COMODO
Creating Trust Online®

Comodo
Internet Security
Software Version 12.2

User Guide
Guide Version 12.2.050420

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 a threat containment system which automatically runs unrecognized files in a secure, virtual environment.

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.
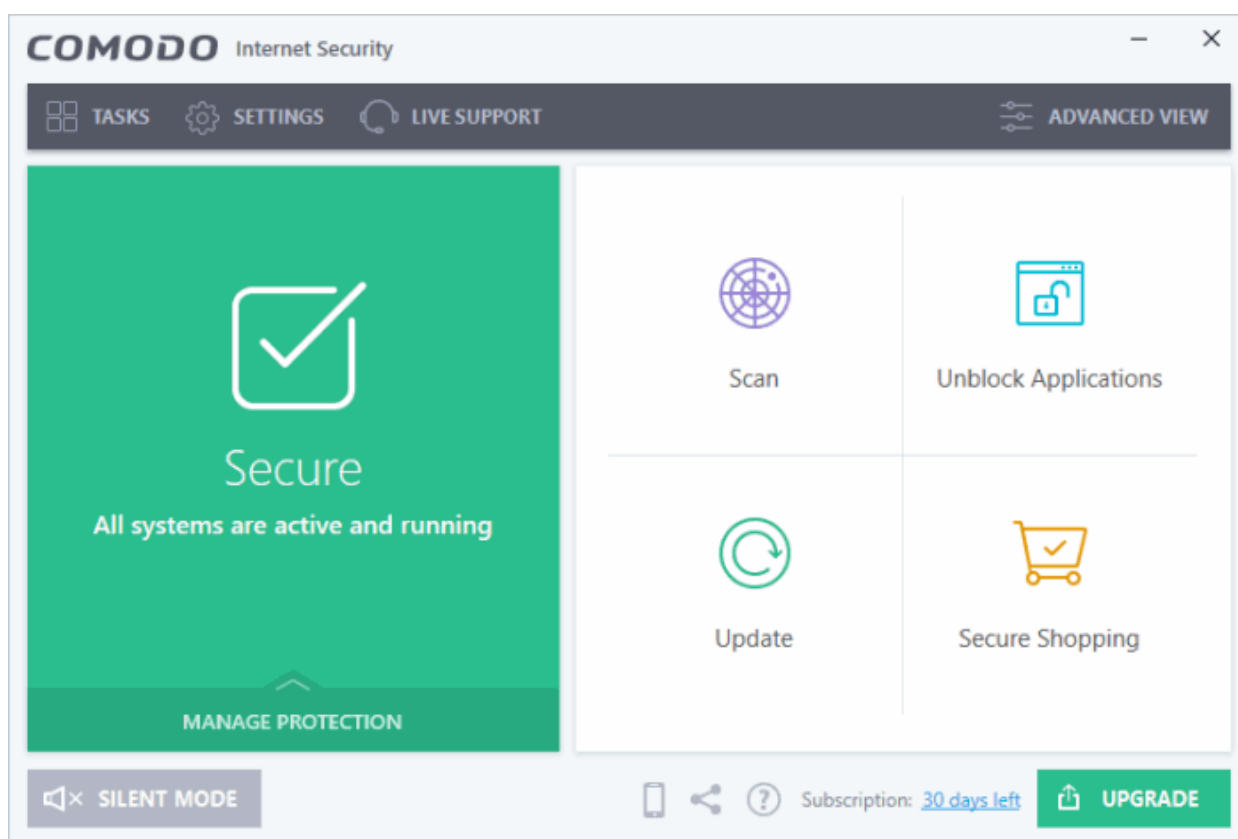
CIS is available in Premium, Pro and Complete editions. While the core CIS software is identical for all three versions, the Pro and Complete packages each offer a range of additional services. The software is designed to be secure 'out of the box' - so even the most inexperienced users need not have 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 types, CIS users can now drag-and-drop items onto the home screen to run an instant scan. The engine also scans any removable storage plugged-in to your computer.

- **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'.

- **Dragon 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**

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;
- Automated scanning of plugged-in external storage devices
- 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 Essentials

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

- • CISE runs as a background process and alerts you if a site uses a potentially malicious certificate

- • Option to disconnect or continue the connection

- • Blocks man-in-the-middle attacks by verifying certificates against Comodo's trusted root certificate list

- • Extremely useful if you are accessing sensitive websites while on public Wi-Fi

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. Download, Installation and Activation

Comodo Internet Security is available in three versions, 'Premium', 'Pro' and 'Complete'. 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

- Premium **- https://www.comodo.com/home/internet-security/free-internet-security.php?track=8234**
- 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. See **https://help.comodo.com/topic-72-1-772-9444-CIS - Installation.html** for a complete outline of the installation process.

Activation

CIS Pro and Complete licenses should be activated after installation. You need to run, and pass, a full antivirus scan on your system in order to activate the Comodo guarantee. 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 help with these items.

System Requirements

Please ensure your PC complies with the minimum system requirements:

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

Note about Windows XP / Vista
• CIS v.12.0.0.6882 and above does not support Windows XP or Vista, period.
• The containment and virtual desktop features haven't worked on XP / Vista since CIS v.8.0 (2014). So even if you use an older CIS, you cannot take advantage of one of our strongest protection features.
Comodo strongly recommends anybody still using XP/Vista to upgrade immediately. Microsoft abandoned support for XP/Vista years ago, and the amount of serious vulnerabilities in these operating systems is almost innumerable. By using XP or Vista, you are exposing yourself to substantial risks which signature-based antivirus cannot protect you against.

1.3. Start 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.**
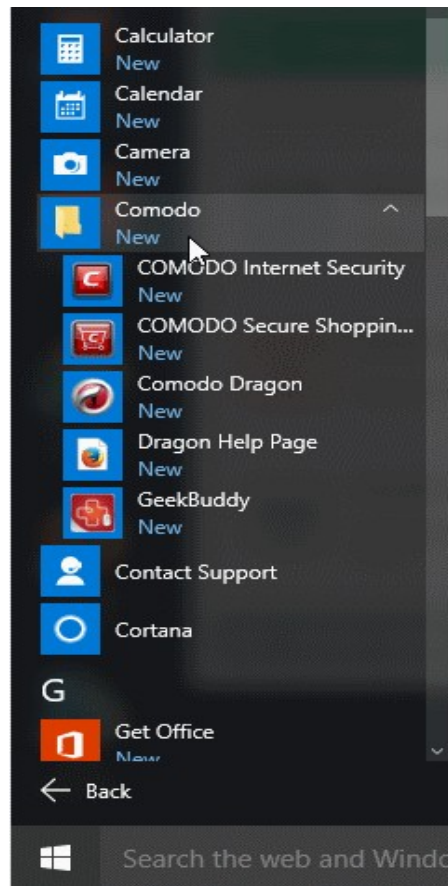
Windows Desktop

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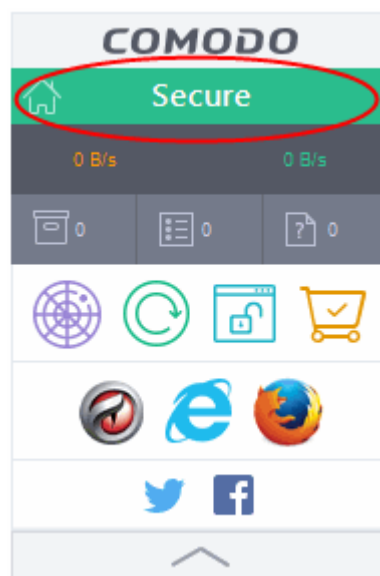
You can also view other details in the widget such as inbound and outbound traffic, number of tasks running, shortcuts to common CIS tasks and browsers and links to social media sites Twitter and Facebook. See '**The Widget**' for more details.

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 tasks with the minimum of fuss. Each tile on the home screen contains important security and update information and lets you 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**' if you need help to change theme.

- Click the 'Home/Tasks' button at 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 on the home screen provide one-click access to the antivirus scanner, updates, Secure Shopping, and more.

- The 'Upgrade' button lets you upgrade to CIS Pro or Complete.

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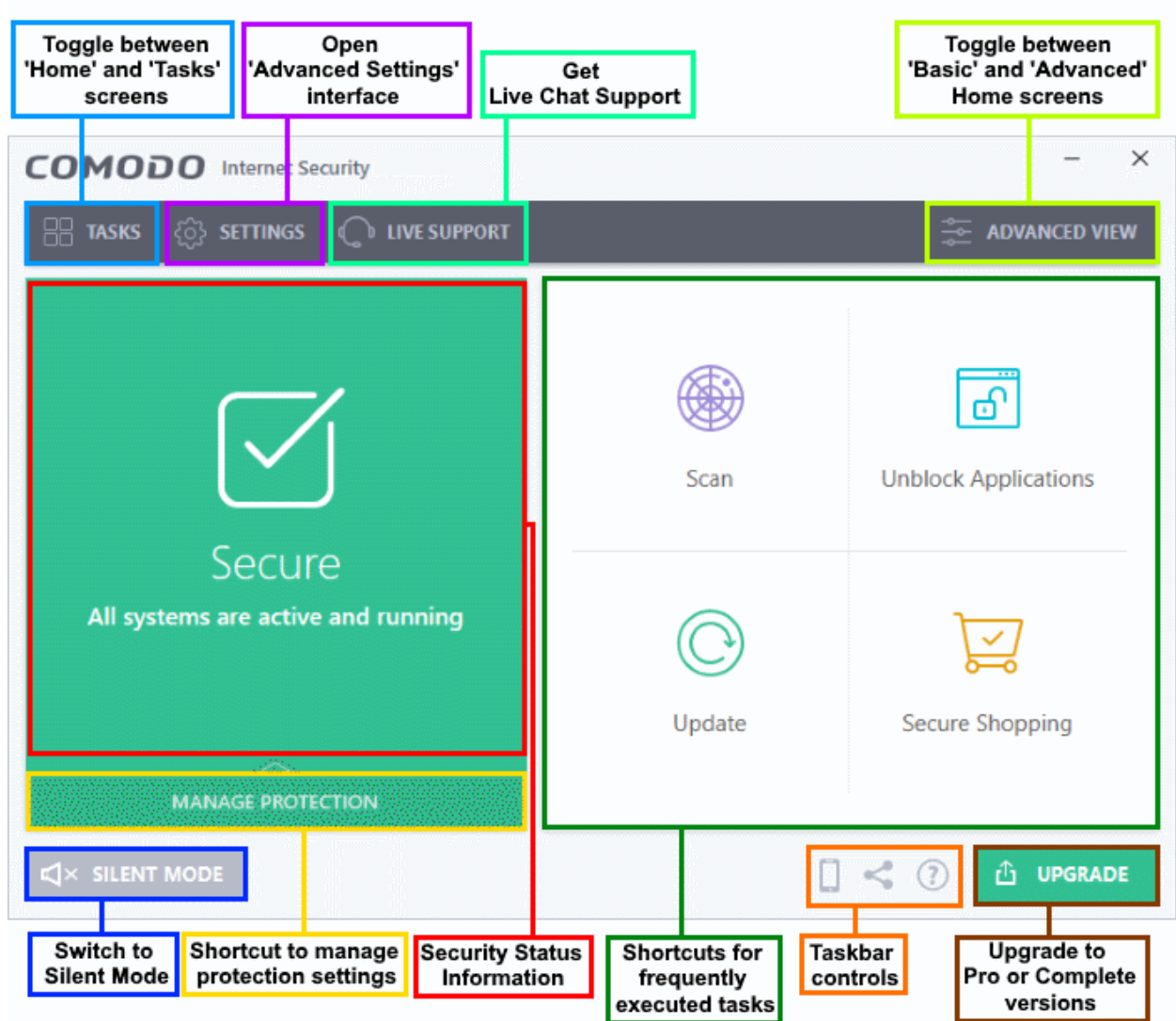
Advanced View
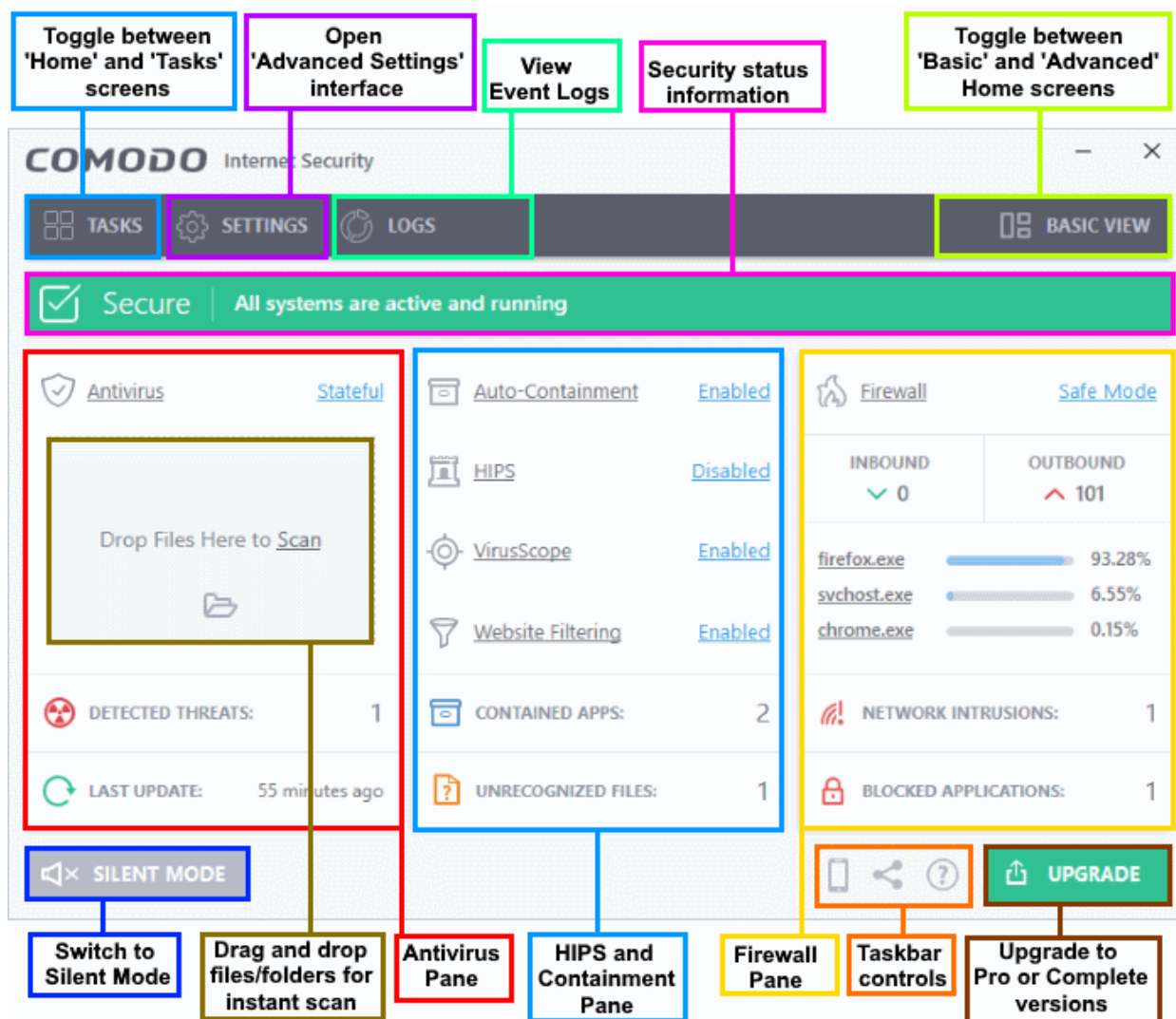
Advanced view shows antivirus, containment, and firewall activity in greater detail. This includes the number of detected threats, last virus database update time, contained apps, unrecognized files, the number of inbound and outbound connections and more.

You can also 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	Click the 'Share' icon 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

Click '?' for the following options:
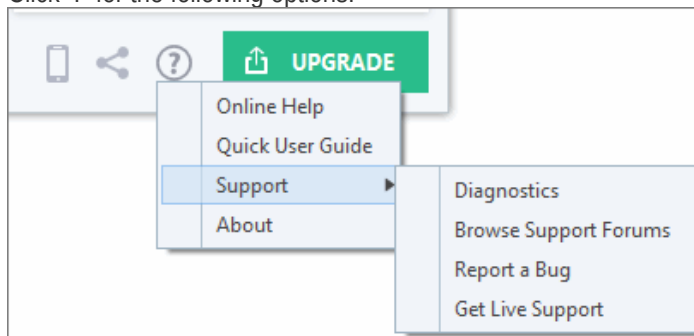
- **Online Help** - Opens Comodo Internet Security's online help guide at **https://help.comodo.com**
- **Quick User Guide** - Open the Comodo Internet Security's quick start guide at **https://help.comodo.com**
- **Support** - Click this link for the following options:
  - **Diagnostics** - Helps to 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 / Complete.
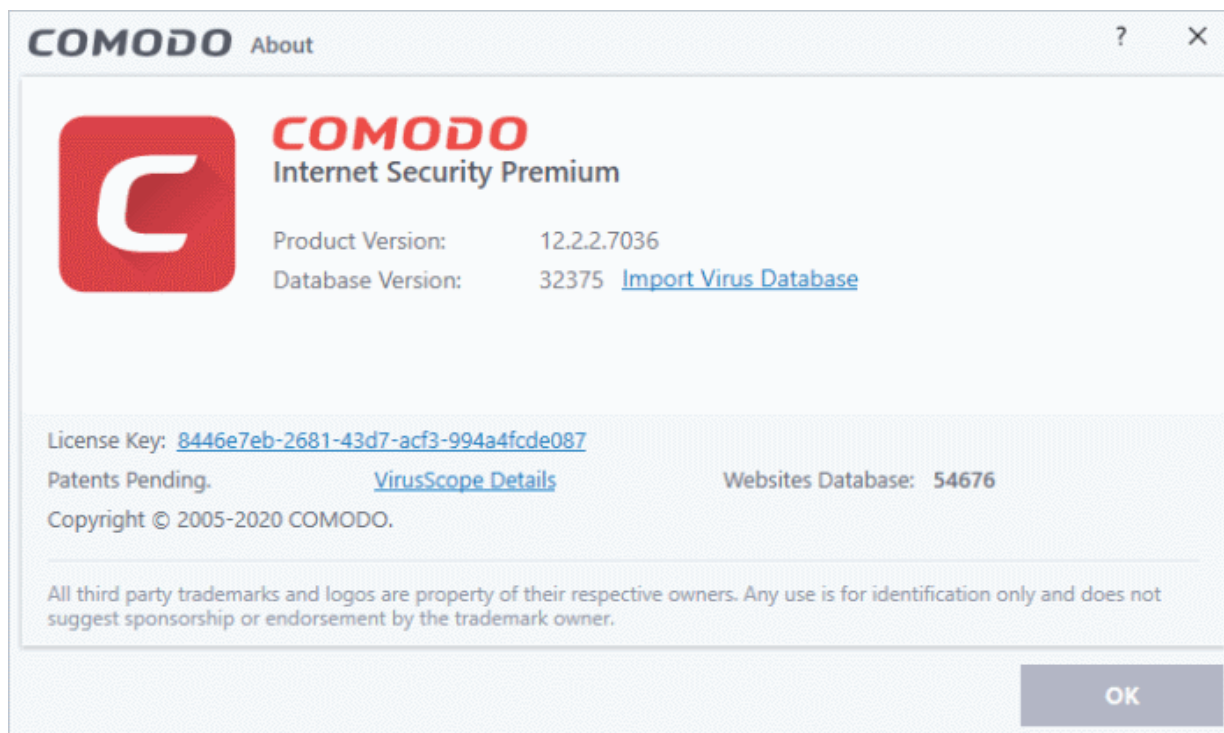
- Click 'Import Virus Database' link to import a locally stored virus signature database into CIS.
- Click 'Enter License Key' or the license key to upgrade to CIS 'Pro' or 'Complete'. See '**Activate CIS Pro/Complete Services**' for more details.
- Click 'VirusScope Details' to open a dialog which shows the VirusScope Recognizers that are active on your system. See '**VirusScope**' for more details.

Advanced Settings

- Click 'Settings' on the home screen

CIS default settings provide the highest levels of protection from the moment you install. The advanced settings area lets you modify all aspects of CIS. You can modify anything from simple preferences like the interface theme, right through to advanced tasks like custom firewall and containment rules.
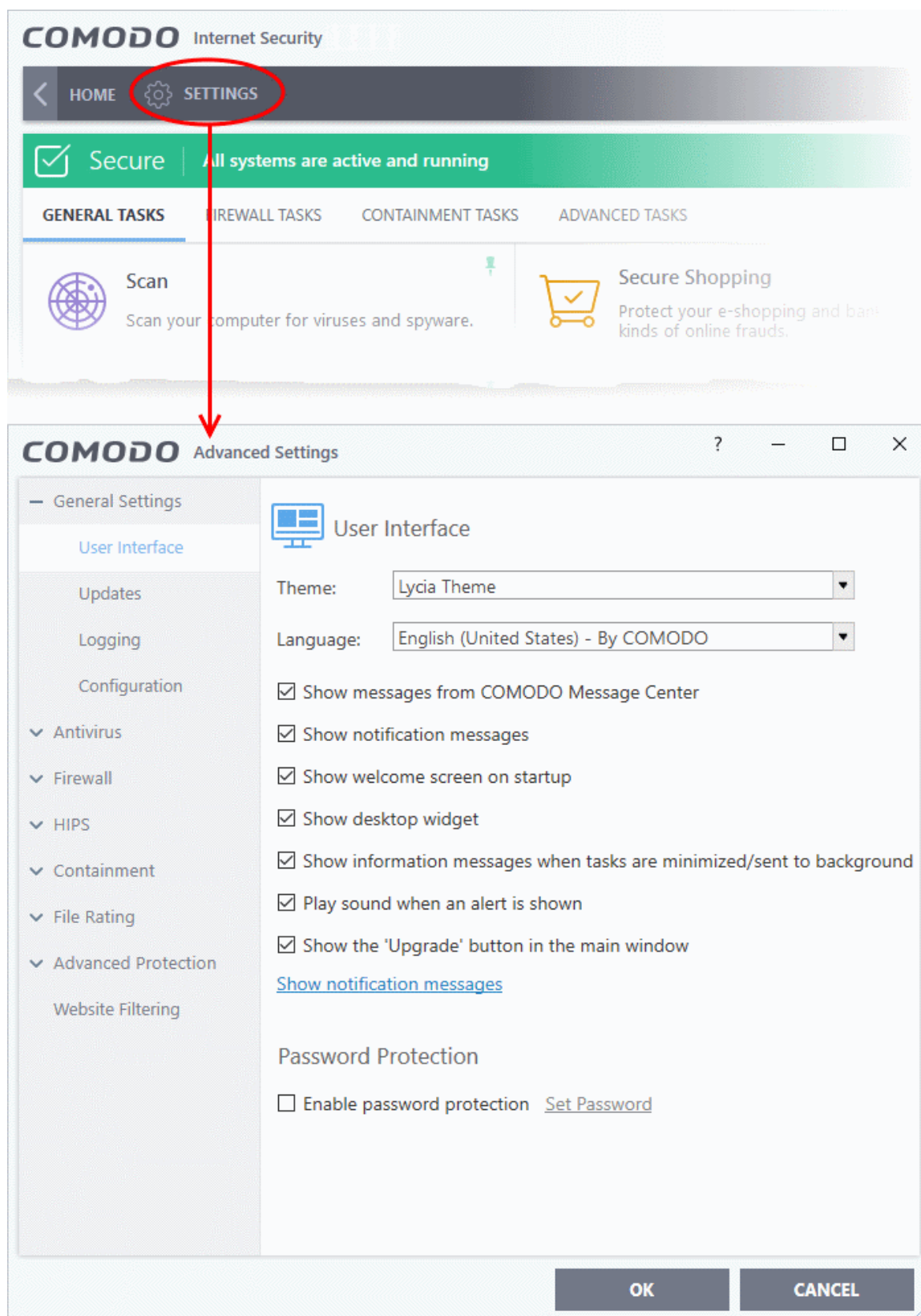
See '**CIS Settings**' for more details about configuring each of the components.

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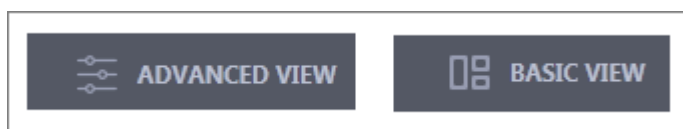
'**Title bar controls**', '**Advanced Settings**' and '**Silent Mode**' are common to both basic and advanced views.

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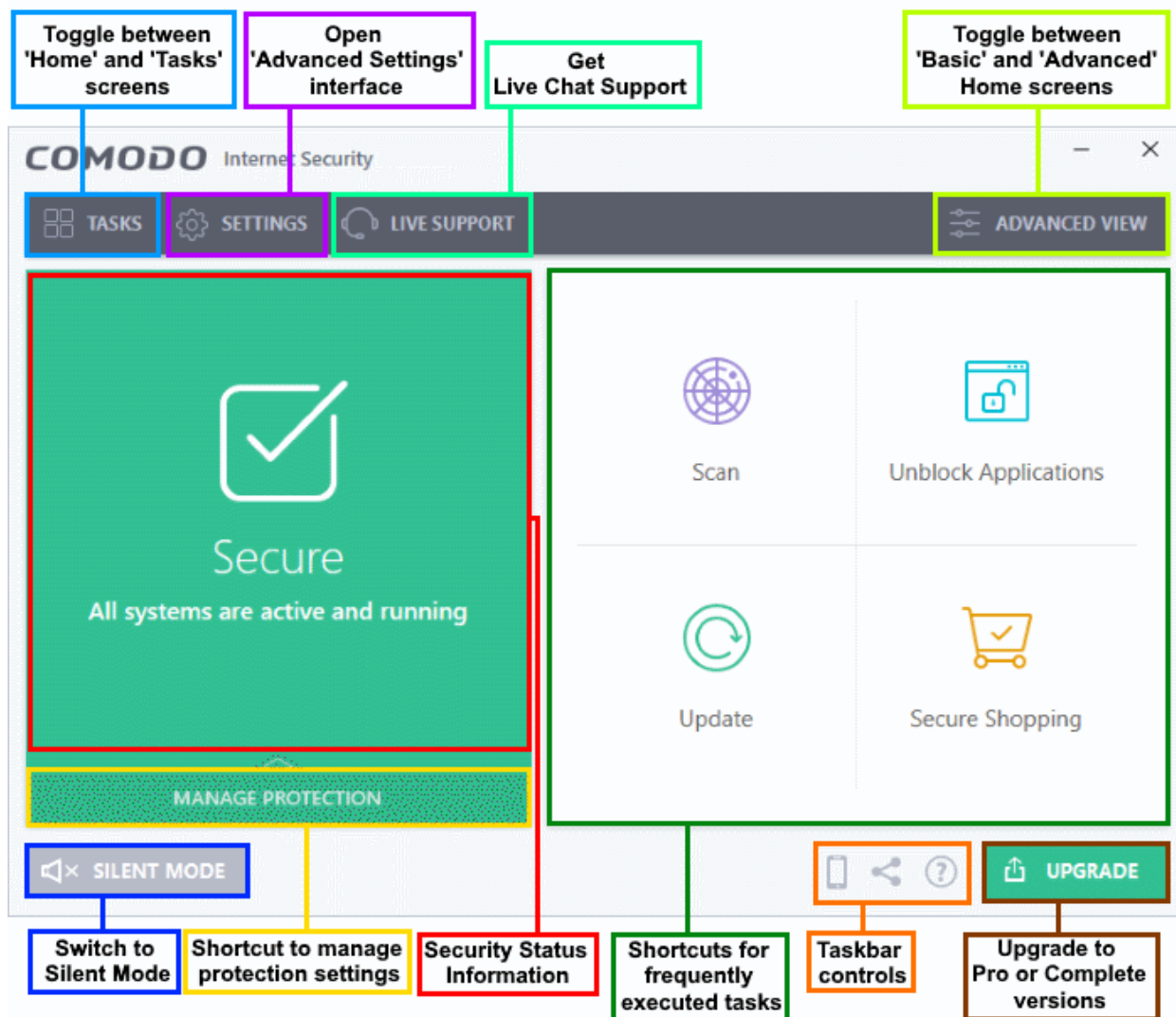
The security information tile on the left will inform you if any component is disabled or any if other problems are found:

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**

Add 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.
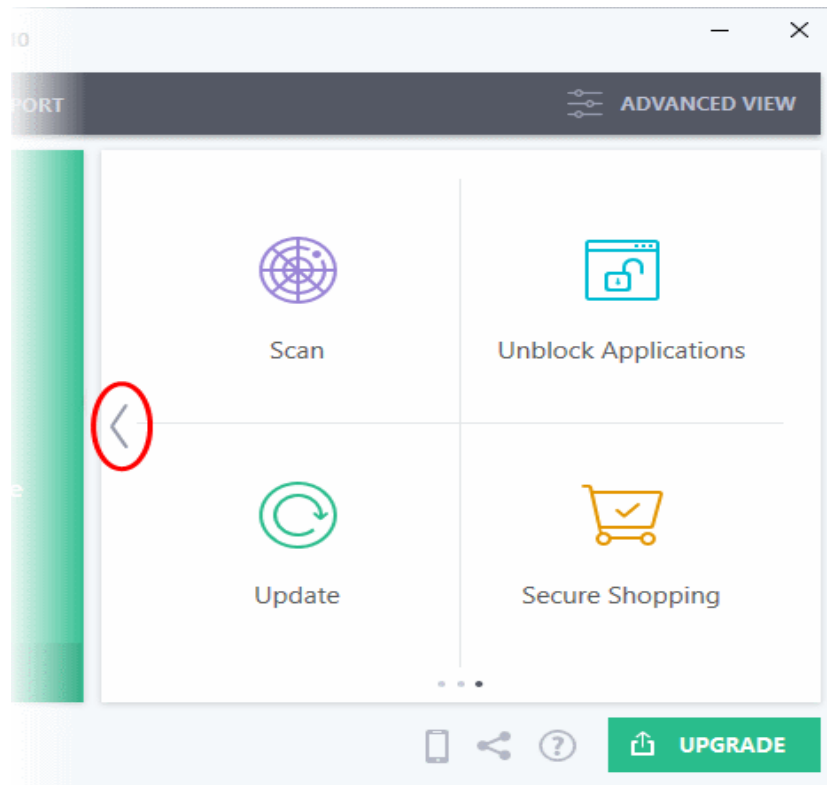
You can add tasks to this pane as follows:

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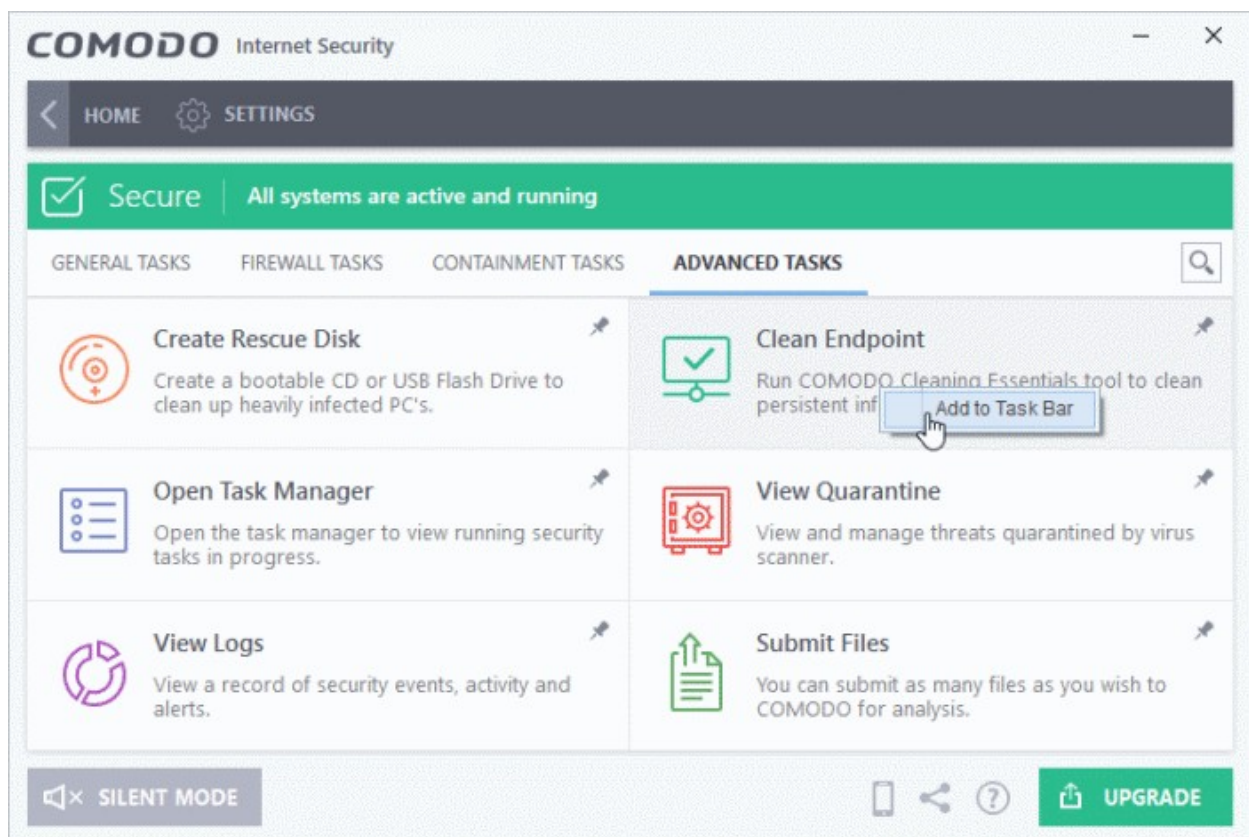
- Alternatively, you can add task shortcuts to the home screen by clicking the 'pin' button at the top-right

---

of any tile:
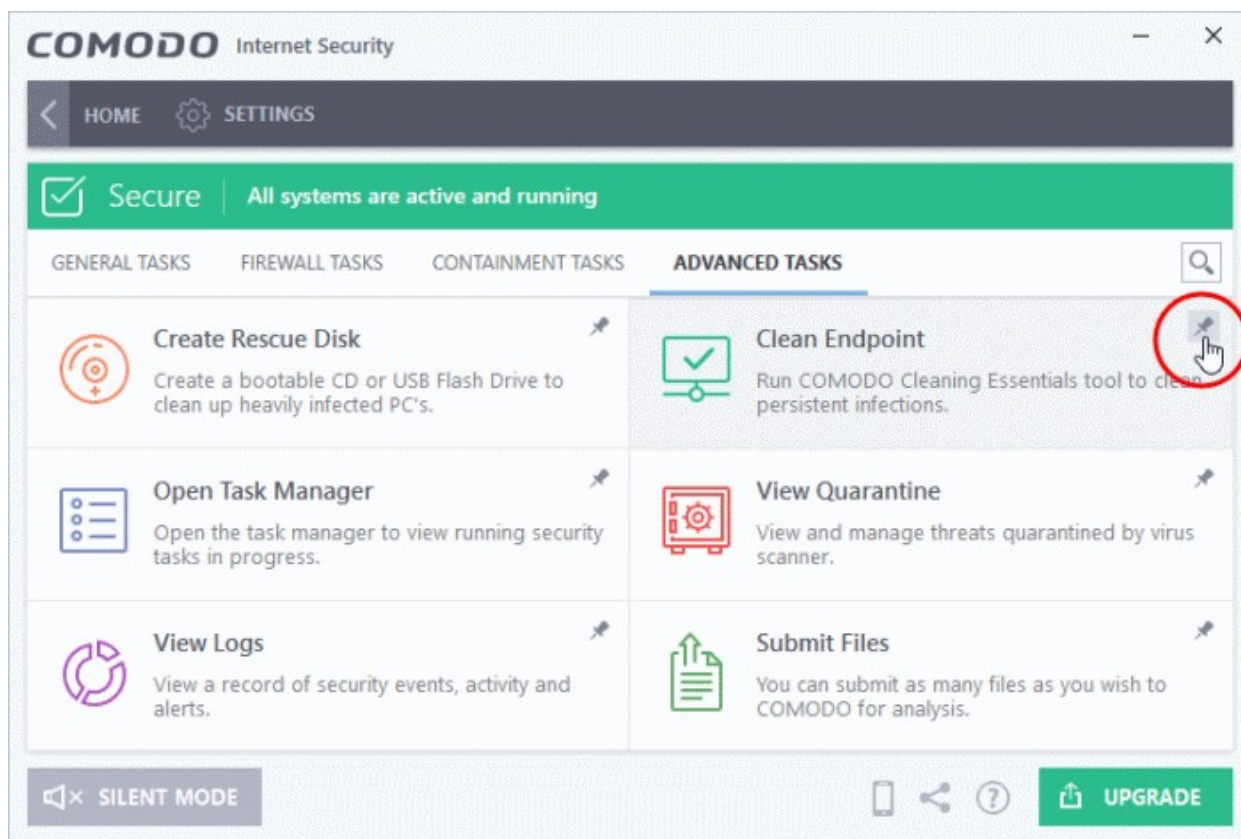
- The selected task will be added to the tasks pane.
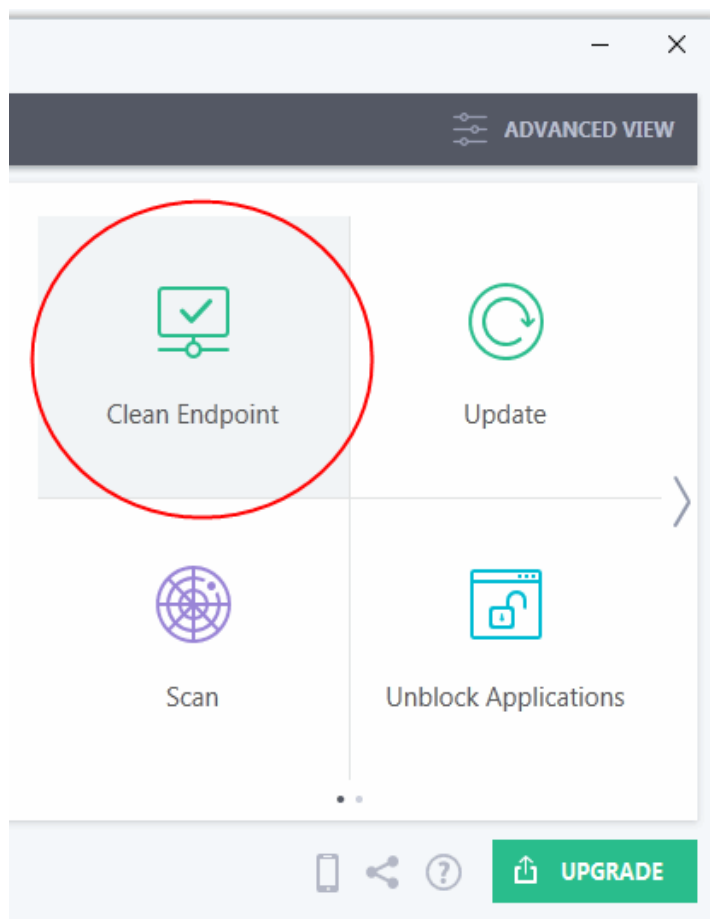
- To remove a task shortcut from the pane, right click on it and choose 'Remove from Task Bar'.
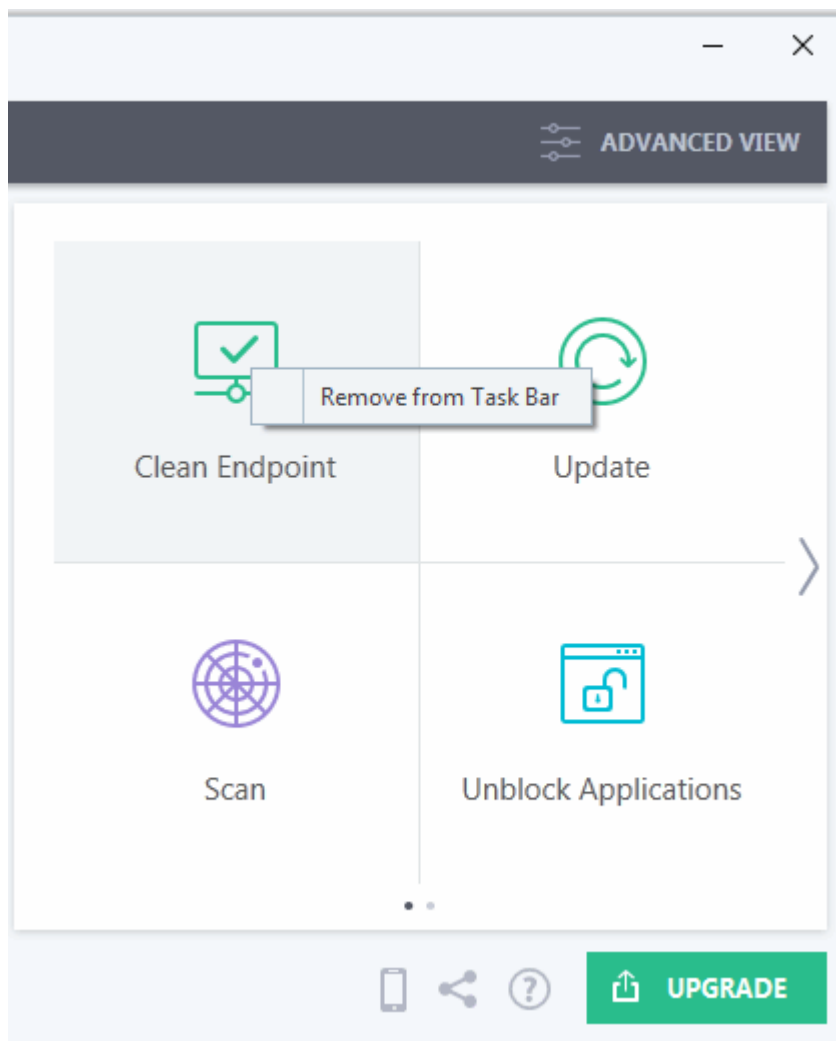
Manage Protection Settings

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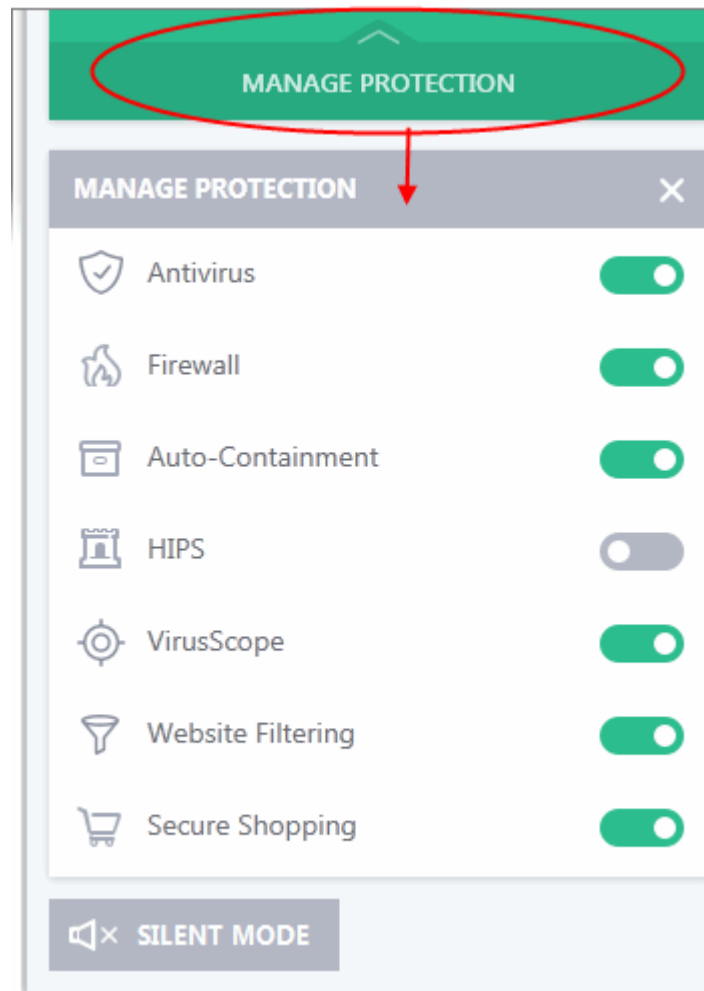
- Use the switch on the right to turn the protection on or off
- Click a component name on the left to open its 'Advanced Settings' screen

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.

- 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.

- Click the 'Advanced View' button at the top-right to switch to advanced view from basic view:
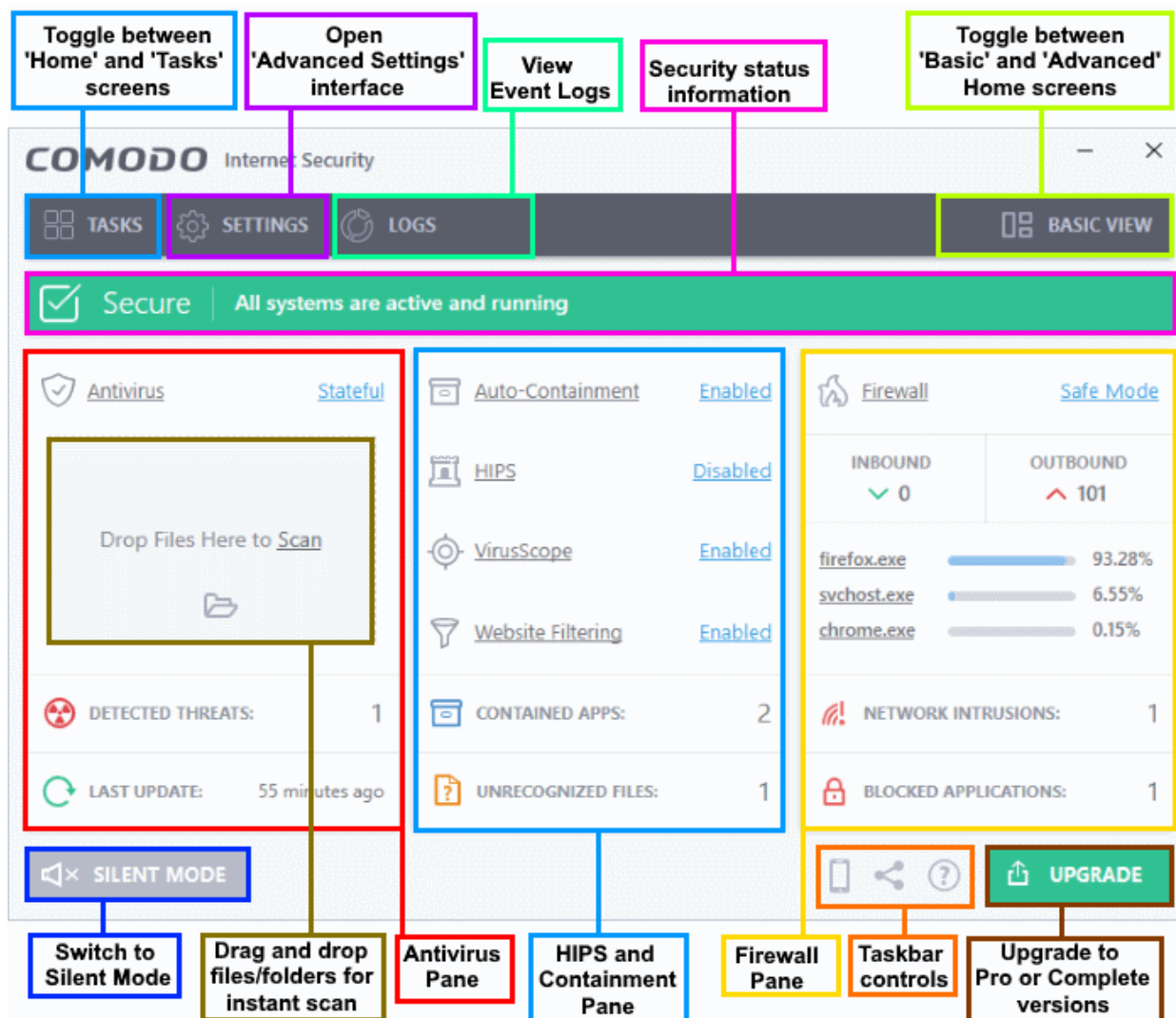
The following sections explain more about each pane:

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

Antivirus Pane

The antivirus pane lets you configure scan mode, instantly scan files and folders, and view virus database and log information.
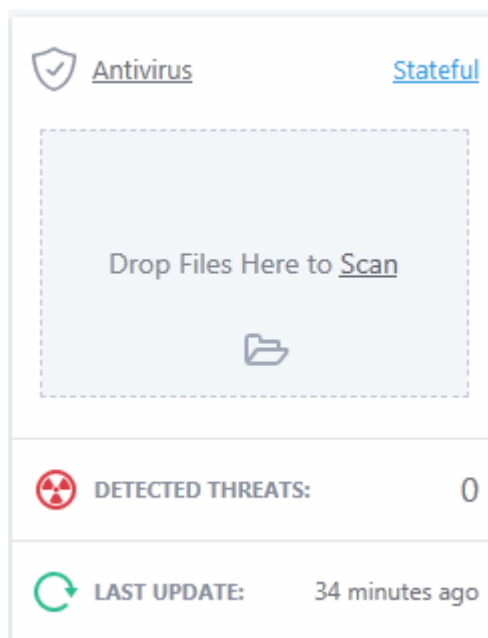
- **Antivirus** - The current security mode of the real-time antivirus scanner.
    - Click on the mode text to view and change mode.
    - Click 'Antivirus' to open the real-time scan settings interface.
    - See '**Real-time Scan Settings**' for more details.
- **Last Update** - Date of the most recent virus database update.
    - Click the text link to start the updates again.
- **Detected Threats** - The number of malware threats discovered so far from the start of current session as a link.
    - Click this number to open the **Antivirus Logs** panel.
- **Drop Files to Scan** - Drag-and-drop files, folders or drives into this box to instantly scan them. See '**Instantly Scan Files and Folders**' for more details.

HIPS and Containment Pane

This panel lets you quickly configure containment, host-intrusion, VirusScope and website filtering. The bottom of the panel shows the number of unrecognized files and contained applications.
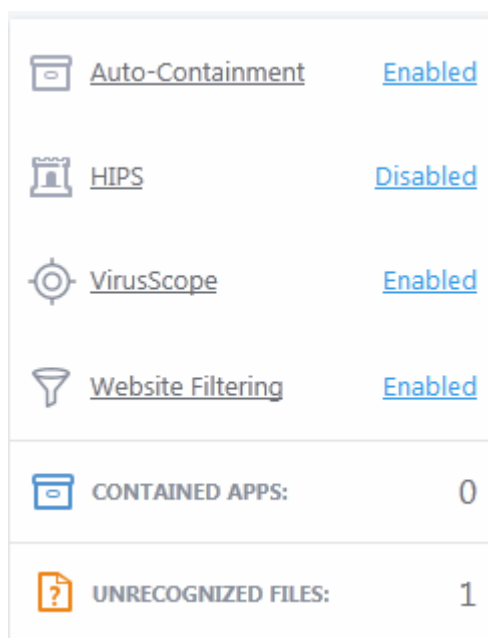
- **Auto-Containment** - If enabled, any files with an 'Unknown' trust rating will be automatically run in the container to prevent them from accessing other processes or your personal data. Unknown files are those that are neither 'known-malicious' nor 'known-safe'. Such files are run in the container 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** - 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** - The number of applications that are currently running inside the container.

  - Click the number to view a list of all processes running in the container. See '**View Active Process List**' for more details.

- **Unrecognized Files** - The number of files on your system that have an 'unrecognized' trust rating. Unrecognized files are those that are neither definitely safe (whitelisted) nor definitely malicious (blacklisted). Unrecognized files should be executed in the container until Comodo provides either a trusted or a malicious rating for them.

  - Click the number to open the 'File List' interface. See '**File List**' for more details.

Firewall Pane

The firewall pane shows the number of inbound and outbound connections, which applications are connected to the internet, and the number of intrusion attempts blocked in the current session.
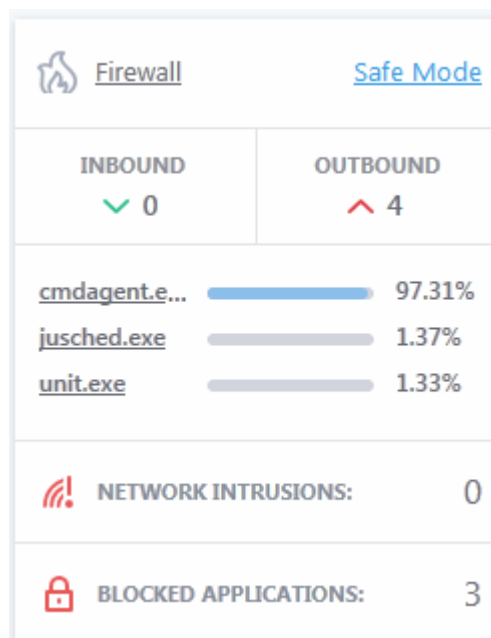
- **Firewall** - The current security mode of the firewall.

  - Click 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.

  - Click on the numbers to see the active internet connections from your computer. See '**View Active Internet Connections**' for more details.

- **Traffic** - Applications that are currently sending or receiving data over the network/internet.

  - Click the name of any application to open the **View Connections** screen.

- **Network Intrusions** - The total number of intrusion attempts blocked by firewall since the start of the current session.

  - Click the number to open the Firewall Logs screen. See '**Firewall Logs**' for more details.

- **Blocked Applications** - The number of applications that are not allowed to connect to the internet.
  - Click the number to view a list of all blocked applications. See **Configure internet access rights for applications** for more details.

Logs

- Click the logs link to view a list of all event logs saved by CIS. See '**View CIS Logs**' for more details.

Silent Mode

Silent mode lets use your system without interruptions or alerts from CIS. 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.

Switch to Silent mode

- Click the 'Silent Mode' button at the bottom-left of the home screen
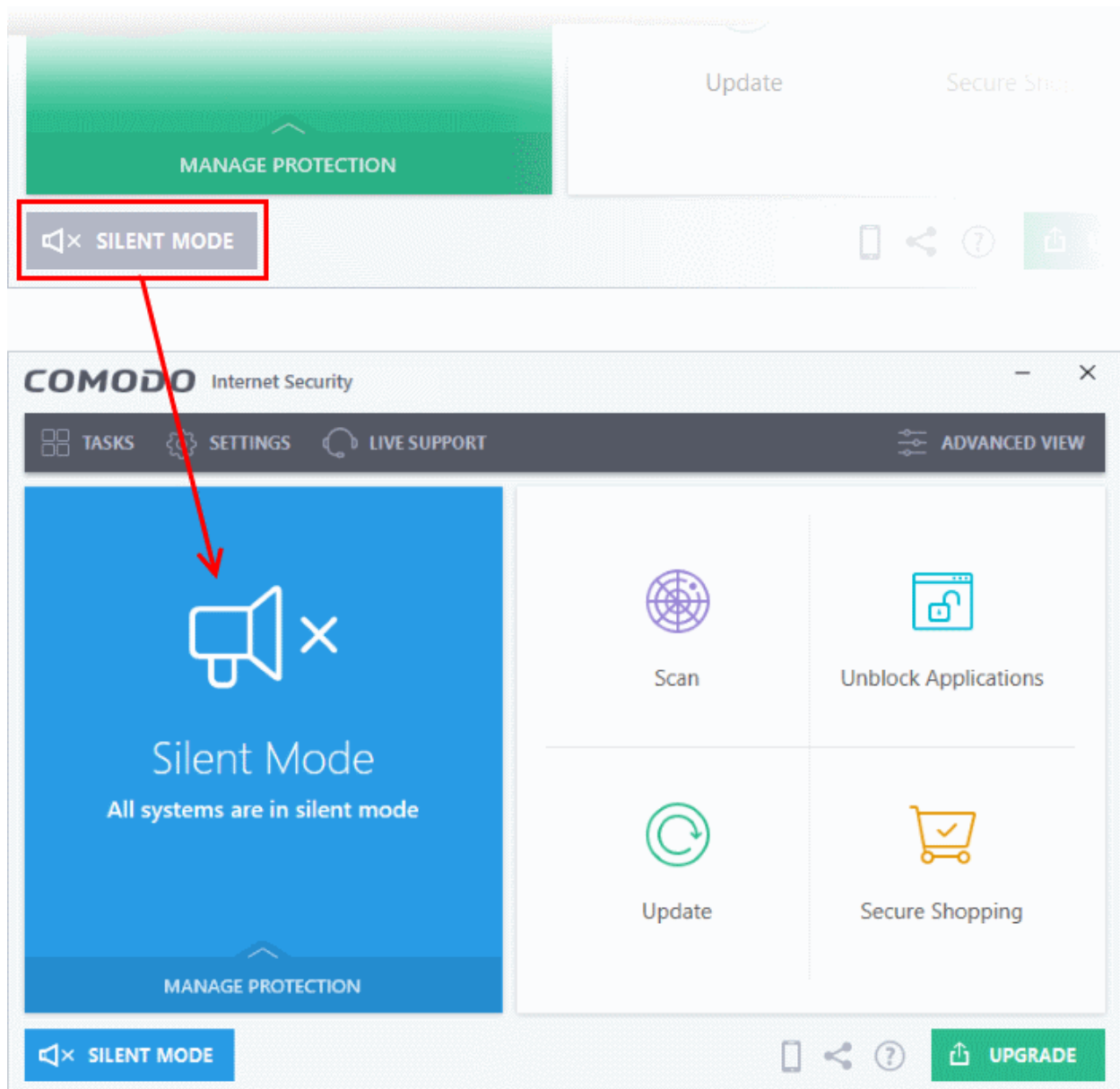
- Deactivate 'Silent Mode' to resume alerts and notifications.

Upgrade

- Click the 'Upgrade' button to place an order for CIS Pro or CIS Complete. Pro and Complete have additional features such as cloud backup, TrustConnect, product warranty and more.

1.4.2. The Tasks Interface

- Click 'Tasks' on the top-left of the home screen
- The tasks area lets you configure every aspect of Comodo Internet Security.
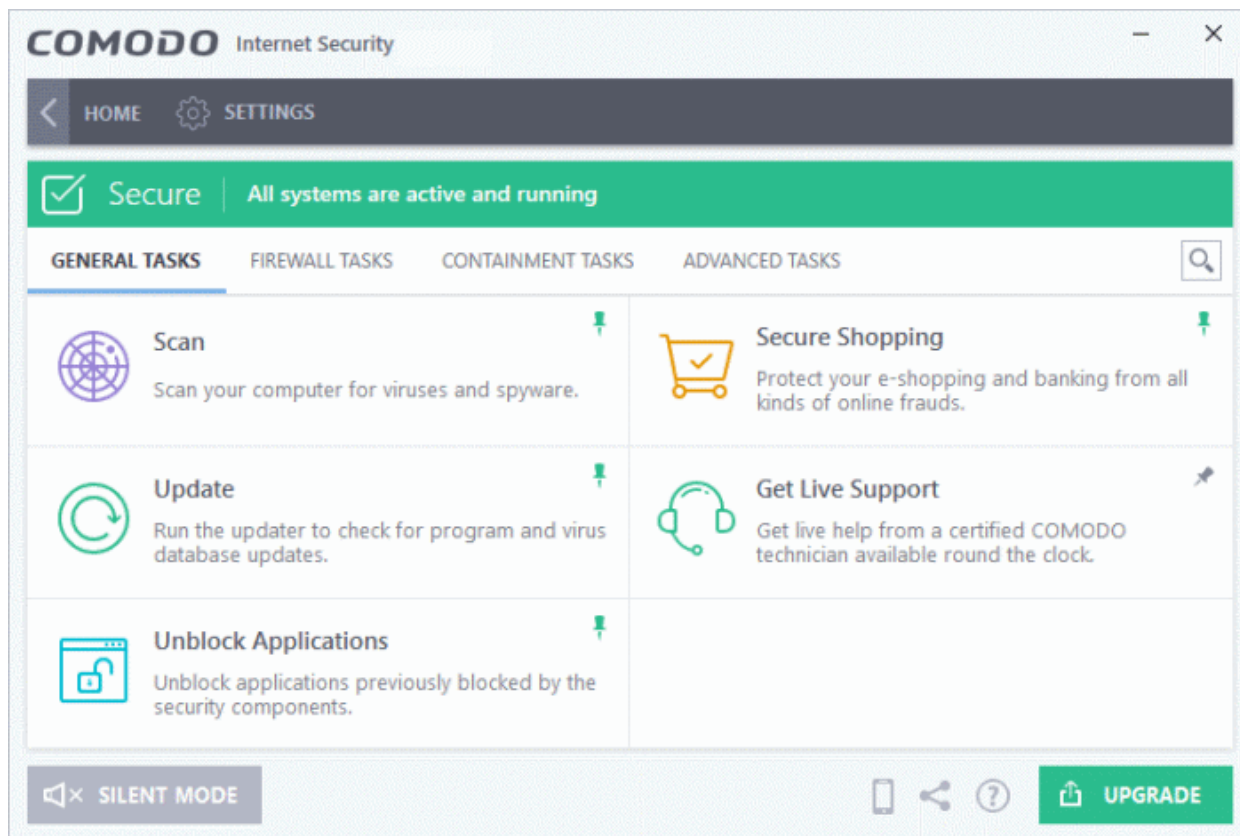
Tasks are broken down into four main categories. Click the following links for more details on each:

- **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 internet access for specific applications, manage networks, view active connections, and more. See '**Firewall Tasks**' for more details.
- **Containment Tasks** - Run applications in a secure virtual environment, start the virtual desktop, view active processes, and more. See '**Containment Tasks**' for more details.
- **Advanced Tasks** - Create a boot disk to clean highly infected systems, manage quarantined items, submit files to Comodo for analysis, and more. See '**Advanced Tasks**' for more details.

1.4.3. The Widget

- The CIS 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**.
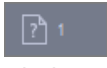
Note: If you can't see the widget, you can enable it as follows:
- Right-click on the CIS system tray icon then select 'Widget' > 'Show'
- Click 'Settings' > 'General Settings' > 'User Interface' > select 'Show desktop widget'

- Right-click on the widget 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.
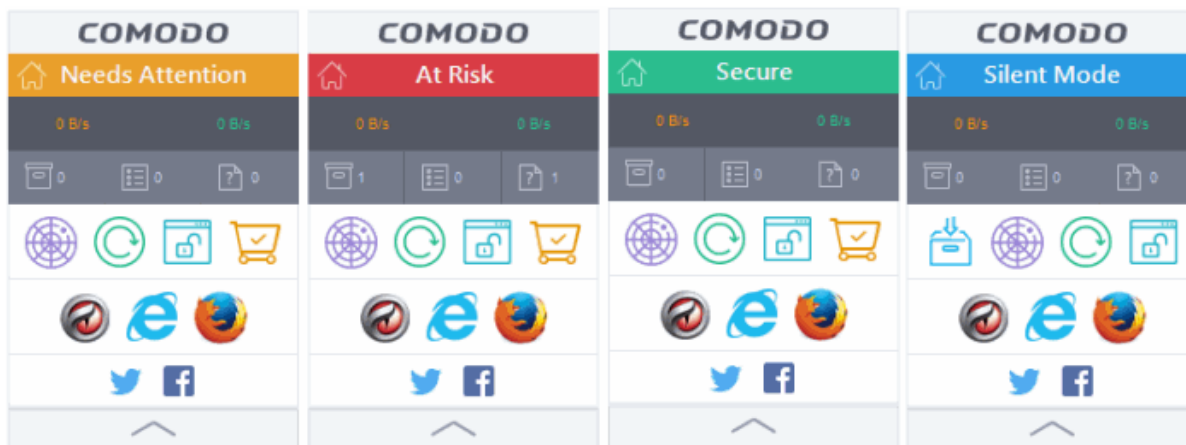
- The color coded row at the top of the widget displays your current security status.

    - Double-click 'At Risk' or 'Needs Attention' to view the recommended fixes.

- The second row shows incoming and outgoing network traffic. The network traffic row is only shown if 'Show Traffic pane' in widget options is enabled. See **The System Tray Icon** for more details. (*Default = Enabled*)

- The third row tells you about various CIS processes:

    - The first button [icon] shows the number of programs/processes that are currently running in the container.
        - Click the button to view a list of all processes running in the container.
        - See **View Active Process List** and **Identify and Kill Unsafe Processes** for more details.

    - The second button [icon] tells you how many CIS tasks are currently running.
        - Click the button to open the '**Task Manager**' interface.

    - The third button [icon] shows how many unrecognized files have been added to the **file list** and are pending submission to Comodo. Click the button to view a list of these files.

    The status row is only shown if 'Show Status Pane' is enabled in 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 only shown if 'Show Common Tasks Pane' is enabled in 'Widget' options. 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. You can tell the browser is running in the container because it will have a green border around it. See '**Run an application inside the container**' for more details.

    - The browsers row is only shown if 'Show Browsers Pane' is enabled in '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 shown if 'Show Connect Pane' is enabled in '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:
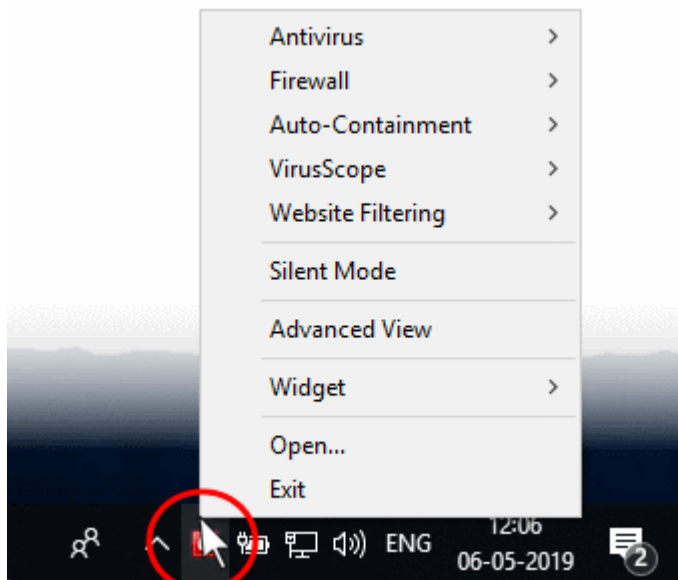
The options available for the Antivirus, Firewall, VirusScope, Auto-Containment, HIPS and Website Filtering menu-items depend on whether you are using **Basic View** or **Advanced View**.

Basic View	Advanced View
Antivirus - Enable or disable the real-time virus monitor.	**Antivirus** - Options available are 'On-Access', 'Stateful' and 'Disabled'. See Antivirus Pane for more details.
Firewall - Enable or disable the firewall.	• Click 'Settings' from the options to open the 'Realtime Scanner Settings' interface.
Auto-Containment - Enable or disable auto-containment. See '**Auto-Containment Rules**' for more details.	• See '**Real-time Scan Settings**' for more details.
VirusScope - Enable or disable VirusScope.	**Firewall** - Options available are 'Block All', 'Custom Ruleset', 'Safe Mode', 'Training Mode' and 'Disabled'.
Website Filtering - Enable or disable the website content filter.	• Click 'Settings' to configure firewall options.
	• See **Firewall Settings** for more details.
	Auto-Containment - Click 'Settings' from the options to open the auto-containment interface.
	• See **Auto-Containment Rules** for more details.
	HIPS - Options available are 'Paranoid Mode', 'Safe Mode', 'Training Mode' and 'Disabled'.
	• Click 'Settings' from the options to open HIPS settings.
	• See **HIPS Settings** for more details.
	VirusScope - Enable or disable VirusScope.
	• Click 'Settings' from the options to open the 'VirusScope' interface.
	• See **VirusScope Configuration** for more details.
	Website Filtering - Enable or disable website filtering.

	• Click 'Settings' from the options to 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:
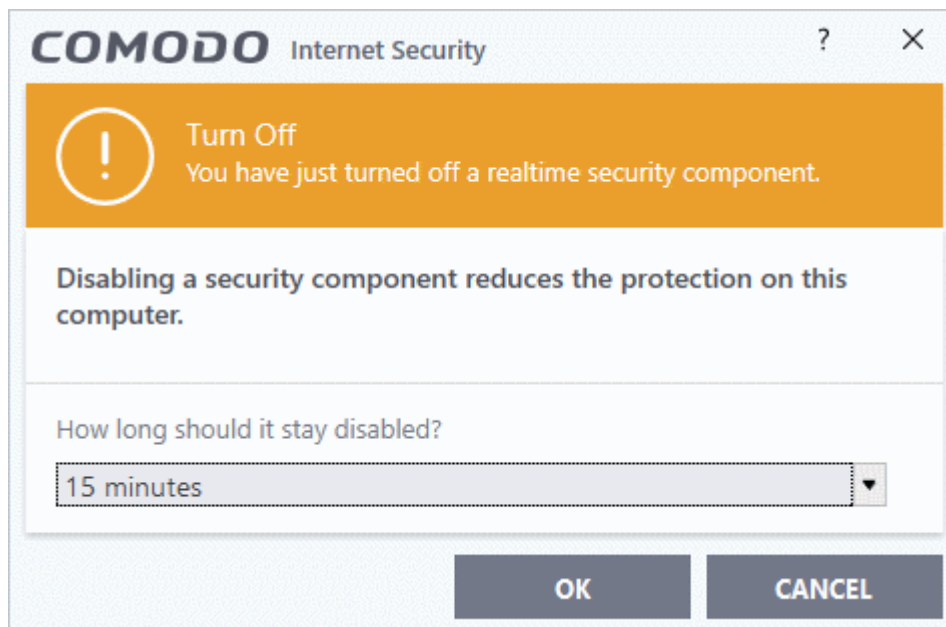
• Select the period and click 'OK'.

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:
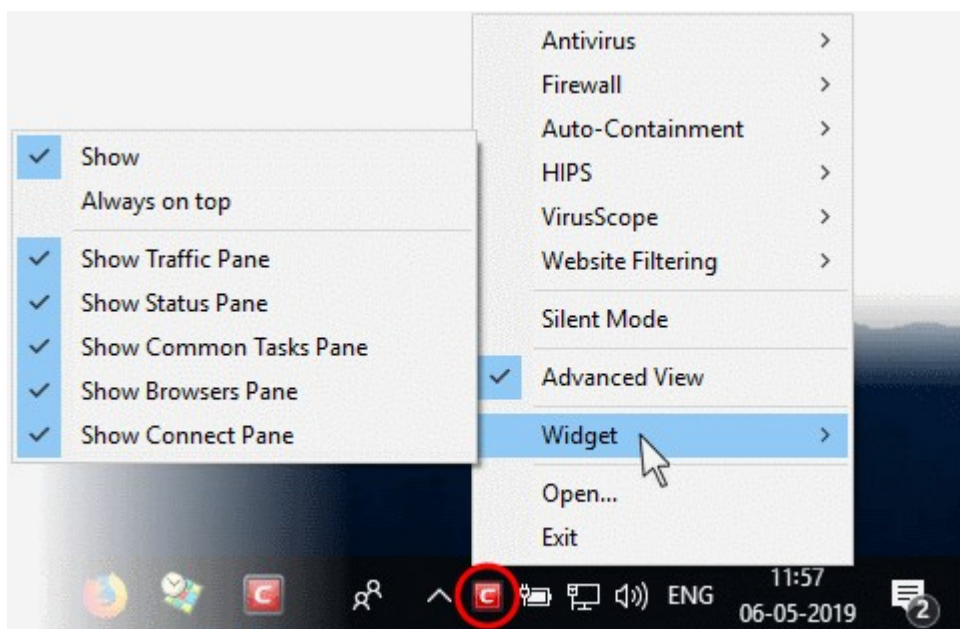
- **Show**: Toggles the widget between on and off (*Default = Enabled*)
- **Always on top**: Displays the widget on top of all windows currently running on your computer. (*Default = Enabled*)
- **Show Traffic Pane**: Displays the network traffic row on the widget. (*Default = Enabled*)
- **Show Status 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. Understand Security Alerts

- **Alerts Overview**
    - **Alert Types**
    - **Severity Levels**
    - **Descriptions**
- **Antivirus Alerts**
- **Auto-Scan 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**

- **File Rating 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

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**.

- **Auto-Scan Alerts** - Shown whenever an external storage device like a USB stick or an external hard disk drive is connected to your computer. Auto-scan alerts are shown only if '**Do not show auto-scan 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:
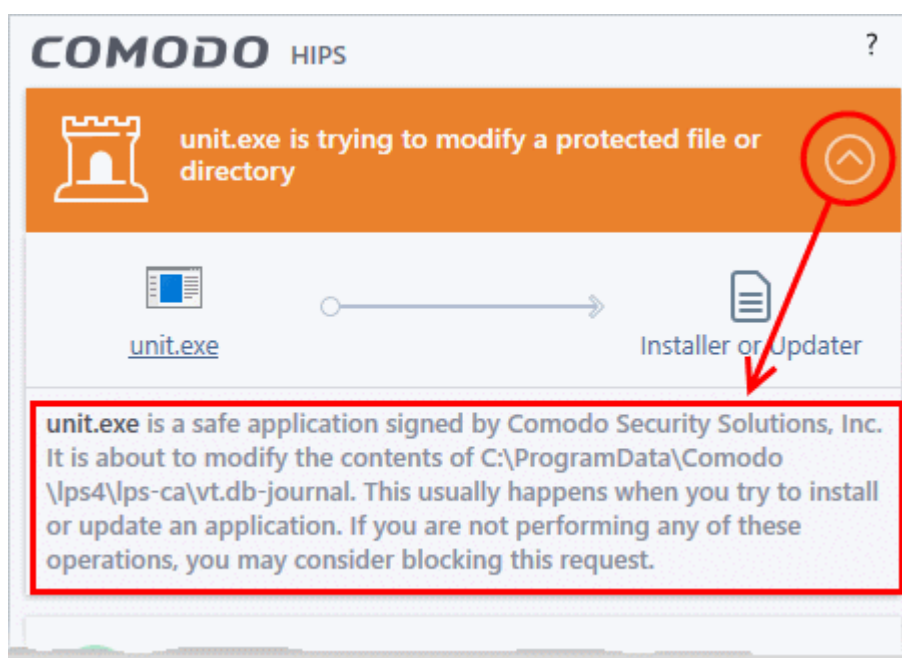
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answer 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.
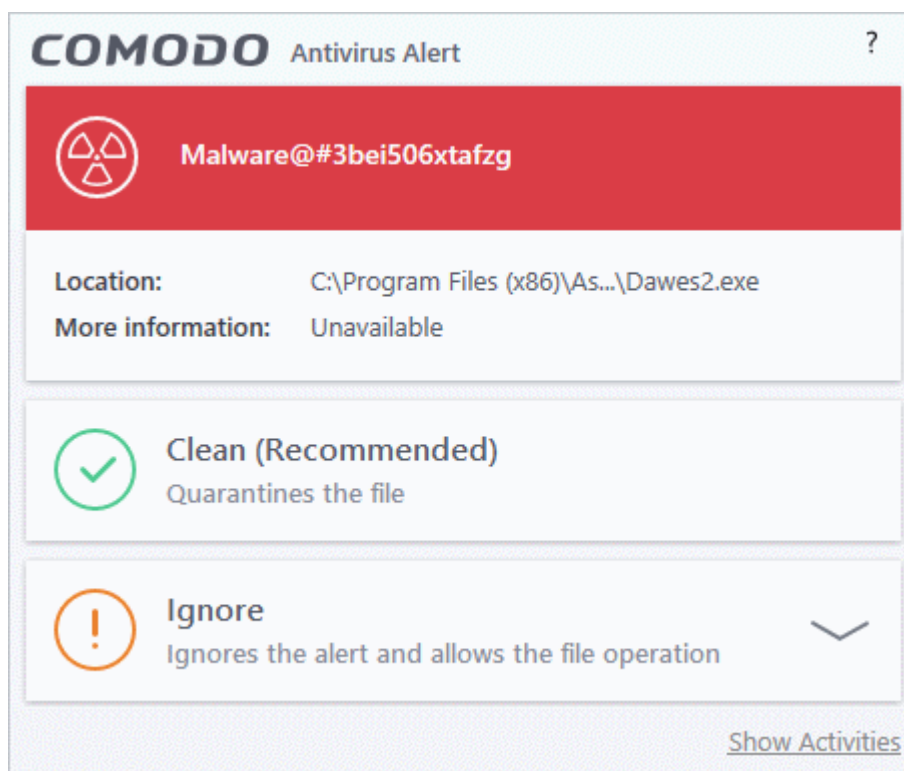
The following response-options are available:

- **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:
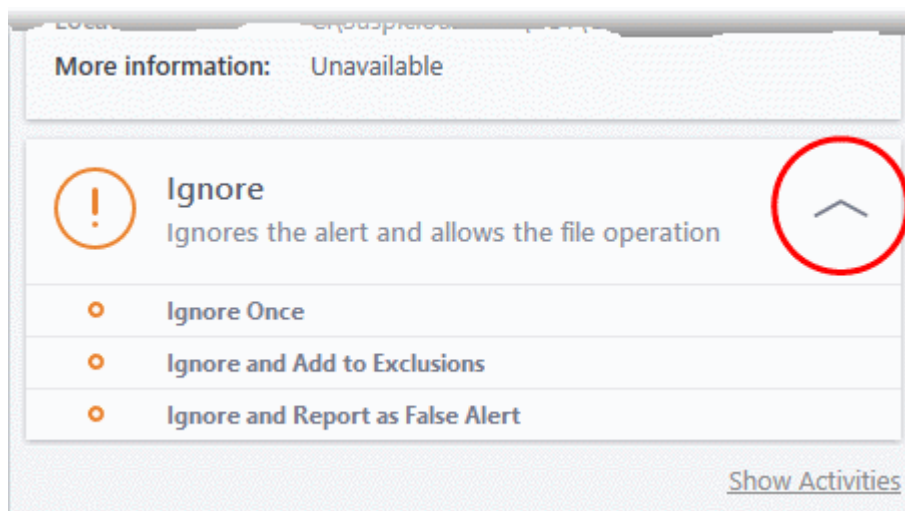
- **Ignore Once** -The file is allowed to run this time only. If the file attempts to execute on future occasions, another antivirus alert is displayed.
- **Ignore and Add to Exclusions** - The file is allowed to run and is moved to the '**Exclusions**' list - effectively making this the 'Ignore Permanently' 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:
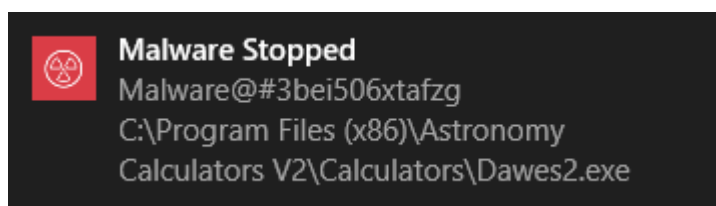
Please note that these antivirus notifications will be displayed only when 'Do not show antivirus alerts' check box in '**Antivirus**' > '**Real-time Scan settings**' screen is selected *and* 'Show notification messages' check box is enabled in '**Settings**' **>** '**User Interface**' screen.

Answer Auto-Scan Alerts

Auto-scan alerts appear when you plug a removable device into your computer (USB stick, portable HDD,etc). The alert asks you whether you want to scan the device for viruses.

These alerts are only shown if 'Do not show auto-scan alerts' is *disabled* in 'Settings > Antivirus > Realtime Scan'. See **Real-time Scan Settings** if you want to read more.
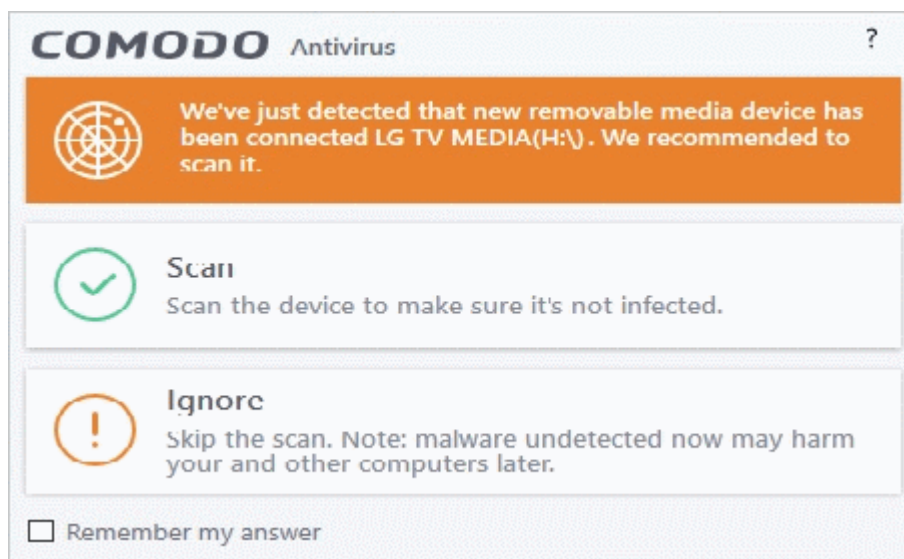
- **Scan** - CIS checks the device for viruses using the settings in the 'Manual Scan' profile. If this is not available then the scan uses the settings in the 'Full Scan' profile.
- **Ignore** - The device is not scanned
  - **Remember my answer** - CIS will automatically carry out your choice of scan or ignore when the device is connected in future. This only applies to the specific device. You will still see an alert if you connect a different device.

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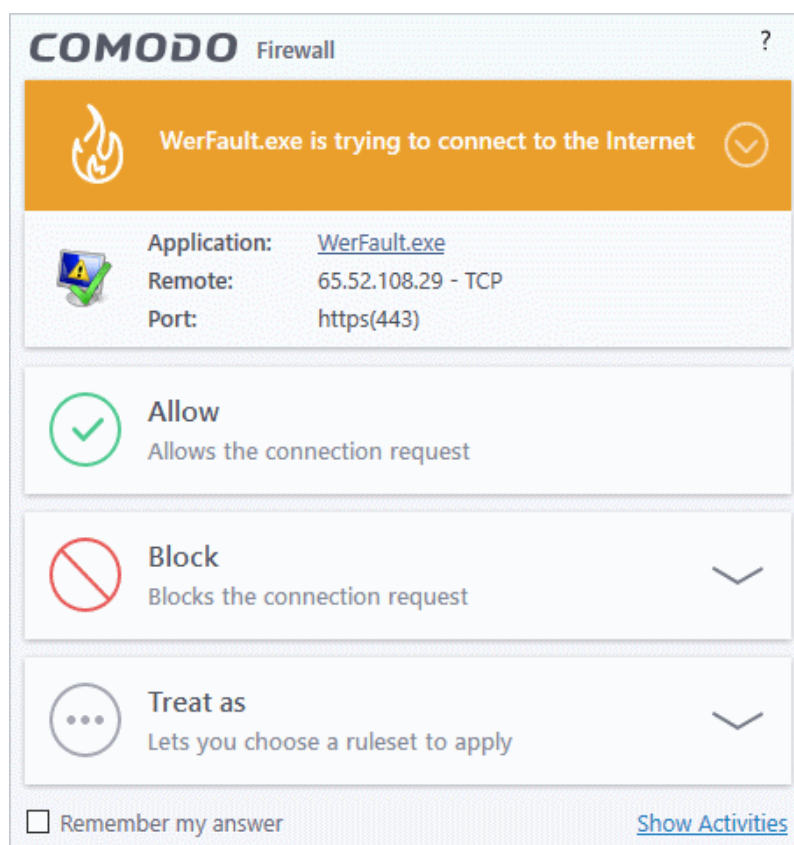
Tip: Clicking the 'Show Activities' link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

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.
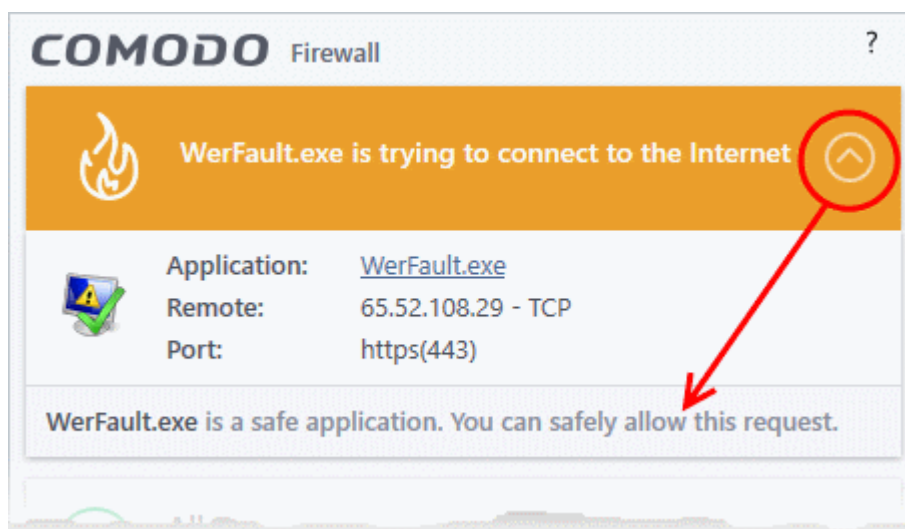
1. Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security 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:
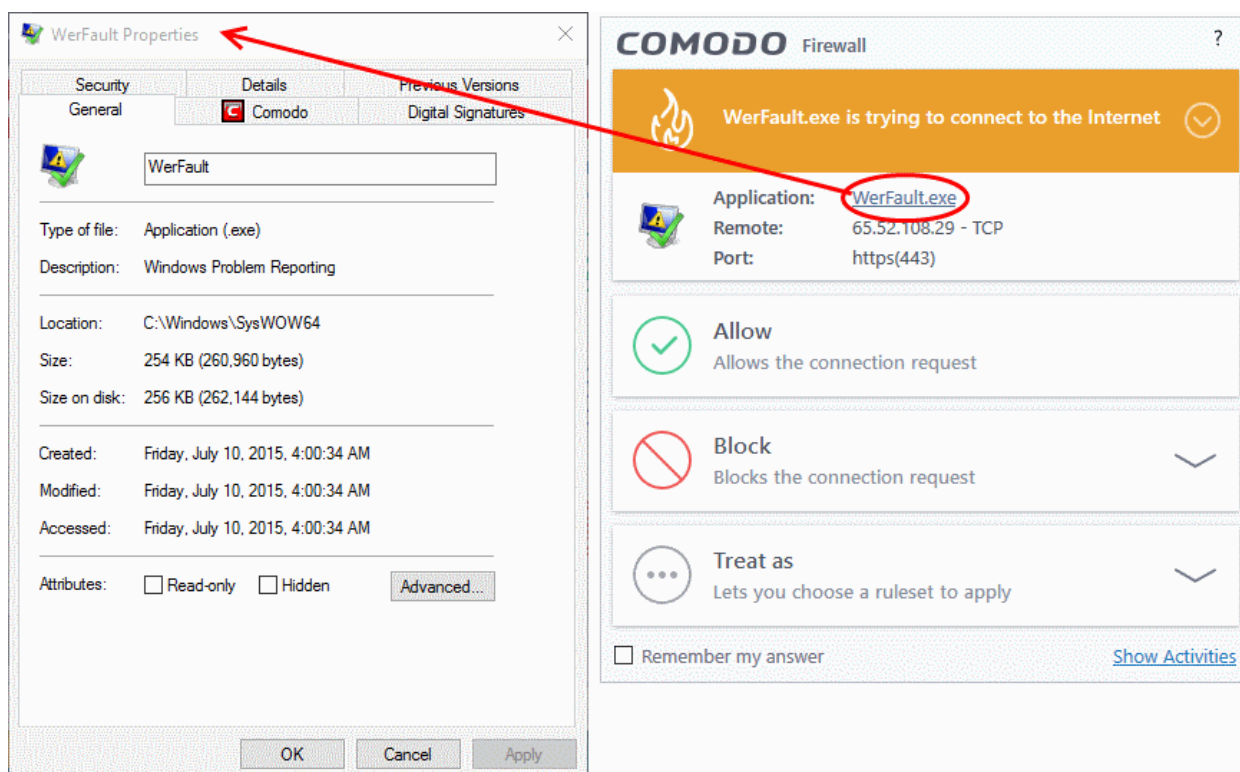
If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand the alert, you can choose to 'Block' the connection (connection is not allowed to proceed), 'Block and Terminate' (connection is not allowed to proceed and the process/application 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).
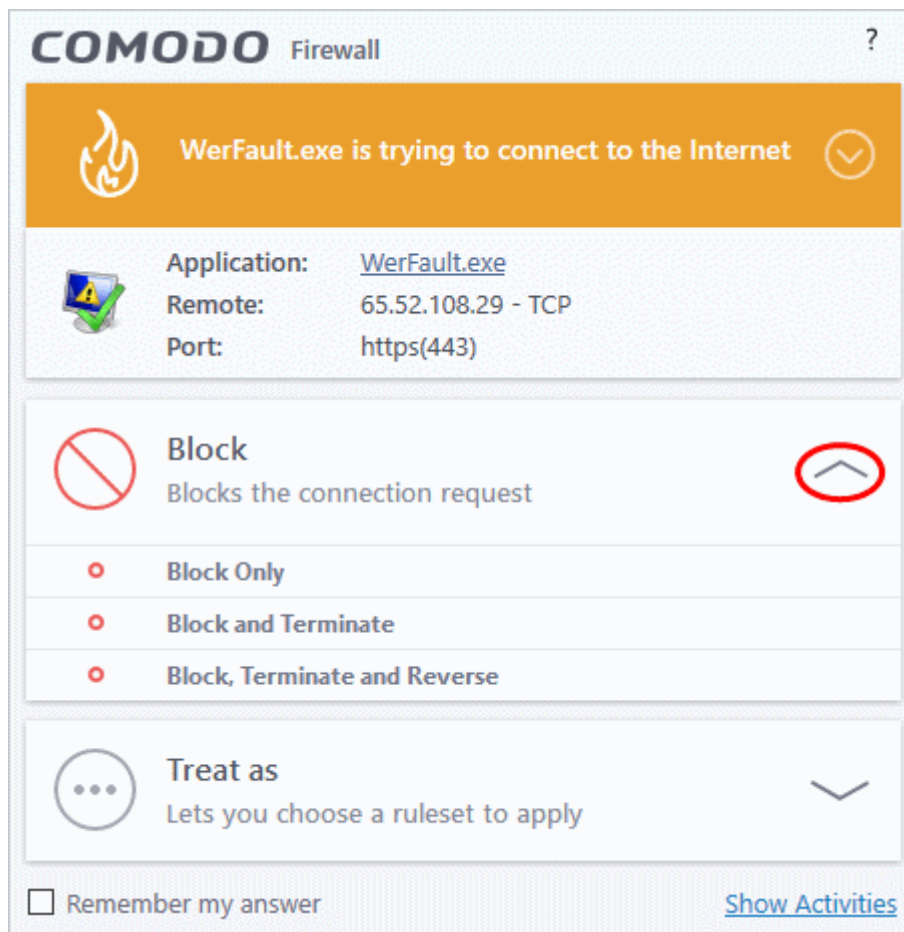
Note: 'Block, Terminate and Reverse' option will be available only if VirusScope is enabled under '**Settings**' **>** '**VirusScope**'. Also, if none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the 'Block, Terminate and 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.
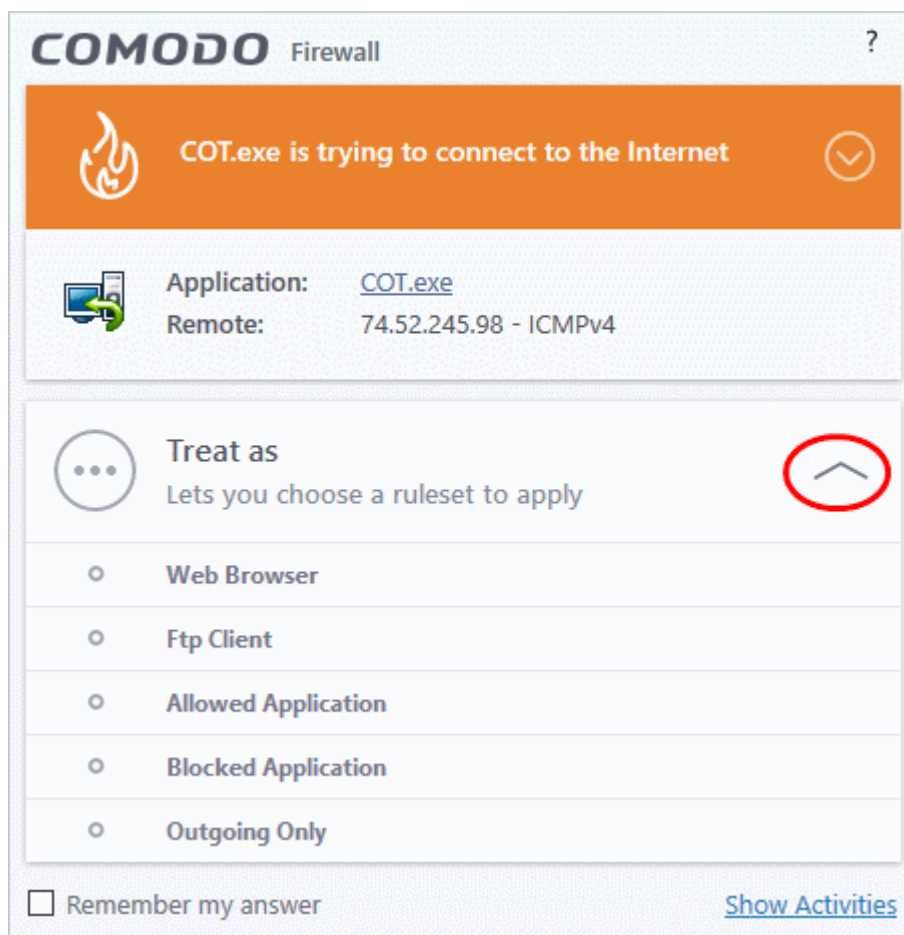
Remember to select '**Remember My Answer**' for ruleset to be created for the application and applied in future.

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.

Answer 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:

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.

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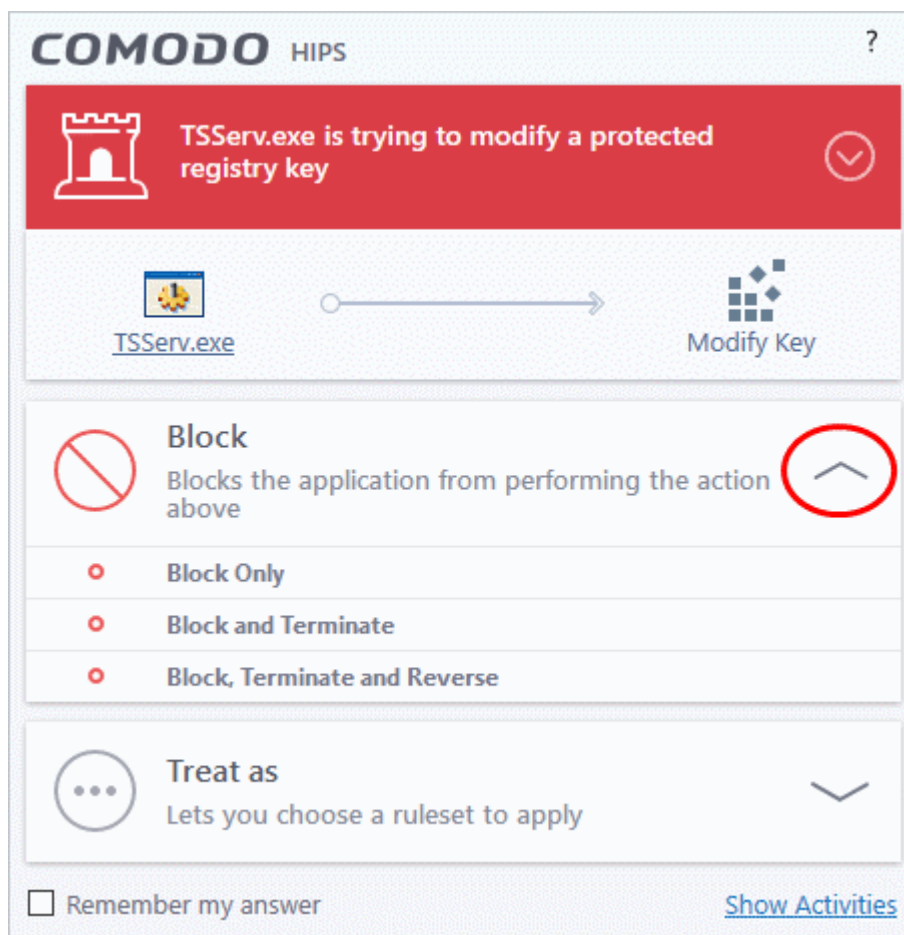
> **Note**: 'Block, Terminate and Reverse' option will be available only if VirusScope is enabled under '**Settings**' **>** '**VirusScope**'.

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.
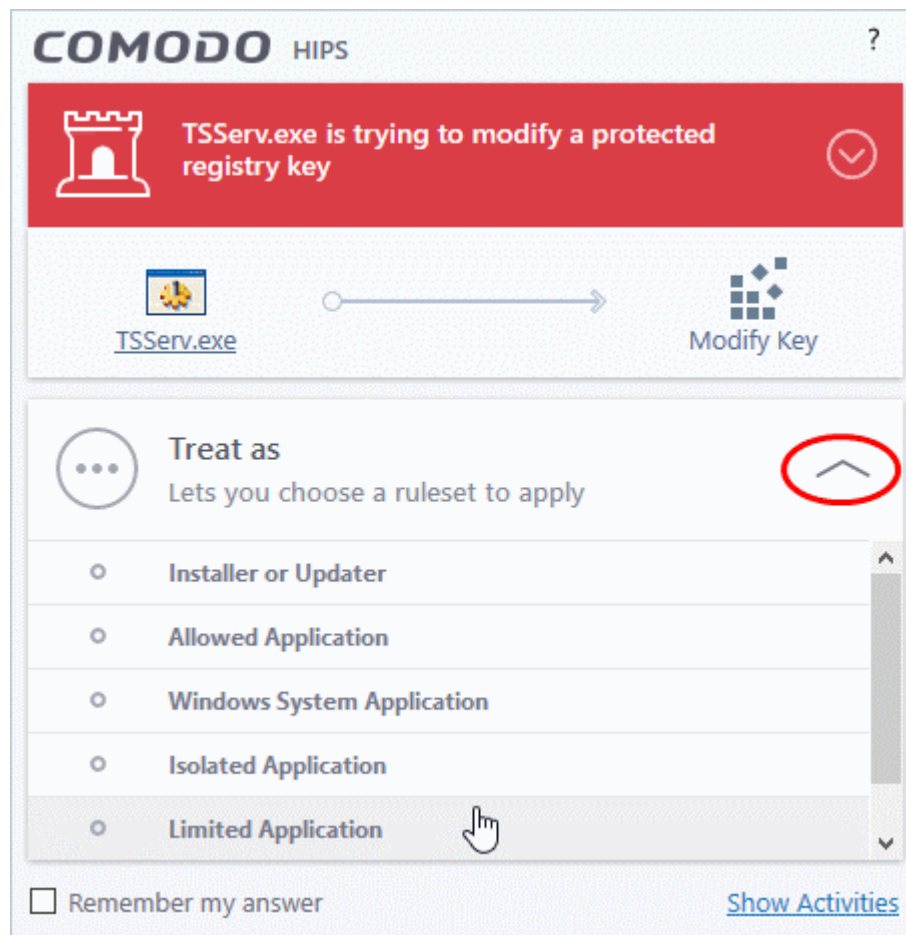
Avoid using the '**Installer or Updater'** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you 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.
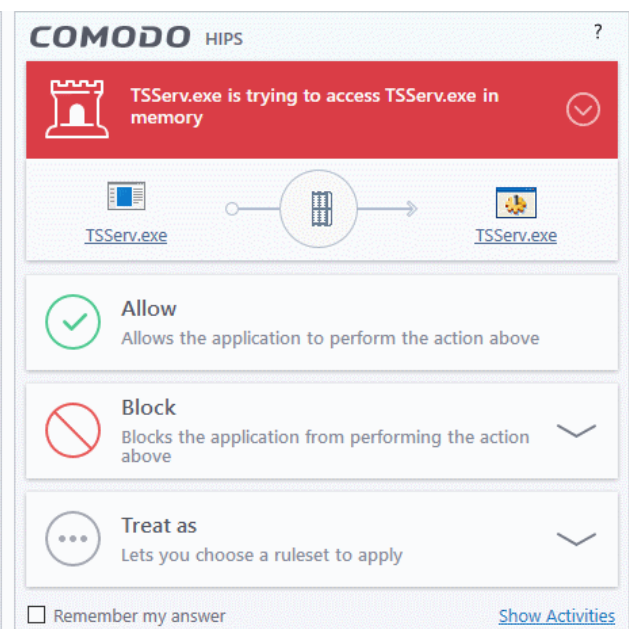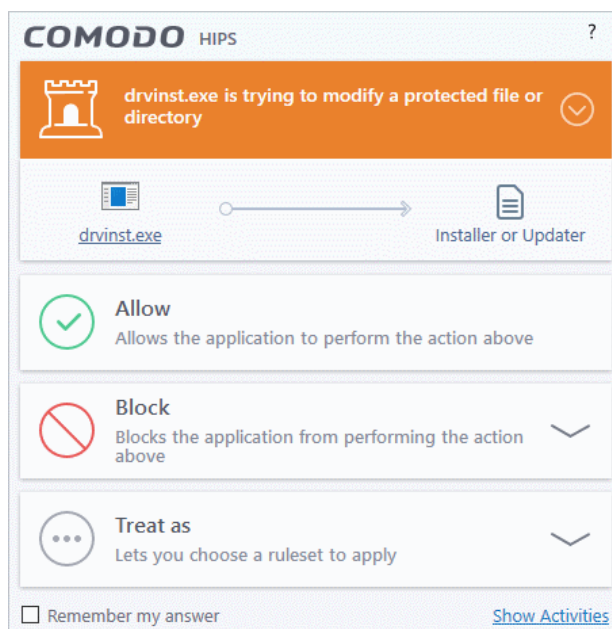
4. '**Protected Registry Key**' Alerts usually occur when you install a new application. If you haven't been installing a new program and do not recognize the application requesting the access , then a 'Protected Registry Key Alert' should be a cause for concern.
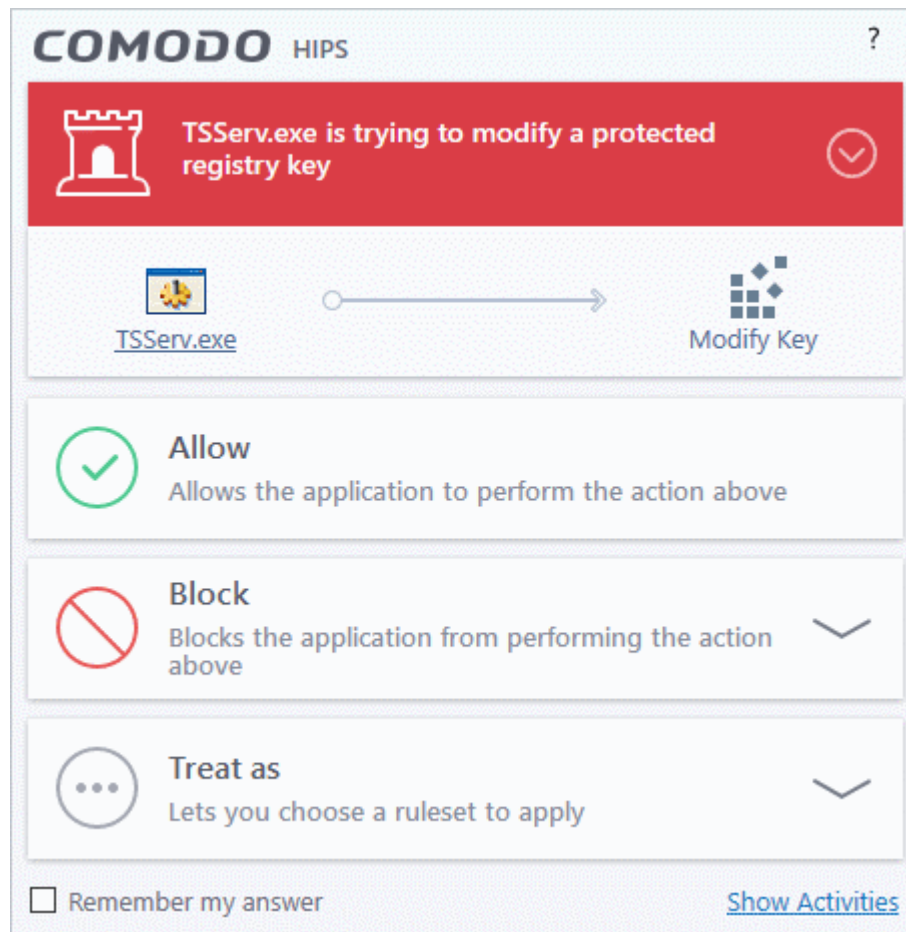
5. '**Protected File Alerts**' usually occur when you try to download or copy files or when you update an already installed application.
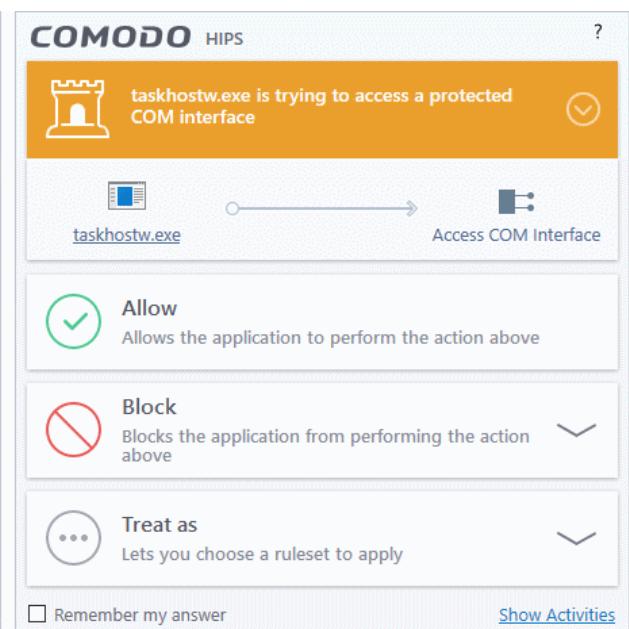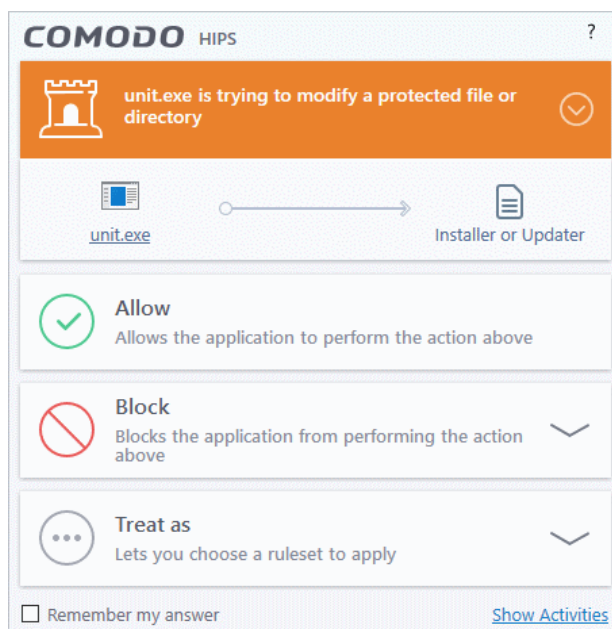
Were you installing new software or trying to download an application from the Internet? If you are

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.

Answer 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:
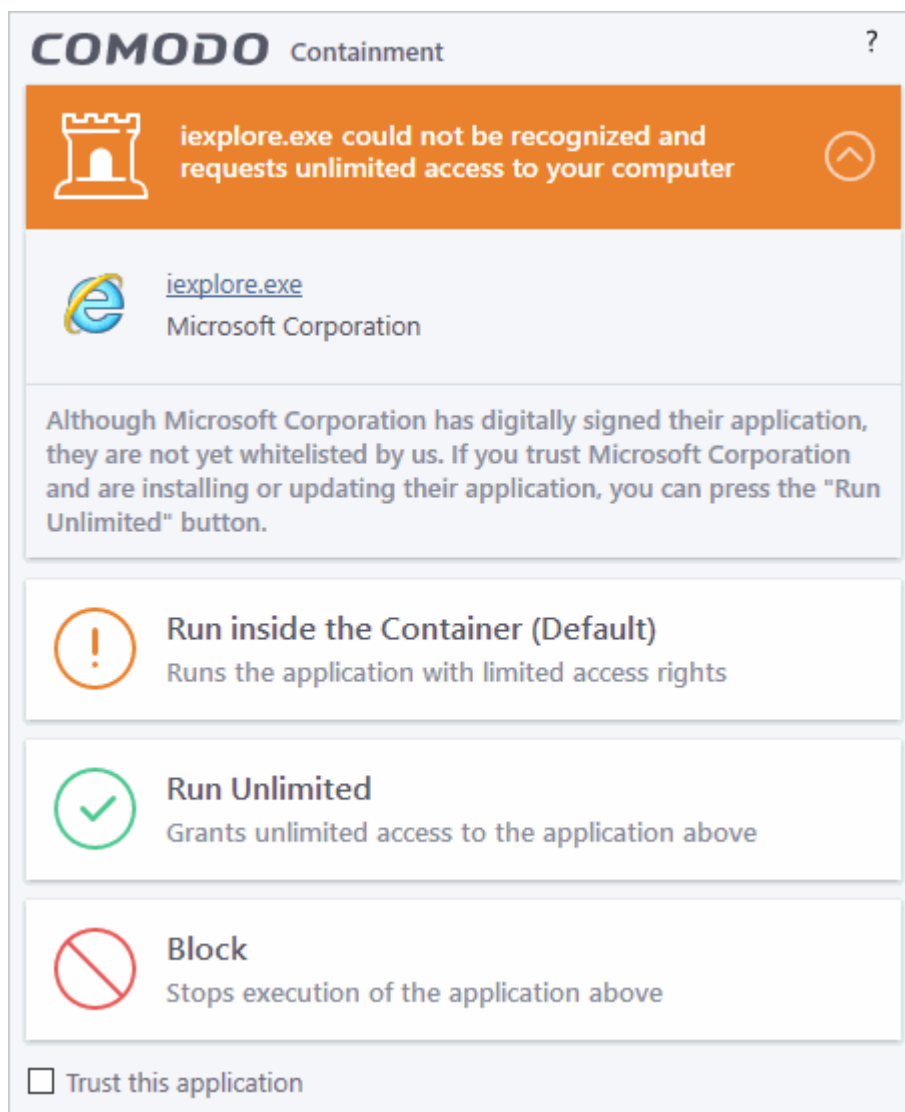
1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Internet Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe to proceed. Similarly, if the application is unknown and cannot be recognized, you are informed of this.
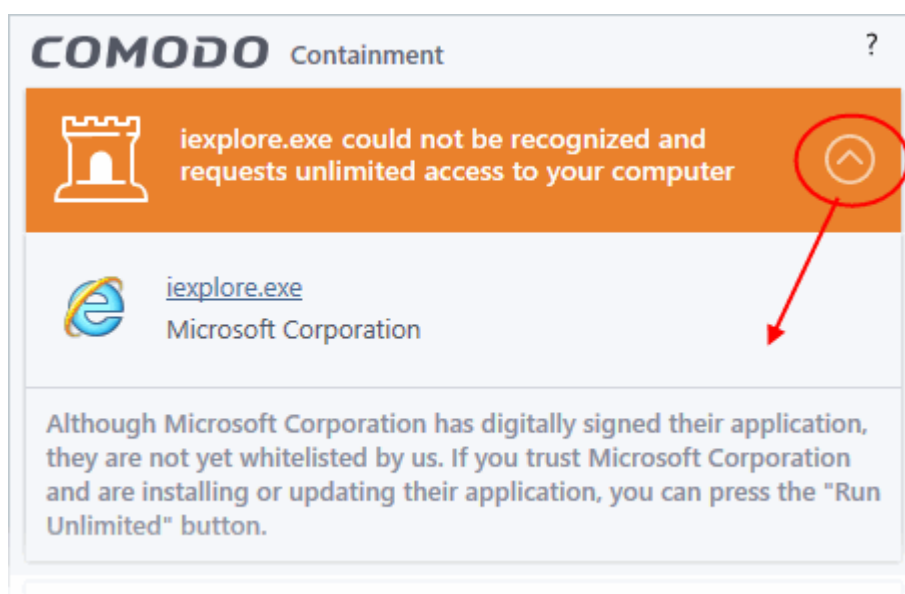
- If you are sure that the application is authentic and safe and you simply want it to be allowed to continue then you should select **Run Unlimited**. If you want the application not to be monitored in future, select 'Trust this application' checkbox. The application will be added to **Trusted Files** list.
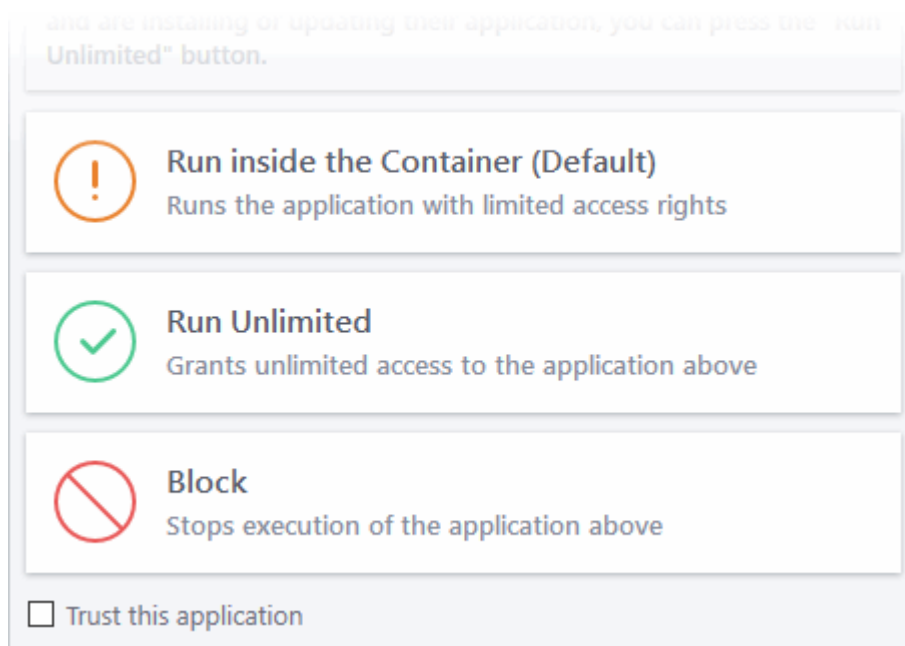
- If you are unsure of the safety of the software, then Comodo recommends that you run it with limited privileges and access to your system resources by clicking the 'Run Isolated' button. See '**Unknown Files: The Scanning process**' for more explanations on applications run with limited privileges.
- 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').
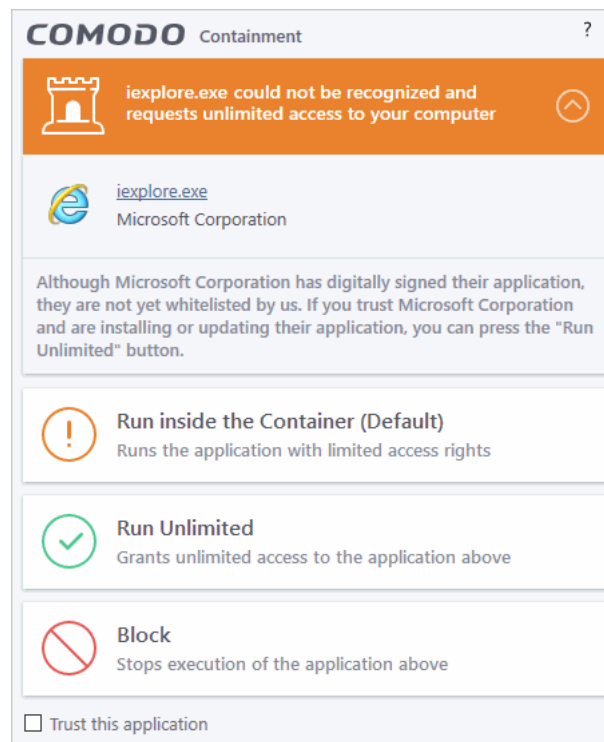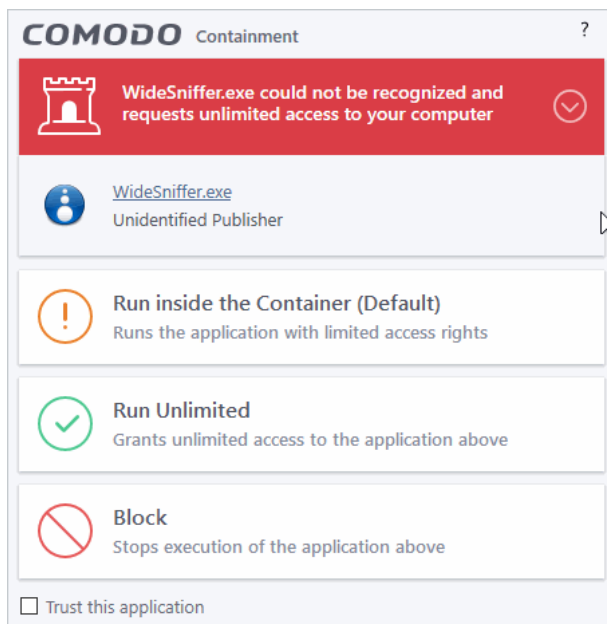
Unknown and not digitally signed   **Unknown and digitally signed but the publisher not yet whitelisted (Not yet a 'Trusted Vendor')**

- 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.
- '**Vendors List**' - for an explanation of digitally signed files and trusted software vendors.

Containment Notification

A notification will be shown when an application is automatically run inside the container by the auto-containment rules.
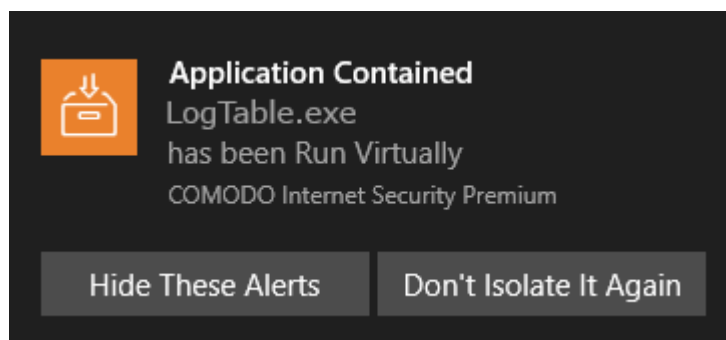
- **Hide These Alerts** - CIS will not show containment alerts if the same application is auto-contained in future.
- **Don't Isolate It Again** - An 'Ignore' rule is added for the application in the Auto-Containment rules. The application will not be auto-contained in future. See **Auto-Containment Rules** for more details.

Answer File Rating Alerts

CIS checks a file's trust rating on our cloud severs as part of a real-time scan. The software can generate alerts when it finds a file with an 'Unrecognized' or 'Malicious' rating.

You will these alerts if you have disabled 'Do not show popup alerts' in 'Settings' > 'File Rating' > 'File Rating Settings'.

- **Unknown files** - The following alert is shown:
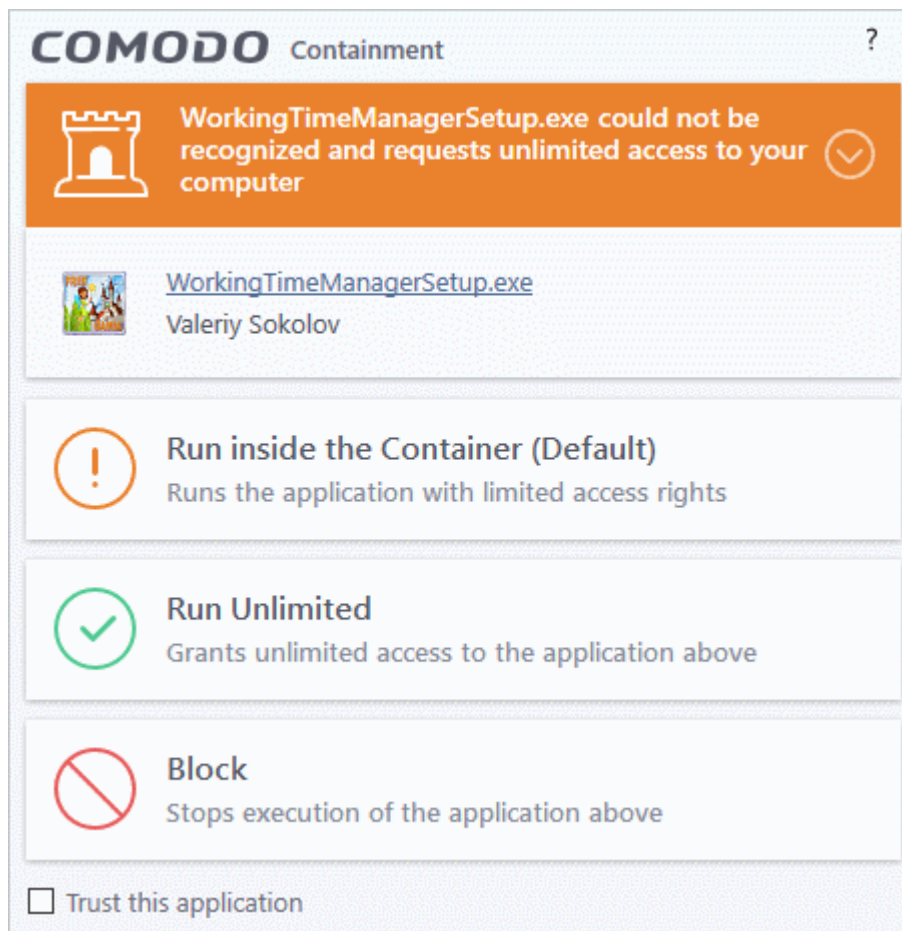
You can choose from these actions:

- **Run inside the Container** - Executes the program inside the container with limited access rights
- **Run Unlimited** - Lets the program run as normal on your computer, outside the container. The file is added to the file list as a 'Trusted' file. See **File List** for more details.
- **Block** - The program is terminated and not allowed to run.
- **Malicious files** - The program is automatically blocked and quarantined. You will see the following type of alert:
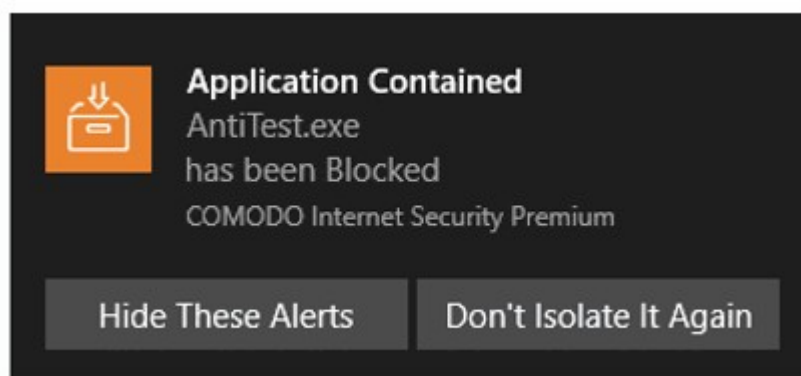
- **Don't Isolate It Again** - Select this option if you are sure you can trust the file.
    - The file is marked as 'Trusted' in your local file list, and will be allowed to run without restriction in future. See **File List** for more details.

Answer VirusScope Alerts

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   ⌄

Show Activities
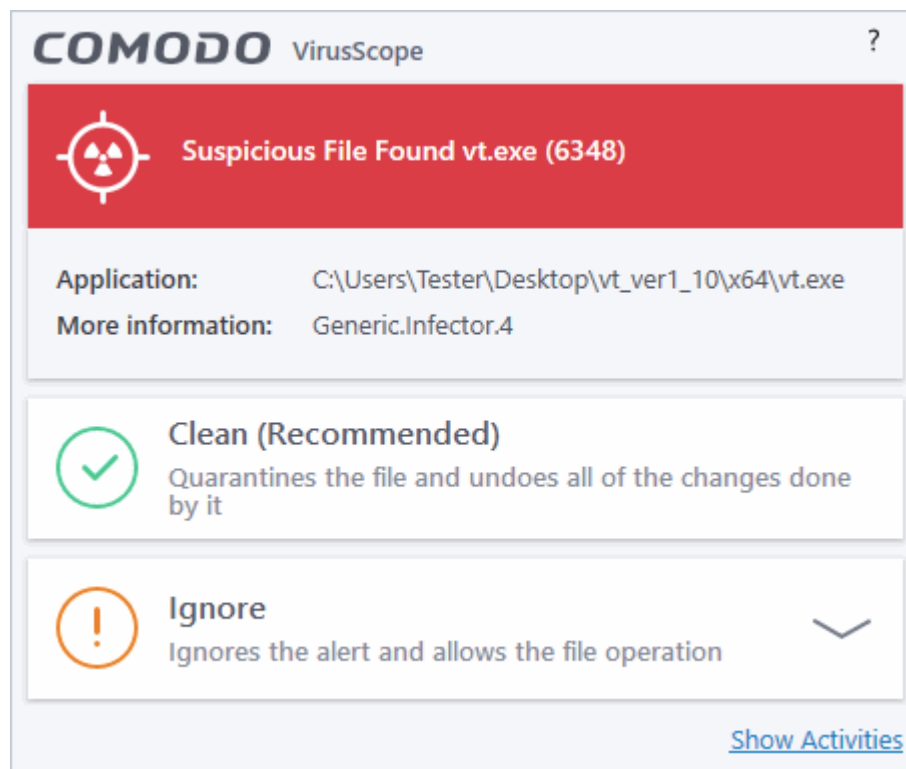
- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking 'Ignore' and selecting the option from the drop-down.
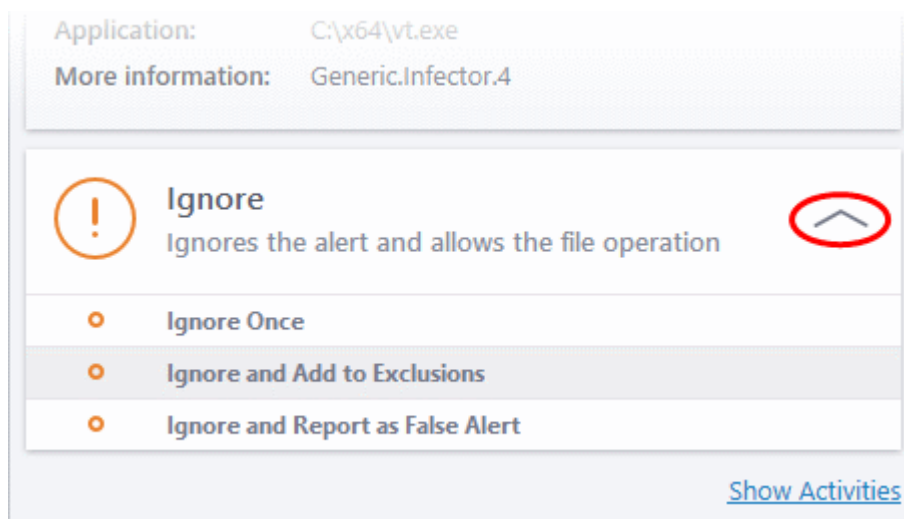
- Ignore Once -The process is allowed to run this time only. If the process attempts to execute on future occasions, another VirusScope alert is displayed.

- 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.
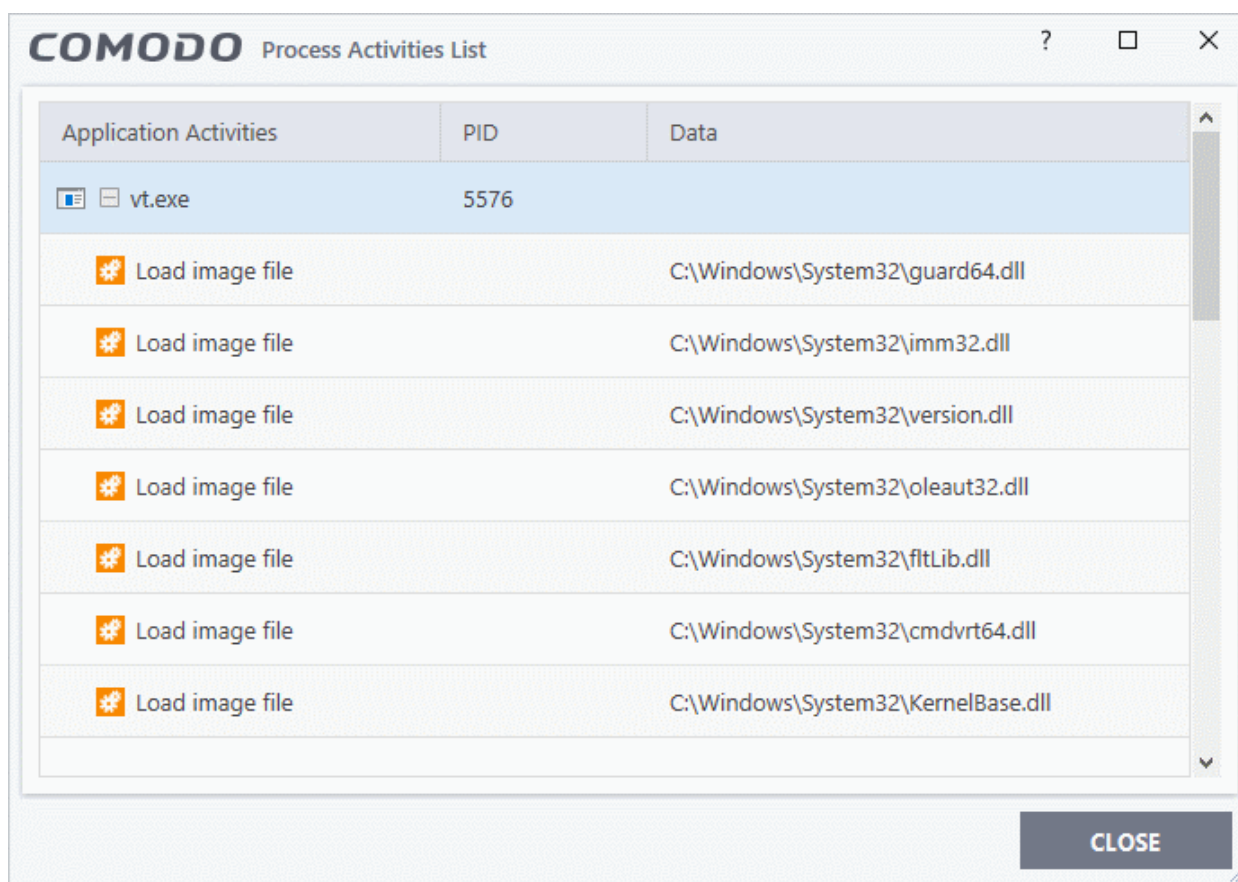
Column Descriptions

- 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.
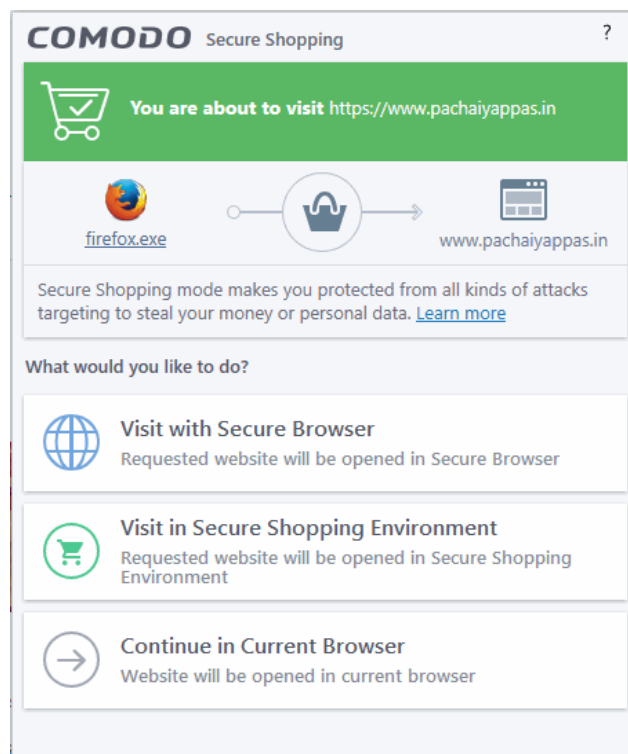
The options available in the alert are:

- 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

Click 'Tasks' > 'General Tasks'

- The general tasks area lets you:
    - Quickly run antivirus scans
    - Update the virus database
    - Open secure shopping
    - Manage blocked files
    - Get live help from Comodo
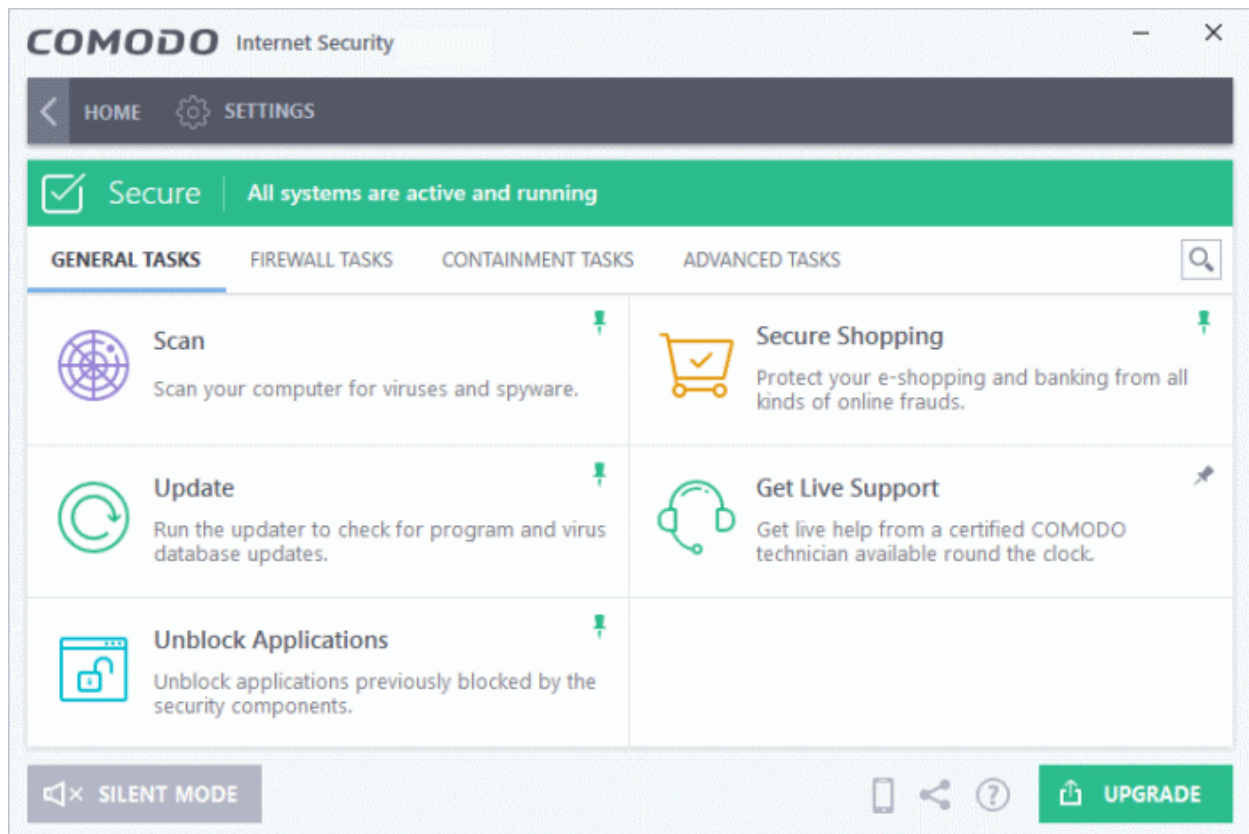
See the following sections for help with each area:

- **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**
- **Process Infected Files**

2.1. Scan and Clean Your Computer

Click 'Tasks' > 'General Tasks' > 'Scan'

- CIS leverages multiple technologies, including real-time and on-demand scans, to detect and remove suspicious files from your computer.
- You can also create your own scan profiles to scan specific files, folders and drives.

- You can schedule automatic scans to run at a set time, and you can also send unrecognized files to Comodo for analysis.

- The scan tile in general tasks lets you launch an on-demand scan

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 'Tasks' > 'General Tasks' > 'Scan'

Any of these methods will open the scan selection screen:
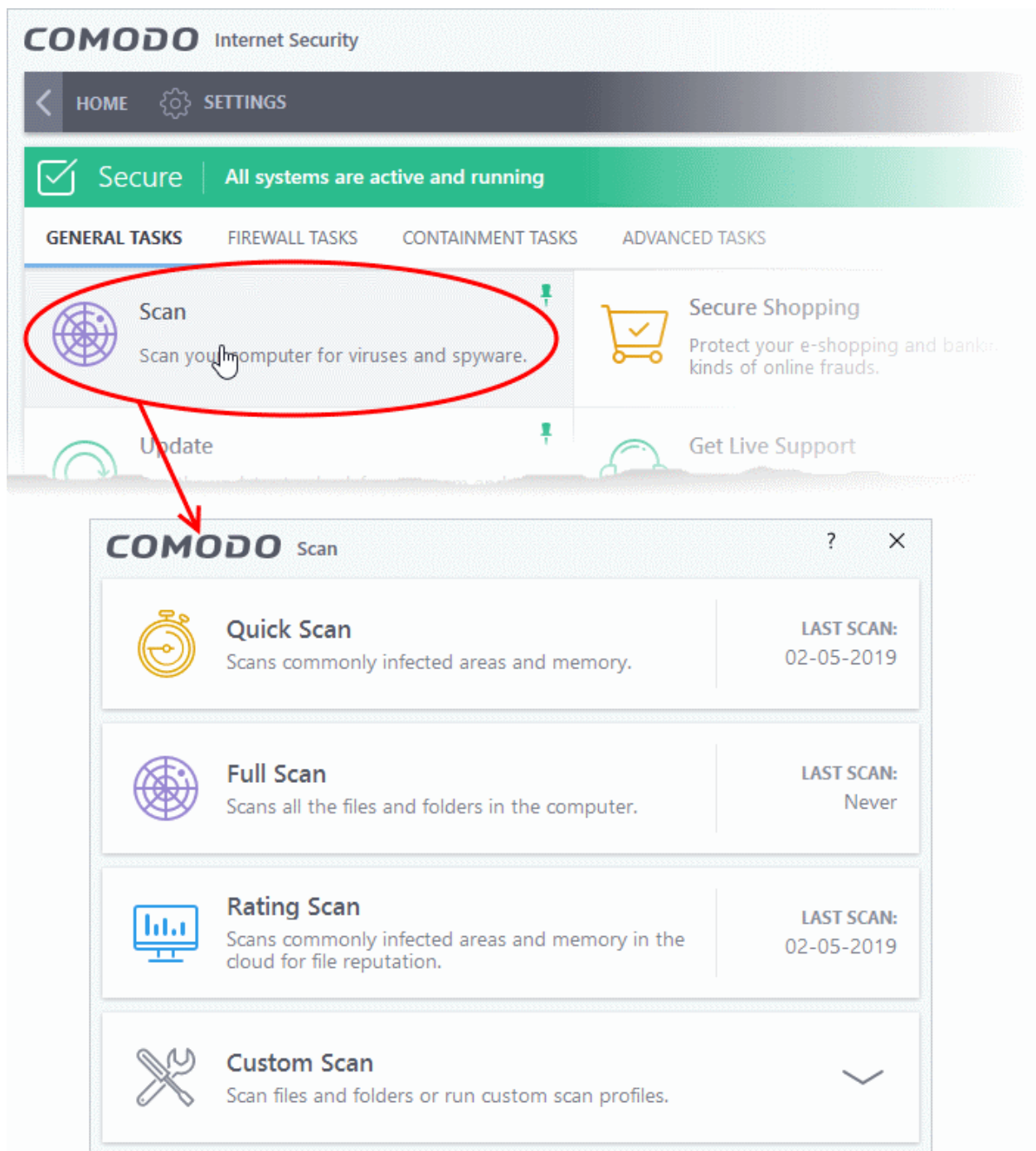
A quick scan will scan commonly infected areas while a full scan will scan your entire computer. The rating scan will assign a trust rating to all files on your computer. A custom scan lets you choose specific areas to scan.

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**
- **Process Infected Files**

2.1.1. Run a Quick Scan

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Quick Scan'

- The quick scan profile scans important areas of your computer which are most prone to attack.
- This includes system files, auto-run entries, hidden services, boot sectors, and important registry keys.
- These areas are of great importance to the health of your computer, so it is essential to keep them free of infection.
- You can change the settings of a quick scan in 'Settings' > 'Antivirus' > 'Scans'. See **Antivirus Configuration** > **Scan Profiles** for help with this.

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.
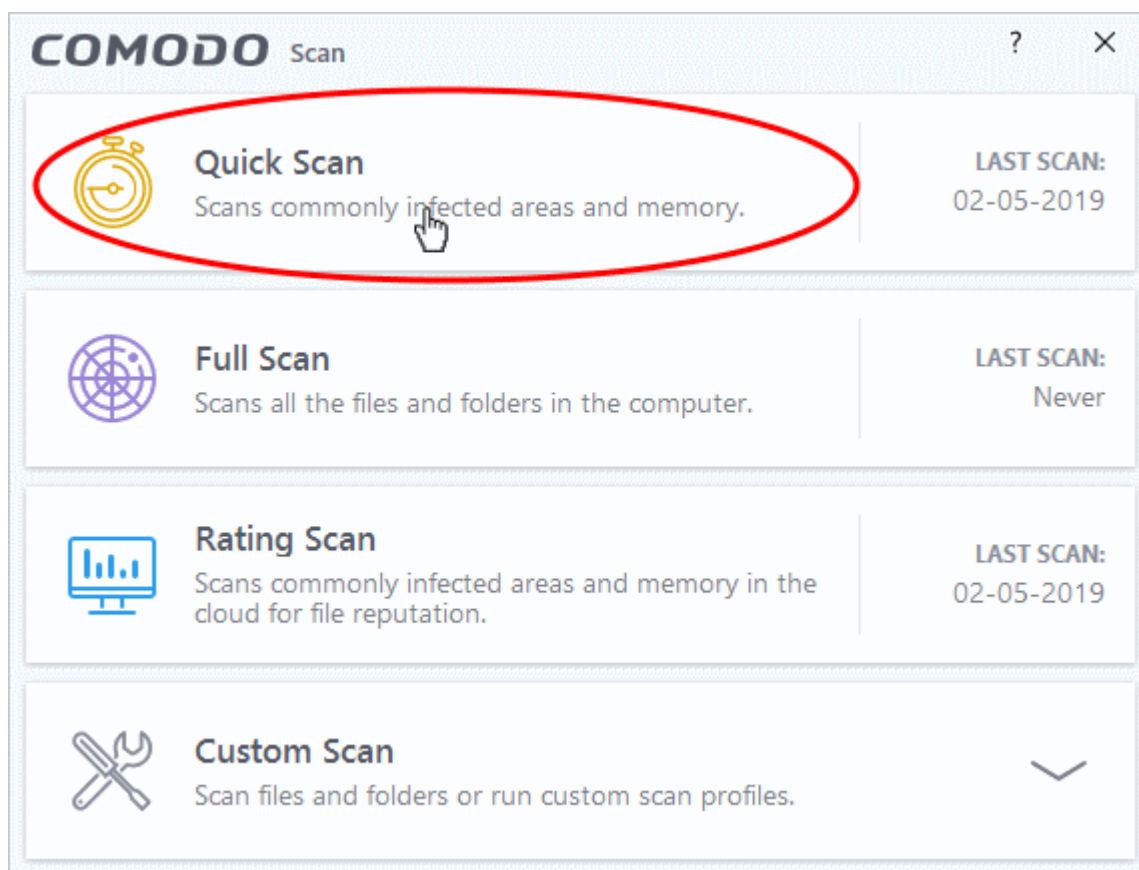
The scanner will start and first check whether your virus signature database is up-to-date:
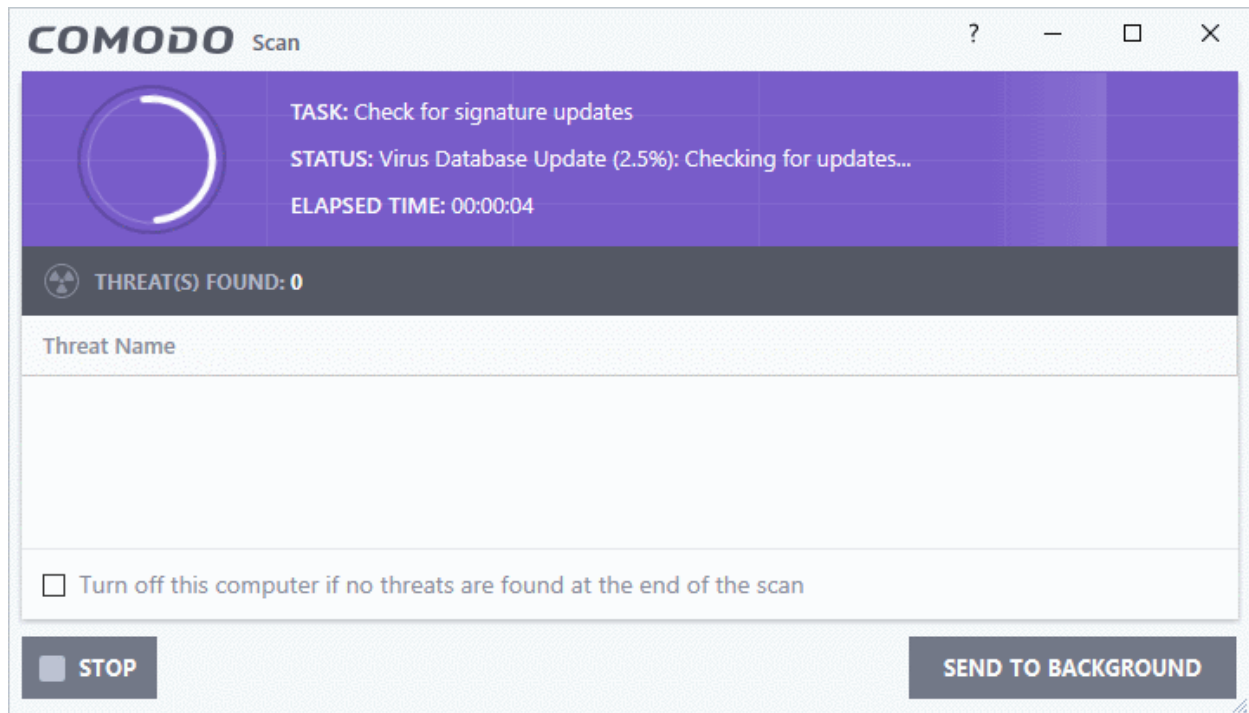
If the database is outdated, CIS will download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:
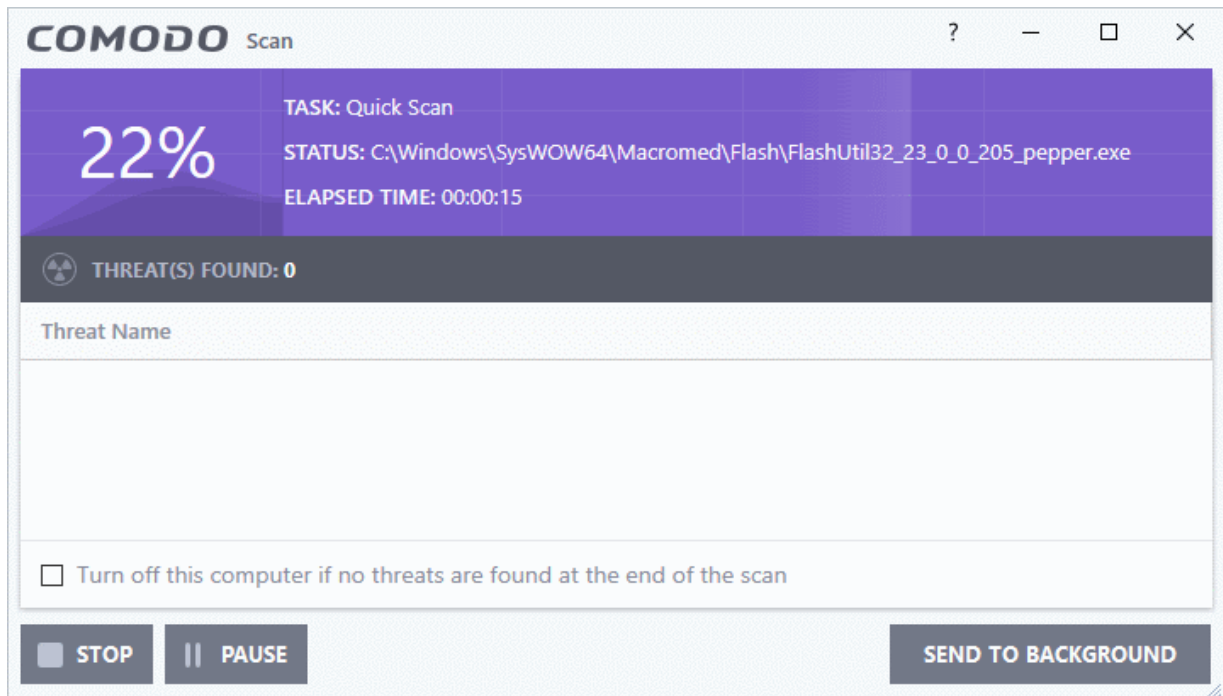
- You can pause, resume or stop the scan by clicking the appropriate button.
- If you want to run the scan in the background, click 'Send to Background'. You can still keep track of the scan progress from the '**Task Manager**' interface. ('Tasks' > 'Advanced Tasks' > 'Open Task Manager')
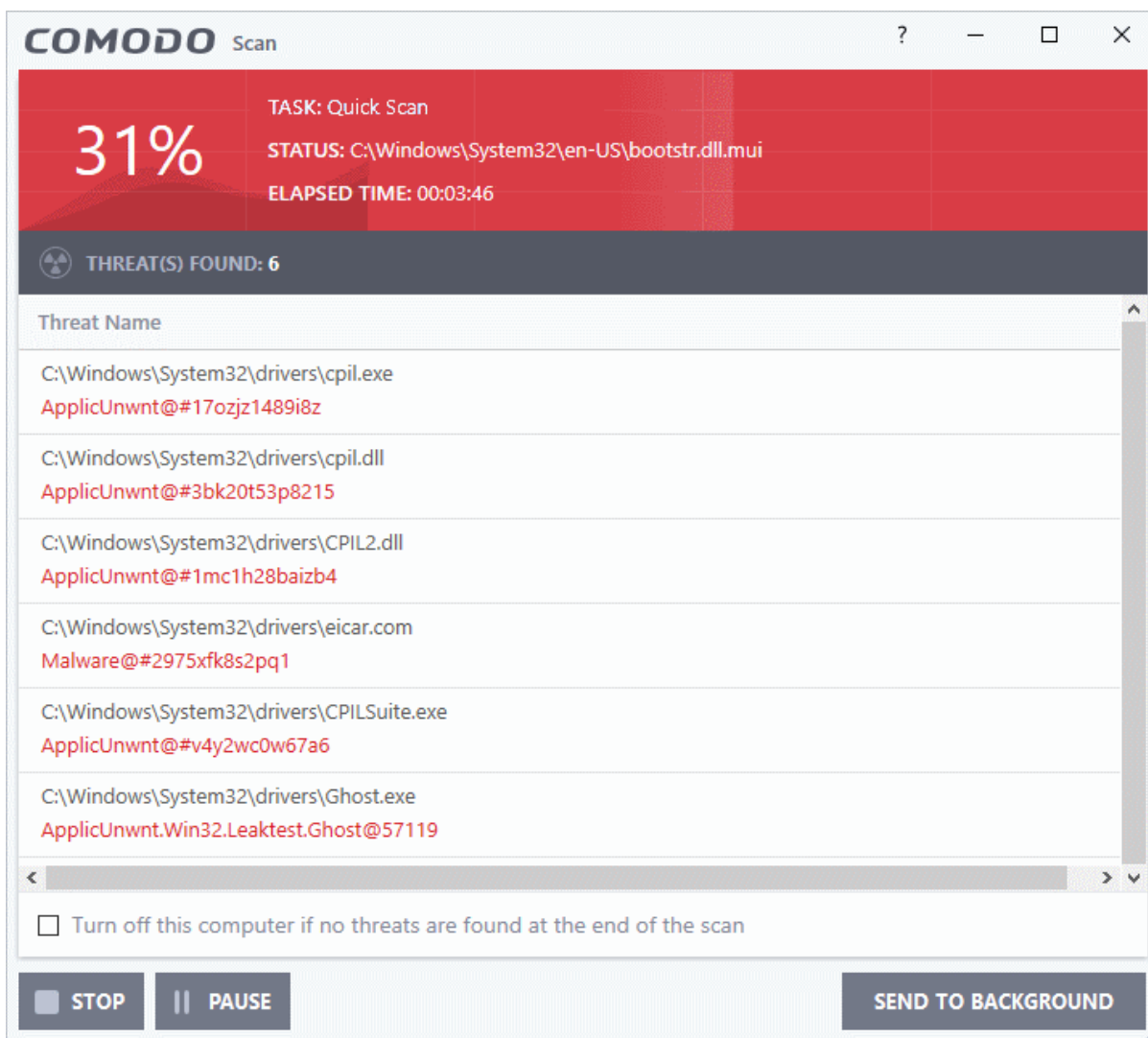
• The results screen shows any malware found by the scan:
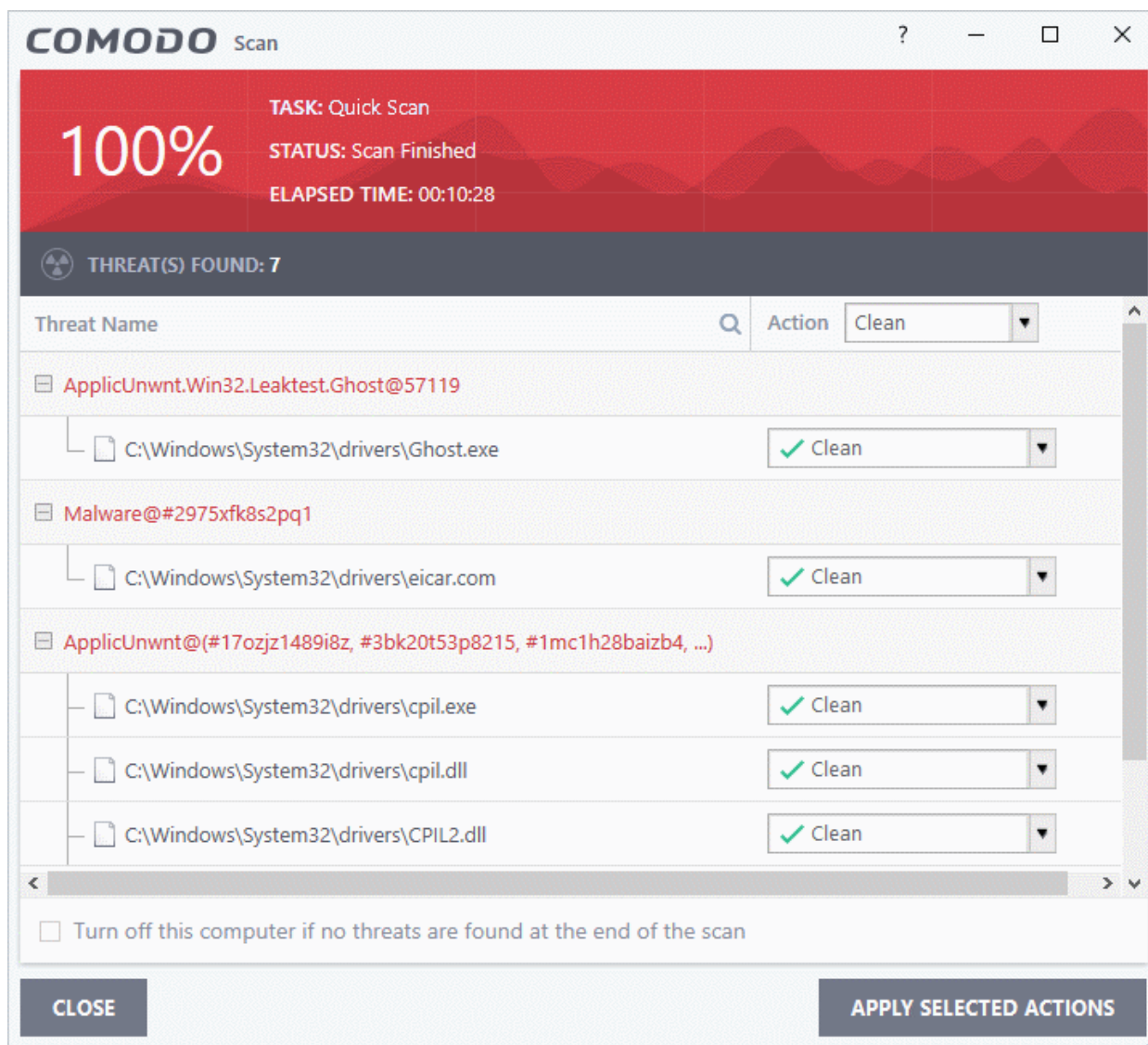
- The results window shows the number of objects scanned and the number of threats (Viruses, Rootkits, Malware).

- Use the drop-down menu to choose whether to clean, move to quarantine or ignore the threat. See '**Process infected files**' for more details.

> **Note**. You will only see the drop-down menus if 'Automatically clean threats' is disabled for quick scans in 'Settings' > 'Antivirus' > 'Scans'. See **Scan Profiles** for help with this.

2.1.2. Run a Full Computer Scan

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Full Scan'

- A full scan checks every file, folder and drive on your computer. USB and other external drives are also scanned.

- You can customize full scans in 'Advanced Settings' > 'Antivirus' > 'Scans'. See **Antivirus Configuration** > **Scan Profiles** for more details.

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':
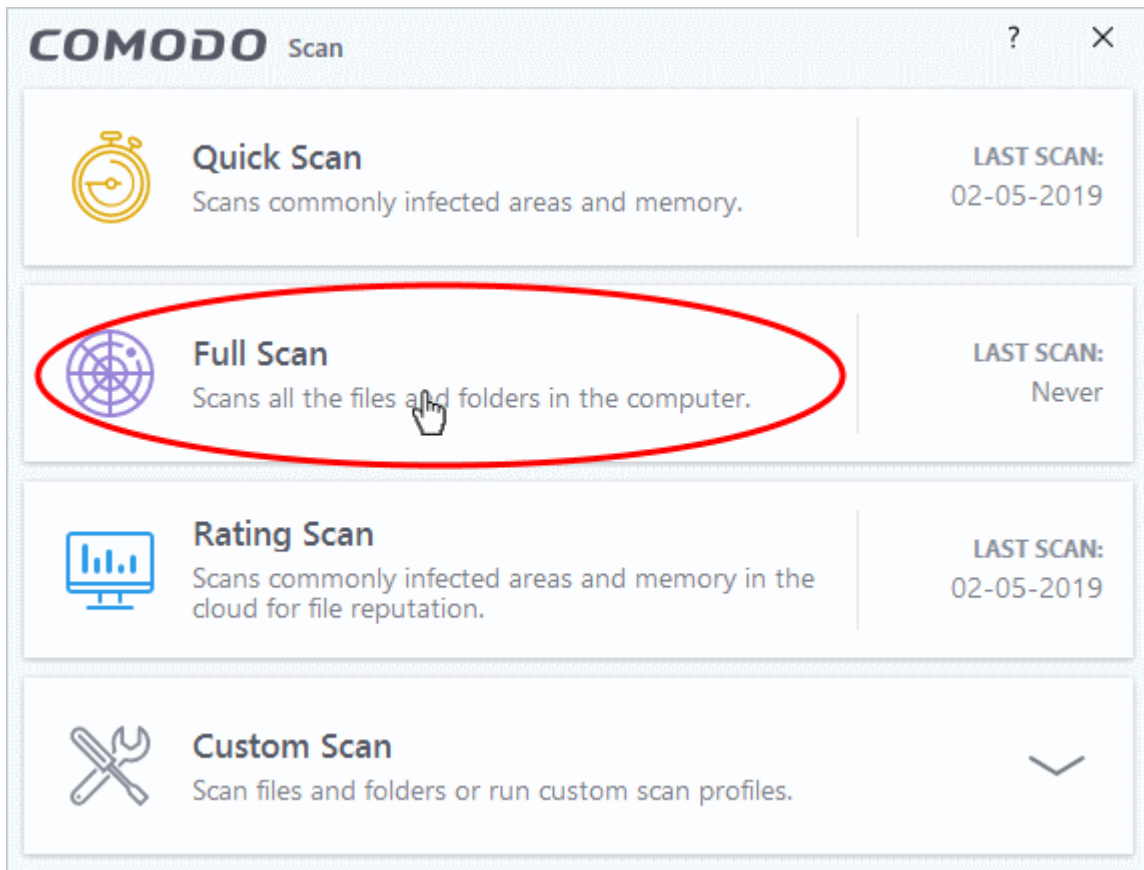
CIS will first check that your virus database is up-to-date:
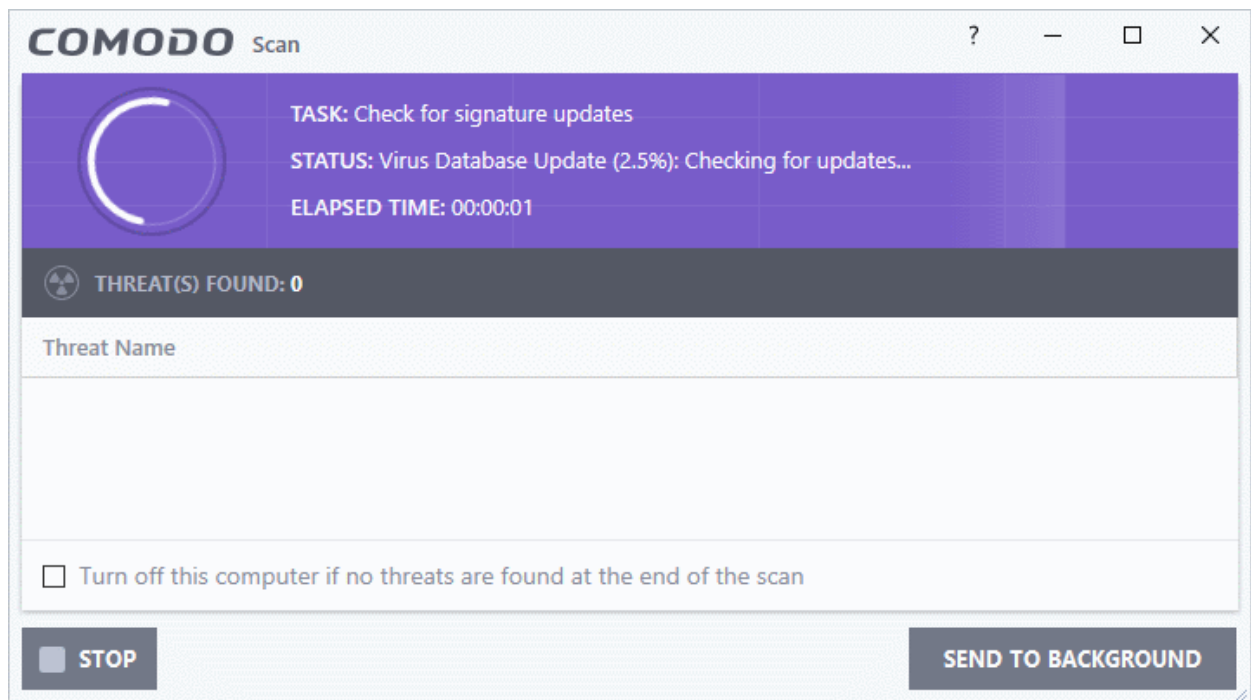
CIS will download any updates before starting the scan:

- You can pause, resume or stop the scan by clicking the appropriate button.
- Click 'Send to Background' to use fewer computer resources on the scan.

You can keep track of scan progress in 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'.

- Any detected threats are shown at the end of the scan:
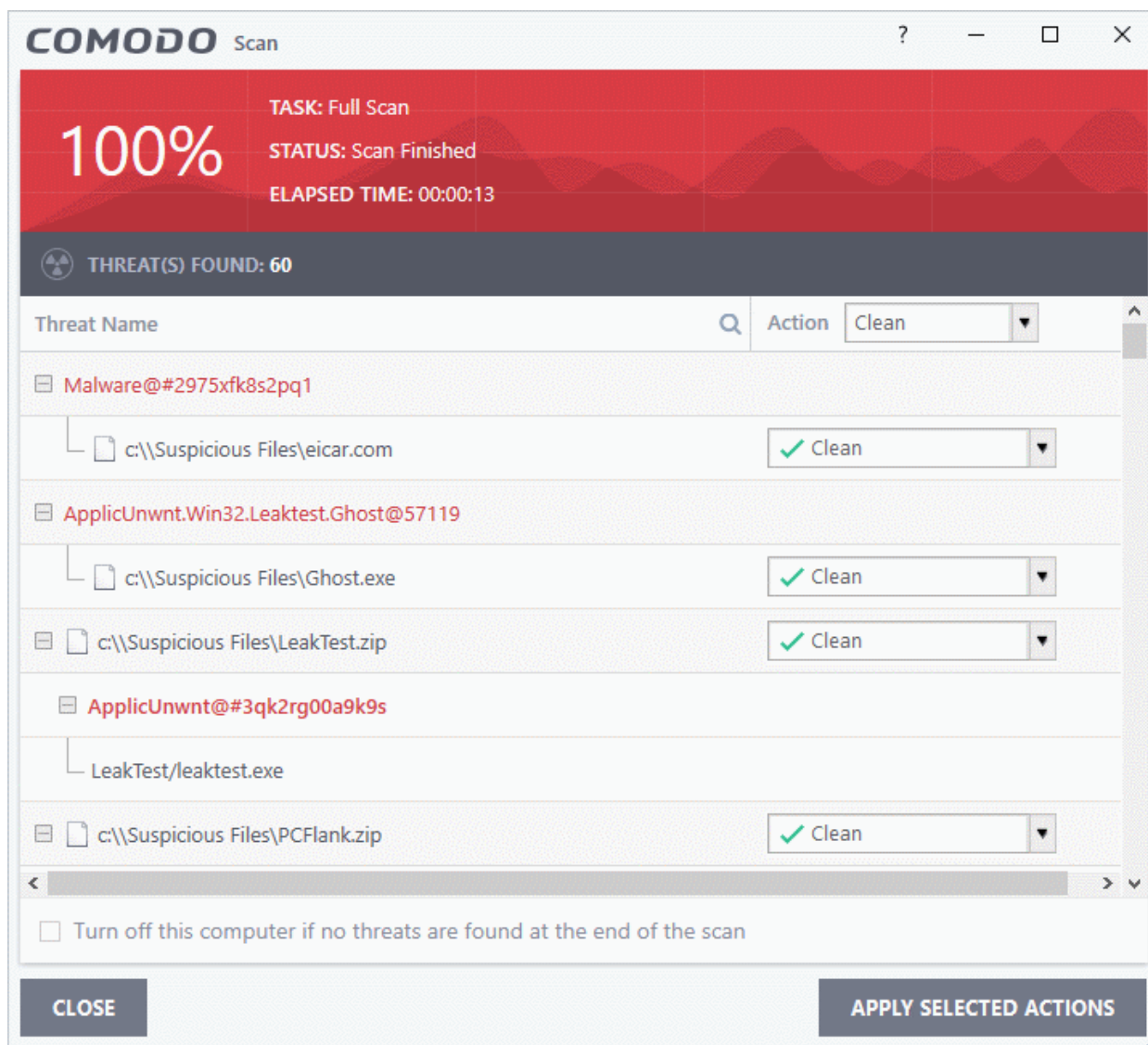
- The results window shows the number of objects scanned and the number of threats (viruses, rootkits, malware).

- 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 see the drop-down menus if 'Automatically clean threats' is disabled for full scans in 'Settings' > 'Antivirus' > 'Scans'. See **Scan Profiles** for help with this.

2.1.3. Run a Rating Scan

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Rating Scan'

- A rating scan checks the trust-rating of files and root certificates on your computer. Root certificates are used by your internet browser to validate the SSL certificates on sites you visit.

- Trust ratings are as follows:

  - **Trusted** - The file is safe to run. The root certificate was issued by a trusted certificate authority (CA).
  - **Untrusted** - The root certificate is not safe. It was not issued by a trusted CA and could be linked to fraud/phishing websites.
  - **Unrecognized** - Comodo does not currently have a trust rating for the file. Unrecognized files should be run in the container to prevent them potentially attacking your computer. You can simultaneously submit them to Comodo for a trust-rating analysis.
  - **Malicious** - The file is malware. Depending on your settings, CIS will either quarantine the file

immediately or present you with disinfection options.

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':
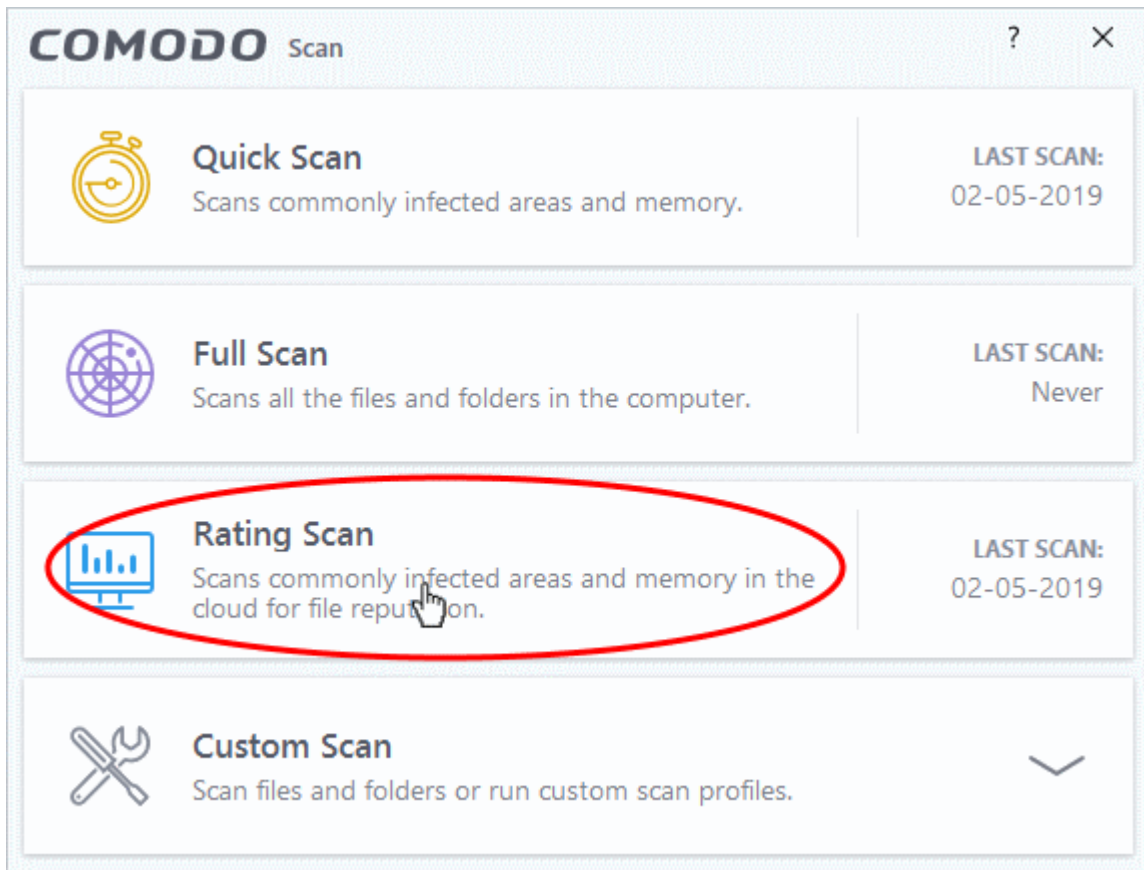
CIS will analyze all files on your computer and assign them a trust rating. File ratings are shown as follows when the scan finishes:
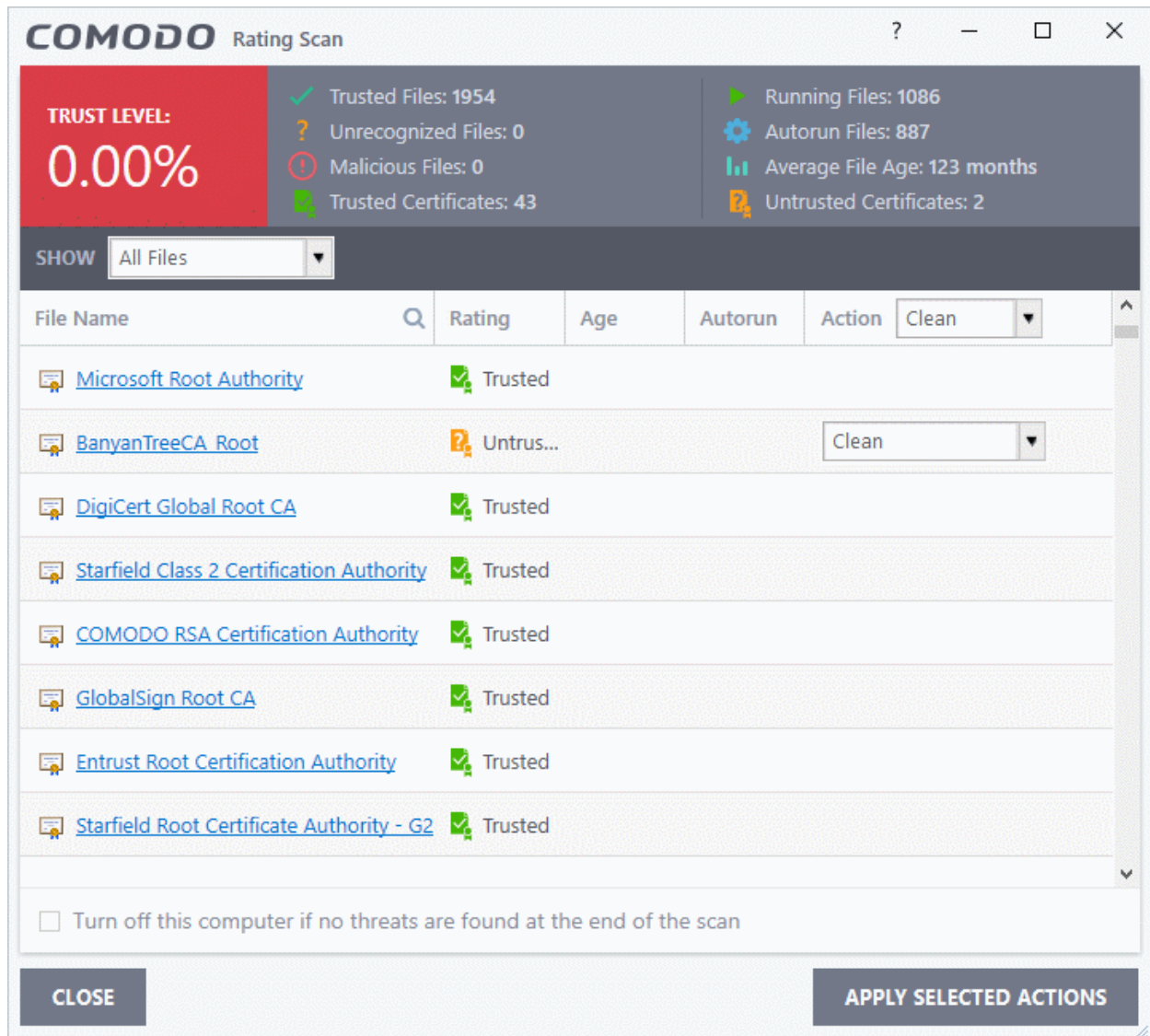
Rating Scan Results Table - Column Descriptions	
Column Header	**Description**
File Name	The label of the scanned item
Rating	The trust level of the file / SSL certificate as per the cloud based analysis. The possible values are: • Trusted • Untrusted • Unrecognized • Malicious
Age	The length of time the item has been on your computer
Autorun	Whether or not the file automatically runs without user intervention.
Action	Select how you want to deal with the listed item. See below table:

The drop-down menus on the right let you handle unrecognized and malicious items:
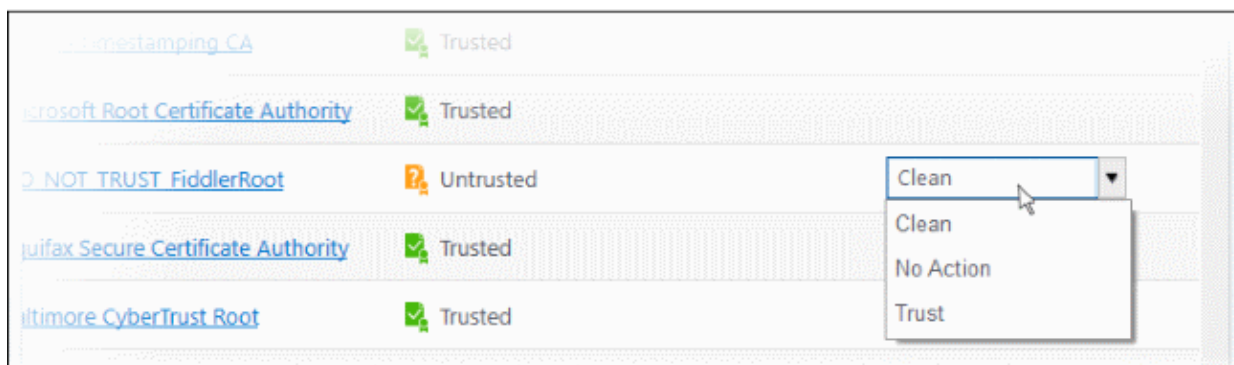
- **Clean** - Available only for untrusted/malicious items. The threat is placed in quarantine for your review. Click 'Tasks' > 'Advanced Tasks' > 'View Quarantine' to open this area. You can restore or permanently delete files from quarantine as required. See **Manage Quarantined Items** for more details.

- **No Action** - Ignores the warning this time only. The file or certificate is not placed in quarantine. Use this option with caution. The file/certificate will be caught again by the next rating scan you run.

- **Trust** - Assigns a trusted rating to the item. Only select this option if you are sure the item is trustworthy.

   - **Files** - The file is awarded trusted status in the **File List** ('Settings' > 'File Rating' > 'File List'). The file will be excluded from any future rating scans.

   - **SSL Certificates** - The certificate authority (CA) who signed the certificate is awarded 'Trusted' status. CIS will allow you to connect to sites whose certificates chain to this root.

- CIS logs all actions taken in the results screen. You can view the logs at 'Tasks' > 'Advanced Tasks' > 'View Logs'.

   - **Files** - See **File List Changes Logs** for more details
   - **SSL Certificates** - See **Trusted Certificate Authorities Changes Logs** for more details

- Use the drop-down in the 'Action' column header to apply your choice to all listed files:
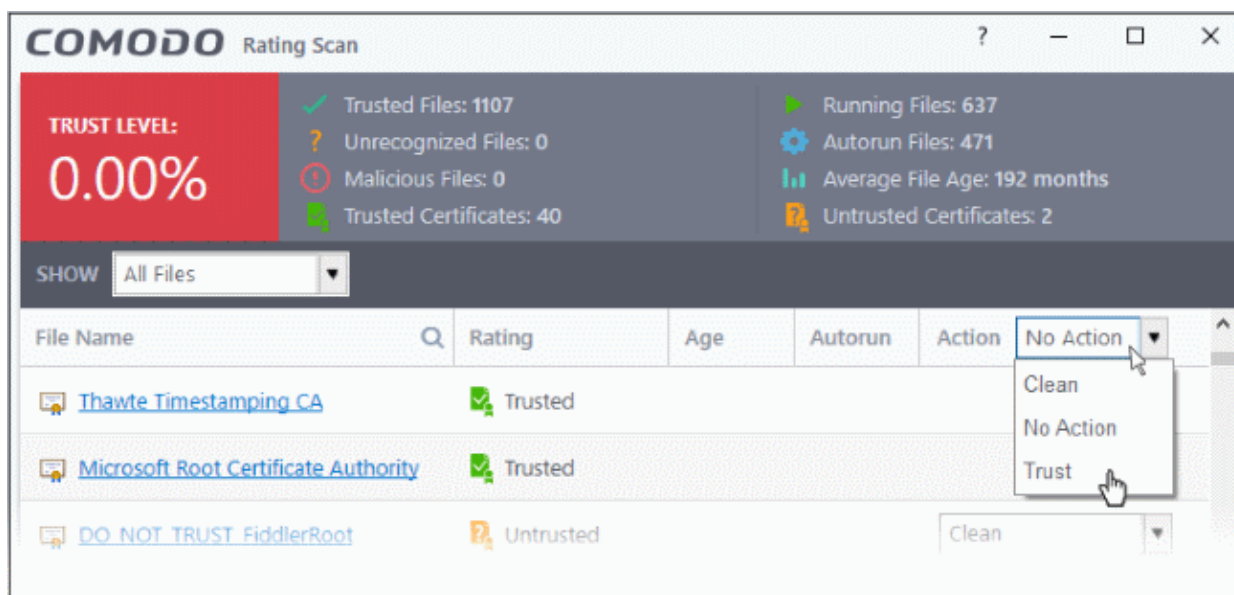
2.1.4. Run a Custom Scan

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan'

- A custom scan lets you check specific files, folders, drives and areas on your computer.

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:
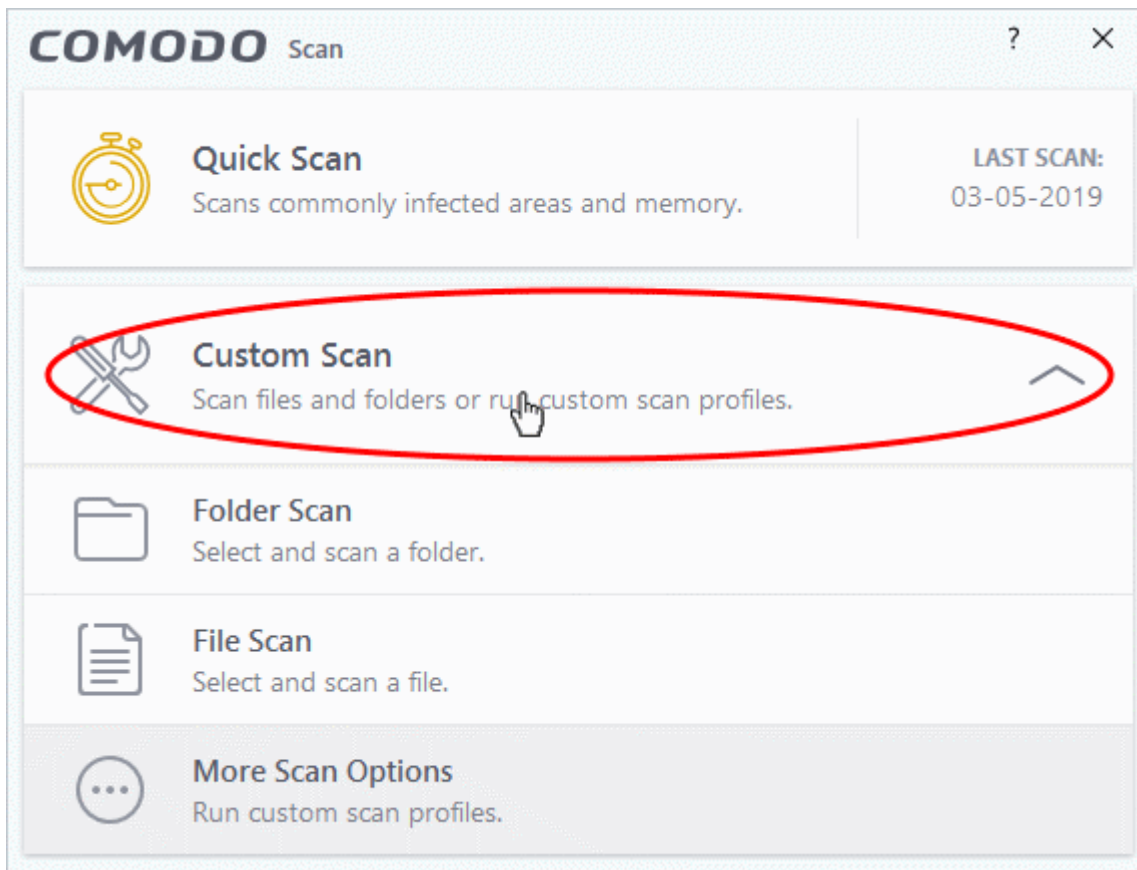
The 'Custom Scan' panel contains the following options:

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

2.1.4.1. Scan a Folder

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'Folder Scan'

- Folder scans let you check specific folders on your hard drive, CD/DVD, or external device.

Tip: Alternatively, you can quickly scan a folder by dragging it onto the CIS home screen. See '**Scan Individual Files and Folders**' for more details.

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' then 'Folder Scan'
- Browse to the folder you want to check and click 'OK':
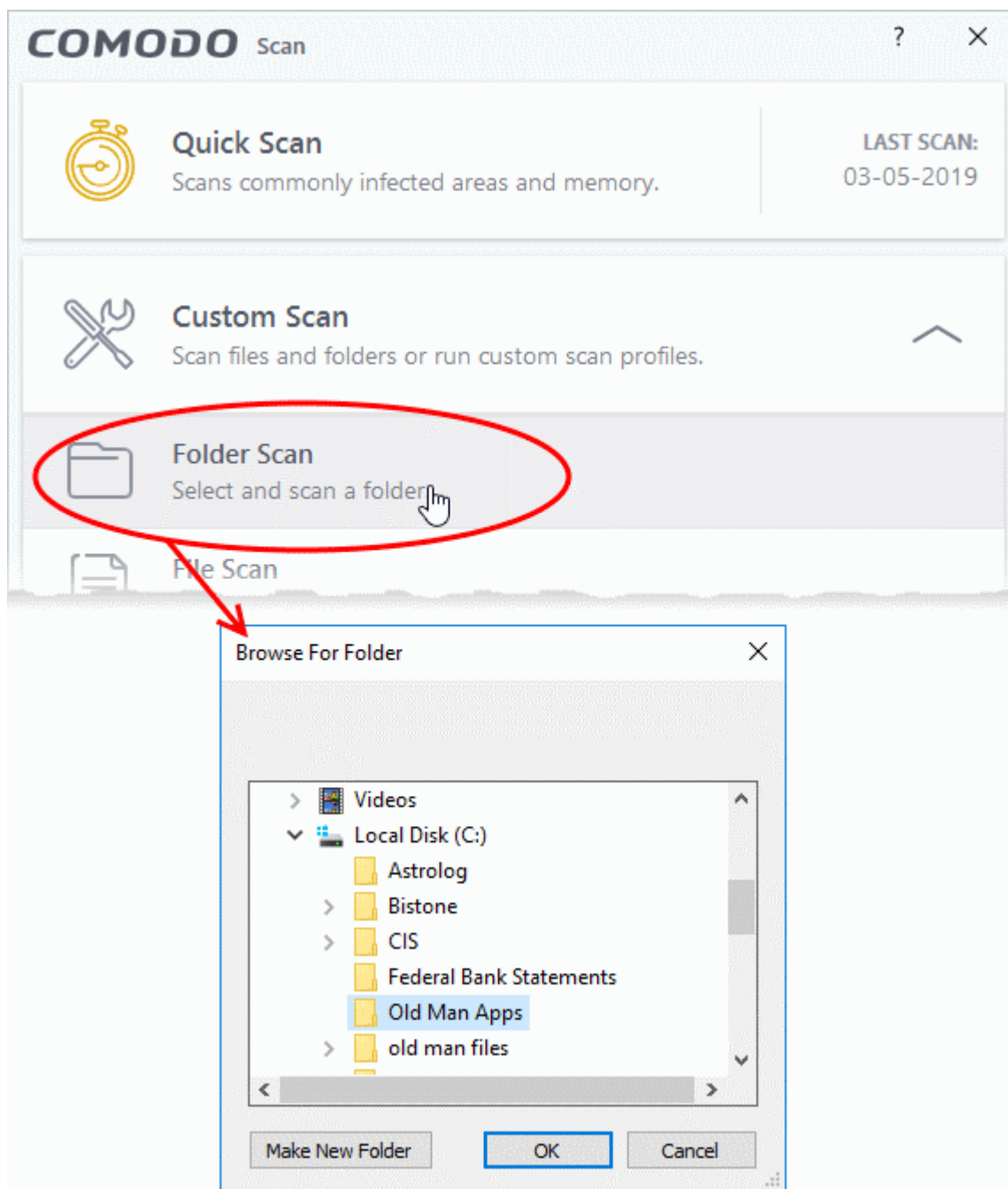
Results are shown at the end of the scan:
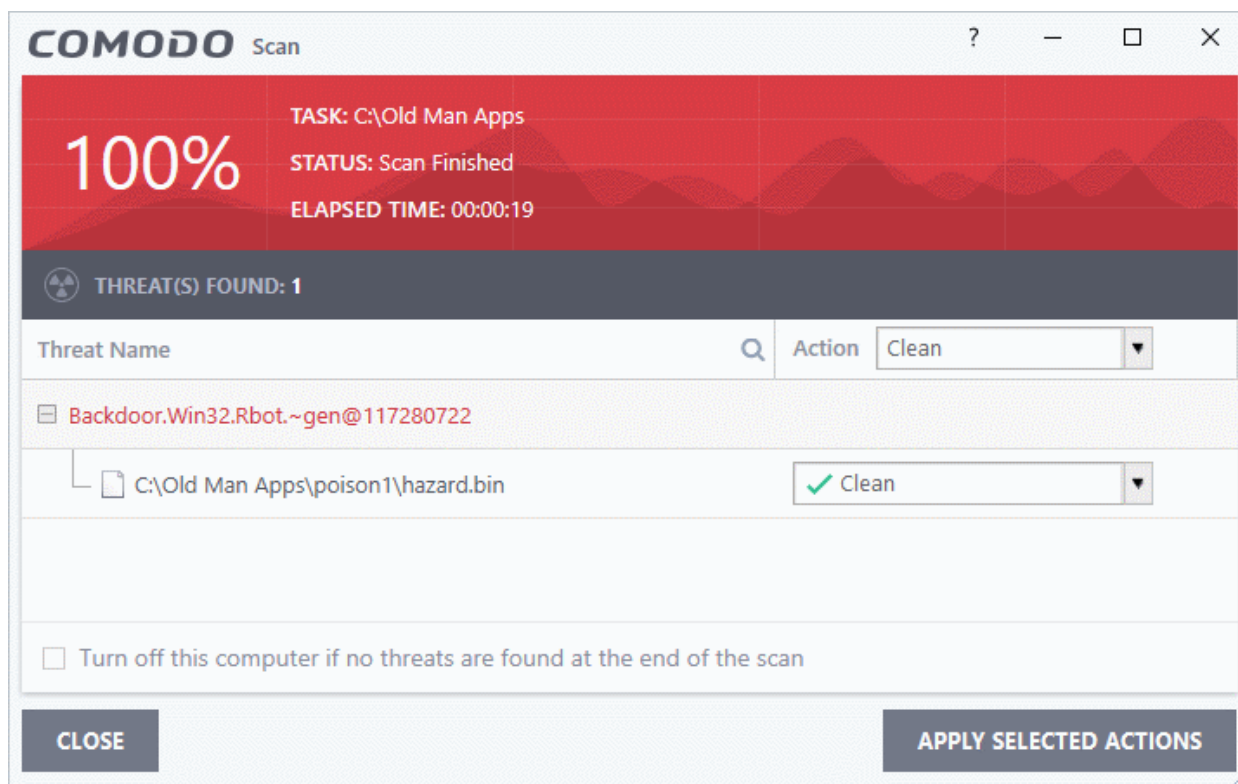
The scan results window shows the number of detected threats (viruses, rootkits, malware and so on). You can clean, move to quarantine, or ignore the threat. See **Process infected files** for more details.

2.1.4.2. Scan a File

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'File Scan'

- File scans let you check specific files 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: Alternatively, you can quickly scan a folder by dragging it onto the CIS home screen. See **Scan Individual Files and Folders** for more details.

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' > 'File Scan'
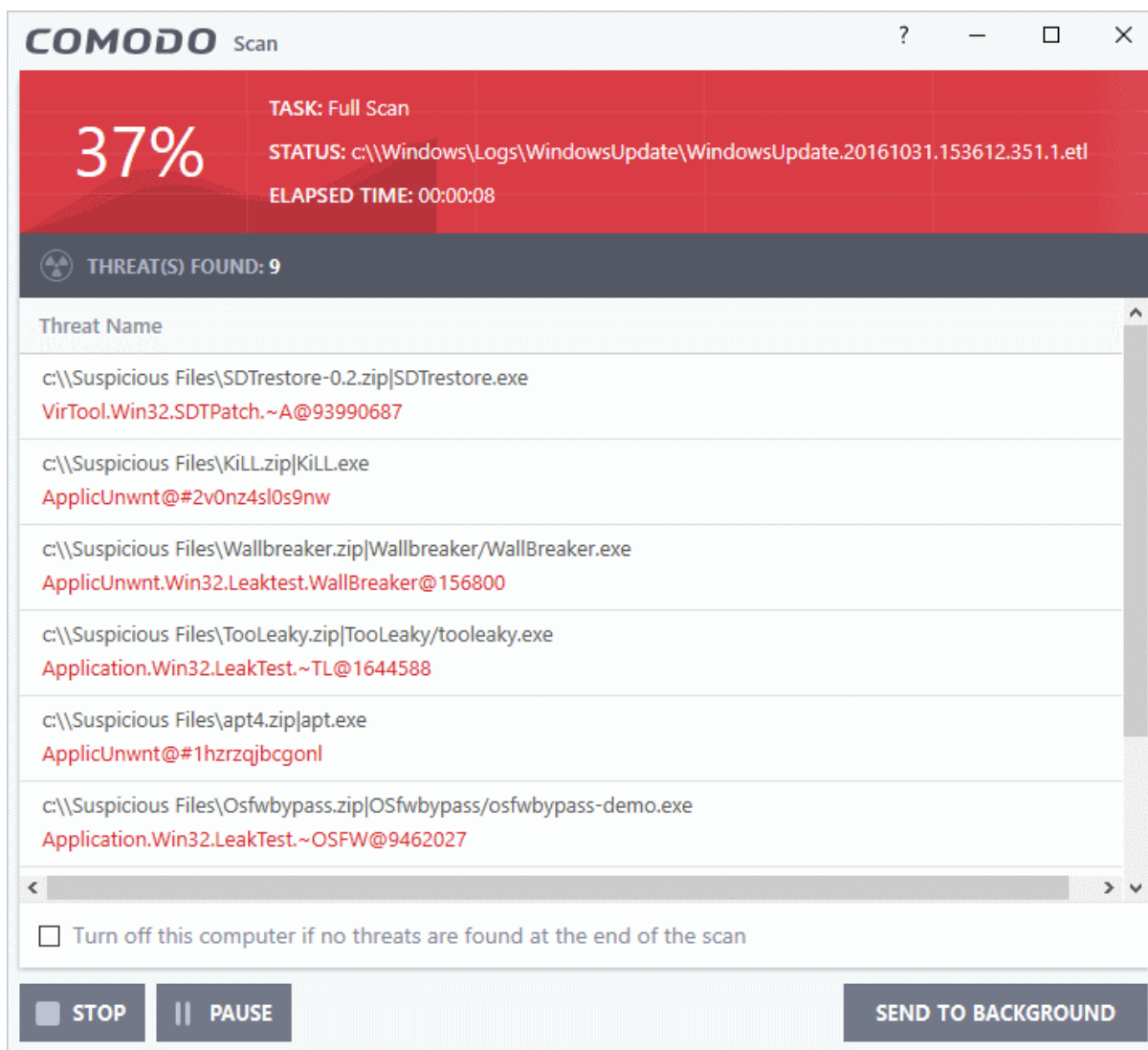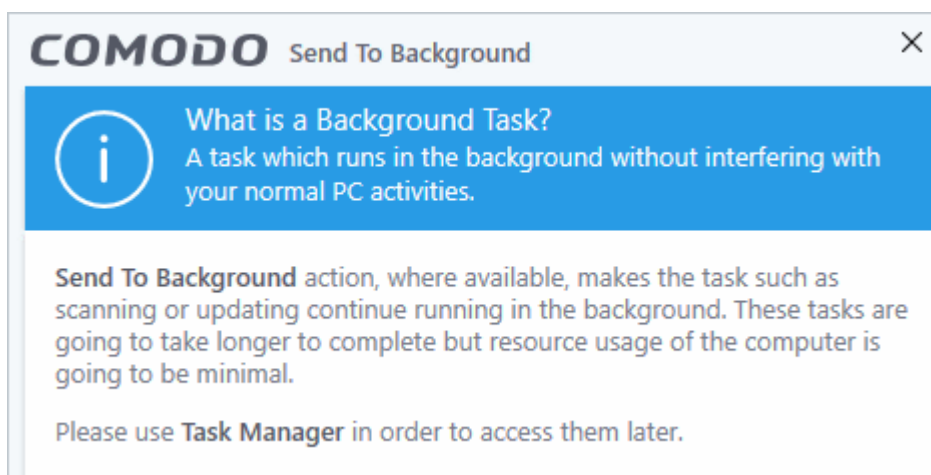- Browse to the file you want to scan and click 'Open'.
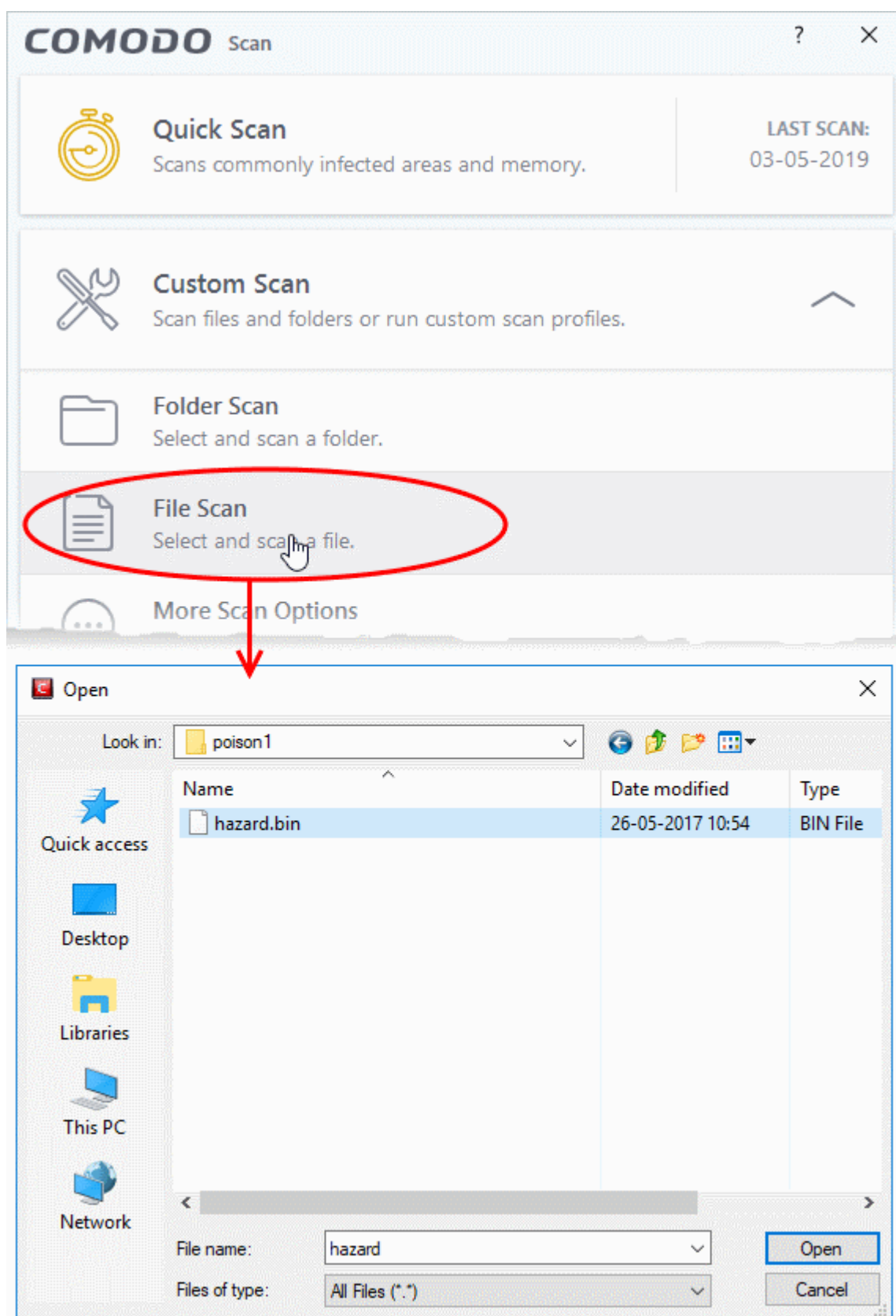
Results are shown at the end of the scan:
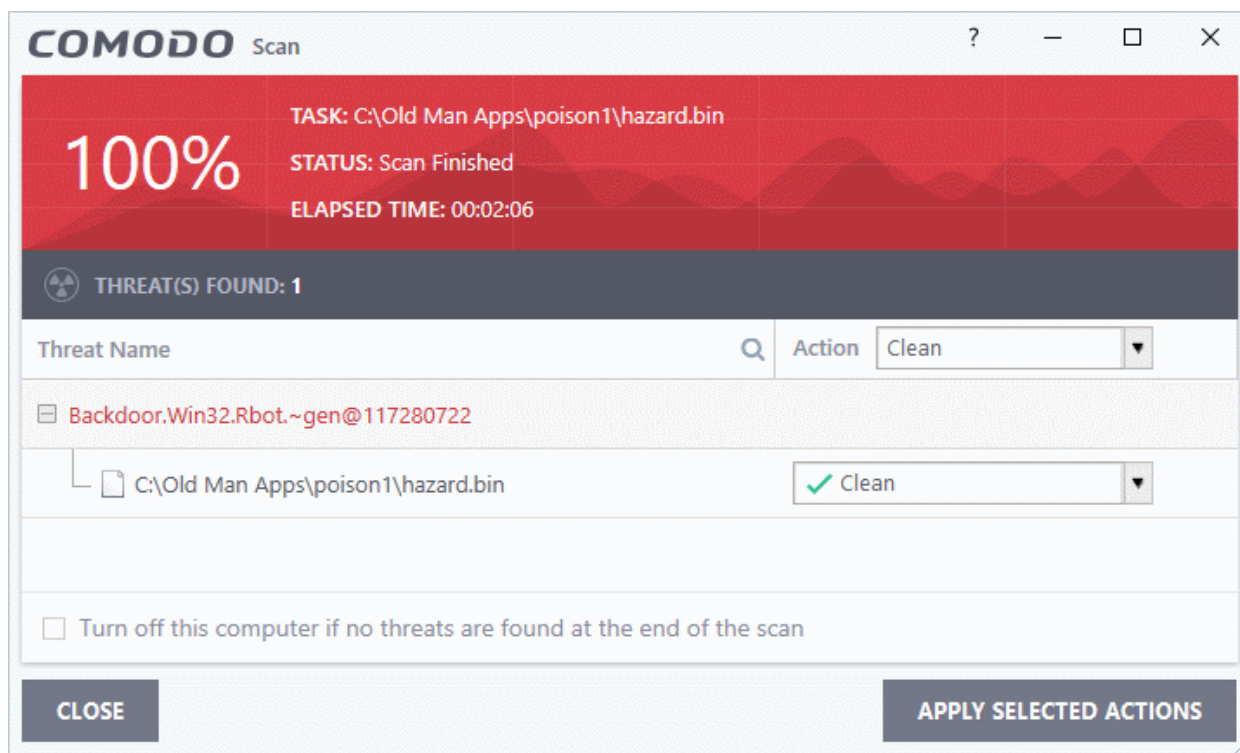
The scan results window shows the number of detected threats (viruses, rootkits, malware and so on). You can clean, move to quarantine, or ignore the threat. See **Process infected files** for more details.

2.1.4.3. Create, Schedule and Run a Custom Scan

Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'More Scan Options'

- A custom scan profile lets you configure your own scan with your own scan settings.
- You can define exactly which files and folders to scan, what time they should be scanned, and configure scan settings.
- Once saved, you can select and run your custom scan at any time in the scans interface.
- See the following for more help:
    - **Create a Scan Profile**
    - **Run a custom scan**

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' then 'More Scan Options'

The 'Scans' page shows pre-defined and user created scan profiles. You can create and manage new profiles in this page:
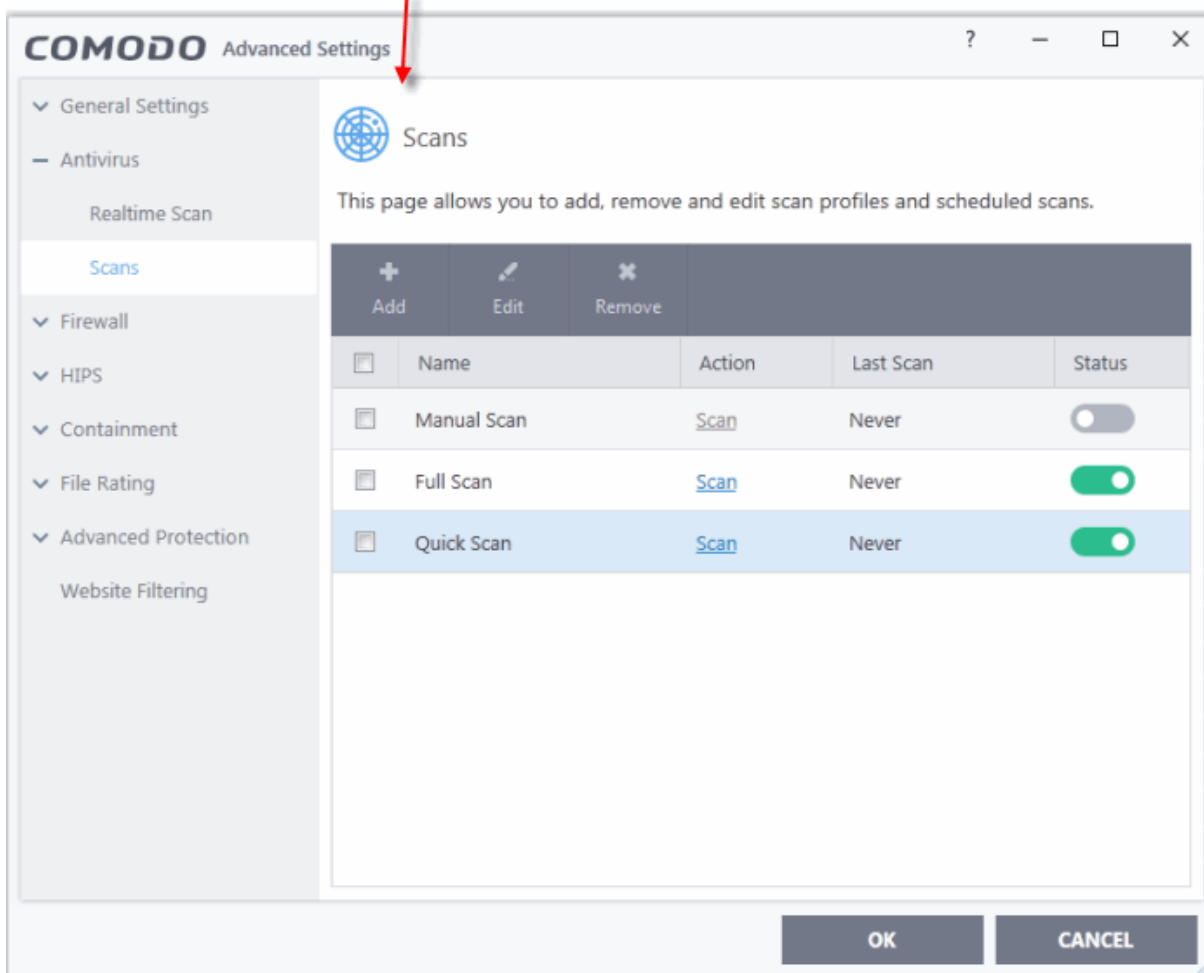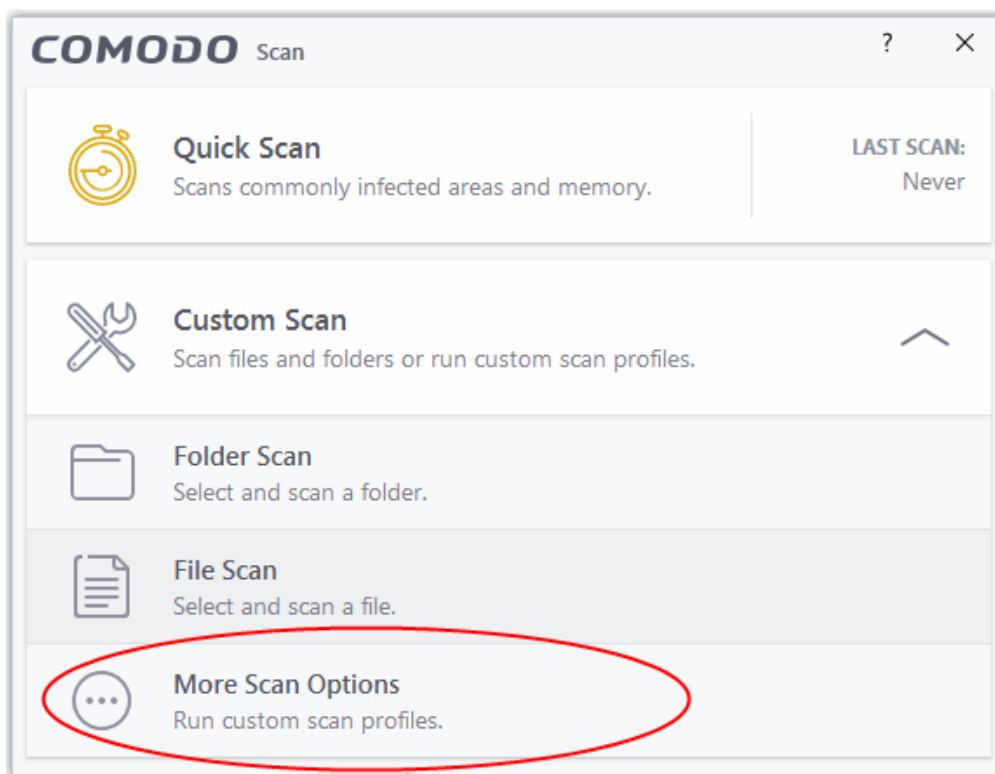
Tip: You can also get to this screen by clicking 'Settings' > 'Antivirus' > 'Scans'.

- Click 'Add' to create a new custom scan profile.
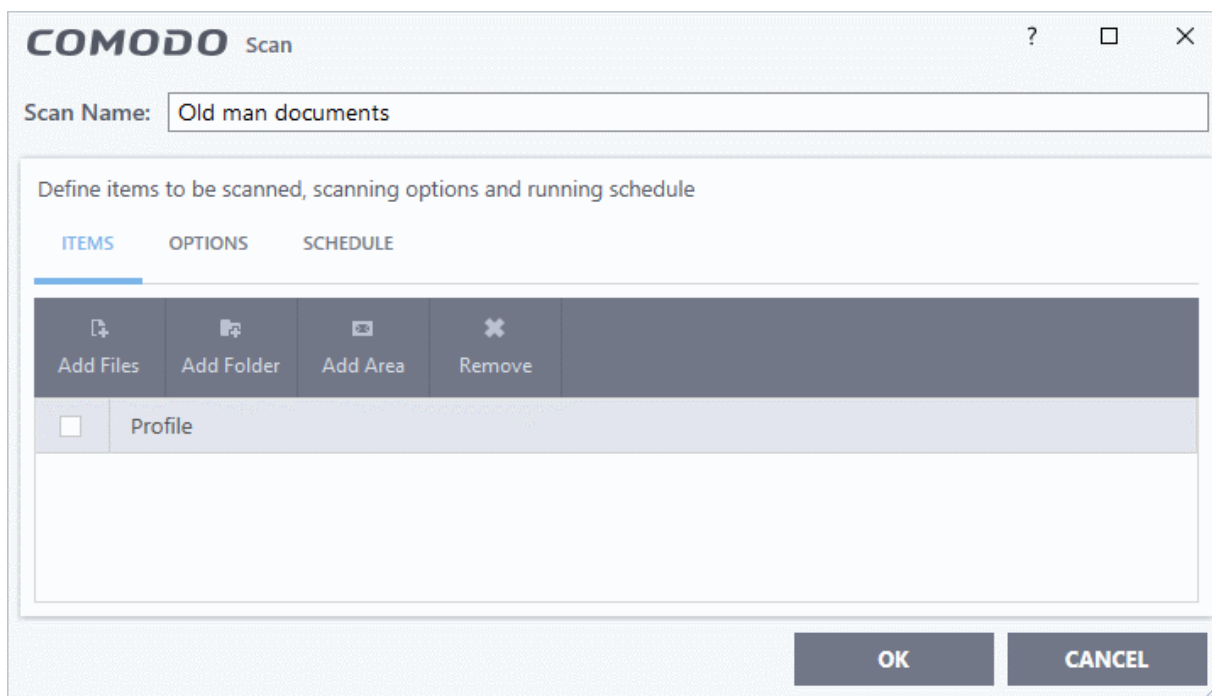
- First, create a name for the profile. The next steps are:
- **Select items to scan**
- **Configure scan options for the profile (optional)**
- **Configure a scan schedule (optional)**

Select items to scan

- Click the 'Items' button at the top of the scan interface.

You can add items as follows:

- **Add File** - Add individual files to the profile. Click the 'Add Files' button and browse to the file you want to include.
- **Add Folder** - Add entire folders to the profile. Click the 'Add Folder' button and choose the folder you want to include. All files in the folder are covered by the scan.
- **Add Area** - Scan a specific region. The choices are 'Full Computer', 'Commonly Infected Areas', 'System Memory' and 'Trusted Root Certificate Store'. See screenshot below:

- Repeat the process to add more items to the profile. You can mix-and-match files, folders and areas in your custom scan.

Configure scan options

- Click the 'Options' button at the top of the scan interface

---

- **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 accuracy by augmenting the local scan with an online look-up of Comodo's latest virus database. This means CIS can detect the latest malware even if your virus database is out-dated *(Default = Disabled)*.

- **Automatically clean threats** - Select whether or not CIS should automatically remove any malware found by the scan.

  - **Disabled** = Results are shown at the end of the scan with a list of any identified threats. You can manually deal with each threat in the results screen. See **Process infected files** for guidance on manually handling detected threats. (*Default*)

- **Enabled** = Threats are handled automatically. Choose the action that CIS should automatically take:
    - **Quarantine Threats** - Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See **Manage Quarantined Items** for more details.
    - **Disinfect Threats** - If a disinfection routine exists, CIS will remove the virus and keep the original file. If not, the file will be quarantined.

- **Show scan results window** - 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 in scans on this profile. You can also set the heuristic sensitivity level. *(Default = Enabled).*

- Background. Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This means CIS can detect brand new threats that are not even in the virus database.

  If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

    - **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts.
      Despite the name, this setting combines a very 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 possible false positives.
    - **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.

- **Limit maximum file size to** - Specify the largest file size that the antivirus should scan. CIS will not scan files bigger than the size specified here *(Default = 40 MB)*.

- **Run this scan with** - If enabled, you can set the priority of scans on this profile The available options are:
    - High
    - Normal
    - Low
    - Background.

- **Update virus database before running** - CIS checks for and downloads the latest virus signatures before starting a scan *(Default = Enabled)*.

- **Detect potentially unwanted applications** - The antivirus also scans 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 installing another 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)*.

- **Apply this action to suspicious autorun processes** - Specify how CIS should handle unrecognized auto-run items, Windows services and scheduled tasks.
    - **Ignore** - The item is allowed to run (*Default*)
    - **Terminate** - CIS stops the process / service
    - **Terminate and Disable** - Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.
    - **Quarantine and Disable** - Auto-run processes are quarantined and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.

  Note 1 - This setting only protects the registry during the on-demand scan itself. To monitor the registry at all times, go to 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'.

    - See **Miscellaneous Settings** for more details

  Note 2 - CIS runs script analysis on certain applications to protect their registry records. You can manage these applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

- See '**Autorun Scans**' in **Script Analysis Settings** for more details

Schedule the scan

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

Schedule options are:

- **Do not schedule this task** - The scan profile is created but not run automatically. The profile will be available for manual, on-demand scans.

- **Every few hours** - Run the scan at the frequency set in 'Repeat scan every NN hour(s)'

- **Every Day** - Run the scan every day at the time specified in the 'Start Time' field.

- **Every Week** - Run the scan on the days 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 dates 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 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 an 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 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.

Run a custom scan

- Click 'Tasks' > 'General Tasks' > 'Scans'
- Click 'Custom Scan' and select 'More Scan Options'

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:
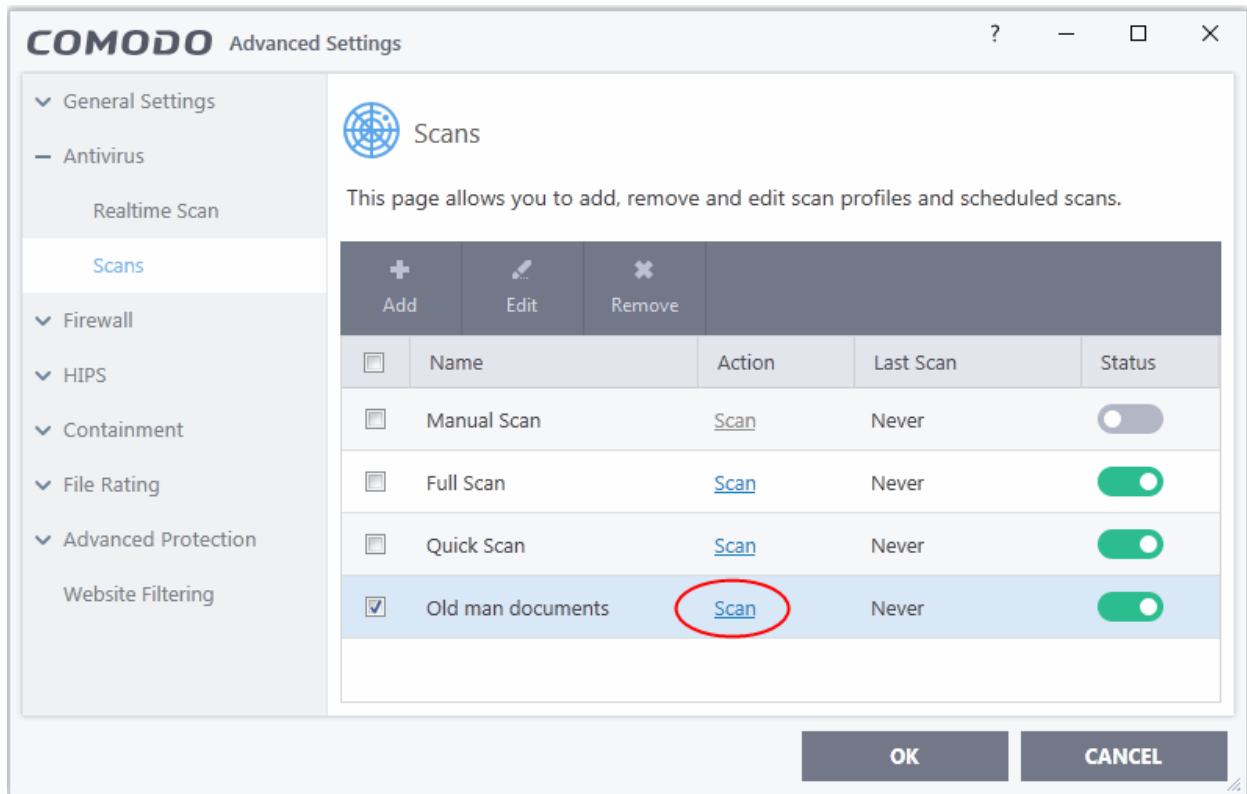
The scan will start immediately. Results are displayed afterwards:
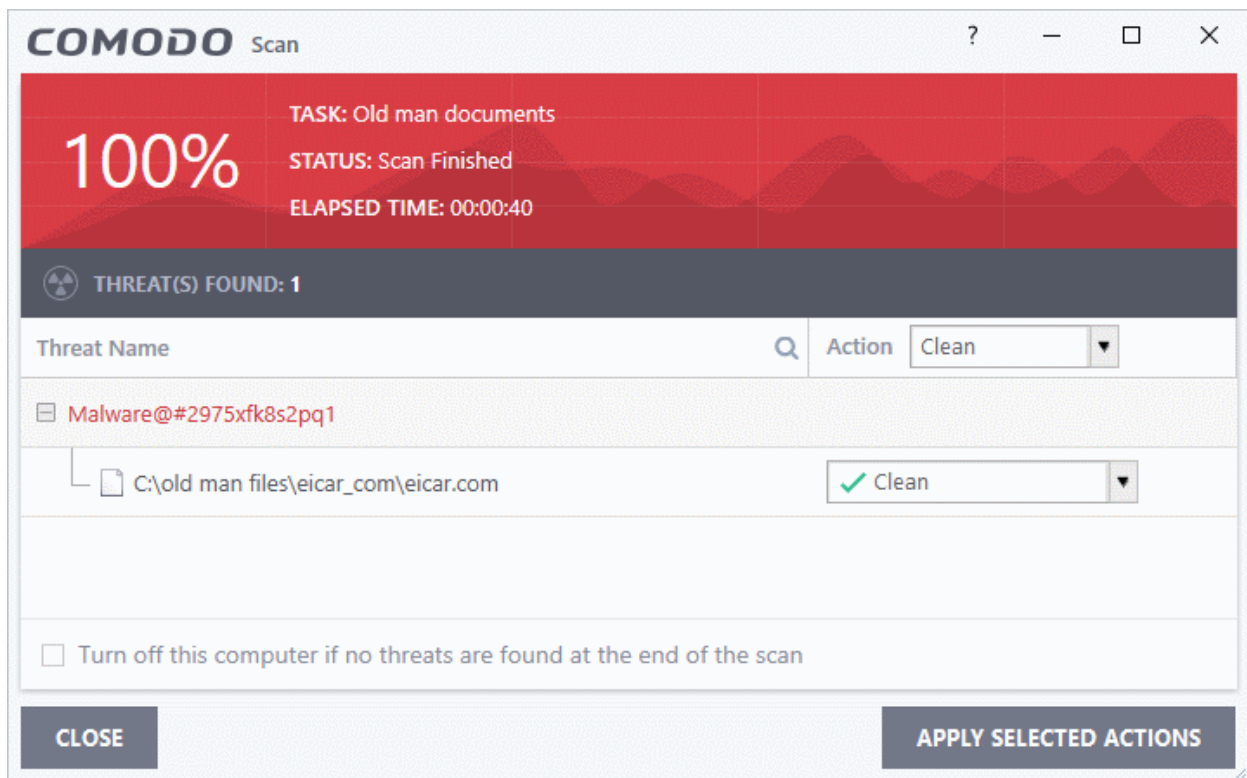
The results screen shows the number of detected threats and lets you decide what to do with them. You can clean, move to quarantine or ignore the threat. See **Process infected files** if you need help to decide.

2.2. Secure Shopping Settings

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

- Secure shopping delivers total protection for online banking and shopping by ensuring you connect to those sites from inside an highly secure virtual environment.
- This creates a threat-resistant tunnel between you and the website which cannot be monitored or attacked by other processes on your computer.
- Secure shopping is covered in more detail in **Comodo Secure Shopping**.

Open Secure Shopping:

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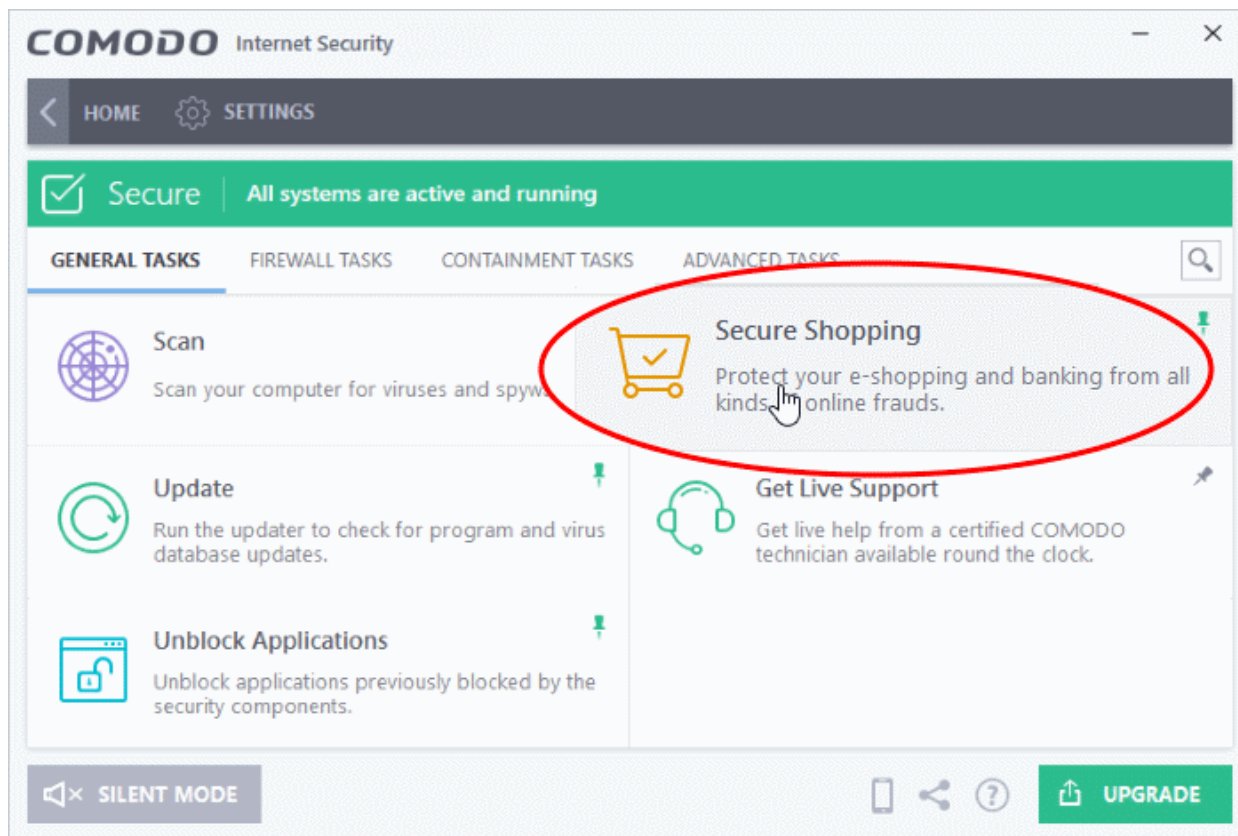
OR

- Click the 'Secure Shopping' icon from the CIS Desktop widget
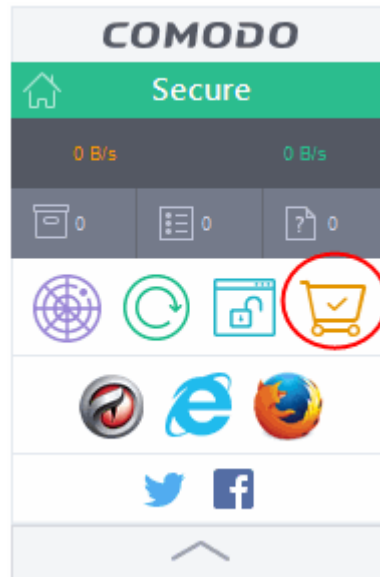
- Alternatively, double-click the secure shopping desktop shortcut:

When you start the application, a welcome screen will appear which explains the benefits of secure shopping:
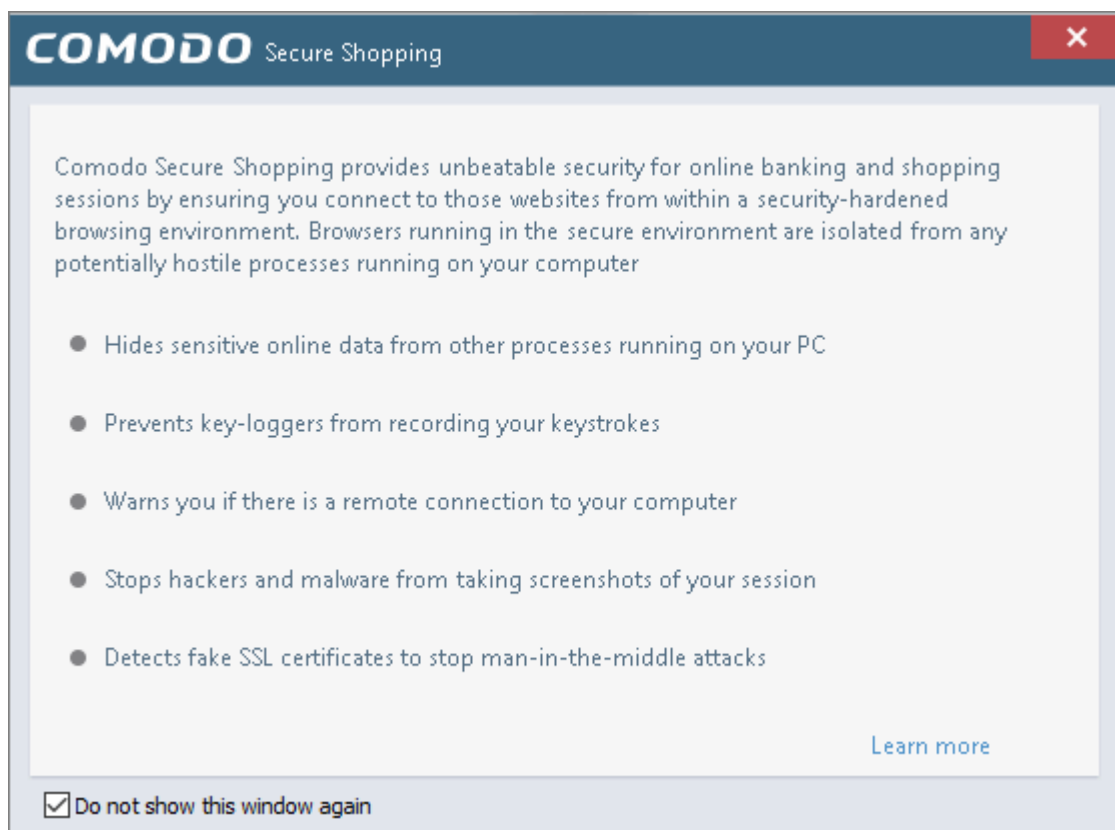
- Check 'Do not show this window again' to disable the welcome screen in future.

2.3. Manage Virus Database and Program Updates

- Click 'Tasks' > 'General Tasks' > 'Update'

In order to guarantee continued and effective antivirus protection, it is imperative that your virus database is kept up to date. Updates can be downloaded **manually** or **automatically**.

> **Prerequisite** - You must be connected to the internet to download updates.

Manually check for the latest virus and program updates

- Click 'Tasks' > 'General Tasks'
- Click the 'Update' tile:
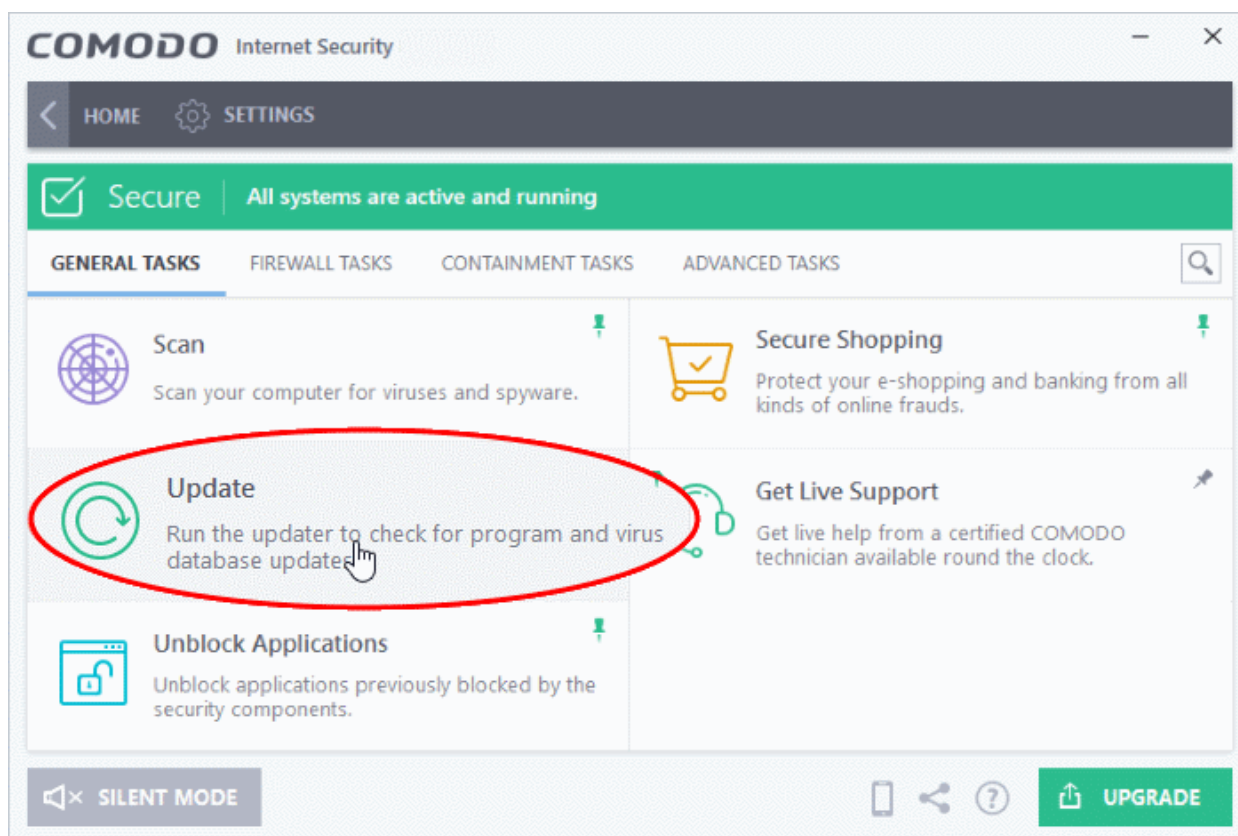
Signature updates are downloaded first if they are available:
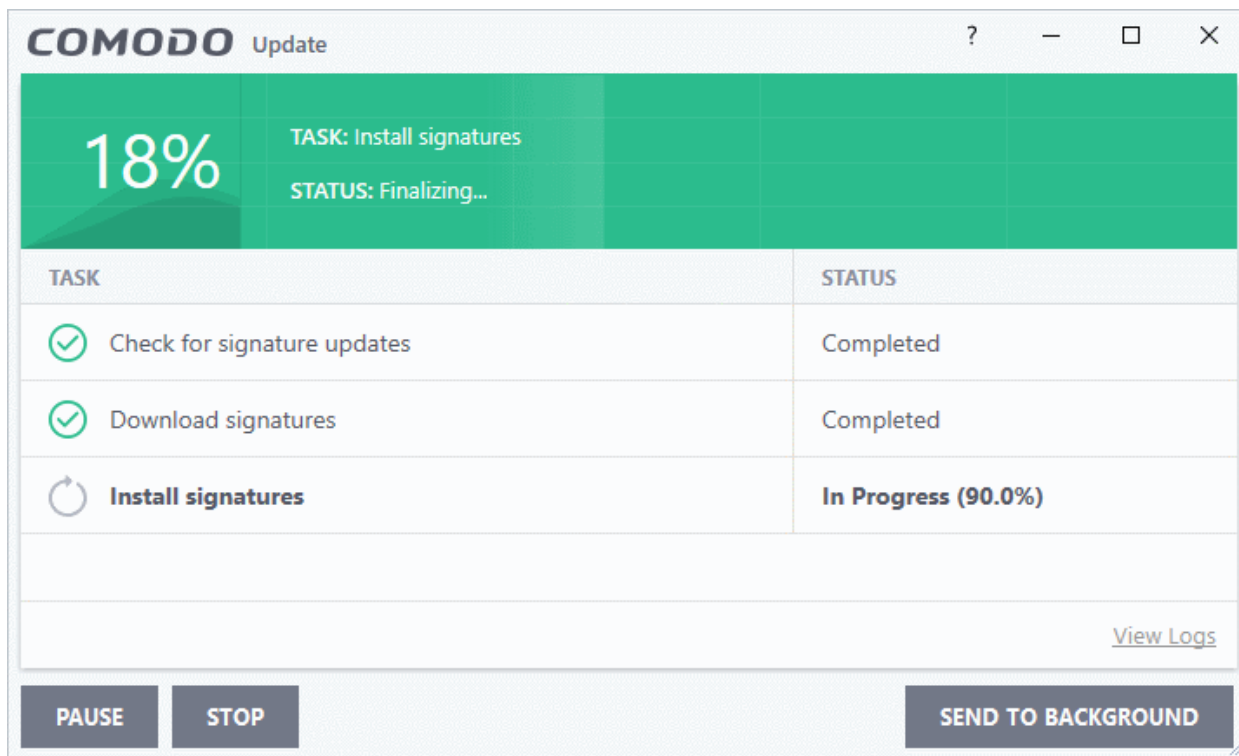
The updater then checks for web filter, VirusScope, and program updates:
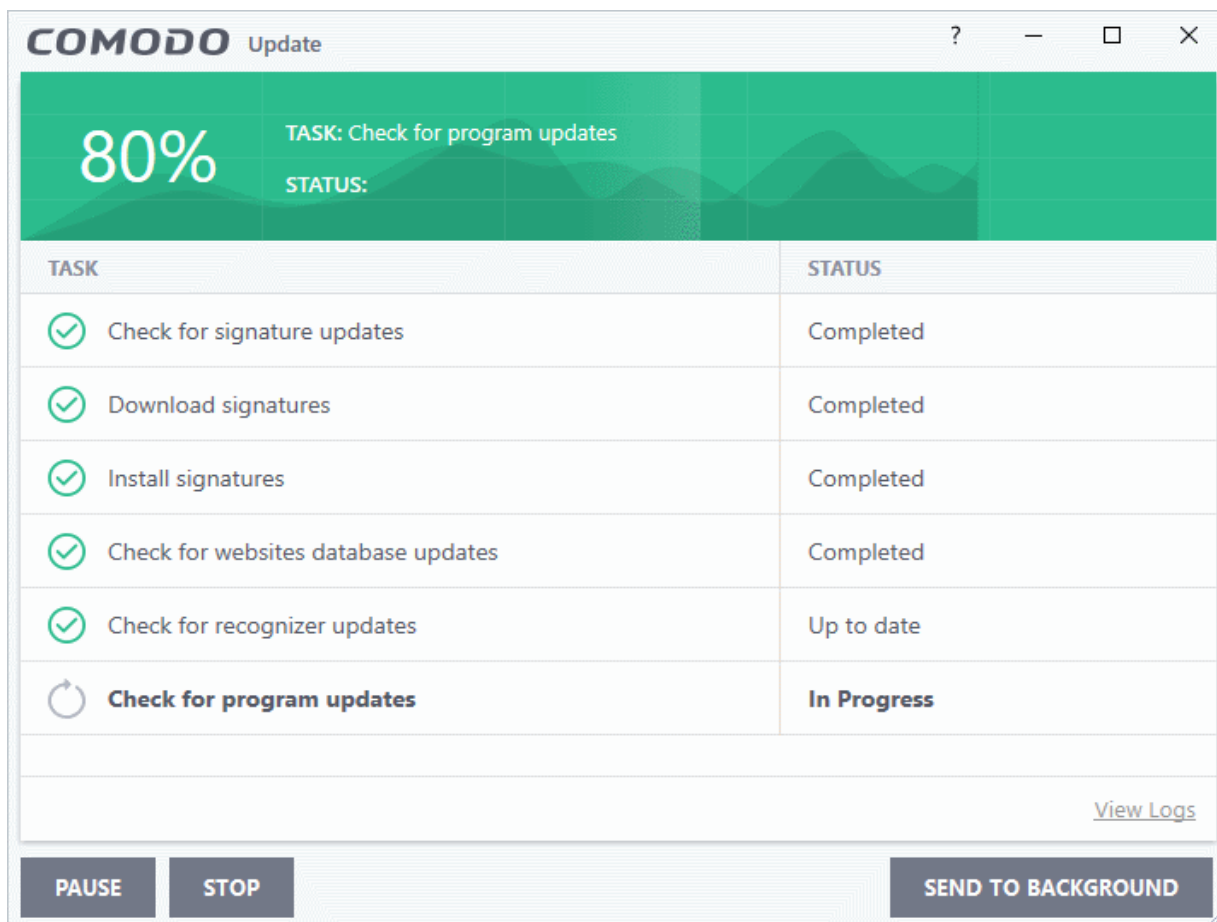
CIS will ask you to confirm the update at the following dialog:
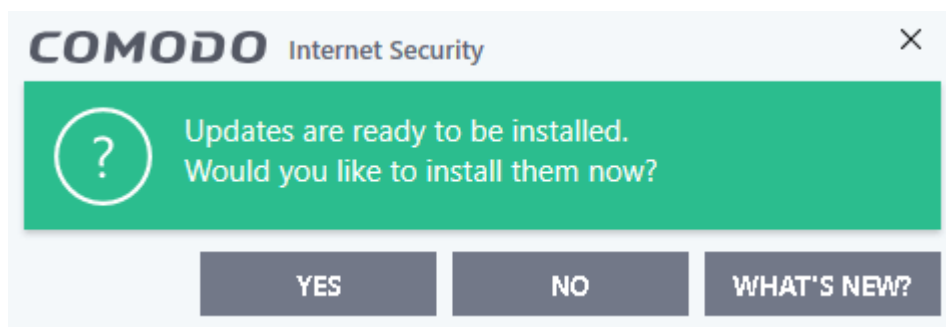
- Click 'Yes' to begin installation.

You need to restart the computer to complete the update process. You can restart immediately or postpone the restart until later:
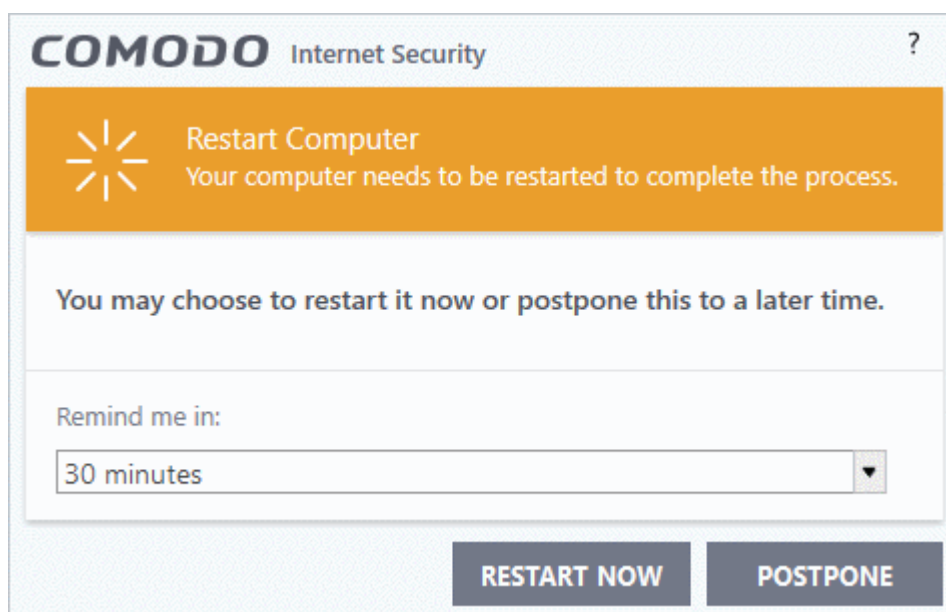
Automatic Updates

By default, Comodo Internet Security automatically checks for and downloads database and program updates. You can modify these settings in '**Settings**' **>** '**General Settings**' **>** '**Updates**'.
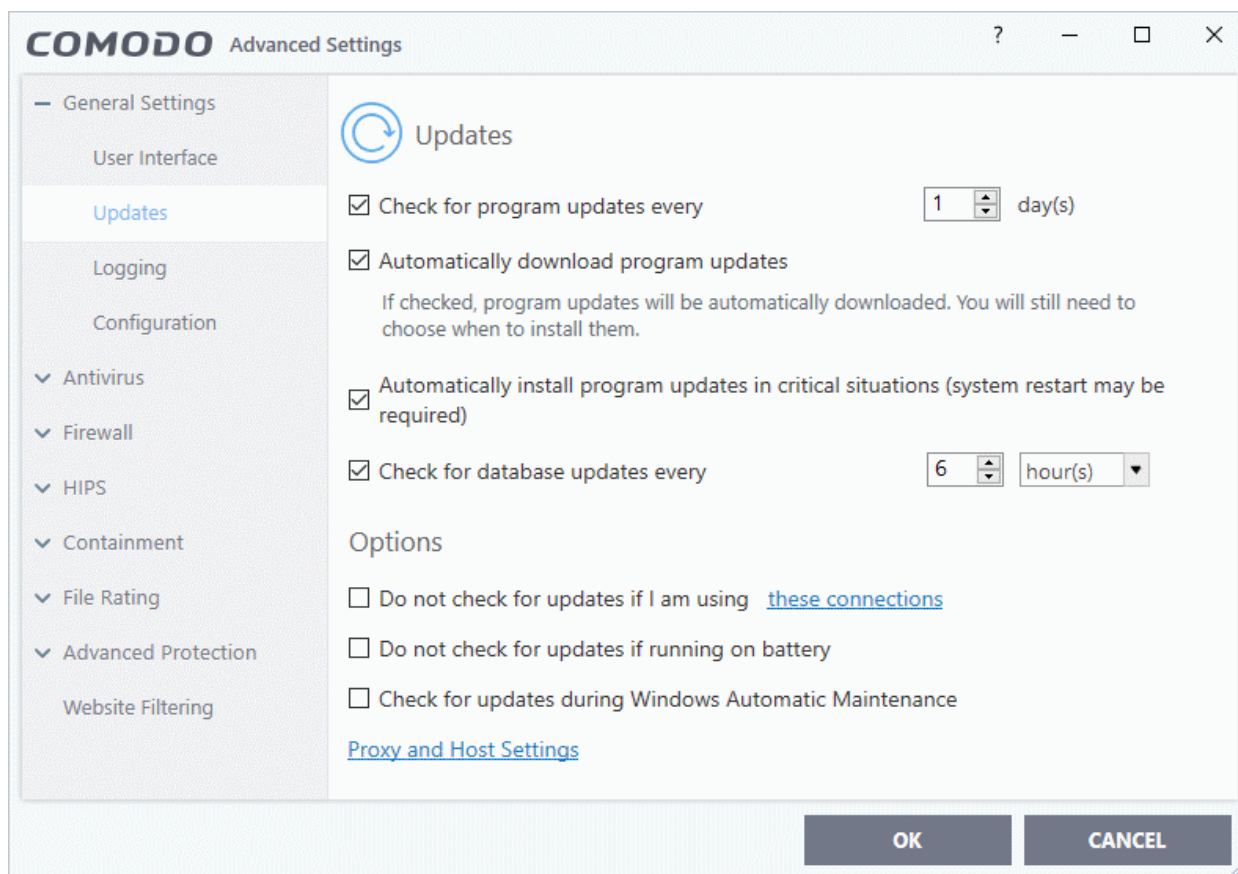
You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. See '**Scan Profiles**' for more details.

2.4. Get Live Support

Click 'Tasks' > 'General Tasks' > 'Get Live Support'

- Comodo GeekBuddy is a chat based support service provided by friendly computer experts at Comodo.
- If you experience issues with your computer, you can start a chat session with our technicians and get them to fix the problem. If you allow, they can even establish a remote connection to your PC and apply fixes right in front of your eyes.
- GeekBuddy is included with CIS Pro and Complete.

Initiate a chat session and get live support

- Click 'Tasks' > 'General Tasks'
- Click the 'Get Live Support' tile
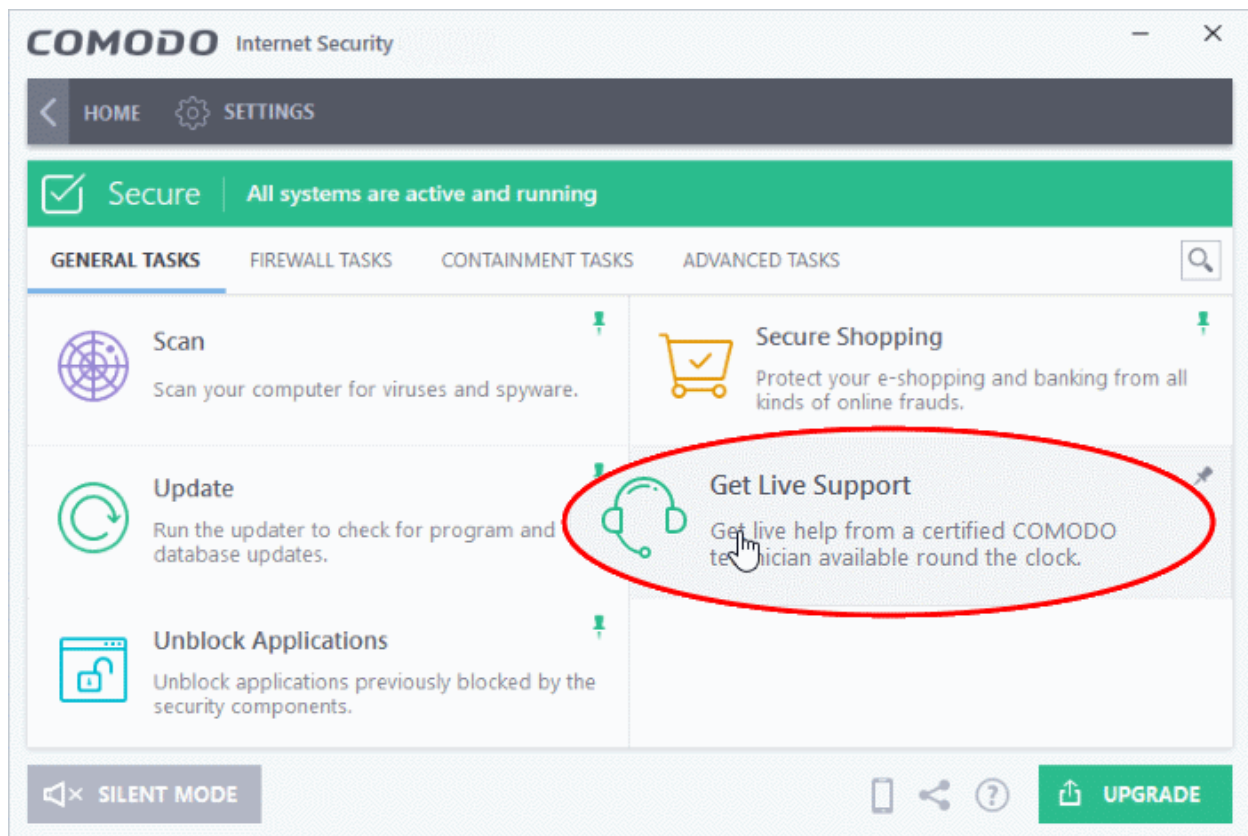
See '**Comodo GeekBuddy**' for more details about the service.

2.5. Manage Blocked Items

Click 'Tasks' > 'General Tasks' > 'Unblock Applications'

- A file may be blocked by any one of the antivirus, containment, firewall or HIPS components.

- The unblock applications screen lets you review all blocked files and release those you consider safe. You can also assign a new trust rating to a blocked file. CIS will handle the file based on the rating in future.

- If you unblock an item, CIS will automatically make changes to allow it to run in future. The change made depends on the component which blocked the file:

  - **Antivirus** - The item is added to the scan exclusion list. Click '**Settings' > 'Advanced Protection' > 'Scan Exclusions**' to manage this list.
  - **Firewall** - An 'Allow' rule is added to application rules. Click '**Settings' > 'Firewall' > 'Application rules**' to manage these rules.
  - **Containment** - An 'Ignore' rule is added to containment rules. Click '**Settings' > 'Containment' > 'Auto-containment**' to manage these rules.
  - **HIPS** - An 'Allow' rule is added to HIPS Rules. Click '**Settings' > 'HIPS' > 'HIPS Rules**' to manage these rules.

- You can unblock from all components, or only the component that blocked it.

View and manage blocked applications

- Click 'Tasks'> 'General Tasks' tab
- Click the 'Unblock Applications' tile
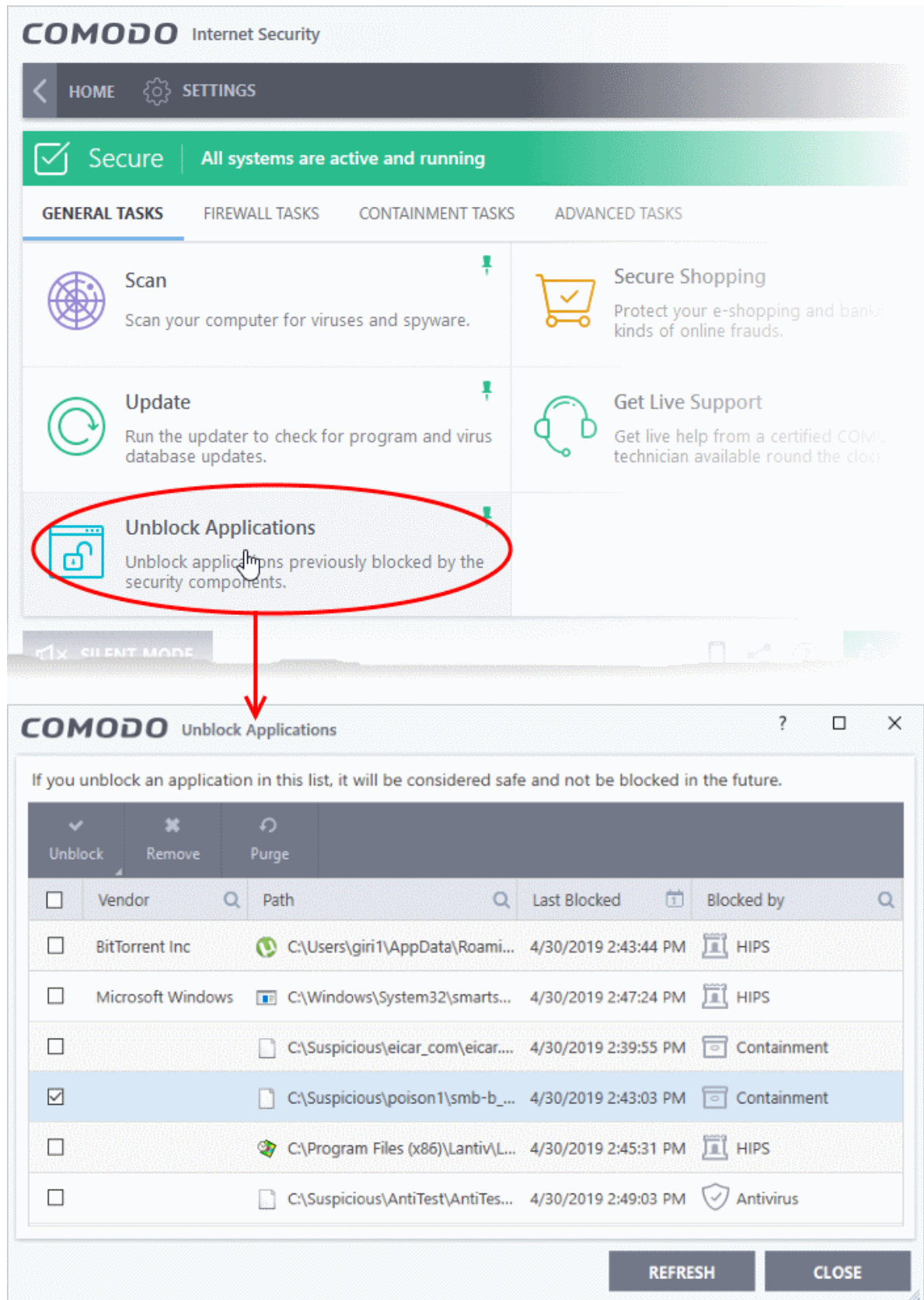
Unblock Applications - Column Descriptions	
Column Header	**Description**
Vendor	The publisher of the blocked application.
Path	The install location of the blocked application

Last Blocked	Date and time the application was most recently stopped from running.
Blocked by	The security component that stopped the application from running. Can be 'Antivirus', 'HIPS', 'Firewall' or 'Containment'.

- Click any column header to sort items in alphabetical order

The interface allows you to:

- **Unblock items and allow them to run**
- **View item details and assign a trust rating**
- **Remove an item from the list**
- **Purge an item in the list**

Release blocked Items

- Click 'Tasks'> 'General Tasks' tab
- Click the 'Unblock Applications' tile
- Select an item or items from the list
- Click 'Unblock' at the top-right

- **Unblock for component(s) shown in 'Blocked by' column** - Item will only be released from the security component that blocked it.
- **Unblock for all security components** - Item will be released from all security components

See the intro for a **list of the rules that are created** per-component for unblocked items.

Example:

In the example shown below, 'LanTime.exe' was blocked by HIPS.
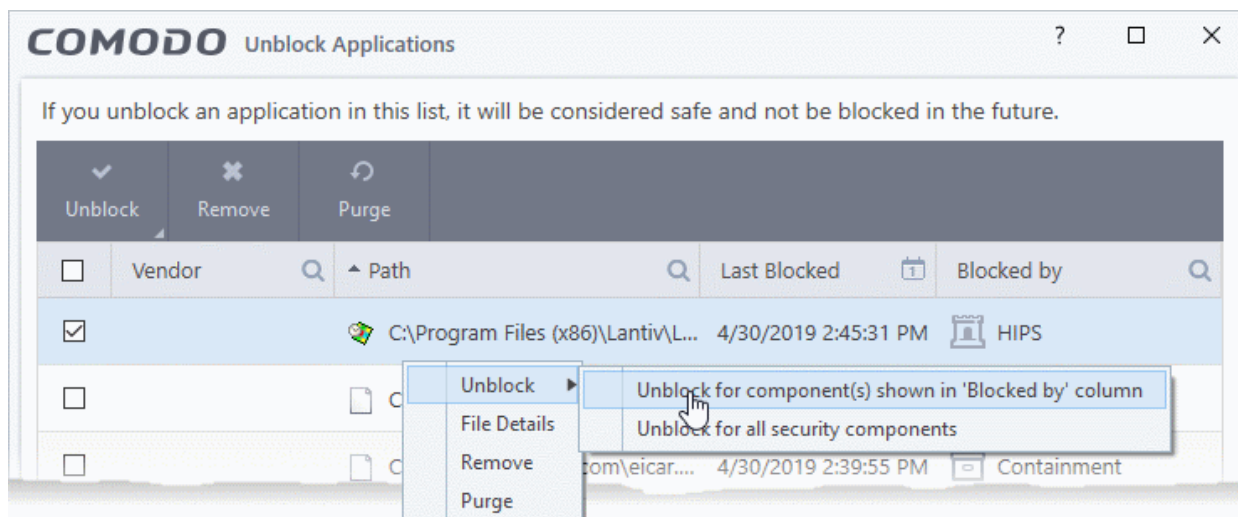
- If you unblock the file, an 'Allowed Application' rule is created in HIPS.

- To view the rule:
    - Click 'Settings' > 'HIPS' > 'HIPS Rules'
    - Select the application and click 'Edit':
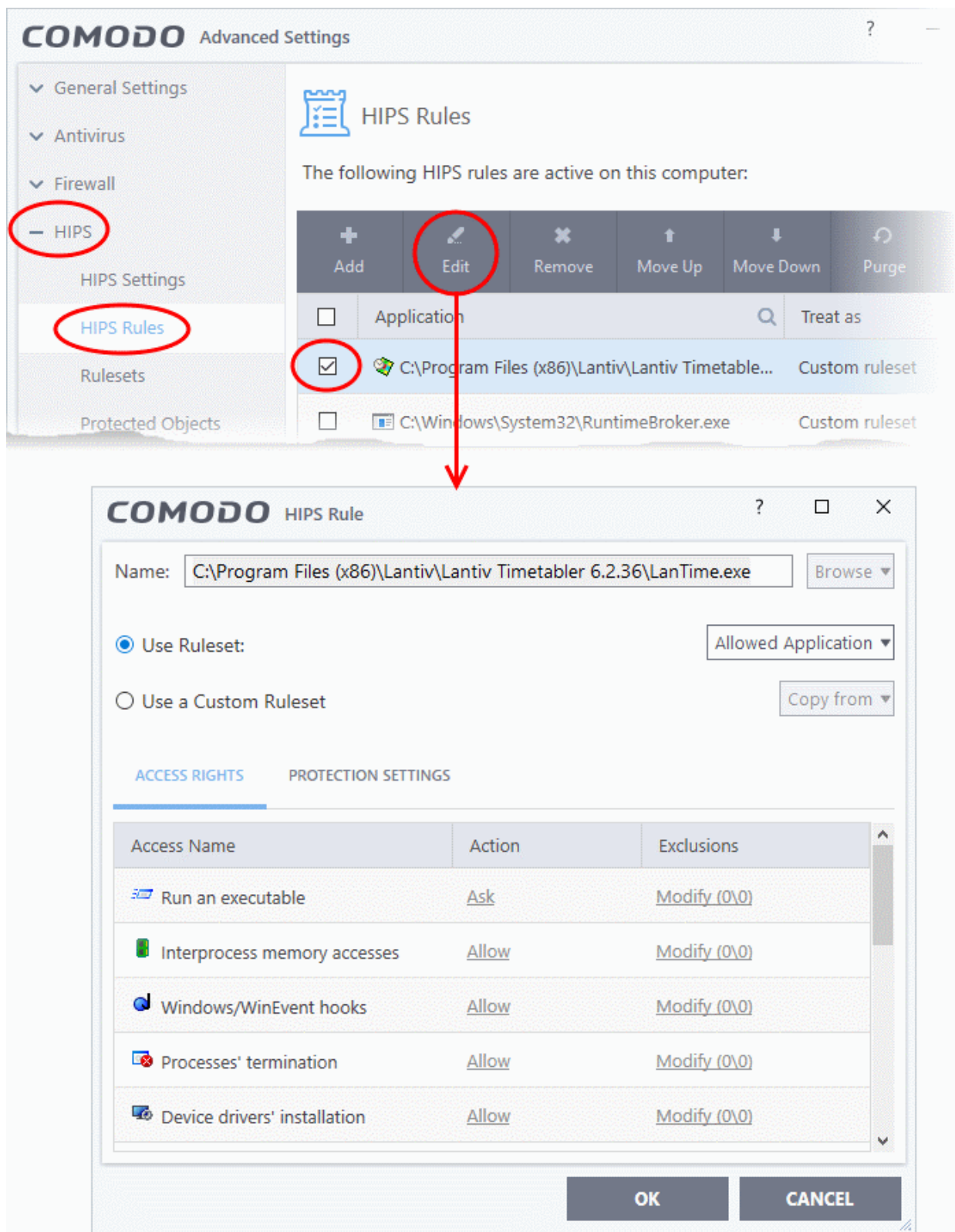
View item details and assign a trust rating

- Click 'Tasks'> 'General Tasks' tab
- Click the 'Unblock Applications' tile

- Right-click on an item and choose 'File Details' from the context sensitive menu.
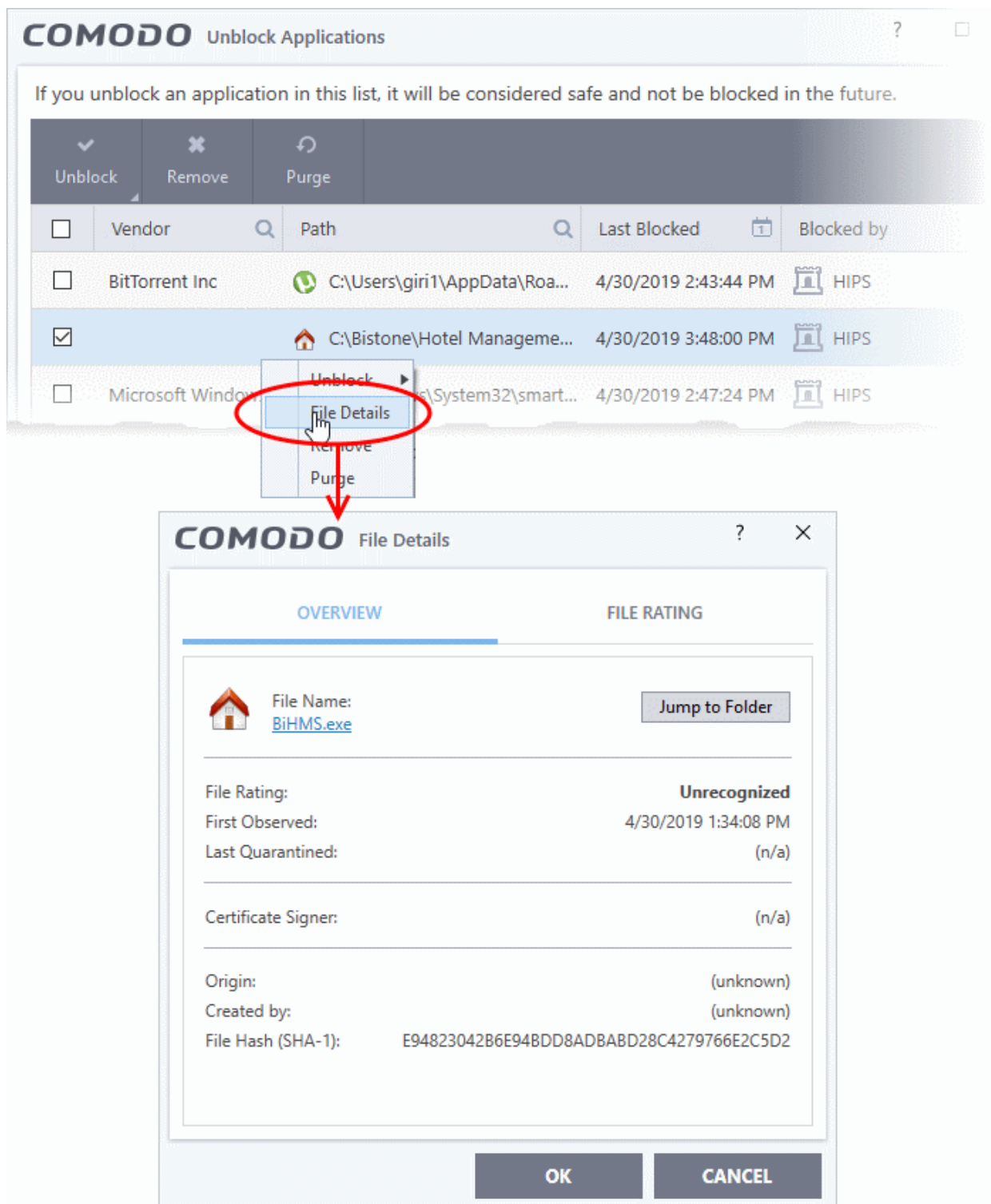
The 'File Details' dialog has two tabs:

- **Overview**
- **File Rating**

Overview

The 'Overview' tab shows general details such as the file rating, discovery date, hash value and publisher (signer):
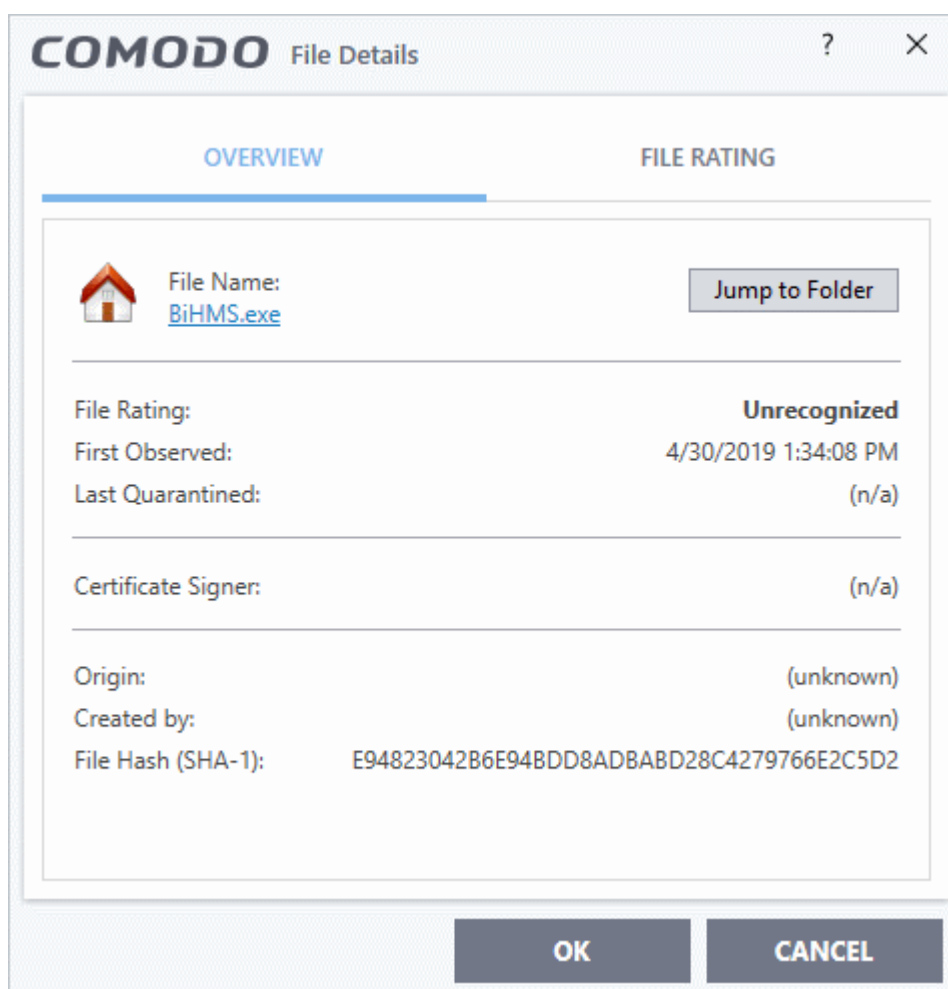
- Click the file name to open the Windows 'File Properties' dialog.
- Click 'Jump to folder' to open the folder containing the file in Windows Explorer, with the respective file selected.

