trusted

First Observed: 11/17/2016 2:48:36 PM

Certificate Signer: (n/a)

Origin: (unknown)

Created by: msiexec.exe

File Hash (SHA-1): 8D44E382 A8D9B78D 5565D1F2 CB...

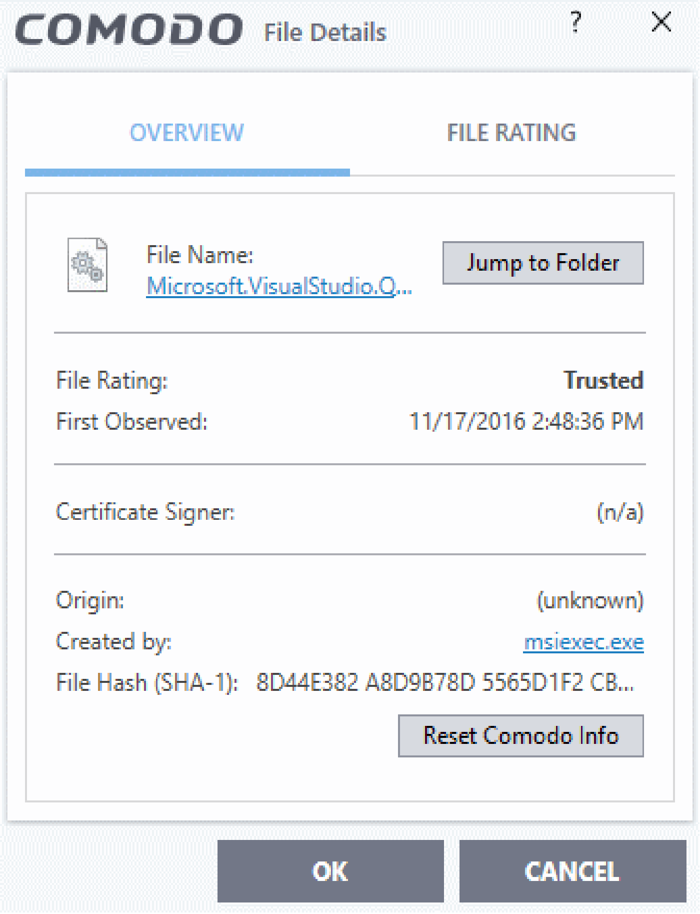
Tip: Alternatively, right click on the selected file inside the 'File List' page and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog contains two tabs:

- Overview
- File Rating

Overview

The 'Overview' tab displays the general details of the file and the publisher details.



File Name: Microsoft.VisualStudio.Q...

File Rating: Trusted

First Observed: 11/17/2016 2:48:36 PM

Certificate Signer: (n/a)

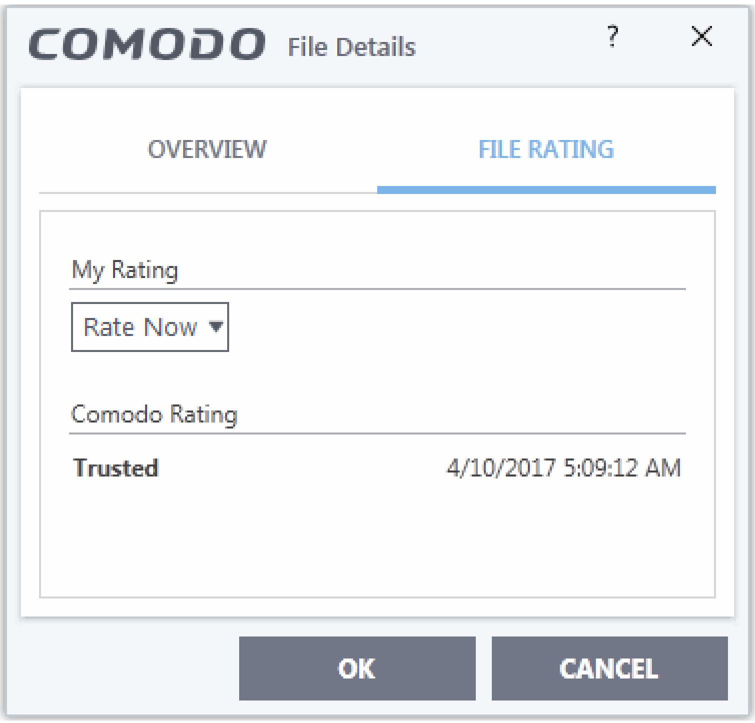
Origin: (unknown)

Created by: msiexec.exe

File Hash (SHA-1): 8D44E382 A8D9B78D 5565D1F2 CB...

- Clicking the file name opens the Windows 'File Properties' dialog.
- Clicking 'Jump to folder' opens the folder containing the file in Windows Explorer, with the respective file selected.

File Rating



My Rating

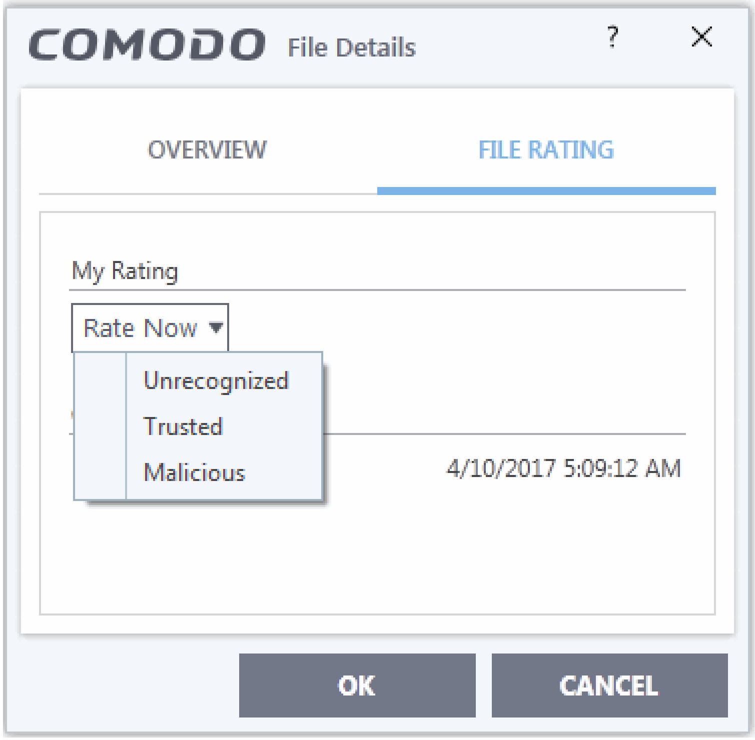
Comodo Rating

Trusted 4/10/2017 5:09:12 AM

The 'File Rating' tab enables you to change the current rating of the file and displays the current rating as per the analysis result from Comodo.

To change the user rating of the file

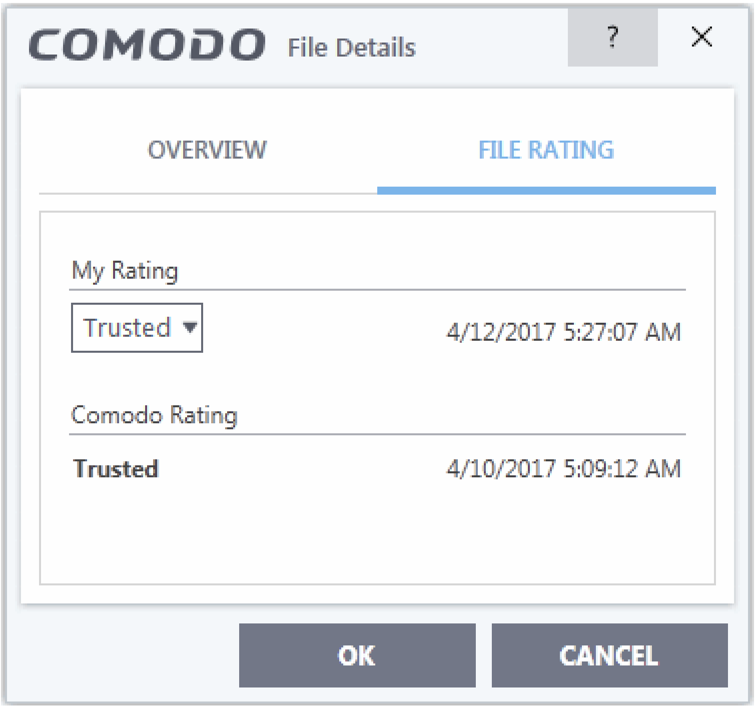
- Select the file from the 'File List' pane and click the 'File Details' button
- Click the 'File Rating' tab from the 'File Details' tab
- Click 'Rate Now' and choose the rating from the drop-down



The options available are:

- Trusted - The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- Unrecognized - The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- Malicious - The file will be deleted or placed in quarantine and will not be allowed to run.

Once you chose a rating for a file it will be displayed under 'My Rating'.



My Rating

Trusted 4/12/2017 5:27:07 AM

Comodo Rating

Trusted 4/10/2017 5:09:12 AM

- Click 'OK' in the 'Files Details' dialog

Tip: Alternatively, right click on a selected file, then choose 'Change File Rating to' from context sensitive menu and select the rating.

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

To remove files(s) from the File list

- Select the file(s) to be removed from the 'File List' pane. You can select several entries to be removed at once by marking the check-boxes beside the entries.
- Click the 'Remove' button at the top from the 'File List' pane. The file is only removed from the list and not deleted from your system.

Tip: Alternatively, right click on a selected file, then choose 'Remove' from context sensitive menu and select options from drop-down menu.

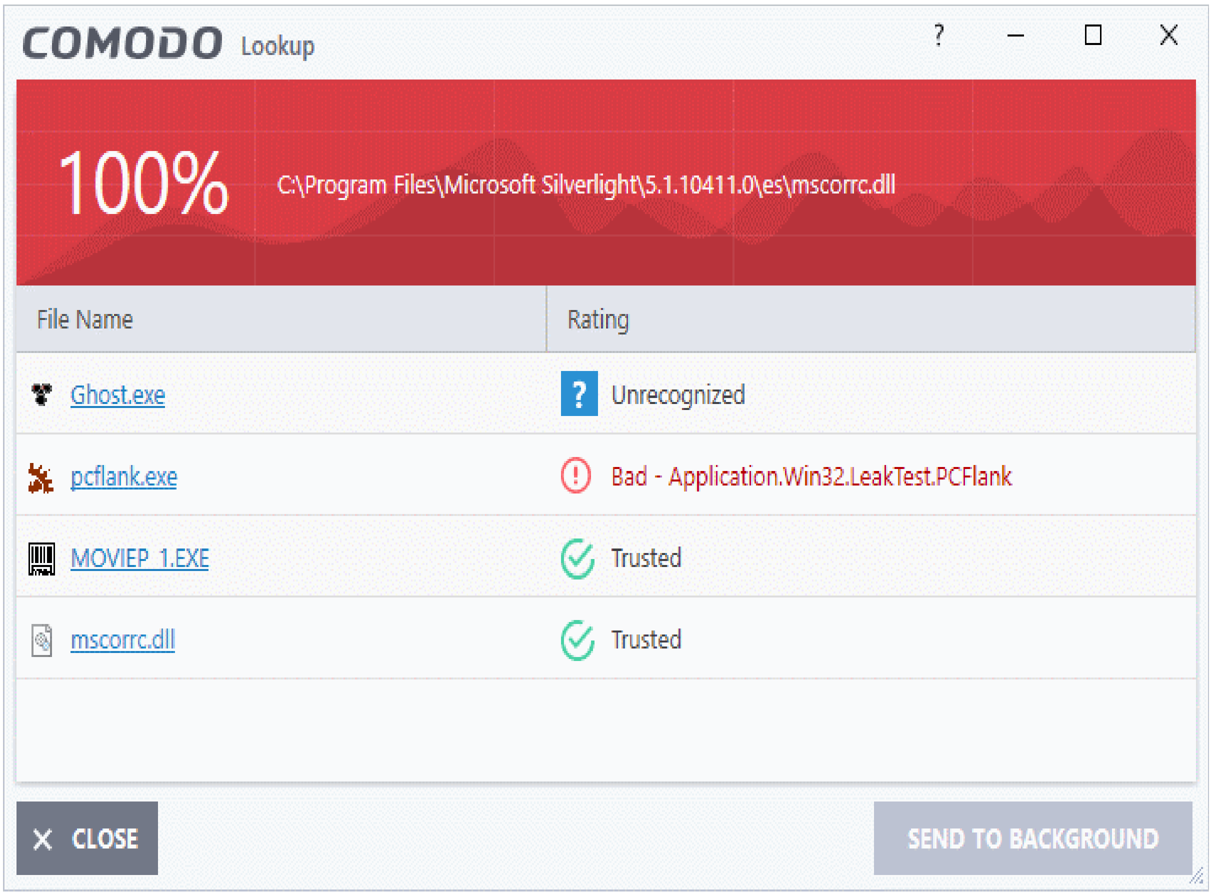
- Click 'OK' for your changes to take effect.

To perform an online lookup for files

- Select the files to be checked from the 'File list' pane. You can select several entries at once by marking the check-boxes beside the entries.
- Click the 'Lookup...' button at the top from the 'File list' pane.

Tip: Alternatively, right click on a selected file, then choose 'Lookup' from the context sensitive menu.

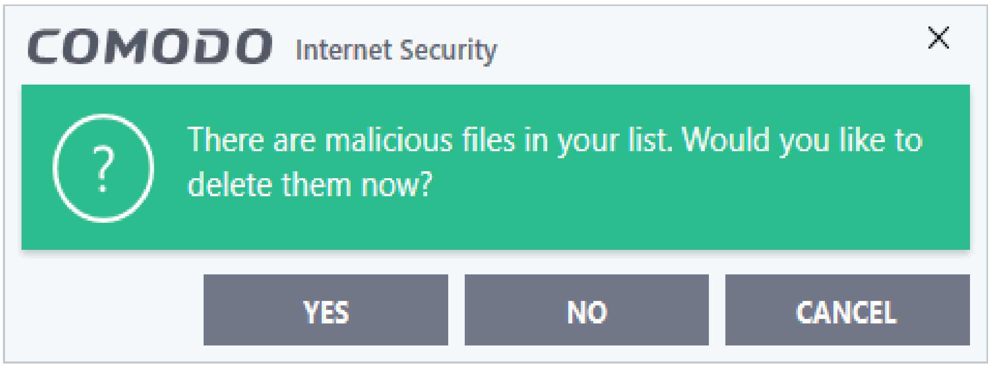
Comodo servers will be contacted immediately to conduct a search of Comodo's master safe list database to check if any information is available about the files in question and the results will be displayed.



C:\Program Files\Microsoft Silverlight\5.1.10411.0\es\mscorrc.dll

File Name	Rating
Ghost.exe	? Unrecognized
pcflank.exe	Bad - Application.Win32.LeakTest.PCFlank
MOVIEP_1.EXE	✓ Trusted
mscorrc.dll	✓ Trusted

If any malicious or unwanted file(s) is/are found, you will be given an option to delete the file from your computer on closing the dialog.



There are malicious files in your list. Would you like to delete them now?

- Click 'Yes' to permanently delete the malicious file(s) from your computer.
- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. See **changing the file rating** in **File Details** for more details.
- If no information is available, it will be indicated as 'Unknown' with a yellow icon. You can submit the file to Comodo for analysis. See **explanation below** for more details.

To manually submit files to Comodo

- Select the file(s) to be submitted from the 'File List' pane. You can select several entries to be sent at once by marking the check-boxes beside the entries.
- Click the 'Submit' button at the top from the 'File List' pane. The file(s) will be immediately sent to Comodo.

Tip: Alternatively, right click on a selected file, then choose 'Submit' from the context sensitive menu.

You can view the list of files you submitted so far, from the '**Submitted Files**' panel.

Exporting and Importing the File List

You can export the list of files with their currently assigned file ratings to an XML file and store the list on a safe place. This is useful to restore your 'File List', in case you are reinstalling the CIS application for some reasons.

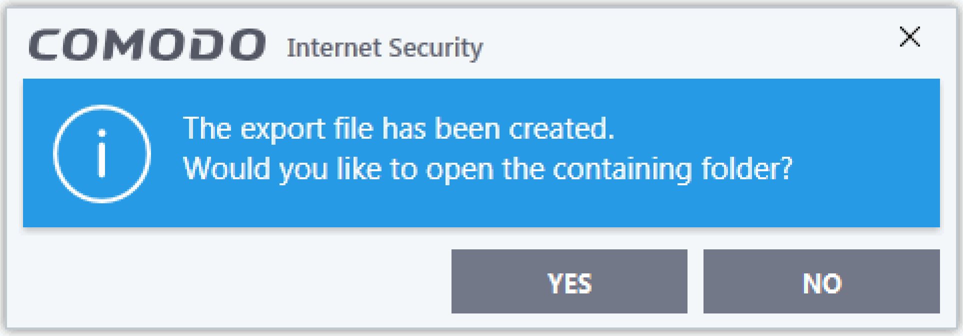
To export the File List

- Click the 'Exchange' button at the top of the 'File List' pane then select 'Export' from the menu

Tip: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Export'

- Navigate to where you want to store the exported list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.



The export file has been created.
Would you like to open the containing folder?

To import a saved file list

- Click the 'Exchange' button at the top of the 'File List' pane, then select 'Import' from the menu.

Tip: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Import'

- Navigate to the location of the XML file containing the file list and click 'Open'.

The 'File List' will be populated as per the imported 'File List'.

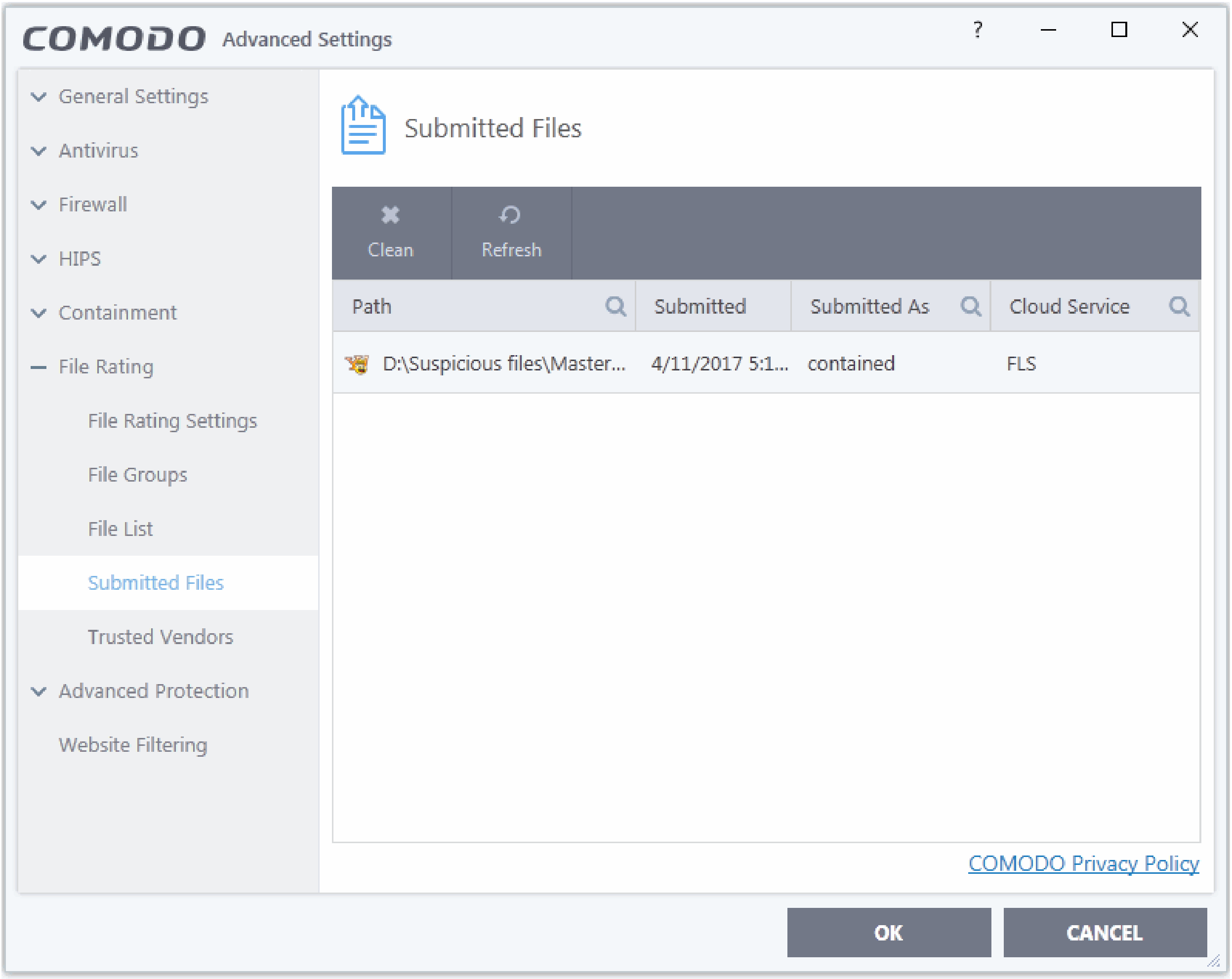
6.6.4. Submitted Files

The 'Submitted Files' panel shows files that were automatically uploaded to Comodo for analysis. The analysis includes a range of static and dynamic behavior tests intended to find out if the file is malicious or not. Submitting files is particularly useful if a file has an 'unknown' trust rating.

Background Note: Background Note: CIS has the capability of automatically submitting unknown files for analysis to Comodo, for example, files that are identified as unknown by a file rating scan will be automatically uploaded. Also, you can submit manually to Comodo for further analysis through the 'Submit File' option in 'Advanced Tasks'. See for <manually submitting files > more details.

To open the 'Submitted Files' interface

- Click 'Settings' on the CIS home screen
- Click 'File Rating' > 'Submitted Files' on the left:



Path	Submitted	Submitted As	Cloud Service
D:\Suspicious files\Master...	4/11/2017 5:1...	contained	FLS

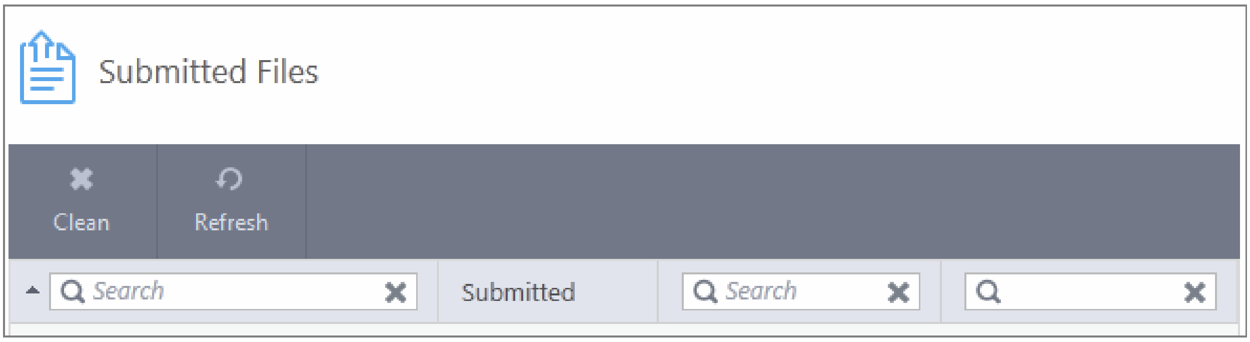
Sorting and searching options

Sorting option

You can sort items in alphabetical / ascending / descending order by clicking the respective column headers.

Searching option

You can use the search icons to find a specific file based on the file path and/or 'submitted as' parameter.



- Enter the file path and/or 'submitted as' in part or full as per the selected criteria in the search field

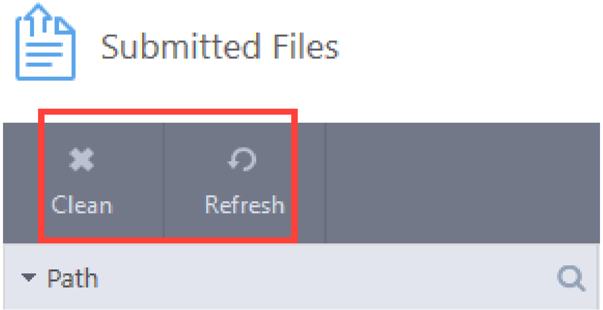
The result for the entered criteria will be listed automatically within a few moments. Click the 'X' icon to clear the search criteria and display all the items again in the list.

- Click the 'X' icon to clear the search criteria and display all the items again in the list.

Column Descriptions:

- **Path** – The location of the file on your computer
- **Submitted** – Date and time the file was uploaded for analysis;
- **Submitted As** – The label under which the file was uploaded. Examples include 'automated' and 'contained'.
- **Cloud Service**- The name of the Comodo cloud service to which the files were submitted. This is usually the Valkyrie analytics system operated by Comodo.

The buttons at the top provide the following options:



- **Clean** - Clears the list
- **Refresh -** Reloads the list to add items that are submitted recently

6.6.5. Trusted Vendors List

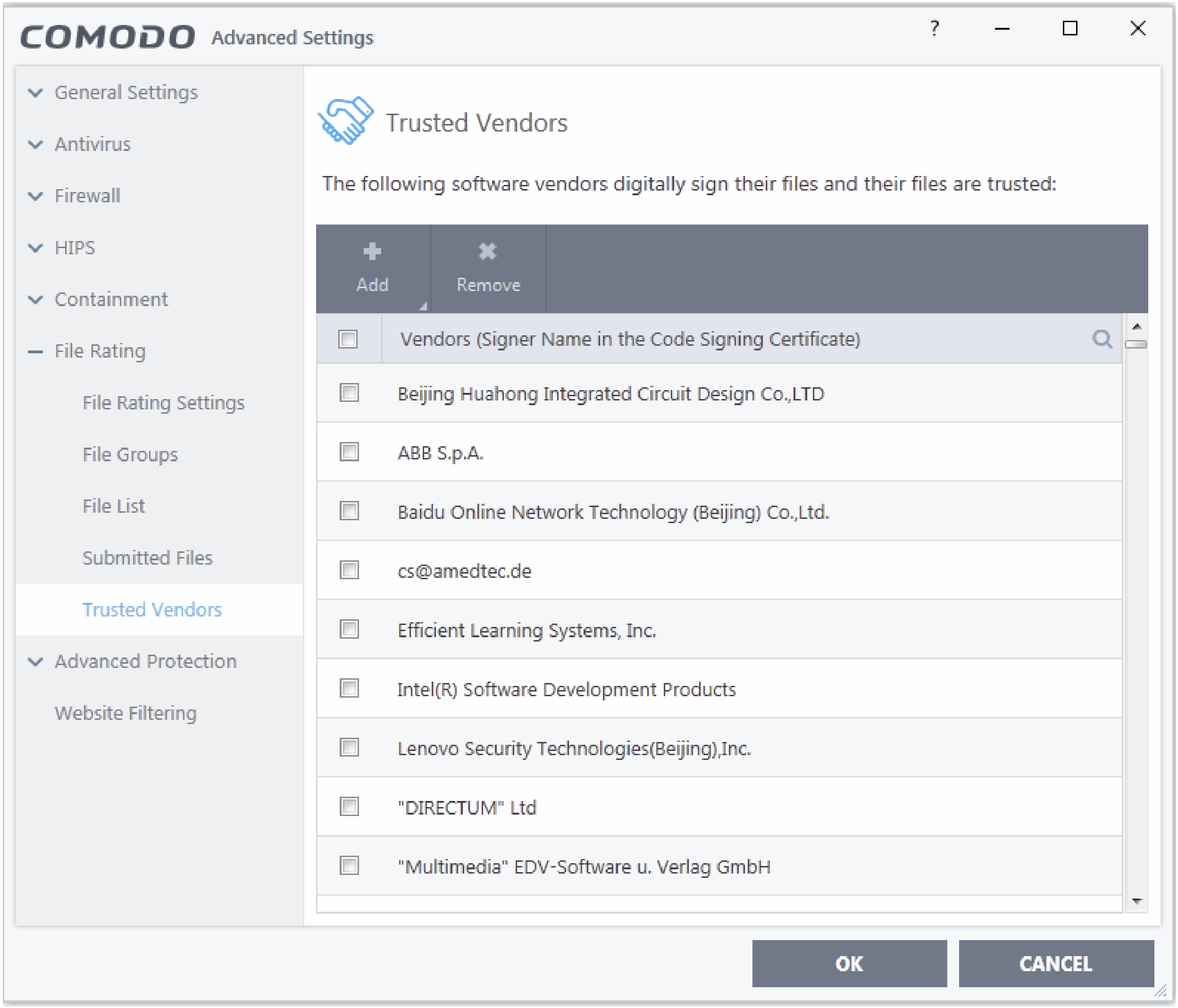
In Comodo Internet Security, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (a white-listed of trusted executables) OR the application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

From this point:

- If the vendor is on the 'Trusted Software Vendor List' AND the user has enabled '**Trust Applications signed by Trusted Vendors**' in the 'File Rating Settings' panel, then the application will be trusted and allowed to run.
- If the vendor is not on the 'Trusted Software Vendor List' OR the user has not enabled 'Trust Applications signed by Trusted Vendors', then the application will be contained. If the application in question is an installer then CIS will generate an elevated privilege alert.

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

The 'Trusted Software Vendors' panel can be opened by clicking Settings > 'File Rating' > 'Trusted Vendors'.



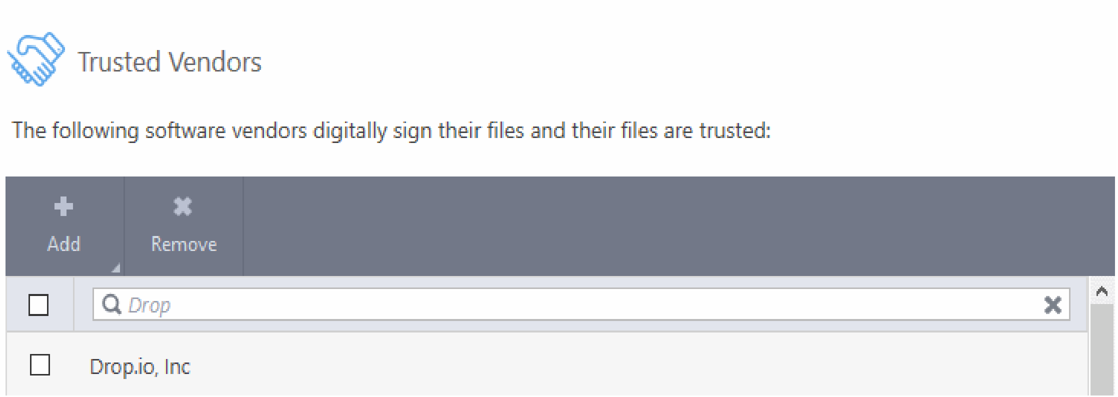
Trusted Vendors

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

□	Vendors (Signer Name in the Code Signing Certificate)
□	Beijing Huahong Integrated Circuit Design Co.,LTD
□	ABB S.p.A.
□	Baidu Online Network Technology (Beijing) Co.,Ltd.
□	cs@amedtec.de
□	Efficient Learning Systems, Inc.
□	Intel(R) Software Development Products
□	Lenovo Security Technologies(Beijing),Inc.
□	"DIRECTUM" Ltd
□	"Multimedia" EDV-Software u. Verlag GmbH

You can use the search option to find a specific vendor in the list.

- To use the search option, click the search icon at the top right



Trusted Vendors

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

□	Drop
□	Drop.io, Inc

- Enter partly or fully the vendor's name in the search field.

The result for the entered criteria will be listed automatically within a few moments.

- Click the 'X' icon to clear the search criteria and display all the items again in the list.
- **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. They know 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 first column in the graphic above.

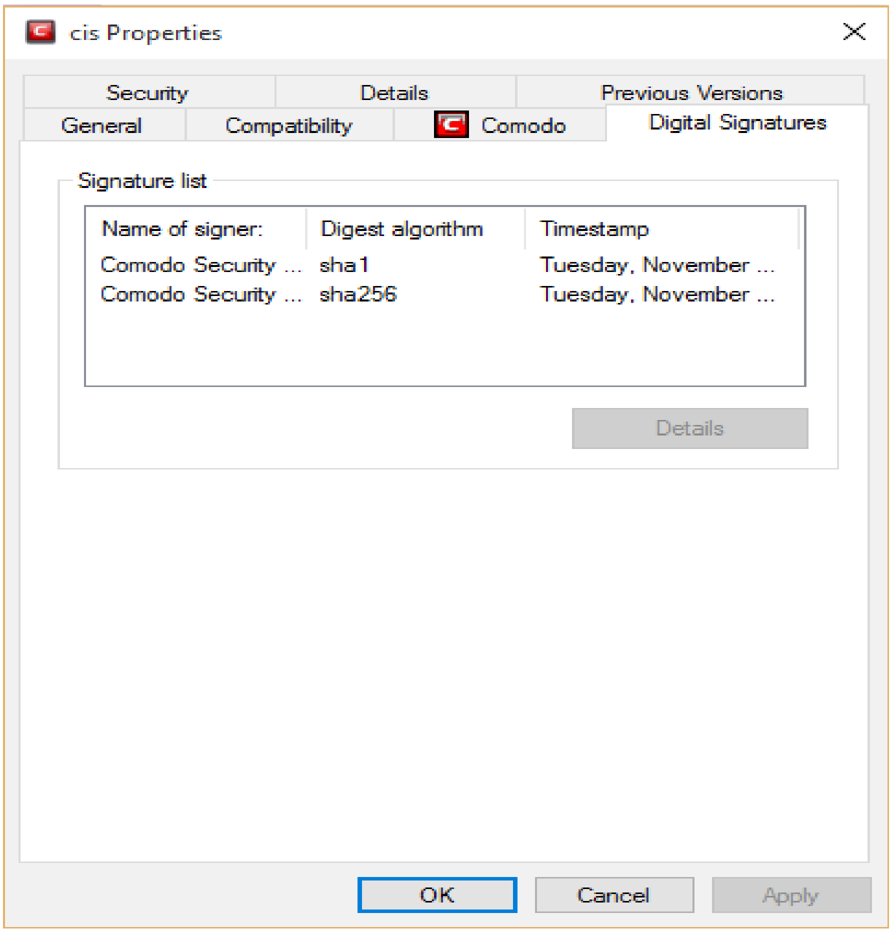
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign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

If a file is signed by a 'Trusted Software Vendor' and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Internet Security (if you would like to read more about code signing certificates, see **http://www.instantssl.com/code-signing/**).

One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Internet Security is called 'cis.exe' and has been digitally 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. They know they are downloading and installing the genuine software.
- The 'Vendors' that digitally sign their software 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 'Certificate Authority' (CA).
- 'Comodo CA Limited' and 'Verisign' are two example CAs who are authorized to counter-sign 3rd party software.
- The counter-signature is critical to the trust process. A CA only counter-signs a certificate after it has conducted detailed background checks on the publisher.
- If a file is signed by a 'Trusted Software Vendor' and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Client Security (if you would like to read more about code signing certificates, see **http://www.instantssl.com/code-signing/**).
- One of the methods of identifying whether an executable file has been digitally signed is by checking the properties of the .exe file in question.
- For example, the main program executable for Comodo Client Security is called 'cis.exe' and has been digitally signed.
  - Browse to the (default) installation directory of Comodo Internet Security.
  - Right click on the file cis.exe.
  - Select 'Properties' from the menu.
  - Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

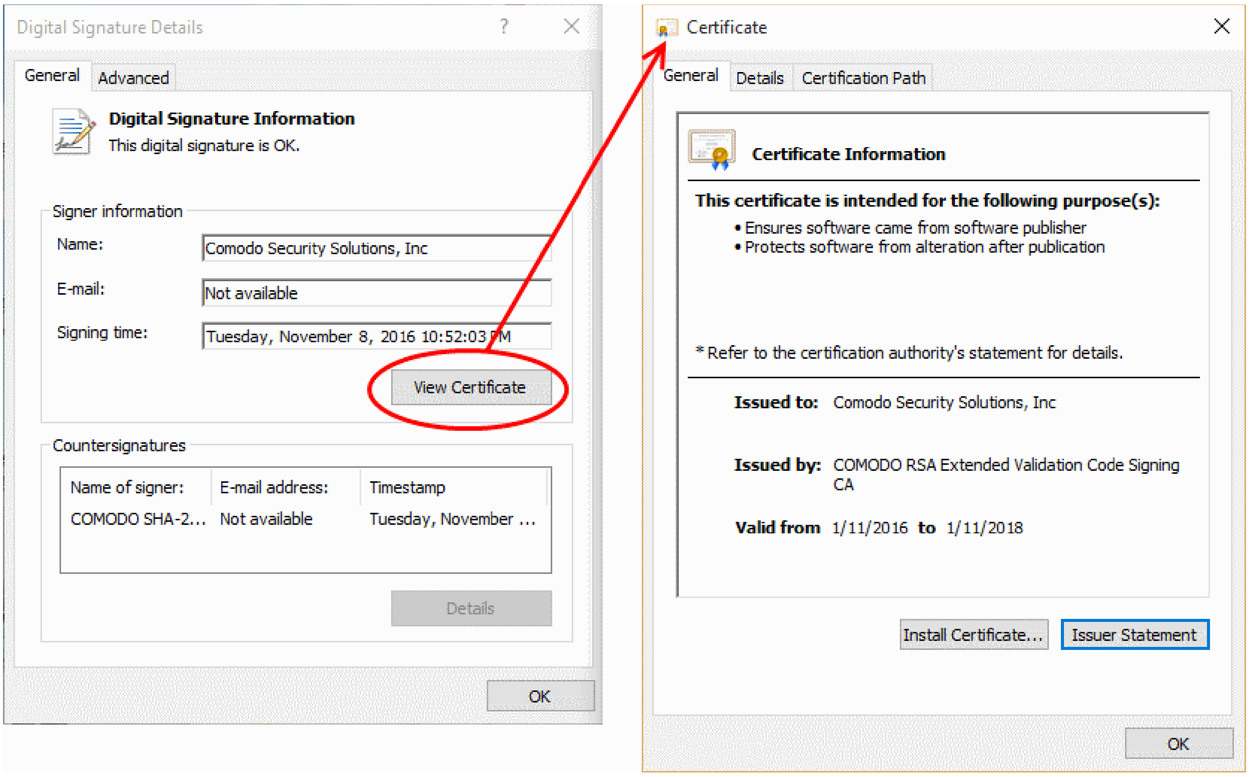
This displays the name of the CA that signed the software as shown below:



Signature list

Name of signer:	Digest algorithm	Timestamp
Comodo Security ...	sha1	Tuesday, November ...
Comodo Security ...	sha256	Tuesday, November ...

Click the 'Details' button to view certificate details. Click the 'View Certificate' button to inspect the actual code signing certificate. (see below).



Digital Signature Information

This digital signature is OK.

Signer information

Name: Comodo Security Solutions, Inc

E-mail: Not available

Signing time: Tuesday, November 8, 2016 10:52:03 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
COMODO SHA-2...	Not available	Tuesday, November ...

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

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

Issued to: Comodo Security Solutions, Inc

Issued by: COMODO RSA Extended Validation Code Signing CA

Valid from 1/11/2016 to 1/11/2018

It should be noted that the example above is a special case in that Comodo, as creator of 'cis.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.

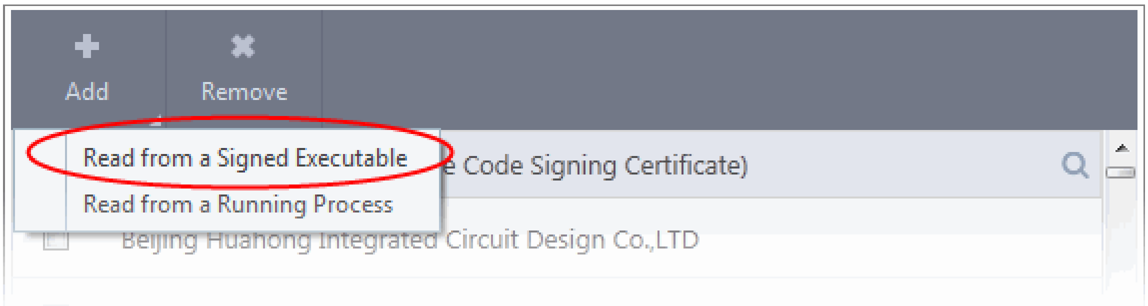
Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

- **By reading the vendor's signature from an executable file on your local drive**
- **By reading the vendor's signature from a running process**

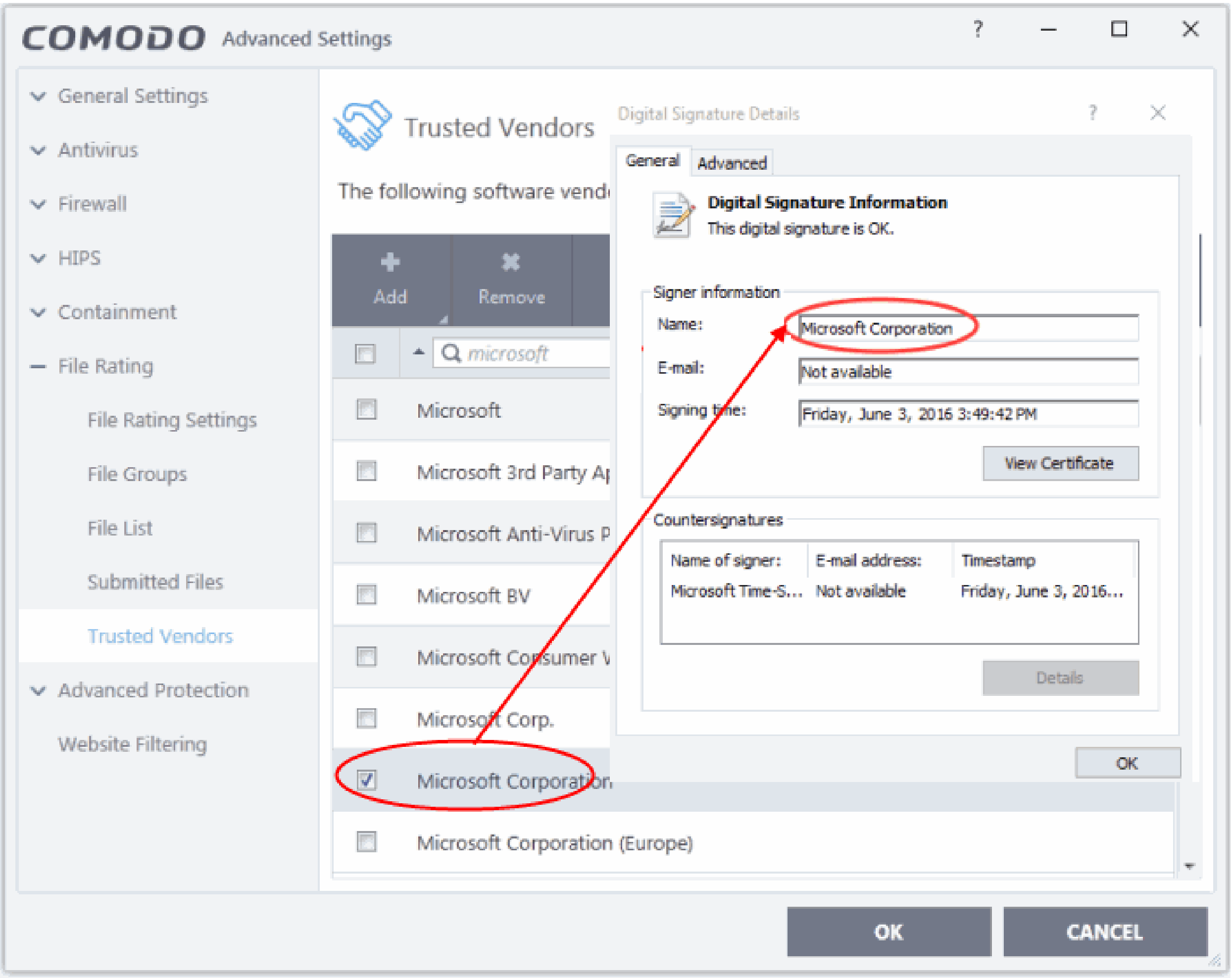
To add a trusted vendor by reading the vendor's signature from an executable

- Click the 'Add' button at the top and select 'Read from a signed executable'


Add
Remove
Read from a Signed Executable
Read from a Running Process
Code Signing Certificate)
Beijing Huahong Integrated Circuit Design Co.,LTD

- Browse to the location of the executable your local drive. In the example below, we are adding the executable 'Microsoft Corporation.exe'.

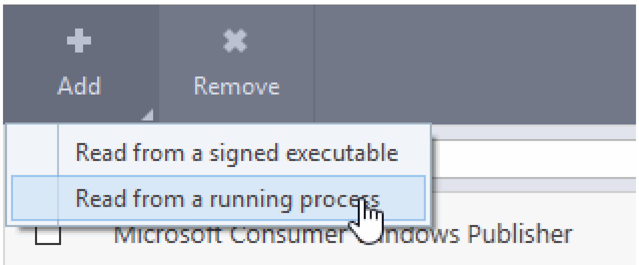
On clicking 'Open', Comodo Internet Security checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the Trusted Vendor list (TVL):



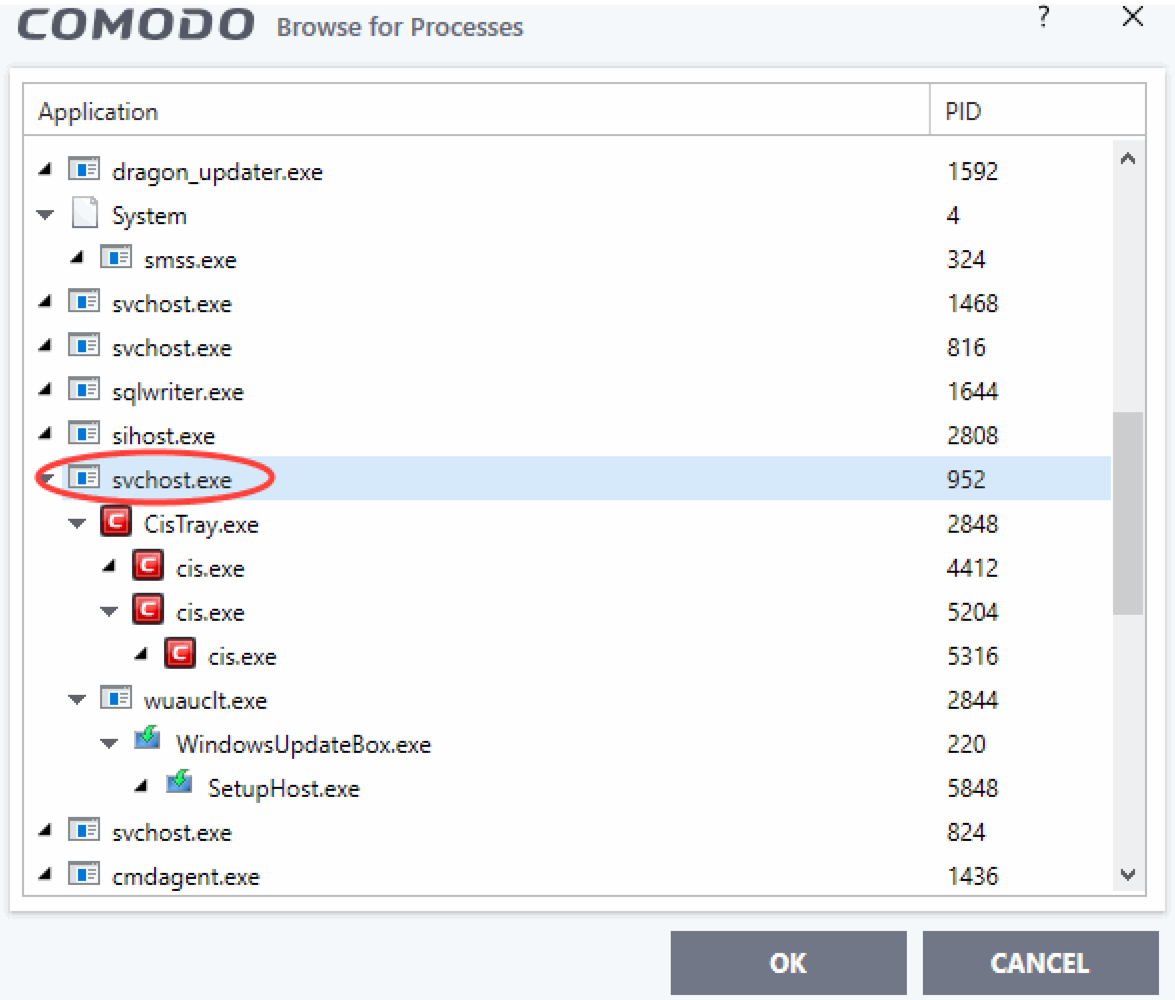
In the example above, Comodo Internet Security was able to verify and trust the vendor signature on ViberSetup.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Viber Media S.à r.l..' is now a 'Trusted Software Vendor' and is added to the list. All future software that is signed by the vendor 'Viber Media S.à r.l..' is automatically added to the Comodo Trusted Vendor list UNLESS you change **this setting in File Rating Settings**.

To add a trusted vendor from a currently running process

- Click the 'Add' button at the top and select 'Read from a running process'


Add
Remove
Read from a signed executable
Read from a running process
Microsoft Consumer Windows Publisher

- Select the signed executable that you want to trust and click the 'OK' button.

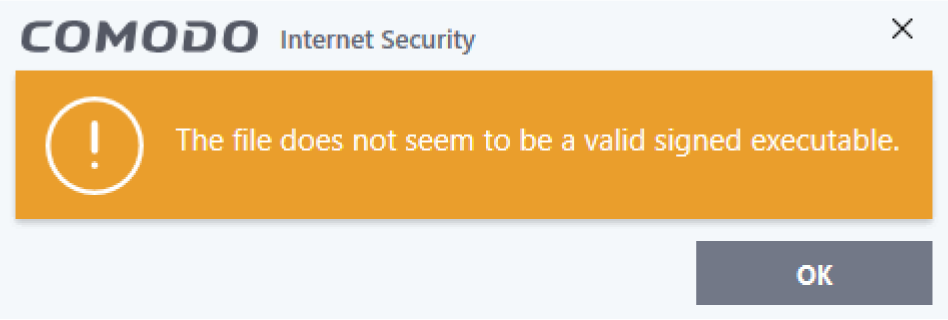


Application	PID
dragon_updater.exe	1592
System	4
smss.exe	324
svchost.exe	1468
svchost.exe	816
sqlwriter.exe	1644
sihost.exe	2808
svchost.exe	952
CisTray.exe	2848
cis.exe	4412
cis.exe	5204
cis.exe	5316
wuauclt.exe	2844
WindowsUpdateBox.exe	220
SetupHost.exe	5848
svchost.exe	824
cmdagent.exe	1436

Comodo Internet Security performs the same certificate check as described above. If the parent application of the selected process is signed, CIS adds the vendor to the Trusted Software Vendors list.

If Comodo Internet Security 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'. In this case, you can see the following error message.

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



COMODO Internet Security

The file does not seem to be a valid signed executable.

- User defined trusted software vendors - As the name suggests, these are added by the user via one of the two methods 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 Internet Security. 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, CIS 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 CIS.

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

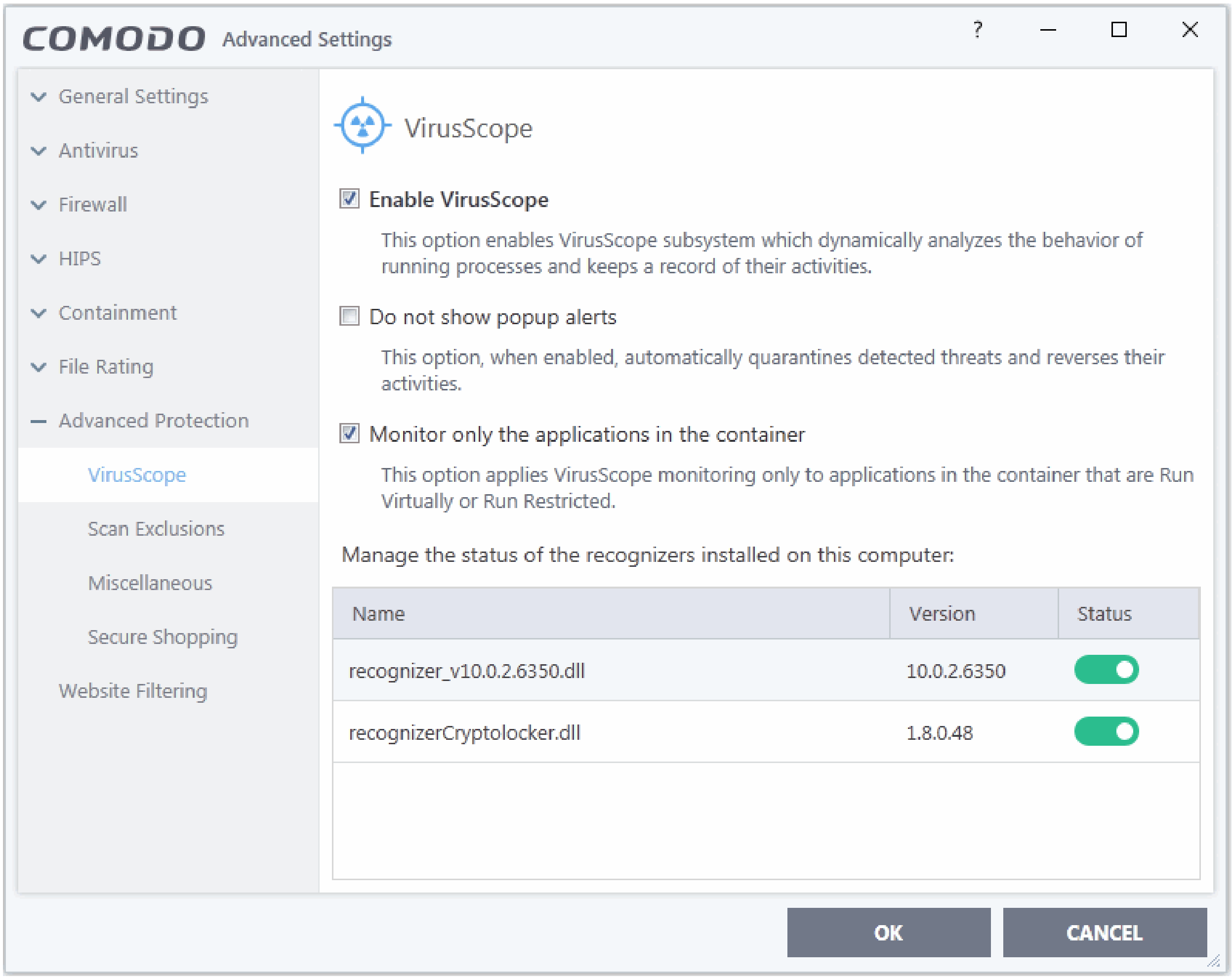
6.7. Advanced Protection Configuration

The 'Advanced Protection' section allows you to:

- Configure VirusScope and Secure Shopping components
- Specify items you wish to exclude from detection during a scan
- Configure miscellaneous other settings.

To open the 'Advanced Protection' area

- Click 'Settings' on the CIS home screen to open the 'Advanced Settings' interface
- Click 'Advanced Protection' on the left:



☑ Enable VirusScope

This option enables VirusScope subsystem which dynamically analyzes the behavior of running processes and keeps a record of their activities.

□ Do not show popup alerts

This option, when enabled, automatically quarantines detected threats and reverses their activities.

☑ Monitor only the applications in the container

This option applies VirusScope monitoring only to applications in the container that are Run Virtually or Run Restricted.

Manage the status of the recognizers installed on this computer:

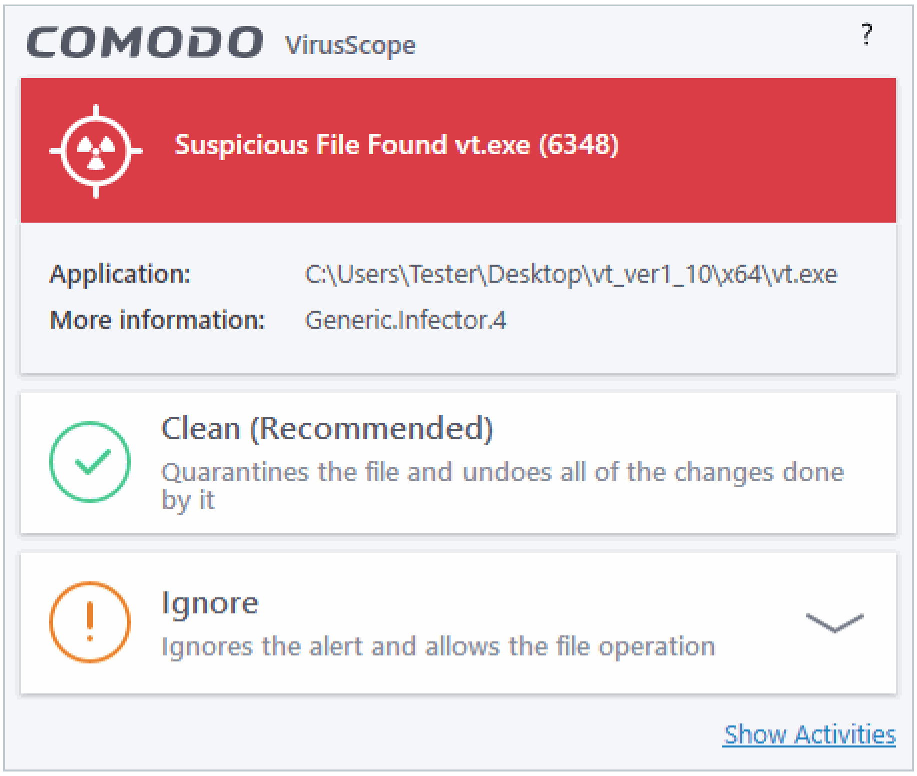
Name	Version	Status
recognizer_v10.0.2.6350.dll	10.0.2.6350	●
recognizerCryptolocker.dll	1.8.0.48	●

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

- **VirusScope Settings** - Configure VirusScope behavior
- **Scan Exclusions** - Add and manage items that are ignored during a scan
- **Miscellaneous Settings** - View and configure analysis of executed code, monitor file types against buffer overflows and set alerts when programs try to modify your browser settings
- **Secure Shopping Settings** - Create a secure place to work and go online

6.7.1. VirusScope Settings

- VirusScope 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.
- VirusScope improves the core process-monitoring functionality of CIS by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely.
  This provides more flexibility over legitimate software which requires certain actions to be implemented in order to run correctly.
- VirusScope alerts give you the opportunity to quarantine the process & reverse its changes, or to let the process go ahead.
- Be especially wary if a VirusScope alert appears 'out-of-the-blue' when you have not made any recent changes to your computer.



COMODO VirusScope

Suspicious File Found vt.exe (6348)

Application: C:\Users\Tester\Desktop\vt_ver1_10\x64\vt.exe

More information: Generic.Infector.4

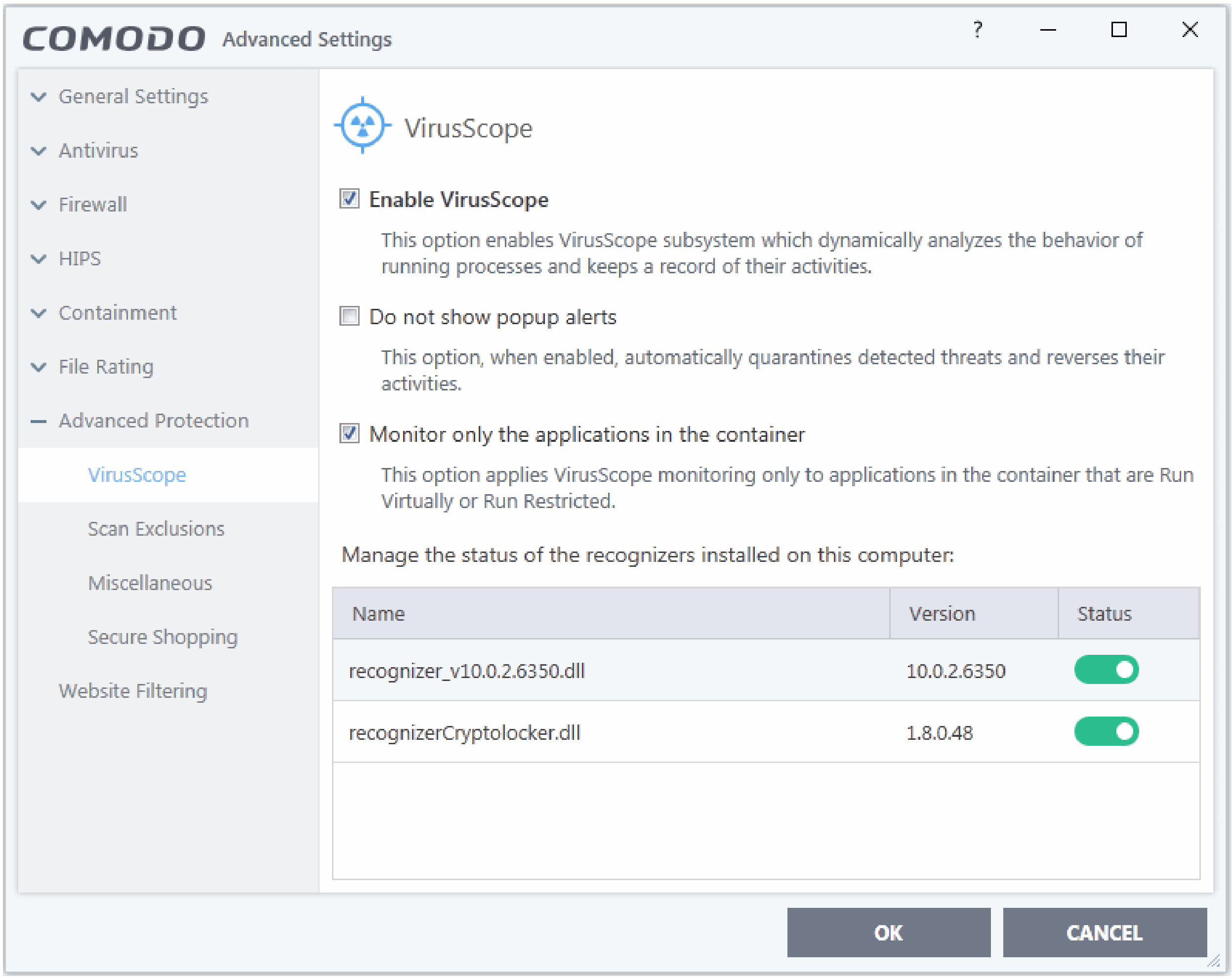
Clean (Recommended)
Quarantines the file and undoes all of the changes done by it

Ignore
Ignores the alert and allows the file operation

Show Activities

To open the 'VirusScope' settings section:

- Click 'Settings' at the top left of the CIS home screen
- Click 'Advanced Protection' > 'VirusScope':



VirusScope

☑ Enable VirusScope

This option enables VirusScope subsystem which dynamically analyzes the behavior of running processes and keeps a record of their activities.

□ Do not show popup alerts

This option, when enabled, automatically quarantines detected threats and reverses their activities.

☑ Monitor only the applications in the container

This option applies VirusScope monitoring only to applications in the container that are Run Virtually or Run Restricted.

Manage the status of the recognizers installed on this computer:

Name	Version	Status
recognizer_v10.0.2.6350.dll	10.0.2.6350	●
recognizerCryptolocker.dll	1.8.0.48	●

VirusScope Settings

VirusScope is capable of monitoring all running processes and, if suspicious activity is detected, can generate alerts that let you quarantine the application and undo its activities.

- **Enable VirusScope -** Enable or disable VirusScope. If enabled, VirusScope monitors the activities of running processes and generates alerts if suspicious activity is detected. ***(Default = Enabled)***
- **Do not show pop-up alerts -** Configure whether or not CIS should show an alert if VirusScope detects a suspicious activity. Choosing 'Do not show pop-up alerts' 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)***
- **Monitor only the applications in the container -** If enabled, VirusScope will only monitor and generate alerts for processes running in the container. ***(Default = Enabled)***

Manage the status of recognizers

- VirusScope detects zero-day malware by analyzing the behavior and actions of an application.
- If the detected behavior corresponds to that of known malware, then VirusScope will generate an alert which allows you to quarantine the application and reverse any changes that it made.
- A 'recognizer' file contains the sets of behaviors that VirusScope needs to look out for.
- If you disable a recognizer, VirusScope will no longer show an alert if an application exhibits behavior described by the recognizer.
- We recommend most users to leave the 'Status' of recognizers at their default settings.
- Advanced users, however, may want to try disabling recognizers if they are experiencing a large number of

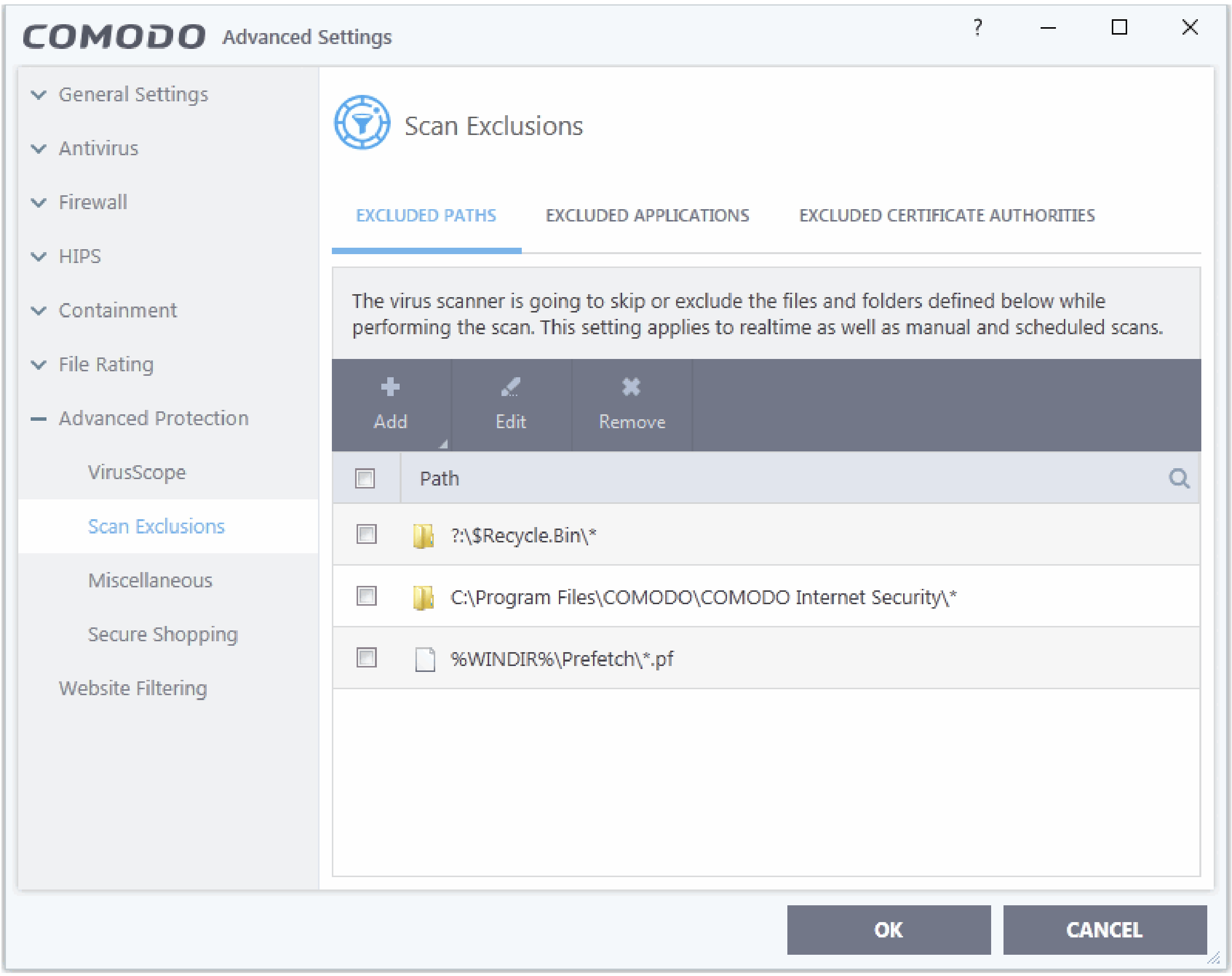
VirusScope false positives.

6.7.2. Scan Exclusions

- The 'Scan Exclusions' panel shows files, paths and certificate authorities which you have chosen to skip during a scan.
- Items may have been added to this because you selected '**Ignore**' at the window, or have added them as exclusion at an alert.
- The 'Exclusions' panel shows paths and files which you have chosen to '**Ignore**' at the '**Scan Results**' window, or have added as an exclusion at an antivirus alert.

To open the 'Scan Exclusions' panel

- Click 'Settings' at the top of the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions' on the left



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	%WINDIR%\Prefetch\*.pf

The 'Scan Exclusions' panel has three tabs:

- **Excluded Paths** -A list of paths/folders/files on your computer which are not included in real-time, on-demand and scheduled antivirus scans. See '**Excluding Drives/Folders/Files from all types of scans**' for more details.
- **Excluded Applications** - A list of applications which are not included in real-time antivirus scans. Items can be excluded by clicking 'Ignore' in the virus '**Scan Results**' or by clicking 'Ignore' at an '**Antivirus' Alert** or by excluding it manually. Note - excluded items are skipped by the real-time scanner but will be scanned during on-demand scans. See '**Excluding Programs/Applications from real-time scans**' for more details on manually adding and removing exclusions.

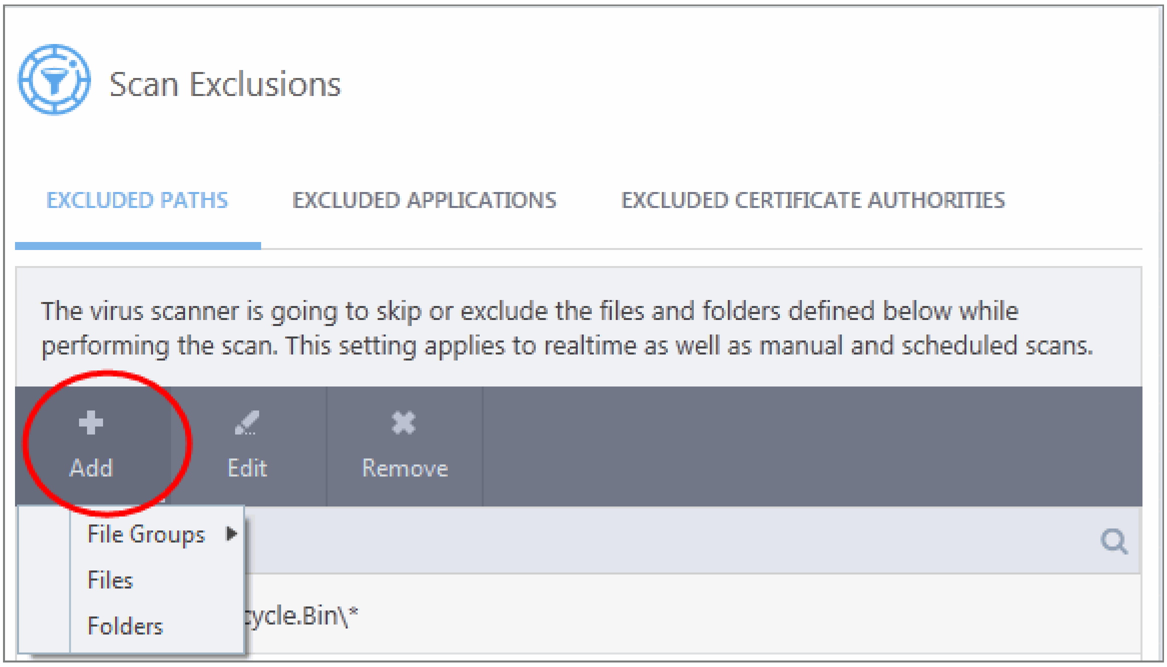
- **Excluded Certificate Authorities -** Displays a list of certificate authorities which will not be included in certificate scans. See '**Excluding Certificate Authorities from certificate scans**' for more details.

Excluding Drives/Folders/Files from all types of scans

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

To add item(s) to excluded paths

- Click 'Add' at the top, under the 'Excluded Paths' tab



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

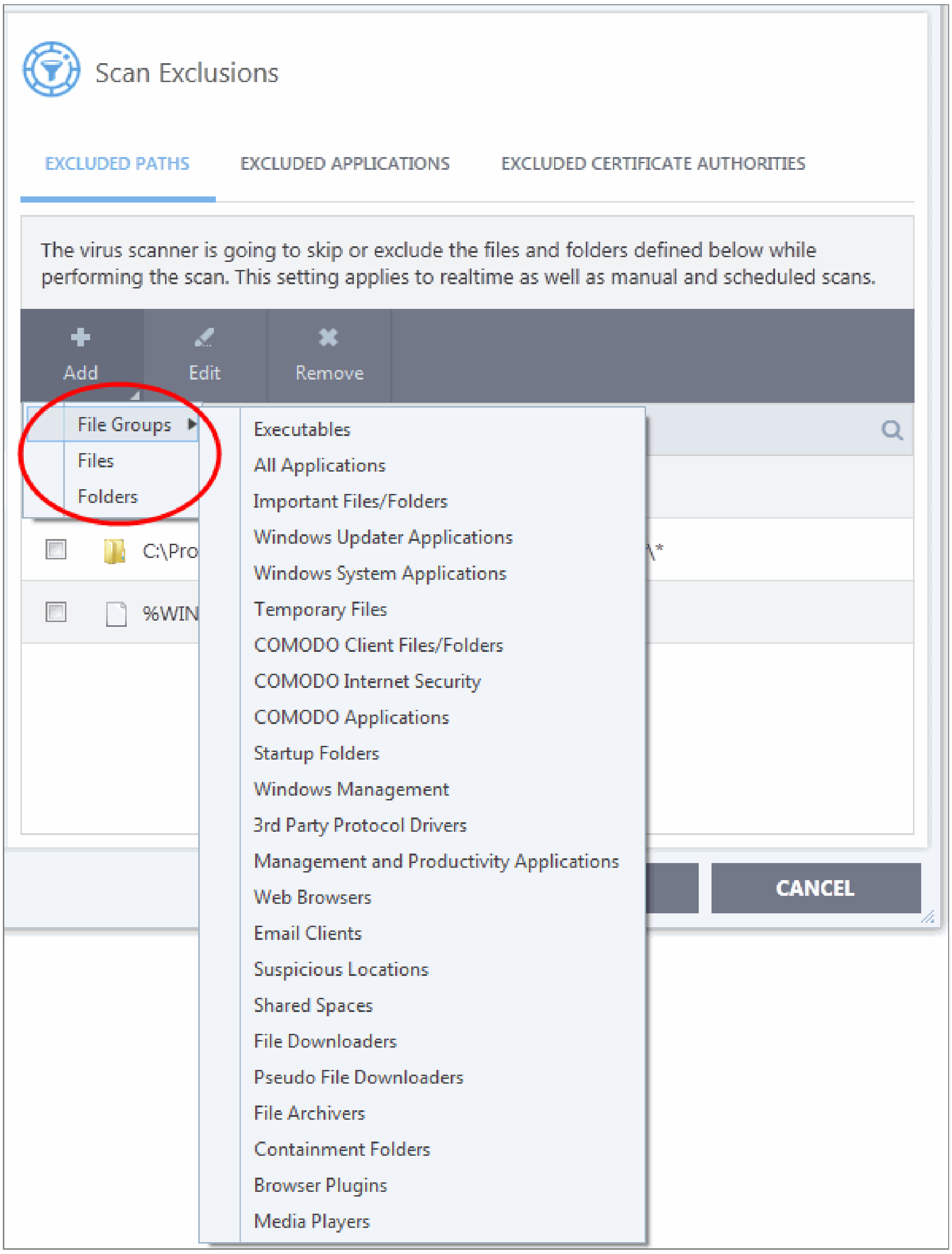
You can add a:

- **File Group**
- **Drive partition/Folder**

  OR
- **An individual file**

Adding a File Group

- Choosing 'File Groups' allows you to exclude a pre-set category of files or folders. This provides a convenient way to apply a generic ruleset to important files and folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl *\cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications' and 'Start Up Folders'.

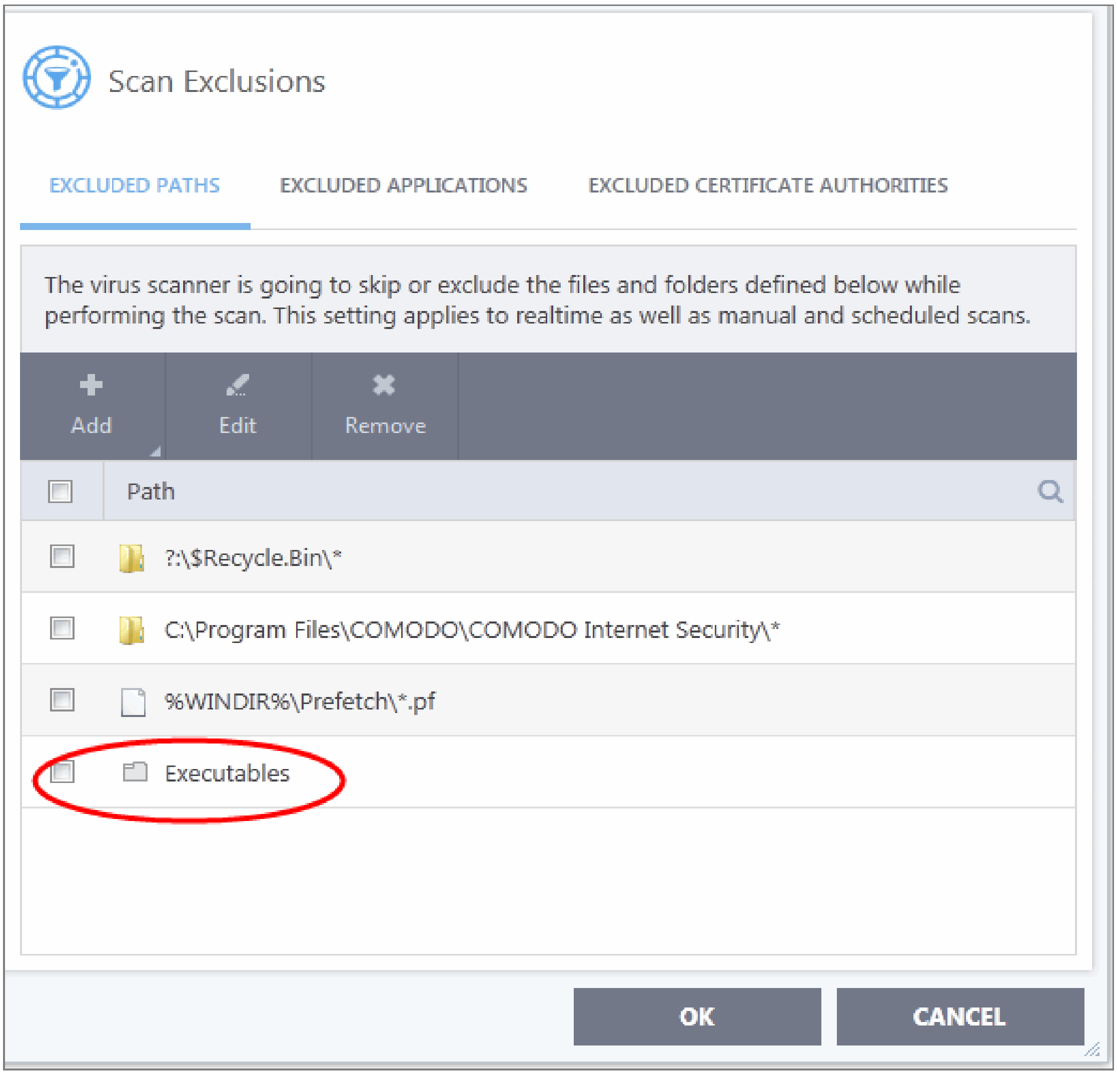


The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

CIS ships with a set of predefined file groups which can be viewed in Advanced Settings > File Rating > '**File Groups**'. You can also add new file groups here which will be displayed in the predefined list.

To add new file groups:

- Click 'Add' > 'File Groups' and select the type of 'File Group' from the list:



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

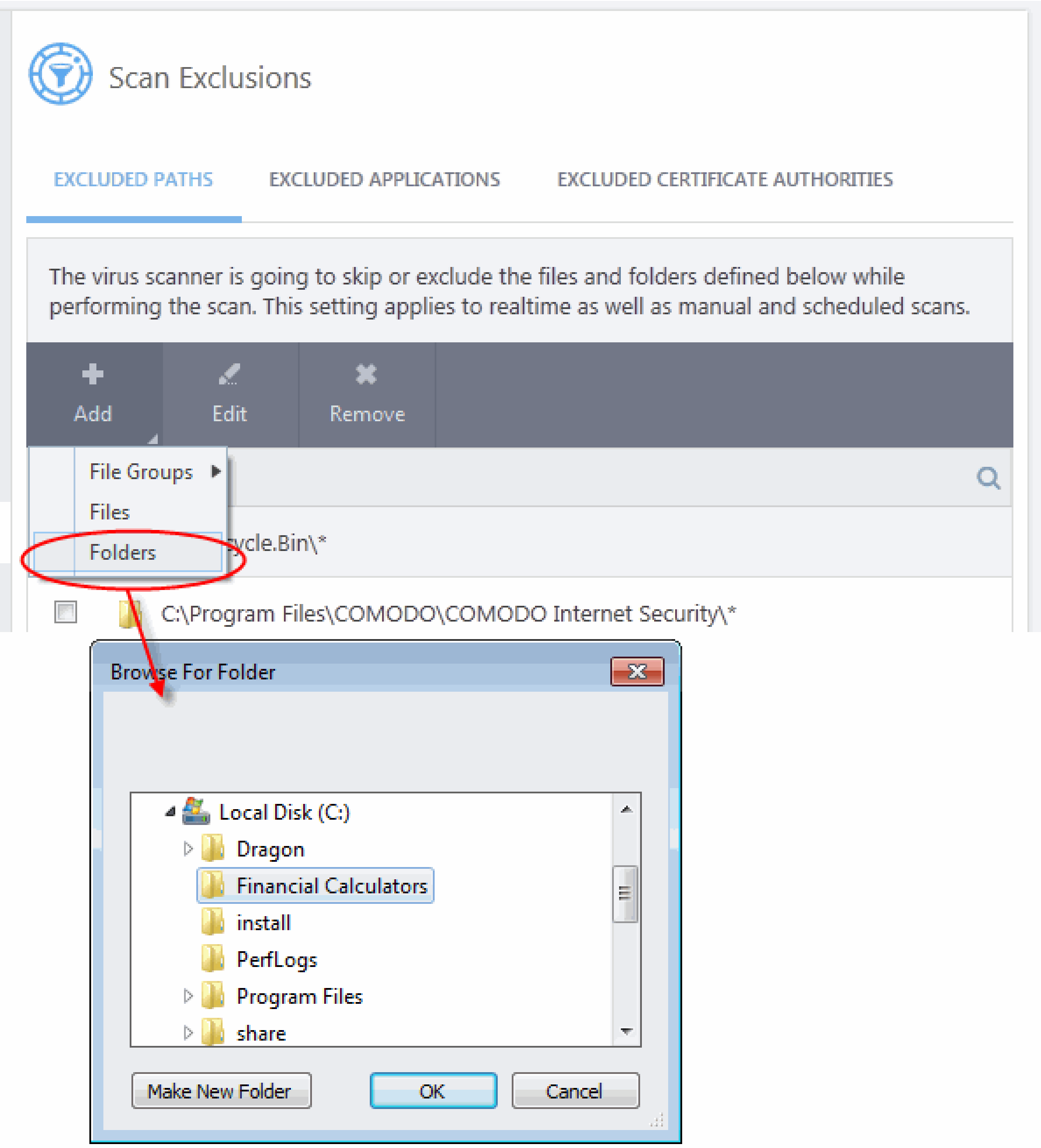
□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	%WINDIR%\Prefetch\*.pf
□	Executables

The file groups will be added to 'Excluded Paths'.

- Repeat the process to add more file groups. Items added to the 'Excluded Paths' will be omitted from all types of future Antivirus scans.

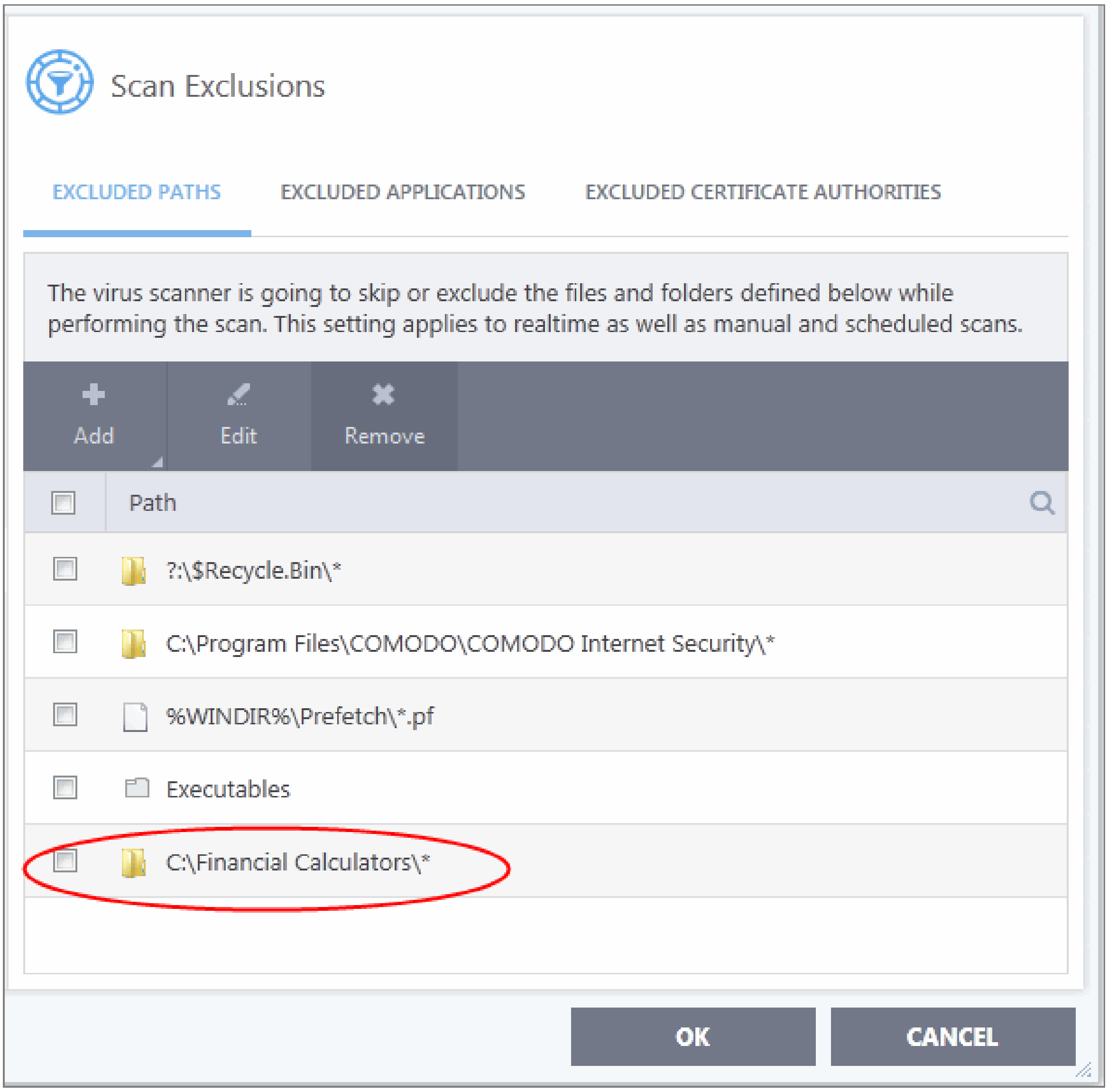
Adding a Drive Partition/Folder

- Click 'Settings' on the CIS home screen
- Click 'Antivirus' > 'Scan Exclusions'
- Select 'Excluded Paths'
- Click 'Add' > 'Folders'
- Navigate to the drive partition or folder you want to add to excluded paths and click 'OK'.



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

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



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

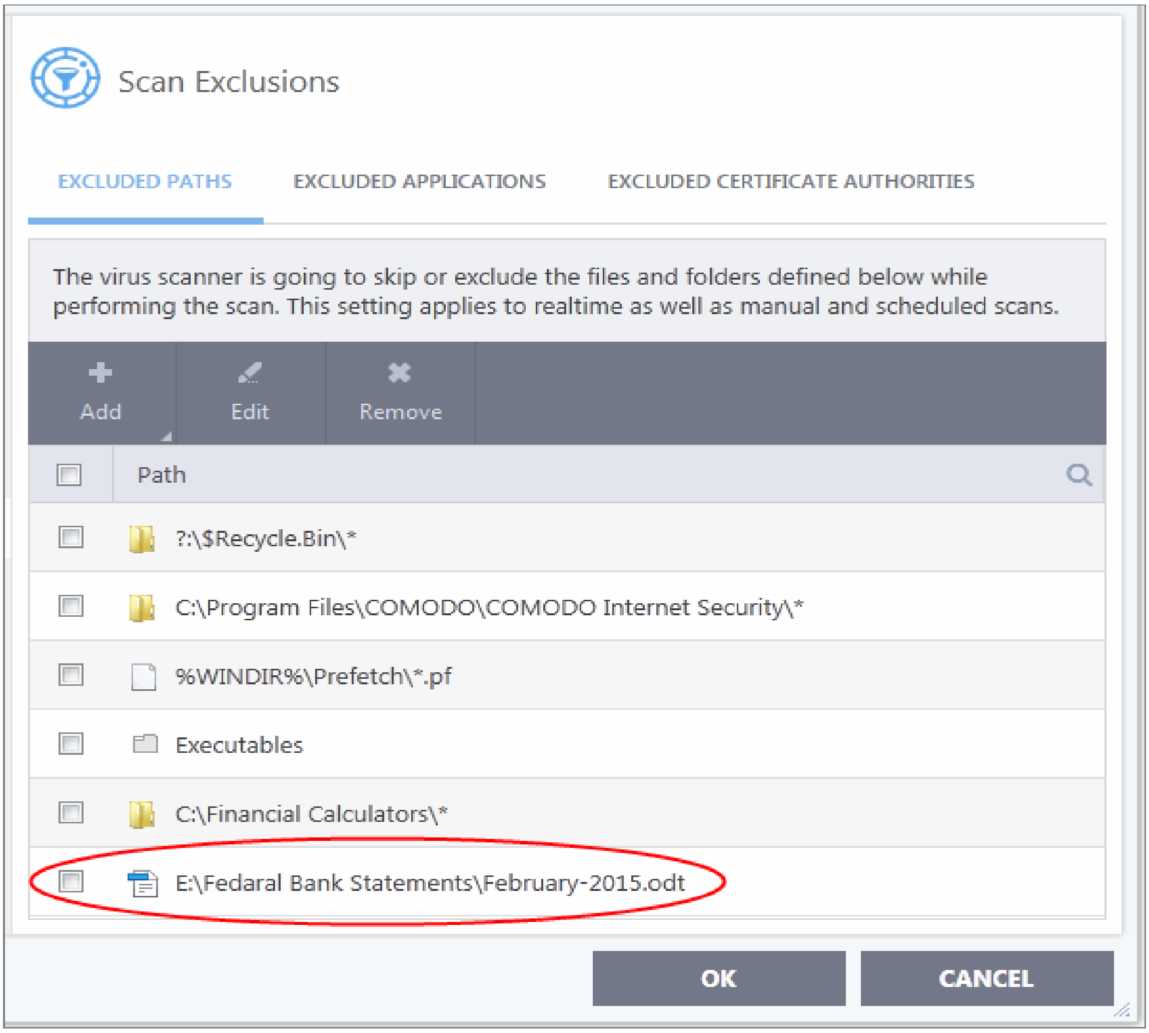
□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	%WINDIR%\Prefetch\*.pf
□	Executables
□	C:\Financial Calculators*

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

Adding an individual File

You can specify even individual files as excluded path.

- Click 'Settings' on the CIS home screen
- Click 'Antivirus' > 'Scan Exclusions'
- Select 'Excluded Paths'
- Click 'Add' > 'Files'
- Navigate to the file you want to add to excluded paths and click 'OK'.
- The file will be added to excluded paths:



Scan Exclusions

EXCLUDED PATHS | EXCLUDED APPLICATIONS | EXCLUDED CERTIFICATE AUTHORITIES

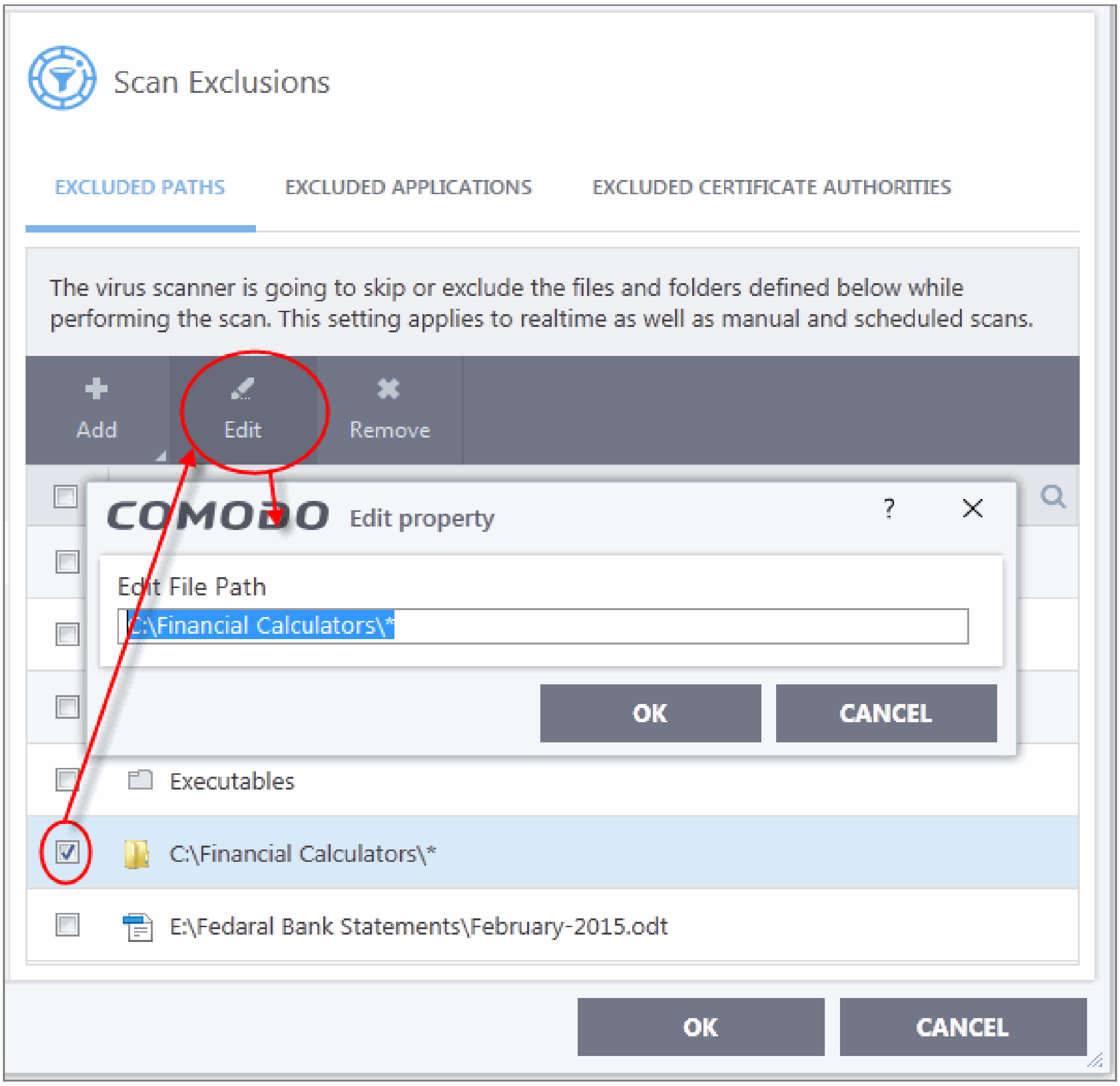
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	%WINDIR%\Prefetch\*.pf
□	Executables
□	C:\Financial Calculators*
□	E:\Fedaral Bank Statements\February-2015.odt

- Repeat the process to add more paths.
- Items added to 'Excluded Paths' will be omitted from all types of virus scan in the future.

To edit the path of an added item

- Select the target item and click 'Edit':



Scan Exclusions

The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

COMODO Edit property

Edit File Path

C:\Financial Calculators*

□ Executables

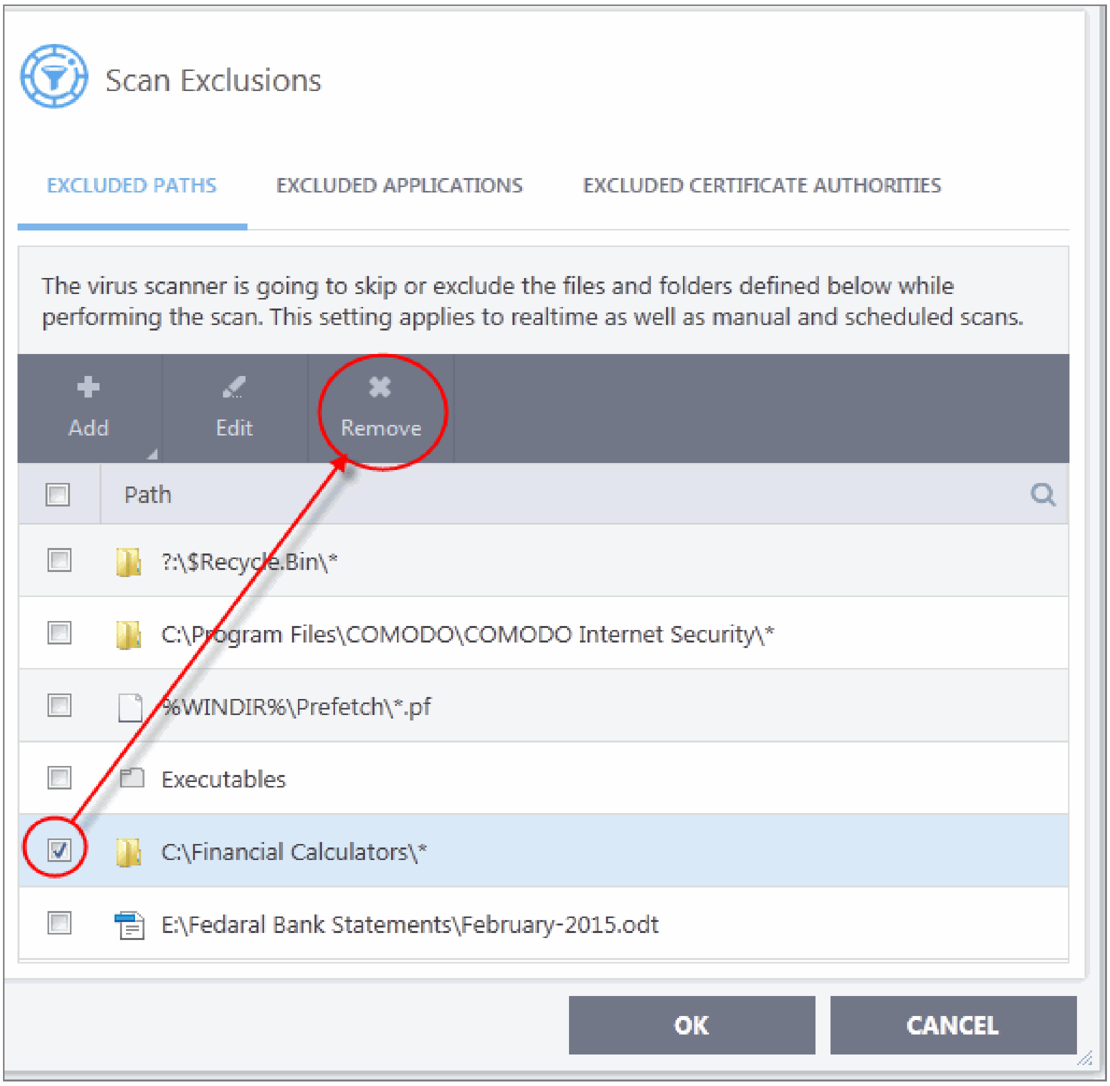
☑ C:\Financial Calculators*

□ E:\Fedaral Bank Statements\February-2015.odt

- Modify the file-path as required and click 'OK'.

To remove an item from Excluded Paths

- Select the target item and click 'Remove':



Scan Exclusions

EXCLUDED PATHS | EXCLUDED APPLICATIONS | EXCLUDED CERTIFICATE AUTHORITIES

The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	%WINDIR%\Prefetch\*.pf
□	Executables
☑	C:\Financial Calculators*
□	E:\Fedaral Bank Statements\February-2015.odt

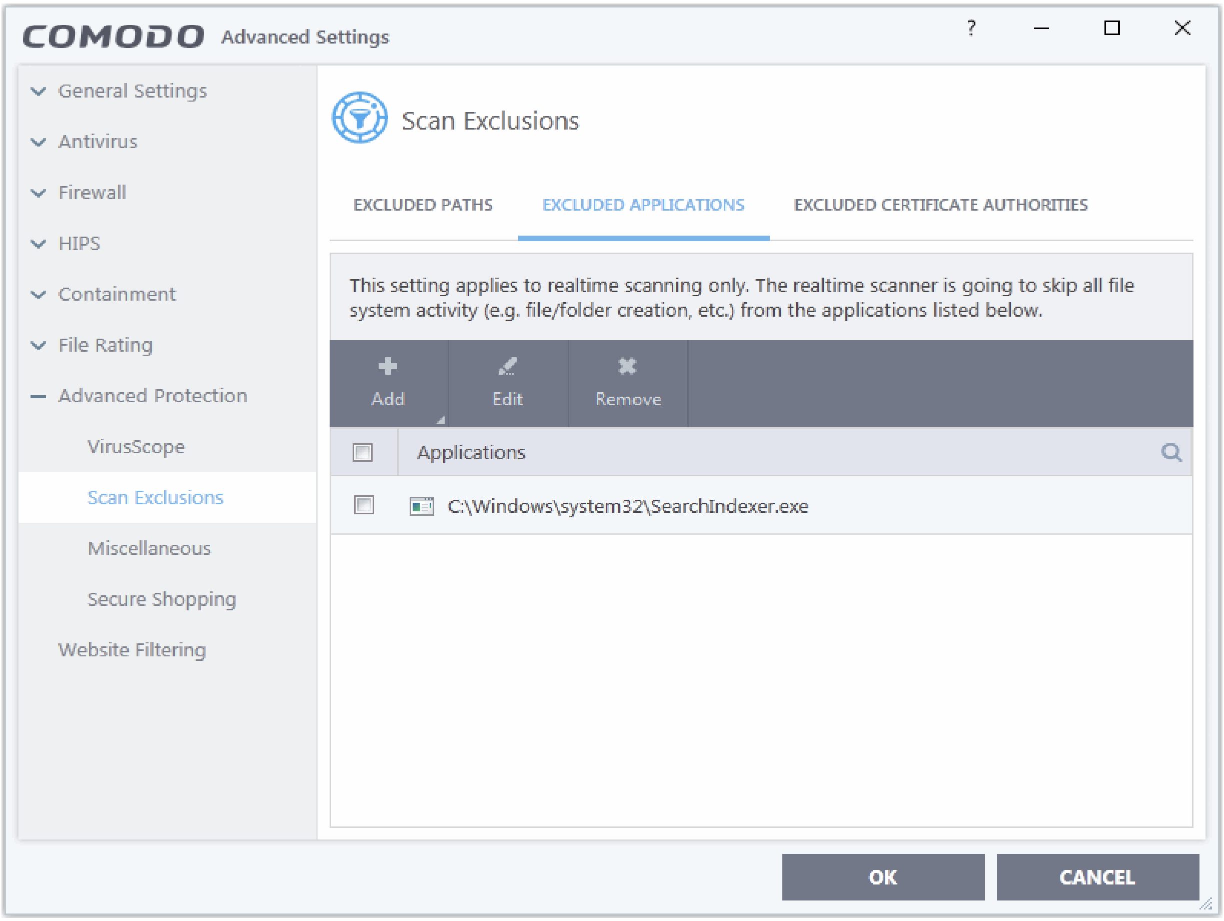
- Click 'OK' for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

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

To open 'Excluded Applications':

- Click 'Settings' on the CIS home screen
- Click 'Antivirus' > 'Scan Exclusions'
- Select the 'Excluded Applications' tab:

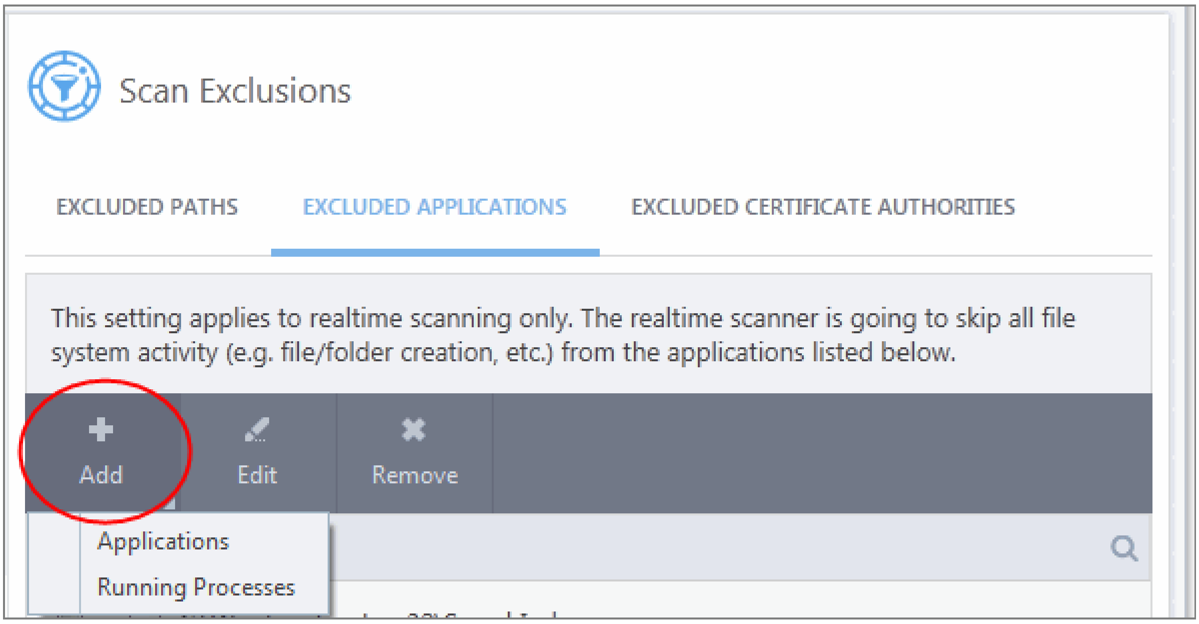


This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

C:\Windows\system32\SearchIndexer.exe

To add an item to Excluded Applications

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



This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

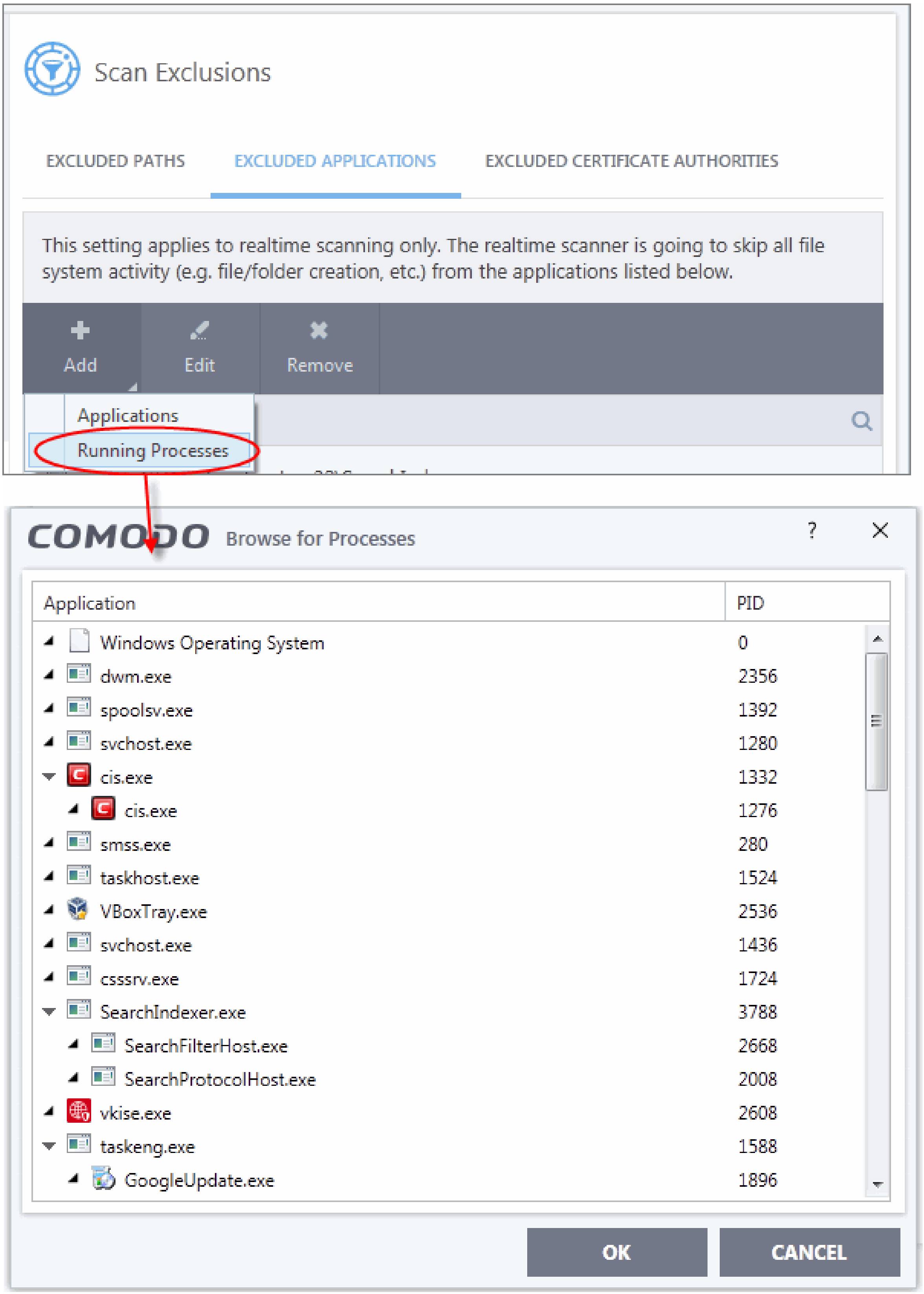
You can choose to add an applications by:

- **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 your computer for the application** - This option is the easiest for most users and simply allows

you to browse to the files which you want to exclude.

