

COMODO
Creating Trust Online®



Comodo Client Security

Software Version 11.1

User Guide
Guide Version 11.1.022719

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

Table of Contents

1.Introduction to Comodo Client Security	6
1.1.Special Features.....	9
1.2.System Requirements.....	11
1.3.Install Comodo Client Security	12
1.4.Start Comodo Client Security.....	22
1.5.The Main Interface	26
1.5.1.The Home Screen.....	27
1.5.2.The Tasks Interface.....	31
1.5.3.The Widget.....	34
1.5.4.The System Tray Icon.....	35
1.6.Understand Security Alerts.....	37
2.General Tasks - Introduction	58
2.1.Scan and Clean Your Computer.....	58
2.1.1.Run a Quick Scan	60
2.1.2.Run a Full Computer Scan.....	62
2.1.3.Run a Rating Scan.....	66
2.1.4.Run a Custom Scan.....	69
2.1.4.1.Scan a Folder	70
2.1.4.2.Scan a File	72
2.1.4.3.Create, Schedule and Run a Custom Scan	74
2.1.5.Automatically Scan Unrecognized Files	83
2.2.Instantly Scan Files and Folders.....	86
2.3.Process Infected Files.....	88
2.4.Manage Virus Database Updates.....	91
2.5.Manage Blocked Autoruns.....	95
2.6.Manage Quarantined Items.....	98
3.Firewall Tasks - Introduction	101
3.1.Allow or Block Internet Access to Applications Selectively	102
3.2.Stealth your Computer Ports	104
3.3.Manage Network Connections.....	105
3.4.Stop all Network Activities.....	106
3.5.View Active Internet Connections.....	107
4.Containment Tasks - Introduction	111
4.1.Run an Application in the Container.....	113
4.2.Reset the Container.....	116
4.3.Identify and Kill Unsafe Running Processes.....	117
4.4.Open Shared Space.....	120
4.5.The Virtual Desktop.....	121
4.5.1.Start the Virtual Desktop.....	122
4.5.2.The Main Interface	124
4.5.3.Run Browsers inside the Virtual Desktop.....	126

4.5.4.Open Files and Run Applications inside the Virtual Desktop.....	127
4.5.5.Close the Virtual Desktop.....	129
4.6.Containment Statistics Analyzer.....	133
5.Advanced Tasks - Introduction.....	137
5.1.Create a Rescue Disk	137
5.1.1.Download and Burn Comodo Rescue Disk.....	139
5.2.Remove Deeply Hidden Malware	143
5.3.Manage CCS Tasks.....	146
5.4.View CCS Logs.....	150
5.4.1.Antivirus Logs.....	152
5.4.1.1.Filter Antivirus Logs.....	153
5.4.2.VirusScope Logs.....	158
5.4.2.1.Filter VirusScope Logs.....	160
5.4.3.Firewall Logs.....	165
5.4.3.1.Filter Firewall Logs.....	167
5.4.4.HIPS Logs.....	175
5.4.4.1.Filter HIPS Logs	176
5.4.5.Containment Logs.....	180
5.4.5.1.Filter Containment Logs.....	182
5.4.6.Device Control Logs.....	189
5.4.6.1.Filter 'Device Control' Logs.....	190
5.4.7.Autorun Logs.....	194
5.4.7.1.Filter 'Autorun' Logs.....	195
5.4.8.'Alerts' Logs.....	201
5.4.8.1.Filter 'Alerts' Logs.....	202
5.4.9.CCS Tasks Logs.....	210
5.4.9.1.Filter 'Tasks' Logs.....	212
5.4.10.File List Changes Logs.....	217
5.4.10.1.Filter 'File List Changes' Logs.....	218
5.4.11.Vendor List Change Logs.....	225
5.4.11.1.Filter 'Vendor List Changes' Logs.....	226
5.4.12.Configuration Changes.....	233
5.4.12.1.Filter 'Configuration Changes' Logs.....	235
5.5.Submit Files for Analysis to Comodo	240
5.6.View Active Process List.....	242
6.CCS Advanced Settings.....	246
6.1.General Settings.....	249
6.1.1.Customize User Interface.....	250
6.1.2.Configure Virus Database Updates.....	253
6.1.3.Log Settings.....	256
6.1.4.Manage CCS Configurations.....	259
6.1.4.1.Comodo Preset Configurations.....	260
6.1.4.2.Import/Export and Manage Personal Configurations.....	260

6.2.Antivirus Configuration	267
6.2.1.Real-time Scanner Settings.....	268
6.2.2.Scan Profiles.....	271
6.3.Firewall Configuration.....	279
6.3.1.General Firewall Settings.....	281
6.3.2.Application Rules.....	285
6.3.3.Global Rules.....	300
6.3.4.Firewall Rule Sets.....	302
6.3.5.Network Zones.....	305
6.3.5.1.Network Zones.....	306
6.3.5.2.Blocked Zones.....	312
6.3.6.Port Sets.....	316
6.4.HIPS Configuration	319
6.4.1.HIPS Settings.....	321
6.4.2.Active HIPS Rules.....	326
6.4.3.HIPS Rule Sets.....	336
6.4.4.HIPS Groups.....	340
6.4.4.1.Registry Groups.....	341
6.4.4.2.COM Groups.....	344
6.5.Protected Objects.....	349
6.5.1.Protected Objects – HIPS.....	349
6.5.1.1.Protected Files.....	350
6.5.1.2.Blocked Files.....	361
6.5.1.3.Protected Registry Keys.....	367
6.5.1.4.Protected COM interfaces.....	370
6.5.2.Protected Objects - Containment.....	373
6.5.2.1.Protected Data Folders.....	373
6.5.2.2.Protected Keys.....	378
6.6.Containment Configuration	381
6.6.1.Containment - An Overview.....	382
6.6.2.Unknown Files: The Scanning Processes.....	383
6.6.3.Containment Settings.....	384
6.6.4.Auto-Containment Rules.....	391
6.6.5.Virtual Desktop Settings.....	419
6.7.File Rating Configuration.....	420
6.7.1.File Rating Settings.....	422
6.7.2.File Groups.....	424
6.7.3.File List.....	431
6.7.4.Submitted Files.....	445
6.7.5.Vendor List.....	447
6.8.Advanced Protection.....	459
6.8.1.VirusScope Settings	460
6.8.2.Exclusions.....	462

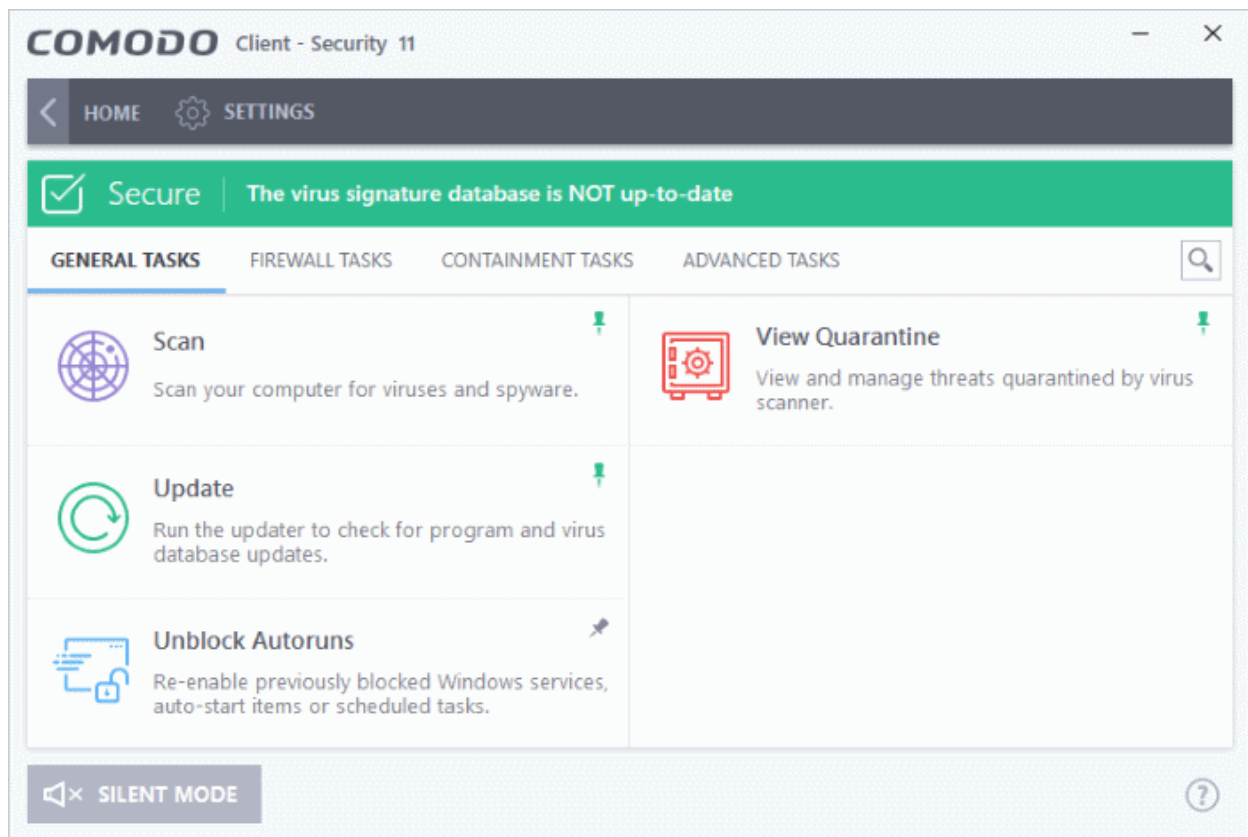
6.8.3.Device Control Settings.....	477
6.8.4.Script Analysis Settings.....	485
6.8.5.Miscellaneous Settings	492
Appendix 1 - CCS How to... Tutorials.....	496
Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily.....	496
Set up the Firewall For Maximum Security and Usability.....	499
Block Internet Access while Allowing Local Area Network (LAN) Access.....	506
Set up HIPS for Maximum Security and Usability.....	511
Create Rules to Auto-Contain Applications.....	513
Run an Instant Antivirus Scan on Selected Items.....	539
Create an Antivirus Scan Schedule.....	540
Run Untrusted Programs inside the Container.....	547
Run Browsers Inside the Container.....	551
Restore Incorrectly Quarantined Item(s).....	553
Submit Quarantined Items to Comodo for Analysis.....	555
Enable File Sharing Applications like BitTorrent and Emule.....	557
Block any Downloads of a Specific File Type.....	562
Disable Auto-Containment on a Per-application Basis	565
Switch Off Automatic Antivirus Updates.....	570
Suppress CCS Alerts Temporarily	572
Control External Device Accessibility.....	573
Appendix 2 - Comodo Secure DNS Service.....	575
Router - Manually Enable or Disable Comodo Secure DNS Service.....	576
Windows XP - Manually Enable or Disable Comodo Secure DNS Service.....	577
Windows 7 / Vista - Manually Enable or Disable Comodo Secure DNS Service.....	582
About Comodo Security Solutions.....	588

1. Introduction to Comodo Client Security

Overview

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

When used individually, each of these modules delivers superior protection against their specific threat challenge. When used together they provide a complete 'prevention, detection and cure' security system for your computer. Once installed on a Windows endpoint, CCS can be remotely configured and monitored from the Endpoint Manager console.



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 Client Security - Key Features:

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

from taking potentially damaging actions. Unrecognized processes and applications will be automatically run inside a security hardened environment known as a container. Once inside, they will be strictly monitored, will not be able to access other processes and will write to a virtual file system and registry. This gives untrusted (but harmless) applications the freedom to operate while untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

- **Advanced Protection** - A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
 - **Viruscope** - Monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Using a system of behavior 'recognizers', Viruscope 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.
- **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** - The advanced tasks section contains links that allow you to install other, free, Comodo security products - Comodo Cleaning Essentials and KillSwitch.

Guide Structure

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

- **Introduction**
 - **Special Features**
 - **System Requirements**
 - **Installation**
- **Starting Comodo Client Security**
- **The Main Interface**
- **Understanding Security Alerts**

The next four sections of the guide cover every aspect of the configuration of Comodo Client Security.

- **General Tasks - Introduction**
 - **Scan and Clean your Computer**
 - **Run a Quick Scan**
 - **Run a Full Computer Scan**
 - **Run a Rating Scan**
 - **Run a Custom Scan**
 - **Automatically Scan Unrecognized Files**
 - **Instantly Scan Files and Folders**
 - **Processing Infected Files**
 - **Manage Virus Database and Program Updates**
 - **Manage Blocked Autoruns**
 - **Manage Quarantined Items**
- **Firewall Tasks - Introduction**
 - **Allow or Block Internet Access to Applications Selectively**
 - **Stealth your Computer Ports**
 - **Manage Network Connections**
 - **Stop all Network Activities**

- **View Active Internet Connections**
- **Containment Tasks - Introduction**
 - **Run an Application in the Container**
 - **Reset the Container**
 - **Identify and Kill Unsafe Running Processes**
 - **Open Shared Space**
 - **The Virtual Desktop**
 - **Containment Statistics Analyzer**
- **Advanced Tasks - An Introduction**
 - **Create a Rescue Disk**
 - **Remove Deeply Hidden Malware**
 - **Manage CCS Tasks**
 - **View CCS Logs**
 - **Submit Files**
 - **View Active Process List**
- **CCS Advanced Settings**
 - **General Settings**
 - **Customize User Interface**
 - **Configure Program and Virus Database Updates**
 - **Log Settings**
 - **Manage CCS Configurations**
 - **Antivirus Configuration**
 - **Real-time Scanner Settings**
 - **Scan Profiles**
 - **Firewall Configuration**
 - **General Firewall Settings**
 - **Application Rules**
 - **Global Rules**
 - **Firewall Rule Sets**
 - **Network Zones**
 - **Port Sets**
 - **HIPS Configuration**
 - **HIPS Settings**
 - **Active HIPS Rules**
 - **HIPS Rule Sets**
 - **Protected Objects - HIPS**
 - **HIPS Groups**
 - **Containment Configuration**
 - **Containment - An Overview**
 - **Unknown Files: The Scanning Processes**
 - **Containment Settings**
 - **Auto-Containment Rules**

- Protected Objects – Containment
- Virtual Desktop Settings
- File Rating Configuration
 - File Rating Settings
 - File Groups
 - File List
 - Submitted Files
 - Vendor List
- Advanced Protection Configuration
 - VirusScope Settings
 - Exclusions
 - Device Control Settings
 - Script Analysis Settings
 - Miscellaneous Settings
- Appendix 1 - CCS How to... Tutorials
 - Enable / Disable AV, Firewall, Auto-Containment and Viruscope Easily
 - Set up the Firewall For Maximum Security and Usability
 - Block Internet Access while Allowing Local Area Network (LAN) Access
 - Set up the HIPS for Maximum Security and Usability
 - Create Rules for Auto-Containing Applications
 - Run an Instant Antivirus Scan on Selected Items
 - Create an Antivirus Scanning Schedule
 - Run Untrusted Programs inside the Container
 - Run Browsers Inside the Container
 - Restore Incorrectly Quarantined Item(s)
 - Submit Quarantined Items to Comodo for Analysis
 - Enable File Sharing Applications like BitTorrent and Emule
 - Block any Downloads of a Specific File Type
 - Disable Auto-Containment on a Per-application Basis
 - Switch Off Automatic Antivirus and Software Updates
 - Suppress CCS Alerts Temporarily
 - Control External Device Accessibility
- Appendix 2 - Comodo Secure DNS Service

1.1. Special Features

Auto-Containment

- Automatically runs unknown files inside a secure container which is isolated from the rest of your computer
- Contained programs cannot cause damage because they are denied access to the operating system, to the registry, and to user data
- This nullifies malware and ransomware by totally removing their ability to interact with the host computer
- Simultaneously, the file is analyzed by our cloud systems to establish the trust rating of the file

Viruscope

- 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

- 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.

Comprehensive Antivirus Protection

- Detects and eliminates viruses from desktops, laptops and workstations;
- Cloud based scans mean you still get 100% protection even if your database is outdated.
- Heuristic techniques identify previously unknown viruses and Trojans;
- Scans registry and system files for possible spyware infection and cleans them;
- Highly configurable on-demand scanner lets you run custom scans on any file, folder or drive;
- Daily, automatic updates of virus definitions;
- Automatically scans external devices when they are plugged in;
- 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

- Summary screen 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 Client Security - Extended Features

Highly Configurable Security Rules Interface

Comodo Client 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 Client 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 Client 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.

Event logging

Comodo Client Security features a vastly improved log management module - allowing users to export records of Antivirus, Firewall and Advanced Protection activities according to several user-defined filters. Beginners and advanced users alike are greatly benefited from this essential troubleshooting feature.

Memory Firewall Integration

Comodo Client 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 'Clean PC' 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. CCS 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 Client Security's 'Containment' 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 CCS to complement and strengthen the Firewall, Advanced Protection, Containment 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.

Device Control

CCS allows you full control over which type of external devices, such as USB pen drives and hard drives, can be connected to endpoints. Allow selected device class or block them all.

1.2. System Requirements

For Comodo Client Security to perform optimally, please ensure your systems comply with the following minimum system requirements:

Windows Endpoints

Windows 10 (Both 32-bit and 64-bit versions)	• 384 MB available RAM
--	------------------------

Windows 8 (Both 32-bit and 64-bit versions) Windows 7 (Both 32-bit and 64-bit versions) Windows Vista (Both 32-bit and 64-bit versions)	<ul style="list-style-type: none"> • 210 MB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer Version 5.1 or above
Windows XP (Both 32-bit and 64-bit versions)	<ul style="list-style-type: none"> • 256 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer Version 5.1 or above

Windows Servers

- Windows Server 2003
- Windows Small Business Server 2003
- Windows Server 2008
- Windows Small Business Server 2008
- Windows Server 2008 R2
- Windows Small Business Server 2011
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

All operating systems

You will also need to open some ports on your firewall to allow updates and various C1/ITarian services to function correctly:

- USA customers - [Click here](#) for port information
- EU customers - [Click here](#) for port information

1.3. Install Comodo Client Security

You can use the Endpoint Manager (EM) interface to deploy Comodo Client Security (CCS) to your endpoints. You can purchase EM as stand-alone application or as a part of the Comodo One (C1)/ITarian portal.

Please see the following links if you do not already have an EM license:

- **C1 / ITarian** - Sign up for C1 at <https://one.comodo.com/>, or for ITarian at <https://www.itarian.com/>
 - After signup, login and click 'Licensed Applications > 'Endpoint Manager'.
- **Stand-alone Endpoint Manager**
 - Visit <https://secure.comodo.com/home/purchase.php?pid=98&license=try> for the trial version or <https://secure.comodo.com/home/purchase.php?pid=98> for the full version.
 - After signup you can access your EM instance at the URL provided during setup.

The following tutorial covers user and device enrollment before moving onto CCS installation:

- **Step 1 - Enroll Users**
- **Step 2 - Enroll Devices**
- **Step 3 - Deploy CCS**


Note - you can skip to step 3 if you have already enrolled your target devices.

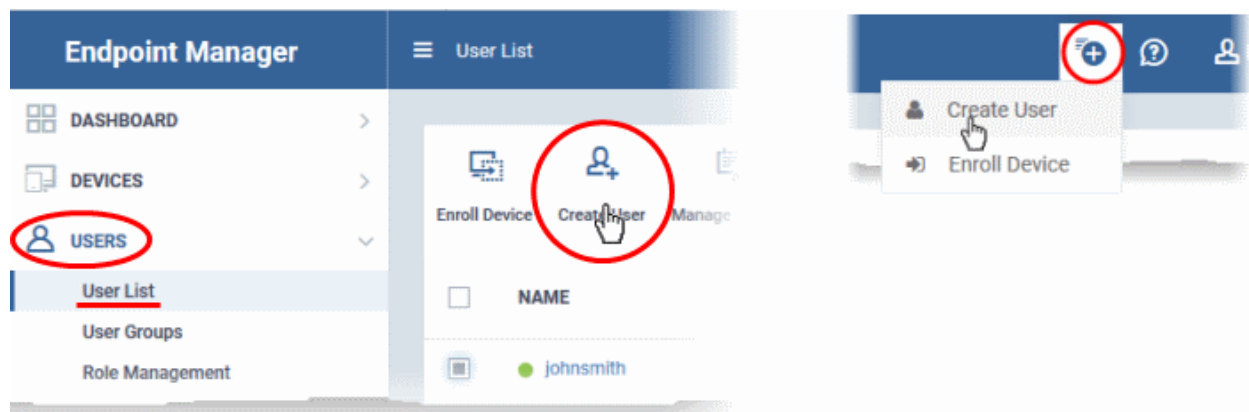
Step 1 - Enroll Users

You can deploy CCS onto endpoints only after adding users to Endpoint Manager.

- **Comodo One/ITarian users** - You can create multiple companies in C1/ITarian, and can enroll users to any of these companies as required.
- **Endpoint Manager Users** - All users are enrolled to the default company.

To add a user

- Click 'Users' > 'User List' > click the 'Create User' button
or
- Click the 'Add' button  on the menu bar and choose 'Create User'.



The 'Create new user' form will open.

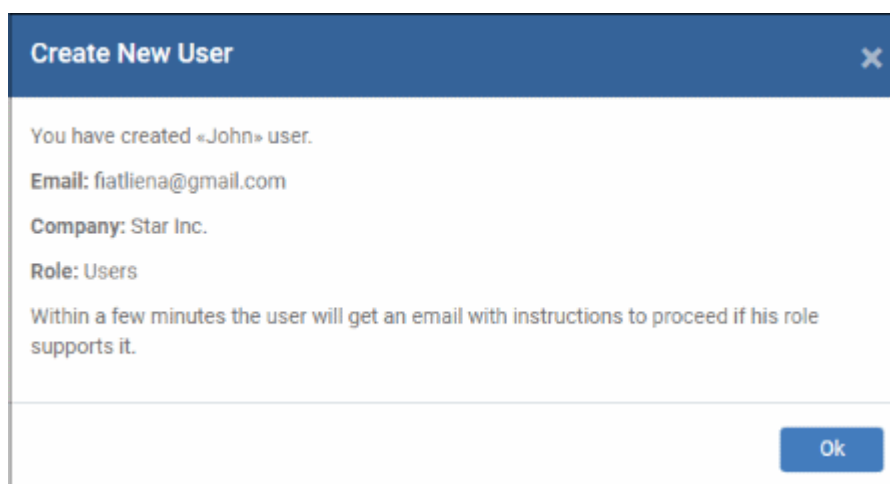
The screenshot shows a 'Create New User' dialog box. It has a blue header with the text 'Create New User' and a close button (X). Below the header are five input fields: 'User Name*' containing 'John', 'Email*' containing 'fiatliena@gmail.com', 'Phone Number' containing 'Phone Number', 'Company*' containing 'Star Inc.', and 'Assign Role' containing 'Users'. At the bottom right of the form is a blue 'Submit' button.

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- **Company**
 - **Comodo One/ITarian Users** - The drop-down shows all companies you have added to C1 / ITarian. Choose the company under which you want to enroll the user.
 - Endpoint Manager users - Leave the selection as 'Default Company'.
- **Role**

A 'role' determines user permissions within the Endpoint Manager console itself. Endpoint Manager ships with two default roles:

- **Administrators** - Full administrative privileges in the Endpoint Manager console. The permissions for this role are not editable.
 - **Users** - In most cases, a 'user' will simply be an owner of a managed device who should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

You will see a confirmation message as follows:



- Repeat the process to add more users.
- New users will be listed in the 'Users' interface (click 'Users' > 'User List')


Step 2 - Enroll Devices

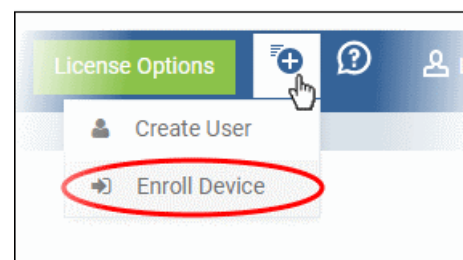
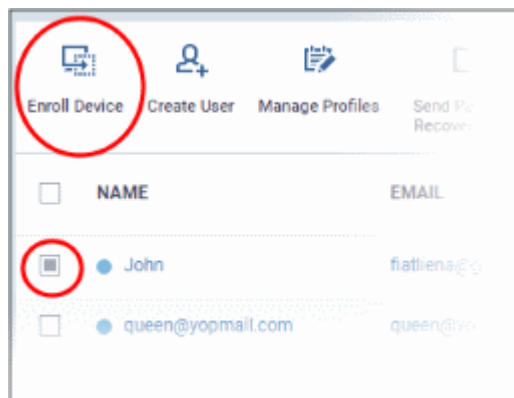
The next step is to enroll user devices. Afterwards, you will be able to manage the devices using Endpoint Manager.

To enroll devices

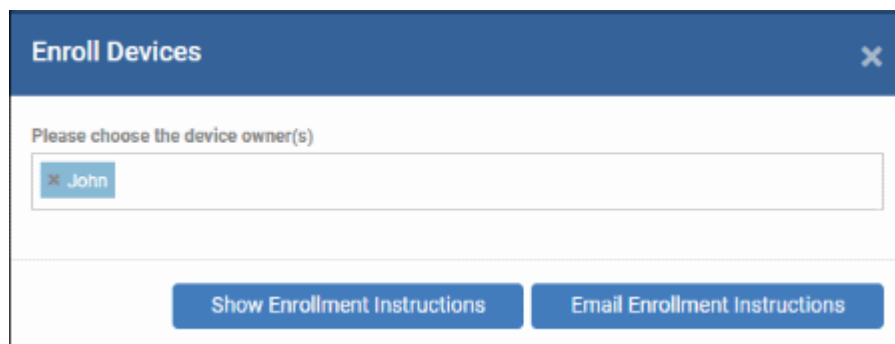
- Click 'Users' then 'User List'
- Select the user(s) whose devices you wish to enroll then click the 'Enroll Device' button

Or

Click the 'Add' button  on the menu bar and choose 'Enroll Device'.

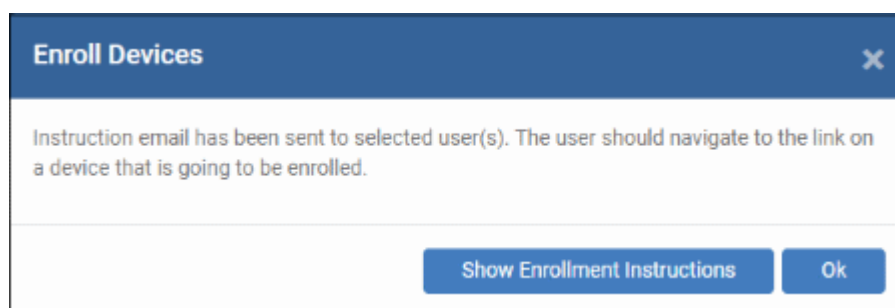


The 'Enroll Devices' dialog will open:

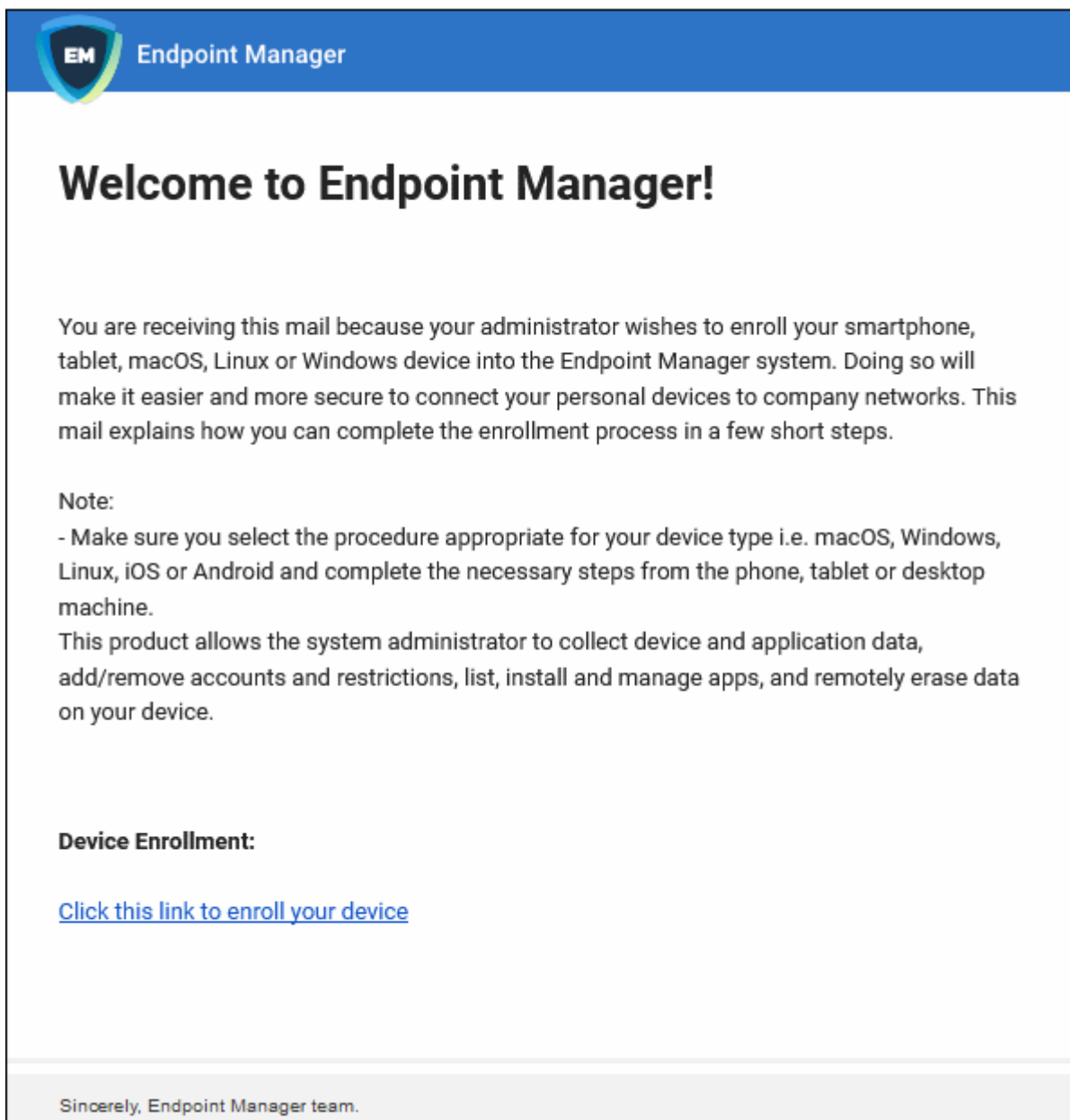


The device owners field is pre-populated with the users you selected in the previous step.

- To add more users, start typing first few letters of their username and choose from the results
- **Show Enrollment Instructions** - Displays enrollment advice in a pop-up. Useful for administrators attempting to enroll their own devices.
- **Email Enrollment Instructions** - Will send device enrollment instructions to all selected users. Users must enroll their own devices by following the instructions in the email. The following confirmation message will be shown after clicking this button:



An example mail is shown below:



EM Endpoint Manager

Welcome to Endpoint Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, macOS, Linux or Windows device into the Endpoint Manager system. Doing so will make it easier and more secure to connect your personal devices to company networks. This mail explains how you can complete the enrollment process in a few short steps.

Note:

- Make sure you select the procedure appropriate for your device type i.e. macOS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, tablet or desktop machine.


This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Device Enrollment:

[Click this link to enroll your device](#)

Sincerely, Endpoint Manager team.

- Clicking the link will take the user to the enrollment page containing the agent/profile download and configuration links.




Welcome to Endpoint Manager!


You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, macOS, Linux or Windows device into the Endpoint Manager system. Doing so will make it easier and more secure to connect your personal devices to company networks. This mail explains how you can complete the enrollment process in a few short steps.

NOTE:
Make sure you select the procedure appropriate for your device type i.e. mac OS, Windows, Linux, iOS or Android and complete the necessary steps from the phone, tablet or desktop machine.

This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

 **FOR WINDOWS DEVICES**

Enroll using this link:
<https://domeaspchennai-domeaspchennai-msp.dmdemo.comodo.com:443/enroll/windows/msi/token/c400cf0776dd77b625b1bbd8a80a097a>

 **FOR APPLE DEVICES**

- Click on the enrollment link under 'For Windows Devices'.

The Endpoint Manager agent setup file will be downloaded.

- Double click on the file to install the agent.

When installation is complete, the device will be automatically enrolled to Endpoint Manager and a confirmation message will be displayed. Once the device is enrolled, the next step is to install CCS onto the endpoint.

Background Note on Endpoint Manager Agent:

- The agent is a small application installed on managed endpoints to facilitate communication between the endpoint and the Endpoint Manager server.
- The agent is responsible for receiving tasks and passing them to Comodo Client Security.
 - Example tasks include changes in security policy, run a virus scan, update the local antivirus database or gather reports that have been requested by the central service.
- For security reasons, agents can only communicate with the instance of Endpoint Manager which provisioned the agent. This means the agent cannot be reconfigured to connect to any other Endpoint Manager service.

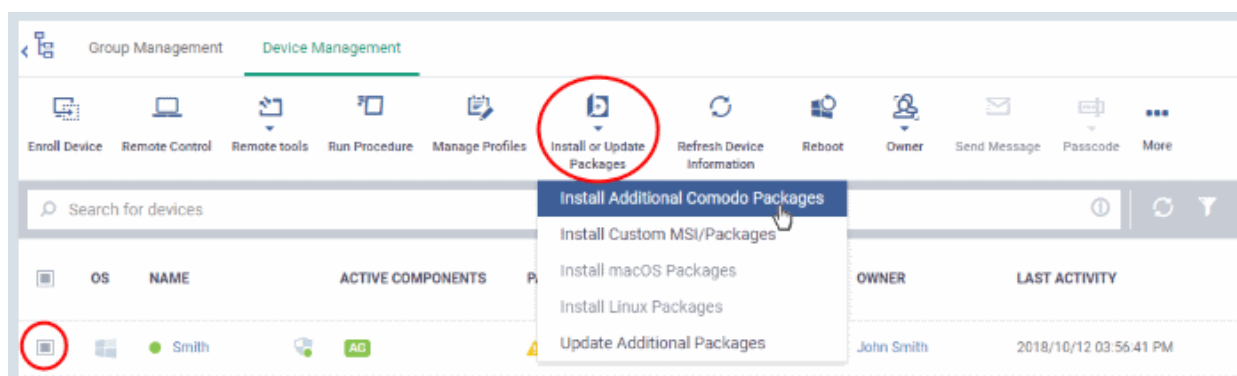
Step 3 - Deploy Comodo Client Security

Note - Before beginning installation, please ensure you have uninstalled any other antivirus products on the endpoint. More specifically, remove any other products of the same type as those Comodo products you plan to install. For example, if you plan to install only the antivirus then you do not need to remove 3rd party firewall solutions and vice-versa. Failure to remove products of the same type could cause conflicts that mean CCS will not function correctly.

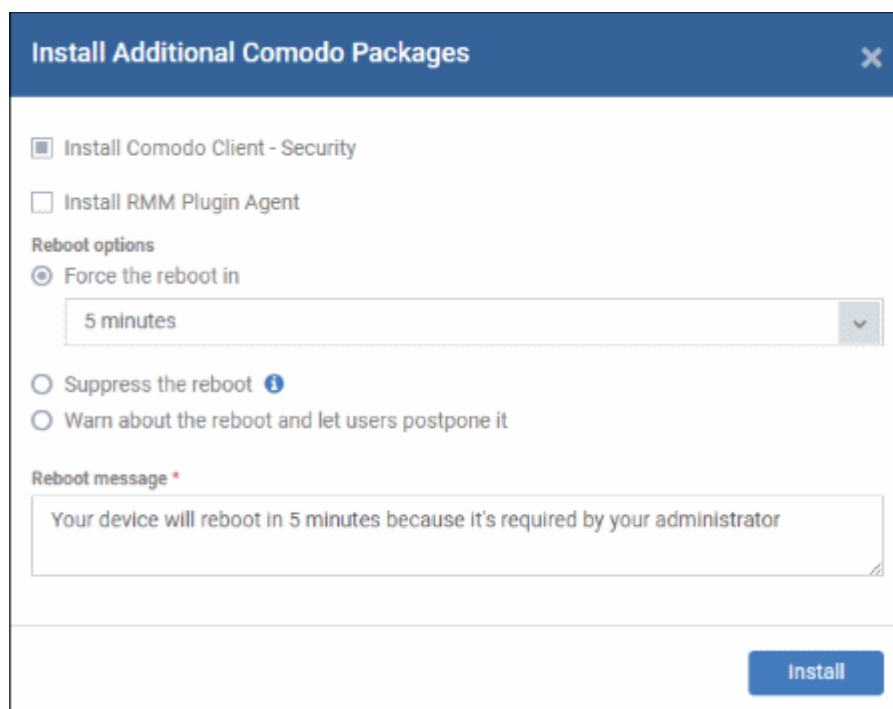
Endpoint Manager allows you to install Comodo applications such as Comodo Client Security (CCS) and other third-party MSI packages from the 'Device List' interface.

To install CCS

- Click 'Devices' and choose 'Device List'
- Select the Windows device(s) onto which you want install CCS



- Click 'Install or Update Packages' > 'Install Additional Comodo Packages'



- Select the 'Install Comodo One Client - Security' check box

CCS requires the endpoint to be restarted in order for the installation to take effect. You can choose how the endpoint(s) are to be restarted from the 'Reboot Options'.

- To restart the end-point after a certain period of time, choose 'Force the reboot in...', choose a time period and click 'Install'.

The following message will be displayed on the device after CCS is deployed on the endpoint:



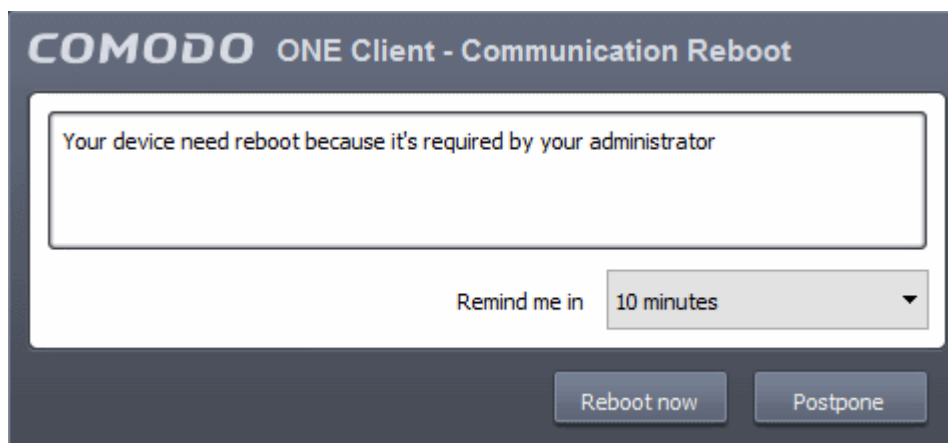
The device will be restarted automatically when the time period elapses.

- If you do not want the endpoint to restart automatically, then choose 'Suppress the reboot' and click 'Install'.

The endpoint will not restart after installation. However, CCS will not be fully functional until the endpoint is rebooted.

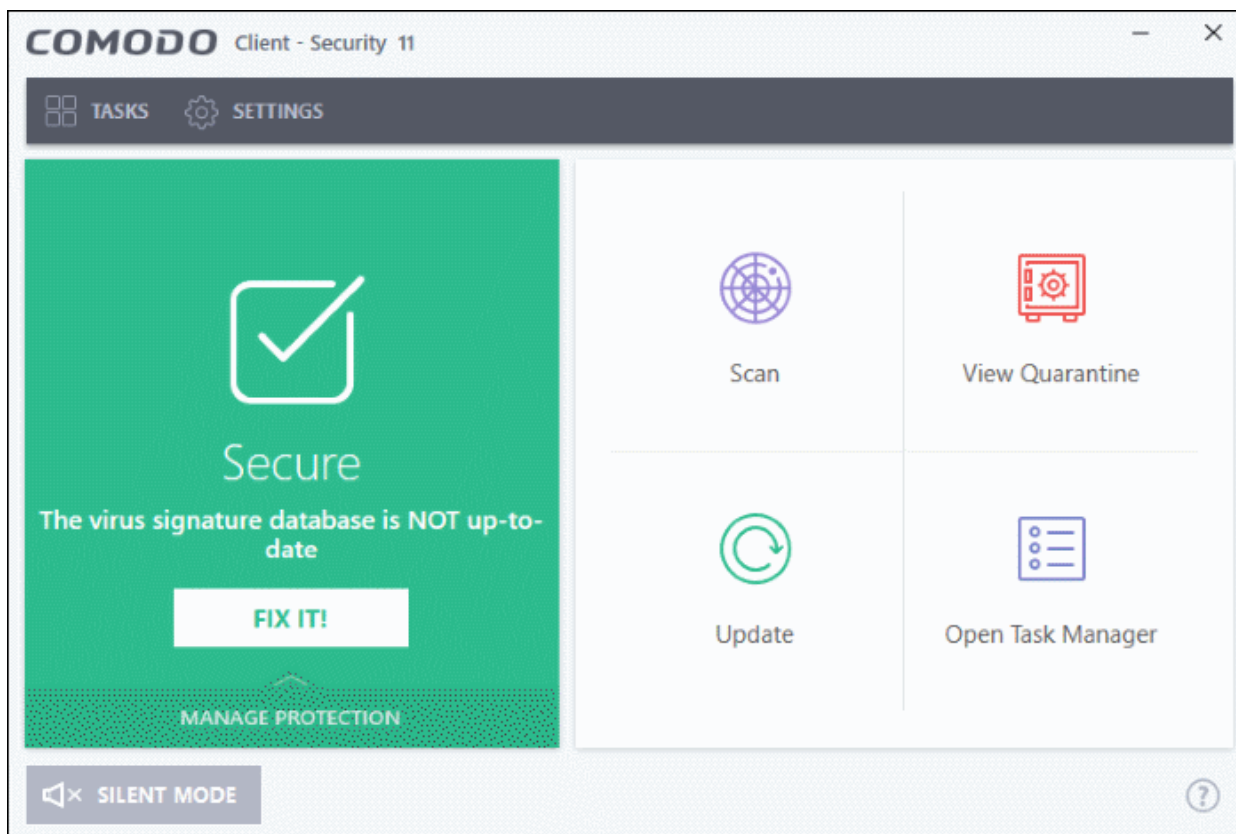
- To give users a choice over restarting, choose 'Warn about the reboot and let users postpone it'. Type a message to be shown to the user in the 'Reboot message' field and click 'Install'.

After installation, the message will be displayed on the device as follows:



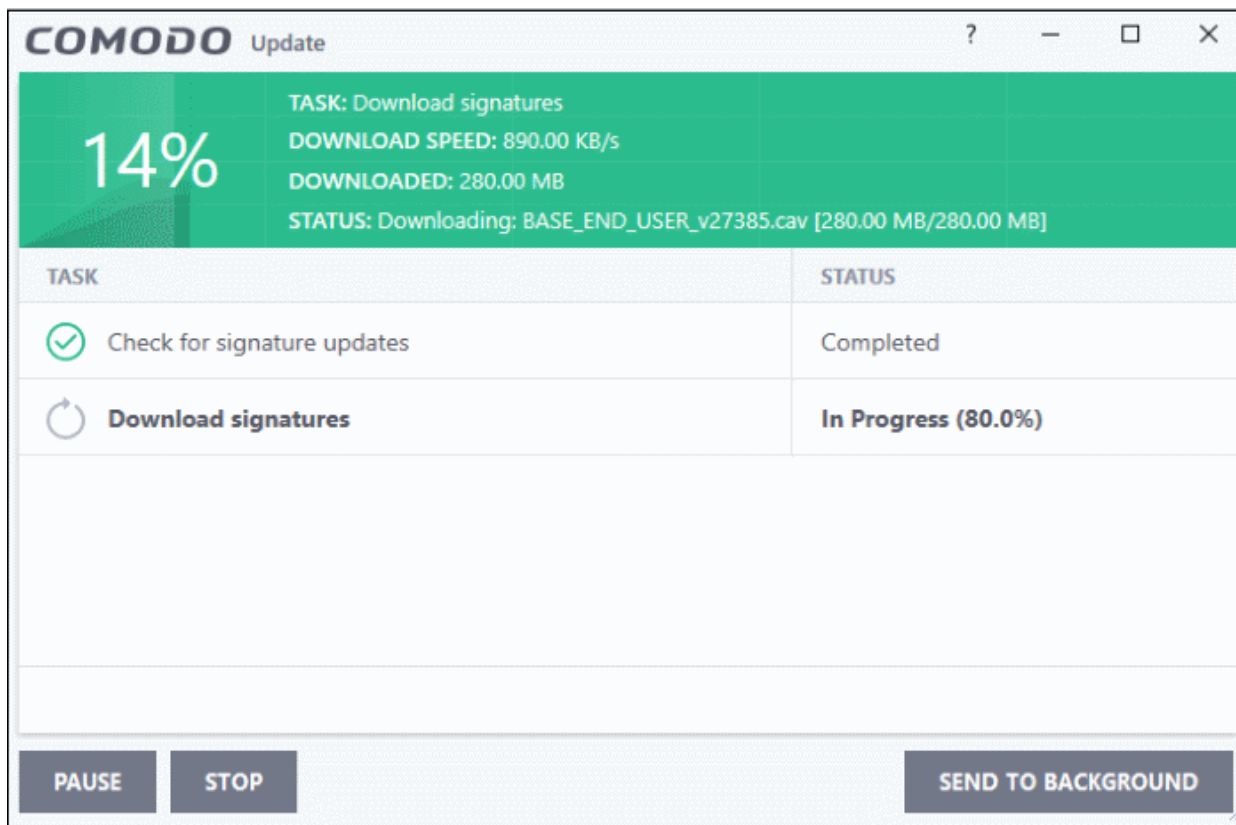
Users can choose to restart the endpoint immediately by clicking 'Reboot now', or postpone the restart by using the 'Remind me in' drop-down. The installation will be active only after the endpoint is restarted.

After installation, the security components that are active depends on the applied Endpoint Manager profile.

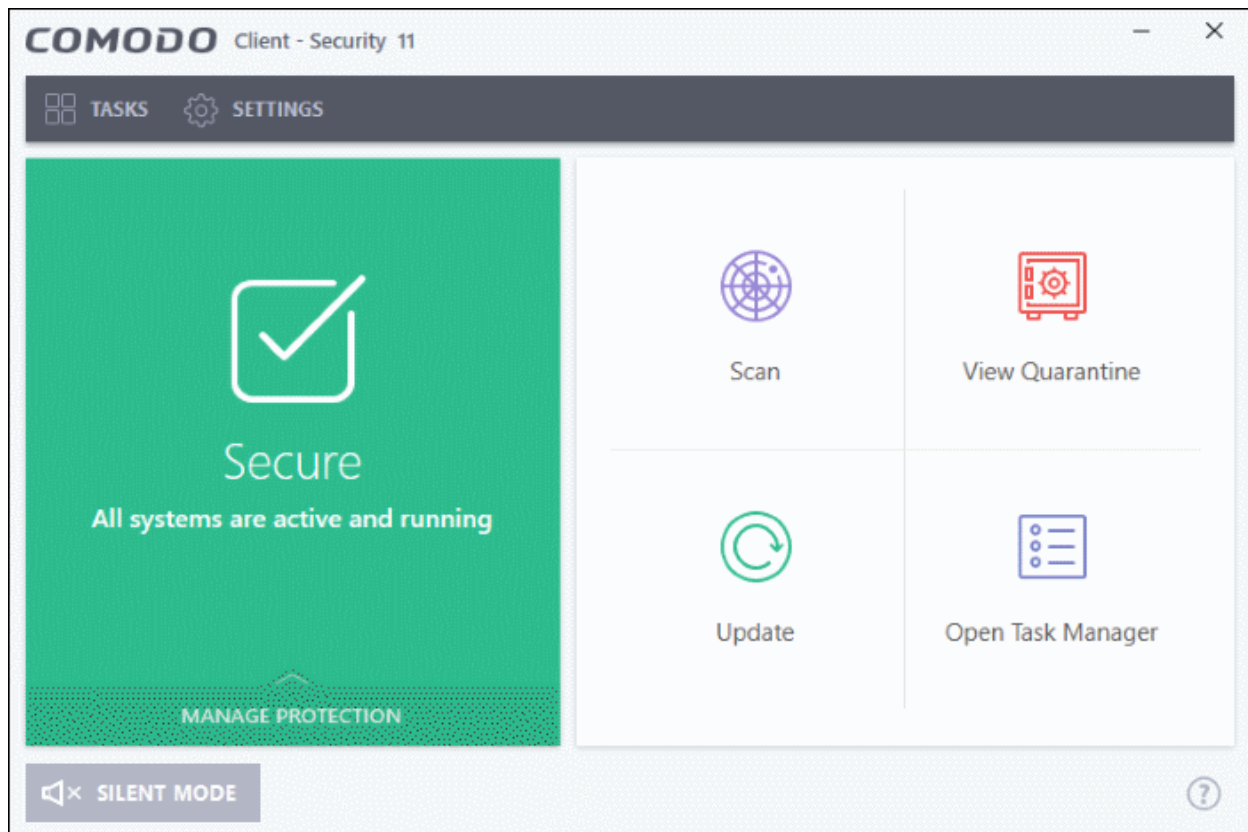


- Click 'Fix It!' to update the virus database.

The virus database will start downloading and...



... on completion, the virus signatures will be installed and system updated.



- Please note the settings in CCS will be configured automatically according to the applied Endpoint Manager profile.
- CCS will retain its default settings if no profiles are applied after installation. The default settings are mentioned in the guide for various configuration screens.
- CCS will retain the settings of the last applied profile if no profiles are applied at any point of time.
- Visit <https://help.comodo.com/topic-399-1-786-10197-Profiles-for-Windows-Devices.html> for more information about how to configure profiles in Endpoint Manager for Windows machines.

1.4. Start Comodo Client Security

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

There are 5 different ways to access the main interface of Comodo Client Security:

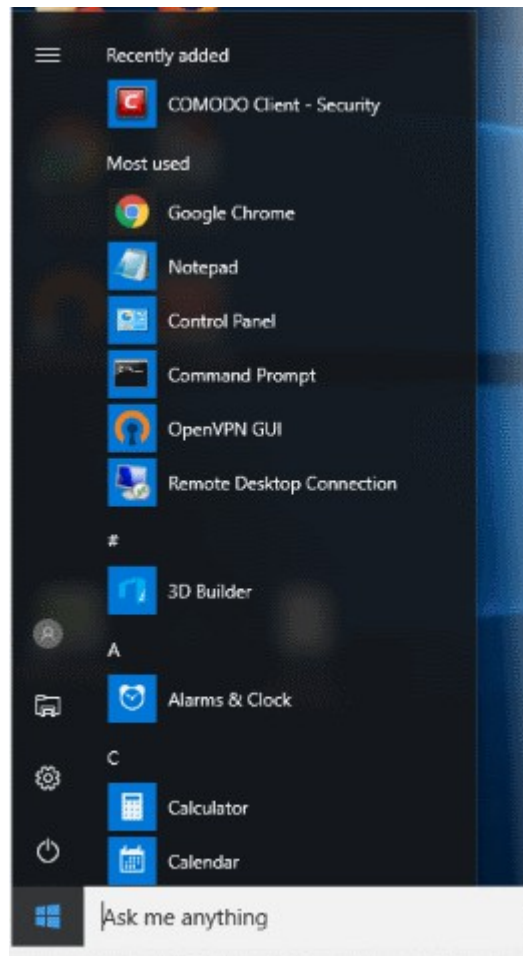
- **Windows Start Menu**
- **Windows Desktop**
- **Widget**
- **System Tray Icon**
- **Windows Defender**

Start Menu

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

- Click **Start** and select **All Apps > Comodo > Comodo Client Security**

(Please note the start menu varies slightly for different Windows versions.)



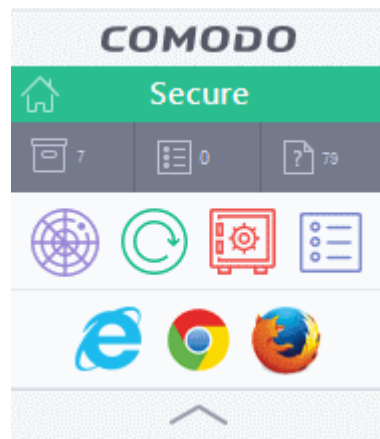
Windows Desktop

- Just double-click the desktop shortcut to start Comodo Client Security. The shortcut will only be visible if 'Show Desktop Shortcut' is enabled in the Endpoint Manager profile applied to the endpoint.



Widget

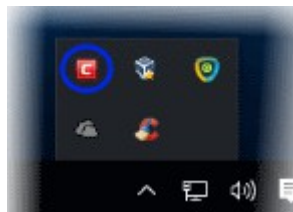
- Just click the information bar in the widget to start CCS. The widget will only be visible if 'Show Desktop Widget' is enabled in the Endpoint Manager profile applied to the endpoint.



The widget also contains other useful data and features. See '[The Widget](#)' for more details.

CCS Tray Icon

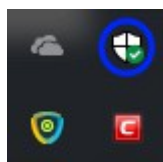
- Double-click the shield icon to start the main interface.



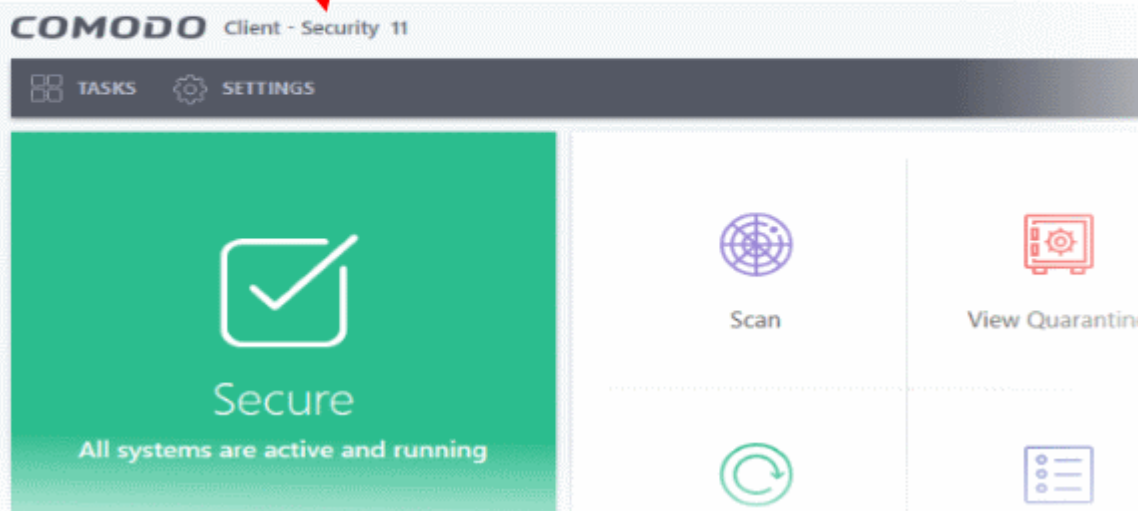
You can also right-click on the tray icon and select 'Open...!'

Windows Defender

- Double-click on the Windows Defender icon to open the application
OR
- Right-click on the tray icon and select 'Open...!'



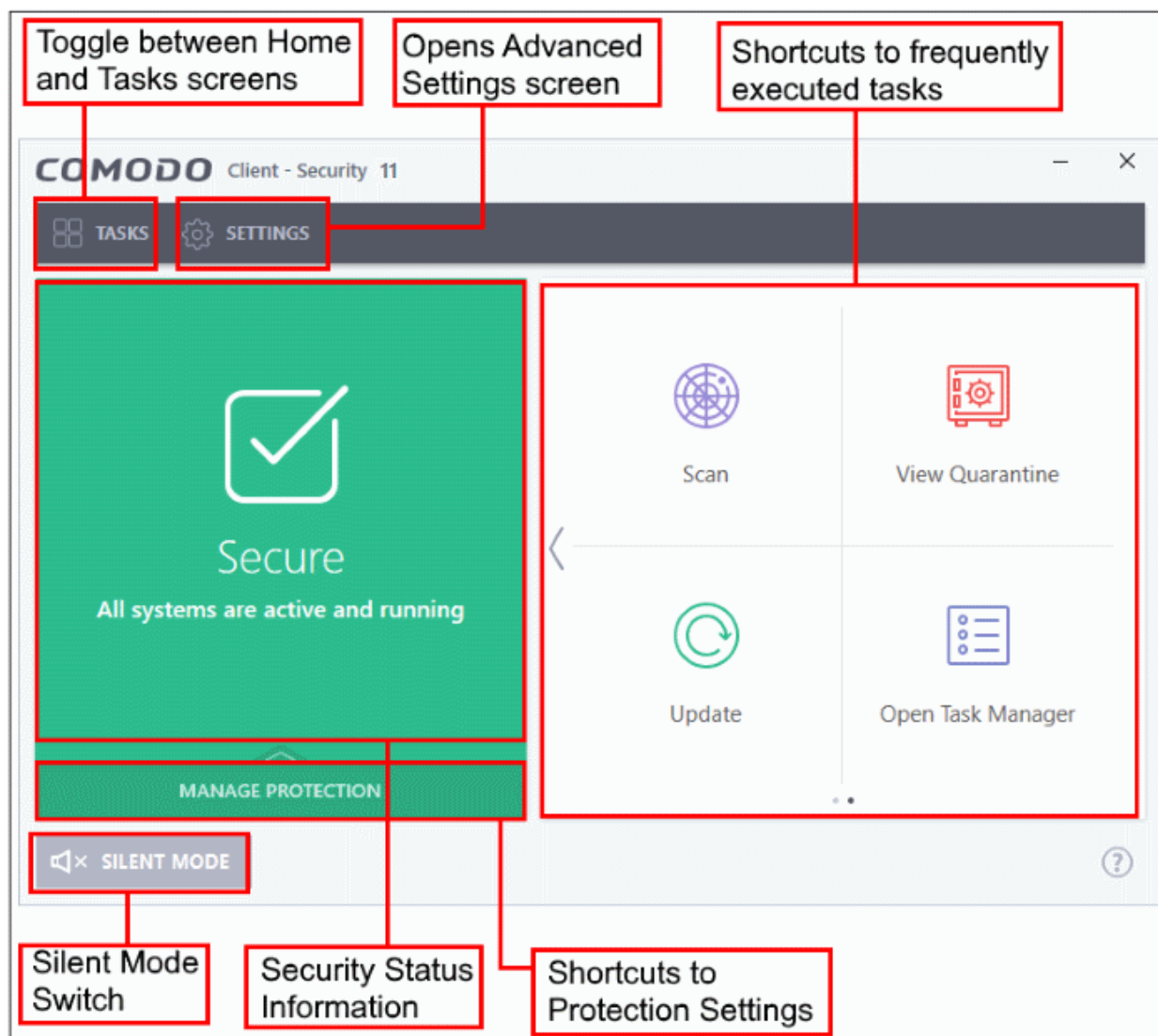
- Click the 'Virus & threat protection' tile
- Click 'Open COMODO Antivirus' to open the Comodo Client Security interface:



1.5. The Main Interface

The CCS interface is designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss.

- Clicking the 'Home/Tasks' button at the upper left lets you switch between the **home screen** and the more advanced **tasks interface**.
- 'Silent Mode' means you will not be interrupted by CCS messages while you perform other tasks.
- The tiles in the home screen allow one-click access to important features such as the antivirus scanner, the update checker and the CCS Task Manager.



Click the following links for more information:

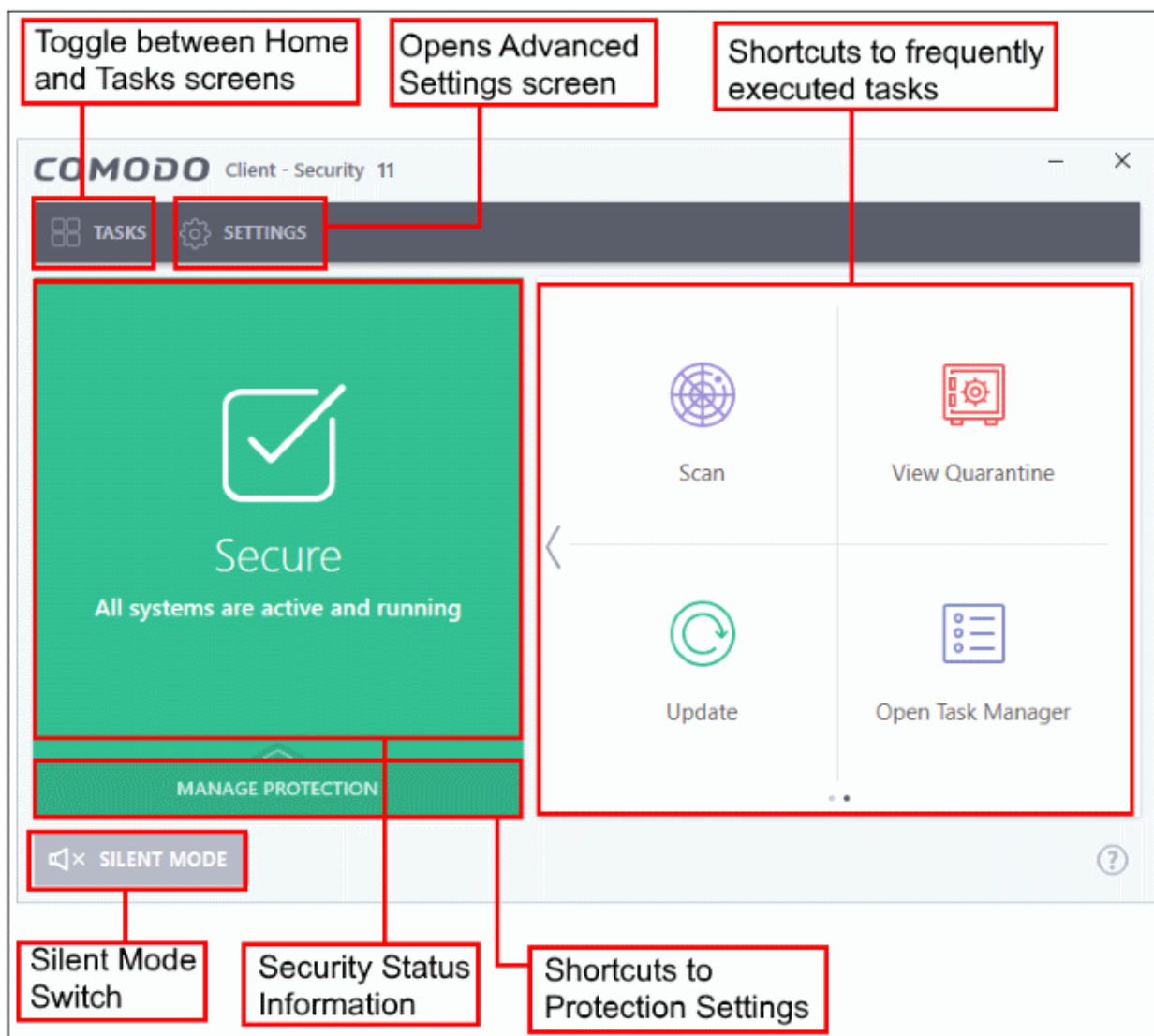
- [The Home Screen](#)
- [The Tasks Interface](#)
- [The Widget](#)
- [The System Tray Icon](#)

1.5.1. 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 presents a simple, easy to understand interface that allows users to quickly launch key tasks and gain an immediate overview of the security of the 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 CCS 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.



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



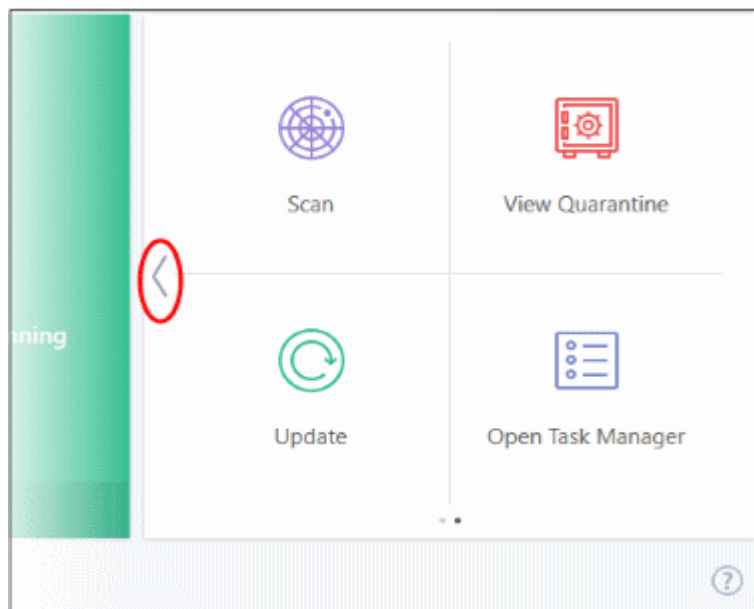
You can easily rectify the issue by clicking the 'FIX IT' button. **'Silent Mode'** and **'Help Window'** are common to both home and tasks screen.

From the home screen you can:

- **Add shortcuts tasks**
- **Manage protection settings**

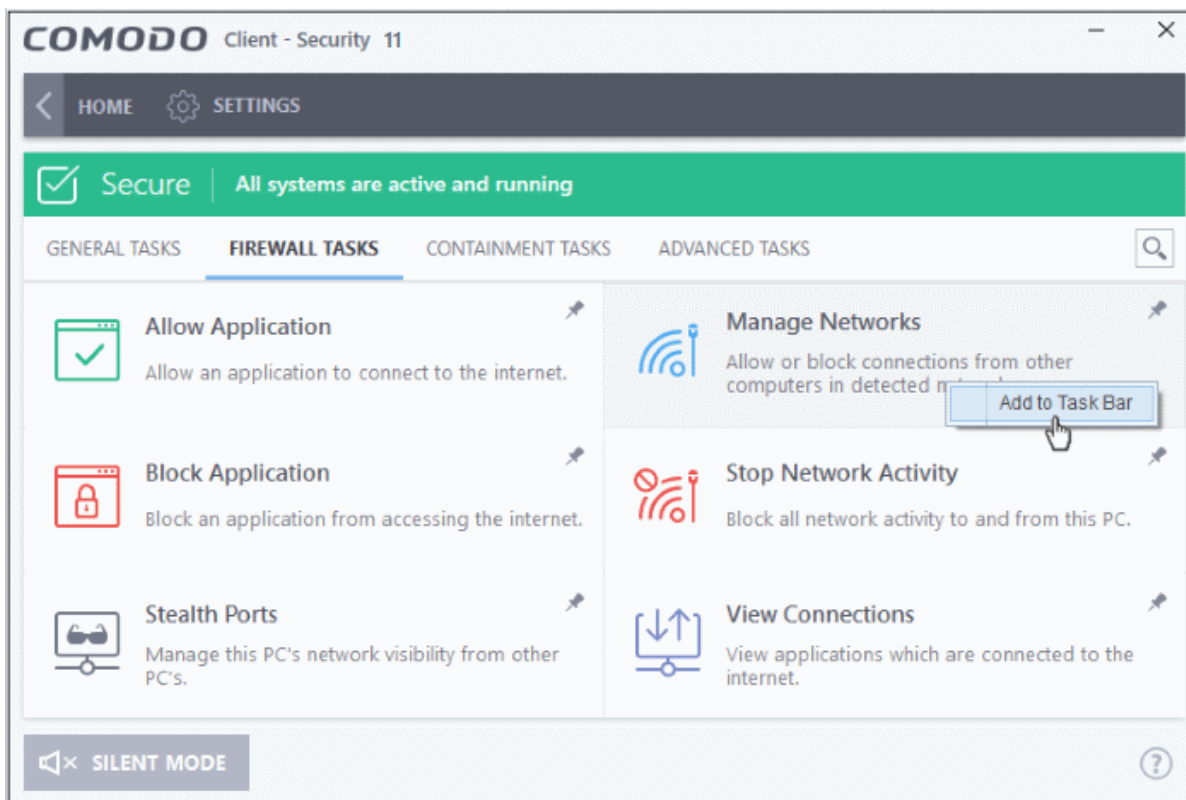
Adding tasks to the home screen


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

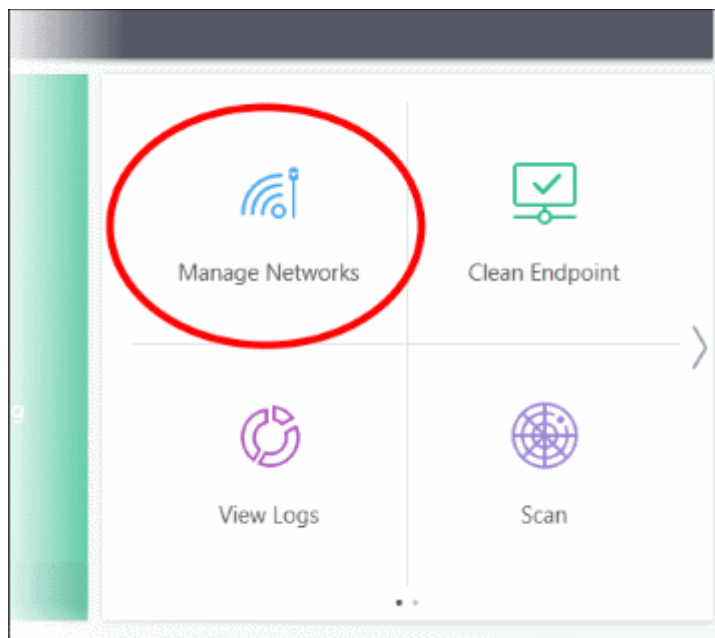


You can add tasks to this pane as follows:

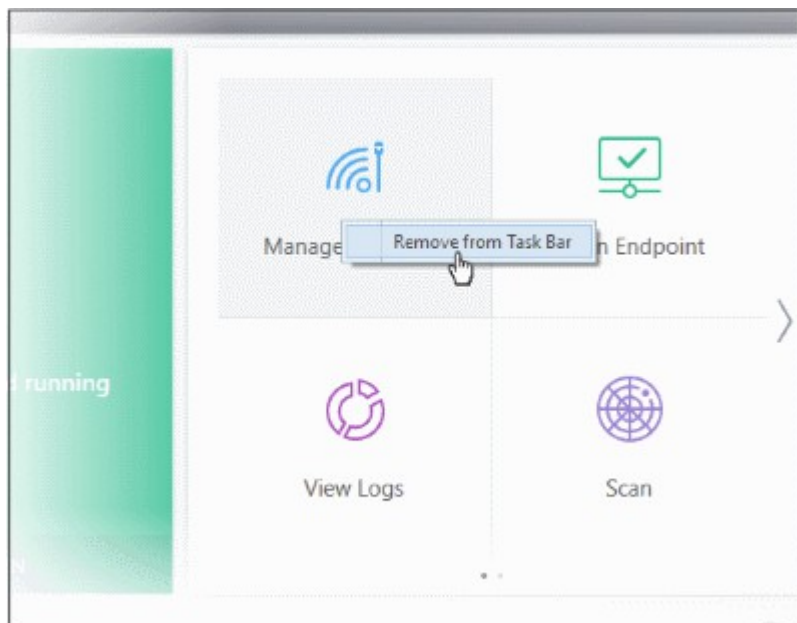
- Open the 'Tasks' interface (click the button at top left to switch between the tasks and home screens).
- Click any of the 'General', 'Firewall', 'Containment' or 'Advanced' tabs
- Right-click on the task you wish to add then click 'Add to Task Bar':



- 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.

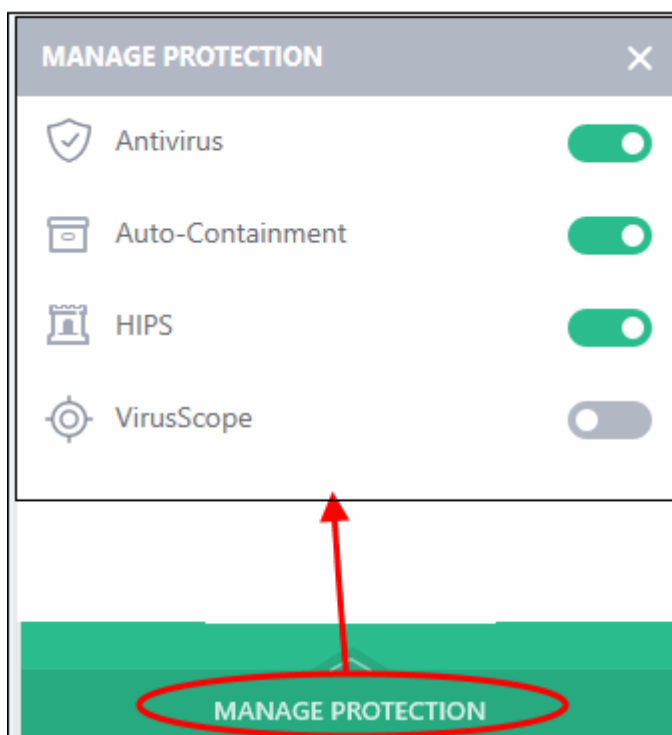


- To remove a task shortcut from the pane, right click on it and choose 'Remove from Task Bar'.



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.

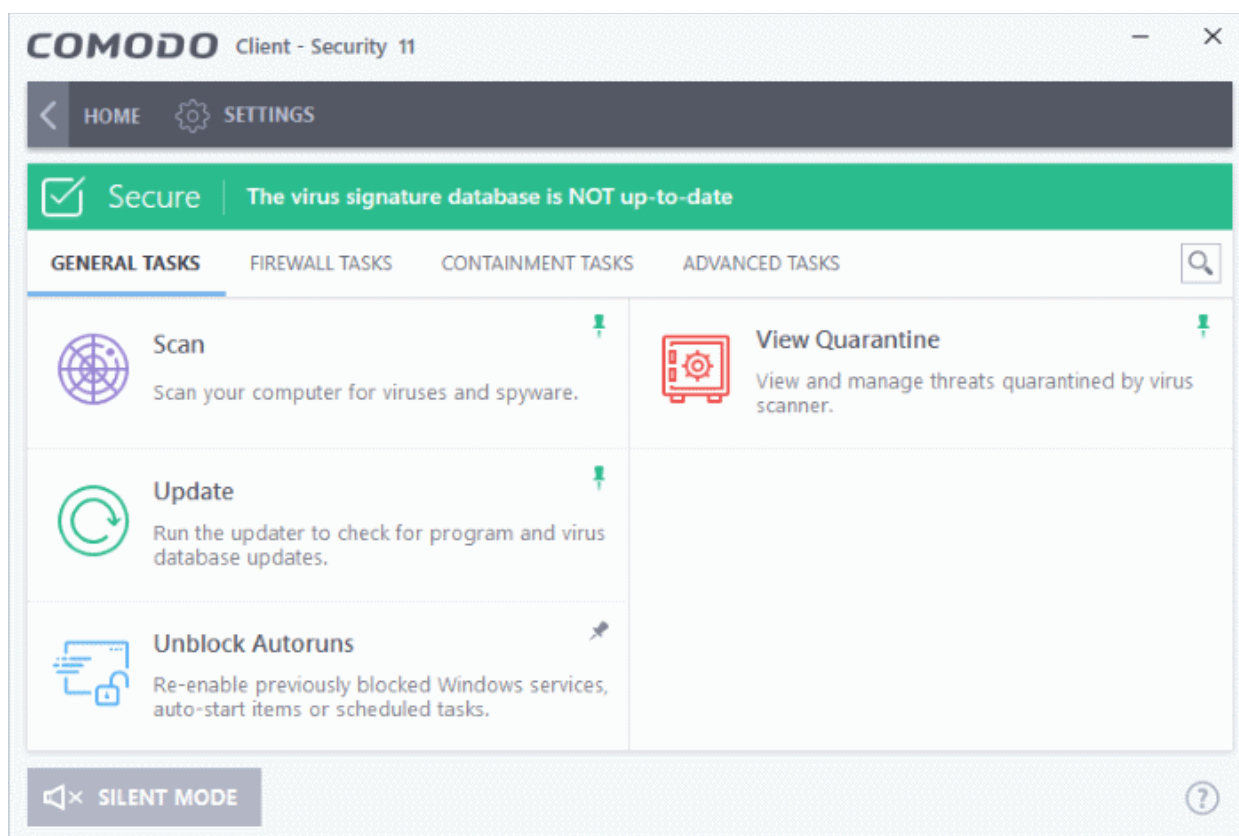


See the following sections for more details about each of the protection settings:

- **Antivirus Configuration**
- **Firewall Configuration**
- **Auto-Containment**
- **HIPS Configuration**
- **VirusScope Configuration**

1.5.2. The Tasks Interface

- The 'Tasks' area allows you to configure every aspect of Comodo Client Security.
- You can switch between the 'Home' screen and the 'Tasks' interface by clicking the 'Home/Tasks' button at the top left of the interface.



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

- **General Tasks** - Run antivirus scans and update the virus database. See '**General Tasks**' for more details.
- **Firewall Tasks** - Allow or block applications, manage ports, manage networks and view applications connected to the internet. See '**Firewall Tasks**' for more details.
- **Containment Tasks** - Run applications in a secure virtual environment and view processes active on the endpoint. See '**Containment Tasks**' for more details.
- **Advanced Tasks** - Create a boot disk to clean up highly infected systems; install other Comodo software like KillSwitch and Cleaning Essentials. See '**Advanced Tasks**' for more details.