File Rating

- Shows the file's current trust rating from Comodo and lets you set your own rating:
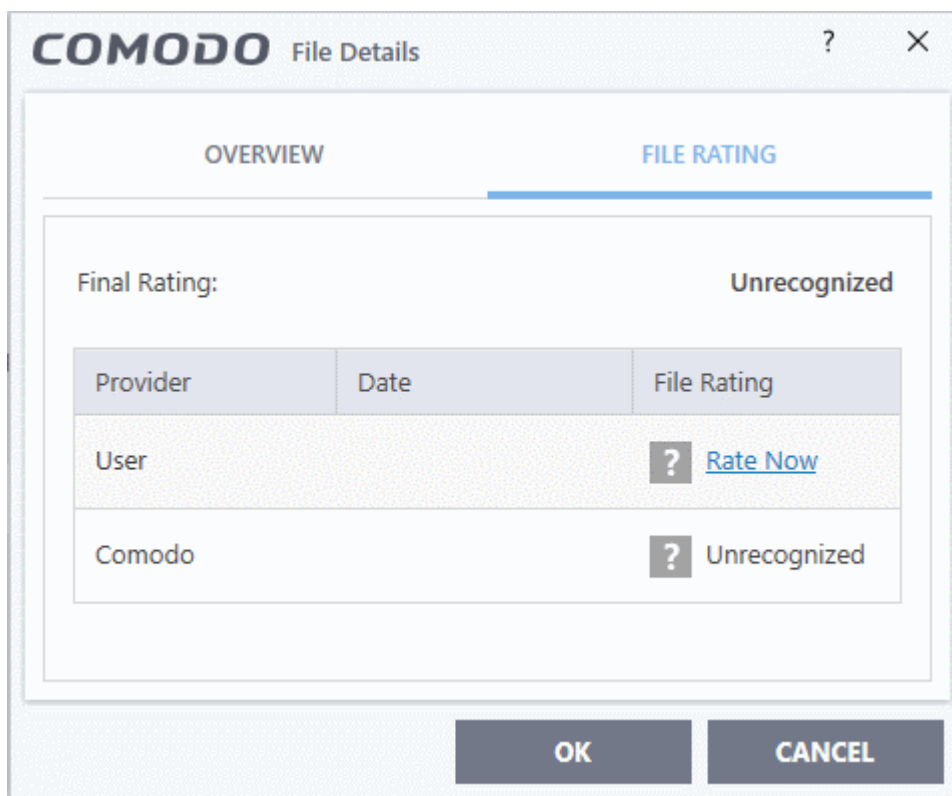
- Click the 'Rate Now' link beside 'User' and choose the rating from the drop-down
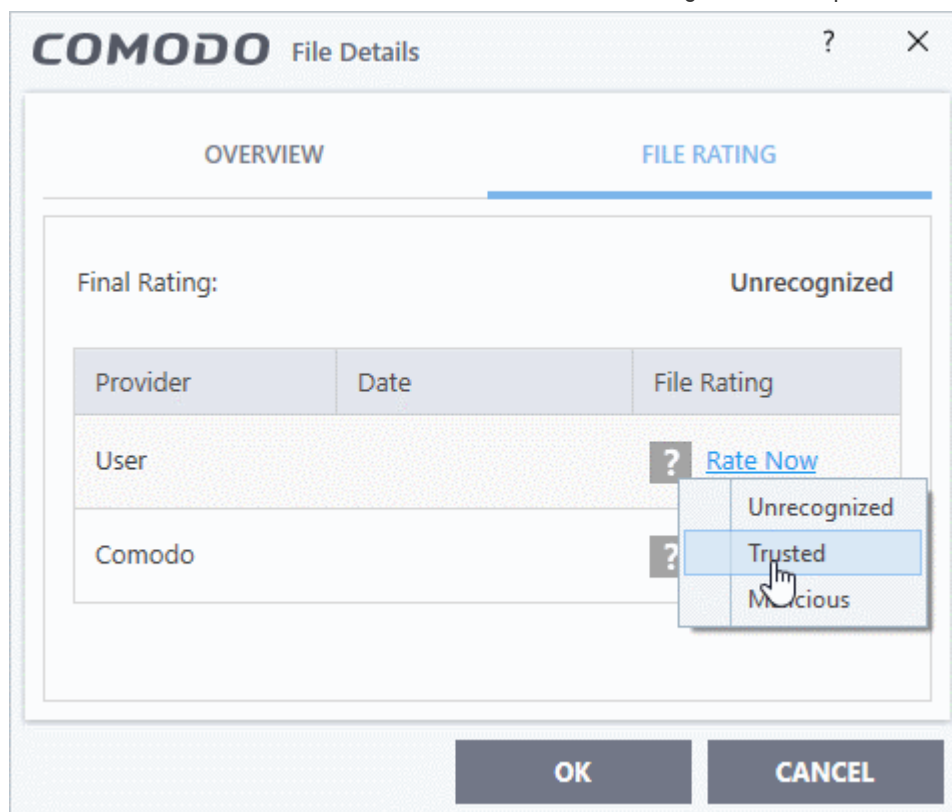
The options available are:

- **Trusted** - The file is considered safe and allowed to run without any alerts
- **Unrecognized** - The file is neither definitely safe nor definitely malicious. The files privileges are determined by your HIPS settings ('Settings' > 'HIPS').
- **Malicious** - The file will be deleted or placed in quarantine.
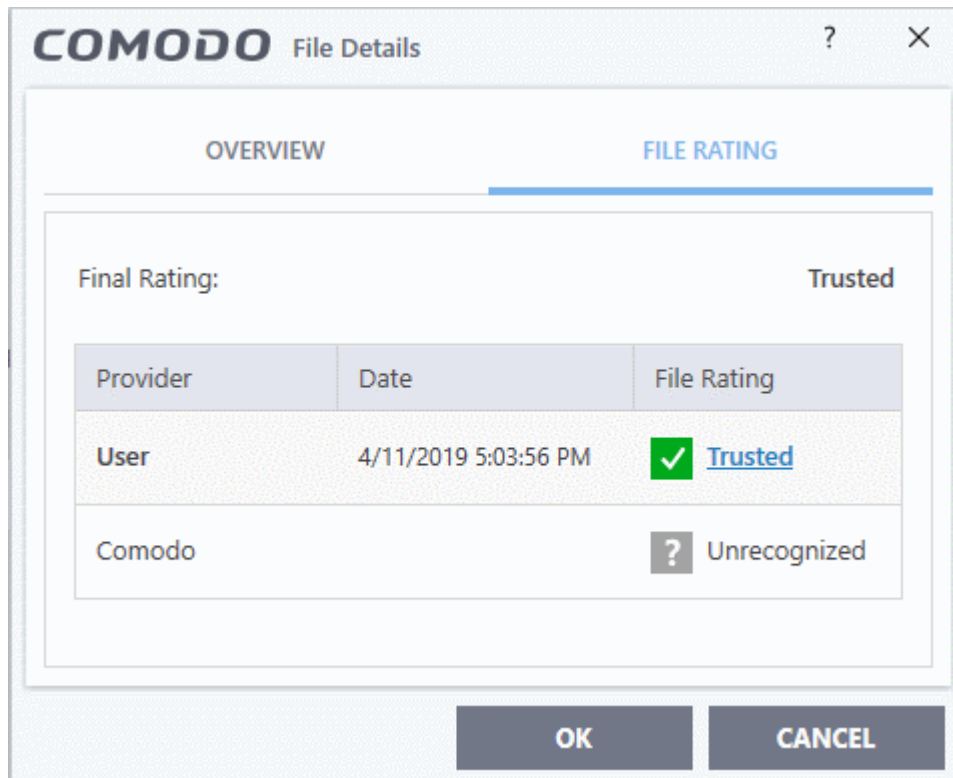
- Click 'OK'.
- Your new rating is applied to the file as a 'User Rating'.
- Click 'Settings' > 'File Rating' > 'File List' to view the file and its rating.

Remove an application from the 'Unblock Applications' list

- Click 'Tasks'> 'General Tasks' tab
- Click the 'Unblock Applications' tile
- Select an item from the list
- Click the 'Remove' button at the top
- Alternatively, right-click on an item and choose 'Remove' from the context sensitive menu.

Purge Files from the 'Unblock Applications' list

CIS checks whether the files in the list are still installed at the path stated. Files that are no longer present are removed from the list.

- Click 'Tasks'> 'General Tasks' tab
- Click the 'Unblock Applications' tile
- Click the 'Purge' button at 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 are wary about an item you have copied from an external source or downloaded from the internet.

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
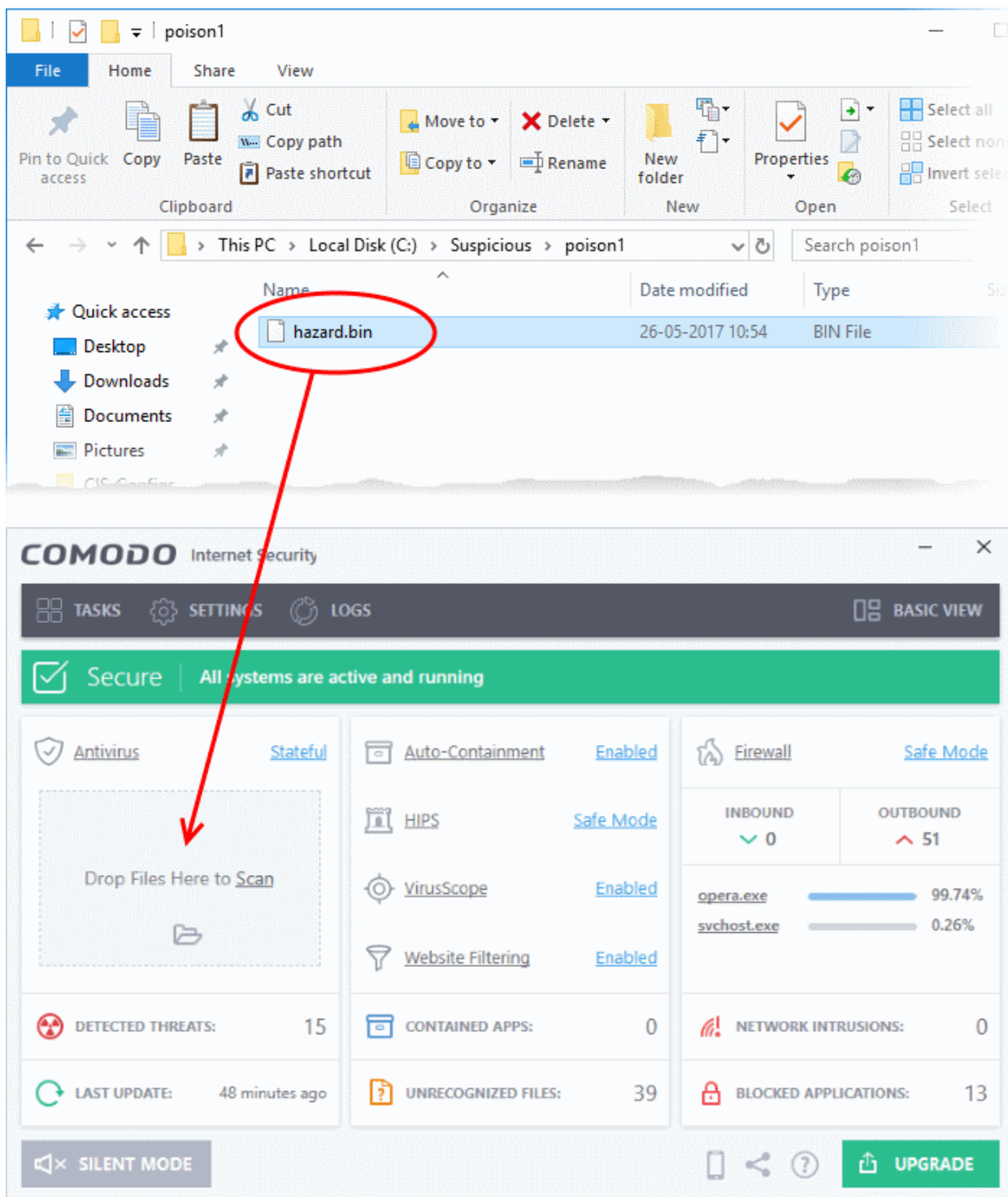
• Right click on a file and select 'Scan with Comodo antivirus' from the context sensitive menu
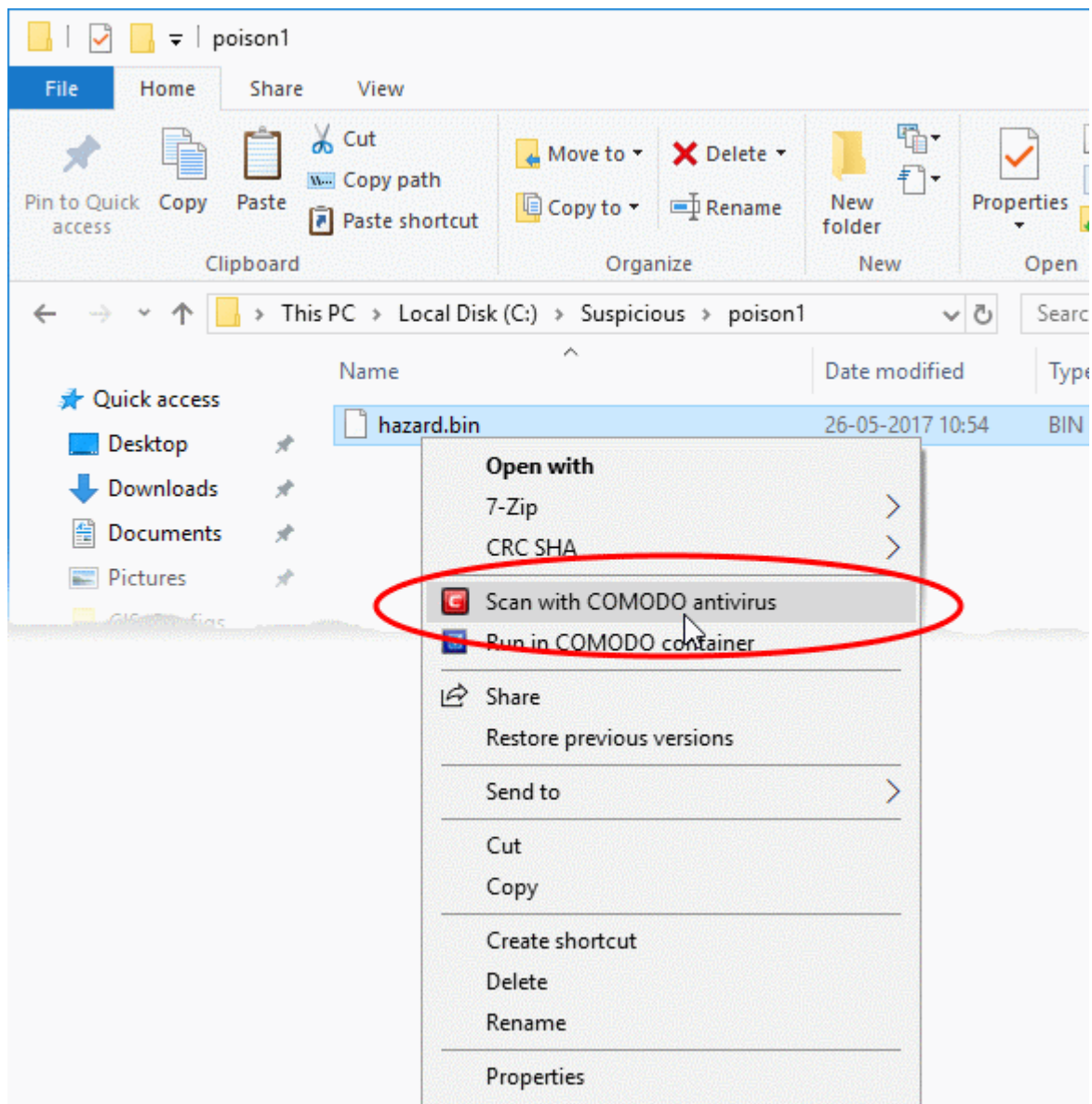
The item will be scanned immediately.

- The scan results screen will be displayed.
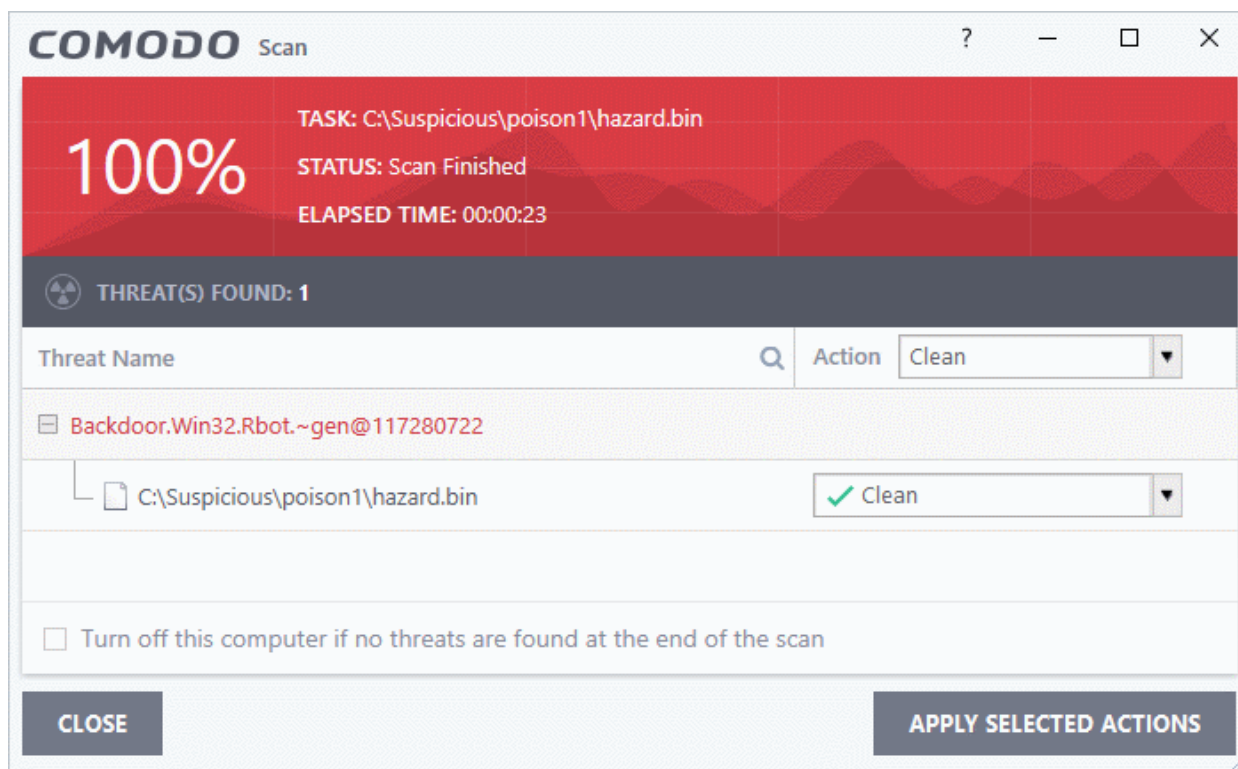
You can choose to clean, quarantine or ignore the threat. See **Process infected files** for more details.

2.7. Process Infected Files

The results table at the end of a scan lists all detected threats:
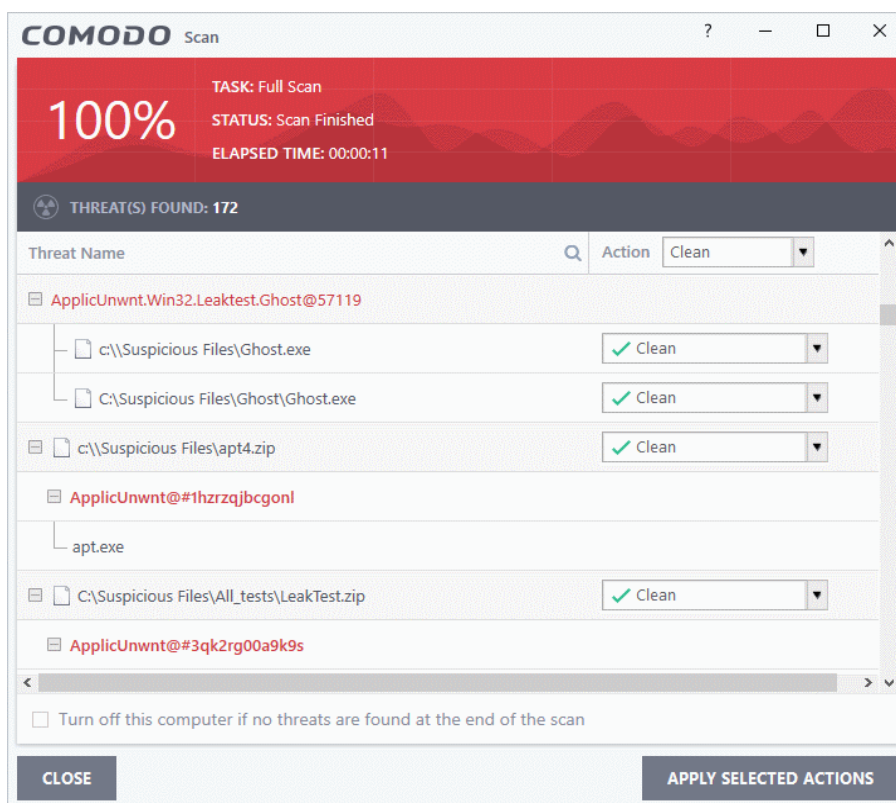
- Use the drop-down menus to apply actions to individual files:
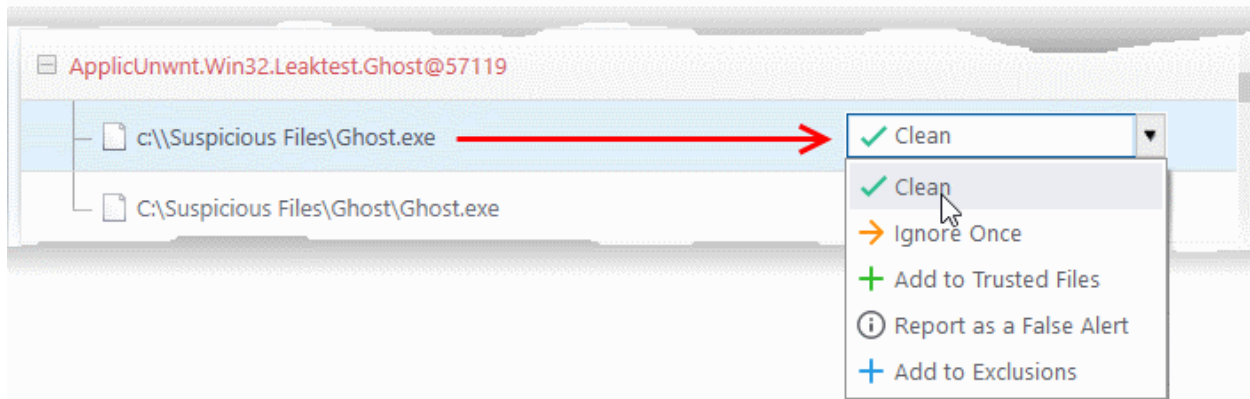
- Or use the 'Action' drop-down at top-right to apply your choice to all threats.
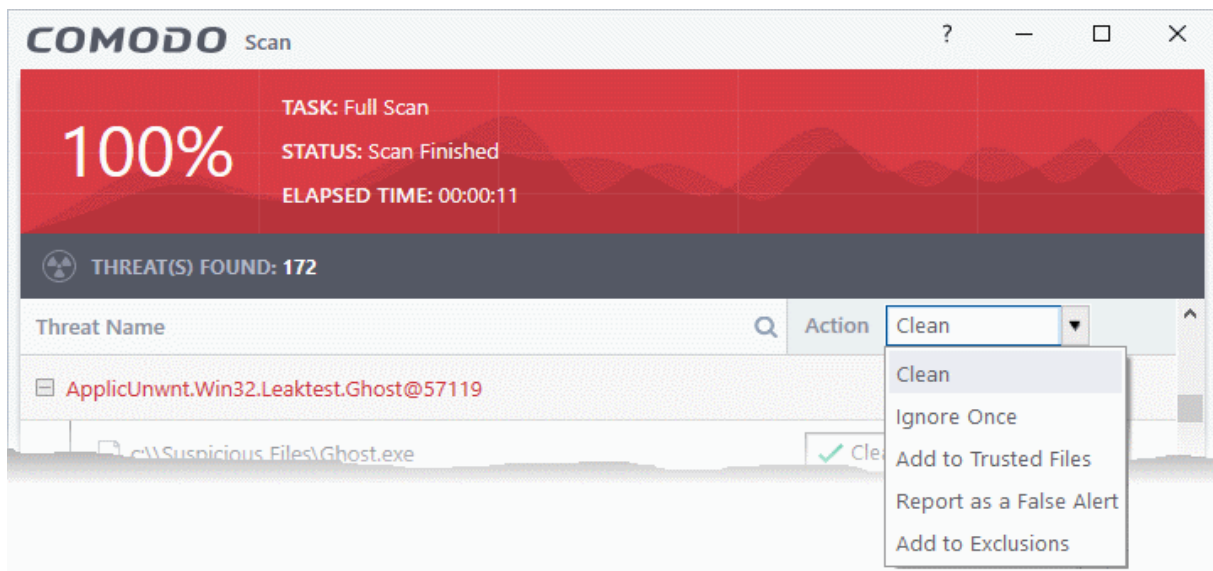
Available actions are:

- **Clean** - The virus is removed from the file if a disinfection routine is available. The clean file is the left at its original location. If no routine exists, the file is placed in quarantine for your review. Click 'Tasks' > 'Advanced Tasks' > 'View Quarantine' to view this area. See **Manage Quarantined Items** for more details.

- **Ignore Once** - Allows the file to run this time only. The file will still get flagged as a threat by future antivirus scans.

- **Add to Trusted Files** - Creates an exception for the file by giving it a 'Trusted' rating in the **File List** ('Settings' > 'File Rating' > 'File List'). The AV scanner will not detect the file as a threat in future scans. Only select this option if you are sure the file is trustworthy.

- **Report as a False Alert** - Sends the file to Comodo for further analysis. Submitting a false positive will also add the item to trusted files, so it won't get flagged by future scans. The file will be added to the global whitelist if Comodo confirms the false-positive.

- **Add to Exclusions** - Creates an exception for the file so it won't get flagged by future virus scans. You can review exclusions at 'Settings > 'Advanced Protection' > '**Scan Exclusions**'. The file's trust rating does not change.

Click 'Apply Selected Actions'. The result is shown in the 'Actions' column:

---
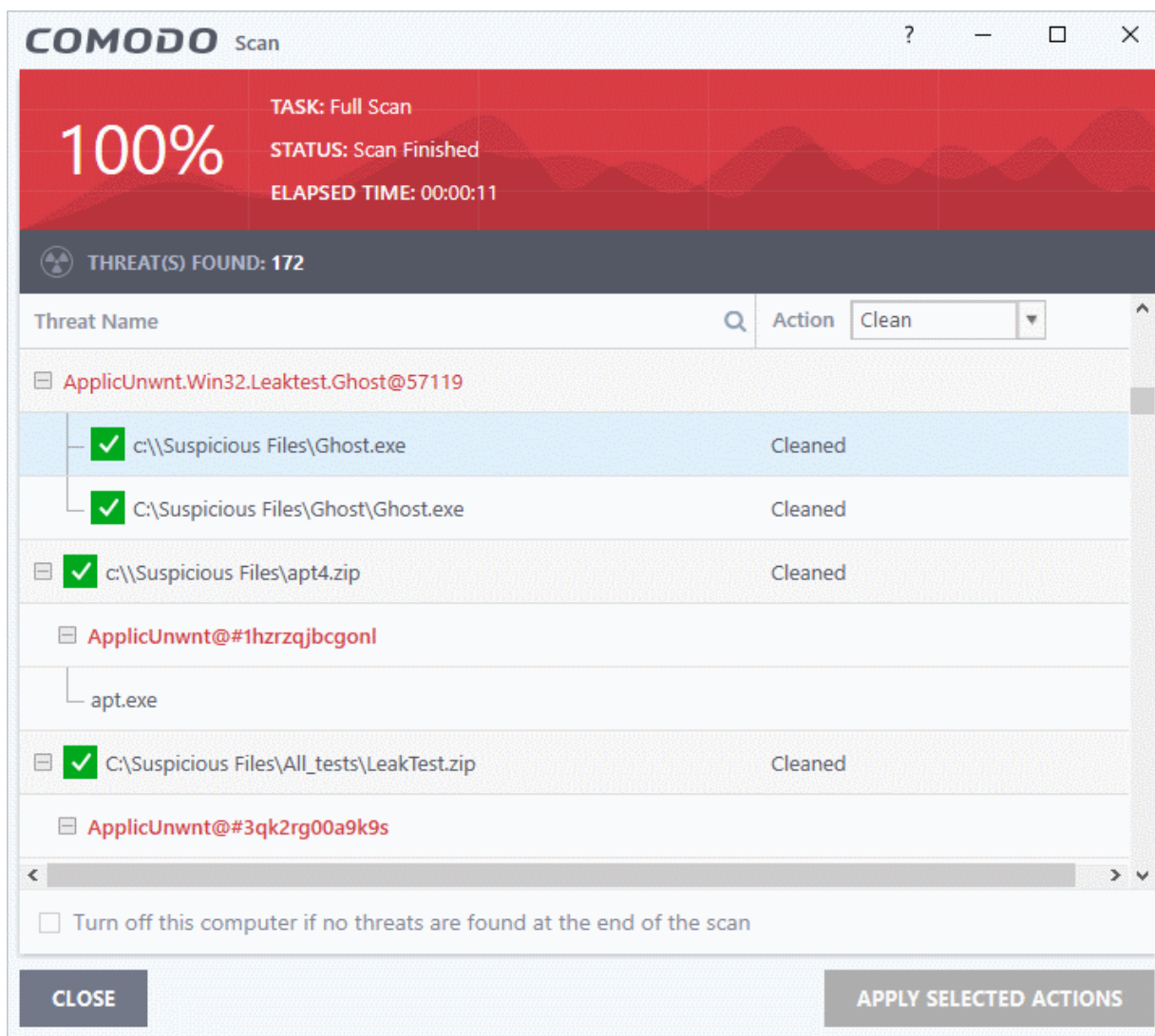
3. Firewall Tasks - Introduction

Click 'Tasks' > 'Firewall Tasks'

- The firewall offers the following main benefits:

    - Monitors all network traffic to protect your computer against inbound and outbound threats

    - Hides your computer's ports from hackers

    - Blocks malicious software from transmitting your confidential data over the internet.

- The firewall tasks area lets you configure internet access rights per-application, stealth your computer ports, view active connections, and even block all traffic in and out of your computer.

    - In addition to this tasks screen, you can also **configure advanced firewall settings** at 'Settings' > 'Firewall'.
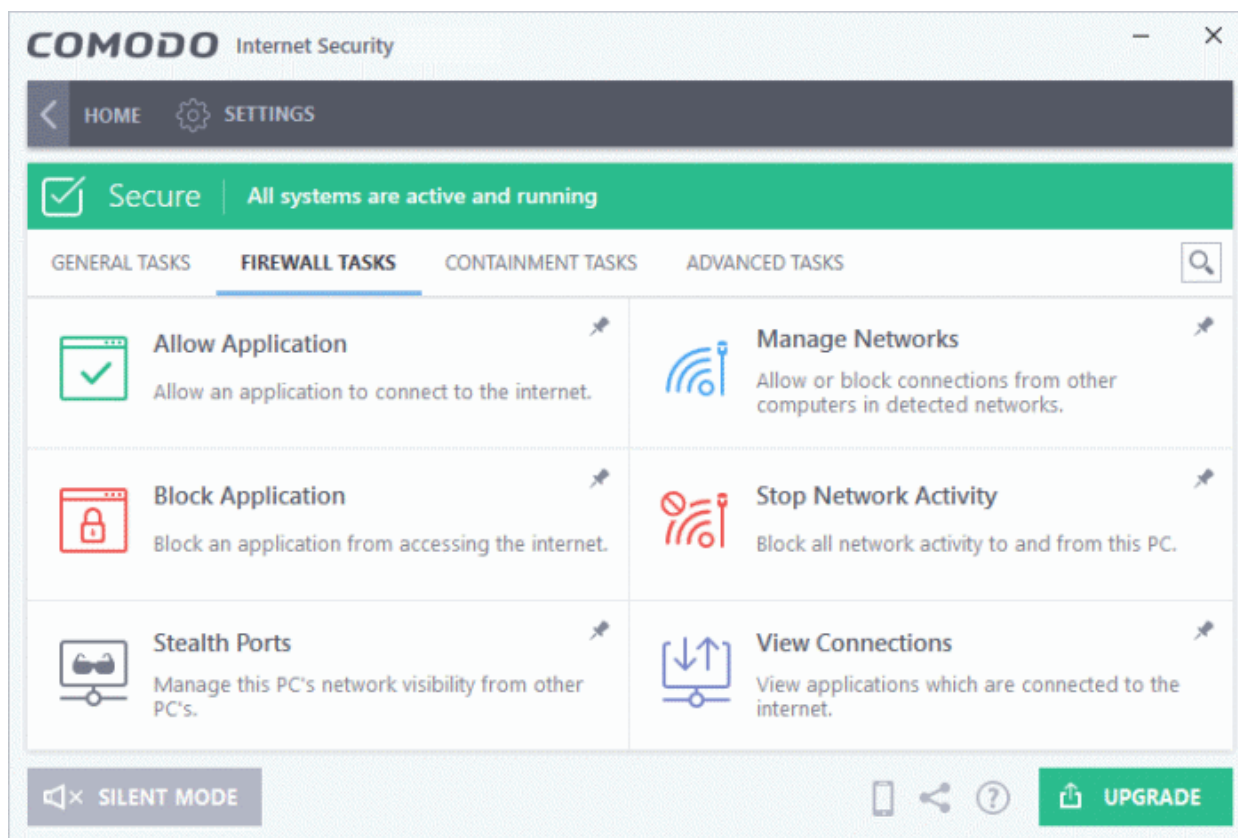
See the following sections for help with each area:

- **Configure internet access rights for applications**
- **Manage network connections**
- **Stop all network activity**
- **Stealth your computer ports**
- **View active Internet connections**

3.1. Configure internet access rights for applications

Click 'Tasks' > 'Firewall Tasks' > 'Allow Application' or 'Block Application'

- The firewall tasks screen lets you quickly allow or block applications from accessing the internet.
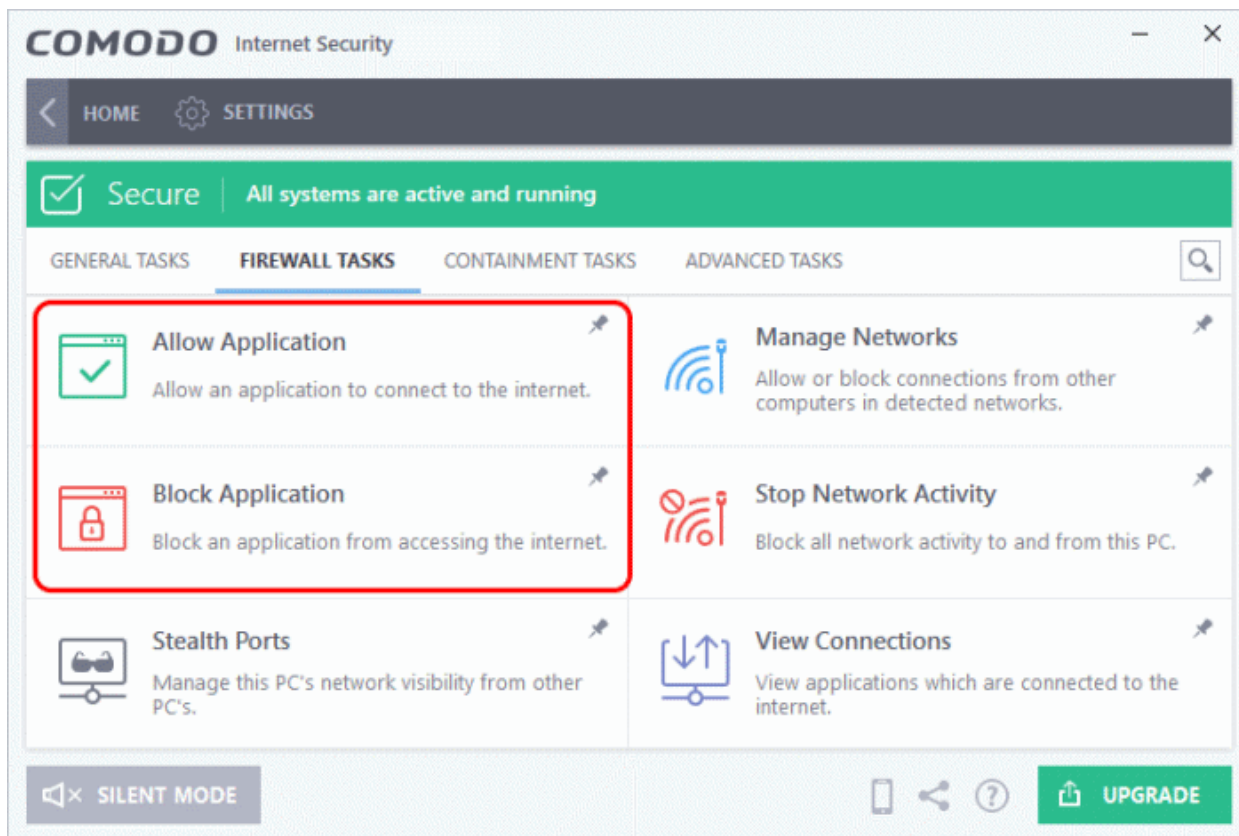
Allow an application to connect to the internet

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Allow Application'
- Browse to the main executable file of the application
- Click 'Open'.
- This will create an 'Allow Request' rule for the application in 'Settings' > 'Firewall' > 'Application Rules'

Block an application's Internet access rights

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Block Application'
- Browse to the main executable file of the application
- Click 'Open'.
- This will create an 'Block Request' rule for the application in 'Settings' > 'Firewall' > 'Application Rules'

See '**Application Rules**' for more info about creating internet access rules.

Tip: If you plan to regularly allow/block applications, right-click on the appropriate tile then select 'Add to Task Bar'. You can then quickly access the action on the CIS home screen and the widget:
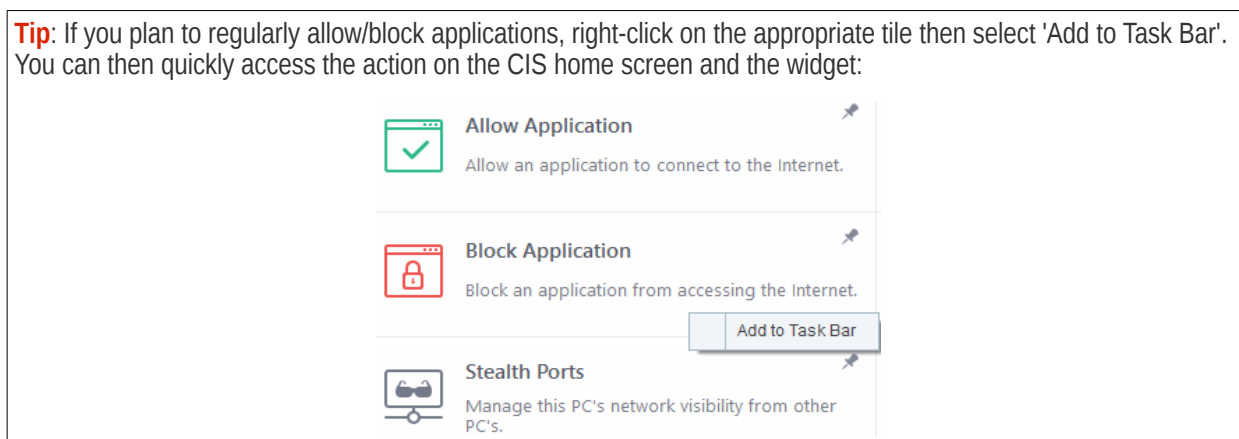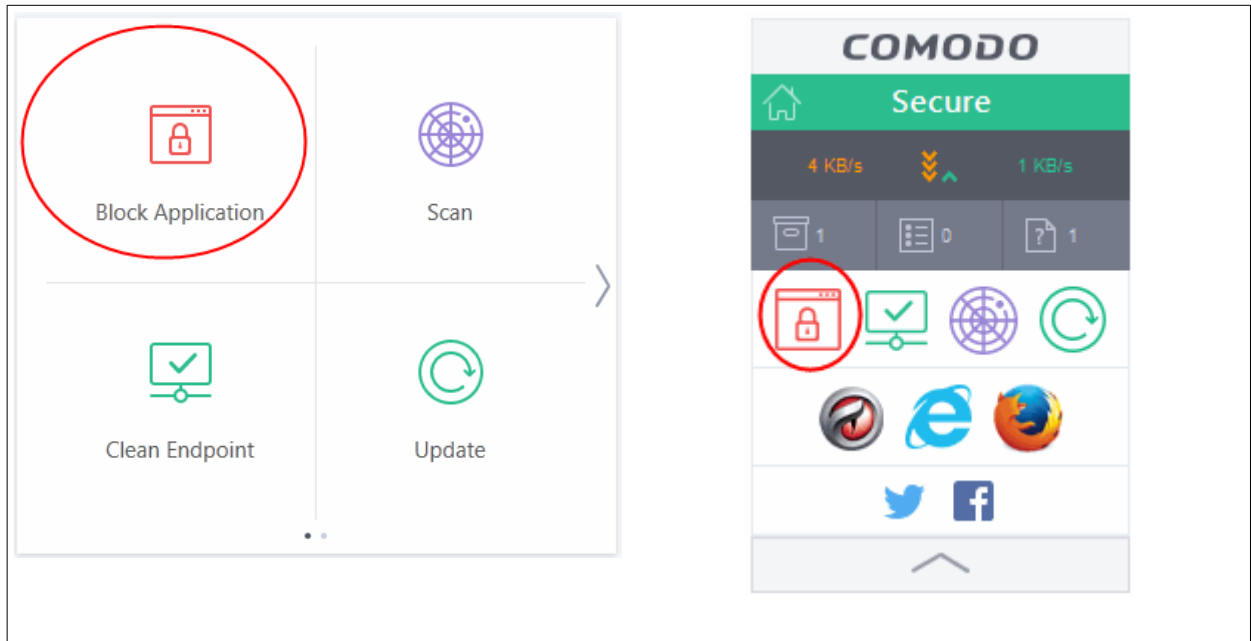
3.2. Manage Network Connections

Click 'Tasks' > 'Firewall Tasks' > 'Manage Networks'

- The manage connections interface lets you quickly view all wired and wireless networks to which your computer is connected.
- The lower half of the panel show each network's name, IP address and gateway.
- You can choose to allow or block a connection from this interface

View all network connections

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Manage Networks'
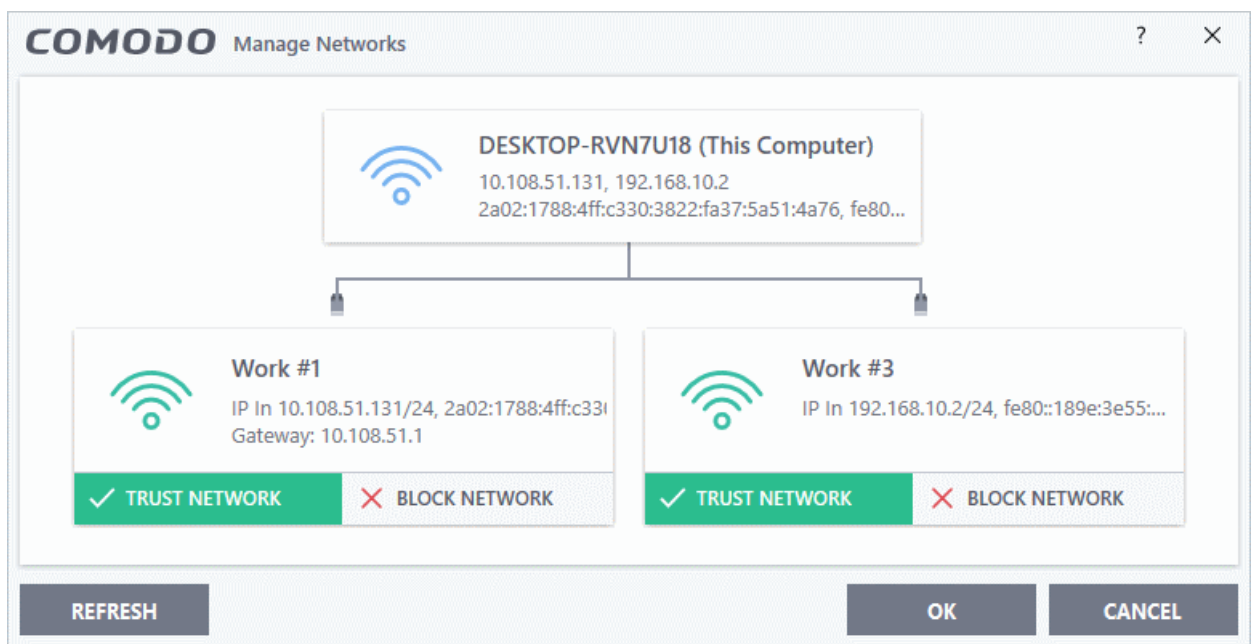
- Use the handles (< >) to scroll through all available networks or computers
- **Trust Network** and **Block Network** - You can trust or block a network by clicking the appropriate button under the network in question. You will no receive any inbound or outbound traffic from blocked networks.

- **Refresh** - Reloads the list with the latest network connections. Click this button if you have recently made network changes that 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

Click 'Tasks' > 'Firewall Tasks' > 'Manage Networks'

- The 'Stop Network Activity' feature terminates all inbound/outbound communication between your computer and outside networks (including the internet).

- Connections will remain closed until you re-enable them by clicking 'Restore Network Activity'.

- This lets you quickly take your computer offline without having to delve into Windows network settings, and without unplugging cables.
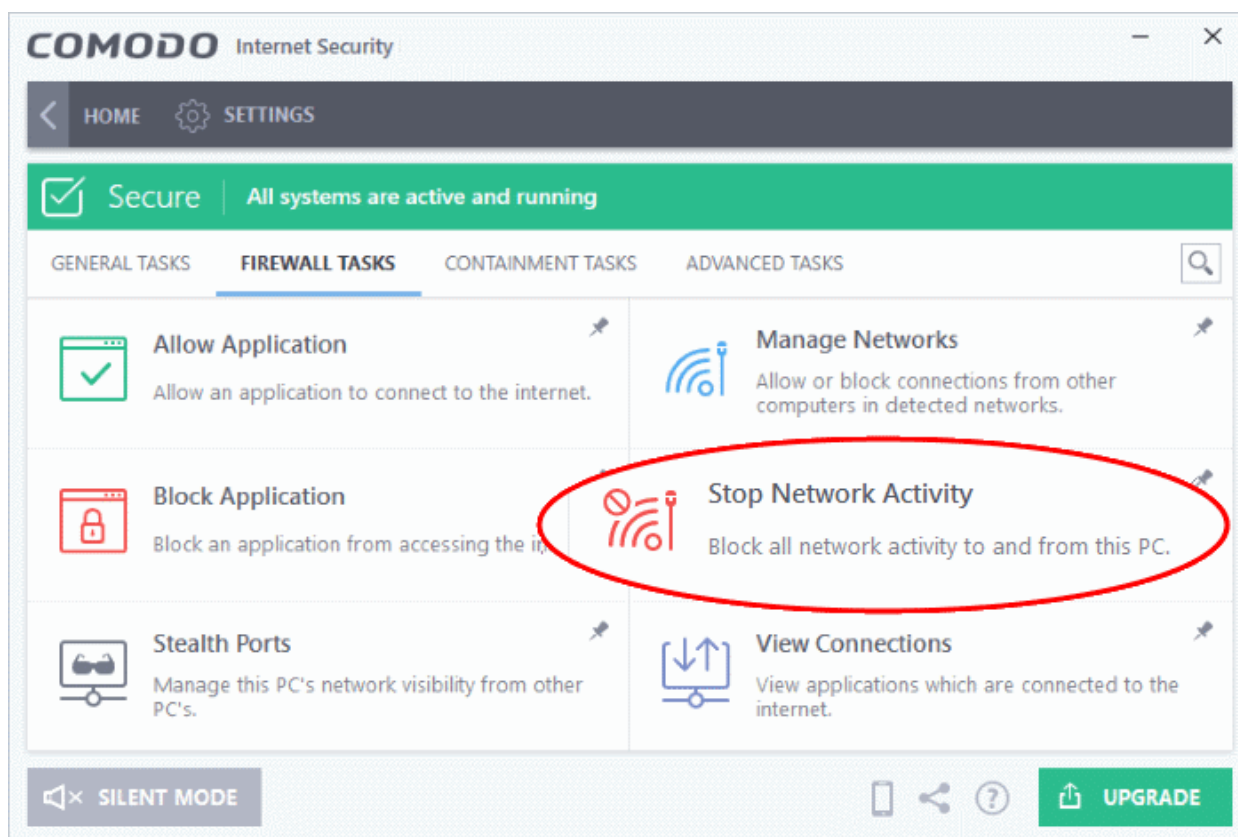
Manage network activities from your computer:

- Click 'Tasks' > 'Firewall Tasks'

- Click 'Stop Network Activity' to disconnect your computer from all networks

- Click 'Restore Network Activity' to re-enable connectivity

- 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

Click 'Tasks' > 'Firewall Tasks' > 'Stealth Ports'

- Port stealthing is a security feature which hides your ports to the outside world, providing no response to port scanners.

What is a port?
Your computer sends and receives data 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 email 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 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 against your machine.

- Stealthing a port effectively makes your computer invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt. A closed port responds with a 'closed' reply, which reveals that there is a PC in existence.

- If a hacker or automated scanner cannot 'see' your computer then they will move on to other targets. You can still connect to the internet and transfer information as usual, but remain invisible to outside threats.

Stealth ports on your computer

- Click 'Tasks' > 'Firewall Tasks'

- Click 'Stealth Ports'
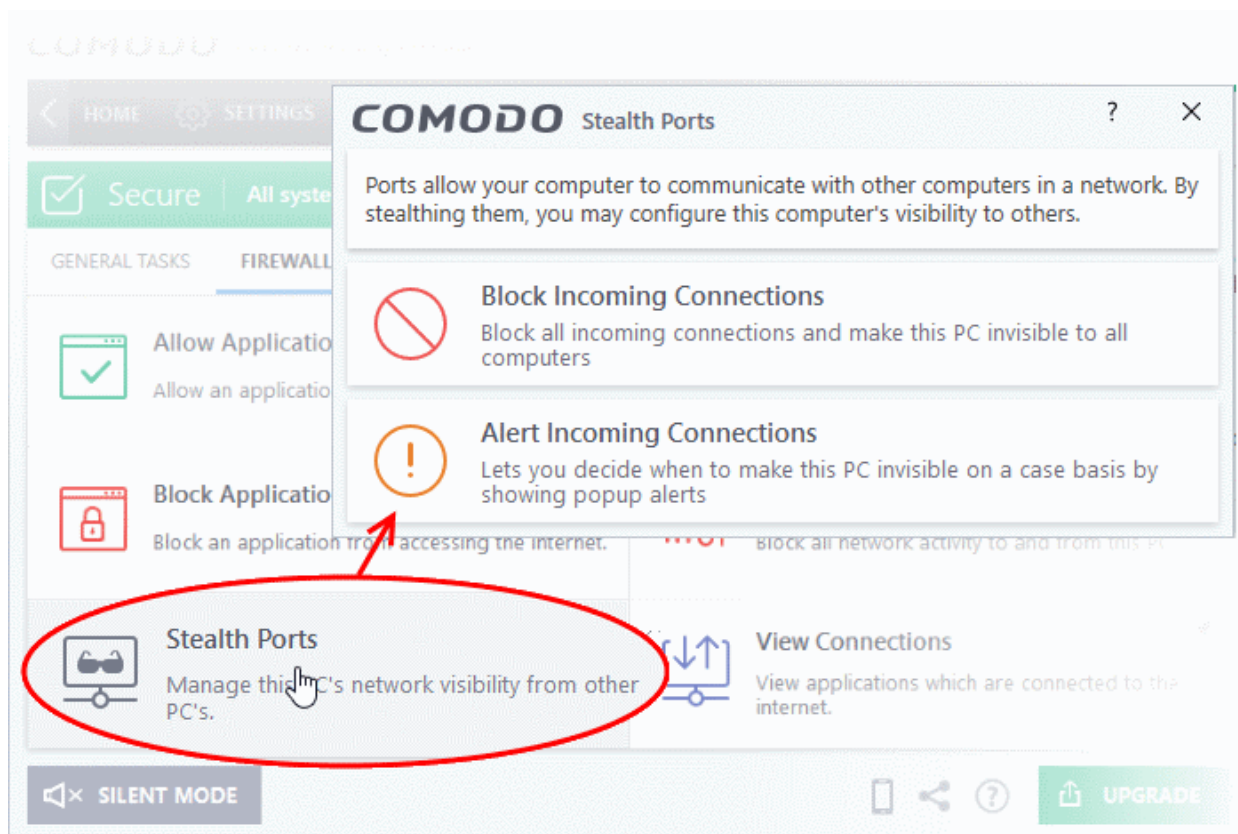
- **Block incoming connections** - Your computer's ports are invisible to all networks, regardless of whether you trust them or not. The average home user (using a single computer that is not part of a home LAN) will find this option the most convenient and secure. You are not alerted when the incoming 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

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

- **Alert incoming connections** - You will see a **firewall alert** every time there is a request for an incoming connection. The alert asks your permission on whether or not you want the connection to proceed. This can be useful for peer-to-peer and remote desktop applications which need to access your ports in order to connect. 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>

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

3.5. View Active Internet Connections

Click 'Tasks' > 'Firewall Tasks' > 'View Connections'

- View connections shows which applications and services currently have an active internet connection.
- You can view 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 opens or drops a 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.

View active internet connections on your computer

- Click 'Tasks' > 'Firewall Tasks'
- Click 'View Connections'

Tip: You can also get to this screen by clicking the number below 'Inbound' or 'Outbound' in the home screen (advanced view).
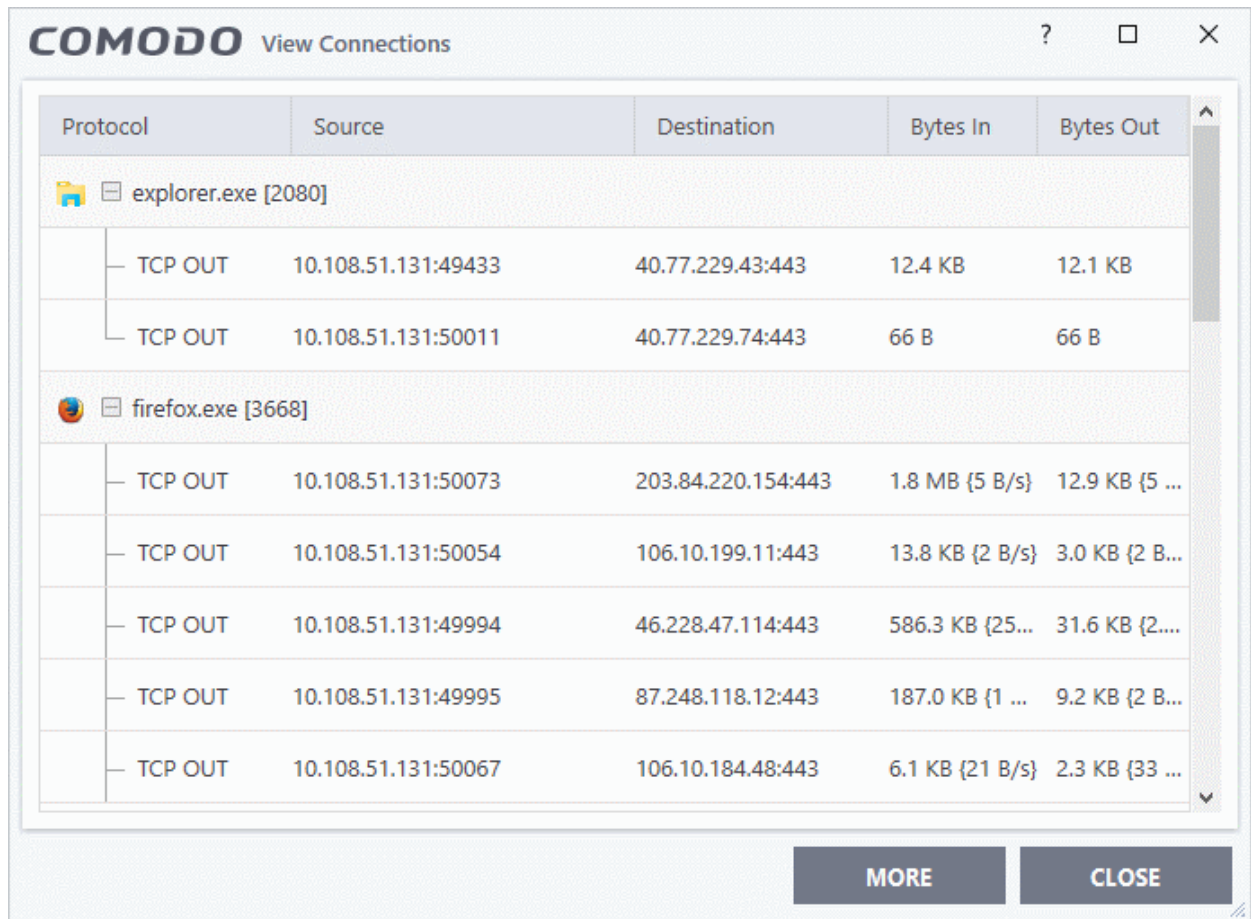
- **Protocol** - The application that is making the connection, the protocol it is using, and the direction of the traffic. Each application may have more than one connection at any time. Click + to expand the list of connections.
- **Source (IP : Port)** - The IP address and port number of the origin of the traffic. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** - The IP address and port number of the target. This is blank if the 'Source' column is 'Listening'.
- **Bytes In** - The total bytes of incoming data since the session started.
- **Bytes Out** - The total bytes of outgoing data since the session started.

Context Sensitive Menu

- Right-click on an item to open the context sensitive menu:
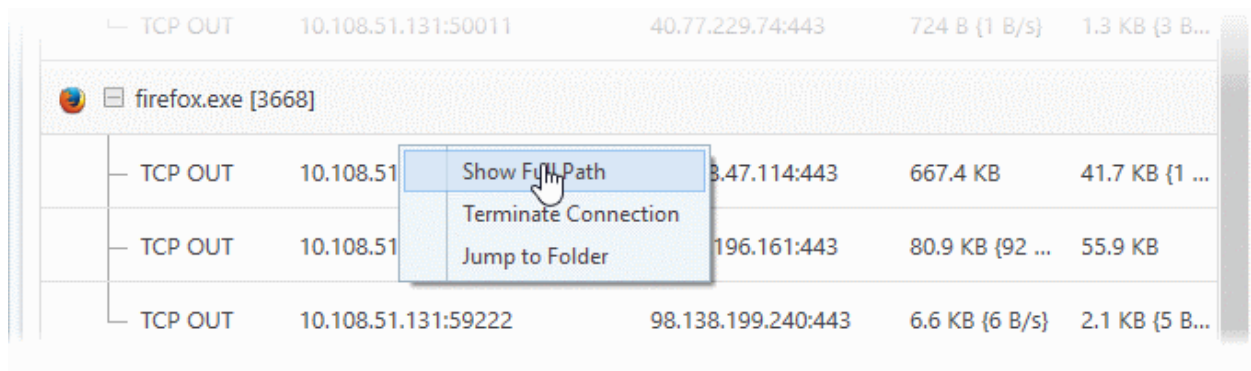
- 'Show Full Path' - View the location of the application
- 'Terminate Connection' - Close the application's connection

---

- 'Jump to Folder' - Open the folder containing the application executable

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.

- Click the 'More' button in the 'View Connections' to directly access Comodo KillSwitch
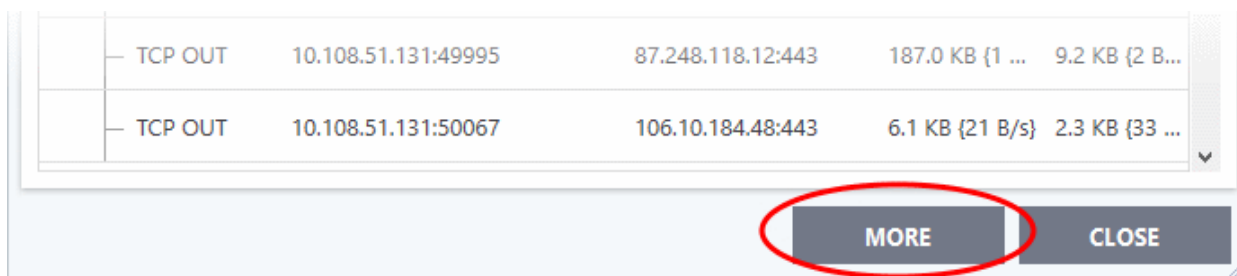
If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.
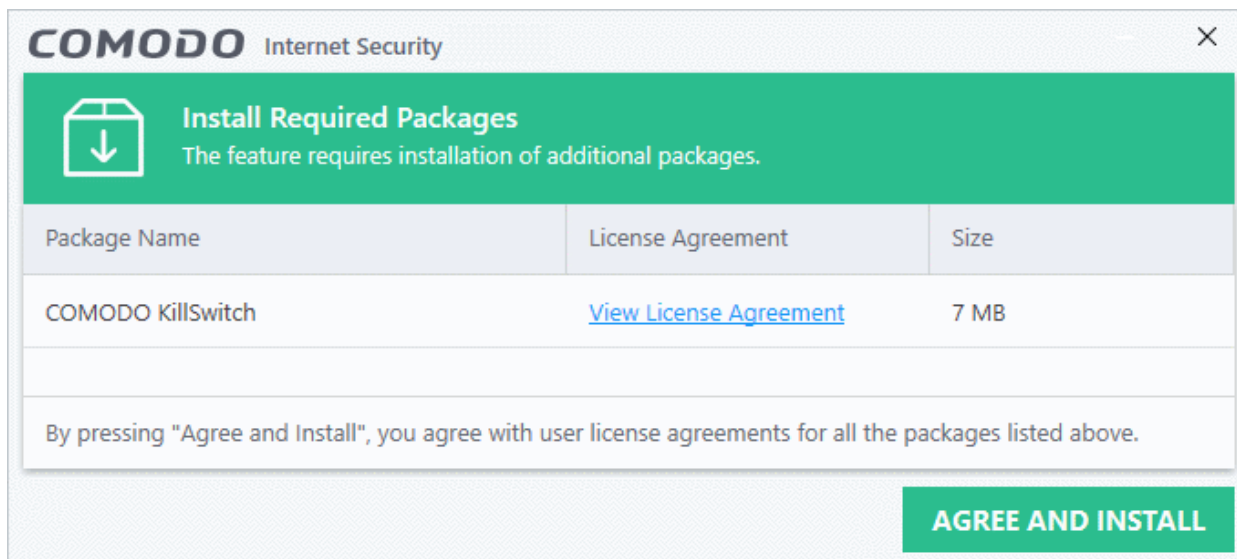
- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.
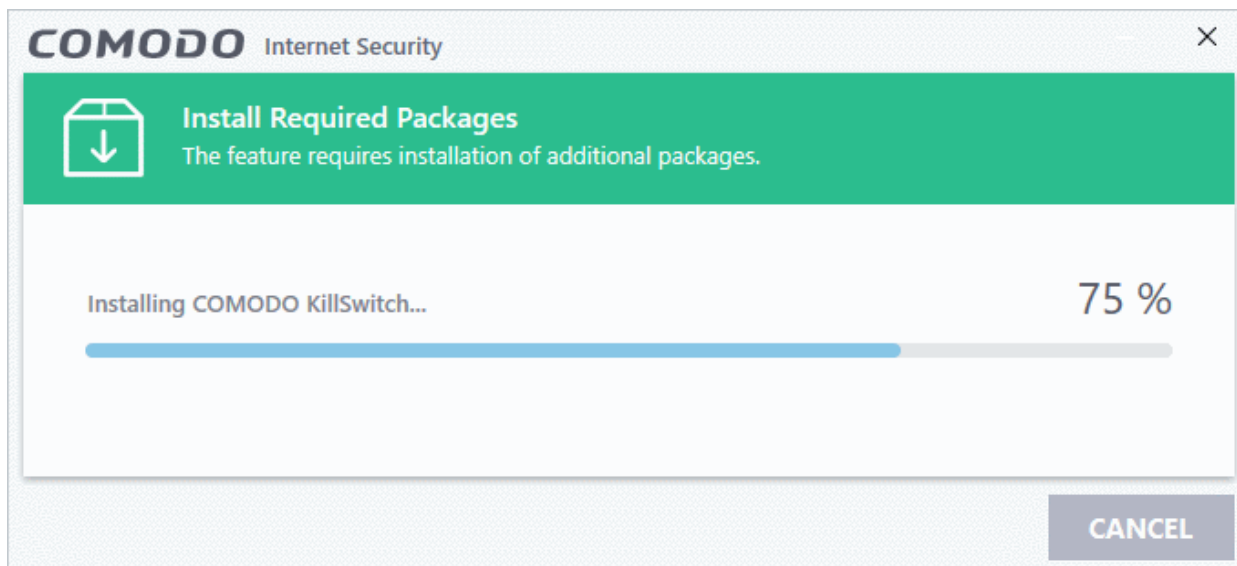
- On completion the Comodo KillSwitch main interface opens.
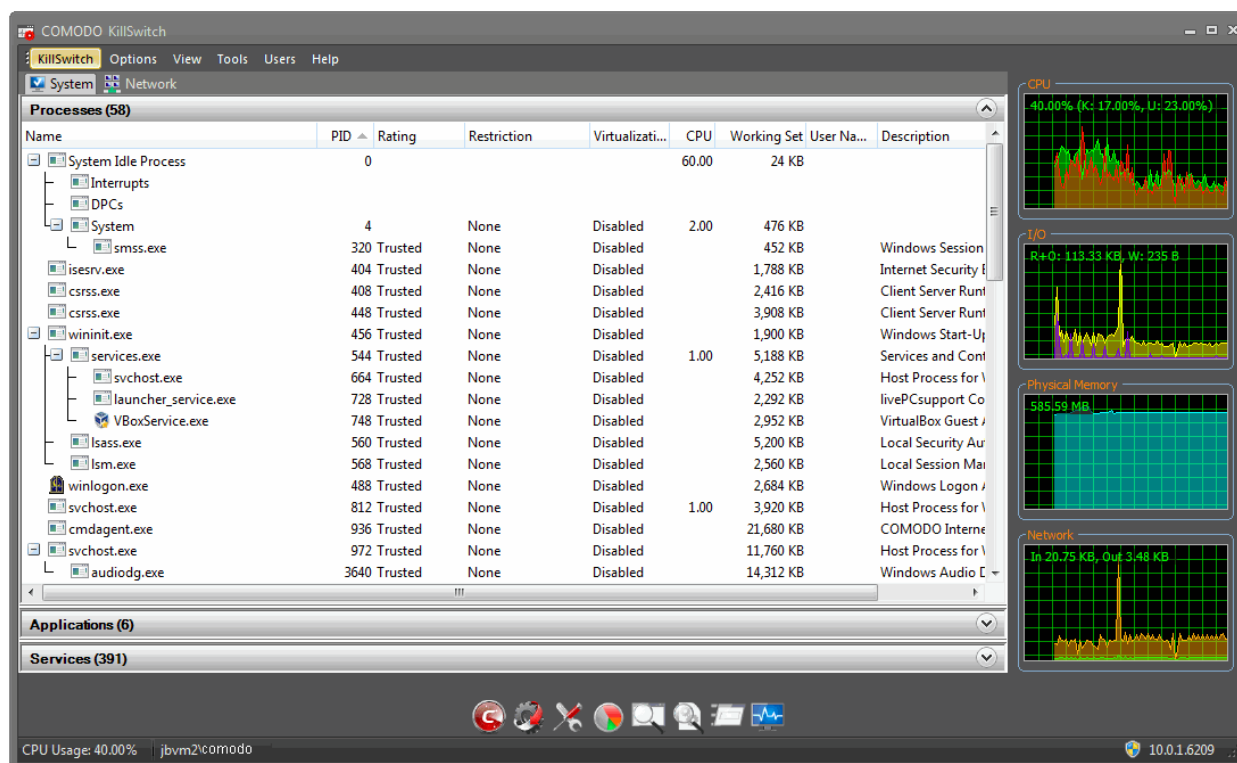
- Details of how to use KillSwitch to view granular details on current network connections and terminate unsafe connections can be found at **http://help.comodo.com/topic-119-1-328-3577-Viewing-and-Handling-Network-Connections-and-Usage.html**.

- 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

Click 'Tasks' > 'Containment Tasks'

- The container is a secure, virtual environment in which you can run unknown, untrusted, and suspicious applications.

- Applications in the container are isolated from the rest of your computer. They are denied access to other processes, write to a virtual file system and registry, and cannot access your personal data.

- This makes it an ideal environment for surfing the internet, because nothing you download can spread to your host system.

- You can run applications in the container on an ad-hoc basis, and you can also create desktop shortcuts to always launch a program in the container.
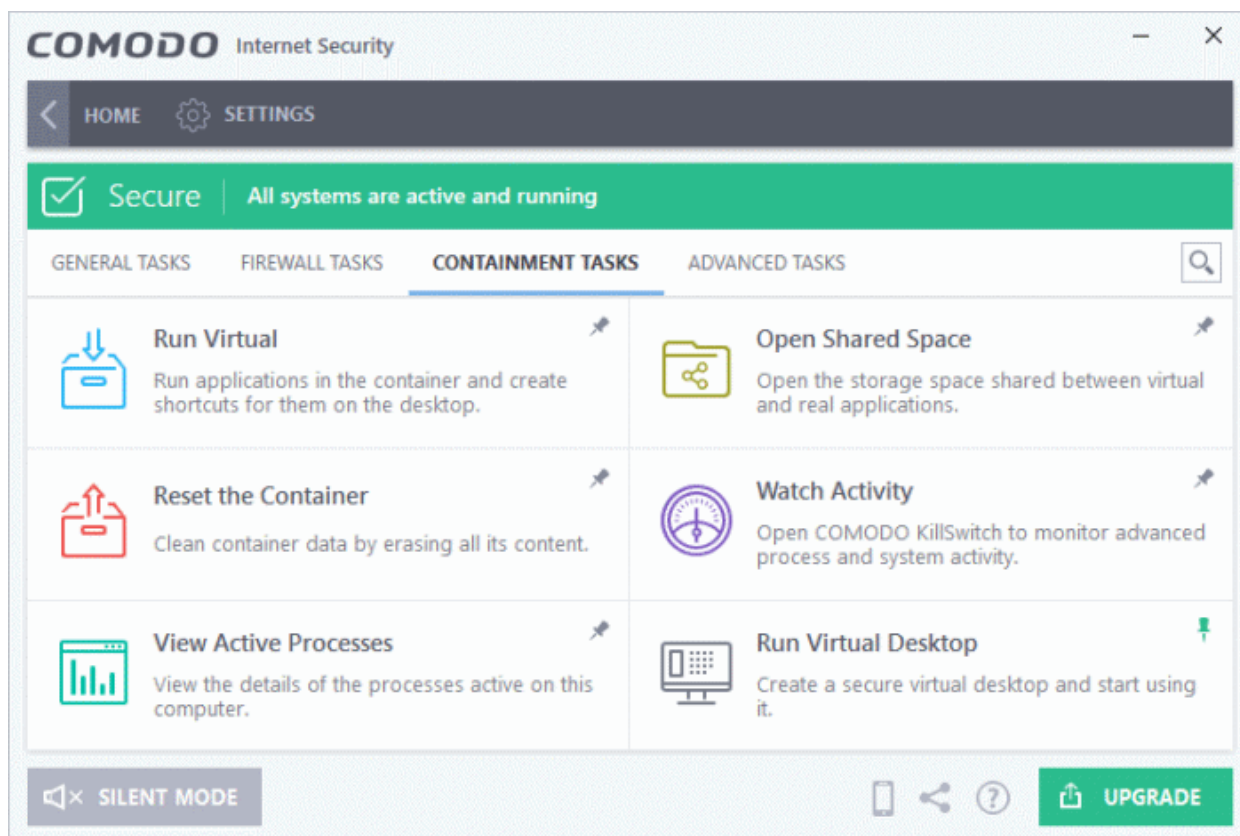
Note - containment is not supported on Windows XP or Windows Server 2003

Containment tasks has the following areas:

- **Run Virtual** - Run individual applications in the container.

- **Open Shared Space** - Shared space is a folder which you can access from both your real desktop and the virtual desktop. When in the virtual desktop, save your files in shared space if you want to open them on your host computer.

- Background. Applications in the container write to a virtual file system and not your local drive. This prevents them from making potentially malicious changes to your files and folders.

  The one exception to this is a folder called 'Shared Space'. This folder can be accessed by both your host operating system and contained programs. Use the folder to share files between your computer and the container.

  The folder is located at 'C:\Documents and Settings\All Users\Application Data\Shared Space'.

- **Reset Container** - Clears all data written by programs inside the container.

- **Watch Activity** - Open Comodo KillSwitch to identify unsafe processes and manage system activity.
- **View Active Process List** - Manage processes which are currently running on your PC. Click the 'More' button to open Comodo **KillSwitch**
- **Run Virtual Desktop** - Start the virtual desktop environment.

4.1. Run an Application in the Container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'
- Choose the program you want to run
- Click 'Open'

This method above 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.

You can also create desktop shortcuts to always launch an application in the container:
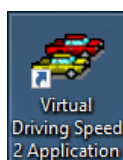
Run an application in the Container
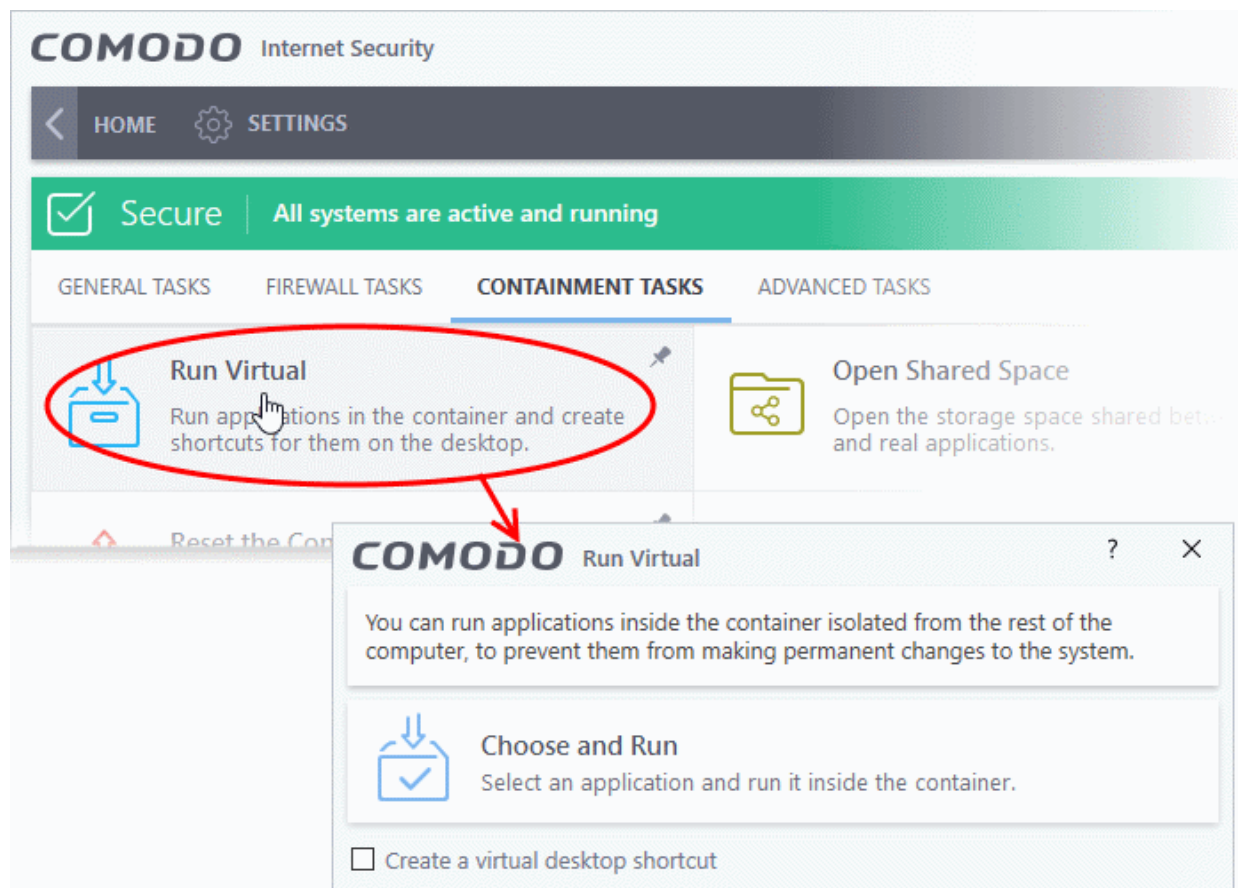
- Click 'Tasks'> 'Containment Tasks'
- Click 'Run Virtual':

- Click 'Choose and Run', browse to your application then click 'Open'.
- The contained application will have a green border around it. Enable 'Create a virtual desktop shortcut' if you plan to run the application in the container in future.
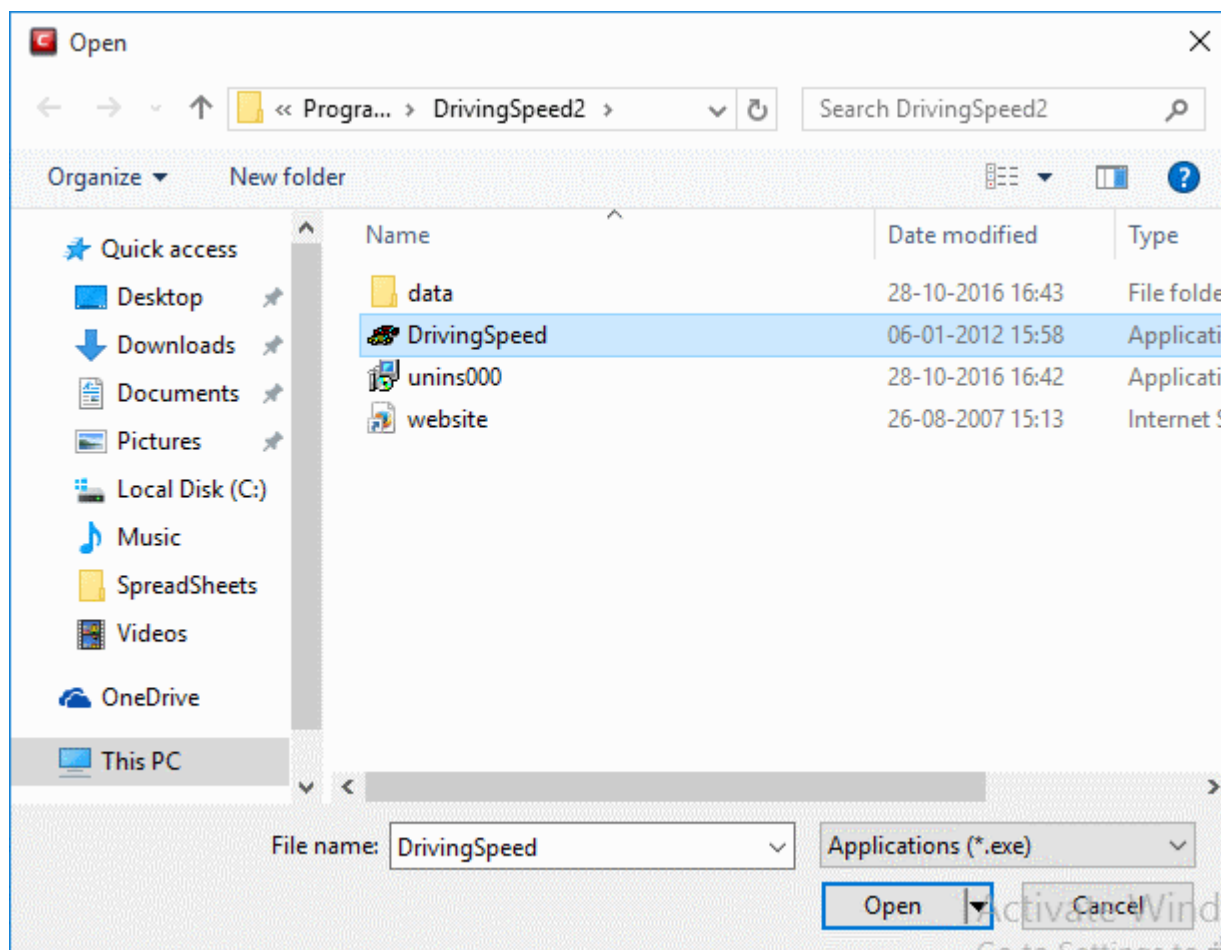
You can also run an applications in the container from the right-click menu:
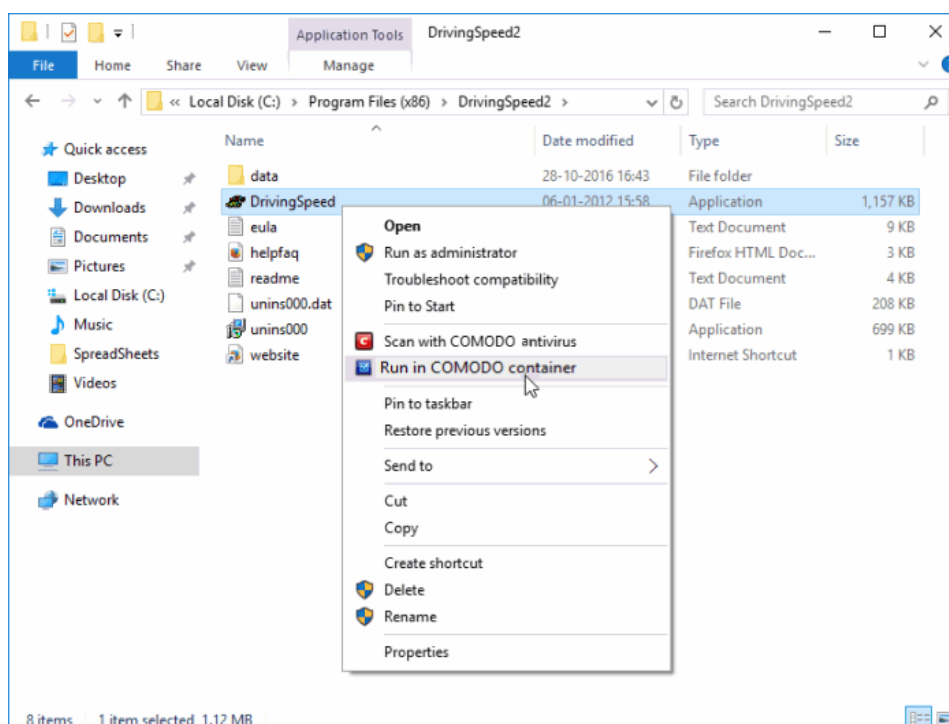
Run Browsers in the container

The CIS widget contains shortcuts to run your browsers in the container::
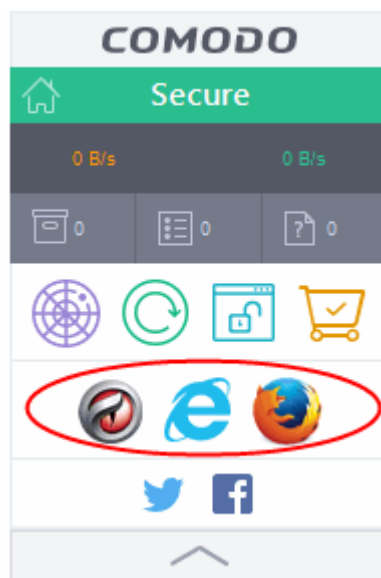
- The green border indicates that the browser is in the container:
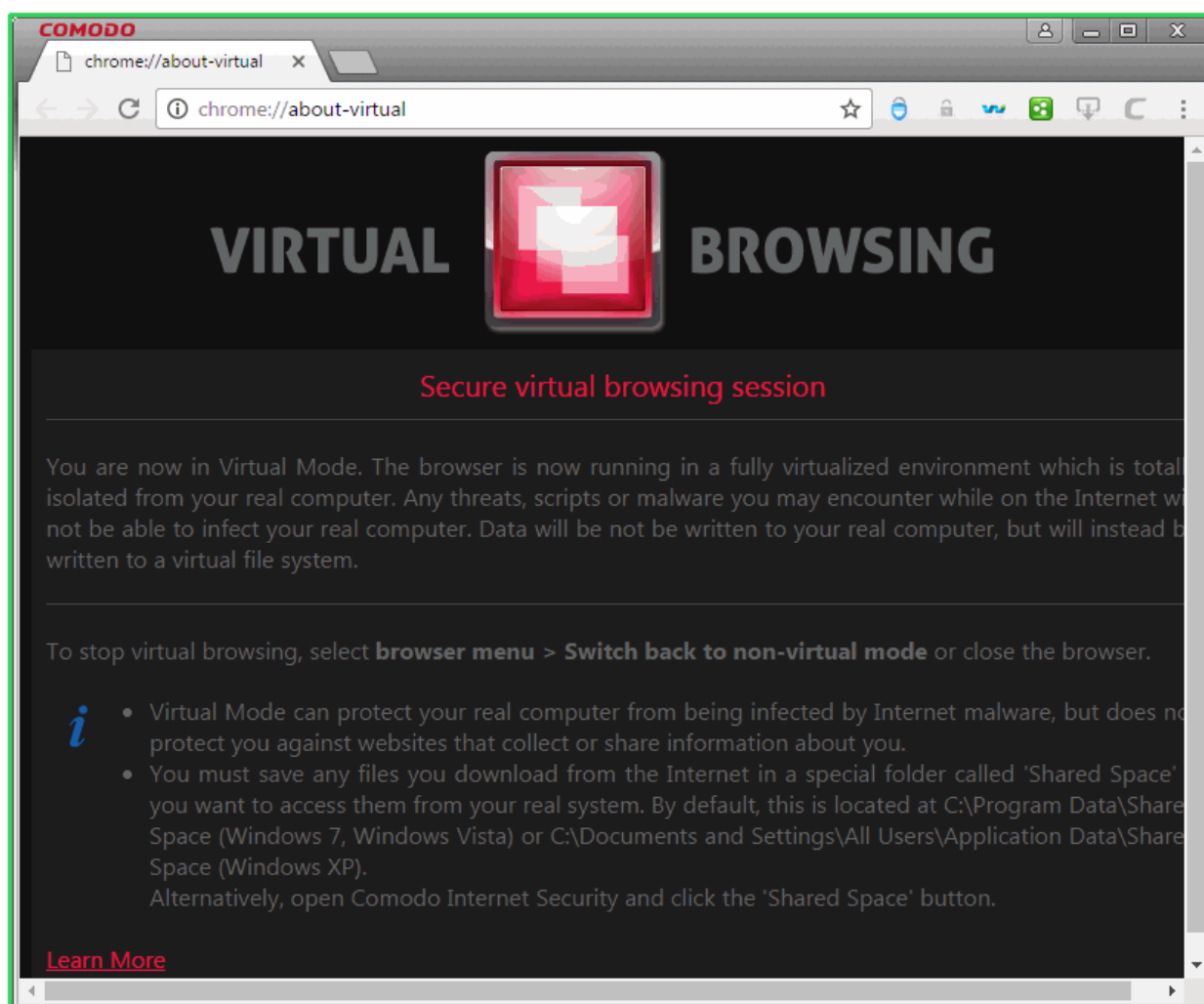
Tip: Running a browser in the container deletes all traces of your activities. This includes your browsing history, cookies, and offline data stored by the websites you visit. Virtualization protects your computer from anything malicious that is downloaded. See **The Virtual Desktop** for more details.

However, for visiting important shopping or banking websites, we recommend you use the Secure Shopping feature.

<table>
<tr><td>

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

The two systems are intended for opposite use cases. The virtual desktop protects your computer from potentially hostile programs running in the container. Secure shopping protects the program in the container from anything hostile on your computer. For example, it prevents any outside processes from interfering with your secure banking sessions.
Secure shopping also has multiple other security technologies to make sure you are totally protected online.

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

</td></tr>
</table>

<table>
<tr><td>

Note. You may see an error if an app on the host tries to update itself at the same time as that app is updating itself in the container. This is a classic Windows sharing violation which is shown when an app attempts to write to a file that is already in use. Please shut down the contained version of the app then run the update on the locally hosted version. The contained version will function correctly once the update to the local version is complete.

</td></tr>
</table>

4.2. Reset the Container

Click 'Tasks' > 'Containment Tasks' > 'Reset the Container'

- Programs in the container write all data and system changes to a virtual file system. This means the program cannot harm your computer or sensitive data.

- Files saved in the container could 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 the Container' option lets you delete all items saved in the container.

Clear the container

- Click 'Tasks' > 'Containment Tasks'

- Click 'Reset the Container':
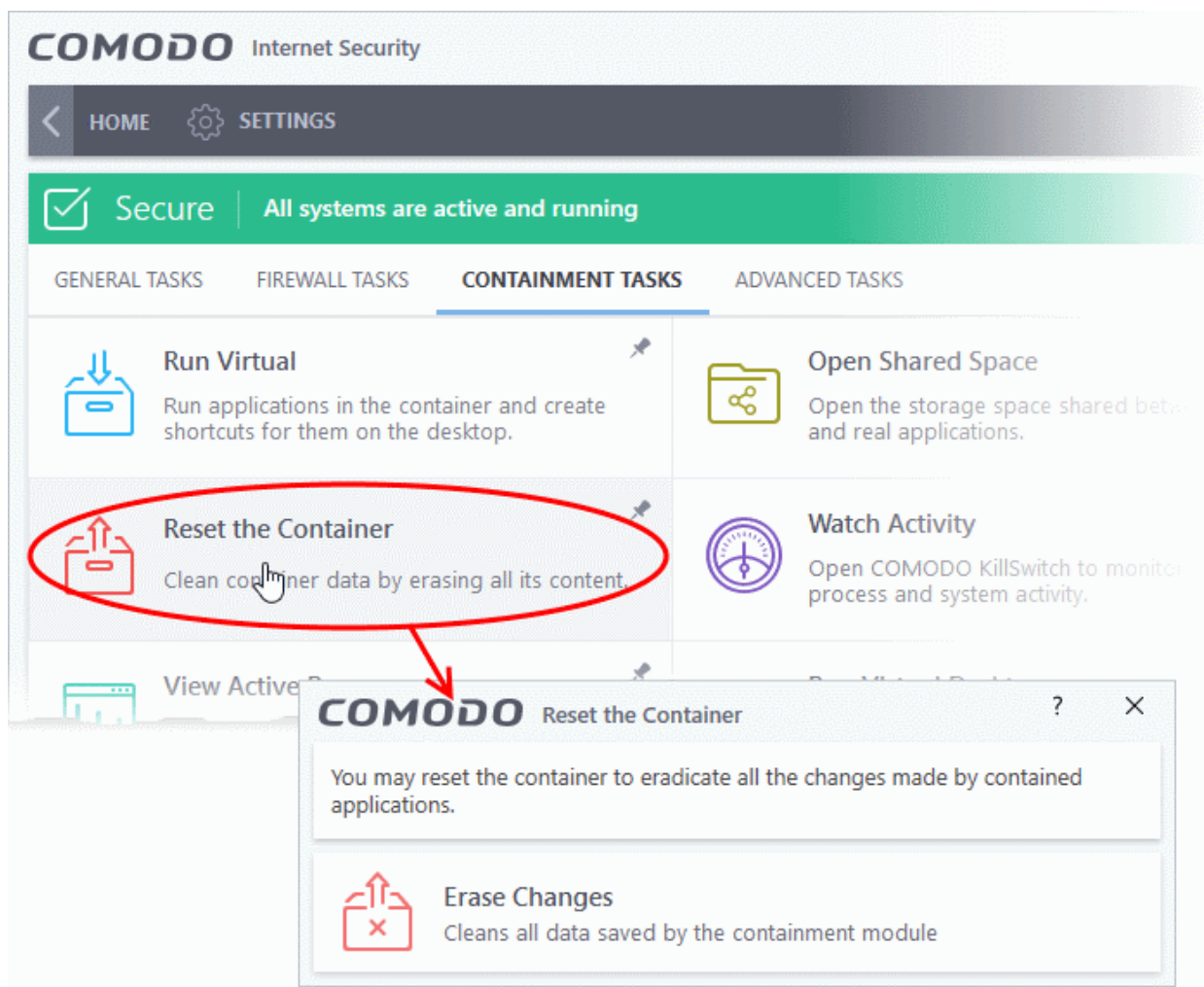
- Click 'Erase Changes'.

The contents in the container will be deleted immediately.
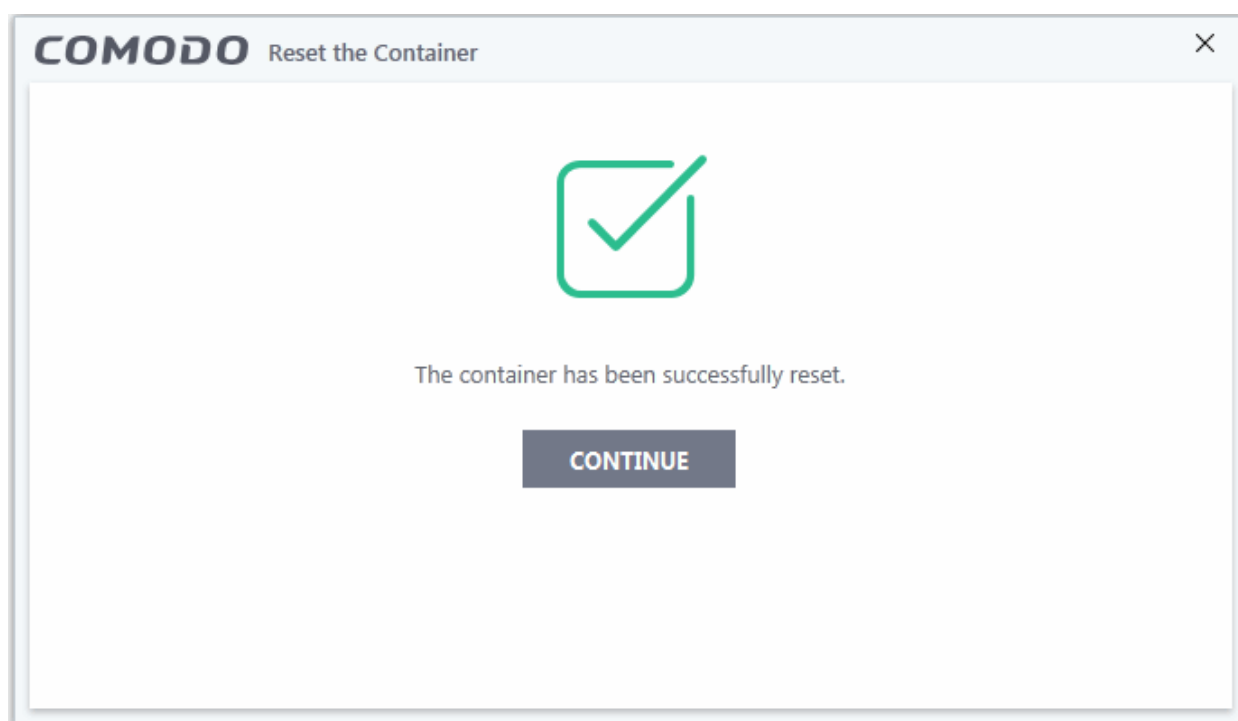
4.3. Identify and Kill Unsafe Running Processes

- Click 'Tasks' > 'Containment Tasks' > 'Watch Activity'

KillSwitch is an advanced system monitor that lets you identify and terminate any unsafe processes on your computer. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides another powerful layer of protection for Windows computers.

KillSwitch can even show processes that were invisible or very deeply hidden. You can identify all unsafe processes with a single click then quickly shut them down. You can also trace back to the software that generated the process.

Open KillSwitch

- Click 'Tasks' > 'Containment Tasks'
- Click the 'Watch Activity' tile
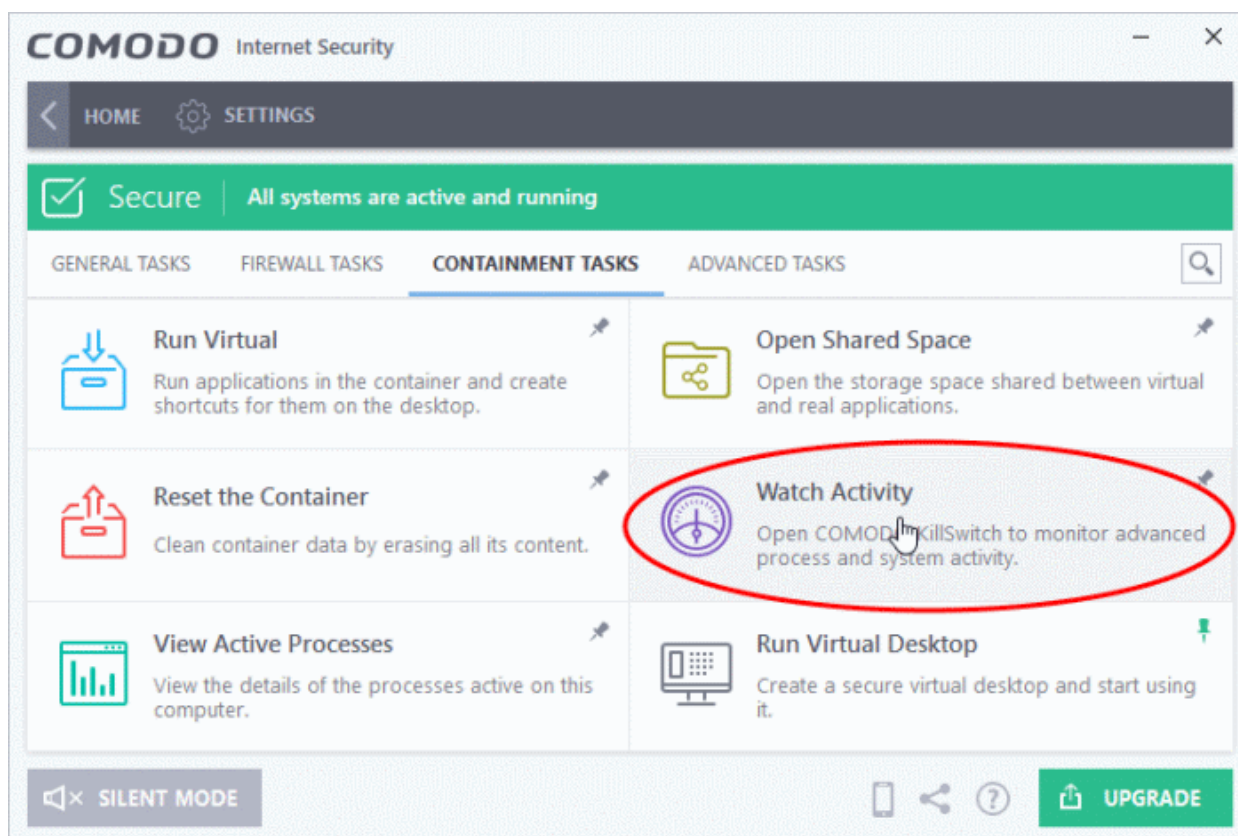
- Killswitch is a component of Comodo Cleaning Essentials. If you have already installed Comodo Cleaning Essentials by clicking 'Clean Endpoint' from the 'Advanced' task interface, clicking the 'Watch Activity' will open the KillSwitch interface directly. See **Remove Deeply Hidden Malware** for more details on installing Cleaning Essentials.

- If Comodo KillSwitch is already installed in your computer, clicking 'Watch Activity' will open the application. If not, CIS will download and install KillSwitch.
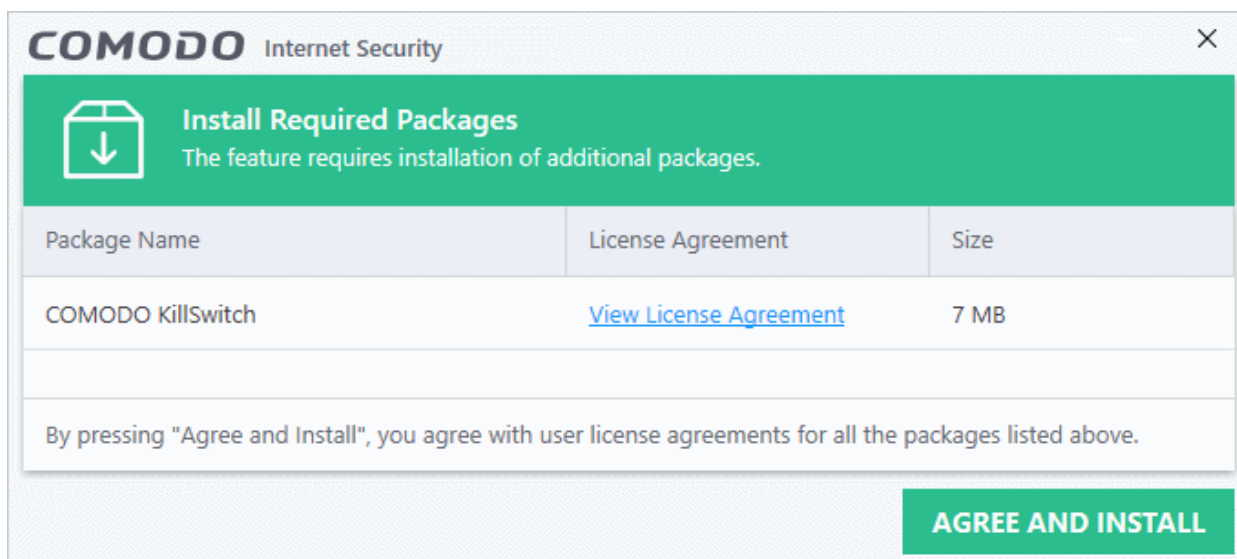
- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.
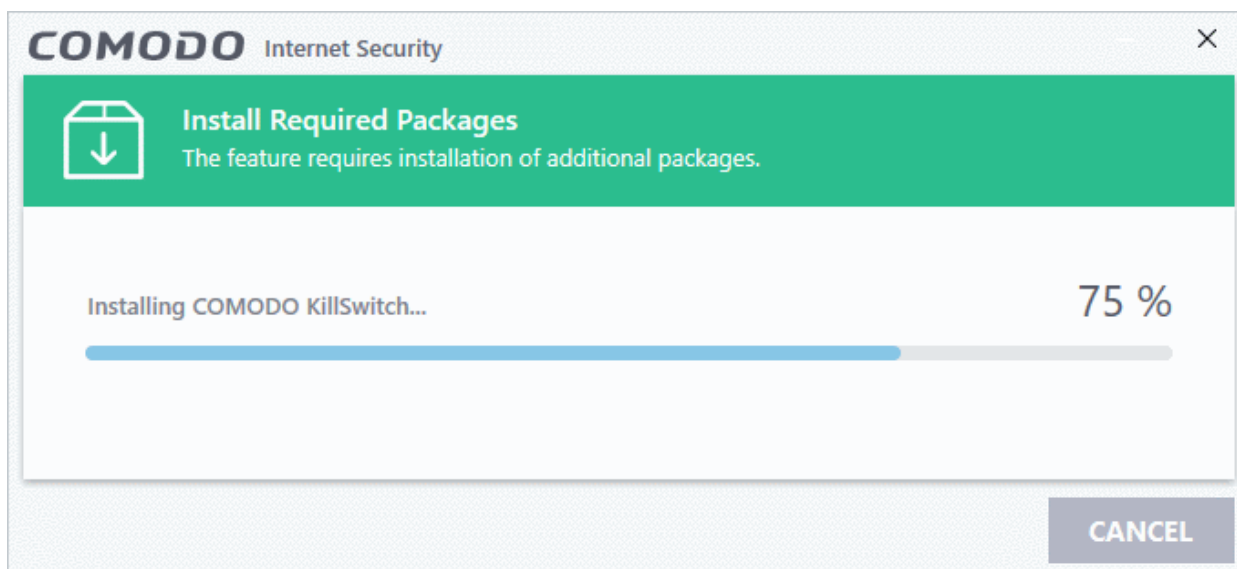
- KillSwitch will open when the installation is over:
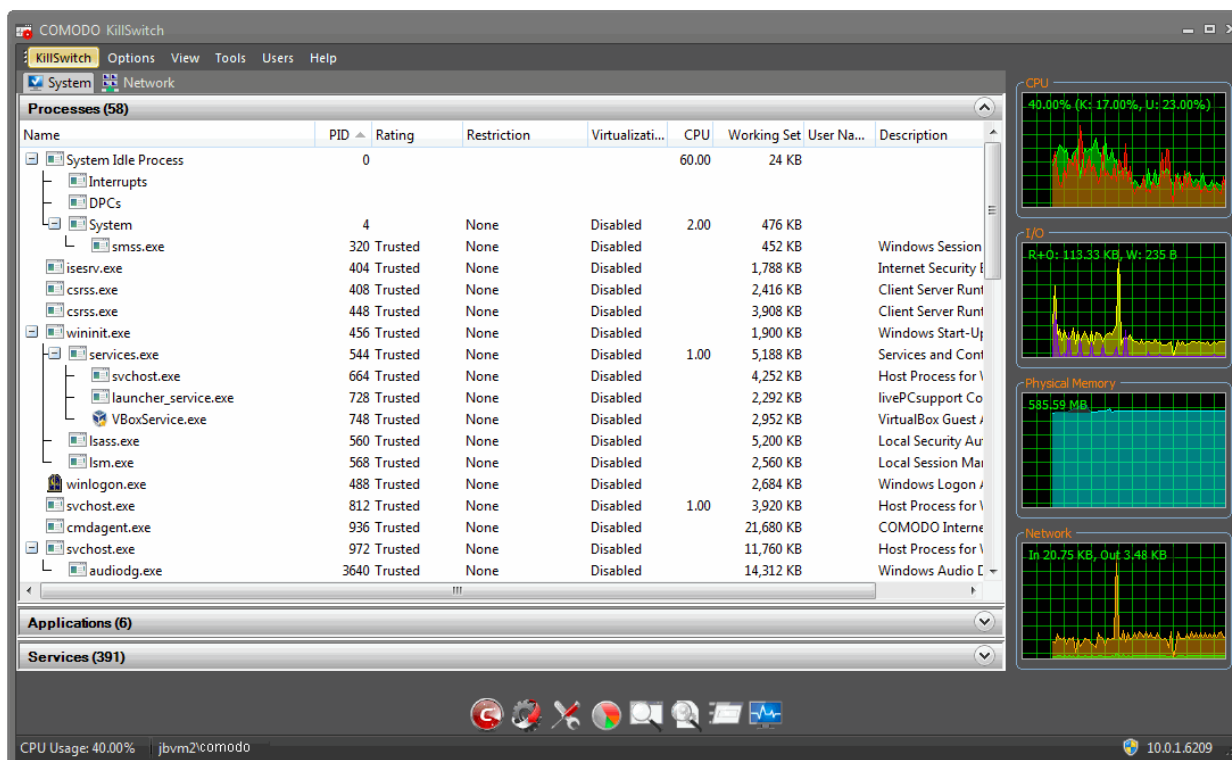
- See the KillSwitch guide for help to use the product - **http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html**

4.4. View Active Process List

Click 'Tasks' > 'Containment Tasks' > 'View Active Processes'.

- The active process list shows all processes started by applications currently running on your system.
- CIS can identify the parent application of a process to detect when a non-trusted application is trying to spawn a trusted application. CIS can then deny access rights to the 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. Here, you can check its trust rating on the latest cloud databases. You can also submit an application to Comodo for analysis.

View the active process list

- Click 'Tasks' > 'Containment Tasks'
- Click the 'View Active Processes' tile:

- • **Application** - The name of the parent executable of the process.
- • **PID** - The unique process identifier.
- • **Company** - The vendor who created the software
- • **User Name** - The user account under which the program is run

- **Restriction** - The security limitations placed on the program by the CIS containment module.
- **Rating** - The trust level of the program as per the local file list ('Settings' > 'File Rating' > File List')
- Right-click on any process to open the context sensitive menu:
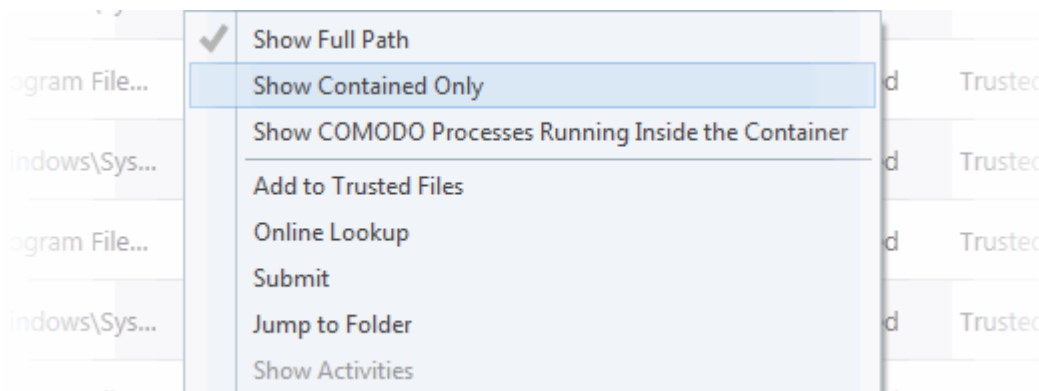
- **Show Full Path** - View the install location of the parent program
- **Show Contained Only** - Hides all processes except those running in the container.
- **Show COMODO Processes Running Inside the Container** - Hide all processes except Comodo processes running in the container.
- **Add to Trusted Files** - Assign 'Trusted' status to the executable that started the process. This allows the file to run as normal in future. You can view trusted files in the CIS '**File List**' ('Settings' > 'File Rating' > 'File List').
- **Online Lookup** - Search for the executable in Comodo's global blacklist and whitelist. The results will tell you if the file is clean, malicious or unknown.
- **Submit** - Uploads the parent executable to Comodo for analysis.
- **Jump to Folder** - Opens the folder containing the executable.
- **Show Activities** - Shows all actions by processes of the application. This option is only available if **VirusScope is enabled** ('Settings' > 'Advanced Protection' > 'VirusScope').
- Click the 'More' button to open Comodo KillSwitch - an advanced system monitor that lets you quickly identify and terminate any unsafe processes on your system.
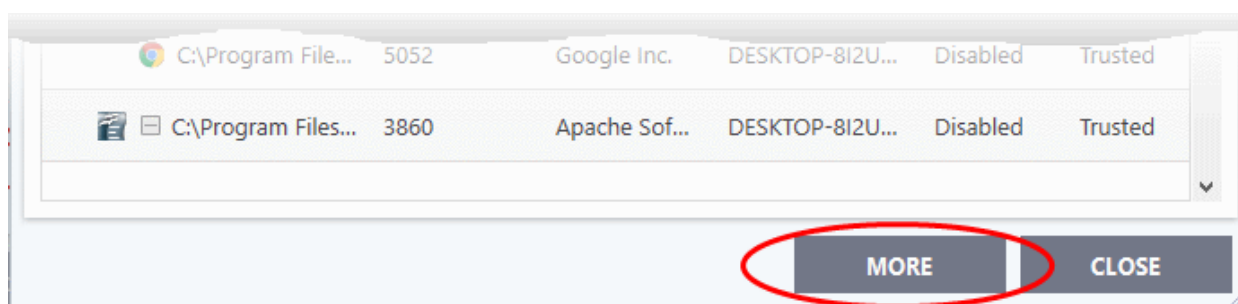
If KillSwitch is not yet installed, clicking this button will prompt you to download the application. See **Identify and Kill Unsafe Running Processes** for more details.

4.5. The Virtual Desktop

Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'

- The virtual desktop is a sandbox environment in which you can run programs and browse the internet without fear those activities will damage your computer.
- Applications 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 normally run in 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.

- Use the 'Shared Space' folder to save any files you want to access from Windows. This folder is the only place that the virtual desktop can write to on the host file system.

- The virtual desktop can be password-protected for added privacy.

- The virtual keyboard lets you securely enter confidential passwords without fear of key-logging software.

- 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.

- Parents may want to consider the virtual desktop as a secure area for children to run programs and surf the web without damaging the host computer. The virtual desktop can be reset and all changes cleared at the end of every session.

Click the following links for more help:

- **Start the Virtual Desktop**
- **The Main Interface**
- **Run Browsers inside Virtual Desktop**

- Open Files and Run Applications inside Virtual Desktop
- Configure the Virtual Desktop
- Close the Virtual Desktop

4.5.1. Start the Virtual Desktop

The virtual desktop can be started in the following ways:

1. Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
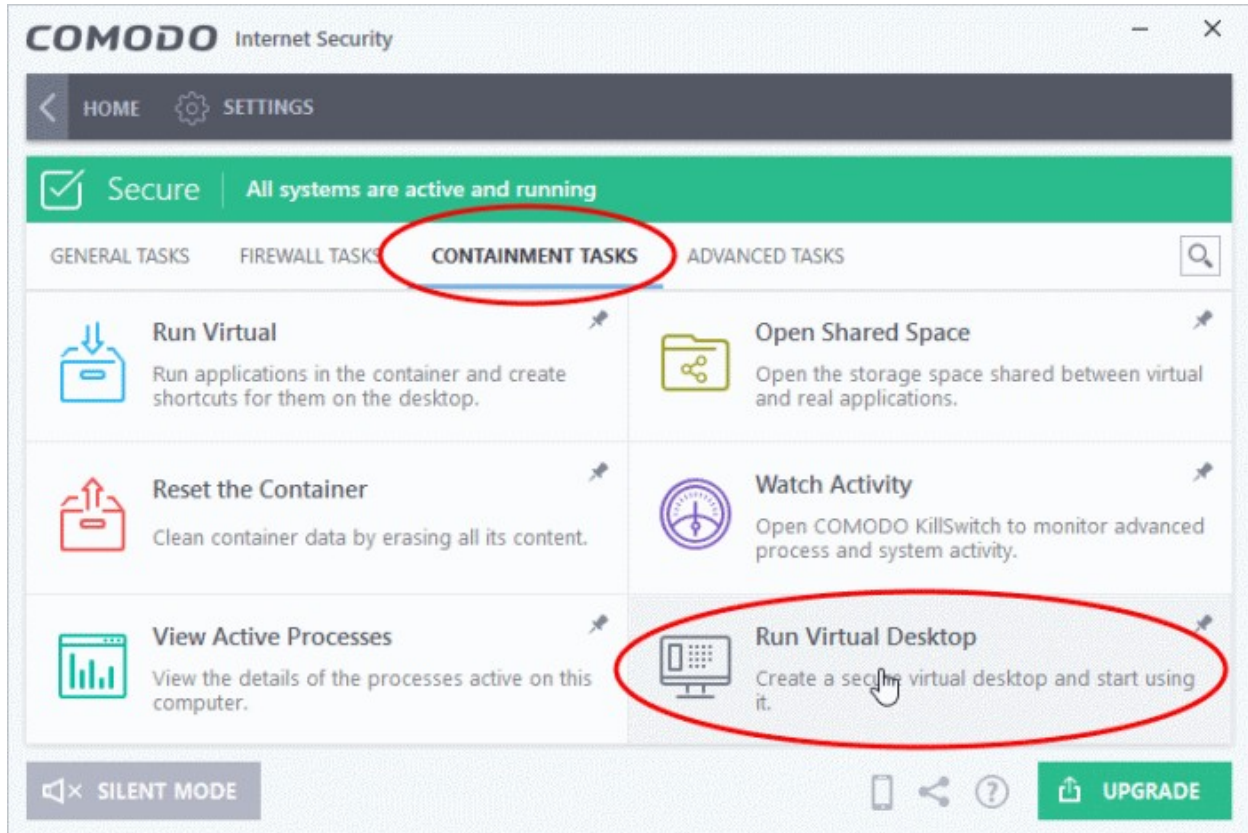
2. Click the 'Run Virtual Desktop' button in the basic view of CIS home screen:
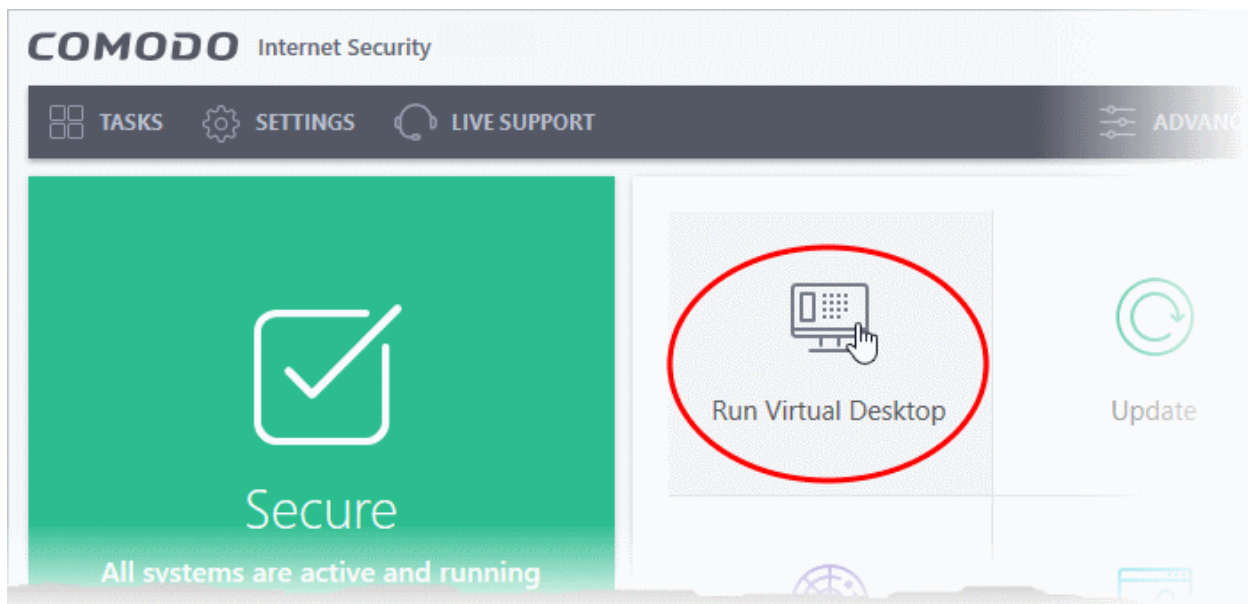
3. Click the 'Virtual Desktop' shortcut in the CIS widget:
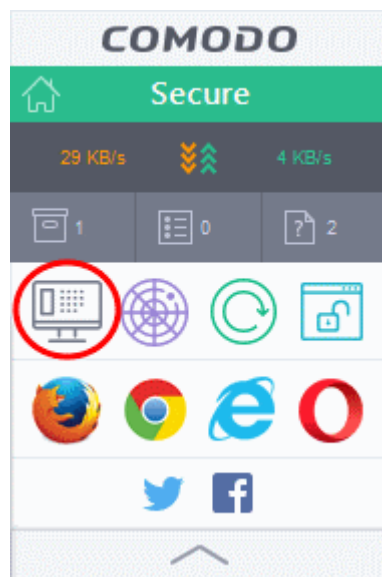
Note: The home screen and widget shortcuts are only available if you have added the 'Virtual Desktop' shortcut:

- Click 'Tasks' on the home screen
- Click 'Containment Tasks'
- Right-click on the virtual desktop tile
- Select 'Add to Task Bar'

See '**Add tasks to the home screen**' if you need more help with this.

The virtual desktop requires the following installed on your computer:

- Comodo Dragon Browser
- Microsoft Silverlight

CIS checks whether these components are installed whenever you run the virtual desktop. If they aren't, you will be prompted to install them.
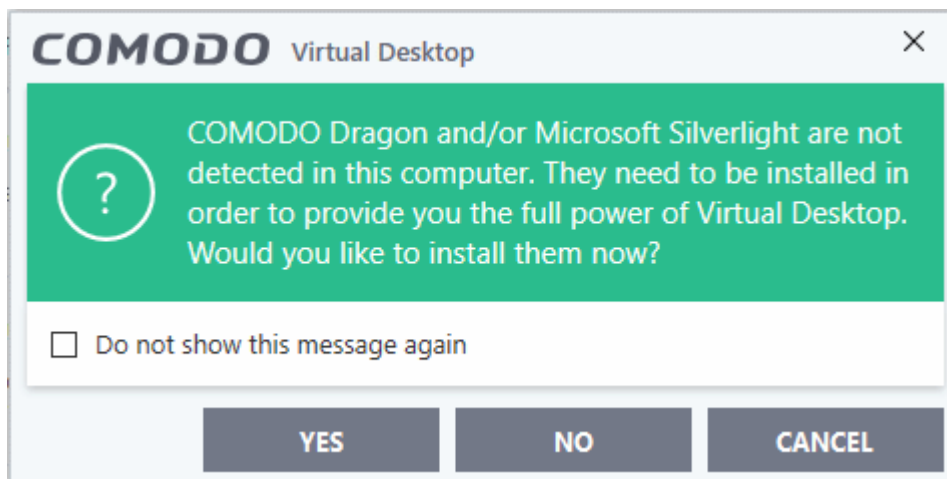
- If you want Comodo Dragon Browser and/or Microsoft Silverlight to be installed this time, click 'Yes'. If not, click 'Cancel'. You will be prompted to install them, next time when you start the Virtual Desktop.
- If you do not want the applications to be installed at all, click 'NO'.

- Click 'Yes' to download and install the software.
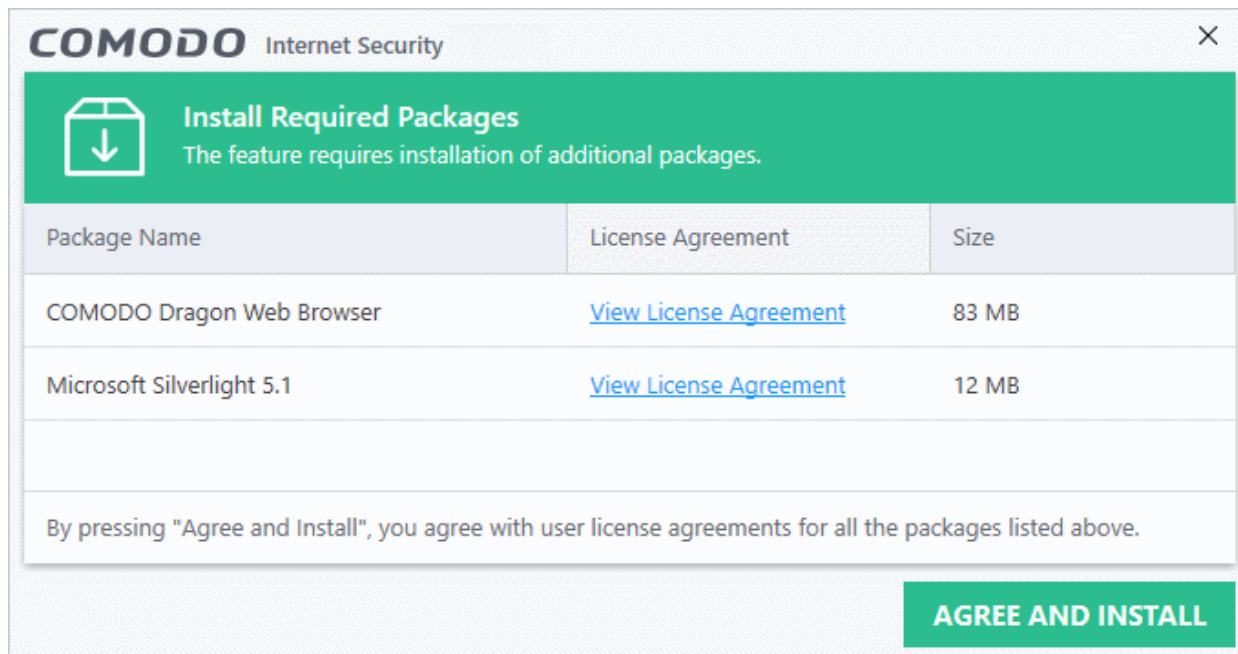
- Click 'View License Agreement' to read the license agreement of the additional software to be installed
- Click 'Agree and Install' to download and install the required software
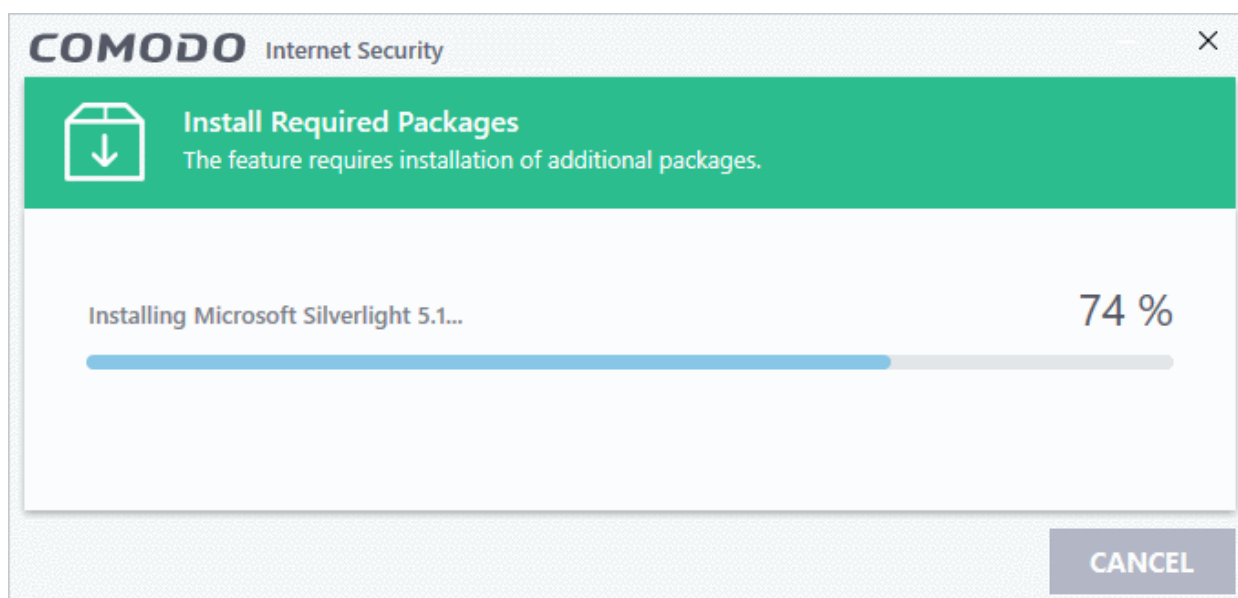
The software package(s) will be downloaded and installed automatically. The Virtual Desktop will open after completion of the installation.

4.5.2. The Main Interface

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'

The virtual desktop has 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 the **table below** for a comparison between the two.
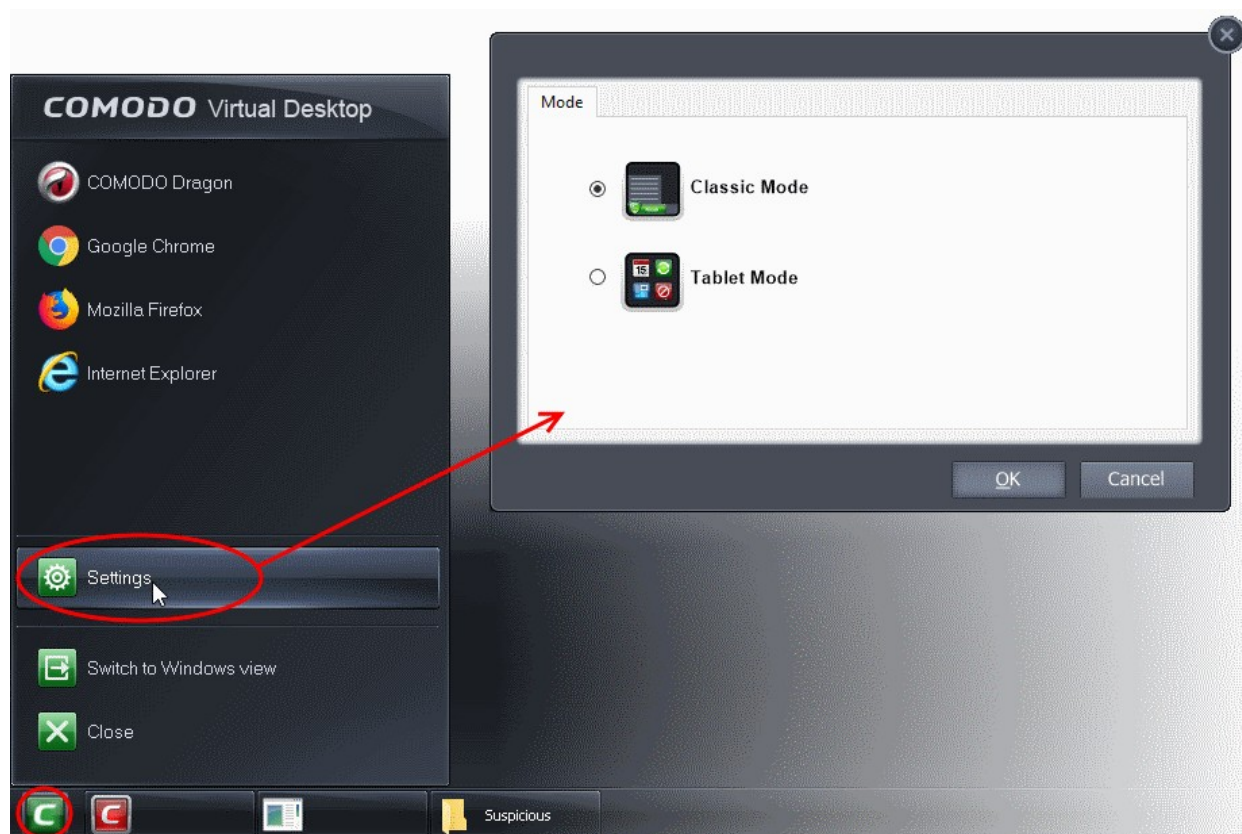
The 'Start' menu

- Click the green 'C' icon to open the start menu:

The menu has the following options:

- **Browsers** - Shows the browsers installed on your computer.
  - Click on a browser to open it inside the virtual desktop. See **Run Browsers inside the Virtual Desktop** for more details.
- **Settings** - Configure the virtual desktop. See **Configure the Virtual Desktop** for more details.
- **Switch to Windows view** - Access your local computer without closing the virtual desktop.

Tools and Taskbar

- Keyboard layout - Click the language button [ENG] at bottom-right and select the keyboard layout you want to use .
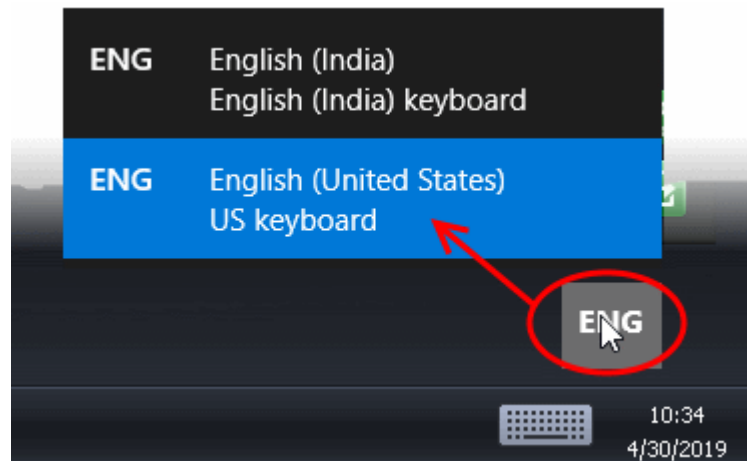
- **Virtual keyboard** - Click the keyboard icon on the system tray to open a virtual keyboard.
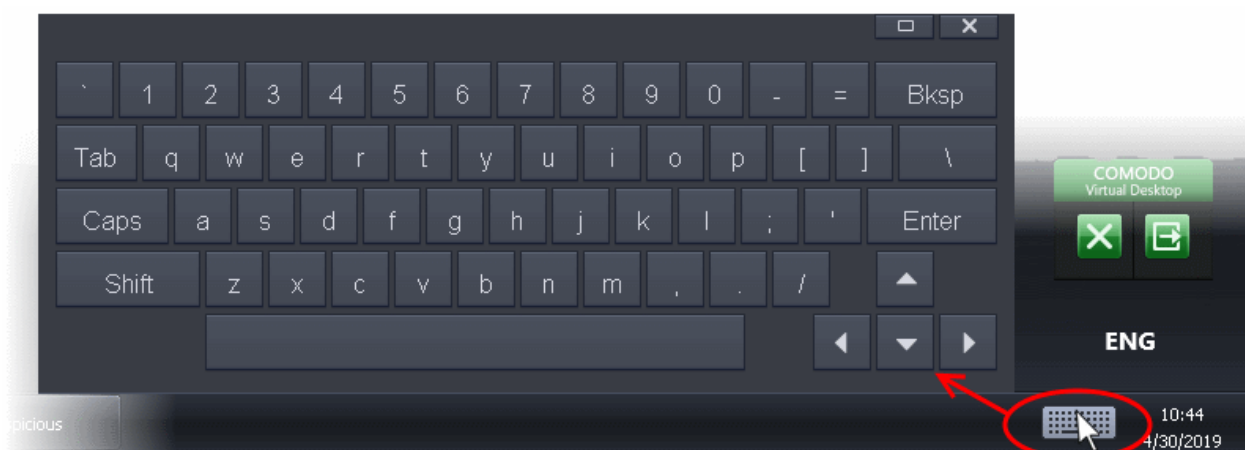
- You can use this to enter confidential data online (usernames, passwords and credit card numbers etc).
- The keyboard can also be used with touch screen displays.
- **Windows Task Manager** - Right-click on the task bar and select 'Watch Activity' to open the 'Windows Task Manager'.

- You can view your computer's performance, close unresponsive programs and to troubleshoot problems with Windows.
- **Close the Virtual Desktop** - The shortcuts a bottom right let you temporarily switch to your real computer system, or fully exit the virtual desktop.
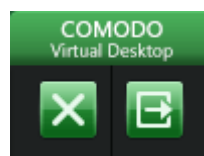
Classic Mode

- Click the green 'C' icon > 'Settings'

- Choose 'Classic Mode' and click 'OK'

- All items on your real desktop are displayed.

- Click the shortcuts to run the program or file inside the virtual computer system.

-
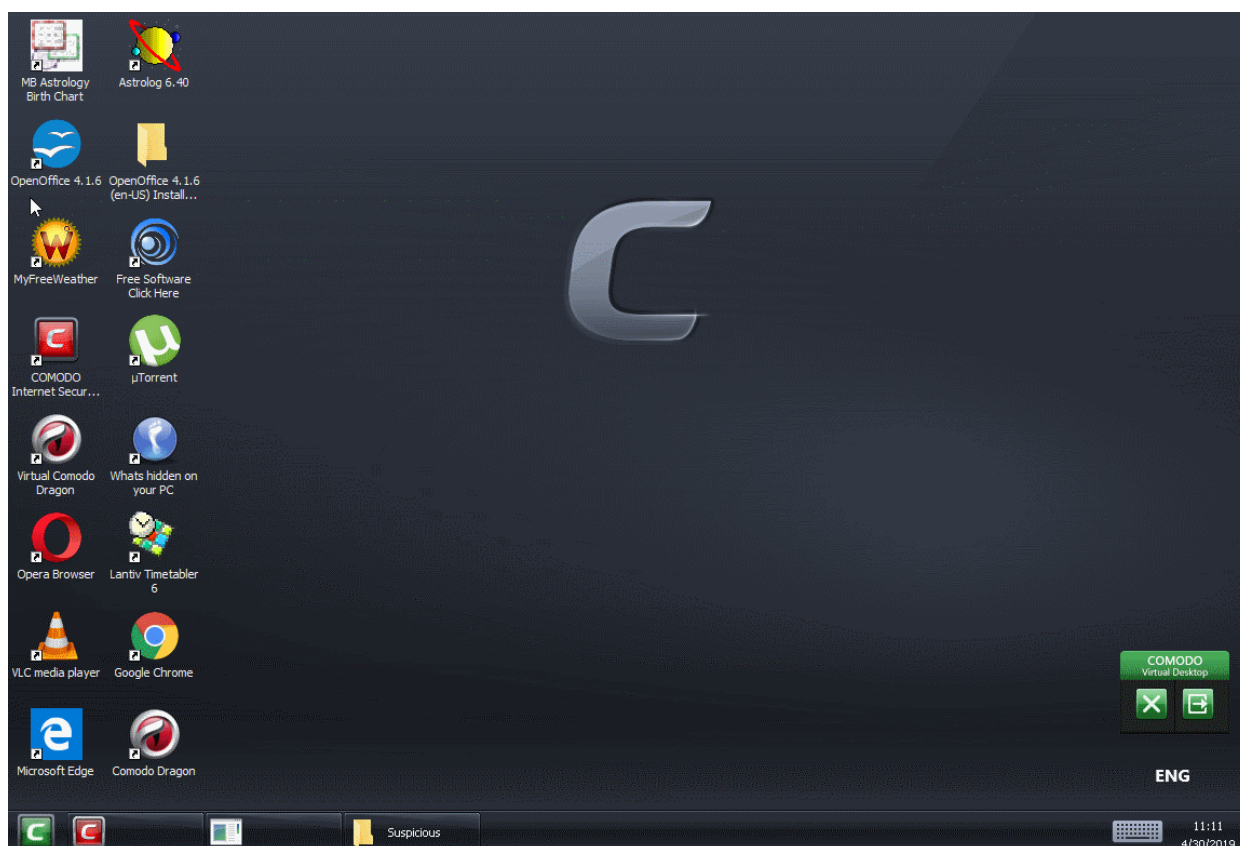
Tablet Mode

- Click the green 'C' icon > 'Settings'

- Choose 'Tablet Mode' and click 'OK'

There are two variants in 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.

    - 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.

    - Click the curved arrow at the top right to swap between the two modes.

    - 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 shown	Apps installed on the tablet are shown	Your real desktop shortcuts and files are shown
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 shown on the launch bar at the bottom	Browser shortcuts are shown 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. Run Browsers Inside the Virtual Desktop

Click 'Tasks' > 'Containment Tasks' > 'Run 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 on your computer.
- Surfing from the virtual desktop removes this threat because websites cannot access your local computer to install malware.
- Furthermore, the virtual keyboard lets you type usernames and passwords without fear that keyloggers will record your keystrokes.

Tip: For visiting important shopping or banking websites, we recommend you use the Secure Shopping environment instead. 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.

Run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left
2. Select the browser you want to run:
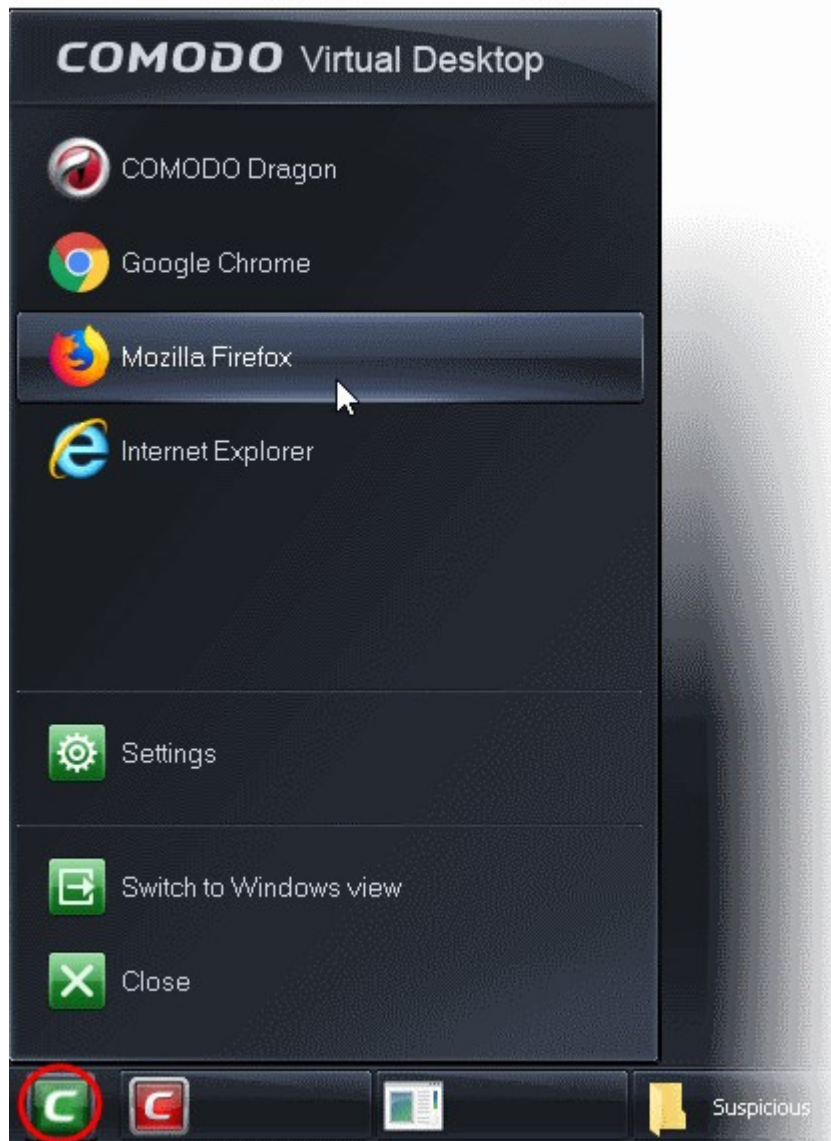
Your choice of browser will open inside the virtual desktop, ready for secure surfing:
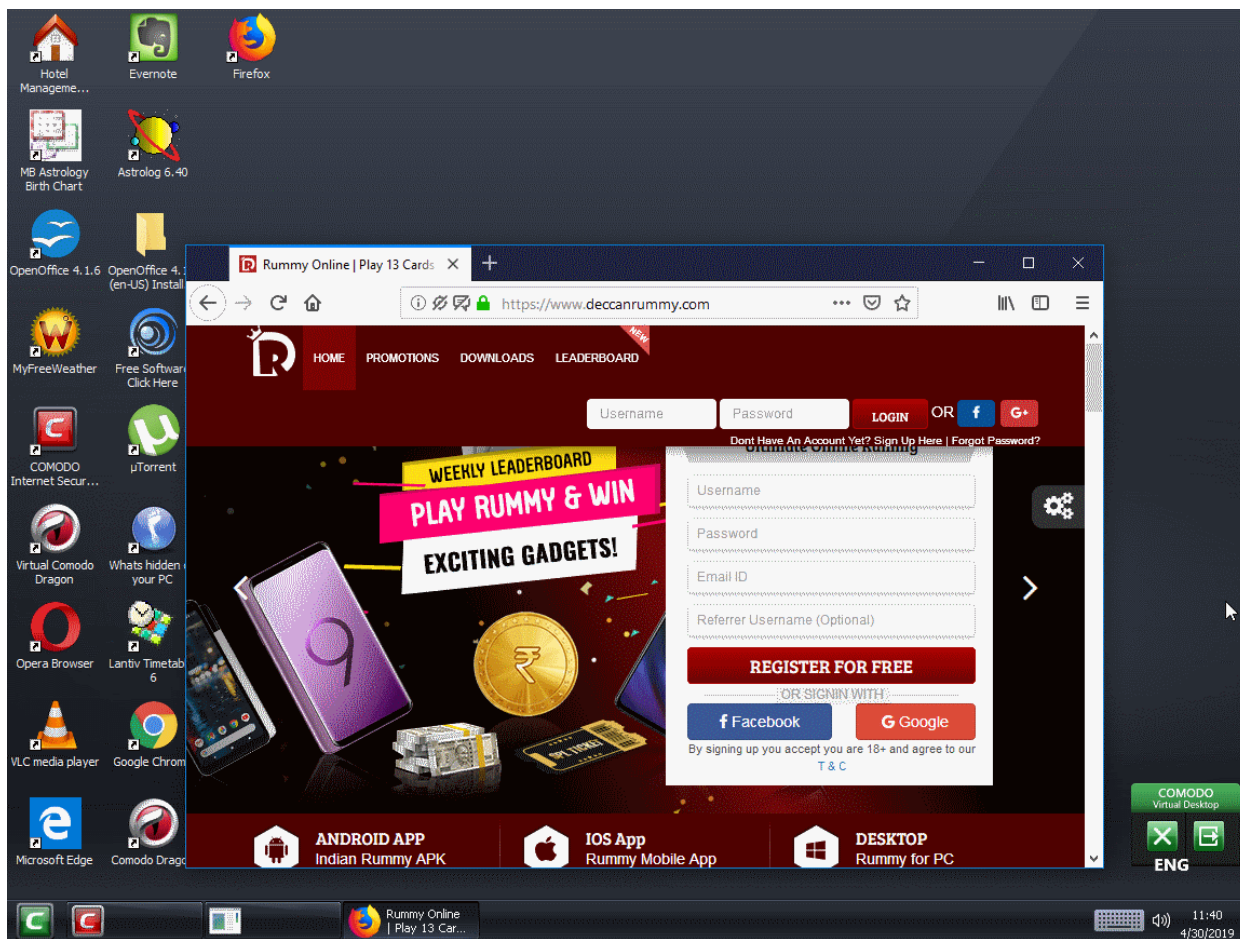
- Browsing history and other records of your internet activity will not be stored on your computer when your session is closed.

4.5.4. Open Files and Run Applications inside the Virtual Desktop

Desktop Shortcuts

- Create a shortcut for a program on your real desktop
- Open the virtual desktop ('Tasks' > 'Containment Tasks' > 'Run Virtual Desktop')
- The shortcuts from your real desktop will be available in the virtual desktop
- Double-click a shortcut to open the application in the virtual desktop

Note: Your desktop shortcuts are only available in in '**Classic Windows Mode**' and '**Tablet + Classic Mode**'.

Shared Space

- The virtual desktop creates a folder called shared space at C:\ProgramData\Shared Space.
- This folder is the only area on your computer that can be accessed by both the host operating system and the virtual desktop.
- You can use it to claim files downloaded in the virtual desktop, or to pass files from the local host to the virtual environment.

Shared space can be accessed in the following ways:

- Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space'
- Click the 'Shared Space' shortcut on the CIS home screen
- Click the 'Shared Space' shortcut on the CIS widget

Open a file from your host system in the Virtual Desktop

1. Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space'
2. Copy the file to the shared space folder

3. Open the virtual desktop (Tasks' > 'Containment Tasks' > 'Run Virtual Desktop')

4. Click the 'Shared Space' icon in the virtual desktop

Note: The shared space icon is only visible in '**Classic Windows Mode**' and '**Tablet + Classic Mode**'.

5. Open the file to run it in the virtual desktop.

4.5.5. Configure the Virtual Desktop

The settings panel lets you change the look and feel of the virtual desktop.

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'

- Click the 'C' button at bottom-left.

- Click 'Settings' in the start menu

- Select 'Classic Mode' or 'Tablet Mode':
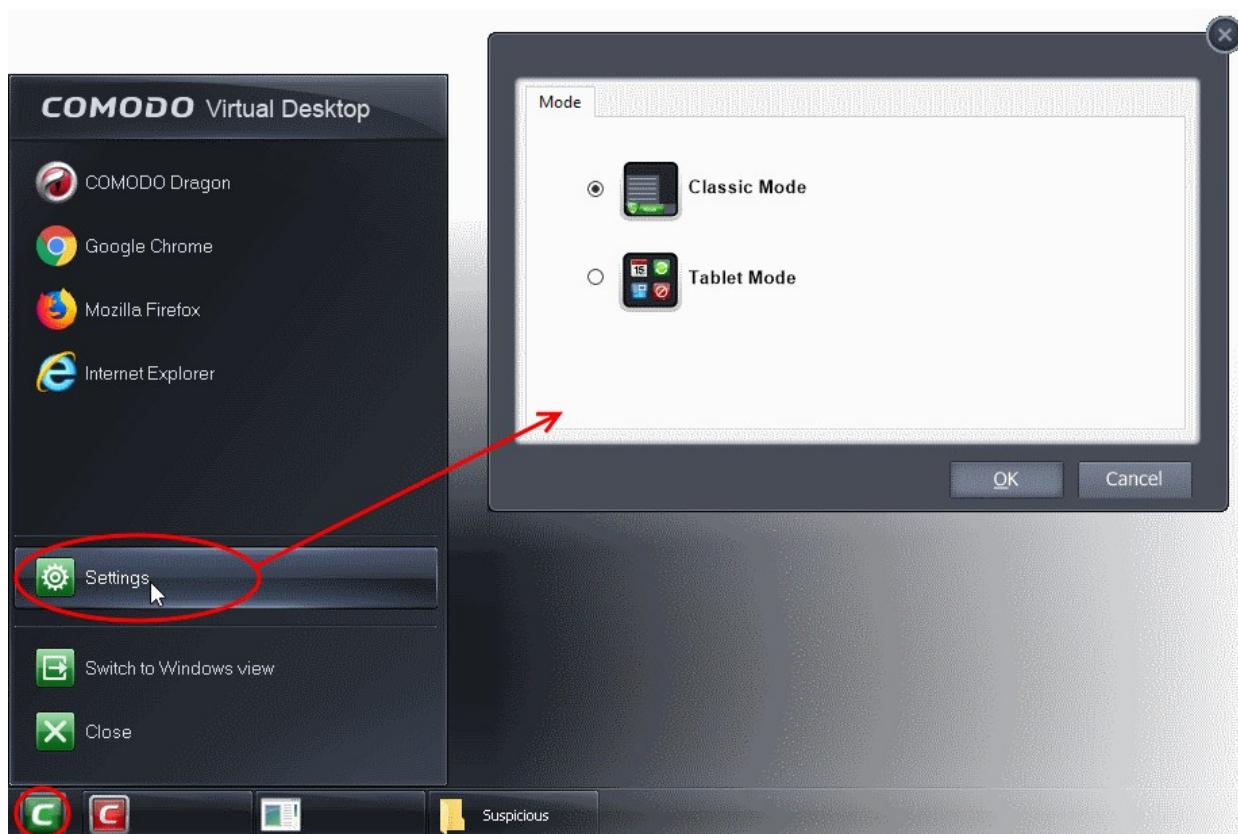
- Click OK for your settings to take effect

4.5.6. Close the Virtual Desktop

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'

- The shortcuts at bottom right let you temporarily switch to your computer desktop, or exit the virtual desktop entirely:
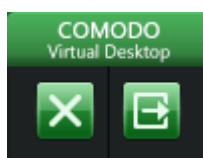
Temporarily switch to your real Windows system
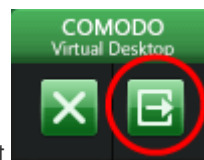
- Click the right button from the shortcuts pane at the bottom right

- 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.

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 'Close' from the 'Virtual Desktop' Start Menu.

    - If password protection is enabled you will need to supply to password to perform either action:
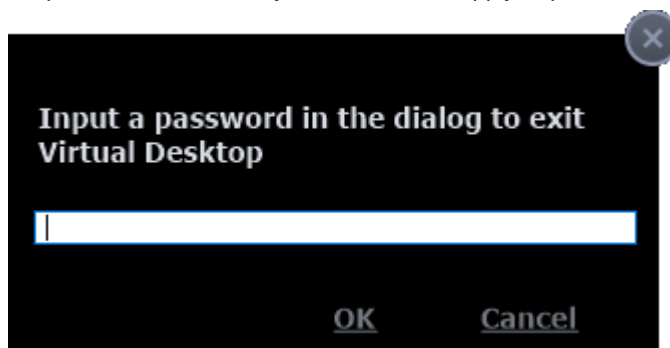
    - Click 'Settings' > 'Containment' > '**Containment Settings**' if you want to enable password protection.

5. Advanced Tasks - Introduction

Click 'Tasks' > 'Advanced Tasks'

- Advanced tasks lets you manage quarantined items, view event logs, submit files to Comodo for analysis, manage CIS tasks, and access other Comodo utilities.
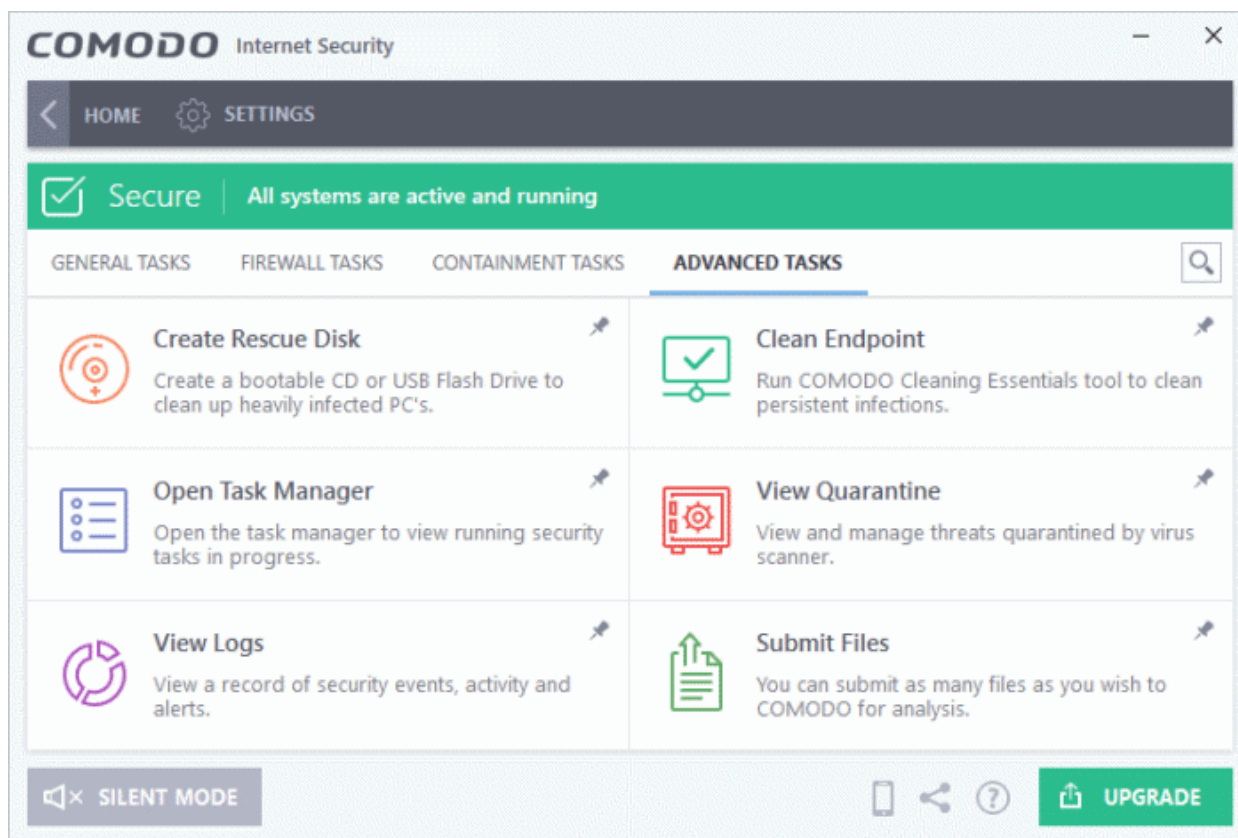
See the following sections to find out more about each feature:

- **Create Rescue Disk - Burn a bootable ISO that lets you run virus scans in pre-boot environments**
- **Clean Endpoint - Deploy Comodo Cleaning Essentials to remove persistent infections from your PC**
- **Task Manager - Stop, pause and resume currently running CIS tasks like antivirus scans and updates**
- **Quarantined Items - Manage files that are moved to quarantine by the virus scanner or 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

Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk'

- Comodo Rescue Disk (CRD) is a bootable disk image that lets you 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 to ISO, CD/DVD, USB or other drive. See **Download and Burn Comodo Rescue Disk** for a walk-through of this process.
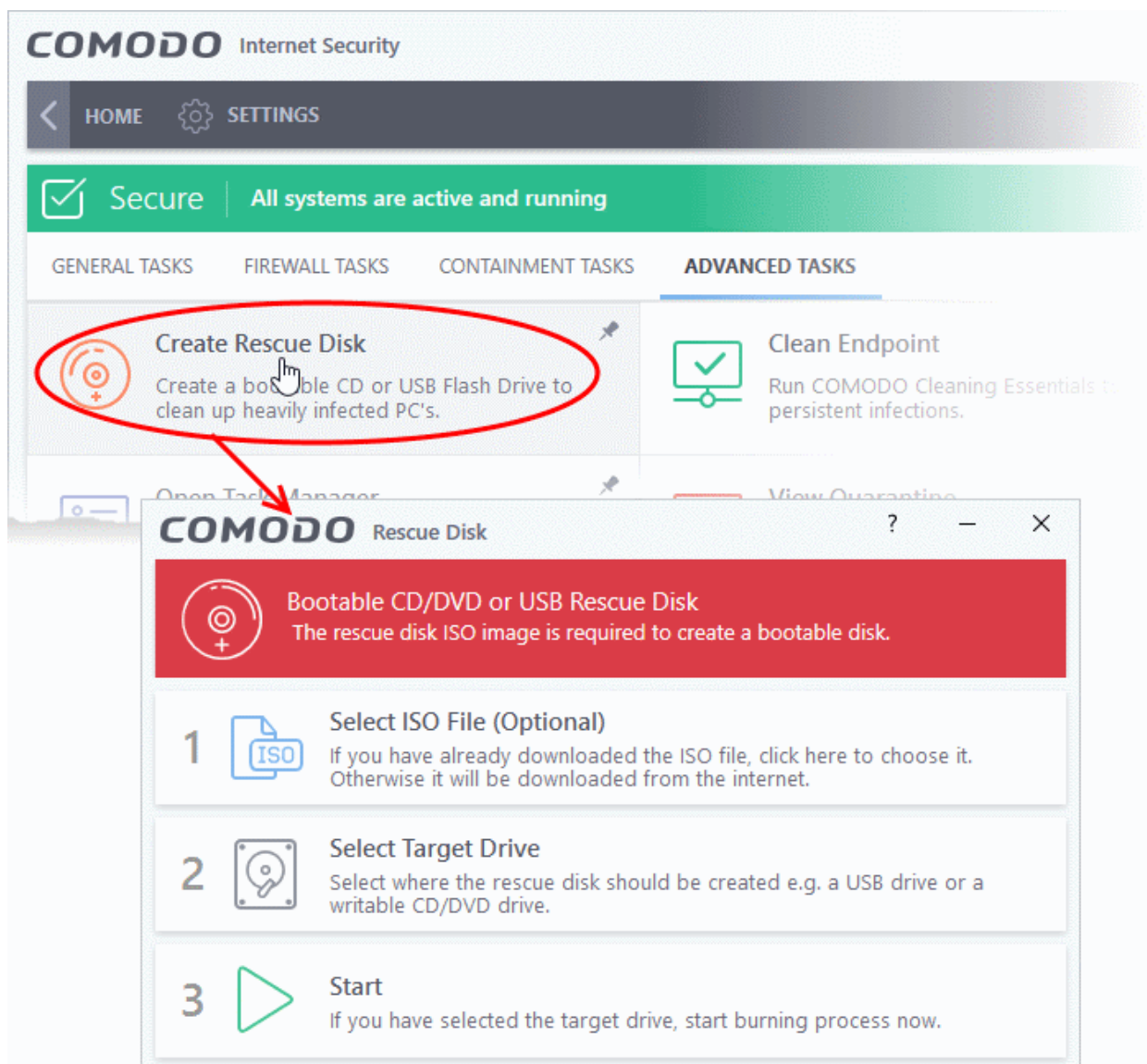
After you have burned the ISO, you need to boot your system to the rescue disk. This will open the scanner in your pre-boot environment.

- Change the boot order on your computer - **http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html**

- Start using CRD - **http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html**

- 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

- Click 'Tasks' > 'Advanced Tasks'
- Click 'Create Rescue Disk'
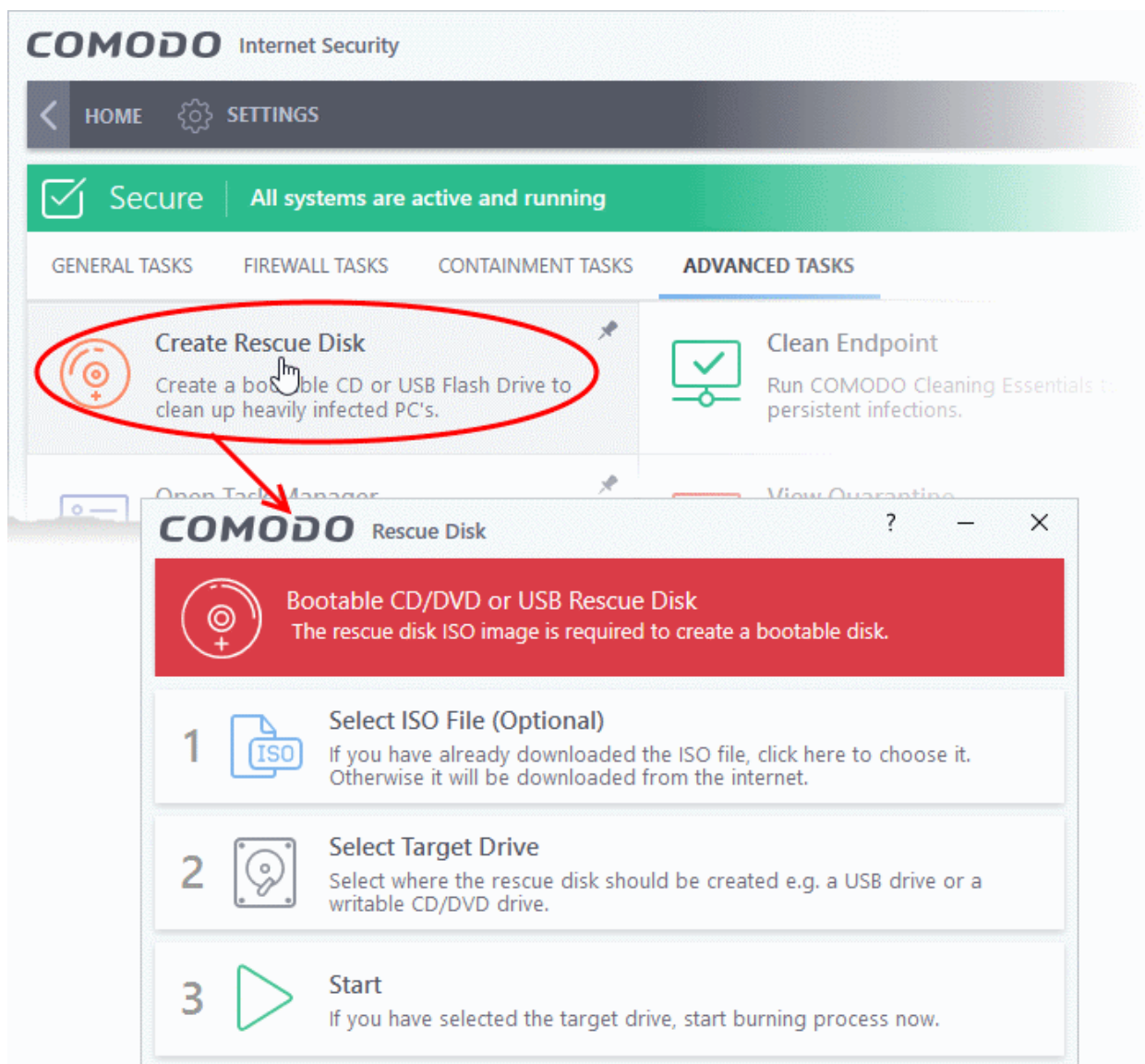
The setup screen shows the steps to create a new rescue disk:

Step 1- Select the ISO file

Optional. If you have already downloaded the rescue disk ISO from Comodo then please select it here. If you haven't yet downloaded then please ignore this step - it will be downloaded automatically during Step 3.

Step 2 Select target drive

Select the CD/DVD or USB on which you want to burn the rescue disk. You will boot to this disk to run the antivirus product.

Burn CD or DVD

- Label a blank CD or a DVD as "Comodo Rescue Disk - Bootable" and load it in your CD/DVD drive.

- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the 'Select Disk' dialog
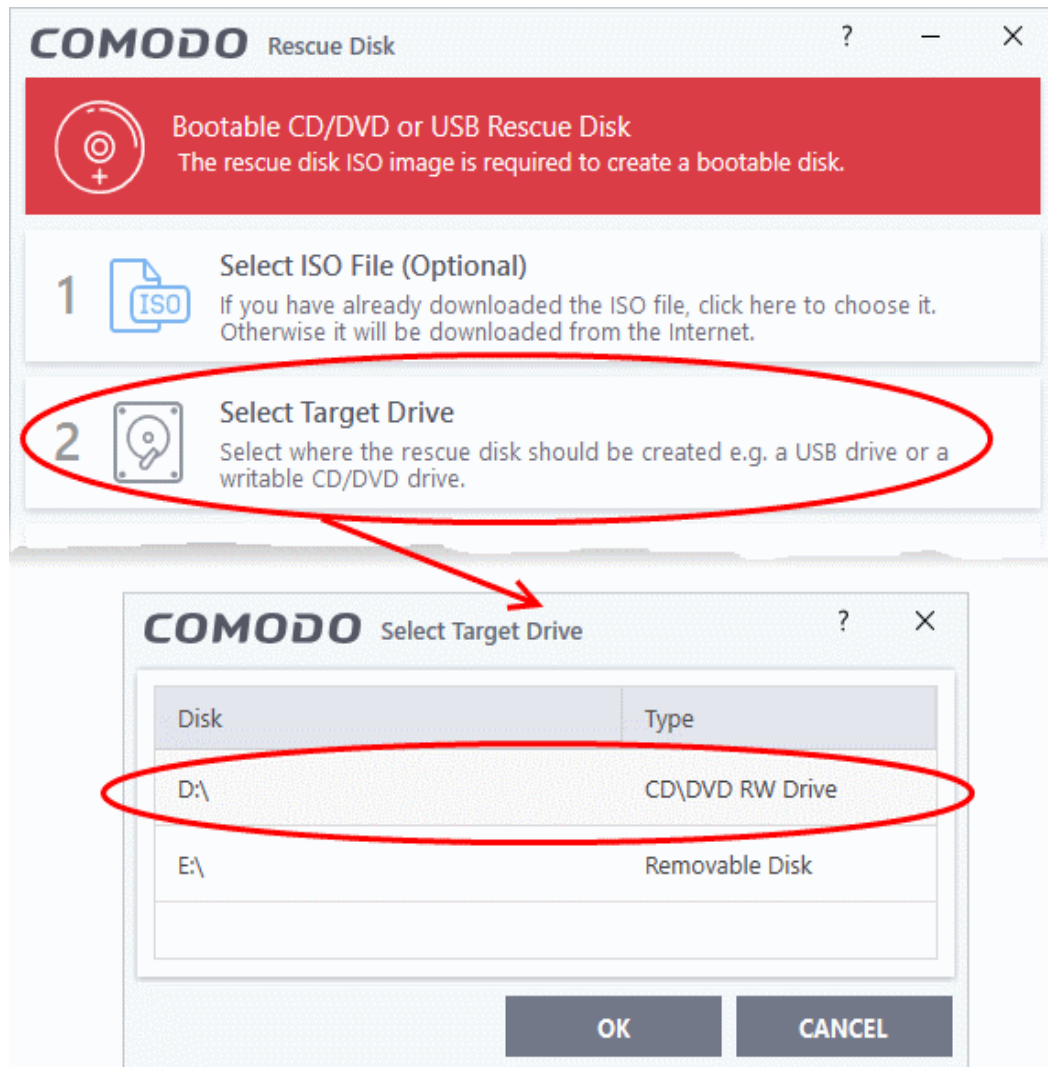
- Click 'OK'

Burn to a USB Drive

- Insert a formatted USB stick in 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

---
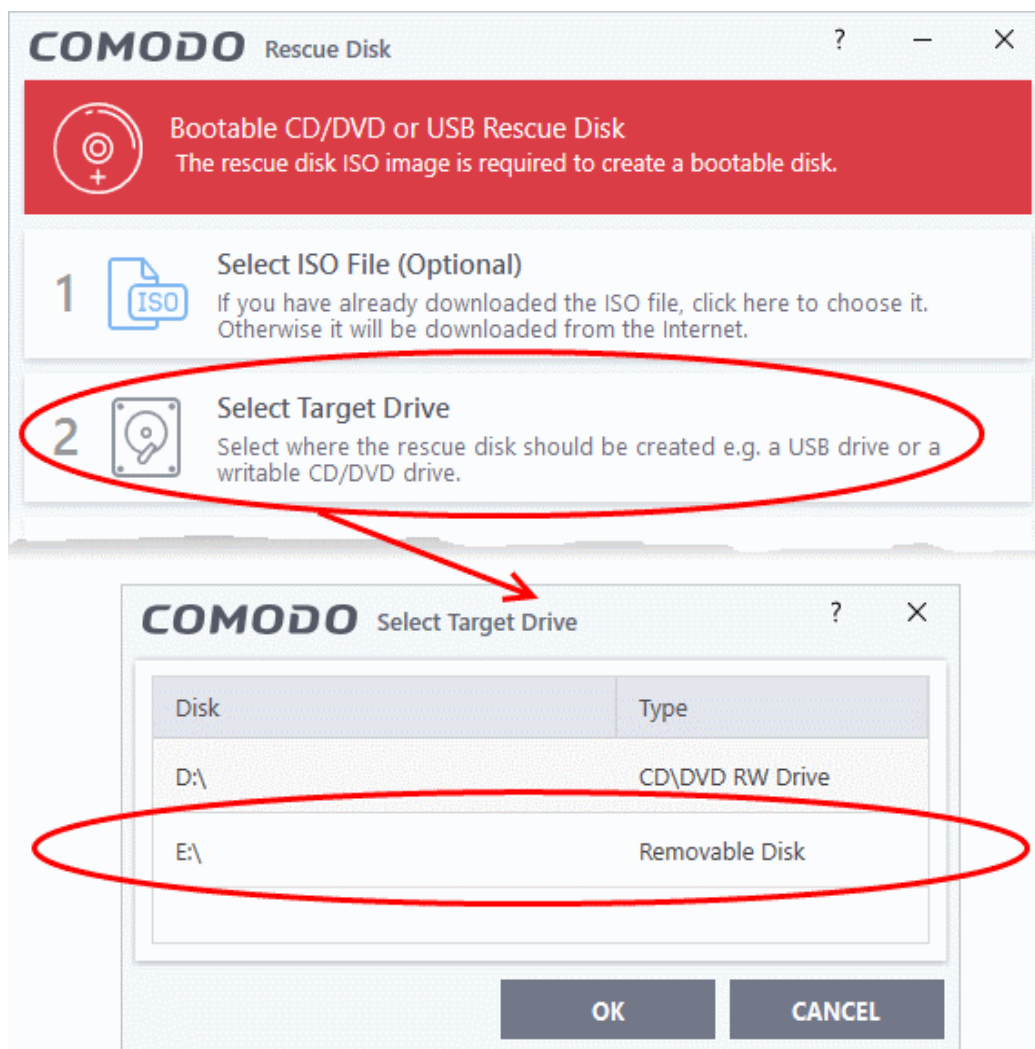
Step 3 - Burn the Rescue Disk

- Click 'Start'
- If you selected a local ISO in step 1 then burning will start immediately. If not, the ISO will be downloaded from Comodo servers:
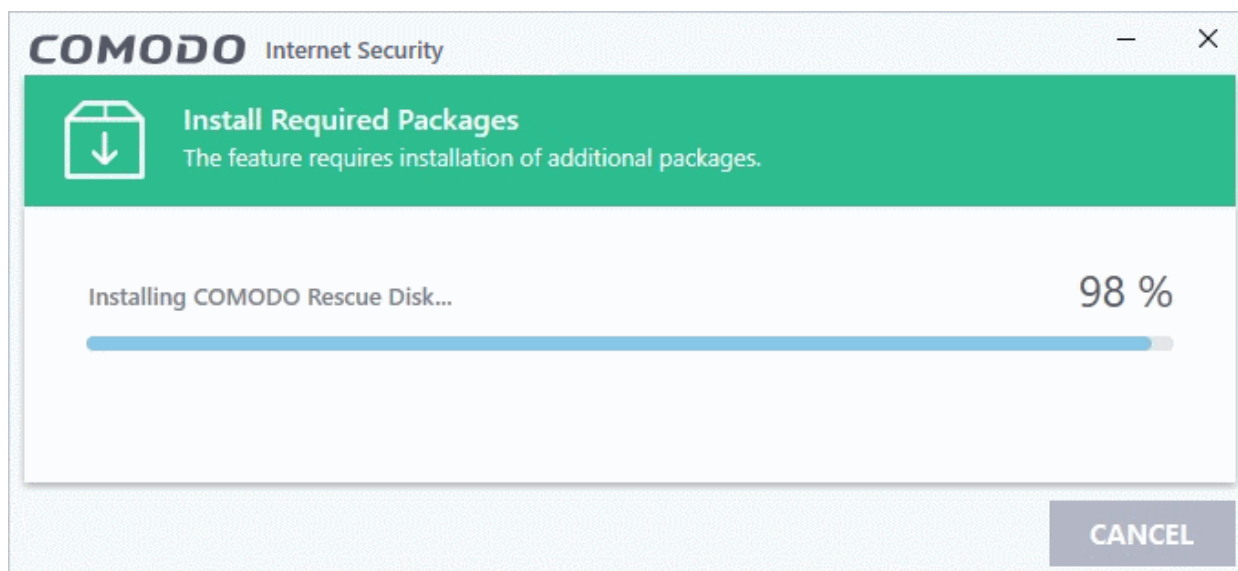
After downloading, setup will burn the ISO to your target drive:
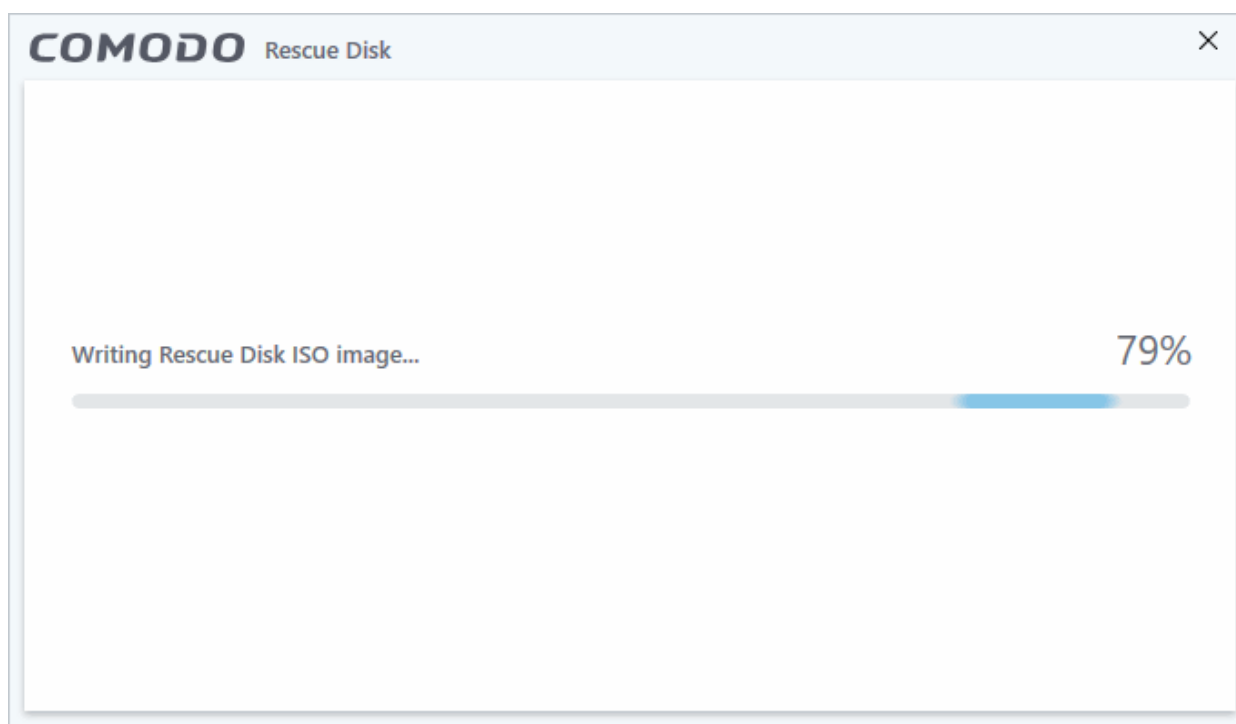
On completion, the files will be written on to the CD/DVD or the USB Drive.

- 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.
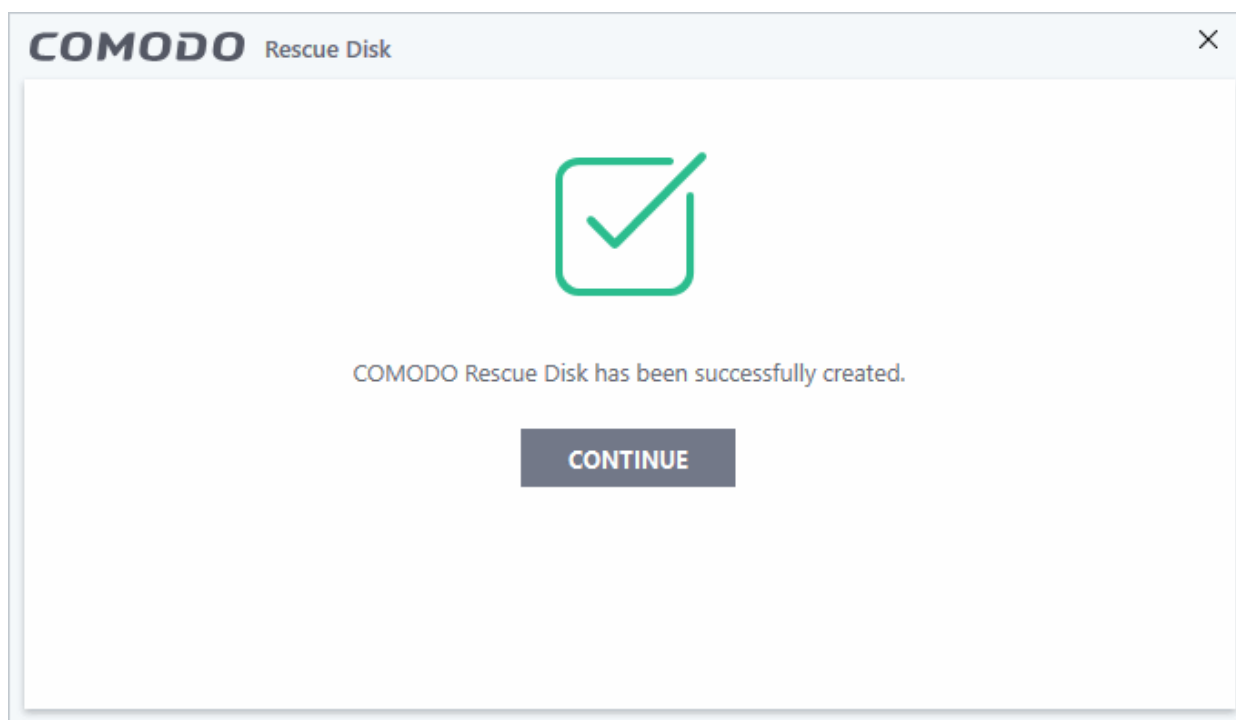
Your bootable Comodo Rescue Disk is ready.

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

5.2. Remove Deeply Hidden Malware

Click 'Tasks' > 'Advanced Tasks' > 'Clean Endpoint'

- Comodo Cleaning Essentials (CCE) help users identify and remove malware and unsafe processes from infected computers.

Major features include:

- **KillSwitch** - A system monitoring tool that lets you identify and terminate unsafe processes on your computer.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** - Allows you to view and control the services and programs which are loaded when your computer 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.

- See the CCE online guide at **https://help.comodo.com/topic-119-1-328-3516-Introduction-to-Comodo-Cleaning-Essentials.html** for more details on the features and usage of the application.

Run CCE from CIS interface

- Click 'Tasks' > 'Advanced Tasks' > 'Clean Endpoint'
- If you have already installed Comodo Cleaning Essentials, clicking 'Clean Endpoint' will open the CCE interface directly.
- When you click 'Clean Endpoint' for the first time, CIS will download and install Comodo Cleaning Essentials. After it is installed, clicking this button in future will open the CCE interface.
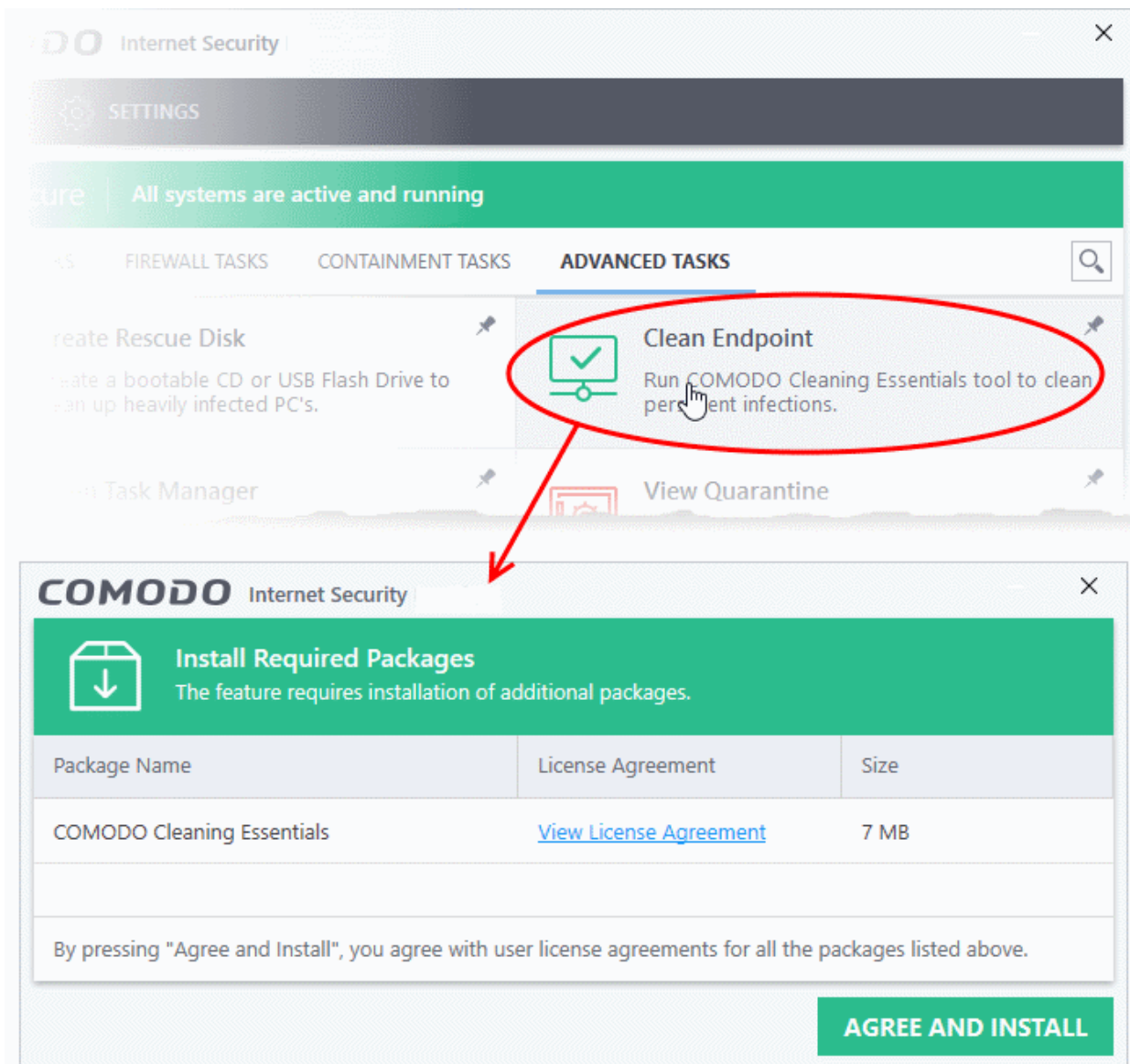
- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.
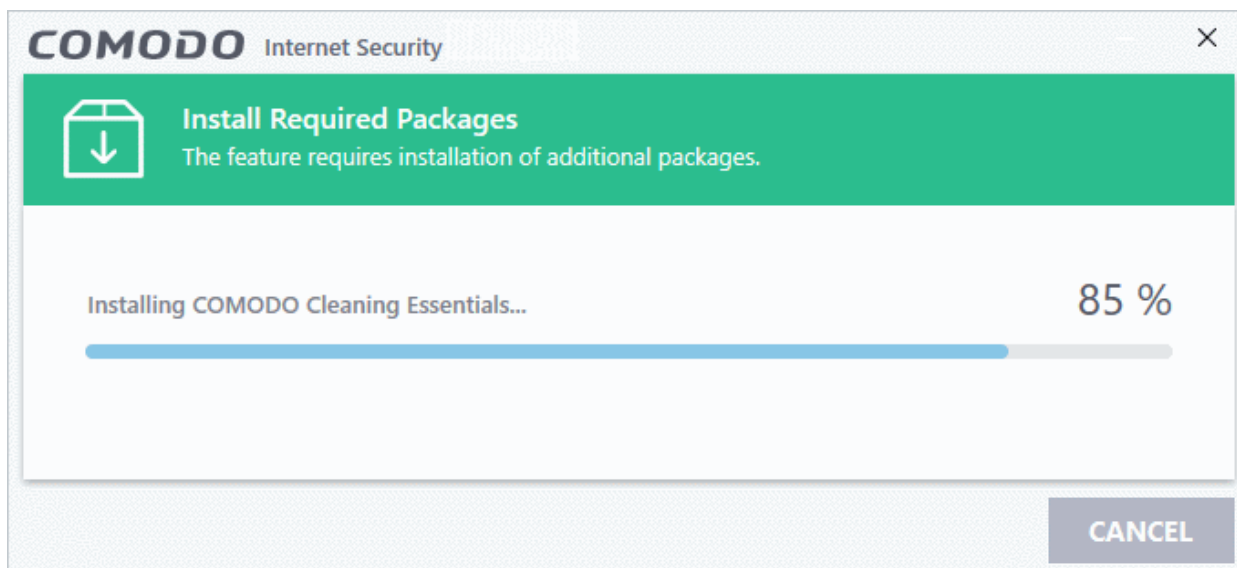
After the installation, the Comodo Cleaning Essentials main interface will open:

- See **https://help.comodo.com/topic-119-1-328-3516-Introduction-to-Comodo-Cleaning-Essentials.html** if you'd like more information on using Comodo Cleaning Essentials.

5.3. Manage CIS Tasks

Click 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'

- Comodo Internet Security can 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.

Open the task manager

- Click 'Tasks' on the CIS home screen
- Click 'Advanced Tasks' > 'Open Task Manager'
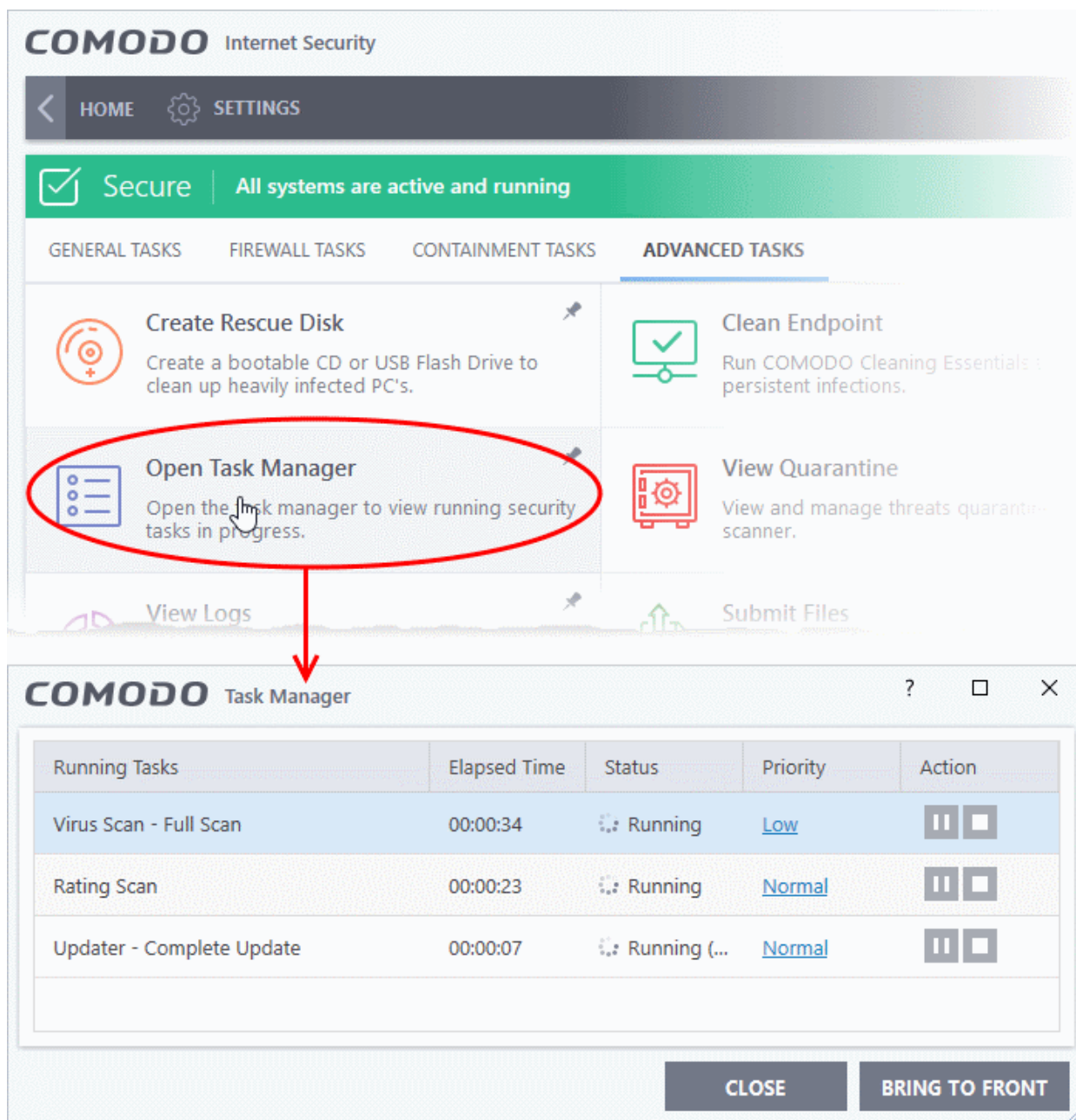
From the Task Manager interface, you can:

- **Reassign task priorities**
- **Pause/resume or stop a running task**
- **Bring a selected task to foreground**

Reassign task priorities

The 'Priority' column show the level of resources committed to the task at run. A higher priority means the task runs more smoothly, but consumes more system resources.

Change the priority of a task

- Click the current priority and select the new one you want to assign:
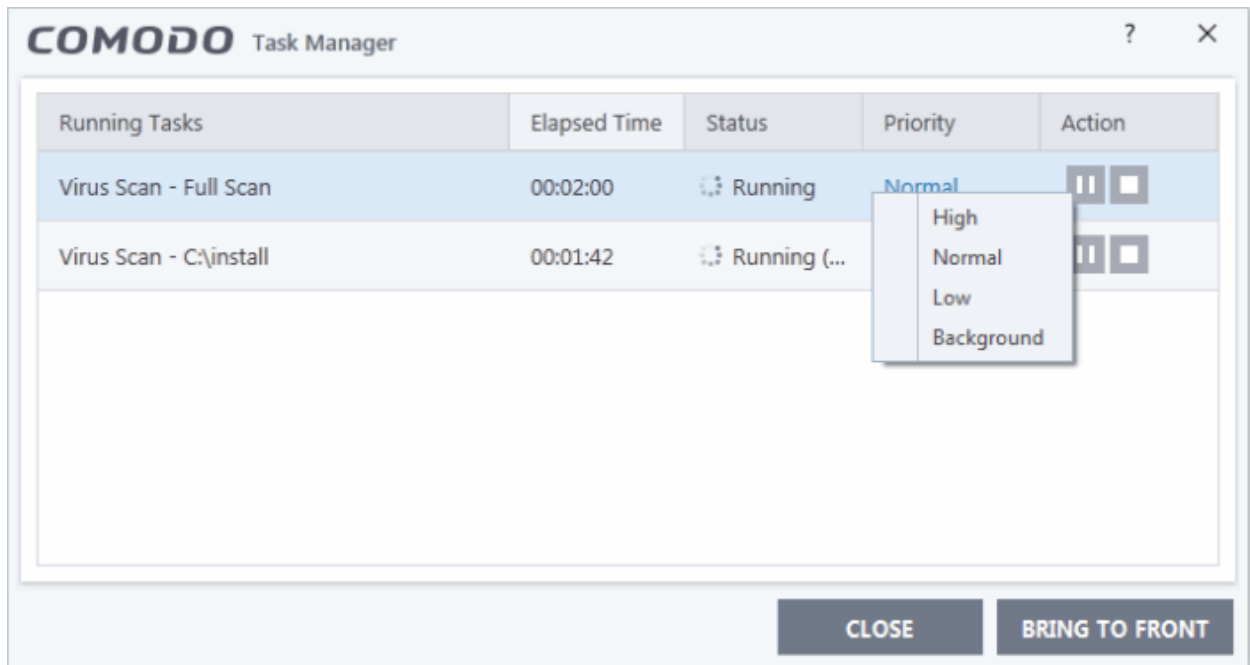
Pause/resume or stop running tasks

Use the buttons in the action column to pause, resume or stop a process:

- To pause a running task, click the 'Pause' button
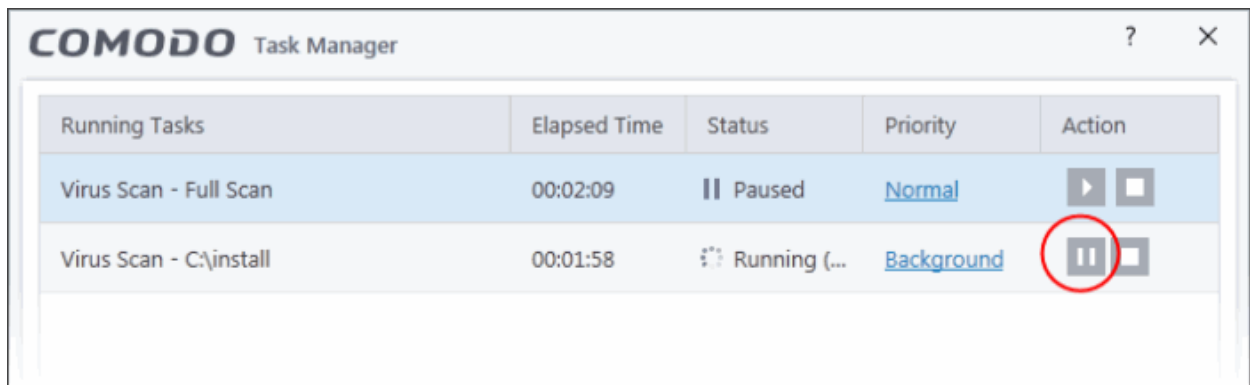
- Click the 'Resume' button to restart a suspended task
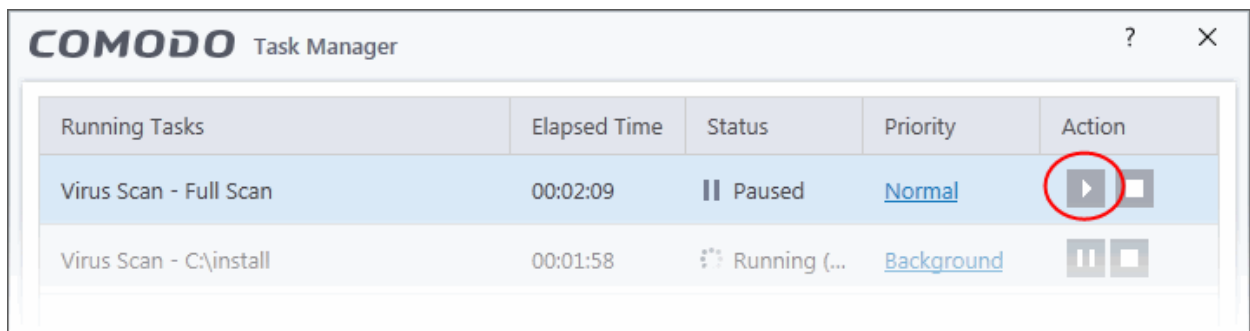
- Click the 'Stop' button to terminate a running task
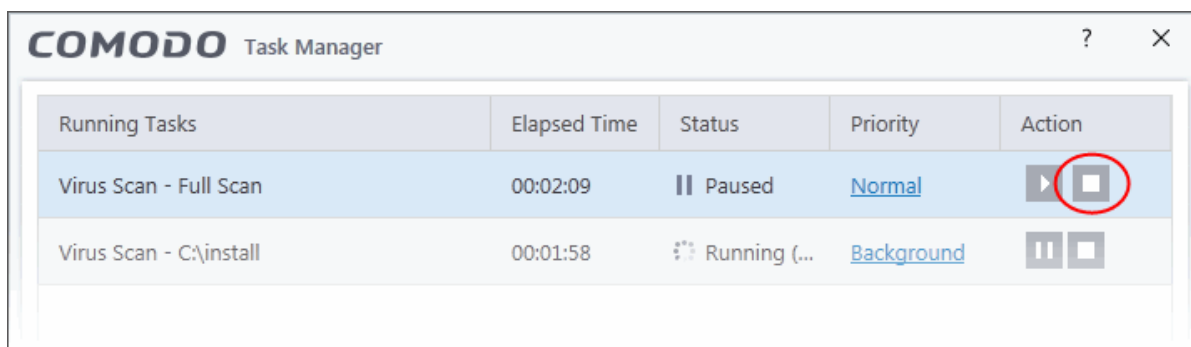
Bring a running task to the foreground

- To view the progress of a background task, select the task and click 'Bring to Front'
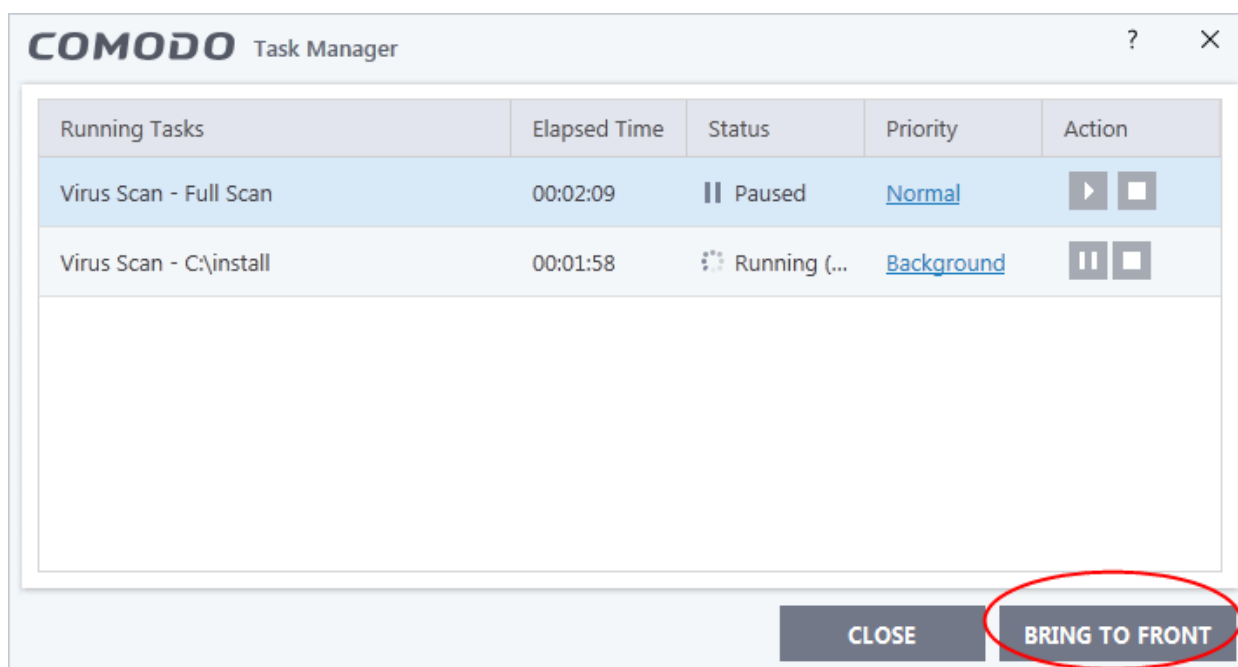
5.4. Manage Quarantined Items

Click 'Tasks' > 'Advanced Tasks' > 'View Quarantine'

- The 'Quarantine' interface contains a list of malicious files which CIS has isolated to prevent them from infecting your system.

- All files in quarantine are encrypted, so they cannot run or cause harm.

- Items are usually quarantined by the antivirus scanner, but it is also possible to manually quarantine items. See '**General Tasks' > 'Scan and Clean Your Computer**' if you want to learn about the AV scanner.

Open the 'Quarantine' interface

- Click 'Tasks' on the CIS home screen

- Click 'Advanced Tasks' > 'View Quarantine'
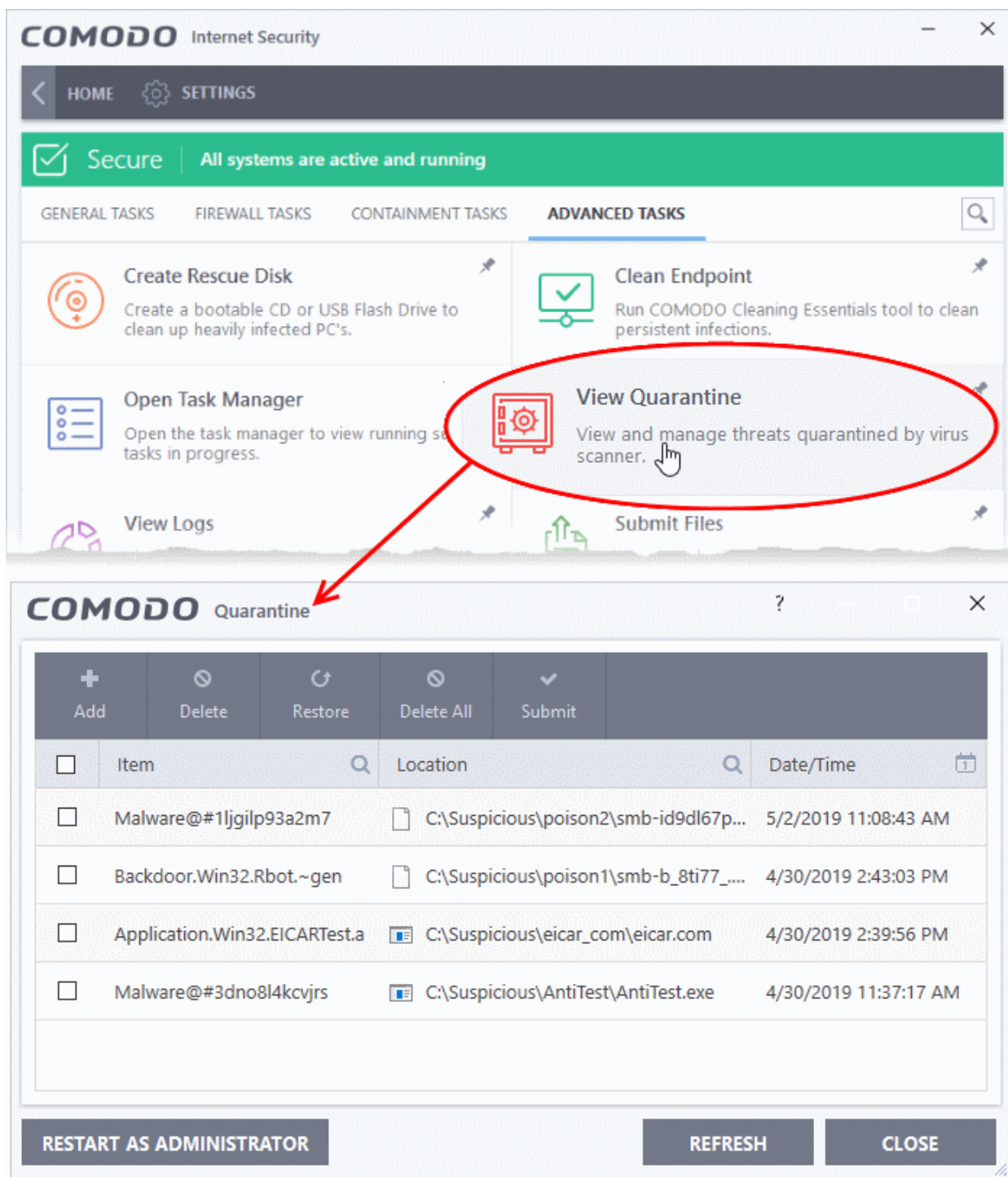
- **Item** - The name of the malicious component
- **Location** - The file path of the item
- **Date/Time** - When the item was moved to quarantine.

The interface lets you review quarantined files and take the following main actions:

- **Permanently delete the file**
- **Restore the file to its original location**
- **Submit the file to Comodo for analysis**
- **Manually add files to quarantine**

Search and filter options:

- Click any column header to sort the items in alphabetical order

---

- Click the search icon in the 'Item' column to search for a file by name.
- Click the search icon in the 'Location' column to search by file-path.
- Click the icon in the 'Date/Time' column to filter results by time period.
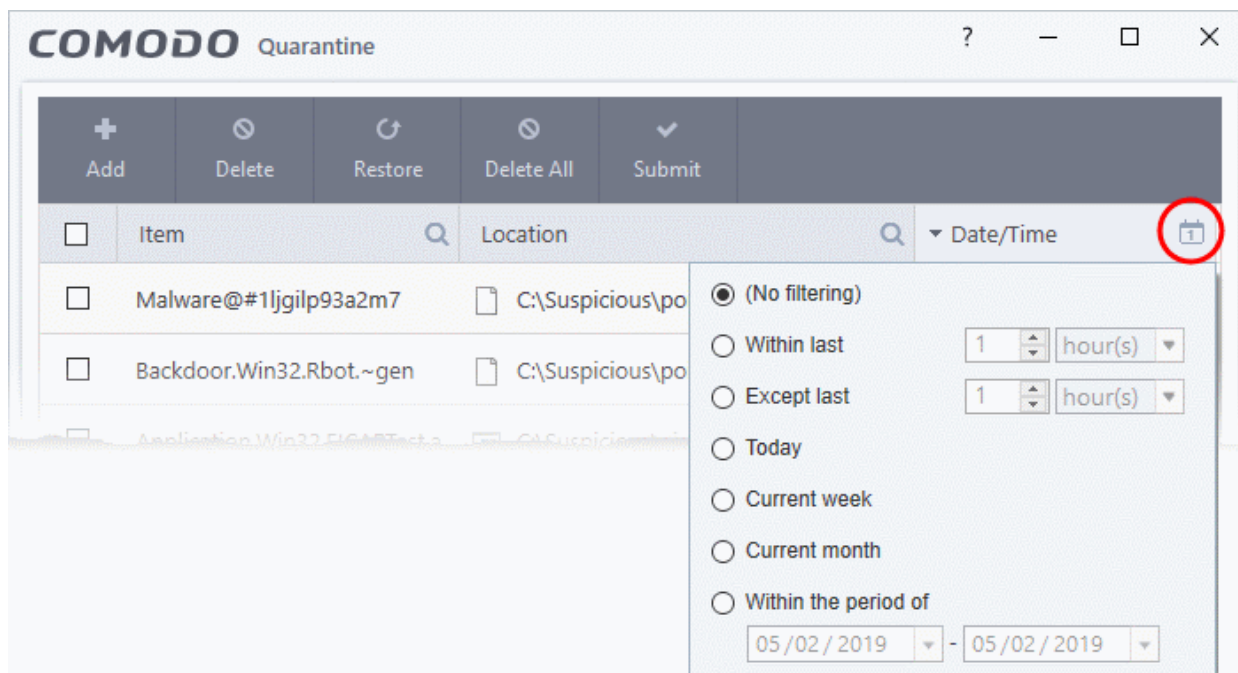
Manually add files to quarantine

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

- Click 'Tasks' on the CIS home screen
- Click 'Advanced Tasks' > 'View Quarantine'
- Click the 'Add' button at the top
- Navigate to the file you want to add to the quarantine and click 'Open'.
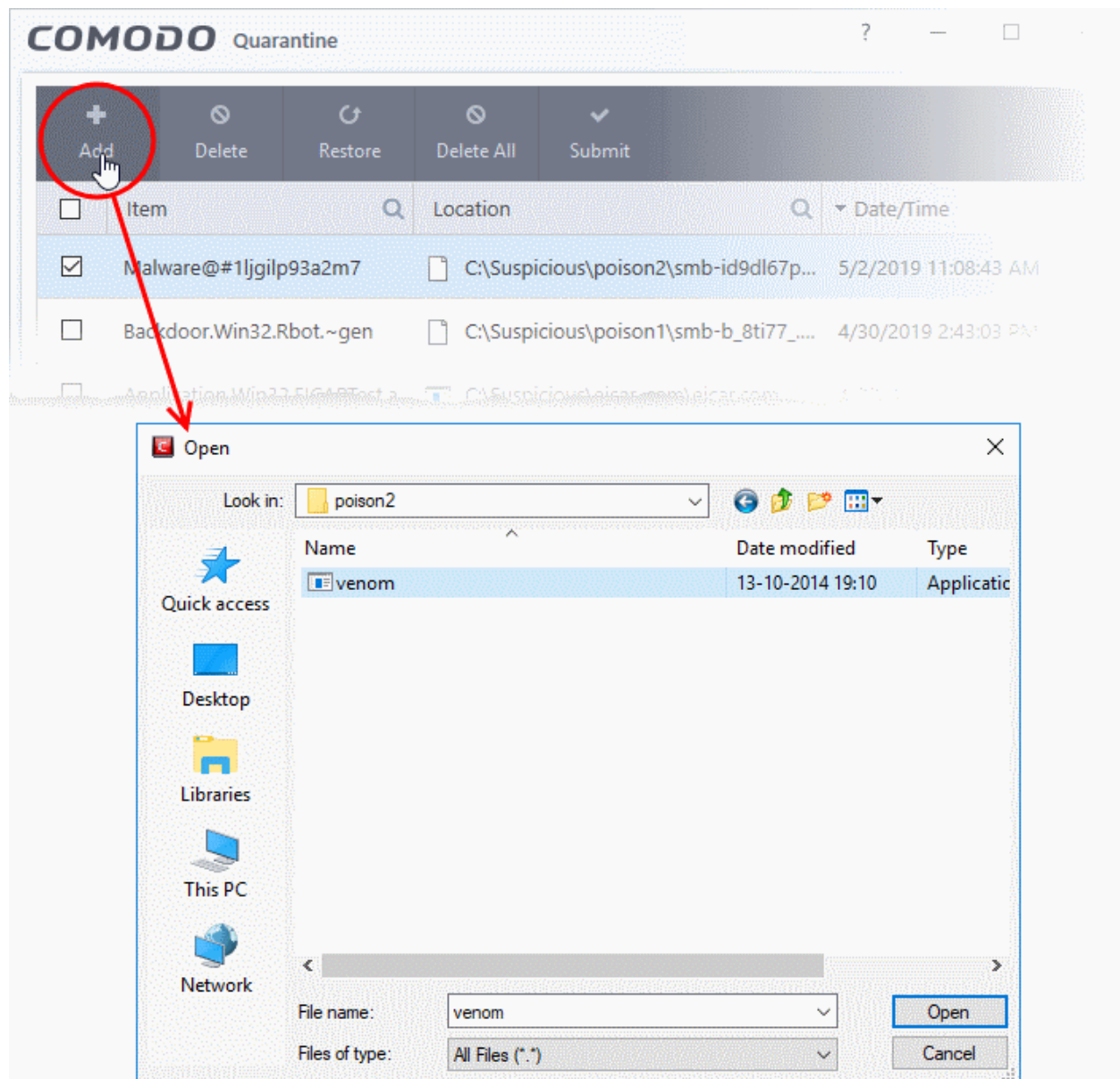
The file will be added to 'Quarantine'. You can even send the file for analysis to Comodo, for inclusion in the white list or black list, by clicking the 'Submit' button.

Remove a quarantined item

- Click 'Tasks' on the CIS home screen

- Click 'Advanced Tasks' > 'View Quarantine'

- Select the items in the quarantine interface and click the 'Delete' button at the top.

- Click the 'Delete All' button if you want to permanently remove all quarantined items.

- The files will be deleted from your computer

Restore a quarantined item

- Click 'Tasks' on the CIS home screen

- Click 'Advanced Tasks' > 'View Quarantine'

- Select the items to be moved back to their original locations and click the 'Restore' button at the top.
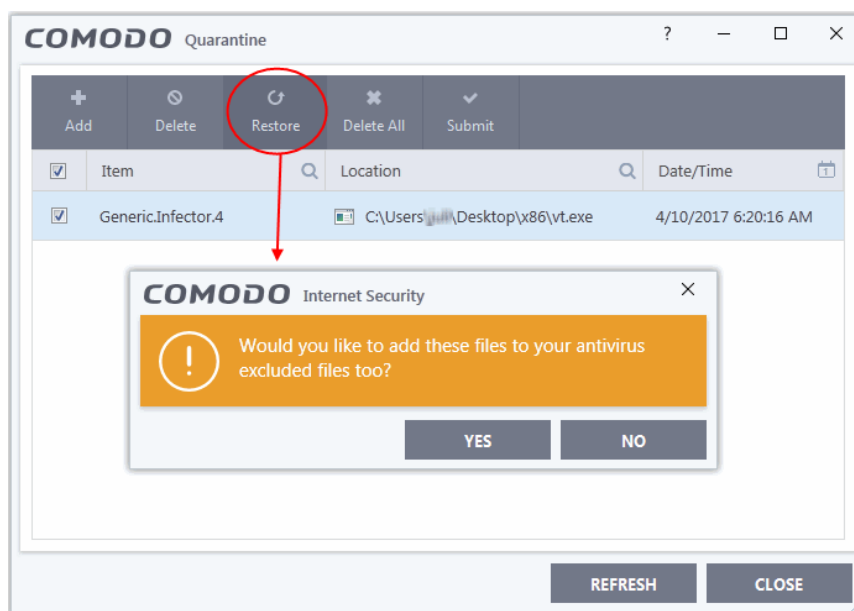
You will be asked if you want to add the item to the **Exclusions** list:

- '**Yes**' - The file will be restored to its original location. It will not be flagged as dangerous nor quarantined by future antivirus scans.

- '**No**' - The file will be restored to its original location. If the file contains malware it will be re-quarantined by the next antivirus scan.

> **Note**:
>
> You need to run CIS with admin privileges in order to restore a file. If you are not logged in as an admin already:
>
> - Click the 'Restart as administrator' button
>
> - Select an admin account, enter the password and click 'Yes'
>
> - CIS will reopen with admin privileges, allowing you to restore items to their original locations:
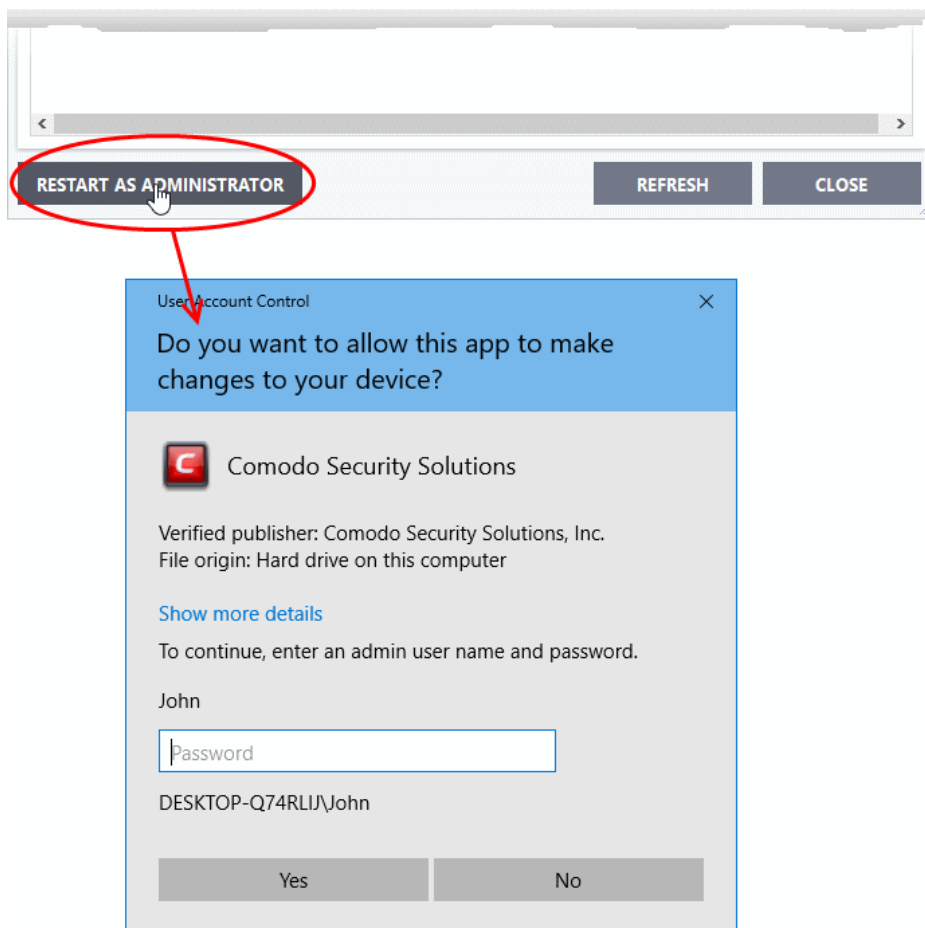
Submit quarantined items to Comodo for analysis

You can submit files which you think are safe but have been mis-identified as malware by CIS (false positives) from the 'Quarantine' interface.

- Click 'Tasks' on the CIS home screen
- Click 'Advanced Tasks' > 'View Quarantine'
- Select the items you want to send then click the 'Submit' button at the top.
- The file will be uploaded to Comodo for analysis.
- 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, they will be added to the database of virus signatures (blacklisted).
- You can see the status of your submitted files from the 'Settings' > 'File Rating' > 'Submitted Files' interface. See **Submitted Files** for guidance on this.

5.5. View CIS Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR
- Click 'Logs' in advanced view of the CIS home screen

CIS logs all events generated by the antivirus, firewall, HIPS, containment and other modules.
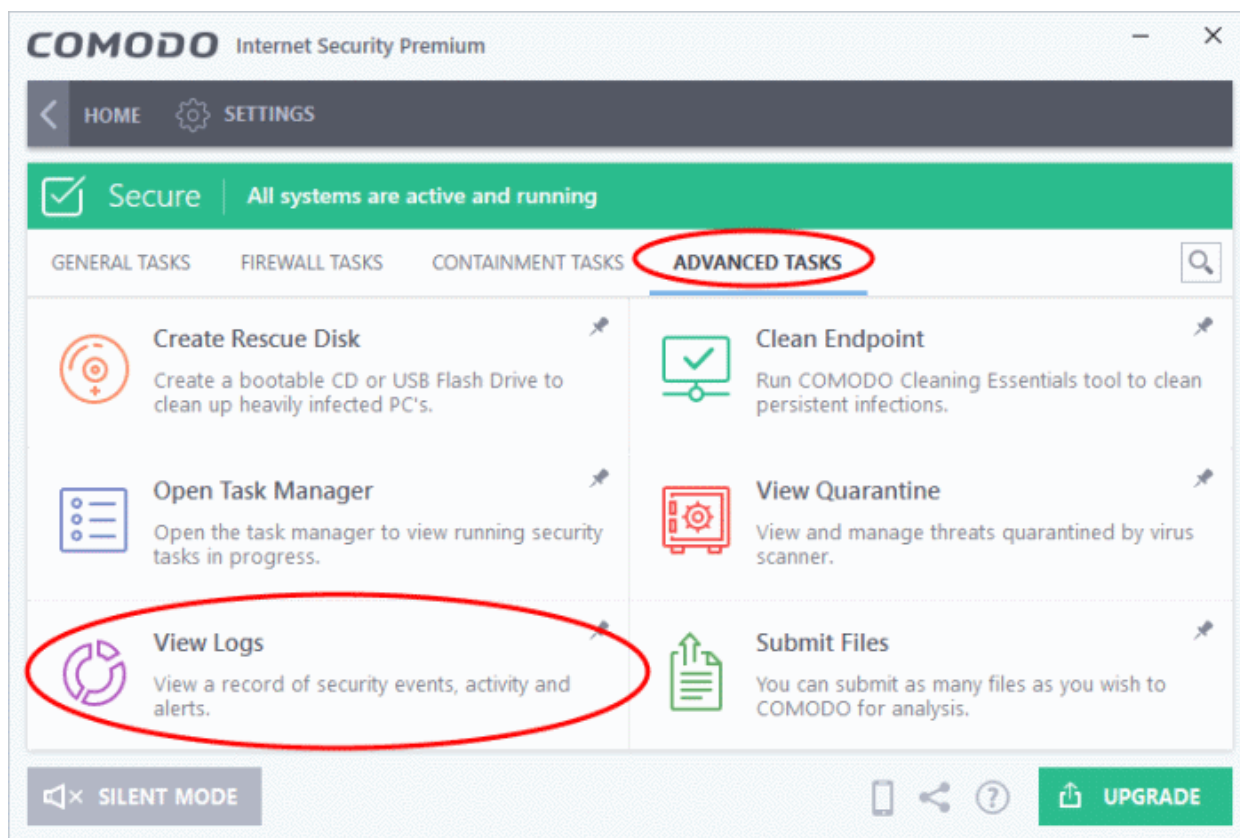
The log dashboard shows a summary of events on the device:
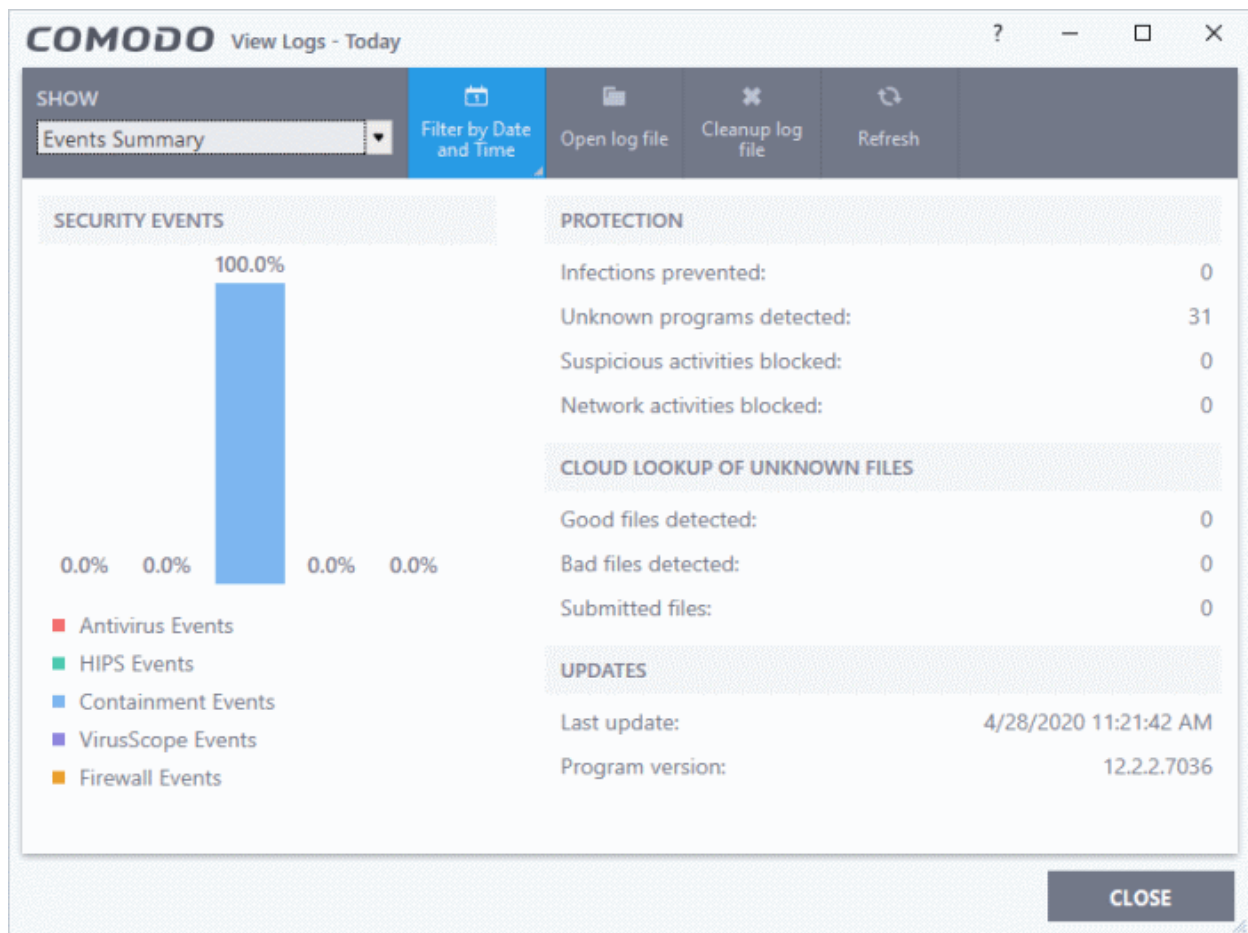
Use the drop-down at top-left to view a specific type of log:

- **Antivirus**
- **VirusScope**
- **Firewall**
- **HIPS**
- **Containment**
- **Website Filtering**
- **Device control**
- **Autoruns Events**
- **Alerts Displayed**
- **Tasks Launched**
- **File List Settings Changes**
- **Vendor List Changes**
- **Trusted Certificate Authorities Changes**
- **Configuration Changes**
- **Secure Shopping Activities**
- **Search and Filter Logs**

5.5.1. Antivirus Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'Antivirus Events' from the drop-down at upper-left

- Antivirus logs contains stats about scanned objects, the settings used for each task, and a history of actions performed on individual files. Logs are recorded for real-time protection events, antivirus database updates and more.

Tip: You can also view these logs by clicking the number next to 'Detected Threats' on the home screen (advanced view).

- **Date & Time** - When the event occurred.

- **Location** - The installation path of the suspicious application

- **Malware Name** - The malicious item that was detected

- **Action** - How the malware was handled by CIS.

- **Status** - Whether the action taken was a success or failure

- **Alert** - Click 'Related Alert' to view the notification generated by the event

Note: Alerts are only shown if 'Do not Show Antivirus Alerts' is disabled in 'Settings' > 'Antivirus' > 'Real-time Scan'.

See **Real-time Scan Settings** for more details.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order

5.5.2. VirusScope Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'VirusScope Events' from the drop-down at upper-left

- **Date & Time** - When the event occurred.

- **Location** - The installation path of the suspicious application

- **Malware Name** - The malicious item that was detected

- **Action** - How VirusScope handled the malware.

  - **Reverse** - VirusScope attempted to undo any changes made by the malicious item

  - **Quarantine** - VirusScope placed the suspicious file in quarantine

  - **Detect** - VirusScope observed malicious activity, but did not quarantine the file or reverse its changes

  - **Ask** - VirusScope detected malicious activity and showed an alert. The alert asks whether you want to quarantine the file or reverse its changes

- **Status** - Whether the action taken was a success or failure

- **Alert** - Click 'Related Alert' to view the notification generated by the event

Note: VirusScope alerts are only shown if 'Do not show pop up alerts' is disabled in 'Settings' > 'Advanced Protection' > 'VirusScope'.

See **VirusScope Configuration** for more details.

- **Activities** - Click 'Related Alert' to view the notification generated by the event. An example is shown below:
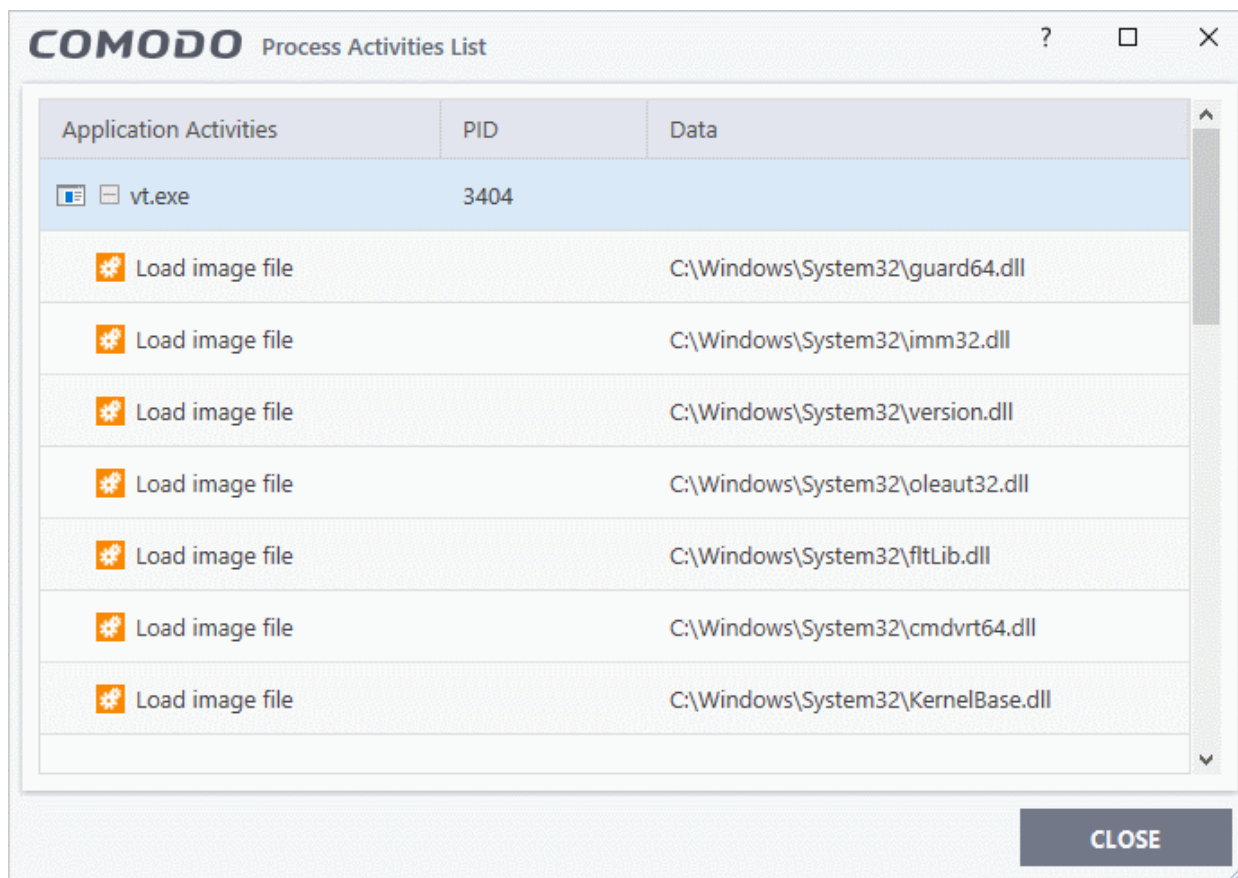
Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order

5.5.3. Firewall Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'Firewall Events' from the drop-down at upper-left

- Firewall events are created for various reasons. Reasons include when a process attempts a connection that breaks a **firewall rule**, or when there is a change in firewall settings.
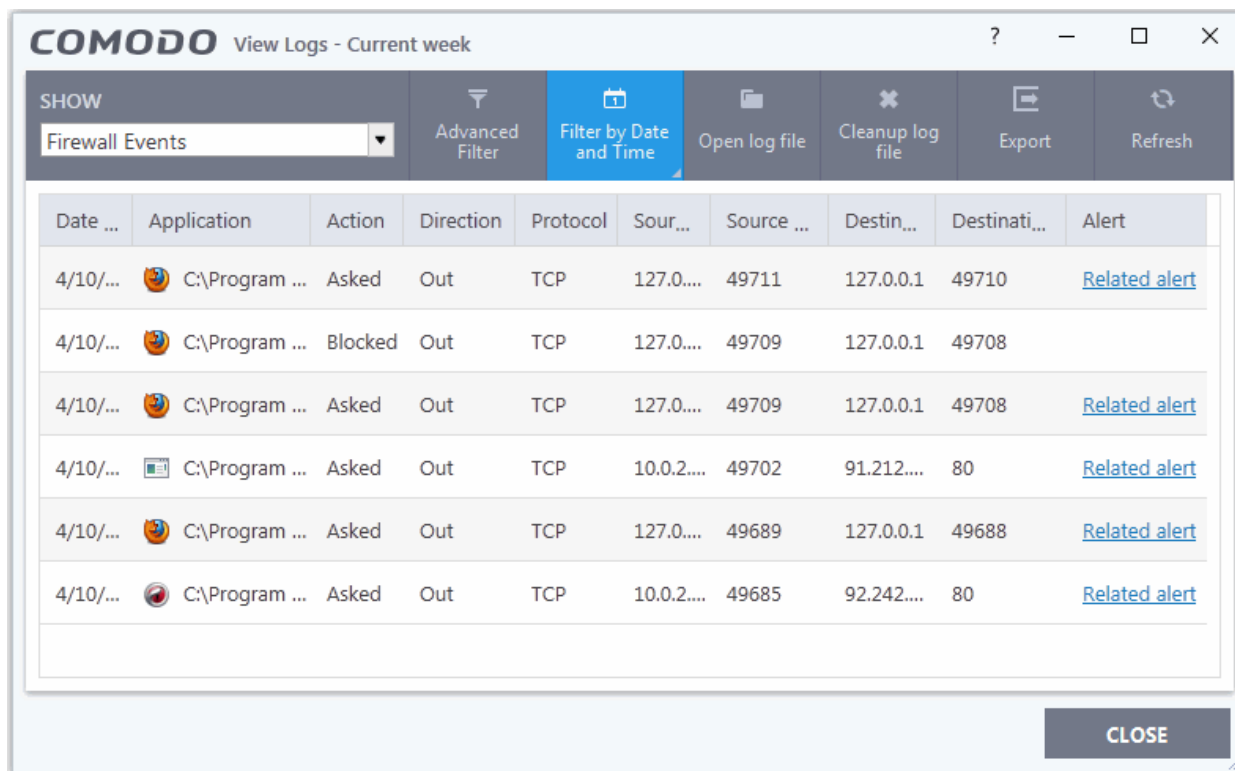
- **Date & Time** - When the event occurred.
- **Application** - The name of the program or process that caused the event.
- **Action** - How the firewall reacted to the connection attempt. For example, whether the attempt was allowed, blocked o r an alert displayed.
- **Direction** - Whether the connection attempt was inbound or outbound.
- **Protocol** - The connection method that the application attempted to use. This is usually TCP/IP, UDP or ICMP, which are the most heavily used networking protocols.
- **Source IP** - The address of the host from which the connection attempt was made. 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.
- **Source Port** - The port number that the source host used to make the connection attempt
- **Destination IP** - The address of the host to which the connection attempt was made. For inbound connections, this is usually the IP address of your computer.
- **Destination Port** - The port number on the destination host which the source tried to connect to.
- **Alert** - Click 'Related Alert' to view the notification generated by the event

> **Note**: Firewall alerts are only shown if 'Do not show pop up alerts' is disabled in 'Settings' > 'Firewall' > 'Firewall Settings'.
>
> See **General Firewall Settings** for more details.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order.

5.5.4. HIPS Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

    OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'HIPS Events' from the drop-down at upper-left

Host intrusion prevention (HIPS) events are generated for various security reasons. These include changes in HIPS settings, when an application attempts to access restricted areas, or when an action contravenes your **HIPS rulesets**.
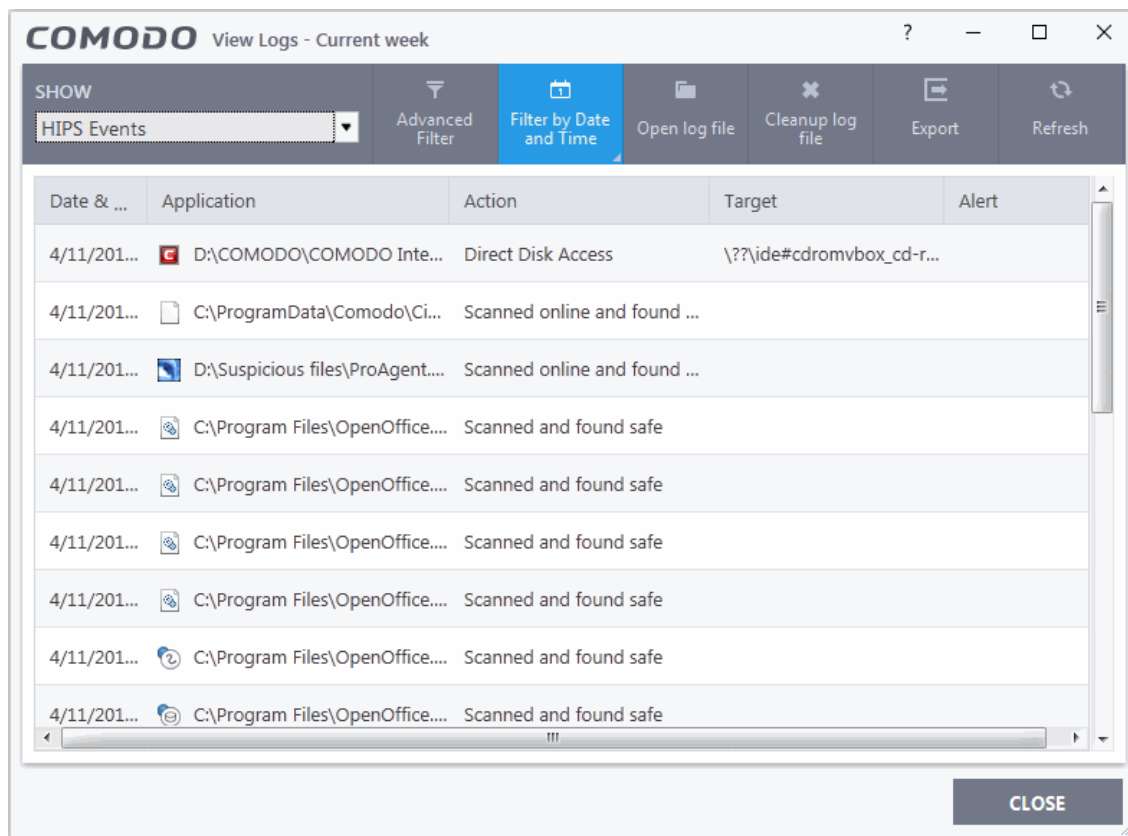
- **Date & Time** - When the event occurred.

- **Application** - The name of the program or process that caused the event.

- **Action** - The activity of the application and how HIPS handled it

    - 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 notification that was shown at the time.

    - This column will state 'Block File' if the action was not allowed.

- **Target** - Location of the file, COM interface or registry key accessed by the process.

- **Alert** - Click 'Related Alert' to view the notification generated by the event

Note: Alerts are only shown if 'Do not pop-up alerts' is *disabled* in 'Settings' > 'HIPS Configuration > 'HIPS Settings'. See **HIPS Settings** for more details.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order.

5.5.5. Containment Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'Containment Events' from the drop-down at upper-left

CIS records all actions taken by the containment module. Events that are recorded include:

- When you manually run an application in the container

- When an an auto-containment rule runs an application in the container

- **Date & Time** - When the event occurred.

- **Application** - The installation path of the application that was run in the container

- **Rating** - The reputation of the contained application. The trust rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Unrecognized files are run in the container until such time as they can be classified as 'Trusted' or 'Malicious'.

- **Action** - How the malware was handled by CIS. This is also the restriction level imposed on the application by the container.

- **Contained by** - The CIS service, policy or user that placed the application in the container.

- **Alert** - Click 'Related Alert' to view the notification generated by the event.

> Note: Containment alerts are shown when an installer, or unknown application requires admin/elevated privileges to run.
> The alerts are only shown if 'Do not show privilege elevation alerts' is disabled in 'Settings' > 'Containment' > 'Containment Settings'.
> See **Containment Settings** for more details.

- **Parent Process** - The program which spawned the contained process.
    - Click the name of the parent process to view the hierarchical order of processes
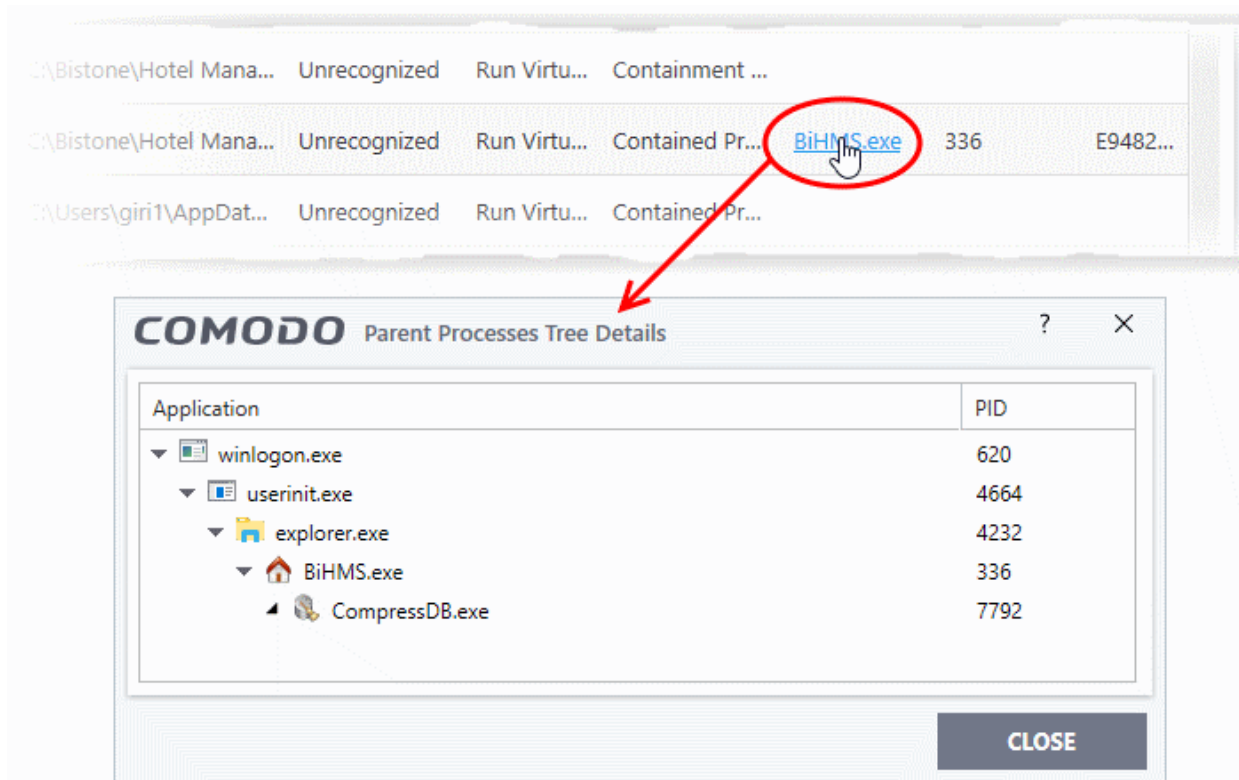
- **Parent Process ID** - The unique identifier that points to the process
- **Parent process hash** - The SHA1 hash value of the program which spawned the contained process.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.6. Website Filtering Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

    OR

- Click 'Logs' in advanced view of the CIS home screen
- Select 'Website Filtering Events' from the drop-down at upper-left

Website filter logs are a record of all sites blocked (or allowed) by CIS. The logs record all attempts made by users to

access blocked or allowed websites.

Background Note:
- You can create filtering rules for specific users in 'Advanced Settings' > 'Website Filtering'.
- See '**Website Filtering**', for more details.
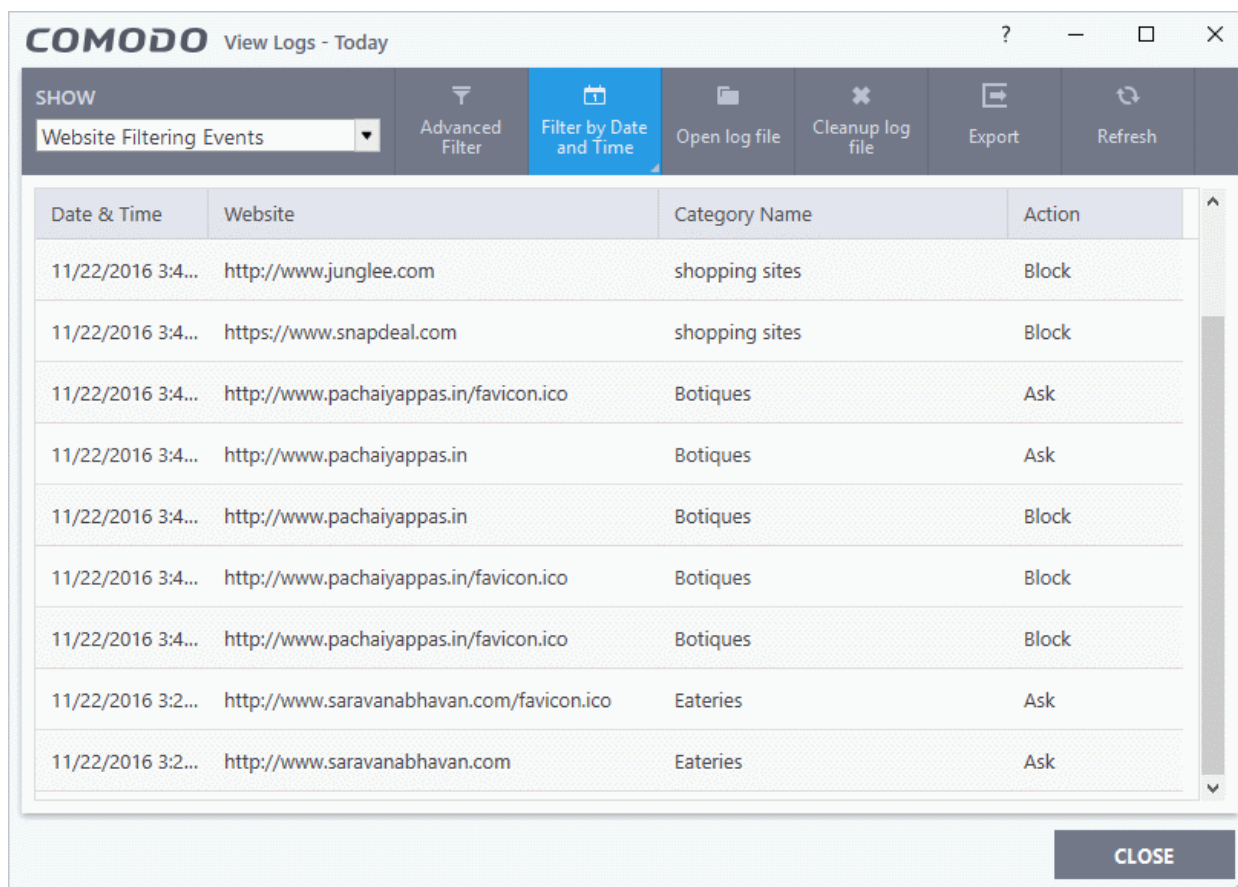
- **Date & Time** - When the event occurred.

- **Website** - The URL of the site that was blocked, or allowed.

- **Category** - The genre of the website. Example categories include 'Shopping sites', 'Social Media', 'Boutiques' etc. You can manage categories in 'Advanced Settings' > 'Website Filtering'.

- **Action** - How the filter reacted to the connection attempt. For example, whether the attempt was allowed, blocked or an alert shown to the user.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.7. Device Control Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR
- Click 'Logs' in advanced view of the CIS home screen

- Select 'Device Control Events' from the drop-down at upper-left

Device control logs record events related to external devices. External devices include USB, optical, and storage drives plugged into your computer.

Events logged include:

- Files copied, deleted and moved
- Device enabled/disabled ('Log detected devices' must be enabled)

See '**Advanced Settings > Device Control Settings**' for more help to configure device control.

- **Date** - When the event occurred.
- **Name** - The type of device associated with the event.
- **Identifier** - The identification string of the device
- **Class** - The GUID (Globally Unique Identifier) string of the category of the device as defined by the Windows operating system.
- **State** - Whether the device was allowed or blocked.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order

5.5.8. Autorun Event Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR
- Click 'Logs' in advanced view of the CIS home screen
- Select 'Autorun Events' from the drop-down at upper-left.

Autorun logs show events where changes were attempted on Windows services, auto-start entries and scheduled tasks.

Background:
- CIS monitors changes to registry items related to Windows Services, Autorun entries and scheduled tasks.
- You can define the response CIS should take against unrecognized autoruns in 'Advanced Settings' >

'Advanced Protection' > 'Miscellaneous'. See **Miscellaneous Settings** for more details.

- You can also define the response to unknown autoruns found by an antivirus scan. See **configure scan options** for more help with this.

- **Date & Time** - When the event occurred.
- **Type** - Whether the detected item is an autorun entry, Windows service, or scheduled task.
- **Location** - The installation path of the affected item, or the location of the new item
- **Modifier** - The location of the application that made the change.
- **Action** - How CIS responded to the event.

Status - Whether the action taken was a success or failure

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order.

5.5.9. Alerts Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen


- Select 'Alerts' from the drop-down at upper-left

Alert logs are a record of all threat notifications generated by CIS, and also record the user's response to the alert.

- **Date & Time** - When the event occurred.
- **Alert Type** - The security module that generated the alert. Alert types include antivirus, firewall, HIPS, containment, VirusScope and secure shopping.
- **Description** - Name of the file or event that caused the alert.
- **Advice** -The recommendation, or informational text in the alert. This text is intended to help users decide to respond to the threat.
- **Answered** - Whether or not the alert was answered by the user. You will see the date and time of the response if an answer was provided.
- **Answer** - The user's response to the alert. For example, 'Allow', 'Block', 'Disinfect', 'Skip'.
- **Option** - Additional settings chosen by the user at the alert. For example, 'Remember My Answer'.
- **Treat As** - Whether or not the user applied a specific ruleset to the file at the alert. The ruleset tells CIS the restriction level to apply to the file in future. Example rulesets include 'Treat as a safe application, or 'Treat as an installer'.

Event - Click 'Related Event' to view more details about the incident that triggered the alert.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

**Open log file** - Browse to and view a saved log file.

**Cleanup log file** - Delete the selected event log

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending / descending order.

5.5.10. CIS Tasks Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'Tasks' in the drop-down at upper-left

A task log is a record of a CIS operation such as a virus scan or database update. The task log area shows all tasks run, their completion status, and other details.

- **Date & Time** - When the event occurred.

- **Type** - The task that was performed. For example, 'Antivirus scan', or 'Database update'.

- **Parameter**:

    - The sub-type of the operation. For example, 'Quick Scan' is a sub-type of 'Antivirus scan'.
      OR

    - The target of the operation. For example, 'C:\Program Files' is the target area scanned.

- **Completed** - The time that the operation finished

- **Code** - Error code generated by Windows for CIS tasks that were not successful. No code is shown if the task finished successfully.

- **Info and additional info** - Shows further details about the task. For update tasks, these fields show the old and new version numbers. For scan tasks, they show the number of items scanned and the number of viruses found.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Refresh - Reload the current list and show the latest logs

Click any column header to sort the entries in ascending \ descending order.

5.5.11. File List Changes Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'File List Changes' in the drop-down at upper-left

The file list is an inventory of executables and applications on your computer. The list shows the file name, vendor, the date the file was discovered, and the file's trust rating.

- You can view the file list in CIS at 'Settings' > 'File Rating' > 'File List'. See **File List** for help on this area.

File list logs are a record of any modifications to these files. Logged actions include adding a new file, removing a file, or changing the trust rating of a file.

- **Date & Time** - When the event occurred.

- **Path** - The location of the file that was changed.

- **Modifier** - The service or user that made the change.

- **Action** - Whether the file was added, removed, or assigned a new rating

- **Property** - Whether the current trust rating was assigned by Comodo, an administrator, or a user.

- **Old Rating** - The trust rating of the file before the change.

  - The rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Under default settings, unrecognized files are run in the container until Comodo classifies them as 'Trusted' or 'Malicious'.

- **New Rating** - The trust rating of the file after the change.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.12.   Vendor List Changes Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

   OR

- Click 'Logs' in advanced view of the CIS home screen

- Select 'Vendor List Changes' in the drop-down at upper-left

CIS ships with a list of trusted vendors who have a reputation of creating legitimate, safe software. CIS allows unknown files which are digitally signed by one of these trusted vendors to run. Click 'Settings' > 'File Rating' > 'Vendor List' to view the list.

- You can also add new vendors, and change the rating of existing vendors. Admin / User ratings supersede the Comodo rating.

- The files published by these vendors are rated depending on the current rating assigned to the vendor

- Any changes to vendors in the list are logged in 'Vendor List Changes'.

- **Date & Time** - When the change event occurred.
- **Vendor** - The name of the software publisher
- **Modifier** - Who made the change (User or Comodo).

- **Action** - Whether the vendor was added, removed, or assigned a new rating
- **Property** - Whether the current rating was assigned by Comodo, an admin, or a user.
- **Old Rating** - The trust rating of the vendor before the change.
    - The rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Under default settings, unrecognized files are run in the container until Comodo classifies them as 'Trusted' or 'Malicious'.
- **New Rating** - The trust rating of the vendor after the change.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.13.   Trusted Certificate Authority Change Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

  OR

- Click 'Logs' in advanced view of the CIS home screen
- Select 'Trusted Certificate Authorities Changes' from the drop-down at upper-left.

Root certificates are a critical part of online security. Your internet browser relies on them to verify that you are connected to the site you think you are connected to.

If a fake root certificate was to find its way into your browser's trusted certificate store (TCS), then you could be tricked into connecting to a fraudulent server instead of the site you intended.

Comodo Internet Security checks the trust rating of all root certificates in your browser's TCS to ensure they are legitimate. It runs this check during the following scans:

- **Rating scan** - Click 'Scan' > 'Rating Scan'
- **Full scan** - Click 'Scan' > 'Full Scan'
- **Custom scan profiles that include the certificate store**. Click 'Scan' > 'Custom Scan' > 'More Scan Options'
- Unrecognized and self-signed certificates are marked as 'Untrusted'.
- You can choose to trust the certificate or remove it. An example is shown below:
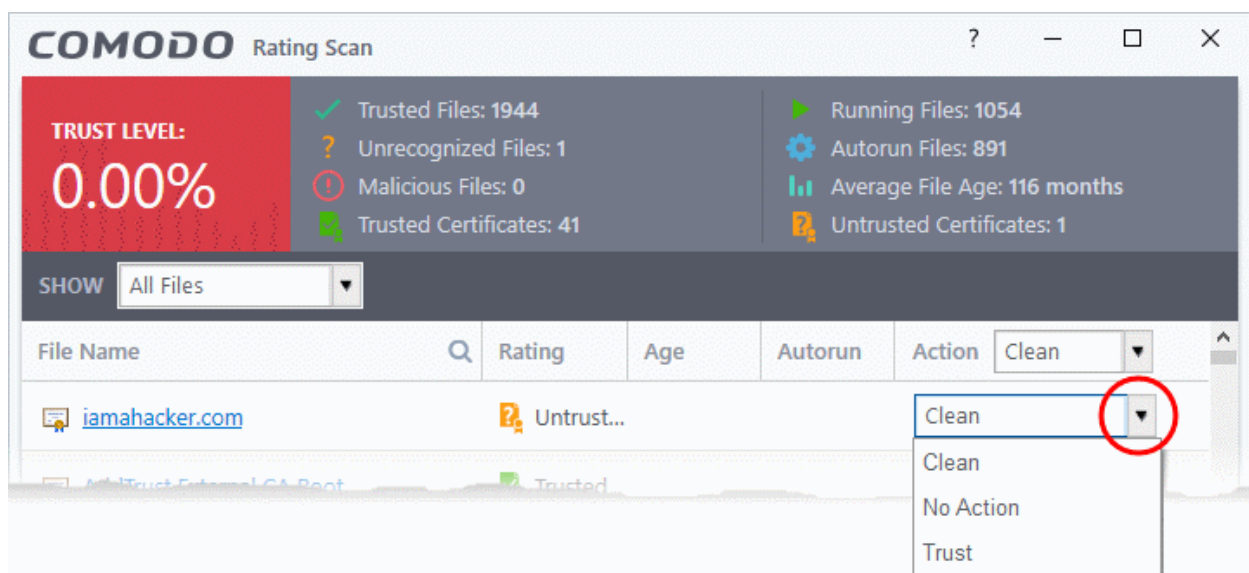
- **Clean** - Removes the certificate from the store

- **Trust** - Assigns 'Trusted' status to the certificate. The certificate is excluded from future scans.
- **No Action** - The certificate keeps its untrusted status, but is not deleted.
- Any changes to the certificate store are logged in 'Trusted Certificate Authorities Changes'.

Background:

- There are two types of certificate involved when you connect to a secure website:

  1. **Website SSL certificate** - These certificates are hosted on the website you connect to. They are used to encrypt the connection between your browser and the site. This is especially important for sensitive transactions like online payments, where you send your credit card information over the internet.
- **Root certificate** - These certificates are embedded into your browser (Chrome, Firefox etc). They are used to validate that the website's SSL certificate (above) is genuine - that it has been issued by a trusted certificate authority.

- You can tell a site is using an SSL certificate by the padlock icon in the browser address bar. You will also notice that the website address begins with https:// (the 's' stands for 'secure').

- Website SSL certificates are issued to site owners by an organization known as a 'Certificate Authority' (CA). The CA checks that the website owner is a legitimate business before they will issue a certificate to them.

- When you connect, your browser checks that the SSL certificate on a site is signed by root certificate from a trusted CA.

- If a fake root certificate got embedded into your browser, it could tell you trust a website run by a hacker.

- CIS detects whether you have any fake root certificates in your browser when you run a rating scan, a full scan, or a custom scan (if so configured).

- **Date & Time** - When the change event occurred.
- **Trusted Certificate Authorities** - The name of the CA who issued the untrusted certificate
- **Action** - Whether the user chose to trust, remove or ignore the certificate

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.14.   Configuration Change Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

    OR

- Click 'Logs' in advanced view of the CIS home screen
- Select 'Configuration Changes' in the drop-down at upper-left

Configuration change logs are a record of changes to CIS settings.

- **Date & Time** - When the configuration change was done.
- **Component** - The CIS interface that was modified.
- **Action** - Short description of the change made to the CIS component. For example, if a setting was changed, or an exclusion was created.
- **Modifier** - The service or user that made the change. Possible modifiers include 'User', 'Antivirus Alert',

'Auto-Learn', 'Firewall Alert', 'HIPS Alert', 'Containment Alert', 'Scheduler' and 'Comodo'.

- **Name** - The item featured in the modification. This will vary depending on the component.
- **Old Setting** - The value before the configuration change.
- **New Setting** - The value after the configuration change.
    - Place your mouse over an entry in the 'Old Value' or 'New Value' column to view the full setting string

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.15.   Secure Shopping Activity Logs

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

    OR

- Click 'Logs' in advanced view of the CIS home screen
- Select 'Secure Shopping Events' from the drop-down at upper-left

Secure Shopping creates a highly secure environment for sensitive online activities such as internet banking and shopping.