Adding an application from a running processes

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



Scan Exclusions

This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

Application	PID
Windows Operating System	0
dwm.exe	2356
spoolsv.exe	1392
svchost.exe	1280
cis.exe	1332
cis.exe	1276
smss.exe	280
taskhost.exe	1524
VBoxTray.exe	2536
svchost.exe	1436
csssrv.exe	1724
SearchIndexer.exe	3788
SearchFilterHost.exe	2668
SearchProtocolHost.exe	2008
vkise.exe	2608
taskeng.exe	1588
GoogleUpdate.exe	1896

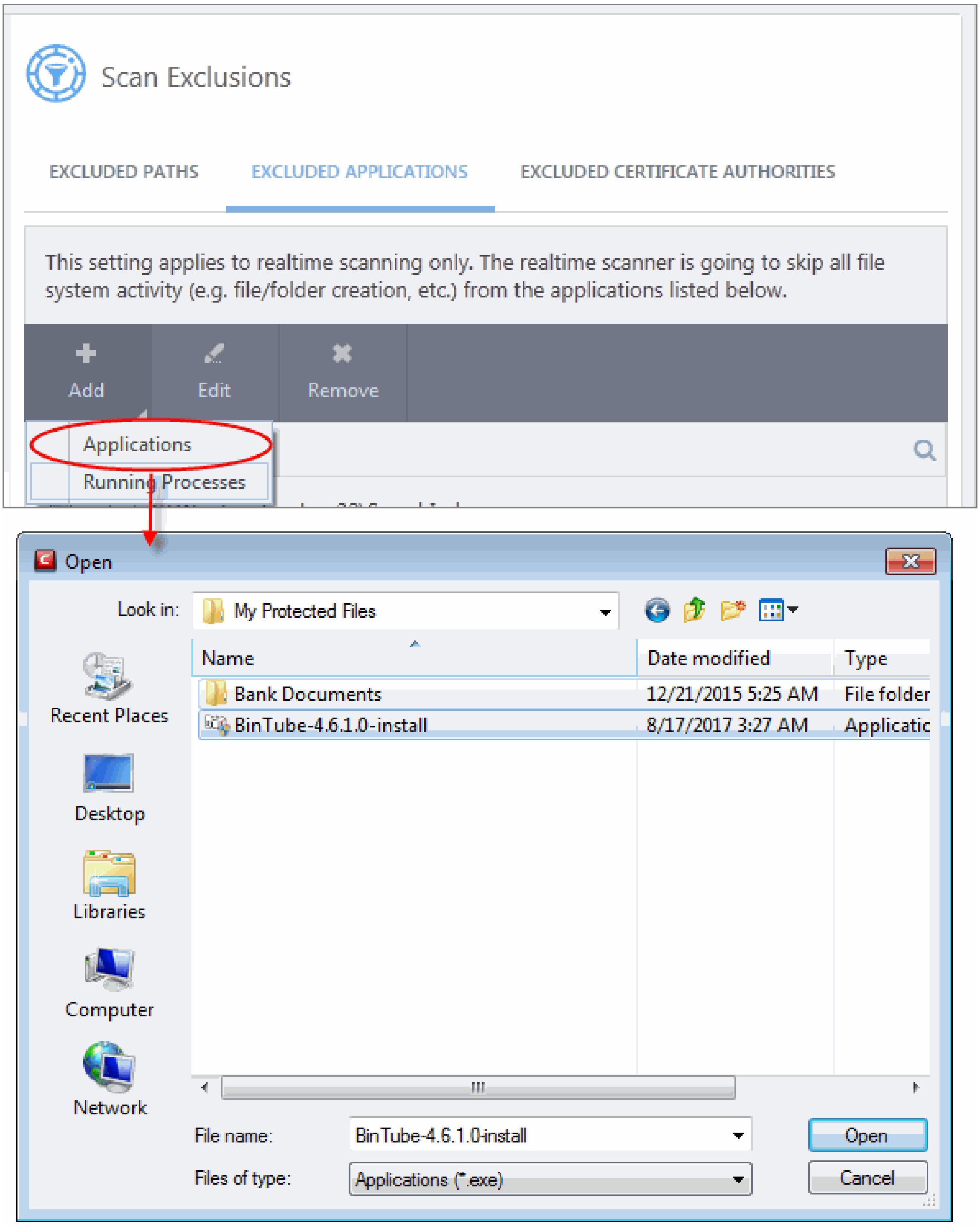
A list of currently running processes in your computer will be displayed:

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

The application will be added to 'Excluded Applications'.

Browsing to the Application

- Choose 'Applications' from the 'Add' drop-down



This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

Look in: My Protected Files

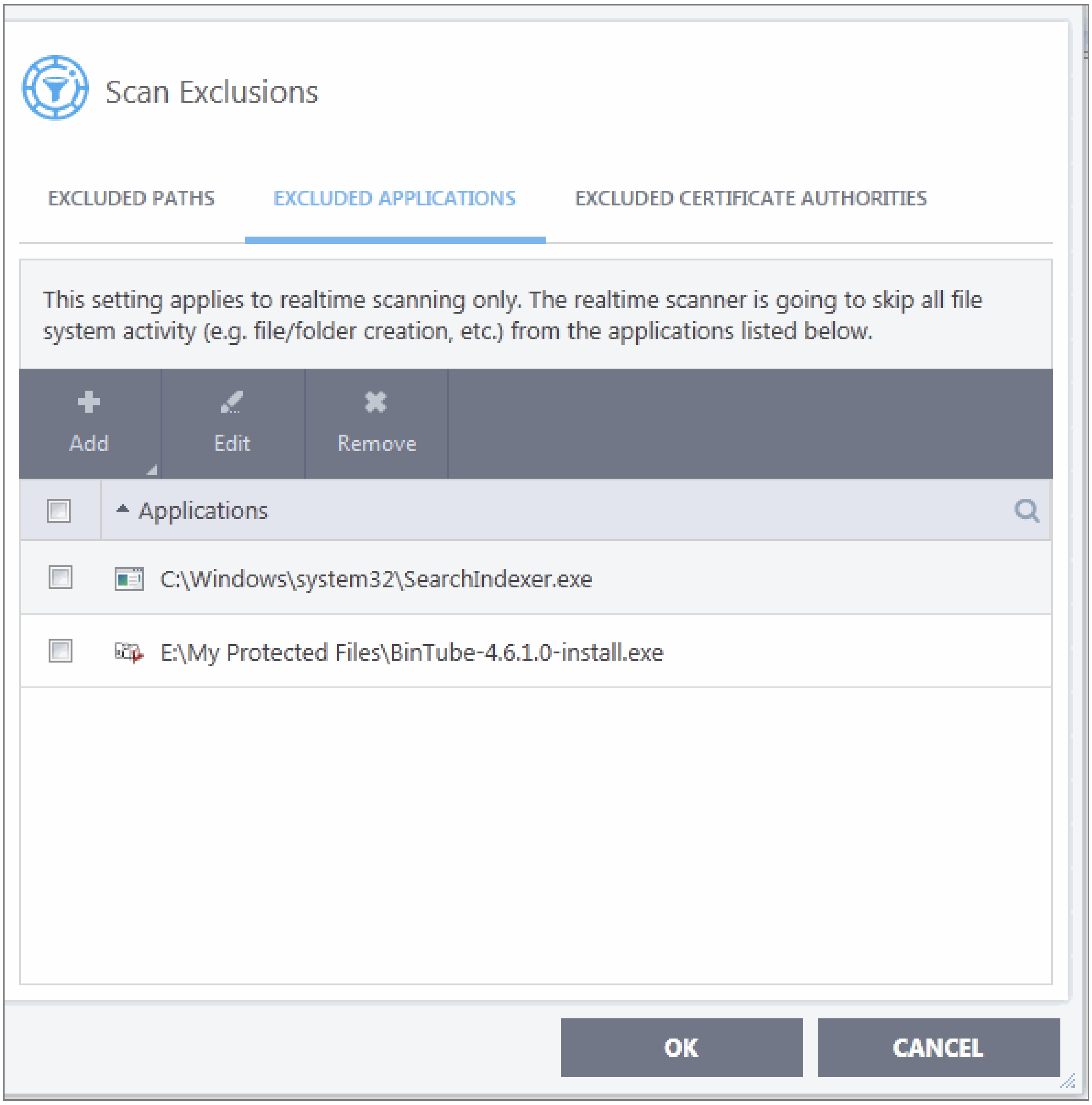
Name	Date modified	Type
Bank Documents	12/21/2015 5:25 AM	File folder
BinTube-4.6.1.0-install	8/17/2017 3:27 AM	Applicatic

File name: BinTube-4.6.1.0-install

Files of type: Applications (*.exe)

- Navigate to the file you want to exclude and click 'Open'.

The file will be added to 'Excluded Applications'.



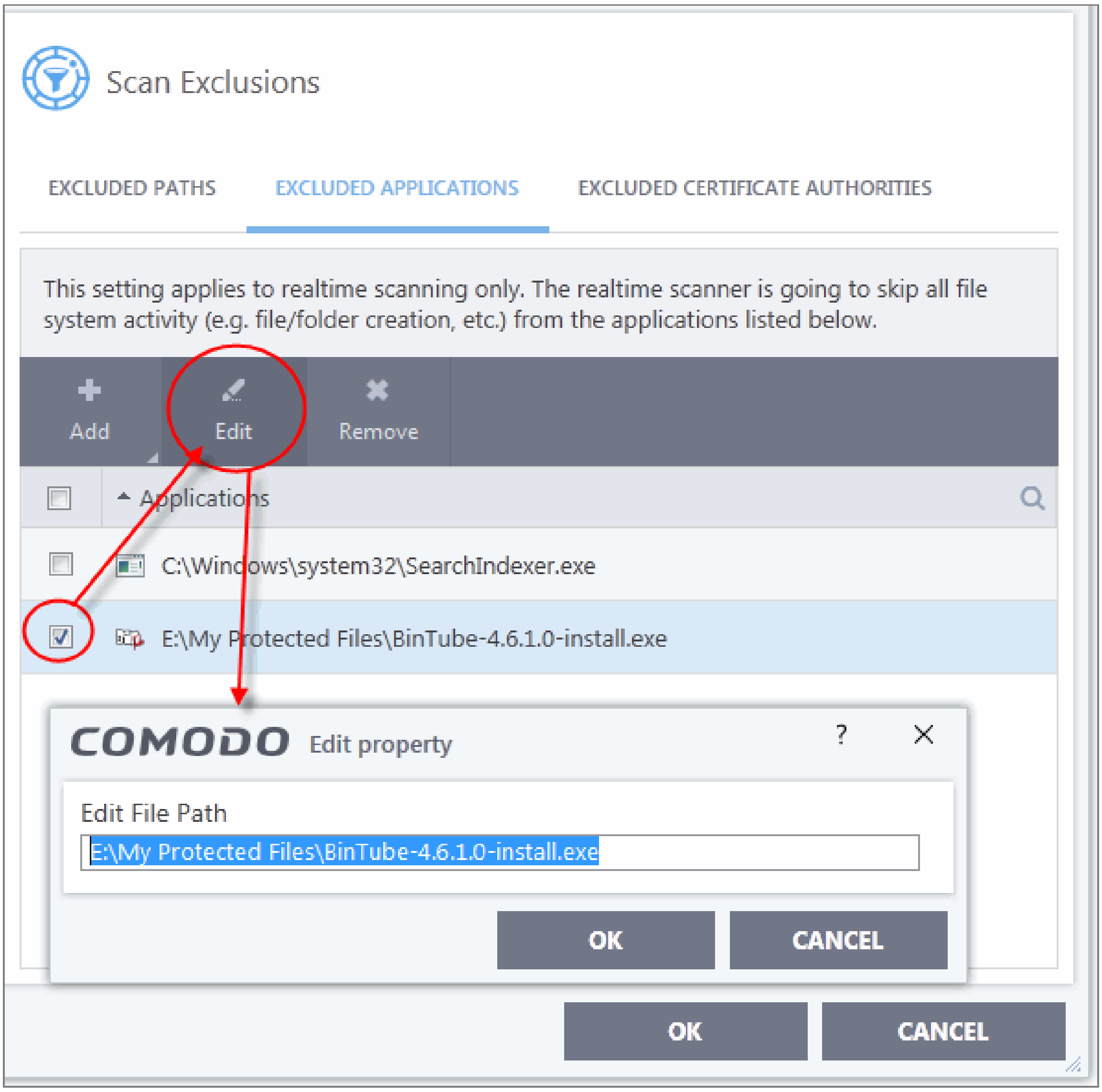
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

□	Applications
□	C:\Windows\system32\SearchIndexer.exe
□	E:\My Protected Files\BinTube-4.6.1.0-install.exe

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

To edit the path of the application added to Excluded Application

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



Scan Exclusions

EXCLUDED PATHS | EXCLUDED APPLICATIONS | EXCLUDED CERTIFICATE AUTHORITIES

This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

□ Applications

□ C:\Windows\system32\SearchIndexer.exe

☑ E:\My Protected Files\BinTube-4.6.1.0-install.exe

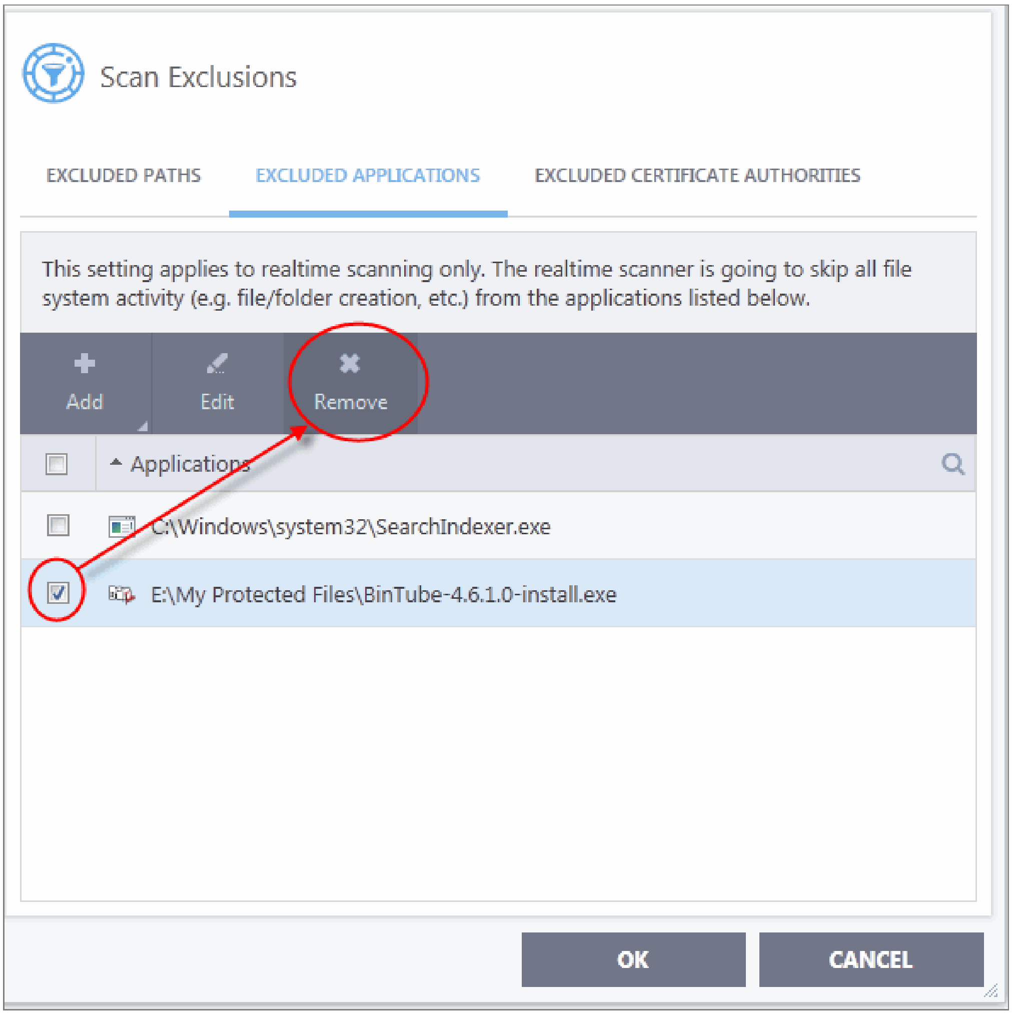
COMODO Edit property

Edit File Path

E:\My Protected Files\BinTube-4.6.1.0-install.exe

To remove an item from the Excluded Applications

- Select the item and click 'Remove' at the top:



Scan Exclusions

This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

	Applications
□	C:\Windows\system32\SearchIndexer.exe
☑	E:\My Protected Files\BinTube-4.6.1.0-install.exe

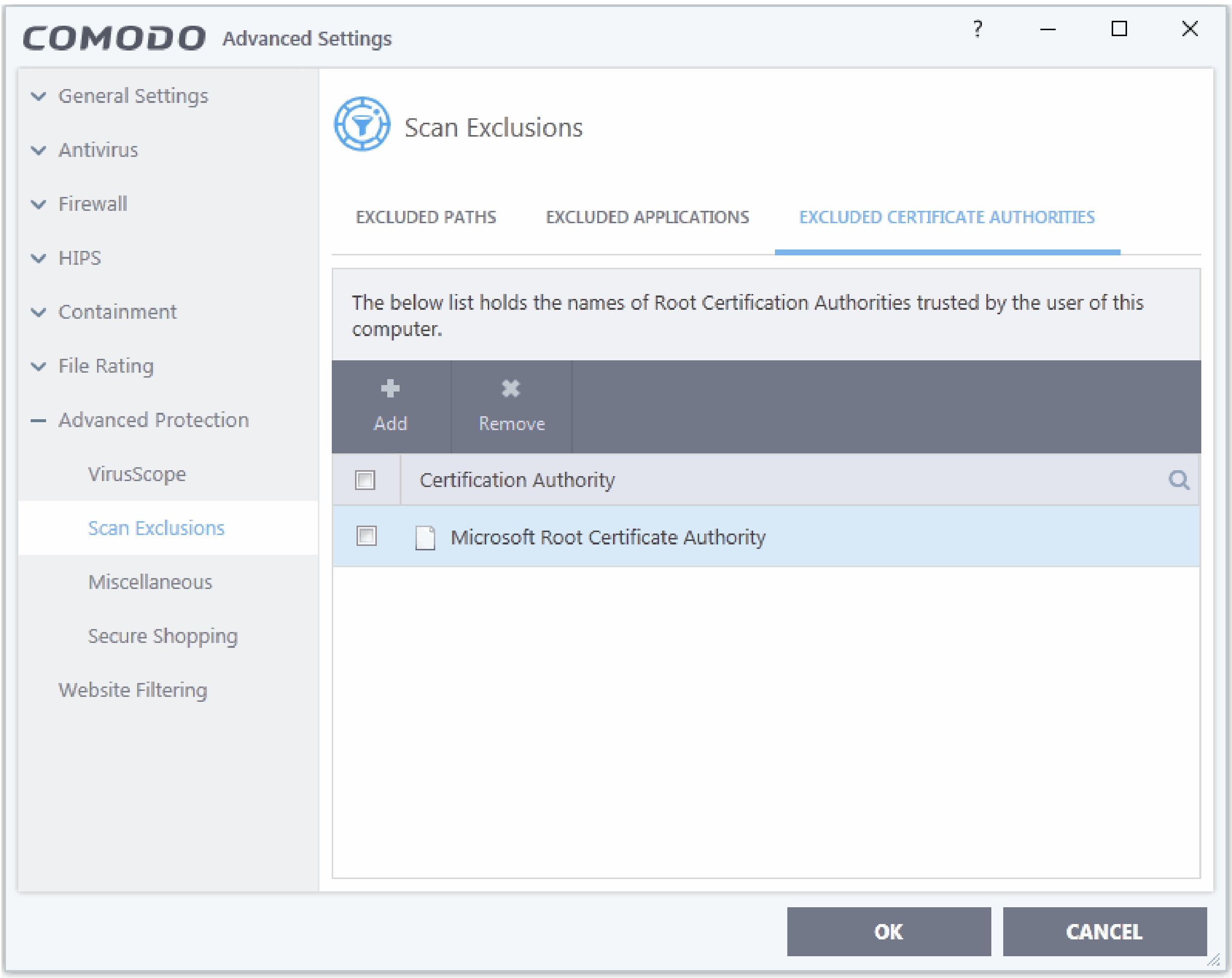
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Certificate Authorities from Certificate Scans

The 'Excluded Certificate Authorities' screen lets you exclude certificates from certificate scans.

To open 'Excluded Certificate Authorities':

- Click 'Settings' on the CIS home screen
- Click 'Antivirus' > 'Scan Exclusions'
- Select the 'Excluded Certificate Authorities' tab:

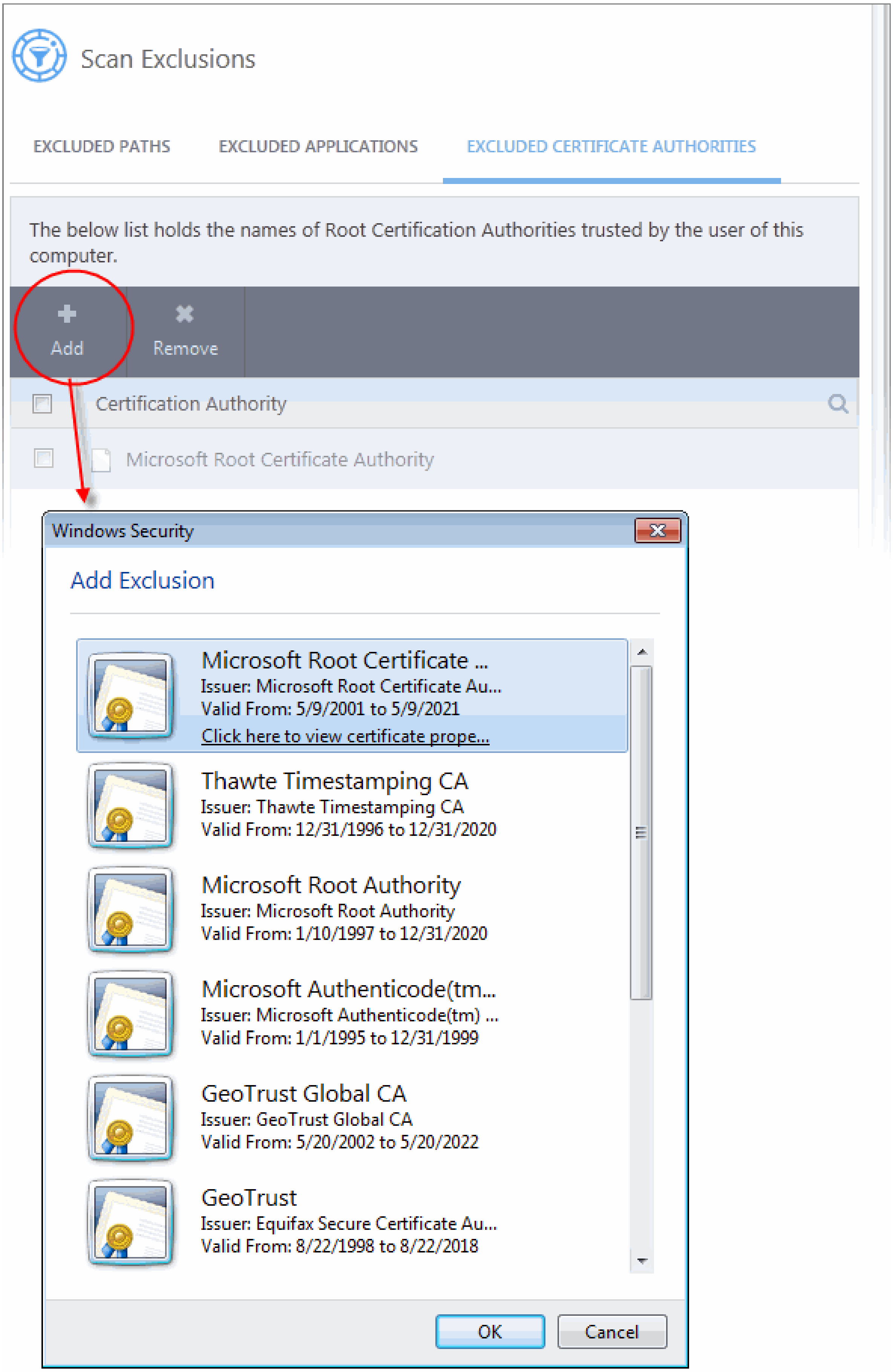


The below list holds the names of Root Certification Authorities trusted by the user of this computer.

□	Certification Authority
□	Microsoft Root Certificate Authority

To add an certificate to Excluded Certificate Authorities

- Click 'Add' at the top of the 'Excluded Certificate Authorities' pane.



The below list holds the names of Root Certification Authorities trusted by the user of this computer.

□ Microsoft Root Certificate Authority

Add Exclusion

Microsoft Root Certificate ...
Issuer: Microsoft Root Certificate Au...
Valid From: 5/9/2001 to 5/9/2021
Click here to view certificate prope...

Thawte Timestamping CA
Issuer: Thawte Timestamping CA
Valid From: 12/31/1996 to 12/31/2020

Microsoft Root Authority
Issuer: Microsoft Root Authority
Valid From: 1/10/1997 to 12/31/2020

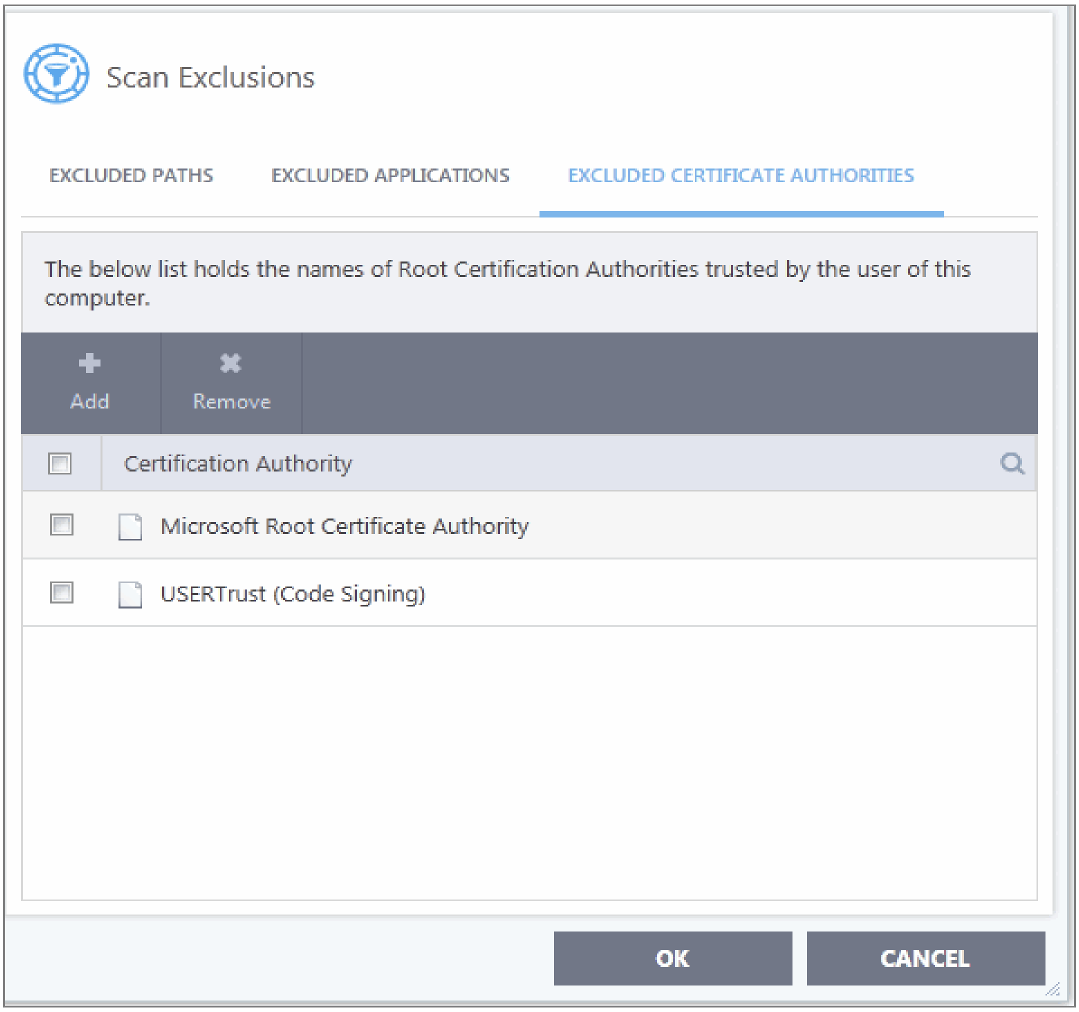
Microsoft Authenticode(tm...
Issuer: Microsoft Authenticode(tm) ...
Valid From: 1/1/1995 to 12/31/1999

GeoTrust Global CA
Issuer: GeoTrust Global CA
Valid From: 5/20/2002 to 5/20/2022

GeoTrust
Issuer: Equifax Secure Certificate Au...
Valid From: 8/22/1998 to 8/22/2018

- Select the certificate type to add excluded authorities and click 'OK'

- The certificate will be added to the list of excluded certificates:



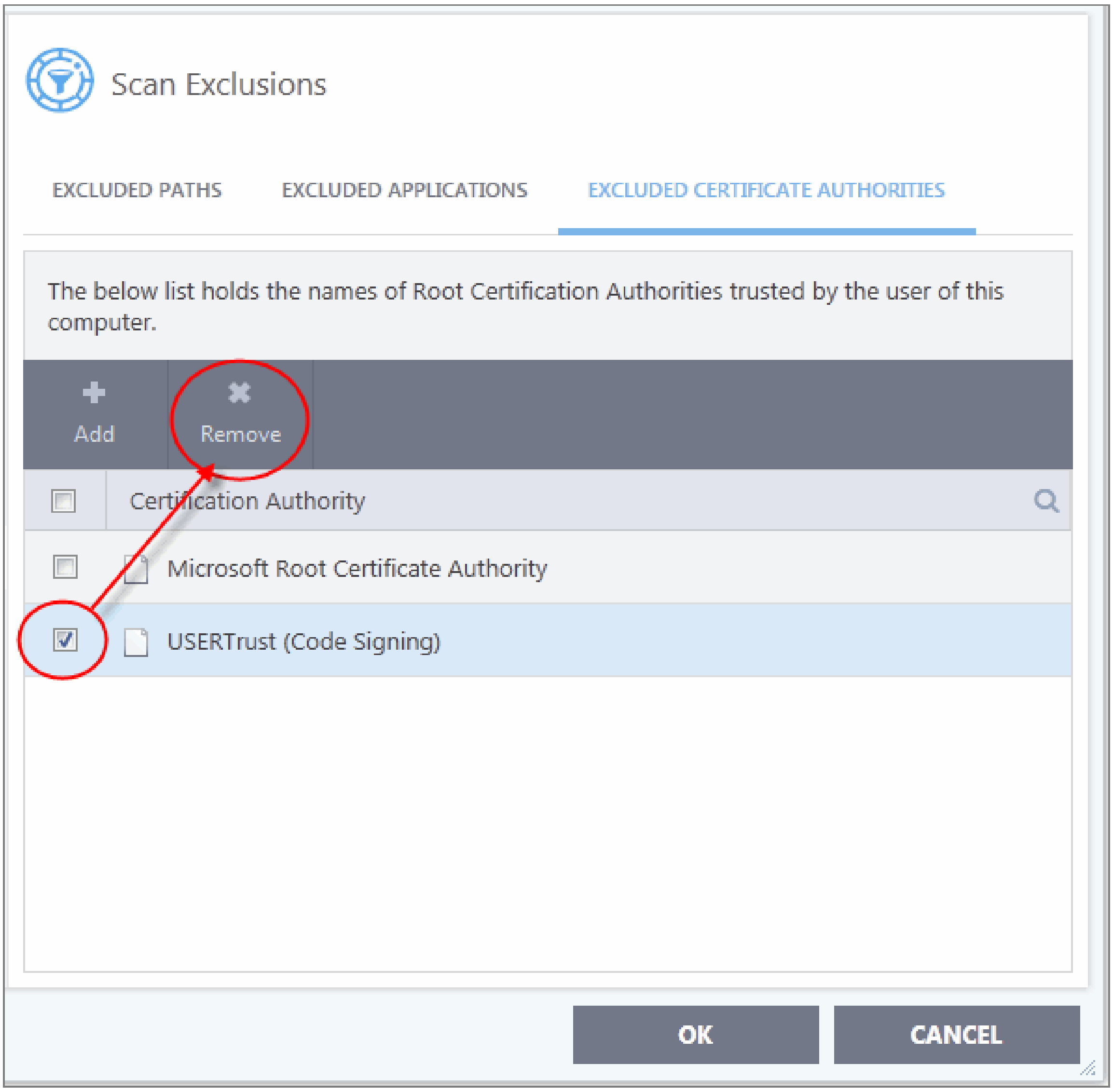
The below list holds the names of Root Certification Authorities trusted by the user of this computer.

□	Certification Authority
□	Microsoft Root Certificate Authority
□	USERTrust (Code Signing)

- Repeat the process to add more certificates. Certificates added to 'Excluded Certificate Authorities' will be omitted from certificate scans in future.

To remove an item from the Excluded Certificate Authorities

- Select the certificate authority and click 'Remove' at the top:


Scan Exclusions

The below list holds the names of Root Certification Authorities trusted by the user of this computer.

□	Certification Authority
□	Microsoft Root Certificate Authority
☑	USERTrust (Code Signing)

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

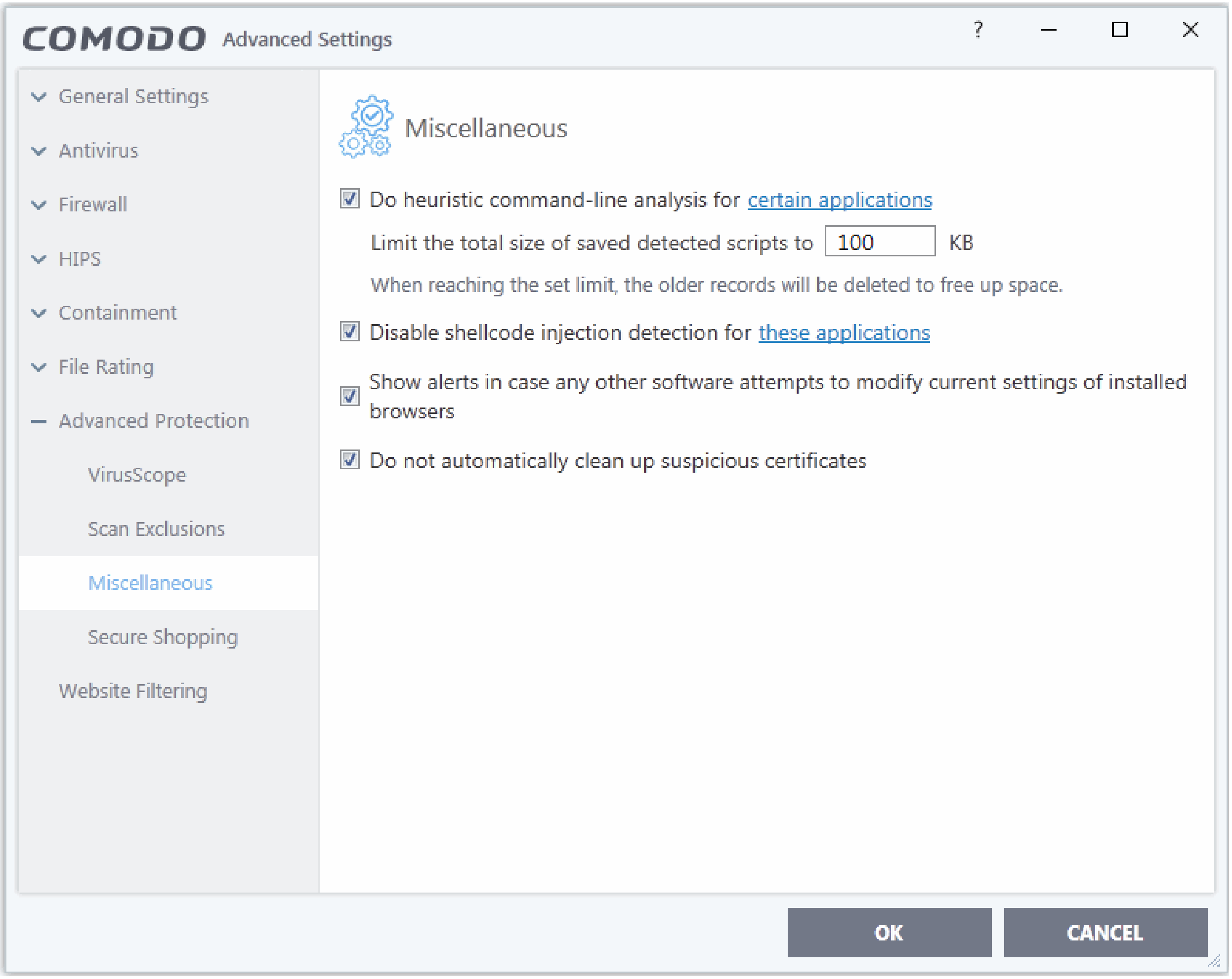
6.7.3. Miscellaneous Settings

The 'Miscellaneous' panel allows you to:

- Configure heuristic command line analysis for certain applications
- Enable Shellcode injections (buffer overflow attacks) and specify exclusions.
- Configure alert when applications try to change your browser's settings.

To open the 'Miscellaneous' interface

- Click 'Settings' from the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Advanced Protection' > 'Miscellaneous':



Miscellaneous

☑ Do heuristic command-line analysis for certain applications

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Disable shellcode injection detection for these applications

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

☑ Do not automatically clean up suspicious certificates

This interface allows you to:

- **Execute heuristic analysis of the applications**
- **Disable shellcode injection**
- **Set alert when a software try to change your browser's settings**
- **Skip automatically clean up suspicious certificates**

Do heuristic command-line analysis for certain applications

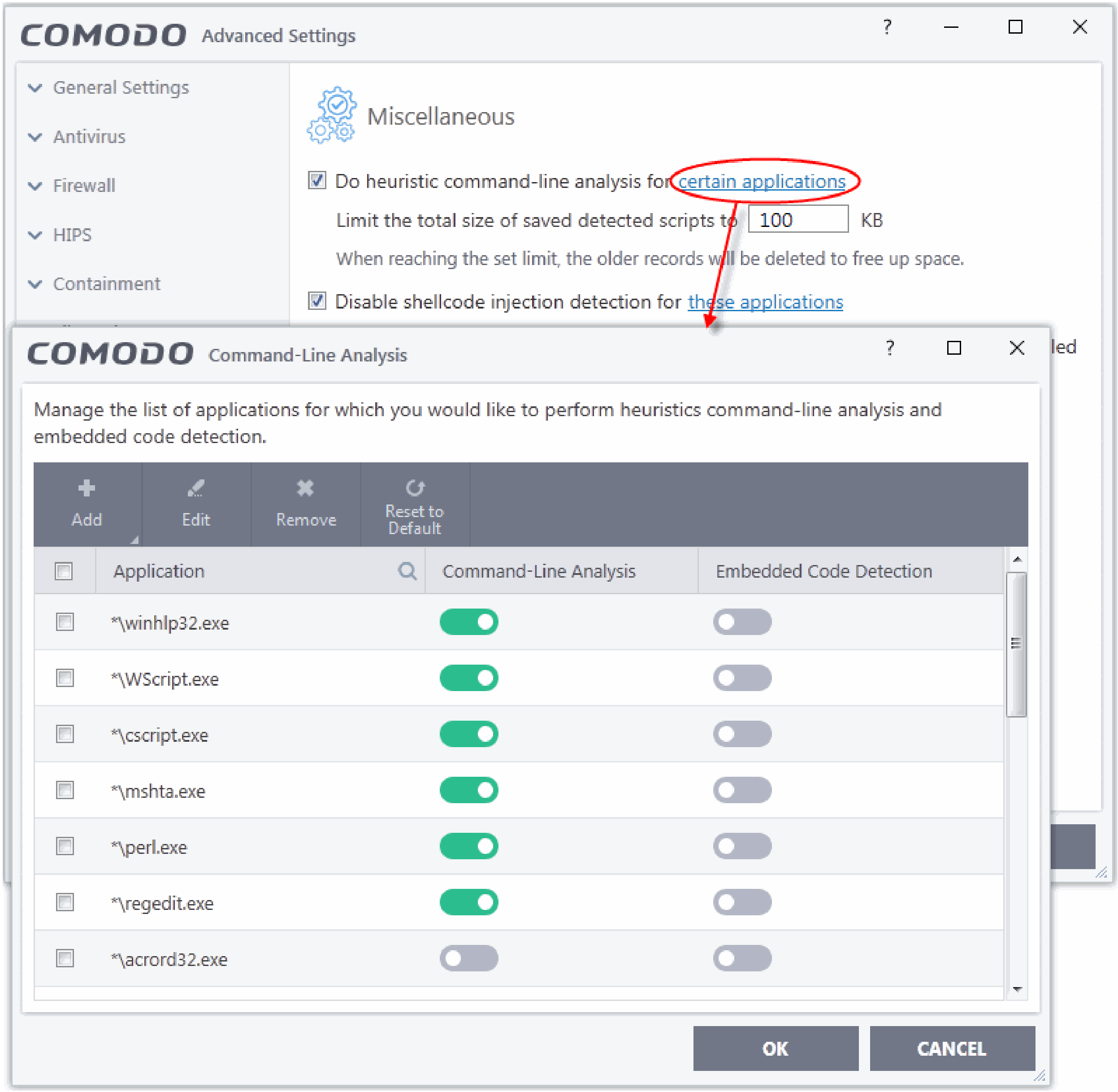
This option instructs CIS to perform heuristic analysis on programs that are capable of executing code. Examples include Visual Basic scripts and Java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe.

For example, the program wscipt.exe can be made to execute Visual Basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CIS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the internet, for example, the alert will state 'test.vbs' is attempting to connect to the internet ***(Default = Enabled).***

If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the Internet'.

Background note: 'Heuristics' describes the method of analyzing a file to ascertain whether it contains codes typical of a virus. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. This helps to identify previously unknown (new) viruses.

Click the 'certain applications' link to view the list of programs that are included by default:



☑ Do heuristic command-line analysis for certain applications

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Disable shellcode injection detection for these applications

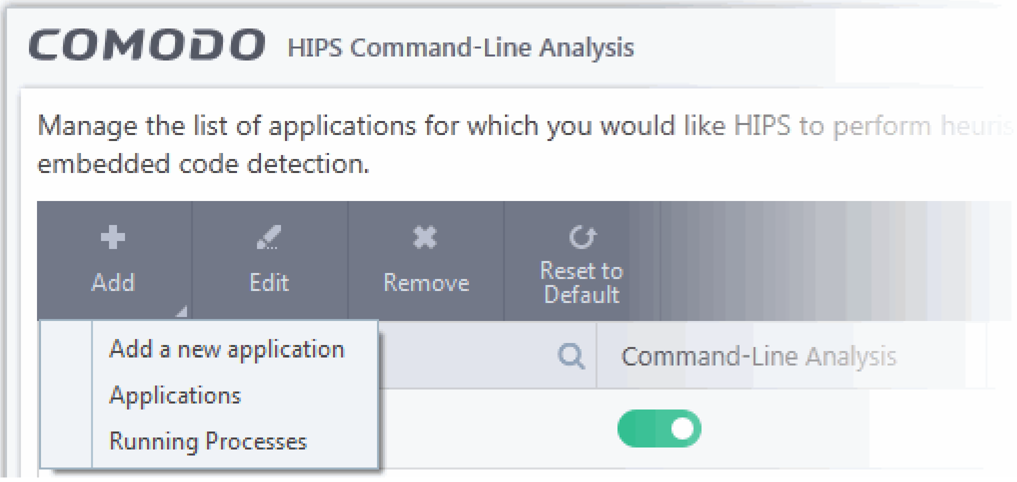
Manage the list of applications for which you would like to perform heuristics command-line analysis and embedded code detection.

□	Application	Command-Line Analysis	Embedded Code Detection
□	*\winhlp32.exe	● On	○ Off
□	*\WScript.exe	● On	○ Off
□	*\cscript.exe	● On	○ Off
□	*\mshta.exe	● On	○ Off
□	*\perl.exe	● On	○ Off
□	*\regedit.exe	● On	○ Off
□	*\acrord32.exe	○ Off	○ Off

Heuristic Command Line Analysis - Column Descriptions	
Column Header	**Description**
Application	Names of existing applications covered by this rule.
Command-Line Analysis	Enable or disable command line tracking.
Embedded Code Detection	Enable or disable embedded code tracking.

To manually add a new application to the list for analysis

- Click 'Add' at the top of the interface



COMODO HIPS Command-Line Analysis

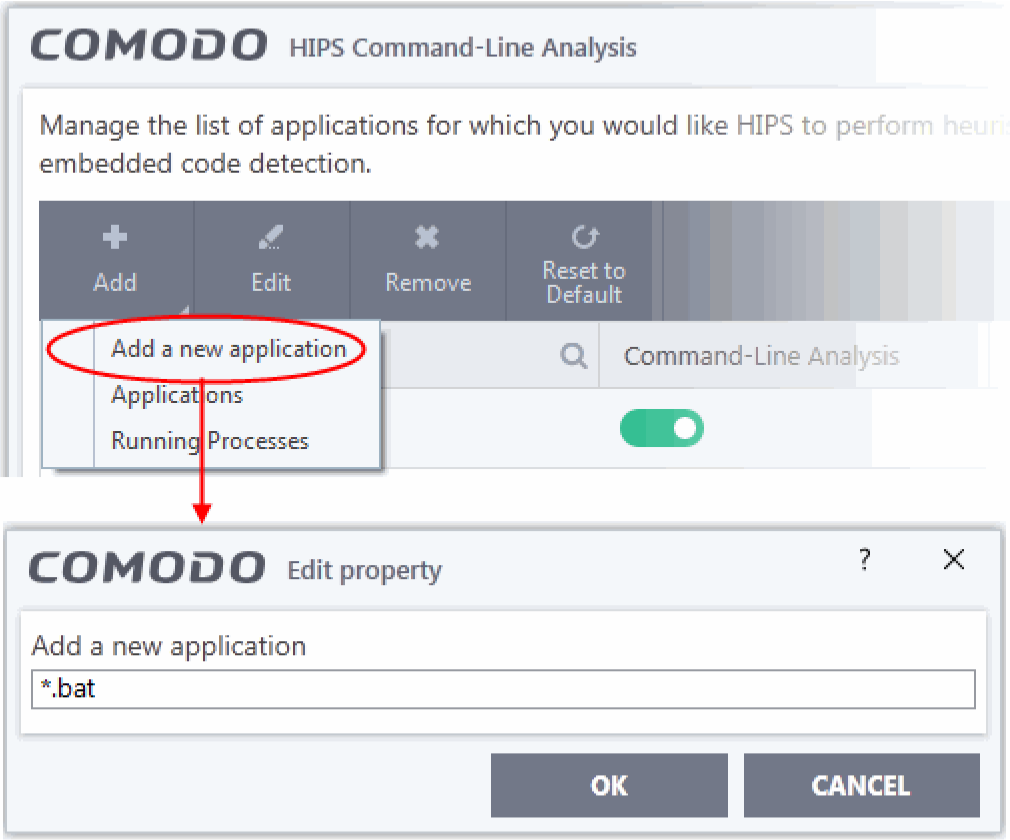
Manage the list of applications for which you would like HIPS to perform heuris embedded code detection.

You can add an application by following methods:

- Add a new application
- Add a current application
- Add application from the currently running processes

Adding a new application

- Click the 'Add new application' at the top right
- Provide the details in the 'Edit Property' dialog and click 'OK'



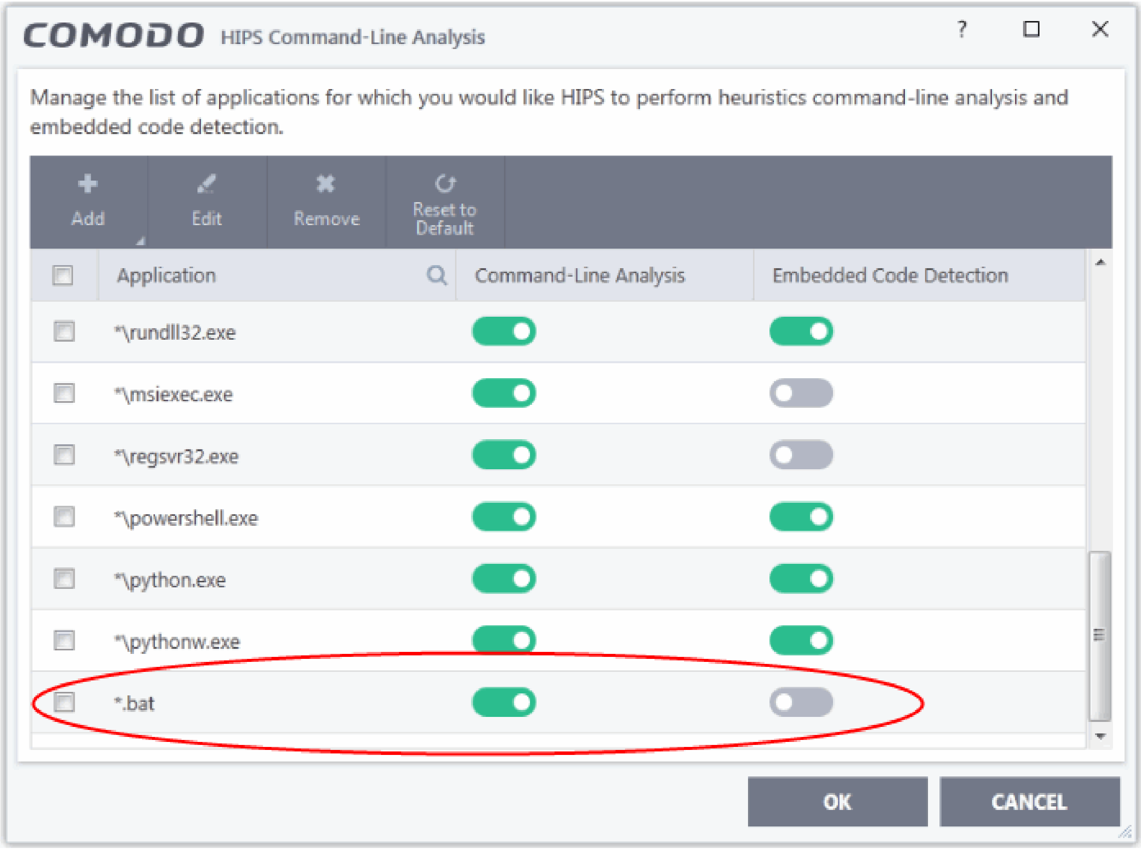
COMODO HIPS Command-Line Analysis

Manage the list of applications for which you would like HIPS to perform heuris embedded code detection.

COMODO Edit property

Add a new application: *.bat

The application will be added and displayed in the list.



Manage the list of applications for which you would like HIPS to perform heuristics command-line analysis and embedded code detection.

□	Application	Command-Line Analysis	Embedded Code Detection
□	*\rundll32.exe	●	●
□	*\msiexec.exe	●	○
□	*\regsvr32.exe	●	○
□	*\powershell.exe	●	●
□	*\python.exe	●	●
□	*\pythonw.exe	●	●
□	*.bat	●	○

Add a current application

- Click the 'Add new application' at the top right and browse for an application to add for analysis
- Navigate to the file you want to add in the 'Open' dialog and click 'Open'
- The file will be added and sent for analysis
- Click “OK” to apply your settings

Add application from running processes

- Choose 'Running Process' from the 'Add' drop-down
- A list of currently running processes in your computer will be displayed
- Select the process whose application is to be added to 'HIPS Comand-Line Analysis'
- Click 'OK' from the Browse for Process dialog
- The application will be added to the selected group
  - Use the slider beside the applications to enable/disable them for analysis.
  - Click the 'Edit' button to update the details of an application.
  - To remove an application, select it from the list and choose 'Remove' at the top.
  - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

Disable shellcode injection detection (i.e. Buffer overflow protection)

By default, shellcode injection protection is enabled for all applications on your computer. Use this setting to define applications which you ***do not*** want to be monitored for shellcode injections.

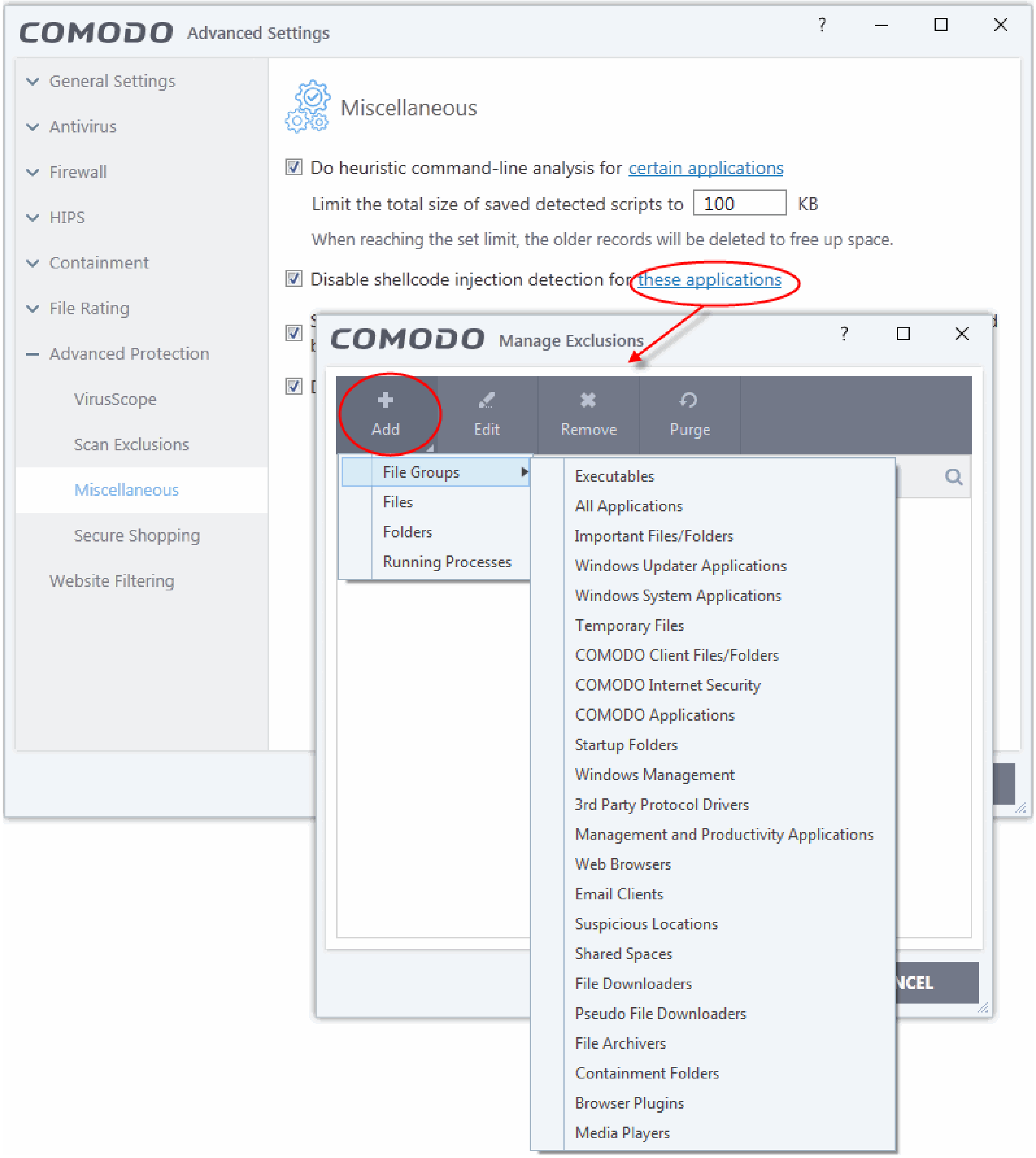
Background:

- A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer.
- The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data. This may cause a process to crash or produce incorrect results.
- Overflows can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

To exclude certain applications from shellcode injection protection

- Make sure 'Disable shellcode injections detection for' checkbox is enabled and click the 'these applications' link. The 'Manage Exclusions' dialog will appear.
- Click the 'Add' button at the top

You can add items by selecting the required option from the drop-down:



Miscellaneous

☑ Do heuristic command-line analysis for certain applications

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Disable shellcode injection detection for these applications

- **File Groups -** Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd. Other such categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc. See **File Groups**, for more details on file groups.
- **Running Processes -** As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.
- **Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
- **Files** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.

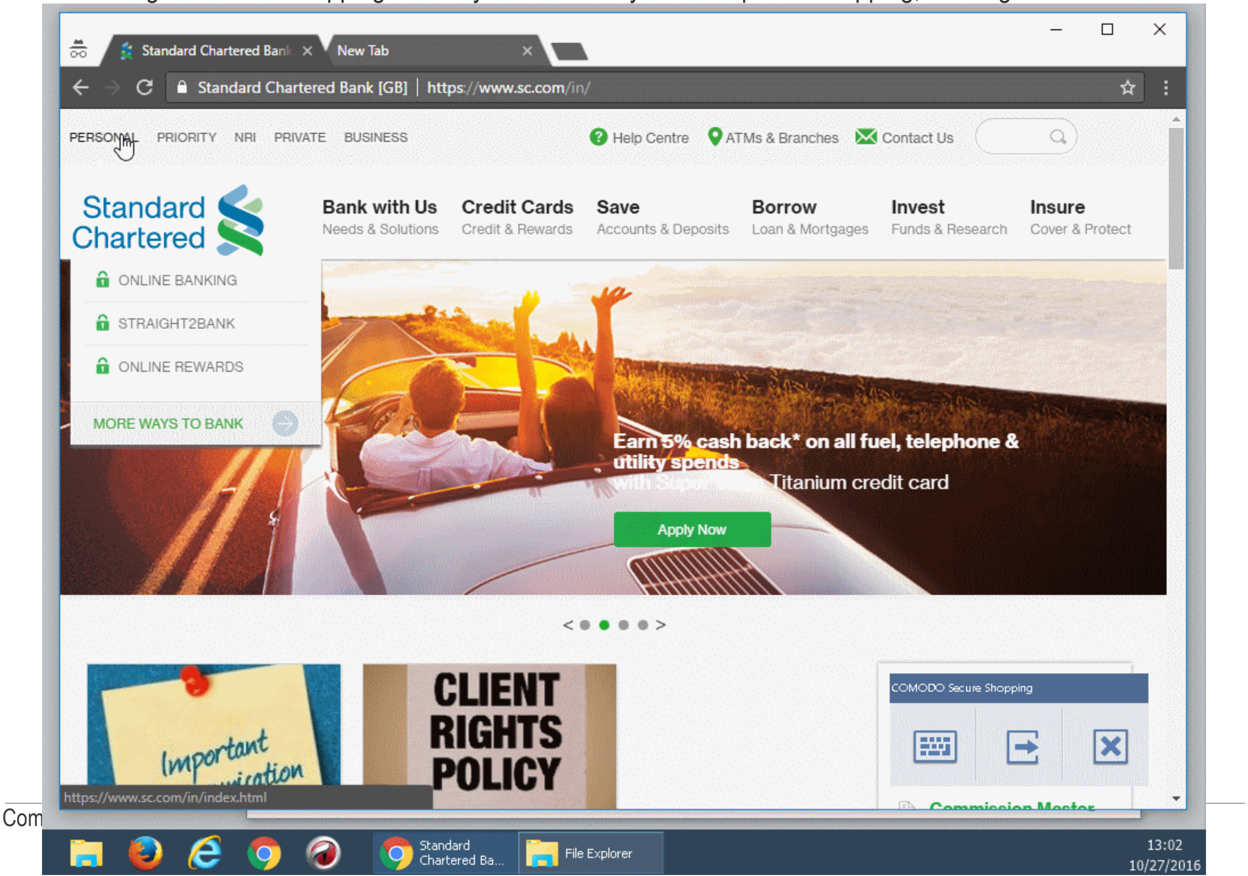
- **Show alerts in case any other software attempts to modify current settings of installed browsers -** Improves online security by warning you when a process tries to change your browser security settings without your consent. Each time a program attempts to modify your browser's settings you will see an alert. ***(Default = Enabled)***
- **Do not automatically clean up suspicious certificates -** If enabled, will not perform automatic cleanup on untrusted certificates. ***(Default = Enabled)***
- Click 'OK' to implement your settings.

6.7.4. Comodo Secure Shopping

Comodo Secure Shopping provides unbeatable security for online banking and shopping sessions by ensuring you connect to those websites from within a security-hardened browsing environment. Browsers running in the secure environment are isolated from any potentially hostile processes running on your computer.

- Hides sensitive online data from other processes running on your PC
- Prevents key-loggers from recording your keystrokes
- Warns you if there is a remote connection to your computer
- Stops hackers and malware taking screenshots of your session
- Detects fake SSL certificates to stop man-in-the-middle attacks

You can configure Secure Shopping to alert you whenever you visit specific shopping, banking and other websites



and ask you if you want to use Secure Shopping environment, open the website in a secure browser window or continue with the same browser.

In addition to websites and browsers, you can also run any 'regular' application inside Secure Shopping. This is especially valuable for applications that process sensitive data, such as:

- Email applications like Outlook and Thunderbird
- Accounting software like Tally and Sage
- Password managers
- Spreadsheet software like Excel and Open Office Calc
- FTP and VPN clients
- Instant messaging and chat applications
- File sharing clients like Drop Box

Data handled by applications inside the virtual environment cannot be tracked by any other process running on your computer.

The technology behind Comodo Secure Shopping is already being used by major point-of-sale and money transfer organizations to secure sensitive customer transactions. With CIS 10, Comodo brings this same level of security to your home. If you need a truly secure place to work and go online, then use Comodo Secure Shopping.

The following sections explain more about:

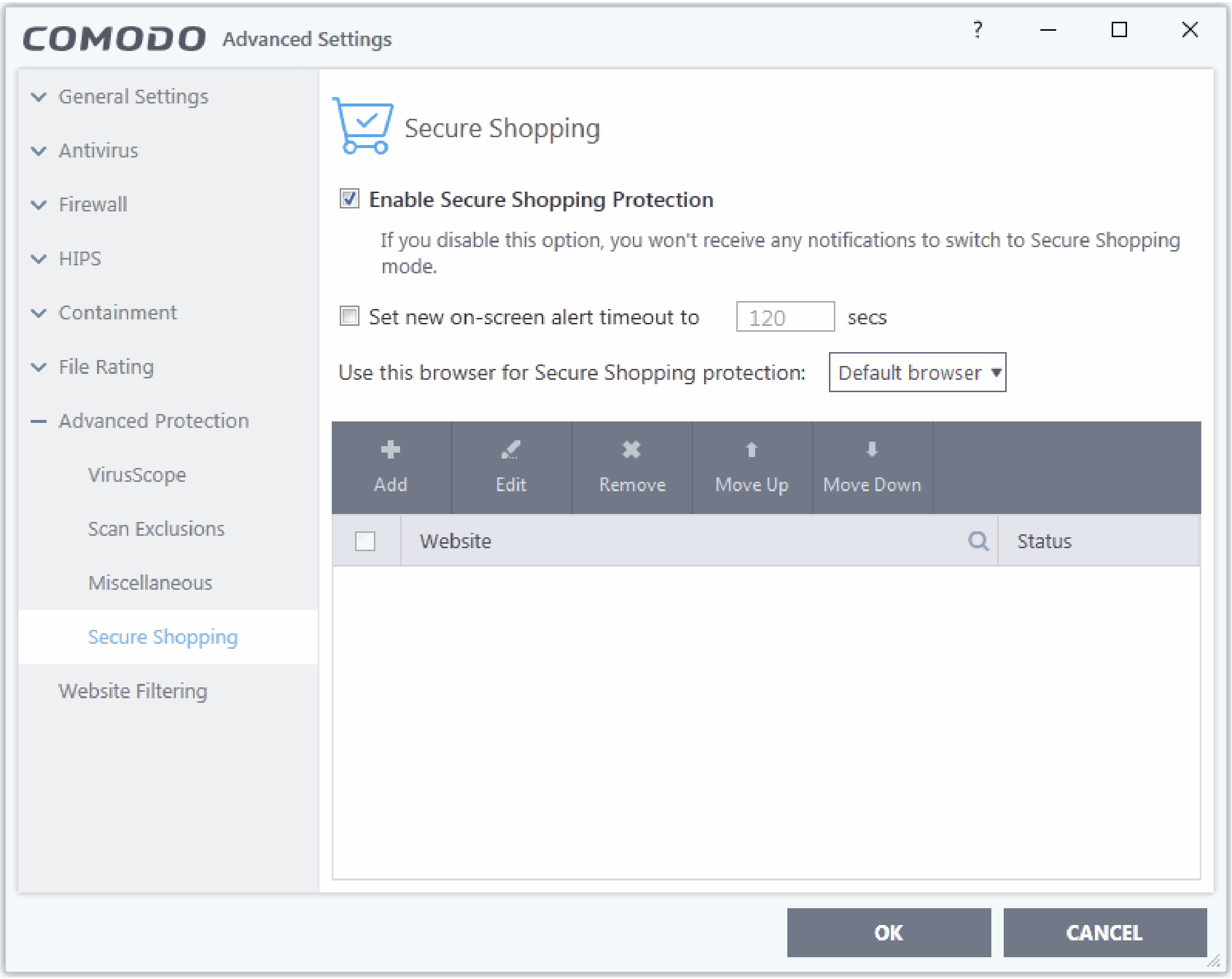
- **Configuring Secure Shopping**
- **Using Secure Shopping Environment**
  - **Shopping and Banking Activities**
  - **Opening applications inside Secure Shopping Environment**

Configuring Secure Shopping

The 'Secure Shopping' configuration screen allows you to add websites for Secure Shopping protection and to configure the general behavior of the module.

To configure Secure Shopping

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Secure Shopping' on the left



COMODO Advanced Settings

Secure Shopping

☑ Enable Secure Shopping Protection

If you disable this option, you won't receive any notifications to switch to Secure Shopping mode.

□ Set new on-screen alert timeout to 120 secs

Use this browser for Secure Shopping protection: Default browser

Secure Shopping Settings

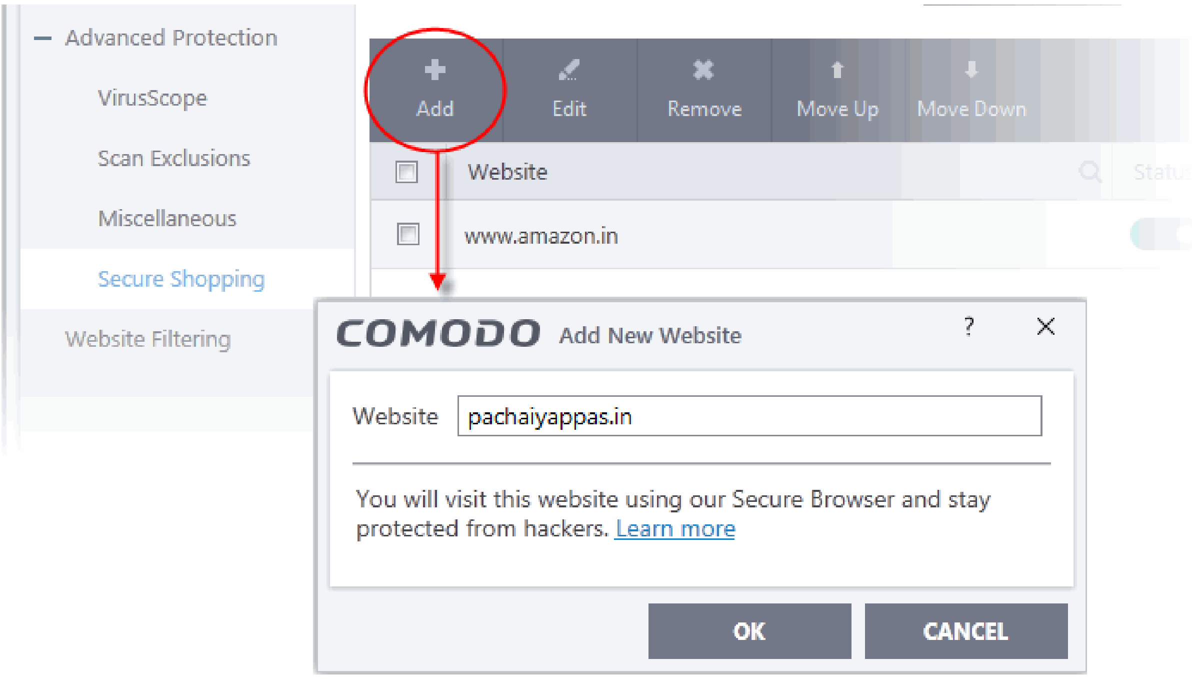
- **Enable Secure Shopping Protection** - Allows you to activate or deactivate Secure Shopping ***(Default = Enabled)***
- **Set new on-screen alert timeout to** - Secure Shopping displays an alert whenever you visit a website configured for Secure Shopping protection and will ask you if you want to enter secure mode. If enabled, this setting allows you to choose how long an unanswered alert can remain on the screen. If the alert is unanswered and times-out, the website will continue in the current browser. (***Default = Disabled***)
- **Use this browser for Secure Shopping protection** - Allows you to choose the web browser to be used when in secure shopping mode. The drop-down lists all browsers installed on your computer:

When adding or editing a web site, you can configure the following options:

- **Website** - URL of the protected website
- **Status** - The toggle switch allows you enable or disable secure shopping protection for the website.

To add websites for Secure Shopping protection

1. Click the 'Add' button' then enter the name of your website.

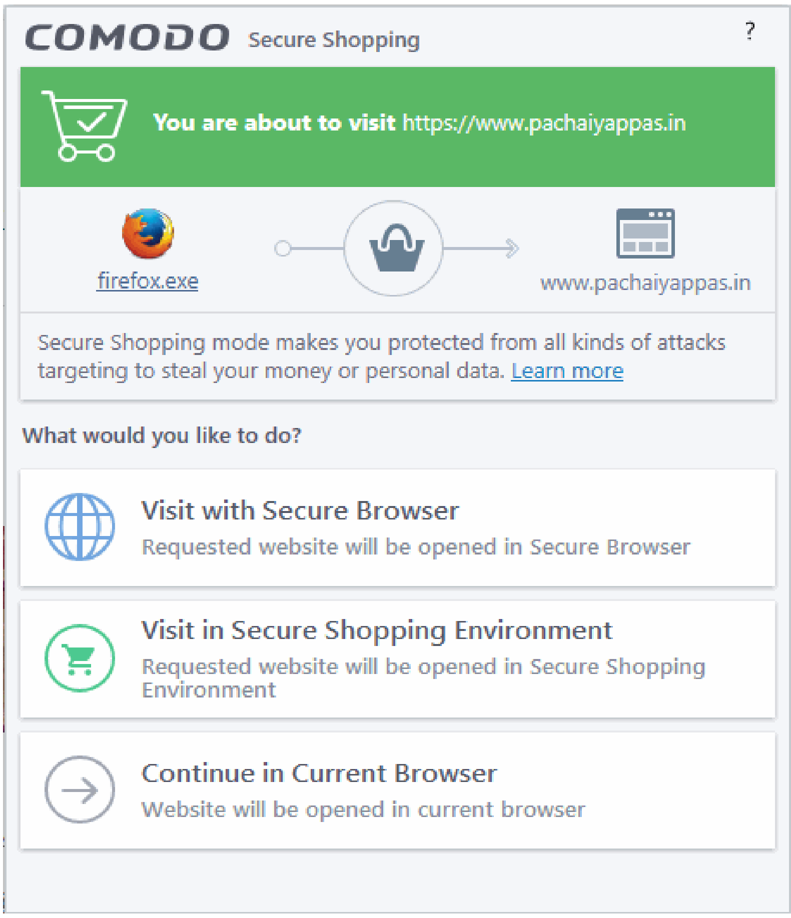


Website: pachaiyappas.in

You will visit this website using our Secure Browser and stay protected from hackers. Learn more

2. Click 'OK' to add the website to the list. Repeat the process to add more websites
3. To edit the settings for a website, select the website and click 'Edit'. The Edit Website dialog will appear, similar to the Add New Website dialog. Edit the parameters as required and click 'OK'.
4. To remove a website, select it and click 'Remove'.
5. Click 'OK' in the 'Advanced Settings' interface to save your changes.

Whenever you visit a website added to the list of websites for secure shopping protection, an alert will be displayed as shown below:



COMODO Secure Shopping

You are about to visit https://www.pachaiyappas.in

Secure Shopping mode makes you protected from all kinds of attacks targeting to steal your money or personal data. Learn more

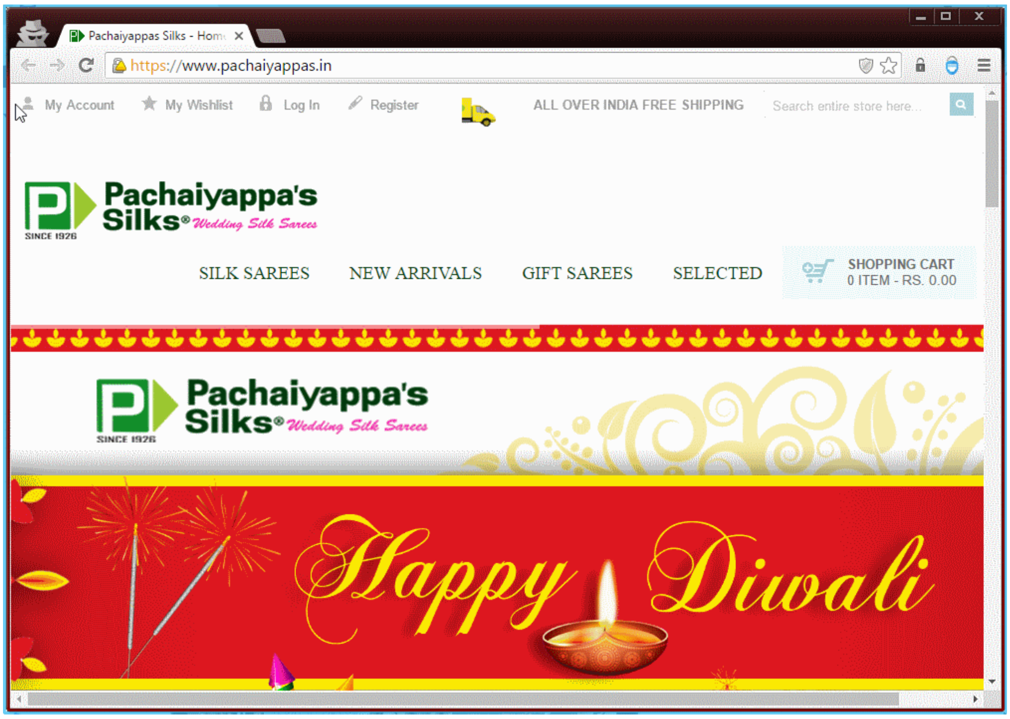
What would you like to do?

Visit with Secure Browser
Requested website will be opened in Secure Browser

Visit in Secure Shopping Environment
Requested website will be opened in Secure Shopping Environment

Continue in Current Browser
Website will be opened in current browser

- You can choose how you want to proceed with the website, from the alert.
  - **Visit with Secure Browser -** The website will open in a browser protected by all Secure Shopping technologies *except* full process isolation is replaced with partial process isolation. The browser window have a blue border around it:



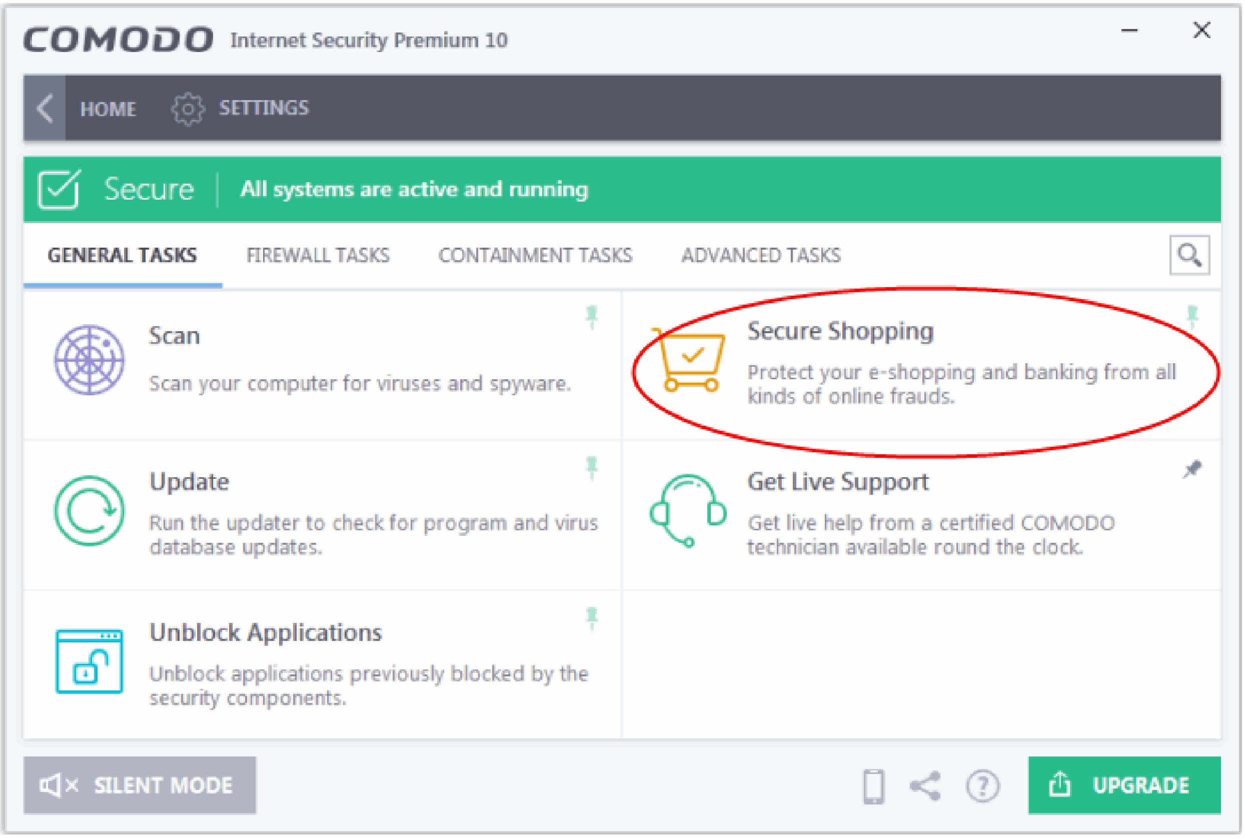
- **Visit in Secure Shopping Environment -** The website will be opened in a security hardened, virtual environment. When inside this environment, your browser cannot be accessed or potentially attacked by other processes running on your computer. Your session will be protected by all Secure Shopping technologies (full process isolation, key-logger protection, remote connection warnings, screenshot blocking and SSL certificate checking). See **Using Comodo Secure Shopping Environment**, for more details on the Secure Shopping Environment.
- **Continue in Current Browser -** Allows you to continue your browsing activities with the same browser through which the website was opened.

Using Secure Shopping Environment

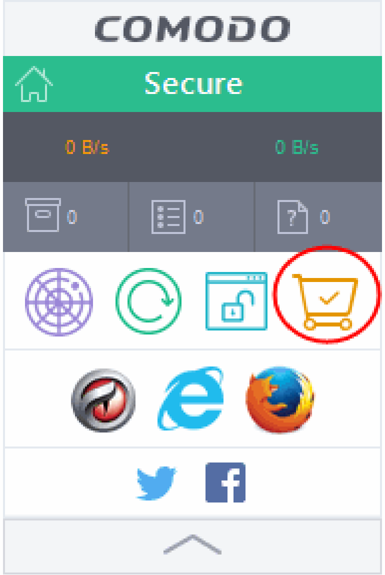
The Secure Shopping environment automatically opens when you choose 'Visit in Secure Shopping Environment' in the Secure Shopping alert.

You can manually open the Secure Shopping environment in the following ways:

- From the CIS Home Screen - Click 'Tasks' > 'General Tasks' > 'Secure Shopping'

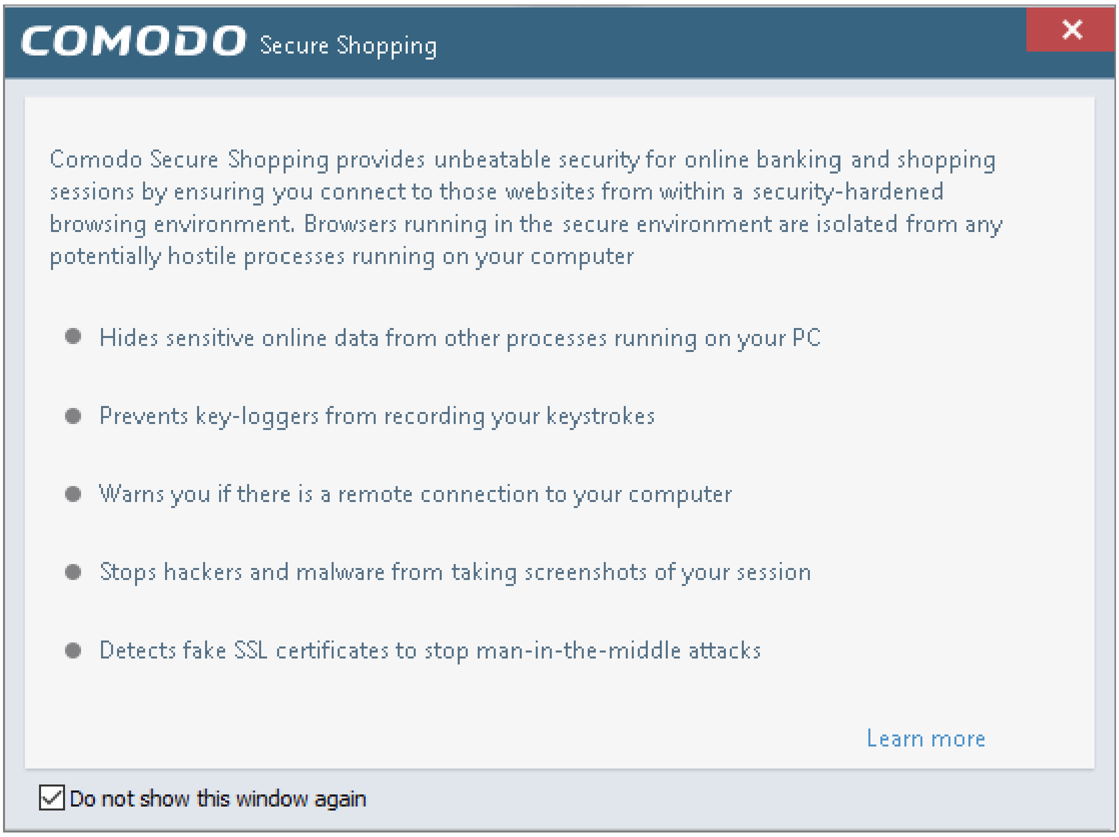

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
SILENT MODE
UPGRADE

- From the CIS Desktop Widget - Click the 'Secure Shopping' icon from the CIS Desktop widget



- From the Windows Start menu - Click Windows Start/Home > All Programs > Comodo > Comodo Secure Shopping
- From the Windows Desktop icon - Double-click the 'Comodo Secure Shopping' shortcut on the desktop:

When you start the application, a welcome screen will appear which explains the benefits of secure shopping:



Comodo Secure Shopping provides unbeatable security for online banking and shopping sessions by ensuring you connect to those websites from within a security-hardened browsing environment. Browsers running in the secure environment are isolated from any potentially hostile processes running on your computer

- Hides sensitive online data from other processes running on your PC
- Prevents key-loggers from recording your keystrokes
- Warns you if there is a remote connection to your computer
- Stops hackers and malware from taking screenshots of your session
- Detects fake SSL certificates to stop man-in-the-middle attacks

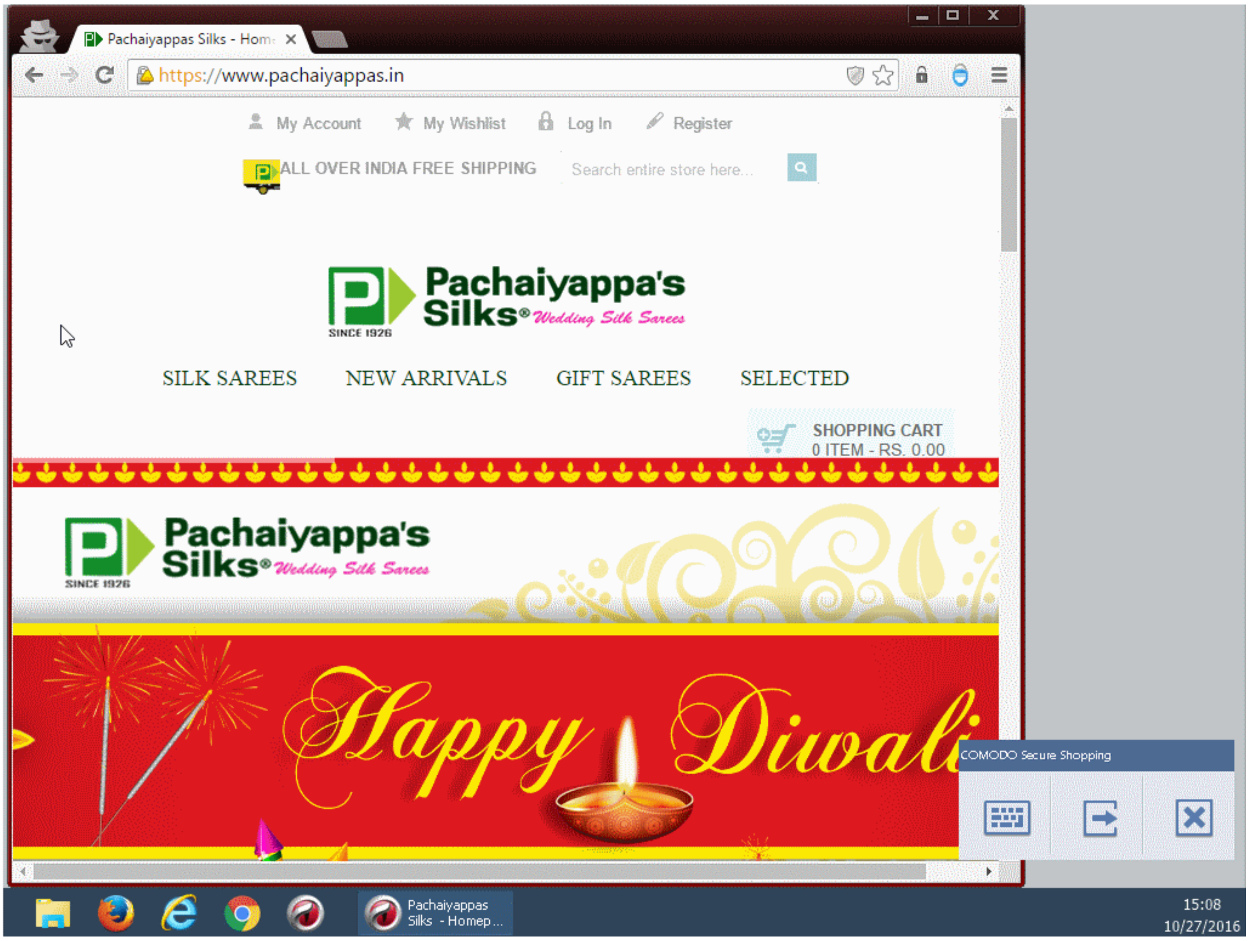
Learn more

☑ Do not show this window again

- Check 'Do not show this window again' to disable the welcome screen in future.

Shopping and Banking Activities

If you are visiting a pre-configured online shopping or a banking website and choose 'Visit in Secure Shopping Environment' from the alert, the environment will open automatically with the website in the browser chosen as per the Secure Shopping configuration. If you are opening the Secure Shopping environment manually, the environment will open with the default browser. You can enter the URL of the website in the address bar of the browser.



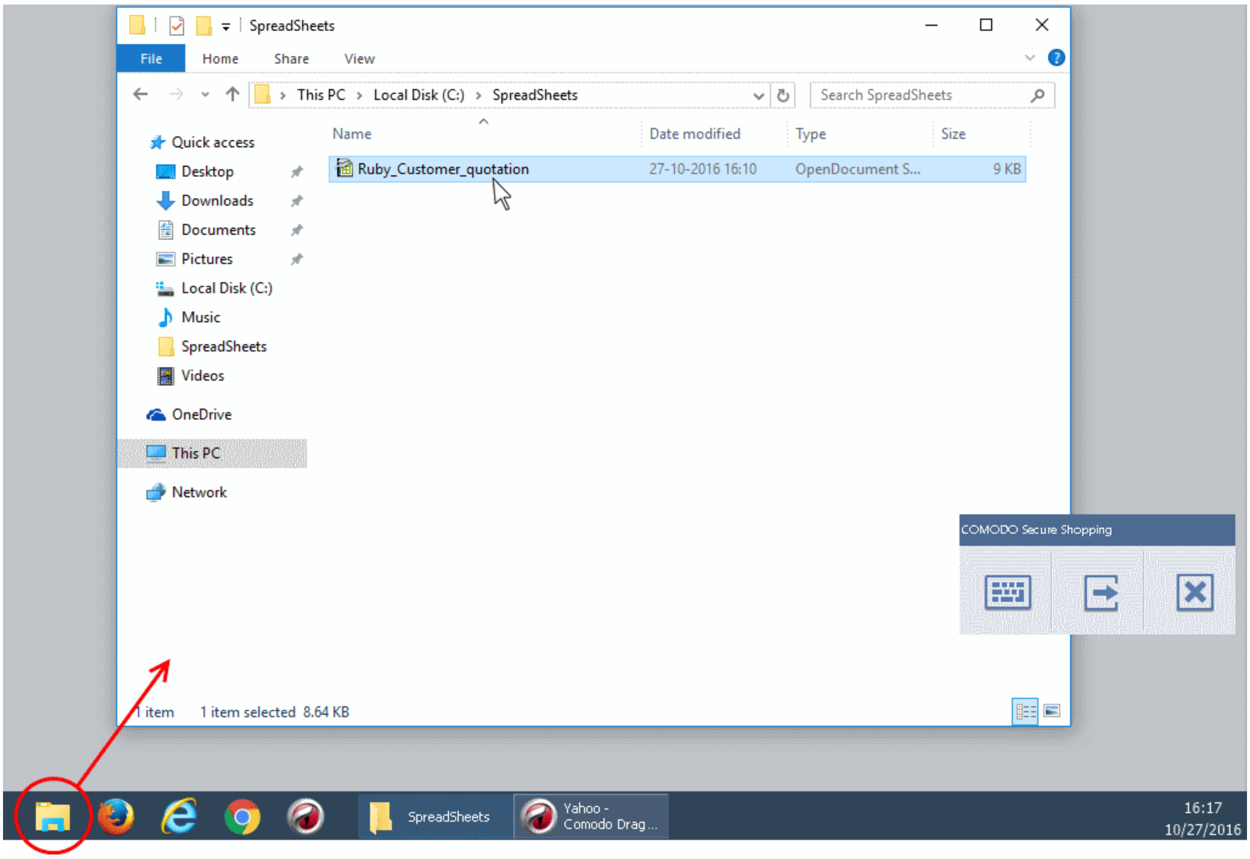
The tools panel at the bottom right of the screen allows you to open the virtual keyboard, temporarily switch back to your desktop, or to fully exit the Secure Shopping virtual environment.

See the explanations given below for:

- Using Virtual Keyboard
- Switching to your Desktop
- Exiting Secure Shopping

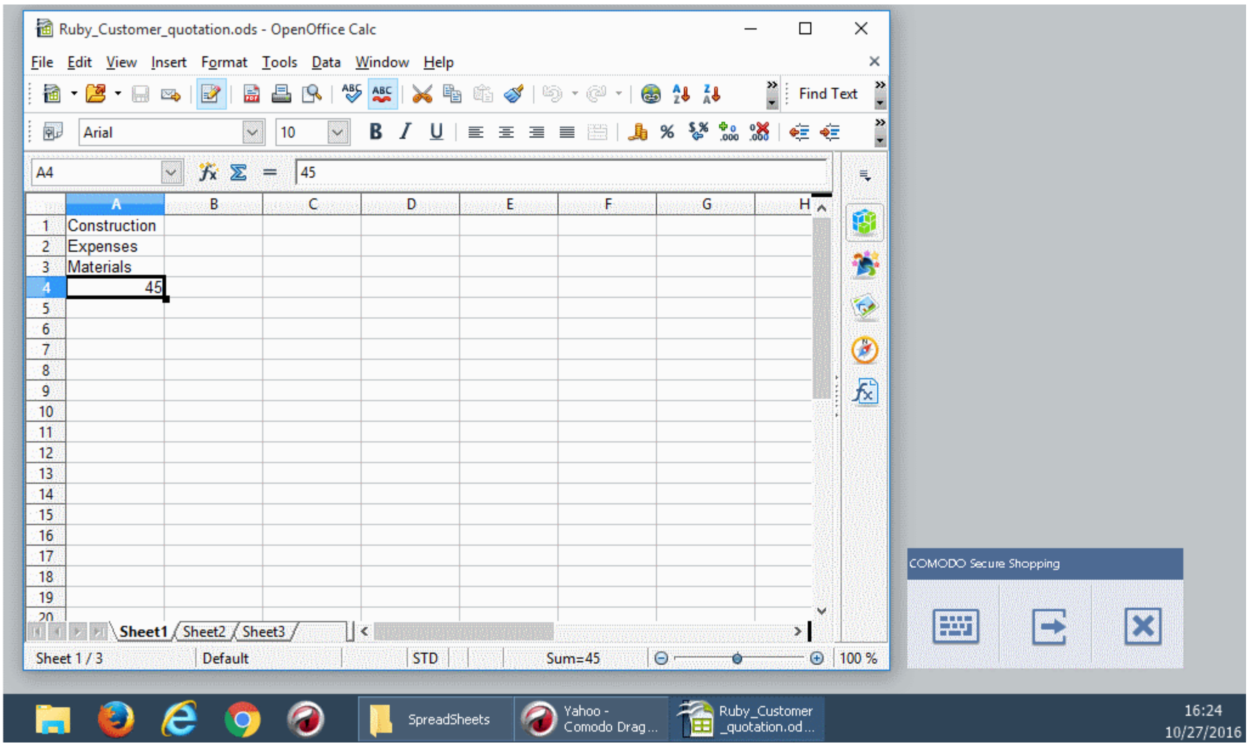
Opening applications inside the Secure Shopping Environment

- Start the Secure Shopping environment and click the folder icon at bottom-left:



- Browse to the application you want to run and open it.

The application will open inside the Secure Shopping environment:

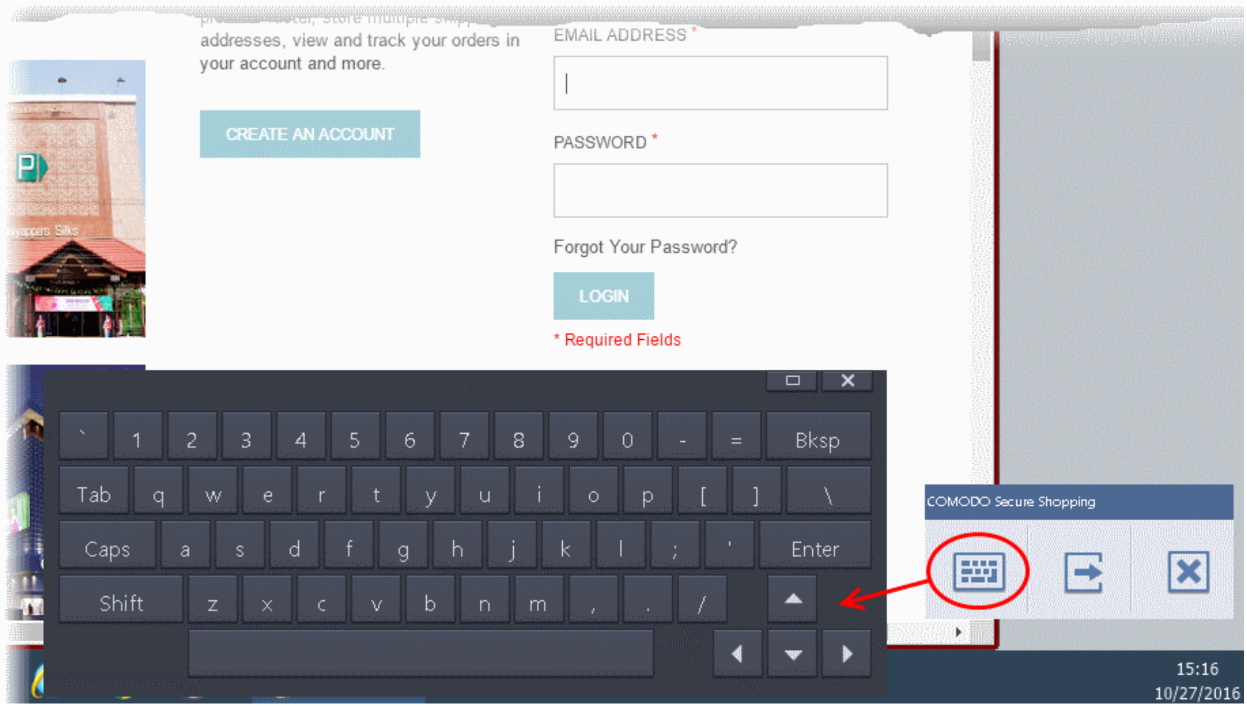


	A
1	Construction
2	Expenses
3	Materials
4	45

The tools panel at the bottom right of the screen allows you to open the virtual keyboard, temporarily switch back to your desktop, or to fully exit the Secure Shopping virtual environment.

To use the virtual keyboard

- Click the keyboard icon on the system tray to opens the on-screen virtual keyboard. This can be used to input confidential data like website user-names, passwords and credit card numbers.



To temporarily switch to your desktop

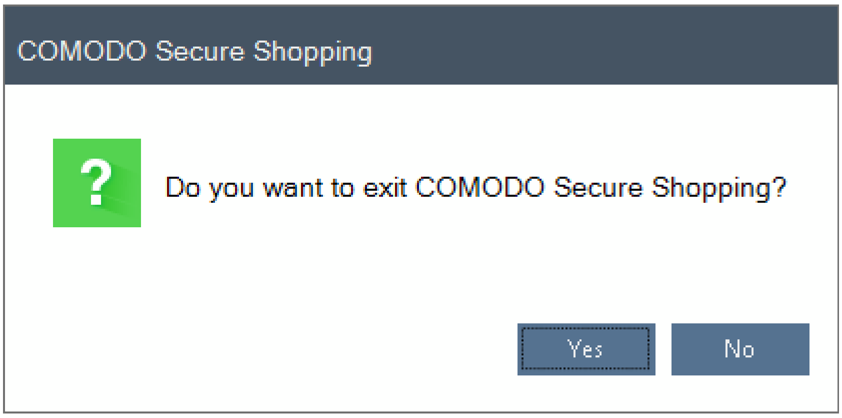
- Click the button from the tools pane at the bottom right.

The Secure Shopping Desktop will be hidden. You can quickly return to it by clicking the button again.

To close the Secure Shopping Desktop

- Click the 'X' button ☒

A confirmation dialog will be displayed.


COMODO Secure Shopping

Do you want to exit COMODO Secure Shopping?

- Click 'Yes' to exit the Secure Shopping Desktop.

6.8. Website Filtering Configuration

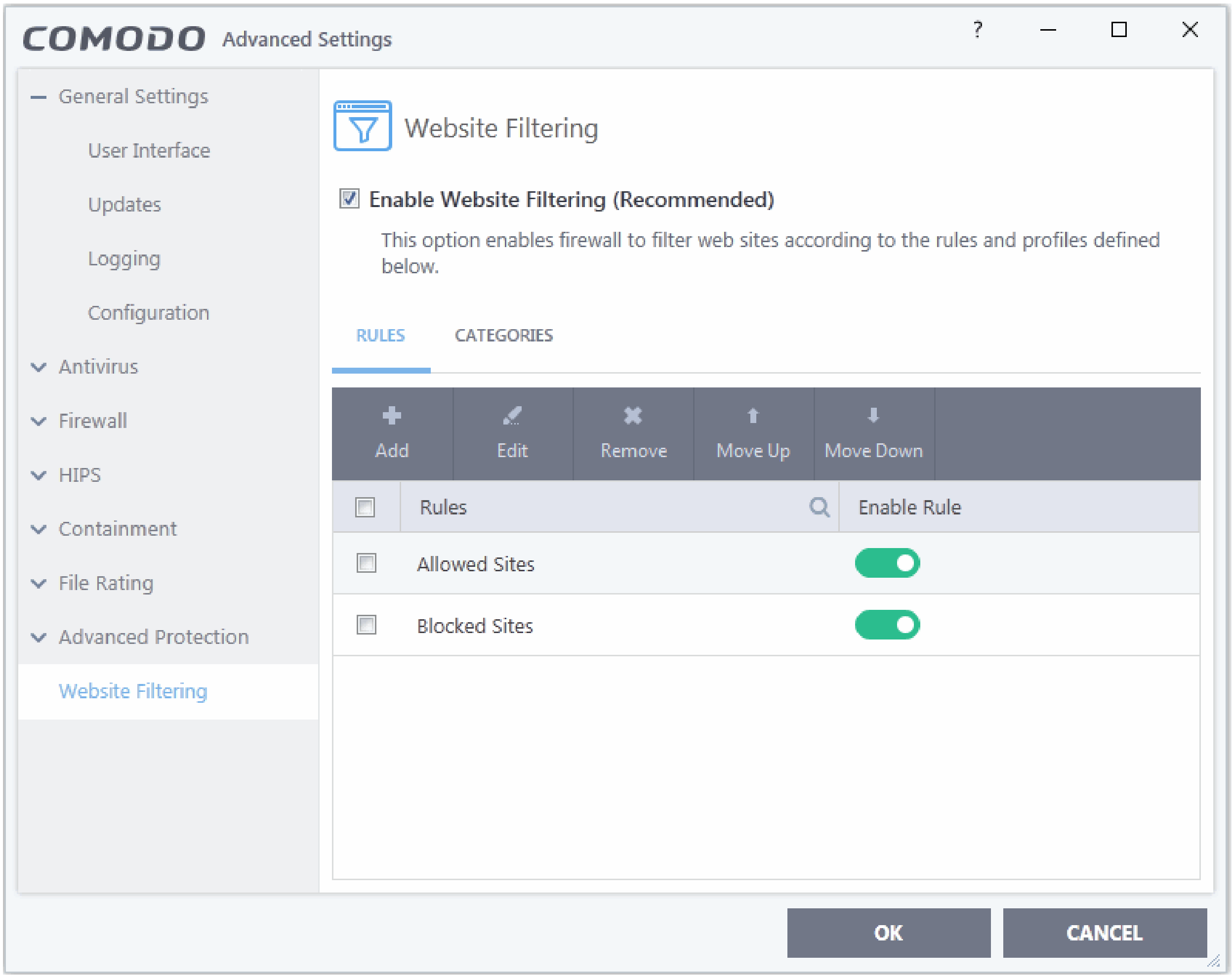
- The 'Website Filtering' section allows you to set up rules to allow or block access to specific websites.
- Rules can be created for particular users of your computer, which makes this feature very useful for both home and work environments. For example, parents can block juvenile users from visiting inappropriate

websites while companies can prevent employees from visiting leisure sites during working hours.

- You also have the option to create a log event whenever a user tries to visit a website which is in conflict with a rule.

To open the 'Website Filtering' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Website Filtering' on the left and choose the 'Rules' tab



☑ Enable Website Filtering (Recommended)

This option enables firewall to filter web sites according to the rules and profiles defined below.

Rules	Enable Rule
Allowed Sites	●
Blocked Sites	●

Overview:

- You add websites to a category then the category to a rule.
  - Rules are constructed by adding one or more 'Categories'.
  - A 'Category' is a collection of one or more 'Websites'
  - A 'Website' can be specified with a full URL, a text string, or text string with a wildcard character (*)
- You must set a rule to be 'Allow', 'Block' or 'Ask' and must specify to which users it should apply.
- The 'Enable Rule' switch allows you to turn a rule on or off.

Categories

- CIS ships with seven preset categories of websites which can be added to rules that you create. All of these of these are non-modifiable lists which are managed by Comodo. The categories are: 'Comodo Safe category', 'Comodo Phishing category', 'Comodo Malware category', 'Comodo PUA category', 'Comodo Malicious category', Comodo Suspicious category'.

- The other two categories, 'Exclusions' and 'Blocked', are empty by default and allow you to specify particular websites that should be allowed or blocked. You should add URLs to the 'Exclusions' category if you require access to a website which is blocked by a category.

Rules

- CIS also ships with two predefined rules, 'Allowed Sites' and 'Blocked sites', both of which are modifiable.
- The 'Blocked Sites' rule will prevent access to sites in the 'Comodo defined Malware sites' and 'Comodo defined Phishing Sites' categories. If you wish, you can add other categories to this rule to expand its coverage.
- The 'Allowed Sites' rule will permit access to websites in the Comodo 'Safe Sites' and 'Exclusions' categories.

To set up a new rule

- Click the 'Rules' tab
- Click 'Add' then name your rule
- Add categories to the rule
- Specify users to whom the rule should apply
- Specify whether the rule should be 'Allow', 'Block' or 'Ask'

The 'Website Filtering' panel has two sections:

- **Rules** - Define rules for website filtering and assign to required users. See '**Website Filtering Rules**' for more details.
- **Categories** - Define categories of websites to be allowed or blocked in website filtering rules. See '**Website Categories**' for more details.