The '**Silent Mode**' and '**Help Window**' options are common to both home and tasks screen.

Silent mode

Silent Mode lets you to use your computer without interruptions or alerts. Operations that could interfere with your work are either suppressed or postponed.

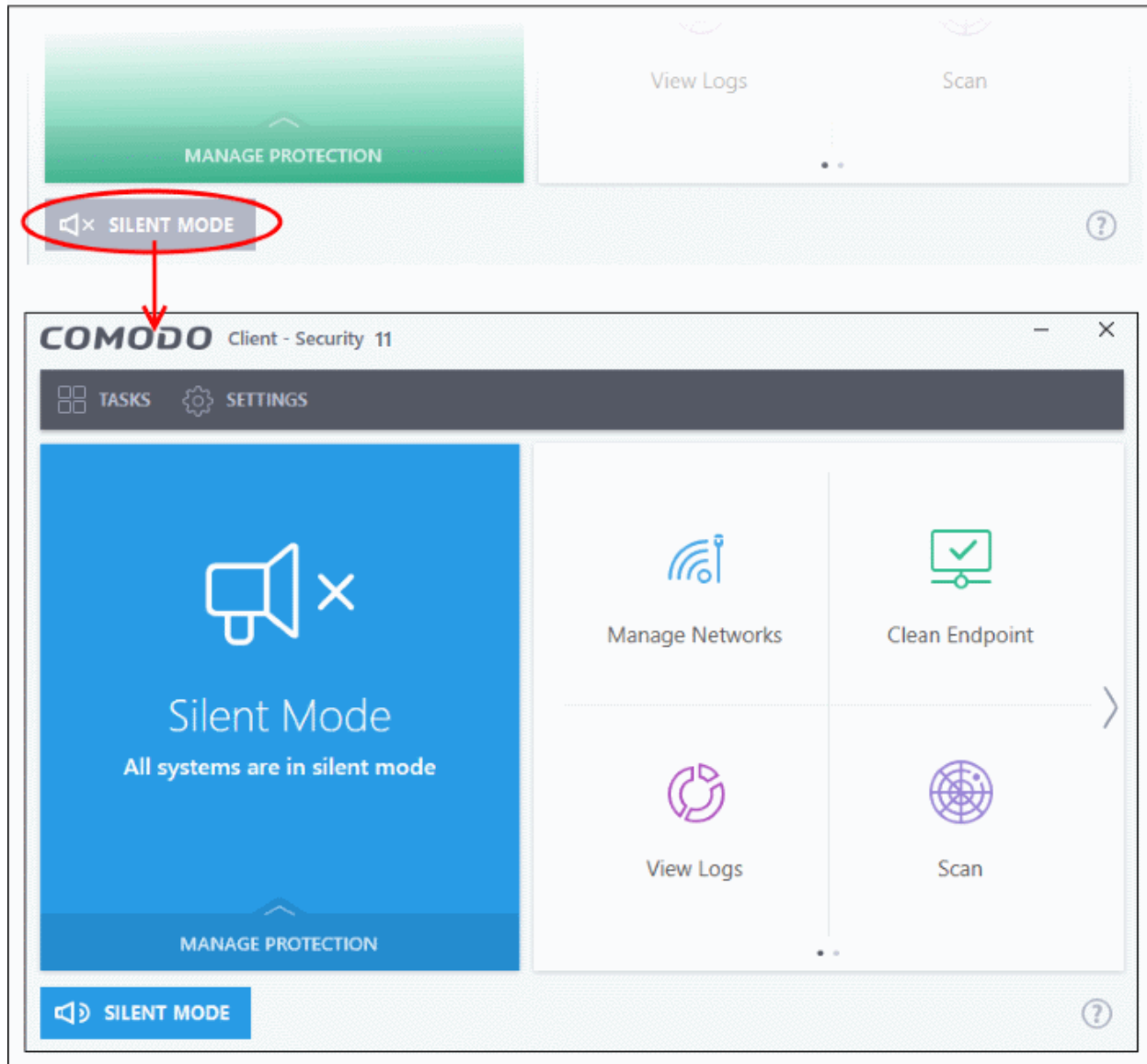
In silent mode:

- HIPS/Firewall alerts are suppressed.

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

To switch to Silent mode

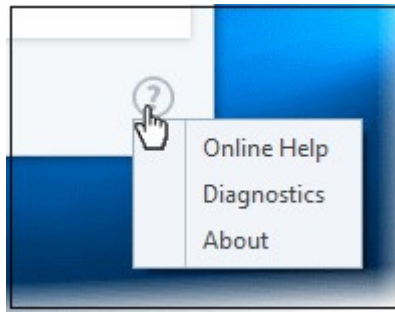
- Click the 'Silent Mode' switch at the bottom left of the 'Home' screen



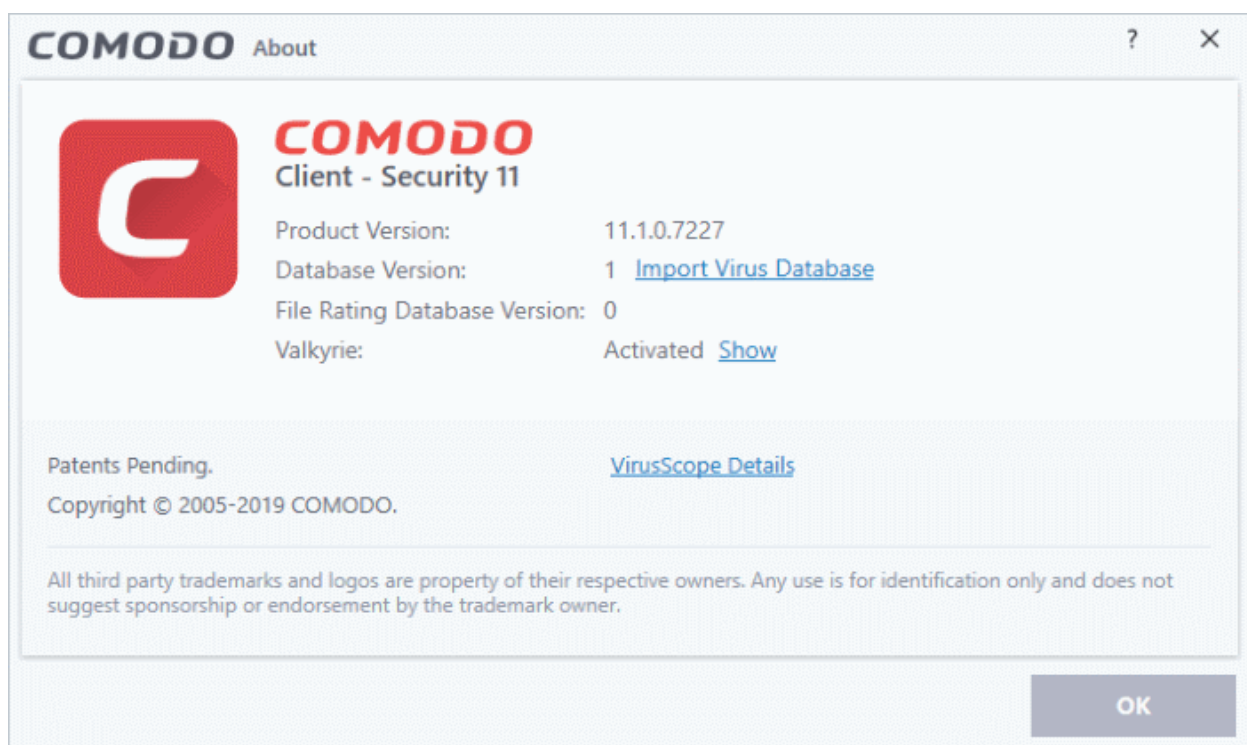
- Deactivate 'Silent Mode' to resume alerts and notifications.

Help Window

The 'Help' button lets you view our online help guide, run a diagnostics test on your installation and view the version of the application.



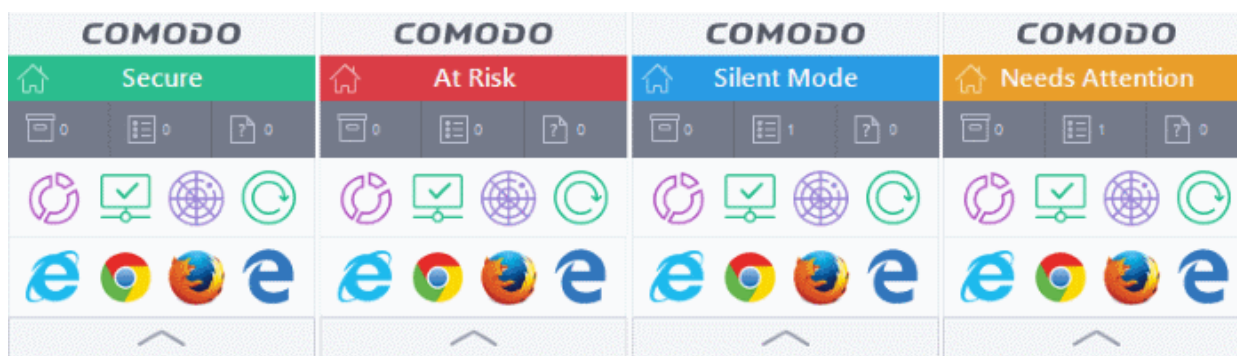
- **Online Help** - Opens Comodo Client Security's online help guide at <http://help.comodo.com>
- **Diagnostics** - Helps to identify any problems with your installation.
- **About** - Displays the product version number and the version numbers of various CCS security components. The 'About' dialog also allows you to import a locally stored virus database.

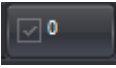
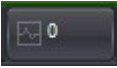
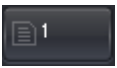


- **Product Version** - The CCS version number.
- **Database Version** - The current virus database version. Click [Import Virus Database](#) to import a locally stored virus signature database into CCS.
- **File Rating Database Version** - The version of the file rating database used by Endpoint Manager server. The file rating interface can be viewed in Endpoint Manager by clicking 'Security Sub-Systems' > 'Application Control'.
- **Valkyrie** - Indicates whether or not Valkyrie is enabled. Click 'Show' to view your Valkyrie account activation number.
- Click [VirusScope Details](#) to open a dialog which shows the Viruscope Recognizers that are active on your system. See '**VirusScope Settings**' for more details.

1.5.3. The Widget

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



- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' will open the appropriate interface for you to take action.
- The second row tells you current status of the CCS application:
 - The first button  displays the number of programs/processes that are currently running in the container. Clicking the button opens the 'Active Process List (Contained Only)', which allows you to identify and terminate unnecessary processes. Clicking the 'More' button in this interface will open the KillSwitch application. If KillSwitch is not yet installed, clicking this button will prompt you to download the application. See '**View Active Process List**' and '**Identify and Kill Unsafe Processes**' for more details.
 - The second button  denotes the number of CCS tasks that are currently running. Click the button to open the '**Task Manager**' interface.
 - The third button  displays how many 'Unrecognized' files have been added to the '**Files list**', pending submission to Comodo for analysis. Click the button to open the '**Files list**' which shows the unrecognized files.

The status row is displayed only if 'Show Status Pane' is enabled under 'Widget options'. Right-click on the widget or the CCS tray icon to view this setting. See '**The System Tray Icon**' for more details. **(Default = Disabled)**

- The third row contains shortcuts for five common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task. The common tasks row is only displayed if 'Show Common Tasks Pane' is enabled under 'Widget' options. Right-click on the widget or the CCS tray icon to view this setting. See '**The System Tray Icon**' for more details. **(Default = Enabled)**
- The fourth row shows the browsers installed on your computer. Click a browser icon to open the browser inside the container for a secure browsing session. You can tell the browser is running in the container because it will have a green border around it. See '**Running an application inside the container**' for more details. The browsers row is only displayed if 'Show Browsers Pane' is enabled under 'Widget' options. Right-click on the widget or the CCS tray icon to view this setting. See '**The System Tray Icon**' for more details. **(Default = Enabled)**

- You can expand or collapse the Widget by clicking the arrow at the bottom.

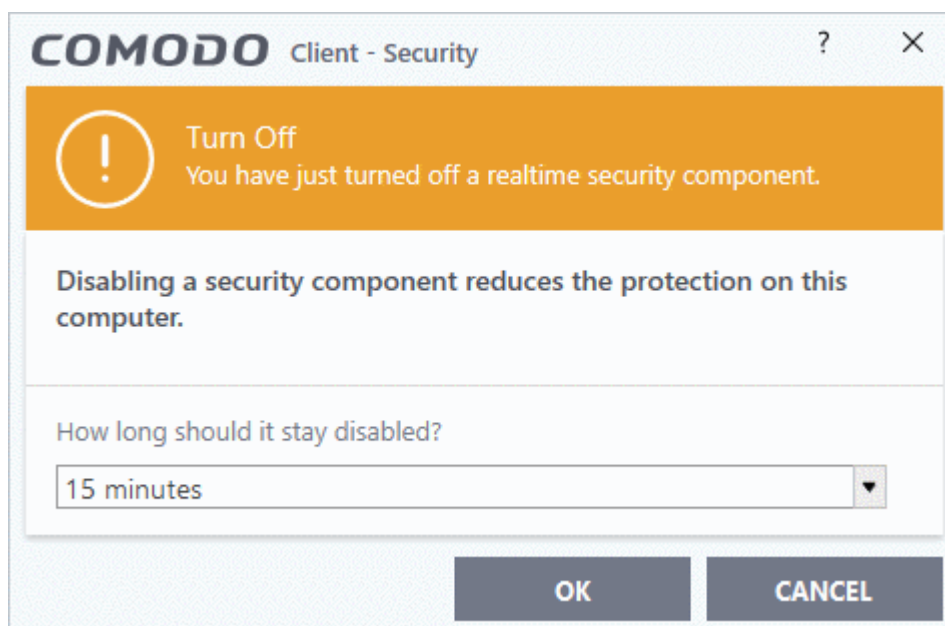
1.5.4. The System Tray Icon

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

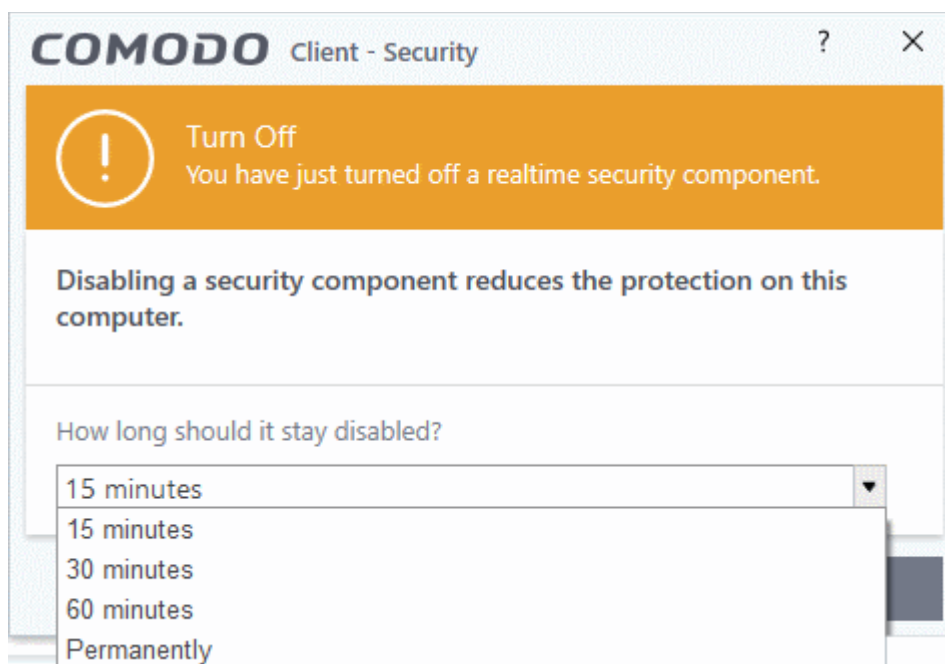


- **Antivirus** - Enable or disable real-time virus monitoring.

If this setting is disabled, the security panel and the widget will turn red, indicating that AV is switched off. In addition, a pop-up alert will be shown:

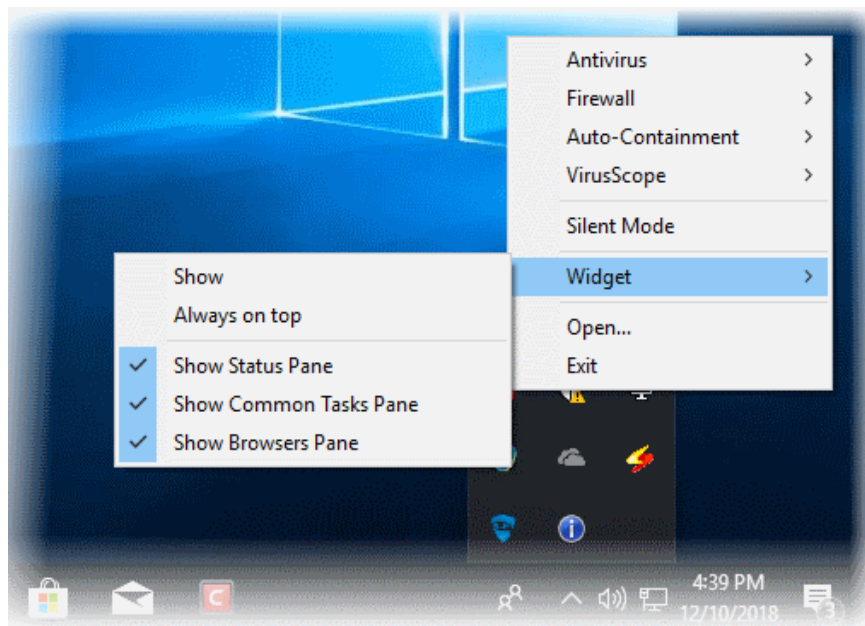


The drop-down lets you choose how long the virus monitor should be turned off for.



Select the period and click 'OK'. If you have selected any of first three time intervals, the security component will be enabled automatically after the chosen period.

- **Firewall** - Enable or disable the Firewall module. See '**Firewall Settings**' for more details.
- **Auto-Containment** - Enable or disable the Auto-Containment module. Auto-containment rules let you specify which types of applications you want to run in the container. See '**Auto-Containment Rules**' for more details.
- **VirusScope** - Enable or disable the VirusScope feature. See '**VirusScope Settings**' for more details.
- **Silent Mode** - Enable or disable silent mode. Silent mode lets you carry out tasks without any interruptions or alerts from CCS. Tasks that can cause interruptions either suppressed or postponed:
 - Advanced Protection/Firewall alert is suppressed.
 - AV database updates and scheduled scans are postponed
 - Automatic isolation of unknown applications and real-time virus detection are still functional.Deactivate Silent mode to resume alerts and scheduled scans.
- **Widget** - Select whether or not the **Widget** is shown and configure widget elements:



- **Show:** Toggle widget visibility. (**Default = Disabled**)
- **Always on top:** Displays the widget on top of all windows currently running on your computer. (**Default = Disabled**)
- **Show Status Pane:** Show overall security status in the widget (**Default = Disabled**)
- **Show Common Tasks Pane:** Show shortcuts to common CCS tasks in the widget. (**Default = Enabled**)
- **Show Browsers Pane:** Show shortcuts to browsers in the widget. (**Default = Enabled**)
- **Open** - Opens the CCS interface.
- **Exit** - Closes the CCS application.

1.6. Understand Security Alerts

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

Alerts Overview

CCS 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 CCS 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.

The screenshot shows a Comodo HIPS alert window. At the top, it says 'COMODO HIPS'. The main alert area has a red header with a castle icon and the text 'TSServ.exe is trying to modify a protected registry key'. Below this, there is a diagram showing 'TSServ.exe' with an arrow pointing to 'Modify Key'. A warning message follows: 'WARNING! C:\Suspicious Files\TrojanSimulator\TSServ.exe is a known malicious file trying to modify HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run. You MUST block this request.' At the bottom, there are three action buttons: 'Allow' (with a green checkmark), 'Block' (with a red prohibition sign), and 'Treat as' (with a three-dot menu icon). A 'Remember my answer' checkbox is at the bottom left, and a 'Show Activities' link is at the bottom right.

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 these options to allow, block or otherwise handle the request

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

Alert Types

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

- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when **Antivirus is enabled** and the option '**Do not show antivirus alerts**' is disabled in **Real-time Scanner Settings**.
- **Firewall Alerts** - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the **Firewall is enabled** and the option '**Do not show popup alerts**' is disabled in **Firewall Settings**.
- **HIPS Alerts** - Shown whenever an application attempts an unauthorized action or tries to access protected areas. HIPS alerts will only be generated if **HIPS is enabled** and **Do NOT show popup alerts** is disabled.
- **Containment Alerts** (including **Elevated Privilege Alerts**) - Shown whenever an application tries to modify operating system or related files and when CCS 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.
- **Device Control Alerts** - Shown whenever an external device that is blocked by the administrator is connected to your system.
- **Auto-Scan Alerts** - Shown whenever an external device is connected to your endpoint. This alert will be shown only if 'Do not show auto-scan alerts' is disabled in '**Realtime Scan**' settings.

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

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

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:



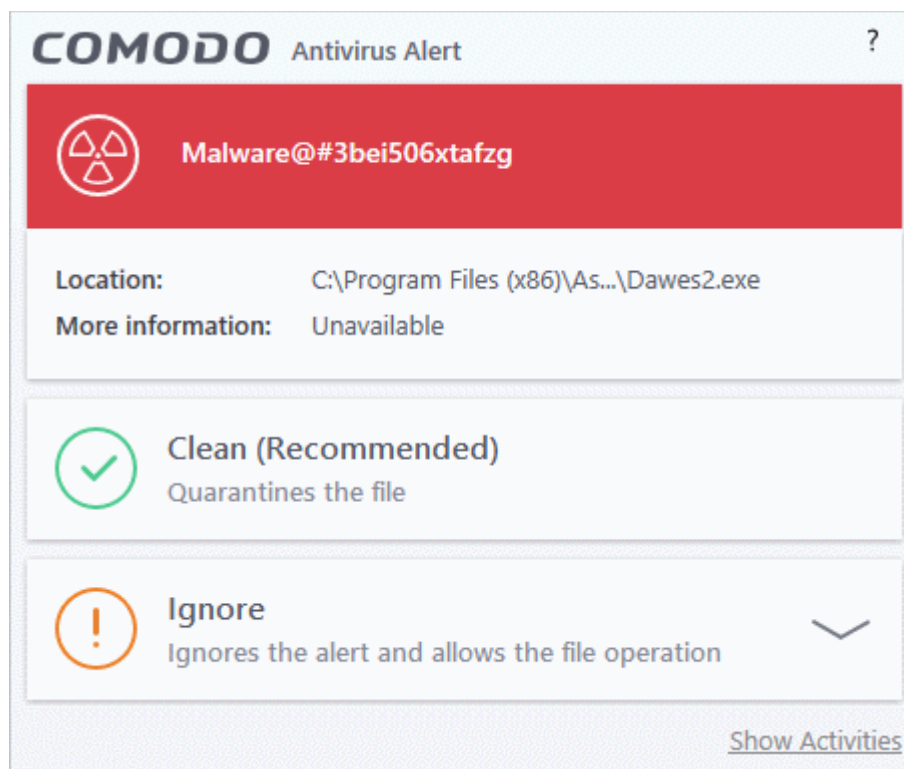
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answering an Antivirus Alert

Comodo Client 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.

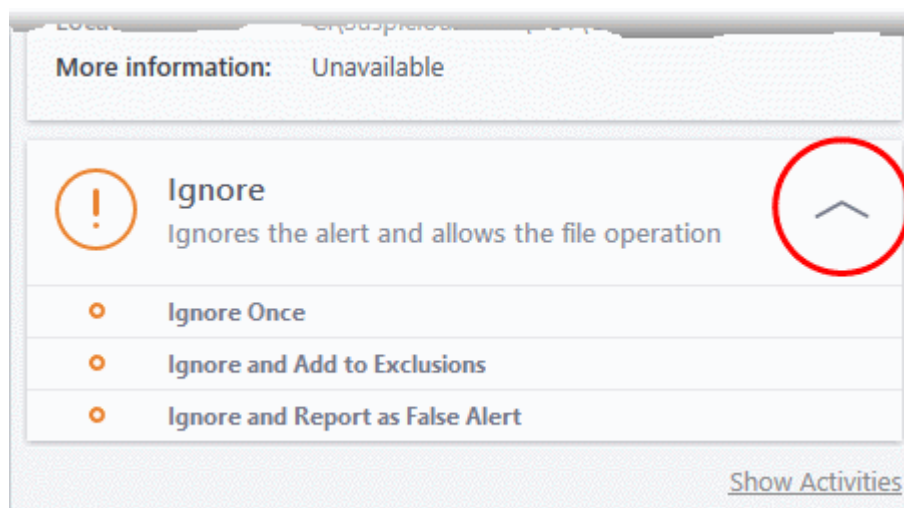


Tip: Clicking the 'Show Activities' link at the bottom right will open the **Process Activities List dialog**. The 'Process Activities' dialog will display the list activities of the processes run by the application.

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

The following response-options are available:

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



- **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'. CCS 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

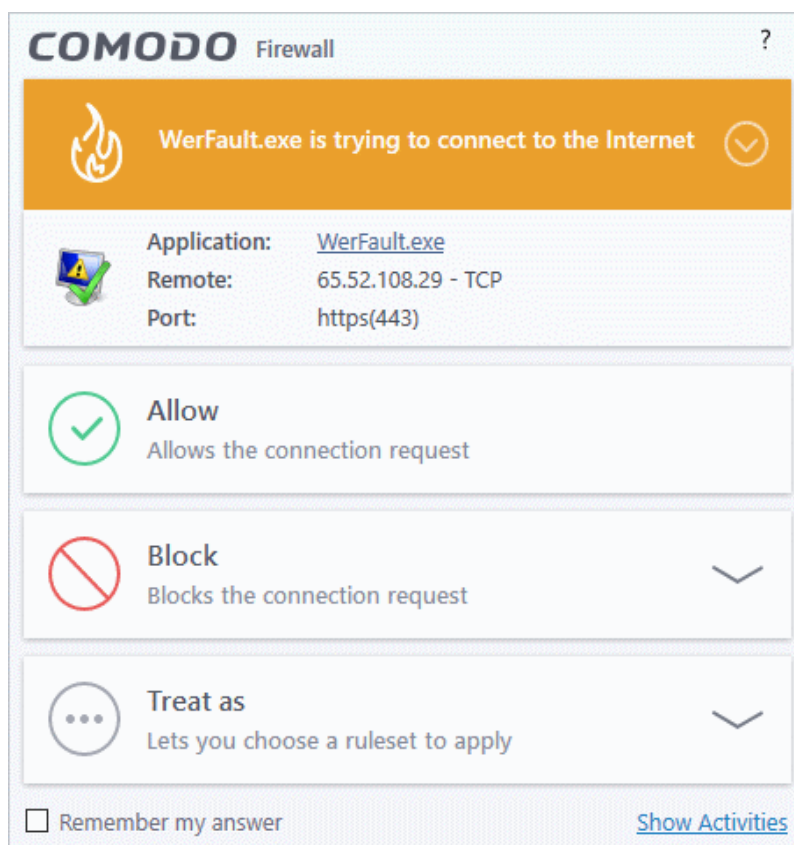
If you have chosen to not to show Antivirus Alerts through **Settings > Realtime Scanner Settings** by leaving the option 'Do not show antivirus alerts' enabled (**default=enabled**) and If CCS identifies a virus or other malware in real time, it will immediately block malware and provide you with instant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

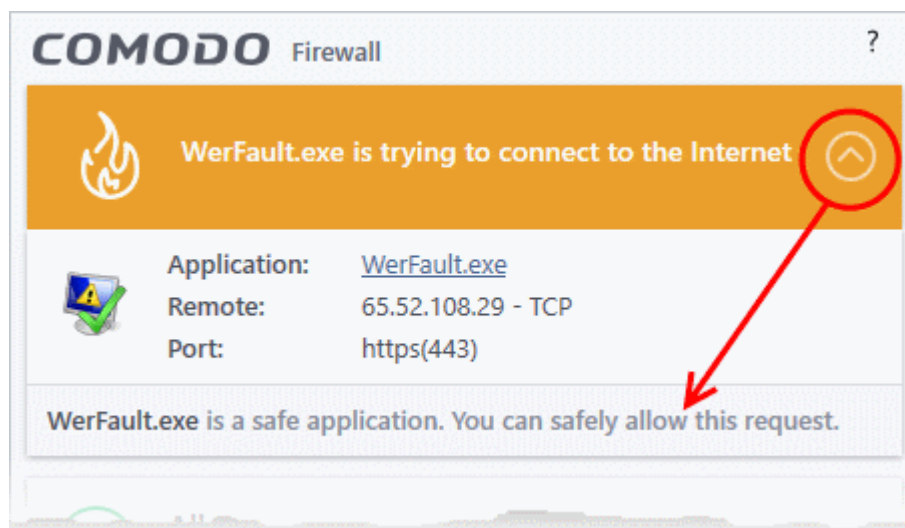
Answering Firewall Alerts

CCS 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 CCS 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.

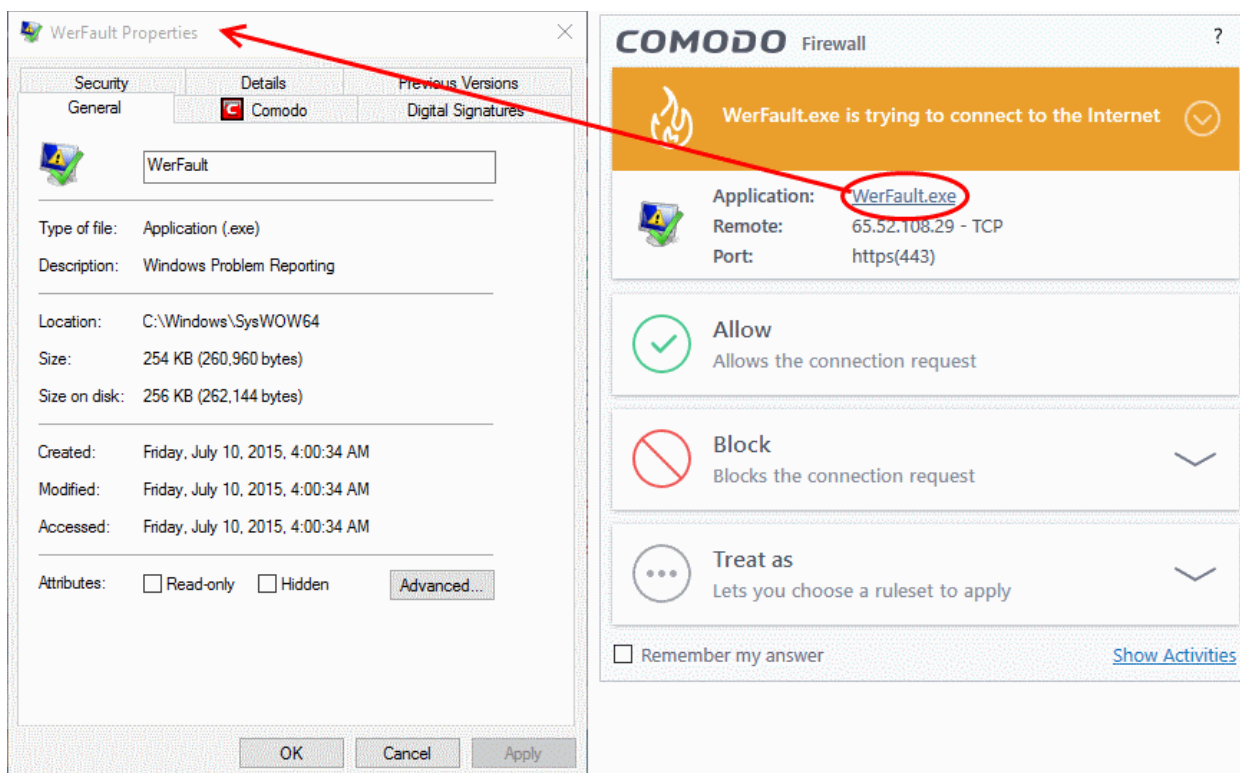
The 'Show Activities' link is available only if VirusScope is enabled under **Settings> VirusScope**. If none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the 'Show Activities' link is disabled and will not open the Process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



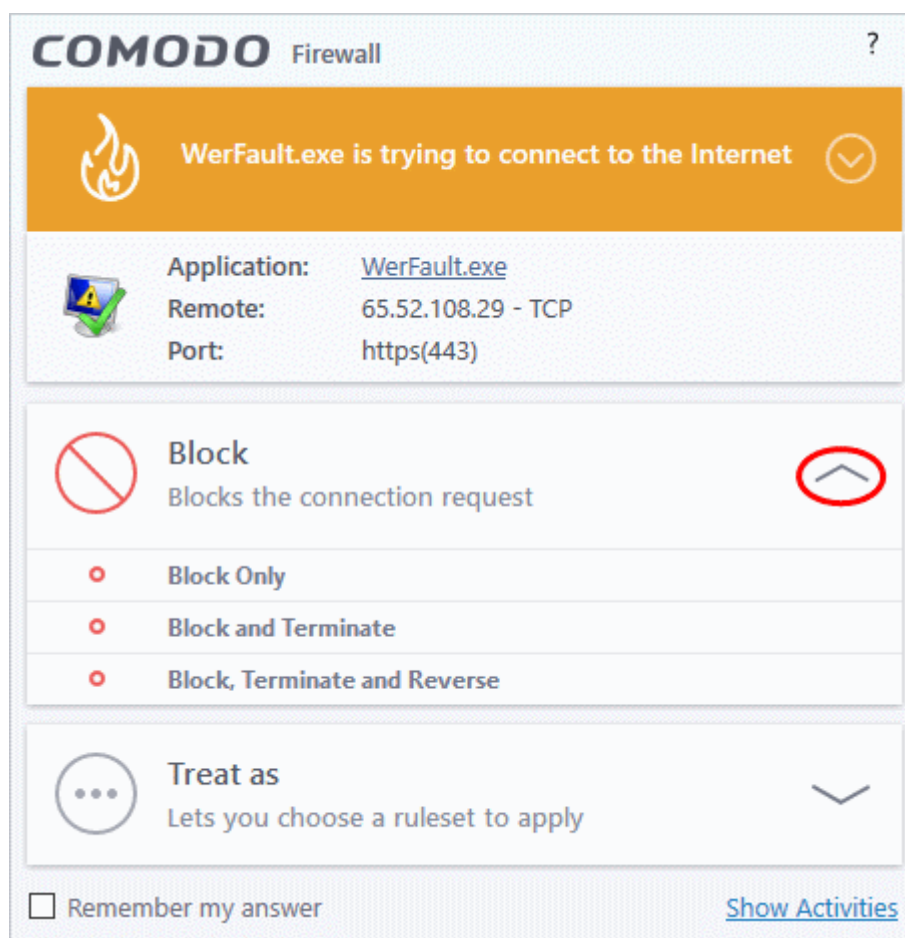
1. Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security 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:

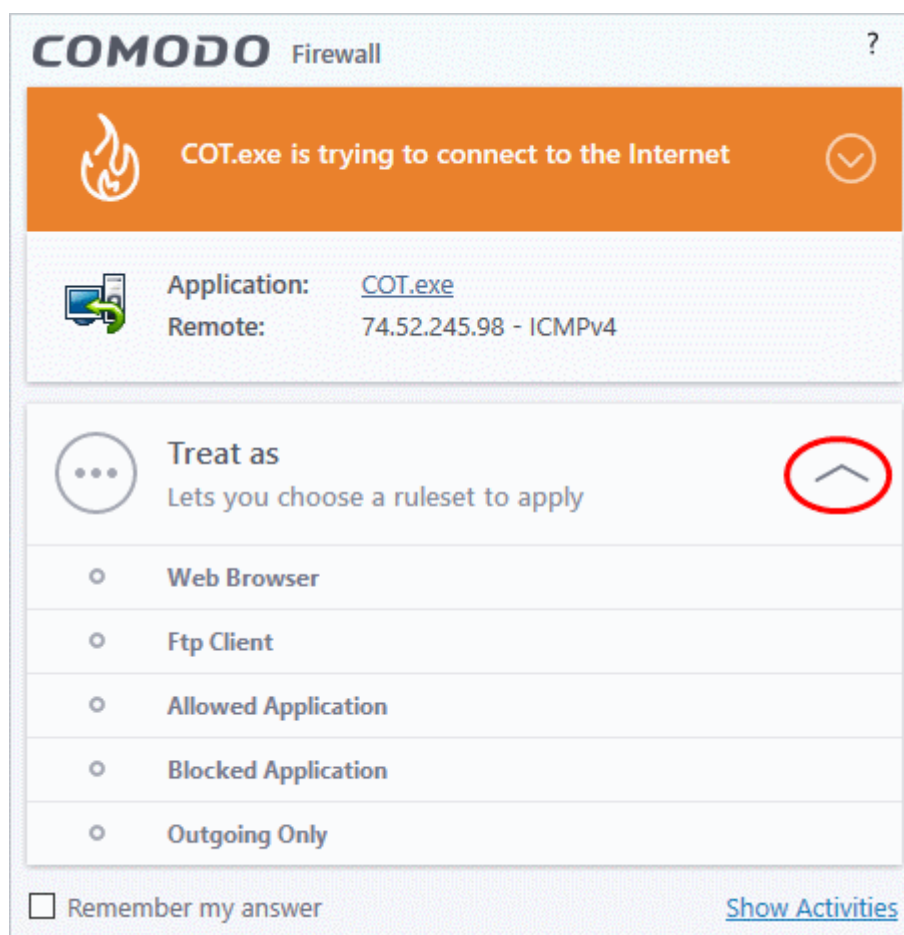


If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand the alert, you can choose to 'Block' the connection (connection is not allowed to proceed), 'Block and Terminate' (connection is not allowed to proceed and the process/application 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.

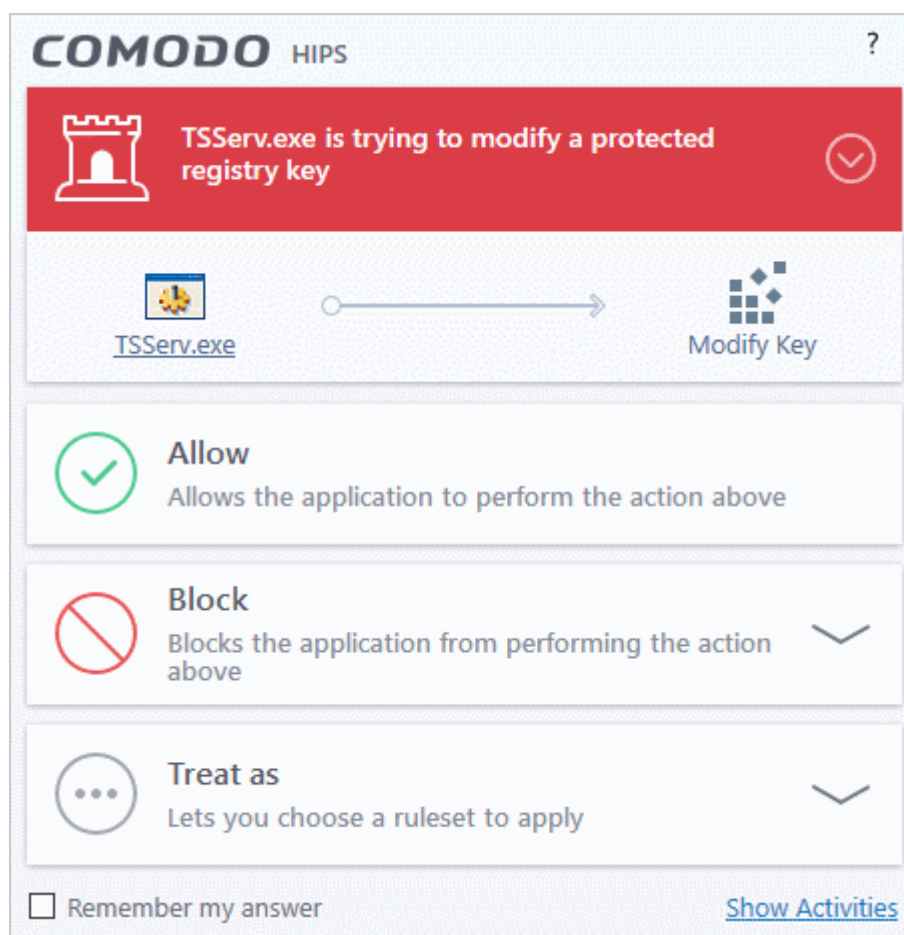


Remember to check the box '**Remember My Answer**' for the ruleset to be applied in future.

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

Answering HIPS Alerts

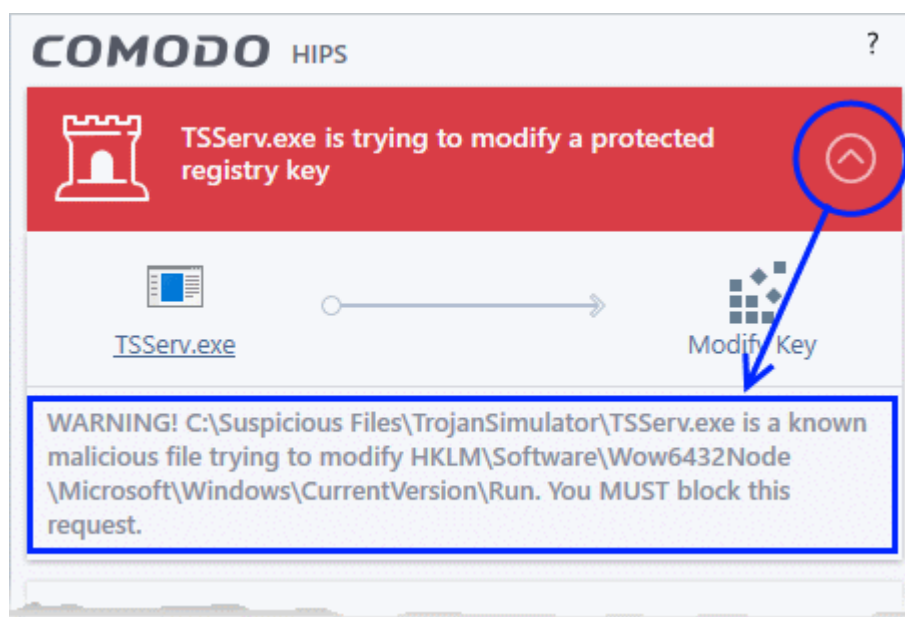
Comodo Client Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:



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.

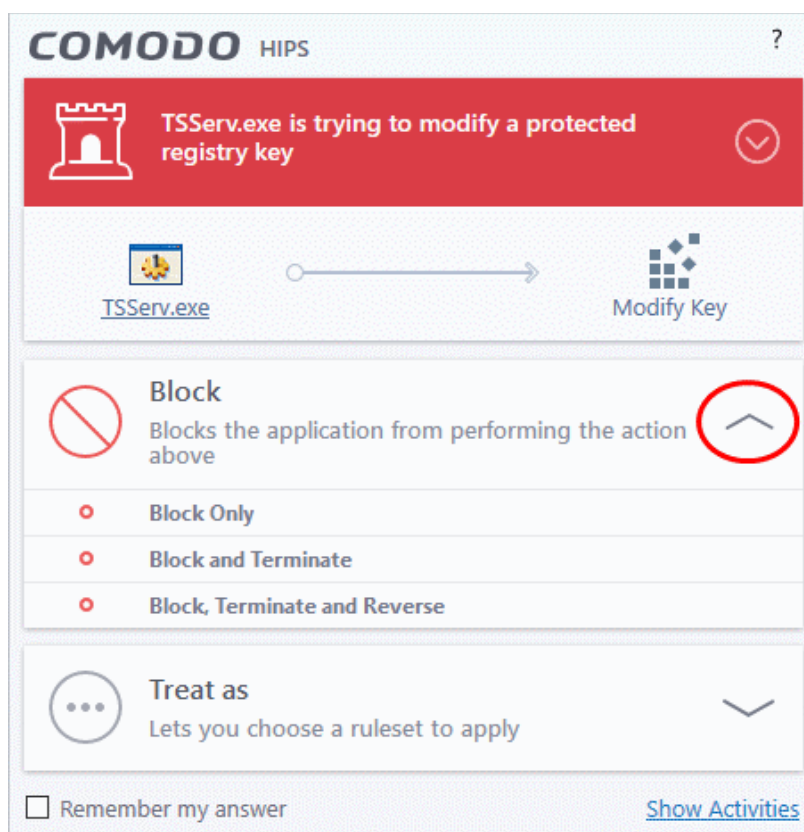
1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Client Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe 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**.

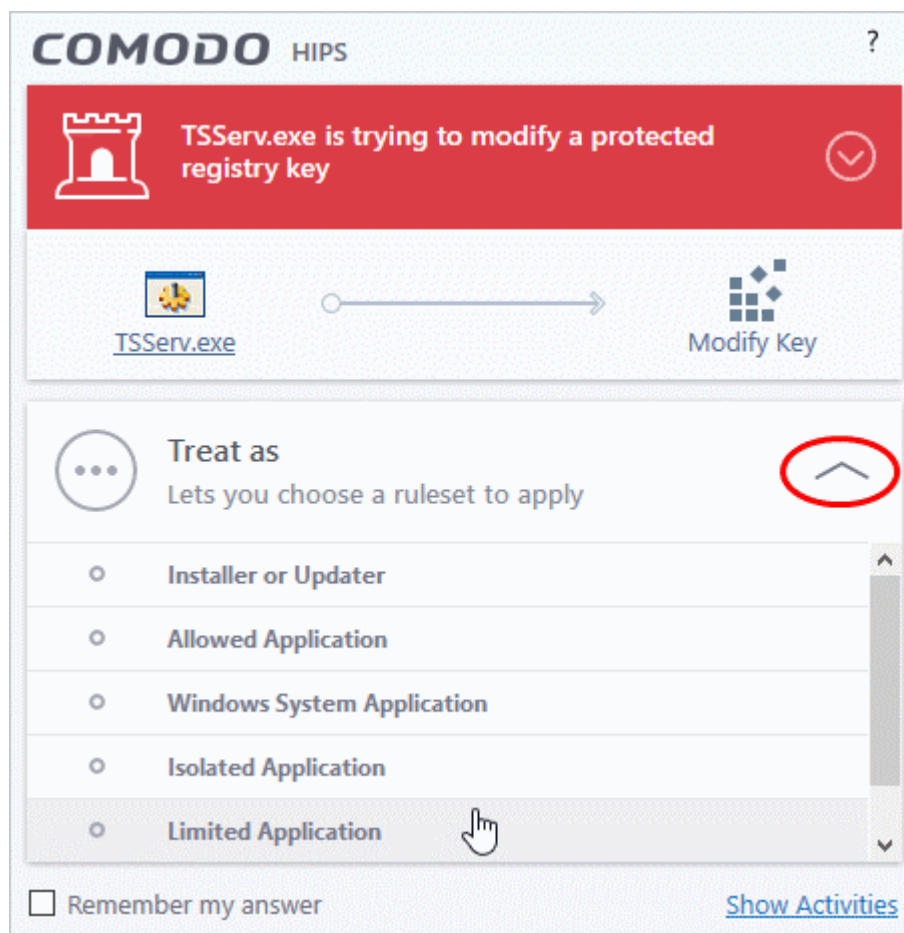
If you don't recognize the application then we recommend you select **Block** the application. By clicking the handle to expand the alert, you can choose to

- '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.



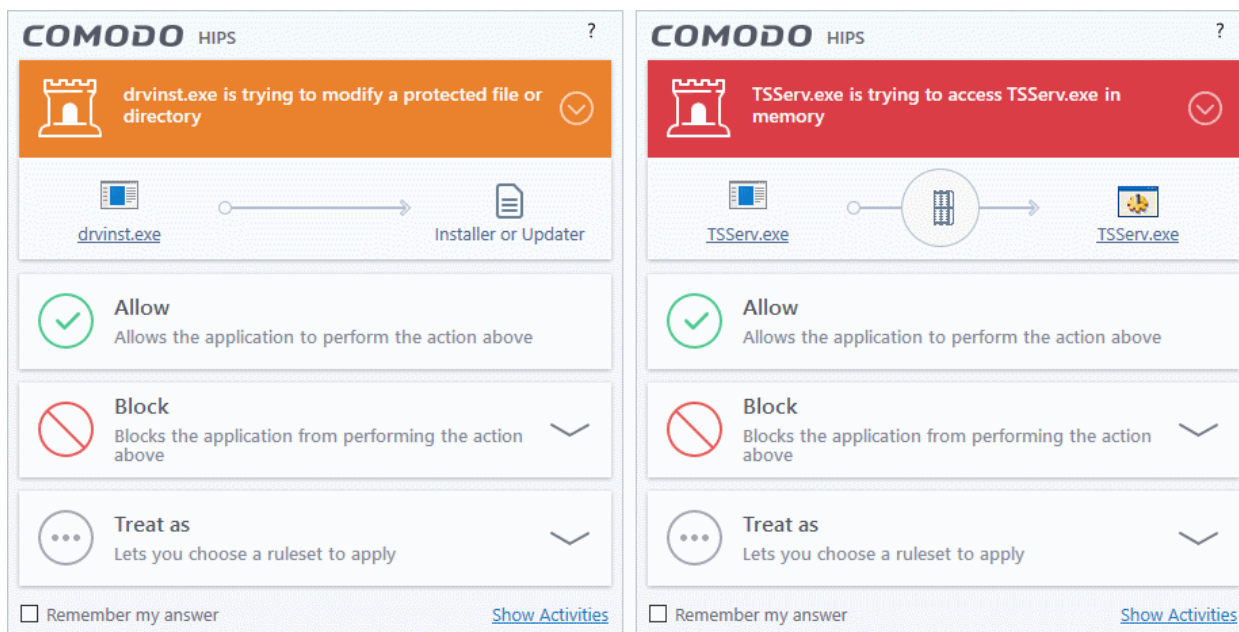
Note: 'Block, Terminate and Reverse' option will be available only if VirusScope is enabled under [Settings > VirusScope](#).

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.

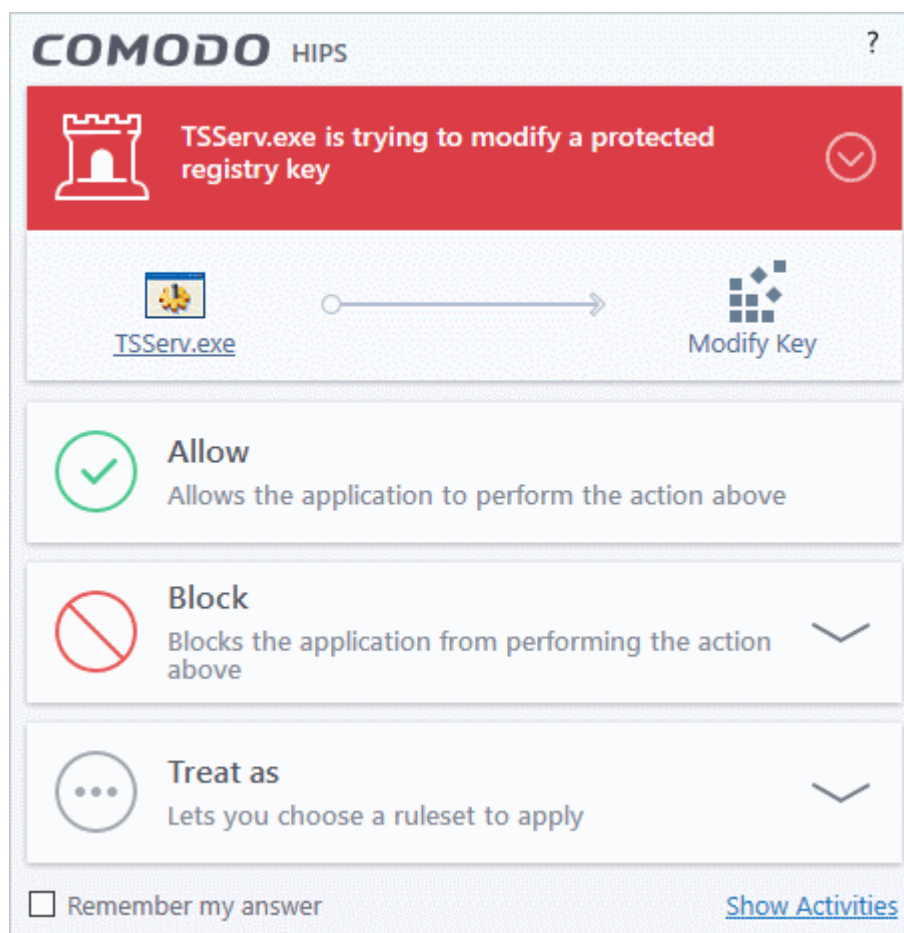


Avoid using the **Installer or Updater** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select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

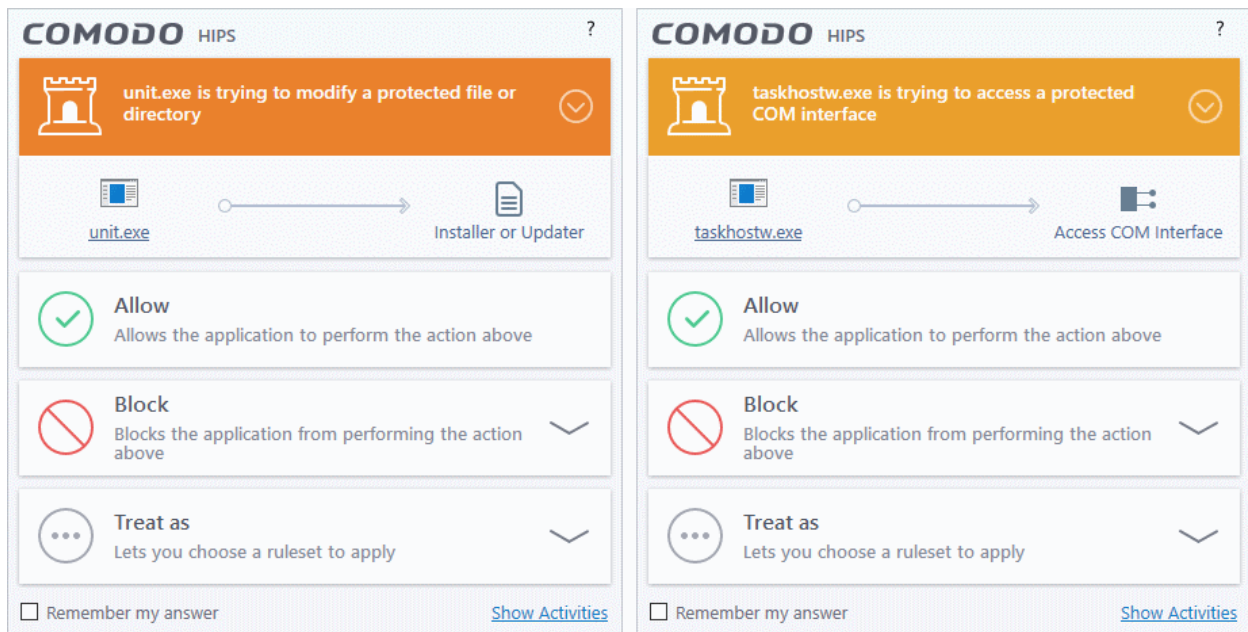
3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity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

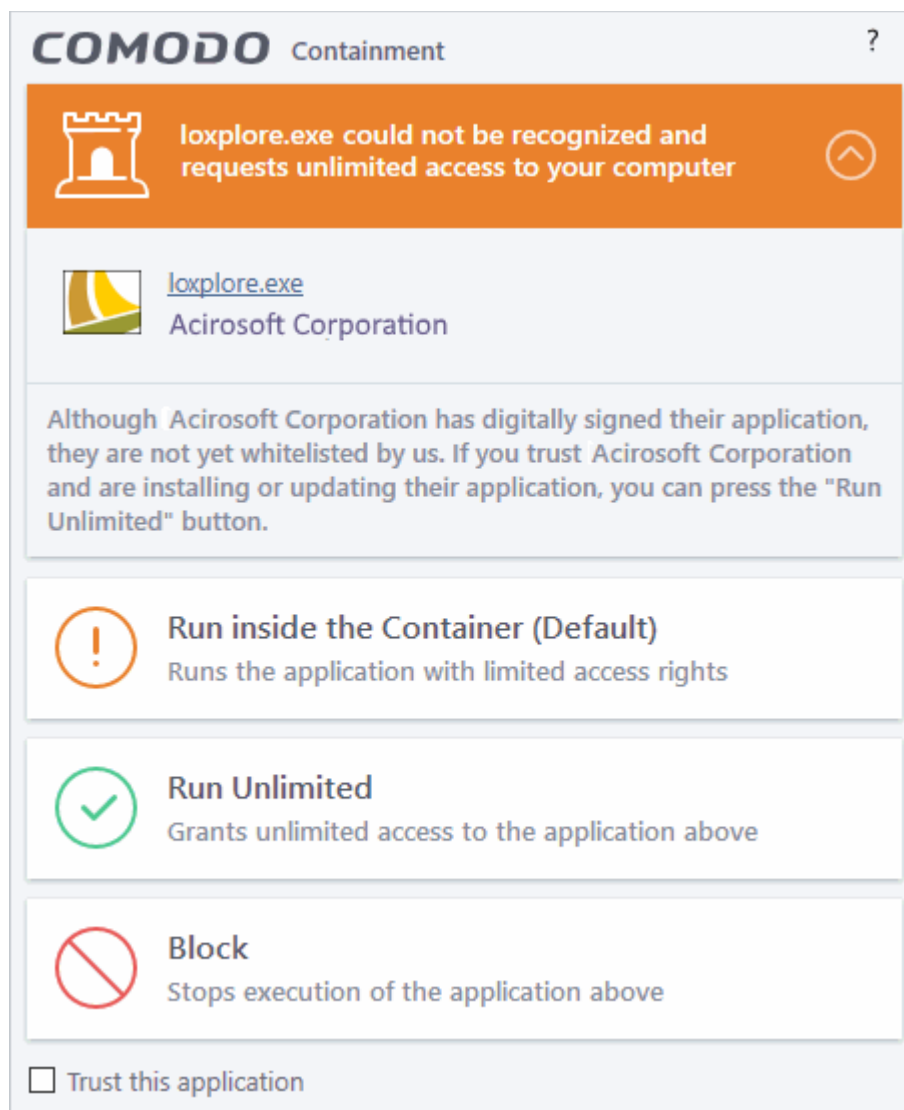
If an application is trying to create a new file with a random file name e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by clicking **Treat As** and choosing **'Isolated Application'** from the options.

6. If a HIPS alert reports a malware behavior in the security considerations area then you should **Block the request** permanently by selecting **Remember My Answer** option. As this is probably a virus, you should also submit the application in question, to Comodo for analysis.
7. Unrecognized applications are not always bad. Your best loved applications may very well be safe but not yet included in the Comodo certified application database. If the security considerations section says "If xxx is one of your everyday applications, you can allow this request", you may allow the request permanently if you are sure it is not a virus. You may report it to Comodo for further analysis and inclusion in the certified application database.
8. If HIPS is in 'Paranoid' mode, you probably are seeing the alerts for any new applications introduced to the system - but not for the ones you have already installed. If required, you may review files with 'Unrecognized' rating in the **'File List'** interface and remove them from the list.
9. Avoid using Trusted Application or Windows System Application policies for you email clients, web browsers, IM or P2P applications. These applications do not need such powerful access rights.

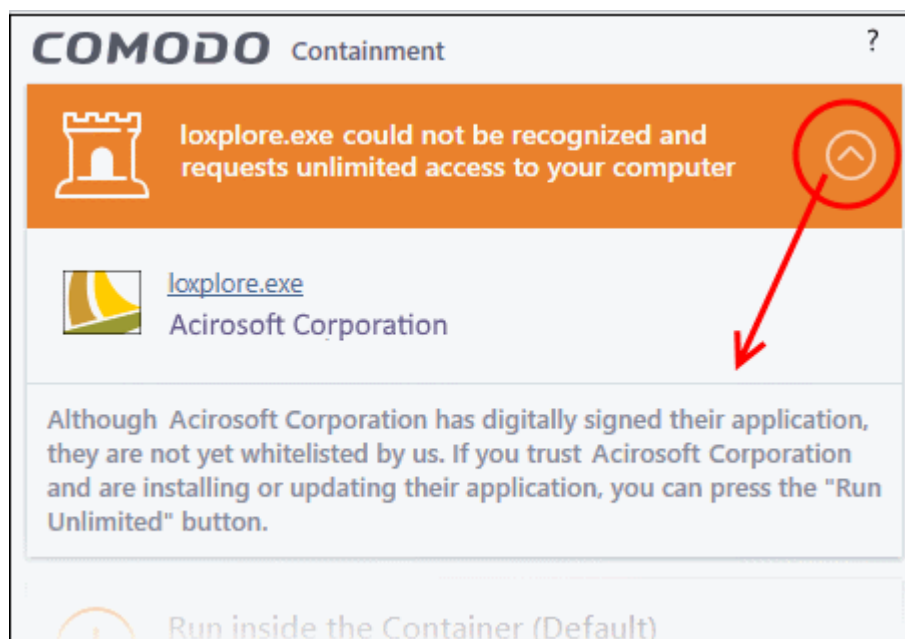
Answering a Containment Alert

Comodo Client 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.

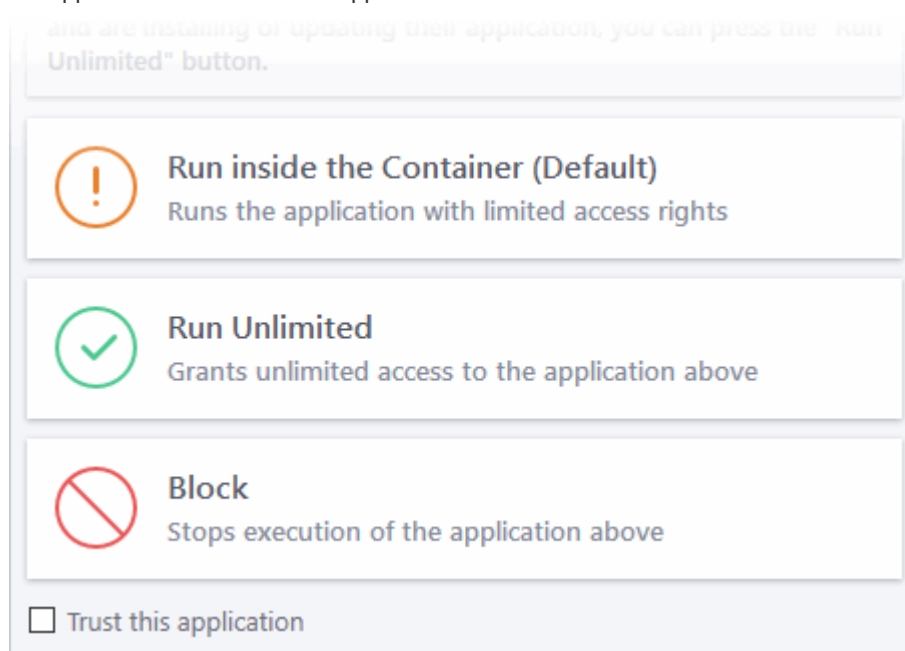
Please read the following advice before answering a Containment alert:



1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Client 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

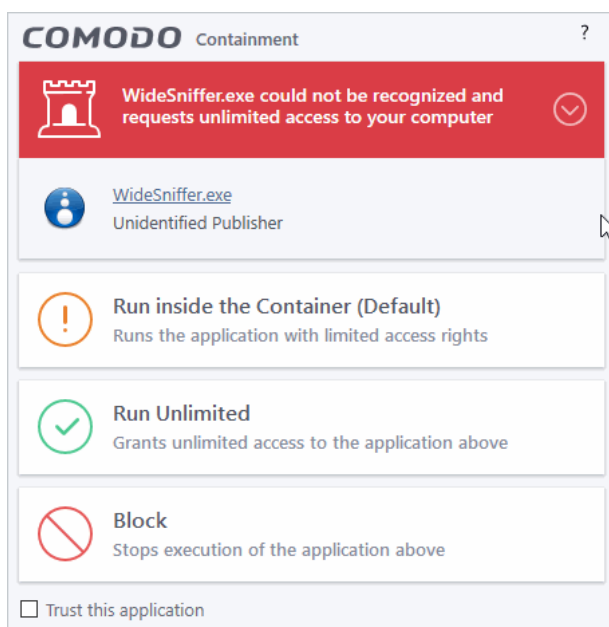
The container will display this kind of alert when the installer of an unknown application requires administrator, or elevated, privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry.

- 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.

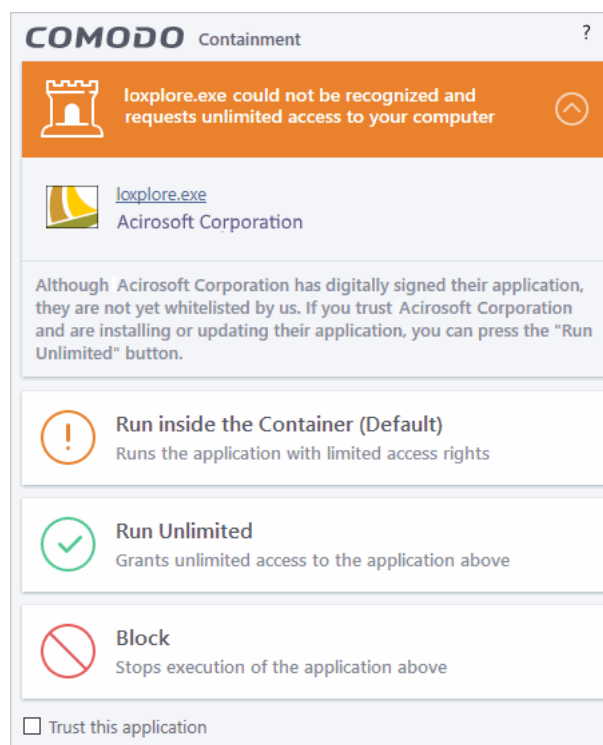
- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted access to your system resources by clicking the 'Run Isolated' button.
- If this alert is unexpected then you should abort the installation by clicking the 'Block' button (for example, you have not 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 CCS 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 the 'Detect programs which require elevated privileges e.g. installers or updaters' option and disabled the 'Do not show privilege elevation alerts' option 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')

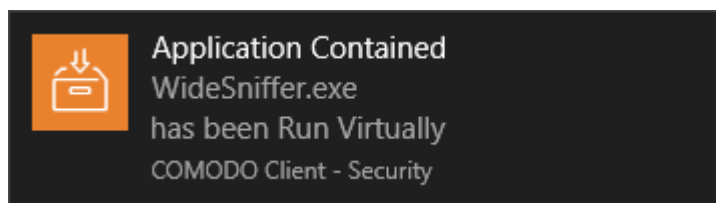
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

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

Containment Notification

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



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

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

Also see:

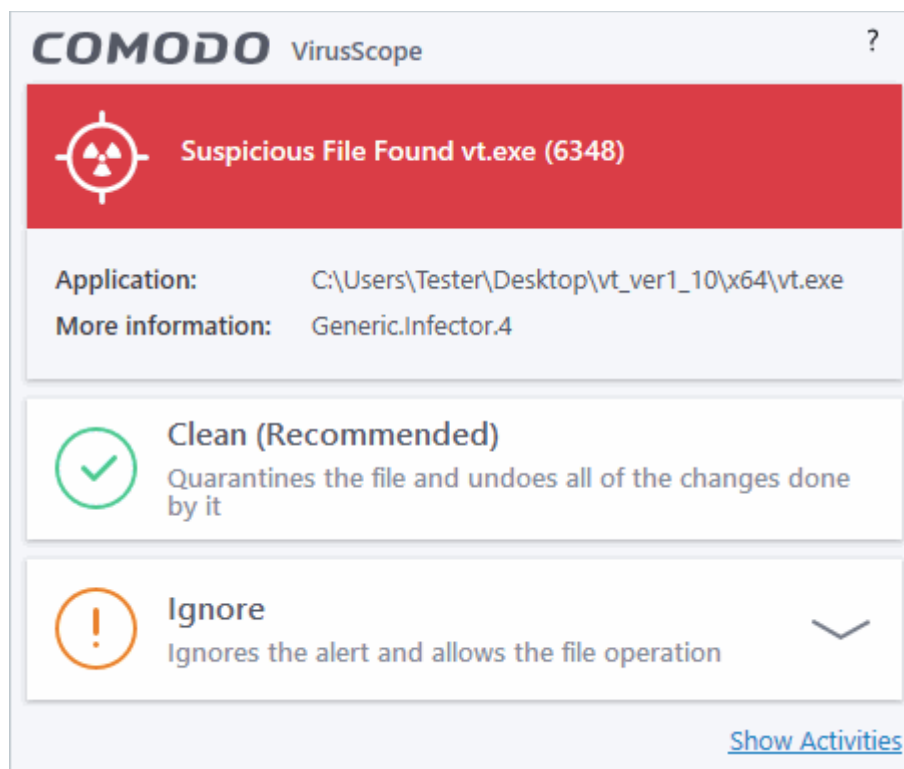
- '**Unknown Files: The Scanning Processes**' - to understand process behind how CCS scans files

Answering a VirusScope Alert

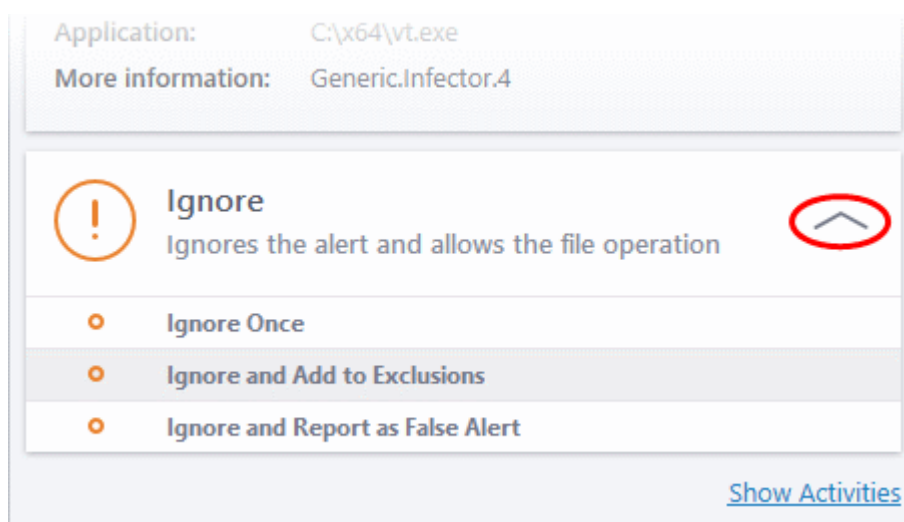
Comodo Client Security generates a VirusScope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that VirusScope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a 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:

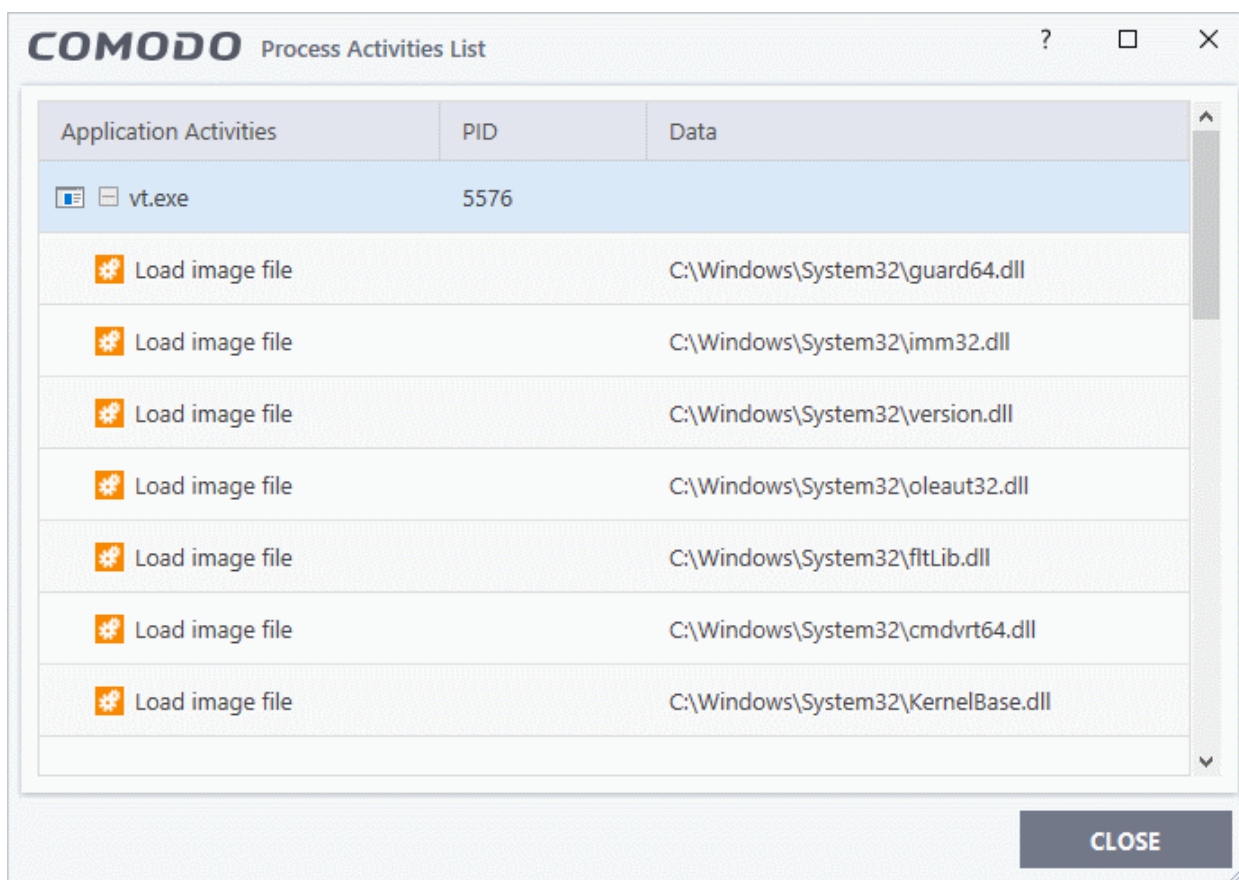
1. Carefully read the information displayed in the alert. The 'More Information' section provides you the nature of the suspicious action.



- 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 False Alert'. CCS 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.



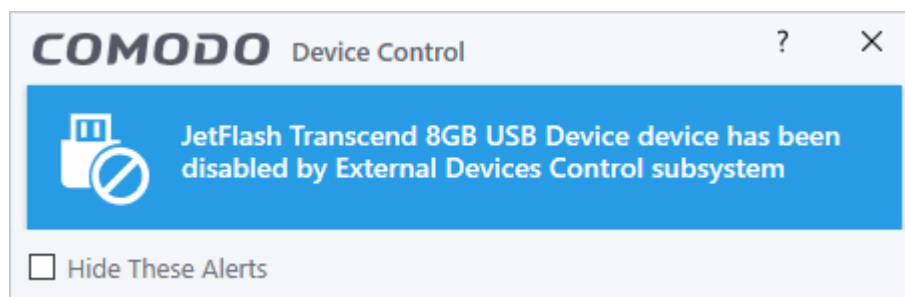
Column Descriptions

- 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.

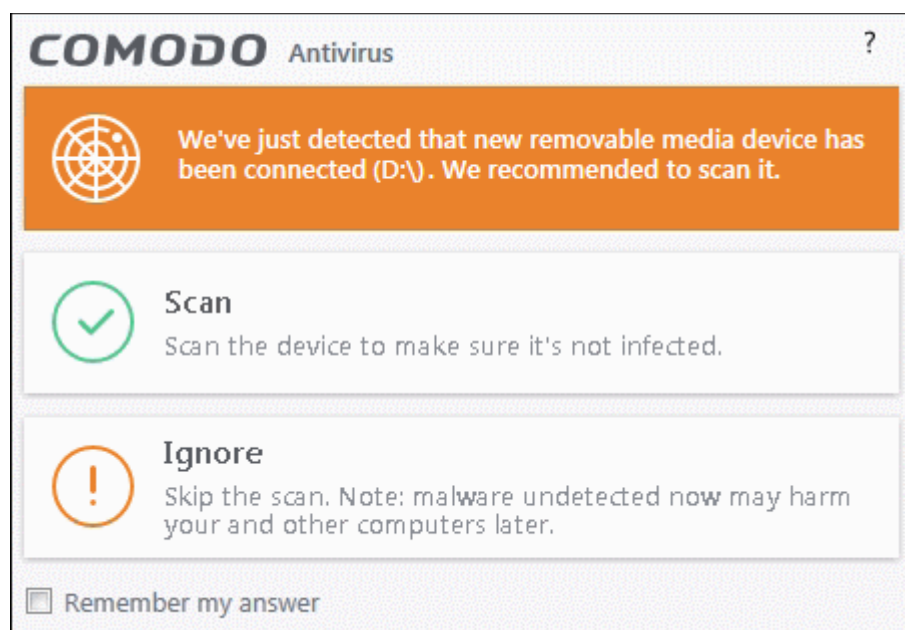
Device Control Alerts

This type of alert is shown if your administrator has blocked you from attaching certain kinds of devices to your computer. See [Device Control Settings](#) to find out more.