- Click 'Settings' > 'Advanced Protection' > 'Secure Shopping' to add websites that should always open inside the Secure Shopping environment.
- CIS will then remind you if you try to visit the website in a normal browser, and will offer to open it in Secure Shopping instead. See '**Comodo Secure Shopping**' for more on the feature.
- Secure shopping logs are a record of when the user was prompted to use secure shopping, and the actions taken.
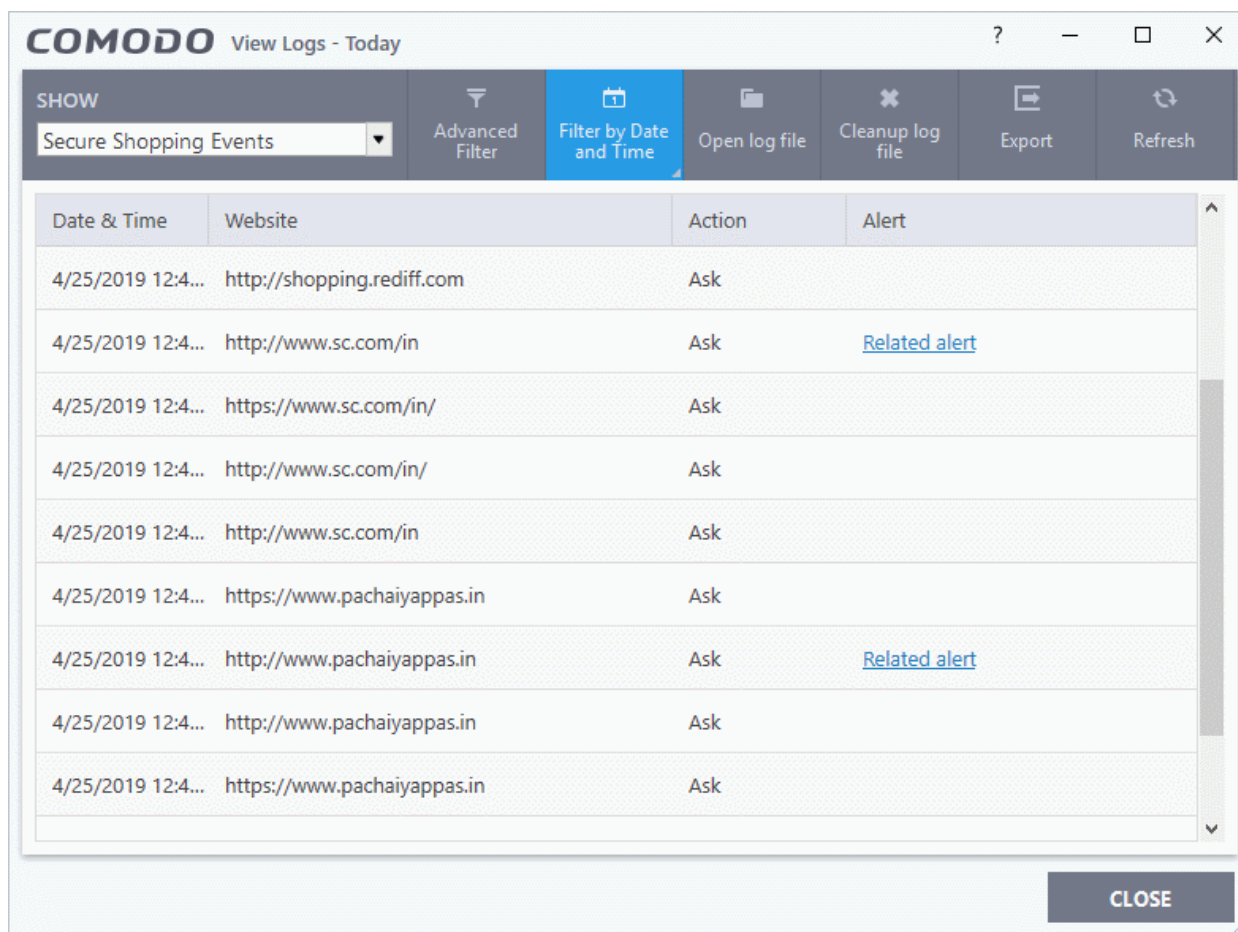
- **Date & Time** - When the event occurred.
- **Website** - The URL of the web-page visited.
- **Action** - States whether an alert is shown if the user connects to the site with a normal browser. 'Ask' = 'Yes, an alert is shown'.
- **Alert** - Click 'Related Alert' to view the notification generated by the event.

Export - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.

Open log file - Browse to and view a saved log file.

Cleanup log file - Delete the selected event log.

Refresh - Reload the current list and show the latest logs.

Click any column header to sort the entries in ascending \ descending order.

5.5.16. Search and Filter Logs

You can run a simple filter of events by date, and use advanced filters to conduct more complex searches.

- **Filter by date/time**
- **Advanced Filters**

Filter by date/time

- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'

    OR

- Click 'Logs' in advanced view of the CIS home screen

- Select an event category from the drop-down at top-left
- Click 'Filter by Date and Time' to choose a specific period:
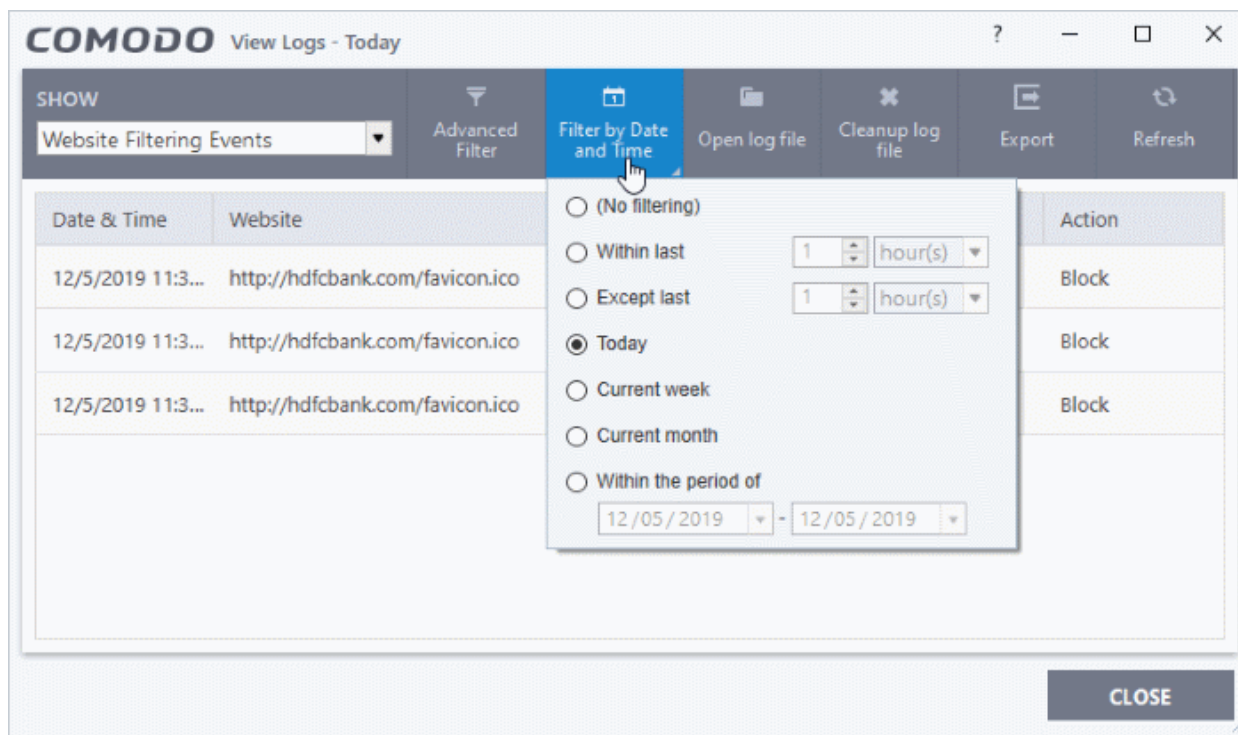
- **No filtering** - Show every event logged since CIS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Show all events logged today, from 12:00 am to the current time. *(Default)*
- **Current Week** - Show all events logged from the previous Sunday to today.
- **Current Month** - Display all events logged from 1st of the current month to today.
- **Within the period of** - Show logs between a custom date range.

You can also right-click inside the log viewer module and choose the time period.
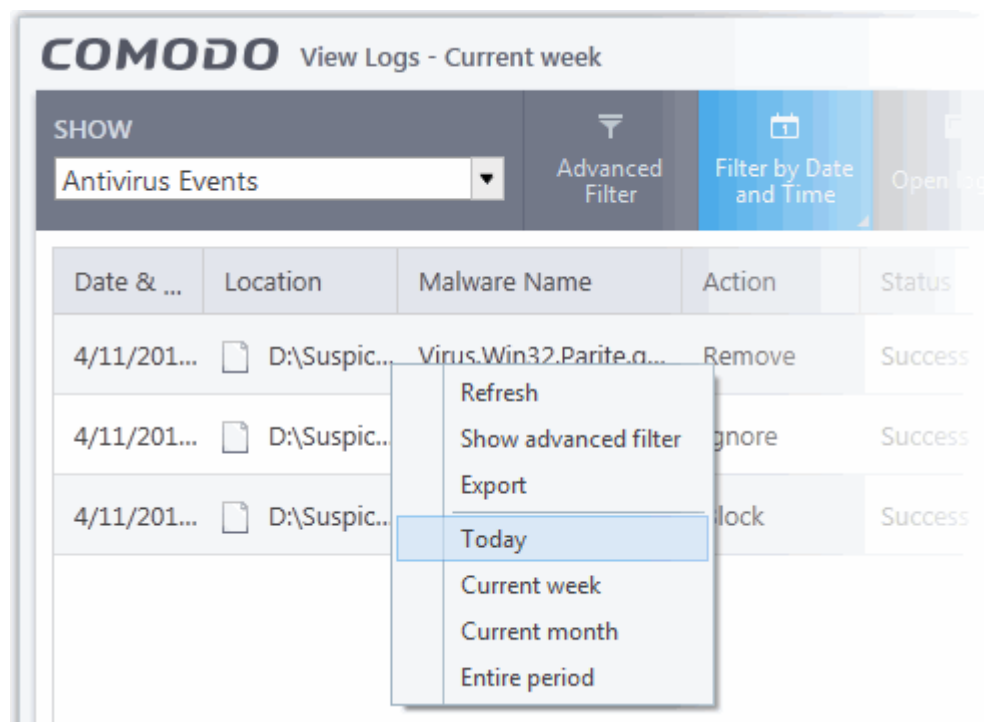
Advanced Filters

Advanced filters let you run complex queries based on a variety of criteria. Search parameters vary from module to module.

- Click 'Logs' in the CIS menu bar
- Select a module in the drop-down on the left
- Click 'Advanced Filter':
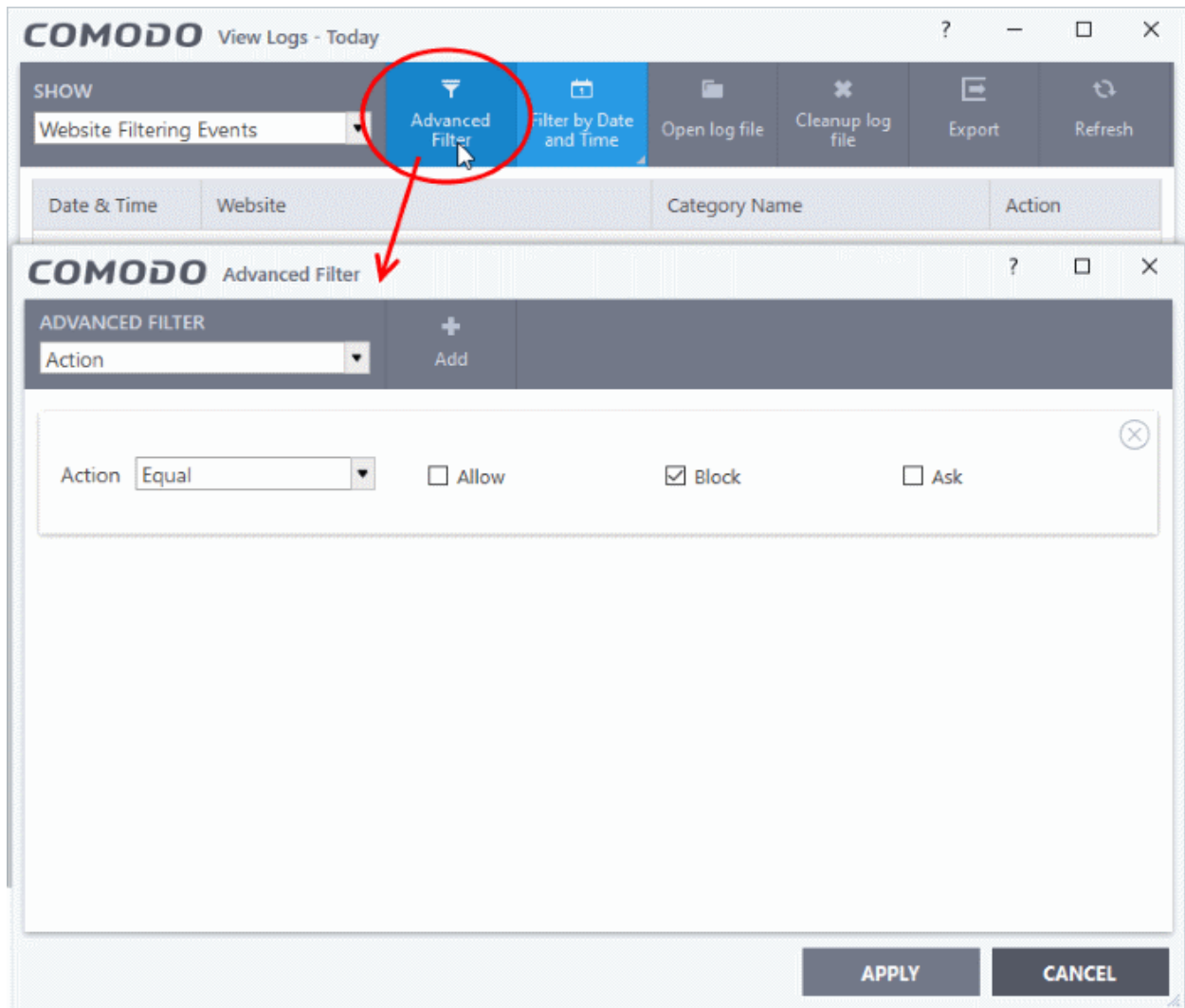
- Select a filter category at top-left then click 'Add'
- Search parameters vary according to the filter category. You can include multiple filter categories to refine your search.

Click the following links to view the options available with each module:

- **Antivirus Events**
- **VirusScope Events**
- **Firewall Events**
- **HIPS Events**
- **Containment Events**
- **Website Filtering Events**
- **Device Control Events**
- **Autorun Events**
- **Alerts**
- **CIS Tasks**
- **File List Changes**
- **Vendor List Changes**
- **Trusted Certificate Authority Change**
- **Configuration Changes**

- **Secure Shopping Events**

Antivirus Events

Filter Category	Description	Parameters
Action	Filter logs based on the action taken by CIS against the detected threat. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • Quarantine: Shows events at which the user chose to quarantine a file • Remove: Shows events at which the user chose to delete the detected threat • Ignore: Shows events at which the user chose to ignore the detected threat • Detect: Shows 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: Shows events at which quarantined applications were restored to original location by admin from Endpoint Manager • Block: Shows events where suspicious applications were stopped • Reverse: Shows events where VirusScope overrode potentially malicious actions • False positive: Shows events where files flagged as threats by CIS were submitted to Comodo by the user as a false positive. • Add To exclusions: Shows events in which the user chose to add an item to antivirus exclusions • Add To trusted files: Shows events in which the user changed the file rating to 'Trusted' • Restore from Quarantine: Shows events in which files were returned to original location from quarantine • Delete from Quarantine: Shows events in which files were removed permanently from quarantine
Location	Filter the log entries related to events logged from a specific location.	• 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 are displayed.
Malware Name	Filter the log entries related to specific malware.	• 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 are shown.
Status	Filter the log entries based on the success or failure of the action taken against the threat	Select the filter parameter: • Success: Shows events in which the actions against the detected threat were successfully

	by CIS. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	executed (for example, the malware was successfully quarantined) • Failure: Shows events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected)

VirusScope Events

Filter Category	Description	Parameters
Action	Filter logs based on the action taken by CIS against the detected threat.	Select the filter parameter: • Quarantine: Shows events at which the user chose to quarantine a file • Remove: Shows events at which the user chose to delete the detected threat • Ignore: Shows events at which the user chose to ignore the detected threat • Detect: Shows 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: Shows events at which quarantined applications were restored to original location by admin from Endpoint Manager • Block: Shows events where suspicious applications were stopped • Reverse: Shows events where VirusScope overrode potentially malicious actions • Add To trusted files: Shows events in which the user changed the file rating to 'Trusted' • Restore from Quarantine: Shows events in which files were returned to original location from quarantine • Delete from Quarantine: Shows events in which files were removed permanently from quarantine
Location	Filter the log entries related to events logged from a specific location.	• 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 are displayed.
Malware Name	Filter the log entries related to specific malware.	• 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 are shown.
Status	Filter the log entries based on the success or failure of the	Select the filter parameter:

| | action taken against the threat by CIS.

Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice | • Success: Shows events in which the actions against the detected threat were successfully executed (for example, the malware was successfully quarantined)

• Failure: Shows events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected) |
|---|---|---|

Firewall Events

Filter Category	Description	Parameters
Action	Filter logs based on events according to the response (or action taken) by the firewall. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • Blocked: Shows events where CIS prevented the connection • Allowed: Shows events where the connection was allowed to proceed • Asked: Shows events where an alert was shown to the users so they could choose whether or not to allow the connection
Application	Filter logs based on events propagated by a specific application	• 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 FW events containing the entry 'cuckoo' in the 'Application' column are displayed
Destination IP	Filter logs based on events with a specific target IP address 1. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice. 2. Select 'IPv4' or 'IPv6' from the drop-down box.	• 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.
Destination Port	Filter logs based on events that involved a specific target port number Select any one of the option the drop-down: • Equal • Greater than • Greater than or Equal • Less than • Less than or Equal	• 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.

Filter Category	Description	Parameters
	• Not Equal	
Direction	Filter logs based on events of inbound or outbound nature. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • In: Shows a list of events involving inbound connection attempts • Out: Shows 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.
Protocol	Filter logs based on events that involved a specific protocol. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • 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.
Source IP	Filter logs based on events that originated from a specific IP address 1. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice. 2. Select 'IPv4' or 'IPv6' from the drop-down box.	• 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.
Source Port	Filter logs based on events that involved a specific source port number Select any one of the option the drop-down: • Equal • Greater than • Greater than or Equal • Less than	• 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.

Filter Category	Description	Parameters
	• Less than or Equal • Not Equal	

HIPS Events

Filter Category	Description	Parameters
Application	Filter logs based on events propagated by a specific application	• 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 are displayed.
Action	Filter logs based on events according to the response (or action taken) by HIPS Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • 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 are displayed.
Target	Filter logs based on events that involved a specified target application.	• 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.

Containment Events

Filter Category	Description	Parameters
Application	Show events propagated by a specific application.	• 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 are displayed.
Rating	Show events which concern files that have a specific trust-rating. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • 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' are displayed.
Action	Show events where a specific action was applied to the file by CIS Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the restriction level(s) applied by the container to the applications, either automatically of or chosen by the user from the alert. • 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 are displayed.
Contained by	Show events where the file was isolated by a specific module or user Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.	Select the source(s) by which the applications were contained. • 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 are displayed.
Parent Process Path	Show files contained based on its source process path. Select 'Contains' or 'Does Not Contain' from the drop-down menu.	• Enter the name of the application associated with the process path, that launched contained item as the search criteria for filtering the logs in the text field. For example, if you choose 'Contains' and enter the phrase 'RuntimeBroker.exe' in the text field, then all events containing the entry 'RuntimeBroker.exe' in the 'Parent Process path' column are displayed.

Filter Category	Description	Parameters
Parent Process Hash	Show events where items was contained based on its source process(es) specified by hash value(s) of executable file(s) associated with the source process(es) Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	• Enter the SHA1 hash value of the executable file associated with the process, that launched contained item as the search criteria.

Website Filtering Events

Filter Category	Description	Parameters
Website	Show only events that involved a specific website Select 'Contains' or 'Does Not Contain' from the drop-down menu.	• Enter the website address in part or full, to filter the logs involving the website. For example, if you choose 'Contains' 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 are displayed.
Category Name	Show events that involved websites which are covered by a website filtering category.	• Enter the website filter category name, to filter the logs involving the category 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 are displayed.
Action	Show only events that involved a specific response by CIS. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the action(s) to filter the logs involving those action(s). • Allow • Block • Ask For example, if you choose 'Equal' and 'Block', then only events where websites blocked are displayed.

Device Control Events

Filter Category	Description	Parameters
Name	Filter the entries based on the type of the device.	• Enter the type of the device in full or part as your filter criteria in the text field. For example, if you choose 'Contains' and type 'USB Input Device' in the text field, you will see logs related to USB input devices like keyboards, mice and finger print scanners.
Identifier	Filter entries based on the device ID of the external device.	• Enter the device ID of the device in full or part as your filter criteria in the text field. For example if you have chosen 'Contains' and entered 'USB\VID_0627&PID_0001', in the text field only those log entries related to external devices whose device ID contains the string are displayed.
Class	Filter the entries based on the	• Enter a Device Class ID (GUID) in part or full as

Filter Category	Description	Parameters
	GUID of the device	your search criteria
		For example, if you select 'Contains' option from the drop-down field and enter '4D36E967', then all events containing the entry '4D36E967' in the 'Class' field are displayed..
State	Filter events based on whether the device connection attempt was allowed or blocked.	Select the parameter to refine your search. • Enabled • Disabled

Autorun Events

Filter Category	Description	Parameters
Type	Filter entries based on the class of autorun Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Choose from: • Windows service • Autostart entry • Scheduled task
Location	Filter entries based on application path Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.	• 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 are displayed.
Modifier	Filter logs by the file or user that launched the event. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the location or a part of it as your filter criteria in the text field. For example if you choose 'Contains' and enter 'C:/Users/tester/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/UnknownAppUI3.exe' in the text field, then only log entries with the same value in the 'Path' column will be displayed.
Action	Filter the events based on CIS response to the detected threat Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	• Ignore - CIS does not take any action • Terminate - CIS stops the process / service • Terminate and Disable - Auto-run processes will be stopped and the corresponding auto-run entry removed. In the case of a service, CIS disables the service. • Quarantine and Disable - Auto-run processes will be quarantined and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.
Detected By	Filter the entries based on the CIS component that discovered the threat Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the specific filter parameter to refine your search. • Autorun monitor • Antivirus Scan

Filter Category	Description	Parameters
Status	Filter the entries based on the success or failure of the action taken against the threat by CIS. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the specific filter parameter to refine your search. • Success: Shows events where the actions against the detected threat were successful. For example, the malware was successfully quarantined. • Failure: Shows events where the intended actions against the detected threat were not successful. For example, the malware was not disinfected.

Alerts

Filter Category	Description	Parameters
Advice	Filter entries by the security recommendation in the alert. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the text or word as your filter criteria. For example, choose 'Contains' and enter the phrase 'you can safely allow this request' in the text field.
Answer	Filter the events based on what action the user selected at the alert. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the parameter to refine your search. • Show • 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

Filter Category	Description	Parameters
		• 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' are displayed.
Answered	Filter logs based on the date the user answered the alerts. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Enter or select the required date from the date picker For example, if you select 'Equal' and select '12/09/2019', only alerts answered on '12/09/2019' are displayed.
Description	Filter the entries based on the description of the attempt displayed in the alert. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• 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 that contain the phrase 'connect to the internet' in the description are displayed.
Option	Filter the log entries where the user selected an additional options like 'Remember my answer', 'Submit as False Positive' from the alert. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the specific filter parameters to refine your search. • 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 are displayed.
Treat as	Filter events where the user chose specific actions on the alert. For example, 'treat as a safe application', 'treat as an installer' and so on. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• 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 are displayed.
Alert Type	Filter the log entries based on the CIS component that triggered the alert Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the specific filter parameters to refine your search. • Antivirus Alert • Firewall Alert • HIPS alert • Containment alert • VirusScope Alert

Filter Category	Description	Parameters
		• Secure Shopping Alert
		• Pre-Expiration Alert
		• Expiration Alert
		• Browser Protection Alert
		• Network alert
		• Auto-Scan alert
		For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of antivirus alerts are displayed.

CIS Tasks

Filter Category	Description	Parameters
Code	Filter the entries based on specified error code Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• 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 are displayed.
Completed	Filter events based on tasks successfully finished on the specified date Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Enter or select the required date from the date picker For example, if you choose 'Equal' and select '08/01/2019', only the logs of tasks completed on 08/01/2019' are displayed.
Parameter	Filter the entries based on the specified 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'. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the text or word as your filter criteria. For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Quick Scan' in the text field, then only the entries of 'Antivirus Scan Tasks' with the scan parameter 'Quick Scan' are displayed.
Type	Filter the entries based on the CIS tasks category. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the specific filter parameters to refine your search. • Antivirus update • Antivirus scan • Log Clearing • Warranty Activation • Product upgrade • Binary update • File Rating DB Upgrade

Filter Category	Description	Parameters
		• Purge file list

File List Changes

Filter Category	Description	Parameters
Location	Filter the entries based on the file path whose trust rating was changed Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• 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 are displayed.
Modifier	Filter events based on who changed the file rating Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the filter parameter to refine your search • User • Comodo For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs of changes done by the users are displayed.
Action	Filter the entries based on the file activity Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the filter parameter to refine your search • Added • Changed • Removed For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only the logs of files that were removed from the file list are displayed.
Property	Filter the entries by who provided the file rating. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Ratings can be provided by: • 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 users are displayed.
Old Rating	Filter the entries based on trust rating of files before the change Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Select the filter parameter to refine your search • 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' in the 'Old Rating' column are displayed.
New Rating	Filter logs by the trust rating of	Select the filter parameter to refine your search

Filter Category	Description	Parameters
	files after the change Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Unrecognized • Trusted • Malicious For example, if you select 'Contains' from the drop-down and select 'Malicious' checkbox, only the logs of files that are rated as 'Malicious' in the 'New Rating' column are displayed.

Vendor List Changes

Filter Category	Description	Parameters
Vendor	Filter logs by the software publisher name whose trust rating was changed Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Type the name of the vendor in full or part in the text field. For example if you choose 'Contains' and enter 'Digital' in the text field, only those log entries related to the vendors who has contain 'Digital' as a part in their name are displayed.
Modifier	Filter logs by who changed the vendor rating Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the filter parameter to refine your search • User • Comodo For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs of changes done by the users are displayed.
Action	Filter logs by the type of change made to the vendor list. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Possible actions: • Added • Changed • Removed For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only the logs of vendors that were removed from the vendor list are displayed.
Property	Filter logs by the entity that provided the vendor rating Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Entities that can provide trust ratings: • 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 vendors that were rated by users are displayed.
Old Rating	Filter logs by the trust rating of the vendor before the change Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not	Select the filter parameter to refine your search • Unrecognized • Trusted • Malicious

Filter Category	Description	Parameters
	Contain' inverts your choice.	For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of vendors that are rated as 'Unrecognized' in the 'Old Rating' column are displayed.
New Rating	Filter logs by the vendor's trust rating after the change. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Possible new trust ratings are: • Unrecognized • Trusted • Malicious For example, if you select 'Contains' from the drop-down and select 'Malicious' checkbox, only the logs of vendors that are rated as 'Malicious' in the 'New Rating' column are displayed.

Trusted Certificate Authorities

Filter Category	Description	Parameters
Vendor	Filter logs by the software publisher name whose trust rating was changed. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Type the name of the vendor in full or part in the text field. For example if you choose 'Contains' and enter 'Digital' in the text field, only those log entries related to the vendors who has contain 'Digital' as a part in their name are displayed.
Modifier	Filter logs by who changed the trusted certificate authorities rating Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the filter parameter to refine your search. • User • Comodo For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs of changes done by the users are displayed.
Action	Filter logs by the type of change made to the trusted certificate authorities list. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Possible actions: • Added • Changed • Removed For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only the logs of trusted certificate authorities that were removed from the vendor list are displayed.
Property	Filter logs by the entity that provided the trusted certificate authorities rating Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Entities that can provide trust ratings: • 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 trusted

Filter Category	Description	Parameters
		certificate authorities that were rated by users are displayed.
Old Rating	Filter logs by the trust rating of the trusted certificate authorities before the change. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Select the filter parameter to refine your search. • Unrecognized • Trusted • Malicious For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of trusted certificate authorities that are rated as 'Unrecognized' in the 'Old Rating' column are displayed.
New Rating	Filter logs by the trusted certificate authorities's trust rating after the change. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Possible new trust ratings are: • Unrecognized • Trusted • Malicious For example, if you select 'Contains' from the drop-down and select 'Malicious' checkbox, only the logs of trusted certificate authorities that are rated as 'Malicious' in the 'New Rating' column are displayed.

Configuration Changes

Filter Category	Description	Parameters
Action	Filter logs by the type of change that was made. For example, rule modified, file exclusion created. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Options are: • Added • Changed • Removed • Option changed
Modifier	Filter events based on who changed the configuration such as the user, administrator and response given to an alert Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	The possible modifiers are: • User • Auto learn • Antivirus Alert • Firewall Alert • HIPS alert • Containment alert • Scheduler • Comodo For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs of changes done by the users are displayed.
Name	Filter the entries based on object label that was affected by the configuration change,	Enter the object name as filter criteria in the text box. For example, if you choose 'Contains' then enter the phrase

Filter Category	Description	Parameters
	for example, Shared Spaces, Windows Management and so on. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	'surfer.exe' in the text field, then you will only see logs with surfer.exe in the name column.
Component	Filter logs by the object modified by the action. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the affected object. It is not possible to list all possible objects in this table. Please consult the list in the search interface.

Secure Shopping Events

Filter Category	Description	Parameters
Website	Show only events that involved a specific website. Select 'Contains' or 'Does Not Contain' from the drop-down menu.	• Enter the website address in part or full, to filter the logs involving the website. For example, if you choose 'Contains' option from the drop-down and enter the phrase 'sc.com' in the text field, then all events that involve the website 'sc.com' in the 'Website' column are displayed.
Action	Filter logs by the type of secure shopping event activity. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Possible activities: • Visit with Secure Browser • Visit in Secure Shopping Environments • Ask For example, if you select 'Equal' from the drop-down and select 'Visit with Secure Browser' checkbox, only the session initiated events are displayed in the 'Action' column.

5.6. Submit Files for Analysis to Comodo

Click 'Tasks' > 'Advanced Tasks' > 'Submit Files'

- Files you submit from this interface are uploaded to Comodo Valkyrie for behavior testing.
- Valkyrie is Comodo's file testing and verdict system. It's purpose is to discover whether or not a file is malicious or safe.
- CIS rates files as either 'trusted', 'malicious' or 'unknown'.
- Files with no rating at all are automatically uploaded when they are executed, or if they are discovered by a **rating scan**.
  - Files awarded an unknown rating by an admin, user, or by Comodo are not auto-uploaded.

Note: Unrecognized files can also be submitted from the '**File List**' interface should you prefer.

Upload files for analysis

- Click 'Tasks' on the CIS home screen
- Click 'Advanced Tasks' then 'Submit Files'
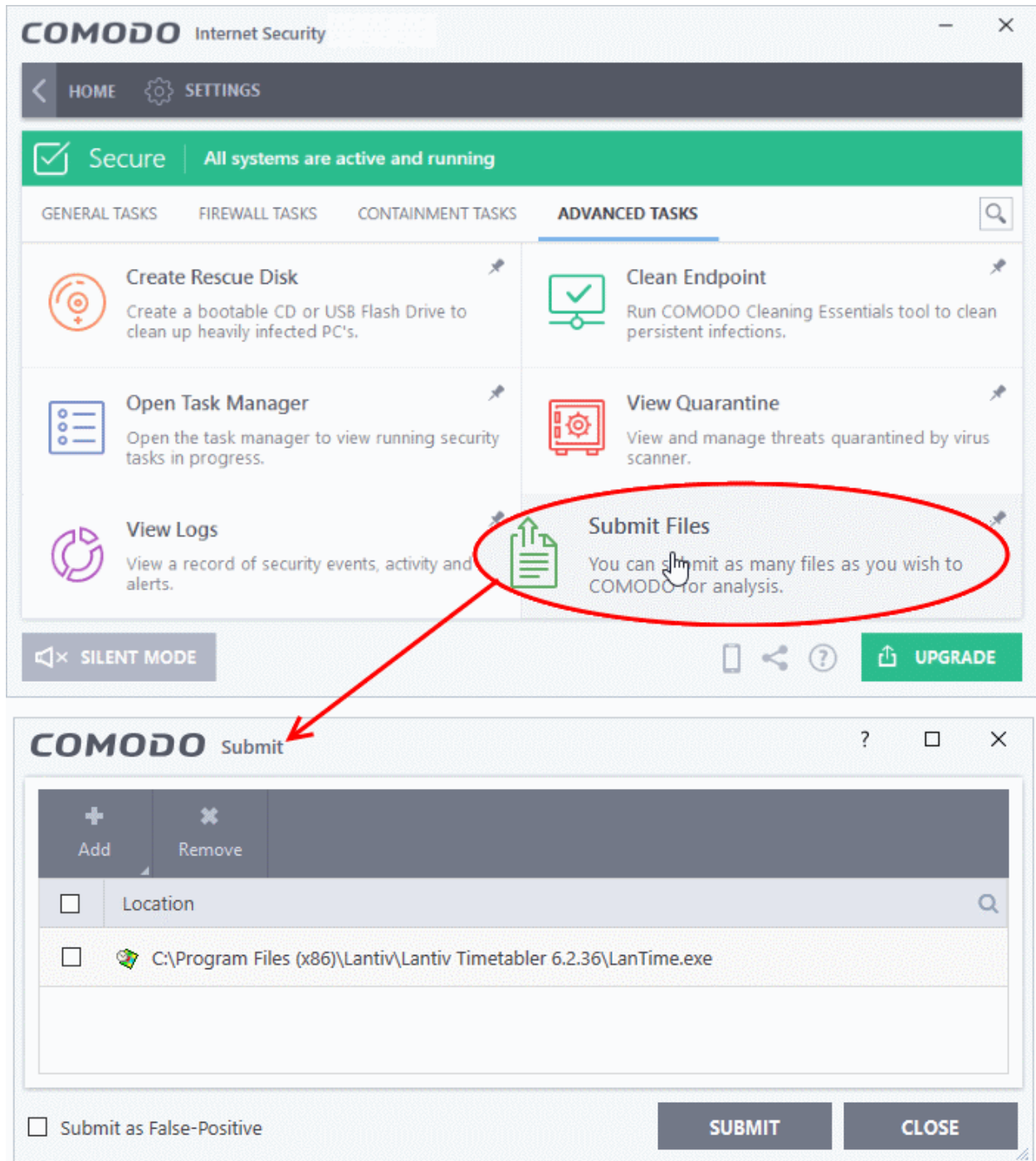
- Click 'Add' at top right.
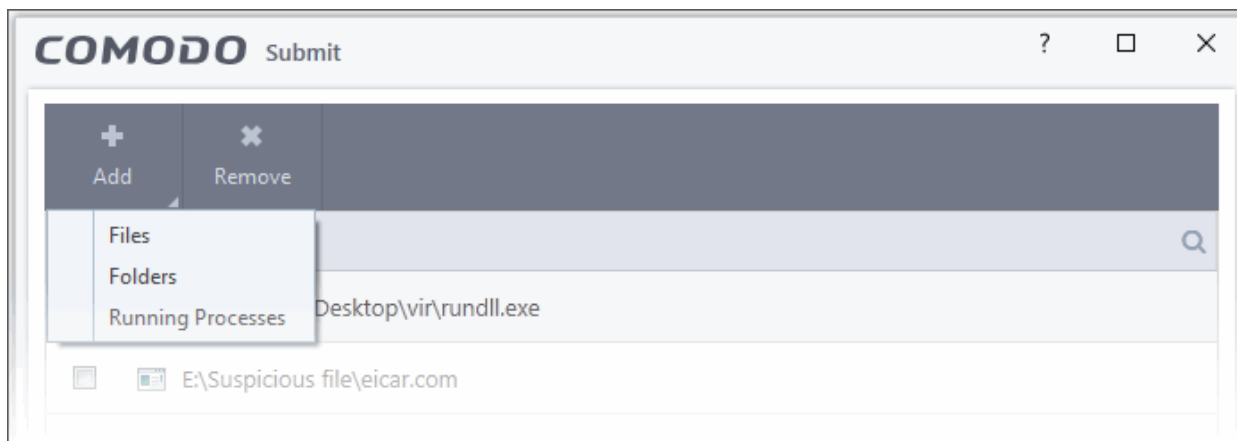
- There are three ways to select a file:

    - **Files** - Browse to the file or executable you want to add to the 'Submit Files' list.

    - **Folders** - Browse to the folder you want to add. All files in the folder will be added to the 'Submit Files' list.

    - **Running Processes** - Select a currently active process. The parent application of the process will be added to the 'Submit Files' list.

- Repeat the process to add more files

- Click the 'Submit' button

The uploading process will commence. You can stop, pause/resume or send the submission process to background by clicking respective buttons.
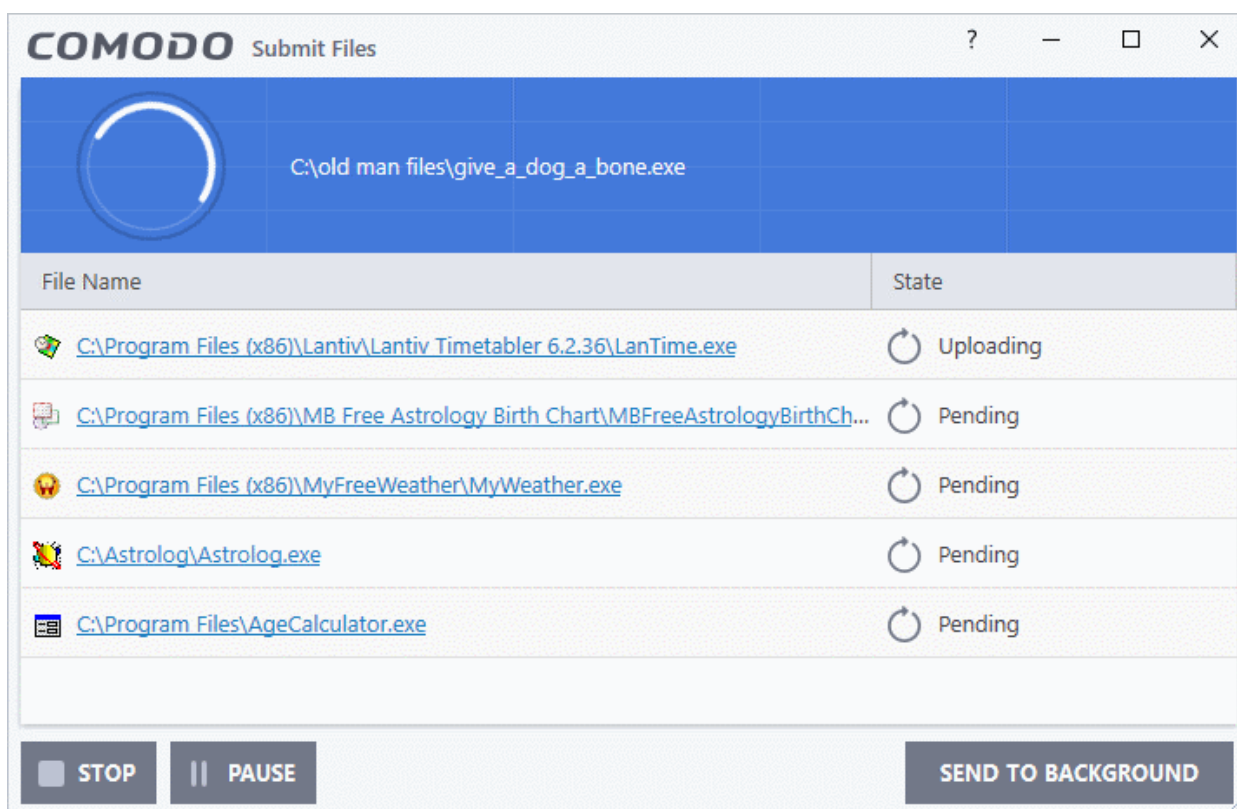
When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen shows the results:
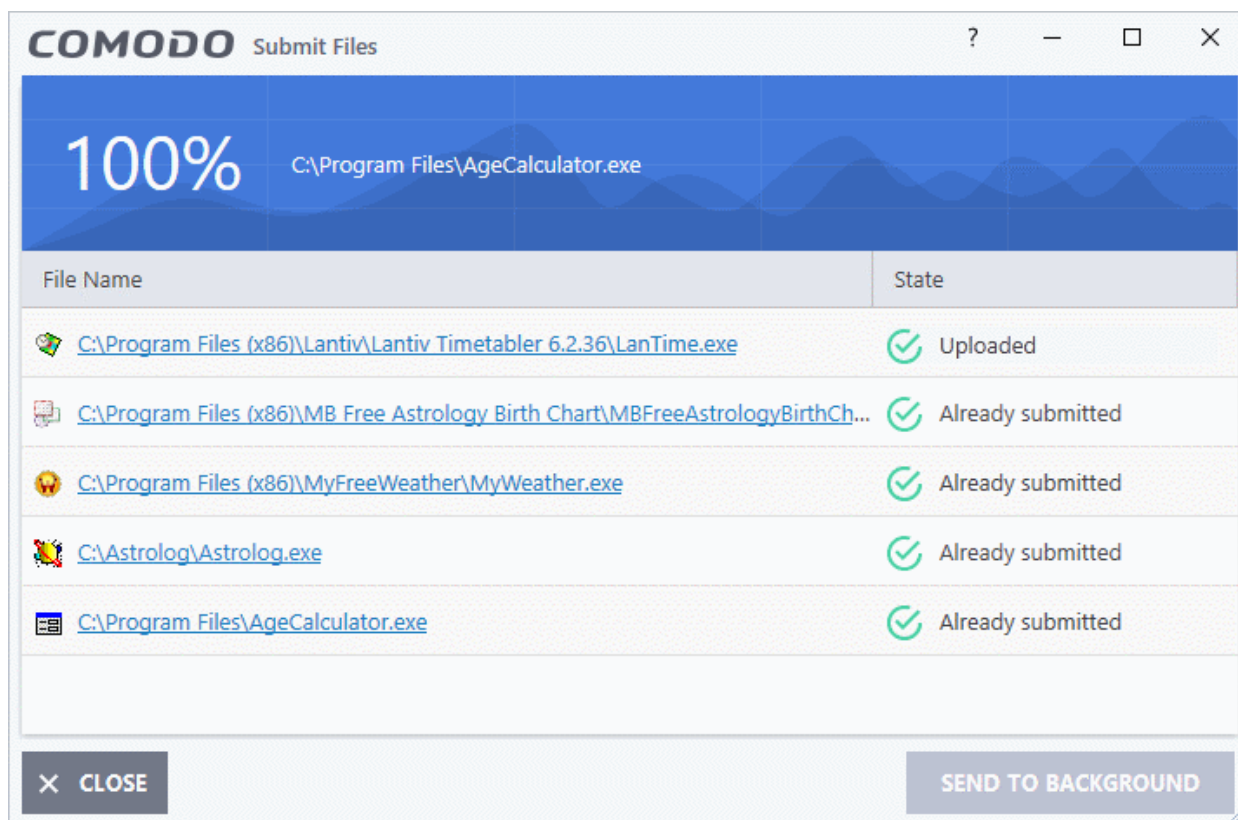
- • **Uploaded** - The file was accepted for review by our research labs. The file's signature was not among the list of files waiting to be tested.
- • **Already submitted** - The file has already been uploaded by another CIS user and is queued for testing. This means the file was not uploaded from your machine.

Comodo will analyze all submitted files. If the file is found to be trustworthy it will be added to the Comodo safe list (white-listed). Conversely, if it is found to be malicious then it will be added to the virus database (black-listed).

Click 'Settings' > 'File List' > 'Submitted Files' to view all files uploaded to our labs. See **Submitted Files** for more details.

6. CIS Settings

Click 'Settings' at the top-left of the CIS home screen

- • The settings area lets you configure every aspect of the operation, behavior and appearance of Comodo Internet Security.
- • **General settings** - Specify top-level preferences regarding the interface, updates and event logs.
- • **Security settings** - Configure each CIS security module. Modules include antivirus, firewall, file-rating, containment, Secure Shopping, and website filtering.
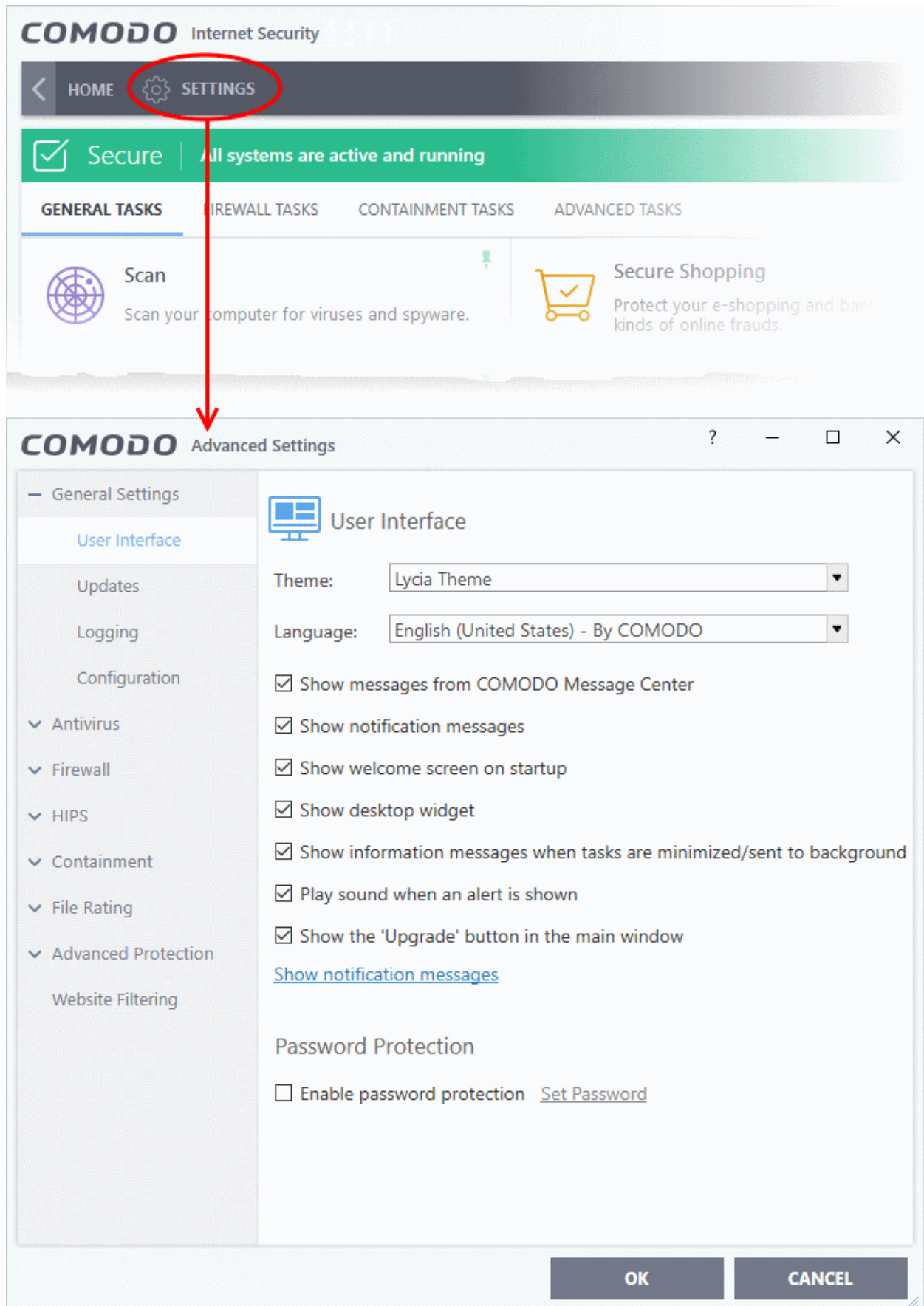
Click the following links for help with specific settings:

- **General Settings** - 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**
- **Firewall Settings**
  - **General Firewall Settings**
  - **Application Rules**
  - **Global Rules**
  - **Firewall Rule Sets**
  - **Network Zones**
  - **Port Sets**
- **HIPS Settings**
  - **General HIPS Settings**
  - **Active HIPS Rules**
  - **HIPS Rule Sets**
  - **Protected Objects**
  - **HIPS Groups**
- **Containment Configuration**
  - **Containment Settings**
  - **Auto-Containment Rules**
- **File Ratings**
  - **File Rating Settings**
  - **File Groups**
  - **File List**
  - **Submitted Files**
  - **Vendor List**
- **Advanced Protection**
  - **VirusScope Settings**
  - **Scan Exclusions**
  - **Device Control Settings**
  - **Script Analysis Settings**
  - **Miscellaneous Settings**
  - **Secure Shopping Settings**
- **Website Filtering Settings**

6.1. General Settings

Click 'Settings' > 'General Settings'

- The general settings area lets you customize the appearance and overall behavior of Comodo Internet Security.
- You can configure interface language, notification messages, automatic updates, logging, and more.

Configure General CIS Settings

- Click 'Settings' on the CIS home screen

- Click 'General Settings' on the left:
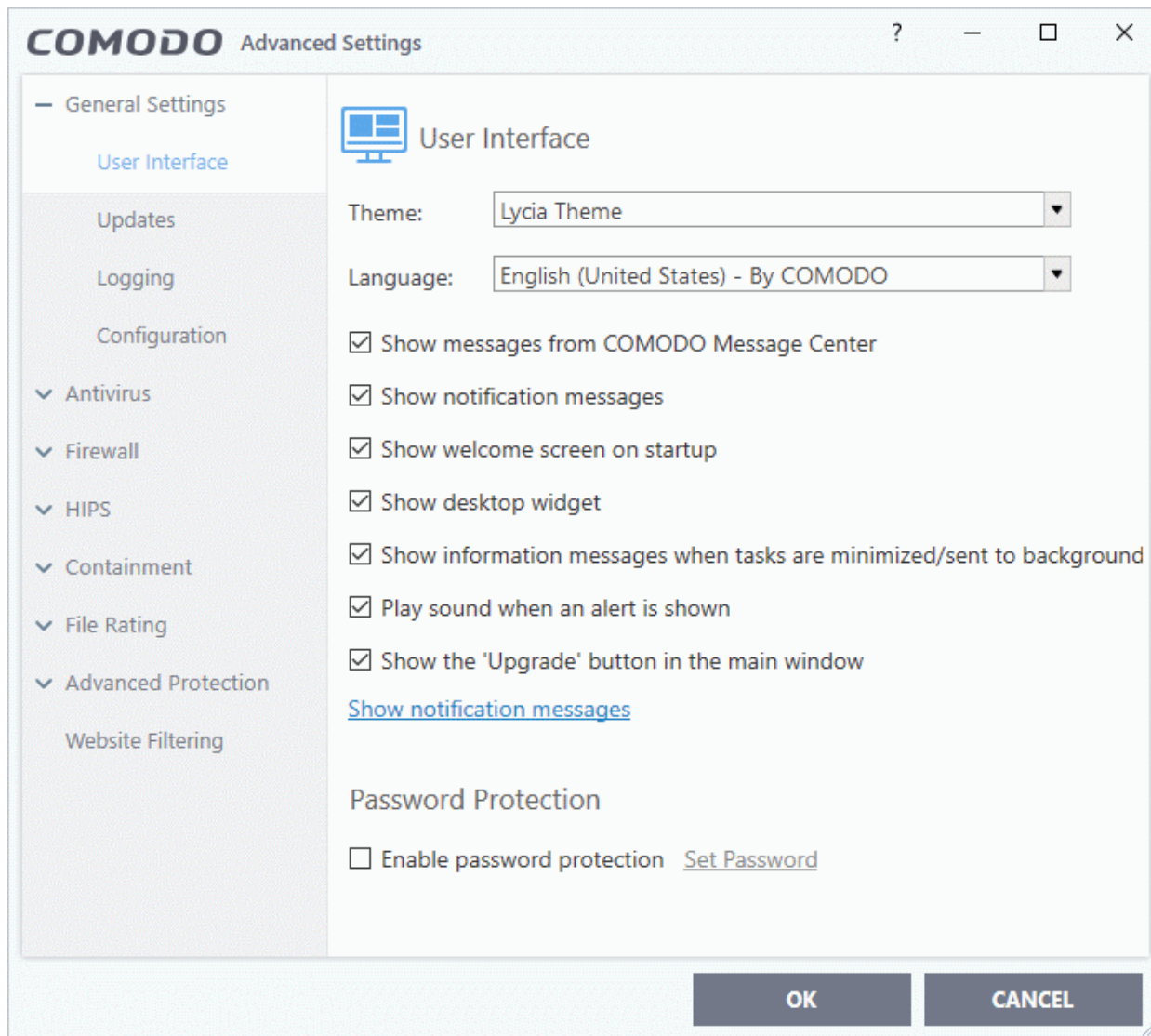
General settings is broken down into the following areas:

- **User Interface**
- **Updates**
- **Logging**
- **Configuration**

6.1.1. Customize User Interface

Click 'Settings' > 'General Settings' > '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 password protect access to important CIS settings.

Open user interface settings:

- Click 'Settings' on the CIS home screen
- Click 'General Settings' > 'User Interface'
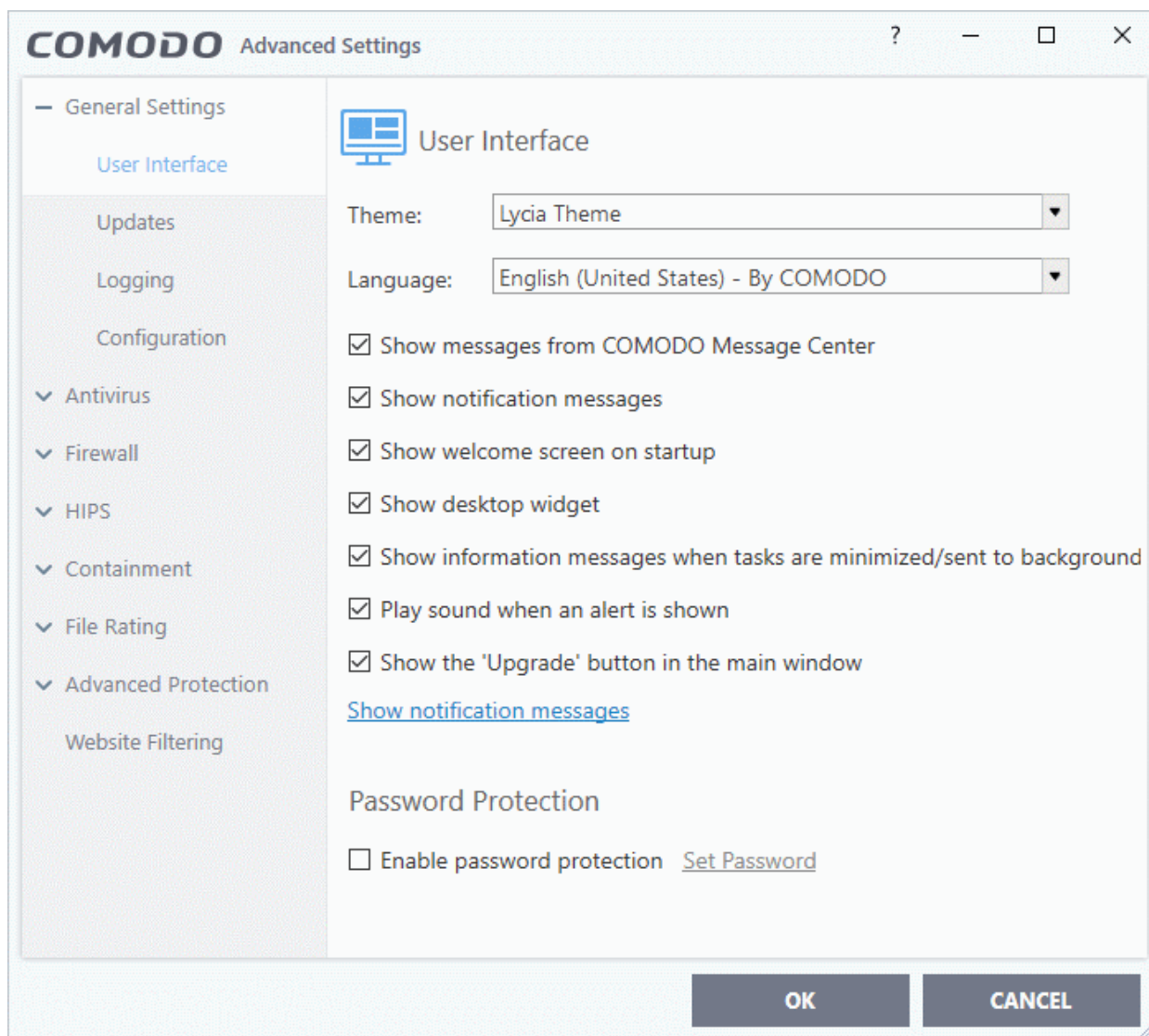
Click the following links for help with each setting:

- **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** - Choose the appearance of the GUI (***Default = Lycia Theme***).
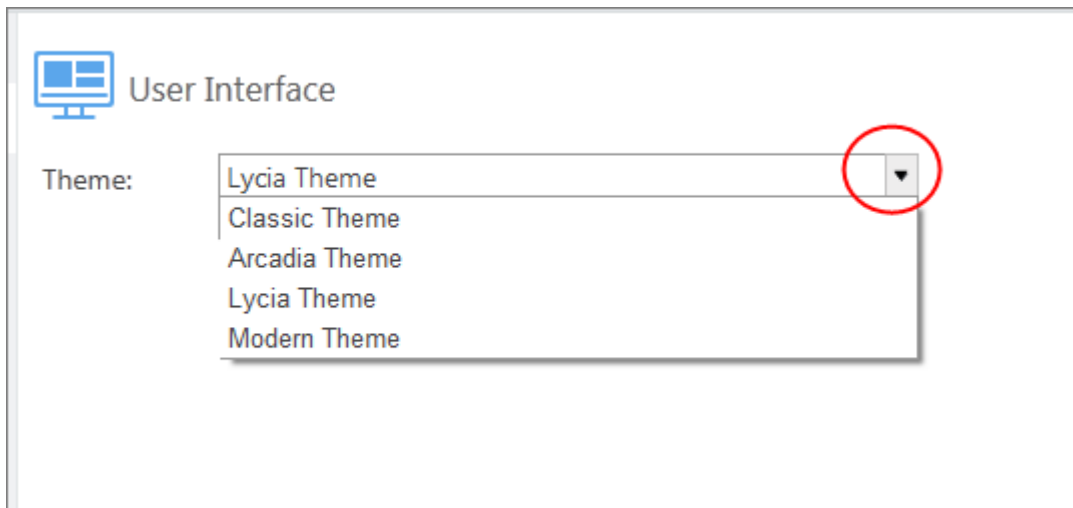
- **Language Settings** - Comodo Internet Security is available in many different languages. Switch languages by clicking the 'Language' drop-down menu:
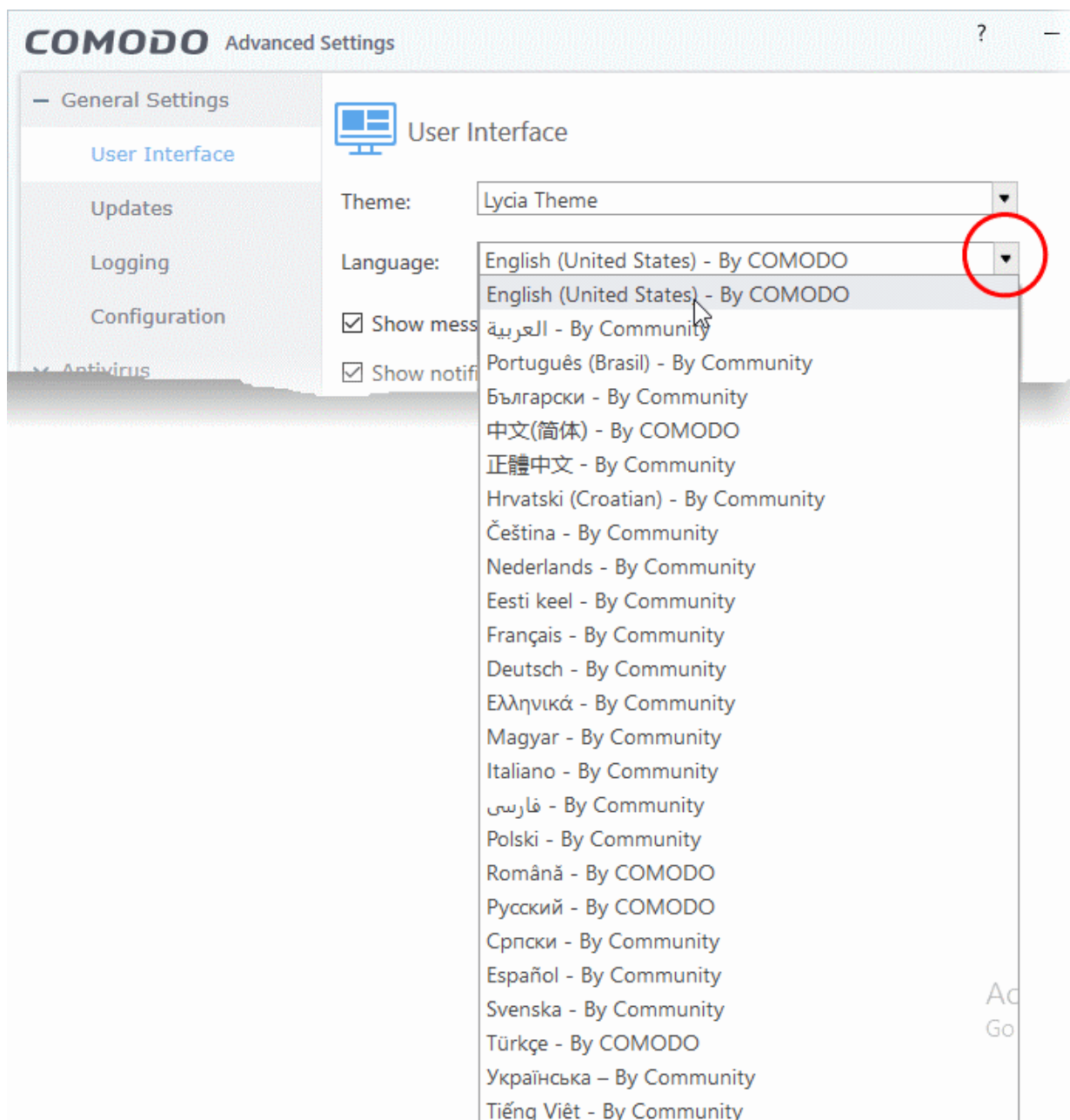
- **Show messages from COMODO Message Center** - Message center messages keep you abreast of Comodo news and special offers. If enabled, the messages will periodically appear as small pop-ups: (*Default = Enabled*).

- **Show notification messages** - CIS system notices appear in the bottom right-hand corner of your screen (just above the tray icons). They inform you about any actions that CIS is taking, and any CIS status updates:
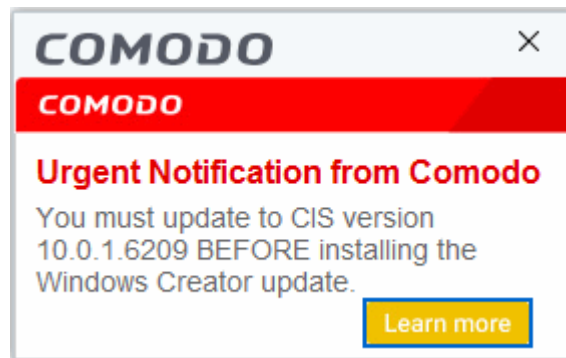
Clear this check box if you do not want to see these system messages (*Default = Enabled*).

Note - To view these messages, you also need to allow notifications from Comodo in Windows 'Notifications and Actions':

- Click the 'Show notification messages' link
- This opens the Windows 'Notifications and Actions' page
- Enable 'Get notifications from apps and other senders'
- Enable 'Comodo Internet Security' in the senders list
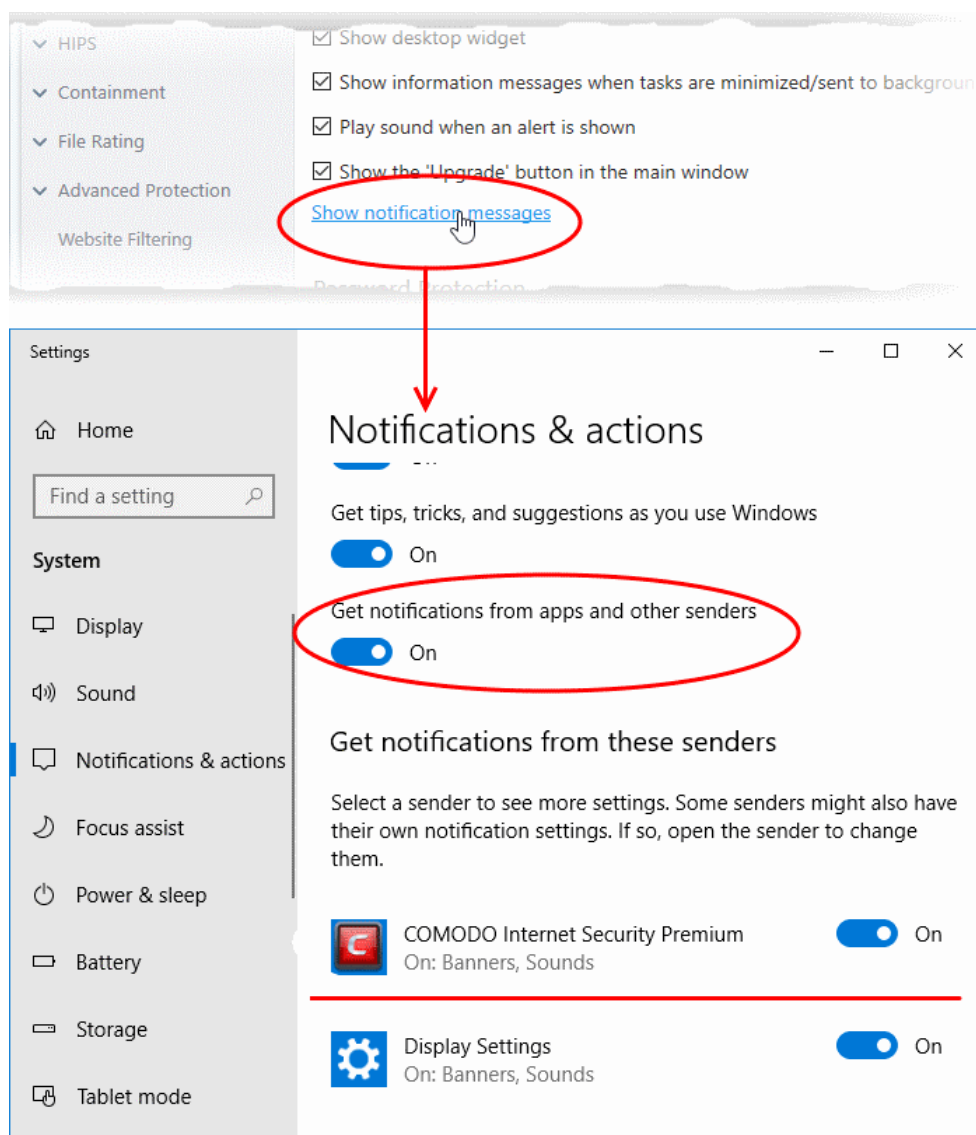
- **Show welcome screen on start up** - Enable or disable the welcome screen shown when the application first starts. *(Default = Enabled):*

> **Tip**: You also can disable the screen by selecting 'Do not show this window again' in the welcome screen itself.

- **Show desktop widget** - The desktop widget shows your overall security status, outgoing and incoming traffic, and any background tasks.

  - The widget also contains shortcuts to open the CIS interface, to open the task manager, to open your browsers, and to visit social network sites.
  - Select this checkbox if you want the widget on your desktop. (*Default = Disabled*)

> **Notes**:
> - The widget is shown by default if 'Show Widget on Desktop at startup' was enabled during CIS installation. See the **Installation Guide** for more details.
> - You can also enable or disable the widget by right-clicking on the CIS system icon.

…
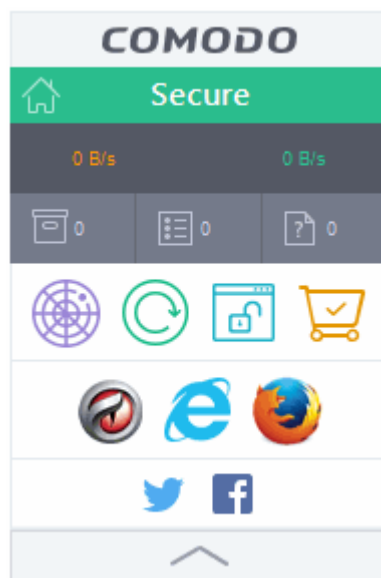
See **The Widget** for more details on the Widget.

- **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	Comodo Send To Background
What is a Minimized Task? A task which doesn't consume as much resources as an active task.	**What is a Background Task?** A task which runs in the background without interfering with your normal PC activities.
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.	**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	☐ Do not show this message again OK

- Disable this setting if you don't want to view these messages (*Default = Disabled*).

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 makes a chime sound whenever it raises a security alert
  - Clear this checkbox if you do not want the sound to be generated. *(Default = Enabled).*
- **Show 'Upgrade' button in the main window** - CIS shows the green upgrade button at the bottom right of the interface.
  - Click the 'Upgrade' button to upgrade to CIS Pro or Complete. *(Default = Enabled)*.
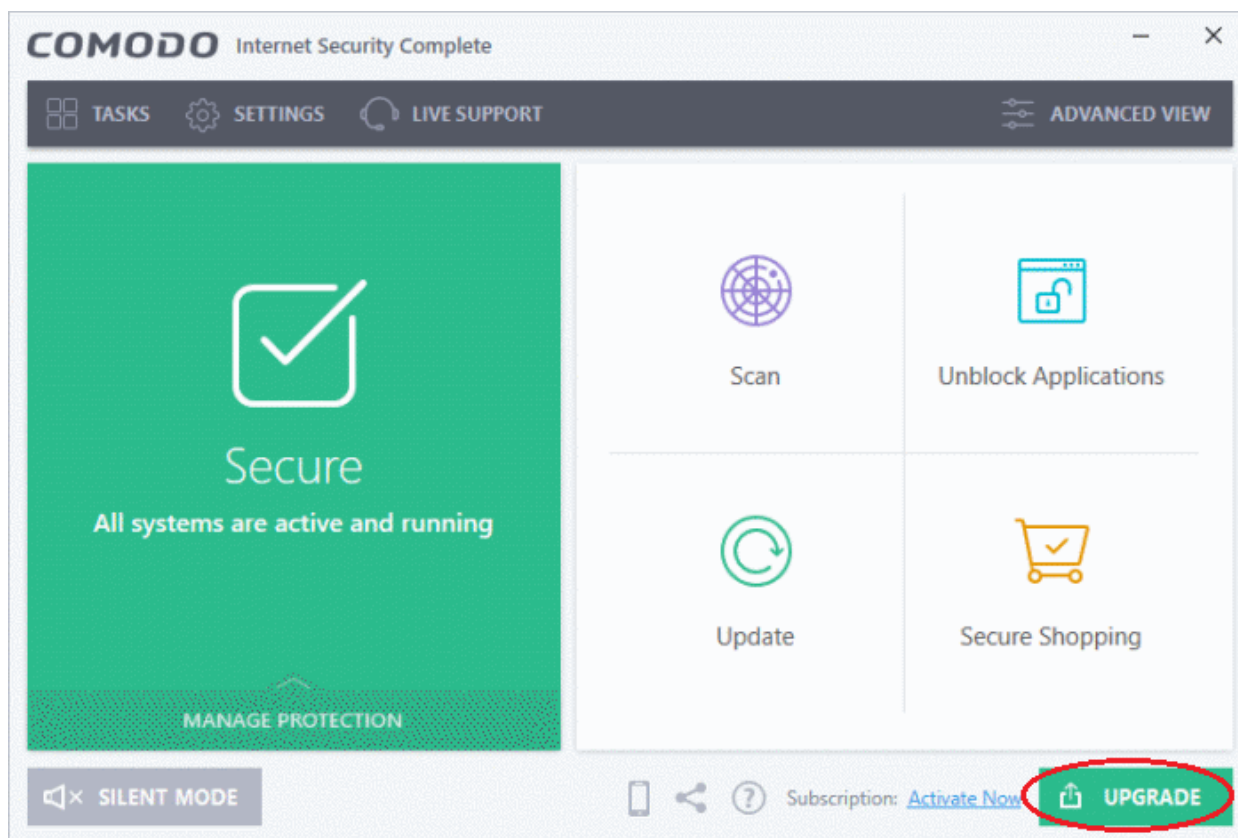
- Deselect this option if you do not want to see the 'Upgrade' button on the main interface.
- **Enable Password Protection** - If enabled, users will need to enter a password to access CIS settings areas and wizards. For example, all sections in the **General Tasks**, **Firewall Tasks**, **Containment Tasks** and **Advanced Tasks** will request the password.

This setting is of value to parents and network admins as it prevents users from changing settings and possibly exposing the machine to threats (**Default = Disabled**).

Enable password protection

- Select the 'Enable Password Protection' check-box then click 'Set Password'.
- Enter and confirm your password then click 'OK':
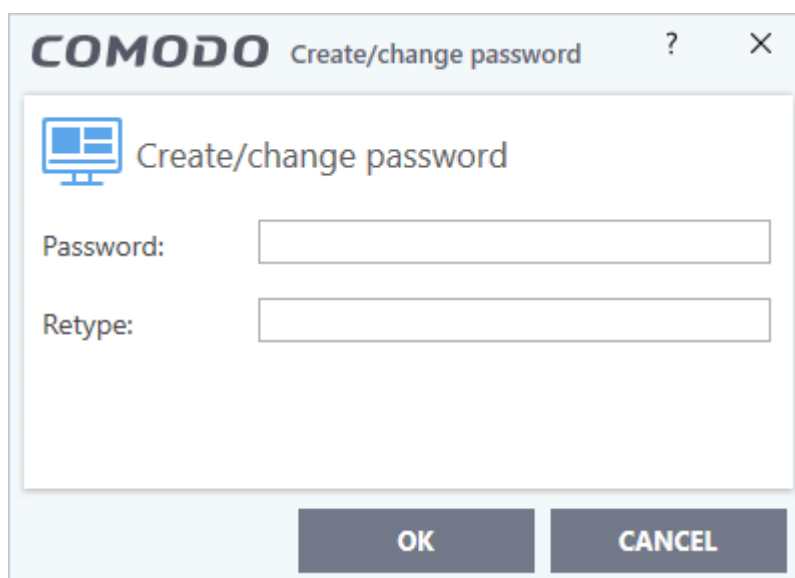
- Make sure to create a strong password containing a mixture of upper and lower case letters,

---

numbers and symbols.

6.1.2. Configure Program and Virus Database Updates

Click 'Settings' > 'General Settings' > 'Updates'

- This area lets you configure CIS program and database updates:

Configure update settings

- Click 'Settings' at the top of the CIS home screen
- Click 'General Settings' > 'Updates' on the left:
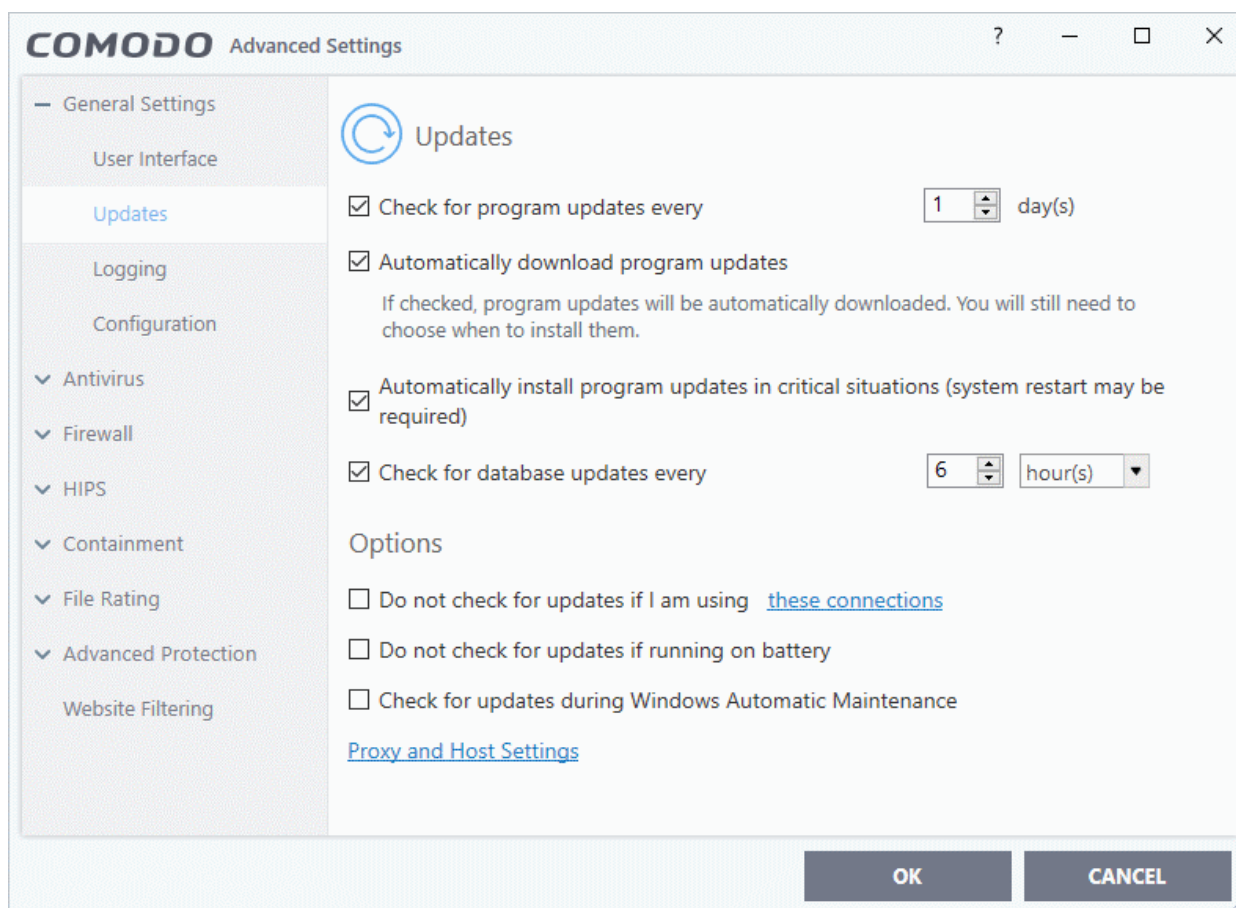
- **Check for database updates every...** - Set how frequently CIS should check for application updates. Updates are downloaded from Comodo servers by default, but you have the option to **set a local server** to handle updates instead. Select the interval in hours / days. (**Default = 1 day**)
- **Automatically download program updates** - CIS will fetch and save program 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.** (**System restart may be required**) - CIS will auto-install updates which fix very serious bugs and incompatibilities. For example, a Windows hotfix may introduce incompatibilities with CIS which need 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...** - Set how frequently CIS should check for virus database updates. **(Default and recommended = 6 hours)**
- **Do not check updates if am using these connections** - CIS will not check for updates if you are using specific internet connections. For example, you may not wish to check for updates when using a wireless connection you know is slow or insecure. **(Default = Disabled)**
    - Enable 'Do not check updates if am using these connections'.

- Click the 'these connections' link.
- Select the connection over which you do not want to check for updates.
- Click 'OK'.
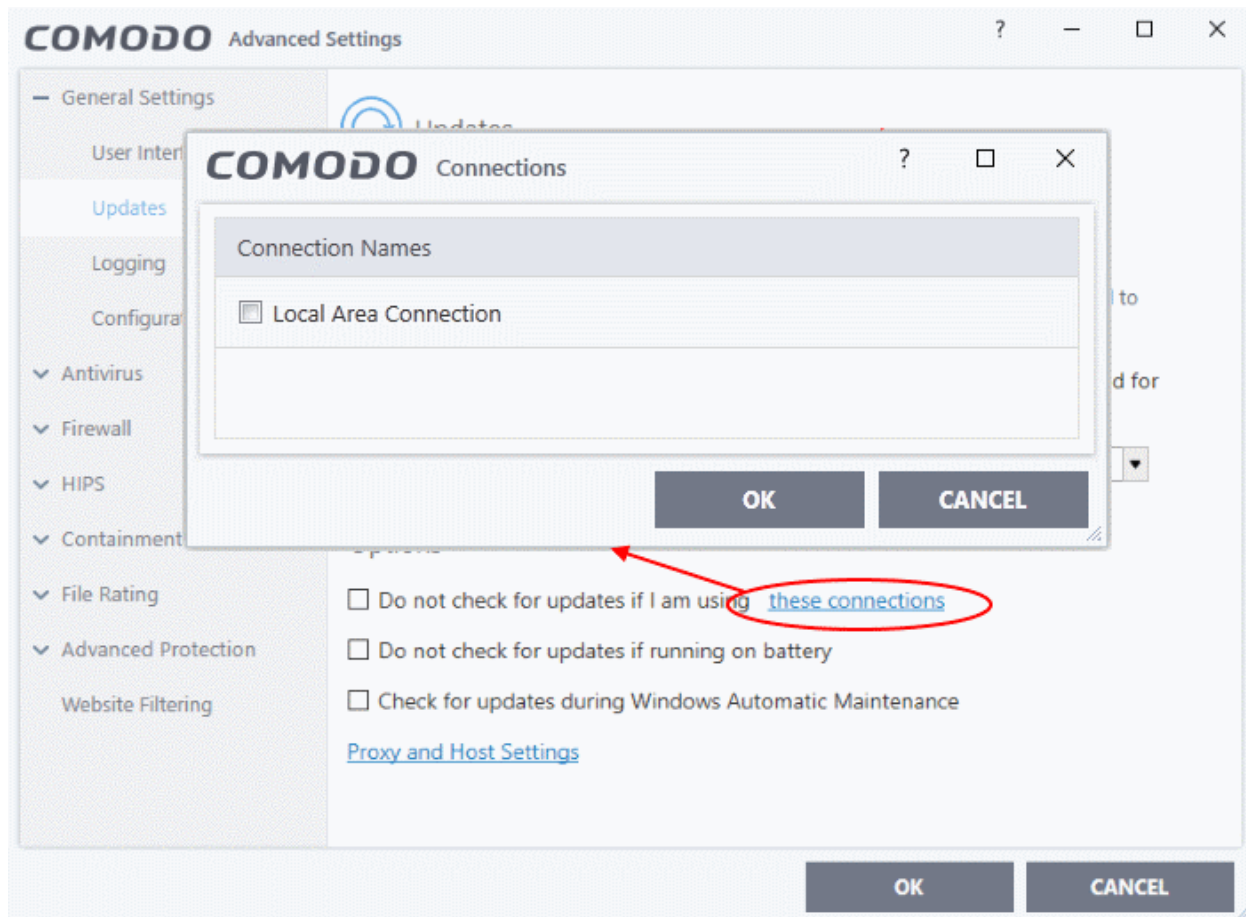
- **Do not check for updates if running on battery** - CIS will not download updates if it detects your computer is running on battery power. This is intended to extend battery lifetime on laptops. *(Default = Disabled)*

- **Check for updates during Windows Automatic Maintenance** - Enables CIS to receive program and virus signature database updates when Windows is updating itself.

- **Proxy and Host Settings** - Lets you specify (1) A proxy server through which CIS should connect to the update servers, and/or (2) Local hosts from which this computer should collect updates. The two are not dependent on each another. You can setup (1) without (2) and vice-versa, or enable both.

  - By default, CIS connects to the internet directly, and downloads updates from Comodo servers.
  - You can specify a proxy through which CIS connects to the update servers. If you do not set a proxy then CIS will continue to use a direct connection.
  - You can also specify a local host to act as a staging server for the updates. Individual endpoints will then fetch updates from the staging server instead of from Comodo servers. This can save bandwidth and accelerate updates in large networks.

Configure proxy and host settings

  - Click 'Proxy and Host Settings' at the bottom of the updates interface:
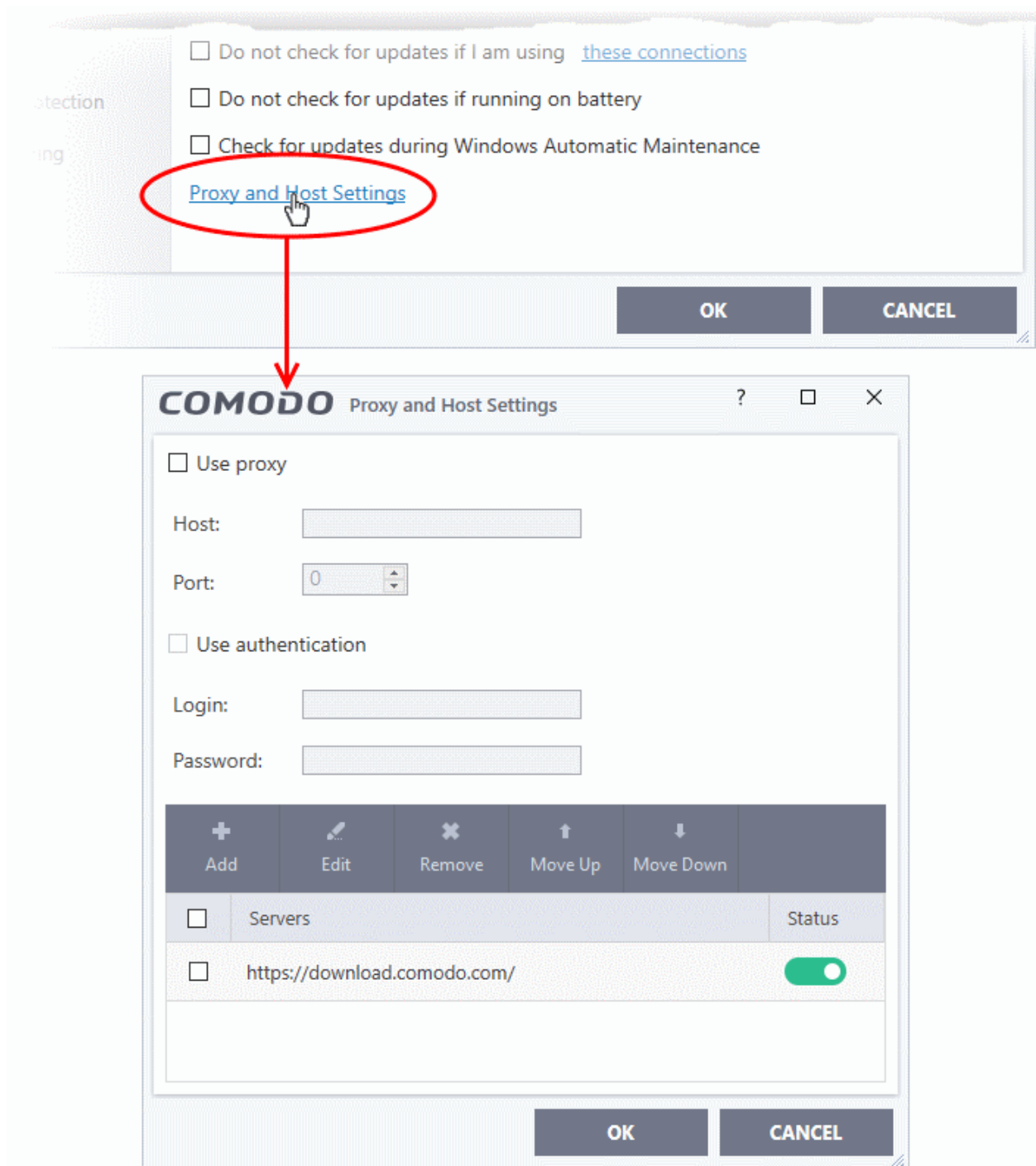
- • **Configure a proxy server**
- • **Add local servers for CIS to download updates from**

Configure a proxy server
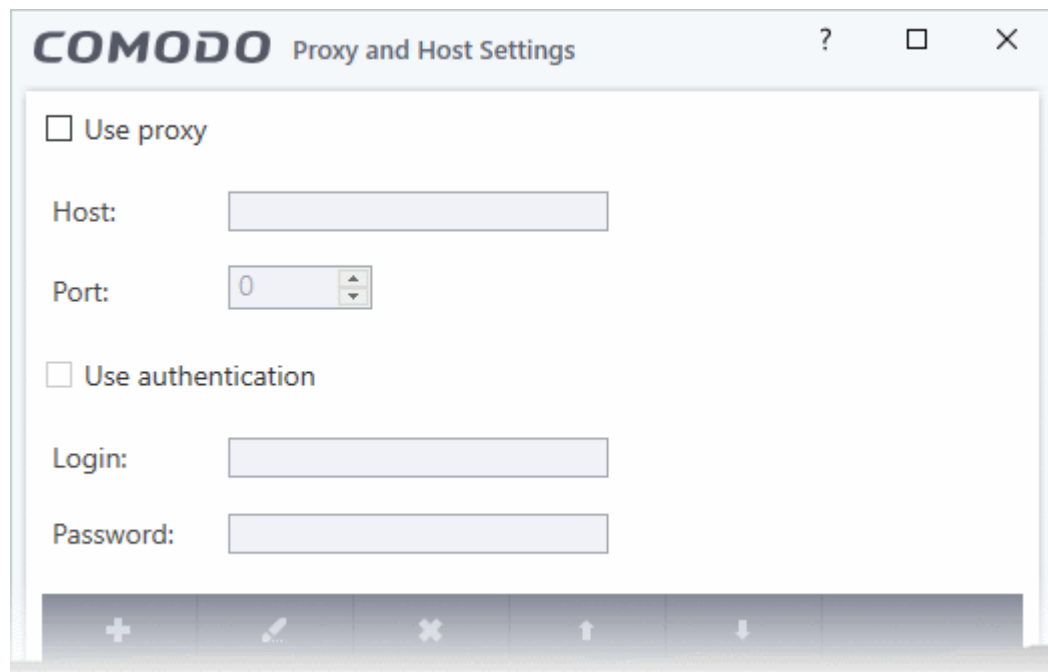
- **Use Proxy** - CIS will connect to the update server through a proxy server.
  - Enter the host name or IP of the proxy and the connection port
- **Use Authentication** - Provide the username and password of the proxy if required.

Configure local update server

Note: You need to install the 'ESM Update Mirror' (ESMUM) utility to download updates to the local update server.

- Download the setup file from
  https://drive.google.com/file/d/0B4qKr5xfENWBS0FOUHM2VDFQMnc/view.

- Run the setup file on a Windows server and follow the wizard to install the application
- Ensure that the service has started:
  - 'Run' > Enter 'services.msc' > locate 'Apache2.2'
  - Click the 'Start' link on the left if the service is not running

---

- Click the 'Add' button in the lower pane
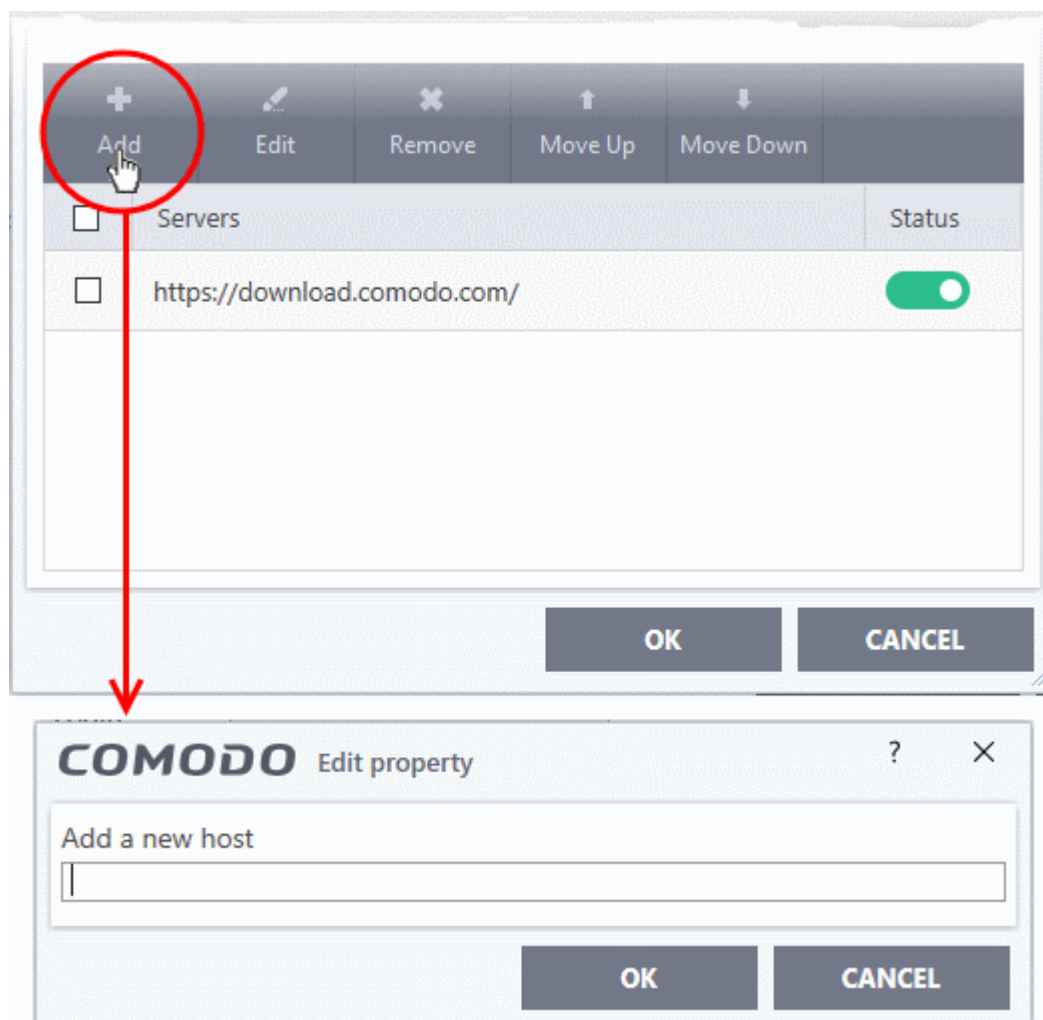
- Enter the IP address or hostname of the server (with 'http://' prefix)
- Repeat the process to add more local update servers
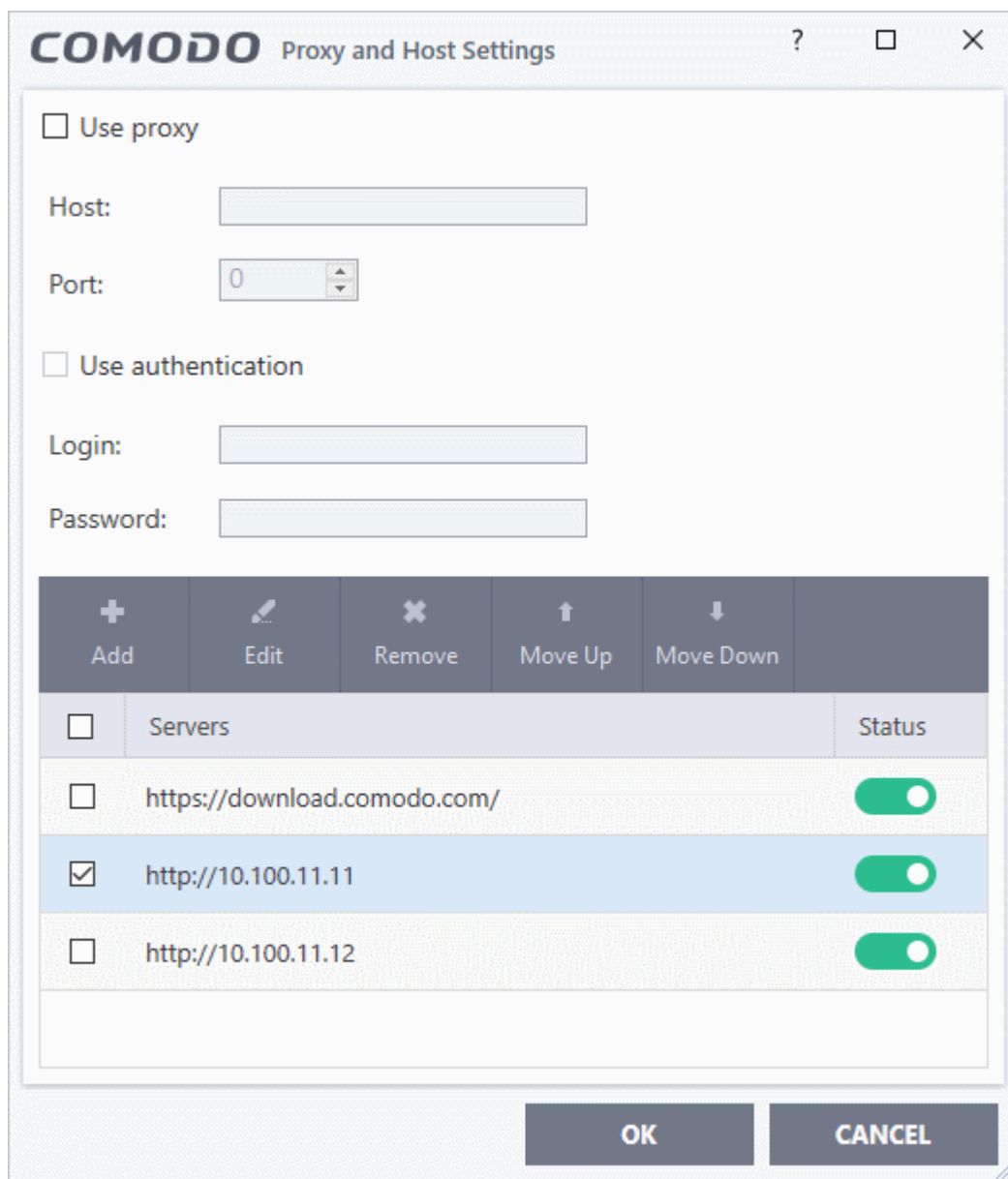
- Use the 'Move Up' and 'Move Down' buttons to choose the order in which servers should be consulted. CIS will download from the first server that contains new updates.
- Use the status switches to activate or deactivate individual servers
- Click 'OK' for your settings to take effect.

Note: Admins who need to manage a large number of endpoints may want to consider Comodo Endpoint Manager. Available as part of the Dragon platform, Endpoint Manager lets you centrally manage the business version of CIS on Windows, MAC and Linux endpoints.

Try out the service at **https://www.comodo.com/aep.php**.

6.1.3. Log Settings

Click 'Settings' > 'General Settings' > 'Logging'

- 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, 'Vendor list changes', 'Trusted Certificate Authorities changes' and 'CIS Configuration Changes'.
- Log settings let you specify the log storage location, the maximum size of log files, and how CIS should

react if the maximum file size is reached.

Note: You can view the logs themselves at 'Tasks' > 'Advanced Tasks' > 'View Logs'.

Configure Log settings

- Click 'Settings' on the CIS home screen

- Click 'General Settings' > 'Logging':
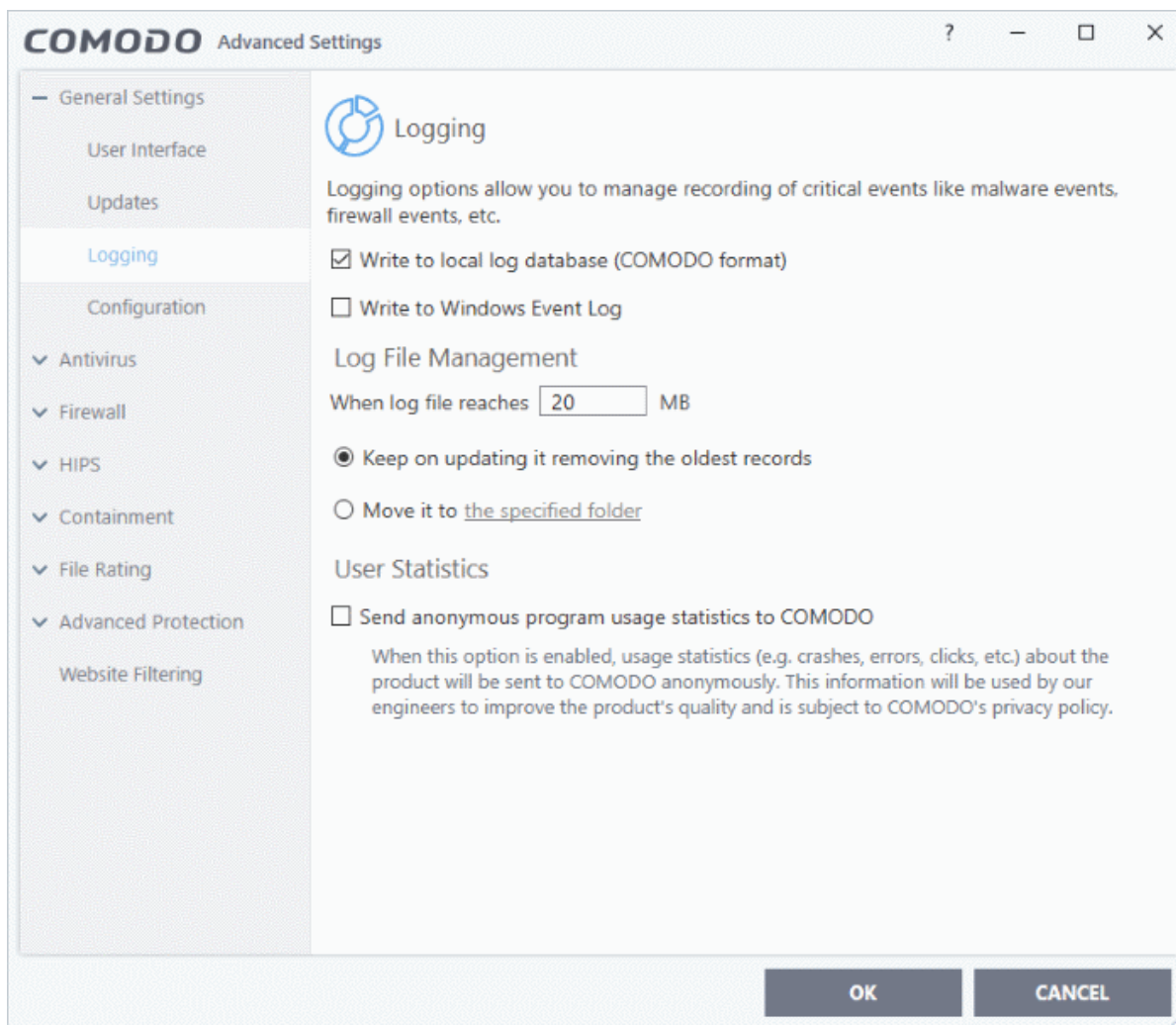
Logging

- **Write to local log database (COMODO format)** - Enable or disable logs in Comodo format *(Default = Enabled*)

- **Write to Windows Event Logs** - CIS logs are appended to 'Windows Event' logs. *(Default = Disabled)*

  - Type 'Event Viewer' in Windows search to view Windows logs

Log File Management

- Specify what should happen when the log file reaches a certain size. You can choose keep the older logs or discard them.

  - **When log file reaches** - Enter the maximum size of a log file in MB. (*Default = 20MB*)

  - **Keep on updating it removing the oldest records** - When a log file reaches the max. size, CIS will delete the earliest log entries to make room for the new entries. (*Default = Enabled*)

  - **Move it to the specified folder** - When a log file reaches the max. size, CIS starts a new log file and moves the old one to a folder of your choice. (*Default = Disabled*)

    - Click 'the specified folder' to choose the storage folder:
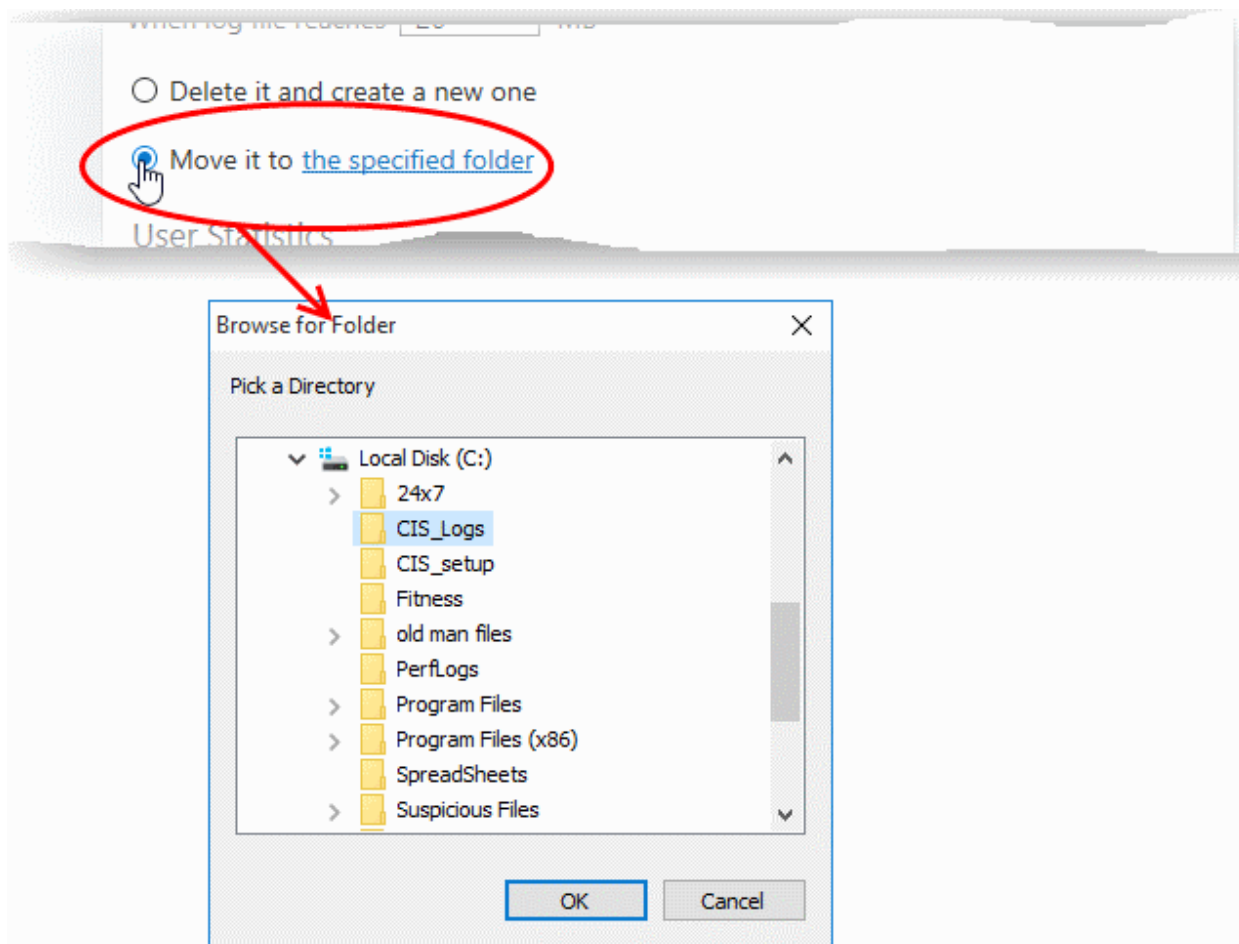
The selected folder path will appear beside 'Move it to'.
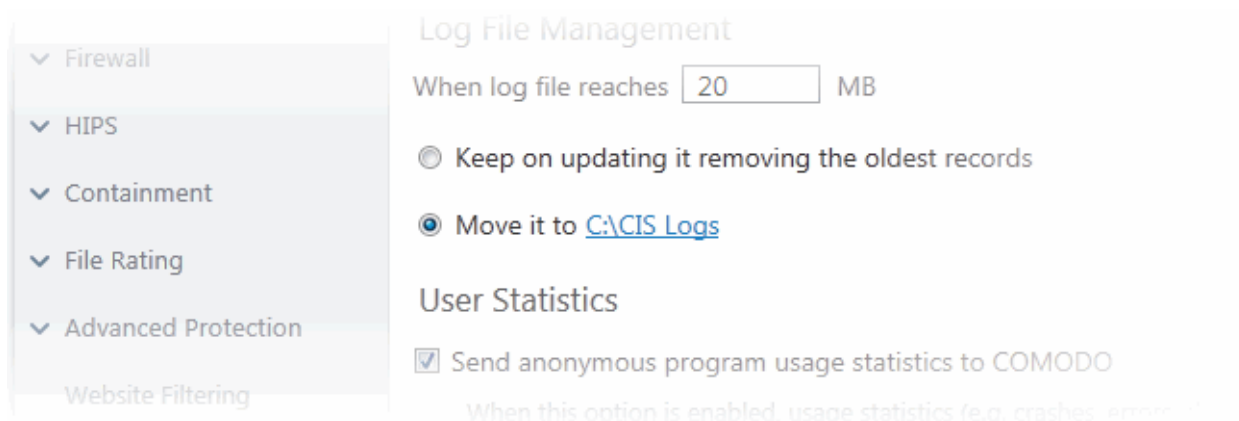
User Statistics

- **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

Click 'Settings' > 'General Settings' > 'Configuration'

- CIS lets you export your current security settings as a profile. You can then import the profile to another computer, or the same computer, and avoid having to configure everything again.

- Exported settings include antivirus, firewall, HIPS, containment, website filtering, VirusScope and secure shopping settings.

- Exporting your CIS settings can be a great time-saver if:

  - You are a network admin looking to roll out a standard configuration to multiple computers.

  - You need to uninstall and re-install CIS or Windows, and want to quickly implement your old settings.

> **Note**: Any changes you make over time are automatically saved in the 'Active' profile. If you want to export your current settings then export the 'Active' profile.

- The 'General Settings' > 'Configuration' interface lets you switch your currently active profile and import/export profiles.

Access the configuration settings interface

- Click 'Settings' at the top of the CIS home screen

- Click 'General Settings' > 'Configuration' on the left:
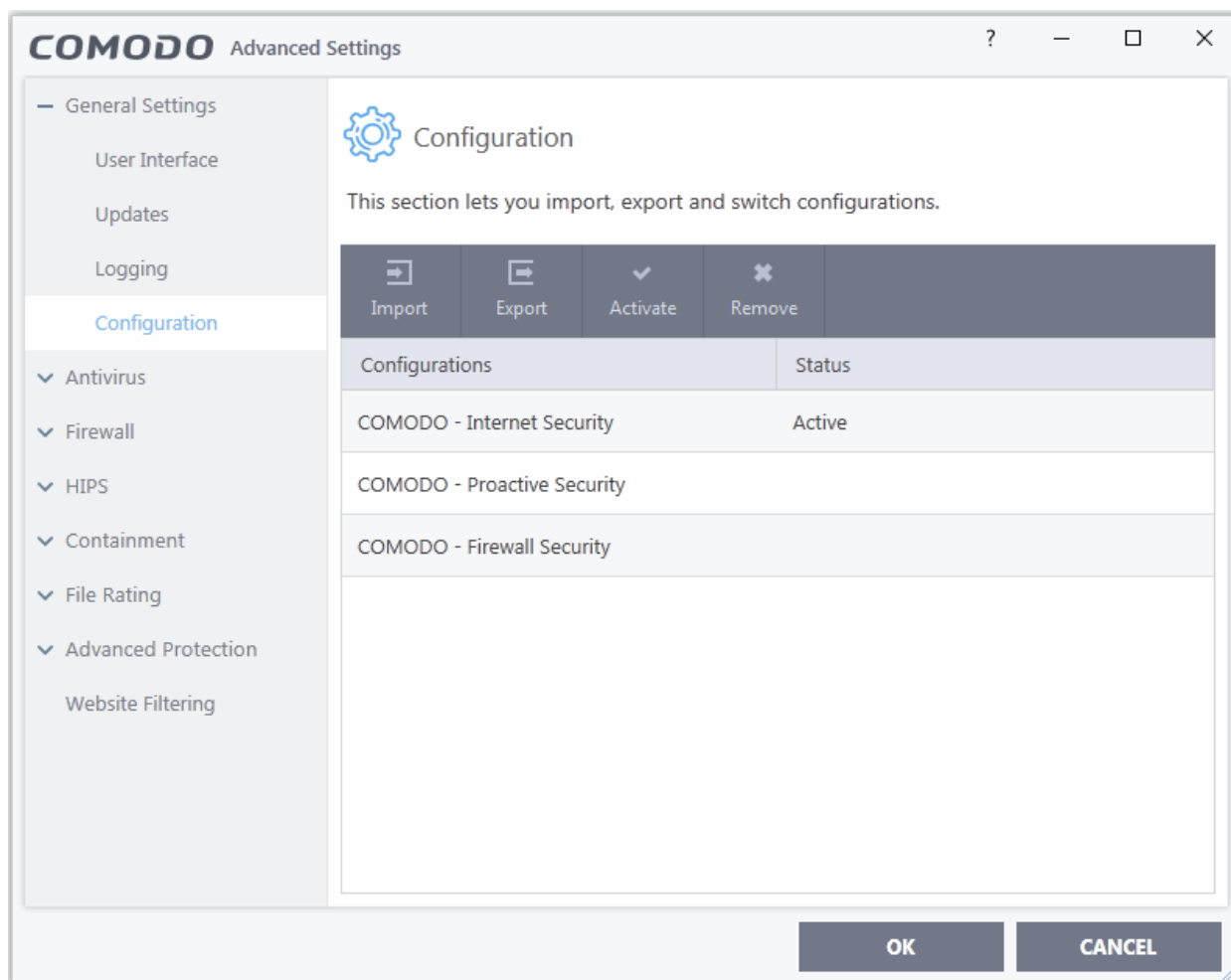
The configurations interface shows all Comodo and user-defined profiles. The 'Active' profile is the one that is currently in effect on your computer. The following sections explain more about:

- **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 in the configuration panel.

COMODO - Internet Security - This configuration is activated by default when both Antivirus and Firewall components are installed. 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. Personal Configurations

Click 'Settings' > 'General Settings' > 'Configuration'

- You can import, export, activate and manage your custom CIS configurations
- Exported Configuration profiles have the file extension .cfgx.
- See the following sections for 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**

Export a stored configuration to a file

- Click 'Settings' on the CIS home screen
- Click 'General Settings' > 'Configuration'

- Select a configuration profile then click 'Export'
- If there are any unsaved changes to the current configuration then you can save them before exporting:
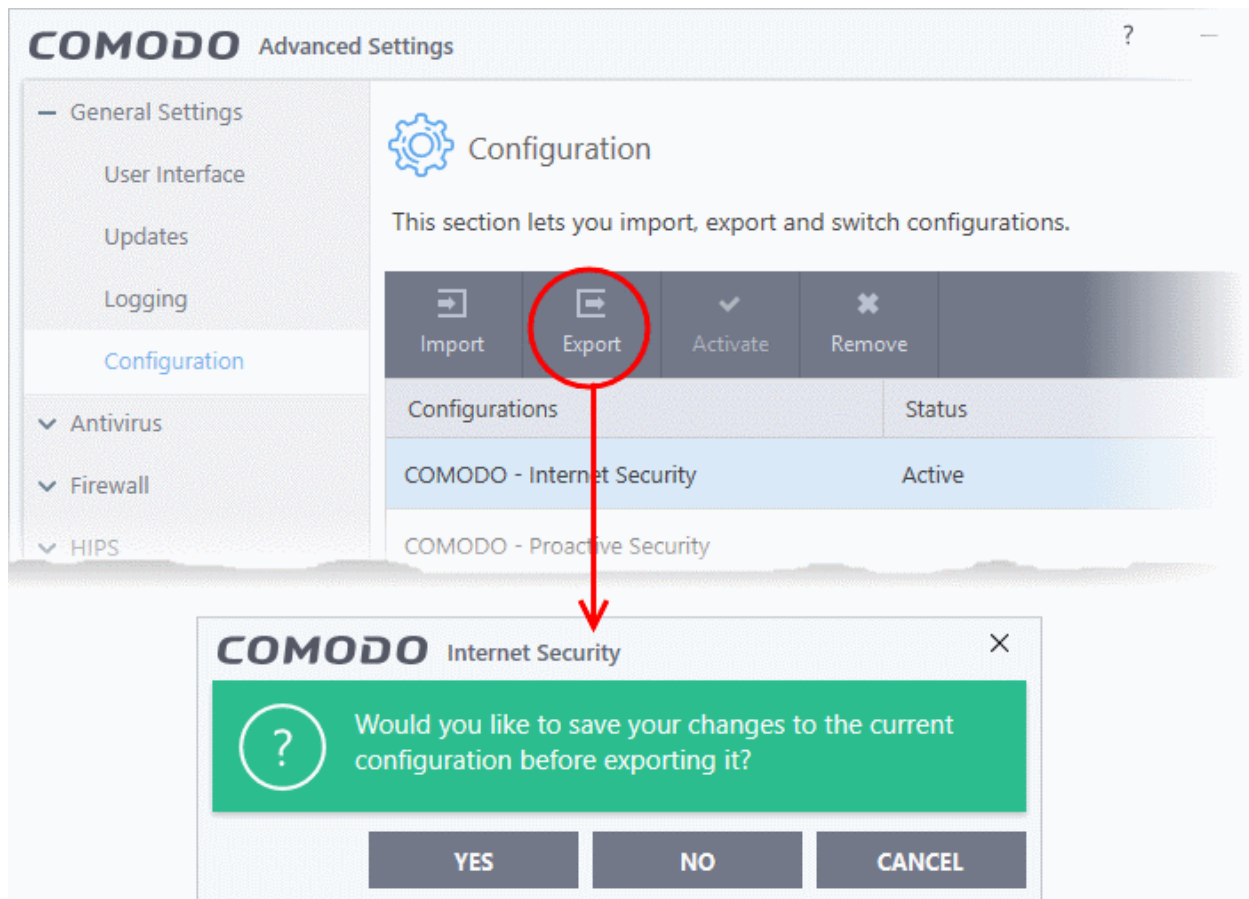
- Next, browse to the location where you want to save the configuration file.
- Create a name for the profile. For example, 'My CIS Settings', or 'CIS Highest Security Settings'
- Click 'Save':
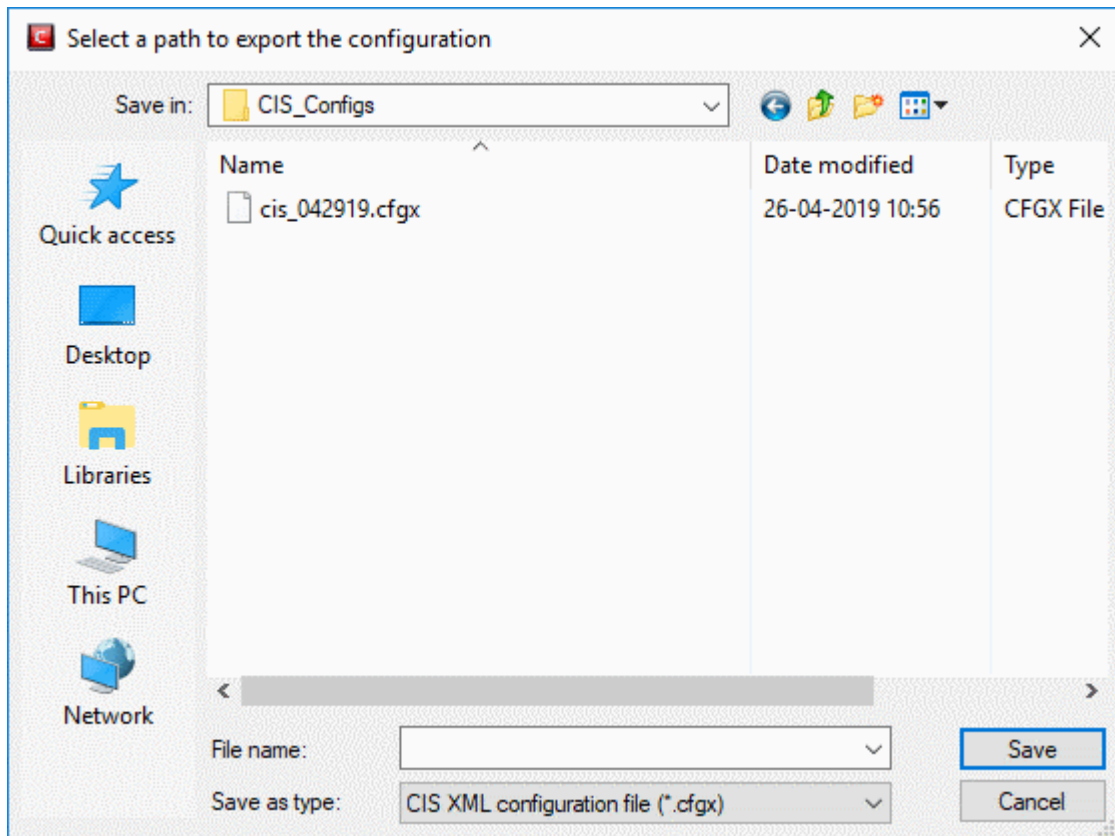
A confirmation dialog will appear if the export is successful:
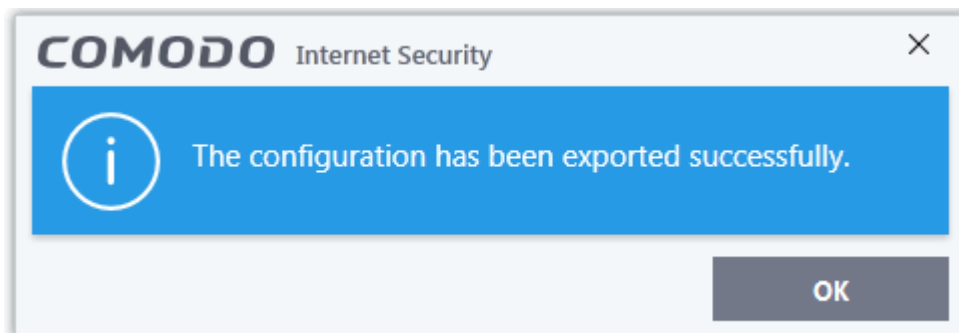
Import a saved configuration from a file

- You can import a CIS configuration from a previously saved file
- Note - any profile you import will not become active until you **activate it**.

Import a profile

- Click 'Settings' at the top of the CIS home screen
- Click 'General Settings' > 'Configuration' on the left
- Click the 'Import' button:
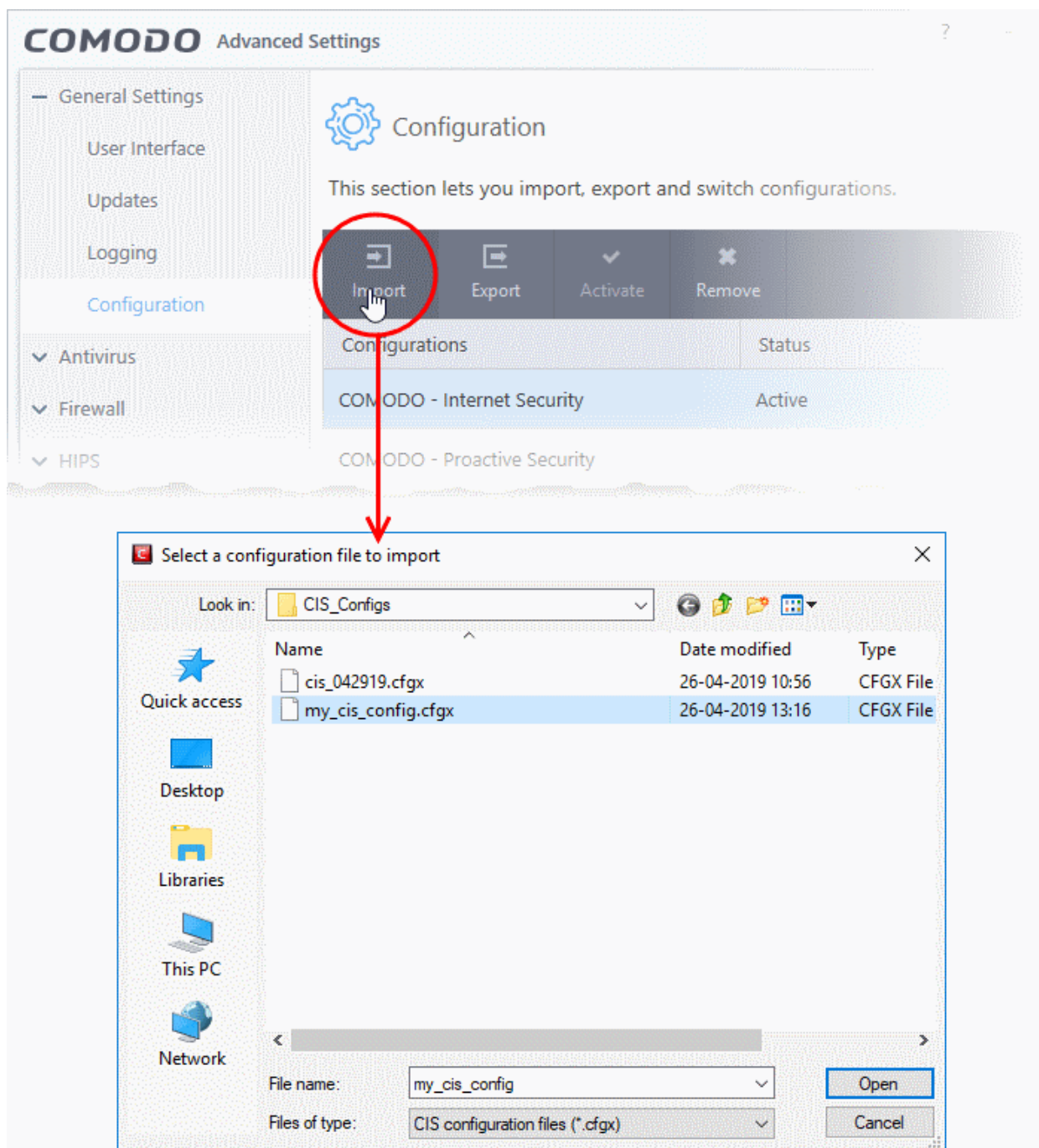
- Navigate to the location of the saved profile and click 'Open'. Configuration files have a .cfgx extension.
- Enter a name for the profile you wish to import and click 'OK'.
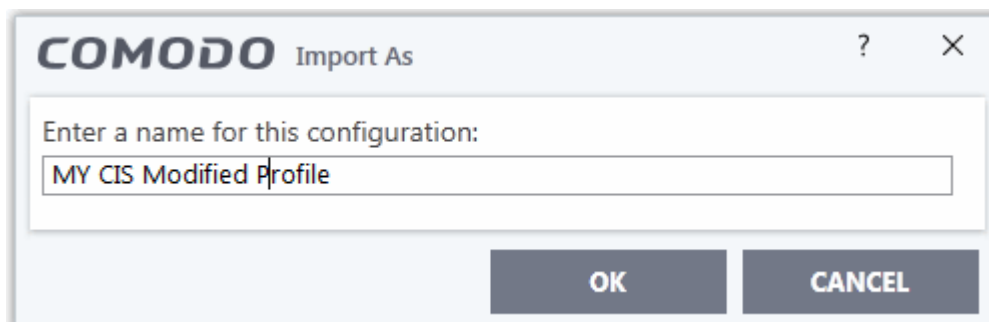
A confirmation dialog will appear indicating the successful import of the profile.
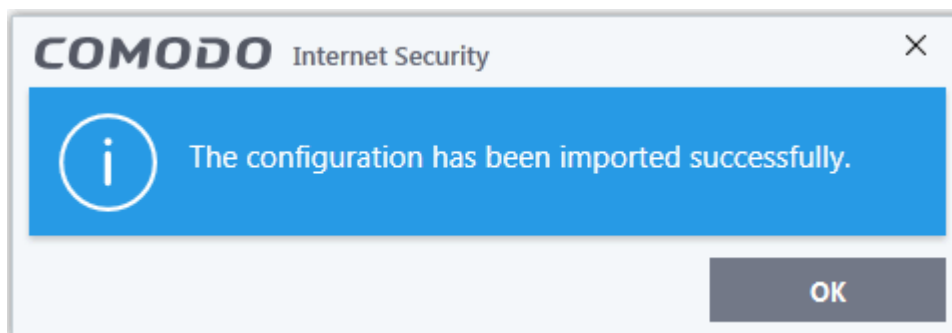
Once imported, the configuration profile can be re-exported or deployed in the current installation by making it **active**.
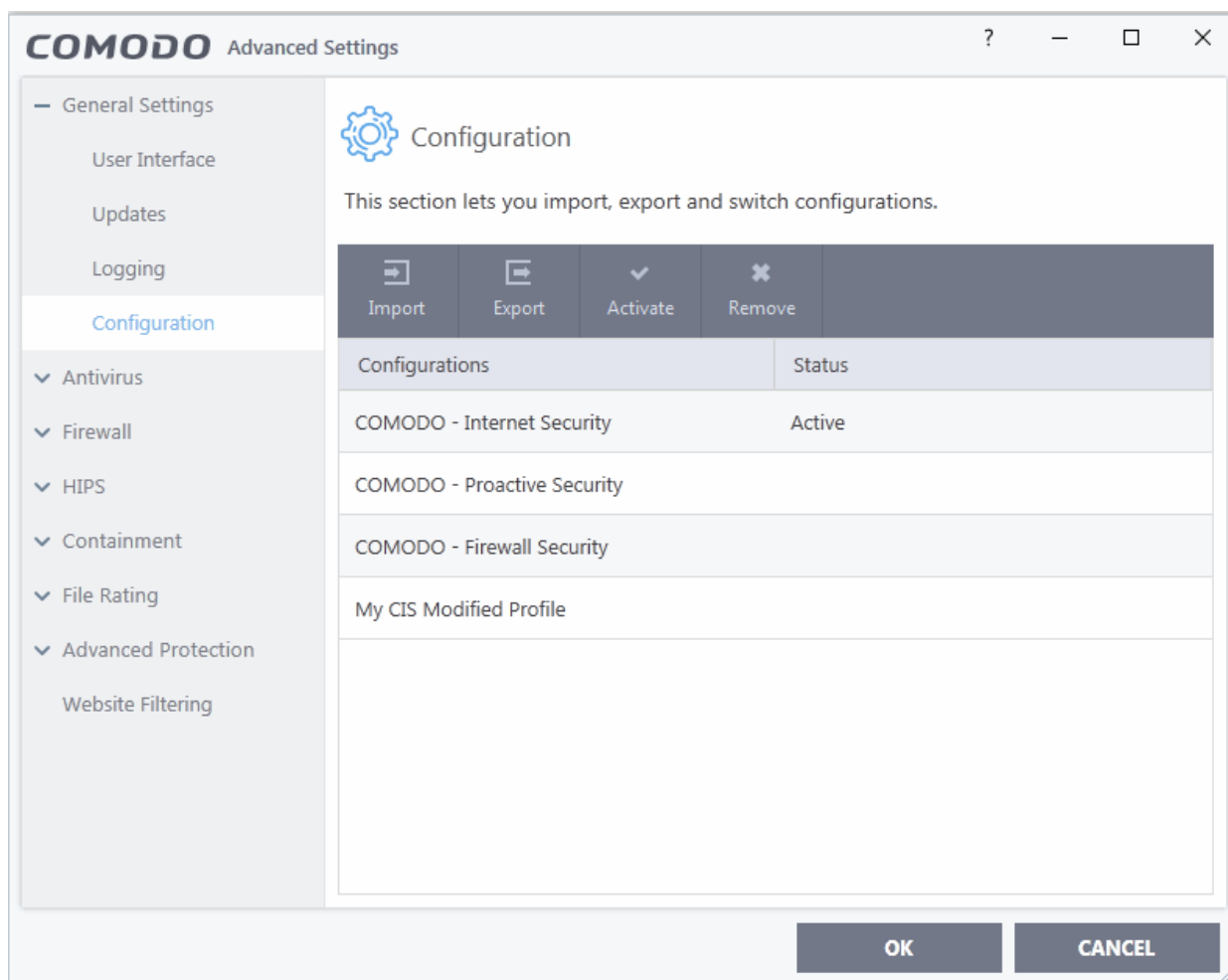
Select and Implement a different configuration profile

You can change the active configuration profile at any time from the 'Configurations' panel

Change the active configuration profile

- Click 'Settings' at the top of the CIS home screen
- Click 'General Settings' > 'Configuration' on the left
- Choose the profile you want to enable and click the 'Activate' button:
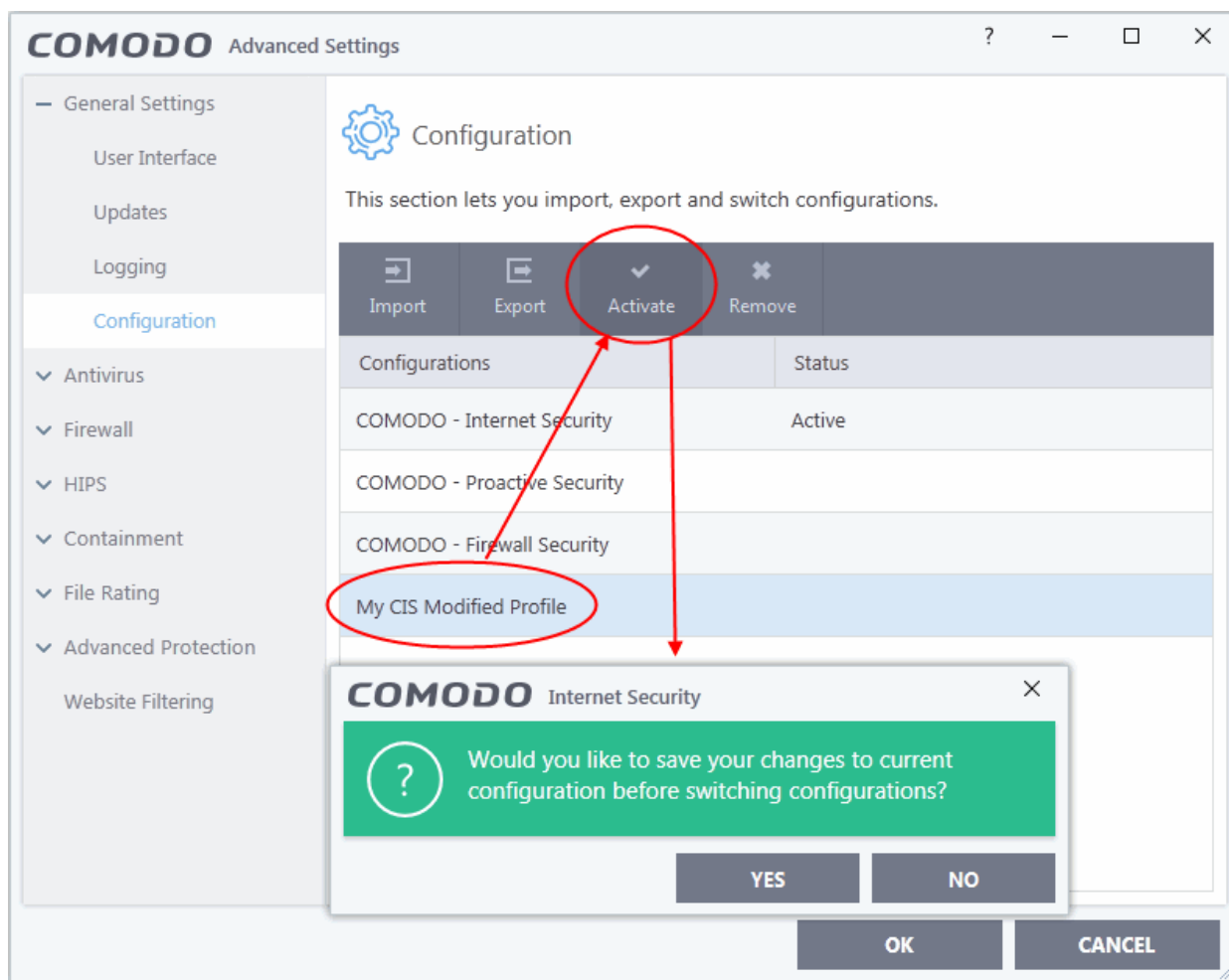
- Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

An activation confirmation dialog will be displayed.
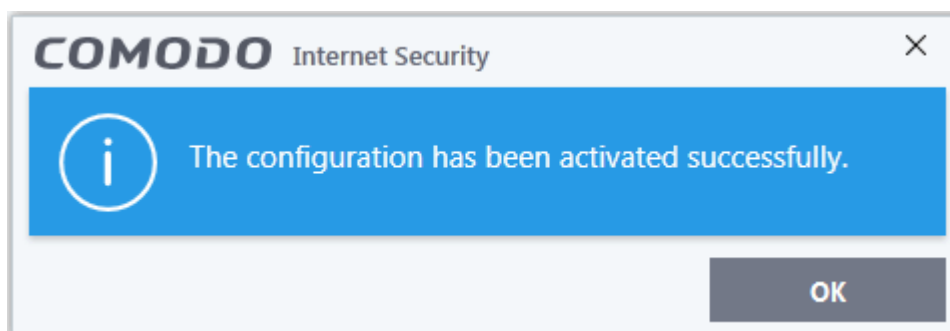
Your new profile will be set active. If you are switching to 'Comodo Proactive Security' profile from a different profile or switching to any other profile from 'Comodo Proactive Security' profile, your computer needs to be restarted for the new profile to be activated. 'A Restart Computer' dialog will appear at the bottom right of the screen.
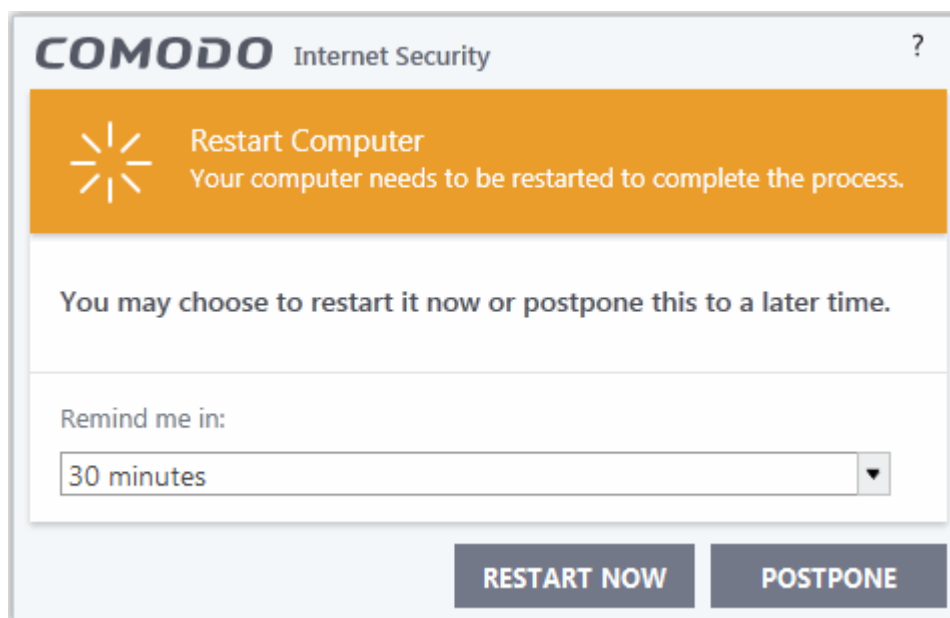
- If your want to restart the computer immediately, save all your work and click 'Restart Now'.
- If you want to restart the computer at a later time, select when you need to be reminded from the drop-down and click 'Postpone'.

Remove an inactive configuration profile

You can remove any unwanted configuration profiles from the list. You cannot delete the currently active profile, only the inactive ones.

- Click 'Settings' on the CIS home screen
- Click 'General Settings' > 'Configuration'
- Choose the configuration profile you want to delete then click the 'Remove' button

A confirmation dialog appears:
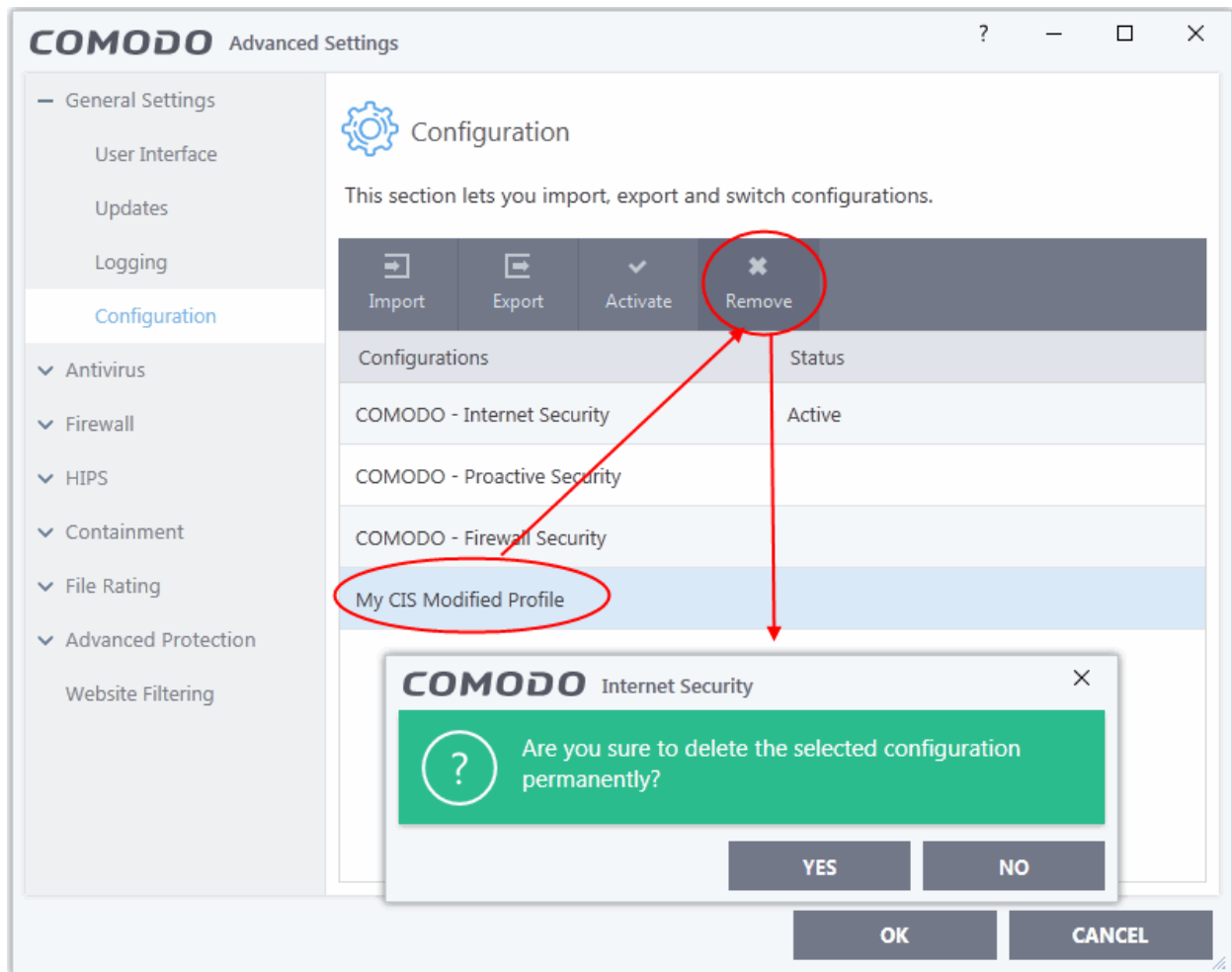
- Click 'Yes'. The configuration profile will be deleted.
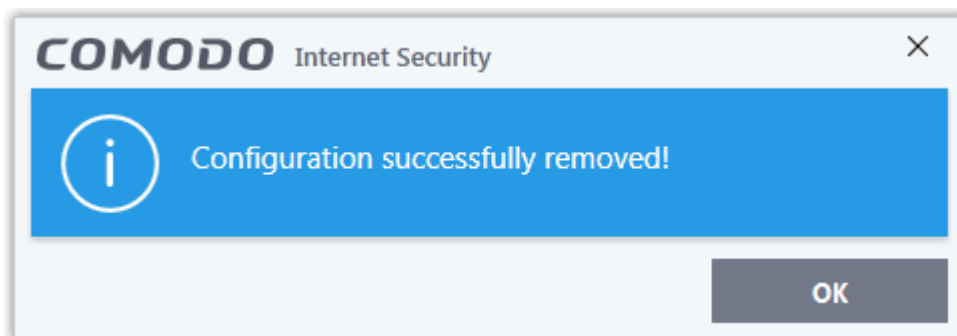
6.2. Antivirus Configuration

- Click 'Settings' > 'Antivirus'

The 'Antivirus' settings area lets you configure:

- The behavior of the real-time antivirus monitor
- Scan profiles for on-demand and scheduled scans
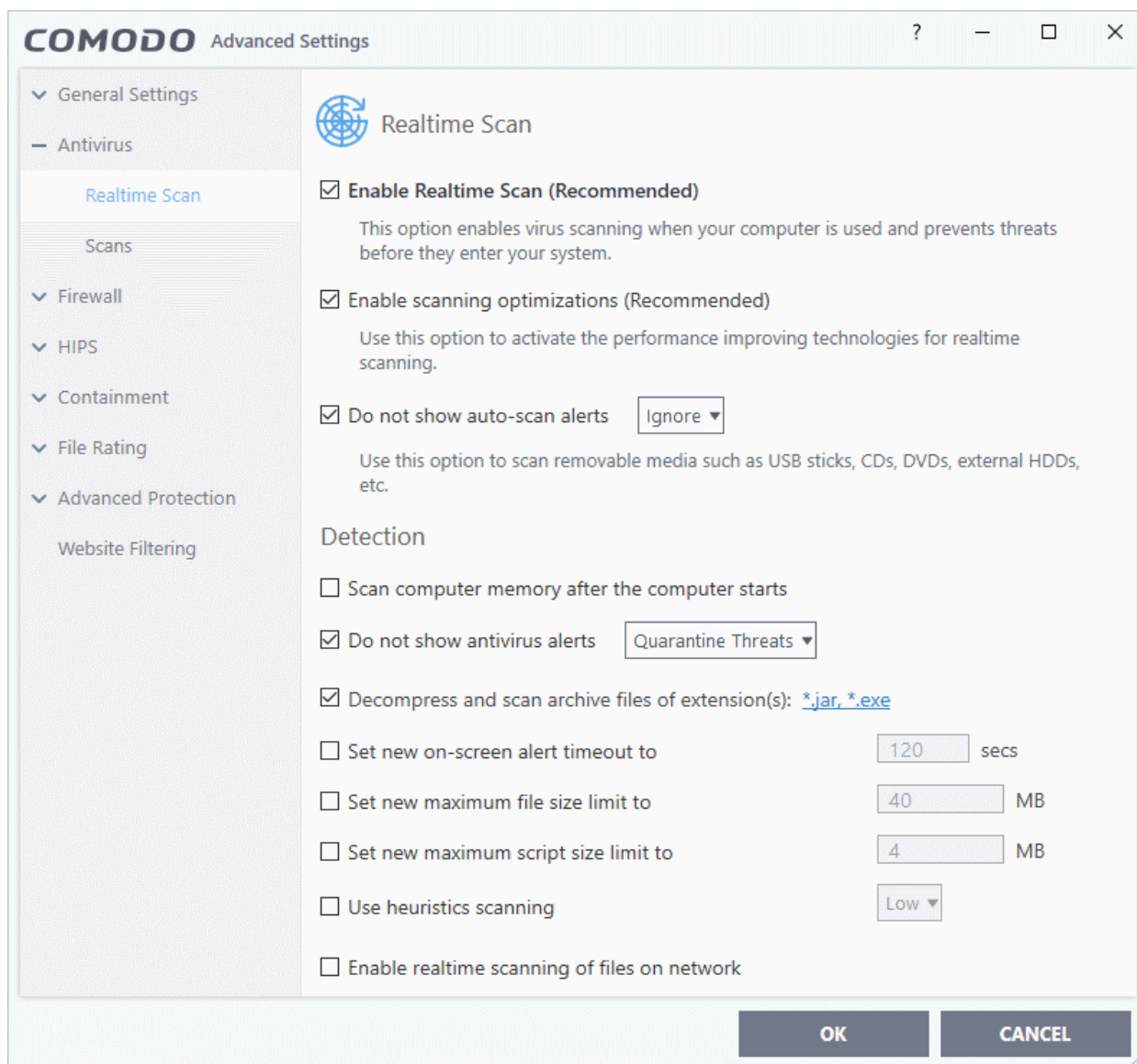
The following sections explain more about:

- **Real-time Scan Settings**
- **Custom Scan Profiles**

6.2.1. Real-time Scan Settings

Click 'Settings' > 'Antivirus' > 'Realtime Scan'

- The real-time scanner automatically checks for viruses whenever you open or move a file. It also monitors background processes for malicious activity.

- This ensures your system is constantly protected against malware and enjoys the highest levels of security.

- The real-time scanner also scans:

    - System memory on system startup

    - Any plugged-in removable storage devices

- You can specify that CIS does not show you alerts when it finds a threat, but automatically deals with it instead. You can choose to automatically quarantine or delete threats if you disable alerts.

- We strongly recommend you leave the real-time scanner enabled at all times.

Configure real-time scans

- Click 'Settings' at the top of the CIS home screen

• Click 'Antivirus' > 'Realtime Scan' on the left
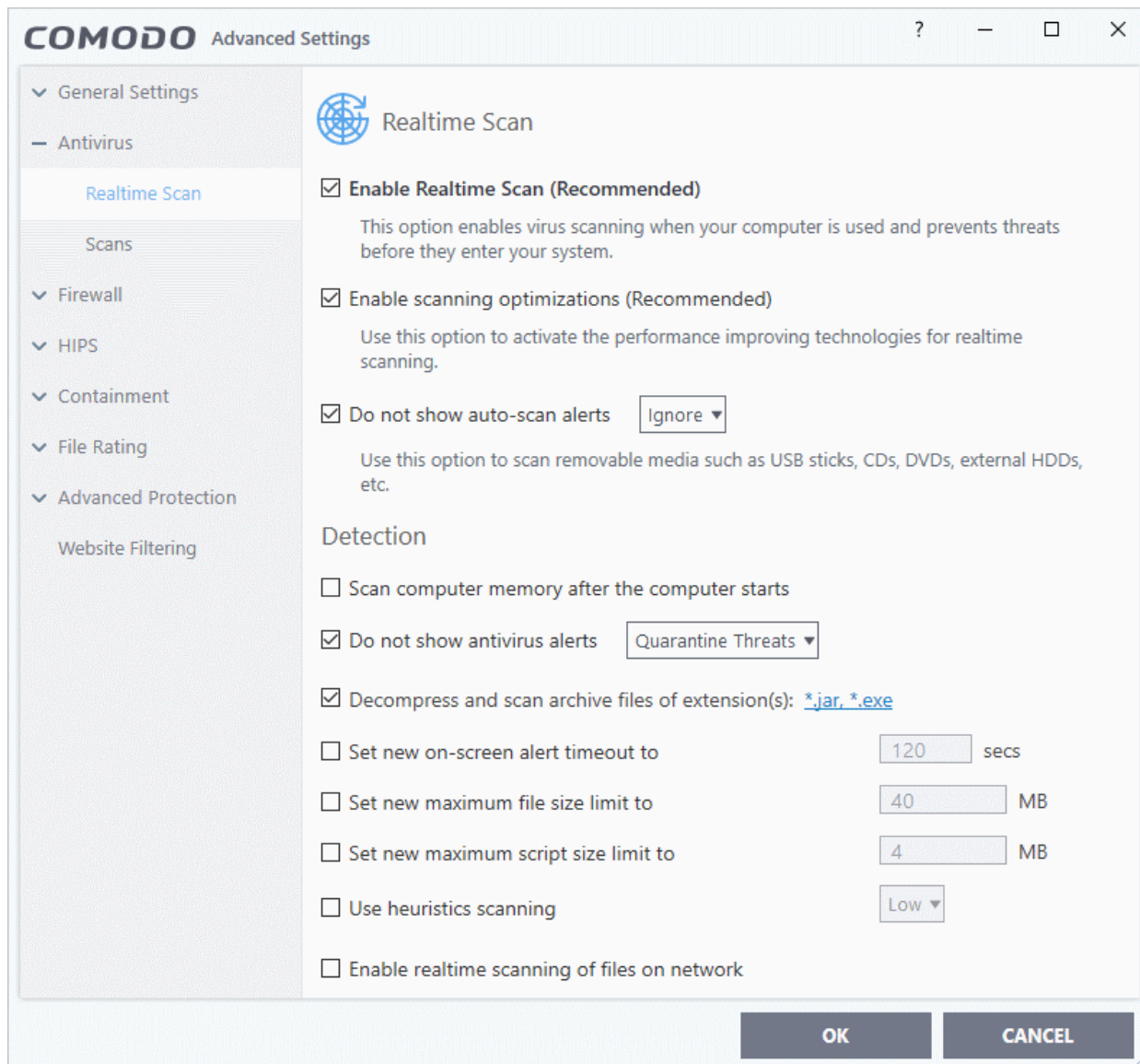
• **Enable Realtime Scan** *(Recommended)* - Activate or deactivate real-time scanning. The real-time scanner continually monitors your computer for malicious activity and protects you from threats as soon as they occur. Comodo strongly recommends you keep this option enabled. *(Default=Enabled)*

• **Enable scanning optimizations** - Will enable various techniques during a virus scan to reduce resource usage and speed-up the scan process. For example, antivirus scans will run in the background. (**Default = Enabled**)

• **Do not show auto-scan alerts** - Choose whether CIS asks if you want to scan removable devices when you plug them in. For example, when you plug in a USB stick, external hard-drive etc.

  • **Enabled** - Alerts are not shown. CIS will automatically take the action you choose in the drop-down box:

    • **Ignore** - The device is not scanned (default)

    • **Scan** - The device is scanned for viruses. The scan uses the settings in the 'Manual Scan' profile. If this is not available then the scan uses the settings in the 'Full Scan' profile.

  • **Disabled** - Alerts are shown when you plug a removable device into your computer. You can choose to scan the device, or skip the scan. An example alert is shown below:

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 CIS finds malware on your computer. (*Default = Enabled*)

   'Do not show antivirus alerts' will minimize disturbance 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** - Prevents the threat from running and moves it to quarantine (*Default*). You can review quarantined files at 'Tasks' > 'Advanced Tasks' > 'View Quarantine'.

   - **Block Threats** - Prevents the threat from running then deletes it from your computer.

   Note: If you disable this option then you will see pop-up alerts when a threat is found. The alert offers you the choice to quarantine or block the threat.

- **Decompress and scan archive files of extension(s)** - 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.
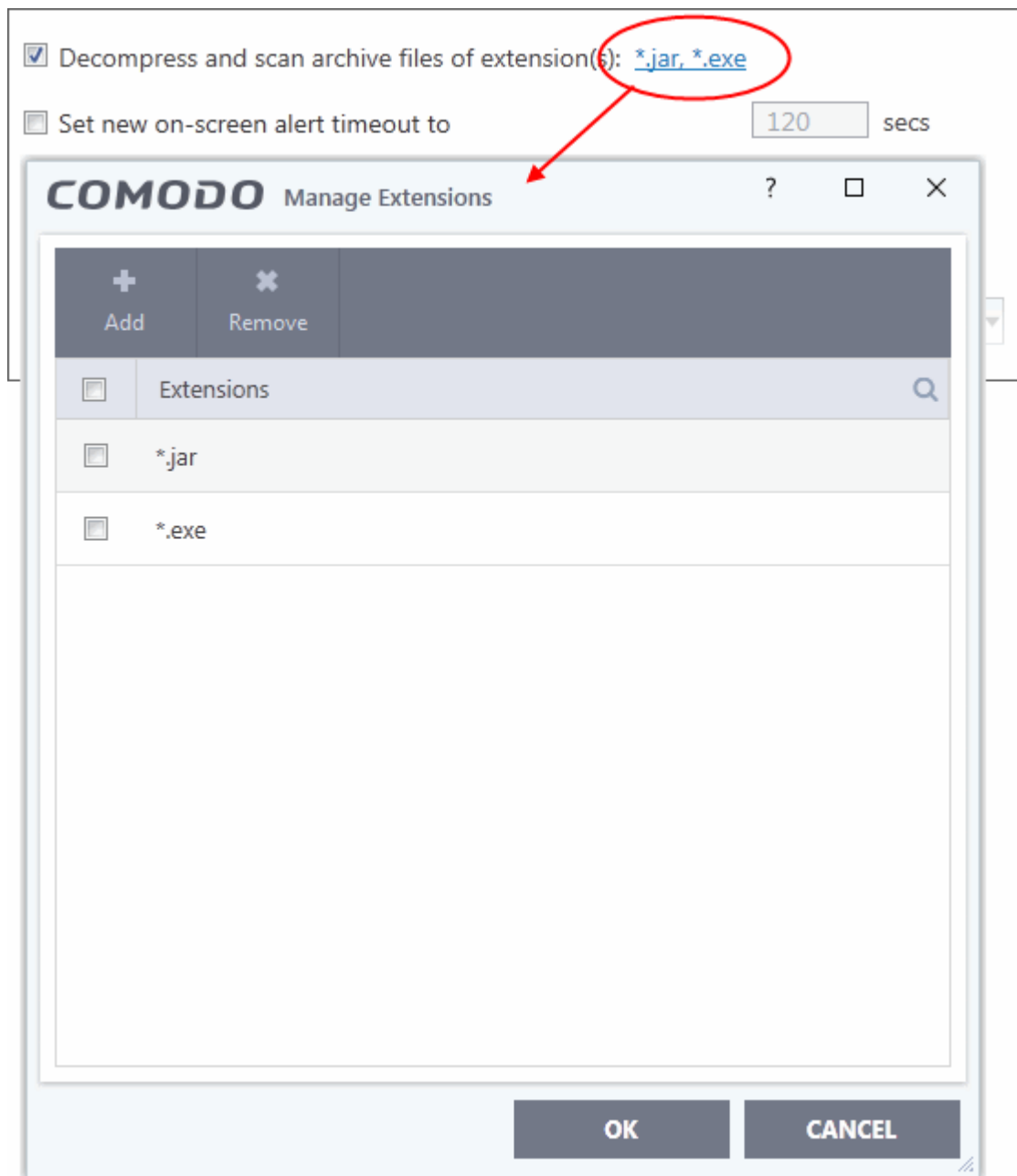
• To add a new archive file type, click 'Add' at the top
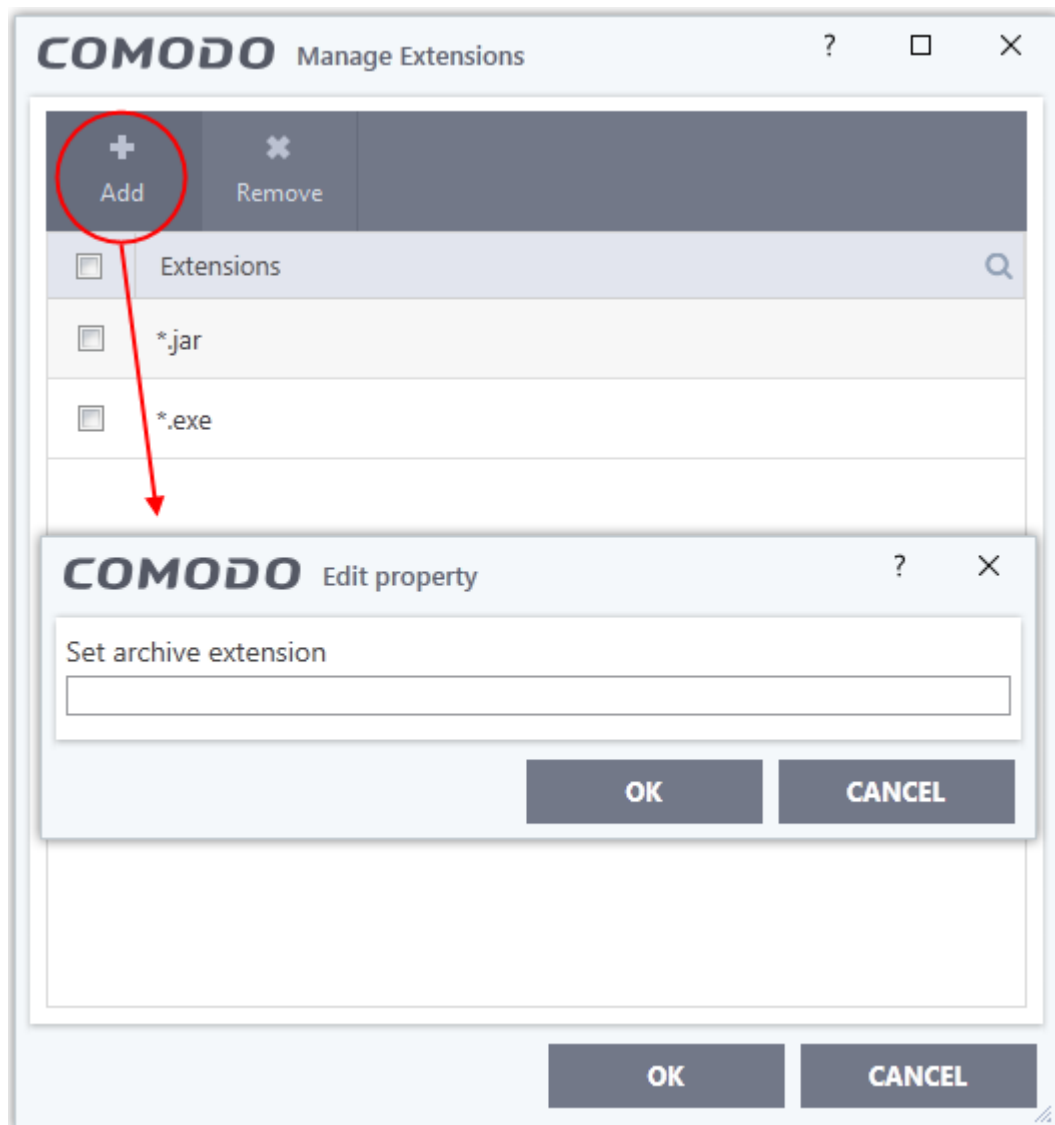
- Enter the extension type you wish to scan and click 'OK'. Example extensions include .zip , .rar, .msi, .7z , .jar and .cab.
- Repeat the process to add more extensions
- Click 'OK' in the 'Manage Extensions' dialog
- To remove an archive file type, choose the file type from the list, click 'Remove' from the top and click 'OK' in the 'Manage Extensions' dialog.

- **Set new on-screen alert timeout to** - Specify the length of time that virus alerts should stay on the screen. *(Default = 120 seconds)*

- **Set new maximum file size limit to** - Specify the largest file size that the antivirus should scan. CIS will not scan files bigger than the size specified here. **(***Default = 40 MB***)**

- **Set new maximum script size limit to** - Specify the largest script size that the antivirus should scan. CIS will not scan scripts bigger than the size specified here. **(***Default = 4 MB***)**

- **Use heuristics scanning** - Enable or disable heuristic scans, and define the sensitivity of the scanner. *(Default = Enabled)*

Background. Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CIS to detect brand new viruses even that are not in the current virus database.

If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

- **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

  Despite the name, this setting combines a very 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 possible false positives.
- **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and 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

- Click 'Settings' > 'Antivirus' > 'Scans'

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.

Open the 'Scans' panel

- Click 'Settings' at the top of the CIS home screen
- Click 'Antivirus' > 'Scans'
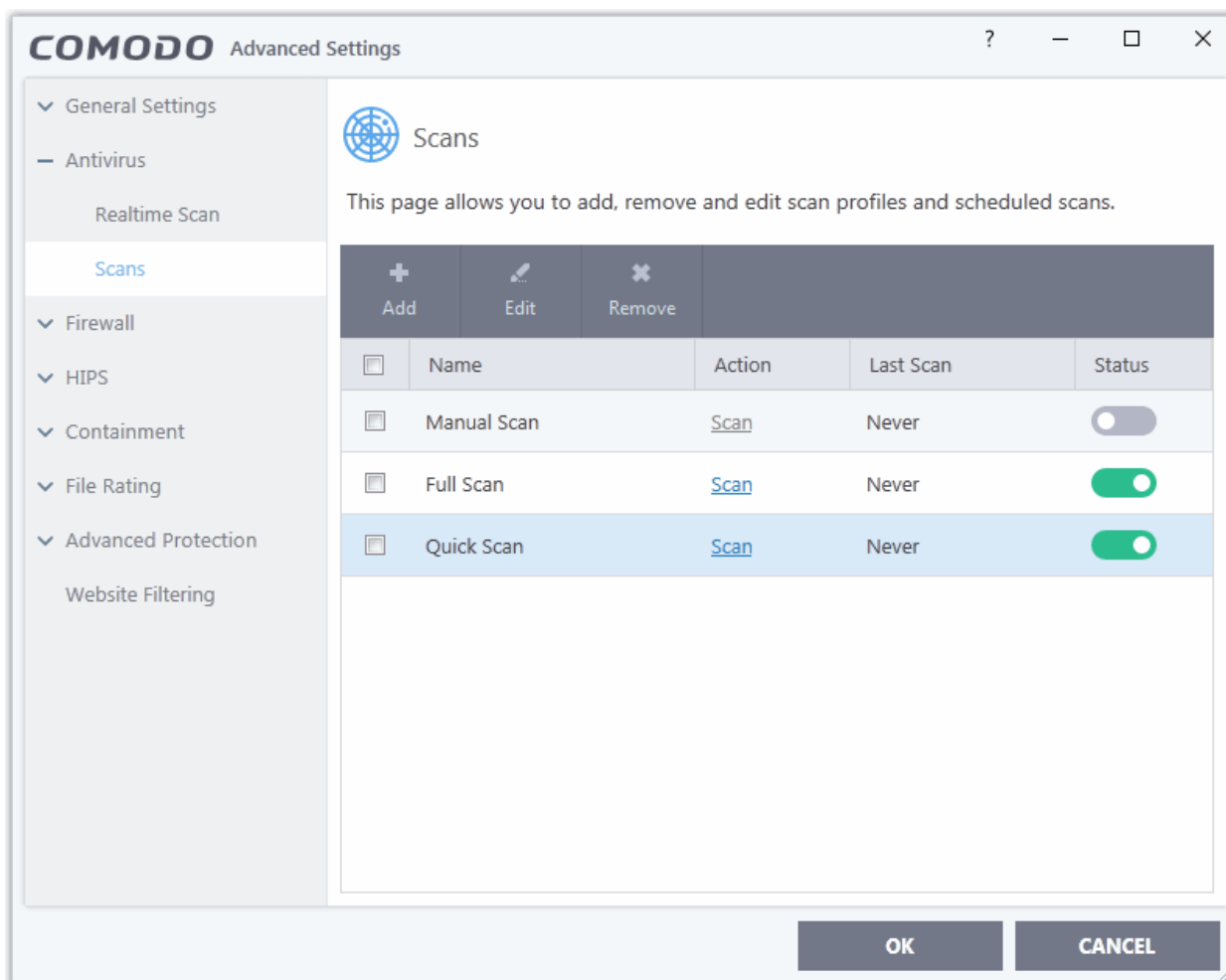
The 'Scans' panel displays a list of pre-defined and user defined scan profiles.

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:

- **Create a Scan Profile**
- **Run a custom scan**

Create a custom profile

- Click 'Settings' at the top of the CIS home screen
- Click 'Antivirus' > 'Scans'

- Click 'Add' from the options at the top.

The profile configuration screen will open:
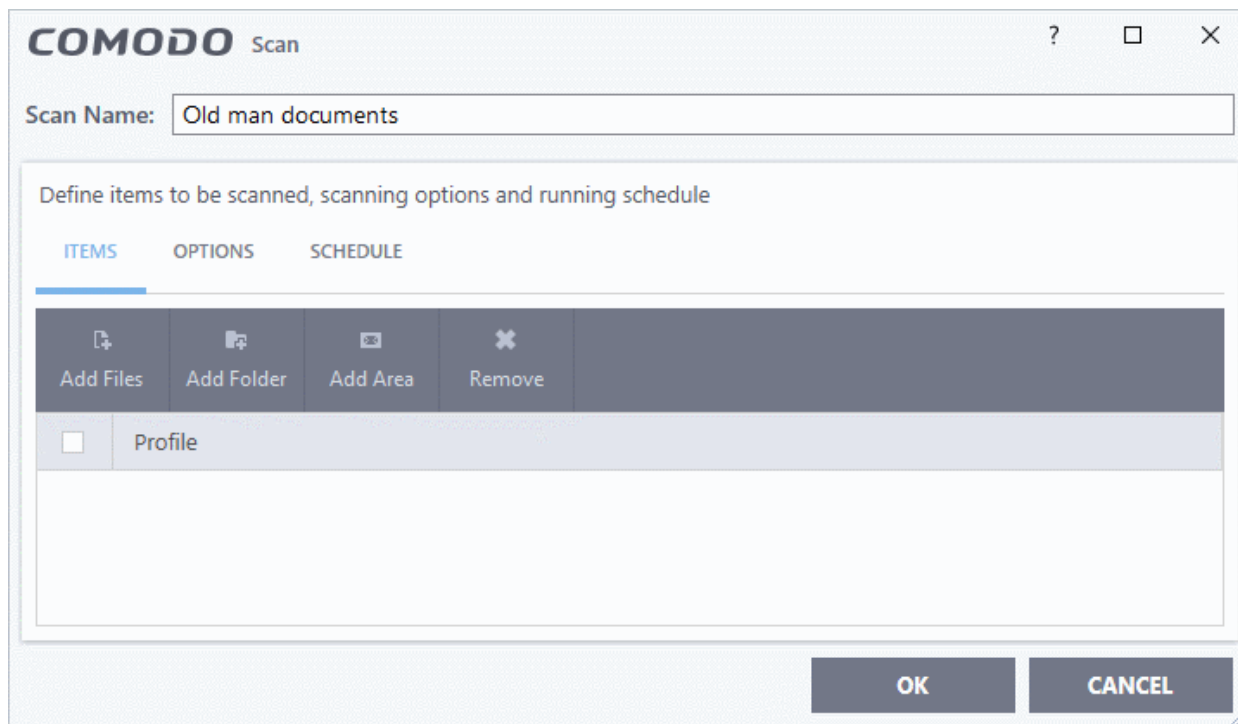
- Type a name for the profile in the 'Scan Name' text box.

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** - Specify individual files to be scanned. Click the 'Add Files' button and navigate to the file you want to include in the scan. Repeat to add more files.
- **Add Folder** - Specify entire folders to be scanned. Click the 'Add Folder' button and choose the folder from the 'Browse for Folder' dialog.
- **Add Area** - Select pre-defined regions to be scanned. Regions include 'Full Computer', 'Commonly Infected Areas' and 'Memory'.
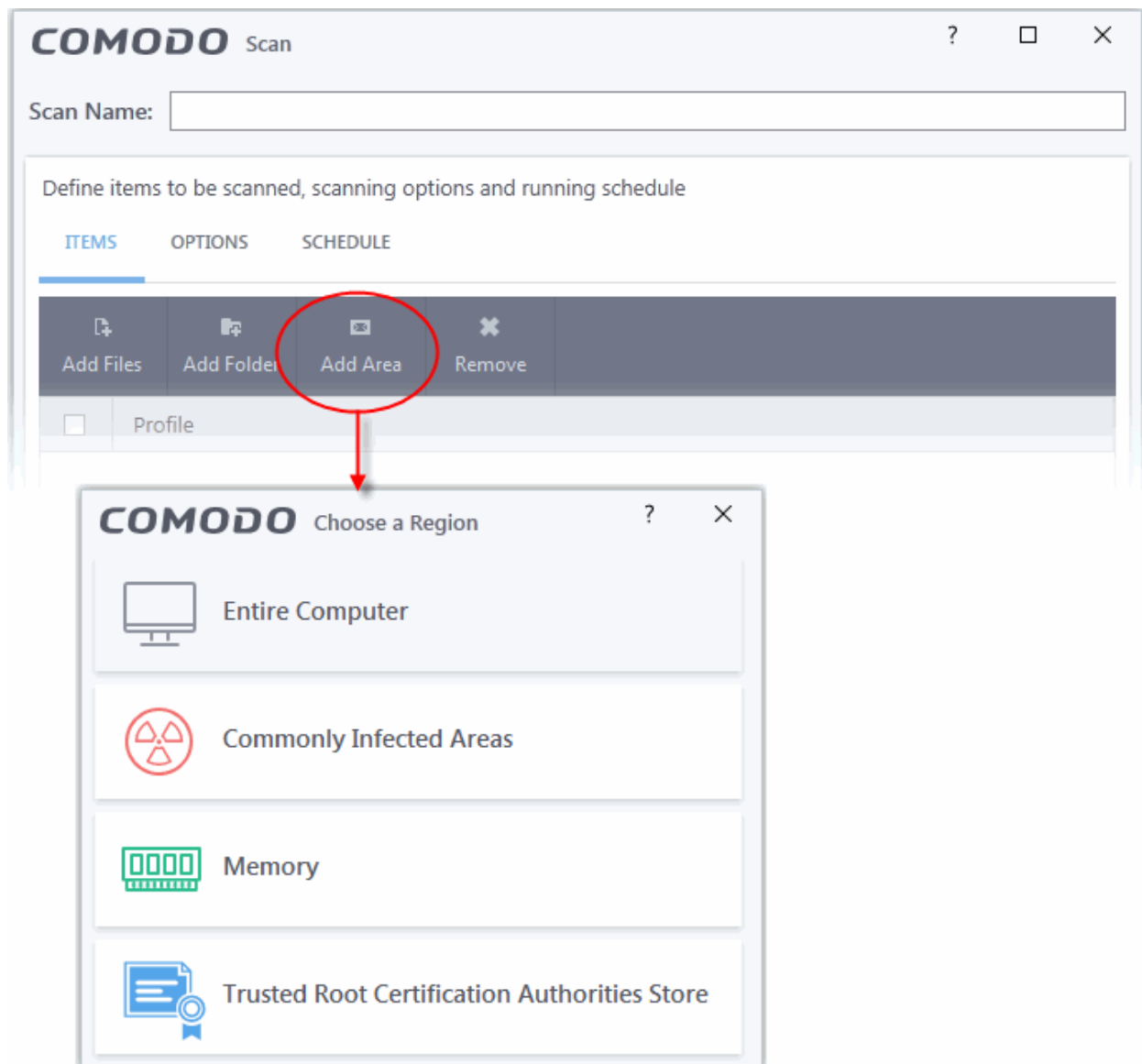
- Repeat the process to add more items to the profile. You can mix-and-match files, folders and areas in your custom scan.

Configure scan options

- Click 'Options' at the top of the scan interface
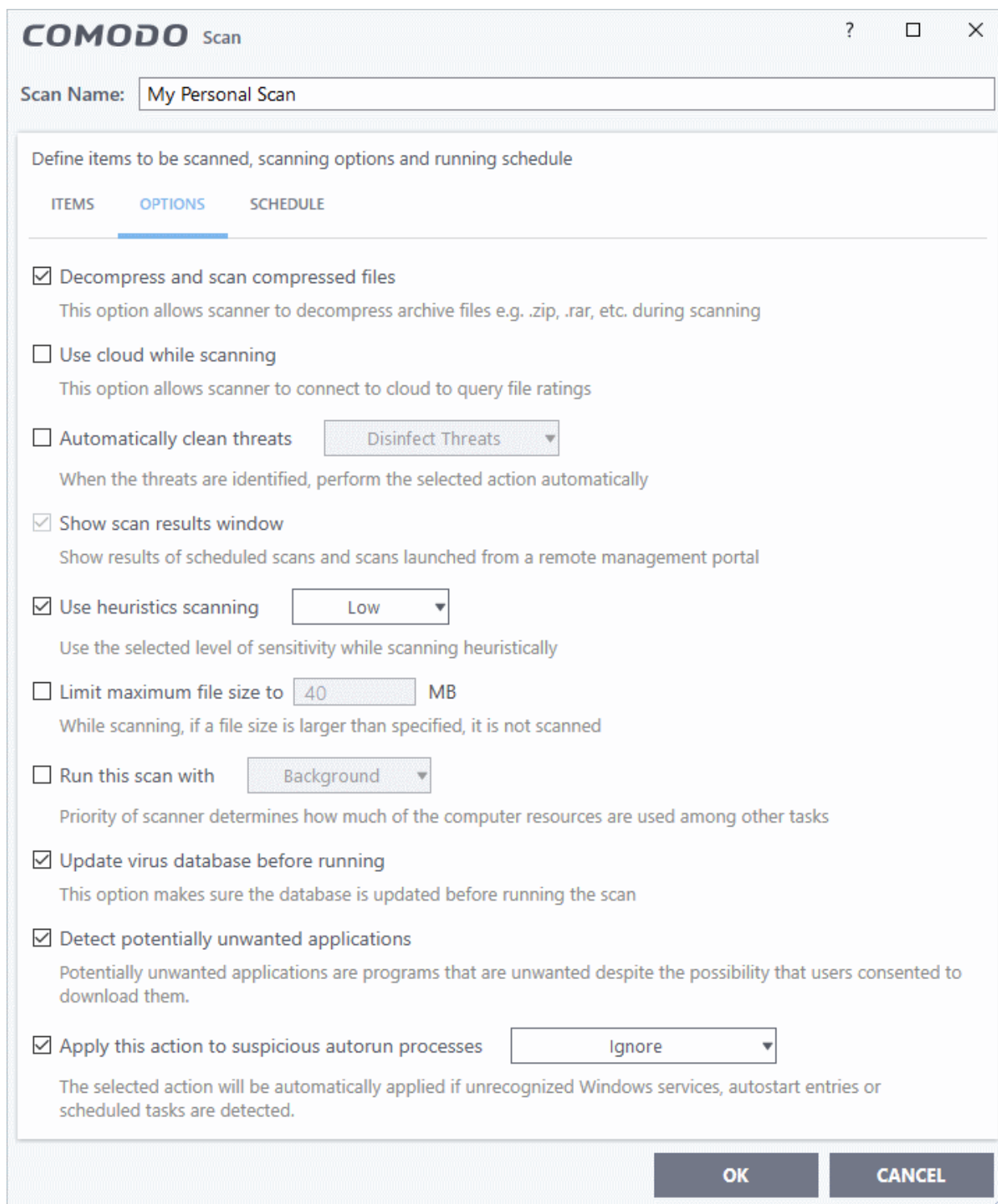
- **Decompress and scan compressed files** - The scan will include archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives *(Default = Enabled)* .

- **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** - Whether or not CIS should automatically remove any malware found by the scan.

  - **Disabled** = Results are shown at the end of the scan with a list of any identified threats. You can select the action to be taken on them individually, or on all items at-once. See **Process Infected Files** for guidance on manually handling detected threats. (*Default*)

  - **Enabled** = You can 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'.

- **Show scan result window** - 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** - Enable or disable heuristic scans, and define the sensitivity of the scanner. (**Default = Enabled**)

  Background. Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CIS to detect brand new viruses even that are not in the current virus database.

  If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

  - **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

    Despite the name, this setting combines a very 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 possible false positives.
  - **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.

- **Limit maximum file size to** - Specify the largest file size that the antivirus should scan. CIS will not scan files bigger than the size specified here **(Default = 40 MB)**.

- **Run this scan with** - Whether you want to set a priority for the scans with this profile
  - **Enabled** = You can set the priority. The available options are:
    - High
    - Normal
    - Low
    - Background.
  - **Disabled** = The scan will be run at the background (**Default**)

- **Update virus database before running** - CIS checks for and downloads the latest virus signatures before starting every scan with this profile (**Default = Enabled**) .

- **Detect potentially unwanted applications** - The antivirus also scans 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 installing another 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).**

- **Apply this action to suspicious autorun processes** - Specify how CIS should handle unrecognized auto-run items, Windows services and scheduled tasks.
  - **Ignore** - The item is allowed to run
  - **Terminate** - CIS stops the process / service
  - **Terminate and Disable** - Auto-run processes will be stopped and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.
  - **Quarantine and Disable** - Auto-run processes will be quarantined and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.

  Note 1 - This setting monitors only registry records during the on-demand scan. To monitor the registry at all times, go to 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'.

- See **Miscellaneous Settings** for more details

Note 2 - CIS ships with a list of applications for which script analysis will be performed to protect the registry records. You can manage the list of applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

- See '**Autorun Scans**' in **Script Analysis Settings** for more details.

Schedule the scan

- Click 'Schedule' at the top of the scan interface.

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 few hours** - Run the scan at the intervals of the hours specified in 'Repeat scan every NN hour(s)'

- **Every Day** - Run the scan daily 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.

Run a custom scan as per a scan profile

- Click 'Tasks' > 'General Tasks' > 'Scan'

- Click 'Custom Scan' from the 'Scans' interface

- Click 'More Scan Options' from the 'Custom Scan' pane

The 'Advanced Settings' interface will open at the 'Scans' panel.

- Click 'Scan' beside the required scan profile.
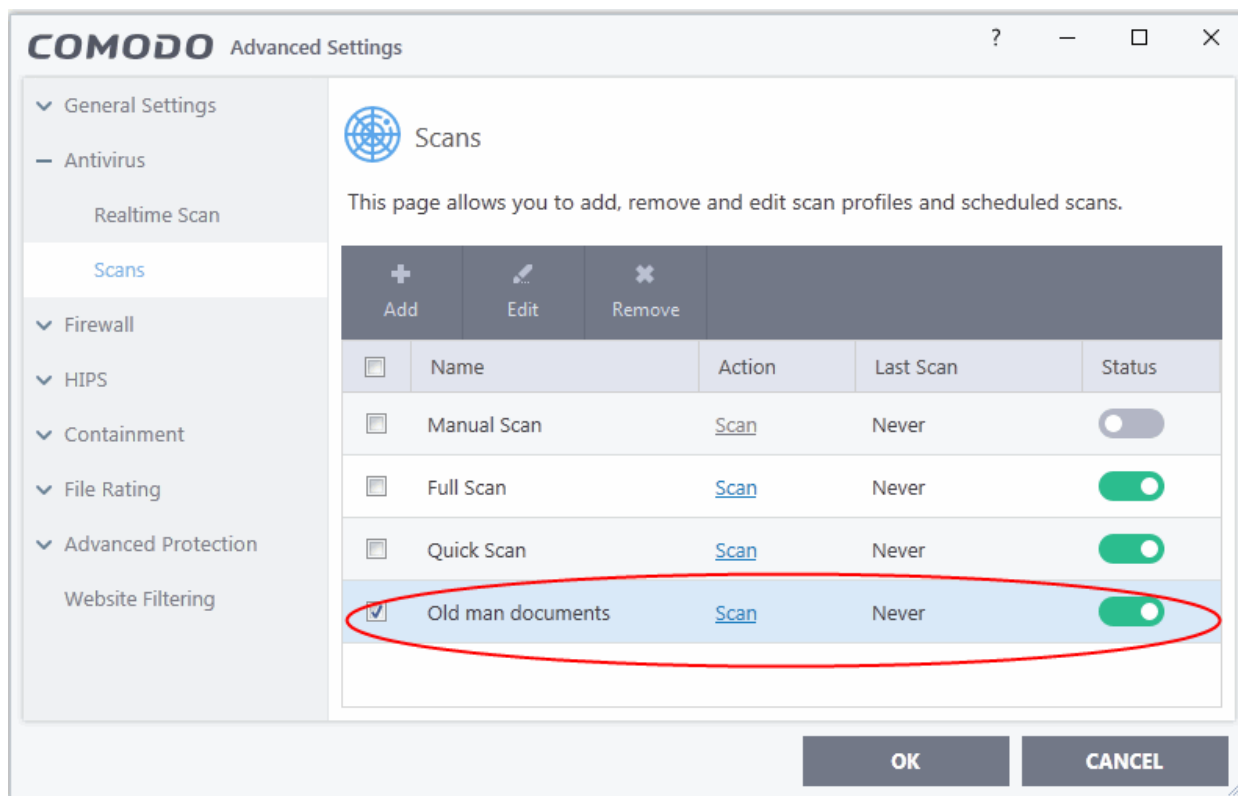
The scan will start immediately. Results will be displayed afterwards:
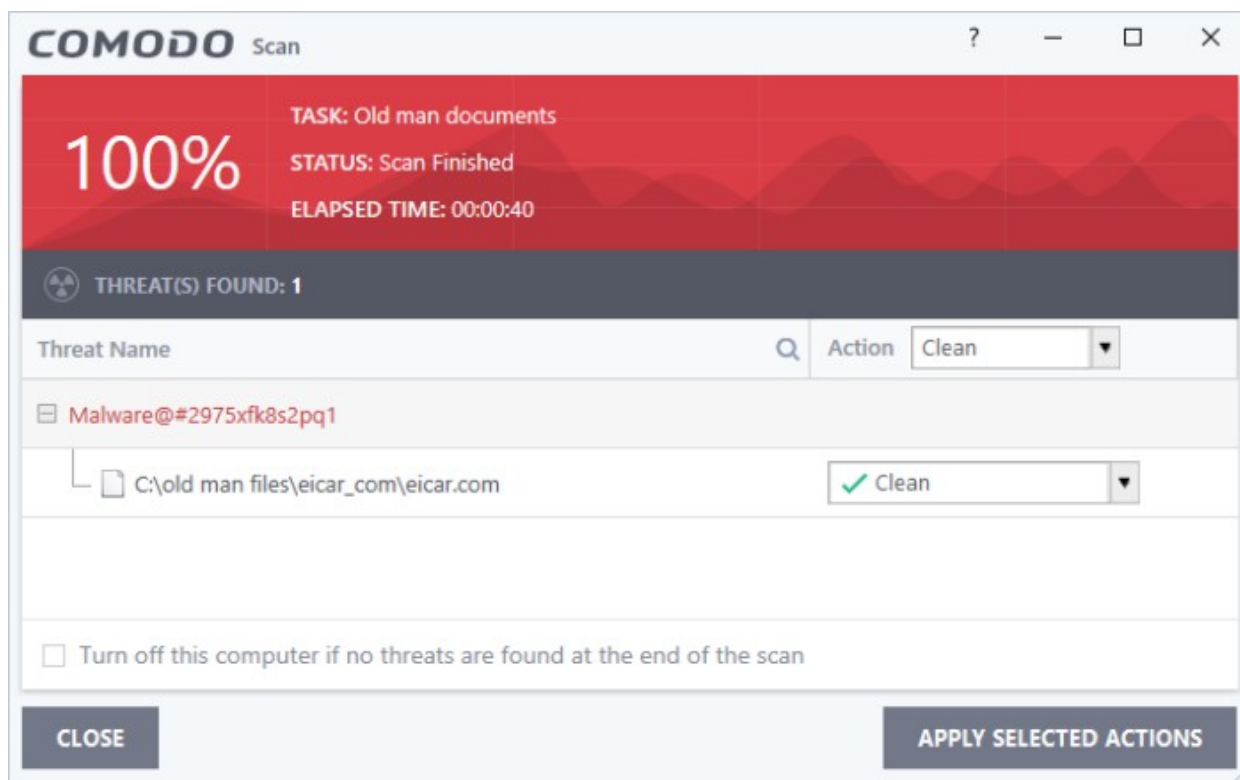
The scan results window displays the number of objects scanned and the number of threats discovered. You can choose to clean, move to quarantine or ignore the threat based on your assessment. See **Processing infected files** for more details.

Edit Predefined and Custom Scan Profiles

- Click 'Settings' at the top of the CIS home screen
- Click 'Antivirus' > 'Scans'
- Select the profile that you want to update from the list and click 'Edit' at the top

---
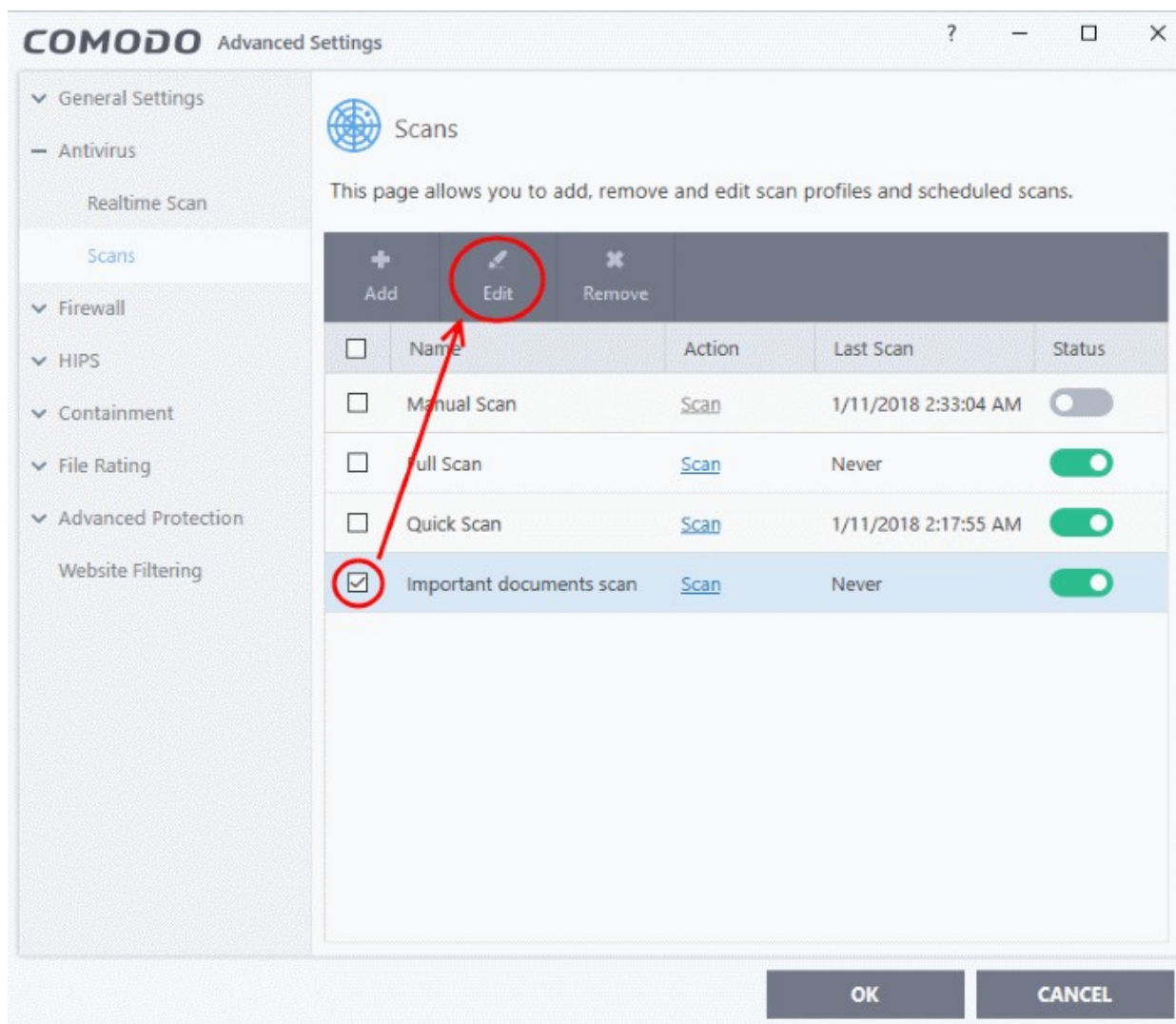
- This will open a screen which allows you to add items, configure options and schedule scans
- Update the profile settings as required. The procedure is similar to **creating** a new profile as explained above.
- Note: you cannot edit the predefined 'full' and 'quick scan' profiles.

Remove Custom Scan Profiles

- Click 'Settings' at the top of the CIS home screen
- Click 'Antivirus' > 'Scans'
- Select the profile that you want to remove from the list and click 'Remove' at the top
- Note: you cannot delete predefined scan profiles (Manual, Full and Quick scans)

6.3. Firewall Configuration

Click 'Settings' > 'Firewall'

- The firewall protects your computer 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.
- The simple rules interface lets you specify exactly which applications can access the internet.
- You can choose to receive alerts if the firewall detects suspicious activity, or have the firewall auto-implement a specific action.

Configure the 'Firewall' module

- Click 'Settings' on the CIS home screen
- Click 'Firewall' on the left:
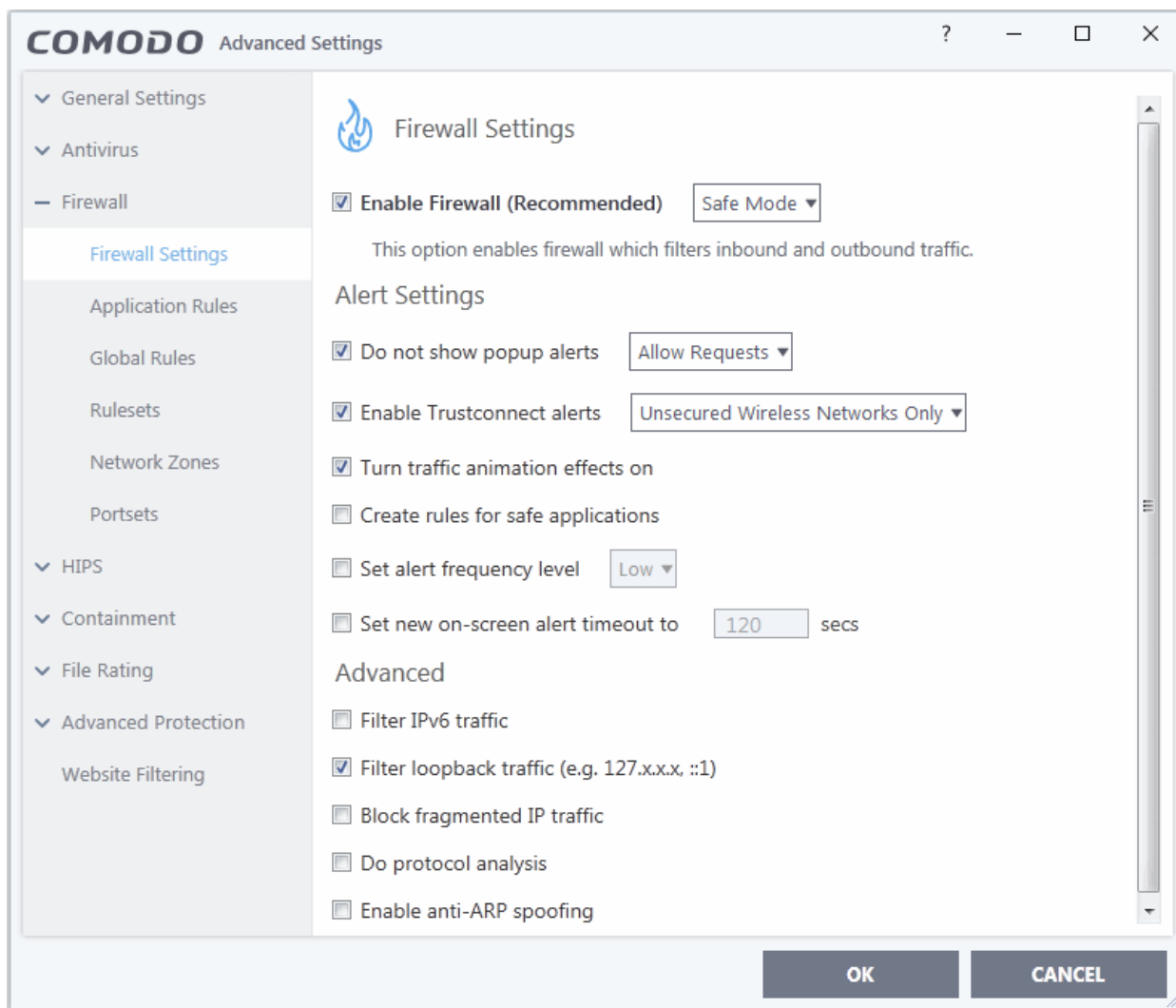
Firewall settings has the following sections:

- **General Firewall Settings** - Settings that govern the overall behavior of the firewall.
- **Application Rules** - Rules which control the network access rights of specific applications, or types of application.
- **Global Rules** - Rules which apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Collections of rules that can be applied to internet capable applications like browsers and email/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 decides whether to allow or block a connection:
Outgoing connections - Application rules are consulted first then global rules.
Incoming connections - Global rules are consulted first then application rules.

6.3.1. General Firewall Settings

Click 'Settings' > 'Firewall' > 'Firewall Settings'

- Firewall settings let you quickly configure the overall behavior of the firewall. Settings are divided into three main areas:

    - **General Settings**
    - **Alert Settings**
    - **Advanced Settings**
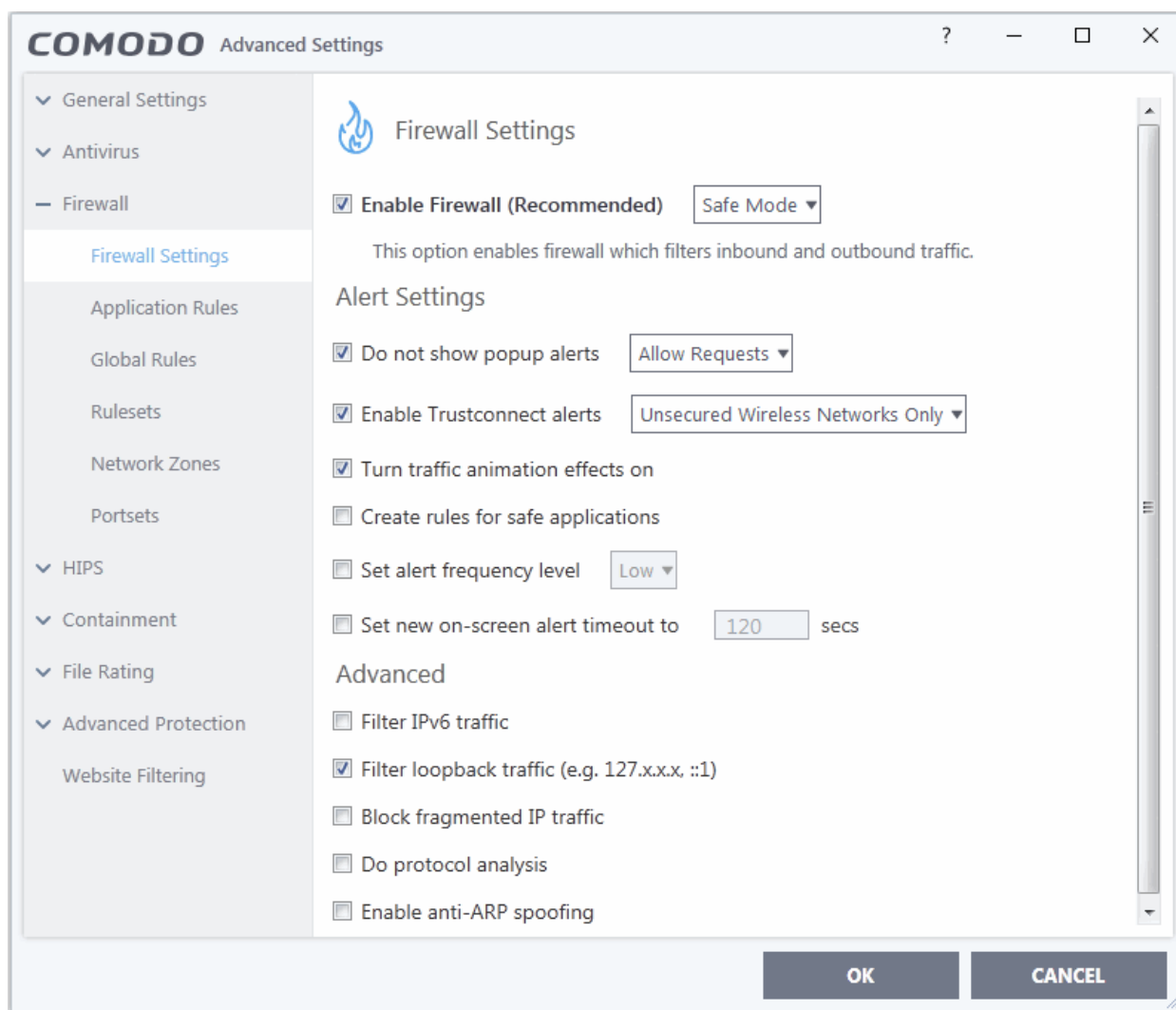
General Settings

- **Enable Firewall** - Activate or deactivate firewall protection. (***Default and recommended = Enabled***)

    - If enabled, you can also choose the security level from the drop-down menu:
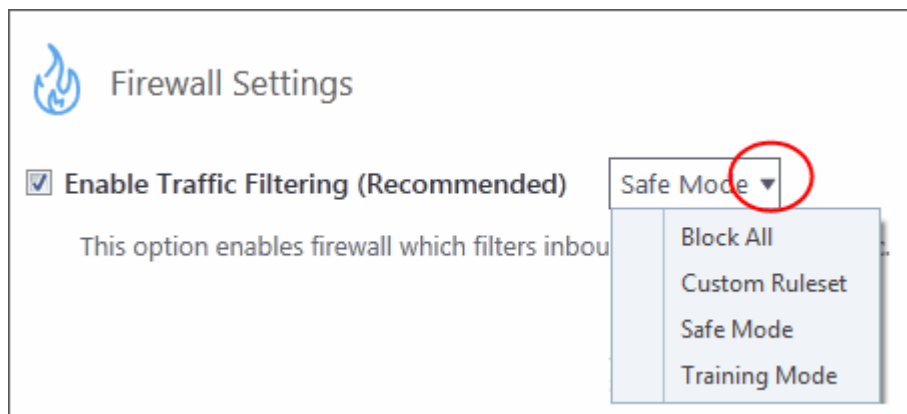
The choices available are:

- **Block All**: The firewall stops all traffic in and out of your computer, regardless of any other settings or rules. The firewall does not attempt to learn the behavior of any application, and does not create traffic rules for any applications. This option prevents your computer from accessing any networks, including the internet.

- **Custom Ruleset Mode:** The firewall applies ONLY **network traffic rules** that you have created. 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 an 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 creates automatic allow rules for all new applications. You will not receive any alerts in 'Training Mode' mode. This mode is intended for advanced users and admins who want to trust existing files on their network. The idea is to keep the firewall in training mode for approximately a week to create a 'baseline' of trusted files. If you choose 'Training Mode', 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** - 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'.
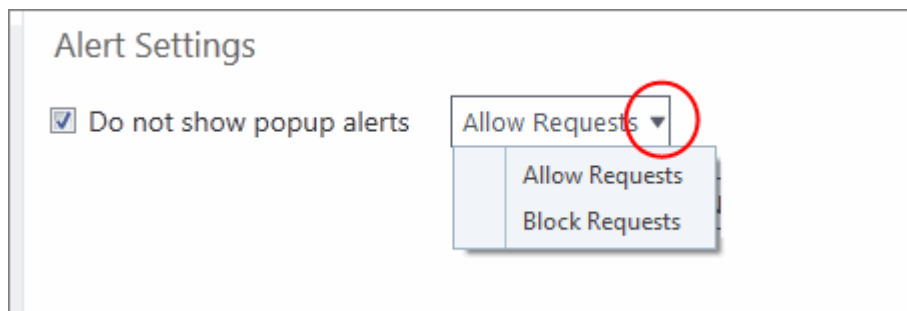
- **Enable Trustconnect alerts** - If you connect to the internet at a public place like an airport or a coffee shop then you are potentially exposing yourself to danger. Insecure public networks can allow others to eavesdrop on your communications or even gain access to your computer. To safeguard against such attempts, Comodo recommends you encrypt your connection at public hotspots with 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:
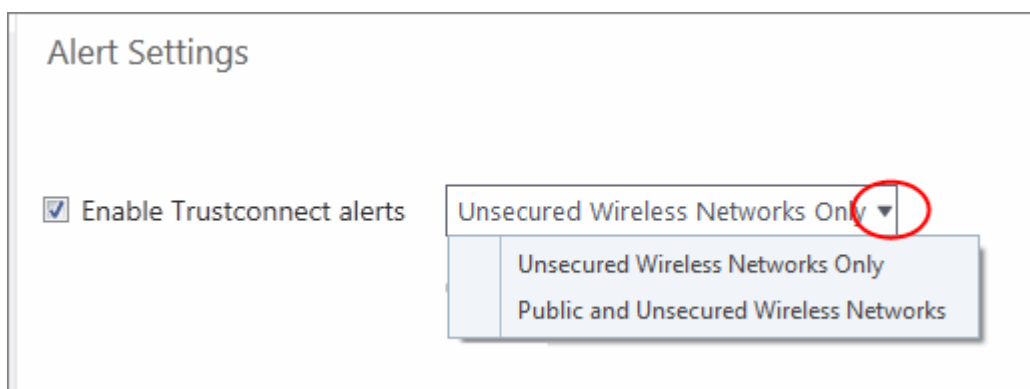
  - **Unsecured Wireless Networks Only** - Alerts are only shown if you connect to an unencrypted wireless network. *(Default)*
  - **Public and Unsecured Wireless Networks only** - Alerts are shown when you connect to an unencrypted network OR a public WiFi.

You will be alerted and offered the opportunity to secure the connection via the following notification:
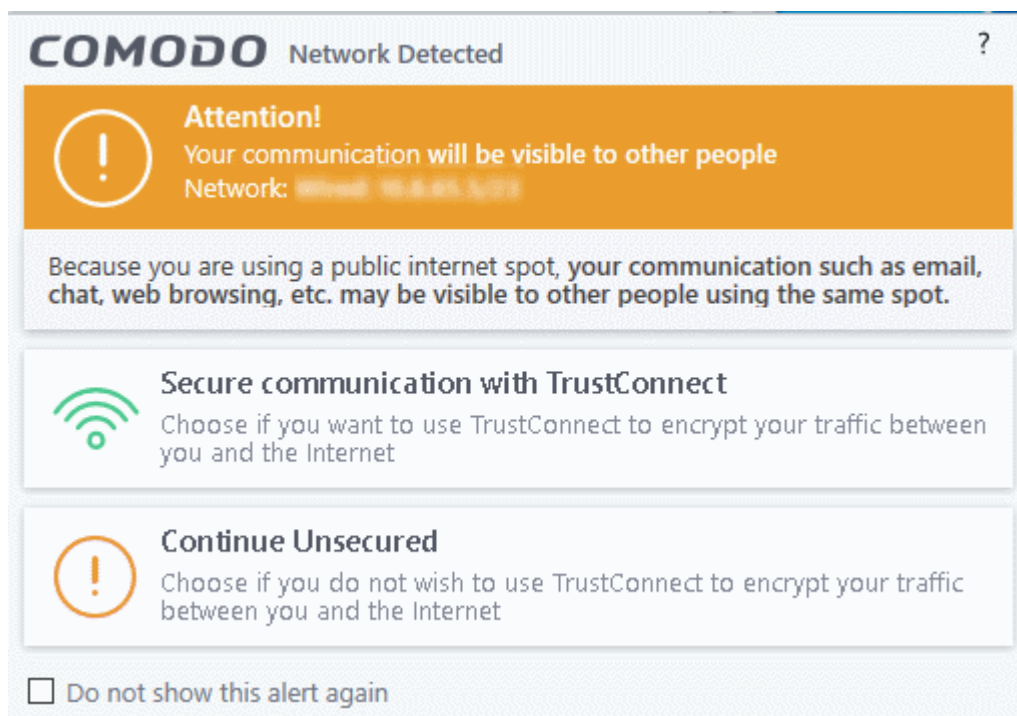
Note: TrustConnect is only available with CIS Complete. On clicking 'Secure communication with TrustConnect', the users of Comodo Internet Security Premium and CIS Pro are taken to the product upgrade page. See **TrustConnect Overview** for more details.

- **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.
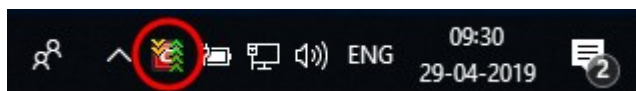
If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the icon. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer.

- 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 is on the Comodo safe list, a global white-list of trusted software.
  - The application has a 'Trusted' rating in the local file list. See **File List** if you need more details.
  - The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file. See **Vendor List** if you need more details.

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 setting 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** - Configure the amount of alerts that the firewall generates. Please note that this does not affect your security level, which is determined by the actual rules you have in place (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 suspicious behavior while not getting overwhelmed with alerts. *(Default=Disabled)*
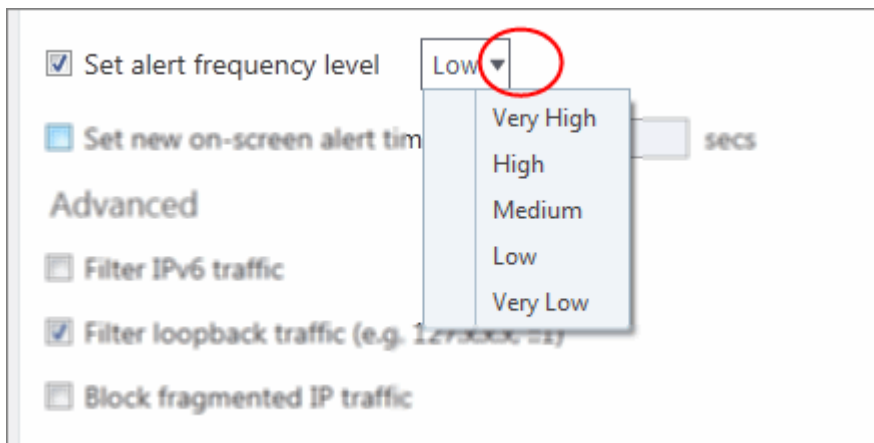
- **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but 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**: How long a firewall alert remains on-screen if it is not answered. The default timeout is 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

Click 'Settings' > 'Firewall' > 'Application Rules'

- Application rules let you manage network access rights for specific applications.

- Whenever an application makes a request for network access, CIS allows or denies the request based on the ruleset applied to the application.

- Firewall rulesets are made up of one or more application rules. Each rule outlines an application's permissions regarding a specific type of traffic.

Rules and Rulesets

- Whenever an application makes a request for network access, CIS allows or denies the request based on the ruleset applied to the application.

- Firewall rulesets are made up of one or more application rules.

- Each rule outlines the application's permissions regarding a specific type of traffic.

Manage Application Rules

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Application Rules'.
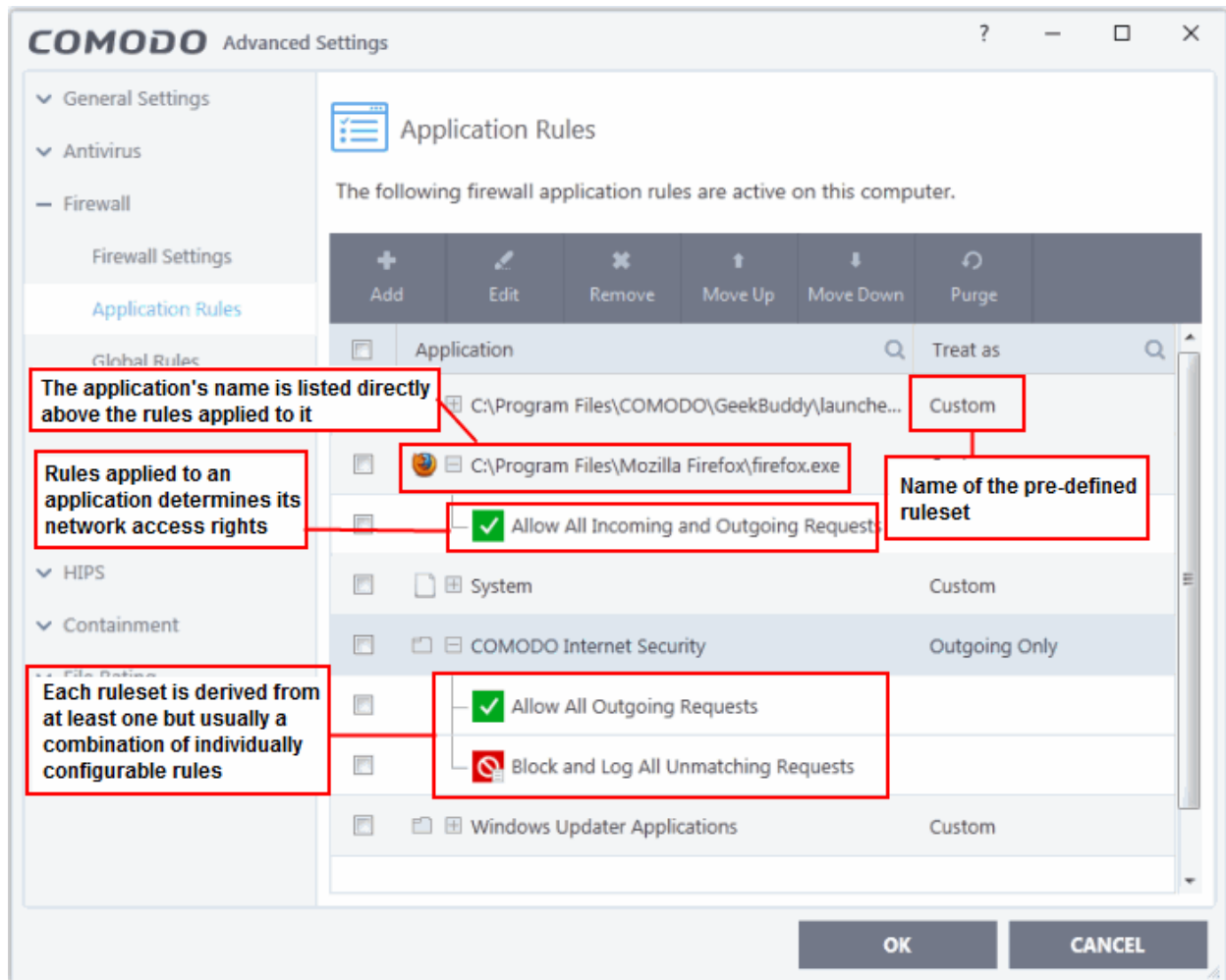
- **Application** - Programs or file groups for which a firewall ruleset has been created. In the case of file groups, all member applications will use the ruleset of the group.

  - Click '+' next to the name to view the rules which apply to the application/group.
- **Treat as** - Name of the ruleset assigned to the application or group.

The controls above the table let you manage the rule sets:
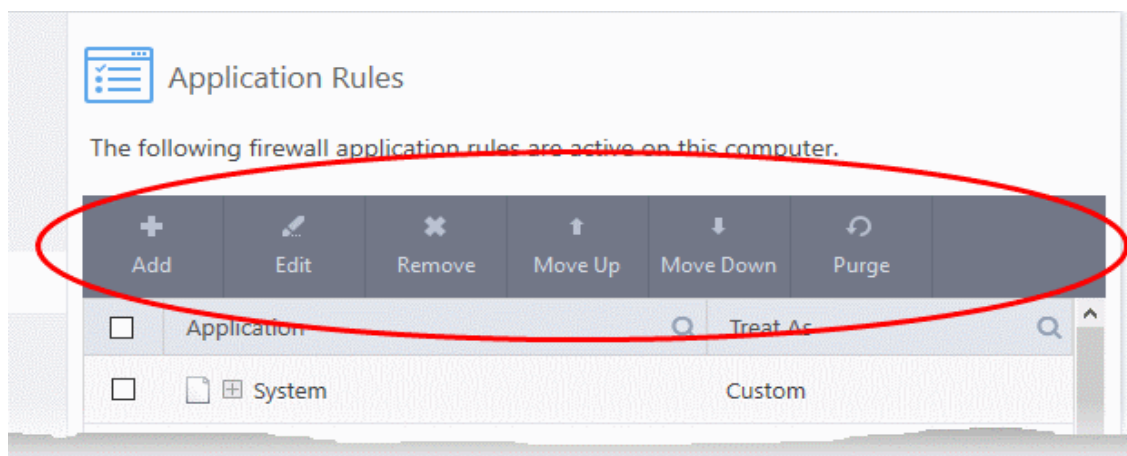
- **Add** - Add a new application/application group then create a ruleset for it.
- **Edit** - Modify an application rule/ruleset.

- **Remove** - Delete the selected rule.
- **Purge** - Check that all applications mentioned in a ruleset are still installed at the paths specified. If not, the rule is removed from the list.
- **Move Up** and **Move Down** - Rules are prioritized top-to-bottom, with those at the top having the higher priority. The 'Move Up' and 'Move Down' buttons let you change the priority of a selected rule.

Predefined rulesets

- Although you could create a ruleset from the ground-up by configuring its individual rules, this practice would be time consuming if performed for every program on your system.
- For this reason, Comodo provide a selection of rulesets according to broad application category. For example, the 'Web Browser' ruleset is designed for applications like 'Internet Explorer', 'Firefox' and 'Chrome'.
- Each predefined ruleset optimizes security for a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see **Predefined Rule Sets.**

Create a firewall ruleset

- **Step 1 - Select the target application or group**
- **Step 2 - Configure the rules**

Step 1 - Select the target application or group

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Application Rules'
- Click the 'Add' button

The 'Application Rule' interface appears:
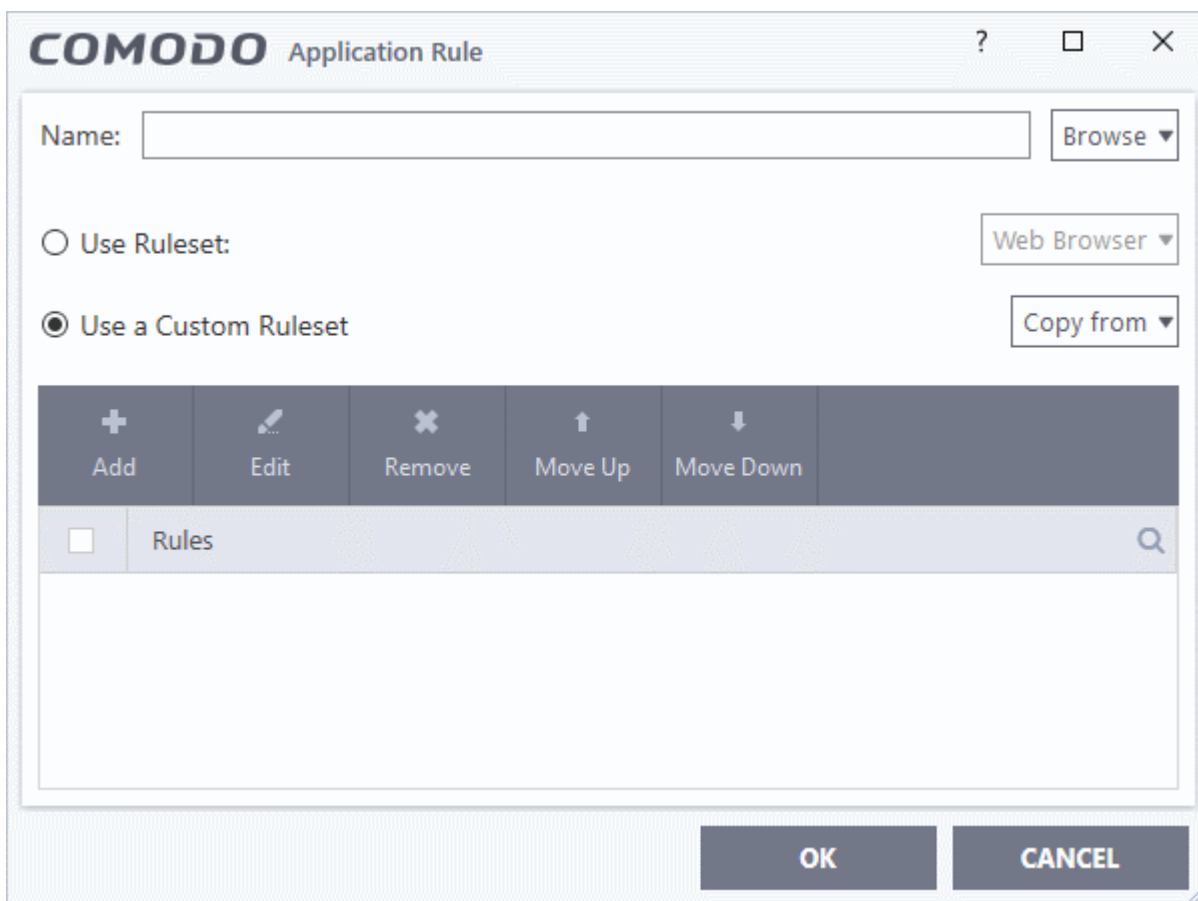
- Click the 'Browse' button beside the 'Name' field:
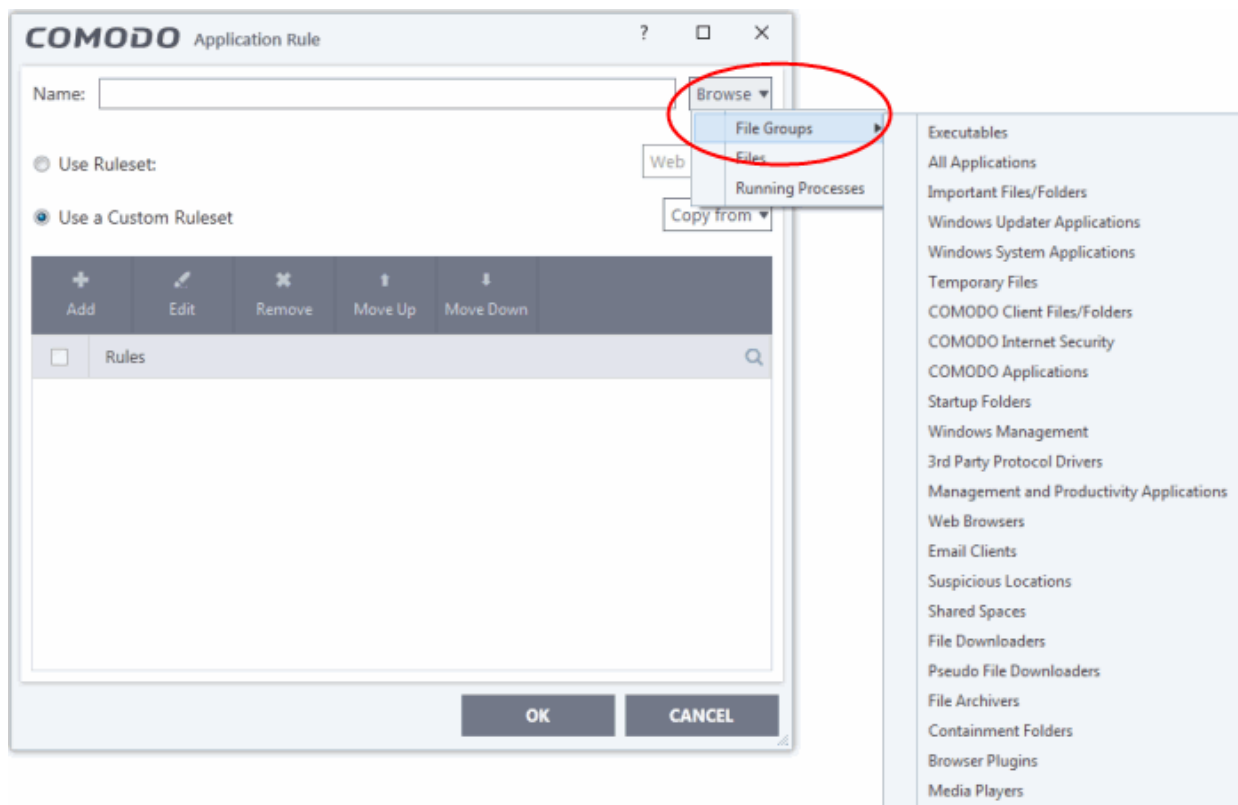
There are three types of target you can add:

- **File Groups** - Apply the ruleset to a predefined file group. All members of the group are covered by the rule. See **File Groups** if you need help with file groups.

- **Files** - Apply the ruleset to a specific application.

- **Running Processes** - Apply the ruleset to an application by selecting its running process

Add a File Group

A file group is category of files or folders. For example, 'Executables', 'Media Players', or 'Important Files/Folders'. See **File Groups** more help with them.

- Choose 'File Groups' from the 'Browse' drop-down.
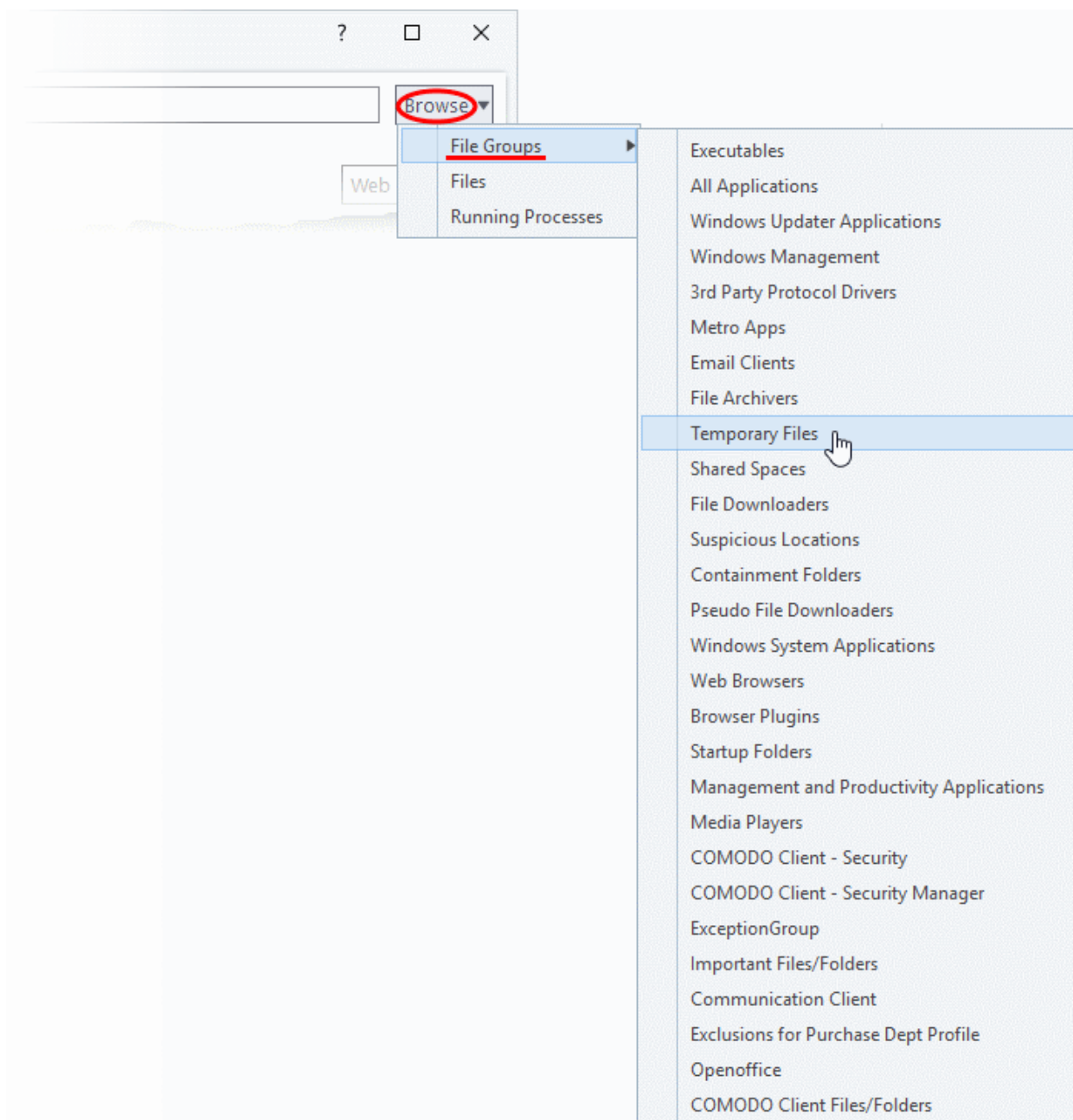
- Select a file group from the drop-down. The ruleset will apply to all executable files in the group.

  - The next stage is **Step 2 - Configure the rules** for the selected file group.

Add an individual File

- Choose 'Files' from the 'Browse' drop-down:
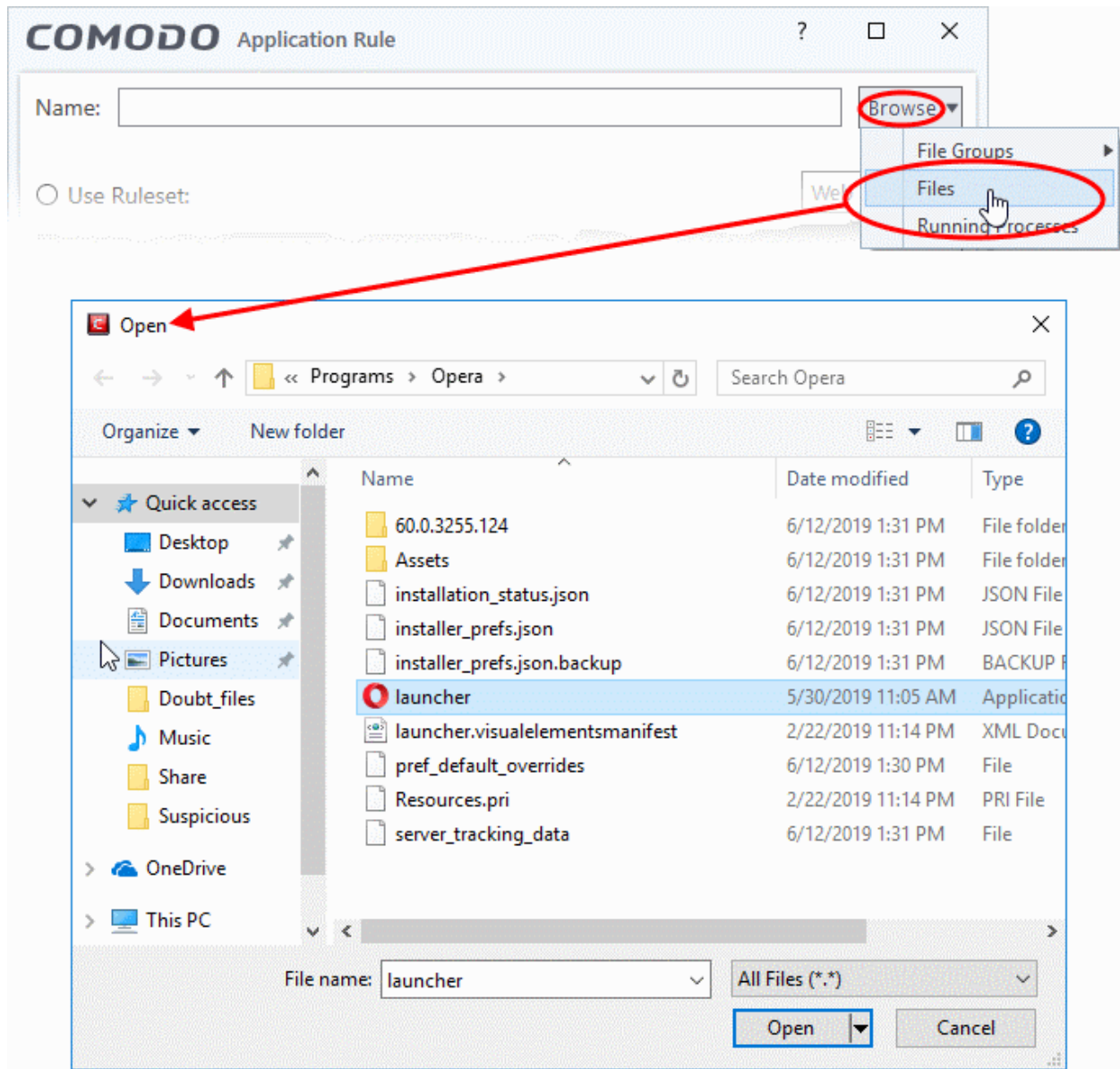
- Navigate to the file you want to add as target and click 'Open'. The rule will apply only to the specific application.

  - The next stage is **Step 2 - Configure the rules** for the selected application.

Add a currently running application by choosing its process

- Choose 'Running Processes' from the 'Browse' drop-down.
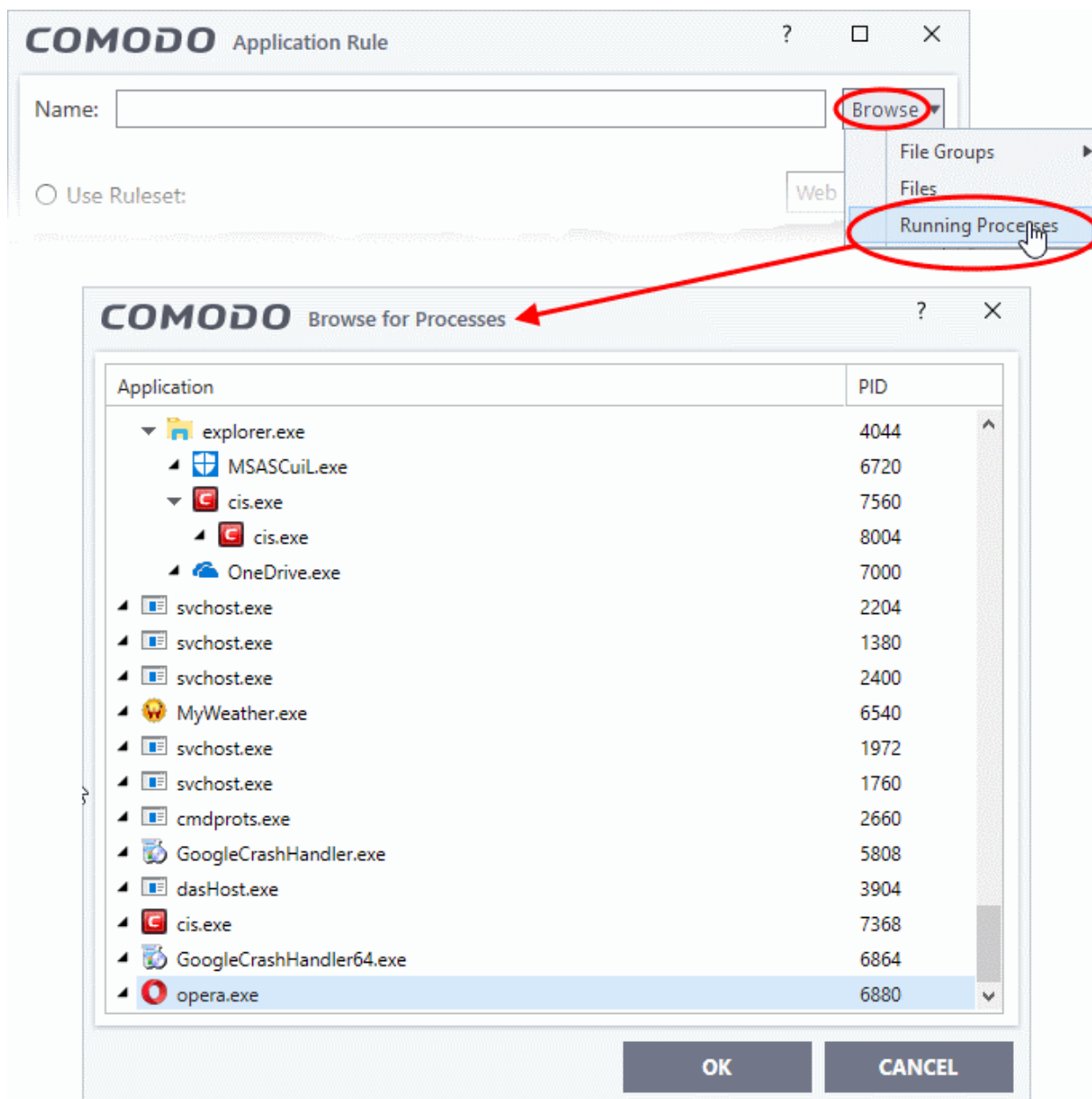
- Select the target process and click 'OK'. The parent application of the process will be added as the target.

The next stage is Step 2 - Configure the rules for the selected application.

Step 2 - Configure the rules in ruleset

There are two broad options available for creating a ruleset. - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

Use Ruleset

- A ruleset is a collection of rules designed to implement optimum security on a specific type of application. You can manage and create rulesets in 'Settings' > 'Firewall Configuration' > 'Firewall Rule Sets'.

- Comodo provides a range of curated rulesets for popular types of application. These include 'Web browser', 'FTP client' and 'Email client'.

- The example below shows us applying the 'Web Browser' ruleset to the Opera browser:
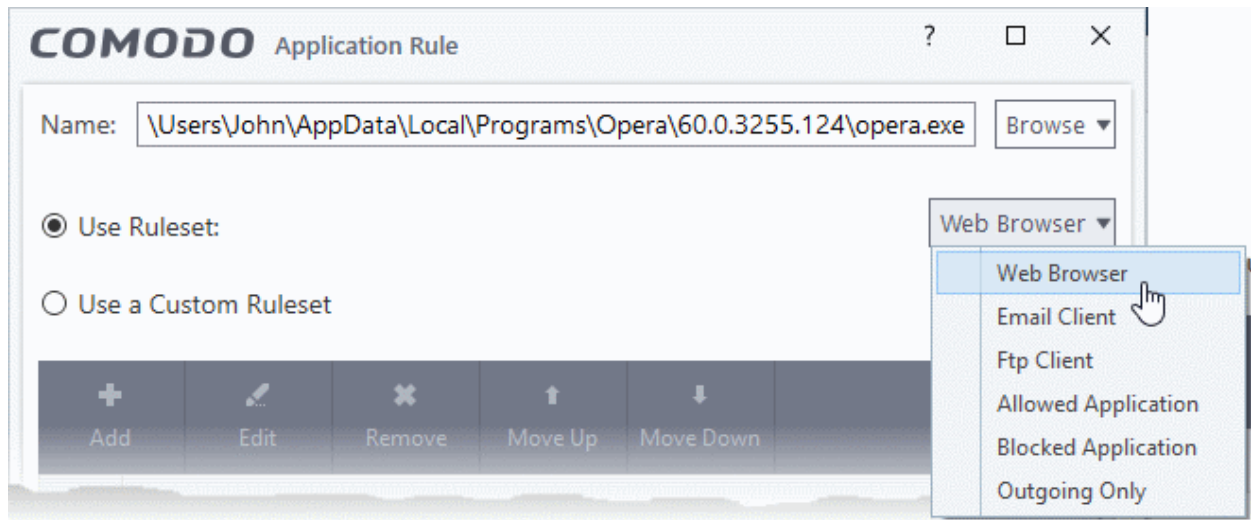
Note: Predefined Rulesets, once chosen, cannot be modified **directly** from this interface - they can only be modified and defined using the **Rulesets** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should 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)*.
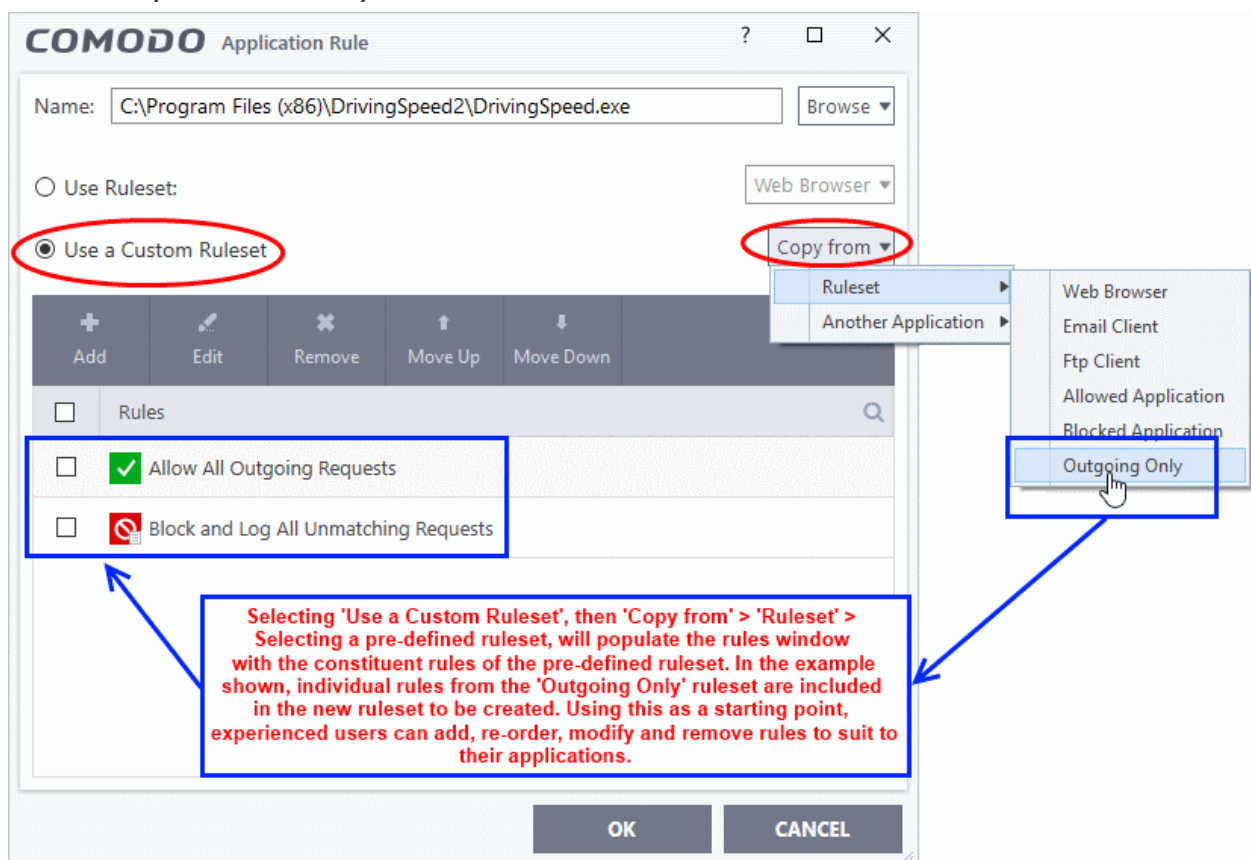
- Select the 'Use custom ruleset' radio button

- **Add** - Create individual rules for the set. See '**Add and Edit a Firewall Rule**' for an overview of the process.
- **Copy From** - Populate the list with the rules of a **Predefined Firewall Rule**. Edit/add/remove rules to create your custom ruleset.

Understand Firewall Rules

At their core, each firewall rule can be thought of as a simple **IF THEN** trigger - a set of **conditions** that a packet of data must meet, and an **action** that is taken if those conditions are met.

As a packet filtering firewall, Comodo firewall analyzes the attributes of every 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.
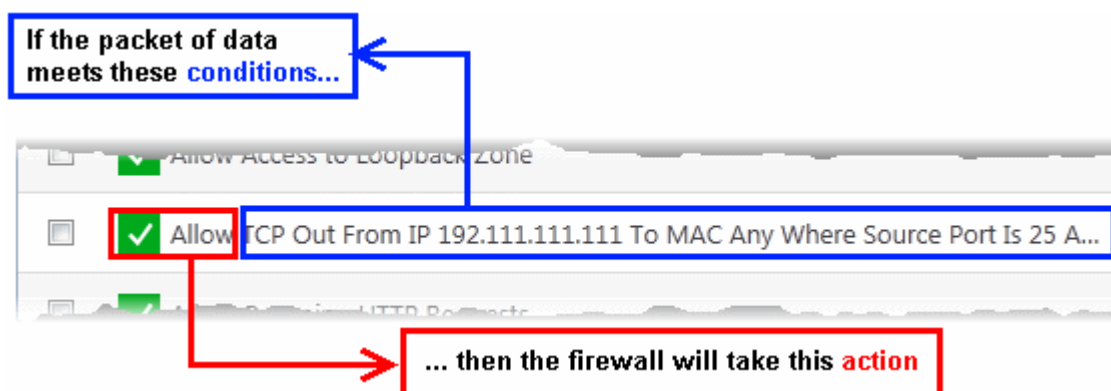
The actual **conditions** (attributes) you see * on a particular rule are determined by the protocol chosen in **Add and Edit a Firewall Rule**

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**

You should now specify the traffic covered by the rule, and the action taken if all conditions are met:

- **Action**: The action the firewall takes when the conditions of the rule are met. The rule shows '**Allow**', '**Block**' or '**Ask**'.**
- **Protocol**: The connection method that the application is attempting to use. Options are '**TCP**', '**UDP**', '**TCP or UDP**', '**ICMP**' or '**IP**'
- **Direction**: Choose whether the rule applies to inbound traffic, outbound traffic, or both. The rule shows '**In**', '**Out**' or '**In/Out**'
- **Source Address**: The origin 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**: The target 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**: The port number that the application is attempting to send through. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **Destination Port**: The ports on the remote host that the application is trying to connect to. Shows '**Where**

Source Port Is' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'

- **ICMP Details**: The Internet Control Message Protocol (ICMP) message that must be detected to trigger the action. Only applies if the protocol is ICMP. See **Add and Edit a Firewall Rule** for details of available messages that can be displayed.

- **IP Details**: The type of internet protocol (IP) that must be detected to trigger the action. See **Add and Edit 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 takes 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 then *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)*

Add and Edit a Firewall Rule

The firewall rule interface is used to configure the actions and conditions of an individual rules. 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 '**Understand Firewall Rules**', '**Overview of Rules and Rulesets**' and '**Create and Modify Firewall Rulesets**'.

General Settings

- **Action:** How the firewall should respond when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' *(Default)*, '**Block**' or '**Ask**'.
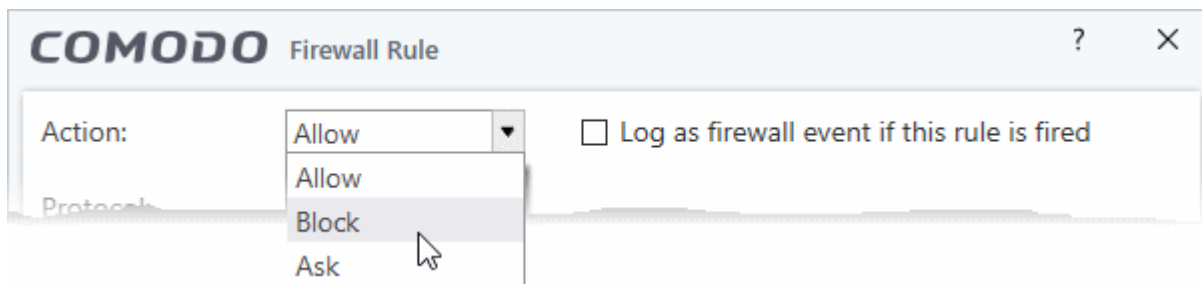
- **Protocol:** Specify which connection method the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' *(Default)*, '**ICMP**' or '**IP**' .

Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- **Direction**: Specify whether the traffic should be inbound or outbound. 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**: Enter a friendly name for the rule. For example, 'Allow Outgoing HTTP requests'. The friendly name is shown in the 'Application Rules' interface.

Protocol

i. **TCP**', '**UPD**' or '**TCP or UDP**'

If you select 'TCP', 'UPD' or 'TCP or UDP' as the protocol, then you also have to set the source and destinations:
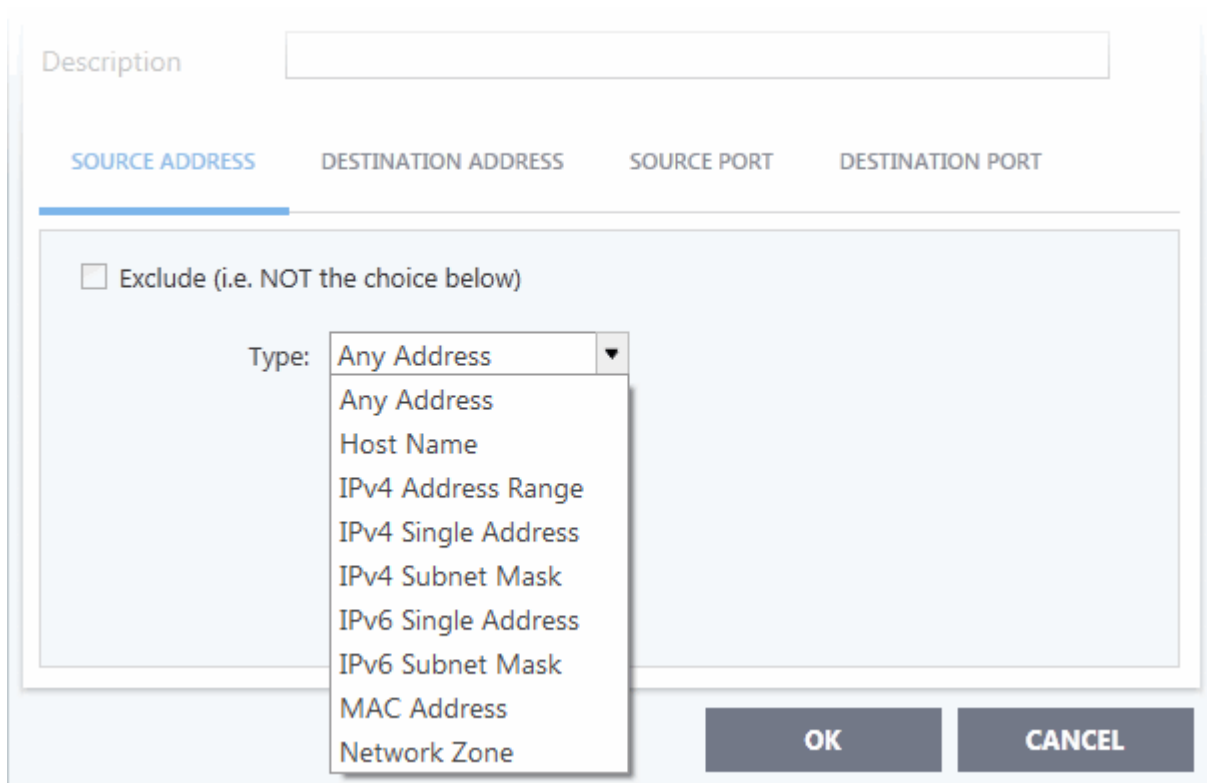
Source Address and Destination Address:

1. **Any** - Defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. **Host Name** - Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field

---

3. **IPv4 Address Range** - Choose all IP addresses covered by a range - for example a range in your private network.

   - Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.

4. **IPv4 Single Address** - Choose a single IPv4 address

   - Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.

5. **IPv4 Subnet mask** - Choose an IPv4 network. 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. **IPv6 Address Range** - Choose all IPv6 addresses covered by a range - for example a segment in your private network

   - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.

7. **Single IPv6 Address** - Choose an IPv6 address

   - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

8. **IPv6 Subnet Mask** - Choose a IPv6 network. 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 in the respective fields

9. **MAC Address** - Choose a single source/destination by specifying its physical address

   - Enter the physical address in the 'MAC Address' text box.

10. **Network Zone** - Choose an entire network. This menu defaults to Local Area Network. But you can also define your own zone by first creating a 'Network Zone' through the '**Network Zones**' area.

- **Exclude (i.e. NOT the choice below)** - Applies the action to all items except the one you specify. For example, you create a block rule, specify an IP address, then select 'Exclude'. The rule will block traffic for every address except the one you specified.

   Source Port and Destination Port:

1. **Any** - Apply the rule to any port number - set by default, 0- 65535.

2. **A Single Port** - Specify a one port number

   - Enter the single port number in the 'Port' drop-down combo-box .

___

3. **A Port Range** - Specify a set of ports covered by a range.

   • Enter the first port number and last port number in the respective fields

4. **A Set of Ports** - Choose a predefined **Port Set**. 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. **'Source' and 'Destination' addresses** - Enter 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. **Type** - Choose the ICMP version.
   3. **Message** - Specify the type 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.
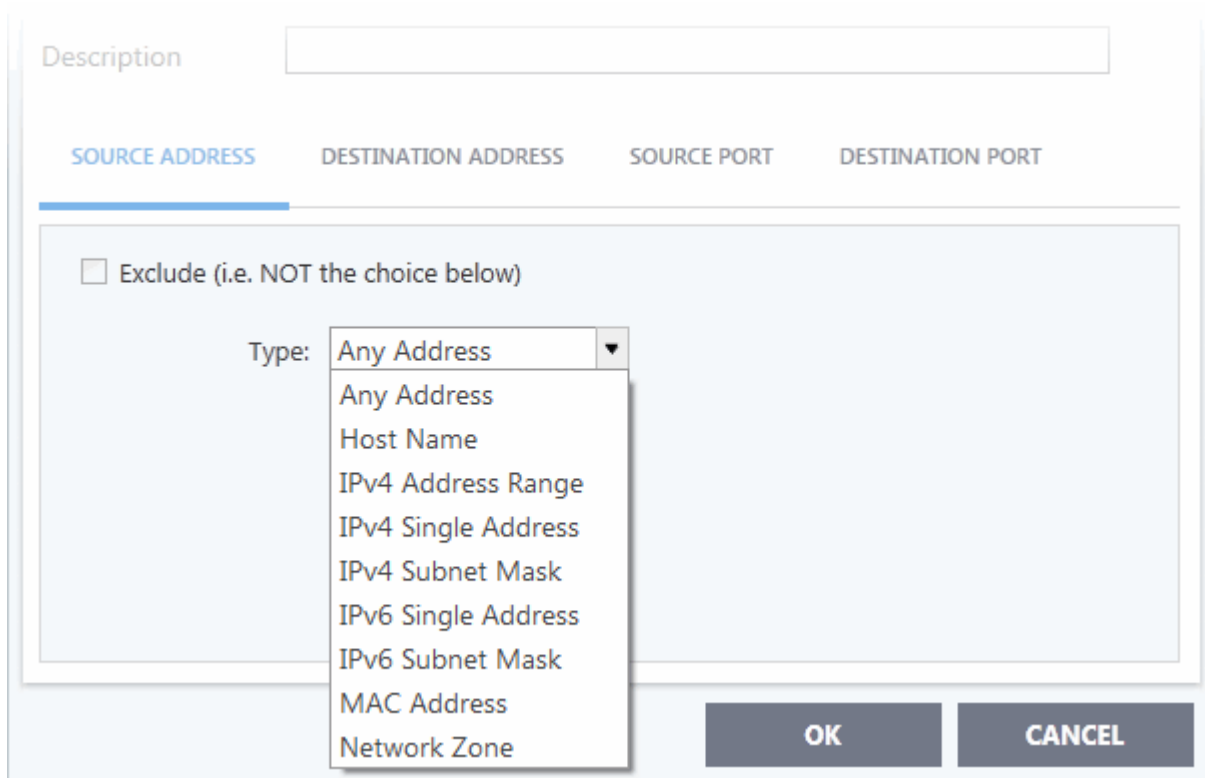
- **IP Details**

Select the types of IP protocol that you wish to allow, from the ones that are listed.
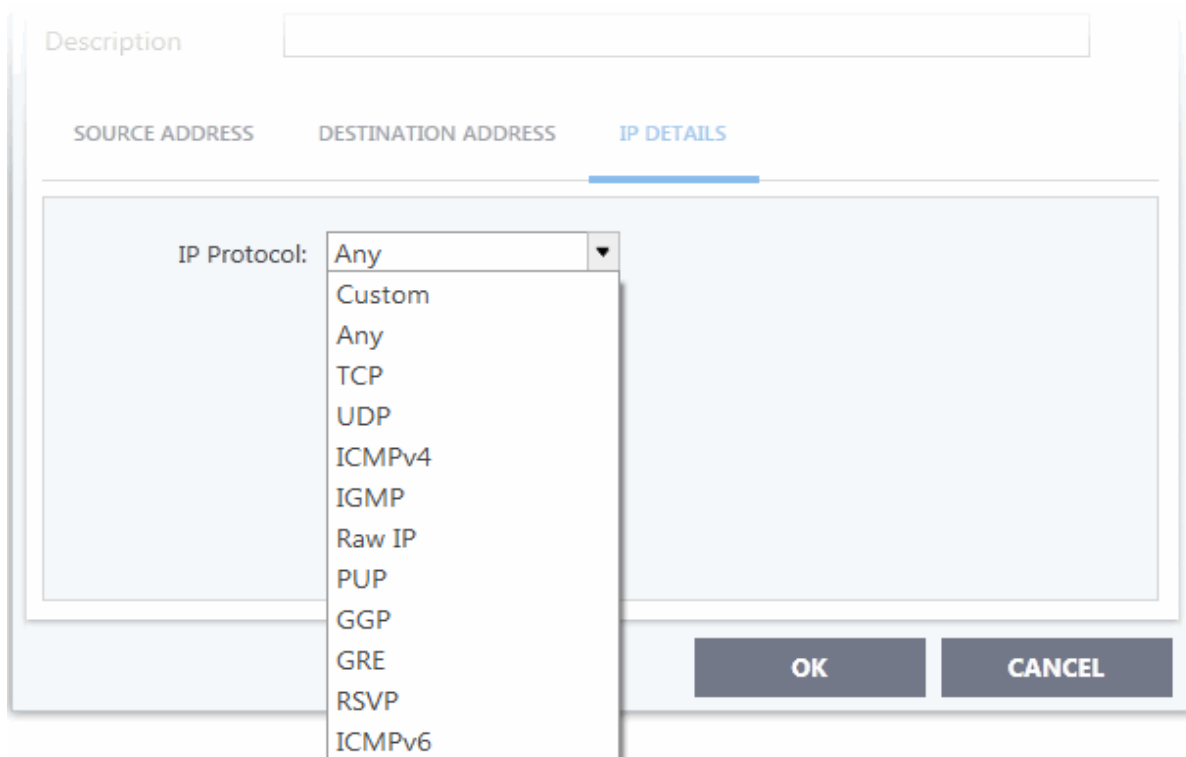
- Click 'OK' to add the firewall rule.
- Repeat the process to add more firewall rules
- Click 'OK' in the 'Advanced Settings' interface for your firewall rules to take effect

6.3.3. Global Rules

Click 'Settings' > 'Firewall' > 'Global Rules'

- 'Global Rules' apply to *all* traffic in and out of your computer. This makes them different to application rules, which apply to the traffic of a specific application.

- Comodo firewall analyzes every packet of data in and out of your PC using combination of application rules 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.
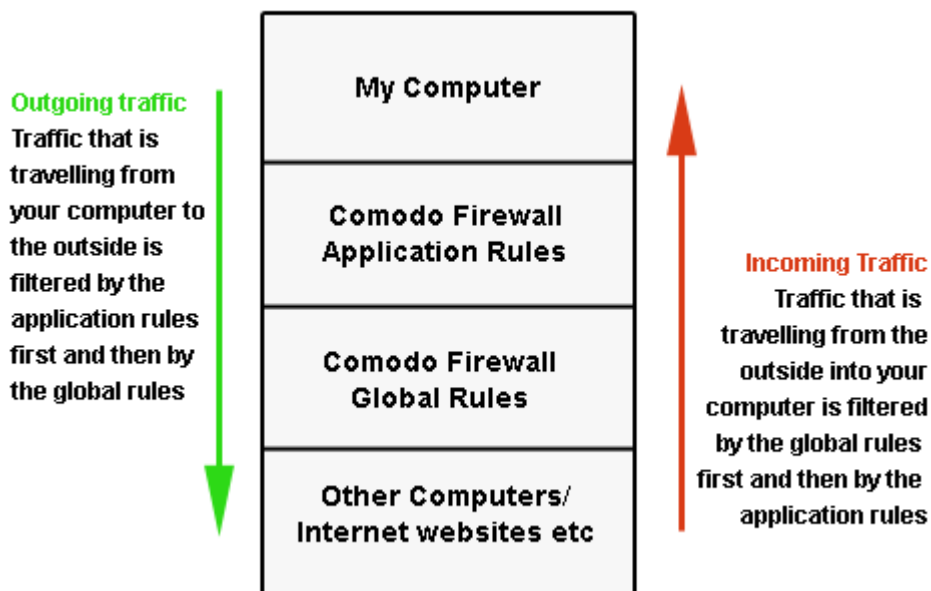
- So outgoing traffic has to pass the application rule first then any global rules before it is allowed out. Similarly, incoming traffic has to pass the global rules first then the application rules.

- Global rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

Manage Global Rules

- Click 'Settings' on the CIS home screen

- Click 'Firewall' > 'Global Rules'.

COMODO
Creating Trust Online®
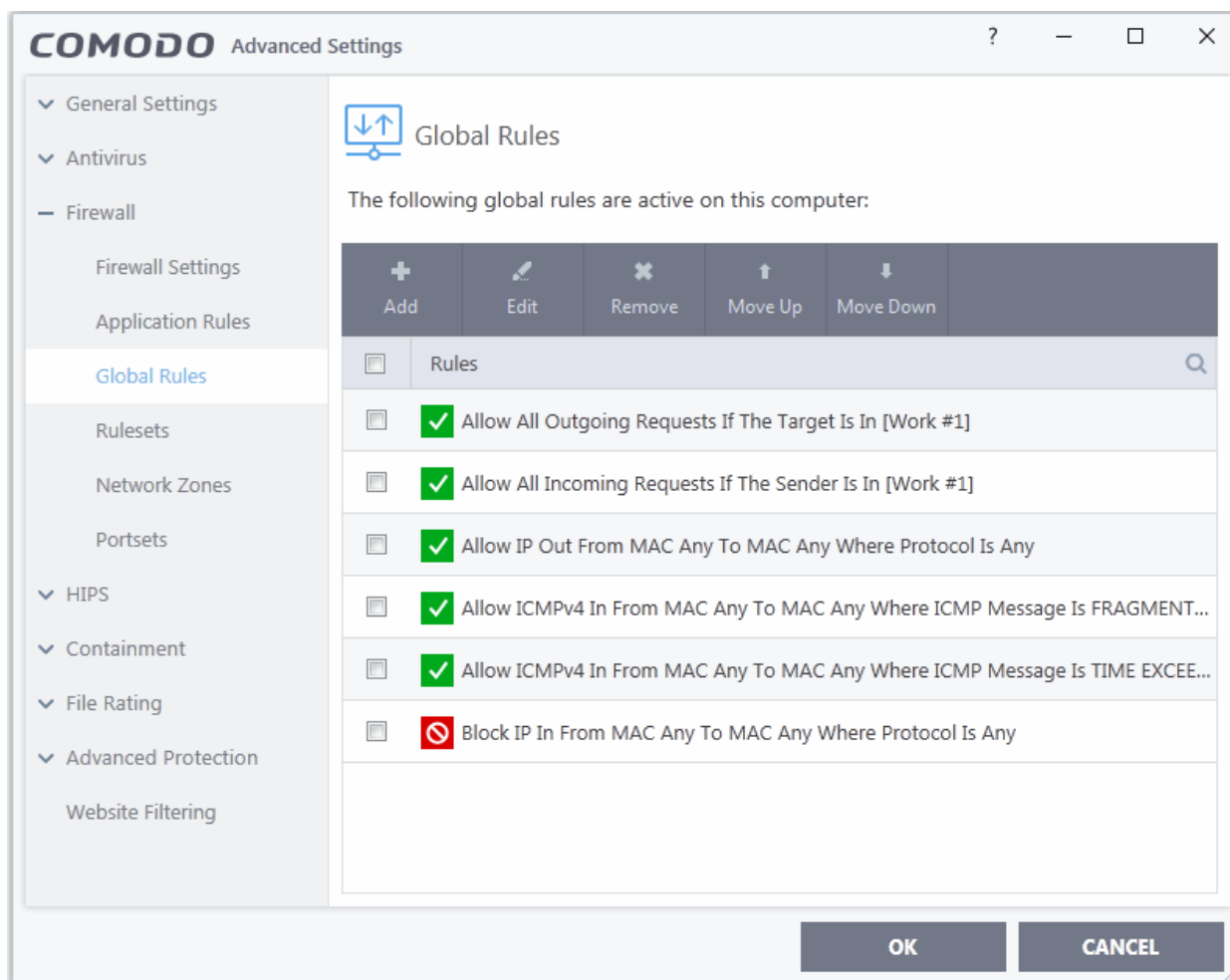
General Navigation:

The controls above the table let you create and manage global rules:
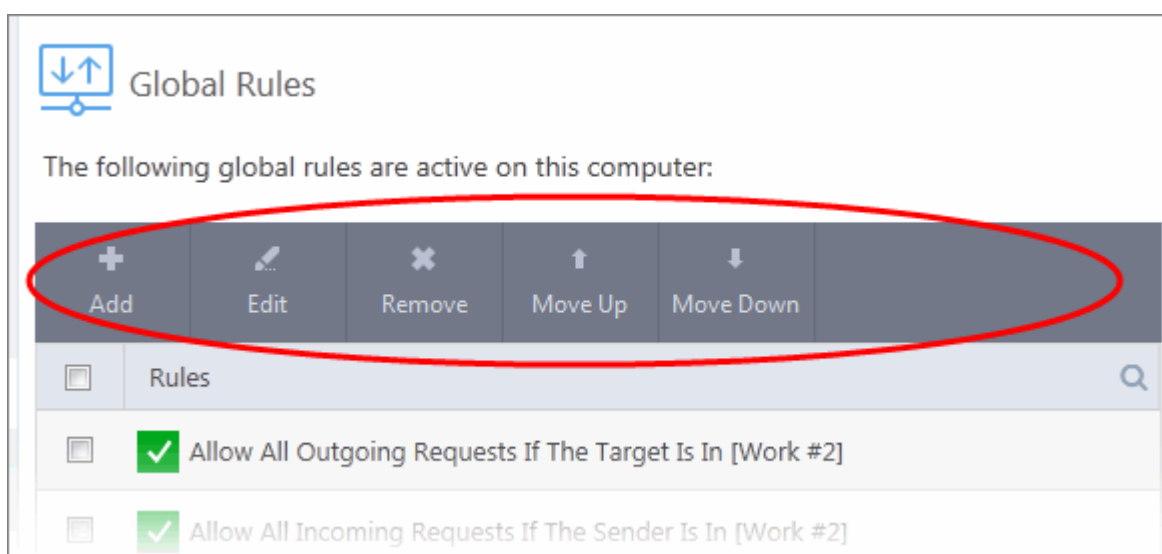
- **Add** - Create a new global rule. See '**Add and Edit a Firewall Rule**' in the previous section 'Application Rules' for guidance on creating a new rule.
- **Edit** - Modify an existing global rule. See '**Add and Edit a Firewall Rule**' in the previous section 'Application Rules' for guidance on 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 from the list.