General Advice:

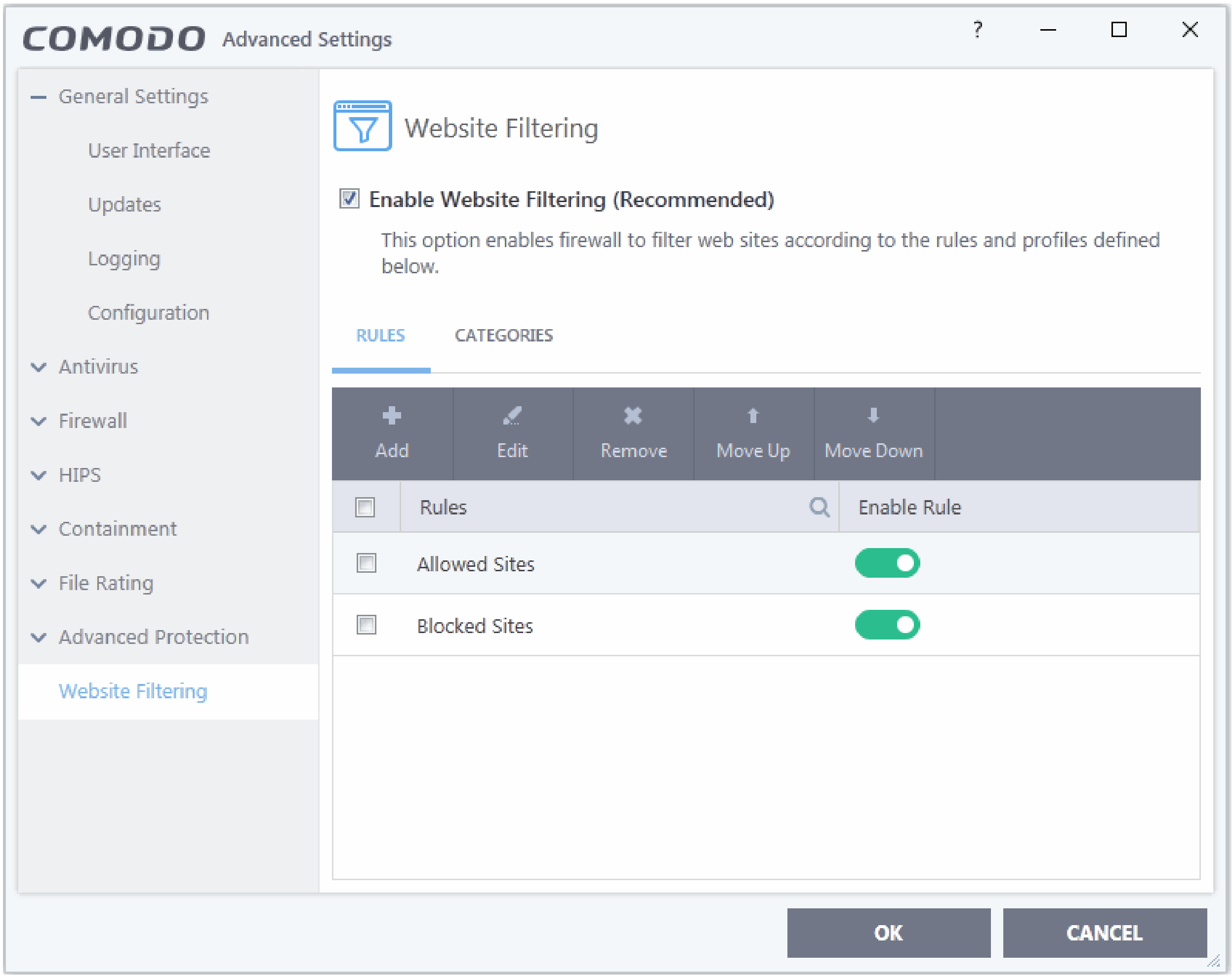
- It is the 'Categories' section where you specify the website(s) that you wish to block or allow, not the 'Rules' section. A rule is mainly for specifying the user(s) for whom a category of URLs should be filtered and whether those categories should be allowed or blocked.
- When creating a new rule, you will be required to specify which categories should be included. You can elect to use just the pre-defined Comodo categories but, if you wish to filter specific websites, you will need to create your own category.
- For example, if you wanted to create a category to block youtube.com and certain other leisure websites, you would *click 'Categories'* > *'Add Category'* > *Type name for category* > *Select your new category in list* > *'Add Website'* > *Type www.youtube.com. Click 'Add Website' again to add more sites.* You will now be able to select this category when creating a rule for a user(s).
- See '**Website Categories**' for more details on specifying website categories.

6.8.1. Website Filtering Rules

- The powerful rule-configuration interface lets you create rules which are as sweeping or as granular as you require. Rules can be created on a per-user basis, allowing you to control exactly which websites certain people can or cannot visit. You can also disable or enable a rule as required at any time.
- Comodo Firewall implements rules in the order they are in this list. Should a conflict exist between individual rules, then the rules at the top takes priority. Click the 'Move Up' or 'Move Down' buttons at the top to change a rule's priority.

To open the 'Website Filtering Rules' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Website Filtering' on the left and choose the 'Rules' tab



☑ Enable Website Filtering (Recommended)

This option enables firewall to filter web sites according to the rules and profiles defined below.

□	Rules	Enable Rule
□	Allowed Sites	●
□	Blocked Sites	●

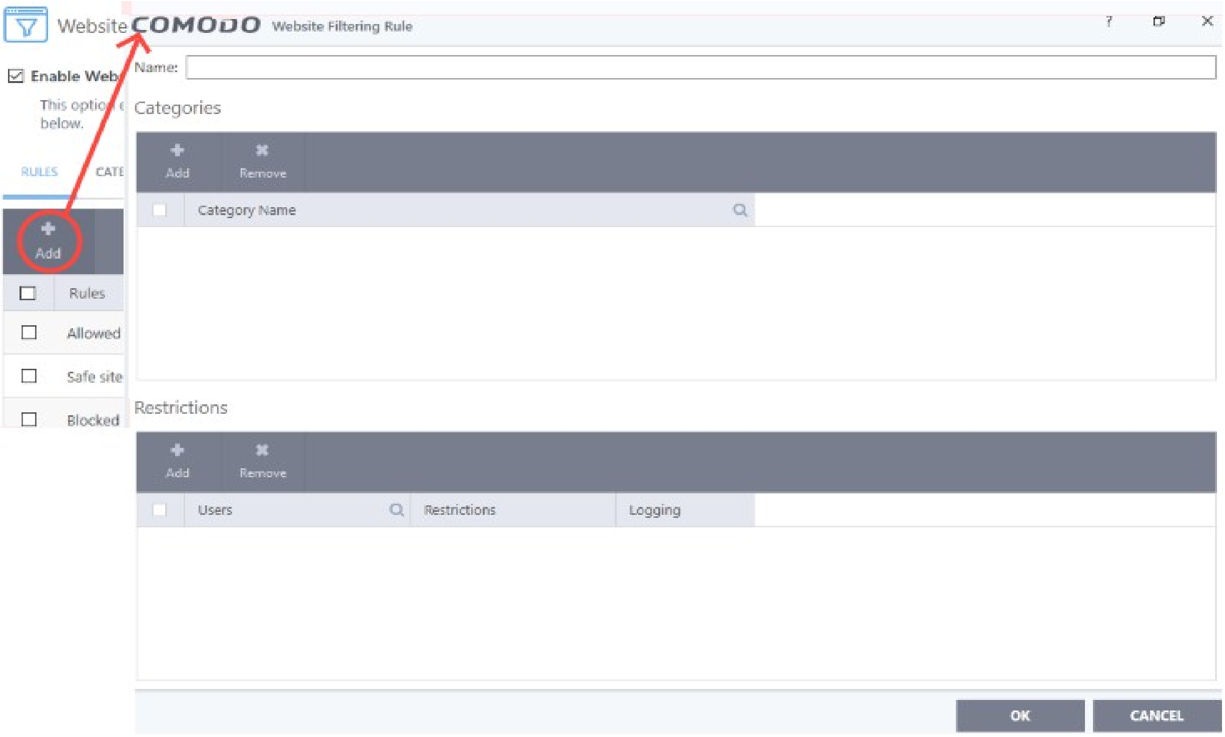
- The 'Enable Rule' switch allows you to turn a rule on or off.
- The check-boxes next to a rule name let you select it for editing, deleting or re-prioritizing.
- Click the magnifying glass icon to search for a specific rule in the list.

The 'Rules' interface allows you to:

- **Create new website filtering rules**
- **Edit existing rules**
- **Remove unwanted rules**
- **Change priority of the rules**

To create a new Website Filtering rule

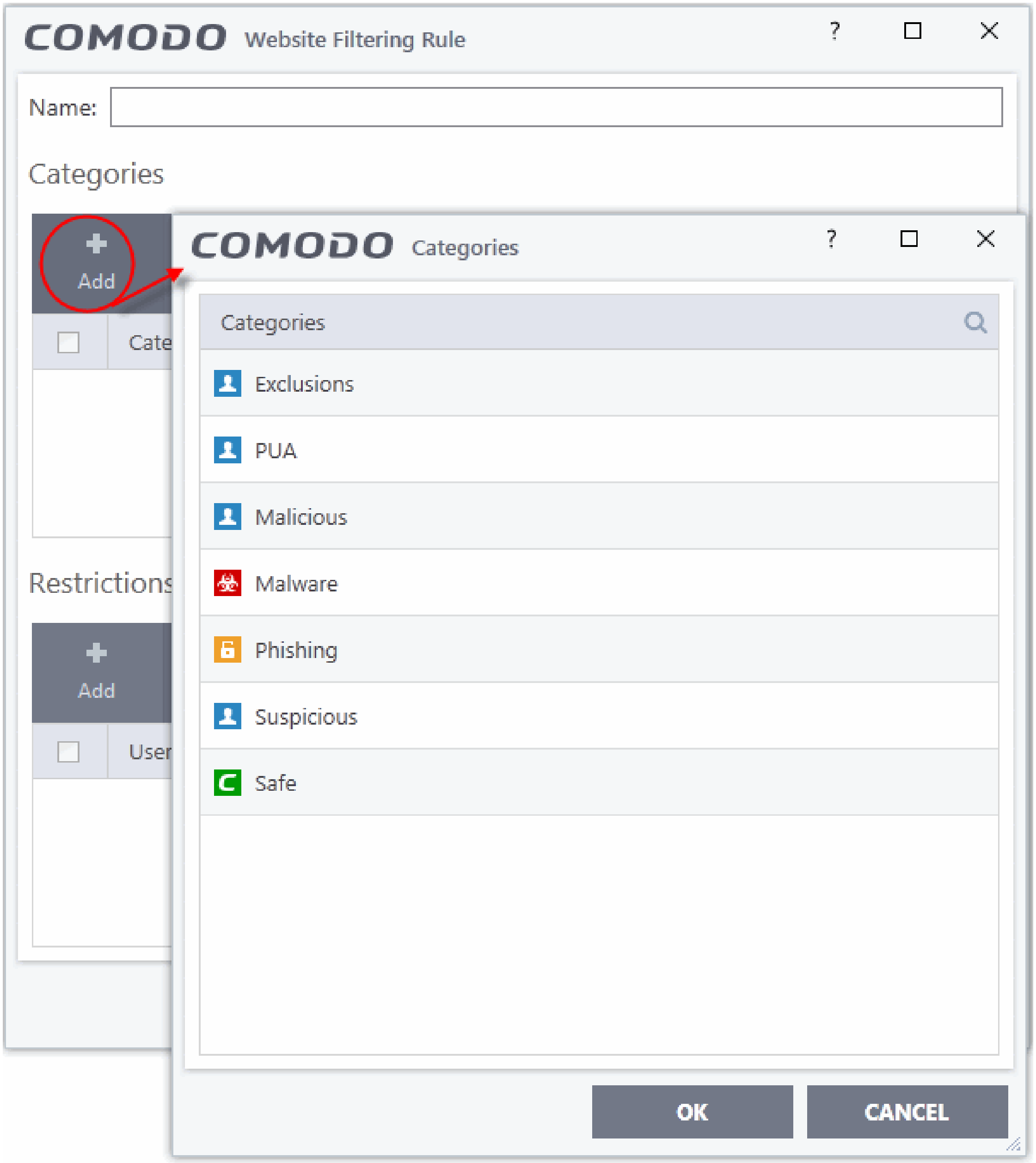
1. Open the 'Website Filtering' Panel by clicking 'Settings' from the CIS home screen and then select 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the 'Add' button at the top.



3. Enter a name for your new filter.

4. Select the categories that should be added to the filter:

    - Click the 'Add' button from the 'Category' pane



- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

The 'Categories' window contains a list of pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Safe Sites** - Websites that are considered safe according to the global whitelist.
- **Phishing Sites** - Fake copies of popular banking, shopping and social media websites that intend to steal customer data.
- **Malware Sites** - The URL leads to a direct malware download. Malware is designed to damage your computer, steal sensitive information or gain unauthorized access to your system.
- **Exclusions** - Websites you have decided to trust and allow connections to for the current session and future sessions.
- **PUA Sites** - Sites that host'Potentially Unwanted Applications' (PUA). While not strictly speaking malware, a PUA is a piece of software that has functionality that may not have been made clear to a user. An example is a browser toolbar which tells you the weather forecast, but which also tracks your online activity or serves you adverts.
- **Malicious Sites** - Sites that are known to host or contain links to malware, malicious scripts or deceptive content. These are intended to cause damage to your computer or steal personal

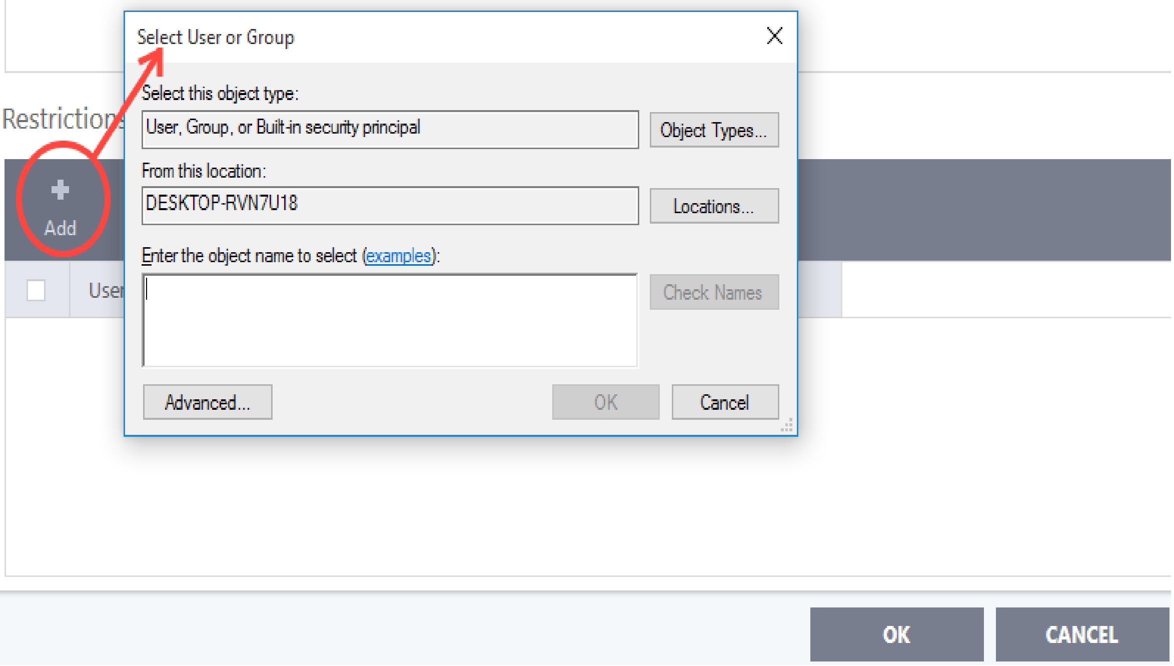
data.

- **Suspicious Sites -** Sites which have shown strong evidence of suspicious behavior but have not yet hosted content which would warrant placing them in the 'Malware' or 'Malicious' categories. Users are advised to be on high alert should they visit these sites.

See **Website Categories**, for more details on creating and modifying user specified categories.

5. Add 'Users' or 'User Groups' to whom the rule should be applied:

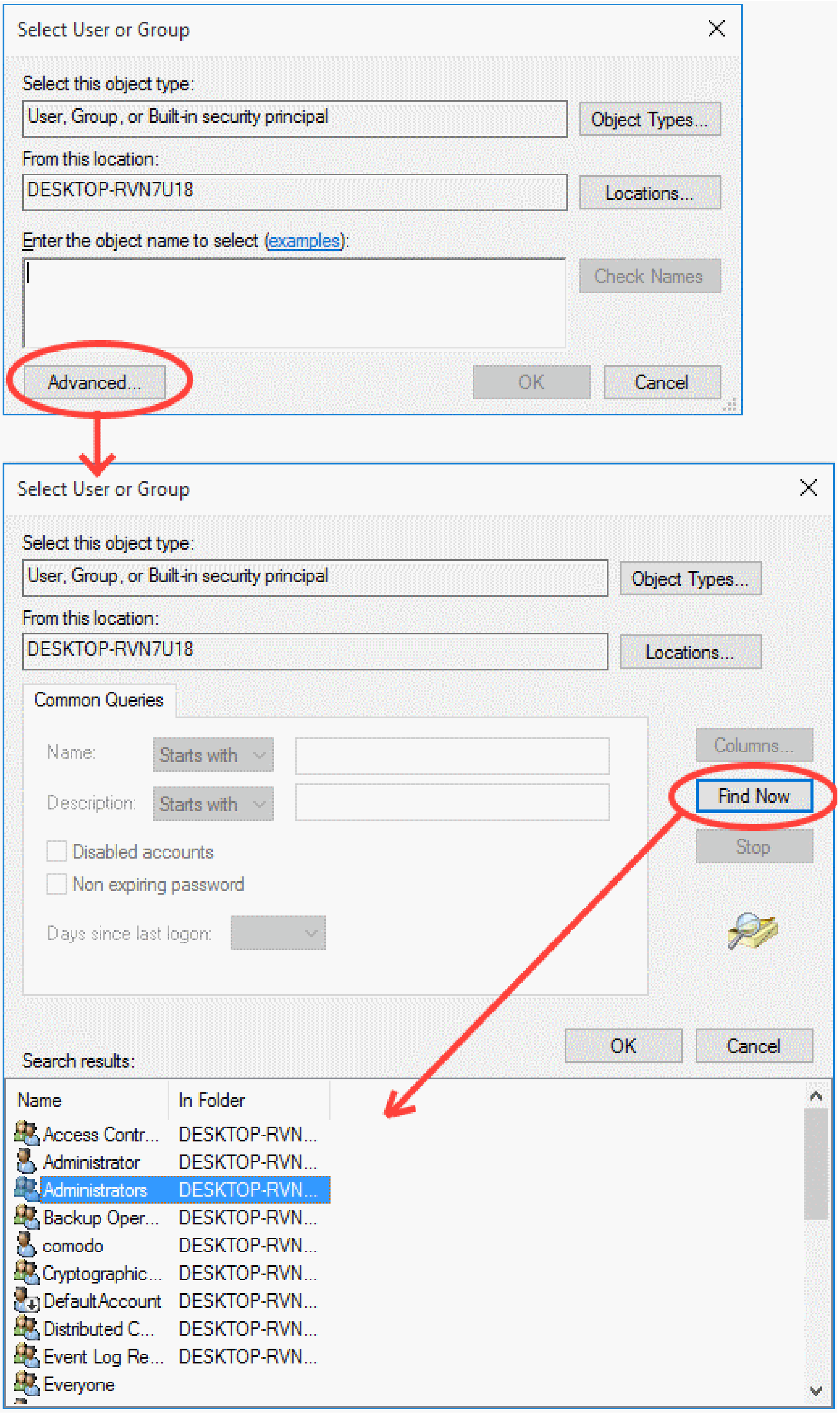
- Click the 'Add' button from the 'Restrictions' pane. The 'Select User or Group' dialog will appear:



- **Enter the object name to select -** add users to whom the filter should be applied. Names should be in the format:

  <domain name>\<user/group name> OR <user/group name>@<domain name>.

  Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



Select User or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
DESKTOP-RVN7U18

Enter the object name to select (examples):

Select User or Group

Select this object type:
User, Group, or Built-in security principal

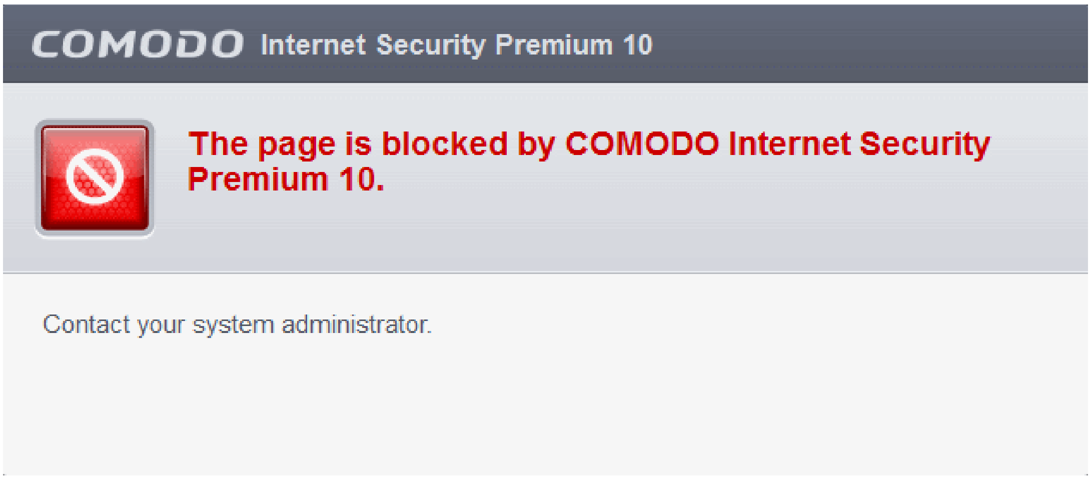
From this location:
DESKTOP-RVN7U18

Search results:

Name	In Folder
Access Contr...	DESKTOP-RVN...
Administrator	DESKTOP-RVN...
Administrators	DESKTOP-RVN...
Backup Oper...	DESKTOP-RVN...
comodo	DESKTOP-RVN...
Cryptographic...	DESKTOP-RVN...
DefaultAccount	DESKTOP-RVN...
Distributed C...	DESKTOP-RVN...
Event Log Re...	DESKTOP-RVN...
Everyone	

You next need to specify whether those users should be allowed or blocked from viewing the websites, or whether they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:

- **Allow -** The websites in the categories can be accessed by the user.
- **Block -** The websites in the categories cannot be accessed by the user.

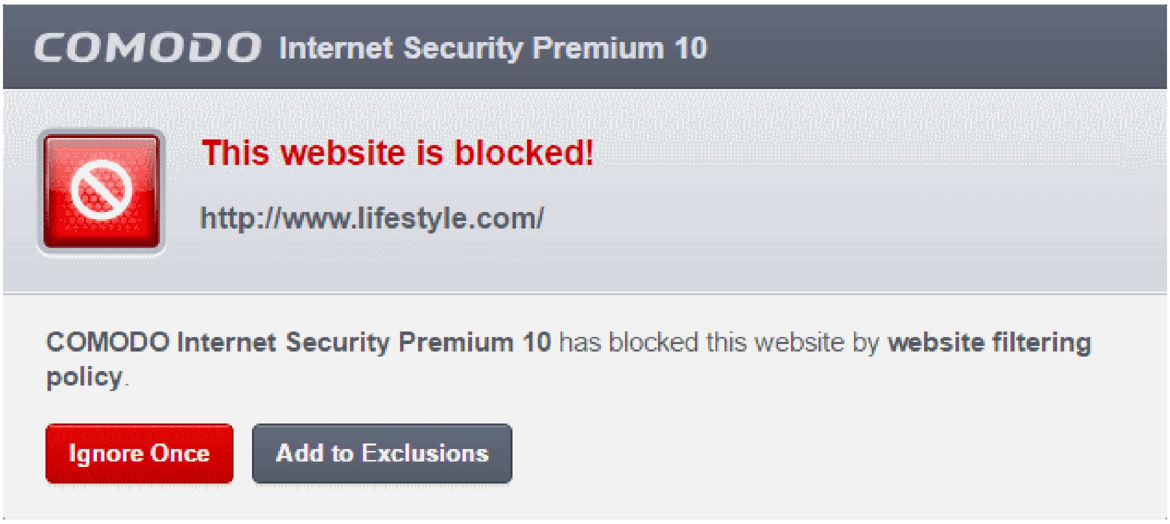


COMODO Internet Security Premium 10

The page is blocked by COMODO Internet Security Premium 10.

Contact your system administrator.

- **Ask -** An alert will be displayed in the browser (shown below) if the user tries to access any of the websites in the category. The user can decide whether to ignore it once or add it to exclusions list. If added to the exclusion list, the warning dialog will not appear for this website again. Please note that only the administrator can remove the websites from the exclusions list.



COMODO Internet Security Premium 10

This website is blocked!

http://www.lifestyle.com/

COMODO Internet Security Premium 10 has blocked this website by website filtering policy.

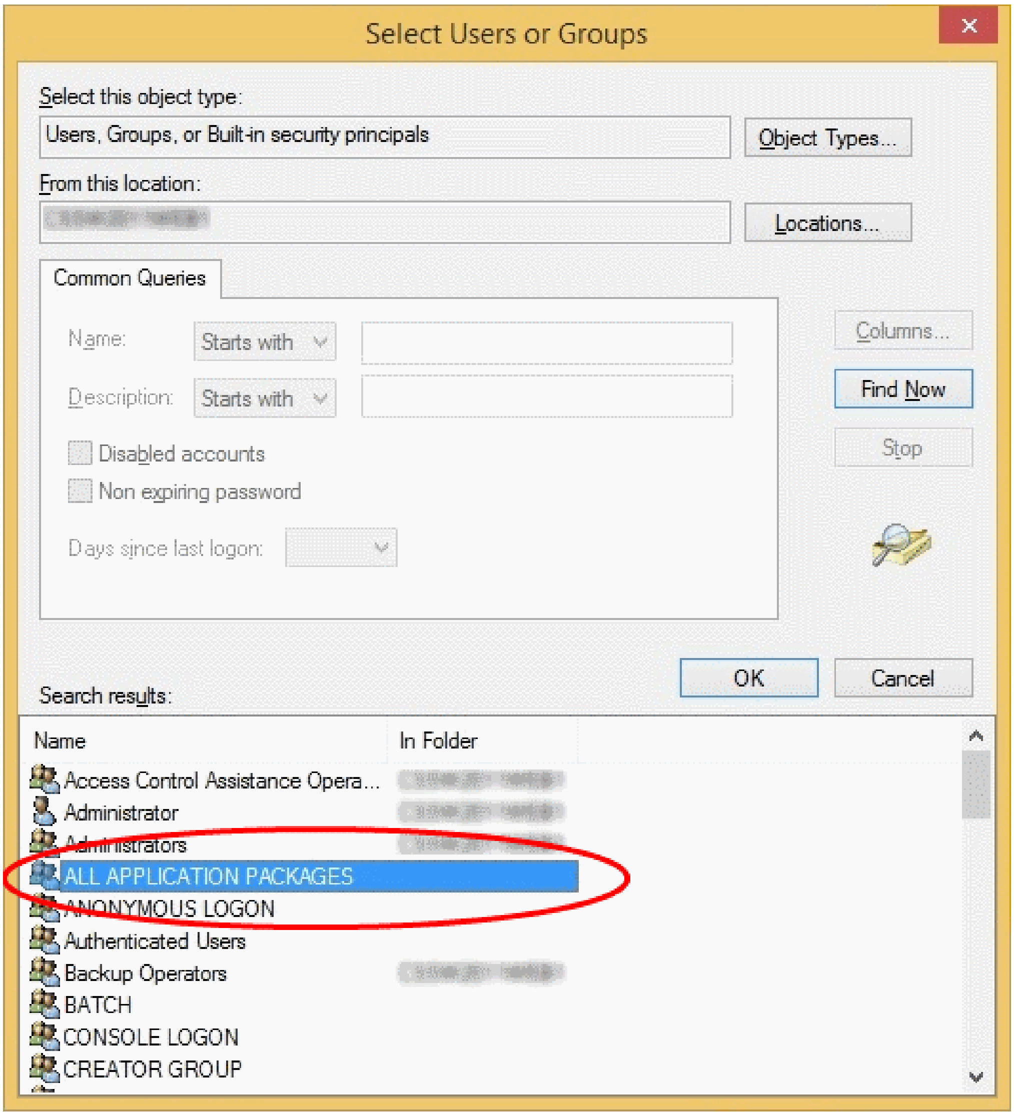
6. Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.
7. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
8. Make sure that the rule is enabled using the toggle switch under the 'Enable Rule' column for the rule to take effect.
    - You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Important Note to Windows 8 and Windows 8.1 users: If you are using Internet Explorer 11 version 11.0.9600.16384, it is mandatory to add the user group 'ALL APPLICATION PACKAGES' to the Restrictions list in addition to the intended users for each rule you create.

If you or other users access websites using Internet Explorer 11 on Windows 8/8.1, then you must add this user group or your rules will have no effect. For example, users will still be able to access blocked websites.

To add 'ALL APPLICATION PACKAGES' to the restrictions list

- Click 'Advanced' in the 'Select User or Group' dialog



Select Users or Groups

Select this object type:

Users, Groups, or Built-in security principals

From this location:

[redacted]

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

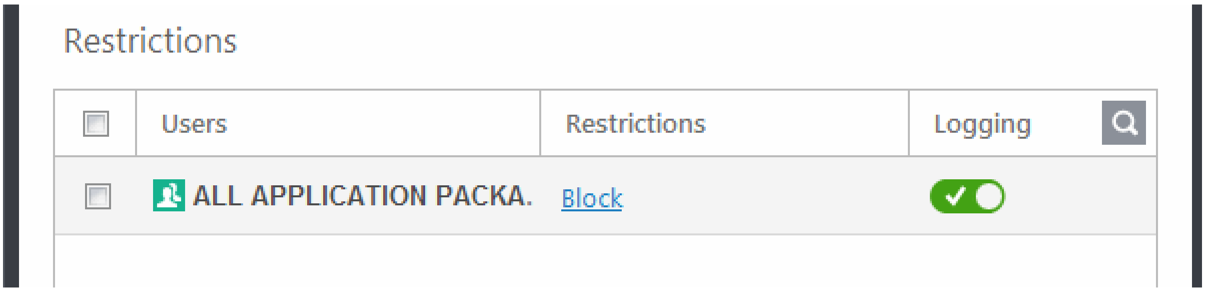
□ Non expiring password

Days since last logon:

Search results:

Name	In Folder
Access Control Assistance Opera...	[redacted]
Administrator	[redacted]
Administrators	[redacted]
ALL APPLICATION PACKAGES	
ANONYMOUS LOGON	
Authenticated Users	
Backup Operators	[redacted]
BATCH	
CONSOLE LOGON	
CREATOR GROUP	

- Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom
- Click 'OK'



Restrictions

□	Users	Restrictions	Logging
□	ALL APPLICATION PACKA.	Block	✓

To edit existing rules

1. Open the 'Website Filtering' Panel by clicking 'Settings' from the CIS home screen and then 'Website Filtering' from the 'Advanced Settings' interface.
2. Choose the website filtering rule to be edited under the 'Rules' tab by selecting the checkbox beside the rule.
3. Click the 'Edit' button at the top.

The ' Website Filtering Rule' interface for the selected rule will open. You can add/remove categories, add/remove users or change the restriction for selected users from this interface. See **To create a new Website Filtering Rule** for more details on this interface.

To remove a Website Filtering Rule

1. Open the 'Website Filtering' panel by clicking 'Settings' then 'Website Filtering' in the 'Advanced Settings' interface.
2. Open the 'Rules' tab. Choose the rule(s) you want to move by selecting the checkbox(es) beside the rule.
3. Click the 'Remove' button at the top.
4. Click 'OK'.

To change the priority of Website Filtering Rules

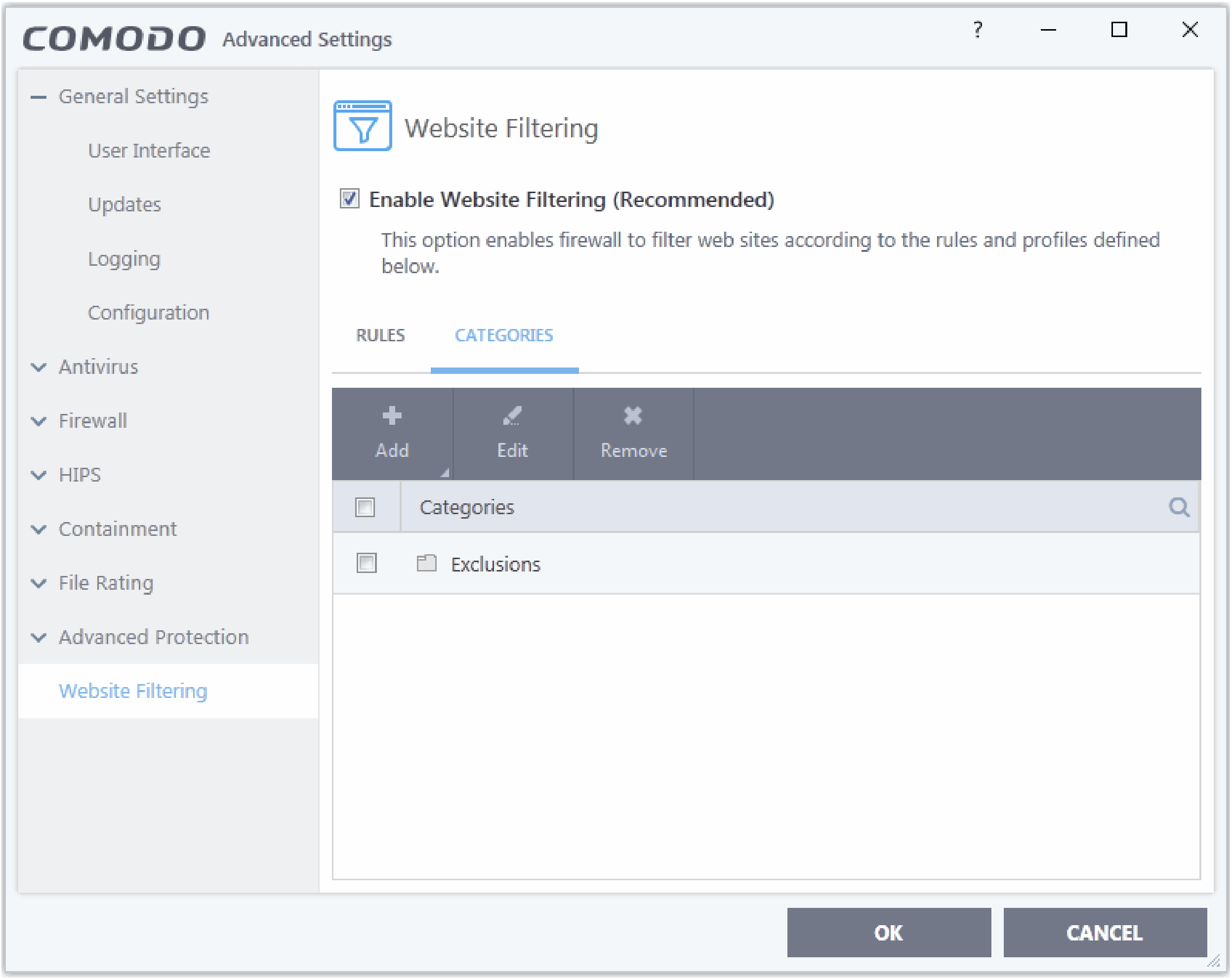
1. Open the 'Website Filtering' panel by clicking 'Settings' then 'Website Filtering' in the 'Advanced Settings' interface.
2. Open the 'Rules' tab. Choose the rule you want to move by selecting the checkbox beside the rule.
3. Click the 'Move Up' or 'Move Down' buttons to change the order of the rules.
4. Click 'OK'.

6.8.2. Website Categories

- The categories pane displays a list of built-in and user-defined web categories.
- Categories contain a list of 'Websites' which can be allowed or blocked in a rule.
- A 'Website' in a category can be specified as a URL or a simple phrase / term. You can use wildcard characters (*) with both URLs and terms.

To open the 'Website Filtering Categories' section

- Click 'Settings' at the top left of the CIS home screen to open the 'Advanced Settings' interface
- Click 'Website Filtering' on the left and choose the 'Categories' tab



Website Filtering

☑ Enable Website Filtering (Recommended)

This option enables firewall to filter web sites according to the rules and profiles defined below.

□	Categories
□	Exclusions

- Click the search icon to find a specific rule header. You can type rule names in full or in part.

The 'Categories' pane allows you to:

- Add a new category of websites
- Rename a category
- Remove unwanted websites from a category
- Remove a category

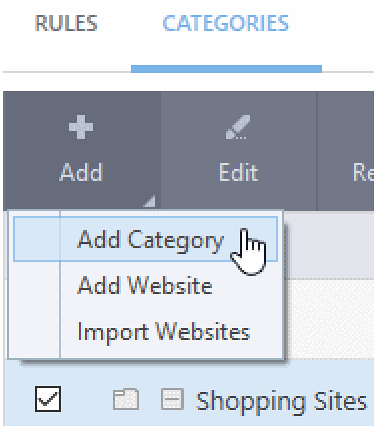
Adding a New Category of Websites

Adding a new category involves two steps:

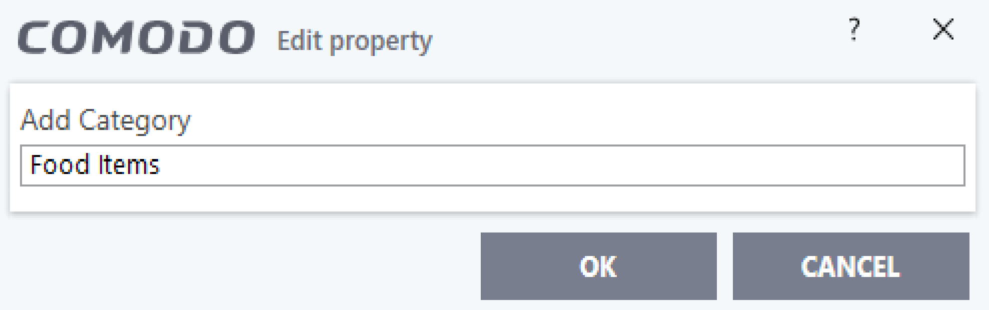
- Step 1 - Define a name for the category
- Step 2 - Add Websites to be included to the category

Step 1 - Define a name for the category

1. Open the 'Website Filtering' Panel by clicking 'Settings' on the CIS home screen then select 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the 'Categories' link to open the 'Categories' pane.
3. Click the 'Add' button at the top and select 'Add Category' from the drop-down menu.



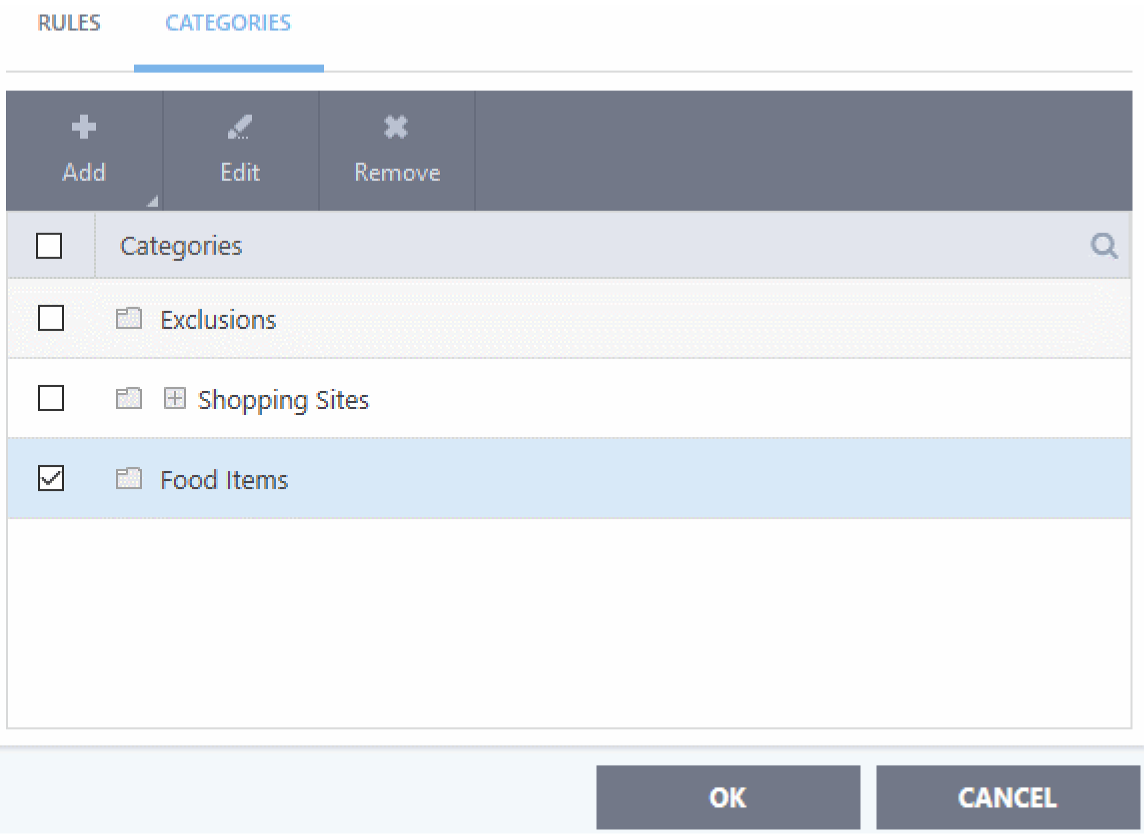
Type a name for the category in the 'Add Category' box:



Add Category

Food Items

The new category will be listed in the 'Categories' tab:



□	Categories
□	Exclusions
□	⊞ Shopping Sites
☑	Food Items

Next, add websites to be included in the category:

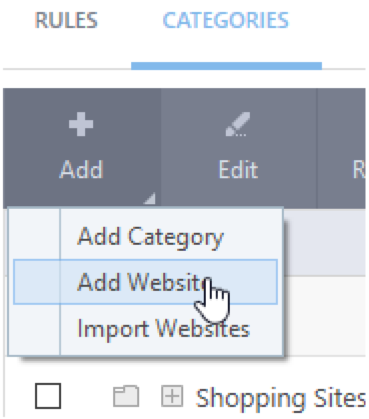
Step 2 - Add URLs to be included to the category

You can add websites to a category in two ways:

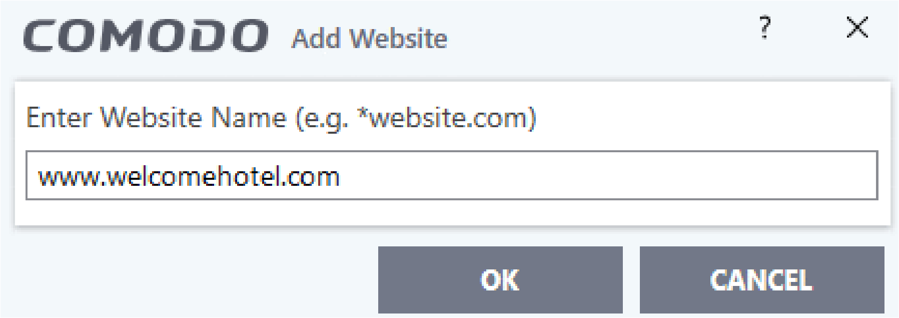
- Manually Specify Websites
- Upload Website URLs from a text file

To manually specify websites

1. Select the 'Category' from the list.
2. Click the 'Add' button.
3. Select 'Add Website' from the drop-down menu.



Type the address of the website you wish to add to the category in the 'Add Website' box:



Enter Website Name (e.g. *website.com)

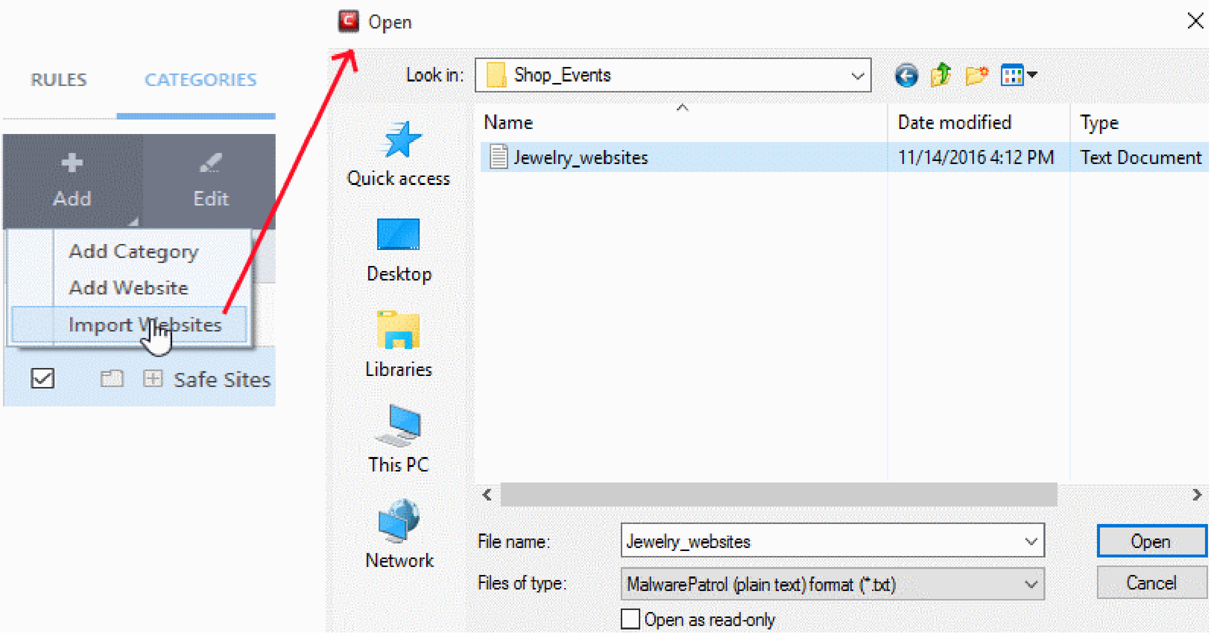
www.welcomehotel.com

- To add a specific webpage, enter the full path to the page.
- To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
- To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, *pizza** will cover 'pizzahut.com', 'pizzacorner.net', and so on.
- To include all the websites with URLs that contain a specific string, add the wildcard character before and after the string. For example, **pizza** will cover hotpizza.com, spicypizza.net and so on.
- Click 'OK'.
- The website will be added to the category.

4. Repeat the process to add more websites.

To upload a list of websites from a text file

1. Select the target category from the list.
2. Click the 'Add' button and select 'Import Websites' from the drop-down menu.
3. Navigate to the file containing your list of URLs.



Note: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.

4. Click 'Open'.

CIS will automatically add the websites specified in the text file into the selected category.

To rename a category

1. Open the 'Website Filtering' panel by clicking 'Settings' on the CIS home screen then 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the 'Categories' link to open the 'Categories' pane.
3. Select the category to be renamed.
4. Right-click and select 'Edit' from the drop-down menu.
5. Enter the new name of the category in the 'Edit Property' dialog box and click 'OK'.

The category will be renamed immediately both under the 'Categories' section and in the 'Website Filtering Rules' to which it is applied.

To remove a Website from a category

1. Open the 'Website Filtering' Panel by clicking 'Settings' from the CIS home screen then select 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the 'Categories' link to open the 'Categories' pane.
3. Click the '+' button beside the category to be edited to expand the website list.
4. Select the Website(s) to be removed.

5. Right-click then select 'Remove' from the drop-down menu.

To remove a Category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' link to open the 'Categories' pane.
3. Select the 'Category' to be removed.
4. Right-click then select 'Remove' from the drop-down menu.

Note: You cannot remove a category if it is currently being used in a website filtering rule. Make sure to first remove the category from any rules in which it is applied.

7. Comodo GeekBuddy

Comodo GeekBuddy is a personalized computer support service provided by friendly computer experts at Comodo. If you have any issues at all with your computer, simply ask your GeekBuddy technician if they can help you out. Click the GeekBuddy icon to begin a chat session.

After requesting your permission, they can even establish a remote connection to your PC and fix the problems right in front of your eyes. No longer do you need to make time consuming calls to help desk support staff - just sit back while our friendly technicians do the work for you.

Visit **https://www.geekbuddy.com/** for more details.

If you have opted not to include GeekBuddy during CIS installation, you can download and install GeekBuddy by clicking 'Live Support' link

at the top of the home screen:

GeekBuddy is included with CIS Pro and Complete. The GeekBuddy section of this guide is broken down into the following sections:

- **Overview of the Services**
- **Activation of Service**
- **Launching the Client and Using the Service**
- **Setting up your Profile Information**
- **Accepting Remote Desktop Requests**
- **Uninstalling Comodo GeekBuddy**

7.1. Overview of Services

Comodo GeekBuddy includes the following services:

- **Virus & Malware Diagnosis / Removal** - Our technicians remotely clear any detected viruses or malware found on your PC.
- **Internet and Online Identity Security** - Optimization of your computer's security settings to prevent loss of sensitive data and identity theft.
- **Printer or Email Account Setup** - Installation or updating of printer software and/or drivers, checking ink levels and configuring your printer to work on a wireless or wired network. We set up your Internet-based email account - any provider, any account. Great for new computers and novice email users.
- **Software Activation** - Installation, configuration, and activation of third party software in your system.
- **General PC Troubleshooting** - Detailed system check to identify and eliminate basic hardware and software conflicts in your Windows PC.

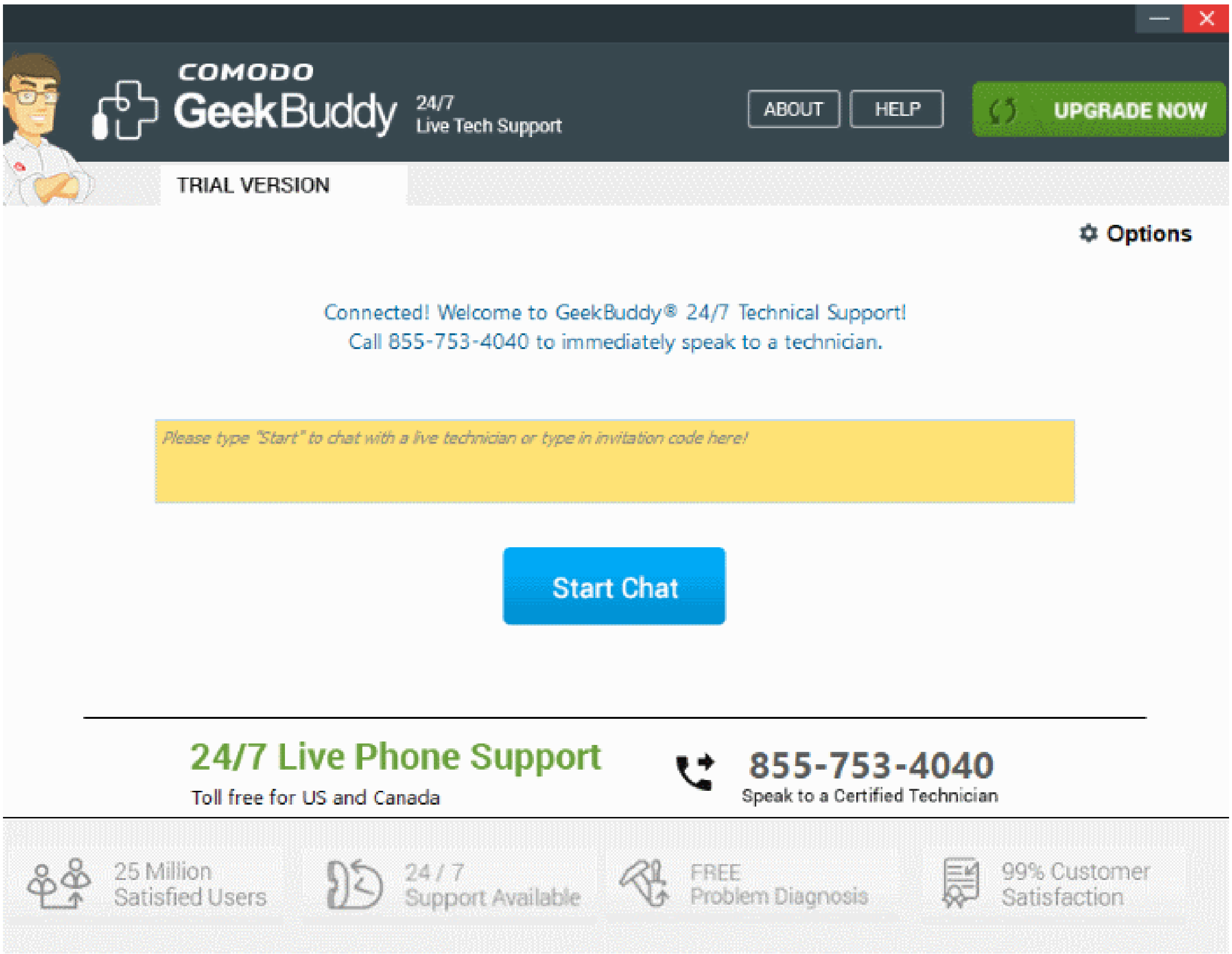
- **Computer Power Setting Optimization -** Optimization of your power management settings based on how you use your computer. Your Geek will help you go green and save money on your electric bill.
- **Printer Set Up -** Let a PC pro install or update software and printer drivers, check ink levels, and configure your printer to work on a wireless or wired network.
- **Comodo Software Installation and Set up -** Installation and support of software supplied by Comodo.
- **Comodo Account Questions -** Clarification of any doubts regarding your account in Comodo.

7.2. Activation of Service

Note - CIS Pro and Complete users can skip this section and go straight to '**Launching the Client and Using the Service**'.

GeekBuddy is installed with Comodo Internet Security with a trial license, but to use the full service, you have to purchase and activate a full license. To do this:

- Start the GeekBuddy client by clicking the desktop shortcut or from the 'Start Menu'.
- The GeekBuddy Chat screen will be displayed.



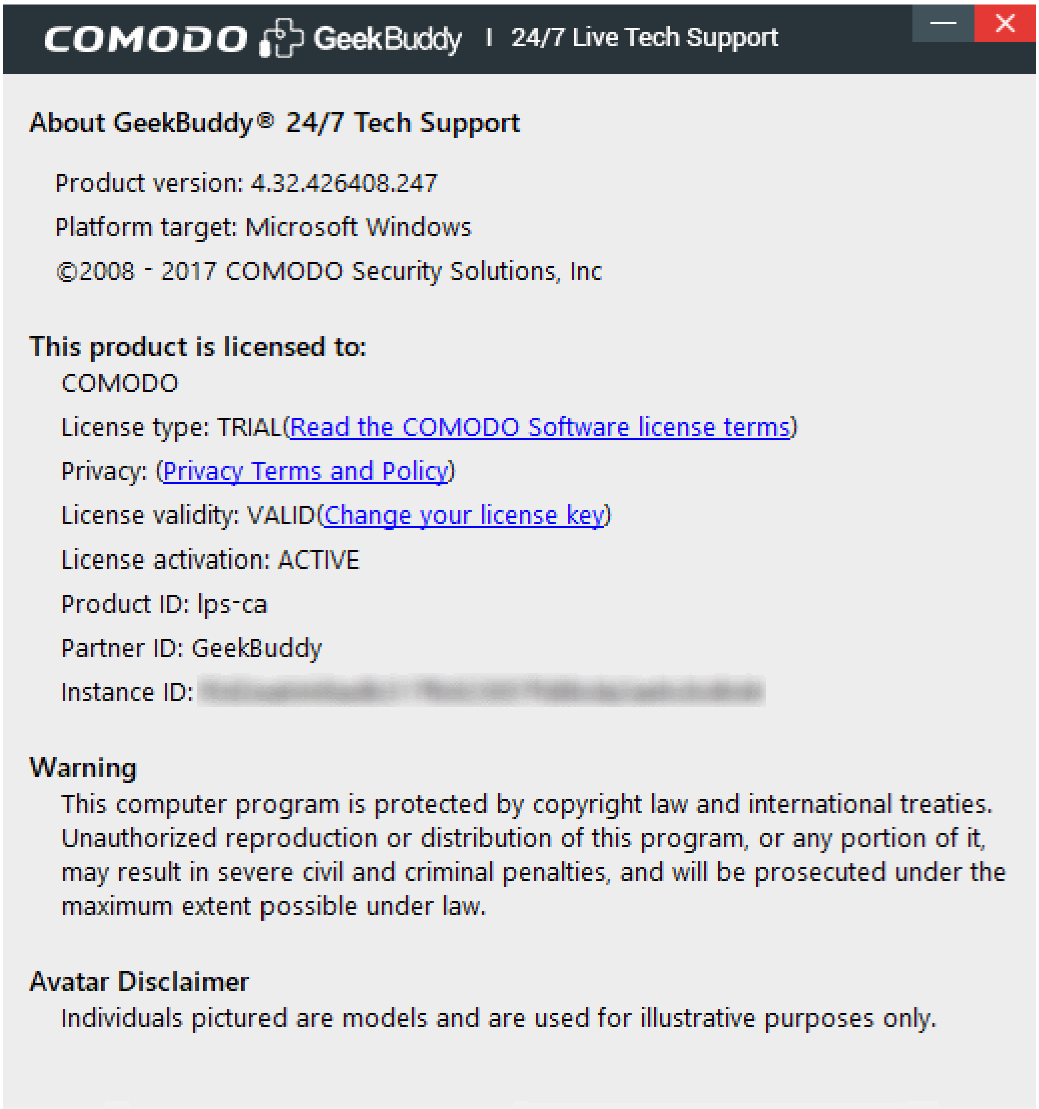
Connected! Welcome to GeekBuddy® 24/7 Technical Support!
Call 855-753-4040 to immediately speak to a technician.

Please type "Start" to chat with a live technician or type in invitation code here!

24/7 Live Phone Support
Toll free for US and Canada

855-753-4040
Speak to a Certified Technician

- Click the 'About' button at the top to open the 'About' GeekBuddy screen



About GeekBuddy® 24/7 Tech Support

Product version: 4.32.426408.247

Platform target: Microsoft Windows

©2008 - 2017 COMODO Security Solutions, Inc

This product is licensed to:

COMODO

License type: TRIAL(Read the COMODO Software license terms)

Privacy: (Privacy Terms and Policy)

License validity: VALID(Change your license key)

License activation: ACTIVE

Product ID: lps-ca

Partner ID: GeekBuddy

Instance ID: [redacted]

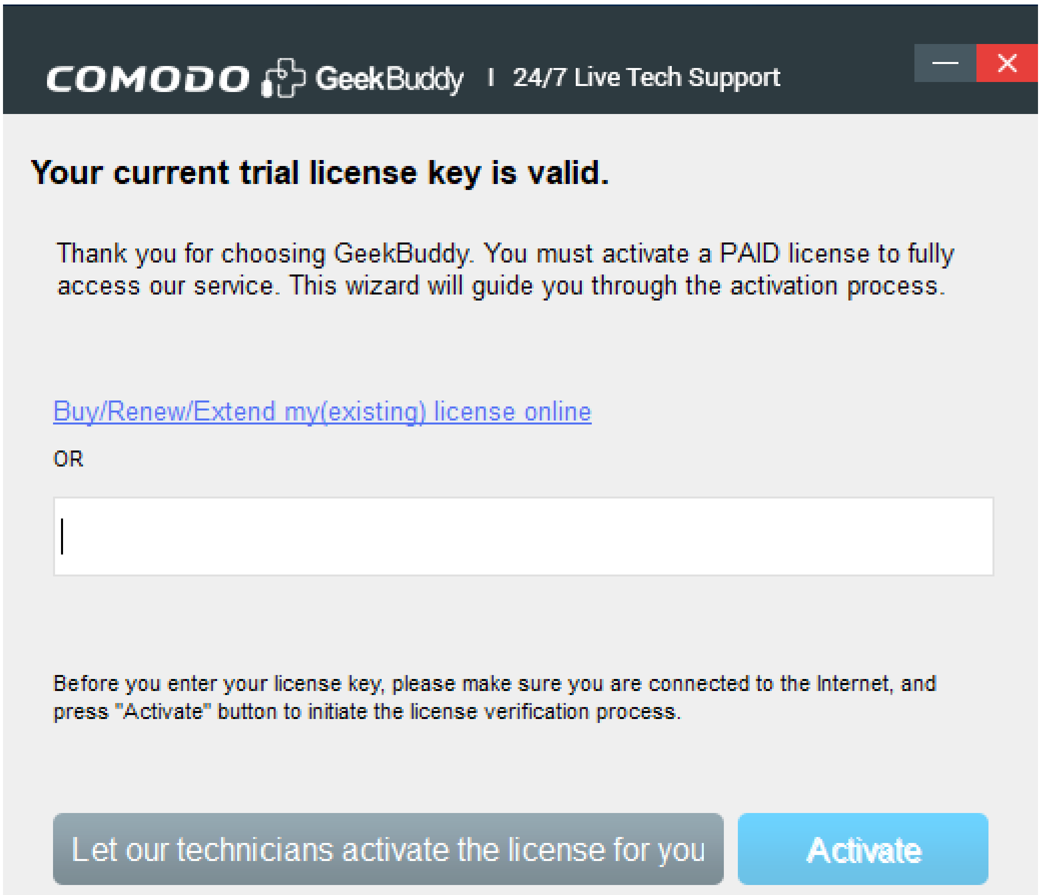
Warning

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted under the maximum extent possible under law.

Avatar Disclaimer

Individuals pictured are models and are used for illustrative purposes only.

- Click 'Change your license key' to open the license management dialog:


COMODO GeekBuddy I 24/7 Live Tech Support

Your current trial license key is valid.

Thank you for choosing GeekBuddy. You must activate a PAID license to fully access our service. This wizard will guide you through the activation process.

Buy/Renew/Extend my(existing) license online
OR

Before you enter your license key, please make sure you are connected to the Internet, and press "Activate" button to initiate the license verification process.

Let our technicians activate the license for you
Activate

- Click 'Buy/Renew/Extend...' to purchase a license online.
- If you have purchased a license and received an activation code, enter it in the field provided and click 'Activate'.

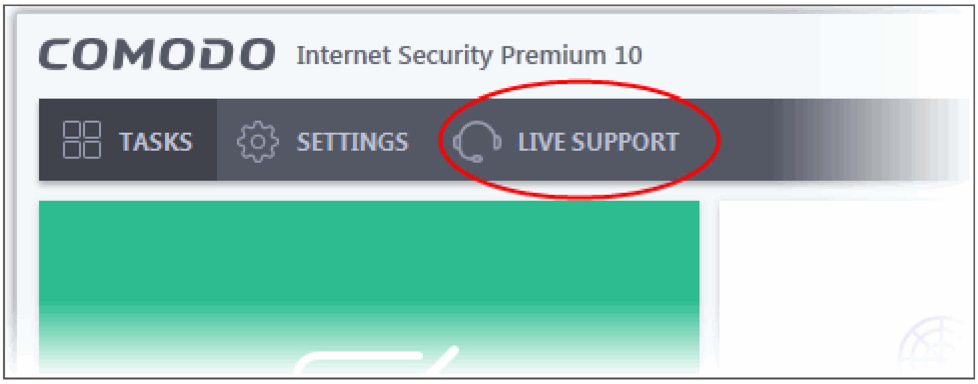
Once your code has been verified, your license will become active and you can begin using the service. Click the following links for more details:

- **Launching the Client and Using the Service**
- **Setting up your Profile Information**
- **Using Free Diagnostic Reports**
- **Scanning My PC**

7.3.Launching the Client and Using the Service

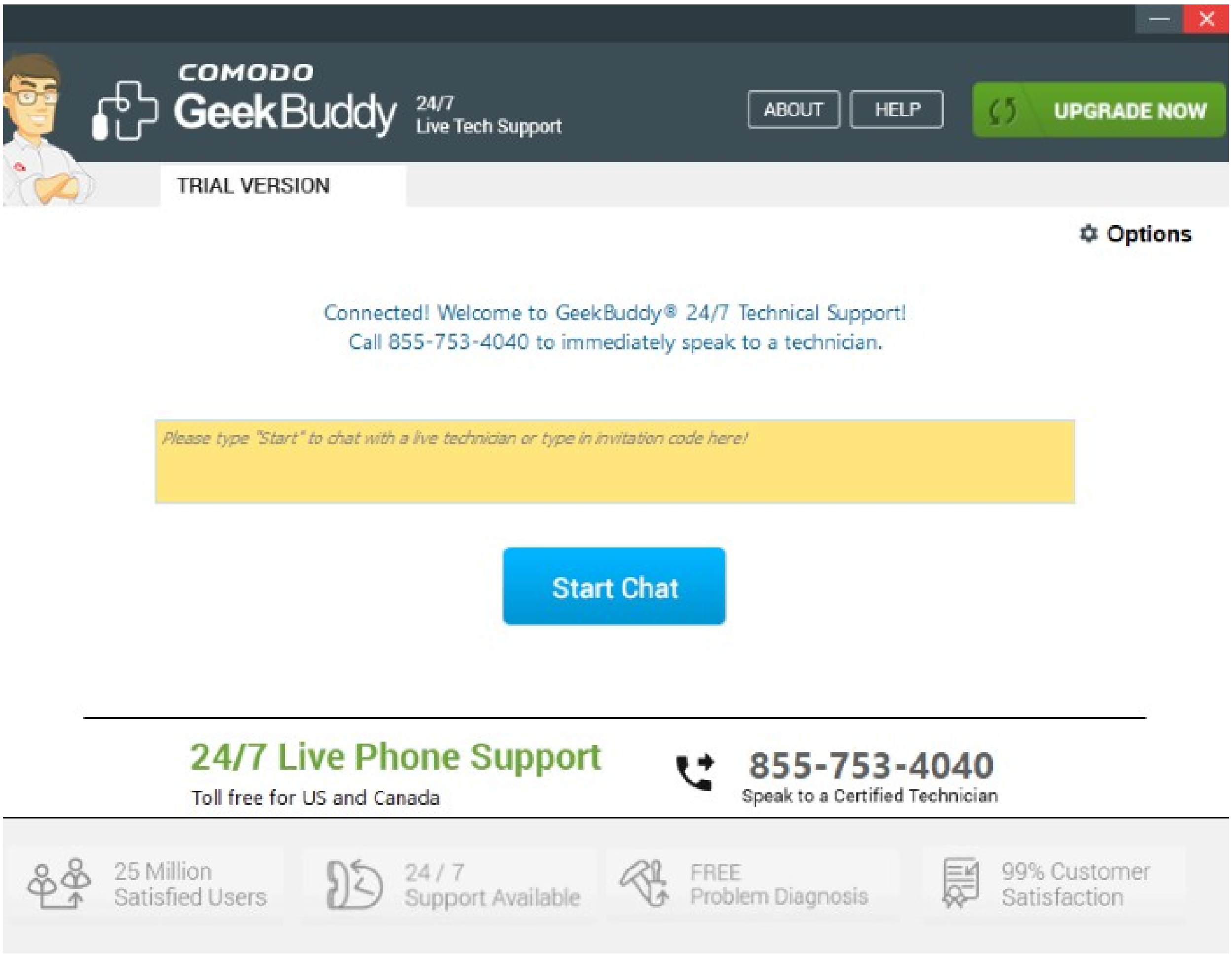
You can start a live chat with a GeekBuddy expert using one of the following methods:

- Double click the GeekBuddy desktop ico
- Click 'Live Support' at the top right of the CIS interface:



- From the Windows Start Menu: *Start* > *All Programs* > *Comodo* > *GeekBuddy* > *GeekBuddy*

The GeekBuddy 'Home' screen will open. To contact a support technician, type your issue in the field or enter an invitation code and click the 'Start Chat' button.

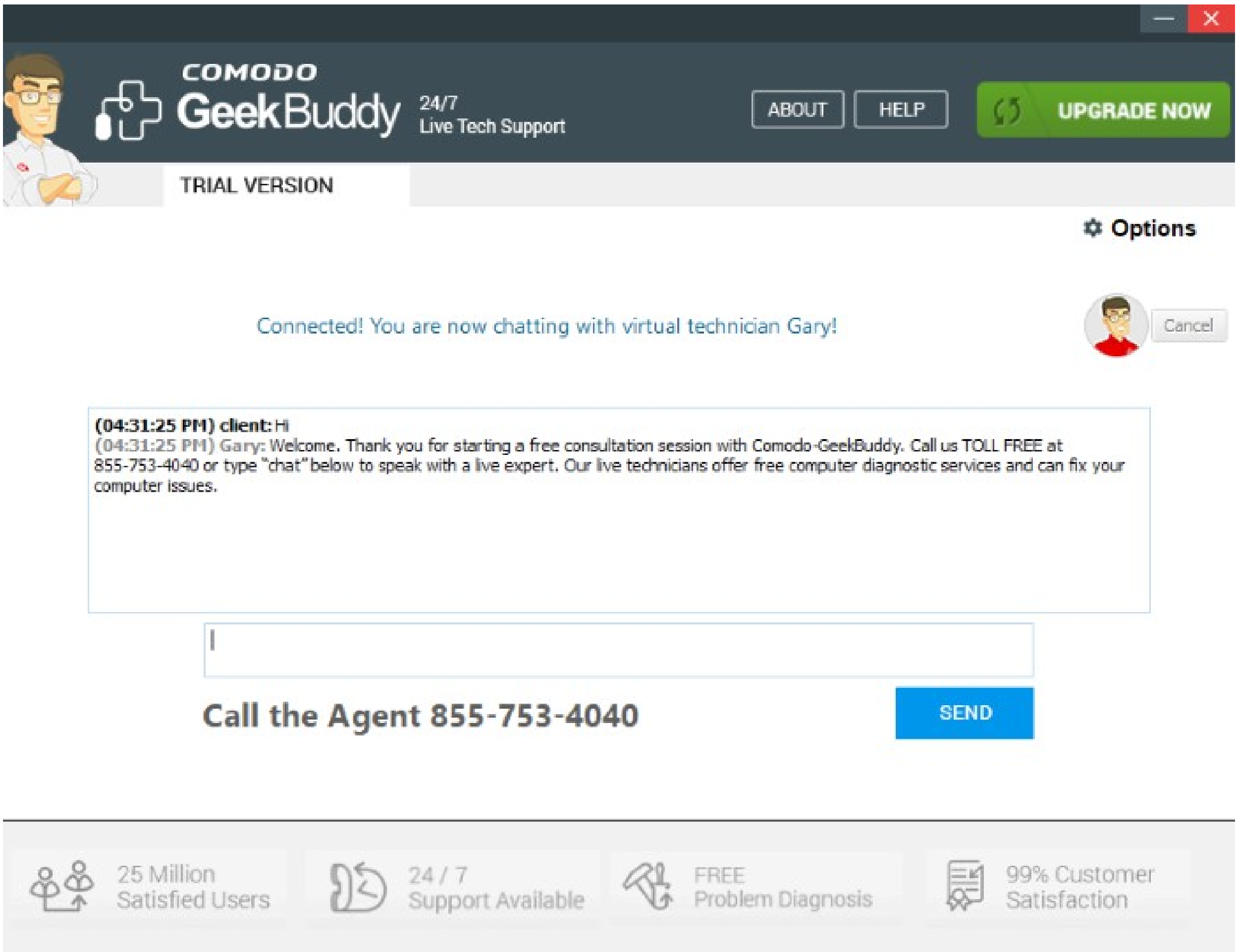

COMODO
GeekBuddy 24/7 Live Tech Support
ABOUT
HELP
UPGRADE NOW
TRIAL VERSION
Options

Connected! Welcome to GeekBuddy® 24/7 Technical Support!
Call 855-753-4040 to immediately speak to a technician.

Please type "Start" to chat with a live technician or type in invitation code here!

Start Chat
24/7 Live Phone Support
Toll free for US and Canada
855-753-4040
Speak to a Certified Technician
25 Million Satisfied Users
24 / 7 Support Available
FREE Problem Diagnosis
99% Customer Satisfaction

- You will be immediately connected to a GeekBuddy.



Connected! You are now chatting with virtual technician Gary!

(04:31:25 PM) client: Hi
(04:31:25 PM) Gary: Welcome. Thank you for starting a free consultation session with Comodo-GeekBuddy. Call us TOLL FREE at 855-753-4040 or type "chat" below to speak with a live expert. Our live technicians offer free computer diagnostic services and can fix your computer issues.

Call the Agent 855-753-4040

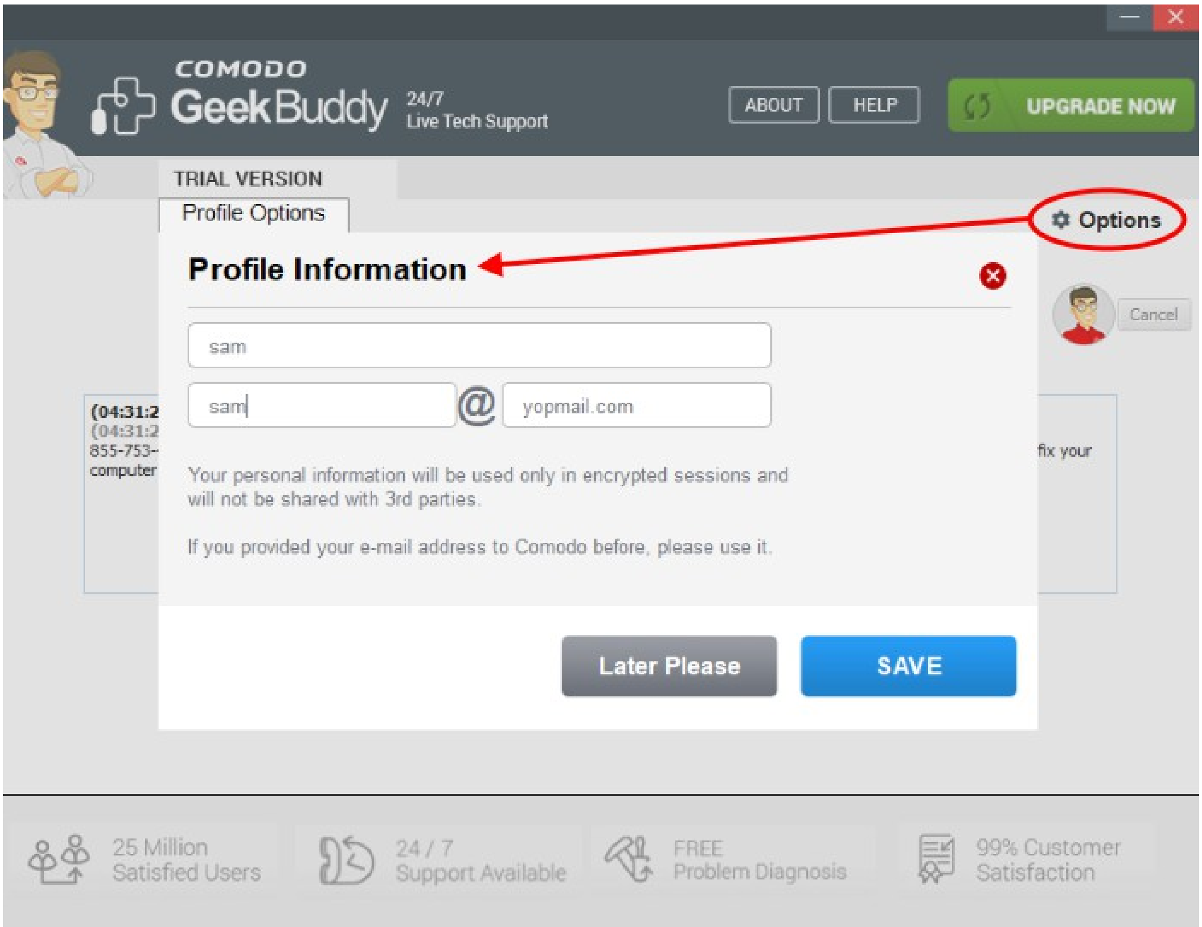
Chat away! Ask for help with any issue that you are experiencing with your PC. The technician will assess your problem, offer advice, work with you to fix issues, and can even connect to your PC and perform system maintenance.

7.4. Setting up your Profile Information

The profile options page also allows you to subscribe to Comodo news and alerts, giving you the inside track on the latest security news, product developments and offers. Enroll today and you'll be the first to know about the next Comodo breakthrough.

To add your profile information

- Launch Comodo Geekbuddy
- Click 'Options'
- Enter your name and email address



Profile Information

sam

sam @ yopmail.com

Your personal information will be used only in encrypted sessions and will not be shared with 3rd parties.

If you provided your e-mail address to Comodo before, please use it.

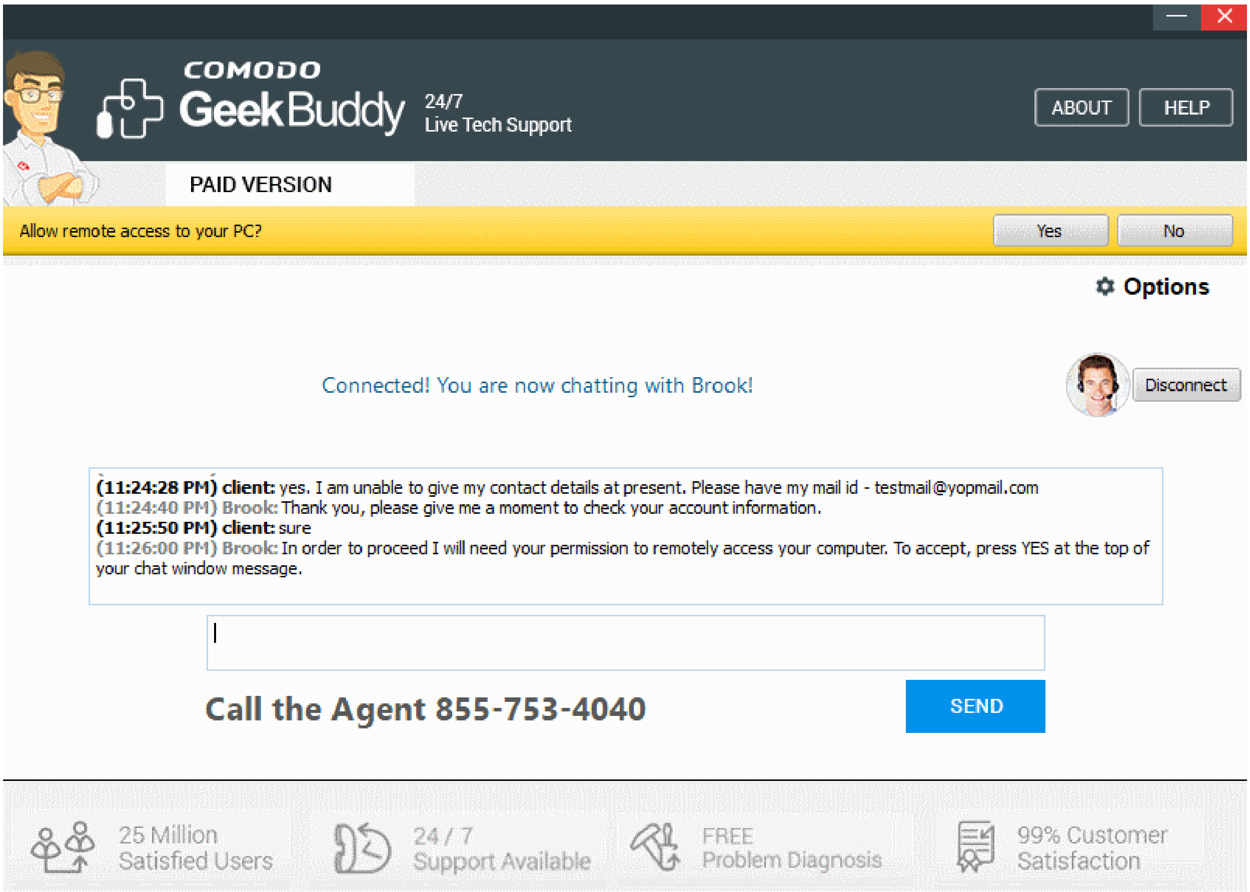
Later Please

SAVE

- Click 'Save'
- Click 'Later Please' to postpone the action

7.5. Accepting Remote Desktop Requests

In order to solve certain issues, the support technician may need to directly connect to your computer via a remote connection. Remote connections can only go ahead if you grant permission for this to happen. Our technicians will always request your permission in the chat window.:



(11:24:28 PM) client: yes. I am unable to give my contact details at present. Please have my mail id - testmail@yopmail.com
(11:24:40 PM) Brook: Thank you, please give me a moment to check your account information.
(11:25:50 PM) client: sure
(11:26:00 PM) Brook: In order to proceed I will need your permission to remotely access your computer. To accept, press YES at the top of your chat window message.

Call the Agent 855-753-4040
SEND
25 Million Satisfied Users
24 / 7 Support Available
FREE Problem Diagnosis
99% Customer Satisfaction

- Click the 'Yes' button in the yellow bar to allow the technician to connect to your computer.

The technician will subsequently ask your permission before he or she makes any changes to your machine. Such changes might include installing programs, creating system restore points or deleting unnecessary/infected files. You can approve the requests directly by typing your message and clicking 'SEND'.

Upon completion of their work, the technician will disconnect from your computer, inform you that the requested tasks have been completed and ask whether you would like help with anything else.

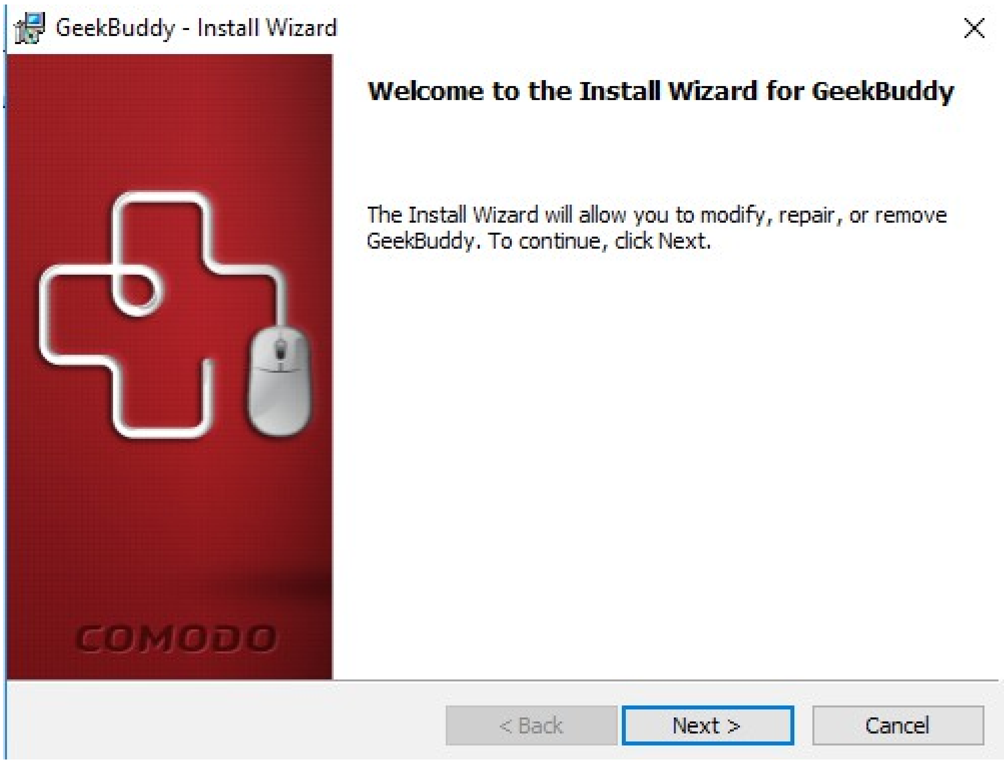
- If you have more questions, simply carry on chatting.
- If you wish to end the remote desktop session, click the 'Disconnect' button.

Congratulations, you just finished your first GeekBuddy support session. We hope you enjoy using your trouble-free computer.

7.6. Uninstalling Comodo GeekBuddy

To uninstall Comodo GeekBuddy

- Open the Windows 'Control Panel' then open 'Programs And Features' ('Add/Remove Programs' in older versions of Windows).
- Select 'GeekBuddy' from the list of currently installed programs then click 'Uninstall' at the top.



Welcome to the Install Wizard for GeekBuddy

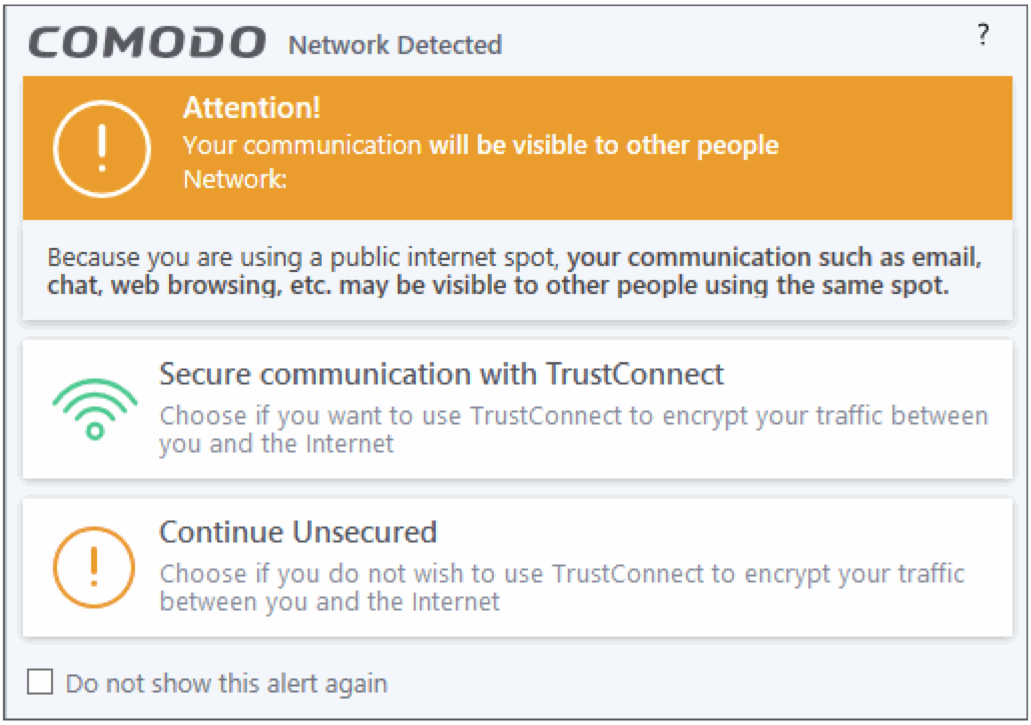
The Install Wizard will allow you to modify, repair, or remove GeekBuddy. To continue, click Next.

The uninstall wizard will begin. Run the wizard to remove GeekBuddy.

- Choose a reason for uninstalling from the list of options and click 'Remove'.

8. TrustConnect Overview

- Comodo TrustConnect is a secure Internet proxy service that creates an encrypted session when users are accessing the Internet over public wireless connections.
- Since these wireless sessions can be relatively easily intercepted, they present a significant data vulnerability gap for businesses and consumers alike.
- Whenever Comodo Internet Security detects unsecured wireless connections it will present you with the opportunity to use your TrustConnect account for the connection.



COMODO Network Detected ?

Attention!
Your communication will be visible to other people
Network:

Because you are using a public internet spot, your communication such as email, chat, web browsing, etc. may be visible to other people using the same spot.

Secure communication with TrustConnect
Choose if you want to use TrustConnect to encrypt your traffic between you and the Internet

Continue Unsecured
Choose if you do not wish to use TrustConnect to encrypt your traffic between you and the Internet

□ Do not show this alert again

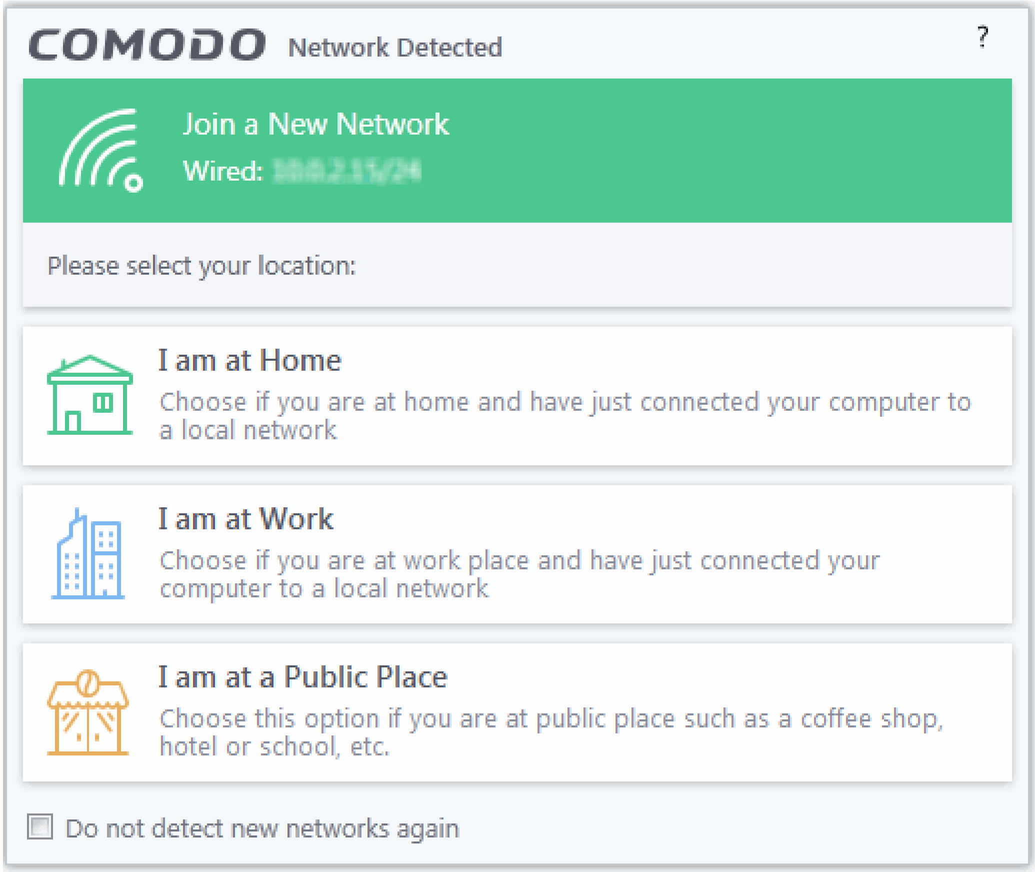
- TrustConnect is designed to eliminate these types of data hijacks by preventing criminals from attacking or scanning your system from the local network that you are using to connect to the Internet.
- It also encrypts all of your traffic destined for the Internet (including Web site addresses, instant messaging conversations, personal information, plain text usernames and passwords and other important information).
- After connecting to the service, the TrustConnect software indicates that traffic is being encrypted as it leaves your system.
- Data thieves and hackers cannot 'sniff' or intercept your data
- They can't determine where your information is coming from because, as you are connecting to the Internet through a **SSL** secured VPN connection to the TrustConnect servers, your requests appear to come from our IP address. Ordinarily, cyber criminals could easily intercept these broadcasts.
- Setting up Comodo TrustConnect is easy, as it works on most operating systems (Windows, Mac OS X) as well as with most firewall applications.
- Typical setup takes less than three minutes. TrustConnect clients are available for Windows, Mac OS, Linux and iPhone mobile devices and can be downloaded by logging into your account at **https://accounts.comodo.com/account/login**.
- Your Comodo Internet Security Complete confirmation email contains confirmation of your the username that you set up during initial sign up and a subscription ID for the service.
- Once logged in, click the TrustConnect tab to add subscriptions, change billing and contact information, and review the ongoing status of your service.
- Your Comodo Internet Security Complete TrustConnect account has a 10 GB/month data transfer limit.
- **Comodo Internet Security - Complete** customers also receive the $99 value 'Live, Expert Computer Support' Comodo GeekBuddy. Please visit **http://www.geekbuddy.com**/ for full product details.
- **TrustConnect System Requirements**
  - Windows 10
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP

- Vac OS X
- Linux (containing kernel 2.4 or later)
- FreeBSD, OpenBSD

For users of Comodo Internet Security, TrustConnect is integrated with the application and need not install the TC client in their systems.

Comodo Internet Security Complete Users

CIS Complete product includes TrustConnect services the application is installed automatically along with CIS. When a new wireless connection is established by your system, a Network Detected dialog will be displayed.



COMODO Network Detected ?

Join a New Network

Wired: [redacted]

Please select your location:

I am at Home

Choose if you are at home and have just connected your computer to a local network

I am at Work

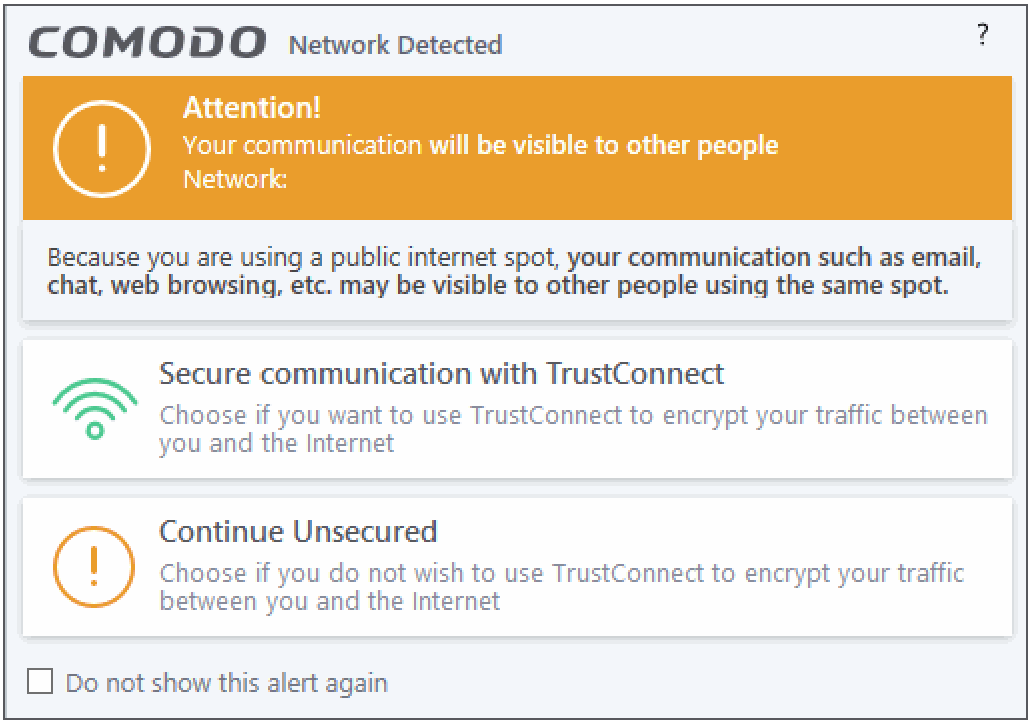
Choose if you are at work place and have just connected your computer to a local network

I am at a Public Place

Choose this option if you are at public place such as a coffee shop, hotel or school, etc.

□ Do not detect new networks again

Select your location from the dialog. A TrustConnect alert will be displayed depending on the settings configured in **Firewall Settings** interface.



COMODO Network Detected

?

Attention!
Your communication **will be visible to other people**
Network:

Because you are using a public internet spot, **your communication such as email, chat, web browsing, etc. may be visible to other people using the same spot.**

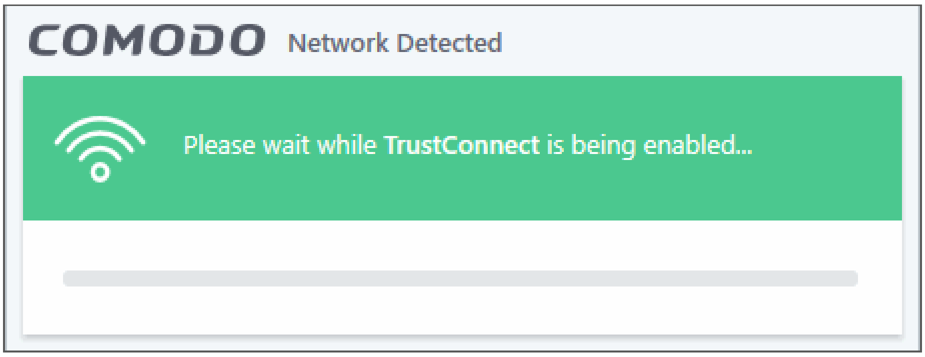
Secure communication with TrustConnect
Choose if you want to use TrustConnect to encrypt your traffic between you and the Internet

Continue Unsecured
Choose if you do not wish to use TrustConnect to encrypt your traffic between you and the Internet

□ Do not show this alert again

Select whether you want to connect to the Internet via TrustConnect thus encrypting the traffic between your system and the Internet or use the unsecured network.

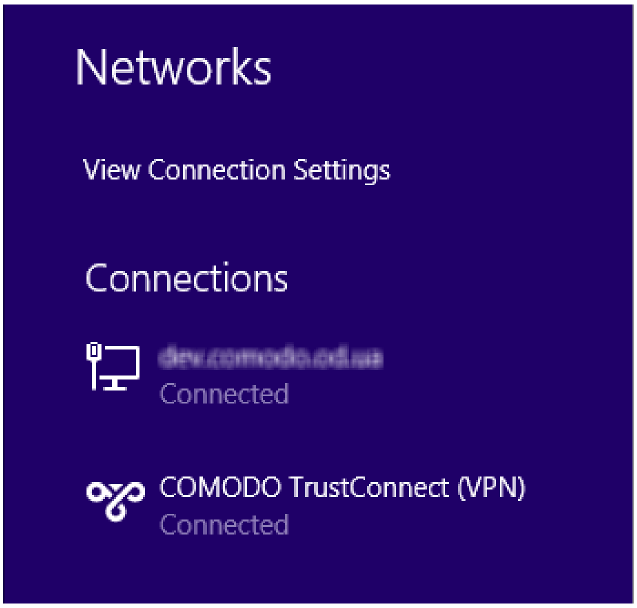
If you choose 'Secure communication with TrustConnect', CIS will establish the connection via TC...



COMODO Network Detected

Please wait while **TrustConnect** is being enabled...

...and on successful connection, you can view the details in the system tray.



Networks

View Connection Settings

Connections

[redacted]
Connected

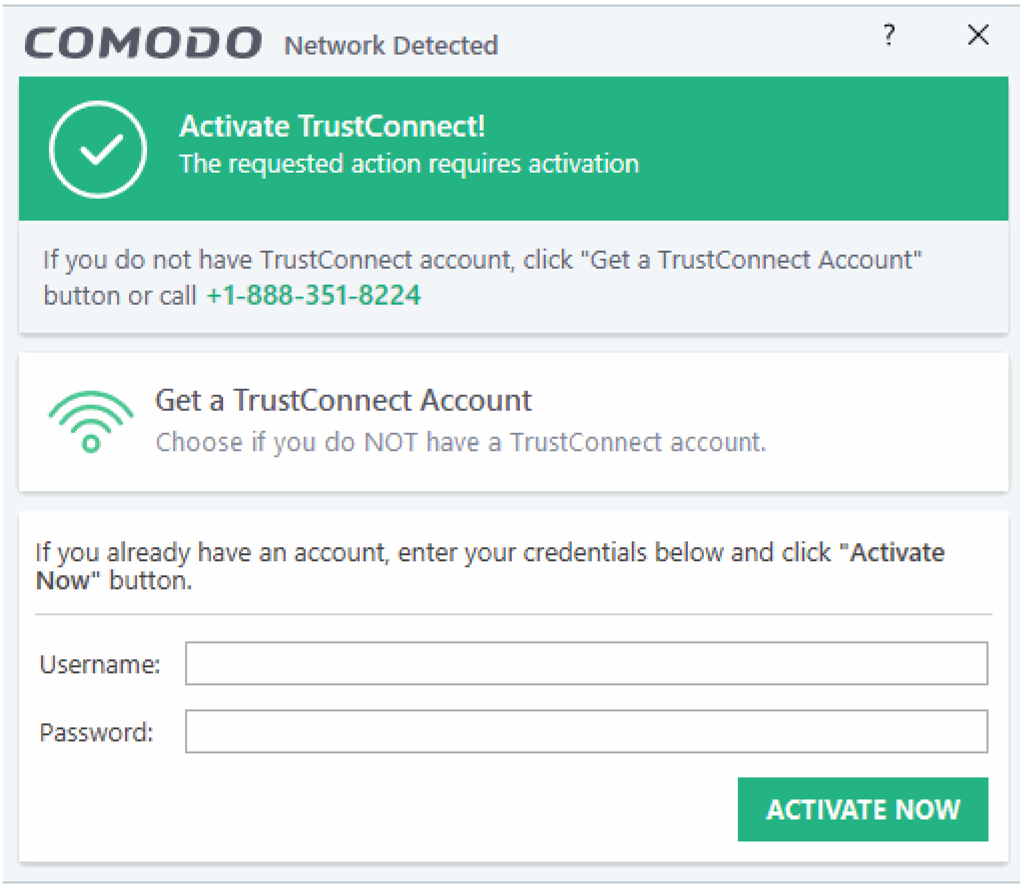
COMODO TrustConnect (VPN)
Connected

Choose 'Continue Unsecured' option if you do not want to establish an encrypted connection.

Comodo Internet Security Pro / Free Users

TrustConnect service is not included with CIS Pro / free and these users should subscribe for using the service. When the option 'Secure communication with TrustConnect is selected, a 'Activate TrustConnect' dialog will be displayed.

- You can purchase the TC service by clicking the 'Get a TrustConnect Account', enter the TC service credentials and activate the service.
- If you already have a TC account, enter the TC service credentials in the Username and Password fields and click the 'Activate Now' button.



COMODO Network Detected

Activate TrustConnect!
The requested action requires activation

If you do not have TrustConnect account, click "Get a TrustConnect Account" button or call +1-888-351-8224

Get a TrustConnect Account
Choose if you do NOT have a TrustConnect account.

If you already have an account, enter your credentials below and click "**Activate Now**" button.

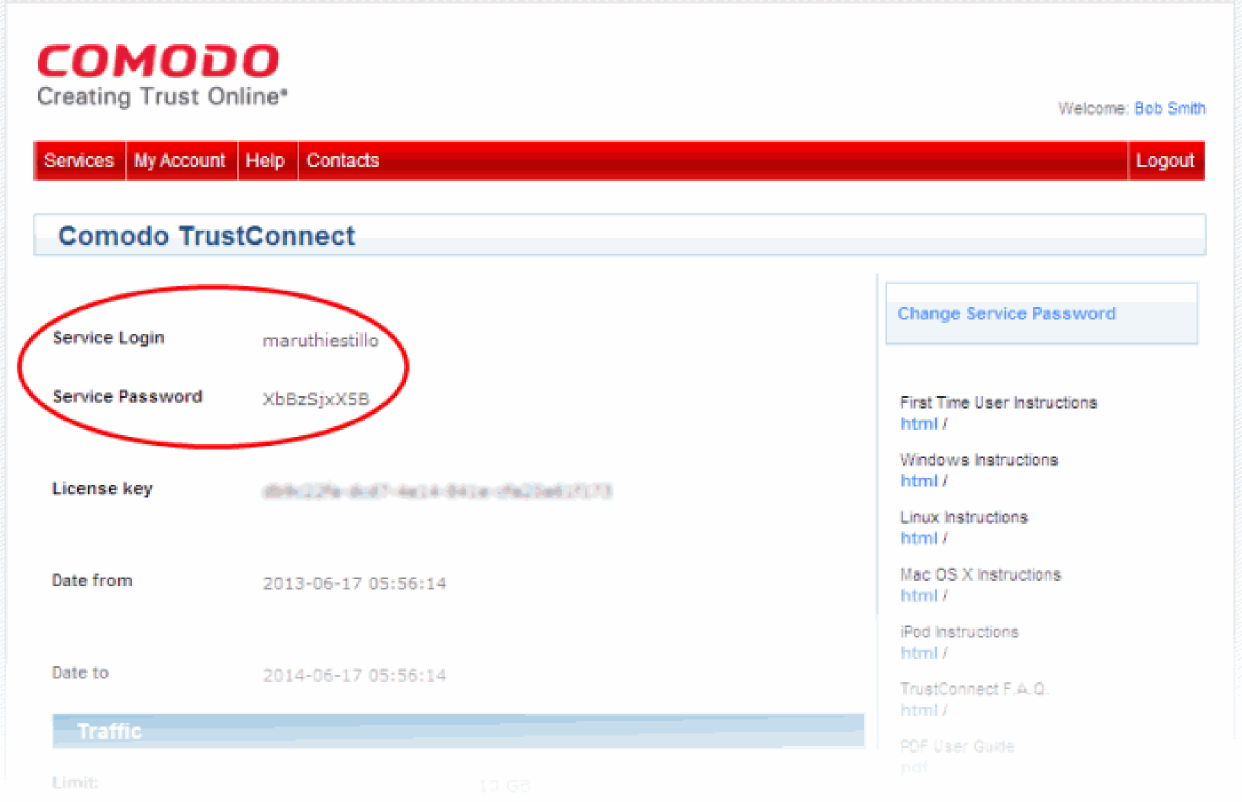
Username:

Password:

To find your TC service credentials

- In the **https://accounts.comodo.com/** page login to your CAM account using the CAM username and password sent via email at the time of account creation.
- Click 'TrustConnect' in the menu bar or in the drop down from 'Services' tab.

The account details of your TC service will be displayed.



Service Login	maruthiestillo
Service Password	XbBzSjxX5B
License key	[redacted]
Date from	2013-06-17 05:56:14
Date to	2014-06-17 05:56:14
Limit:	10 GB

The TC Service Login and Service Password for your account should be entered in the Username and Password fields respectively in the 'Activate TrustConnect' dialog.

Please note that this activation dialog will appear only for the first time you are trying to connect via TC. After the activation process is successfully completed, subsequent attempts to connect via TC to the Internet will be automatically established.

9. Dragon Browser

Dragon is a fast and versatile Internet Browser based on Chromium and infused with Comodo's unparalleled level of security.

To help make your internet browsing experience even safer, Dragon is installed on your computer as a part of Comodo Internet Security. Dragon provides the complete complement of features offered by Chromium with superior security and privacy.

- **Dragon Features**
- **Starting Dragon**
- **Dragon Help**

Features:

- Improved Privacy over Dragon
- Lightning Fast Page Load Times

- Instantly Scan Web Pages for Malware with Web Inspector
- Built-in Media Downloader Allows You To Quickly Save Streaming Video
- Greater Stability and Less Memory Bloat
- Incognito Mode Stops Cookies, Improves Privacy
- Very easy to switch from your current browser to Dragon

Dragon Security:

- Has privacy enhancements that surpass those in Chromium's technology
- Has Domain Validation technology that identifies and segregates superior SSL certificates from inferior ones
- Stops cookies and other Web spies
- Prevents all Browser download tracking to ensure your privacy

Starting Dragon

Dragon is installed in your computer along with Comodo Internet Security. You can start the browser in two ways:

From the Start menu:

- Click *Start* > *All Programs* > *Comodo* > *Dragono* > *Comodo Dragon*

From the Desktop Icon:

- Double click on the Dragon Desktop icon created during the installation:

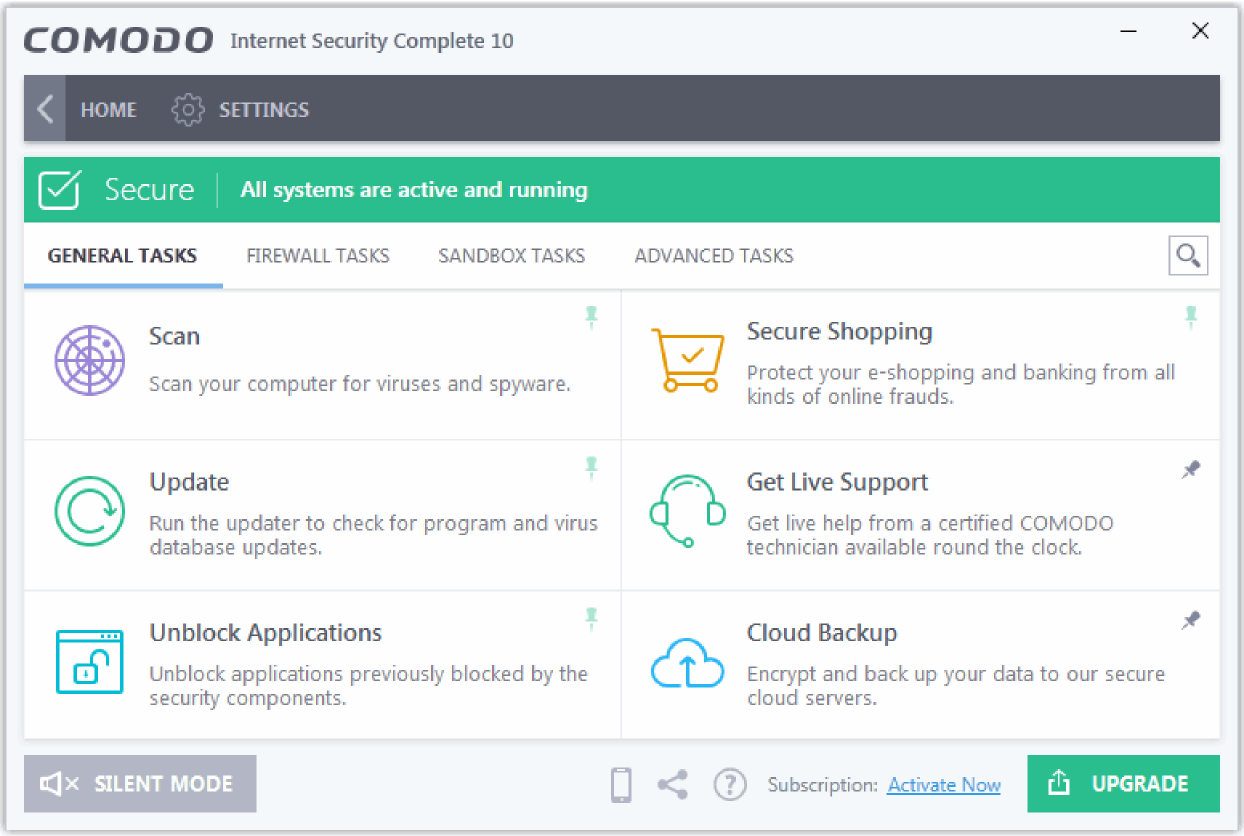
Dragon Help

Dragon's intuitive multi-tabbed interface enables easy and fast access to sophisticated features of the browser. Please refer to the Dragon online help guide at **https://help.comodo.com/topic-120-1-279-2524-Comodo-Dragon---Introduction.html** for more details on using the browser.