Auto Scan Alert

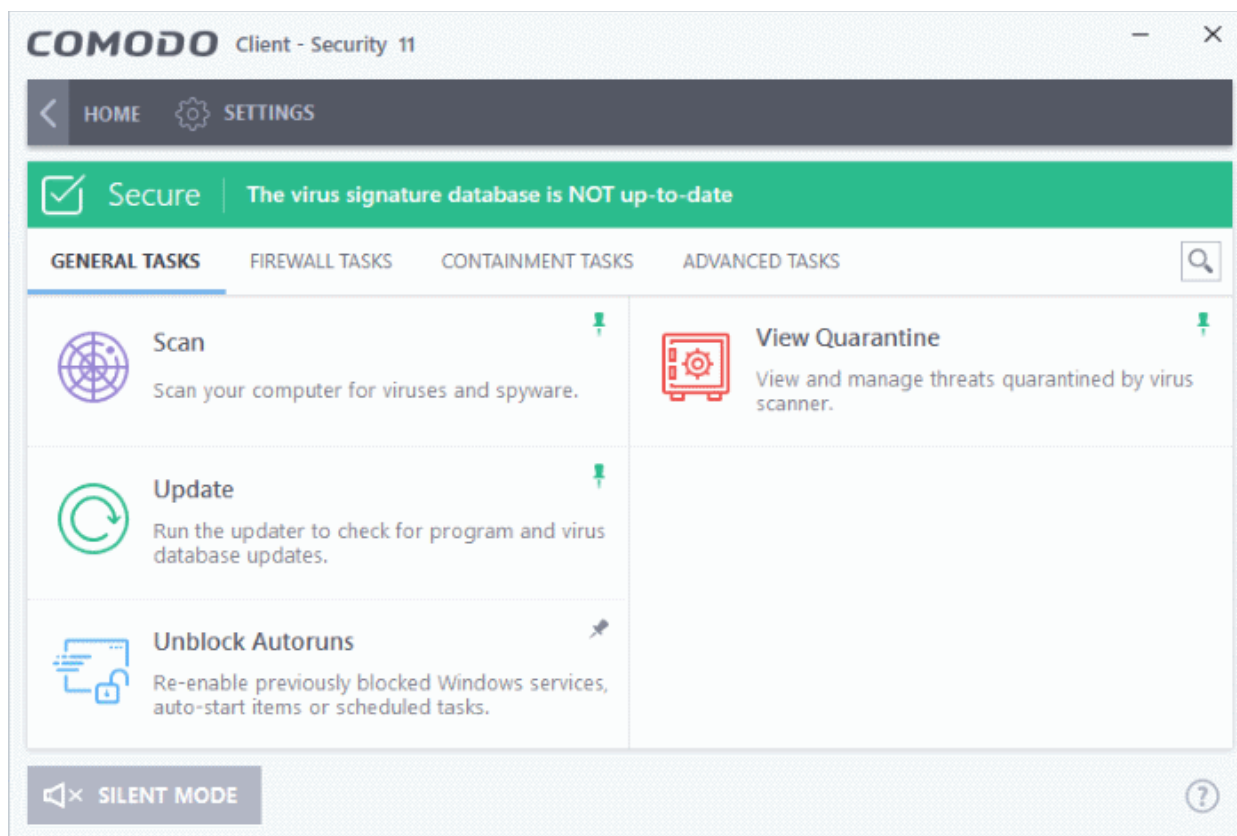
CCS will alert you when an external device such as a USB drive is connected to your computer. The alert asks you if you want to run a virus scan on the device:



- Click 'Settings' > 'Antivirus' > 'Realtime Scan' to turn these alerts on or off ('Do not show auto-scan alerts' setting)

2. General Tasks - Introduction

The 'General Tasks' interface allows you to quickly run an antivirus scan, and to check for virus database and program updates.



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

- [Scan and Clean your Computer](#)
- [Instantly Scan Files and Folders](#)
- [Processing Infected Files](#)
- [Manage Virus Database Updates](#)
- [Manage Blocked Autoruns](#)
- [Quarantined Items](#)

2.1. Scan and Clean Your Computer

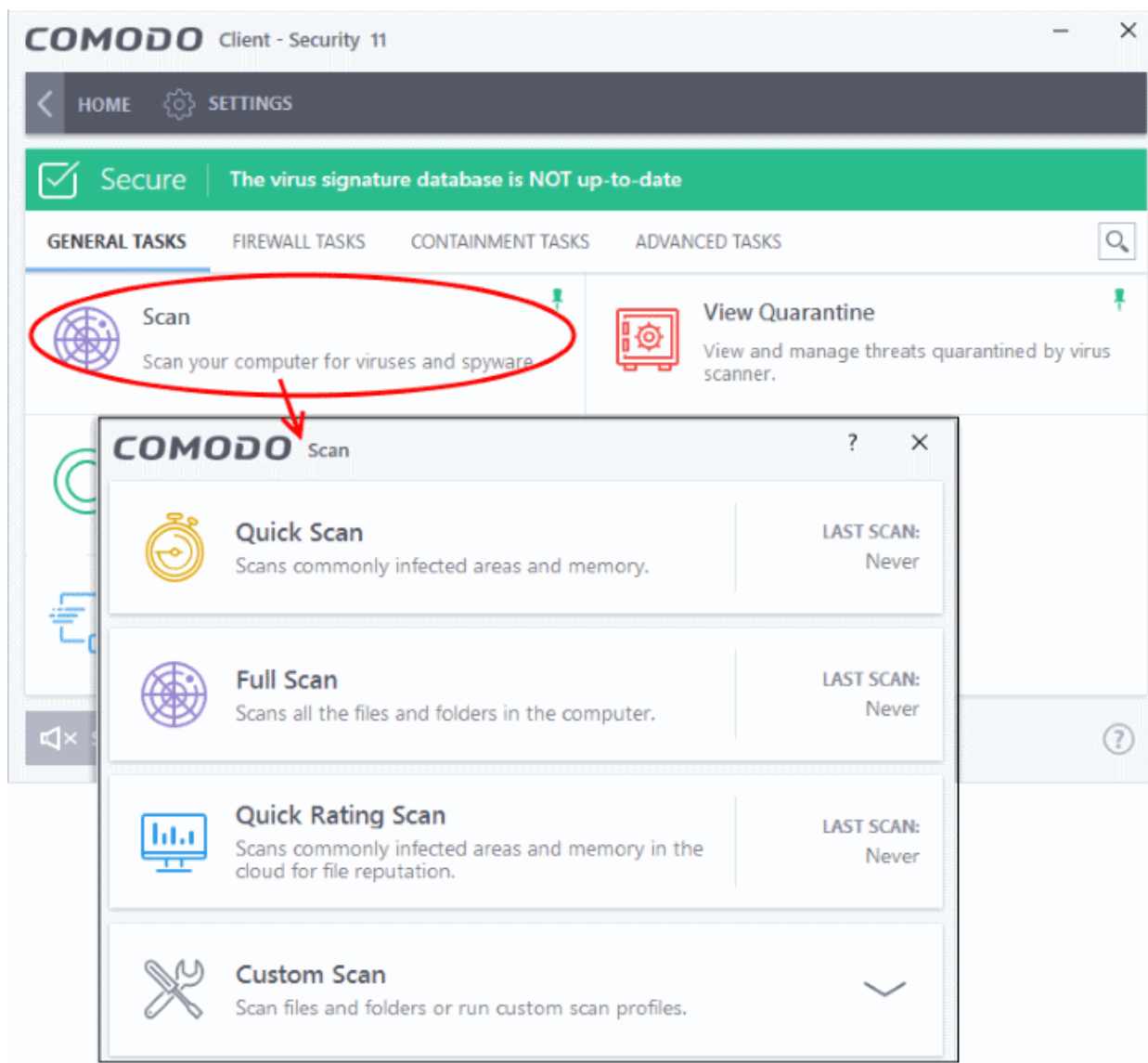
- Comodo Client Security leverages multiple technologies, including real-time monitoring and on-demand scans, to keep endpoints totally free of malware.
- You can launch an on-demand scan at any time to instantly check selected items

To run an on-demand virus scan:

- Click the 'Scan' tile on the CCS 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 check 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**
- **Scan individual file/folder**

- [Processing Infected Files](#)
- [Manage Blocked Autoruns](#)
- [Manage Quarantined Items](#)

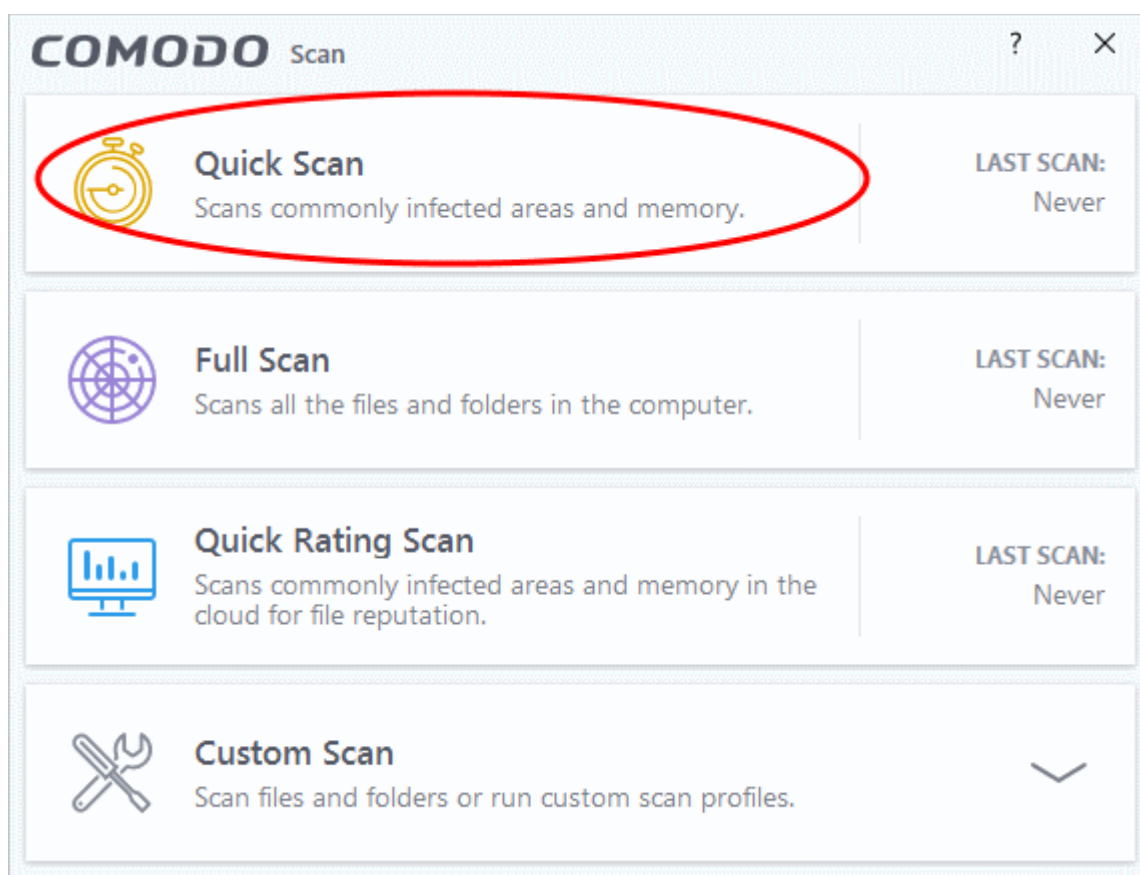
2.1.1. Run a Quick Scan

- A quick scan is a targeted scan of critical areas of your computer which are most prone to attack from malware.
- Areas scanned include system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are of great importance to the health of your computer so it is essential to keep them free of infection.

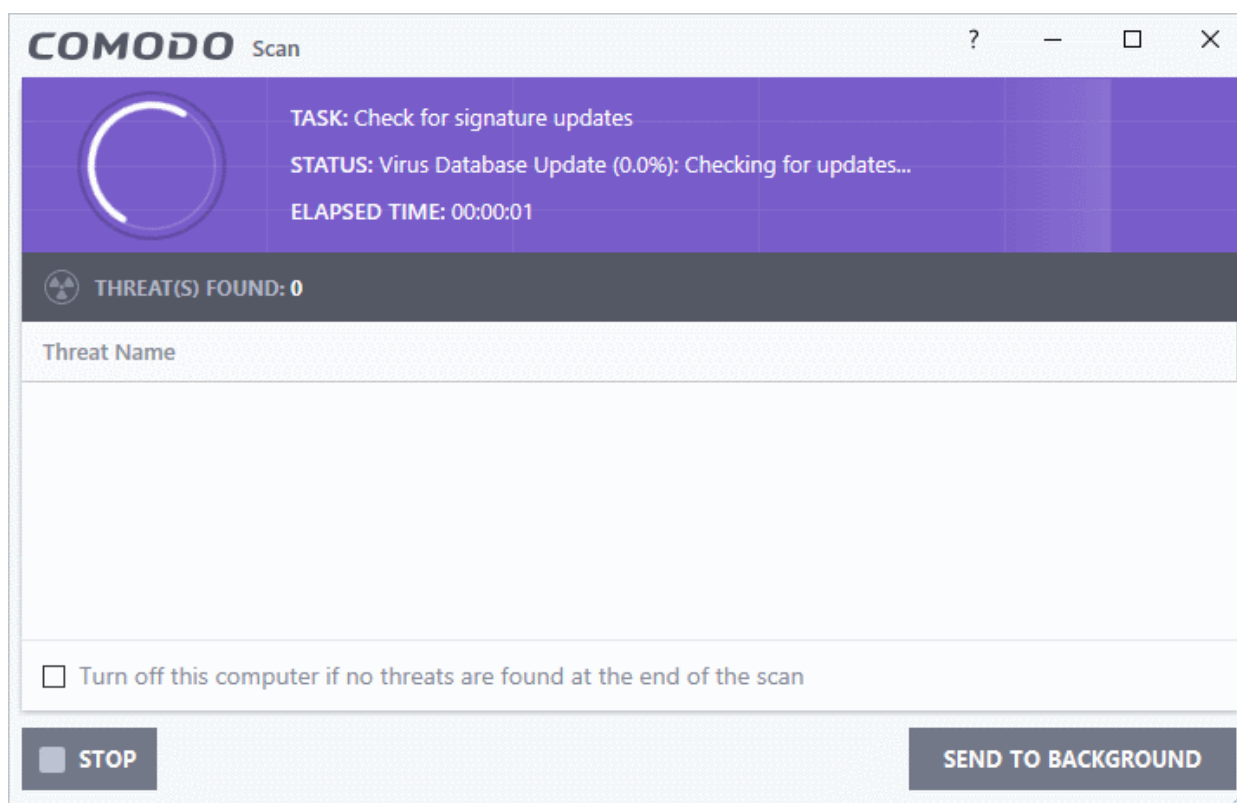
You can customize the scan parameters and create a quick-scan schedule in the 'Advanced Settings' interface. See [Antivirus Configuration](#) > [Scan Profiles](#) for more details.

To run a Quick Scan

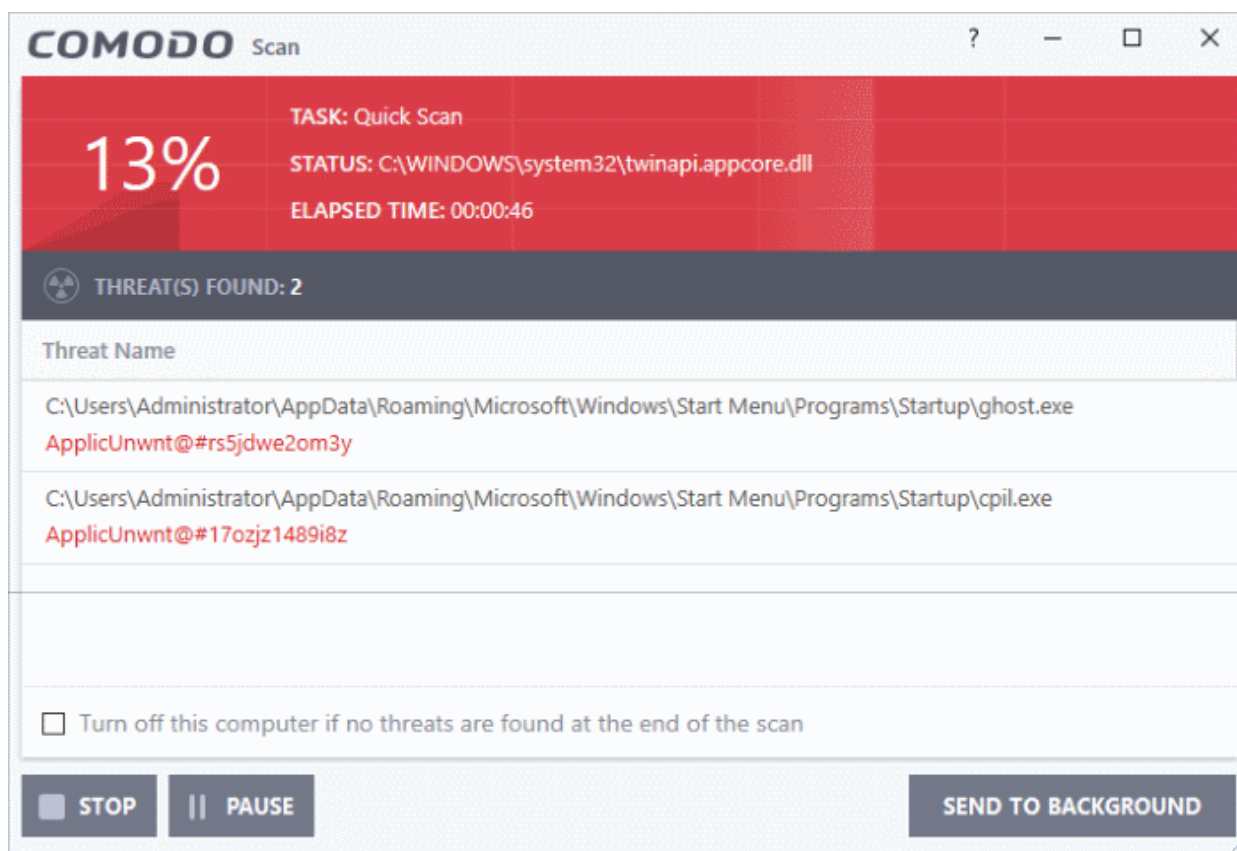
- Click the 'Scan' tile on the CCS home screen ([click here](#) for alternative ways to open the 'Scan' interface)
- Select 'Quick Scan' from the 'Scan' interface.



Depending on the quick scan settings, the scanner will start and check whether your virus signature database is up-to-date:

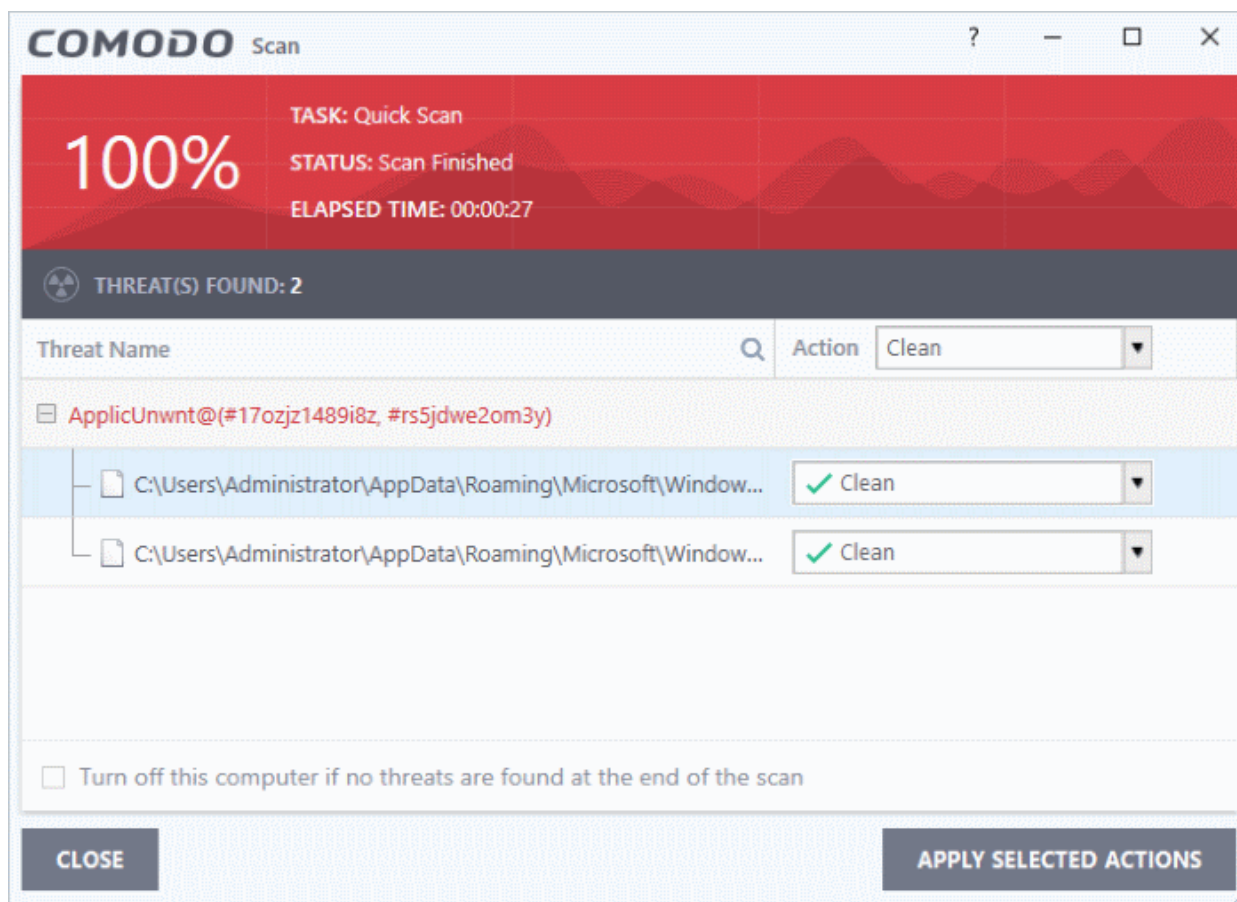


If the database is outdated, the scanner will first download and install the latest database. Once CCS has the latest database, the scanner starts the scan and the progress will be displayed:



- 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.

Scan results will be shown once the scan finishes:



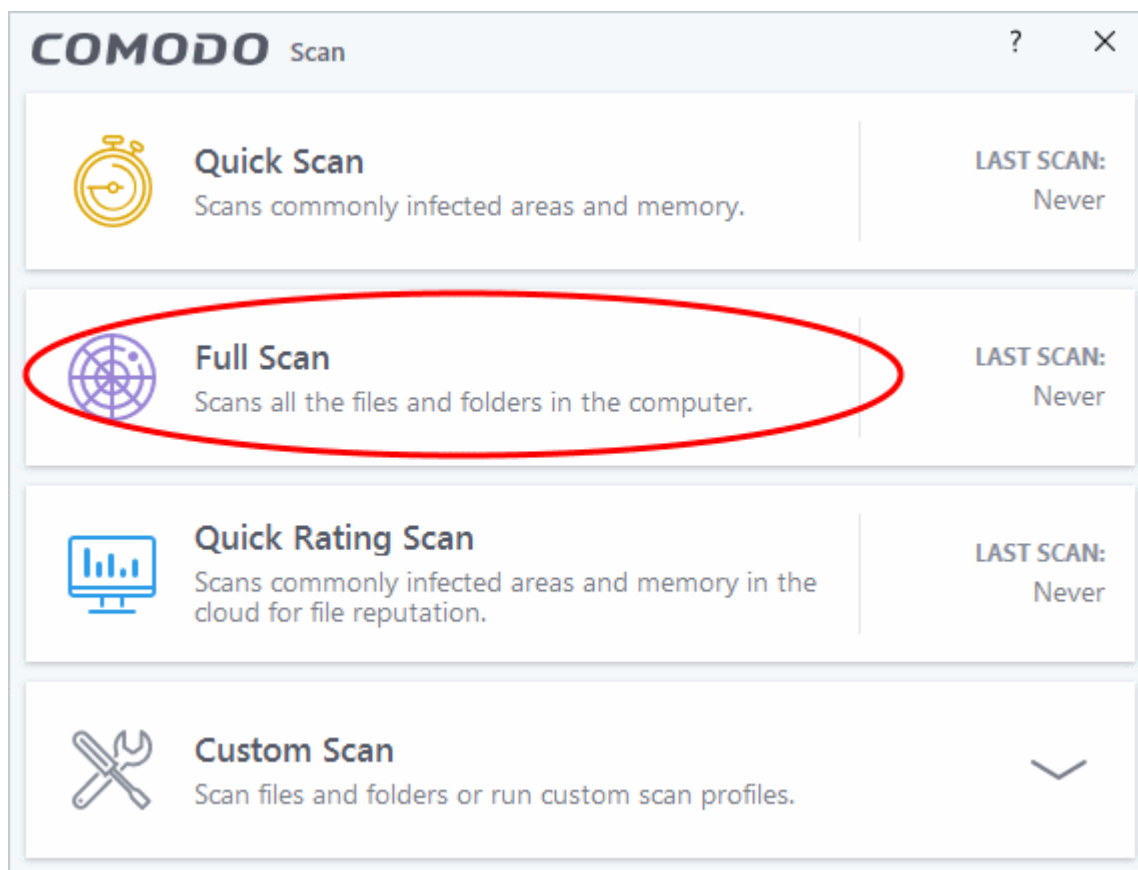
- The results window shows the number of objects scanned and the number of threats (viruses, rootkits, malware).
- Use the drop-down menu to choose whether to clean, move to quarantine or ignore the threat. See **'Processing infected files'** for more details.
- Note. You will only be presented with the options drop-down if 'Automatically clean threats' is disabled for quick scans.

2.1.2. Run a Full Computer Scan

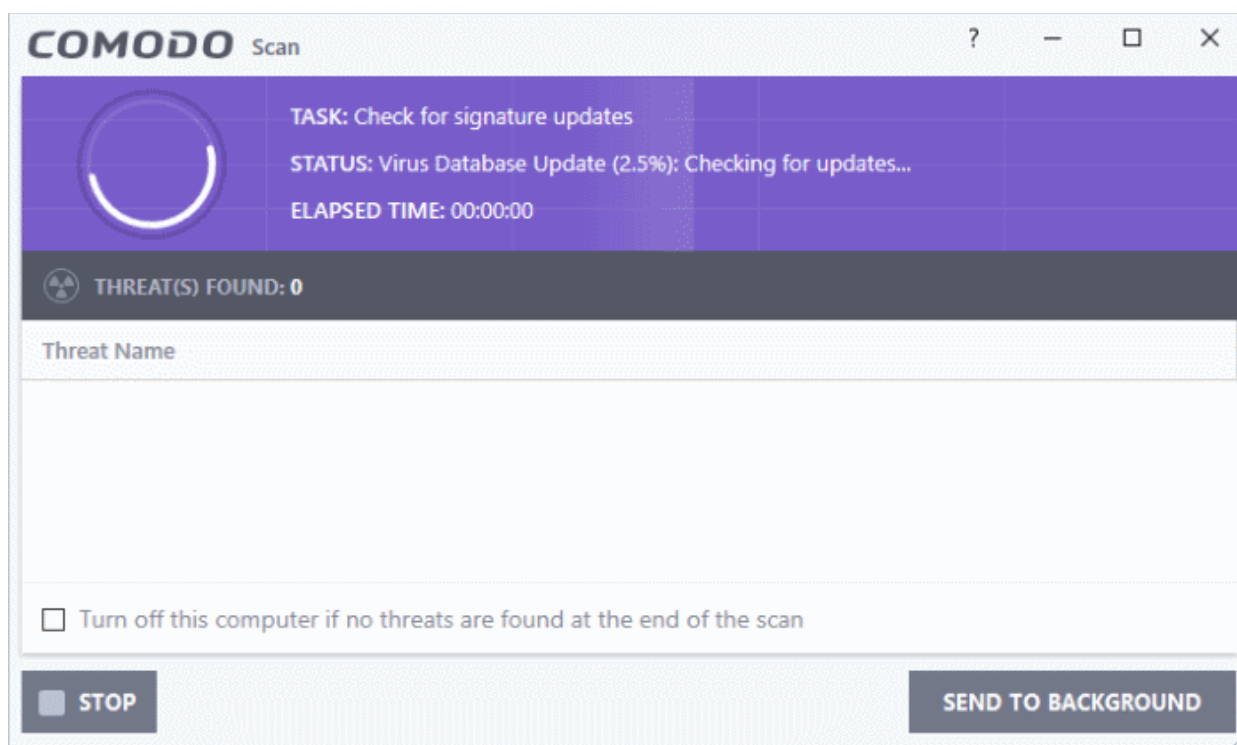
- A full system scan checks every local drive, folder and file on your system. Any connected devices like USB drives and digital cameras are also scanned.
- The advanced task interface lets you customize which items are scanned in a 'Full Scan', and to set-up a scan schedule. See **Antivirus Configuration > Scan Profiles** for more details on this.

To run a Full Computer Scan

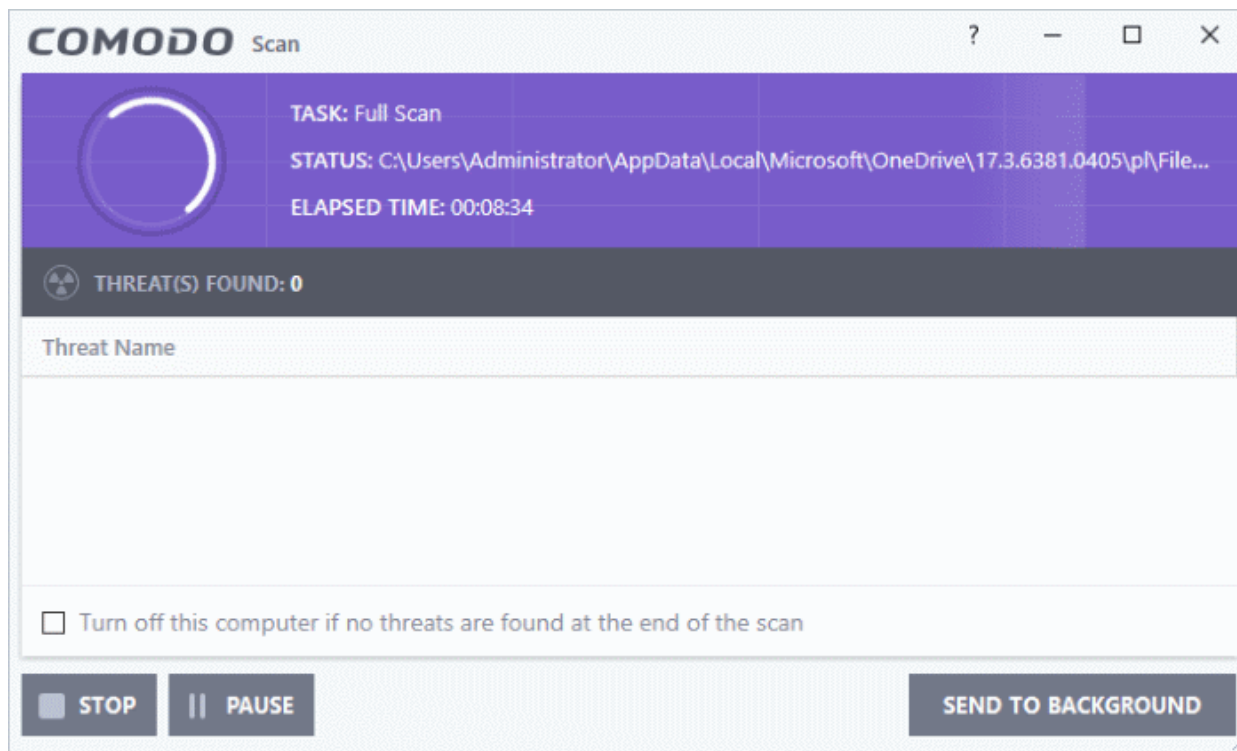
- Click the 'Scan' tile on the CCS home screen ([click here](#) for alternative ways to open the 'Scan' interface)
- Select 'Full Scan' from the 'Scan' interface.



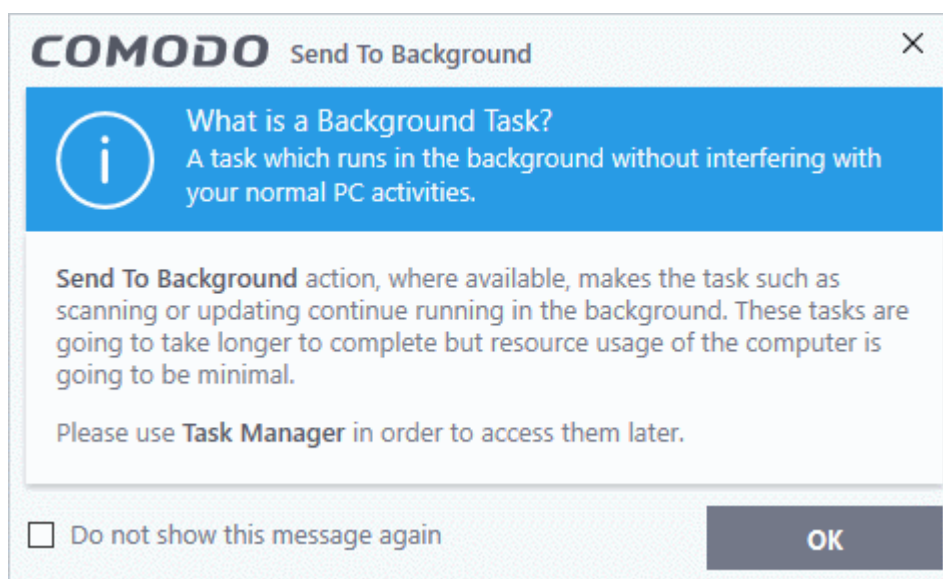
Depending on the full scan settings, the scanner will start and check whether your virus signature database is up-to-date:



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

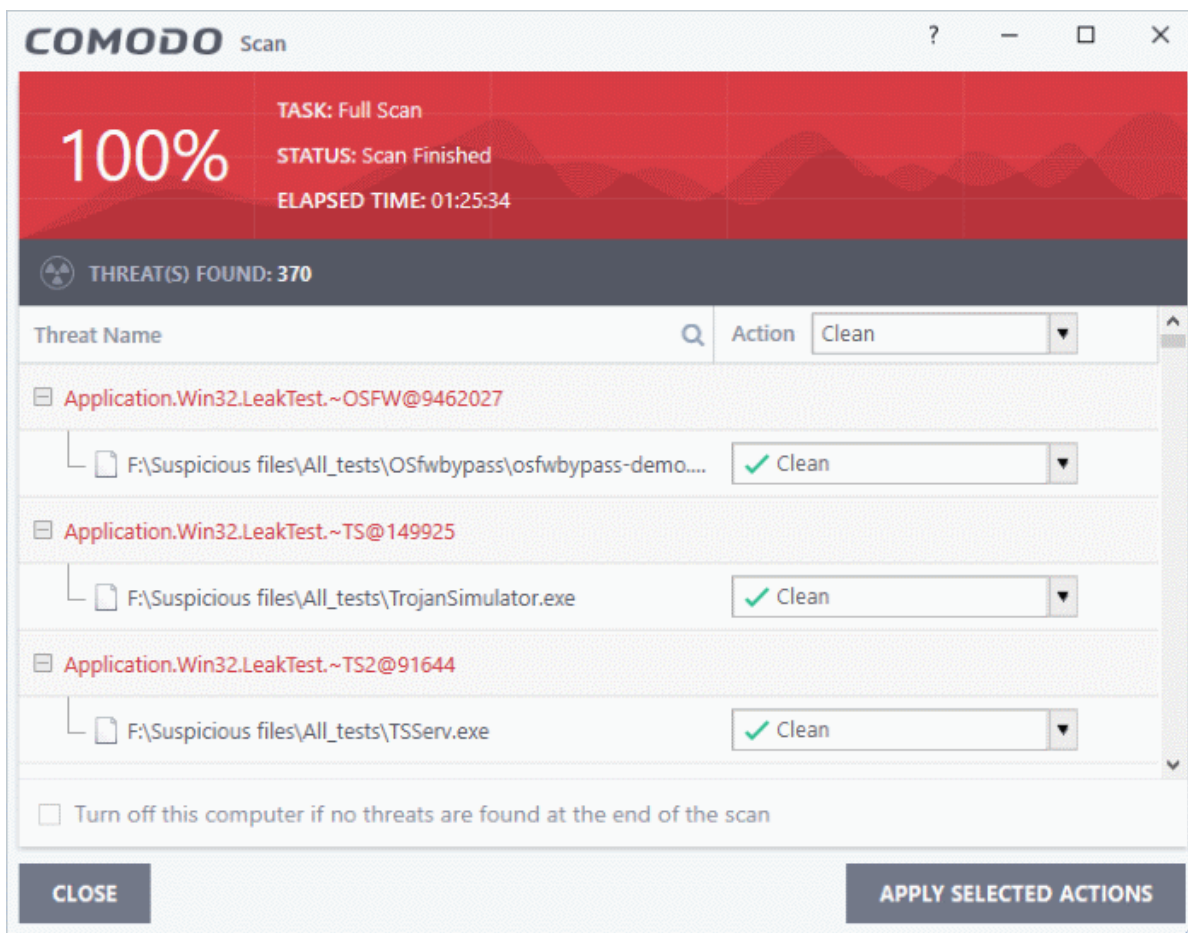


- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



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

- On completion of scanning, the results window will be displayed.



- 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 infected files**' for more details.
- Note. You will only be presented with the options drop-down if 'Automatically clean threats' is disabled for full scans.

2.1.3. Run a Rating Scan

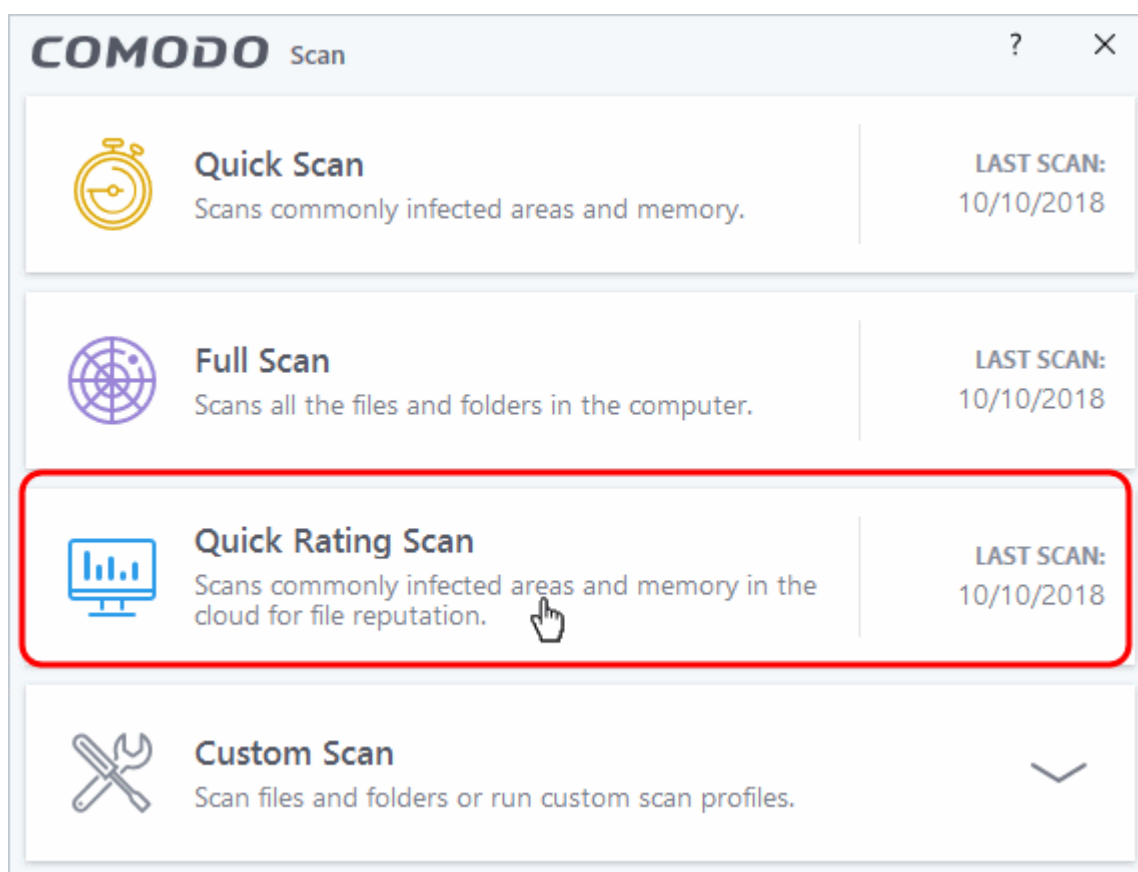
- The 'Quick Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.
- Scanned areas include system memory, auto-run entries, hidden services, system files and important registry keys.

File ratings are as follows:

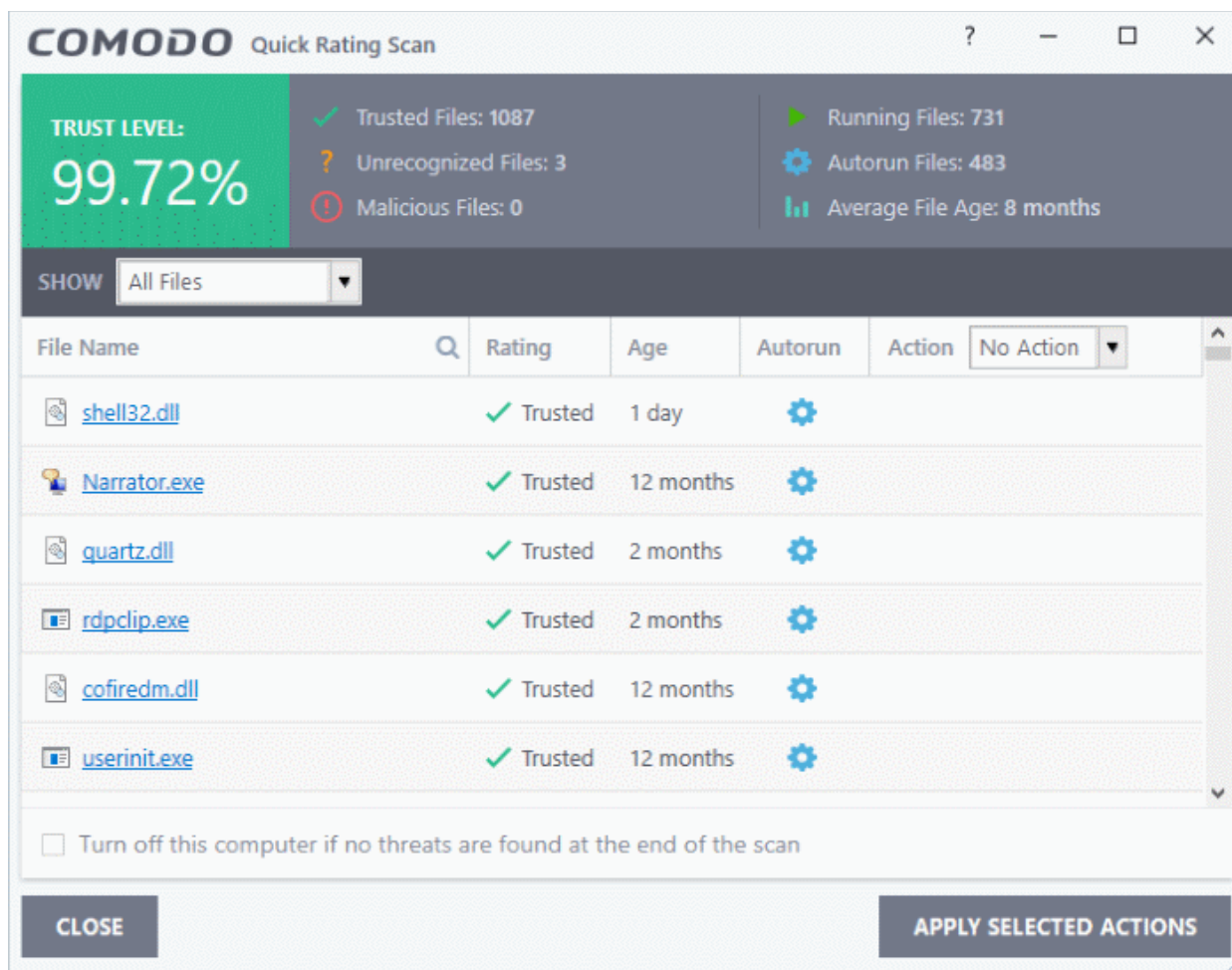
- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Malicious - the file is unsafe and contains harmful code. You will be presented with disinfection options for such files.

To run a Quick Rating scan

- Click the 'Scan' tile on the CCS home screen
- Select 'Quick Ratings Scan':



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

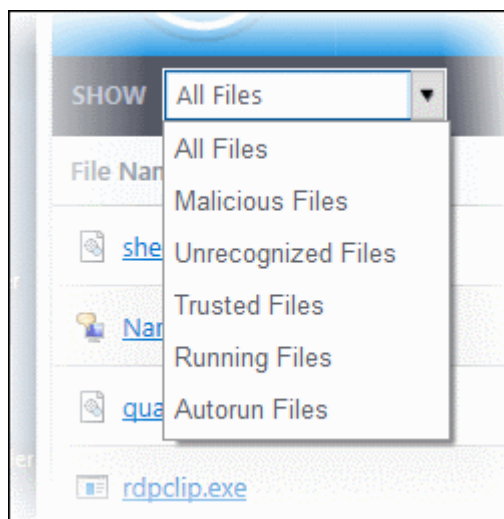


Rating Scan Results Table - Column Descriptions	
Column Header	Description
File name	The label of the scanned file
Rating	The reputation of the file. This is awarded after the rating scan. Possible values are: <ul style="list-style-type: none"> Trusted Unrecognized Malicious
Age	The period of time that the file has been on your computer
Auto-run	Indicates whether the file runs automatically or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately.
Action	Lets you implement an action on selected files.

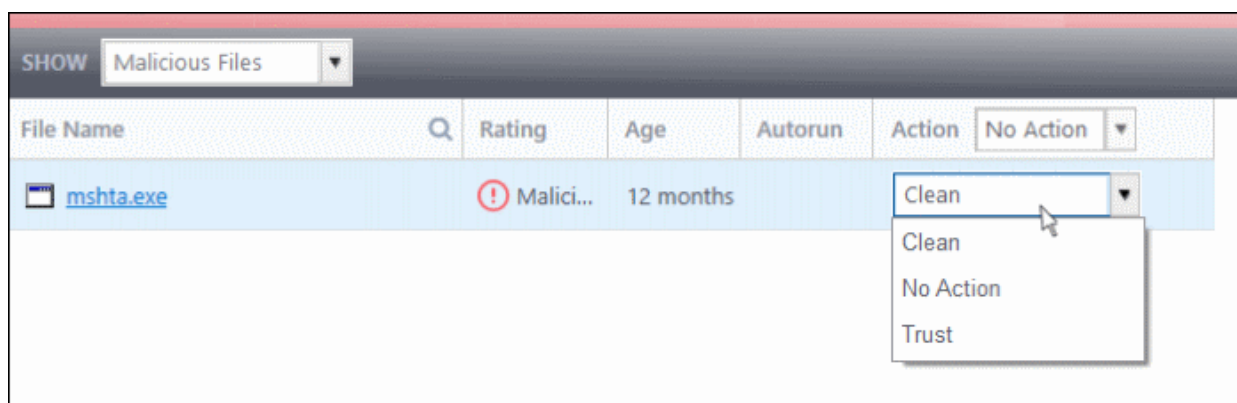
Files are rated as:

- Trusted - the file is safe
- Unrecognized - the trustworthiness of the file could not be assessed and submitted to Valkyrie for analysis.
- Malicious - the file is unsafe and contains harmful code. You are presented with disinfection options for such files.

Use the the 'Show' drop-down to filter results by file rating or file type:

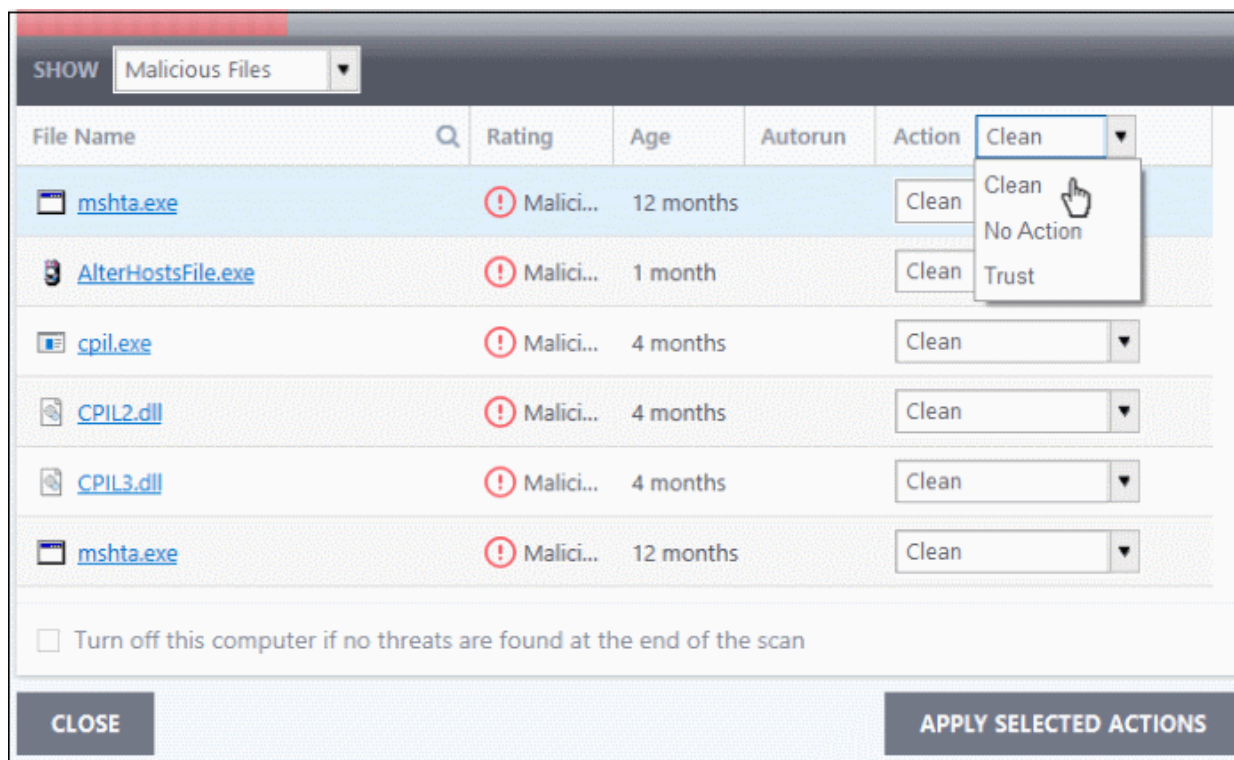


- The drop-down menu next to a malicious file gives you the following options:



- **Clean** - The file will be disinfected if a disinfection routine exists. It will be moved to quarantine if no disinfection routine exists. See '[Manage Quarantined Items](#)' for more info.
- **No Action** - Ignores the warning. The file will be flagged again the next time it is scanned.
- **Trusted** - Locally whitelists the file. It will be allowed to run as normal and will not be flagged by future rating or antivirus scans.

To apply the same action to all 'Unrecognized' and 'Malicious' files, first filter the category from the 'Show' drop-down and select 'Unrecognized' / 'Malicious'. Then choose the action from the drop-down menu at the top of the 'Action' column.



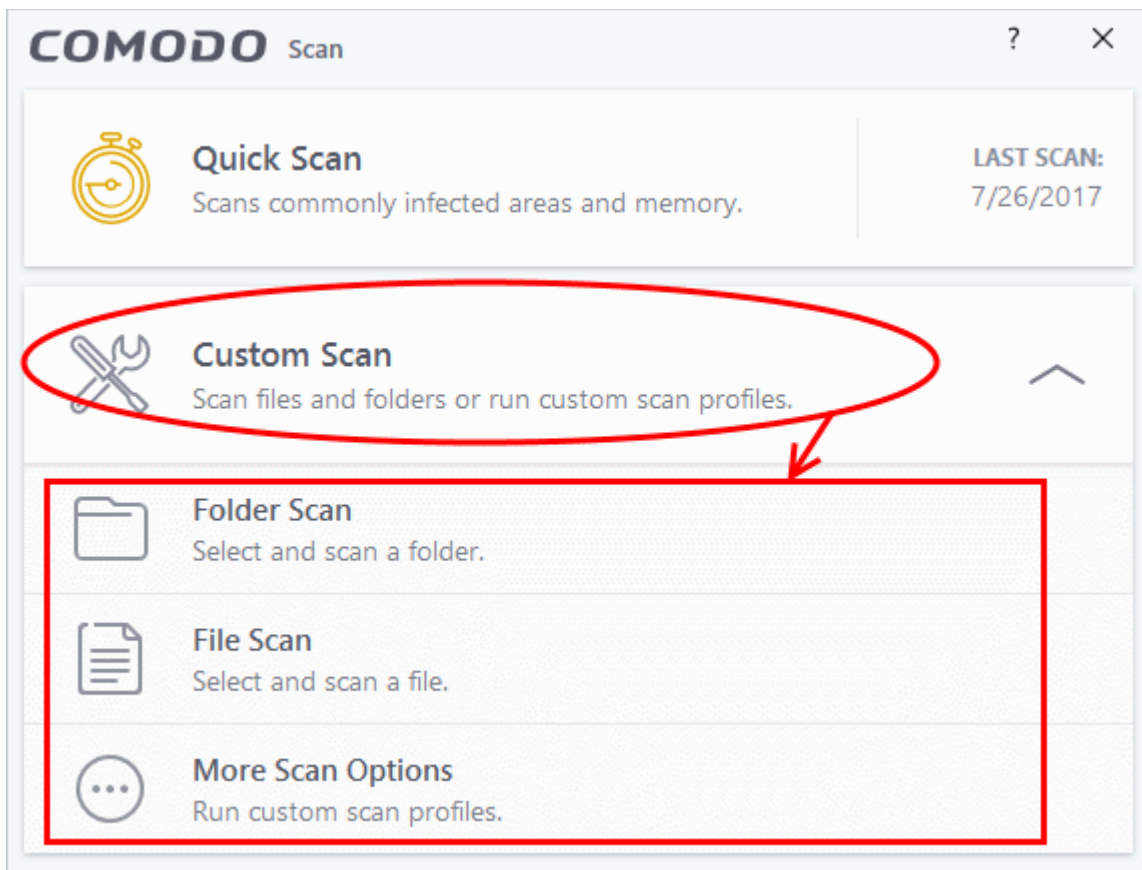
- Click 'Apply Selected Actions' to implement your choice. The selected actions will be applied and a progress bar will be displayed underneath the results.
- Click 'Close' to exit.

2.1.4. Run a Custom Scan

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

To run a custom scan

- Click the 'Scan' tile on the CCS 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 individual folders
- **File Scan** - scan an individual file
- **More Scan Options** - create a custom scan profile here

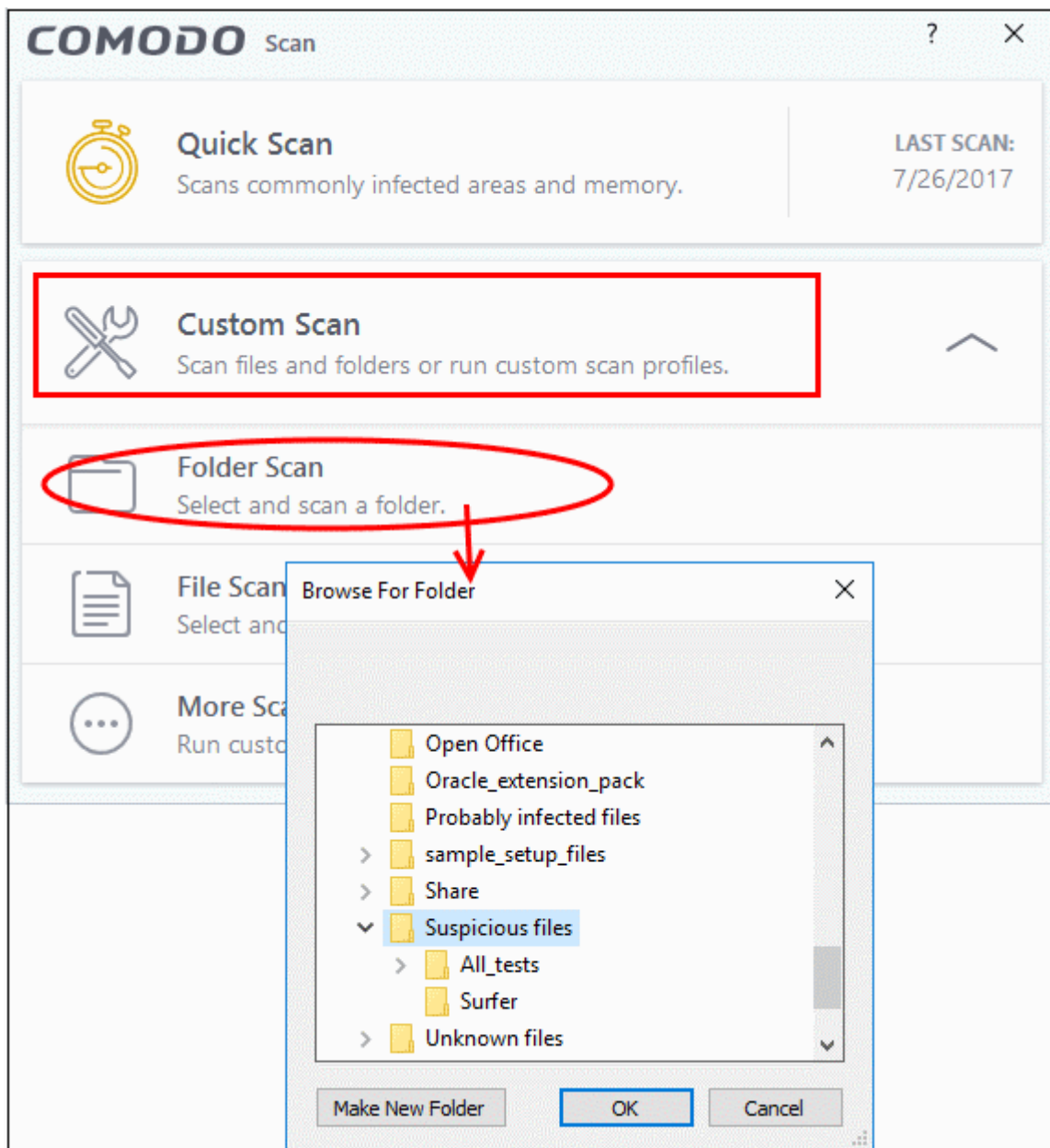
2.1.4.1. Scan a Folder

The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from the internet and want to scan it for viruses and other threats before you open it.

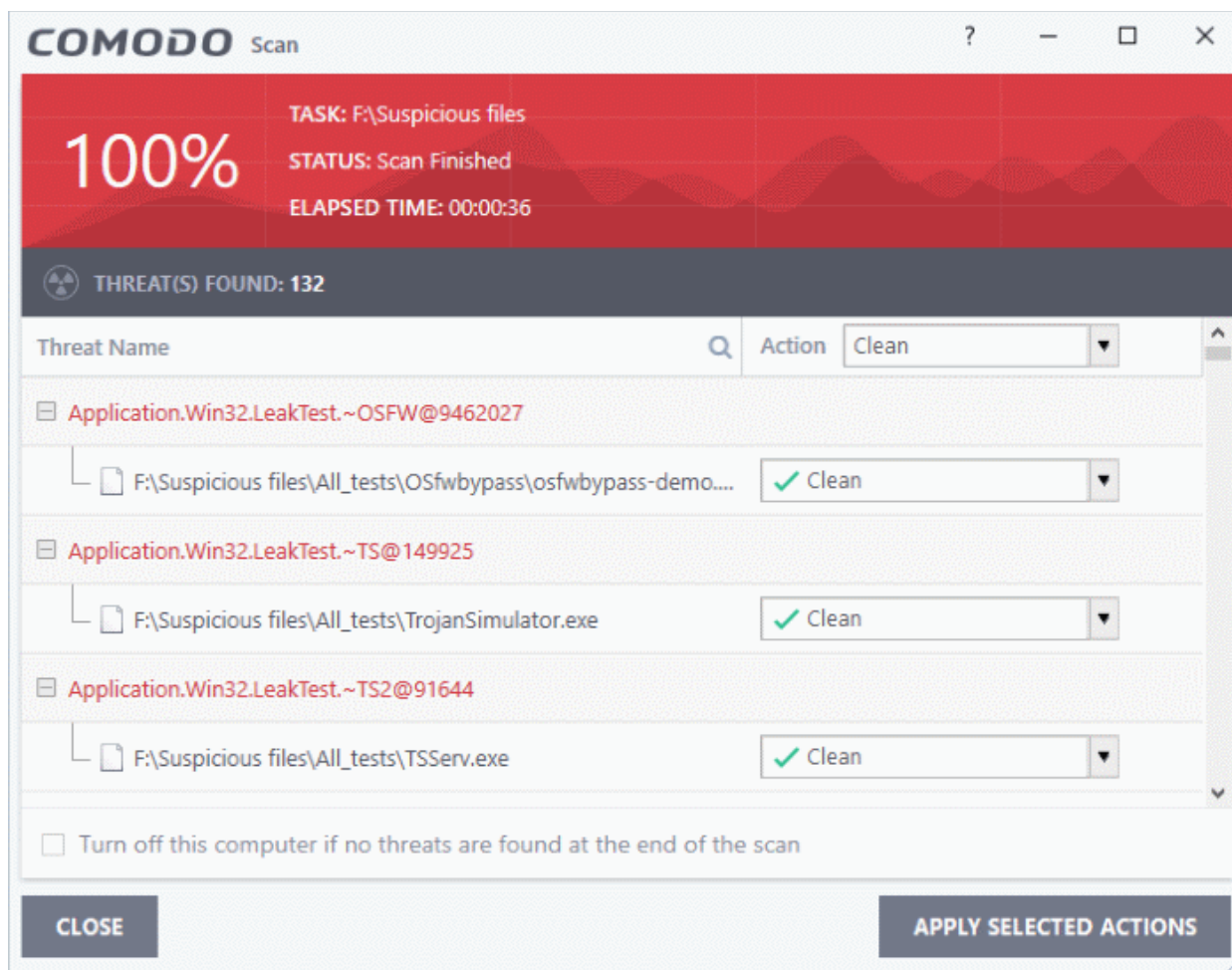
Tip: As an alternative, you can quickly scan a folder by right clicking on it and selecting the option 'Scan with Comodo Antivirus'. See '**Instantly Scan Individual Files and Folders**' for more details.

To scan a specific folder

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



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



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

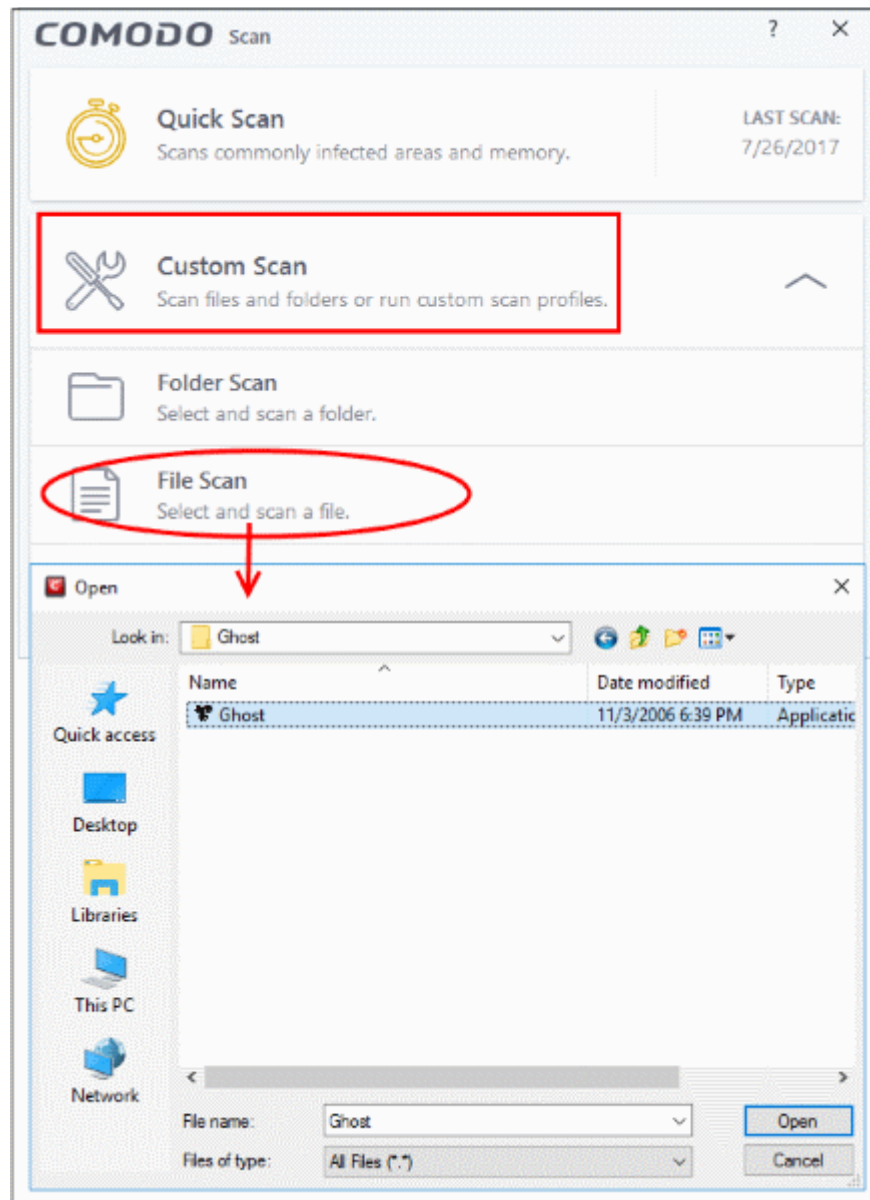
2.1.4.2. Scan a File

A custom scan allows you to scan specific files on your hard drive, CD/DVD or external device. For example, you might have downloaded a file from the internet which you want to scan for threats before you open.

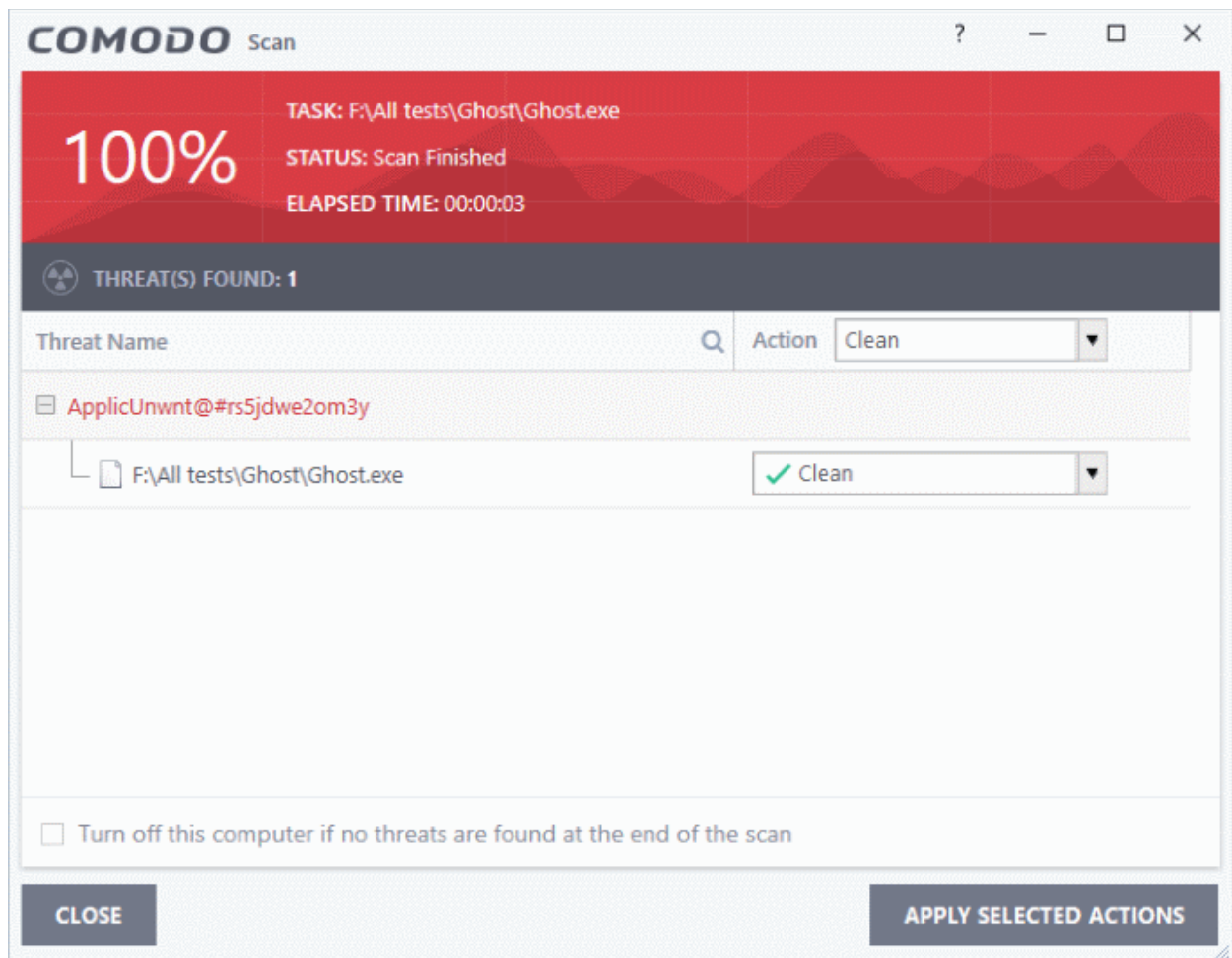
Tip: As an alternative, you can quickly scan a file by right clicking on it and selecting the option 'Scan with Comodo Antivirus'. See '[Instantly Scan Individual Files and Folders](#)' for more details.

To scan a specific file

- Click the 'Scan' tile on the CCS home screen ([click here](#) for alternative ways to open the 'Scan' interface)
- Select 'Custom Scan' from the 'Scan' interface then 'File Scan'



- Browse to the file you want to scan and click 'Open'.



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

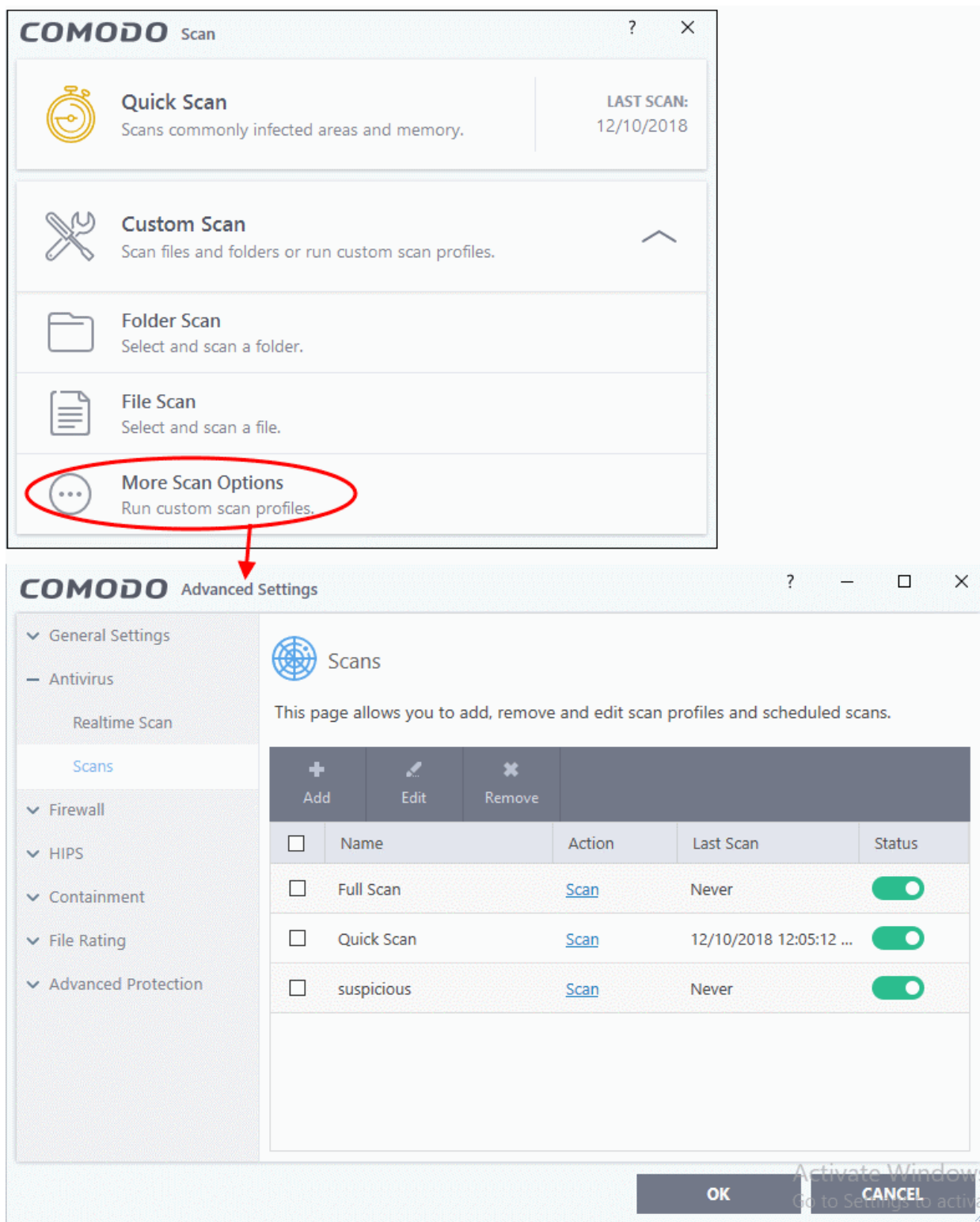
2.1.4.3. Create, Schedule and Run a Custom Scan

- Custom scan profiles let you configure a scan of specific areas with your own scan settings.
- Each profile lets you define exactly which items to scan, what time they should be scanned, and other scan parameters.
- Once created and saved, your profile will appear in the 'scans interface' and can be run at any time.
 - [Creating a Scan Profile](#)
 - [Running a custom scan](#)

To create a custom profile

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

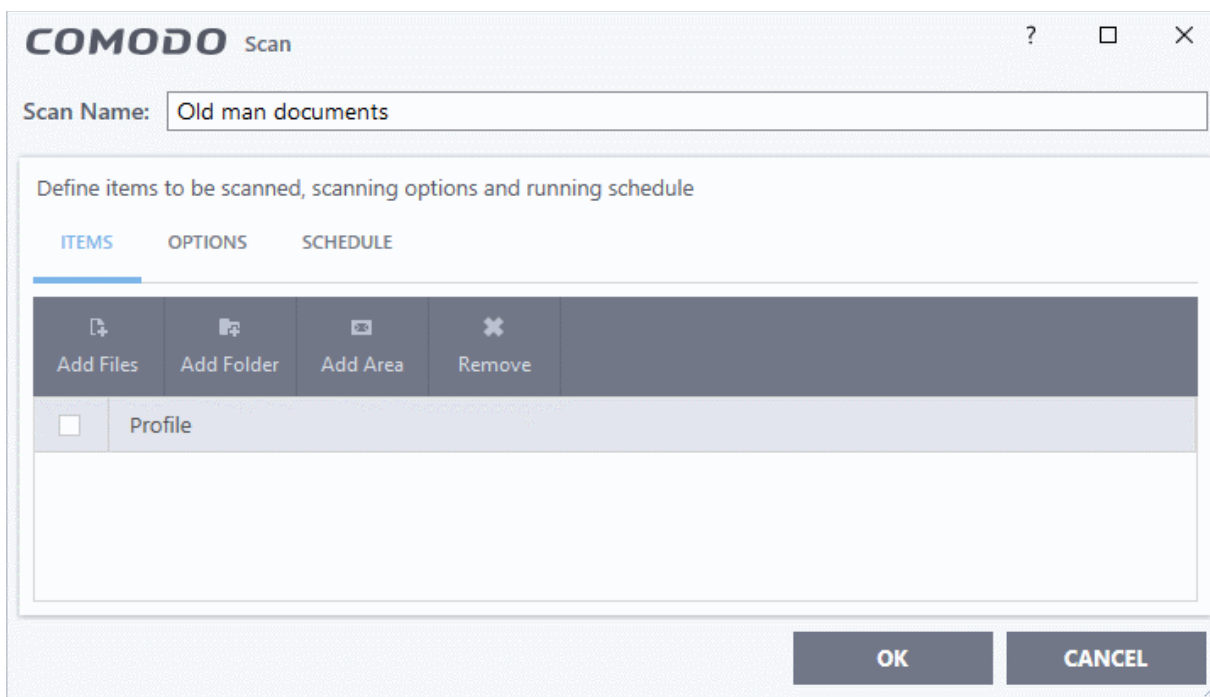
The 'Advanced Settings' interface will open at the 'Scans' page. This shows a list of pre-defined and user created scan profiles. You can create and manage new custom scan profiles from this interface:



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

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

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



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

The next steps are to:

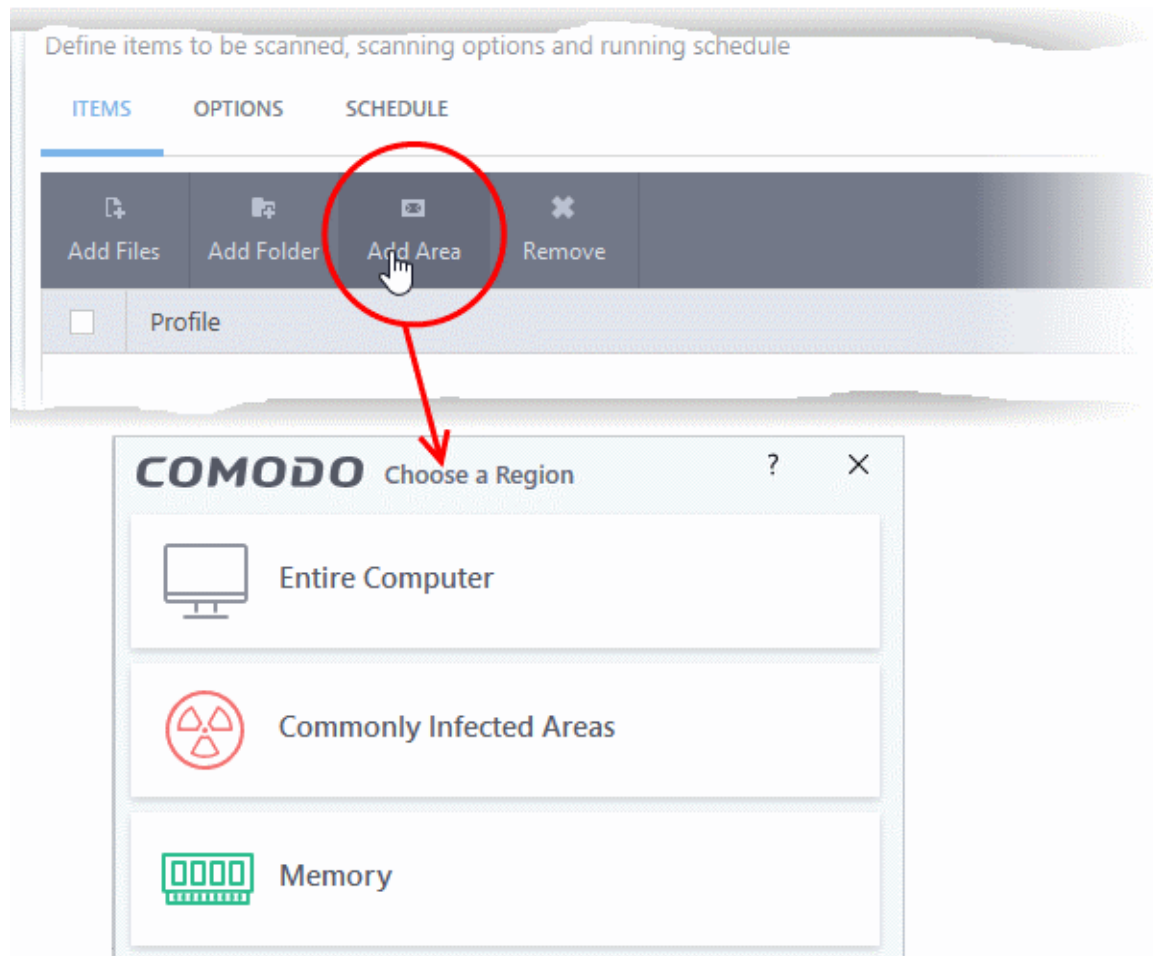
- **Select the items to scan**
- **Configure the scanning options for the profile (Optional)**
- **Configure a schedule for the scan to run periodically (Optional)**

Select the items to scan

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

The buttons along the top let you add three types of item to the scan:

- **Files** - Add individual files to the profile. Click the 'Add Files' button and navigate to the file you want to include in the scan. Repeat to add more files.
- **Folders** - Add entire folders to the profile. Click the 'Add Folder' button and choose the folder from the 'Browse for Folder' dialog.
- **Areas** - Add pre-defined regions to the profile. Regions include 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.