- • **Move Up and Move Down** - Rules at the top of the list have a higher priority. In the event of a conflict in settings for a piece of traffic, CIS will apply the setting in the rule nearer the top of the list. The 'Move Up' and 'Move Down' buttons let you change the priority of a rule.

- • The configuration of global rules is identical to that of application rules. See **Application Rules** for an introduction to the rule setting interface.

- • See **Understand Firewall Rules** for an overview of the meaning, construction and importance of individual rules.

- • See '**Add and Edit a Firewall Rule**' for an explanation of individual rule configuration.

6.3.4. Firewall Rule Sets

Click 'Settings' > 'Firewall' > 'Rulesets'

- • A firewall ruleset is a collection of one or more firewall rules which can be deployed to applications on your computer.

- • CIS ships with six predefined rulesets that provide a very high level of protection. You can also create your own, custom rulesets.

This section contains advice on the following:

- • **Predefined Rulesets**
- • **Custom Rulesets**
- • **Create a new ruleset**

Open the Rulesets panel

- • Click 'Settings' at the top of the CIS home screen
- • Click 'Firewall' > 'Rulesets' on the left.
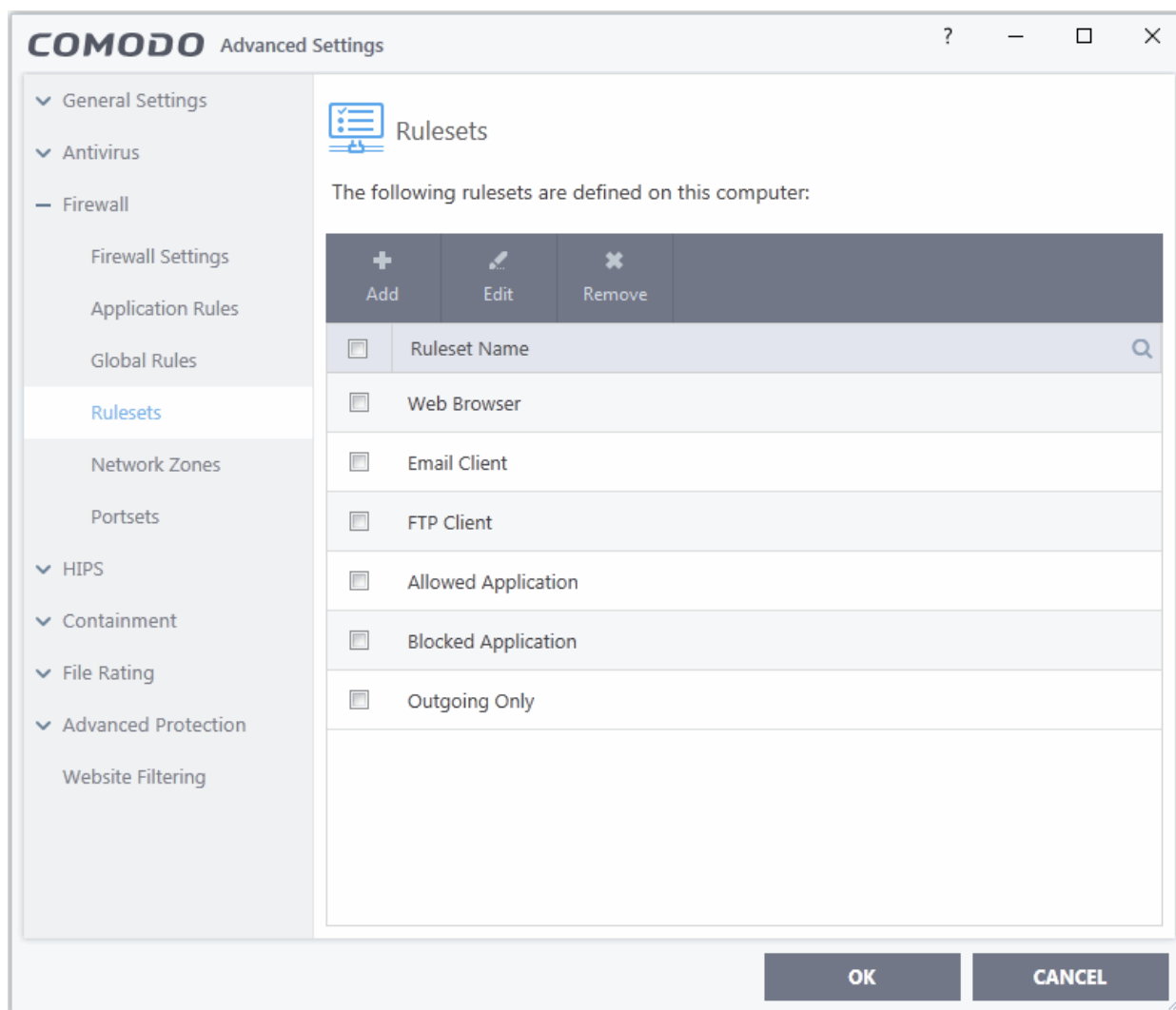
- The interface shows all existing rulesets. These may be Comodo predefined rules, or custom rulesets.
- Use the search feature to look for a specific ruleset

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 **Add and Edit Firewall Rules** in 'Application Rules'.

Custom Rulesets

You can create new rulesets with custom network access control rules as per your requirements. These can then be applied to specific applications when **creating an application rule**.

The Firewall Alert

You can apply a firewall ruleset to an application at a firewall alert. Both predefined and custom rulesets are made available. An example alert is shown below:
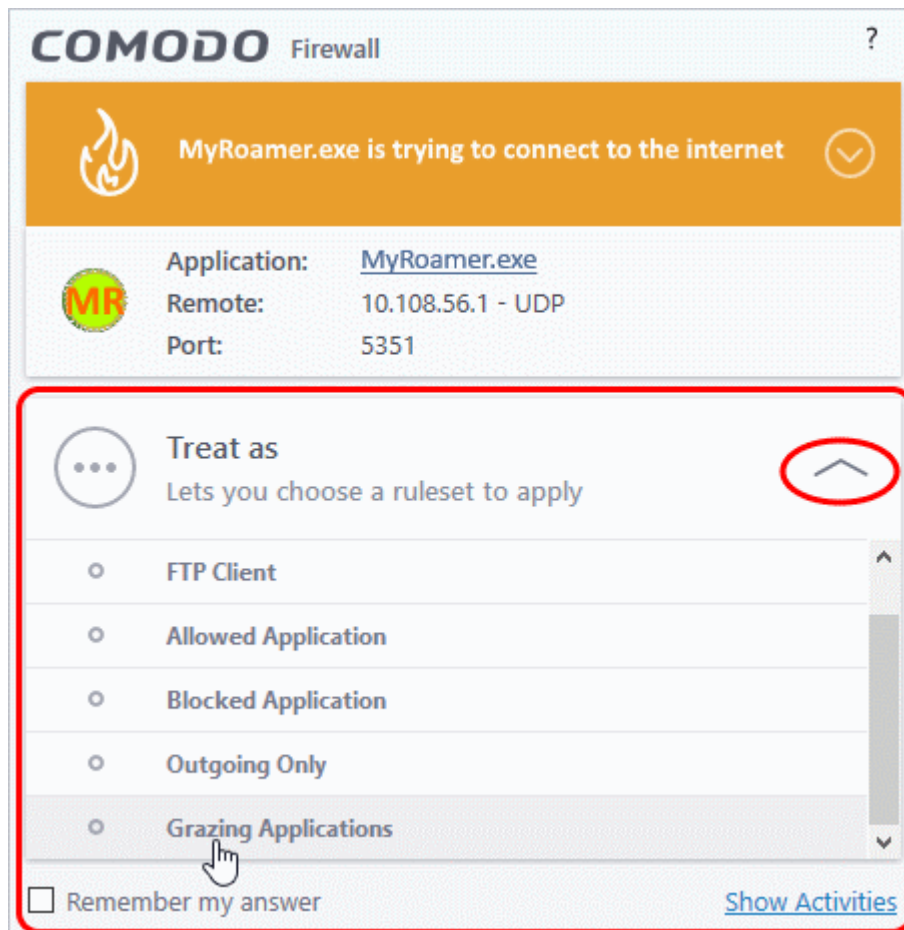
- See **answer firewall alerts** if you want more help with alerts.

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.
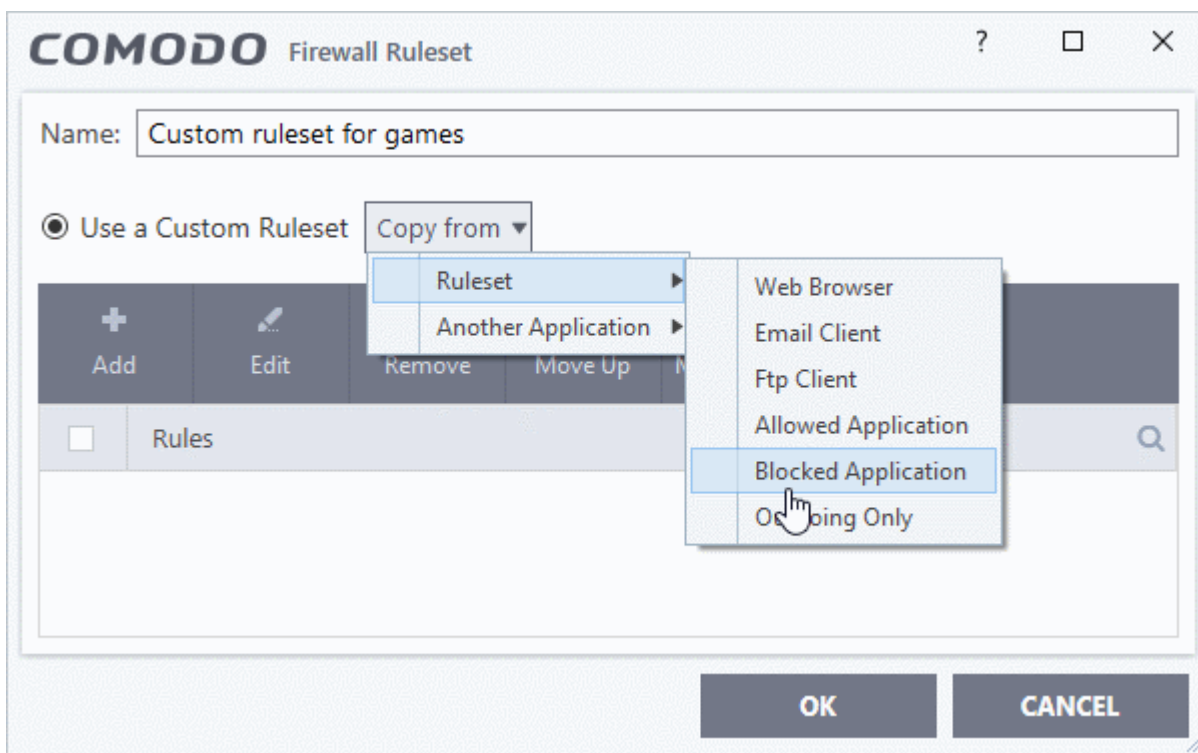
- As this is a new ruleset, you need to name it in the text field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for.
- Next you should add and configure the individual rules for this ruleset. You can choose to use an existing ruleset as a starting point and add/edit rules as required. See '**Add and Edit 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:
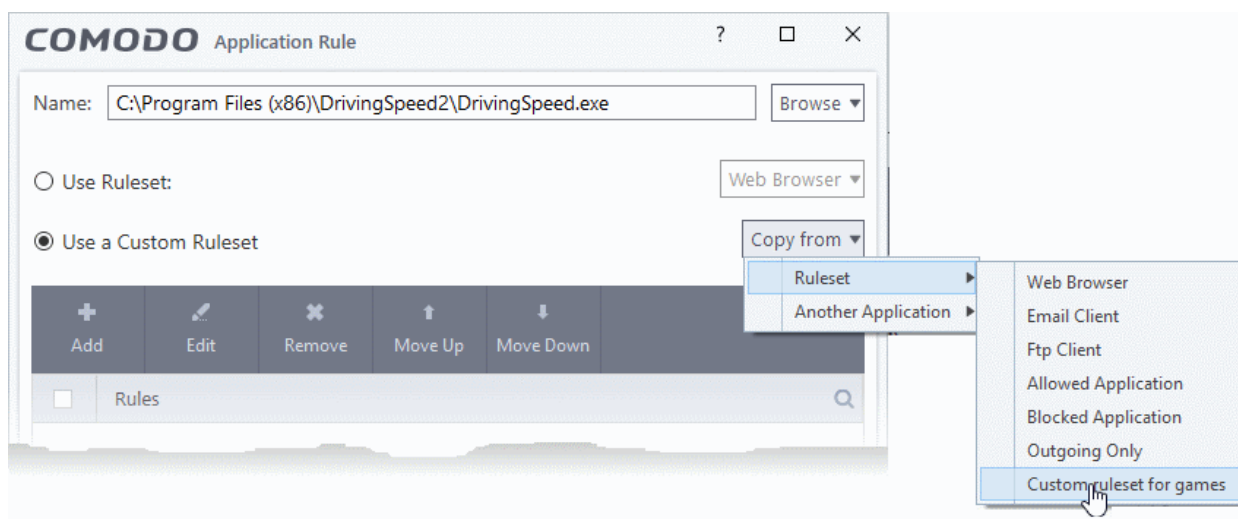
View or edit an existing predefined Ruleset

- 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

Click 'Settings' > 'Firewall' > 'Network Zones'

- A 'Network Zone' can consist of an individual machine (like a 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 lets you configure:

  - Automatic detection of networks to which your computer can connect
  - Alerts for network connections
  - Trusted network zones which you want to allow
  - Untrusted network zones which you want to block

Open the Network Zones panel

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Network Zones'.
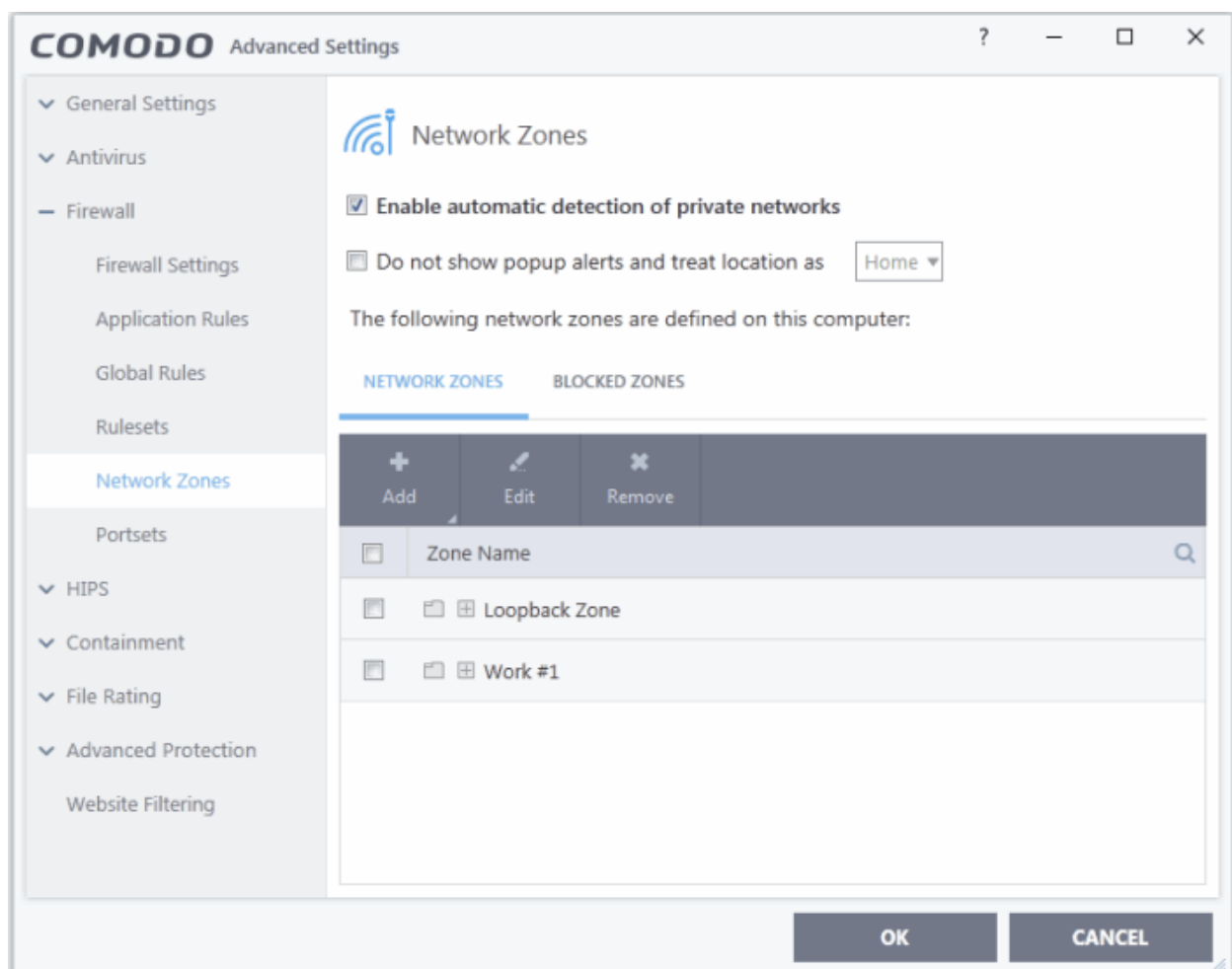
Network Monitoring Settings:

- **Enable automatic detection of private networks** - The firewall monitors attempted connections to any new wired or wireless network *(Default = Enabled)*. Deselect this option if you are an experienced user and wish to manually set-up your 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** - CIS can show an alert when your computer attempts to connect to a new network.

  - **Disabled** - The alert is shown. Select the appropriate network type for your connection. CIS will

---

optimize the firewall for security and usability based on your choice. (*Default*)

- **Enabled** - The alert is not shown. You now need to pick a default network type from 'Home', 'Work', or 'Public'. CIS will automatically apply your choice of network type to all new connections.
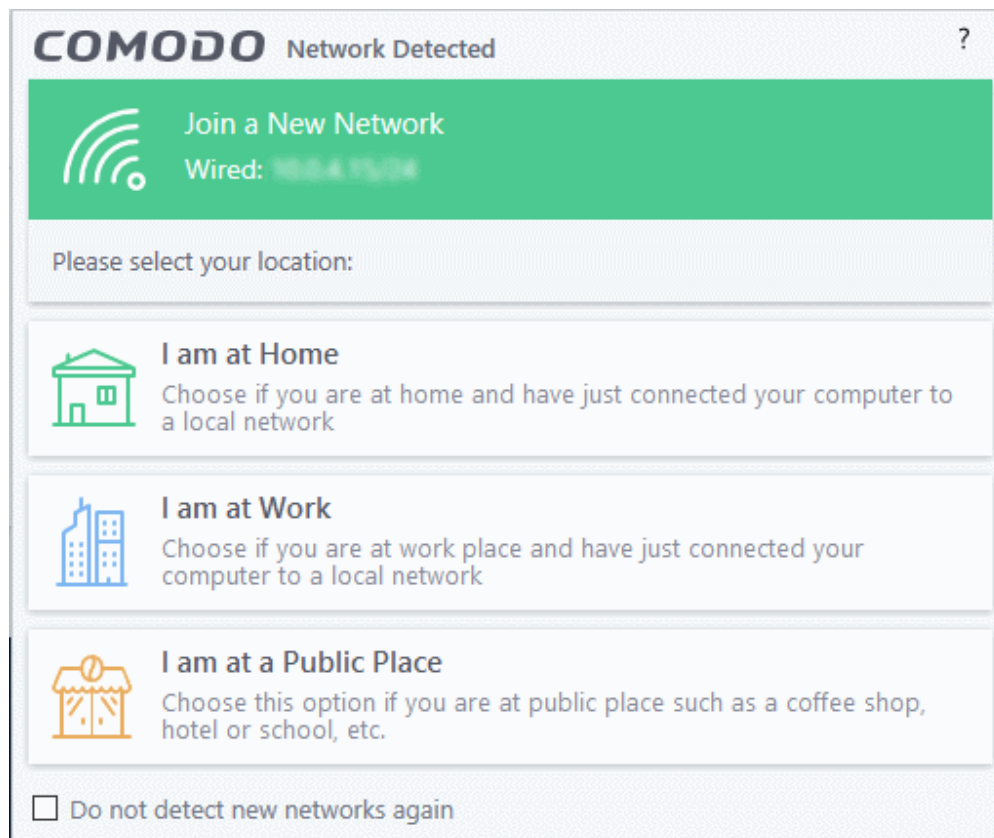
- Select 'Do not detect new networks again' If you are an experienced user that wishes to manually set-up their own trusted networks. This can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**'.

The panel has two tabs:

- **Network Zones** - Define network zones with specific access rights. Application access privileges are specified in the **Application Rule** interface. See '**Create or Modify Firewall Rules**' for more details.

- **Blocked Zones** - Define networks that are not trusted. CIS will deny all connections to blocked zones.

6.3.5.1. Network Zones

Click 'Settings' > 'Firewall' > 'Network Zones' > 'Network Zones' tab

- A 'Network Zone' can consist of an individual machine (like a home computer connected to the 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 cabled or wireless connection.

- A network allows users to share information and resources with other computers/users on the network.

- There are some networks which you trust and want 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 panel lets you configure trusted and untrusted networks.

Add and manage network zones

- Click 'Settings' on the CIS home screen

- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab
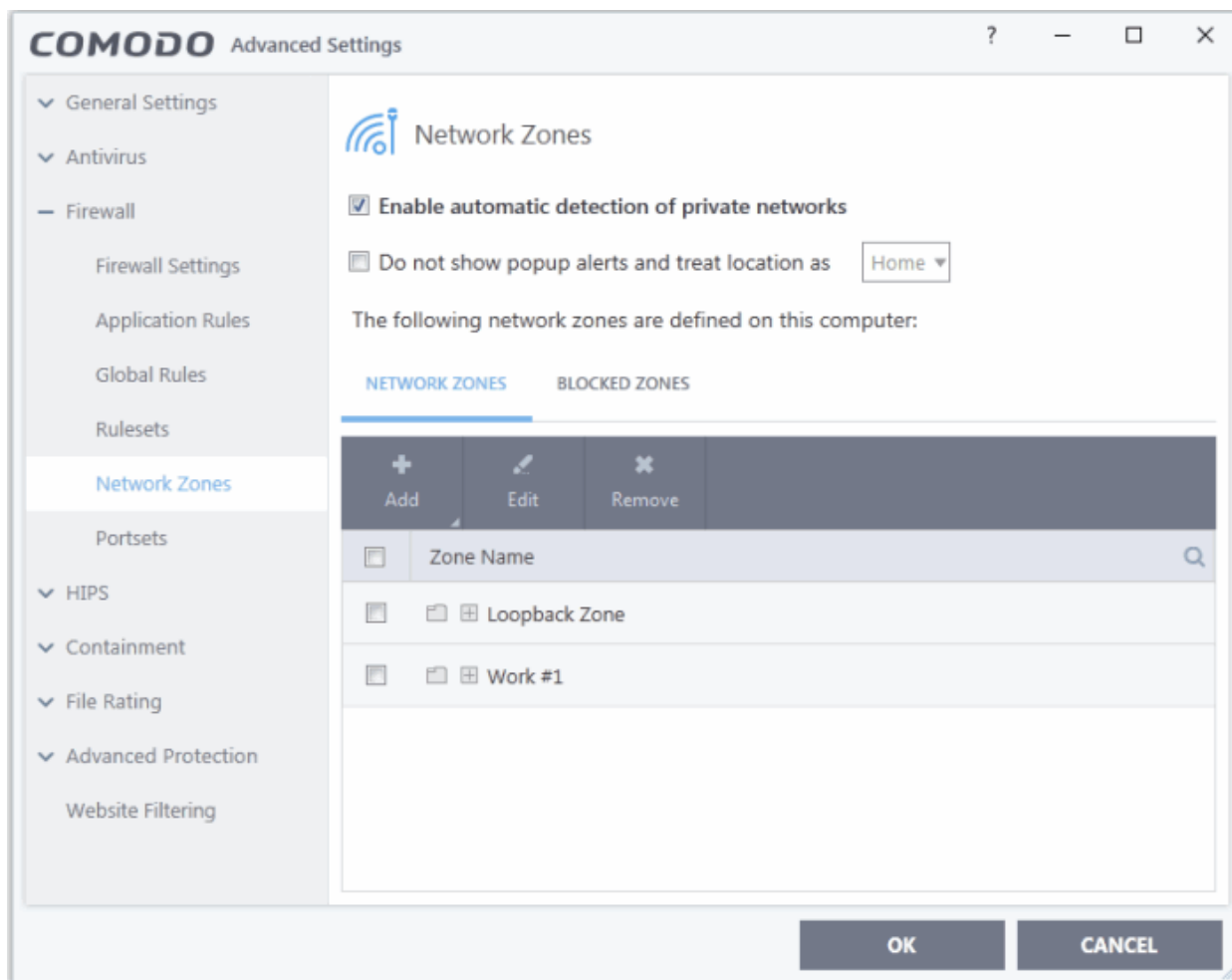
The network zones tab shows zones that have already been added to CIS. You can add new zones and manage existing zones.

Note 1: Adding a zone to this area does not, by itself, define any permissions or access rights to the zone. This area lets you define the zones so you can 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.

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.

Define 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 'Settings' on CIS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab
- Click the 'Add' button at the top of the list and choose 'New Network Zone' from the options.
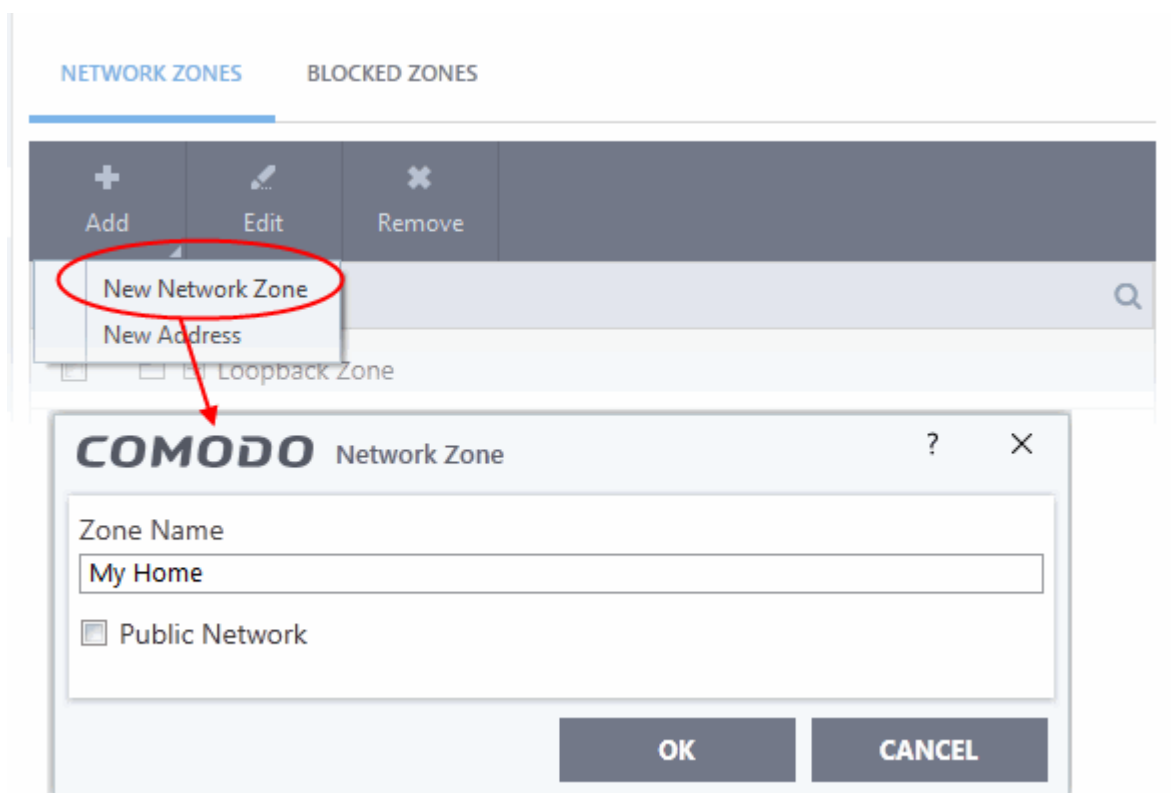
- Choose a name that accurately describes the network zone you are creating.
- Select 'Public Network' if you are defining a network zone for a network in a public place. For example, when you are connecting to a Wi-Fi network at an airport, restaurant etc. The firewall will optimize the connection accordingly.
- Click 'OK' to confirm your zone name.

This adds your new zone to the 'Network Zones' list:
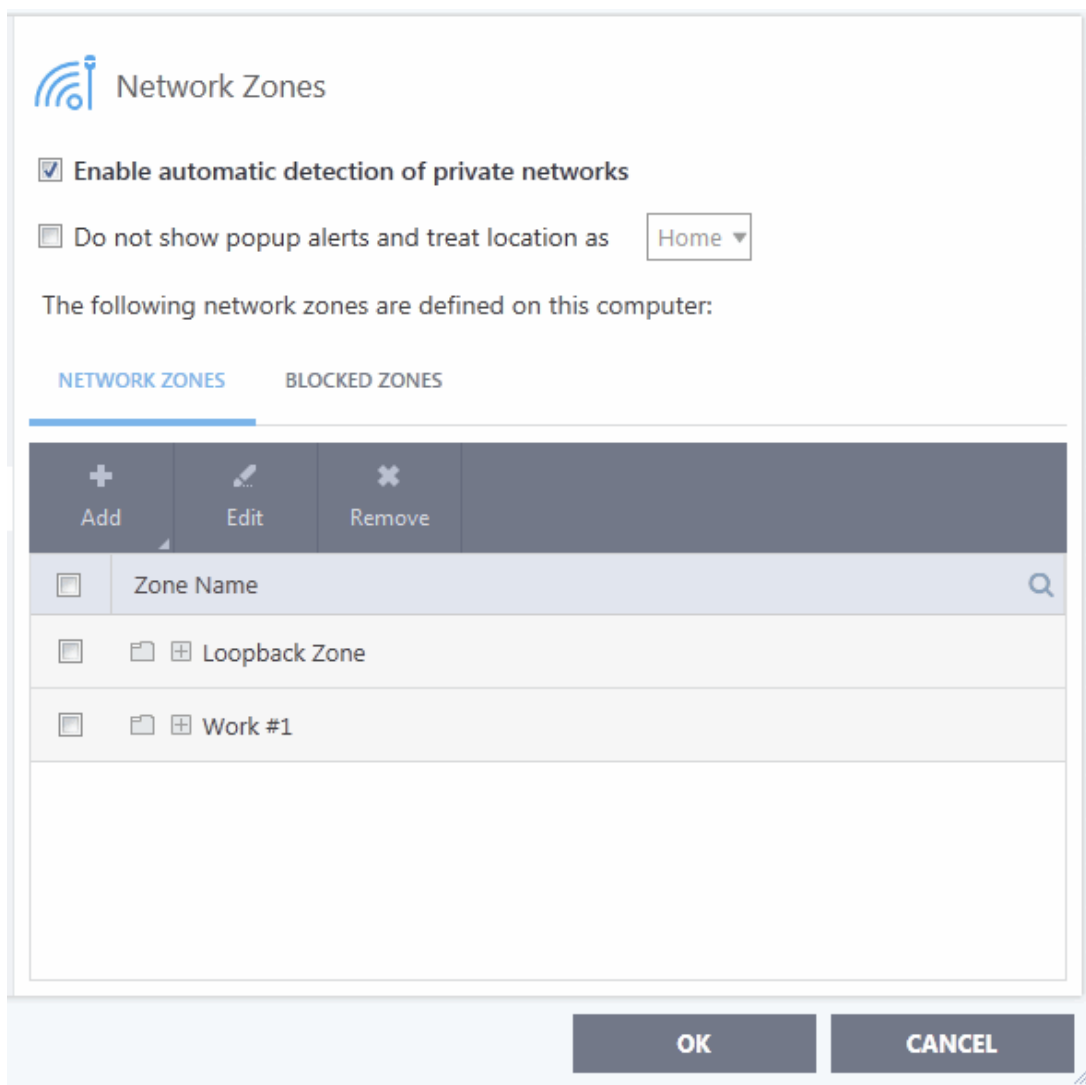
Step 2 - Select the addresses to be included in this zone

- 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'
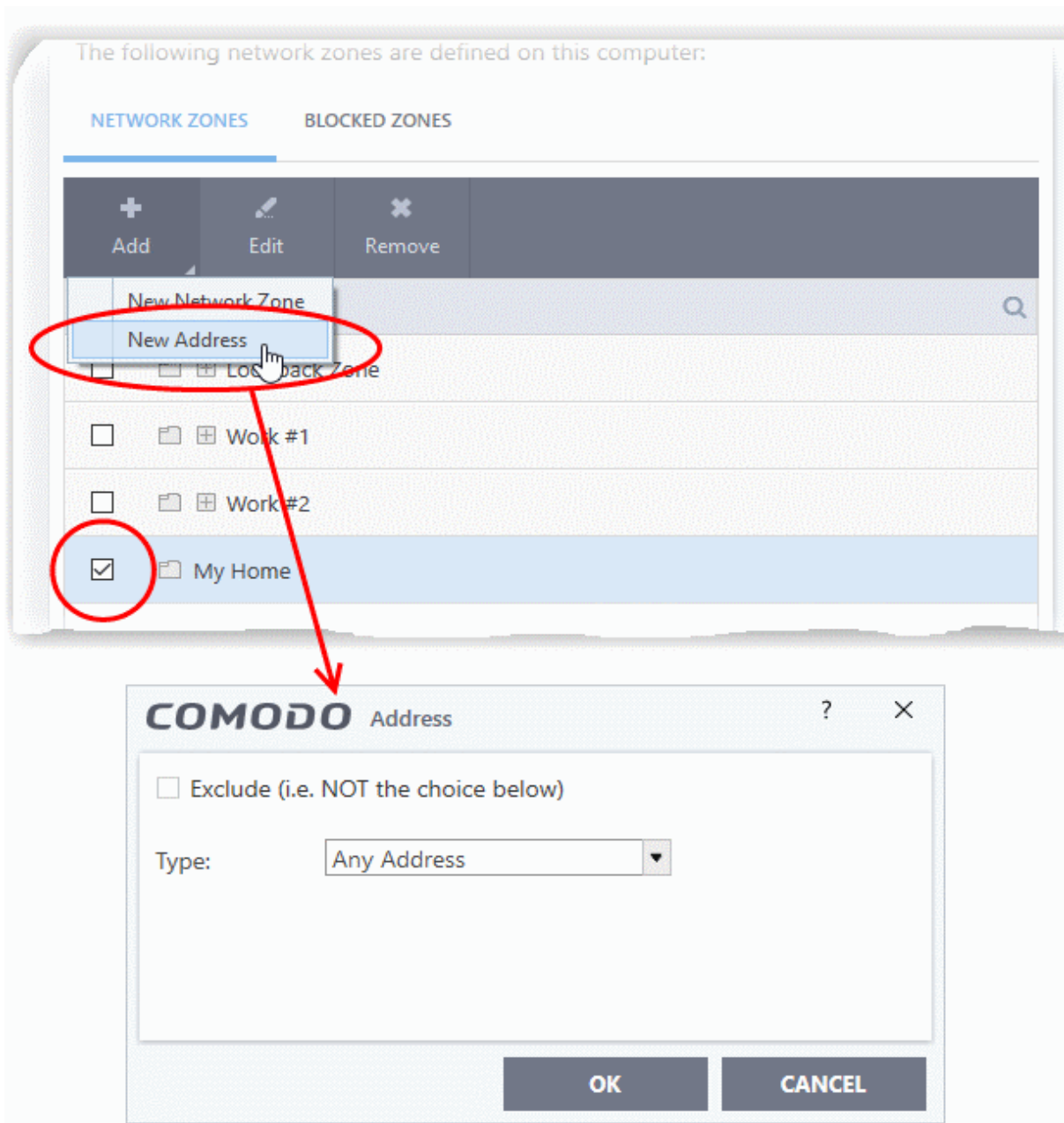
Address Types:

1. **Any** - Defaults to an IP range of 0.0.0.0- 255.255.255.255 to block connection from all IP addresses.

2. **Host Name** - Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field

3. **IPv4 Address Range** - Choose all IP addresses covered by a range - for example a range in your private network.

   • Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.

4. **IPv4 Single Address** - Choose a single IPv4 address

   • Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.

5. **IPv4 Subnet mask** - Choose an IPv4 network. 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. **IPv6 Address Range** - Choose all IPv6 addresses covered by a range - for example a segment in your private network

- • Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.

7. **Single IPv6 Address** - Choose an IPv6 address

- • Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

8. **IPv6 Subnet Mask** - Choose a IPv6 network. 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 in the respective fields

9. **MAC Address** - Choose a single source/destination by specifying its physical address

- • Enter the physical address in the 'MAC Address' text box.

- • **Exclude (i.e. NOT the choice below)** - The opposite of what you specify is applicable.

- • 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**

- • Quickly called and designated as a blocked zone from the '**Blocked Zones**' interface

Edit the name of an existing Network Zone

- Click 'Settings' on the CIS home screen

- Click 'Firewall' > 'Network Zones'

- Click the 'Network Zones' tab

- Select the zone from the list (e.g., My Home) and click the 'Edit' button from the top or double click on the network zone name.
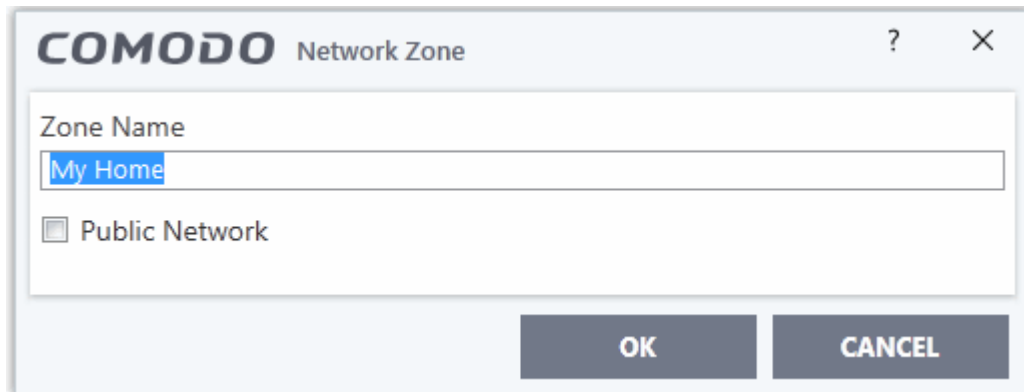
- Change the name of the zone and click 'OK'.

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**.

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**.

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

Click 'Settings' > 'Firewall' > 'Network Zones' > 'Blocked Zones' tab

- A computer network lets you share information and resources with other users and computers.

- There are some networks which you trust and want 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 'Blocked Zones' section allows you to configure restrictions on network zones that you do not trust.

Note: We advise new or inexperienced users to first read '**Network Zones**', '**Stealth Ports Wizard**' and '**Application Rules**' before blocking zones in this interface.

Add and manage blocked zones

- Click 'Settings' on the CIS home screen

- Click 'Firewall' > 'Network Zones'

- Click the 'Blocked Zones' tab
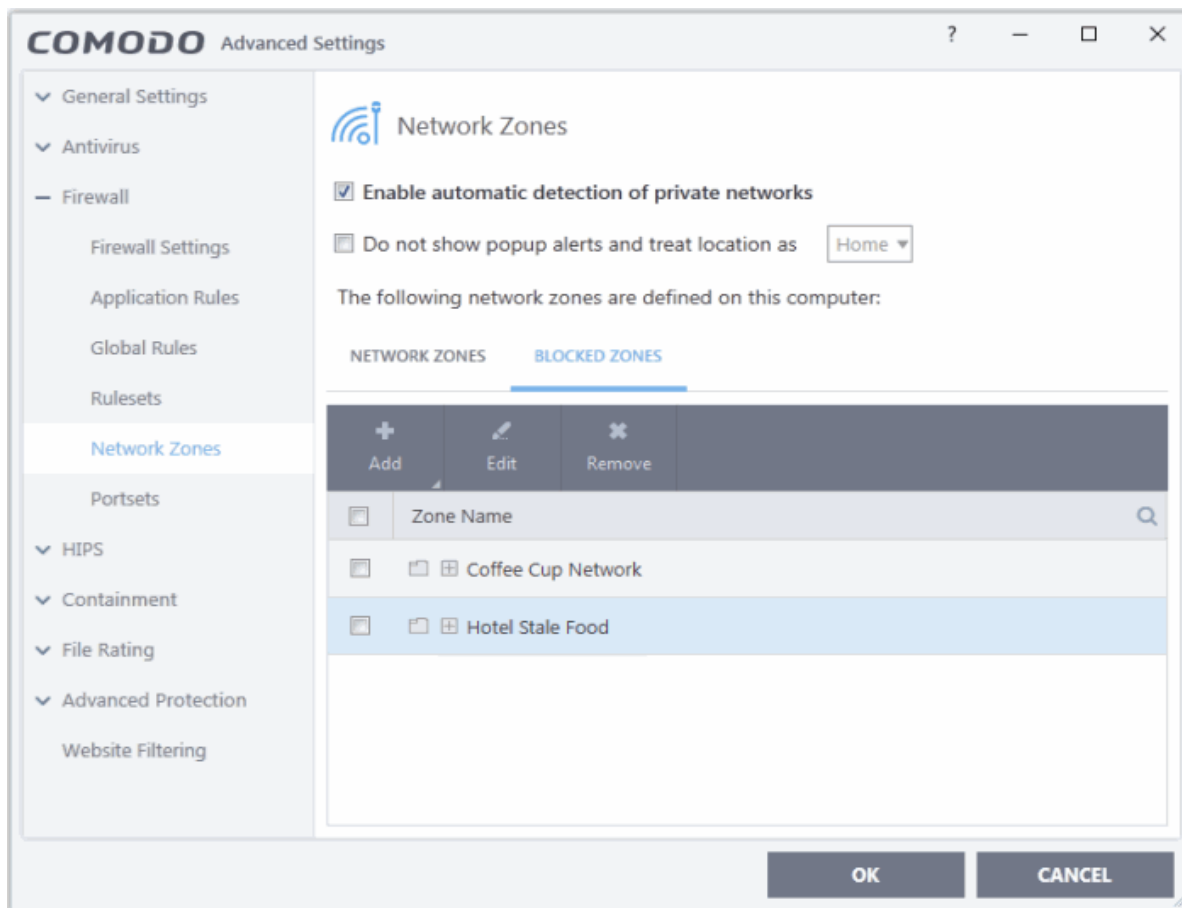
The 'Blocked Network Zones' tab allows you to:

- **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.

Deny access to an existing network zone

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab
- Click 'Add' button at the top and choose 'Network Zones' from the options
- Select the particular zone you wish to block.
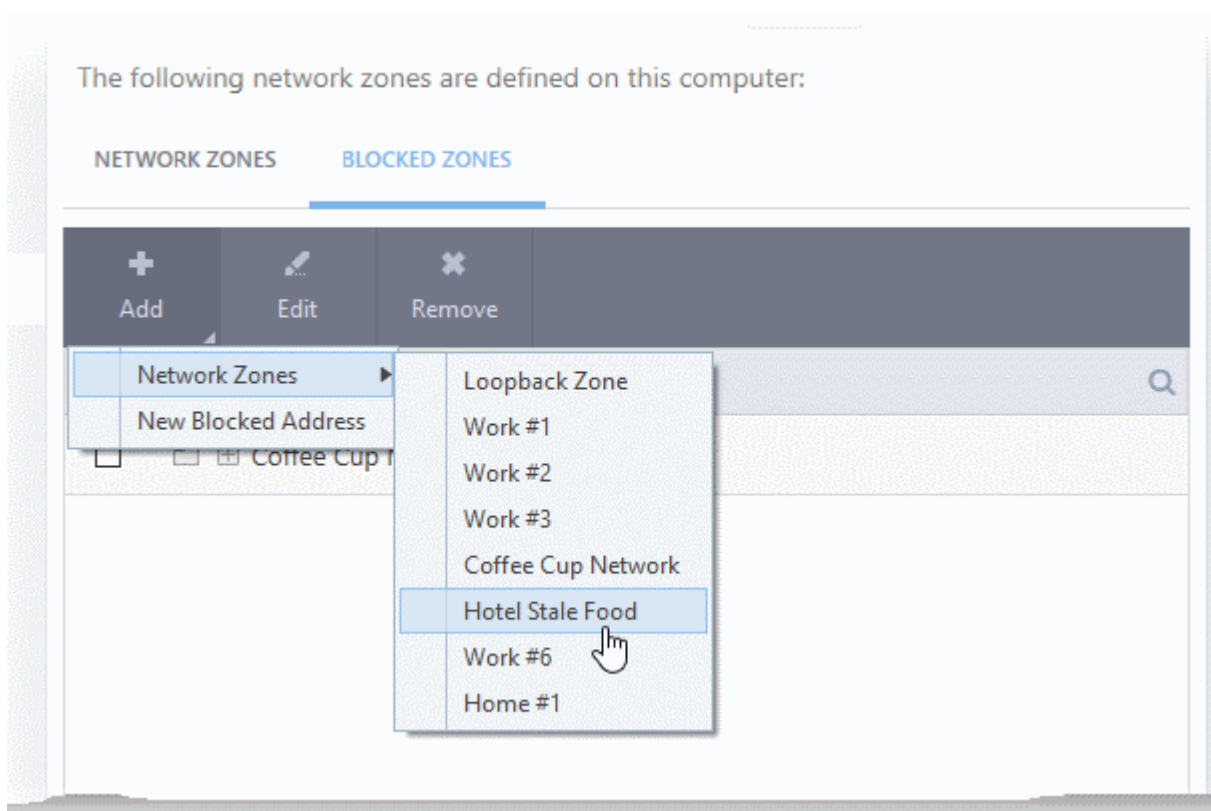
The selected zone will appear in the 'Blocked Zones' interface.
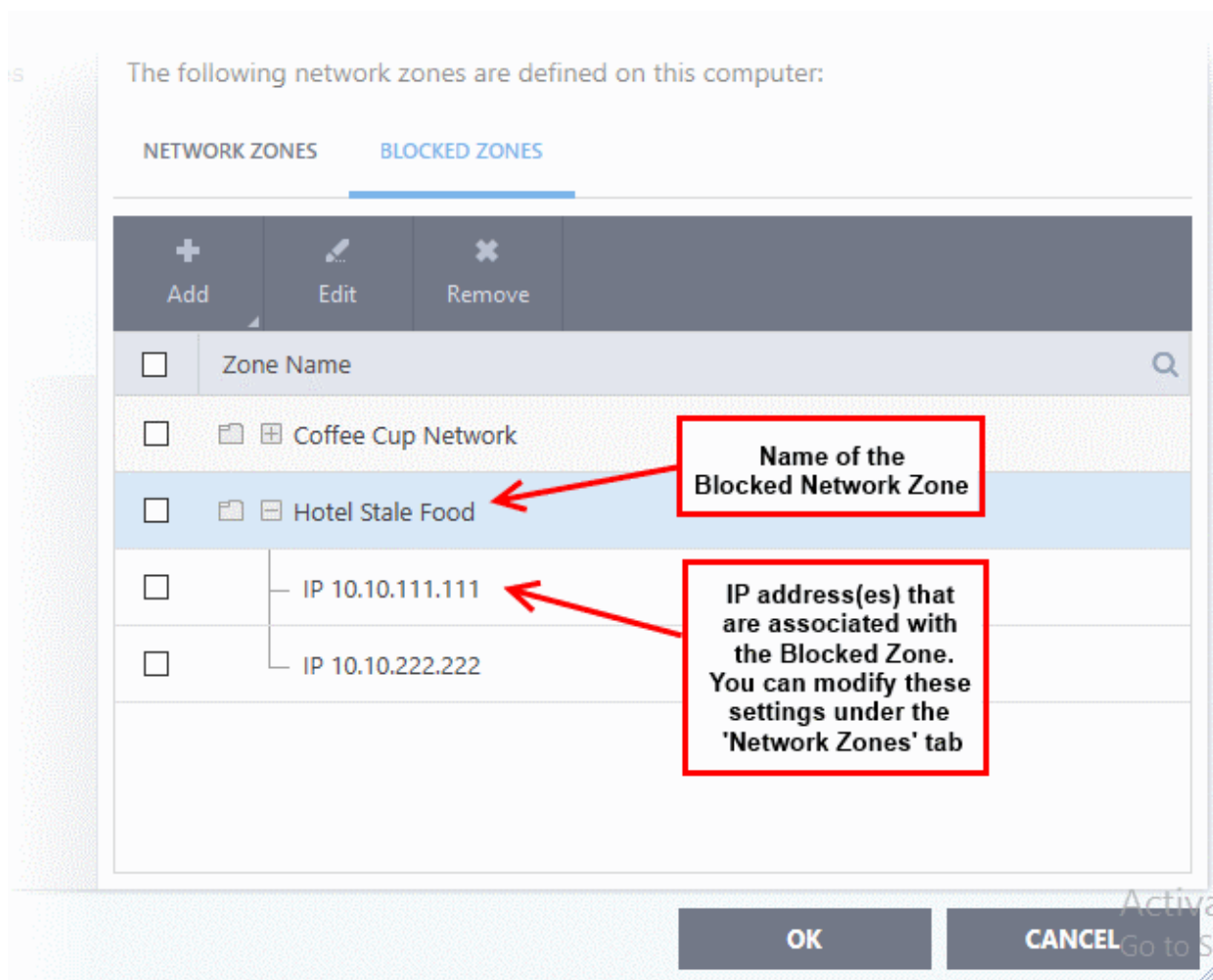
- Click 'OK' to confirm your choice.
- All traffic to and from devices in this zone is now blocked.

Deny access to a network by manually defining a new blocked zone

- Click 'Settings'on the CIS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab
- Click the 'Add' button and choose 'New Blocked Address':
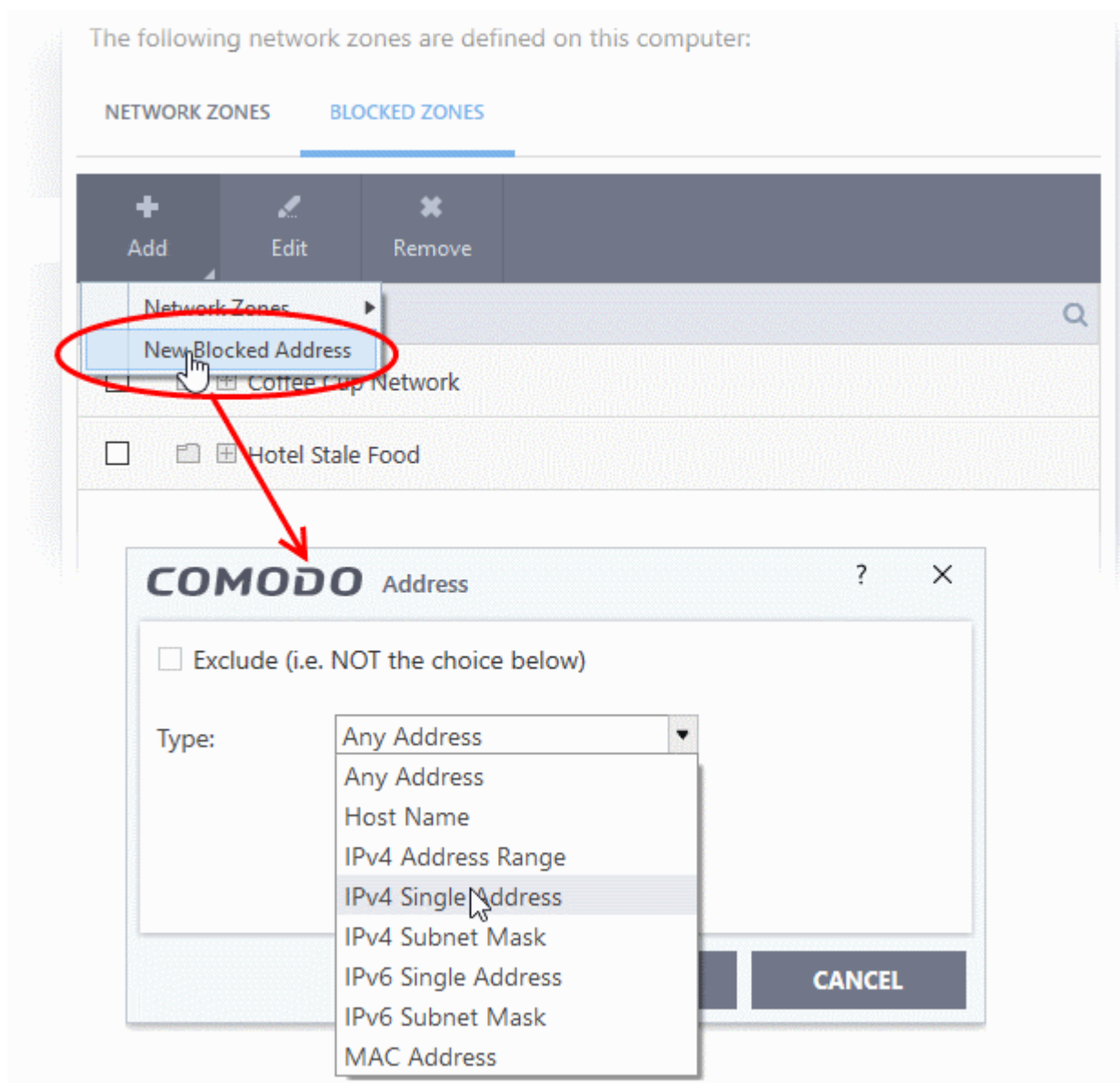
Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

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.

- 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'.

- 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

Click 'Settings' > 'Firewall' > 'Portsets'

- Port sets are predefined groups of one or more ports. These sets can be named as the target of **Application Rules** and **Global Rules**. For example, you might want to block all inbound traffic to certain set of ports.

- The port sets panel lets you add, view and manage port sets

Open the Portsets panel

- Click 'Settings' at the top of the CIS home screen

- Click 'Firewall' > 'Portsets'
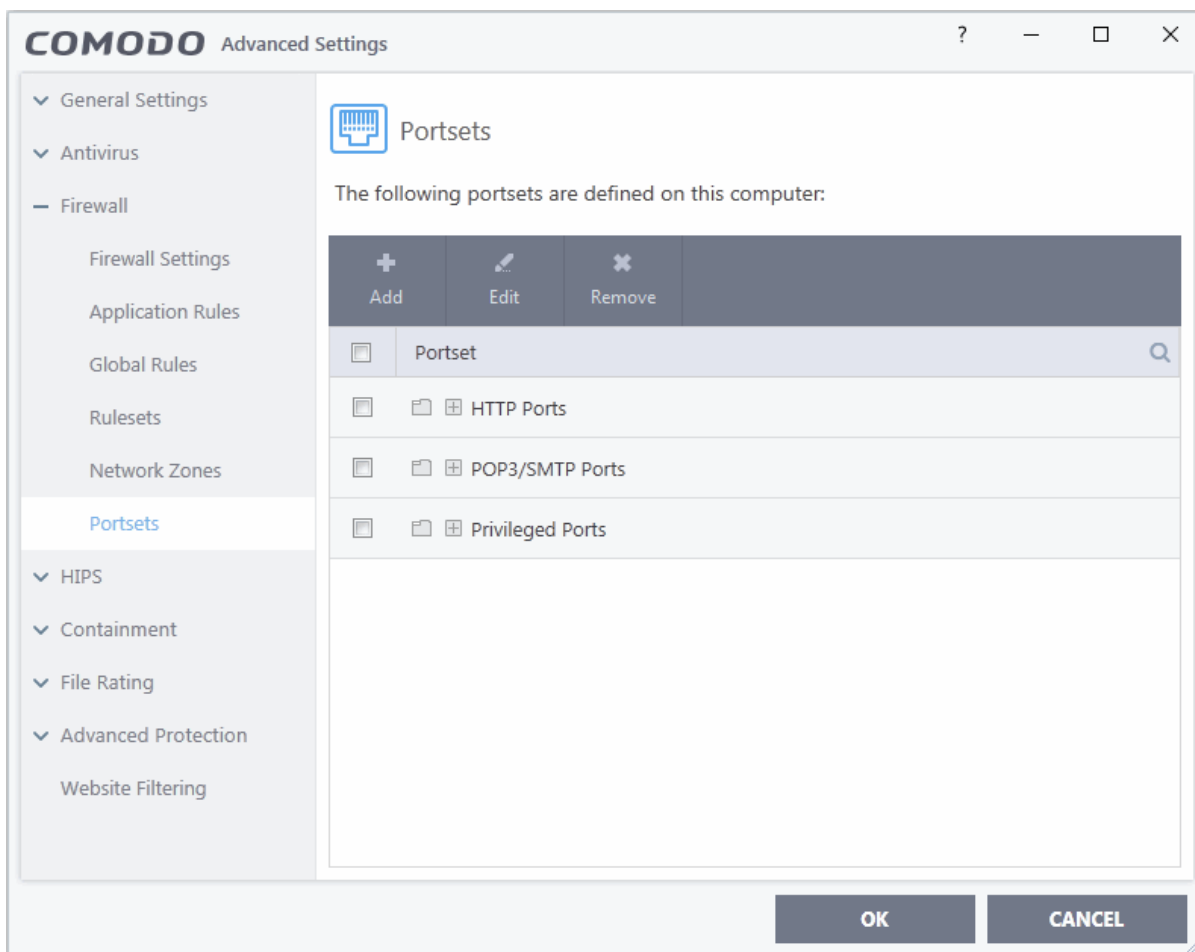
- The interface lists all existing port sets. Click the + button to view all ports in the set.

- 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**.** 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. This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range.

Define a new Port Set

After defining a new port set, you can apply it to applications through the **Application Rule** interface. See '**Create or Modify Firewall Rules**' for more details.

Add a new portset

- Click 'Settings' on the CIS home screen
- Click 'Firewall' > 'Portsets'
- Click the 'Add' button at the top.
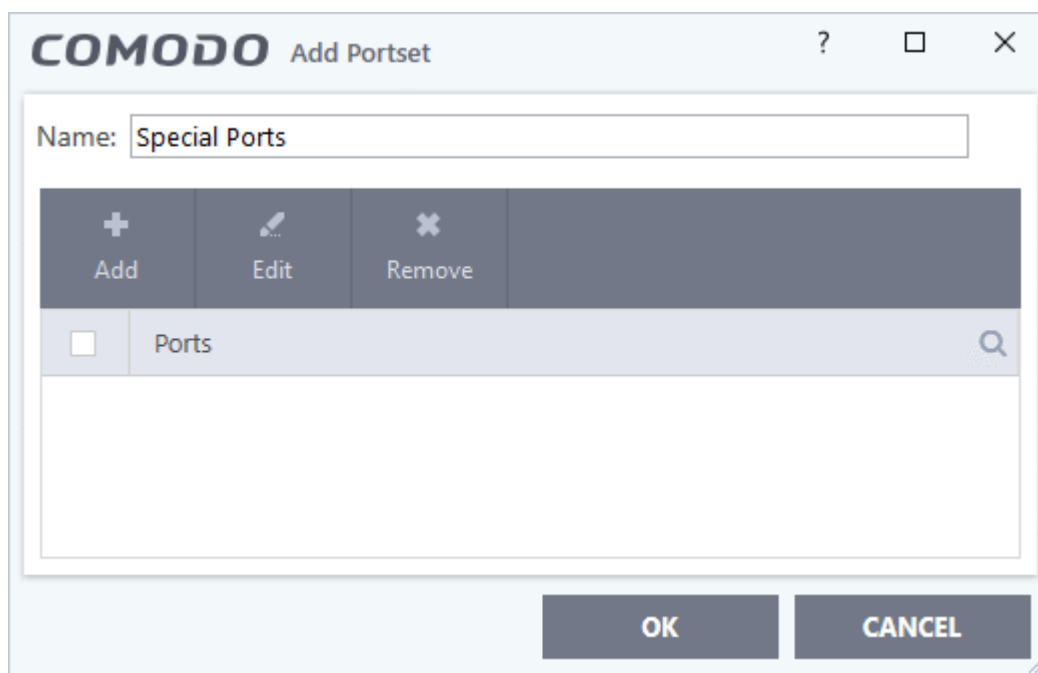
- Create a name for the port set
- Click 'Add' to specify ports and port ranges for the set:
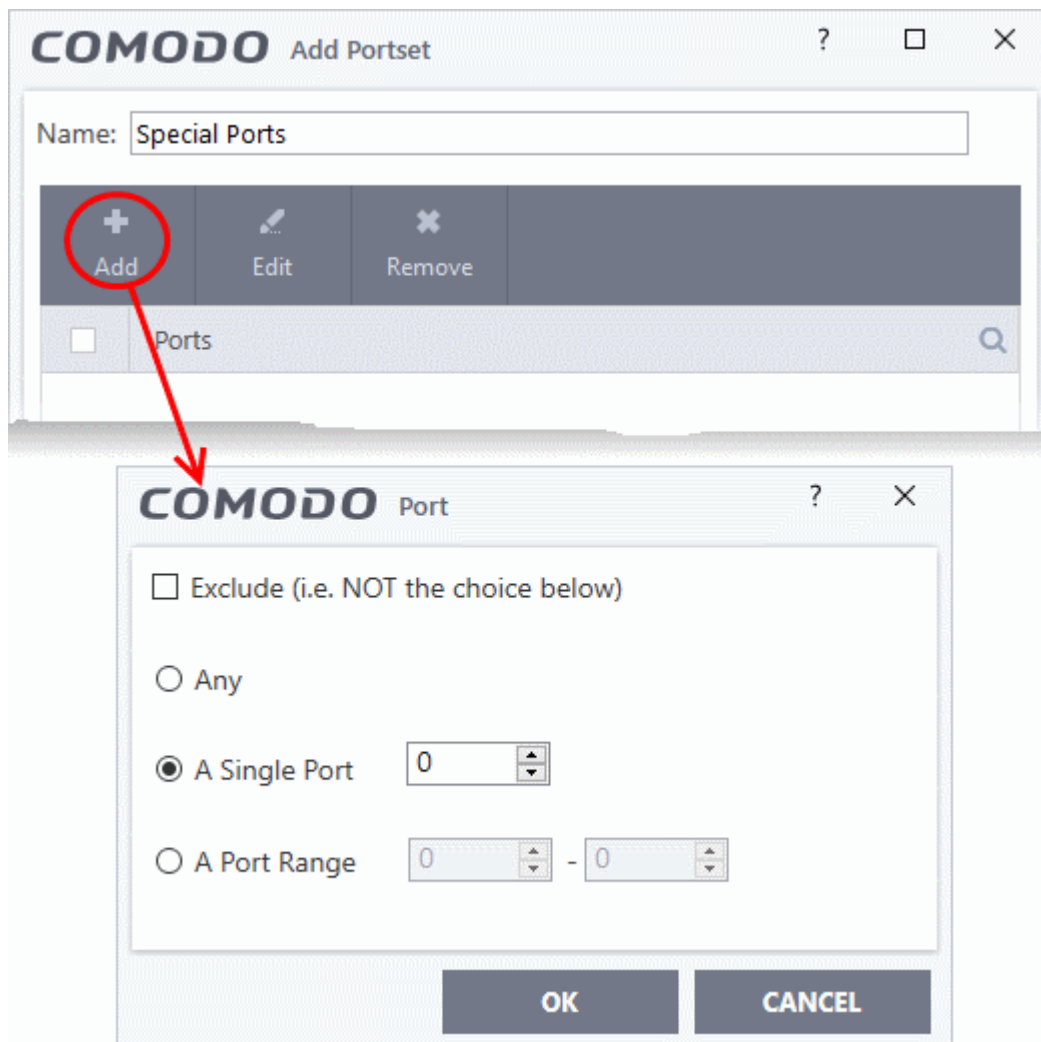
- Specify the ports to be included in the new portset:

  - **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.

- Click 'OK' in the 'Port' dialog then 'OK' in the 'Add Port sets' interface.

  You can now select 'A Set of Ports', then choose this rule-set, when **creating or modifying a Firewall Ruleset**.
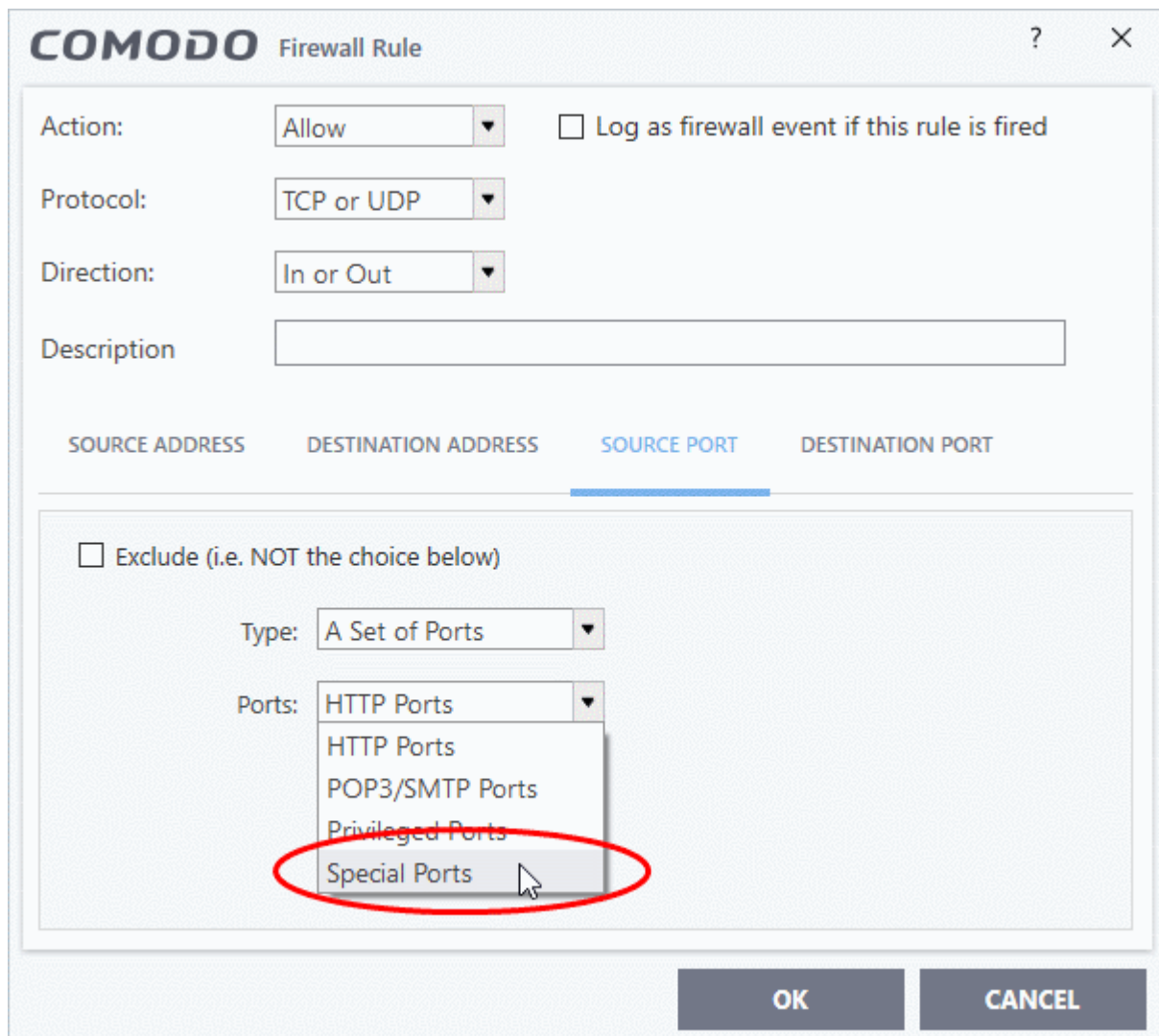
Edit an existing port set

- Click 'Settings' on the CIS home screen

- Click 'Firewall' > 'Portsets'

- Select the port set from the list

- Click the 'Edit' button

- The editing procedure is similar to **adding the portset** explained above.

6.4. HIPS Configuration

Click 'Settings' > 'HIPS'

- The host intrusion protection system (HIPS) constantly monitors system activity and stops processes from modifying important files and interfaces.

- 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.

Configure 'HIPS' components

- Click 'Settings' on the CIS home screen to open the 'Advanced Settings' interface.

- Click 'HIPS' on the left:
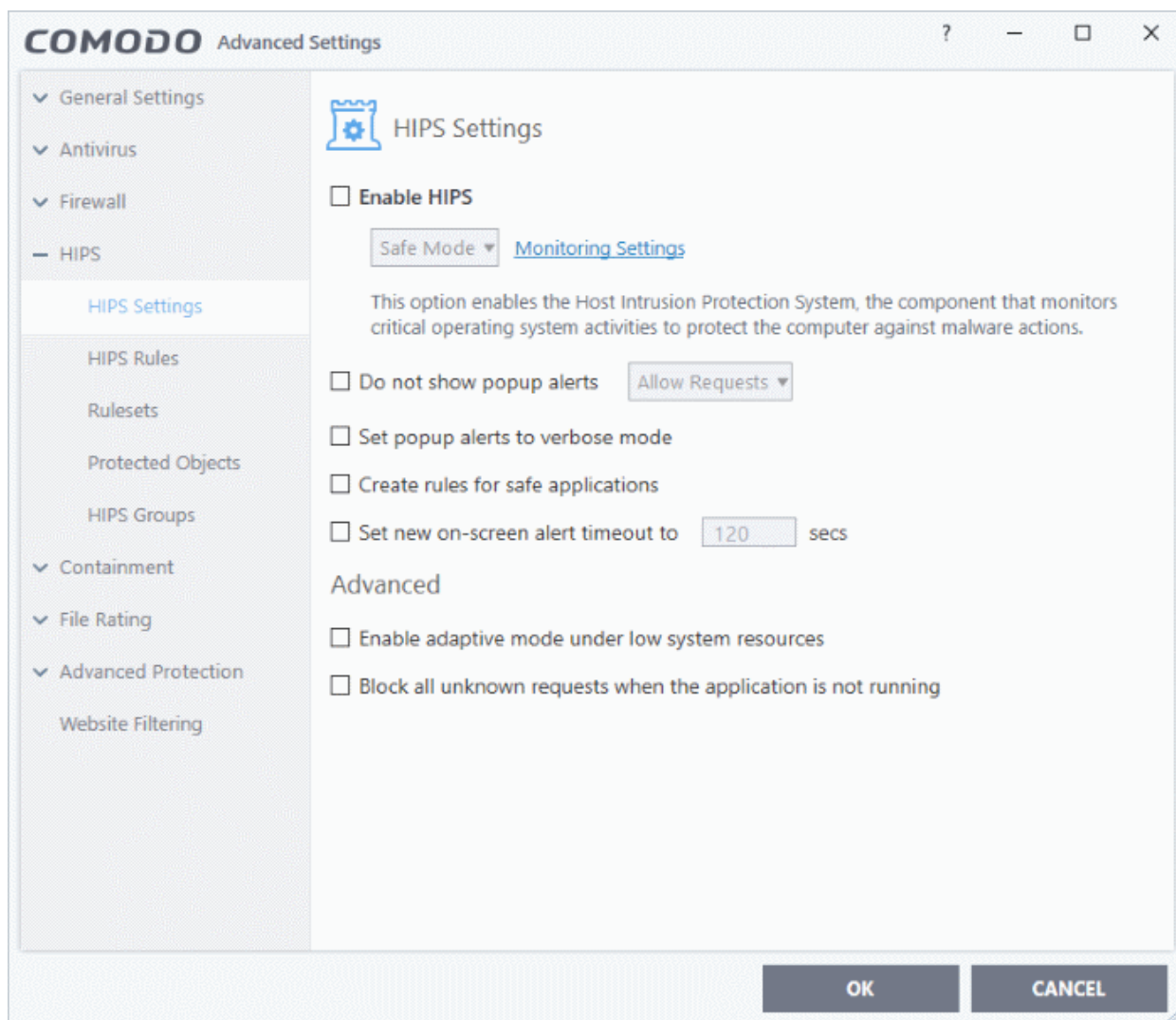
- **HIPS Settings** - General settings that govern the overall behavior of the HIPS component.

- **HIPS Rules** - These rules determine what actions an application is allowed to perform, and what level of protection it enjoys from other processes.

- **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

Click 'Settings' > 'HIPS' > 'HIPS Settings'

• HIPS settings let you enable/disable HIPS, set HIPS security level, and configure the general behavior of the HIPS module.

Open the 'HIPS Settings' panel

• Click 'Settings' on the CIS home screen

• Click 'HIPS' > 'HIPS Settings'
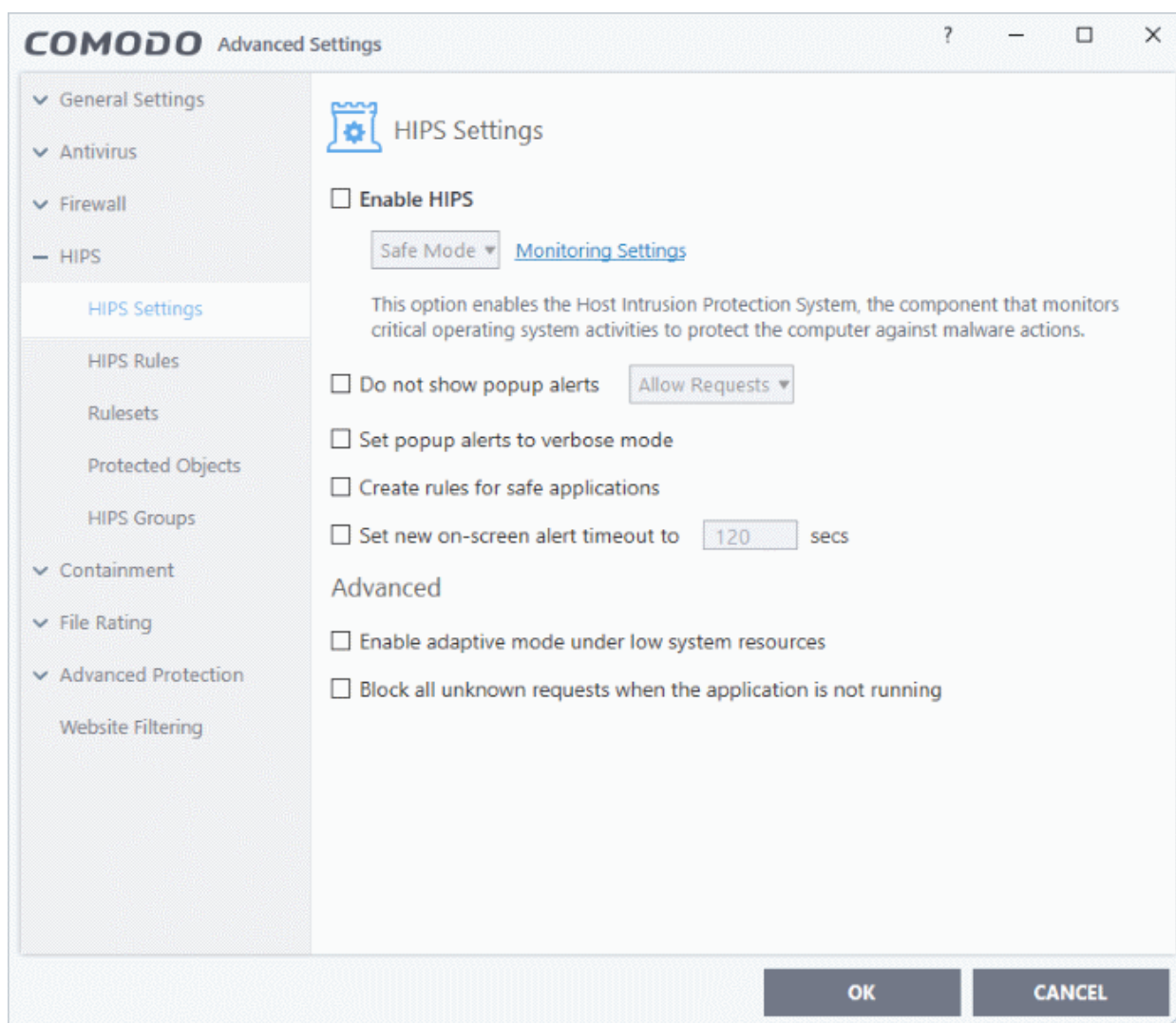
• **Enable HIPS** - Activate or deactivate the HIPS protection. *(Default=Disabled)*

If enabled, you can configure the HIPS security level and monitoring settings:

Configure HIPS Security Level

• Choose the security level from the drop-down under the 'Enable HIPS' check-box:
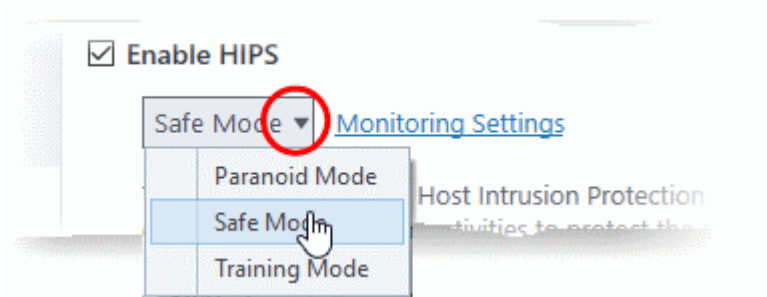
The choices available are:

- **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.

Configure 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.
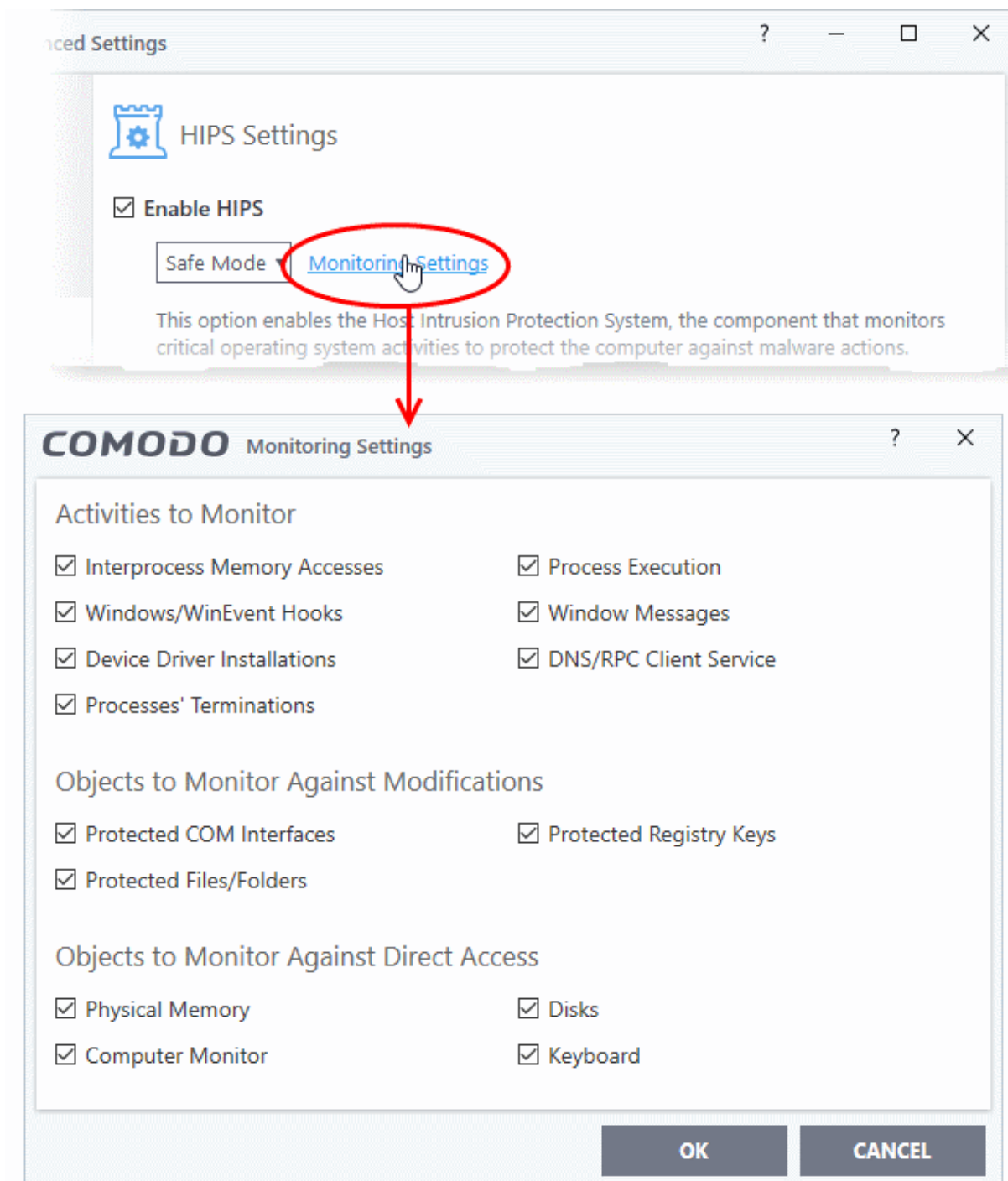
Activities To Monitor:

- **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'.
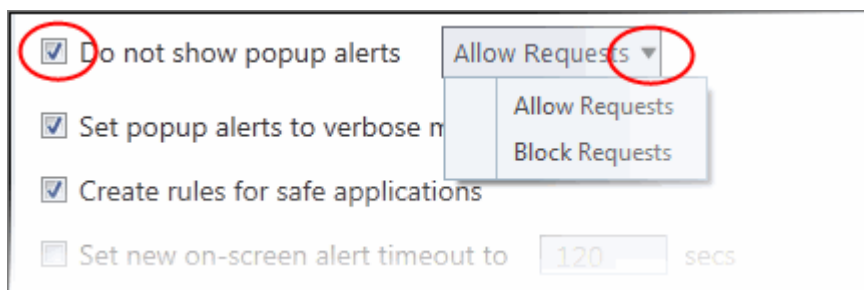
- **Set popup alerts to verbose mode** - HIPS alerts provide more information and options for the user to allow or block the requests *(Default = Disabled).*

- **Create rules for safe applications** - HIPS trusts applications if:

  - The application is on the Comodo safe list, a global white-list of trusted software.
  - The application has a 'Trusted' rating in the local file list. See **File List** if you need more details.
  - The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file. See **Vendor List** if you need more details.

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)*

6.4.2. Active HIPS Rules

Click 'Settings' > 'HIPS' > 'HIPS Rules'

- The rules screen shows your installed applications classified into file groups, and the HIPS ruleset that applies to them.

- You can change the ruleset of a specific application or file group, and create your own custom rulesets.

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.
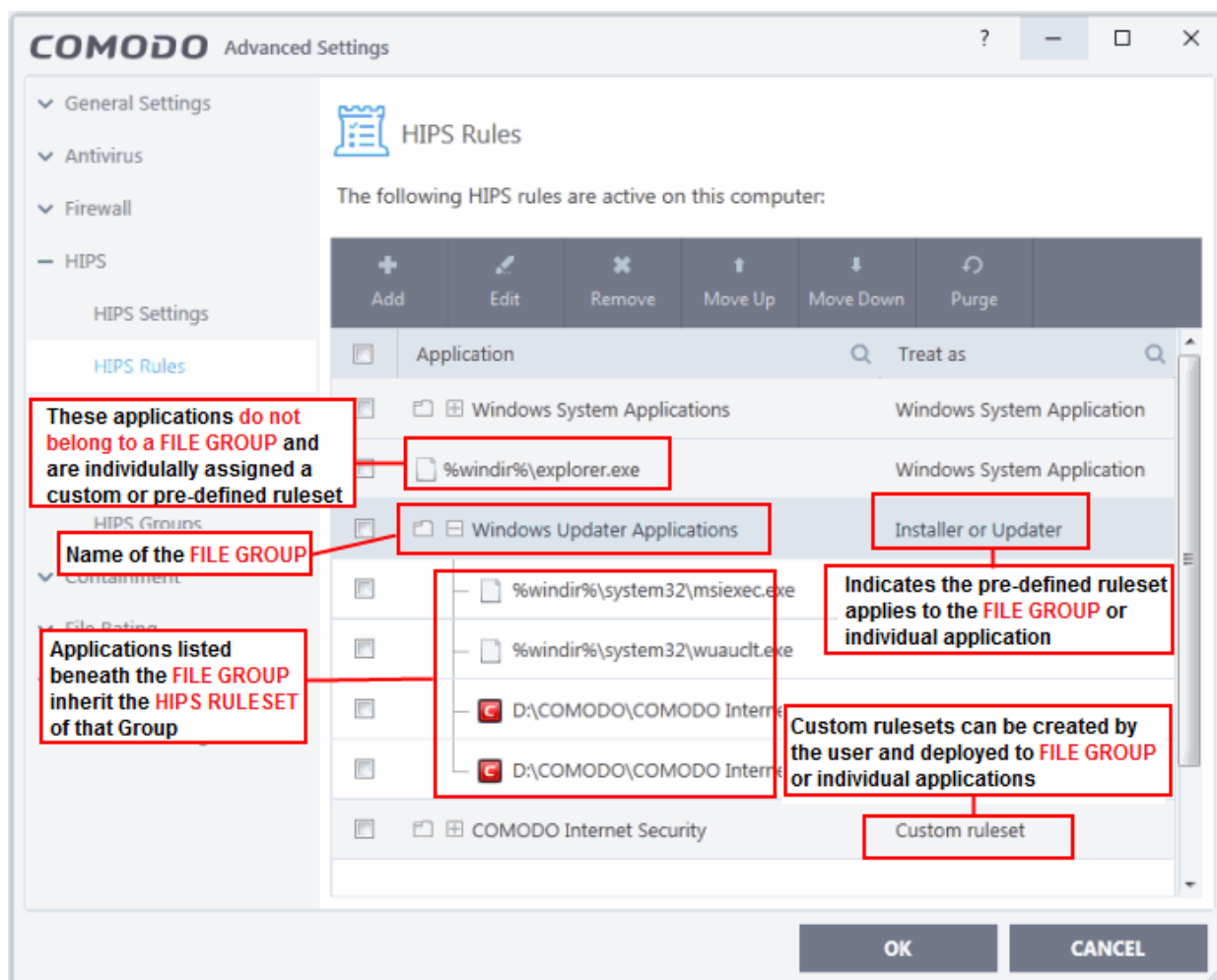
The first column, **Application**, displays a list of the applications on your system for which a HIPS ruleset has been defined. If the application belongs to a file group, then all member applications assume the ruleset of the group. The second column, **Treat As**, displays the name of the HIPS ruleset 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.
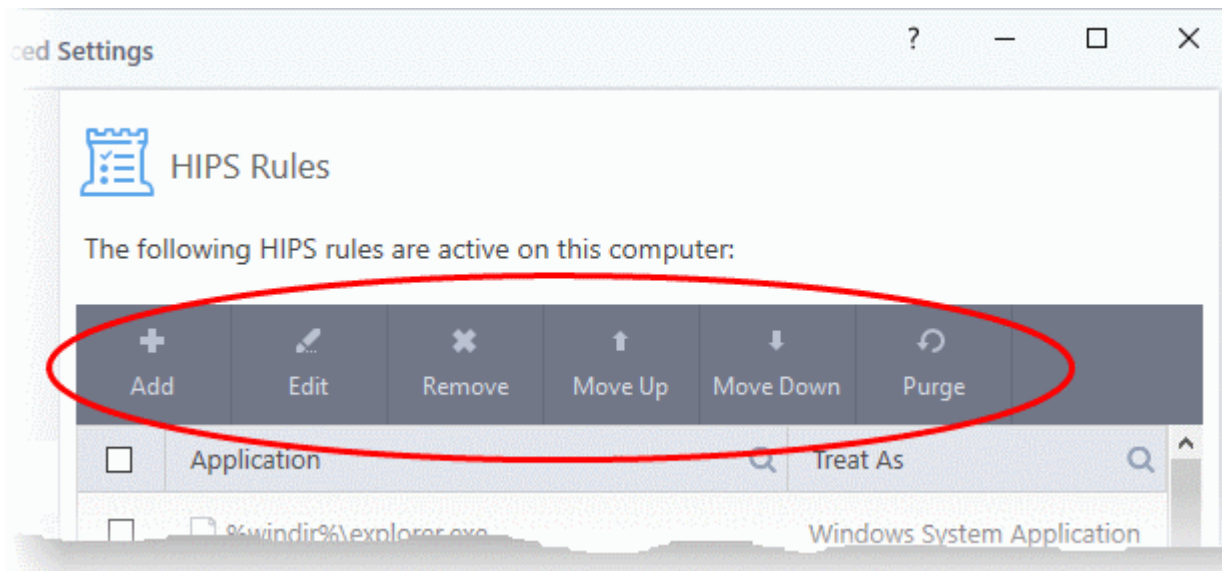
General Navigation:

The control buttons at the top of the list enable you to create and manage application rule sets.

- **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.
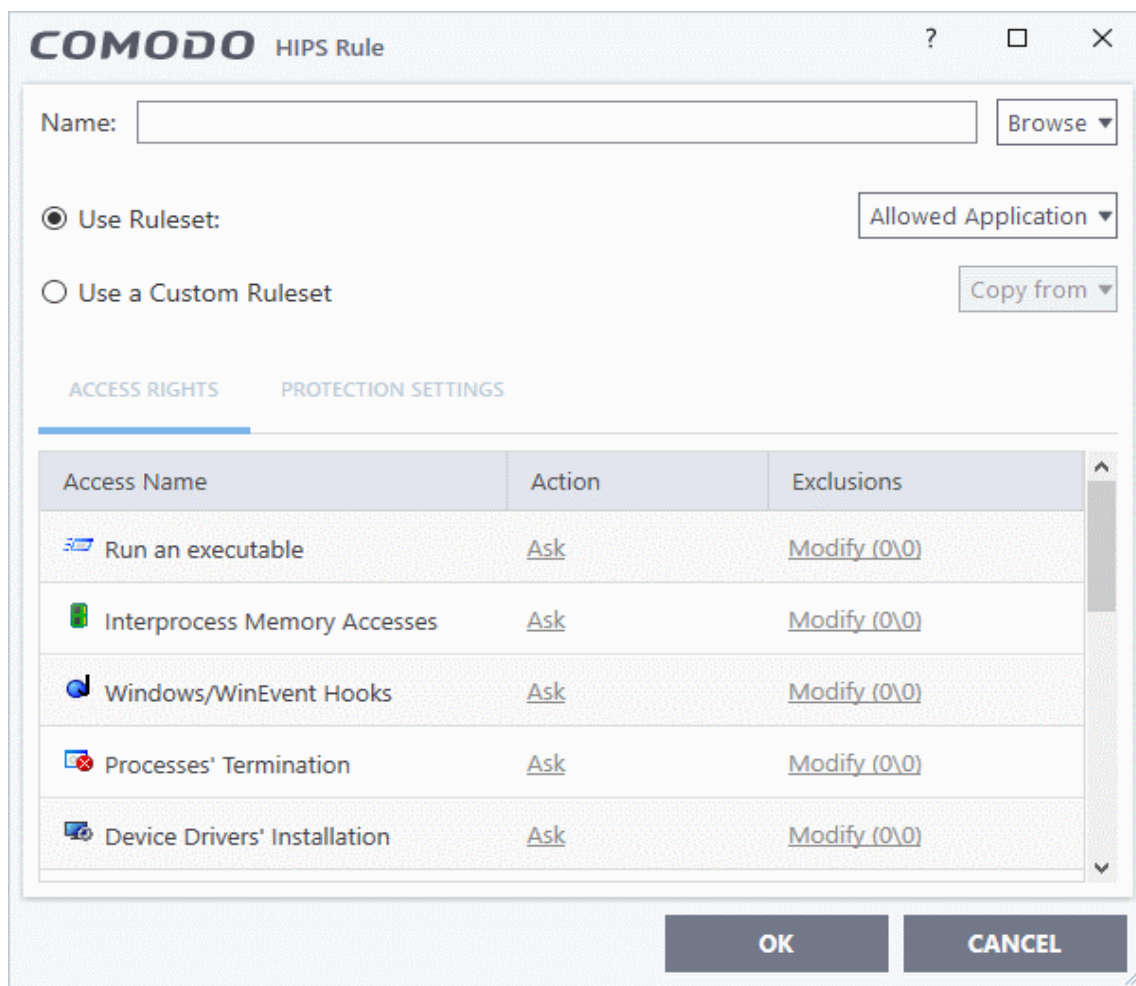
The 'Name' box is blank because you are defining a HIPS rule settings for a new application. If you were editing an existing rule, this field would show the application name and its installation path, or the application group name.

- 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.
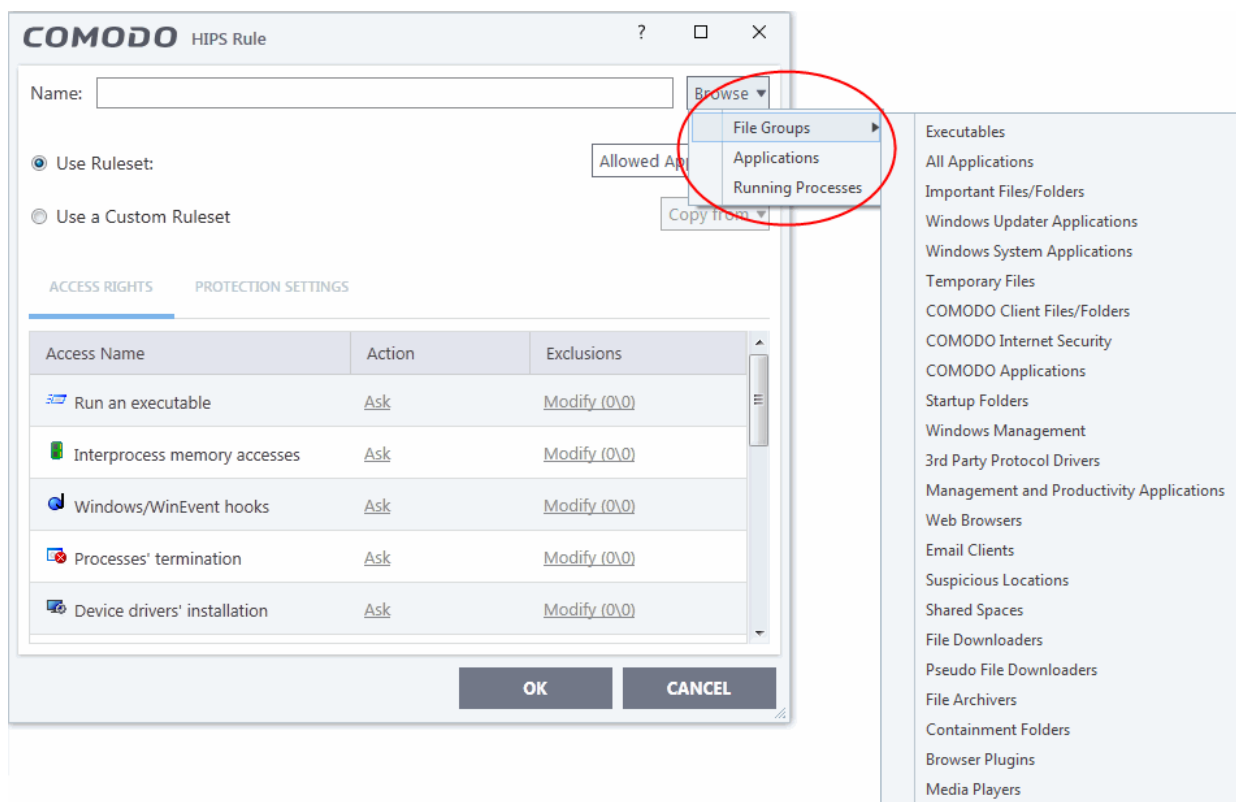
To view the file types and folders that are affected by choosing one of these options, you need to visit the '**File Groups**' interface.

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.

---
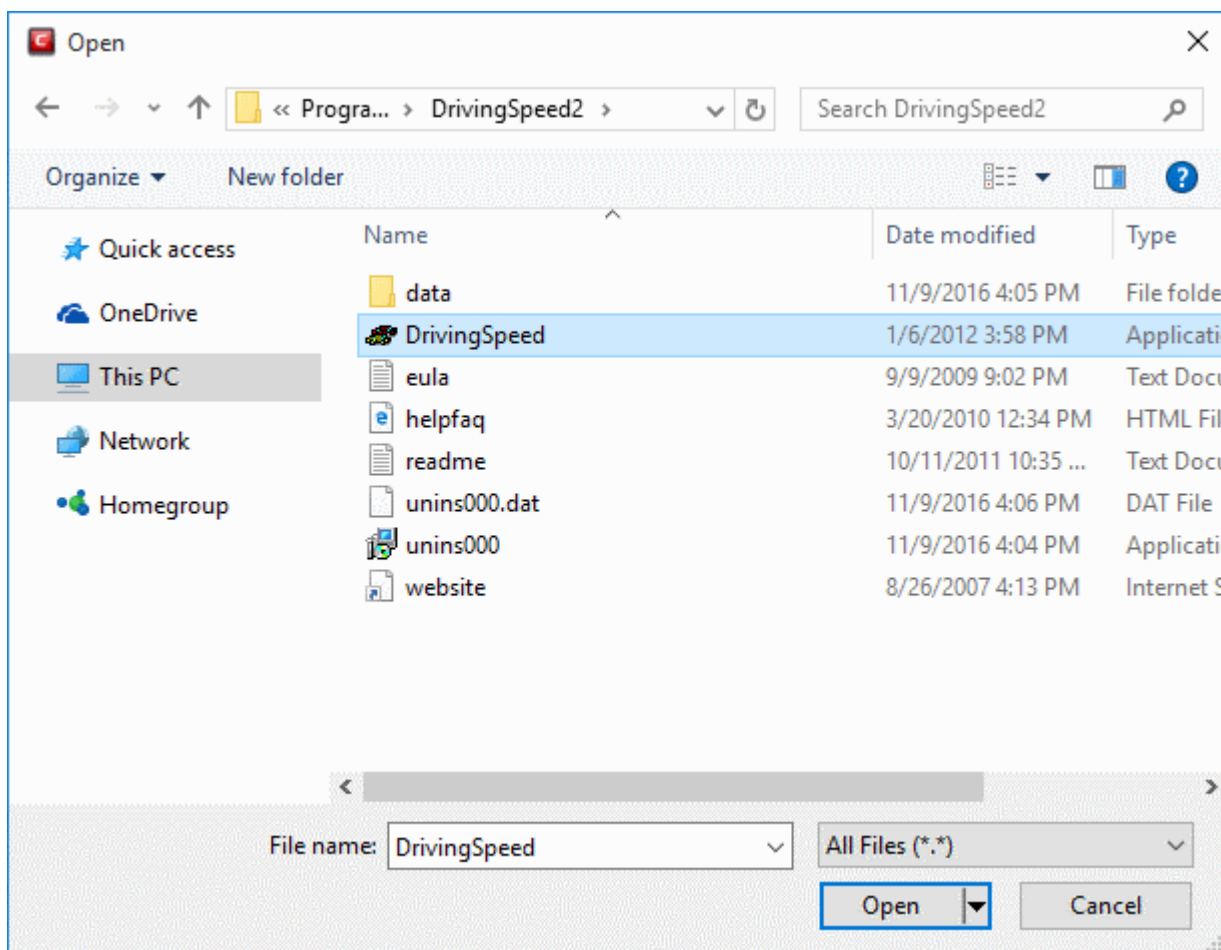
3. **Running Processes** - as the name suggests, this option allows you choose any process that is currently running on your PC in order to create and deploy a ruleset for its parent application.
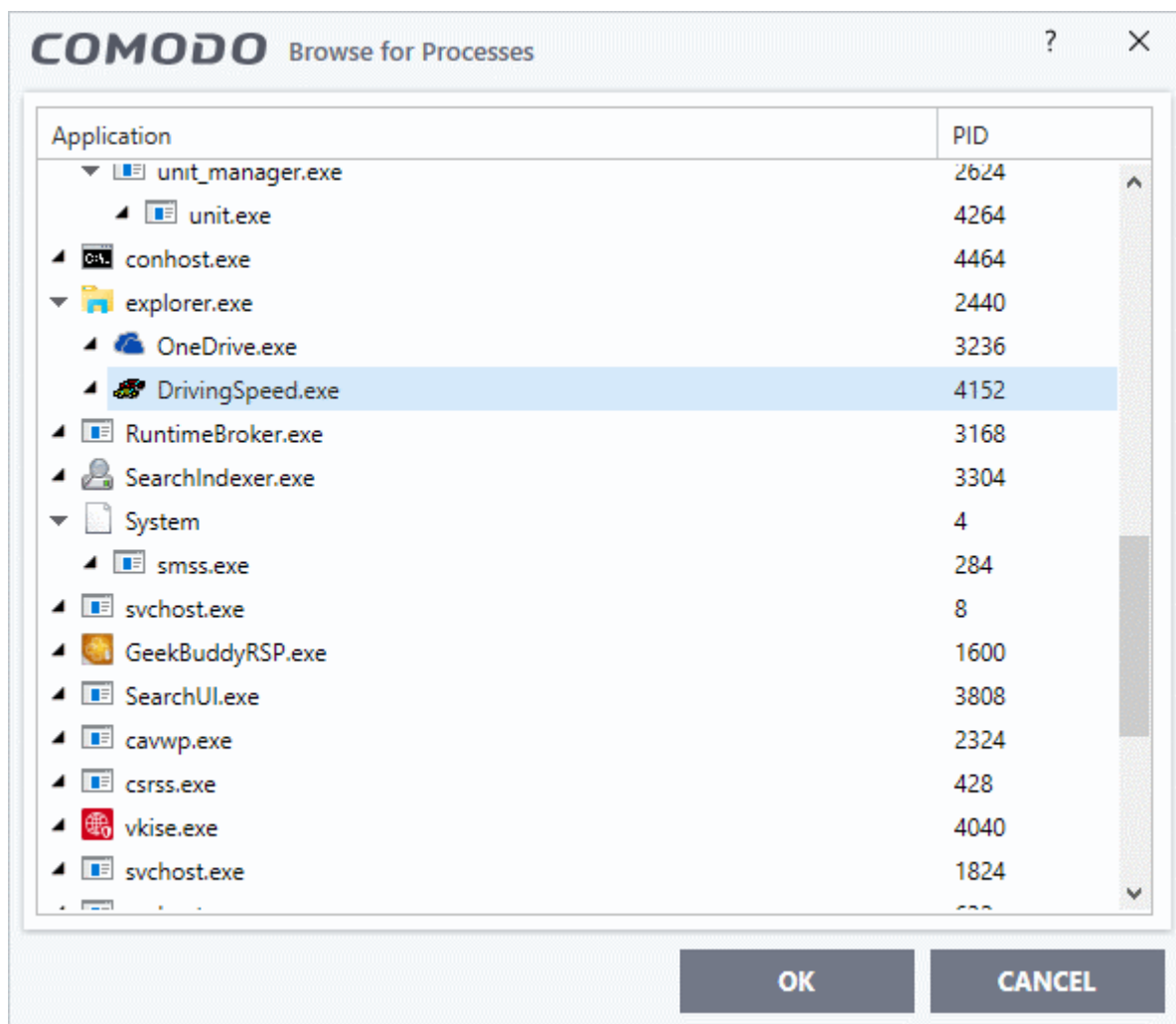
Having selected the individual application, running process or file group, the next stage is to configure the rules for this ruleset.

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).*
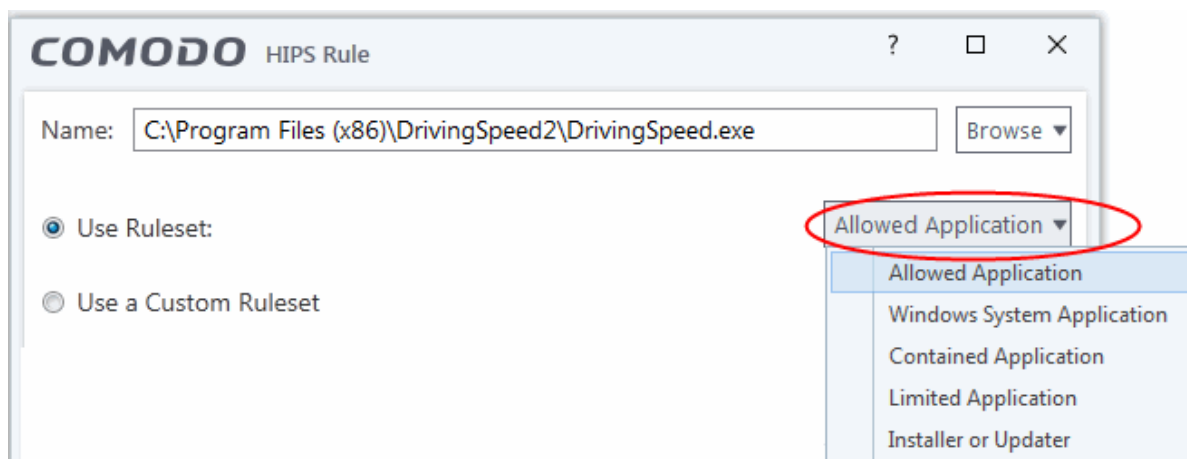
Note on 'Installer or Updater' Rule : Applying this rule to an application defines it as a trusted installer. All files created by this application will also be trusted. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo 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.
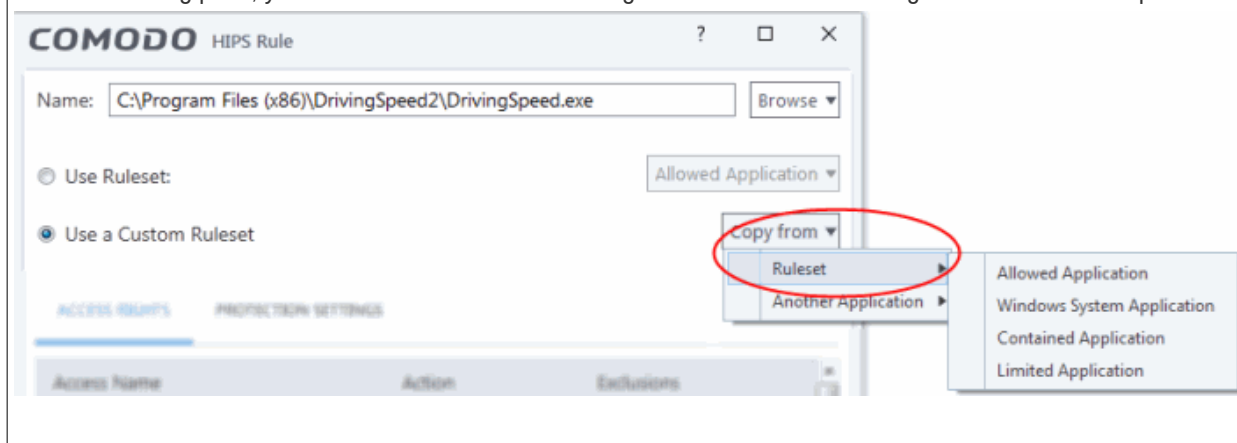
   i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset. These activities are called 'Access Names'.
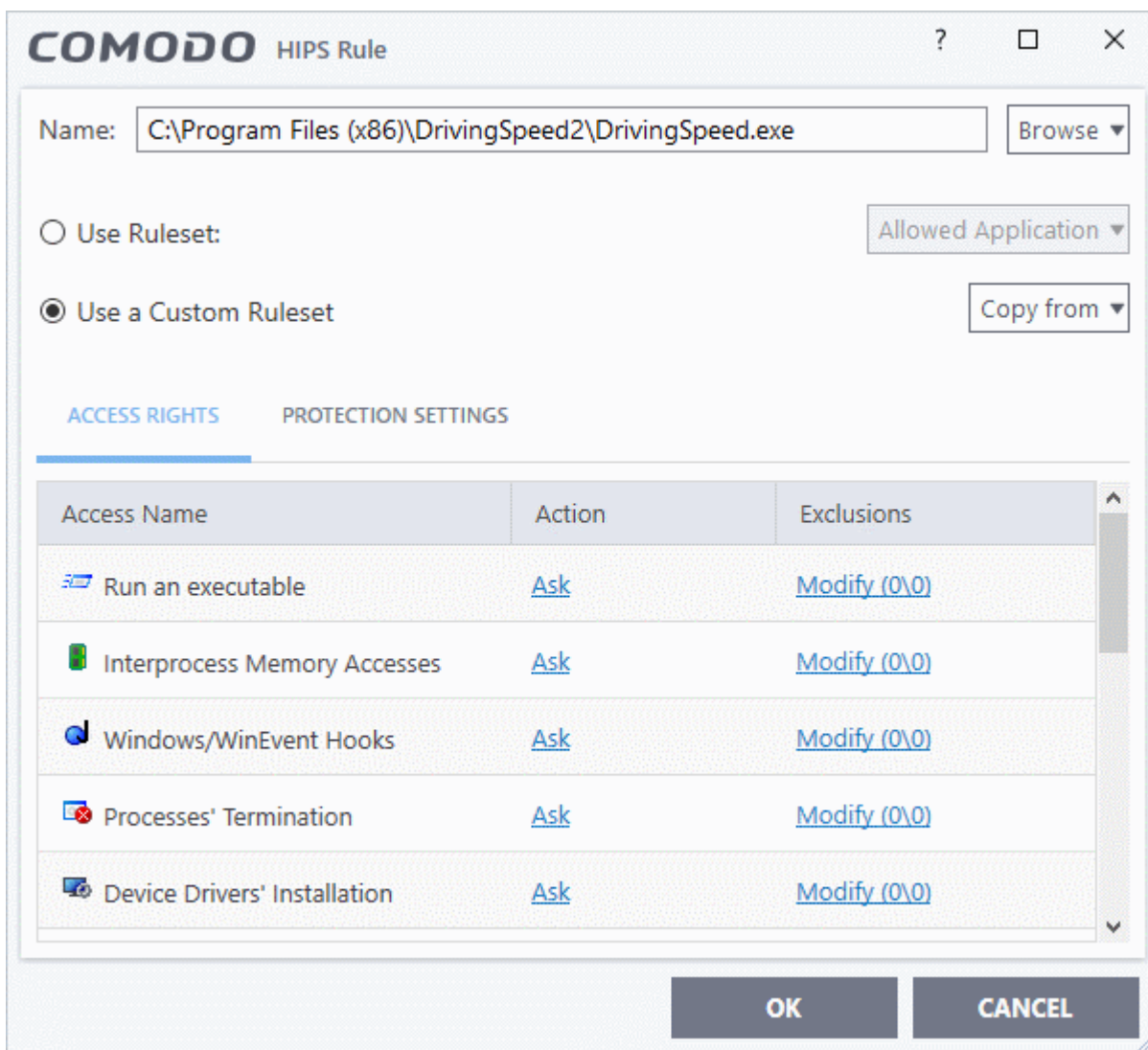
See **HIPS Settings > Activities to Monitor** to see definitions of the 'Action Names' listed above, and the implications of choosing 'Ask', 'Allow' or 'Block':
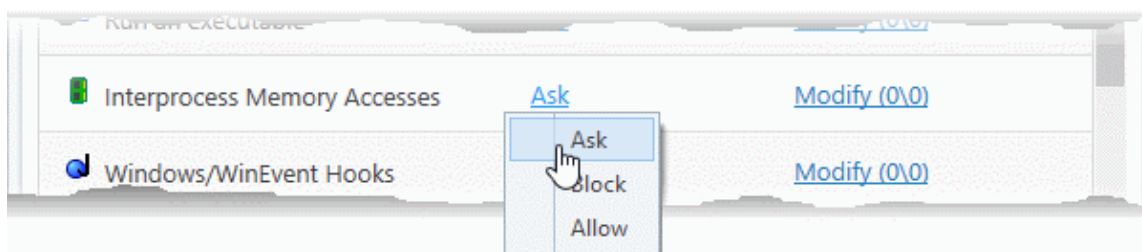
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.

- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.
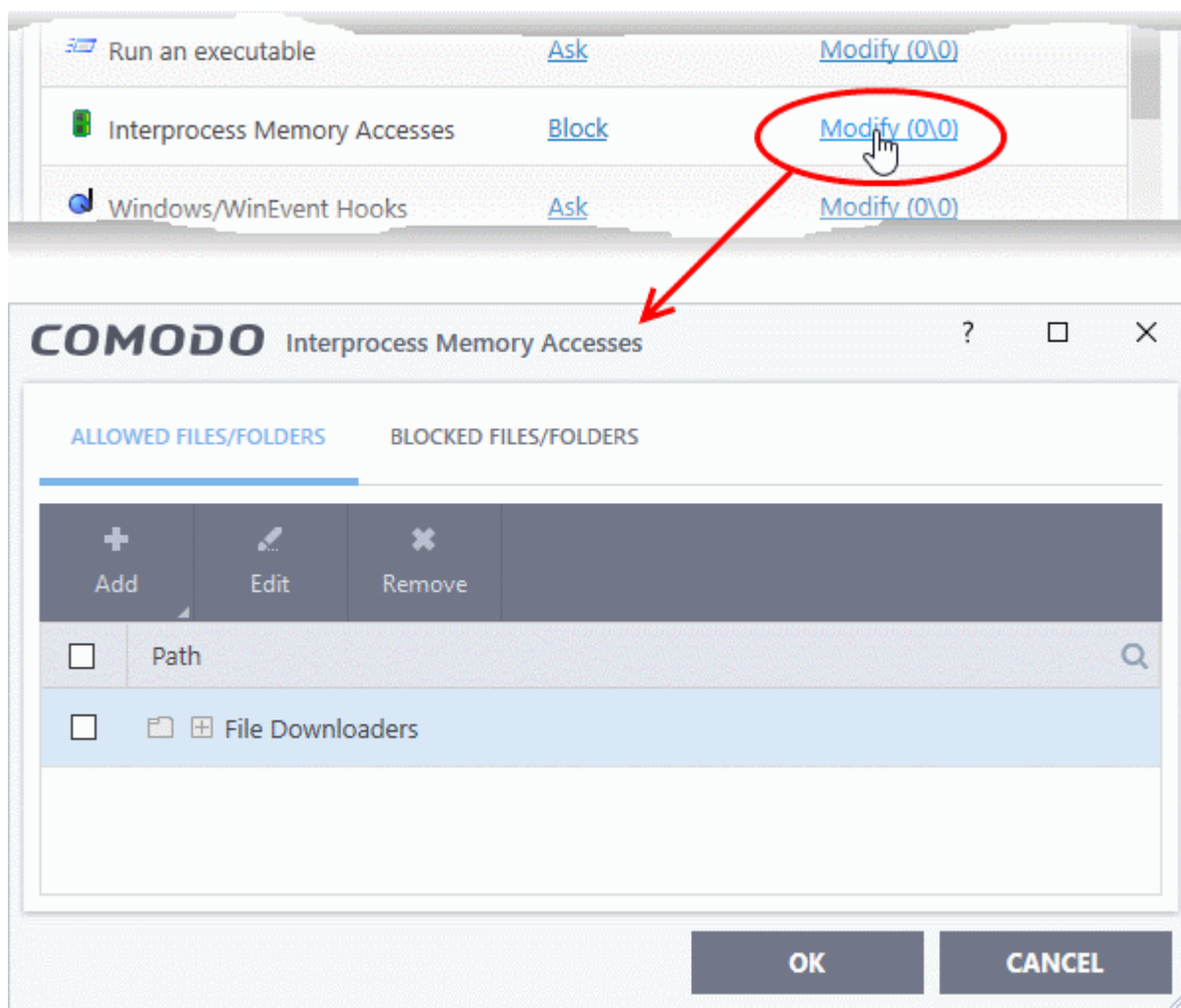
Clicking the 'Add' button at the top allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

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'.
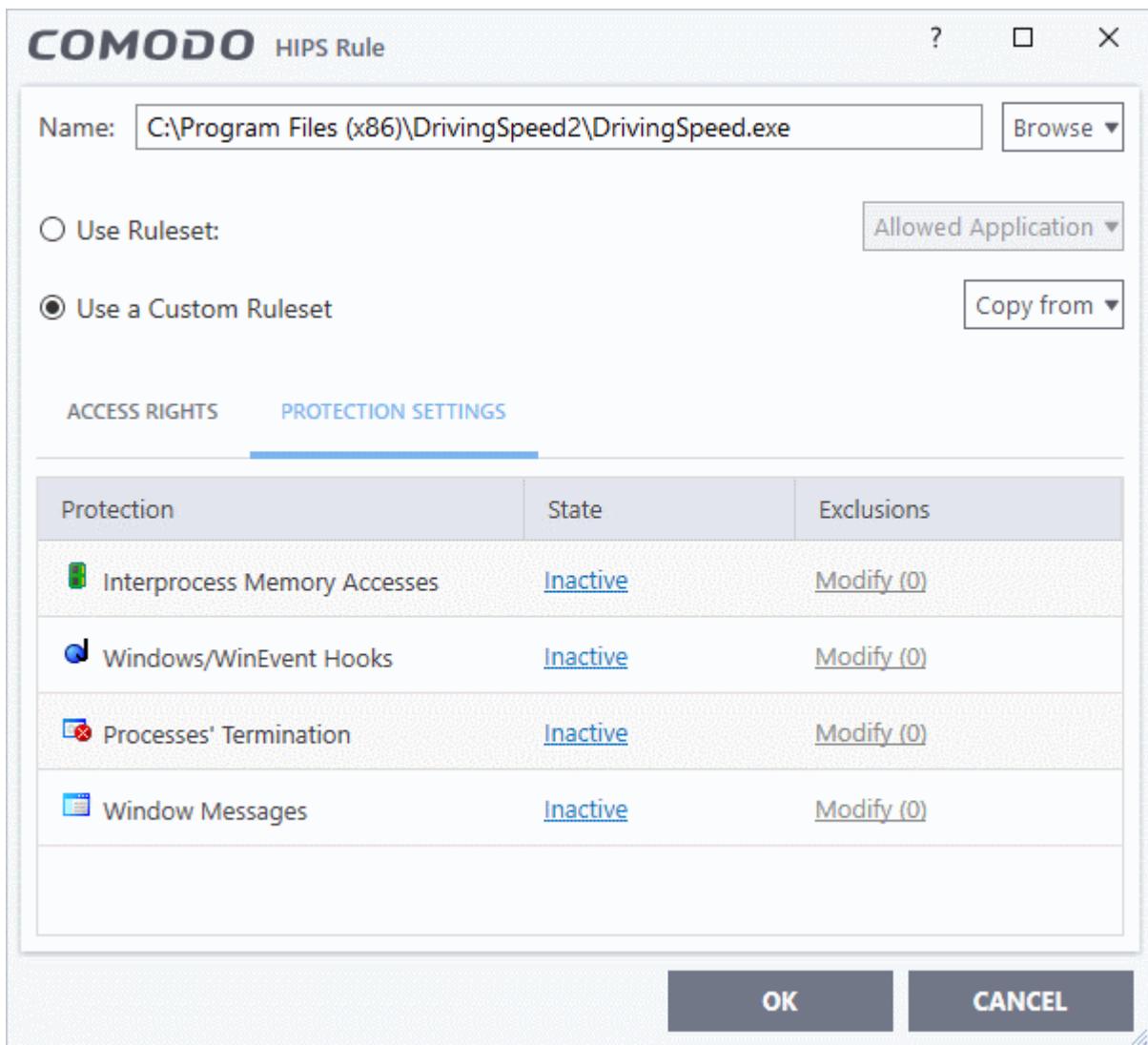
- Set the 'State' as 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection' column. Select 'Inactive' to disable such protection.

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

Click 'Settings' > 'HIPS' > 'Rulesets'

- A ruleset is a collection of **access rights and protection settings** that can be deployed to applications on your computer.
- 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.
- CIS ships with six predefined rulesets that provide a very high level of protection. You can also create your own.

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 provide a set of pre-defined rulesets which optimize security on a range of application types.

- You can modify these predefined rulesets to suit your requirements.
- You can also create new custom rule sets with your own constituent rules
- You can also apply a HIPS ruleset to an application at a HIPS alert. Both predefined and custom rulesets are made available. An example alert is shown below:
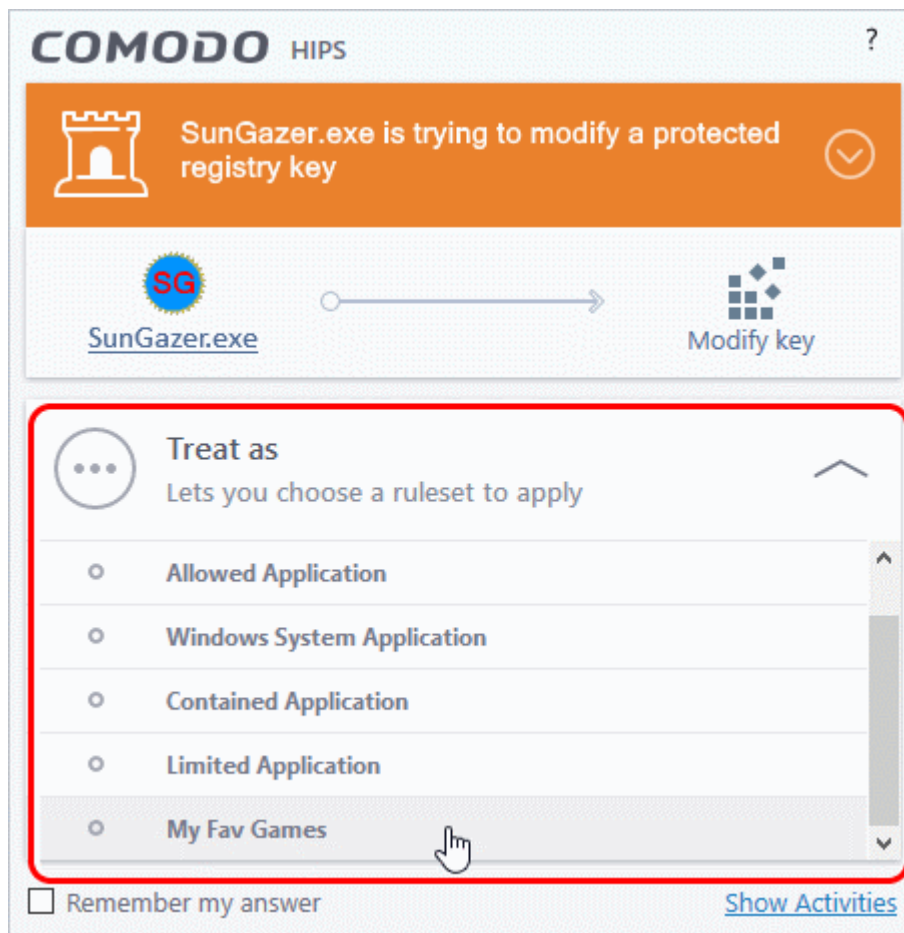
- See **answering HIPS alerts** if you want more help with alerts.

View the list of HIPS Rulesets

- Click 'Settings' at the top of the CIS home screen
- Click 'HIPS' > 'Rulesets' on the left.
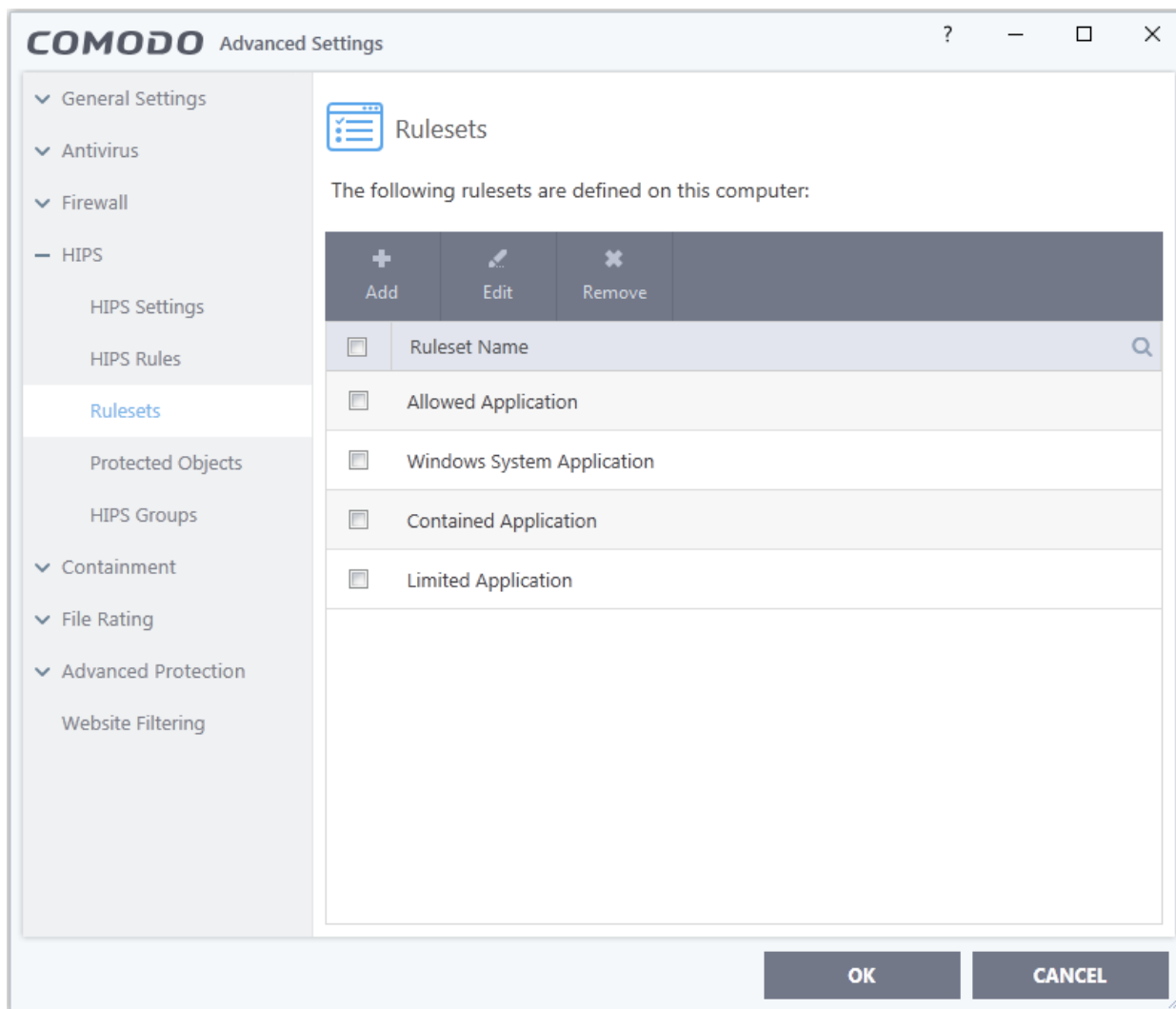
- Click the search icon and enter the name of a ruleset name in full or part to search for a specific ruleset.

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.

Create a new ruleset

- Click the 'Add' button at the top of the interface
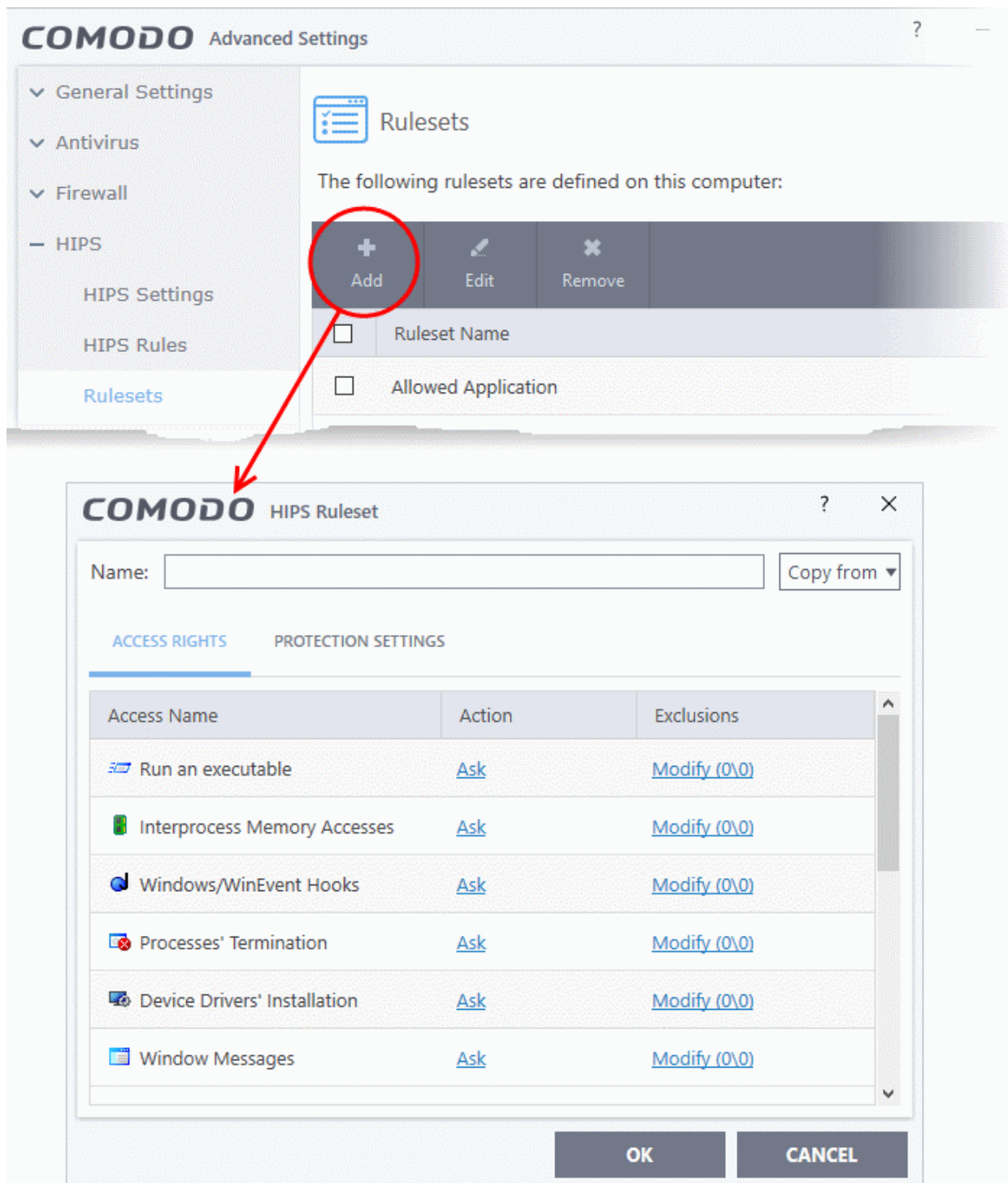
- Enter a name for the new ruleset.
- To copy the **Access Rights** and **Protection Settings** from an existing ruleset, click 'Copy From' and choose the ruleset from the drop-down.
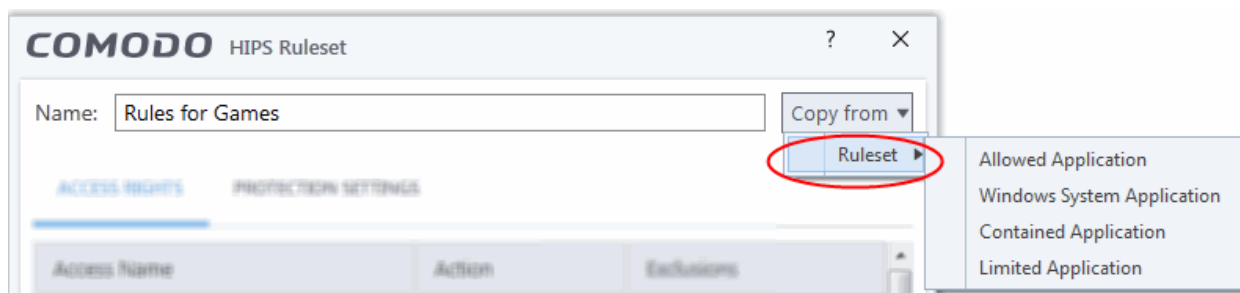
- To customize the **Access Rights** and **Protection Settings** of this new rule set, follow the procedure explained under **Use a Custom Ruleset** in the section **Active HIPS Rules**.

- Click 'OK' to save the new ruleset.
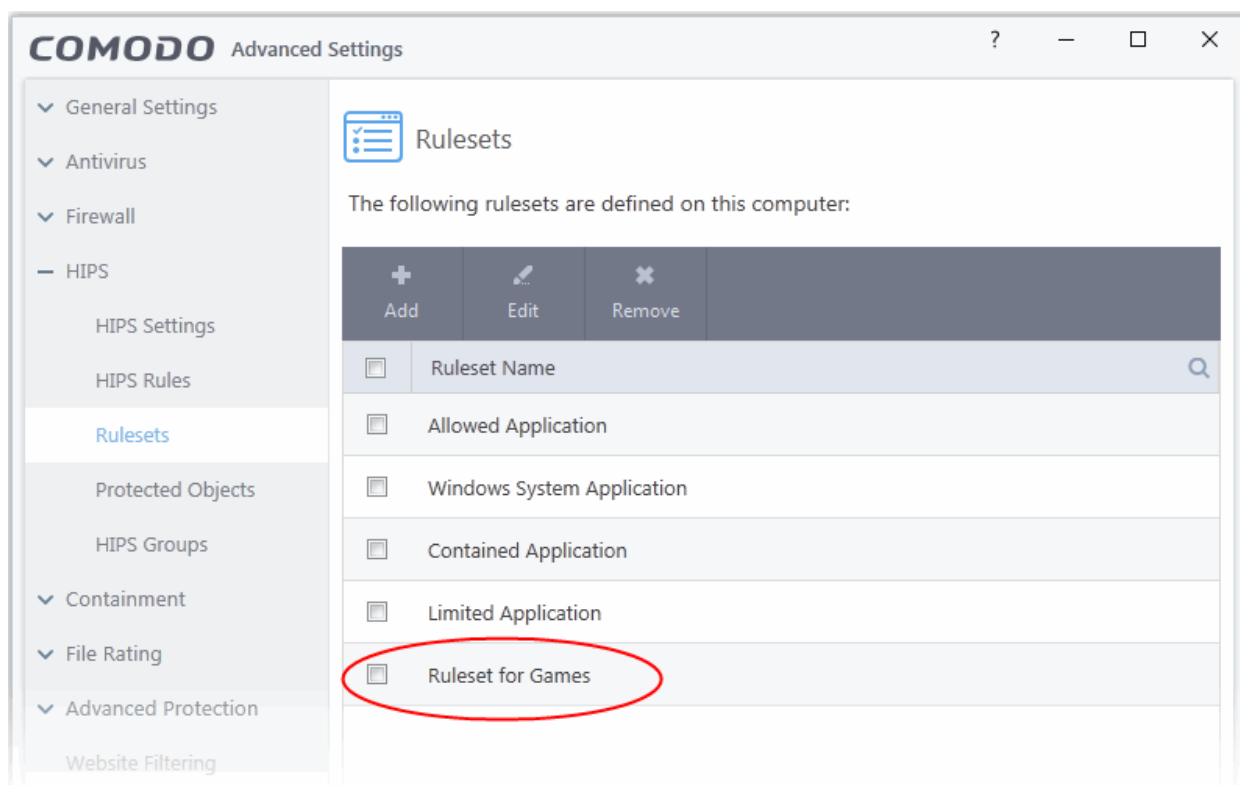
Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.
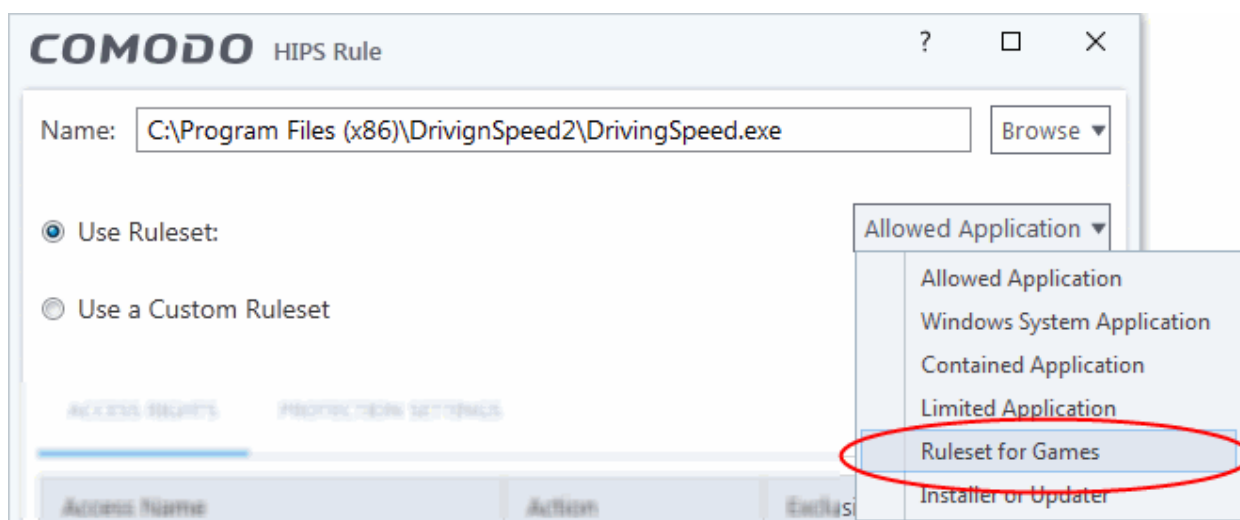
6.4.4. Protected Objects

Click 'Settings' > 'HIPS' > 'Protected Objects'

- The protected objects area lets you specify varying levels of access restriction to files/folders/registry keys on your computer.

    - **Protected Files / Registry Keys / COM interfaces** - Items you add to these areas can be read by other processes, but not modified by them.

    - **Blocked Files** - Items you place in here are completely prevented from opening on your computer. Other processes and users have no access rights at all to them.

    - **Protected Data** - Items in here are invisible to programs which are running in the container. They cannot be seen, accessed or modified by contained applications.

- You can protect files, folders, registry keys and COM interfaces

Open the protected objects interface

- Click 'Settings' at the top-left of the CIS home screen

- Click 'HIPS' > 'Protected Objects':
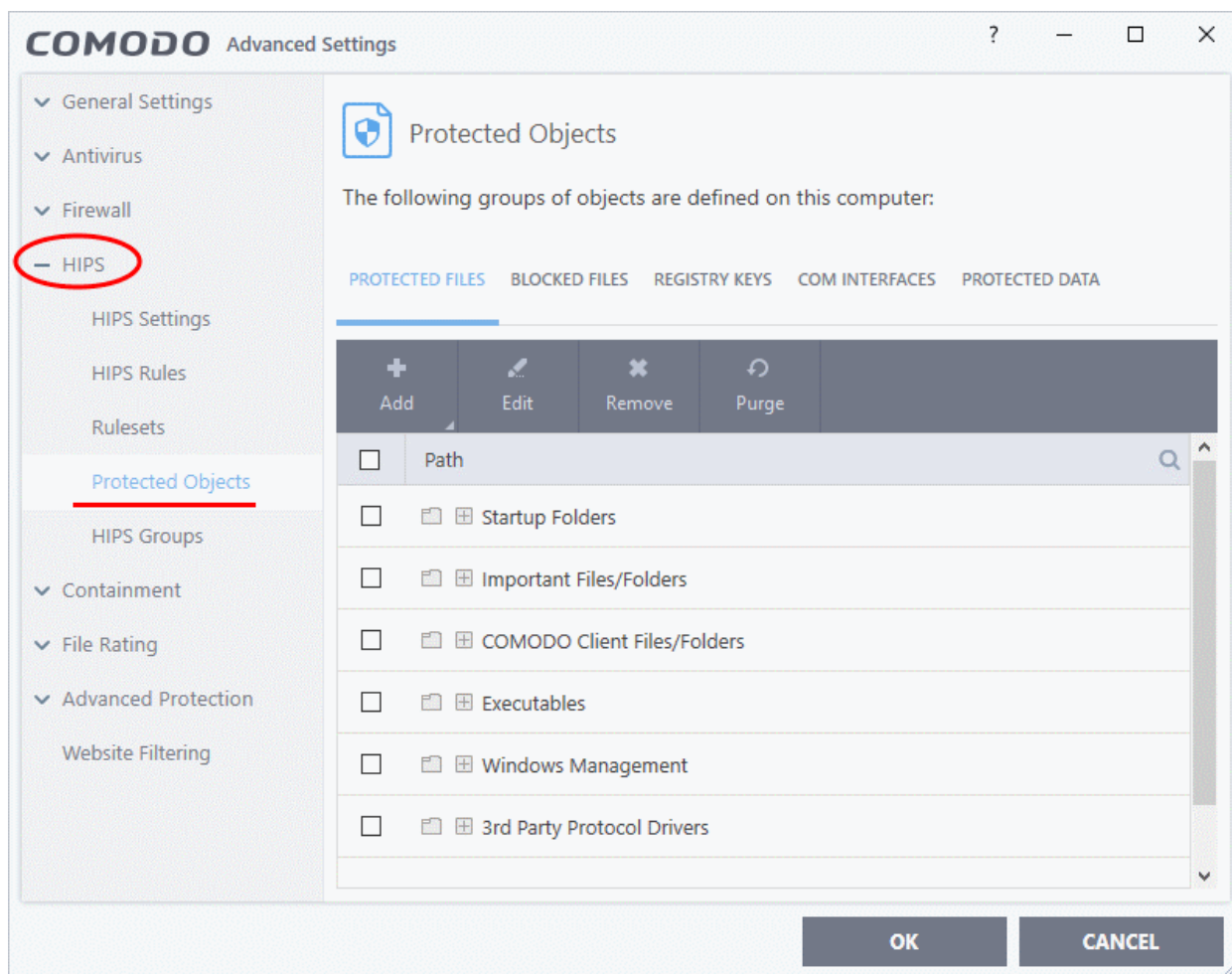
Click the following links to jump to the section you need help with:

- **Protected Files**

- **Blocked Files**

- **Registry Keys**

- **COM Interfaces**

- **Protected Data**

6.4.4.1. Protected Files

Click 'Settings' > 'HIPS' > 'Protected Objects' > 'Protected Files'

- The protected files screen shows file groups to which other processes have read-only access. Programs on your computer can read the items in here, but cannot modify them.

- This prevents malicious programs from modifying important personal or system data.

- A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). This will allow web browsers to use the file as normal, but block any attempts to modify it.

- You could also use this feature to safeguard valuable files (spreadsheets, databases, documents) against accidental or deliberate sabotage.

- You can create exceptions should you want to grant write-privileges to specific applications. See **Exceptions** for more on this.

Open the 'Protected Files' interface

- Click 'Settings' at the top-left of the CIS home screen

- Click 'HIPS' > 'Protected Objects'

- Click the 'Protected Files' tab:
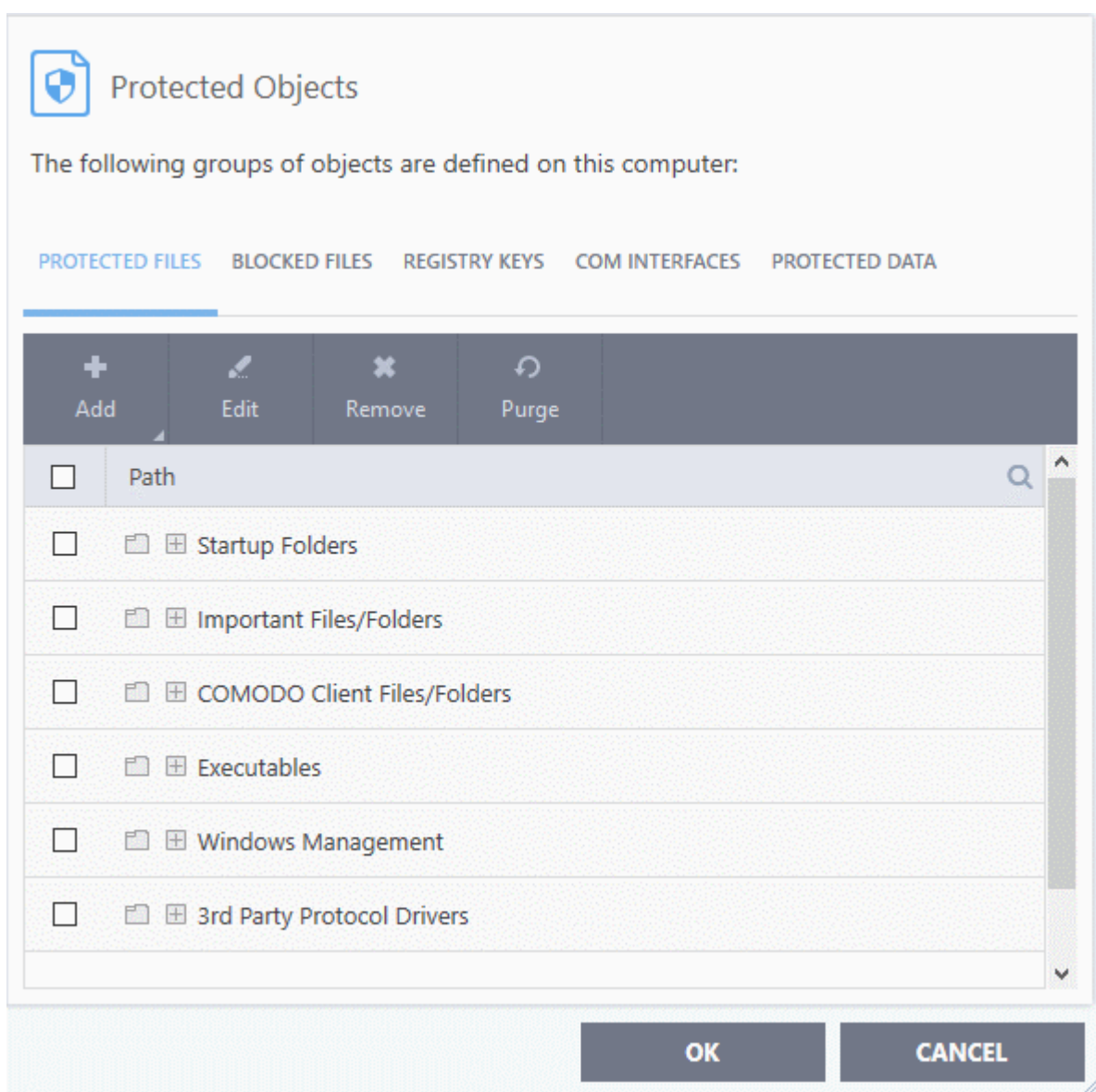
Controls:

The buttons at the top provide the following options:

- **Add** - Protect a new file, file-group, folder or running process
- **Edit** - Modify the path/location of the target item
- **Remove** - Delete a file or file group from protected files
- **Purge** - Runs a check to verify that all files in the list are actually installed at the path specified. If not, the item is removed from the list.

Right-click Options:

- Right-click on an item to open a menu which lets you add, edit, remove and purge files:
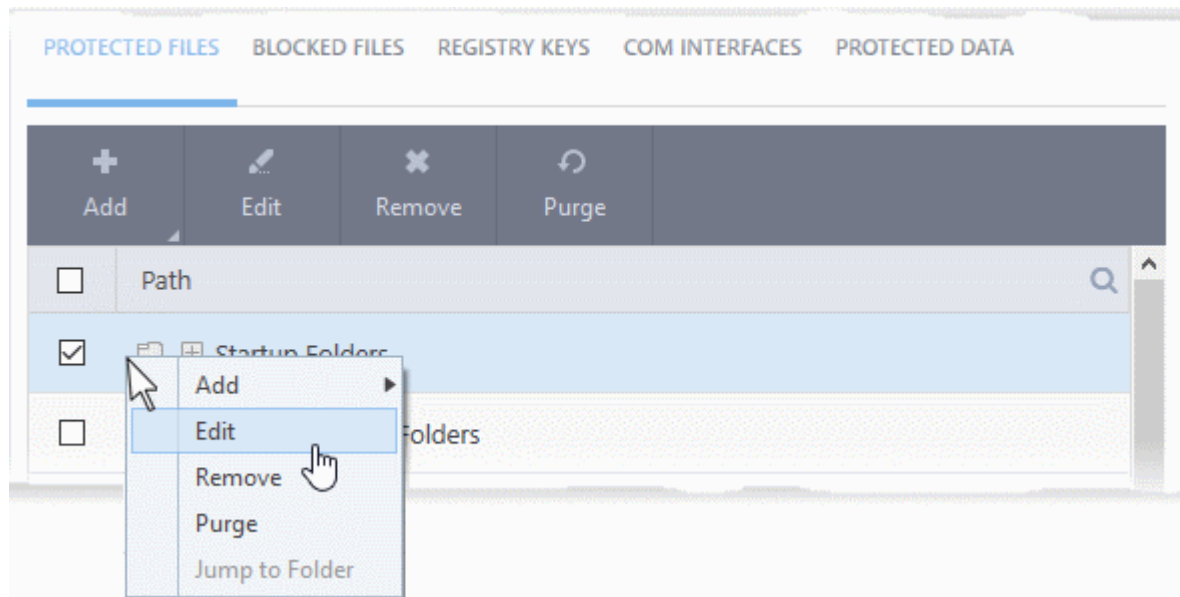
The options available are as described **above**.

See the following sections for help with each task:

- **Add a file. folder or file group to protected files list**
- **Edit the path of a protected item**
- **Remove a protected item from the list**

Manually add an individual file, folder or file group

- Click 'Settings' on the CIS home-screen
- Click 'HIPS' > 'Protected Objects' > 'Protected Files'
- Click the 'Add' button
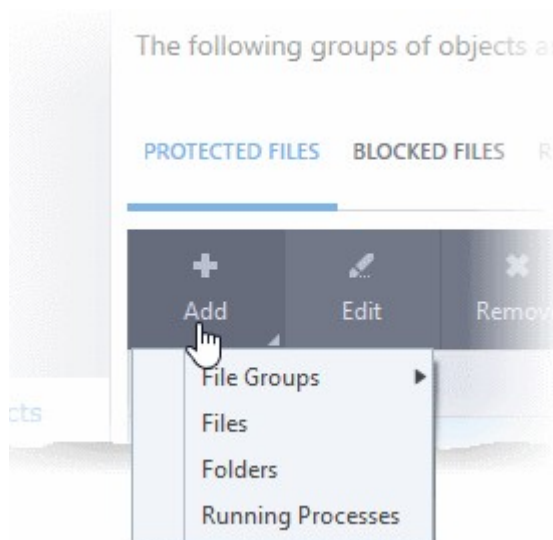
You can add items using any of the following methods:

- **Select from File Groups**
- **Browse to a File**
- **Browse to a Folder**
- **Select from currently running processes**

Add a File Group

- A file group is a pre-set category of files or folders. Adding a file group to protected files is a convenient way to protect an entire class of files and folders.
- For example - by protecting the 'Executables' group, CIS protects all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl *\cmd.exe, *.bat, and *.cmd.
- Other groups protected by default include 'Startup Folders', 'Important Files/Folders' and 'Comodo Client File/Folders'.
- CIS ships with a set of predefined file groups which can be viewed in 'Advanced Settings' > 'File Rating' > 'File Groups'.
- You can also create your own file groups, and add your new group to 'Protected Files'. All items in your group will be covered, including any files you add to the group in future. See **File Groups** if you want to learn more about groups.

Protect a file group

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Files' tab
- Click 'Add' > 'File Groups':
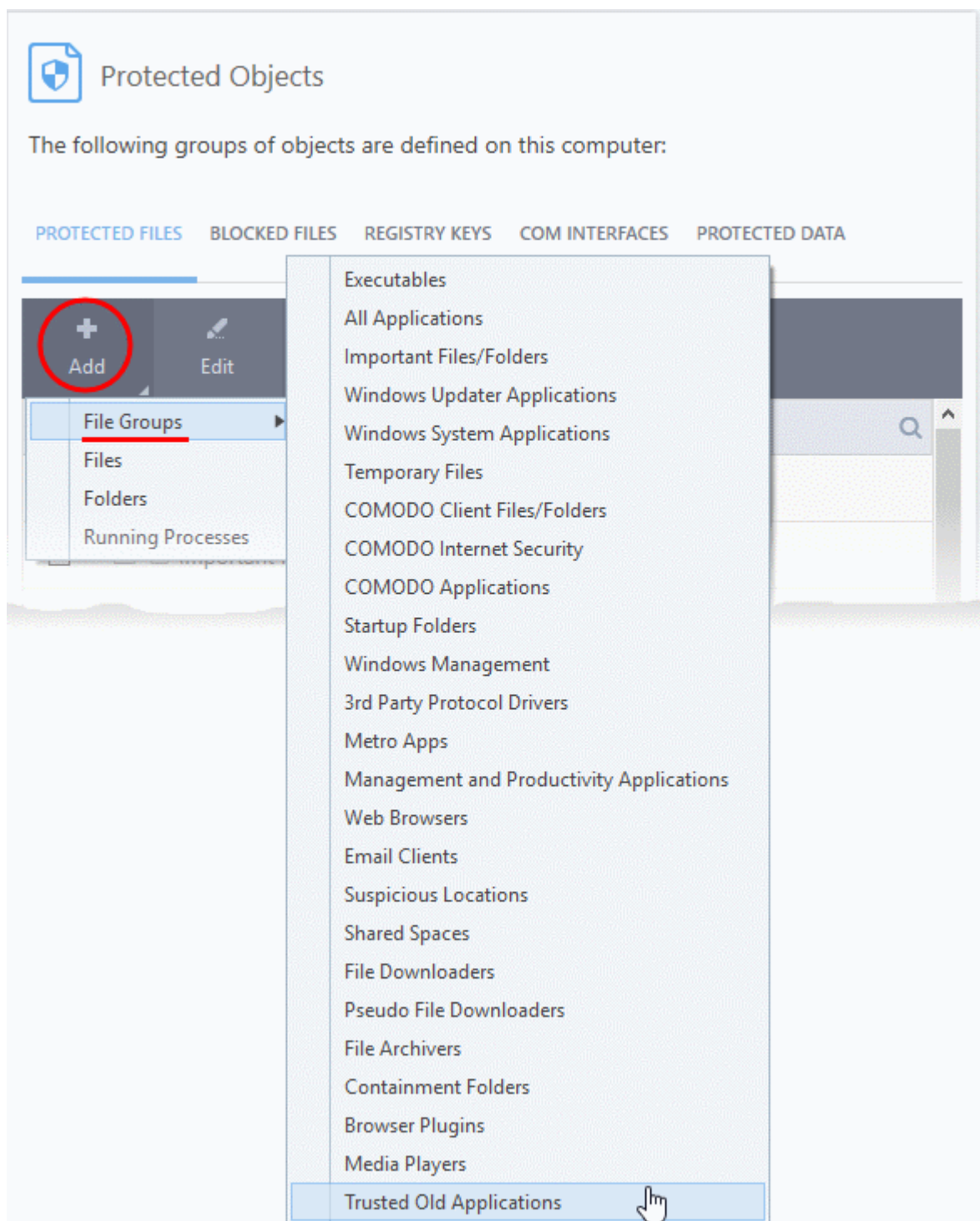

- Select the target group from the list.
- The file group will be added to 'Protected Files' list:

- Repeat the process to add more file groups.
- Click 'OK' in the 'Advanced Settings' interface to save your settings

Add an individual File

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Files' tab
- Click 'Add' > 'Files'

- Navigate to and select the files you want to add and click 'Open'.
- Repeat the process to add more files.
- Click 'OK' in the 'Advanced Settings' interface to save your settings

Add a Drive Partition/Folder

All files in the folder or drive will be protected. This includes items added after the folder was added to 'Protected Files'.

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Files' tab
- Click 'Add' > 'Folders'
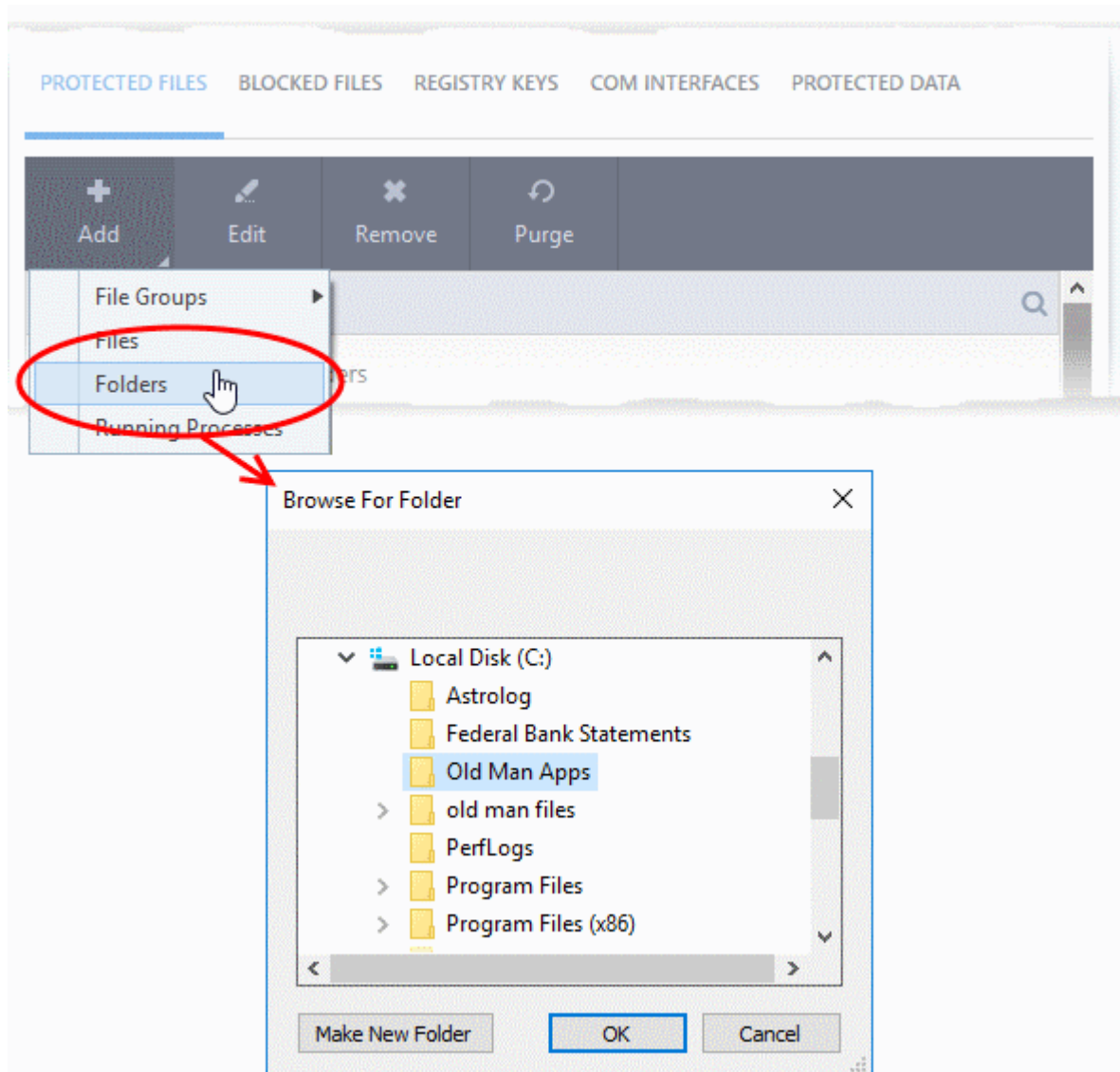
- Browse to the drive or folder you want to protect and click 'OK'.

- Repeat the process to add more folders.

- Click 'OK' in the 'Advanced Settings' interface to save your settings

Add an application from a running process

Adding a running process will add the parent application to protected files.
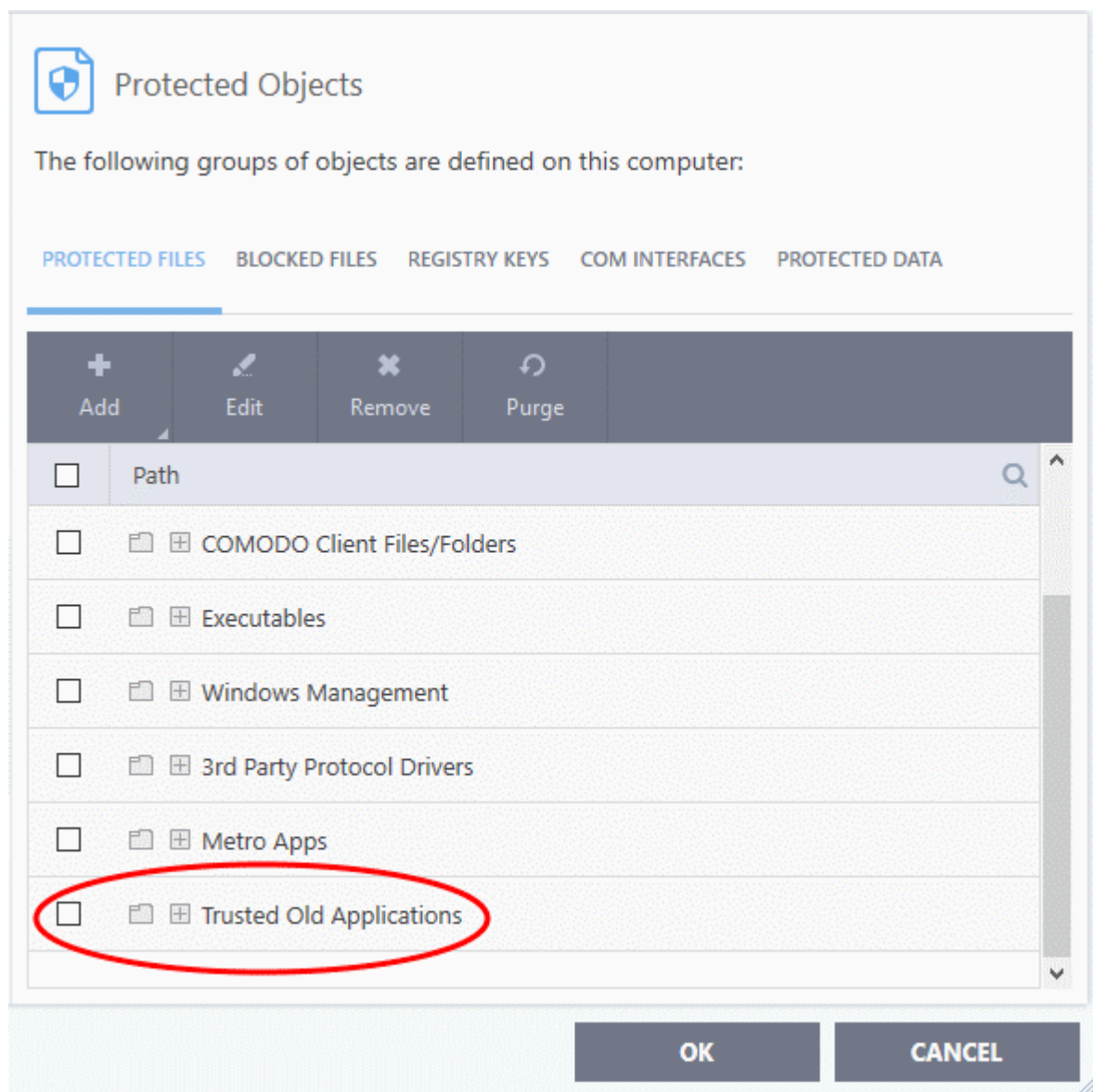
- Click 'Settings' on the CIS home screen

- Click 'HIPS' > 'Protected Objects'

- Open the 'Protected Files' tab

- Click 'Add' > 'Running Processes'
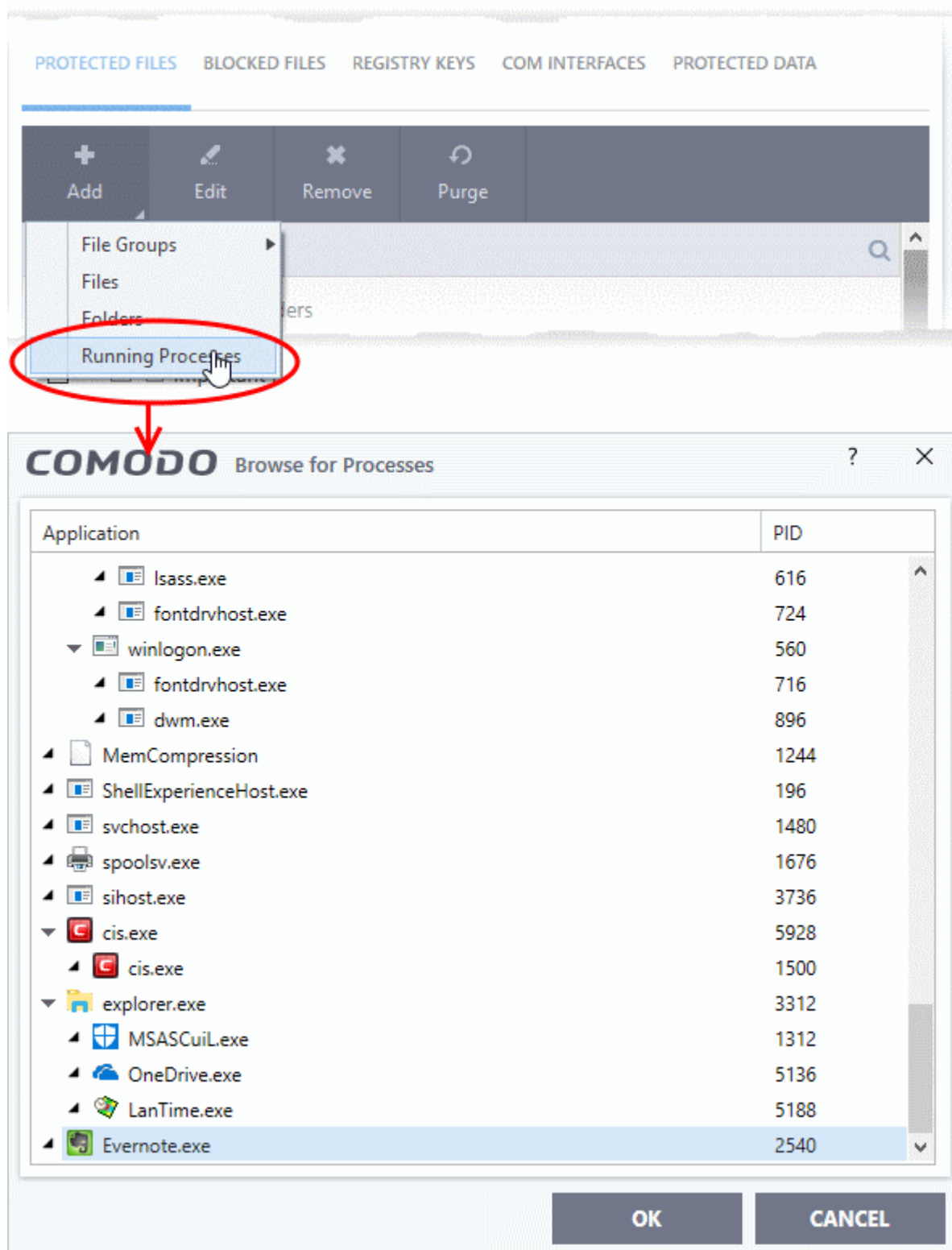
A list of currently running processes in your computer will be shown.

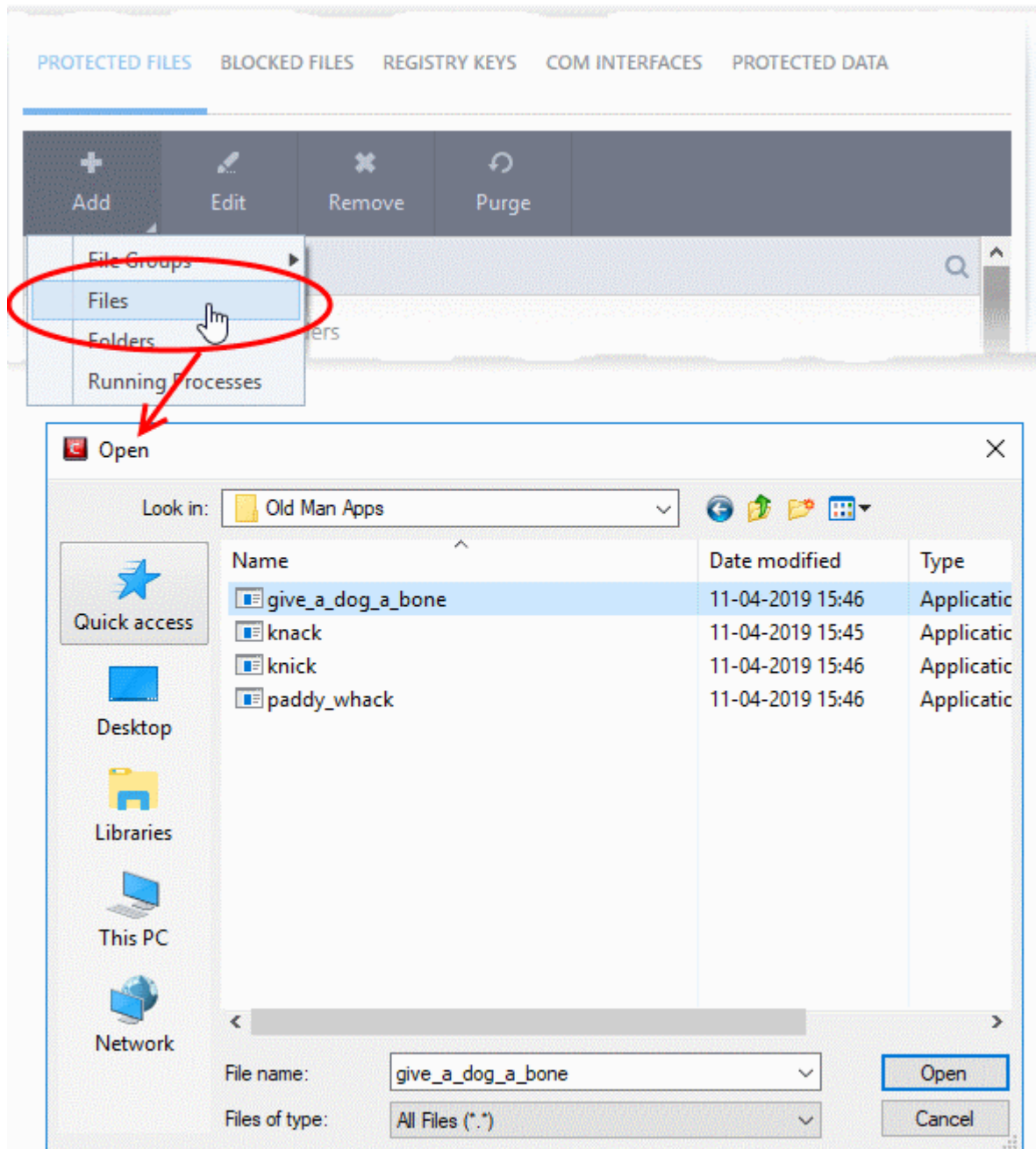- Select the process you want to protect and click 'OK'. The parent application of the process is added to protected files.

- Repeat the process to add more files.

- Click 'OK' in the 'Advanced Settings' interface to save your settings

Edit an item in the Protected Files list

- Click 'Settings' on the CIS home screen

- Click 'HIPS' > 'Protected Objects'

- Open the 'Protected Files' tab

- Select the item from the list and click the 'Edit' button or right-click on an item and choose 'Edit'

- Edit the file path, if you have relocated the file and click 'OK'

- Click 'OK' in the 'Advanced Settings' interface to save your settings

Delete an item from Protected Files list

- Click 'Settings' on the CIS home screen

- Click 'HIPS' > 'Protected Objects'

- Open the 'Protected Files' tab

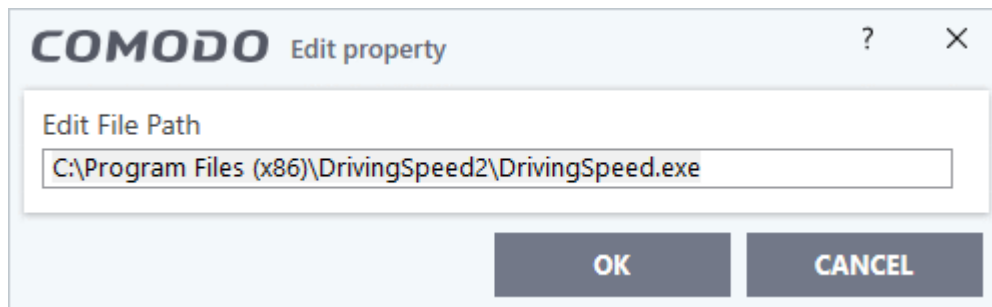- Select the item from the list and click the 'Remove' button or right-click on an item and choose 'Remove'

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

- Exceptions let you selectively allow certain applications or file groups to access a protected item.

- You create the exception by adding an 'Allow' rule for the application in the **HIPS Rules** area ('Settings' > 'HIPS' > 'HIPS Rules')

  - For example, imagine an Open Office document called 'April - 2019.odt', which contains important information. You want the 'Open Office Writer' program to modify the file as you are working on it, but you don't want other applications to access it.

  - You would first add 'April - 2019.odt' to 'Protected Files'. Once added, go to '**HIPS Rules**' and create an allow rule for 'swriter.exe'. This means Open Office Writer alone is allowed to modify 'April - 2019.odt'.

- Add 'April - 2019.odt' to protected files as shown below:
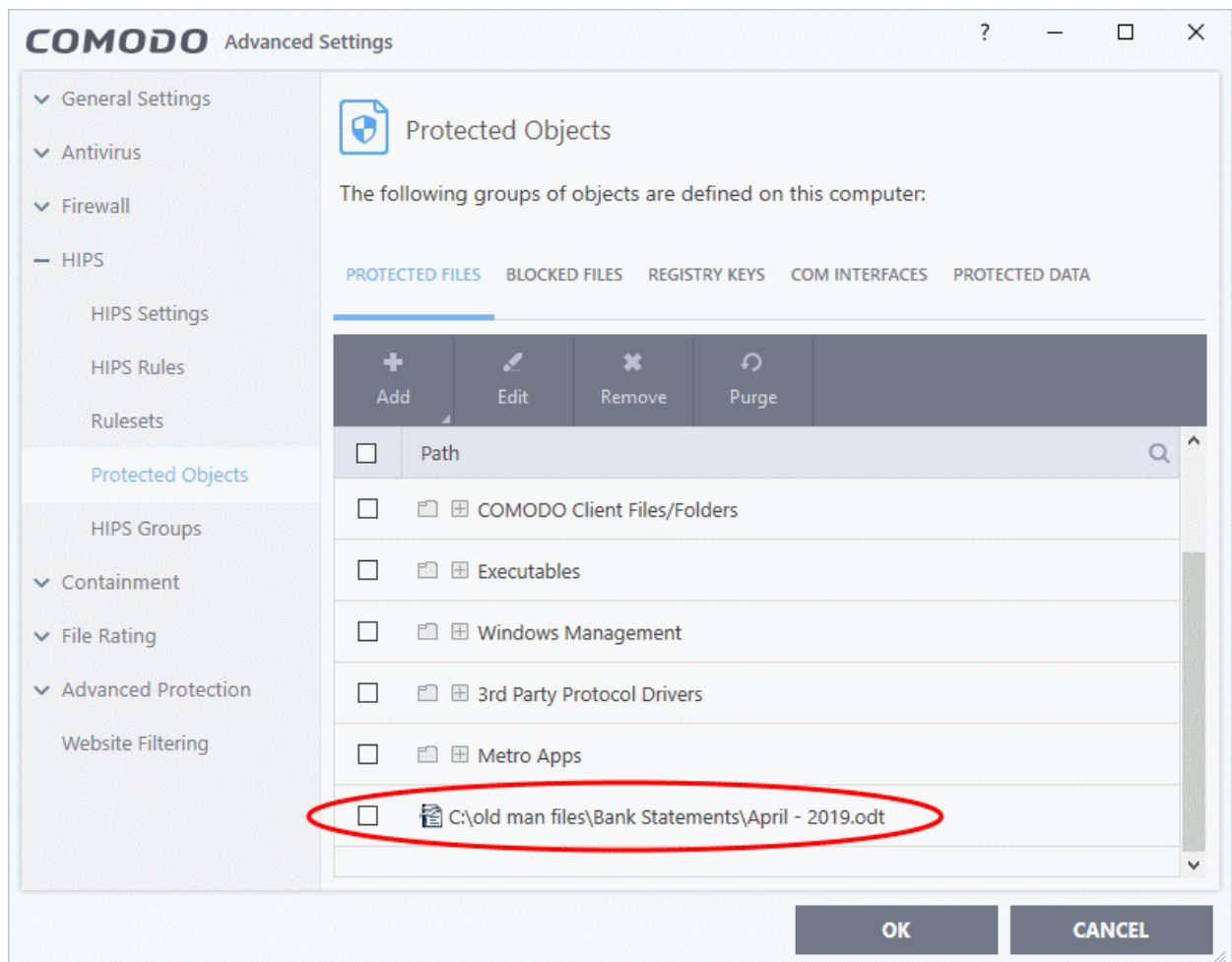
- Then go to 'HIPS Rules' interface and add it to the list of applications.
- Click the 'Edit' button after selecting the checkbox beside it.
- In the 'HIPS Rule' interface, select 'Use a Custom Ruleset'.
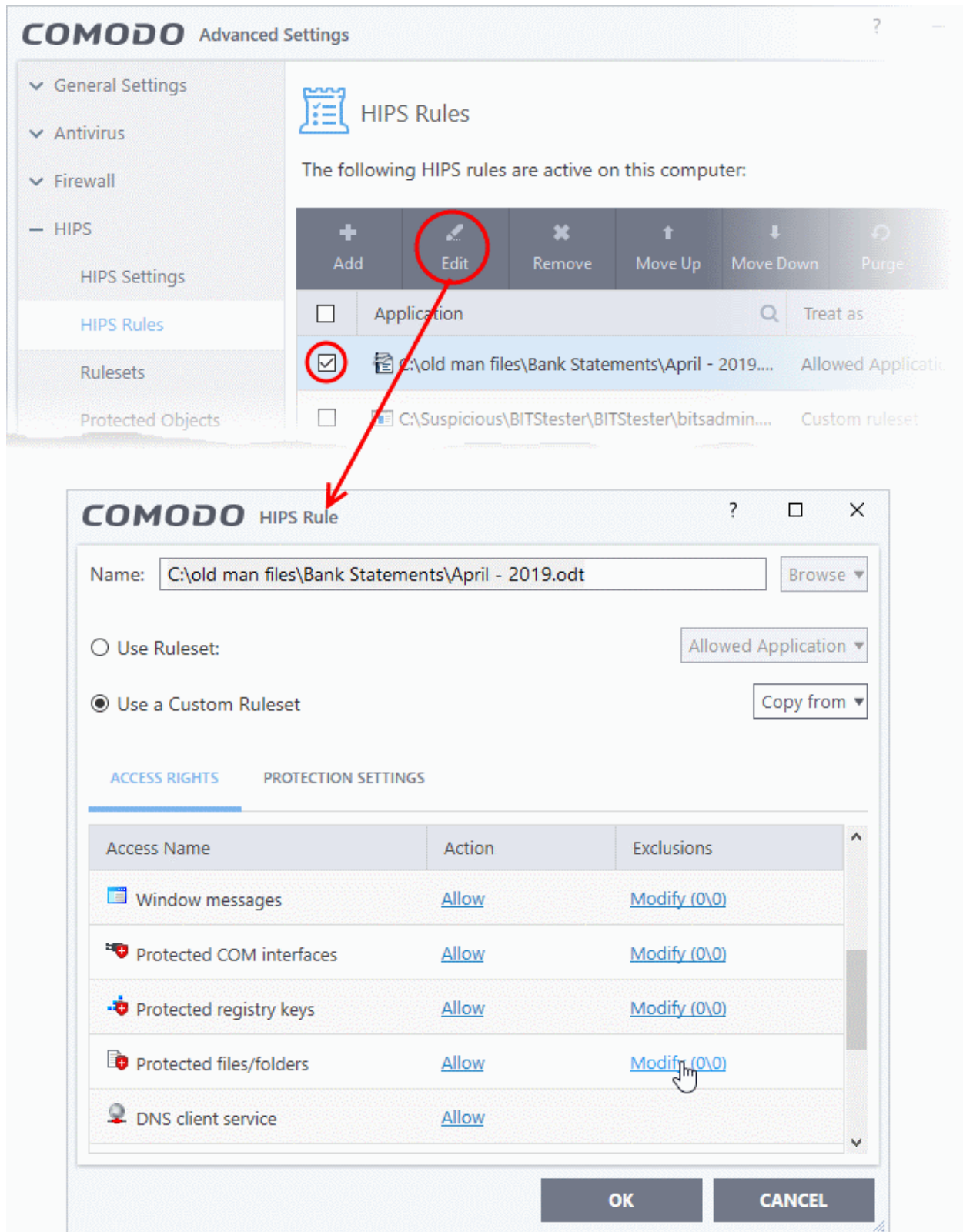
- Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'. The 'Protected Files/Folders' interface will appear.
- Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add swriter.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.
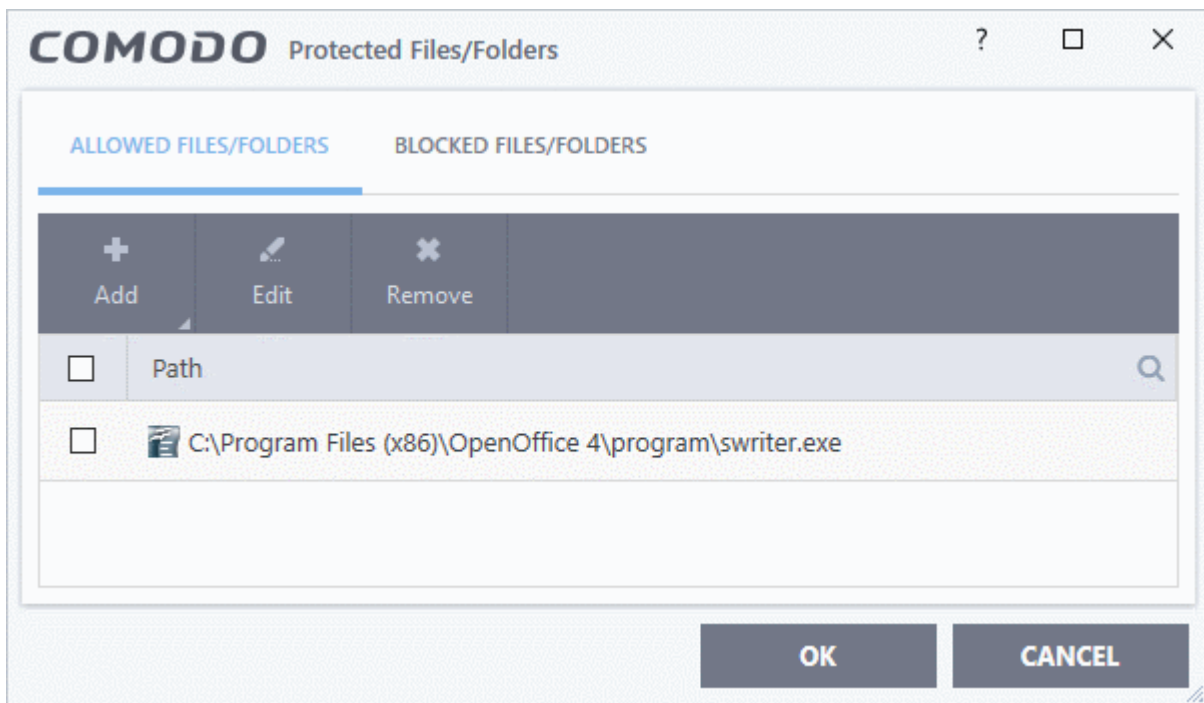
Another example of where protected files should be given selective access is the Windows system directory at 'c:\
windows\system32'. Files in this folder should be off-limits to modification by anything except certain Windows. In
this case, you would add the directory c:\windows\system32* to the 'Protected 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

Click 'Settings' > 'HIPS' > 'Protected Objects' > 'Blocked Files'

- If you block a file or folder then you completely prevent access to it from other processes or users -
  effectively cutting it 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', you cannot selectively allow access a blocked file.

Open the 'Blocked Files' area

- Click 'Settings' at the top-left of the home screen

- Click 'HIPS' > 'Protected Objects' on the left

- Click the 'Blocked Files' tab
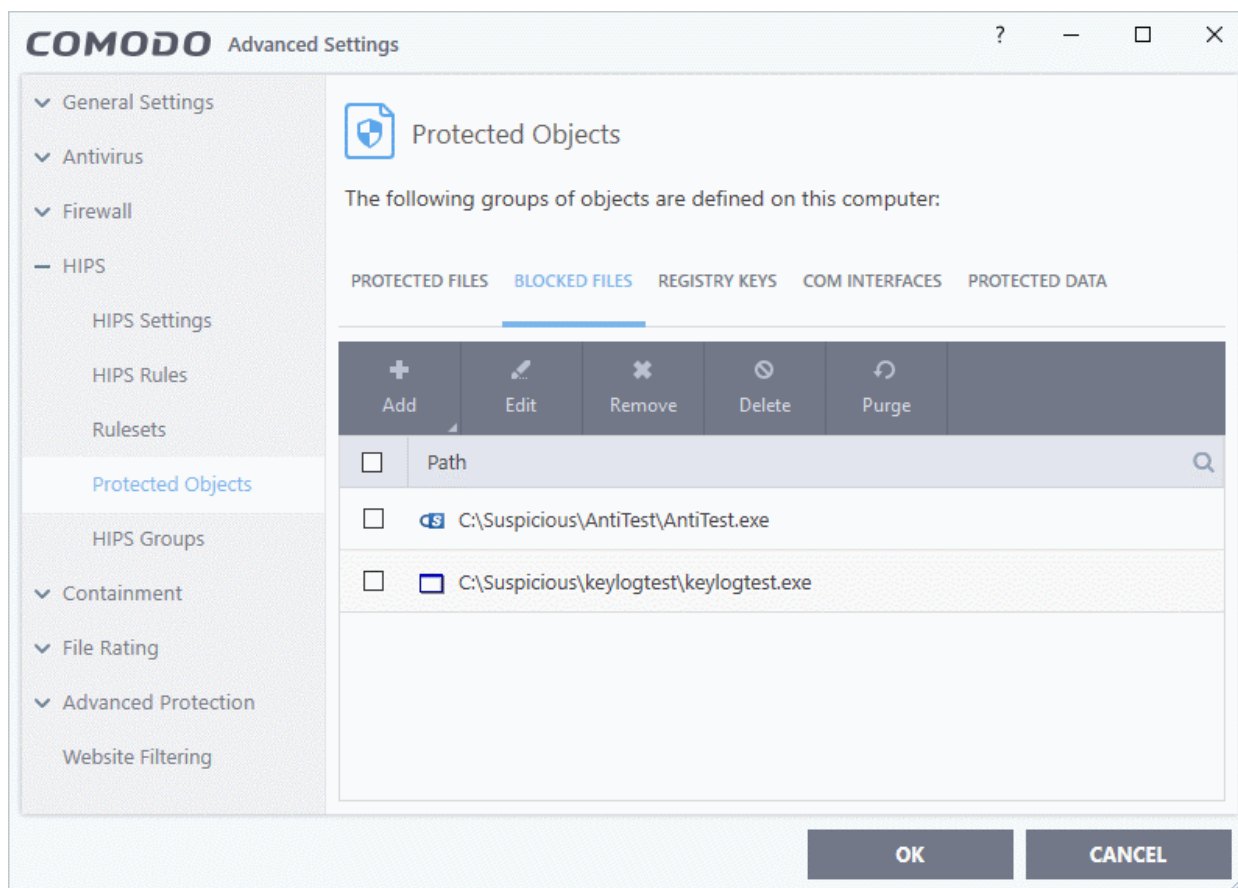
Search Option:

- Click the search icon at upper-right and enter the name of a file in full or part.

Controls:

The buttons at the top provide the following options:

- **Add** - Block a new file, file-group, folder or running process
- **Edit** - Modify the path/location of the target item
- **Remove** - Release a file from the blocked files list.
- **Delete** - Removes the highlighted file from your computer
- **Purge** - Runs a check to verify that all files in the list are actually installed at the path specified. If not, the item is removed from the list.

Right-click Options:

- Right-click on an item to add, edit, remove/delete, and purge files:
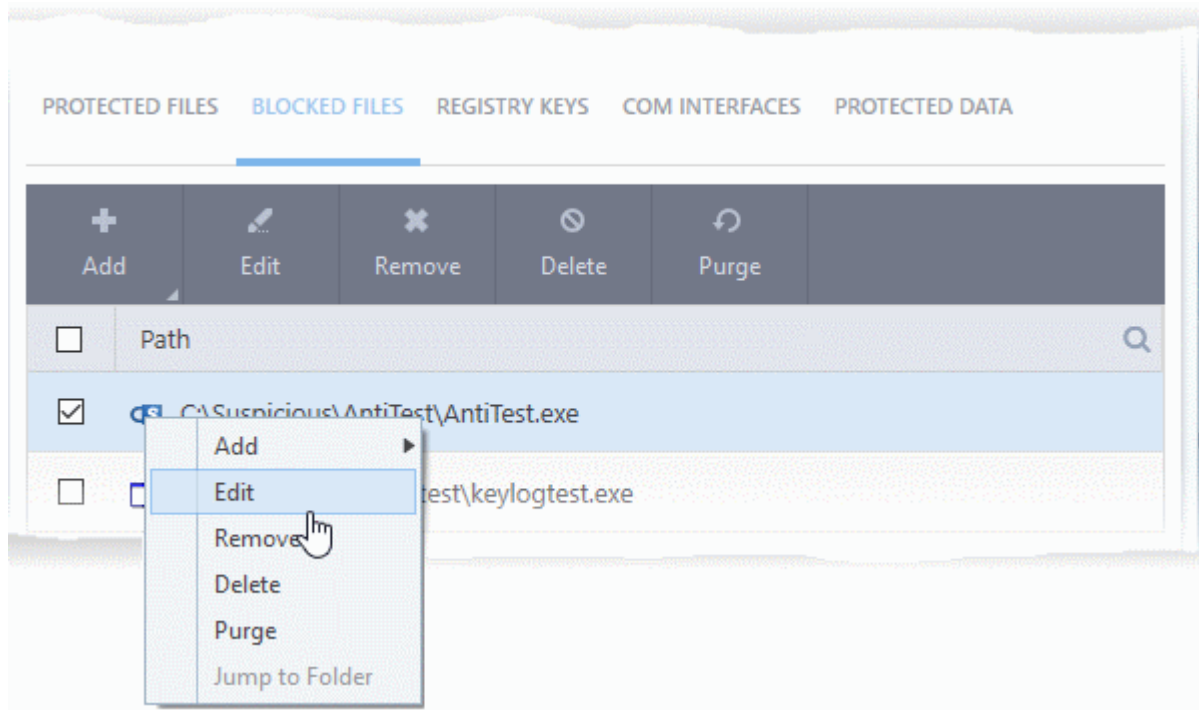
The options available are same as described **above**.

See the following sections if you need more help:

- **Add an application to blocked files**
- **Edit the path of a blocked item**
- **Release a blocked file**
- **Delete a blocked file from your computer**

Manually add an individual file or application to blocked file list

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'Blocked Files' tab
- Click the 'Add' button
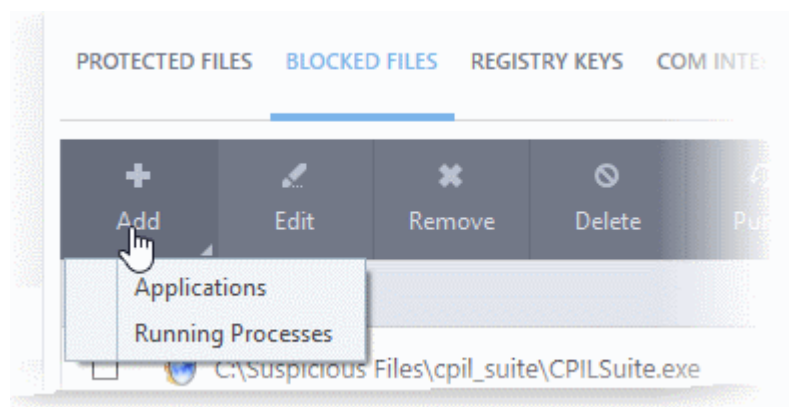
You can add applications to be blocked by following methods:

- **Select a File**
- **Specify a currently running process**

Add a File

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'Blocked Files' tab
- Click 'Add' > 'Applications'
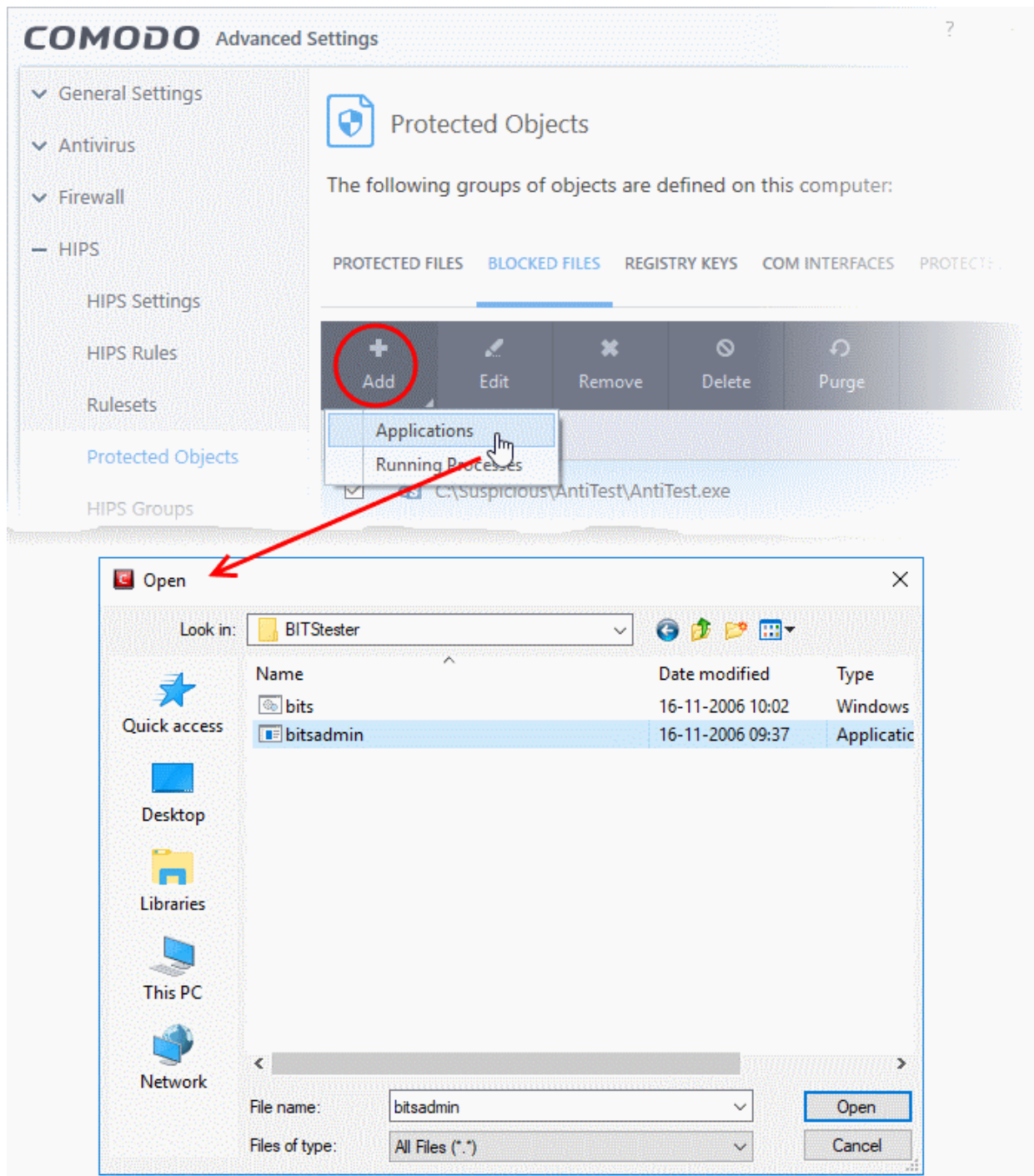
- Navigate to the file you want to add to 'Blocked Files' and click 'Open'.

The file will be added to 'Blocked Files' list:
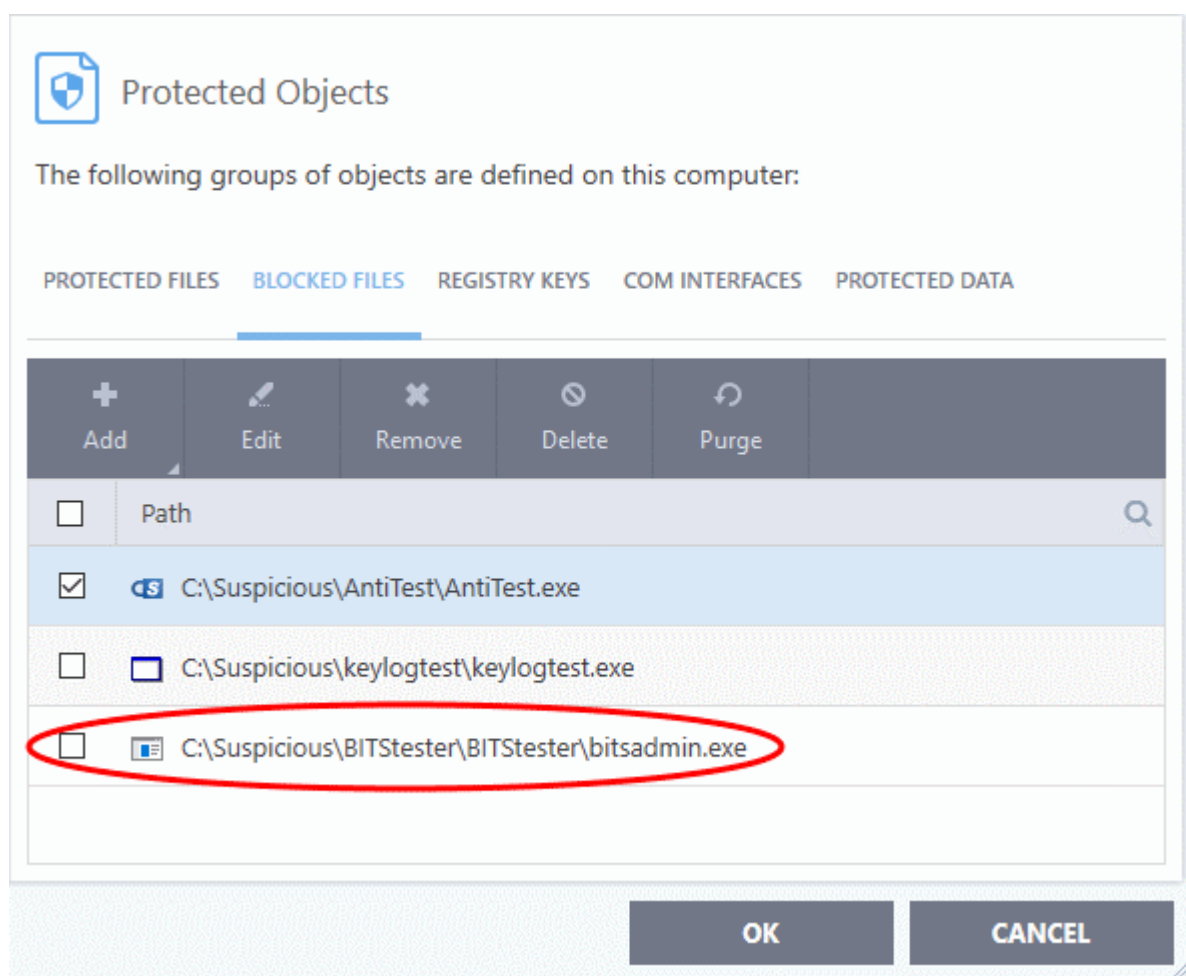
- Repeat the process to add more files.
- Click 'OK' to save your changes.

Add an application from a running process

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'Blocked Files' tab
- Click 'Add' > 'Running Processes'
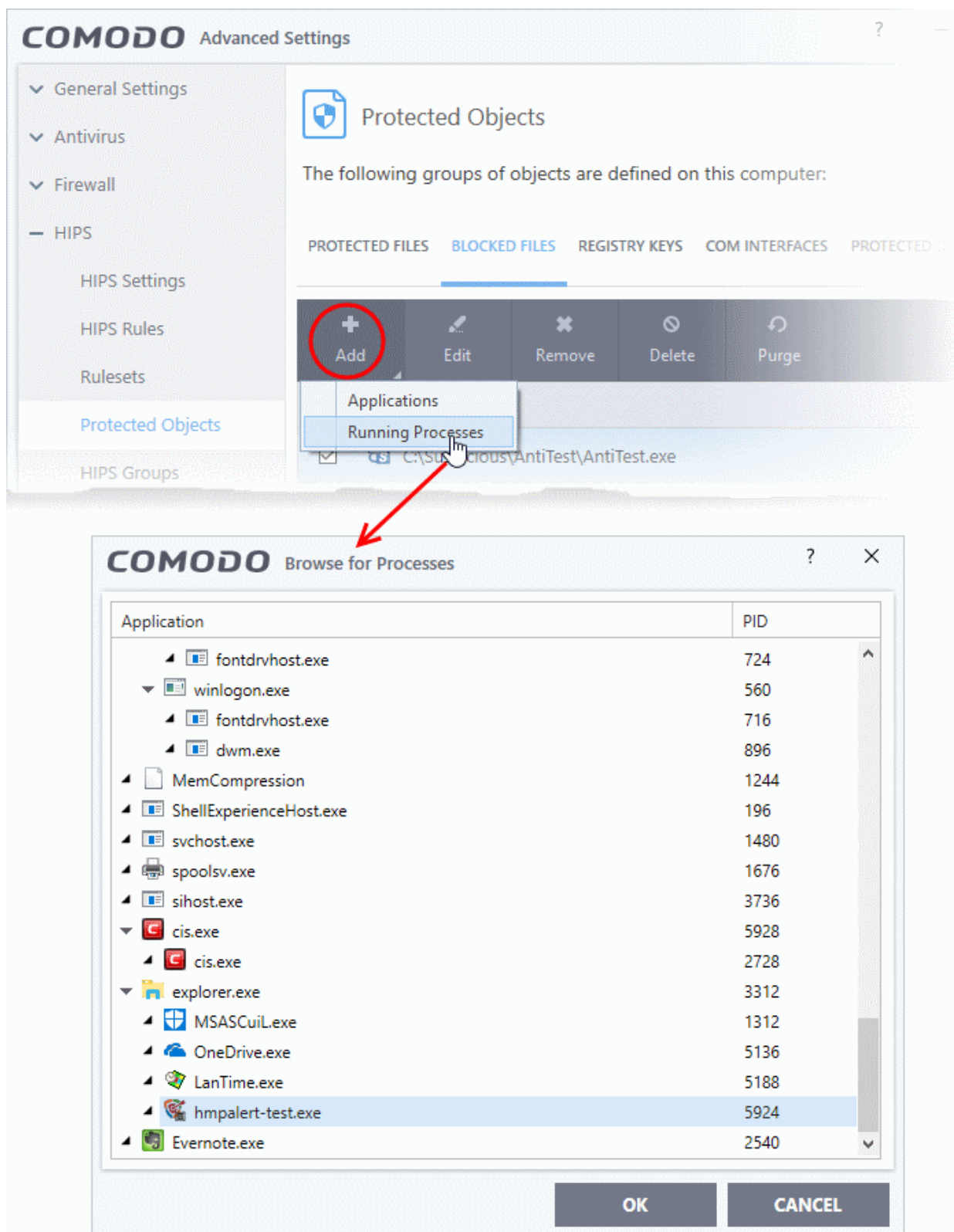
This shows a list of processes currently running on in your computer.

- Select the process you want to block and click 'OK'. The parent application of the process is added to blocked files.
- Repeat the process to add more applications
- Click 'OK' to save your changes

Change the file path of an item in the blocked files list

- Click 'Settings' on the CIS home screen

- Click 'HIPS' > 'Protected Objects'
- Click the 'Blocked Files' tab
- Select an item and click the 'Edit' button or right-click on an item and choose 'Edit'
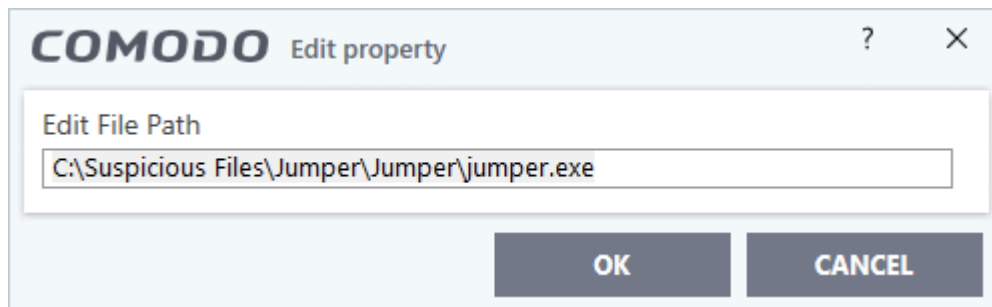
- Edit the file path, if you have relocated the file and click 'OK'

Release an item from blocked files list

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'Blocked Files' tab
- Select the item from the list and click the 'Remove' button or right-click on an item and choose 'Remove'

The selected item will be removed from the 'Blocked Files' list. CIS will not stop the application from opening in the future.

Permanently delete a blocked file from your system

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'Blocked Files' tab
- 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

Click 'Settings' > 'HIPS' > 'Protected Objects' > 'Registry Keys'

- The registry keys area lets you prevent modifications to critical Windows registry keys.
- Irreversible damage can be caused to your system if important registry keys are corrupted or modified.

Open the registry keys section

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'Registry Keys' tab
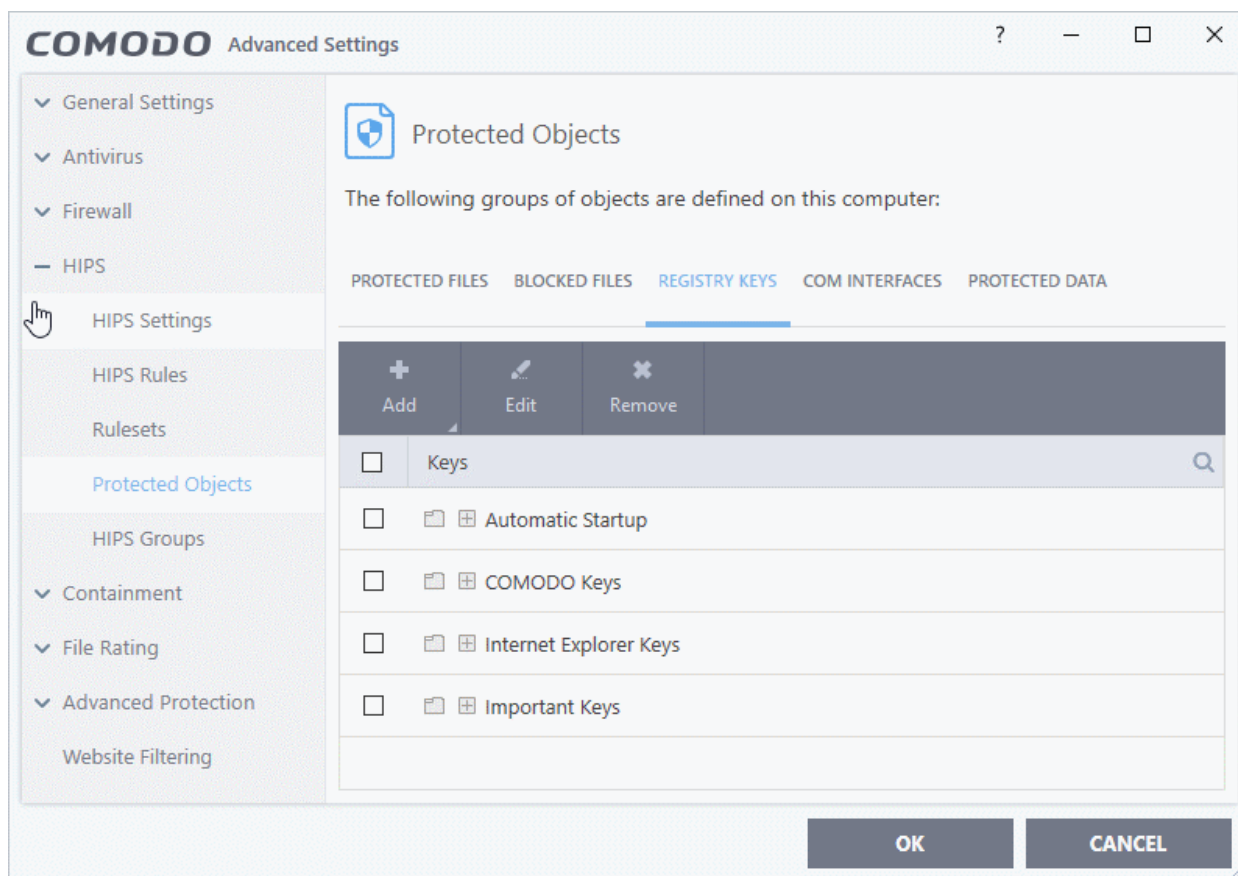
Controls:

The buttons at the top provide the following options:

- **Add** - Protect new individual keys or registry groups.
- **Edit** - Modify the path/location of the target item
- **Remove** - Delete a key or key group from the protected list.

**Right-click Options**:

- Right-click on an item to edit the key path, add / remove keys, and more.
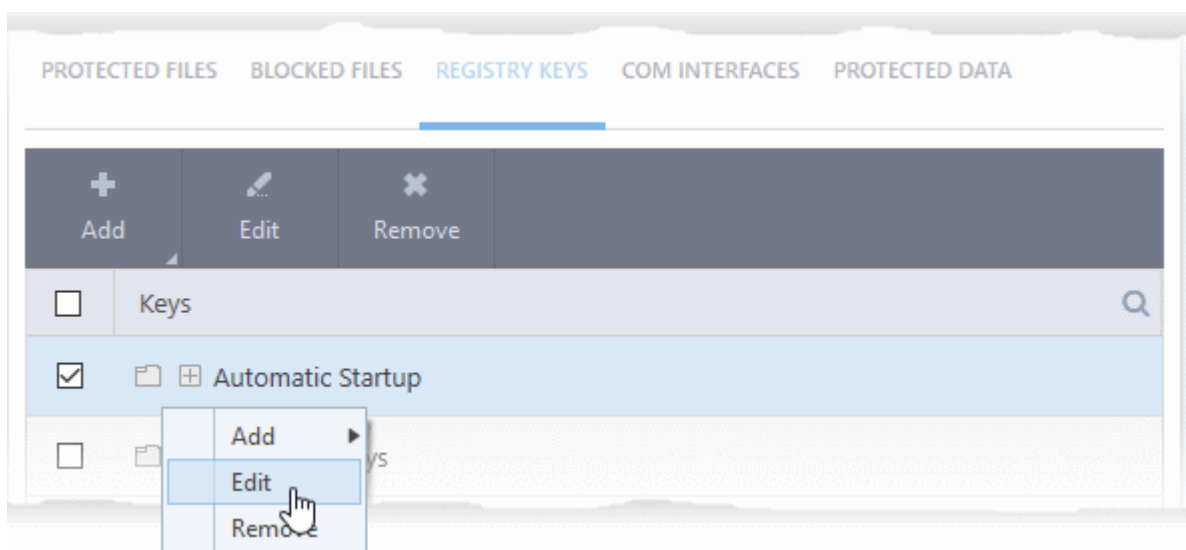
The options available are as described **above**.

See the following sections if you need more help:

- **Add registry groups or Individual registry keys to protected registry keys list**
- **Edit the path of a key**
- **Remove registry groups or keys from the protected registry keys list**

Manually add an individual registry key or registry group

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects' > 'Registry Keys'
- Click the 'Add' button
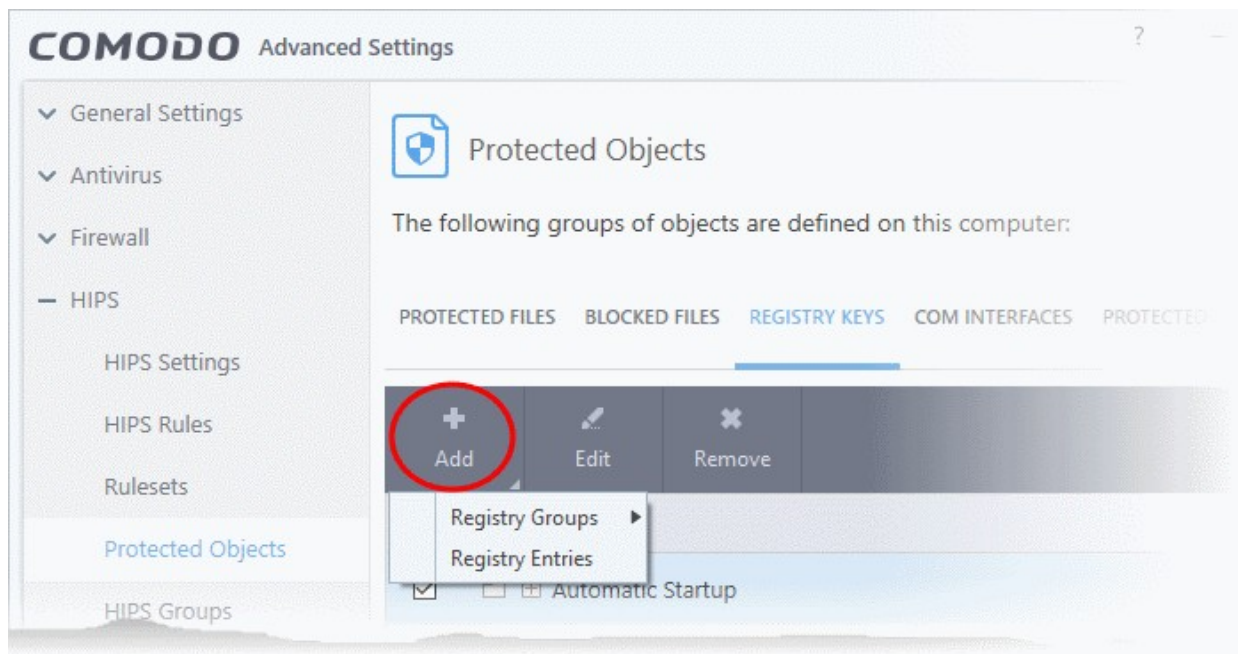
- **Registry Groups** - Lets you batch select and import groups of important registry keys. Comodo Internet Security provides the following, pre-defined groups - 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.

  You can also create custom registry groups containing keys you wish to protect.

  See **Registry Groups** in the **HIPS Groups** section for general help on registry groups.
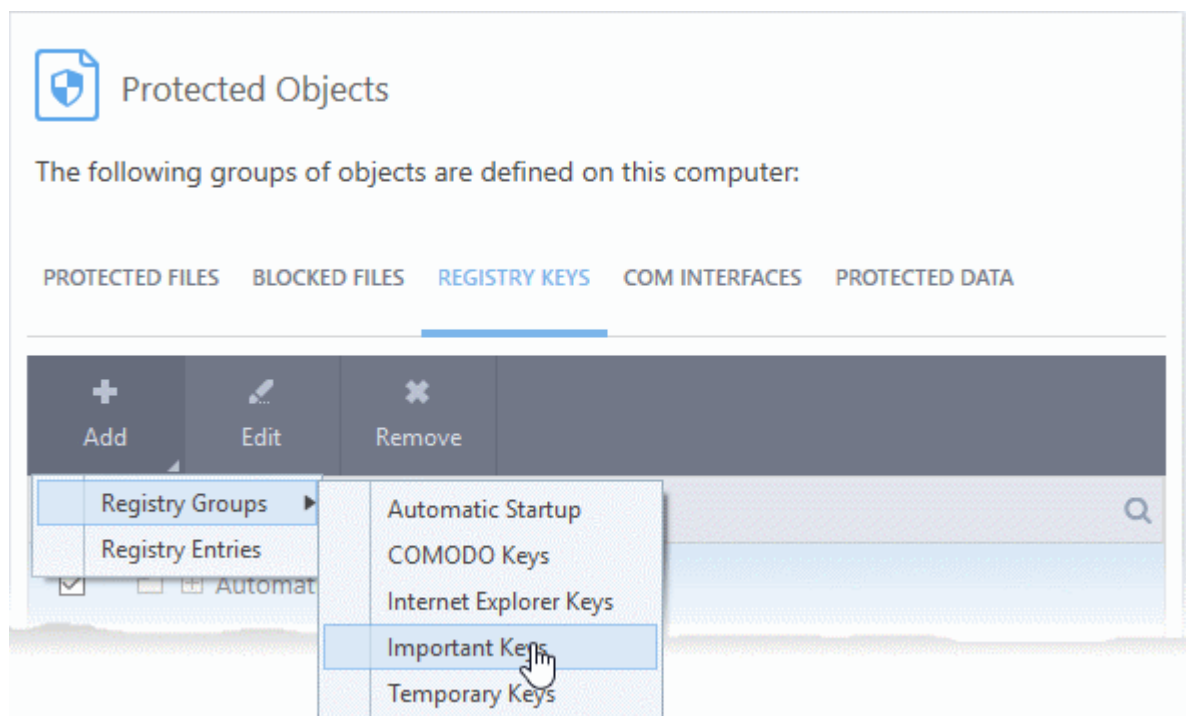
- Select the predefined group from the list and click 'OK'
- **Registry Entries** - Add individual keys to the protected list
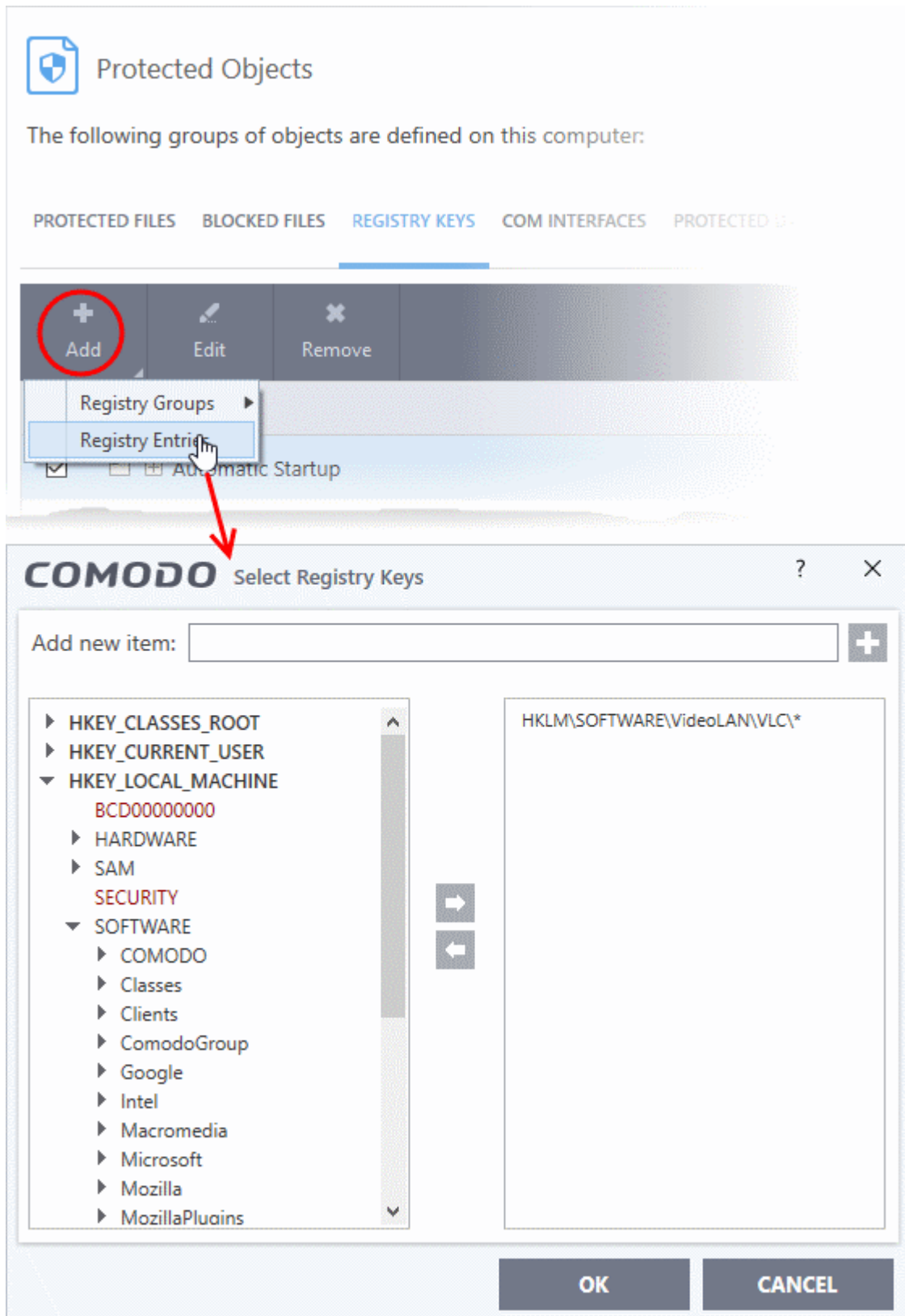
- Select a key on the left then click the right arrow button to add it to protected keys.
- To add an item manually, enter its name in the 'Add new item' field and press the '+' button.

Edit an item in the protected registry keys list

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects' > 'Registry Keys'
- Select a key in the list and click the 'Edit' button or right click on a key and choose 'Edit'.
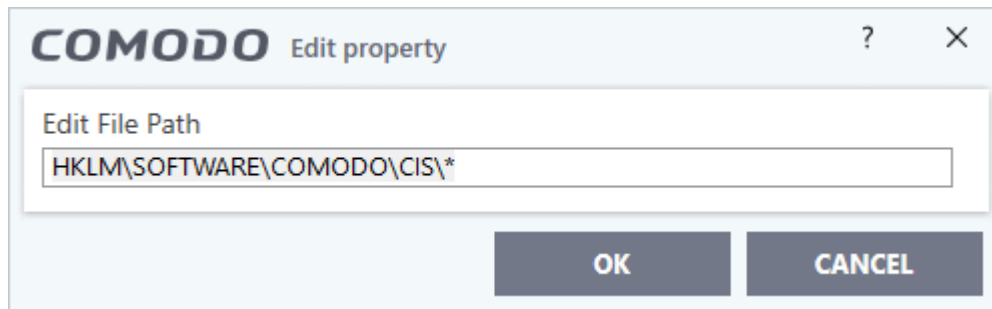
- Edit the key path, if you have relocated the key and click 'OK'.

> **Note**: The 'Registry Groups' cannot be edited from this interface. You can edit only from **Registry Groups** in **HIPS Groups** section.

Delete an item from the protected registry keys list

- Click 'Settings' on the CIS home screen

- Click 'HIPS' > 'Protected Objects' > 'Registry Keys'

- Select an item from the list and click the 'Remove' button or right click on an item and choose 'Remove'

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

Click 'Settings' > 'HIPS' > 'Protected Objects' > 'COM Interfaces'

- The Component Object Model (COM) is Microsoft's object-oriented programming model. This model defines how objects interact within a single application, or between applications.

- COM is used as the basis of Active X and OLE - two items which are often attacked by hackers and malware.

- Comodo Internet Security automatically protects COM interfaces against modification and manipulation by malicious processes.

- CIS ships with a set of COM interface groups. These groups are category-based collections of important COM components. Click 'Settings' > 'HIPS Groups' > 'COM Groups' to view these groups.

- You can also create custom COM Interface groups as required. See **COM Groups** for more details.

Open the protected COM interfaces section

- Click 'Settings' on the CIS home screen

- Click 'HIPS' > 'Protected Objects'

- Click the 'COM Interfaces' tab
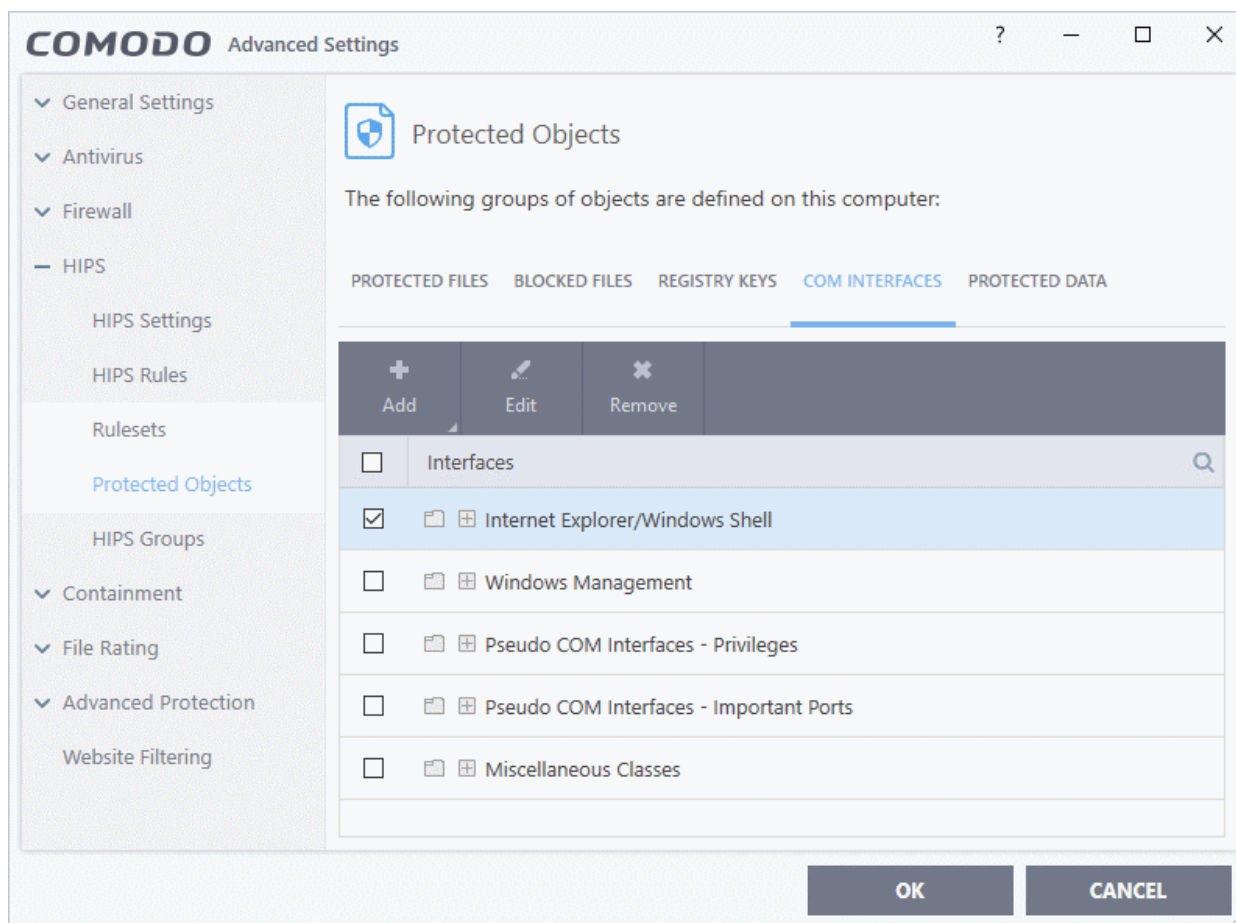
Controls:

The buttons at the top provide the following options:

- **Add** - Protect a new COM group or individual COM component.
- **Edit** - Change the COM class file path of a COM interface.
- **Remove** - Delete a COM group or COM component

Right-click Options:

- Right-click on an item to edit the name of the COM interface, add / remove COM interfaces, and more.
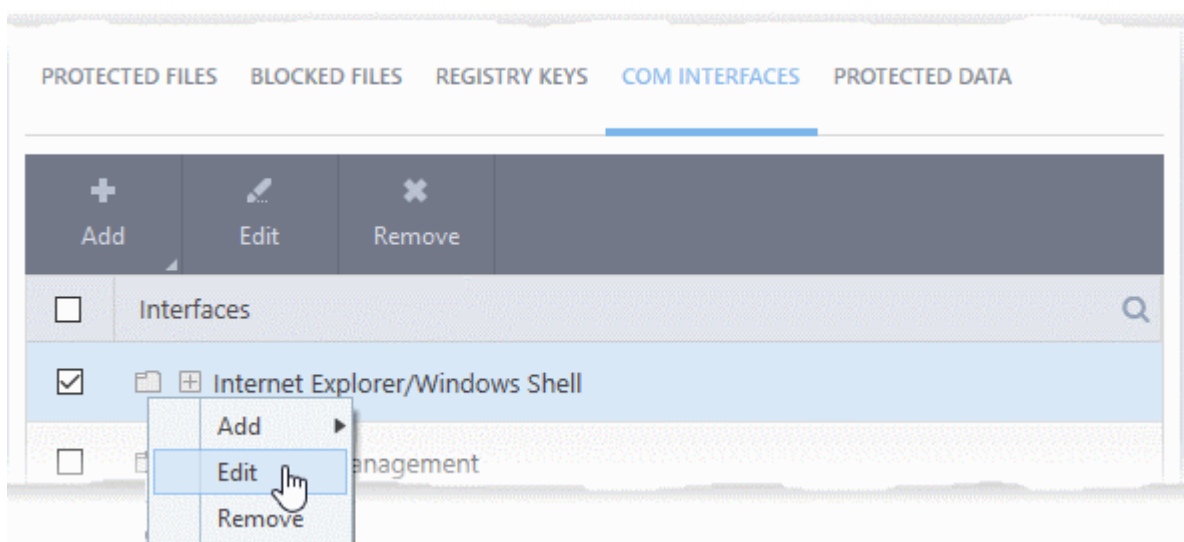
The options available are same as described **above**.

See the following sections if you need more help:

- **Add a COM group or individual COM interface to protected COM interfaces list**
- **Edit the COM Class file path of a COM interface**
- **Remove COM groups or individual COM interfaces from the protected COM interfaces list**

Manually add a COM group or individual COM component

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Click the 'COM Interfaces' tab
- Click the 'Add' button
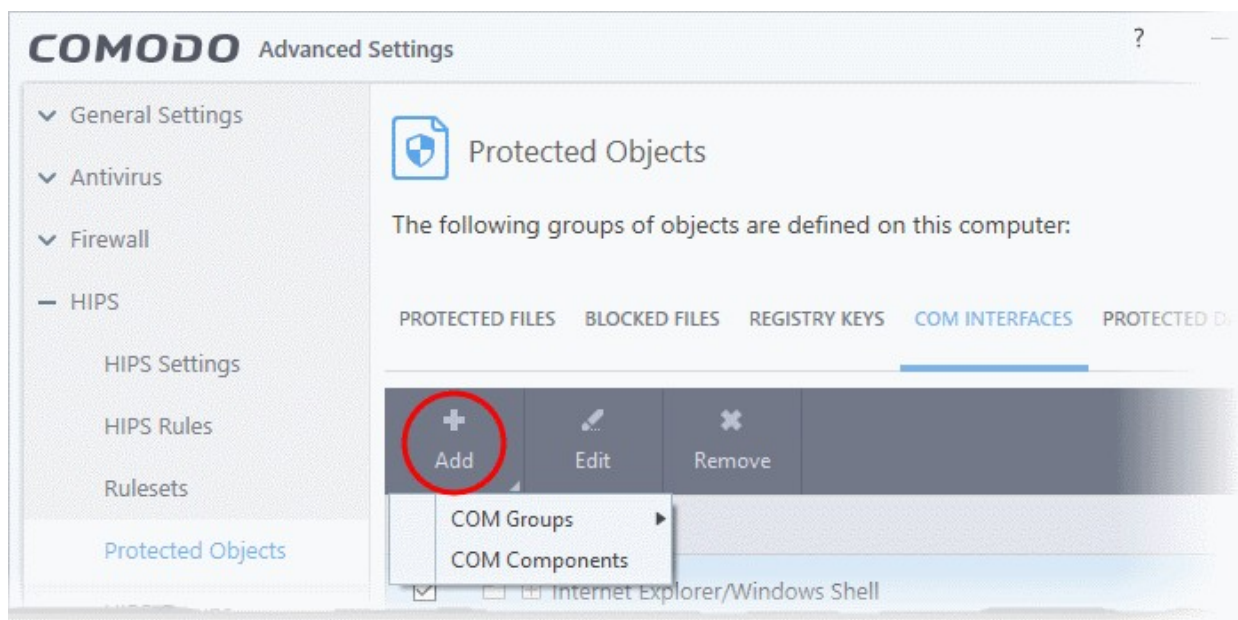
- **COM Groups** - Add predefined groups of important COM interface components. Comodo Internet Security ships with following, pre-defined groups - 'Internet Explorer/Windows Shell', 'Windows Management', 'Miscellaneous Classes', 'Pseudo COM Interfaces - Privileges' and Pseudo COM Interfaces - Important Ports'

  You can also create custom COM groups containing COM interfaces you wish to protect.

  See **COM Groups** for general help to manage COM groups.
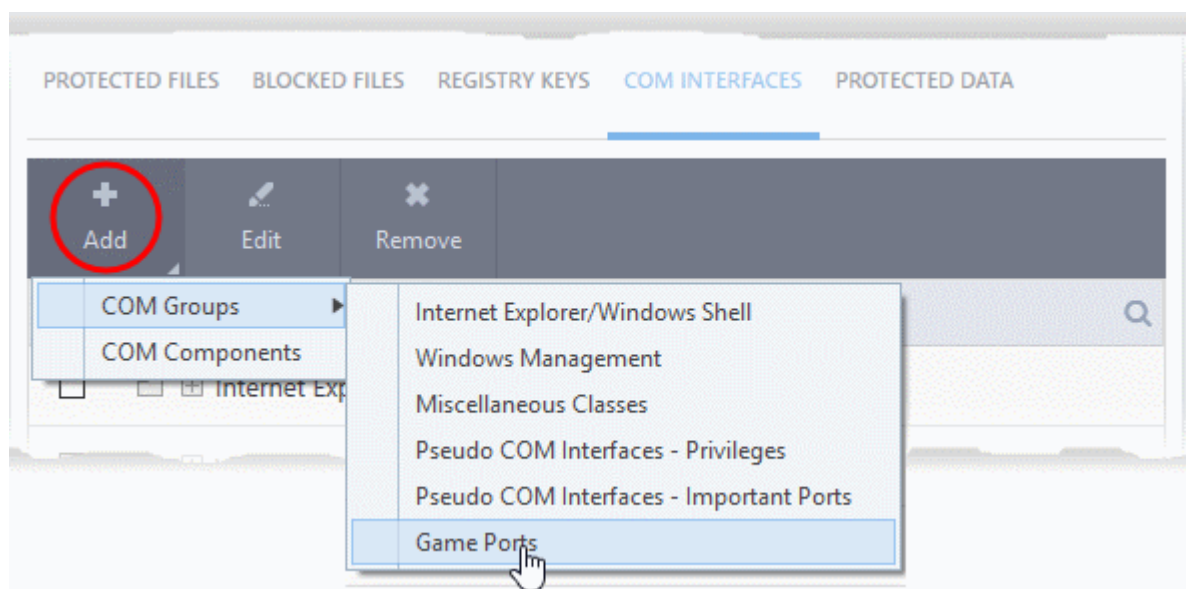
- Select the predefined group from the list and click 'OK'
  - **COM Components -** Lets you add individual COM components.
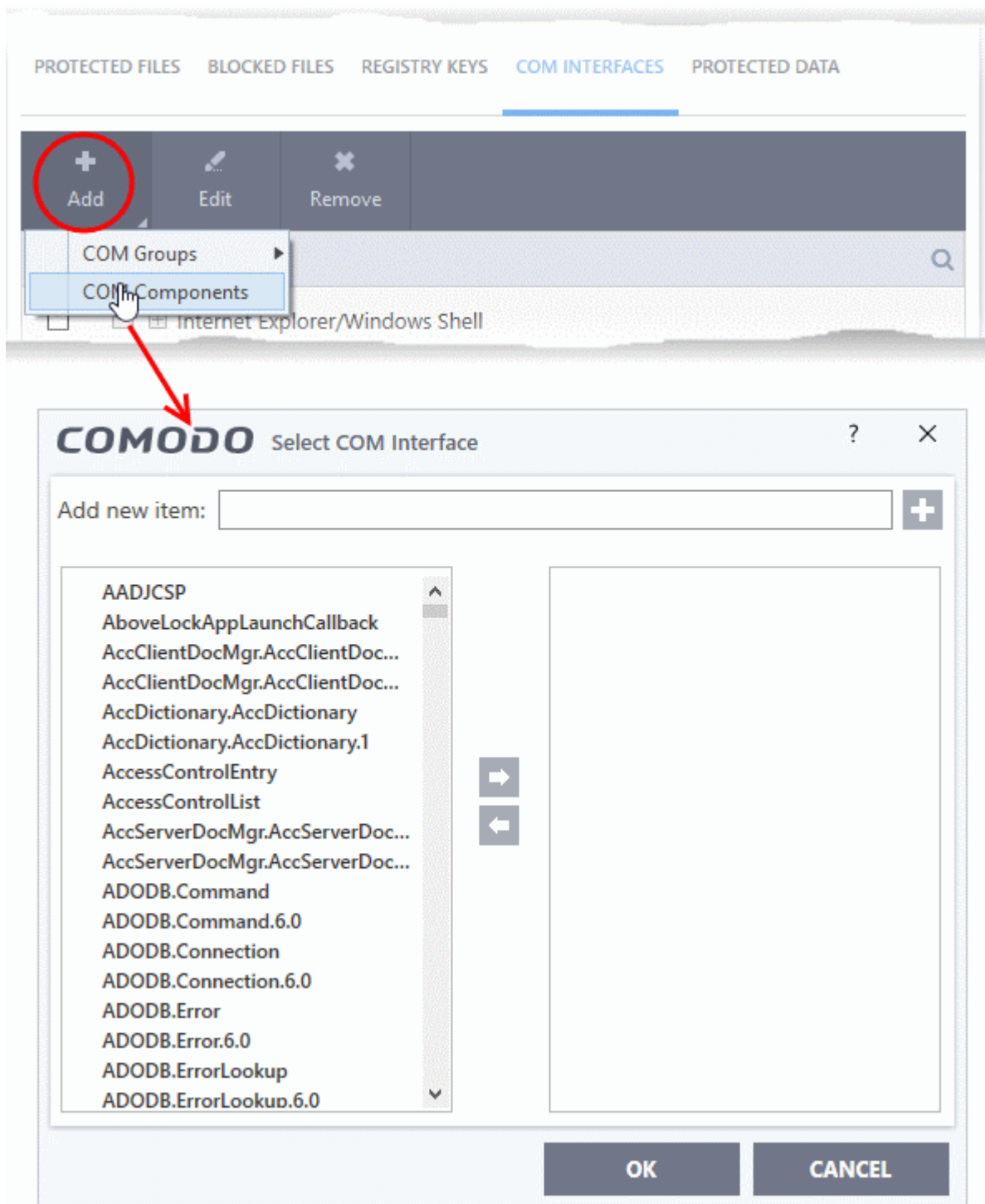
- Select an item from the left pane and move it to the right pan by clicking the right arrow button.
  - To manually add an item, enter its name in the 'Add new item' field and press the '+' button.
  - Repeat the process to add more COM interfaces to the protected COM interfaces list.
- Click 'OK' to save your changes

Edit an item in the COM interfaces protection list

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects' > 'COM Interfaces'
- Select the COM component from the list and click the 'Edit' button or right click on a COM interface and

---

choose 'Edit':
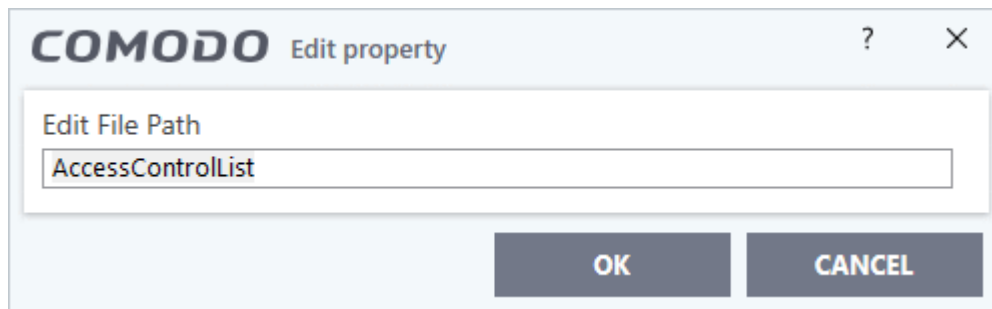
- Edit the COM Class file path and click 'OK'

> **Note**: The COM Groups cannot be edited from this interface. You can edit only from **COM Groups** in **HIPS Groups** section.

Remove an item from protected COM interfaces list

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects' > 'COM Interfaces'
- Select an item from the list and click the 'Remove' button or right click on an item and choose 'Remove'

The selected item will be deleted from the 'COM Interfaces' protection list. CIS will not generate alerts if the COM component/group is modified by other processes.

6.4.4.5. Protected Data Files and Folders

Click 'Settings' > 'HIPS' > 'Protected Objects' > 'Protected Data'

- Items in 'Protected Data' cannot be seen, accessed or modified by applications running in the container.
- This fortifies files containing sensitive data from unrecognized and potentially malicious programs.

> **Protected Files and Protected Data**
>
> - Items in '**Protected Files**' can be read by any program, but not modified by them. This contrasts to items in 'Protected Data', which are totally hidden to contained programs.
>   - If you want a file/folder to be read by other programs, but protected from modification, then add it to 'Protected Files' list.
>   - If you want to totally conceal an item from contained programs, but allow read/write access to trusted programs, then add it to 'Protected Data'.
>   - You can add the same item to both areas. This means trusted programs have read-only access to the file, and contained programs have no access rights.

Add and manage protected data

- Click 'Settings' on the CIS home screen.
- Click 'HIPS' > 'Protected Objects'
- Select the 'Protected Data' tab
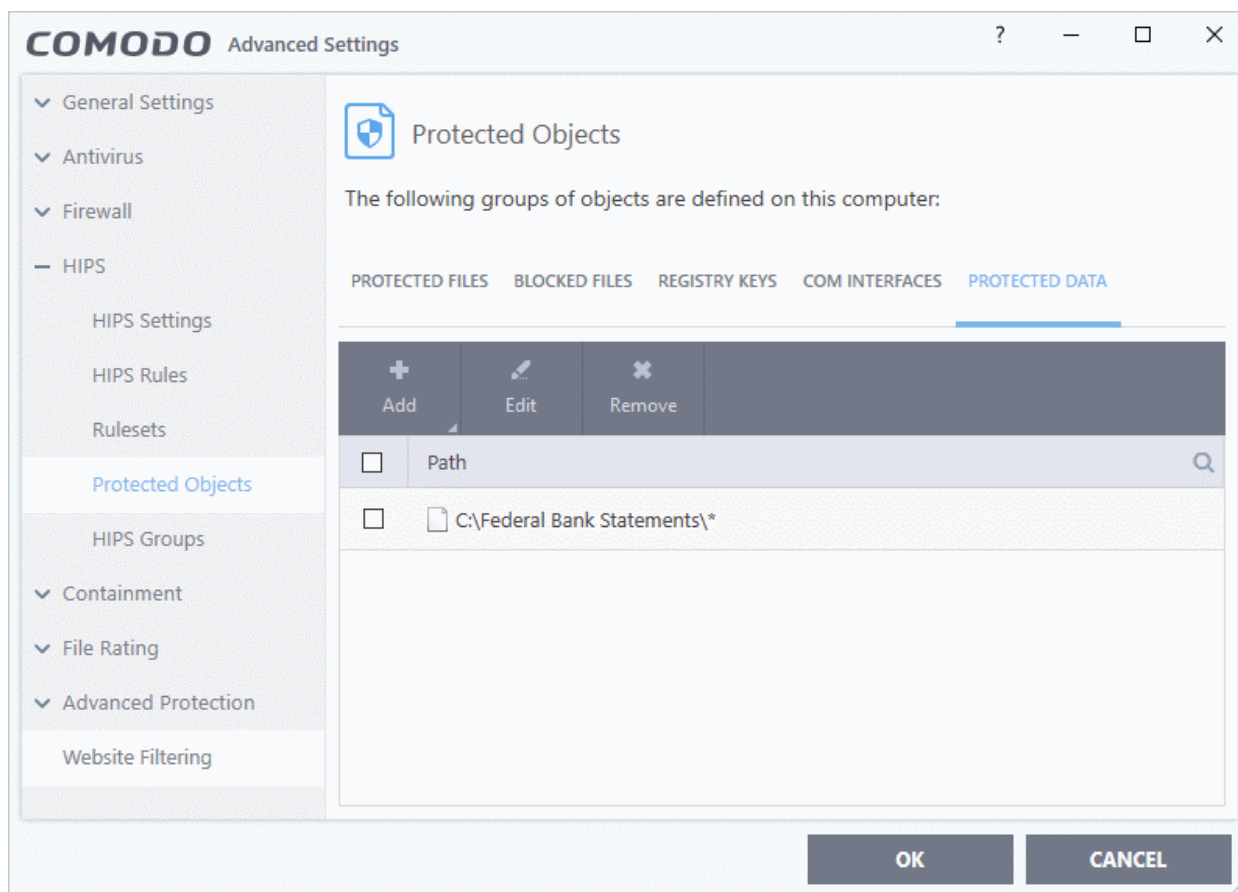
The interface allows you to:

- **Add files, folders or file groups to protected data list**
- **Modify the path of the protected items if they are relocated**
- **Remove items from protection**

Search Option:

- Click the search icon at upper-right and enter the name of a file or folder in full or part.

Controls:

The buttons at the top provide the following options:

- **Add** - Add files, folders or file groups to protected data.
- **Edit** - Change the file path of protected items
- **Remove** - Delete items that you no longer want to hide from contained programs

Add a file, folder or file group to be protected

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Data' tab
- Click the 'Add' button:
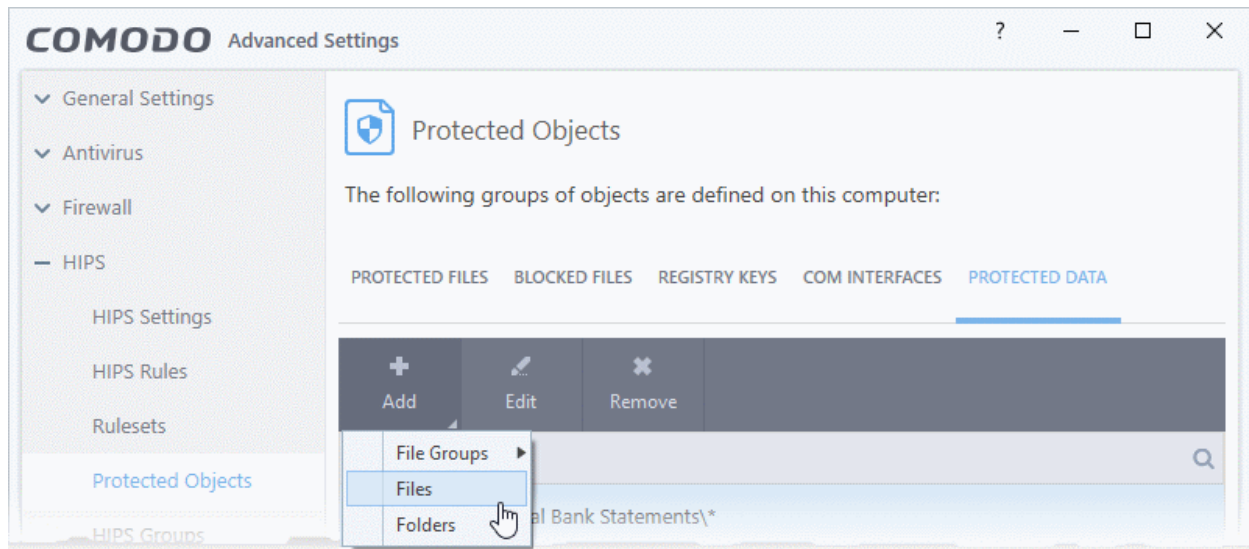
You can add:

- **File Groups**
- **Drive partitions/Folders**

  OR

- **Individual files**

Add a File Group

- Choose 'File Groups' to include a pre-set category of files or folders. This is a convenient way to protect an entire category of important files and folder.
- For example, selecting 'Executables' will protect all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, cmd.exe, .bat, and .cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications' and 'Start Up Folders'.
- CIS ships with a set of predefined file groups which can be viewed in 'Advanced Settings' > 'File Rating' > 'File Groups'.
- You can also create your own file groups. All files in that group will be covered, including files added to the group after adding it to 'Protected Data'. See **File Groups** for more details.

Add a file group to be protected

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Data' tab
- Click 'Add' > 'File Groups'
- Select the target file group from the list:
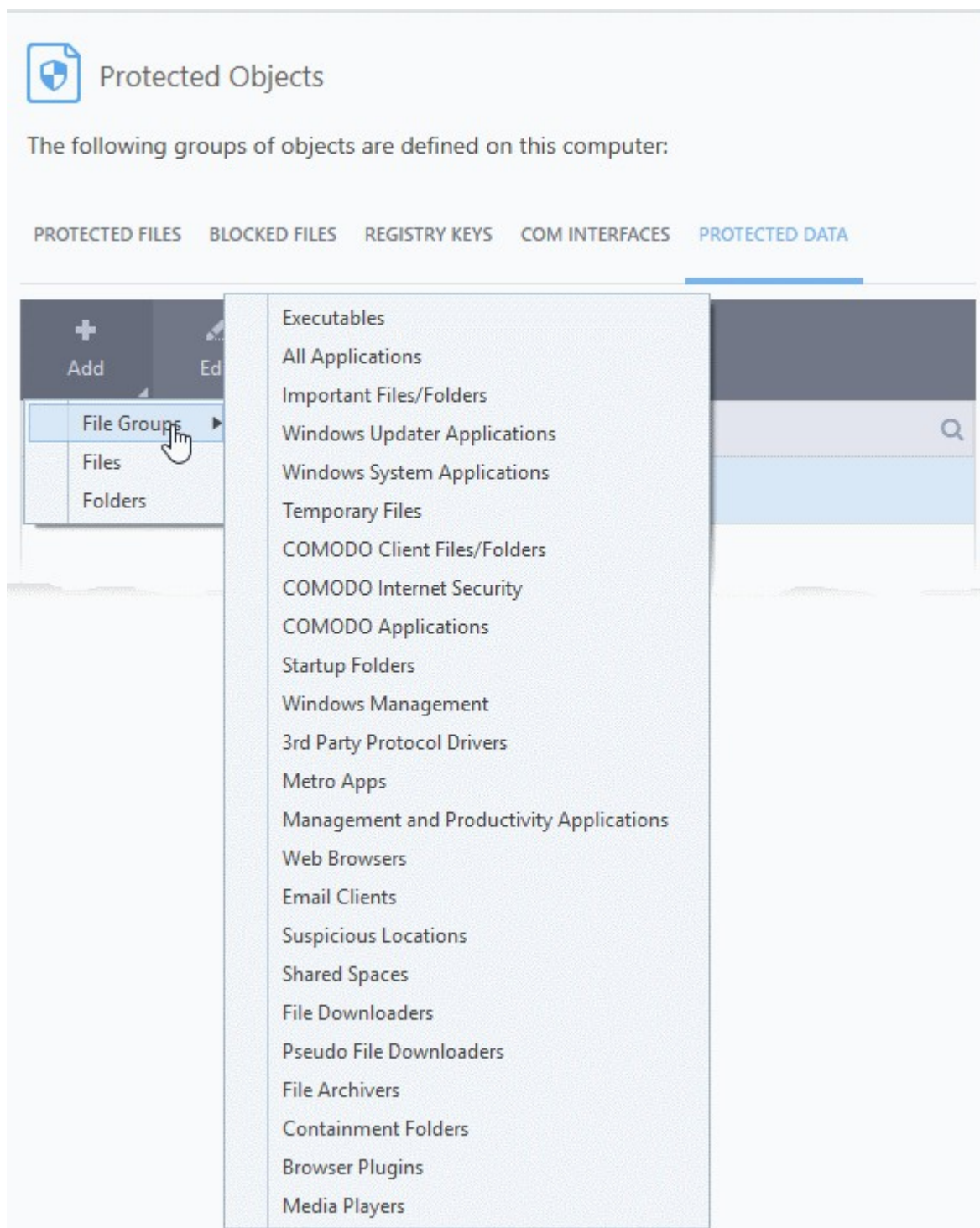
- Repeat the process to add more file groups.
- Click 'OK' in the 'Advanced Settings' interface to save your settings

Add drive partitions / folders

- You an add disk drive partitions and data folders containing sensitive files to protected data
- All sub-folders and files included in the folder/drive will be covered by the protection. This includes items added after the folder was added to 'Protected Data'.

Add a drive / folder to be protected

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Data' tab

- Click 'Add' > 'Folders'

- Navigate to the drive partition or folder you want to add to protected data list and click 'OK'.
- Repeat the process to add more folders.
- Click 'OK' in the 'Advanced Settings' interface to save your settings

Add individual files to be protected

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Data' tab
- Click 'Add' > 'Files'
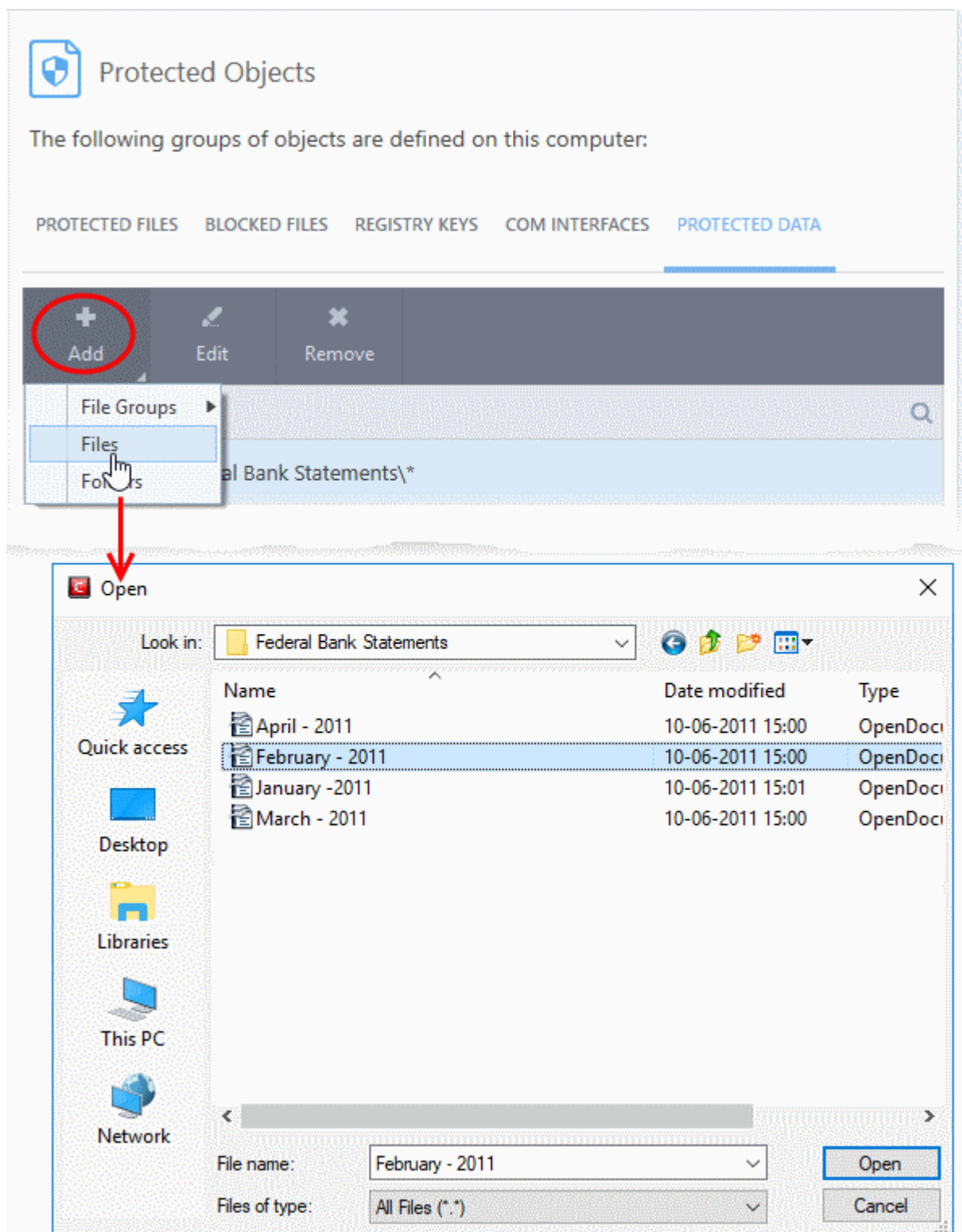
- Navigate to and select the files you want to add to protected data and click 'Open'.
- Repeat the process to add more files.
- Click 'OK' in the 'Advanced Settings' interface to save your settings

Edit path of protected items
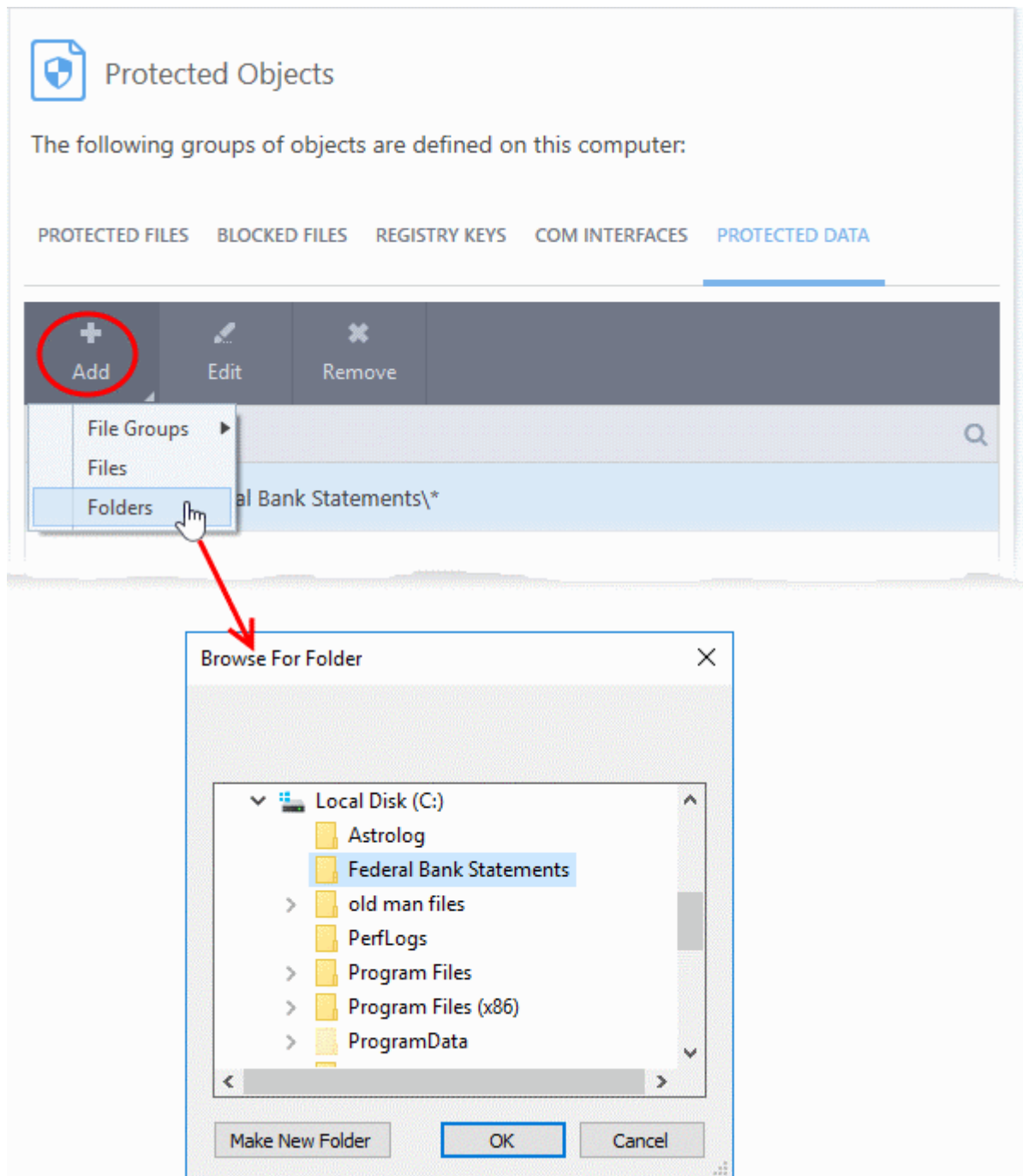
- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Data' tab
- Select the item to be edited and click the 'Edit' button
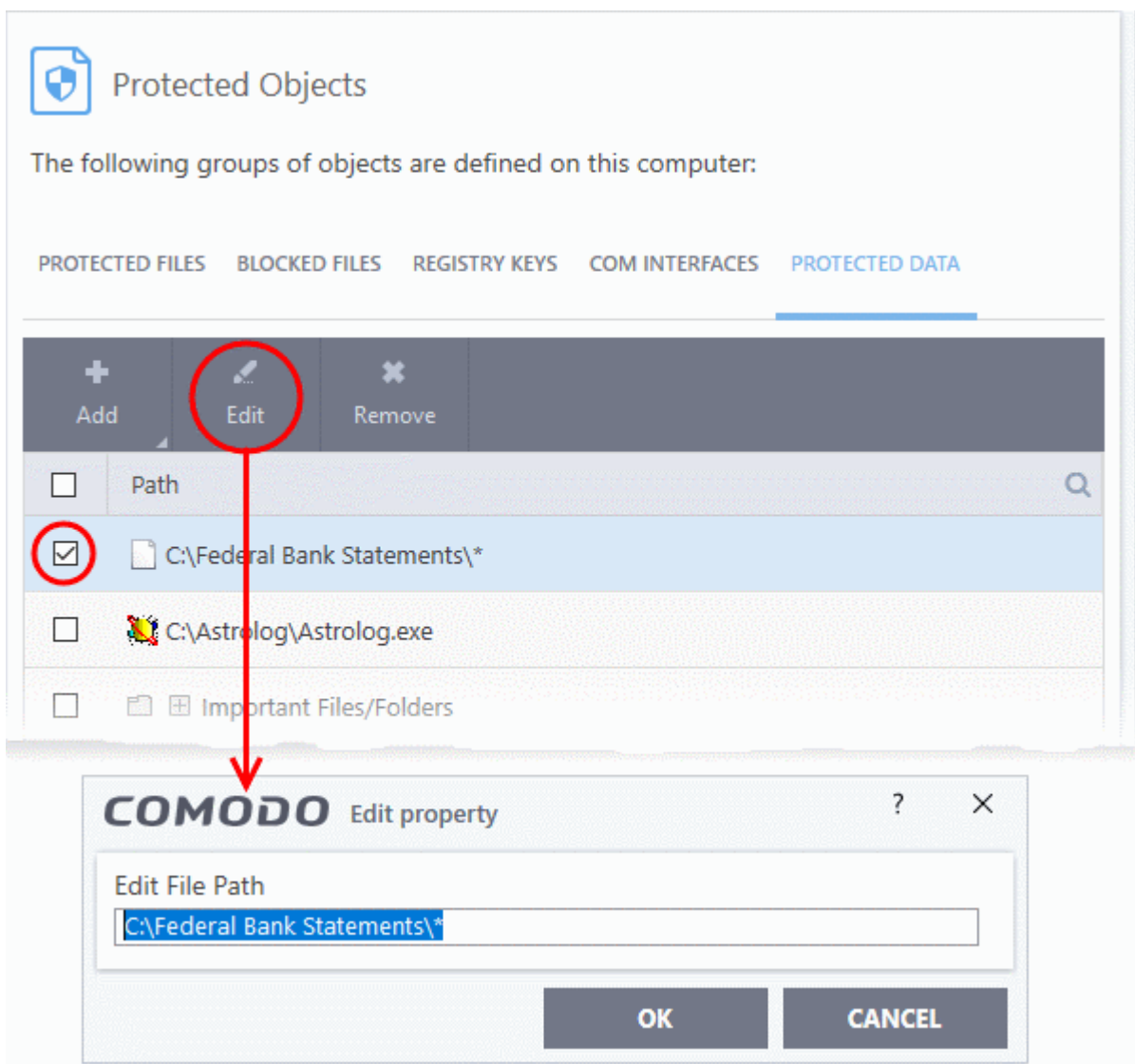
- Modify the file-path as required and click 'OK'.
- Click 'OK' in the 'Advanced Settings' interface to save your settings

Remove protection for files and folders

You can remove items you no longer want to protect:

- Click 'Settings' on the CIS home screen
- Click 'HIPS' > 'Protected Objects'
- Open the 'Protected Data' tab
- Select the item to be remove and click the 'Remove' button
- Click 'OK' in the 'Advanced Settings' interface to save your settings

The selected item will be removed from the protected data list. CIS will not generate an alert if the item is accessed.

6.4.5. HIPS Groups

Click 'Settings' > 'HIPS' > 'HIPS Groups'

- HIPS groups are collections of one or more COM interfaces or registry keys.
- After defining a HIPS group, it will be available for selection and protection in the **Registry Keys** and **COM Interfaces**.
- CIS ships with predefined 'Registry' and 'COM' groups, and allows you to add new groups.
- You can view manage all groups in the 'HIPS Groups' interface.