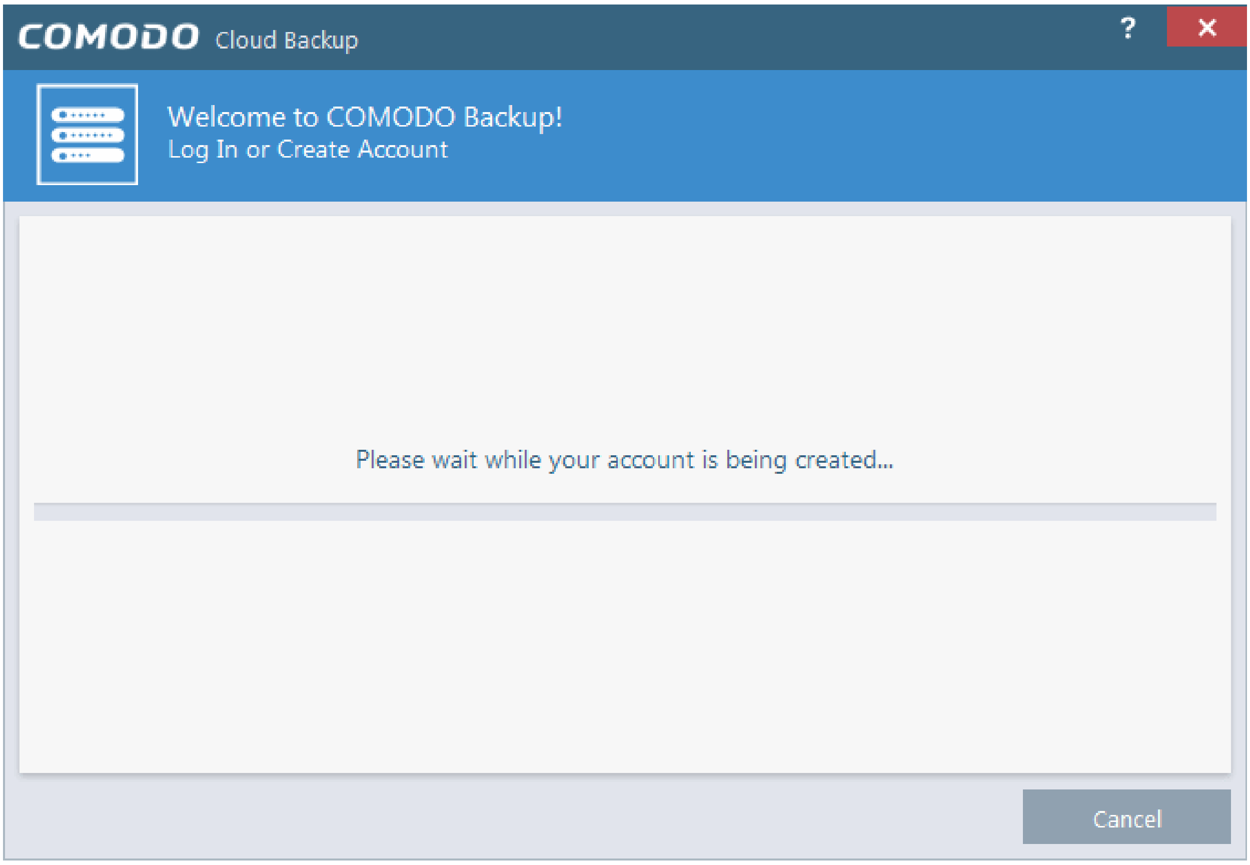
10. Comodo Backup

Comodo Cloud Backup provides essential disaster recovery for mission critical or otherwise important files in the event of damage. Files and data stored on Comodo's cloud servers and can be accessed over the Internet from anywhere in the world.

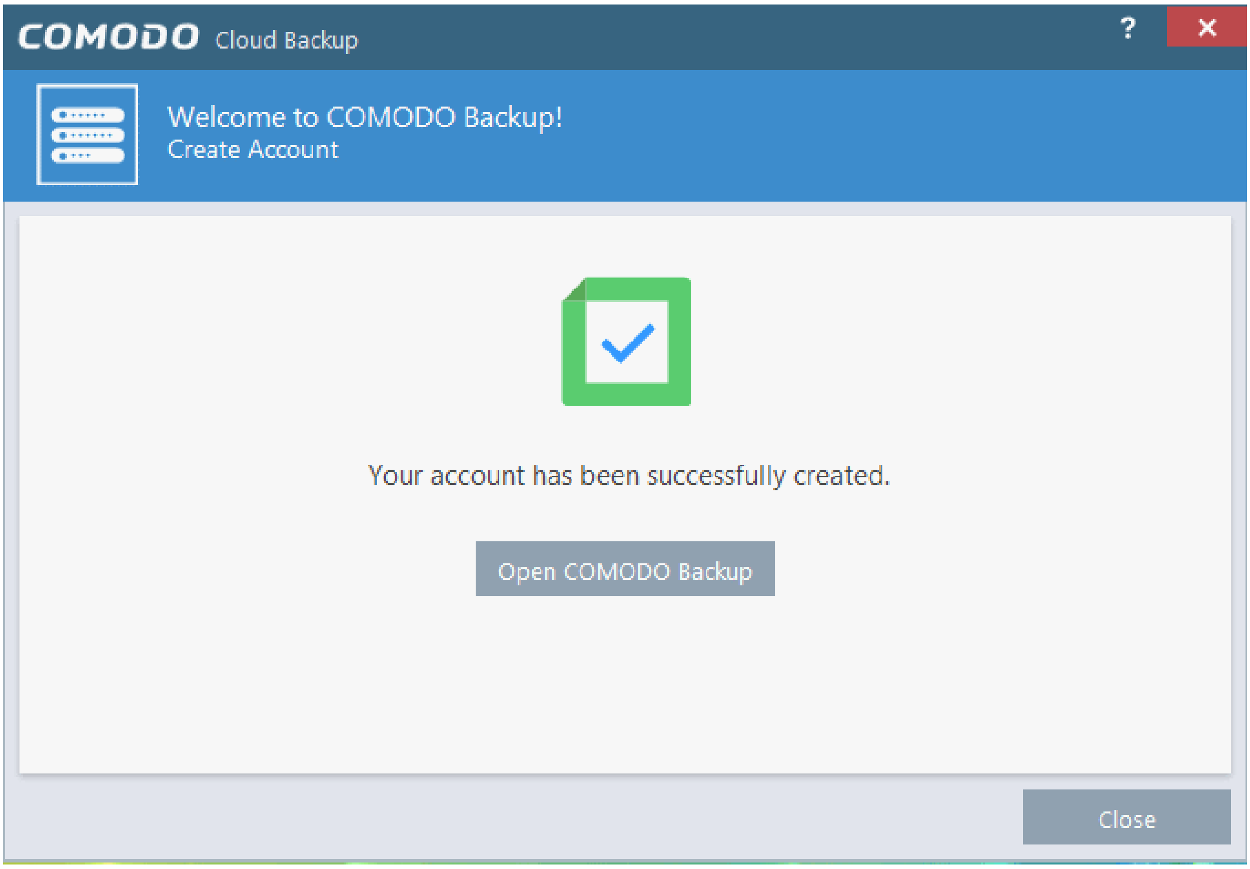
You can access the Comodo Backup by opening 'General Tasks' from the Tasks interface then clicking 'Cloud Backup'.


COMODO Internet Security Complete 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
SANDBOX TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
Cloud Backup
Encrypt and back up your data to our secure cloud servers.
SILENT MODE
Subscription: Activate Now
UPGRADE

If you have not activated CIS, then you can create an account from the 'Create New Account' form and if you have already activated CIS using the license key, an account will be created for you automatically.


COMODO Cloud Backup
?
×
Welcome to COMODO Backup!
Log In or Create Account
Please wait while your account is being created...
Cancel

Account will be created and the dialog displayed.



Your account has been successfully created.

- Click 'Open COMODO Backup' to access your online backup management console.

For more details about how to use Cloud Backup, refer to the online admin guide of our cloud backup partner at **www.acronis.com/en-us/support/documentation/Acronis_Backup_Cloud/index.html**.

Appendix 1 - How To Tutorials

The 'How To...' section of the guide contains guidance on key tasks of Comodo Internet Security. Use the links below to go to each tutorial's page.

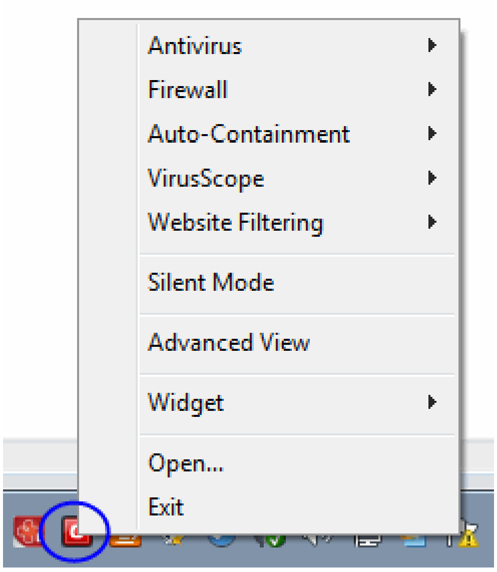
How to...:

- **Enable / Disable AV, Firewall Auto-Containment, VirusScope and Website Filter easily** - How to quickly enable or disable various CIS modules.
- **Setup the Firewall for maximum security and usability** - How to set up a secure connection to the internet
- **Block Internet Access while allowing local network (LAN) Access** - Configure the Firewall to only allow intranet/LAN connections while blocking the internet
- **Block/allow websites selectively to users of your computer** - Configure rules to block or allow access to certain websites for specific users of your computer.
- **Setup HIPS for maximum security and usability** - How to set up Host Intrusion Protection for the optimum balance between security and usability
- **Create Rules for Auto-Contained Applications** - How to set auto-containment rules for maximum security against untrusted applications
- **Password Protect Your CIS Settings** - Explains how to protect your CIS settings
- **Reset a Forgotten Password (Advanced)** - Explains how to create a new password for CIS
- **Run an instant Antivirus scan on selected items** - Guidance on initiating a manual scan on selected folders/files to check for viruses and other malware.
- **Create an Antivirus scanning schedule** - Set up antivirus scans to automatically run at specific times
- **Run an untrusted program inside the container** - Launch programs that you do not trust inside the container to eliminate the possibility of them causing damage to your computer.
- **Run Browsers inside the Container -** Guidance on running your browser, inside the container when you plan to visit untrusted websites.
- **Run Untrusted Programs inside Virtual Desktop** - Guidance on executing a program that you do not trust to be safe, inside the virtual Desktop.
- **Run Browsers inside the Virtual Desktop** - Guidance on running your browser, inside virtual Desktop when you plan to do online banking, online shopping and so on.
- **Restore incorrectly blocked item(s)** - Help to restore files and executables that were moved to quarantine by mistake
- **Enable file sharing applications like BitTorrent and Emule** - Explains how to configure Comodo Firewall for file sharing through popular software
- **Block any downloads of a specific file type** - Explains how to configure HIPS to block downloads of files of a specific type
- **Switch between complete CIS suite and individual components (just AV or FW)** - Explains how to uninstall or install Firewall or Antivirus components after installation.
- **Switch Off Automatic Antivirus and Software Updates** - Explains how to stop automatic software and virus updates
- **Temporarily suppress alerts when playing games** - Helps you to switch off CIS pop-up alerts to avoid interruptions while playing games
- **Renew or upgrade your license** - Explains how to renew or upgrade your license
- **How to use CIS Protocol Handlers** - Explains how to run tasks from your browser using CIS commands

- **Configure Secure Shopping** - Explains how to add and manage secure shopping environment
- **Comodo Cloud Backup** - Helps you to create or login to Cloud Backup account to secure you data

Enable / Disable AV, Firewall, Auto-Containment, VirusScope and Website Filter Easily

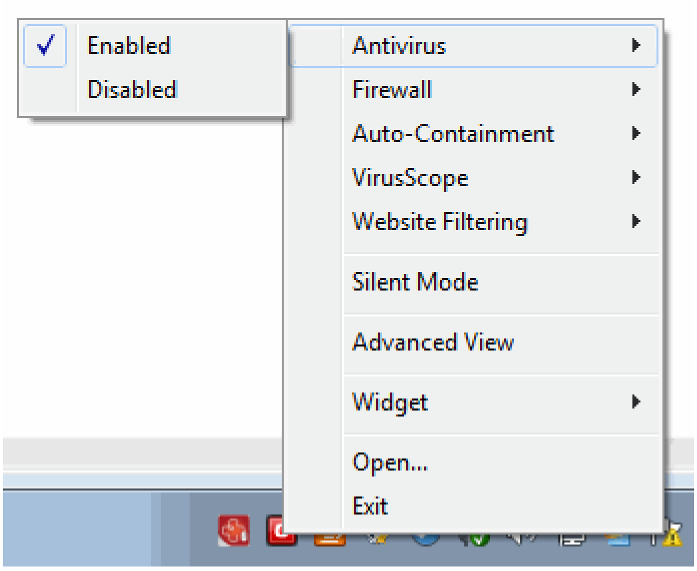
Right-click on the CIS tray icon to quickly switch on or off the **Antivirus**, **Firewall**, **Auto-containment**, **VirusScope** or **Website Filter** components:



Antivirus

To enable/disable the Antivirus

1. Right-click on the system tray icon with CIS in Basic View.
2. Move your mouse over 'Antivirus'



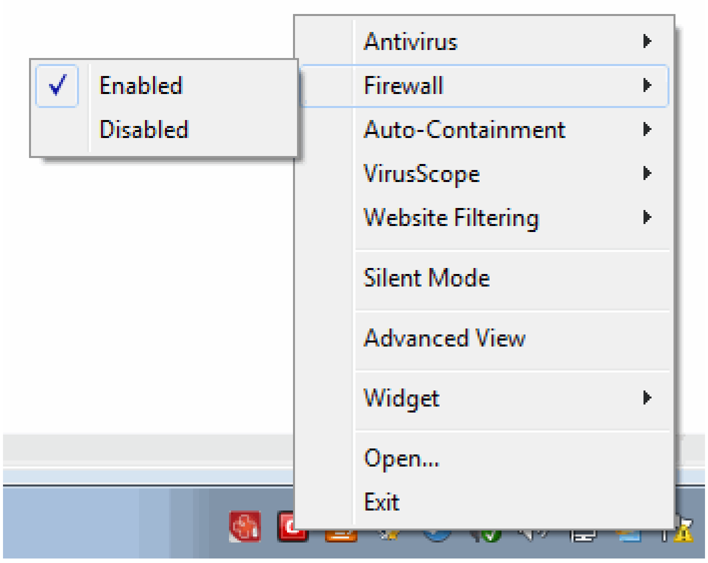
3. Choose 'Enabled' or 'Disabled' as required

You can also set the security level from **the Home Screen**.

Firewall

To enable/disable the Firewall

1. Right-click on the system tray icon with CIS in Basic View.
2. Move your mouse over 'Firewall'



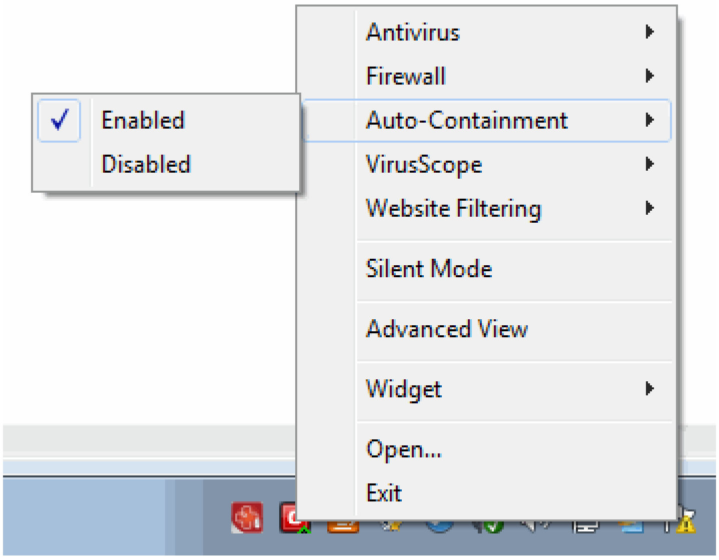
3. Choose 'Enabled' or 'Disabled' as required

You can also set the security level from **the Home Screen**.

Auto-Containment

To enable/disable the Auto-Containment

1. Right-click on the system tray icon with CIS in Basic View.
2. Move your mouse over 'Auto-Containment'



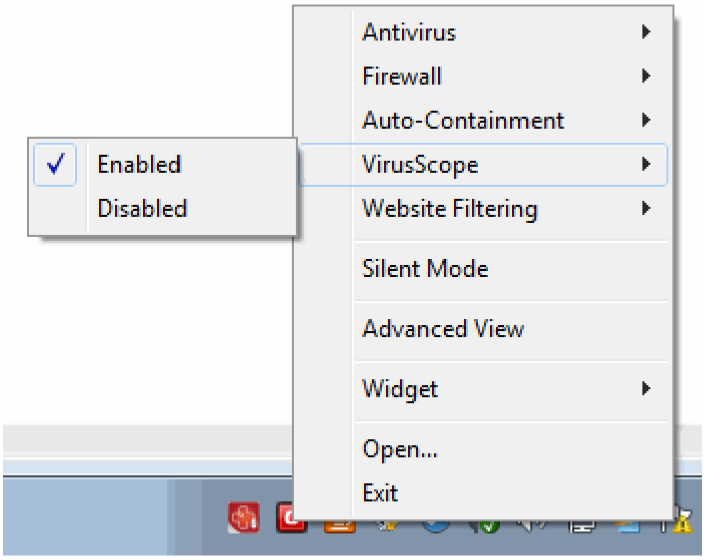
3. Choose 'Enabled' or 'Disabled' as required

You can also set the security level from **the Home Screen**.

VirusScope

To enable/disable VirusScope

1. Right-click on the system tray icon with CIS in Basic View.
2. Move your mouse over 'VirusScope'



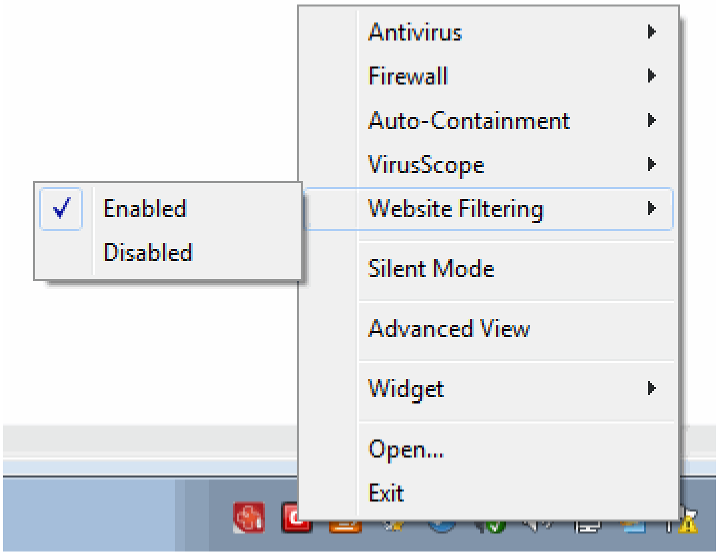
3. Choose 'Enabled' or 'Disabled' as required

You can also set the security level from **the Home Screen**.

Website Filter

To enable/disable the Website Filtering

1. Right-click on the system tray icon with CIS in Basic View.
2. Move your mouse over 'Website Filtering'



3. Choose 'Enabled' or 'Disabled' as required

You can also set the security level from **the Home Screen**.

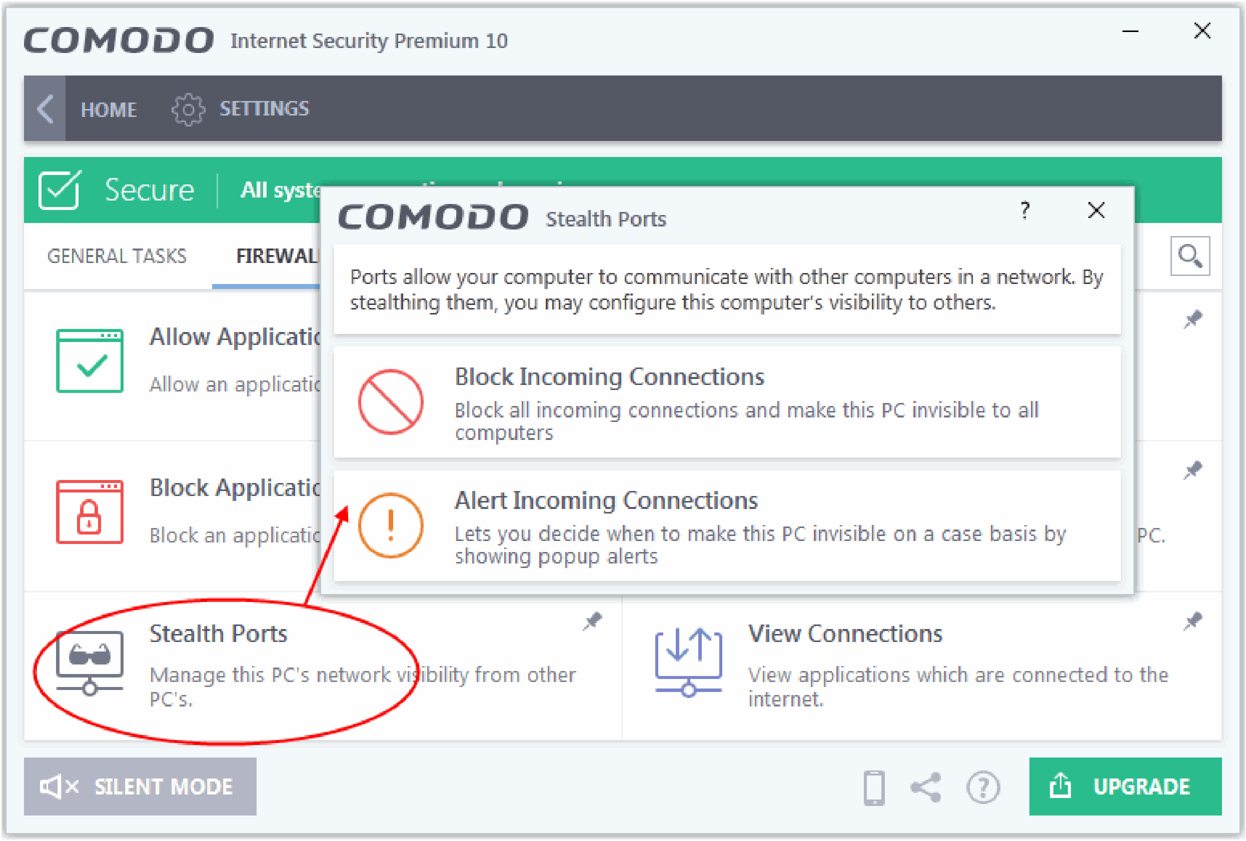
Set up the Firewall For Maximum Security and Usability

This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the internet.

Stealth Ports

Port stealthing is a security feature whereby ports on an internet connected PC are hidden from sight, sending no response to opportunistic port scans.

1. Click 'Tasks' at the top-left of the CIS screen
2. Click the 'Firewall Tasks' tab
3. Open the 'Stealth Ports' interface by clicking the 'Stealth Ports' icon on the 'Firewall Tasks' panel



COMODO Stealth Ports

Ports allow your computer to communicate with other computers in a network. By stealthing them, you may configure this computer's visibility to others.

Block Incoming Connections
Block all incoming connections and make this PC invisible to all computers

Alert Incoming Connections
Lets you decide when to make this PC invisible on a case basis by showing popup alerts

4. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

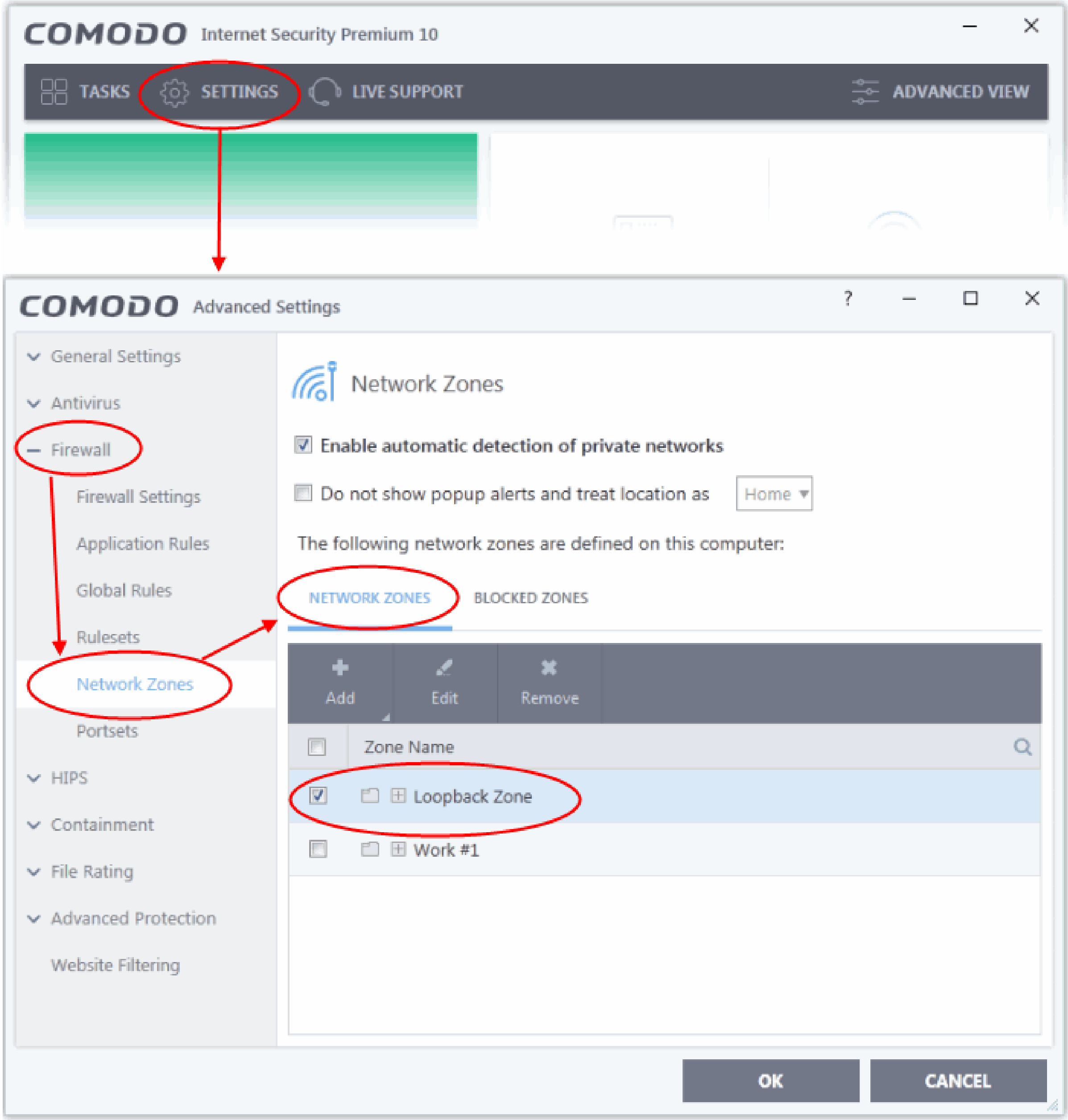
Click here for more information about port stealthing

Network Zones Settings

'Network Zones' settings allow you to configure the protection level for connections to a router/home network (this is usually done **automatically** for you).

To view the configurations

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'Network Zones' under 'Firewall' on the left.
3. Click the 'Network Zones' tab in the 'Network Zones' interface



4. Inspect the 'Loopback zone' and 'Local Area Network #1' (exact name may vary) by clicking the '+' button beside the zone name.
    - In most cases, the loopback zone IP address should be 127.0.01/255.0.0.0
    - In most cases, the IP address of the auto -detected Network zone should be 10.nnn.nnn.nnn/255.255.255.0
5. Click 'OK'.

Click here for more details on Network Zones settings

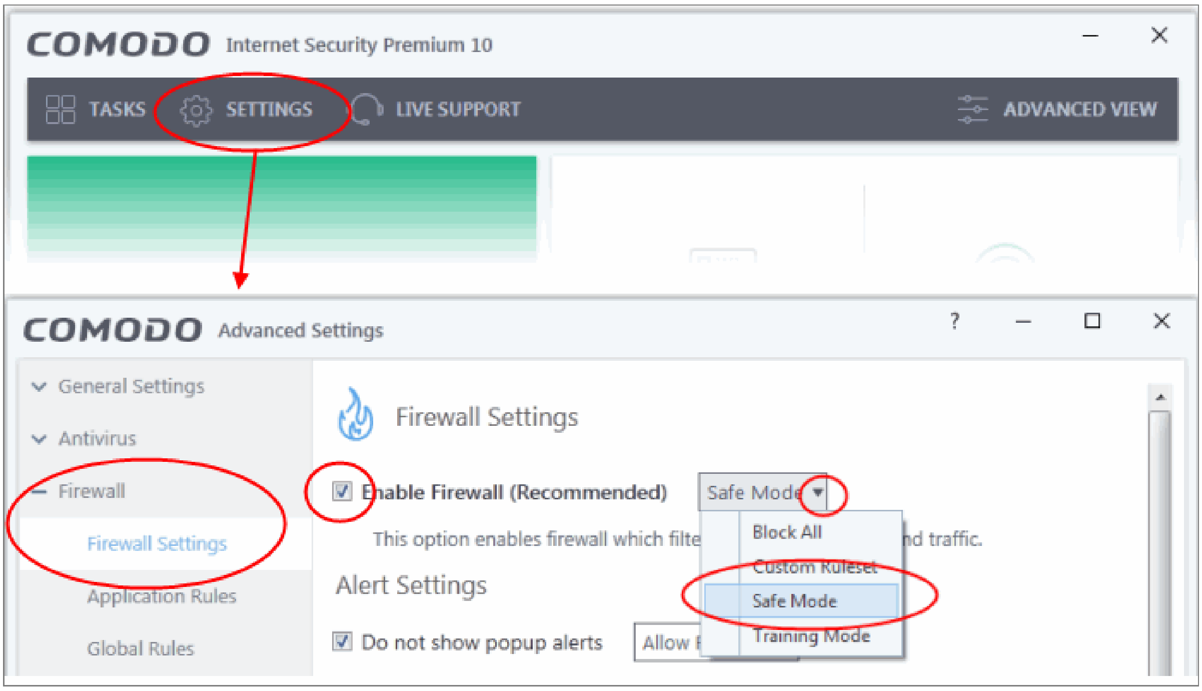
Firewall Settings

The Firewall settings option allows you to configure the protection level for your internet connection and the frequency of alerts generated.

To open the Firewall settings panel

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Firewall' > 'Firewall Settings' on the left

3. Select 'Enable Firewall' and choose 'Safe Mode' from the drop-down



☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filte... nd traffic.

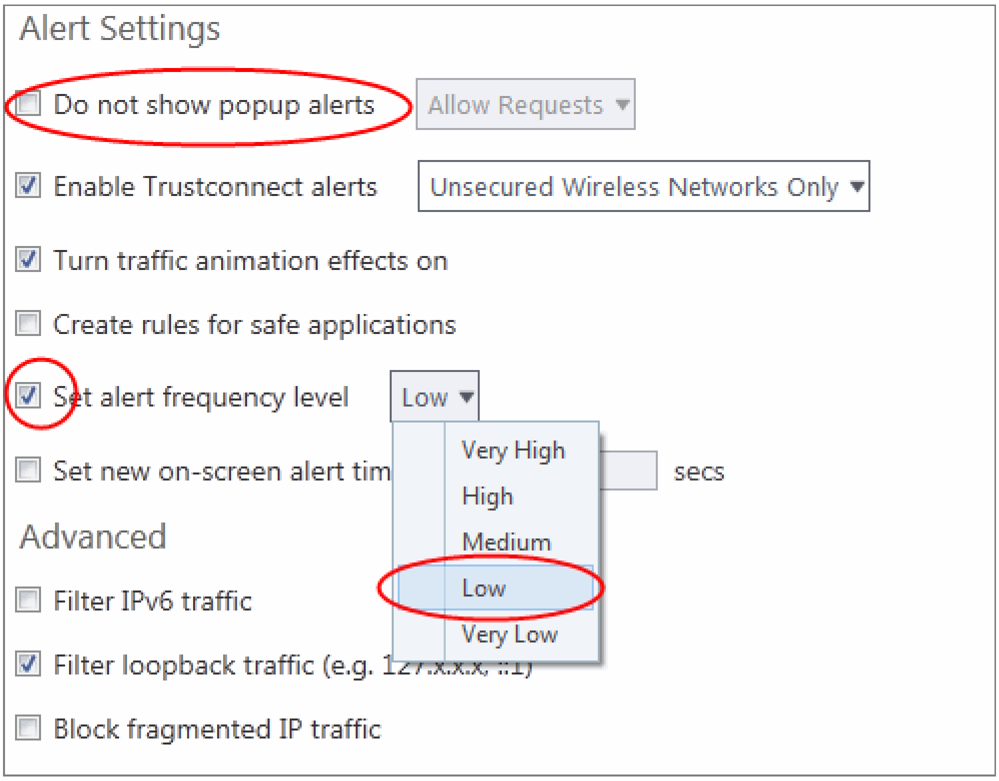
☑ Do not show popup alerts

Safe Mode: While filtering network traffic, the firewall will automatically create rules which allow traffic for application components certified as 'Safe' by Comodo. For non-certified, new, applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

Under 'Alert Settings' in the same interface:

- Deselect 'Do not show popup alerts'
- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.



Alert Settings

□ Do not show popup alerts | Allow Requests

☑ Enable Trustconnect alerts | Unsecured Wireless Networks Only

☑ Turn traffic animation effects on

□ Create rules for safe applications

☑ Set alert frequency level | Low

□ Set new on-screen alert tim... secs

Advanced

□ Filter IPv6 traffic

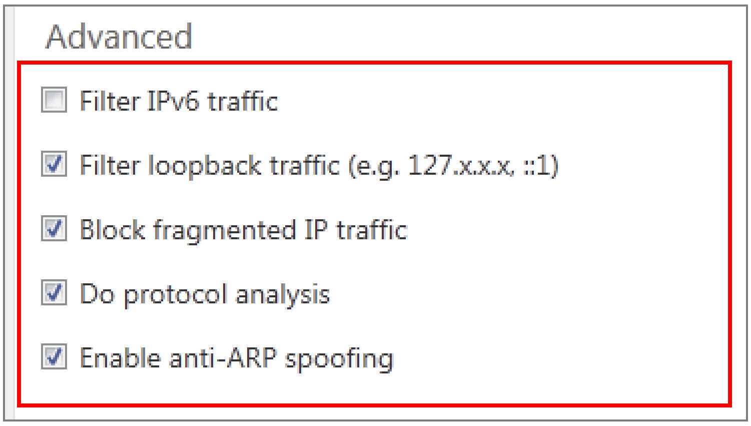
☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

□ Block fragmented IP traffic

Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- Select 'Filter loopback traffic'
- Ensure that the 'Block fragmented IP traffic' is selected
    - Block fragmented IP traffic - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time.
- Select the 'Do Protocol Analysis' checkbox to detect fake packets used in denial of service attacks
- Select 'Enable anti-ARP spoofing'



Advanced

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☑ Block fragmented IP traffic

☑ Do protocol analysis

☑ Enable anti-ARP spoofing

4. Click 'OK' for your settings to take effect.

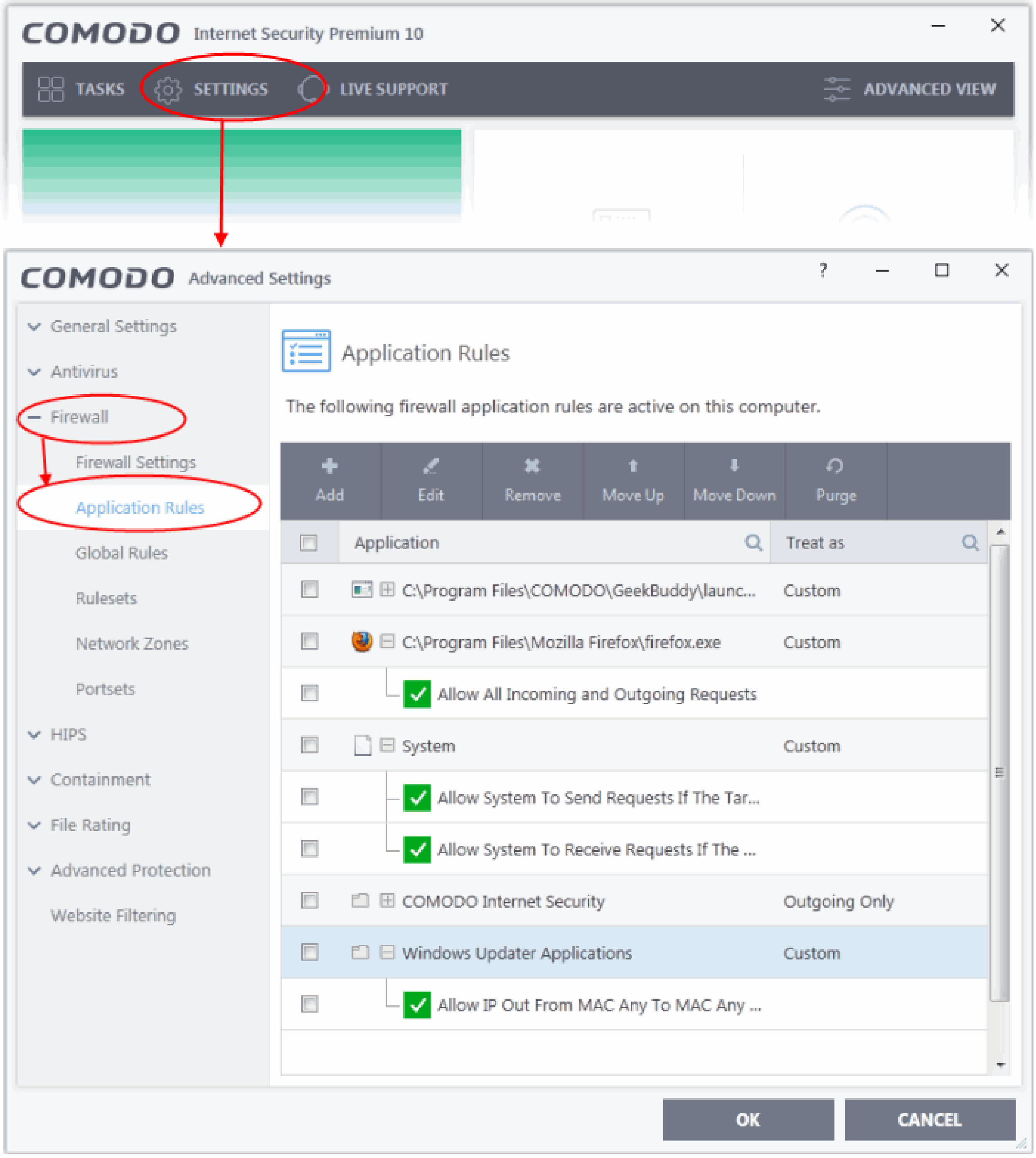
Click here for more details on Firewall Settings

Setting-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules and policies on an application-specific and global basis.

To view the Application Rules

1. Click 'Settings' at the top of CIS home screen
2. Click 'Application Rules' under 'Firewall' on the left.



Application Rules

The following firewall application rules are active on this computer.

Application	Treat as
C:\Program Files\COMODO\GeekBuddy\launc...	Custom
C:\Program Files\Mozilla Firefox\firefox.exe	Custom
✓ Allow All Incoming and Outgoing Requests	
System	Custom
✓ Allow System To Send Requests If The Tar...	
✓ Allow System To Receive Requests If The ...	
COMODO Internet Security	Outgoing Only
Windows Updater Applications	Custom
✓ Allow IP Out From MAC Any To MAC Any ...	

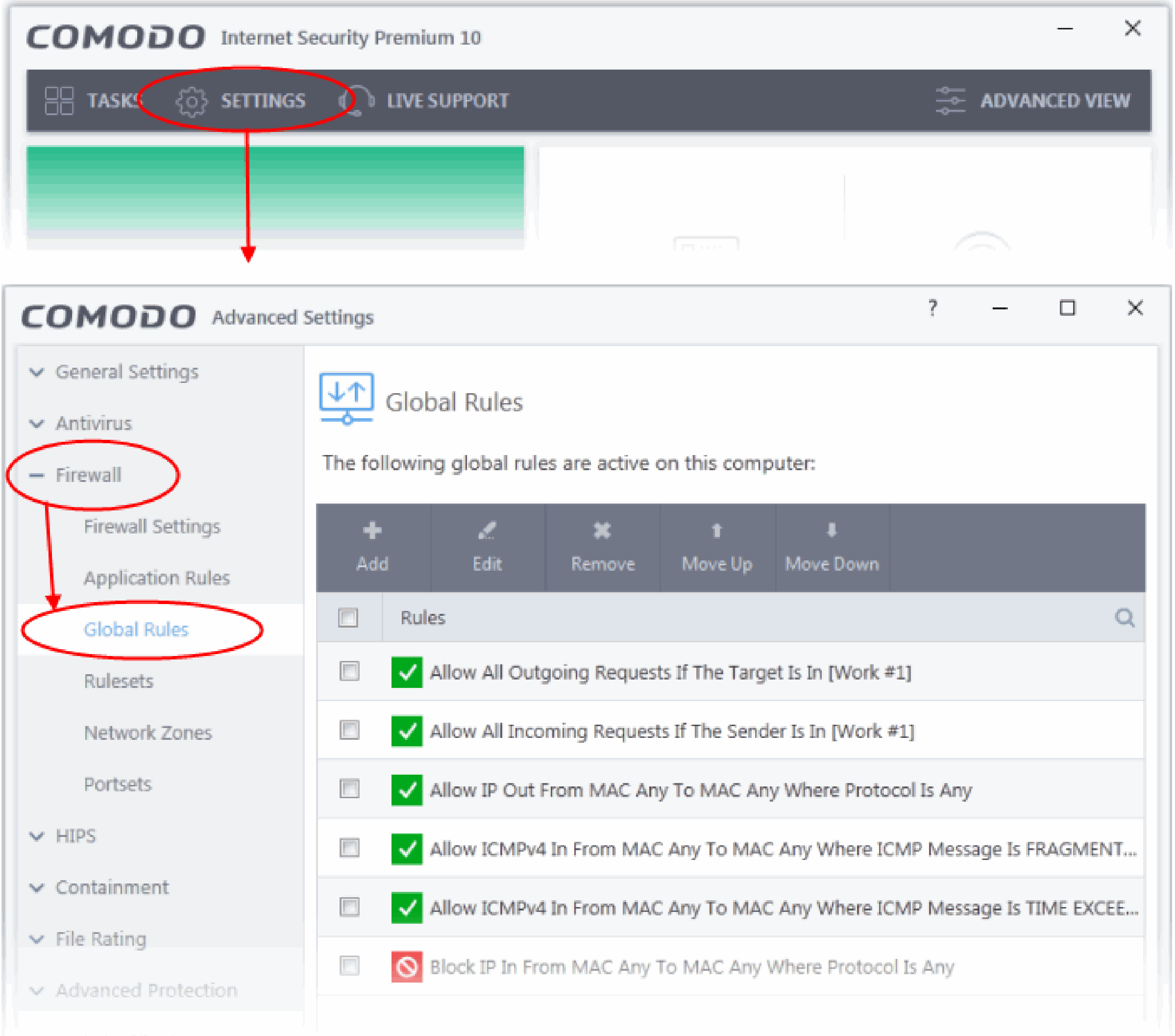
3. Click 'Add' to add a new application rule

4. Select a rule and click 'Edit' to edit the rules for a specific application manually or click 'Remove' to remove them.
5. Click 'OK' for your settings to take effect.

Click here for more details on Application Rules

To view the Global Rules

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'Global Rules' under 'Firewall' on the left.



The following global rules are active on this computer:

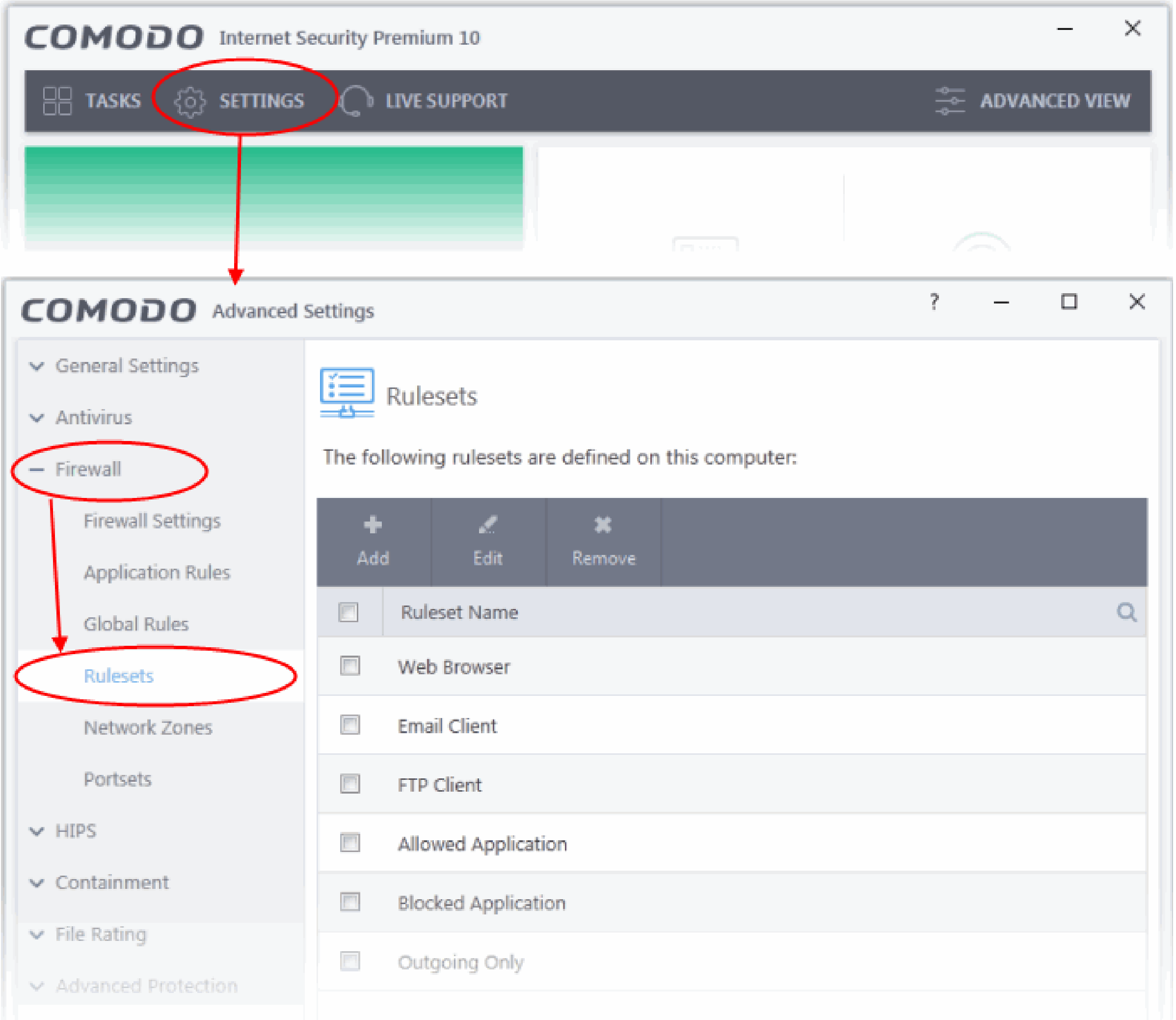
- Allow All Outgoing Requests If The Target Is In [Work #1]
- Allow All Incoming Requests If The Sender Is In [Work #1]
- Allow IP Out From MAC Any To MAC Any Where Protocol Is Any
- Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is FRAGMENT...
- Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME EXCEE...
- Block IP In From MAC Any To MAC Any Where Protocol Is Any

3. Click 'Add' to add a new global rule
4. Select a rule and click 'Edit' to edit the a rule manually or click 'Remove' to remove them.
5. Click 'OK' for your settings to take effect.

Click here for more details on Global Rules

To view Predefined Firewall rulesets

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Firewall' > 'Rulesets' on the left



The following rulesets are defined on this computer:

□	Ruleset Name
□	Web Browser
□	Email Client
□	FTP Client
□	Allowed Application
□	Blocked Application
□	Outgoing Only

3. Click 'Add' to add a new ruleset
4. Select a ruleset and click 'Edit' to edit the rules manually or click 'Remove' to remove them.
5. Click 'OK' for your settings to take effect.

You need not make your own rulesets, the defaults are usually enough.

Click here for more details on pre-defined firewall rulesets

Block Internet Access while Allowing Local Area Network (LAN) Access

You can configure Comodo Firewall to block internet access while allowing connections to an internal network (intranet or LAN).

Example scenarios:

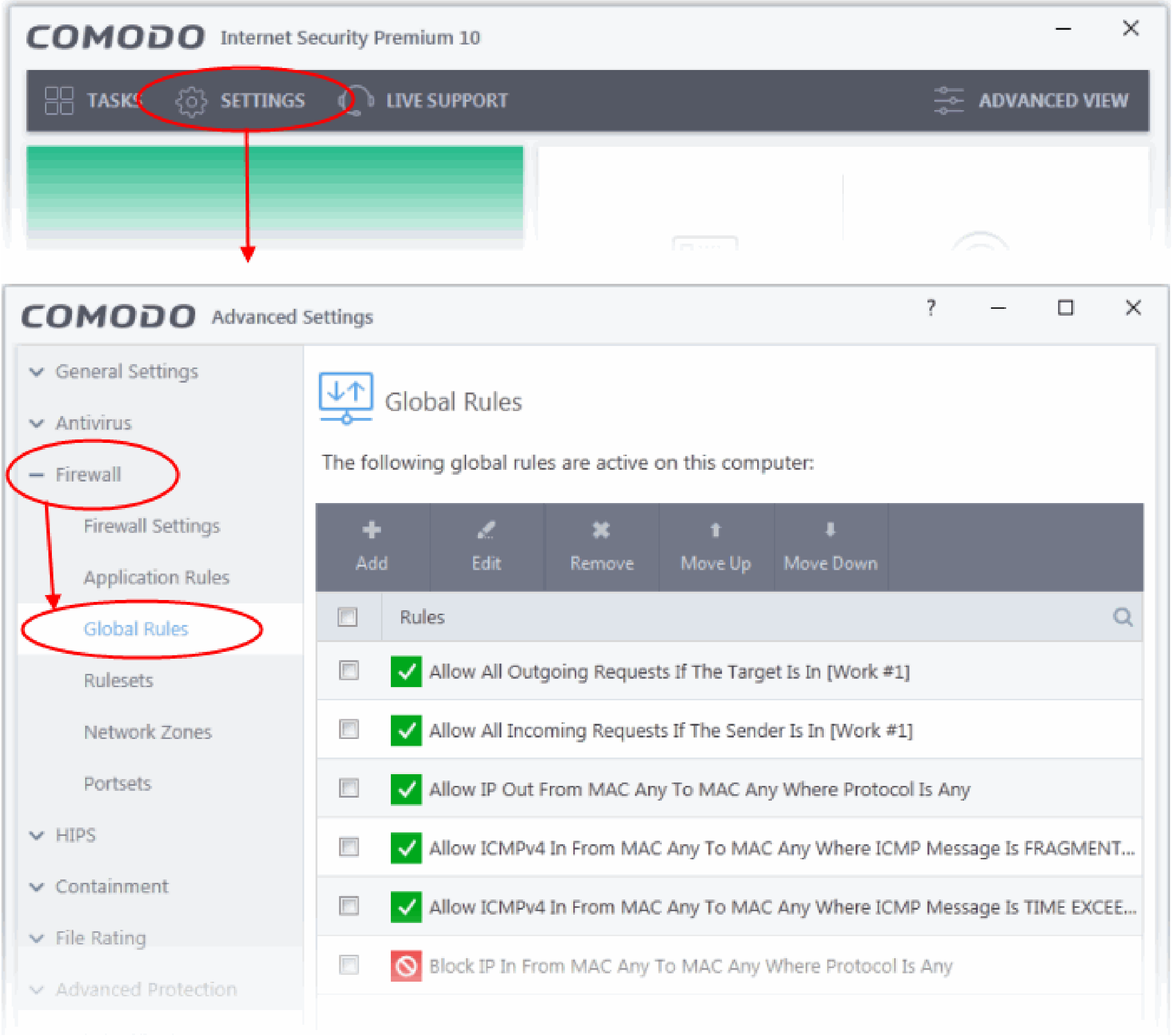
- In your network at home, you want your child's computer to connect to other computers at home but disable their internet access for safety reasons
- In your corporate network, you want your employee's computers to connect to your network machines but disable internet access for bandwidth reasons

> *Side note. If you just want to block access to certain websites, see '***Block/allow websites selectively to users of your computer***' instead.*

To block internet access while allowing connections to an internal network, you need to create a 'Global Rule' under firewall settings. You should also password protect your configuration to prevent others from altering it.

To create Global Rules

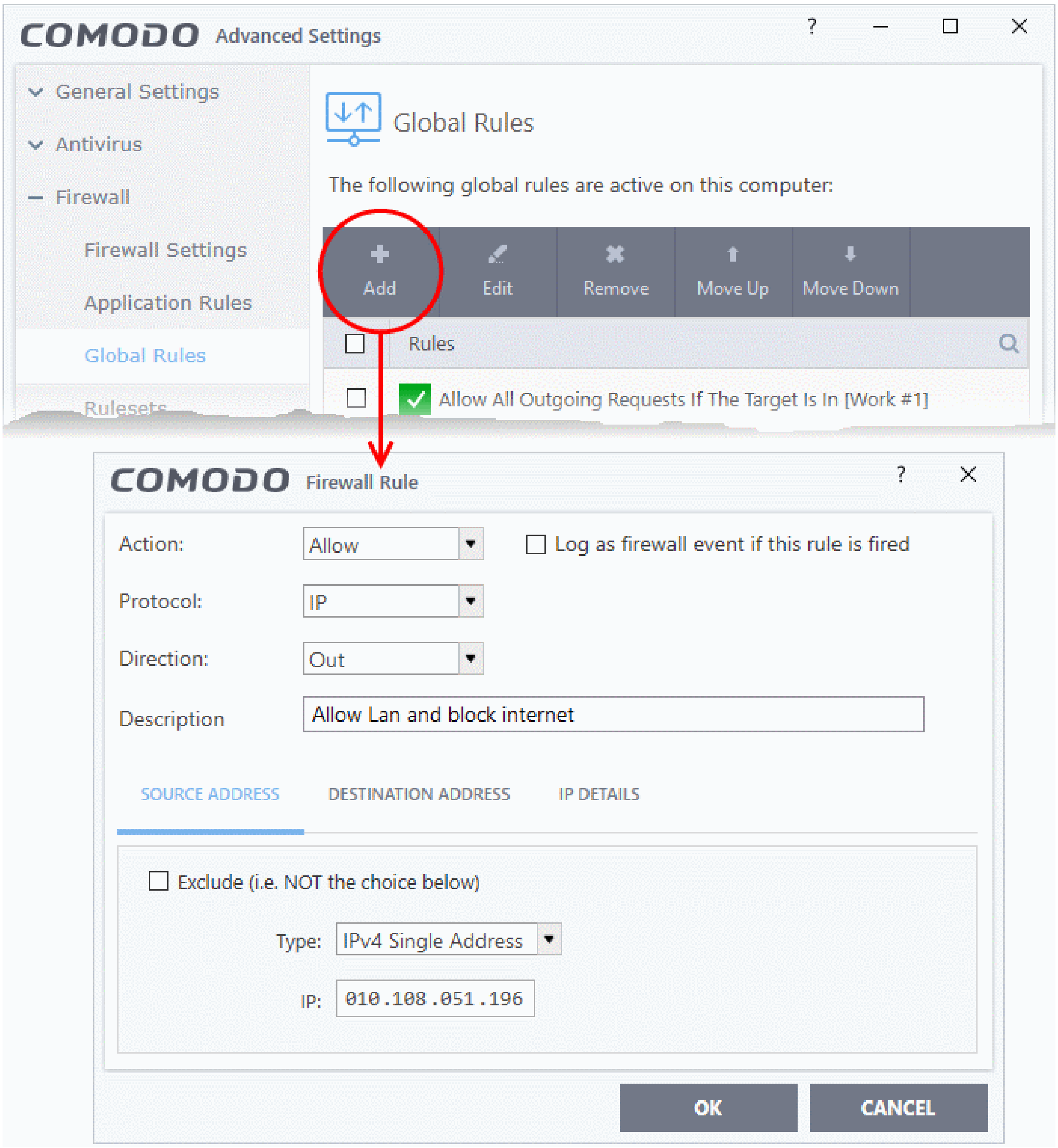
1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'Global Rules' under 'Firewall' on the left.



The following global rules are active on this computer:

□	Rules
□	✓ Allow All Outgoing Requests If The Target Is In [Work #1]
□	✓ Allow All Incoming Requests If The Sender Is In [Work #1]
□	✓ Allow IP Out From MAC Any To MAC Any Where Protocol Is Any
□	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is FRAGMENT...
□	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME EXCEE...
□	⊘ Block IP In From MAC Any To MAC Any Where Protocol Is Any

3. Choose 'Add' from the options at the top. The 'Firewall Rule' interface will open.



The following global rules are active on this computer:

□ ☑ Allow All Outgoing Requests If The Target Is In [Work #1]

Action: Allow

□ Log as firewall event if this rule is fired

Protocol: IP

Direction: Out

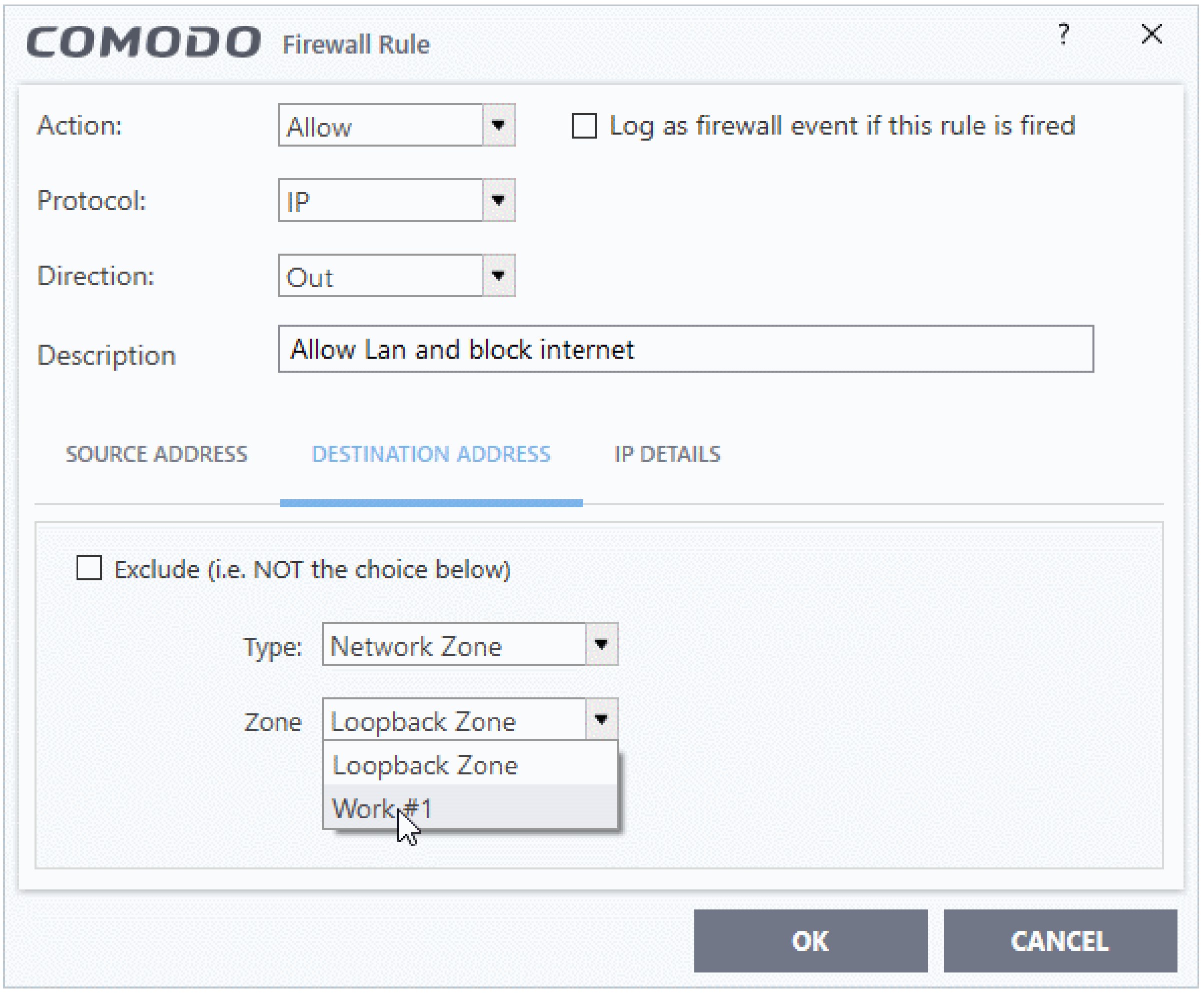
Description: Allow Lan and block internet

□ Exclude (i.e. NOT the choice below)

Type: IPv4 Single Address

IP: 010.108.051.196

4. Choose the following options from the respective drop-downs:
    - Action = 'Block';
    - Protocol = 'IP';
    - Direction = 'Out'.
5. Enter a description for the new rule in the 'Description' text box.
6. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network and enter the IP address of the computer in the IP text box.
7. Click the 'Destination Address' tab, choose 'Network Zone' from the 'Type' drop-down and choose your local area network from the 'Zone' drop-down



COMODO Firewall Rule

Action: Allow

☐ Log as firewall event if this rule is fired

Protocol: IP

Direction: Out

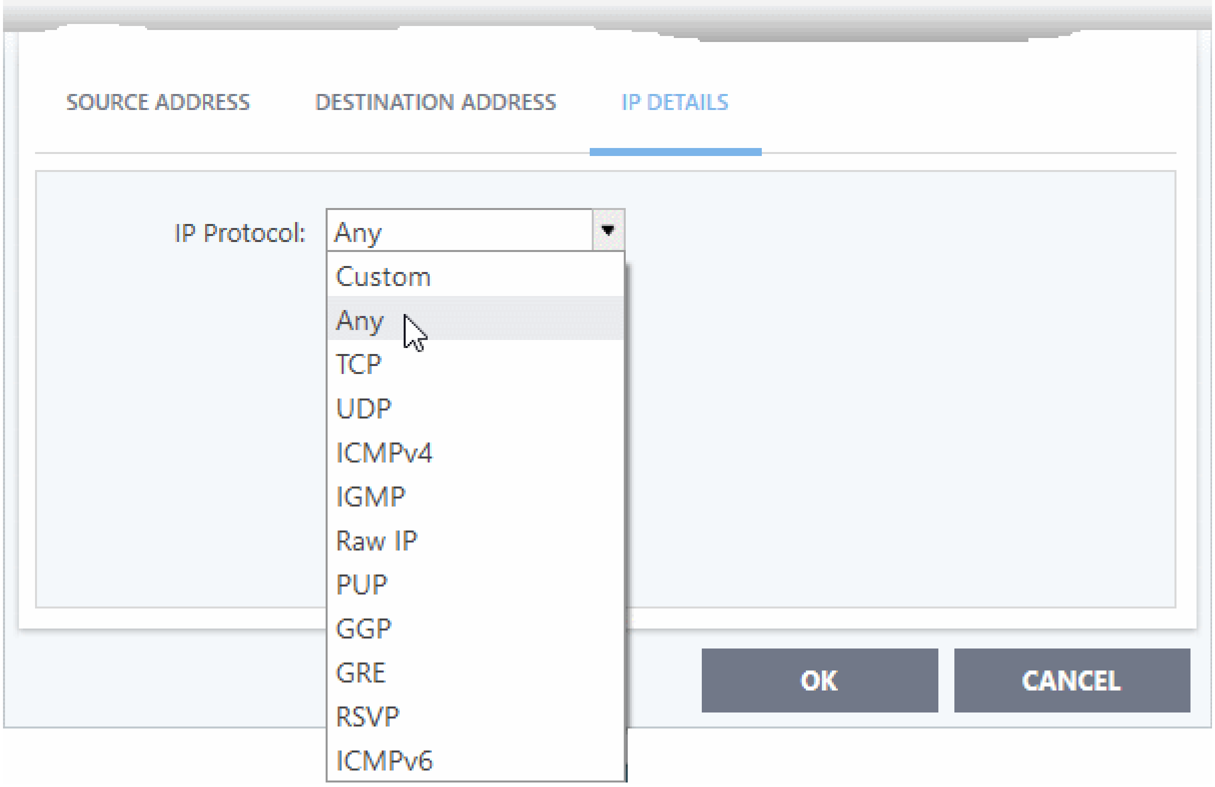
Description: Allow Lan and block internet

☐ Exclude (i.e. NOT the choice below)

Type: Network Zone

Zone: Loopback Zone

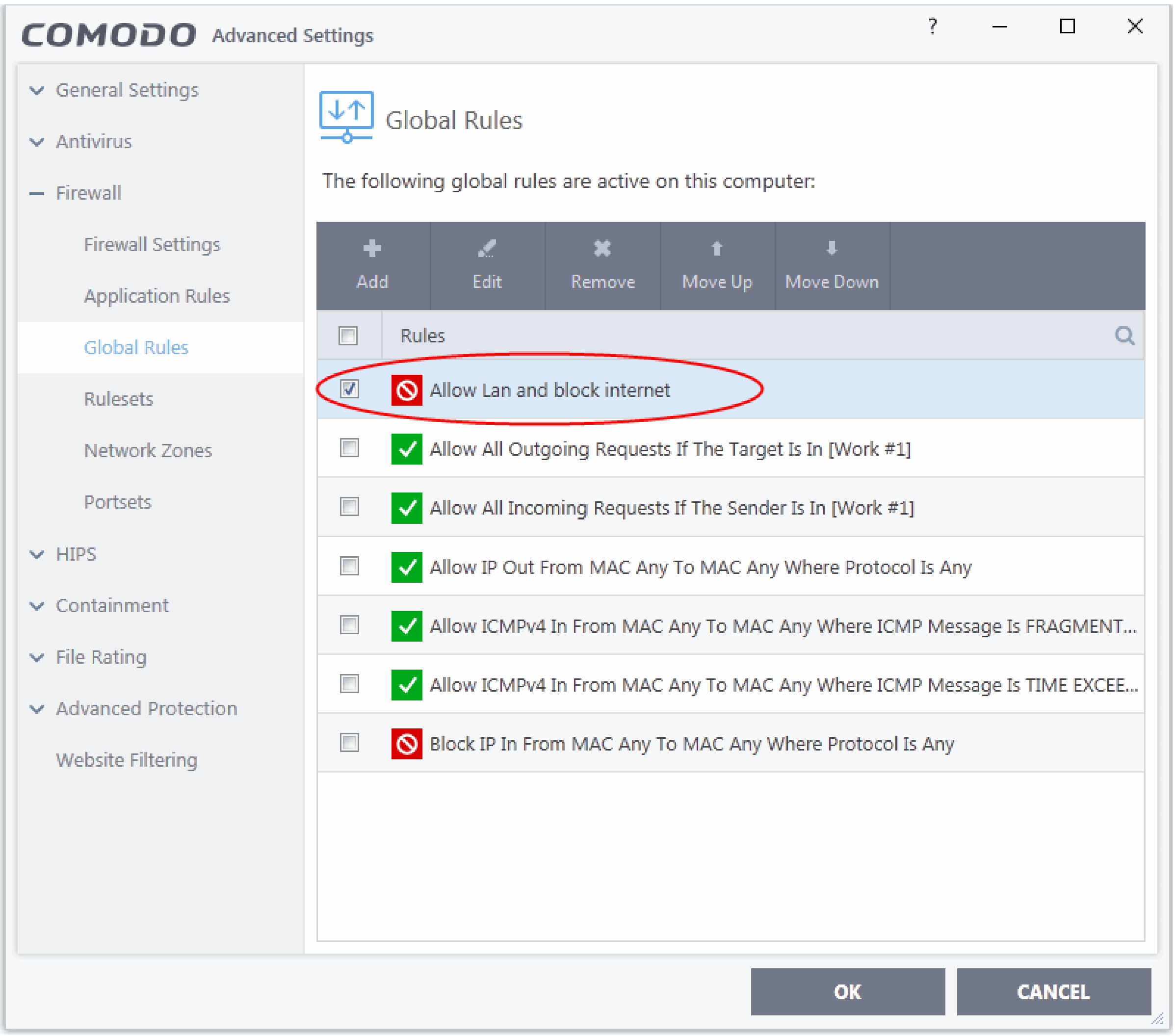
8. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.



IP Protocol: Any

9. Click 'OK'. The created policy will be added to the list of 'Global Rules'.

10. Select the rule and click the 'Move Up' button until the rule is in first position:



Global Rules

The following global rules are active on this computer:

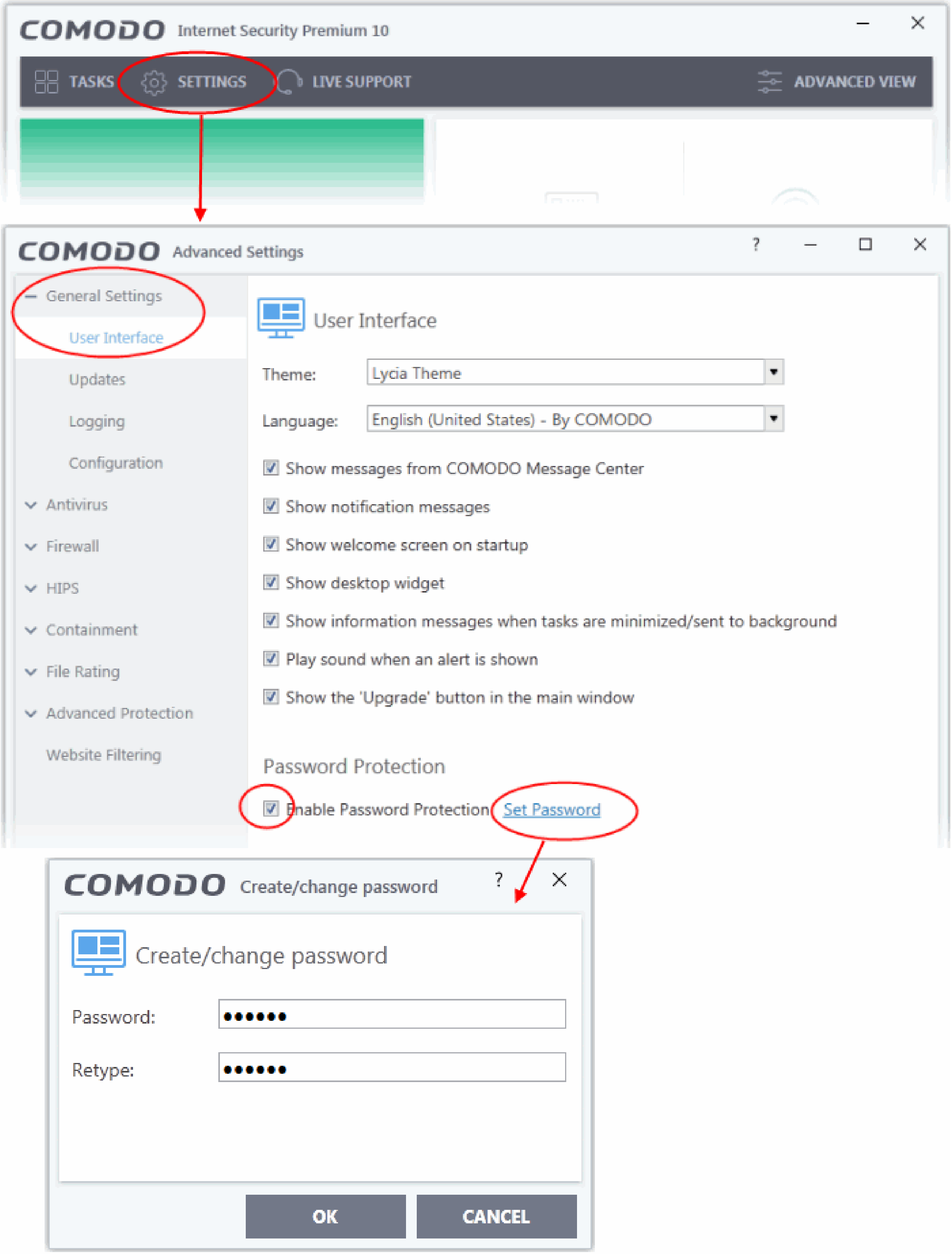
☐	Rules
☑	🚫 Allow Lan and block internet
☐	✓ Allow All Outgoing Requests If The Target Is In [Work #1]
☐	✓ Allow All Incoming Requests If The Sender Is In [Work #1]
☐	✓ Allow IP Out From MAC Any To MAC Any Where Protocol Is Any
☐	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is FRAGMENT...
☐	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME EXCEE...
☐	🚫 Block IP In From MAC Any To MAC Any Where Protocol Is Any

11. Click 'OK' for your configuration to take effect.

Your firewall is now configured to allow access to the internal network but to block internet access. Now you need to password protect this configuration to prevent others from changing it.

To password protect your configuration

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'User Interface' under 'General Settings' on the left.
3. Select 'Enable Password Protection' under 'Password Protection' and click the 'Set Password' link. The Create/change password' dialog will appear:



COMODO Internet Security Premium 10

COMODO Advanced Settings

User Interface

Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show welcome screen on startup

☑ Show desktop widget

☑ Show information messages when tasks are minimized/sent to background

☑ Play sound when an alert is shown

☑ Show the 'Upgrade' button in the main window

Password Protection

☑ Enable Password Protection Set Password

COMODO Create/change password

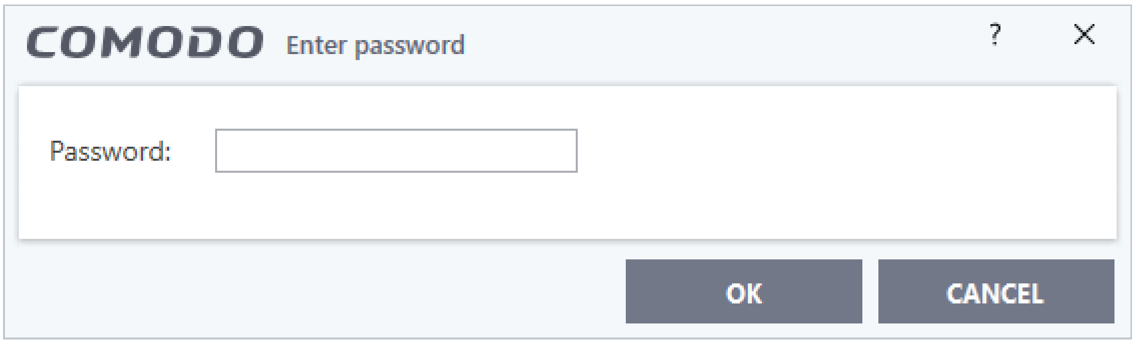
Create/change password

Password: ●●●●●●

Retype: ●●●●●●

4. Enter and confirm your password then click 'OK'. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

The configuration is now password protected. From the next attempt to change any configuration changes to CIS, you will be prompted to enter the password to proceed.



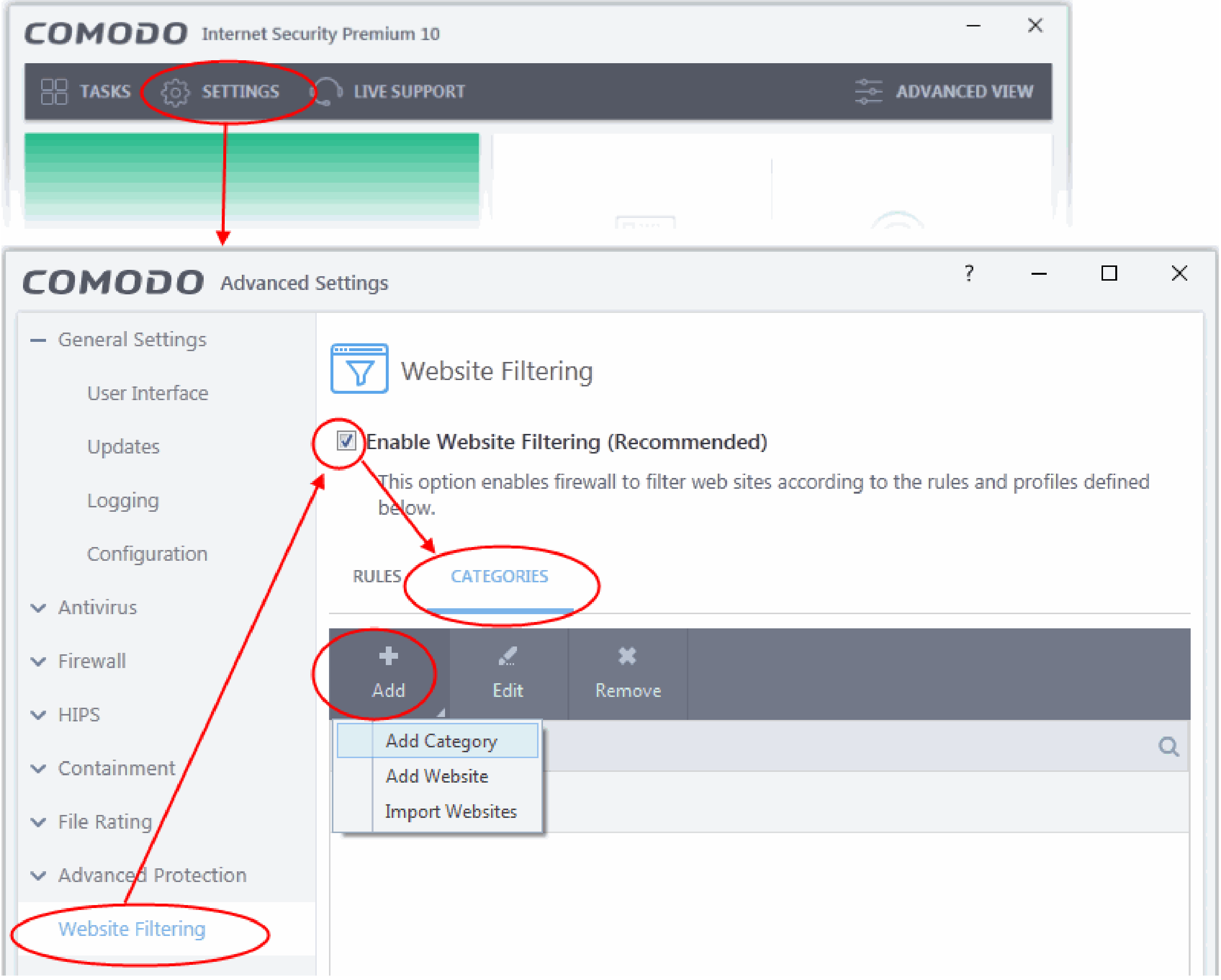
Block / Allow Specific Websites to Specific Users

Comodo Internet Security allows you to block or allow access to specific websites, or groups of websites, to different users. This involves two steps:

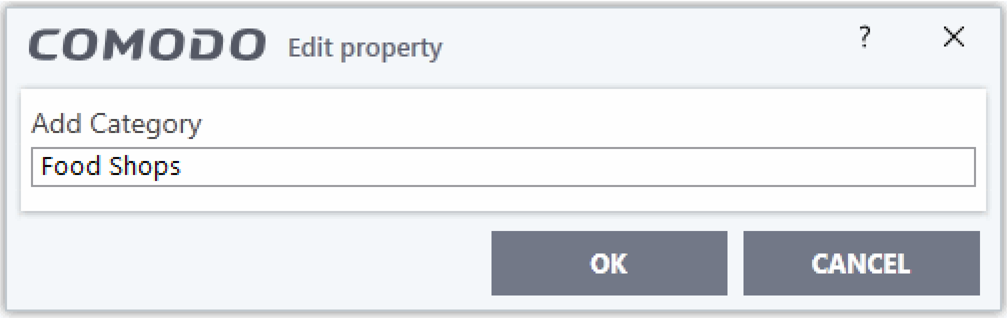
- **Define Website Categories and add websites**
- **Create Firewall rules for allowing or blocking website categories to selected users**

To define website categories

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface.
2. Click 'Website Filtering' on the left.
3. Click the 'Categories' tab from the 'Website Filtering' interface.

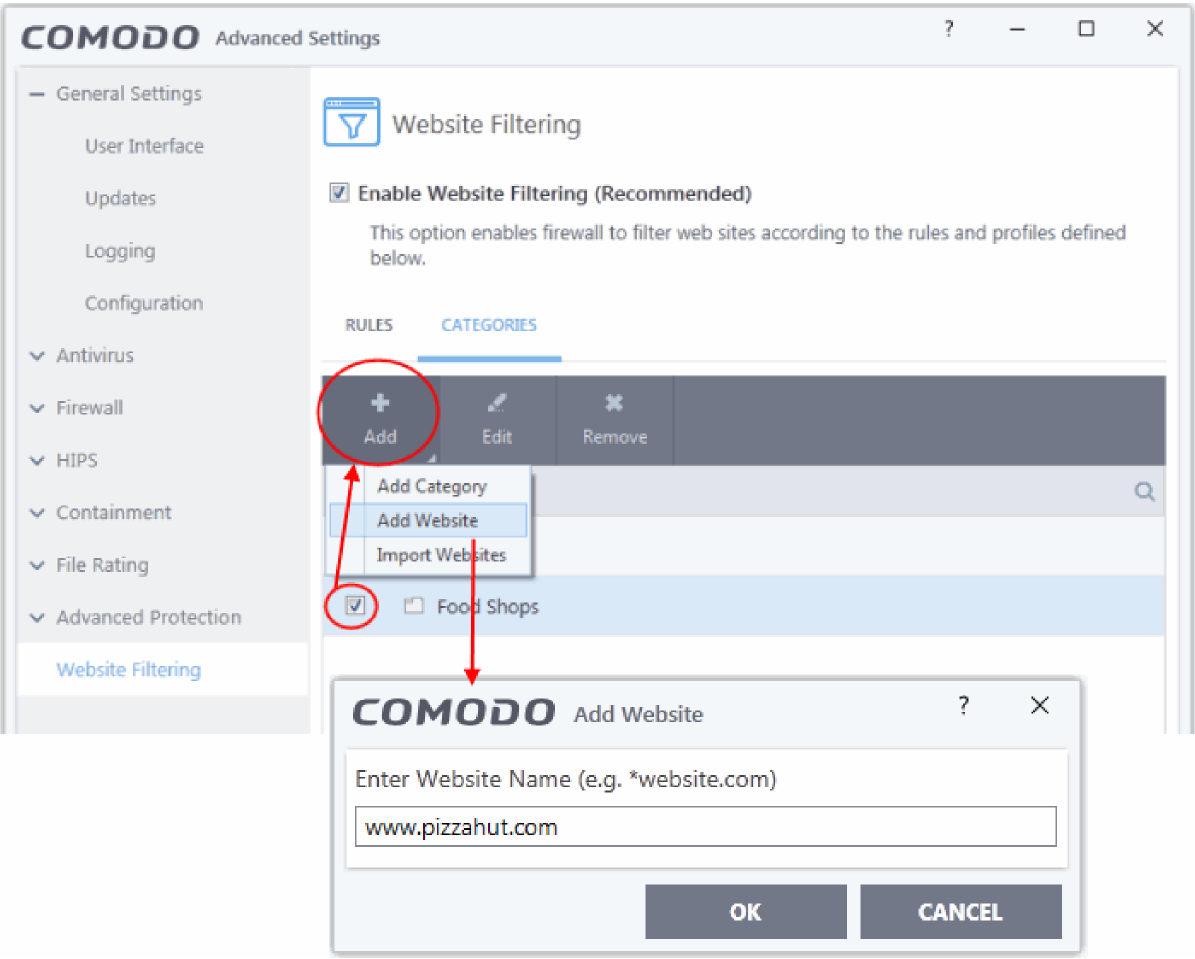


4. Click 'Add' from the options at the top and choose 'Add Category' from the drop-down. The 'Edit Property' dialog will open:



5. Enter a name for the category and click 'OK'. The new category will be created and added under the 'Categories' tab.

6. Select the new category > Click 'Add' from the options at the top > Choose 'Add Website' from the drop-down. The 'Add Website' dialog will open:



7. Type the website or text string you wish to add to the category. See the following notes for advice on this:

- To add a specific website/webpage, enter the full URL of the website/webpage
- To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
- To include all websites with URLs that start with a specific string, add a wildcard character after

the string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.

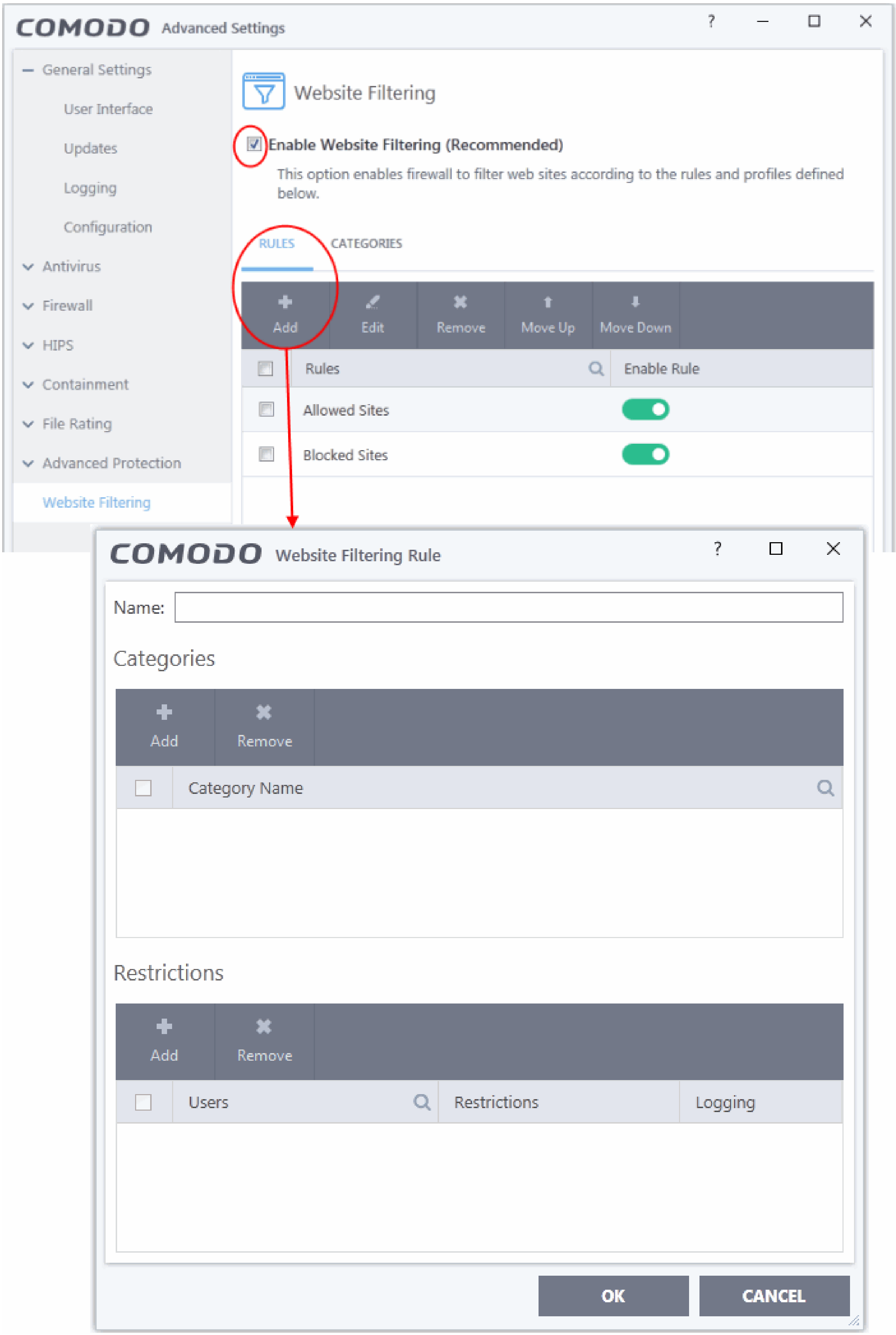
- To include all websites with URLs that contain a specific string, add the wildcard character before and after the string. For example, “*pizza*” will cover hotpizzanow.com, spicypizzadishes.net and so on.

The website(s) will be added to the category.

8. Repeat the process to add more websites to the category.
9. Repeat the process to add more website categories
10. Click 'OK' in the 'Advanced Settings' interface to save your settings

Create rules to block or allow websites to specific users

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface.
2. Click 'Website Filtering' on the left.
3. Ensure that the 'Enable Website Filtering' checkbox is selected.
4. Click the 'Rules' tab and click 'Add' from the options at the top. The 'Website Filtering Rule' dialog will be opened.



☑ Enable Website Filtering (Recommended)

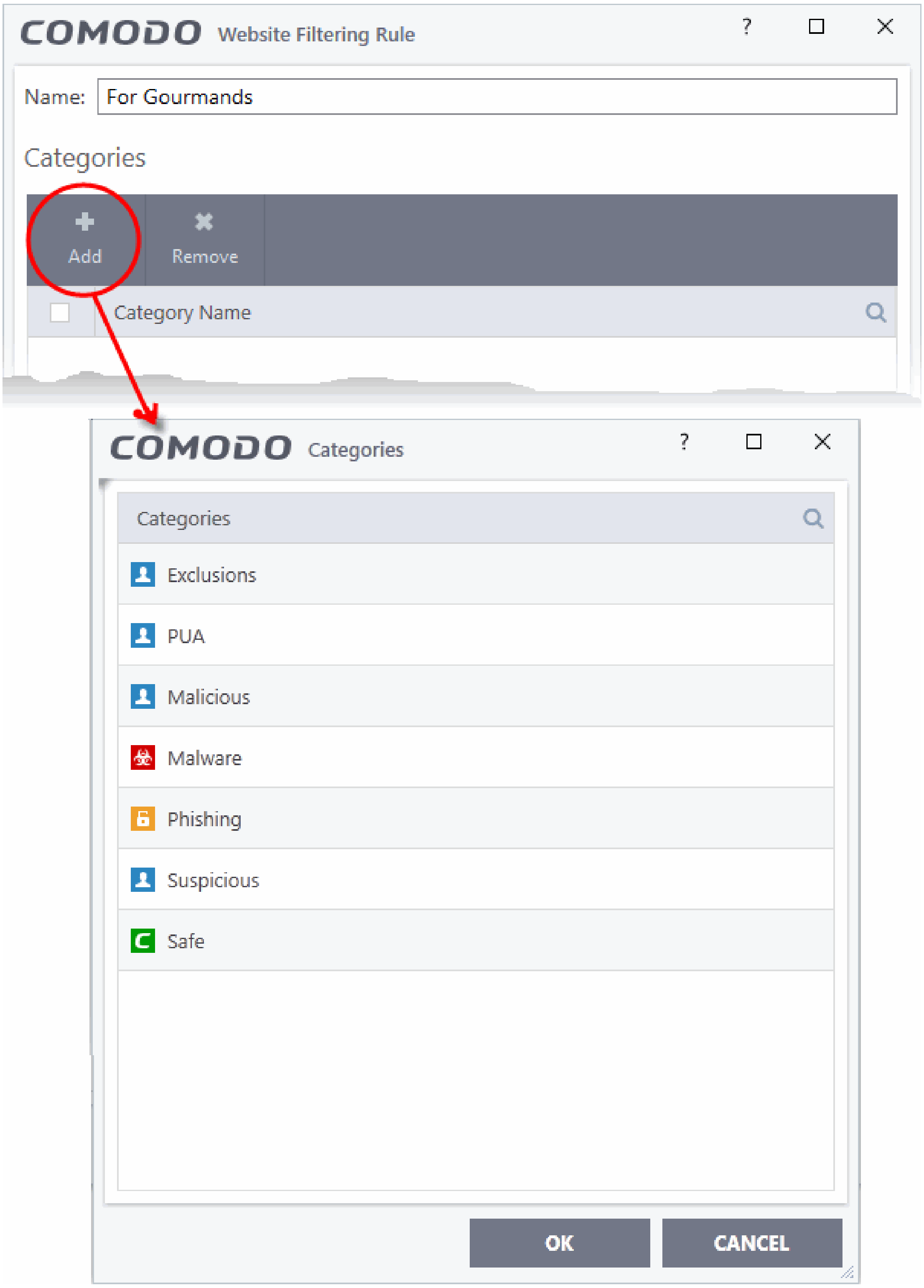
This option enables firewall to filter web sites according to the rules and profiles defined below.

Rules	Enable Rule
Allowed Sites	●
Blocked Sites	●

5. Enter a name for your new filter in the 'Website Filtering Rule' dialog.

6. Select the categories that should be added to the filter:

    - Click 'Add' under the Categories'.



The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Safe Sites -** Websites that are considered safe according to the global whitelist
- **Phishing Sites -** Fake copies of popular banking, shopping and social media websites that

intend to steal customer data

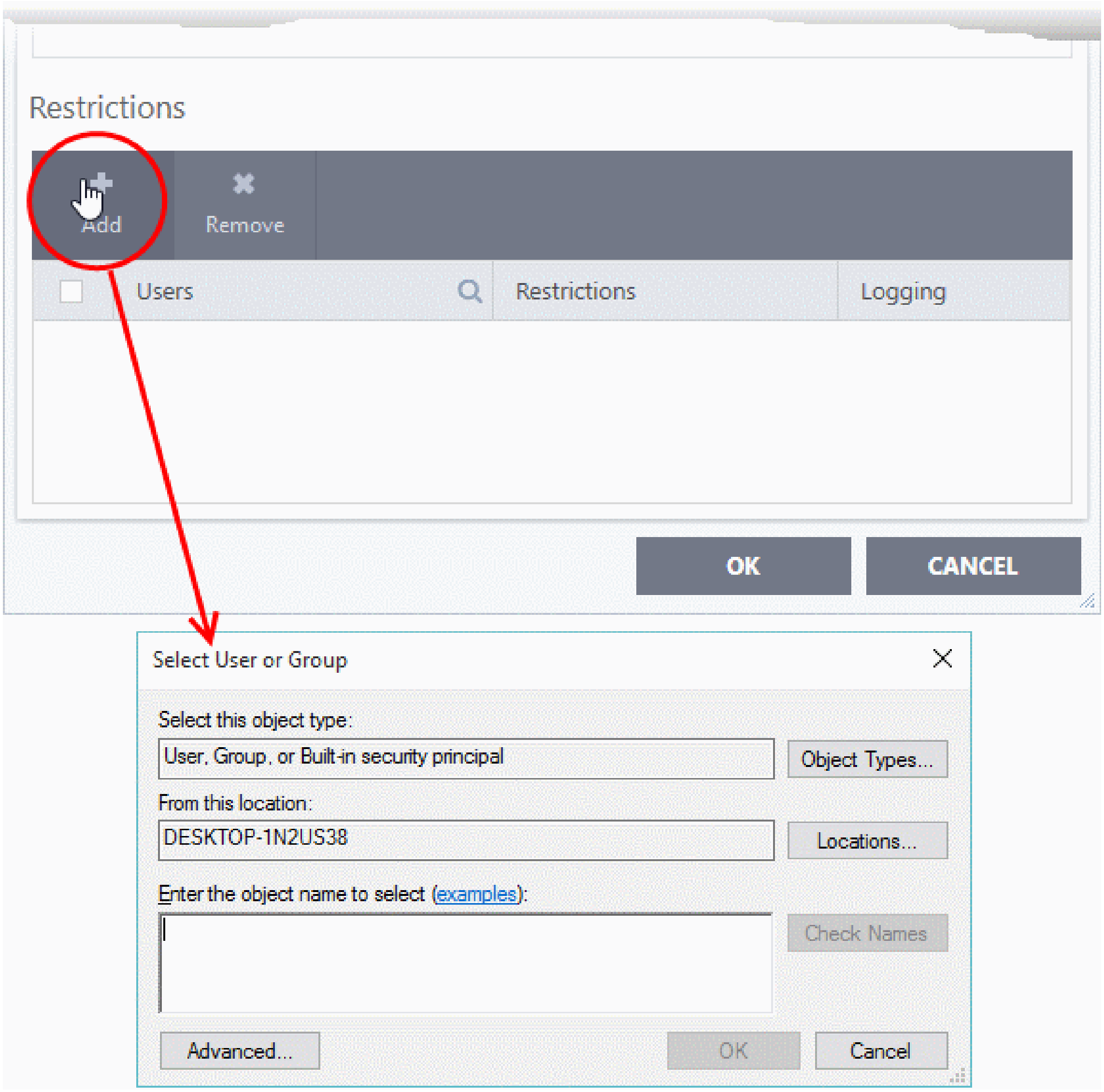
- **Malware Sites -** The URL leads to a direct malware download. Malware is designed to damage your computer, steal sensitive information or gain unauthorized access to your system.
- **Exclusions** - Websites you have decided to trust and allow connections to for the current session and future sessions.
- **PUA Sites** - Sites that host'Potentially Unwanted Applications' (PUA). While not strictly speaking malware, a PUA is a piece of software that has functionality that may not have been made clear to a user. An example is a browser toolbar which tells you the weather forecast, but which also tracks your online activity or serves you adverts.
- **Malicious Sites** - Sites that are known to host or contain links to malware, malicious scripts or deceptive content. These are intended to cause damage to your computer or steal personal data.
- **Suspicious Sites** - Sites which have shown strong evidence of suspicious behavior but have not yet hosted content which would warrant placing them in the 'Malware' or 'Malicious' categories. Users are advised to be on high alert should they visit these sites.

- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

For more details on creating and modifying categories, see **Website Categories.**

7. Add Users or User Groups to whom the rule should be applied:

- Click 'Add' from the options at the top beneath the 'Restrictions' pane. The 'Select User or Group' dialog will appear:



Select this object type:

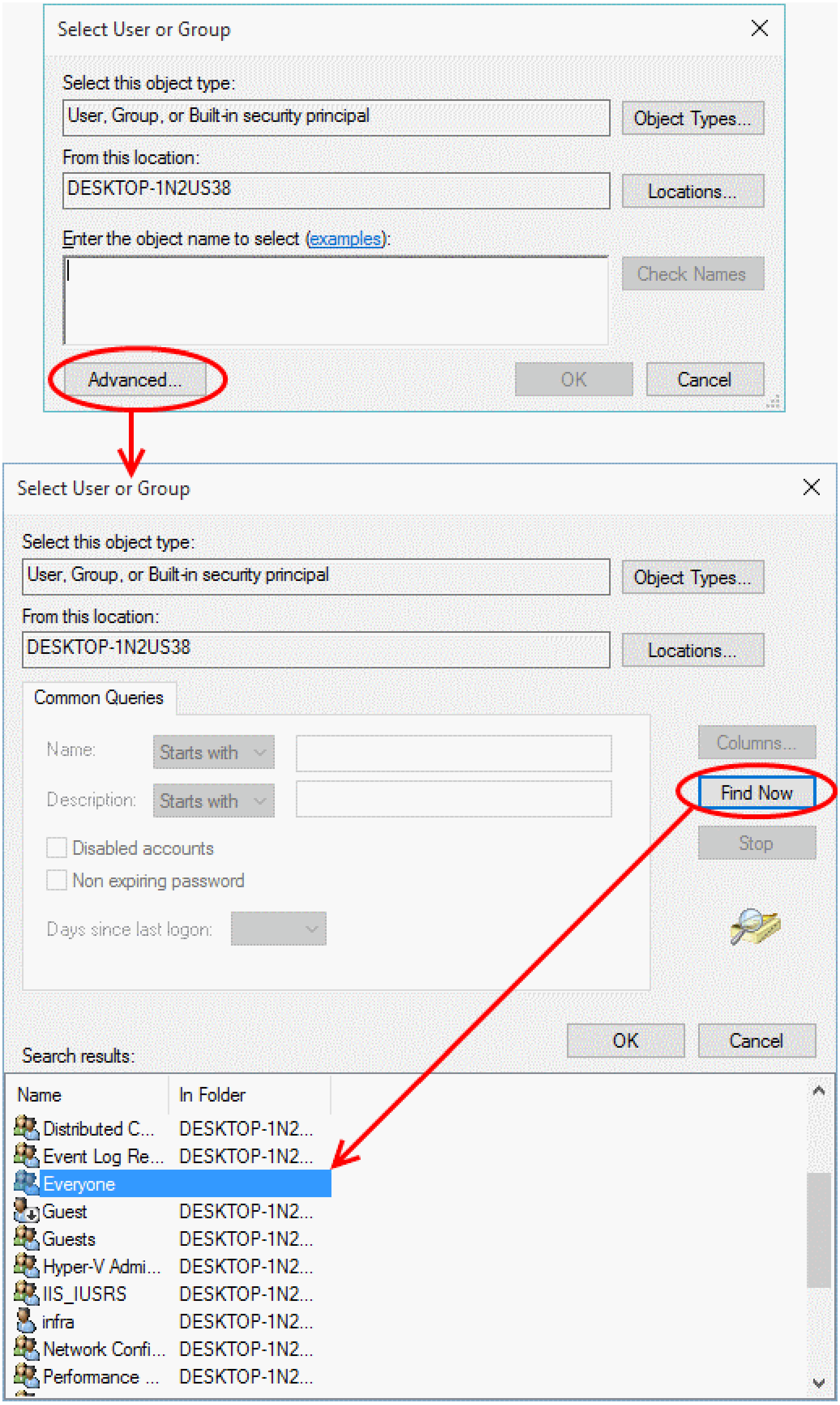
User, Group, or Built-in security principal

From this location:

DESKTOP-1N2US38

Enter the object name to select (examples):

- Enter the names of users to whom the filter should apply in the 'Enter the object name to select' box. Use the format [domain name]/[user/group name] or [user/group name]@[domain name]. Alternatively, click 'Advanced' then 'Find Now' to locate specific users.



Select this object type:
User, Group, or Built-in security principal

From this location:
DESKTOP-1N2US38

Enter the object name to select (examples):

Select this object type:
User, Group, or Built-in security principal

From this location:
DESKTOP-1N2US38

Name: Starts with

Description: Starts with

□ Disabled accounts

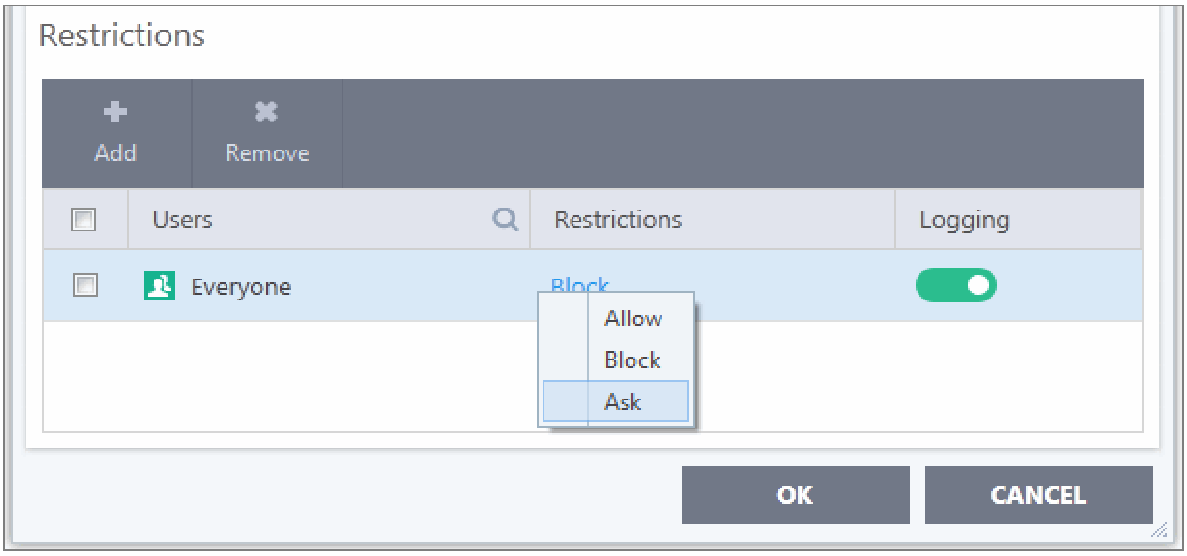
□ Non expiring password

Days since last logon:

Search results:

Name	In Folder
Distributed C...	DESKTOP-1N2...
Event Log Re...	DESKTOP-1N2...
Everyone	
Guest	DESKTOP-1N2...
Guests	DESKTOP-1N2...
Hyper-V Admi...	DESKTOP-1N2...
IIS_IUSRS	DESKTOP-1N2...
infra	DESKTOP-1N2...
Network Confi...	DESKTOP-1N2...
Performance ...	DESKTOP-1N2...

- After adding users or groups, you need to specify what restriction will apply to them. You can allow or block them from viewing the websites in the category or ask them if they want to continue. This is done by modifying the link in the 'Restrictions' column:



Allow - The websites in the categories can be accessed by the user.

Block - The websites in the categories cannot be accessed by the user.

Ask - An alert will be displayed in the browser if the user tries to access any of the websites in the category. The user can decide whether or not to continue.

- Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.

8. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
9. Ensure that the rule is enabled using the toggle switch under the 'Enable Rule' column for the rule to take effect.