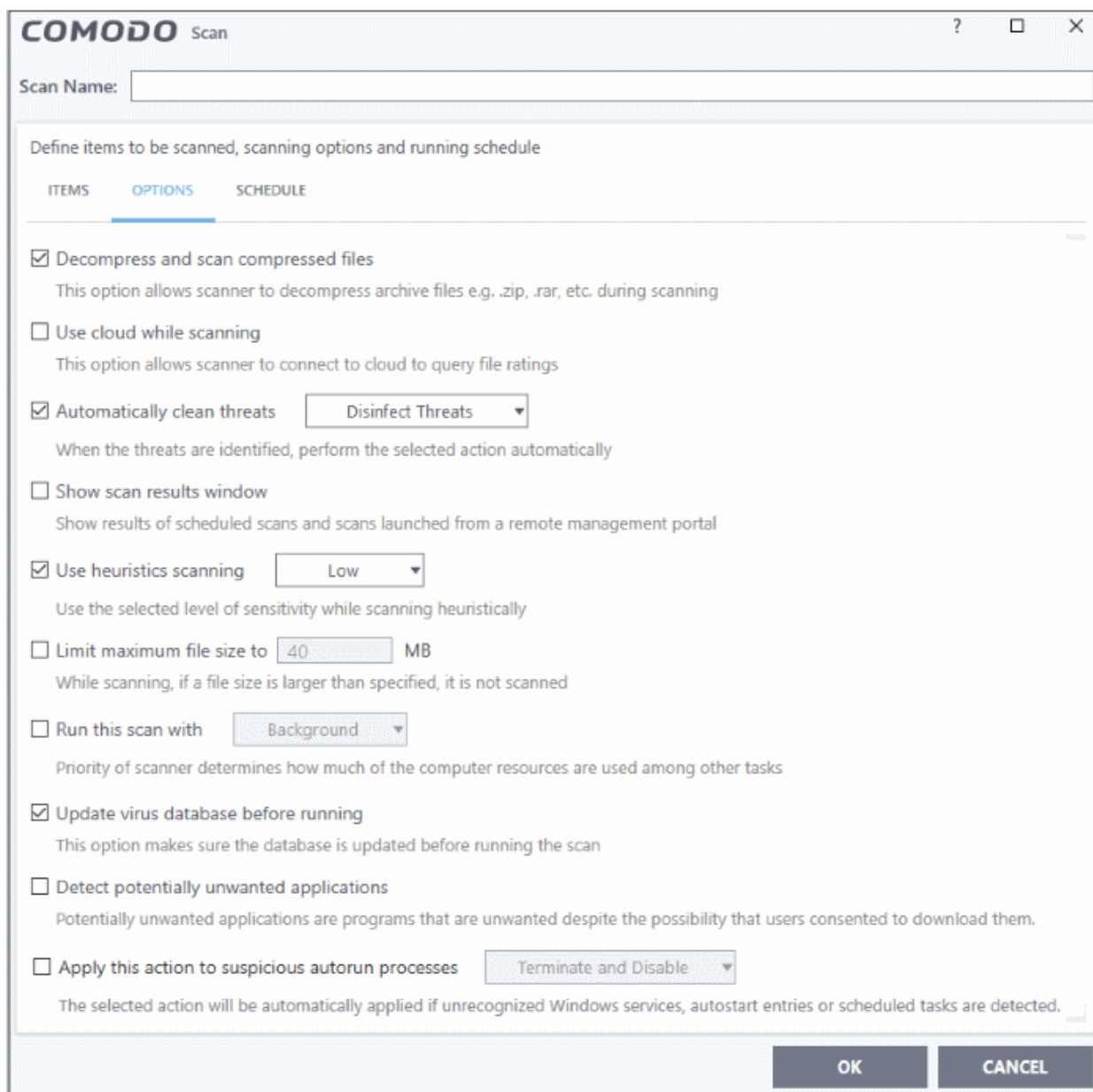


- Repeat the process to add more items to the profile.
- To remove an item, select it and click 'Remove'.

To configure Scanning Options

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

The options to customize the scan will be displayed.



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

The available options are:

- **Quarantine Threats** - Malicious items will be moved to quarantine. You can view the items in the quarantine and choose to remove them or restore them (in case of false positives). See **'Manage Quarantined Items'** for more details.
- **Disinfect Threats** - If a disinfection routine is available for the detected threat, the antivirus will remove the threat from the infected file and retain the application safe. Otherwise the item will be moved to 'Quarantine'.
- **Show scan results window** - If selected, displays the number of objects scanned and the number

of threats (Viruses, Rootkits, Malware and so on) found during scheduled scan and scan executed from remote management portal.

- **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. (**Default = Enabled**).

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

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

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

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

Note 2 - CCS 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**.

To schedule the scan to run at specified times

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

The screenshot shows the 'COMODO Scan' dialog box with the 'SCHEDULE' tab selected. The 'Scan Name' field is empty. The 'Define items to be scanned, scanning options and running schedule' section has three tabs: 'ITEMS', 'OPTIONS', and 'SCHEDULE'. Under 'Frequency', the 'Do not schedule this task' option is selected. Other options include 'Every few hours', 'Every Day', 'Every Week', and 'Every Month'. The 'Additional Options' section contains four unchecked checkboxes: 'Run only when computer is not running on battery', 'Run only when computer is IDLE', 'Turn off computer if no threats are found at the end of the scan', and 'Run during Windows Automatic Maintenance'. 'OK' and 'CANCEL' buttons are at the bottom right.

You have the following options:

- **Do not schedule this task** - The scan profile will be created but will not run automatically. The profile will be available for manual, on-demand scans.
- **Every few hours** - Scans the areas defined in the profile every 'x' hours. You can specify the number of hours in the 'Repeat scan 'x' hours' field.
- **Every Day** - Scans the areas defined in the profile every day at the time specified in the 'Start Time' field.
- **Every Week** - Scans the areas defined in the profile on the day(s) specified in 'Days of the Week' field at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- **Every Month** - Scans the areas defined in the profile on the date(s) specified in 'Days of the month' field at the time specified in the 'Start Time' field. You can select the dates of the month by

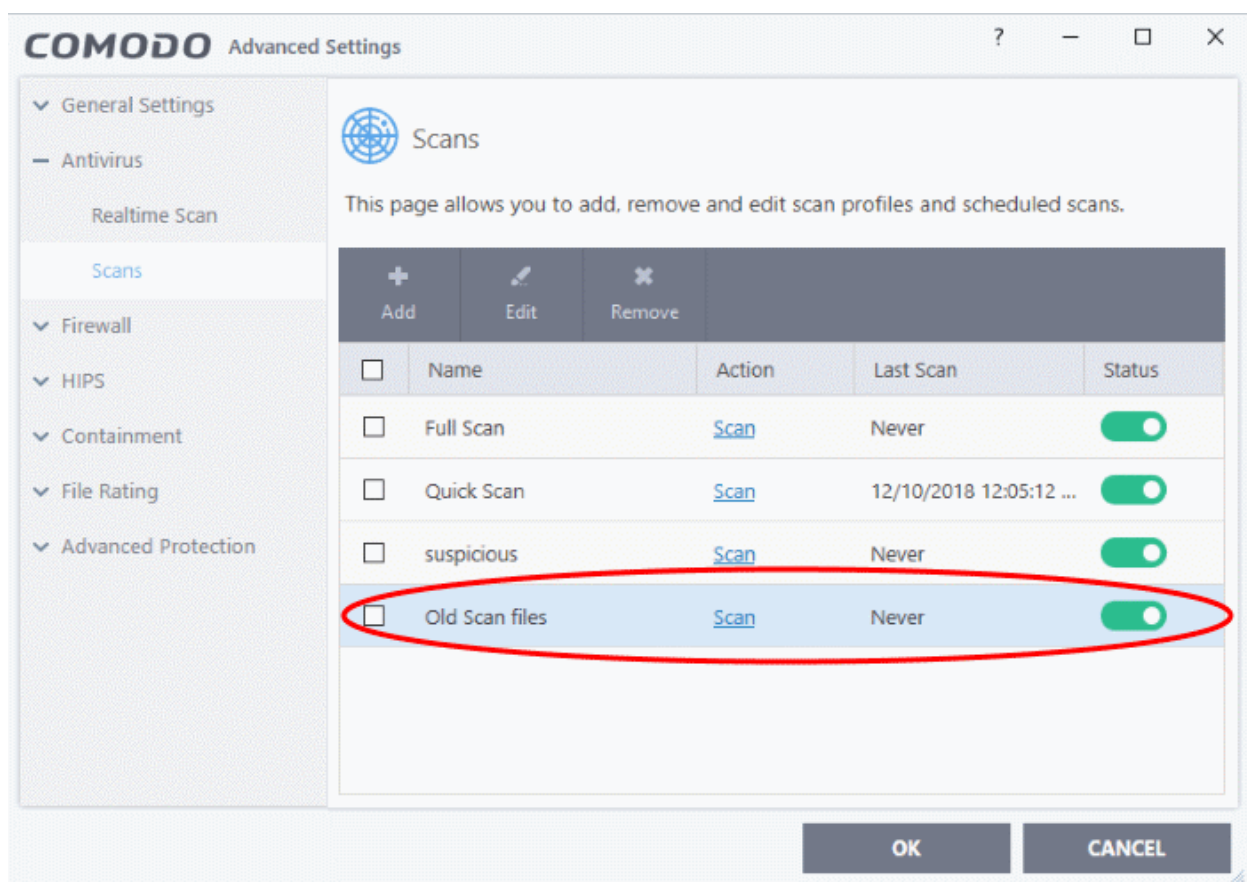
clicking on them.

- **Run only when computer is not running on battery** - The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or any other battery driven portable computer.
- **Run only when computer is IDLE** - The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- **Run during Windows Maintenance** - Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.
- The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See the explanation of **Automatically Clean Threats** above.

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

- Click 'OK' to save the profile.

The profile will be available for deployment in future.



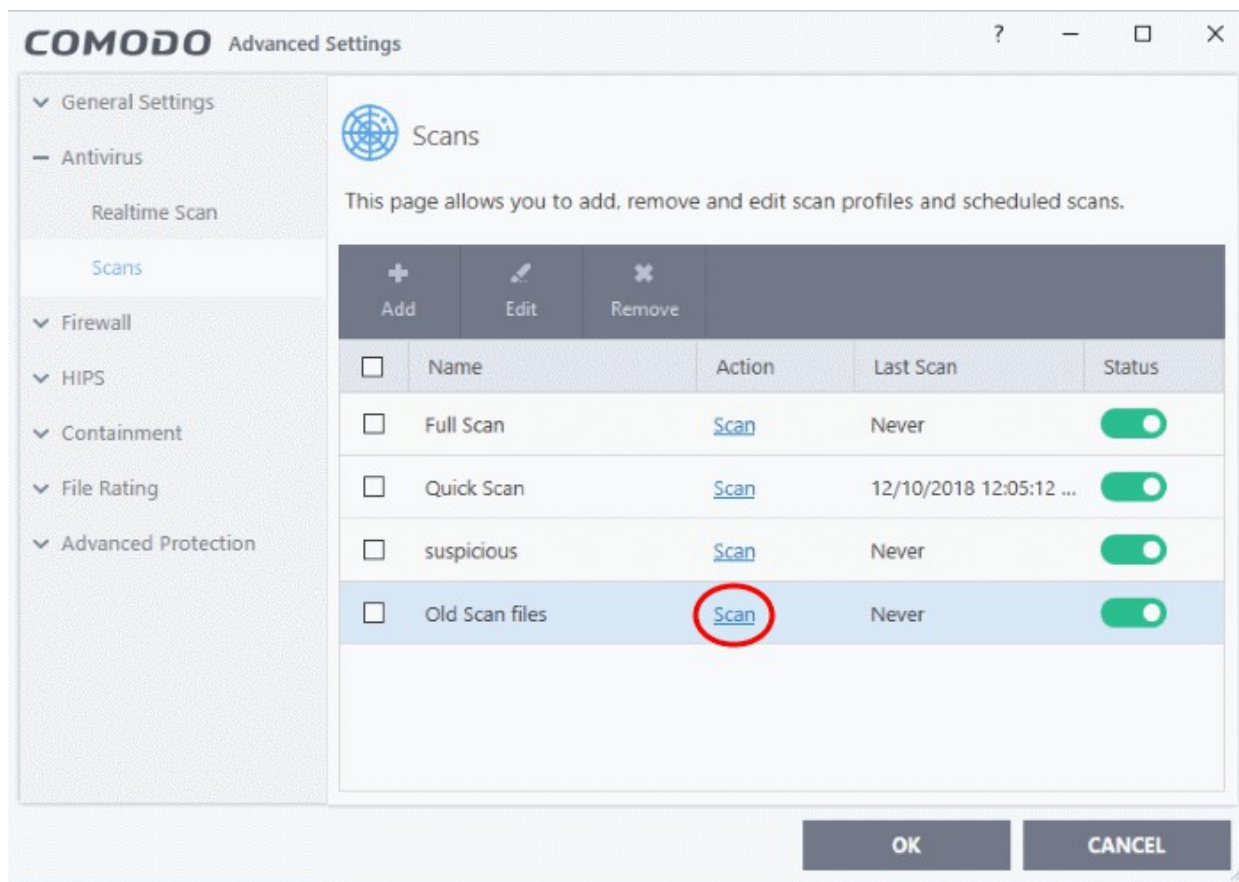
To run a custom scan

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

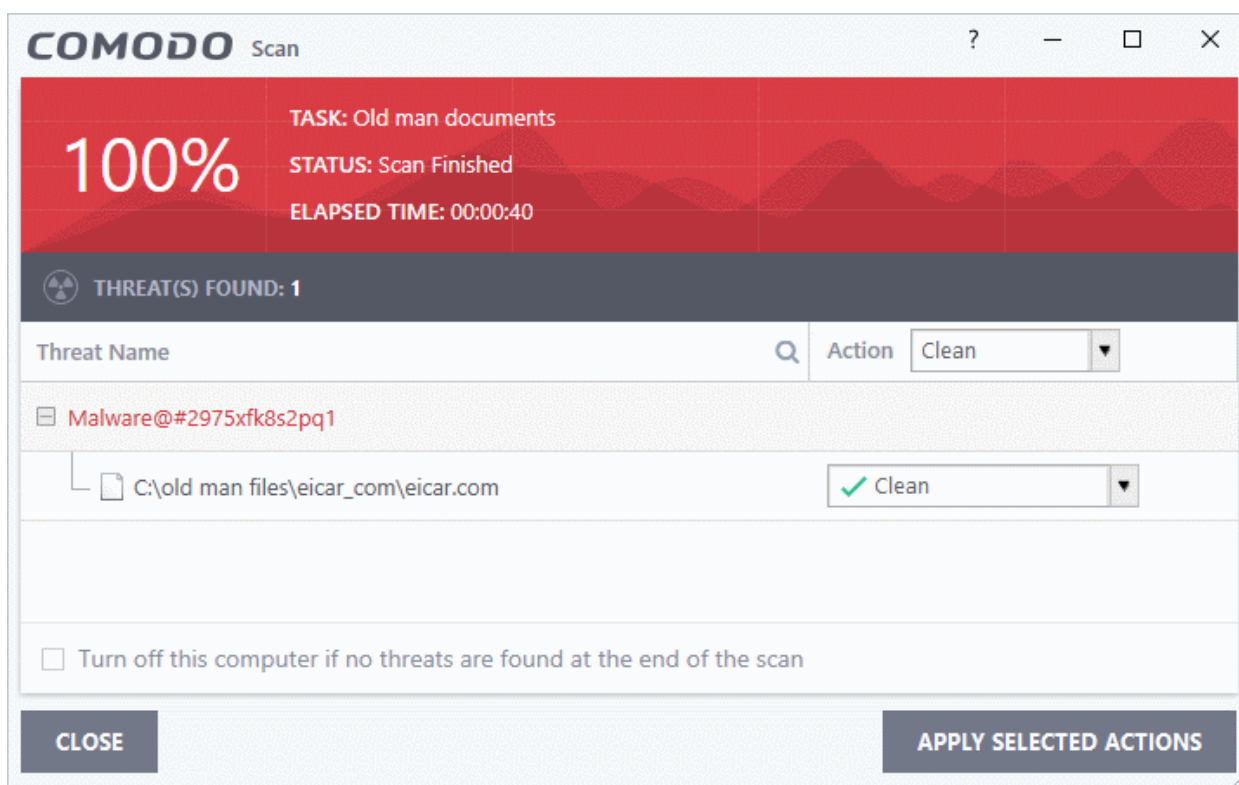
- Click 'More Scan Options' from the 'Custom Scan' pane

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

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



The Antivirus will start scanning the locations defined in the profile. On completion of scanning, if any threats are found, an alert screen will be displayed.



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

2.1.5. Automatically Scan Unrecognized Files

- CCS rates a file as either 'trusted', 'malicious' or 'unknown' when the file is first run
- The rating is obtained by checking the file's reputation on our master whitelist and blacklist
- If no file rating is available then CCS checks the trust rating of the software vendor
 - CCS will apply the vendor reputation to the file if a rating exists. CCS first checks the vendor's local reputation in the 'Vendor List'. If no local rating is available then it checks the FLS.
- There are two ways a file can get an 'unrecognized' rating:
 1. Because there is no rating available for the file in Comodo's blacklist or whitelist, and no user has assigned a rating to the file.

OR

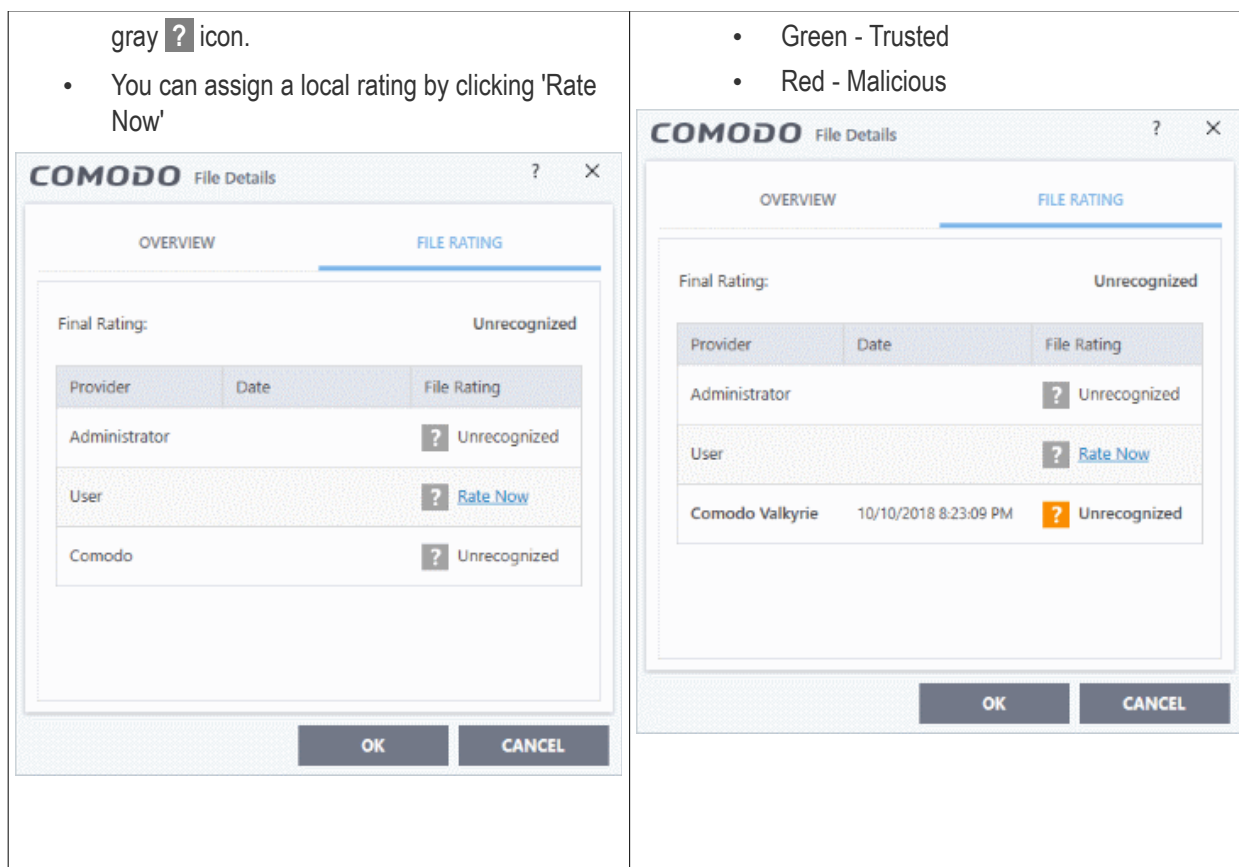
2. Because an admin, user or Comodo specifically assigned an 'unrecognized' rating to the file.

To view the rating:

- Go to 'File Rating' > 'File List' > select an unrecognized file and click 'File Details'
- Click the 'File Rating' tab in the 'File Details' dialog.

See the following examples of files with rating and no rating:

<ul style="list-style-type: none"> • The interface lists 3 ratings, one each from the user (you), the admin and Comodo. • Unknown files with no rating are shown with a 	<ul style="list-style-type: none"> • A colored icon in the file rating column indicates it has been rated. <ul style="list-style-type: none"> • Yellow - Unrecognized
---	--



CCS will handle unrecognized files differently depending on whether the rating was proactively applied or not:

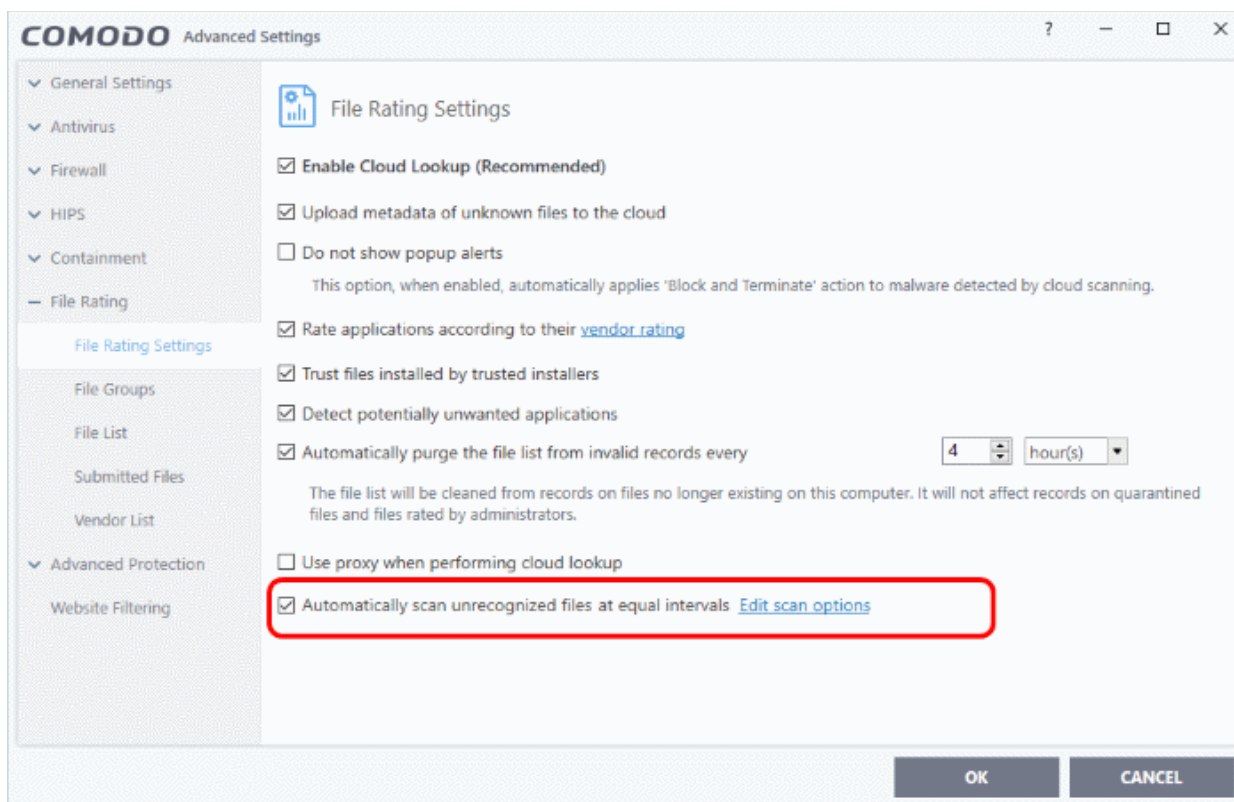
- Files proactively awarded an unrecognized rating (by admin, user or Comodo) are **not** uploaded to Valkyrie.
- All other unrecognized files are uploaded to Valkyrie when executed, or if they are discovered by a **rating scan**. You can also submit them manually.

Regardless of the above, all unrecognized files are run in the container by default. If required, you can change auto-containment rules in 'Settings' > 'Containment' > 'Auto-Containment'. See '**Auto-Containment Rules**' for more information.

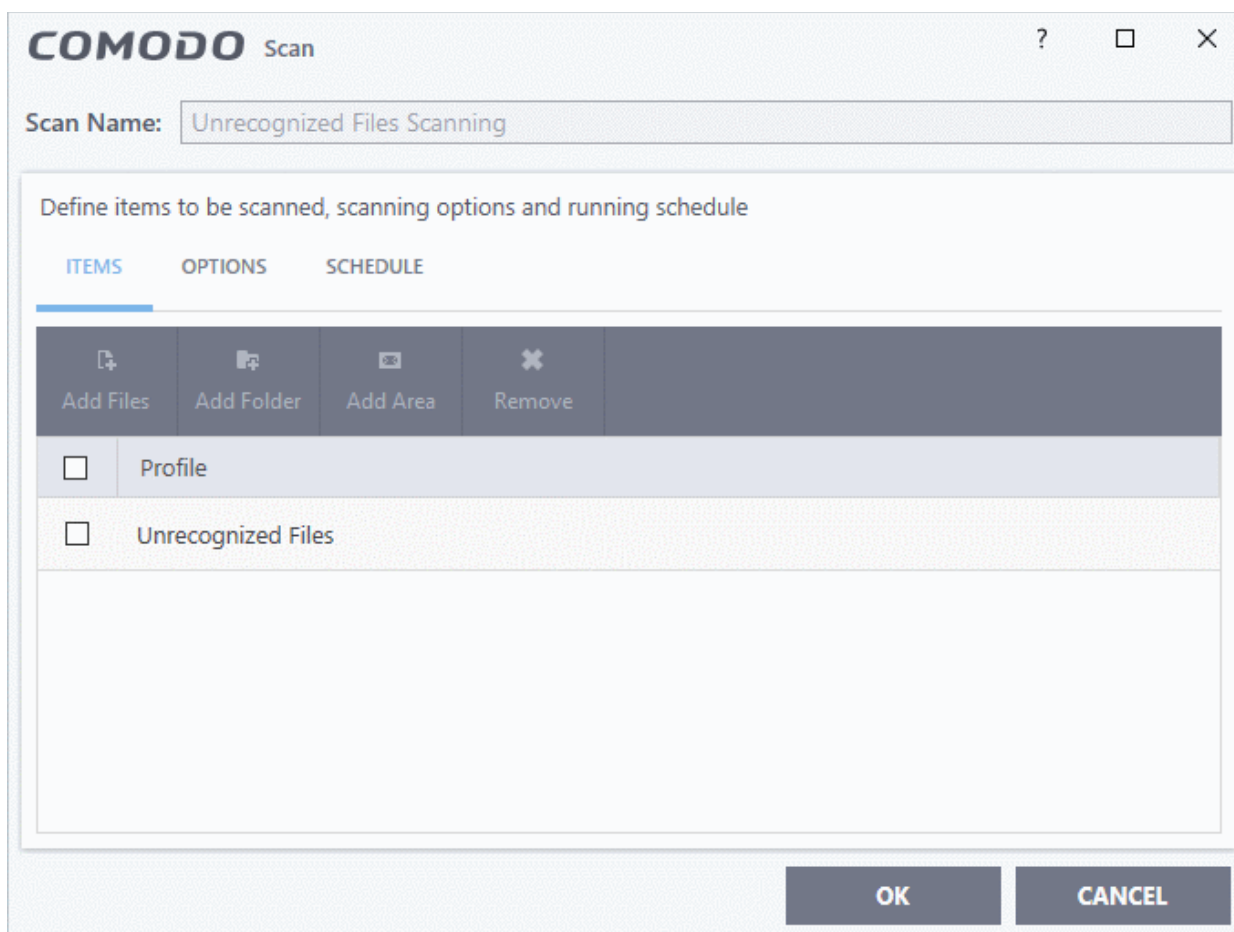
Configure scan settings for unrecognized files

CCS will periodically scan all unrecognized files to see if a new rating is available for them.

- Click 'Settings' on the home screen
- Click 'File Rating' > 'File Rating Settings'



- 'Automatically scan unrecognized files at equal intervals' is enabled by default and set for every 4 hours.
- Click 'Edit scan options' to open the predefined 'Unrecognized File Scanning' profile



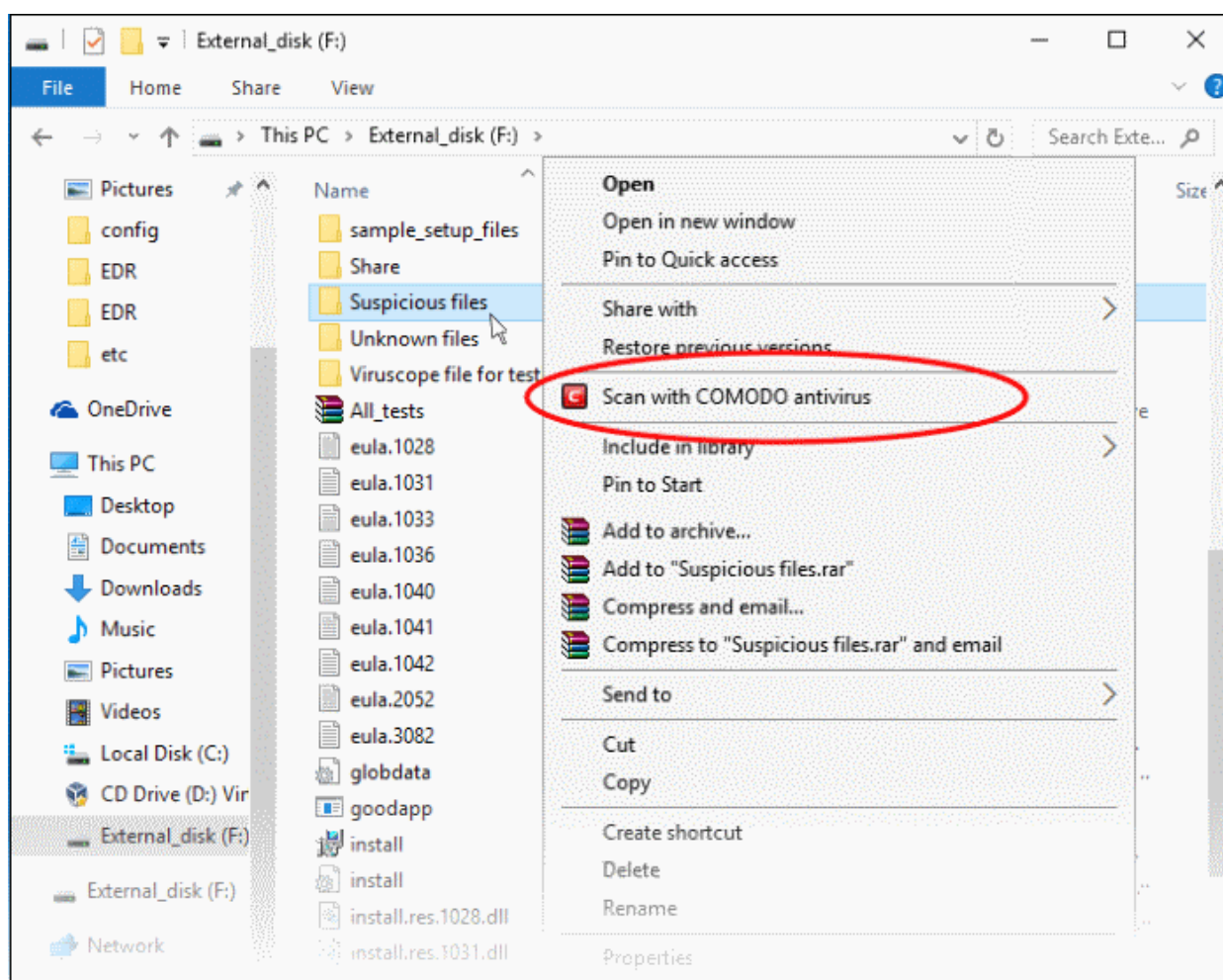
- Scan Name - The scan name cannot be edited.
- Items - The profile is pre-configured for unrecognized files and cannot be edited. Note - You cannot add files, folders or area in this profile.
- Scan Options - Same as explained for a custom scan. [Click here](#) to view.
- Schedule - This is set to scan every 4 hours by default. This is same as explained for a custom scan. [Click here](#) to view.
- Click 'OK' and again in the 'Advanced Settings' screen for your changes to take effect.

2.2. Instantly Scan Files and Folders

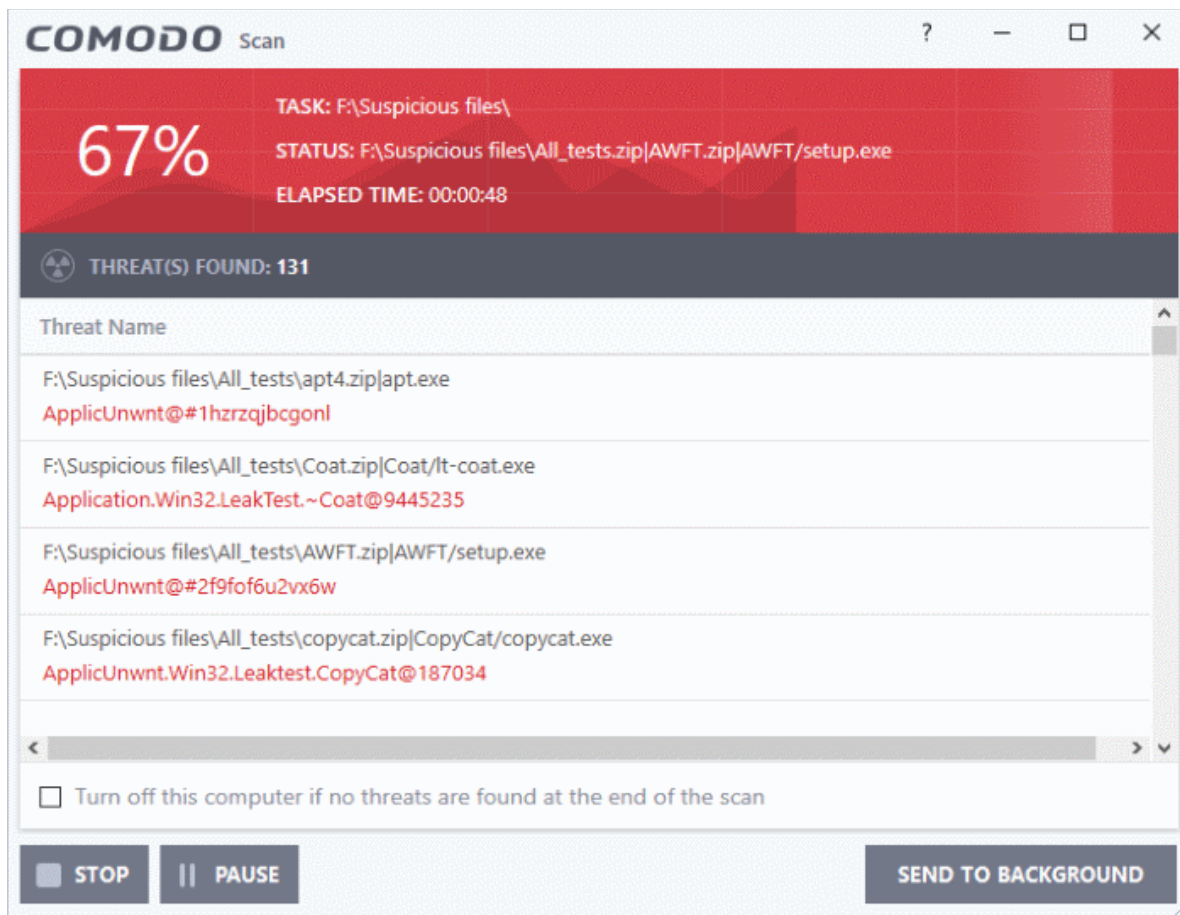
You can scan individual files or folders instantly to check whether they contain any threats or infections.

To instantly scan an item

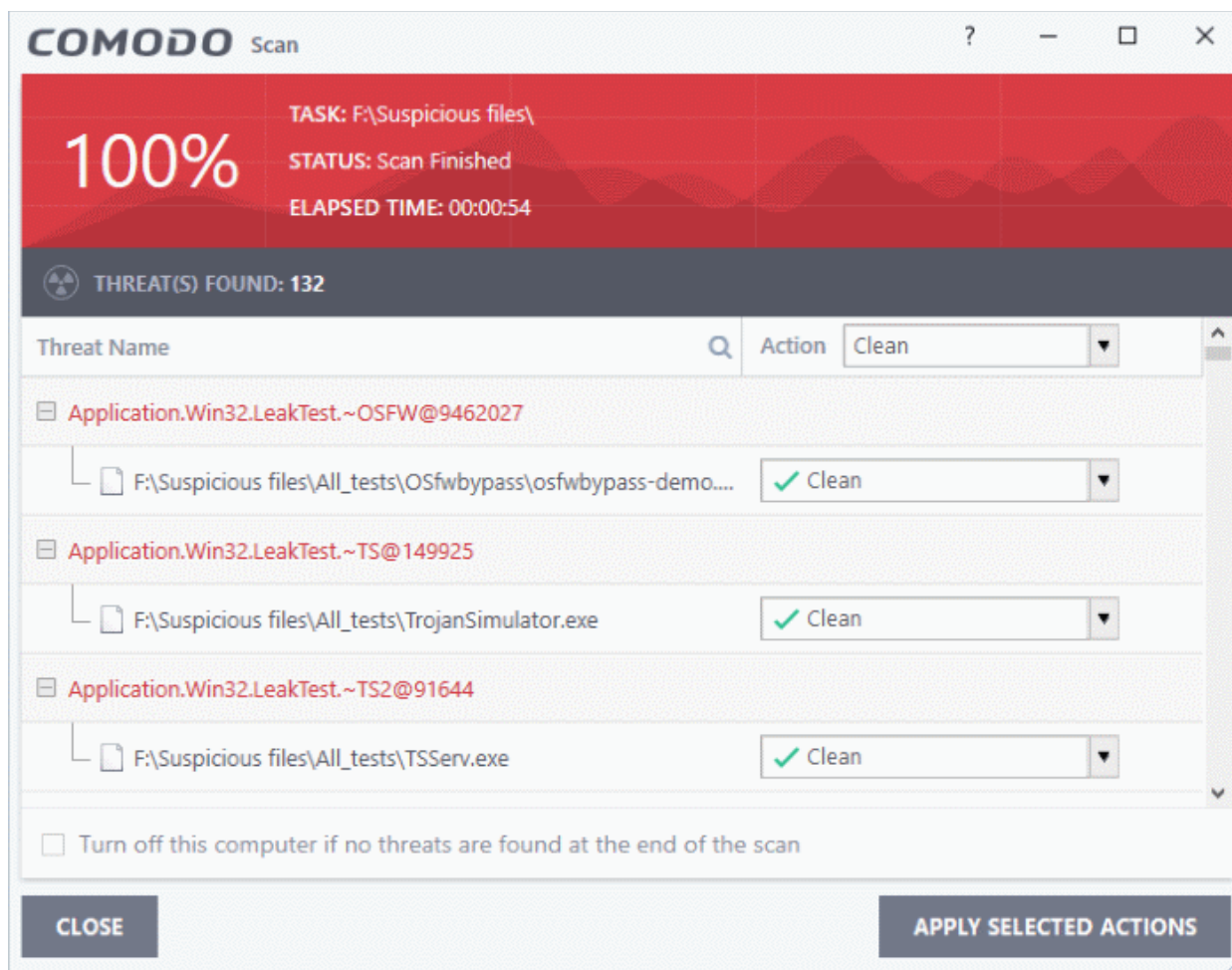
- Right click on the item and select 'Scan with Comodo Antivirus' from the context sensitive menu



The item will be scanned immediately.



- Any threats found will be shown at the end of the scan:

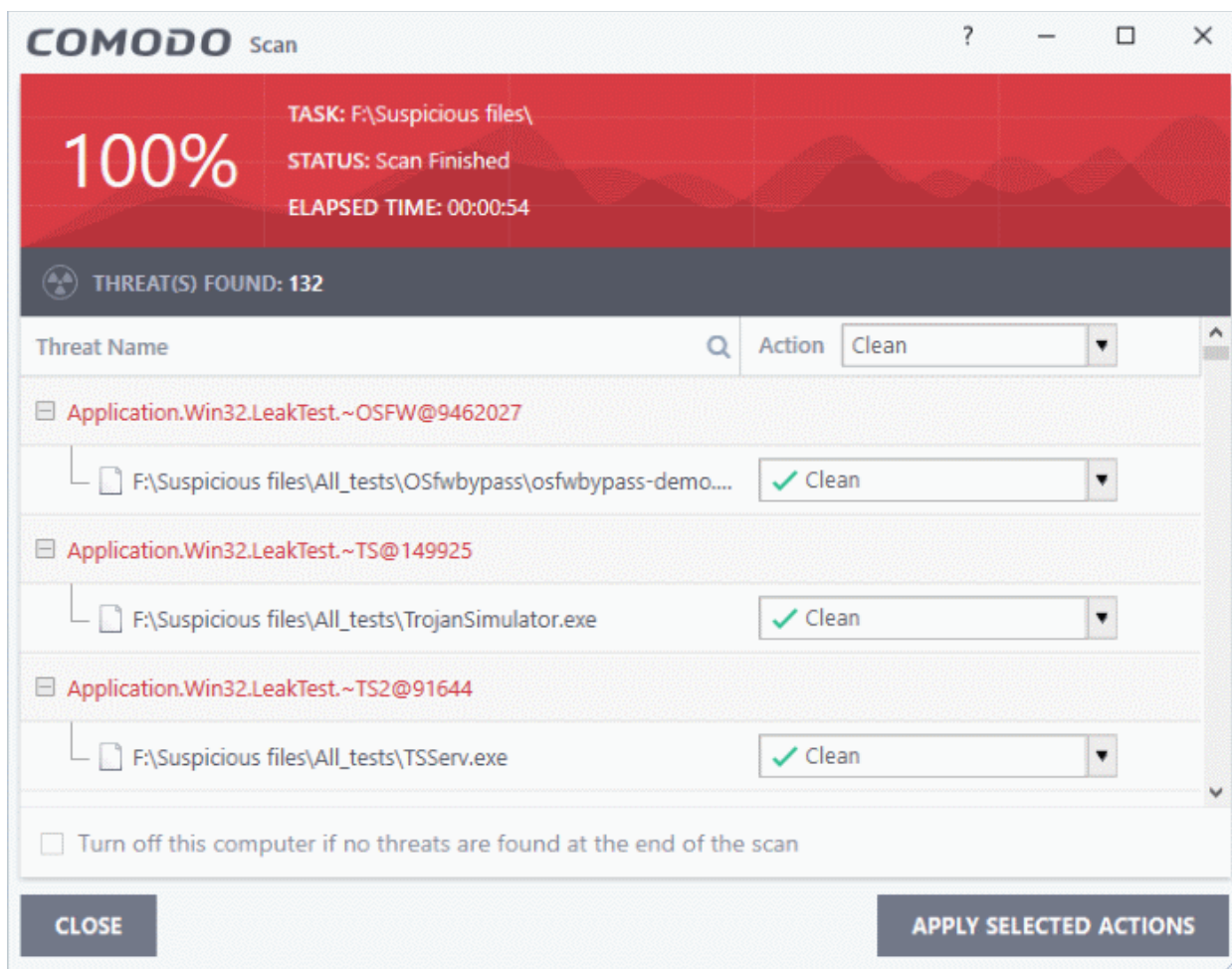


You can choose to clean, quarantine or ignore the threat. See '[Processing Infected Files](#)' for more details.

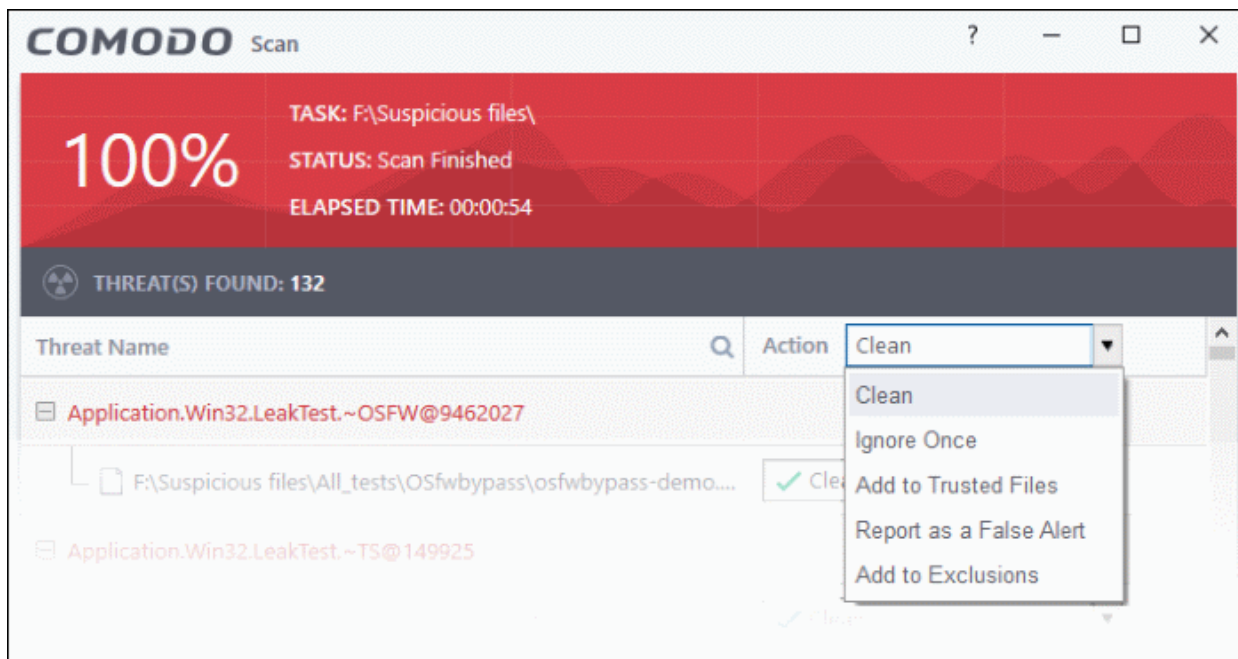
2.3. Process Infected Files

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

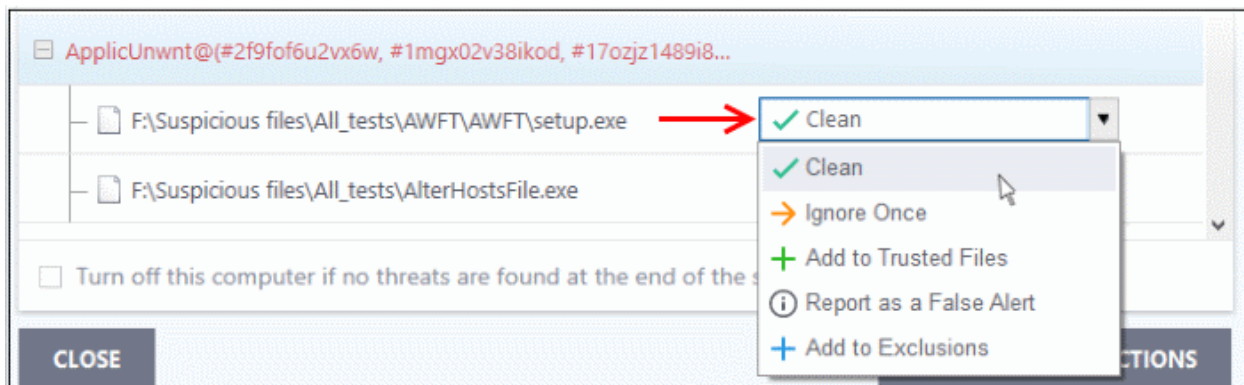
1. For profile driven scans, malware will be automatically dealt with if 'Automatically Clean Threats' is enabled in the scan profile applied to the device. See [configuring scanning options](#) for more details.
2. For all other on-demand or scheduled scans, an alert screen will be displayed. The alert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



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

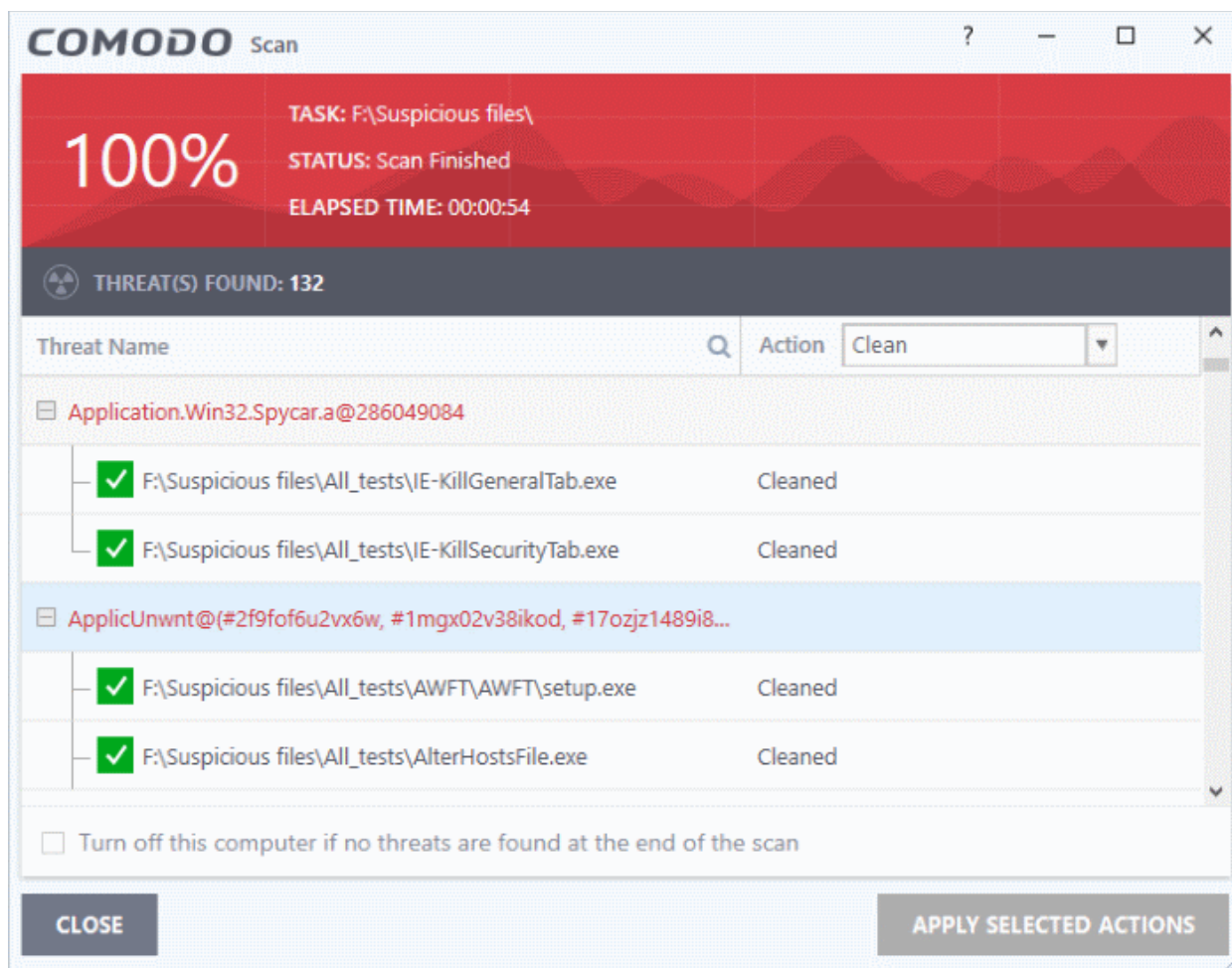


... or the actions to be applied to individual items from the drop-down beside each item.



Available actions are:

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



- Click 'Close' to close the results window.

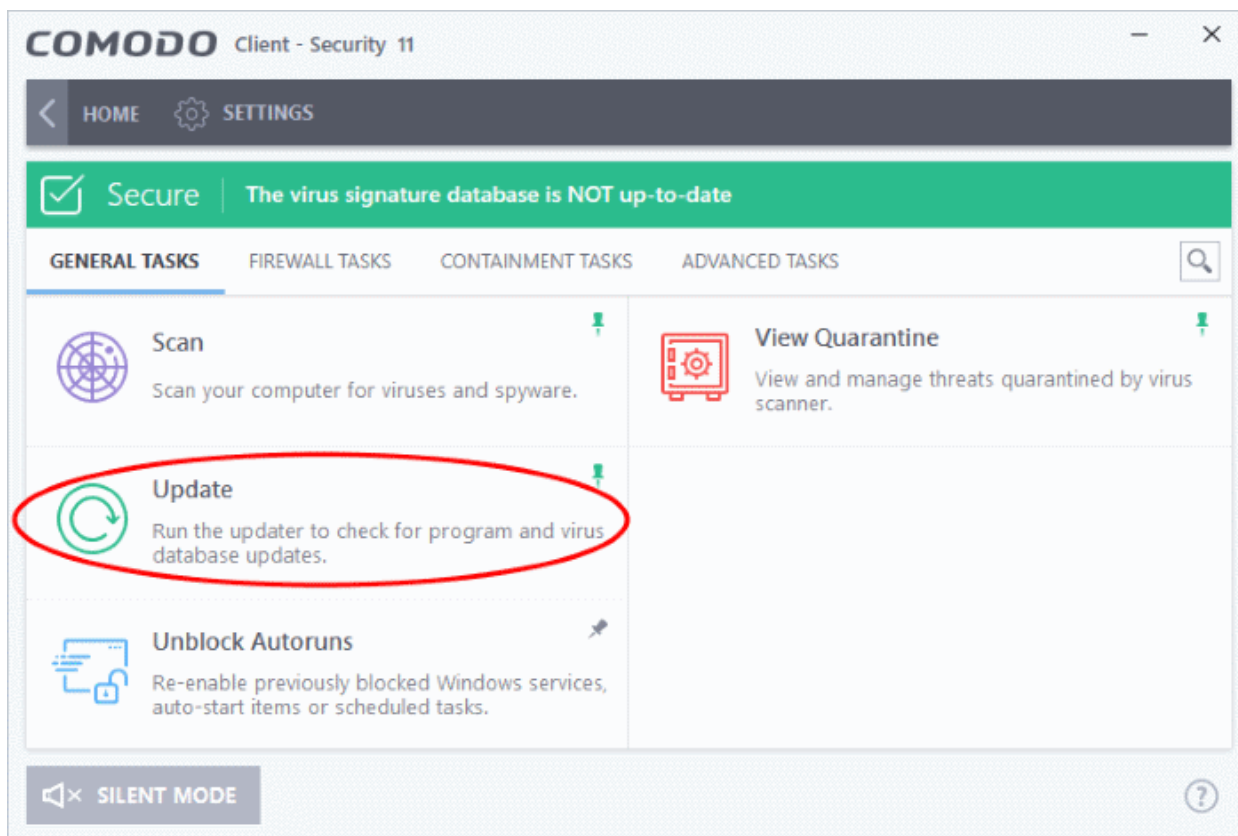
2.4. Manage Virus Database Updates

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

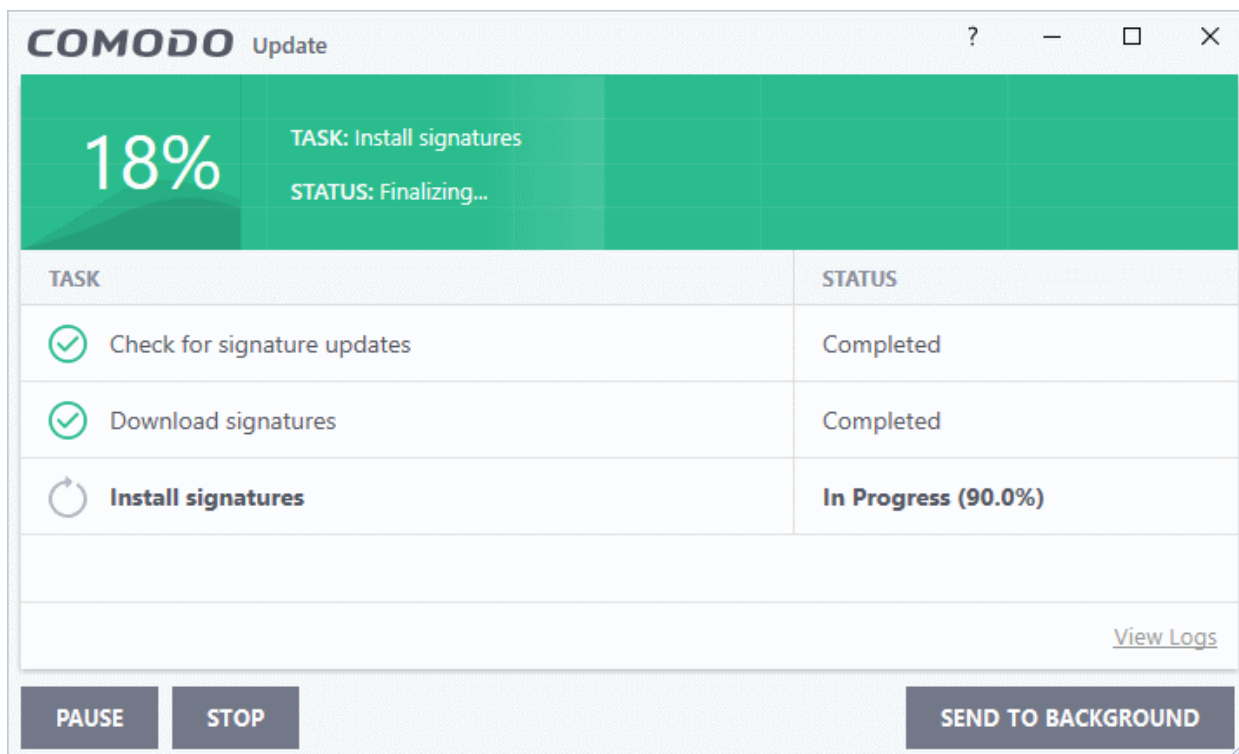
Note: You must be connected to the internet to download updates.

Manually check for updates

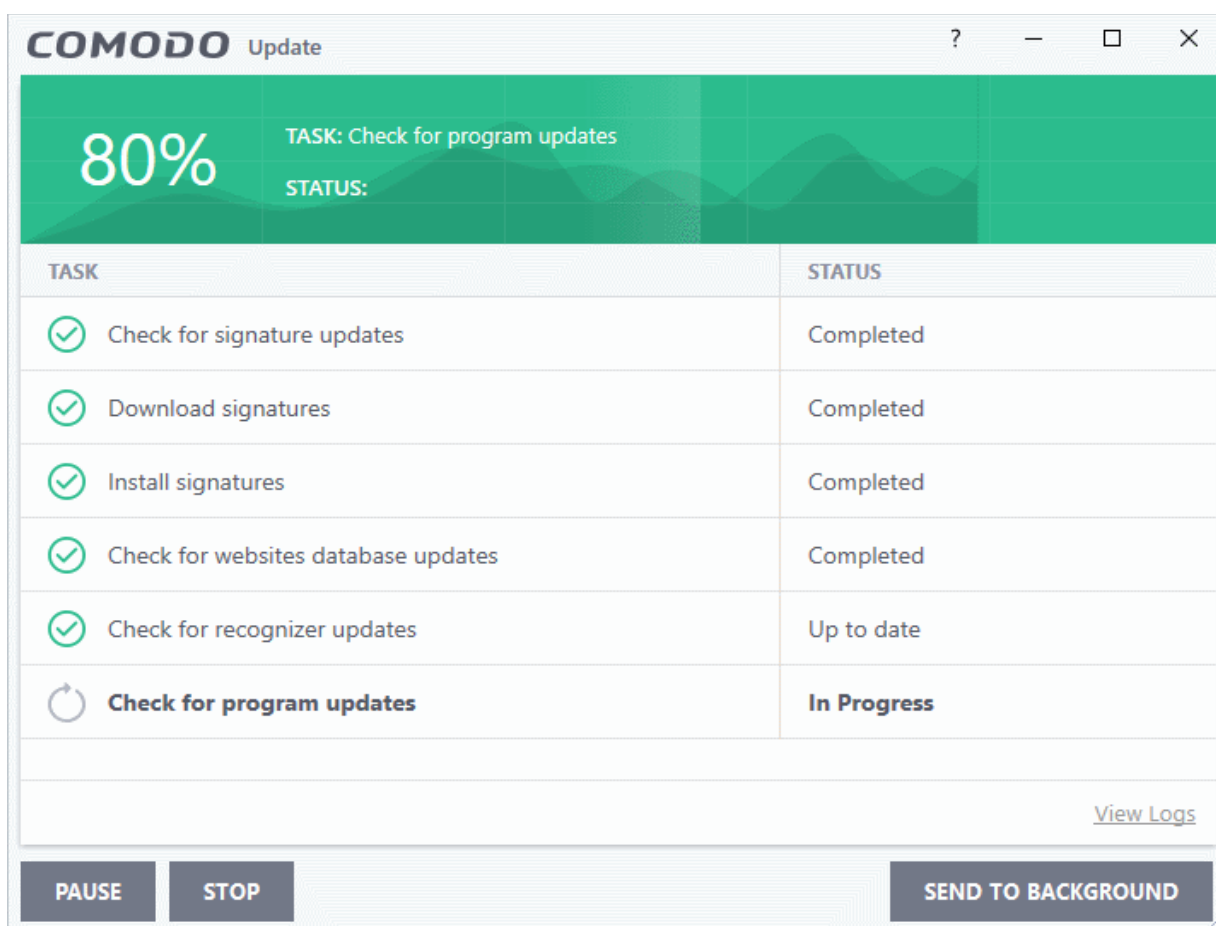
1. Switch to the 'Tasks' screen and click 'General Tasks'
2. Click 'Update'. The application will check for database updates.



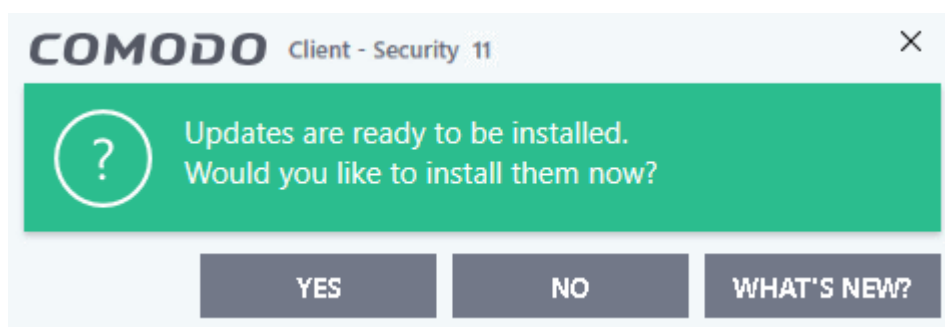
Signature updates are downloaded and installed first:



The updater will then check for VirusScope (recognizer) updates:

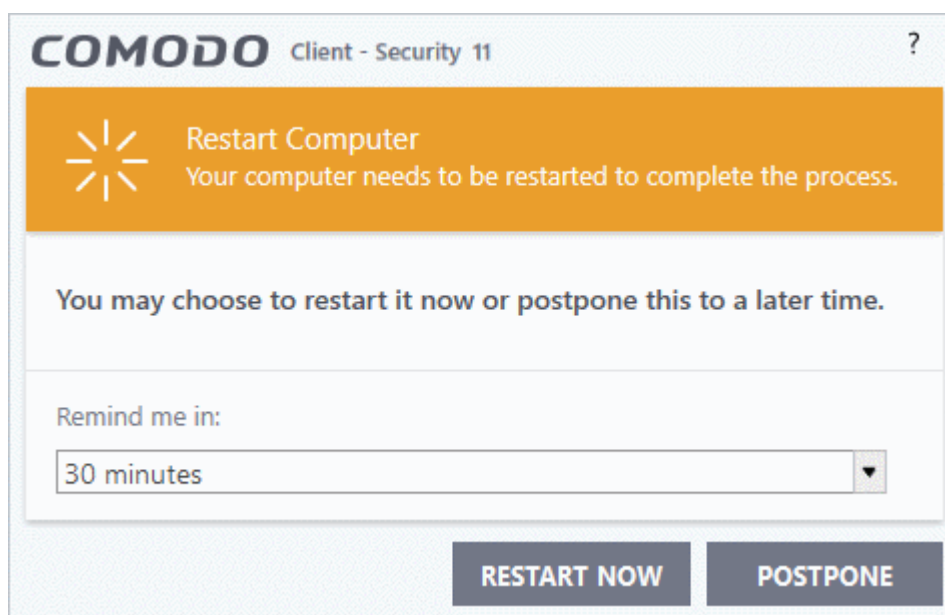


If any updates are available, you will be asked to confirm installation at the following dialog:

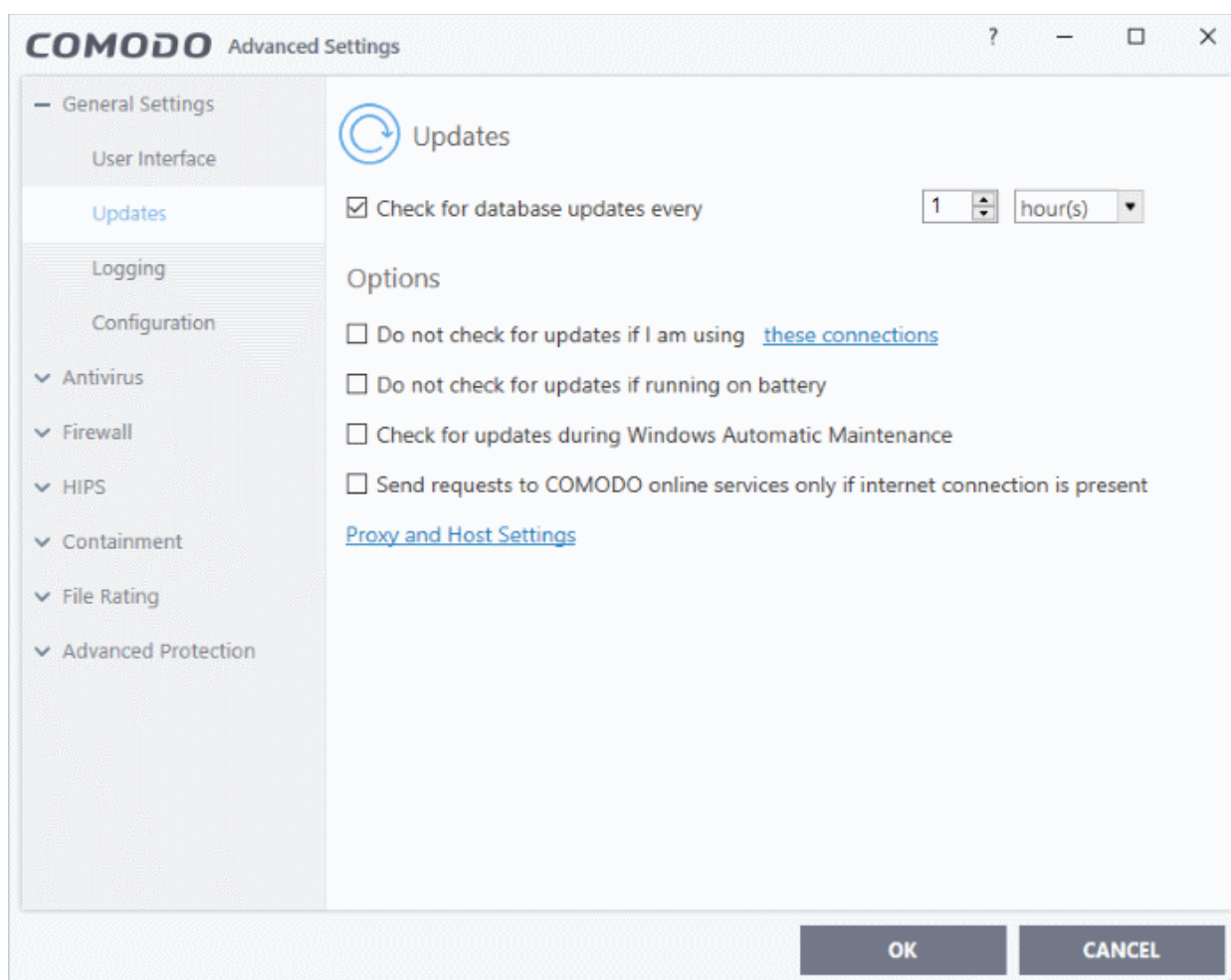


- Click 'Yes' to begin installation:

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



Automatic Updates



By default, the application automatically checks for and downloads database 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

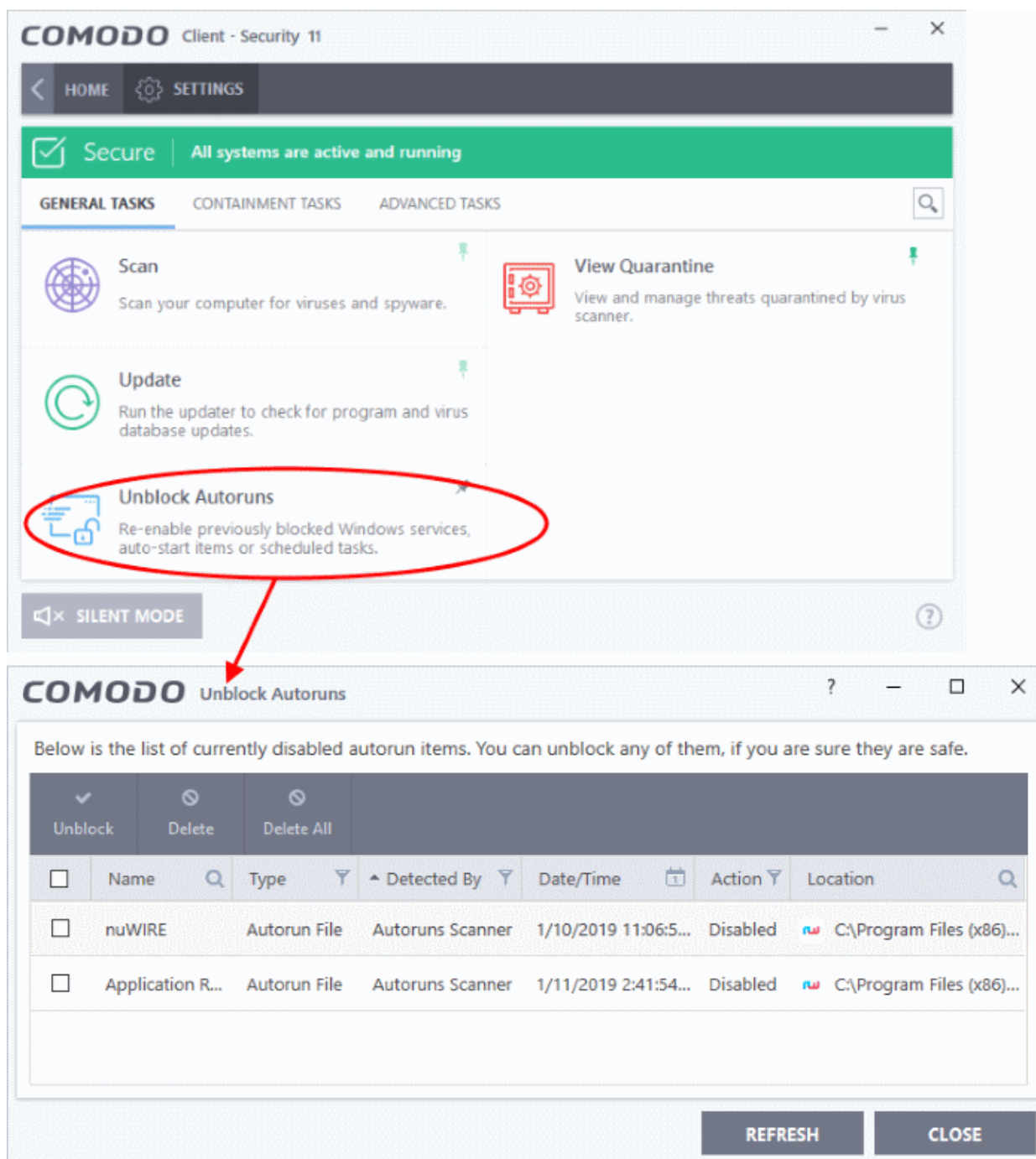
'**Scan Profiles**' for more details.