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
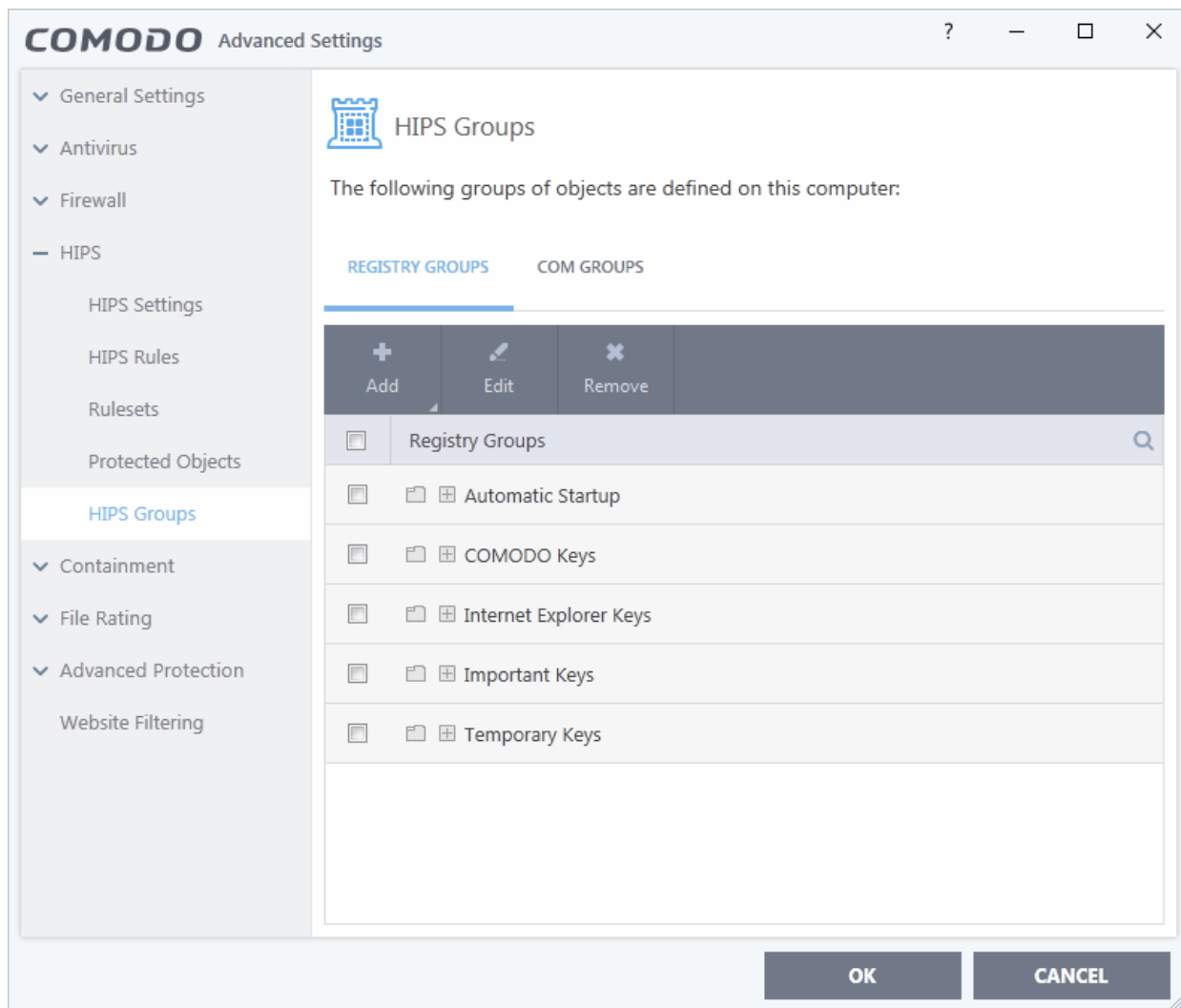
Please note, this area is just where you can view and define the groups. To actually apply the protections you need to select the group in the **Protected Objects** interface.

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

Click 'Settings' > 'HIPS' > 'HIPS Groups' > '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.

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
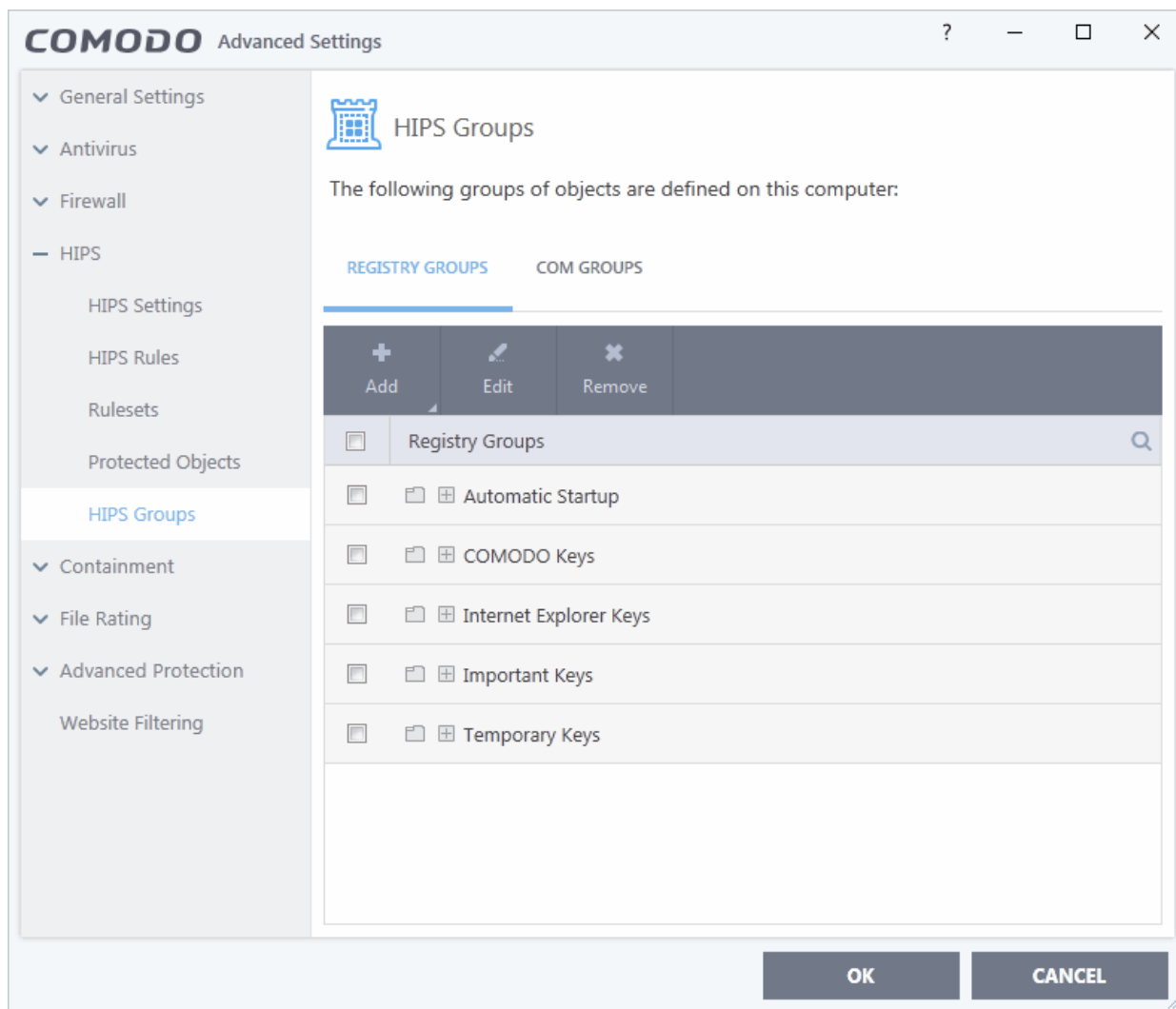
- Click the search icon on the right to find a specific item. You can enter a full or partial name.

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
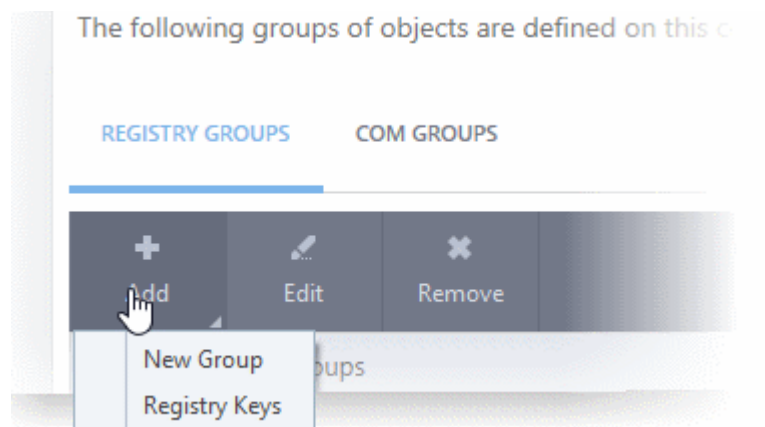
---

- **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'.
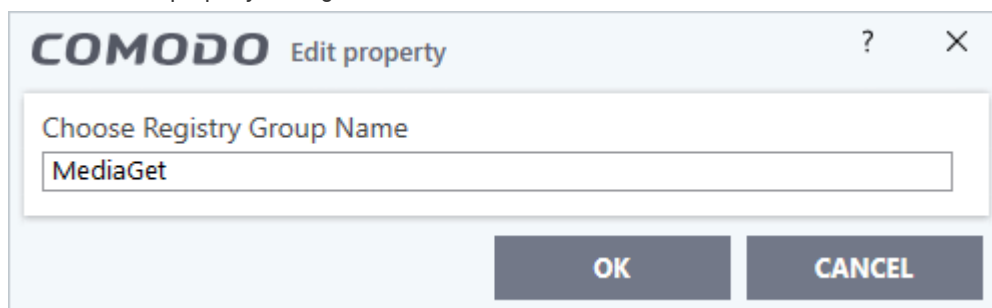
The group will be added to the list.

- **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.
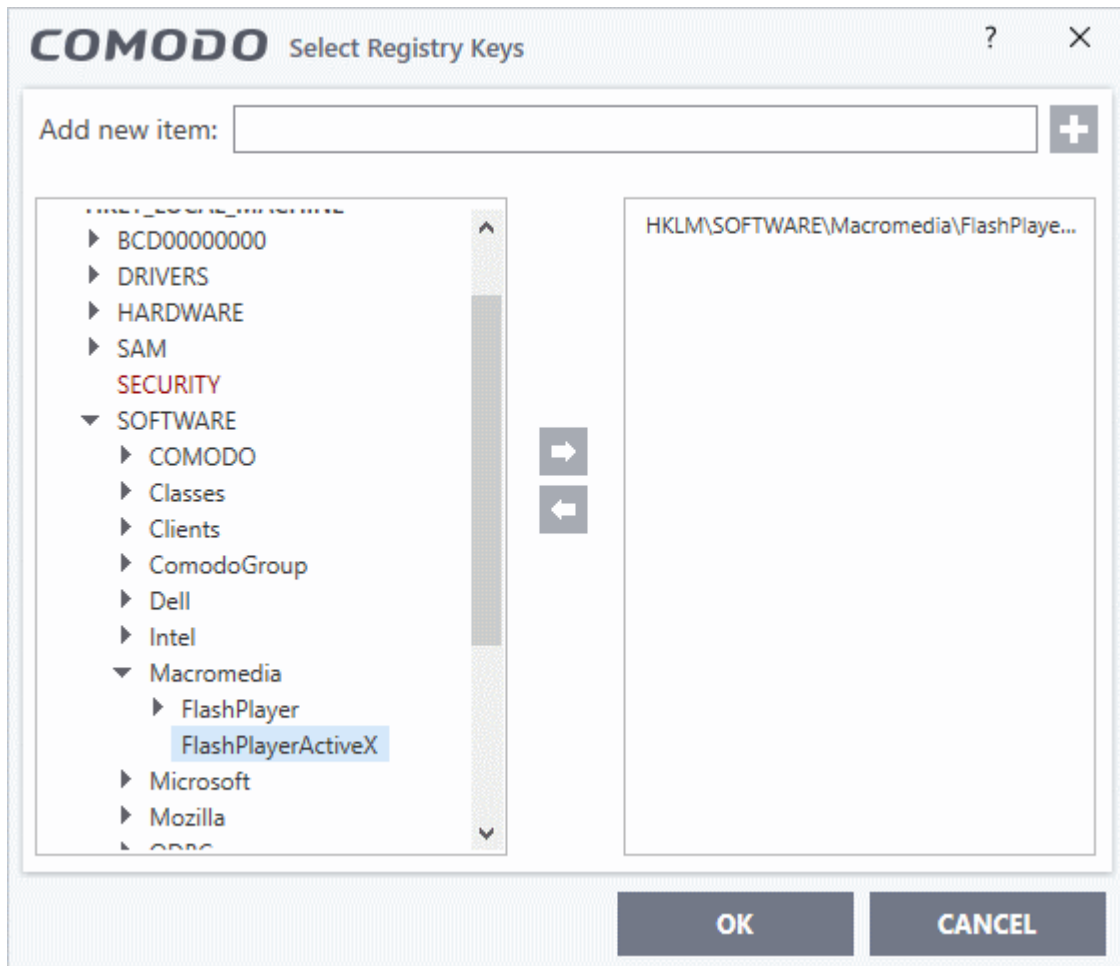
- Select a key on the left then click the right arrow to add a new key to the group. You can add a key manually by typing its name in the 'Add new item' field then clicking the '+' button.

- To edit an existing group, select the group from the list and click the 'Edit' button.
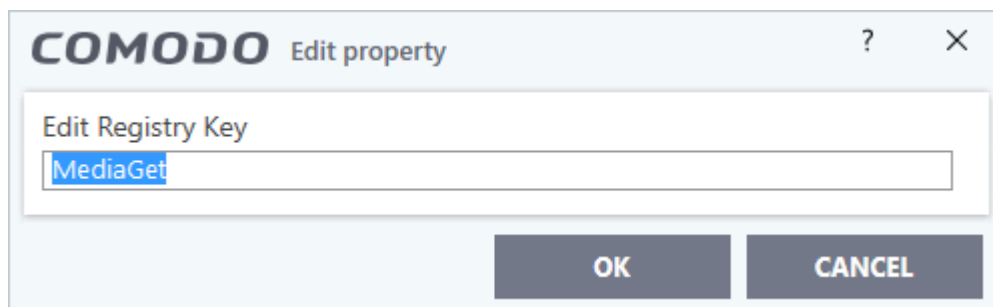
- Modify the name of the group as required and click 'OK'.

- To remove a group, select the group from the list and click the 'Remove' button.
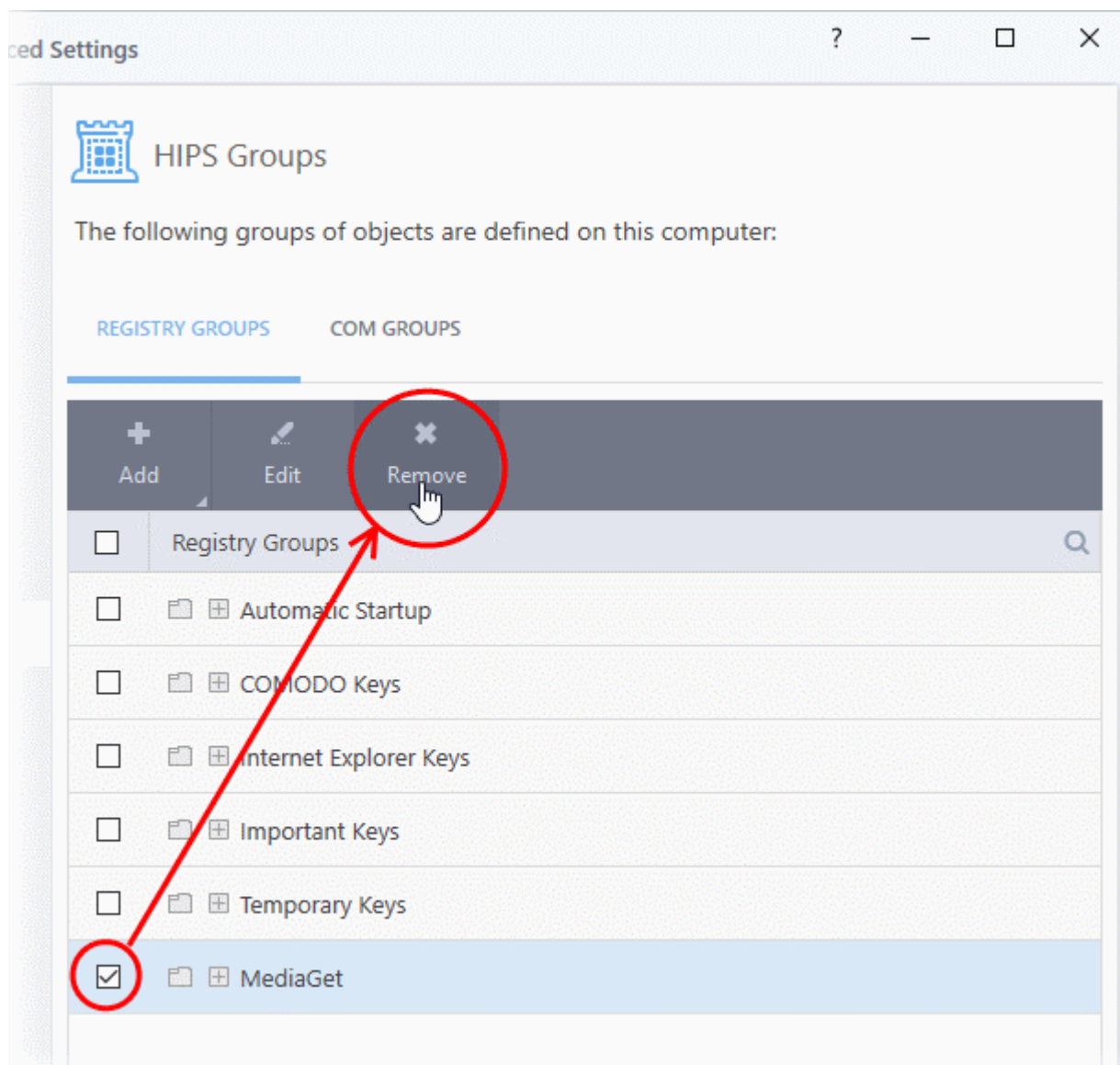
- To remove a key from a group, first expand the group by clicking its '+' symbol, select the key to be removed and click the 'Remove' button.

6.4.5.2. COM Groups

Click 'Settings' > 'HIPS' > 'HIPS Groups' > '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.

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
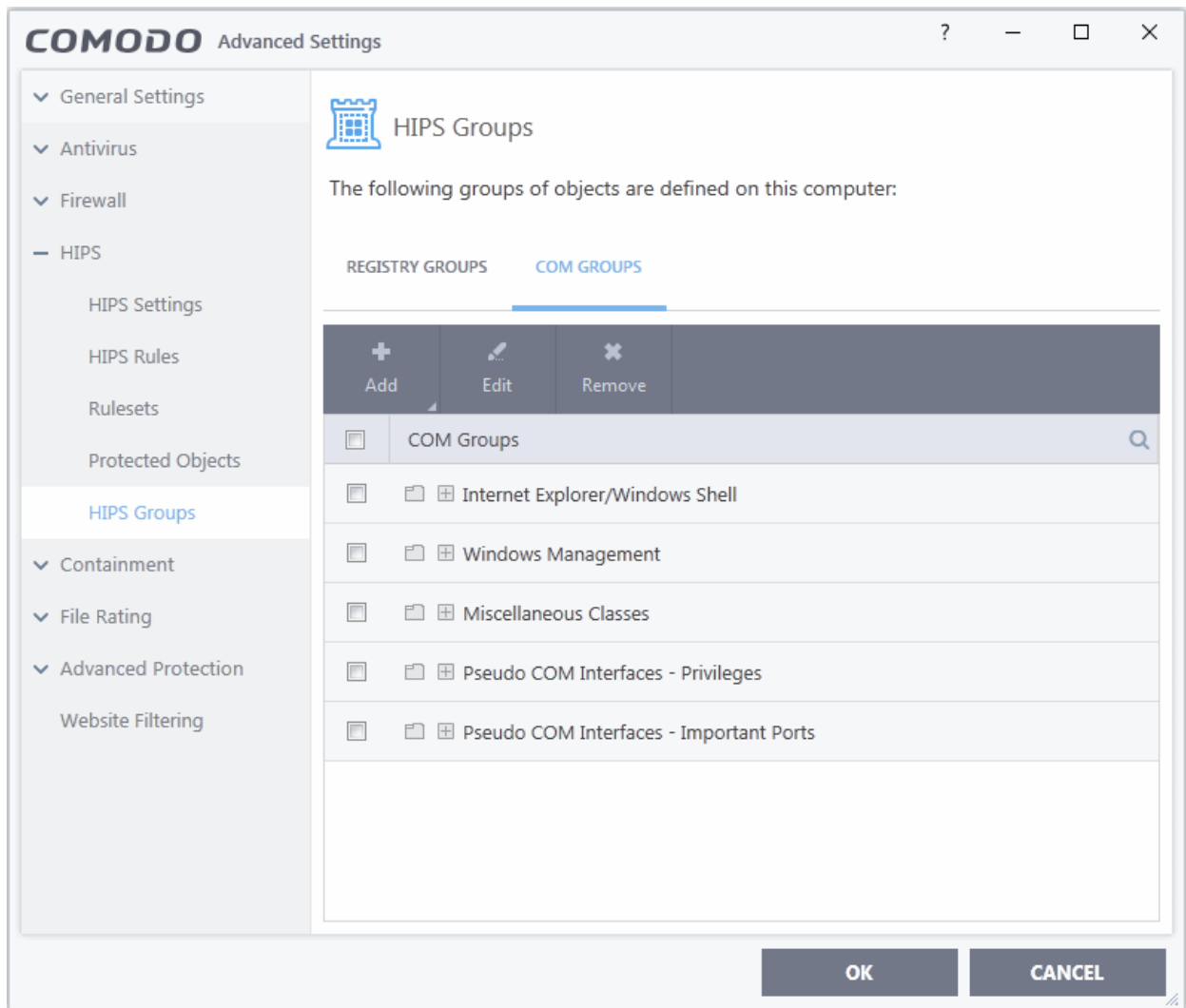
- Click the search icon on the right to find a specific item. You can enter full or partial names.

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
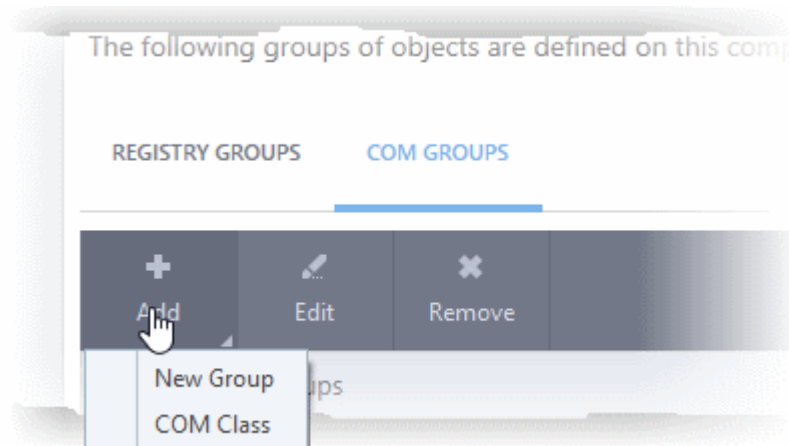
- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.
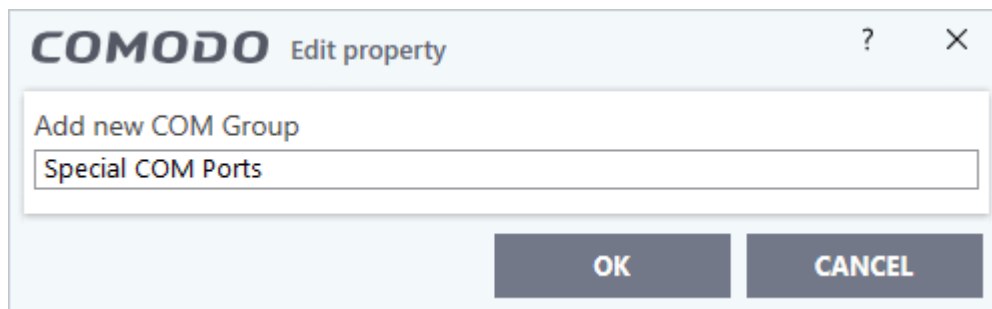
The group will be added to the list.

- **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.
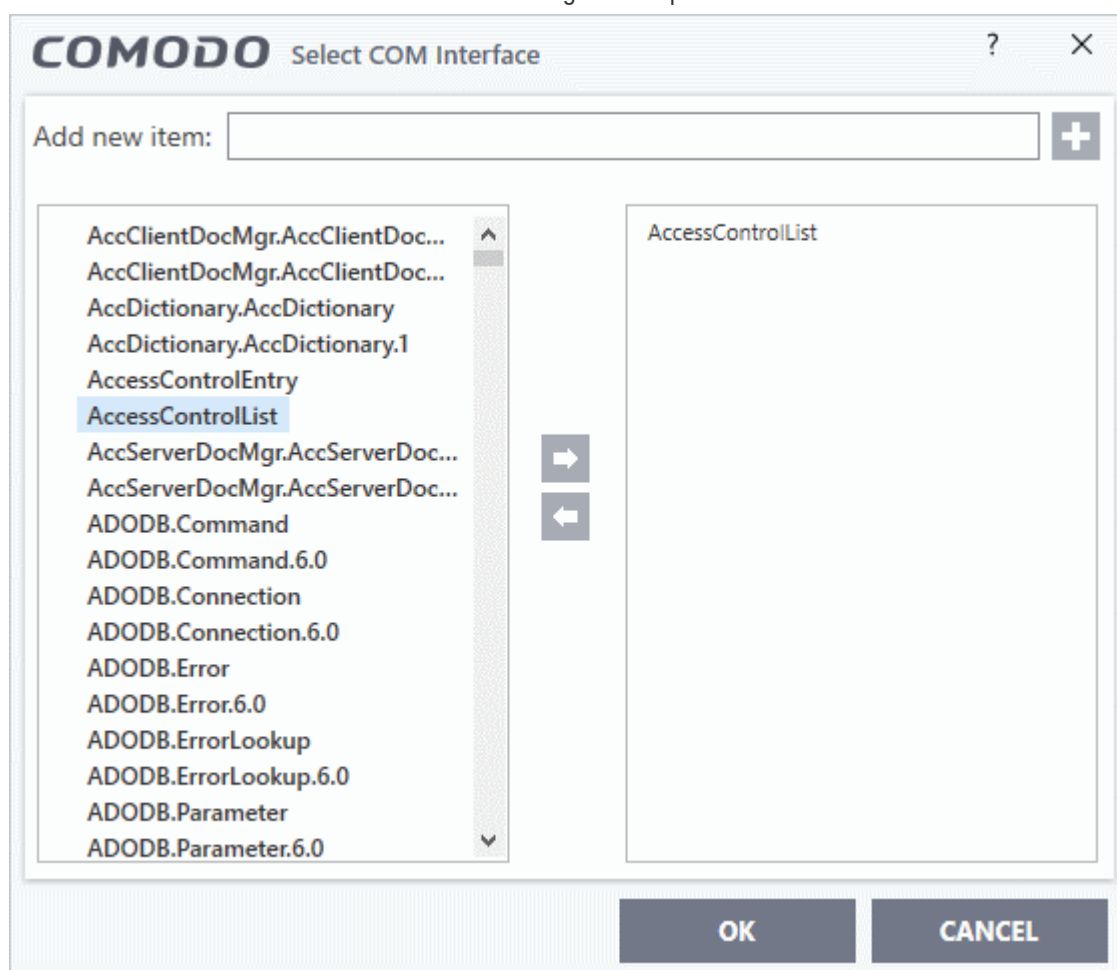
You can add new items by selecting them on the left and clicking the right arrow button. To add items manually, type their name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group from the list and click the 'Edit' button.
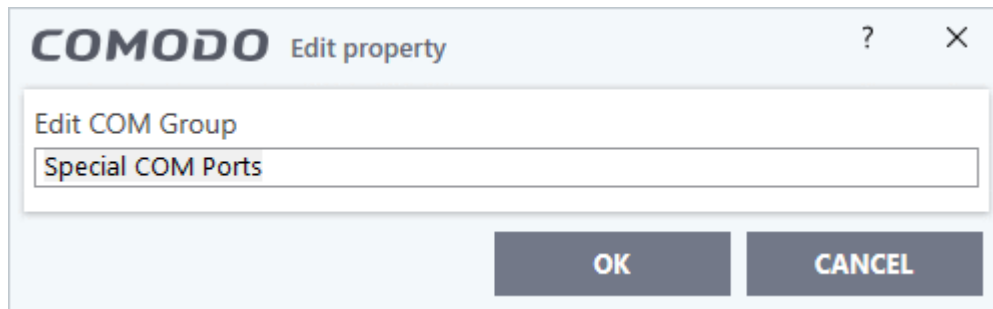
- Edit the name of the group in the 'Edit Property' dialog and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.
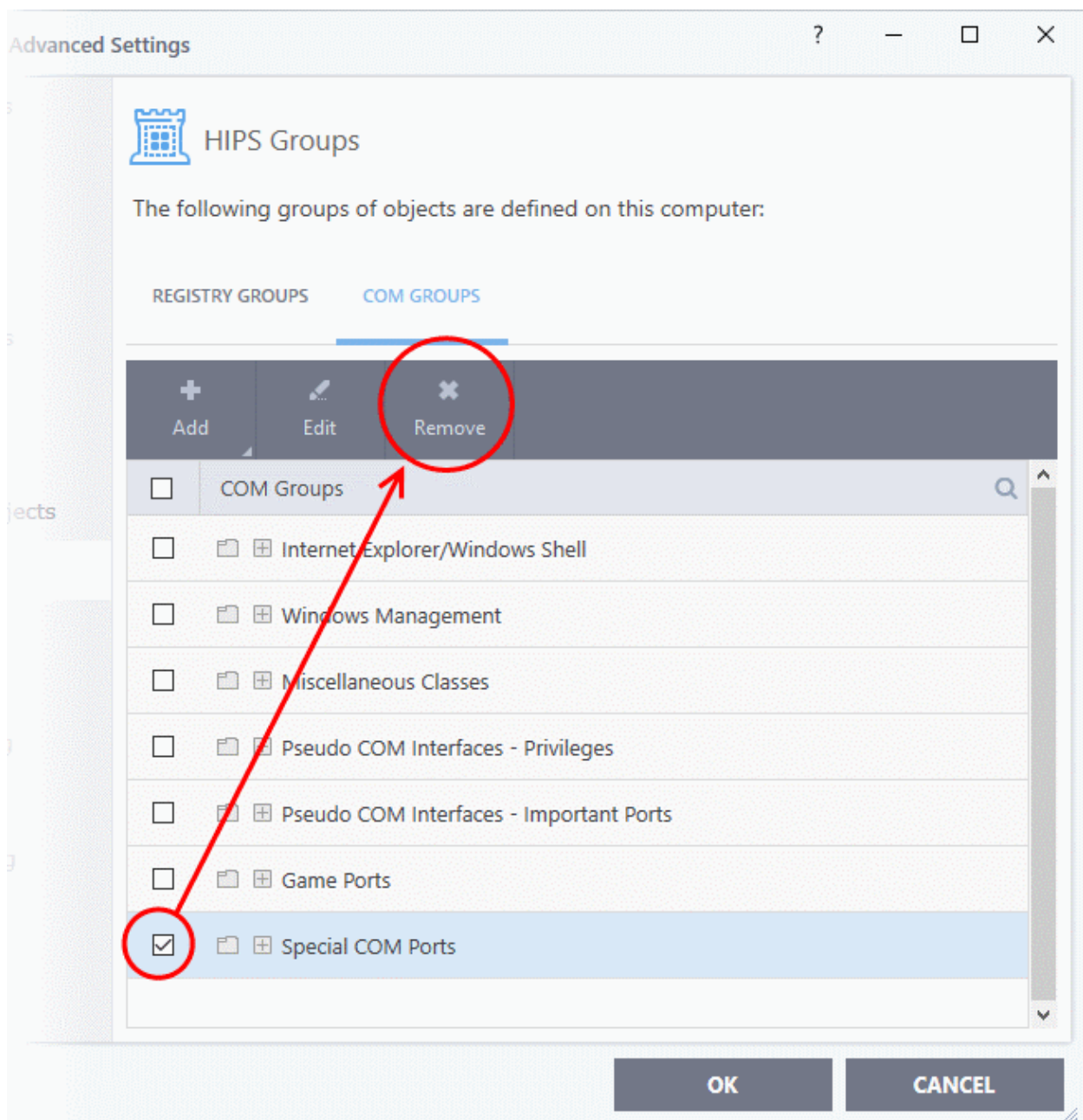
- To remove an individual COM component from a group, click + at the left of the group to expand the group, select the item to be removed and click the 'Remove' button.

6.5. Containment Configuration

Click 'Settings' > 'Containment' to open the section

- If CIS encounters a file that has a trust rating of 'Unknown' then you have the option to automatically run that file in the container.

- The container is a secure, virtual environment where unknown files can run, but cannot affect the rest of your computer.

  - Files in the container are isolated from other processes, write to a virtual file system and registry, and cannot access your user data.

- Shared Space - Applications in the container cannot save files to your local file system. Because of this, CIS creates a special folder at 'C:\ProgramData\Shared Space' for you to save files created or downloaded in the container. You can access files in this folder from your local desktop.

- The containment settings area lets you configure all aspects of the container:
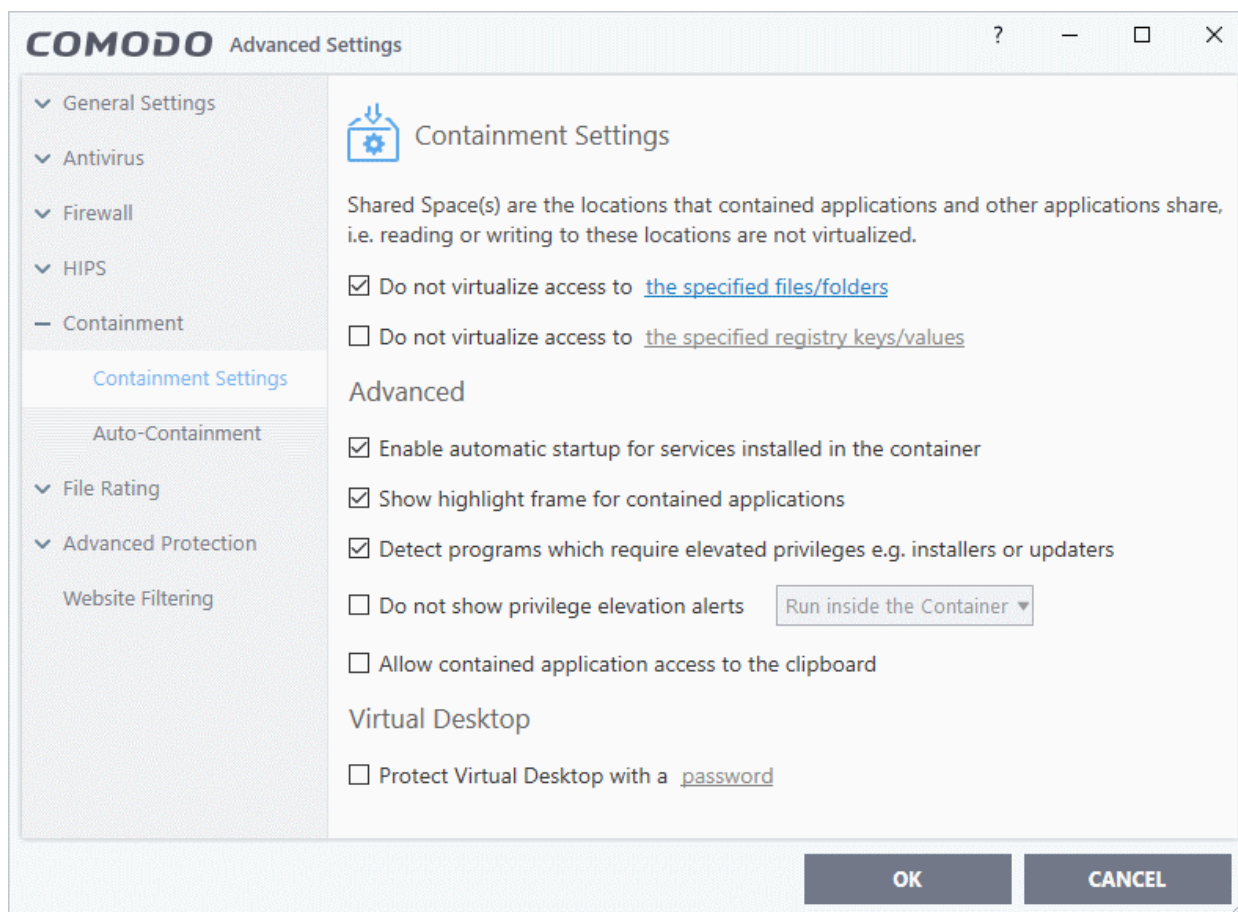
See the following sections for more help:

- **Containment Settings** - Configure exceptions to virtualization and other general settings
- **Auto-Containment Rules** - Create and manage rules which tell CIS how to handle unknown files.
- **Containment - An Overview** - Background information about the containment process
- **Unknown Files: The Scanning Processes** - Background information on how CIS determines the reputation of a file.

Note: The containment feature is not supported on the following platforms:
- Windows XP 64 bit
- Windows Server 2003 64 bit

6.5.1. Containment Settings

Click 'Settings' > 'Containment' > 'Containment Settings'

- The settings area lets you configure how proactive the auto-containment feature should be, and which types of files it should check.
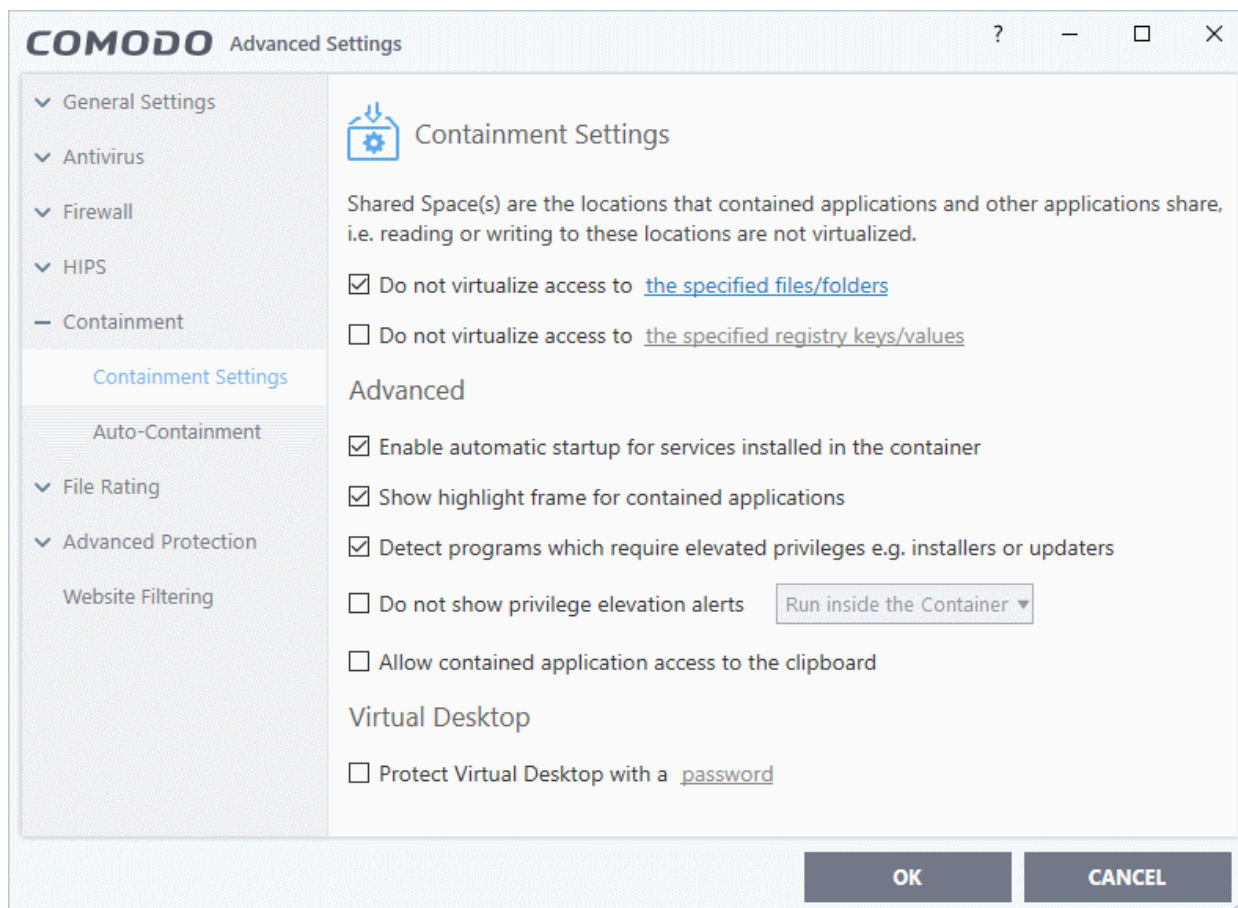
- By default, contained applications can access folders, files and registry keys on your local system, but cannot make changes to them.

- The 'Do not virtualize...' settings let you create exceptions to these policies if required.

- You can also adjust settings for the clipboard, display mode, virtual desktop, and more.

Do not virtualize access to the specified files/folders - Specify files/folders on the host computer that contained applications are allowed to write to. By default, contained applications write to a virtual file system, and cannot access files/folders on the host system.

- Enable the option then click 'the specified files/folders' link.

- The exclusions dialog shows files and folders that can be modified by contained applications. By default, 'Shared Space' is the only folder they can write to:
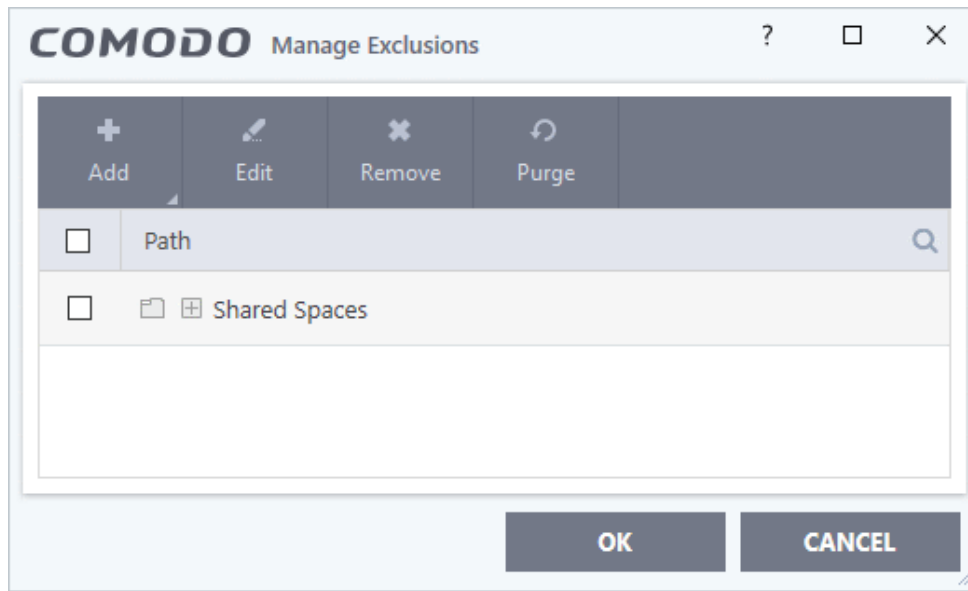
- Click the 'Add' button then select the item you want to exclude:
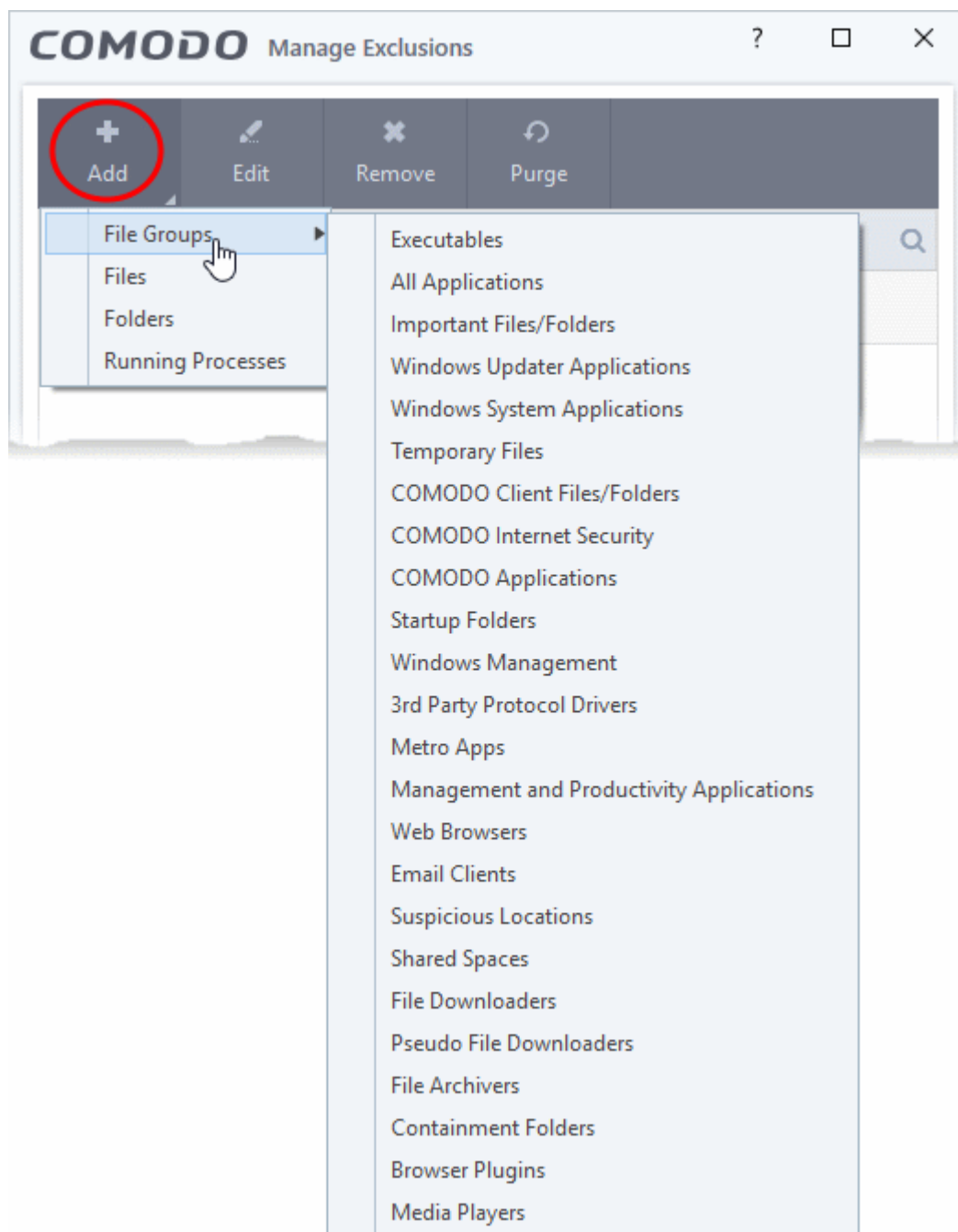
- **File Groups** - Choose a category of files or folders to which access should be granted.
- For example, select 'Executables' to allow access to files with extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd.

  See **File Groups** if you want more help with file groups.
- **Files** - Pick specific files on the host that contained applications can access.
- **Folders** - Specify folders that can be accessed by contained applications. Access is granted to all files in the folder.
- **Running Processes** - Choose a process currently running on your computer. The parent application of the process is added to the exclusions.
- **Edit** - Select an item and click 'Edit' to change the target file or folder
- **Remove** - Select an item and click 'Remove' to delete an exception
- **Purge** - Checks that all files and folders covered in exceptions are still present on your computer. Purge automatically removes any items it can no longer locate.
- Click 'OK' to implement your settings

Do not virtualize access to the specified registry keys/values - Specify registry keys on the host computer that contained applications are allowed to write to. By default, contained applications write to a virtual registry, and cannot access the real registry on the host system.

- Select the option then click 'the specified registry keys/values' link.

- The exclusions dialog shows keys on the host which contained applications are allowed to access.
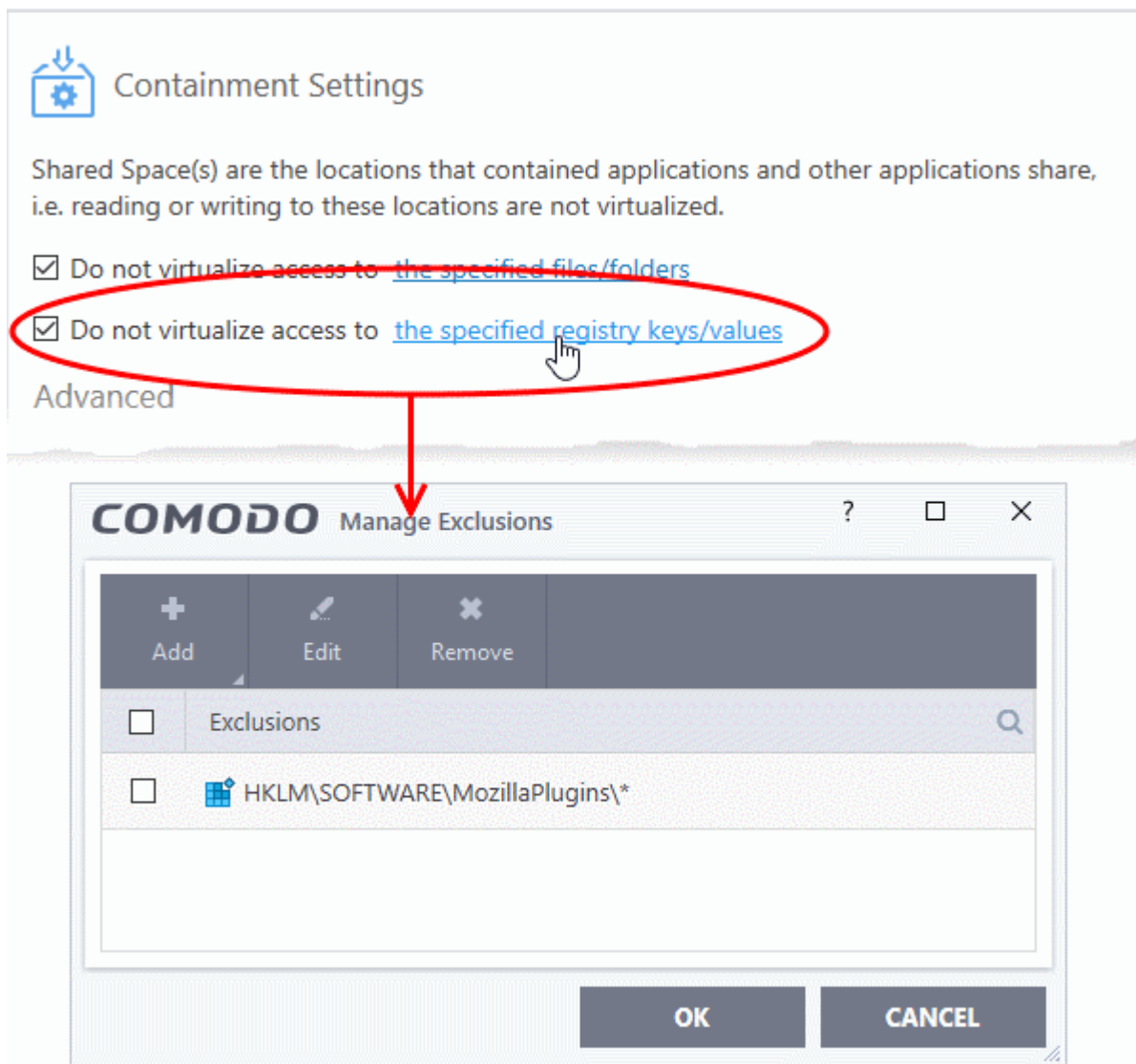
- Click the 'Add' button then select the keys you want to exclude:
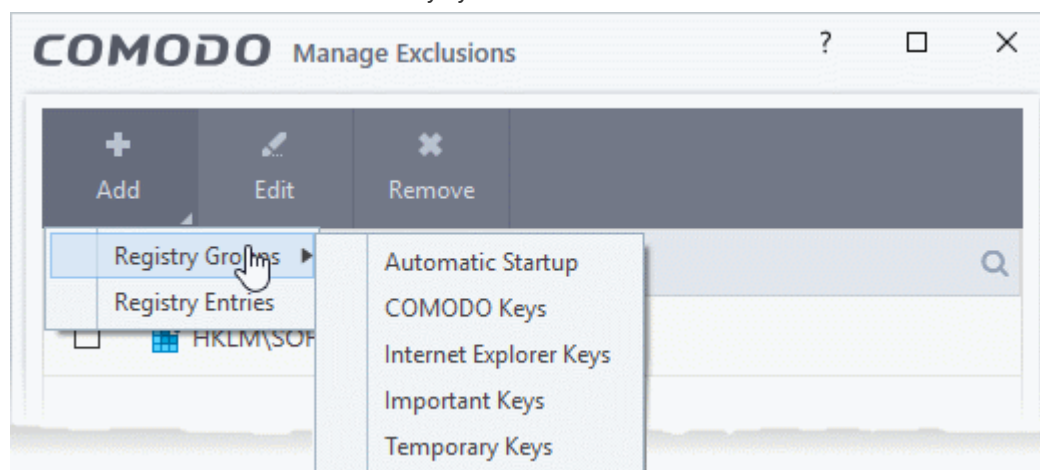
- **Registry Groups** - Exclude a predefined collection of registry keys. See '**Registry Groups**' for an explanation of registry groups as defined in CIS.
- **Registry Entries** - Exclude individual registry keys:
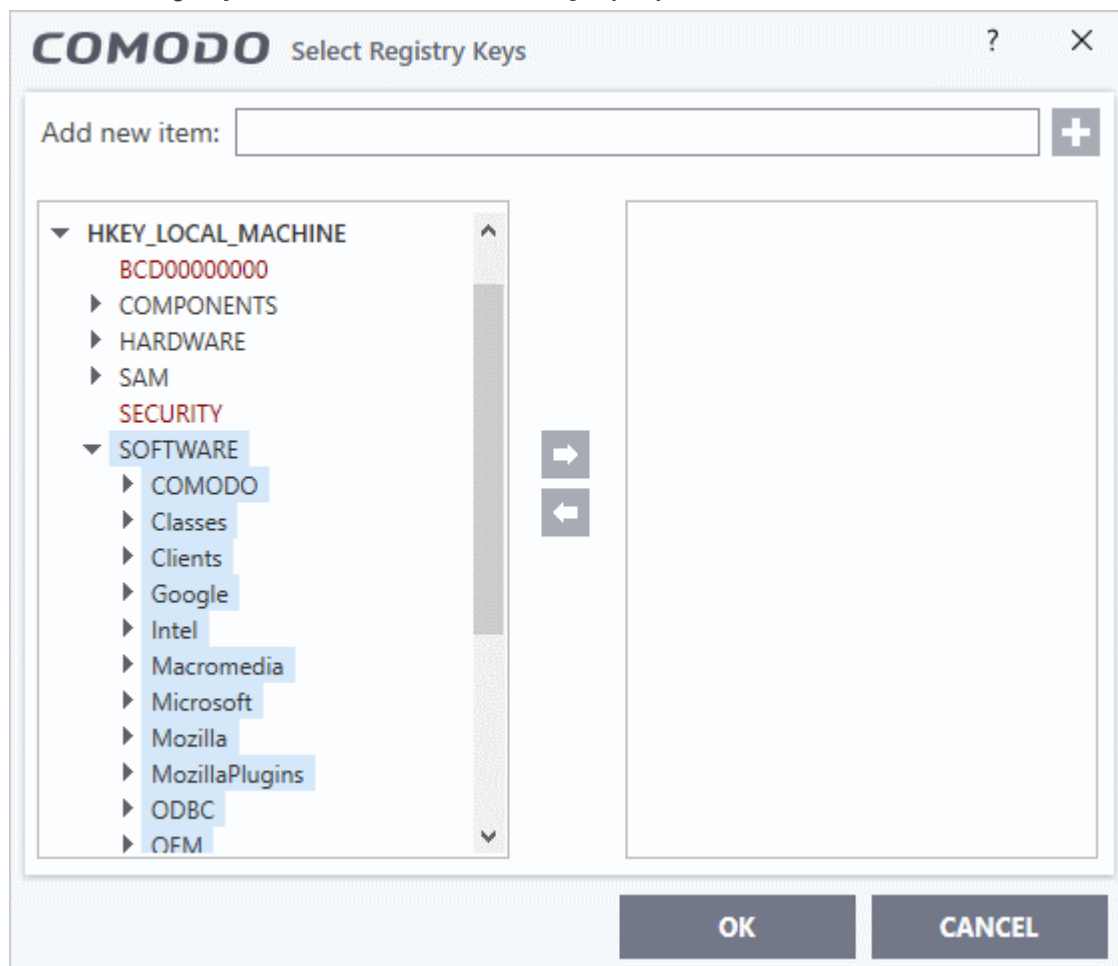
- **Edit** - Select an item and click 'Edit' to change the target path
- **Remove** - Select a key or group and click 'Remove' to delete the exception
- Click 'OK' to implement your settings

Advanced Settings:

- **Enable automatic startup for services installed in the container** - CIS launches contained services at Windows startup if this option is enabled. (**Default = Enabled**)
  - Clear this box if you do not want those services to run at startup.
- **Show highlight frame for contained applications** - CIS displays a green border around the windows of programs that are running in the container. (**Default = Enabled**)

The following screenshot shows an Open Office document running in the container:
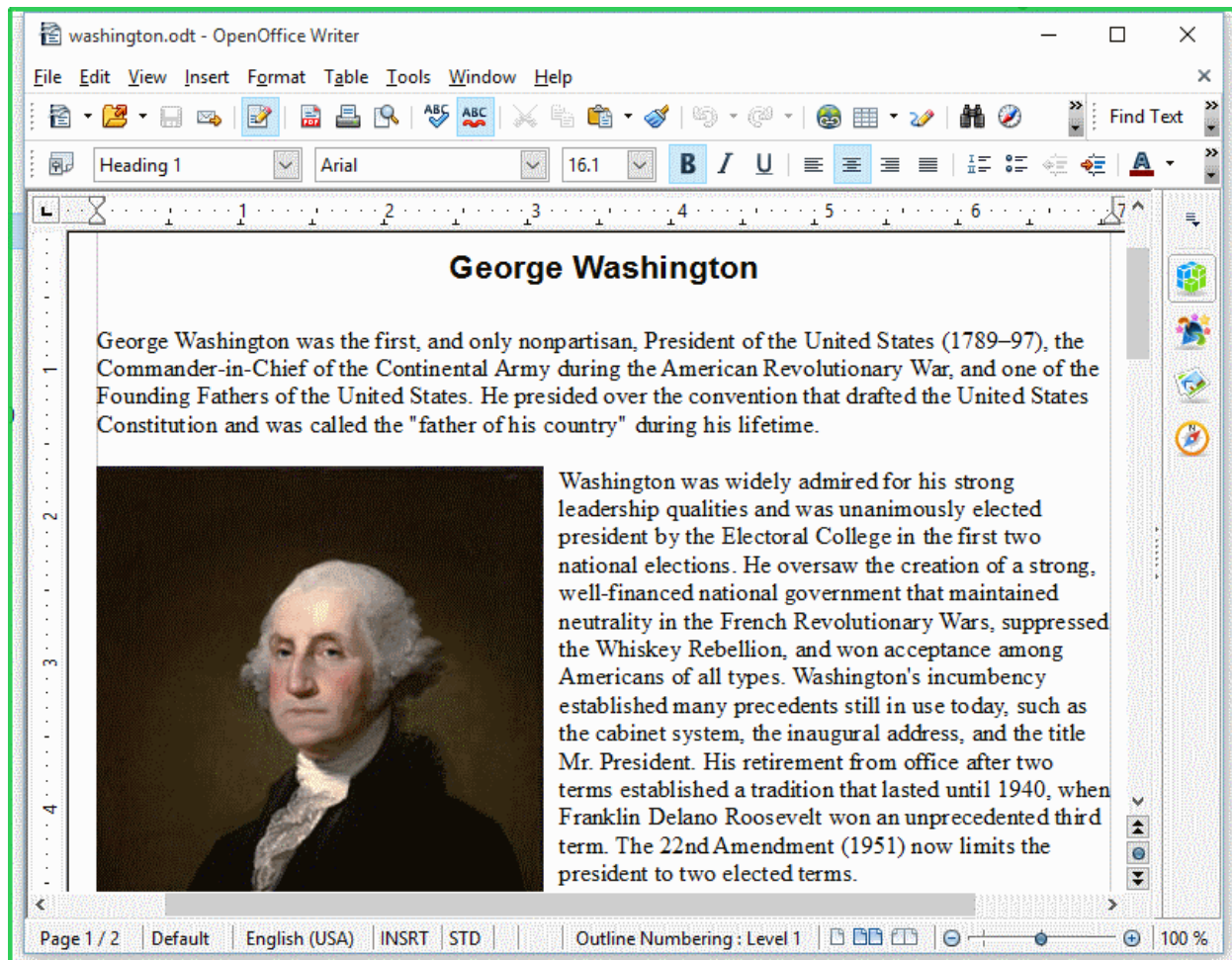
- **Detect programs which require elevated privileges e.g. installer or updaters**: CIS generates an alert when it detects an installer/updater that requires admin/elevated privileges to run. An installer that is allowed to run with elevated privileges can make changes to important areas of your computer such as the registry. (**Default = Enabled**)

- Example alert:
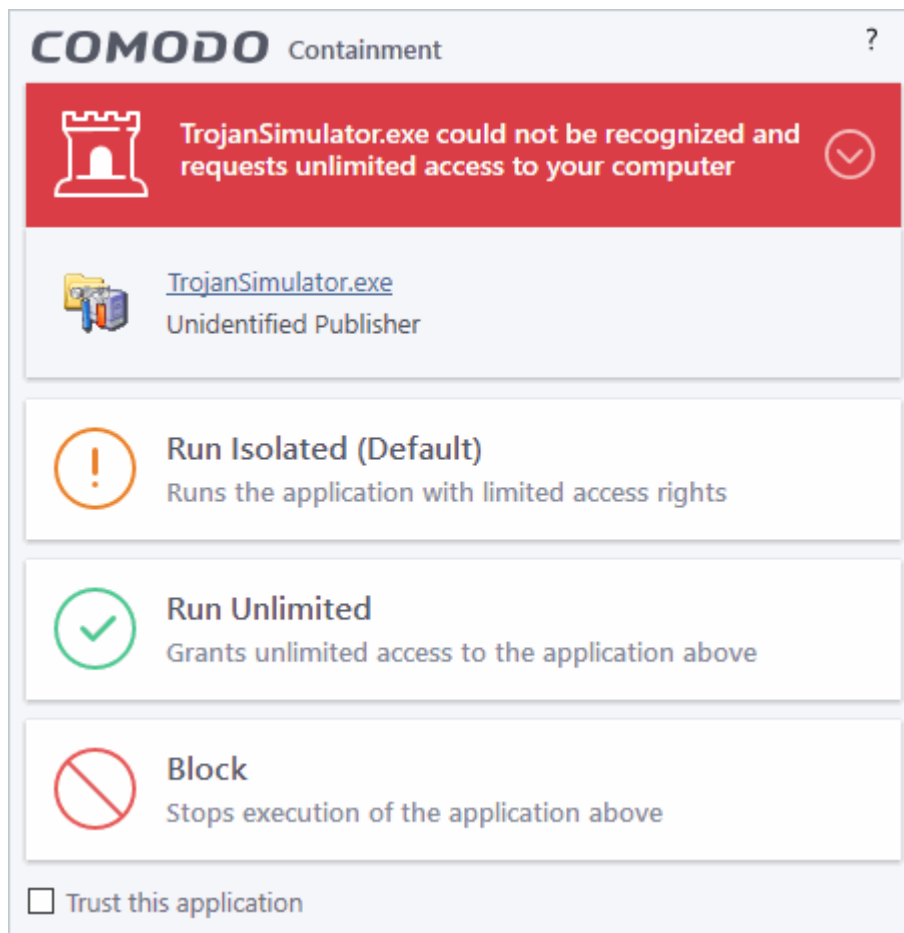
- Run Isolated - Runs the installer/updater in the container
- Run Unlimited - Runs the installer/updater on your local computer, outside the container.
- Block - Terminates the installer/updater.
- See '**Understand Security Alerts**' for more details.
  - Disable this option if you want CIS not to monitor applications that request elevated privileges on your computer
- **Do not show privilege elevation alerts**: Whether or not CIS shows alerts (as shown above) when a new or unrecognized application requires admin or elevated privileges to run.
  - If you disable alerts, you need to choose a default action that CIS should implement when it detects such an application:
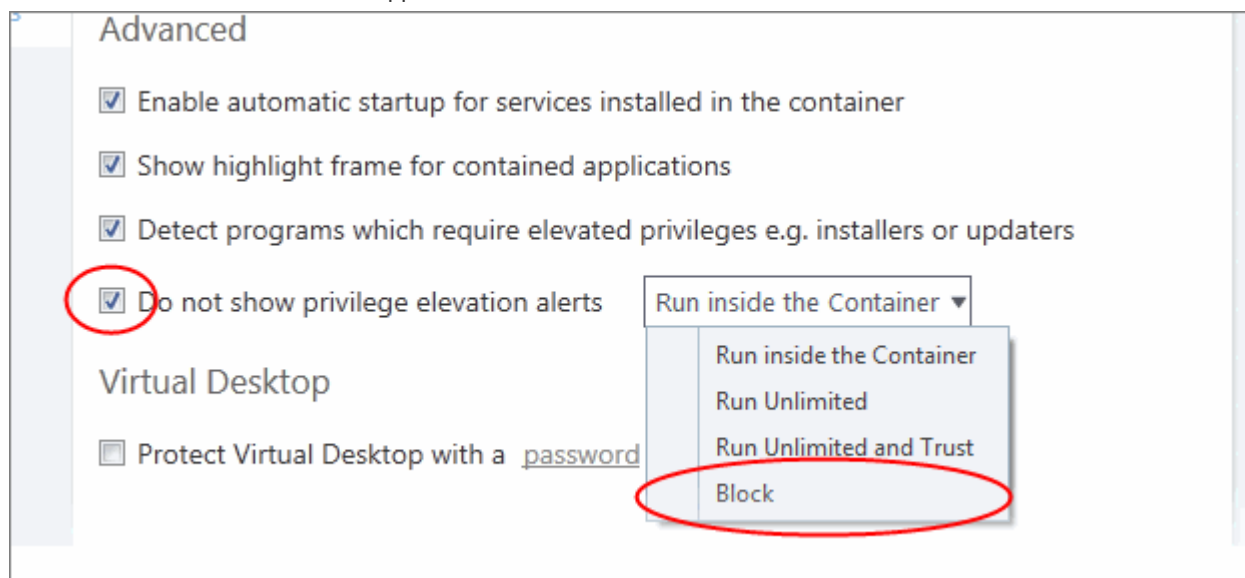
- **Allow contained application access to clipboard**: By default, applications in the container cannot access data in your clipboard. This can sometimes cause inconvenience when trying to copy and paste.
  - Enable this option to grant contained applications access the clipboard. This change requires a system restart.
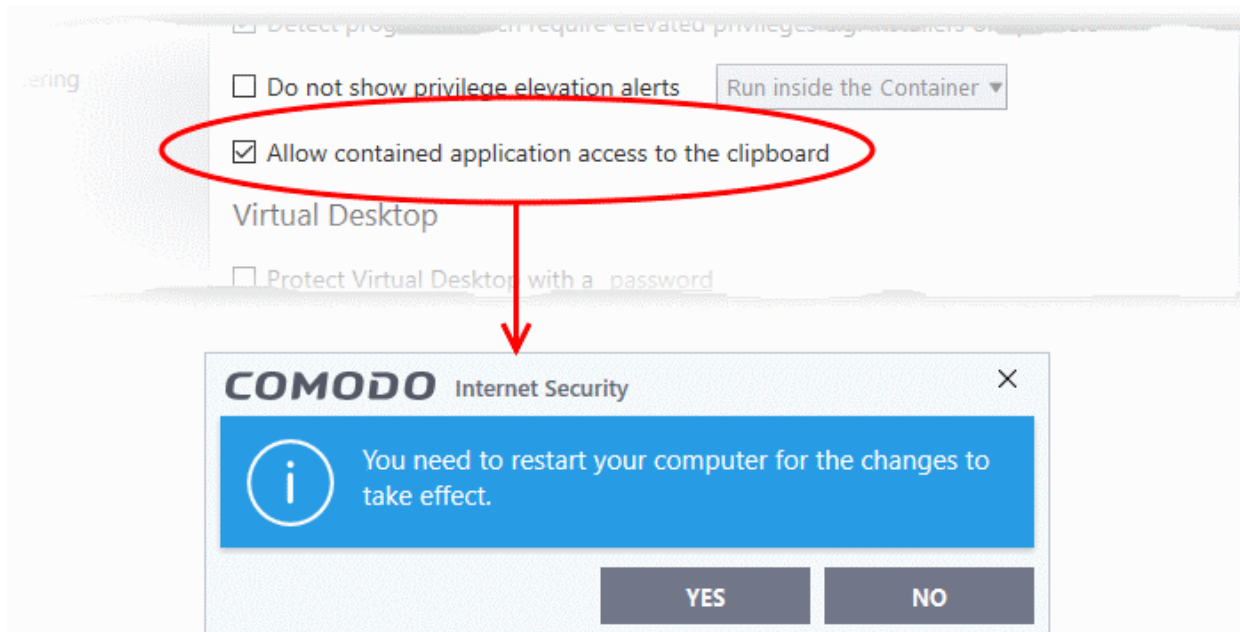
- Click 'Yes' to confirm your setting.
- Contained apps can access your clipboard after the next restart of your computer.

Virtual Desktop Settings

The 'Virtual Desktop' Settings area allows you to password protect your Virtual Desktop. Once set, the password has to be entered in order to close the Virtual Desktop:
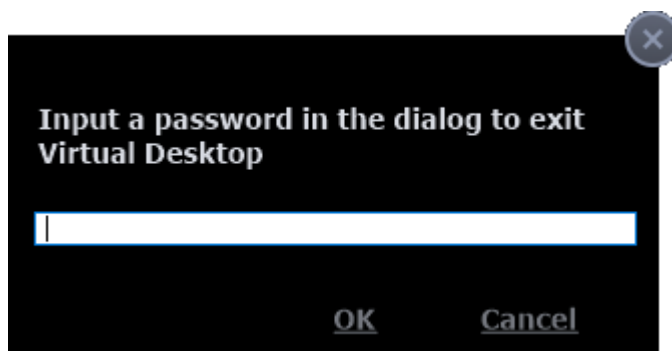
This is a security measure to prevent guests or younger users from closing the Virtual Desktop and accessing the host, potentially exposing your computer to danger.

Set an exit password for the Virtual Desktop:

- Check the 'Protect Virtual Desktop with a password' box then click the password link. The 'Create/change password' dialog will appear:
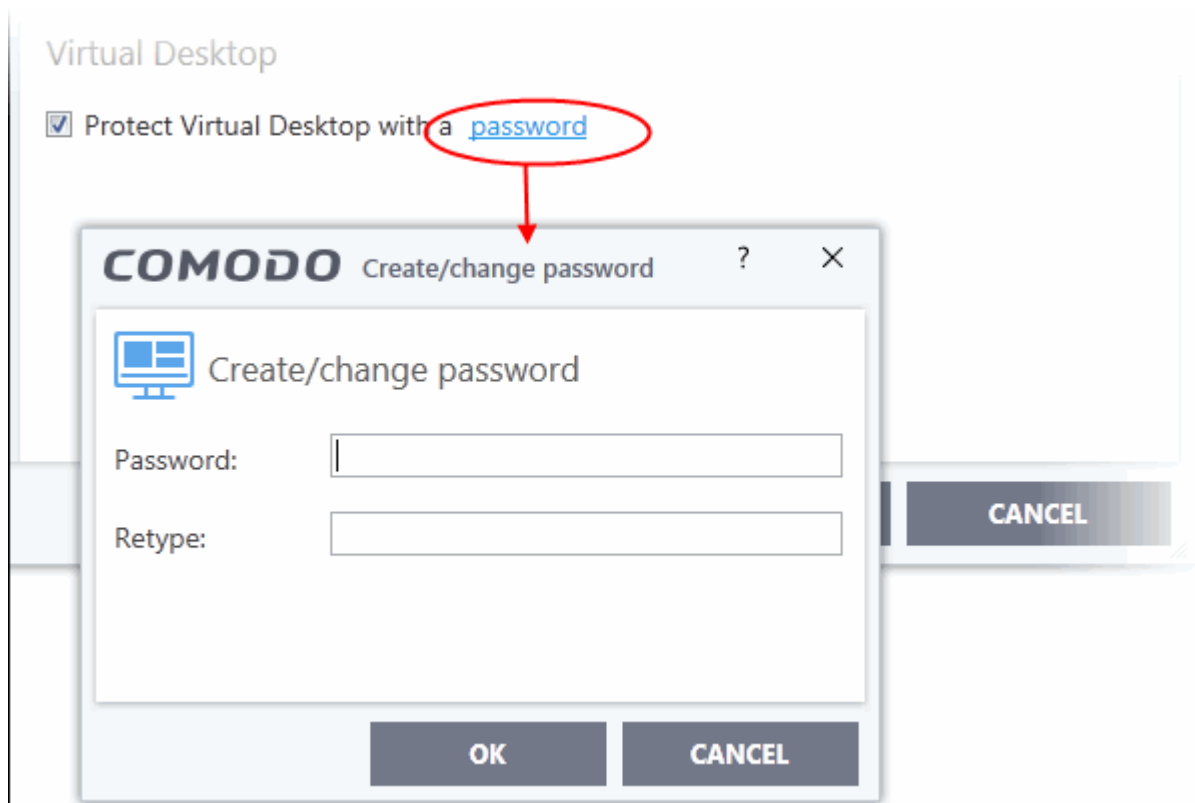
- Type a password that cannot easily be guessed. It should be at least 8 characters long and contain a combination of uppercase and lowercase letters, numbers and special characters.
- Re-enter the password in the 'Retype' field then click 'OK'.

You will now be asked for a password every time you exit the Virtual Desktop.

> **Note**. You may see an error if an app on the host tries to update itself at the same time as that app is updating itself in the container. This is a classic Windows sharing violation which is shown when an app attempts to write to a file that is already in use. Please shut down the contained version of the app then run the update on the locally hosted version. The contained version will function correctly once the update to the local version is complete.

6.5.2. Auto-Containment Rules

Click 'Settings' > 'Containment' > 'Auto-Containment'

- Auto-containment rules determine whether a program is allowed to run as normal, run with restrictions, or run in the virtual environment.
- 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.
- CIS consults these rules whenever you open an application. Rules at the top of the list have higher priority. You can re-prioritize rules using the 'Move Up' and 'Move Down' buttons.
- Programs running in the container have a green border around them.
- CIS ships with a set of pre-configured rules which provide maximum protection against unknown, potentially malicious applications. You can also create your own custom rules.

Manage Auto-Containment rules

- Click 'Settings' on the CIS home screen.
- Click 'Containment' > 'Auto-Containment':
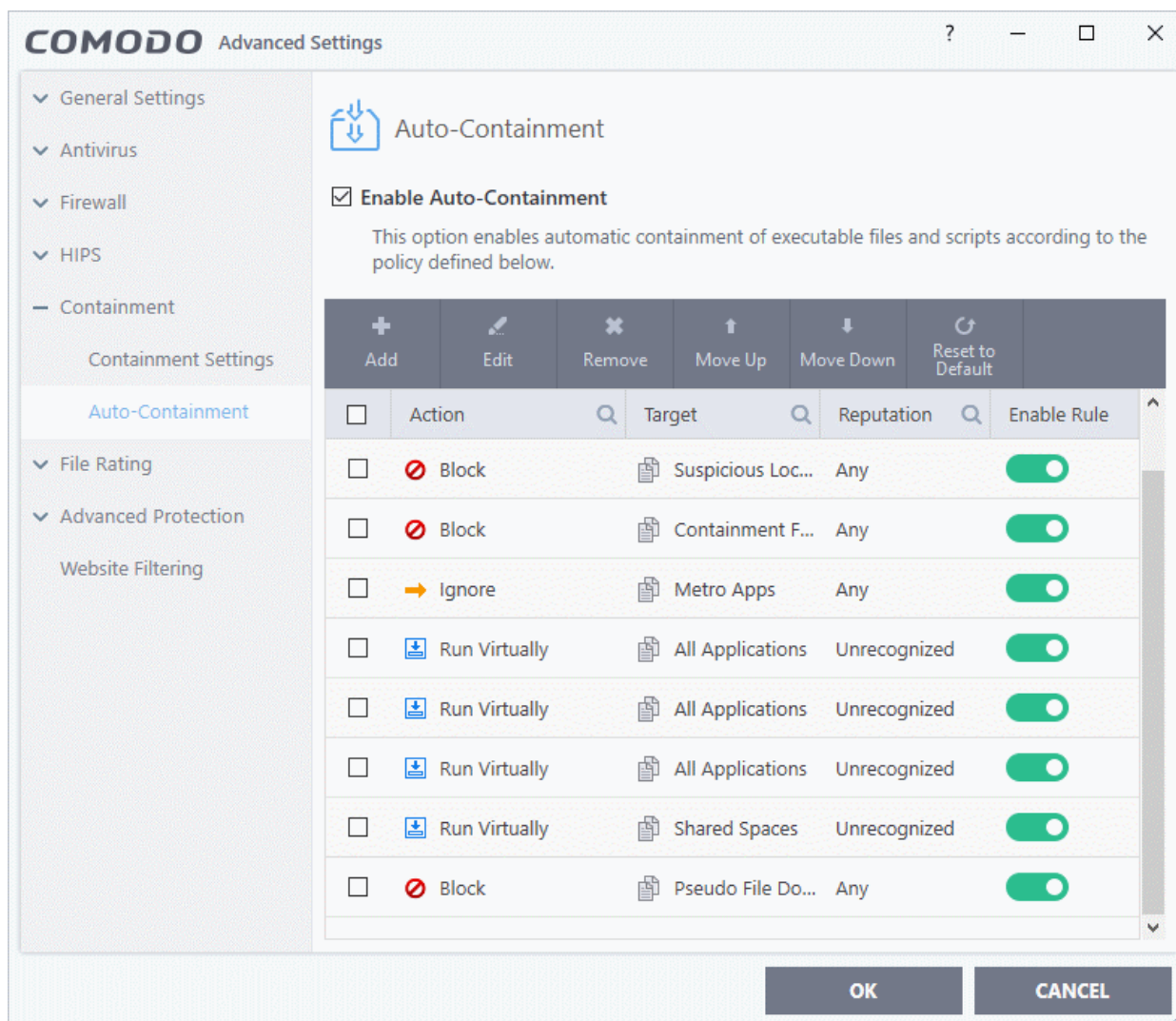
- The higher a rule is in the list, the higher priority it has. Use the move up/down buttons to change a rule's priority. In the event of a conflict in settings, CIS will obey the rule that is higher in the list.

- You can also add new rules and manage existing rules from this panel.

General Settings

- **Enable Auto-Containment** - Enable or disable the containment system. If enabled, applications are run in the container as per the rules in this interface. (*Default = Enabled*)

Containment Rules

A rule performs a specific action on targets which have a certain reputation.

Containment Rules - Column Descriptions	
Column Header	**Description**
Action	The operation that the containment system should perform on the target if the rule is triggered.
Target	The file, file group, or location on which the rule should run.
Reputation	The trust status of the target item - 'Malware', 'Trusted' 'Unrecognized' or 'Any'. The rule will apply to target items which have the reputation you choose here.
Enable Rule	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.
- There are four 'Block' rules, four 'Run Virtually' rules, and one 'Ignore' rule.
- The rule numbers indicate their default priority in CIS. If there is a conflict, CIS implements the rule with the highest priority. You can, of course, rearrange priorities as required.
- The following tables show the settings of the pre-defined rules.

'Block' Rules

1 - Block and quarantine any malicious application

2 - Block any file in the 'Suspicious locations' file group (i.e. anything in CIS quarantine and recycle bin)

3 - Block any file in the folders Comodo uses for the container (i.e. anything in the \vtroot\ folder)

9 - Block pseudo file downloaders which are downloaded by browsers. Example downloaders are wscript.exe, powershell.exe, perl.exe etc.

Rule Number			1	2	3	9
Action			Block	Block	Block	Block
Target			File Group - All Applications	File Group - Suspicious Locations	File Group - Contained Folders	File Group - Pseudo File Downloaders
File Reputation			Malicious	Any	Any	Any
File origin	Source of file creation	Application	Any	Any	Any	Any
		Process(es)	Any	Any	Any	Web Browsers Rating = Any
		user(s)	Any	Any	Any	Any
	Downloaded from		Any	Any	Any	Any
Vendor			Any	Any	Any	Any
Age of file			Any	Any	Any	Any
Log Action			On	On	On	On
Restriction Level			N/A	N/A	N/A	N/A
Limit Maximum Memory			N/A	N/A	N/A	N/A
Limit Program Execution Time			N/A	N/A	N/A	N/A
Quarantine			On	Off	Off	N/A
Exclude child processes from the action			N/A	N/A	N/A	N/A

'Run Virtually' Rules

5 - Virtualize any unknown file which is less than 3 days old

6 - Virtualize unknown files created/downloaded by software types in the 'Application' row

7 - Virtualize any unknown file obtained from the internet, intranet, or removable media

8 - Virtualize any unknown file in shared space

Rule Number	5	6	7	8
Action	Run Virtually	Run Virtually	Run Virtually	Run Virtually
Target	File Group - All	File Group - All	File Group - All	File Group -

	Applications	Applications	Applications	Shared Spaces
File Reputation	Unrecognized	Unrecognized	Unrecognized	Unrecognized
File origin / **Source of file creation** / **Application**	Any	Web Browsers Email Clients File Downloaders Pseudo File Downloaders File Archivers Management and Productivity Applications Browser Plugins Media Players	Any	Any
Process(es)	Any	Any	Any	Any
user(s)	Any	Any	Any	Any
Downloaded from	Any	Any	Intranet Removable Media Internet	Any
Vendor	Any	Any	Any	Any
Age of file	Less than 3 days	Any	Any	Any
Log Action	On	On	On	On
Restriction Level	Off	Off	Off	Off
Limit Maximum Memory	Off	Off	Off	Off
Limit Program Execution Time	Off	Off	Off	Off
Quarantine	N/A	N/A	N/A	N/A
Exclude child processes from the action	N/A	N/A	N/A	N/A

Ignore Rule

4 - Do not auto-contain metro apps

Rule Number	**4**
Action	Ignore
Target	File Group - Metro Apps
File Reputation	Any
File origin / **Source of file creation** / **Application**	Any
Process(es)	Any
user(s)	Any
Downloaded from	Any
Vendor	Any
Age of file	Any

Log Action	On
Restriction Level	N/A
Limit Maximum Memory	N/A
Limit Program Execution Time	N/A
Quarantine	N/A
Exclude child processes from the action	Off

Add an Auto-Containment Rule

- Auto-containment rules can be created for a single application, for all applications in a folder/file group, for running processes, or for a file/process hash value.

- You can create precision rules by specifying 'file creation source', 'file rating of the source', 'file origin', 'file rating' or 'file age'.

- 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:
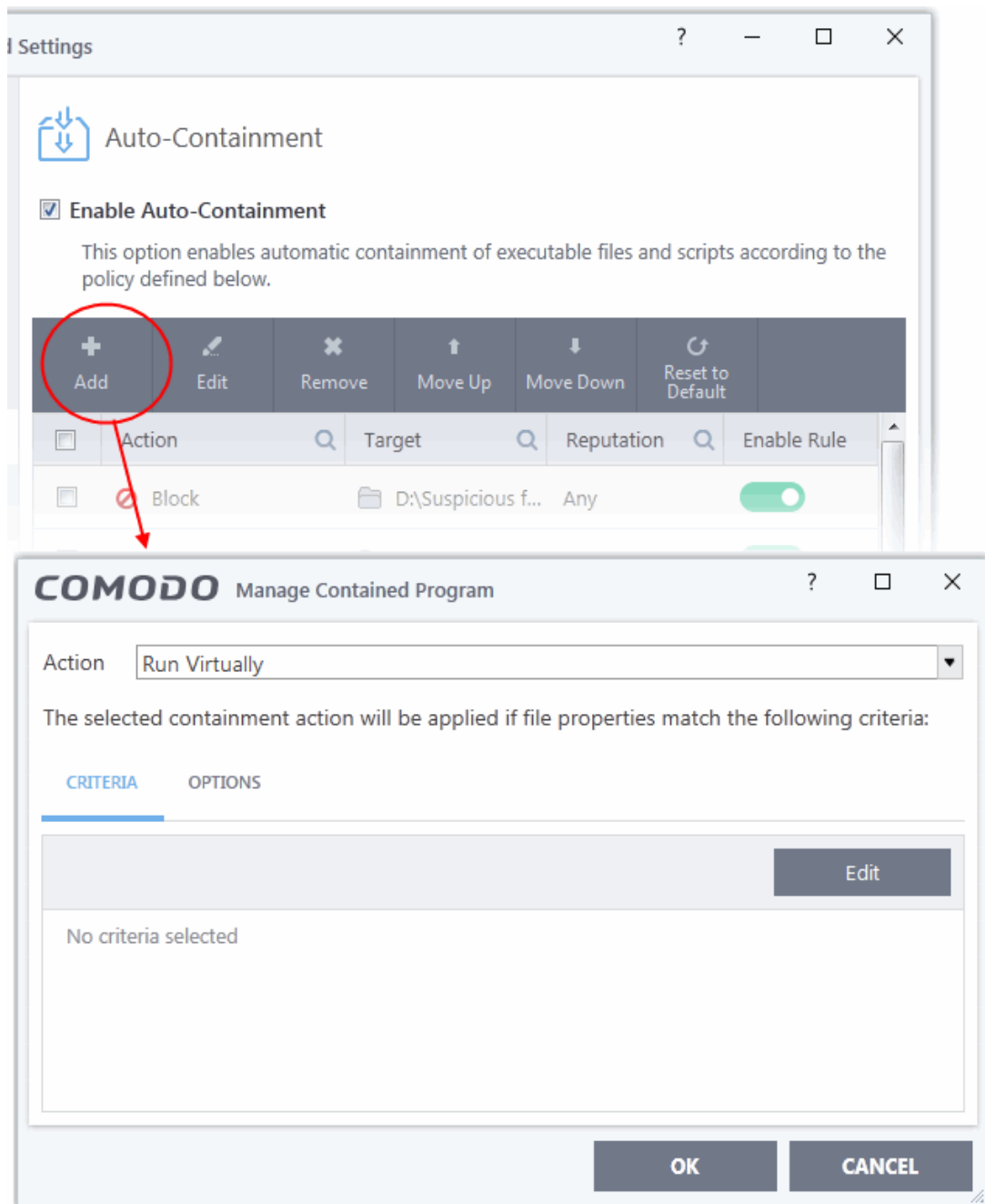
- The 'Manage Contained Program' dialog will appear. The 'Manage Contained Program' displays the action at the top and contains two tabs:

- **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.
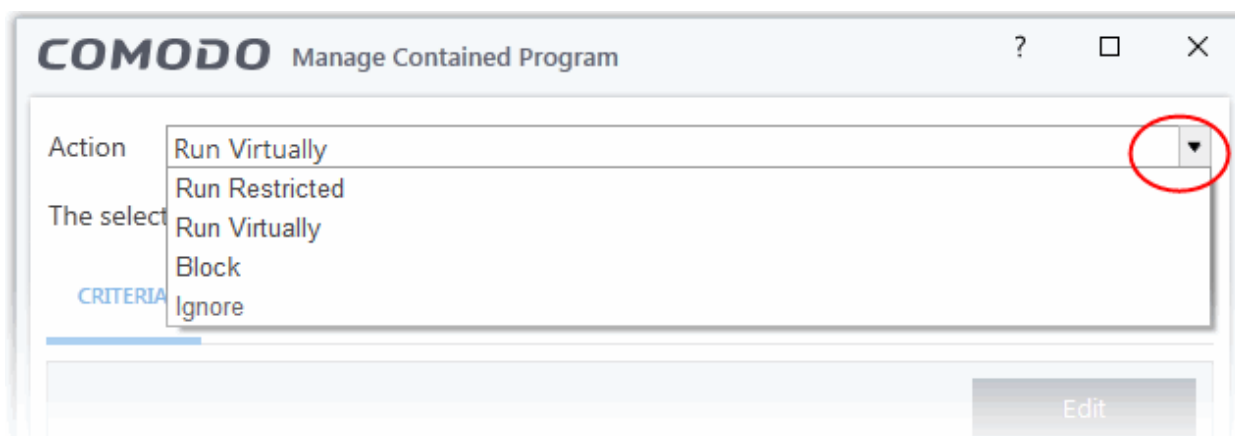
The options available under the 'Action' drop-down are:

- **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

- The next step is to select the target files and configure filters.
- You can filter a rule so it applies to specific types of file.
    - For example, you can specify 'All executables' as the target, then add a filter so it only affects executables 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, then add 'Files created by a specific user' as the filter.

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
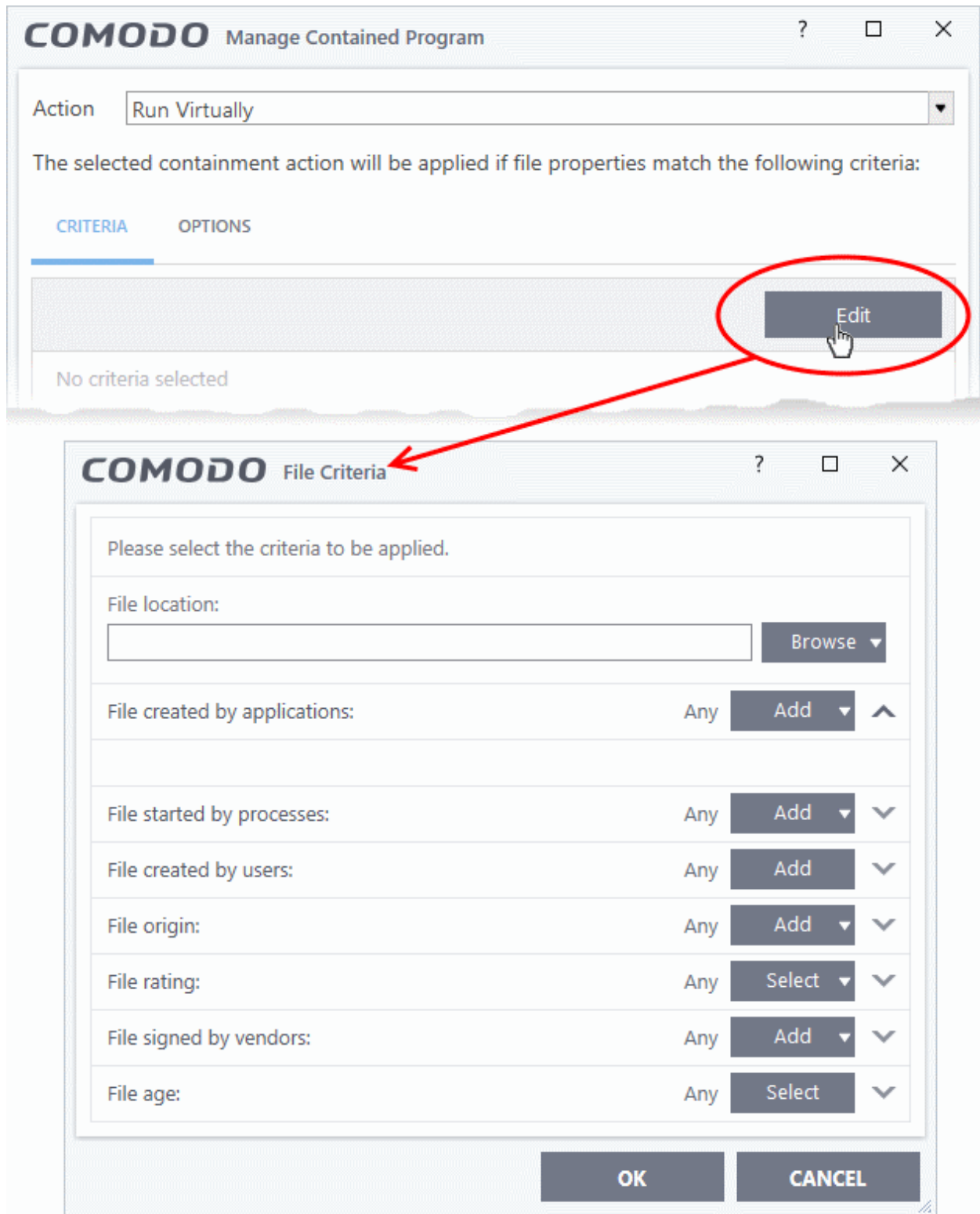
The 'File Criteria' dialog will open. The file criteria dialog allows you:

- **Select the target**
- **Configure the filter criteria**

Select the target

- To select the target, click the 'Browse' button beside the 'File Location' field
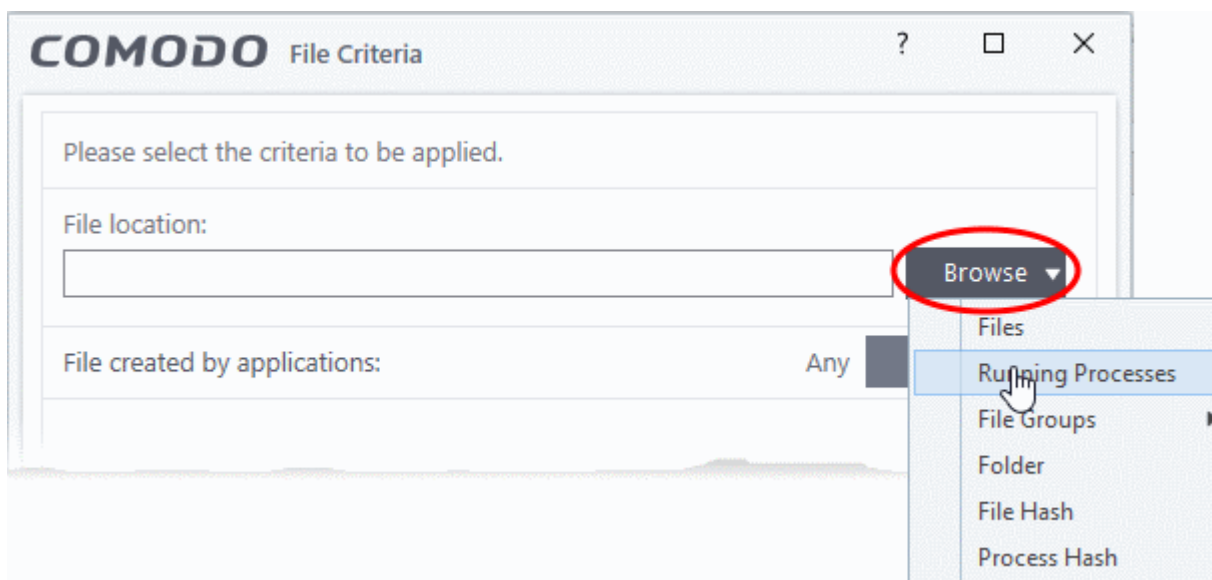
There are six types of target you can add:

- **Files** - Apply the rule to specific files.
- **Running Processes** - Apply the rule to a process that is currently running on your computer.
- **File Groups** - Apply the rule to predefined file groups. See **File Groups** for help to add or modify a file group.
- **Folder** - Apply the rule to a folder or drive.
- **File Hash** - Create a hash value from a file and use it as the rule target. A hash value is a large number which is generated by passing the file through a hashing algorithm. The number uniquely identifies and represents the file, and it is extremely unlikely that two files will ever generate the same hash value. The benefit of using a file hash is that the rule will still work even if the file name changes.
- **Process Hash** - Create a hash value of a process and use it as the rule target. Please see description above if required.

Add an individual File

- Choose 'Files' from the 'Browse' drop-down.

- 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**.
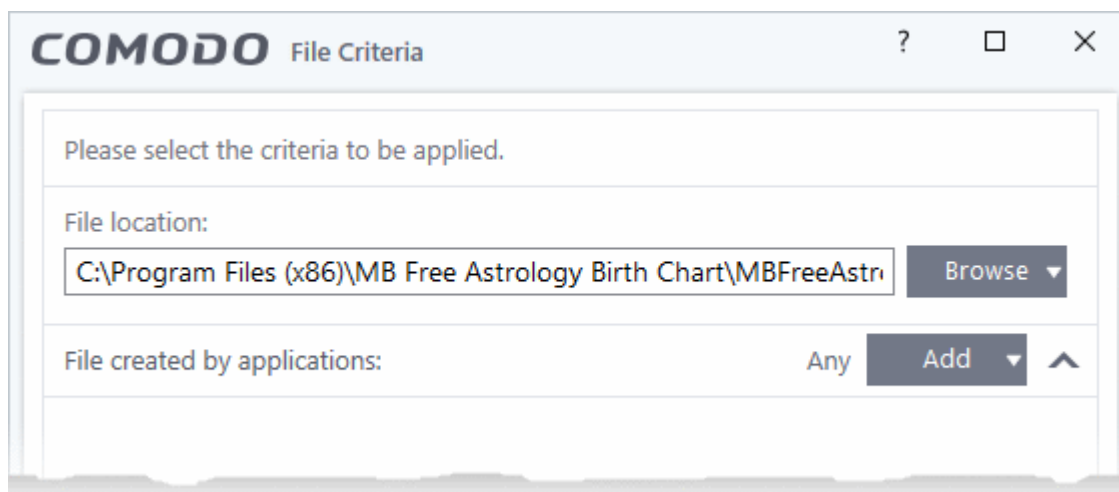
- Click 'OK', if you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options.

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.

Add a currently running application by choosing its process

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

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 parent application of the process is added as target and run as per the action chosen in **Step 1**.
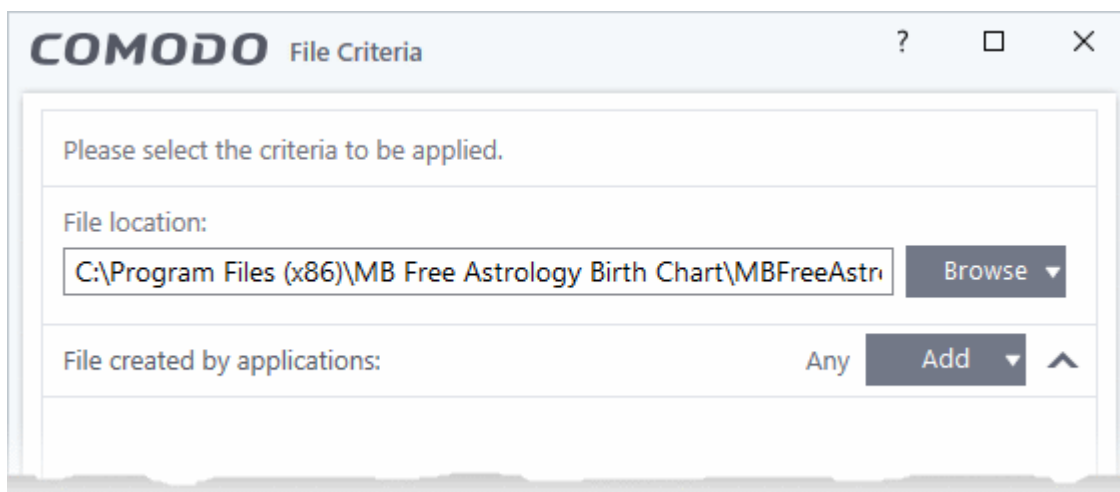
- Click 'OK', if you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options.

- 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.

Add 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'. See **File Groups**, for more details on viewing and managing pre-defined and user-defined file groups

---
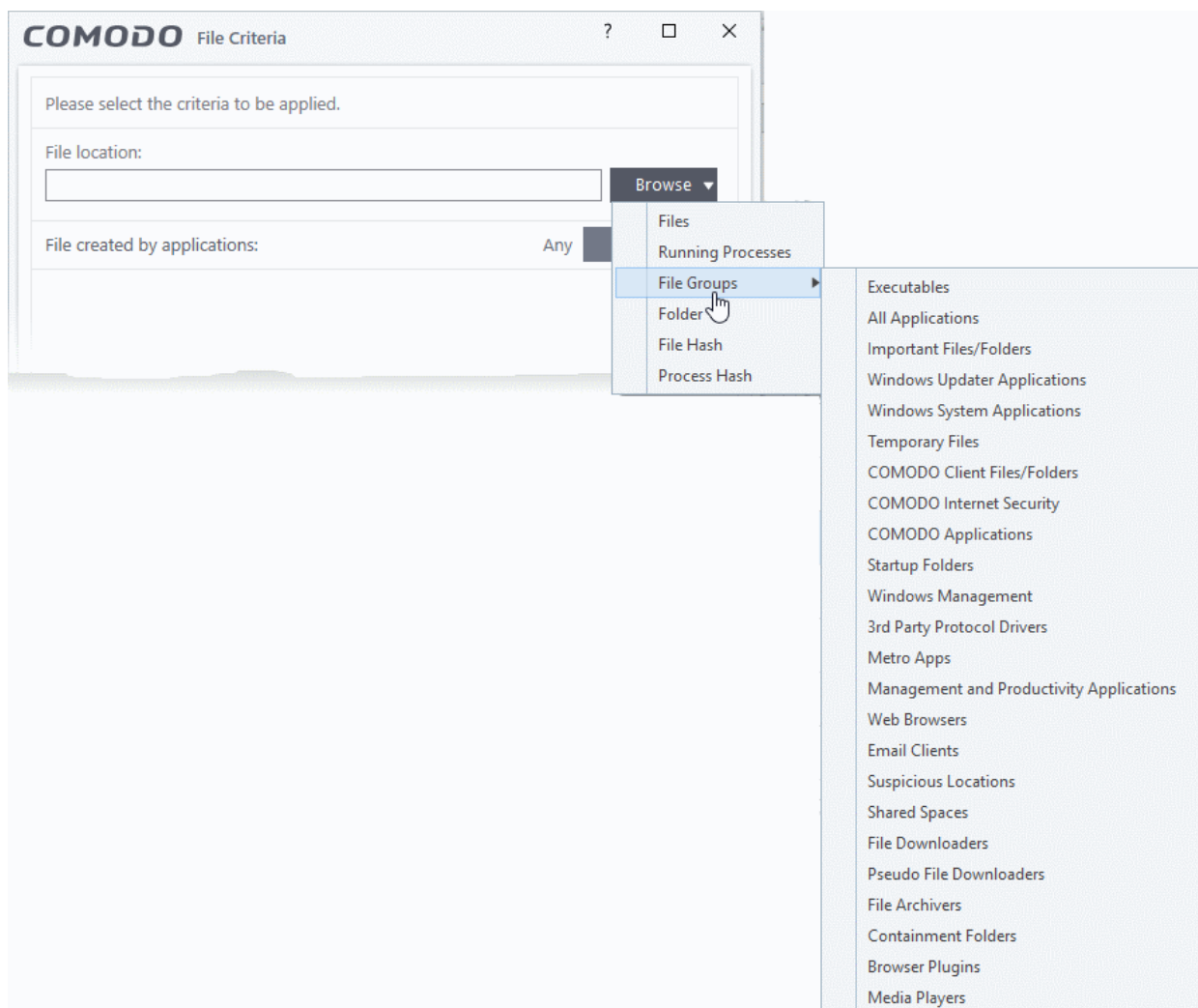
- Select the file group from the drop-down.

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.

Add 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**.
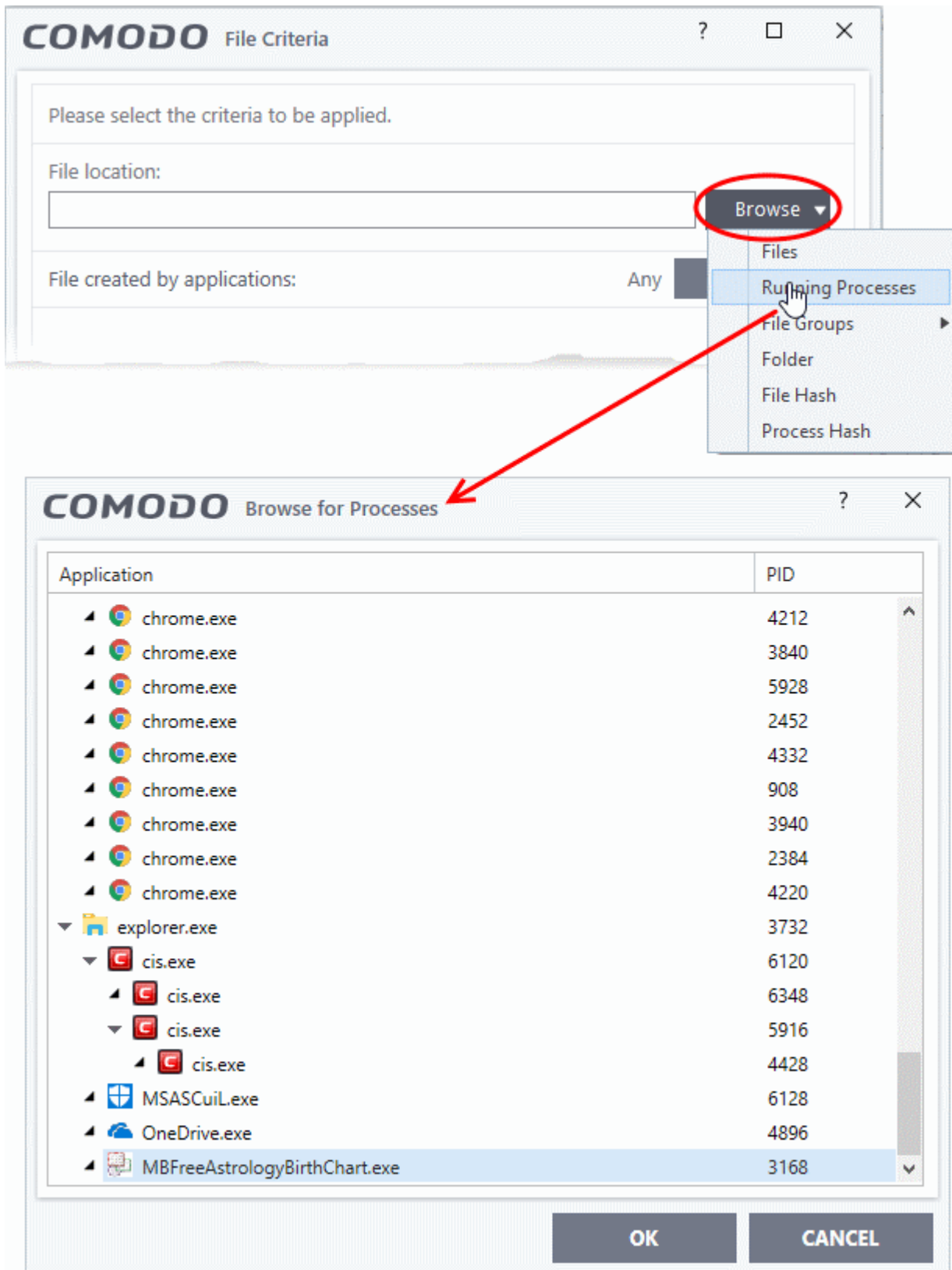
- Click 'OK', if you want to just add the applications for a particular action as selected in **Step 1** without specifying any filters or options.

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.

Add 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'
- 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.

- If required you can **configure filter criteria and file rating** and **options** for the rule.

- CIS generates the hash value of the parent file and stores that as the target.

- CIS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

Add an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.
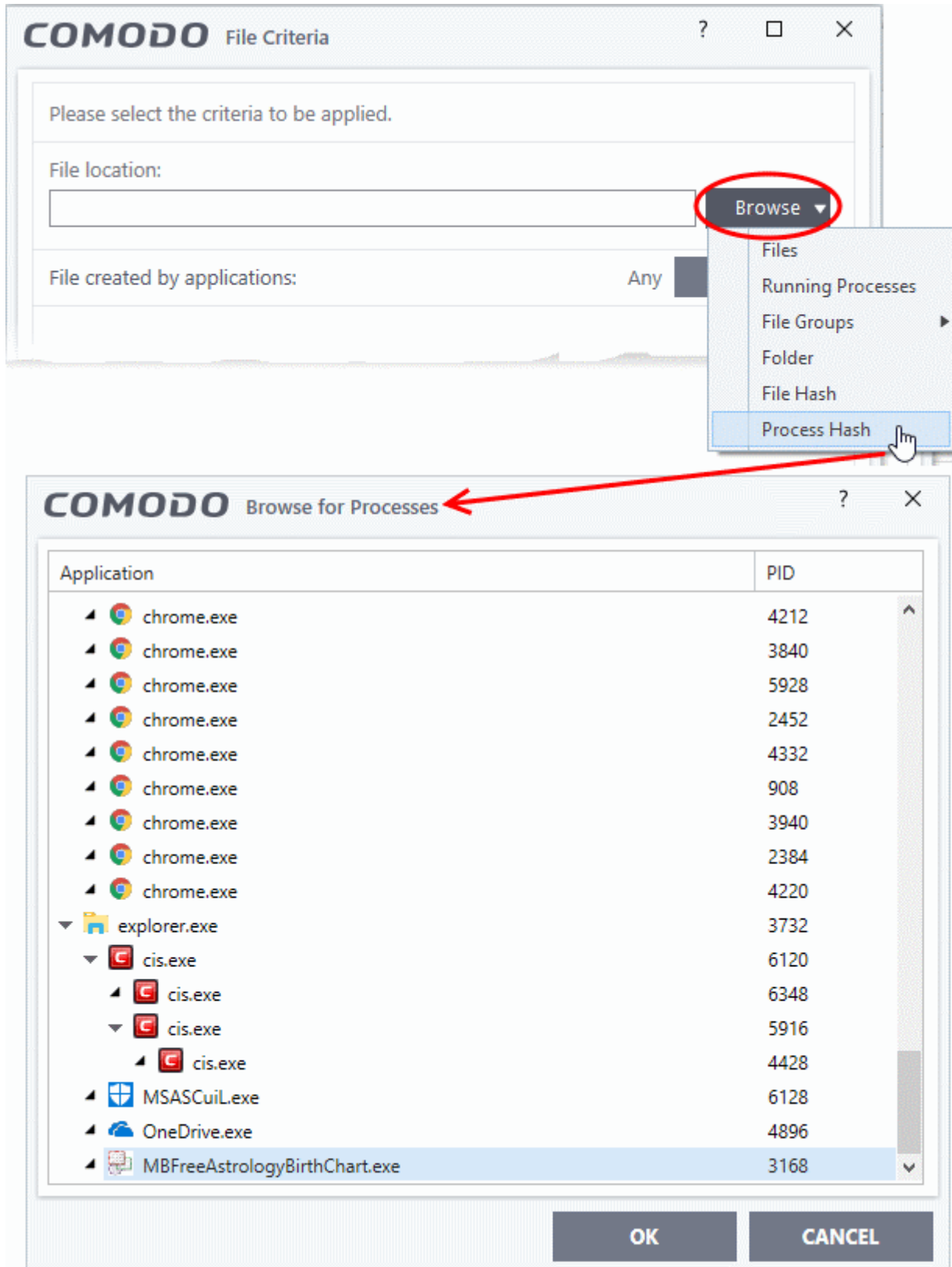
A list of currently running processes in your computer is shown.

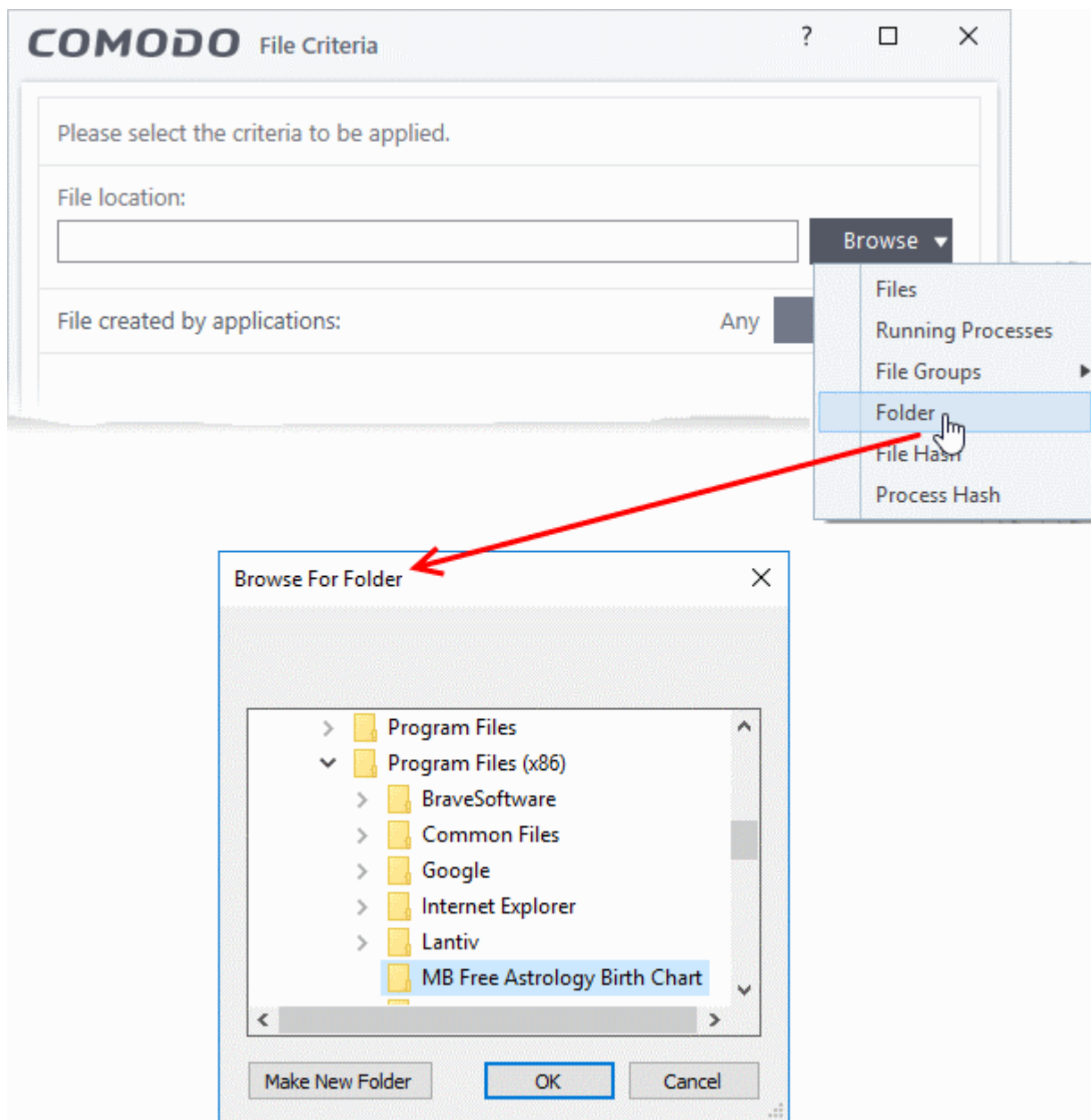- Select the process, to add the hash value of its parent application as the target and click 'OK'
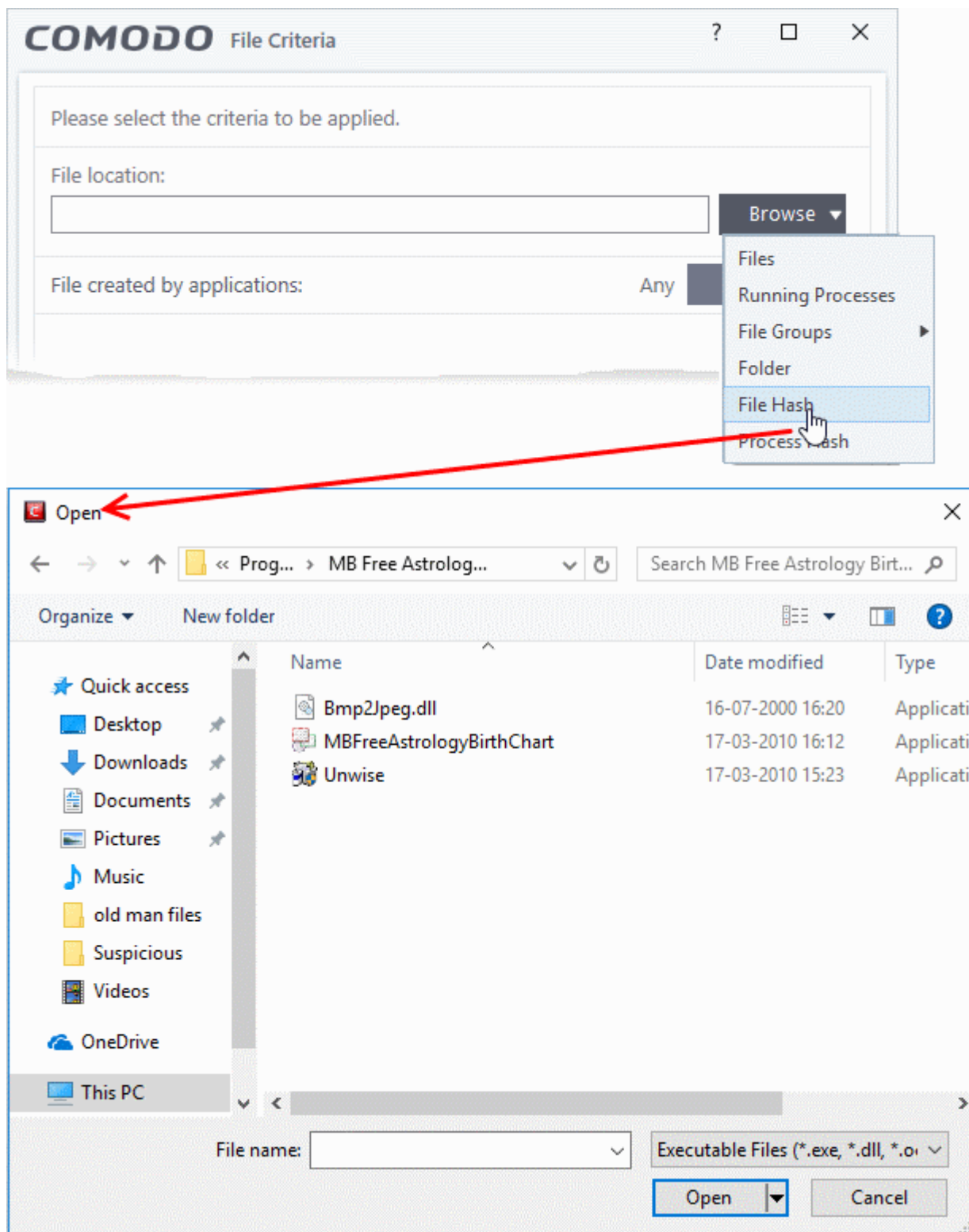- Click 'OK', if you want to just add the application for a particular action as selected in Step 1 without specifying any filters or options.
- If required you can **configure filter criteria and file rating** and **options** for the rule.
- CIS generates the hash value of the parent file and stores that as the target.
- CIS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the process name changes.

Configure the Filter Criteria and File Rating

You can apply an action to a file if the file meets certain criteria.

The available criteria are:

- **By application that created the file**
- **By process that created the file**
- **By user that created the file**
- **By file origin**
- **By file rating**
- **By vendor who signed the file**
- **By file age**

Auto-contain a file if it was created by a specific application

- You can create a filter to apply an action to a file based on its source application.
- You can also specify the file rating of the source application. The rule will then only contain a file if its parent app has a certain trust rating.

To specify source application(s)

- Click the 'Add' button in the 'File Created by applications' stripe.
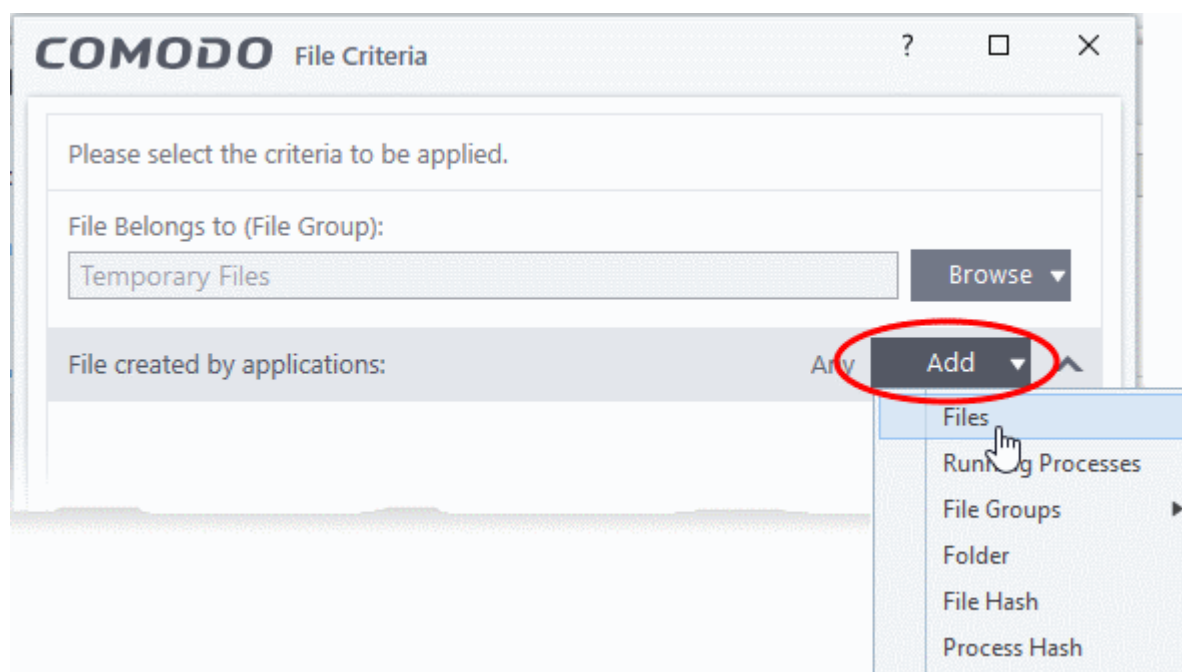
- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.

The selected source application, file group or the folder will be added.

- Click the 'Any' link beside 'File Rating' and select the file rating of the source
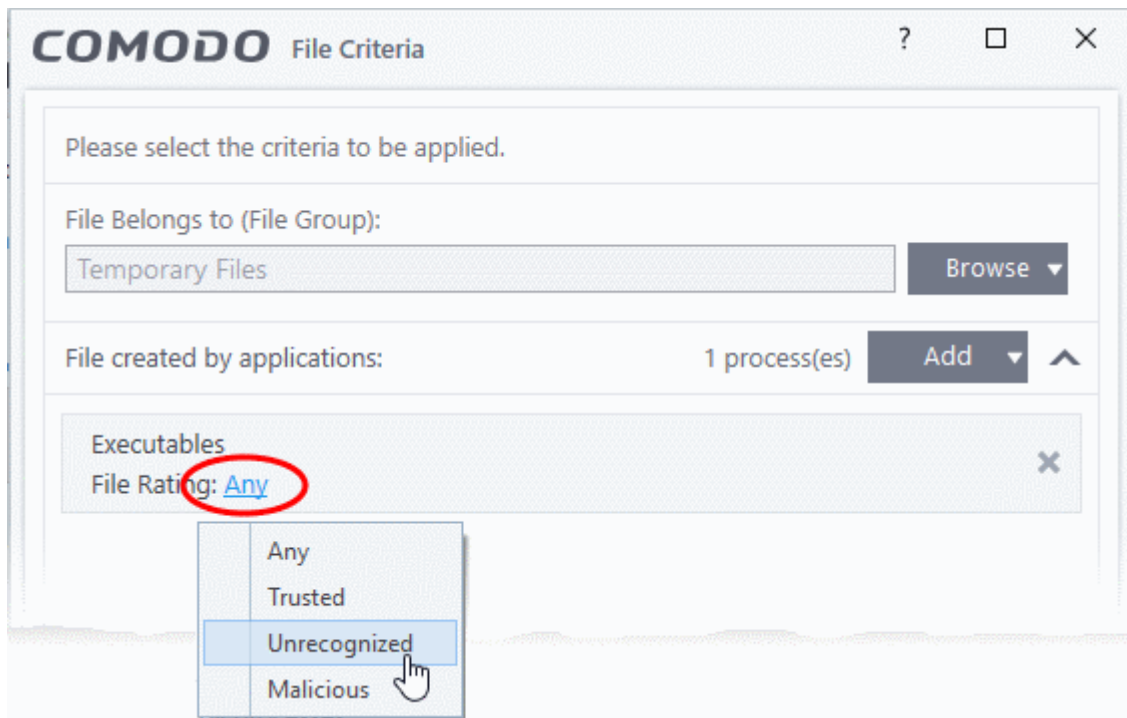
- Repeat the process to add more applications or groups/folders.

Auto-contain a file if it was created by a specific process

- You can create a filter to apply an action to a file based on its parent process.
- Optionally, you can also specify:
  - The file rating of the source. The rule will then only contain a file if its parent process has a certain trust rating.
  - The number of levels in the process chain that should be inspected.

To specify source process(es)

- Click the 'Add' button in the 'File Created by Process(es)' stripe.
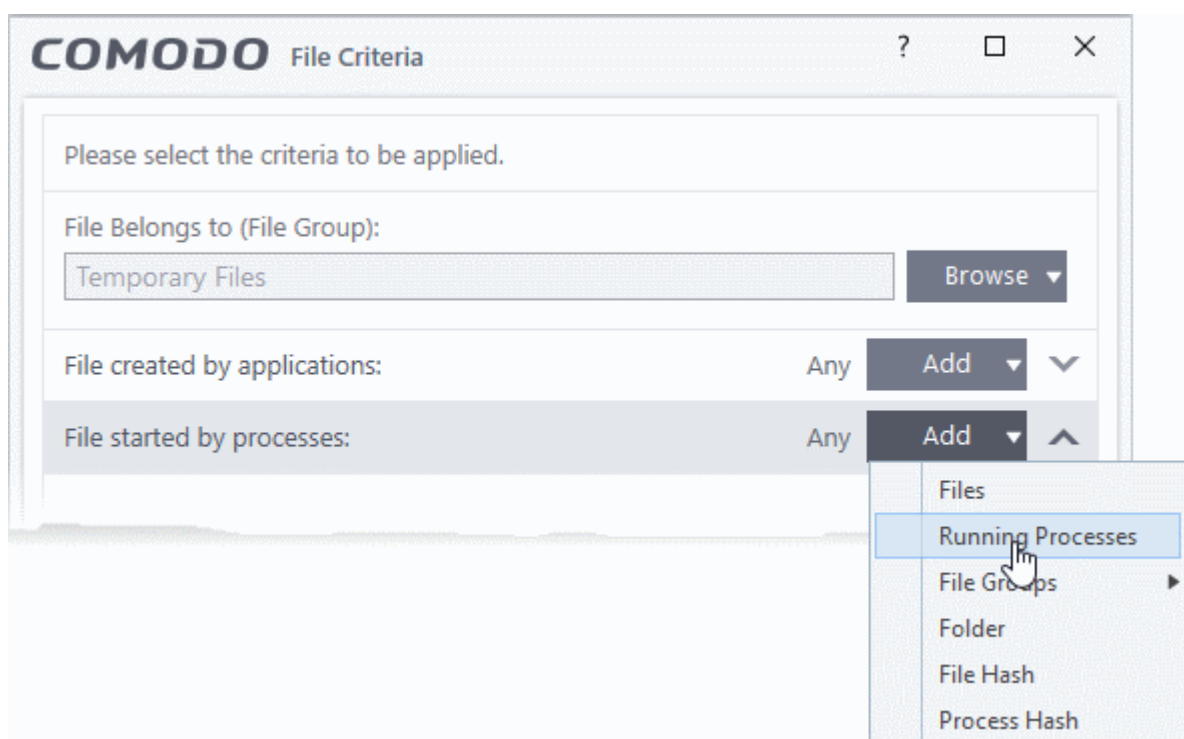
- The options available are same as those available under the 'Browse' button beside 'Target', as explained **above**.

- The selected source application, file group or the folder will be added. The file created / invoked by the process, started by the selected source will be added as the target for the rule.

- Click the 'Any' link beside 'File Rating' and select the file rating of the source
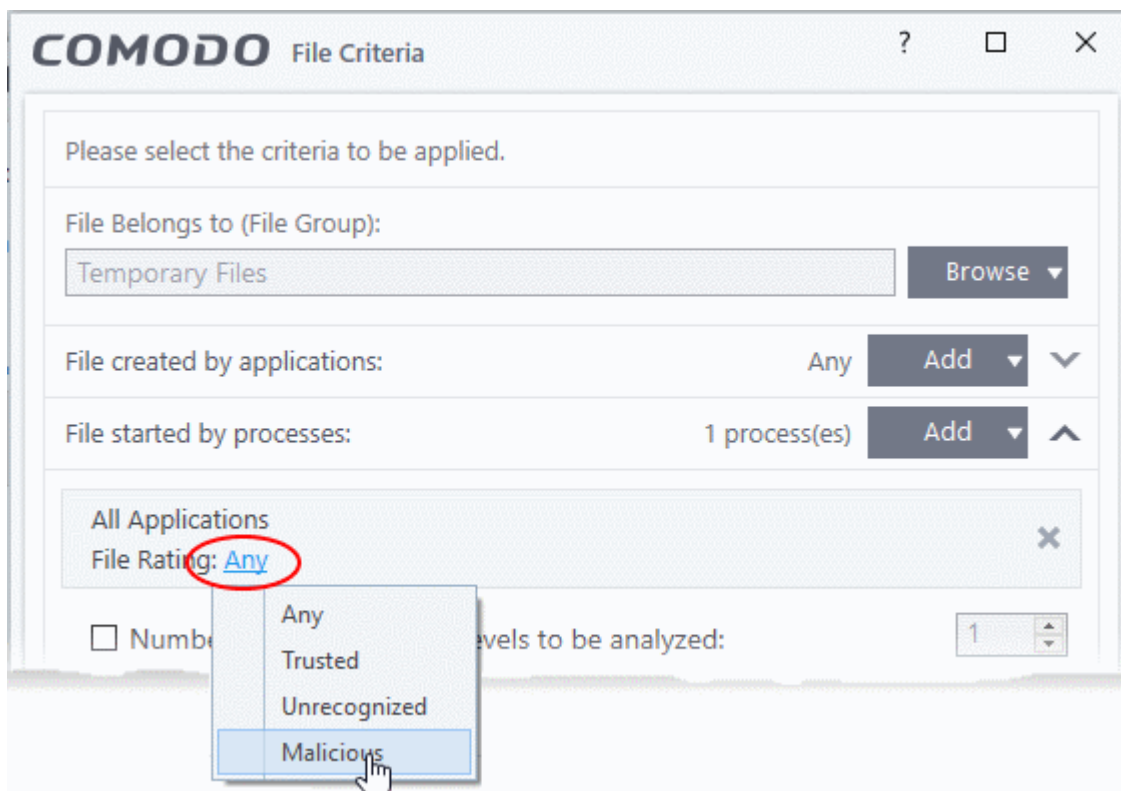
- '**Number of parent process levels to be analyzed**' - Specify how far up the process tree CIS should check when inspecting the file's sources. 1 = will only check the file's parent process. 2 = will check the parent process and the grand-parent process, etc., etc.
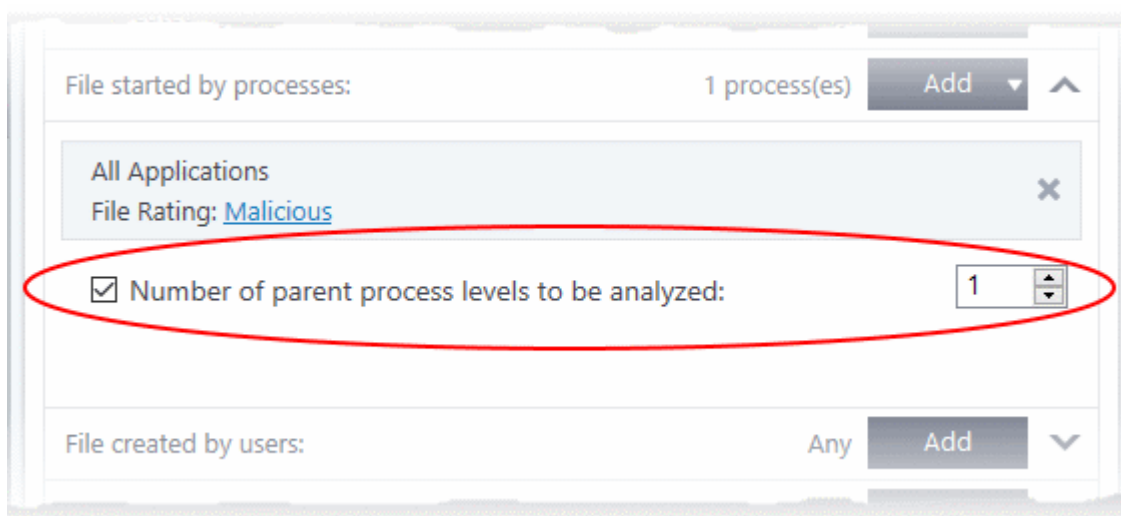
- Repeat the process to add more process(es)

Auto-contain a file created by specific users

- Click the 'Add' button in the 'File Created by User(s)' stripe.
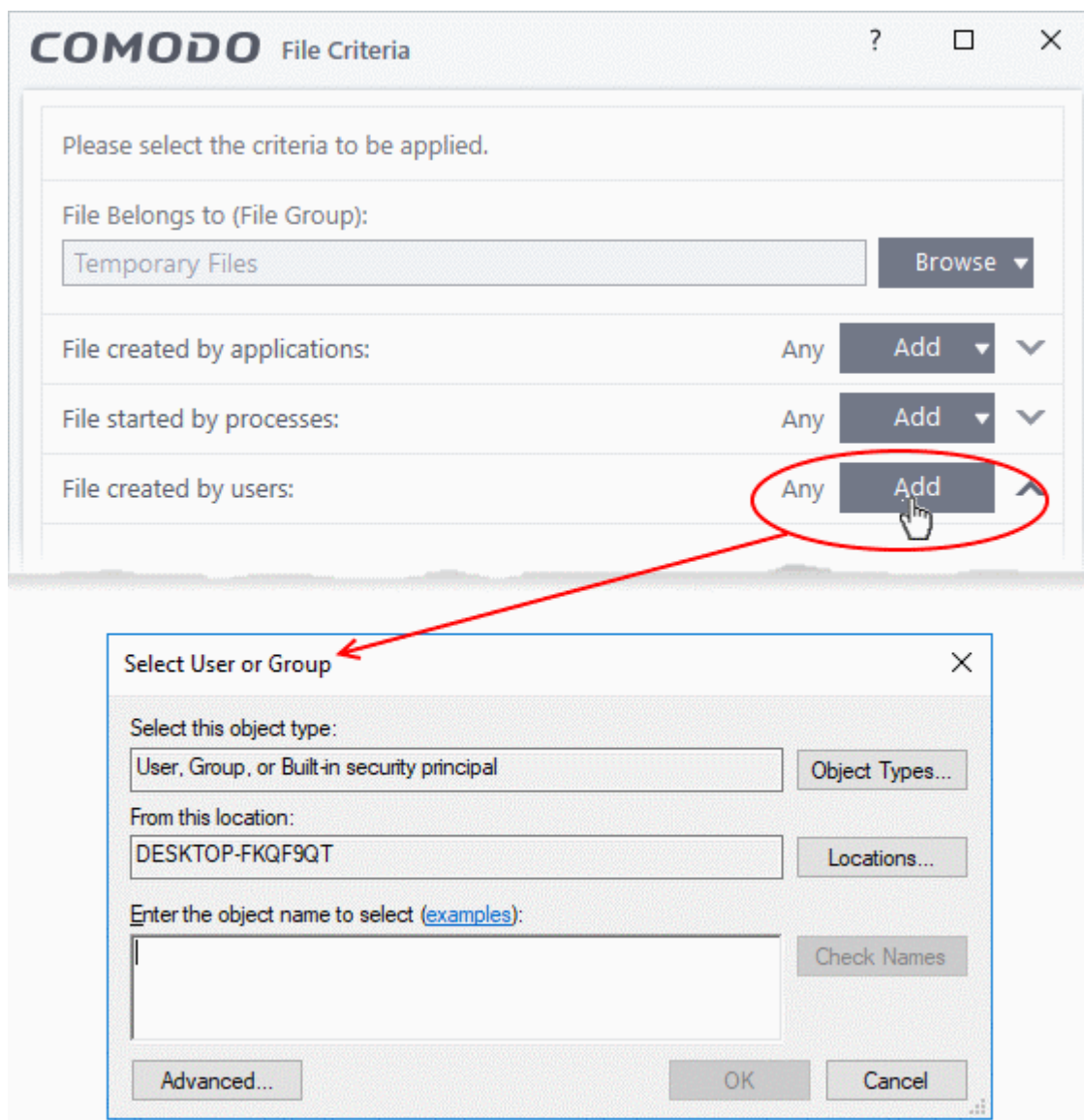
- The 'Select User or Group' dialog will appear.

    - 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.
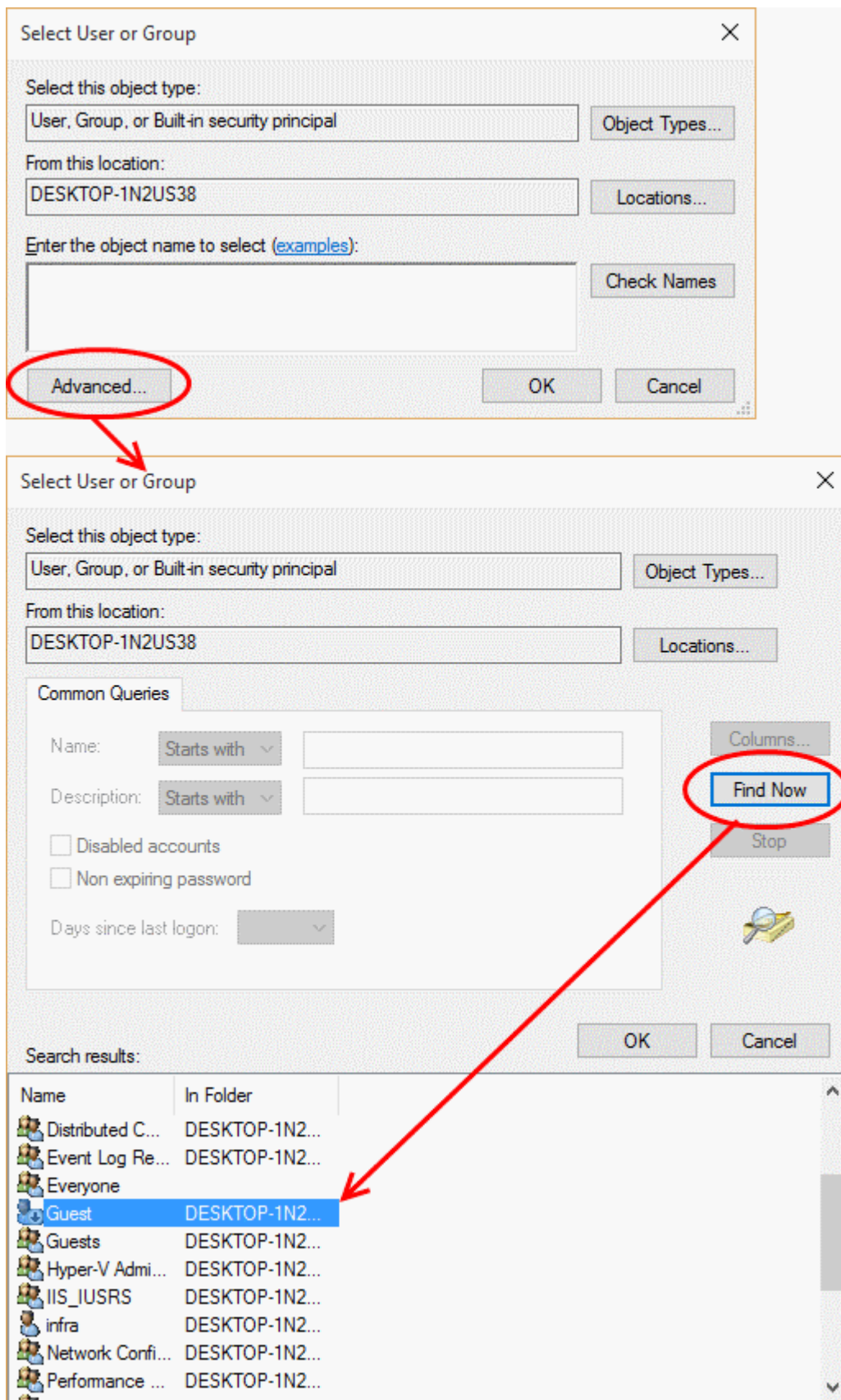
The user will be added to the list.
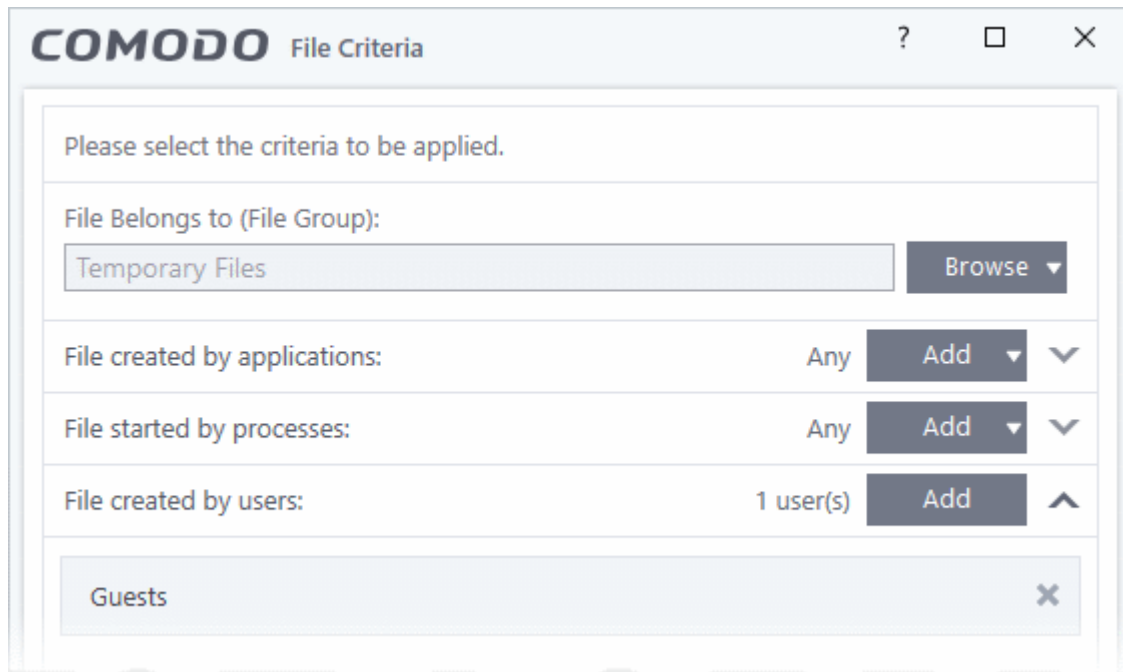
- Repeat the process for adding more users.
- To remove the user added by mistake or no longer needed in the list, click the 'X' icon at the right end of the user name.

Auto-contain a file if it was downloaded/copied from a specific source

- Click the 'Add' button in the 'File Origin' stripe.
- Choose the source from the options:
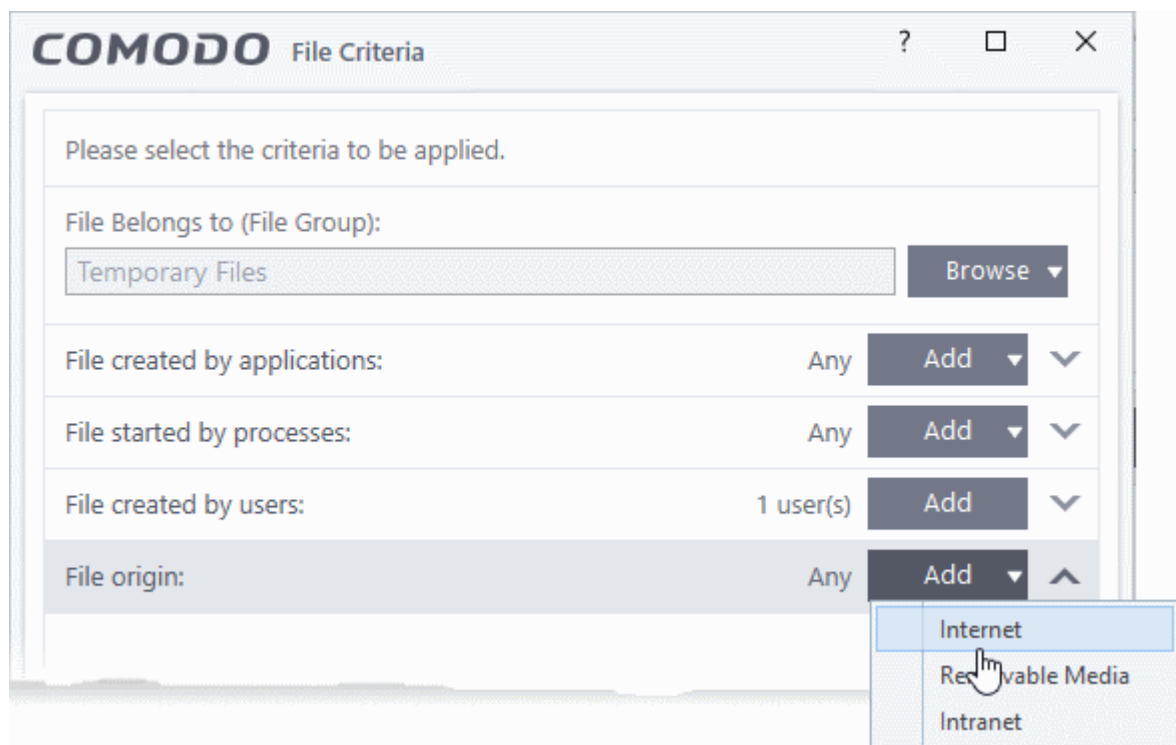
- **Internet** - The rule will only apply to files that were downloaded from the internet.
- **Removable Media** - The rule will apply only to items copied to the computer from removable storage devices like a USB drive, CD/DVD or portable hard disk drive
- **Intranet** - The rule will only apply to files that were downloaded from the local intranet.

- • Repeat the process to add more sources

Select the file rating as filter criteria
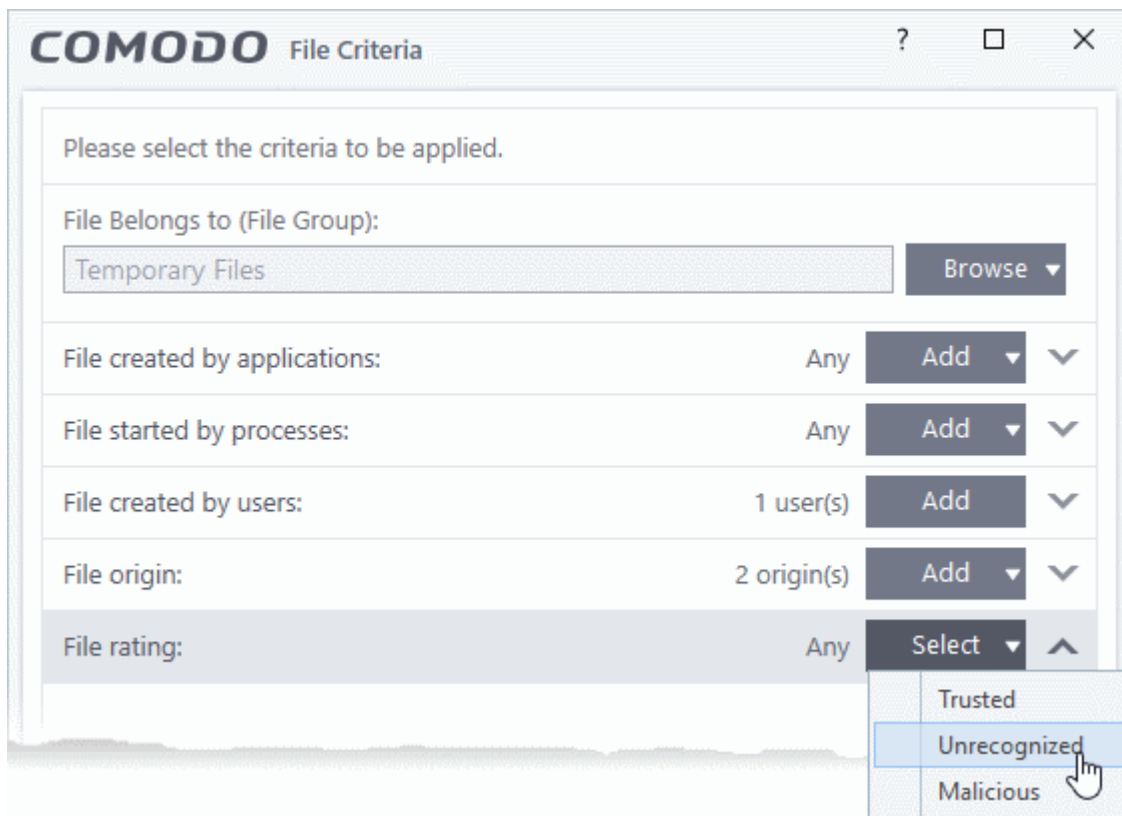
- • Click the 'Select' button in the 'File Rating' stripe

- • This will apply the rule to files which match the trust rating you set. You can choose from the following trust ratings:

  - • **Trusted** - Applications are categorized as 'Trusted' if:

    - • The file is on the global whitelist of safe files
    - • The file is signed by a trusted company in the **Vendor List**
    - • The file was installed by a trusted installer
    - • The file was given a trusted rating in the **File List** by the user

  - • See **File Rating Settings** for more information.

  - • **Unrecognized** - Files that do not have a current trust rating. The file is on neither the blacklist nor the safelist, so is given an 'unknown' trust rating. See **File List** for more information.

  - • **Malware** - Malicious files - those that are on the blacklist of known harmful files.

Auto-contain a file based on the software vendor

- • You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.

- • You can also specify the file rating of the vendor. The rule will only contain a file if its vendor has the stated trust rating.

Specify vendors:

- • Click the 'Add' button in the 'File Created by Process(es)' stripe.

- There are three ways you can add a vendor:

    1. Directly select a vendor

    - Choose 'Vendor from a Vendor List' from the drop-down
    - The 'Add Vendor' dialog opens with a list of vendors in the **Vendor List**

- Use the sort and filter options in the column headers to search for the vendor to be specified
- Choose the vendor and click 'OK'. The vendor will be added as a criterion.

2. Specify an executable file on your local drive

- Choose 'File Signer' from the drop-down
- Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
- CIS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

3. Select a currently running process

- Choose 'Running Process Signer' from the drop-down
- A list of all processes running at present on your computer is shown
- Select the process to specify the publisher of the application that started the process and click 'OK'
- CIS checks that the .exe file that started the process is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

The selected vendor is added:

- **Vendor Rating** - The rule will only apply to the vendor's files IF the vendor has this rating at the time the file is checked. Note, the rating you set here can be different to the actual vendor rating in 'Settings' > 'File Rating' > 'File List' > 'Vendor Rating'.

  - Example. If you select 'Trusted' here, then CIS will apply the rule if the vendor is trusted at the time the file is checked. If the vendor's rating changes to 'Malicious' or 'Unrecognized', then the rule isn't applied.

- Repeat the process to add more vendors

Set the file age as filter criteria

- Click the 'Select' button in the 'File age' stripe.

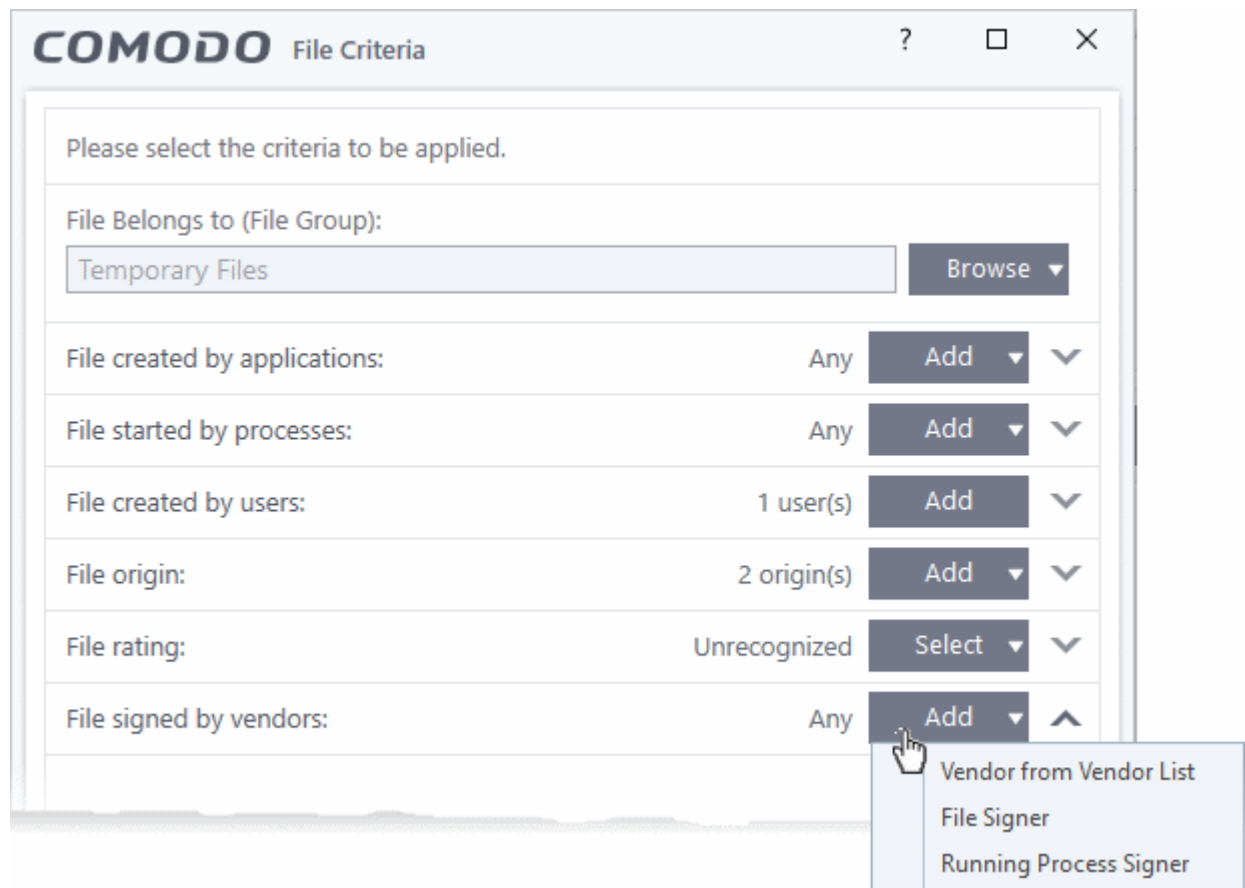The 'File Age' dialog will appear. You can set the file age in two ways:

- **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.

Step 3 - Select options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

- Click the 'Options' tab.

The options available depend on the 'Action' chosen in **Step 1**.

The '**Ignore**' action has the following options:

- **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 those started by the target application.

    - This option is disabled by default, so the ignore rule also applies to child processes.

    - If enabled, the ignore rule does not apply to child processes. Each child process will be inspected individually and all relevant rules applied.

The '**Run Restricted**' and '**Run Virtually**' actions have the following options:

- **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 '**Block**' action has the following options:

- **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.
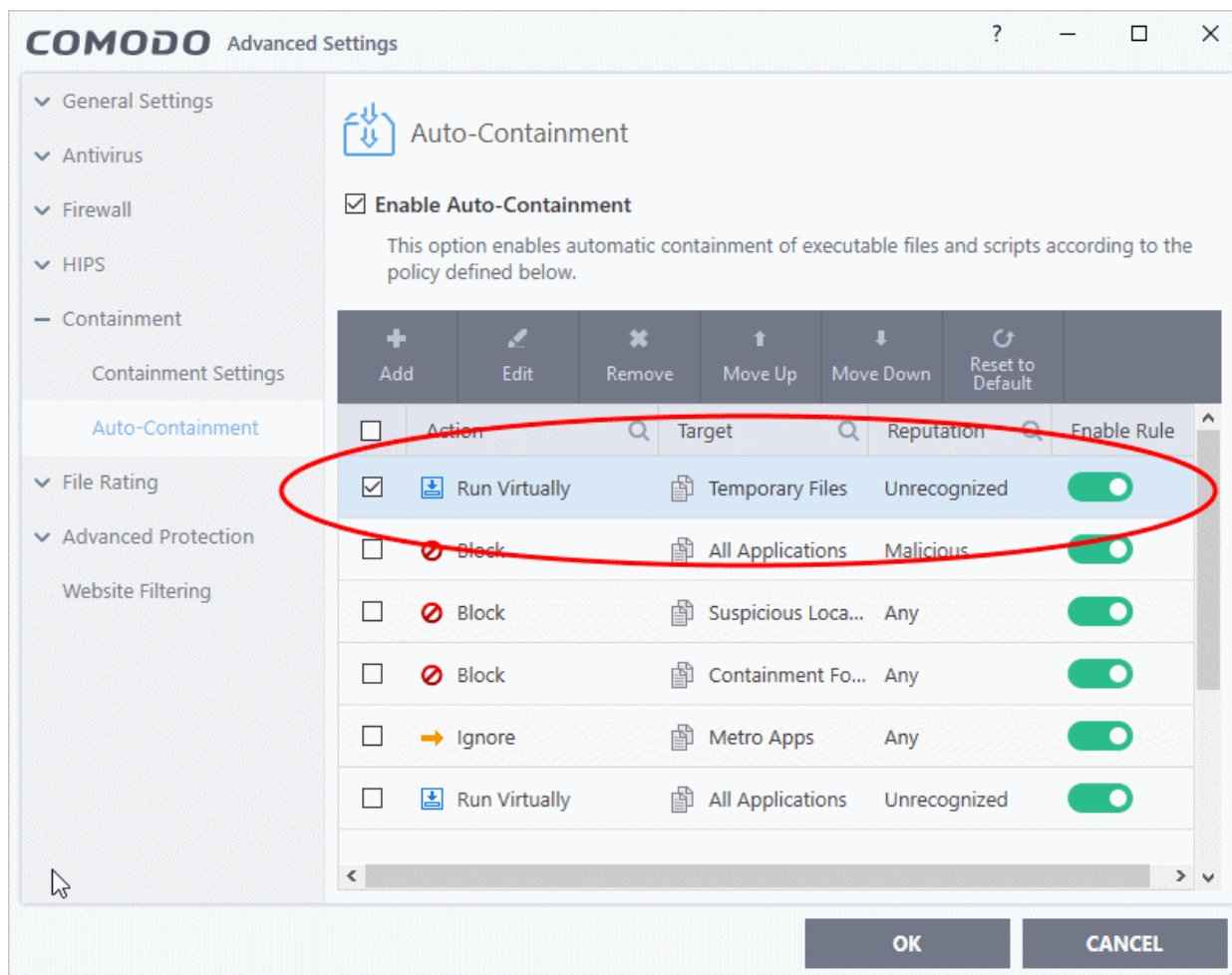
You can move the rule up or down the list to change its priority.

Edit an Auto-Containment Rule

- Select a rule from the list in the Auto-Containment panel and click 'Edit' from the top.
- The edit procedure is similar to a**dding an auto- containment Rule**.
- Click 'OK' to save the rule changes.

Important Note: Please make sure auto-containment rules do not conflict. In the event of a conflict, the setting in the rule that is higher in the list prevails. The 'Reset to Default' button lets you restore the original rules.

6.5.3. 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.

6.5.4. 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.
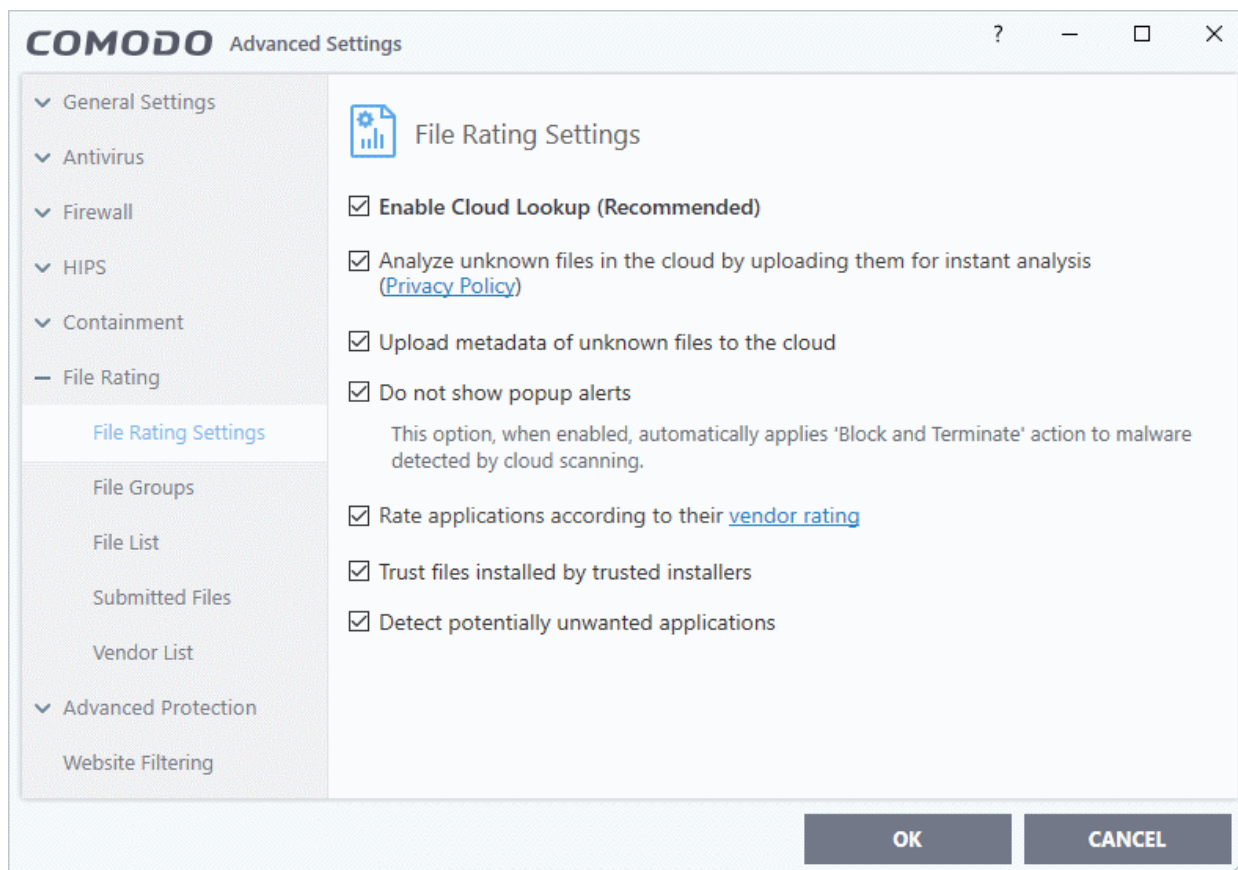
6.6. File Rating Configuration

Click 'Settings' > 'File Rating' to open the section

- The file rating area lets you view and manage all trusted, malicious and unrecognized files.
- File ratings in CIS are obtained from our online file look-up service (FLS). This is a huge database of trust ratings of known files.
- When a file is first opened, CIS will consult the FLS to check the file's reputation on our global whitelist and blacklists.
- CIS will award 'Trusted' status to the file if:
  - The application is on our global whitelist of safe files.
  - The application has a 'Trusted' status in the CIS **File List**
  - The application is from a vendor rated as 'Trusted' in the **Vendor List**
- Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource use.
- Conversely, files which are on the blacklist of harmful files are given a status of 'Malicious'. These files are quarantined or deleted automatically.
- Files which are on neither the blacklist nor the whitelist are awarded 'Unrecognized' status.
- You can review unrecognized files in the **File List** interface ('Settings' > 'File Rating' > 'File List').
- You can also submit unknown files to Comodo for further analysis, or to run an on-demand file-lookup.

The 'File Rating' area lets you:

- • Manually add files to the file list and assign them a rating.
- • Submit unrecognized files for a file look-up, and view all files you have submitted previously.
- • View and manage the vendor list, and assign trust ratings to vendors.
- • Click 'Settings' on the CIS home-screen
- • Click 'File Rating':

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.
- • **Vendor List** - View and manage the list of software publishers. Manually add vendors and assign trust ratings to them.

6.6.1. File Rating Settings

Click 'Settings' > 'File Rating' > 'File Rating Settings'

- • A file rating determines how CIS interacts with a file:
  - • 'Trusted' files are safe to run.
  - • 'Untrusted' files are malware so they get quarantined or deleted.
  - • 'Unknown' files are run in the container until they get rated as trusted or untrusted.
- • The rating of a file can change over time, especially in the case of 'unknown' files. For example, an 'unknown' file might be re-classified as 'trusted' or 'untrusted' after it has been tested.
- • You can also configure whether CIS should auto-upload unknown files to Comodo for analysis.

Open the file rating settings interface

- Click 'Settings' on the CIS home screen.
- Click 'File Rating' > 'File Rating Settings':
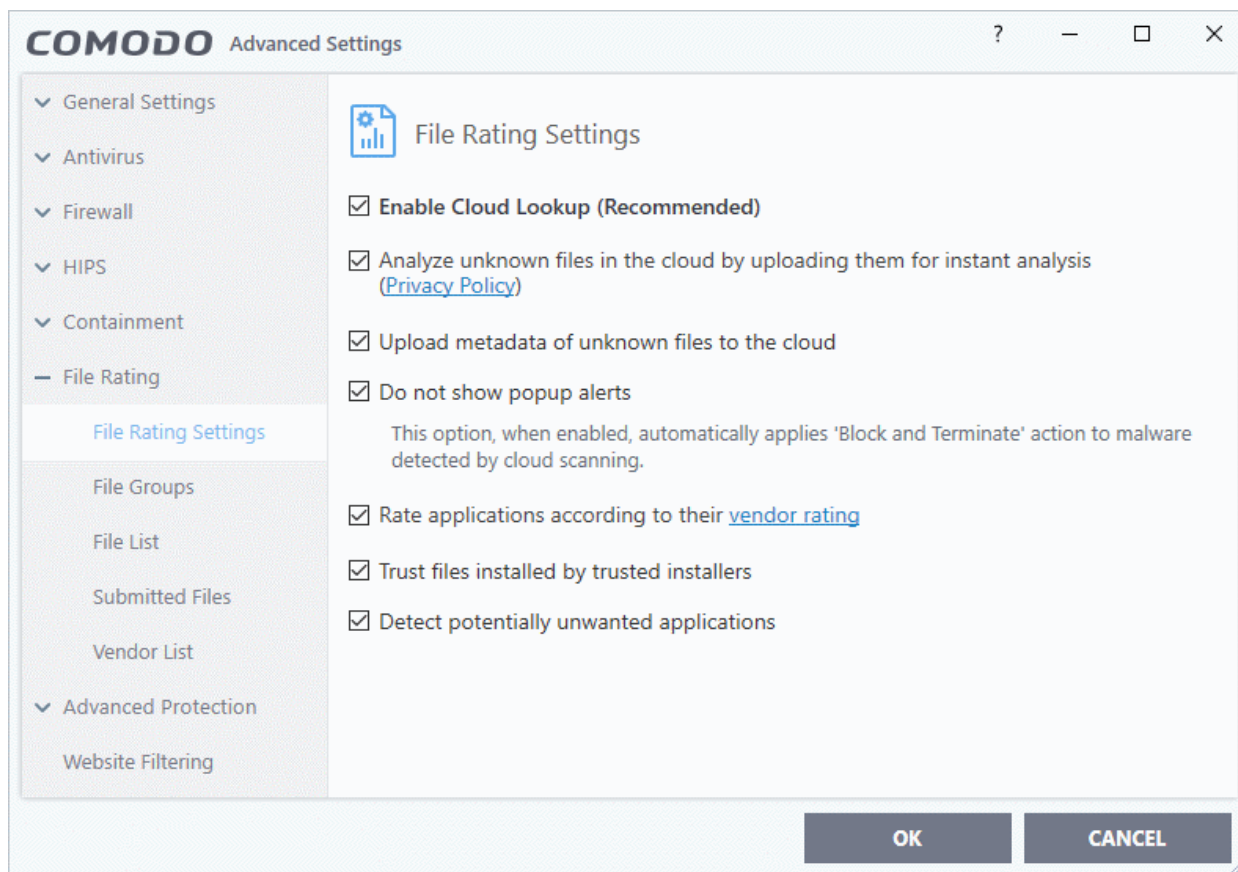
- **Enable Cloud Lookup** - CIS checks a file's trust rating on our cloud severs as part of the real-time scan process. **(Default and recommended = Enabled)**

- **Analyze unknown files in the cloud by uploading them for instant analysis** - CIS uploads files with an 'unknown' trust rating to Comodo for further analysis. Our experts will analyze the file, award it a trust rating, and add it to the global whitelist or blacklist as appropriate. **(Default = Enabled)**

- **Upload metadata of unknown files to the cloud** - Metadata is basic file information such as file source, author, date of creation and so on. If enabled, CIS will also send the file metadata when uploading unknown files to Comodo **(Default =Enabled)**

- **Do not show popup alerts** - Whether or not CIS should show an alert when an unrecognized or malicious file is detected by the cloud scanner (FLS). (**Default = Enabled**)

  - **Enabled** - No alerts are shown. This minimizes disturbances but at some loss of user awareness.

    CIS will automatically take the following actions based on the file trust rating:

    - **Unrecognized or Unknown files** - These are run in the container as per your auto-containment rules. See **Auto-Containment Rules** for more details.

    - **Malicious files** - Automatically blocked and quarantined.

  - **Disabled** - A containment alert is shown for unknown and malicious files.

    - **Unrecognized or Unknown files** - The following alert is shown:
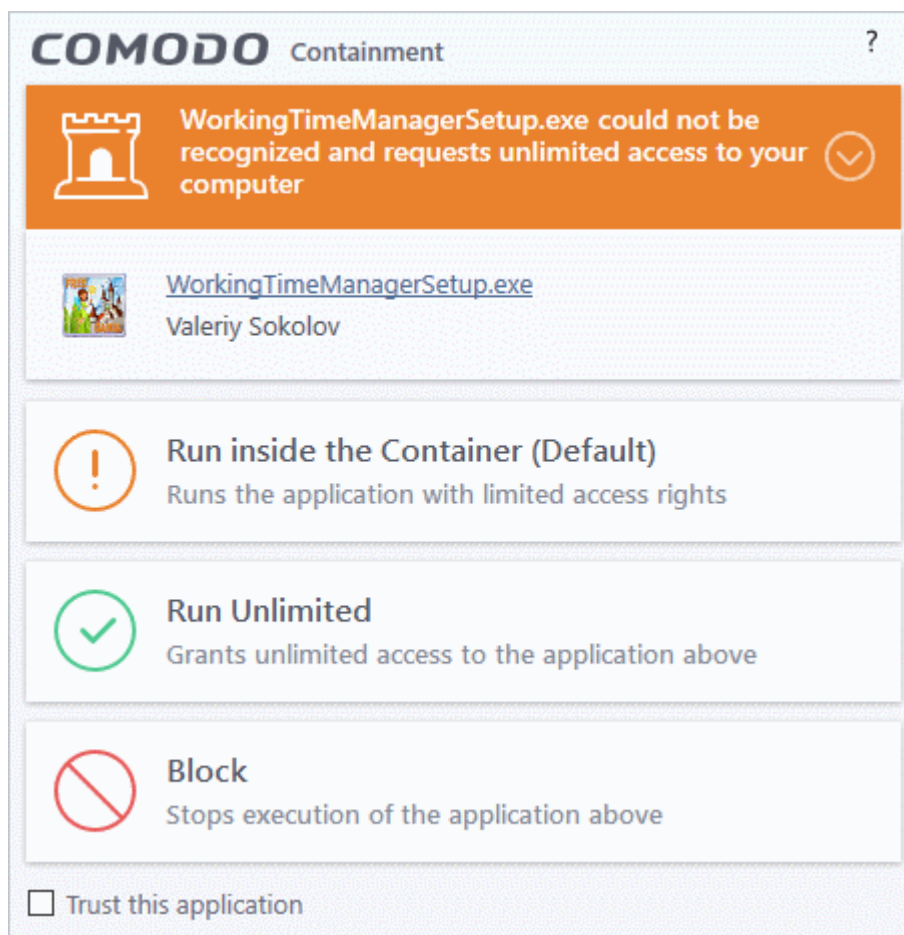
You can choose from these actions:

- **Run inside the Container** - Executes the program inside the container with limited access rights
- **Run Unlimited** - Lets the program run as normal on your computer, outside the container. The file is added to the file list as a 'Trusted' file. See **File List** for more details.
- **Block** - The program is terminated and not allowed to run.
  - **Malicious files** - The program is automatically blocked and quarantined. You will see the following type of alert:
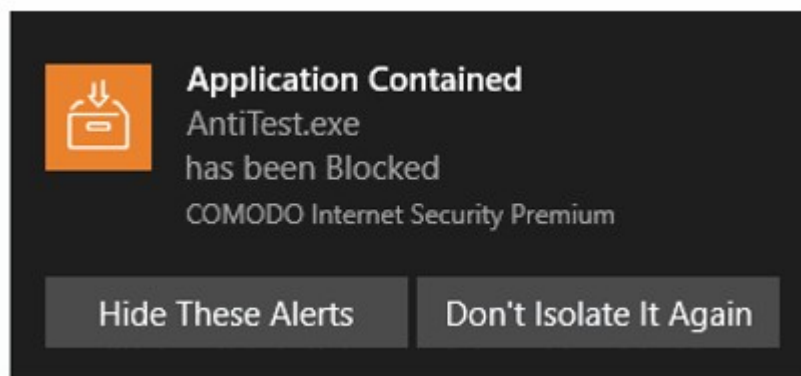
  - **Don't Isolate It Again** - Select this option if you are sure about the trustworthiness of the program / publisher.
    - The file will be assigned 'Trusted' rating in your local file list, and will be allowed to run without restriction in future. See **File List** for more details.
- **Rate applications according to their vendor rating** - CIS will give files the same rating as the trust rating of the publisher (software creator). For example - if the vendor is trusted, then all files created by the vendor will be trusted. (*Default = Enabled*)

- The vendor is the software company who created and digitally signed the file.
- You can view vendor trust ratings in 'Advanced Settings' > 'File Rating' > 'Vendor List'.
- CIS ships with a list of vendors with 'Trusted' status. You can add new vendors to the list and set your own vendor ratings as required.
- Click the 'Vendor Rating' link to open the 'Vendor List' screen. See **Vendor List** for more details.

- **Trust files installed by trusted installers** - CIS awards trusted status to files whose parent applications are listed in the 'Installer or Updater' rule in **HIPS Rules**. *(Default = Enabled)*

- **Detect potentially unwanted applications** (PUA) - Antivirus scans will flag applications that:

    (i) a user may or may not be aware is installed on their computer

    (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 that tells you the weather may also contain code that tracks your online activity. (*Default = Enabled*).
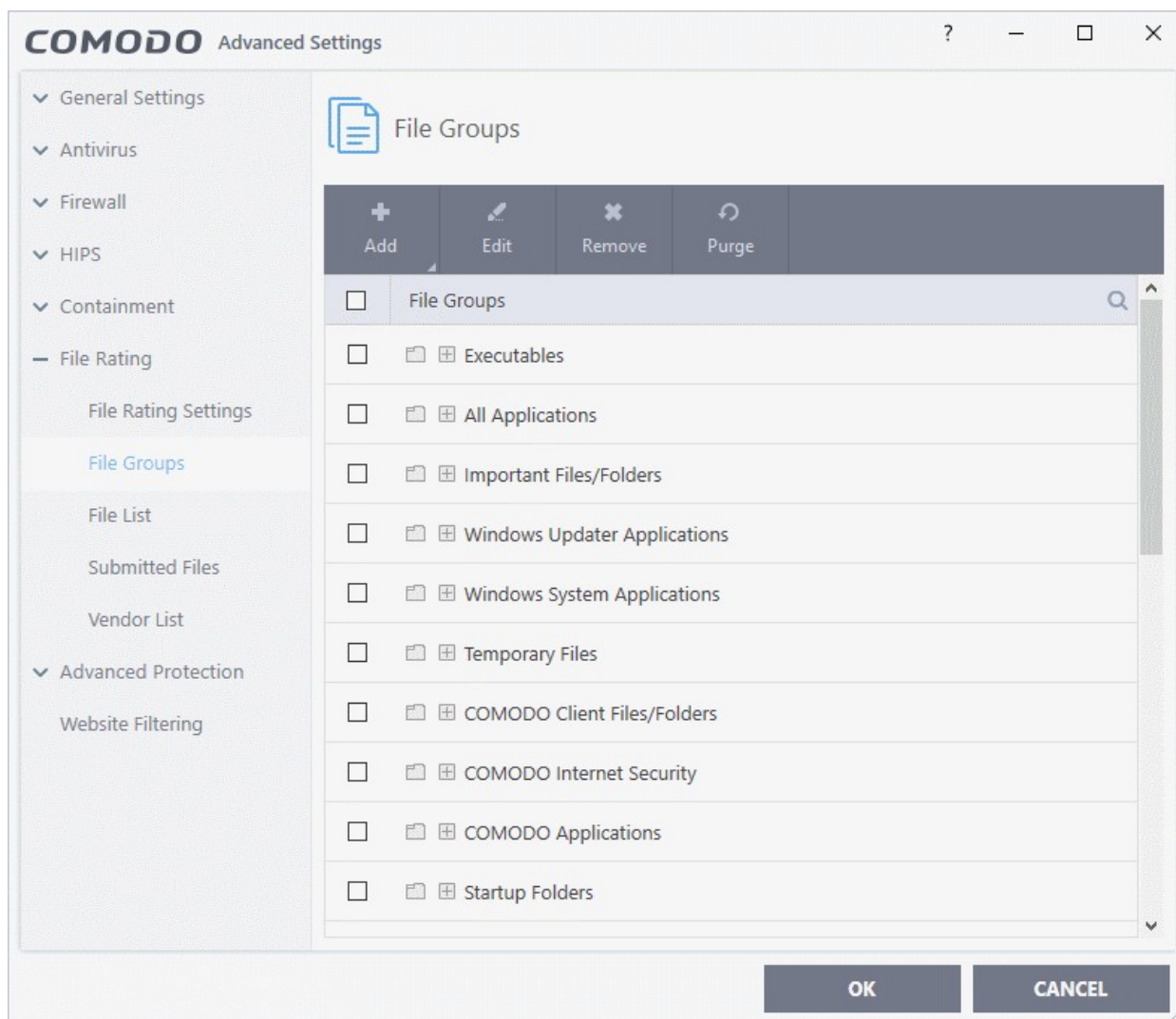
6.6.2. File Groups

Click 'Settings' > 'File Rating' > 'File Groups'

- As the name suggests, a file group is a collection of one or more file types. For example, the 'Executables' group is a list of file types that can run code on your computer.
- Once created, file groups can be named as the target of a rule in other areas of CIS. This makes 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 groups and edit existing groups as required.

Open the file groups interface

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File Groups':

Search Option:

- Click the search icon at upper-right and enter the name of a file group in full or part.

Controls:

The buttons at the top provide the following options:

- **Add** - Create a new file group. Add files, folders or running processes to an existing group.
- **Edit** - Rename a group. Change the file path of items in a file group.
- **Remove** - Delete a file group, or specific items in a group.
- **Purge** - Runs a check to verify that all files in a group are actually installed at the path specified. If not, the file or file group is removed from the list.

See the following links if you need more help:

- **Create a new File Group**
- **Edit the name of an Existing File Group**
- **Add a file to an existing file group**
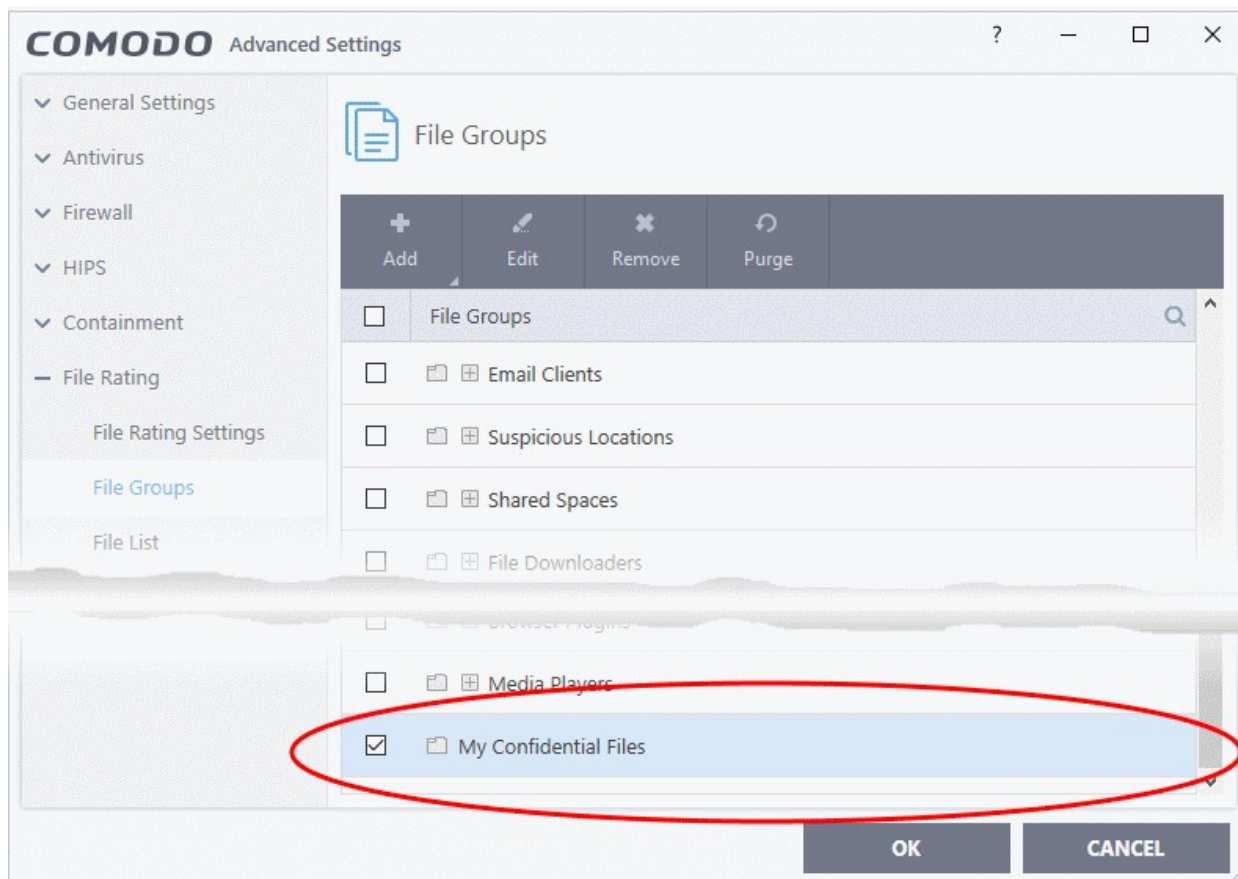- **Remove existing file group(s) or individual file(s) from existing group**

Create a File Group

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File Groups'
- Click the 'Add' button and select 'New Group':
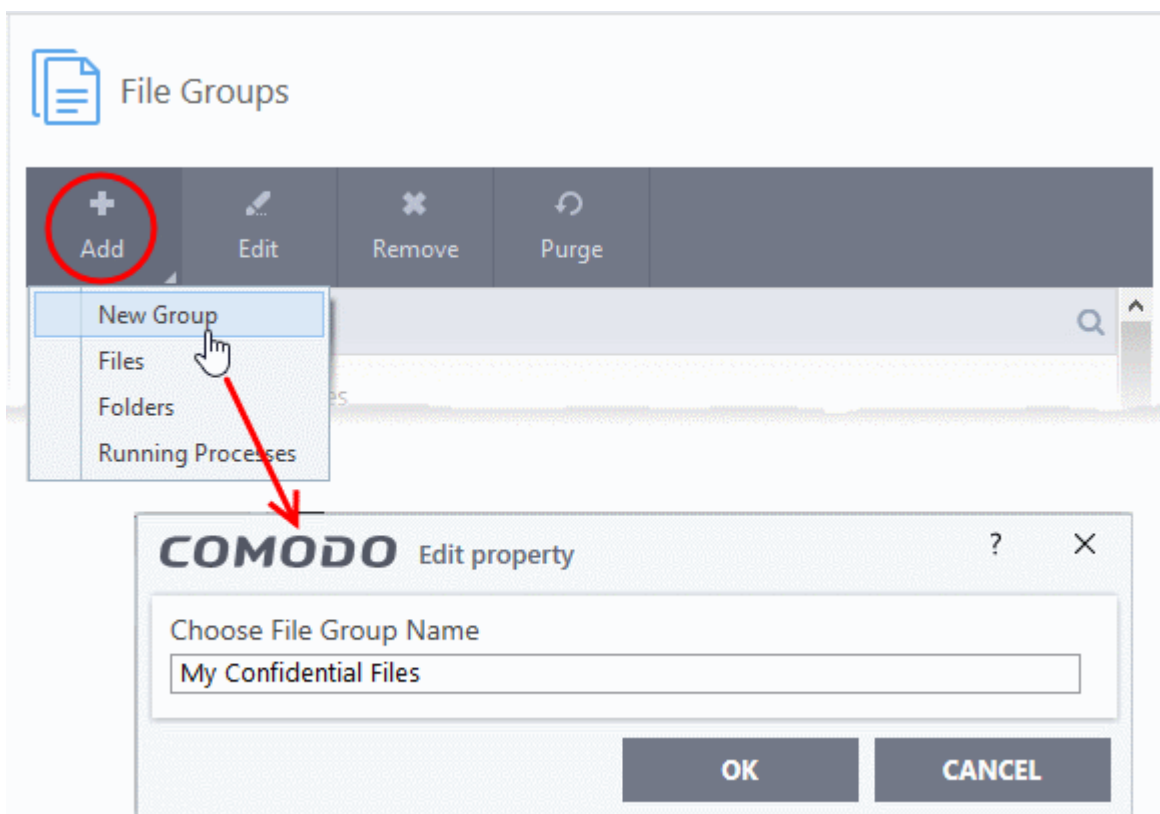
- Create a label for the file group and click 'OK'.
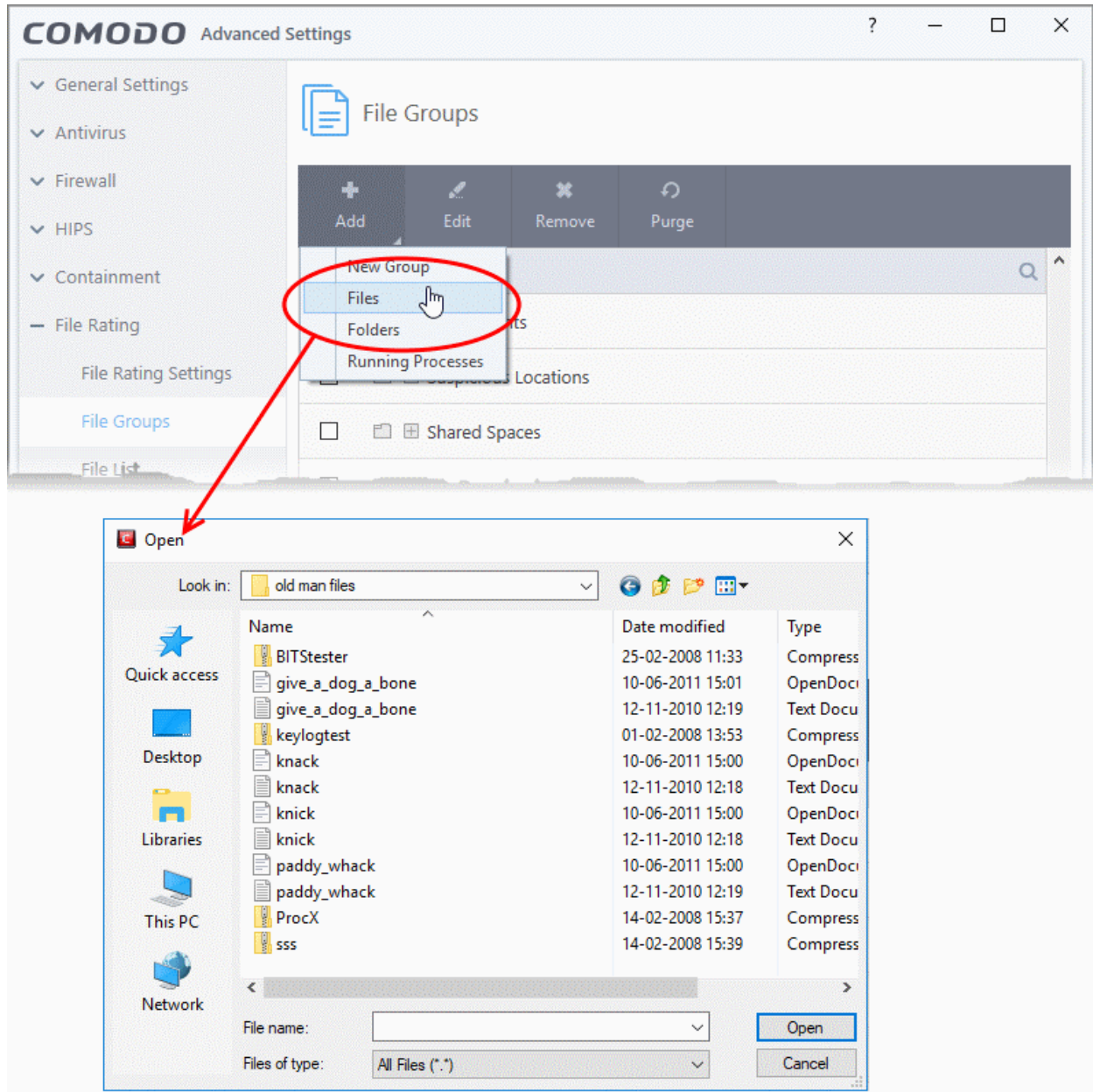
The new group will be added and shown in the list:

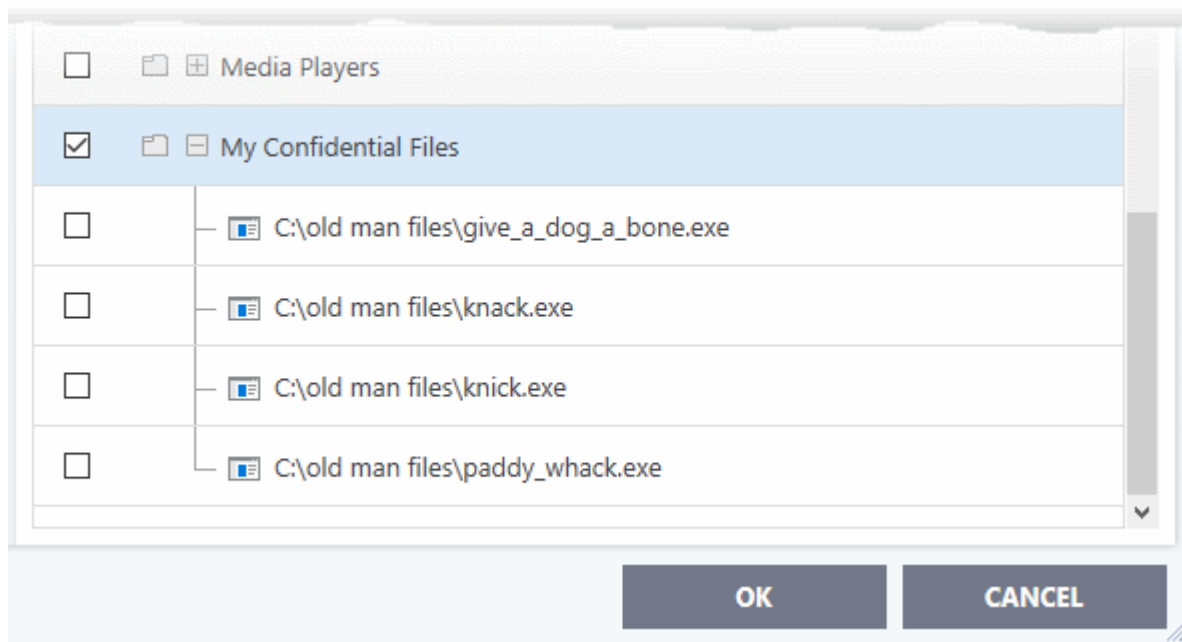**Add files or folder to a group**

- Click 'Settings' on the CIS home-screen

- Click 'File Rating' > 'File Groups'

- Select the group from the list

- Click the 'Add' button > Choose from 'Files', 'Folders' or 'Running Processes'

Add individual files or folders

- Choose 'Files' or 'Folders' from the 'Add' drop-down menu.

- Navigate to the file or folder you want to add to the group. Click 'OK'

- Repeat the process to add more files or folders.

Add an application from a running process

- Click the 'Add' button then 'Running Processes'
- This opens a list of processes currently running on your computer:
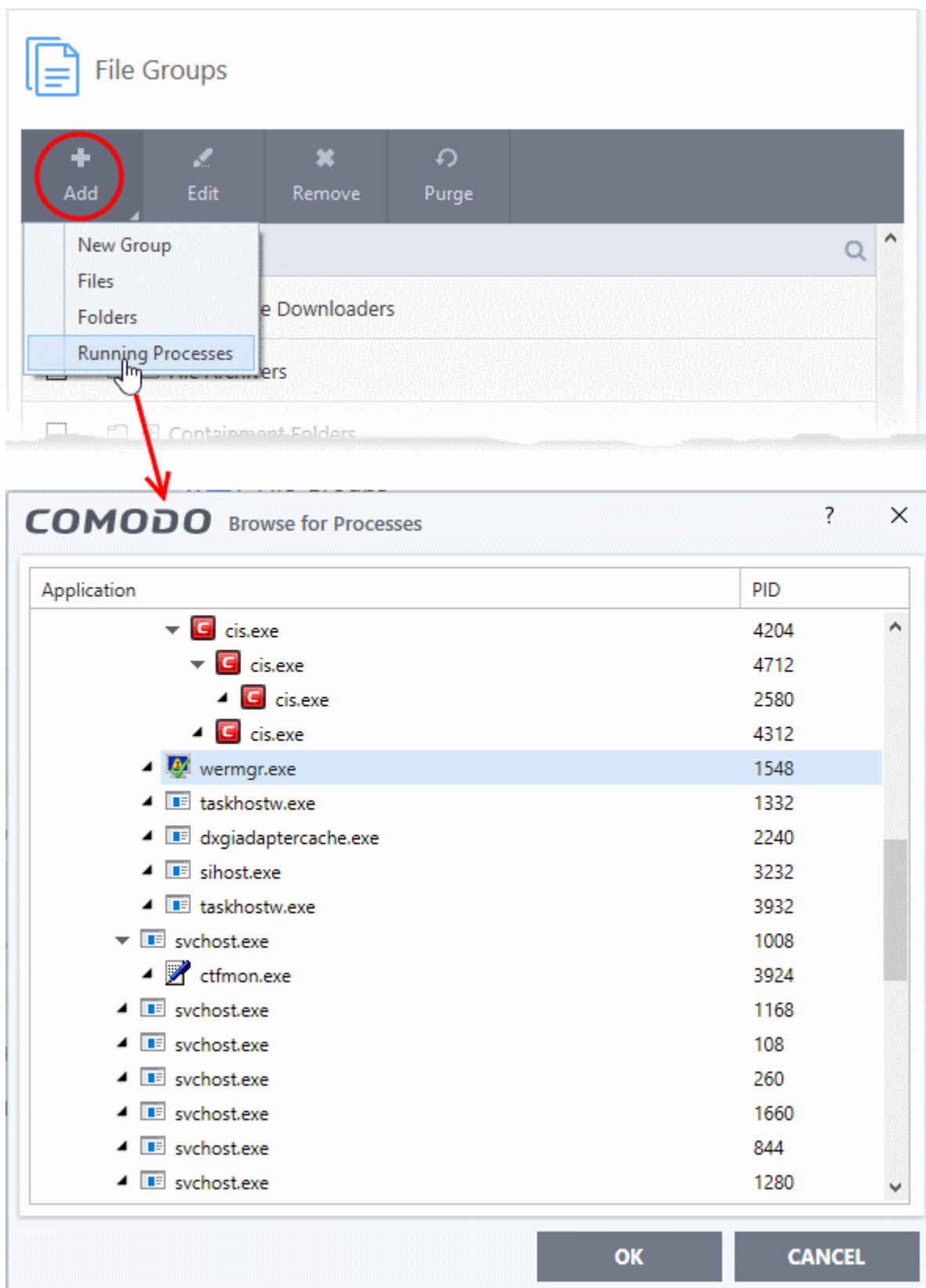
- • Select the desired process. The parent application of the process will be added to the group.
- • Click 'OK'.

Edit an item in the files groups list

- • Select the item from the list and click the 'Edit' button. The 'Edit property' dialog is shown:

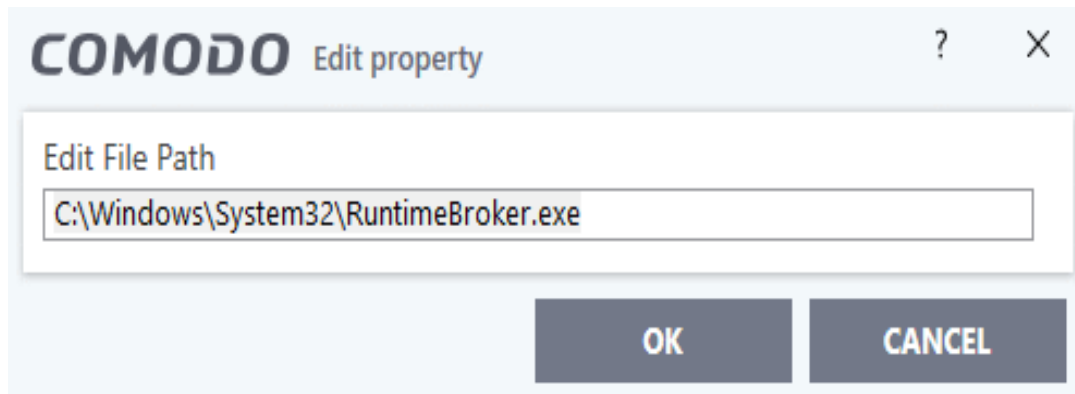- Edit the file path if required and click 'OK'.

Delete a file group or an individual file from a group

- To remove a file group, select it from the list and click the 'Remove' button.
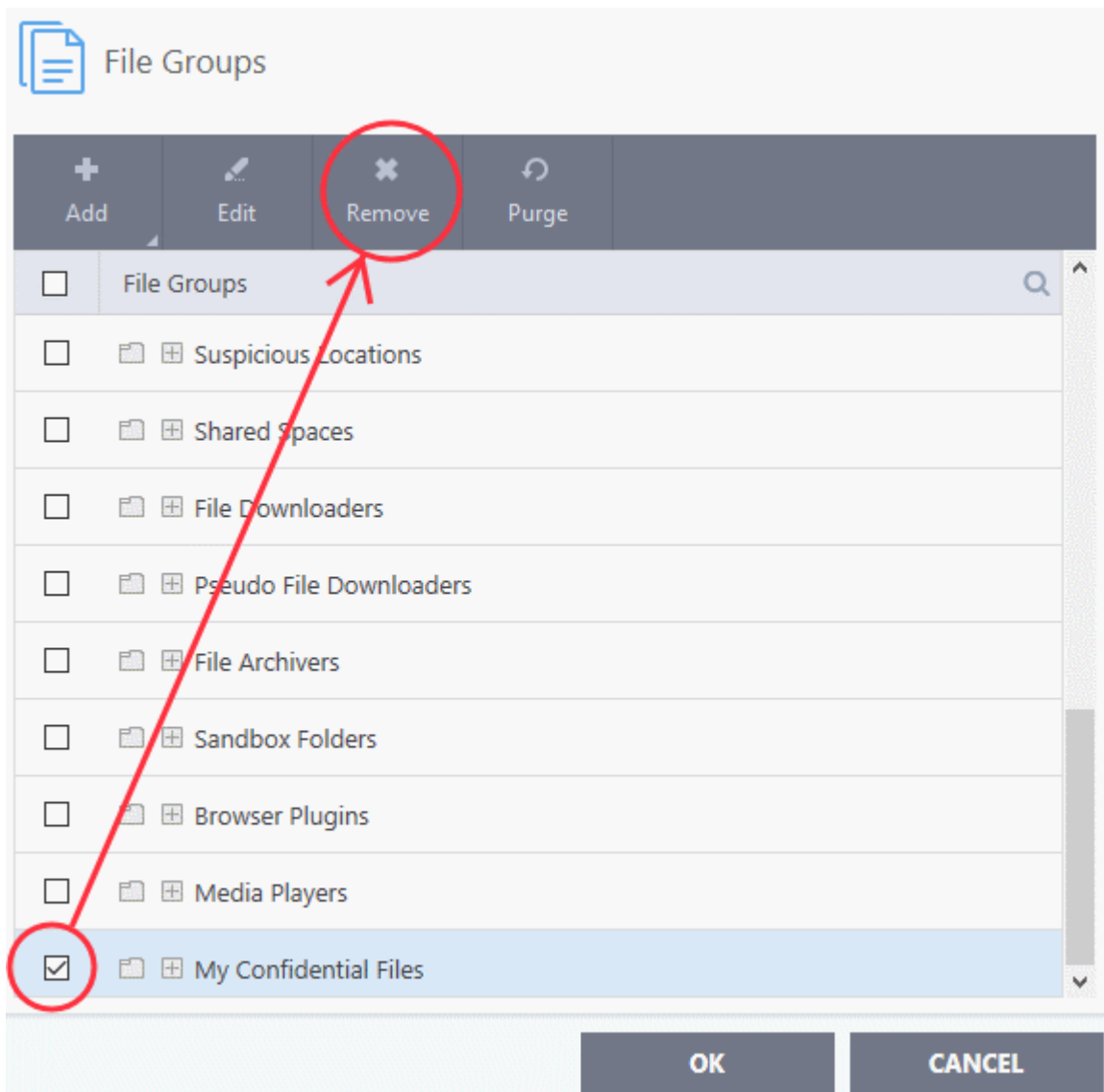
- To remove an individual file from a group - expand the group by clicking '+' at the left of the group, select the file to be removed and click the 'Remove' button.
- Alternatively, right-click on a file and choose remove from drop-down menu.

6.6.3. File List

Click 'Settings' > 'File Rating' > 'File List'

- The file list is an inventory of executable files and applications discovered on your computer.
- The list also shows the file vendor, the date the file was discovered, and the file's trust rating.

CIS rates files as:

- **Trusted**
- **Unrecognized**
- **Malicious**

Trusted Files

Files can be awarded a 'Trusted' status in the following ways:

- **Cloud-based file lookup service** (FLS) - When a file is first opened, CIS will check the file's reputation on our global whitelist and blacklists. It will award trusted status if the file is on the global whitelist of safe files.
- **Vendor rating** - The application is from a software publisher who has a 'Trusted' status in the **Vendor List**
- **User Rating** - You can manually assign a trusted rating to a file as follows:
  - Click 'Settings' > 'File Rating' > 'File List'
  - Select the target file then click the 'File Details' button
  - Click the 'File Rating' tab
  - Click the 'Rate Now' link
  - Set the rating as 'Trusted'
  - Click 'OK'
  - See **change the file rating** in **File Details** if you want more help on this.

Unrecognized Files

- Once installed, HIPS monitors and verifies all file 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.
- Any executable that is modified is also given 'Unrecognized' status. This protects you 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 a 'Trusted' rating. See '**Change the file rating**' for more details. You can also submit files to Comodo for analysis. Experts at Comodo will test the files and add them to global white-list or black-list accordingly.

Malicious Files

Files identified as malware are given a 'Malicious' rating, and are blocked and quarantined.

Open the file list interface

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List':
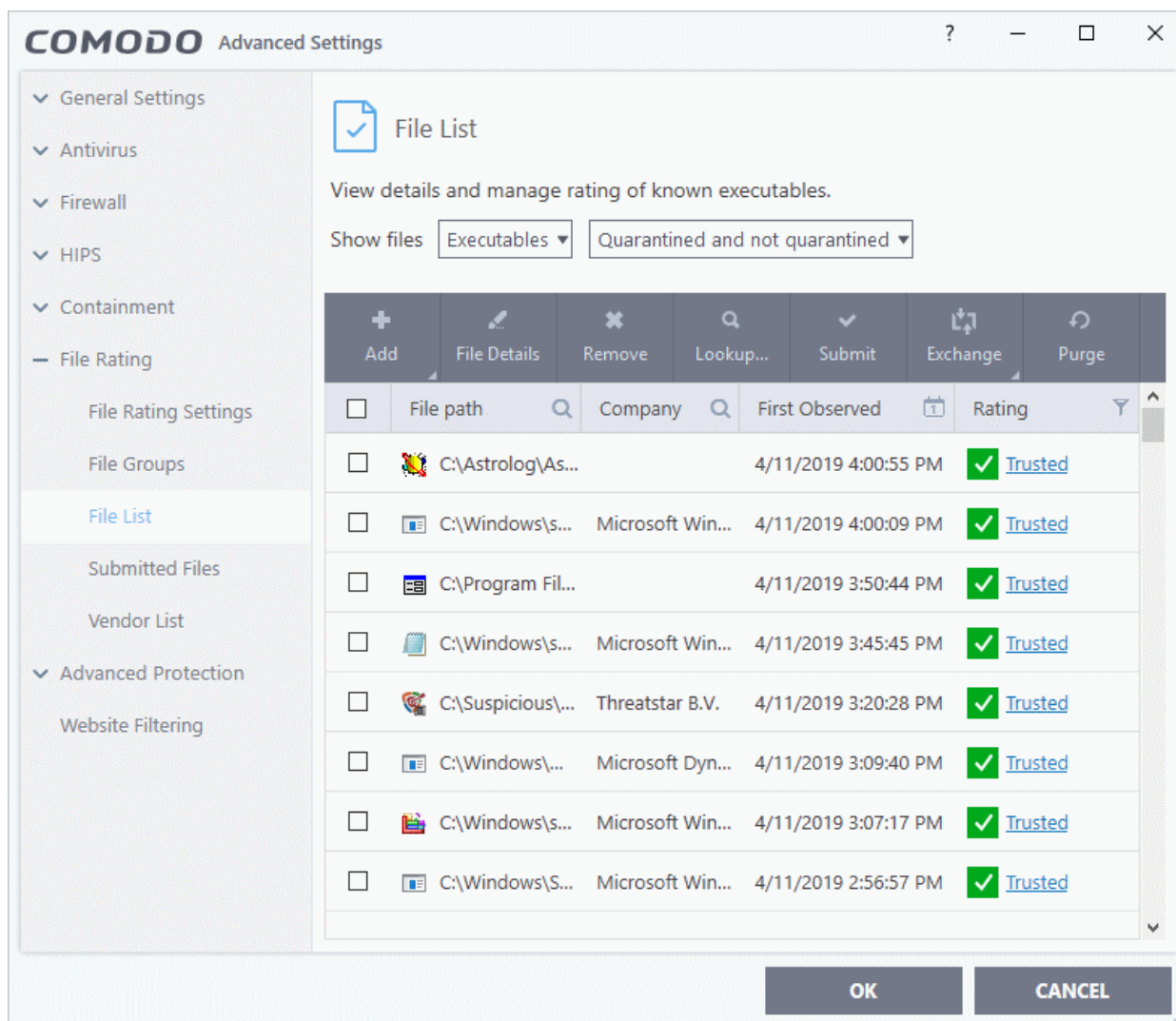
The file list shows applications and executable files discovered on your computer.

- **File Path**- The location of the file on your computer
- **Company** - The software vendor that published/created the file
- **First Observed** - Date and time at which the file was first discovered by CIS.
- **File Rating** - Current trust 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 - only applies if your CIS installation is remotely managed by an administrator.
2. User rating - A rating that you or another user awarded to a file.
3. FLS rating - The rating of the file on Comodo's online file look-up service (FLS).

There are three ways you can set user rating for a file:

1. Right-click on a file in the file list
- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List'
- Right-click on a file > Select 'Change File Rating to' > Choose a new rating:
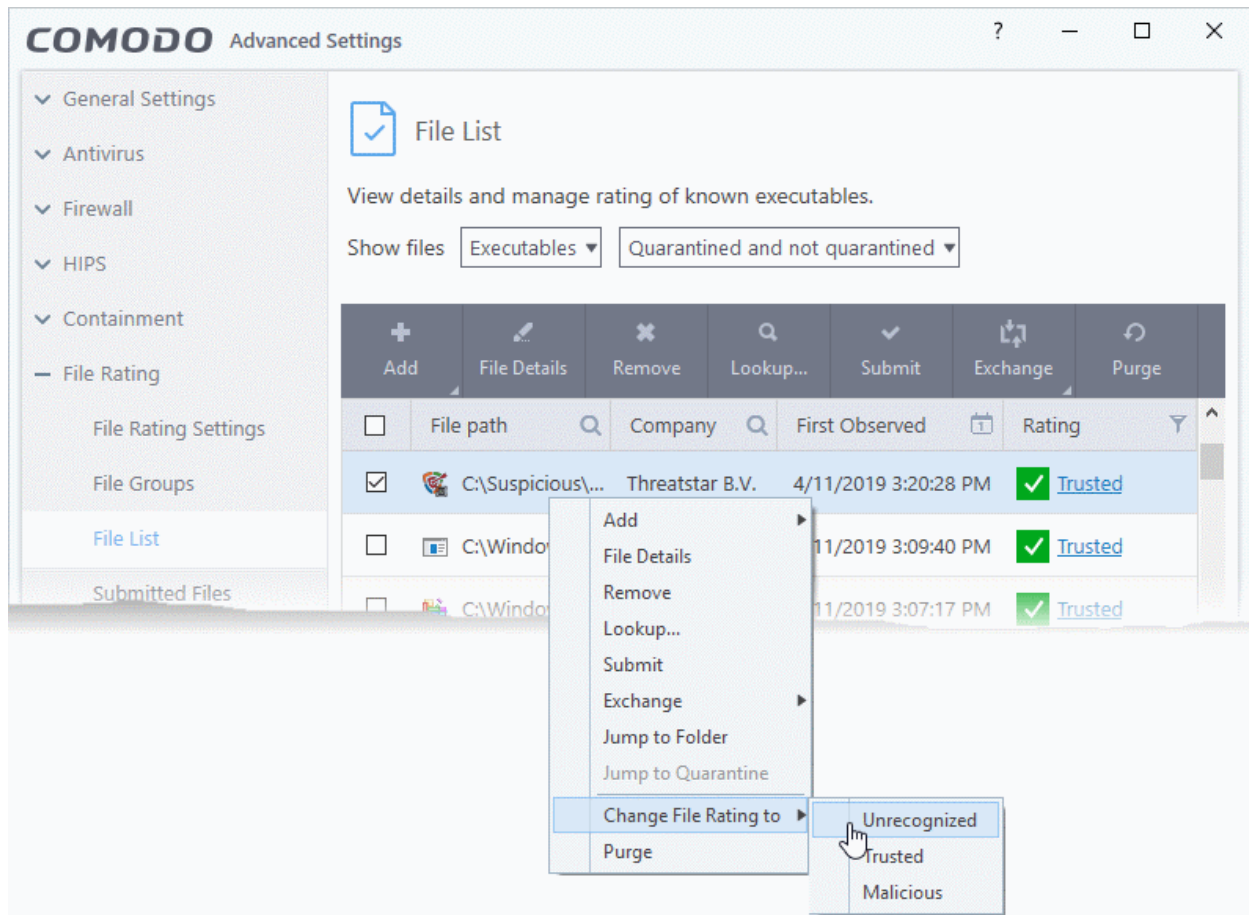
2.   In the file rating column

•   Click on the rating of a file in the 'Rating' column

•   Choose a new rating from the options:
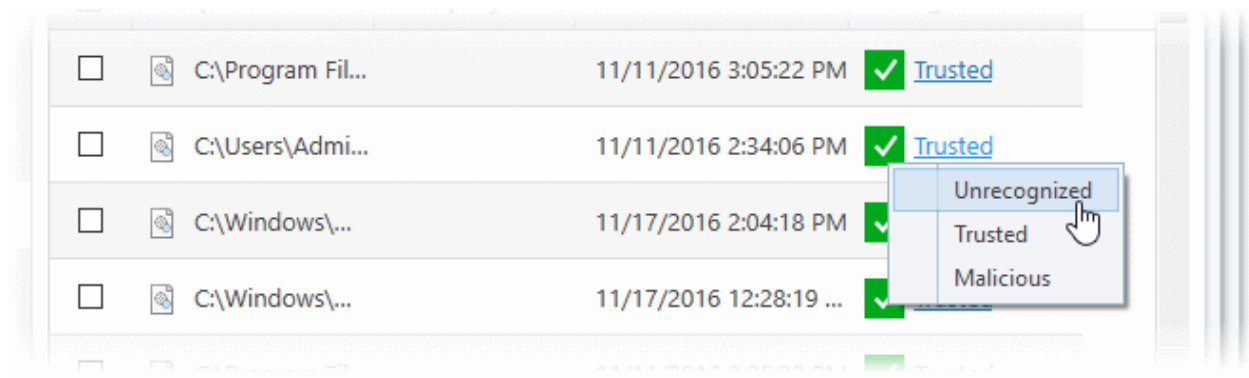
3.   From the 'File Details' dialog.

•   Select a file in the file list

•   Click the 'File Details' button at the top

•   Click the 'File Rating' tab

•   Click the 'Rate Now' link

•   Set the rating as required

•   Click 'OK'

Context Sensitive Menu

•   Right-click on a file to open 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.
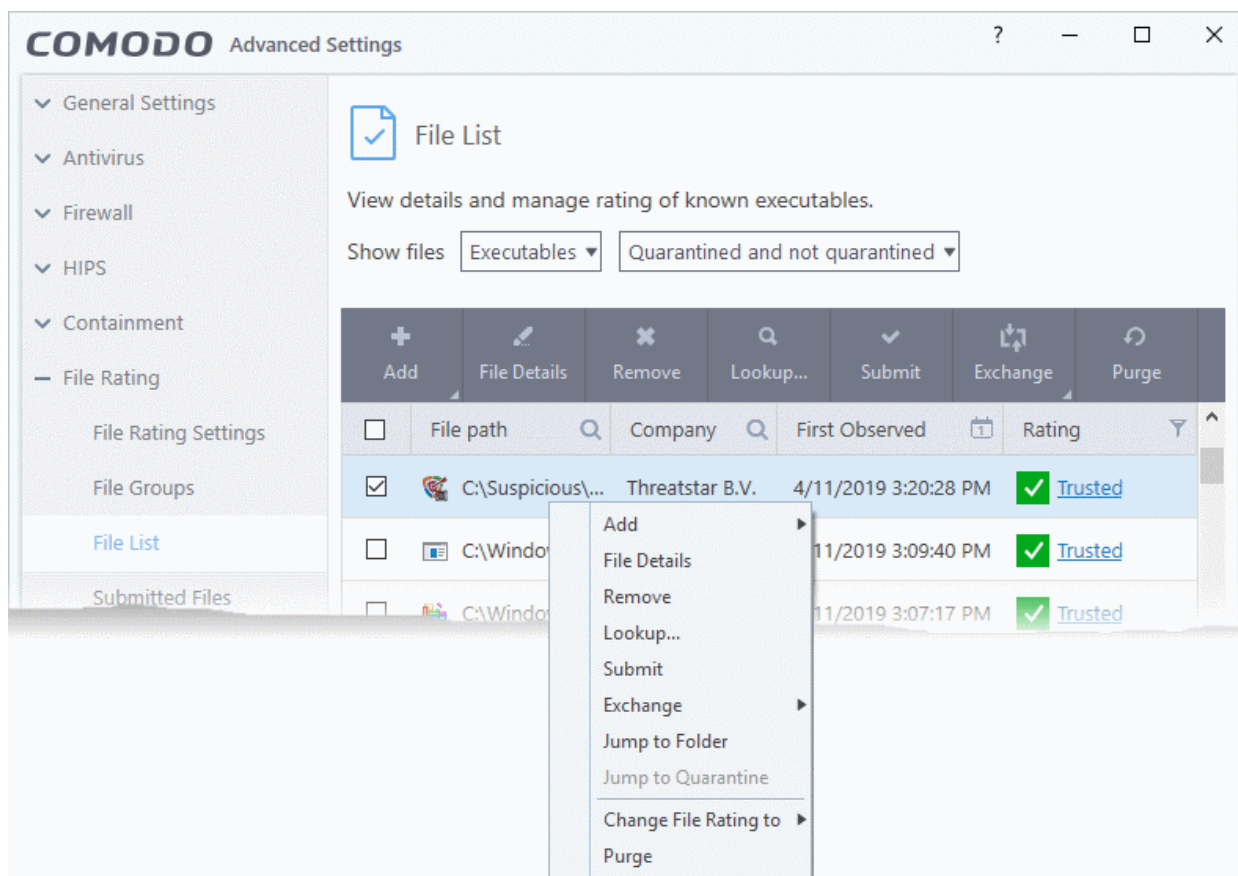
- **Add** - Manually add a file to the list and specify its trust rating

- **File Details** - View information about the selected item. You can also set the file rating from here.

- **Remove** - Delete files from the list.

- **Lookup** - Check the file-lookup server for more details about the file, including the latest trust rating.

- **Submit** - Uploads selected item to Comodo for analysis.

- **Import** - Add files to the list from an XML file

- **Export** - Save the current list as an XML file

- **Jump to Folder** - Opens the folder containing the file in Windows Explorer.

- **Jump to Quarantine** - Opens the 'Quarantine' interface of CIS to view or restore the file. Available only for items moved to quarantine. See **Manage Quarantined Items** for more details.

- **Change File Rating to** - Set user defined trust rating to the file.

- **Purge** - Check that all files in the list are still installed at the path specified. If not, the file is removed from the list.

Sorting, searching and filtering options

Sort option

- Click any column header to sort the items in alphabetical / ascending / descending order of entries in that column

Search options

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'.

- Click the search icon at the far right in the 'File path' and/or 'Company' column header.
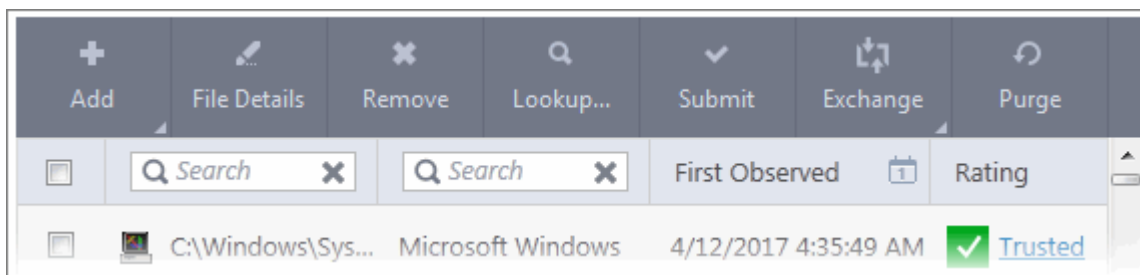
• Enter the file path and/or the name of company in part or full as per the selected criteria in the search field

The result for the entered criteria will be listed automatically. Click the 'X' icon to clear the search criteria and display all the items again in the list.

Filter options

• The 'Show files' filters on the top lets you select whether you want to view only executables, non executables, or all files:
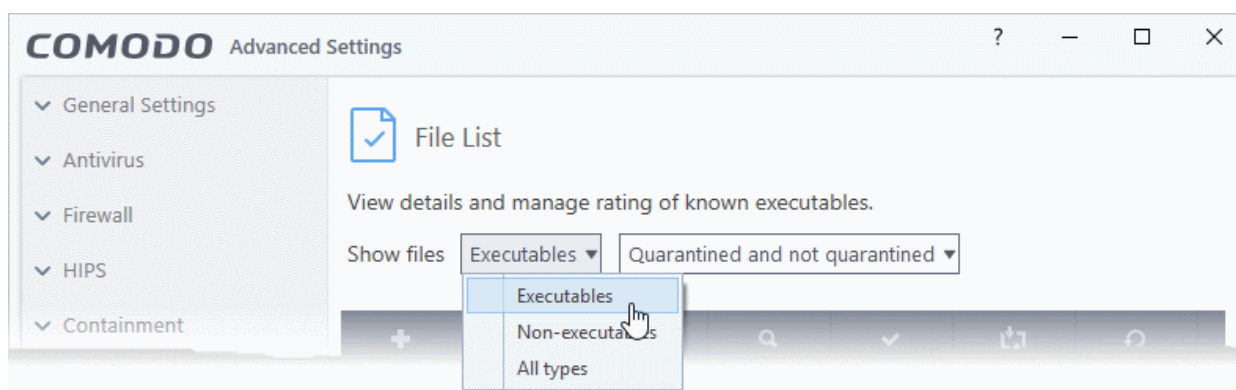
• Select the file type from the drop-down on the left
• Select whether you want to view only items moved to quarantine, items not moved to quarantine, or all files:
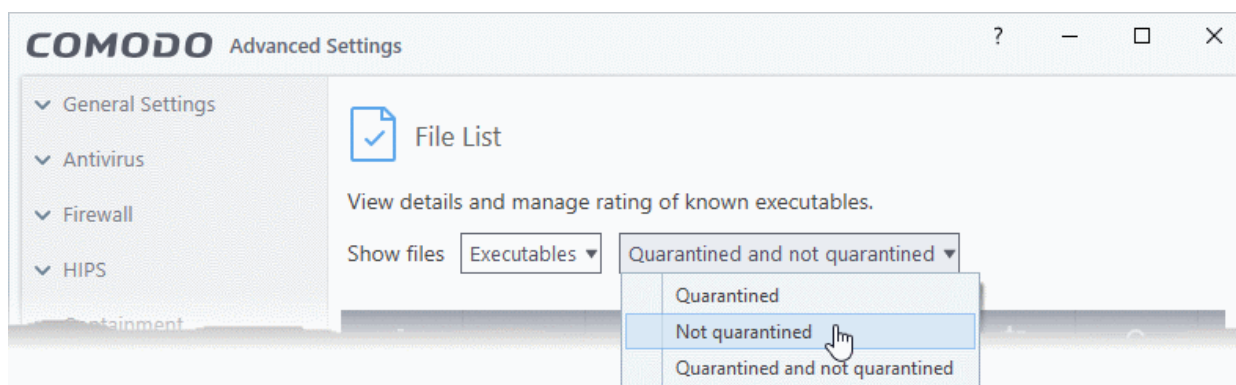
• Only the items that meet the criteria chosen from the filters are shown in the file list.

• Click the calendar icon at the right of the 'First Observed' column

• Choose the time period you require

• This will show only those files discovered in the time-frame you set:
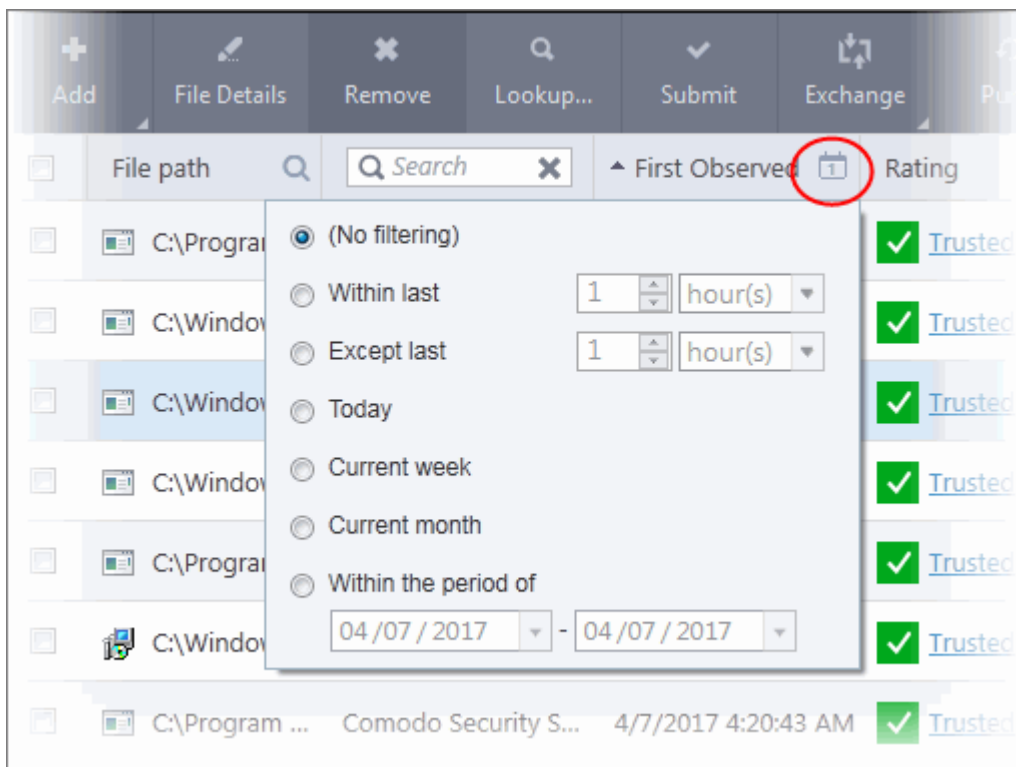
- Click the funnel icon at the right of the 'File Rating' column to filter files by rating:
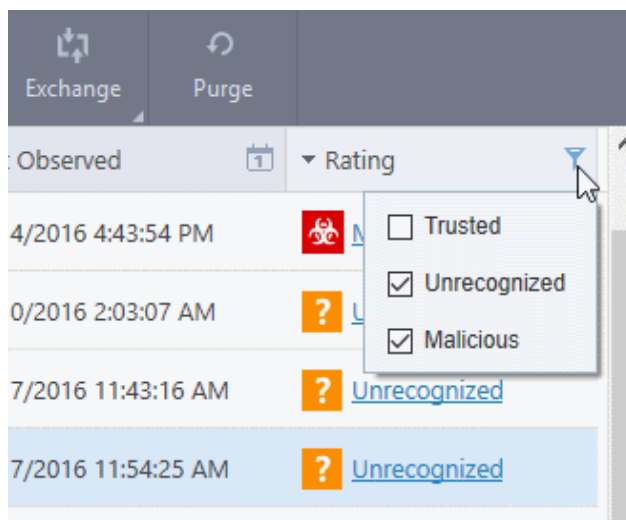
Control Buttons

The buttons at the top provide the following options:

- **Add** - Manually add a file to the list and specify its trust rating
- **File Details** - View information about the selected item. You can also set the file rating from here.
- **Remove** - Delete files from the list.
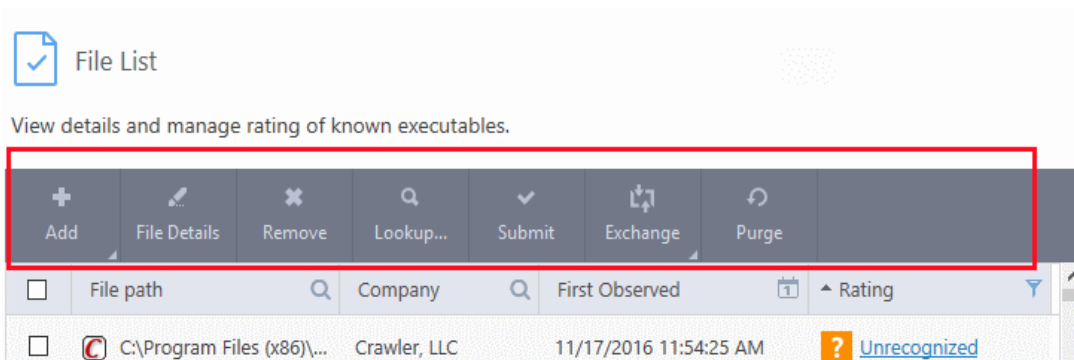- **Lookup** - Check the file-lookup server for more details about the file, including the latest trust rating.
- **Submit** - Uploads selected item to Comodo for analysis.
- **Exchange** - Consists of two options (**Import** and **Export**).
  - **Import** - Add files to the list from an XML file
  - **Export** - Save the current list as an XML file
- **Purge** - Check that all files in the list are still installed at the path specified. If not, the file is removed from the list.

Manually add files to file list

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Add' button at the top
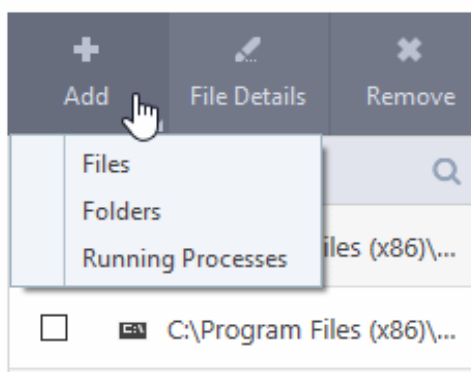
> **Tip**: Alternatively, right click inside the 'File List' page and choose 'Add' from the context sensitive menu.

You can add three types of item:

- **Files** - Browse to the file you want to add and assign a rating.
- **Folders** - Browse to the folder you want to add an assign a rating. All files in the folder will inherit the rating you gave to the folder.
- **Running Processes** - Select a currently active process and assign a rating. The parent application of the process will be added to the file list with the rating you assign.

View the file details and change the rating

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List'
- Select a file and click the 'File Details' button.
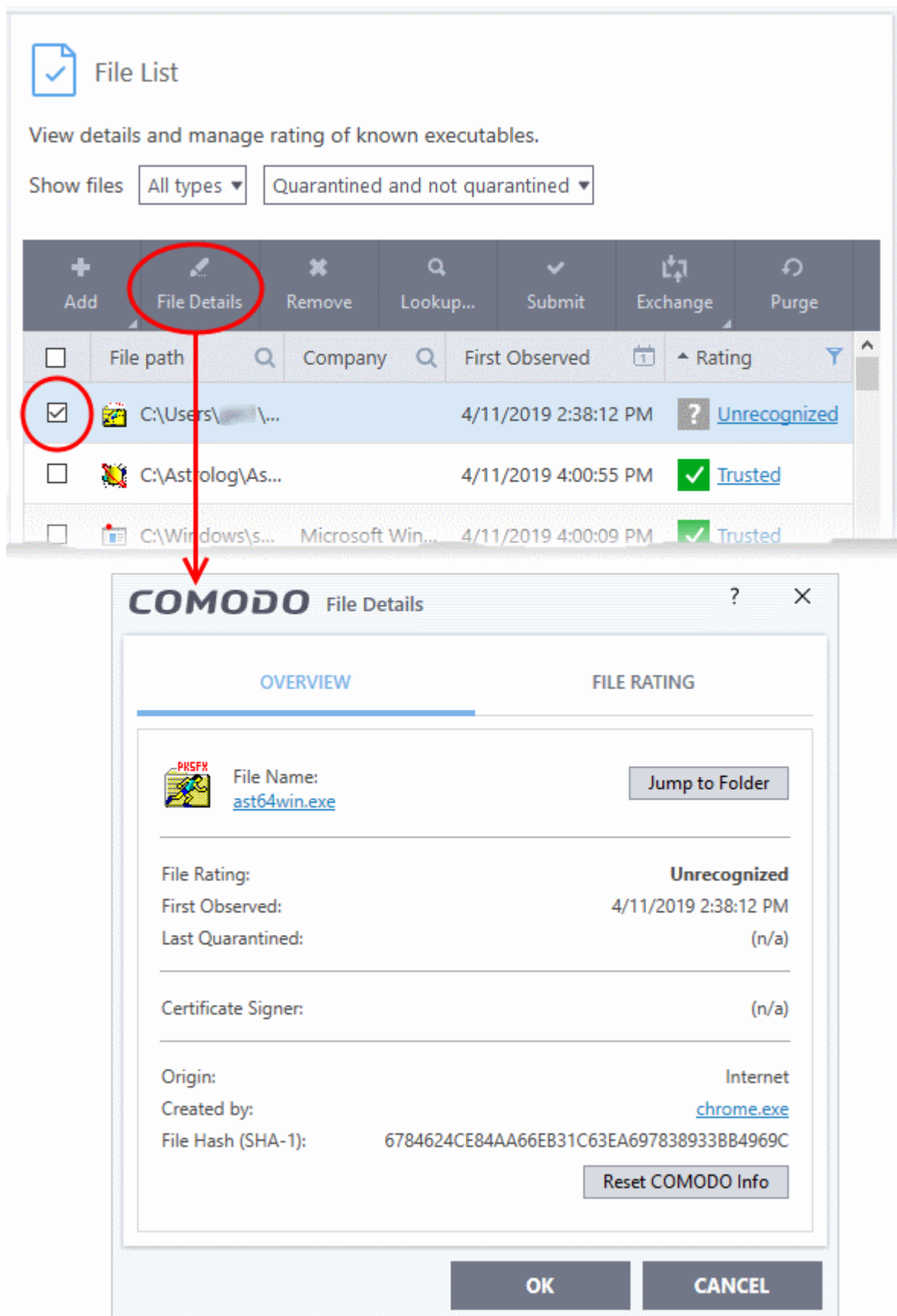
Tip: Alternatively, right click on the selected file inside the 'File List' page and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog has two tabs:

- • **Overview**
- • **File Rating**

Overview

The 'Overview' tab shows general details such as the file rating, discovery date, hash value and publisher (signer):
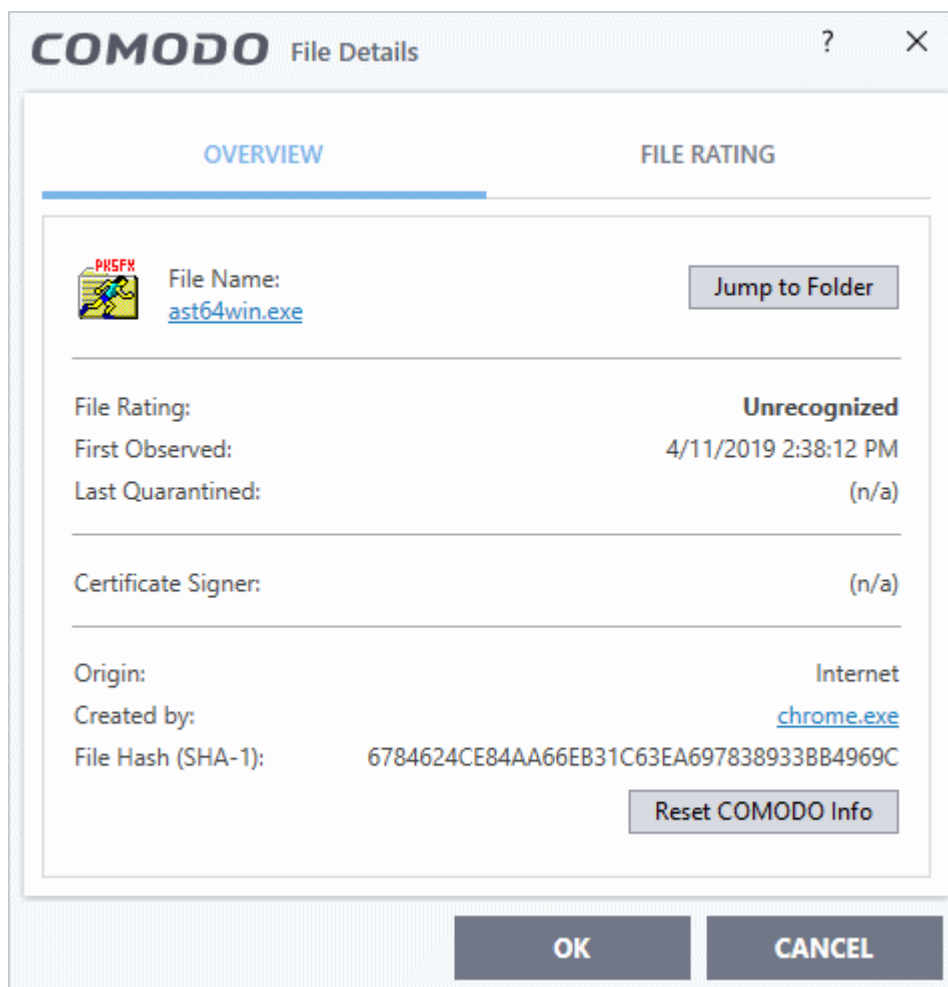
- • Click the file name to open the Windows 'File Properties' dialog.
- • Click 'Jump to folder' to open the folder containing the file in Windows Explorer, with the respective file selected.
- • Click 'Reset COMODO Info' to refresh the information from Comodo FLS database

File Rating

Shows the file's current trust rating from Comodo and lets you set your own rating:
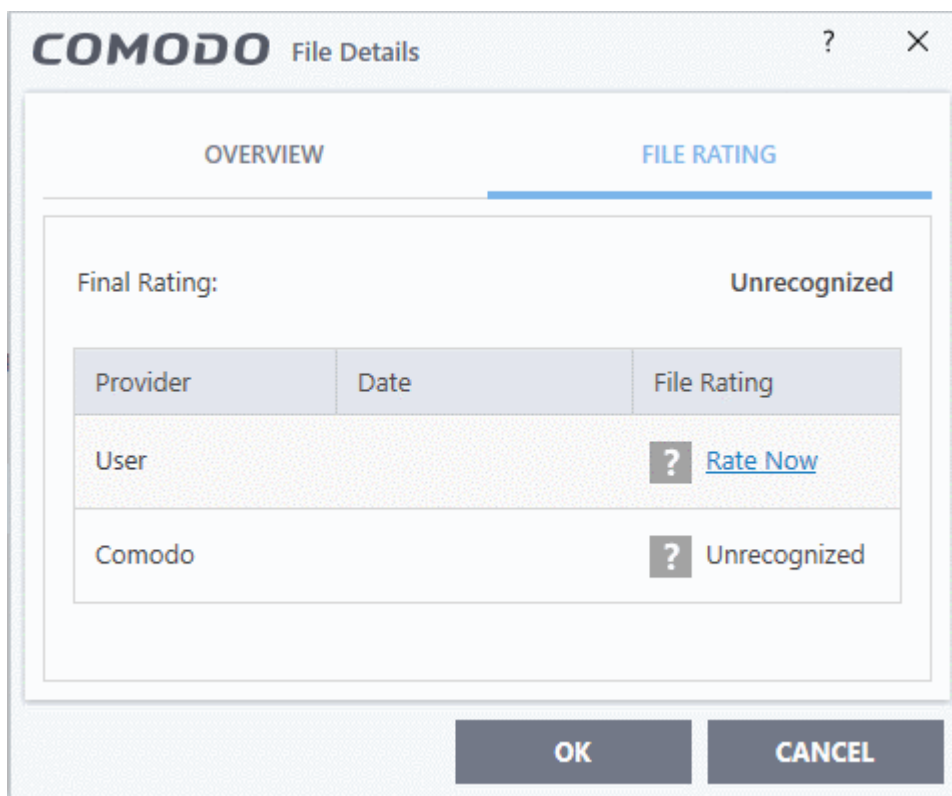
Change the user rating of the file

- 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 the 'Rate Now' link beside 'User' and choose the rating from the drop-down
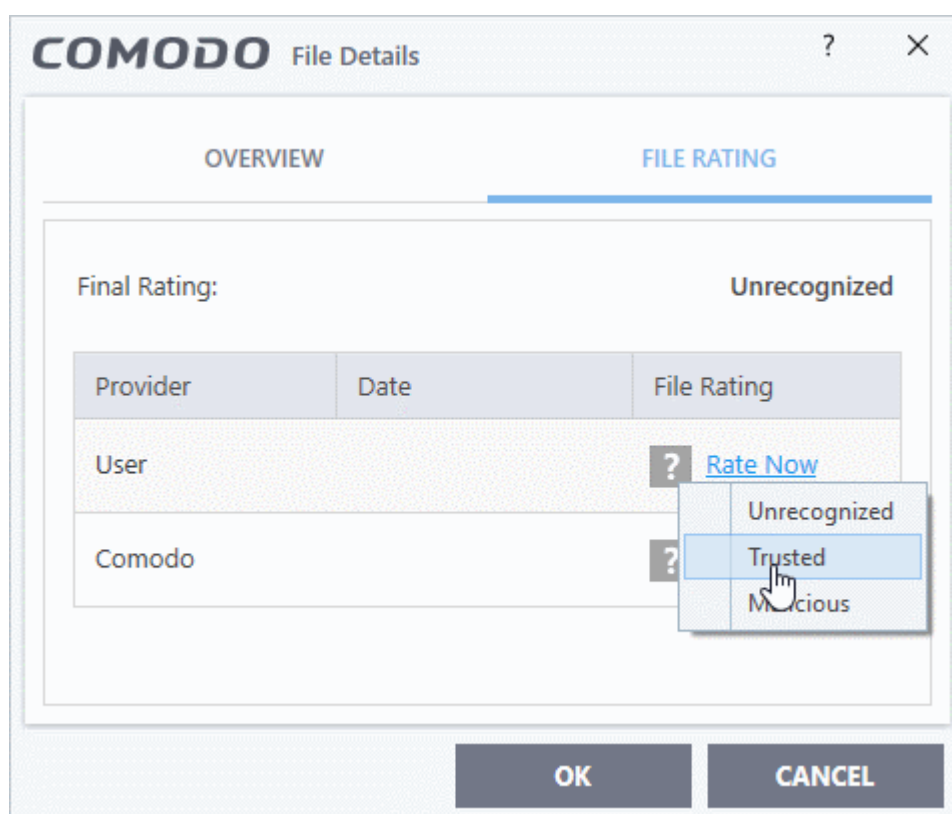
The options available are:

- 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.

- Click 'OK' in the 'Files Details' dialog
- The trust rating of the file will be updated for the file with the user rating in the 'File List' interface.
- You can change the rating for the file at anytime by following the same process

Tip: Alternatively, right click on a file then choose 'Change File Rating to'

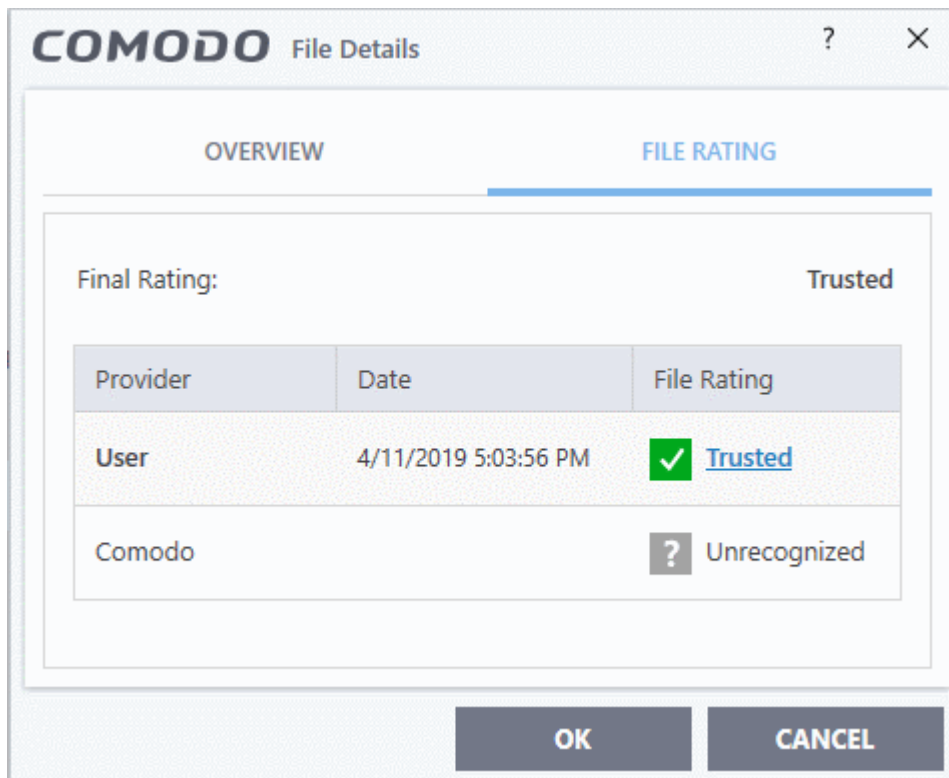- Click 'OK' in the 'Advanced Settings' interface to save your settings.

Remove files from the file list

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be removed
- Click the 'Remove' button at the top. The file(s) is / are only removed from the list and not deleted from your system.

Tip: Alternatively, right click on a file then choose 'Remove' from context sensitive menu.

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

Perform an online lookup for files

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be checked from the 'File list' pane.
- 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.
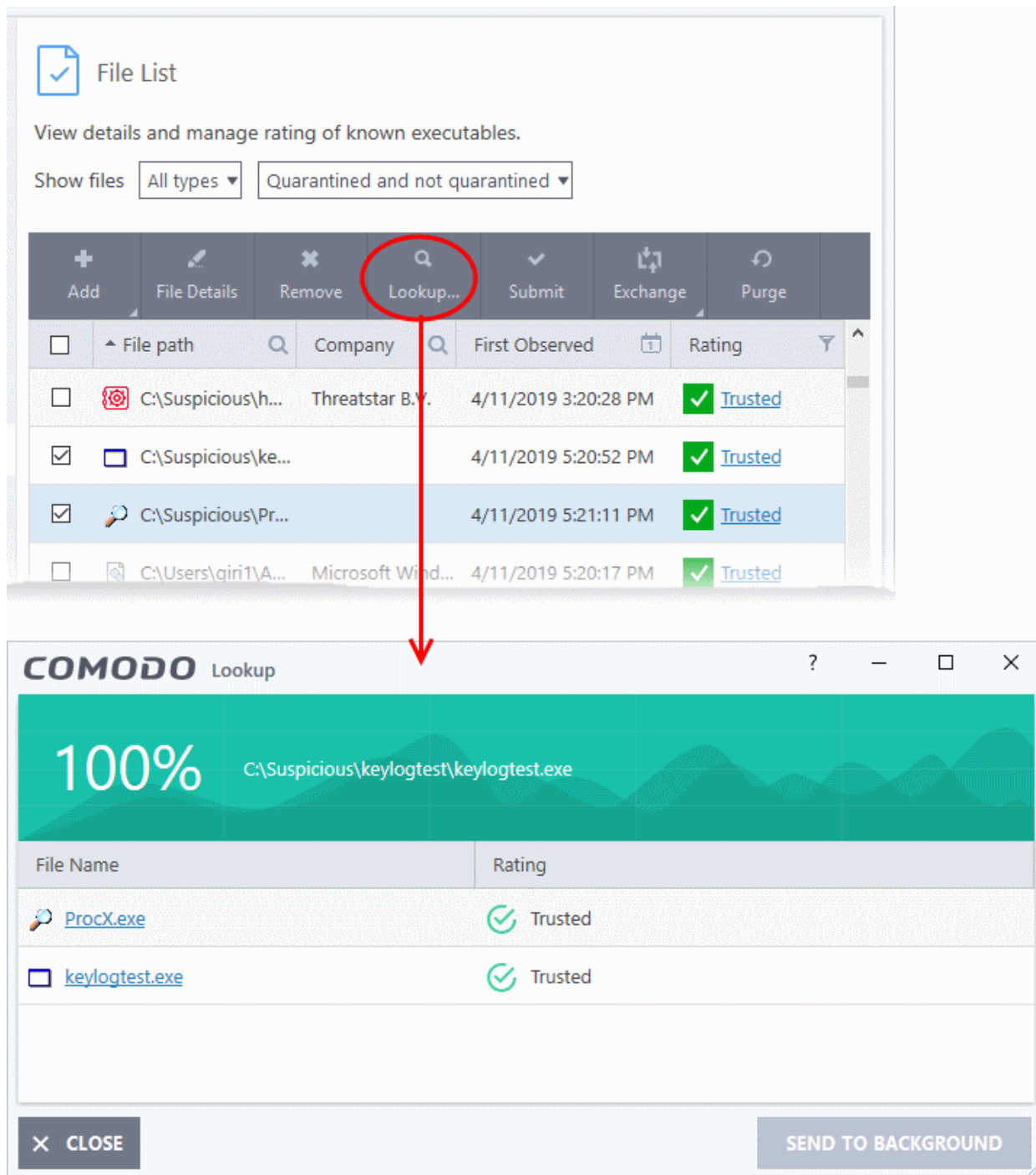
If any malicious or unwanted file(s) is/are found, you will be given an option to delete the file from your computer on closing the dialog.
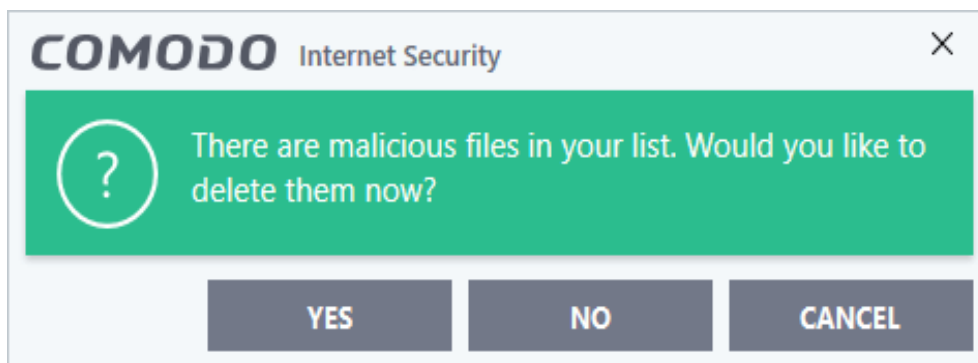
- Click 'Yes' to permanently delete the malicious file(s) from your computer.
- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. See **changing the file rating** in **File Details** for more details.
- If no information 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.

Manually submit files to Comodo

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be submitted from the 'File List' pane.
- 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.

Export and Import the File List

You can save the list of files with their currently assigned ratings to an XML file and store it in a safe place. This is useful to restore your list if you have to uninstall/reinstall CIS, or if you want to implement the same list on another machine that has CIS installed.

Export the File List

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > '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.
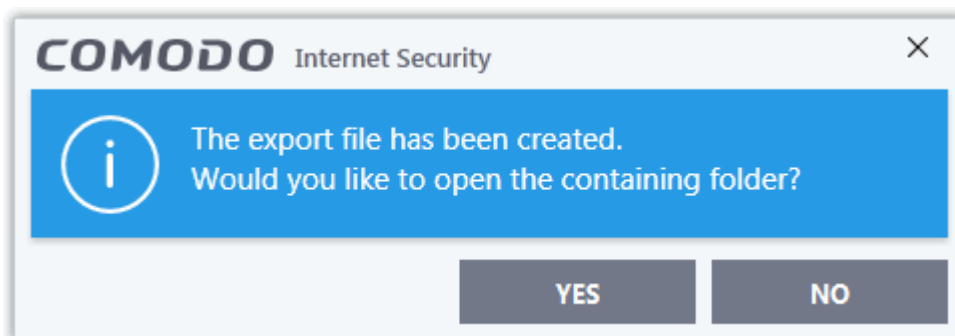
To import a saved file list

- 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

Click 'Settings' > 'File Rating' > 'Submitted Files'

- The 'Submitted Applications' area lets you review and manage the files that you have uploaded to Comodo for analysis.

- You can submit suspicious, unknown or false-positive files for analysis. 'Unknown' files are those that do not yet have a trust rating. 'False positives' are files you think CIS has incorrectly classified as malware.

- Once uploaded, our automated systems test the file to establish whether or not it is trustworthy. After the automated tests, the file is manually inspected by our technicians and added to the global whitelist or blacklist as appropriate.

Tip: You can have CIS automatically submit unknown files to Comodo for analysis. To set this up:
- Click 'Settings' > 'File Rating' > 'File Rating Settings'
- Enable 'Analyze unknown files in the cloud by uploading them for instant analysis'
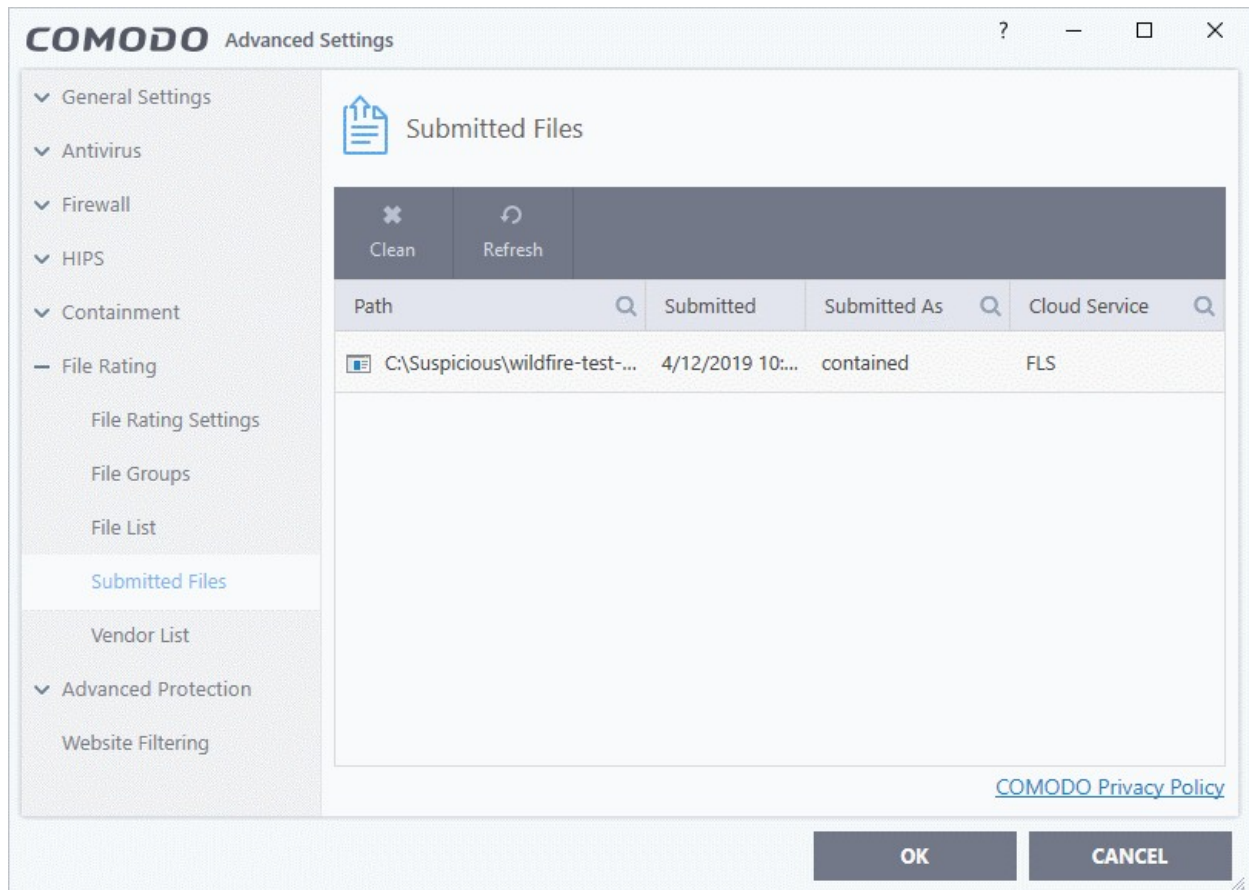- Click 'OK'

Open the submitted files interface

- Click 'Settings' on the CIS home screen
- Click 'File Rating' > 'Submitted Files' on the left:

- **Path** - The location of the file on your computer
- **Submitted** - Date and time the file was uploaded for analysis;
- **Submitted As** - The status 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 file look-up server (FLS), or Comodo Valkyrie. Valkyrie is Comodo's automated file-testing service.

Context Sensitive Menu

- Right-click on a file to view further options:
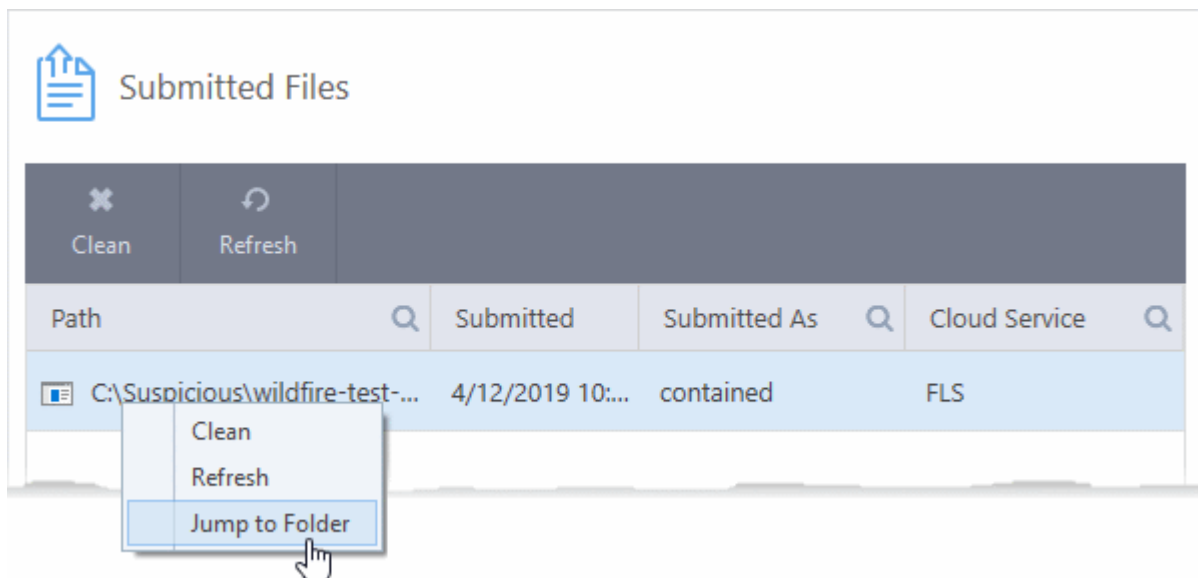
- **Clean** - Clears the file list

- **Refresh** - Reloads the list to show recently submitted items
- **Jump to Folder** - Opens the directory in which the file is located

You can also use the buttons at the top to clean and refresh the list:

Sort and search options

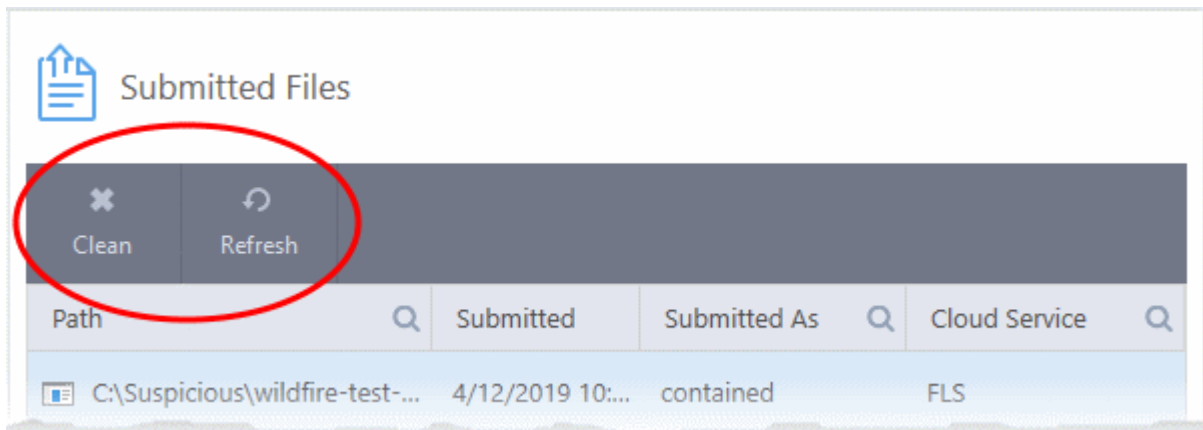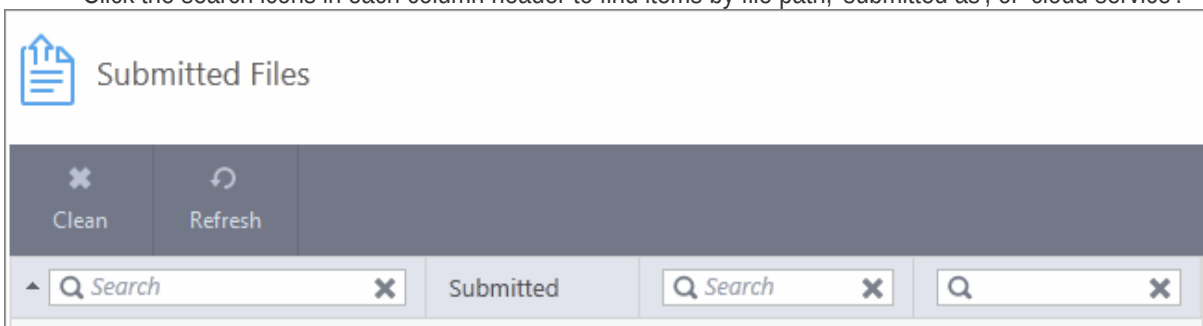- Click any column header to sort items in order of the entries in that column
- Click the search icons in each column header to find items by file path, 'submitted as', or 'cloud service':

- Click the 'X' icon to clear search criteria and display all items.

6.6.5. Vendor List

- Click 'Settings' > 'File Rating' > 'Vendor List'

There are three ways that a file can be treated as safe in CIS:

- The file is on the Comodo safe list (a global white-list of trusted software)
- The user has assigned 'Trusted' rating to the file in the CIS file list ('**Settings' > 'File Rating' > 'File List**')
- The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file.

With regards to vendor settings, CIS handles *unknown* files as follows:

- The file is allowed to run normally if:
    - The vendor rating is 'Trusted' AND you have enabled 'Rate applications according to their vendor rating' in **File Rating Settings**
- The file is run in the container if:
    - The vendor rating is 'Unrecognized' AND you have enabled 'Rate applications according to their vendor rating' in **File Rating Settings**
    - The vendor is not in the vendor list (regardless of whether you have enabled 'Rate applications according to their vendor rating')
- The file is blocked and quarantined if:
    - The vendor rating is 'Malicious' AND you have enabled 'Rate applications according to their vendor

rating' in **File Rating Settings**

Vendor List

- CIS ships with a list of trusted vendors who have a reputation of creating legitimate, safe software. CIS allows unknown files which are digitally signed by one of these vendors to run.

- Click 'Settings' > 'File Rating' > 'Vendor List' to view this list of trusted vendors.

- You can also add new vendors, and change the rating of existing vendors. User ratings supersede the Comodo rating.

- Software publishers can get themselves added to trusted vendors by contacting Comodo with their software details. **Click here** to read more about the trusted vendor program.

  - **Click here** to read background information on digitally signed software.