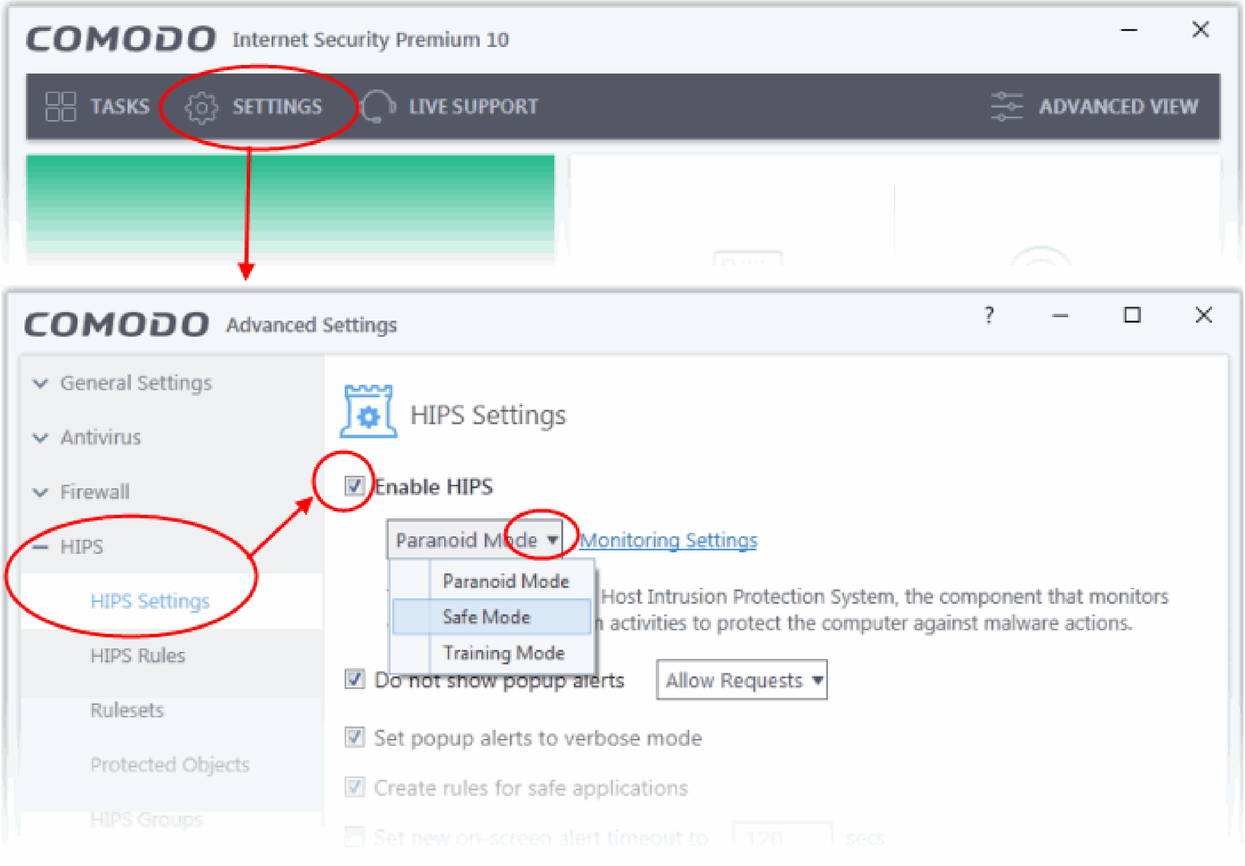
You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Set up HIPS for Maximum Security and Usability

This page explains how to configure the Host Intrusion Prevention System (HIPS) component to provide maximum security against malware and hackers.

To configure HIPS

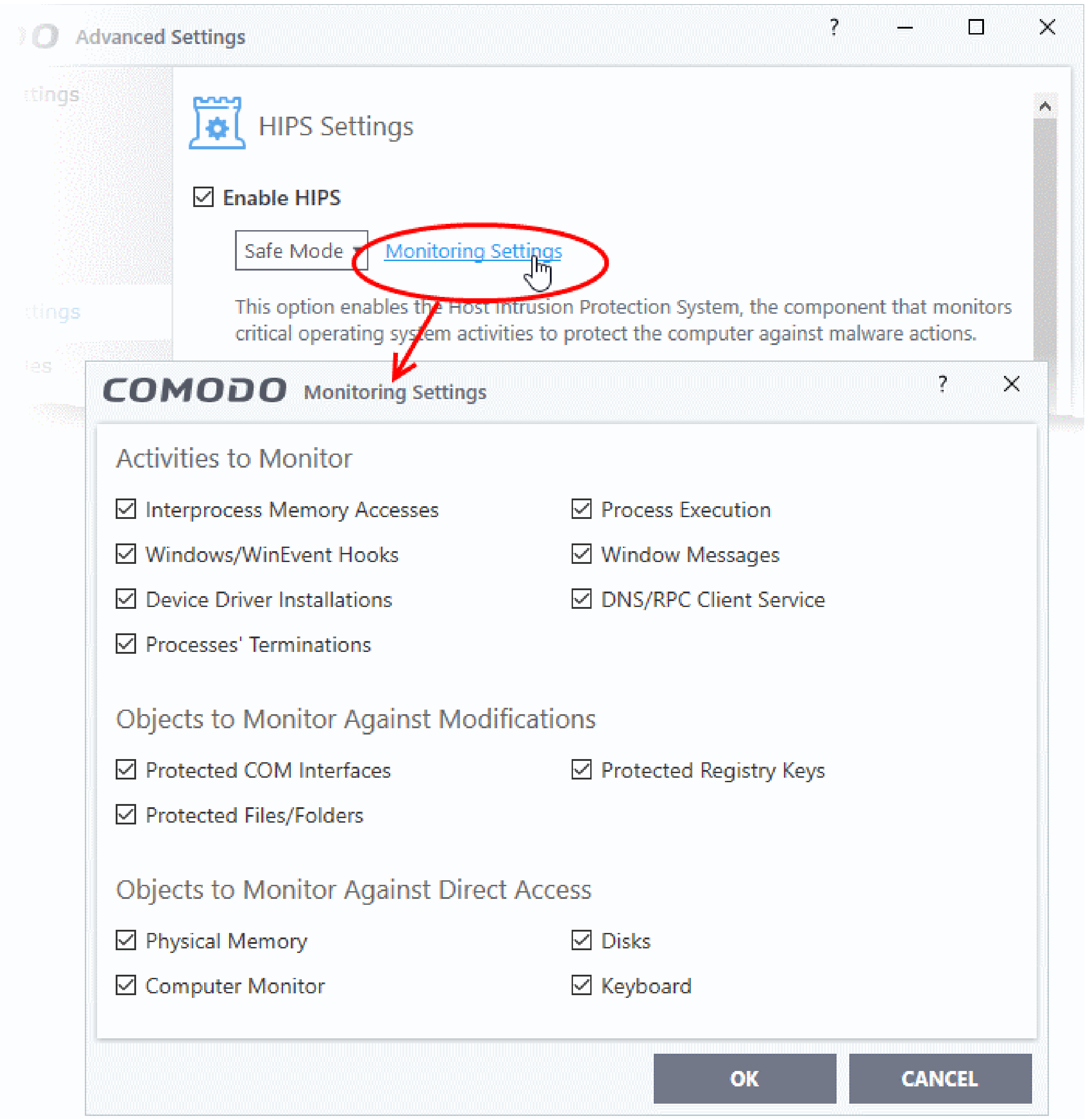
1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'HIPS Settings' under 'HIPS' on the left.
3. Select 'Enable HIPS'



4. Choose 'Safe Mode' from the drop-down. See **HIPS Settings** for more details.

Monitoring Settings

1. Click the 'Monitoring Settings' link in the 'HIPS Settings' interface



Advanced Settings

HIPS Settings

☑ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

COMODO Monitoring Settings

Activities to Monitor

☑ Interprocess Memory Accesses
☑ Windows/WinEvent Hooks
☑ Device Driver Installations
☑ Processes' Terminations
☑ Process Execution
☑ Window Messages
☑ DNS/RPC Client Service

Objects to Monitor Against Modifications

☑ Protected COM Interfaces
☑ Protected Files/Folders
☑ Protected Registry Keys

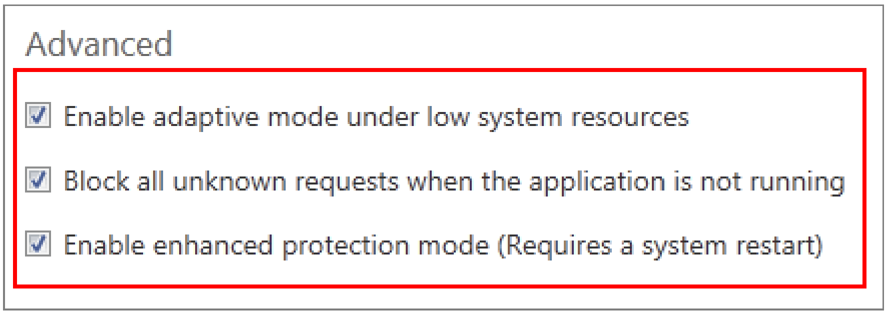
Objects to Monitor Against Direct Access

☑ Physical Memory
☑ Computer Monitor
☑ Disks
☑ Keyboard

2. Make sure that all the check boxes are selected and click 'OK'

Advanced Settings

1. Enable the following settings in the 'Advanced' area of the HIPS Settings interface:



Advanced

☑ Enable adaptive mode under low system resources

☑ Block all unknown requests when the application is not running

☑ Enable enhanced protection mode (Requires a system restart)

- Optional - Enable 'Block all unknown requests if the application is not running'. Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already ‘clean’ and are looking just to enable the highest CIS security settings, then it is 'OK' to leave this box unchecked.

- If you are using a 64-bit system, in order to maximize the security, it is important to select 'Enable enhanced protection mode (Requires a system restart)' - Enabling this mode will activate additional host intrusion prevention techniques in HIPS to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures.
- Because of limitations in Windows 7x64, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS functionality.

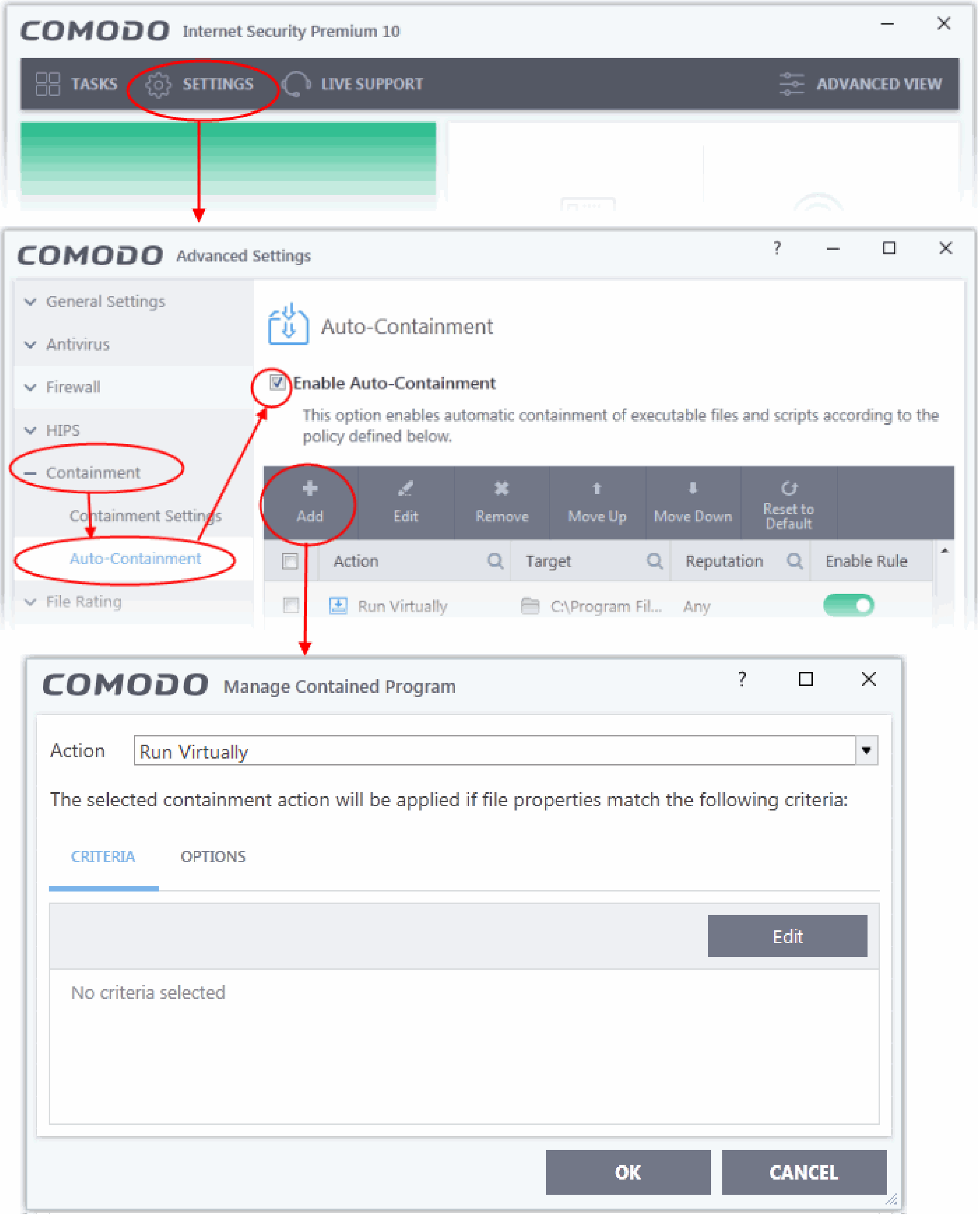
Click here for more details on HIPS Settings

Create Rules to Auto-Contain Applications

- Auto-containment rules allow you to define which types of files should be automatically contained.
- You can contain files based on various criteria, including location and file source.
- A contained application has much less opportunity to damage your computer because it is run isolated from your operating system and your files.
- CIS ships with a set of pre-defined auto-containment rules that are configured to provide maximum protection for your system.
- Before creating a rule, first check if your requirements are met by the default rules. See **Rules for Auto-Containment** for more details.

To create auto-containment rules

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Containment' > 'Auto-Containment' on the left
3. Ensure that 'Enable Auto-Containment' is selected
4. Click 'Add'



Auto-Containment

☑ Enable Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

Action	Target	Reputation	Enable Rule
Run Virtually	C:\Program Fil...	Any	●

Action: Run Virtually

The selected containment action will be applied if file properties match the following criteria:

No criteria selected

The 'Manage Contained Program' dialog will open. It contains two tabs:

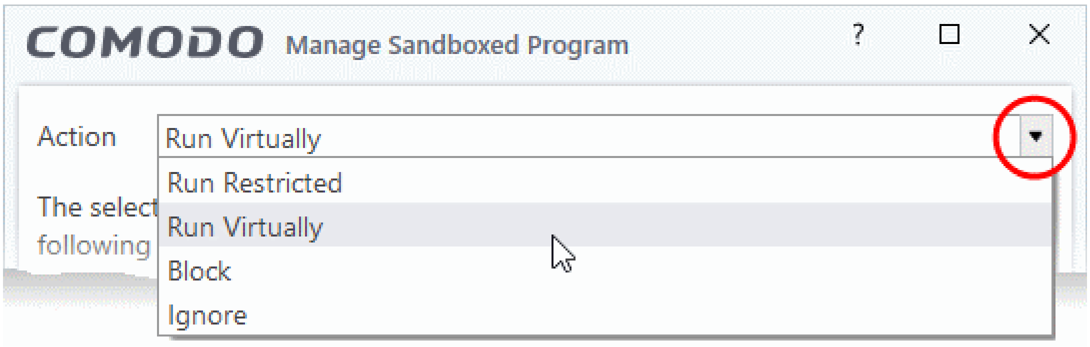
- **Criteria** - Allows you to define conditions upon which the rule should be applied.
- **Options** - Allows you to configure additional actions like logging, memory usage and execution time restrictions.

You can create new containment rules from the 'Manage Contained Program' interface in three steps:

- Step 1 - Choose the action
- Step 2 - Select the target file/group and set the filter criteria for the target files
- Step 3 - Select the options

Step 1 - Select the Action

The options in the 'Action' drop-down combined with the restriction level in the 'Options' tab determine the amount of privileges an auto-contained application has to access other software and hardware resources on your computer.



The options available under the 'Action' button are:

- **Run Virtually** - The application will be run in a virtual environment, completely isolated from your operating system and files on the rest of your computer.
- **Run Restricted** - The application is allowed to access limited operating system resources. The application is not allowed to execute more than 10 processes at a time and has few access rights. Some applications, like computer games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be contained and allowed to run with all privileges.

- Choose the action from the options.

Step 2 - Select the target file/group and set the filter criteria for the target files

The next step is to select the target application(s)/file(s) and to configure the filter parameters. If you want to include multiple items in a rule but only want the rule to be applied under certain conditions, then you can do so in this step.

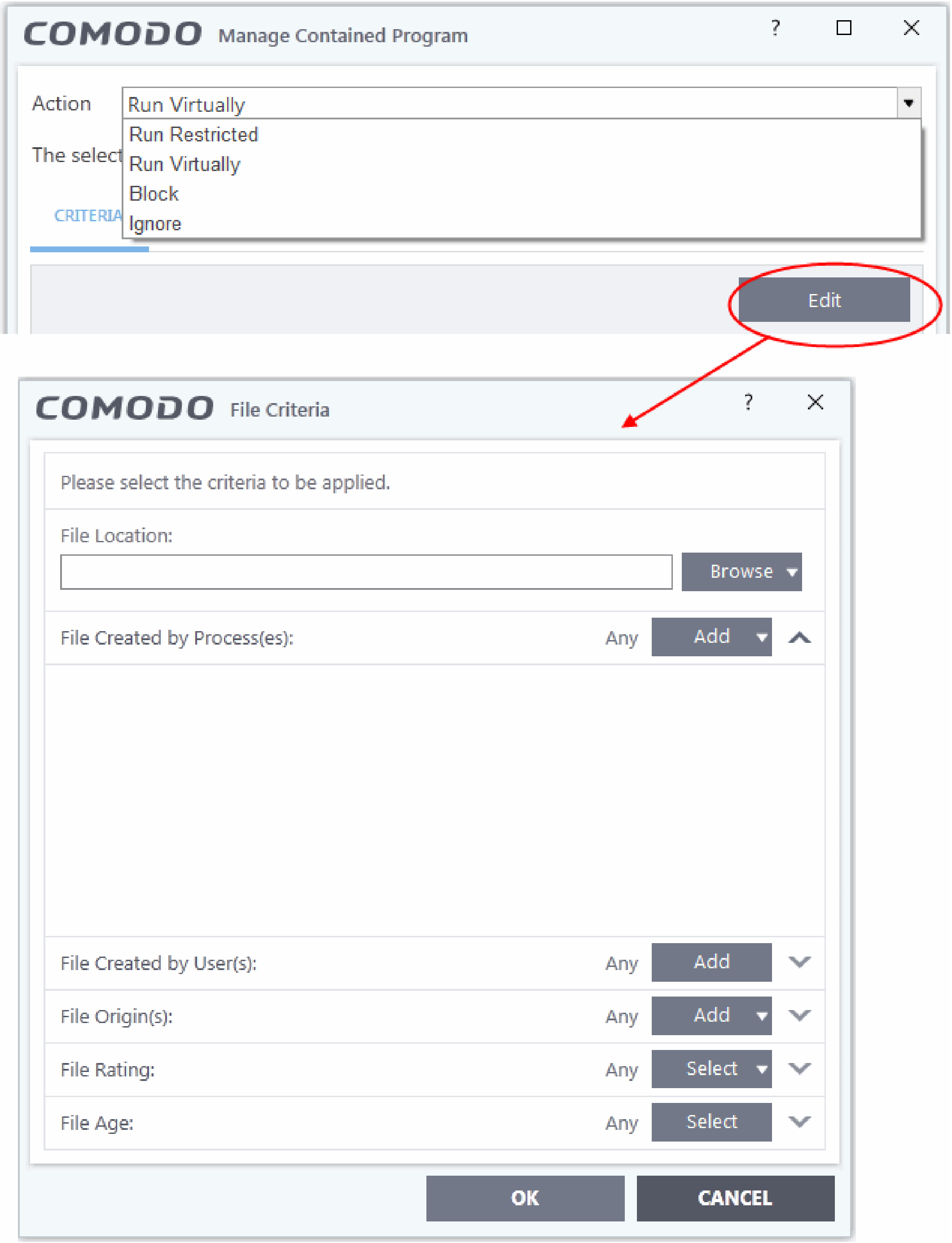
For example, you may want to include all executables in the 'Target' but only want the rule to be applied to executables downloaded from the internet. Another example is if you want to run unrecognized files created by a specific user outside the container - you would create an 'Ignore' rule with 'All Applications' as the target and files created by the specific user as the filter criteria.

To select the target and set the filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- To add new target and filter criteria, click the 'Edit' button at the far right



COMODO Manage Contained Program

Action: Run Virtually

Run Restricted
Run Virtually
Block
Ignore

The select

CRITERIA

Edit

COMODO File Criteria

Please select the criteria to be applied.

File Location:

Browse

File Created by Process(es): Any

Add

File Created by User(s): Any

Add

File Origin(s): Any

Add

File Rating: Any

Select

File Age: Any

Select

OK

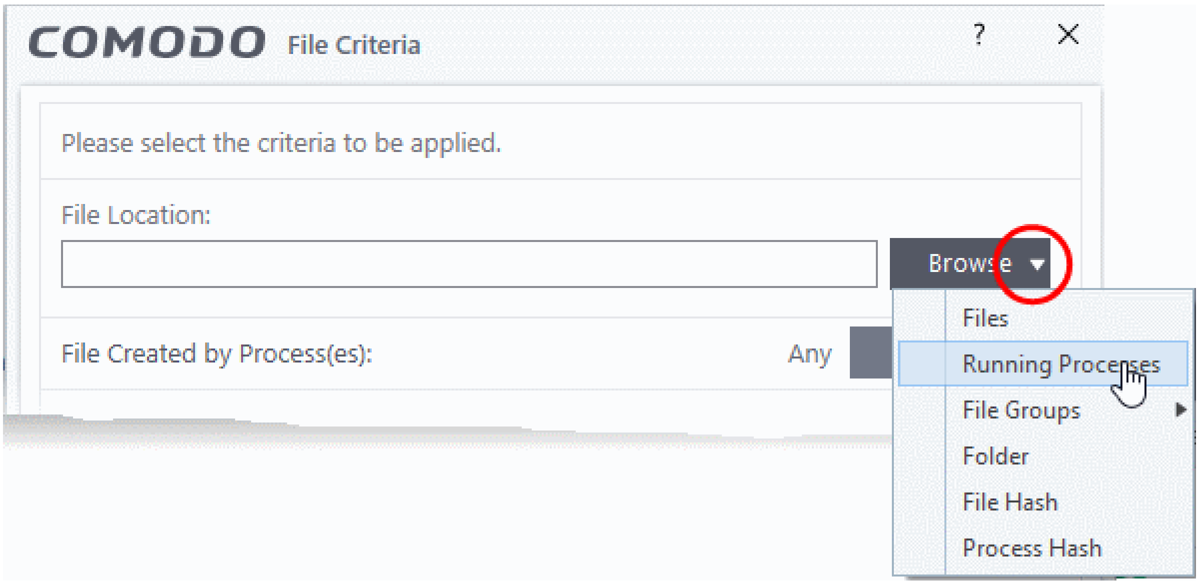
CANCEL

The 'File Criteria' dialog will open. The file criteria dialog allows you:

- Select the target
- Configure the filter criteria

Select the target

- To select the target, click the 'Browse' button beside the 'File Location' field

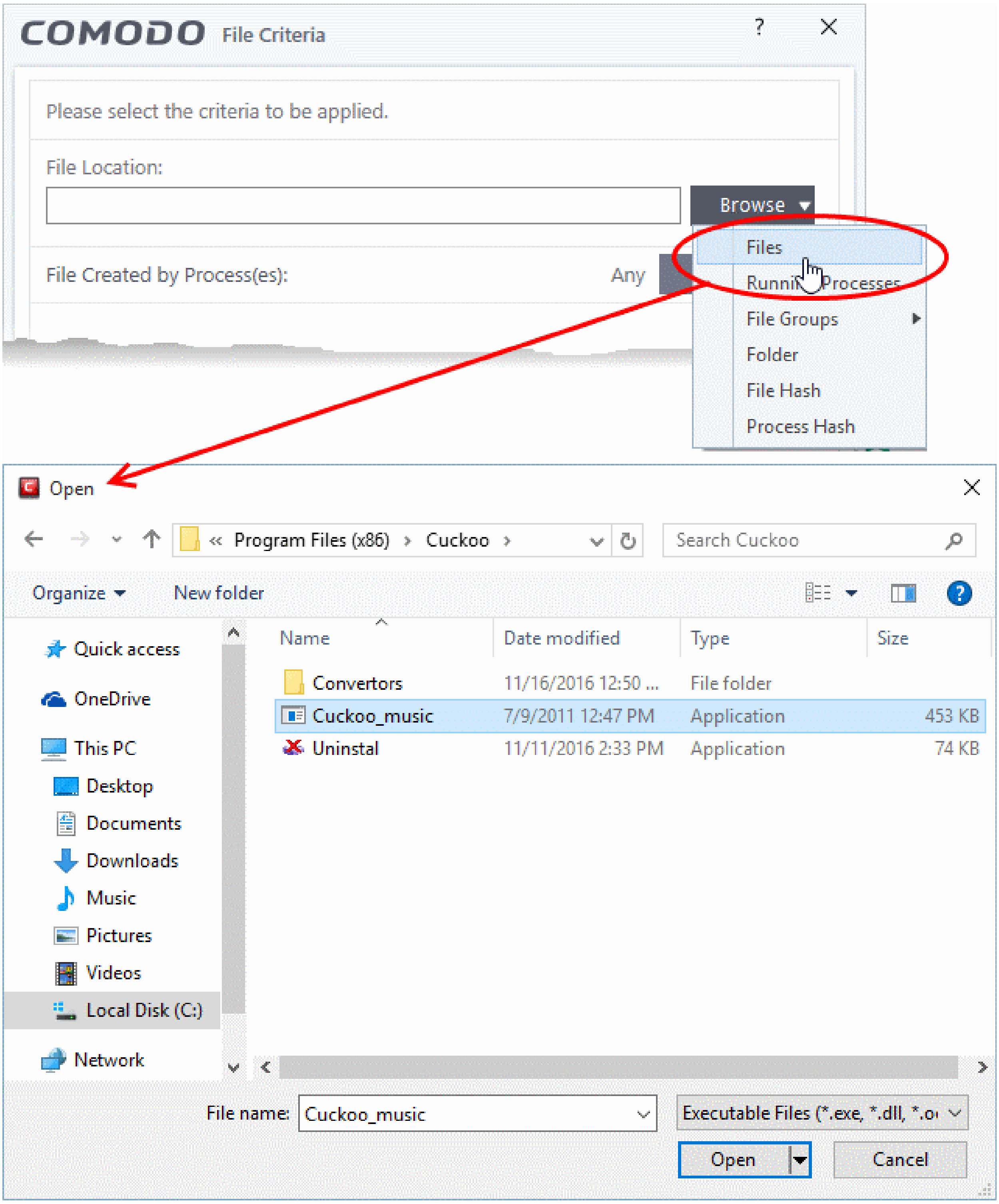


You have six options available to add the target path:

- **Files** - Allows you to add individual files as the target.
- **Running Processes** - As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** - Allows to add predefined File Groups as target. See **File Groups**, to add or modify a predefined file group
- **Folder** - Allows you to add a folder or drive as the target
- **File Hash** - Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

Adding an individual File

- Choose 'Files' from the 'Browse' drop-down.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

File Created by Process(es): Any

Open

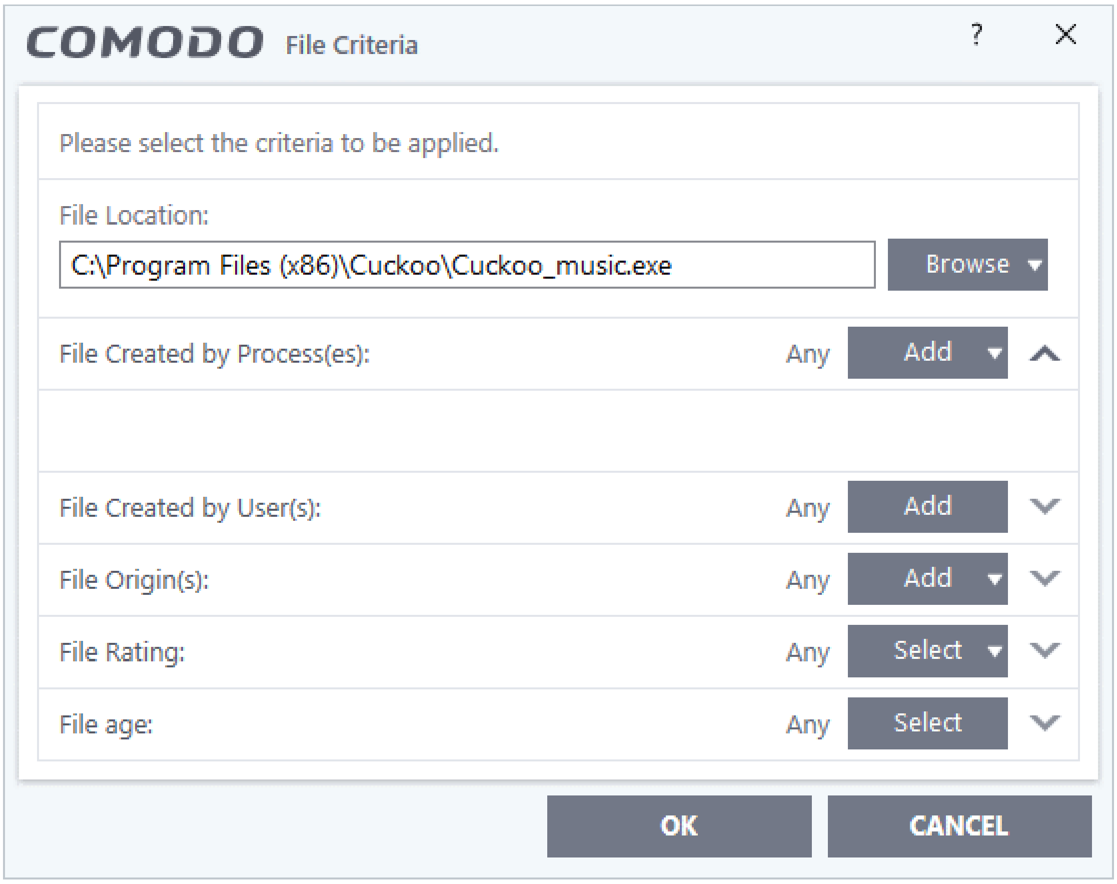
« Program Files (x86) › Cuckoo ›

Name	Date modified	Type	Size
Convertors	11/16/2016 12:50 ...	File folder	
Cuckoo_music	7/9/2011 12:47 PM	Application	453 KB
Uninstal	11/11/2016 2:33 PM	Application	74 KB

File name: Cuckoo_music

Executable Files (*.exe, *.dll, *.o

- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'
- The file will be added as target and will be run as per the action chosen in **Step 1.**



File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

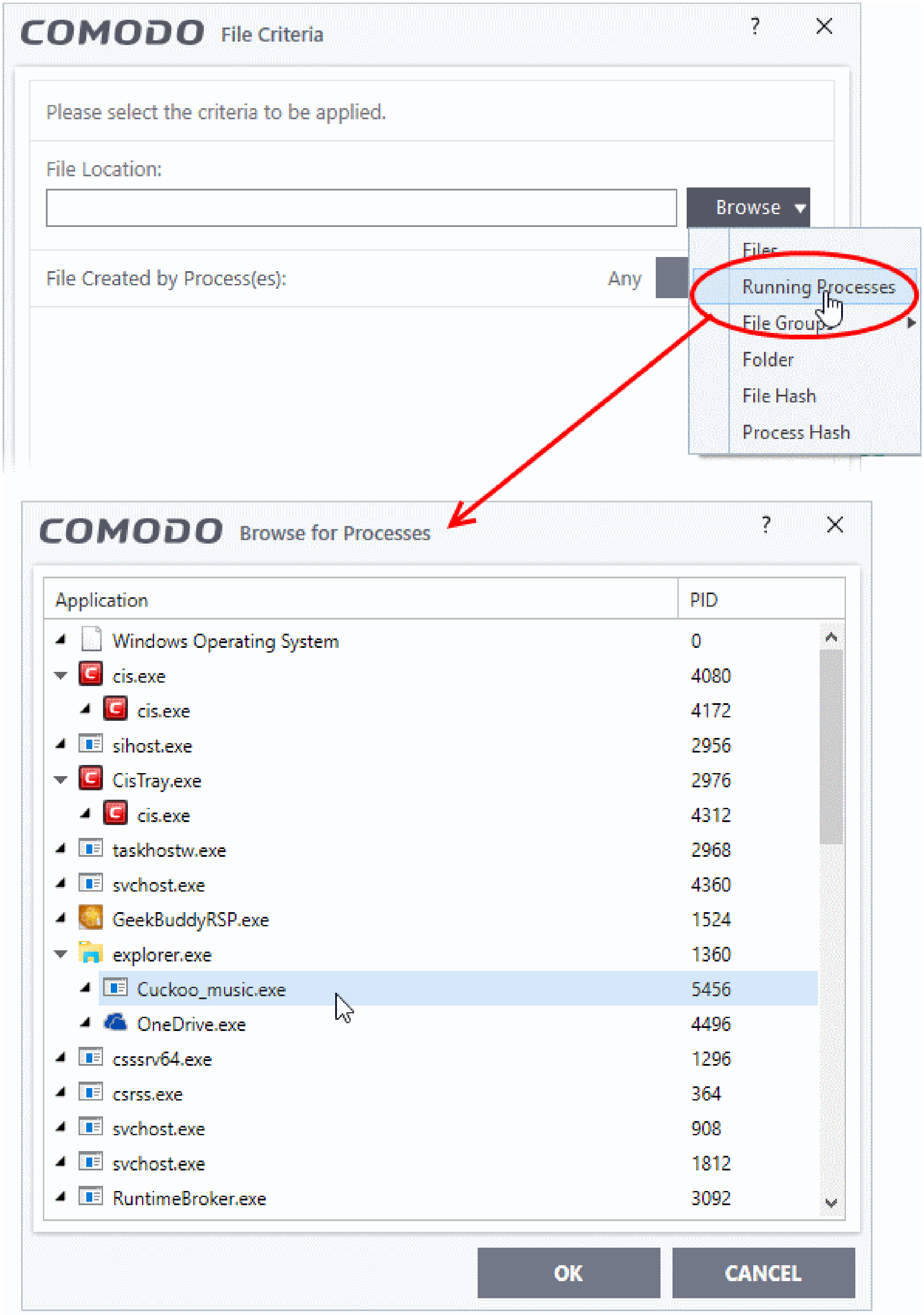
File Rating: Any

File age: Any

If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any'. For 'Options' it will be 'Log when this action is performed'. If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Add a currently running application by choosing its process

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



Please select the criteria to be applied.

File Location:

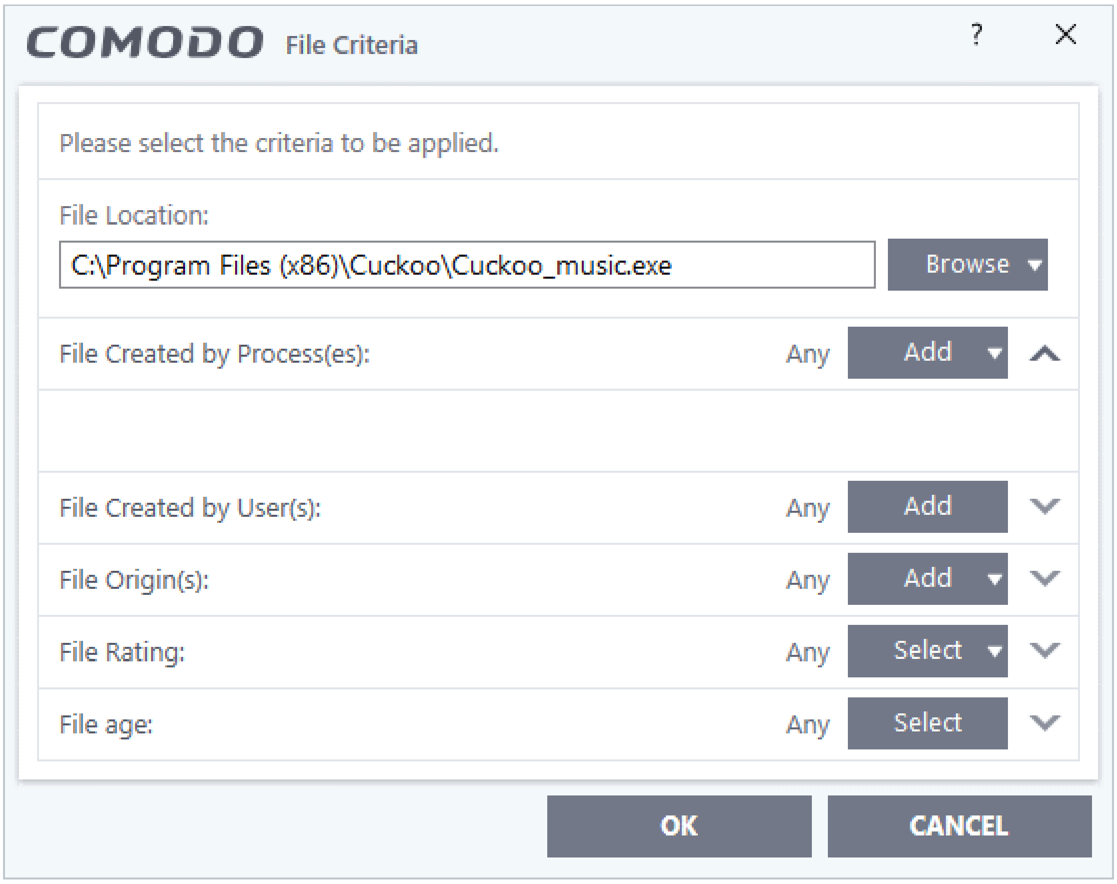
File Created by Process(es): Any

Application	PID
Windows Operating System	0
cis.exe	4080
cis.exe	4172
sihost.exe	2956
CisTray.exe	2976
cis.exe	4312
taskhostw.exe	2968
svchost.exe	4360
GeekBuddyRSP.exe	1524
explorer.exe	1360
Cuckoo_music.exe	5456
OneDrive.exe	4496
csssrv64.exe	1296
csrss.exe	364
svchost.exe	908
svchost.exe	1812
RuntimeBroker.exe	3092

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

- Select the process belonging to the parent application you want to add and click 'OK'.

The file will be added as the target and will be run as per the action chosen in **Step 1**



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

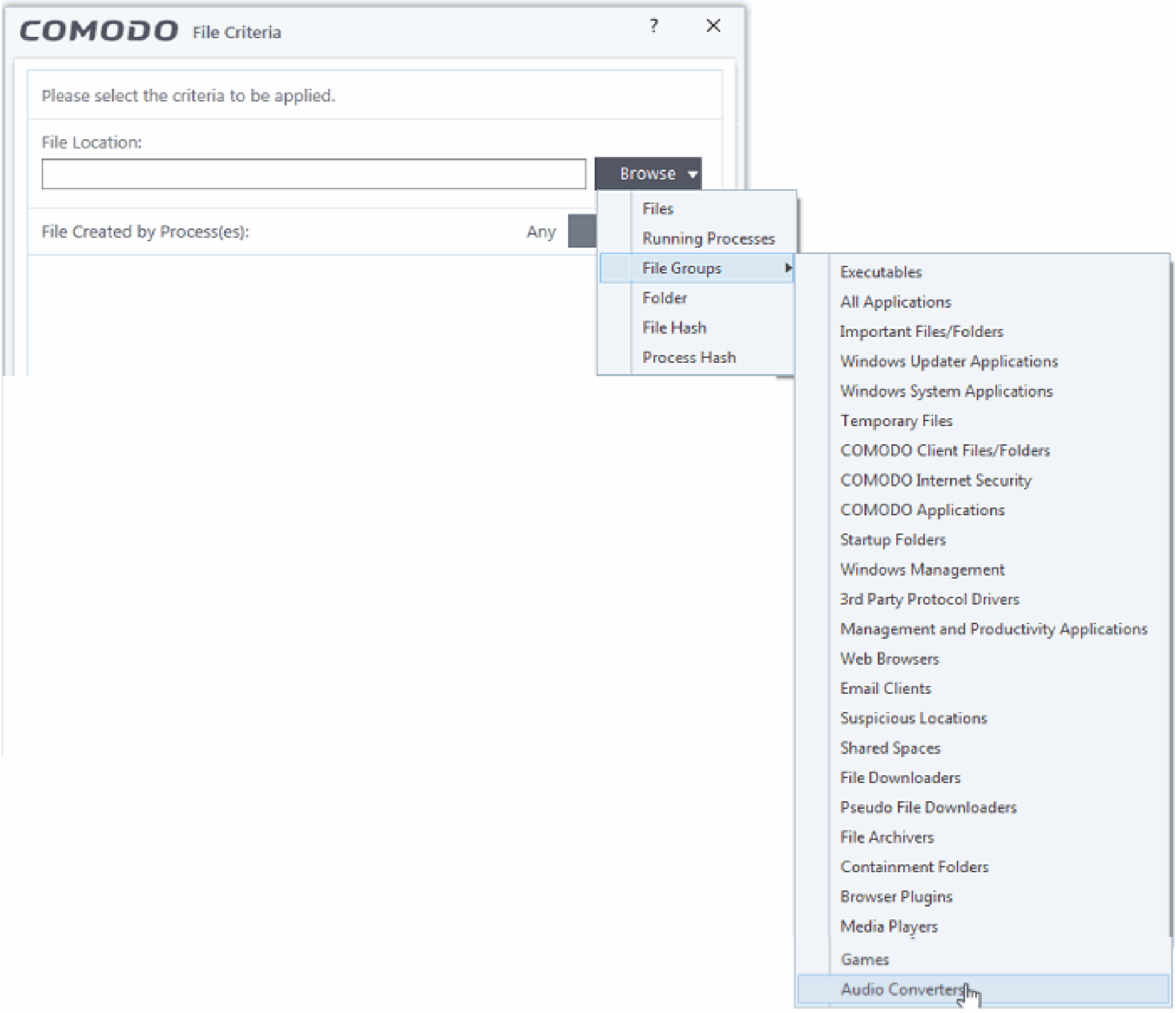
File Rating: Any

File age: Any

If you just want to add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for 'filter criteria' and 'file rating' will be 'Any'. For 'Options' it will be 'Log when this action is performed'. If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a File Group

- Choose 'File Groups' from the 'Browse' drop-down. This allows you to include a category of files or folders configured as a 'File Group'. See **File Groups**, for more details on viewing and managing pre-defined and user-defined file groups.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

File Created by Process(es): Any

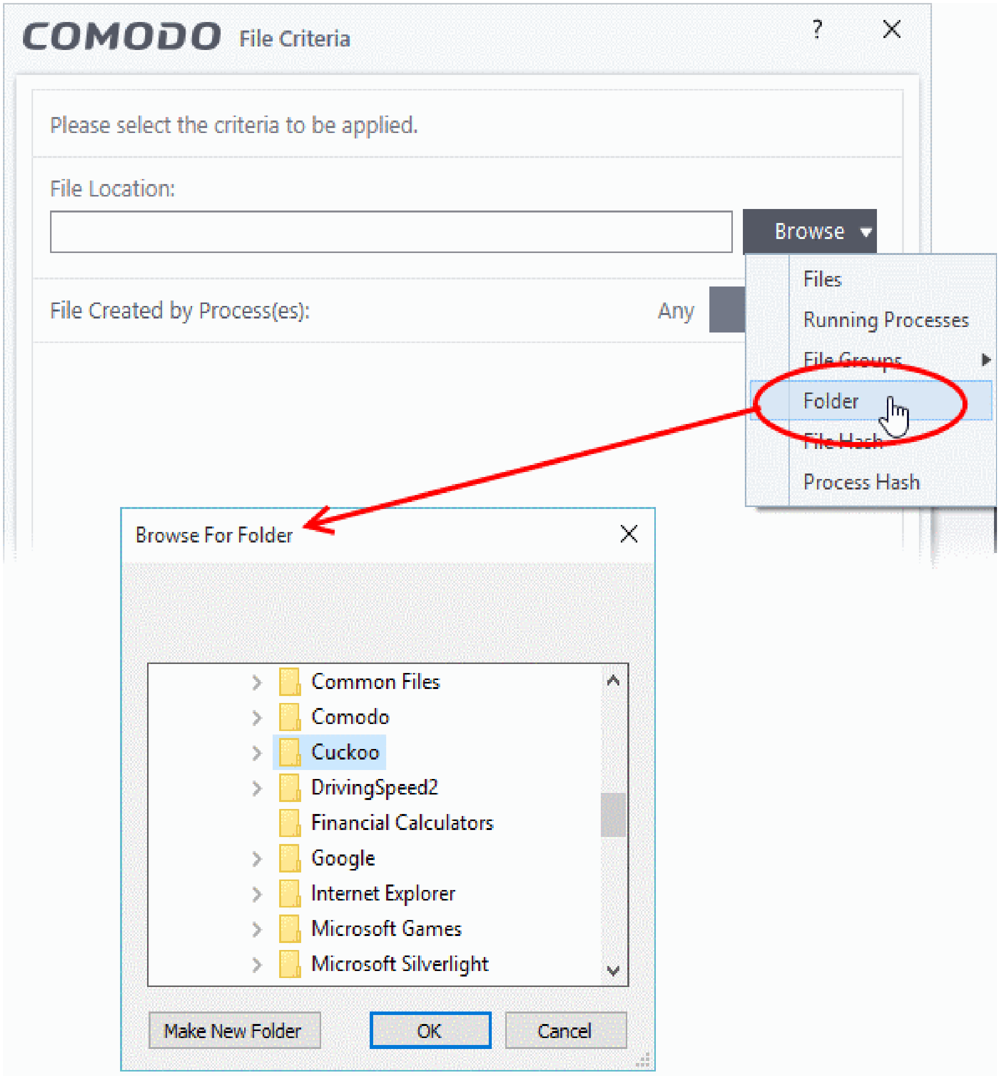
- Select the file group from the drop-down.

The file group will be added as target and will be run as per the action chosen in **Step 1**.

If you want to just add the applications in the file group for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.



The 'Browse for Folder' dialog will appear.

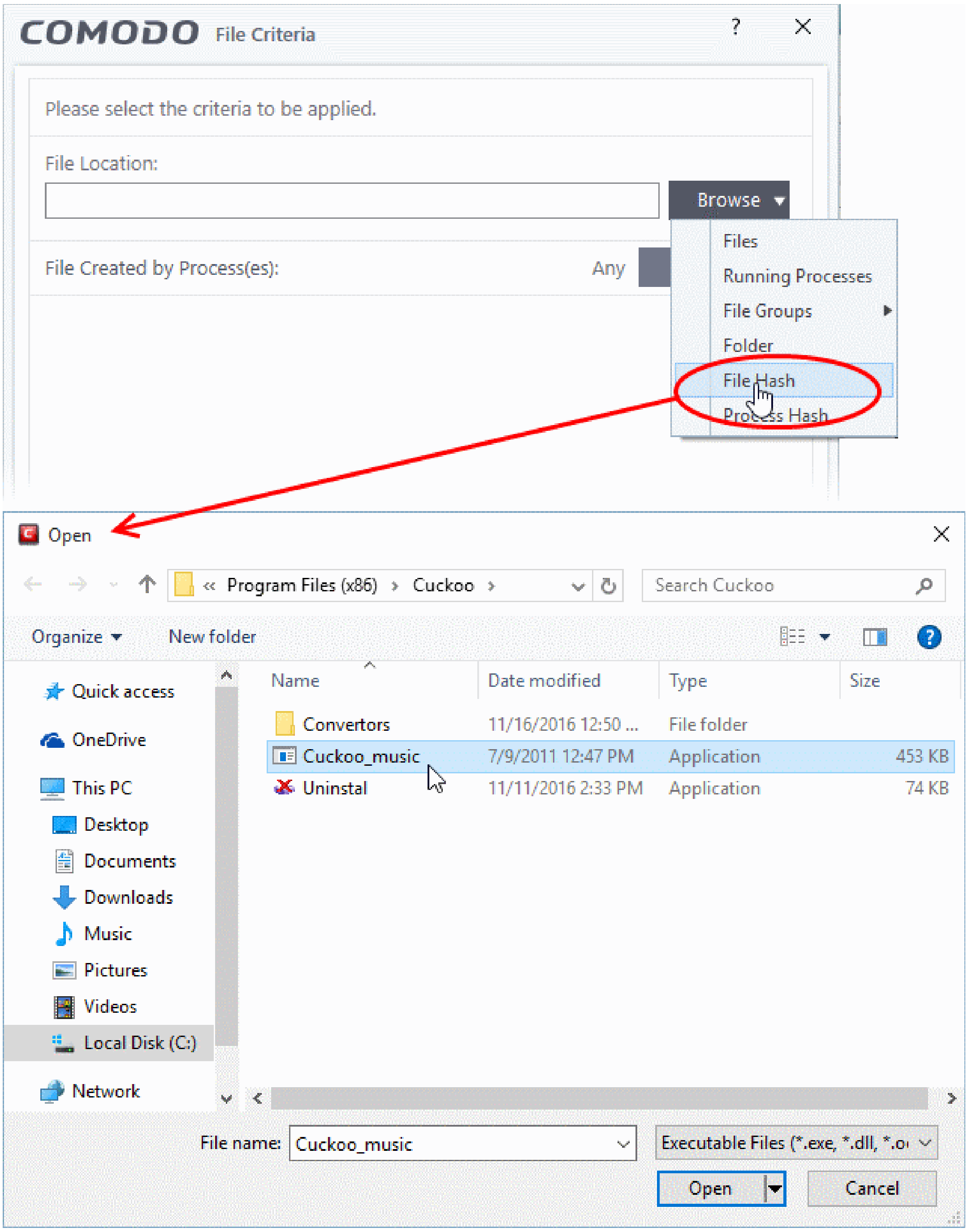
- Navigate to the drive partition or folder you want to add as target and click 'OK'

The drive partition/folder will be added as the target. All executable files in the folder will be run as per the action chosen in **Step 1**.

If you want to just add the applications in the folder/partition for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a file based on its hash value

- Choose 'File Hash' from the 'Browse' drop-down.



Name	Date modified	Type	Size
Convertors	11/16/2016 12:50 ...	File folder	
Cuckoo_music	7/9/2011 12:47 PM	Application	453 KB
Uninstal	11/11/2016 2:33 PM	Application	74 KB

File name: Cuckoo_music

Executable Files (*.exe, *.dll, *.o

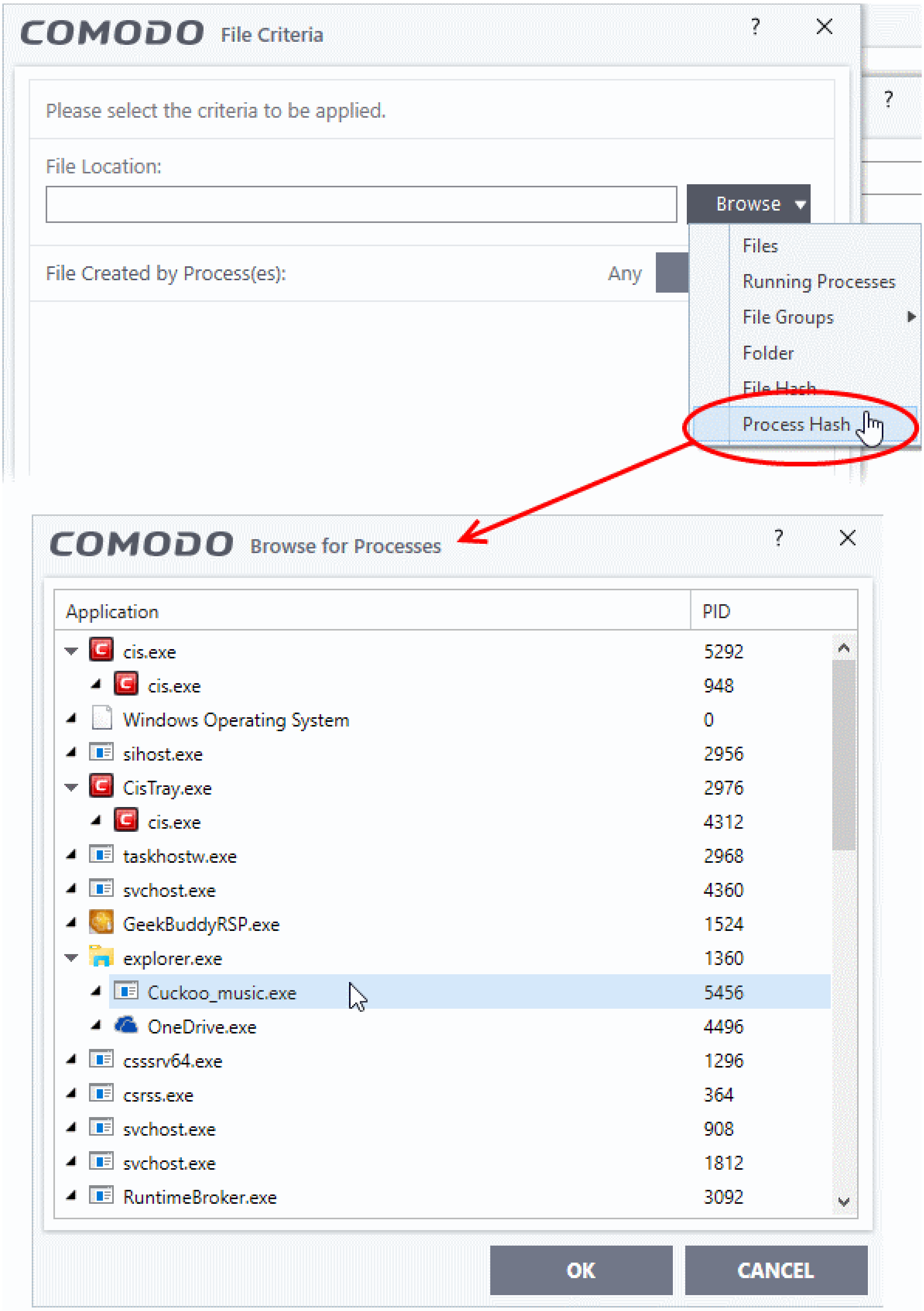
- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'

The file will be added as target and will be run as per the action chosen in **Step 1**.

If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



COMODO File Criteria

Please select the criteria to be applied.

File Location:

File Created by Process(es): Any

COMODO Browse for Processes

Application	PID
cis.exe	5292
cis.exe	948
Windows Operating System	0
sihost.exe	2956
CisTray.exe	2976
cis.exe	4312
taskhostw.exe	2968
svchost.exe	4360
GeekBuddyRSP.exe	1524
explorer.exe	1360
Cuckoo_music.exe	5456
OneDrive.exe	4496
csssrv64.exe	1296
csrss.exe	364
svchost.exe	908
svchost.exe	1812
RuntimeBroker.exe	3092

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

- Select the process, to add the hash value of its target application to target and click 'OK' from the 'Browse for Process' dialog.

The hash value of the parent executable file will be added as the target and the file will be run as per the action chosen in **Step 1**.

If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

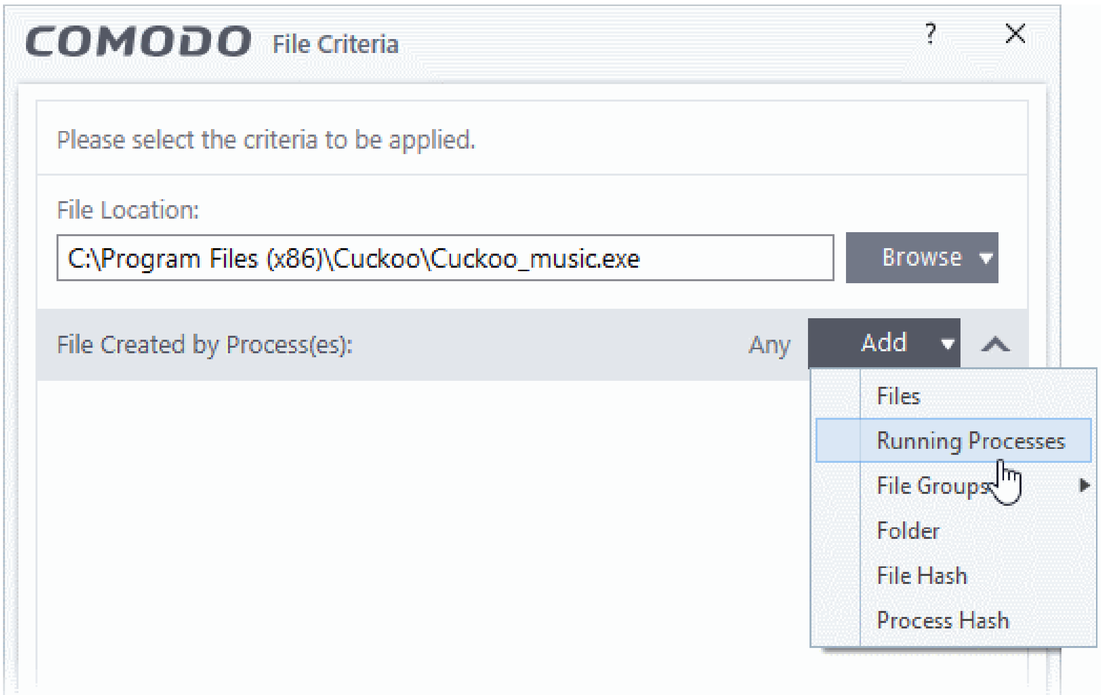
Configure the Filter Criteria and File Rating

You can set the filter criteria, so that the auto-contained action will be applied only to those items that meet the criteria, from the set of items contained in the target. The available filter criteria are:

- **Process(es) that created the file**
- **User(s) that created the file**
- **The origin from which the file was downloaded**
- **The file rating**
- **The age of the file**

To choose the source process(es) to auto-contained the files created by them

- Click the 'File Created by Process(es)' stripe and then click the drop-down arrow beside 'Add'

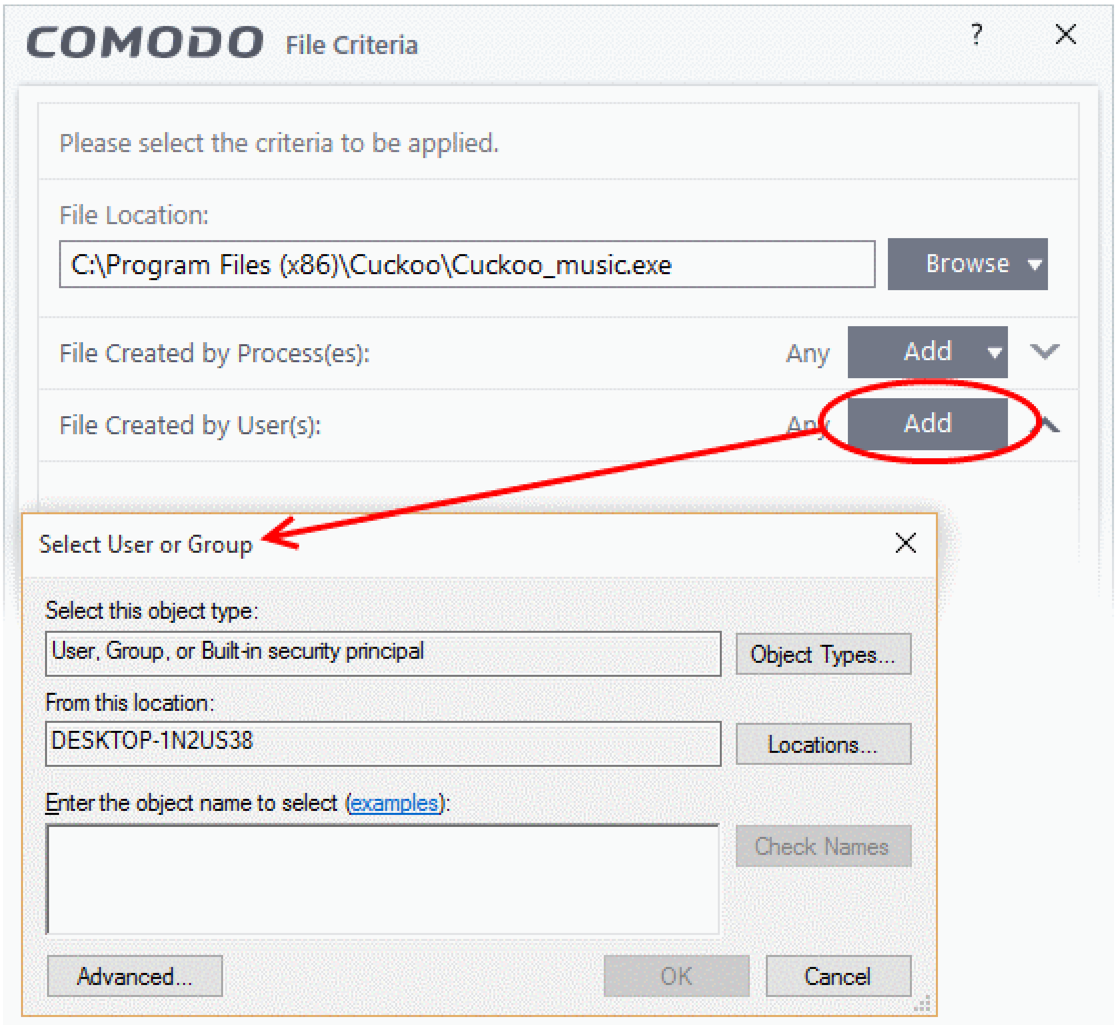


COMODO File Criteria
?
X
Please select the criteria to be applied.
File Location:
C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe
Browse
File Created by Process(es):
Any
Add
Files
Running Processes
File Groups
Folder
File Hash
Process Hash

The options available are the same as adding a Target as explained **above**. Refer to the previous section for more details on each option. You can add multiple items as targets.

To choose the user(s) to auto-contained files created by them

- Click the 'File Created by User(s)' stripe and then click the 'Add' button.



Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

File Created by User(s): Any

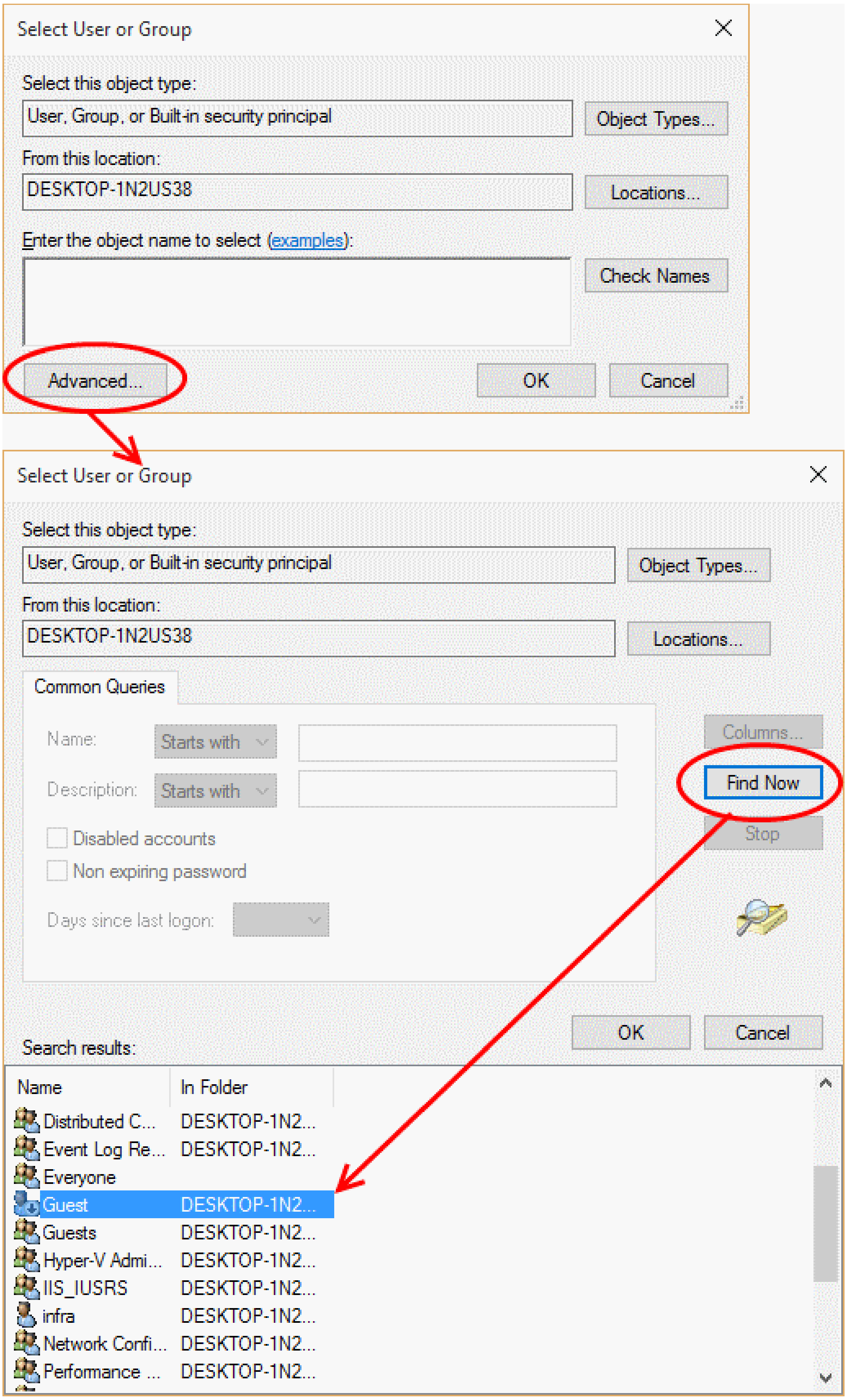
Select this object type: User, Group, or Built-in security principal

From this location: DESKTOP-1N2US38

Enter the object name to select (examples):

The 'Select User or Group' dialog will appear:

- Enter the names of the users to be added to the rule in the 'Enter the object name to select' text box. Use the format <domain name>\<user/group name> or <user/group name>@<domain name>.
- Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



Select User or Group

Select this object type: User, Group, or Built-in security principal

From this location: DESKTOP-1N2US38

Enter the object name to select (examples):

Select User or Group

Select this object type: User, Group, or Built-in security principal

From this location: DESKTOP-1N2US38

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

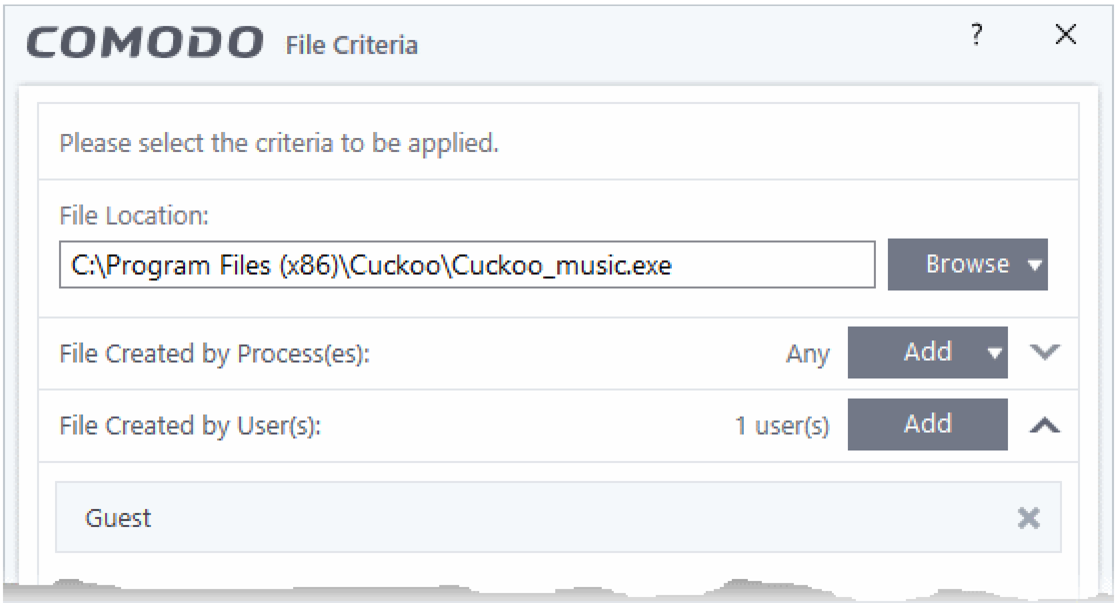
□ Non expiring password

Days since last logon:

Search results:

Name	In Folder
Distributed C...	DESKTOP-1N2...
Event Log Re...	DESKTOP-1N2...
Everyone	
Guest	DESKTOP-1N2...
Guests	DESKTOP-1N2...
Hyper-V Admi...	DESKTOP-1N2...
IIS_IUSRS	DESKTOP-1N2...
infra	DESKTOP-1N2...
Network Confi...	DESKTOP-1N2...
Performance ...	DESKTOP-1N2...

The user will be added to the list.



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

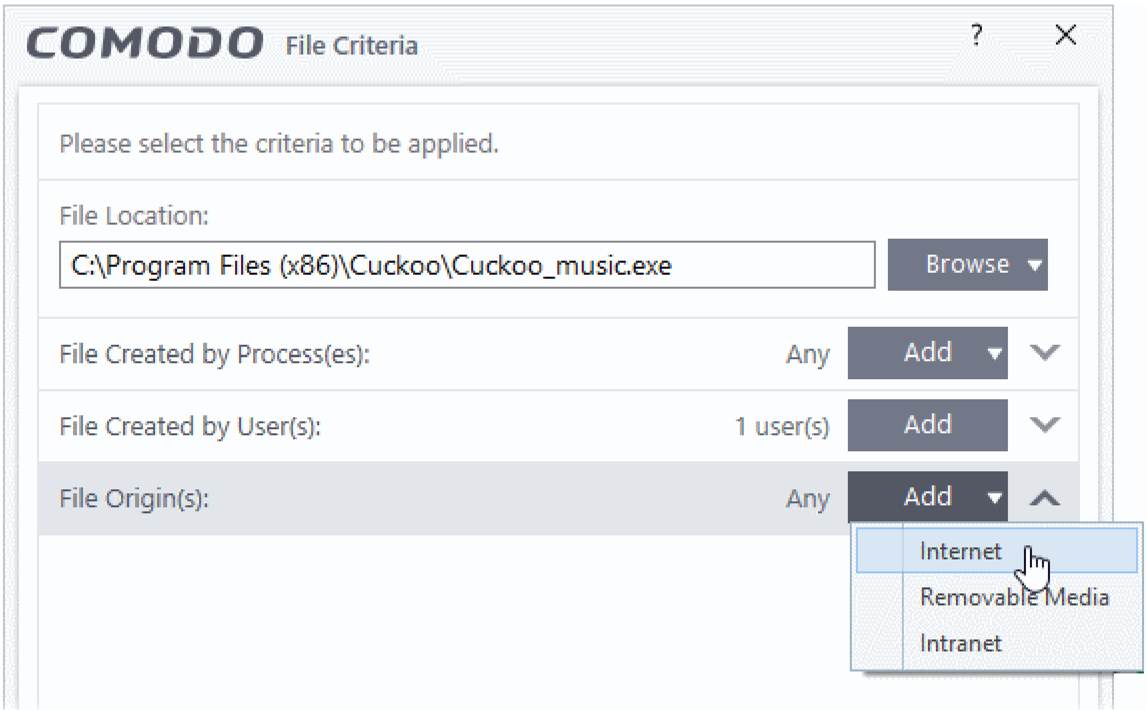
File Created by User(s): 1 user(s)

Guest

- Repeat the process for adding more users.
- To remove the user added by mistake or no longer needed in the list, click the 'X' icon at the right end of the user name.

To select the sources(s) from which the file was downloaded/copied to the computer

- Click the 'Add' button in the 'File Origin(s)' stripe.
- Choose the source from the options:



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

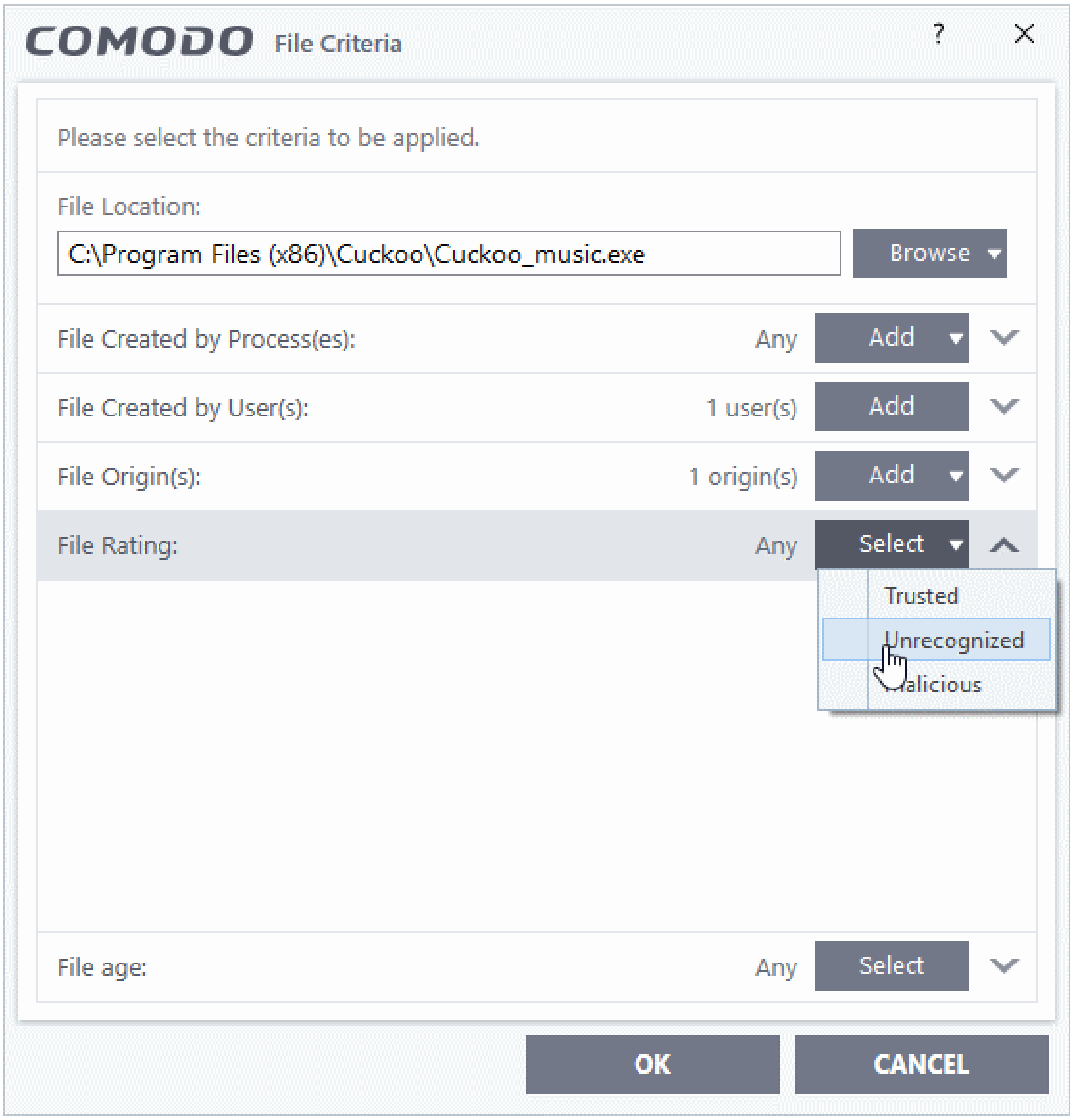
File Created by User(s): 1 user(s)

File Origin(s): Any

- Choose the source from the options:
  - Internet - The rule will only apply to files that were downloaded from the internet.
  - Removable Media - The rule will apply only to items copied to the computer from removable storage devices like a USB drive, CD/DVD or portable hard disk drive
  - Intranet - The rule will only apply to files that were downloaded from the local intranet.
- Repeat the process to add more sources

To select the file rating as filter criteria

- Click the 'Select' button in the 'File Rating' stripe



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\Cuckoo_music.exe

File Created by Process(es): Any

File Created by User(s): 1 user(s)

File Origin(s): 1 origin(s)

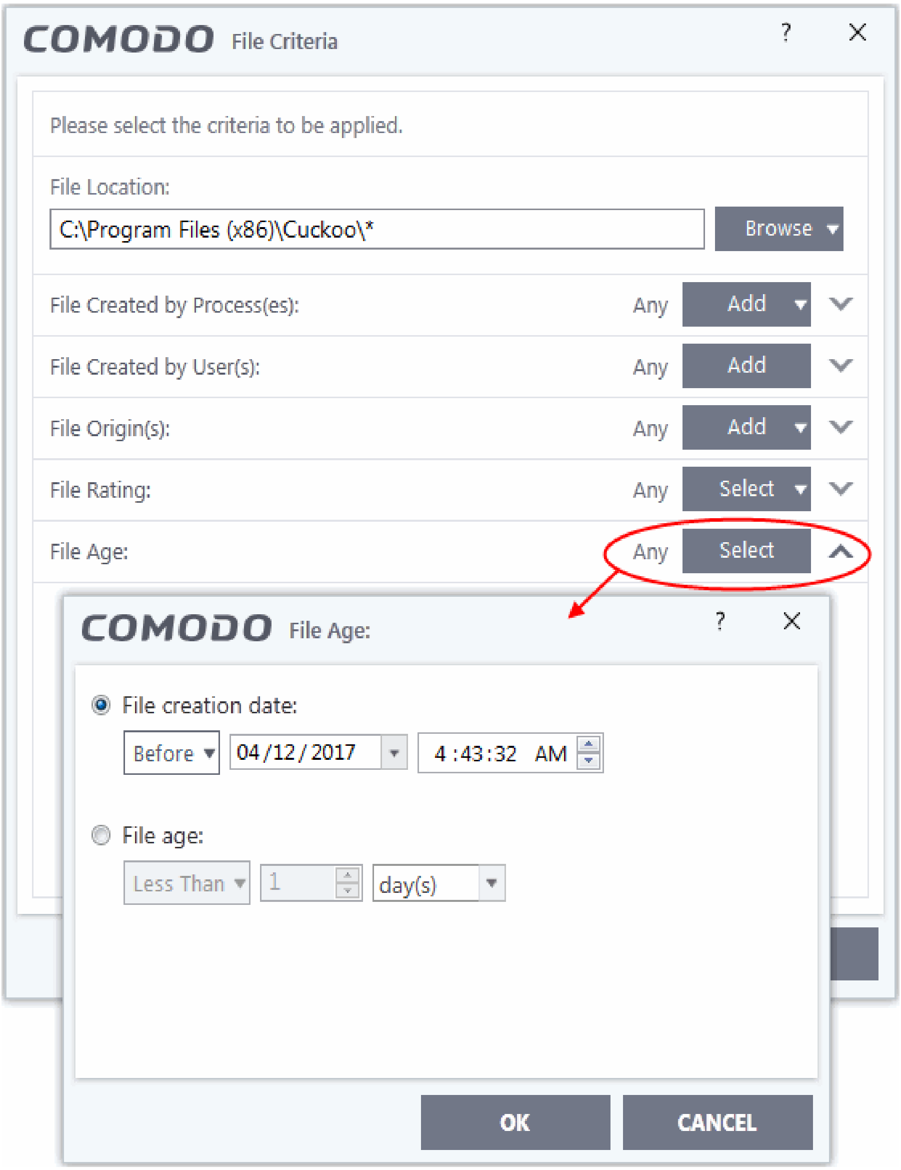
File Rating: Any

File age: Any

- Choose the source from the options:
  - **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by CIS. See **File Rating Settings** for more information.
  - **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. See **File List** for more information.
  - **Malware** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. See **Unknown Files - The Scanning Process** for more information.

To set the file age as filter criteria

- Click the 'Select' button in the 'File age' stripe.



COMODO File Criteria

Please select the criteria to be applied.

File Location: C:\Program Files (x86)\Cuckoo\*

File Created by Process(es): Any

File Created by User(s): Any

File Origin(s): Any

File Rating: Any

File Age: Any

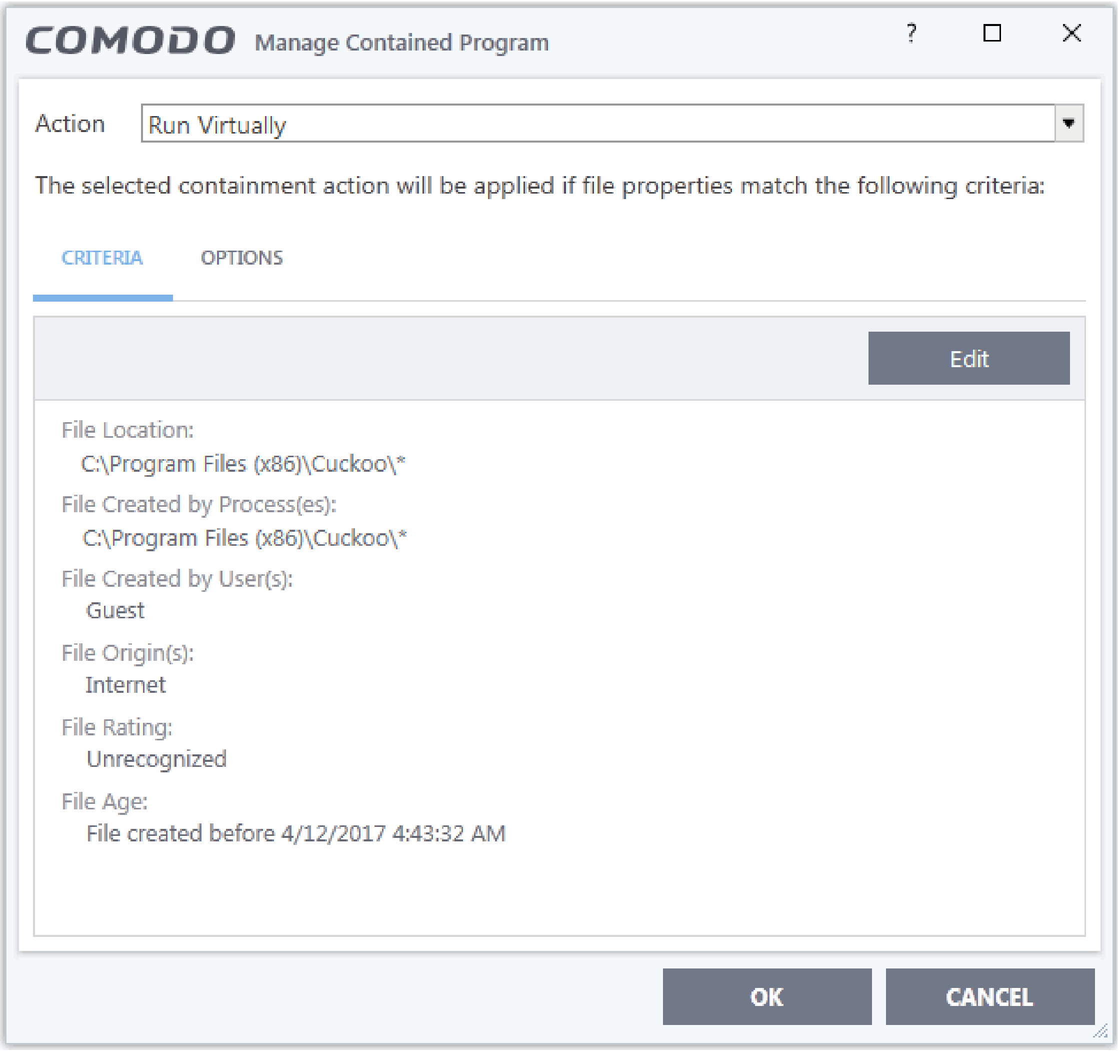
COMODO File Age:

● File creation date: Before 04/12/2017 4:43:32 AM

○ File age: Less Than 1 day(s)

The 'File Age' dialog will appear. You can set the file age in two ways:

- **File creation date** - To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- **File age** - To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - **Less Than** - CIS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)
  - **More Than** - CIS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)
- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.



Action: Run Virtually

The selected containment action will be applied if file properties match the following criteria:

File Location:
C:\Program Files (x86)\Cuckoo\*

File Created by Process(es):
C:\Program Files (x86)\Cuckoo\*

File Created by User(s):
Guest

File Origin(s):
Internet

File Rating:
Unrecognized

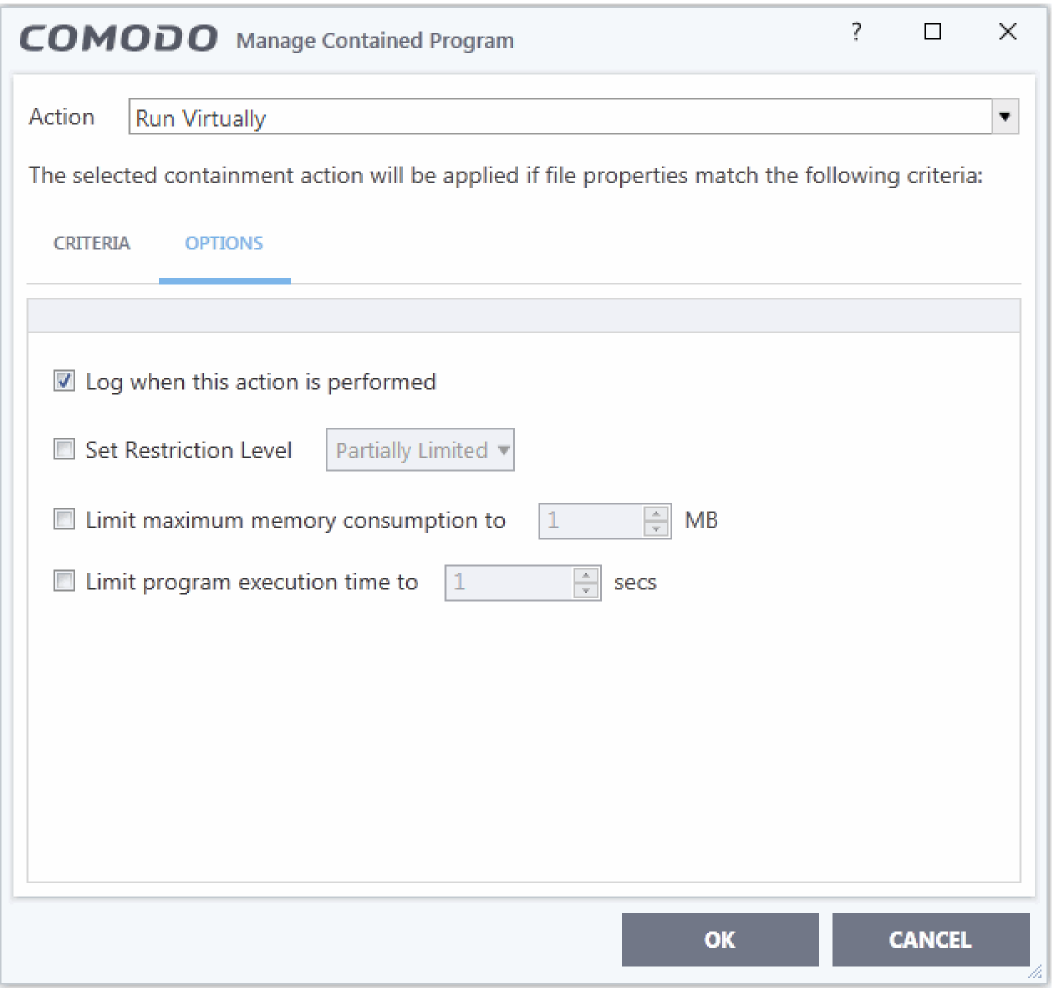
File Age:
File created before 4/12/2017 4:43:32 AM

Step 3 - Select the Options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

To select the options

- Click the 'Options' tab.



COMODO Manage Contained Program

Action: Run Virtually

The selected containment action will be applied if file properties match the following criteria:

☑ Log when this action is performed

□ Set Restriction Level: Partially Limited

□ Limit maximum memory consumption to 1 MB

□ Limit program execution time to 1 secs

The options will be displayed, depending on the 'Action' chosen in **Step 1**.

The options available for '**Ignore**' action are:

- **Log when this action is performed -** Whenever this rule is applied for the action, it will be added to CIS Containment logs.
- **Don't apply the selected action to child processes -** Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CIS treats all the child processes as individual processes and forces them to run as per the file rating and the Containment rules.
  - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
  - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Containment rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the 'Ignore' action only.

The options available for '**Run Restricted**' and '**Run Virtually**' actions are:

- **Log when this action is performed -** Whenever this rule is applied for the action, it will be logged.
- **Set Restriction Level -** When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
  - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(***Default***)

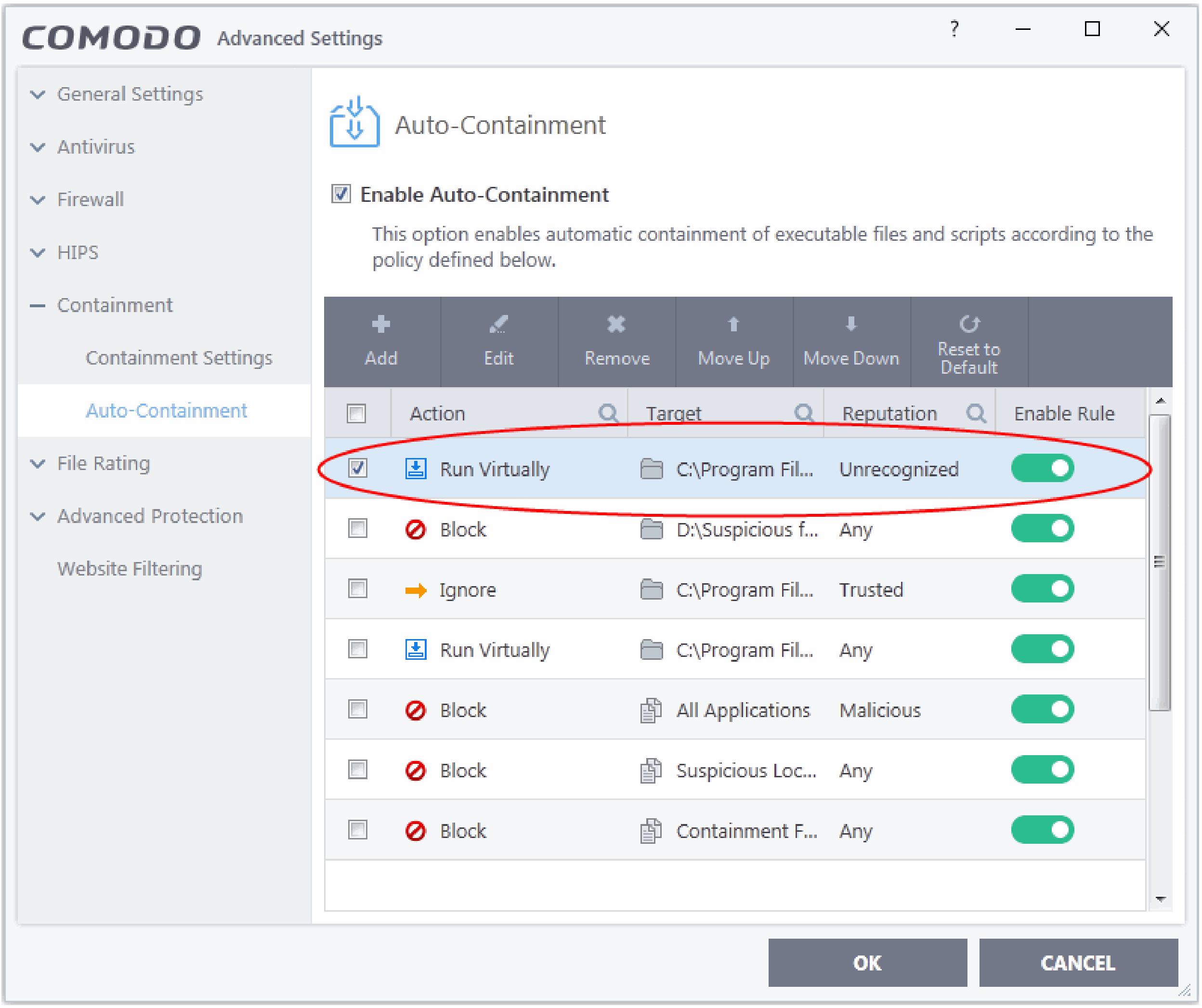
- **Limited** - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
- **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Untrusted -** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.

- **Limit maximum memory consumption to -** Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to -** Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For '**Block**' action, the following options are available:

- **Log when this action is performed -** Whenever this rule is applied for the action, it will be logged.
- **Quarantine program** - If checked, the programs will be automatically quarantined. See **Manage Quarantined Items** for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



Auto-Containment

☑ Enable Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
☑	Run Virtually	C:\Program Fil...	Unrecognized	●
□	Block	D:\Suspicious f...	Any	●
□	Ignore	C:\Program Fil...	Trusted	●
□	Run Virtually	C:\Program Fil...	Any	●
□	Block	All Applications	Malicious	●
□	Block	Suspicious Loc...	Any	●
□	Block	Containment F...	Any	●

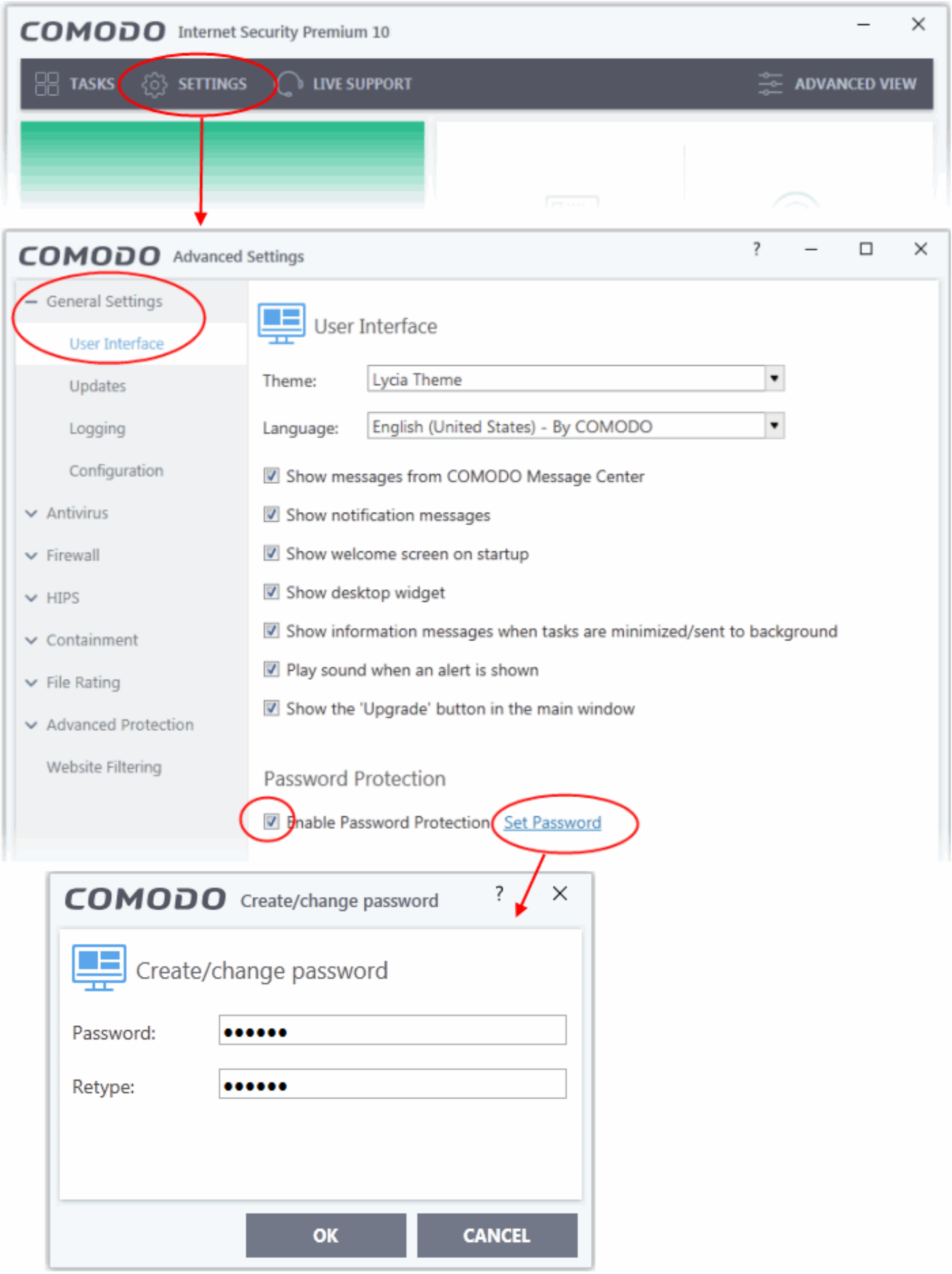
Important Note: Please make sure the auto-containment rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail. You can restore the rules to default rules at any time by clicking the 'Reset to Default' button at the top.

Password Protect Your CIS Settings

This page explains how to password protect access to the CIS interface. Password protection means other users will not be able to open the CIS interface to modify or over-ride the security settings you have implemented.

To enable password protection

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'User Interface' under 'General Settings' on the left.
3. Check 'Enable Password Protection' box under 'Password Protection' and click 'Set Password' link. The Create/change password' dialog will appear:



User Interface

Theme: Lycia Theme

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center
☑ Show notification messages
☑ Show welcome screen on startup
☑ Show desktop widget
☑ Show information messages when tasks are minimized/sent to background
☑ Play sound when an alert is shown
☑ Show the 'Upgrade' button in the main window

Password Protection

☑ Enable Password Protection Set Password

Create/change password

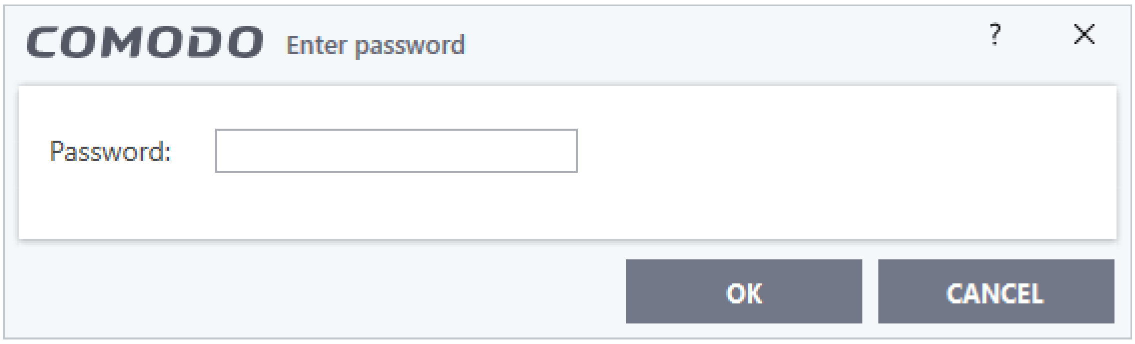
Password: ••••••

Retype: ••••••

4. Enter and confirm your password then click 'OK'. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed

by others.

The configuration is now password protected. From the next attempt to change any configuration changes to CIS, you will be prompted to enter the password to proceed.



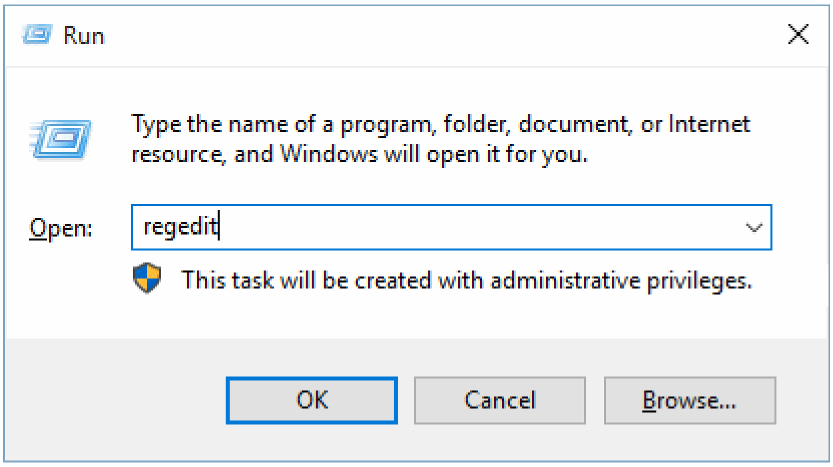
Reset Forgotten Password (Advanced)

This page explains how to remove password protection and reset your password in case you forgot it.

Note: It is not possible to 'retrieve' a forgotten password - you can only reset it. To do this involves modification of the Windows registry and is only recommended for experienced users.

To disable password protection in CIS

1. Open the 'Run' Window by pressing 'Windows' key + 'R' from the keyboard
2. Type 'regedit' in the text box and click 'OK'



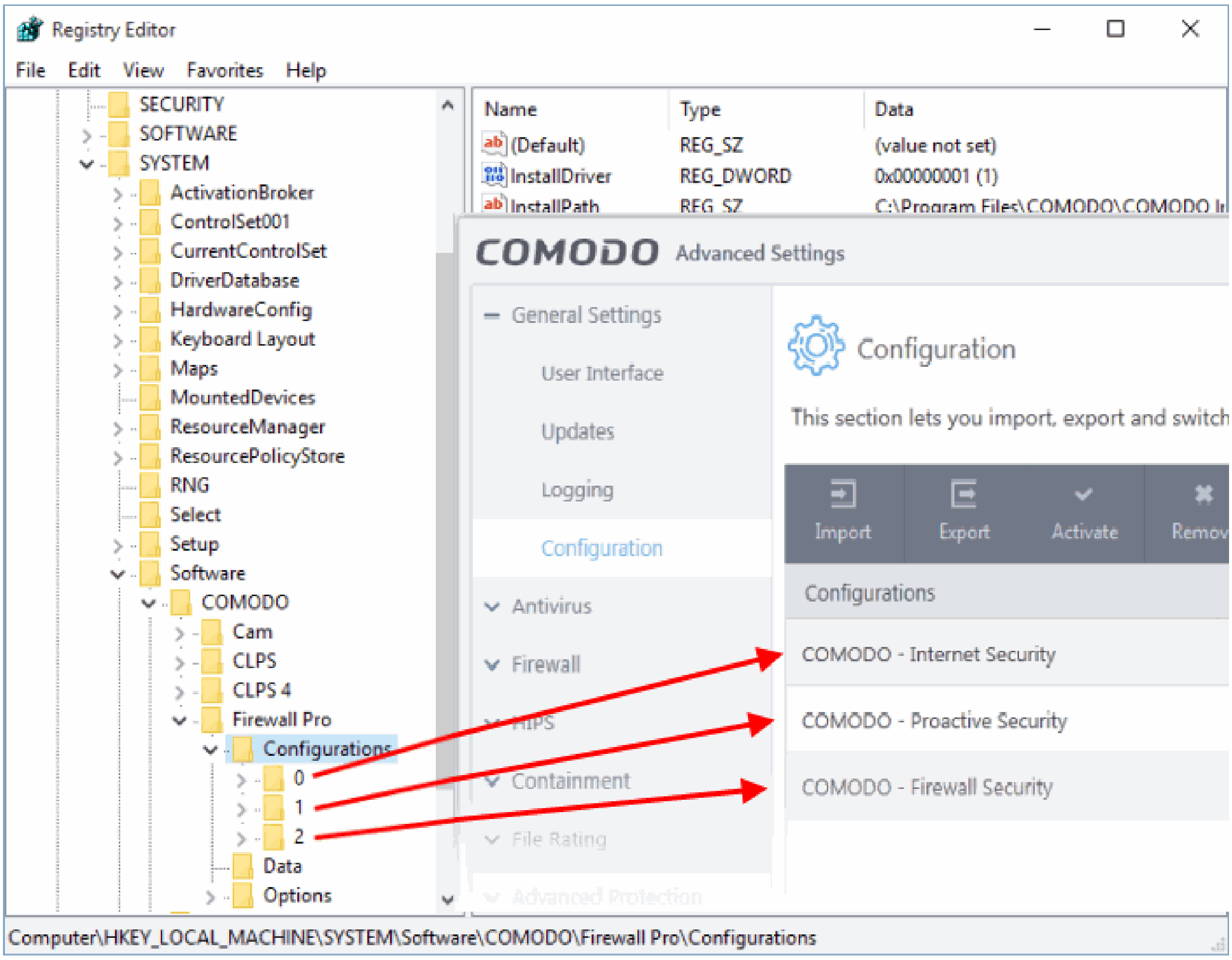
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

This task will be created with administrative privileges.

3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\

Under the 'Configurations' folder you will see sub-folders named 0,1,2,... depending on the number of preset configurations in CIS. These folders contain registry keys for the settings of the preset configurations in the order of the configurations displayed in **Advanced Settings > General Settings > Configuration** interface. For example, the folder 0 contains the keys for COMODO - Internet Security, the folder 1 contains the keys for COMODO - Proactive Security and so on.



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallDriver	REG_DWORD	0x00000001 (1)
InstallPath	REG_SZ	C:\Program Files\COMODO\COMODO In

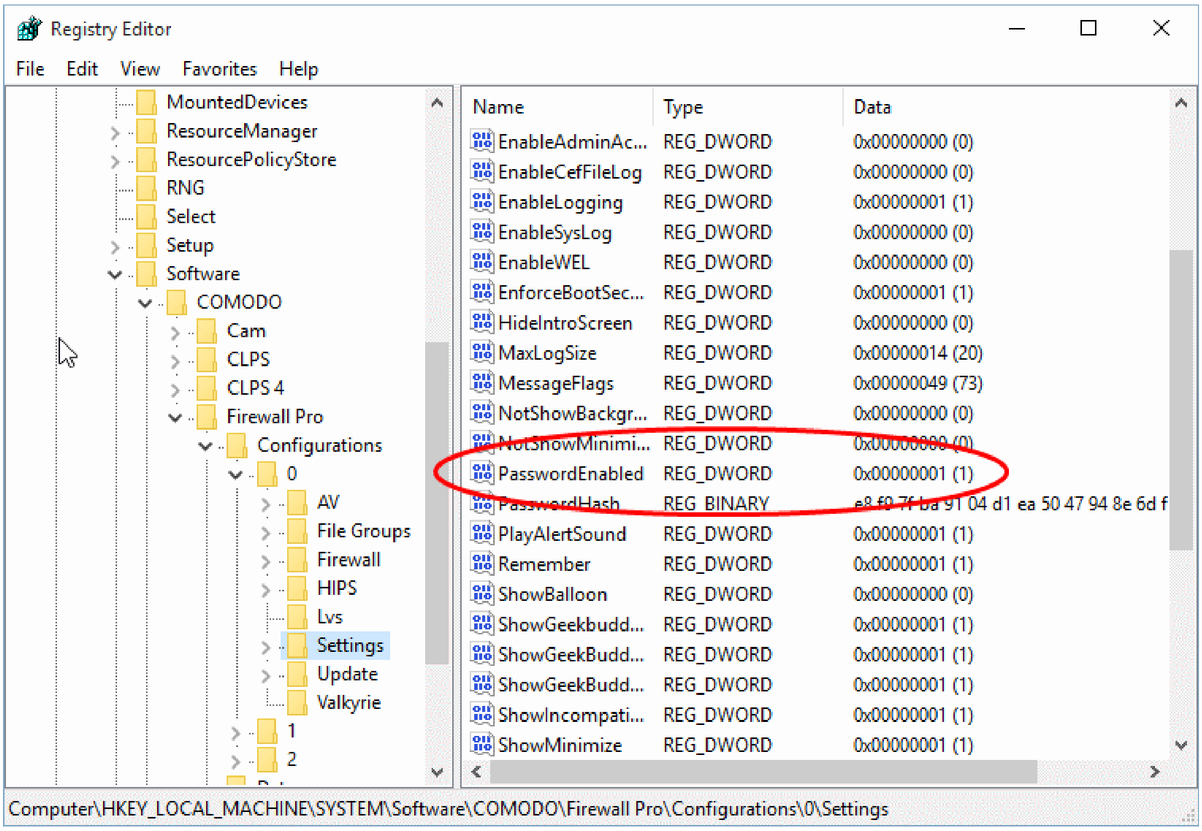
Configuration

This section lets you import, export and switch

Configurations
COMODO - Internet Security
COMODO - Proactive Security
COMODO - Firewall Security

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Software\COMODO\Firewall Pro\Configurations

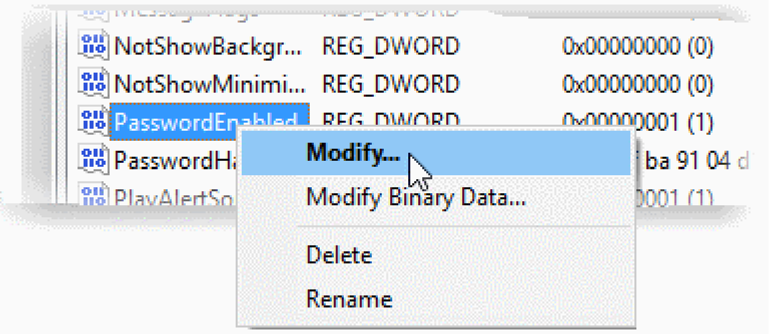
4. Select the folder corresponding to the configuration for which you wish to reset the password and navigate to Settings, for example, navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\0\Settings to reset password in COMODO - Internet Security configuration.