2.5. Manage Blocked Autoruns

- The 'Unblock Autorun' area shows applications that were blocked by the boot protection feature of CCS.
- The feature monitors attempted changes to the registry records of Windows services, auto-start entries and scheduled tasks. The feature can be managed in the following locations:
 - **Realtime Scans** - Click 'Advanced Settings' > 'Scans' > 'Scan Options' > 'Apply this action to suspicious auto-run processes'
 - **On-Demand Scans** - Click 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous' > 'Apply the selected action to unrecognized autorun entries to new/modified registry items'
- CCS will terminate and quarantine apps that attempt to modify protected registry items
- If you feel that a particular application is safe, you can unblock it.

View and manage blocked autorun items

- Click 'Tasks' at the top-left of the home screen
- Open the 'General Tasks' tab and choose 'Unblock Autoruns'
- The interface shows all auto-run items blocked by CCS:



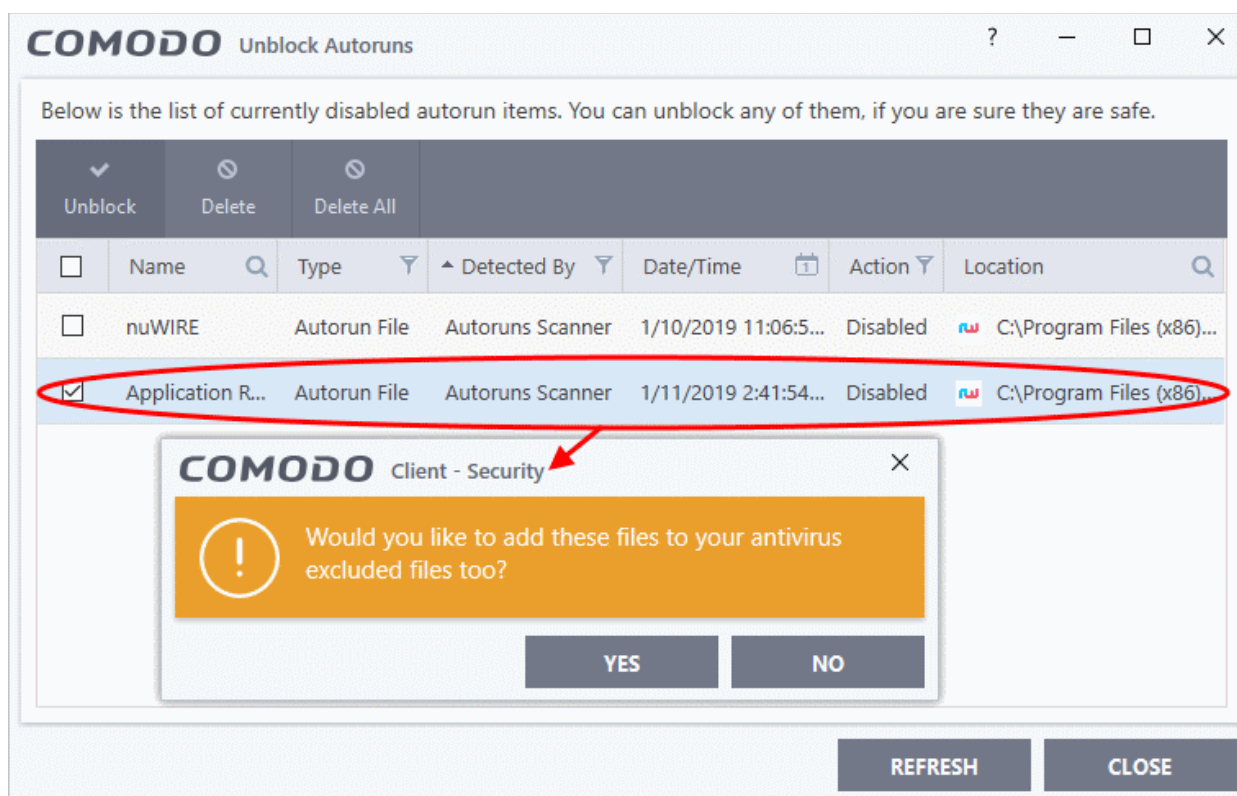
Unlock Autoruns - Column Descriptions

Column Header	Description
Name	The label of the blocked application
Type	The category of auto-run. For example, 'Scheduled Task' or 'Windows Service'.
Detected By	The security module which identified the threat
Date/Time	The time and date the file was detected
Action	The response to the threat. The possible actions are: <ul style="list-style-type: none"> Ignore

	<ul style="list-style-type: none"> • Terminate • Terminate and Disable • Quarantine and Disable • To set this action: • Click 'Advanced Settings' > 'Scans' > 'Scan Options' > 'Apply this action to suspicious auto-run processes'
Location	Path of the autorun process

Restore Autorun entries from the 'Unblock Autoruns' screen:

- Click 'General Tasks' > 'Unblock Autoruns'
- Select the items you want to release
- Click the 'Unblock' button:



- Click 'Yes' if you do not want this file to be blocked in future.

Restore Autoruns from the 'Quarantine' screen:

- Click 'Advanced Tasks' > 'View Quarantine'
- Select the items you want to release
- Click the 'Restore' button:

Delete Autoruns entries:

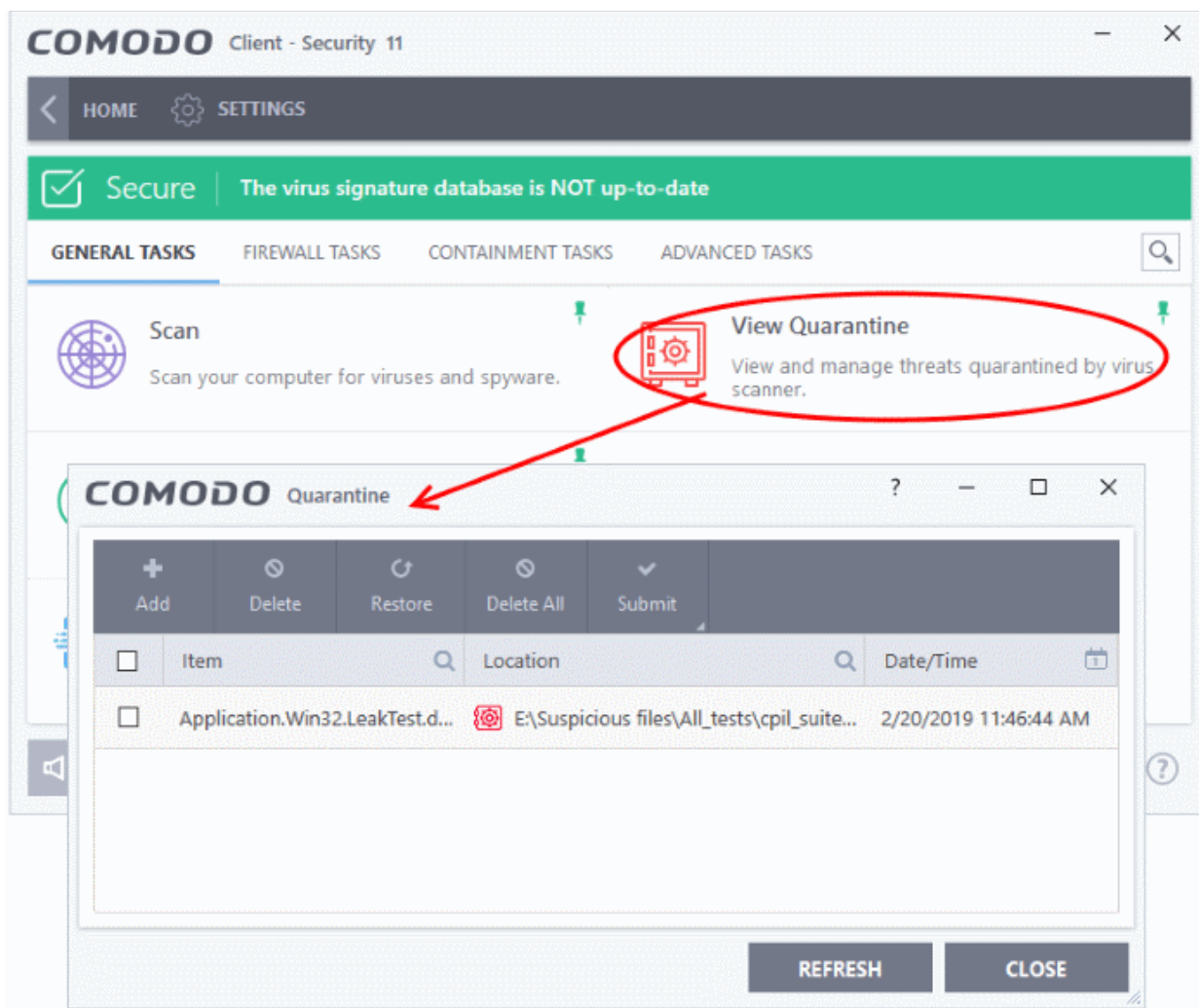
- Click 'General Tasks' > 'Unblock Autoruns'
- Select the items you want to remove
- Click the 'Delete' button

2.6. Manage Quarantined Items

- The quarantine area shows all malicious files which have been isolated by CCS to prevent them from infecting your system.
- CCS encrypts all files it place in quarantine so they cannot be run or executed.

To access the quarantine area

- Open the 'General Tasks' interface and click 'View Quarantine'
- This will display a list of items quarantined by the virus scanner or quarantined manually:



Column Descriptions

- **Item** - Application or process propagated the event
- **Location** - Location where the application or the file is stored
- **Date/Time** - Date and time when the item is moved to quarantine
- To search for a specific quarantine item, executables location, click the lens icon at top right of the 'Item' or 'Location' column headers, enter the item name in full or part, or enter the path correspondingly
- To filter the list based on the date of file installation, click the calendar icon at top right of the 'Date/Time' column header and choose the time/date/period

From here you can:

- **Manually add applications, executables or other files to Quarantine**

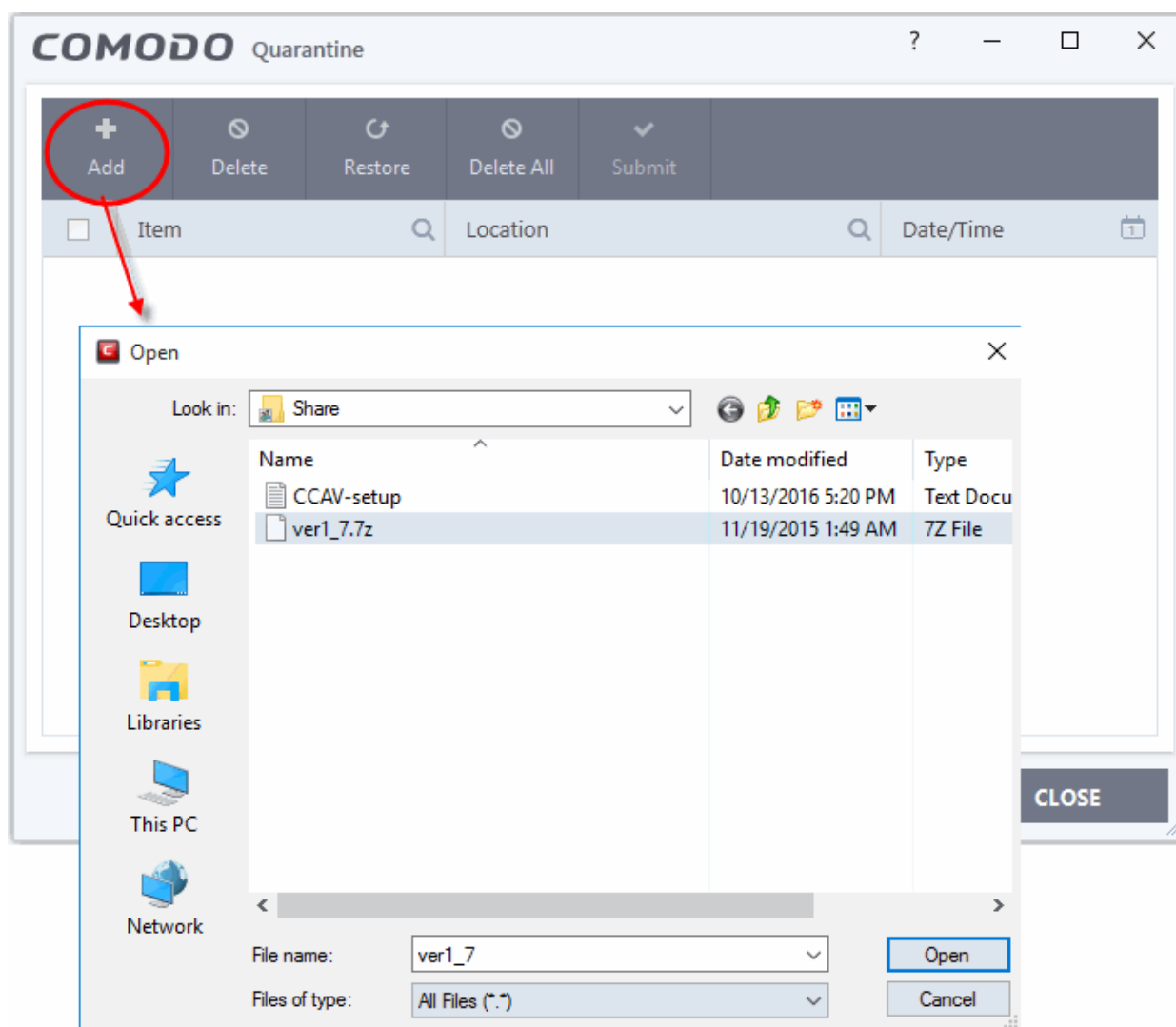
- **Delete a selected quarantined item from the system**
- **Restore a quarantined item to its original location**
- **Delete all quarantined items**
- **Submit selected quarantined items to Valkyrie for analysis**

Manually adding files as Quarantined Items

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

To manually add a Quarantined item

1. Click 'Add' button at the top of the screen
2. Navigate to the file you want to add to the quarantine and click 'Open'



- The file will be added to 'Quarantine'. To send the file for analysis to Comodo, for inclusion in the white list or black list, click 'Submit' button.

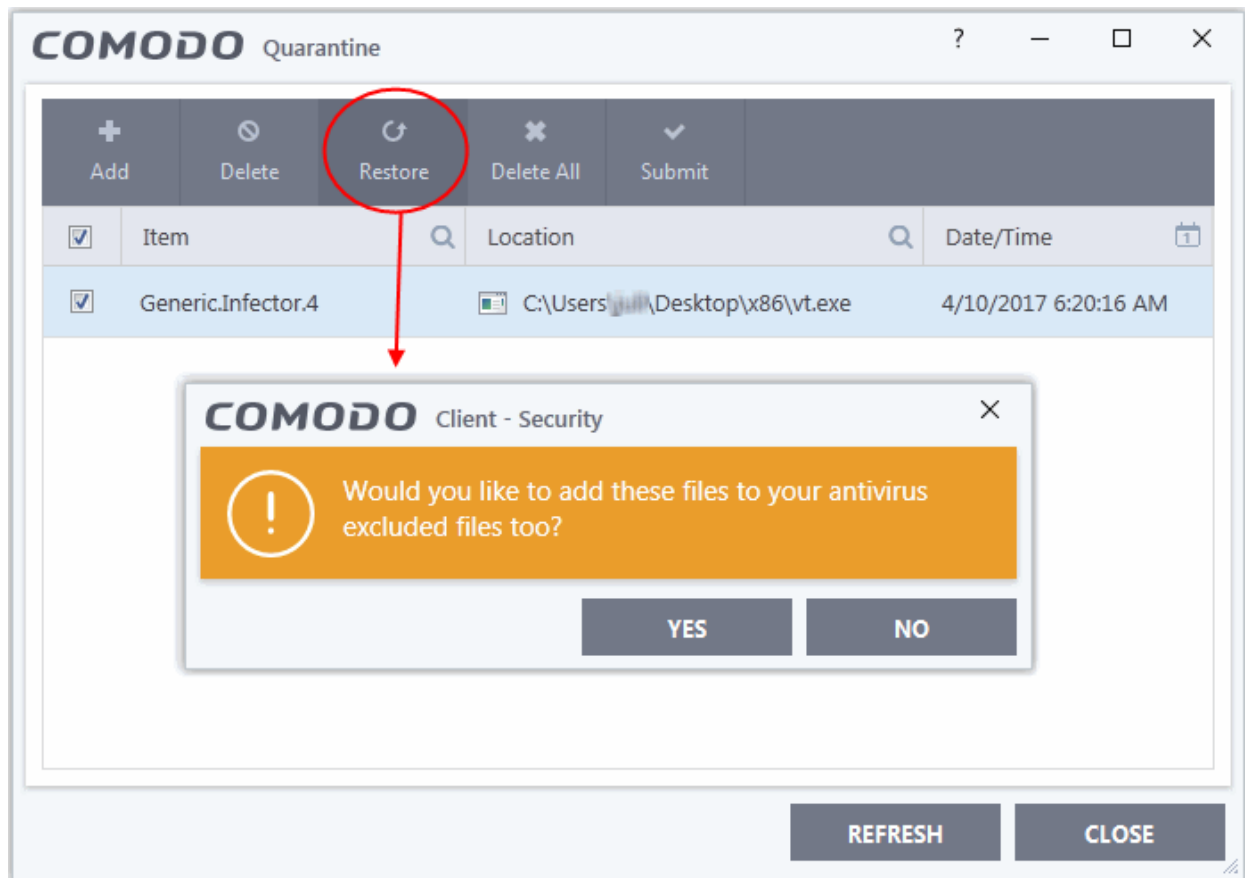
To delete a quarantined item from the system

- Select the item(s) from the 'Quarantine' interface
- Click 'Delete' button at the top

This deletes the file(s) from the system permanently.

To restore a quarantined item to its original location

- Select the item(s) from the 'Quarantine' interface and click the 'Restore' button at the top



An option will be provided to add the file(s) to **Exclusions** list.

- If 'Yes' is opted, these files will not be scanned again. The file will be restored to its original location.
- If the restored item does not contain malware it will operate as usual.
- If it contains malware it will be flagged as a threat immediately if real-time scanning is enabled (or during the next scan if real time scanning is disabled). The file will not be flagged if it is on the 'Exclusions' list.

Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

To remove all the quarantined items permanently

- Click the 'Delete All' option at the top.

All the quarantined items will be deleted from your system permanently.

Submit selected quarantined items to Valkyrie for analysis

Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.

- Open the 'General Tasks' interface and click 'View Quarantine'
- Use the check-boxes to select the items you want to submit. You can send several files at once.
- Click 'Submit' > 'Submit to Valkyrie' in the top-menu. The files will be immediately sent to Valkyrie for analysis.

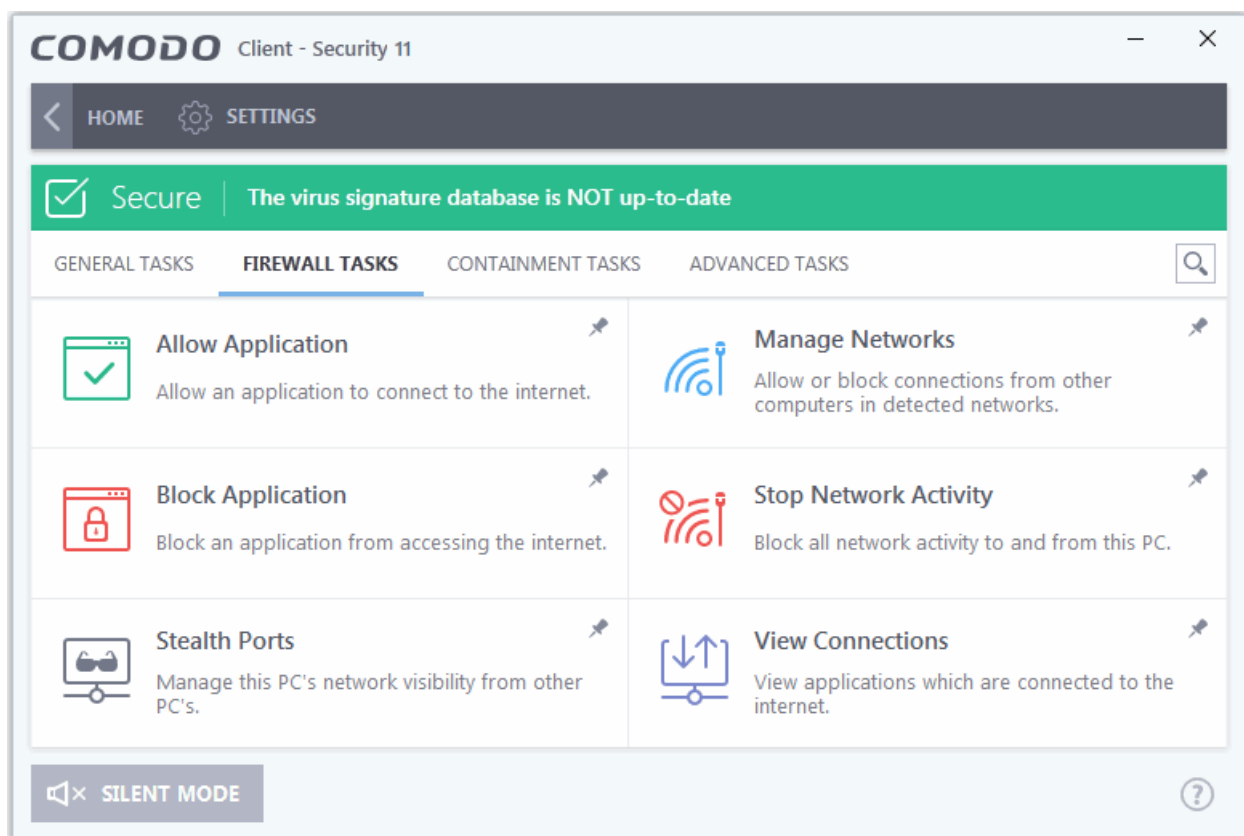
Tip: Alternatively, right click an item then choose 'Submit to Valkyrie' from the menu.

- All submitted files are analyzed at Valkyrie. If they are found to be trustworthy, they will be added to the

Comodo safe list (white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (blacklisted).

3. Firewall Tasks - Introduction

- The 'Firewall' component of Comodo Client Security offers the highest levels of security against inbound and outbound threats, hides your computer's ports from hackers and blocks malicious software from transmitting your confidential data over the internet.
- The firewall makes it easy for you to specify exactly which applications are allowed to connect to the internet and immediately warns you when there is suspicious activity.
- There are two places where you can configure the firewall:
 - Click 'Firewall Tasks' on the home-screen. From here you can configure internet access rights per-application, stealth your computer ports, block or allow networks and monitor all connections to and from your computer. This area is covered in this section of the guide.
 - Click 'Settings' on the home-screen then 'Firewall'. From here you can configure advanced settings, create firewall rules/rulesets, configure network zones and create port sets. See '[Firewall Configuration](#)' for more details about advanced firewall settings.



The following sections explain more about each area:

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

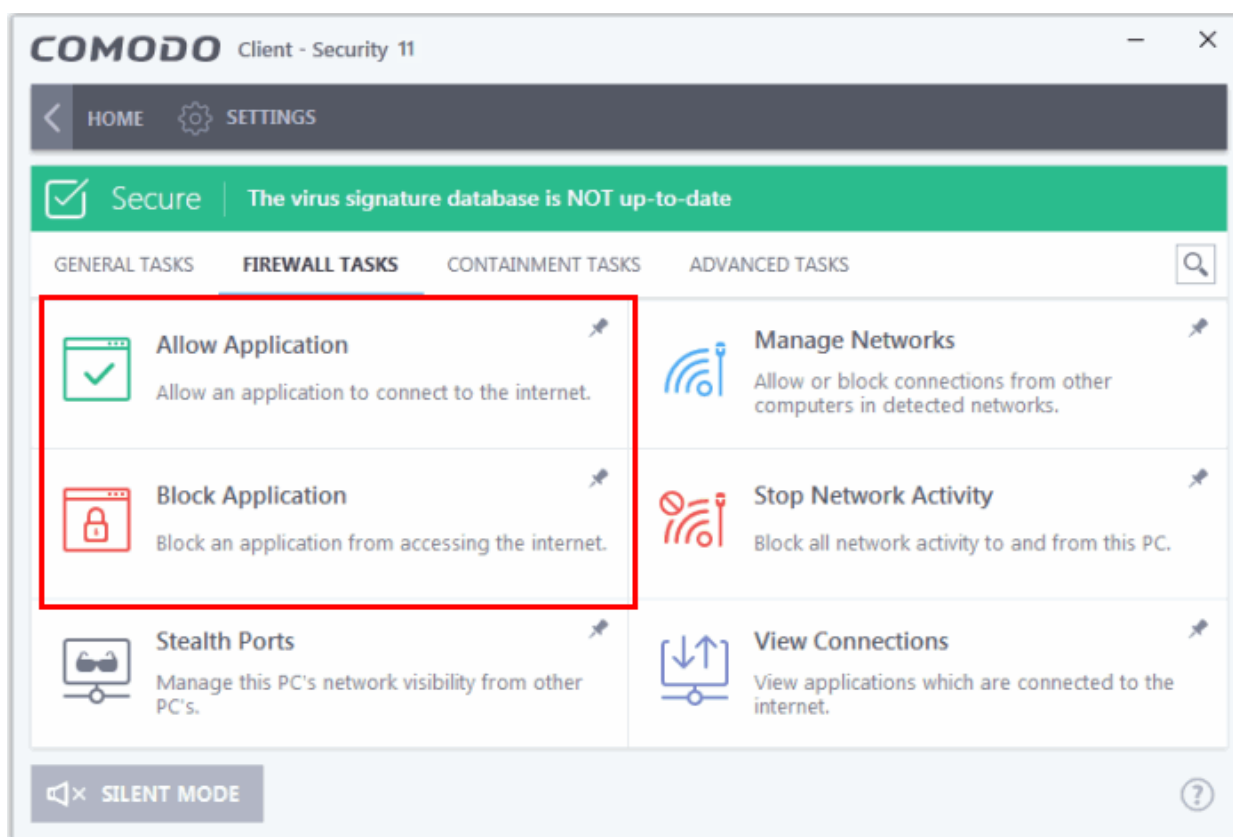
- **View active Internet connections**

3.1. Allow or Block Internet Access to Applications Selectively

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

To open the Firewall interface

- Click 'Tasks' at the top left of the CCS home screen
- Click 'Firewall Tasks' from the 'Tasks' interface:



To allow an application to access to the internet

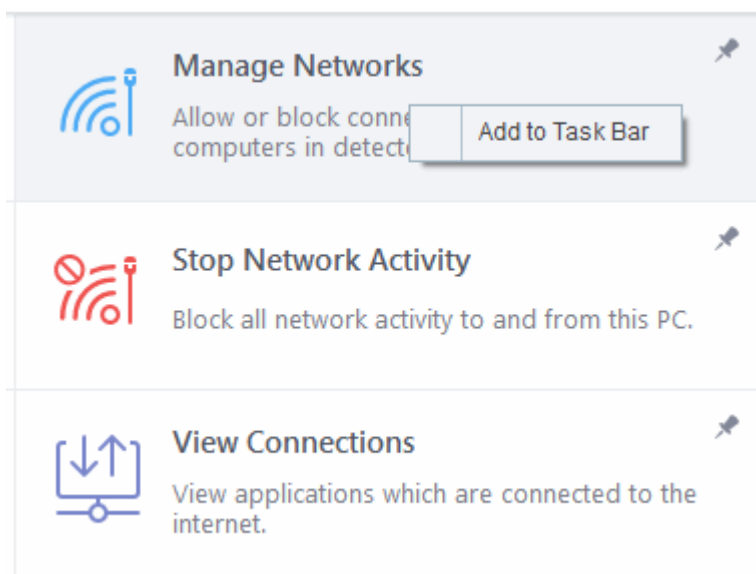
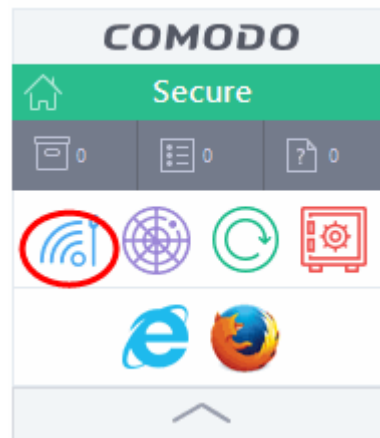
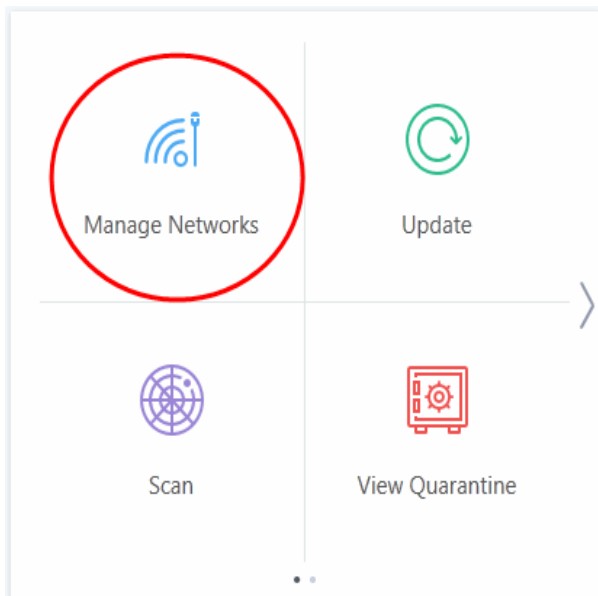
- Click 'Allow Application'
- Navigate to the main executable of the application in the 'Open' dialog
- Click 'Open'. A rule will be created to allow Internet access to the selected application

To block an application's Internet access rights

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

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

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



3.2. Stealth your Computer Ports

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

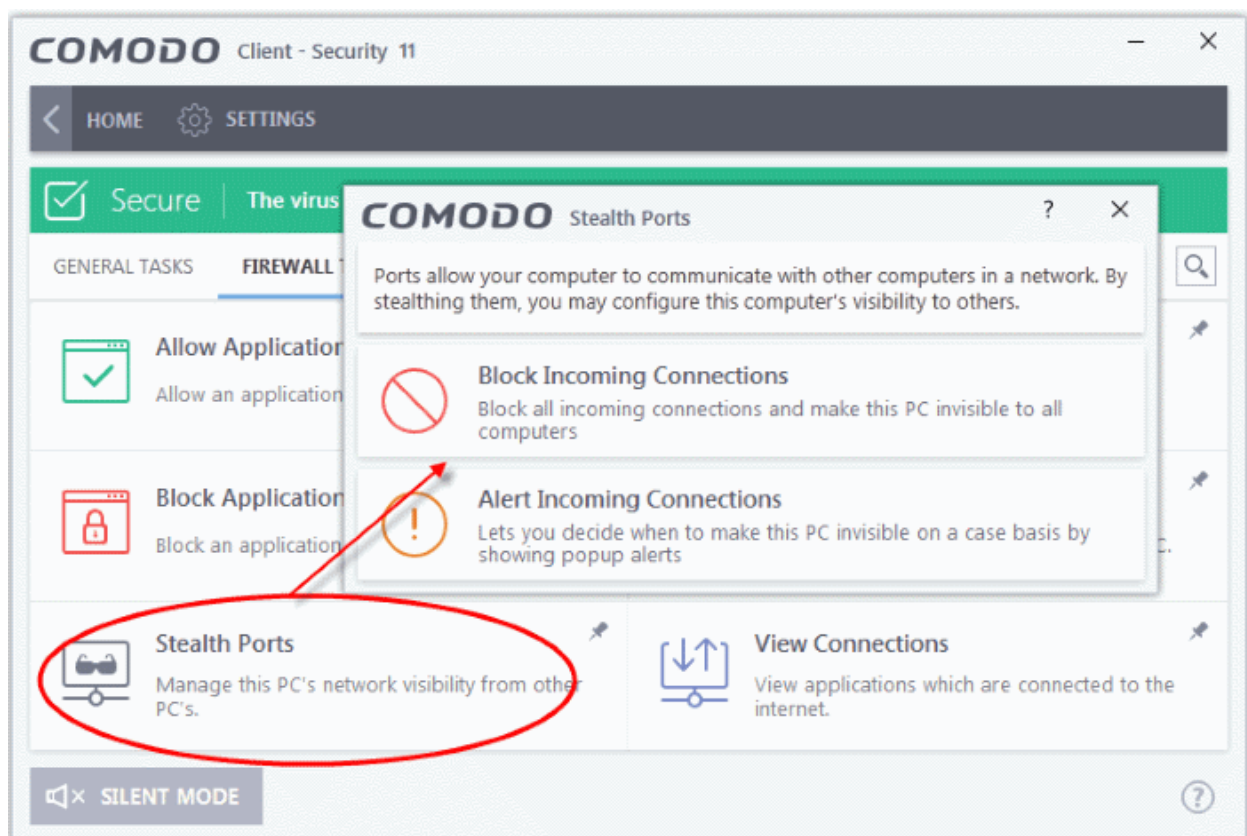
General Note:

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

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

To stealth ports on your computer:

- Click 'Tasks' at the top left of the CCS home screen
- Click 'Firewall Tasks' from the 'Tasks' interface then click 'Stealth Ports'



You have two options to choose from:

Block incoming connections

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

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

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


If you would like more information on the meaning and construction of rules, please [click here](#).


Alert incoming connections


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


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

Block| ICMP | In| From Any IP Address| To Any IP Address | Where Message is ECHO REQUEST

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

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

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

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

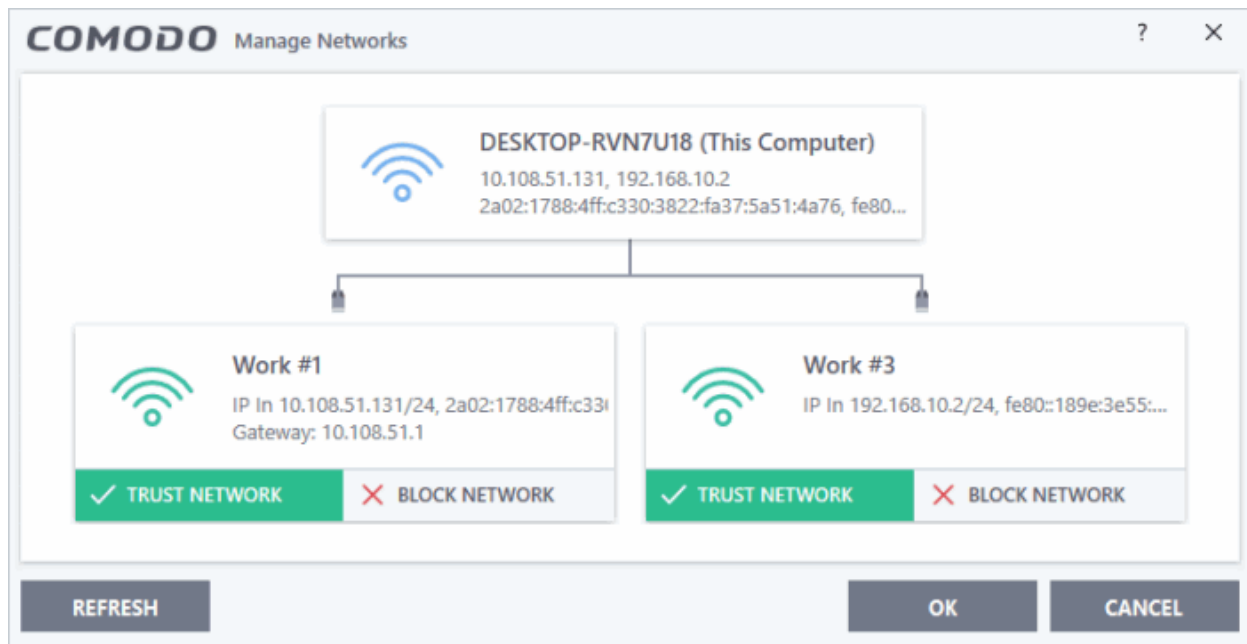
If you would like more information on the meaning and construction of rules, please [click here](#).

3.3. Manage Network Connections

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

To view the network connections of your computer

- Click 'Tasks' at the top left of the CCS home screen
- Click 'Firewall Tasks' from the 'Tasks' interface then click 'Manage Networks'



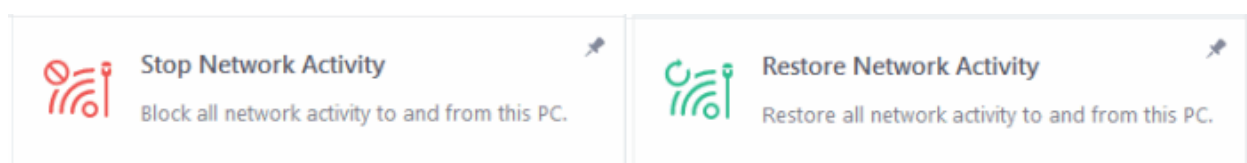
- You can choose to trust or block a network by selecting the appropriate button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks
- Use the handles (< >) to scroll through all available networks or computers
- Use the refresh button if you have recently made network changes and these are not yet visible in the interface
- To view, create or block **Network Zones**, click 'Settings' > 'Firewall' > 'Network Zones'

3.4. Stop all Network Activities

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

To manage network activities from your computer

- Click 'Tasks' at the top left of the CSS home screen
- Click 'Firewall Tasks' from the 'Tasks' interface
- To disconnect your computer from all networks, click 'Stop Network Activity'
- To re-enable connectivity, click 'Restore Network Activity'



- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have previously blocked in '**Manage Network Connections**' or '**Network Zones**' will remain blocked

- You can assign networks into network zones in the '**Network Zones**' area
- You can configure rules per network zone in the '**Global Rules**' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the '**Manage Network Connections**' area

3.5. View Active Internet Connections

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

To view active internet connections on your computer

- Click 'Tasks' at the top left of the CCS home screen
- Click 'Firewall Tasks' from the 'Tasks' then click 'View Connections'

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

Protocol	Source	Destination	Bytes In	Bytes Out
svchost.exe [1544]				
UDP OUT	10.0.2.15:64179	239.255.255.250:1900	0 B	831 B {111 ...
svchost.exe [1308]				
UDP OUT	10.0.2.15:56104	192.168.70.1:53	496 B	89 B
ITSMService.exe [1664]				
TCP OUT	10.0.2.15:49298	52.59.11.165:443	7.2 KB {13.7 ...	1.8 KB {3.3 ...
TCP OUT	10.0.2.15:49162	69.4.89.243:443	28.8 KB {4 B/s}	20.4 KB {3 ...
TCP OUT	10.0.2.15:49291	35.157.49.4:443	9.3 KB {4 B/s}	6.6 KB {9 B/s}

MORE
CLOSE

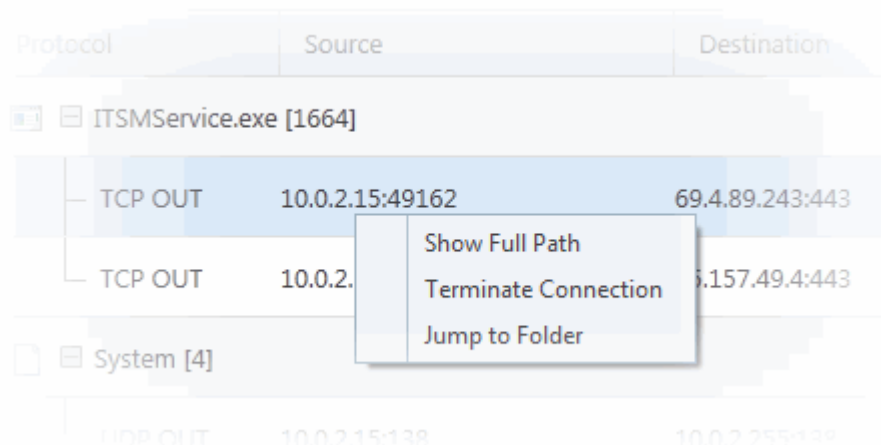
The 'View Connections' interface displays a list of all the currently active connections initiated by various applications as a tree structure.

Column Descriptions

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

Context Sensitive Menu

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



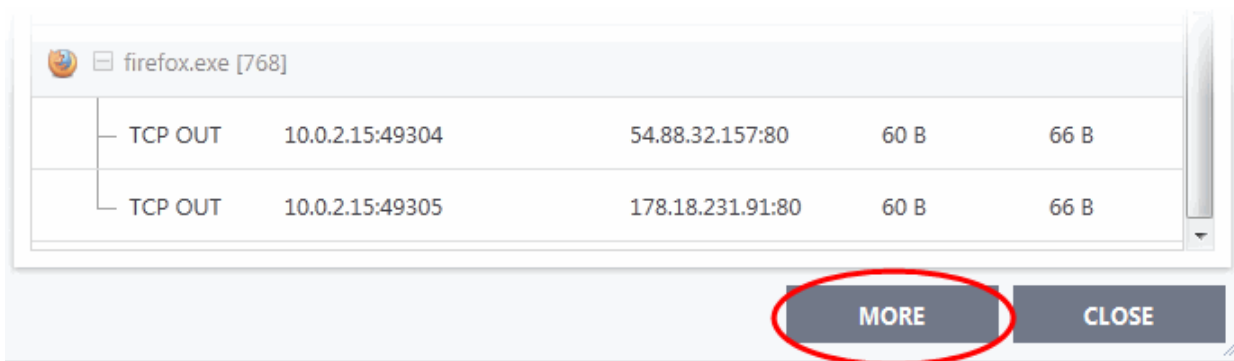
- 'Show Full Path' - view the location of the application
- 'Terminate Connection' - close the application's connection
- Click 'Jump to Folder' to open the folder containing the executable file of the application

Identify and kill unsafe network connections

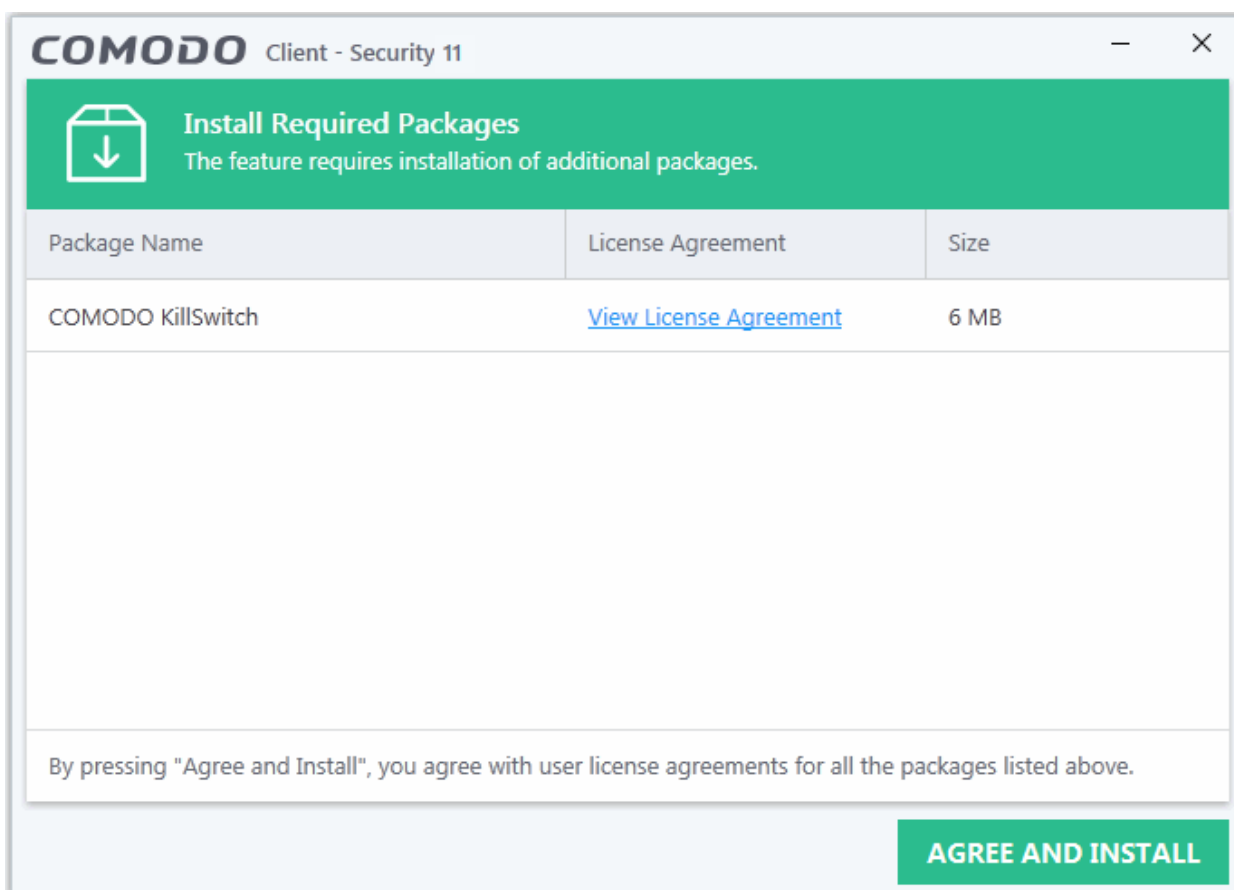
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides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

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

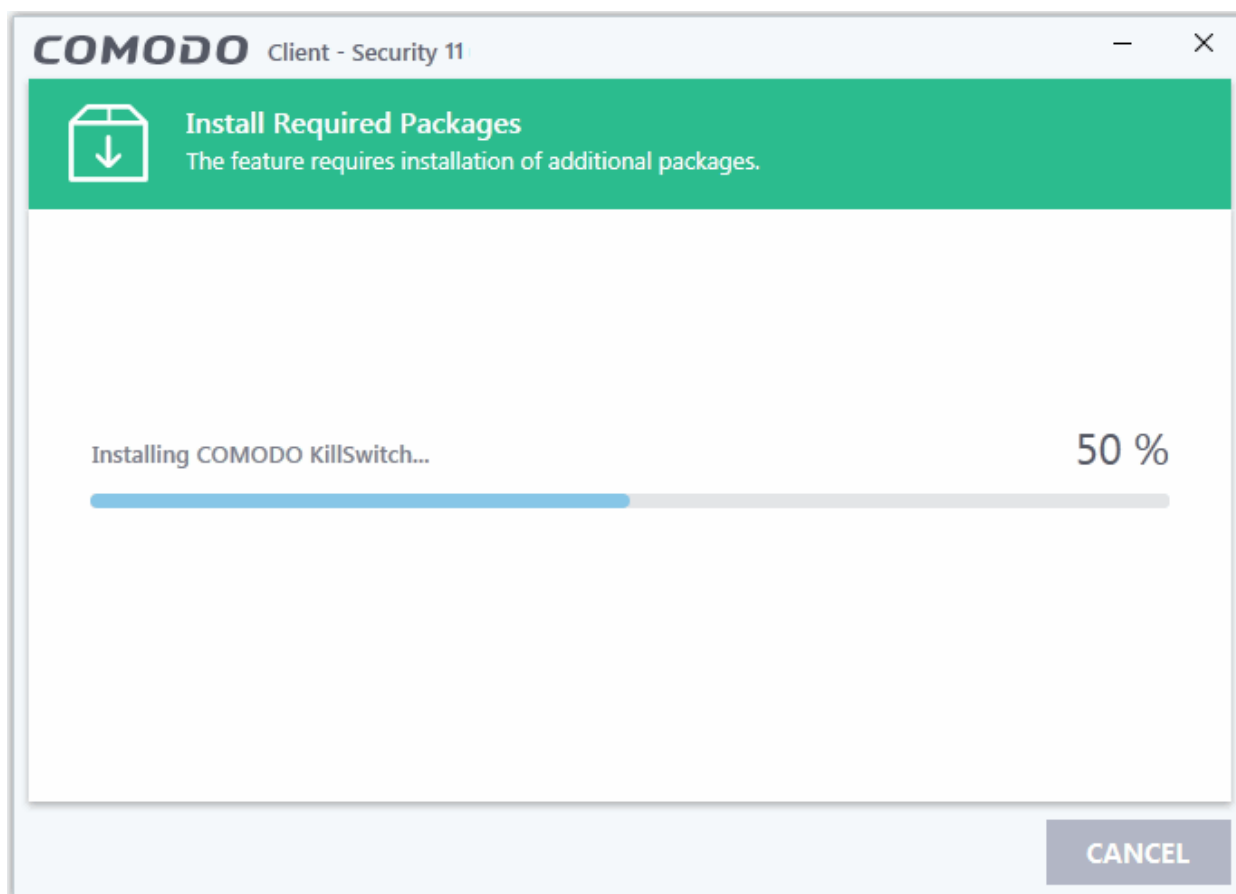
- You can directly access Comodo KillSwitch from the 'View Connections' screen by clicking the 'More' button:



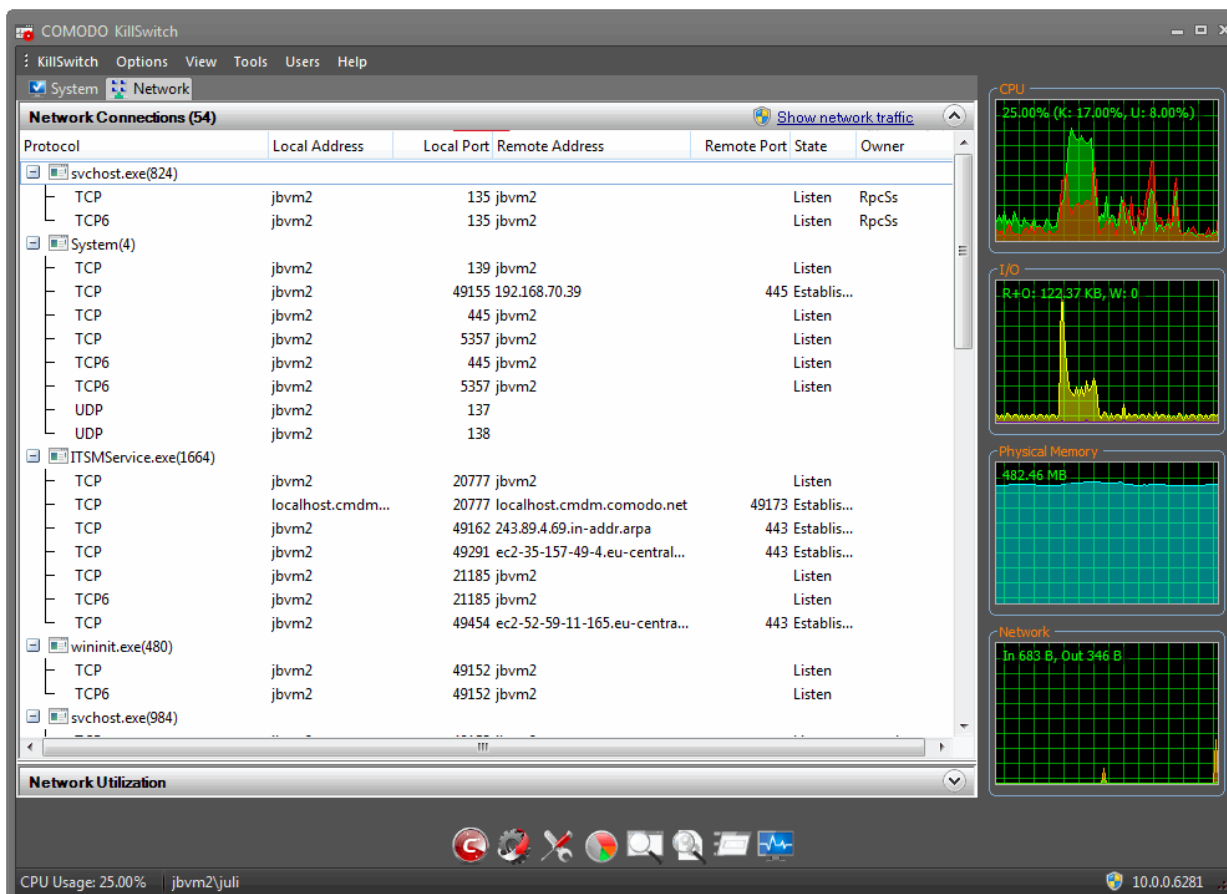
- If Comodo KillSwitch is already installed in your computer, click 'More' to open the application
- If not, CCS will download and install Comodo Killswitch.



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

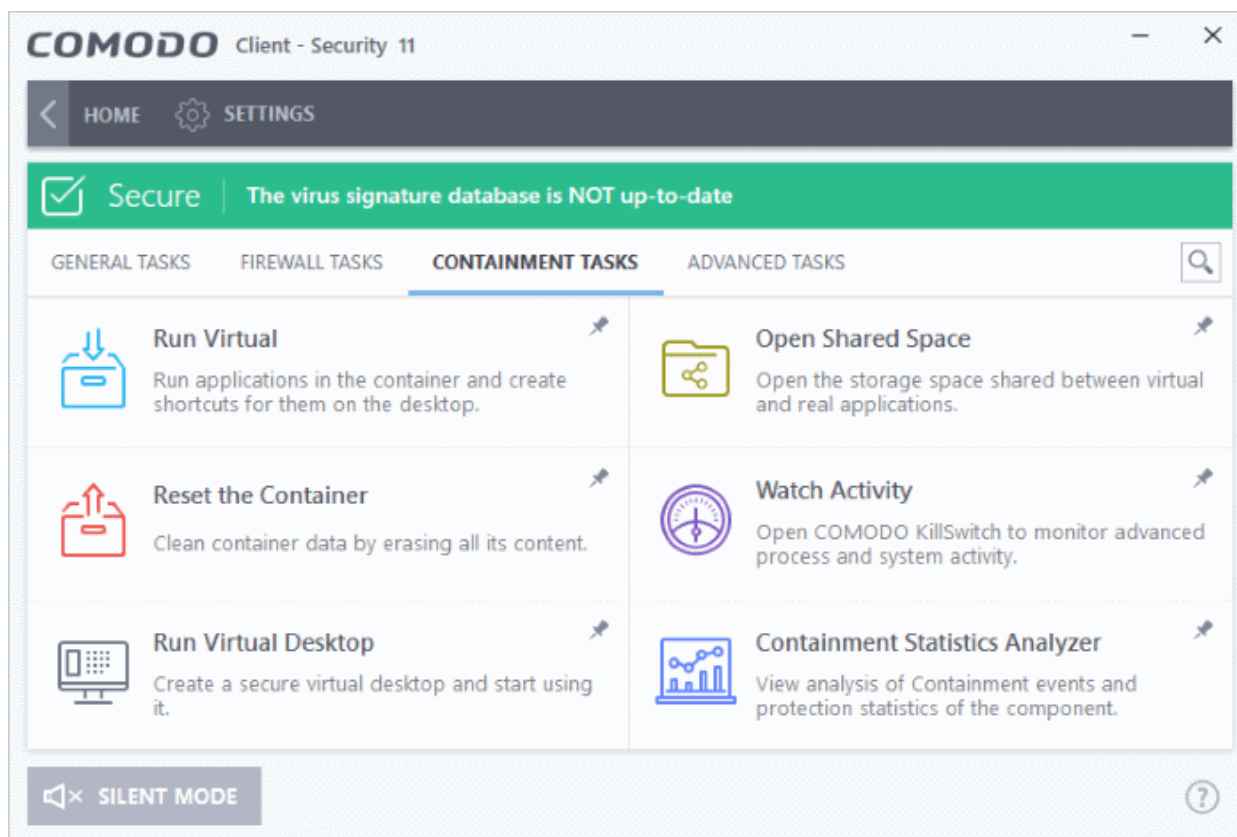


On completion of installation, the Comodo KillSwitch main interface will open. Clicking the 'Network' tab will display the 'Network Connections' and 'Network Utilization' panes.



4. Containment Tasks - Introduction

- Comodo Client Security features a secure, virtual environment called a 'container' in which you can run unknown, untrusted and suspicious applications.
- Contained applications are denied access to other processes, programs or data on your computer. This isolation allows safe programs to run as normal, but denies malicious programs the access they need to steal data or cause damage.
- You can run applications inside the container on an ad-hoc basis. You can also create desktop shortcuts that will launch an application in the container.



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

- Windows XP 64 bit
- Windows Server 2003 64 bit

The Containment Tasks interface the following shortcuts:

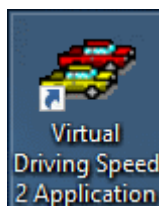
- **Run Virtual** - Allows you to run individual applications in the container.
- **Open Shared Space** - 'Shared Space' is a folder that can be accessed by both the host/local computer and by contained applications. If you want to save files from the container, then you should save them to the shared space folder.

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

- **Reset Containment** - Allows you to clear all data written by programs inside the container.
- **Watch Activity** - Opens Comodo KillSwitch. KillSwitch lets you identify unsafe processes and manage system activity.
- **Run Virtual Desktop** - Starts the Virtual Desktop.
- **Containment Statistics Analyzer** - Detailed information about the processes running on your computer. Processes are split into contained and non-contained processes.

4.1. Run an Application in the Container

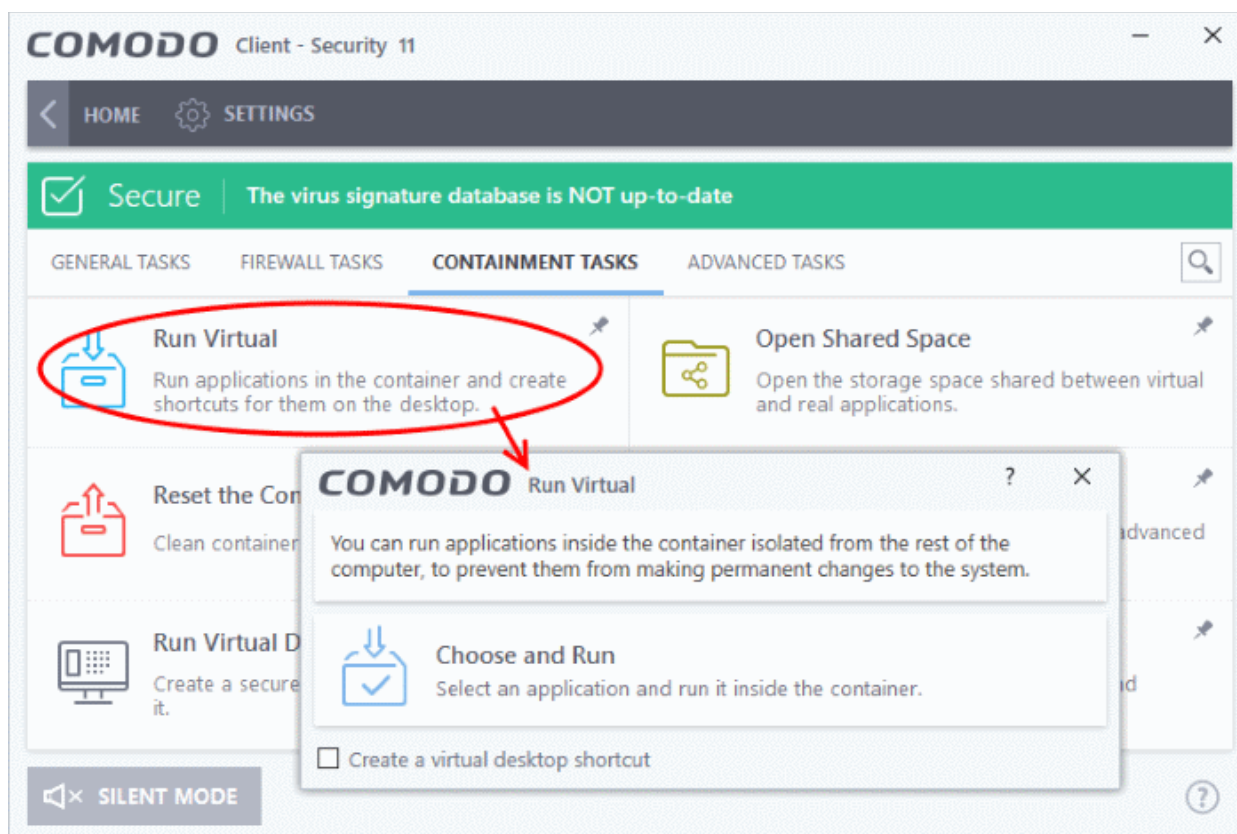
- Comodo Client Security allows you to run programs in containment on a 'one-off' basis.
- This is helpful to test the behavior of new programs you have downloaded or for applications that you are not sure about.
- This method will run the application in the container one-time only. On subsequent executions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



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

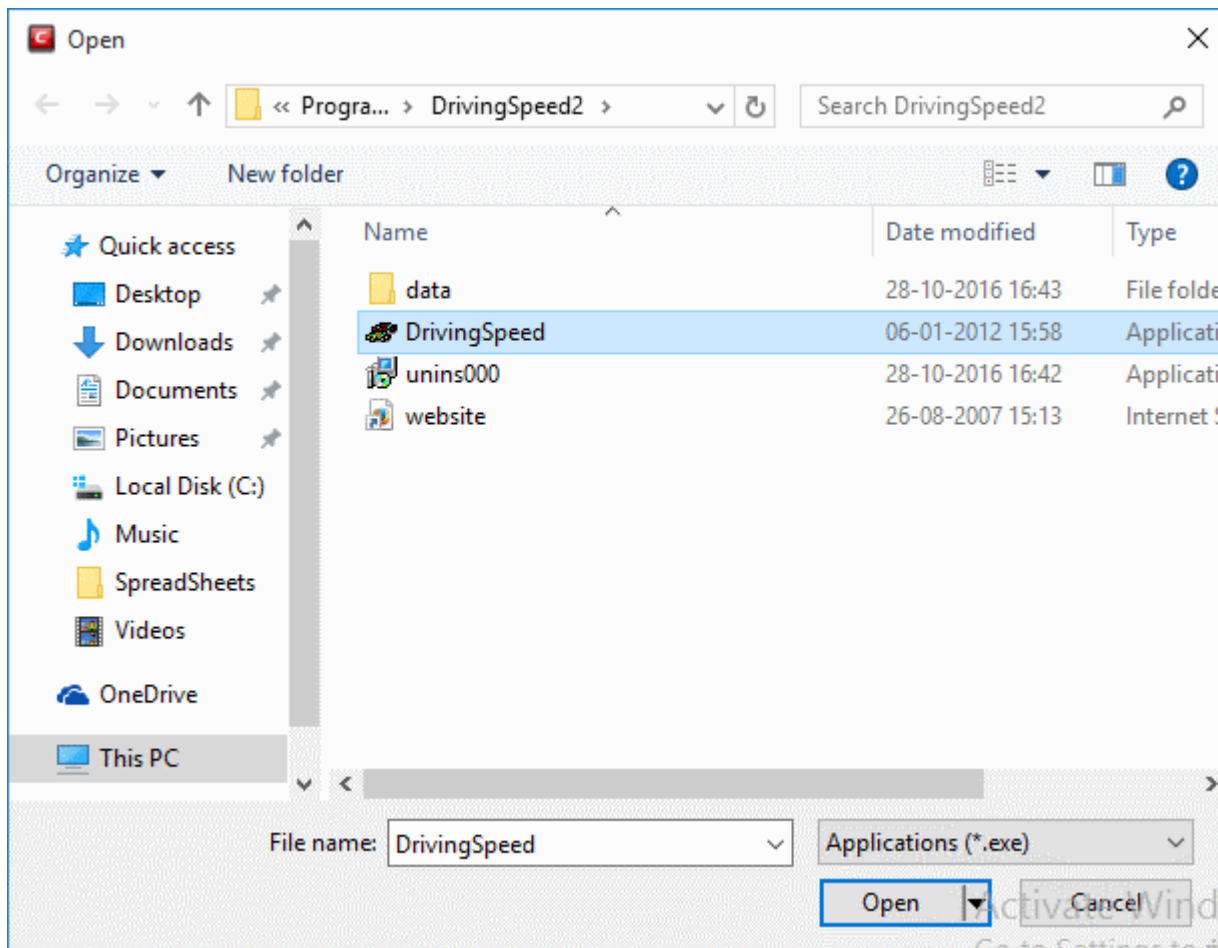
To run an application in the Container

1. Click 'Tasks' at the top left of the CCS home screen
2. Click the 'Containment Tasks' tab
3. Click 'Run Virtual':



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

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

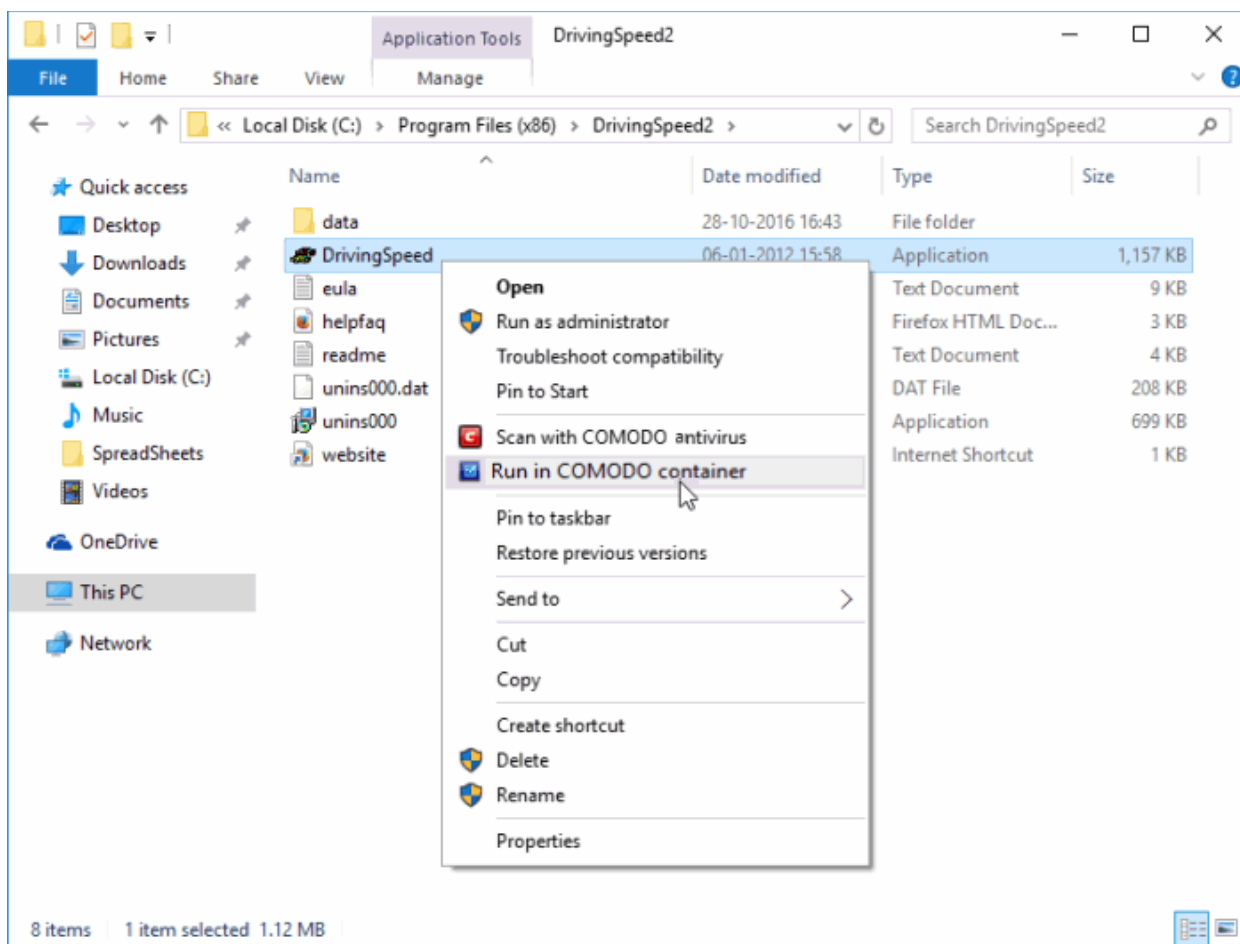


You can also run applications in the container on a one-off basis using the following methods:

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

Running a program from the context sensitive menu

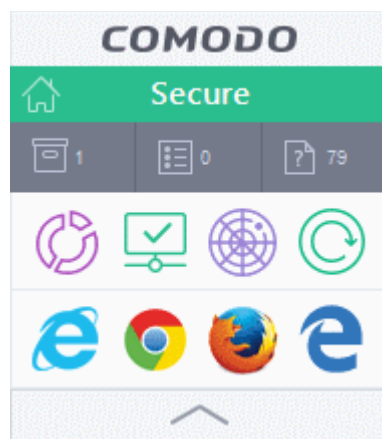
- Navigate to the program in your system that you want to run in the container and right click on it



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

Running Browsers inside the container

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



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

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

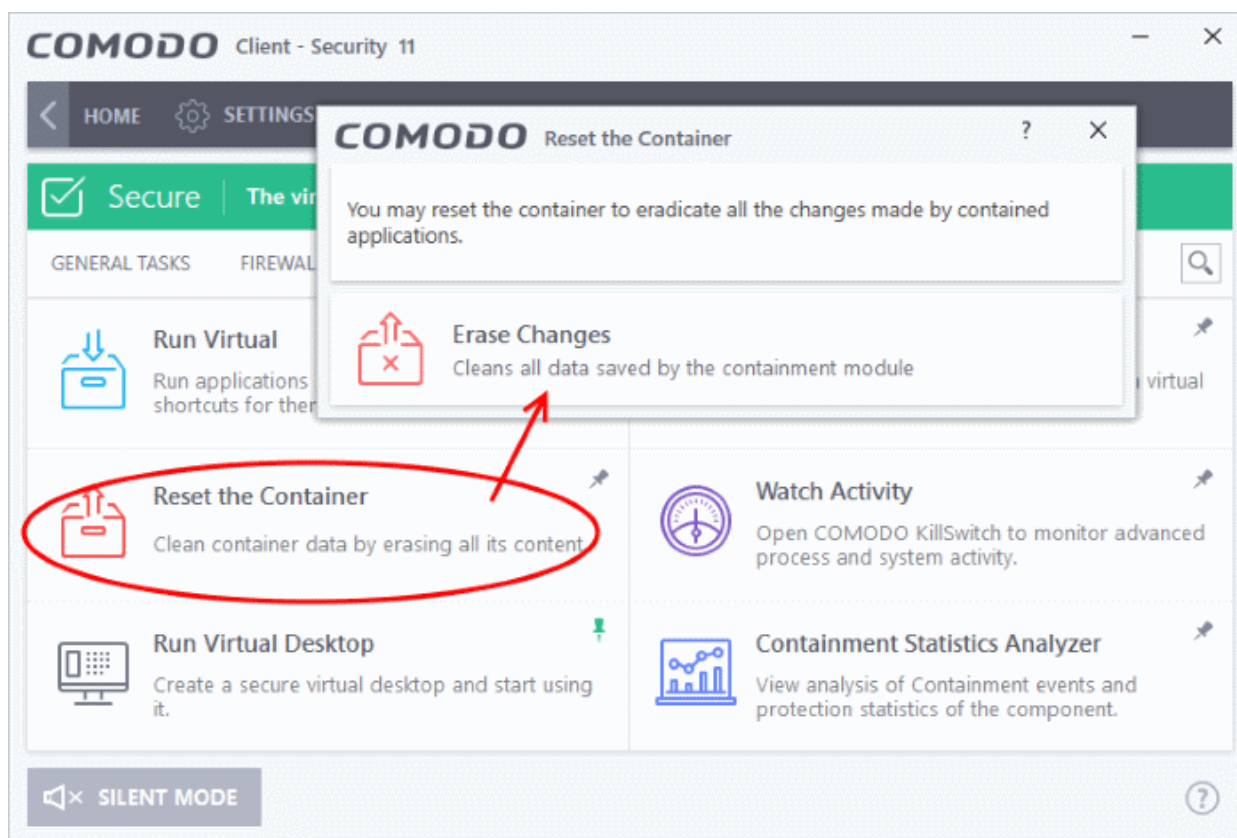
4.2. Reset the Container

- Programs running inside the container write all data and system changes inside the container itself. This means the contained program cannot harm your computer or access your private data.
- Files saved in the container could contain malware 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.

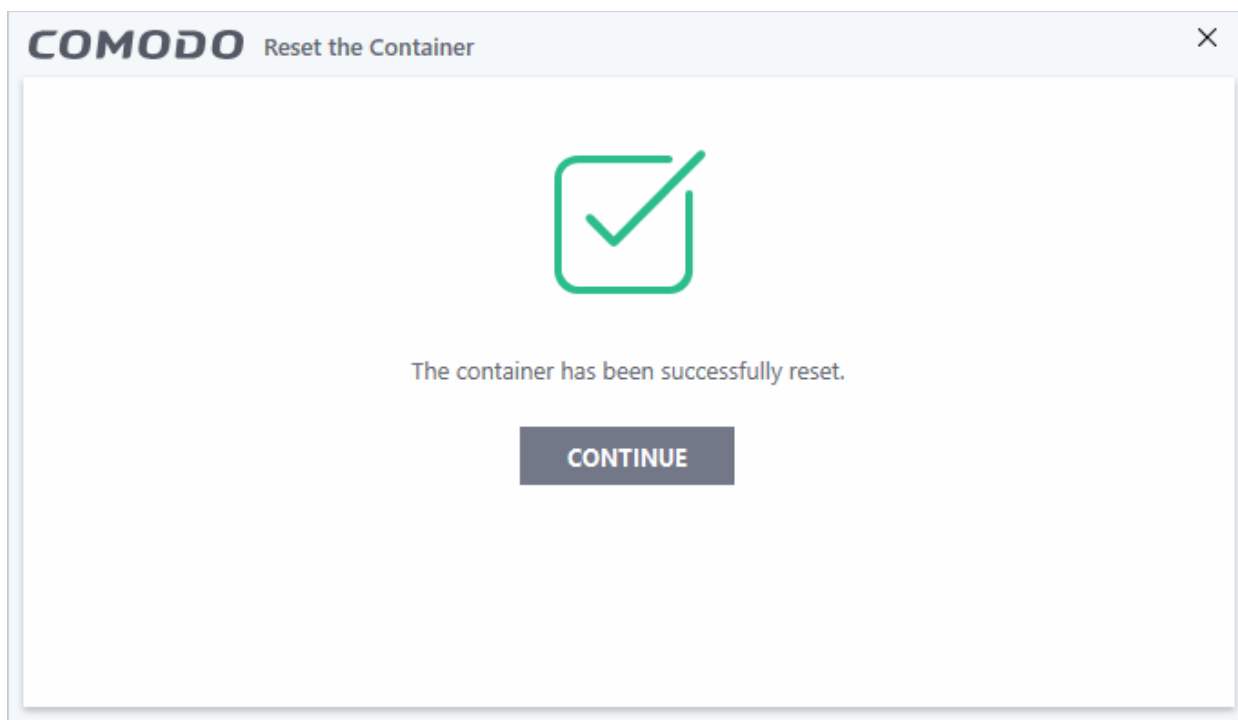
The 'Reset Containment' option lets you to delete all items stored in the container.

To clear the container

- Click 'Tasks' on the CCS home screen
- Click the 'Containment Tasks' tab
- Click 'Reset the Container':
- Click 'Erase changes' in the reset dialog:



The contents in the container will be deleted immediately.



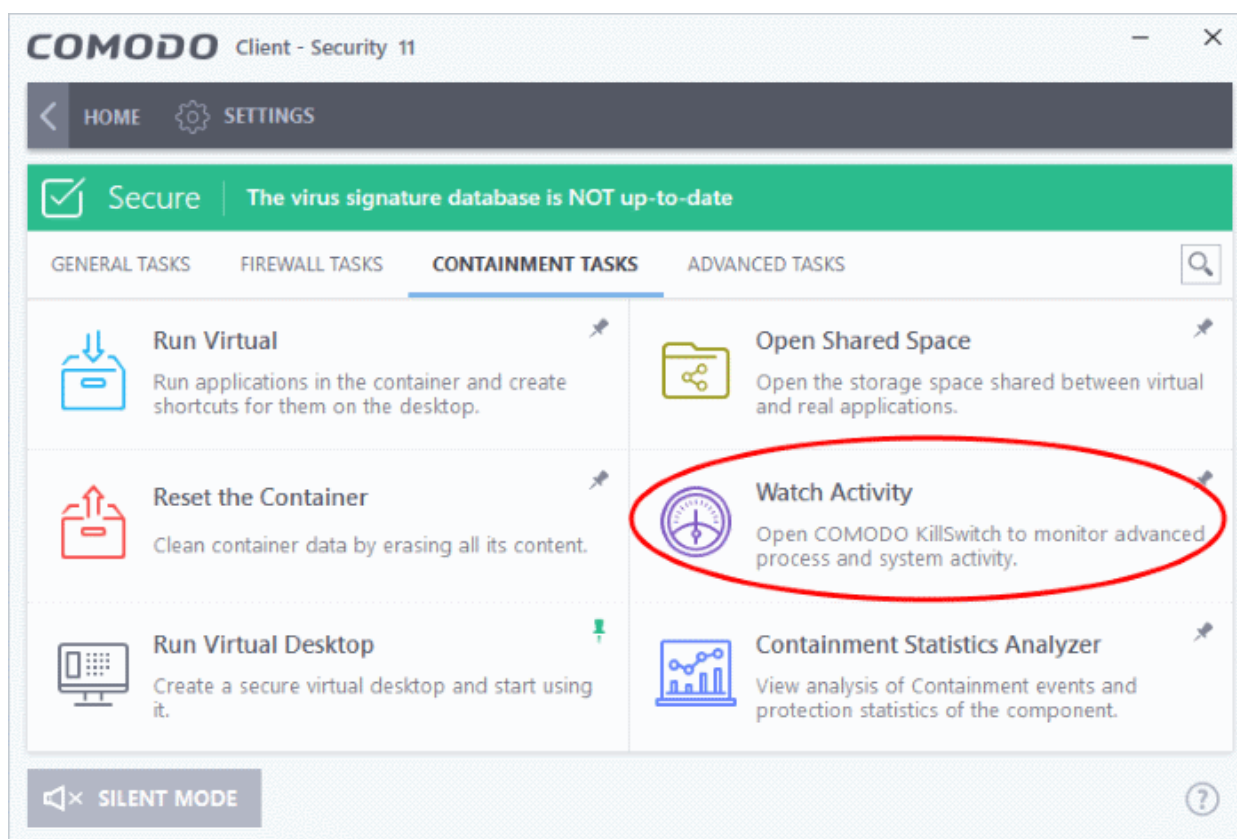
- Click 'Continue' to close the dialog.