Open the 'Vendor List' interface

- Click 'Settings' on the CIS home-screen

- Click 'File Rating' > 'Vendor List':
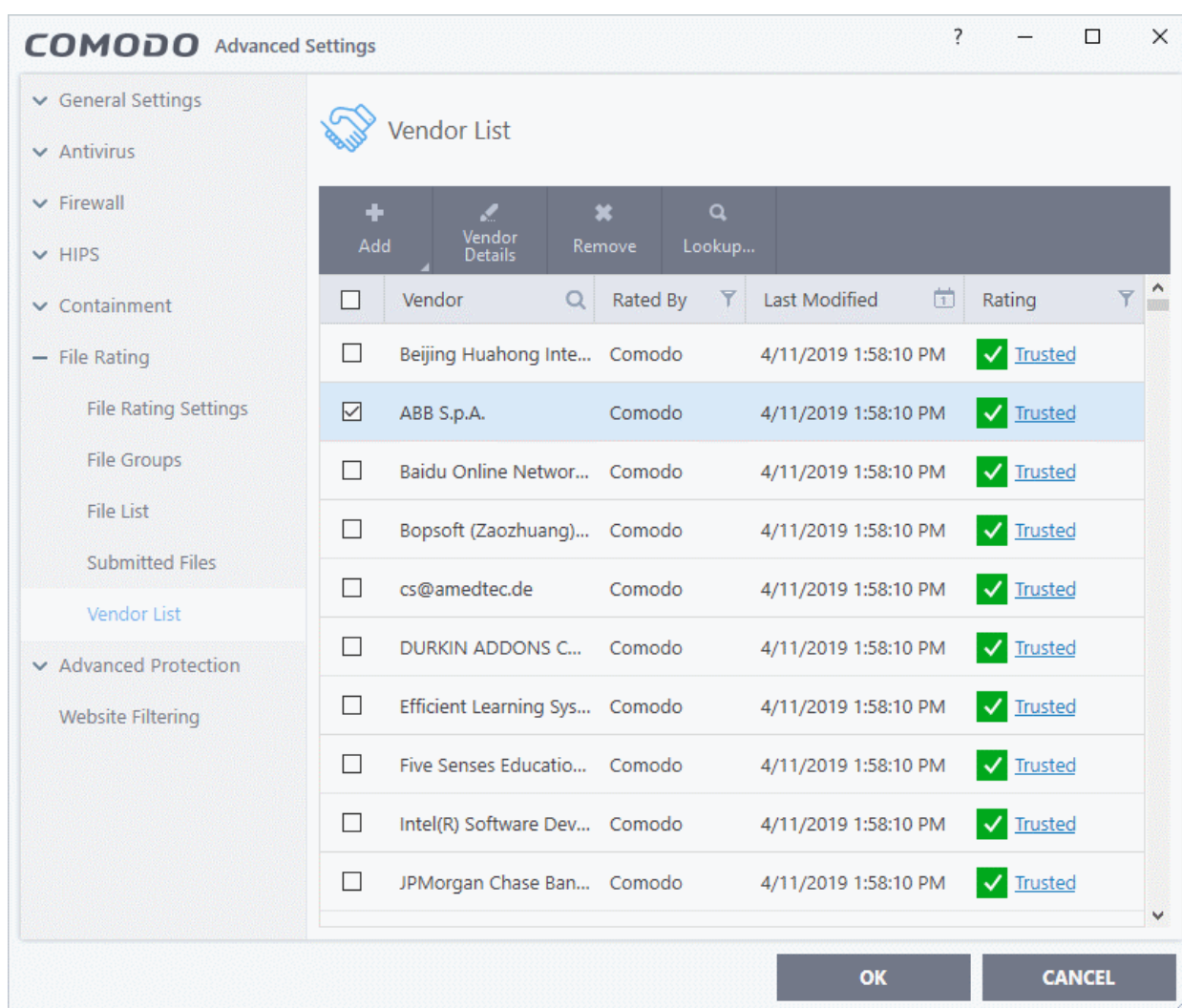
The interface allows you to:

- **Add a new vendor to the list**

- **View details of vendors and assign user rating**

- **Perform an online lookup for vendors**

- **Remove vendors from the list**

Column Descriptions:

- **Vendor**- The name of the software publisher

- **Rated By** - The entity that assigned the rating you see in the 'Rating' column. This can be 'Comodo' or 'User' rating.

- **Last Modified** - Date and time the rating was most recently updated.

- **Rating** - Current trust rating of the vendor. The possible values are:

  - Trusted
  - Unrecognized
  - Malicious

- Click on the rating to assign a new rating

- CIS obeys user ratings over and above Comodo ratings.

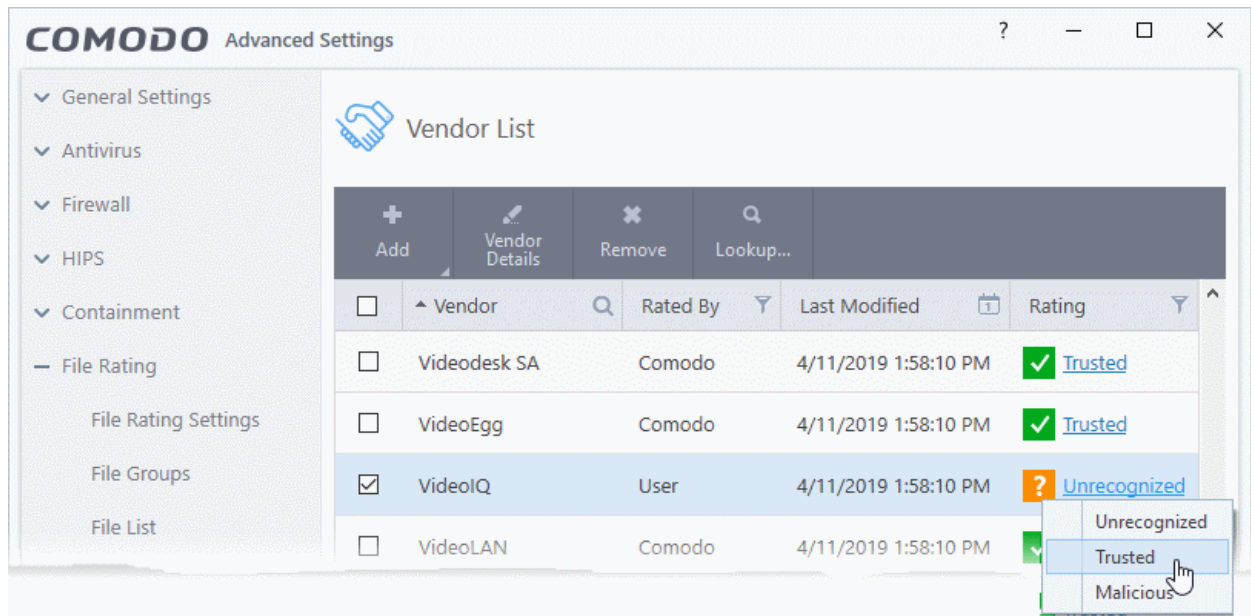There are three ways you can set a vendor rating:

1. **Right-click on a vendor in the 'Vendor List'**

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'Vendor List'
- Right-click on a vendor > Select 'Change File Rating to' > Choose a new rating:
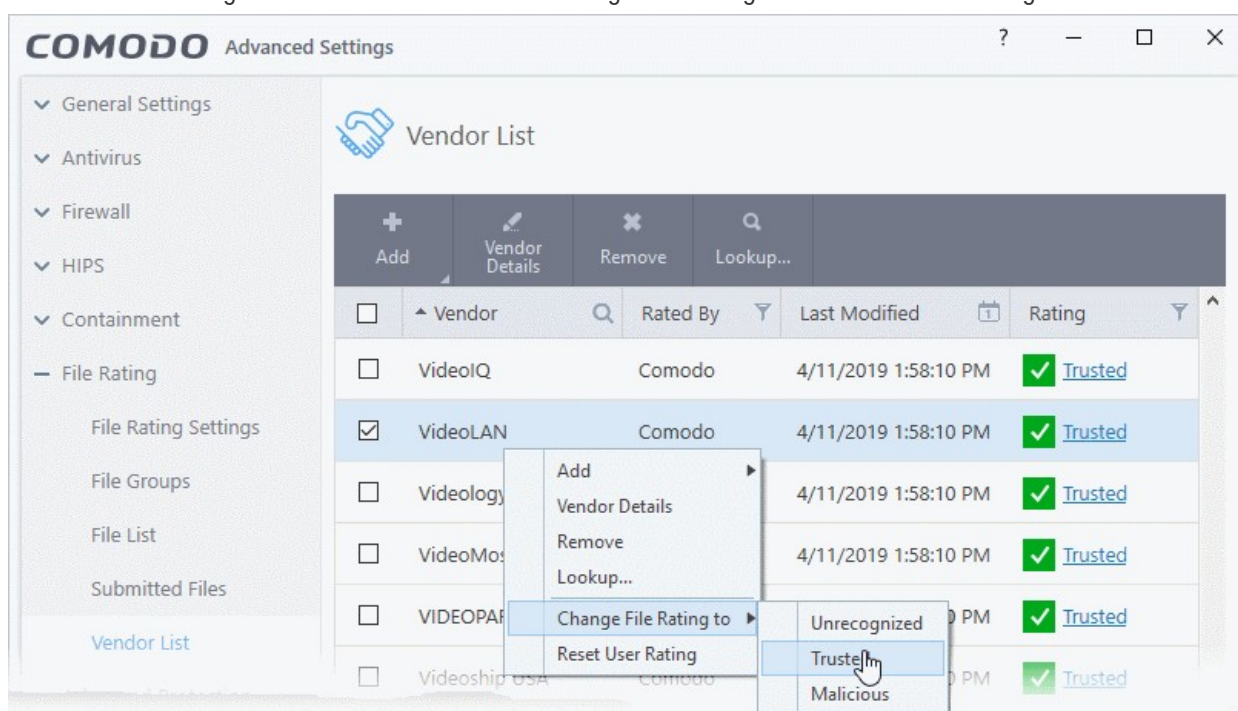
2. In the file rating column

- Click on the rating of a vendor in the 'Rating' column
- Choose a new rating from the options:

---

3. From the 'File Details' dialog

- Select a vendor in the file list
- Click the 'Vendor Details' button at the top
- Click the 'Vendor Rating' tab
- Click the 'Rate Now' link beside 'User'
- Set the rating as required
- Click 'OK'

Context Sensitive Menu

- Right-click on a vendor to open a context sensitive menu that allows you to view the 'Vendor Details' dialog, assign a rating to a vendor, add / remove vendors, and more.
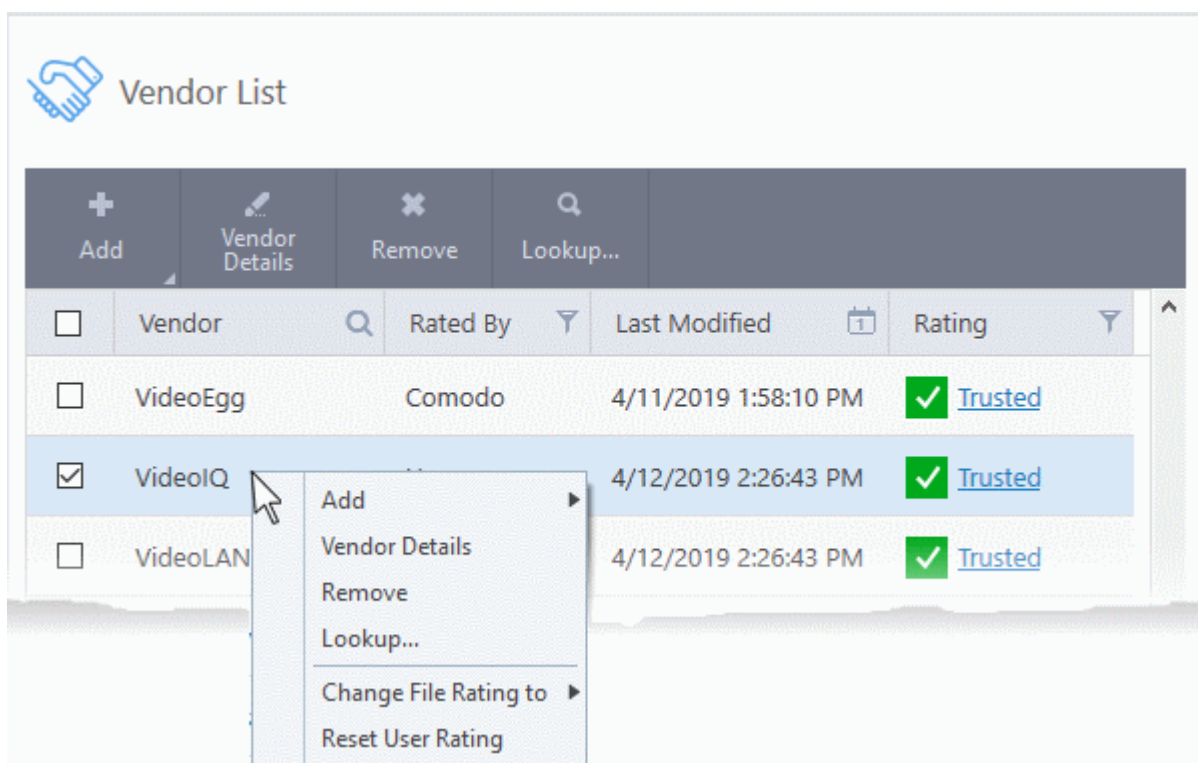
- **Add** - Manually add a new vendor to the vendor list. You can select an executable file or a currently running process to add the publisher who signed that file to the list.

- **Vendor Details** - View the information about the vendor. You can also assign user defined trust rating to the vendor
- **Remove** - Delete the vendor from the list
- **Lookup**... - Check details of the vendor from the master Comodo trusted vendor list
- **Change File Rating to** - Set user defined trust rating to the vendor
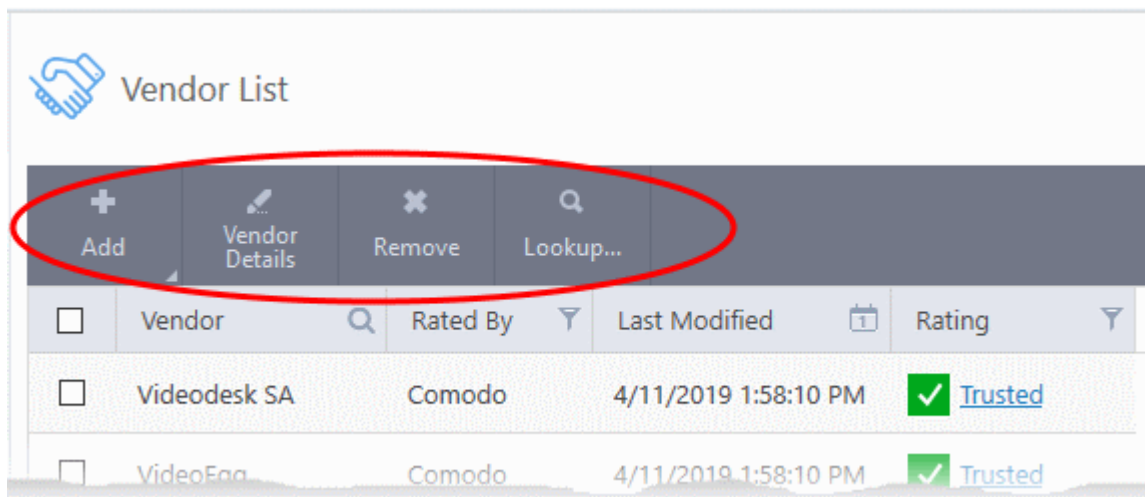- Reset User Rating --Clear user rating and reinstate Comodo rating

Controls

The buttons at the top provide the following options:

- **Add** - Manually add a new vendor to the list. You can add a vendor by simply selecting a file or a running process. CIS will extract the publisher who signed the file/process.
- **Vendor Details** - View information about the selected vendor. You can also set your own trust rating for the vendor from here.
- **Remove** - Delete selected vendors from the list.
- **Lookup...** - Check details of a vendor on Comodo's online trusted vendor list

Sort, Search and Filter options

- Click any column header to sort the list in order of the entries in that column
- Click the search icon in the 'Vendor' column header to look for specific vendors
- Click the calendar icon in the 'Last Modified' column header to filter vendors by date modified:
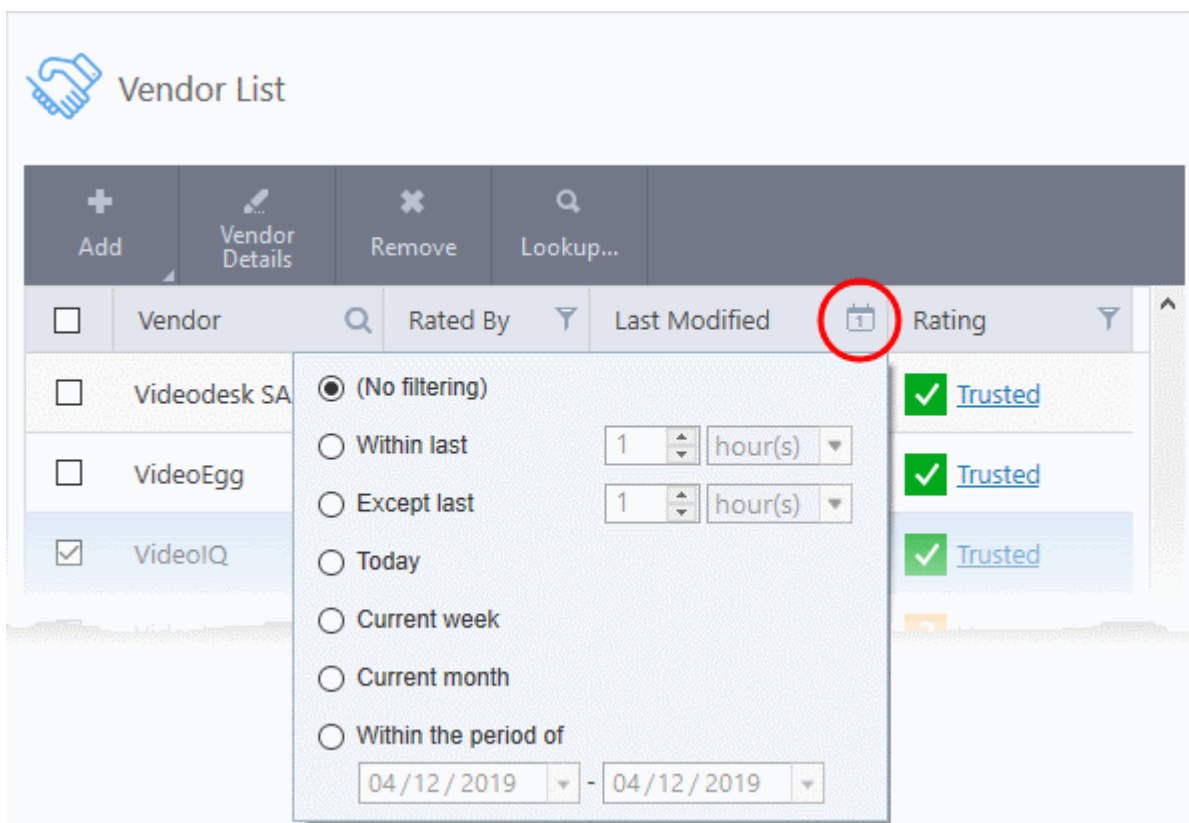
- Click the funnel icon in the 'Rated By' / 'Rating' columns to filter vendors by trust rating, and by who assigned the rating:
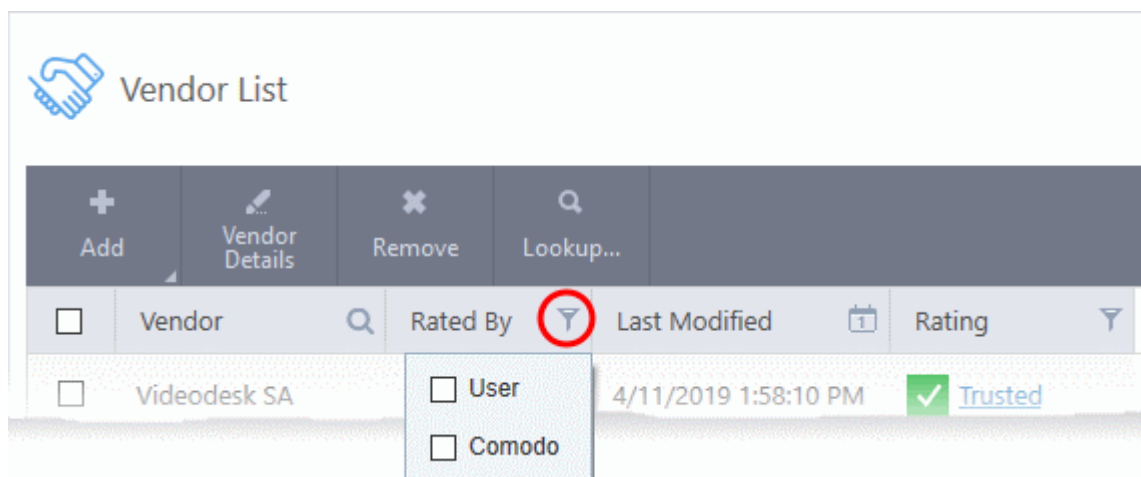
Add a new vendor to the list

- You can add vendors simply by browsing to a file they have digitally signed
- CIS will read the vendor's signature from the file and add them to the list
- You can then assign your own rating to the vendor

There are two ways to add vendors:

- **Specify an executable file on your local drive**
- **Select a currently running process**

Add a vendor by reading the vendor's signature from an executable

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'Vendor List'

- Click the 'Add' button at the top and select 'Read from a signed executable'
- Alternatively, right-click inside the vendor list and select 'Add' > 'Read from a signed executable'
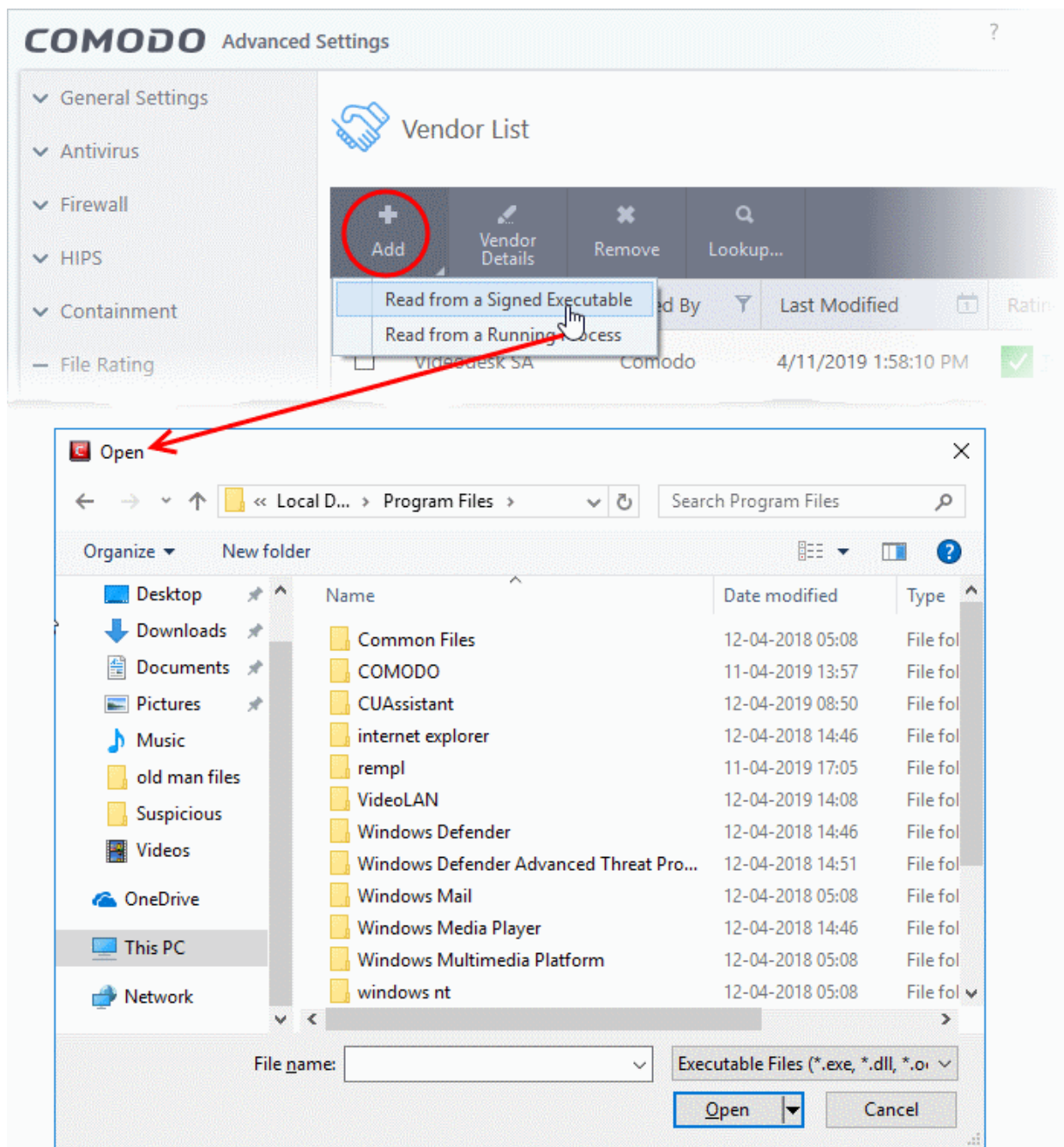
- Navigate to the executable file whose publisher you want to add to the vendor list and click 'Open'.

CIS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, you can add the vendor to the list by assigning your trust rating'.

- Choose your rating and click 'OK'
- The vendor will be added to the list with your rating.

If the vendor is already on the list you will be notified:

You can assign your own rating to the existing vendor:
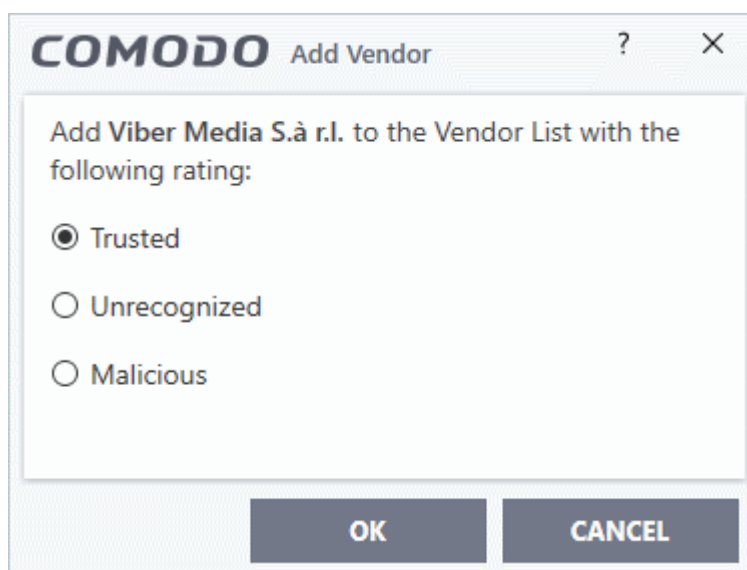
- Choose your rating and click 'OK'
- The user rating for the vendor will be assigned as you set.
- If CIS cannot verify that the software certificate is signed by a Trusted CA then it does not add the software vendor to the vendor list. In this case, you can see the following error message.
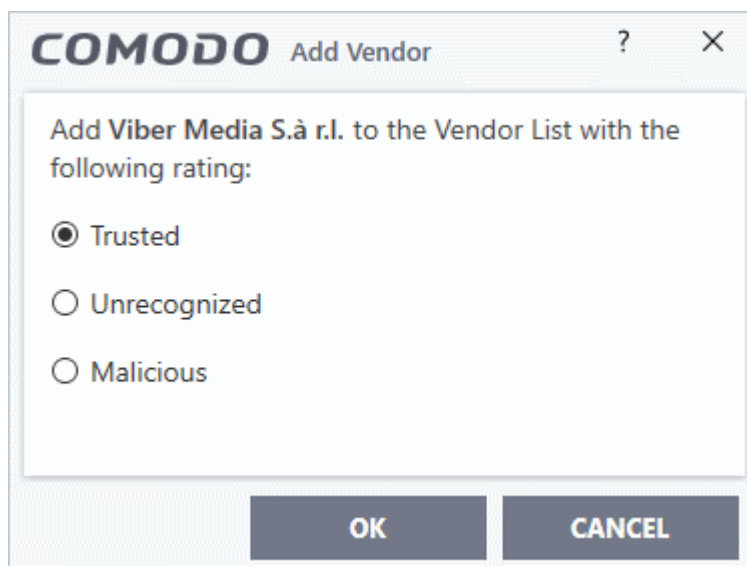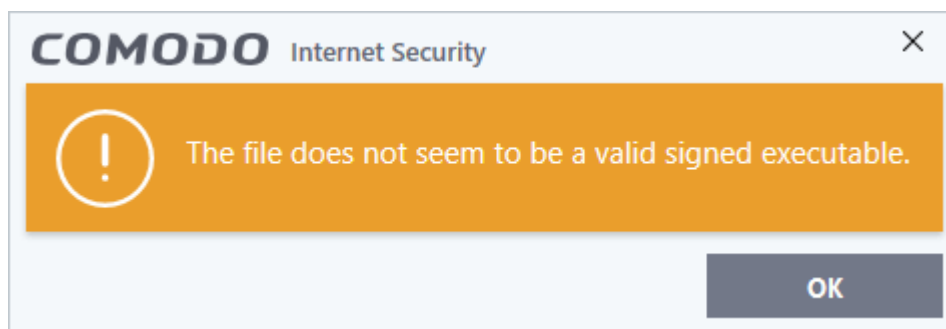
Add a trusted vendor from a currently running process

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'Vendor List'
- Click the 'Add' button at the top and select 'Read from a Running Process'
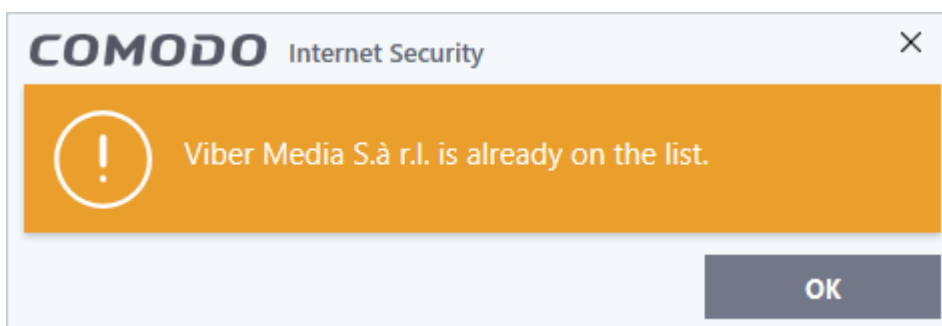- Alternatively, right-click inside the vendor list and select 'Add' > 'Read from a Running Process'
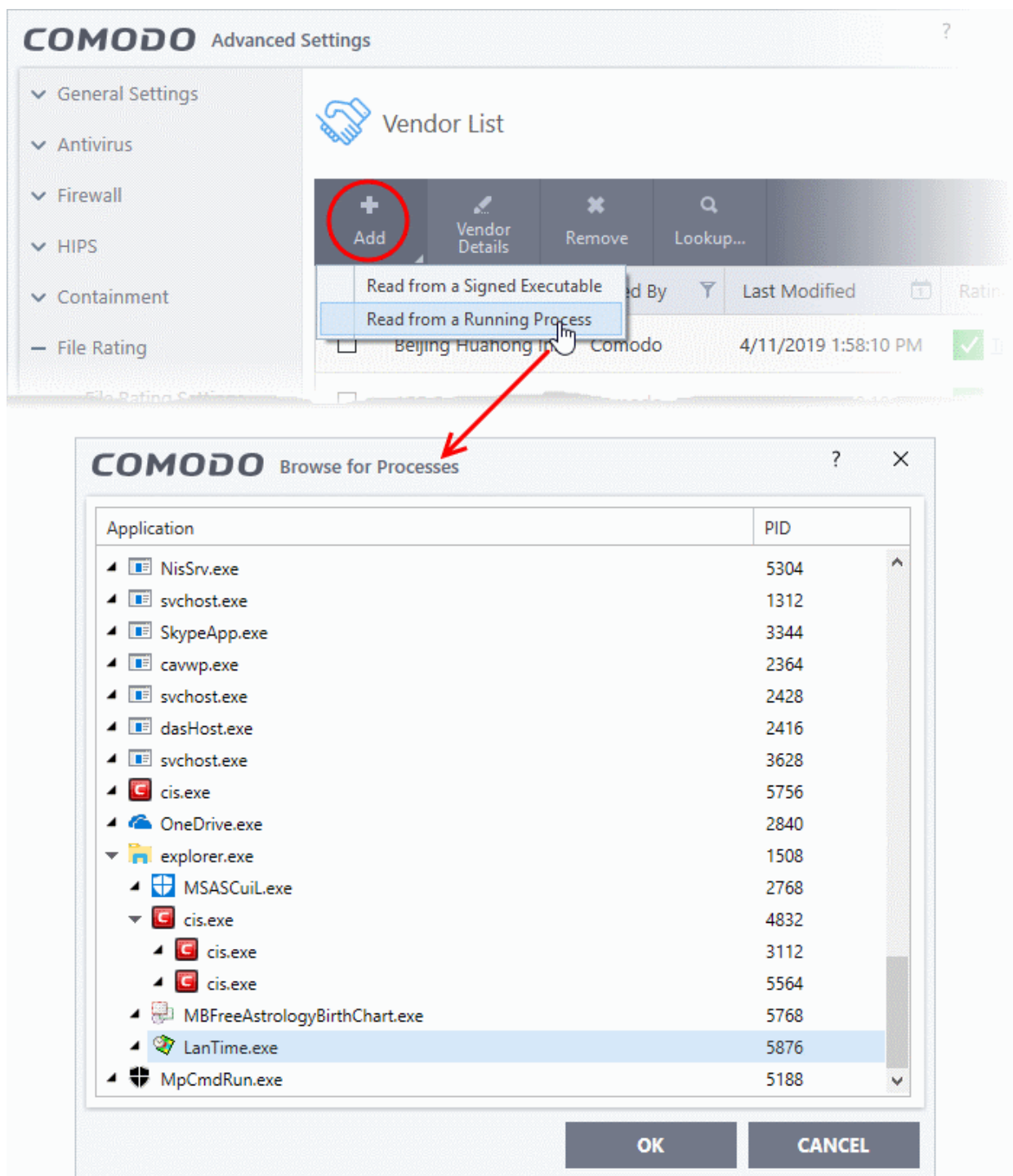
- Select the signed executable that you want to trust and click the 'OK' button.

- Comodo Internet Security performs the same certificate check as described above. If the parent application of the selected process is signed, you will be able to assign a rating and add the vendor as described **above**.

View details of vendors and assign user rating

- Click 'Settings' on the CIS home-screen

- Click 'File Rating' > 'Vendor List'

- Select a vendor and click the 'Vendor Details' button

- Alternatively right-click on a vendor and select 'Vendor Details'
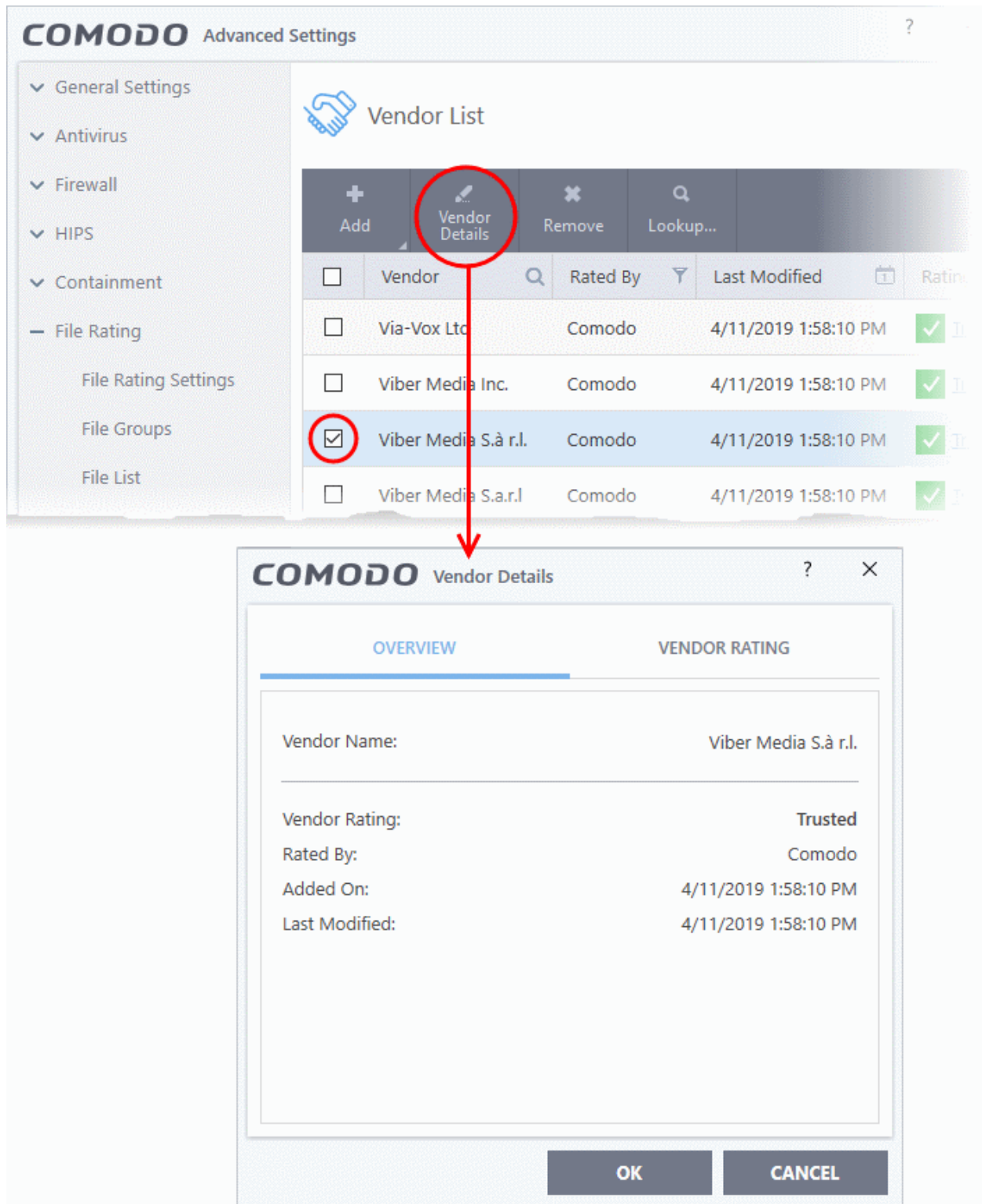
The 'Vendor Details' dialog will open. The dialog has two tabs:

- **Overview**
- **Vendor Rating**

Overview

The 'Overview' tab shows general details such as the vendor name, Comodo assigned rating, when the vendor was added and more:
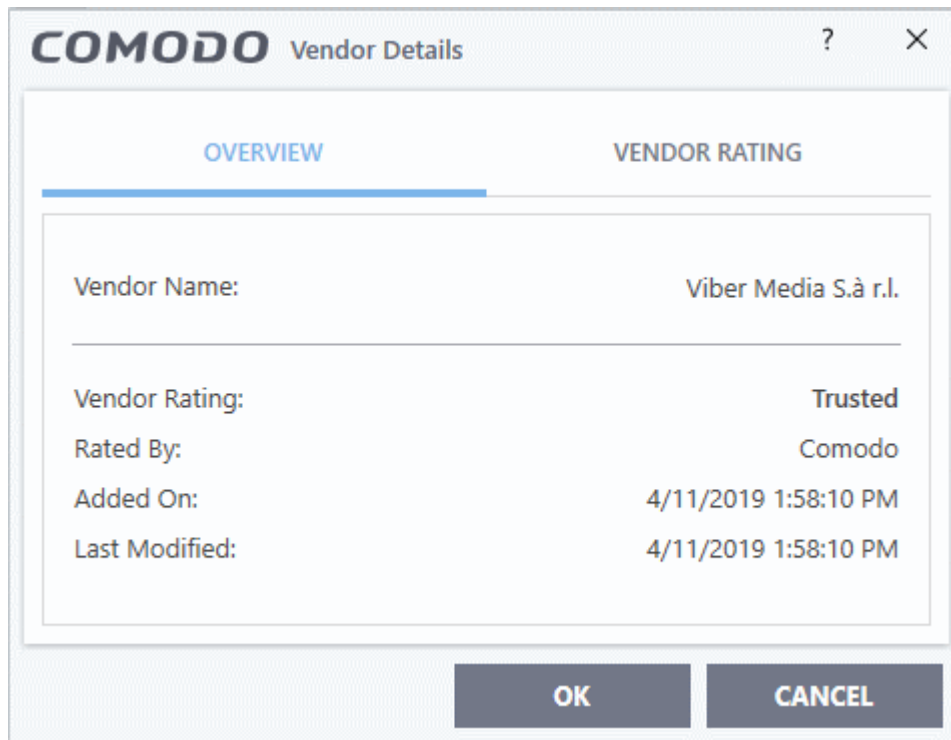
Vendor Rating

The 'Vendor Rating' tab shows the vendor's current trust rating from Comodo and lets you set your own rating:
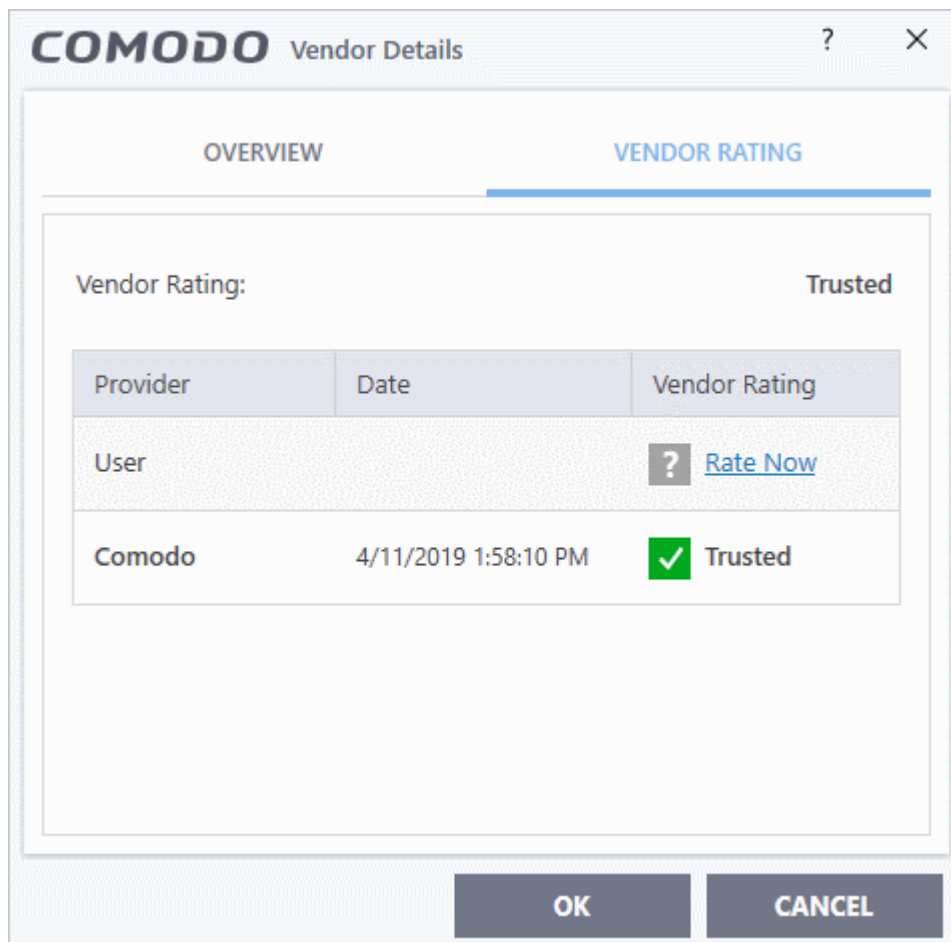
Change the user rating of the file

- Select the vendor from the 'Vendor List' pane and click the 'Vendor Details' button
- Click the 'Vendor Rating' tab from the 'Vendor Details' pane
- Click the 'Rate Now' link beside 'User' and choose the rating from the drop-down
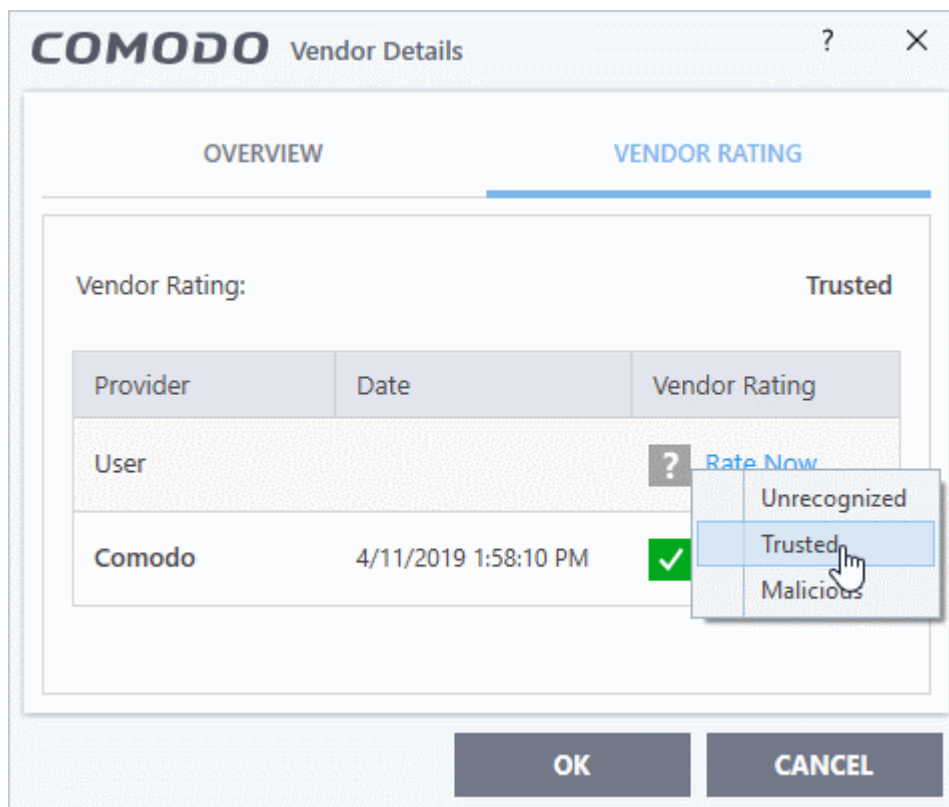
- Click 'OK'
- The trust rating of the vendor will be updated with the user rating in the 'File List' interface.
- You can change the rating for the vendor at anytime by following the same process

Tip: Alternatively, right click on a selected vendor, 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.

Perform an online lookup for vendors

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'Vendor List'
- Select vendor(s) and click the 'Look Up...' button
- Alternatively right-click on a vendor and select 'Look up...'

Comodo servers will be contacted immediately to conduct a search of Comodo's trusted vendor list database to check if any information is available about the vendor in question and the results will be displayed.
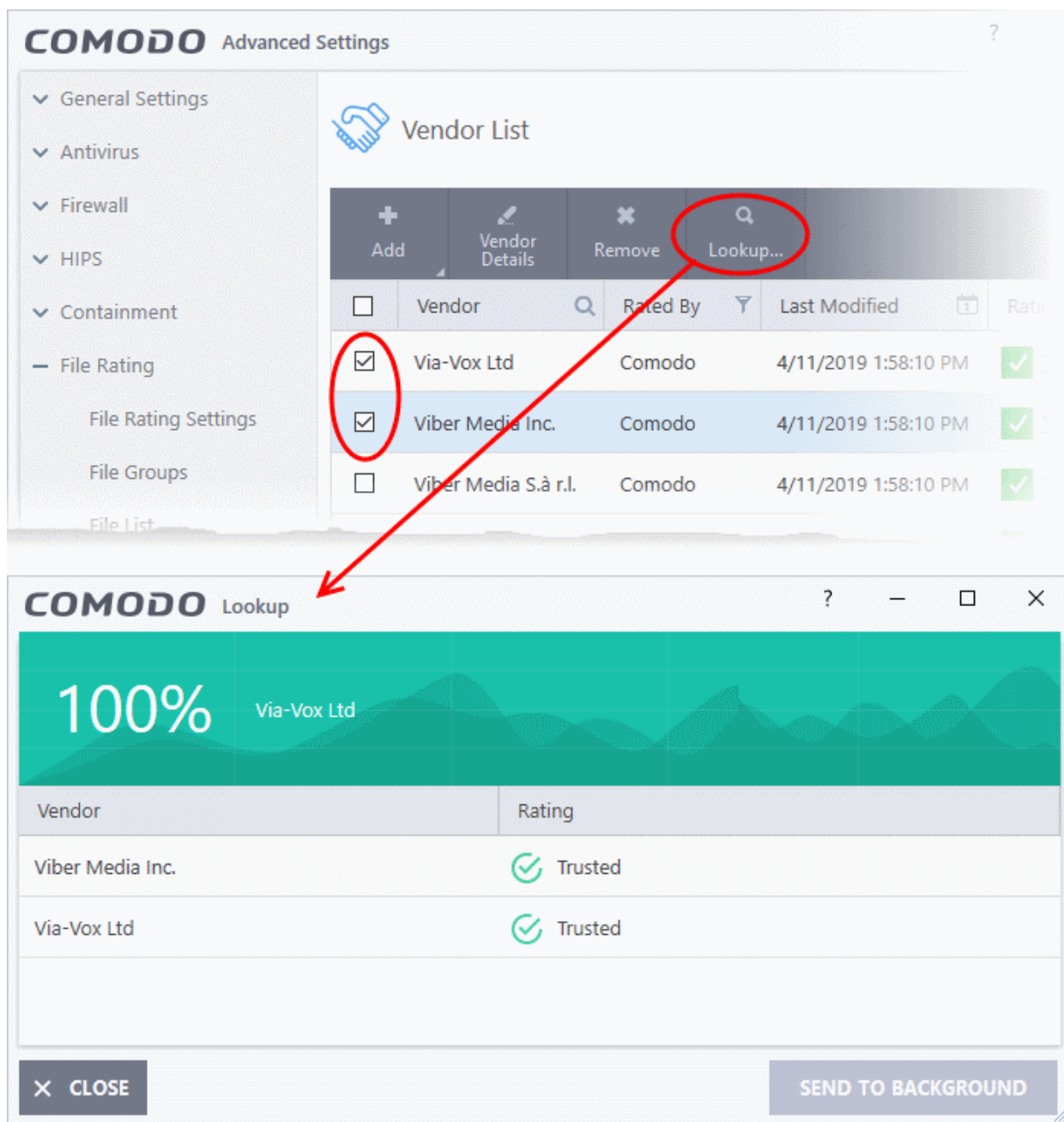
Remove vendors from the list

- Click 'Settings' on the CIS home-screen
- Click 'File Rating' > 'Vendor List'
- Select vendor(s) and click the 'Remove' button
- Alternatively right-click on a vendor and select 'Remove'

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 vendor list.

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'. 'Sectigo', 'Identrust' and 'Digicert' are examples of trusted CA's authorized to counter-sign 3rd party software. The counter-signature is critical to the trust process, so a CA only counter-signs a certificate after conducting strict background checks on the vendor.

If a file is signed by a vendor with 'Trusted' rating in the vendor list and the user has 'Rate applications according to their vendor rating' in the 'File rating Settings' then it will be automatically trusted by Comodo Internet Security.

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 executable for Comodo Internet Security is called 'cis.exe', which has been counter-signed by Sectigo certificate authority.

- 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 vendor list

- 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.

- 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 Internet 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:
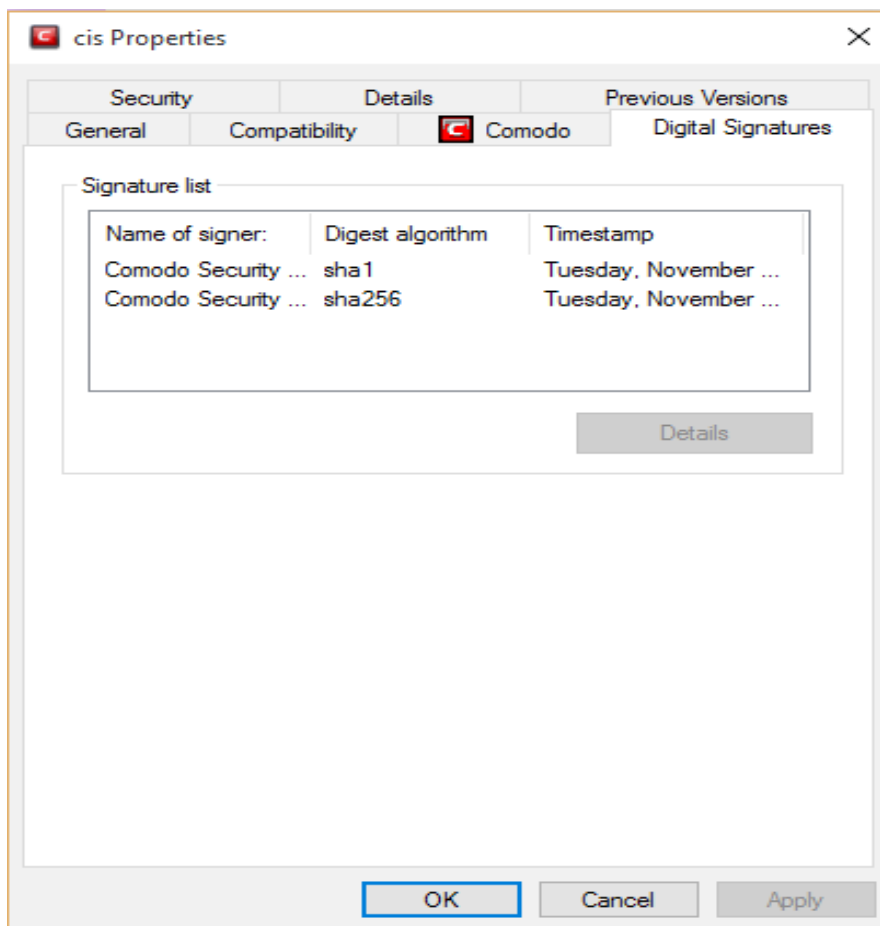
Click the 'Details' button to view certificate details. Click the 'View Certificate' button to inspect the actual code signing certificate. (see below).
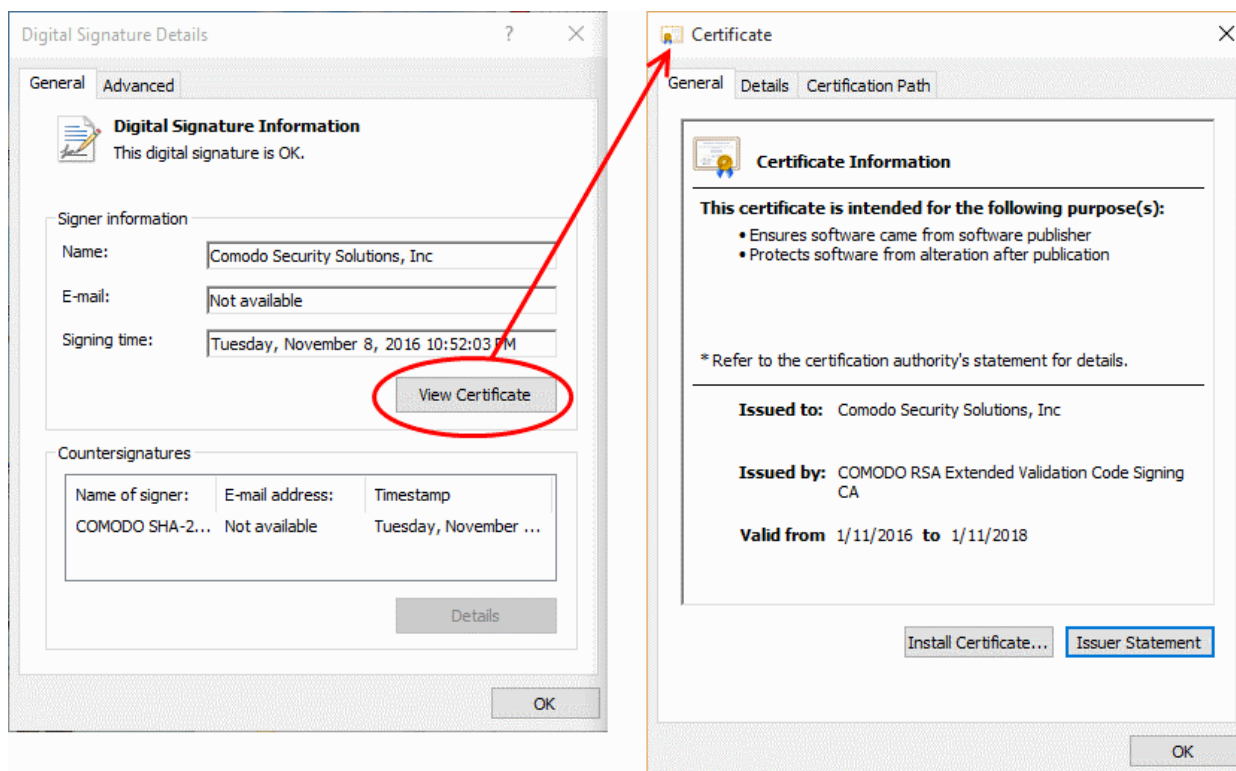
It should be noted that the example above is a special case in that Comodo, as creator of 'cis.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default 'Vendor List' with 'Trusted' status 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 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 modules
- Specify items you want to exclude from detection during a virus scan
- Configure heuristic command line analysis and embedded code detection on files that can execute code
- Configure miscellaneous settings.

Open the 'Advanced Protection' area

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' on the left:
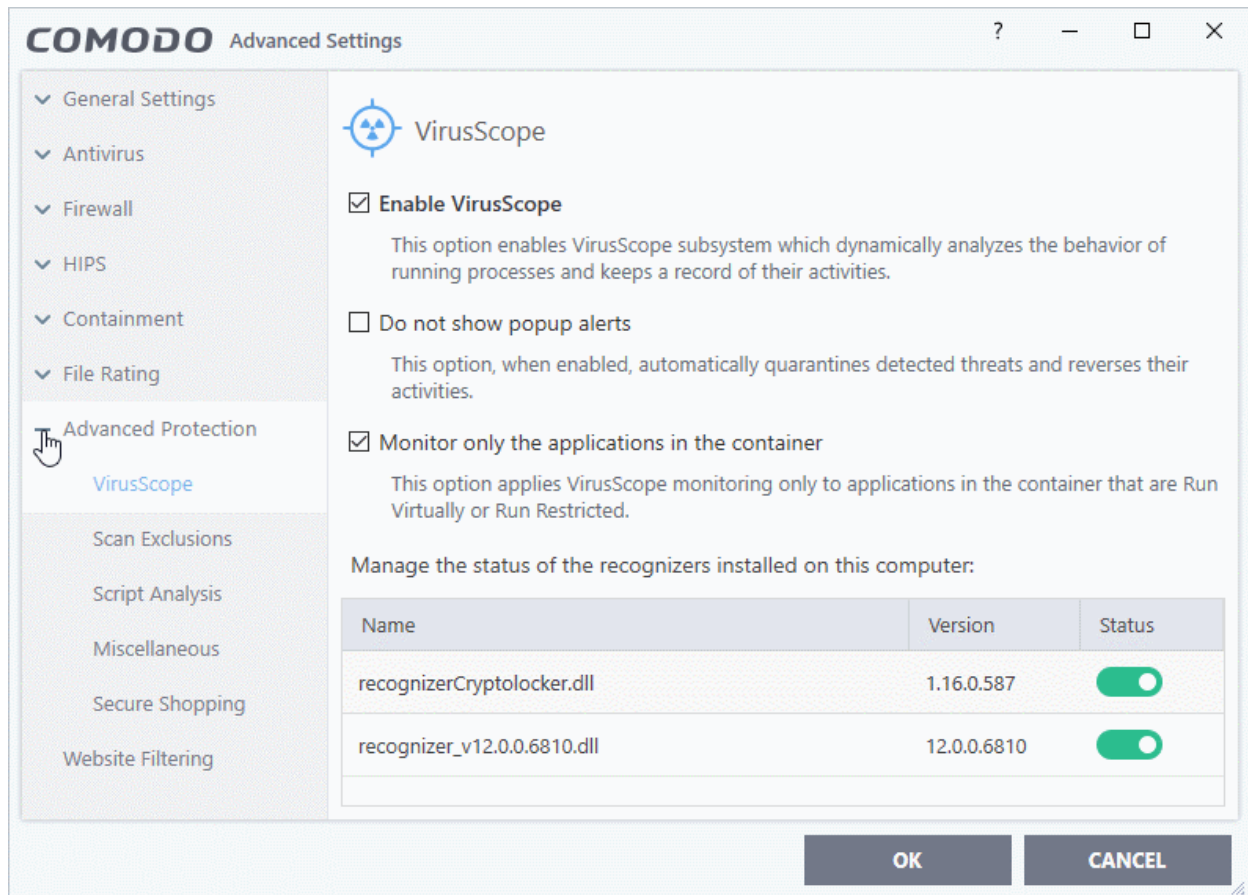
Click the following links to jump to the section you need help with:

- **VirusScope Settings** - Configure VirusScope behavior

- **Scan Exclusions** - Add and manage items that should be ignored during a scan

- **Script Analysis Settings** - Manage heuristic command line analysis and embedded code detection.

- **Miscellaneous Settings** - Exclude files from buffer overflow monitoring, configure browser alerts, and more

- **Secure Shopping Settings** - Create a secure place to work and go online

6.7.1. VirusScope Settings

Click 'Settings' > 'Advanced Protection' > 'VirusScope'

- 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 also allows you to reverse the actions of software without blocking the software itself. 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.
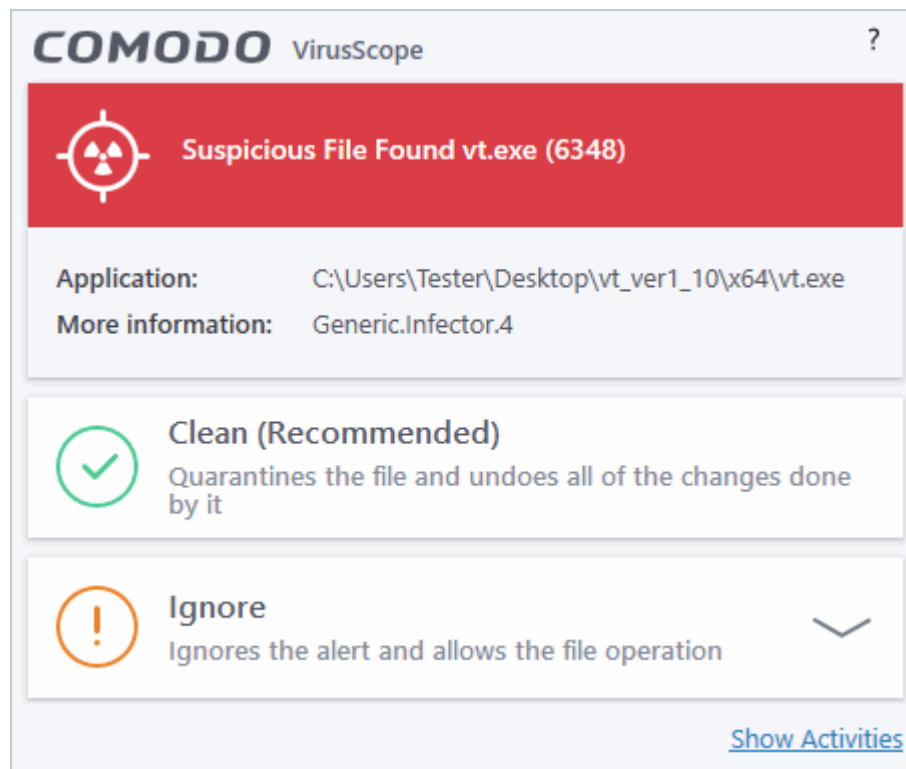
Open the 'VirusScope' settings section

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'VirusScope':
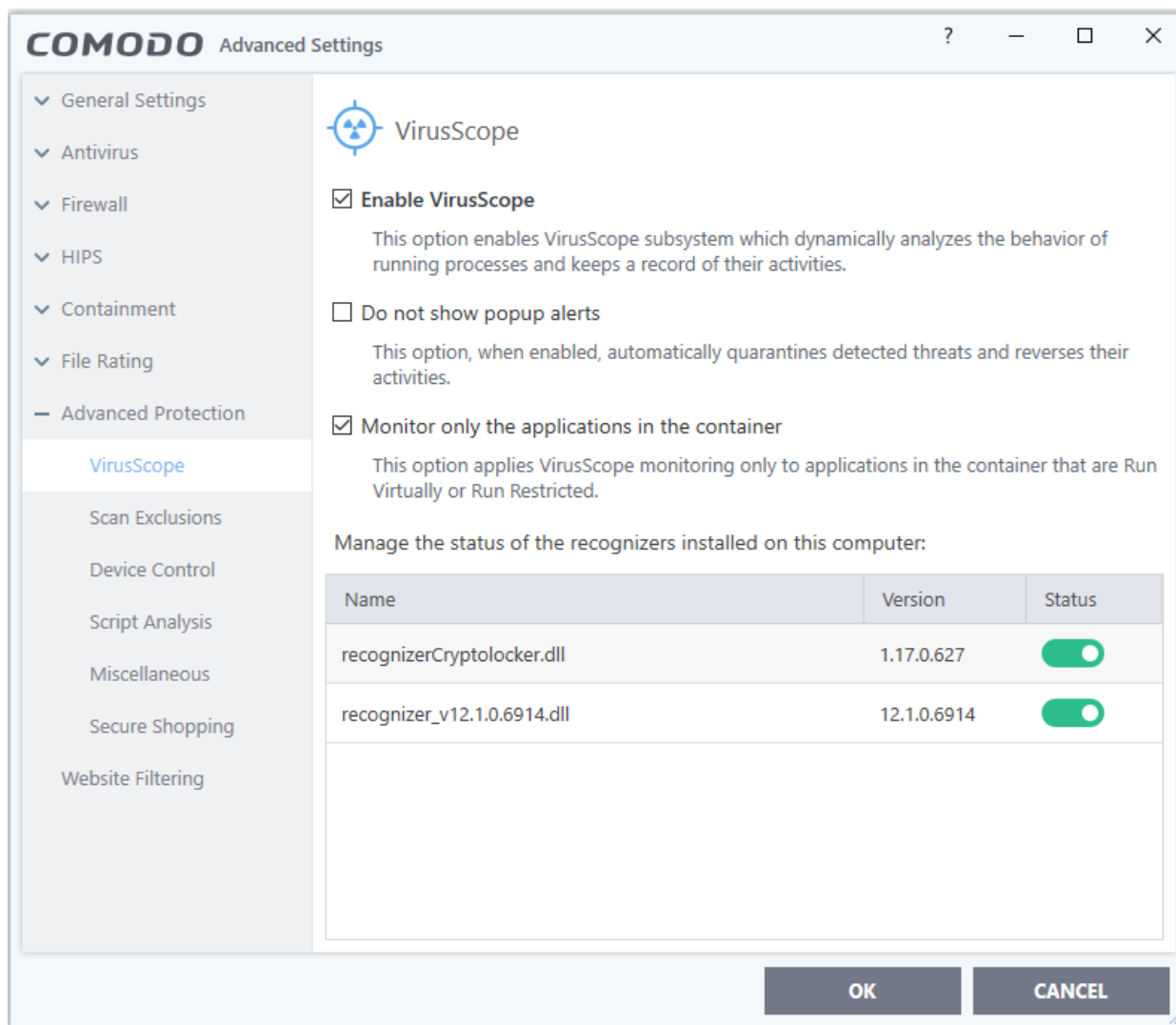
VirusScope Settings

VirusScope monitors running processes and alerts you to suspicious activity. You then have the option to quarantine the suspicious file and undo its activities.

- **Enable VirusScope** - Activate 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** - Whether CIS should show an alert if VirusScope detects suspicious activity. (*Default = Disabled*)

  - If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed.

- **Monitor only the applications in the container** - VirusScope only tracks the activities of processes that a running in the container. It will not track processes directly running on the host (Default = Enabled)

- Applications can be made to run in the container in two ways:

  - Run a program in the container on a 'one-off' basis. See **Run an Application in the Container** for more details.

  - Create a rule to auto-contain programs that match certain criteria. See **Auto-Containment Rules** for more details.

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.
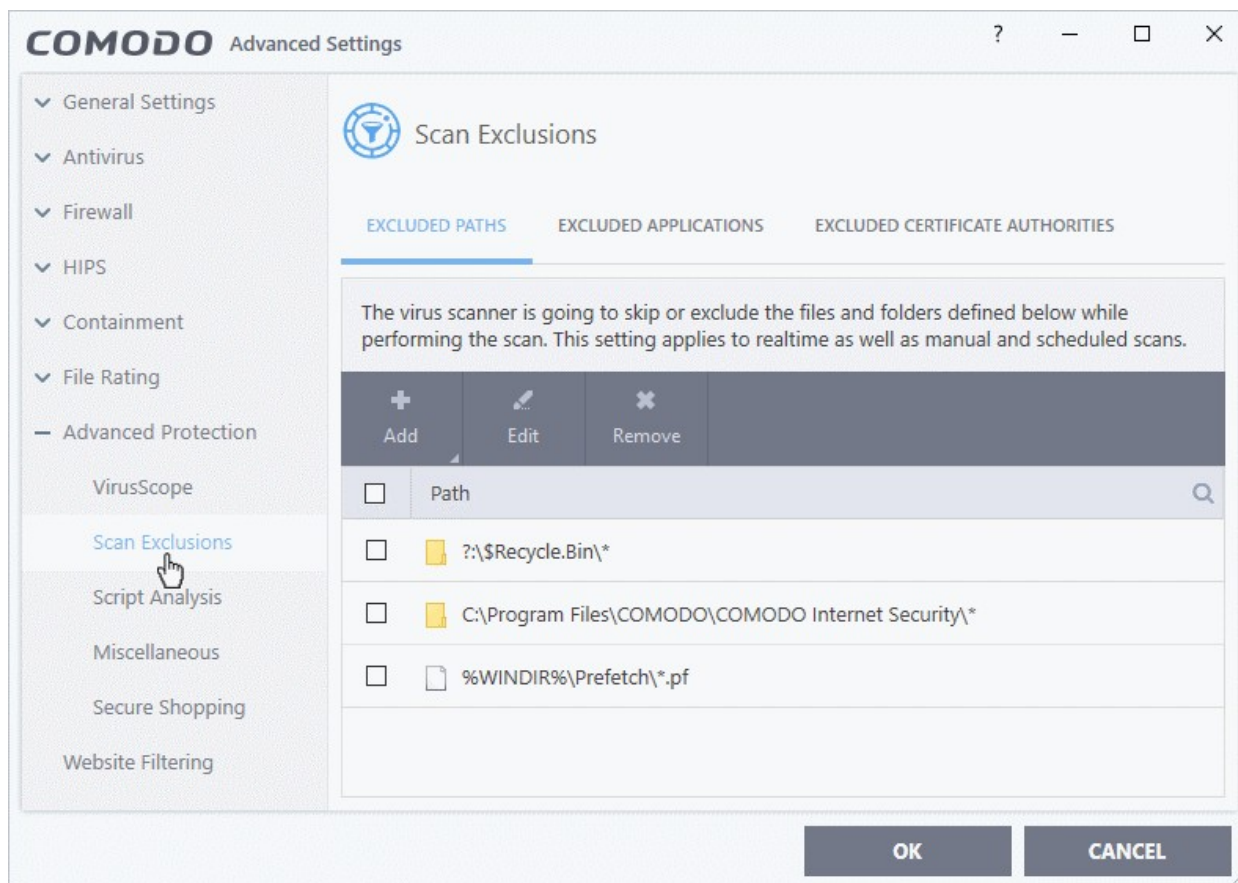
6.7.2. Scan Exclusions

Click 'Settings' > 'Advanced Protection' > 'Scan Exclusions'

- The 'Scan Exclusions' panel shows files, paths and certificate authorities which you have chosen to skip during a virus scan.

- CIS will not generate an alert for an excluded item, even if the item is rated as malicious in the global blacklist.

- Items may have been added to this list because you selected 'Ignore' at the scan results window, or because you added them to exclusions at an alert.

Open the scan exclusions panel

- Click 'Settings' at the top to open the 'Advanced Settings' interface

- Click 'Advanced Protection' > 'Scan Exclusions' on the left


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 '**Exclude 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 '**Exclude 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 '**Exclude Certificate Authorities from certificate scans**' for more details.

Exclude Drives/Folders/Files from all types of scans

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click the 'Add' button:
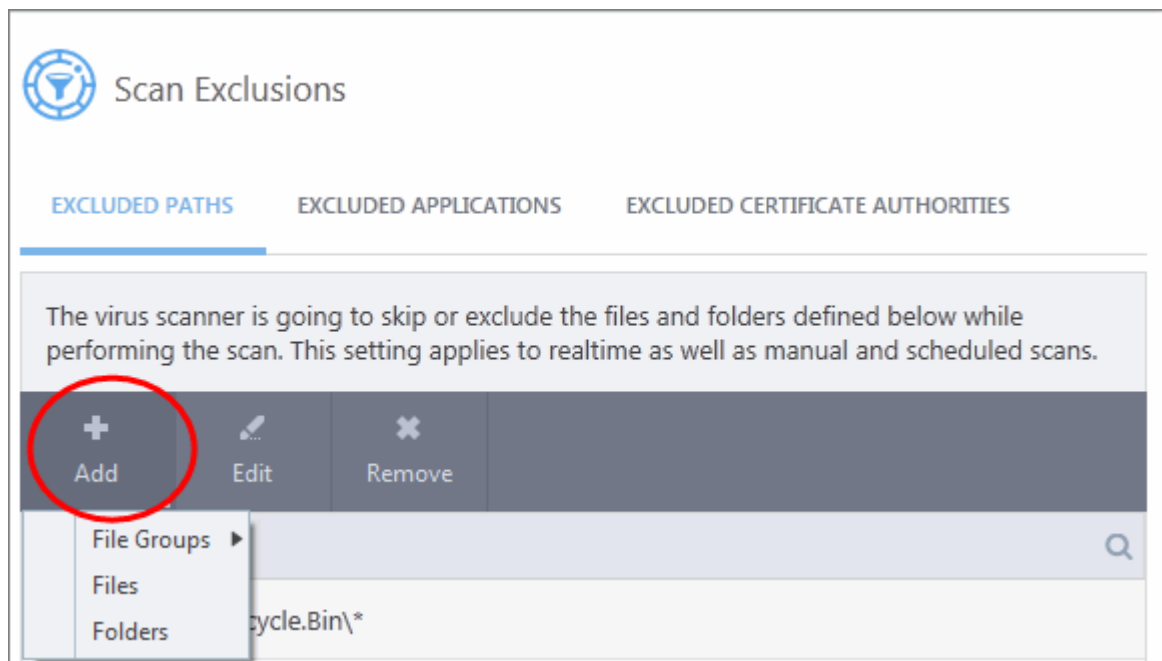
You can add a:

- **File Group**
- **Drive partition/Folder**

    OR
- **An individual file**

Add a file group

- Choose 'File Groups' 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'.
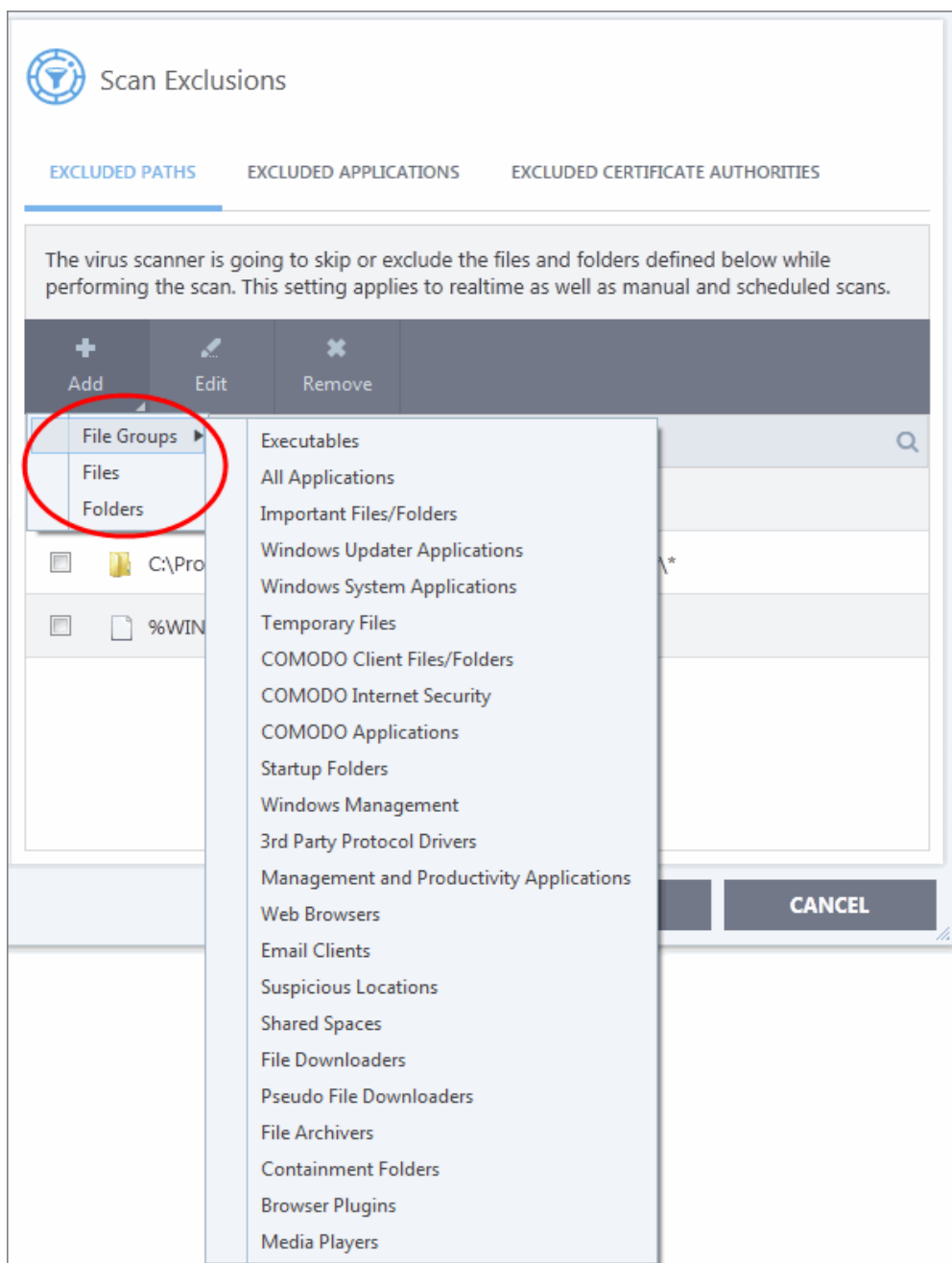
- CIS ships with a set of predefined file groups which can be viewed in 'Advanced Settings' > 'File Rating' > 'File Groups'.
- You can also add new file groups as required. See **File Groups** for more details.

Add new file groups to exclusions

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Click 'Add' > 'File Groups'
- Select the target file group from the list:
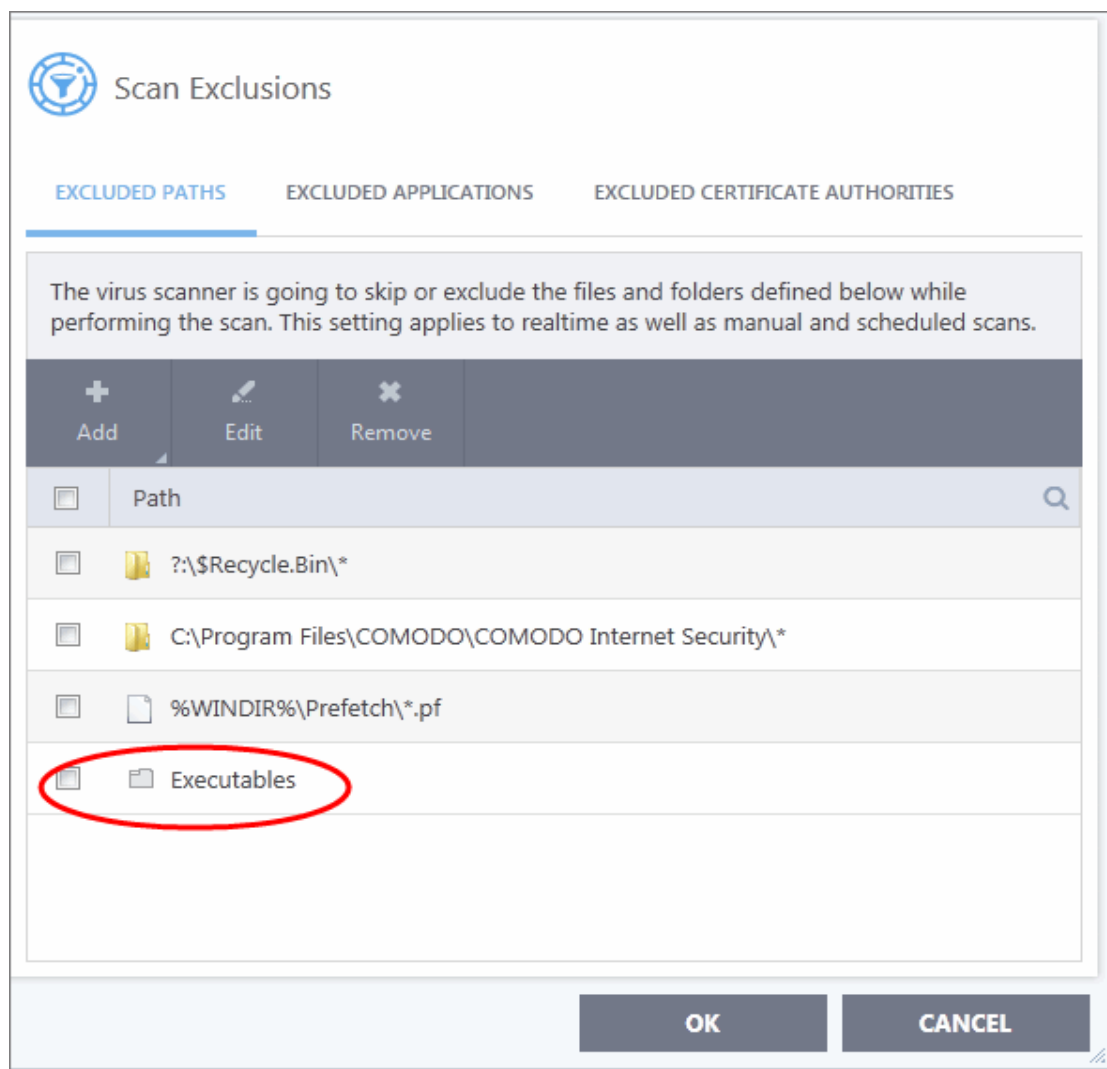
- Repeat the process to add more file groups.
- Items added to the 'Excluded Paths' will be omitted from all types of future Antivirus scans.

Add a drive partition / folder

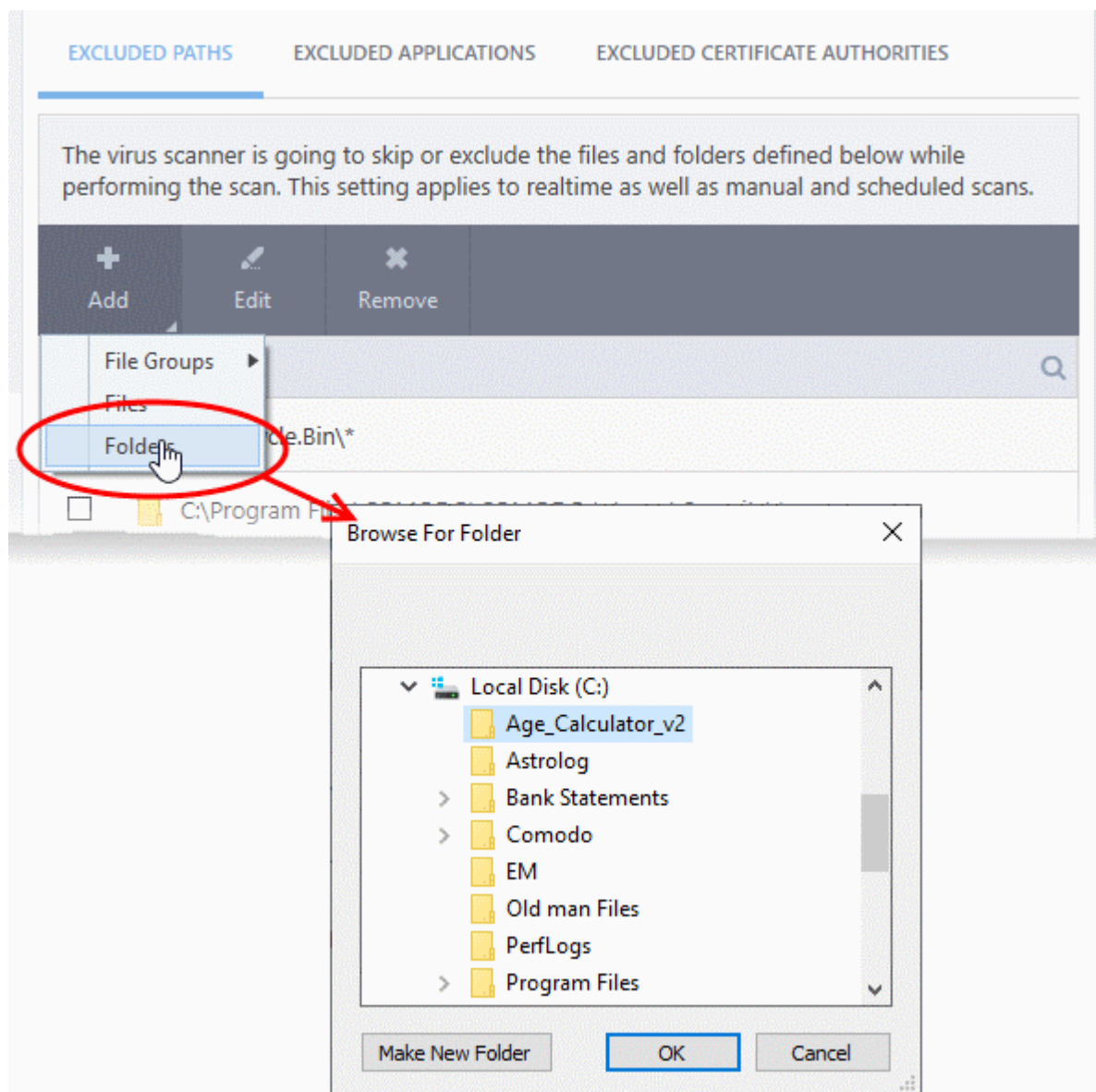- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Click 'Add' > 'Folders'
- Navigate to the drive partition or folder you want to add to excluded paths and click 'OK'.

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

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

Add an individual file

You can specify even individual files as excluded path.

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > '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:

- Repeat the process to add more files.
- Items added to 'Excluded Paths' will be omitted from all types of virus scan in the future.

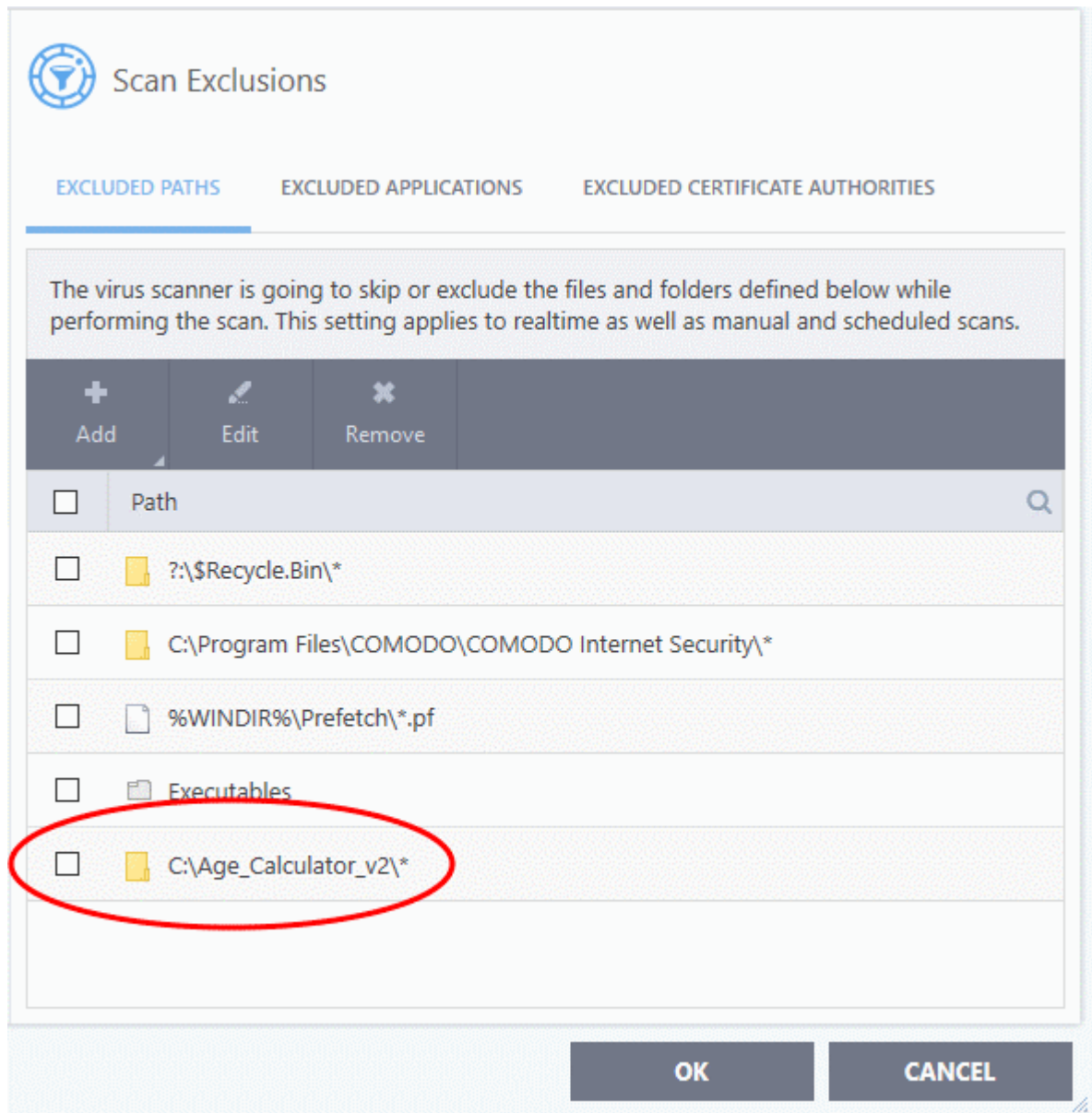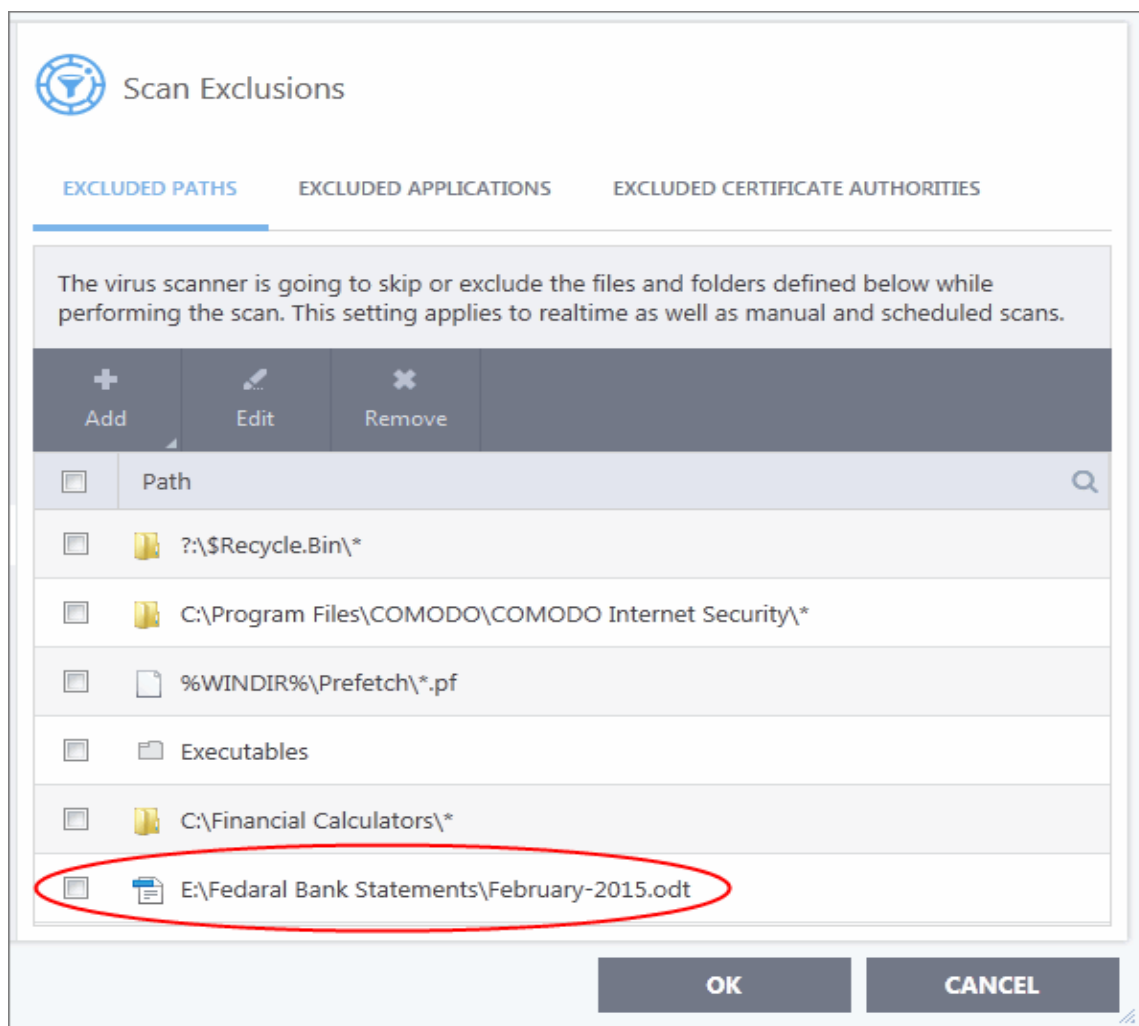**Edit the path of an added item**

- Select the target item and click 'Edit':

- Modify the file-path as required and click 'OK'.

Remove an item from excluded paths

- Select the target item and click 'Remove':
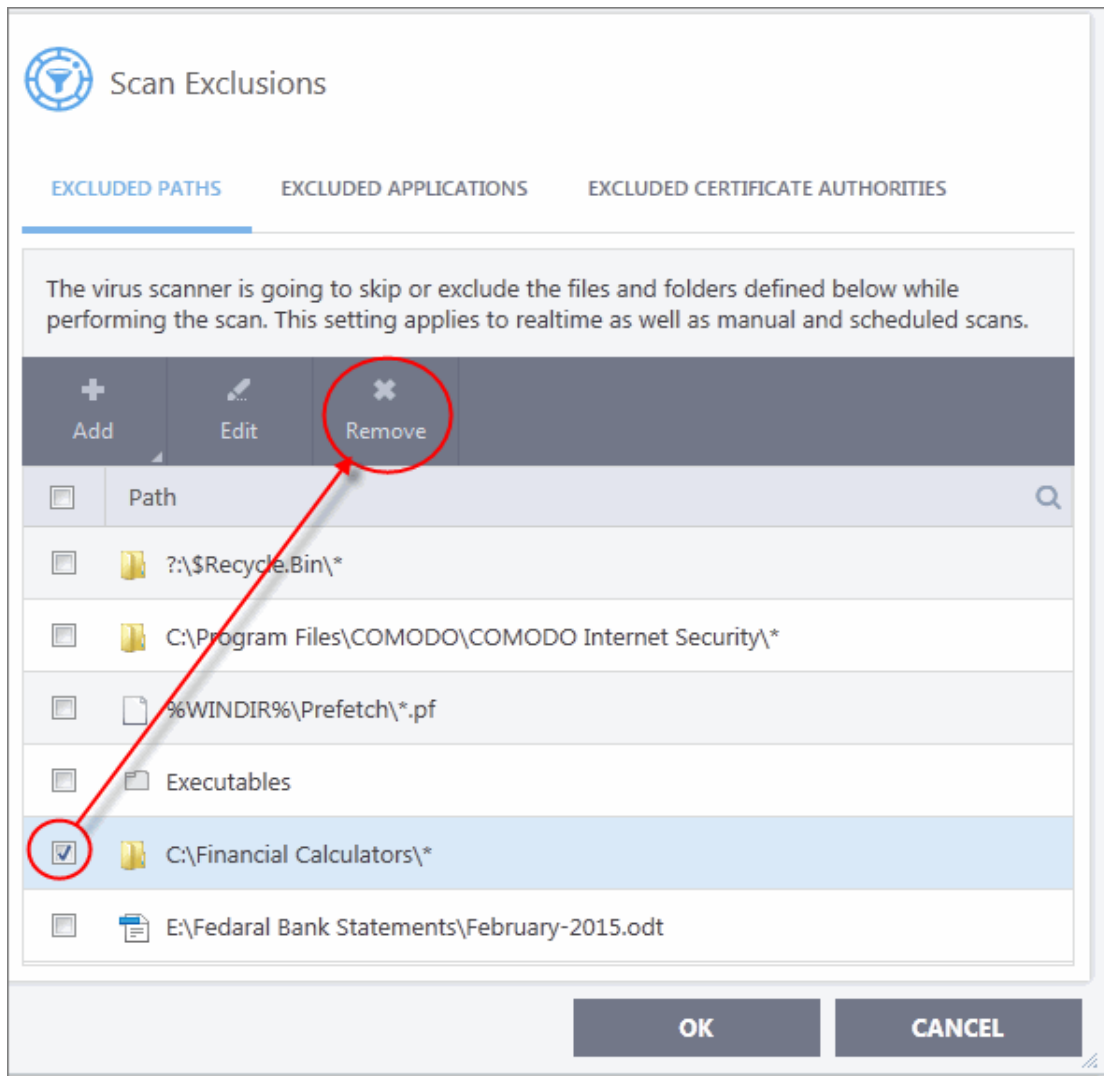
- Click 'OK' for your settings to take effect.

Exclude Programs/Applications from Real-time Scans

- The 'Excluded Applications' screen lets you specify programs which should be skipped by 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

Open excluded applications

- Click 'Settings' on the CIS home screen

- Click 'Advanced Protection' > 'Scan Exclusions'

- Select the 'Excluded Applications' tab:
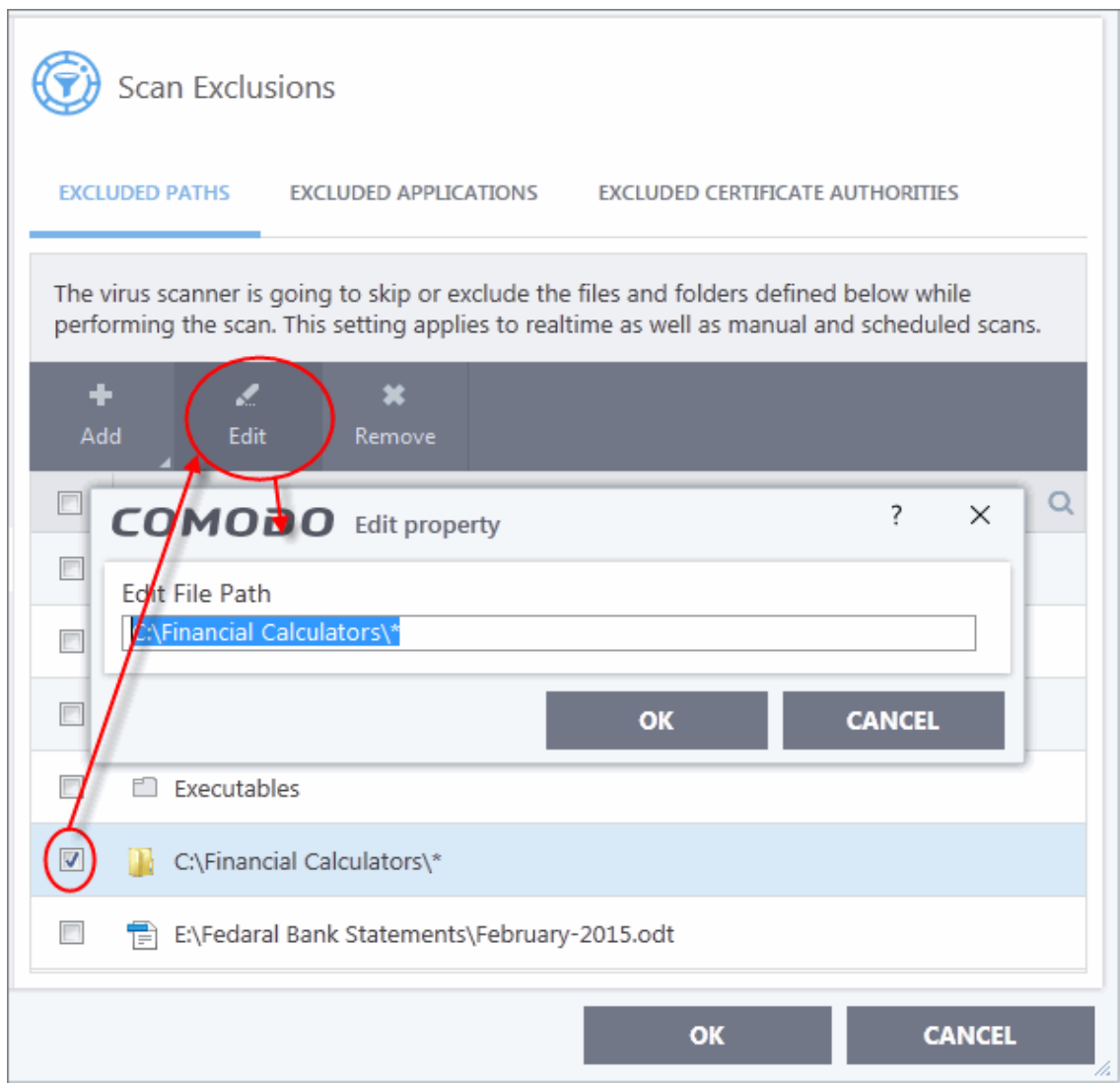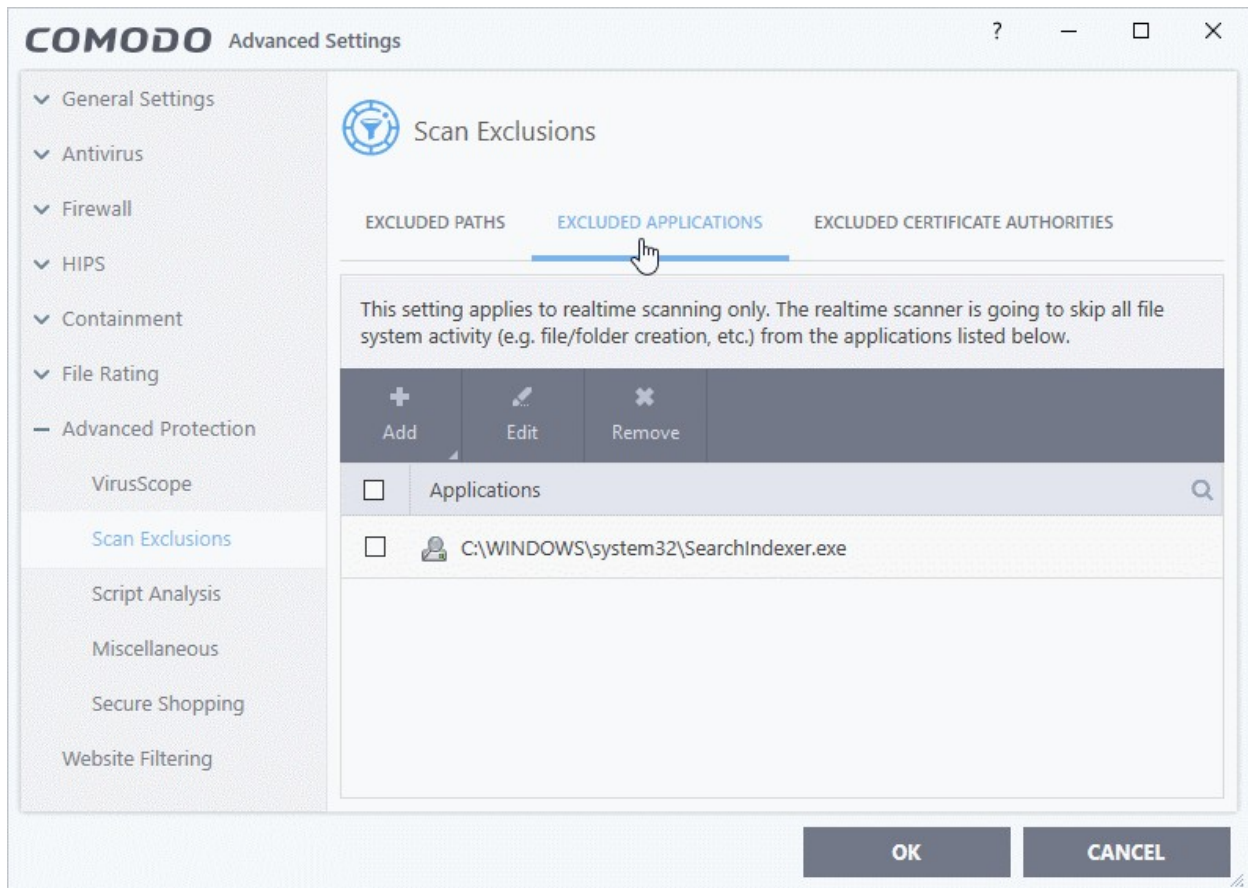
Add an item to excluded applications

- Click 'Settings' on the CIS home screen

- Click 'Advanced Protection' > 'Scan Exclusions'

- Select the 'Excluded Applications' tab

- Click 'Add' at the top of the 'Excluded Applications' pane.
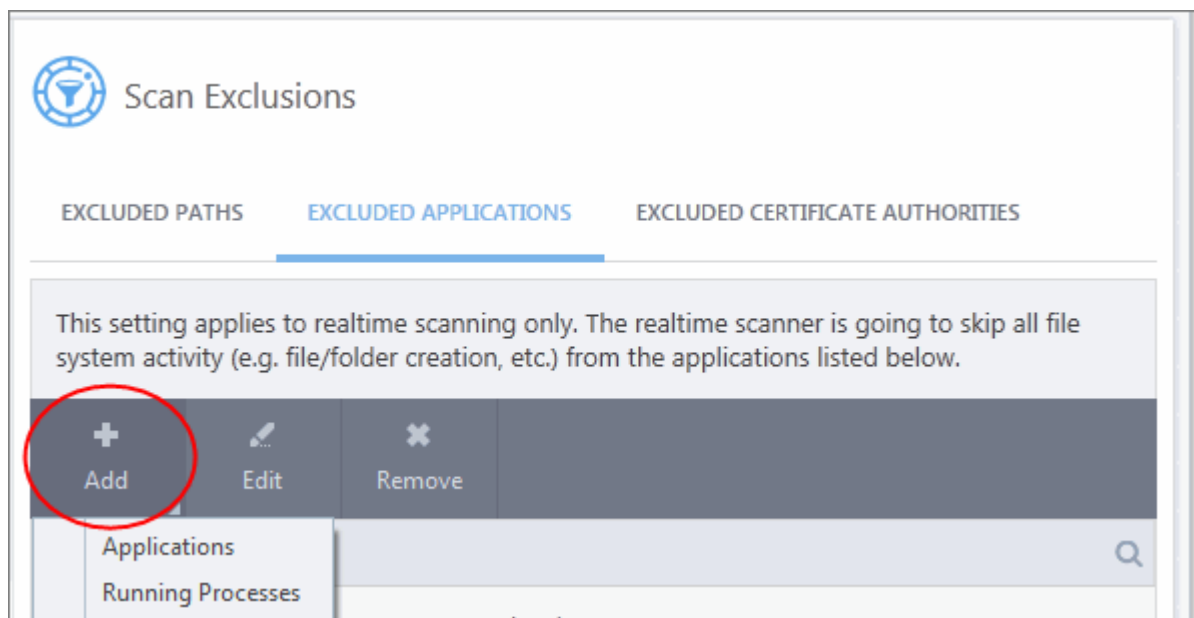
You can choose to add an applications by:

- **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.

Add an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down
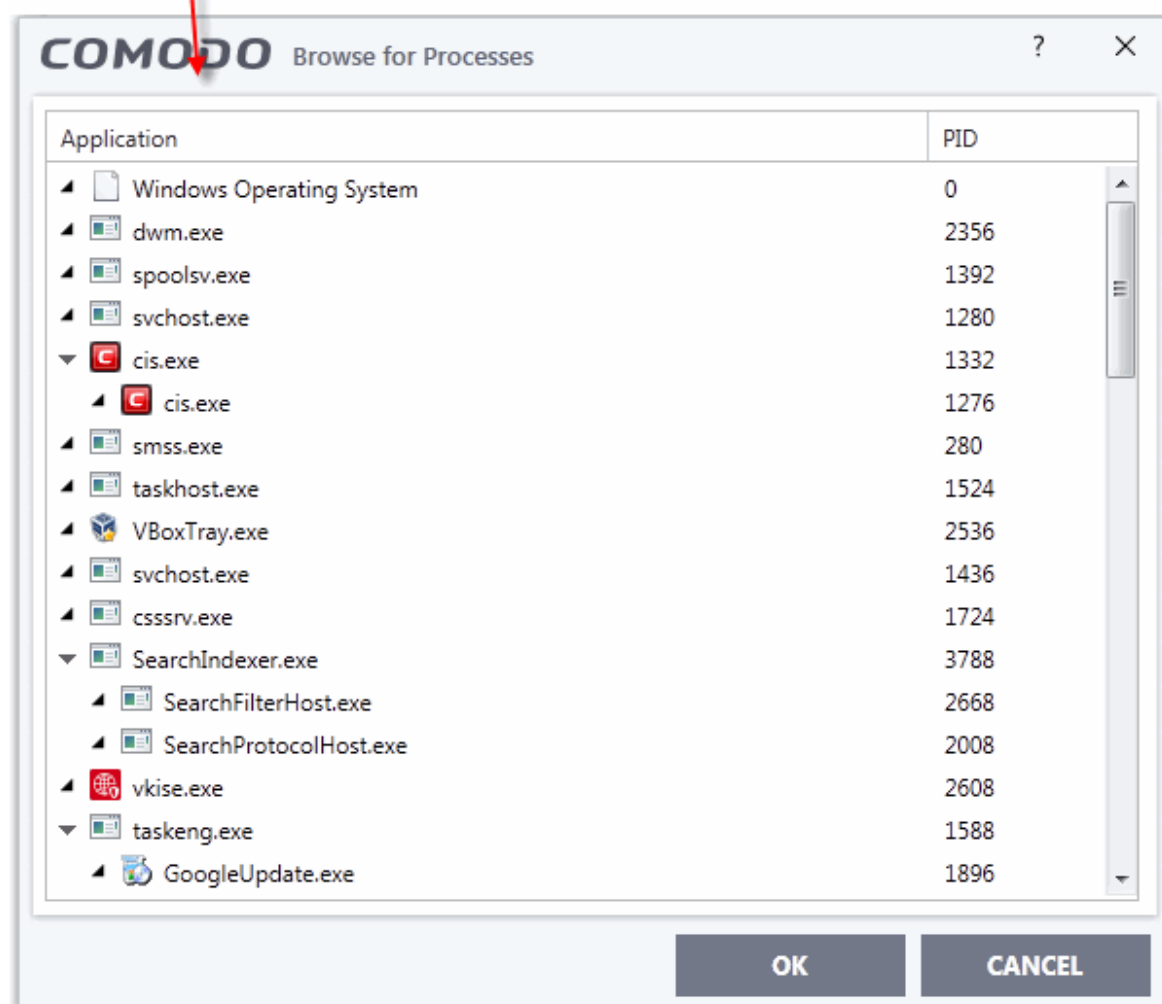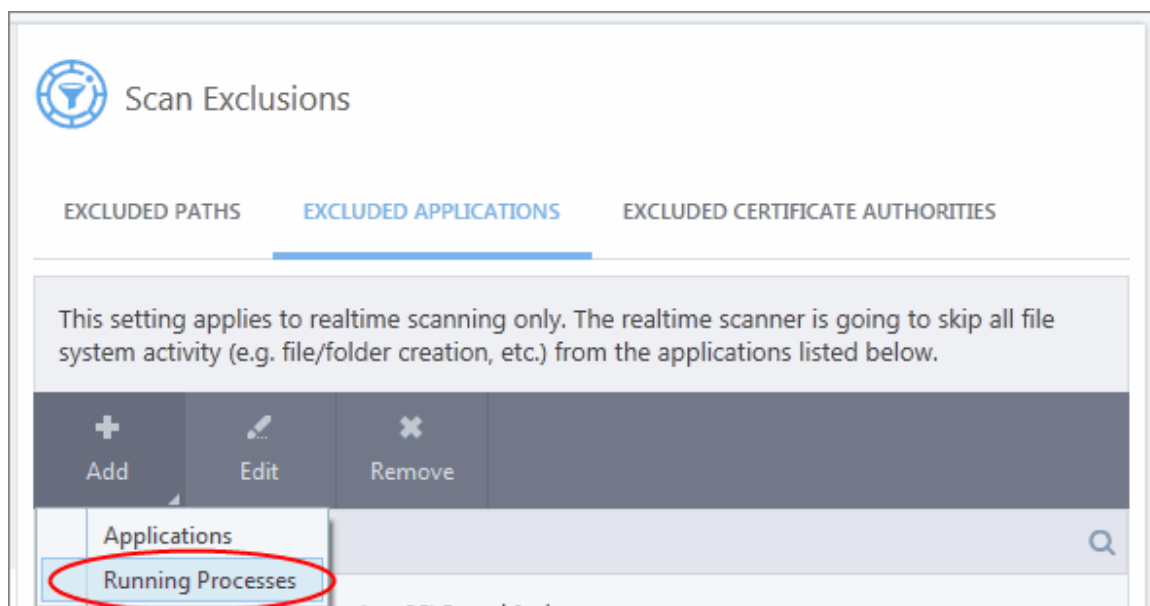
A list of currently running processes in your computer will be displayed:

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

The application will be added to 'Excluded Applications'.

Browse to the application

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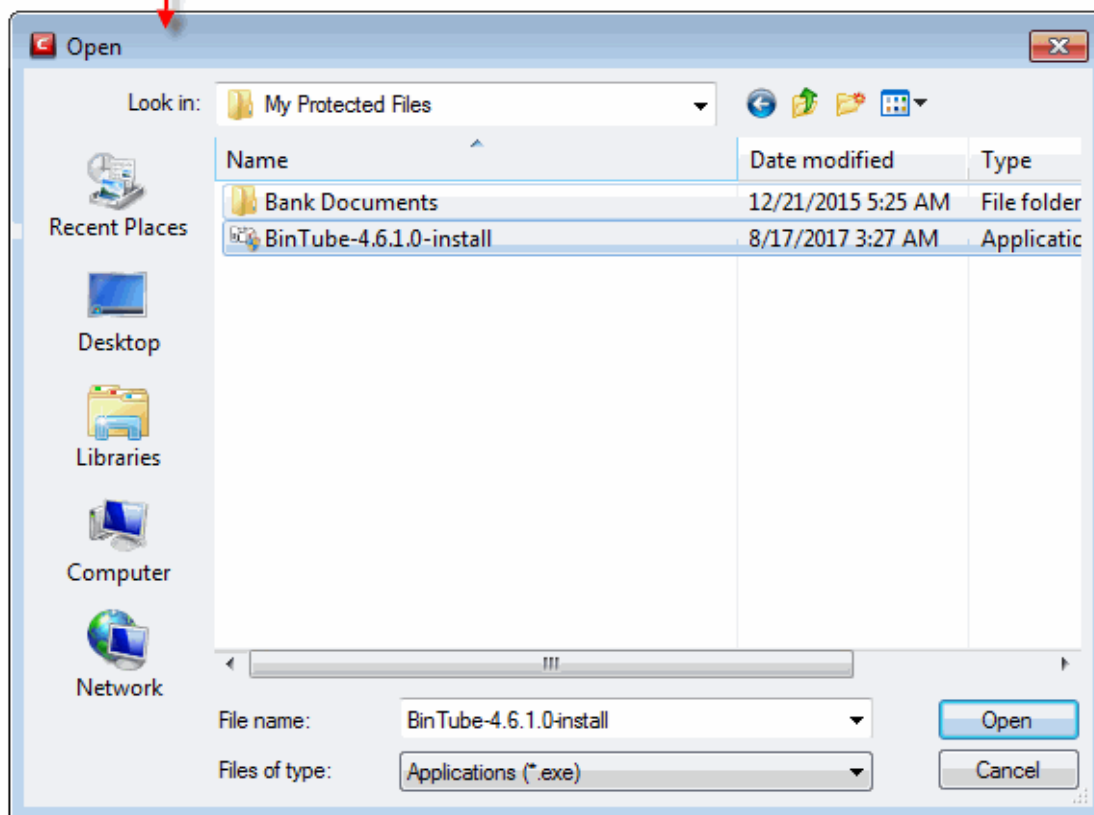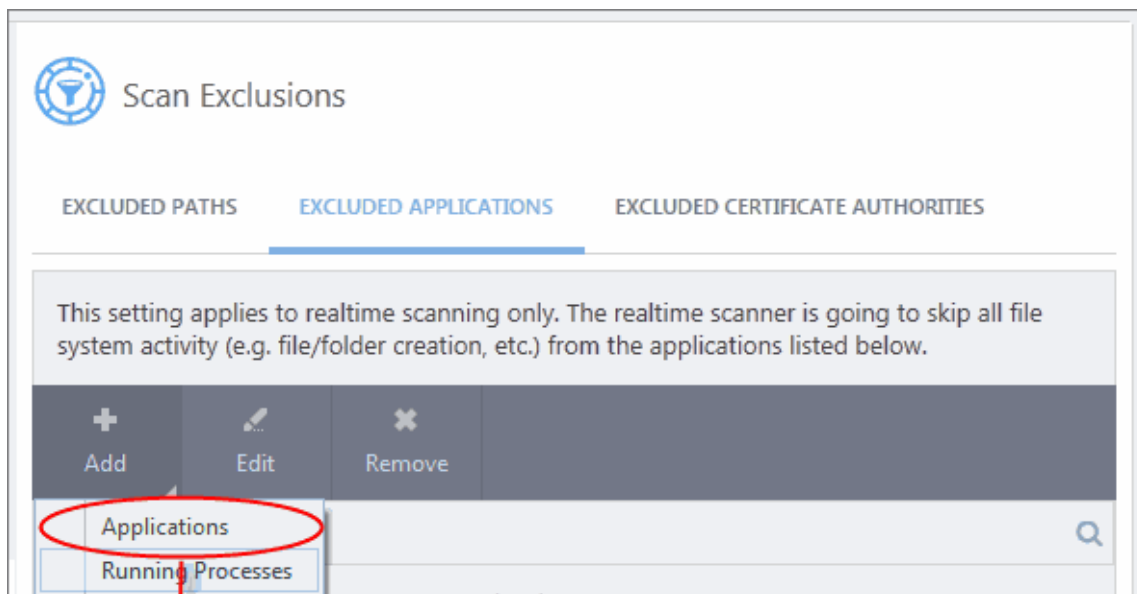
- Navigate to the file you want to exclude and click 'Open'.

The file will be added to 'Excluded Applications'.
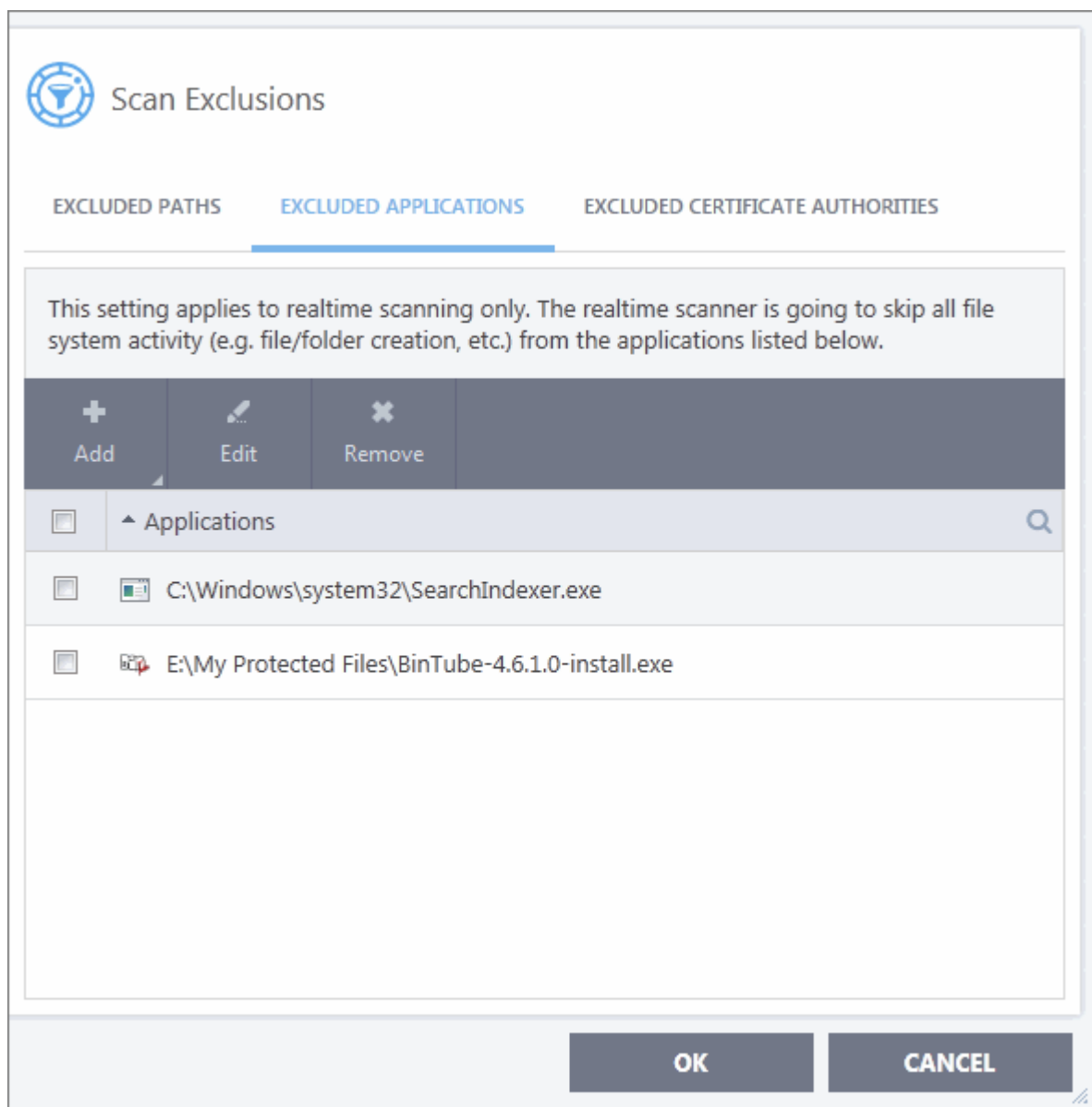
- Repeat the process to add more items. Excluded items will be skipped from future real-time scans.

Edit the path of the application added to excluded applications

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Select the 'Excluded Applications' tab
- Select the application and click 'Edit' at the top.
- Make the required changes for the file path in the 'Edit Property' dialog.
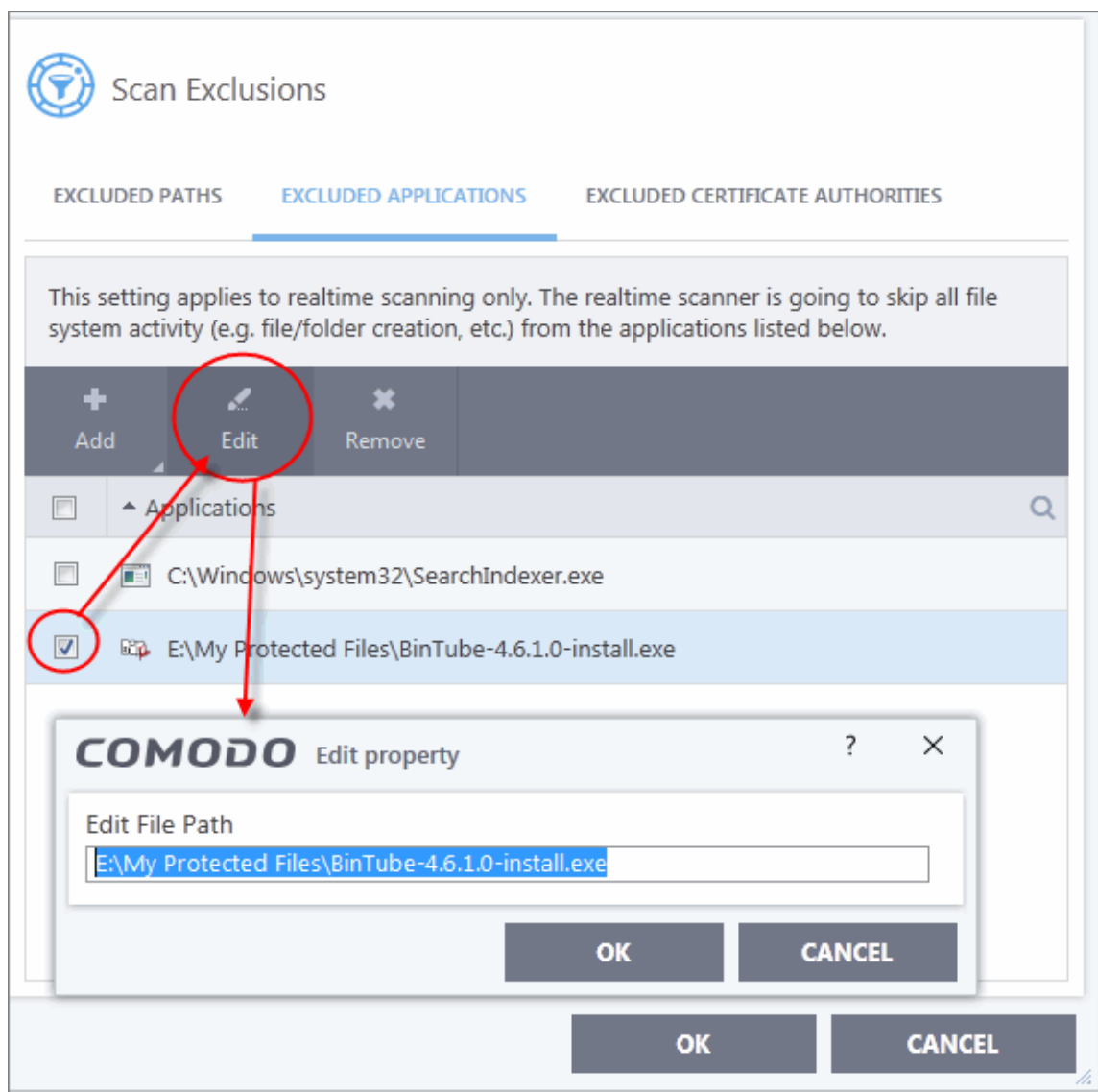
Remove an item from the excluded applications

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Select the 'Excluded Applications' tab
- Select the item and click 'Remove' at the top:
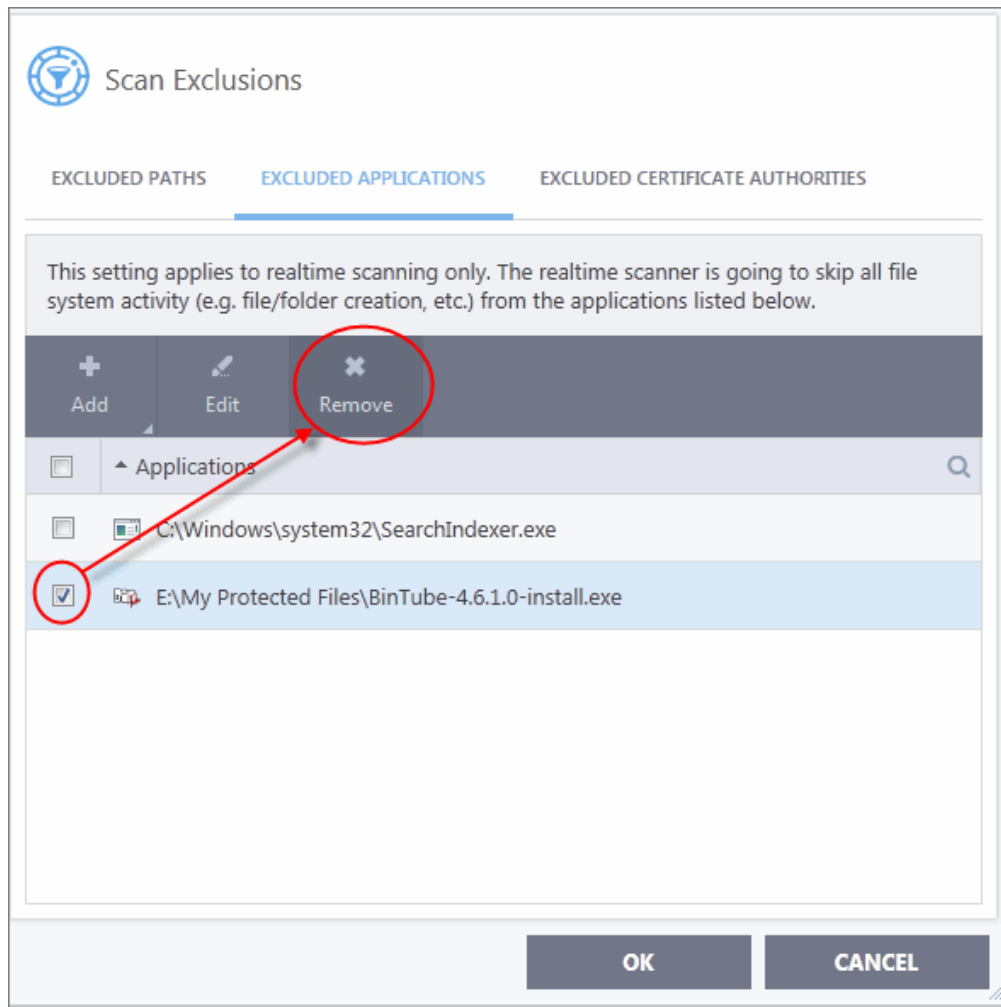
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Exclude Certificate Authorities from Certificate Scans

The 'Excluded Certificate Authorities' screen lets you specify certificate authorities, so that SSL certificates signed by them are skipped from certificate scans.

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Select the 'Excluded Certificate Authorities' tab:
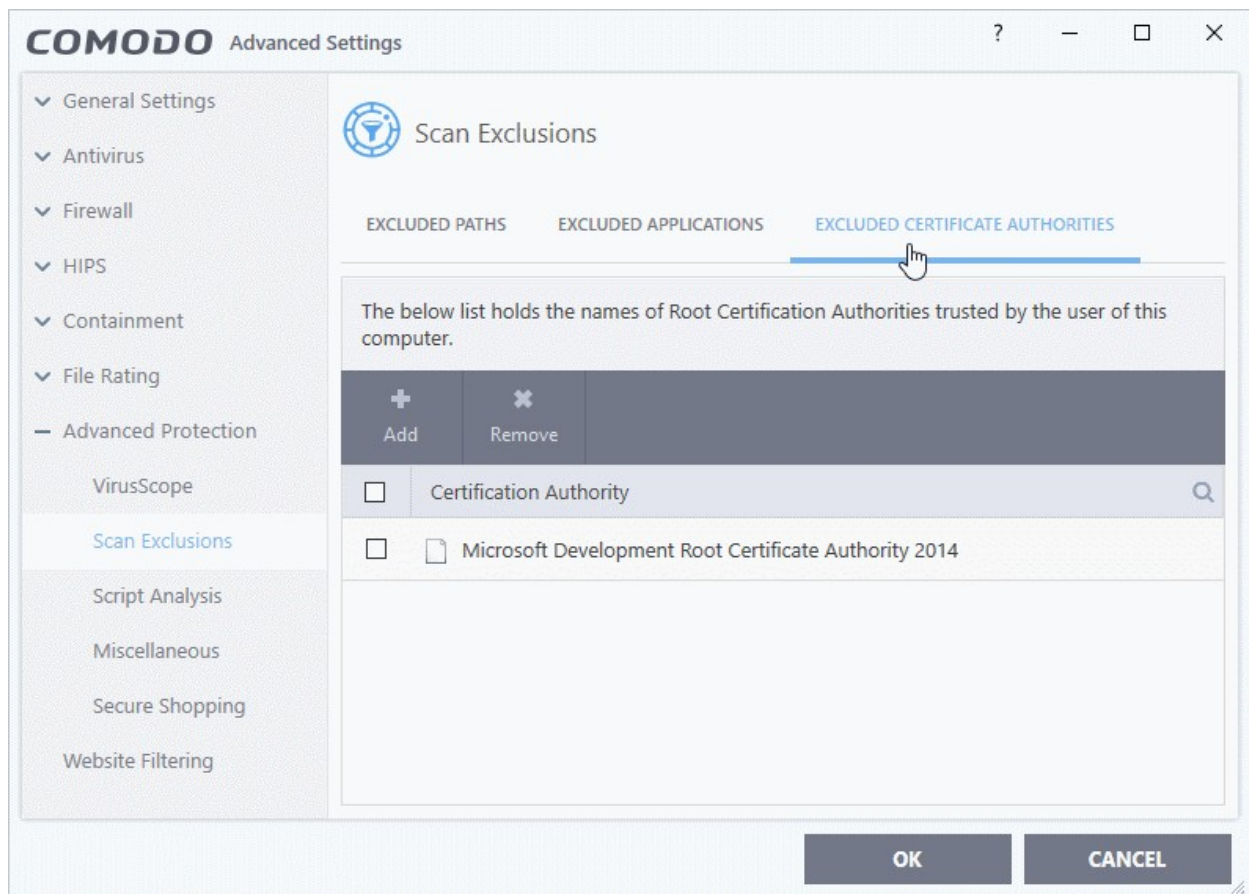
Add a certificate to excluded certificate authorities

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Select the 'Excluded Certificate Authorities' tab:
- Click 'Add' at the top of the 'Excluded Certificate Authorities' pane.
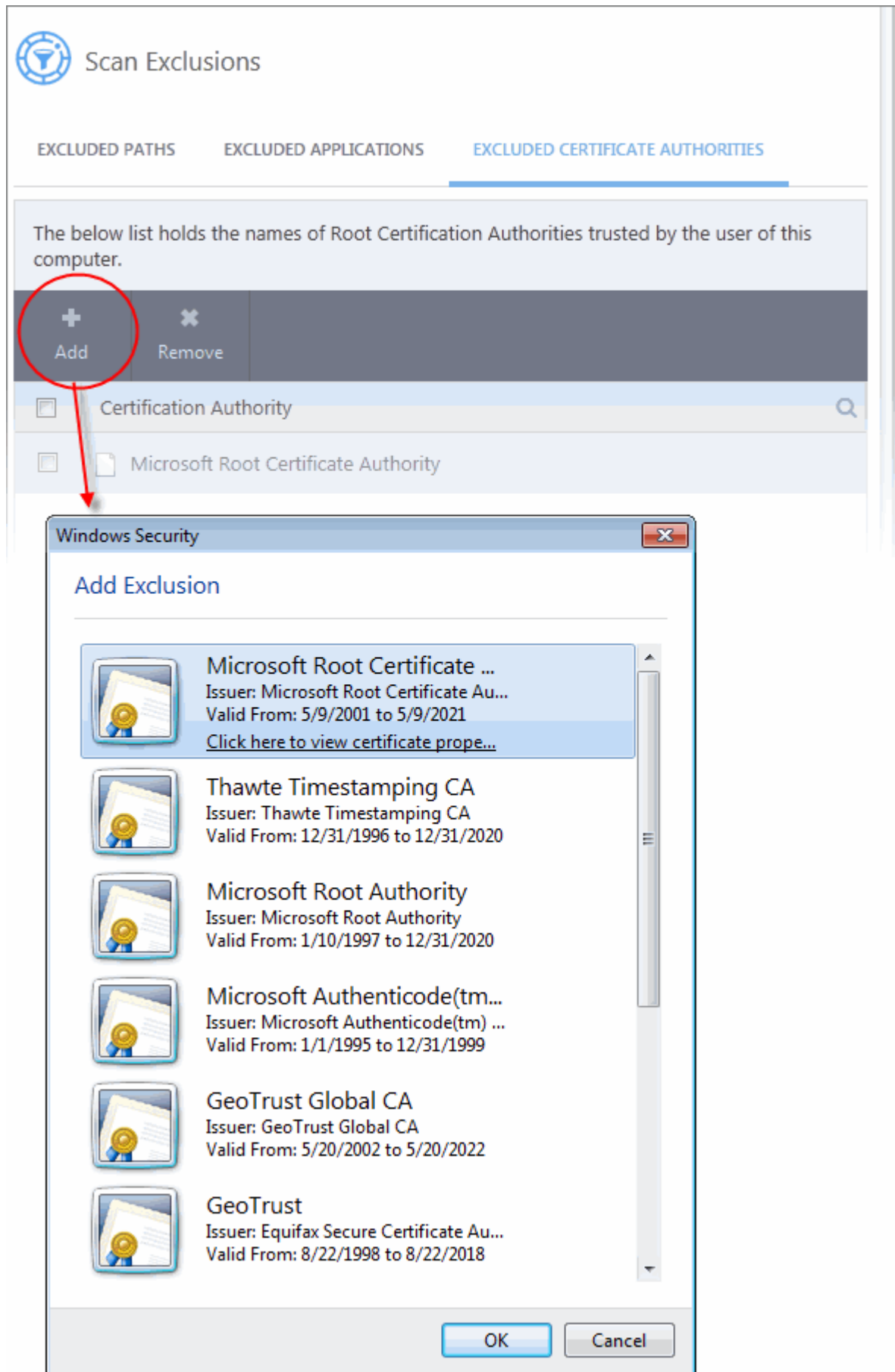
- Select the certificate type to add excluded authorities and click 'OK'
- The certificate will be added to the list of excluded certificates:
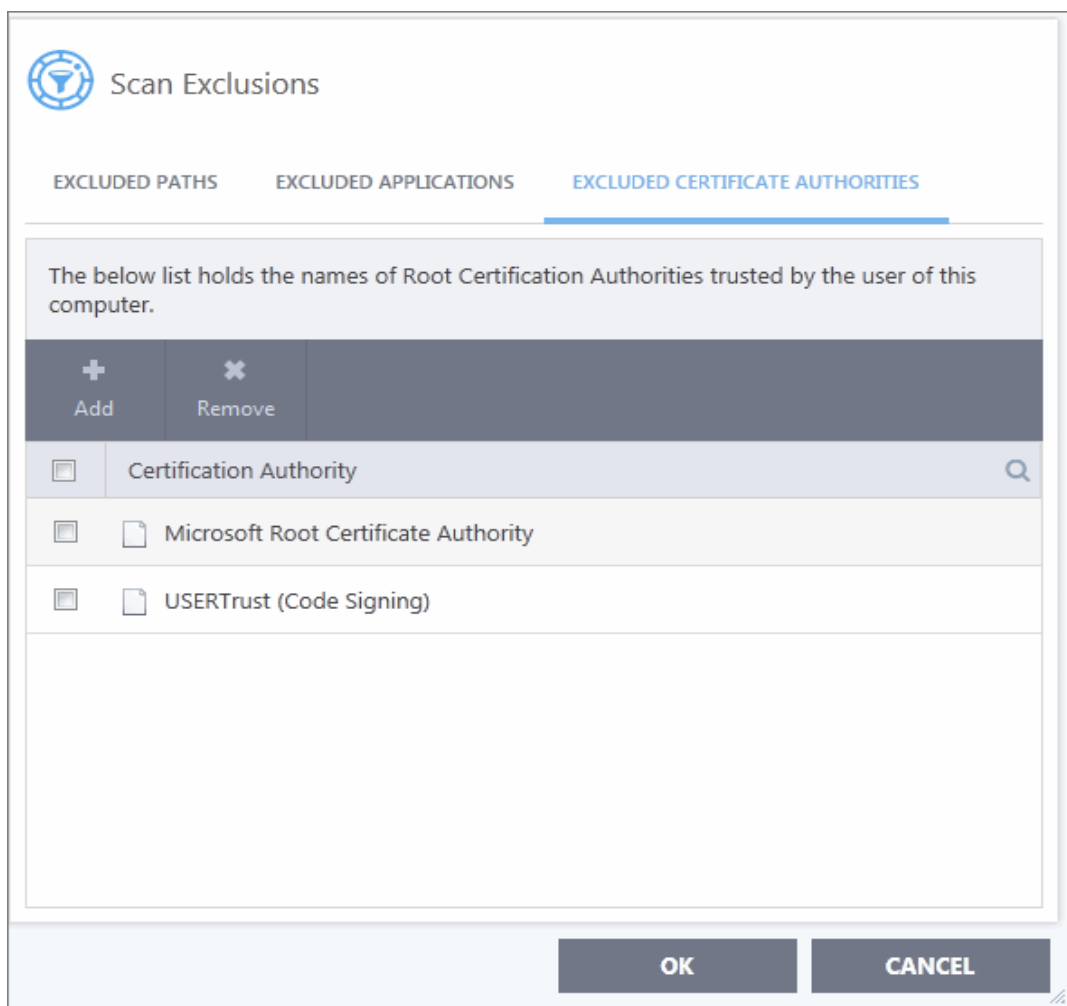
- Repeat the process to add more certificates. Certificates added to 'Excluded Certificate Authorities' will be omitted from certificate scans in future.

Remove an item from the excluded certificate authorities

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Select the 'Excluded Certificate Authorities' tab:
- Select the certificate authority and click 'Remove' at the top:
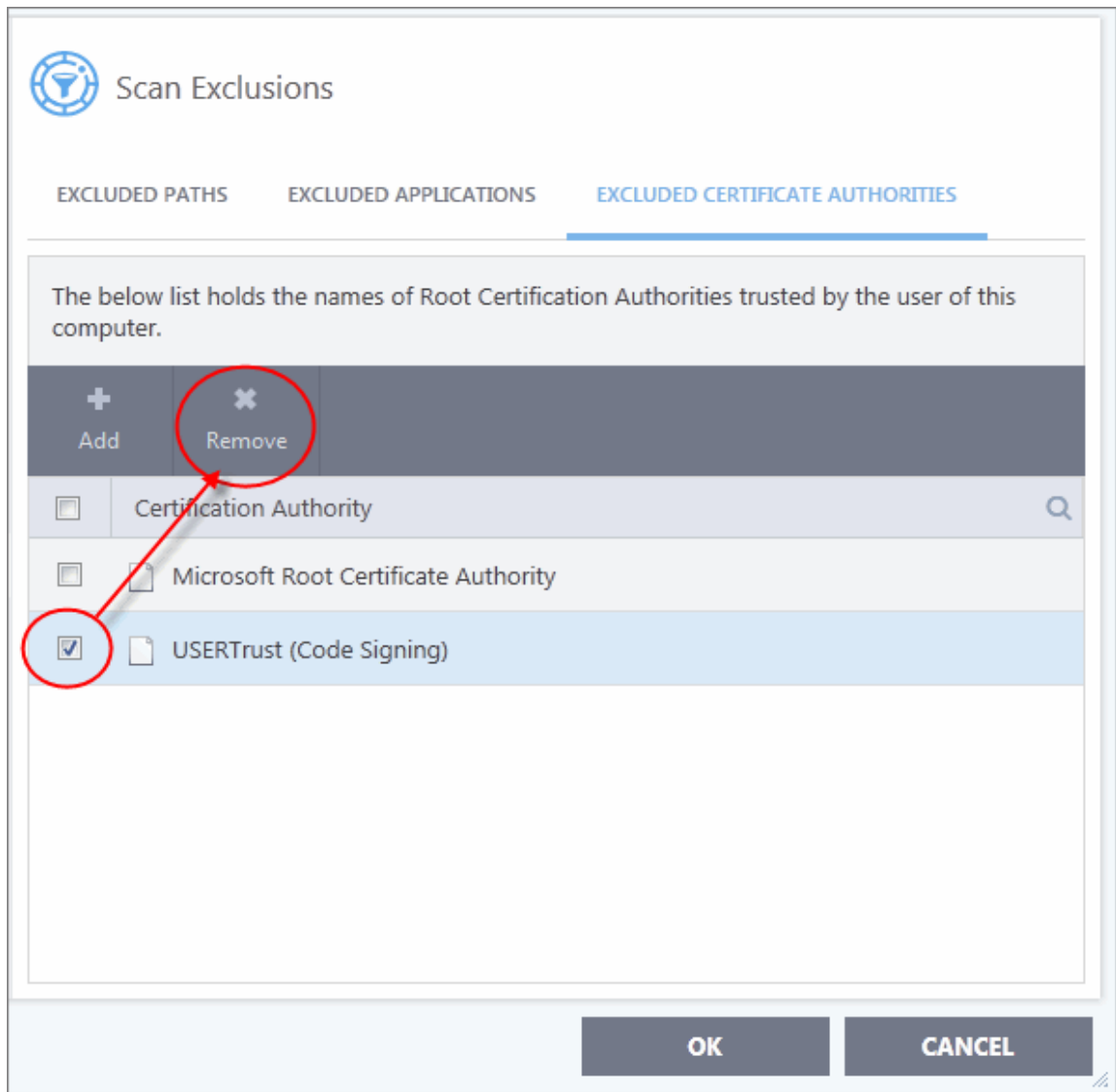
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

6.7.3. Device Control Settings

Click 'Settings' > 'Advanced Protection' > 'Device Control'

- Device control lets you block certain device classes from connecting to your computer. For example, 'USB drives'.
- You can then define exceptions if there are specific devices you want to allow. The fastest way to define an exception is to connect the target device then select 'Exclusions' > 'Add existing Device'.

Open the device control panel

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Device Control'
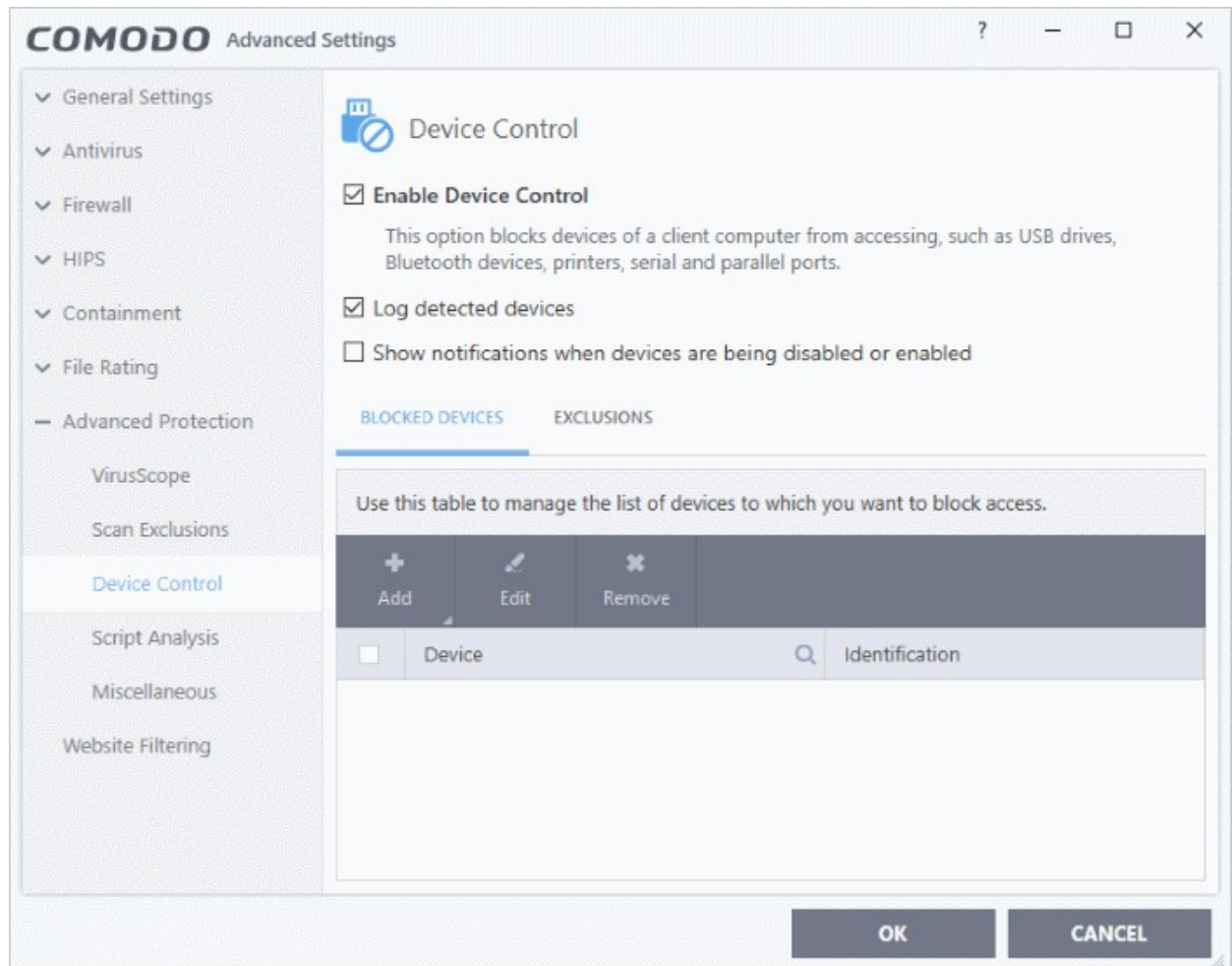
- **Enable Device Control** - Activate the device control functionality to selectively prohibit access to external devices. You should specify devices to be banned in the 'Blocked Devices' pane. *(Default = Enabled)*

- **Log Detected Devices** - CIS logs events like connection attempts of external devices *(Default = Enabled)*

- **Show Notifications when devices are being disabled or enabled** - CIS displays an alert whenever an external device is connected or disconnected.*(Default = Disabled)*

- **Blocked Devices** - List of external device classes which are not allowed to connect to the endpoint. Example classes include 'USB Storage Devices', 'CD/DVD Drives', 'BlueTooth Devices' and 'Firewire Devices'.

- **Exclusions** - Add exceptions to a blocked class. For example, if you wish block the class 'USB Devices' but wish to allow access for your company's authentication tokens, then you should add those USB tokens as exceptions.

Click the following links for more information on blocked devices and exclusions:

- **Block devices**
- **Specify exclusions**

Block Devices

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button
  - Choose the device class you wish to block:
    - For example, to block all USB devices that are plugged to your computer, select "Portable devices" from the list

- If you want to exclude any specific device from this class, enter the device name in the exclusion list.
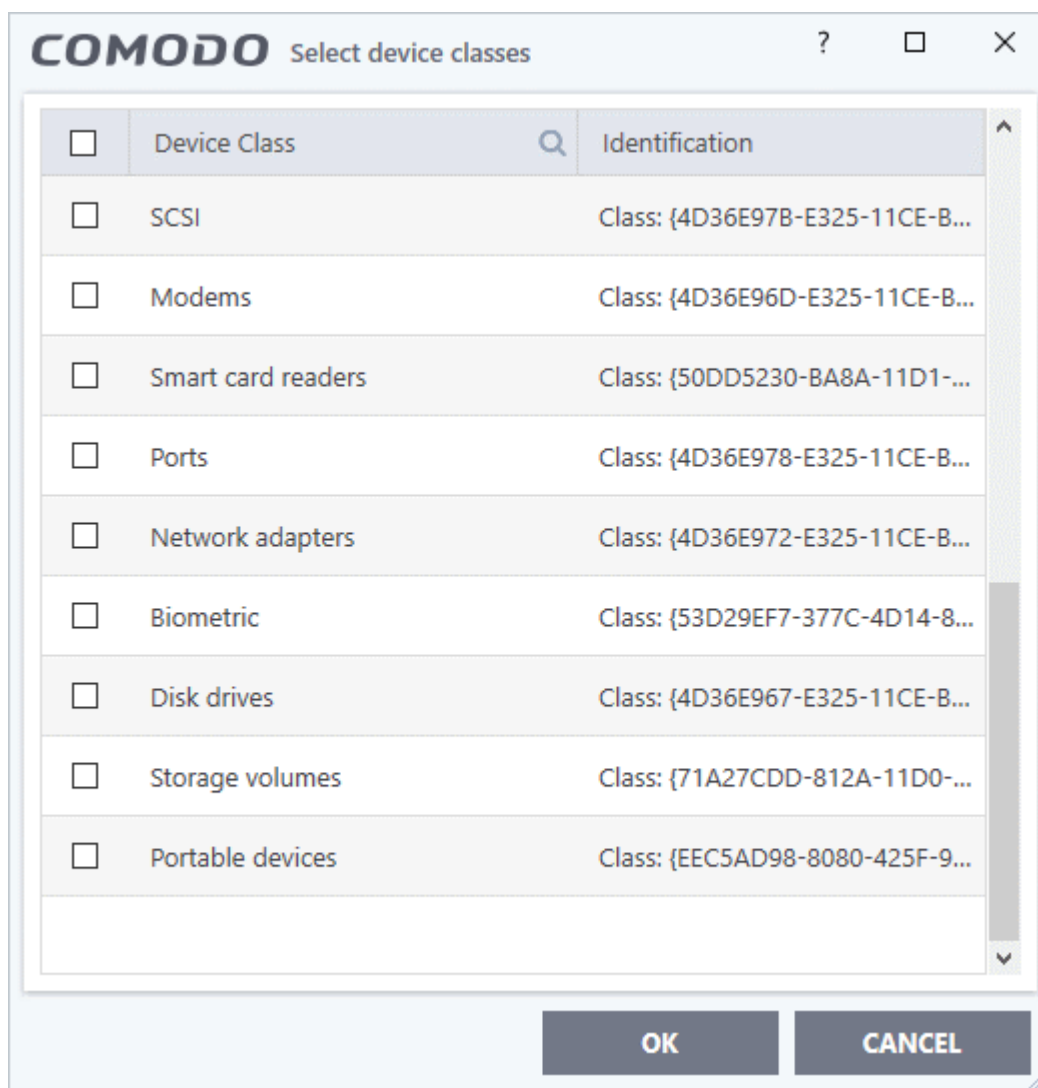
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

Specify exclusions

The 'Exclusions' tab lets you allow access to specific devices that fall within a blocked device class.

You can specify the exceptions in two ways:

- **Select from currently connected devices**
- **Specify a custom device**

Add exclusions from currently connected devices

You need to add the device to the exclusion list before blocking the device class.

- Make sure the external device is connected to the computer
- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Exclusions' tab then click the 'Add' button
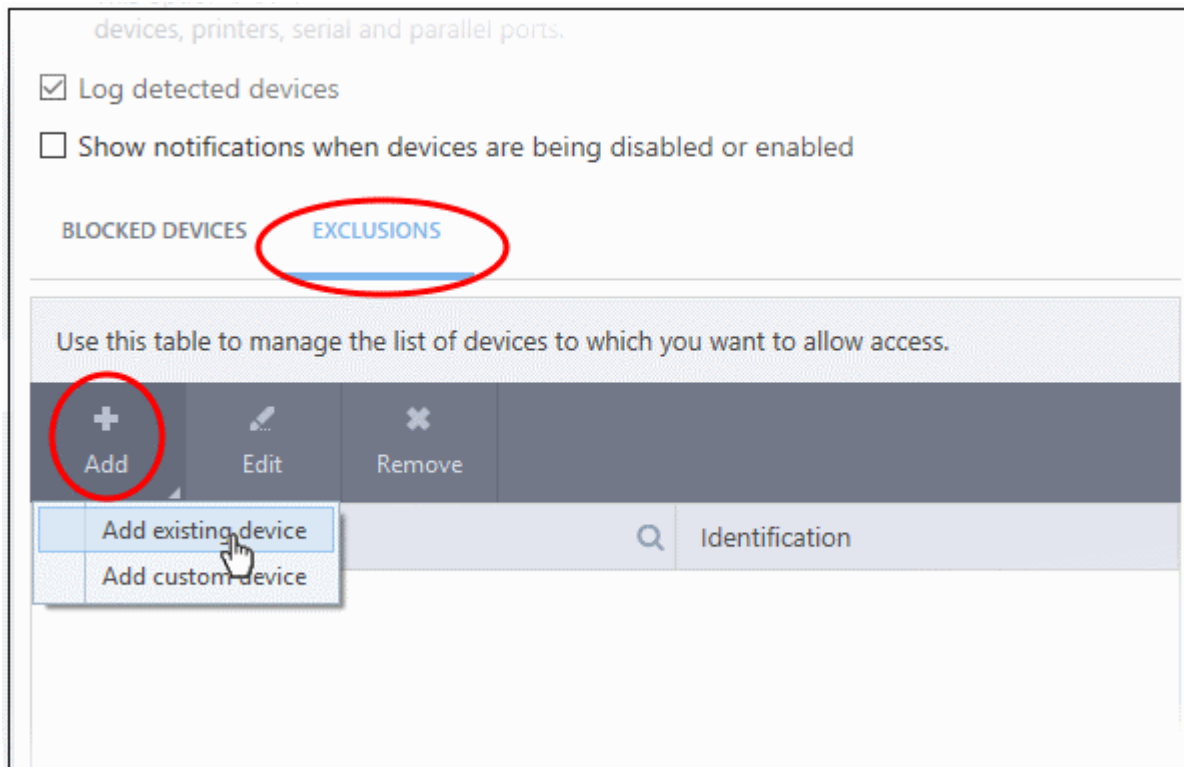
- Select 'Add existing device' from the options
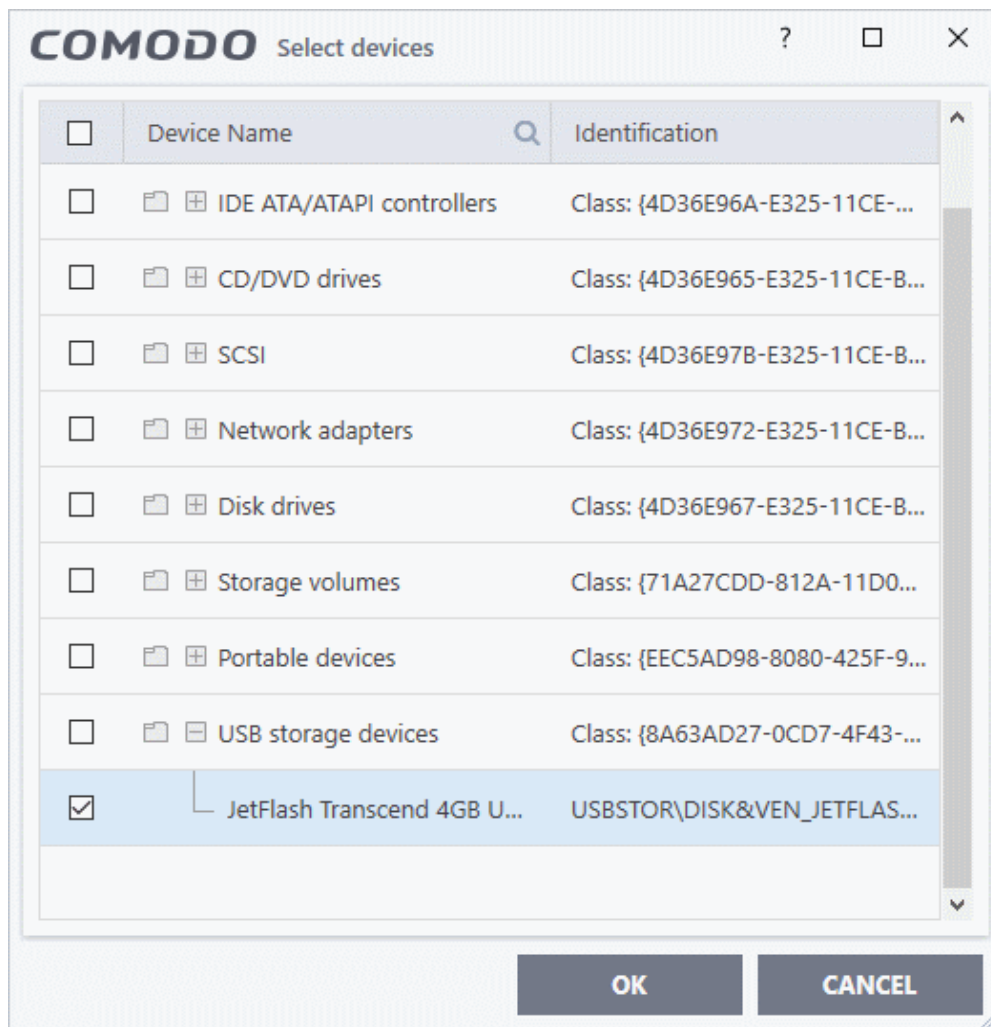
- Click the '+' sign of the class to which your device belongs
- Select the device(s) you wish to exclude
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

Add custom device to be excluded

- You can also add exclusions by specifying the device Ids.
- For example, you want to block all USB storage devices apart from the type of SANDISK devices used by your company, you could specify a device exclusion ID of 'USBSTOR\DISK&VEN_SANDISK\4C5310*'.
- You can also use the wildcard character - ' * ' to cover a range of devices

Specify custom devices to be excluded

- Click 'Settings' on the CIS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Exclusions' tab then click the 'Add' button
- Select 'Add custom device' from the options
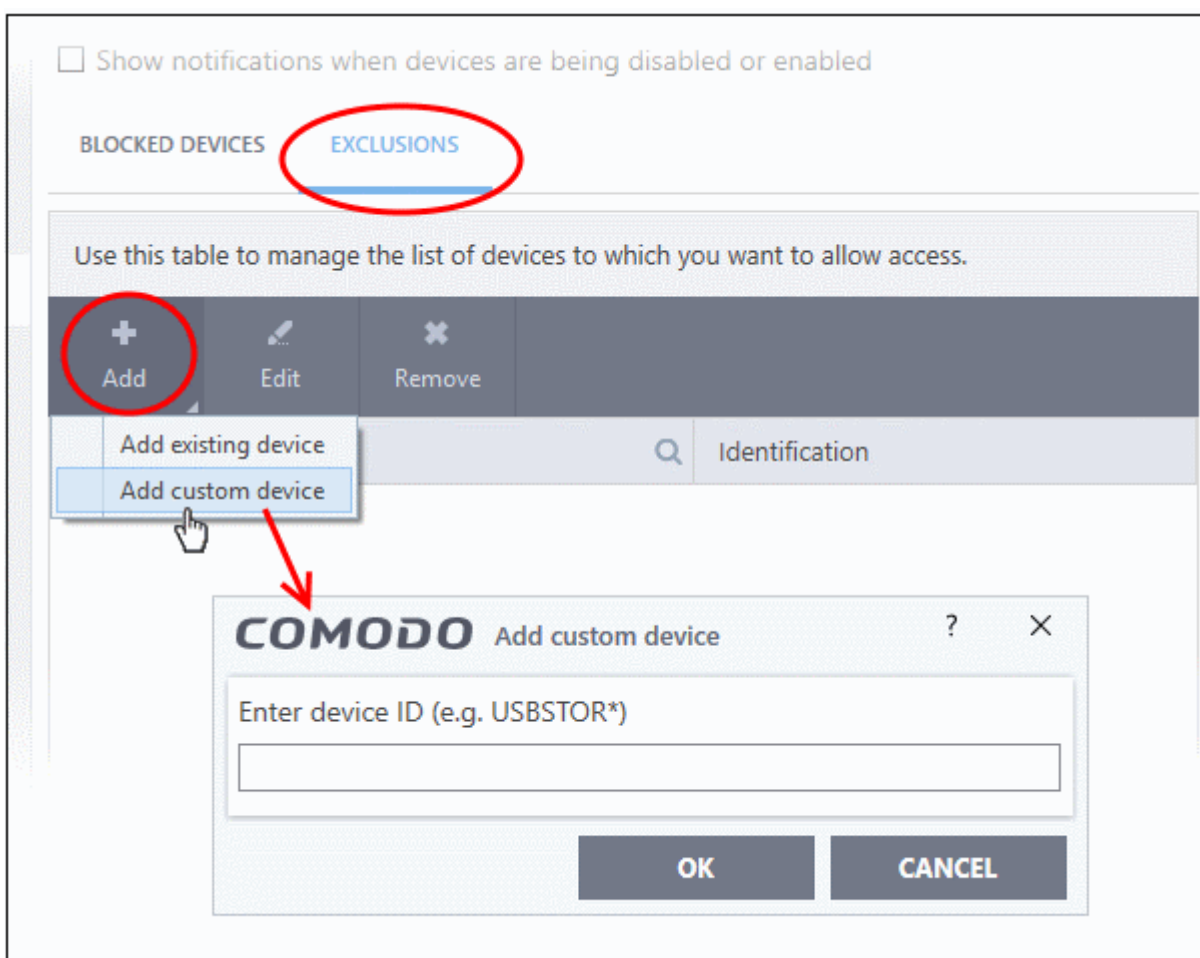
- Enter the unique device identifier in the 'Device ID' field, for example to exclude all USB storage devices whose device IDs start with "4C5310", you could enter: USBSTOR\DISK&VEN_SANDISK\4C5310*
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

6.7.4. Script Analysis Settings

Click 'Settings' > 'Advanced Protection' > 'Script Analysis'

- The script analysis settings panel lets you:

- Configure heuristic command line analysis for applications in real-time
- Configure heuristic command line analysis for auto-run entries. Auto-run entries include Windows services, auto-start items and scheduled tasks.

> **Background note**: 'Heuristics' is a technology which analyzes a file to see if it contains code typical of a virus. Heuristics is about detecting 'virus-like' traits in a file. This helps to identify previously unknown (new) viruses.

Open the script analysis settings panel

- Click 'Settings' on the home screen to open the 'Advanced Settings' interface
- Click 'Advanced Protection' > 'Script Analysis' on the left:
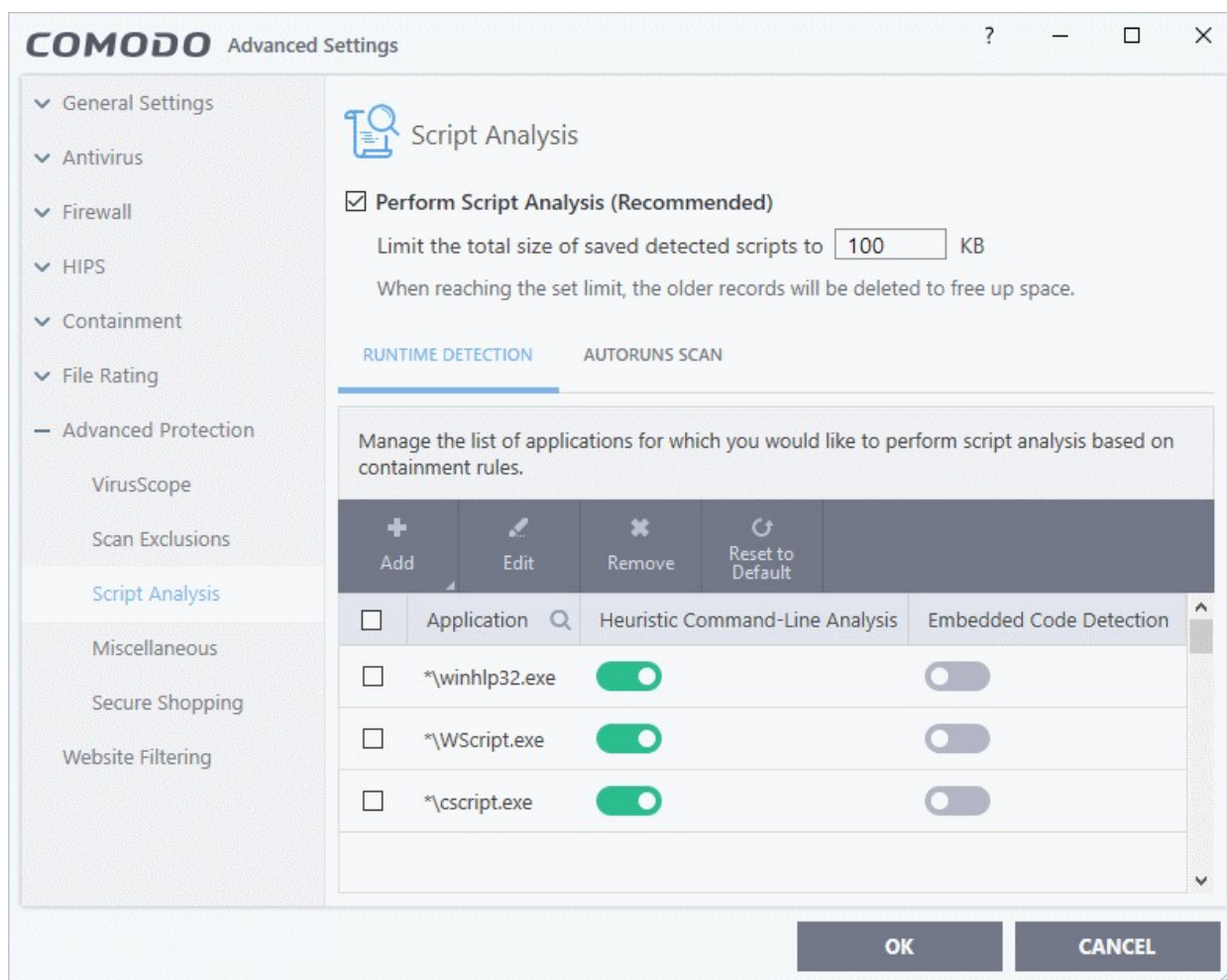
- **Perform Script Analysis (Recommended)** - Enable / disable script analysis of managed applications *(Default = Enabled)*
  - **Limit the total size of saved detected scripts to 'N' KB** - CIS stores the list of executing scripts that are run by the managed applications for analysis. This options allows you to specify the total size of the stored scripts. When the set limit is reached, the older scripts are deleted automatically.

The interface has two tabs:

- **Runtime Detection**
- **Autoruns Scans**

Runtime Detection

CIS performs heuristic analysis on certain programs because they are capable of executing code. Example programs are wscript.exe, cmd.exe, java.exe and javaw.exe. Example code includes Visual Basic scripts and Java applications.

- For example, the program wscript.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

- If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the internet'.

- Relevant settings are applied to the scripts. For example, if a script is detected by the containment module, then auto-containment rules are applied. Each module (AV, FW, VirusScope and so on) that detects a script will apply its appropriate settings.
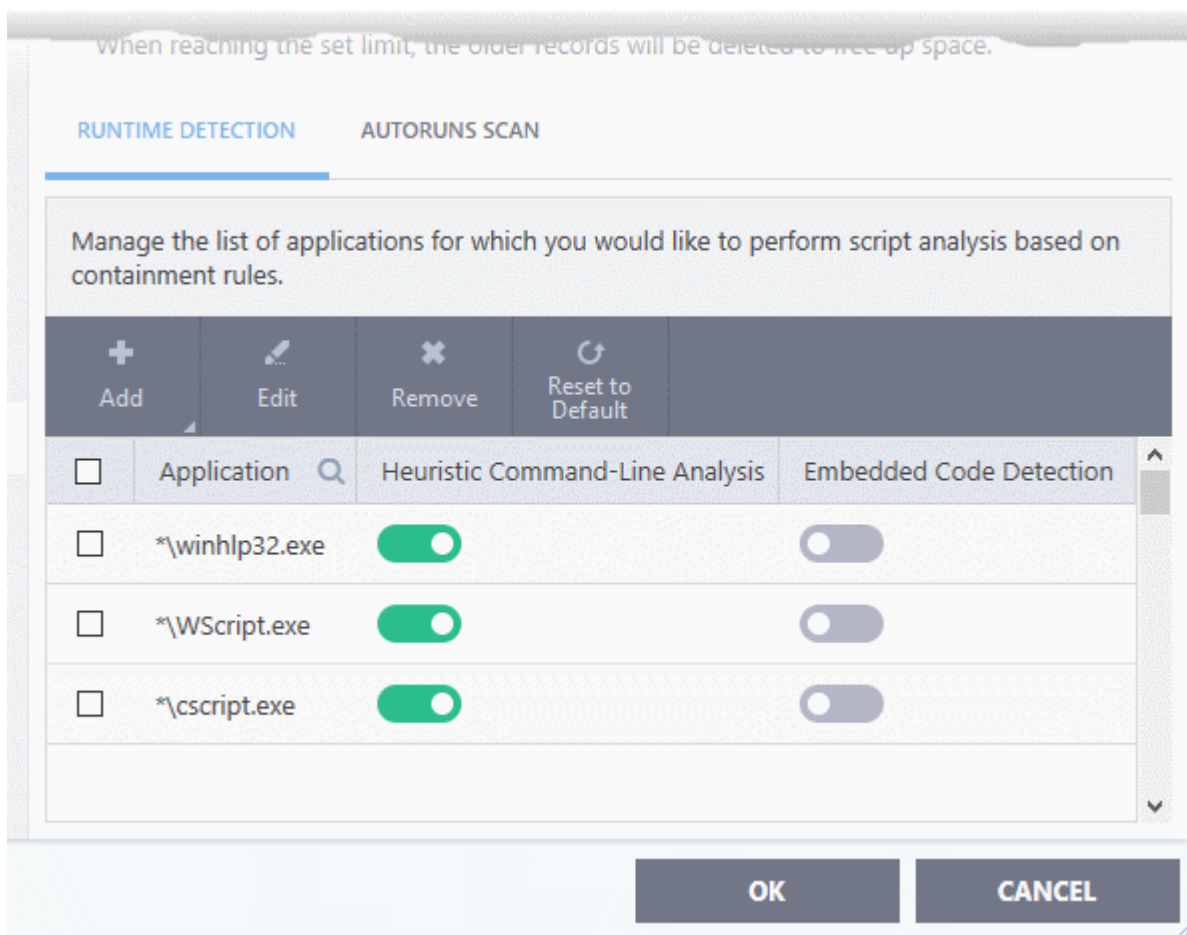
Runtime Detection - Column Descriptions	
Column Header	Description
Application	Name of existing application covered by this rule
Heuristic Command-Line Analysis	Enable or disable command line tracking
Embedded Code Detection	Enable or disable embedded code tracking

Manually add a new application to the list for analysis

- Click 'Add' at the top

You can add an application by following methods:

- **Add a new application**
- **Add a current application**
- **Add application from the currently running processes**

Add a new application

- Click 'Add new application' from the 'Add' drop-down
- Provide the details in the 'Edit Property' dialog and click 'OK'

The application will be added and displayed in the list.
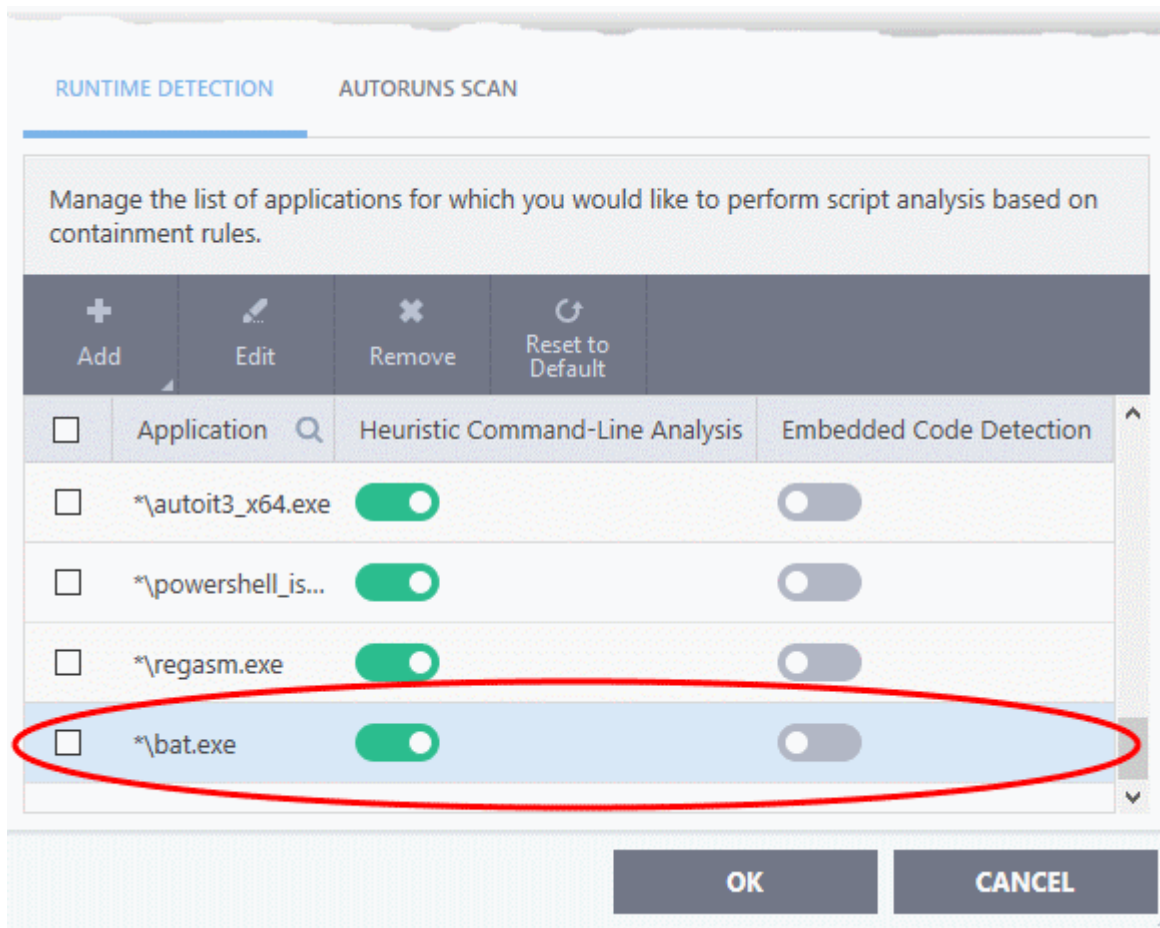
- Click "OK" to apply your settings

Add a currently running application

- Click 'Add' then 'Applications' from the drop-down
- Navigate to the file you want to add in the 'Open' dialog and click 'Open'
- The file will be added to the list
- 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 parent application you wish to add for analysis
- Click 'OK' from the 'Browse for Process' dialog
- The application will be added to the list

- Use the switches beside the applications to enable/disable heuristic command line analysis and / or embedded code detection 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.

Autoruns Scans

- Add and manage applications for which you want to perform heuristic command-line analysis and embedded code detection in order to protect Windows services, autostart items and scheduled tasks.

- CIS ships with a list of predefined applications for which it performs heuristic analysis on programs that are capable of executing code.

- The applications added here are applicable for the settings in:

    - '**Scan Options**' > '**Apply this action to suspicious autorun processes**' (monitors only during on-demand scans)
    - 'Advanced Settings' > '**Miscellaneous**' > '**Apply the selected action to unrecognized autorun entries related to new/modified registry items**' (monitors constantly)

Open the 'Autoruns Scans' interface

- Click 'Settings' on the home screen to open the 'Advanced Settings' interface

- Click 'Advanced Protection' > 'Script Analysis' on the left:

- Click the 'Autoruns Scan' tab
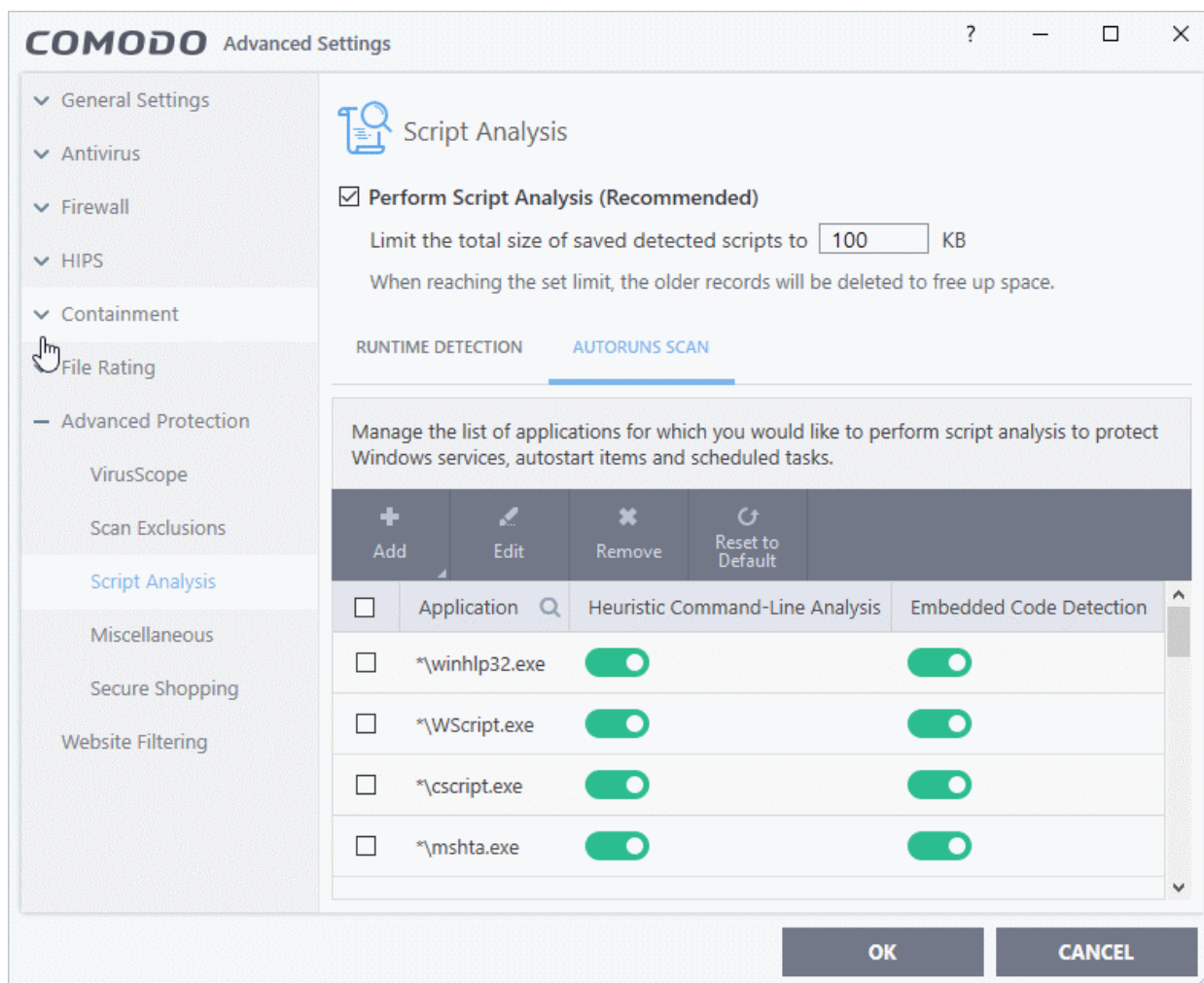
Autroruns Scans - Column Descriptions	
Column Header	**Description**
Application	Name of existing applications covered by this rule
Heuristic Command-Line Analysis	Enable or disable command line tracking
Embedded Code Detection	Enable or disable embedded code tracking

Manually add a new application to the list for analysis

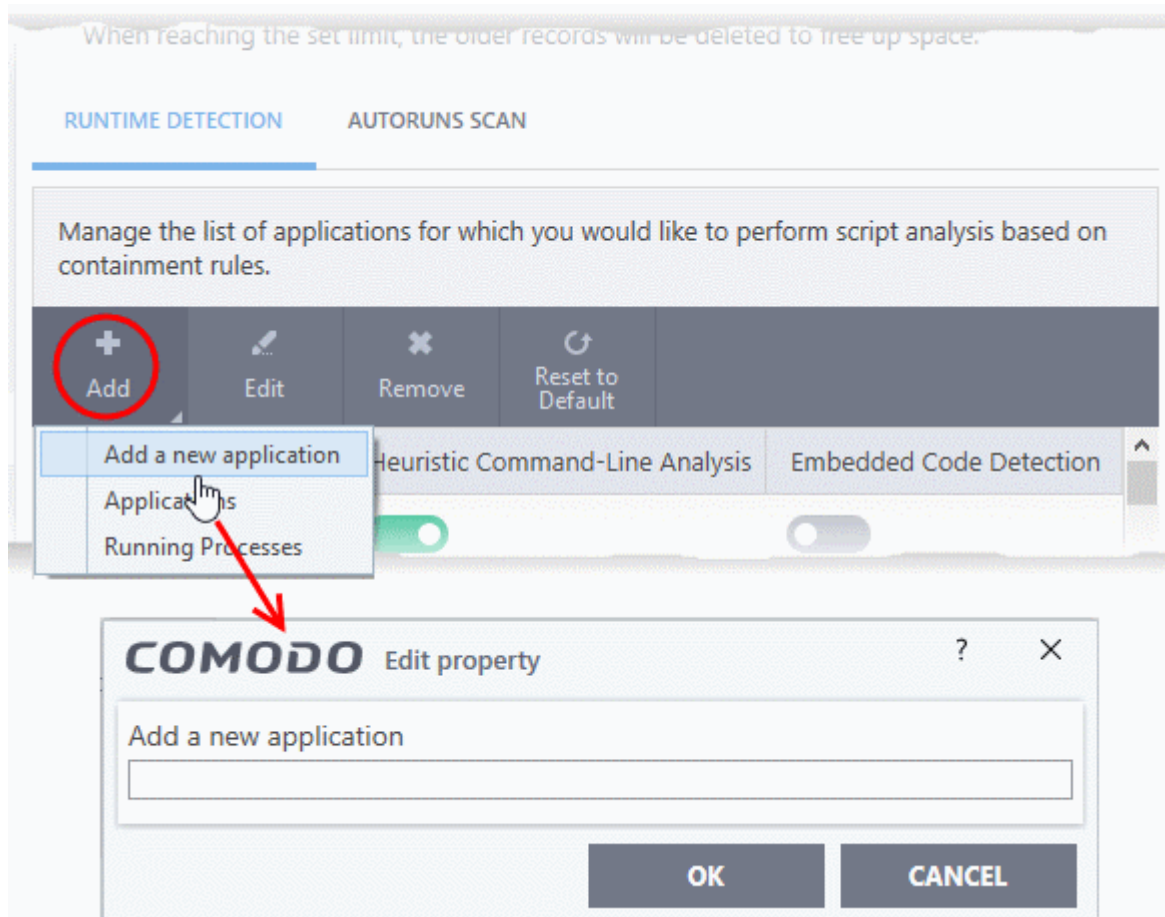- Click 'Add' at the top

---

You can add an application by following methods:

- **Add a new application**
- **Add a current application**
- **Add application from the currently running processes**

Add a new application

- Click 'Add new application' from the 'Add' drop-down
- Provide the details in the 'Edit Property' dialog and click 'OK'

The application will be added and displayed in the list.

- Click "OK" to apply your settings

Add a current application

- Click 'Add' then 'Applications' from the drop-down
- Navigate to the file you want to add in the 'Open' dialog and click 'Open'
- The file will be added to the list
- 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 parent application you wish to add for analysis
- Click 'OK' from the 'Browse for Process' dialog
- The application will be added to the list

- Use the switches beside the applications to enable/disable heuristic command line analysis and / or embedded code detection 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.

6.7.5. Miscellaneous Settings

Click 'Settings' > 'Advanced Protection' > 'Miscellaneous'

- The 'Miscellaneous' panel allows you to:

  - Configure protection against shellcode injections (buffer overflow attacks)
  - Show alerts if applications try to change your browser settings
  - Skip automatic cleanup of suspicious certificates.
  - Specify what actions are taken if CIS detects unrecognized auto-start entries or scheduled tasks
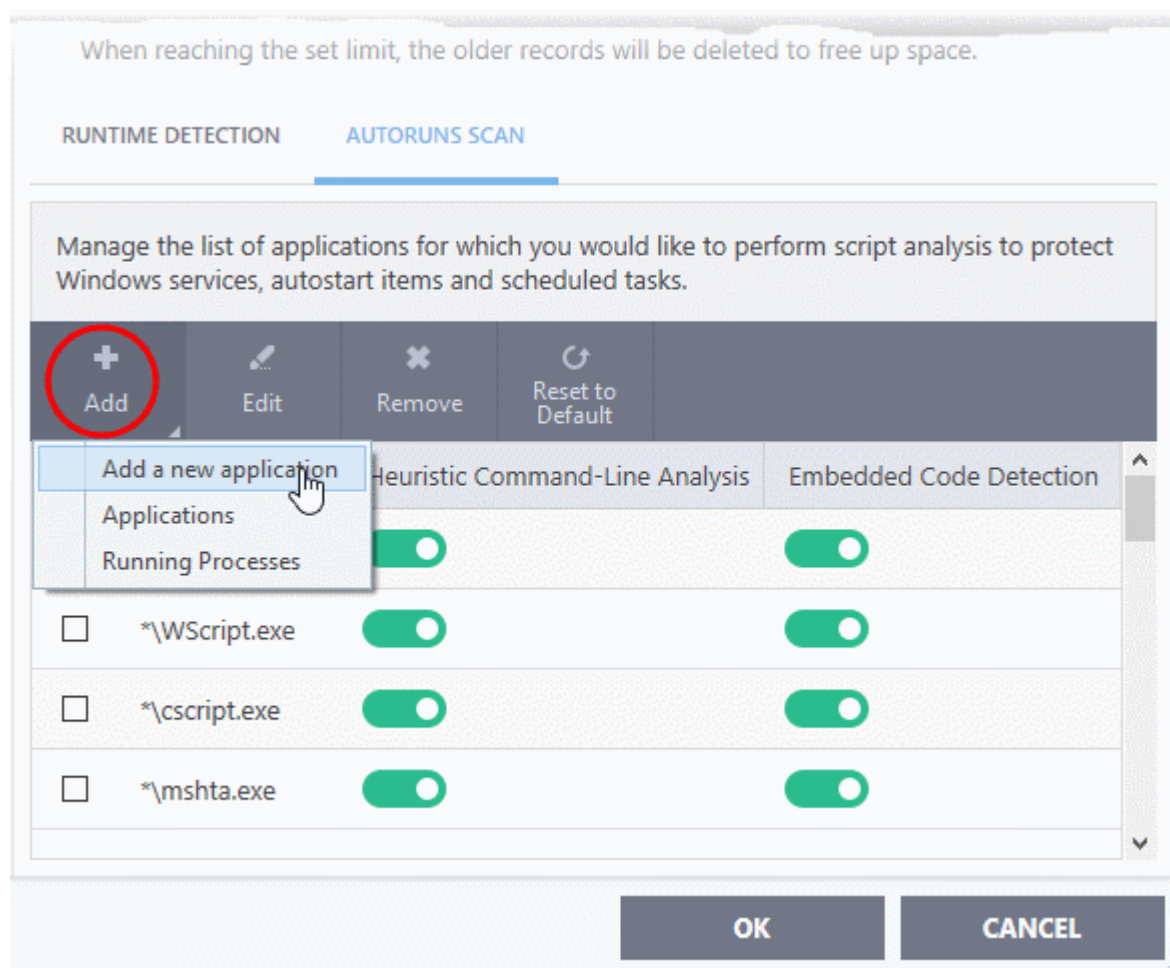
Open the miscellaneous interface

- Click 'Settings' on the home screen to open the 'Advanced Settings' interface
- Click 'Advanced Protection' > 'Miscellaneous':
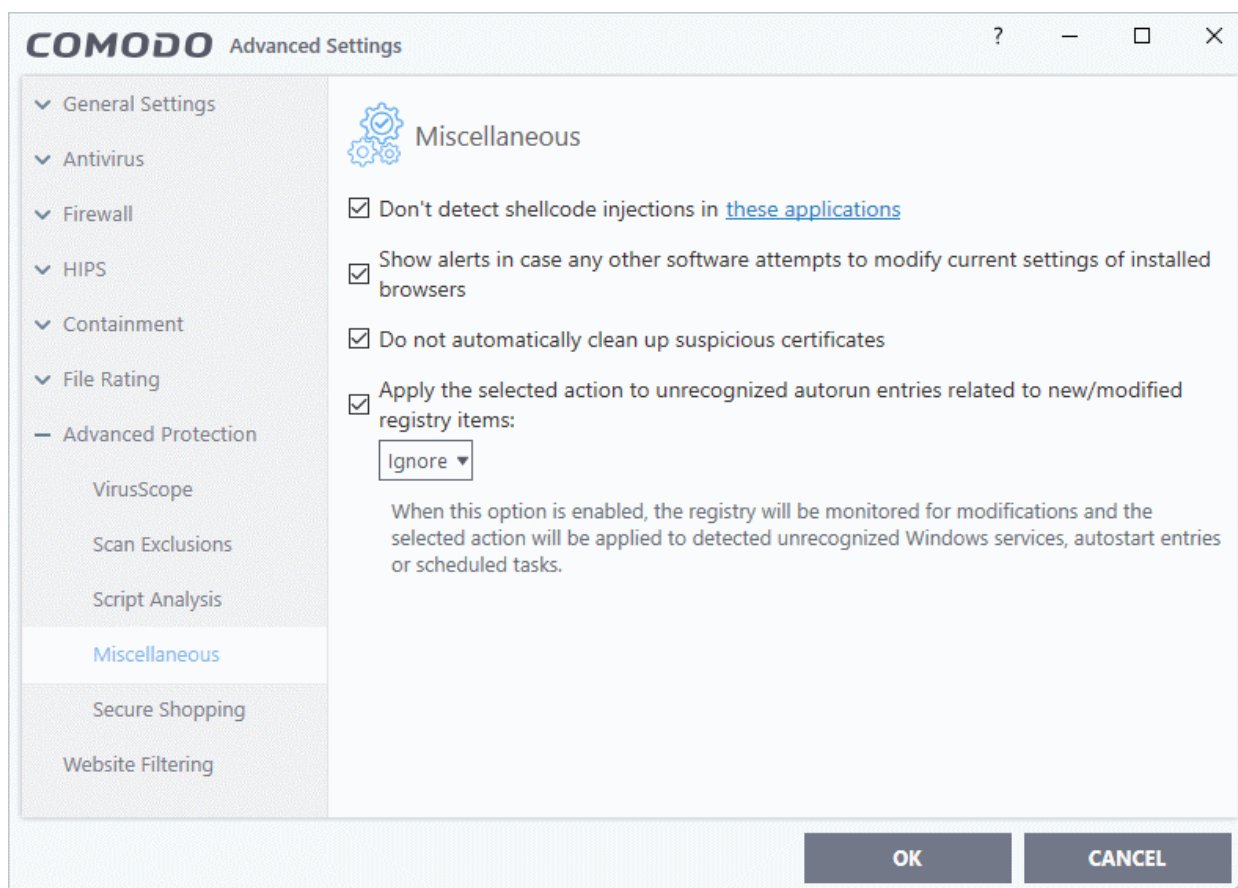
This interface allows you to:

- **Disable shellcode injection detection for certain applications**
- **Enable alerts if a software tries to change your browser settings**
- **Skip automatically clean-up suspicious certificates**
- **Define actions to be taken on unrecognized auto-start entries/scheduled tasks**

Disable shellcode injection detection

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:

- Shellcode injection is a malicious technique which allows an attacker to cause a buffer overflow on your system.
- A buffer overflow occurs when a process attempts to store data beyond the boundaries of a fixed-length buffer. A buffer is an area of memory designed to hold a specific amount of data.
- The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.
- Overflows can be caused by inputs specifically designed to execute malicious code or make the program operate incorrectly. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

Exclude certain applications from shellcode injection protection

- Make sure 'Don't detect shellcode injections in these applications' is enabled and click the 'these applications' link. The 'Manage Exclusions' dialog appears.
- Click the 'Add' button at the top

You can add items by selecting the required option from the drop-down:
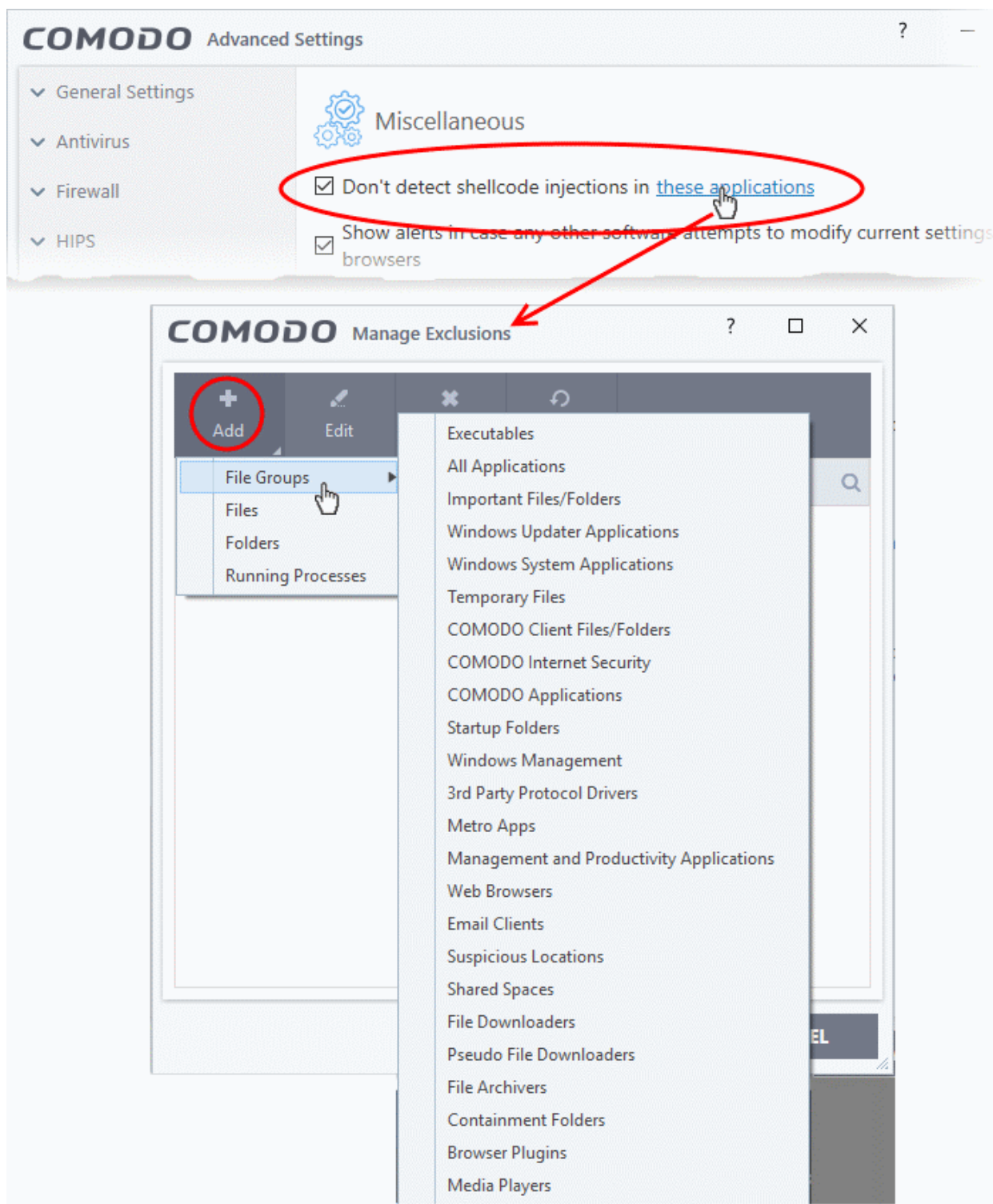
- **File Groups** - Select a category of pre-set files or folders. For example, 'Executables' lets you create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *cmd.exe *.bat, *.cmd. Other categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc **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.

Click 'OK' to implement your settings.

Enable alerts if any software tries to change your browser settings

- **Show alerts in case any other software attempts to modify current settings of installed browsers** - Improves online security by warning you each time a program tries to change your browser's settings without your consent. The browser settings include home page, default search engine and more. *(Default = Enabled).*

Do not automatically cleanup suspicious certificates

- Choose whether or not to delete any root certificates that were not signed by a trusted certificate authority.

- By default, CIS warns you if any fake root certificates are found in your browsers but does not delete them.

- Disable this option if you want CIS to delete those fake certificates whenever they are found

---

Background:

- SSL certificates are used by websites to encrypt the connection between your browser and their web-server.

- This ensures nobody can intercept the traffic sent between you and the site. All information sent from your browser to the site is private. This is especially important for sensitive transactions like online payments, where you send your credit card information over the internet.

- You can tell a site is using an SSL certificate by the padlock icon in the browser address bar.

- SSL certificates are issued to website owners by an organization known as a 'Certificate Authority' (CA). The CA checks that the applicant owns the website in question, and is a legitimate business.

- Once these checks have been passed, the CA will sign the applicant's certificate with what is known as a 'root certificate'. You should only trust websites whose certificates have been signed by the root certificate of a trusted CA.

- These trusted root certificates are embedded in your browser (Firefox, Chrome, Edge etc). Your browser checks that the SSL certificate on a site is signed by a trusted root each and every time you visit the site.

- A fake root certificate would, therefore, bypass this check of legitimacy. It could tell you to trust a website run by a hacker.

- CIS can detect and remove fake root certificates from the endpoint during on-demand and scheduled scans. Disable 'Do not automatically cleanup suspicious certificates' to activate this feature.

Define actions to be taken on unrecognized auto-start entries/scheduled tasks

- **Apply the selected action to unrecognized autorun entries related to new / modified registry items** - Specify what CIS should do if applications added to **Script Analysis** > **Autoruns Scans** try to create or modify one of the following registry items:

  - Windows services
  - Auto-start entries
  - Scheduled tasks

The available options are:

- **Ignore** - CIS does not take any action (*Default*)
- **Terminate** - CIS stops the process / service
- **Terminate and Disable** - Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.
- **Quarantine and Disable** - Auto-start processes are quarantined and the corresponding auto-start entry removed. In the case of a service, CIS disables the service.

Background:

- CIS can perform heuristic command-line analysis and embedded code detection in order to protect Windows services, autostart items and scheduled tasks.

- CIS ships with a list of predefined applications for which it performs heuristic analysis on programs that are capable of executing code.


- You can also add programs for which you want CIS to perform heuristics analysis in 'Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autoruns Scan'. See **Autoruns Scans** in **Script Analysis Settings** for more details on this.

- Click 'OK' to save your settings.

6.7.6. 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
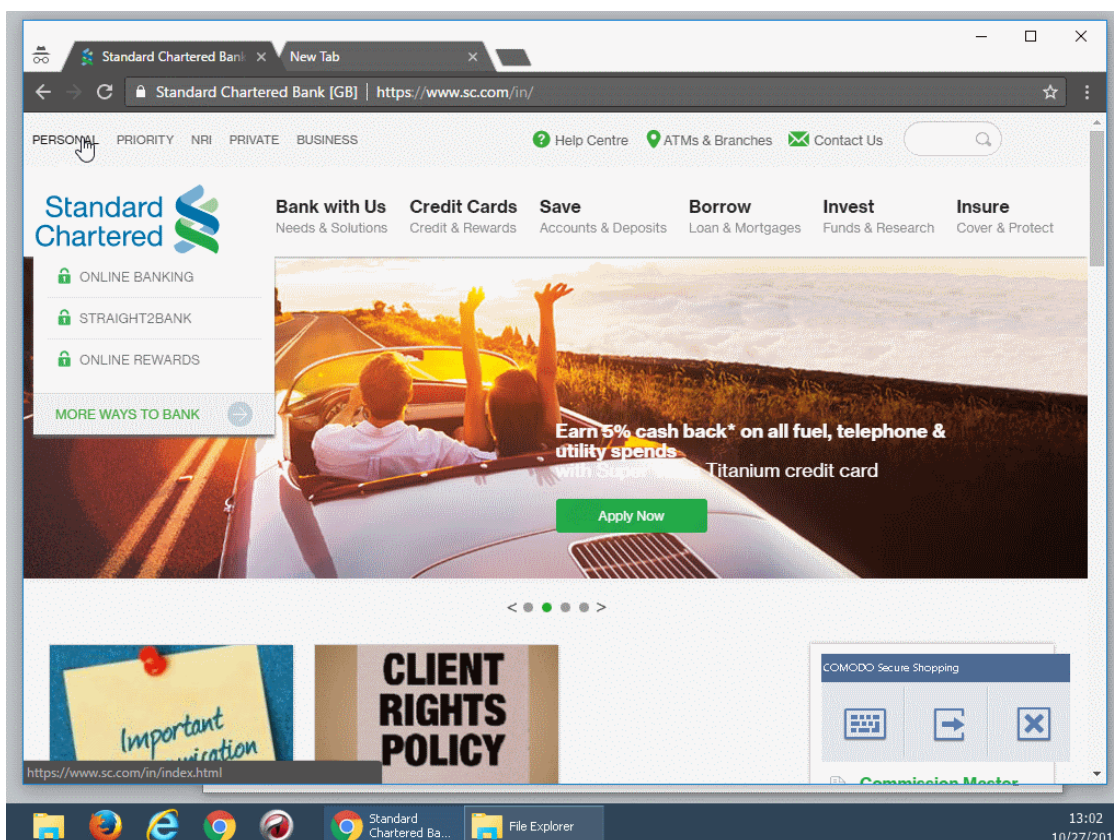
You can configure Secure Shopping to alert you whenever you visit specific shopping, banking and other websites and ask you if you want to use Secure Shopping environment, open the website in a secure browser window or continue with the same browser.

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 Comodo Internet Security, we bring 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:

- • **Configure Secure Shopping**

- • **Use Secure Shopping Environment**

  - • **Shopping and Banking Activities**
  - • **Open applications inside Secure Shopping Environment**

Configure 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.

Configure Secure Shopping

- • Click 'Settings' on the CIS home screen

- • Click 'Advanced Protection' > 'Secure Shopping' on the left
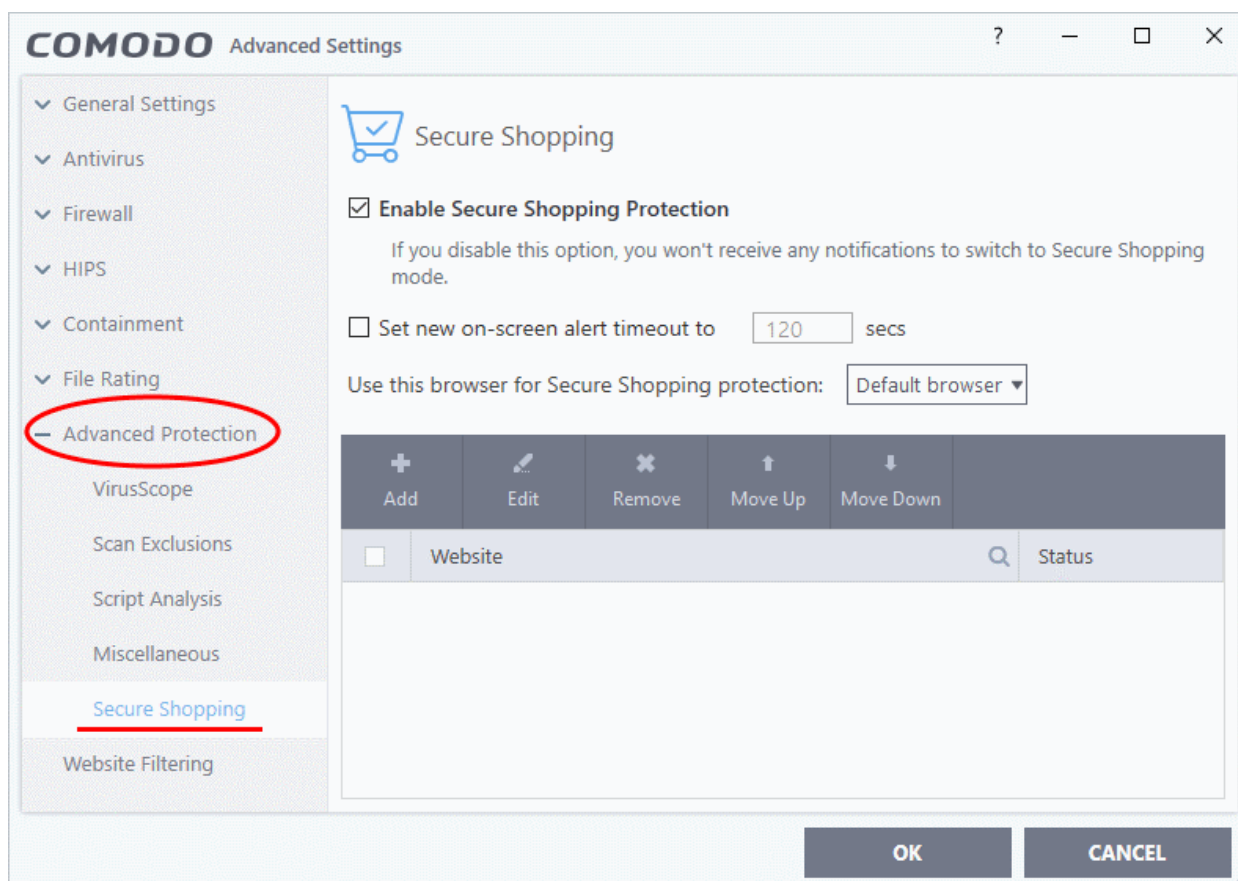
Secure Shopping Settings

- • **Enable Secure Shopping Protection** - 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** - Choose the web browser to be used when in secure shopping mode. The drop-down lists all browsers installed on your computer:

Add Websites for Secure Shopping Protection

You can configure the following options when adding or editing a web site:

- **Website** - URL of the protected website
- **Status** - The toggle switch allows you enable or disable secure shopping protection for the website.

Add a website

1. Click the 'Add' button' then enter the domain name of your website.
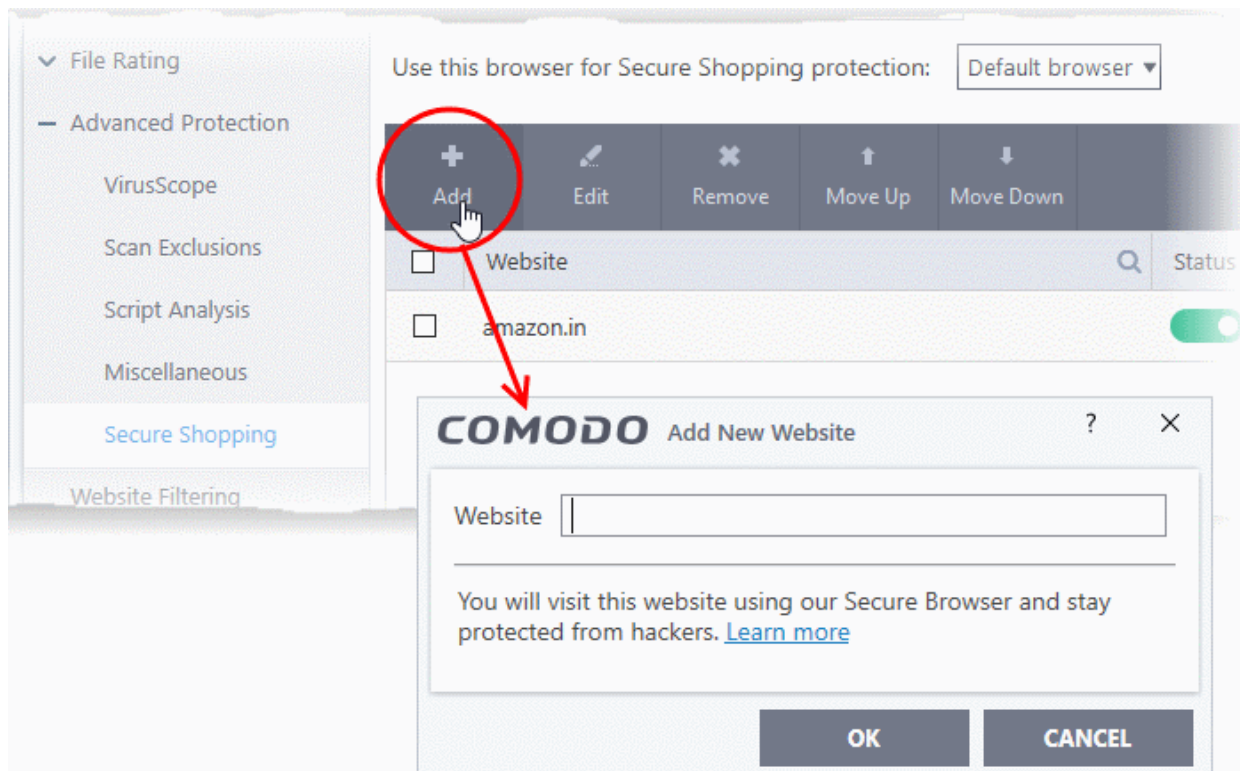
2. Click 'OK' to add the website to the list. Repeat the process to add more websites

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.

An alert is displayed whenever you visit a website added to the list of websites for secure shopping protection. as shown below:
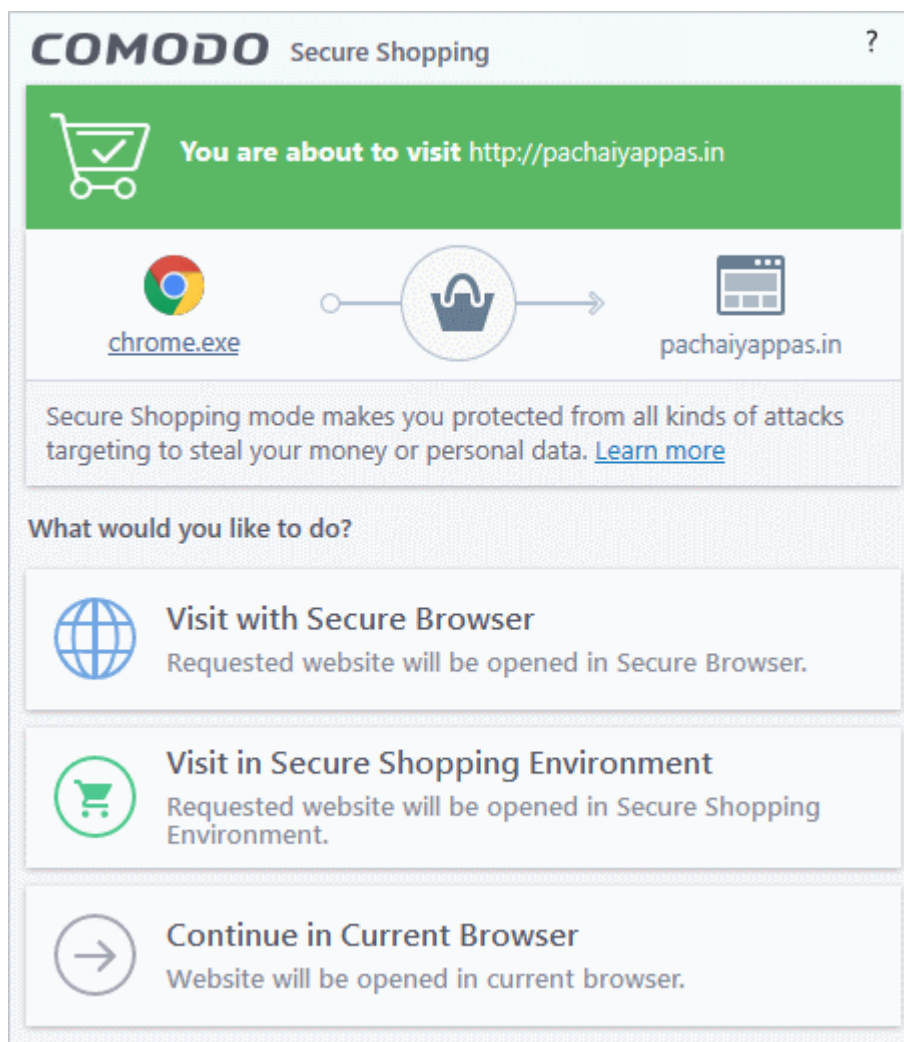
- You can choose how you want to proceed with the website, from the alert.

  - **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:
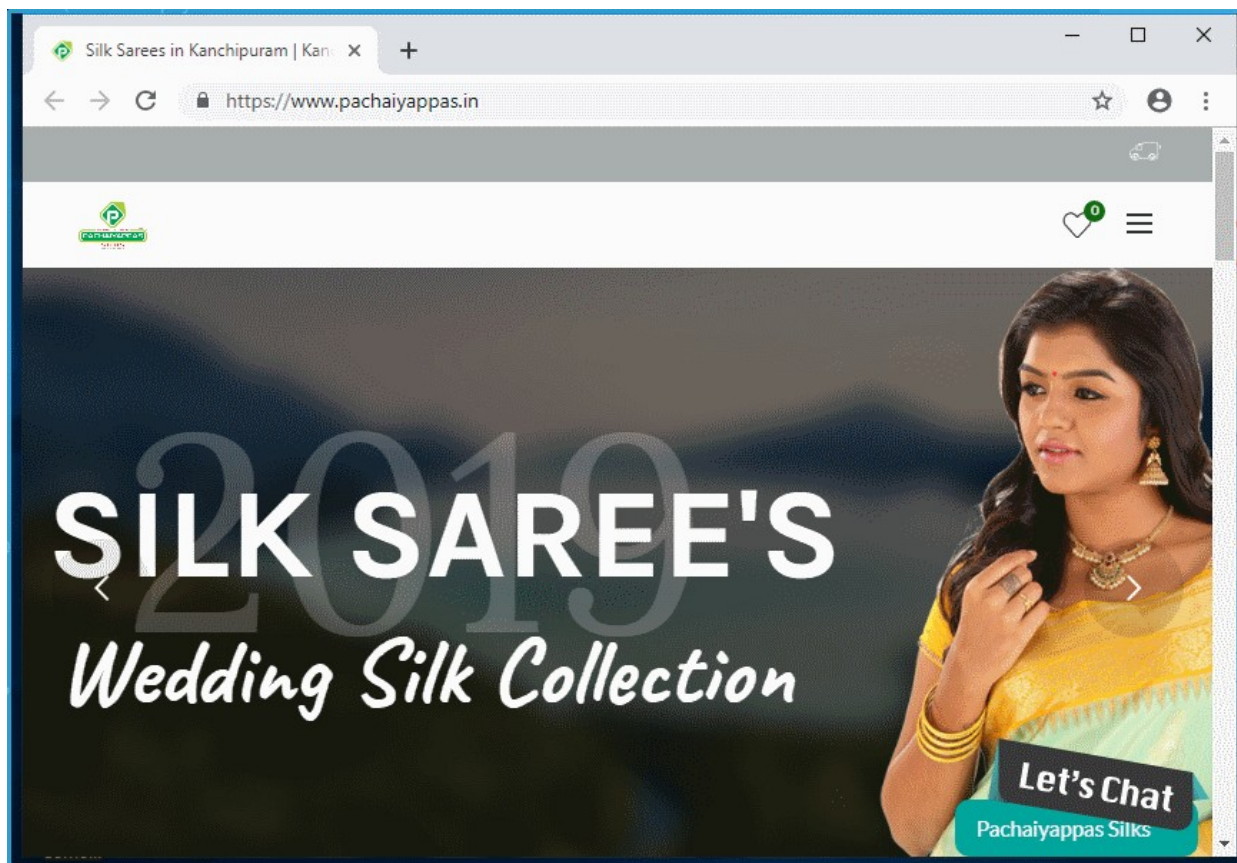
- **Visit in Secure Shopping Environment -** The website will be opened in a security hardened, virtual environment. When inside this environment, your browser cannot be accessed or potentially attacked by other processes running on your computer. Your session will be protected by all Secure Shopping technologies (full process isolation, key-logger protection, remote connection warnings, screenshot blocking and SSL certificate checking). See **Use 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.

Use 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:

- **CIS Home Screen** - Click 'Tasks' > 'General Tasks' > 'Secure Shopping'
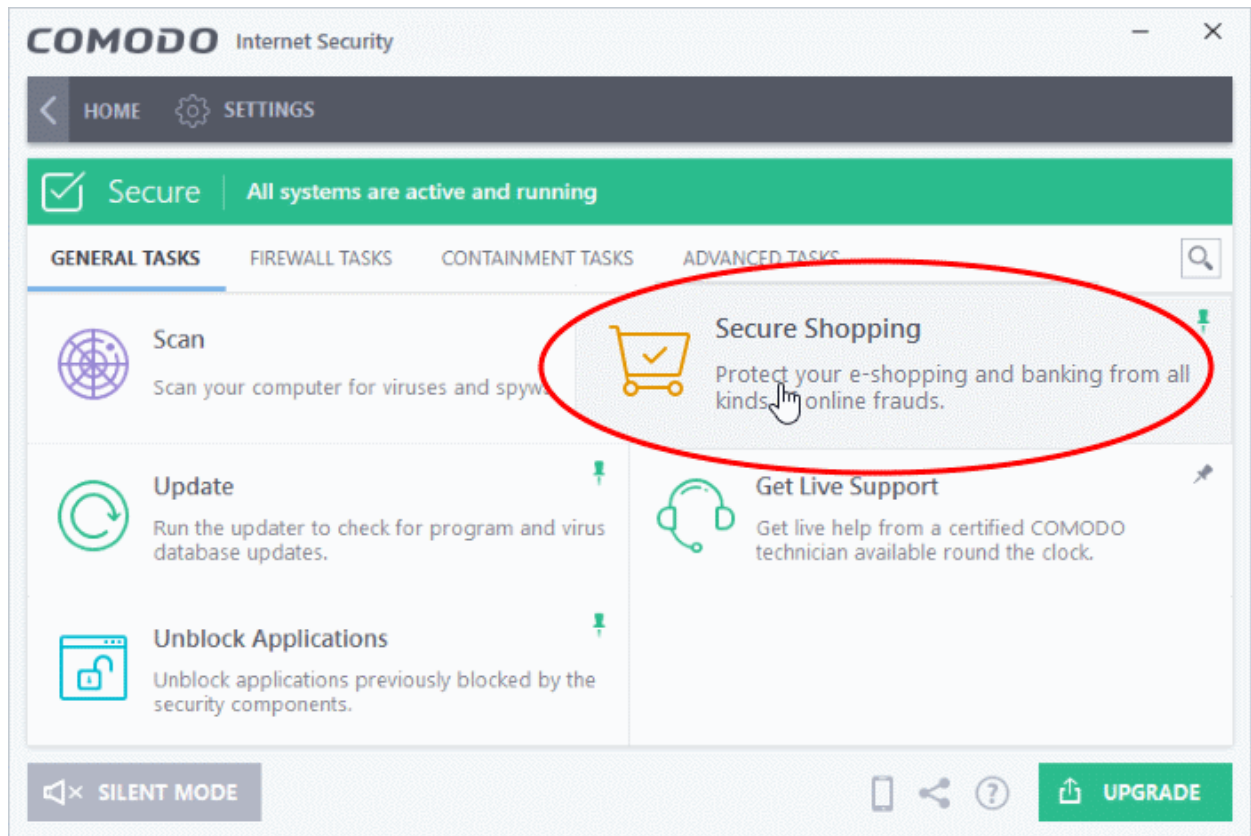
- **CIS Desktop Widget** - Click the 'Secure Shopping' icon from the CIS Desktop widget
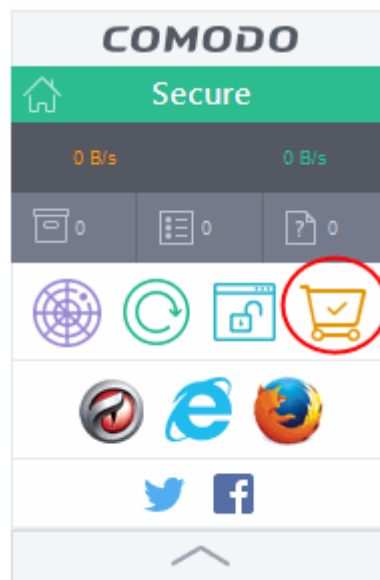
- From the Windows Start menu - Click Windows Start/Home > All Programs > Comodo > Comodo Secure Shopping
- From the Windows Desktop icon - Double-click the 'Comodo Secure Shopping' shortcut on the desktop:

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

- 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. 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 browser chosen as per the Secure Shopping configuration. 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 lets 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 more help on the tools panel:

- **Use Virtual Keyboard**
- **Switch to your Desktop**
- **Exit Secure Shopping**

Open applications inside the Secure Shopping Environment

- **Start the Secure Shopping** environment and click the folder icon at bottom-left:
- Browse to the application or file you want to run and open it.

The application opens inside the Secure Shopping environment:

The Tools Panel

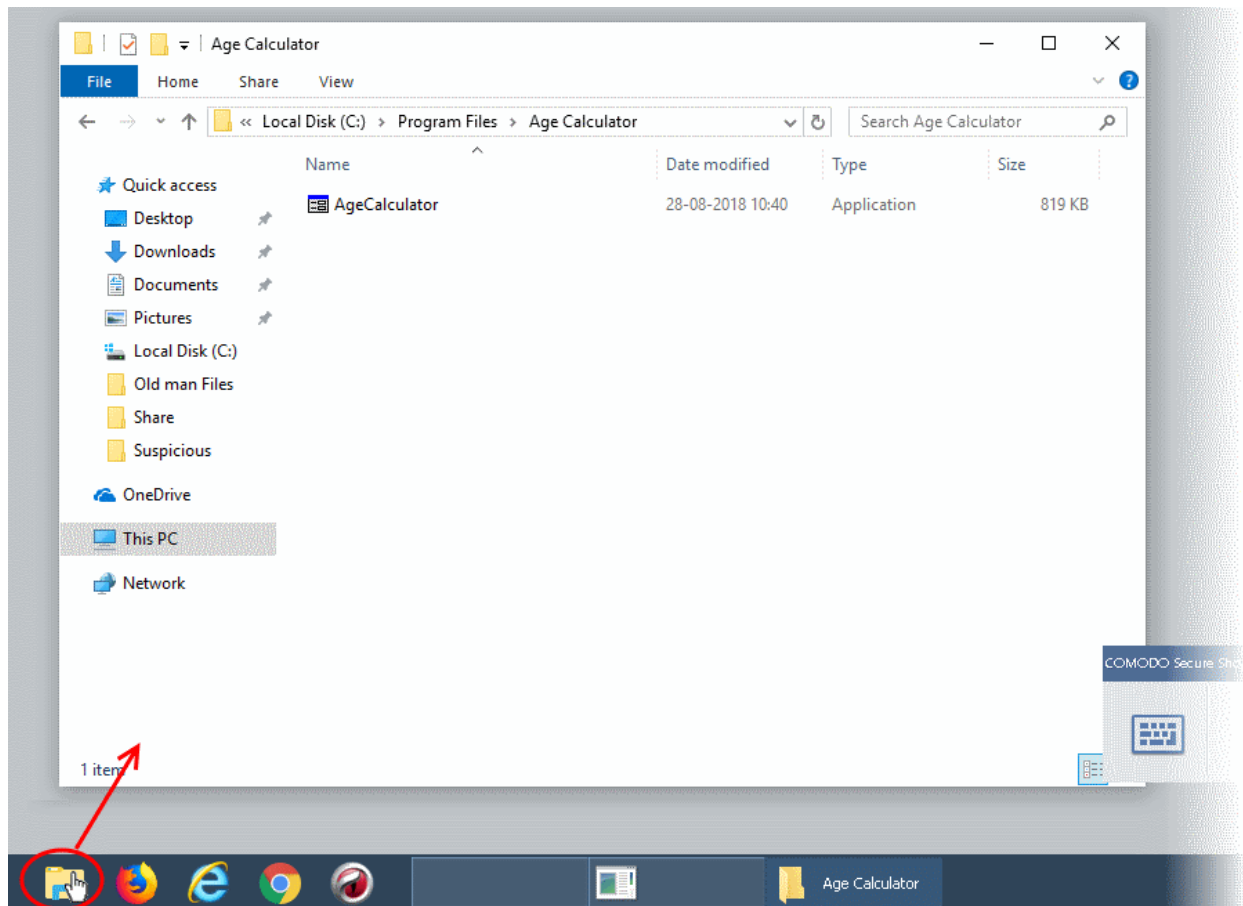The tools panel at the bottom right of the screen allows you to open the virtual keyboard, temporarily switch back to your desktop, or to fully exit the Secure Shopping virtual environment.

Use the virtual keyboard

The Secure Shopping environment features an on-screen virtual keyboard that helps you in entering confidential information like website user-names, passwords and credit card numbers.

- Click the language button ![ENG] at the bottom-right and select the keyboard layout you want to use.

- Click the keyboard icon in the tools panel to open the on-screen virtual keyboard.

Temporarily switch to your desktop

- Click the ![button] button in the tools pane.

The Secure Shopping Desktop will be hidden. You can quickly return to it by clicking the button again.

Close the Secure Shopping Desktop

- Click the 'X' button ![X] in the tools pane

A confirmation is shown:
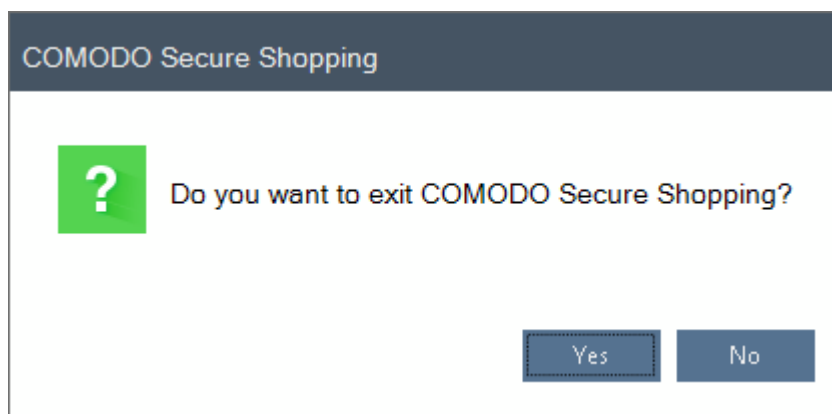
- Click 'Yes' to exit the Secure Shopping Desktop.

6.8. Website Filtering Configuration

Click 'Settings' > 'Website Filtering'

- The website filtering section lets 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.

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
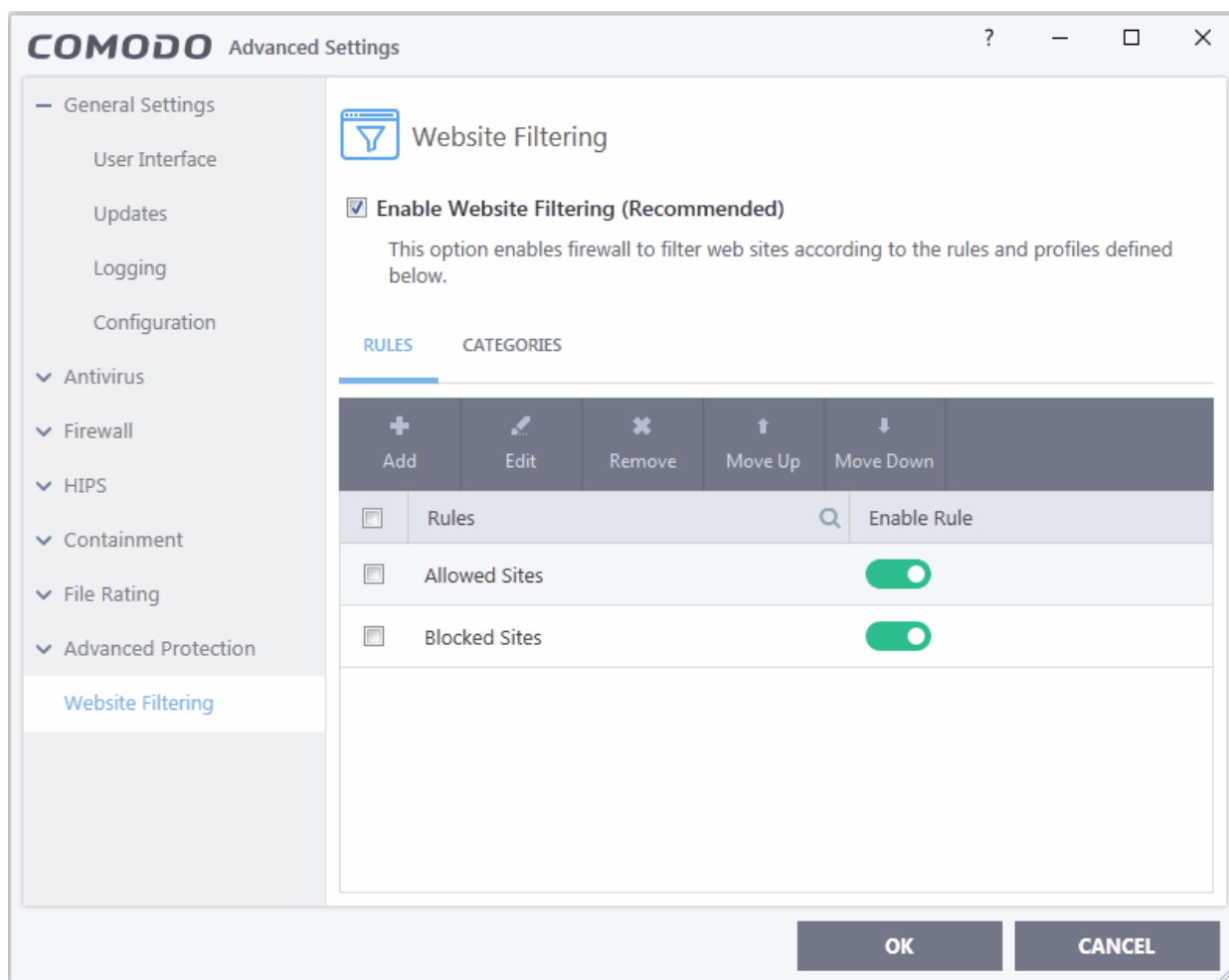
Overview:

- 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.

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

Click 'Settings' > 'Website Filtering' > 'Rules' tab

- The website filtering 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.

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
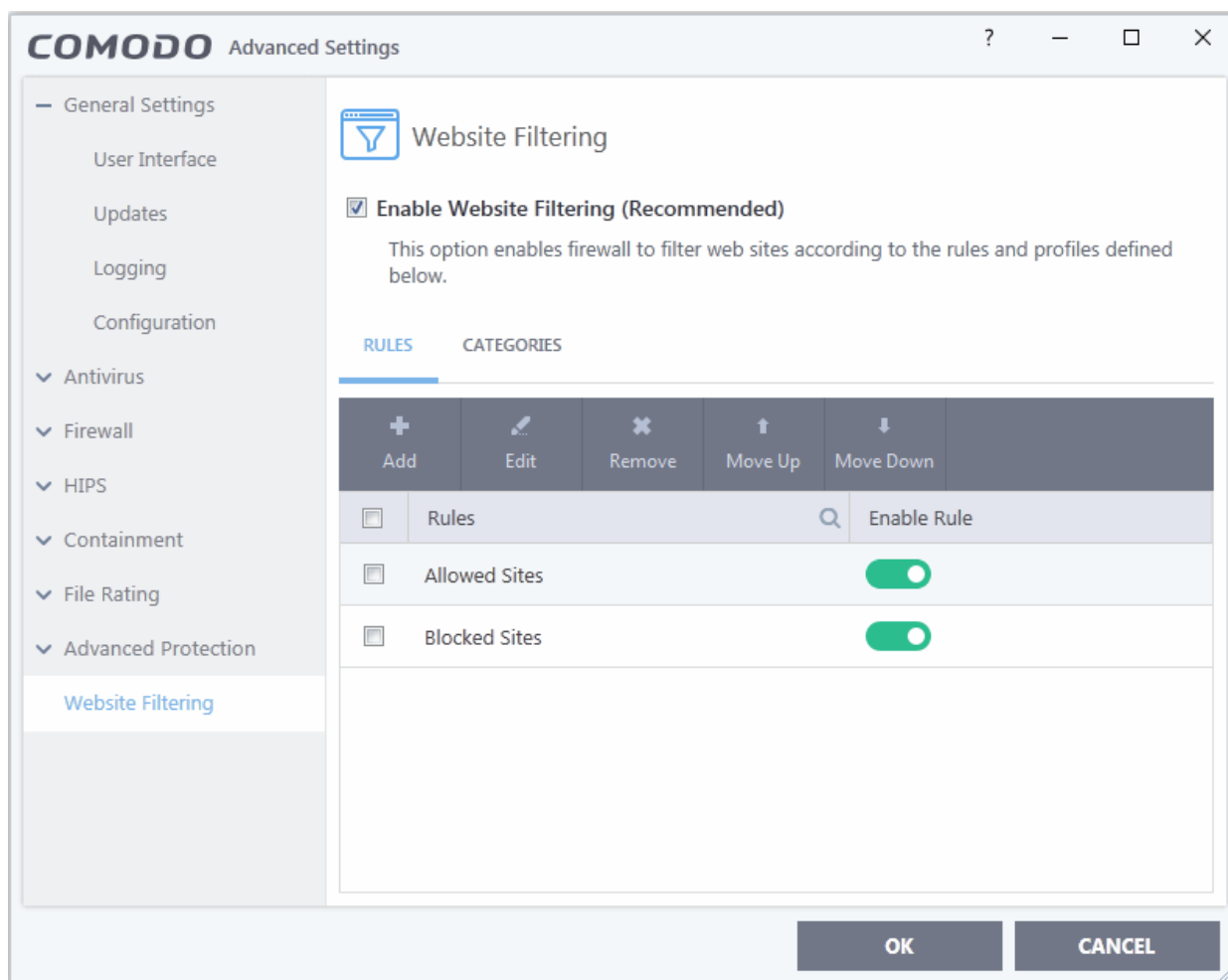
- The 'Enable Rule' switch allows you to turn a rule on or off.

- 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**

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.
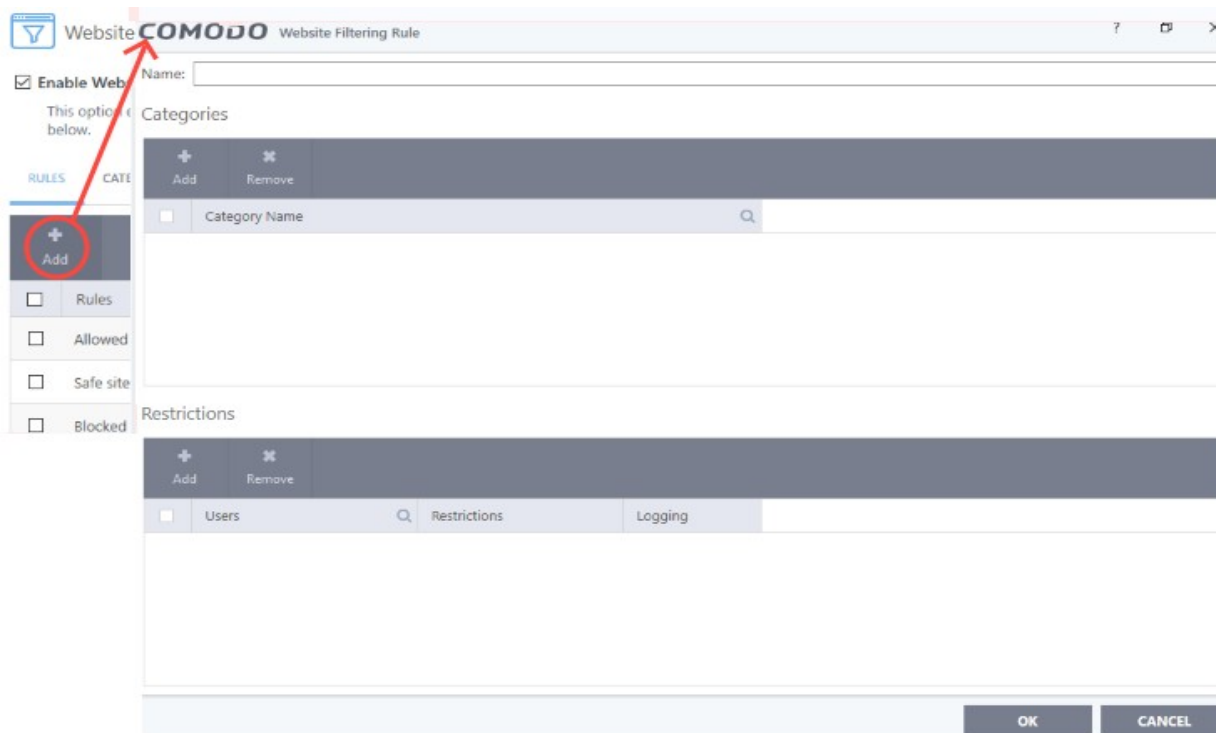
3. Enter a name for your new filter.

4. Select the categories that should be added to the filter:

   • Click the 'Add' button from the 'Category' pane
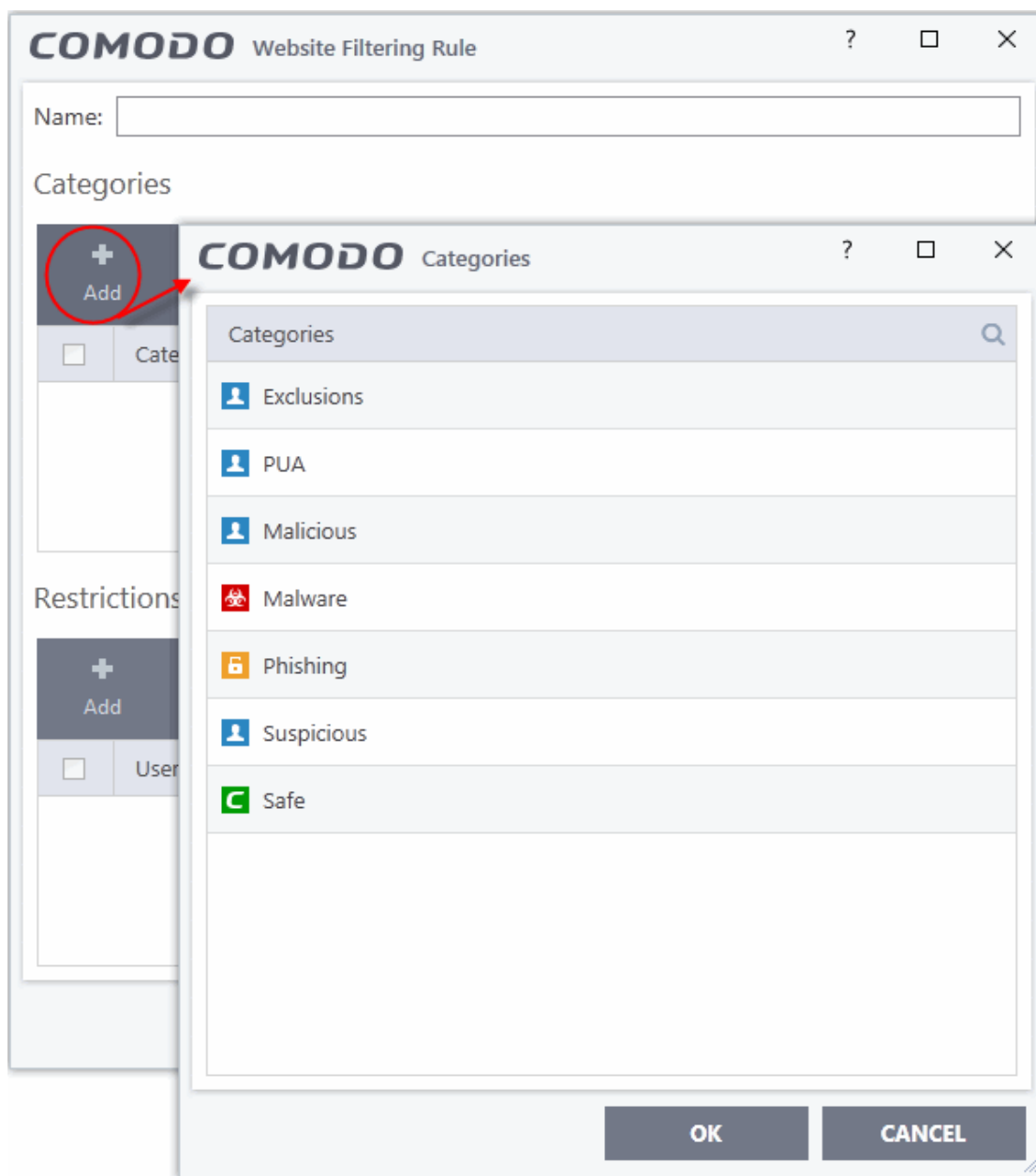
- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

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:
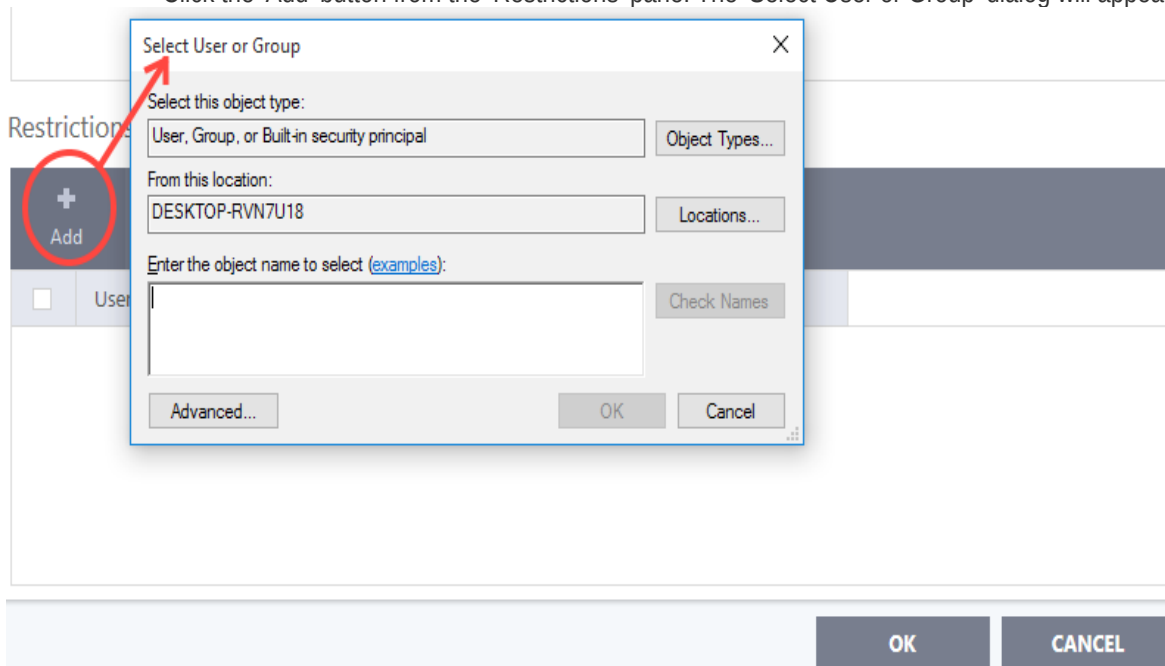
- • **Enter the object name to select** - add users to whom the filter should be applied. Names should be in the format:

  <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.
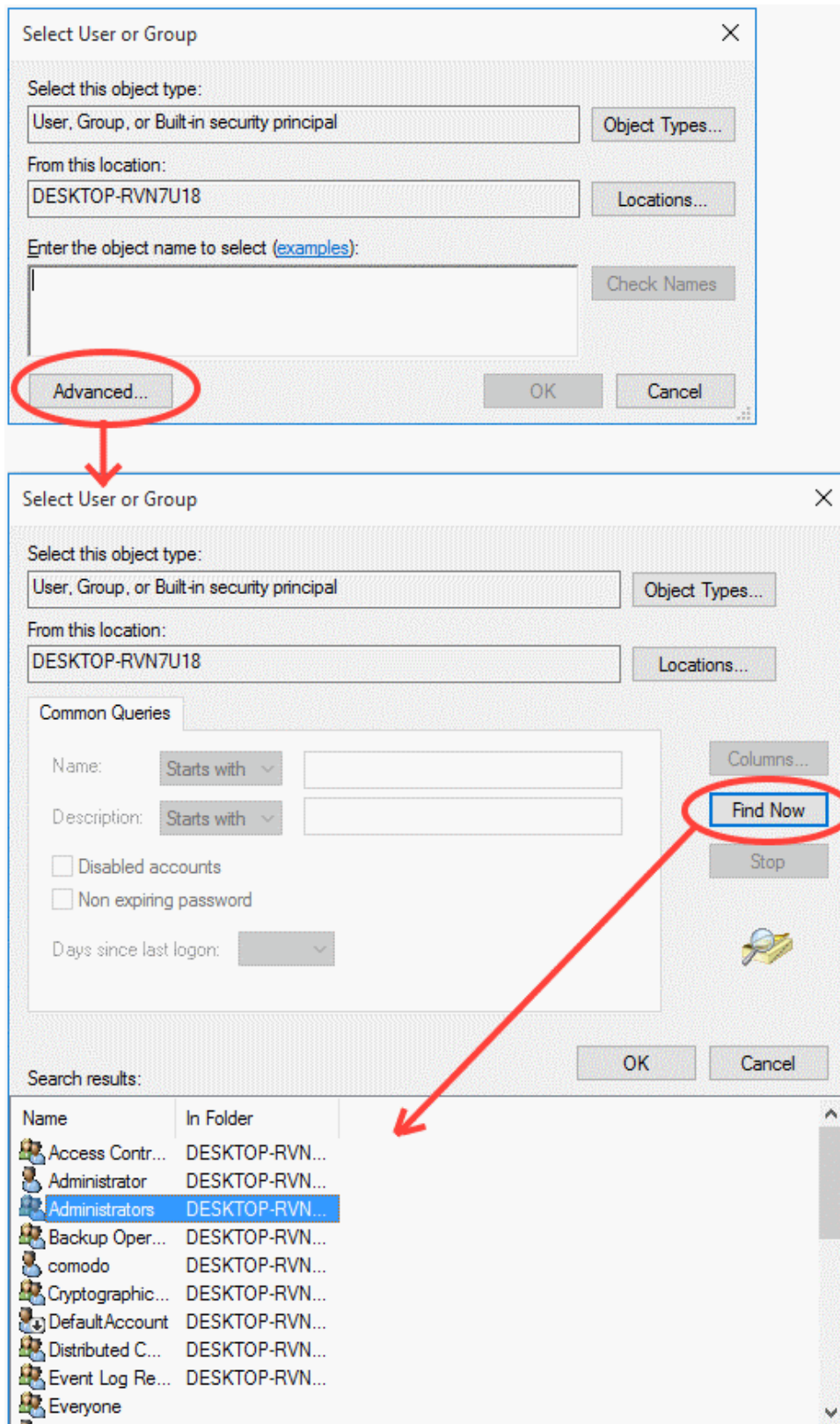
You next need to specify whether those users should be allowed or blocked from viewing the websites, or whether they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:

- **Allow** - The websites in the categories can be accessed by the user.
- **Block** - The websites in the categories cannot be accessed by the user.

- **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 lis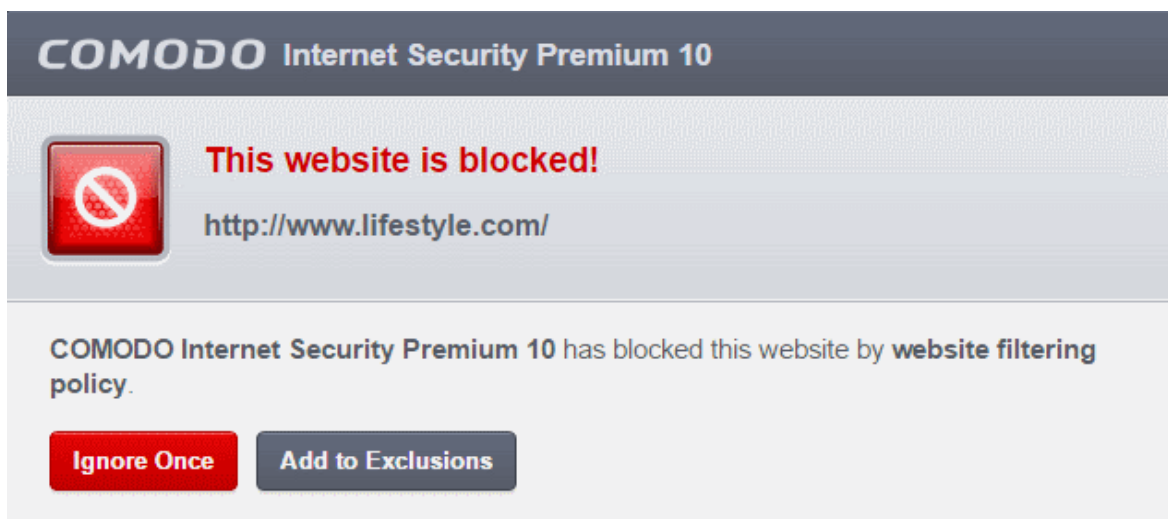t. If added to the exclusion list, the warning dialog will not appear for this website again. Please note that only the administrator can remove the websites from the exclusions list.

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
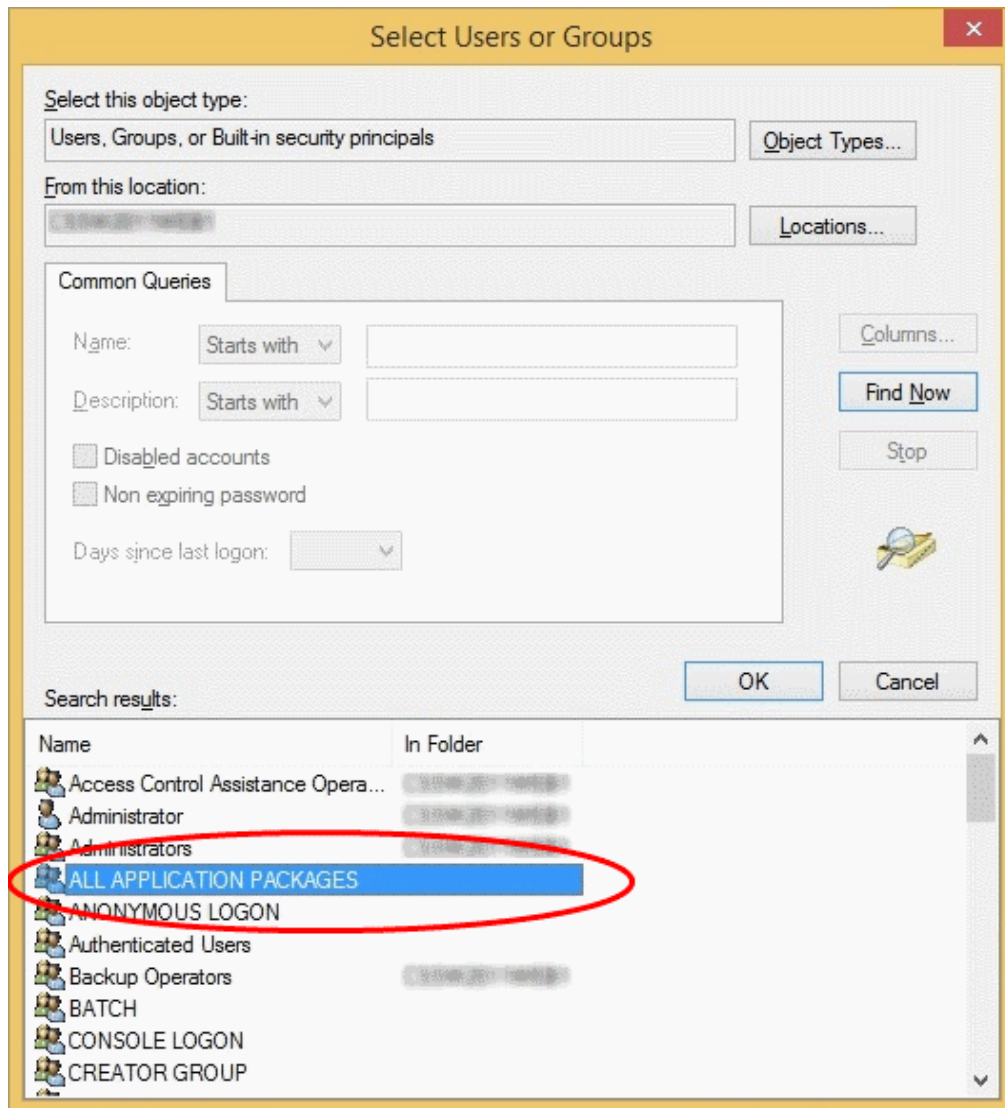
- Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom
- Click 'OK'
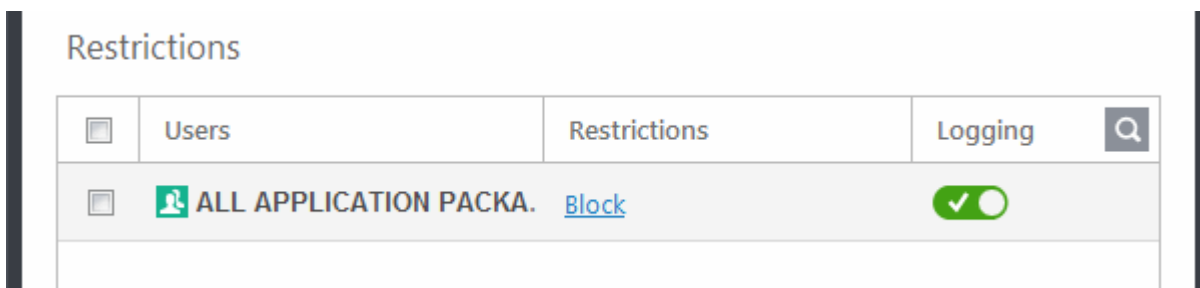
Edit existing rules

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.

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'.

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

Click 'Settings' > 'Website Filtering' > 'Categories' tab

*   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.

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
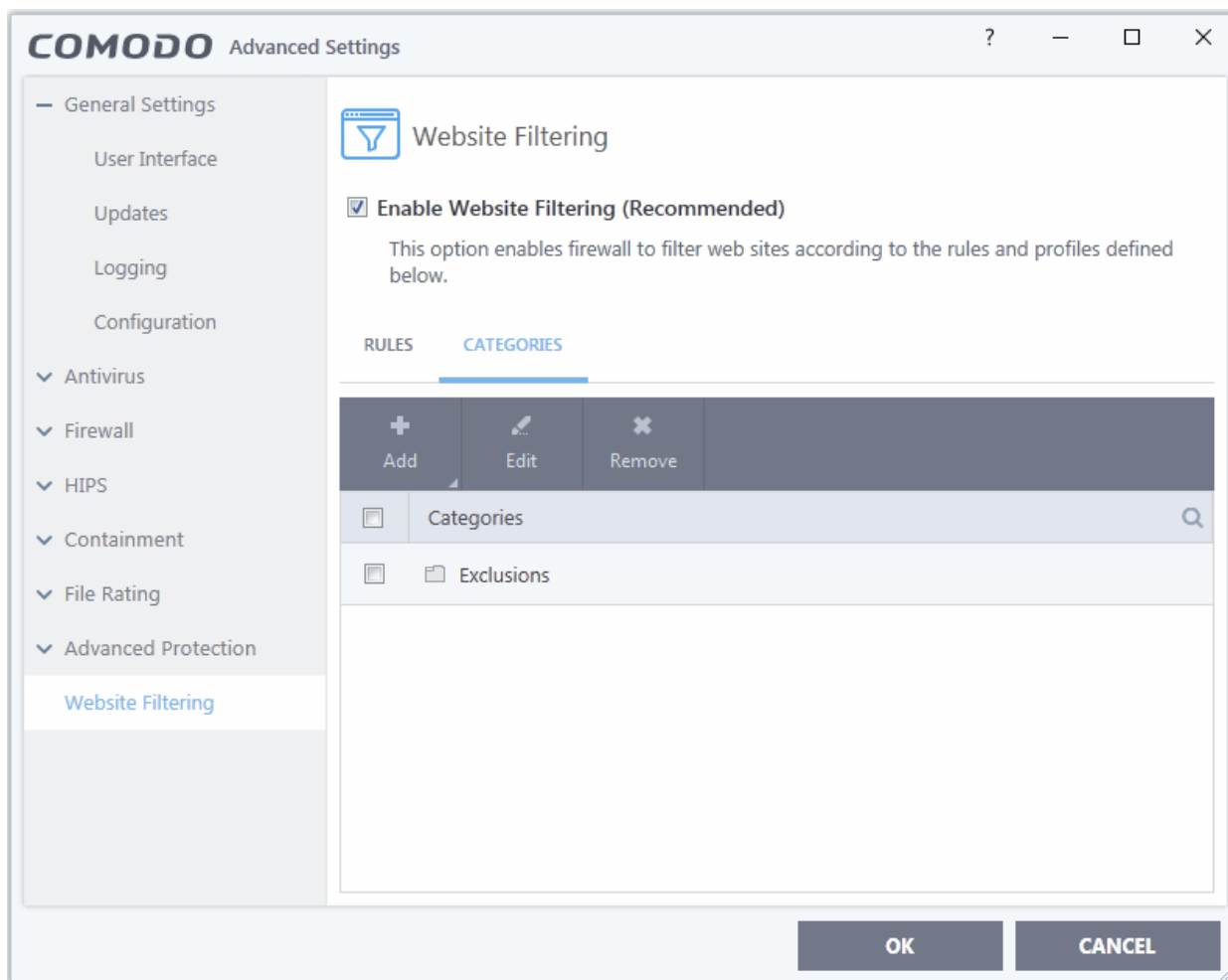
- Click the search icon to find a specific rule header. You can type rule names in full or in part.

The categories pane allows you to:

- **Add a new category of websites**
- **Rename a category**
- **Remove unwanted websites from a category**
- **Remove a category**

Add 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.
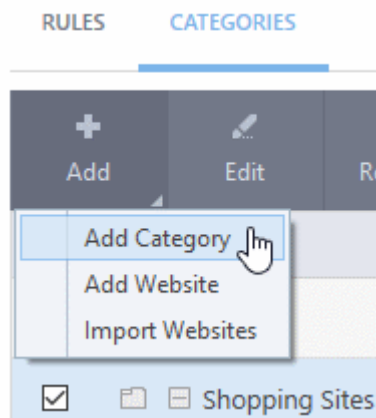
Type a name for the category in the 'Add Category' box:
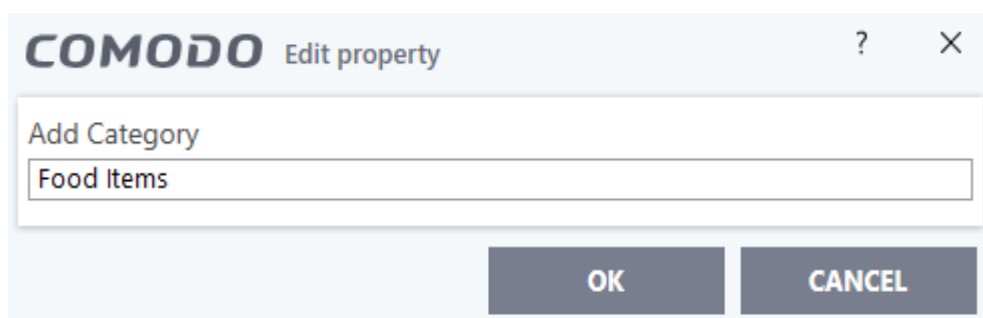
The new category will be listed in the 'Categories' tab:

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**

Manually specify websites

1. Select the 'Category' from the list.

2. Click the 'Add' button.

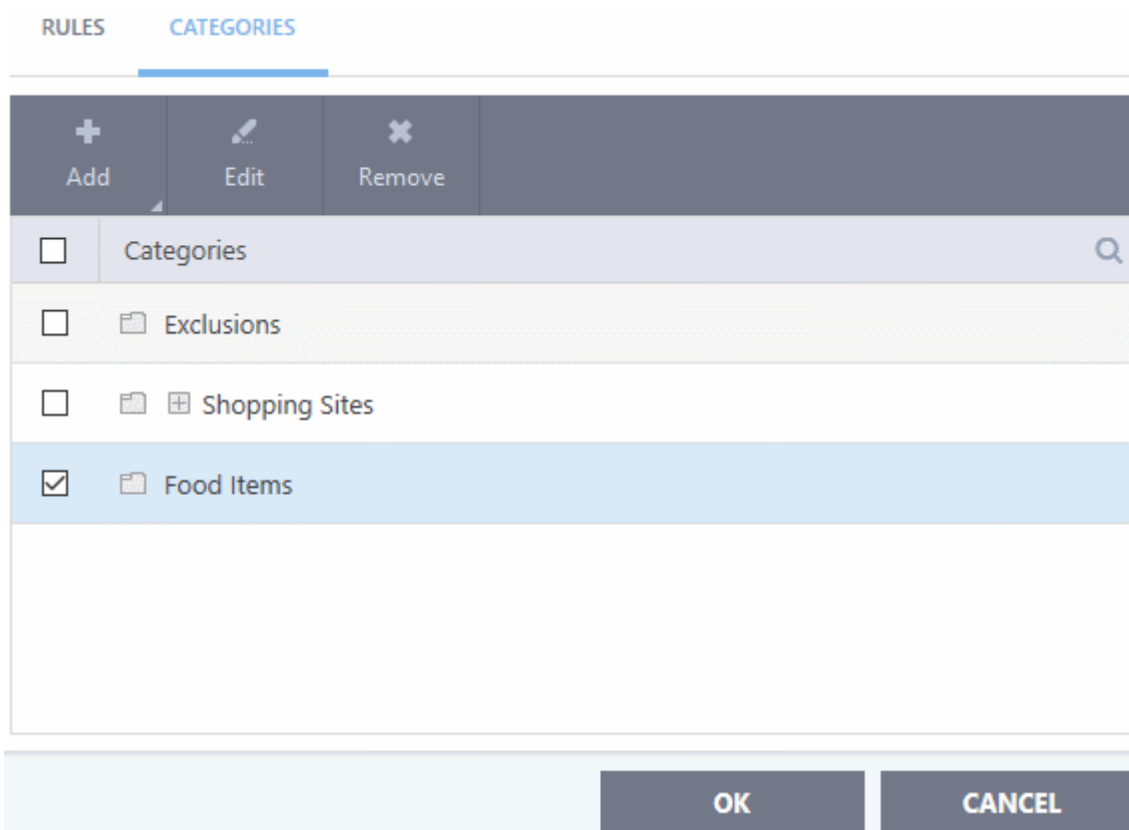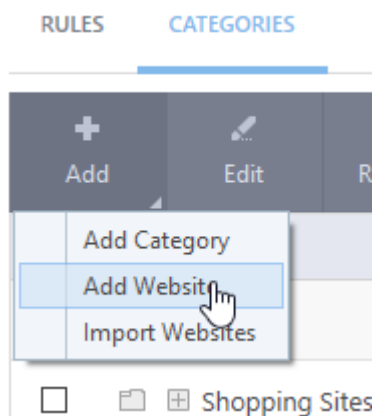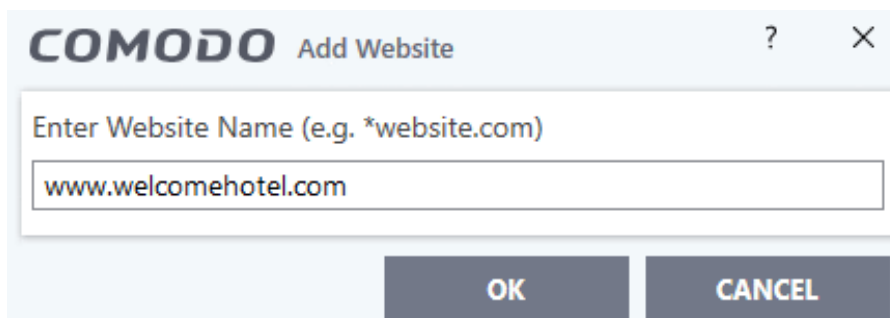3. Select 'Add Website' from the drop-down menu.