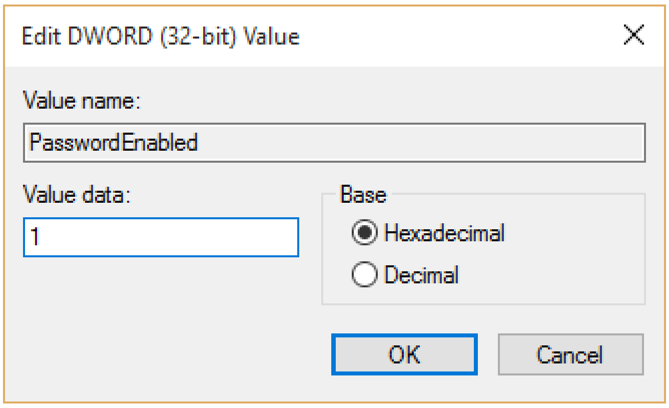
Name	Type	Data
EnableAdminAc...	REG_DWORD	0x00000000 (0)
EnableCefFileLog	REG_DWORD	0x00000000 (0)
EnableLogging	REG_DWORD	0x00000001 (1)
EnableSysLog	REG_DWORD	0x00000000 (0)
EnableWEL	REG_DWORD	0x00000000 (0)
EnforceBootSec...	REG_DWORD	0x00000001 (1)
HideIntroScreen	REG_DWORD	0x00000000 (0)
MaxLogSize	REG_DWORD	0x00000014 (20)
MessageFlags	REG_DWORD	0x00000049 (73)
NotShowBackgr...	REG_DWORD	0x00000000 (0)
NotShowMinimi...	REG_DWORD	0x00000000 (0)
PasswordEnabled	REG_DWORD	0x00000001 (1)
PasswordHash	REG_BINARY	e8 f0 7f ba 91 04 d1 ea 50 47 94 8e 6d f
PlayAlertSound	REG_DWORD	0x00000001 (1)
Remember	REG_DWORD	0x00000001 (1)
ShowBalloon	REG_DWORD	0x00000000 (0)
ShowGeekbudd...	REG_DWORD	0x00000001 (1)
ShowGeekBudd...	REG_DWORD	0x00000001 (1)
ShowGeekBudd...	REG_DWORD	0x00000001 (1)
ShowIncompati...	REG_DWORD	0x00000001 (1)
ShowMinimize	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Software\COMODO\Firewall Pro\Configurations\0\Settings

5. Right-click 'PasswordEnabled' key and select 'Modify'


NotShowBackgr... REG_DWORD 0x00000000 (0)
NotShowMinimi... REG_DWORD 0x00000000 (0)
PasswordEnabled REG_DWORD 0x00000001 (1)
PasswordH
PlayAlertSo
Modify...
Modify Binary Data...
Delete
Rename

6. In the 'Edit DWORD Value dialog box, change the 'Value data' from 1 to 0



Value name: PasswordEnabled

Value data: 1

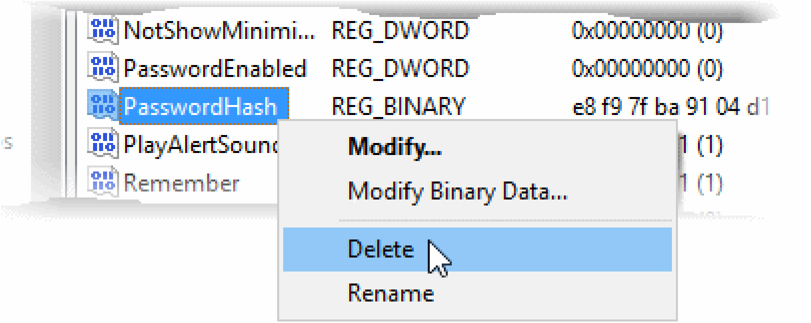
Base

● Hexadecimal

○ Decimal

7. Click 'OK'

8. Right-click 'PasswordHash' and select 'Delete'.



NotShowMinimi...	REG_DWORD	0x00000000 (0)
PasswordEnabled	REG_DWORD	0x00000000 (0)
PasswordHash	REG_BINARY	e8 f9 7f ba 91 04 d1
PlayAlertSounc		1 (1)
Remember		1 (1)

9. Restart the system for the changes to take effect

Now you should be able to access all settings, uninstall CIS and set a new password.

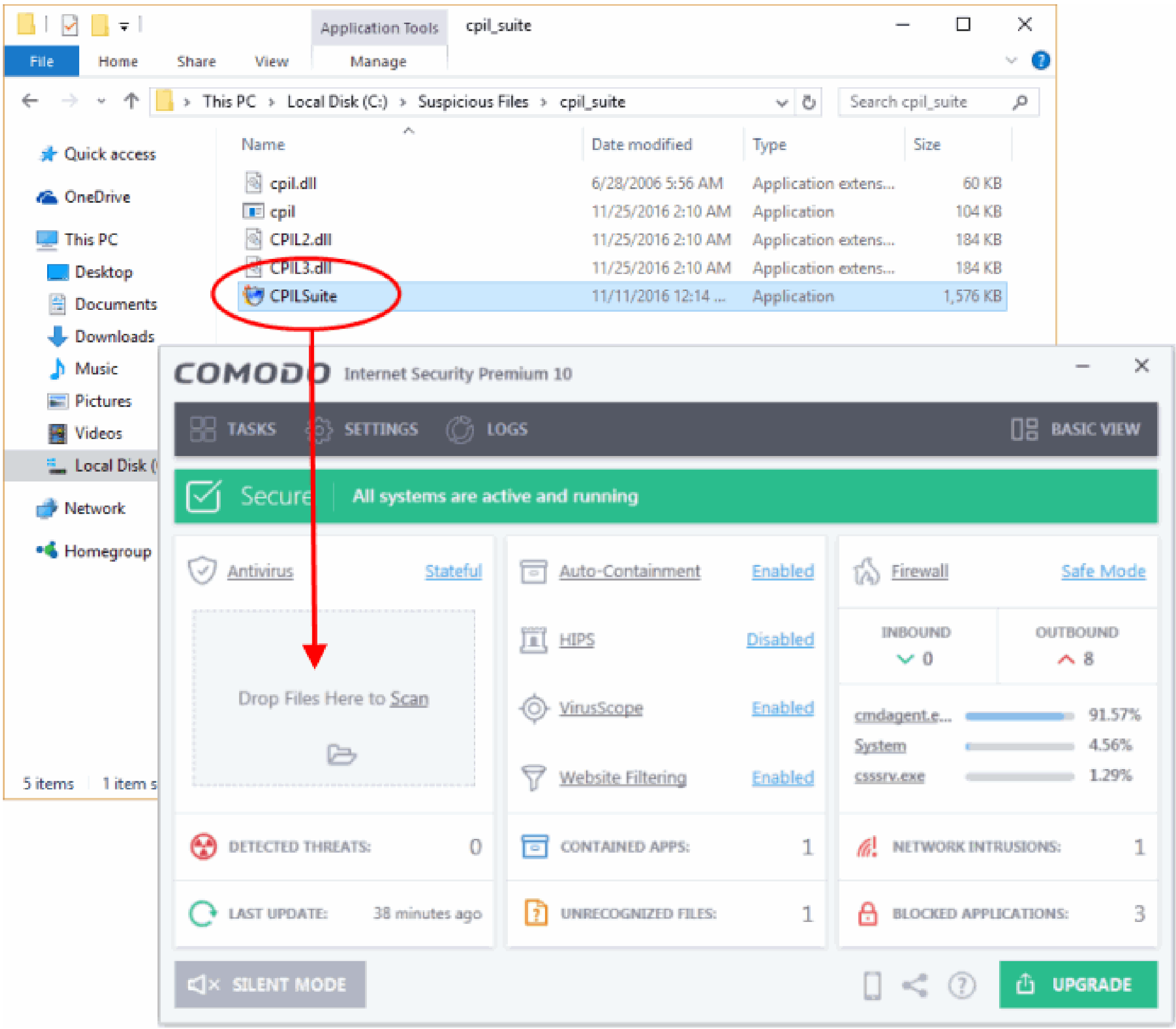
Note: If CIS doesn't allow regedit to change those registry items, try to boot in safe mode and repeat the above steps.

Run an Instant Antivirus Scan on Selected Items

You can run an instant virus scan on files, folders and entire drives. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives and digital cameras.

To instantly scan an item

- Click 'Advanced View' on the CIS home screen
- Drag and drop the item inside the box marked 'Drop Files to Scan' or click the 'Scan' link inside the box and navigate to the item



Name	Date modified	Type	Size
cpil.dll	6/28/2006 5:56 AM	Application extens...	60 KB
cpil	11/25/2016 2:10 AM	Application	104 KB
CPIL2.dll	11/25/2016 2:10 AM	Application extens...	184 KB
CPIL3.dll	11/25/2016 2:10 AM	Application extens...	184 KB
CPILSuite	11/11/2016 12:14 ...	Application	1,576 KB

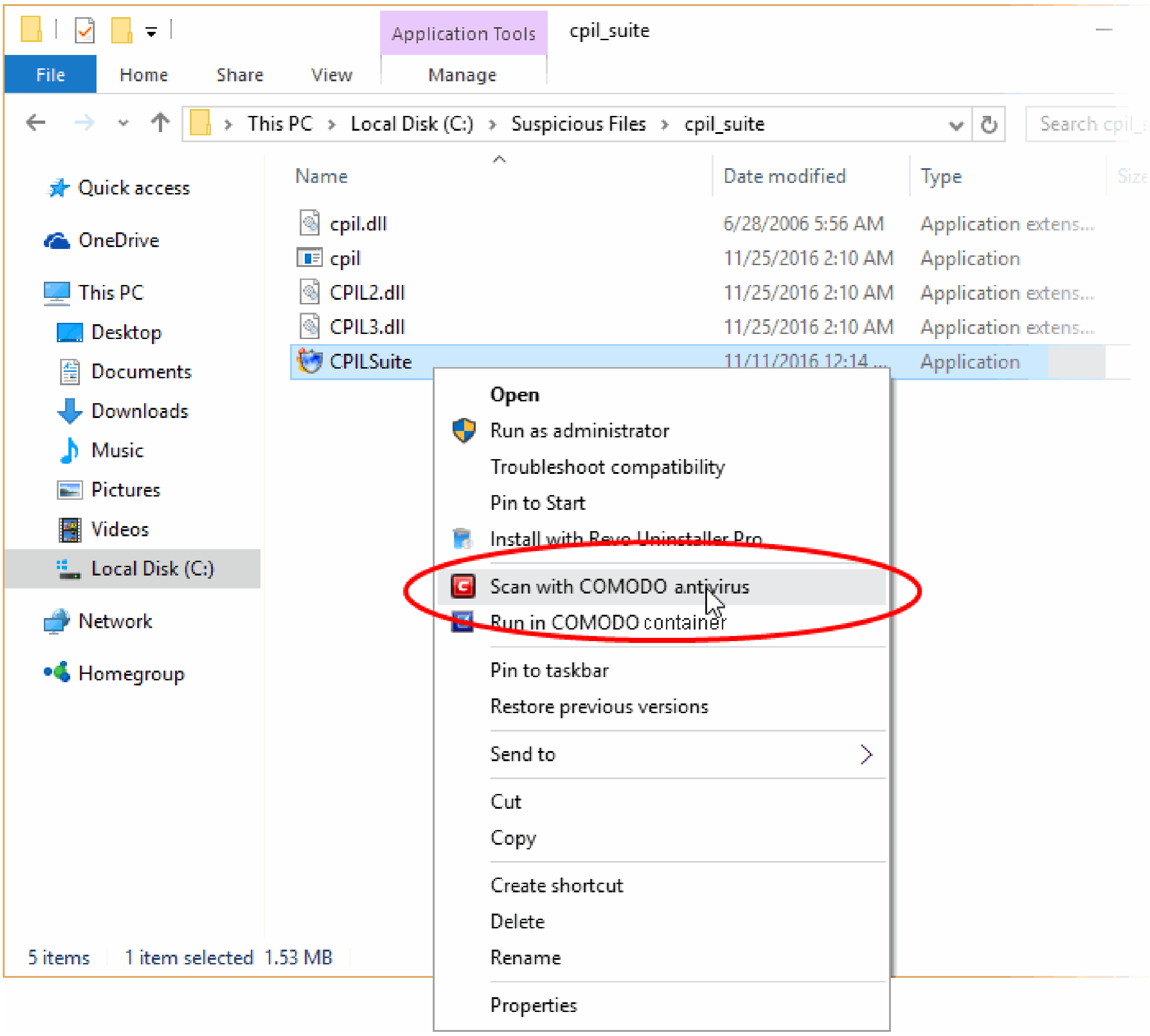
All systems are active and running

cmdagent.e...	91.57%
System	4.56%
csssrv.exe	1.29%

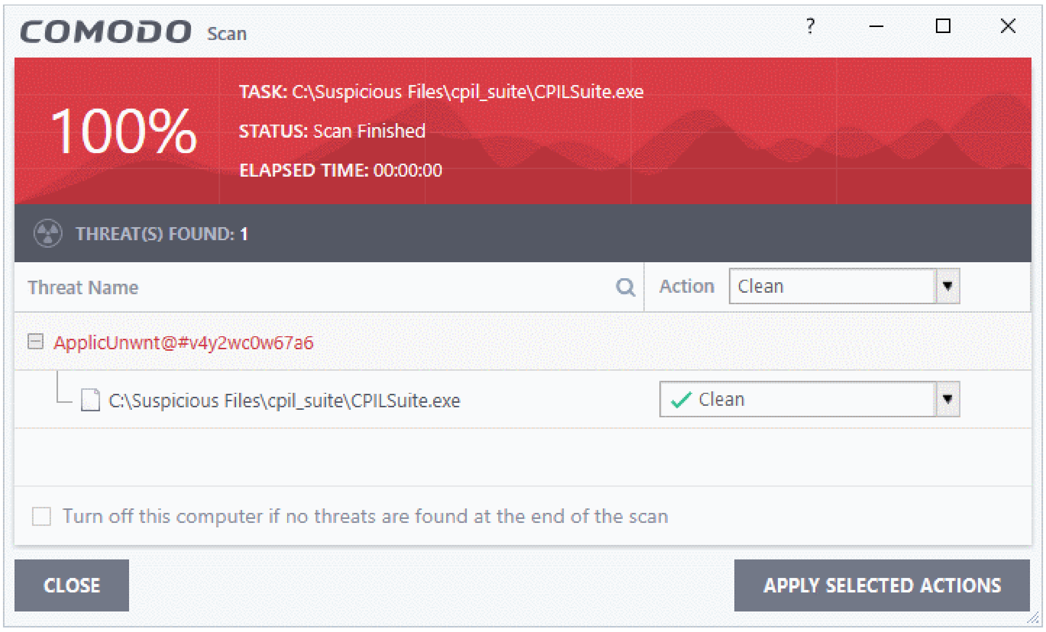
DETECTED THREATS:	0
LAST UPDATE:	38 minutes ago
CONTAINED APPS:	1
UNRECOGNIZED FILES:	1
NETWORK INTRUSIONS:	1
BLOCKED APPLICATIONS:	3

OR

- Right click on the item and select Scan with 'Comodo antivirus' from the context sensitive menu


Application Tools
cpil_suite
File
Home
Share
View
Manage
This PC > Local Disk (C:) > Suspicious Files > cpil_suite
Search cpil_s
Quick access
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Homegroup
Name
Date modified
Type
Size
cpil.dll 6/28/2006 5:56 AM Application extens...
cpil 11/25/2016 2:10 AM Application
CPIL2.dll 11/25/2016 2:10 AM Application extens...
CPIL3.dll 11/25/2016 2:10 AM Application extens...
CPILSuite 11/11/2016 12:14 ... Application
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
Install with Revo Uninstaller Pro
Scan with COMODO antivirus
Run in COMODO container
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
5 items 1 item selected 1.53 MB

The item will be scanned immediately. Any threats found will be shown at the end of the scan:



100%

TASK: C:\Suspicious Files\cpil_suite\CPILSuite.exe

STATUS: Scan Finished

ELAPSED TIME: 00:00:00

THREAT(S) FOUND: 1

Threat Name	Action: Clean
ApplicUnwnt@#v4y2wc0w67a6	
C:\Suspicious Files\cpil_suite\CPILSuite.exe	✓ Clean

□ Turn off this computer if no threats are found at the end of the scan

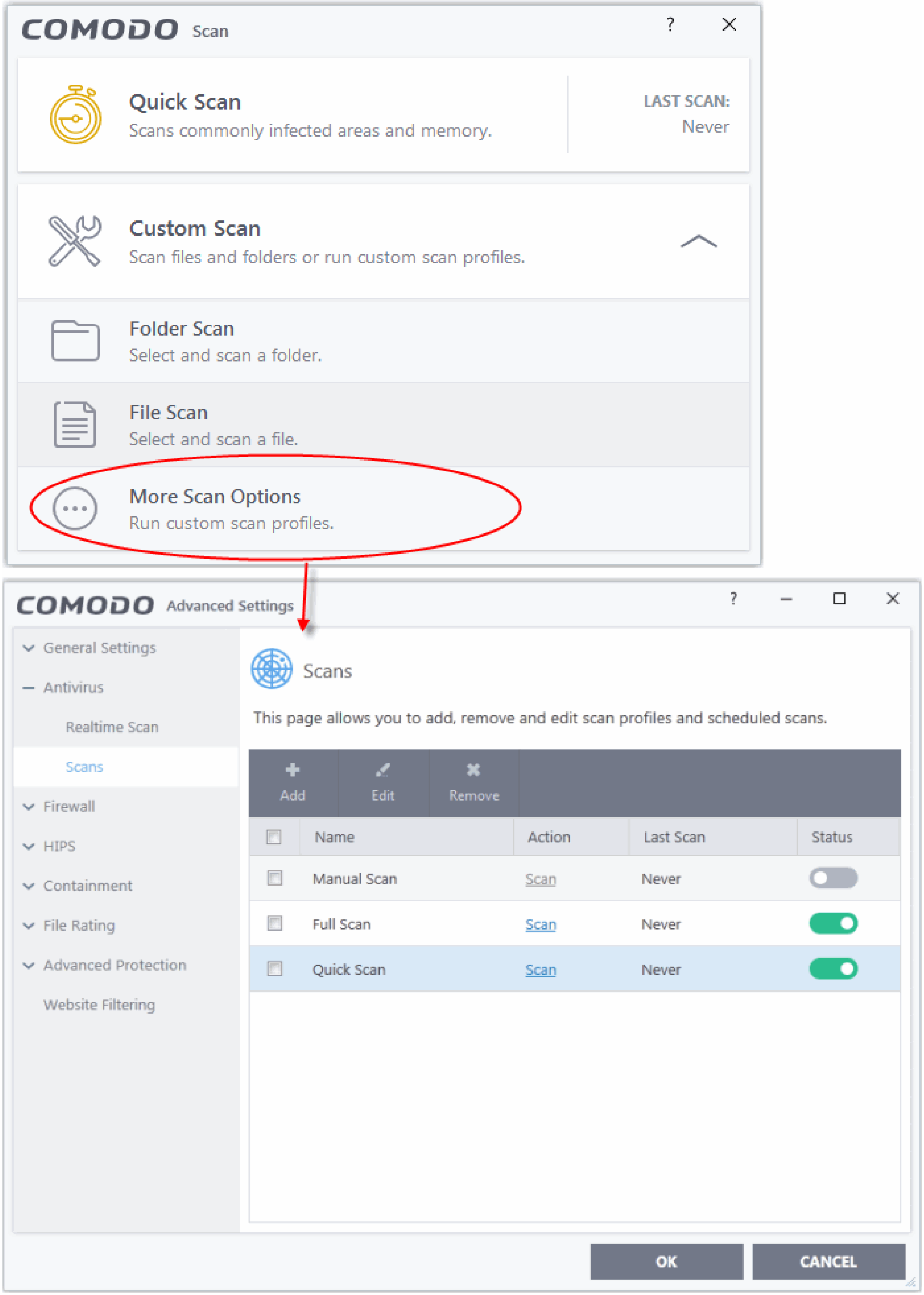
Click here for more details to take action on the infected item(s).

Create an Antivirus Scan Schedule

Comodo Internet Security allows you to schedule antivirus scans on your entire system or specific areas. You can create a scan profile defining exactly which files and folders are scanned, when they are scanned, and how they are scanned.

To create a scan schedule

- Click 'Tasks' at the top left of the CIS home screen to open the 'Tasks' interface
- Click 'General Tasks' from the 'Tasks' interface:
- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane



COMODO Scan

Quick Scan
Scans commonly infected areas and memory.
LAST SCAN: Never

Custom Scan
Scan files and folders or run custom scan profiles.

Folder Scan
Select and scan a folder.

File Scan
Select and scan a file.

More Scan Options
Run custom scan profiles.

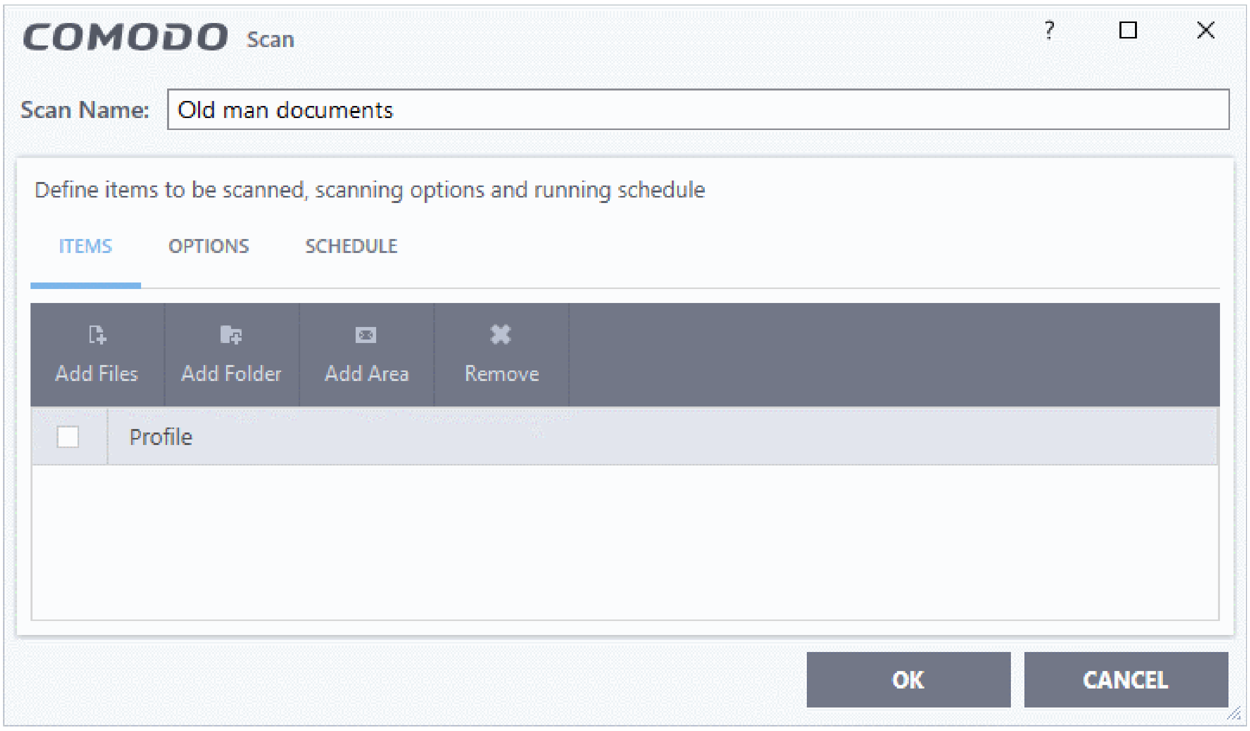
COMODO Advanced Settings

Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	Off
□	Full Scan	Scan	Never	On
□	Quick Scan	Scan	Never	On

- Click 'Add' at the top to create a new custom scan profile



Scan Name: Old man documents

- Type a name for the profile in the 'Scan Name' text box.

The next steps are to:

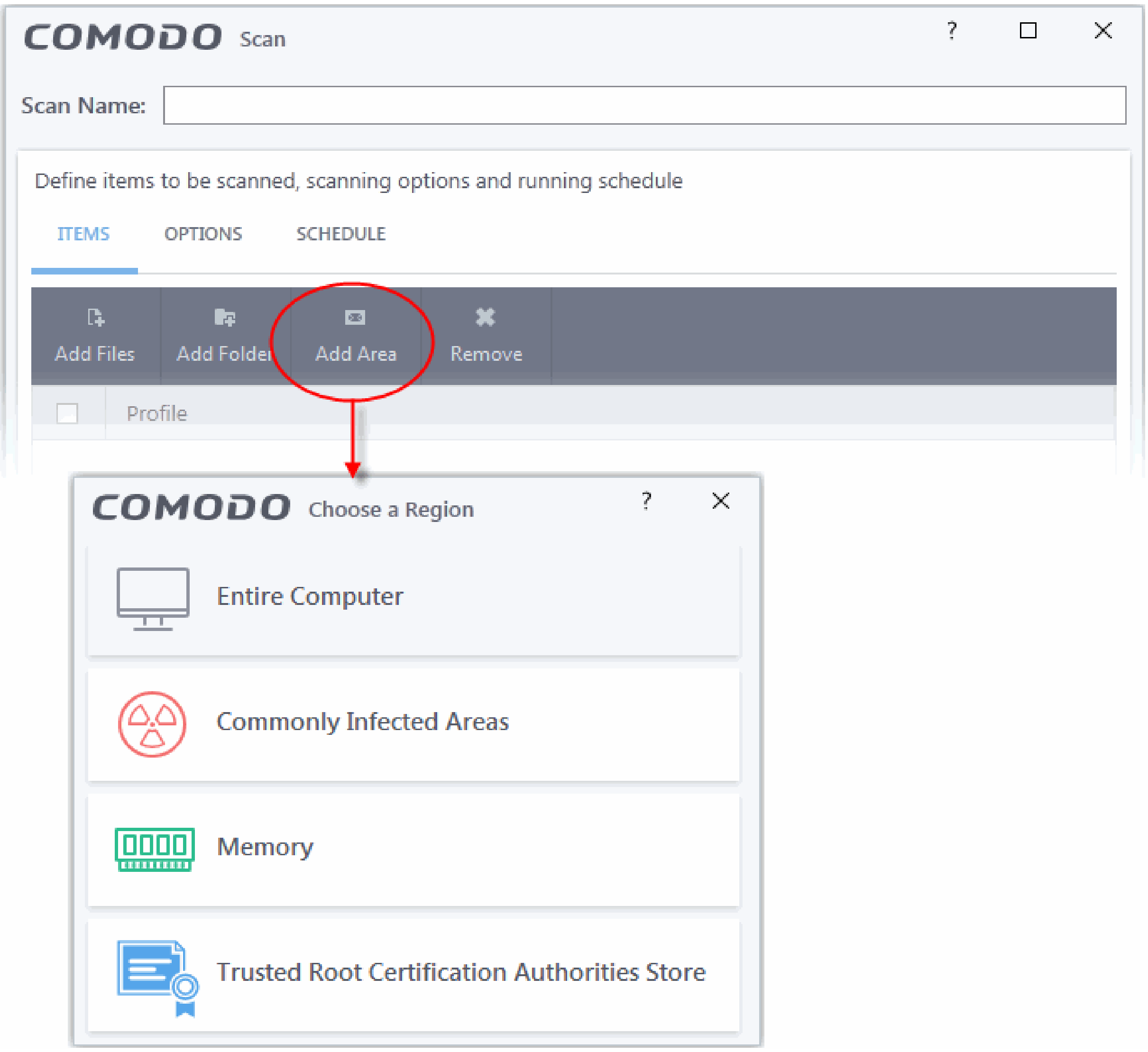
- Select the items to be scanned
- Configure the scanning options for the profile (Optional)
- Configure a schedule for the scan to run periodically (Optional)

To select the items to be scanned

- Click 'Items' at the top of the 'Scan' interface.

The buttons at the top allow you to add the items to be scanned in three ways:

- Add File - Allows you to add individual files to the profile. Click the 'Add Files' button and navigate to the file to be scanned in the Open dialog and click 'Open'.
- Add Folder - Allows you to select entire folders to be included in the profile. Click the Add Folder button and choose the folder from the 'Browse for Folder' dialog.
- Add Region - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas', 'System Memory' and 'Trusted Root Certificate Store').

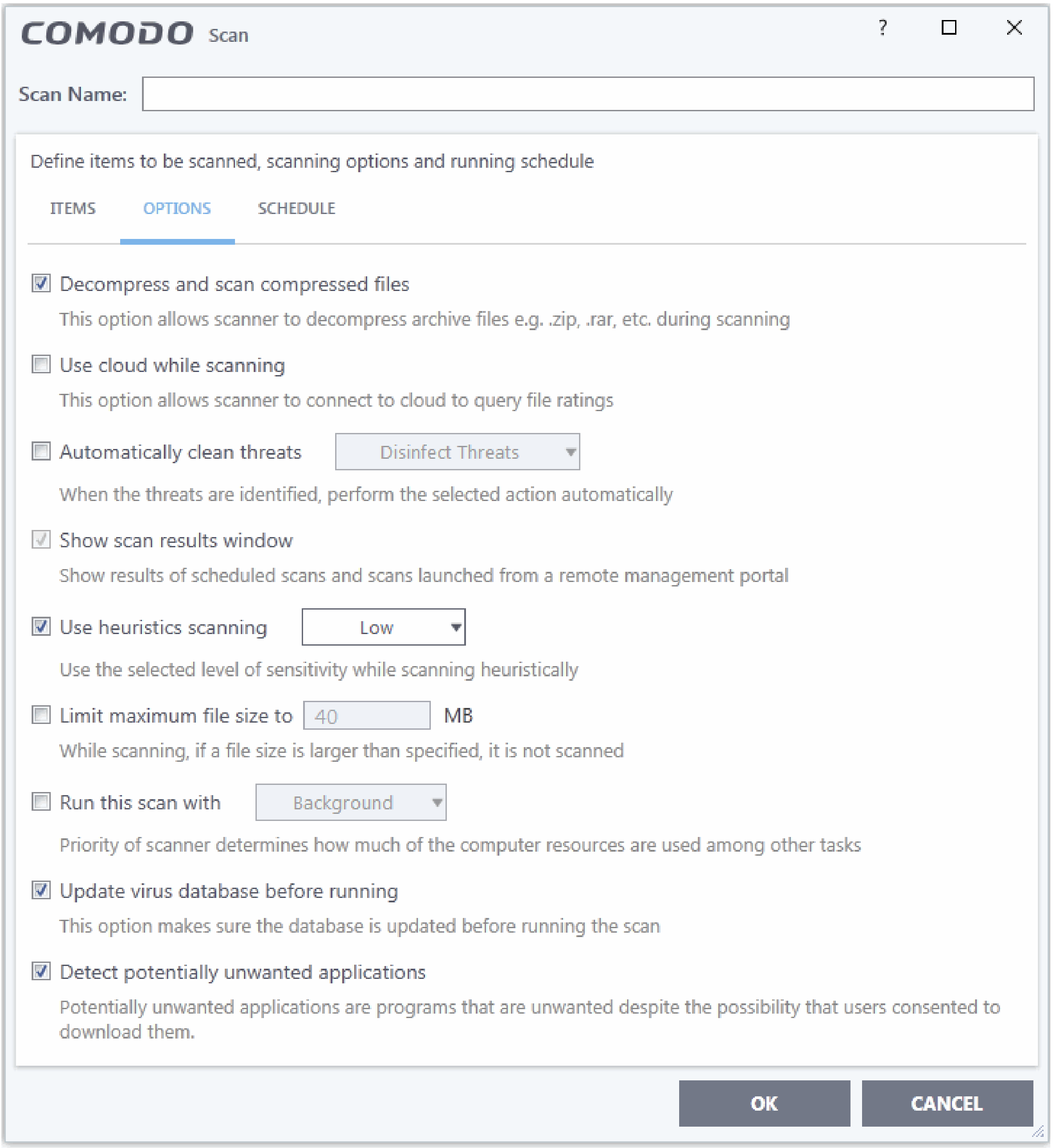


- Repeat the process to add more items to the profile.
- To remove an item, select it and click 'Remove'.

To configure Scanning Options

- Click 'Options' at the top of the 'Scan' interface

The options to customize the scan will be displayed.



COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

☑ Decompress and scan compressed files

This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

☐ Use cloud while scanning

This option allows scanner to connect to cloud to query file ratings

☐ Automatically clean threats: Disinfect Threats

When the threats are identified, perform the selected action automatically

☑ Show scan results window

Show results of scheduled scans and scans launched from a remote management portal

☑ Use heuristics scanning: Low

Use the selected level of sensitivity while scanning heuristically

☐ Limit maximum file size to 40 MB

While scanning, if a file size is larger than specified, it is not scanned

☐ Run this scan with: Background

Priority of scanner determines how much of the computer resources are used among other tasks

☑ Update virus database before running

This option makes sure the database is updated before running the scan

☑ Detect potentially unwanted applications

Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download them.

- **Decompress and scan compressed files -** If enabled, the antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
- **Use cloud while scanning -** Selecting this option enables the antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local anitvirus database is out-dated. ***(Default = Disabled)***.
- **Automatically clean threats -** If selected, you can choose the action to be automatically taken against the threats and infected files detected by the scan. (***Default = Disabled***).

The available options are:

- **Quarantine Threats -** The infected items will be moved to Quarantine. You can view the items in the quarantine and choose to remove them or restore them (in case of false positives).

See **Manage Quarantined Items** for more details.

- **Disinfect Threats -** If a disinfection routine is available for the detected threat, the antivirus will remove the threat from the infected file and retain the application safe. Else, the item will be moved to

'Quarantine'.

- **Show scan results window -** If selected, displays the number of objects scanned and the number of threats found by local and remotely run scans.
- **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Enabled).***

Background Info:

- Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans.
- 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses.
- If it is found to do so then the application deletes the file or recommends it for quarantine.
- Heuristics is about detecting 'virus-like' traits or attributes rather than looking for a signature that exactly matches a signature on the virus blacklist.

This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

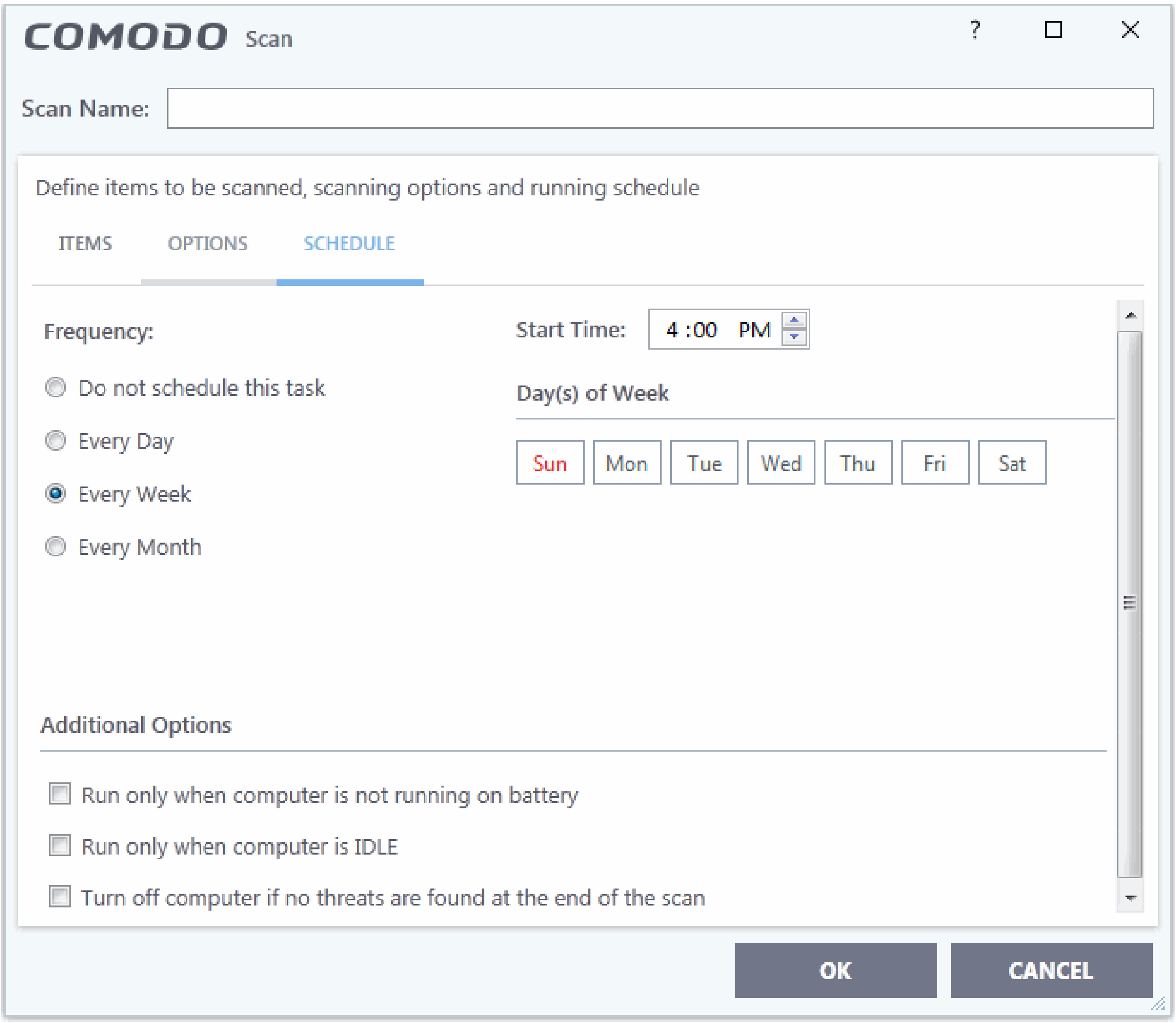
On selecting this option, you can choose the level for heuristic scanning from the drop-down.

  - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. ***(Default)***
  - **Medium -** Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High -** Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

- **Limit maximum file size to -** Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run this scan with -** Enables you to set the priority of the scan profile. ***(Default = Disabled)***. You can select the priority from the drop-down. The available options are:
  - High
  - Normal
  - Low
  - Background.
- **Update virus database before running** Instructs Comodo Internet Security to check for and download the latest database updates before starting the scan (***Default = Enabled***).
- **Detect potentially unwanted applications** If selected, the antivirus will also scan for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional 'utility' when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the internet. ***(Default = Enabled)***

To schedule the scan to run at specified times

- Click 'Schedule' from the top of the 'Scans' interface.



COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

Frequency:

○ Do not schedule this task

○ Every Day

● Every Week

○ Every Month

Start Time: 4 :00 PM

Day(s) of Week

Additional Options

□ Run only when computer is not running on battery

□ Run only when computer is IDLE

□ Turn off computer if no threats are found at the end of the scan

The options to schedule the scans will be displayed.

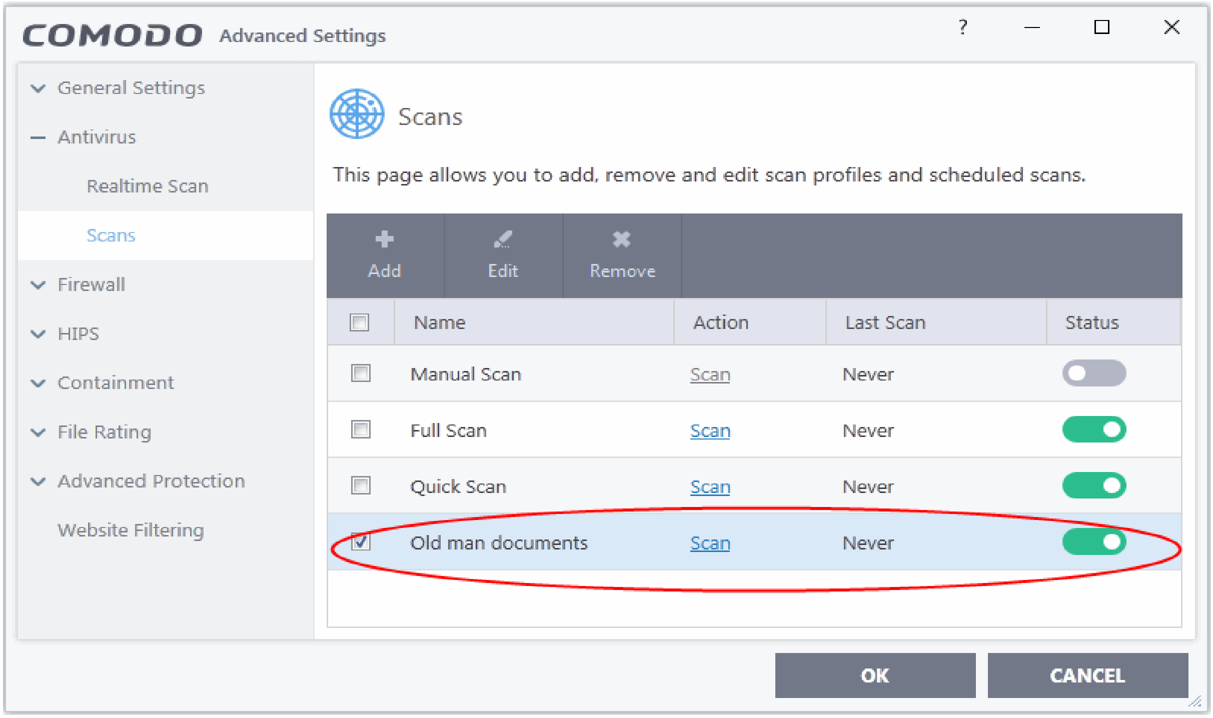
- **Do not schedule this task -** The scan profile will be created but will not run automatically. The profile will be available for manual, on-demand scans.
- **Every Day -** Scans the areas defined in the profile every day at the time specified in the 'Start Time' field.
- **Every Week -** Scans the areas defined in the profile on the day(s) specified in 'Days of the Week' field at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- **Every Month -** Scans the areas defined in the profile on the date(s) specified in 'Days of the month' field at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery -** The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or any other battery driven portable computer.
- **Run only when computer is IDLE -** The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan -** Selecting this option turns your computer off if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- **Run during Windows Maintenance -** Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.

The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See the explanation of **Automatically Clean Threats** above.

Note: The scheduled scan will run only if the scan profile is enabled. Use the switch in the 'Status' column to toggle a profile on or off.

- Click 'OK' to save the profile.

The profile will be available for deployment in future.



Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	○
□	Full Scan	Scan	Never	●
□	Quick Scan	Scan	Never	●
☑	Old man documents	Scan	Never	●

Run Untrusted Programs in the Container

Comodo Internet Security allows you to run programs inside the Container on a 'one-off' basis. This is helpful for testing new programs you have downloaded, for applications that you are not sure that you trust, and for running beta software. You can also create a desktop shortcut to run the application inside the container on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:

Comodo Internet Security allows you to run a program in the container:

- **From the right click options**
- **From the 'Containment Tasks' interface**
- **Running browsers inside container**

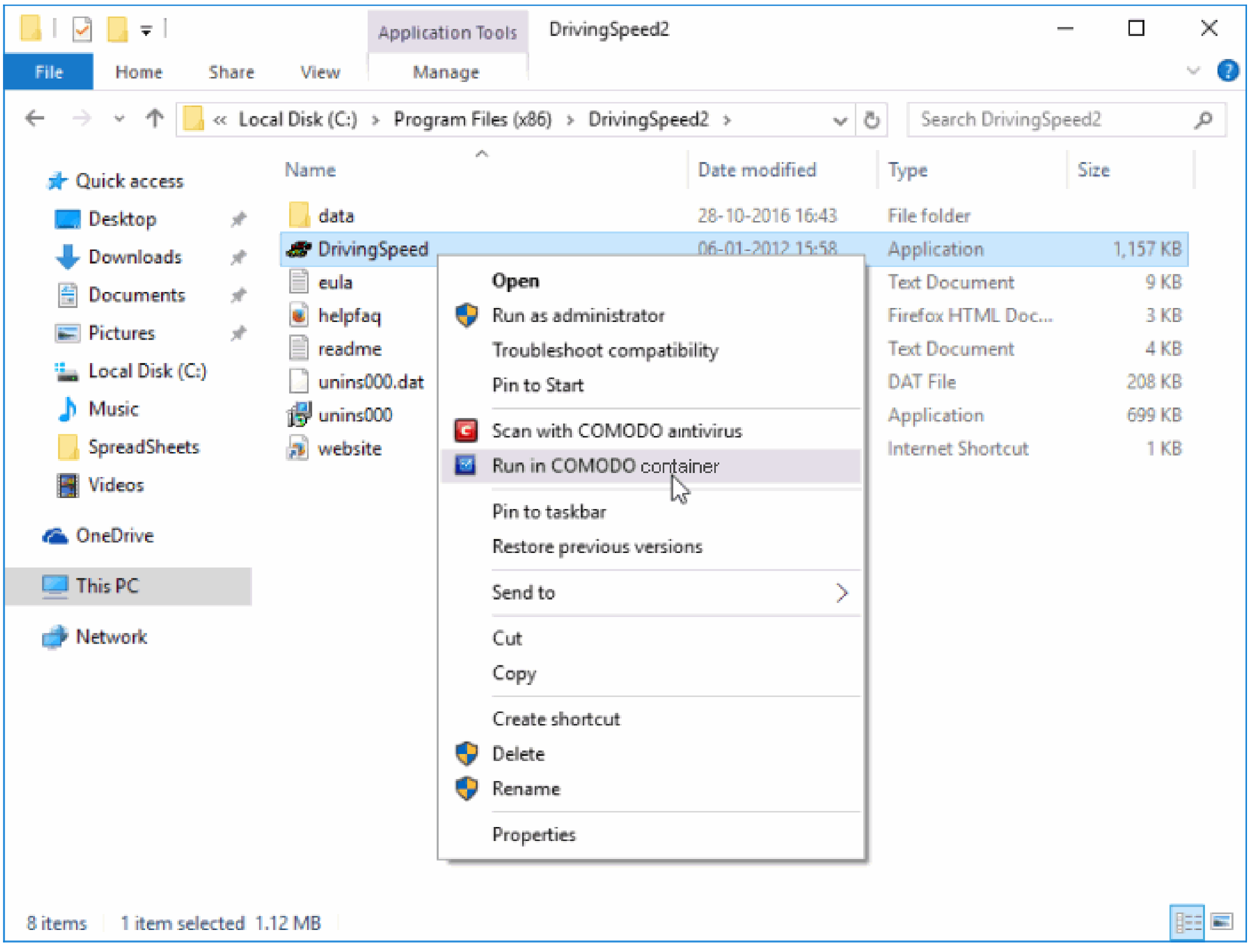
Note: If you wish to run an application in the container on a long-term basis then **add the file to the Container.**

Right-click menu

1. Open Windows Explorer and navigate to the program you want to run in the container

2. Right-click on the program

3. Choose 'Run in COMODO container' from the context sensitive menu:

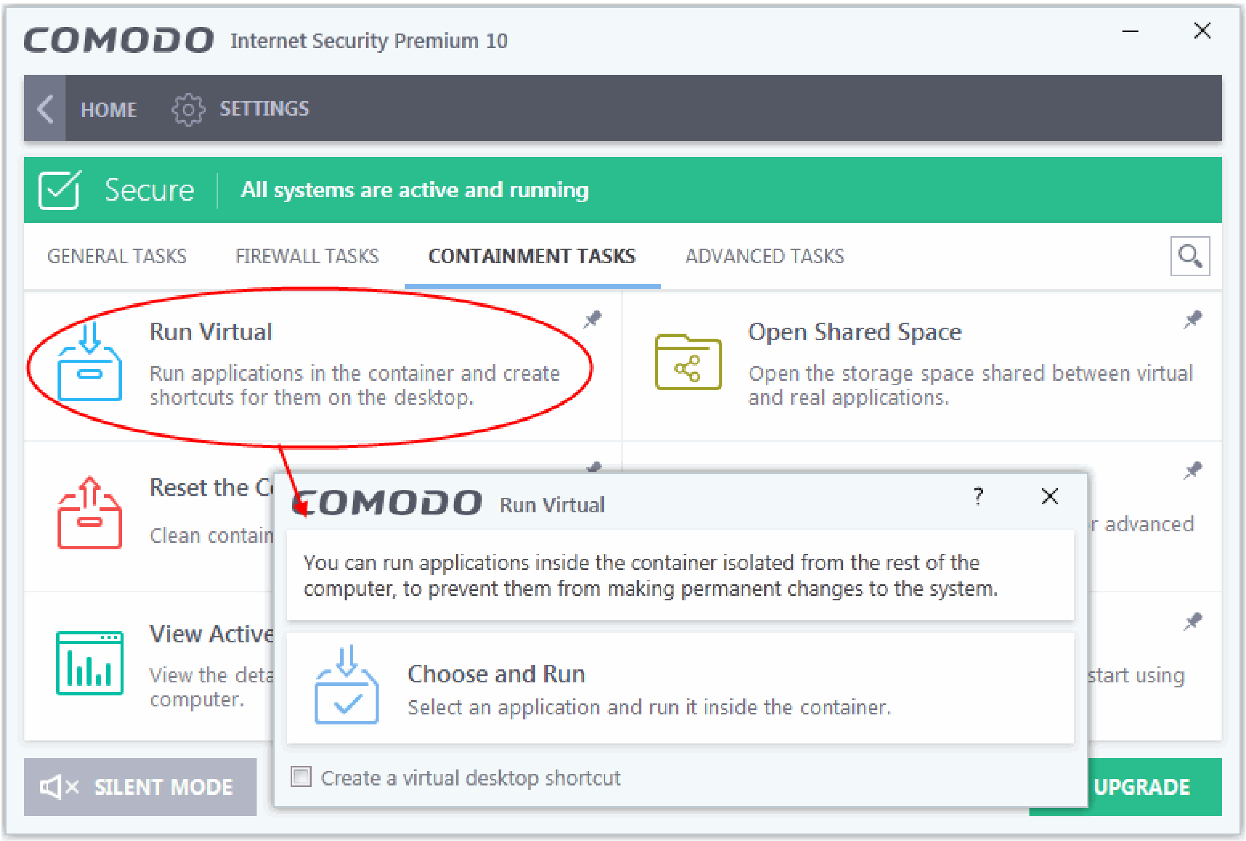


From the 'Containment Tasks' interface

1. Open the 'Tasks' interface by clicking 'Tasks' from the top left of the CIS home screen

2. Click the 'Containment Tasks' tab

3. Click 'Run Virtual' from the 'Containment Tasks' interface



You can run applications inside the container isolated from the rest of the computer, to prevent them from making permanent changes to the system.

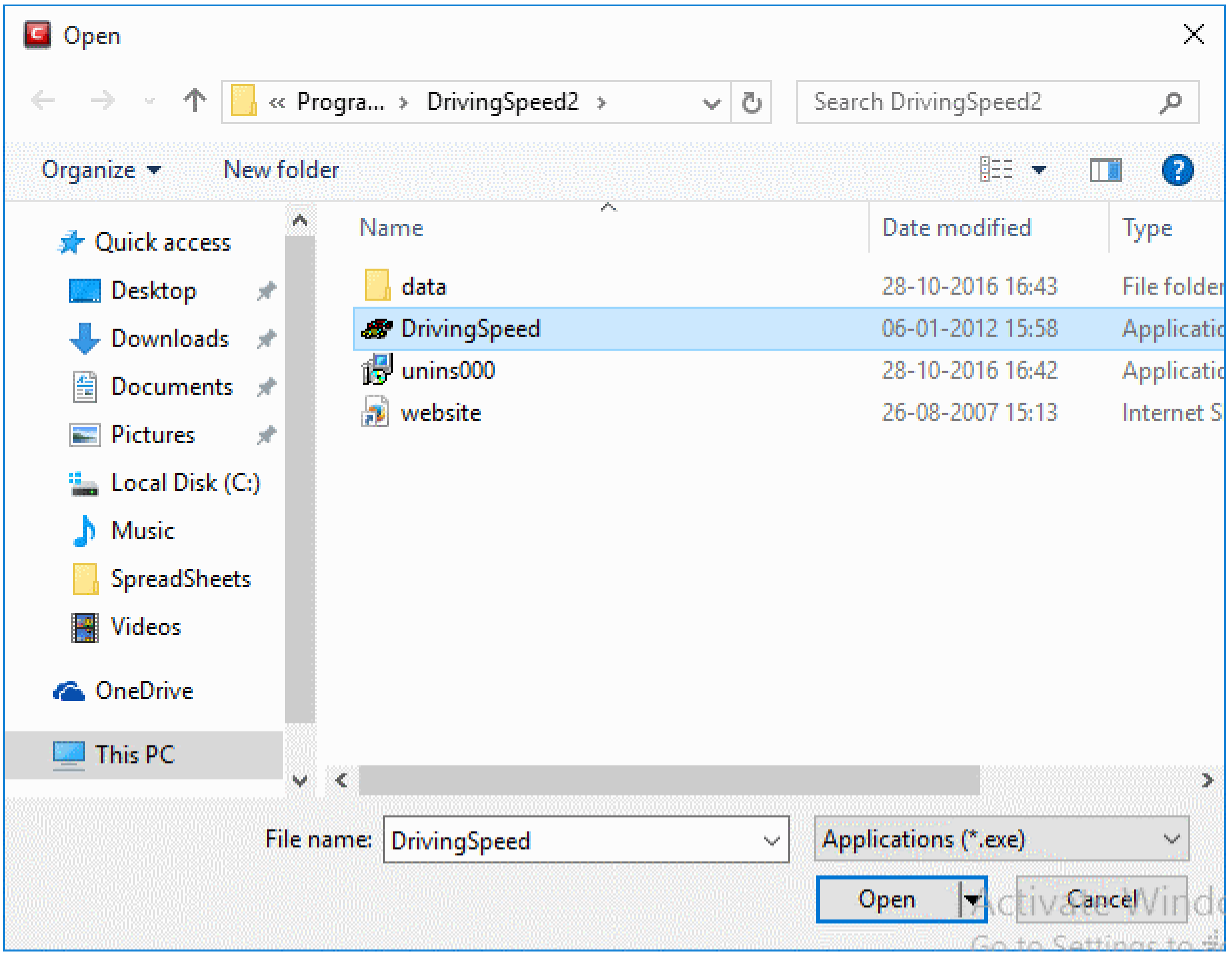
Choose and Run

Select an application and run it inside the container.

□ Create a virtual desktop shortcut

The 'Run Virtual' dialog will be displayed.

4. To run an application inside the container, click 'Choose and Run' then browse to the application. The contained application will run with a green border around it. Select 'Create a virtual desktop shortcut' to quickly run the application in the container in future.



Name	Date modified	Type
data	28-10-2016 16:43	File folder
DrivingSpeed	06-01-2012 15:58	Applicatio
unins000	28-10-2016 16:42	Applicatio
website	26-08-2007 15:13	Internet S

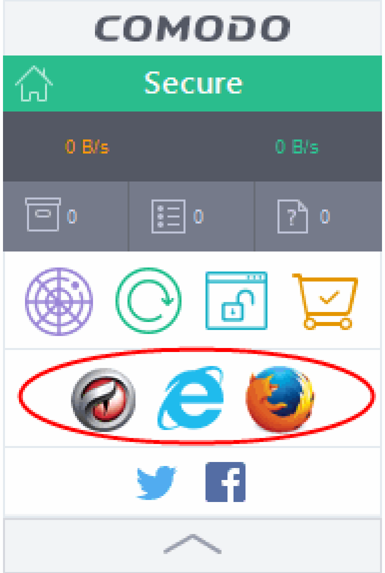
File name: DrivingSpeed

Applications (*.exe)

5. Browse to the application and click 'Open'.

Running Browsers inside the Container

The CIS widget contains shortcuts to the browsers installed on your computer:

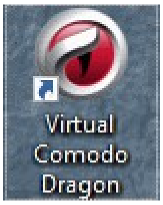


- Click a browser icon to start the browser inside the container
- The application will run in the container on this occasion only.
- You can create a 'virtual shortcut' for the browser by selecting the check-box 'Create a virtual desktop shortcut' in step 2. This will allow you to quickly launch a containerized instance of the browser in future.

- If you wish to run an application in the container on a permanent basis then **add the file to the Container.**

Run Browsers in the Container

- This topic explains how to run your internet browser inside the container.
- Surfing the internet from within the container is the same as normal, with the benefit that any malicious files you inadvertently download cannot damage your real computer.
- You can also create a desktop shortcut to run the browser inside the container on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:

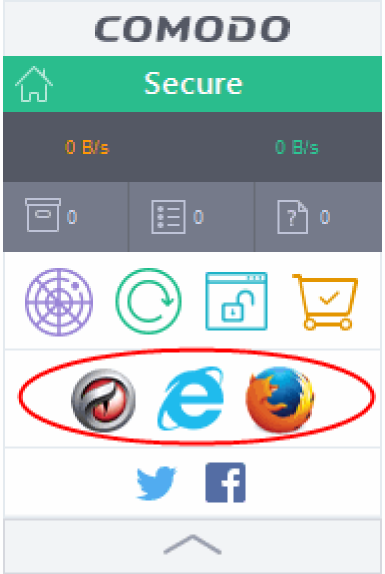


There are two ways to run a browser in the container:

- **From the desktop widget**
- **From the 'Containment Tasks' interface**

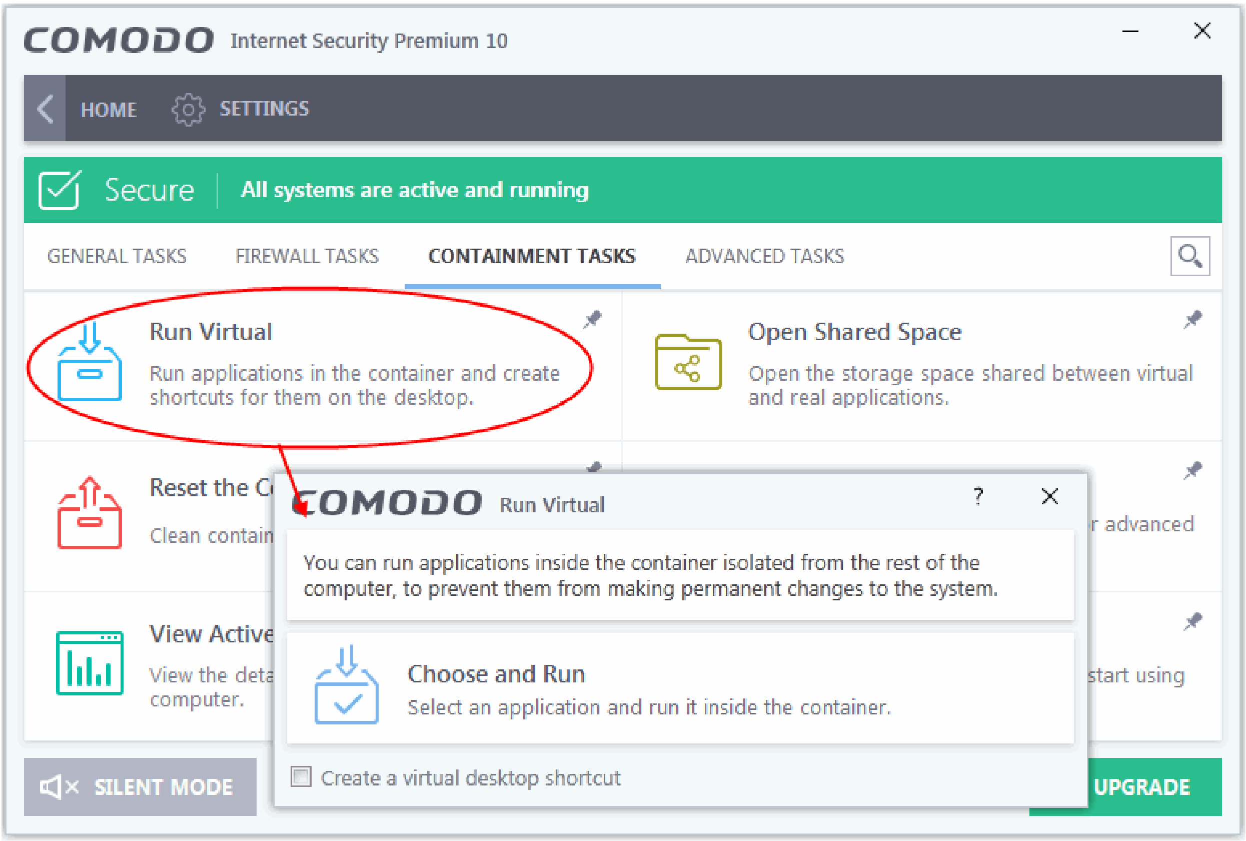
Start a browser from the desktop widget

- Click 'Tasks' at the top left of the CIS home screen
- Click the 'Containment Tasks' tab
- Click 'Run Virtual'



Start a browser from the 'Containment Tasks' interface

- Click Tasks' at the top-left of the CIS home screen
- Click the 'Containment Tasks' tab
- Click 'Run Virtual':


COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Run Virtual
Run applications in the container and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset the C
Clean contain
View Active
View the deta computer.
r advanced
start using
SILENT MODE
UPGRADE

COMODO Run Virtual

You can run applications inside the container isolated from the rest of the computer, to prevent them from making permanent changes to the system.

Choose and Run

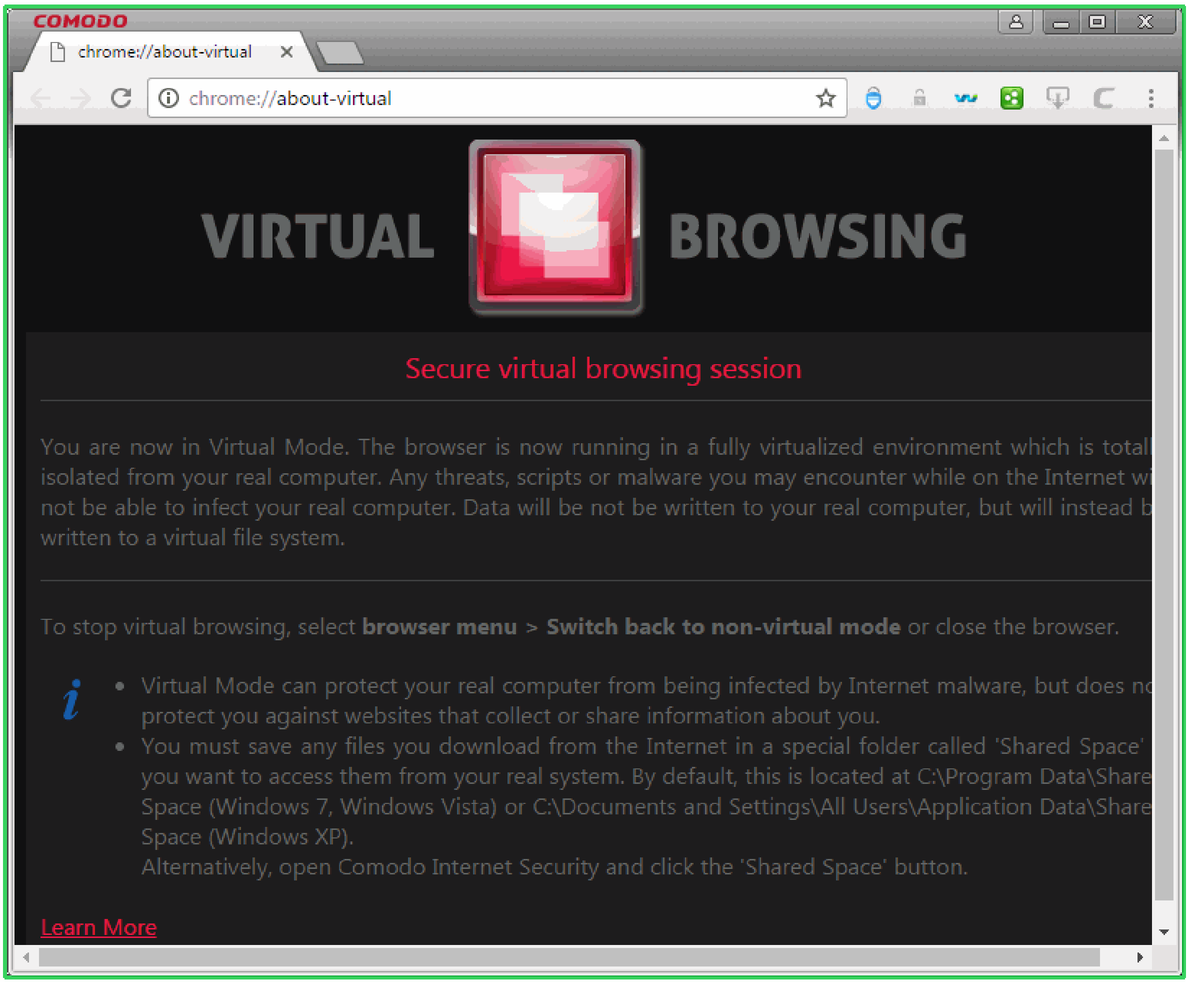
Select an application and run it inside the container.

☐ Create a virtual desktop shortcut

The 'Run Virtual' dialog will open:

- To run a browser inside the container, click 'Choose and Run'.
- Navigate to the installation location of the browser and select the .exe file of the browser.
- Select 'Create a virtual desktop shortcut' to quickly run the application in the container in future.

The browser will run with a green border indicating that it is contained.



Secure virtual browsing session

You are now in Virtual Mode. The browser is now running in a fully virtualized environment which is total isolated from your real computer. Any threats, scripts or malware you may encounter while on the Internet wi not be able to infect your real computer. Data will be not be written to your real computer, but will instead b written to a virtual file system.

To stop virtual browsing, select **browser menu** > **Switch back to non-virtual mode** or close the browser.

- Virtual Mode can protect your real computer from being infected by Internet malware, but does no protect you against websites that collect or share information about you.
- You must save any files you download from the Internet in a special folder called 'Shared Space' you want to access them from your real system. By default, this is located at C:\Program Data\Share Space (Windows 7, Windows Vista) or C:\Documents and Settings\All Users\Application Data\Share Space (Windows XP).
  Alternatively, open Comodo Internet Security and click the 'Shared Space' button.

Learn More

Run Untrusted Programs in the Virtual Desktop

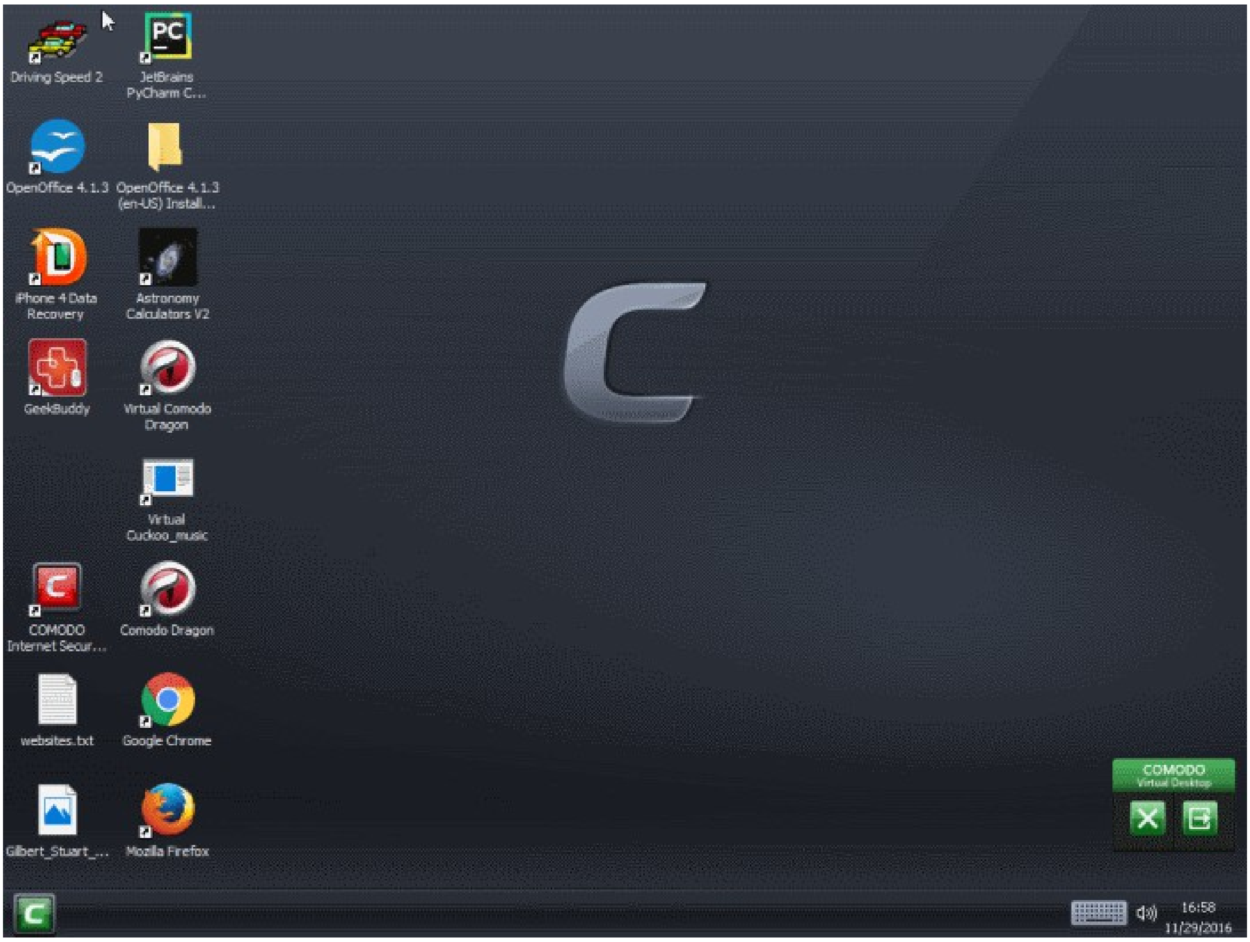
This page explains how to run untrusted programs inside the Virtual Desktop. Applications running in the virtual desktop leave no trails or history behind on your real system, making it ideal for testing out beta/unstable software.

Applications or files can be opened in the Virtual Desktop using the following methods:

- **Open applications/files from desktop shortcuts**
- **Use the 'Shared Space' folder to access applications/files**

Desktop Shortcuts

- You can create shortcuts to files or applications in Virtual Desktop on the desktop of your real system.
- The shortcuts on your real desktop will be available in the Virtual Desktop. Double-click them to while in the Virtual Desktop to run the application virtually.



Note: You must use **Classic Windows Mode** or **Tablet + Classic Mode** to view the icons/shortcuts on your real desktop.

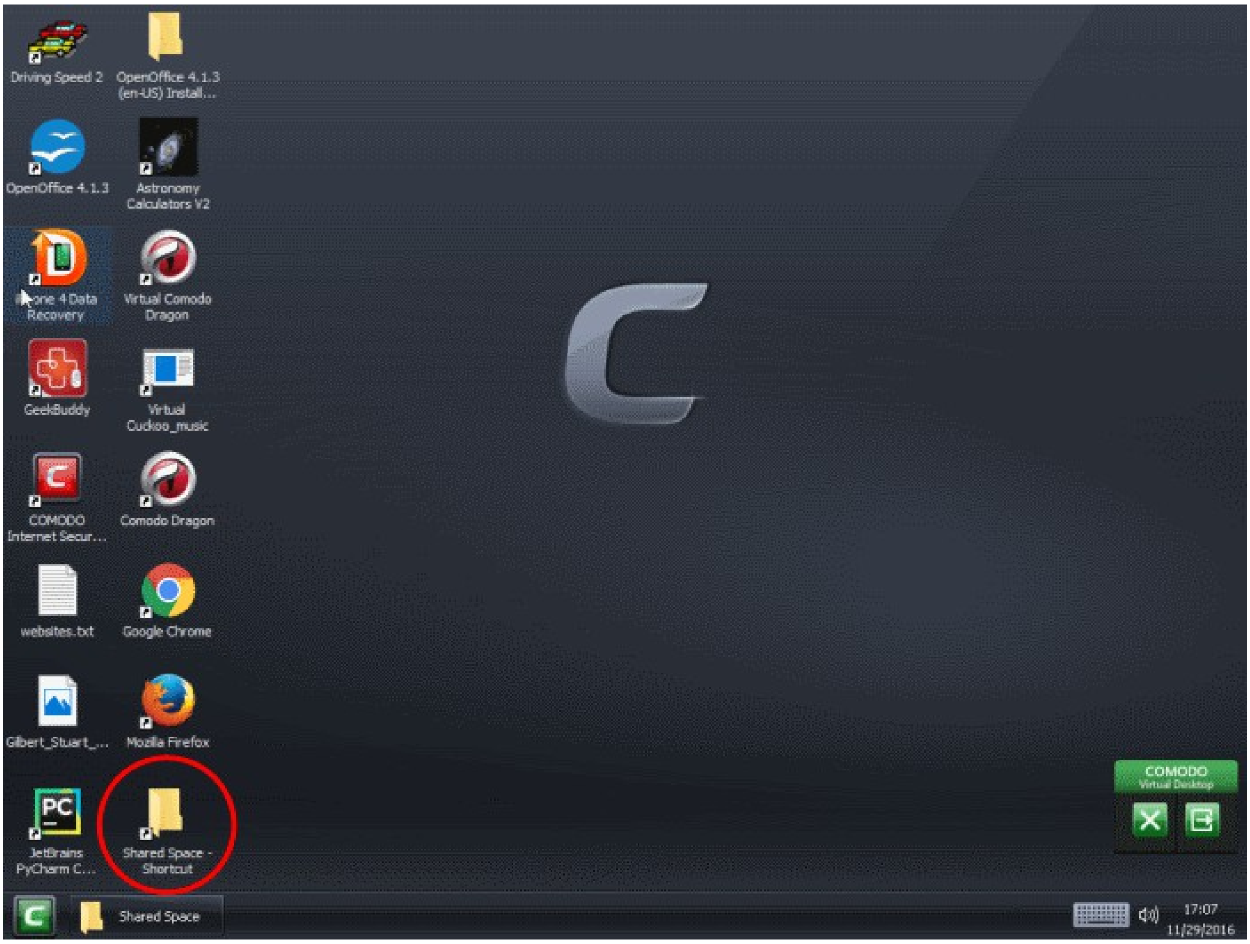
Shared Space

1. The virtual desktop creates a folder called 'Shared Space' at **C:\Program** Data\Shared Space.

- This folder can be accessed by your host operating system and the virtual desktop. You can use this folder to move files between the two systems.
- Shared space can be opened as follows:
  - Click 'Tasks' > 'Containment' > 'Open Shared Space'
    OR
  - Click the 'Shared Space' shortcut on the CIS widget

To open an application or file from your host system in the Virtual Desktop

2. Open the 'Shared Space' as mentioned above
3. Copy/Move the application or the file to be opened into the Shared Space
4. Create a desktop shortcut for the Shared Space folder by browsing to **C:\Program** Data > right-click on the 'Shared Space' folder > Choose 'Send to'...'Desktop'
5. Start 'Virtual Desktop' by clicking 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
6. Open 'Shared Space' inside the 'Virtual Desktop' by clicking the 'Shared Space' shortcut icon in the home screen.



Note: You must use **Classic Windows Mode** or **Tablet + Classic Mode** to view the icons/shortcuts on your real desktop.

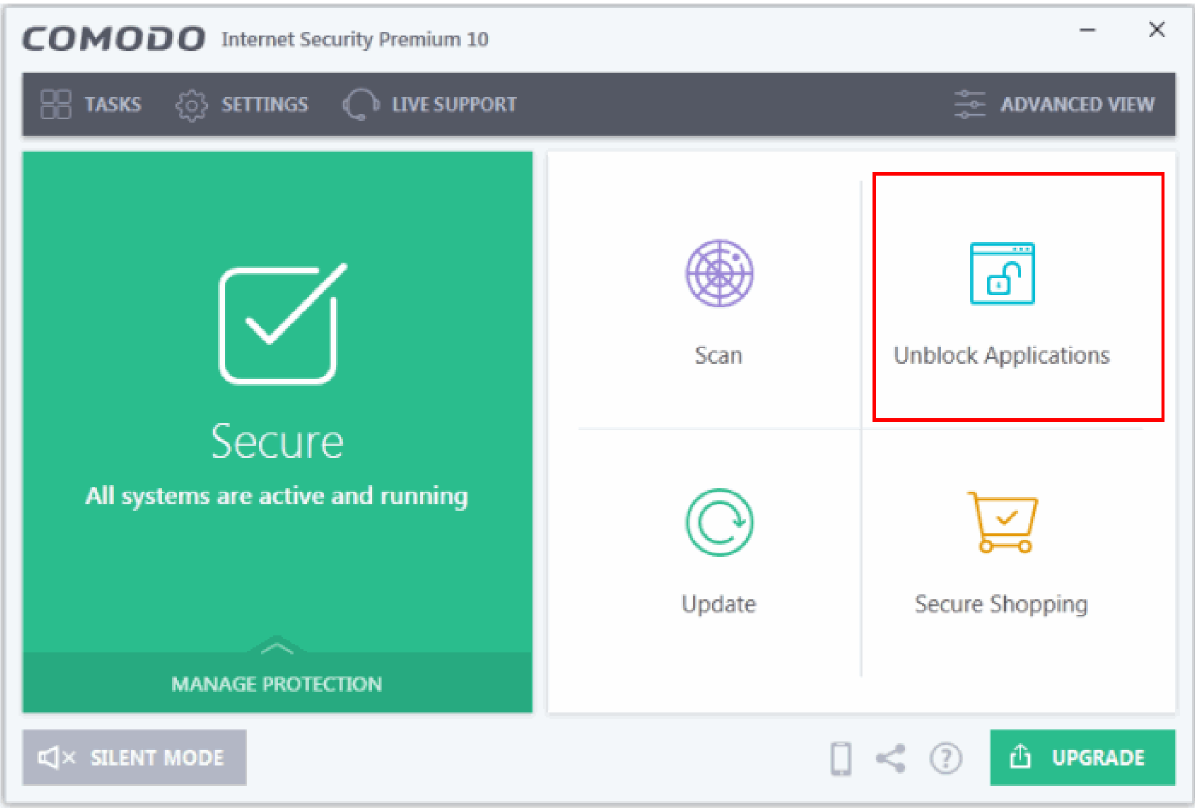
6. Double click on the application/file in the shared space to open it inside the 'Virtual Desktop'.

Restore Incorrectly Blocked Items

If you feel an item has been incorrectly blocked by CIS (a false positive) then you can restore it using one of the following methods:

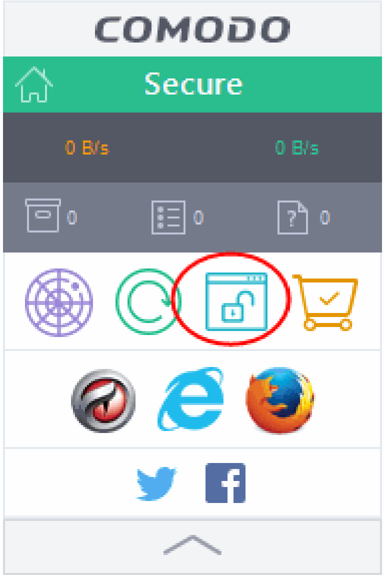
To release blocked applications

- Click 'Unblock Applications' in the 'Basic' view of the CIS home screen:



OR

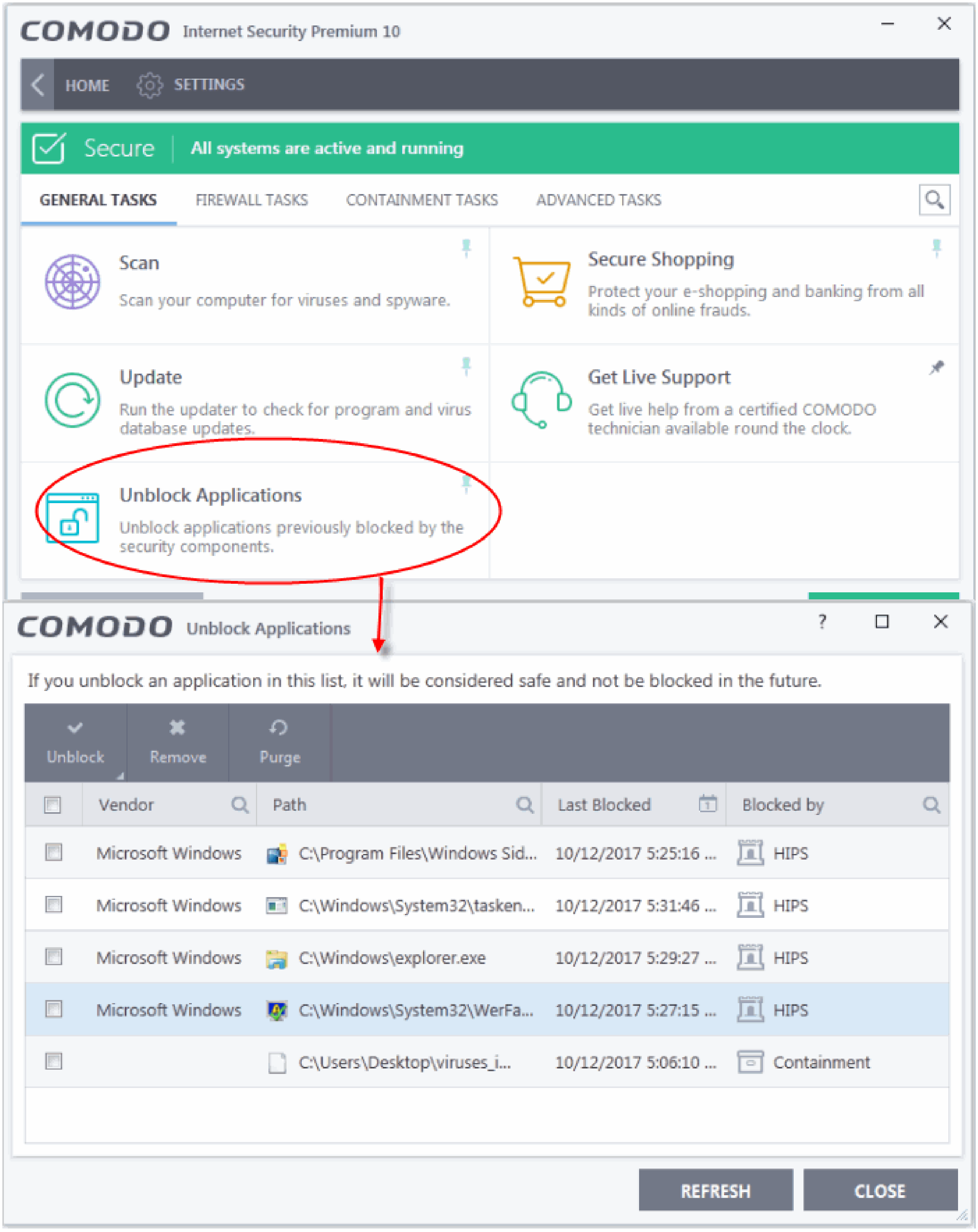
- Click the 'Unblock Applications' icon on the CIS Widget:



OR

- Click 'Tasks' at the top-left of the home screen then 'General Tasks' > 'Unblock Applications'

The 'Unblock Applications' interface shows a list of applications and programs that were blocked by different components of CIS.



Scan
Scan your computer for viruses and spyware.

Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.

Update
Run the updater to check for program and virus database updates.

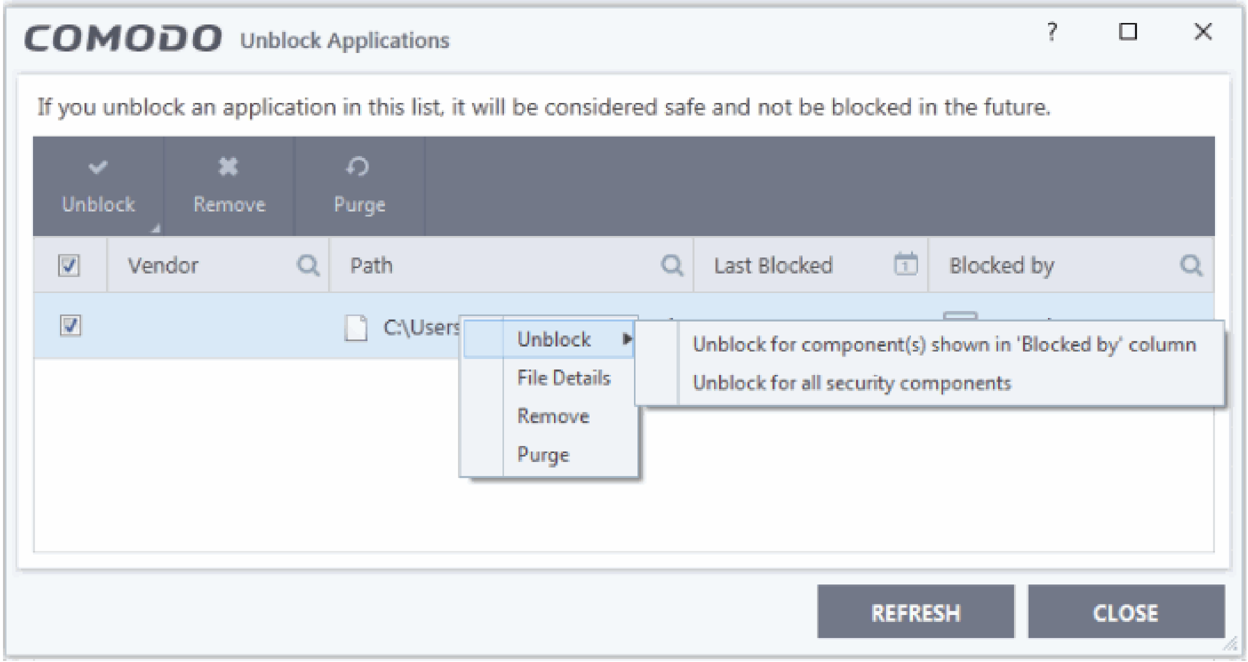
Get Live Support
Get live help from a certified COMODO technician available round the clock.

Unblock Applications
Unblock applications previously blocked by the security components.

If you unblock an application in this list, it will be considered safe and not be blocked in the future.

□	Vendor	Path	Last Blocked	Blocked by
□	Microsoft Windows	C:\Program Files\Windows Sid...	10/12/2017 5:25:16 ...	HIPS
□	Microsoft Windows	C:\Windows\System32\tasken...	10/12/2017 5:31:46 ...	HIPS
□	Microsoft Windows	C:\Windows\explorer.exe	10/12/2017 5:29:27 ...	HIPS
□	Microsoft Windows	C:\Windows\System32\WerFa...	10/12/2017 5:27:15 ...	HIPS
□		C:\Users\Desktop\viruses_i...	10/12/2017 5:06:10 ...	Containment

- To unblock applications that you consider safe, select the application(s) and click 'Unblock':
  - Unblock for component(s) shown in 'Blocked by' column' - Item(s) will be released only from the security component(s) that blocked them in the first place.
  - Unblock for all security components - item(s) will be released by all security components


COMODO Unblock Applications
? □ ✕
If you unblock an application in this list, it will be considered safe and not be blocked in the future.
Unblock
Remove
Purge
☑ Vendor
Path
Last Blocked
Blocked by
☑ C:\Users
Unblock
File Details
Remove
Purge
Unblock for component(s) shown in 'Blocked by' column
Unblock for all security components
REFRESH
CLOSE

OR

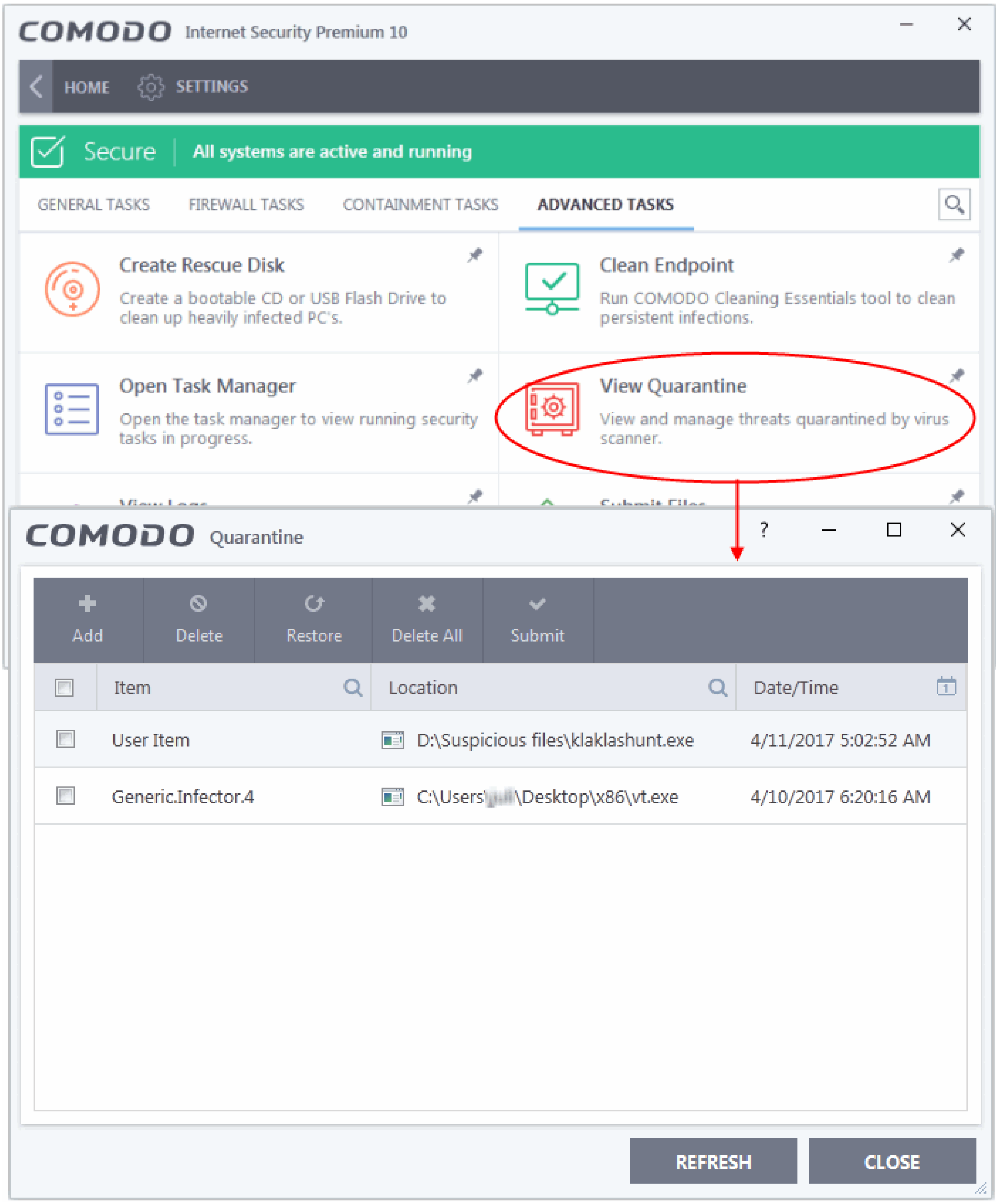
- Right-click on an item and choose 'Unblock' > 'Unblock for component(s) shown in 'Blocked by' column' or 'Unblock for all security components'

Restore Incorrectly Quarantined Item(s)

If you have incorrectly quarantined an item then you can restore it as follows:

- Click 'Tasks' at the top left of the CIS home screen
- Click the 'Advanced Tasks' tab
- Click 'View Quarantine'

The 'Quarantine' interface lists items automatically quarantined by the AV and those that were manually quarantined:



COMODO Internet Security Premium 10

Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

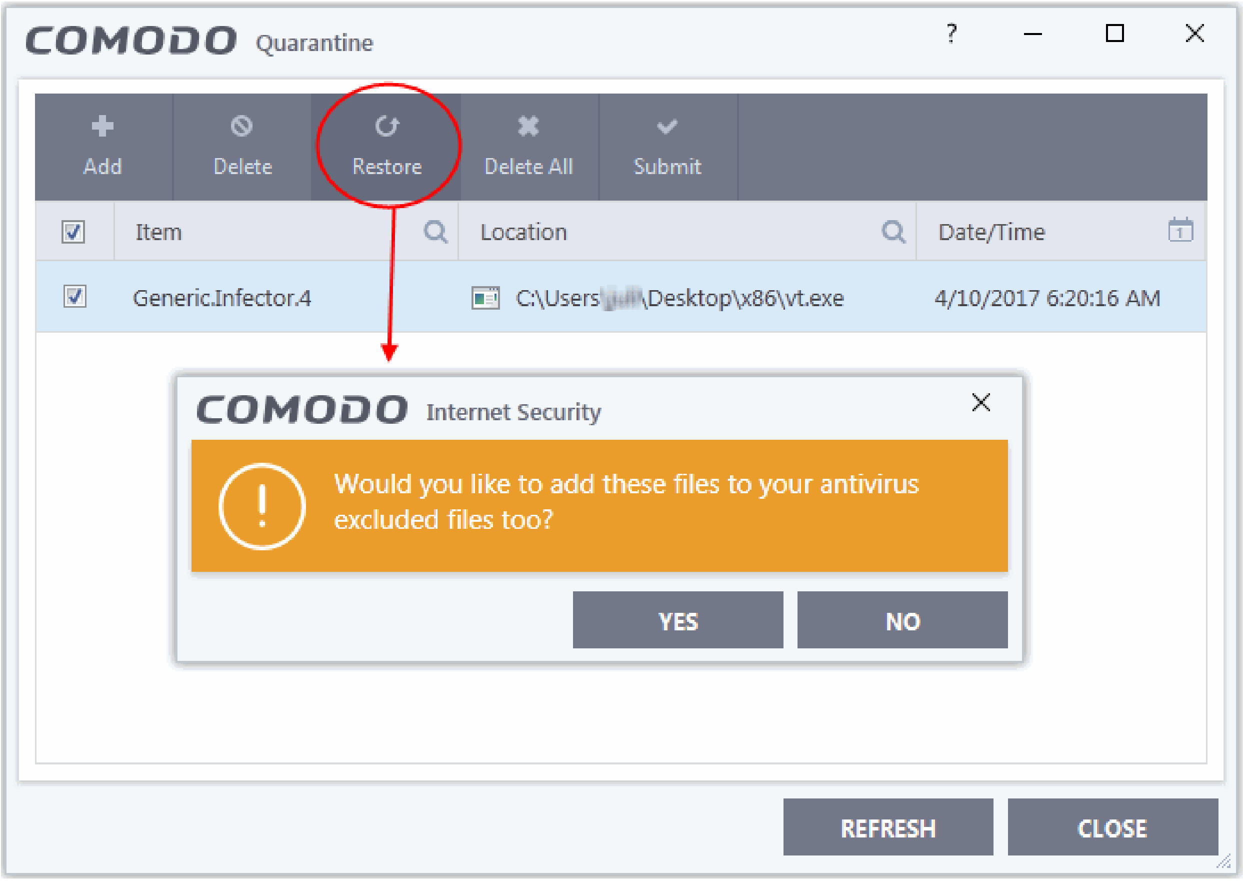
Open Task Manager
Open the task manager to view running security tasks in progress.

View Quarantine
View and manage threats quarantined by virus scanner.

COMODO Quarantine

□	Item	Location	Date/Time
□	User Item	D:\Suspicious files\klaklashunt.exe	4/11/2017 5:02:52 AM
□	Generic.Infector.4	C:\Users\[redacted]\Desktop\x86\vt.exe	4/10/2017 6:20:16 AM

- Select the item(s) you wish to move out of quarantine and click the 'Restore' button.
- You will then be asked if you wish to create an exclusion for the file so that it will not be flagged by future antivirus scans:



☑	Item	Location	Date/Time
☑	Generic.Infector.4	C:\Users\[redacted]\Desktop\x86\vt.exe	4/10/2017 6:20:16 AM

Would you like to add these files to your antivirus excluded files too?

- 'Yes' - the items will be restored to their original locations and added to the antivirus exclusion list. These files will be skipped during future scans.
- 'No' - the items will be restored to their original locations BUT may still be flagged by future antivirus scans.
- Click 'Close' to exit.

See **Managing Quarantined Items** and **Submit Quarantined Items to Comodo for Analysis** for more information on this topic.

Submit Quarantined Items to Comodo for Analysis

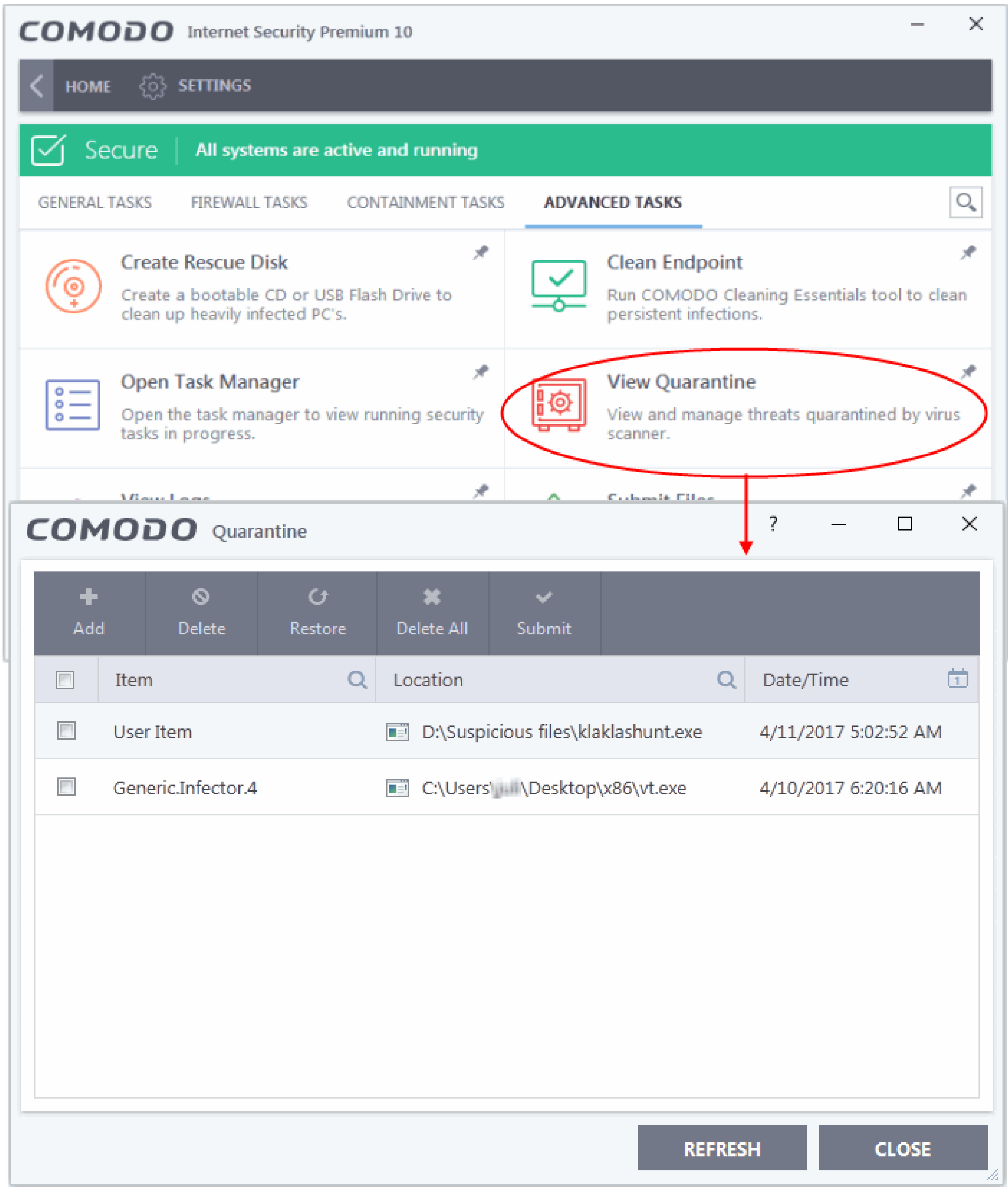
Items which have been quarantined as a result of an antivirus scan can be sent to Comodo for analysis. Comodo will attempt to establish the trustworthiness of the file using automatic and manual behavior tests.

- If the submitted item is found to be a false positive, it will be added to the Comodo white-list.
- If it is found to be malware, it will be added to the virus black-list.
- Submitting files helps Comodo enhance its virus signature database and benefits millions of CIS users. See **Quarantined Items** for more detailed information on the quarantine system.

To submit quarantined items

1. Click 'Tasks' at the top-left of the CIS home screen
2. Click the 'Advanced Tasks' tab
3. Click 'View Quarantine'

The 'Quarantine' interface will open. The interface lists files moved to quarantine by the antivirus scanner and files that were manually moved to quarantine.



COMODO Internet Security Premium 10

Create Rescue Disk – Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint – Run COMODO Cleaning Essentials tool to clean persistent infections.

Open Task Manager – Open the task manager to view running security tasks in progress.

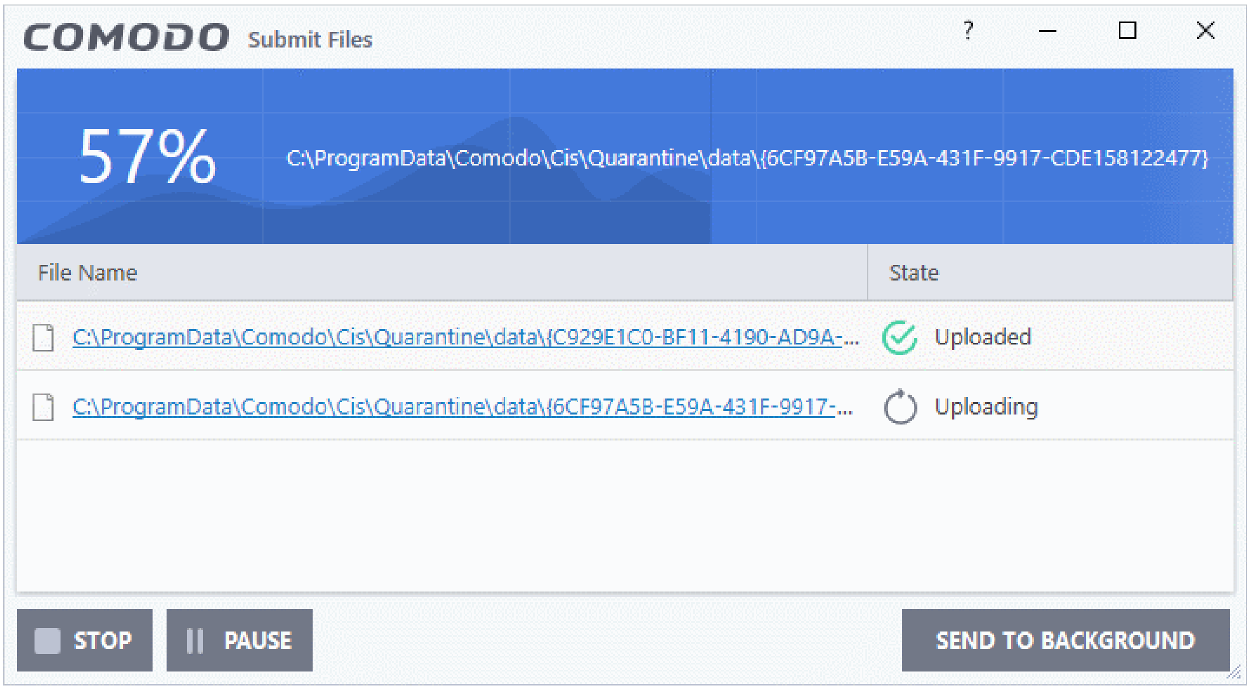
View Quarantine – View and manage threats quarantined by virus scanner.

COMODO Quarantine

□	Item	Location	Date/Time
□	User Item	D:\Suspicious files\klaklashunt.exe	4/11/2017 5:02:52 AM
□	Generic.Infector.4	C:\Users\[redacted]\Desktop\x86\vt.exe	4/10/2017 6:20:16 AM

4. Select the item(s) you wish to send for analysis and click the 'Submit' button at the top.

The submission progress will start:


COMODO Submit Files
?
57%
C:\ProgramData\Comodo\Cis\Quarantine\data\{6CF97A5B-E59A-431F-9917-CDE158122477}
File Name
State
C:\ProgramData\Comodo\Cis\Quarantine\data\{C929E1C0-BF11-4190-AD9A-...
✓ Uploaded
C:\ProgramData\Comodo\Cis\Quarantine\data\{6CF97A5B-E59A-431F-9917-...
Uploading
STOP
PAUSE
SEND TO BACKGROUND

The results will state whether the file was successfully submitted or whether it was already submitted by other users and is pending analysis.

Run Browsers in the Virtual Desktop

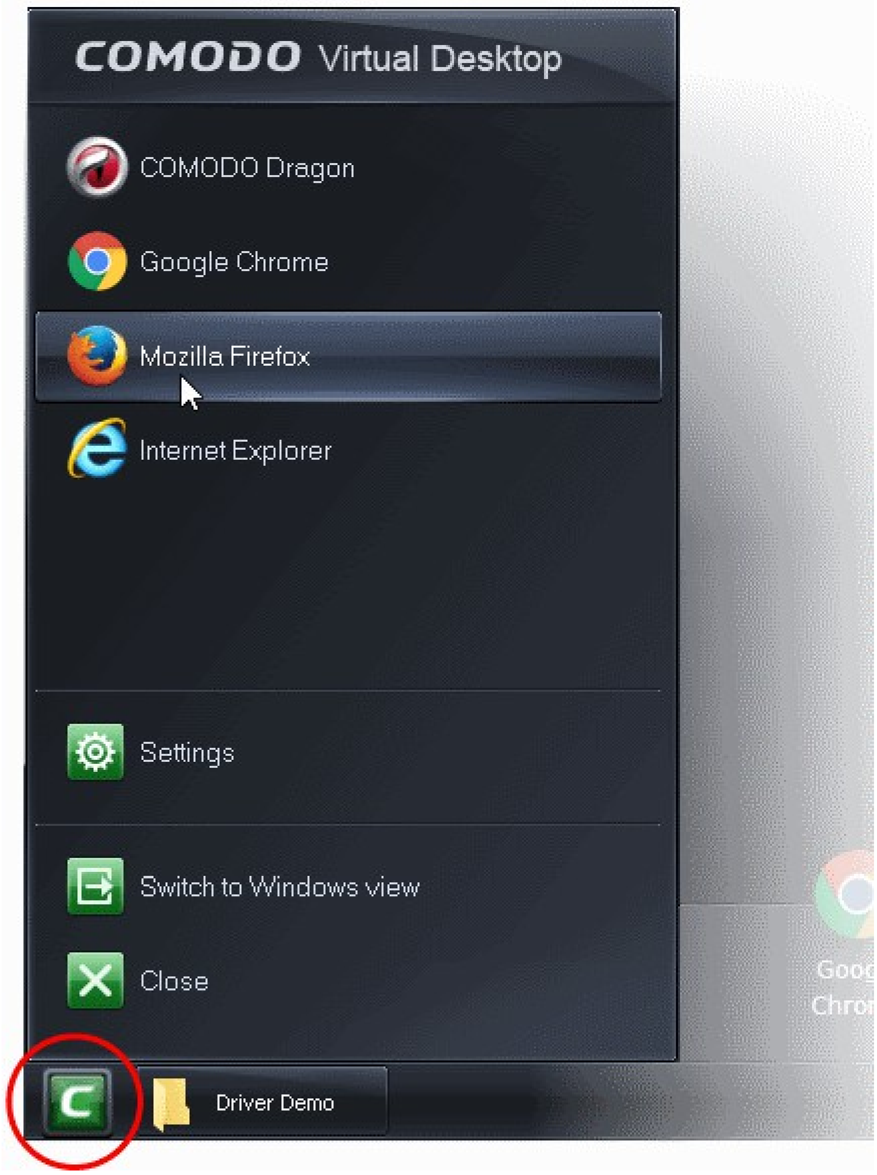
- The Virtual Desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer.
- Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information.
- Surfing the internet from inside the virtual desktop removes this threat by preventing websites from installing applications on your real computer.
- Furthermore, the Virtual Keyboard allows you to securely enter your user-names and passwords without fear of key-logging software recording your keystrokes.