4.3. Identify and Kill Unsafe Running Processes

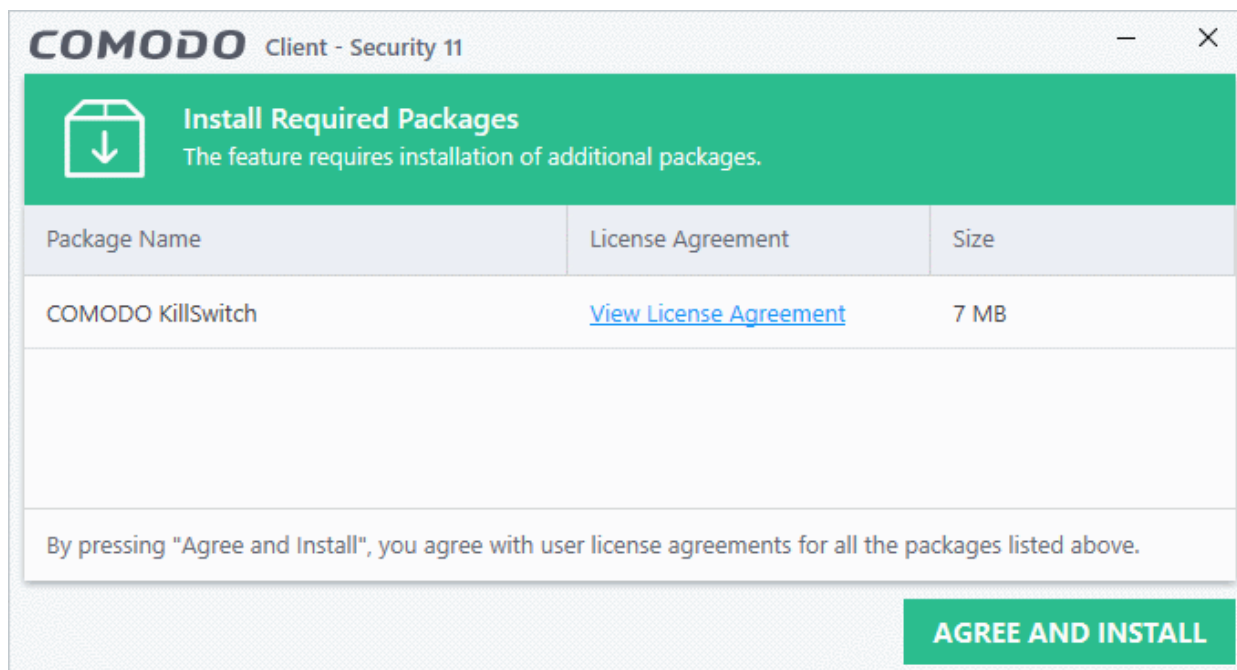
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer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

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

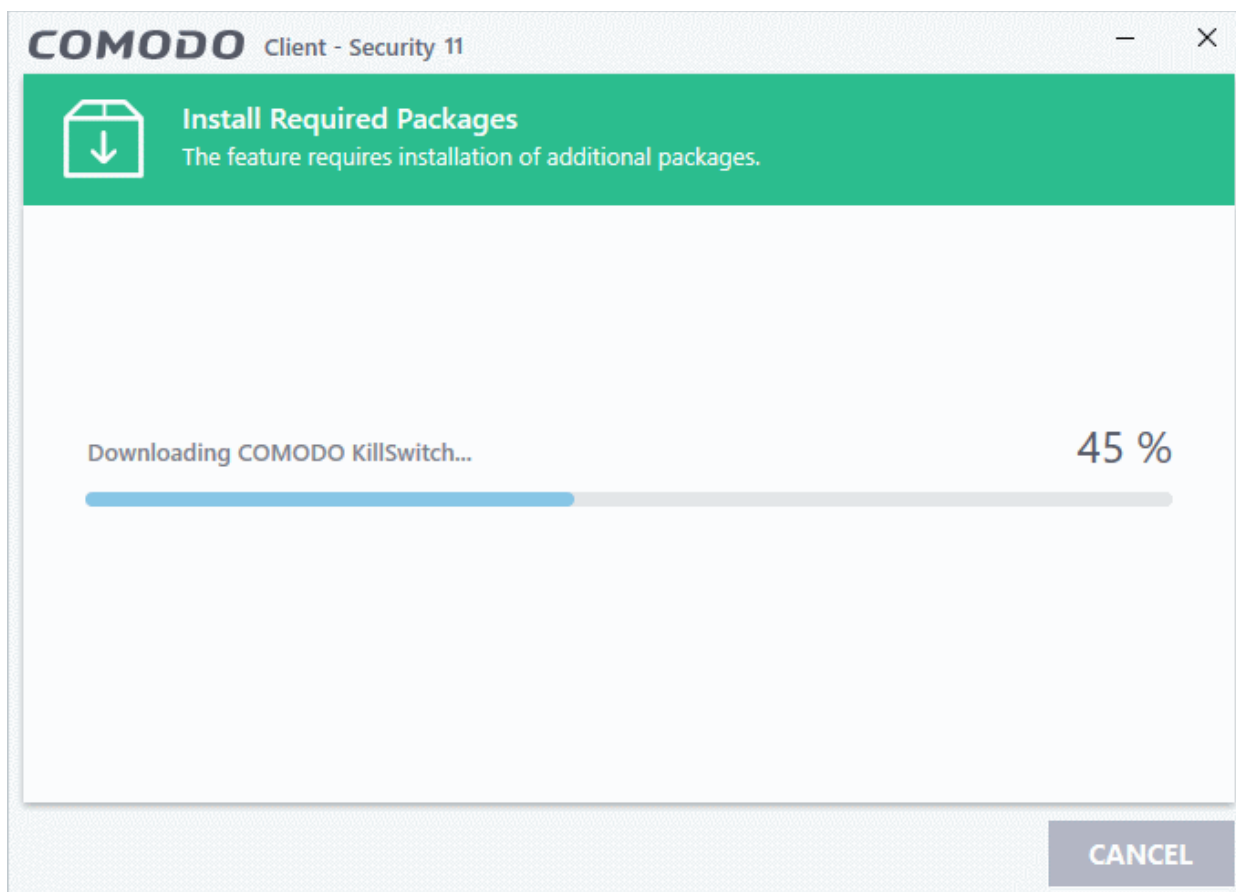
Comodo KillSwitch can be directly accessed from the CCS interface by clicking the 'Watch Activity' button in the 'Containment Tasks' interface.



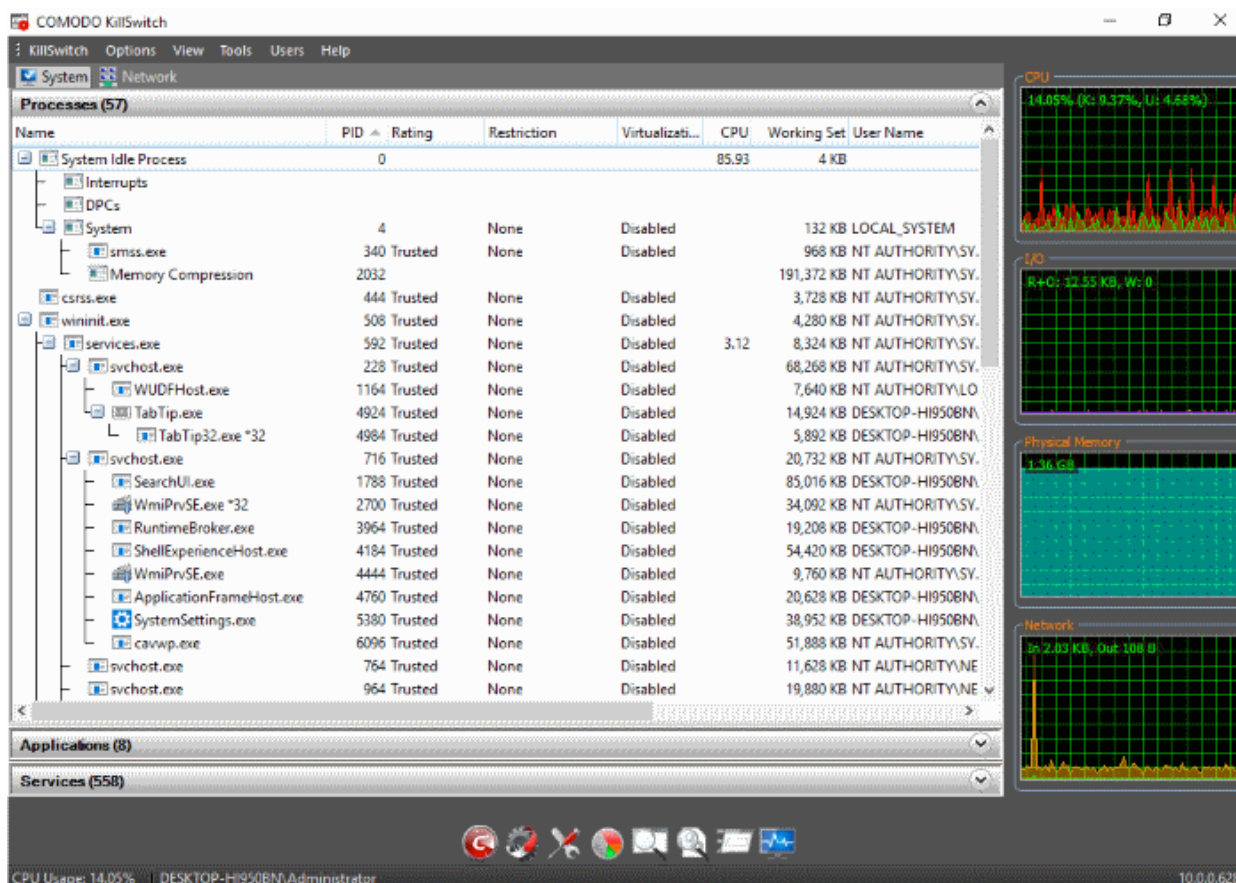
- When you click 'Watch Activity' for the first time, CCS will download and install Comodo Killswitch. After it installed, clicking this button in future will open the Killswitch interface.



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



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

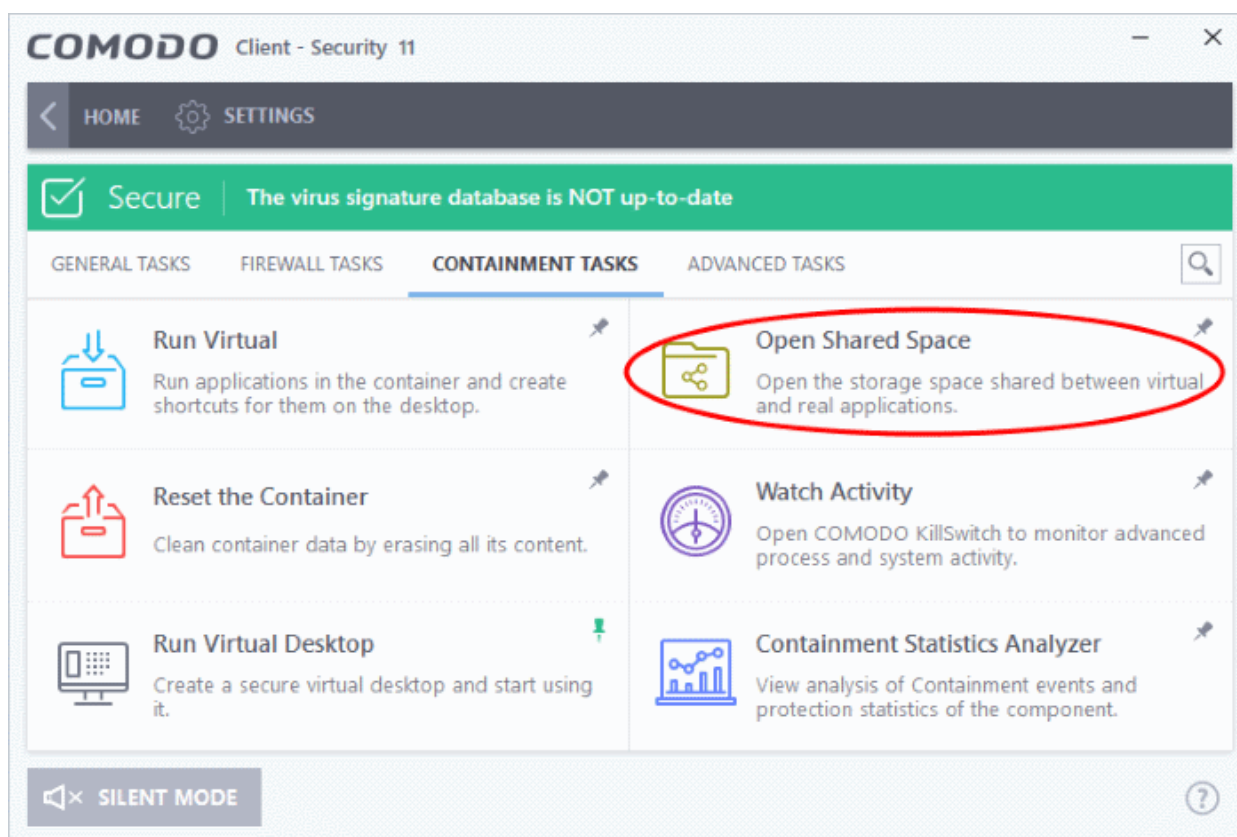


On clicking the 'Watch Activity' button from next time onwards, Comodo Killswitch will be opened.

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

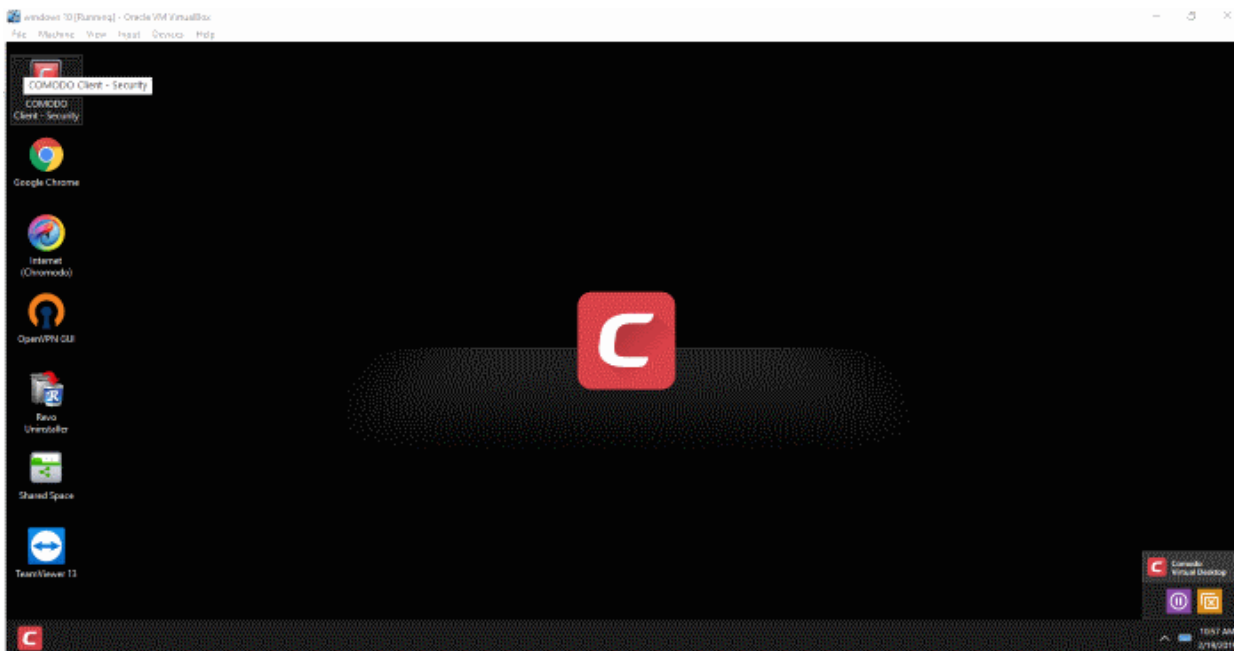
4.4. Open Shared Space

- Applications running in the container are not allowed to write to your local drive for security reasons. Instead, they write all data, and save all files, to a virtual drive.
- If you want to access files in the container from your local system, then you should download them to the 'Shared Space'. Shared space is a special folder on your local drive to which contained applications are allowed to write.
- Files in shared space can also be accessed by non-contained applications. The default location of the shared folder is 'C:/Program Data/Shared Space'.
- Use the shared space desktop shortcut to quickly access all files saved/generated by contained applications.
 - Alternatively, open 'Tasks' > 'Containment Tasks' > 'Open Shared Space' in the CCS interface:



4.5. The Virtual Desktop

- Go to '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 risk-free internet surfing 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 originals on your host system. Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Save any files you wish to access from your host operating system to 'Shared Space'.
- The virtual desktop can be password-protected for added privacy.
- The virtual keyboard allows you to securely enter confidential passwords without fear of key-logging software.
- Apart from testing software, parents may want to consider the virtual desktop as a secure area for children to run programs and surf the web. Any actions they take will not damage 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](#)
- [Close the Virtual Desktop](#)

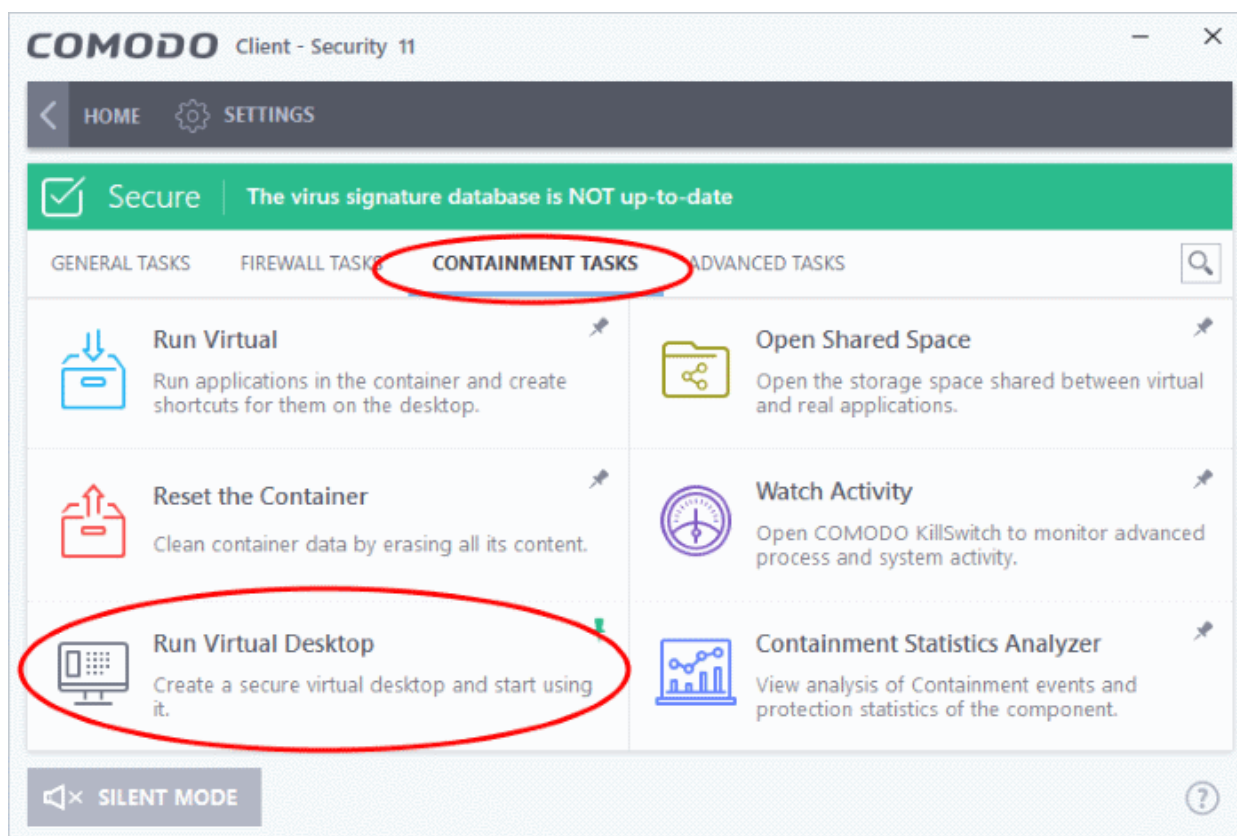
4.5.1. Start the Virtual Desktop

There are three ways you can start the virtual desktop:

- **From the Containment tasks screen**
- **From the CCS widget / taskbar**
- **When you login**

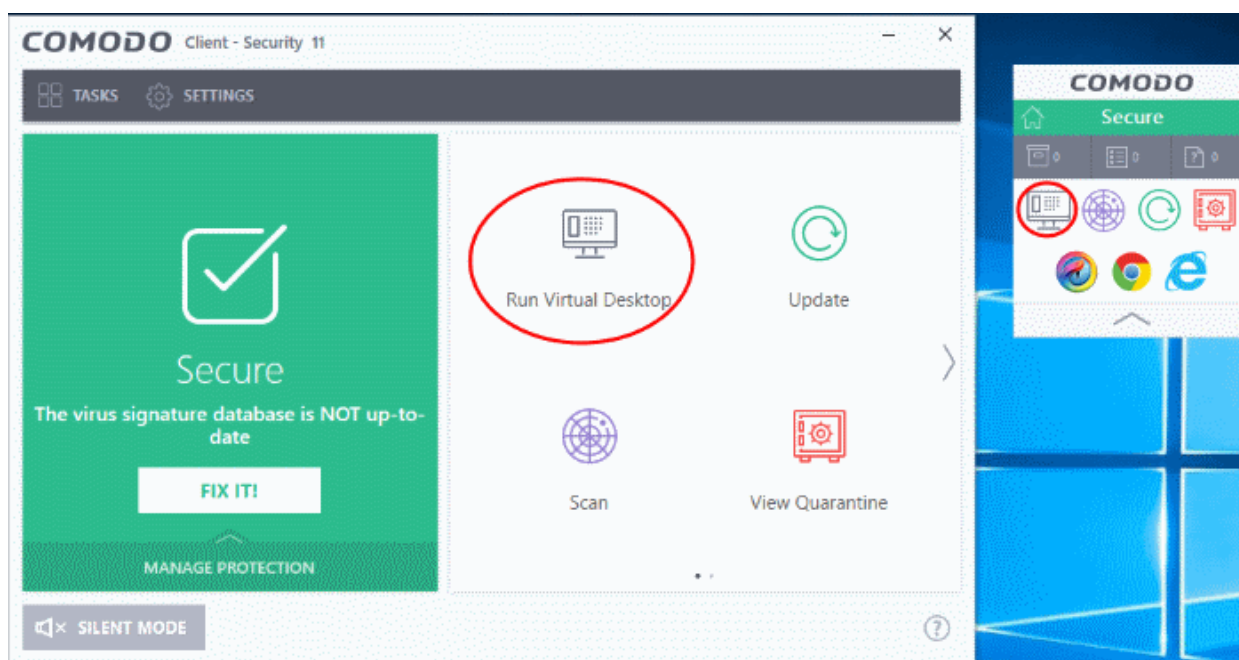
Open Virtual Desktop from the Containment tasks screen

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



Open Virtual Desktop from CCS widget / taskbar

- Click the virtual desktop icon on the CCS widget:



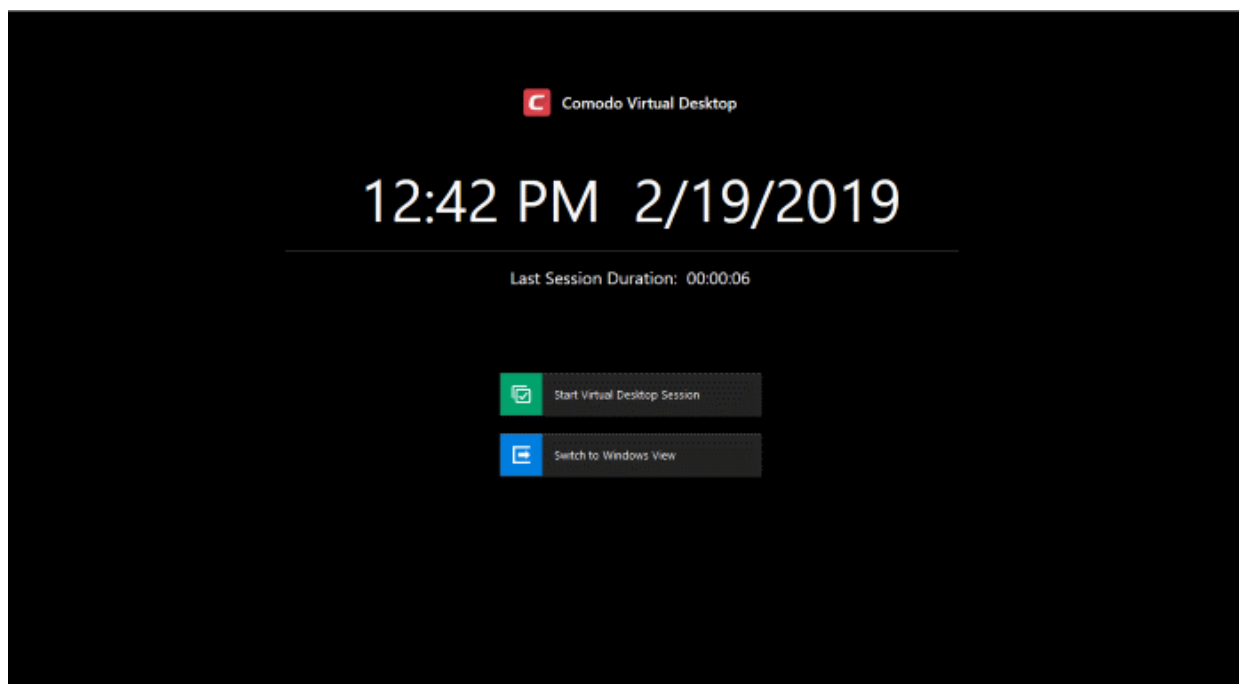
Note: The shortcuts on the taskbar and widget are only available if you have added the 'Virtual Desktop' shortcut. See **'Add tasks to the home screen'** in **'The Home Screen'** for more details.

User login

You can instruct CCS to launch the virtual desktop every time you logon to the computer:

- Open Comodo Client Security
- Click 'Settings' on the home screen
- Click 'Containment' > 'Virtual Desktop'
- Enable 'Launch Virtual Desktop upon user login'
 - See **'Virtual Desktop Settings'** if you need more help with this

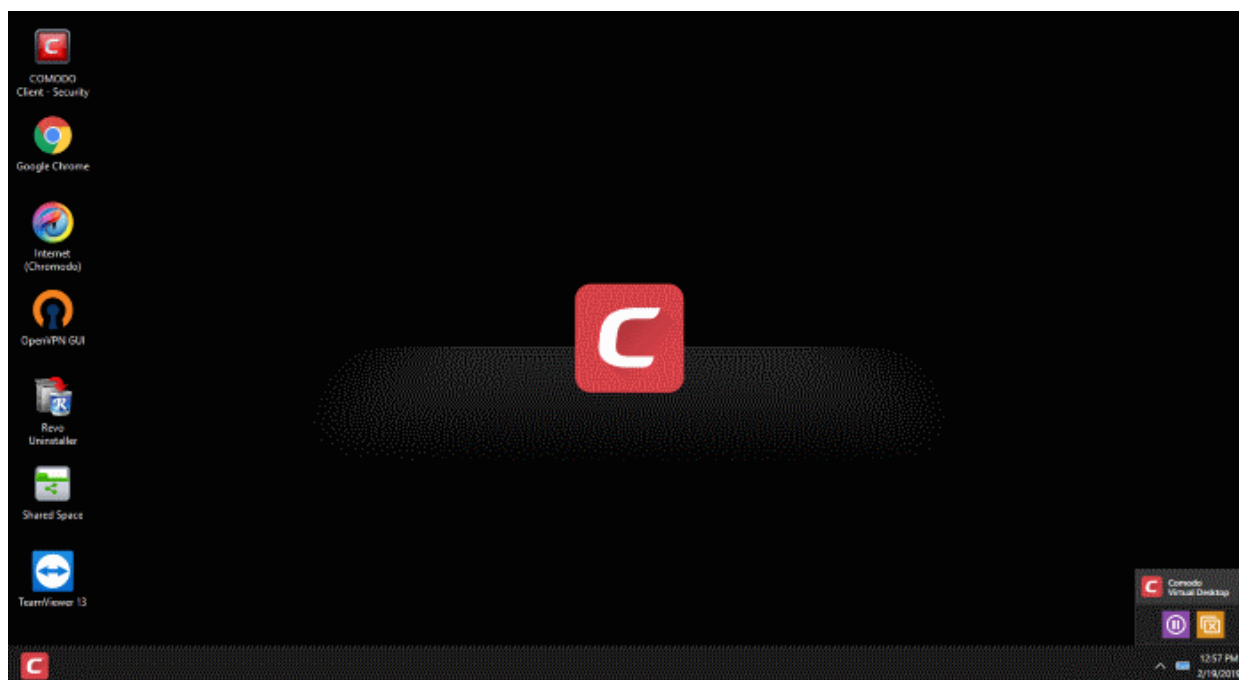
The virtual desktop appears as follows at logon:



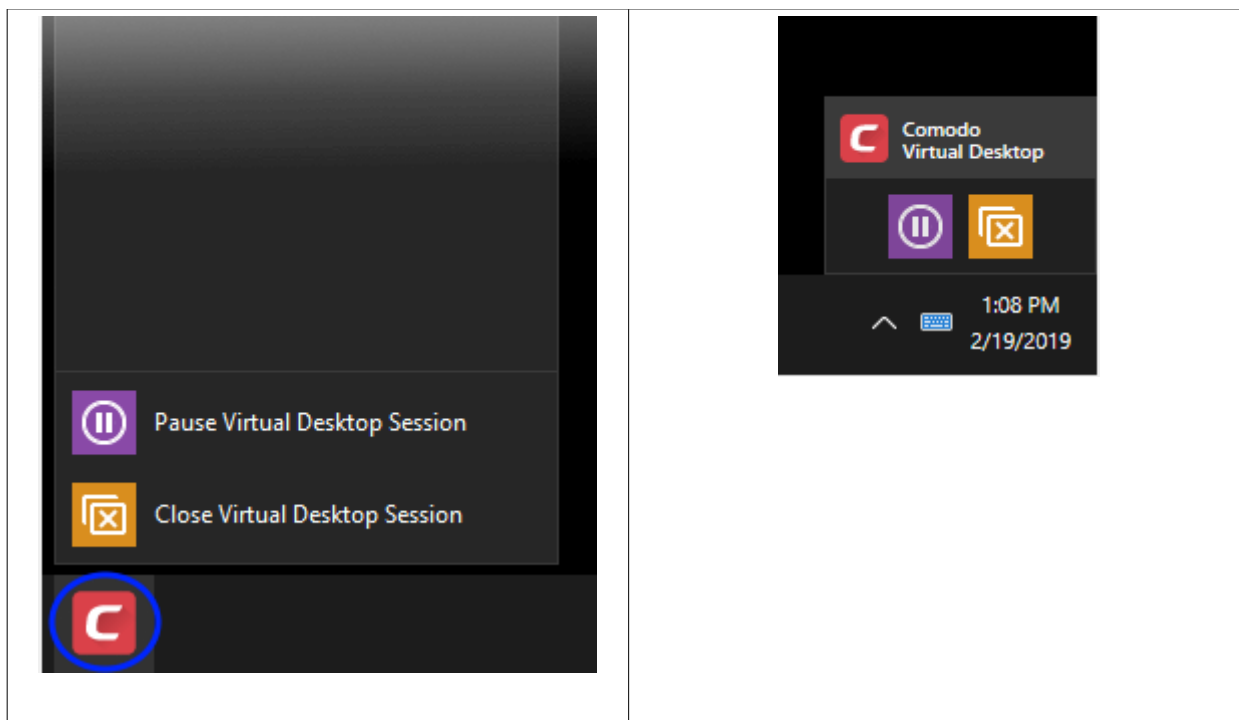
- Click 'Start Virtual Desktop Session' button

4.5.2. The Main Interface

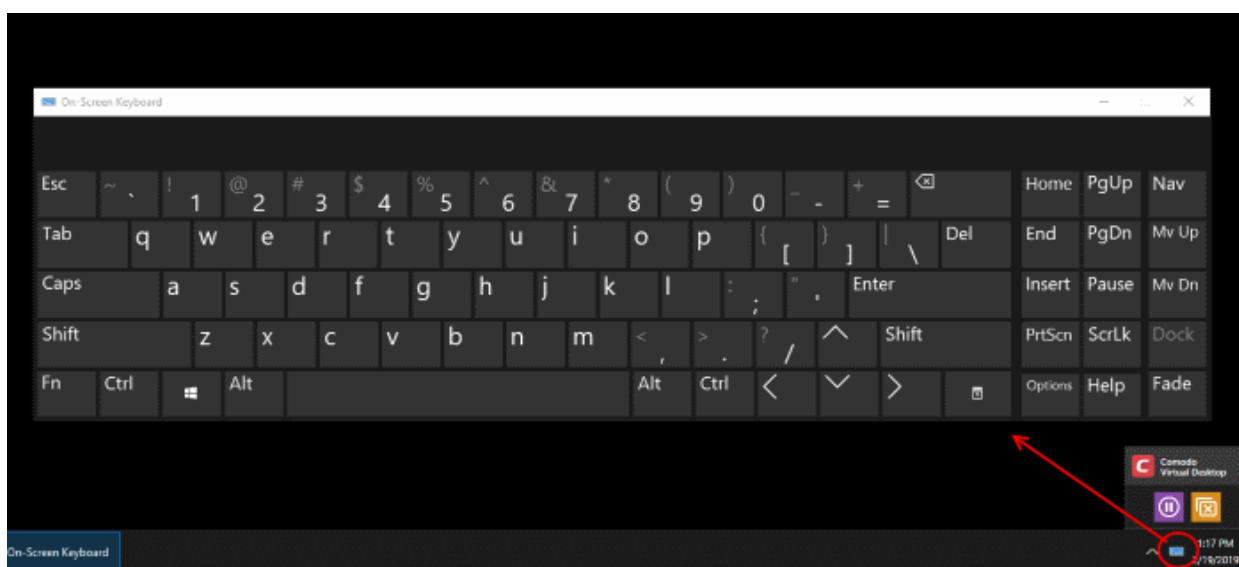
- All application shortcuts from your real desktop are shown on the left of the virtual desktop.
- The bottom-left corner of the screen has controls to switch between the virtual desktop and Windows, pause the session and more.



- You can also click the 'C' at bottom right to switch to Windows, pause, or close the Virtual Desktop:



- The virtual keyboard can be used to input confidential data like website user-names, passwords and credit card numbers. Using the keyboard prevents key-logger software from recording your keystrokes. The keyboard is compatible with touch screen displays:

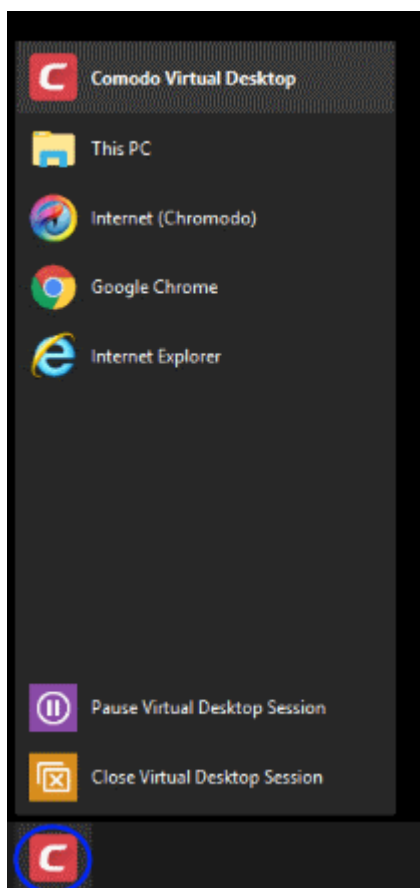


4.5.3. Run Browsers inside the Virtual Desktop

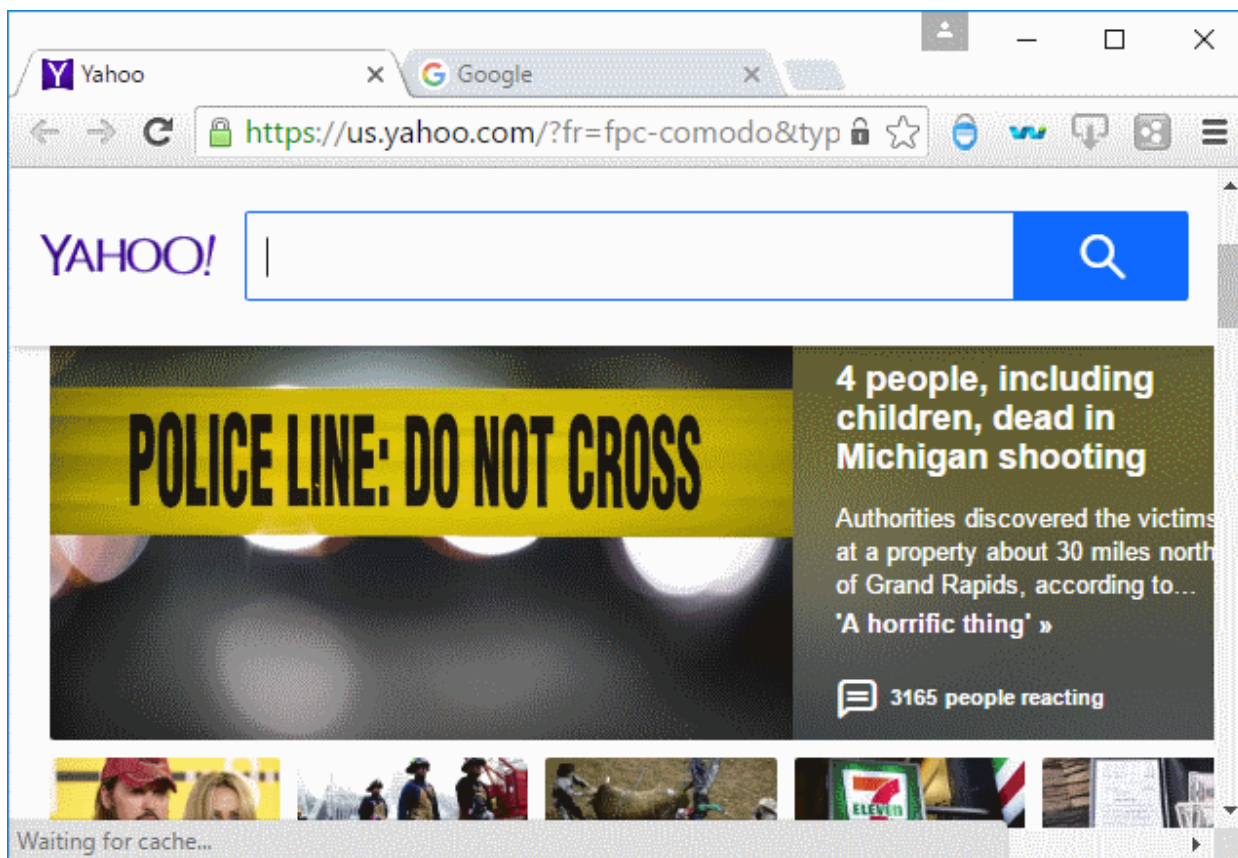
- The virtual desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer.
- Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer.
- Surfing the internet from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

Run a browser inside the Virtual Desktop

- All browsers installed on your computer are also available in the virtual desktop
- Click a browser shortcut on the desktop, or click the 'C' button at bottom-left:



- Select the browser that you want to run



Browsing history and other records of your internet activity are not stored on your computer when you close the session.

4.5.4. Open Files and Run Applications inside the Virtual Desktop

You can use any of the following methods to launch a local program or file in the virtual desktop:

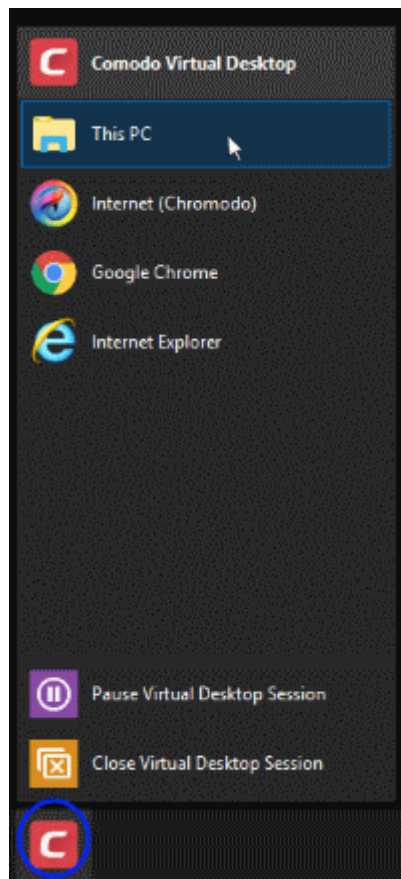
- **Open applications/files from the desktop shortcuts**
- **Navigate to the application/file**
- **Place the application/file in the 'Shared Space' folder**

Desktop Shortcuts

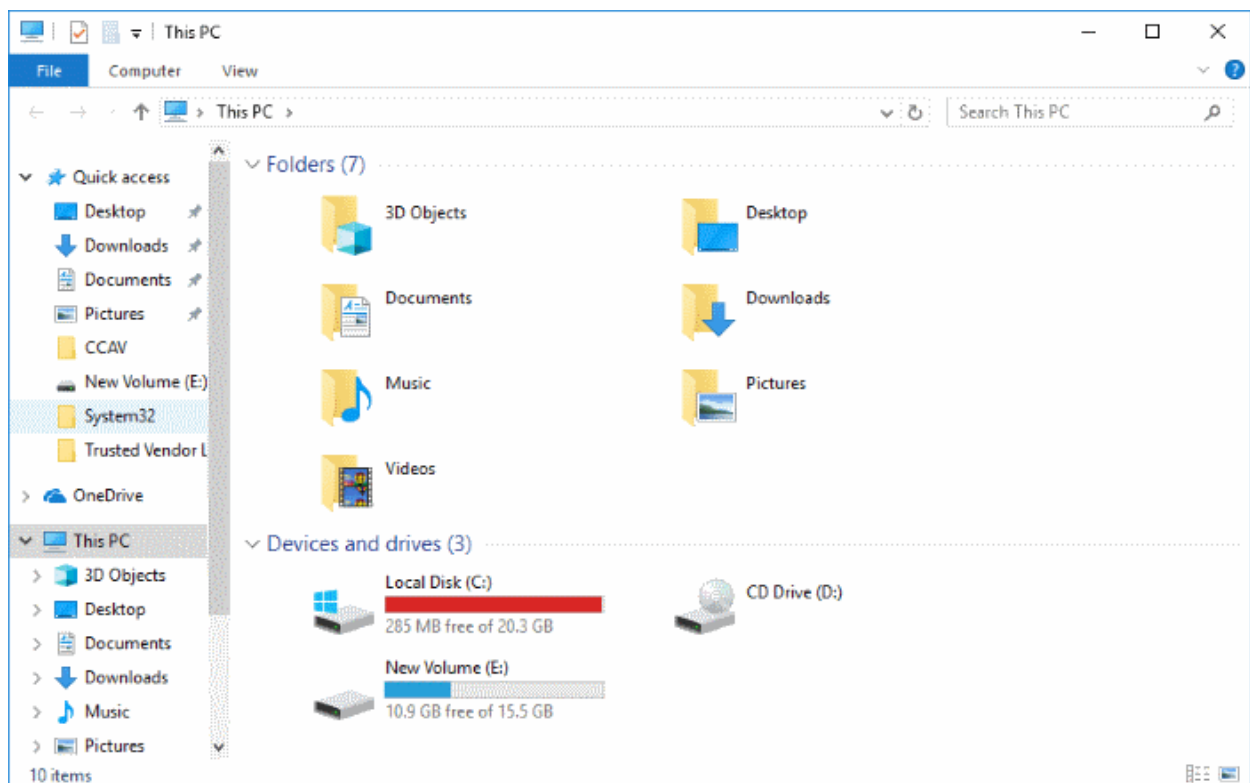
- Create a shortcut for the target application/file on the desktop of your real system.
- All your desktop shortcuts are also available in the virtual desktop.
- Open the virtual desktop and double-click on a shortcut to run the target in the virtual desktop.

Navigate to Application / File

- Click the 'C' button at bottom-left, then 'This PC'



- Navigate to the application / file and open it. The file will open in the virtual desktop.



Shared Space

- The virtual desktop creates a folder called 'Shared Space' at "C:\ProgramData\Shared Space".
- Items in this folder can be accessed by both your host operating system and the virtual desktop.
- For example, you can use this folder to save items downloaded from the internet in a virtual browsing session. You can then access these items from your host computer.

You can use any of the following methods to access shared space:

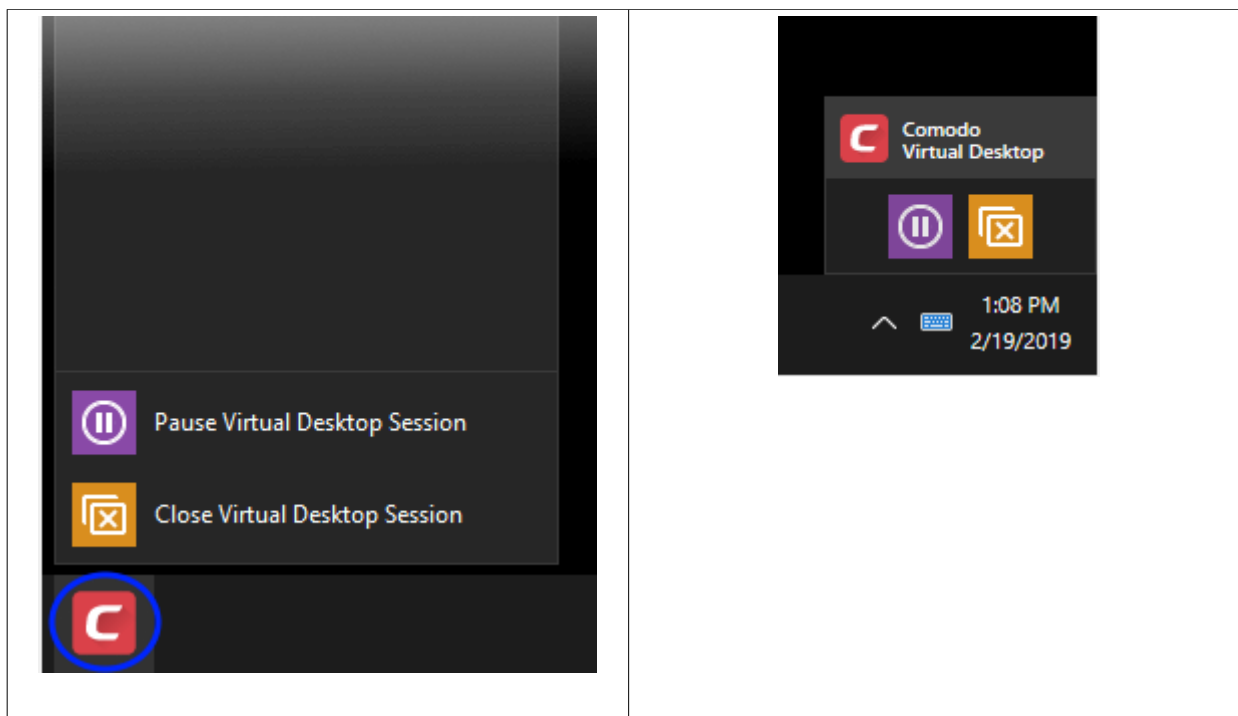
- Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space'
- Click the 'Shared Space' shortcut on the CCS home screen
- Click the 'Shared Space' shortcut icon on the CCS widget

Run a local application or file in the Virtual Desktop

1. Open 'Shared Space' folder as mentioned above
2. Copy or move the item to the shared space folder
3. Start the virtual desktop ('Tasks' > 'Containment Tasks' > 'Run Virtual Desktop')
4. Click the 'Shared Space' icon on the virtual desktop home screen.
5. Open the application/file you just copied there. The file will run inside the virtual desktop.

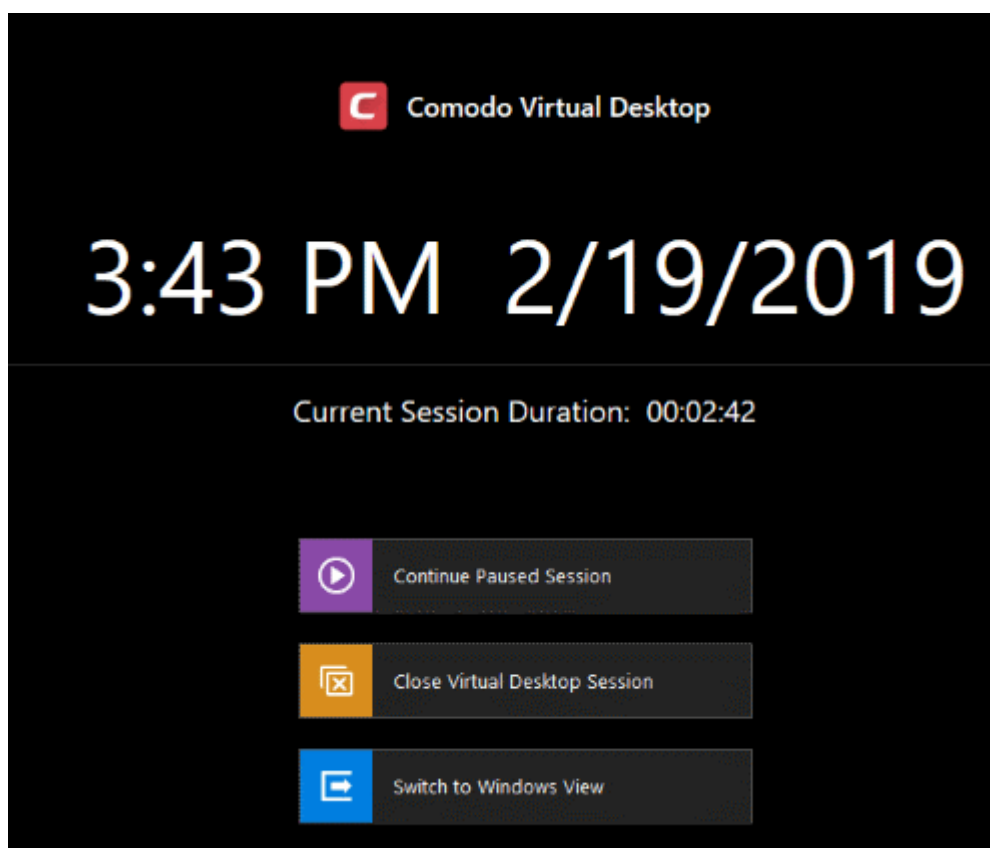
4.5.5. Close the Virtual Desktop

- The shortcuts at the bottom-right and bottom-left of the Virtual Desktop, allow you to temporarily switch to your real computer system

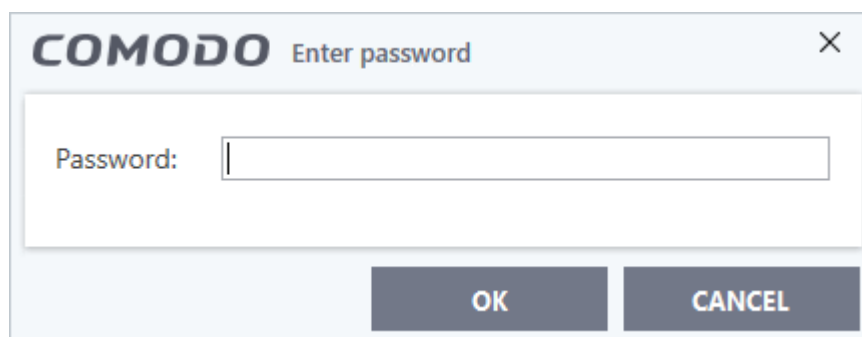


To temporarily switch to your real Windows system

- Click the 'Pause' button on the bottom-right
- Alternatively, click the 'C' button at bottom left and choose 'Pause Virtual Desktop Session' from the Virtual Desktop Start Menu.

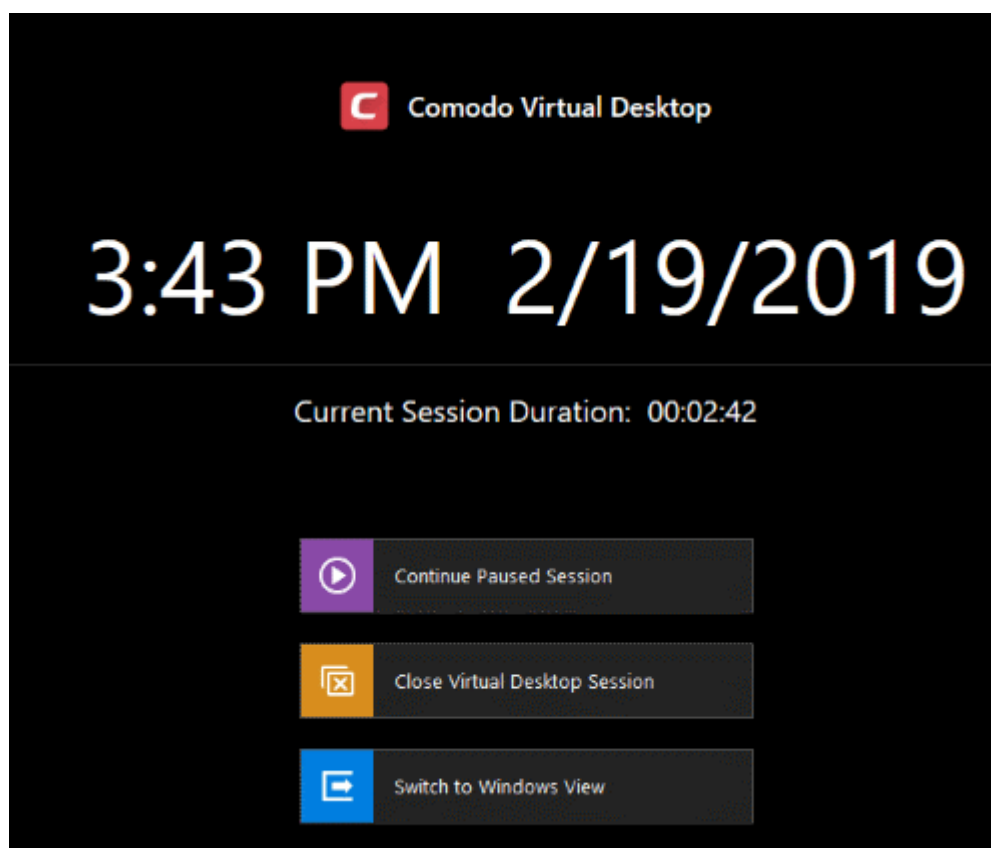


- Click 'Switch to Windows View'



- Enter password if configured in 'Advanced Settings' > 'Containment' > 'Virtual Desktop' > 'Request password when exiting Virtual Desktop'
- Click 'OK'

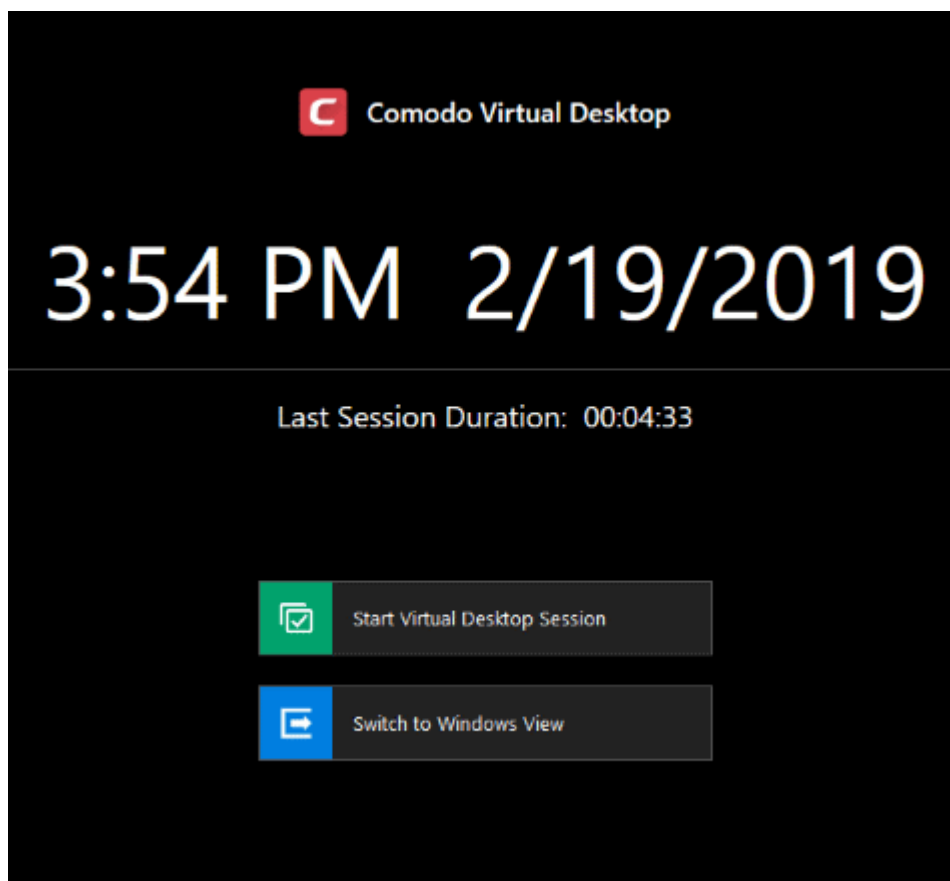
The 'Virtual Desktop' will be temporarily closed. You can quickly return to it by clicking the right switch from the 'Virtual Desktop' shortcut buttons displayed at the bottom right of your Windows Desktop or by clicking 'Run Virtual Desktop' from the 'Containment Tasks' interface.



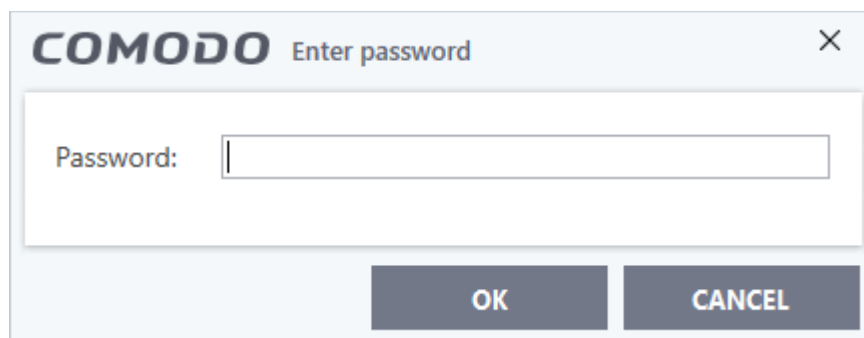
- Click 'Continue Paused Session' to return to your previous Virtual Desktop session.

To close the Virtual Desktop

- Click the X button from the Virtual Desktop shortcuts pane at the bottom-right
- Alternatively, click the 'C' button at bottom left and choose 'Close Virtual Desktop Session' from the 'Virtual Desktop' Start Menu.



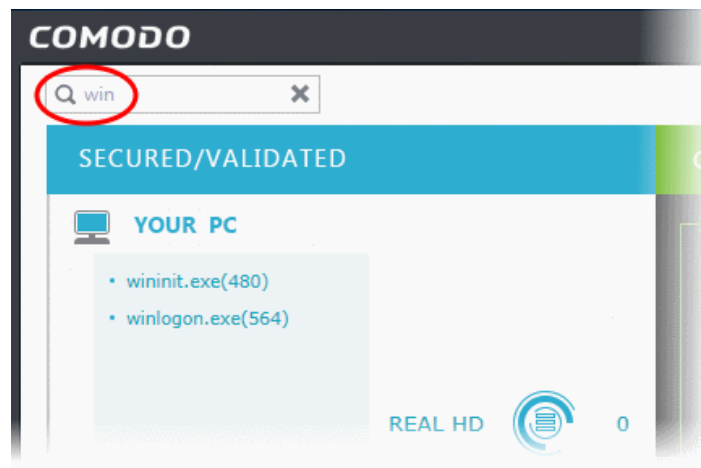
- Click 'Switch to Windows View'



- Enter password if configured in 'Advanced Settings' > 'Containment' > 'Virtual Desktop' > 'Request password when exiting Virtual Desktop'
- Click 'OK'

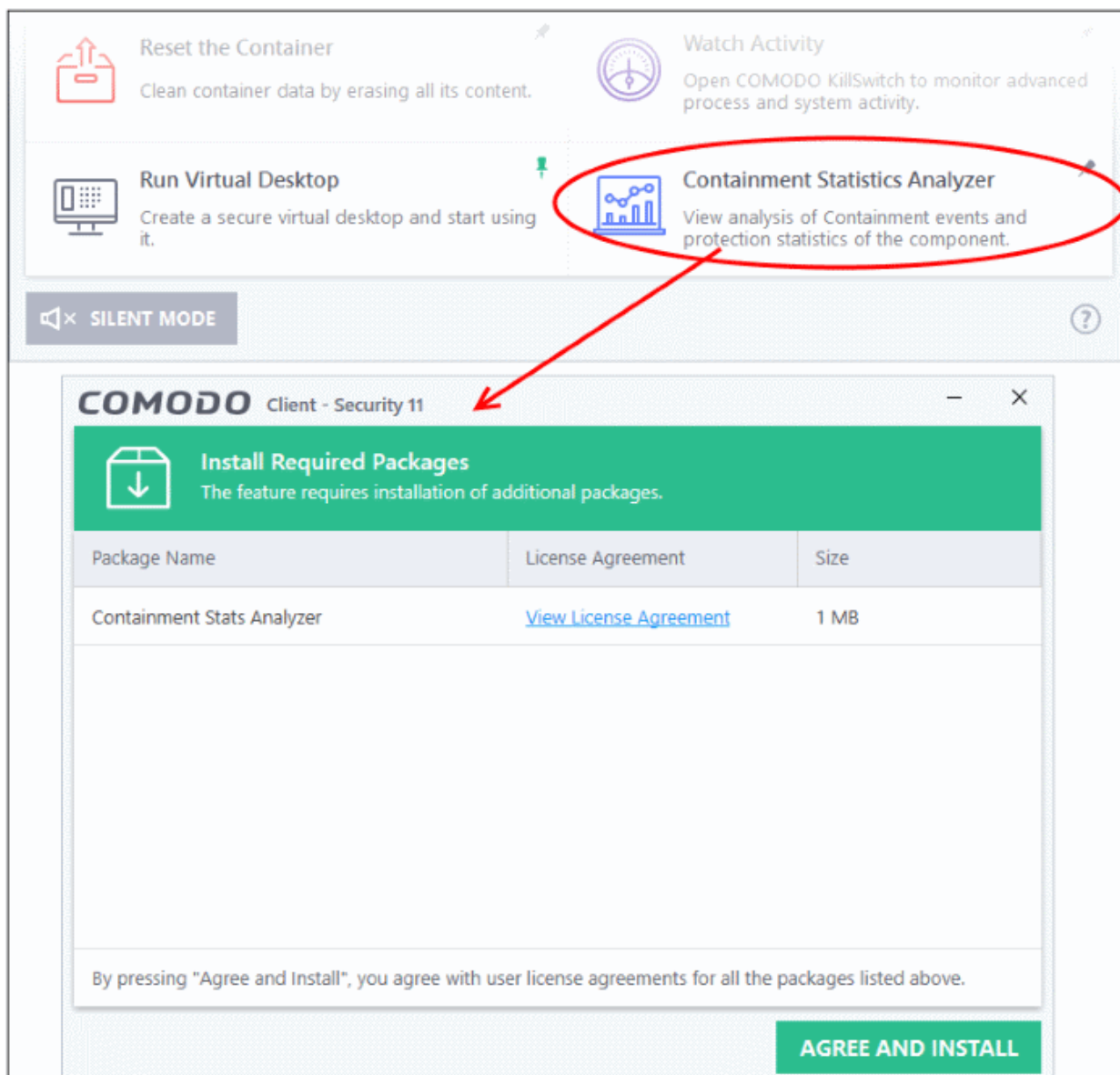
4.6. Containment Statistics Analyzer

- Click 'Tasks' > 'Containment Tasks' > 'Containment Statistics Analyzer' in the CCS interface.
- The 'Containment Statistics Analyzer' area allows you to view data about activities of processes running in the container.
- You can view the statistics of each process name by clicking on the process name folder
- You can search for specific file processes using the search option at the top-left of the application.



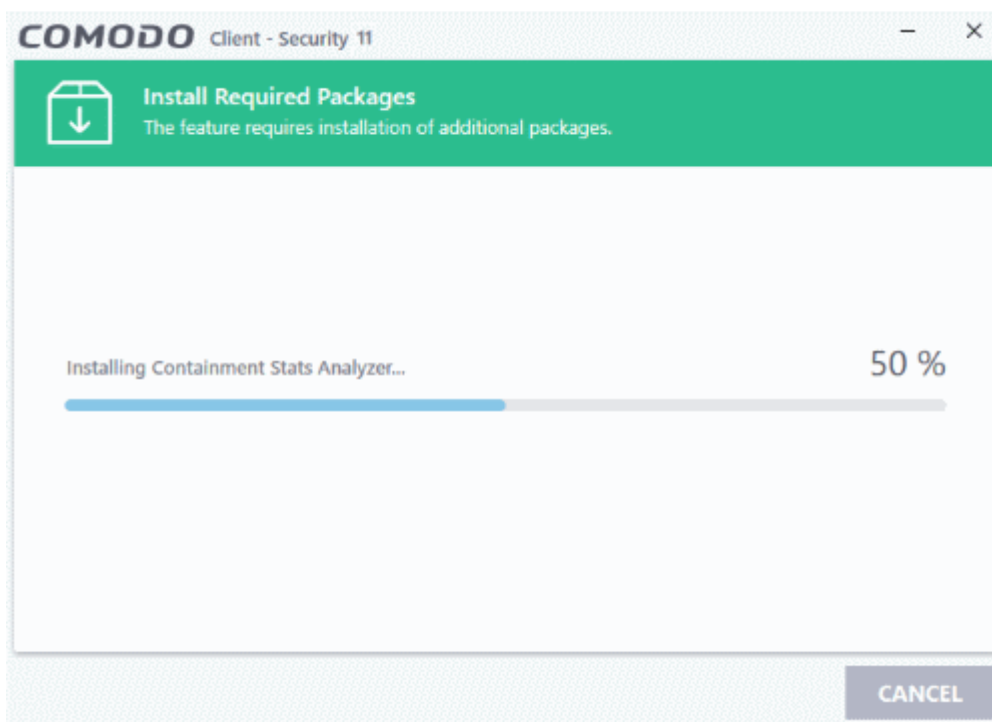
To install the application:

- Click 'Tasks' > 'Containment Tasks' > 'Containment Statistics Analyzer' in the CCS interface.

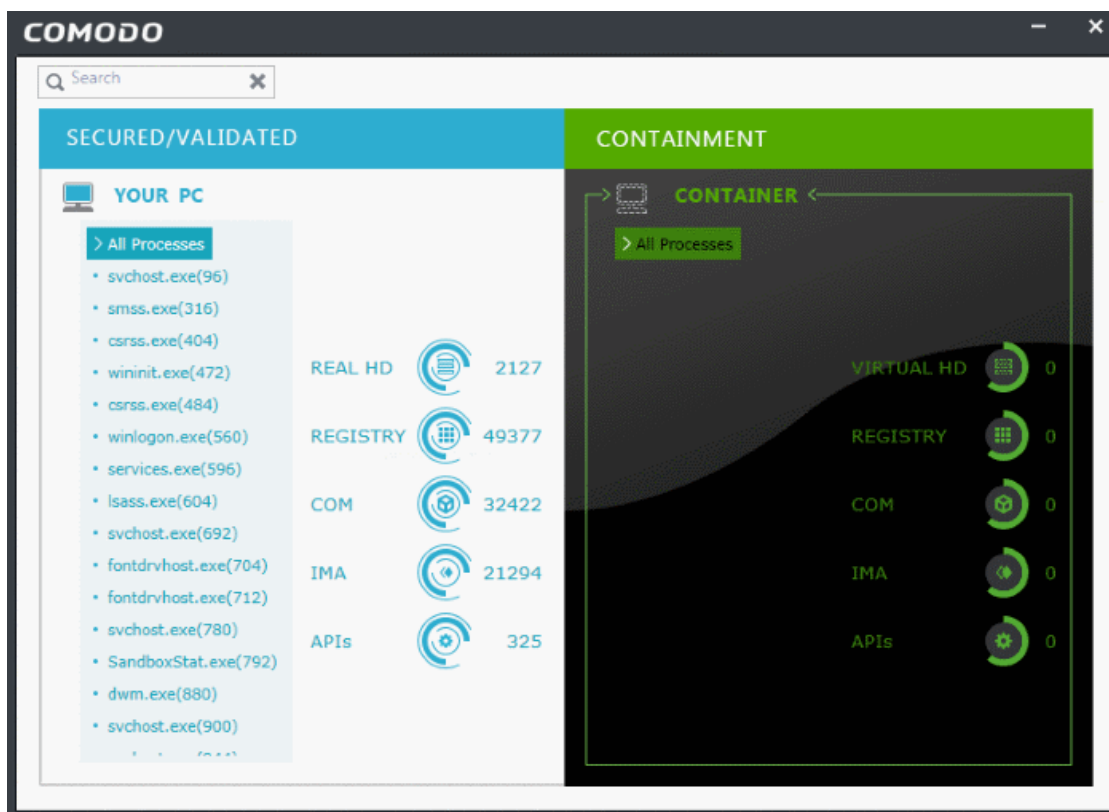


The 'license Agreement' screen will open:

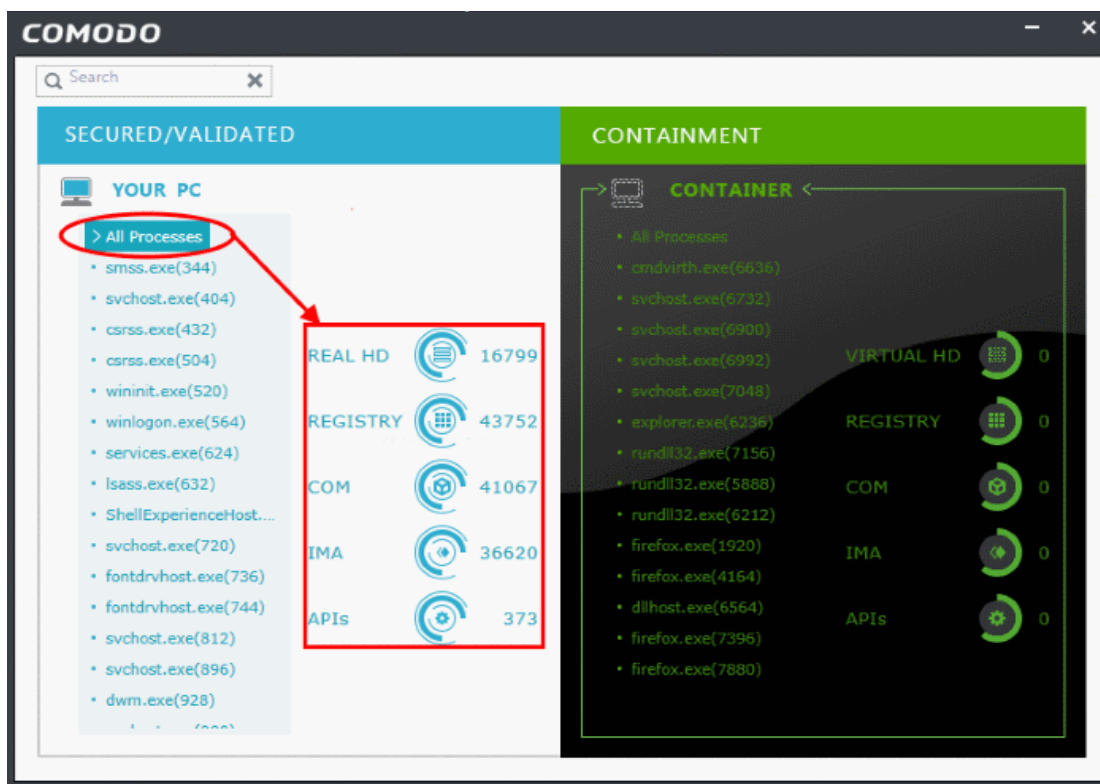
- View the terms and conditions and click 'AGREE AND INSTALL'



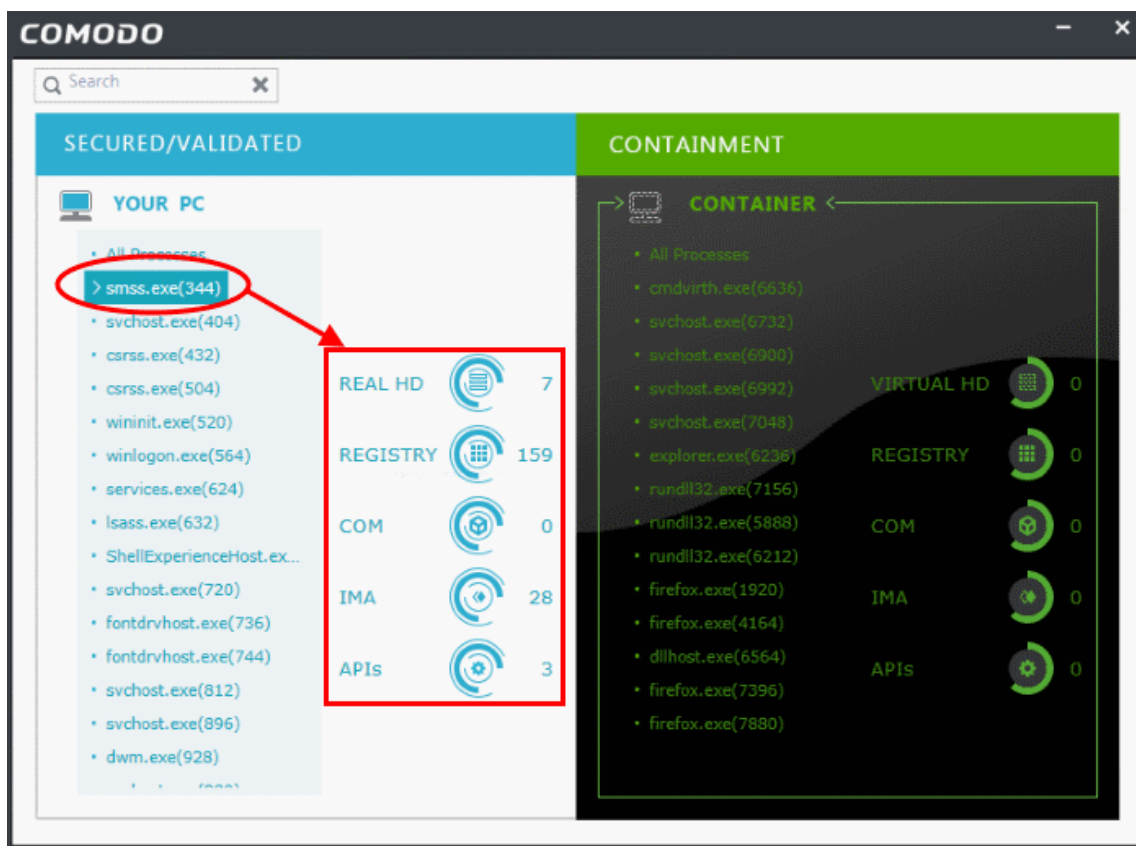
The app installs and displays the containment statistics screen:



- The tool shows processes running in the container and outside of the container (Your PC). You can view five major components through which each process runs.
- Click 'All Processes' to view all running processes.