Type the address of the website you wish to add to the category in the 'Add Website' box:

- 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.

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.
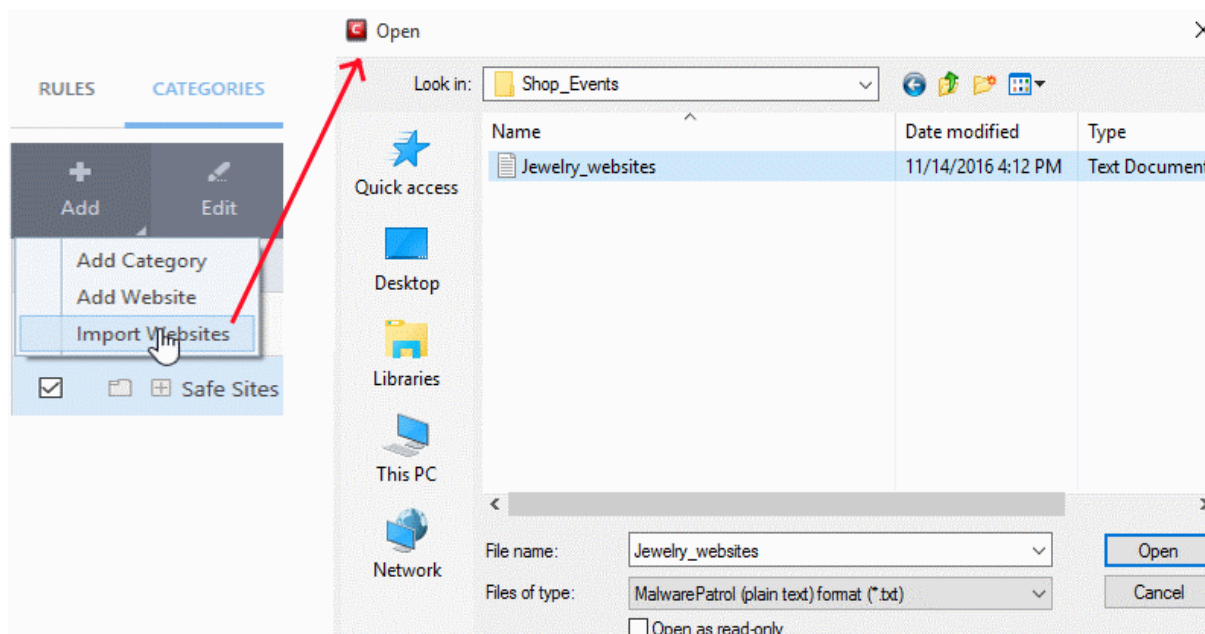
Note: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.

4.   Click 'Open'.

CIS will automatically add the websites specified in the text file into the selected category.

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.

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.

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.

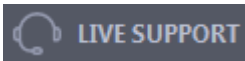4. Right-click then select 'Remove' from the drop-down menu.

> **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 technicians do the work for you.

Visit **https://www.geekbuddy.com/** for more details.

*   Click [LIVE SUPPORT] at the top of CIS home screen to open a chat session in your default web browser.

*   Download and install the GeekBuddy chat tool from **www.geekbuddy.com/cgb** to take advantage of the full suite of support services. Services include remote desktop support and PC optimization.

GeekBuddy is included with CIS Pro and Complete. The GeekBuddy section of this guide is broken down into the following sections:

*   **Download and Install GeekBuddy**
*   **Overview of the Services**
*   **Activation of Service**
*   **Launch the Client and Using the Service**
*   **Accept Remote Desktop Requests**
*   **Uninstall Comodo GeekBuddy**

7.1. Download and Install GeekBuddy

*   Download the Geekbuddy setup file from **https://www.comodo.com/home/download/download.php? prod=geekbuddy** and save it on your hard drive.

*   Double click on 'Setup.exe' and click 'Run' to start the installation wizard.
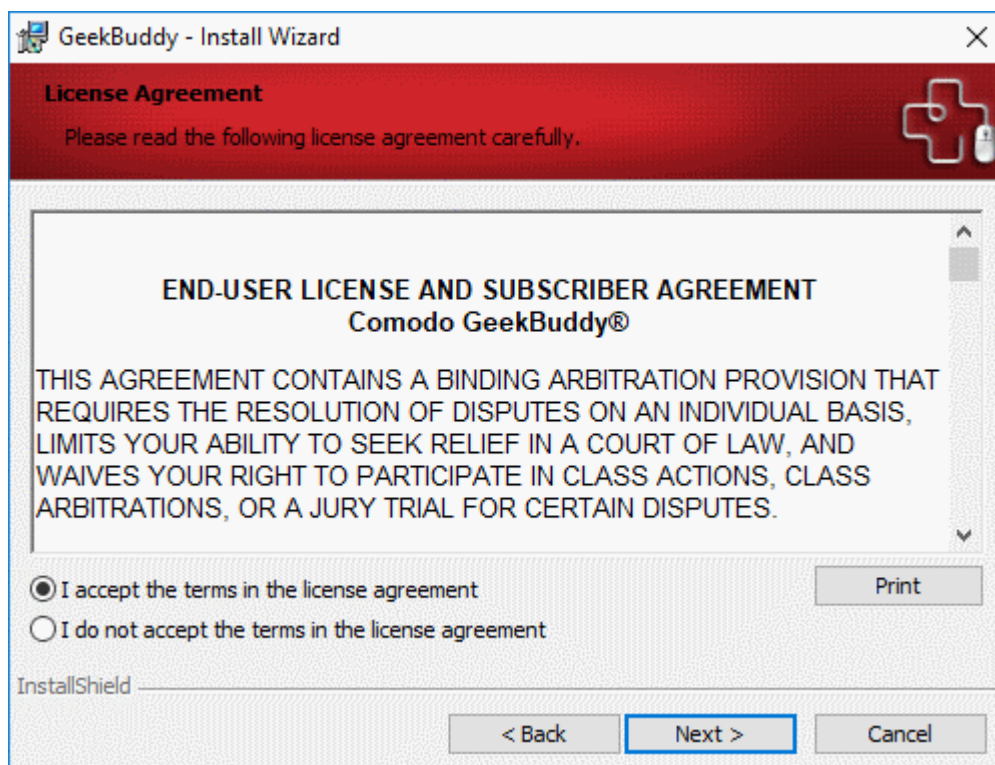
Step 1 - Welcome Screen

The setup program starts automatically:

- Click 'Next'

Step 2 - End User License Agreement

Complete the initialization phase by reading and accepting the EULA.

- Click 'I accept the terms in the license agreement' and click 'Next' to continue installation.

Next, choose whether you want to also install Comodo Internet Security Essentials:.

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

- Click 'Next'

Step 3 - Installation

The installation starts with the following notification screen:
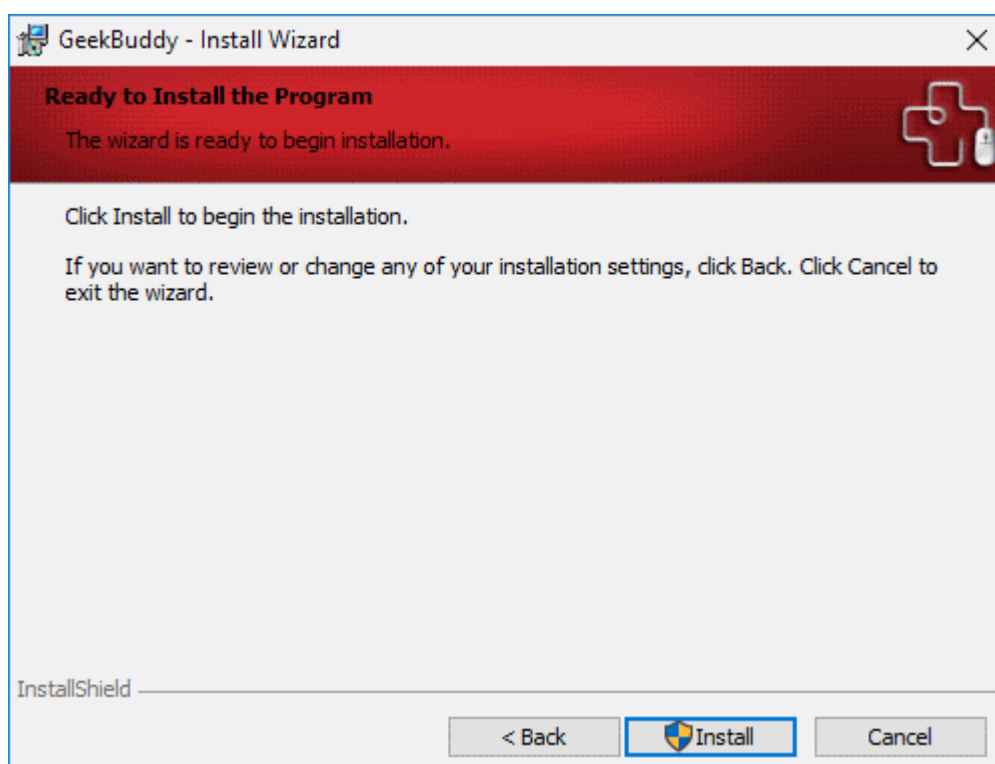
- Click 'Install' to start the installation:
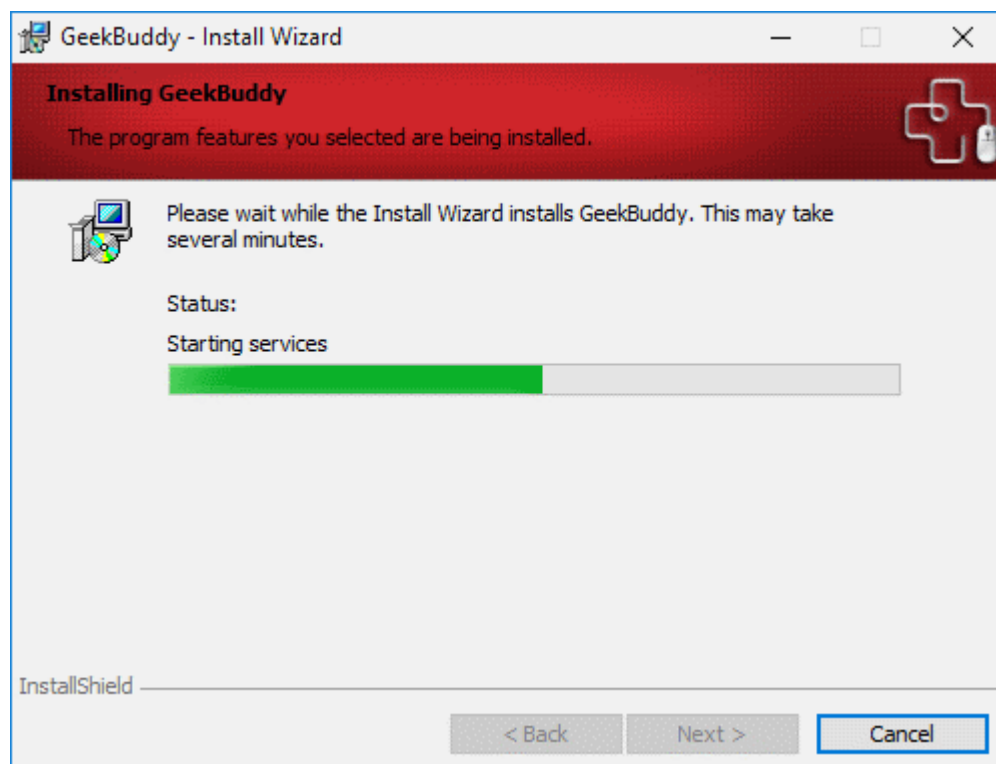
The following dialog will be shown when installation is complete:
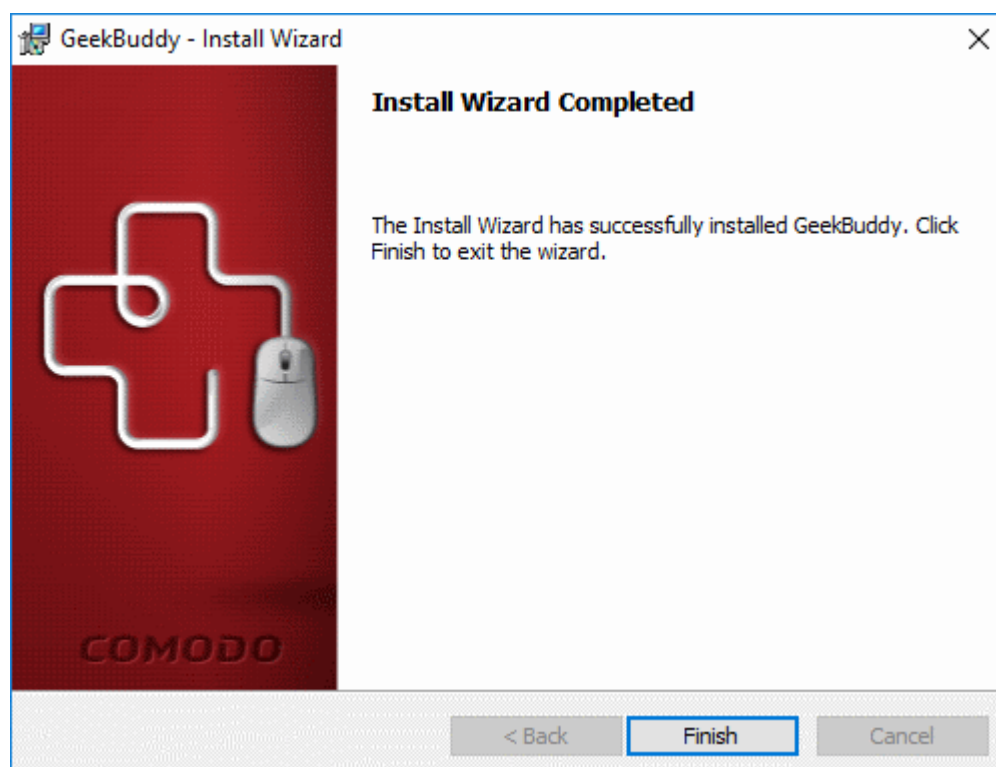
- Click the 'Finish' button to complete installation and launch the program:

- Click 'Connect to Your Geek' in the last page to start the chat session:

- Type 'start' in the text box and click the 'Start' button

7.2. 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.
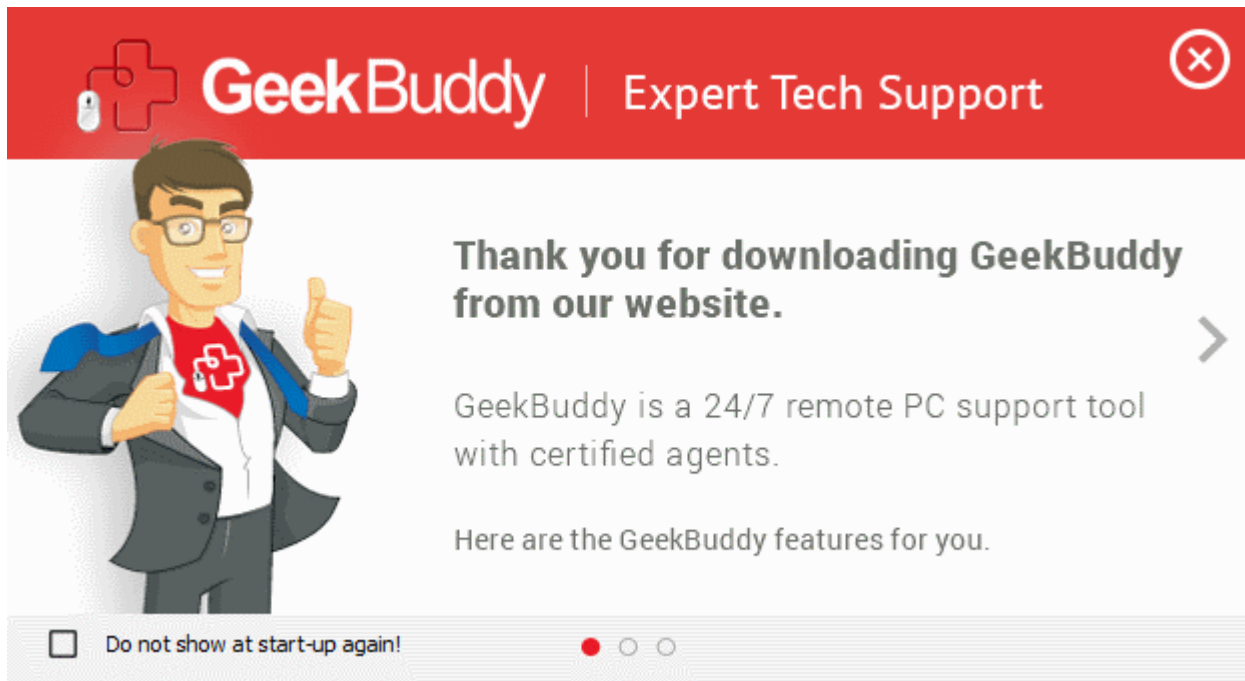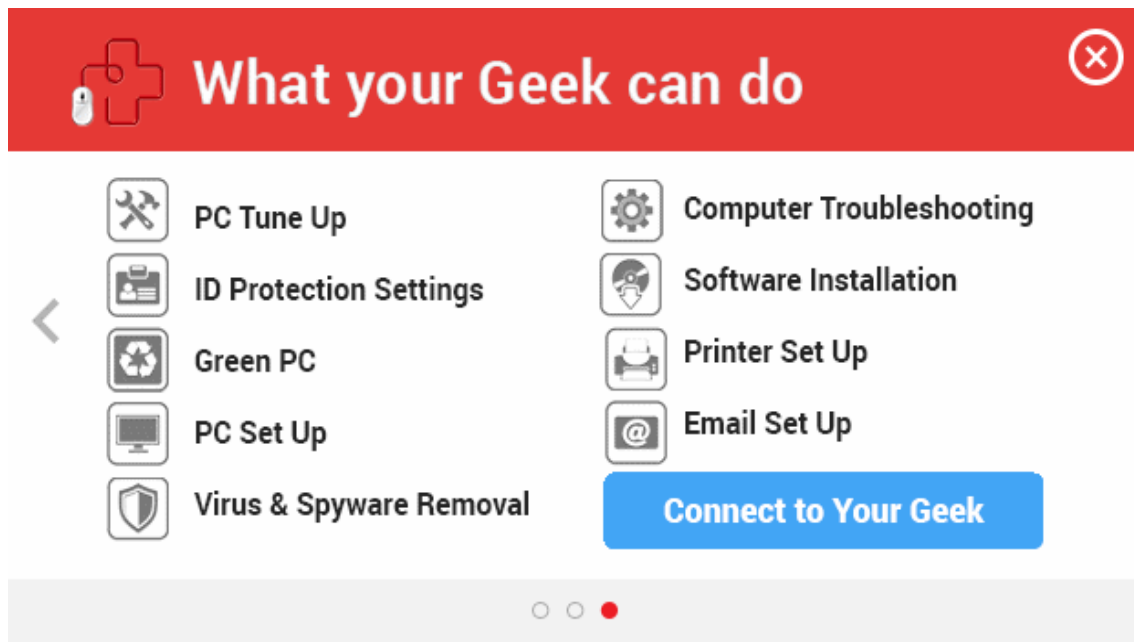- **Internet and Online Identity Security** - Optimization of your computer's security settings to prevent loss of sensitive data and identity theft.
- **Printer or Email Account Setup** - Installation or updating of printer software and/or drivers, checking ink levels and configuring your printer to 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.

7.3. Activation of Service

GeekBuddy installs with a trial license, but you should purchase a full license to get the most out of the service.

- Click the desktop shortcut to start GeekBuddy

- The GeekBuddy chat screen will open:

- Click the 'About' link at top-right then click 'Change your license key':
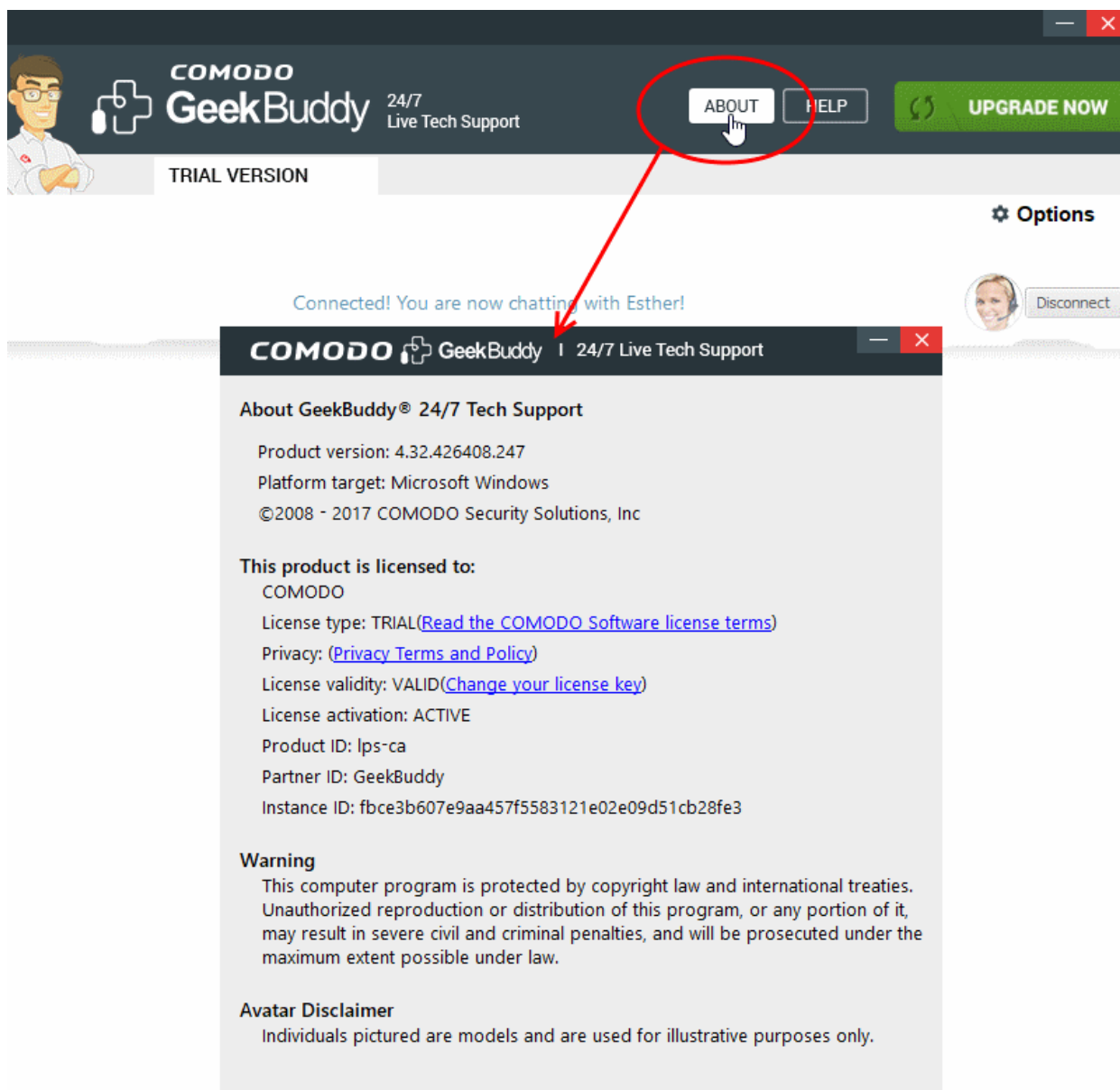
This opens the license activation screen:
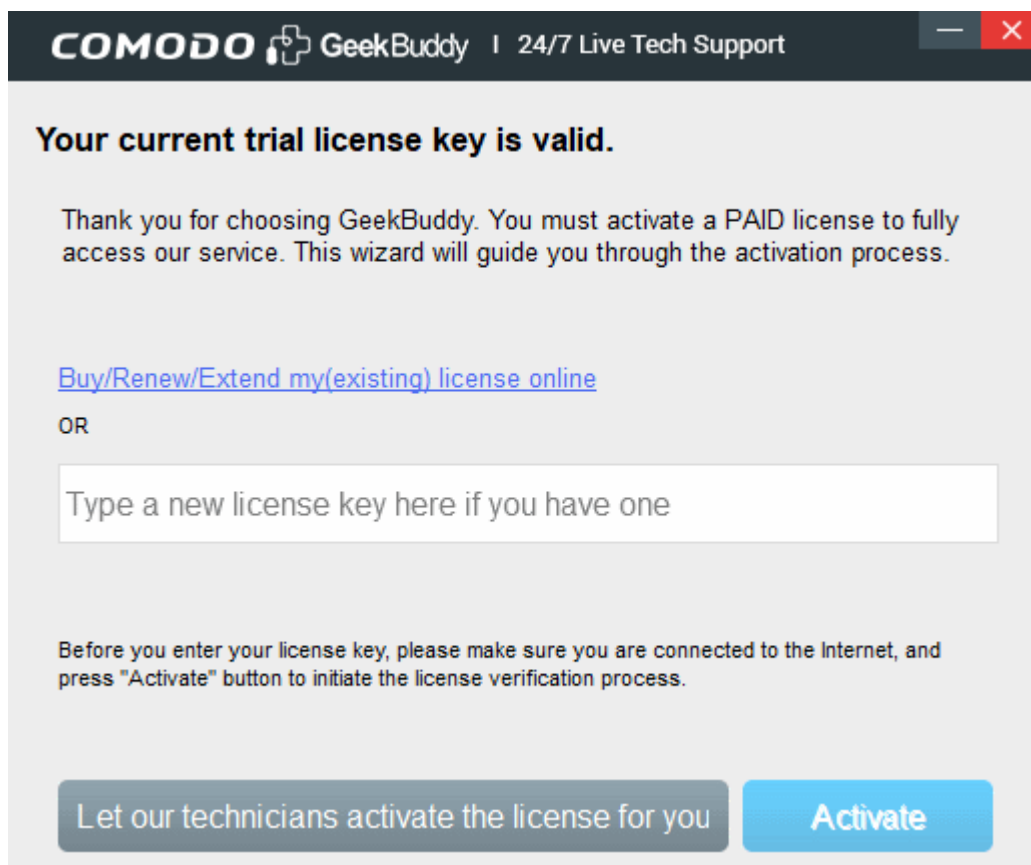
- Click 'Buy/Renew/Extend...' to purchase a license online.
- CIS Pro and Complete users - enter your CIS license key in the space provided and click 'Activate'.

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:

- **Launch the Client and Use the Service**
- **Accept Remote Desktop Requests**

7.4. Launch the Client and Use the Service

You can start a live chat with a GeekBuddy expert as follows:

- Double-click the GeekBuddy desktop icon:

    OR

- Click 'Live Support' at the top-right of the CIS interface:
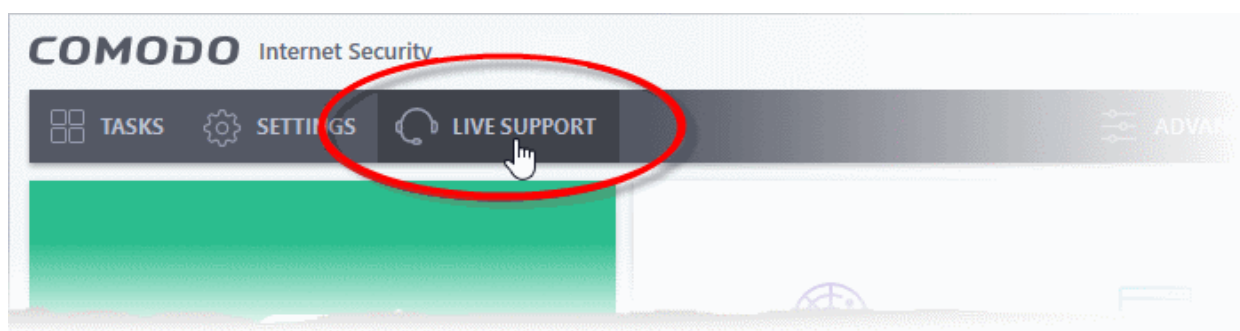
OR

- Windows Start Menu: Click *Start* > *All Programs* > *Comodo* > *GeekBuddy* > *GeekBuddy*

The GeekBuddy home screen opens:
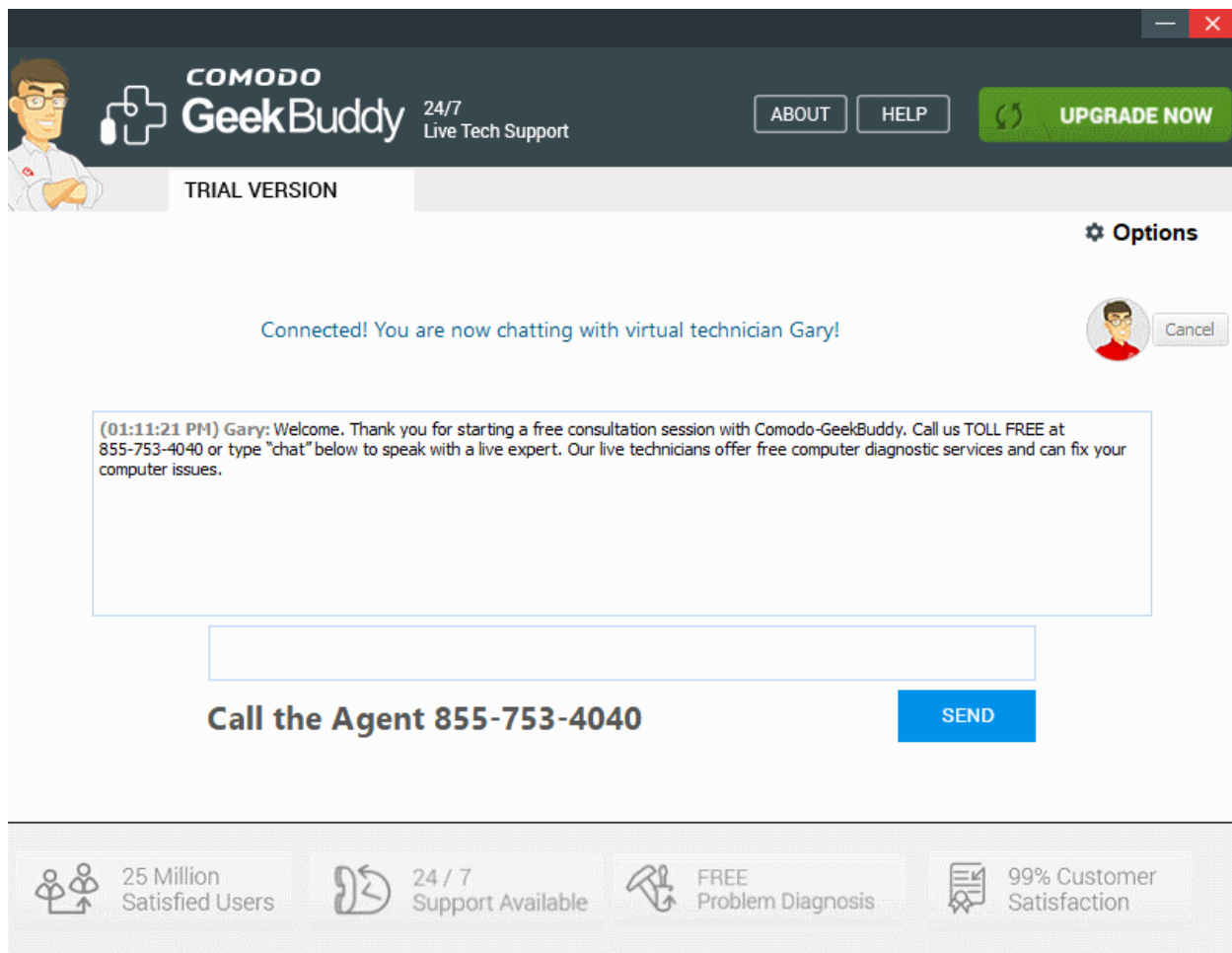
- Type your issue in the field OR enter an invitation code
- Click the 'Send' button.
- You will be immediately connected to a GeekBuddy.

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

7.5. Accept 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:
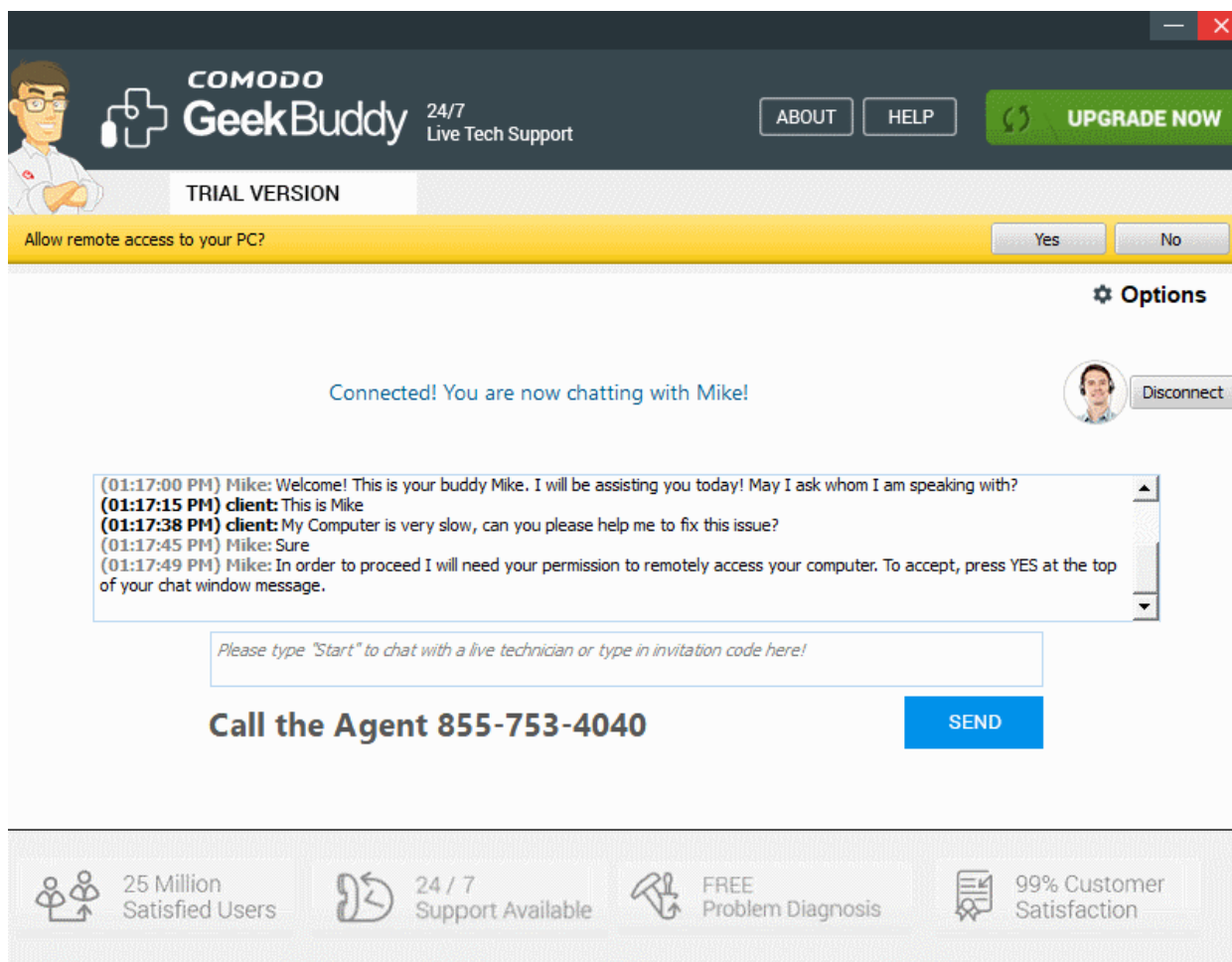
- Click the 'Yes' button in the yellow bar to allow the technician to connect to your computer.

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 answer and clicking 'SEND'.

The technician will disconnect from your computer when their work is complete and ask if you need 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. Uninstall Comodo GeekBuddy

- Open Windows settings then 'Apps' > 'Apps and Features'

  OR

- Type 'Add Remove Programs' into Windows search
- Select 'GeekBuddy' from the list of currently installed programs then click 'Uninstall':
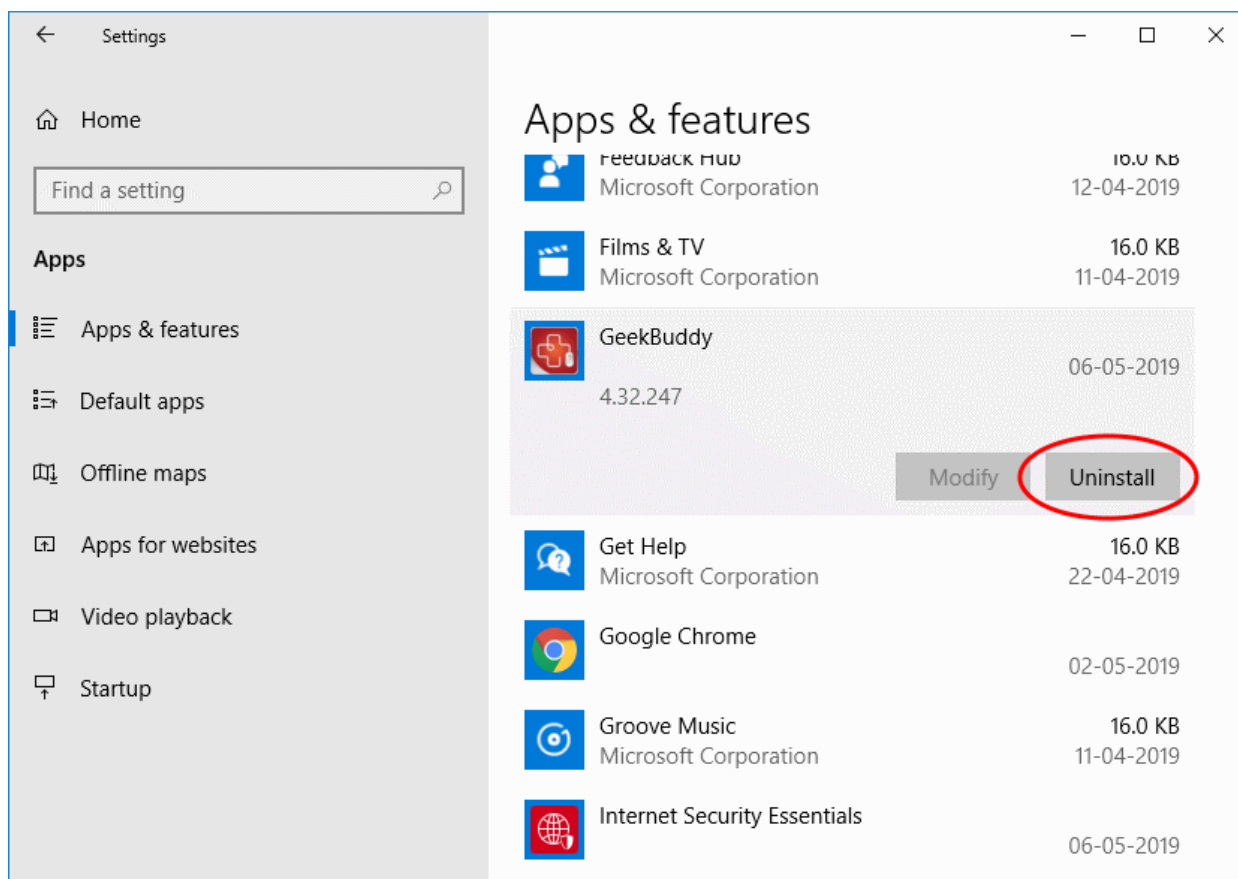
- The application will be removed from your system.

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.
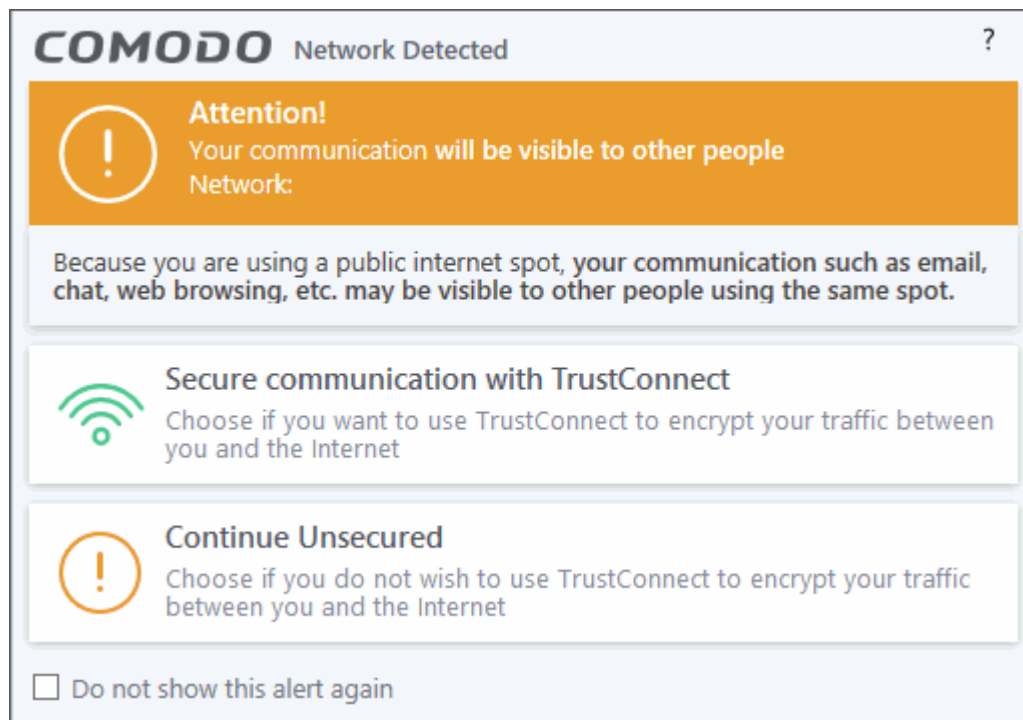
- TrustConnect is designed to eliminate these types of data hijacks by preventing criminals from attacking or scanning your system from the local network that you are using to connect to the Internet.

- 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 and the application is installed automatically along with CIS. When a new wireless connection is established by your system, a Network Detected dialog is displayed.
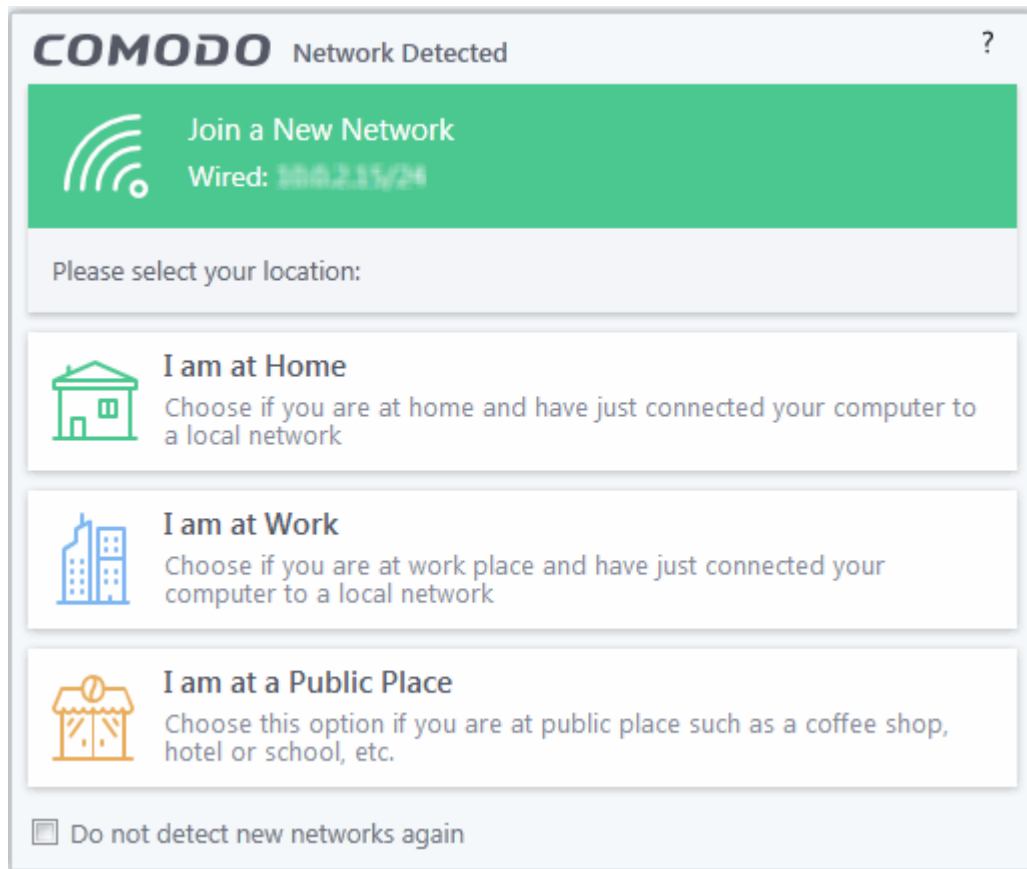
Select your location from the dialog. A TrustConnect alert is displayed depending on the settings configured in **Firewall Settings** interface.
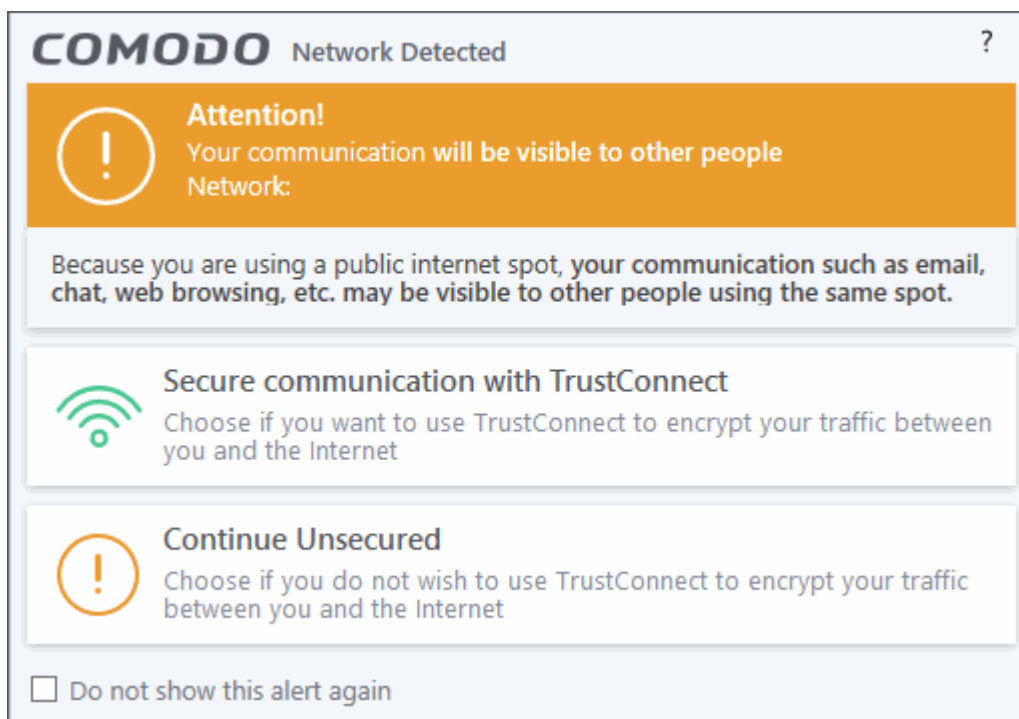
Select whether you want to connect to the Internet via TrustConnect thus encrypting the traffic between your system and the Internet or use the unsecured network.

If you choose 'Secure communication with TrustConnect', CIS will establish the connection via TC.
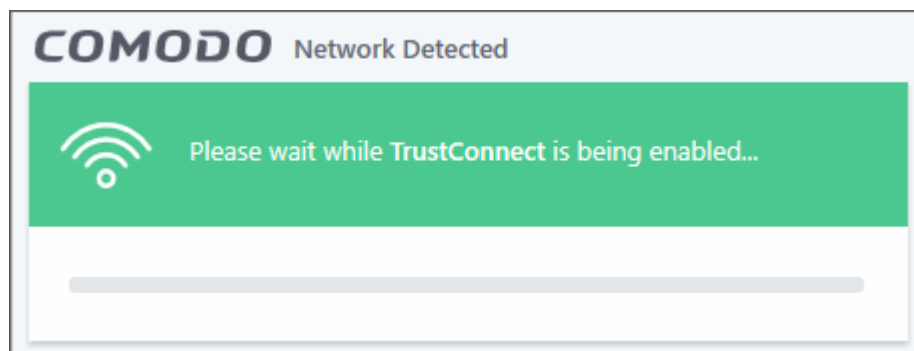
...and on successful connection, you can view the details in the system tray.
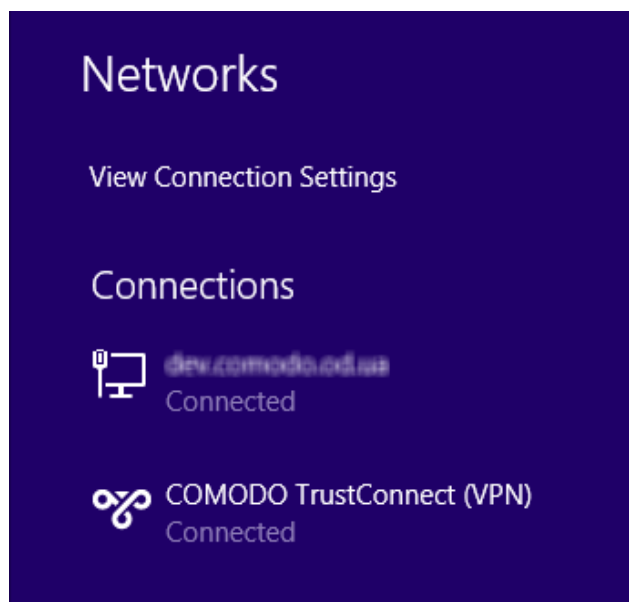
Choose 'Continue Unsecured' option if you do not want to establish an encrypted connection.

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.
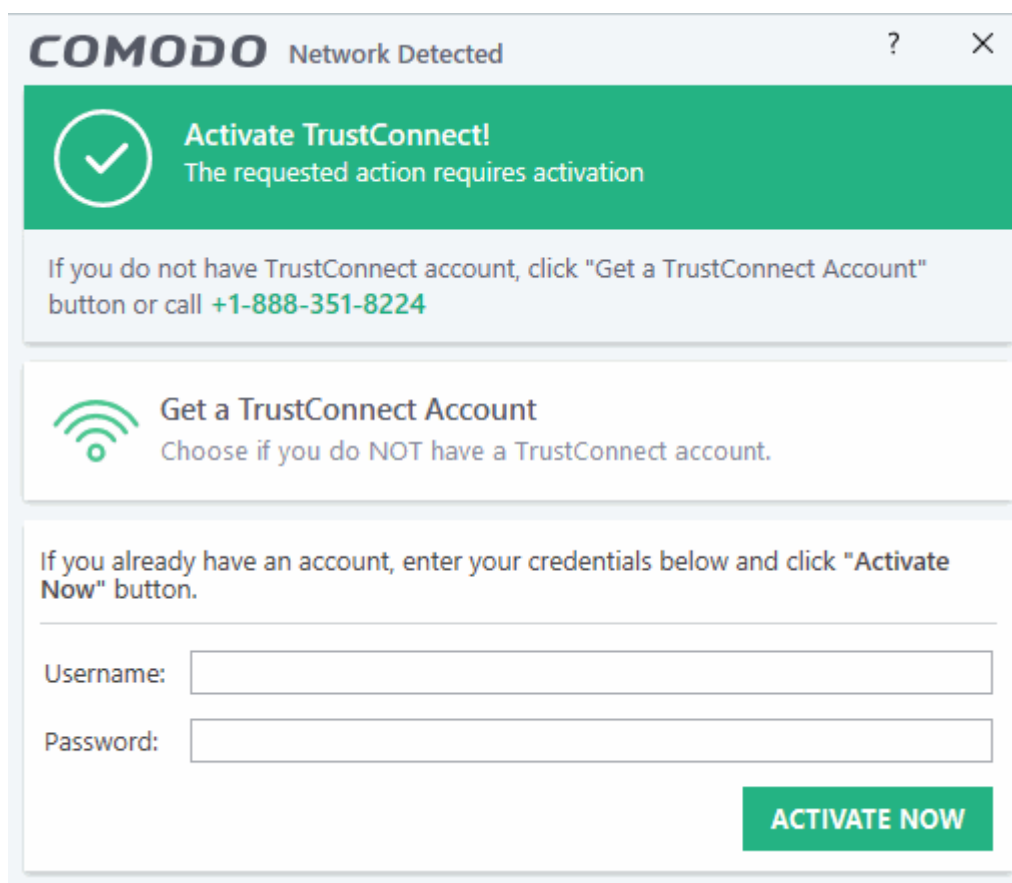
Find your TC service credentials

- 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 is displayed.

The TC service login and 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 is 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.

- Click 'Tasks' > 'General Tasks' > 'Cloud Backup'
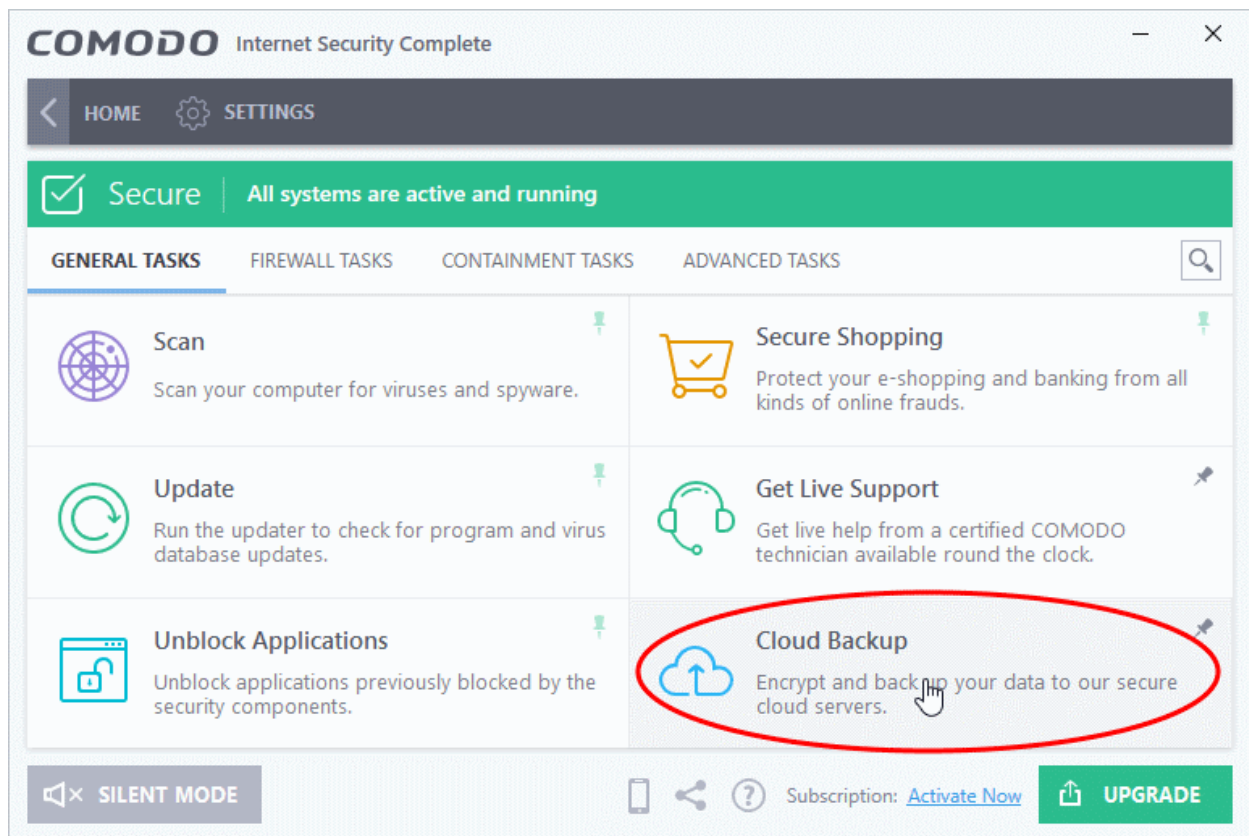
If you have not activated CIS, then you can create an account from the 'Create New Account' form. If you have already activated CIS using the license key, an account is created for you automatically.
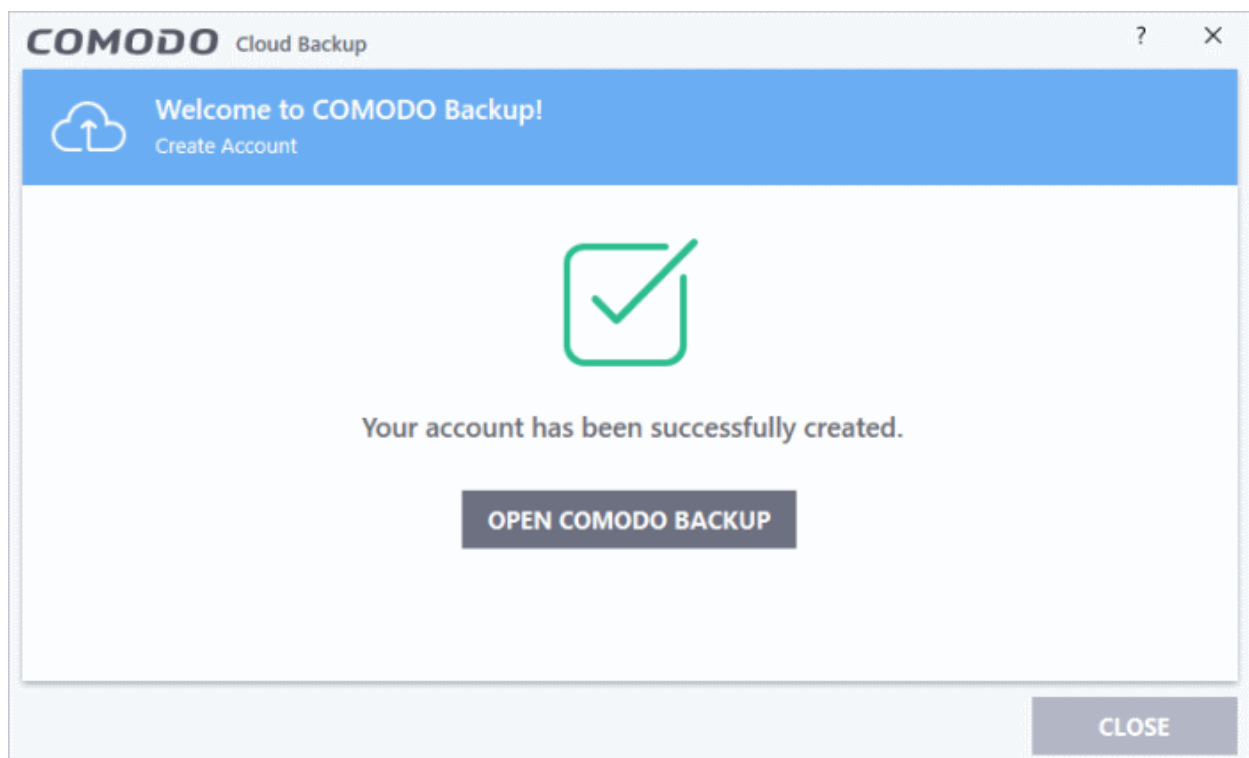
- Click 'Open COMODO Backup' to access your online backup management console.

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**.

11. Comodo Internet Security Essentials

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

Please use the following links to find out more:

- **What is Comodo Internet Security Essentials?**
- **What is a man-in-the-middle attack?**
- **How does Comodo Internet Security Essentials protect me from a man-in-the-middle attack?**
- **What is the install location of Comodo Internet Security Essentials?**
- **How do I update CISE?**
- **Understand alerts and configure exceptions**
- **How do I view CISE help?**
- **How do I view the version number and release notes?**
- **How do I remove Comodo Internet Security Essentials**

What is Comodo Internet Security Essentials?

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

CISE runs as a background process and will alert you if a site uses a potentially malicious certificate. You will have the option to discontinue the connection (recommended) or to continue.
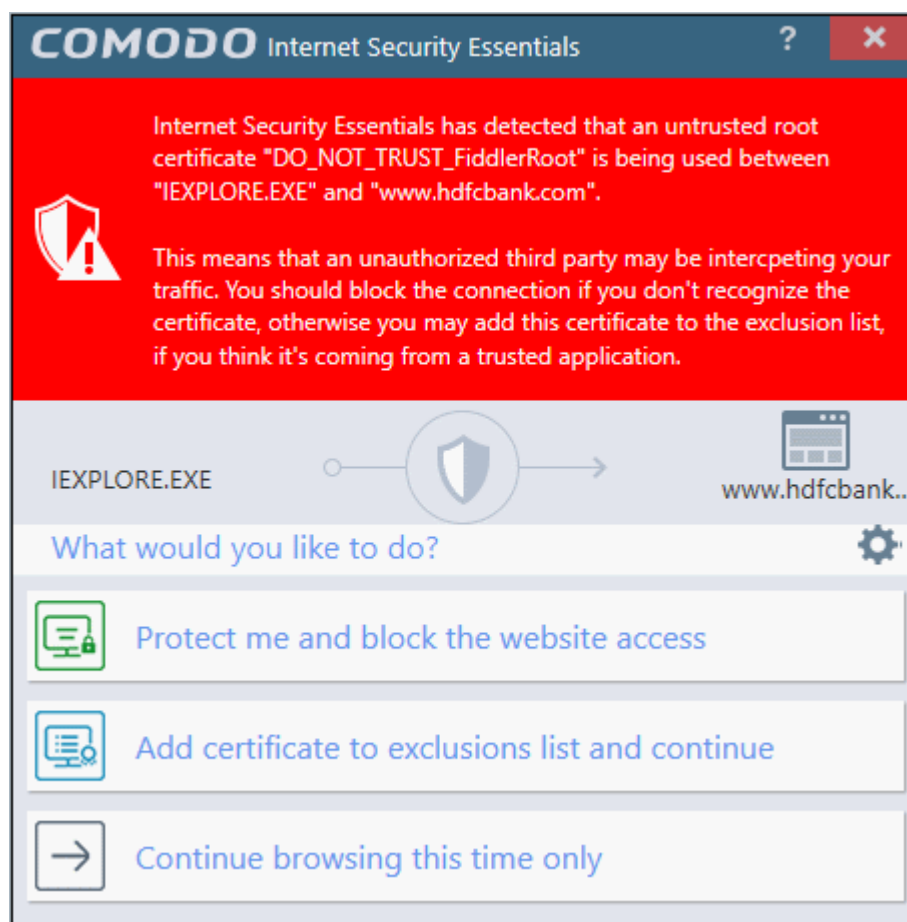
CISE blocks man-in-the-middle attacks attempts by verifying certificates against Comodo's trusted root certificate list. This functionality is especially important if you are accessing sensitive websites while on a public Wi-Fi such as those found in an cafe, park or airport.

Please note, Internet Explorer is currently the only supported browser.

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

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

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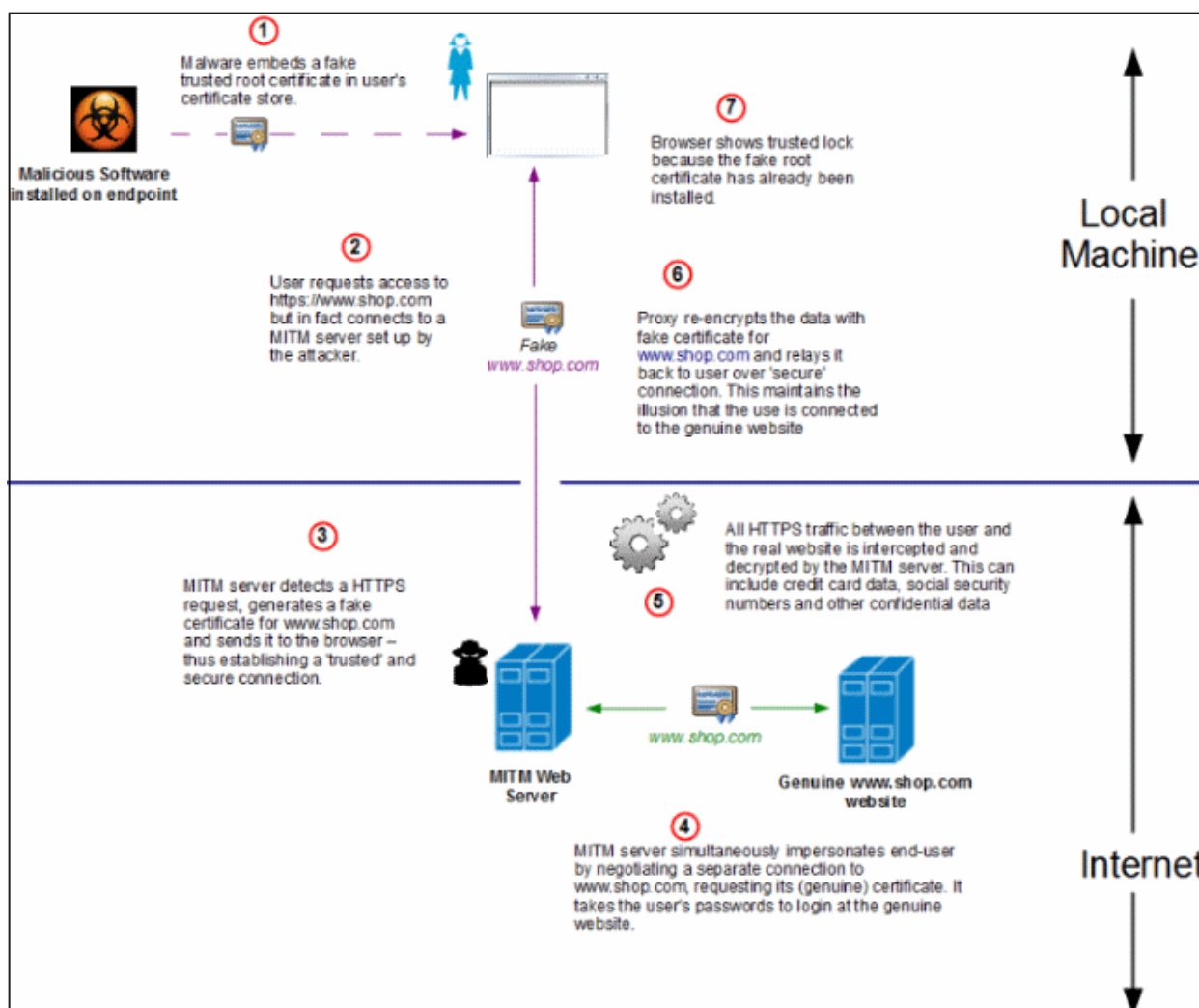
How does Comodo Internet Security Essentials protect me from a man-in-the-middle attack?

Comodo Internet Security Essentials blocks these attacks by independently verifying all certificates used for secure connections against an internal, verified list of trusted root certificates. The following diagram shows how CISE will

thwart a man-in-the-middle attack:
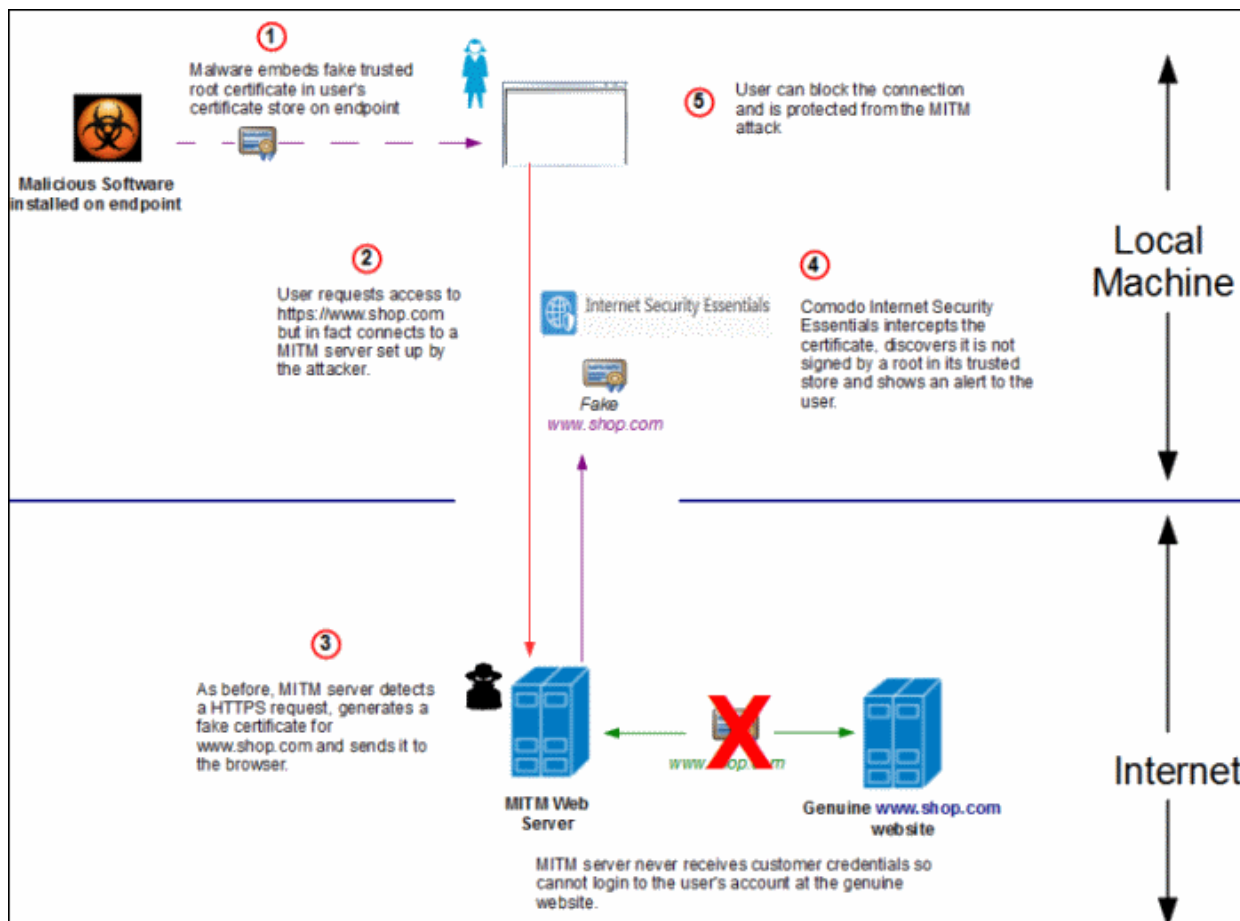
What is the install location of Comodo Internet Security Essentials?

By default, Comodo Internet Security Essentials is installed at:

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

How do I update CISE?

You can update manually or configure automatic updates.

To check and update manually

- Open Comodo Internet Security Essentials
- Click the help icon at the top right
- Select 'Check for Updates' from the options:
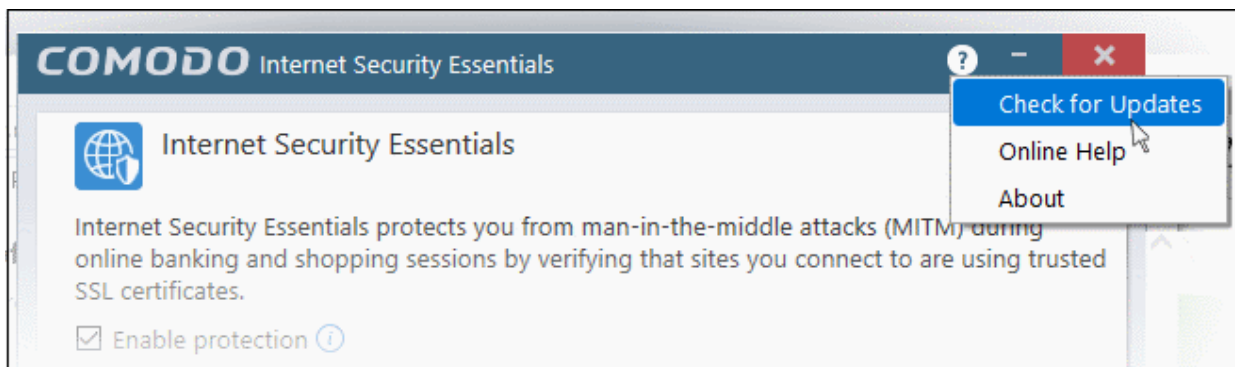
- CISE will check Comodo servers for any updates. Please make sure your internet connection is active.

- Click 'Apply'

Updates will be automatically installed if available:

- Click the 'Finish' button to finalize the installation.

- Click 'Re-start system now' to apply the updates.

To configure automatic updates

Open the CISE configuration screen

- via the Windows Start Menu:

    Click Start and select All Programs > Comodo > Internet Security Essentials

    OR

- by clicking the cog icon in the alert:

This will open the CISE configuration screen:
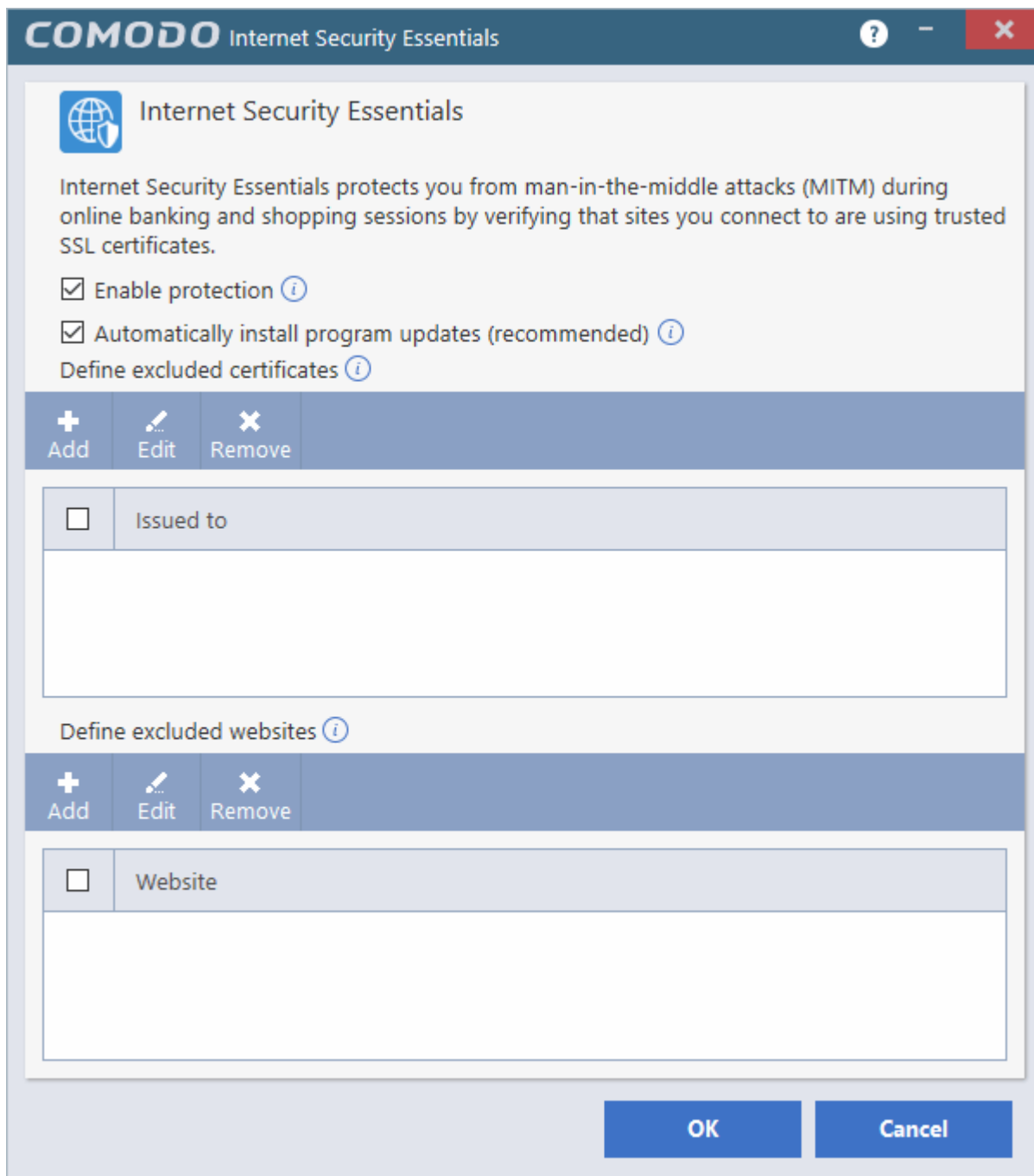
- Enable 'Automatically install program updates (recommended)'
- CISE will check Comodo servers every day for updates
- You will be alerted if an update is available:
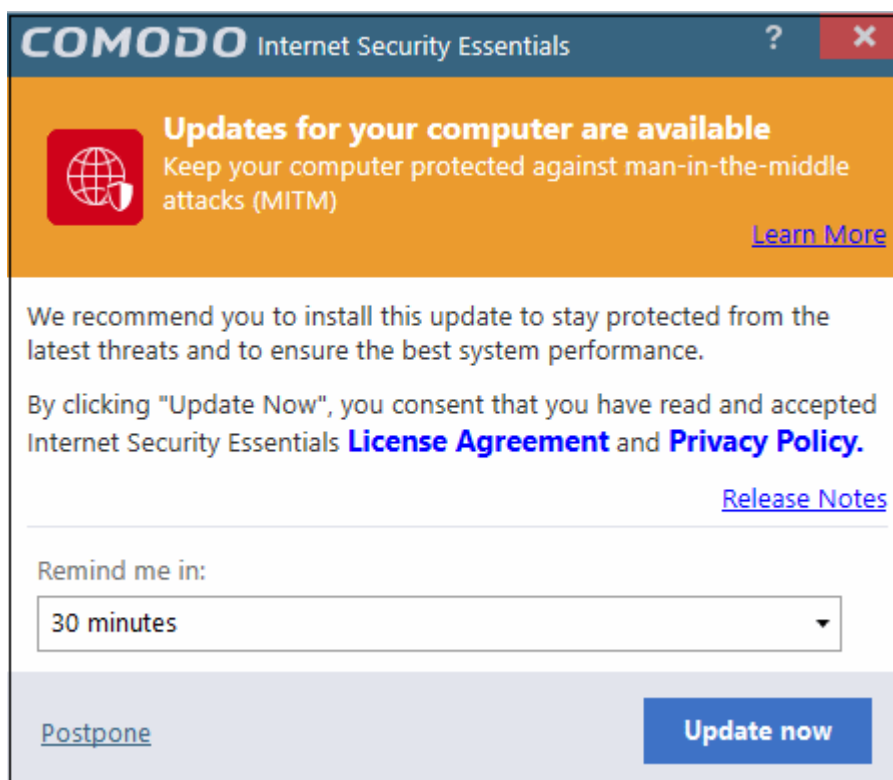
- Click 'Update Now' to apply the update immediately.
- To apply the update later, select when you would like to be reminded from the drop-down and click 'Postpone'.
- You will see the following confirmation when the updates have been successfully installed:
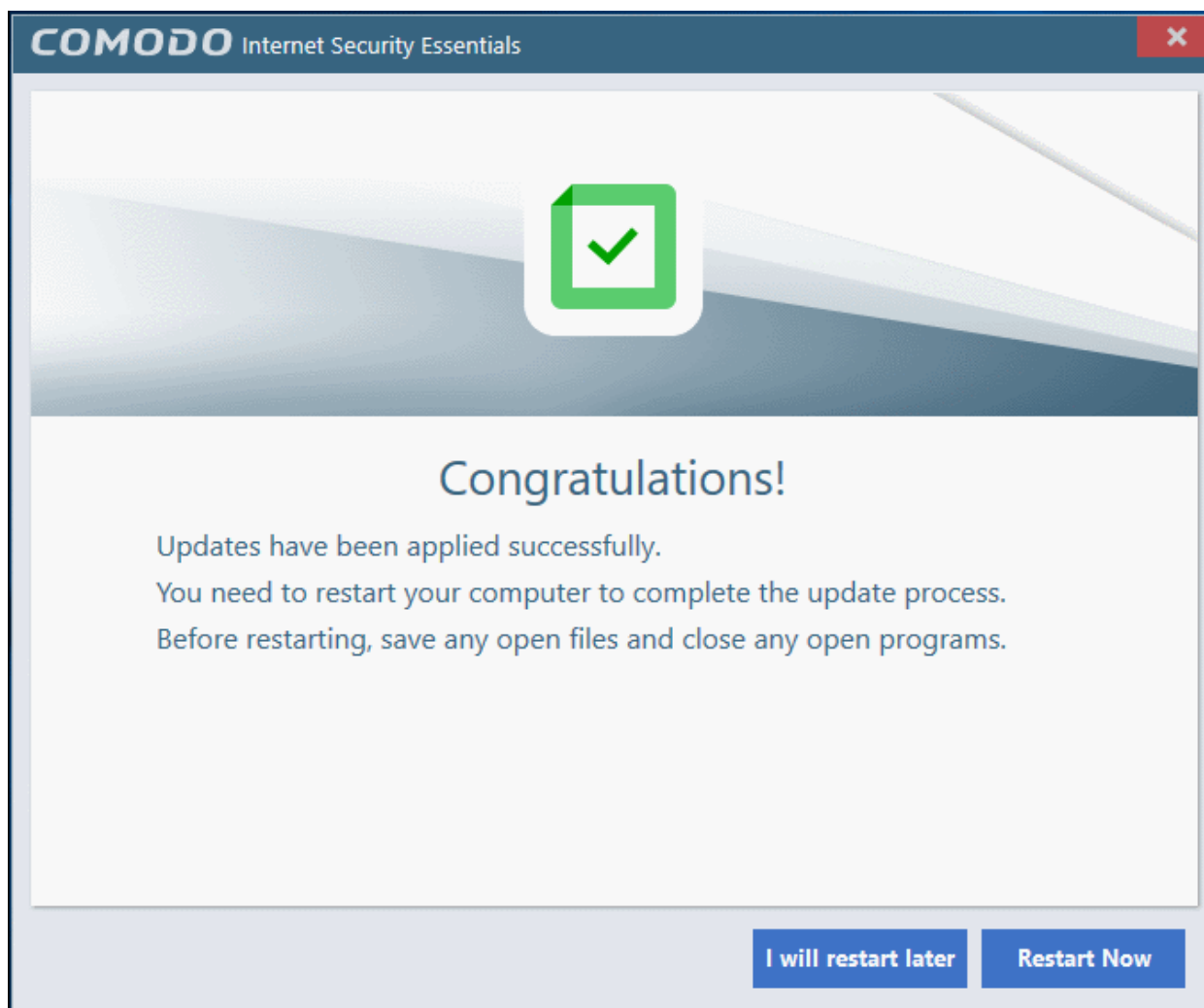
- Click 'Restart Now' to reboot your computer and finalize the update

- Click 'I will restart later' to restart at later time

Note: CISE will automatically install updates if:

1. The application has not been updated for a long time and has become obsolete.
2. There are compatibility issues with the existing build or a serious vulnerability has emerged.

These kind of updates will be applied even if automatic updates are disabled.

The following dialog will be shown after a forced update:
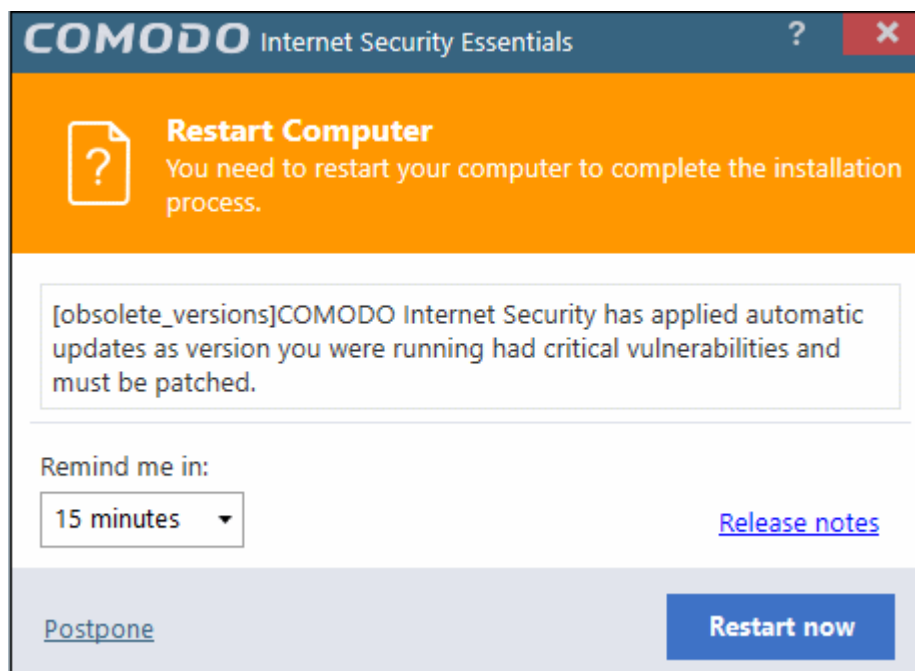
- Click 'Restart Now' to restart the system immediately.

To apply the update later, select when you would like to be reminded from the drop-down and click 'Postpone'.

Understanding alerts and configuring exceptions

If CISE detects that a website is potentially using a fraudulent certificate it will present you with an alert similar to the following:
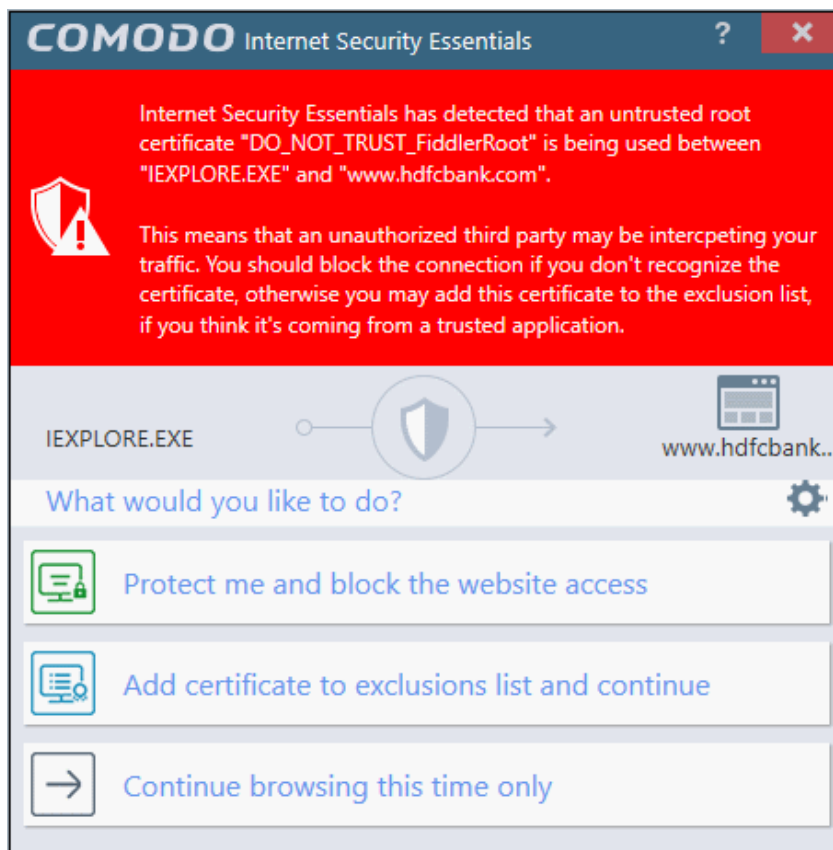
The alert means that the website you are visiting may be fraudulent as it is using a certificate signed by a root that is not in CISE's internal store of trusted root certificates.

- Protect me and block website access - Closes your connection to the website (recommended)

- Add certificate to exception list and continue - Adds the certificate to the whitelist and allows the connection to proceed. The root certiicate will not be flagged if CISE detects it in future on any sites. Only choose this option if you are sure the website can be trusted or is using, for example, a self-signed certificate that you have already been made aware of. Do not choose this option if this is one of your regular shopping or banking websites.

- Continue browsing this time only - Accept the connection only for the current session. CISE will warn you again if it detects this certificate next time.

You can whitelist certificates and websites in two ways:

- via the Windows Start Menu:

  Click Start and select All Programs > Comodo > Internet Security Essentials

  OR

- by clicking the cog icon in the alert:
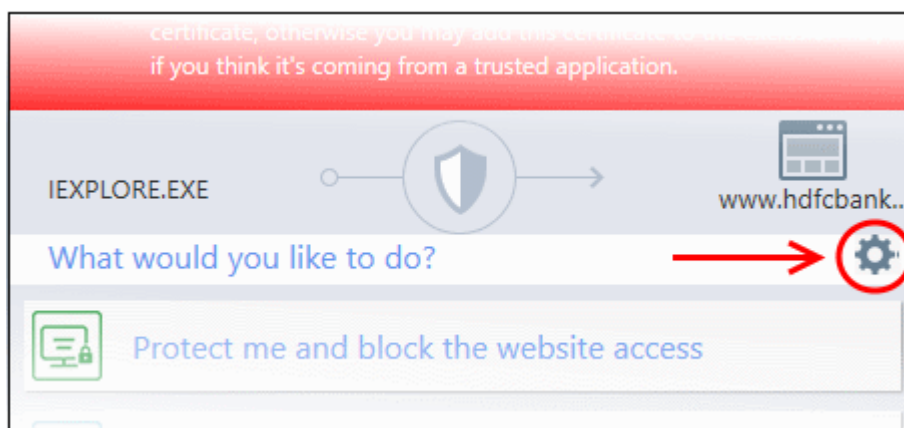
This will open the CISE configuration screen:
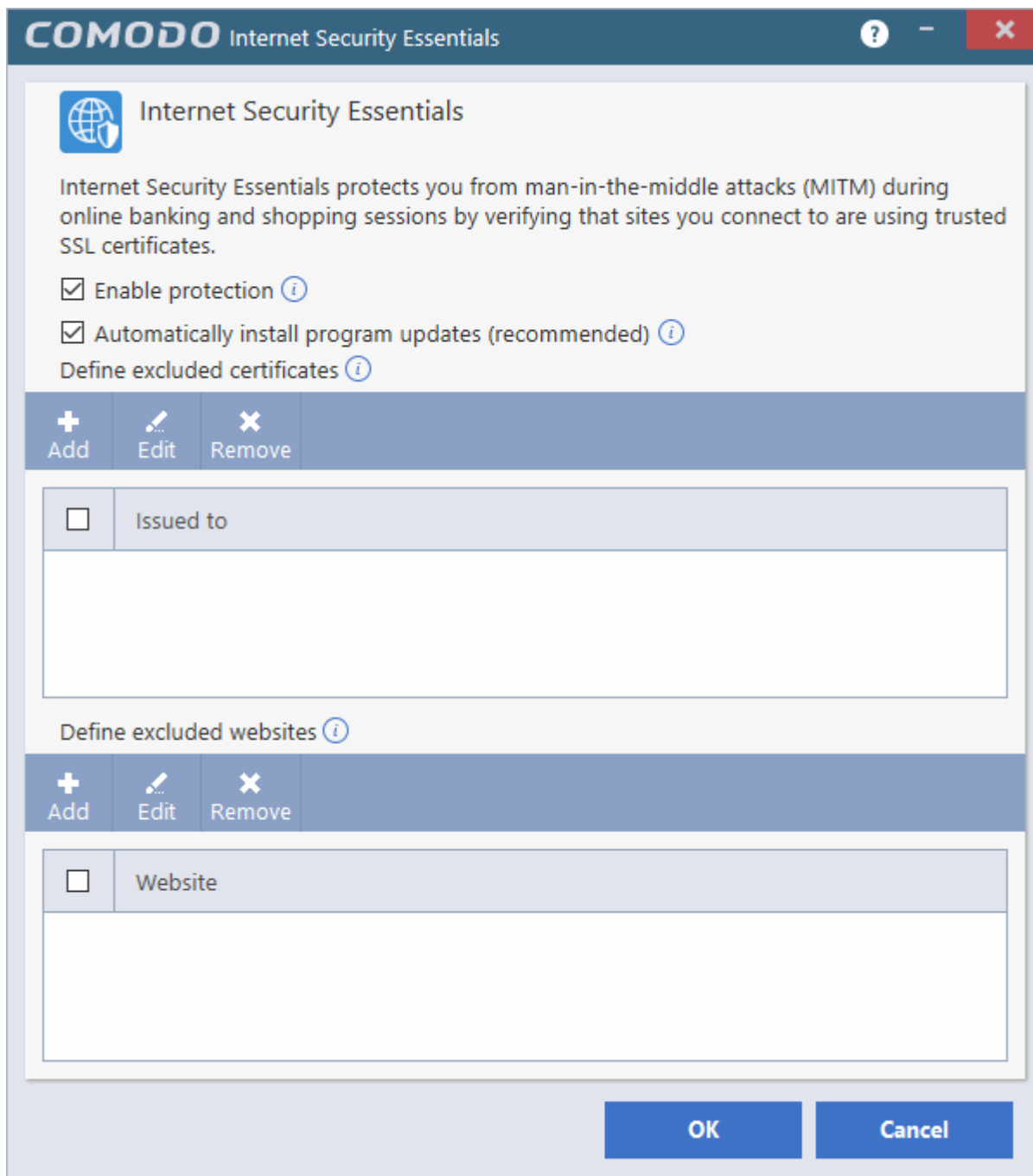
- Enable protection - CISE will monitor the SSL certificates used on the sites you visit and will warn you if a potentially fraudulent certificate is used.

- Automatically install program updates (recommended) - CISE will check with Comodo servers every day for any updates.

You can add certificates and/or website(s) to the list of exceptions:

- Certificate exception - Certificates added to this list will not be flagged by CISE in future.

- Website exception - CISE will not flag any certificates on the domains you add here.

Add a certificate to exceptions

- Click 'Add' under 'Define excluded certificates' to open the certificate configuration dialog:
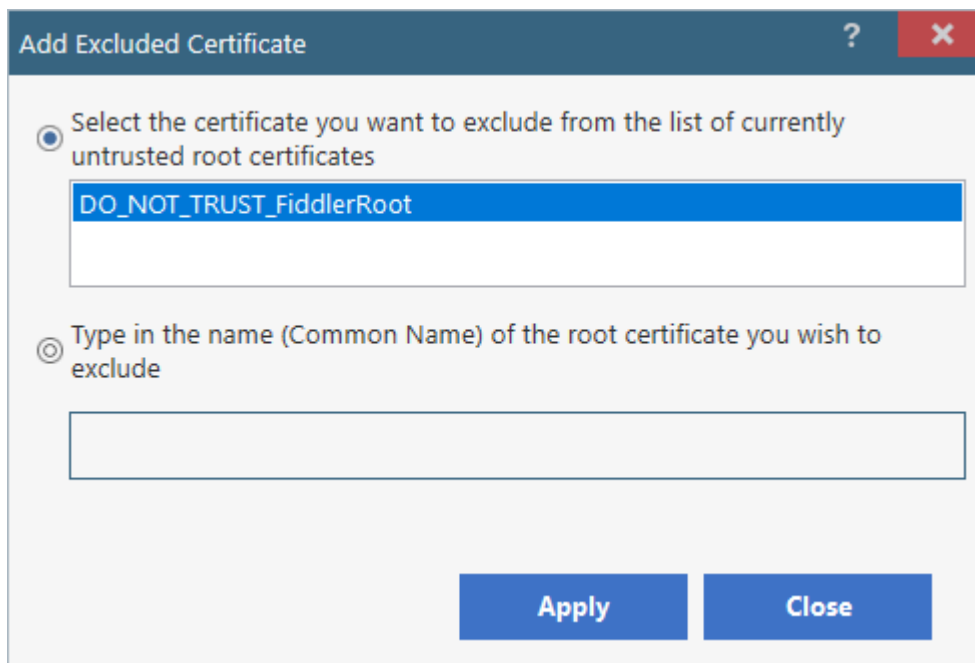
- Select the certificate you wish to whitelist from the list of untrusted certificates that CISE has encountered since installation.

OR

- Manually type the name (Common Name) of the root certificate you wish to exclude.
- Click 'Apply' for your settings to take effect.
- The certificate(s) will be added to the list of exceptions.

- Repeat the process to add more certificates.

Add a website to the exclusion list

- Click 'Add' under 'Define excluded websites' to open the website whitelist configuration dialog:
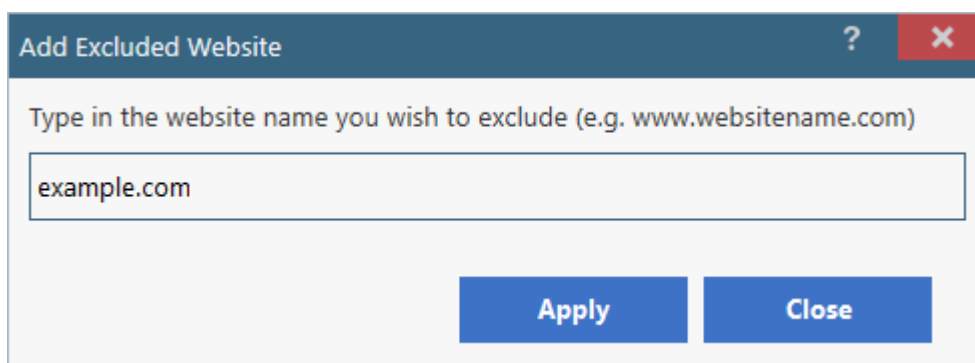
- Enter the URL of the web site you wish to exclude in the field provided then click 'Apply'.
- CISE will no longer flag potentially fraudulent certificates found on whitelisted domains.
- Click 'OK'. Repeat the process to add more websites.

Edit / remove a certificate / website

- To edit a website name or a certificate, select it and click 'Edit'.
- To remove a website or a certificate, select it and click 'Remove'.

Click 'OK' for your settings to take effect

How do I view CISE help?

- Click the help icon at the top right of the application or an alert

- Select 'Online Help' to view the product help guide at **https://help.comodo.com/topic-435-1-841-10768-Introduction-to-Comodo-Internet-Security-Essentials.html**
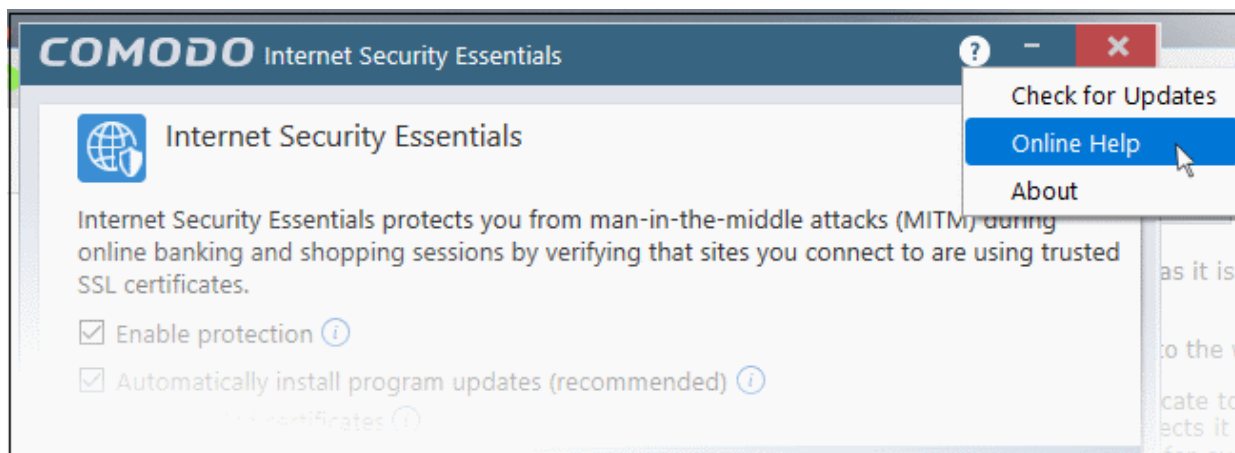
How do I view the version number and release notes?

- Click the help icon at the top right of the application or an alert

- Select 'About':
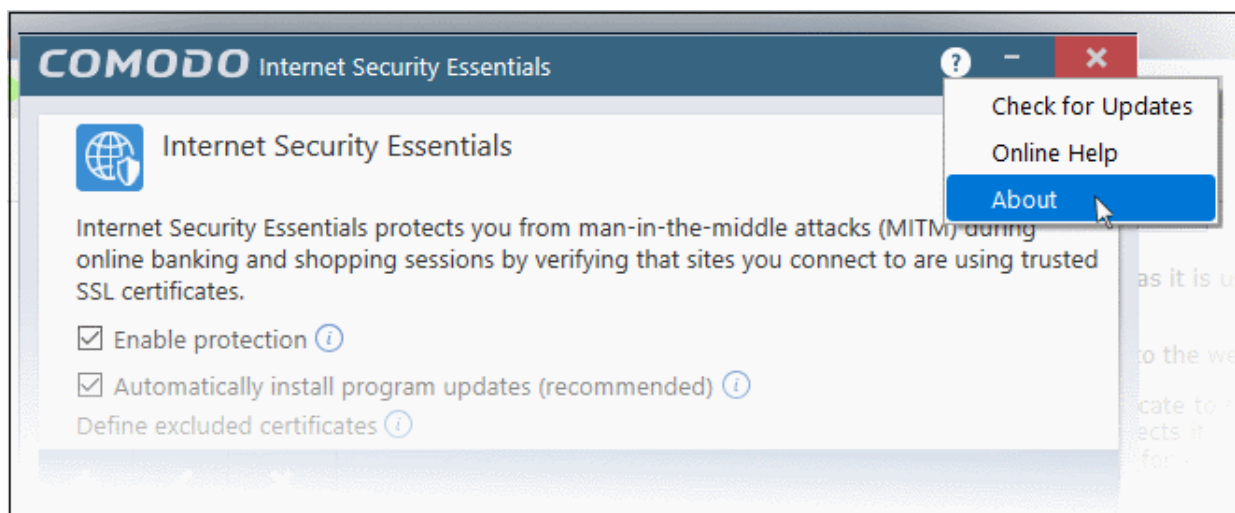
The 'About' screen contains:

- Version details including copyright information.

- A link to the latest release notes where you can find out about new features and bug fixes.

How do I remove Comodo Internet Security Essentials?

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

To remove Comodo Internet Security Essentials:

- Open the Windows control panel then open 'Programs and Features' (or 'Add/Remove Programs' on older versions of Windows)
- Select 'Internet Security Essentials' in the list of programs
- Click 'Uninstall'
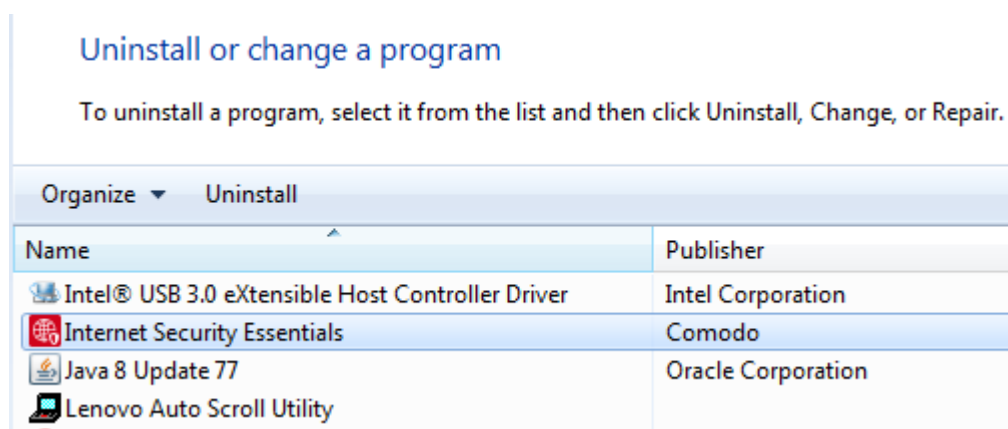
- The uninstallation wizard will start. Click 'Uninstall' to remove the program:
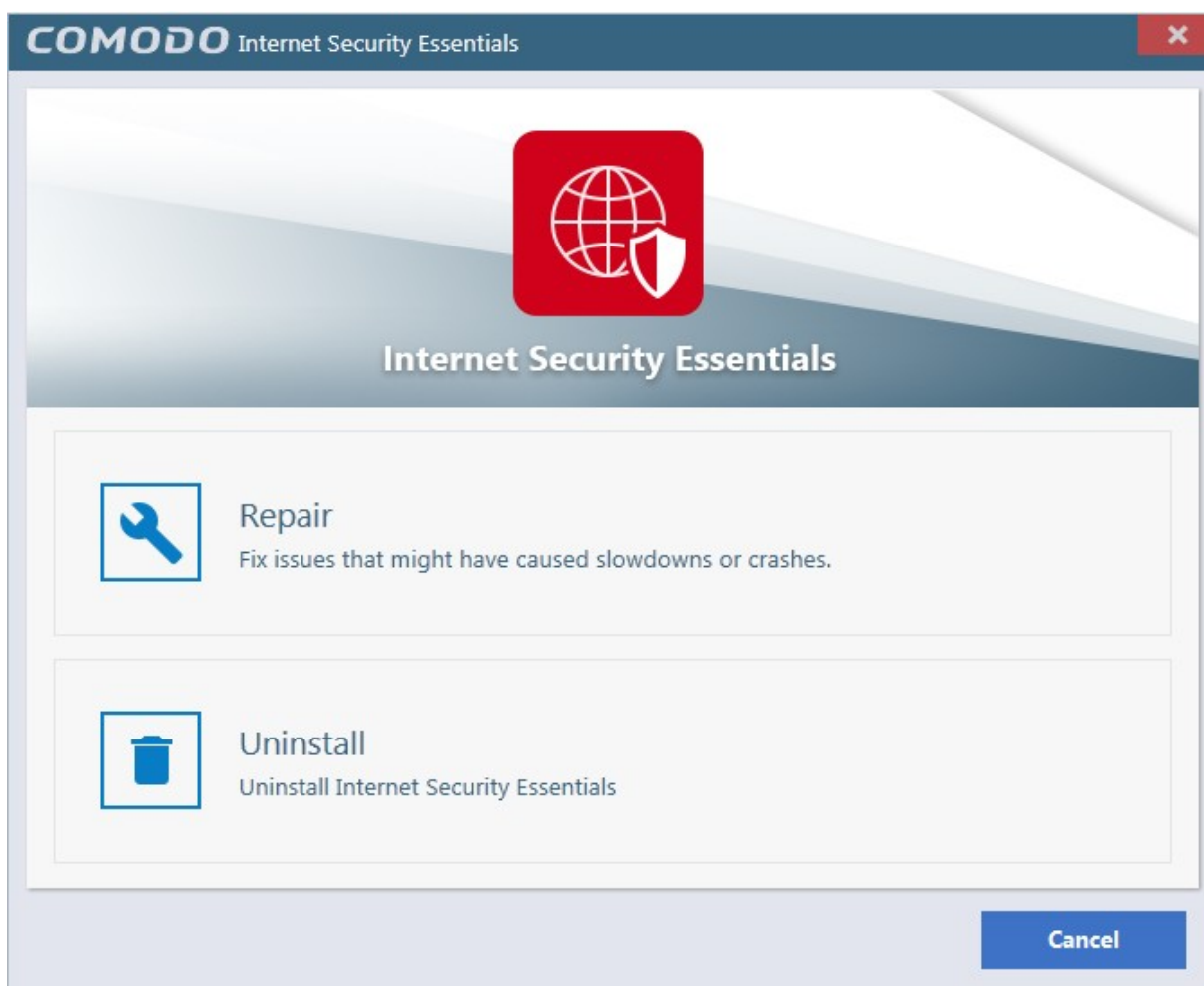
- Please provide us with valuable feedback by specifying the reason that you are uninstalling Comodo Internet Security Essentials:
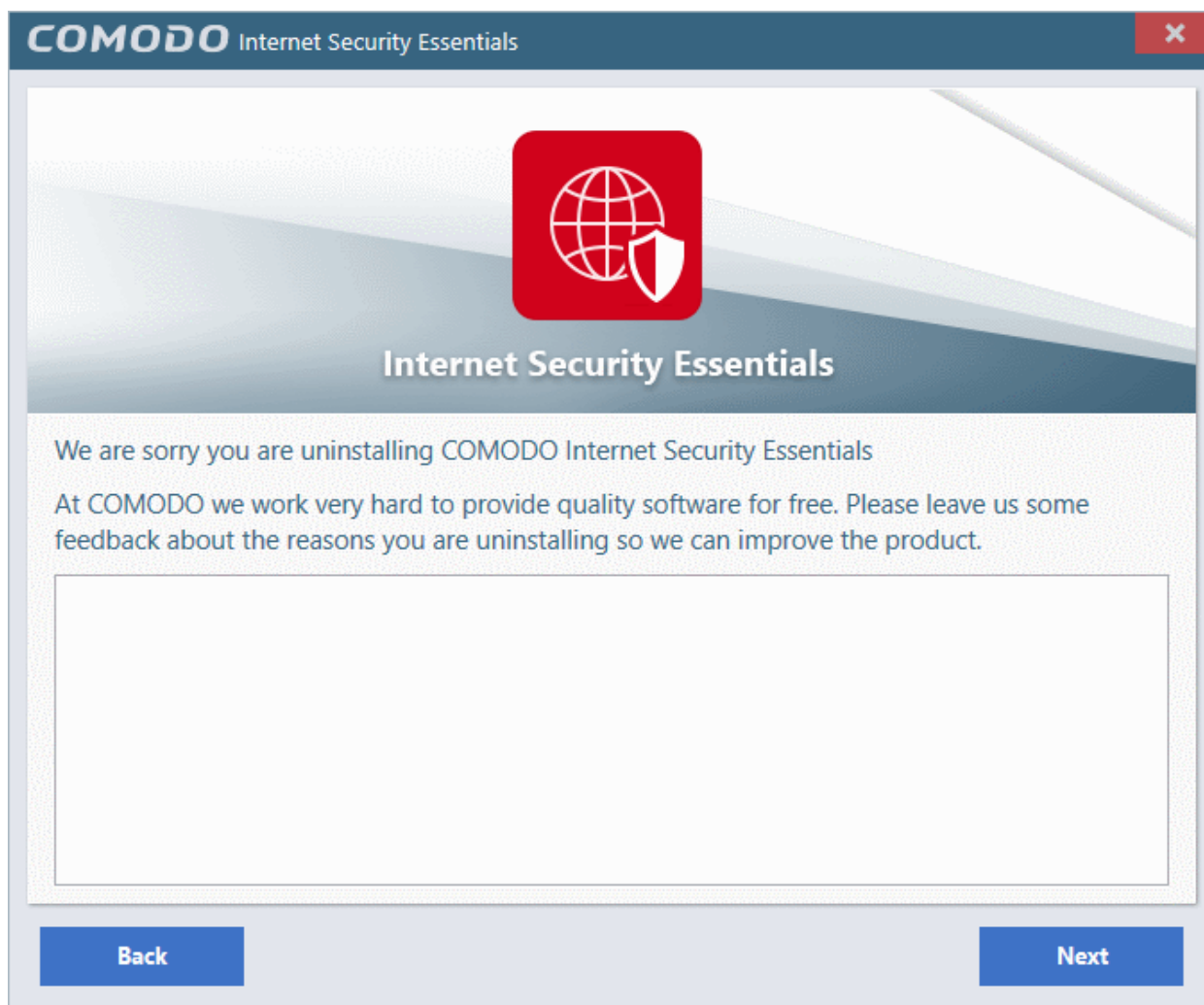
- Click 'Next' to complete the uninstall:
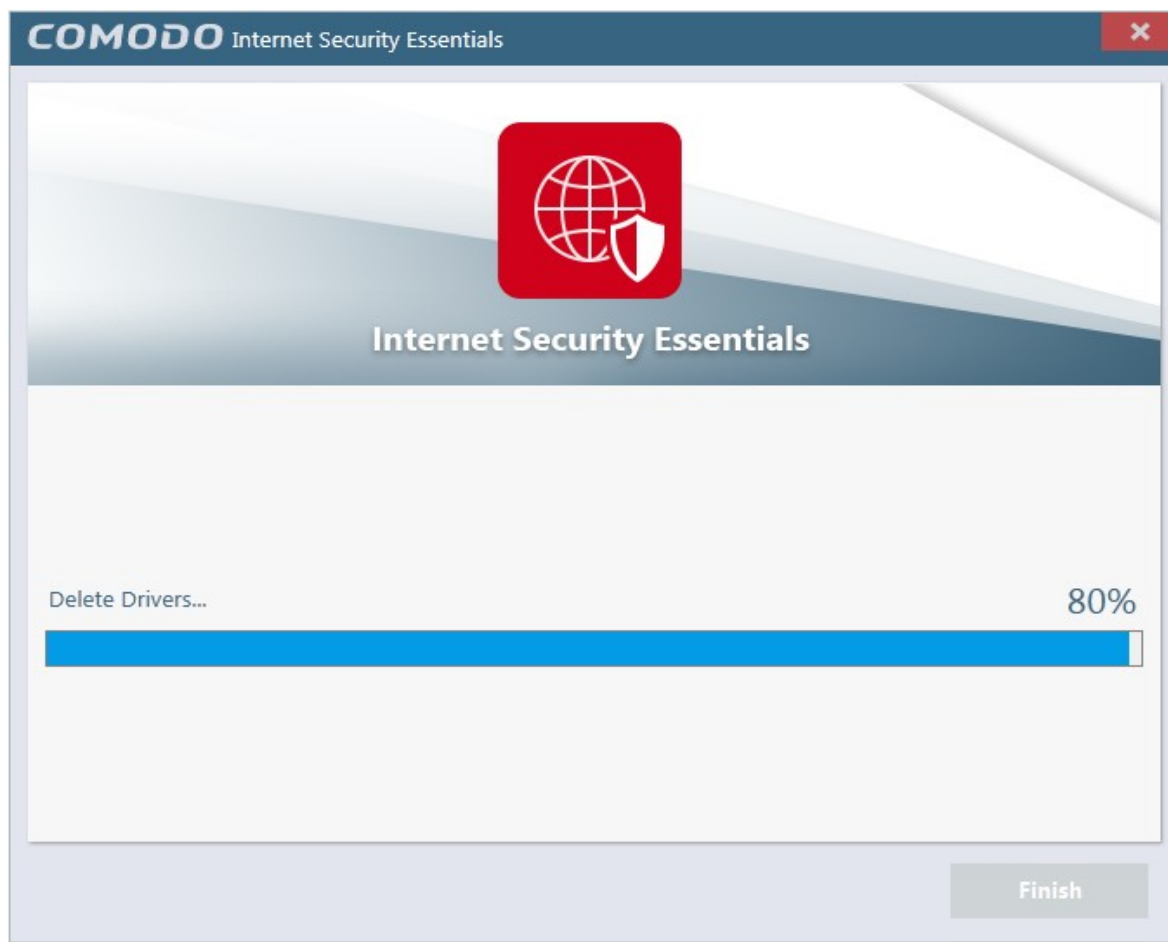
That's it! Click 'Finish' to close the program.

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

- • **Give contained applications write access to folders and files** - How to exclude the files and folders that are contained

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:
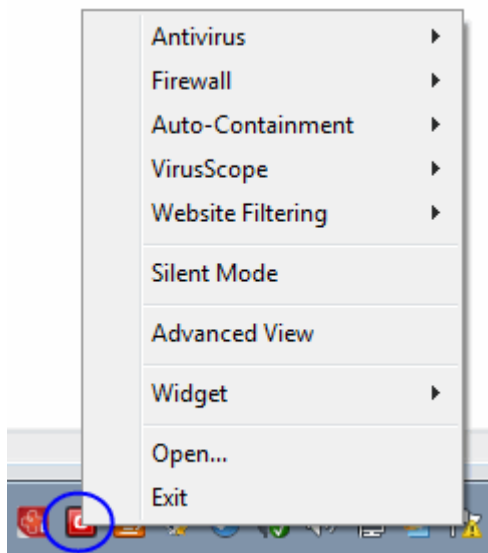
Antivirus

To enable/disable the Antivirus

1. Right-click on the system tray icon with CIS in Basic View.

2. Move your mouse over 'Antivirus'
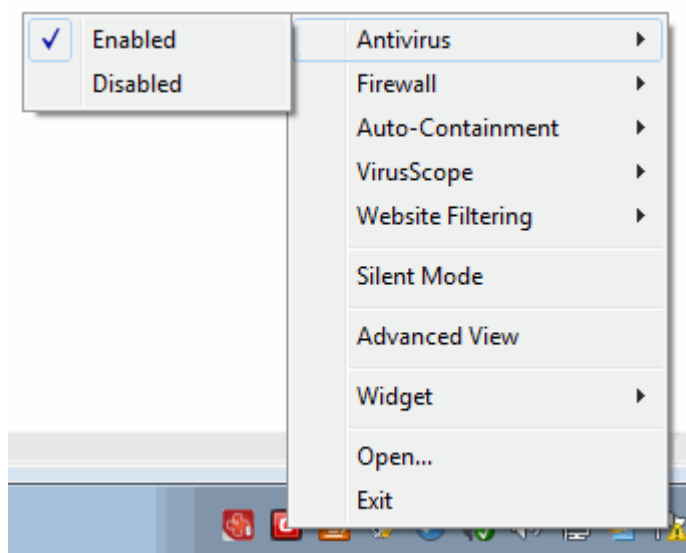
3. Choose 'Enabled' or 'Disabled' as required

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'
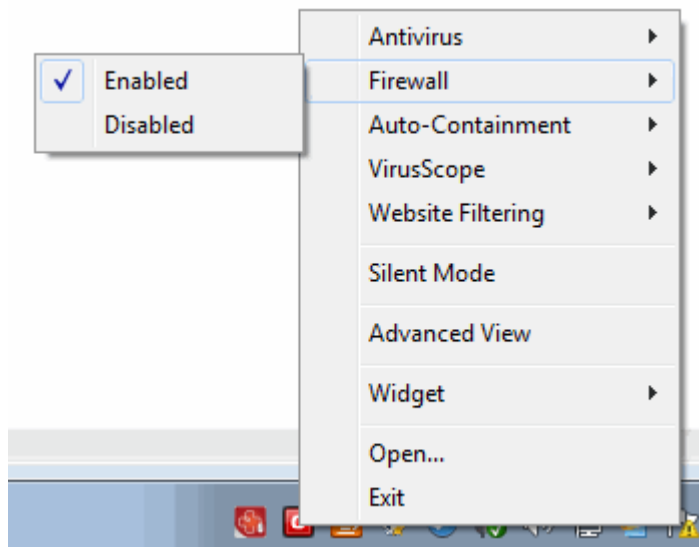
3. Choose 'Enabled' or 'Disabled' as required

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'
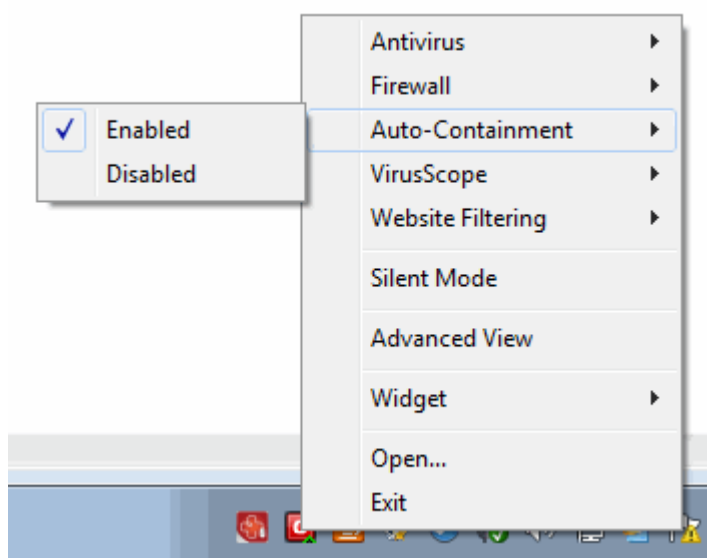
3. Choose 'Enabled' or 'Disabled' as required

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'
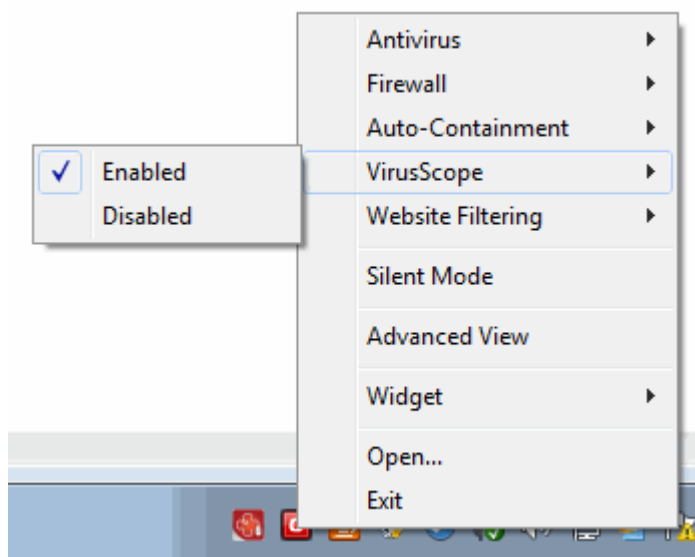
3. Choose 'Enabled' or 'Disabled' as required

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'
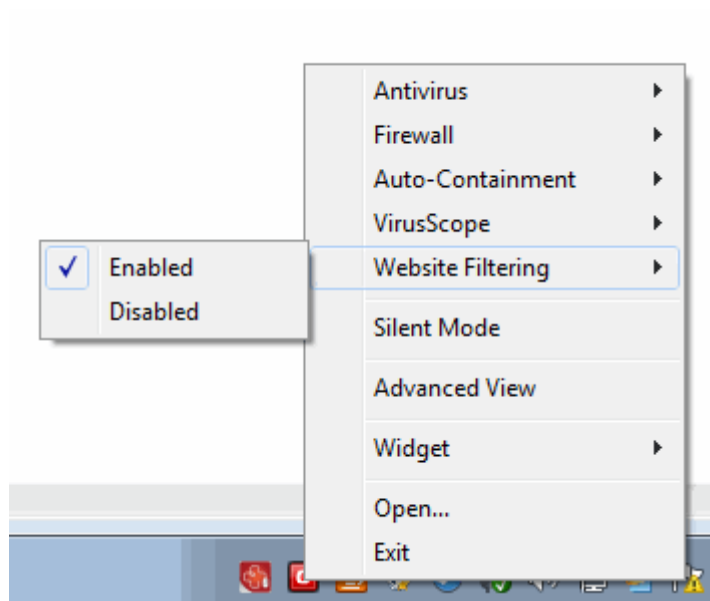
3. Choose 'Enabled' or 'Disabled' as required

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' > 'Firewall Tasks'
2. Click 'Stealth Ports'
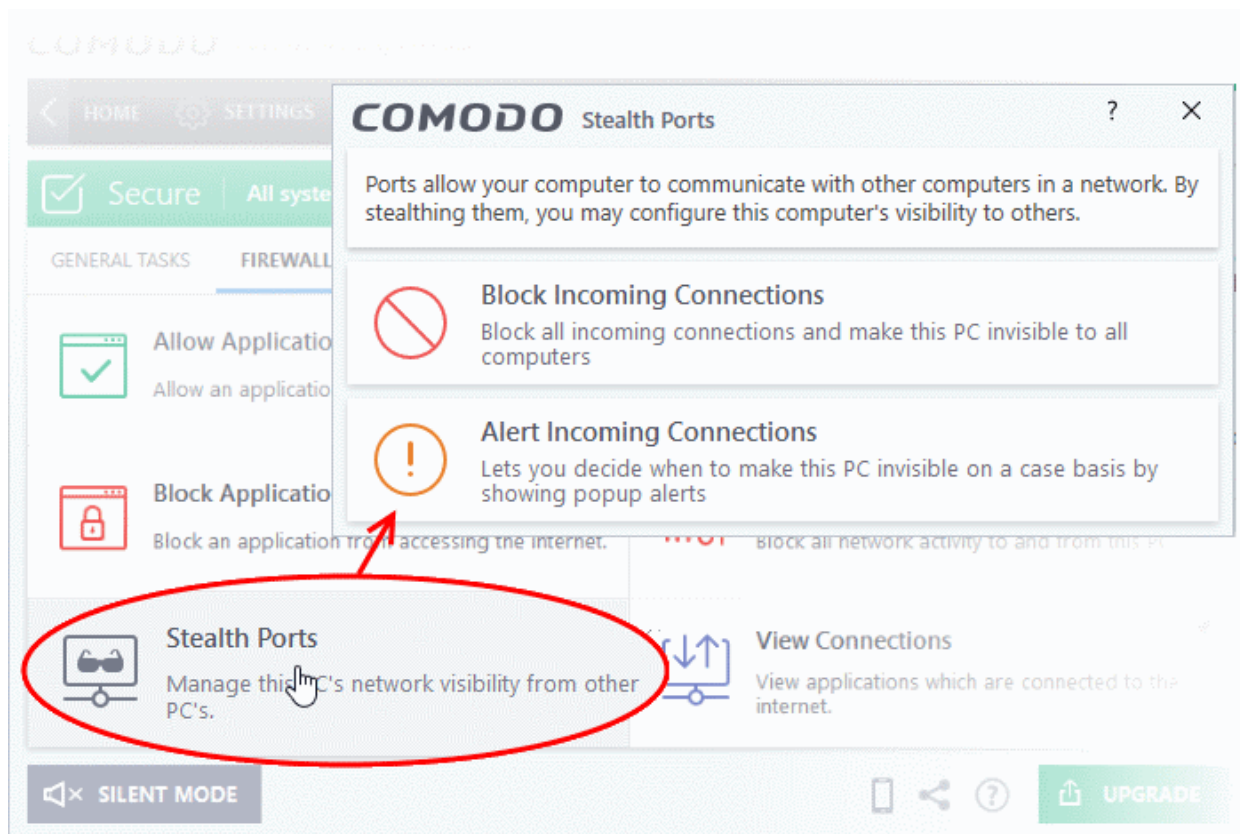
4. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

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).

View the configurations

1. Click 'Settings' on the CIS home screen

2. Click 'Firewall' > 'Network Zones'

3. Click the 'Network Zones' tab
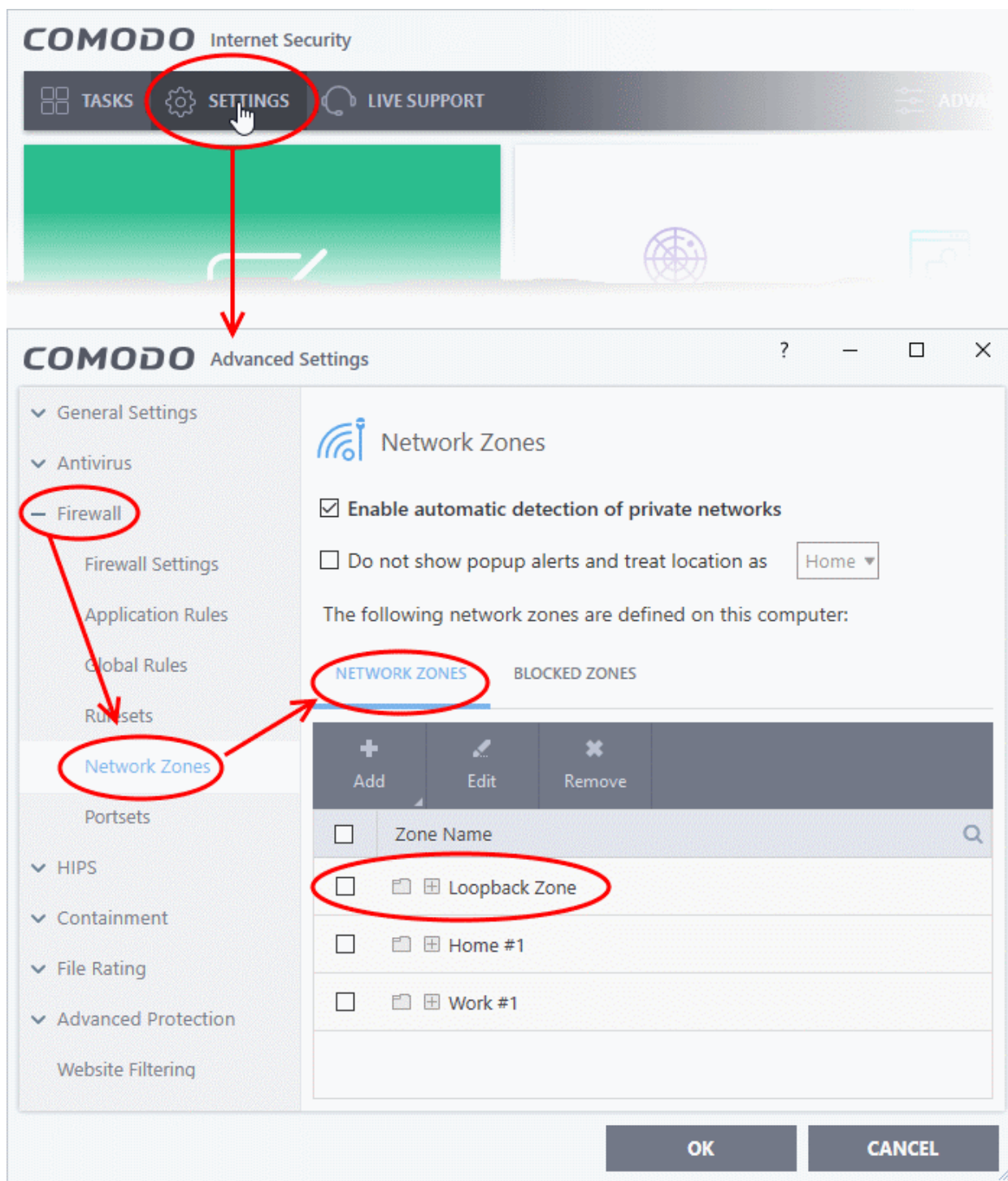
4. Inspect the 'Loopback zone' and 'Local Area Network #1' (exact name may vary) by clicking the '+' button beside the zone name.

    •   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 Zone settings

Firewall Settings

The firewall settings option lets you configure the protection level for your internet connection, and the frequency of alerts generated.

1. Click 'Settings' at the top of the CIS home screen
2. Click 'Firewall' > 'Firewall Settings'
3. Select 'Enable Firewall' and choose 'Safe Mode' from the drop-down
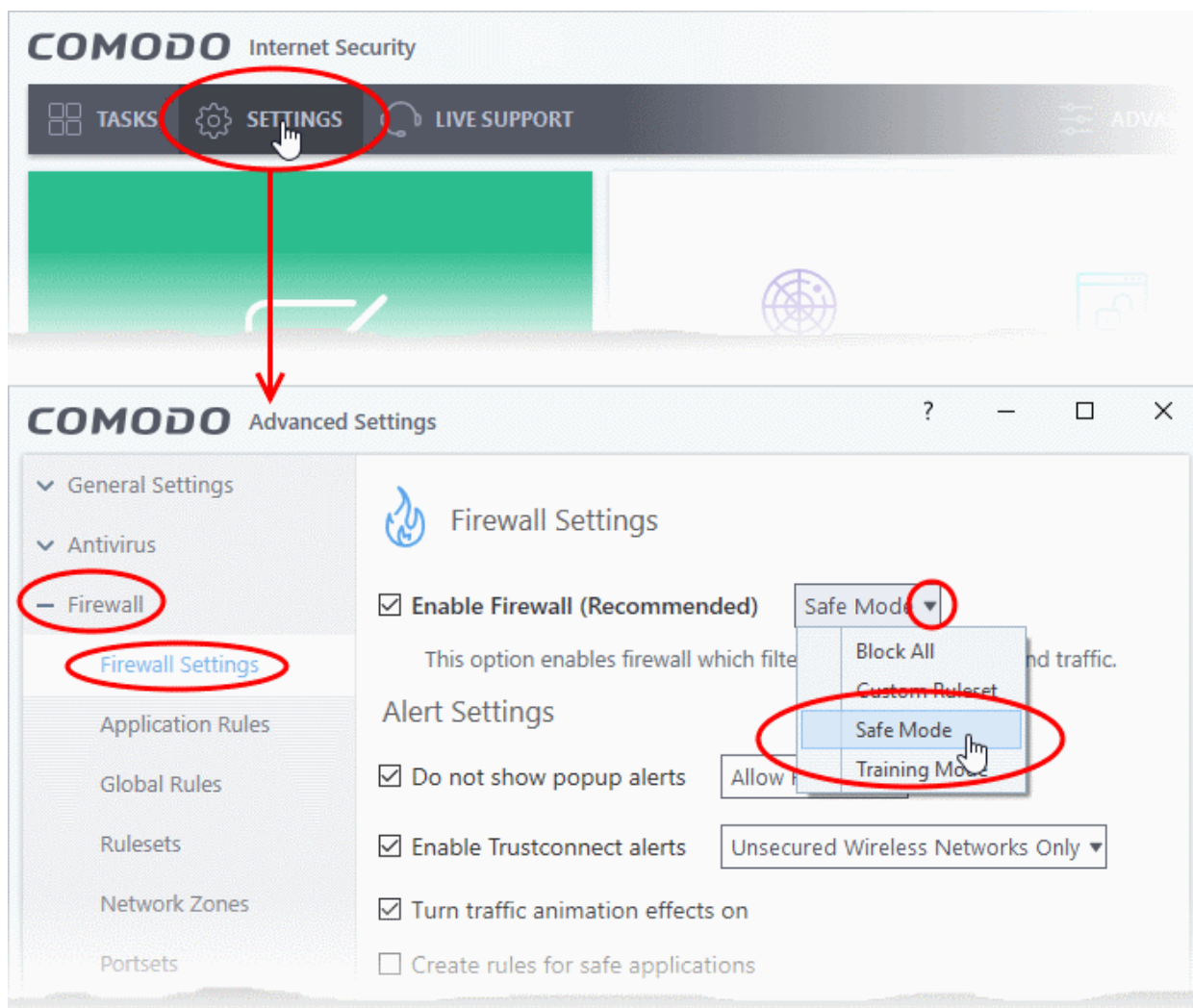
Safe Mode: While filtering network traffic, the firewall will automatically create rules which allow traffic for application components certified as 'Safe' by Comodo. For non-certified, new, applications, you will receive an alert whenever that application attempts to access the network. Should you choose, 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.
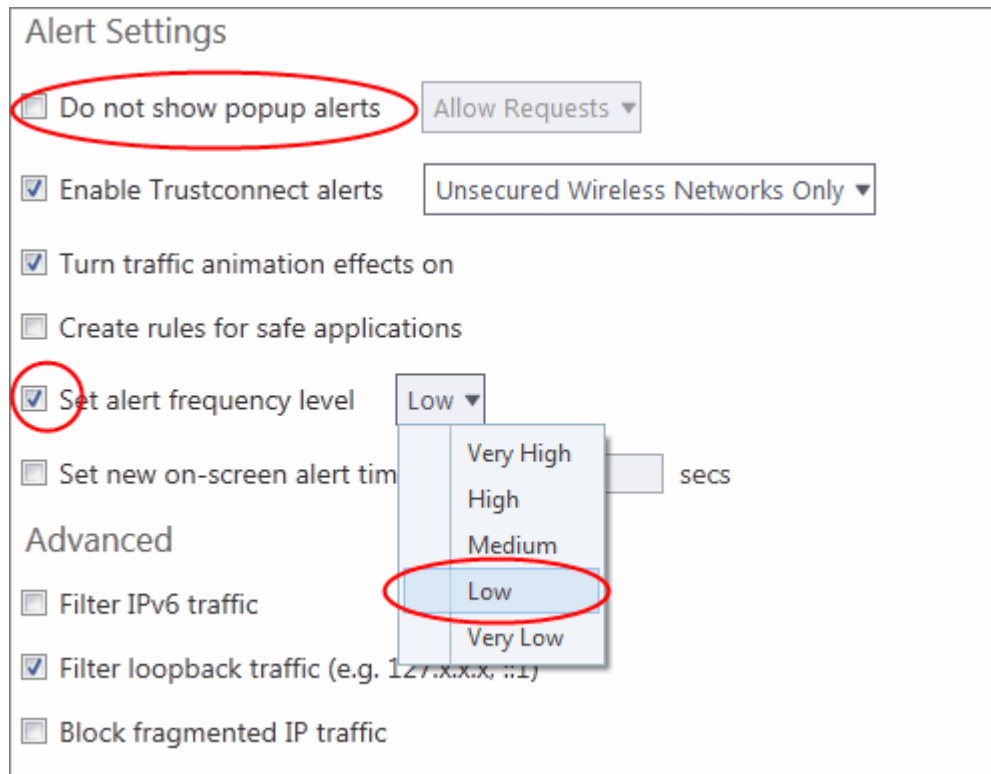
Advanced Settings

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'
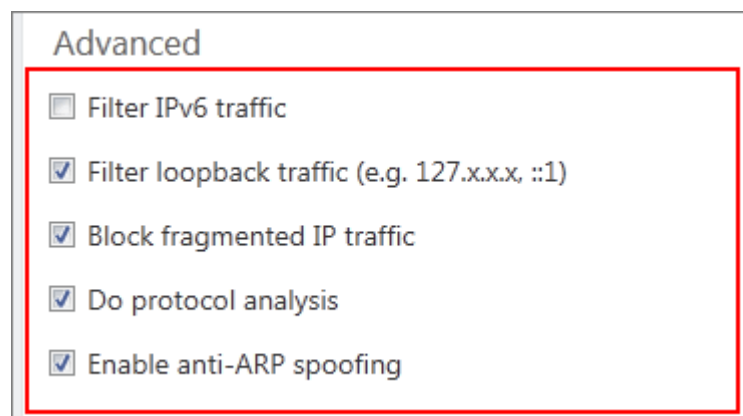
4. Click 'OK' for your settings to take effect.

Click here for more details on Firewall Settings

Set-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.

View the Application Rules

1. Click 'Settings' on the CIS home screen
2. Click 'Firewall' > 'Application Rules'
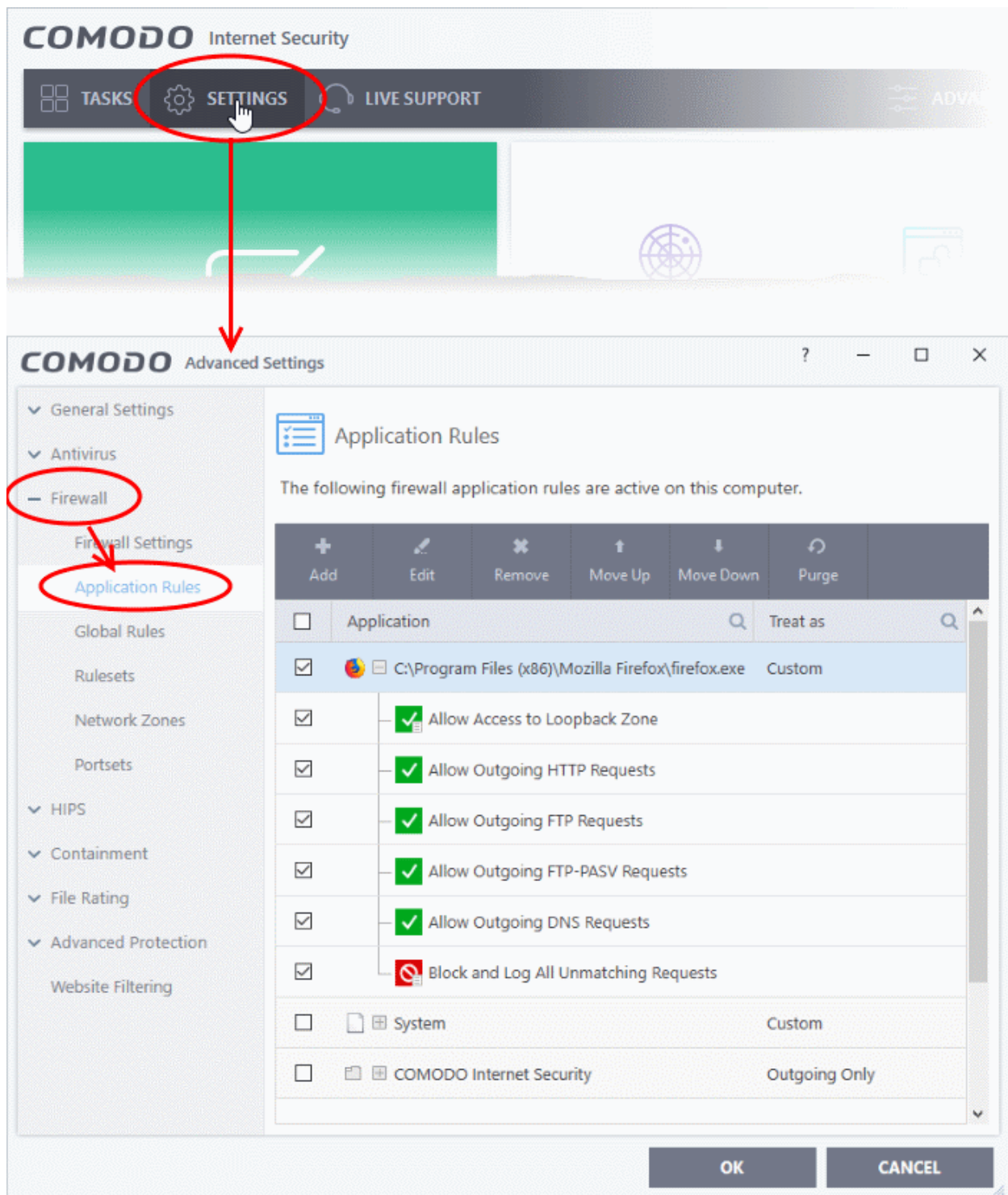
3. Click 'Add' to create a new application rule

---

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

View the Global Rules

1. Click 'Settings' on the CIS home screen

2. Click 'Firewall' > 'Global Rules'.
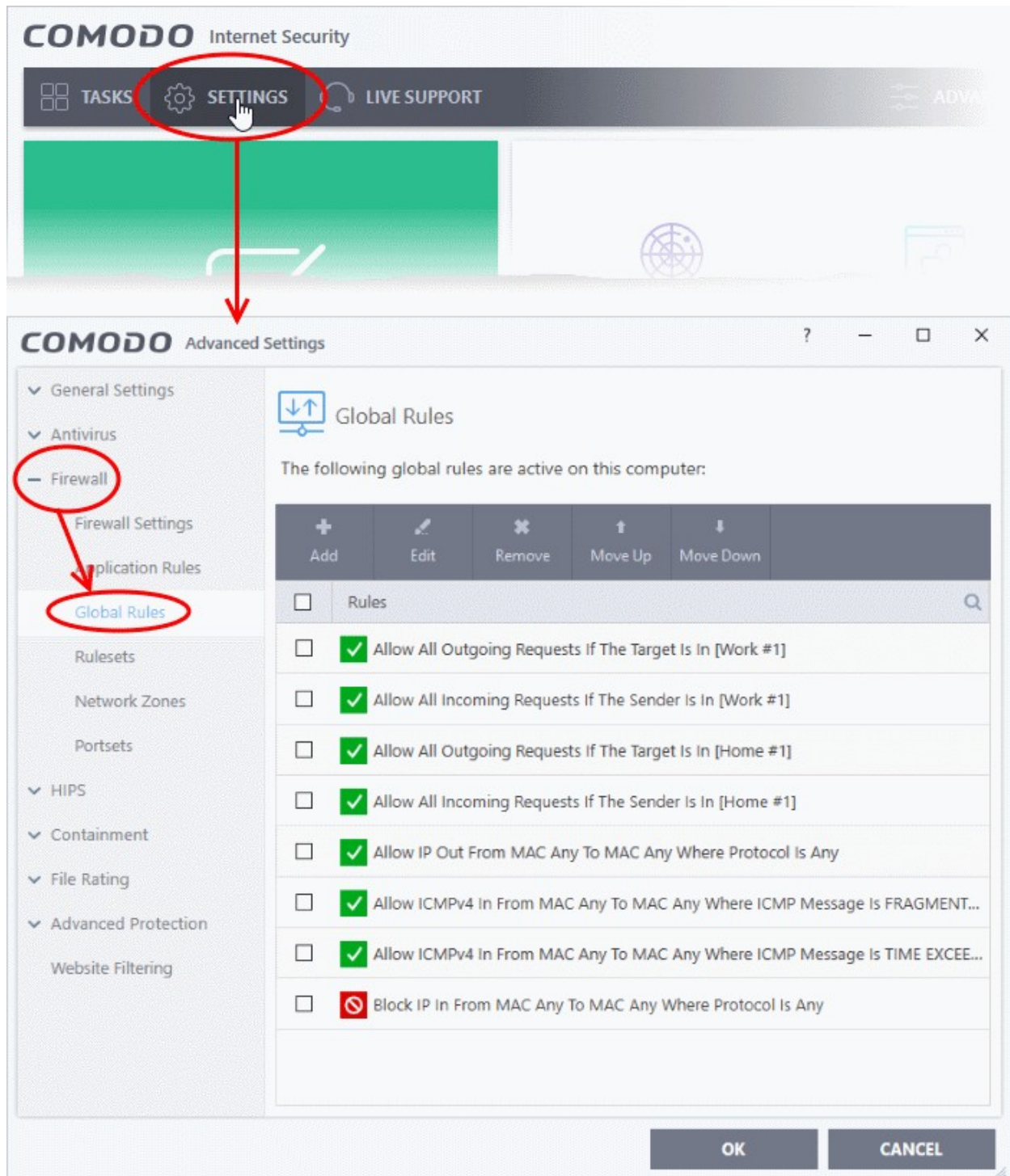
3. Click 'Add' to create a new global rule

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

View Predefined Firewall rulesets

1.   Click 'Settings' on the CIS home screen

2.   Click 'Firewall' > 'Rulesets'
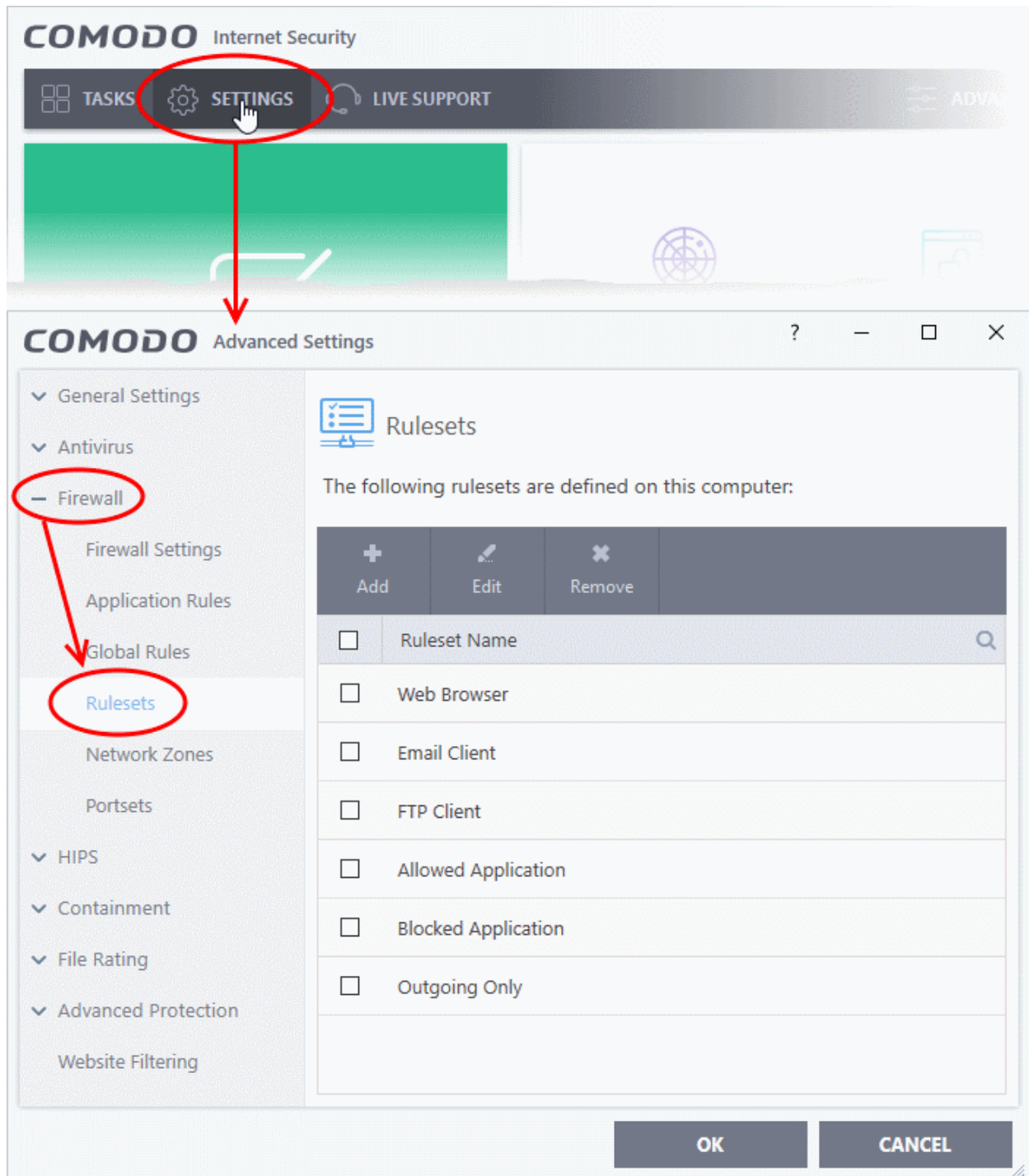
3.   Click 'Add' to create a new ruleset

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 the 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 a company network, you want employee computers to connect to your network 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.*

You need to create a global firewall rule to block internet access while allowing internal connections. You should also password protect your configuration to prevent others from altering it.

Create the Global Rule

1. Click 'Settings' on the CIS home screen
2. Click 'Firewall' > 'Global Rules'

---
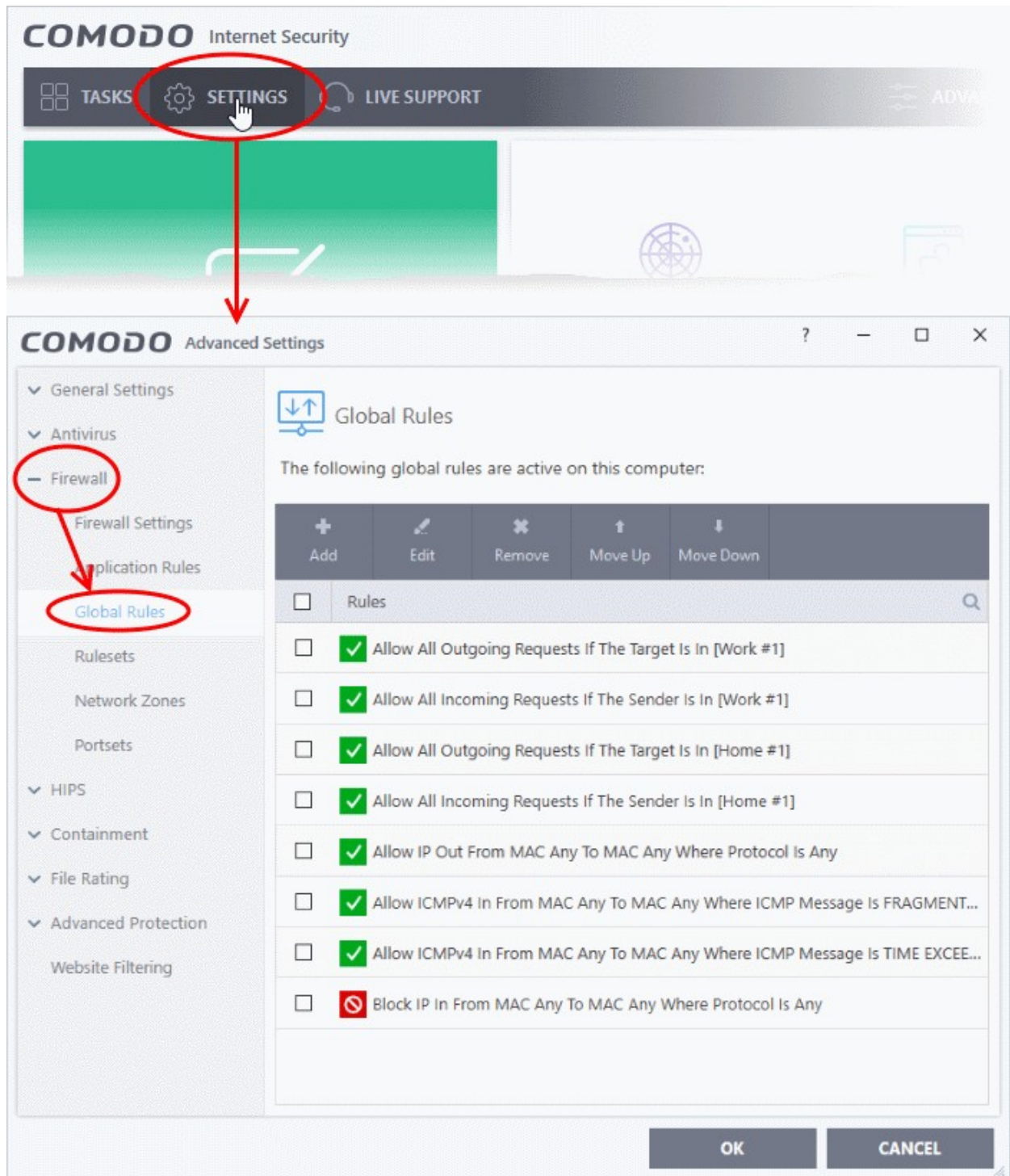
3.   Choose 'Add' from the options at the top. The 'Firewall Rule' interface will open.
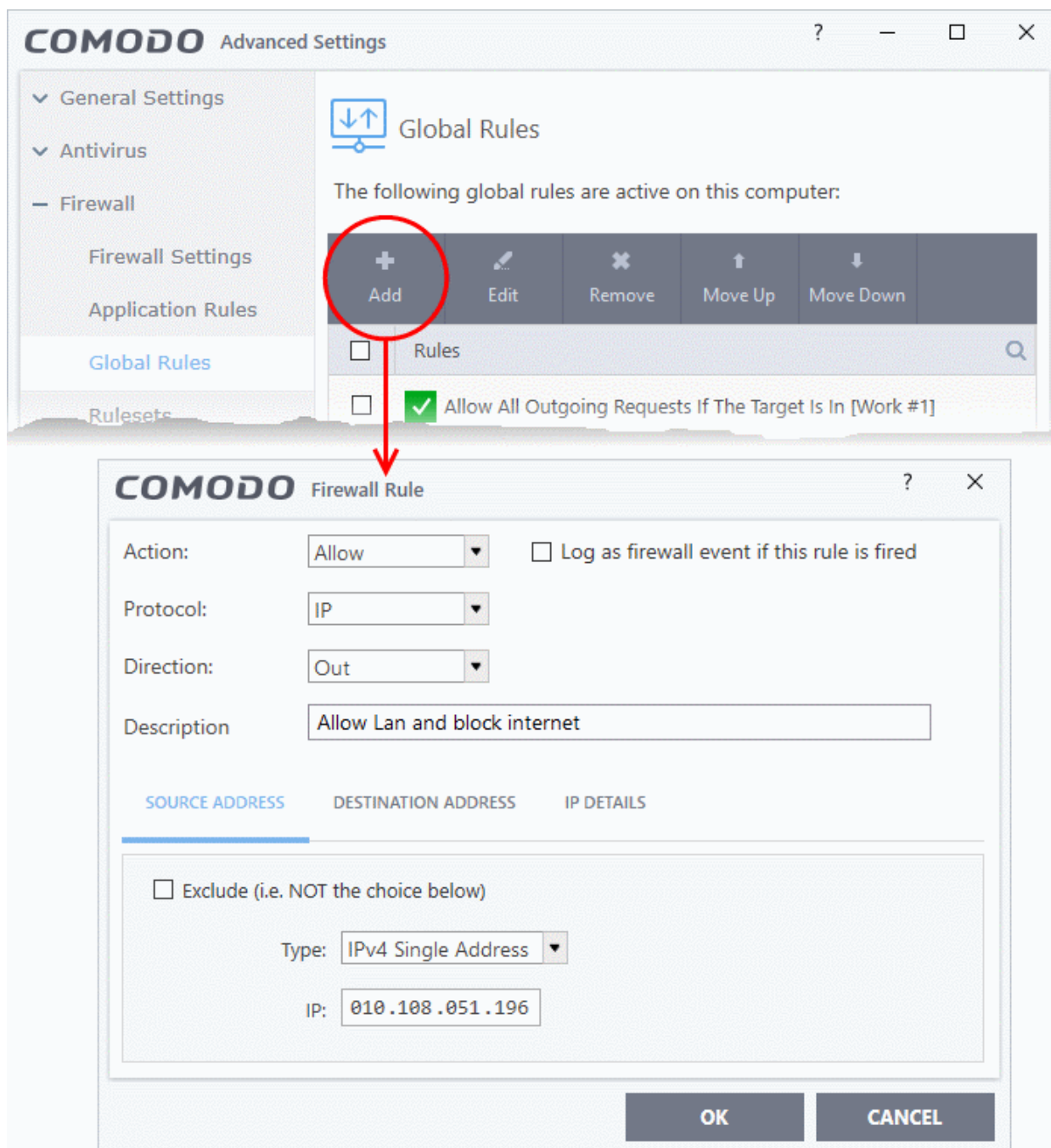
4. Choose the following options from the respective drop-downs:

- 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
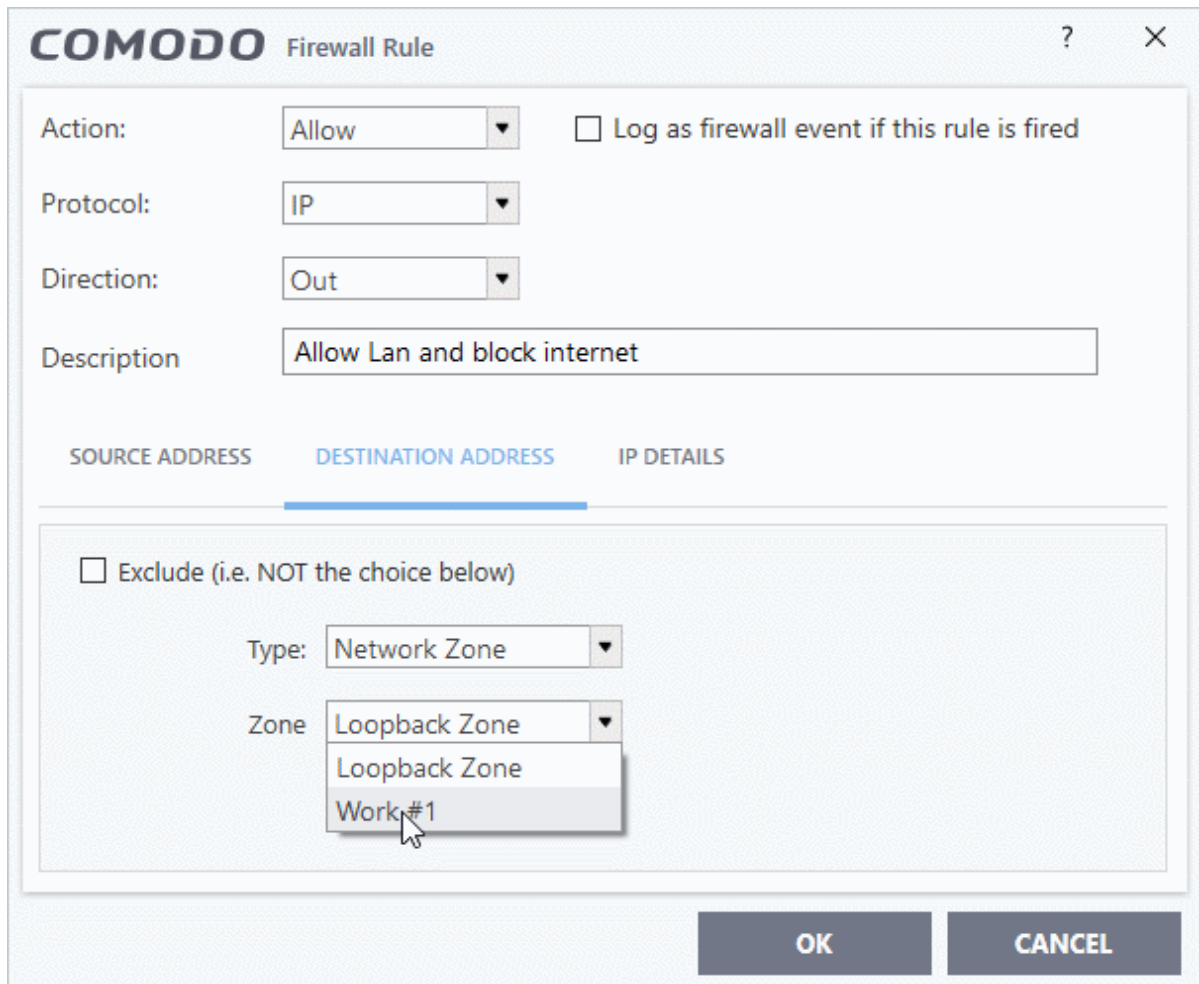
8.   Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.
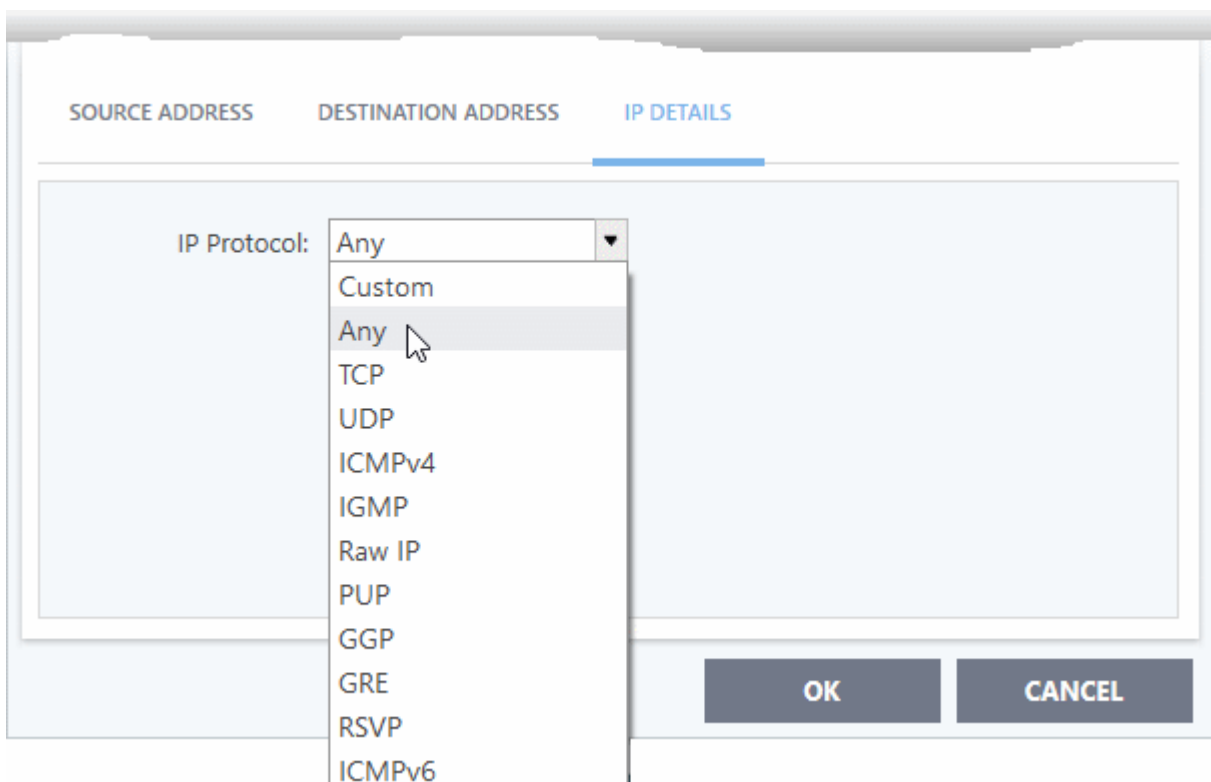
9.   Click 'OK'. The created policy will be added to the list of 'Global Rules'.

10. Select the rule and click the 'Move Up' button until the rule is in first position:
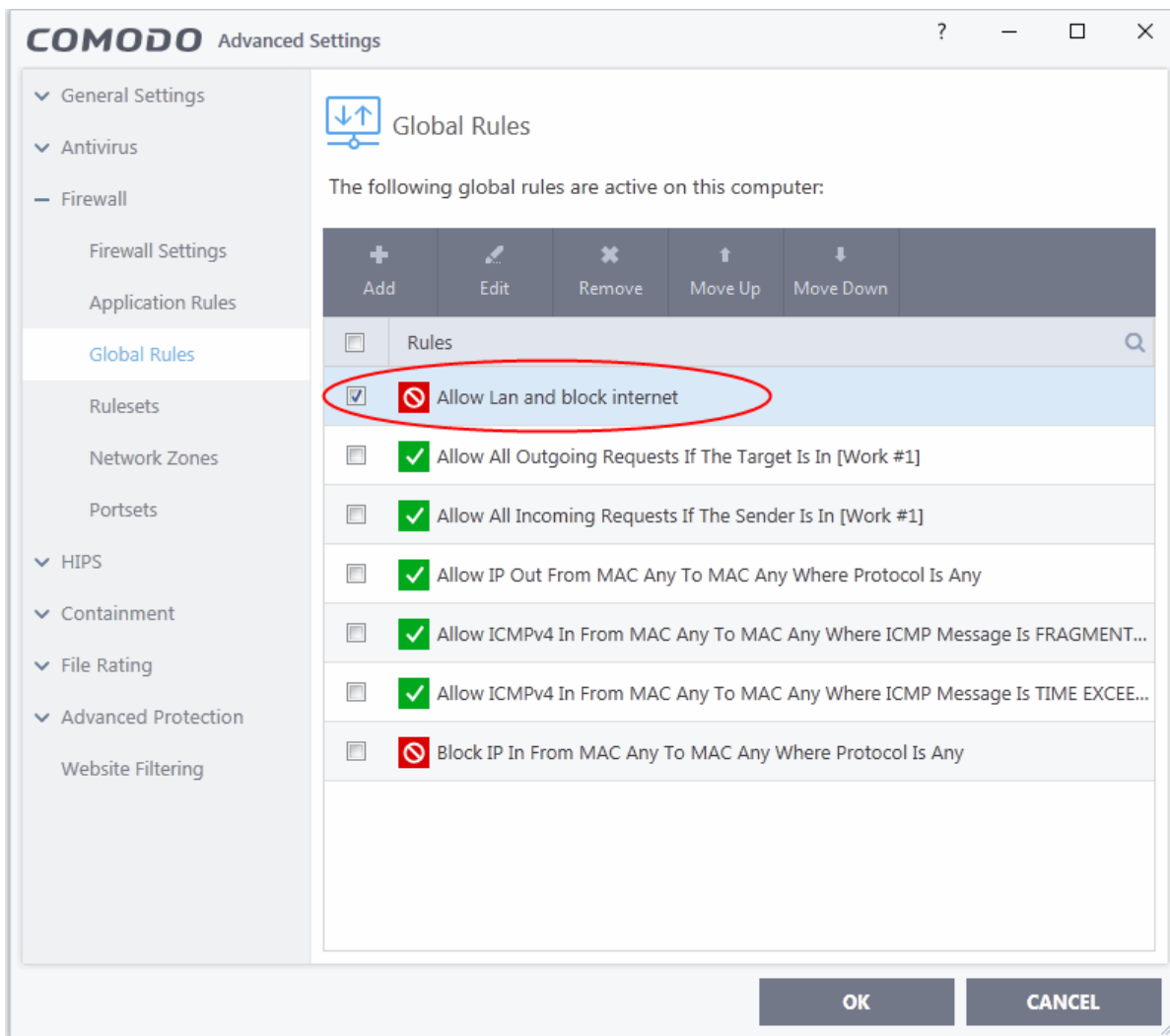
11. Click 'OK' for your configuration to take effect.

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.
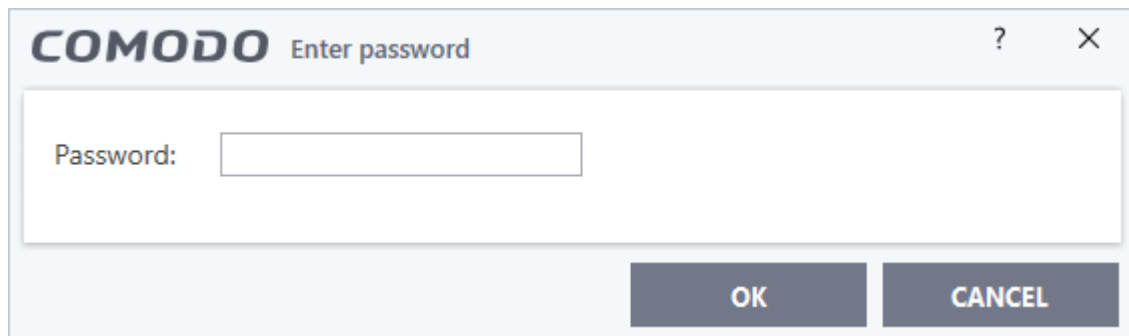
Password protect your configuration

1.   Click 'Settings' on the CIS home screen

2.   Click 'General Settings' > 'User Interface'

3.   Select 'Enable Password Protection' under 'Password Protection' and click the 'Set Password' link. The Create/change password' dialog will appear:
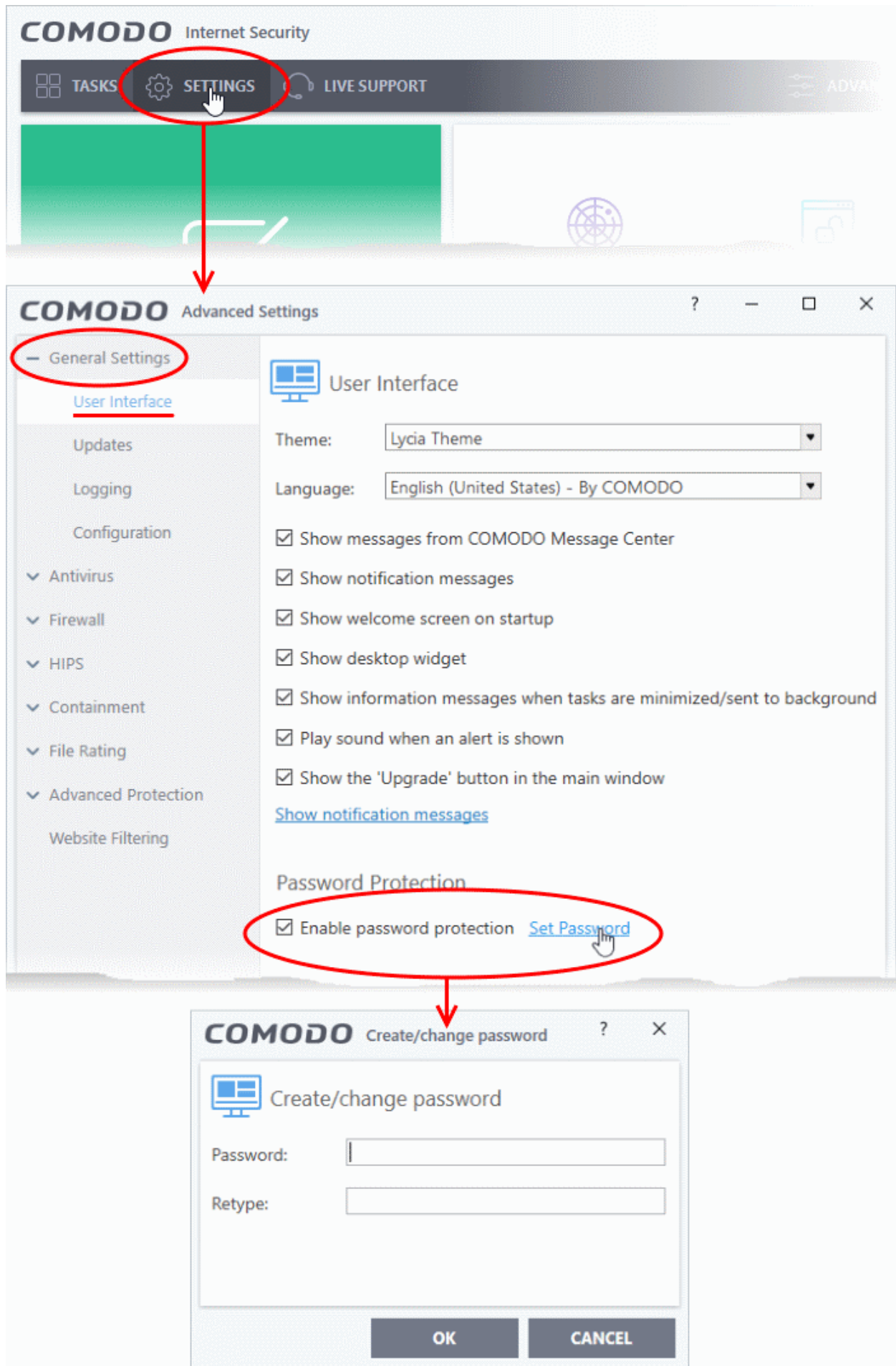
4. Enter and confirm your password then click 'OK'. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

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

Define website categories

1. Click 'Settings' on the CIS home screen

2. Click 'Website Filtering' > 'Categories'

3. Click 'Add' > 'Add Category':
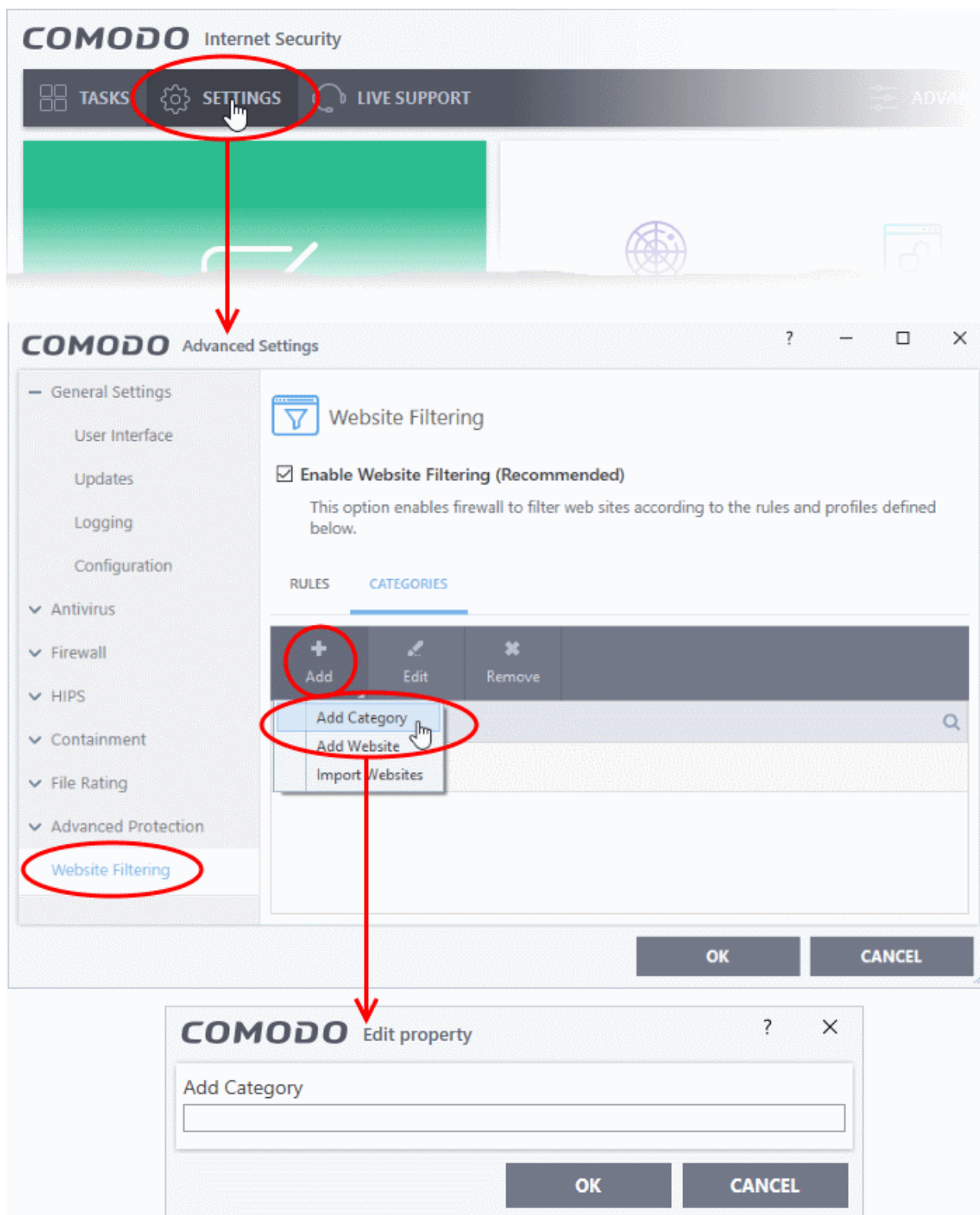
4. Enter a name for the category and click 'OK'. The new category will be listed in the categories tab.

5. 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:

---
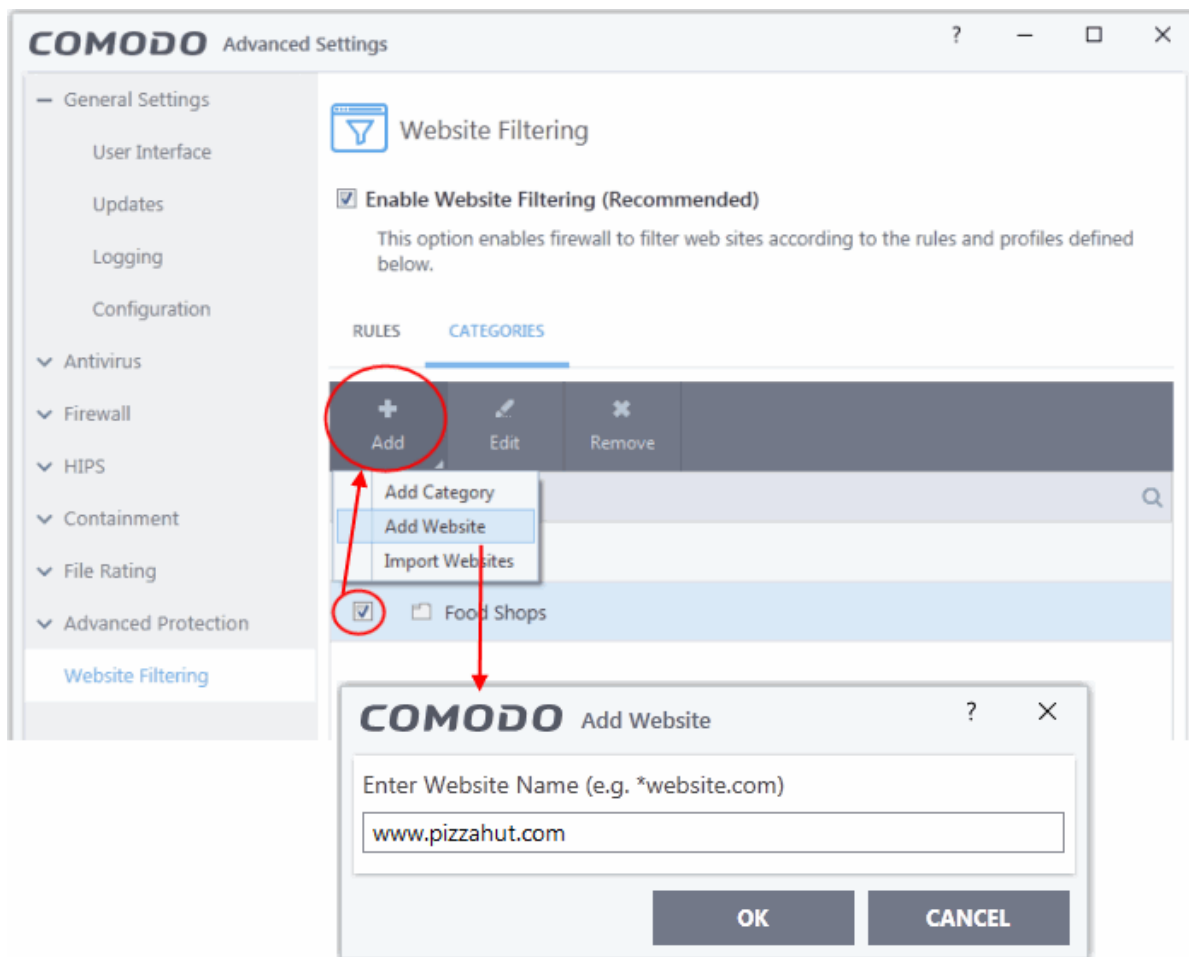
6. Type the website or text string you wish to add to the category. See the following notes for advice on this:

    •   Enter a FQDN to filter a specific domain. For example, **www.example.com**

    •   Place an asterisk in front of the URL to include all sub-domains of the website. For example, *.friskywenches.com will cover friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on. The asterisk is also known as a wildcard character.

    •   Place an asterisk before a keyword to cover all URLs that start with a specific string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.

    •   Place asterisks before and after the keyword to cover all sites that contain the string. For example, "*pizza*" will cover hotpizzanow.com, spicypizzadishes.net and so on.

7. Repeat the process to add more websites to the category.

8. Repeat the process to add more website categories

9. Click 'OK' in the 'Advanced Settings' interface to save your settings

Create rules to block or allow websites to specific users

1. Click 'Settings' on the CIS home screen

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.
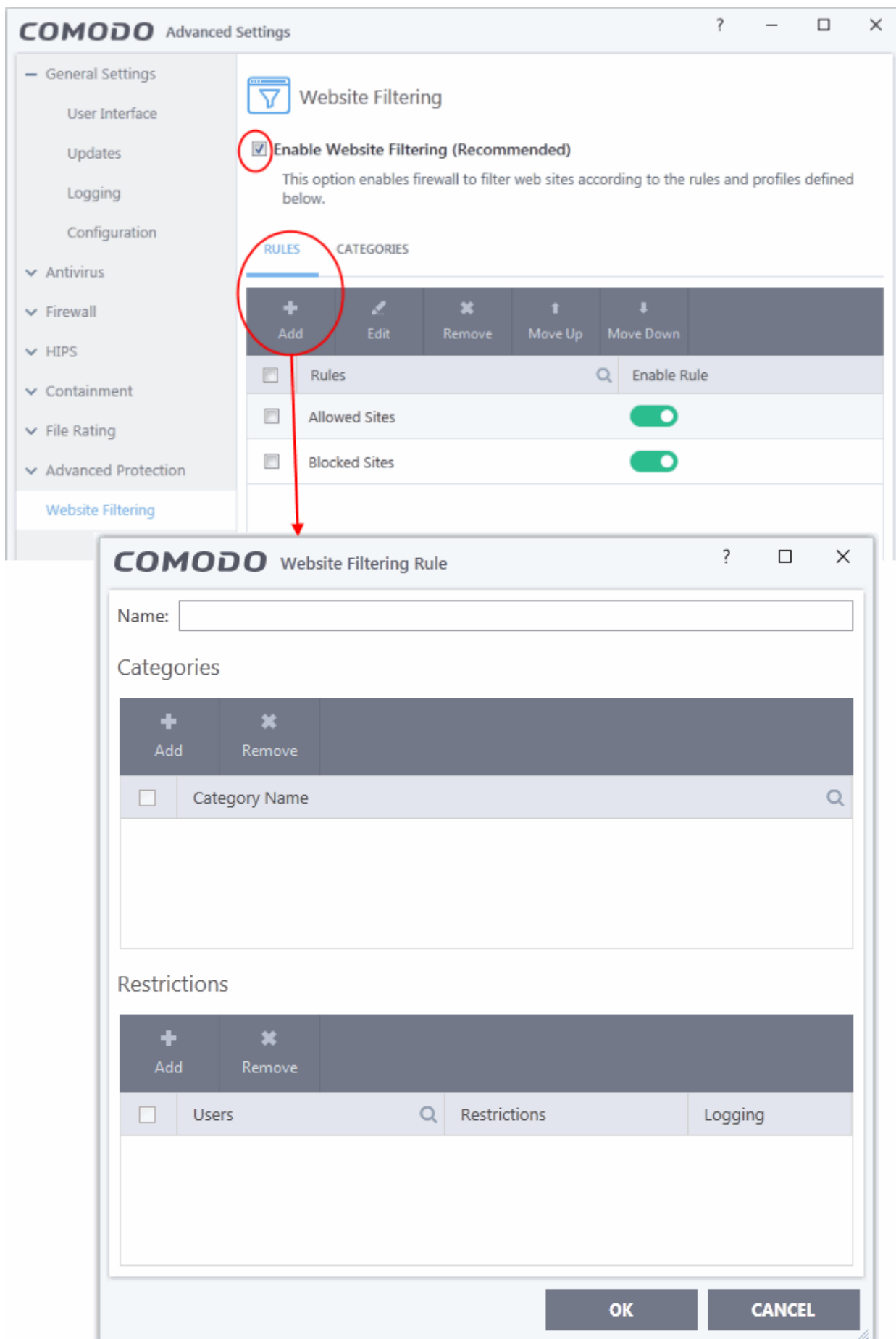
5. Enter a name for your new filter in the 'Website Filtering Rule' dialog.

6. Select the categories that should be added to the filter:

- Click 'Add' under the Categories'.
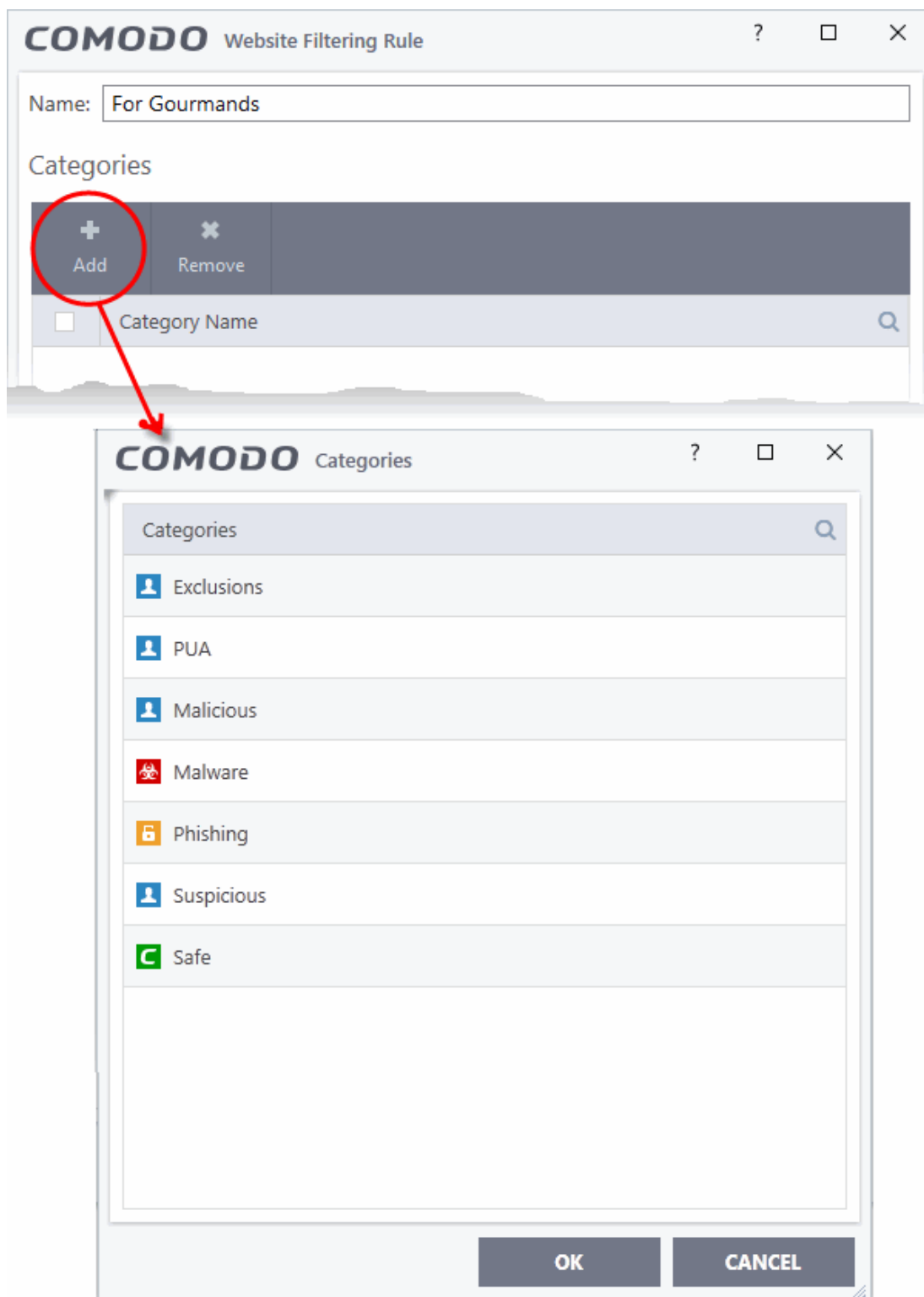
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **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:
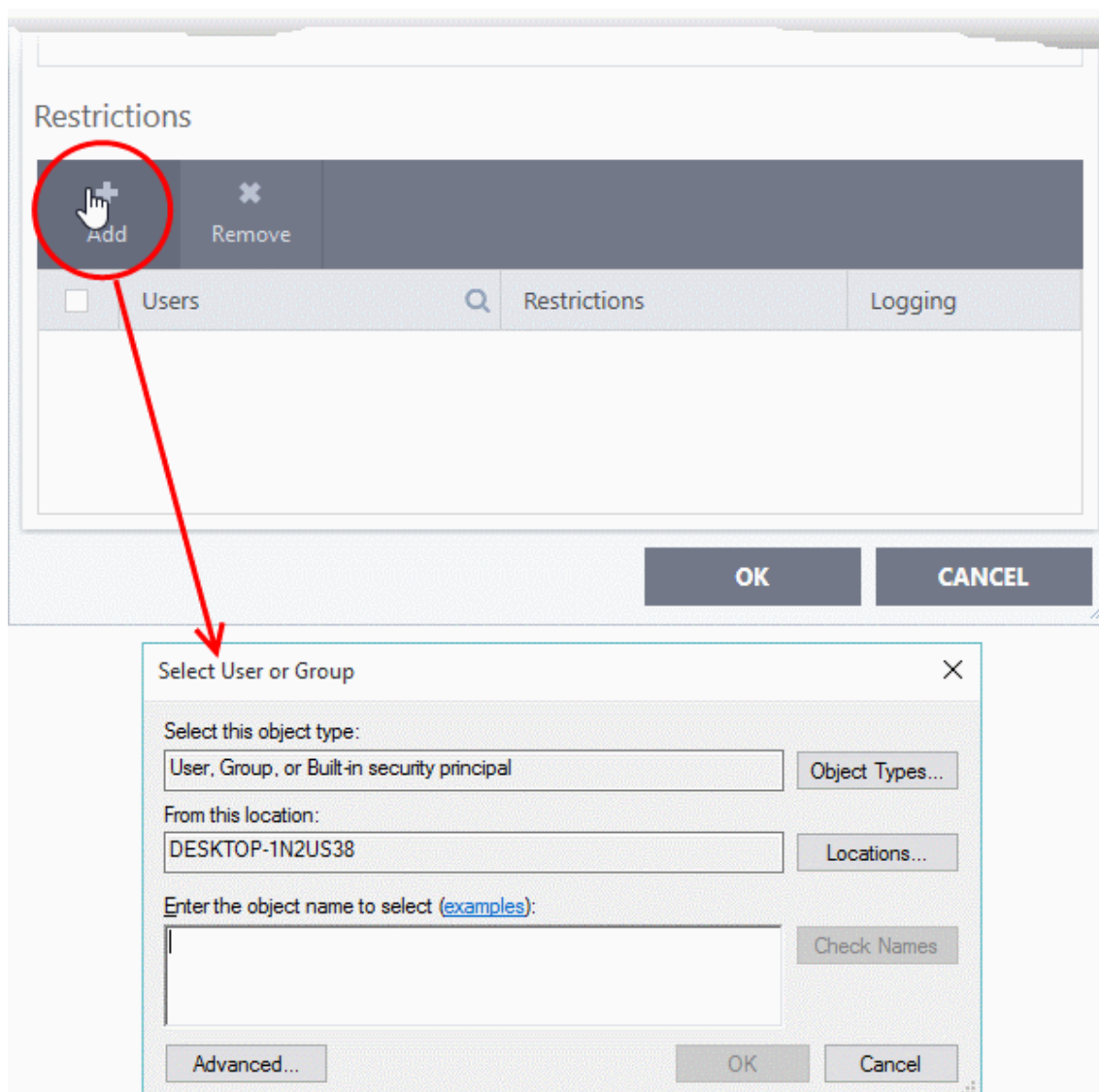
- Enter the names of users to whom the filter should apply in the 'Enter the object name to select' box. Use the format [domain name]/[user/group name] or [user/group name]@[domain name]. Alternatively, click 'Advanced' then 'Find Now' to locate specific users.
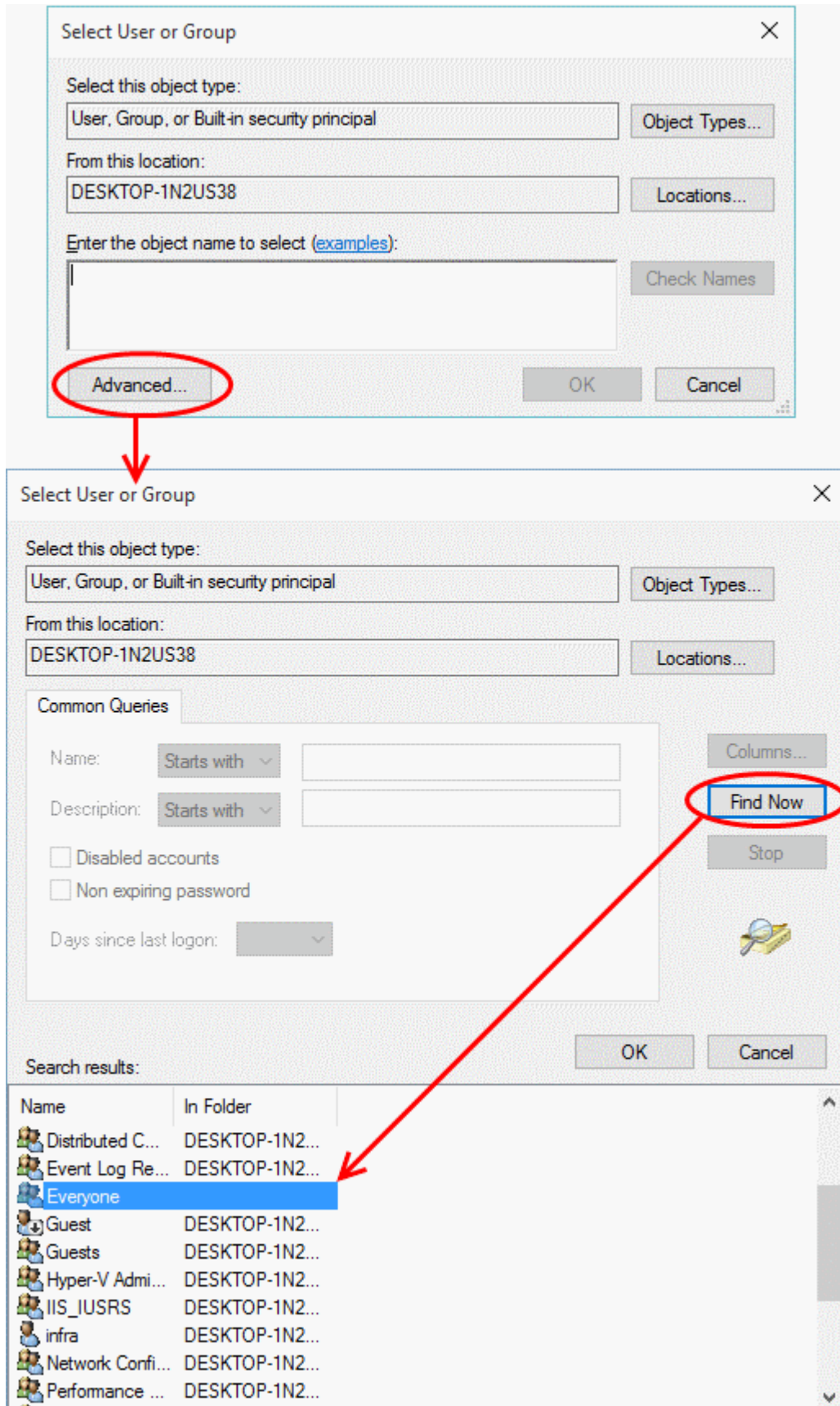
- After adding users or groups, you need to specify what restriction will apply to them. You can allow or block them from viewing the websites in the category or ask them if they want to continue. This is done by modifying the link in the 'Restrictions' column:
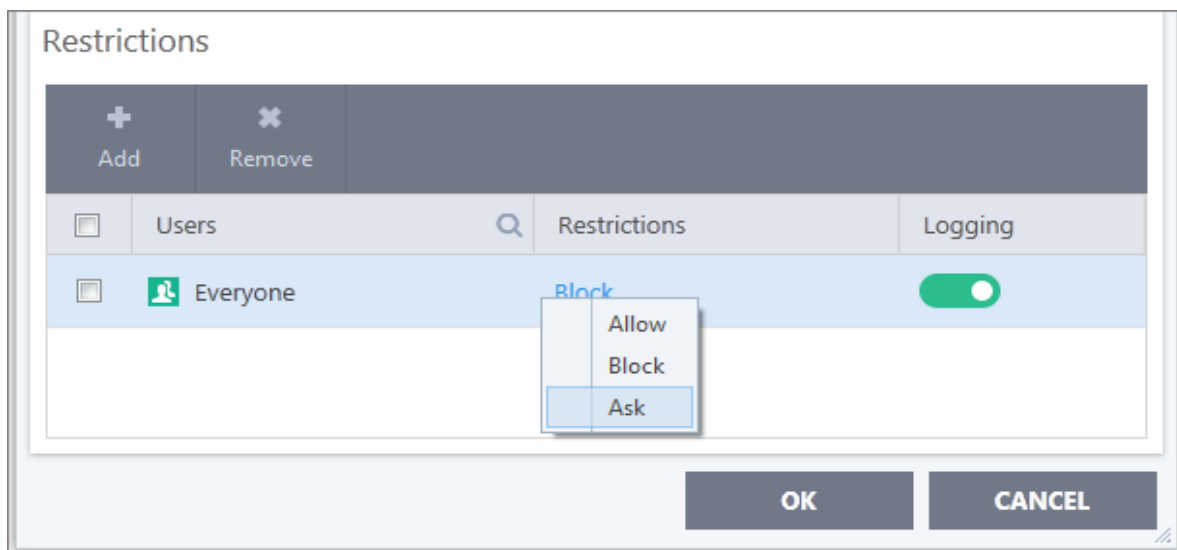
Allow - The websites in the categories can be accessed by the user.

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) to provide maximum security against malware and hackers.

1. Click 'Settings' on the CIS home screen

2. Click 'HIPS' > 'HIPS Settings'

3. Select 'Enable HIPS'
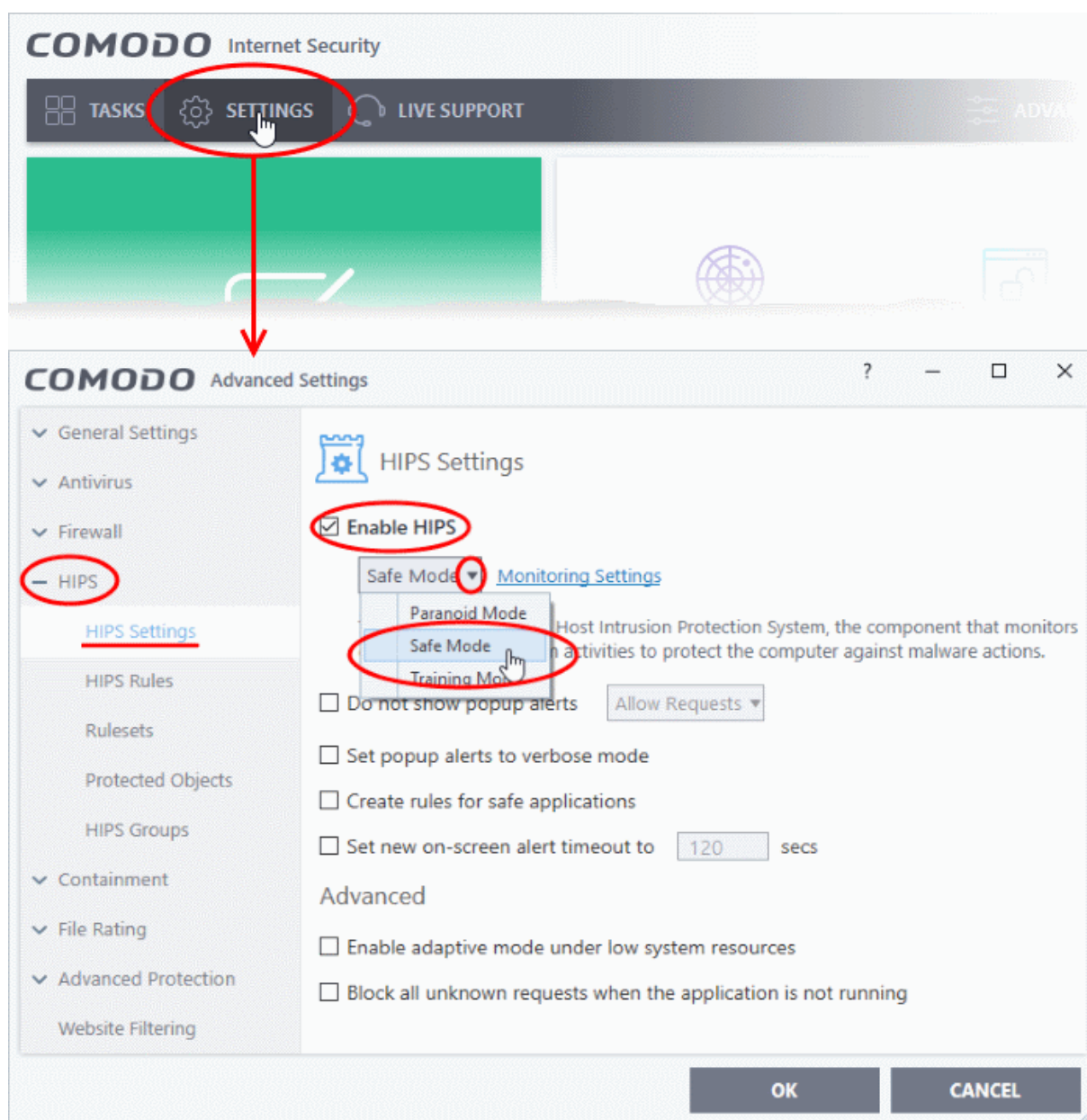
4.   Choose 'Safe Mode' from the drop-down.

See **HIPS Settings** for more details.

Monitoring Settings

5.   Click the 'Monitoring Settings' link in the 'HIPS Settings' interface
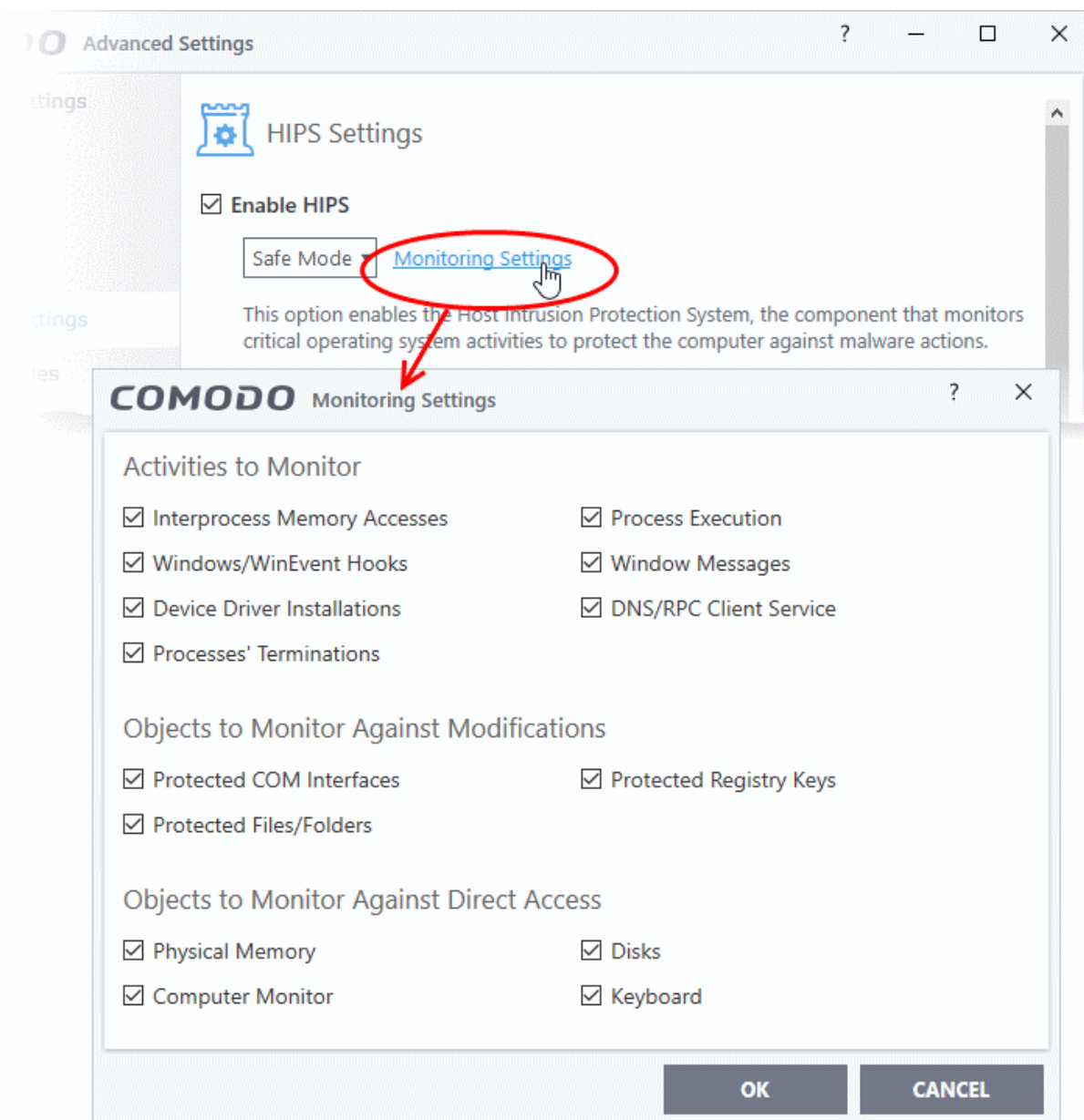
6. Make sure that all the check boxes are selected and click 'OK'

Advanced Settings

- Enable the following settings in the 'Advanced' area of the HIPS Settings interface:
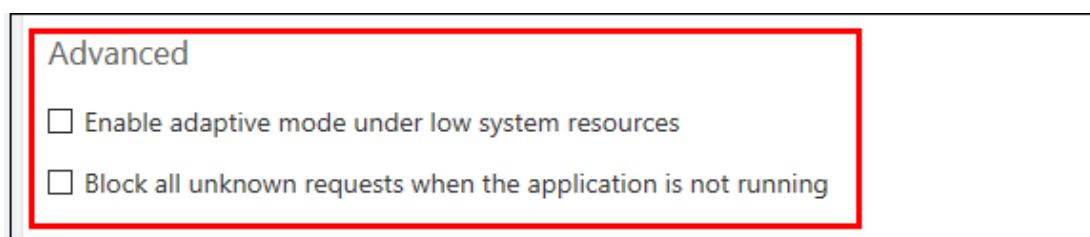
- Optional - Enable adaptive mode under low system resources - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. With this option enabled, CIS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems

- 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.

Click here for more details on HIPS Settings

Create Rules to Auto-Contain Applications

- Click 'Settings' > 'Containment' > 'Auto-Containment'

- Auto-containment rules determine whether a program is allowed to run as normal, run with restrictions, or run in the virtual environment.

- 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.

- CIS consults these rules whenever you open an application. Rules at the top of the list have a higher priority. You can re-prioritize rules using the 'Move Up' and 'Move Down' buttons.

- Programs running in the container have a green border around them.

- CIS ships with some pre-defined rules configured to provide maximum protection for your system. **Click here** to check whether these rules meet your needs before creating a custom rule.

- The rest of this tutorial explains how to create a custom auto-containment rule.

Create an auto-containment rule

1. Click 'Settings' on the CIS home screen

2. Click 'Containment' > 'Auto-Containment'

3. Make sure 'Enable Auto-Containment' is selected

4. Click 'Add'
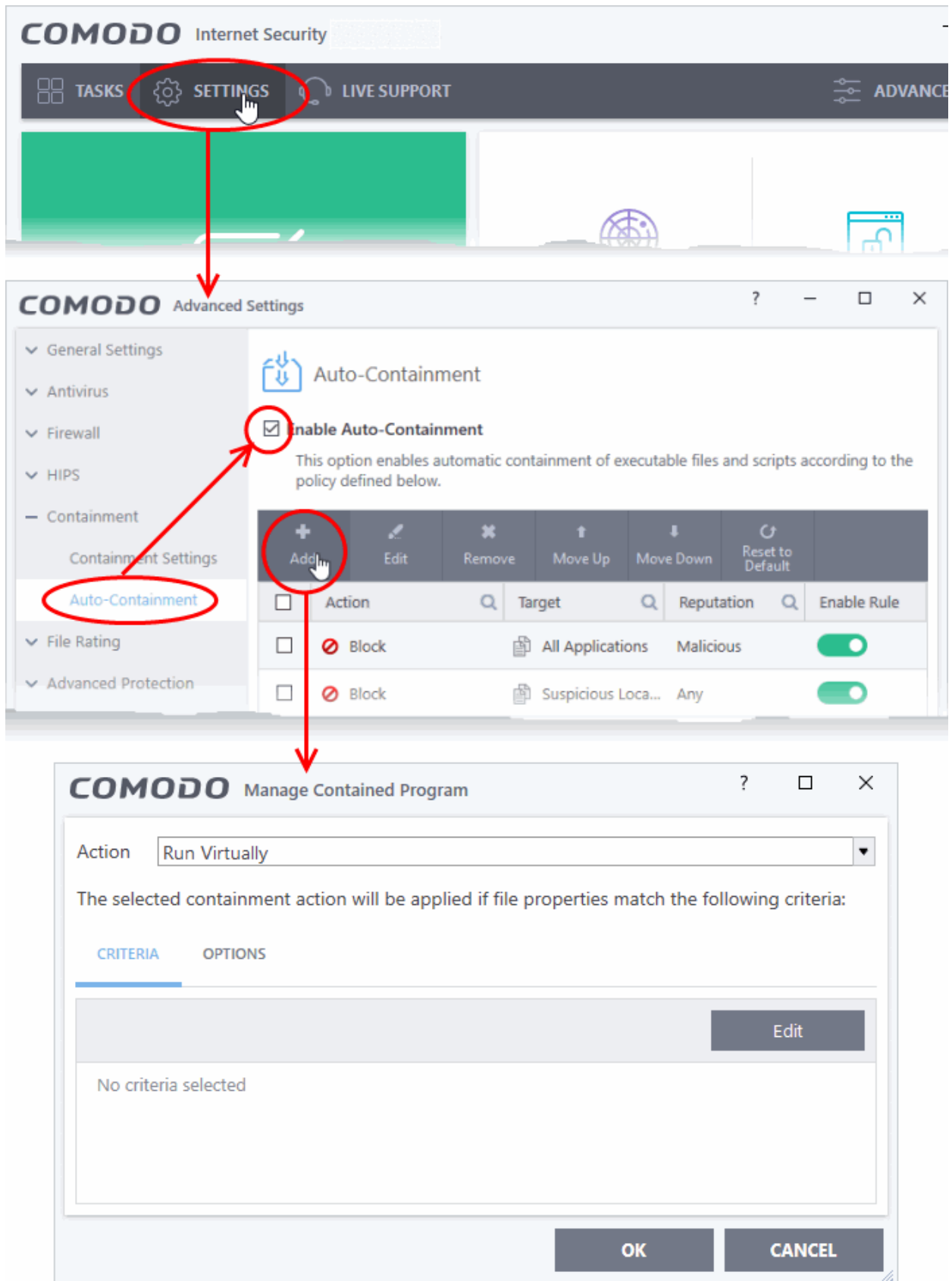
The add rule screen contains two tabs:

- **Criteria** - Define the conditions of the rule.
- **Options** - Configure additional actions like logging, memory usage and time restrictions.

There are 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 - Choose additional options**

Step 1 - Choose the action

The setting in the action drop-down combined with the restriction level in the options tab determine the privileges of an auto-contained application. These items specify what right the application has to access other processes and hardware resources.
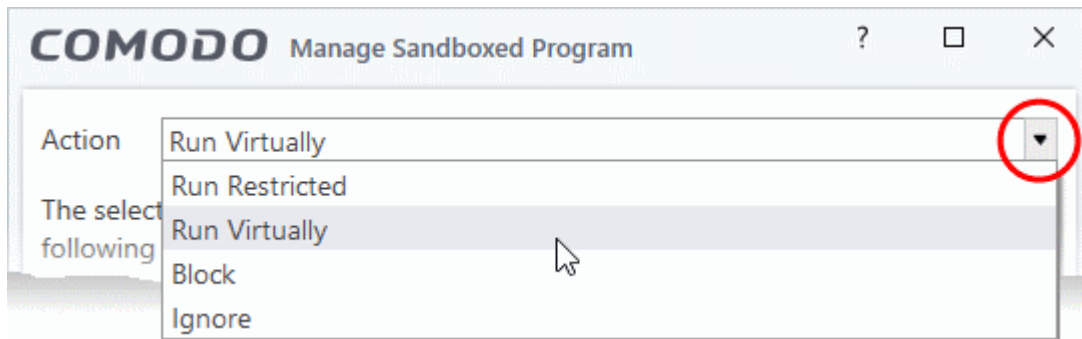
Choose one of the following actions:

- **Run Virtually** - The application will run in a virtual environment, completely isolated from your operating system and the rest of your files.
- **Run Restricted** - The application is allowed limited access to operating system resources. The application is not allowed to execute more than 10 processes at a time. Some applications, like games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application is not contained. It is allowed to run as normal on your computer.

Step 2 - Select the target file/group and set the filter criteria

- The next step is to select the target files and configure filters.
- You can add rule filters so the rule only 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.

Select targets and filters

- Click the 'Criteria' tab.
- Click the 'Edit' button at the far right:
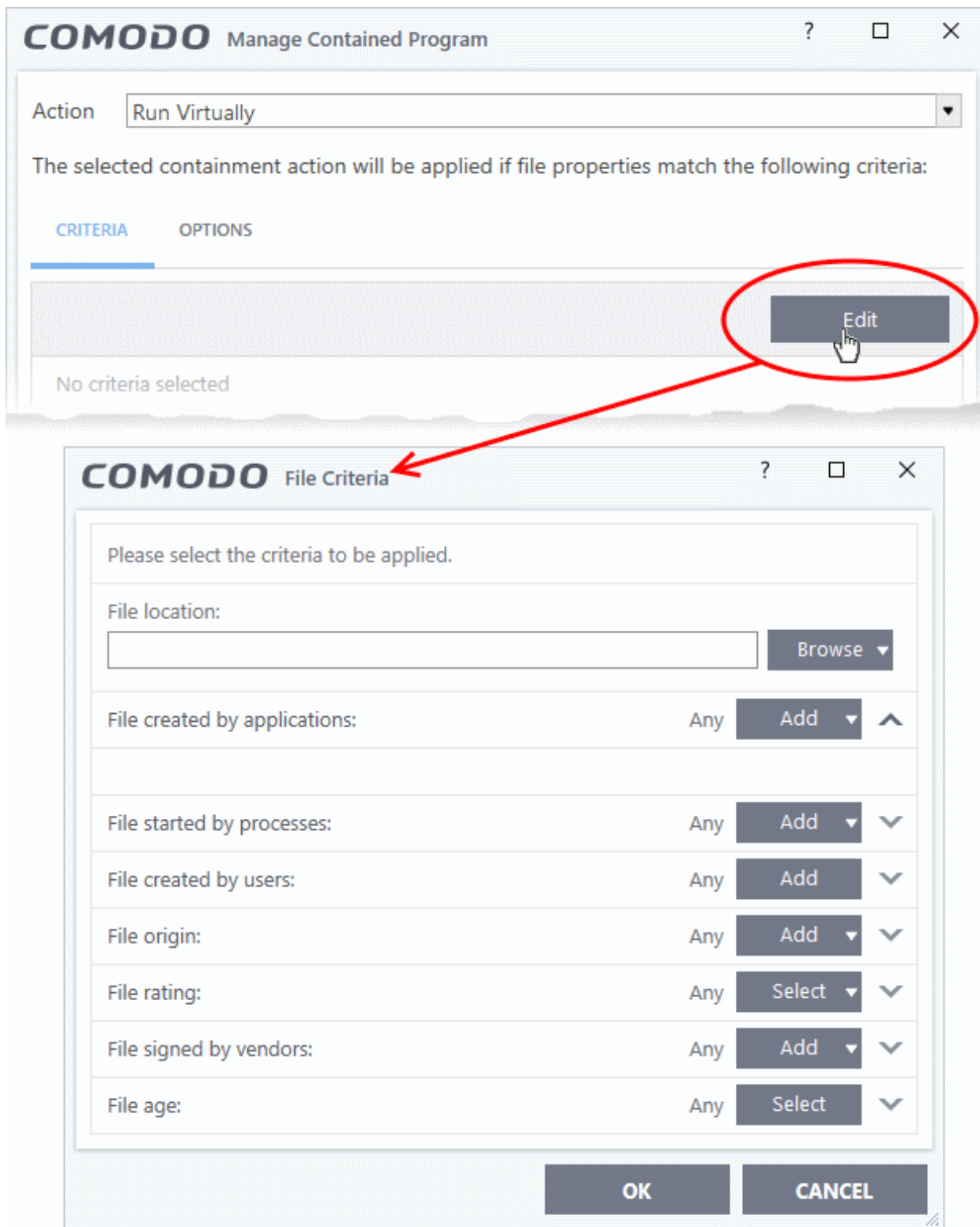
Next:

- • **Select the target**
- • **Configure filters**

Select the target

- • Click the browse button next to the file location field:
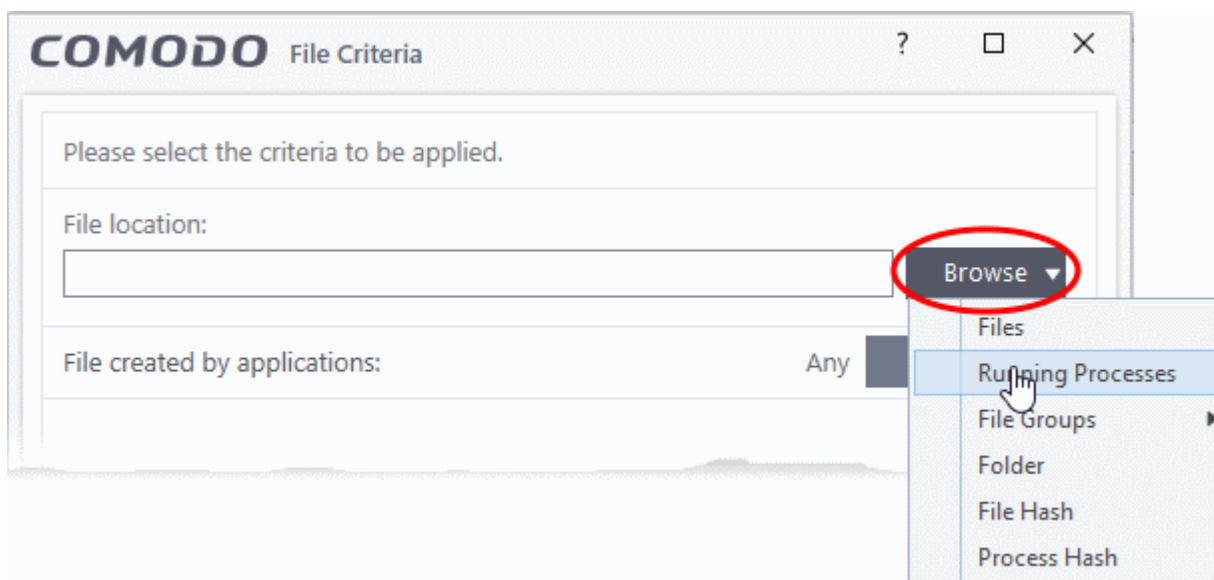
Select one of the following target types:

- **Files** - Add individual files as the target.
- **Running Processes** - Add any process that is currently running on your computer. This targets the parent application of the process.
- **File Groups** - Add a predefined file group as the target. For example, the 'Executables' group contains a list of file types that can run code on your computer. Click 'Settings' > 'File Rating' > 'File Groups' to add or modify a file group.
- **Folder** - Add a directory or drive as the target. All files in the target folder are covered by the rule.
- **File Hash** - Add a file's hash value as the target of the rule. A hash value is a number derived from the file itself, which uniquely identifies and represents the file. It is extremely unlikely that two files can ever generate the same hash value. The rule will apply to the target file, even if the file name changes.
- **Process Hash** - Add a processes hash value as the target of the rule. Please see description above if required.

Add an individual file

- Choose 'Files' from the 'Browse' drop-down.
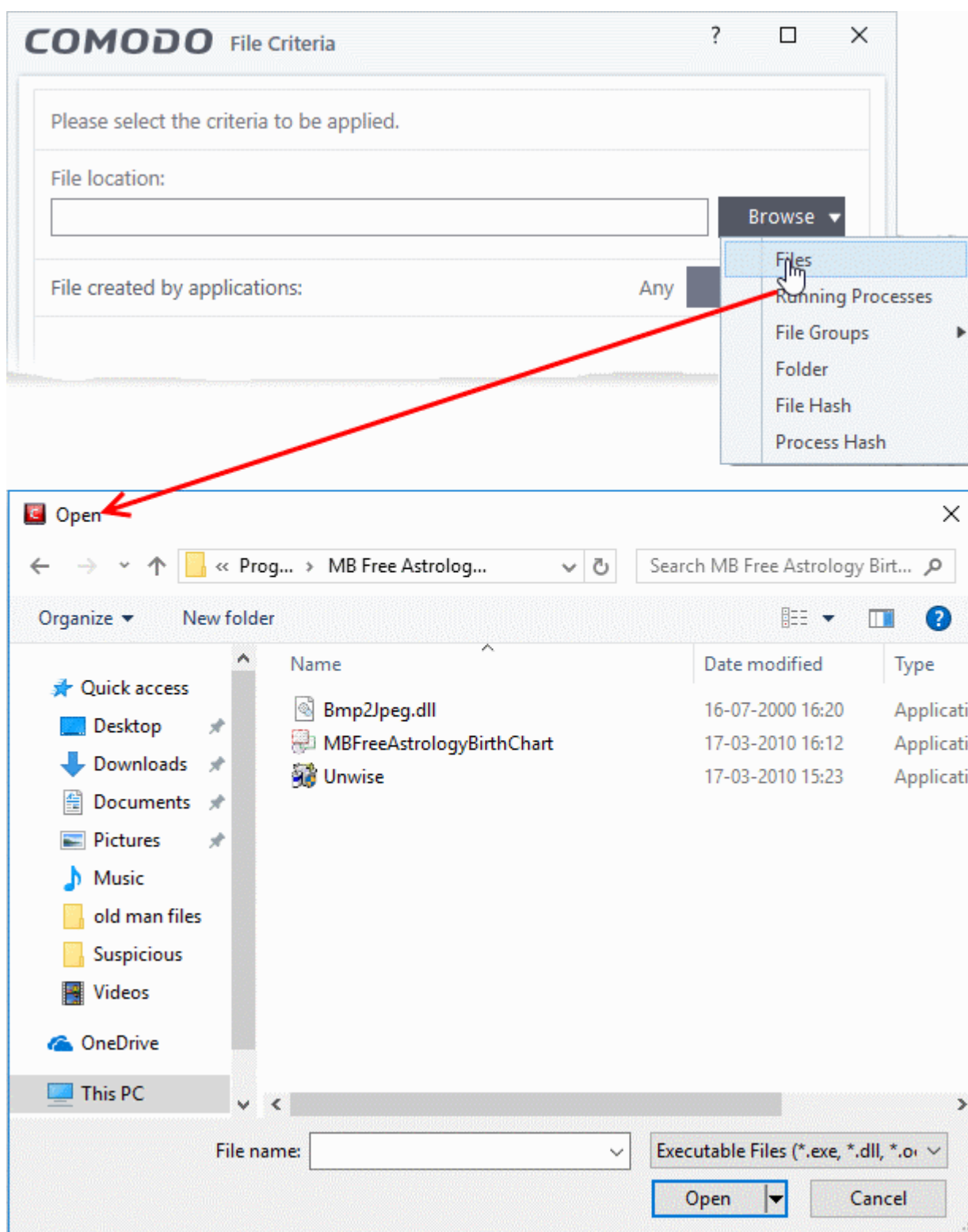
- Navigate to the target file and click open
- The file will be added as the target and run as per the action chosen in **Step 1.**
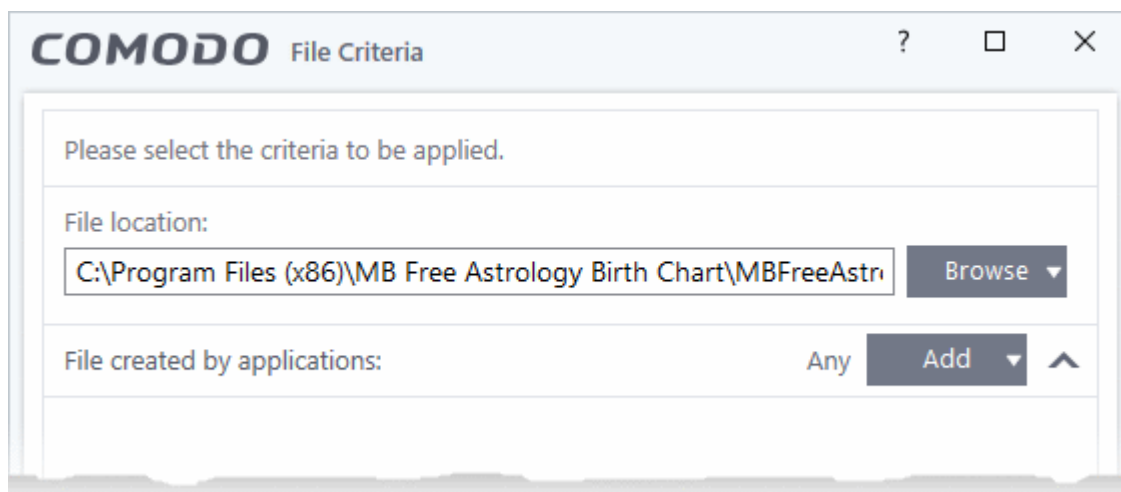
- Click 'OK' if you don't want to specify any filters or options.
- If required ,you can **configure filter criteria and file rating** and **Options** for the rule.

Add a currently running process

- Choose 'Running Processes' from the drop-down:
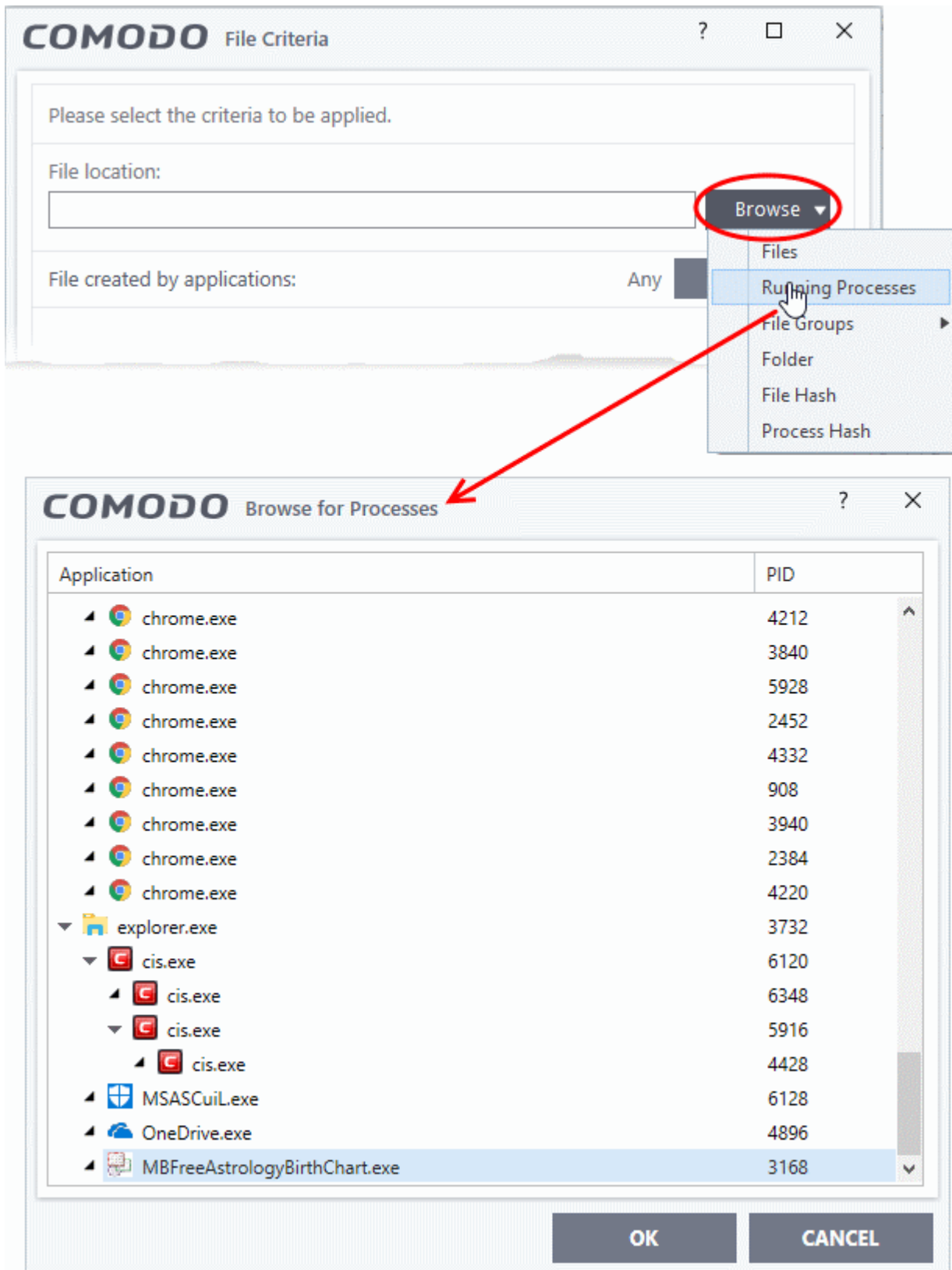
- Select the process belonging to the parent application you want to add and click 'OK'.
- The parent application of the process is added as the target and run as per the action in **Step 1**.
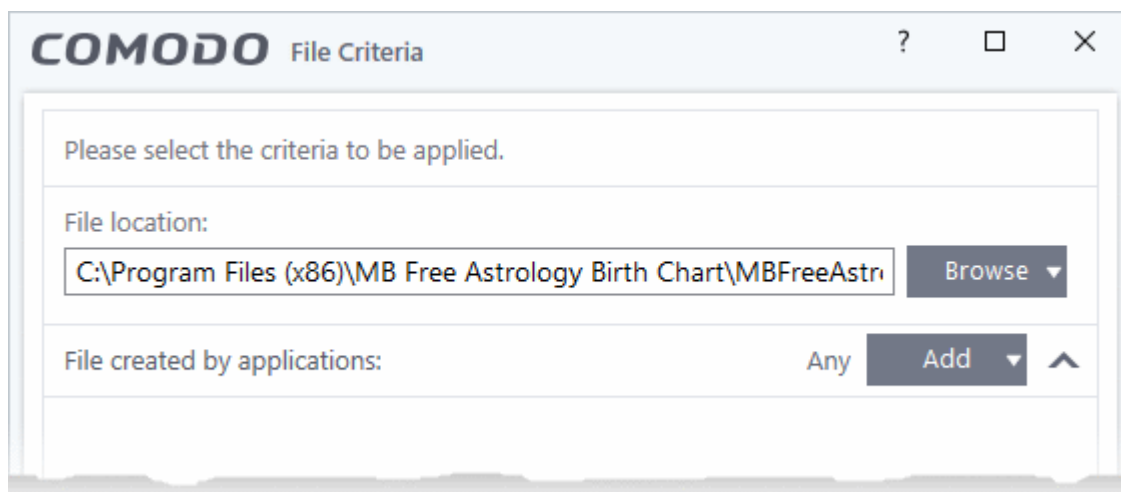
- Click 'OK' if you don't want to specify any filters or options.
- If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Add a file group

- Choose 'File Groups' from the drop-down.
  - For example, the 'Executables' group contains a list of file types that can run code on your computer. Click 'Settings' > 'File Rating' > 'File Groups' to add or modify a file group.
- Select the file group you want to target with the rule:
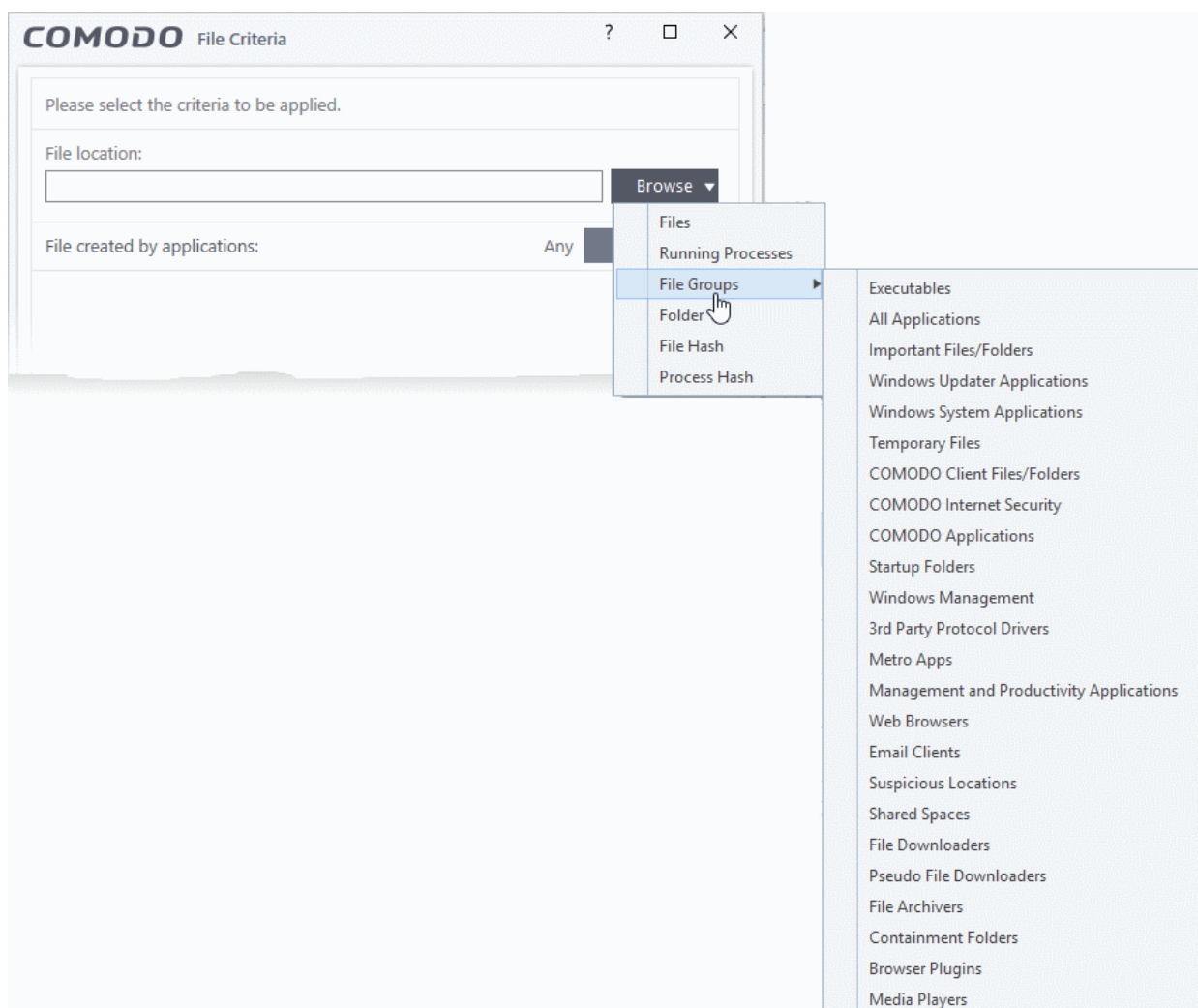
- Click 'OK' if you don't want to specify any filters or options.
- If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Add a folder/drive partition

- Choose 'Folder' from the drop-down:
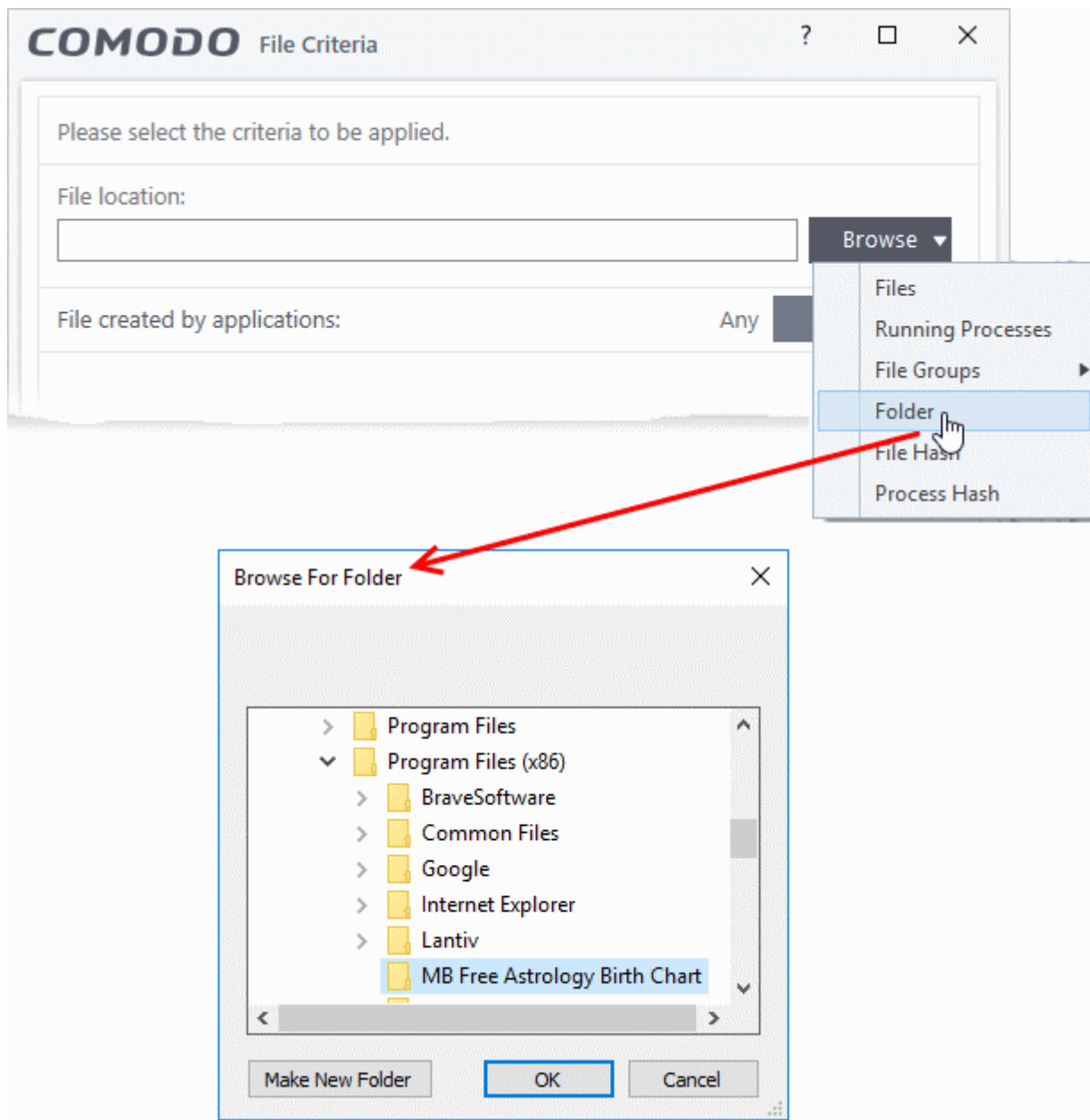
- Navigate to the drive partition or folder you want to add as target and click 'OK'
- Click 'OK', if you don't want to specify any filters or options.

    If required you can **configure filter criteria and file rating** and **Options** for the rule.

Add a file using its hash value

- Choose 'File Hash' from the drop-down:
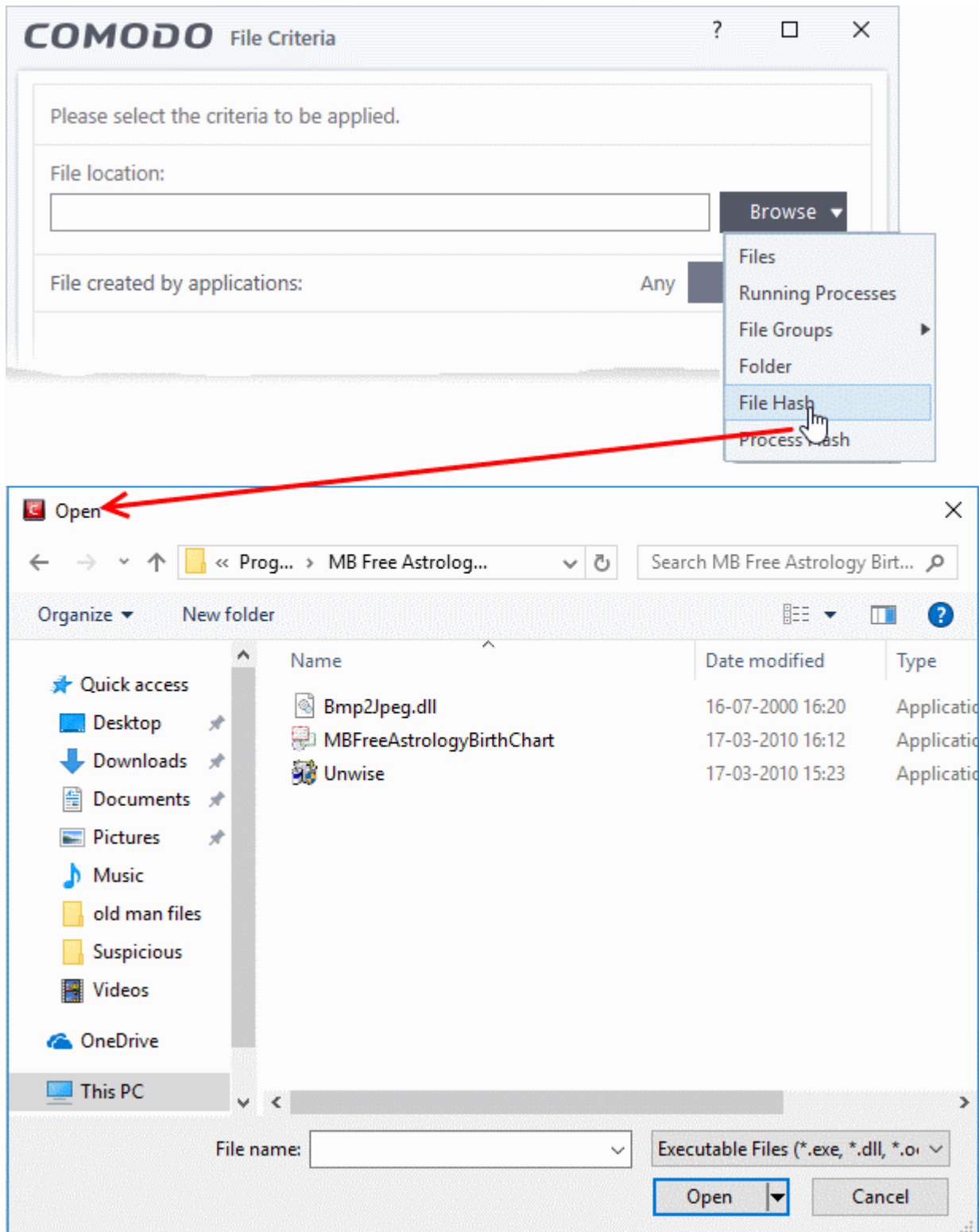
- Navigate to the file whose hash value you want to add as target and click 'Open'

- Click 'OK', if you don't want to specify any filters or options.

- If required you can **configure filter criteria and file rating** and **Options** for the rule.

- CIS generates the hash value of the parent file and stores that as the target.

- CIS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

Add an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.
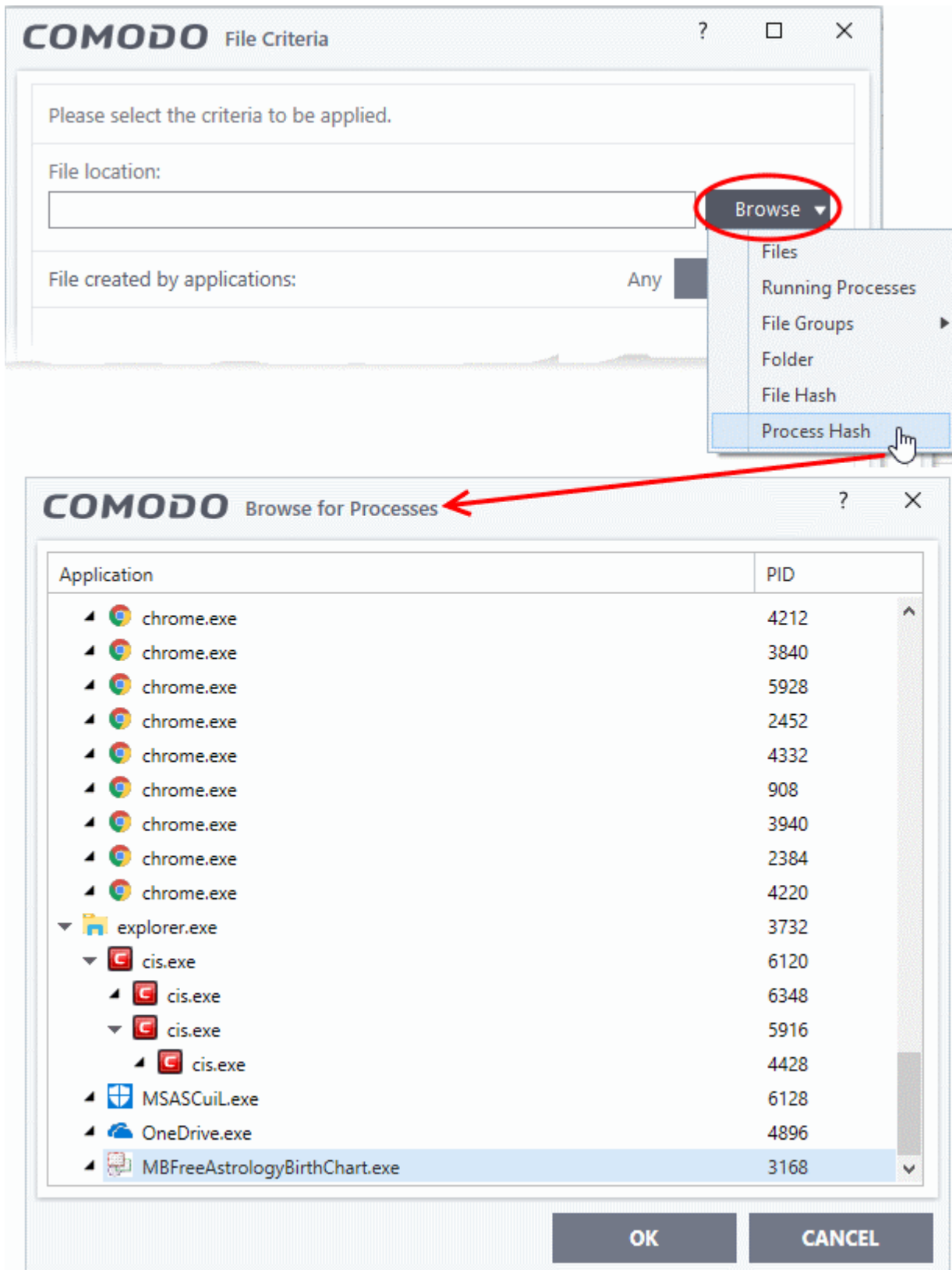
- • Select the process, to add the hash value of its parent application to target and click 'OK' from the 'Browse for Process' dialog.

- • Click 'OK', if you don't want to specify any filters or options.

- • If required you can **configure filter criteria and file rating** and **Options** for the rule.

- • CIS generates the hash value of the parent file and stores that as the target.

- • CIS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if

the file name changes.

Configure Filter Criteria and File Rating

You can apply an action to a file if the file meets certain criteria.

The available criteria are:

- **By application that created the file**
- **By process that created the file**
- **By user that created the file**
- **By file origin**
- **By file rating**
- **By vendor who signed the file**
- **By file age**

Auto-contain a file if it was created by a specific application

- This will apply the rule to a file based on its parent application.
- You can also specify the file rating of the parent application. The rule will then only contain a file if the parent app has a certain trust rating.

Specify parent applications

- Click the add button in the 'File Created by applications' stripe:
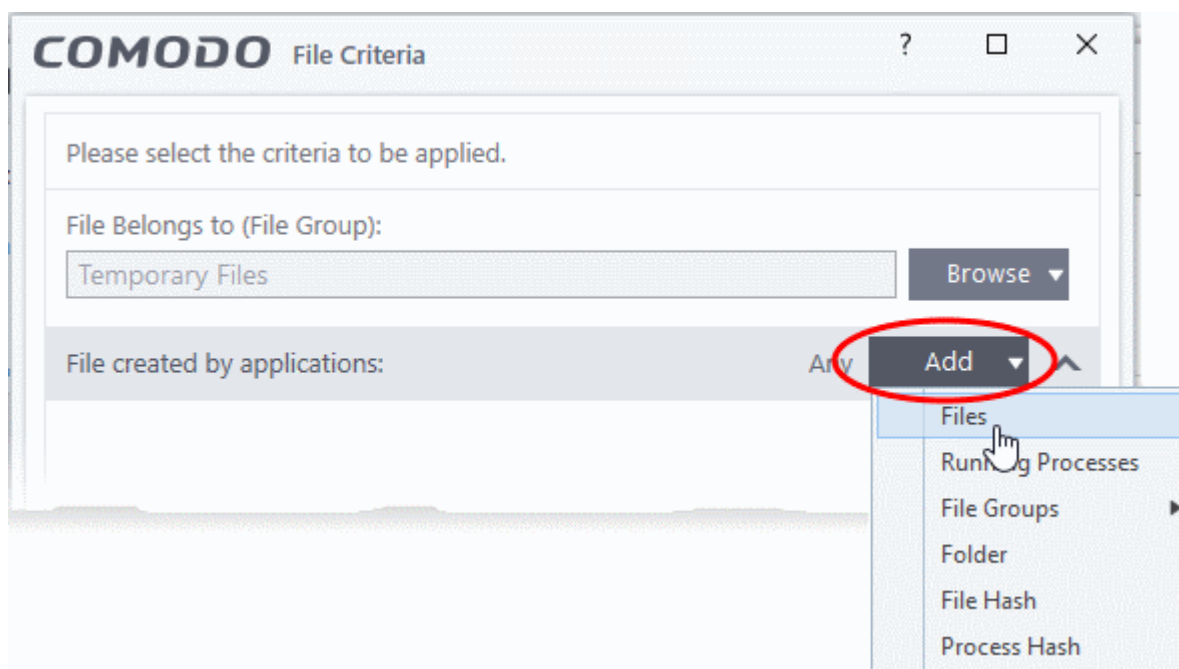
- Browse to and select the parent application. Click 'OK'.
- Click the 'Any' link beside 'File Rating' to select the rating of the parent application:
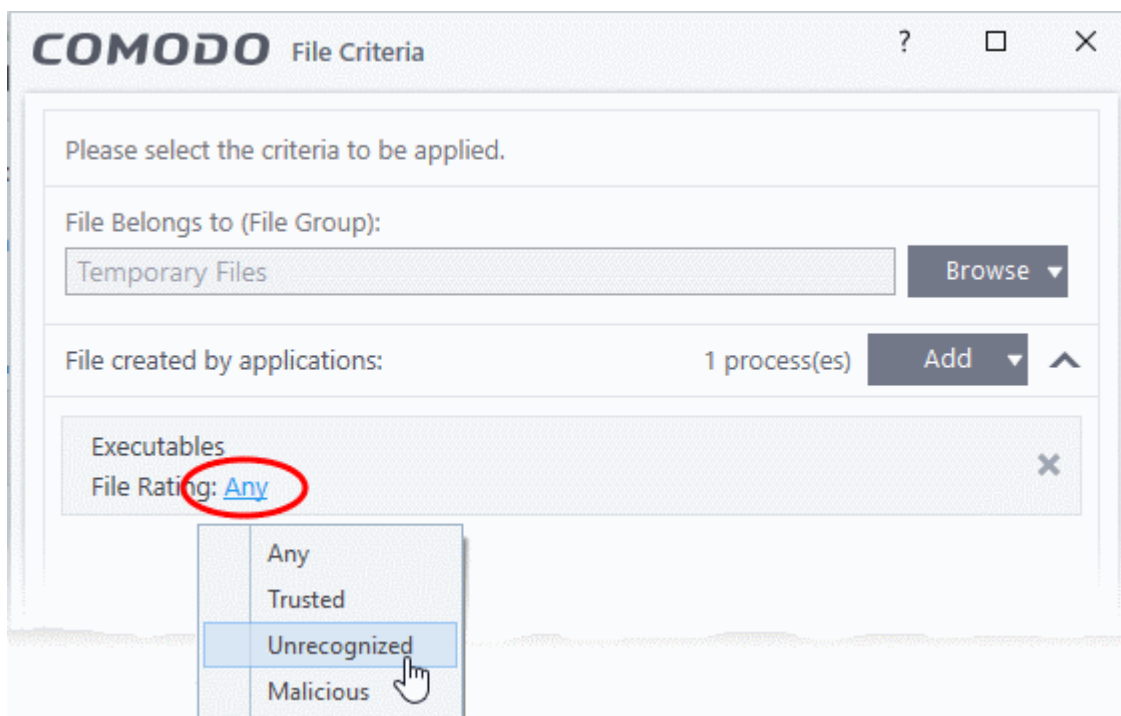
- Select 'Trusted', 'Unrecognized' or 'Malicious'. For example, select 'Unrecognized' to contain all files created by programs which have no trust rating.

- Leave this at 'Any' to contain all files created by the target application.

- Repeat the process to add more applications or groups/folders.

Auto-contain a file if it was created by a specific process

- This will apply the rule to a file based on its based on its parent process.

- You can also specify:

  - The trust rating of the parent process. The rule will then only contain a file if the parent process has a certain trust rating.

  - The number of levels in the process chain that should be inspected.

To specify source process:

- Click the 'Add' button in the 'File Created by Processes' stripe:
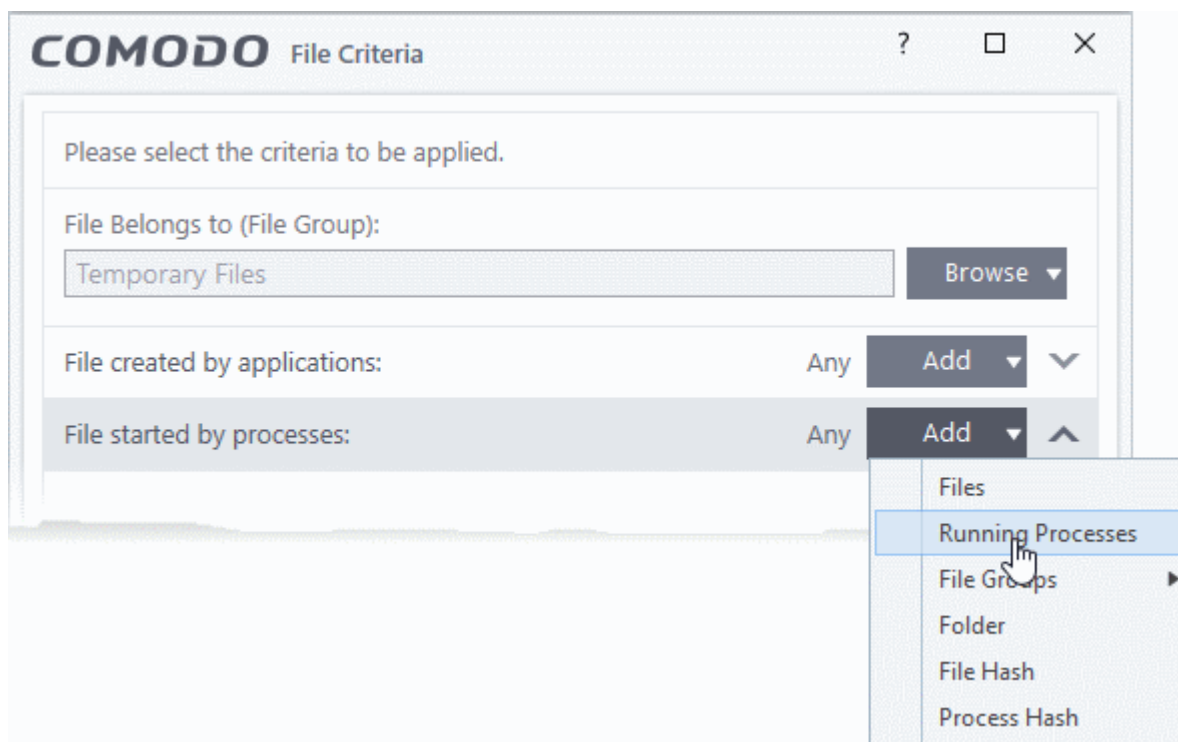
- Browse to and select the target process. Click 'OK'.
- Click the 'Any' link beside 'File Rating' to select the rating of the parent application:
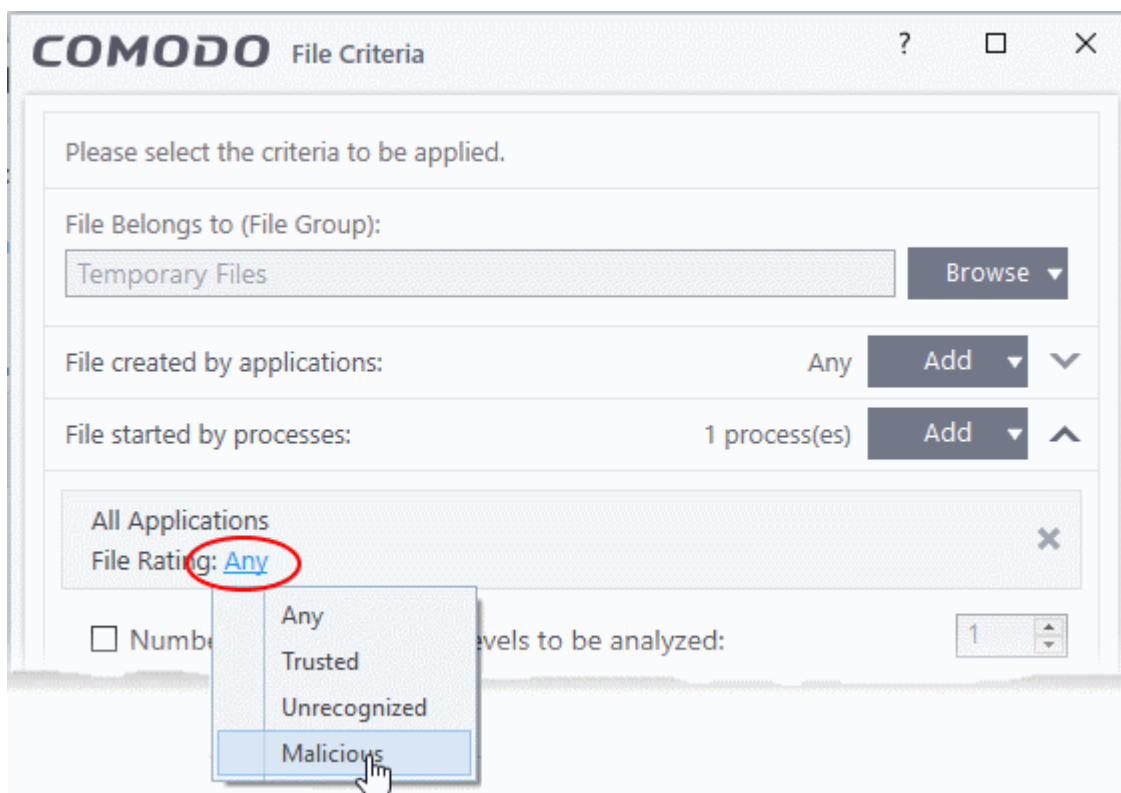
- **'Number of parent process levels to be analyzed'** - Specify how far up the process tree CIS should check. 1 = will only check the trust rating of the file's parent process. 2 = will check the trust rating of the parent process and the grand-parent process. Etc.
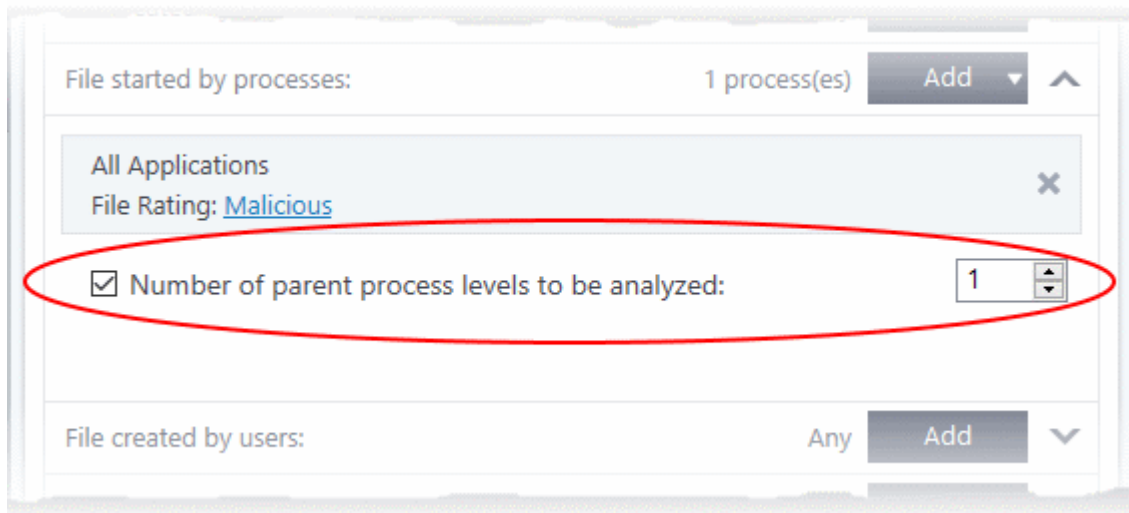
- Repeat the process to add more processes

Auto-contain a file created by specific users

- Click the 'File Created by Users' stripe and then click the 'Add' button.
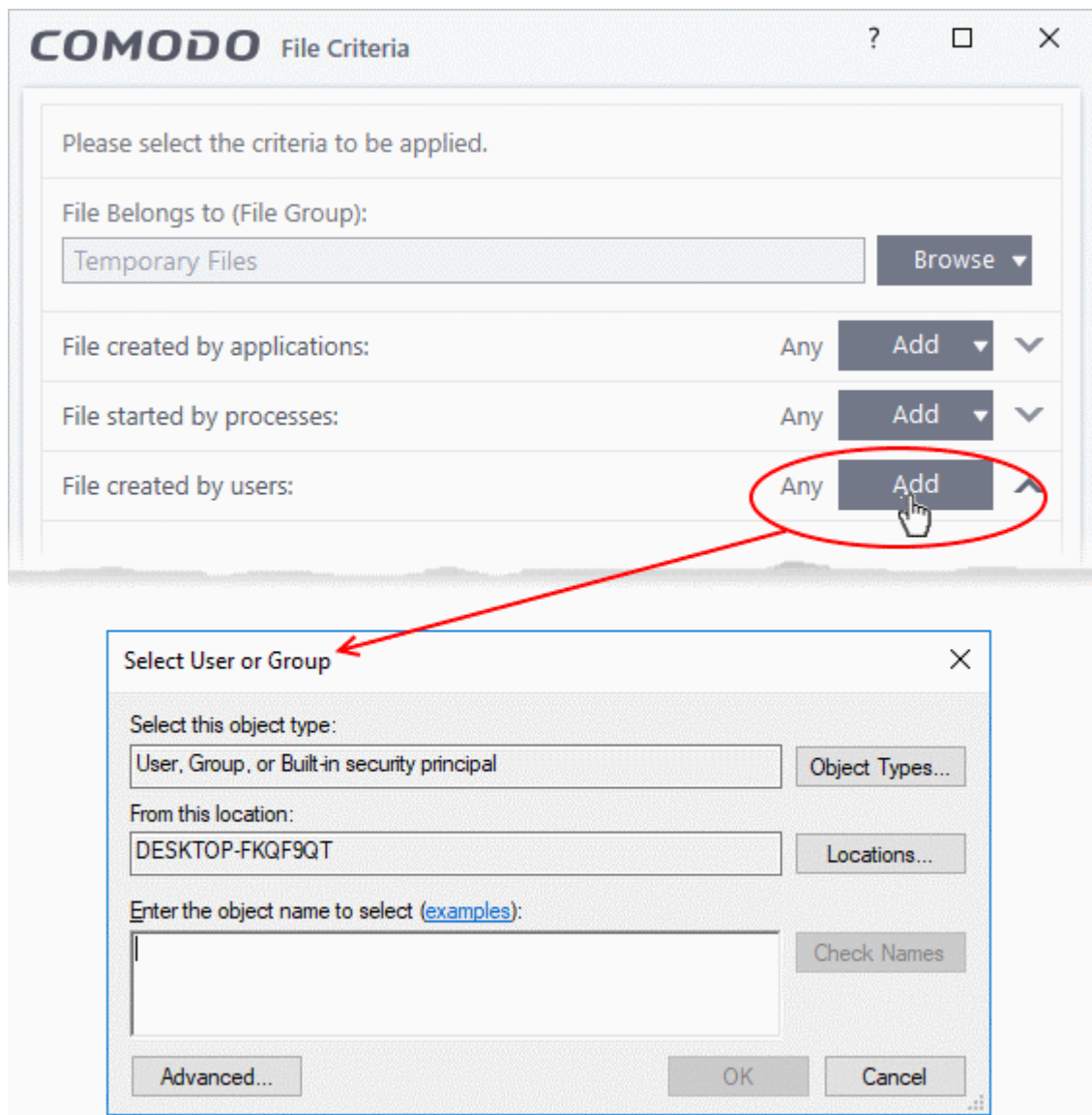
- Enter the names of the users you want to add in the large text box.