To start the Virtual Desktop

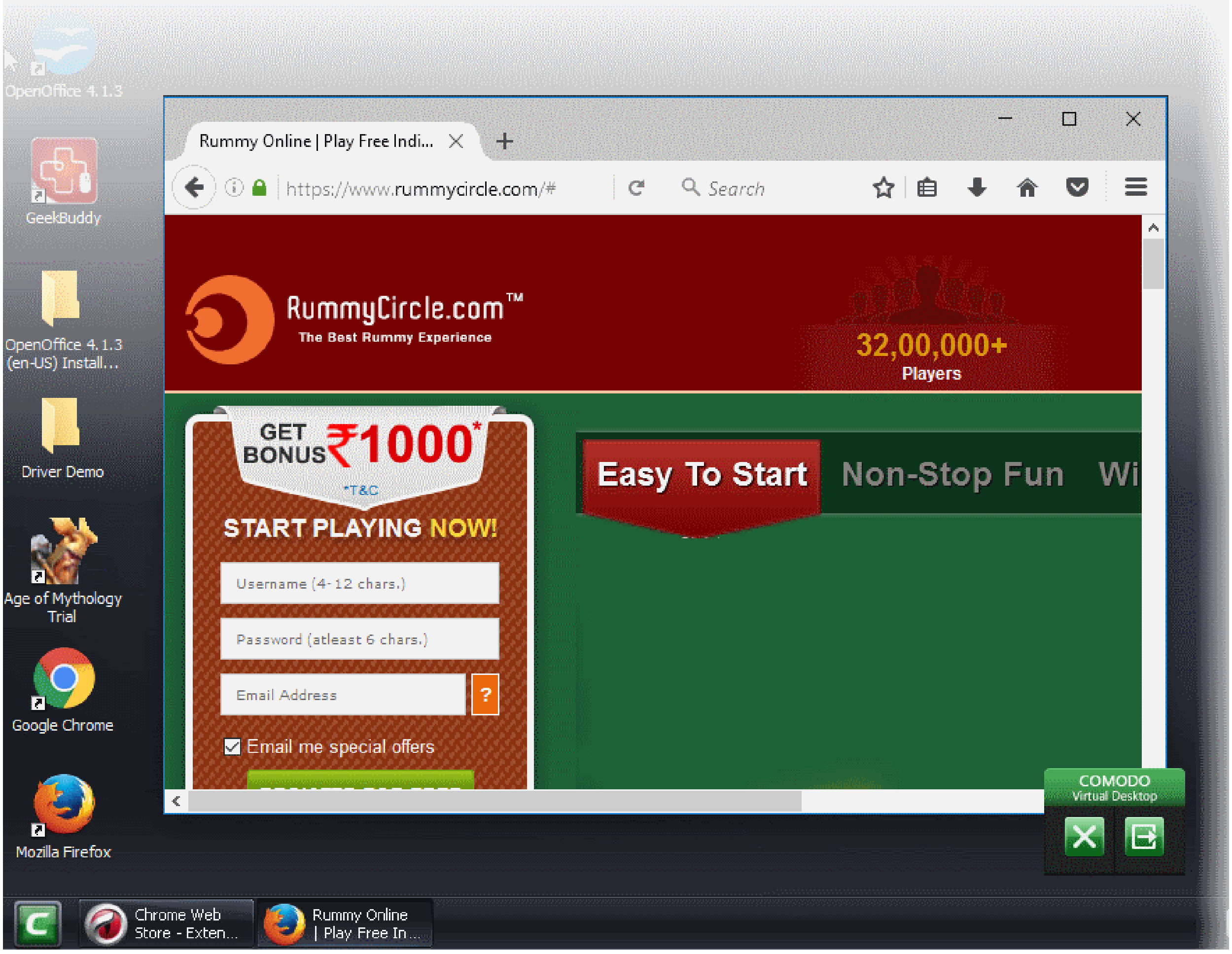
1. Click 'Tasks' at the top-left of the CIS home screen
2. Click the 'Containment Tasks' tab
3. Click 'Run Virtual Desktop'

To run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left of the Virtual Desktop
2. Select the browser you want to run



Your choice of browser will open inside the virtual desktop, ready for secure surfing:



Browsing history and other records of your internet activity will not be stored on your computer when your session is closed.

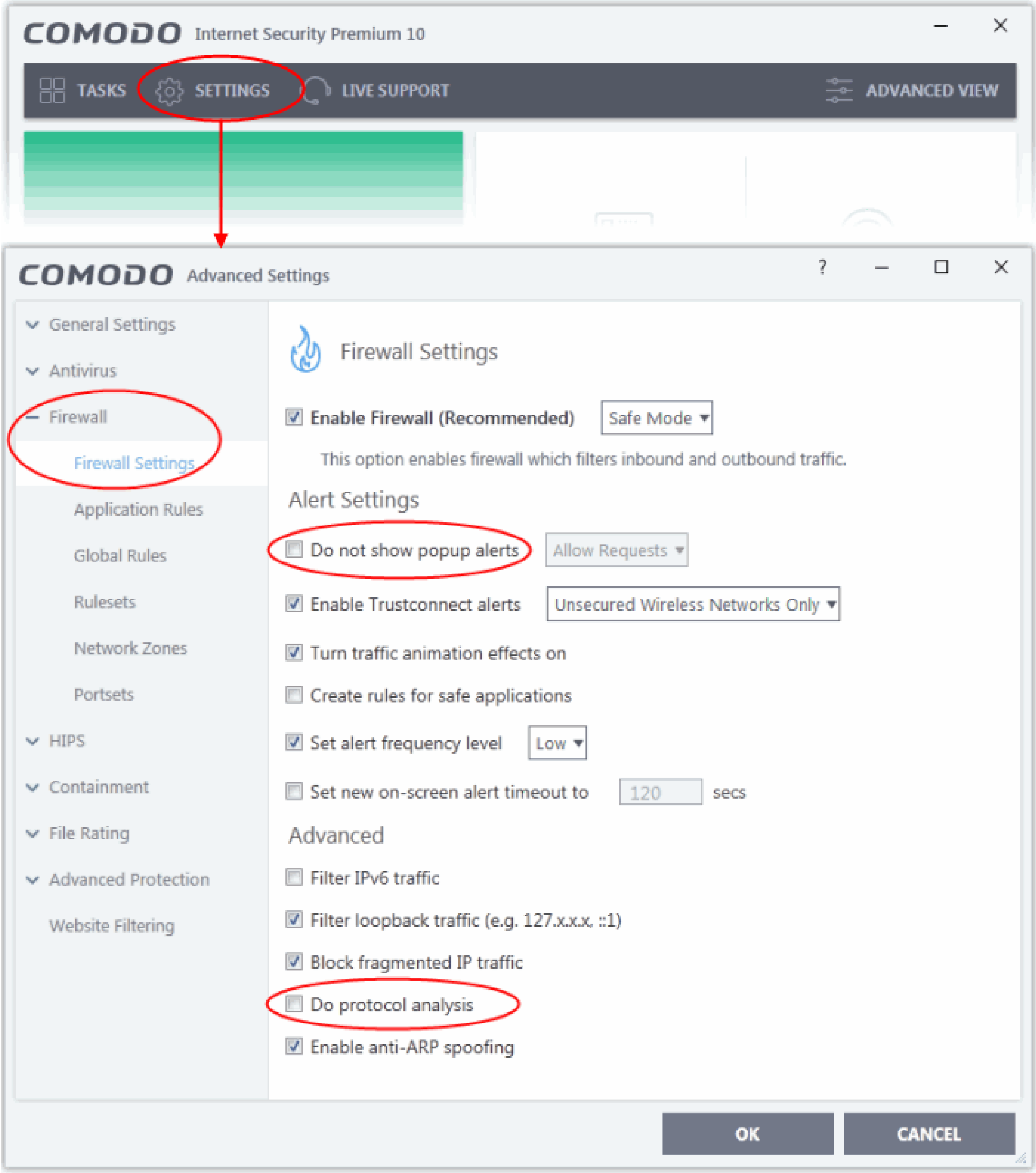
Enable File Sharing Applications like BitTorrent and Emule

This topic explains how to configure Comodo Firewall to work with file sharing applications like Shareaza/Emule and BitTorrent/UTorrent. To allow these file sharing applications, you must:

- **Disable 'Do Protocol analysis'** ***(disabled, by default)***
- **Create a 'Redefined Firewall Ruleset' for Shareaza/Emule**
- **Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent**

To Disable 'Do Protocol analysis'

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Firewall Settings' under 'Firewall' on the left



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

□ Do not show popup alerts Allow Requests

☑ Enable Trustconnect alerts Unsecured Wireless Networks Only

☑ Turn traffic animation effects on

□ Create rules for safe applications

☑ Set alert frequency level Low

□ Set new on-screen alert timeout to 120 secs

Advanced

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☑ Block fragmented IP traffic

□ Do protocol analysis

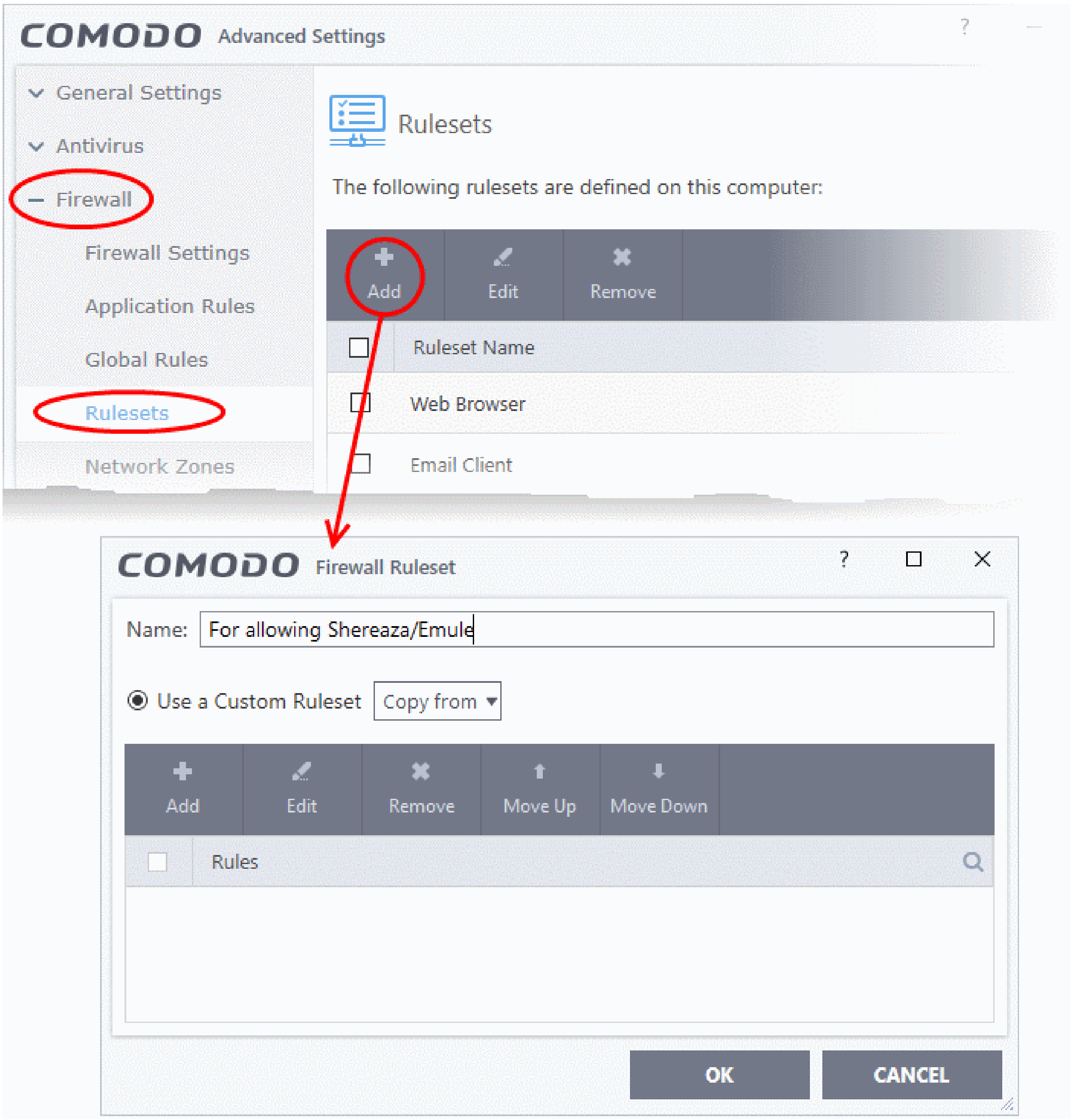
☑ Enable anti-ARP spoofing

3. Disable 'Do not show popup alerts' so CIS will generate alerts when you open Shareaza or Emule.
4. Disable 'Do Protocol Analysis'
5. Click 'OK' to save your settings.

To create a 'Predefined Firewall Ruleset' for Shareaza/Emule

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Rulesets' under 'Firewall' on the left.
3. Click 'Add' from the options at the top.

The 'Firewall Ruleset' interface will open:



The following rulesets are defined on this computer:

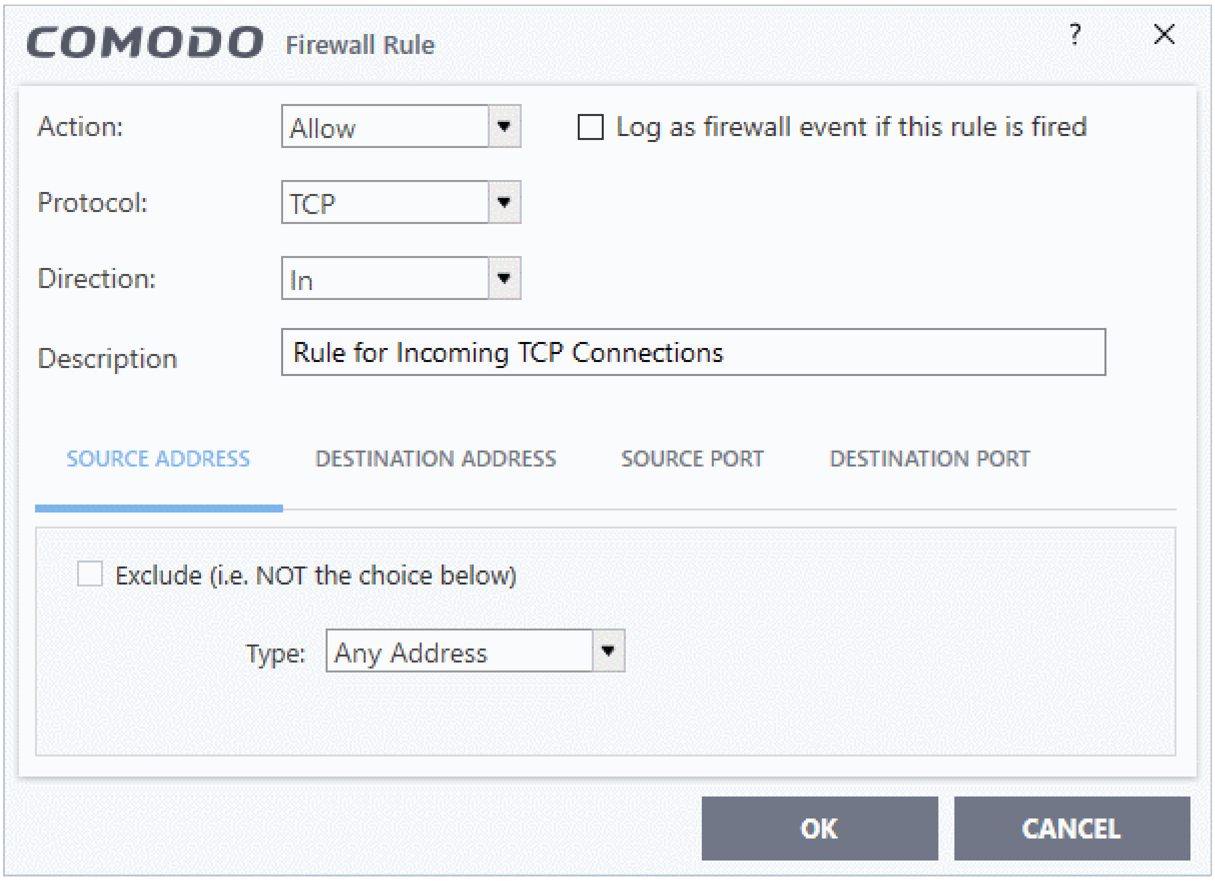
□	Ruleset Name
□	Web Browser
□	Email Client

Name: For allowing Shereaza/Emule

● Use a Custom Ruleset   Copy from ▾

□	Rules

4. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing Shareaza/Emule'.
5. Now you need to create six rules for the new ruleset:
   - Click 'Add' to open the 'Firewall Rule' interface
   - Choose options for each setting as described in 'Rule 1' below
   - After the rule is created, click 'OK' to add the rule
   - Repeat until all 6 rules have been added



Action: Allow

□ Log as firewall event if this rule is fired

Protocol: TCP

Direction: In

Description: Rule for Incoming TCP Connections

□ Exclude (i.e. NOT the choice below)

Type: Any Address

Rule 1

- Action : Allow
- Protocol : TCP
- Direction : In
- Description : Rule for incoming TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1024 / End Port = 65535)
- Destination port : A Single Port : (Port : Your TCP port of Shareaza/Emule)

Rule 2

- Action : Allow
- Protocol : UDP
- Direction : In
- Description : Rule for incoming UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1024 / End Port = 65535)
- Destination port : A Single Port : (Port : Your UDP port of Shareaza/Emule)

Rule 3

- Action : Allow
- Protocol : TCP or UDP
- Direction : Out

- Description : Rule for outgoing TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1024 / end port = 65535)
- Destination port : A port range : (start port = 1024 / end port = 65535)

Rule 4

- Action : Allow
- Protocol : ICMP
- Direction : Out
- Description : Ping the server (edk network)
- Source Address : Any Address
- Destination Address : Any Address
- ICMP Details : Message : ICMP Echo Request

Rule 5

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1024 / end port = 65535)
- Destination port : Type : Single Port; (Port : 80)

Rule 6

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.
7. Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start Shareaza or Emule. When CIS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'For allowing Shareaza/Emule')
- Select 'Remember my answer'.

To create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Rulesets' under 'Firewall' on the left
3. Click 'Add' from the options at the top.

The 'Firewall Ruleset' interface will open:

4. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing For allowing BitTorrent/Utorrent'.

5. Now you need to create six rules for the newly created ruleset.

   To do so,

   - Click 'Add' to open the 'Firewall Rule' interface
   - Choose options for each setting as described in 'Rule 1' below
   - After the rule is created, click 'OK' to add the rule
   - Repeat until all 6 rules have been added

Rule 1

- Action : Allow
- Protocol : TCP or UDP
- Direction : In
- Description : Rule for incoming TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port : A Single Port (Port: The port of BitTorrent/Utorrent)

Rule 2

- Action : Allow
- Protocol : TCP
- Direction : Out
- Description : Rule for outgoing TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port : A Port Range : (Start port = 1024 / End port = 65535)

Rule 3

- Action : Allow
- Protocol : UDP
- Direction : Out
- Description : Rule for outgoing UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Single Port: Port: the port of utorrent
- Destination port : A Port Range : (Start port = 1024 / End port = 65535)

Rule 4

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)

- Destination port ; A Single Port (Port = 80)

Rule 5

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.
7. Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start BitTorrent or Utorrent. When CIS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'BitTorrent/Utorrent')
- Select 'Remember my answer'.

Block any Downloads of a Specific File Type

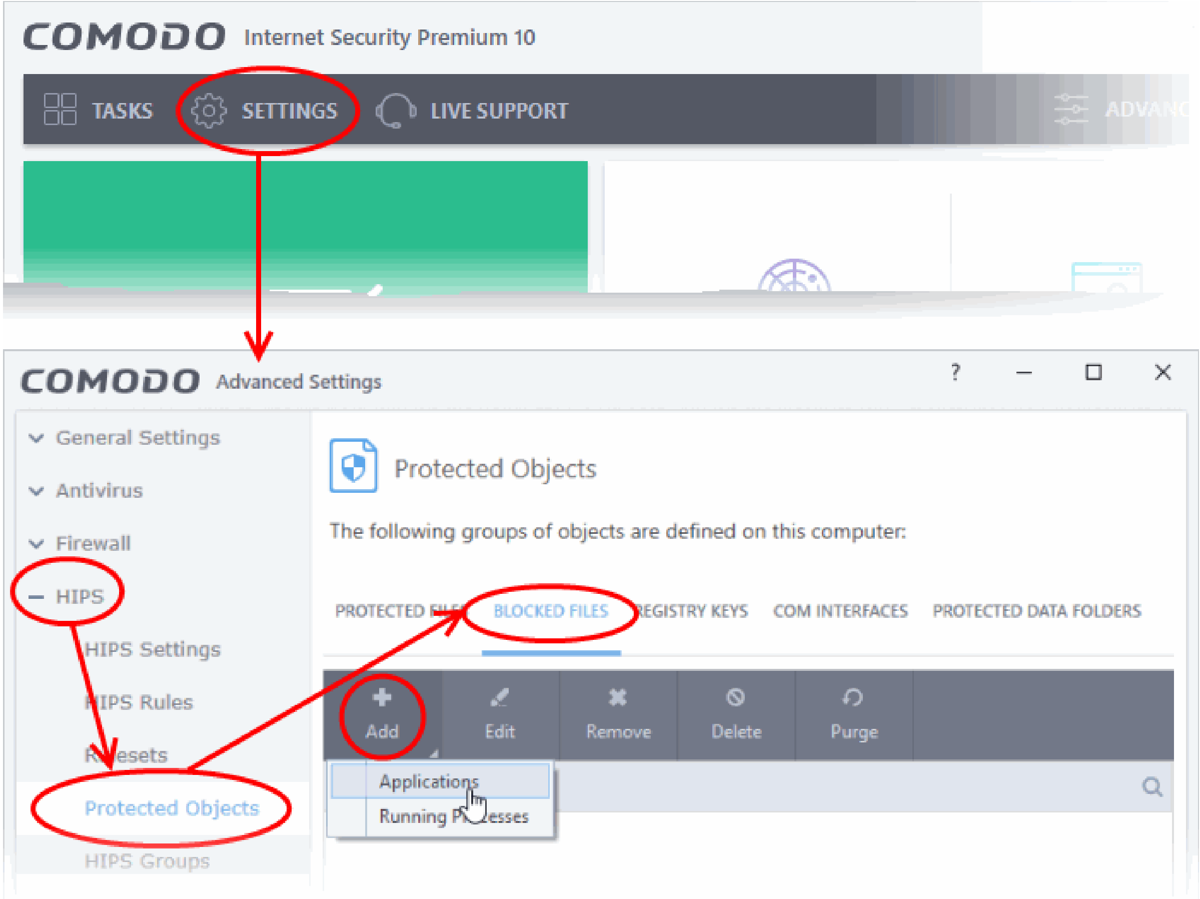
Comodo Internet Security can be configured to block downloads of specific types of file.

Example scenarios:

- Some malicious websites try to push downloads of malware in .exe file format. .exe files are programs which can execute commands on your computer. If the .exe is malicious then these commands could install a virus, initiate a buffer overflow attack or could contain code to turn your PC into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You may want to block the download of audio files (.wma, .mp3, .wav, .midi), video files (.wmv, .avi, .mpeg, .swf) or image files (.bmp. .jpg, .png) for various reasons.

You can block downloads of a specific file type in the HIPS section:

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'HIPS' > 'Protected Objects' on the left
3. Click the 'Blocked Files' tab

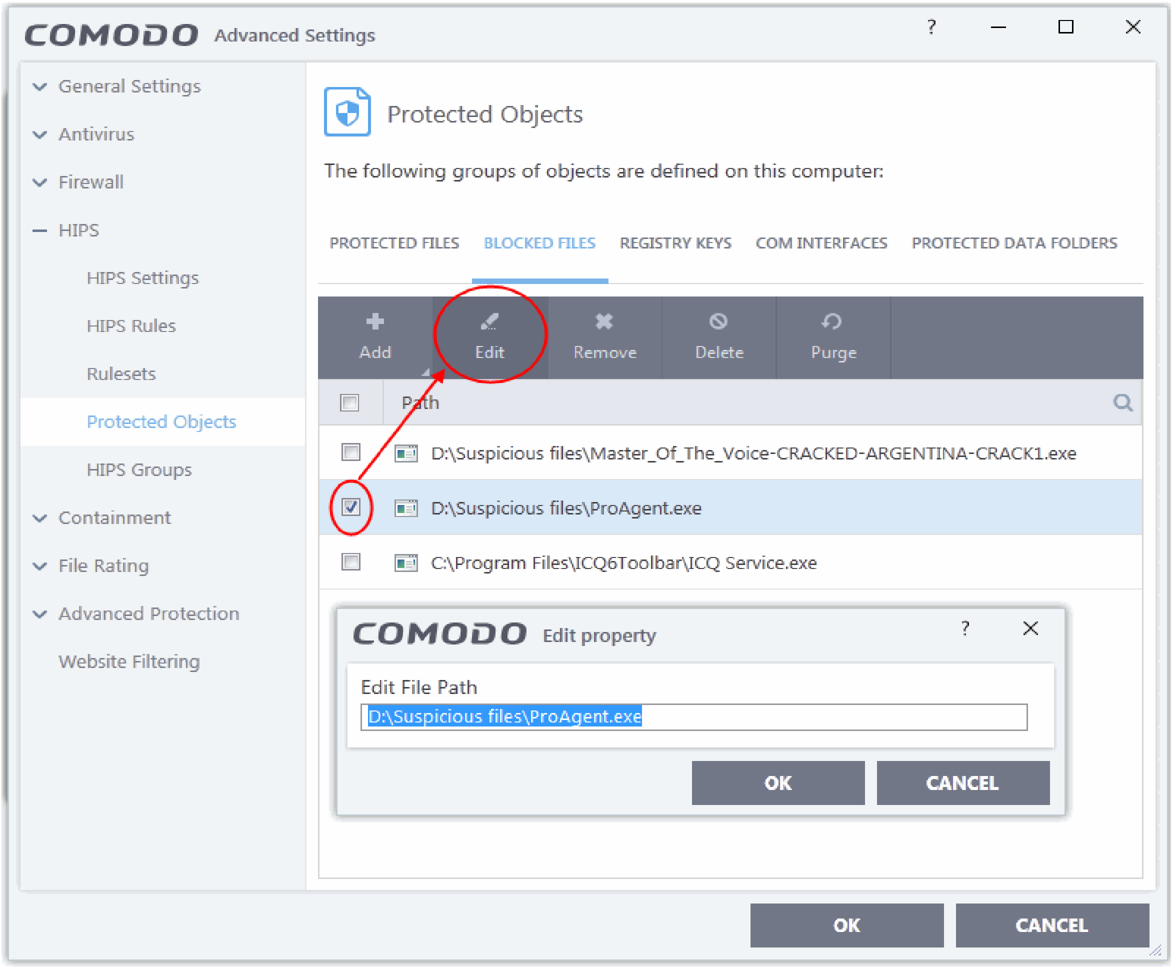


4. Click 'Add' > 'Applications'.
5. Browse to the default download folder for your browser from the 'Open' dialog:

The default download location for most browsers is C:\Users\[username]\Downloads

6. Select any file from the folder and click 'Open'.

The file will be added to the 'Blocked Files' list.



Protected Objects

The following groups of objects are defined on this computer:

	Path
□	D:\Suspicious files\Master_Of_The_Voice-CRACKED-ARGENTINA-CRACK1.exe
☑	D:\Suspicious files\ProAgent.exe
□	C:\Program Files\ICQ6Toolbar\ICQ Service.exe

COMODO Edit property

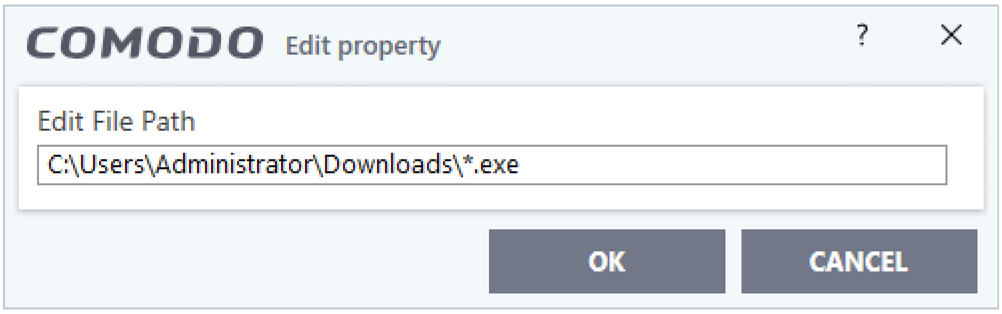
Edit File Path

D:\Suspicious files\ProAgent.exe

7. Select the entry from the Blocked Files interface, and click 'Edit' at the top

The 'Edit Property' dialog will appear.

8. Replace the name of the file with simply '*.file_extension', where 'file_extension' is the file type you wish to block. For example:
   - Change 'C:\Users\[username]\Downloads\file-name.pdf' to C:\Users\[username]\Downloads*.exe to block all files with *.exe extension.
   - Change 'C:\Users\[username]\Downloads\file-name.xls' to C:\Users\[username]\Downloads*.jpg to block all files with *.jpg extension.



Edit File Path

C:\Users\Administrator\Downloads*.exe

9. Click 'OK' in the 'Edit Property' dialog

10. Click 'OK' in the 'Advanced Settings' interface to save your settings

This will block browser downloads of the specific file type to your 'Downloads' folder. Repeat the process if other browsers on your system have a different download folder.

Note: Blocking files in this way will only block downloads of specific file types to specific folders. If you change the folder for browser downloads then the download will be allowed.

Tip:

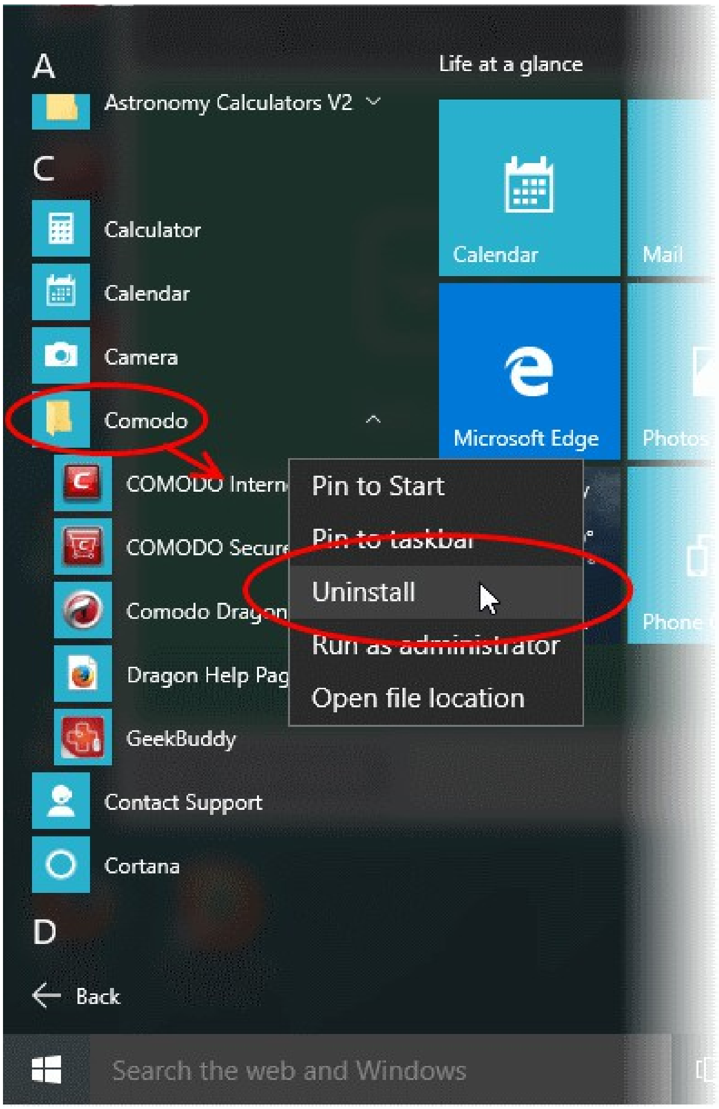
- To unblock future downloads, go to 'HIPS' > 'Protected Objects' > 'Blocked Files', select the file path, and choose 'Remove'.
- To unblock individual files, go to 'General Tasks' > 'Unblock Applications' and choose 'Unblock'.

Switch Between Complete CIS Suite and Individual Components (just AV or FW)

- Comodo Internet Security can be installed as a complete security suite or as individual components. You can choose what to install **during installation**.
- After installation, you can also add or remove components without having to uninstall the entire software.

To switch the installation type

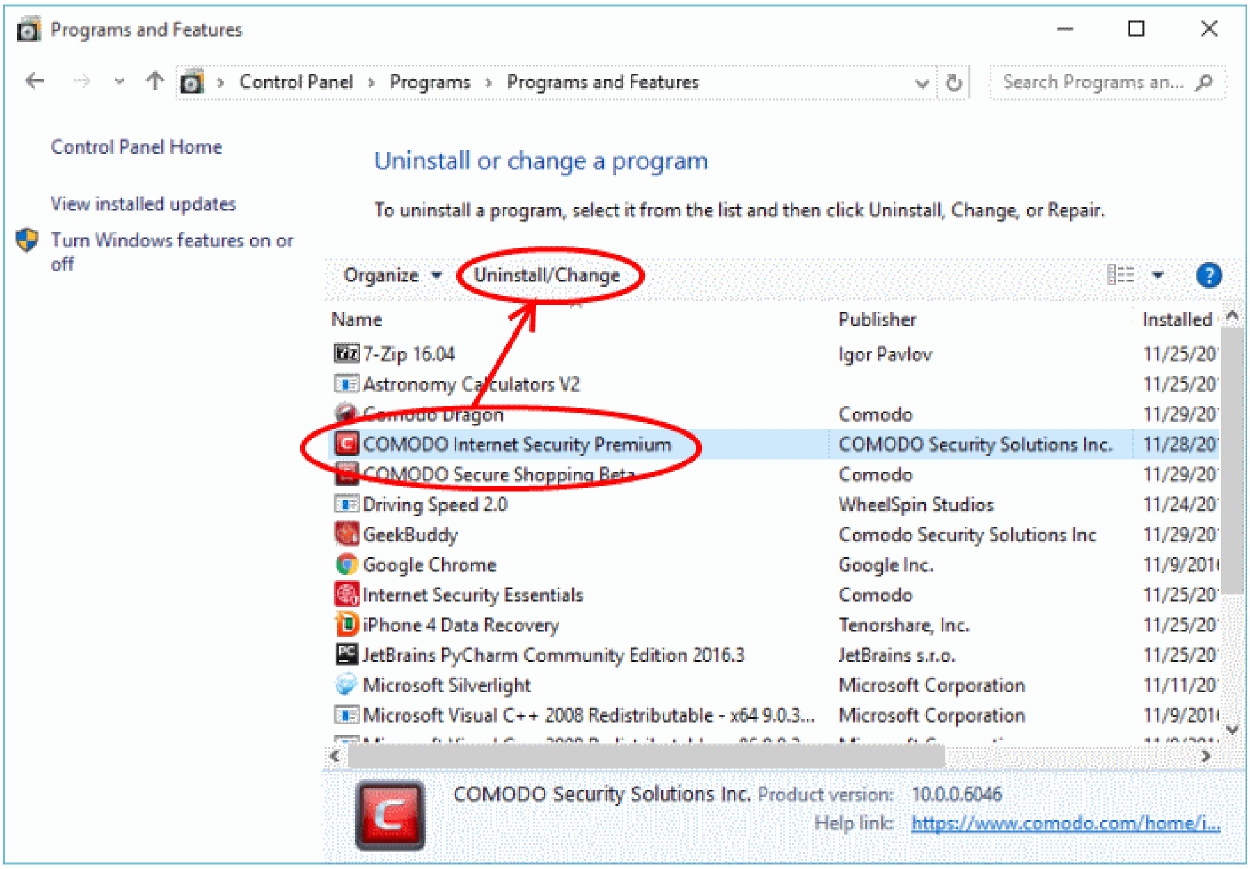
- Click 'Windows Home' button > 'All Apps' > 'Comodo' > 'COMODO Internet Security' > 'Uninstall'



OR

- Click 'Windows Start' button > 'Control Panel' > 'Programs > 'Programs and Features'

The 'Programs and Features' interface will open with a list of applications installed on your computer.



Uninstall or change a program

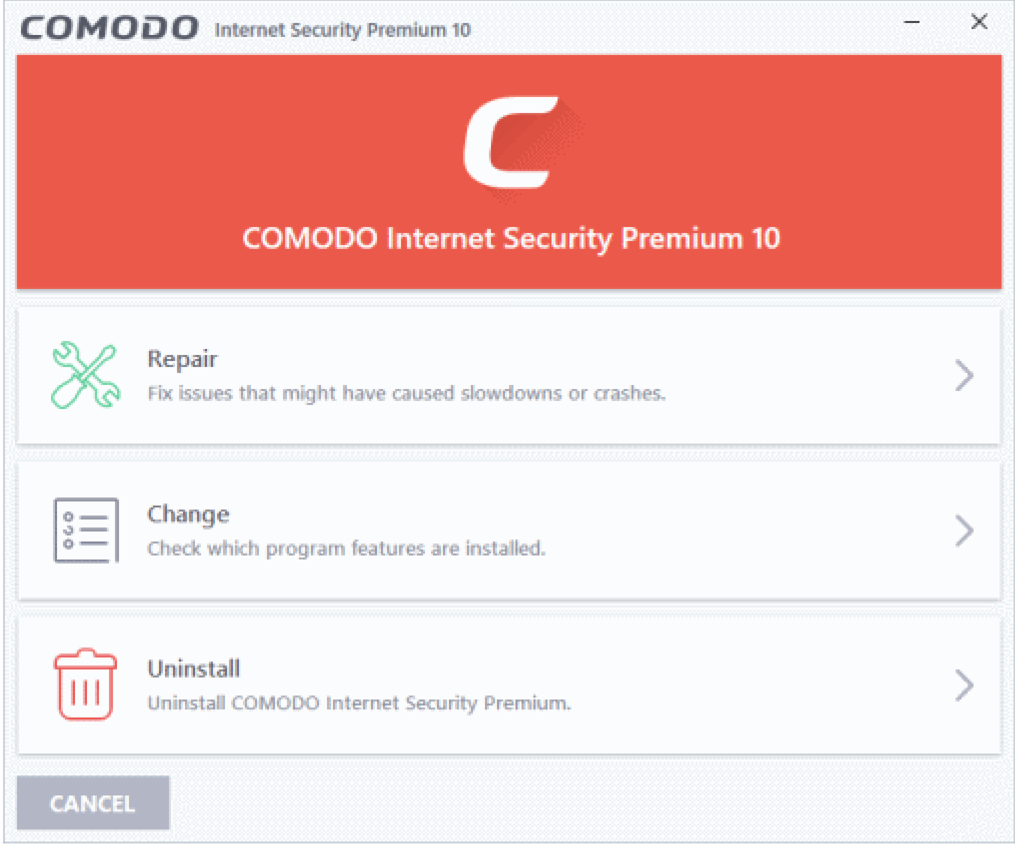
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed
7-Zip 16.04	Igor Pavlov	11/25/20
Astronomy Calculators V2		11/25/20
Comodo Dragon	Comodo	11/29/20
COMODO Internet Security Premium	COMODO Security Solutions Inc.	11/28/20
COMODO Secure Shopping Beta	Comodo	11/29/20
Driving Speed 2.0	WheelSpin Studios	11/24/20
GeekBuddy	Comodo Security Solutions Inc	11/29/20
Google Chrome	Google Inc.	11/9/201
Internet Security Essentials	Comodo	11/25/20
iPhone 4 Data Recovery	Tenorshare, Inc.	11/25/20
JetBrains PyCharm Community Edition 2016.3	JetBrains s.r.o.	11/25/20
Microsoft Silverlight	Microsoft Corporation	11/11/20
Microsoft Visual C++ 2008 Redistributable - x64 9.0.3...	Microsoft Corporation	11/9/201

COMODO Security Solutions Inc. Product version: 10.0.0.6046
Help link: https://www.comodo.com/home/i...

- Select 'Comodo Internet Security' and 'Uninstall/Change' from the top

The Configuration Wizard will start.



COMODO Internet Security Premium 10

COMODO Internet Security Premium 10

Repair

Fix issues that might have caused slowdowns or crashes.

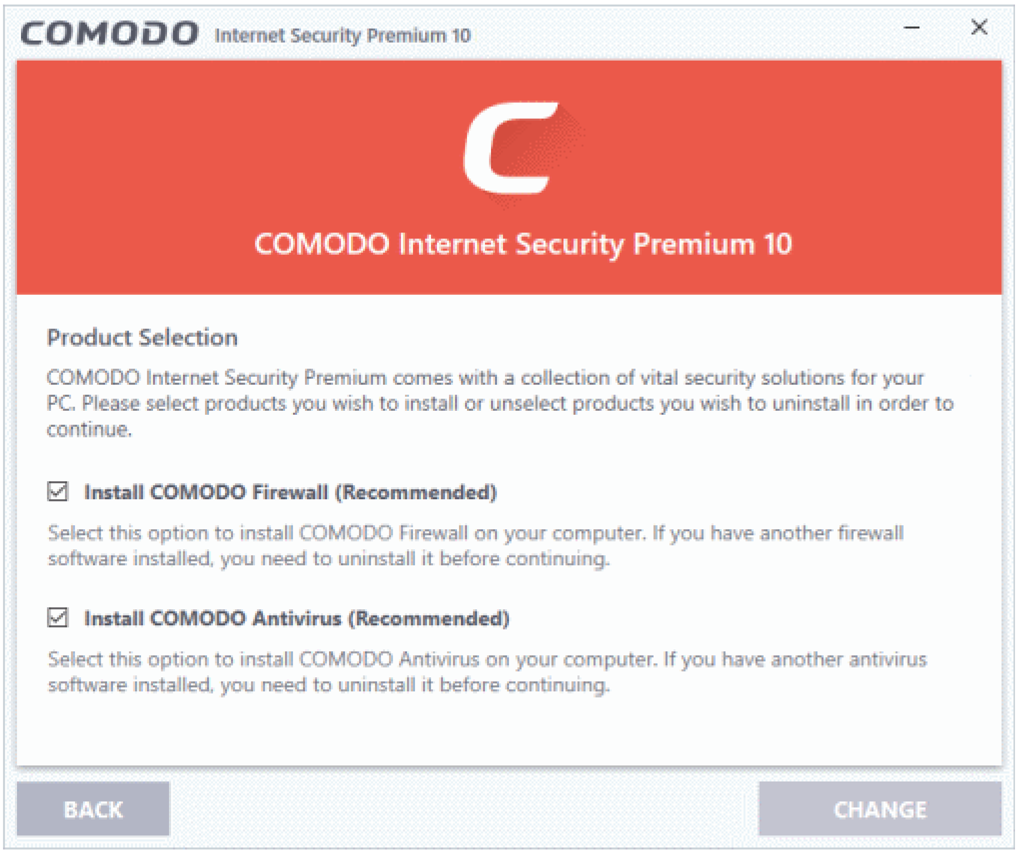
Change

Check which program features are installed.

Uninstall

Uninstall COMODO Internet Security Premium.

- Select 'Change' button to modify the installed features. The product selection screen will appear:



COMODO Internet Security Premium 10

COMODO Internet Security Premium 10

Product Selection

COMODO Internet Security Premium comes with a collection of vital security solutions for your PC. Please select products you wish to install or unselect products you wish to uninstall in order to continue.

☑ **Install COMODO Firewall (Recommended)**

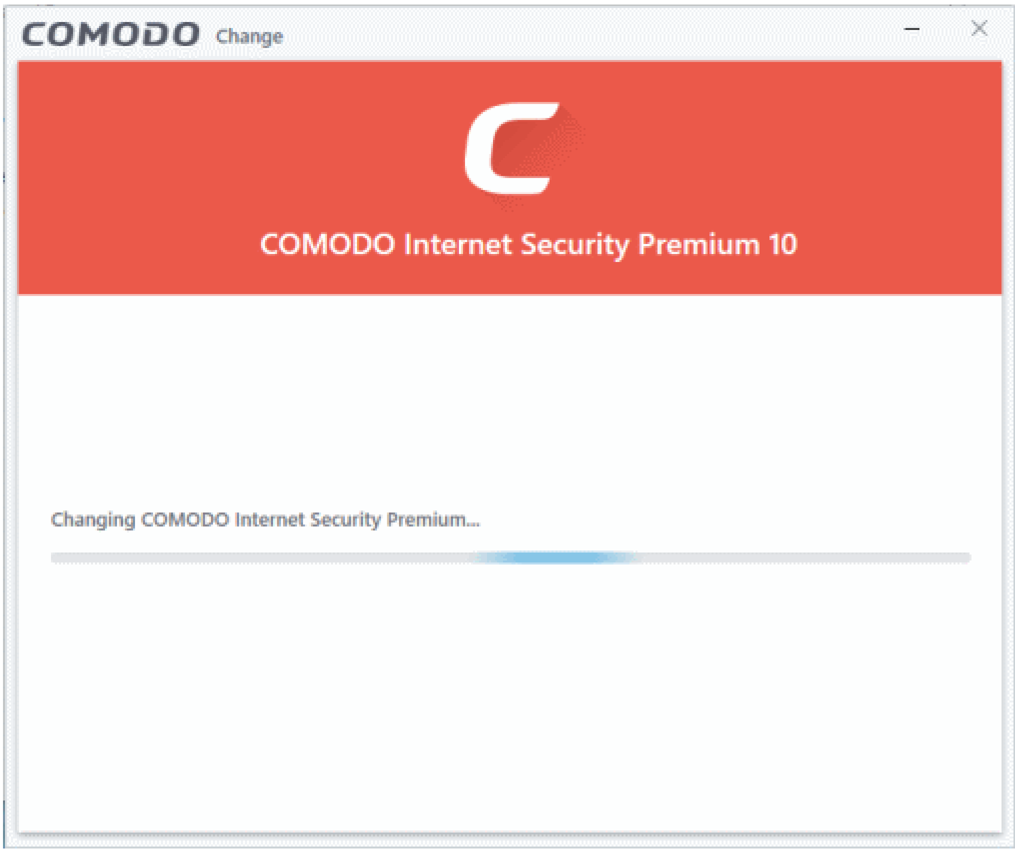
Select this option to install COMODO Firewall on your computer. If you have another firewall software installed, you need to uninstall it before continuing.

☑ **Install COMODO Antivirus (Recommended)**

Select this option to install COMODO Antivirus on your computer. If you have another antivirus software installed, you need to uninstall it before continuing.

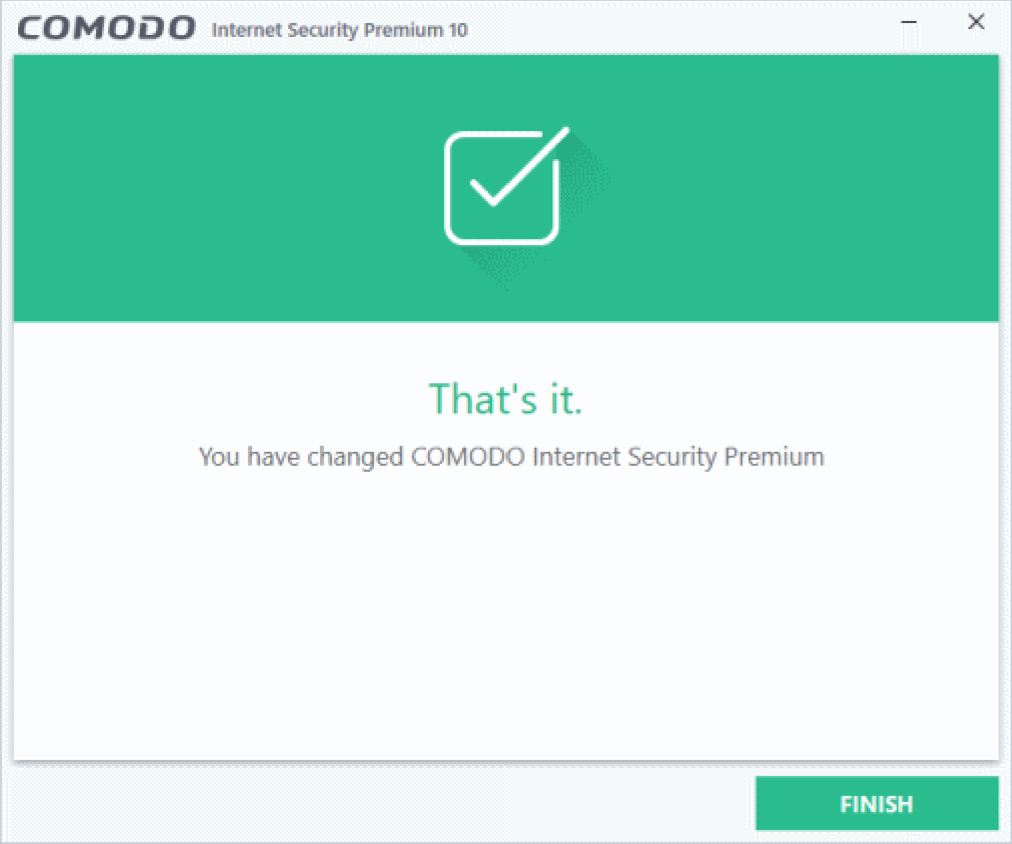
Select the installation type.

- If you want the complete installation, select both 'Install COMODO Antivirus' and 'Install COMODO Firewall'.
- If you only want the antivirus, clear the 'Install Comodo Firewall' box and ensure 'Install COMODO Antivirus' is selected.
- If you only want the firewall, clear the 'Install Comodo Antivirus' box and ensure 'Install COMODO Firewall' is selected.
- Click 'Change'. CIS will begin installing or uninstalling components as required.



Changing COMODO Internet Security Premium...

Click the 'Finish' button when the process is complete to exit the wizard.

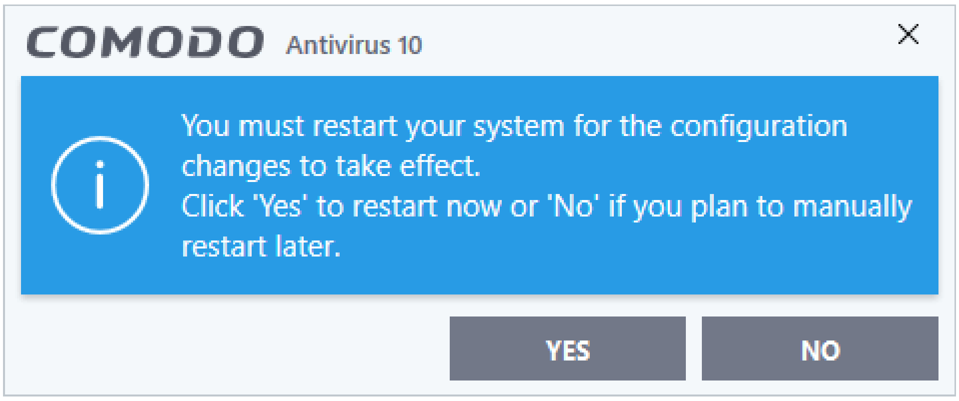


COMODO Internet Security Premium 10

That's it.

You have changed COMODO Internet Security Premium

Your computer needs to be restarted for the configuration change to take effect. A 'Restart Computer' dialog will be displayed.



COMODO Antivirus 10

You must restart your system for the configuration changes to take effect.
Click 'Yes' to restart now or 'No' if you plan to manually restart later.

- If you want to restart the system at a later time, click 'No'.
- If you want to restart the system immediately, please save any unsaved data and click 'Yes'.

Note: The change will take effect only on the next restart of the computer.

Switch Off Automatic Antivirus and Software Updates

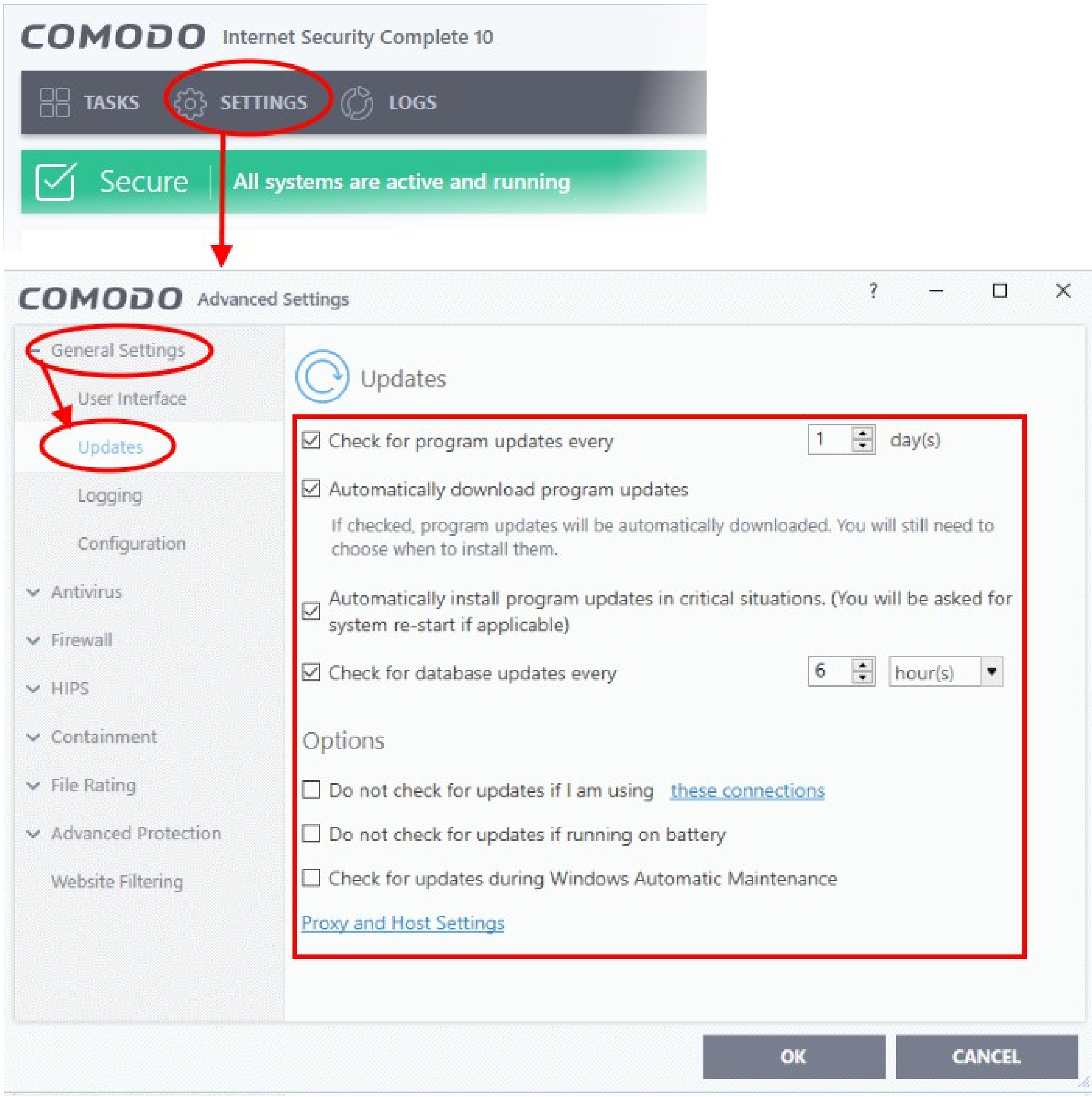
By default, Comodo Internet Security will automatically check for software and Antivirus database updates. However, some users like to have control over when the updates are downloaded. For example, network administrators may not wish to automatically download because it will take up to much bandwidth during the day. Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activities.

CIS provides full control over virus and software updates. Click the appropriate link below to find out more:

- **Switch off automatic software and virus signature database updates entirely**
- **Switch off automatic software and virus signature database selectively**
- **Switch off automatic virus signature database updates prior to Antivirus Scans**

To switch off automatic updates entirely:

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click 'Updates' under 'General Settings' on the left
3. Deselect the check boxes 'Check for program updates every xxx day(s)' and 'Check for database updates every xxx hour(s)'



Updates

☑ Check for program updates every 1 day(s)

☑ Automatically download program updates

If checked, program updates will be automatically downloaded. You will still need to choose when to install them.

☑ Automatically install program updates in critical situations. (You will be asked for system re-start if applicable)

☑ Check for database updates every 6 hour(s)

Options

☐ Do not check for updates if I am using these connections

☐ Do not check for updates if running on battery

☐ Check for updates during Windows Automatic Maintenance

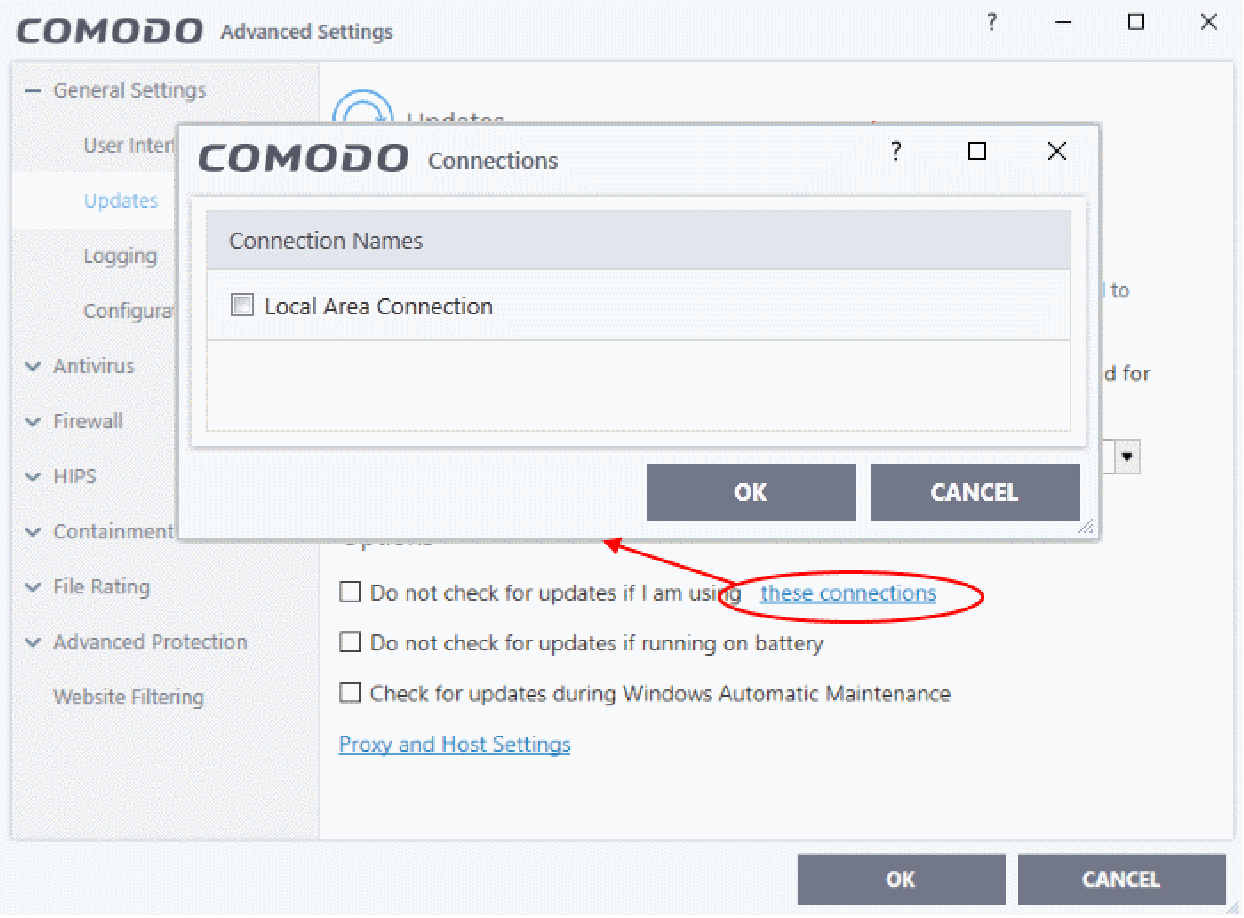
Proxy and Host Settings

4. Click 'OK' in the 'Advanced Settings' panel to save your changes.

To switch off automatic updates selectively:

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface

2. Click 'Updates' under 'General Settings' on the left



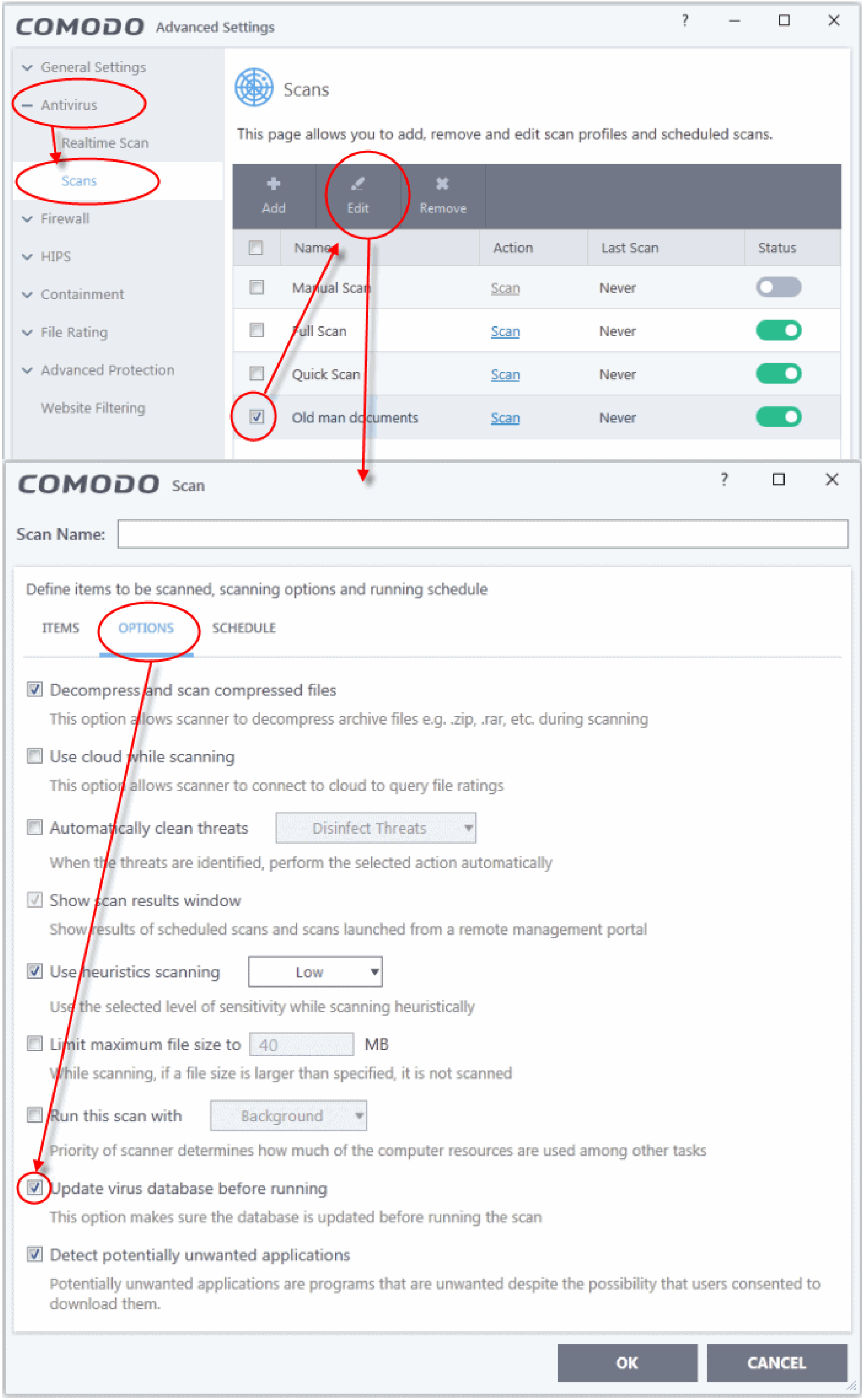
- If you want to suppress automatic updates when you are connected to internet through certain networks
    - Select the 'Do not check updates if am using these connections' check-box
    - Then click the 'these connections'. The 'Connections' dialog will appear with the list of connections you use.
    - Select the connection through which you do not want CIS to check for updates and click 'OK.'
- If you want to suppress automatic updates when your computer is running on battery
    - Select the 'Do not check for updates if running on battery' checkbox

To switch off automatic virus signature database updates prior to AV Scans:

1. Click 'Settings' at the top of the CIS home screen to open the 'Advanced Settings' interface
2. Click ' Antivirus' > 'Scans' on the left.

A list defined scan profiles will be displayed.

3. Select the scan profile for which you do want the automatic virus database updates prior to the scan



COMODO Advanced Settings

- General Settings
- Antivirus
  - Realtime Scan
  - Scans
- Firewall
- HIPS
- Containment
- File Rating
- Advanced Protection
- Website Filtering

Scans

This page allows you to add, remove and edit scan profiles and scheduled scans.

	Name	Action	Last Scan	Status
□	Manual Scan	Scan	Never	○
□	Full Scan	Scan	Never	●
□	Quick Scan	Scan	Never	●
☑	Old man documents	Scan	Never	●

COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

☑ Decompress and scan compressed files

This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

□ Use cloud while scanning

This option allows scanner to connect to cloud to query file ratings

□ Automatically clean threats Disinfect Threats

When the threats are identified, perform the selected action automatically

☑ Show scan results window

Show results of scheduled scans and scans launched from a remote management portal

☑ Use heuristics scanning Low

Use the selected level of sensitivity while scanning heuristically

□ Limit maximum file size to 40 MB

While scanning, if a file size is larger than specified, it is not scanned

□ Run this scan with Background

Priority of scanner determines how much of the computer resources are used among other tasks

☑ Update virus database before running

This option makes sure the database is updated before running the scan

☑ Detect potentially unwanted applications

Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download them.

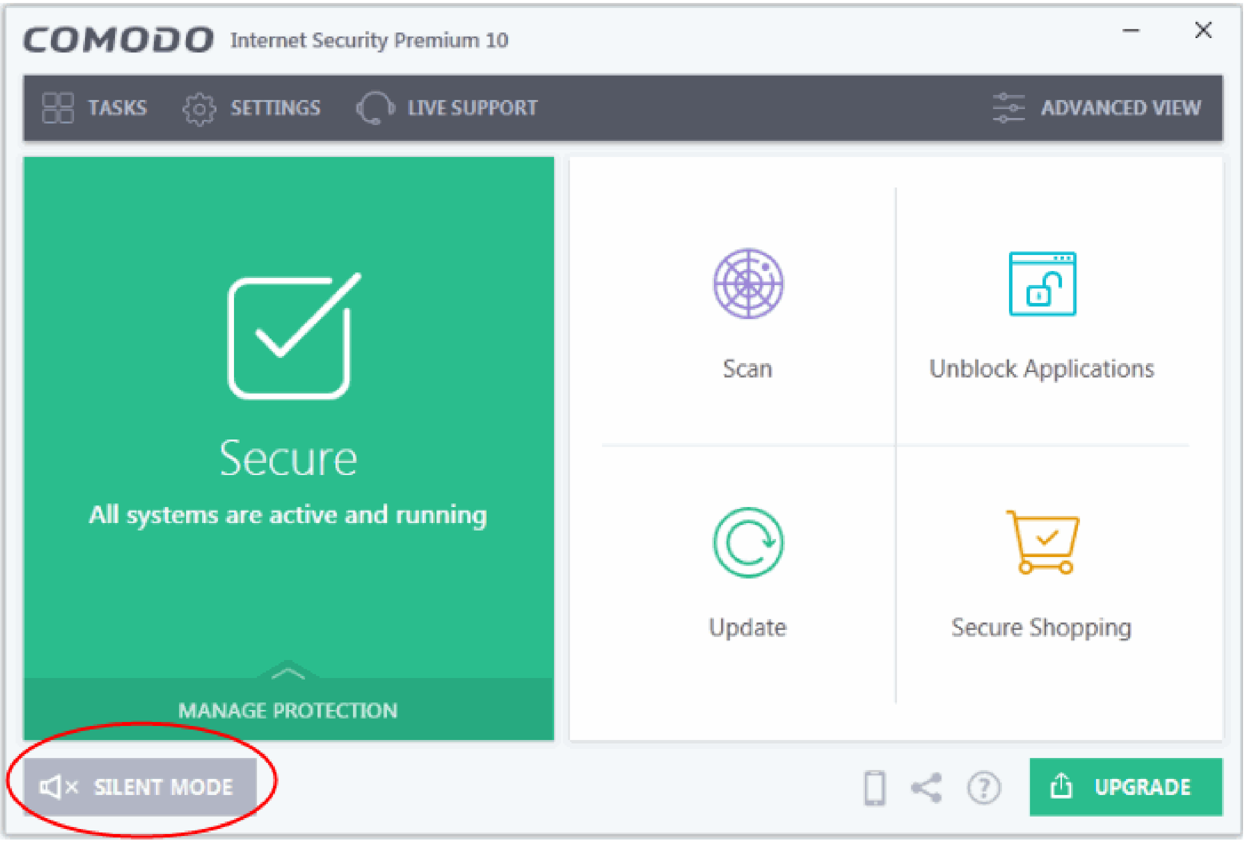
4. Click 'Edit' from the options at the top
5. Click 'Options' to open the 'Options' pane, scroll down and deselect 'Update virus database before running' checkbox.
6. Click 'OK' on the 'Scans' interface.
7. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

Suppress CIS Alerts Temporarily while Playing Games

- CIS generates alerts if it discovers a potential security threat and also shows alerts for general system messages.
- 'Silent mode' lets you temporarily disable alerts so they don't interrupt you while playing a game or running a presentation/product demo etc.
- During this time, operations that can interfere with the user experience are either suppressed or postponed. All protection components are still 100% active in silent mode.

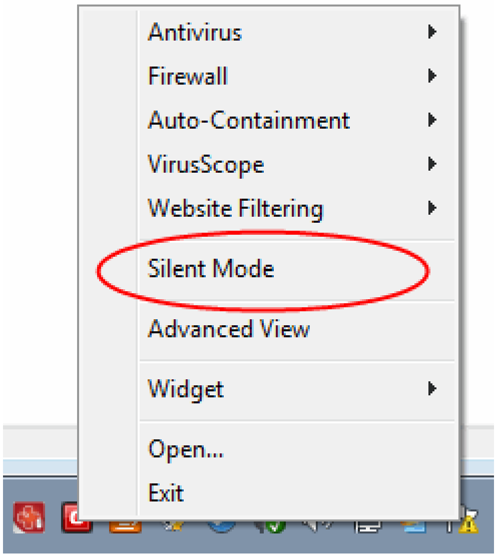
To temporarily stop pop-up alerts

- Click 'Silent Mode' button from CIS Home screen



OR

- Right click on the CIS System Tray icon and select 'Silent Mode' from the options.

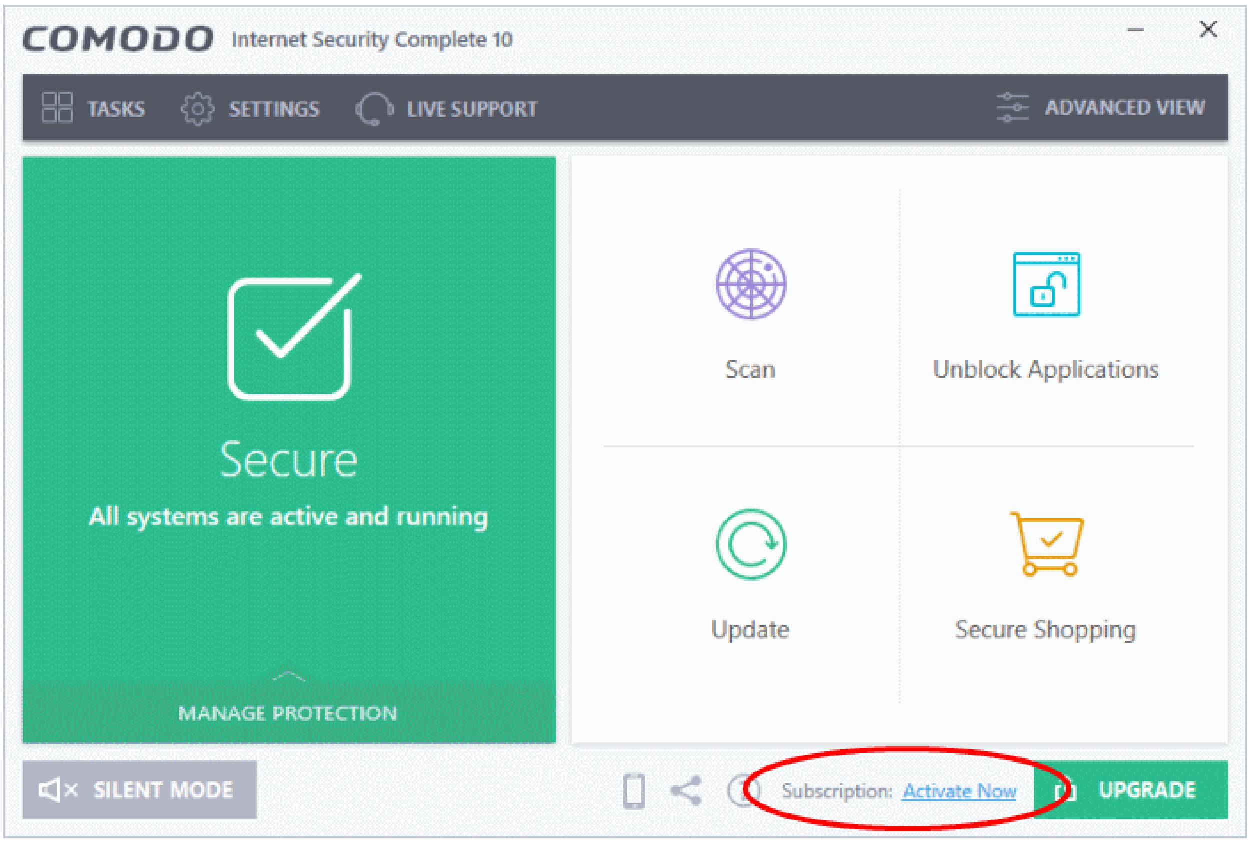


The alerts are now suppressed. To resume alerts and scheduled scans, just de-activate Silent Mode from the Home screen or the system tray icon right click options.

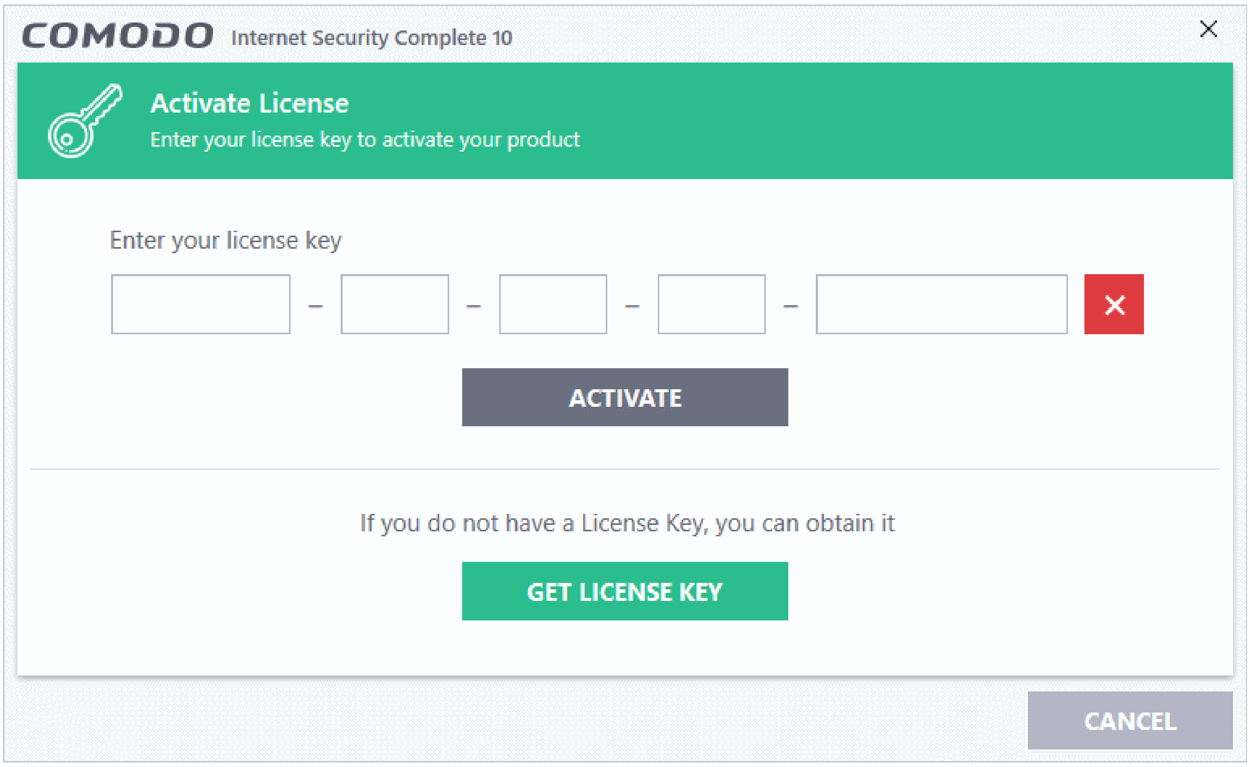
Renew or Upgrade your License

In order to enjoy continued protection from Comodo Internet Security, you will need to renew your license when it is due to expire.

- To renew or upgrade your license, click the 'Activate Now' link on the CIS home screen (alternatively, click 'No. of days left').



The 'Product Activation Wizard' will start.



COMODO Internet Security Complete 10
Activate License
Enter your license key to activate your product
Enter your license key
ACTIVATE
If you do not have a License Key, you can obtain it
GET LICENSE KEY
CANCEL

- Click the 'Get License Key'. You will be taken to the purchase page at **https://secure.comodo.com/home/purchase.php?afl=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDlDNDE4MzBDQjc1NDlENUlzRkY&lid=&**
- Select your CIS Package.
- Select 'Existing Comodo User' checkbox in 'Enter Customer Details' area, enter your login and password and complete the payment procedure.
- The License key will be sent to you by email. Enter the license key and click the 'Activate' button.
- After successful validation, your subscription will be activated and a confirmation screen will be displayed.

If you are renewing a license for the same CIS product then entering the license key will upgrade the license without requiring re-installation. If you are upgrading license types, then installation of the new product type will begin automatically. You may need to restart your computer to finalize the upgrade.

If you are using any of the trial versions of CIS, you have to purchase the license at the end of trial period in order to continue using the product. An alert will be displayed after the expiry of trial period.

- Click the 'Renew Now' button in the alert screen and follow the same purchase and activation procedure explained above.

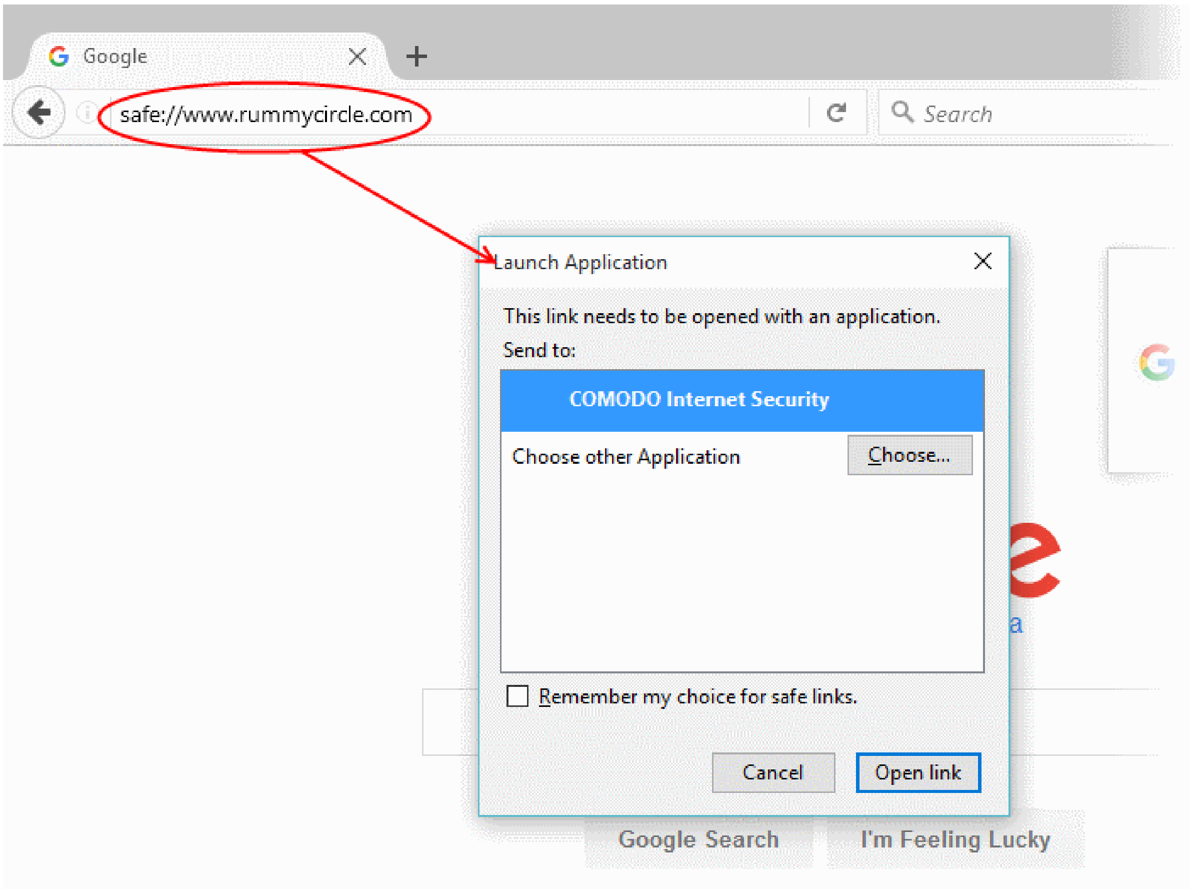
Use CIS Protocol Handlers

COMODO Internet Security has its own protocol handlers that allow you to perform certain tasks from a web page. Example tasks include opening a web page in a contained browser or starting a virus database update. CIS supports the protocol handlers listed below:

1 - safe://

Type 'safe://' before any web address to open the website inside the container.

For example: Try *safe://www .rummycircle.com*



Launch Application

This link needs to be opened with an application.

Send to:

COMODO Internet Security

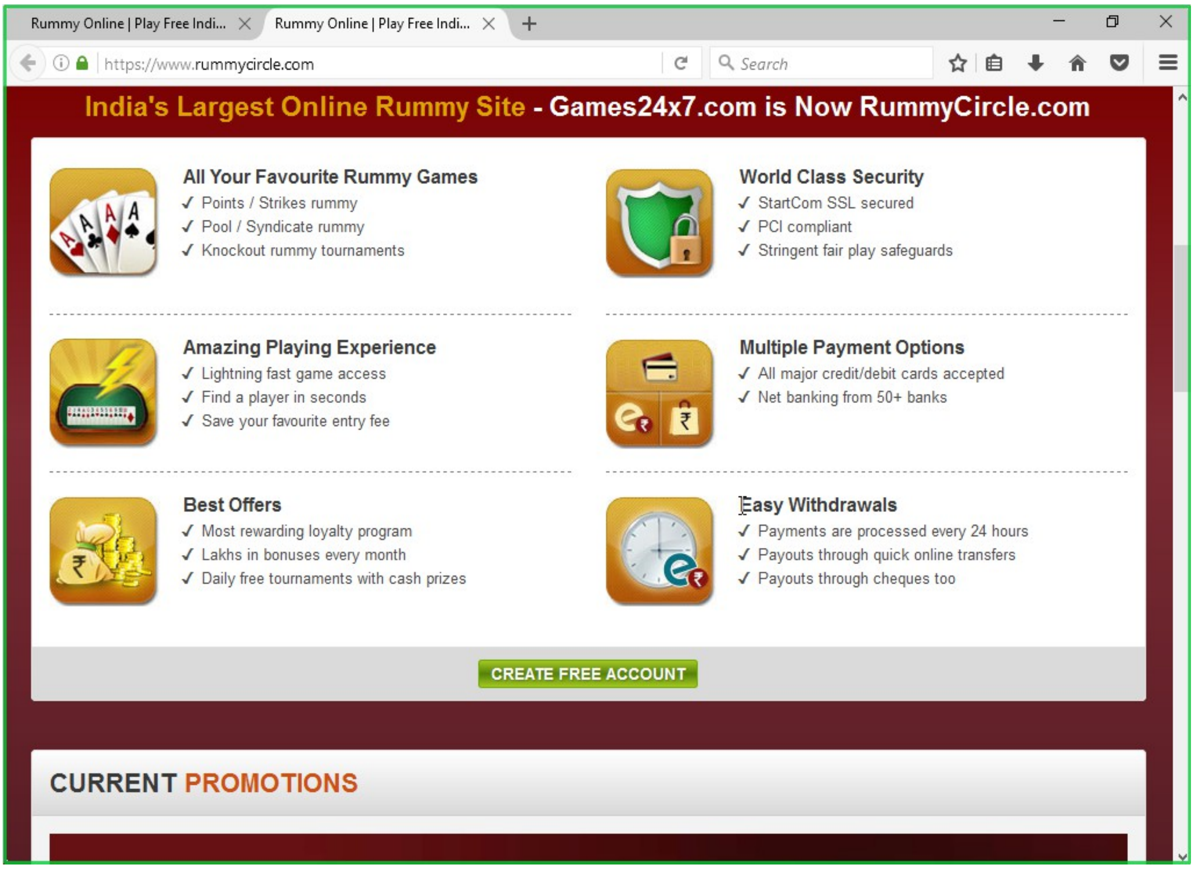
Choose other Application — Choose...

☐ Remember my choice for safe links.

Cancel | Open link

- Allow the application

The URL will be open in a contained browser. Note the green border:


Rummy Online | Play Free Indi...
Rummy Online | Play Free Indi...
https://www.rummycircle.com
Search
CREATE FREE ACCOUNT

India's Largest Online Rummy Site - Games24x7.com is Now RummyCircle.com

All Your Favourite Rummy Games
- ✓ Points / Strikes rummy
- ✓ Pool / Syndicate rummy
- ✓ Knockout rummy tournaments

World Class Security
- ✓ StartCom SSL secured
- ✓ PCI compliant
- ✓ Stringent fair play safeguards

Amazing Playing Experience
- ✓ Lightning fast game access
- ✓ Find a player in seconds
- ✓ Save your favourite entry fee

Multiple Payment Options
- ✓ All major credit/debit cards accepted
- ✓ Net banking from 50+ banks

Best Offers
- ✓ Most rewarding loyalty program
- ✓ Lakhs in bonuses every month
- ✓ Daily free tournaments with cash prizes

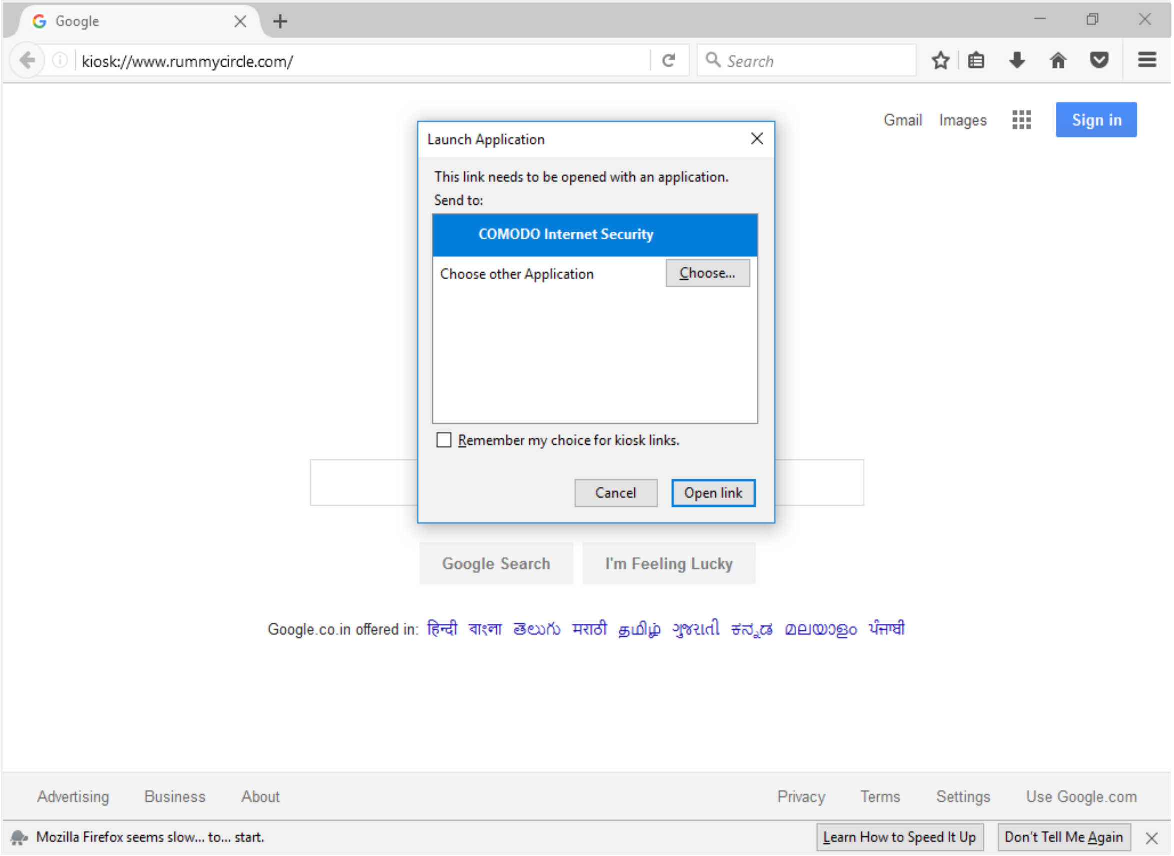
Easy Withdrawals
- ✓ Payments are processed every 24 hours
- ✓ Payouts through quick online transfers
- ✓ Payouts through cheques too

CURRENT PROMOTIONS

2 - kiosk://

Type 'kiosk://' before any web address to open the website in the Virtual Desktop.

E.g. Try *kiosk://wwww.rummycircle.com*



Launch Application

This link needs to be opened with an application.

Send to:

COMODO Internet Security

Choose other Application — Choose...

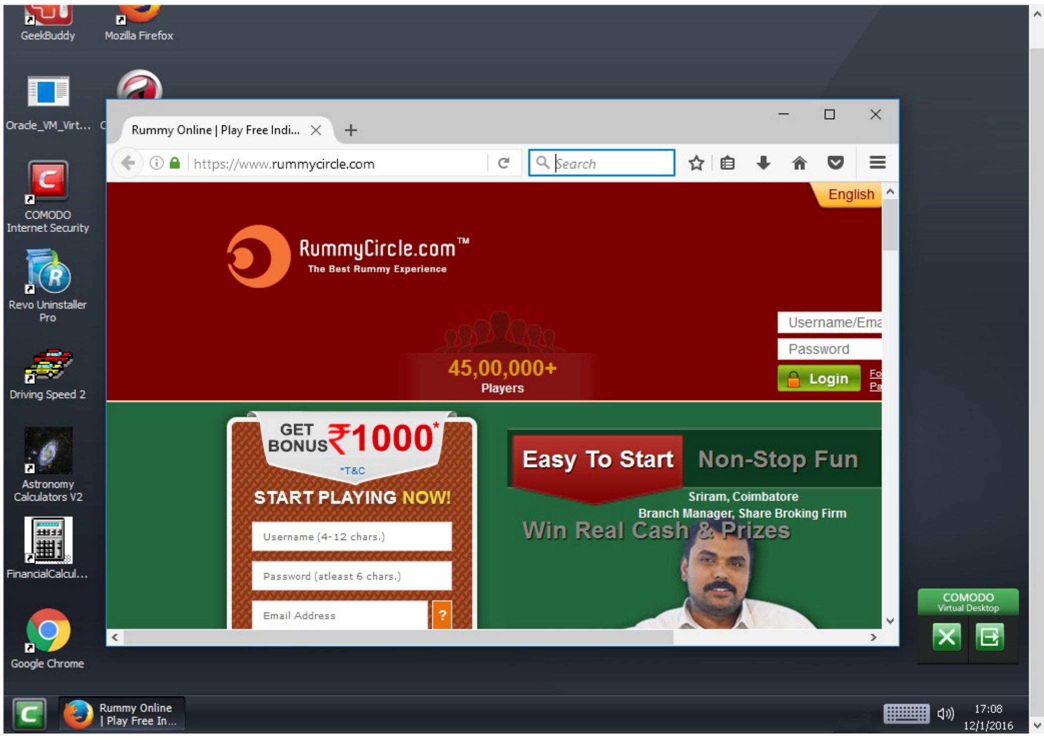
□ Remember my choice for kiosk links.

Cancel — Open link

Mozilla Firefox seems slow... to... start. — Learn How to Speed It Up — Don't Tell Me Again

- Allow the application

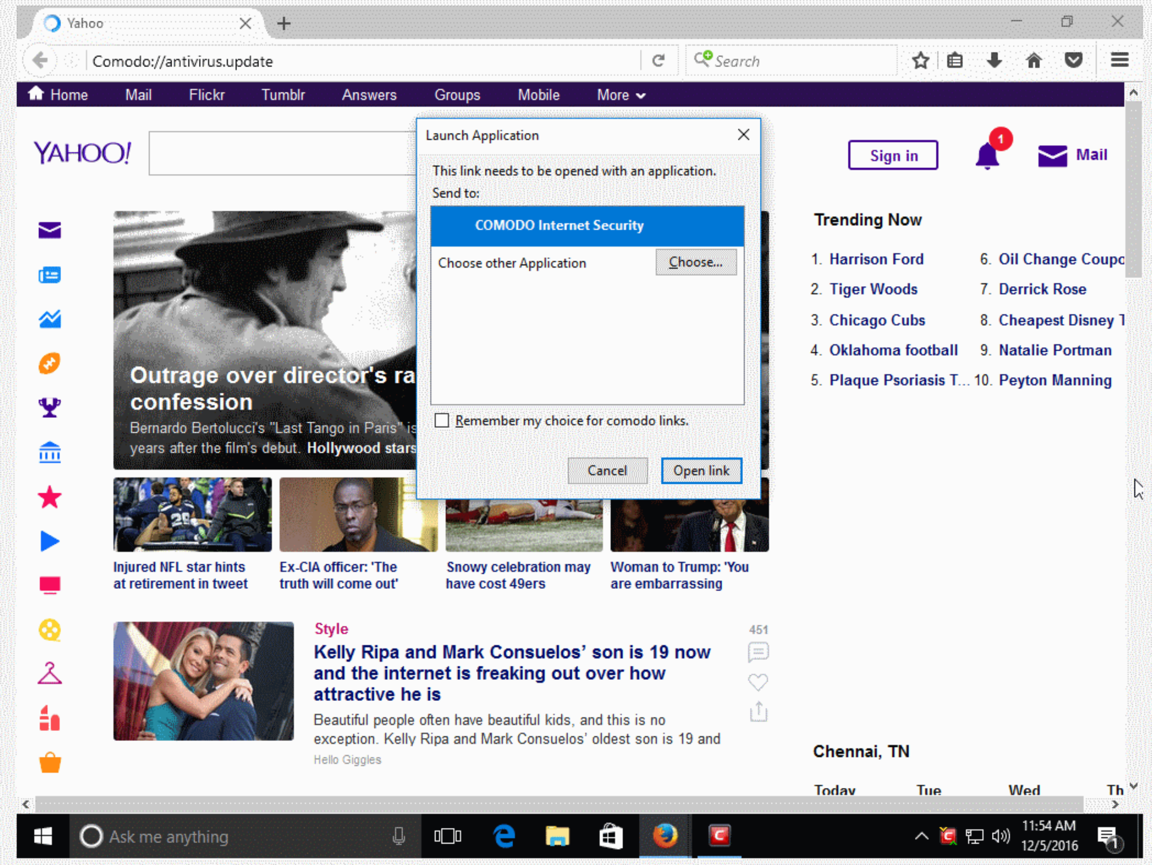
The webpage will be displayed in a browser inside the Comodo Virtual Desktop:



3 - Comodo://

Type 'Comodo://' before the command line parameter for the action to be executed. Refer to the table below for more details.

For example *Comodo://antivirus.update*



Comodo://antivirus.update

Launch Application

This link needs to be opened with an application.

Send to:

COMODO Internet Security

Choose other Application

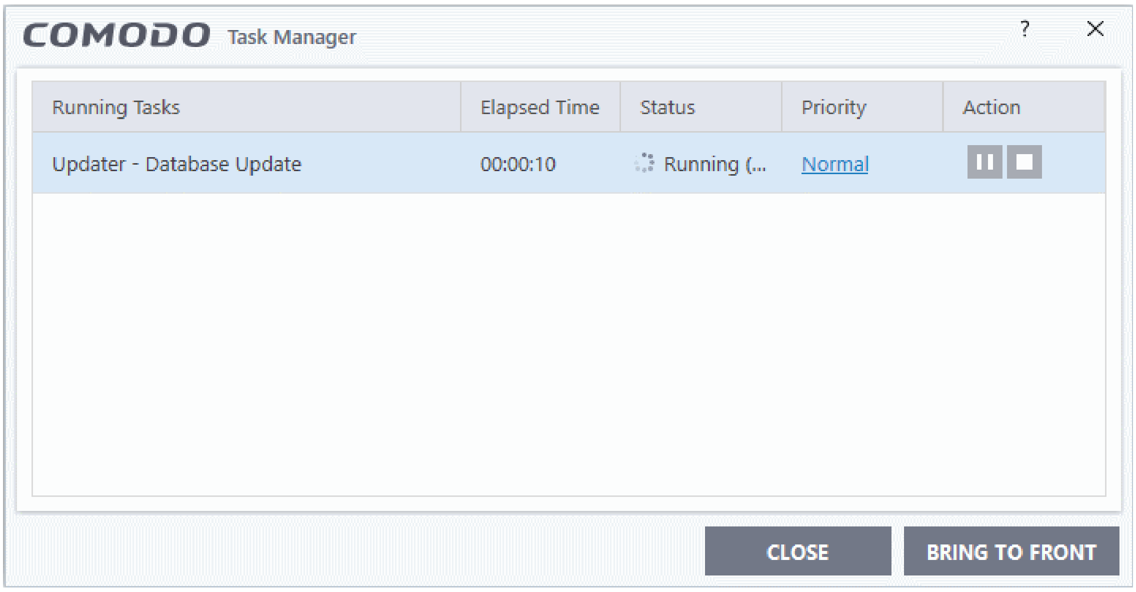
☐ Remember my choice for comodo links.

Yahoo
Search
Home
Mail
Flickr
Tumblr
Answers
Groups
Mobile
More
YAHOO!
Choose...
Cancel
Open link
Sign in
Mail
Trending Now
Outrage over director's ra confession
Injured NFL star hints at retirement in tweet
Ex-CIA officer: 'The truth will come out'
Snowy celebration may have cost 49ers
Woman to Trump: 'You are embarrassing
Style
Kelly Ripa and Mark Consuelos' son is 19 now and the internet is freaking out over how attractive he is
Chennai, TN
Ask me anything
11:54 AM
12/5/2016

- Click 'Open link'

The 'Antivirus' update will run in the background

If you want to view the update progress then click 'Task' > 'Advanced Tasks'> then choose 'Open Task Manager'



COMODO Task Manager

Running Tasks	Elapsed Time	Status	Priority	Action
Updater - Database Update	00:00:10	Running (...	Normal	

The following is a list of all possible commands. Commands can be entered into any browser address bar.

Command	Description
safe:<URL>	Runs the target website in the container.
safe:<path>	Runs the target application in the container.
kiosk:<URL>	Runs the target website in the virtual kiosk.
kiosk:<path>	Runs the target application in the virtual kiosk.
comodo://antivirus.Update	Updates the virus and web-filtering databases.
comodo://antivirus.Scan?predefined=Quick	Runs a quick antivirus scan.
comodo://antivirus.Scan?predefined=Full	Runs a full antivirus scan.
comodo://antivirus.Scan?path=<Path>	Scan a specific file or folder.
comodo://antivirus.ImportAvdb?path=<Path>	Import an AV database from a specific location.
comodo://urlfilter.continue? token=<token>&action=<once|exclude|falsepositive>	Internal command for URL filtering feature.

Configure Secure Shopping

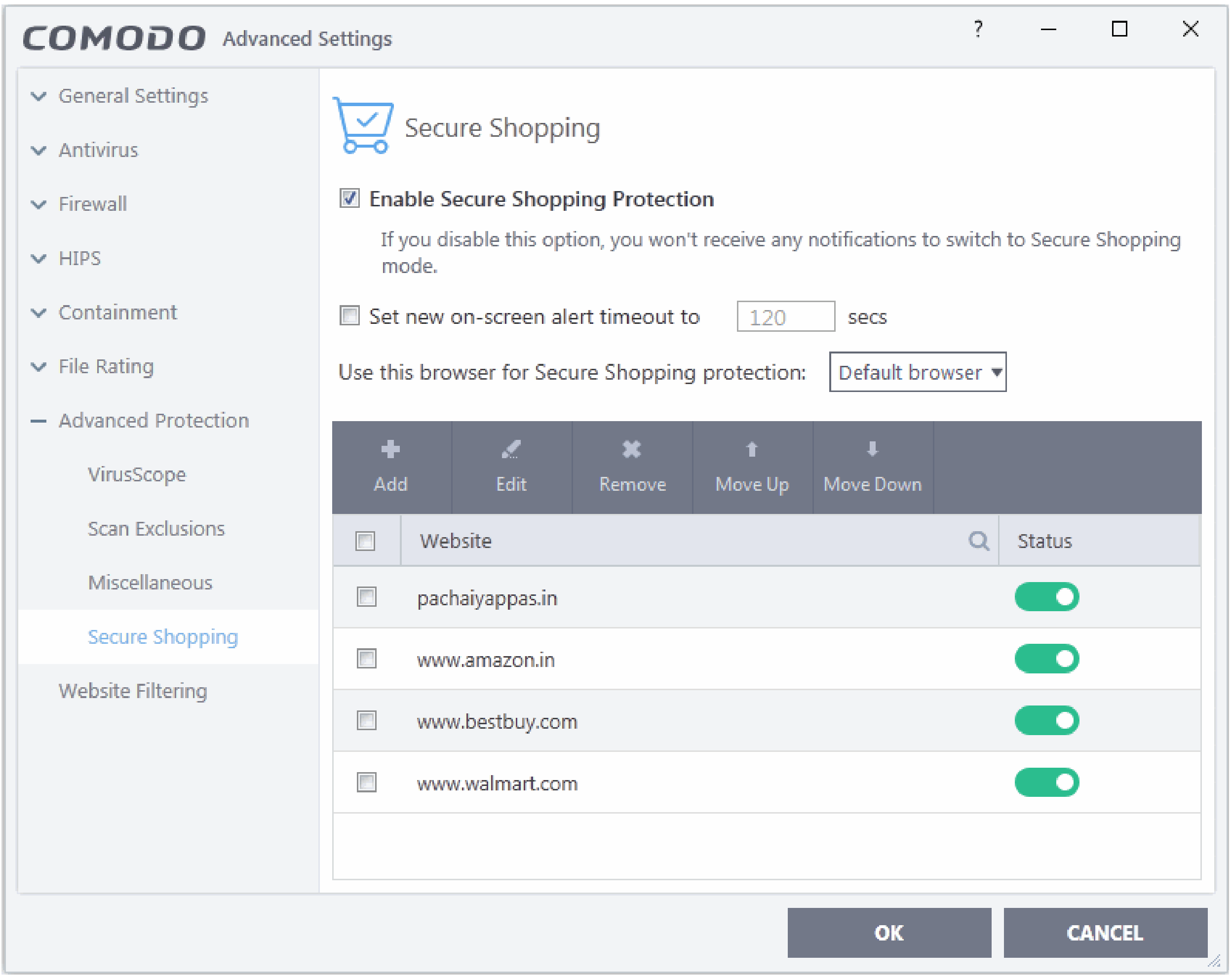
- Comodo Secure Shopping provides unbeatable security for online banking and shopping sessions by ensuring you connect to those websites from within a dedicated, security-hardened browsing environment.
- You also have the option to create alerts when you visit certain sites, so you can choose whether or not to open the site in the secure environment.

In addition to websites and browsers, you can also run any 'regular' application inside Secure Shopping. This is especially valuable for applications that process sensitive data, such as:

- Email applications like Outlook and Thunderbird
- Accounting software like Tally and Sage
- Password managers
- Spreadsheet software like Excel and Open Office Calc
- FTP and VPN clients
- Instant messaging and chat applications
- File sharing clients like Drop Box

To configure Secure Shopping

- Click 'Settings' on the menu bar to open the 'Advanced Settings' interface
- Click 'Advanced Protection' then 'Secure Shopping' on the left



Secure Shopping

☑ Enable Secure Shopping Protection

If you disable this option, you won't receive any notifications to switch to Secure Shopping mode.

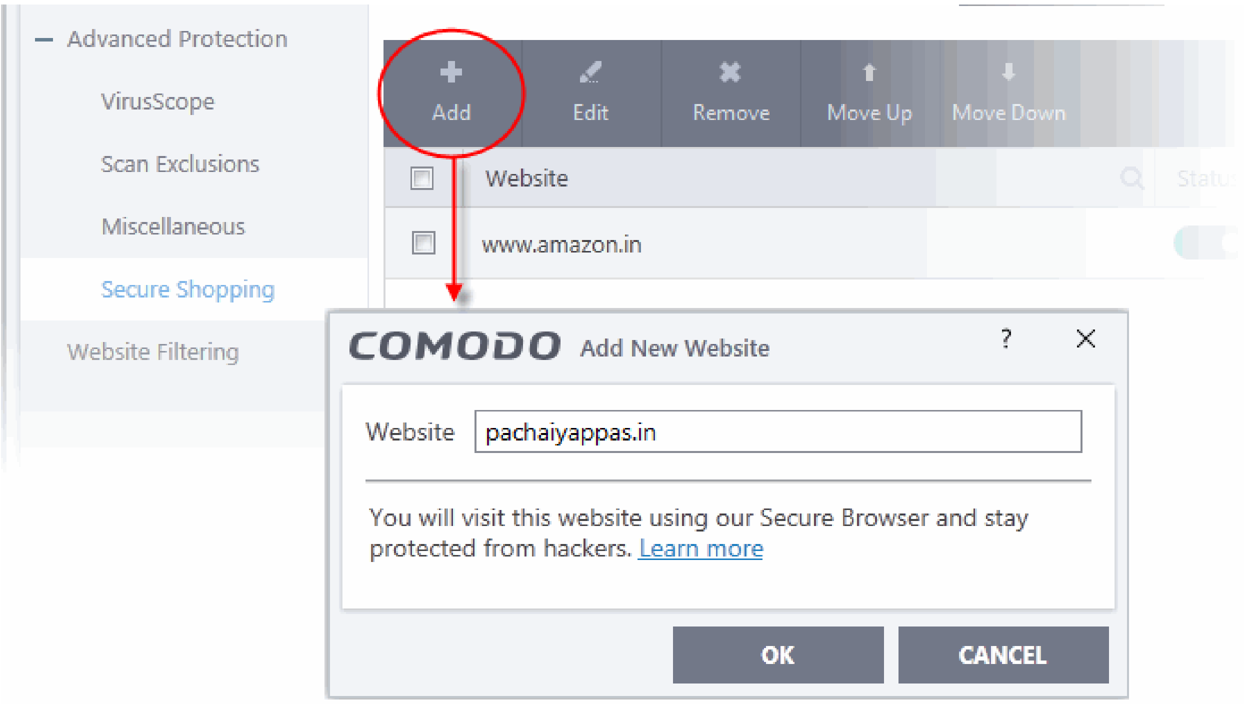
□ Set new on-screen alert timeout to 120 secs

Use this browser for Secure Shopping protection: Default browser

Website	Status
pachaiyappas.in	●
www.amazon.in	●
www.bestbuy.com	●
www.walmart.com	●

To add websites for Secure Shopping Protection

- Click the 'Add' button then enter the name of your website.