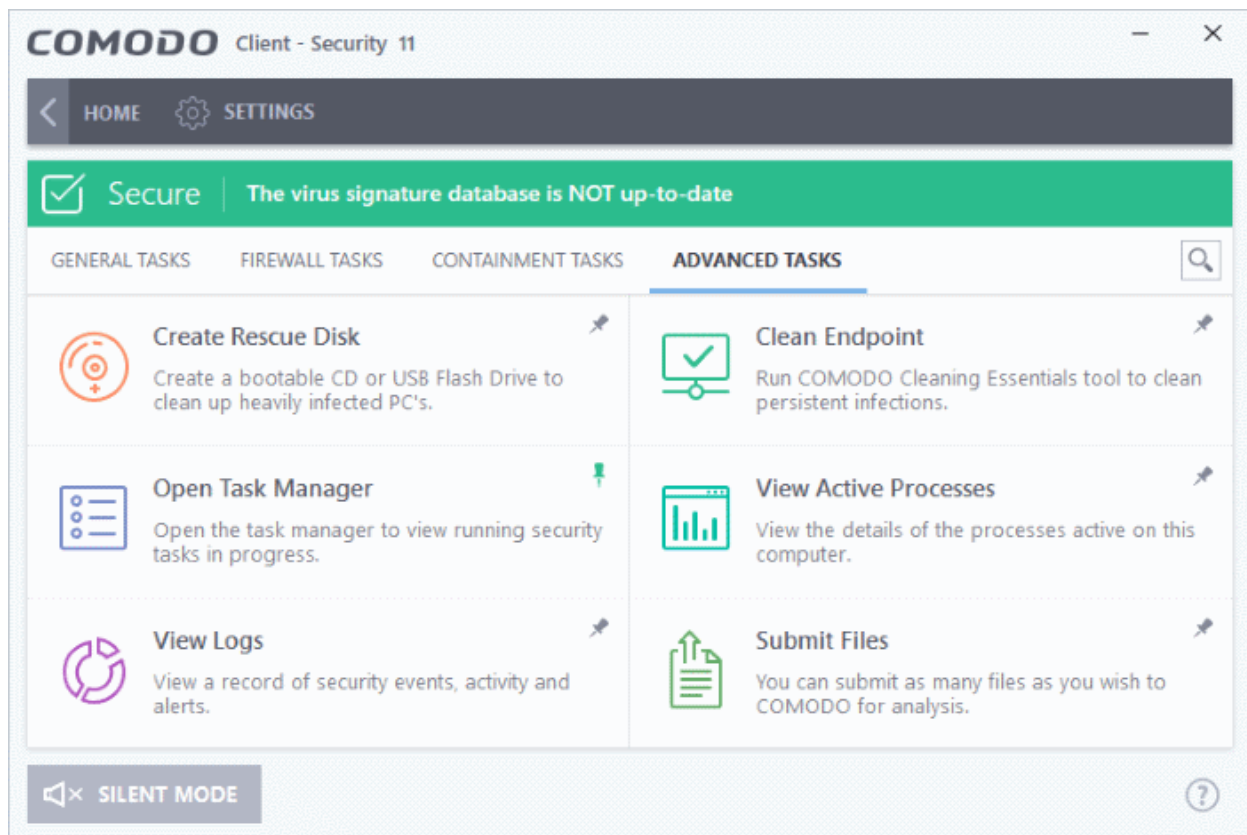


- Click a process name to view the number of its processes accessing the five components shown on the right.



5. Advanced Tasks - Introduction

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



The following links explain more about each topic:

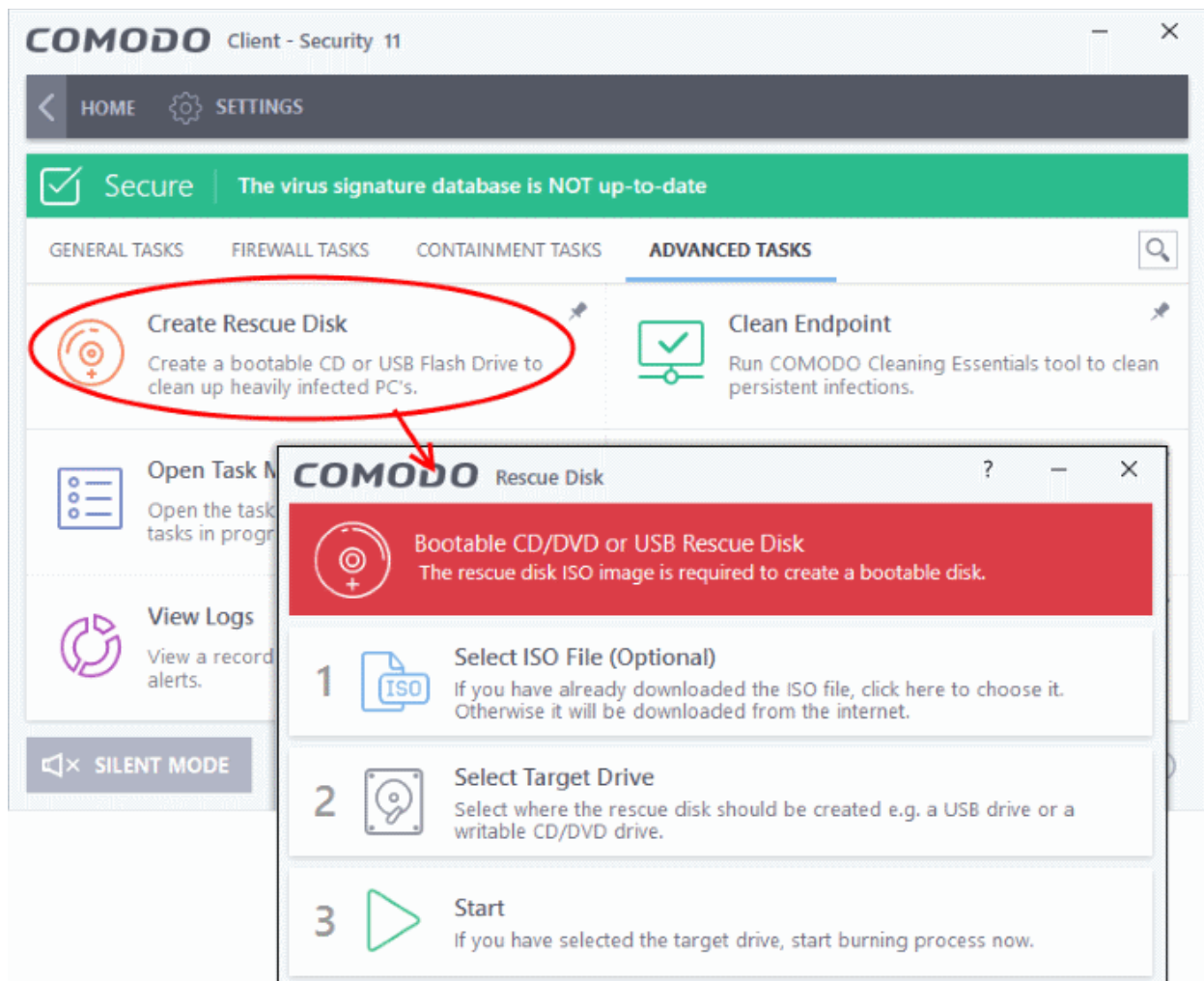
- **Create Rescue Disk** - Burn a bootable ISO that to run virus scans in pre-boot environments
- **Task Manager** - Stop, pause and resume currently running CCS tasks like antivirus scans and updates
- **Clean Endpoint** - Deploy Comodo Cleaning Essentials to delete persistent malware from your PC
- **View Active Process List** - View processes which are currently running on your PC. Clicking the 'More' button will open Comodo **KillSwitch**, or present you with the opportunity to install KillSwitch if you do not have it installed.
- **CCS Logs** - Log of Antivirus, Firewall, VirusScope, Containment and HIPS events
- **Submit Files** - Submit unknown/suspicious files to Comodo for analysis

5.1. Create a Rescue Disk

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

- CRD can eliminate infections that are preventing Windows from booting in the first place.
- It is useful for removing malware which has embedded itself so deeply that regular AV software cannot remove it.
- CRD contains tools to explore files in your hard drive, take screen-shots and browse web pages.

- Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk' to download and burn the CRD ISO to a CD/DVD, USB or other drive. See [Downloading and Burning Comodo Rescue Disk](#) for a walk-through of this process.

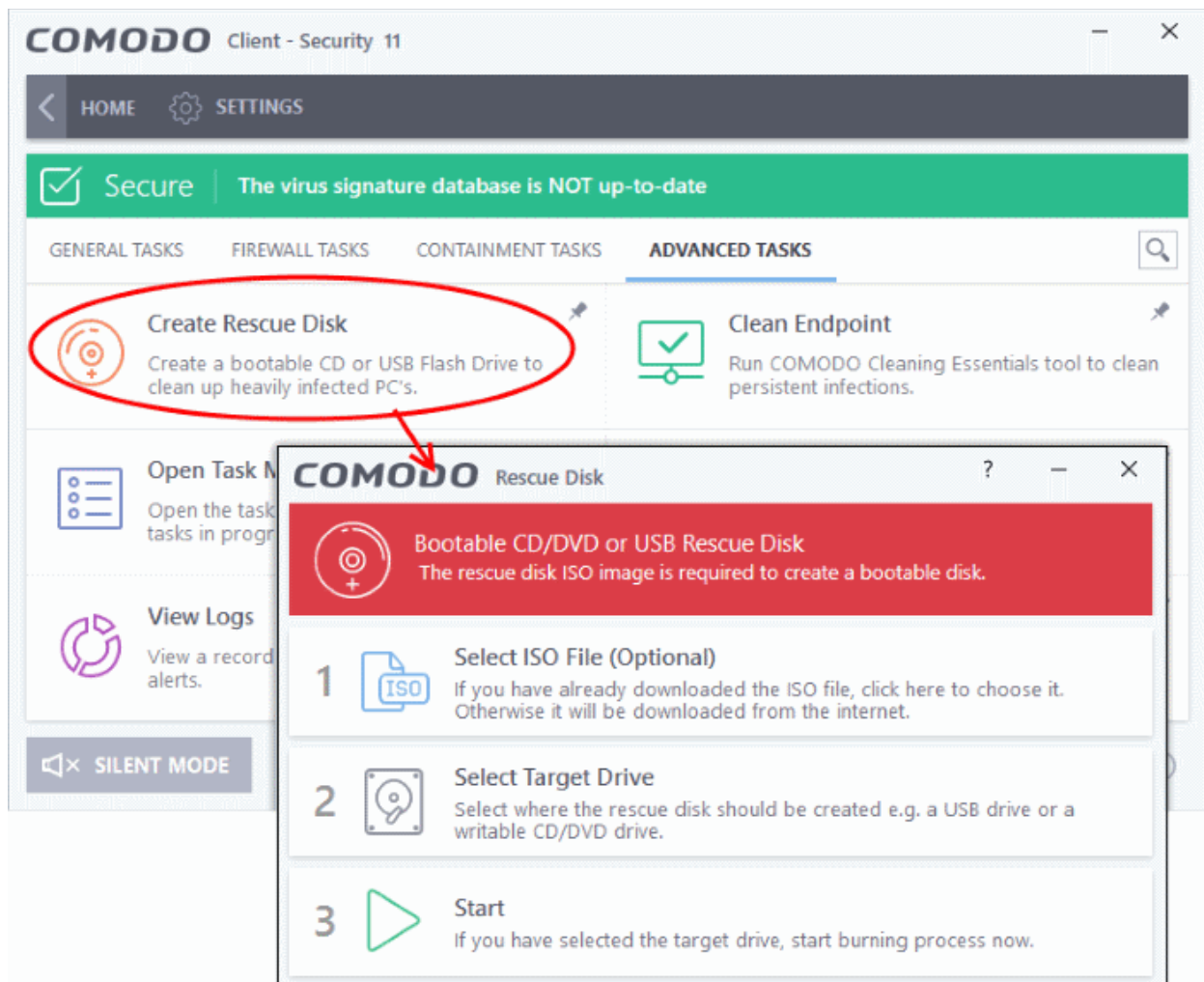


After you have burned the ISO, boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

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

5.1.1. Download and Burn Comodo Rescue Disk

- Click 'Create Rescue Disk' in the 'Advanced Tasks' interface to open the rescue disk wizard:



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

Step 1- Select the ISO file

Optional.

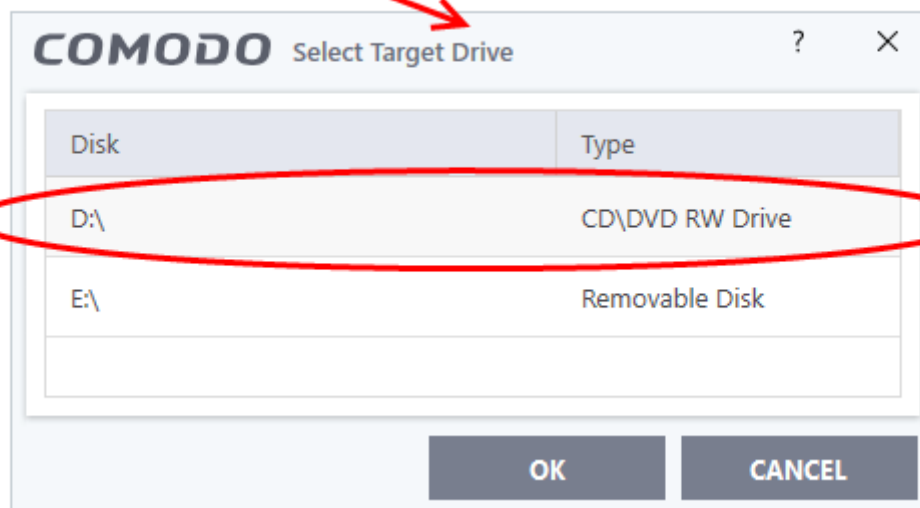
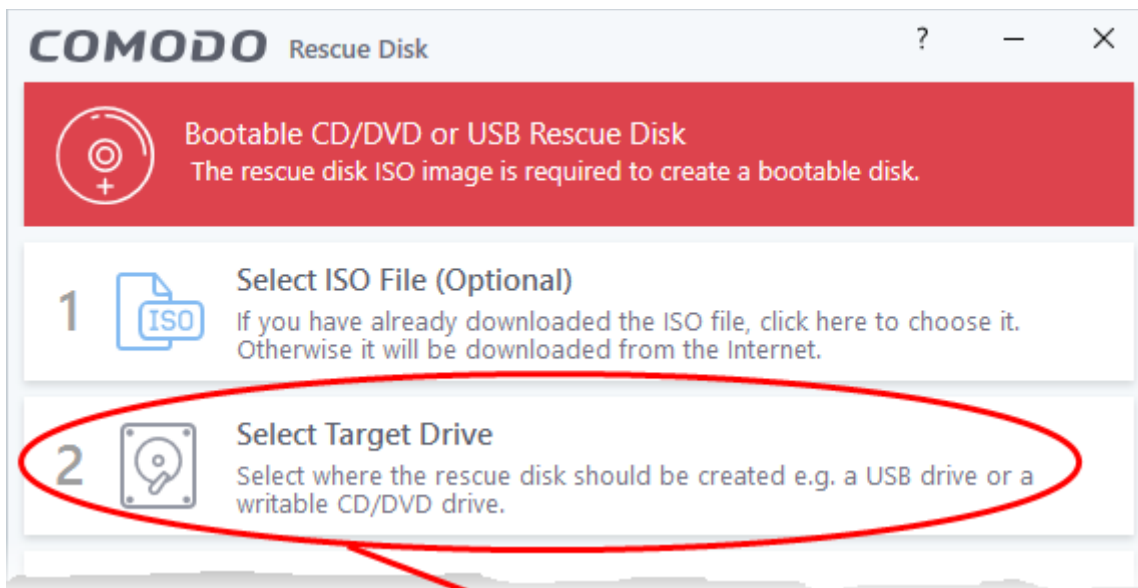
- If you have already downloaded the rescue disk ISO from Comodo, browse the location on your hard-drive where it is stored and select it
- Ignore this step if you haven't downloaded the ISO. It will be downloaded automatically prior to execution of Step 3 - Burning the Rescue Disk

Step 2 - Select target drive

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

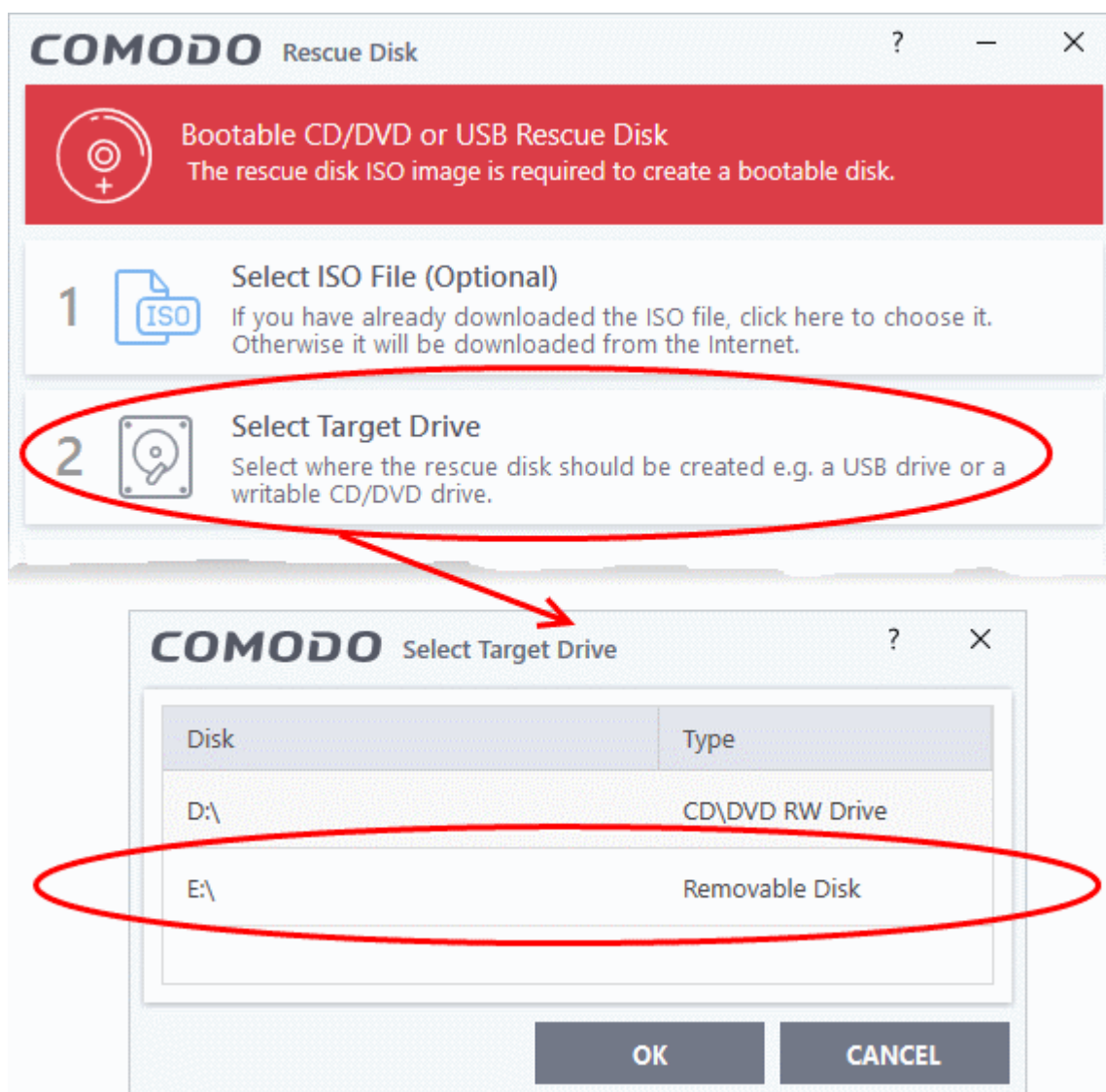
To burn the Rescue disk to a CD or a DVD

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



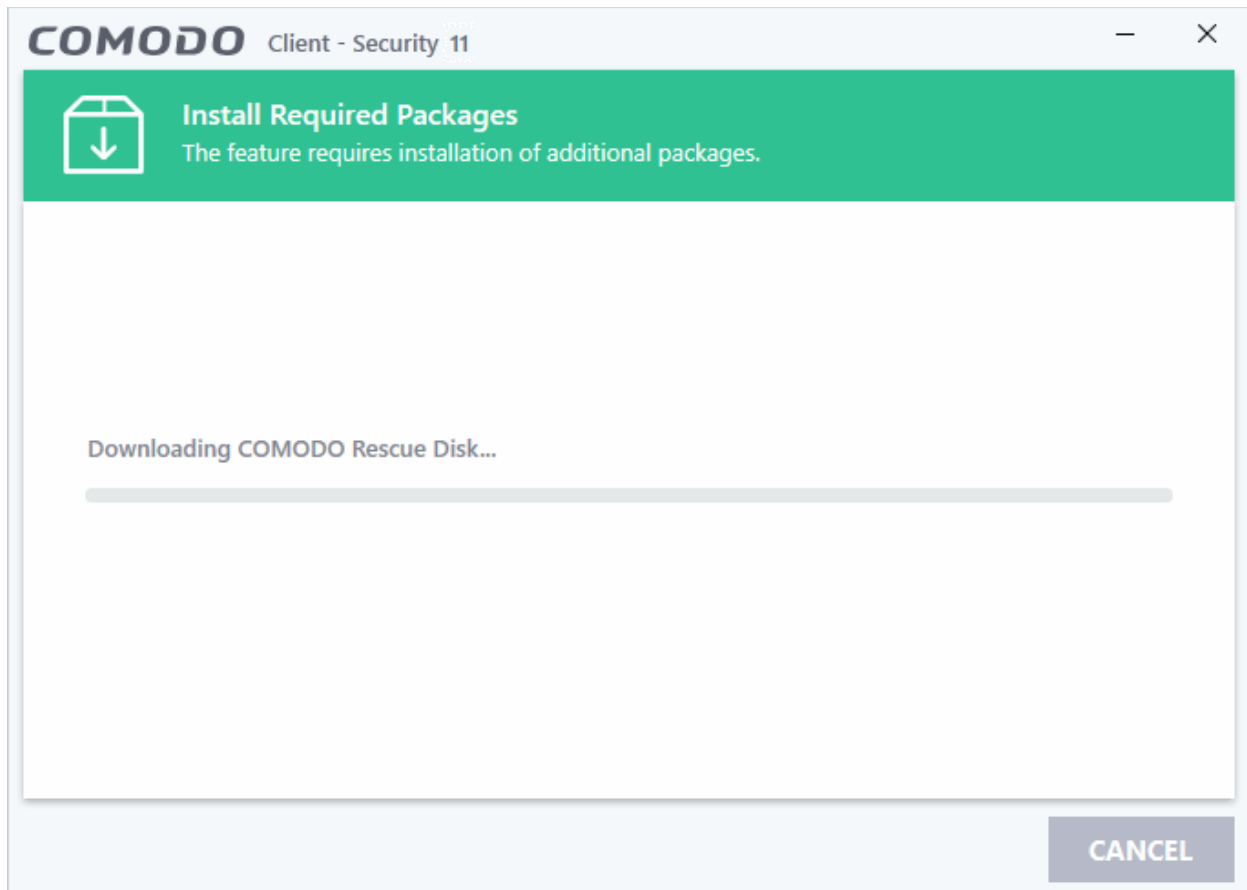
To burn the Rescue disk on a USB Drive

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

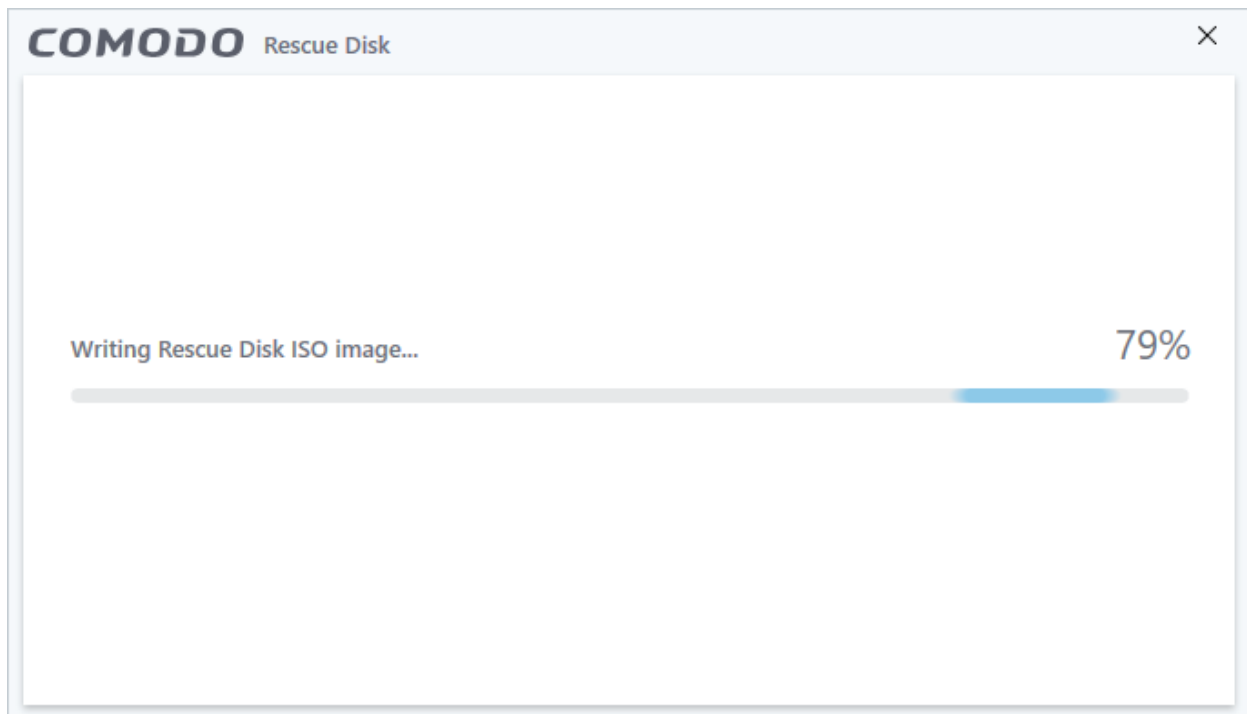


Step 3 - Burn the Rescue Disk

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

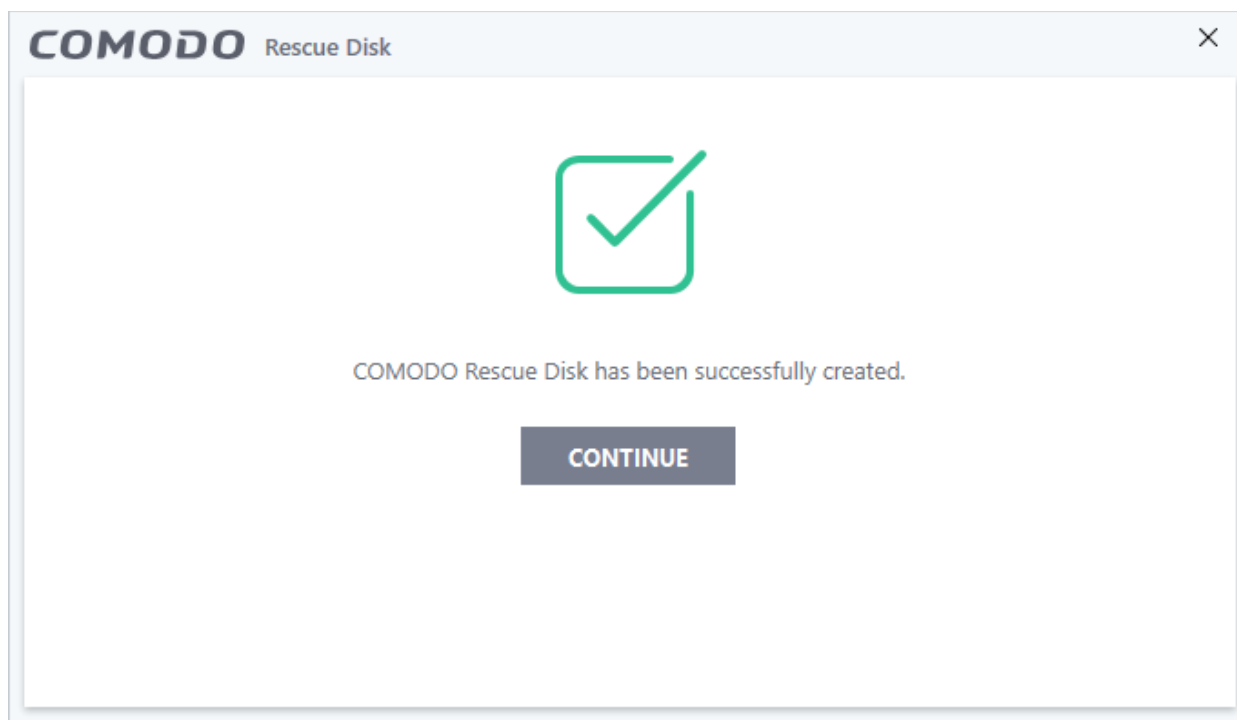


Once downloaded, the creation of rescue disk will start.



On completion, 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 CCS interface

5.2. Remove Deeply Hidden Malware

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

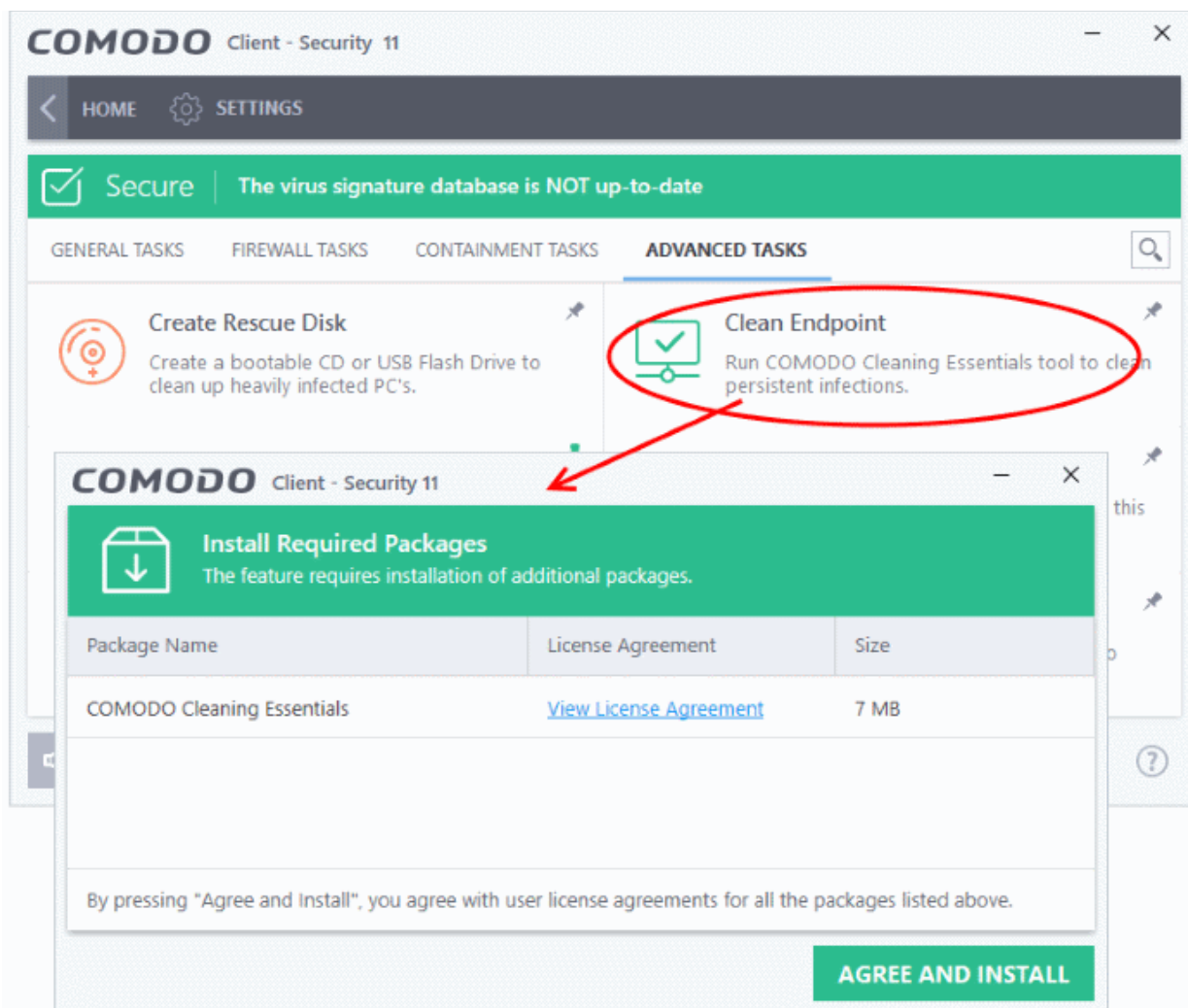
Major features include:

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

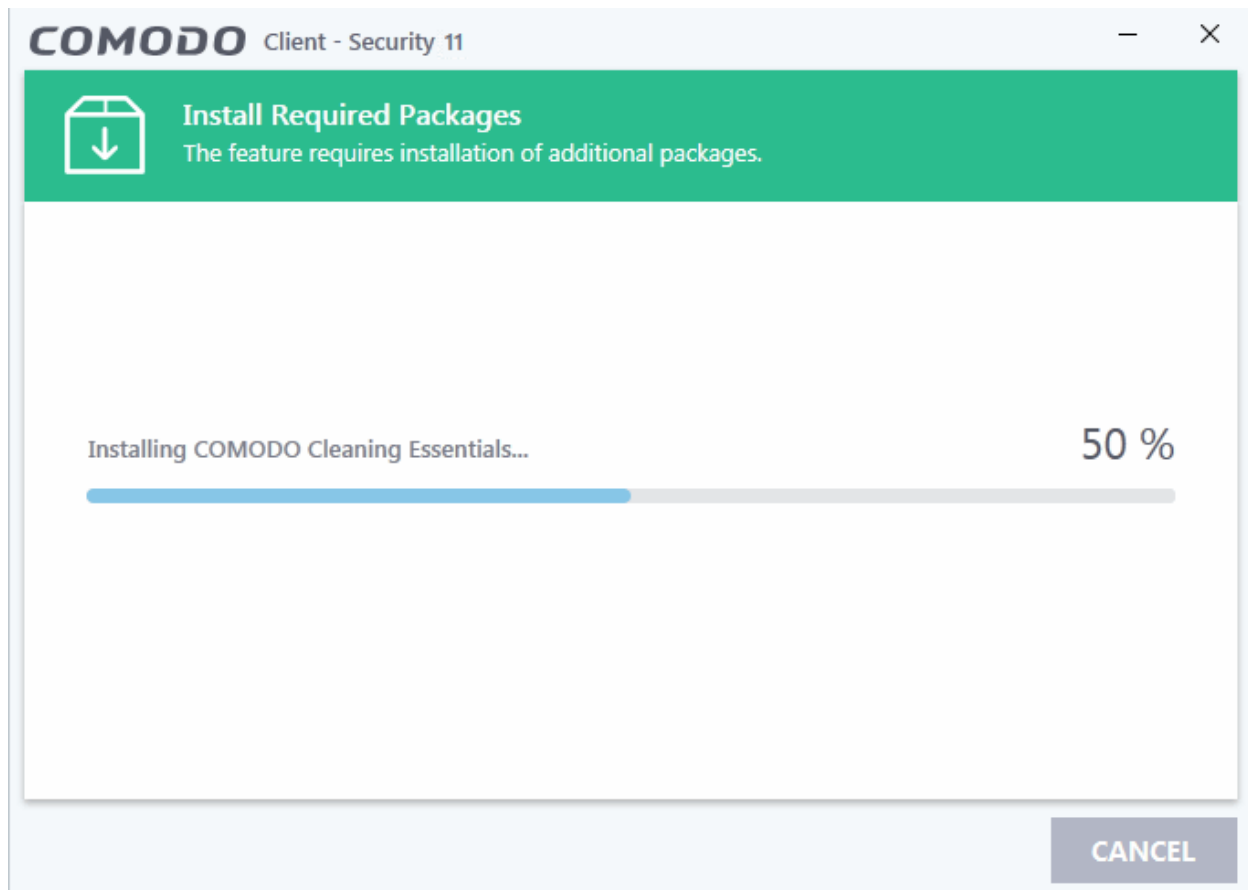
CCE enables home users to quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.

Comodo Cleaning Essentials can be directly accessed by clicking the 'Clean Endpoint' button in the 'Advanced Tasks' interface.

- If you do not have CCE installed, click the 'Clean Endpoint' button to download and install Comodo Cleaning Essentials
- Once installed, click this button in future to open the CCE interface



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



After installation, the Comodo Cleaning Essentials interface will open:



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

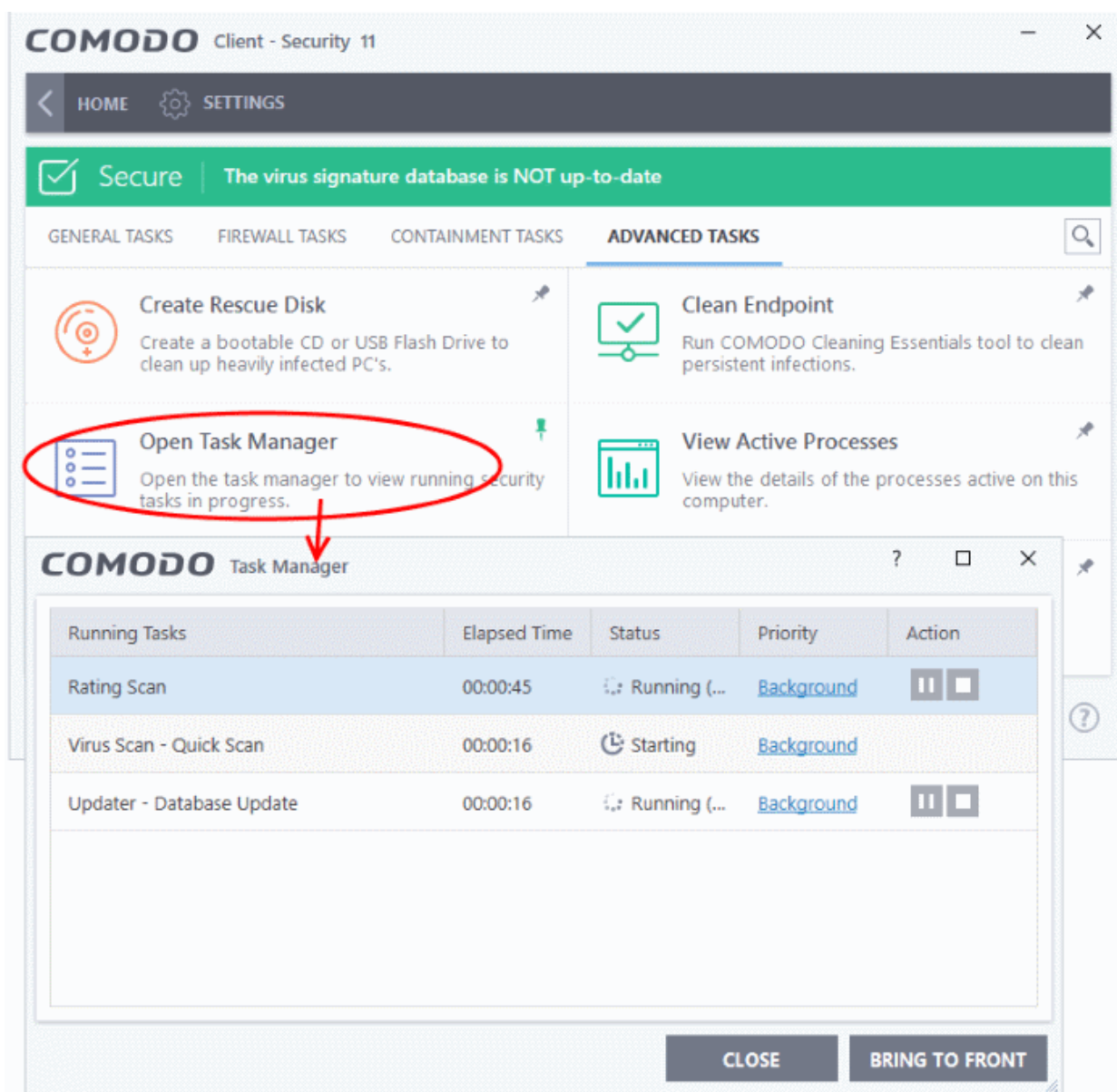
5.3. Manage CCS Tasks

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

To open and manage the task manager

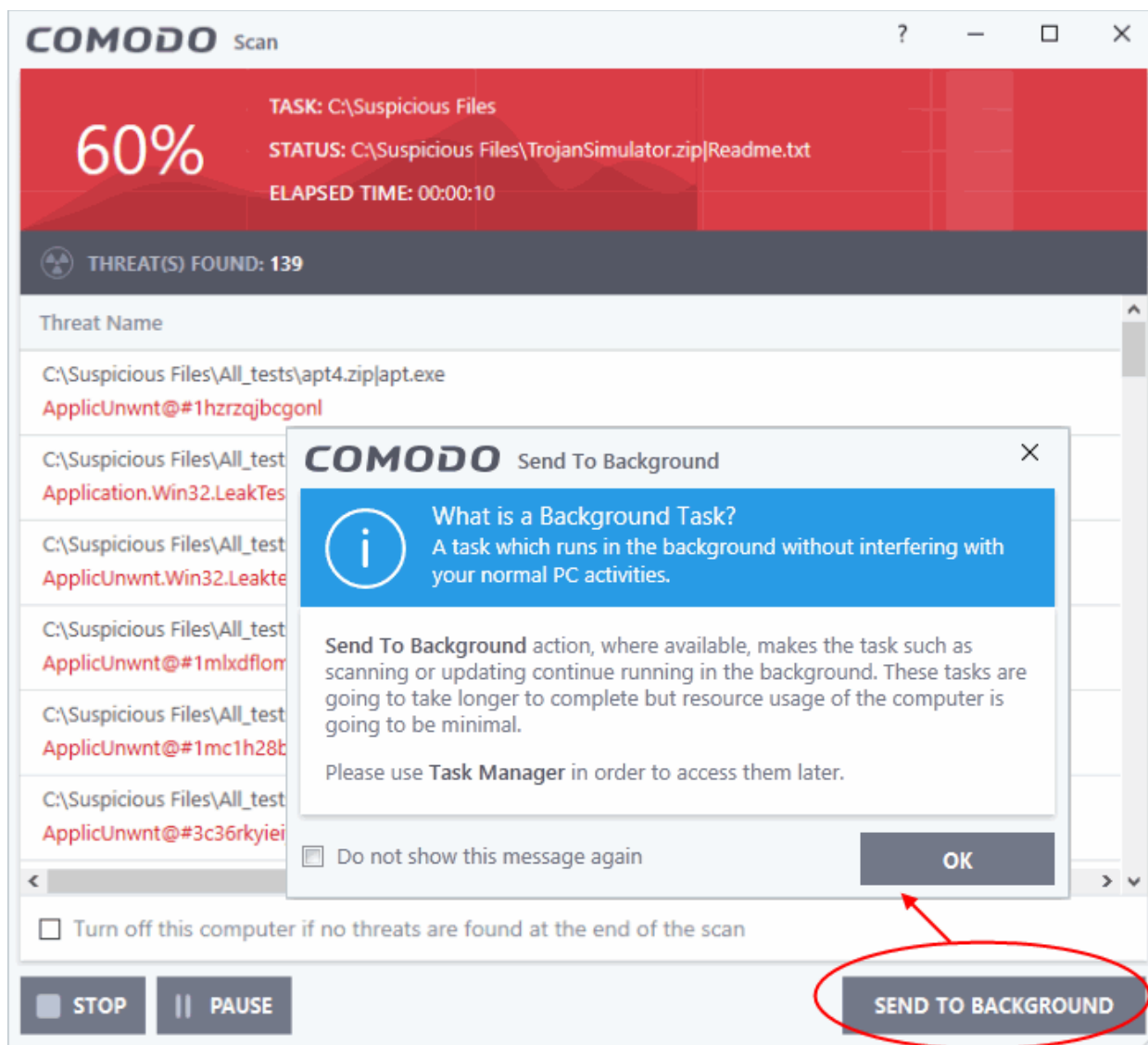
- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' tab
- Click 'Open Task Manager'

The 'Task Manager' dialog will open:



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

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



The following options are available in the 'Task Manager':

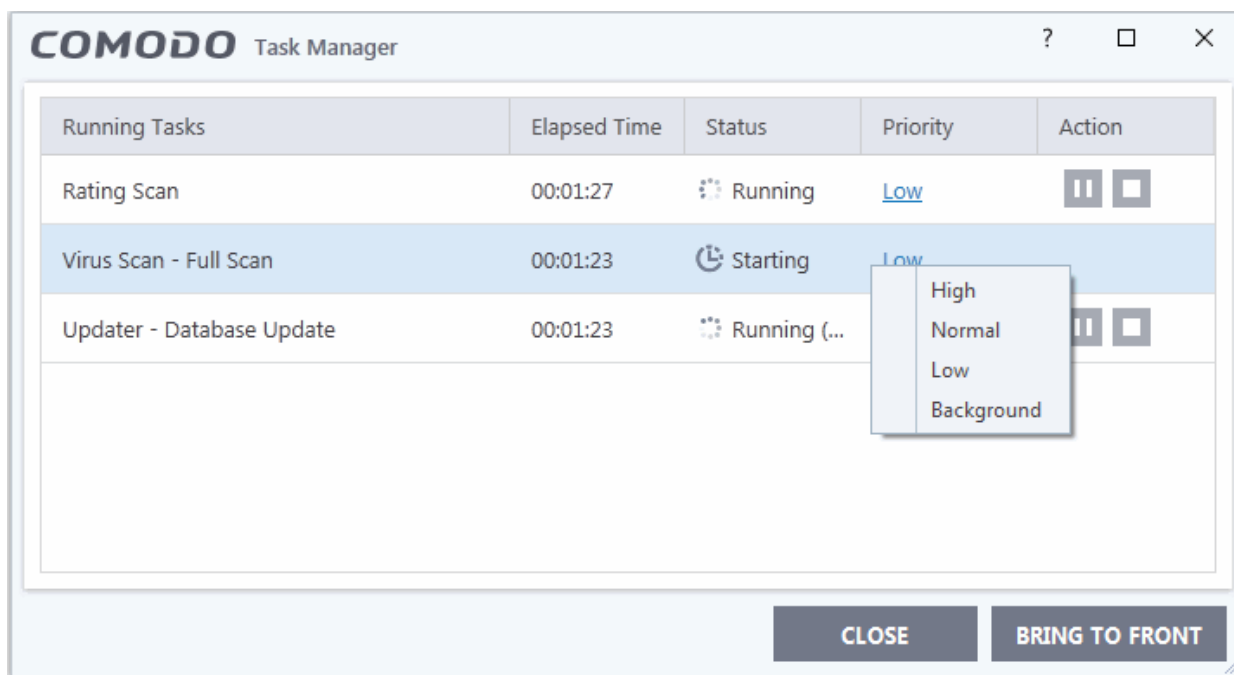
- **Reassign priorities to the tasks**
- **Pause/Resume or Stop a running task**
- **Bring a selected task to foreground**

Reassigning Priorities for a task:

The current priority assigned for each task will be shown in the 'Priority' column.

To change the priority for a task

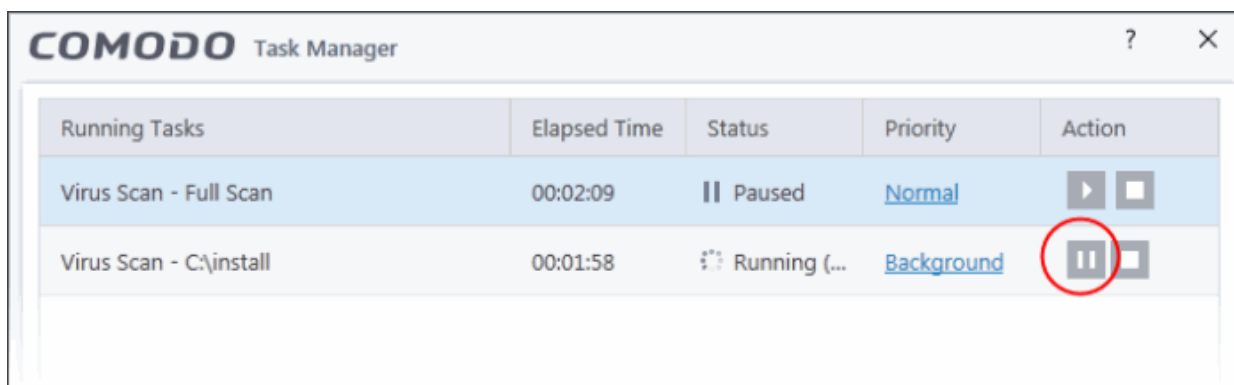
- Click the current priority and select the priority you want to assign from the options



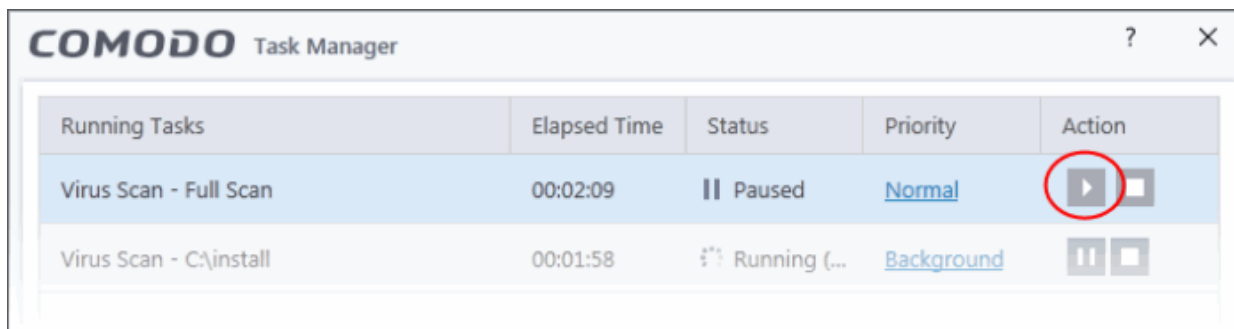
Pausing/Resuming or Stopping running tasks

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

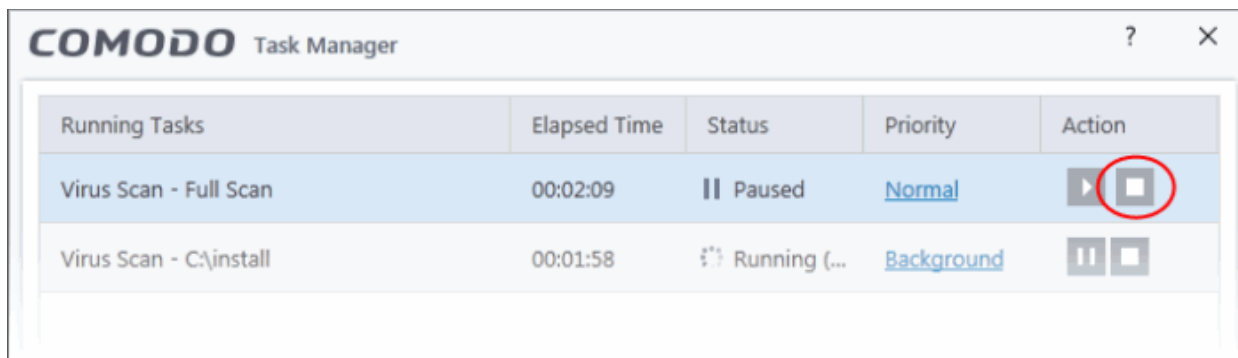
- To pause a running task, click the 'Pause' button



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

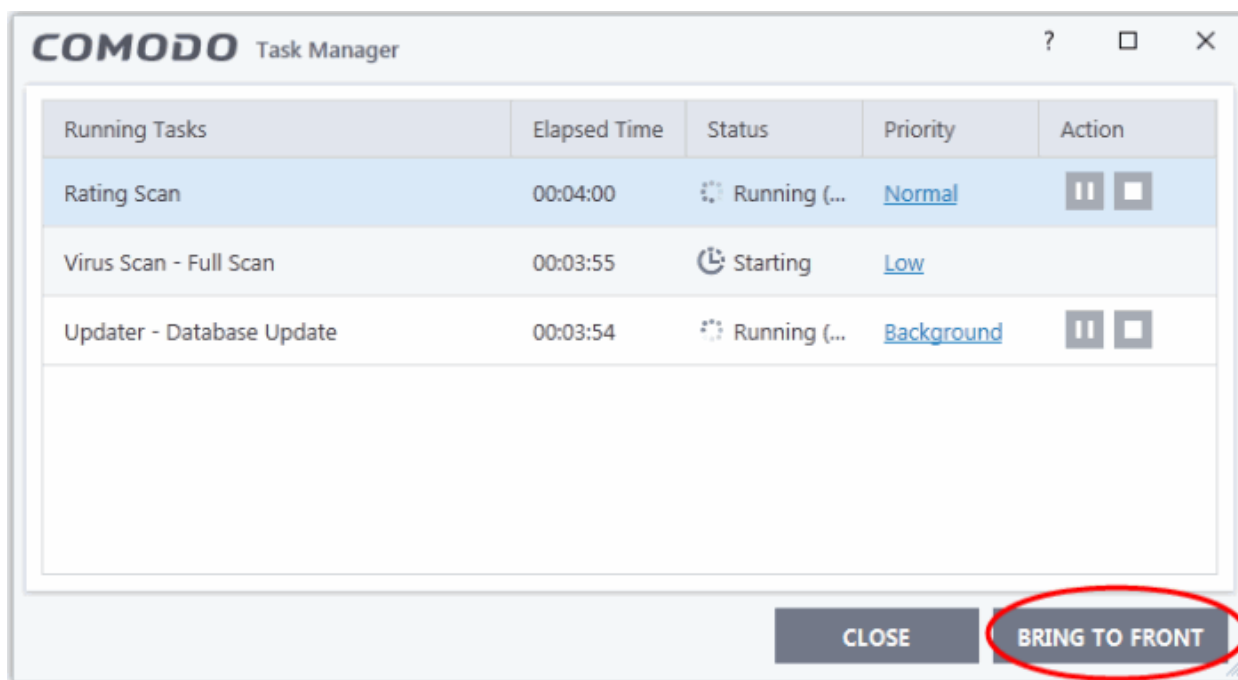


- To stop a running task, click the 'Stop' button



Bringing a running task to foreground

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



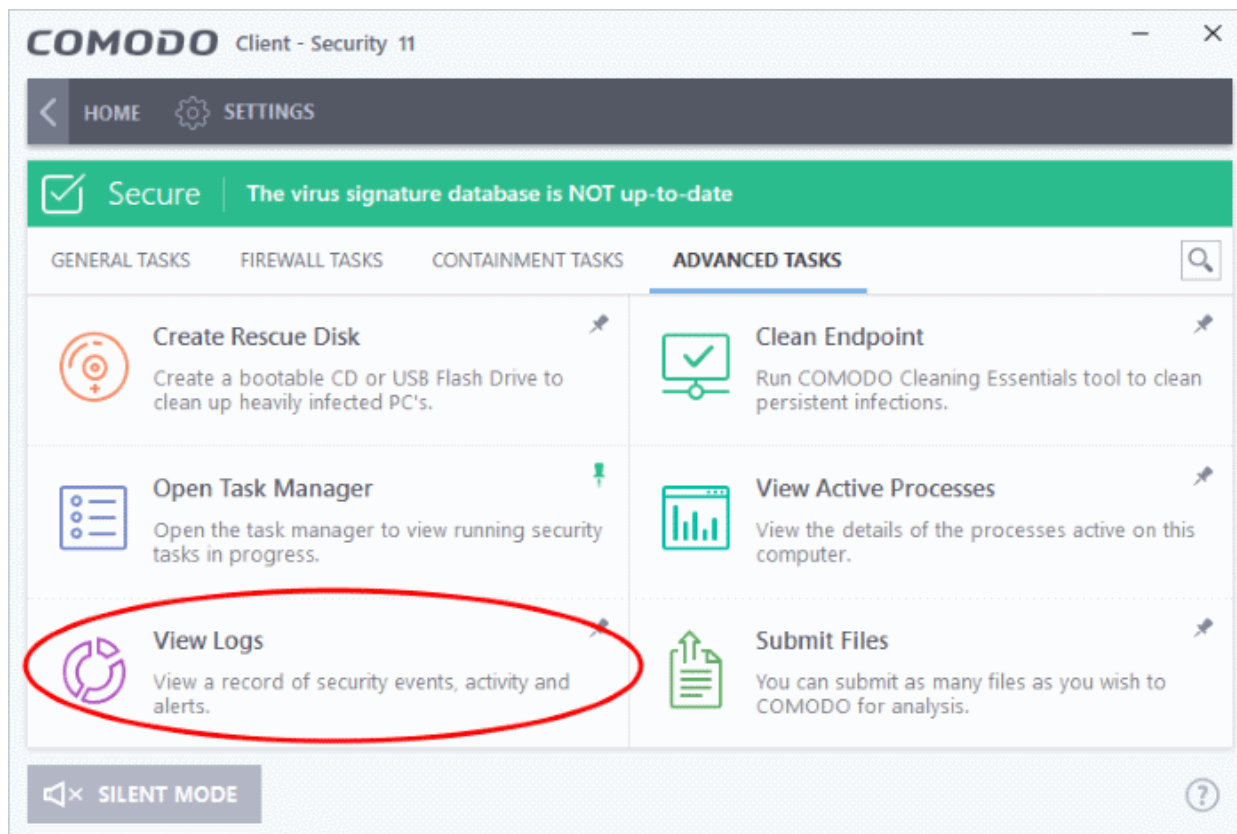
The progress window of the task will be displayed. When the task is complete, the results window will be displayed.

5.4. View CCS Logs

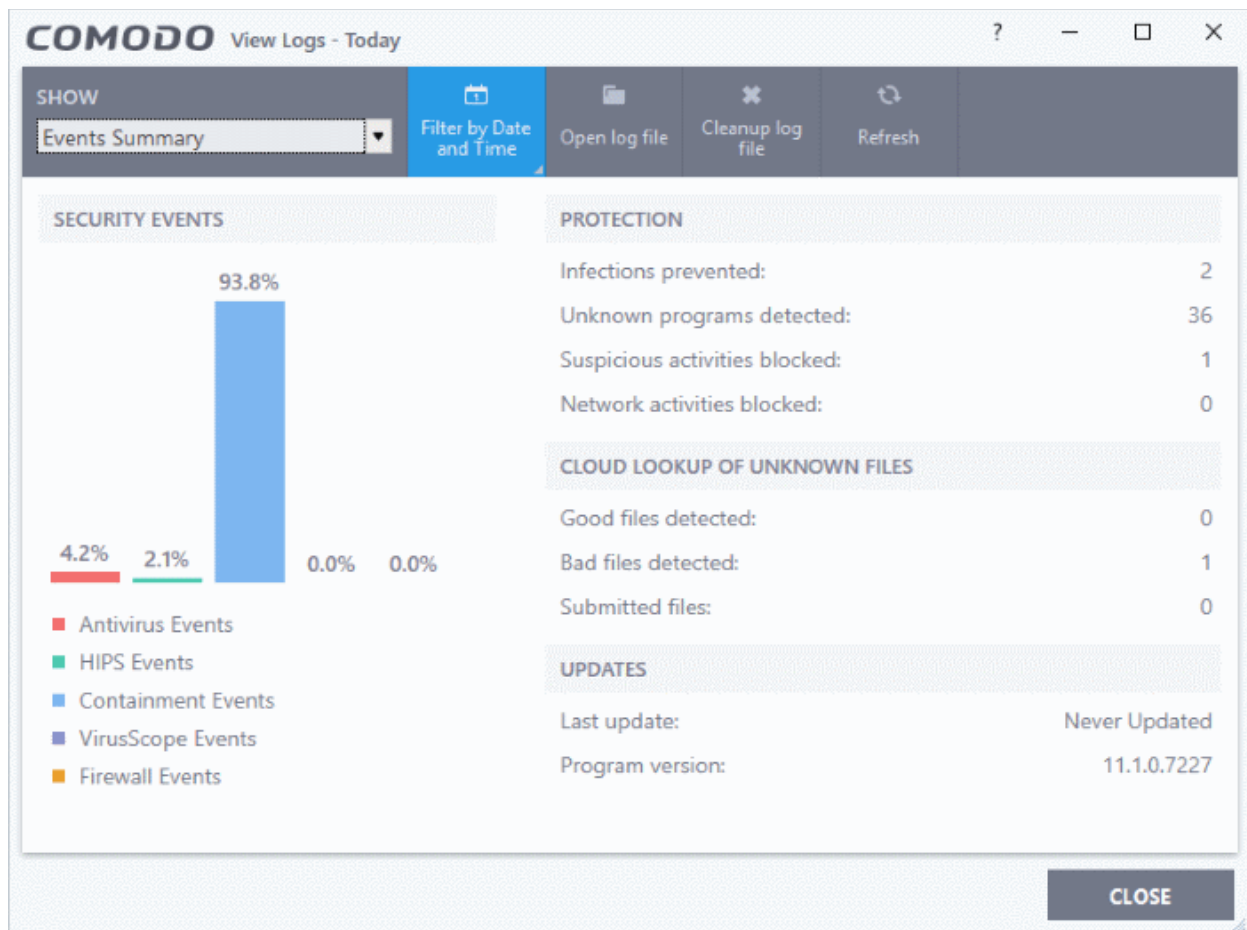
CCS keeps logs of antivirus, firewall, HIPS, Containment and other events. These can be viewed at anytime from the 'Log Viewer' module.

To access the 'Log Viewer' module

- Click 'Tasks' at the top-left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs':



The 'View Logs' interface will open, showing a summary of CCS events:



- The graph on the left shows the percentage of events generated by each module.
- The right side shows a summary of events, the results of look-ups on unknown files, and product update information
- Use the drop-down at top-left to change which events are shown.
- To open a saved log file, click 'Open log file' button beside the drop-down and browse to the location where the CCS log file is stored
- To clear the logs, click the 'Cleanup log file' button
- To refresh the logs, click the 'Refresh' button

The following sections contain more details about each type of log:

'Logs per Module':

- **Antivirus**
- **VirusScope**
- **Firewall**
- **HIPS**
- **Containment**
- **Device Control**
- **Autoruns**
- **Alerts Displayed**
- **Tasks Launched**

- **File List Settings Changes**
- **Vendors List Changes**
- **Configuration Changes**

5.4.1. Antivirus Logs

- Comodo Antivirus documents the results of all actions it performs in extensive but easy to understand logs.
- A detailed scan report contains statistics on all scanned objects. The report also include settings used for each task and a history of actions performed on individual files.
- Reports are also generated during real-time protection, and after update to the database or application.

To view 'Antivirus' Logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs':
- Select 'Antivirus Events' from the 'Show' drop-down:

Date & ...	Location	Malware Name	Action	Status	Alert	Activities
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Ignore	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Quarantine	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Ignore	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Ignore	Success	Related alert	
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Quarantine	Success		
11/11/20...	C:\Suspicious File...	Application.Win32.Le...	Quarantine	Success		
11/11/20...	C:\Program Files ...	Malware@#3ri4ye99...	Quarantine	Success	Related alert	
11/11/20...	C:\Program Files ...	Malware@#2nm567u...	Quarantine	Success	Related alert	
11/11/20...	C:\Program Files ...	Malware@#1i04f6cq...	Quarantine	Success	Related alert	

Column Descriptions

1. **Date & Time** - The precise date and time of the event.
2. **Location** - The installation location of the application detected as a threat.
3. **Malware Name** - Name of the malware detected at that event.
4. **Action** - Action taken against the malware through Antivirus.
5. **Status** - The status of the action taken. It can be either 'Success' or 'Fail'.
6. **Alert** - The 'Related Alert' link opens the 'Alerts' interface of the Log Viewer and displays the details of the

alert defined during the event.

7. **Activities** - Details of activities executed by the processes running by the infected application.
 - **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
 - **'Open log file'** - view a saved log file.
 - **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
 - **'Cleanup log file'** - Deletes all logs from all modules

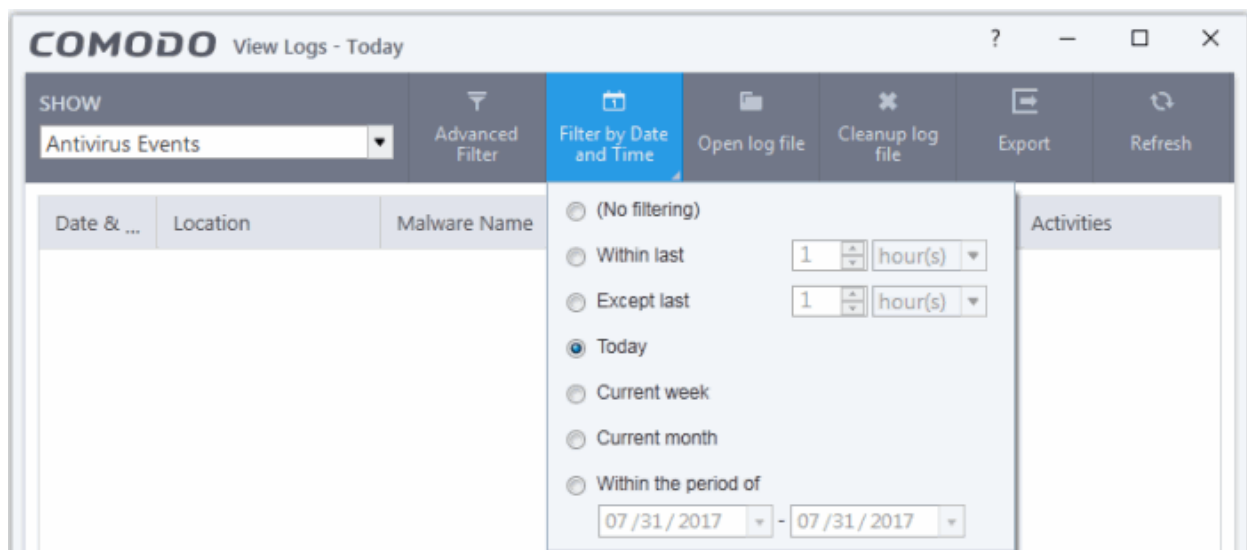
5.4.1.1. Filter Antivirus Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

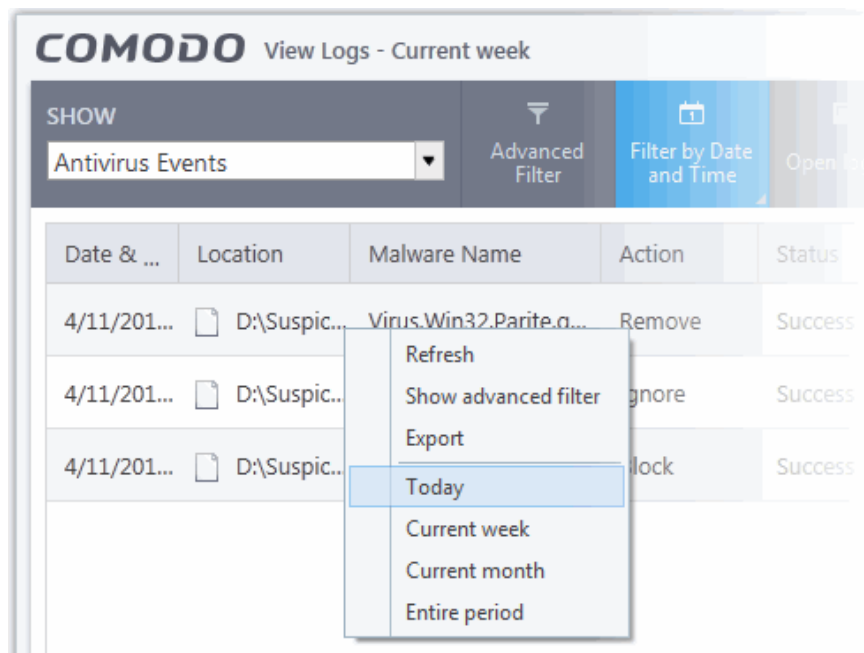
Preset Time Filters:

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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.

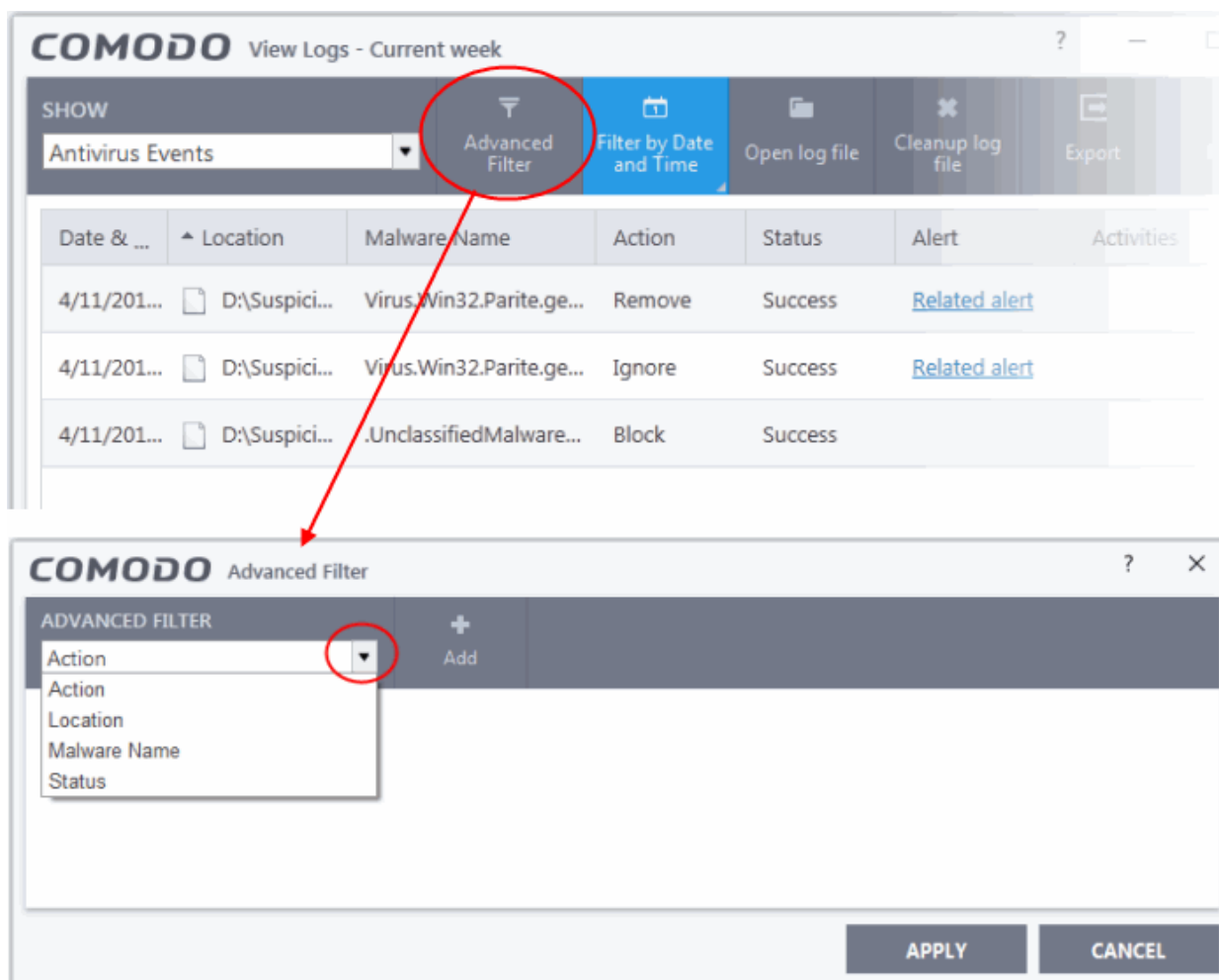


Having chosen a **preset time filter**, you can further refine which events are shown by using the following additional parameters:

- **Action** - Events according to the response (or action taken) by the antivirus
- **Location** - Displays only events logged from a specific location
- **Malware Name** - Displays only those events that reference a specific piece of malware
- **Status** - Show events according to whether the logged action was successful or not. Status options are 'Success' or 'Fail'.

To configure Advanced Filters for Antivirus events

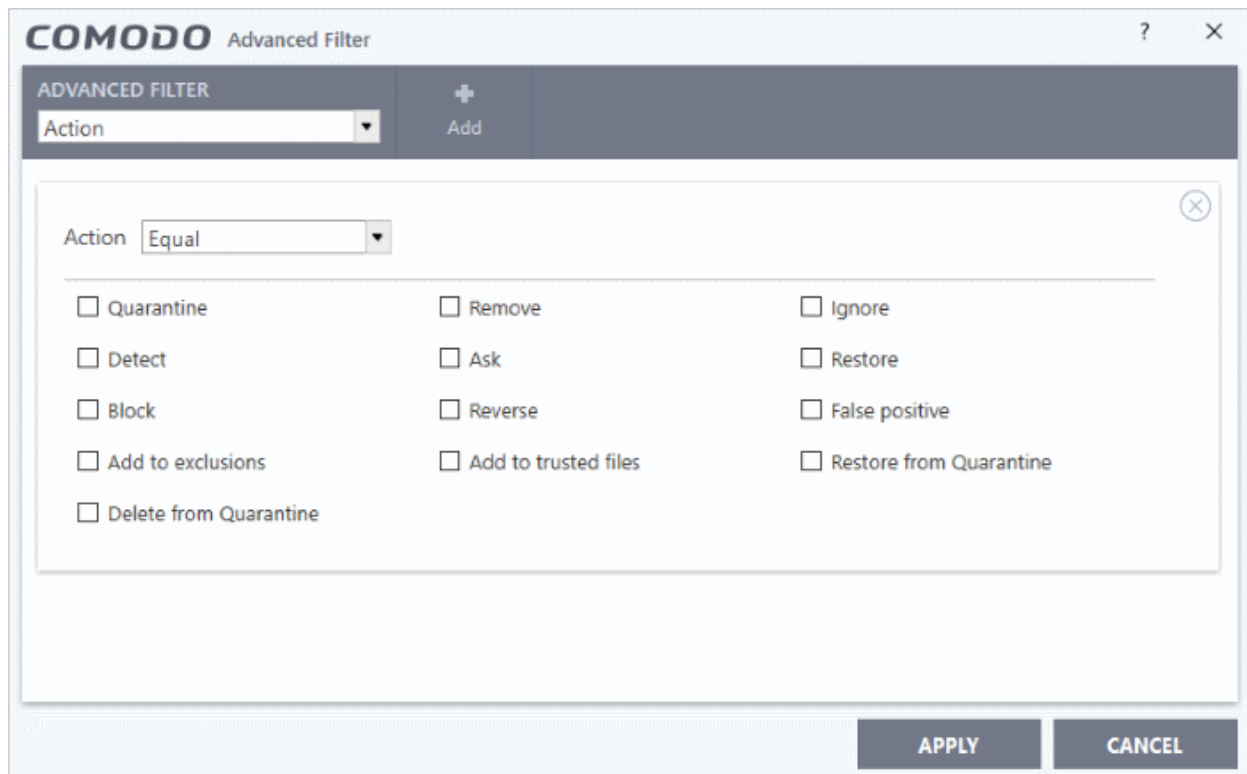
- Click the 'Advanced Filter' button from the title bar or right click inside the log viewer module and choose 'Advanced filter' from the context sensitive menu. The 'Advanced Filter' interface for AV events will open.
- Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



There are four categories of filters you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

- i. **Action:** The 'Action' option allows you to filter logs based on the action taken by CCS against the detected threat. To filter logs by CCS action, select 'Action' from the drop-down then click 'Add':

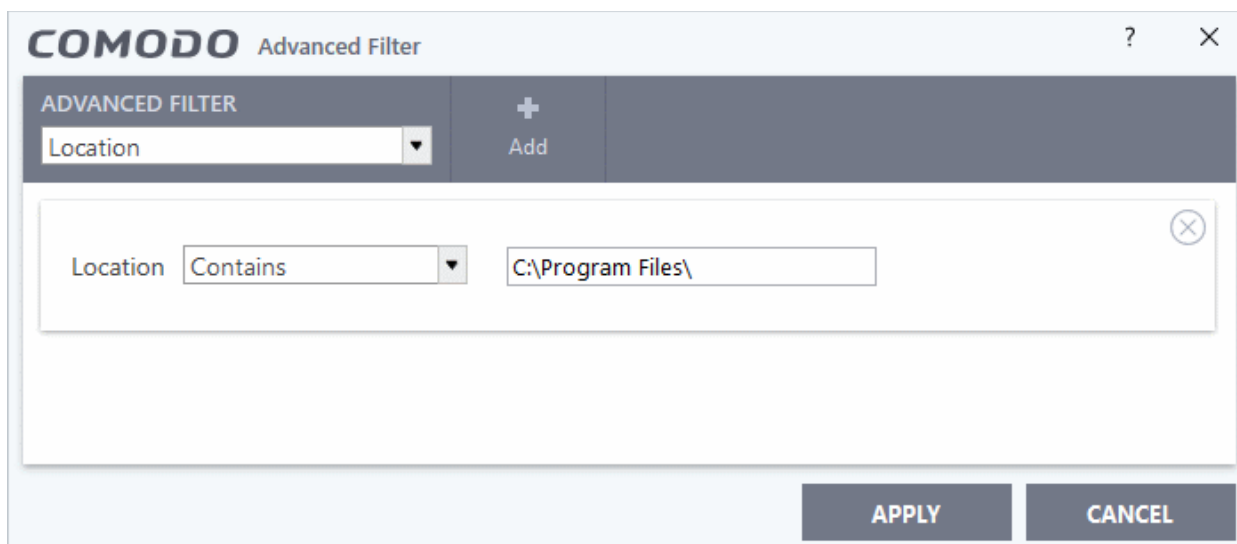


You should now choose the actions by which you want to filter the logs:

- a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
 - Quarantine: Displays events at which the user chose to quarantine a file
 - Remove: Displays events at which the user chose to delete the detected threat
 - Ignore: Displays events at which the user chose to ignore the detected threat
 - Detect: Displays events involving only the detection of malware
 - Ask: Displays events where an alert was shown to the user so they could choose an action against a piece of detected malware
 - Restore: Displays events at which quarantined applications were restored
 - Block: Displays event where suspicious applications were blocked
 - Reverse: Displays events where VirusScope reversed potentially malicious actions
 - False positive: Displays events where files flagged as threats by CCS were submitted to Comodo by the user as a false positive.
 - Add To exclusions: Displays events in which the user chose to add an item to antivirus exclusions
 - Add To trusted files: Displays events in which the user changed the file rating to 'Trusted'

For example, if you check the 'Quarantine' box then select 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

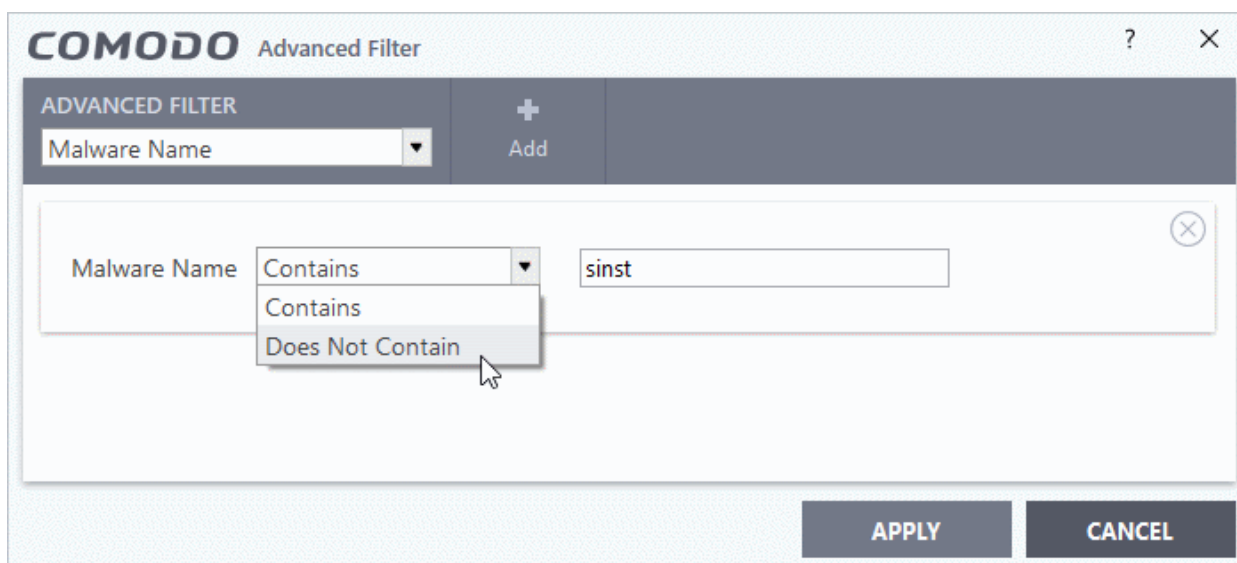
 - Restore from Quarantine: Displays events in which files were restored from quarantine
 - Delete from Quarantine: Displays events in which files were deleted from quarantine
- ii. **Location:** The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field
- b. Enter the text or word that needs to be filtered

For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:/Program Files/' in the text field, then all events containing the entry 'C:/Program Files/' in the 'Location' field will be displayed. If you select the 'Does Not Contain' option from the drop-down field and enter the phrase 'C:/Program Files/' in the text field, then all events that do not have the entry 'C:/Program Files/' will be displayed.