- Name 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 your choice.
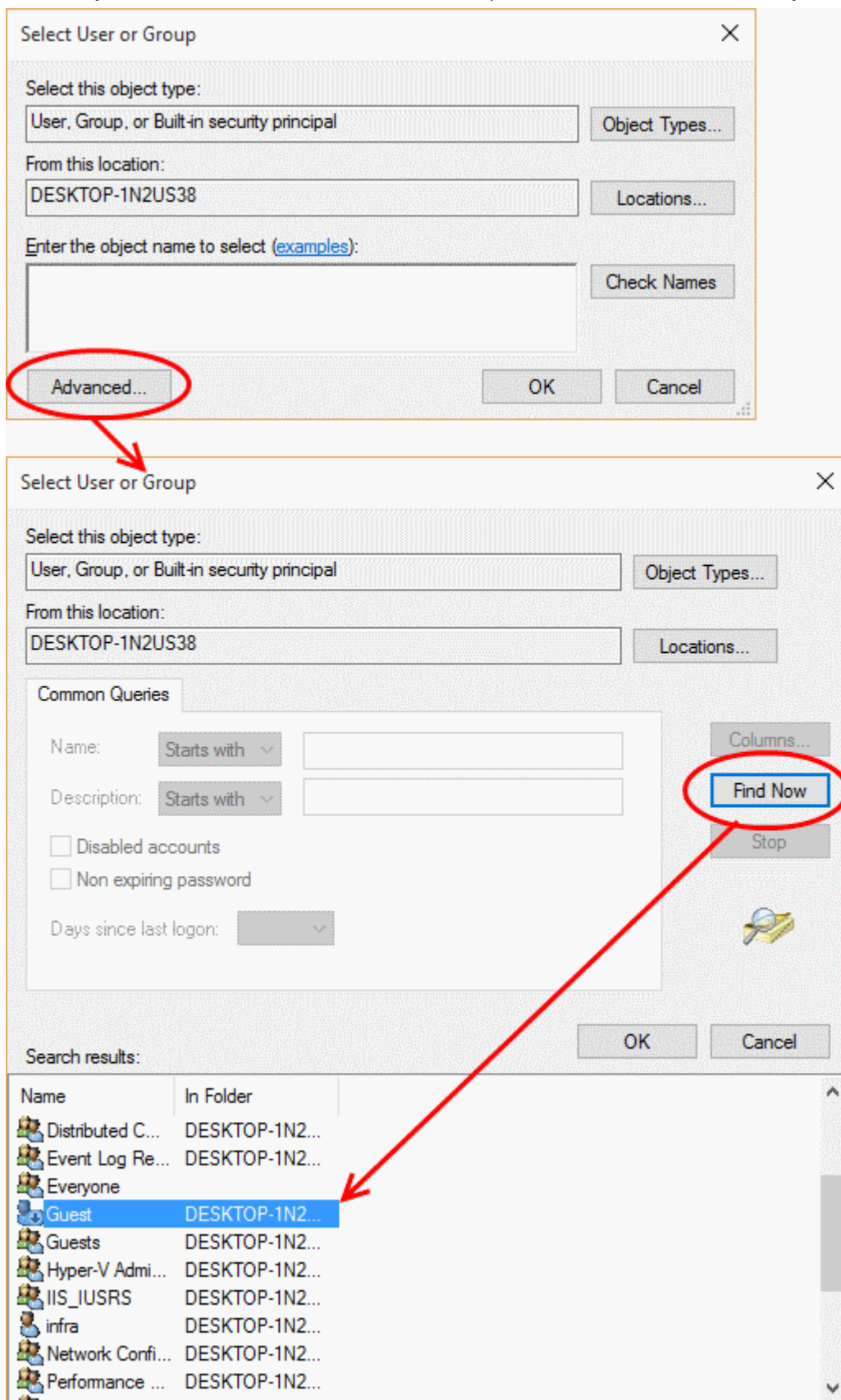
The user will be added to the list.
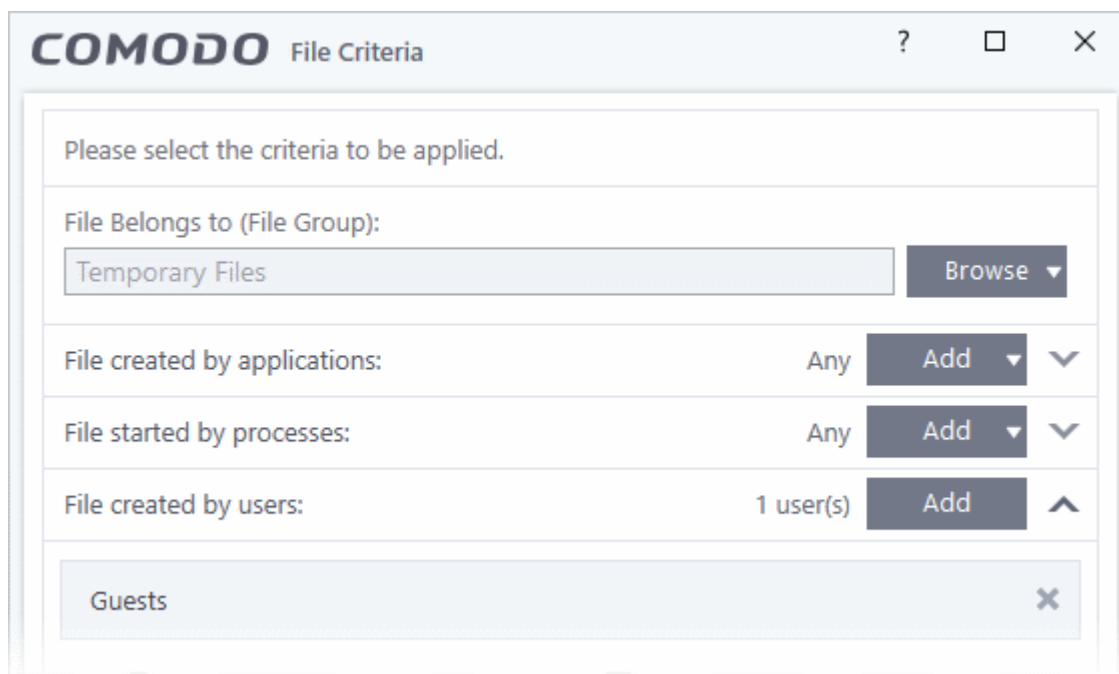
- Repeat the process to add more users.

Auto-contain a file if it was downloaded/copied from a specific source

- Click the 'Add' button in the 'File Origin' stripe:
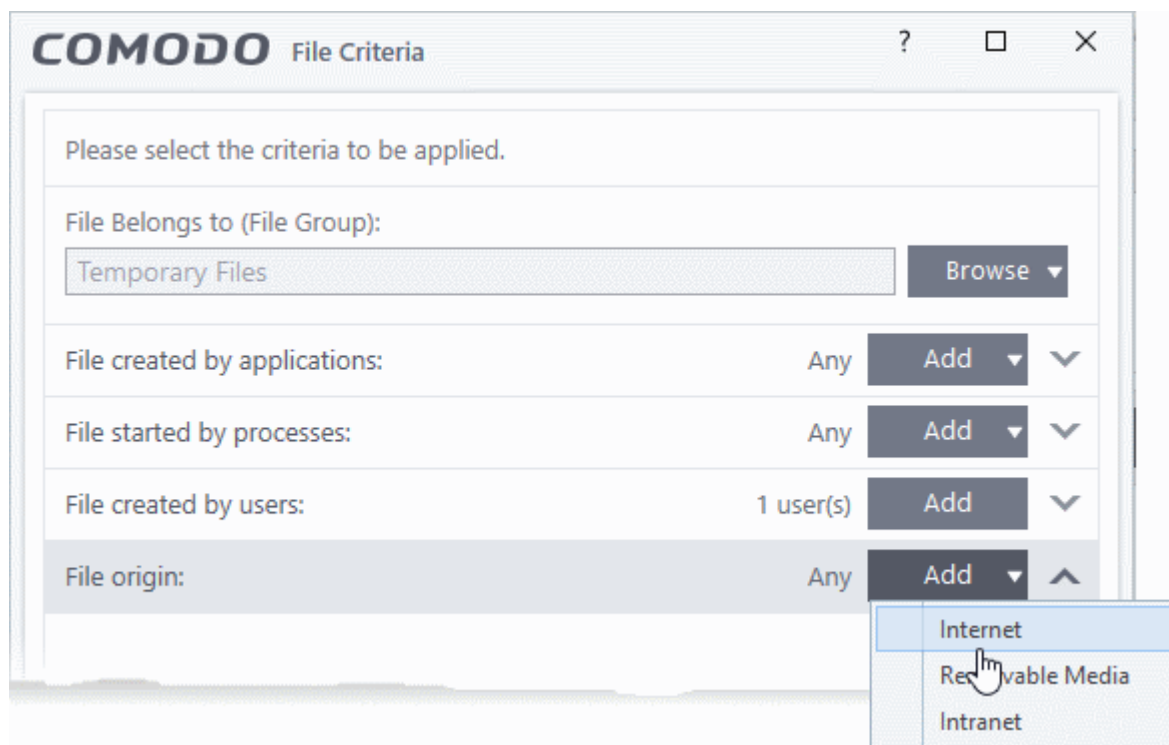
- Choose the source from the options:

  - **Internet** - Apply the rule to files that were downloaded from the internet.
  - **Removable Media** - Apply the rule to items copied to your computer from removable storage devices.
  - **Intranet** - Apply the rule to files downloaded from the local intranet.

- Repeat the process to add more sources

Select file rating as filter criteria
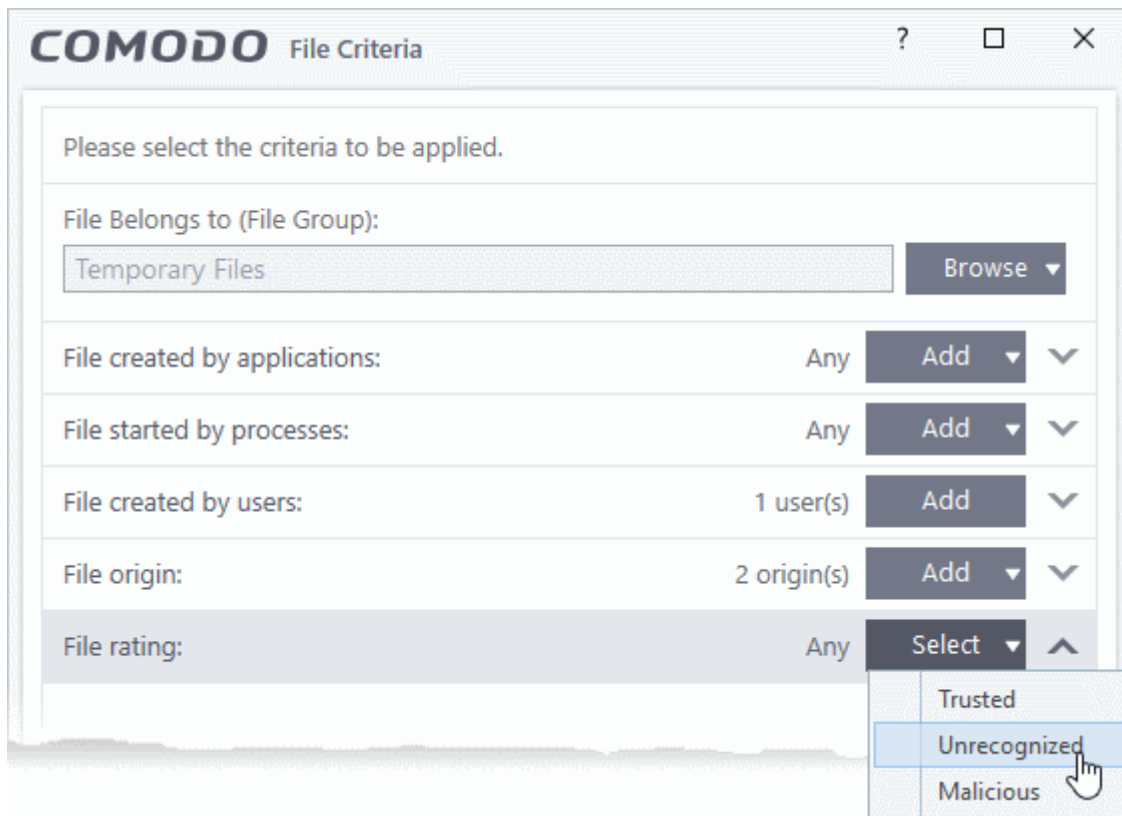
- Click the 'Select' button in the 'File Rating' stripe

- This will apply the rule to files which match the trust rating you set. You can choose from the following trust ratings:

    - **Trusted** - Applications are categorized as 'Trusted' if:

        - The file is on the global whitelist of safe files

        - The file is signed by a trusted company in the **Vendor List**

        - The file was installed by a trusted installer

        - The file was given a trusted rating in the **File List** by a user

    - See **File Rating Settings** for more information.

    - **Unrecognized** - Files that do not have a current trust rating. The file is on neither the blacklist nor the safelist, so is given an 'unknown' trust rating. See **File List** for more information.

    - **Malware** - Malicious files - those that are on the blacklist of known harmful files.

Auto-contain a file based on the software vendor

- You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.

- You can also specify the trust rating of the vendor. The rule will only contain a file if its vendor has the stated trust rating.

Choose vendors:

- Click the 'Add' button in the 'File Created by Processes' stripe.

- There are three ways you can add a vendor:

    1. **Directly select a vendor**

        - Choose 'Vendor from a Vendor List' from the drop-down
        - The 'Add Vendor' dialog opens with a list of vendors in the **Vendor List**

- Use the sort and filter options in the column headers to search for the vendor to be specified
- Choose the vendor and click 'OK'. The vendor will be added as a criterion.

2. Specify an executable file on your local drive

- Choose 'File Signer' from the drop-down
- Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
- CIS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

3. Select a currently running process

- Choose 'Running Process Signer' from the drop-down
- A list of all processes running at present on your computer is shown
- Select the process to specify the publisher of the application that started the process and click 'OK'
- CIS checks that the .exe file that started the process is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

The selected vendor is added:

- **Vendor Rating** - The rule will only apply to the vendor's files IF the vendor has this rating at the time the file is checked. Note, the rating you set here can be different to the actual vendor rating in 'Settings' > 'File Rating' > 'File List' > 'Vendor Rating'.
  - Example. If you select 'Trusted' here, then CIS will apply the rule if the vendor is trusted at the time the file is checked. If the vendor's rating changes to 'Malicious' or 'Unrecognized', then the rule isn't applied.

- Repeat the process to add more vendors

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.

Step 3 - Select options

The next step is to choose additional options and restrictions on items contained by the rule.

- Click the 'Options' tab.

The options available depend on the 'Action' chosen in **Step 1**.

The '**Ignore**' action has the following options:

- **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 those started by the target application.

    - This option is disabled by default, so the ignore rule also applies to child processes.
    - If enabled, the ignore rule does not apply to child processes. Each child process will be inspected individually and all relevant rules applied.

The '**Run Restricted**' and '**Run Virtually**' actions have the following options:

- **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.

The '**Block**' action has the following options:

- **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 moved to CIS quarantine. See **Manage Quarantined Items** for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.
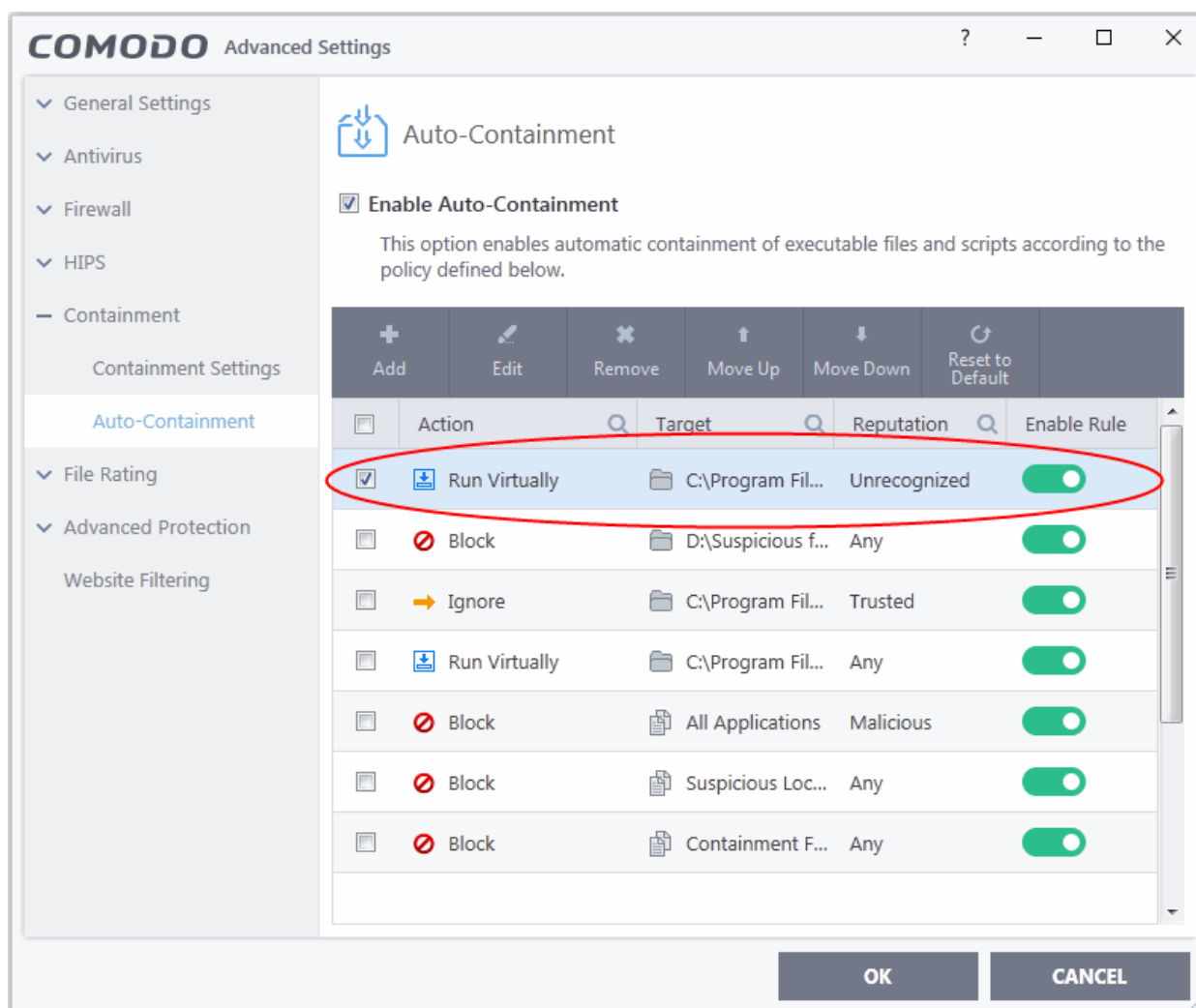
You can move the rule up or down the list to change its priority.

Important Note: Please make sure auto-containment rules do not conflict. In the event of a conflict, the setting in the rule that is higher in the list prevails. The 'Reset to Default' button lets you restore the original rules.

Password Protect Your CIS Settings

- This page explains how to password protect access to the CIS settings interface.

- This helps block other users from changing or disabling the security settings you have implemented.

Enable password protection

1. Click 'Settings' on the CIS home screen

2. Click 'General Settings' > 'User Interface'

3. Select 'Enable Password Protection' then click the 'Set Password' link:
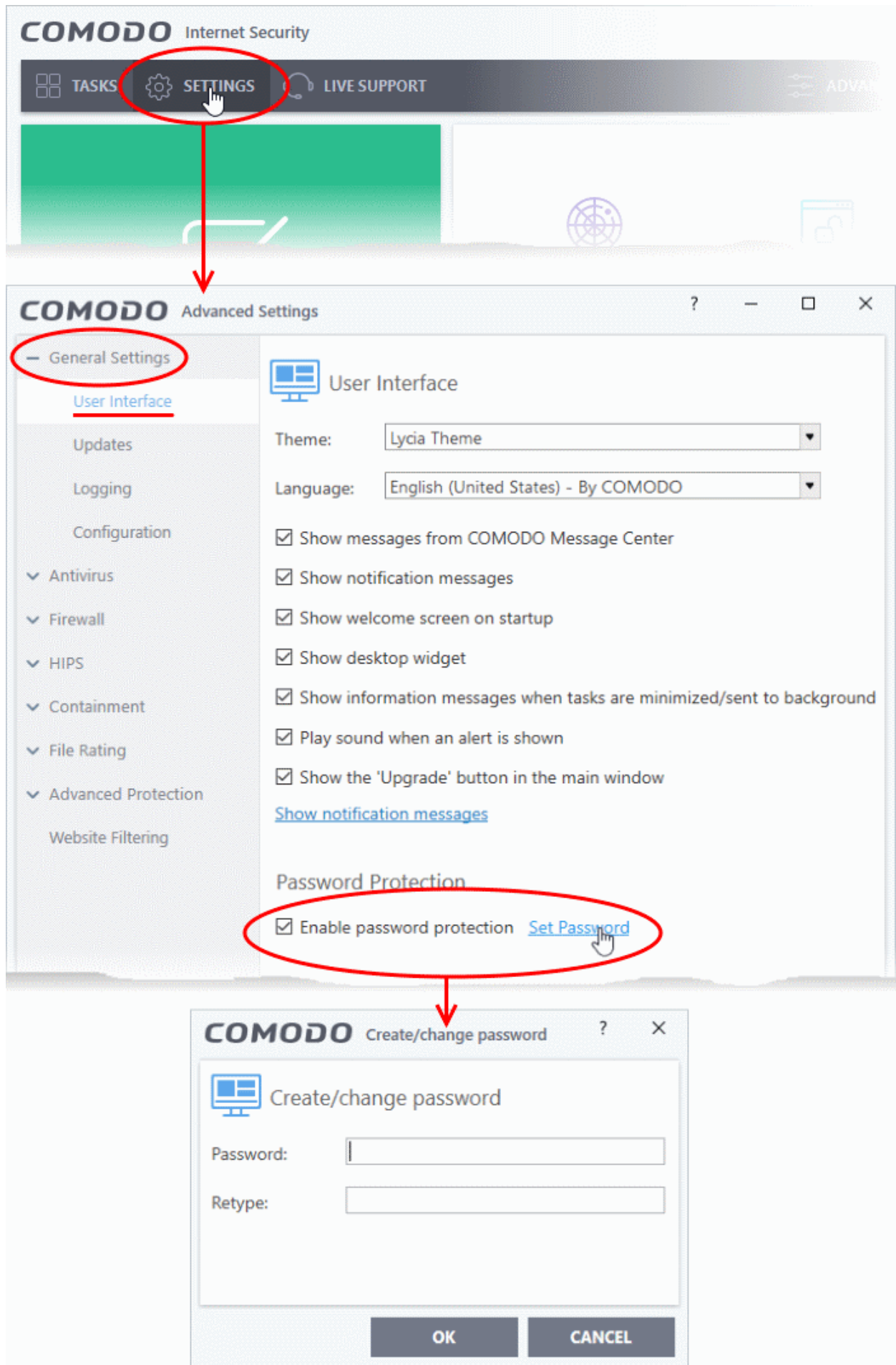
4.   Enter and confirm your password then click 'OK'. Make sure to create a strong password with a mix of upper/ lowercase letters, numbers and symbols.

Users will now need to enter the password to access the settings area:
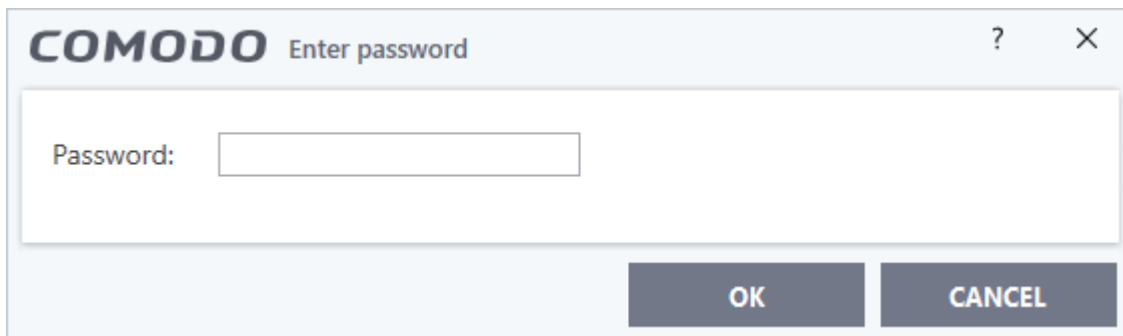
Reset Forgotten Password (Advanced)

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.

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'
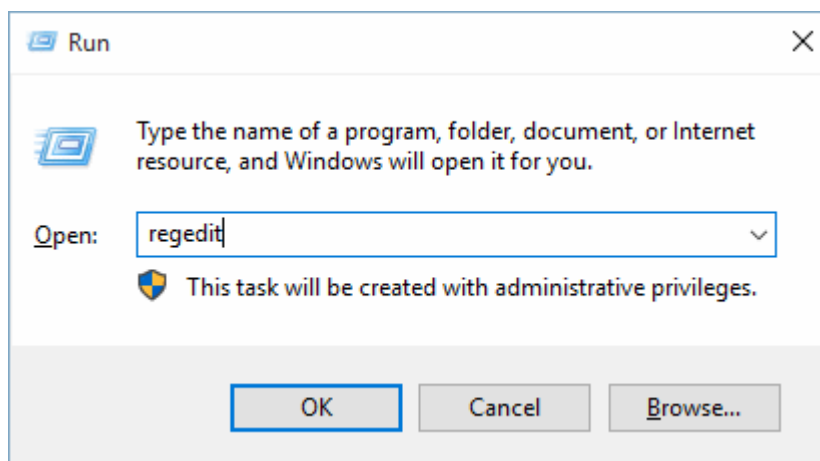
3.   Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\

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.
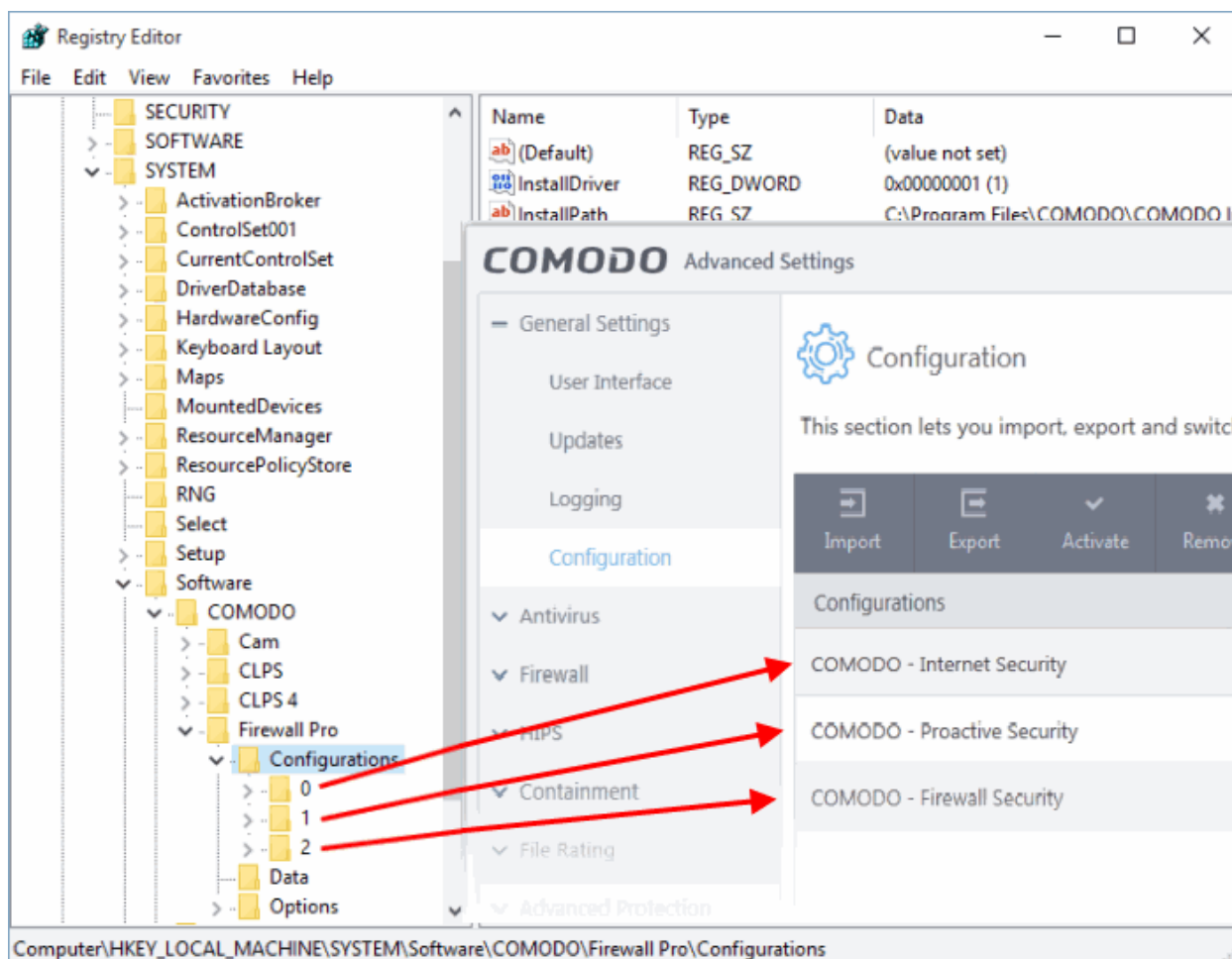
4.   Select the folder corresponding to the configuration for which you wish to reset the password and navigate
       to Settings, for example, navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\
       Configurations\0\Settings to reset password in COMODO - Internet Security configuration.
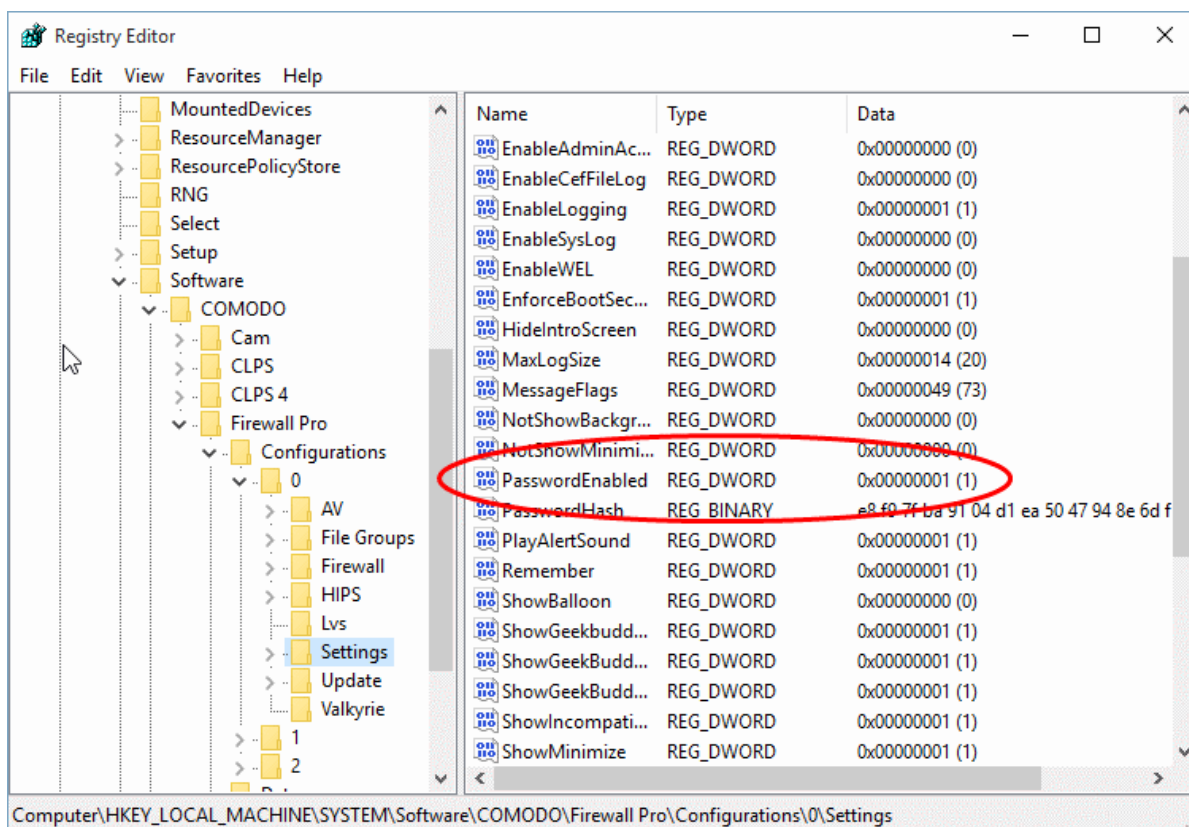
5.   Right-click 'PasswordEnabled' key and select 'Modify'
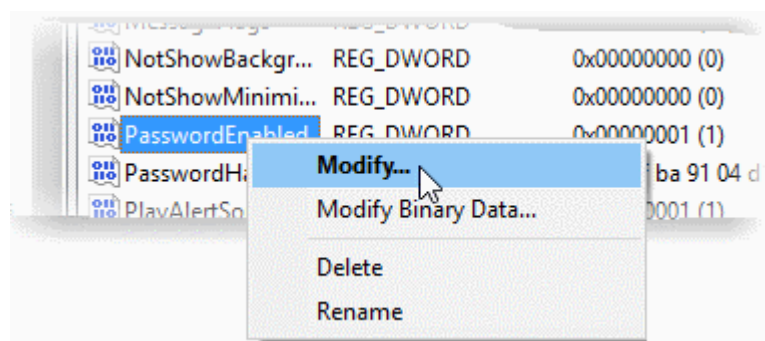
6.   In the 'Edit DWORD Value dialog box, change the 'Value data' from 1 to 0
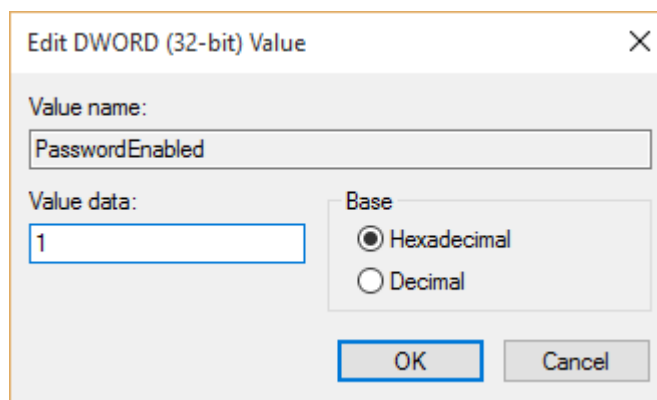
7.   Click 'OK'

8.   Right-click 'PasswordHash' and select 'Delete'.
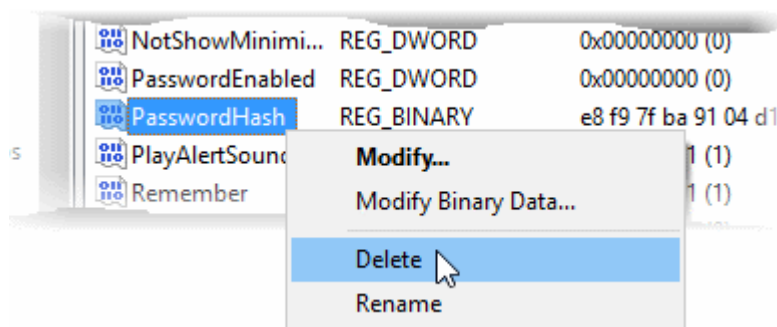
9. Restart the system for the changes to take effect

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 scan individual files or folders instantly to check whether they contain any threats.
- This is useful if you are wary about an item you have copied from an external source or downloaded from the internet.

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' box:

OR
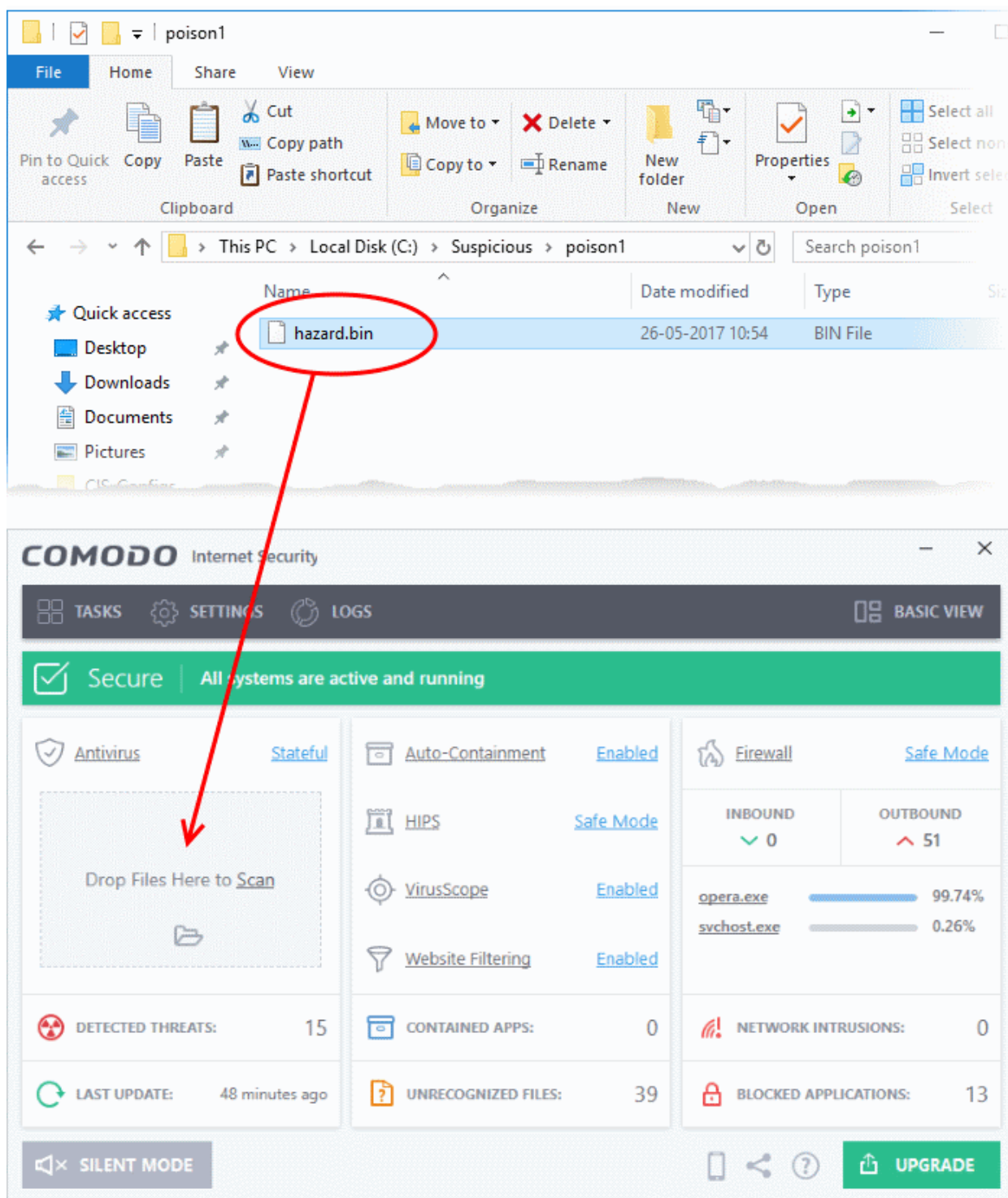
- Right-click on a file and select 'Scan with Comodo antivirus':
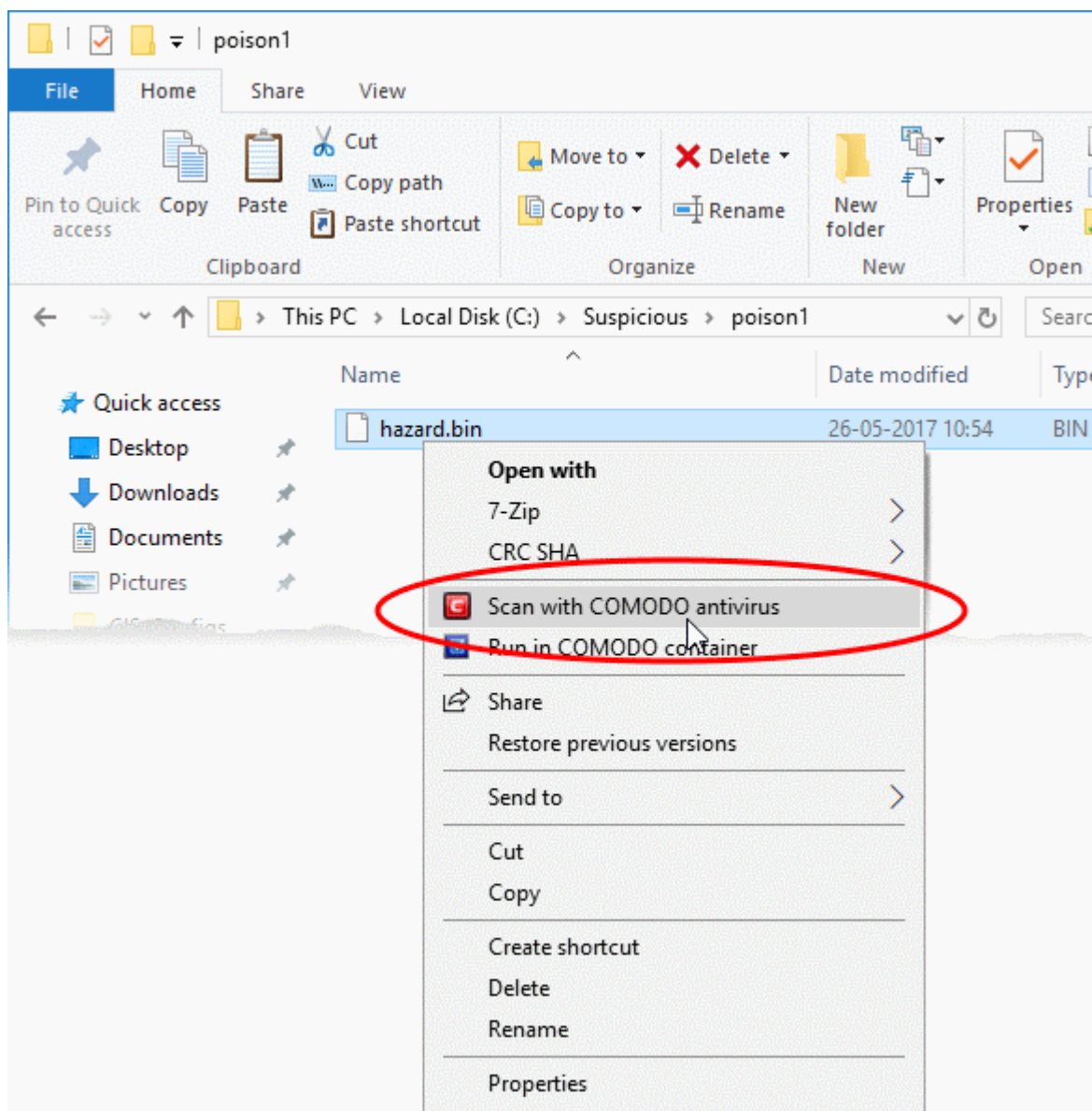
The item will be scanned immediately.
  • Any threats found are shown in the results at the end of the scan:
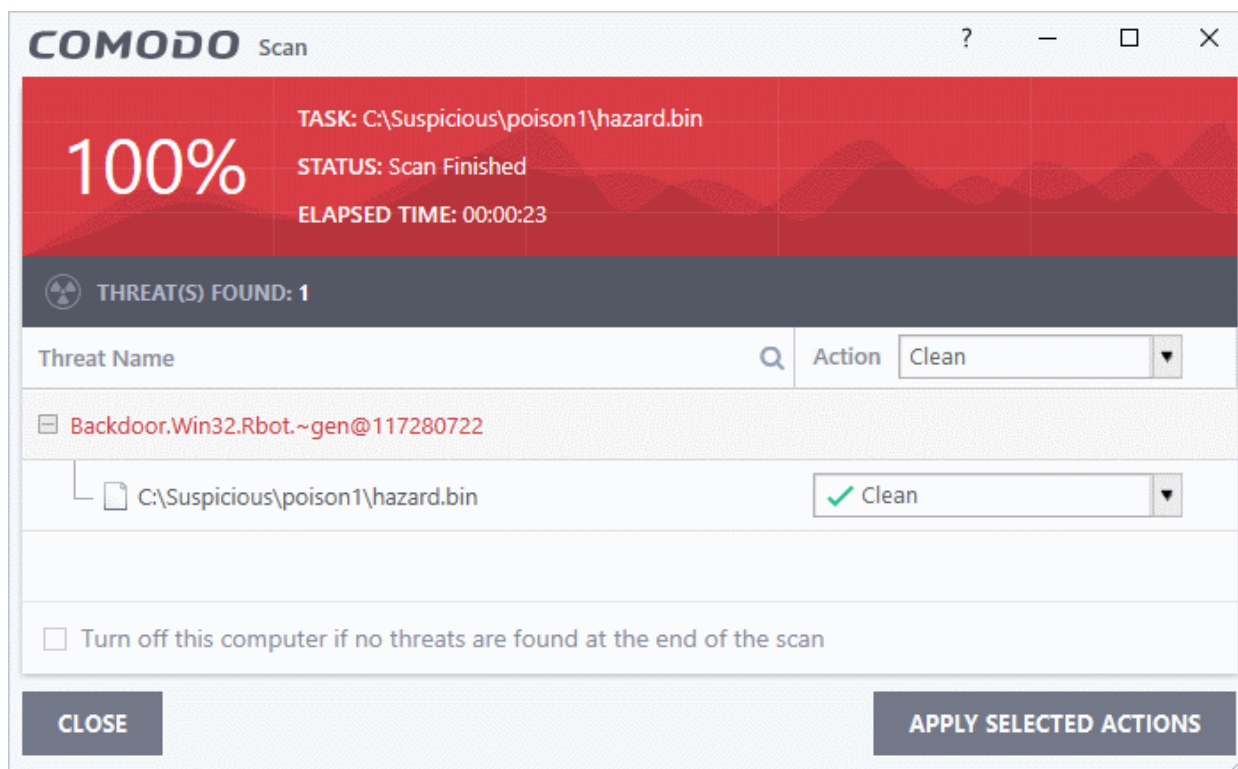
You can choose to clean, quarantine or ignore the threat. See **Process infected files** for more details.

Create an Antivirus Scan Schedule

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'More Scan Options'
- A custom scan profile lets you configure your own scan with your own scan settings.
- You can define exactly which files and folders to scan, what time they should be scanned, and configure scan settings.

Create a scan schedule

- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Custom Scan' then 'More Scan Options'

The 'Scans' page shows pre-defined and user created scan profiles. You can create and manage new profiles in this page:
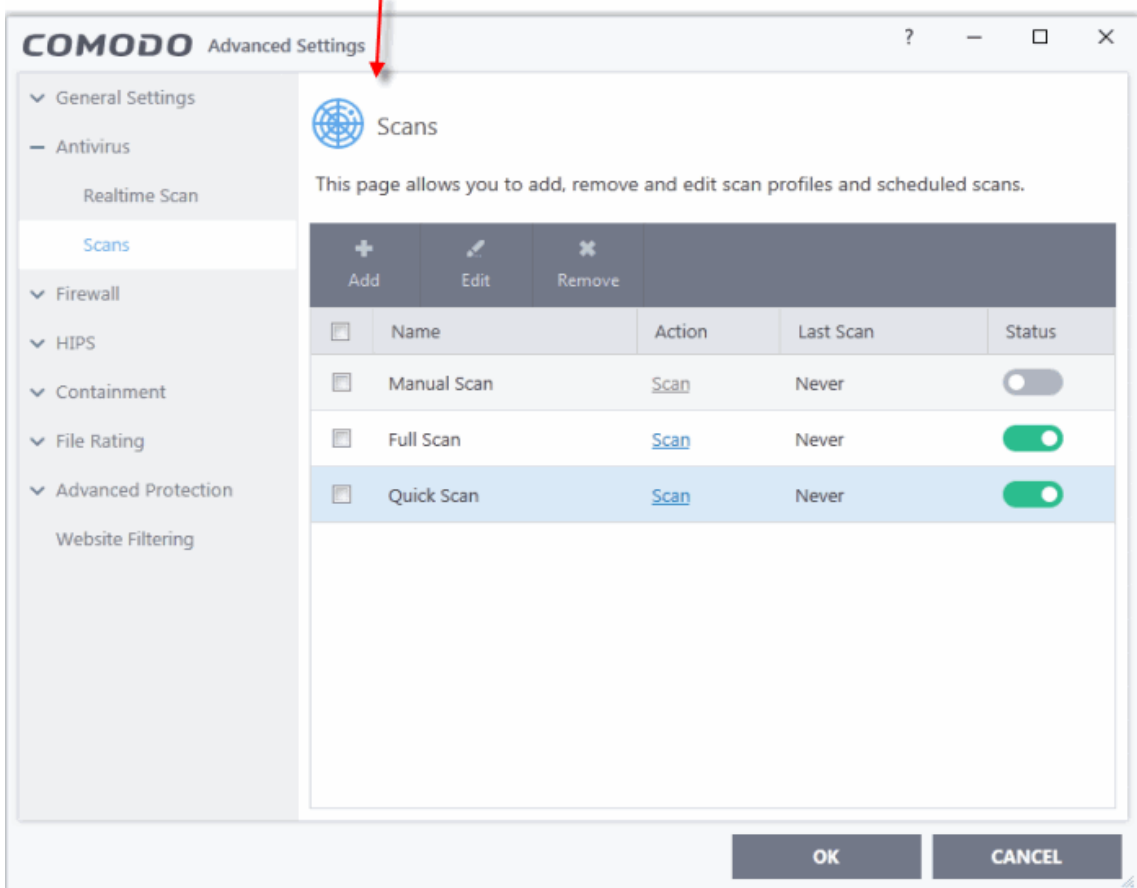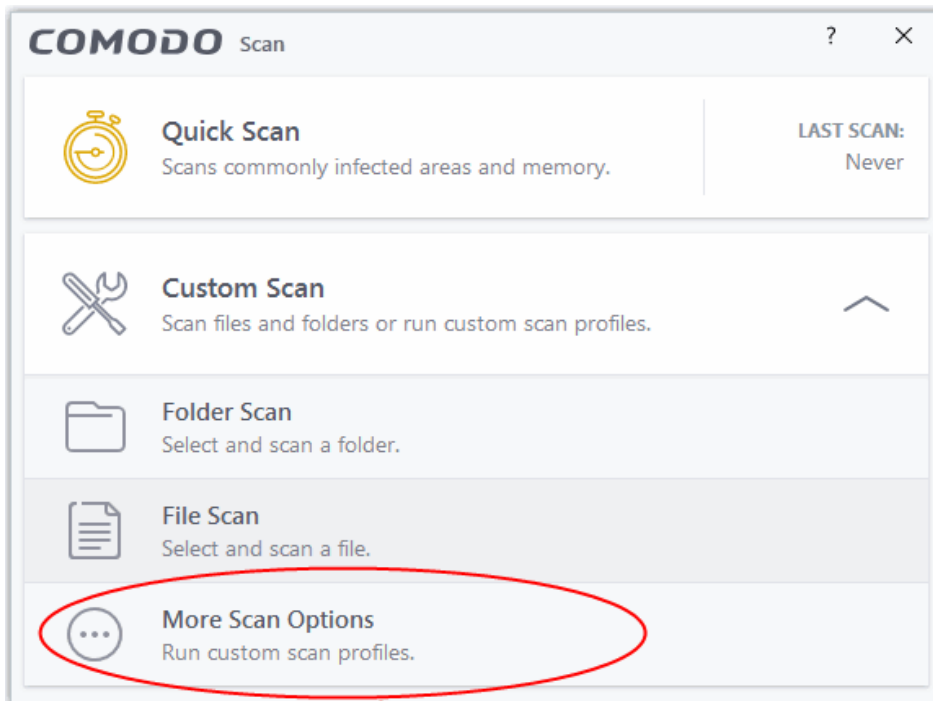
- Click 'Add' to create a new custom scan profile.
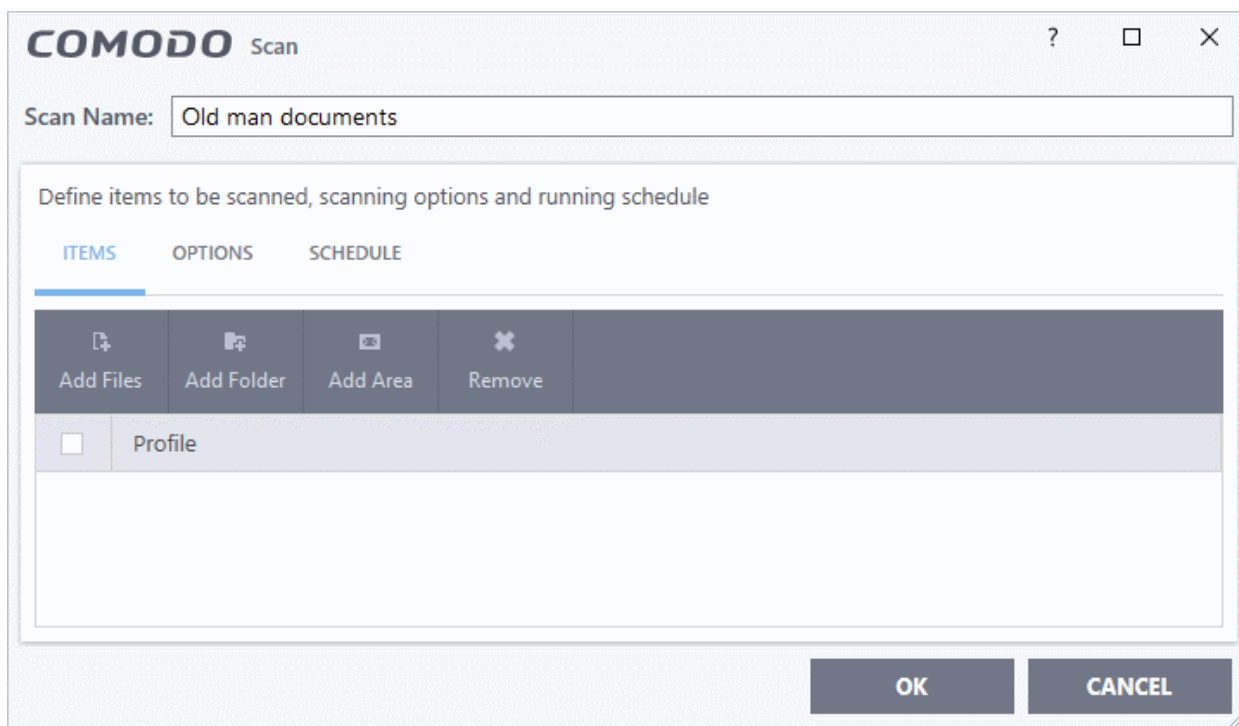
- First, create a name for the profile. The next steps are:
- **Select items to scan**
- **Configure scan options for the profile (optional)**
- **Configure a scan schedule (optional)**

Select the items to scan

- Click the 'Items' button at the top of the scan interface.

You can add items as follows:

- **Add File** - Add individual files to the profile. Click the 'Add Files' button and browse to the file you want to include.
- **Add Folder** - Add entire folders to the profile. Click the 'Add Folder' button and choose the folder you want to include. All files in the folder are covered by the scan.
- **Add Area** - Scan a specific region. The choices are 'Full Computer', 'Commonly Infected Areas', 'System Memory' and 'Trusted Root Certificate Store'. See screenshot below:

- Repeat the process to add more items to the profile. You can mix-and-match files, folders and areas in your custom scan.

Configure scan options

- Click the 'Options' button at the top of the scan interface

---

- **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 accuracy by augmenting the local scan with an online look-up of Comodo's latest virus database. This means CIS can detect the latest malware even if your virus database is out-dated. *(Default = Disabled)*.
- **Automatically clean threats** - Specify whether or not CIS should automatically remove any malware found by the scan.
    - **Disabled** =Results are shown at the end of the scan with a list of any identified threats. You can manually deal with each threat in the results screen. See **Process Infected Files** for guidance on manually handling detected threats. (*Default*)
    - **Enabled** = Threats are handled automatically. Choose the action that CIS should

automatically take:

- **Quarantine Threats** - Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See **Manage Quarantined Items** for more details.
- **Disinfect Threats** - If a disinfection routine exists, CIS will remove the virus and keep the original file. If not, the file will be quarantined

- **Show scan results window** - Show the number of objects scanned and the number of threats found at the end of the scan.

- **Use heuristics scanning** - Select whether or not heuristic techniques should be used in scans on this profile. You can also set the heuristic sensitivity level. *(Default = Enabled).*

  Background. Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This means CIS can detect brand new threats that are not even in the virus database.

  If enabled, please select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

  - **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts.

  Despite the name, this setting combines a very 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 possible false positives.
  - **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.

- **Limit maximum file size to** - Specify the largest file size that the antivirus should scan. CIS will not scan files bigger than the size specified here *(Default = 40 MB)*.

- **Run this scan with** - If enabled, you can set the priority of scans on this profile The available options are:
  - High
  - Normal
  - Low
  - Background. (*Default*)

- **Update virus database before running** - CIS checks for and downloads the latest virus signatures before starting a scan *(Default = Enabled)*.

- **Detect potentially unwanted applications** - The antivirus also scans 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 installing another 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)*.

- **Apply this action to suspicious autorun processes** - Specify how CIS should handle unrecognized auto-run items, Windows services, and scheduled tasks.
  - **Ignore** - The item is allowed to run (*Default*)
  - **Terminate** - CIS stops the process / service
  - **Terminate and Disable** - Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.
  - **Quarantine and Disable** - Auto-run processes are quarantined and the corresponding auto-run entry removed. In the case of a service, CIS disables the service.

  Note 1 - This setting only protects the registry during the on-demand scan itself. To monitor the registry at all times, go to 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'.

  - See **Miscellaneous Settings** for more details

  Note 2 - CIS runs script analysis on certain applications to protect their registry records. You can

---

manage these applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

- See '**Autorun Scans**' in **Script Analysis Settings** for more details.

Configure a scan schedule

- Click the 'Schedule' button at the top of the scan interface:

Schedule options are:

- **Do not schedule this task** - The scan profile is created but not run automatically. The profile will be available for manual, on-demand scans.
- **Every few hours** - Run the scan at the frequency set in 'Repeat scan every NN hour(s)'
- **Every Day** - Run the scan every day at the time specified in the 'Start Time' field.
- **Every Week** - Run the scan on the days 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 dates 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 is useful when you are using a laptop or any other mobile device.
- **Run only when computer is IDLE** - The scan will run only if the computer is in an 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.

Run Untrusted Programs in the Container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'
    - Choose the program you want to run
    - Click 'Open'
- CIS lets you run programs inside the container on a 'one-off' basis.
- This is helpful to test new/beta programs you have downloaded but are not yet sure you trust.
- You can also create a desktop shortcut to run the application inside the container on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:
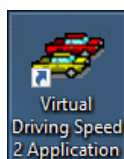
Use any of the following methods to run a program in the container:

- **Right-click menu**
- **From the 'Containment Tasks' area**

- • **From the widget (browsers only)**

Right-click menu

1. 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:
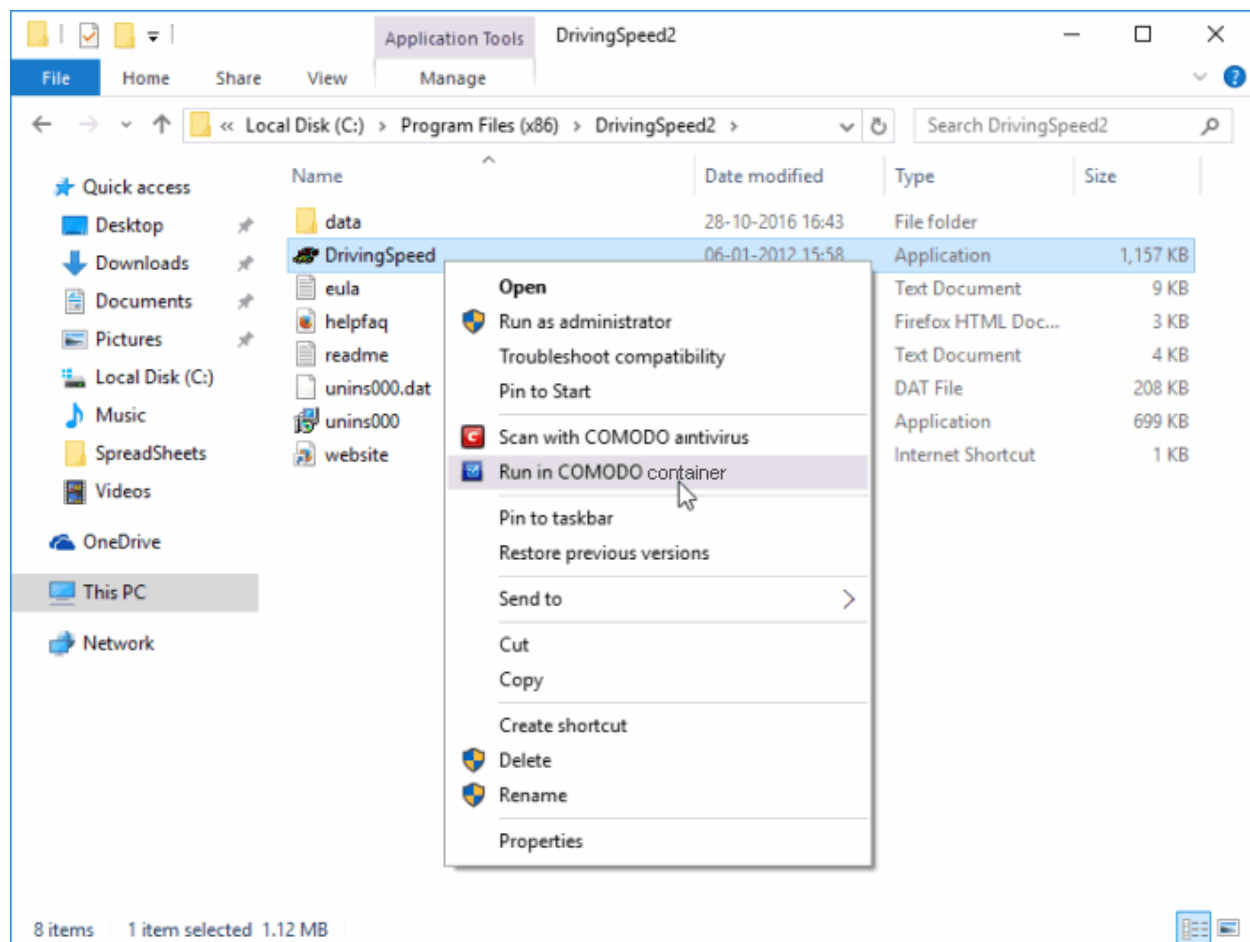
The 'Containment Tasks' interface

- • Click 'Tasks' > 'Containment Tasks'

- • Click the 'Run Virtual' tile
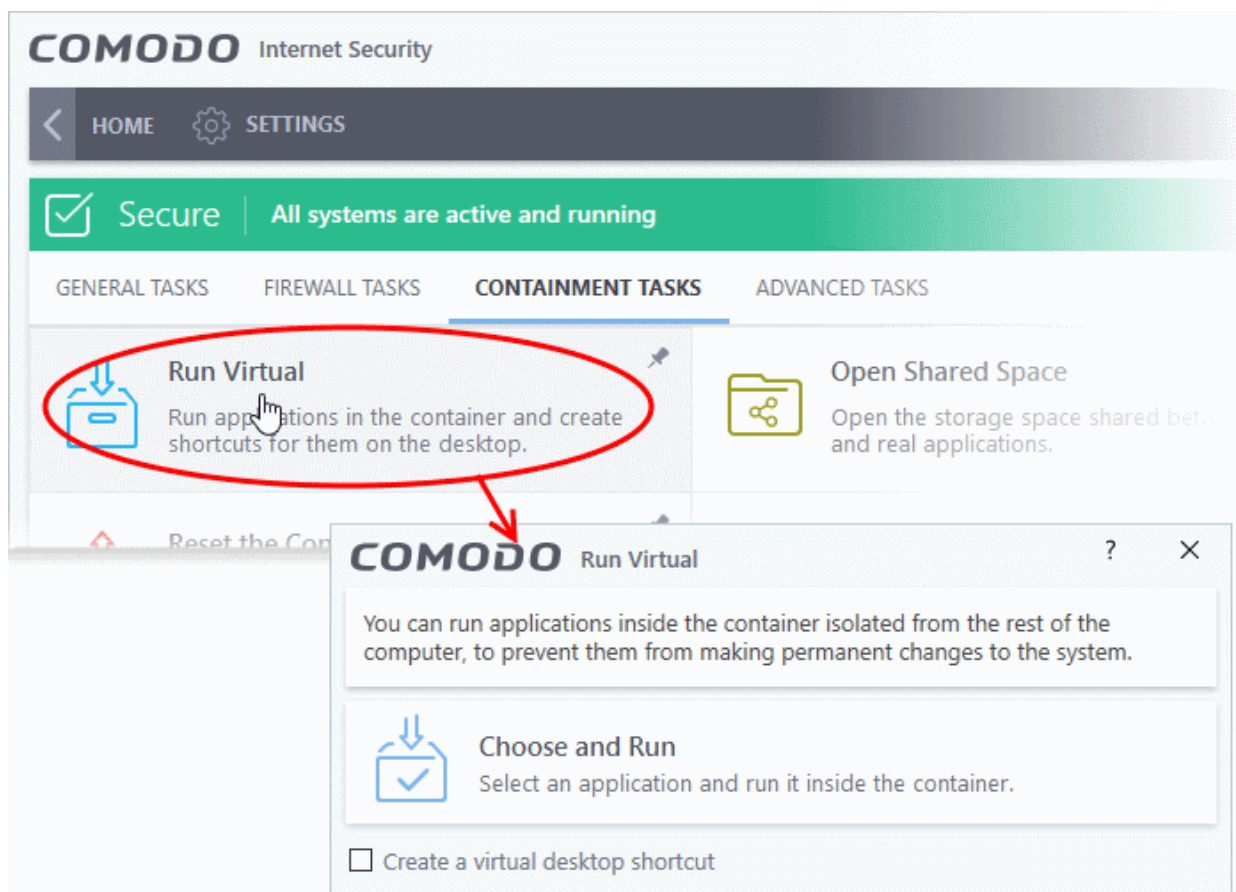
- Click 'Choose and Run', browse to your application then click 'Open'.
- The contained application will have a green border around it. Enable 'Create a virtual desktop shortcut' if you plan to run the application in the container in future.
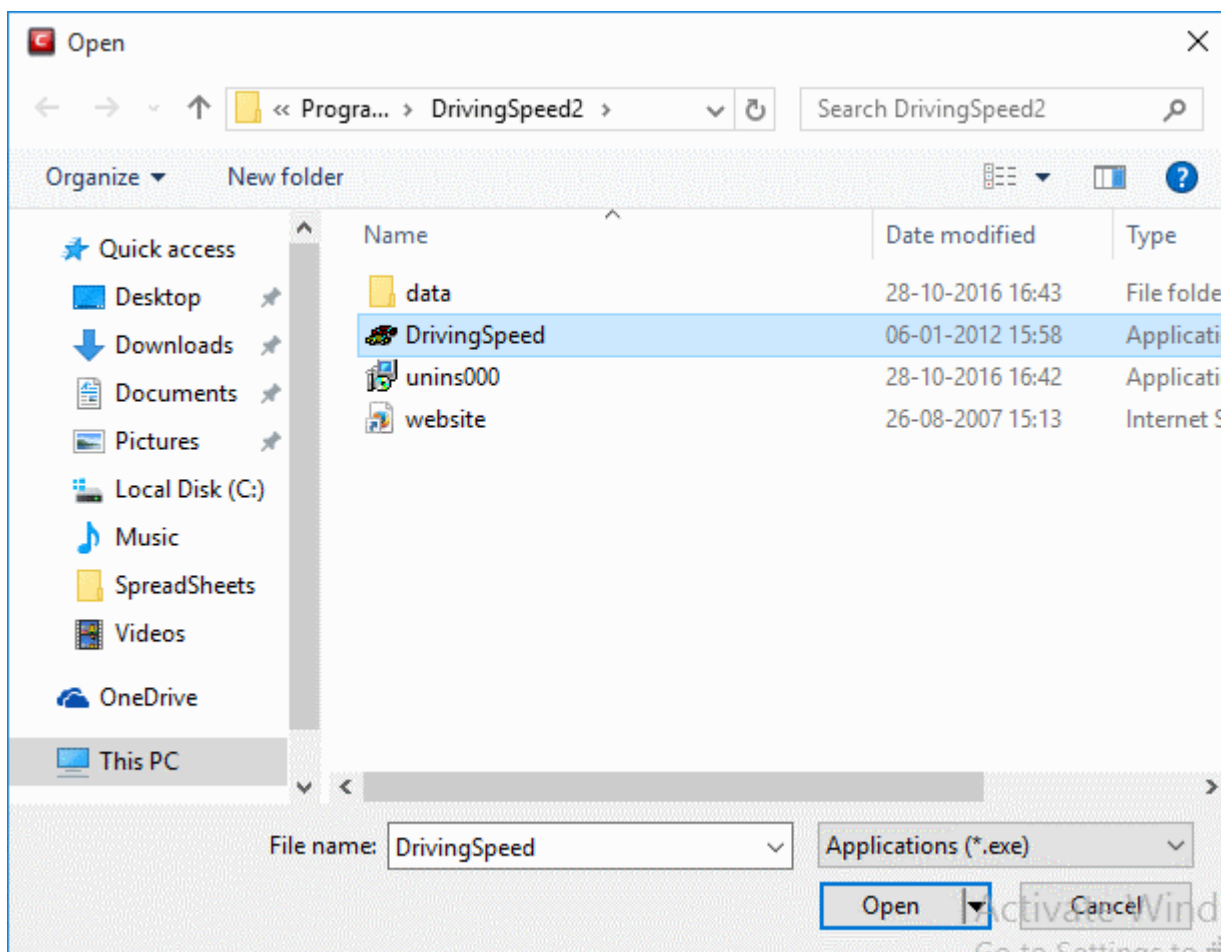
Run browsers in the container

The CIS widget contains shortcuts to run your browsers in the container:
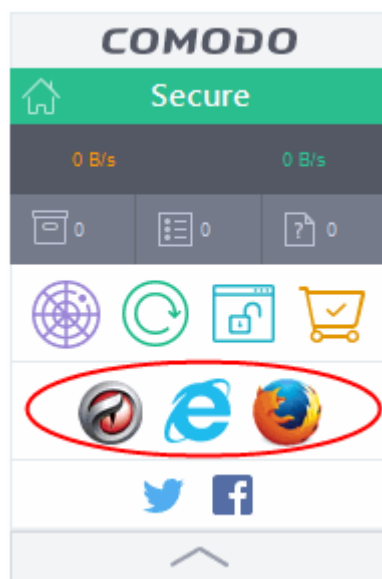
- The green border indicates that the browser is in the container:
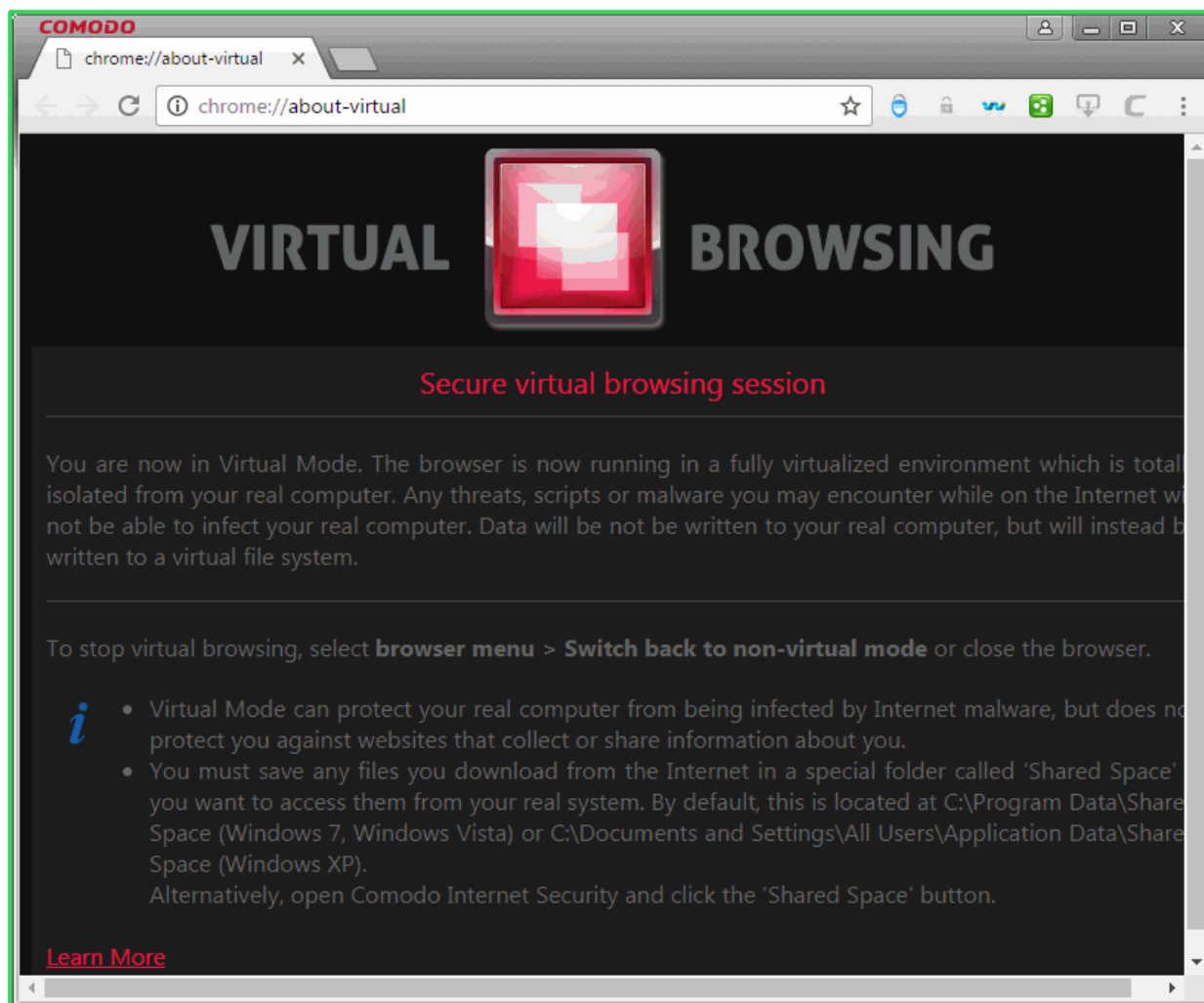
Run Browsers in the Container

- 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

The CIS widget contains shortcuts to run your browsers in the container:
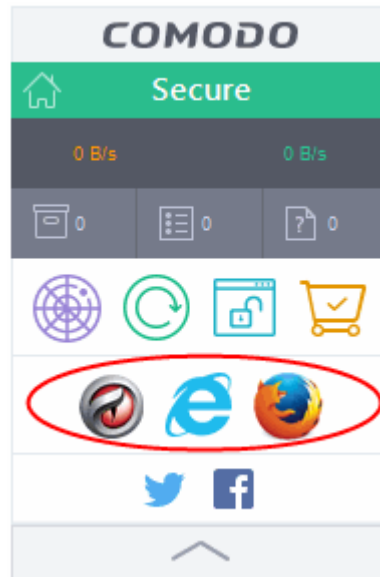
Start a browser from the 'Containment Tasks' interface

- Click 'Tasks' > 'Containment Tasks'
- Click 'Run Virtual':
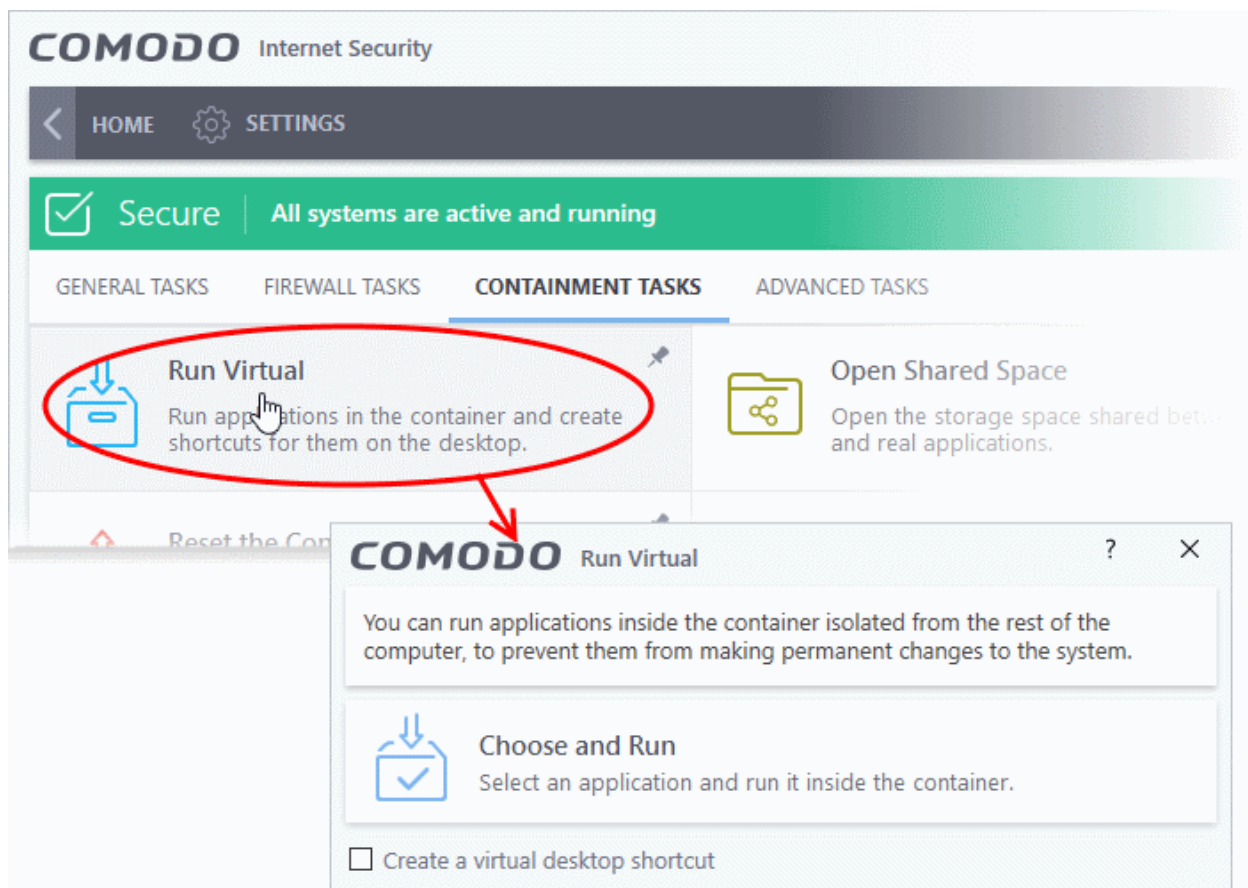
- Click 'Choose and Run' then navigate to the install location of the browser. Select the .exe file of the browser.
- Select 'Create a virtual desktop shortcut' to quickly run the application in the container in future.

The browser will run with a green border around it, indicating that it is contained:
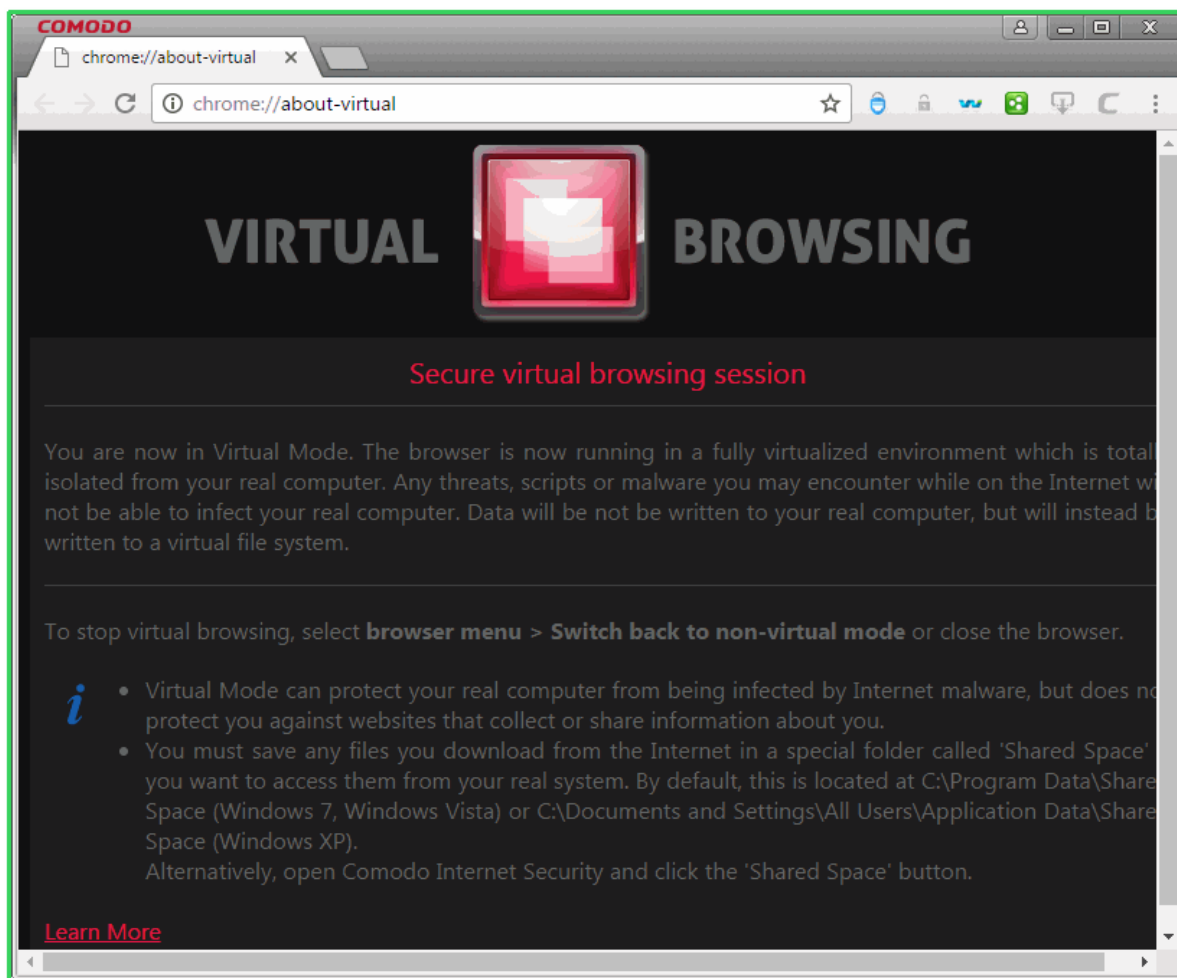
Run Untrusted Programs in the Virtual Desktop

This page explains how to run untrusted programs inside the virtual desktop. Applications in the virtual desktop cannot make changes to your real system, making it ideal for testing out beta/unstable software.

There are two ways to open programs in the virtual desktop:

- **Open applications/files from desktop shortcuts**
- **Use the 'Shared Space' folder to access applications/files**

Desktop Shortcuts

- You can create program or file shortcuts on the desktop of your real system.
- The shortcuts on your real desktop are also available in the virtual desktop.
- Double-click them to open them in the virtual desktop.

Note: You must use **Classic Windows Mode** or **Tablet + Classic Mode** to view the icons/shortcuts on your real desktop.

Shared Space

- The virtual desktop creates a folder called 'Shared Space' at C:\Program Data\Shared Space.

- This folder can be accessed from both your host operating system and the virtual desktop. You can use this folder to move files between the two systems.

- You can open shared space as follows:

   - Click 'Tasks' > 'Containment' > 'Open Shared Space'

     OR

   - Click the 'Shared Space' shortcut on the CIS widget

Open an application or file from your host system in the virtual desktop

1. Open the 'Shared Space' folder as mentioned above
2. Copy / move the application or the file into the shared space
3. 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'
4. Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop' to start the virtual desktop
5. Click the 'Shared Space' shortcut icon in the home screen of the virtual desktop.

> **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

This page explains how to restore an item that you feel CIS has incorrectly blocked (a false positive). A file may be blocked by the antivirus, containment, firewall or HIPS components.

- Click 'Unblock Applications' in the 'Basic' view of the CIS home screen:

OR
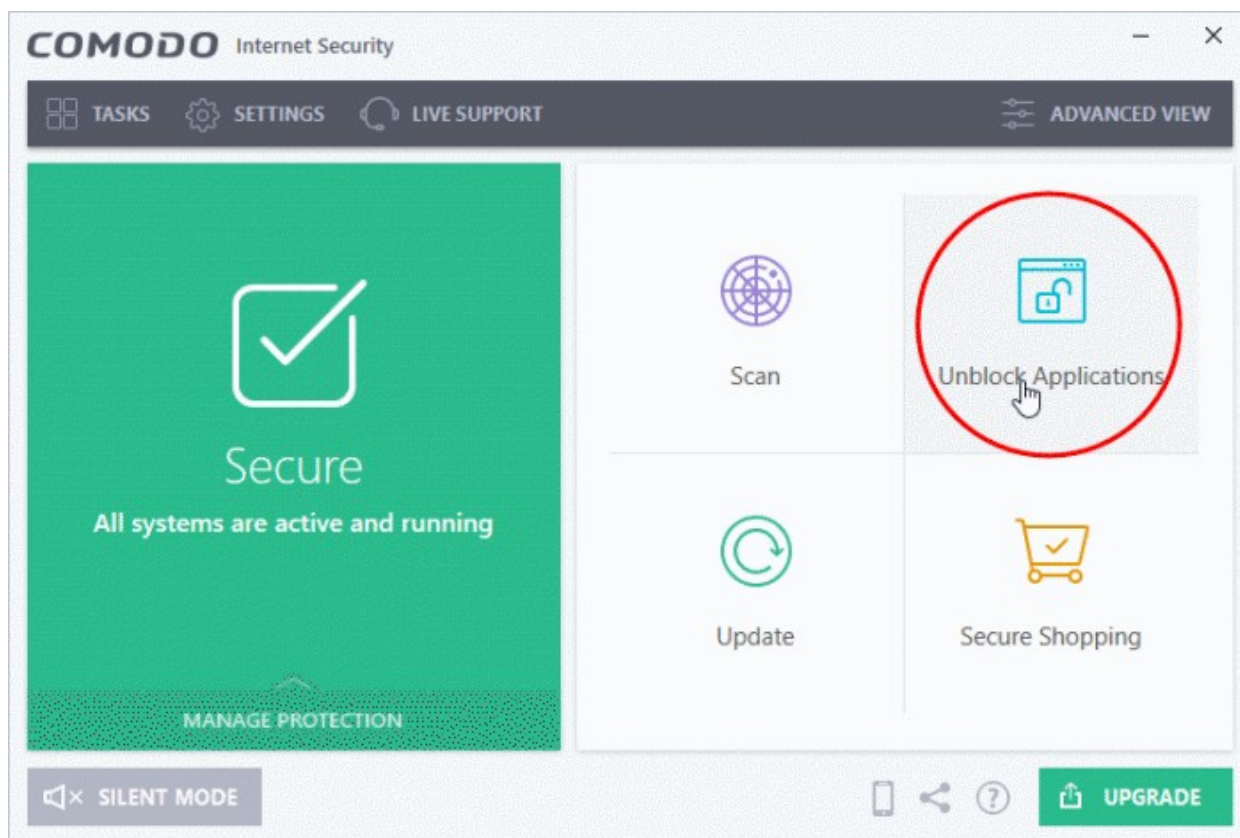
- Click the 'Unblock Applications' icon on the CIS Widget:
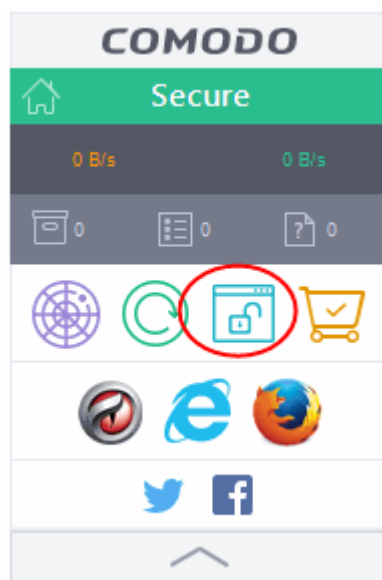
OR

- Click 'Tasks' at the top-left of the home screen then 'General Tasks' > 'Unblock Applications'
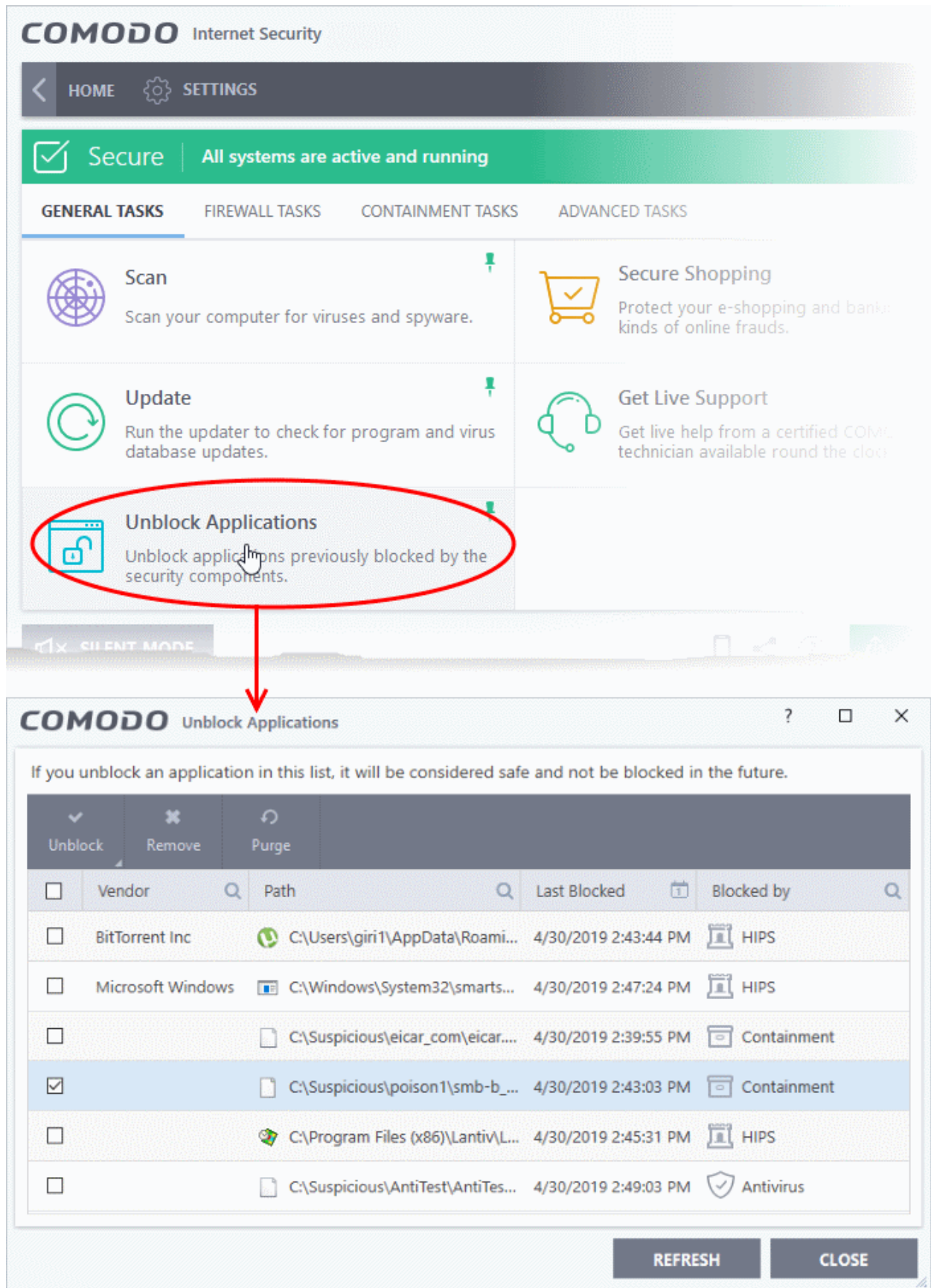
This open a list of files that were blocked by different components of CIS.

- Select the application that you consider safe, click 'Unblock' and choose an unblock option:

OR

- Right-click on an item, select 'Unblock' and choose an unblock option:
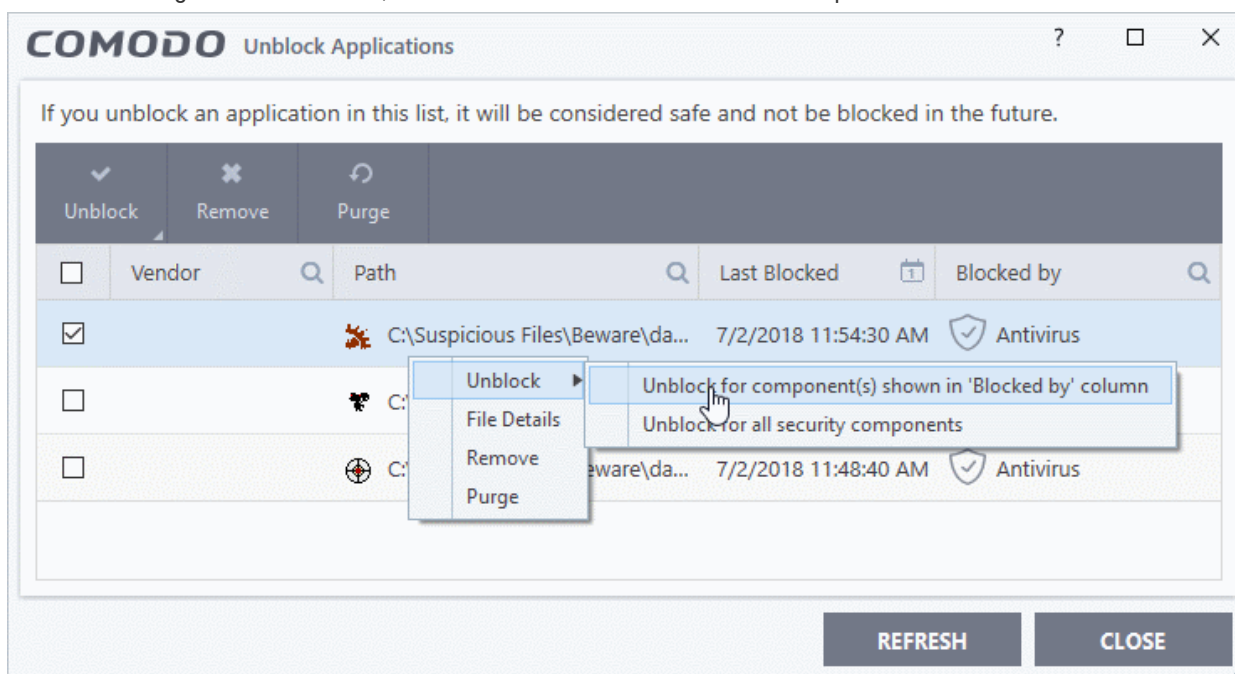
- **Unblock for component(s) shown in 'Blocked by' column** - Item will only be released from the security component that blocked it.
- **Unblock for all security components** - Item will be released from all security components

Restore Incorrectly Quarantined Items

This page explains how to restore an item from quarantine. You may want to do this if

- You think CIS has incorrectly classed it as malicious (a false positive)
- It was manually moved to quarantine by mistake

Restore an item from quarantine

- Click 'Tasks' > 'Advanced Tasks'
- Click 'View Quarantine'
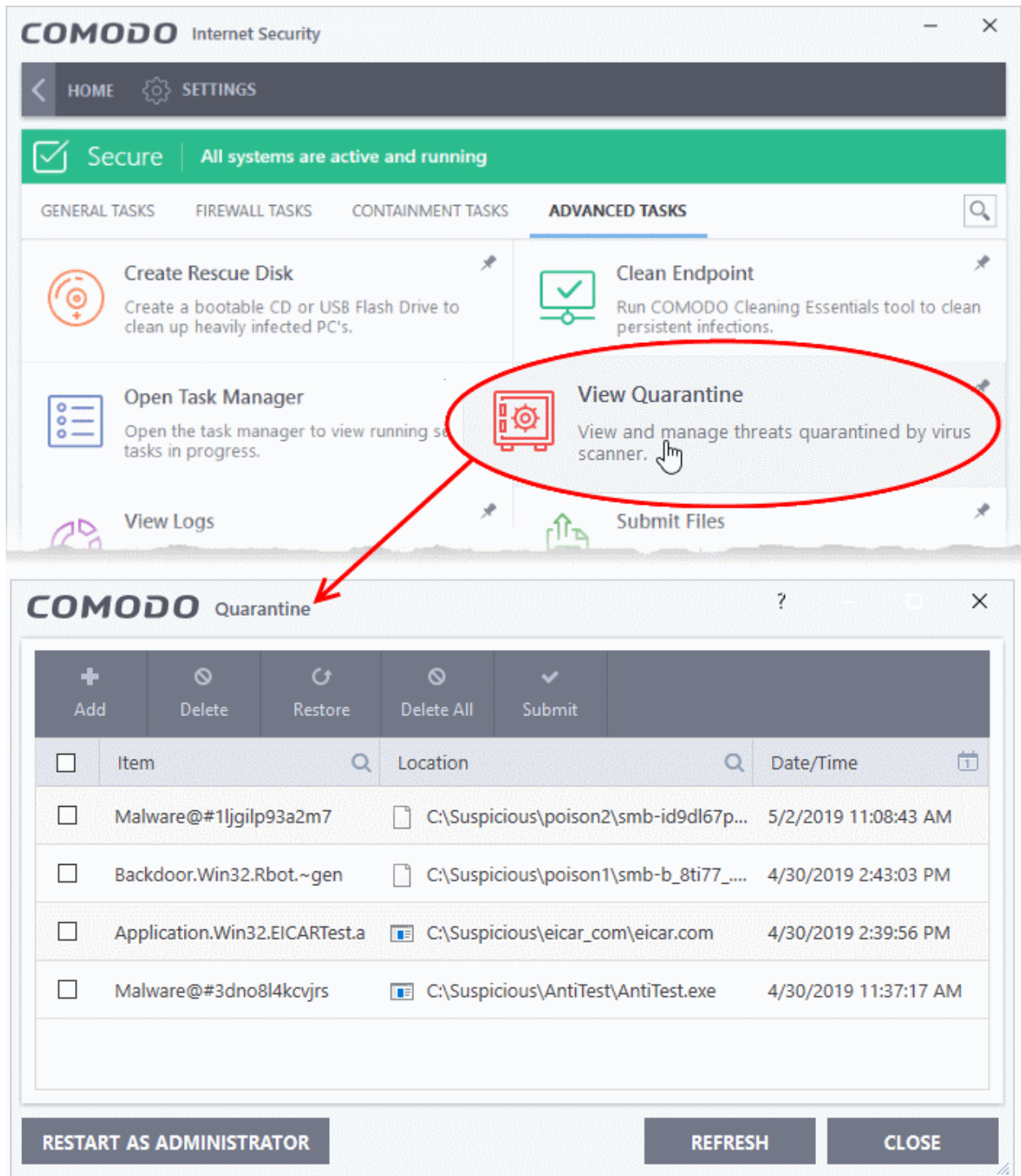
Important Note:

CIS requires admin privileges to restore quarantined items to their original locations. Follow this process if you are logged in as a regular user:

- Click 'Restart as Administrator' as shown below:
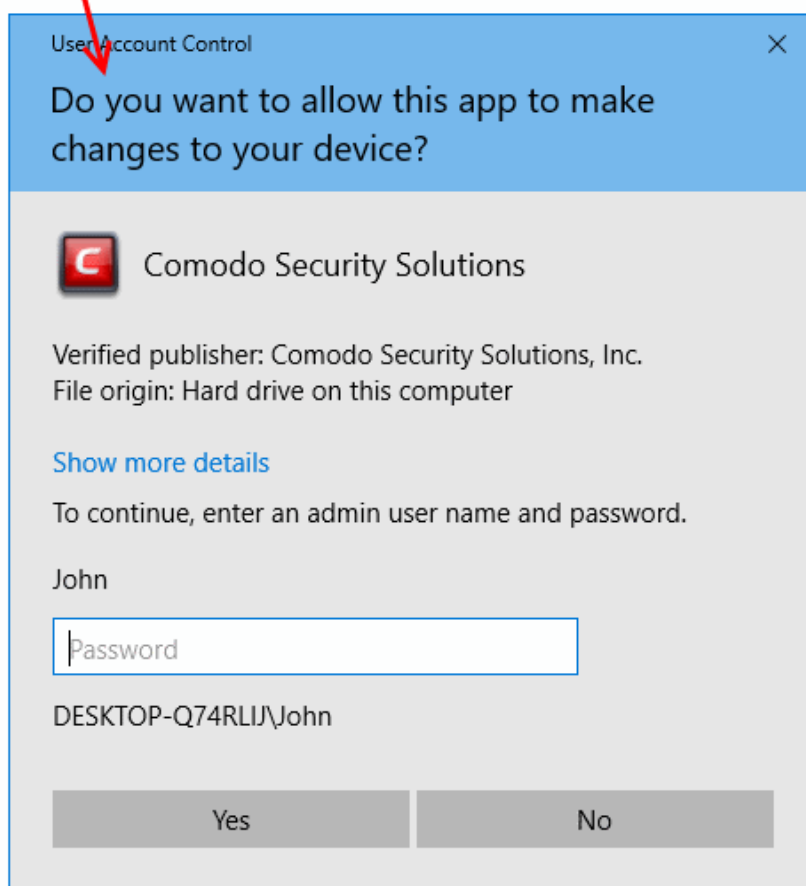
- Select an admin account, enter its password and click 'Yes'.

The quarantine interface will re-open and you can now restore the selected items to their original locations.

- 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:
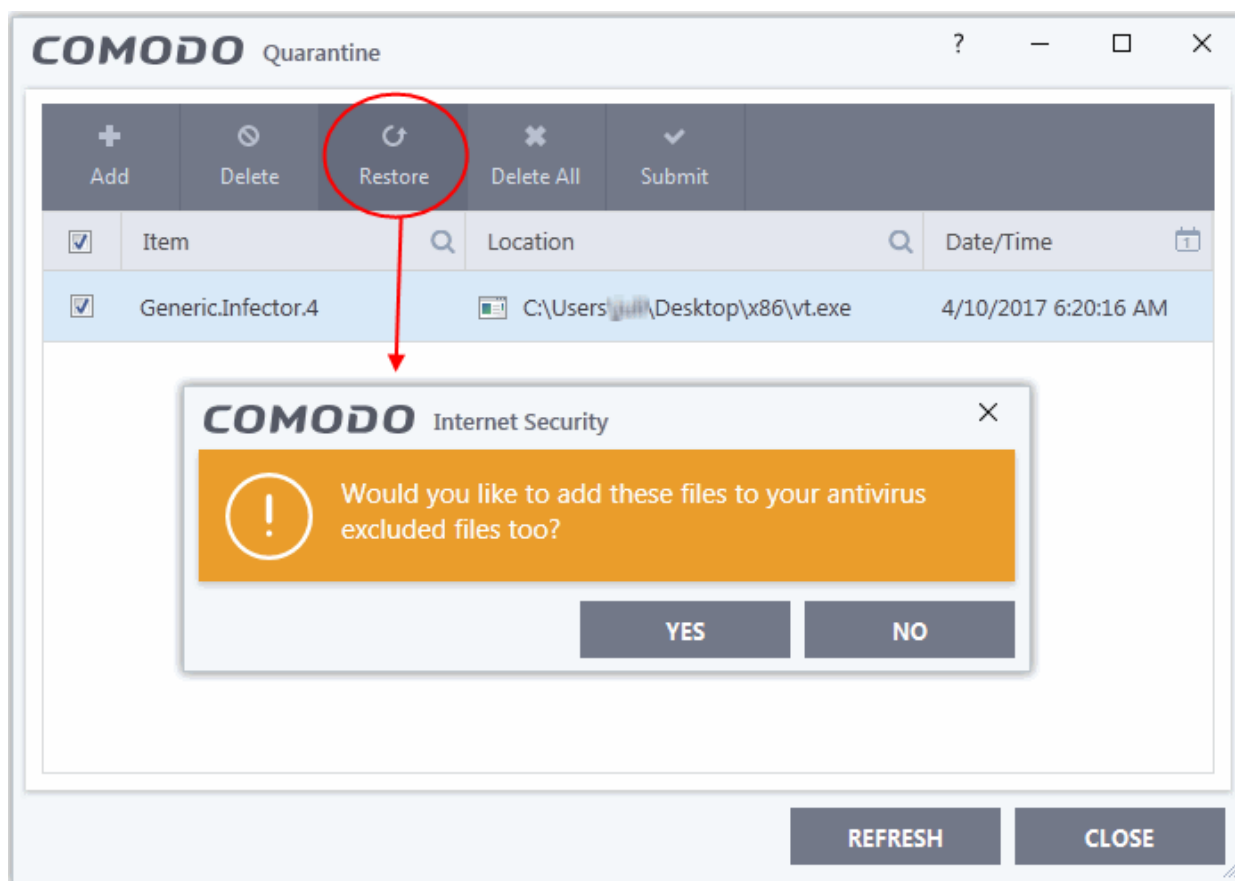
- 'Yes' - The items will be restored to their original locations and added to the antivirus exclusion list. The restored files will be skipped in future AV scans.
- 'No' - The items will be restored to their original locations but may still be flagged by future AC scans.
- Click 'Close' to exit.

See **Manage Quarantined Items** and **Submit Quarantined Items to Comodo for Analysis** for more information on this topic.

Submit Quarantined Items to Comodo for Analysis

You can send quarantined items to Comodo for analysis. You may want to do this if you think the item is a false positive - it was incorrectly flagged as malicious by CIS.

Submit a quarantined item for analysis by Comodo

1. Click 'Tasks' > 'Advanced Tasks'
2. Click 'View Quarantine'
3. Select the items you want to send and click the submit button

The submission progress will start:
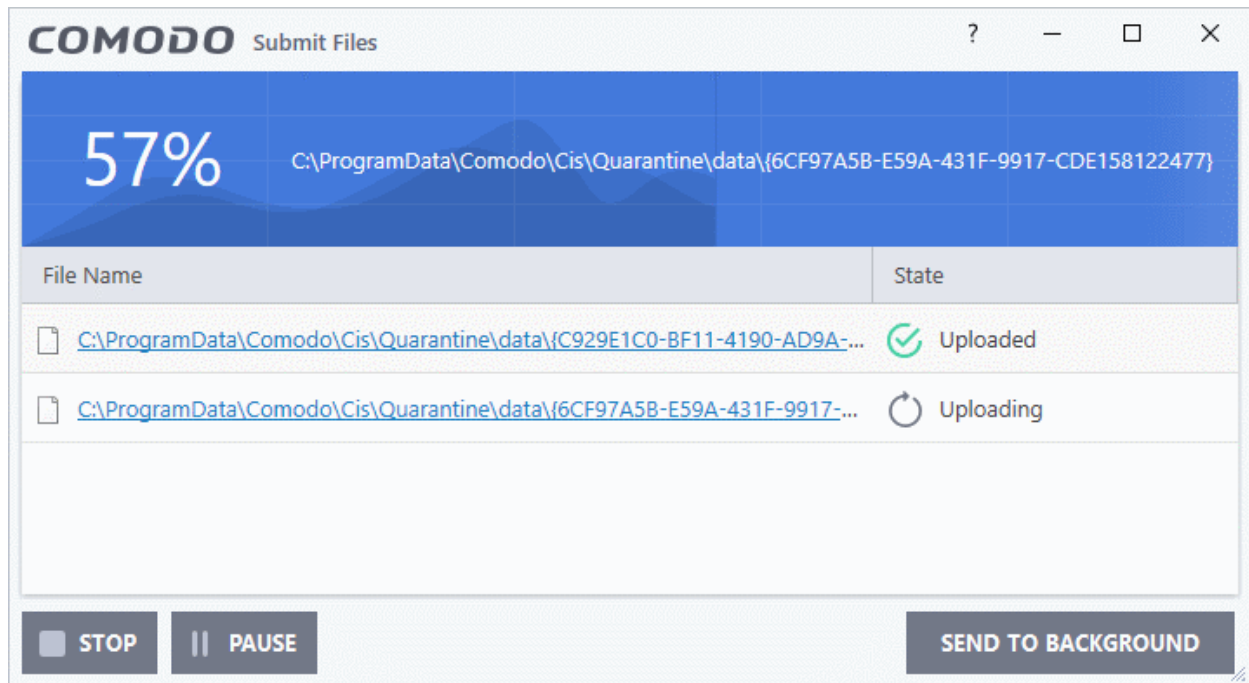
The results state whether the file was successfully submitted, or whether it has already been submitted by other users and is pending analysis.

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 malware 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 lets you securely enter usernames/passwords without fear of key-loggers recording what you type.

Start the Virtual Desktop

1. Click 'Tasks' > 'Containment Tasks'
2. Click 'Run Virtual Desktop'

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
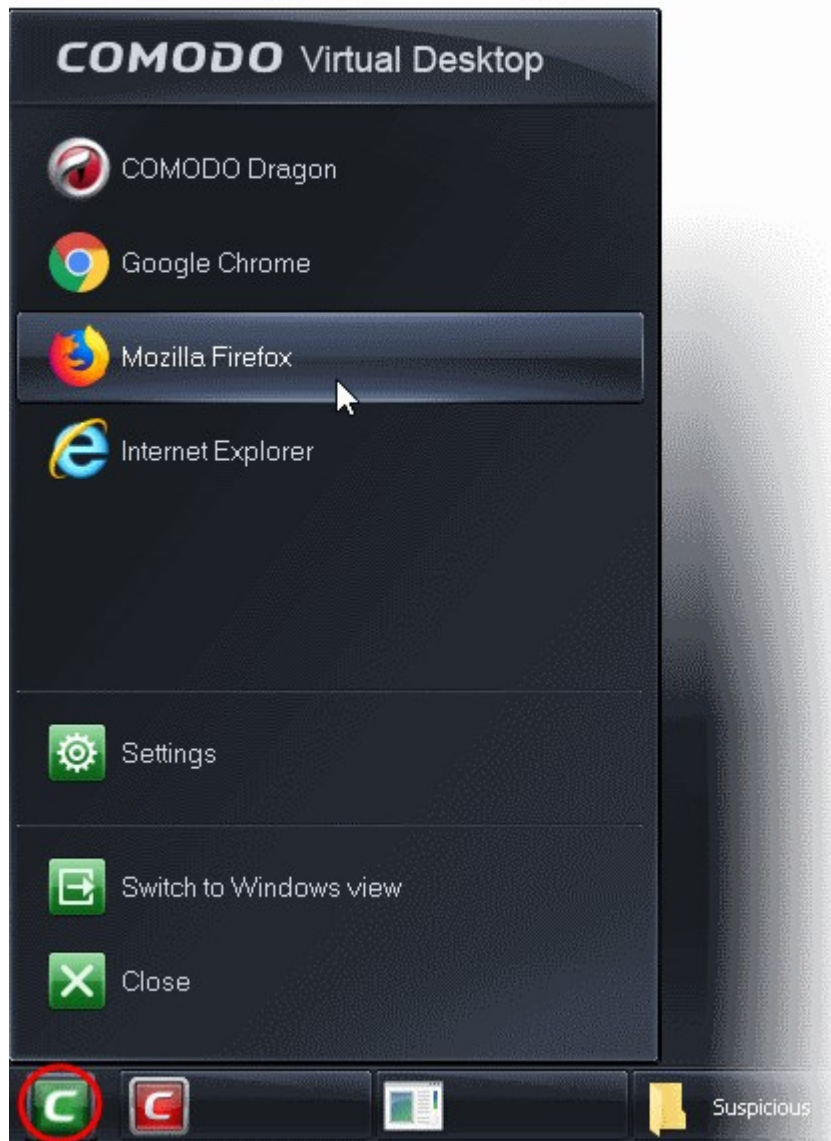
Your choice of browser will open inside the virtual desktop, ready for secure surfing:
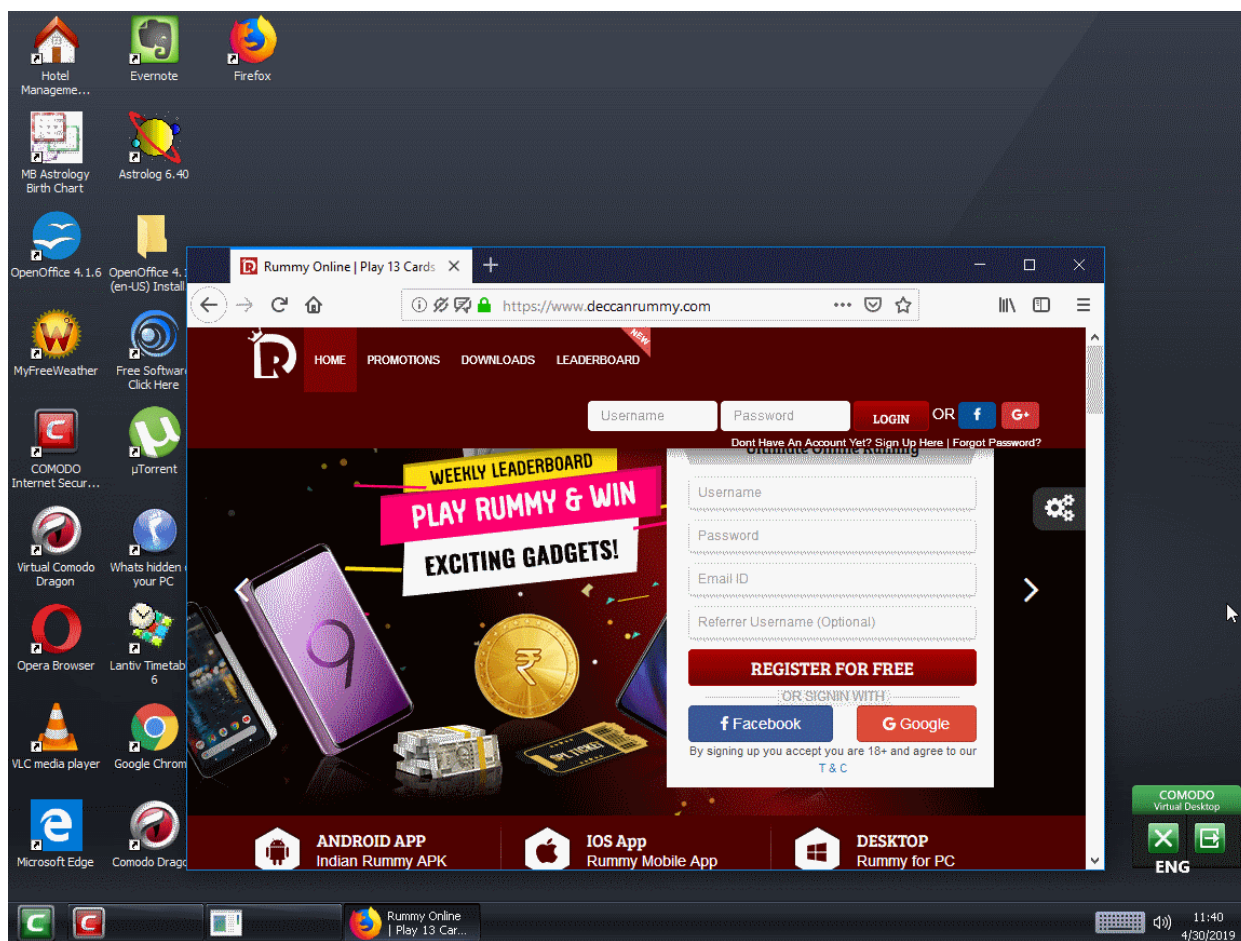
- Browsing history and other records of your internet activity will not be stored on your computer when your session is closed.

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**

Disable 'Do Protocol analysis'

1. Click 'Settings' on the CIS home screen
2. Click 'Firewall' > 'Firewall Settings'
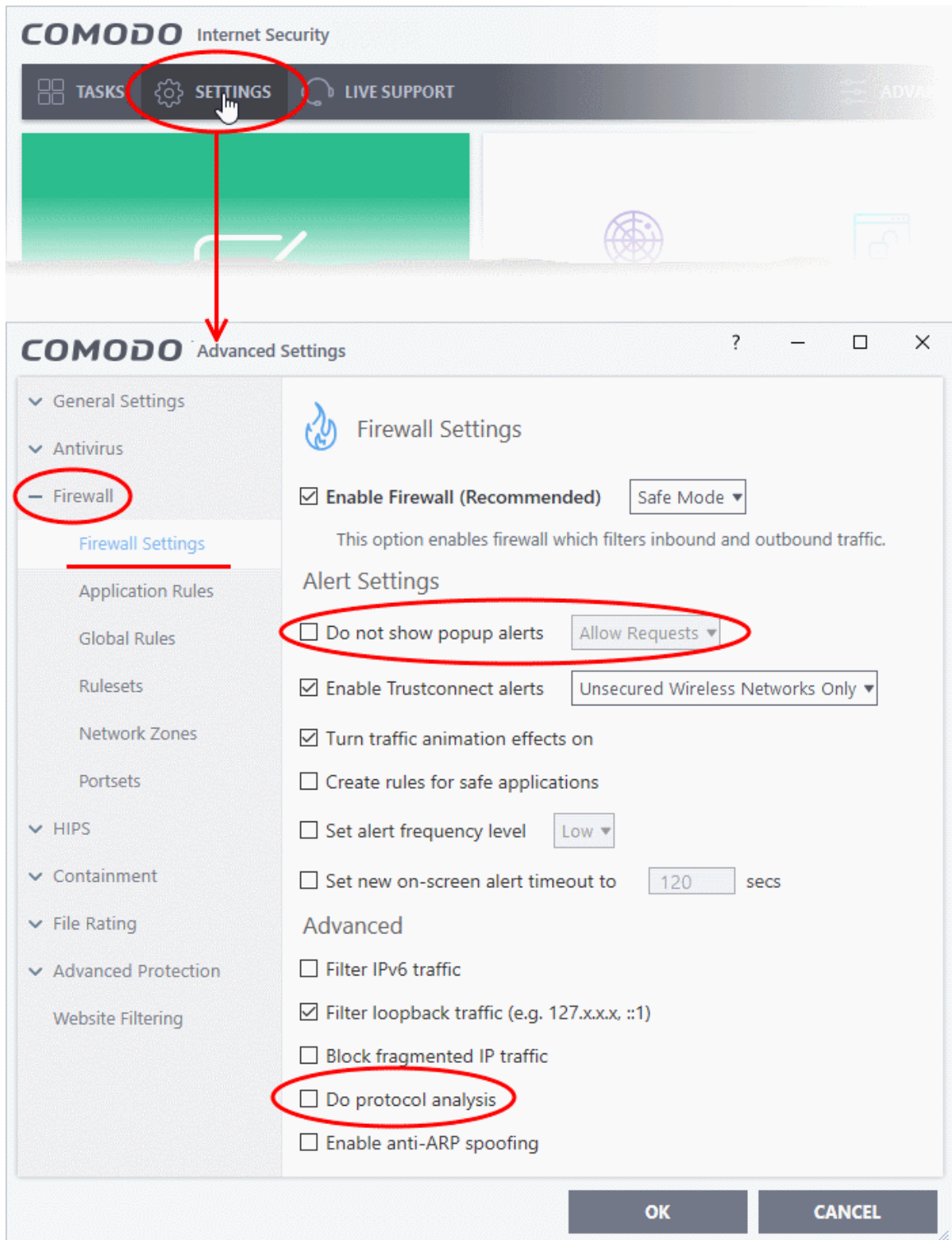
3. Disable 'Do not show popup alerts' so CIS will generate alerts when you open Shareaza or Emule.

4. Disable 'Do Protocol Analysis'

5. Click 'OK' to save your settings.

Create a 'Predefined Firewall Ruleset' for Shareaza/Emule

1. Click 'Settings' on the CIS home screen

2. Click 'Firewall' > 'Rulesets'

3.   Click 'Add' from the options at the top.

The 'Firewall Ruleset' interface will open:
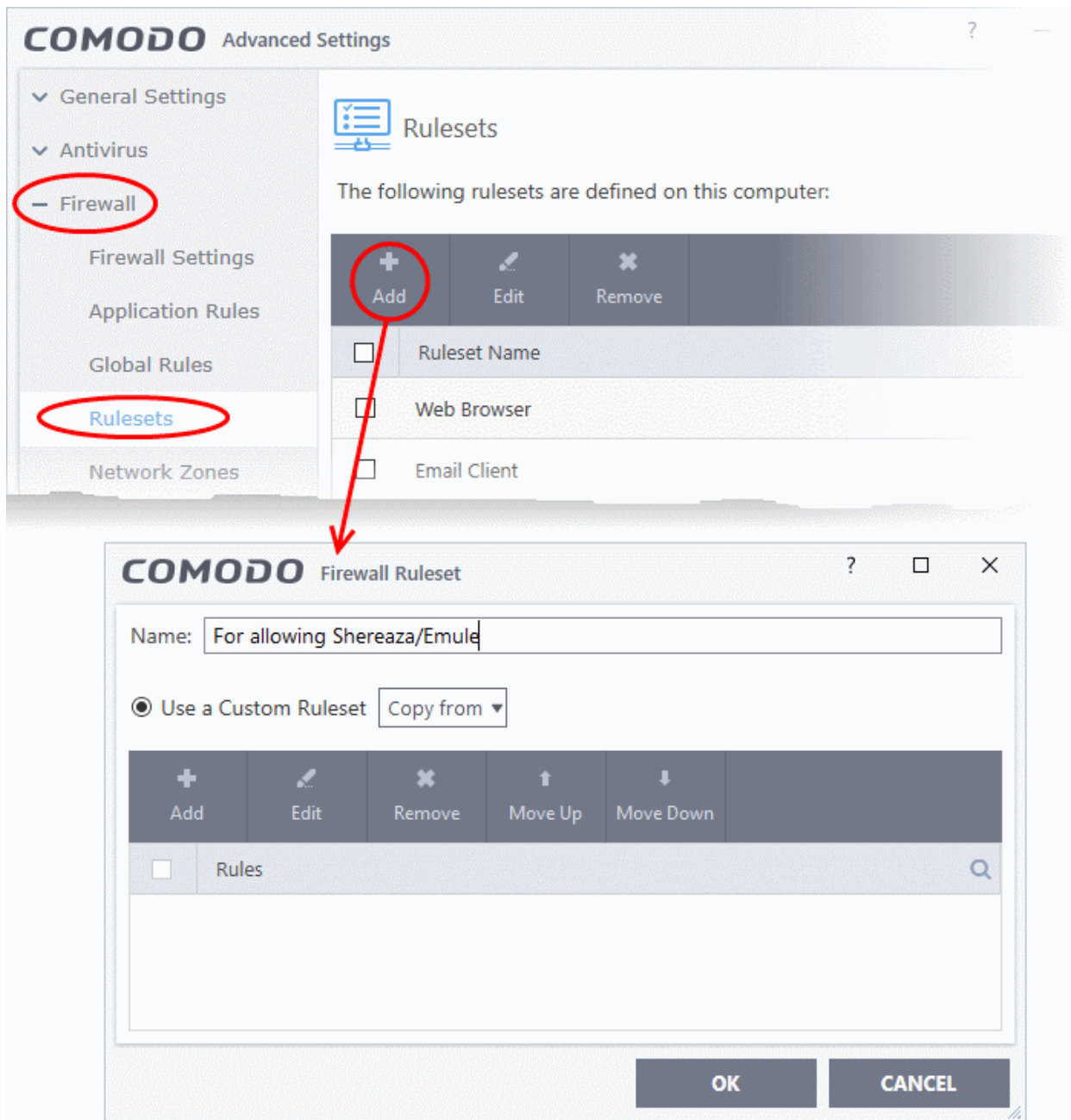
4.   Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing Shareaza/Emule'.

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
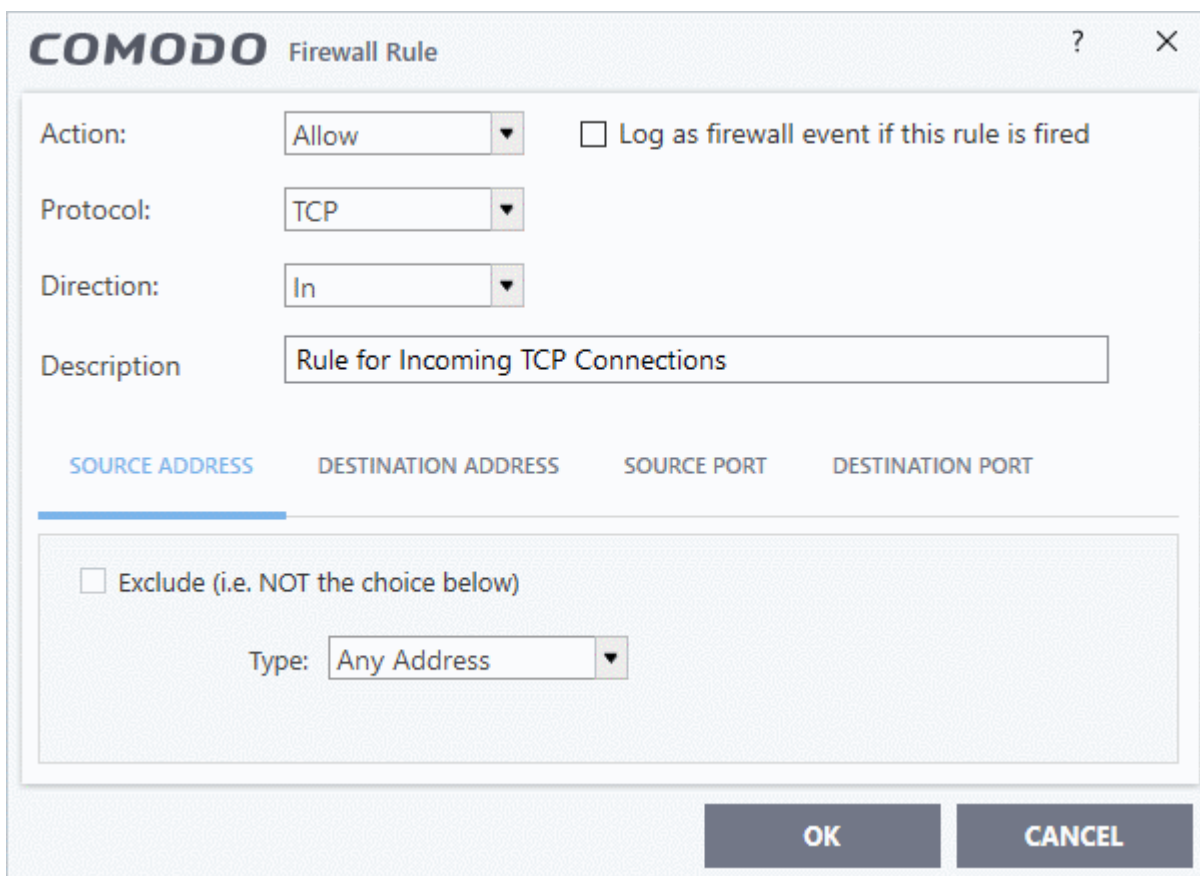
Rule 1

- 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'.

Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Settings' on the CIS home screen

2. Click 'Firewall' > 'Rulesets'

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

This page explains how to configure CIS to prohibit downloads of specific types of file.

Example scenarios:

- • Some malicious websites try to push malware in .exe file format. These files, known as executables, can run 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 also 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' on the CIS home screen

2. Click 'HIPS' > 'Protected Objects'

3. Click the 'Blocked Files' tab
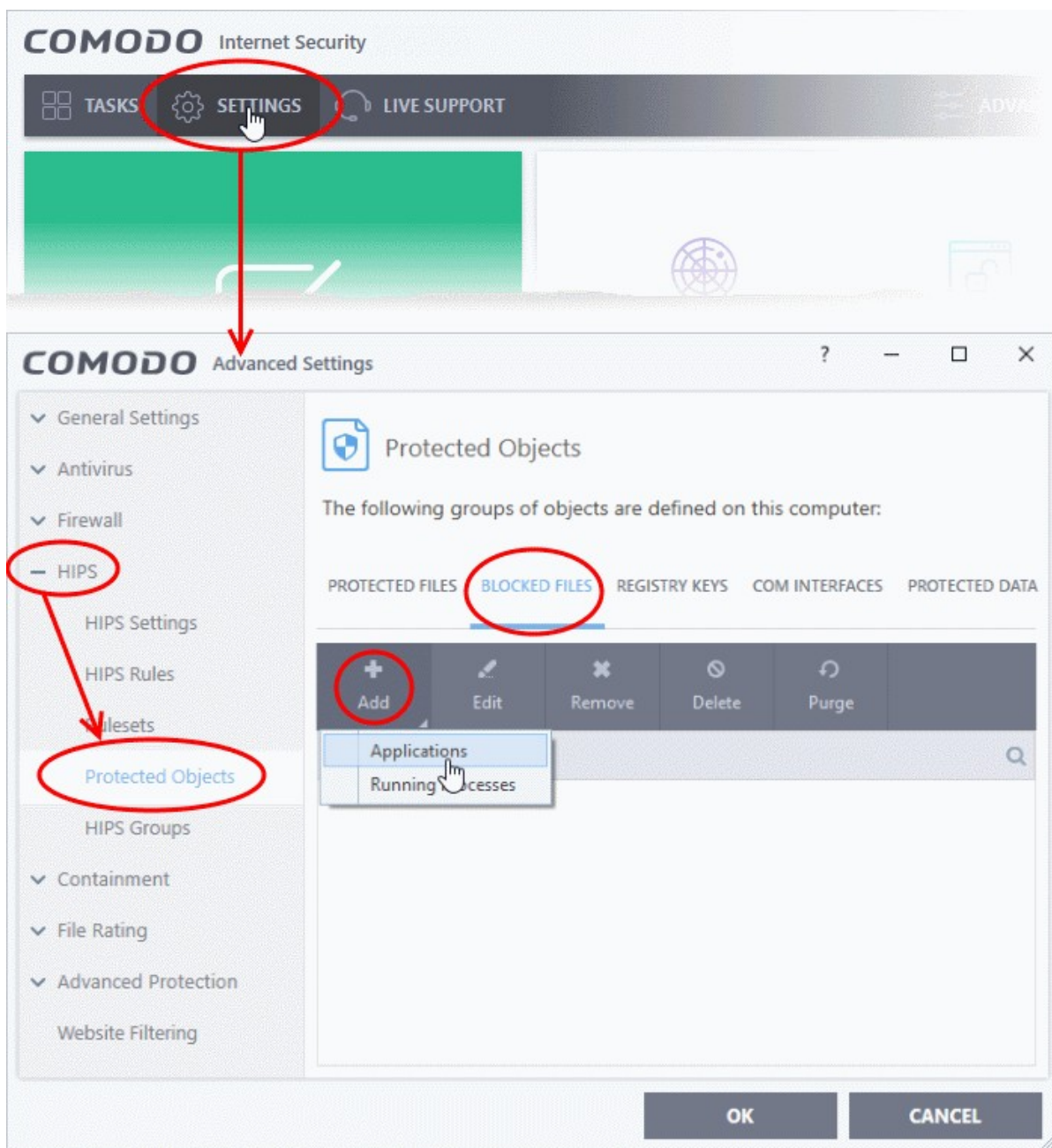
4. Click 'Add' > 'Applications'.

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.

---
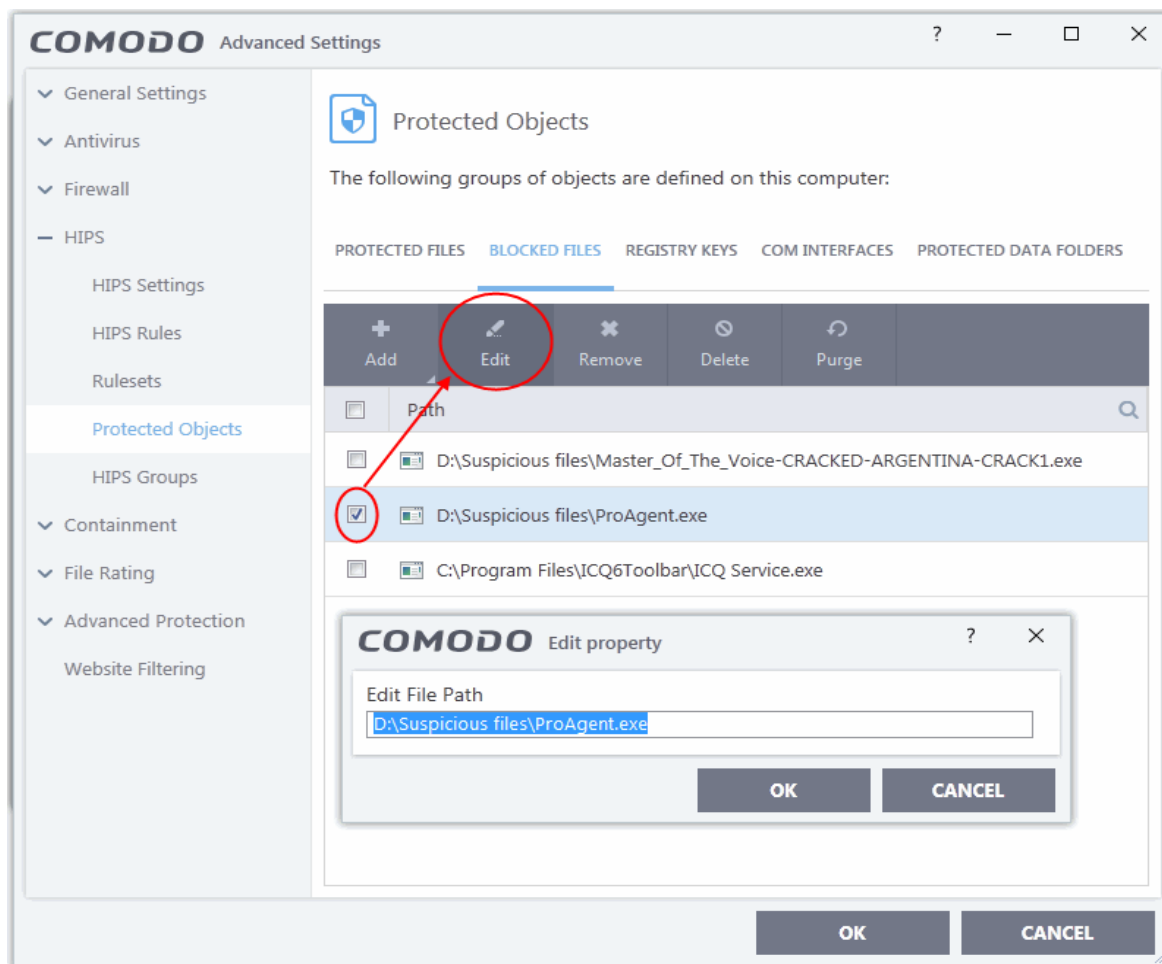
7.   Select the entry from the Blocked Files interface, and click 'Edit' at the top

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.
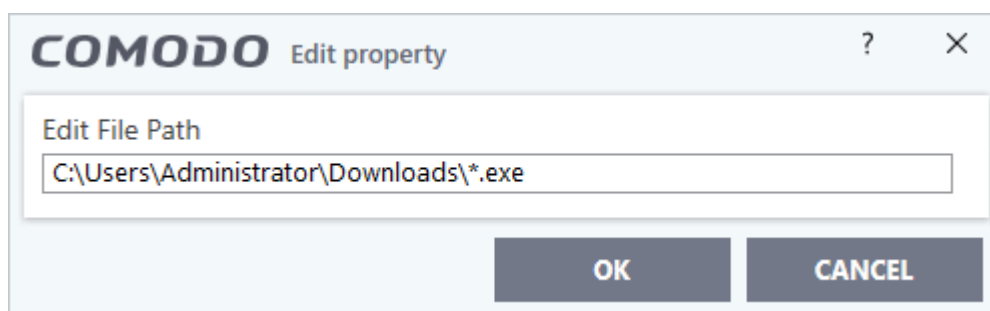
9.   Click 'OK' in the 'Edit Property' dialog

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**.

- You can also add or remove components after installation.

Switch the installation type

- Click 'Windows Home' button > 'All Apps' > 'Comodo' >

- Right-click on 'COMODO Internet Security' and select 'Uninstall'
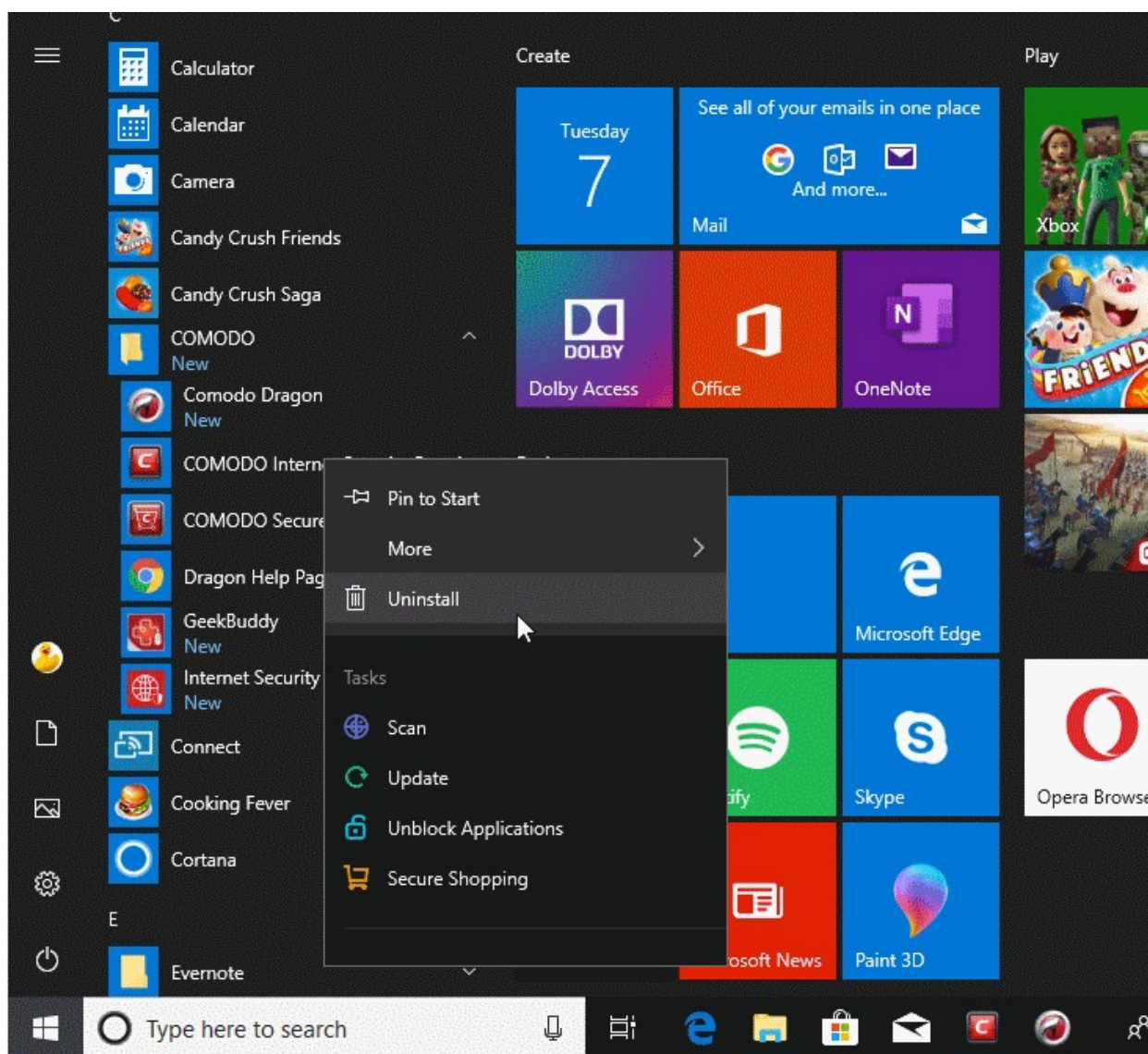
    OR

- Click 'Windows Start' button > 'Settings' icon ⚙

- Select 'Apps' from the Windows 'Settings' pane

- Select 'Apps & Features' on the left

- Scroll down the list of installed applications in the left and select 'Comodo Internet Security'
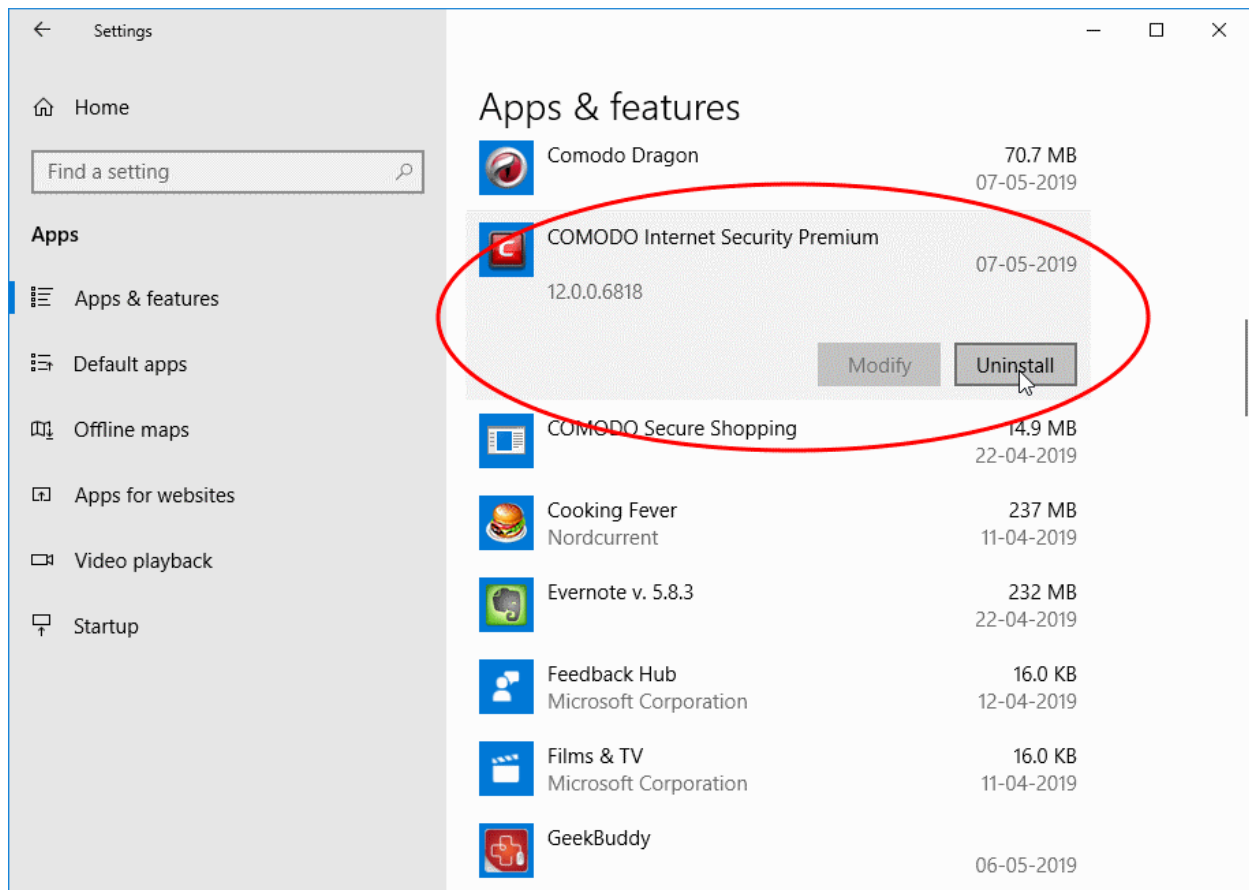
- Click 'Uninstall'

The configuration wizard starts:
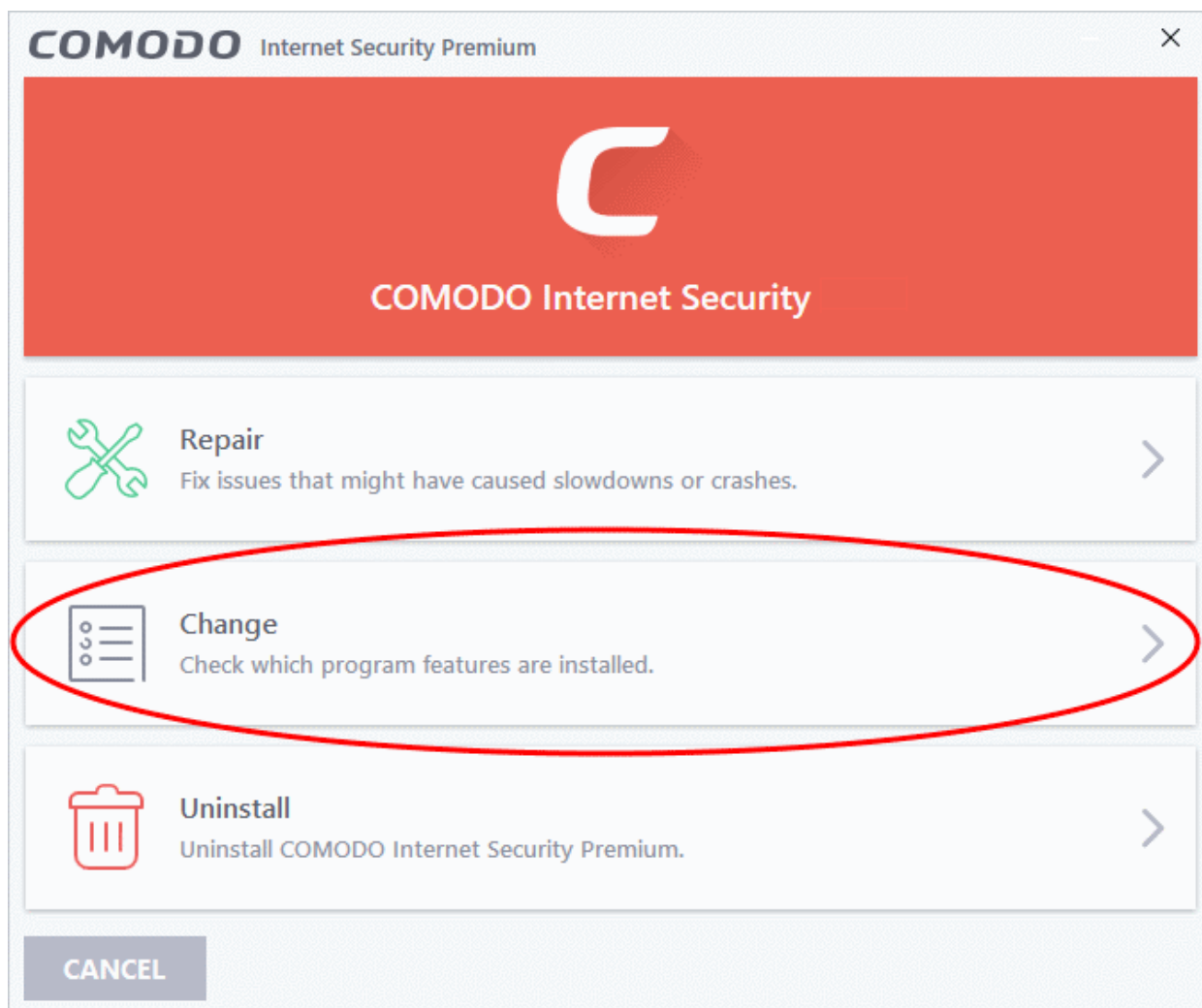
- Select 'Change' to modify the installed features.
- Choose the features you want to add or remove:
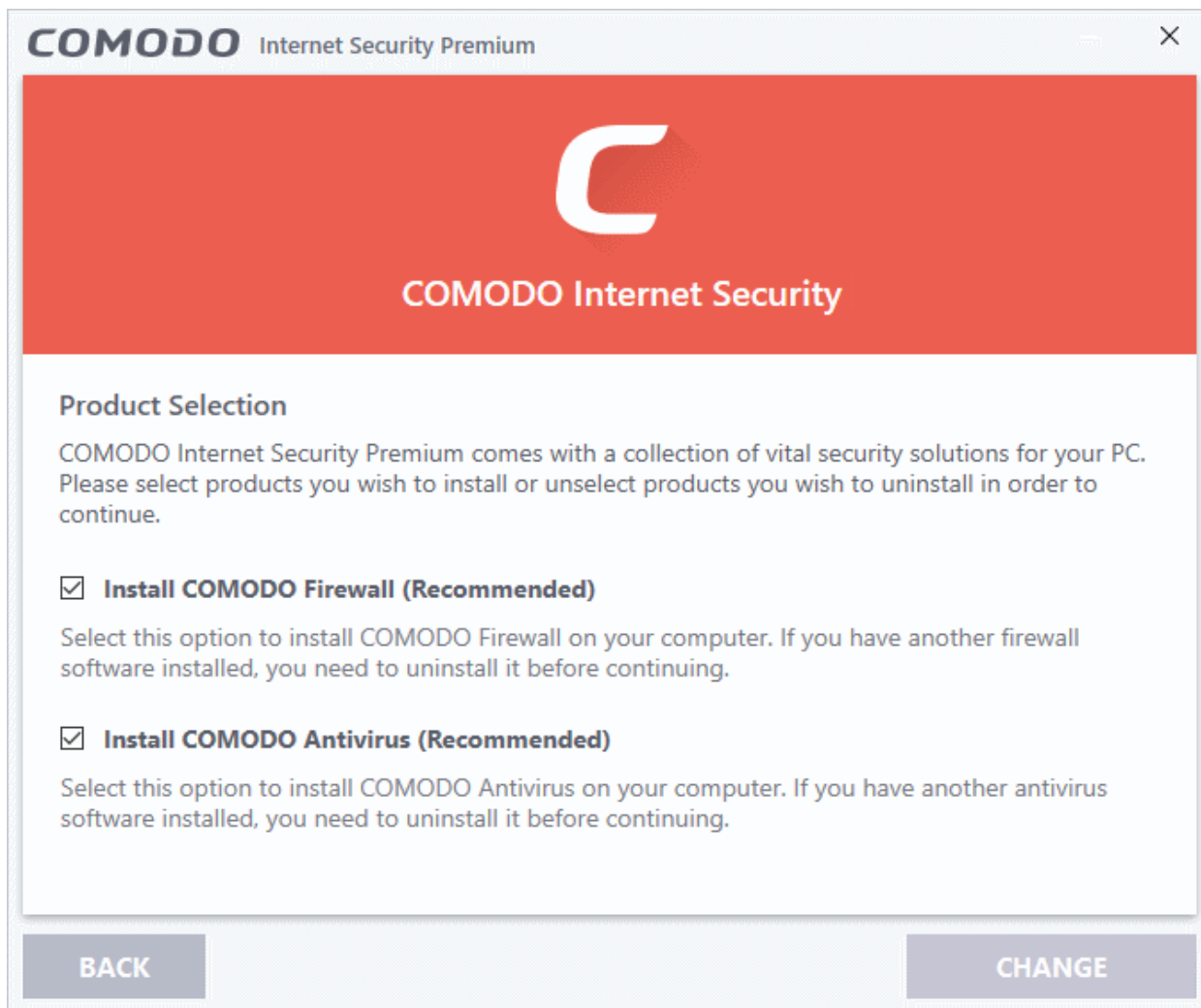
- Click 'Change'. CIS will begin installing or uninstalling components:
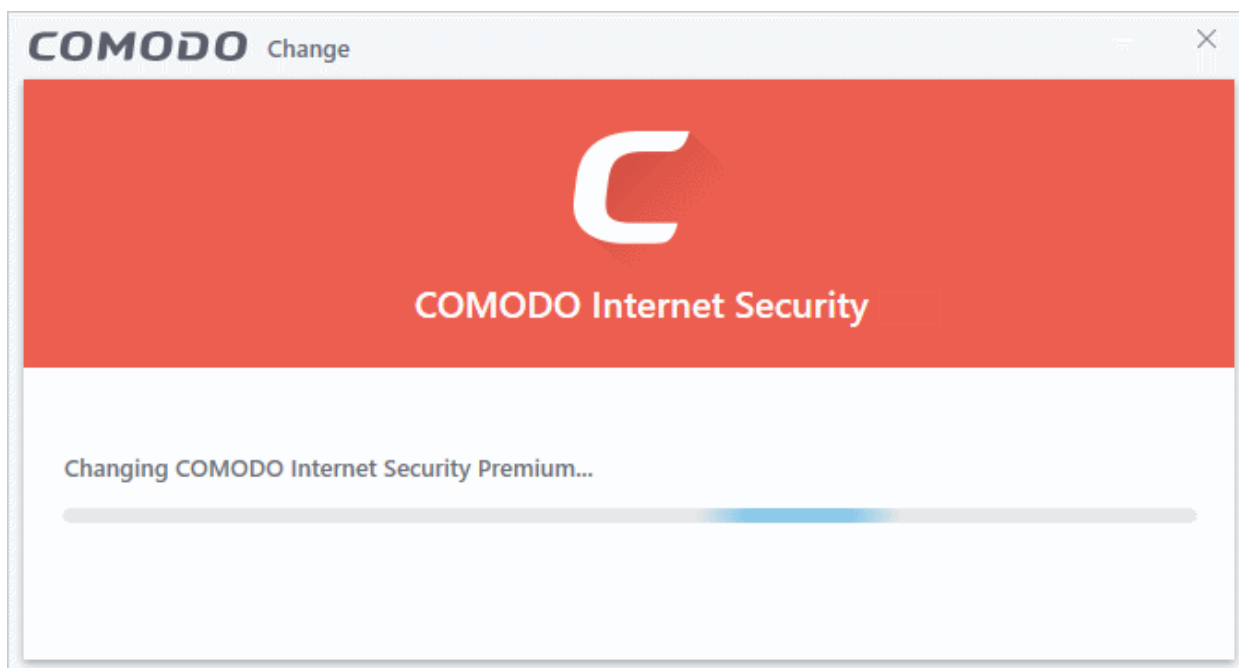
- Click the 'Finish' button when the process is complete.
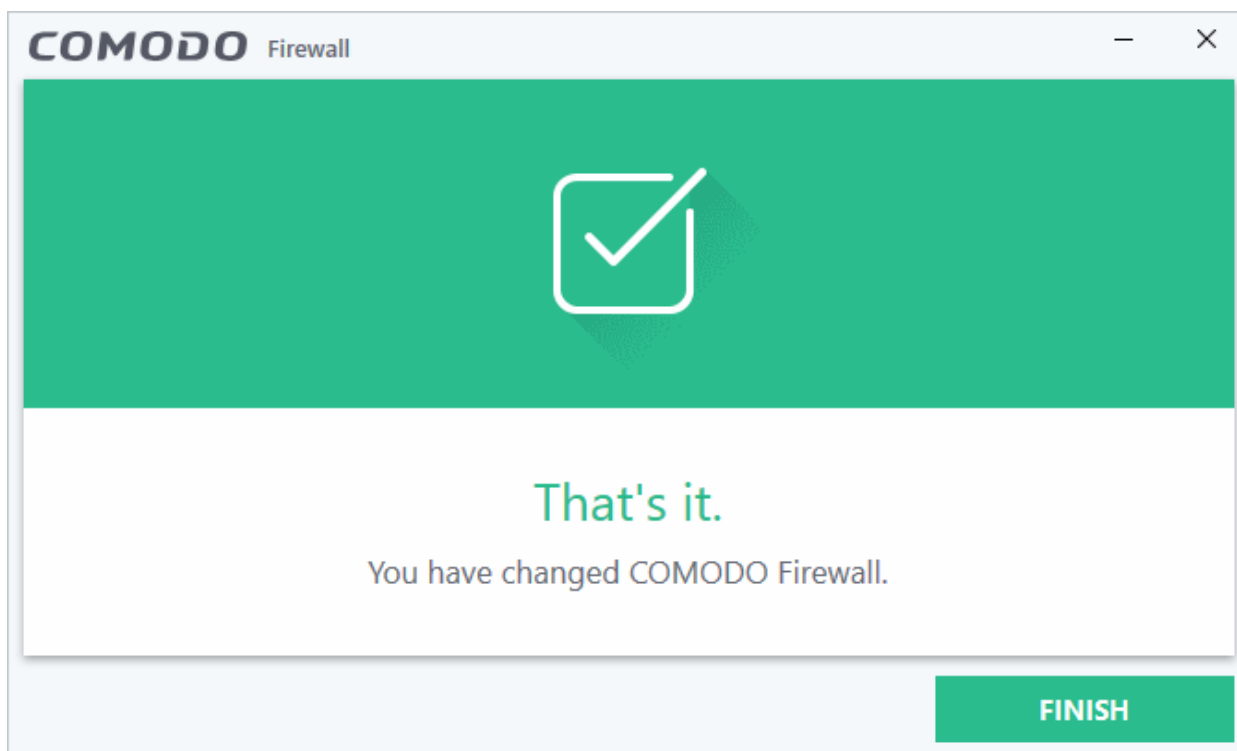
Your computer needs to be restarted for the change to take effect.
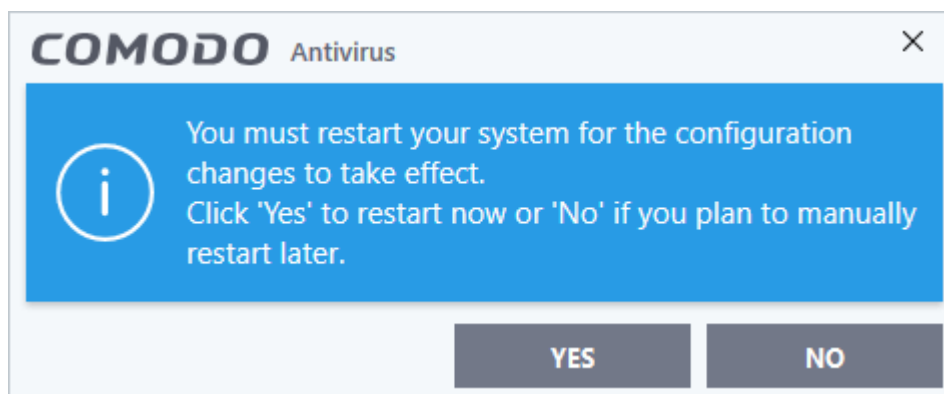
- If you want to restart the system at a later time, click 'No'.
- If you want to restart the system immediately, please save any unsaved data and click 'Yes'.

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 automatically downloads software and antivirus database updates.
- However, some users like to control when updates are downloaded. For example, network admins may not want automatic updates because they take up too much bandwidth during the day.

CIS provides full control over virus and software updates. Click the appropriate link below to find out more:

- **Switch off automatic updates entirely**
- **Switch off auto-updates selectively**

- **Switch off auto-updates prior to virus scans**

Switch off automatic updates entirely

1. Click 'Settings' on the CIS home screen

2. Click 'General Settings' > 'Updates'

3. Disable both options shown below:
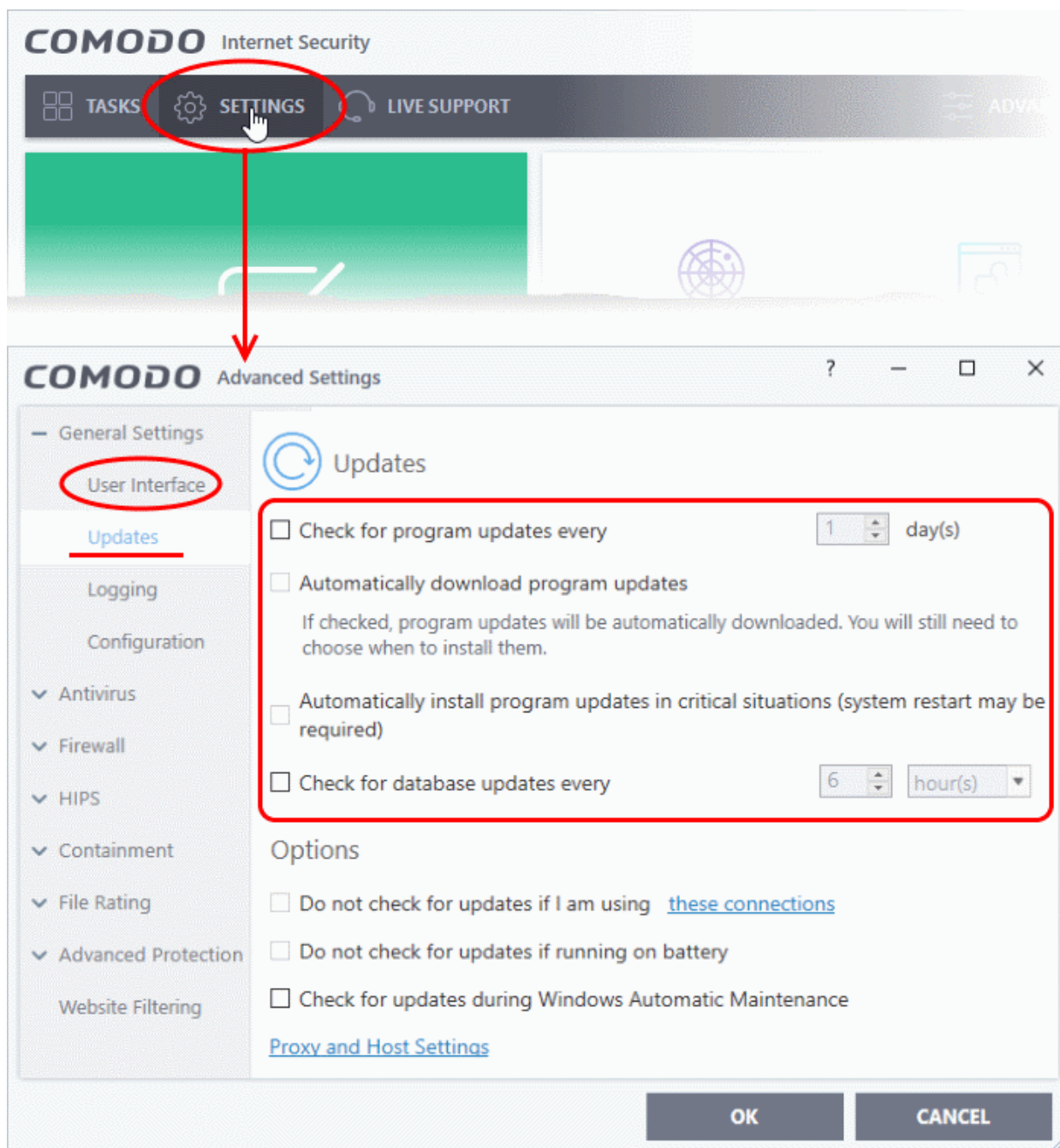
4. Click 'OK' to apply your changes.

Switch off automatic updates selectively

1. Click 'Settings' on the CIS home screen

2. Click 'General Settings' > 'Updates'
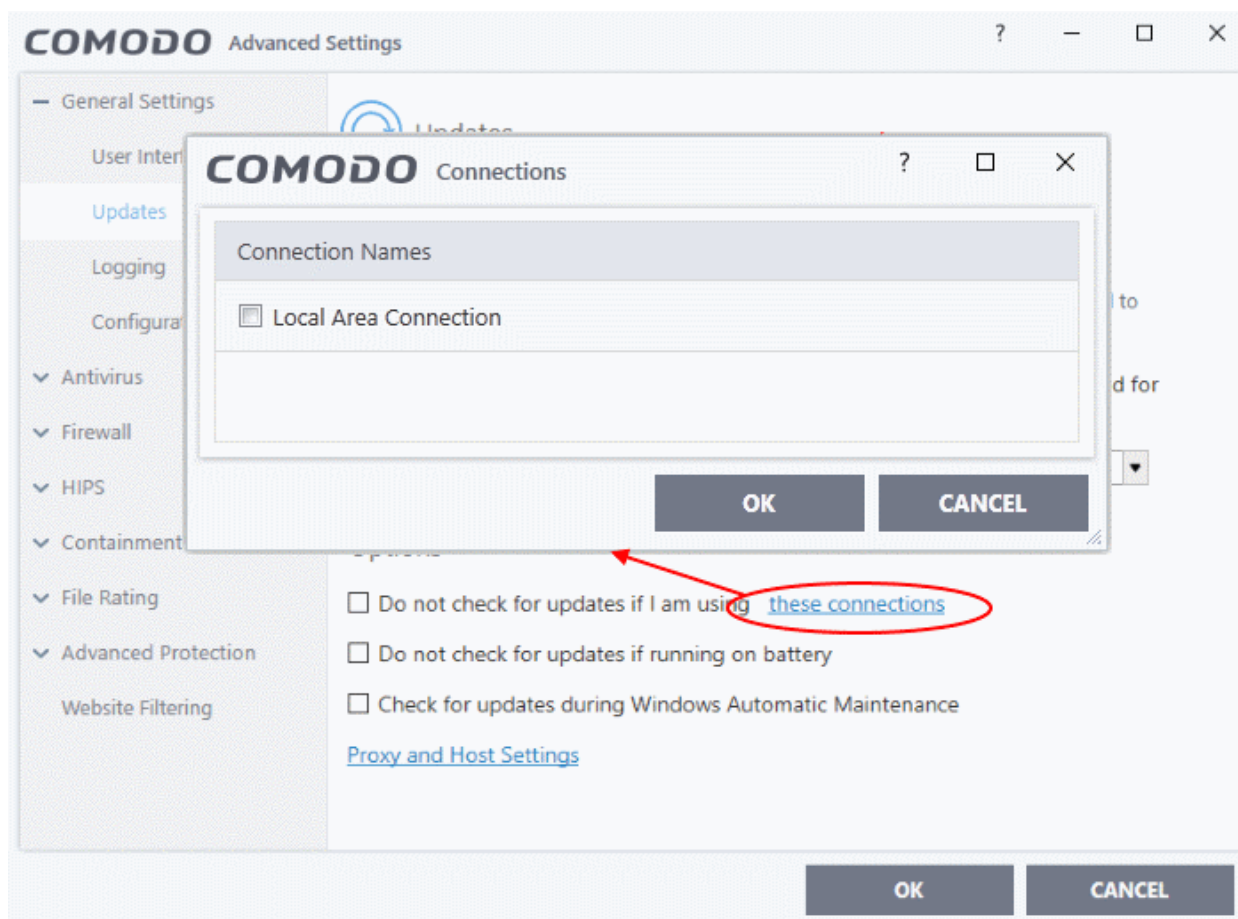
- Suppress automatic updates when using certain networks:
  - Select the 'Do not check updates if am using these connections' check-box
  - Then click 'these connections' to view a list of connections you use.
  - Select the connection over which you do not want CIS to check for updates and click 'OK.'
- Do not check for updates if running on battery - Will only download updates when the computer is plugged in to the mains.

Switch off automatic virus signature database updates prior to AV Scans:

1. Click 'Settings' on the CIS home screen

2. Click ' Antivirus' > 'Scans'

3. Select a target scan profile

4. Click 'Edit' from the options at the top

5. Click 'Options', scroll down, and clear the 'Update virus database before running' checkbox.
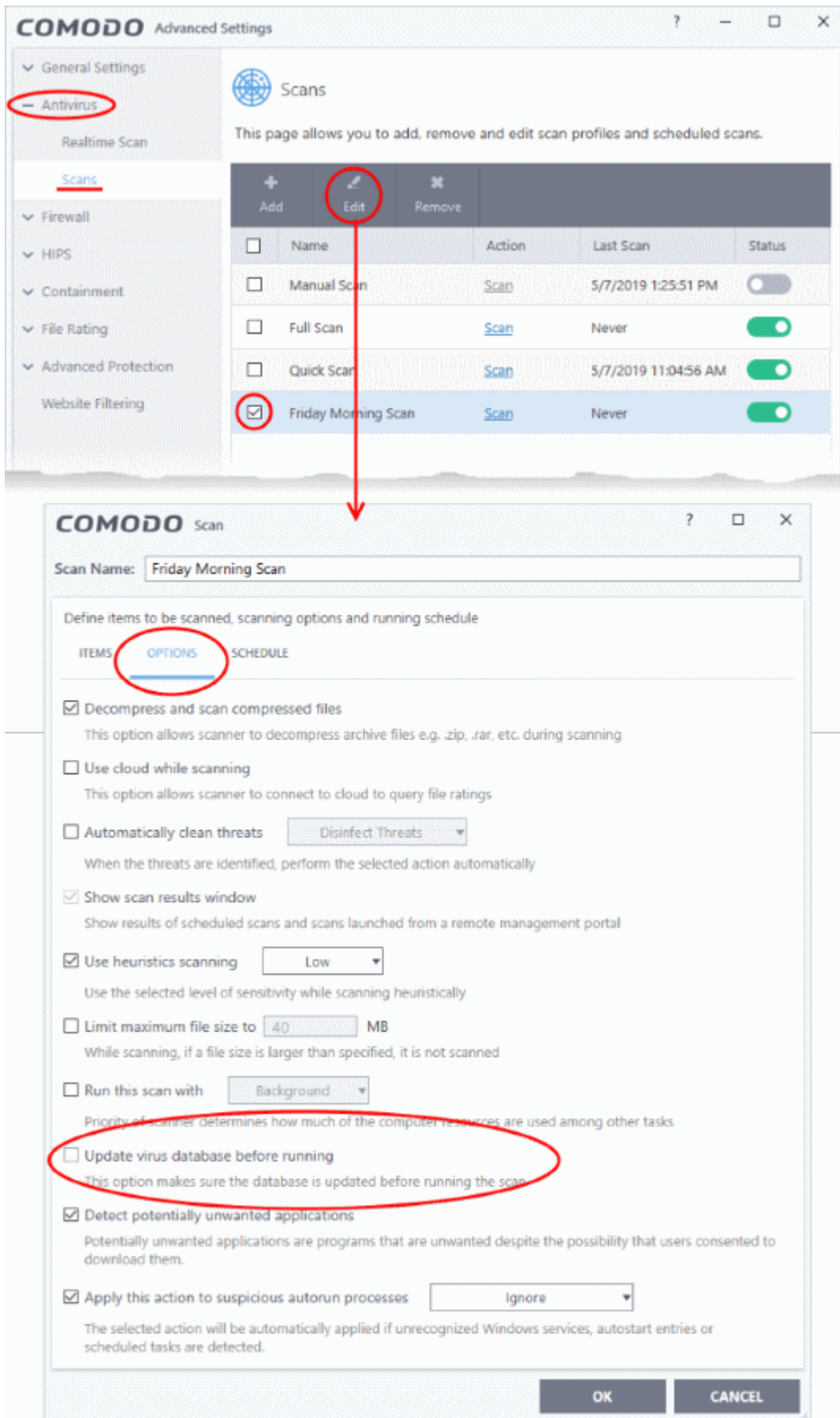
6. Click 'OK'

7. Click 'OK' in the 'Advanced Settings' screen for your changes to take effect.

Suppress CIS Alerts Temporarily while Playing Games

- CIS shows you an alert if it finds a security threat, and also shows alerts for general system messages.
- 'Silent mode' lets you temporarily disable these alerts so they don't interrupt games or a presentation etc.
- During this time, operations that can interfere with user experience are either suppressed or postponed. This includes alerts and scheduled scans.
- All protection components are still 100% active in silent mode.

Temporarily stop pop-up alerts

- Click 'Silent Mode' button on the CIS home screen:
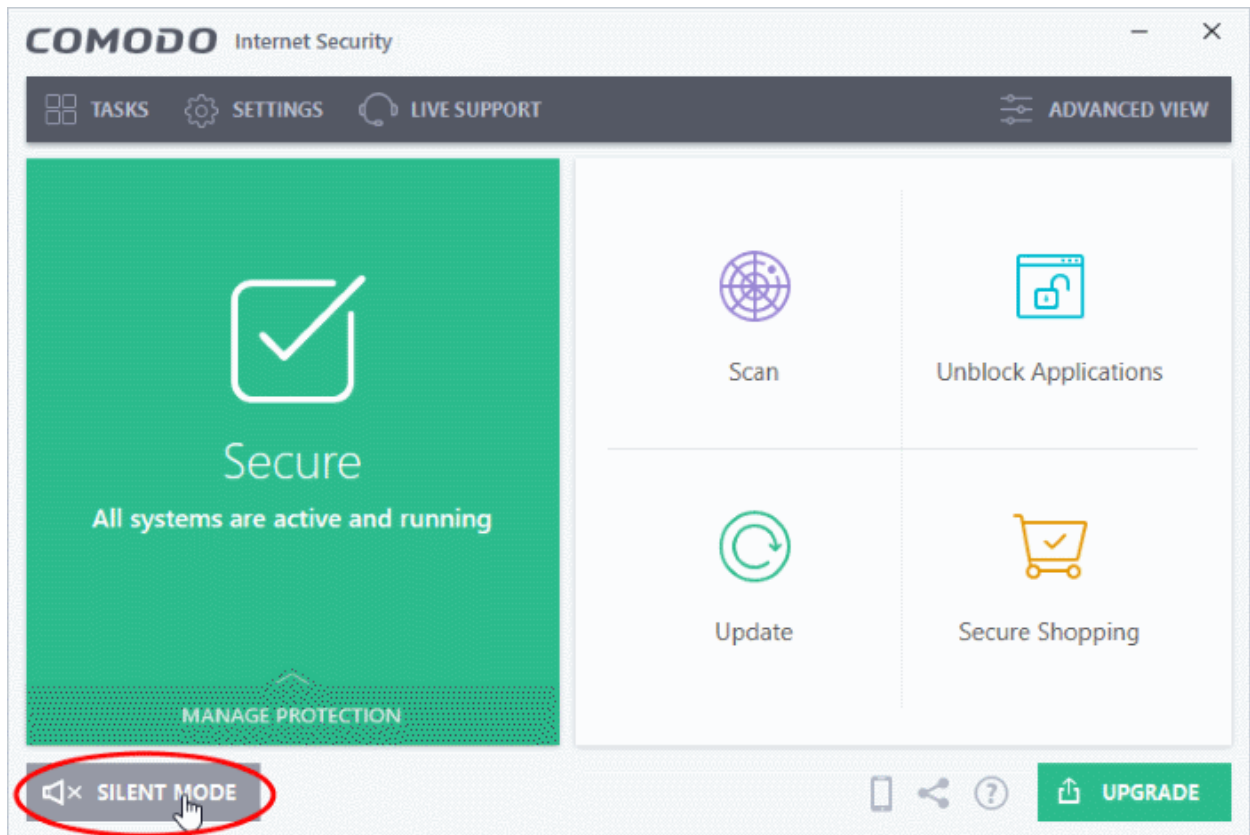
OR

- Right-click on the CIS tray icon and select 'Silent Mode':
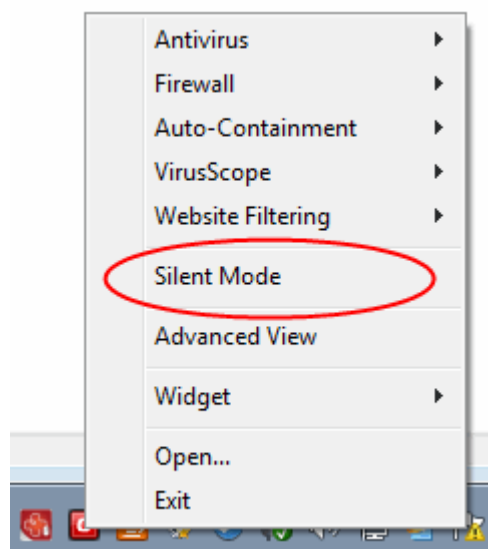
The alerts are now suppressed.

- To resume alerts and scheduled scans, just deactivate 'Silent Mode' from the home screen or tray icon.
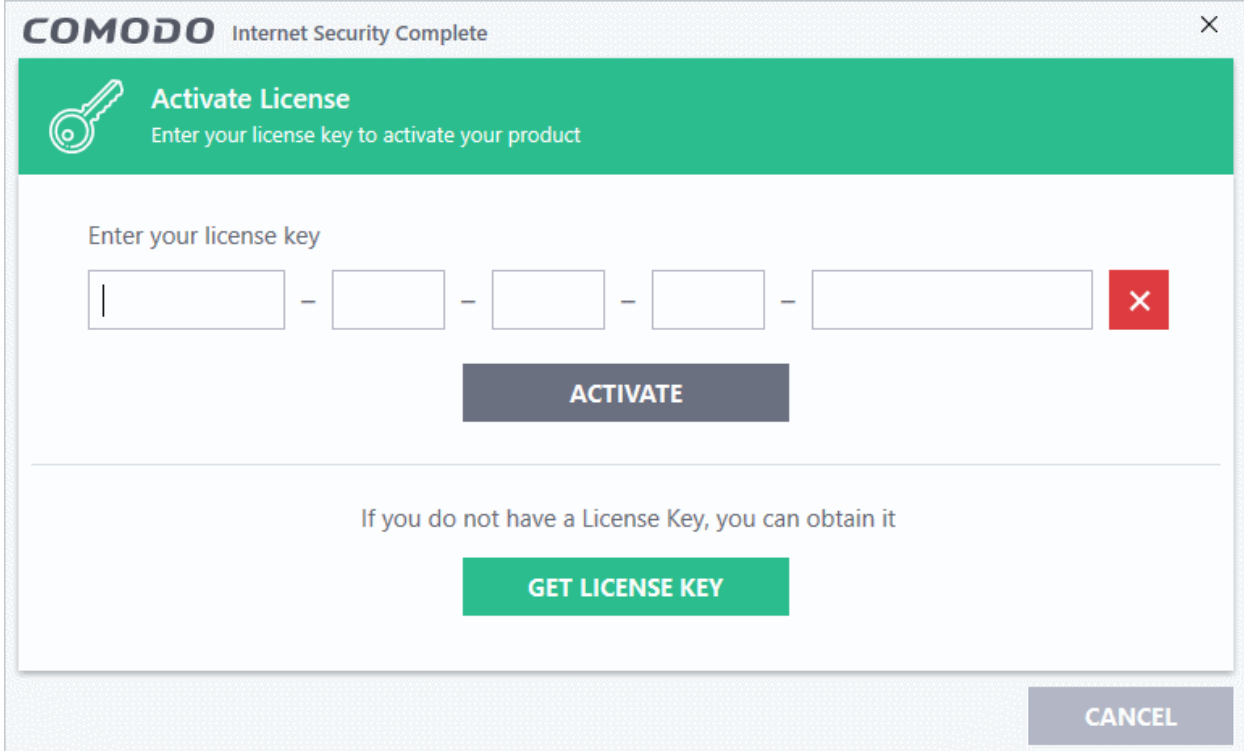
Renew or Upgrade your License

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').
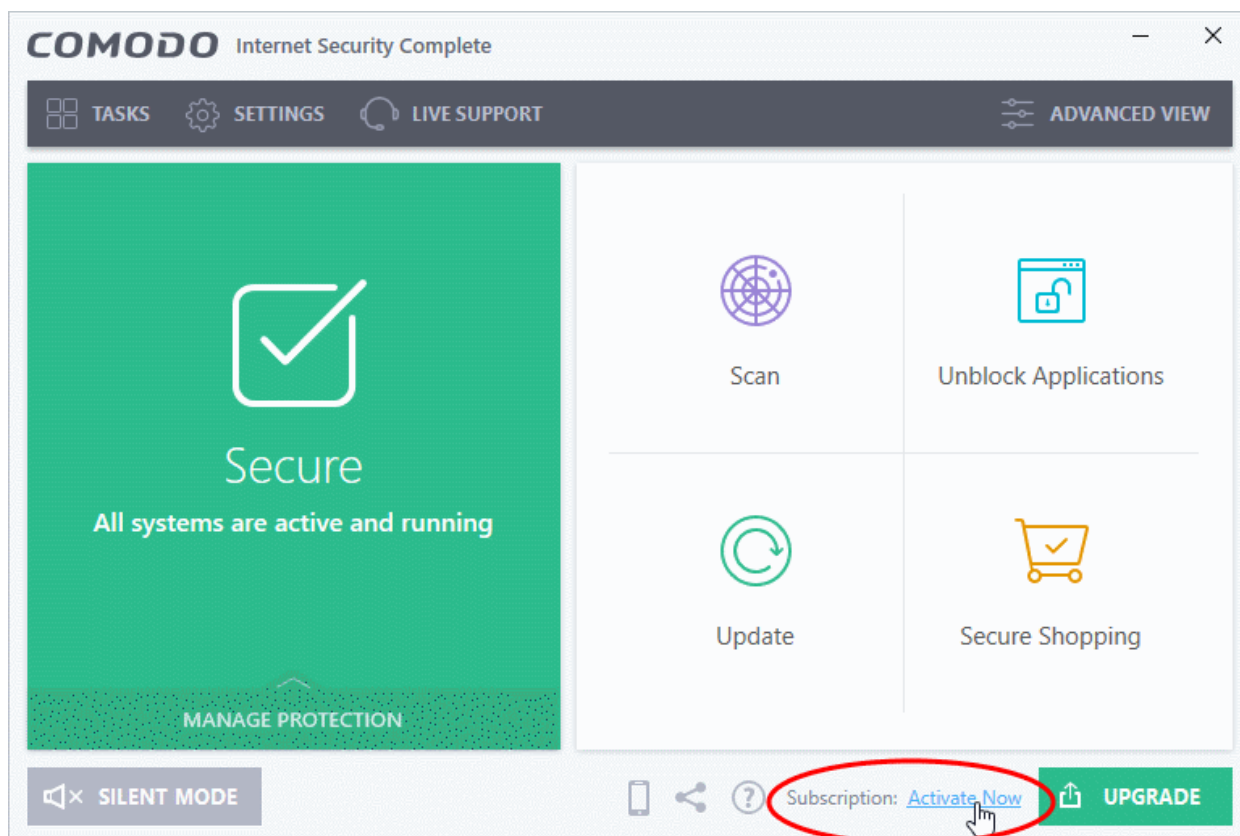
The 'Product Activation Wizard' will start.

- 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=RkJEMUZENjMzQUM4RDlDNDE4MzBDQjc1NDlENUIzRkY&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*
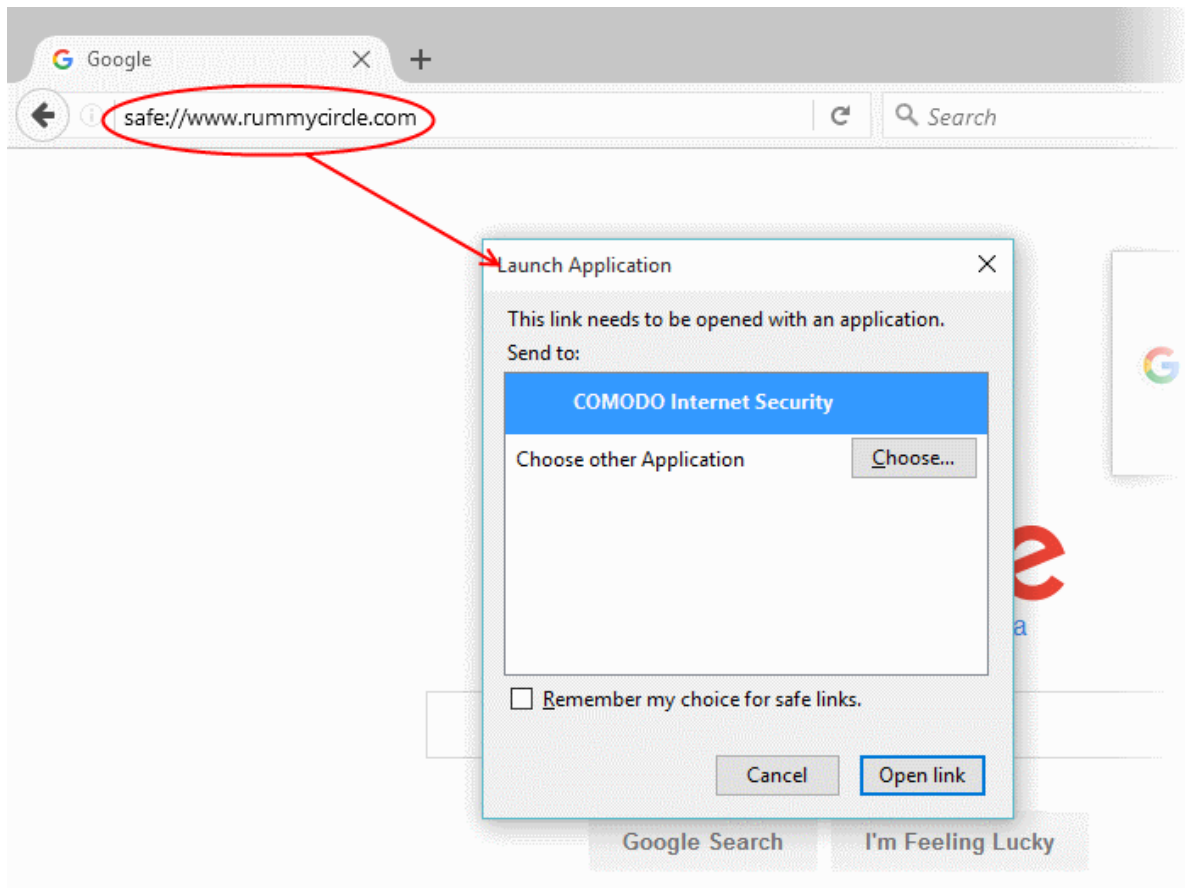
- Allow the application

The URL will be open in a contained browser. Note the green border:
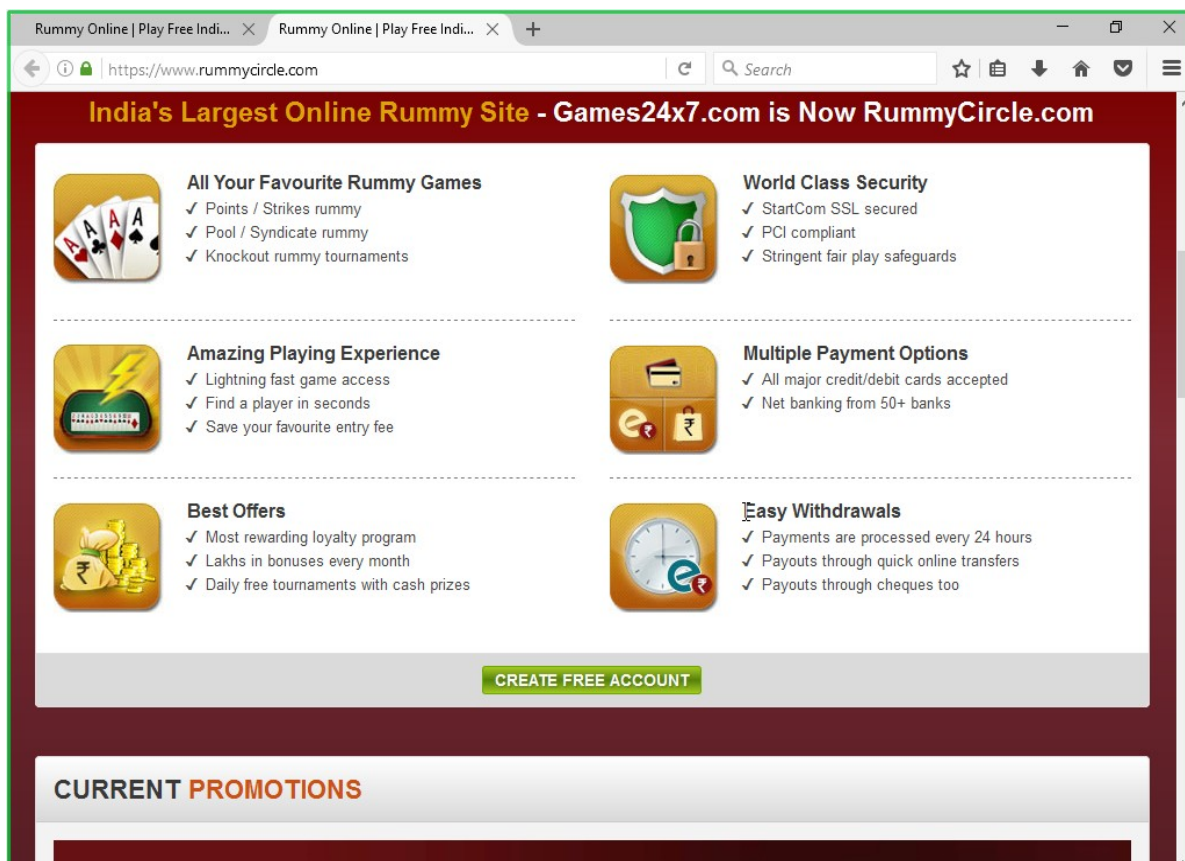
2 - kiosk://

Type 'kiosk://' before any web address to open the website in the Virtual Desktop.

E.g. Try *kiosk://wwww.rummycircle.com*
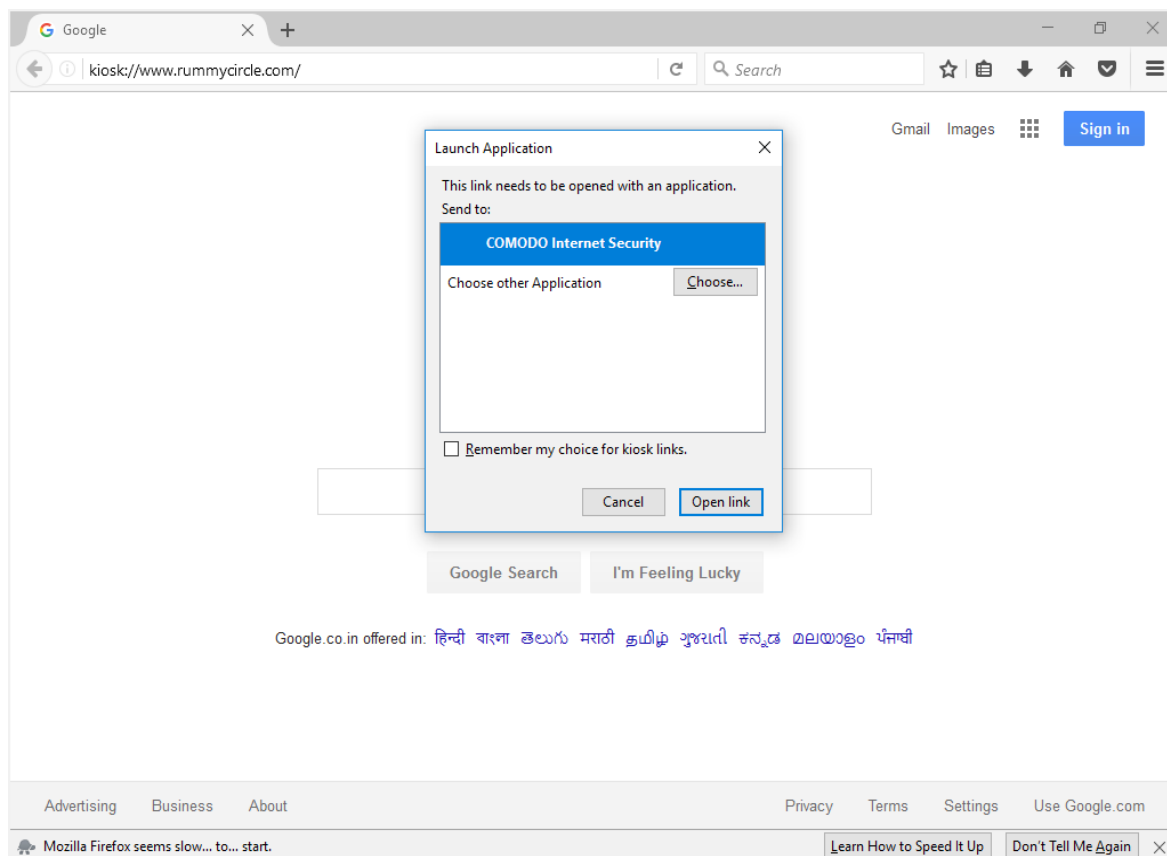
• Allow the application

The webpage will be displayed in a browser inside the Comodo Virtual Desktop:
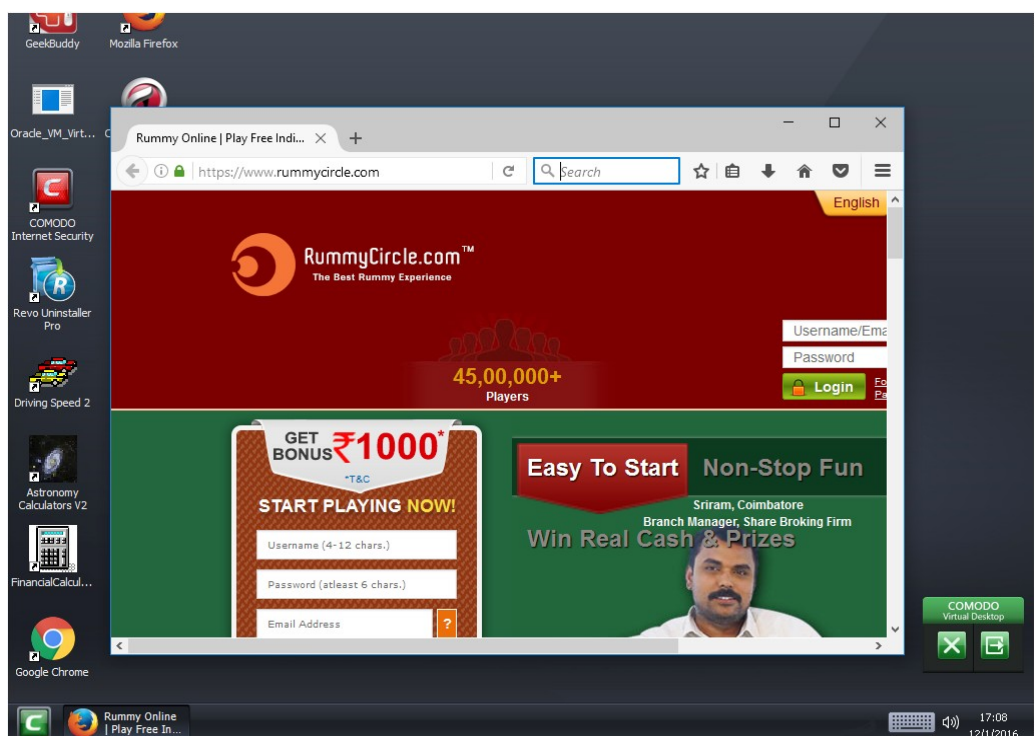
3 - Comodo://

Type 'Comodo://' before the command line parameter for the action to be executed. See the table below for more details.

For example *Comodo://antivirus.update*
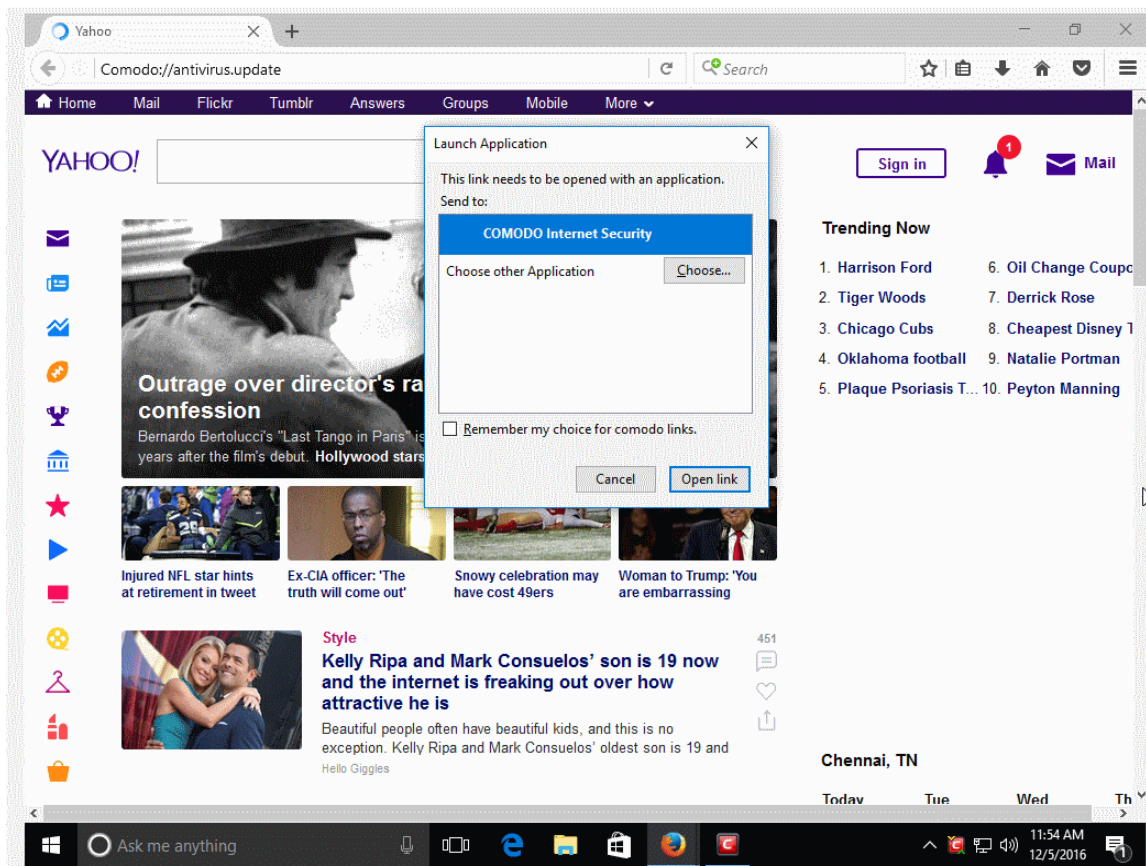
- Click 'Open link'

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'
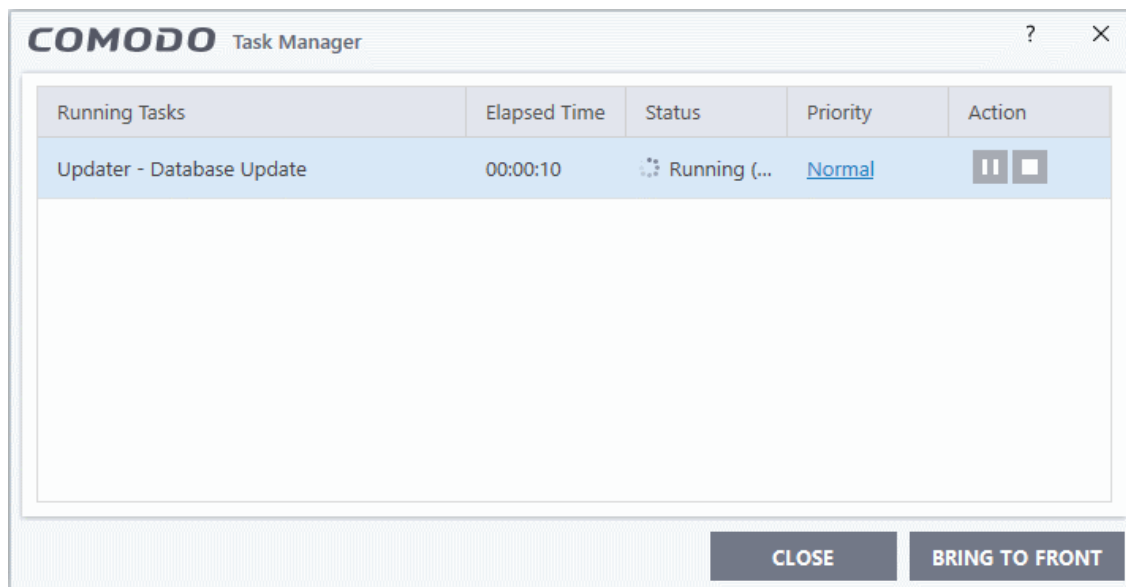
The following is a list of all possible commands. Commands can be entered into any browser address bar.

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

Configure Secure Shopping

• Click 'Settings' on the CIS home screen

• Click 'Advanced Protection' > 'Secure Shopping'
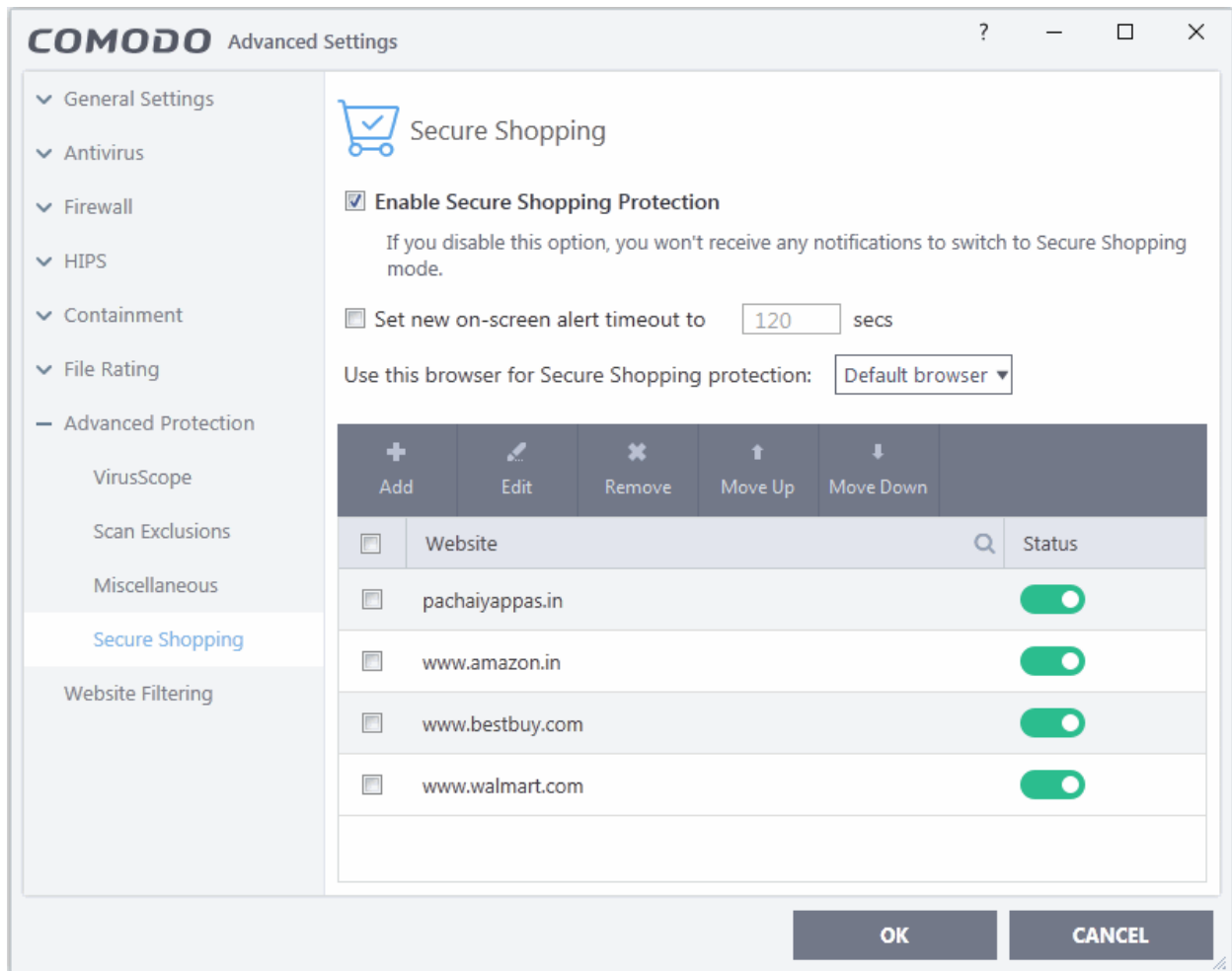
Add websites for Secure Shopping Protection

- Click the 'Add' button then type the URL of the site you want to visit securely:
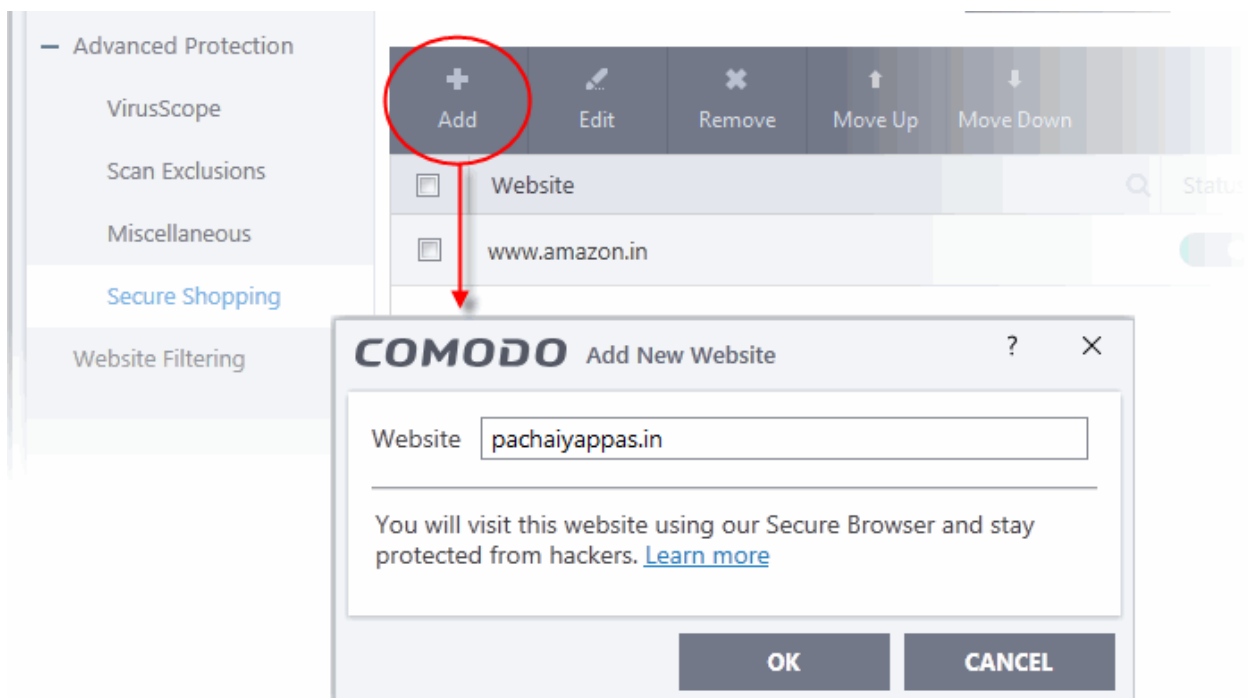
- Click 'OK' to add the site to the list. Repeat the process to add more sites
- Click 'OK' in the 'Advanced Settings' interface to save your changes.

An alert is shown if you visit a site on the secure shopping list:
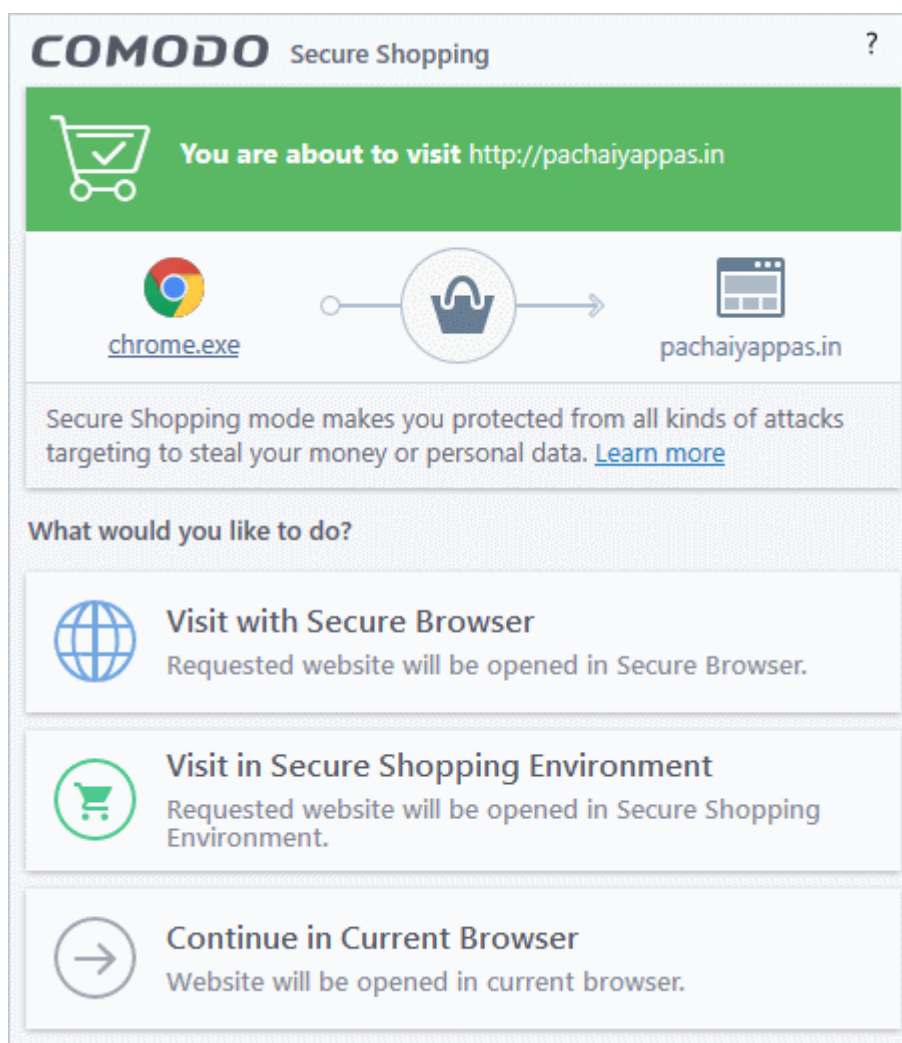
- Choose how you want to proceed:
  - **Visit with Secure Browser** - The site opens in a browser protected by all secure shopping technologies except full process isolation. Full process isolation is replaced with partial process isolation. The browser window will have a blue border around it:
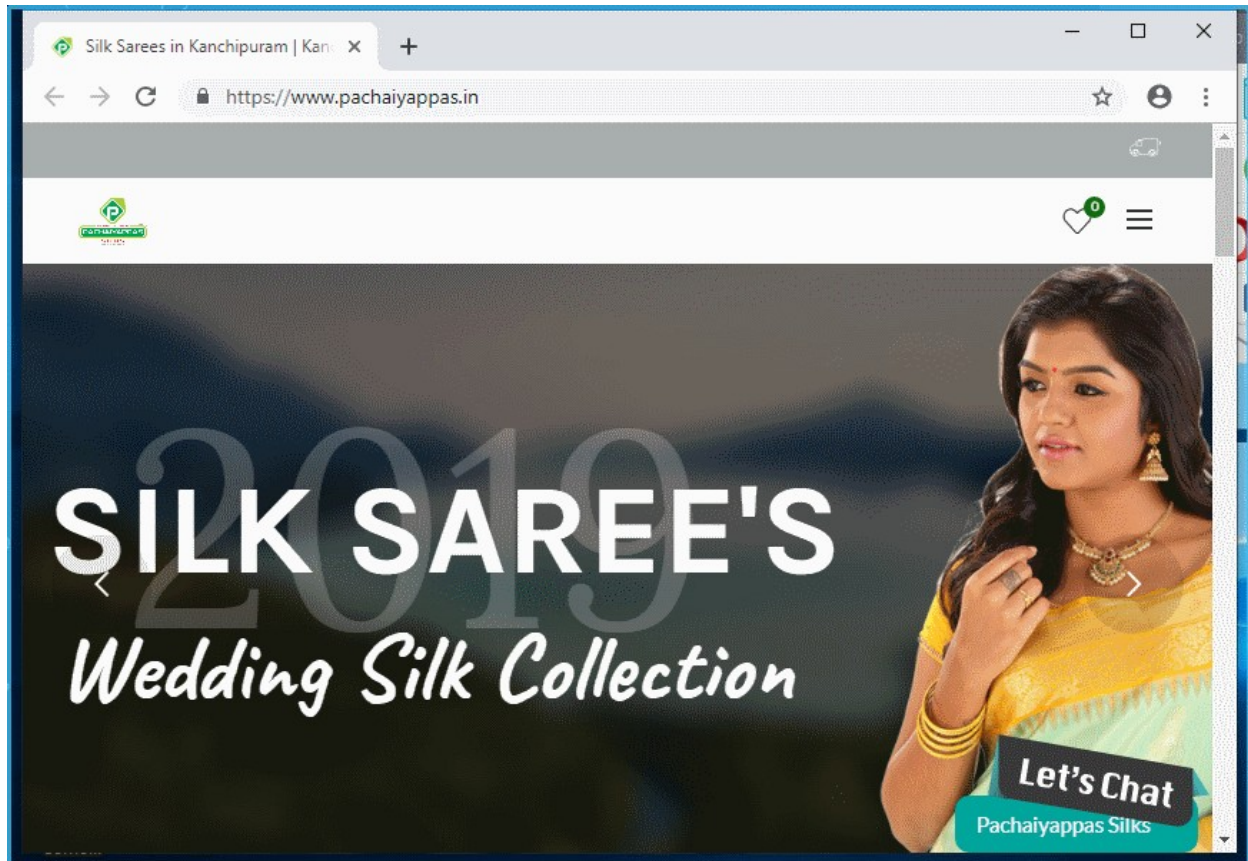
- **Visit in Secure Shopping Environment** - The website opens in a security hardened, virtual environment. When inside this environment, your browser cannot be accessed or potentially attacked by other processes running on your computer. The environment also features a virtual keyboard which allows you to enter confidential information without fear of your keystrokes being tracked. See **Use Comodo Secure Shopping Enviroment** for more details.

- **Continue in Current Browser** - Access the site in the same browser you are using.

Use 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:

- **CIS Home Screen** - Click 'Tasks' > 'General Tasks' > 'Secure Shopping'
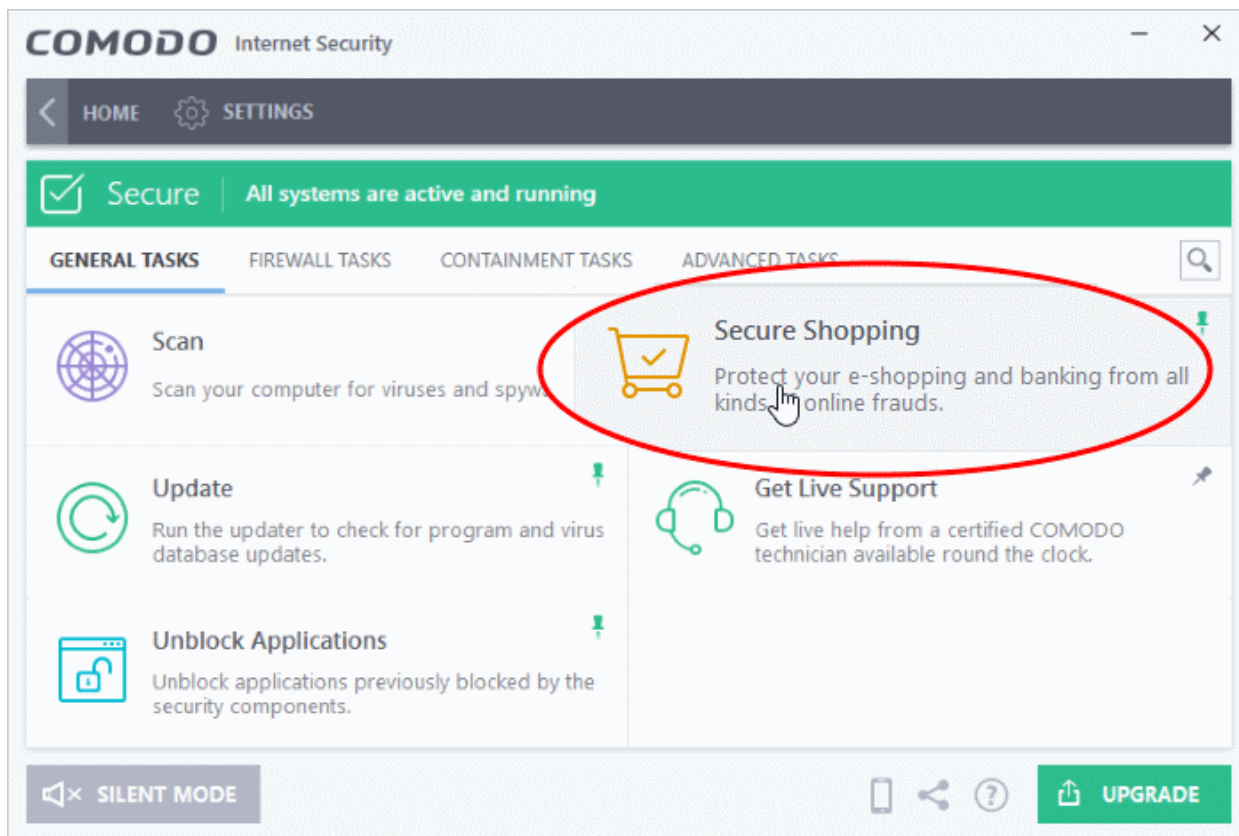
- **CIS Desktop Widget** - Click the 'Secure Shopping' icon from the CIS desktop widget
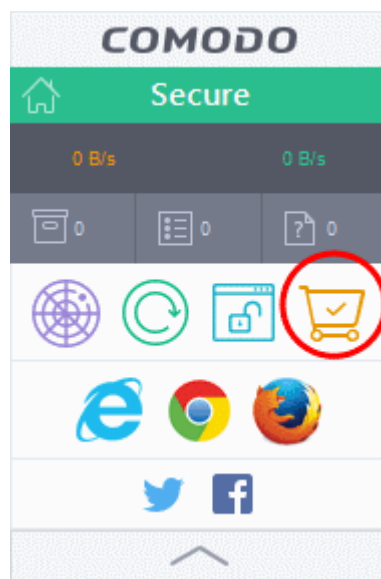
- **Windows 'Start' menu** - Click Windows Start/Home > All Programs > Comodo > Comodo Secure Shopping
- **Windows desktop icon** - Double-click the 'Comodo Secure Shopping' shortcut on the desktop

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

- • 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. 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 browser chosen as per the configuration. 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 lets 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 more help on the tools panel:

- • **Use virtual keyboard**
- • **Switch to your desktop**
- • **Exit Secure Shopping**

Open applications inside the secure shopping Environment

- • **Start the Secure Shopping** environment and click the folder icon at bottom-left:
- • Browse to the application or file you want to run and open it.

The application opens inside the Secure Shopping environment:

The Tools Panel

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.

Use the virtual keyboard

The Secure Shopping environment features an on-screen virtual keyboard that helps you in entering confidential information like website user-names, passwords and credit card numbers.

- Click the language button ![ENG] at the bottom-right and select the keyboard layout you want to use.

- Click the keyboard icon in the tools panel to open the on-screen virtual keyboard.

Temporarily switch to your desktop

- Click the ![button] 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.

Close Secure Shopping

- Click the 'X' button ![X]

A confirmation is shown:
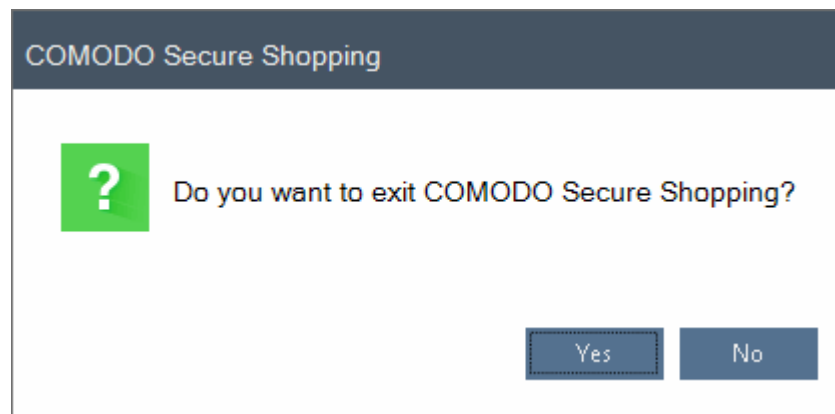
- Click 'Yes' to exit the Secure Shopping environment.

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'.
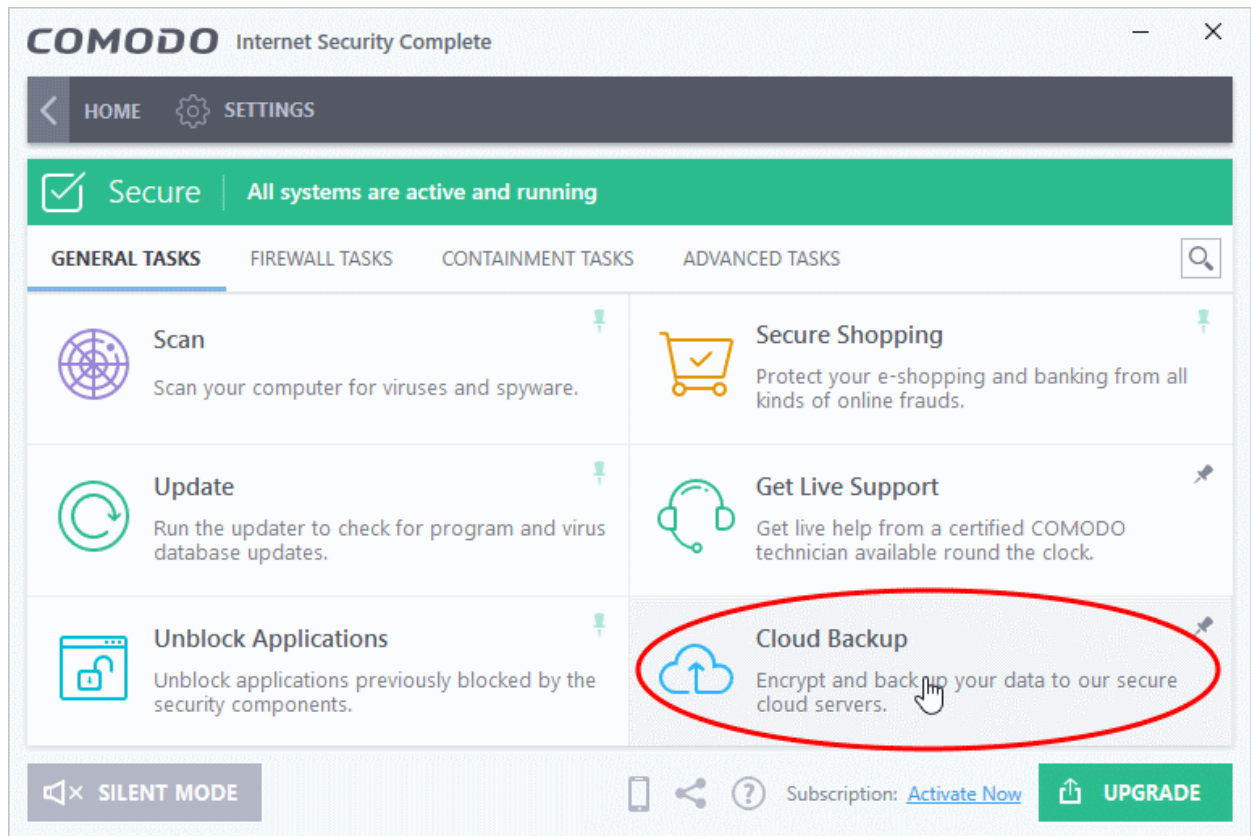
If you have not activated CIS, then you can create an account from the 'Create New Account' form and if you have already activated CIS using the license key, an account will be created for you automatically.

Account will be created and the dialog displayed.
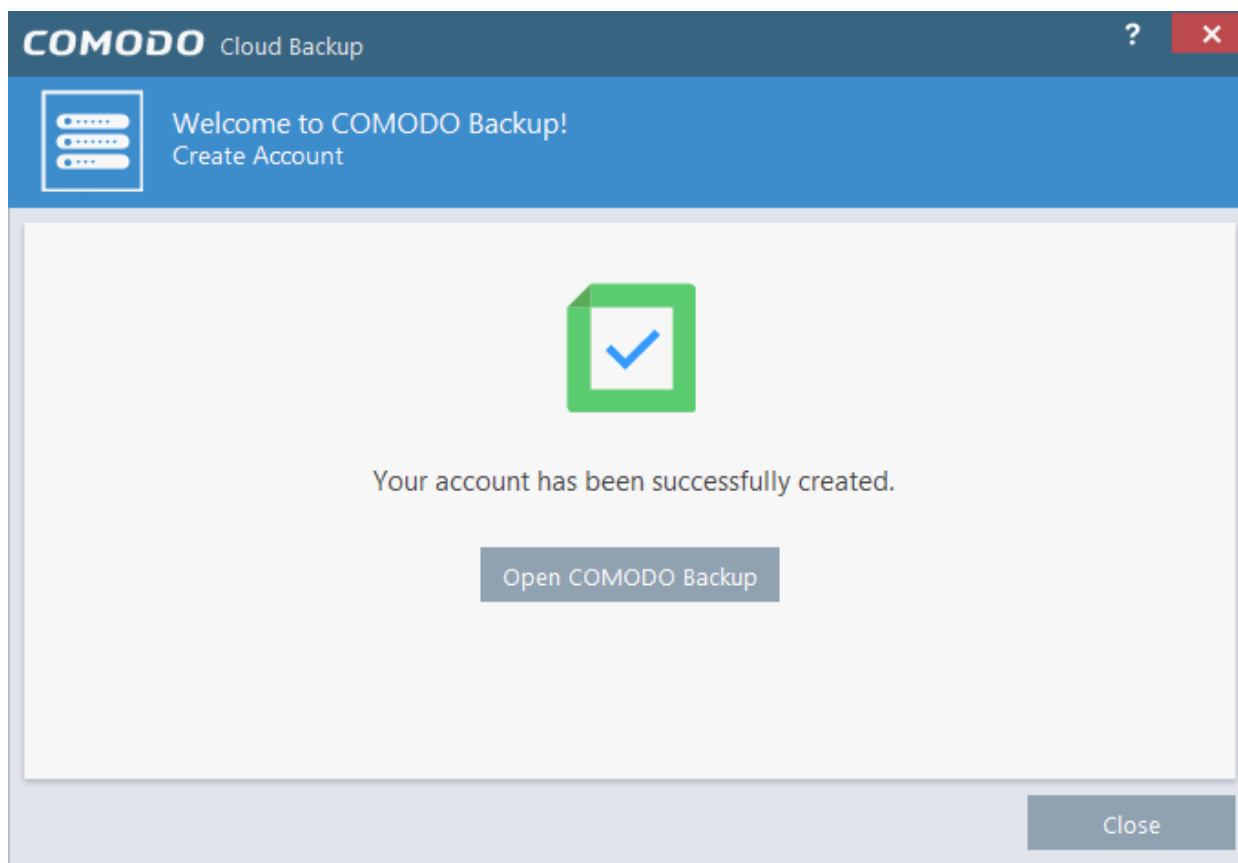
- Click 'Open COMODO Backup' to access your online backup management console.

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**.

Give Contained Applications Write Access to Local Folders

- By default, applications running in the container can access files on your computer but cannot save changes to them.
- You can define exceptions to this rule in containment settings

Add exclusions to contained files and folders

- Click the 'Settings' icon on the CIS home screen
- Click 'Containment' > 'Containment Settings'
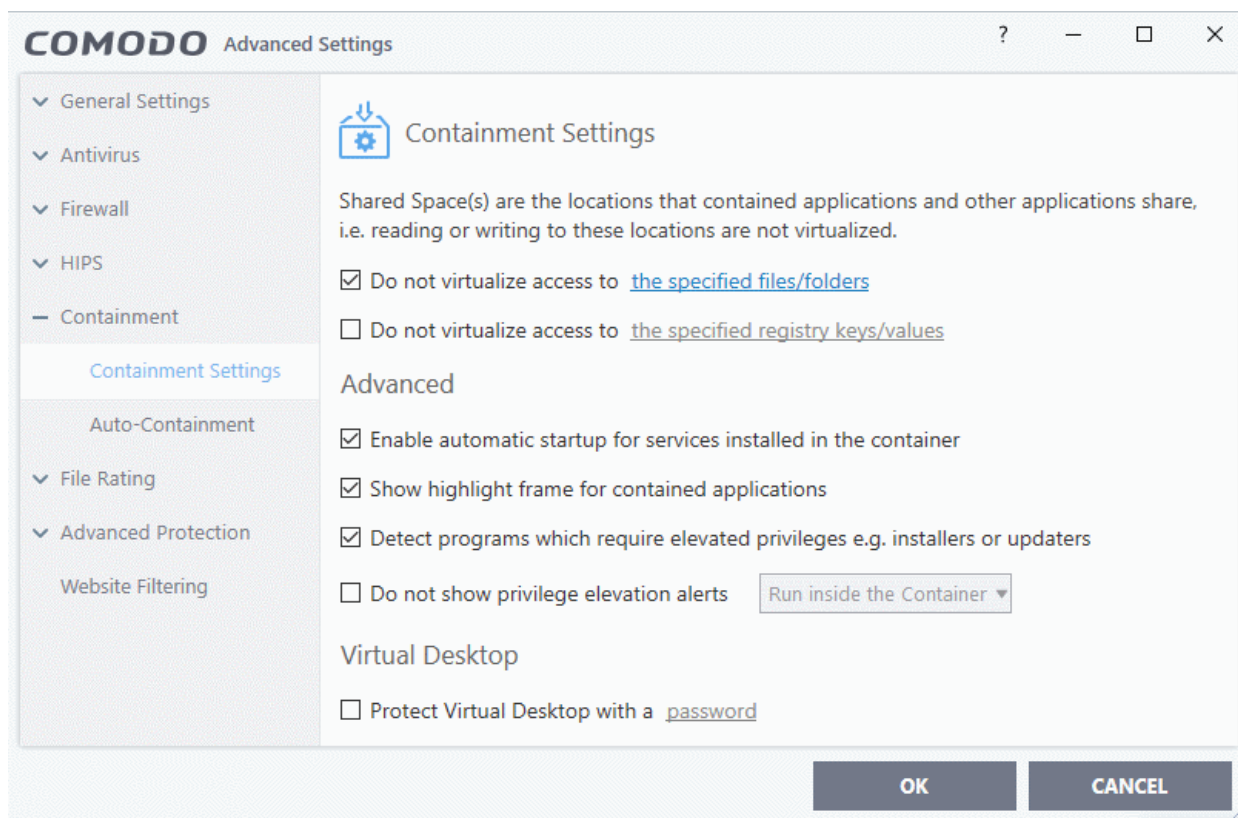
- Enable 'Do not virtualize access to the specified files/folders' then click 'the specified files/folders' link.

- The 'Manage Exclusions' dialog shows files and folders that can be modified by contained applications. By default, 'Shared Space' is the only folder they can write to:
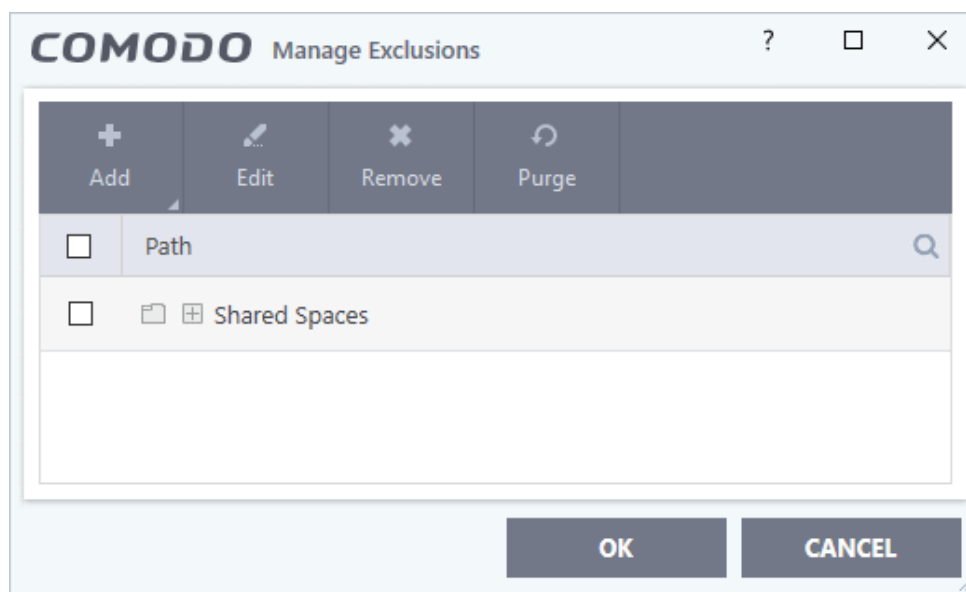
Add a file/folder exception

- Click the 'Add' button in the 'Manage Exclusions' dialog.
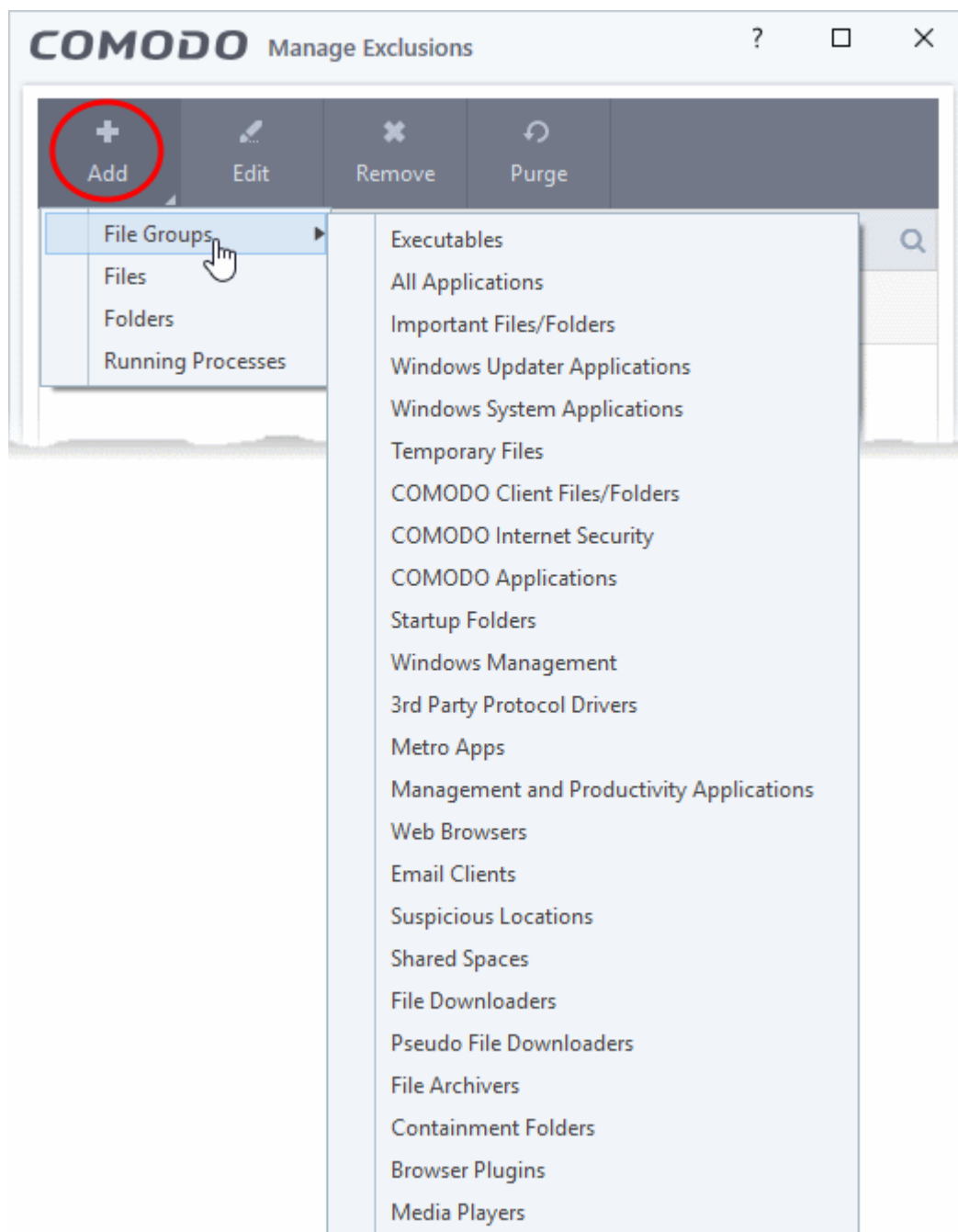
- **File Groups** - Choose a category of files or folders to which access should be granted. For example, select 'Executables' to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd. See '**File Groups**', for more details on file groups.

- **Files** - Pick specific files or applications that contained applications can access

- **Folders** - Specify folders that can be accessed by contained applications. Access is granted to all files in the folder.

- **Running Processes** - Choose a process currently running on your computer. The parent application of the process is added to the exclusions.

- Click 'OK' in the 'Manage Exclusions' dialog

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

Use the Comodo Uninstaller Tool

- **Note.** This tool should only be used if you are having difficulties removing Comodo products using the traditional 'Add/Remove' programs method.
- Users who simply wish to uninstall are strongly advised to remove the product via the Windows control panel:
- Type 'Add/Remove Programs' into the Windows search box
    - Windows 10 - The search box is pinned to the task bar
    - Windows 7 and other versions - Click the 'Start' button to view the search box
        - Locate the Comodo product you wish to remove in the list of programs
        - Click 'Uninstall'
- The Comodo uninstaller tool lets admins and advanced users scan hosts for Comodo products and remove them.
- Products that can be removed by this tool include Comodo Internet Security, Comodo Firewall, Comodo Antivirus, Comodo Client Security, and Comodo Advanced Endpoint Protection (AEP).

64-bit version - **http://download.comodo.com/cis/download/installs/ciscleanuptool/ciscleanuptool_x64.exe**

32-bit version - **http://download.comodo.com/cis/download/installs/ciscleanuptool/ciscleanuptool_x86.exe**

The tool creates a system restore point prior to performing the uninstall operation.

Uninstall Comodo products

- Download the setup file from the URLs mentioned above.
- Run the setup file.
- Read the advisory, agree to the EULA then click 'I accept' to commence the uninstallation:
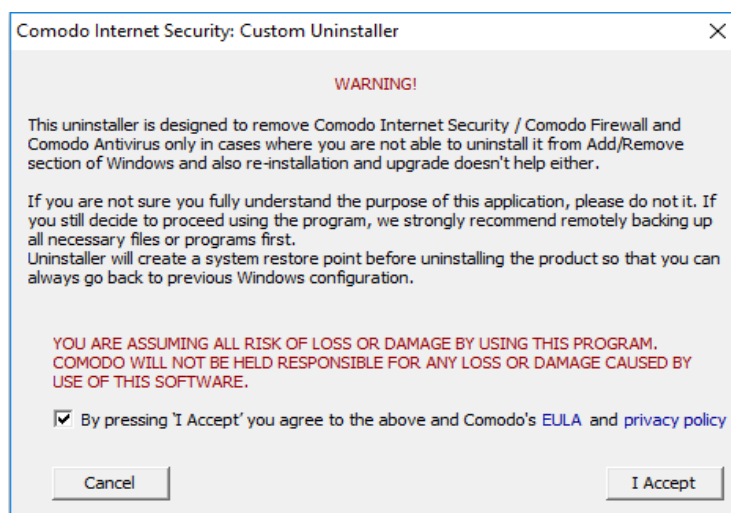
- Click 'Scan' to search for Comodo Internet security products. If the tool detects any of the specified products, click 'Continue' to remove them.
- Click 'Restart' after the cleanup process is complete.
- The tool requires a second restart to finalize the removal.

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 address) or a 128-bit number (IPv6 address). 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 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. 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**

Router - Enable 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).
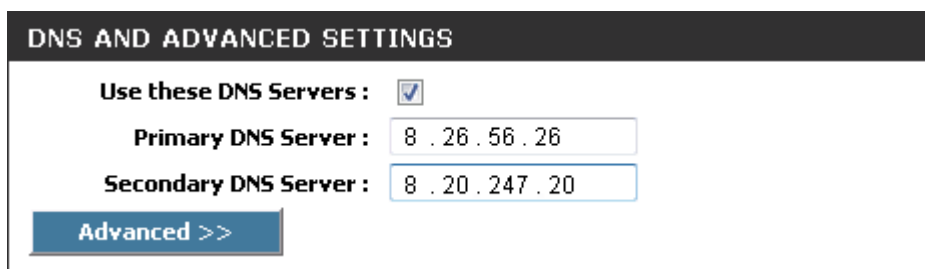
3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

   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.

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 - Enable Comodo Secure DNS

You can manually enable Comodo Secure DNS by changing your DNS server addresses to:

- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

Enable Comodo Secure DNS

1. Click the Windows 'Start' menu

2. Type 'control panel' into the search box then click the program name.
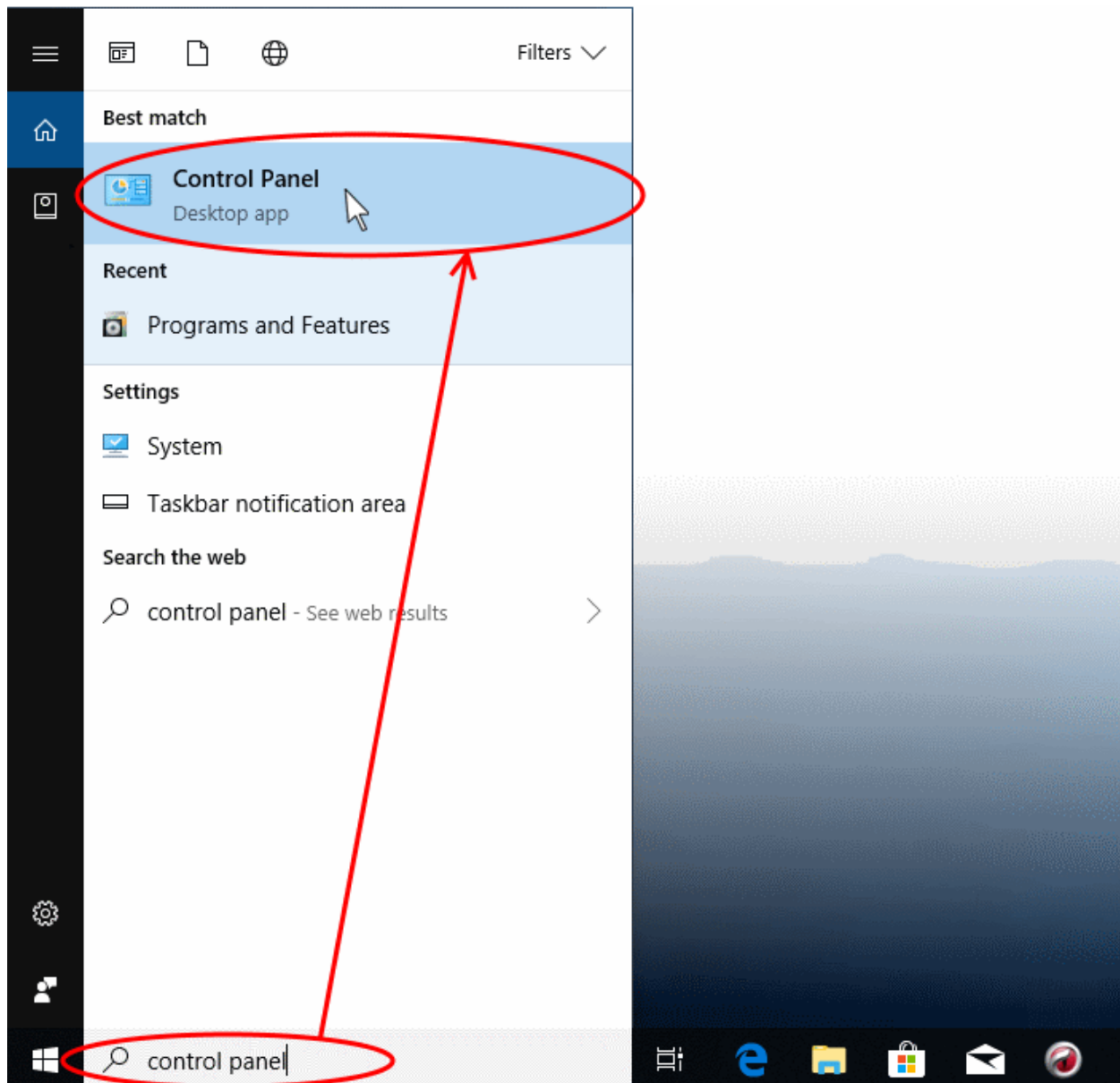
3. Select 'Network and Internet' from the control panel menu:

---
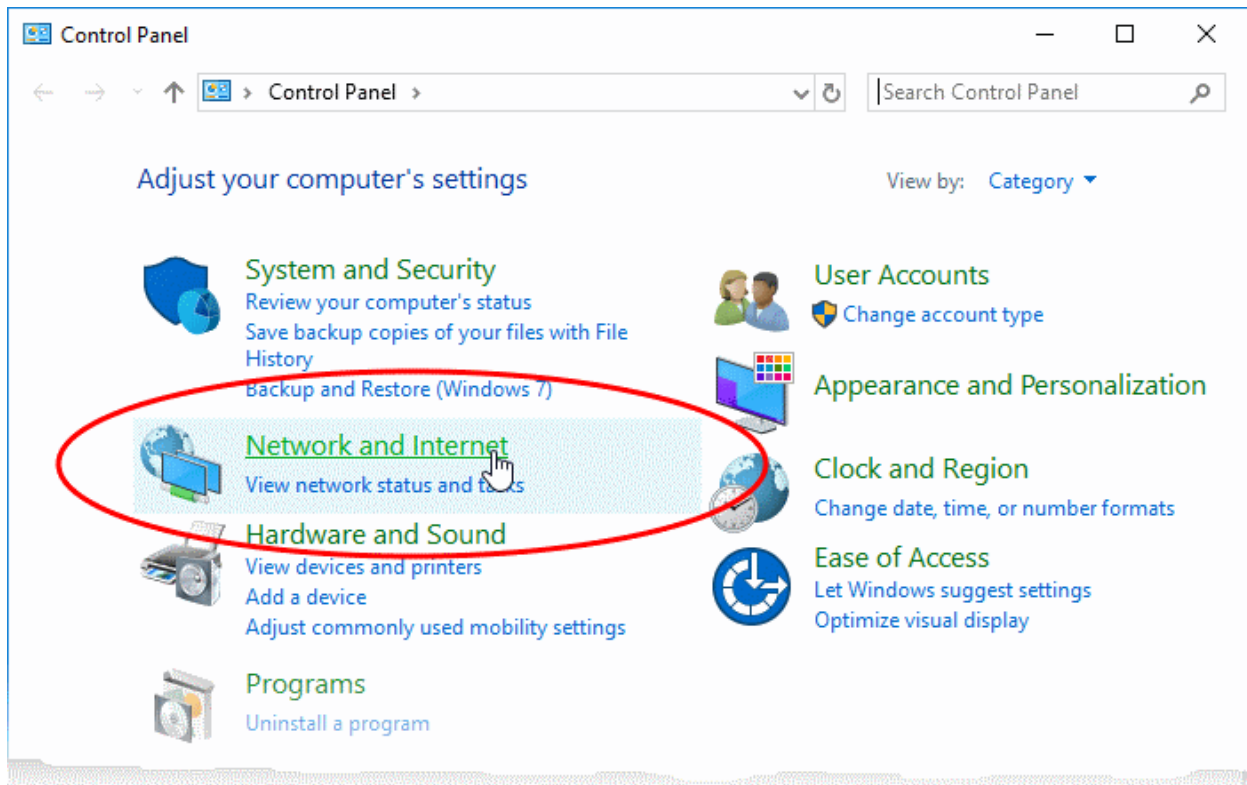
4. Select 'View network status and tasks' under Network and Sharing Center' as shown below:
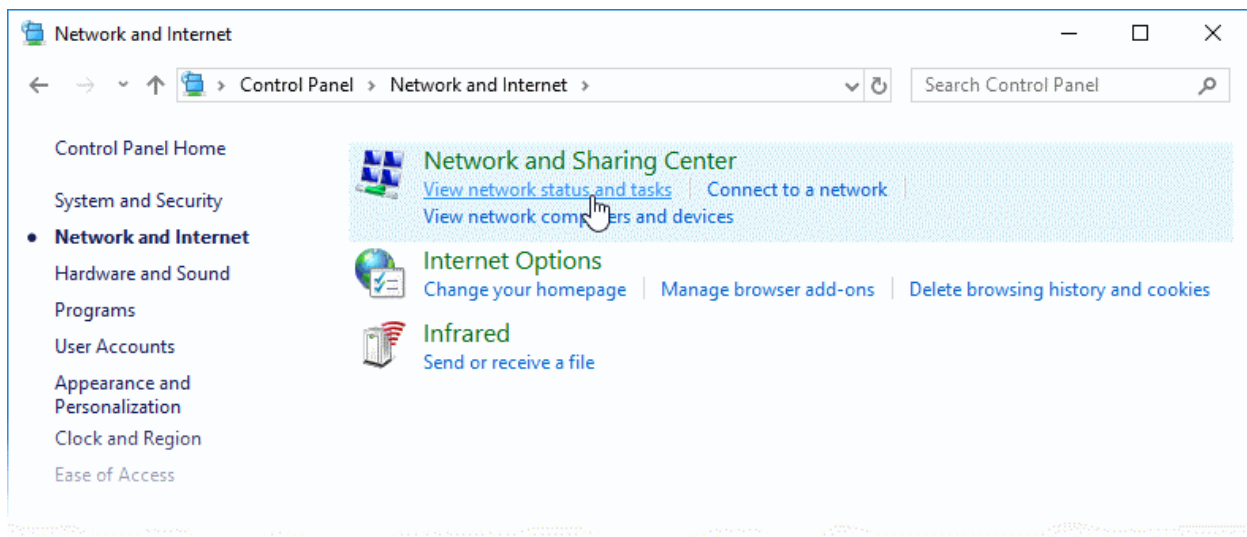
The list of networks to which you are currently connected is shown.

5. Click the network type link in the network through which you are connected to internet:
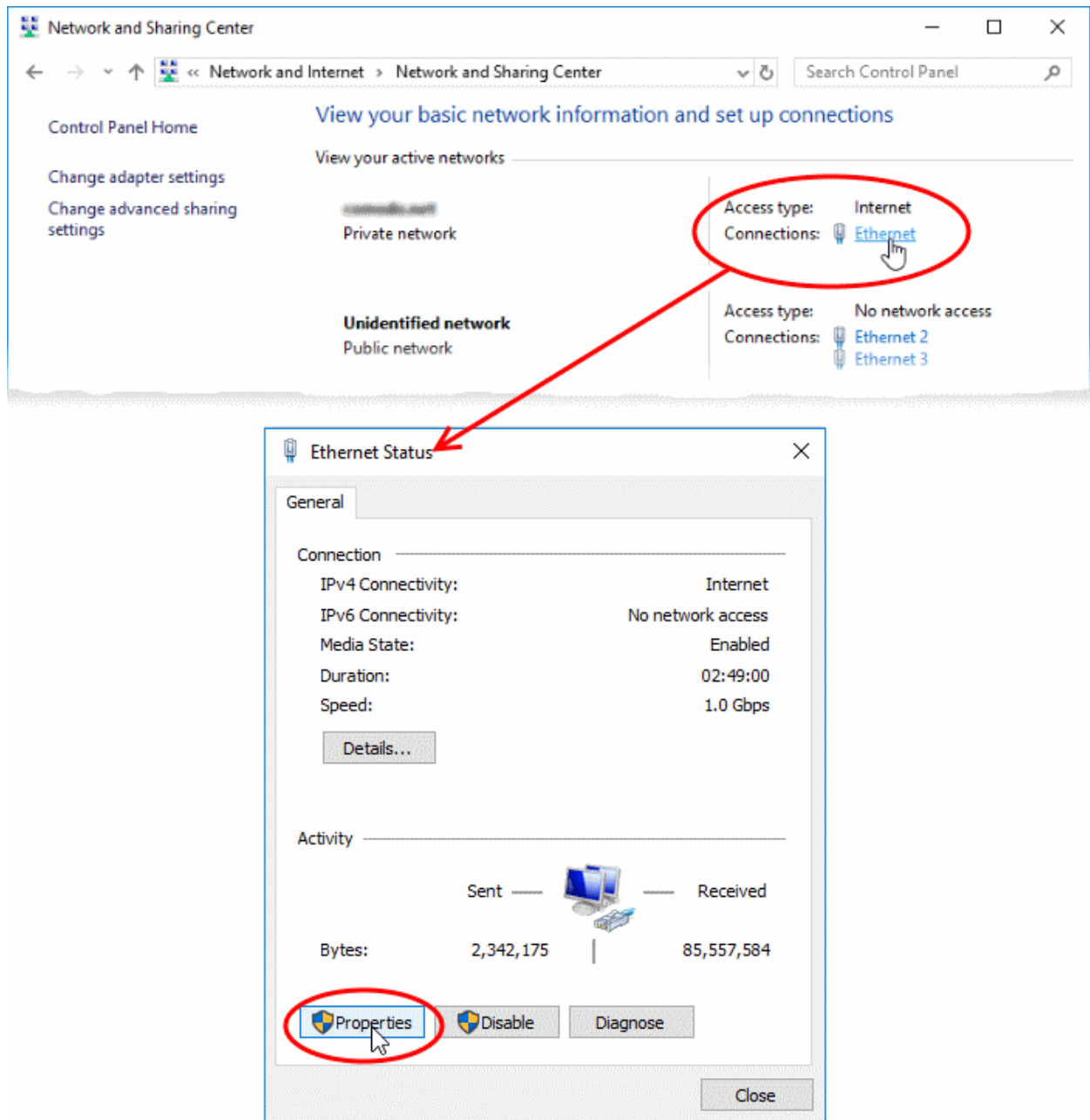
This opens the 'Status' dialog for the selected connection.

6. Click "Properties' in the status dialog

- At this point, Windows might ask for your permission to continue or request that you enter an administrator password.
- Once you have granted permission/entered an admin password, the 'Connection Properties' dialog appears:
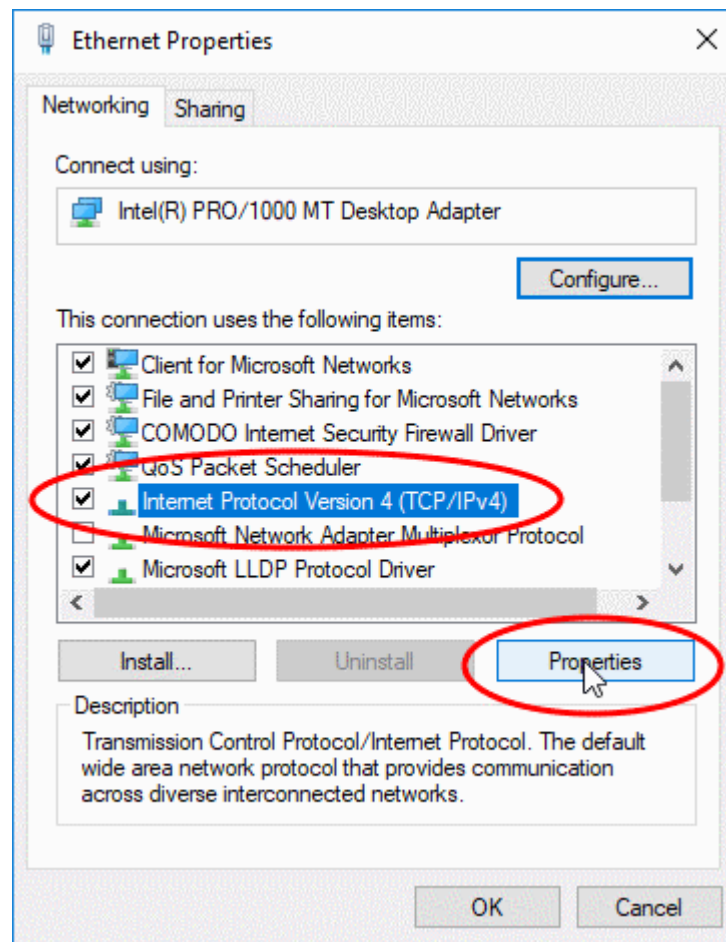
7. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button as shown above.

8. Enable 'Use the following DNS server addresses'.

9. Enter the addresses listed below:

    Preferred DNS : 8.26.56.26

    Alternate DNS : 8.20.247.20
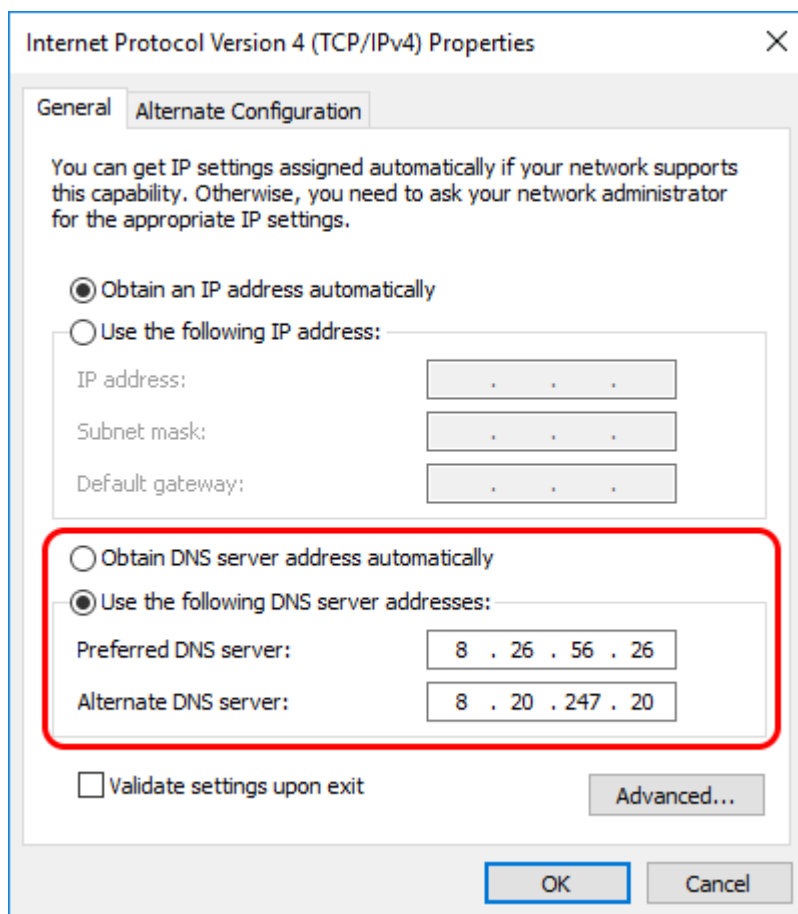
10. Click 'OK' to save your settings

11. Click 'OK' in the connection properties dialog to activate your settings

- Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the internet.

Disable Comodo DNS

You can revert to the DNS servers provided by your ISP at anytime by instructing Windows to automatically obtain the address of a DNS servers.

- Follow steps 1 to 7 of the '**Enable Comodo DNS**' tutorial to open the IP4 properties dialog

- Enable 'Obtain DNS server address automatically' then click 'OK'.
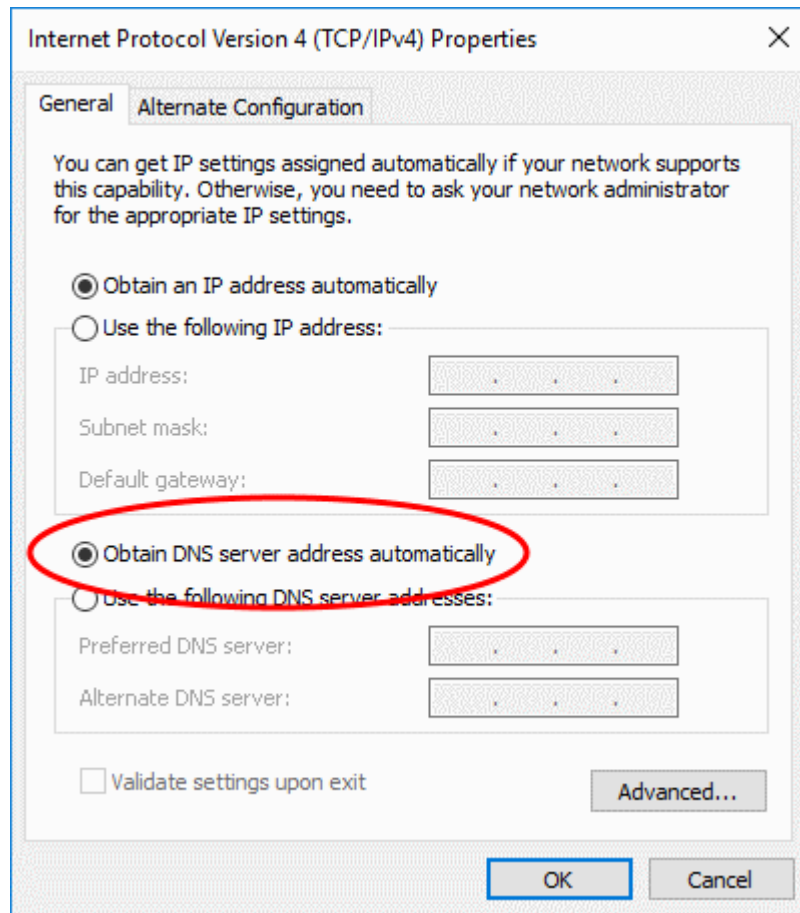
Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

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.

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.

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

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.

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.

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.

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.

Bug

Error in a program that cause problems.

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.

<div align="right">

Back to the top

</div>

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.

<div align="right">

Back to the top

</div>

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.

<div align="right">

Back to the top

</div>

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.

<div align="right">

Back to the top

</div>

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.

<div align="right">

Back to the top

</div>

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.

<div align="right">

Back to the top

</div>

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 - Premium, 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), Internet Security Essentials 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, Internet Security Essentials and a Acronis Backup Cloud account.

Product	Includes									Price*
	Antivirus	Firewall	GeekBuddy	TrustConnect	Acronis Back Up	Secure Shopping	Internet Security Essentials	Protection Plan Virus Free Guarantee (VFG) / Identity Protection (IDP)	Virus Removal Service	
CIS Premium	✔	✔	✔	✖	✖	✔	✔	✖	✖	$4.99/ per year
CIS Pro 12.x	✔	✔	✔	✖	✖	✔	✔	✔	✔	$4.99/ per year
CIS Complete 12.x	✔	✔	✔	✔ (10 GB / Month)	✔ (50 GB Free. Upgrades available)	✔	✔	✔	✔	$89.99 /year or $8.99/ month
CAV	✔	✖	✖	✖	✖	✖	✖	✖	✖	$4.99/ per year
Comodo Firewall	✖	✔	✖	✖	✖	✖	✖	✖	✖	$4.99/ per year

* 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.

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.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**