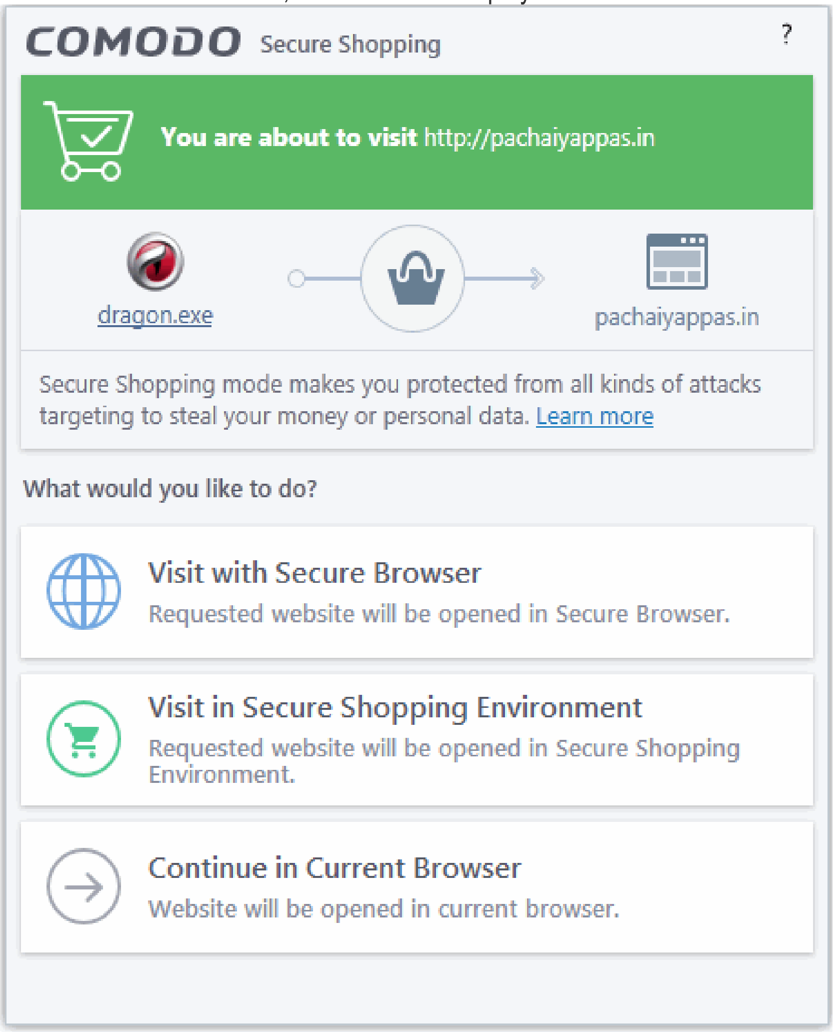


Website: pachaiyappas.in

You will visit this website using our Secure Browser and stay protected from hackers. Learn more

- Click 'OK' to add the website to the list. Repeat the process to add more websites
- To edit the settings for a website, select the website and click 'Edit'. The Edit Website dialog will appear, similar to the Add New Website dialog. Edit the parameters as required and click 'OK'.
- To remove a website, select it and click 'Remove'.
- Click 'OK' in the 'Advanced Settings' interface to save your changes.

Whenever you visit a website added to the list, an alert will be displayed as shown below:



COMODO Secure Shopping

You are about to visit http://pachaiyappas.in

Secure Shopping mode makes you protected from all kinds of attacks targeting to steal your money or personal data. Learn more

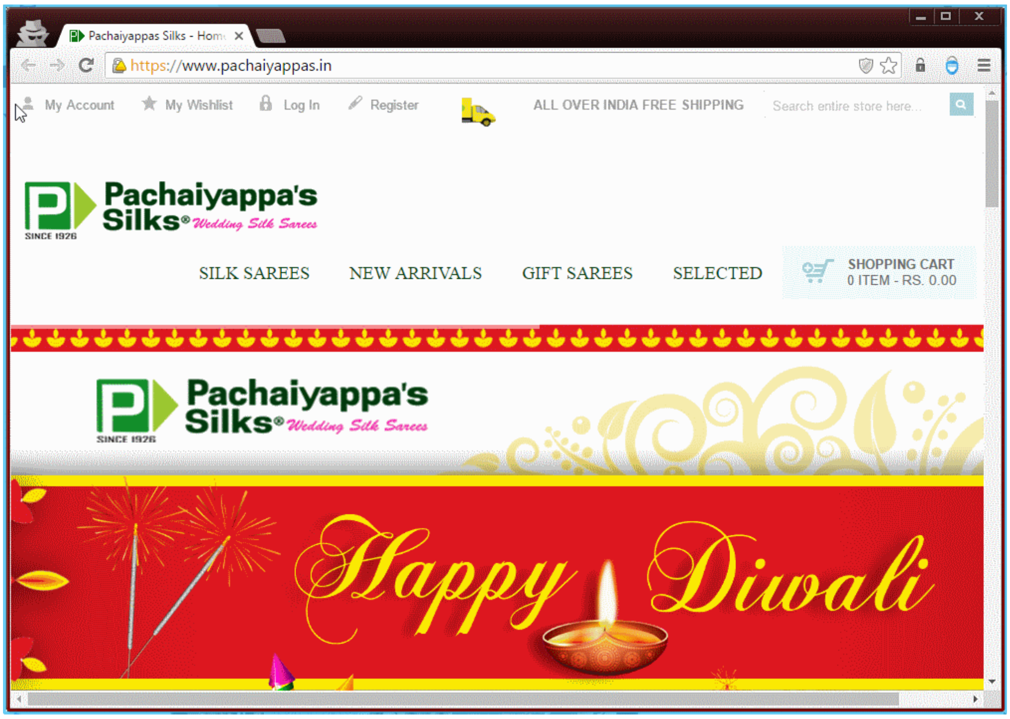
What would you like to do?

Visit with Secure Browser
Requested website will be opened in Secure Browser.

Visit in Secure Shopping Environment
Requested website will be opened in Secure Shopping Environment.

Continue in Current Browser
Website will be opened in current browser.

- You can choose how you want to proceed with the website, from the alert.
    - **Visit with Secure Browser -** The website will be opened in a new secure shopping browser window in incognito/private mode. Your browsing history will be immediately deleted on completion of your browsing session, including cookies which might be installed by the website. The browser window have a blue border around it:


Pachaiyappas Silks - Home
https://www.pachaiyappas.in
My Account
My Wishlist
Log In
Register
ALL OVER INDIA FREE SHIPPING
Search entire store here...
Pachaiyappa's Silks® Wedding Silk Sarees
SINCE 1926
SILK SAREES
NEW ARRIVALS
GIFT SAREES
SELECTED
SHOPPING CART
0 ITEM - RS. 0.00
Happy Diwali

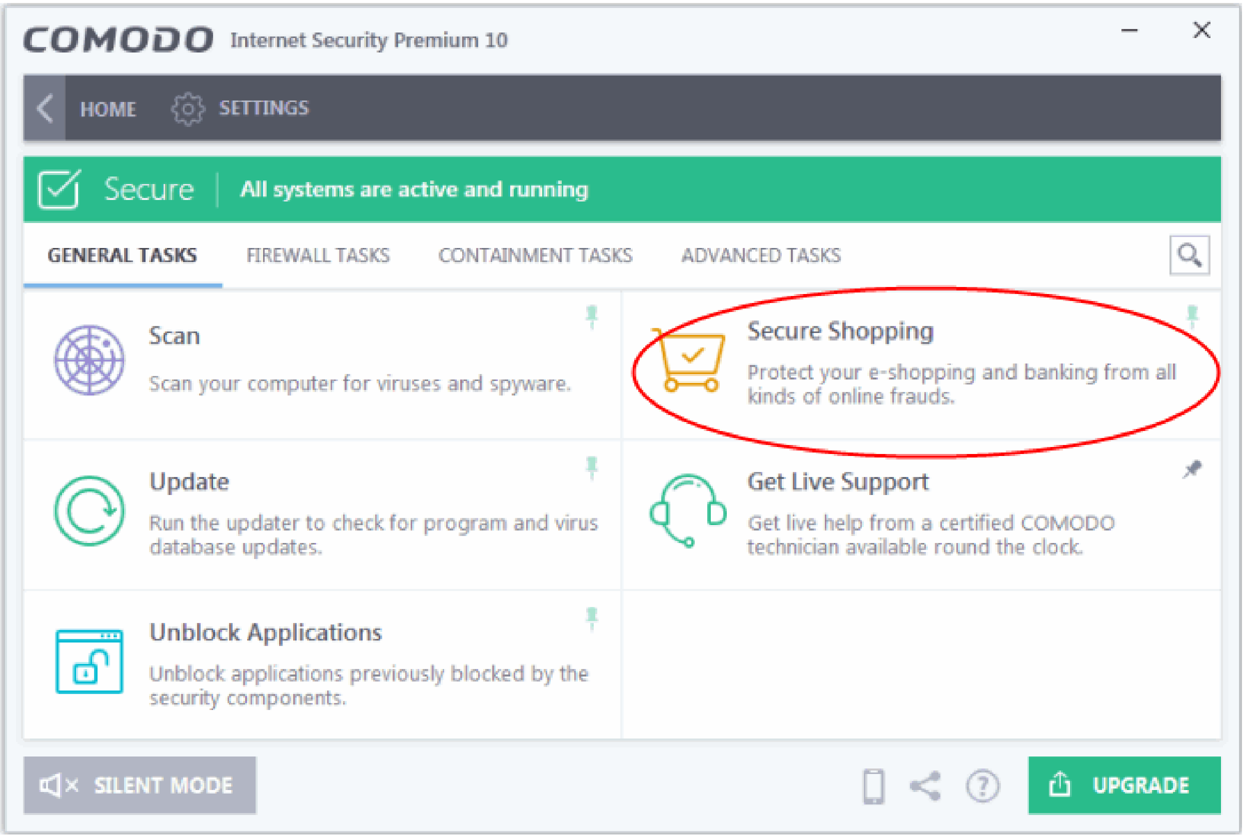
- **Visit in Secure Shopping Environment -** The website will be opened in a security hardened, virtual environment. When inside this environment, your browser cannot be accessed or potentially attacked by other processes running on your computer. The environment also features a virtual keyboard which allows you to enter confidential information without fear of your keystrokes being tracked. See **Using Comodo Secure Shopping Enviroment**, for more details on the Secure Shopping Environment.
- **Continue in Current Browser -** Allows you to continue your browsing activities with the same browser through which the website was opened.

Using Comodo Secure Shopping Environment

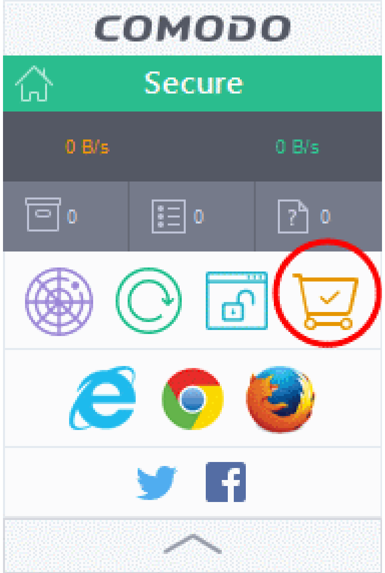
The Secure Shopping environment automatically opens when you choose 'Visit in Secure Shopping Environment' in the Secure Shopping alert.

You can manually open the Secure Shopping environment in the following ways:

- From the CIS Home Screen - Click 'Tasks' > 'General Tasks' > 'Secure Shopping'

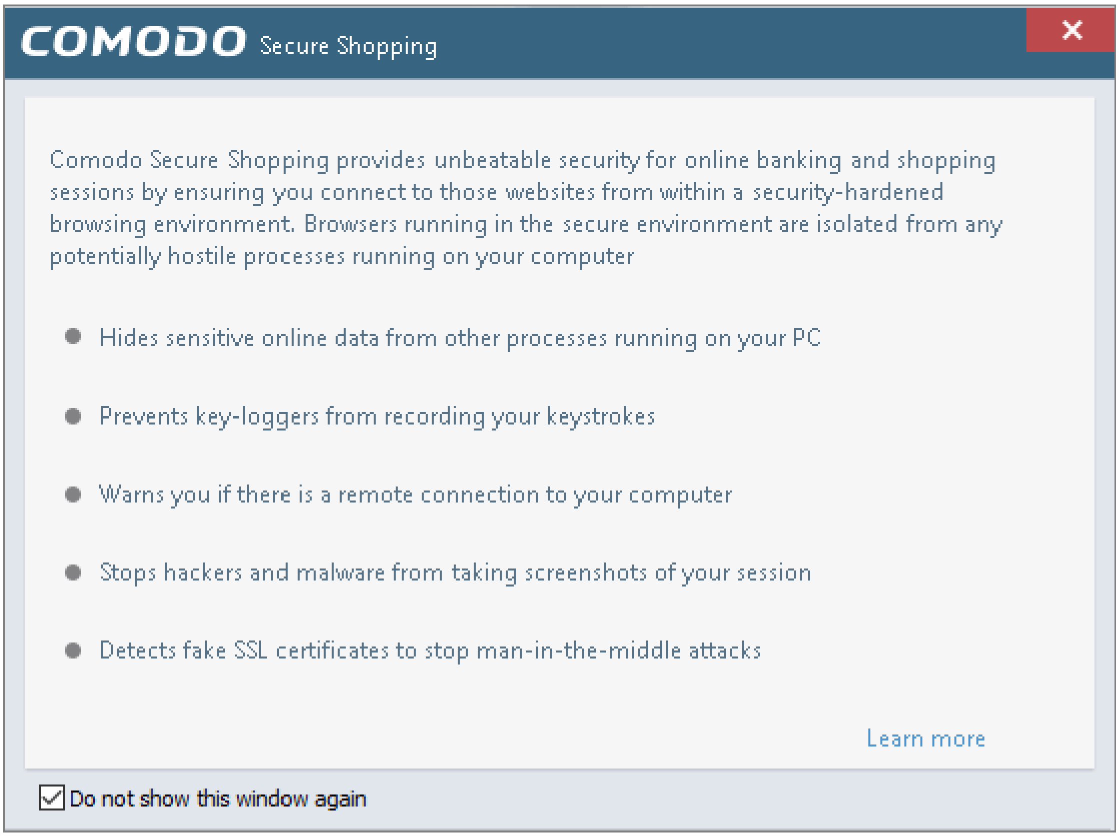

COMODO Internet Security Premium 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
CONTAINMENT TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
SILENT MODE
UPGRADE

- From the CIS Desktop Widget - Click the 'Secure Shopping' icon from the CIS Desktop widget



- From the Windows Start menu - Click Windows Start/Home > All Programs > Comodo > Comodo Secure Shopping
- From the Windows Desktop icon - Double-click the 'Comodo Secure Shopping' shortcut on the desktop

When you start the application, a welcome screen will appear which explains the benefits of secure shopping:



Comodo Secure Shopping provides unbeatable security for online banking and shopping sessions by ensuring you connect to those websites from within a security-hardened browsing environment. Browsers running in the secure environment are isolated from any potentially hostile processes running on your computer

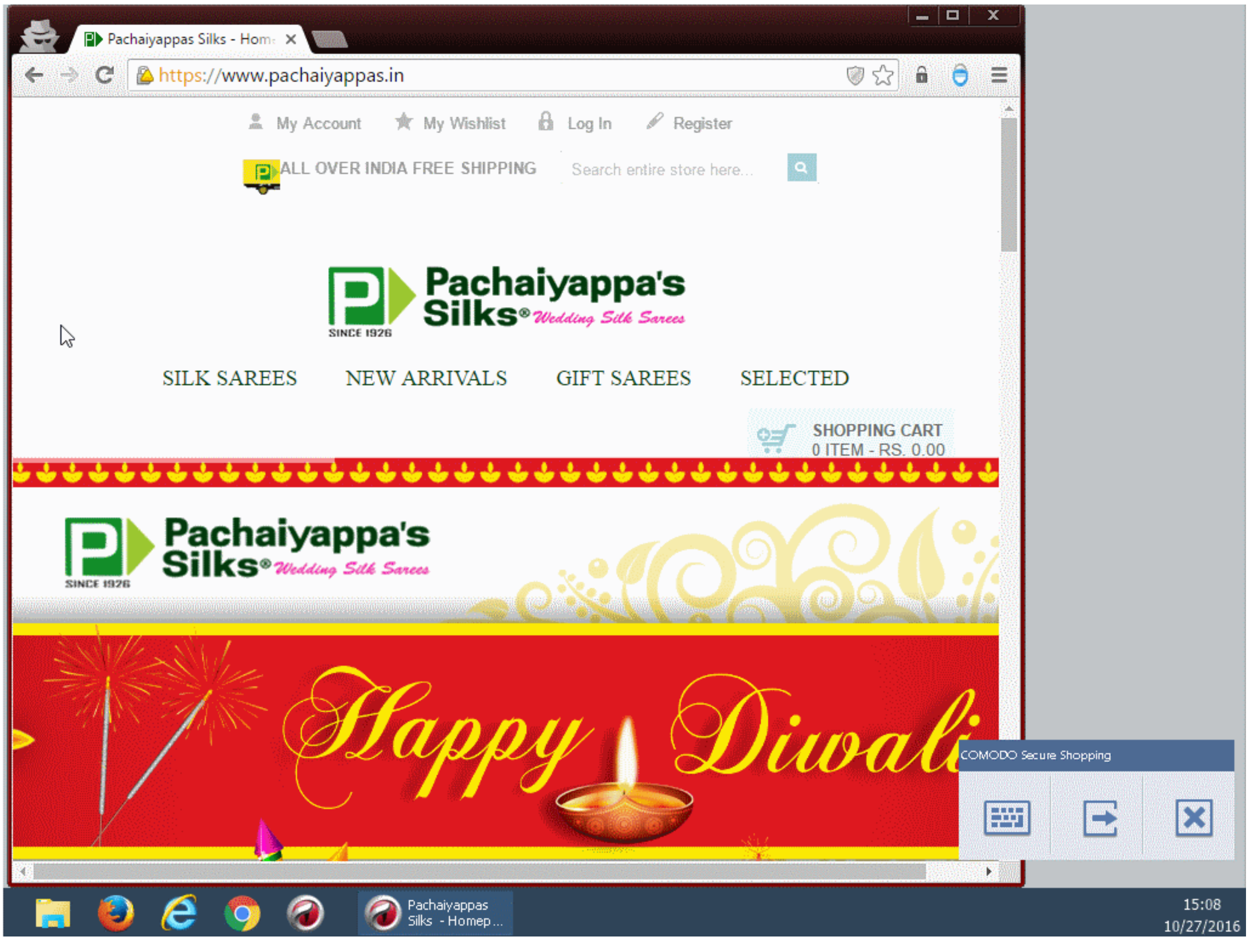
- Hides sensitive online data from other processes running on your PC
- Prevents key-loggers from recording your keystrokes
- Warns you if there is a remote connection to your computer
- Stops hackers and malware from taking screenshots of your session
- Detects fake SSL certificates to stop man-in-the-middle attacks

☑ Do not show this window again

- Check 'Do not show this window again' to disable the welcome screen in future.

Shopping and Banking Activities

If you are visiting a pre-configured online shopping or a banking website and choose 'Visit in Secure Shopping Environment' from the alert, the environment will open automatically with the website in the browser chosen as per the Secure Shopping configuration. If you are opening the Secure Shopping environment manually, the environment will open with the default browser. You can enter the URL of the website in the address bar of the browser.


Pachaiyappas Silks - Home
https://www.pachaiyappas.in
My Account
My Wishlist
Log In
Register
ALL OVER INDIA FREE SHIPPING
Search entire store here...
Pachaiyappa's Silks® Wedding Silk Sarees
SINCE 1926
SILK SAREES
NEW ARRIVALS
GIFT SAREES
SELECTED
SHOPPING CART
0 ITEM - RS. 0.00
Happy Diwali
COMODO Secure Shopping
Pachaiyappas Silks - Homep...
15:08
10/27/2016

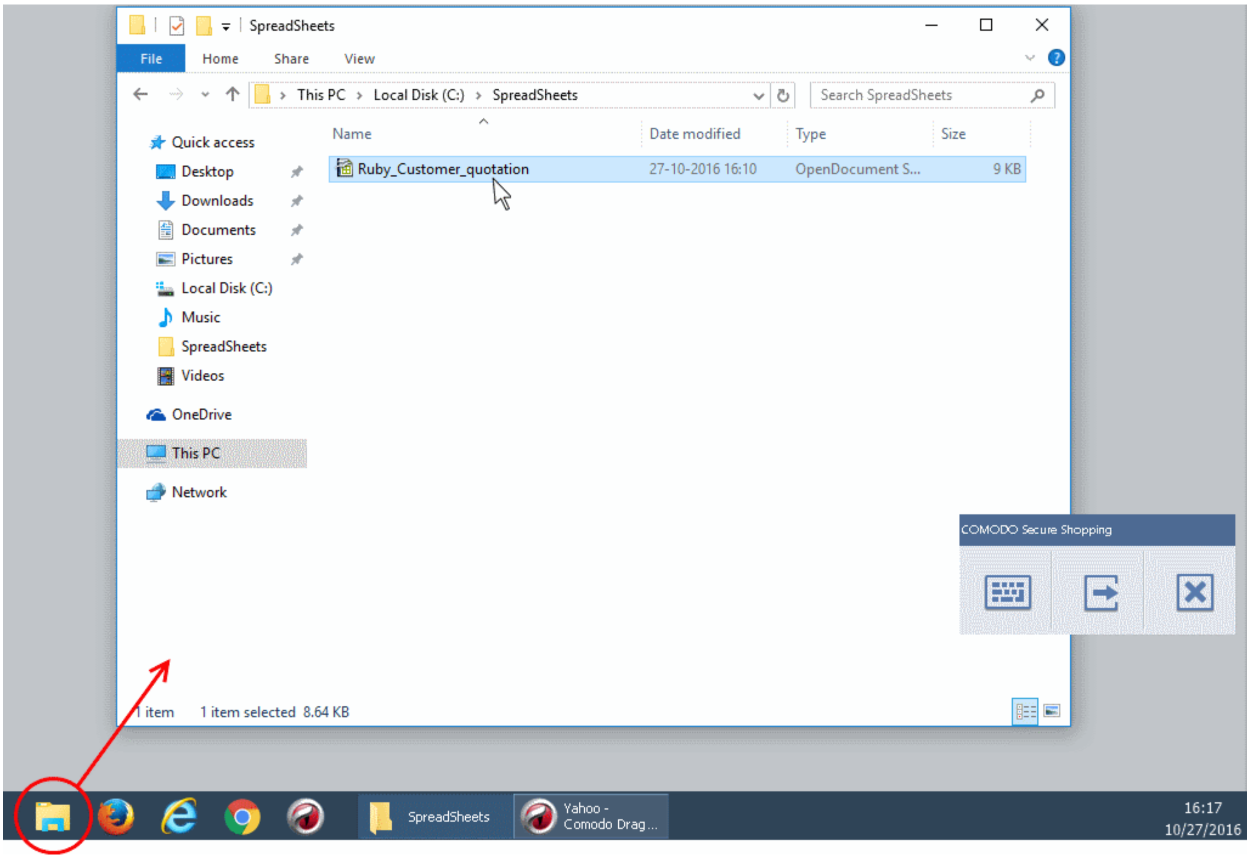
The tools panel at the bottom right of the screen allows you to open the virtual keyboard, temporarily switch back to your desktop, or to fully exit the Secure Shopping virtual environment.

See explanations given below for:

- Opening applications inside the Secure Shopping Environment
- Using Virtual Keyboard
- Switching to your Desktop
- Exiting Secure Shopping

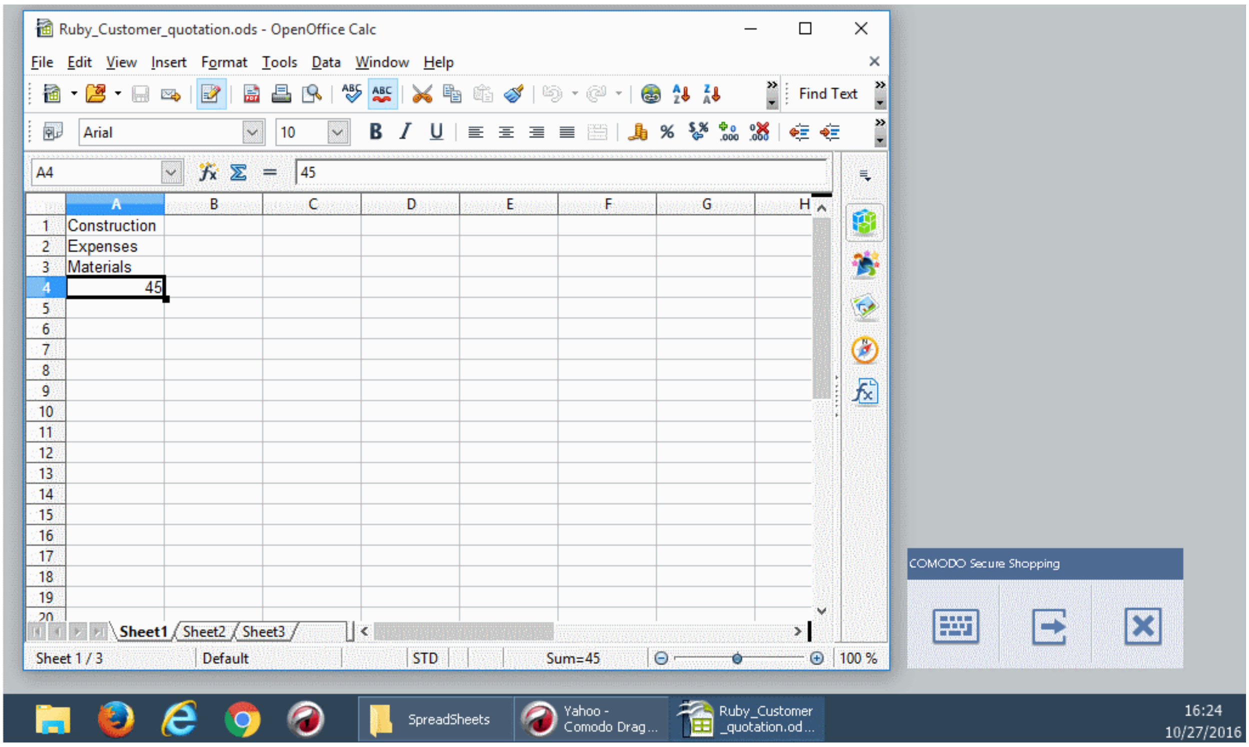
Opening applications inside the Secure Shopping Environment

- Start the Secure Shopping environment and click the folder icon at bottom-left:



- Browse to the application you want to run and open it.

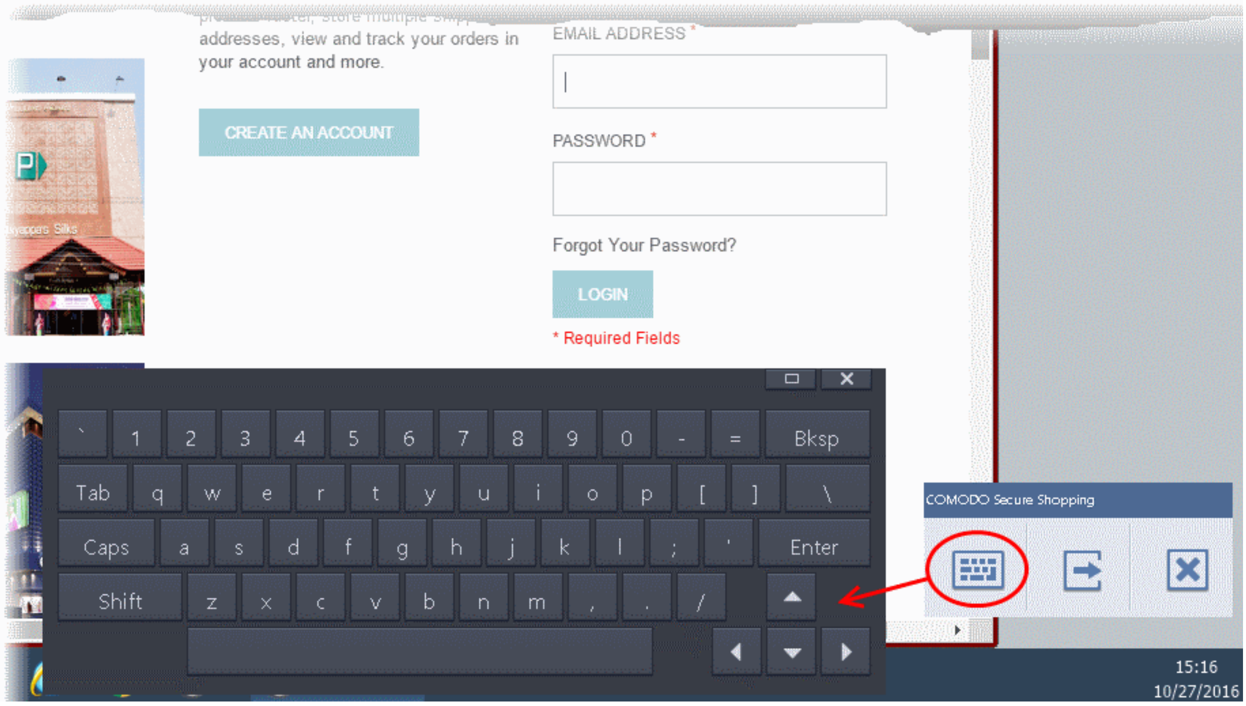
The application will open inside the Secure Shopping environment:



The tools panel at the bottom right of the screen allows you to open the virtual keyboard, temporarily switch back to your desktop, or to fully exit the Secure Shopping virtual environment.

To use the virtual keyboard

- Click the keyboard icon on the system tray to opens the on-screen virtual keyboard. This can be used to input confidential data like website user-names, passwords and credit card numbers.


addresses, view and track your orders in your account and more.
CREATE AN ACCOUNT
EMAIL ADDRESS *
PASSWORD *
Forgot Your Password?
LOGIN
* Required Fields
` 1 2 3 4 5 6 7 8 9 0 - = Bksp
Tab q w e r t y u i o p [ ] \
Caps a s d f g h j k l ; ' Enter
Shift z x c v b n m , . /
COMODO Secure Shopping
15:16
10/27/2016

To temporarily switch to your desktop

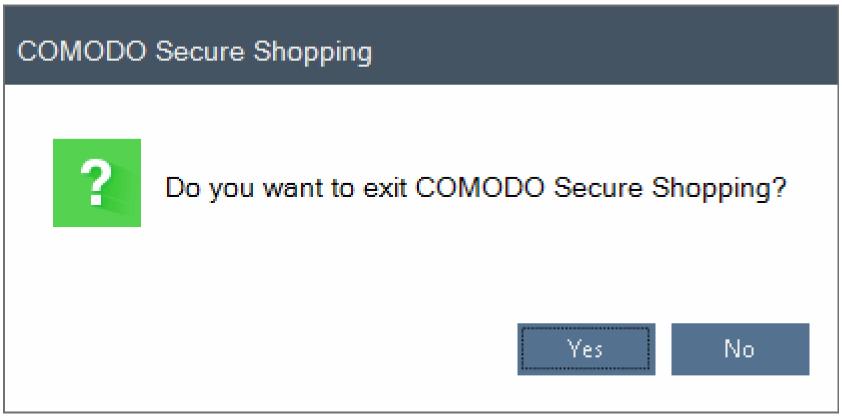
- Click the ➡ button from the tools pane at the bottom right.

The Secure Shopping Desktop will be hidden. You can quickly return to it by clicking the button again.

To close the Secure Shopping Desktop

- Click the 'X' button ☒

A confirmation dialog will be displayed.



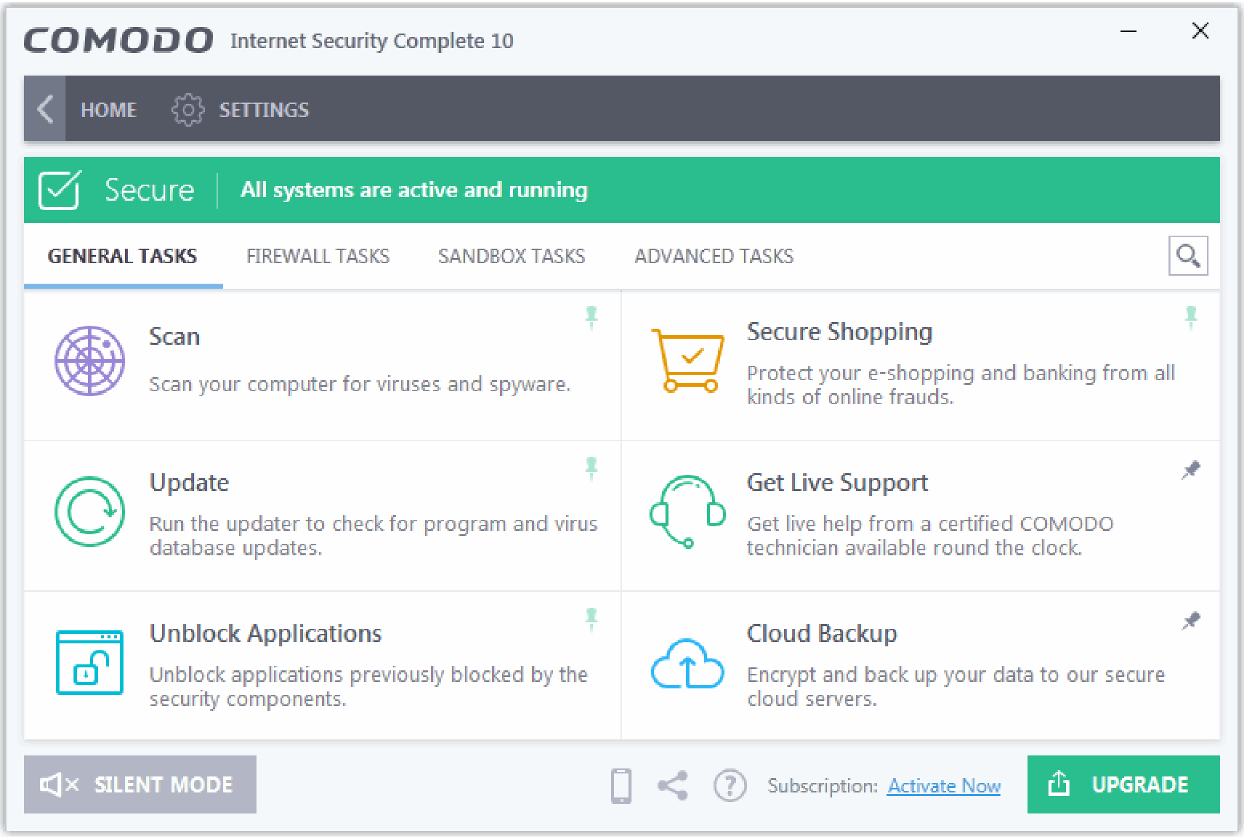
Do you want to exit COMODO Secure Shopping?

- Click 'Yes' to exit the Secure Shopping Desktop.

Comodo Cloud Backup

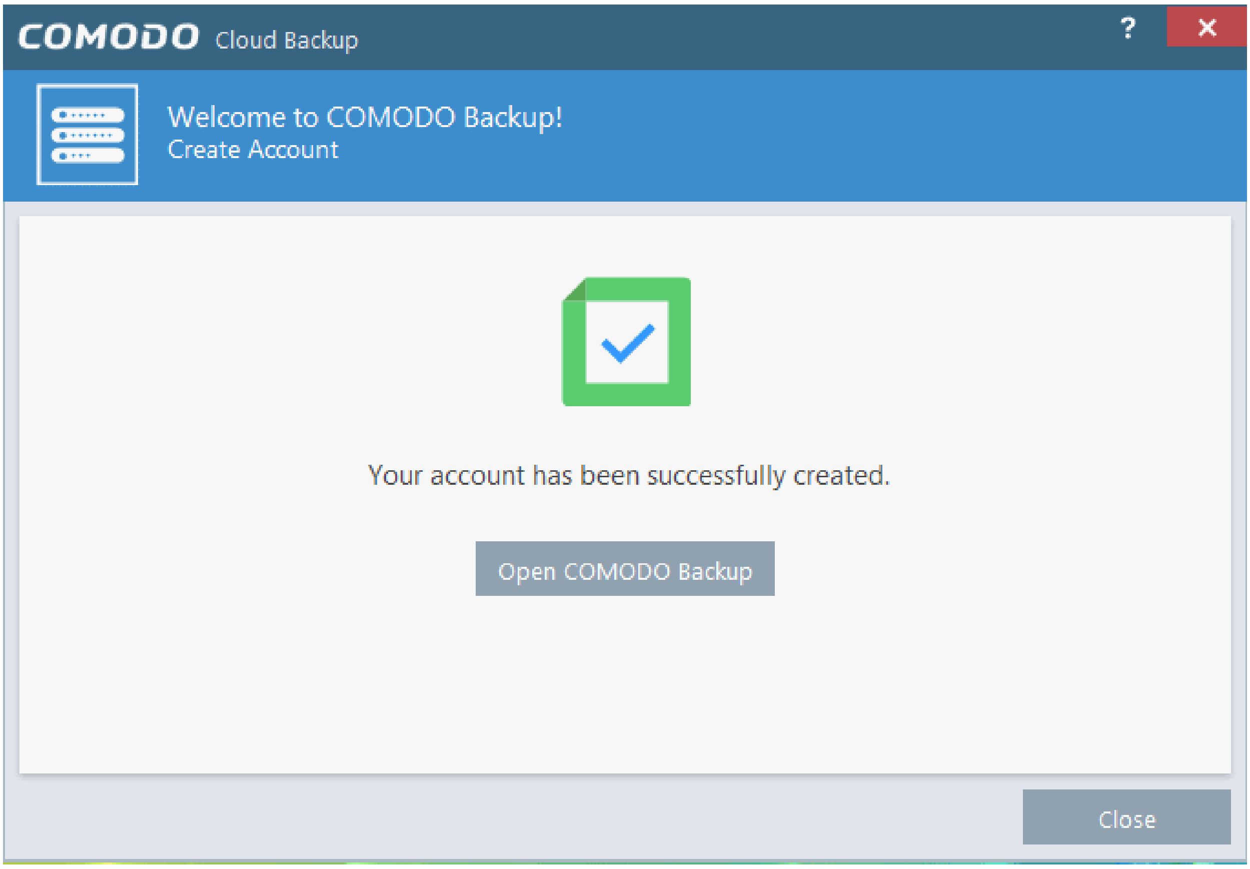
Comodo Cloud Backup provides essential disaster recovery for mission critical or otherwise important files in the event of damage. Files and data stored on Comodo's cloud servers and can be accessed over the Internet from anywhere in the world.

You can access the Comodo Backup by opening 'General Tasks' from the Tasks interface then clicking 'Cloud Backup'.


COMODO Internet Security Complete 10
HOME
SETTINGS
Secure
All systems are active and running
GENERAL TASKS
FIREWALL TASKS
SANDBOX TASKS
ADVANCED TASKS
Scan
Scan your computer for viruses and spyware.
Secure Shopping
Protect your e-shopping and banking from all kinds of online frauds.
Update
Run the updater to check for program and virus database updates.
Get Live Support
Get live help from a certified COMODO technician available round the clock.
Unblock Applications
Unblock applications previously blocked by the security components.
Cloud Backup
Encrypt and back up your data to our secure cloud servers.
SILENT MODE
Subscription: Activate Now
UPGRADE

If you have not activated CIS, then you can create an account from the 'Create New Account' form and if you have already activated CIS using the license key, an account will be created for you automatically.

Account will be created and the dialog displayed.



Your account has been successfully created.

- Click 'Open COMODO Backup' to access your online backup management console.

For more details about how to use Cloud Backup, refer to the online admin guide of our cloud backup partner at **www.acronis.com/en-us/support/documentation/Acronis_Backup_Cloud/index.html**.

Appendix 2 - Comodo Secure DNS Service

Introduction

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Most of the networks use recursive DNS services that are provided by their ISP or that reside on their own set of small DNS servers but it becomes essential to have a secure and broadly distributed DNS service to have a faster and safe DNS resolution.

Background Note: Every device on the Internet is uniquely identified by a 32-bit number (IPv4) or a 128-bit number (Ipv6). While this is perfectly satisfactory for computers, humans are far more comfortable remembering names rather than a string of numbers. The Domain Name System (DNS) provides the translation between those names and numbers. Virtually every piece of software, device, and service on the Internet utilizes DNS to communicate with one another. DNS also makes this information available across the entire span of the Internet, allowing users to find information remotely.

Comodo Secure DNS is a broadly distributed Recursive DNS service that gives you full control to determine how your clients interact with the Internet. It requires no hardware or software and provides reliable, faster, smarter and safer Internet experience.

- Reliable - Comodo Secure DNS Directory Services Platform currently spans across five continents around the world. This allows us to offer you the most reliable fully redundant DNS service anywhere. Each node has multiple servers, and is connected by several Tier 1 carriers to the Internet.
- Faster - Our strategically placed nodes are located at the most optimal intersections of the Internet. Unlike most DNS providers, Comodo Secure DNS Directory Services Platform uses Anycast routing technology - which means that no matter where you are located in the world, your DNS requests are answered by the closest available Comodo Secure DNS set of servers. Combine this with our huge cache and we can get the answers you seek faster and more reliably than anyone else. Furthermore, our "name cache invalidation" solution signals the Comodo Secure DNS recursive servers anytime one of our authoritative customers or partners updates a DNS record, fundamentally eliminating the concept of a TTL.
- Smarter - Comodo's highly structured search and guide pages get you where you want to be, when you inadvertently attempt to go to a site that doesn't exist.
- Safer - As a leading provider of computer security solutions, Comodo is keenly aware of the dangers that plague the Internet today. Secure DNS helps users keep safe online with its malware domain filtering feature. Secure DNS references a real-time block list (RBL) of harmful websites (i.e. phishing sites, malware sites, spyware sites, excessive advertising sites, etc.) and will warn you whenever you attempt to access a site containing potentially threatening content. Additionally, our 'name cache invalidation' solution signals the Comodo Secure DNS recursive servers whenever a DNS record is updated - fundamentally eliminating the concept of a TTL. Directing your requests through highly secure servers can also reduce your exposure to the DNS Cache Poisoning attacks that may affect everybody else using your ISP.

To start Comodo Secure DNS service the DNS settings of your computer has to be modified to point to our server's IP addresses. Comodo Internet Security automatically modifies the DNS settings of your system during its installation to get the services. You can also modify the DNS settings of your system manually, if you haven't selected the option during installation. You can also revert to the previous settings if you want, at anytime.

Click the following links to get the instructions for manually modifying the DNS settings on your router or on your computer.

- **Router**
- **Windows XP**
- **Windows 7/ Windows Vista**

Router - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Router by modifying the DNS settings accessible through DNS Server settings of your router. Comodo recommends making the change on your router so that with one change, all the computers on your network can benefit from Comodo Secure DNS.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Primary DNS : 8.26.56.26

Secondary DNS : 8.20.247.20

To stop Comodo Secure DNS service

- **Modify the DNS server IP address to your previous settings**.

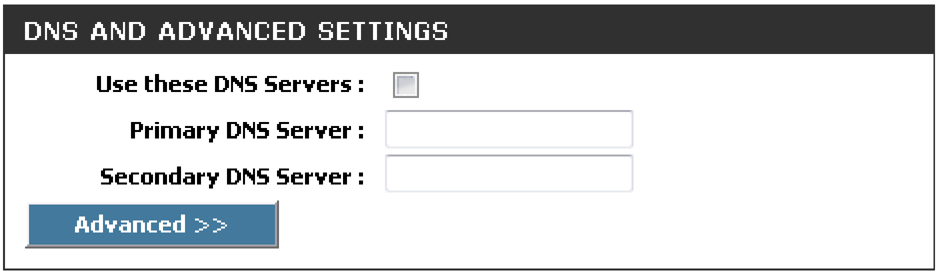
To modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

   http://192.168.0.1
   http://192.168.1.1
   http://192.168.10.1

   If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).



DNS AND ADVANCED SETTINGS

Use these DNS Servers : □

Primary DNS Server :

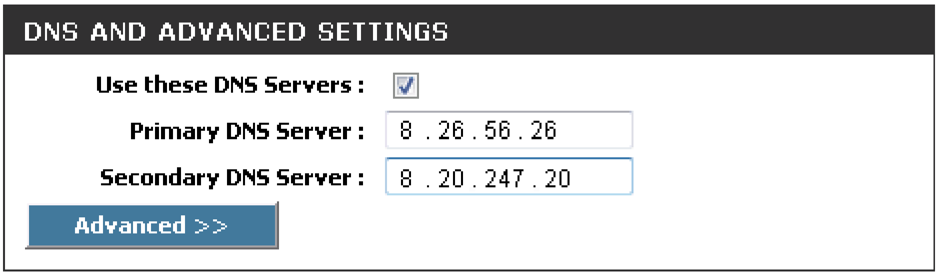
Secondary DNS Server :

3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

   Primary DNS server address for Comodo Secure DNS is: 8.26.56.26

   Secondary DNS server address for Comodo Secure DNS is: 8.20.247.20

   When you are done, the above example would look like this.



DNS AND ADVANCED SETTINGS

Use these DNS Servers : ☑

Primary DNS Server : 8 . 26 . 56 . 26

Secondary DNS Server : 8 . 20 . 247 . 20

You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.

Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Windows XP computer by modifying the DNS settings accessible through Control Panel > Network Connections.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Preferred DNS : 8.26.56.26

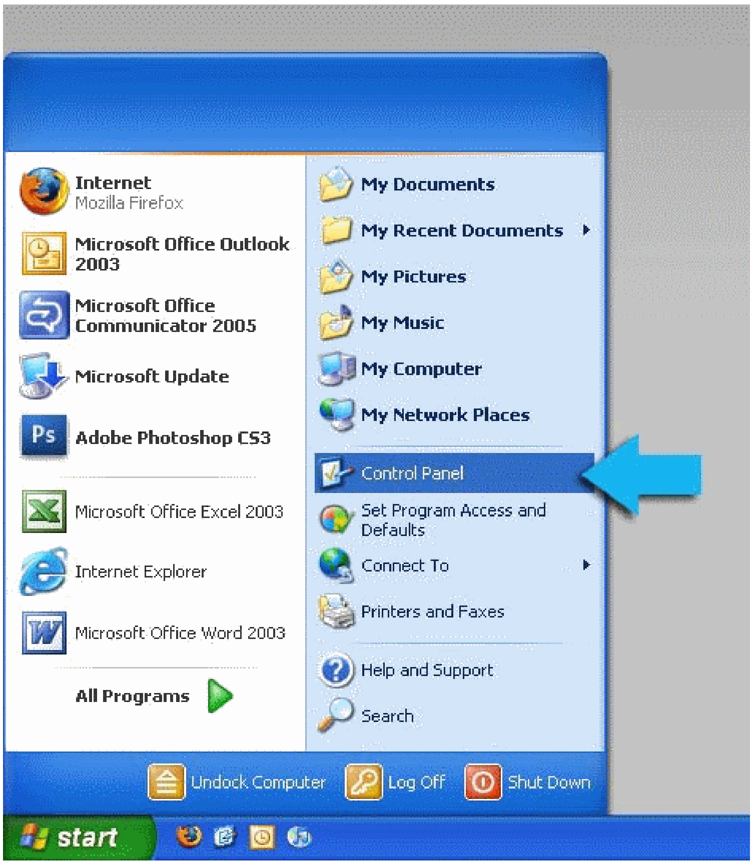
Alternate DNS : 8.20.247.20

To stop Comodo Secure DNS service

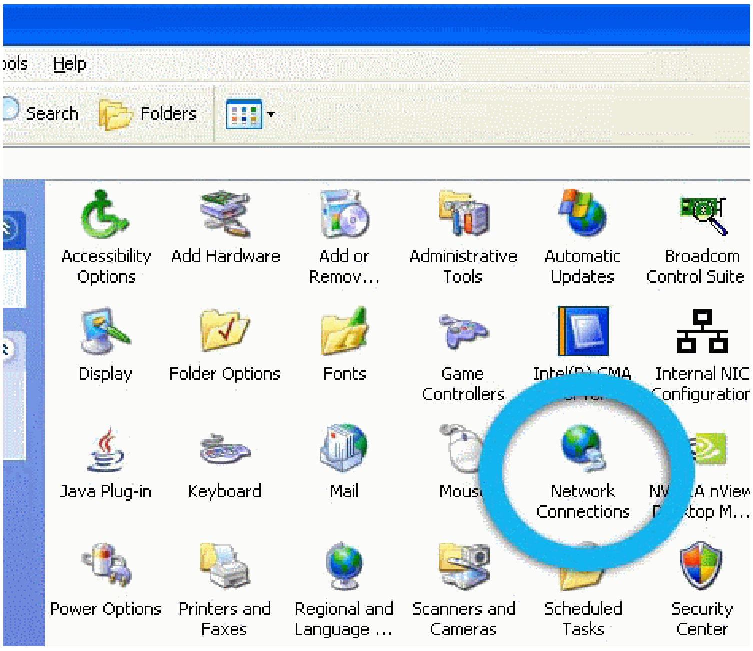
- **Modify the DNS server IP address to your previous settings**.

To modify the DNS settings

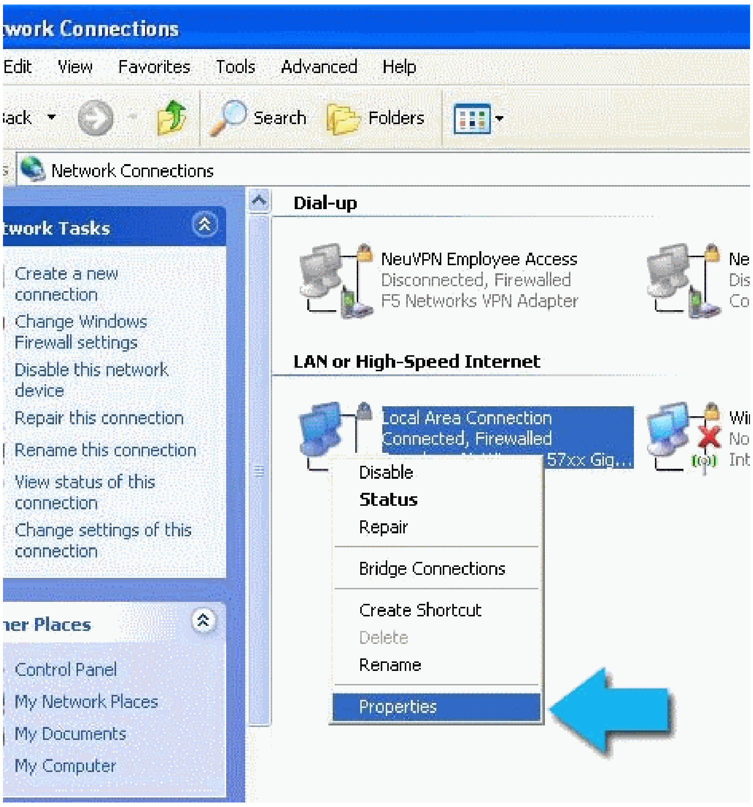
1. Select the 'Control Panel' from the Start Menu.



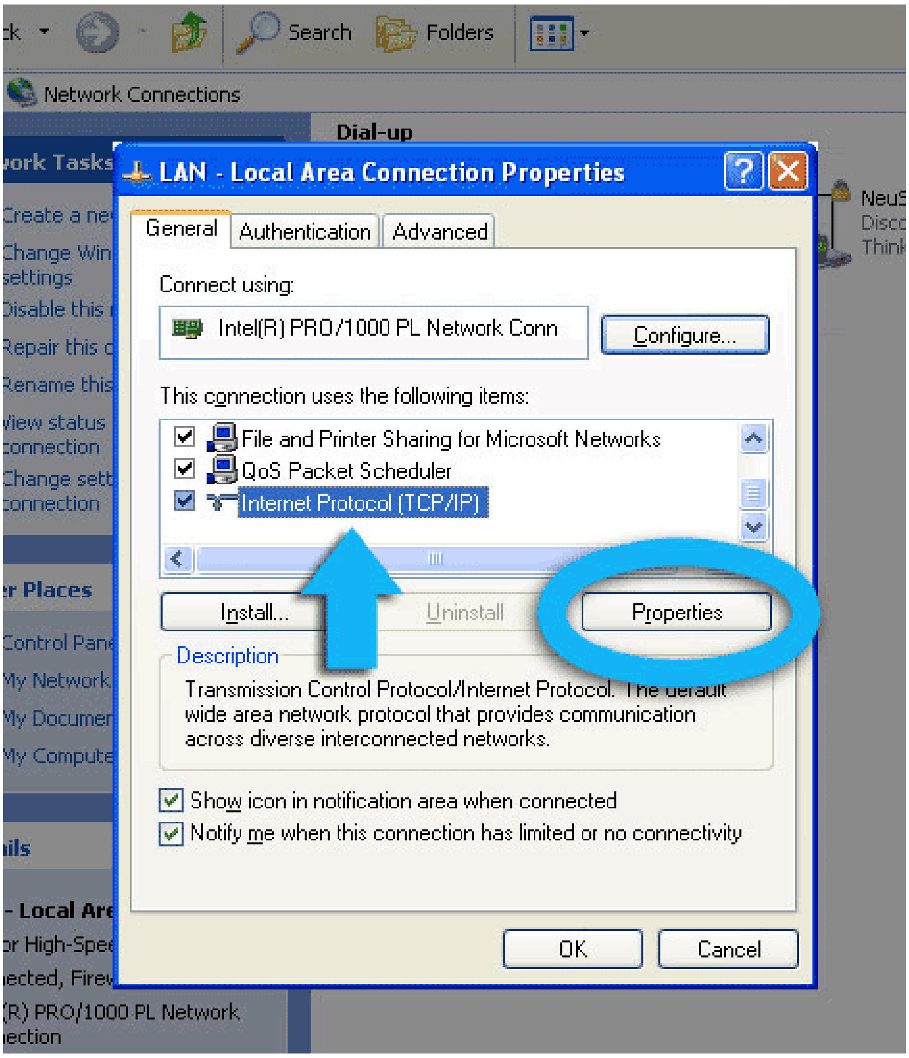
2. Click 'Network Connections' from the Control Panel options.



3. Right click on your connection from the Network Connections window and click 'Properties'.



4. Select 'Internet Protocol (TCP/IP)' and click 'Properties'.



LAN - Local Area Connection Properties

Connect using:

Intel(R) PRO/1000 PL Network Conn

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks

☑ QoS Packet Scheduler

☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

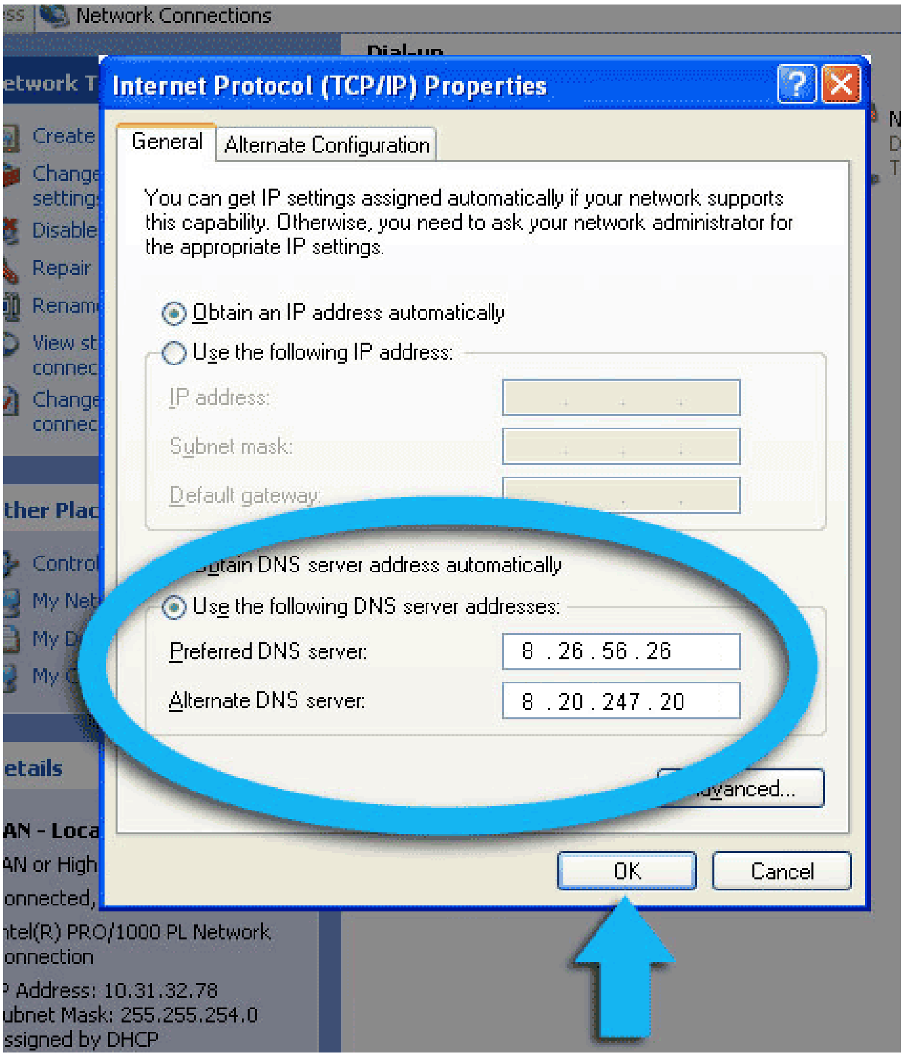
☑ Notify me when this connection has limited or no connectivity

5. Click the radio button Use the following DNS server addresses and type in Comodo Secure DNS addresses in the Preferred DNS server and Alternate DNS server fields.

   Please note down your current DNS settings before switching to Comodo Secure DNS, in case you want to return to your old settings for any reason.

   Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26

   Alternate DNS server address for Comodo Secure DNS is: 8.20.247.20



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

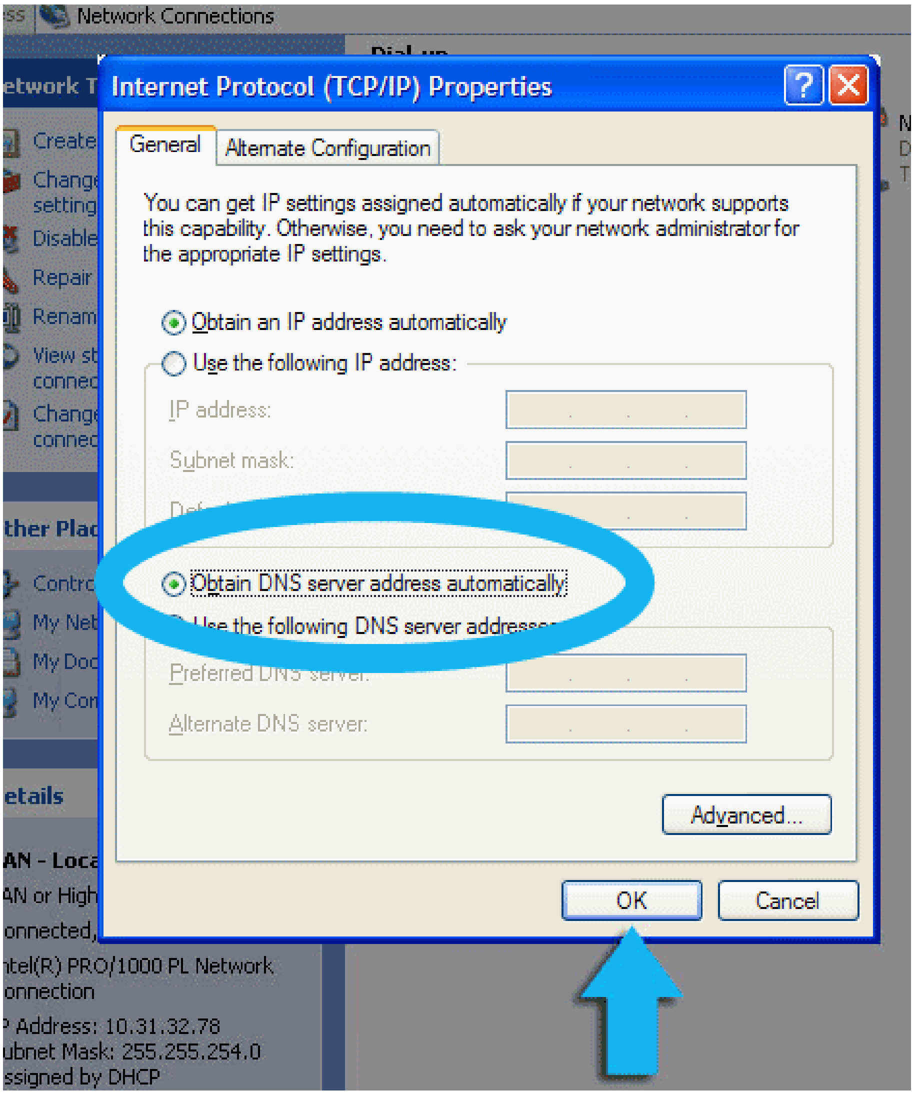
Preferred DNS server: 8 . 26 . 56 . 26
Alternate DNS server: 8 . 20 . 247 . 20

You can disable Comodo Secure DNS by:

- Selecting 'Obtain DNS server address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable the Comodo Secure DNS service by changing your DNS server addresses to:

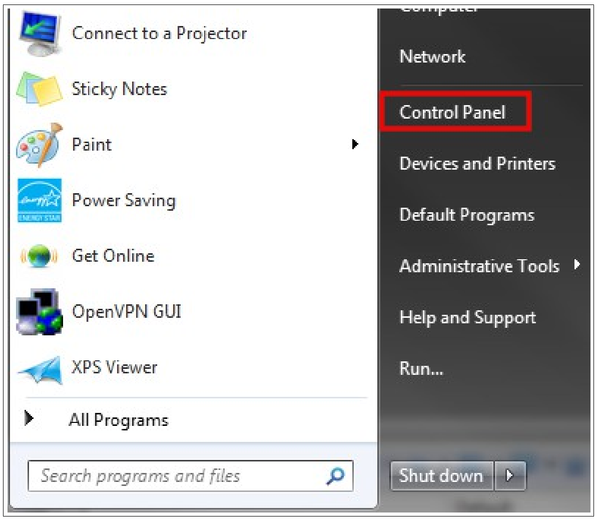
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

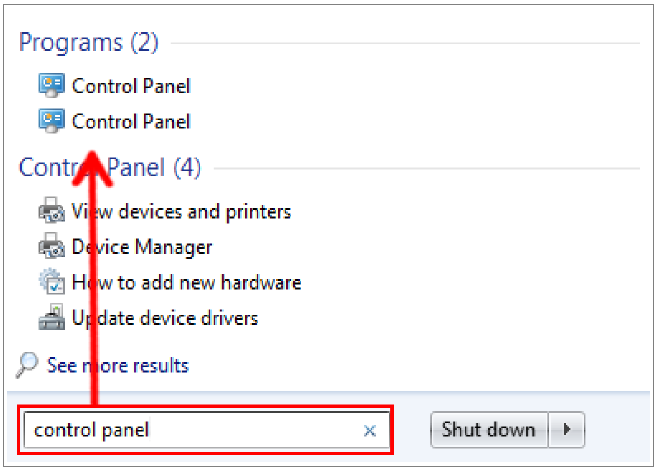
Enabling Comodo DNS in Windows 7 / Vista

Disabling Comodo DNS in Windows 7 / Vista

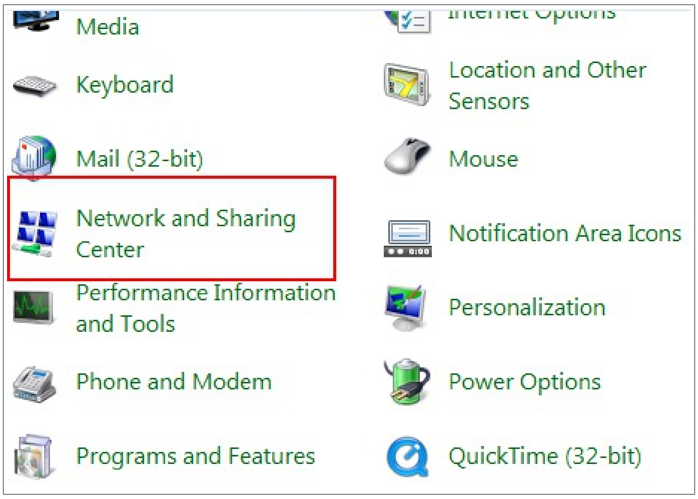
Enabling Comodo DNS in Windows 7 / Vista

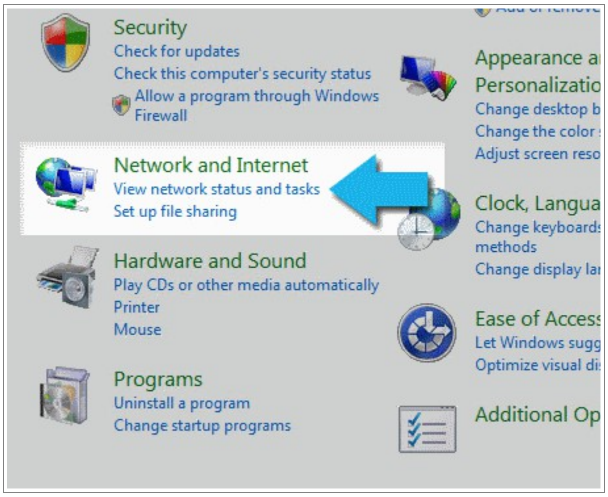
1. Open the control panel by either selecting it from the Windows 'Start' menu or by typing 'control panel' into the search box then clicking the program name.



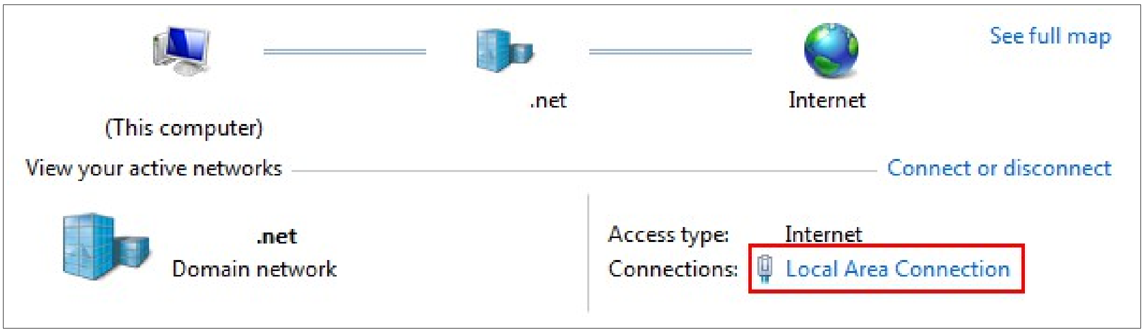


2. From the control panel menu, select 'Network and Sharing Center' (Windows 7) or 'Network and Internet (Vista):

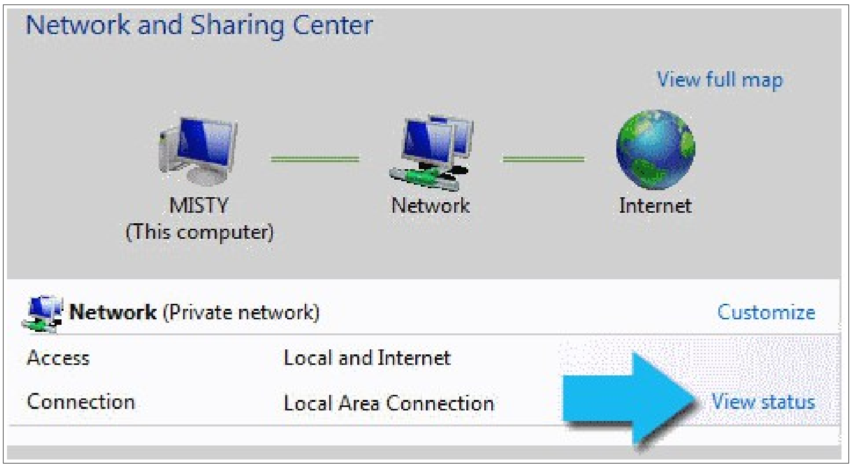




3. In the Network and Sharing center, click the connection type next to 'Connections' (Windows 7):



or 'View Status' (Vista):


Network and Sharing Center

View full map

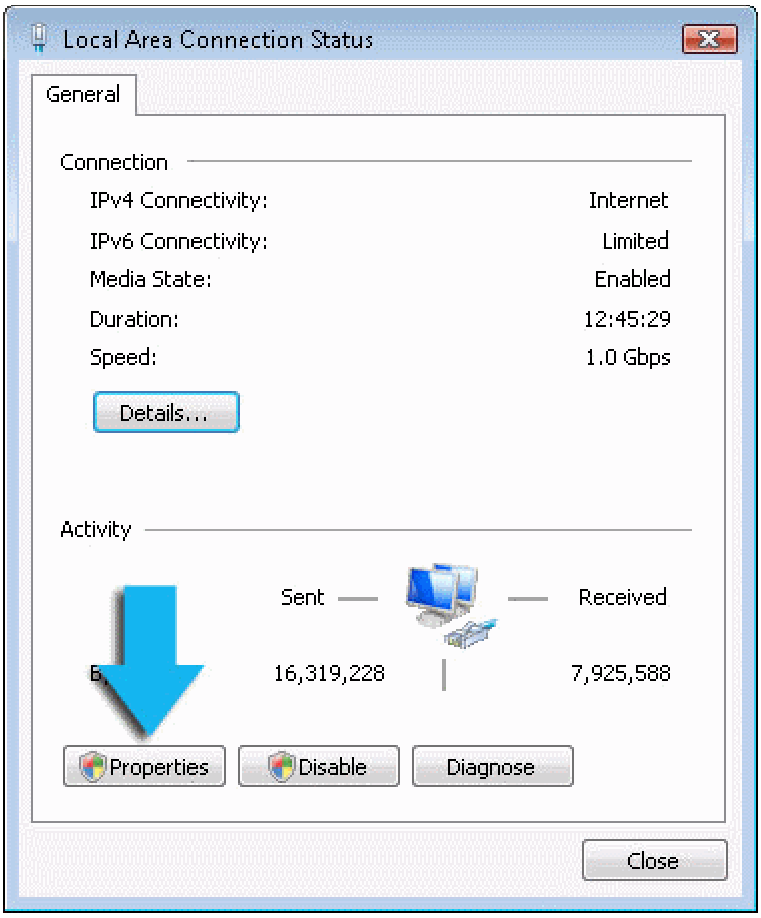
MISTY (This computer) — Network — Internet

Network (Private network) Customize

Access	Local and Internet
Connection	Local Area Connection

View status

4. This will open the 'Local Area Connection Status' dialog. Click the 'Properties' button:


Local Area Connection Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	Limited
Media State:	Enabled
Duration:	12:45:29
Speed:	1.0 Gbps

Details...

Activity

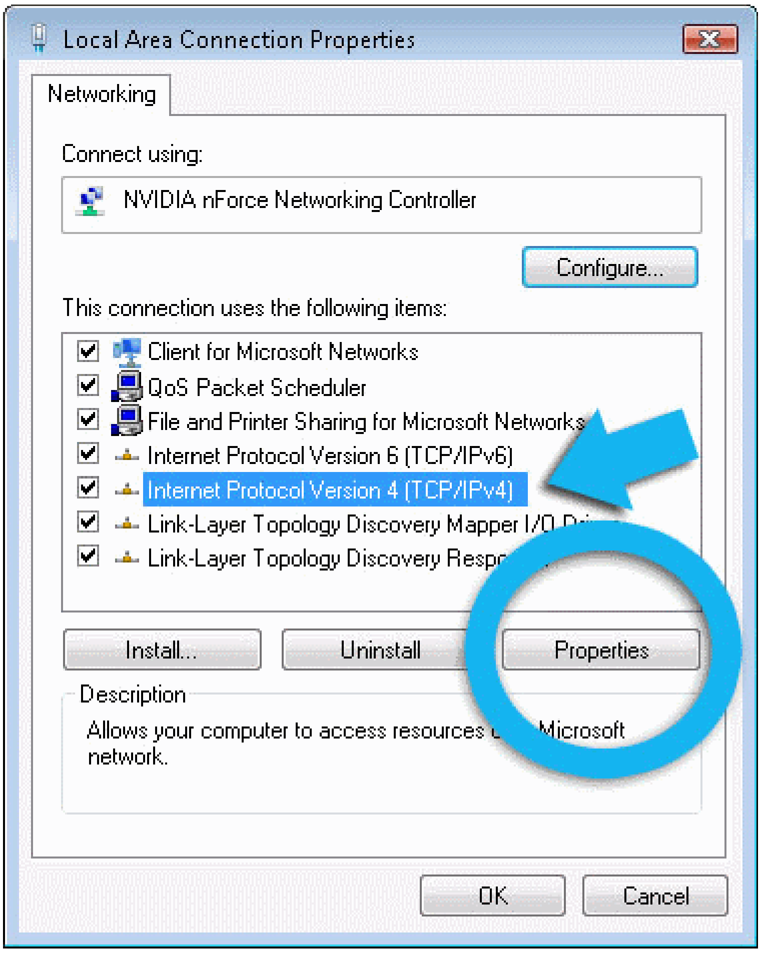
	Sent	Received
B	16,319,228	7,925,588

Properties Disable Diagnose

Close

At this point, Windows might ask for your permission to continue or request that you enter an Administrator password.

5. Once you have granted permission/entered an admin password, you will be presented with the 'Local Area Connection Properties' dialog. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button:



Connect using:

NVIDIA nForce Networking Controller

This connection uses the following items:

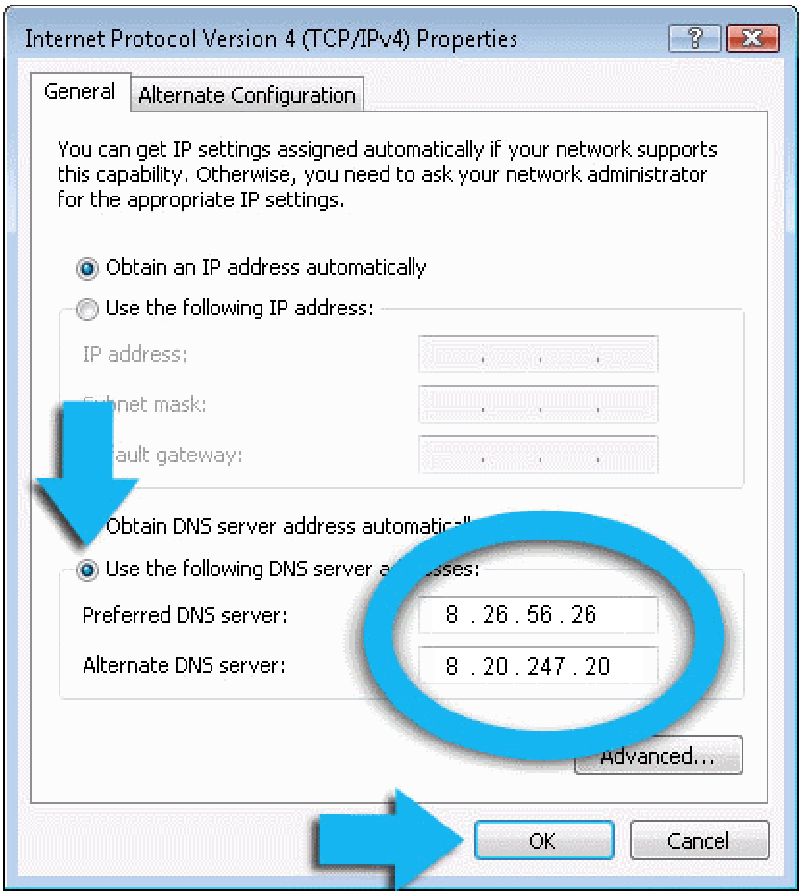
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Dri
- ☑ Link-Layer Topology Discovery Respo

Description

Allows your computer to access resources o Microsoft network.

6. Enable 'Use the following DNS server addresses'. Doing so will allow you to enter the addresses of Comodo DNS servers in the fields provided. Enter the addresses listed below then click 'OK' to activate your settings:

    - Preferred DNS : 8.26.56.26
    - Alternate DNS : 8.20.247.20



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 26 . 56 . 26

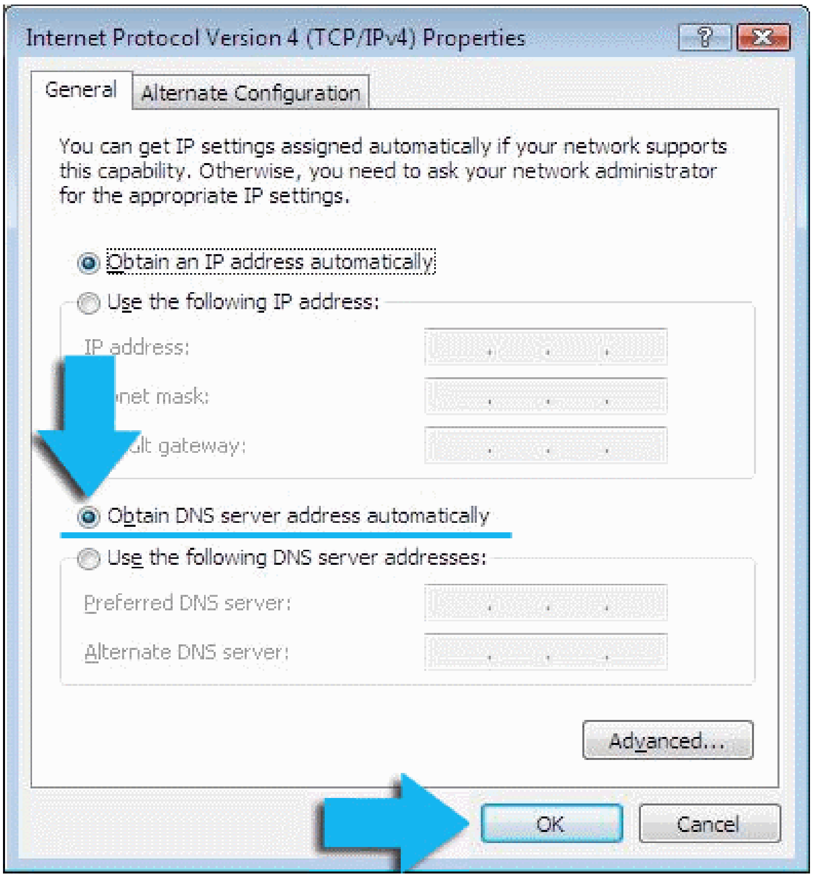
Alternate DNS server: 8 . 20 . 247 . 20

Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the Internet.

Disabling Comodo DNS in Windows 7 / Vista

To disable Comodo DNS, you need to instruct Windows to automatically obtain the address of a DNS server. Doing so means you will use the DNS server provided by your ISP. To do this:

- Follow steps 1 to 7 of the '**Enabling Comodo DNS in Windows 7 / Vista**' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

Appendix 3 - Glossary Of Terms

A B C D E F G H I J K L M N O P Q R S U V W X Y Z

A

ACK

The acknowledgment bit in a TCP packet. (ACKnowledgment code) - Code that communicates that a system is ready to receive data from a remote transmitting station, or code that acknowledges the error-free transmission of data.

Back to the top

Acronis Backup

Acronis Backup Cloud solution enables protection of unlimited storage capacity of any data source and destination including Windows, Mac, Linux, Hyper-V, VMware, RHEV, XEN, KVM, Oracle VM, Microsoft Exchange and SQL, as well as XEN, KVM, Linux, Virtuozzo, Docker, Open-Xchange, and MySQL by accessing directly from the Comodo Internet Security 9. It delivers enterprise customers and end users complete and safe file access, sharing, backup, recovery of all files.

Back to the top

Adware

Adware is software which displays advertising content that is unwanted by users and is often installed without their explicit consent as part of another piece of software. Examples of Adware behavior are replacing your home page, redirecting you to web sites you did not request and displaying constant pop-up ads that can adversely impact your online experience.

Back to the top

Antivirus

An antivirus software is an application which is capable of detecting and removing malicious software such as viruses, trojans, worms and scripts from a computer system. A traditional (or 'classic') antivirus relies on a system of 'black-listed' signatures to detect malicious software. Under this system, antivirus vendors create digital signatures of any executable identified as malware. They then send this list of signatures to their customer's local antivirus software via regular (often daily) updates. The customer's antivirus software will then flag as a virus any program with a signature matching a signature on the blacklist.

One drawback with the signature system is its reactive nature - it can only detect 'known' threats. The vendor has to first identify the file as a virus before they can create a signature of it. In many cases, this means the virus has to have already infected someones computer before a signature can be created to combat it.

Because of this limitation, most modern anti-viruses now deploy a wide range of layered technologies to determine the threat level of a particular file. Such technologies include heuristics, behavior analysis, cloud-based scanning, sand-boxing, host intrusion prevention and file-look up services.

Back to the top

Antivirus Scan

An audit performed by an antivirus application in order to detect malware and viruses in the file system and/or memory of a computer.

Back to the top

ARP

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address, also known as MAC address, in an Ethernet local area network.

Back to the top

Attached Resource Computer NETwork (ARCNET)

ARCNET is a local area network (LAN) protocol, similar in purpose to Ethernet or Token Ring. ARCNET was the first widely available networking system for microcomputers and became popular in the 1980s for office automation tasks. It has since gained a following in the embedded systems market, where certain features of the protocol are especially useful.

Back to the top

Auto-containment

Auto-containment describes the process whereby applications and processes which are unknown to Comodo Internet Security will be automatically run in a isolated operating environment. Contained applications are run under a set of access restrictions so they cannot cause damage the underlying file structure or operating system. The access restriction level applied to contained applications can be set by the user and includes 'Limited', 'Partially Limited', 'Restricted', 'Untrusted', 'Blocked' and 'Fully Virtualized'.

Conceptually, the auto-containment is designed to securely handle 'unknown' executables - those which are not present on Comodo's black-list (definitely malicious) or white-list (definitely safe). If the unknown file turns out to be malicious then it cannot cause any harm because the sand-boxing process denied it access to critical system resources. On the other hand, programs that are unknown but perfectly harmless will run just as well in the container. This allows safe applications the freedom to run as intended while denying malicious applications the ability to cause damage.

The auto-containment process is further enhanced if it is married to a system that can subsequently classify these unknown files as either 'safe' or 'malicious'. In Comodo Internet Security, contained files can be submitted to Comodo servers* for automated behavior analysis. If this analysis discovers the file is malicious then it is added to the black-list which is distributed to all CIS users. If the file does not exhibit malicious behavior it is passed to Comodo labs for more in-depth tests and possible inclusion on the white-list.

** if enabled by the user*

Back to the top

B

Behavior Analysis

An activity performed by CIS to determine whether an unknown application in the conatiner is malicious or not. Unknown files are analyzed by Comodo Cloud Scanners and Comodo's Instant Malware Analysis (CIMA) servers. If found to be safe, they will be submitted to Comodo labs for further checks.

Back to the top

Behavior Blocker

A Host Intrusion Protection (HIPS) mechanism that monitors the behavior of software and files in your system and prevents them from taking actions that would cause damage.

Back to the top

Brute-force

Brute-force search is a trivial but very general problem-solving technique, that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

Back to the top

Buffer Overflow

A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations, often causing the process to crash or produce incorrect results. Hackers use buffer overflows as a trigger to execute to execute malicious code.

Back to the top

Bug

Error in a program that cause problems.

Back to the top

C

CA - Certification Authority

A Certificate Authority (CA) is trusted third party that validates ownership information about a web-server then issues an SSL/TLS certificate to the organization that owns the server. The certificate is then placed on the web-server and is used to secure connections between the server and any clients (browsers) that connect to it. For example, an online store would use a certificate to secure its order forms and payment pages.

A Certificate Authority (CA) such as Comodo CA will sign the certificates it issues with their private key. However, for the website's certificate to operate correctly, there is a reciprocal client side requirement - the internet browser that the visitor is using MUST physically contain the certificate authority's 'root certificate'. This root is required to successfully authenticate any website certificates that have been signed by the CA. If the root certificate is not embedded in a browser, then the website's certificate will not be trusted and visitors will see an error message. Certificate Authorities proactively supply browser vendors with their root certificates for inclusion in the browser's 'certificate store' - an internal repository of root certificates that ships with each browser.

Back to the top

CIS Widget

The CIS Widget is a handy control panel that shows information about the security status of your computer, the speed of outgoing and incoming traffic and other useful information. The widget also has shortcuts to common CIS tasks and allows users to launch contained instances of any internet browser they have installed on their system. By default, the widget is displayed on the desktops of Windows computers running CIS version 6.0 and above.

Back to the top

COM Interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on a computer. Comodo Internet Security automatically protects COM interfaces against modification.

Back to the top

Computer Network

A computer network is a connection between computers through a cable or some type of wireless connection. It enables users to share information and devices between computers and other users within the network.

Back to the top

D

Debugging

The process of identifying a program error and the circumstances in which the error occurs, locating the source(s) of the error in the program and fixing the error.

Back to the top

DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices to connect to a network and be automatically assigned an IP address.

Back to the top

Digital Certificate

A digital certificate is a file used to cryptographically bind a company's Public Key to its identity. Like a driving license or passport binds a photograph to personal information about its holder, a digital certificate binds a Public Key to information about that company. They are issued for between 1 and 5 year validity periods.

Digital certificates are issued by a Certificate Authority like Comodo. Each CA acts as a trusted third party and conducts background checks on a company to ensure they are legitimate before issuing a certificate to them. Apart from providing an encrypted connection between a internet browser and a website, digital certificates are intended to reassure website visitors that the company they are about to make a purchase from can be trusted.

To get a digital certificate, a company must first generate a Certificate Signing Request (CSR) on their web-server. This CSR contains their public key and their identity information. They then enroll and pay for the certificate and send their CSR to the CA.

The CA's validation department will check that the identity information in the CSR is correct by conducting background checks and will sometimes request that the company supplies documentation such as articles of incorporation. Once validation is satisfactorily completed, the CA will issue the certificate to the customer. The customer will then install it on their website to secure sensitive areas like payment pages.

Back to the top

Digital Signature

Digital signatures are used for authentication and integrity, meaning it guarantees that the person sending a message is indeed the same person who he/she claims to be and the message has not been altered. To authenticate oneself using a digital signature, a person needs to download and install Digital Certificates in their systems from Certificate Authorities such as Comodo. The client certificate then can be imported into their browsers and email clients. The same certificate can also be used to digitally sign a document before sending it. The recipient can easily find out if the document has been tampered with en-route.

Back to the top

DNS

DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. When a user searches for a website name like 'www.domain.com', their browser will first contact a DNS server to discover the IP address associated with that domain name. Once it has this information, it can successfully connect to the website in question.

Back to the top

Dynamic IP

The procedure of allocating temporary IP addresses as they are needed. Dynamic IP's are often, though not exclusively, used for dial-up modems.

Back to the top

E

Encryption

Encryption is a technique that is used to make data unreadable and make it secure. Usually this is done by using secret keys and the encrypted data can be read only by using another set of secret keys. There are two types of encryption - symmetric encryption and asymmetric encryption.

Symmetric encryption is applying a secret key to a text to encrypt it and use the same key to decrypt it. The problem with this type of encryption lies during the exchange of secret keys between the sender and the recipient over a large network or the Internet. The secret keys might fall into wrong hands during the exchange process.

Asymmetric encryption overcomes this problem by using two cryptographically related keys, a key pair - a public key and a private key. The private key is kept secret in your system and the public key is made available freely to anyone who might want to exchange messages with you. Any message, be it text, documents or binary files that are encrypted using the public key can be decrypted using the corresponding private key only. Similarly anything that is encrypted using the private key can be decrypted using the corresponding public key. Typically public keys are made available to everyone by using Digital Certificates. The certificates are issued by a Certificate Authority (CA), which identifies a server or user and usually contains information such as the CA who issued it, the organization's name, email address of the user and country and the public key of the user. When a secure encrypted communication is required between a client and a server, a query is sent over to the other party for the certificate and the public key can be extracted from it.

Back to the top

End User

The person who uses a program after it's been compiled and distributed.

Back to the top

EPKI Manager

Enterprise Public Key Infrastructure Manager. The EPKI Manager allows you to issue bulk numbers of:

- SSL Certificates for use on domain names owned by your Company;
- SecureEmail Certificates (S/MIME) for use by employees of your Company.

Your nominated EPKI Manager Administrator(s) will be able to manage all the company's Certificates from a central web based console. Additional certificates may be purchased through the console in minutes; ensuring new servers and employee email may be secured in minutes rather than days. For more information about EPKI Manager click **here**.

Back to the top

Ethernet

Ethernet is a frame-based computer networking technology for local area networks (LANs). The name comes from the physical concept of ether. It defines wiring and signaling for the physical layer, and frame formats and protocols for the media access control (MAC)/data link layer of the OSI model. Ethernet is mostly standardized as IEEEs 802.3. It has become the most widespread LAN technology in use during the 1990s to the present, and has largely replaced all other LAN standards such as token ring, **FDDI**, and **ARCNET**.

Back to the top

Executable Files

An 'executable' is a file that instructs a computer to perform a task or function. Every program, application and device run on computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. For example, when Microsoft Word is started, the executable file 'winword.exe' instructs the computer to start and run the Word application. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Back to the top

F

False Positive

When an antivirus scan is run and the scanner reports that some programs are infected with malware which may not be the actual case and the files are safe. This kind of false alert is called 'False Positive'. Too much of False Postive results can be annoying and the user might just ignore legitimate warning or delete legitimate files causing the relevant program or operating system to malfunction.

Back to the top

Firewall

A firewall is an application that helps an user or administrator to have a control over how the system should be connected with other network/systems or over the Internet.

Back to the top

FS type

Type of file system.

Back to the top

FTP

File Transfer Protocol (FTP) is a protocol used for file transfer from computer to computer across a TCP network like the Internet. An anonymous FTP is a file transfer between locations that does not require users to identify themselves with a password or log-in. FTP uses the TCP/IP protocols to enable data transfer. FTP is most commonly used to download files from a server or to upload a file to a server.

Back to the top

G

Graphical User Interface (GUI)

The visual symbols and graphics with which a user controls a piece of software or device. Most software has a GUI that comprises of windows, menus, and toolbars. The user interacts with the GUI by clicking their mouse on a GUI element. Operating systems like Windows use GUI's because most users find them easier to use than less friendly interfaces like a command line.

Back to the top

H

Heuristics

Heuristics is a technique that continuously evolves based on experience for solving problems, discovery and learning. When the term is used in computer security parlance, Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist. Comodo Internet Security applies this technology in the application, which is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

Back to the top

HIPS

A Host Intrusion Protection System (HIPS) is designed to identify and block zero malware by monitoring the behavior of all applications and processes. It is designed to prevent actions that could cause damage to your operating system, system-memory, registry keys or personal data.

Security software using a HIPS system will generally enforce rules prescribing the permitted activities of processes and executables at the point of execution. Examples of such activities can include changes to files or directories, accessing protected COM interfaces, modifications to the registry, starting up another application or writing to the memory space of another application. The precise nature of these rules can be set by the user or pre-configured by the vendor.

If an executable or process attempts to perform an action that transgresses these rules then the HIPS system will block the attempt and generate an alert notifying the user of that action. Most HIPS alerts will also include security advice.

Back to the top

HTTP

HTTP (Hypertext Transfer Protocol) is the foundation protocol of the World Wide Web. It sets the rules for exchanges between browser and server. It provides for the transfer of hypertext and hypermedia, for recognition of file types, and other functions.

Back to the top

I

ICMP

The Internet Control Message Protocol (ICMP) is part of Internet Protocol (IP) suite and used to report network applications communications errors, network congestion, timeouts and availability of remote hosts.

Back to the top

IDS

An Intrusion Detection System (IDS) is software/hardware that detects and logs inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Back to the top

IMAP

Internet Message Access Protocol'. IMAP is a method of distributing email. It is different from the standard POP3 method in that with IMAP, email messages are stored on the server, while in POP3, the messages are transferred to the client's computer when they are read. Thus, using IMAP allows you to access your email from more than one machine, while POP3 does not. This is important because some email servers only work with some protocols.

Back to the top

Information Security Exposure

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

Back to the top

Internet Service Provider (ISP)

A company or organization that provides the connection between a local computer or network, and the larger Internet.

Back to the top

IP - Internet Protocol

The Internet Protocol (IP) is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched network. An IP address is a numeric address that is used to identify a network interface on a specific network or subnetwork. Every computer or server on the Internet has an IP address. When a user types a domain name such as www.domain.com into the address bar of their browser, the browser still needs to find the IP address associated with that domain in order to reach the website. It finds the IP address by consulting with a DNS server.

There are currently two versions of IP in use today - IPv4 and Ipv6.

IPv4 (Internet Protocol version 4) was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available.

IPv6 is intended to replace IPv4, which uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

Back to the top

K

Key Logger

Key logger is a software application or a hardware device that keeps tracks of computer activity in real time including the keys that are pressed. Key loggers are used to troubleshoot technical problems in computer systems. The application can also be used for malicious purposes such as to steal passwords and other sensitive information.

Back to the top

L

LAN

A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology running at 10, 100 or 1,000 Mbit/s (1,000 Mbit/s is also known as 1 Gbit/s).

Back to the top

Leak Test

Leak Test is a way to find out how well your system is protected by your security software from external and internal threats. Typically these tests are down-loadable and should not cause any harm to your system while being run. The Firewall Leak Tests are used to test how effective the firewall component of your security software is at detecting and blocking outgoing connection attempts. If an application is able to connect to the Internet without your knowledge, it poses a real danger meaning it can easily retrieve private and confidential information from your system and transmit it.

Host Intrusion Prevention System (HIPS) tests are designed to test how well your security software is capable of protecting your internal system from malicious attacks such as viruses. A good HIPS system will deny the malware from accessing your critical operating system files, registry keys, COM interfaces and running processes.

Back to the top

License

The official terms of use for a specific program. A software license is a legal document since it formally restricts the rights of the user.

Back to the top

M

MAC Address

A Media Access Control (MAC) address is a number that is hardwired in network adapters and is used to identify the device or system in which it is installed.

Every device on a network has two addresses: a MAC (Media Access Control) address and an IP (Internet Protocol) address. The MAC address is the address of the physical network interface card inside the device, and never changes for the life of the device (in other words, the network card inside the PC has a hard coded MAC address that it keeps even if installed it in a different machine). On the other hand, the IP address can change if the machine moves to another part of the network or the network uses DHCP to assign dynamic IP addresses. In order to correctly route a packet of data from a host to the destination network card it is essential to maintain a record of the correlation between a device's IP address and it's MAC address. The Address Resolution Protocol performs this function by matching an IP address to its appropriate MAC address (and vice versa). The ARP cache is a record of all the IP and MAC addresses that the computer has matched together.

Back to the top

Malicious File

Often called 'Malware', a malicious file is software designed to damage computer systems, steal sensitive information or gain unauthorized access to private computer systems. For example it may be coded to gather sensitive information from a system such as passwords, credit card details and send them back to the creator of the malware.

Back to the top

Malware

Malware is short for 'malicious software'. It is an umbrella term that describes a wide range of malicious software including viruses, trojans, worms, scripts and root kits. When installed on a computer system or network, malware can disrupt operations, steal sensitive and personal information, delete important data, create zombie networks and perform other destructive operations.

Back to the top

N

Network (computer)

Networking is the scientific and engineering discipline concerned with communication between computer systems. Such networks involves at least two computers, which can be separated by a few inches (e.g. via Bluetooth) or thousands of miles (e.g. via the Internet). Computer networking is sometimes considered a sub-discipline of telecommunications.

Back to the top

Network Zone

A Network Zone can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied. The creation of network zones helps an administrator to apply changes for all the computer(s) in selected zone(s).

Back to the top

NIDS

NIDS - Network-Based Intrusion Detection System. Detects intrusions based upon suspicious network traffic. A network intrusion detection system (NIDS) is a system that tries to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic.

Back to the top

NNTP

Network News Transfer Protocol - Refers to the standard protocol used for transferring Usenet news from machine to machine. A protocol is simply a format used to transfer data to two different machines. A protocol will set out terms to indicate what error checking method will be used, how the sending machine will indicate when it is has finished sending the data, and how the receiving machine will indicate that it has received the data.

Back to the top

O

Operating System (OS)

The essential software to control both the hardware and other software of a computer. An operating system's most obvious features are managing files and applications. An OS also manages a computer's connection to a network, if one exists. Microsoft Windows, Macintosh OS, and Linux are operating systems.

Back to the top

P

Ping

Ping is a computer network tool used to test whether a particular host is reachable across an IP network.

Back to the top

PKCS

PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security.

Back to the top

PKCS#7

See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS).

Back to the top

PKCS#10

See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.

Back to the top

PKCS#12

Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

Back to the top

Plugin

A program that allows a Web browser to display a wider range of content than originally intended. For example: the Flash plugin allows Web browsers to display Flash content.

Back to the top

POP2

There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Back to the top

POP3

POP3 is the abbreviation for Post Office Protocol - a data format for delivery of emails across the Internet.

Back to the top

Ports

A computer port is an interface that allows communication between applications or processes running on a host computer and other computers, devices or networks.

Your computer sends and receives data to other computers and to the Internet through a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to Internet using port 80 and port 443. Your e-mail application connects to your mail server through port 25.

Back to the top

Potentially Unwanted Applications

A potentially unwanted application (PUA) is a piece of software that (i) a user may or may not be aware is installed on their computer, and/or (ii) may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. Because of this ambiguity, many antivirus companies use the term 'Potentially Unwanted Application' to identify such software.

Back to the top

Q

Quarantined Files

After an antivirus scan, files that are detected as malware may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any files moved into quarantine are encrypted so they cannot be run or executed. This prevents infected files from corrupting the rest of a computer.

Back to the top

R

Registry Keys

The Windows Registry serves as an archive for collecting and storing the configuration settings of all computer hardware, software and Windows components. Every time an application or hardware is started, it will access the registry keys relating to it. Applications will also access and modify their registry keys constantly during the course of their execution. As the registry is one of the most regularly accessed parts of Windows, it plays a critical role in the stability, reliability and performance of a computer. Indeed, many computer problems are caused by registry errors. Corrupt keys and invalid keys left by uninstalled applications can often cause severe degradation in system performance, crashes and, in extreme cases, can render a system un-bootable. Inexperienced users are, however, discouraged from making manual adjustments to the registry because a single change can have potentially devastating consequences. There are several dedicated registry cleaners available today, including **Comodo PC TuneUp**.

Back to the top

S

Secure Shopping

New security environment Secure Shopping environment for online banking and shopping sessions by ensuring you connect to those websites from within a dedicated, security-hardened browsing environment. It opens inside a virtual environment which is isolated from other your computers that prevent stealing your credit card, collect personal and financial information or infect your machine with malware and viruses and other online frauds.

Back to the top

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email encapsulated in MIME.

Back to the top

Single User Certificate

A single use certificate refers to the x.509 and associated private key generated by SecureEmail on Alice; stored on SES and downloaded by Bob after a successful SSL client authentication.

Back to the top

SMB

A message format used by DOS and Windows to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include Lan Manager, Windows for Workgroups, Windows NT, and Lan Server. There are also a number of products that use SMB to enable file sharing among different operating system platforms.

Back to the top

SMTP

Simple Mail Transfer Protocol is the most widely used standard for email transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred.

Back to the top

SNMP

Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Back to the top

Spyware

Spyware is a program that performs certain actions without the consent of the user such as displaying advertisements, collecting personal and sensitive information and changing the configuration of the computer. Not all tracking software are malicious since you may have agreed to the conditions as a trade-off for obtaining certain services for free. The tracking software will monitor your online activities to decide what kind of ads should be shown for you.

Back to the top

SSL

Secure Sockets Layer (SSL) is a commonly used protocol for ensuring secure message transmission on the internet. It facilitates an encrypted connection between a web server and an internet browser. It was developed by Netscape in 1994 as a direct response to growing concerns over internet security.

The encryption provided by SSL means that all data passed between a web server and a browser is private and cannot be eavesdropped on. You can tell if you are in an SSL session if the URL begins with https.

SSL is used on the payment pages of millions of websites to protect their online transactions with their customers.

Back to the top

STATIC IP

An IP address which is the same every time you log on to the Internet. See IP for more information.

Back to the top

Stealth Port

Port Stealthing is a security technique whereby ports on an Internet connected PC are hidden so that they provide no response to a remote port scan.

A computer sends and receives data to other computers and to the Internet through an interface called a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, most computers connect to the internet using ports 80 and port 443. Most e-mail applications connect to their mail server through port 25. A 'port scanning' attack consists of sending a message to each port to find out which are open and which are being used by services. With this knowledge, a hacker can determine which attacks are likely to work against a particular computer. Port stealthing effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt ('closed' ports respond with a 'closed' reply- revealing to the hacker that there is actually a PC in existence).

Back to the top

Stateful Packet Inspection

Stateful Packet Inspection, also known as SPI, is an enhanced firewall technique that uses dynamic packet filtering method over the older method of static packet filtering. SPI scrutinizes the packet contents, monitors traffic and keeps track of the sources of packets. A network administrator can configure the firewall that uses SPI according to the needs of the organization, for example, close ports until requested by legitimate users to open them.

Back to the top

SYN

SYN (synchronize) is a type of packet used by the Transmission Control Protocol (TCP) when initiating a new connection to synchronize the sequence numbers on two connecting computers. The SYN is acknowledged by a SYN/ACK by the responding computer.

Back to the top

T

TCP

TCP stands for Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Back to the top

Token-Ring

LAN technology was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5 by the Institute of Electrical and Electronics Engineers. Initially very successful, it went into steep decline after the introduction of 10BASE-T for **Ethernet** and the EIA/TIA 568 cabling standard in the early 1990s. A fierce marketing effort led by IBM sought to claim better performance and reliability over Ethernet for critical applications due to its deterministic access method, but was no more successful than similar battles in the same era over their Micro Channel architecture. IBM no longer uses or promotes Token-Ring. Madge Networks, a one time competitor to IBM, is now considered to be the market leader in Token Ring.

Back to the top

Trojan

A Trojan is a type of malware that looks like a legitimate piece of software and users are tricked to install and execute in their computers. The malware takes the name from the Greek mythology, Trojan Horse, a wooden horse that was used by the Greeks to infiltrate the city of Troy. Once the malware is activated, it can damage the system, spread other computer viruses and also create a back door so as to allow online fraudsters to take access or control the system.

Back to the top

Trusted Files

In Comodo Internet Security, a trusted file is one that is considered safe and is allowed to run on a user's computer. This type of file can also be referred to as a 'safe' file or a 'white-listed' file.

A file will be treated as safe if it is in the 'Trusted Files' list OR if it is digitally signed by a 'Trusted Software Vendor'. Comodo Internet Security ships with a list of trusted files and a list of Trusted Vendors. Users can add their own trusted files and vendors to their local installation. They can also submit files and vendors to Comodo so they can be considered for inclusion in future safe lists.

Back to the top

Trusted Software Vendor

A Trusted Software Vendor (TSV) is a publisher of software that is automatically trusted by Comodo Internet Security software. Executable files that have been digitally signed by a TSV will be allowed to run normally and will not be placed in the container.

Many software vendors digitally sign their software with a code signing certificate. Digitally signed software helps a user to identify the publisher and to be sure that the software he/she is downloading is genuine and has not been tampered with. Each code signing certificate is counter-signed by a trusted certificate authority (CA) after the CA has conducted detailed checks that the vendor is a legitimate company.

Back to the top

U

User

A person who uses a computer, including a programmer or **end user**.

Back to the top

V

Virtual Desktop

The Virtual Desktop is a standalone sandbox featured in Comodo Internet Security which allows users to run any applications in a completely virtual environment. Software in the virtual desktop will not affect other processes, programs or data on the user's computer. Similarly, internet browsers running in the virtual desktop leave behind no personally identifying cookies or history on an employee's real system. The virtual desktop also features a virtual keyboard which provides additional security when entering usernames and passwords on website login pages. Although the virtual desktop is primarily intended for users to test unknown or beta software and for launching highly secure browsing sessions, it can be used to run most software. The virtual desktop interface is available in both desktop and tablet optimized versions.

Back to the top

Virtual Machine (VM)

Virtual machine is a software application that emulates a computing environment in which a program or an operating system can be installed and run. There are many advantages in using a VM such as for testing out new applications or procedures without affecting the host system.

Back to the top

Virus

A computer virus is an executable application capable of causing damage to computer files, folders and components. Viruses are also capable of self-replication so can infect multiple items on a system if left unchecked. The malicious activities performed by a virus are wide ranging and include stealing confidential information, modifying user data, overwriting or damaging files and erasing hard disk content.

Back to the top

VirusScope

VirusScope is an innovative subsystem that monitors all the processes running on a computer in real time to find any suspicious actions taken by any of the processes. If a suspicious activity is identified, VirusScope generates an alert. The alert allows the user to quickly block the process, reverse the effects of the action and move the parent application of the process to quarantine, if the activity is found to be malicious, or to allow the process, if the action is found to be legitimate.

Back to the top

Virus Database

A database of the digital signatures of all known computer viruses and malware. This database, sometimes referred to as a 'black list', enables antivirus software to detect any malware running on a customer's computer.

Every time a file or executable is identified as being malware, antivirus companies will create a digital signature of the file and add it to their database of blacklisted files. This database is then distributed to their customers as an update to their antivirus software. If the blacklisted signature of the malware is found anywhere on a customers computer, then the file is flagged as infected and may be quarantined or deleted.

Comodo has a dedicated team of technicians and crawlers that are continually searching for new virus strains to add to our database. Comodo's virus database is available for public download at **http://internetsecurity.comodo.com/updates/vdp/database.php**.

Back to the top

Vulnerability

In network security, a vulnerability refers to any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network.

Back to the top

W

Website Filtering

Website Filtering is a security technique whereby access to specific websites can be selectively blocked or allowed to particular users of the computer. The website filtering is very useful for parental control as it allows to block inappropriate websites to juvenile users. Also, in work environments, administrators can prevent employees from visiting social networking sites during working hours.

Back to the top

Web server

The term Web server can mean one of two things:

1. A computer that is responsible for accepting **HTTP** requests from clients, which are known as Web browsers, and serving them Web pages, which are usually HTML documents and linked objects (images, etc.).

2. A computer program that provides the functionality described in the first sense of the term.

Back to the top

Worm

A Worm, another type of malware, unlike virus is capable of spreading from computer to computer without any human help. The worm with its capability to replicate itself several times over consumes most of the system memory causing the computer to slow down or crash altogether. It can also cause bandwidth jam while spreading to other computers in the network.

Back to the top

Wildcard

Wildcards are symbols that add flexibility to a keyword search by extending the parameters of a search word. A wildcard item is usually denoted with the asterisk symbol, '*'. This stands for one-or-more characters (useful for all suffixes or prefixes). In digital certification terms, a 'wildcard certificate' means that the certificate will secure the domain plus unlimited sub-domains of that domain. A wildcard certificate is applied for using the format '*.domain.com'.

Back to the top

X

X.509

An internationally recognized standard for certificates that defines their required parts

Back to the top

Z

Zero-Day Malware

Zero-day malware describes new computer viruses or worms that have been discovered in the public realm but which antivirus vendors have not yet created a digital signature for. The term means that the antivirus companies have had 'zero-days' to react. New malware can reasonably be called 'zero-day' for the the length of time between its discovery and the creation of a signature to combat it. For most antivirus vendors, this is usually measured in a matter of hours. Of course, the malware itself may have been at large for a much longer period of time before it was discovered. Because of this window of vulnerability, most security software has grown beyond a reliance on traditional, signature based detection. Most antivirus software now contains layers of prevention-based technologies intended to detect and neutralize 'unknown' malware until such time as a signature can be created. Example technologies include heuristic detection, host intrusion prevention (HIPS), automatic containment and real-time behavior analysis.

Back to the top

Appendix 4 - CIS Versions

Comodo Internet Security is available in three versions - free, Pro and Complete. The Pro version includes **Comodo GeekBuddy** (Comodo support experts available 24/7 to fix any problem with your computer), Secure Shopping (security for online banking and shopping sessions) and the Virus Free Guarantee (if your computer becomes damaged as a result of malware and Comodo support services cannot return it to a working condition then we'll pay the costs of getting it repaired. Please see the **End User License Agreement** for full details). CIS Complete includes GeekBuddy, the Virus Free Guarantee, **TrustConnect** (a secure Internet proxy service that ensures 128 bit encrypted connectivity from any public wireless hotspot), Secure Shopping and a Acronis Backup Cloud account.

Product	Includes								Price*
	Antivirus	Firewall	GeekBuddy	TrustConnect	Acronis Back Up	Secure Shopping	Protection Plan Virus Free Guarantee (VFG) / Identity Protection (IDP)	Virus Removal Service	
CIS 10.x	✓	✓	✓	✘	✘	✓	✘	✘	Free
CIS Pro 10.x	✓	✓	✓	✘	✘	✓	✓	✓	$39.99/ year or $3.99/ month
CIS Complete 10.x	✓	✓	✓	✓ (10 GB / Month)	✓ (50 GB Free. Upgrades available)	✓	✓	✓	$89.99/ year or $8.99/ month
CAV Free	✓	✘	✘	✘	✘	✘	✘	✘	Free
CAV Advanced	✓	✘	✘	✘	✘	✘	✘	✓	$19.99/ year or $3.49/ month
Comodo Firewall	✘	✓	✘	✘	✘	✘	✘	✘	Free

* Most CIS products also have discounts for multi-year purchases.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

The Comodo Threat Research Labs is a global team of IT security professionals, ethical hackers, computer scientists and engineers analyzing and filtering input from across the globe. The team analyzes millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day, using the insights and findings to secure and protect its current customer base and the at-large public, enterprise and internet community.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets. With offices in the US, China, Turkey, India, Romania and Ukraine, Comodo secures the online and offline eco-systems of thousands of clients worldwide.

Comodo Security Solutions, Inc

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.6361

Tel : +1.703.581.6361

Email: **EnterpriseSolutions@Comodo.com**

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