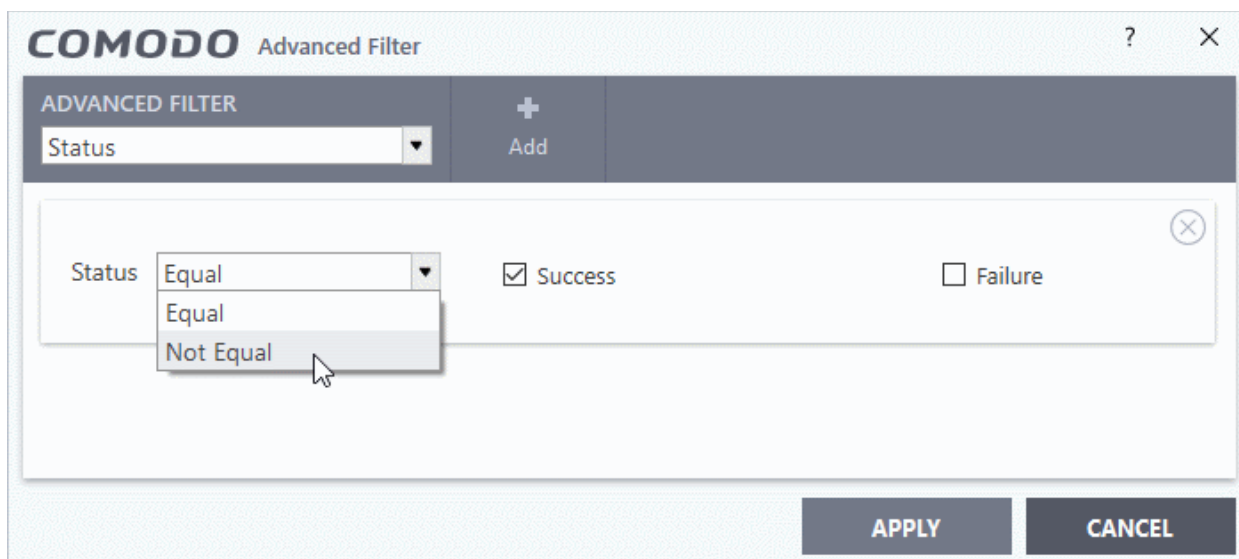
- iii. **Malware Name:** The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and type 'siins' in the text field, then all events with 'siins' in the 'Malware Name' field will be shown. If you choose 'Does Not Contain' and type 'siins', then all events that do not have 'siins' in the 'Malware Name' field will be shown.

- iv. **Status:** The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CCS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Success: Displays events in which the actions against the detected threat were successfully executed (for example, the malware was successfully quarantined)
 - Failure: Displays events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected)

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

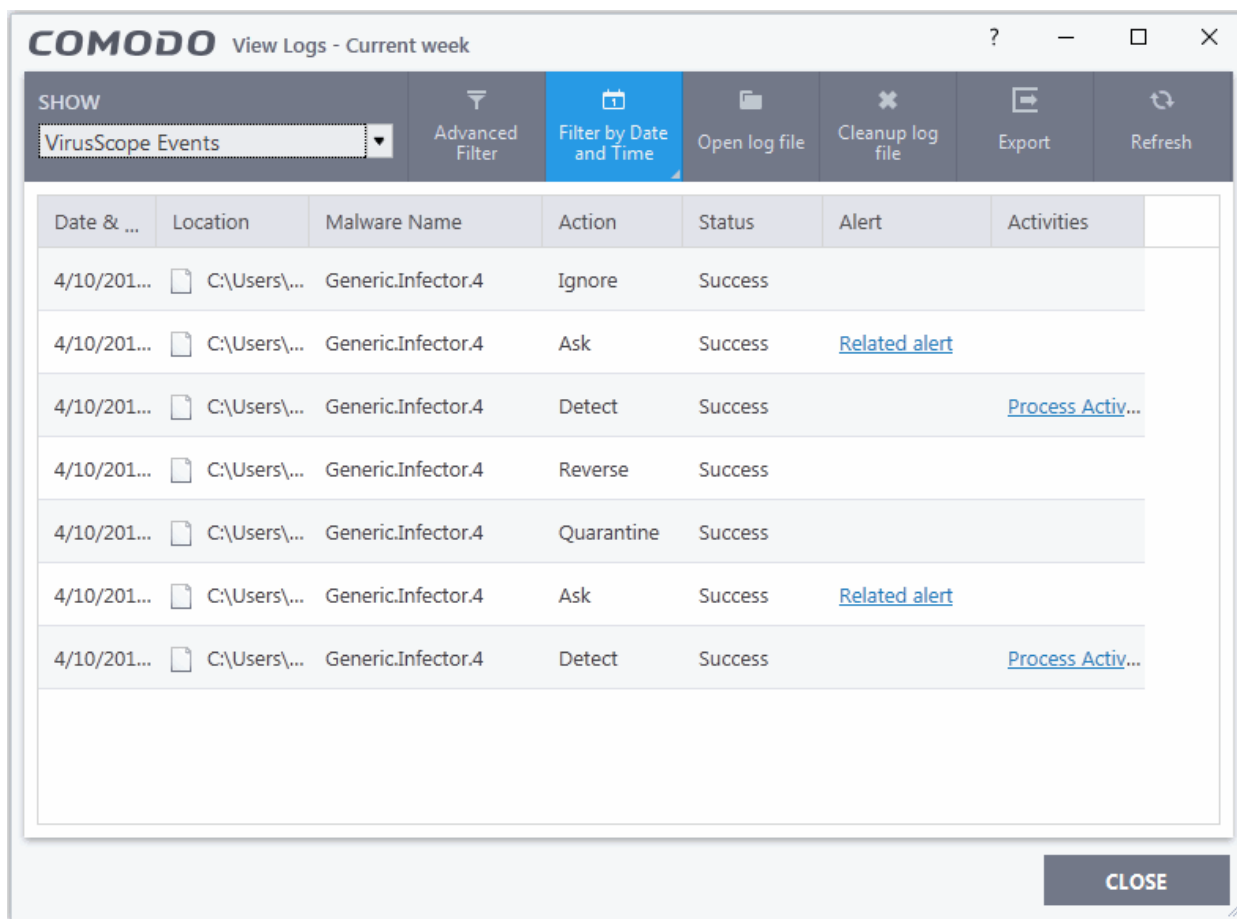
- Click 'Apply' for the filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

5.4.2. VirusScope Logs

Event logs are created whenever VirusScope blocks or reverses a suspicious activity.

To access the 'VirusScope' Logs

- Click 'Advanced Tasks' then select 'View Logs'
- Select 'VirusScope Events' from the 'Show' drop-down

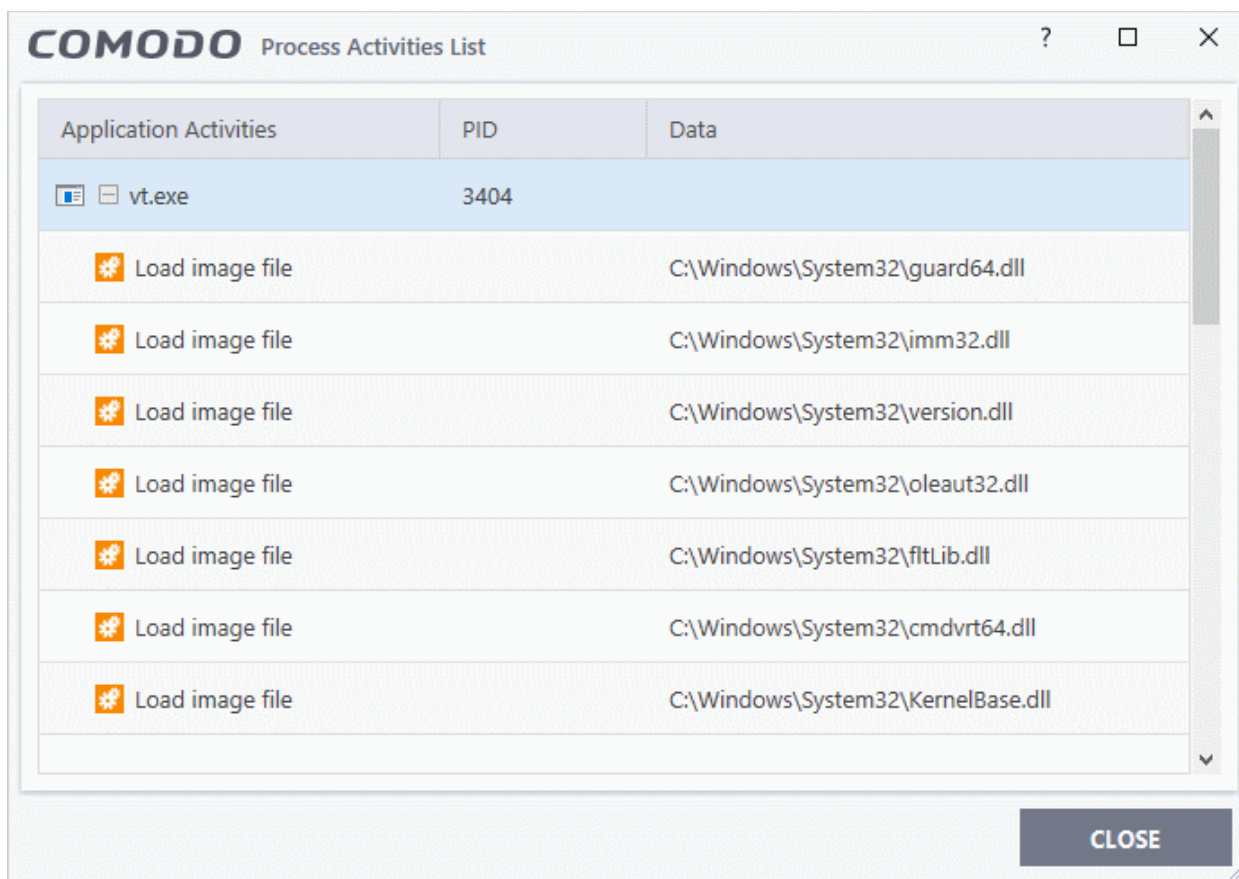


Column Descriptions

- Date & Time** - Indicates the precise date and time of the occurrence of the event.
- Location** - Indicates where the suspicious executable is stored.
- Malware Name** - Name of the detected malware.
- Action** - Indicates the action taken by VirusScope in response to the event.
 - Reverse - VirusScope detected suspicious activity and attempted to reverse any changes made to the file system.
 - Quarantine - VirusScope placed the suspicious file into quarantine
 - Detect - VirusScope detected malicious activity but did not quarantine the executable or reverse its changes
 - Ask - VirusScope detected malicious activity and presented a pop-up asking the user whether it should quarantine the executable or reverse the changes.
- Status** - Status of the action taken - 'Success' or 'Fail'.
- Alert** - Click the 'Related Alert' link will show details of the alert displayed during the event.

Note: VirusScope alerts are displayed only if the option 'Do not pop up alerts' is disabled in VirusScope Settings. See [VirusScope Configuration](#) for more details.

- Activities** - Click the 'Process Activities' link to view the details of activities executed by the processes that were run by the infected application. An example is shown below.



- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
- **'Open log file'** - view a saved log file.
- **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
- **'Cleanup log file'** - Deletes all logs from all modules

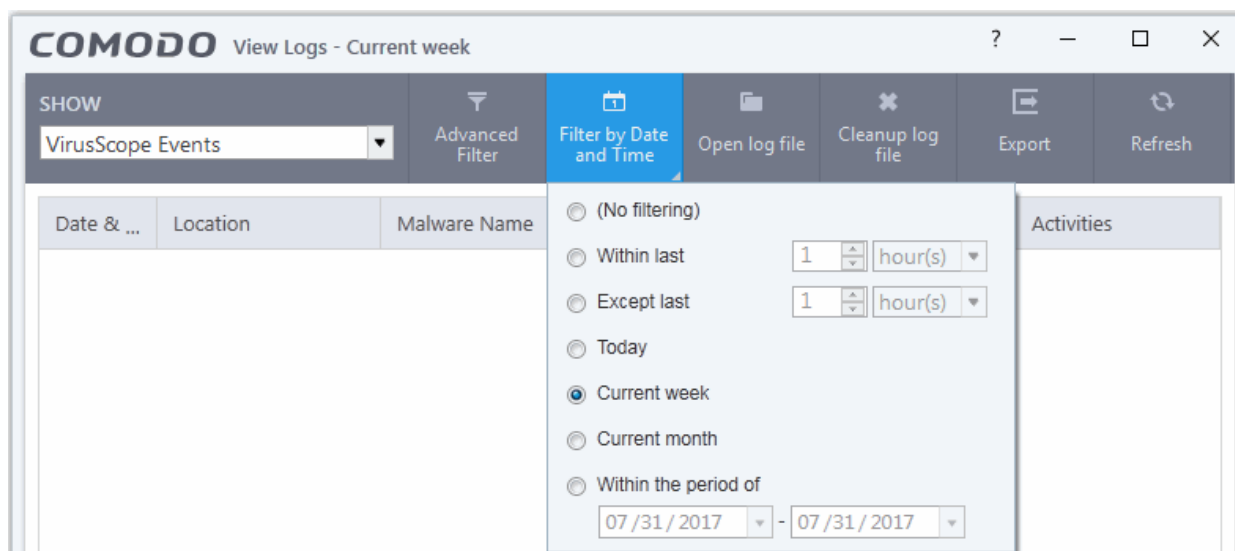
5.4.2.1. Filter VirusScope Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

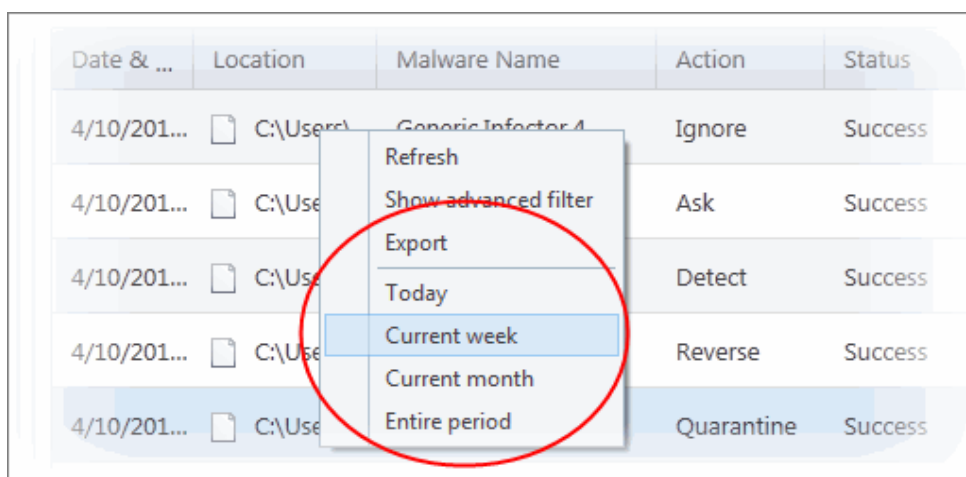
Preset Time Filters:

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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.



To configure Advanced Filters for VirusScope events

Having chosen a **preset time**, you can further refine which events are shown by using the following additional parameters:

- **Action** - Displays events according to the response (or action taken) by the VirusScope
- **Location** - Displays only the events logged from a specific location
- **Malware Name** - Displays only those events that reference a specific piece of malware

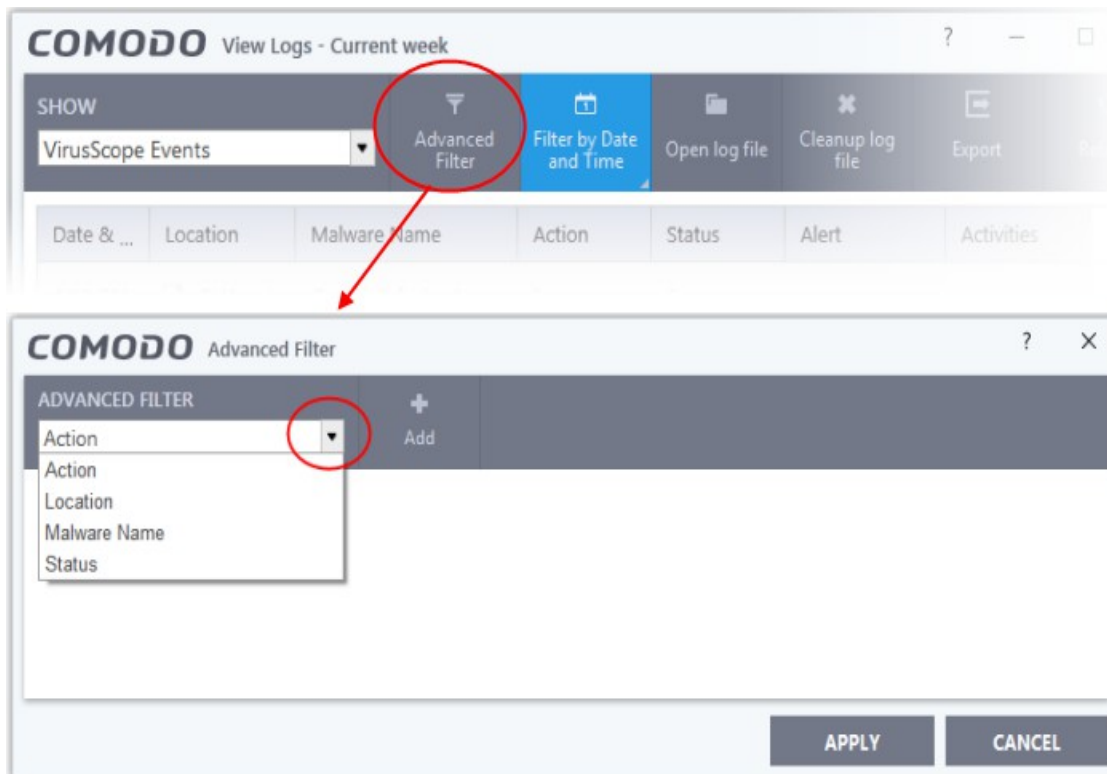
- **Status** - Show events according to whether the logged action was successful or not. Status options are 'Success' or 'Fail'.

To configure Advanced Filters for VirusScope events

1. Click the 'Advanced Filter' button from the title bar or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

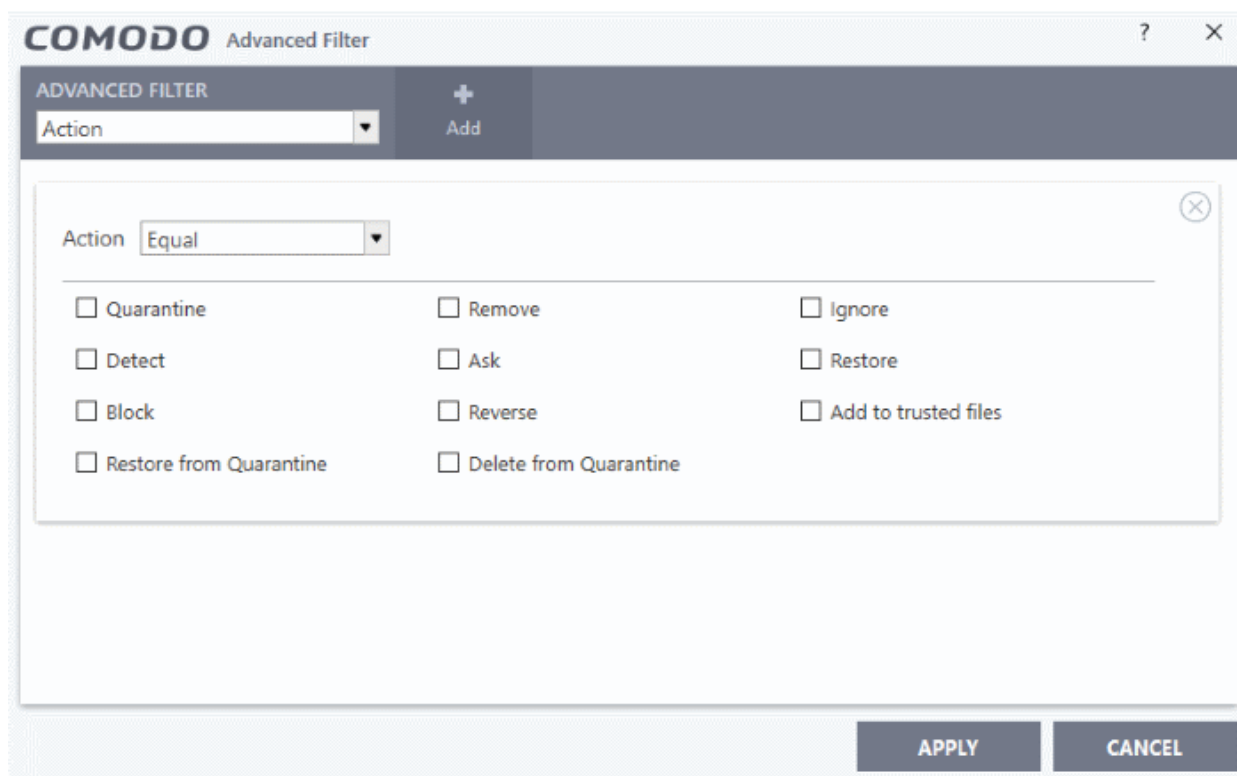
The 'Advanced Filter' interface for VirusScope Logs will open:

2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



There are four categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

- i. **Action:** The 'Action' option allows you to filter logs based on the actions taken by CCS against the detected threat. To filter logs by CCS action, select 'Action' from the drop-down then click 'Add':

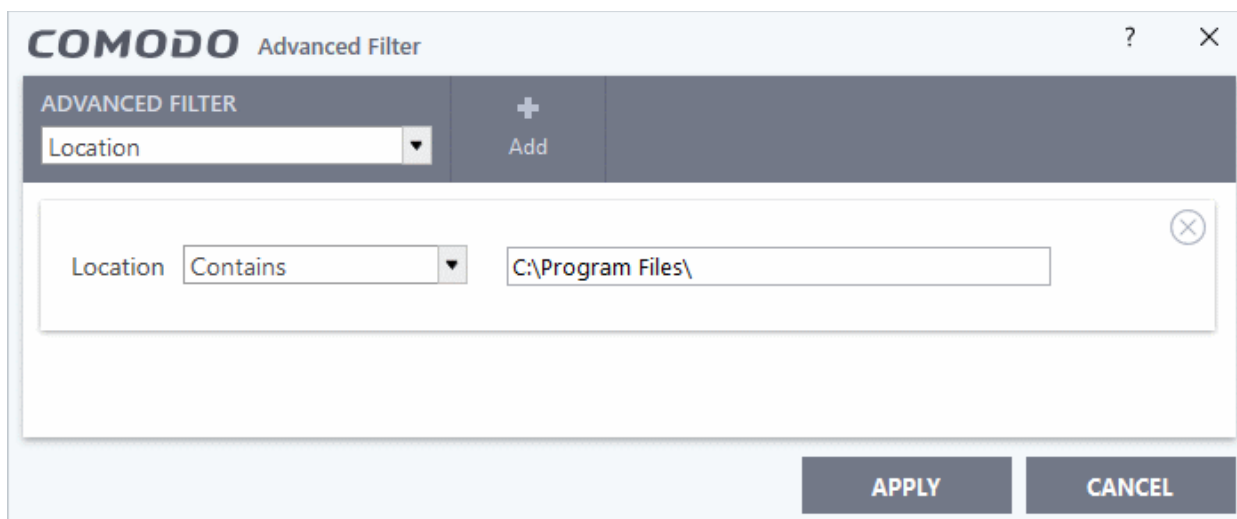


- a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b. Now select the check boxes of the specific filter parameters to refine your search. The parameter available are:

- Quarantine: Displays events at which the user chose to quarantine a file
- Remove: Displays events at which the user chose to delete the detected threat
- Ignore: Displays events at which the user chose to ignore the detected threat
- Detect: Displays events involving only the detection of malware
- Ask: Displays events where an alert was shown to the user so they could choose an action against a piece of detected malware
- Restore: Displays events at which quarantined applications were restored
- Block: Displays event where suspicious applications were blocked
- Reverse: Displays events where VirusScope reversed potentially malicious actions
- Add to trusted files: Displays events in which the user changed the file rating to 'Trusted'

For example, if you checked the 'Quarantine' box then selected 'Not Equal', you would see only those Events where the Quarantine Action was not selected at the virus notification alert.

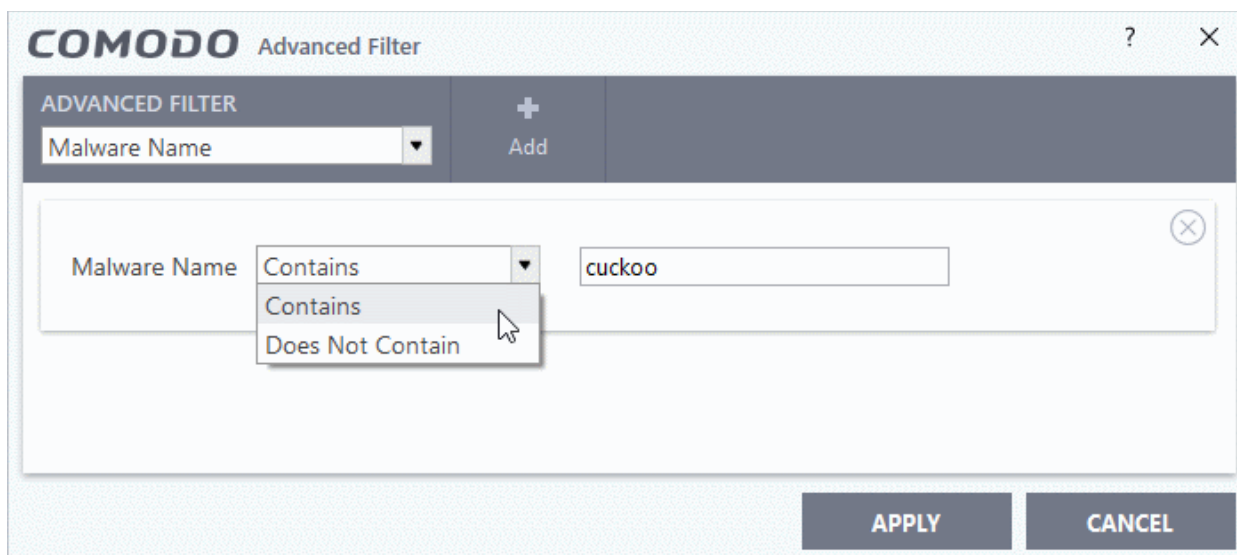
- Restore from Quarantine: Displays events in which files were restored from quarantine
 - Delete from Quarantine: Displays events in which files were deleted from quarantine
- ii. **Location:** The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and type 'C:/Program Files/' in the text field, then all events with 'C:/Program Files/' in the 'Location' field will be shown. If you choose 'Does Not Contain' and type 'C:/Program Files/', then all events that do not have 'C:/Program Files/' in the 'Location' field will be shown.

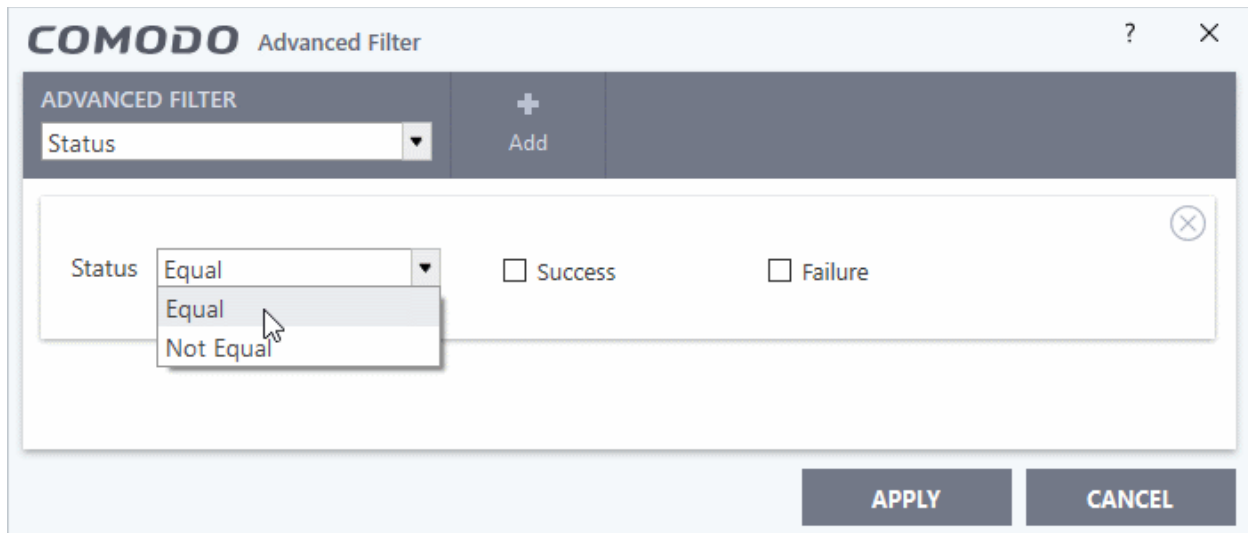
- iii. **Malware Name:** The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text in the name of the malware that needs to be filtered.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Malware Name' field will be displayed. If you choose the 'Does Not Contain' option from the drop-down and enter the phrase 'cuckoo' in the text field, then all events that do not have the entry 'cuckoo' in the 'Malware Name' field will be displayed.

- iv. **Status:** The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CCS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Success: Displays events where the actions against the detected threat were successful. For example, the malware was successfully quarantined.
 - Failure: Displays events where the intended actions against the detected threat were not successful. For example, the malware was not disinfected.

Note: Multiple filters can be added in the 'Advanced Filter' pane. After adding a filter, select the next filter type and click 'Add'. You can remove filters by clicking the 'X' button at the top right of the filter pane.

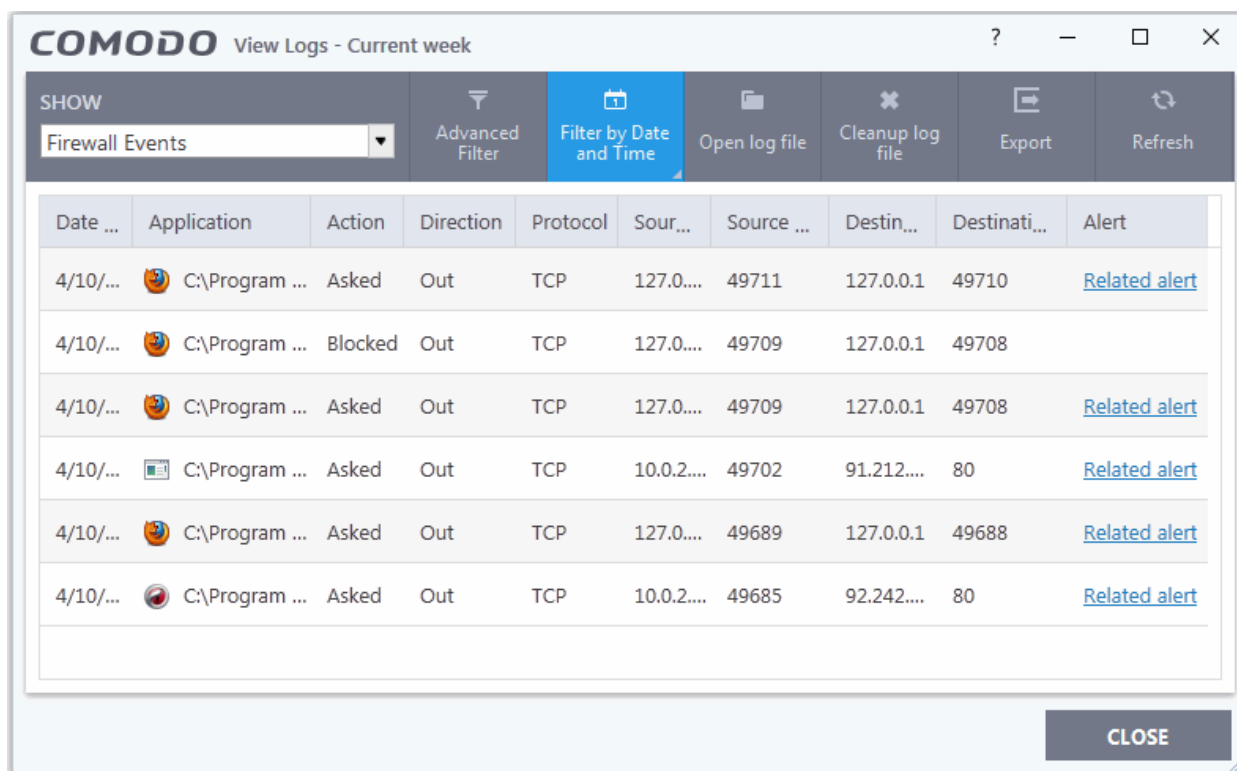
- Click 'Apply' for the filters to be applied to the VirusScope log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.3. Firewall Logs

Comodo Client Security records a history of all actions taken by the firewall. 'Firewall Events' are generated and recorded for various reasons - including whenever an application or process makes a connection attempt that contravenes a rule in your **Rule sets**, or whenever there is a change in firewall configuration.

To access 'Firewall' Logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs'
- Select 'Firewall Events' from the 'Show' drop-down



1. **Date & Time** - Indicates the precise date and time of the event.
2. **Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used.
3. **Action** - Indicates how the firewall reacted to the connection attempt. For example, whether the attempt was allowed, blocked or an alert displayed to the user so they could choose an action.
4. **Direction** - Indicates whether the connection attempt is inbound or outbound.
5. **Protocol** - The protocol used by the application that attempted to create the connection. This is usually TCP/IP, UDP or ICMP, which are the most heavily used networking protocols.
6. **Source IP** - Displays the IP address of the host that made the connection attempt. For outbound connections, this is usually the IP address of your computer. For inbound connections, it is usually the IP address of the external server.
7. **Source Port** - The port number on the host at the source IP which was used to make the connection attempt.
8. **Destination IP** - Displays the IP address of the host to which the connection attempt was made. For inbound connections, this is usually the IP address of your computer.
9. **Destination Port** - The port number on the host at the destination IP to which the connection attempt was made.
10. **Alert** - Click the 'Related Alert' link to view details of the alert displayed during the event.

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

- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
- **'Open log file'** - view a saved log file.
- **'Refresh'** - reload the list to view the latest logs

- Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
- **'Cleanup log file'** - Deletes all logs from all modules

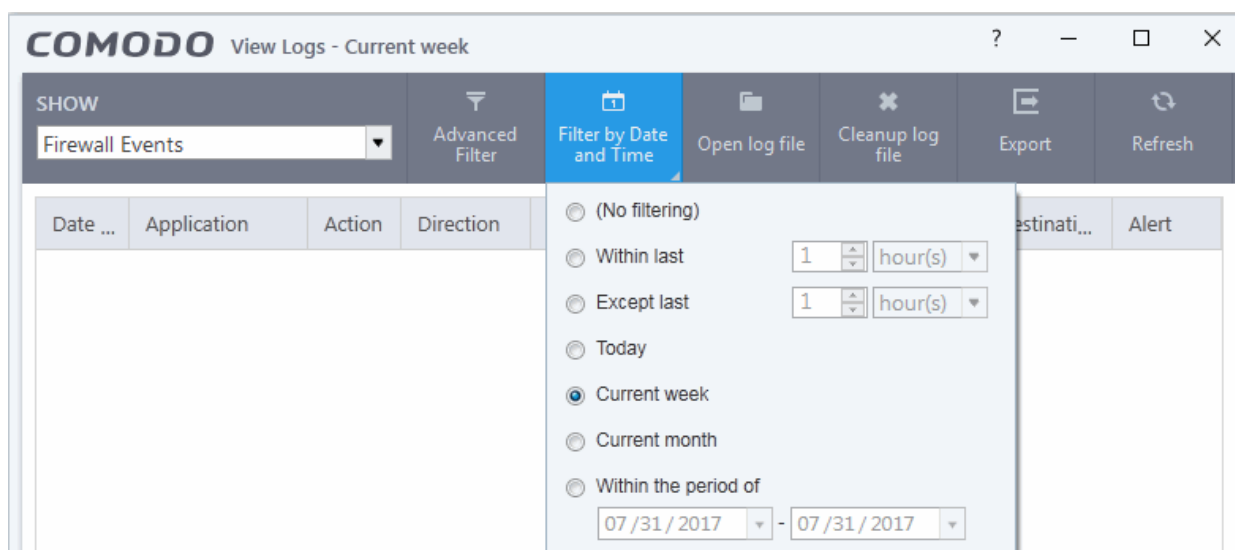
5.4.3.1. Filter Firewall Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

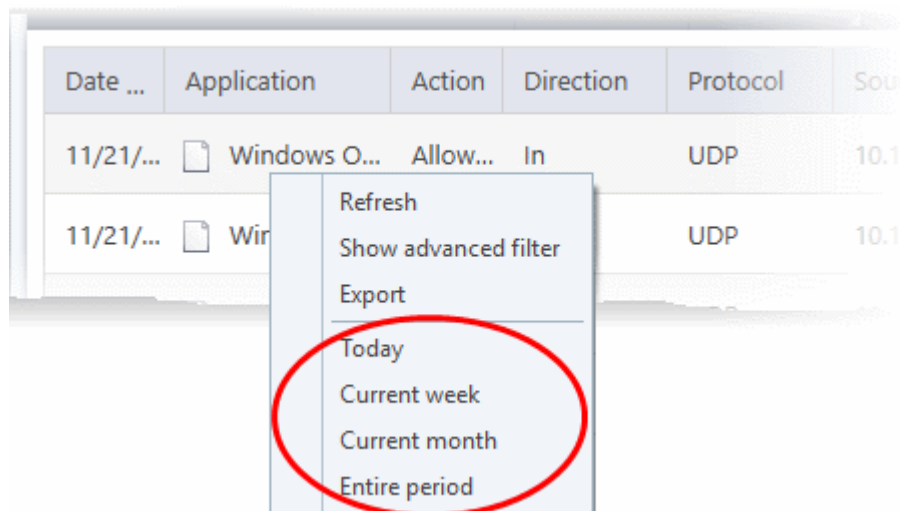
Preset Time Filters:

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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.



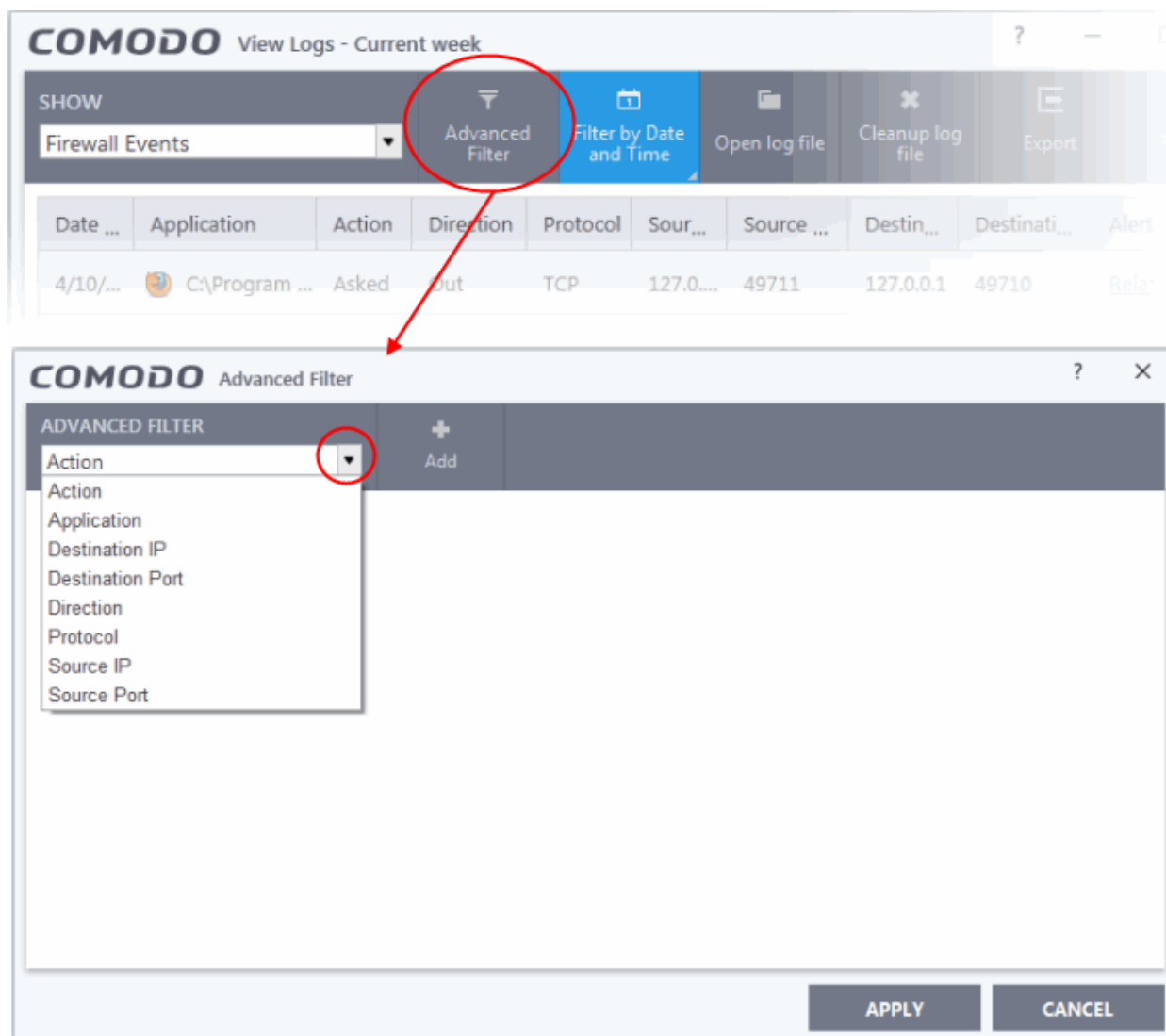
Advanced Filters

Having chosen a **preset time filter**, you can further refine the displayed events according to specific filters. Following are available filters for 'Firewall' logs and their meanings:

- **Action** - Displays events according to the response (or action taken) by the firewall
- **Application** - Displays only the events propagated by a specific application
- **Destination IP** - Displays only the events with a specific target IP address
- **Destination Port** - Displays only events that involved a specific target port number
- **Direction** - Displays only the events of Inbound or Outbound nature
- **Protocol** - Displays only events that involved a specific protocol
- **Source IP address** - Displays only the events that originated from a specific IP address
- **Source Port** - Displays only events that involved a specific source port number

To configure Advanced Filters for Firewall events

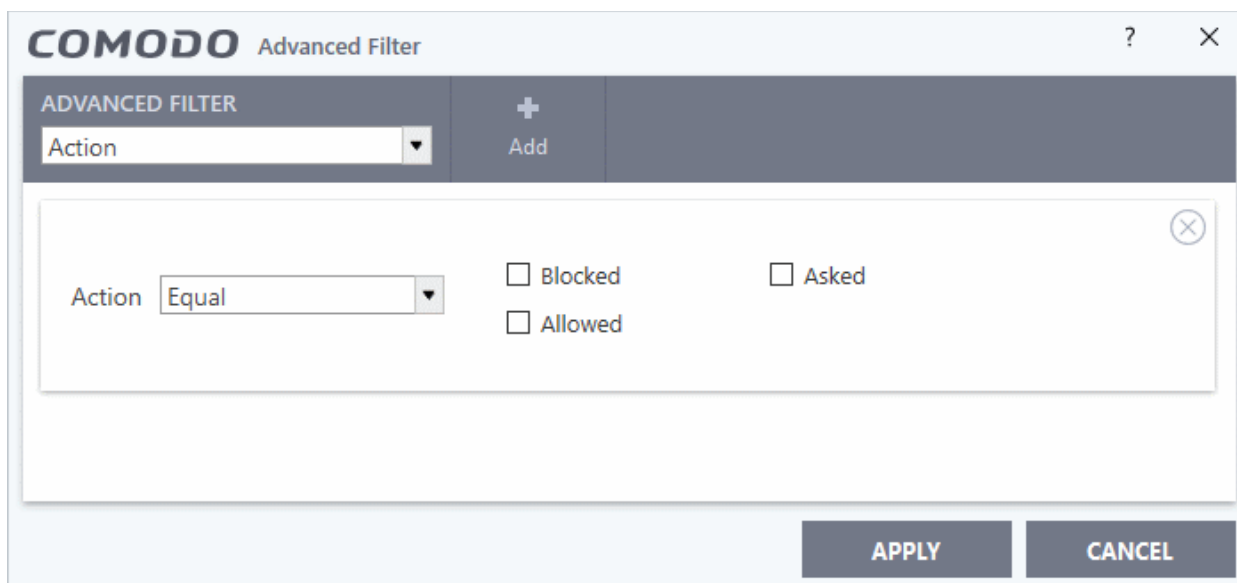
1. Click the 'Advanced Filter' button on the title bar or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.
2. The 'Advanced Filter' interface for Firewall Events will open.
3. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.



There are 8 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are the options available in the 'Advanced Filter' drop-down:

- i. **Action:** Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



COMODO Advanced Filter

ADVANCED FILTER

Action

+ Add

Action Equal

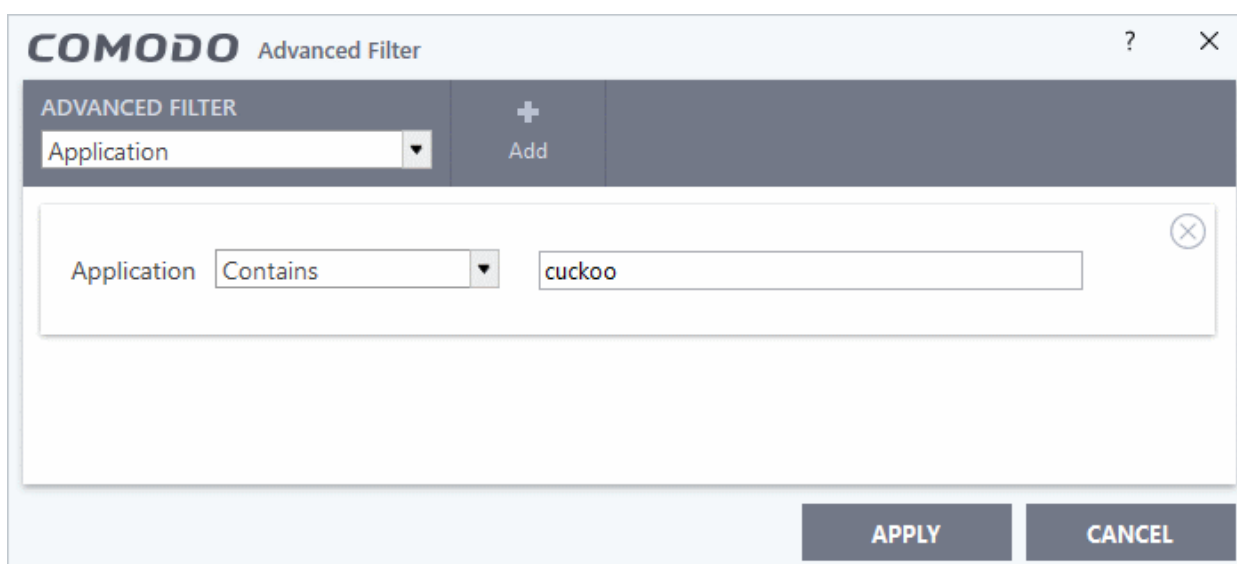
Blocked Asked

Allowed

APPLY CANCEL

You should now choose the actions by which you want to filter the logs:

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Blocked: Displays events where CCS prevented the connection
 - Allowed: Displays events where the connection was allowed to proceed
 - Asked: Displays events where an alert was shown to the user so they could choose whether or not to allow the connection
- ii. **Application:** Selecting the 'Application' option displays a drop-down box and text entry field.



COMODO Advanced Filter

ADVANCED FILTER

Application

+ Add

Application Contains

cuckoo

APPLY CANCEL

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box.
- b. Enter the text or word that needs to be filtered.

For example, if you choose 'Contains' from and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column will be displayed. If you select 'Does Not Contain'

and enter the phrase 'cuckoo' in the text field, then all events that do not have the entry 'cuckoo' in the 'Application' column will be displayed.

- iii. **Destination IP:** Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.

The screenshot shows the 'COMODO Advanced Filter' window. At the top, there is a header with the COMODO logo and the text 'Advanced Filter'. Below this, there is a dark grey bar with a dropdown menu set to 'Destination IP' and an 'Add' button. The main area of the dialog contains a filter rule: 'Destination IP' followed by a dropdown menu set to 'Equal', a text input field containing '192.168.111.11', and another dropdown menu set to 'IPv4'. A mouse cursor is hovering over the 'IPv4' dropdown, which has opened to show options for 'IPv4' and 'IPv6'. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

- Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- 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.

- iv. **Destination Port:** Selecting the 'Destination Port' option displays a drop-down box and text entry field.

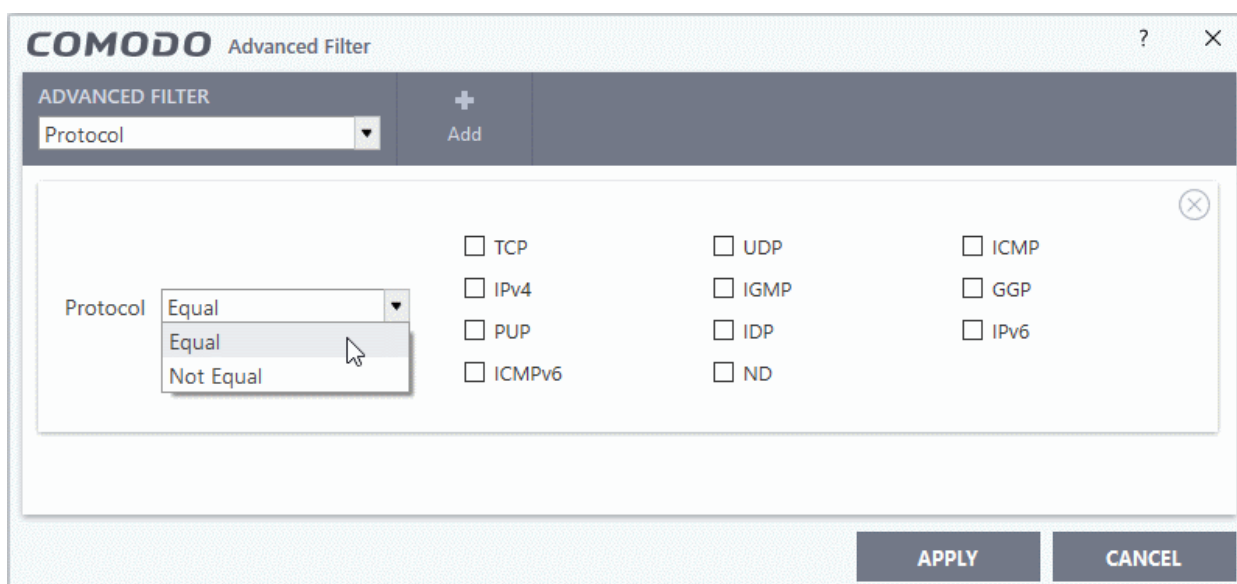
The screenshot shows the 'COMODO Advanced Filter' window. At the top, there is a header with the COMODO logo and the text 'Advanced Filter'. Below this, there is a dark grey bar with a dropdown menu set to 'Destination Port' and an 'Add' button. The main area of the dialog contains a filter rule: 'Destination Port' followed by a dropdown menu with a list of comparison operators: 'Equal', 'Greater Than', 'Greater Than Or Equal', 'Less Than', 'Less Than Or Equal', and 'Not Equal'. A mouse cursor is hovering over the 'Equal' option. To the right of the dropdown is a text input field containing '8080'. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

- Select any one of the option the drop-down:
 - Equal

- Greater than
 - Greater than or Equal
 - Less than
 - Less than or Equal
 - Not Equal
- b. Now enter the destination port number in the text entry field.
- For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.
- v. **Direction:** Selecting the 'Direction' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

The screenshot shows the 'COMODO Advanced Filter' dialog box. It features a dark header with the text 'ADVANCED FILTER' and an 'Add' button. Below this, there is a 'Direction' dropdown menu. The dropdown is open, showing three options: 'Equal', 'Equal', and 'Not Equal'. To the right of the dropdown are two checkboxes: 'In' (checked) and 'Out' (unchecked). At the bottom right of the dialog are 'APPLY' and 'CANCEL' buttons.

- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the check box of the specific filter parameters to refine your search. The parameter available are:
- In: Displays a list of events involving inbound connection attempts
 - Out: Displays a list of events involving outbound connection attempts
- For example, if you choose 'Equal' option from the drop-down and select the 'In' checkbox, then all inbound connection attempts will be displayed.
- i. **Protocol:** Selecting the 'Protocol' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

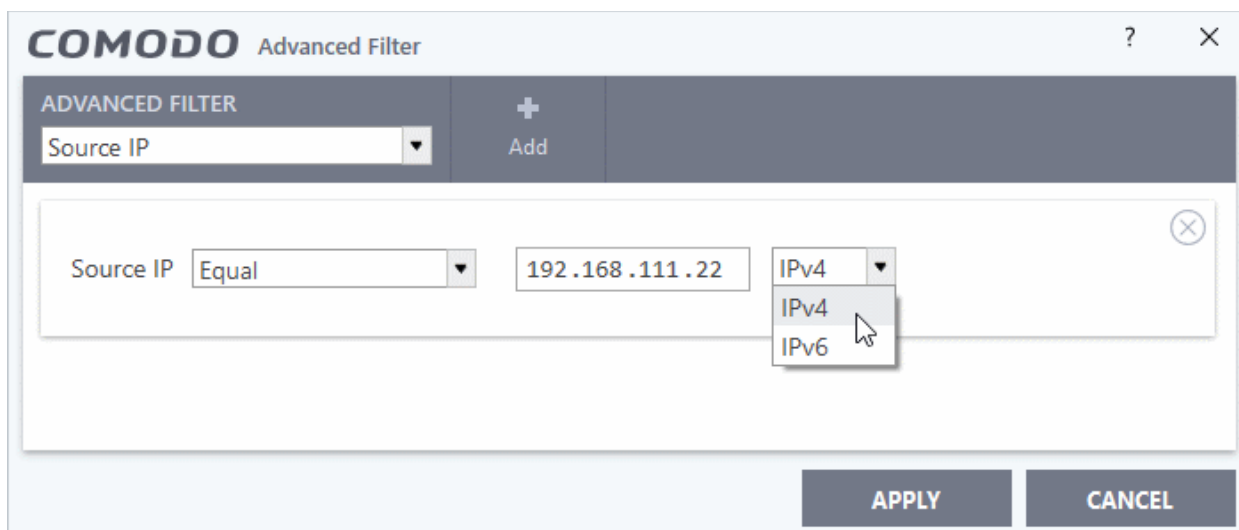


- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- TCP
- UDP
- ICMP
- IPV4
- IGMP
- GGP
- PUP
- IDP
- IPV6
- ICMPV6
- ND

For example, if you choose 'Equal' option from the drop-down and select the 'TCP' checkbox, then all connection attempts involving TCP protocol will be displayed.

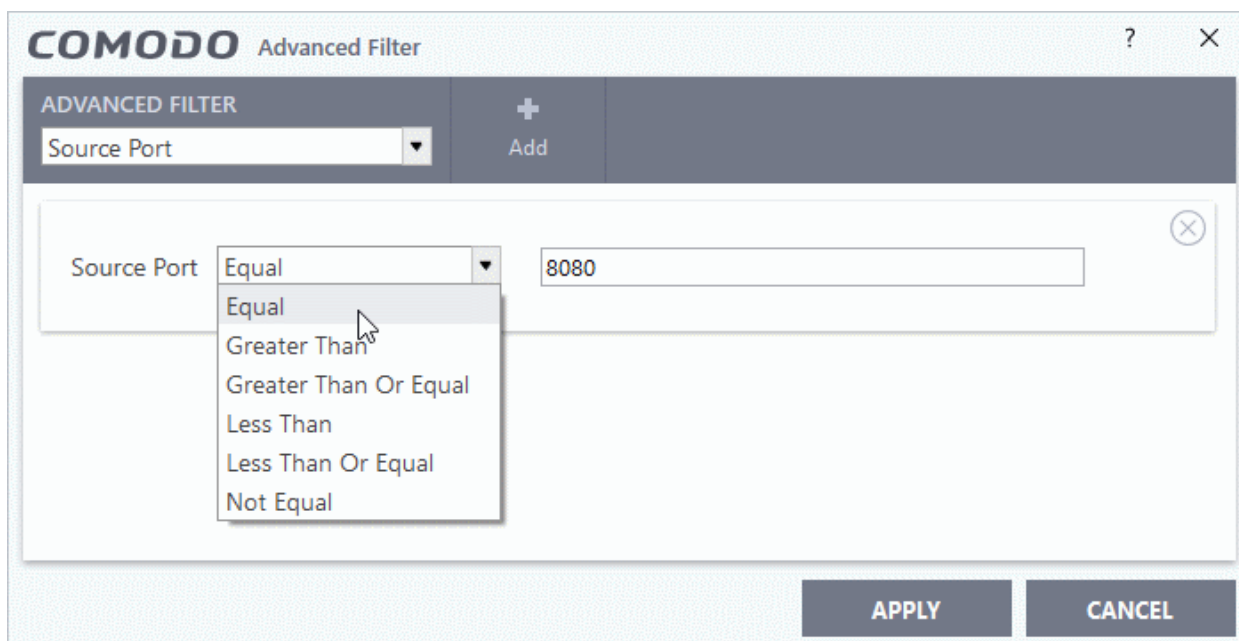
- vii. **Source IP:** Selecting the 'Source IP' option displays two drop-down boxes and a set specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Select 'IPv4' or 'IPv6' from the drop-down box.
- a. Enter the IP address of the source server or host, to filter the events that involve the connection attempts from/to that source server or host system.

For example, if you choose 'Contains' then select IPv4 and enter 192.168.111.22 in the text field, then all events containing the entry '192.168.111.11' in the 'Source IP' column will be displayed.

- viii. **Source Port:** Selecting the 'Status' option displays a drop-down box and a set specific filter parameters that can be selected or deselected.



- a. Select any one of the following option the drop-down box.
 - Equal
 - Greater than
 - Greater than or Equal
 - Less than
 - Less than or Equal

- Not Equal
- b. Now enter the source port number in the text entry field.

For example, if you choose 'Equal' and enter 8080 in the text field, then all events containing the entry '8080' in the 'Source Port' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

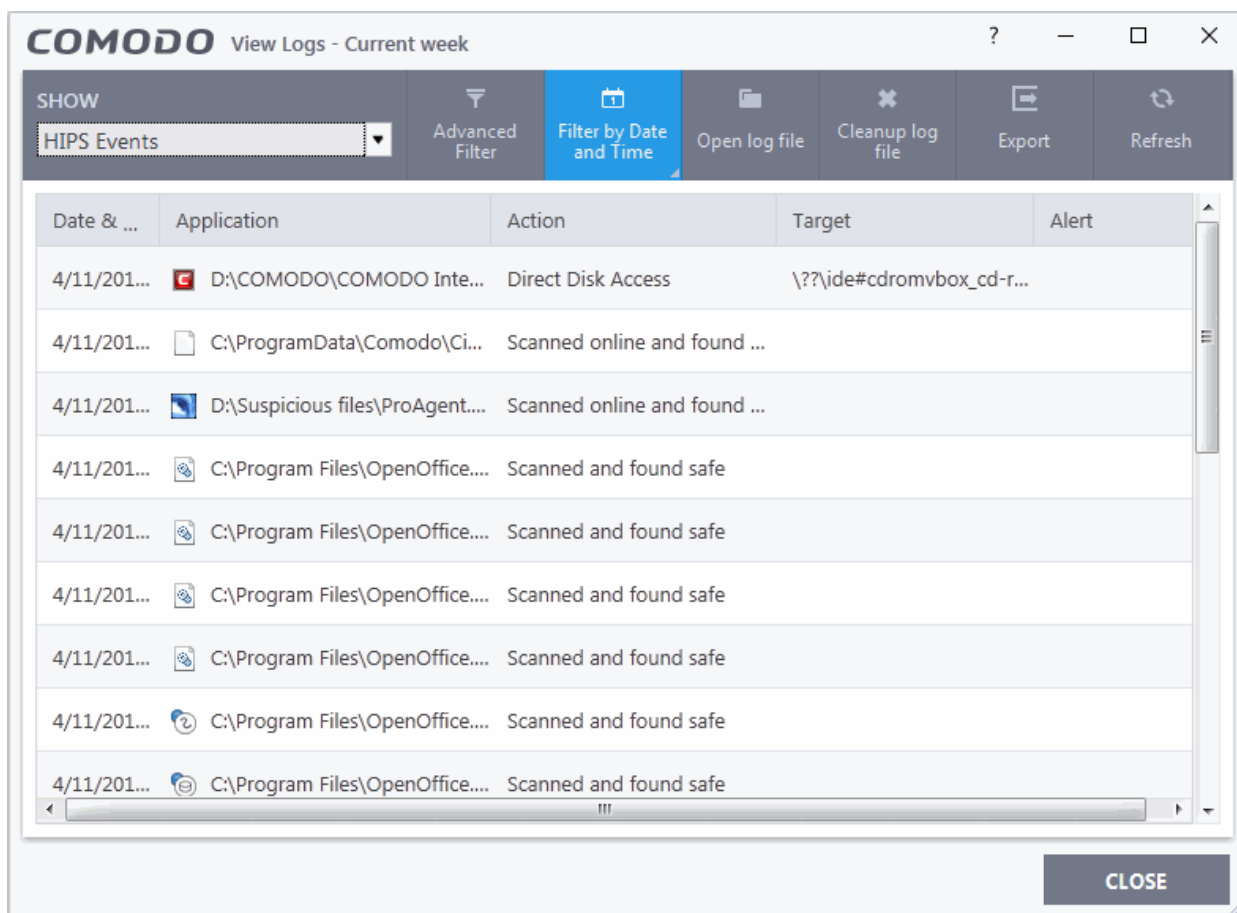
- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.4. HIPS Logs

Comodo Client Security records a history of all actions taken by HIPS. 'HIPS Events' are generated and recorded for various reasons. Examples include changes in HIPS settings, when an application is auto-contained, when an application or process attempts to access restricted areas or when an action occurs that contravenes your **HIPS Rulesets**.

To access 'HIPS' Logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs'
- Select 'HIPS Events' from the 'Show' drop-down



Column Descriptions

1. **Date & Time** - Indicates the precise date and time of the event.
2. **Application** - Indicates the application or process that propagated the event. If the application has no icon then the default system icon for executable files are used.
3. **Action** - If the action was allowed to proceed then this column will show the result of that action. Click the 'Related Alert' link to see the alert that was displayed at the time. If the action was not allowed then this column will state 'Block File'.
4. **Target** - Location of the target file, COM interface or registry key accessed by the process.
5. **Alert** - Click the 'Related Alert' link to view details of the alert displayed during the event.

Note: HIPS alerts are only displayed if 'Do not show pop up alerts' is disabled in HIPS Settings. See [HIPS Settings](#) for more details.

- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
- **'Open log file'** - view a saved log file.
- **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
- **'Cleanup log file'** - Deletes all logs from all modules

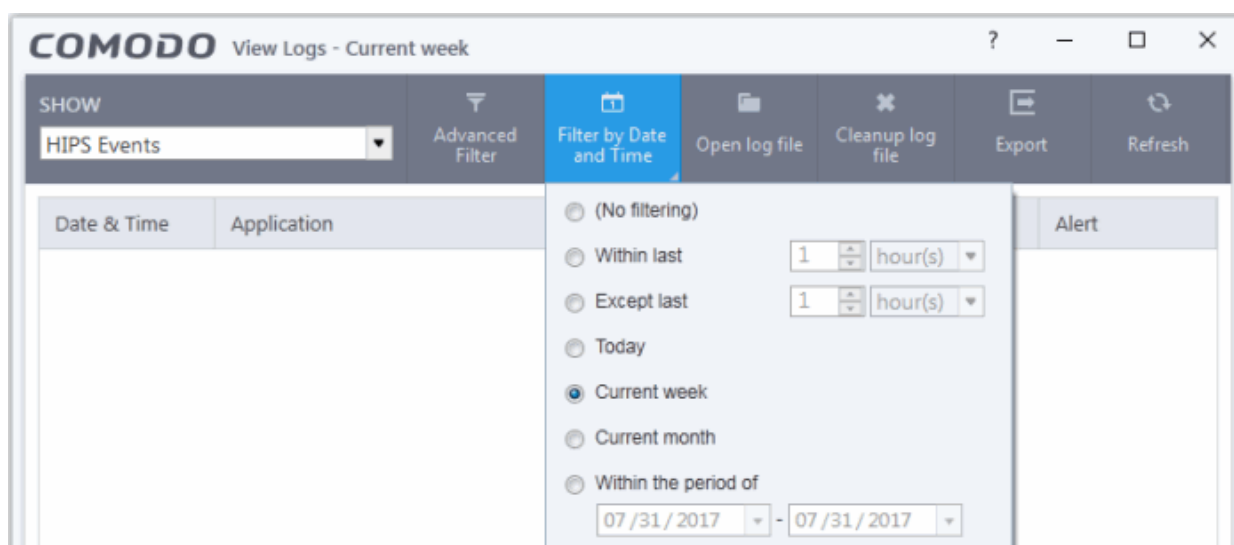
5.4.4.1. Filter HIPS Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters:

- Click 'Filter by Date and Time' to display logs for a specific time period:

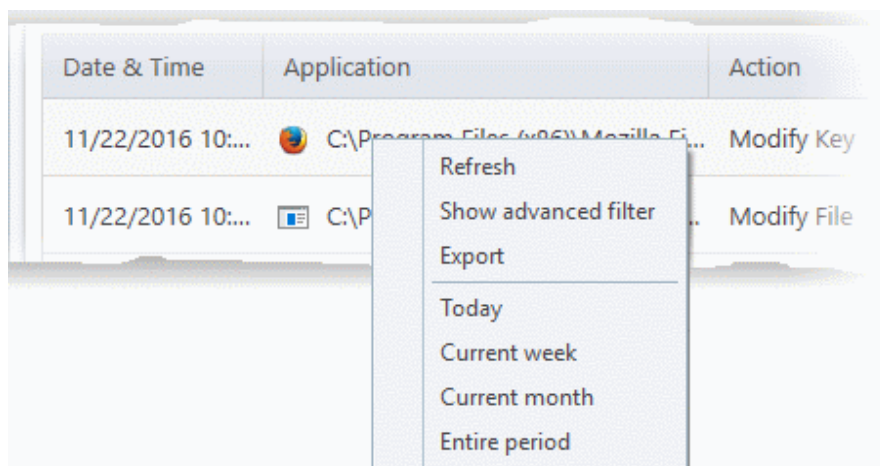


- **No filtering** - Show every event logged since CCS was installed. If you have cleared the logs since

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.
- **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

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. Following are available filters for HIPS logs and their meanings:

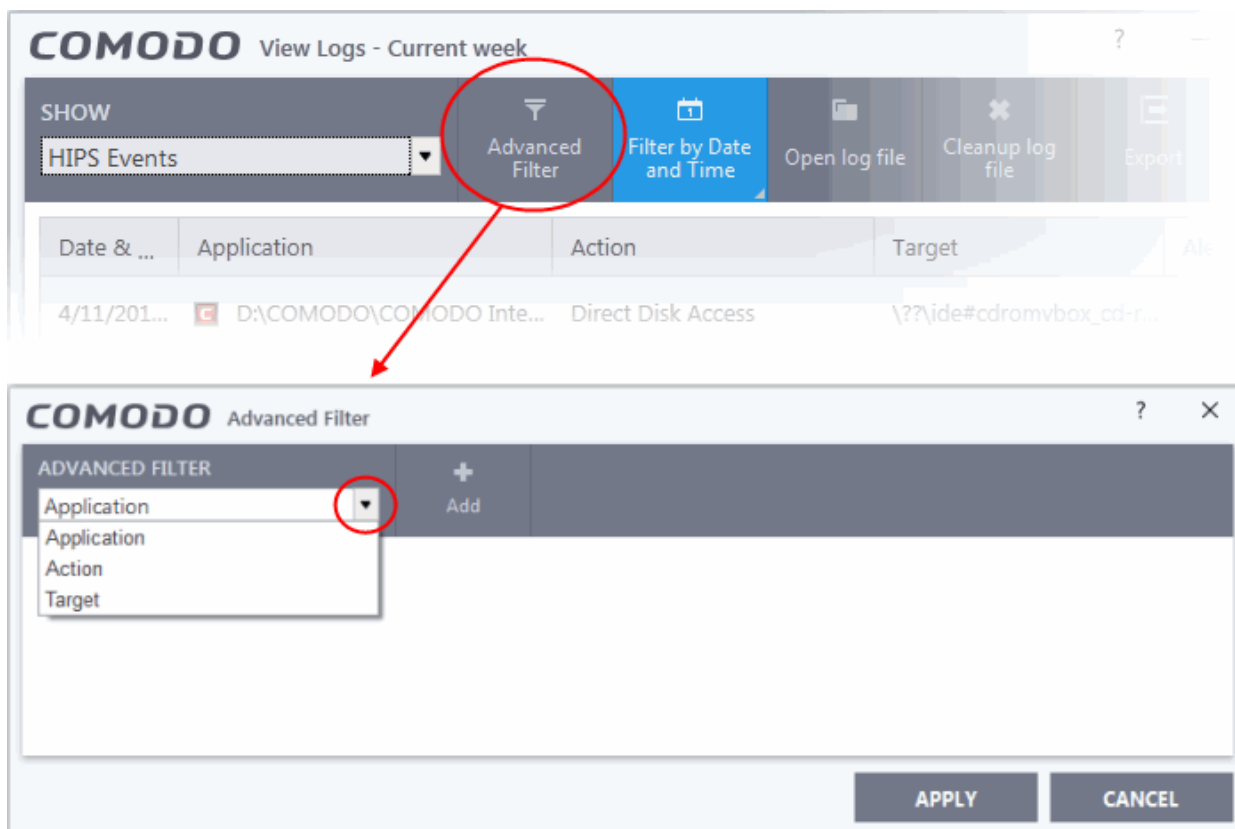
- **Application** - Displays only the events propagated by a specific application
- **Action** - Displays events according to the response (or action taken) by HIPS
- **Target** - Displays only the events that involved a specified target application

To configure Advanced Filters for HIPS events

1. Click the 'Advanced Filter' button on the title bar or right click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

The 'Advanced Filter' interface for HIPS Events will open:

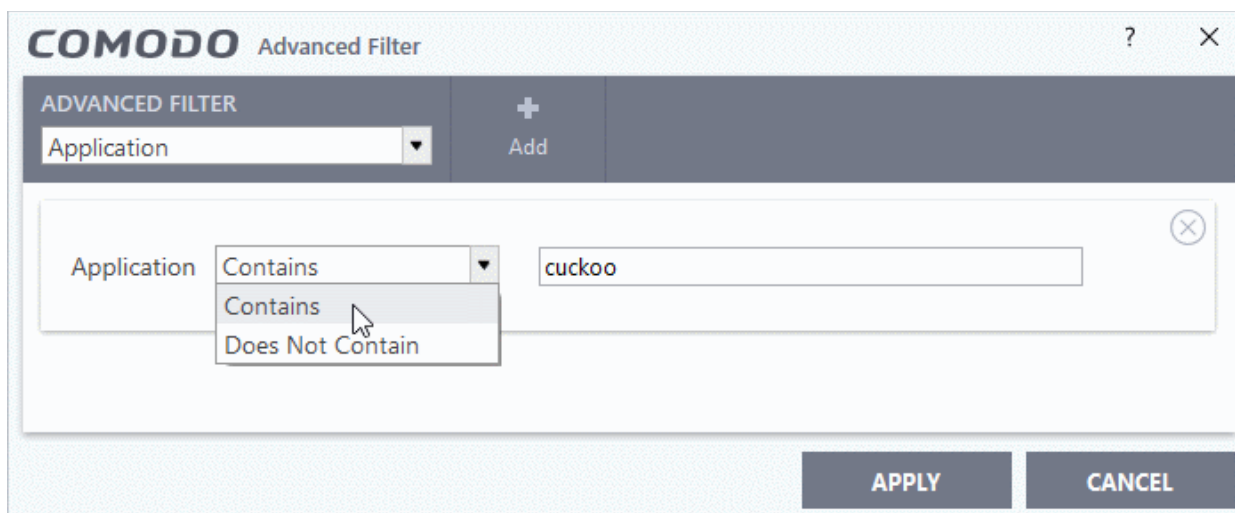
2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.



There are 3 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following options are available in the 'Advanced Filter' drop-down:

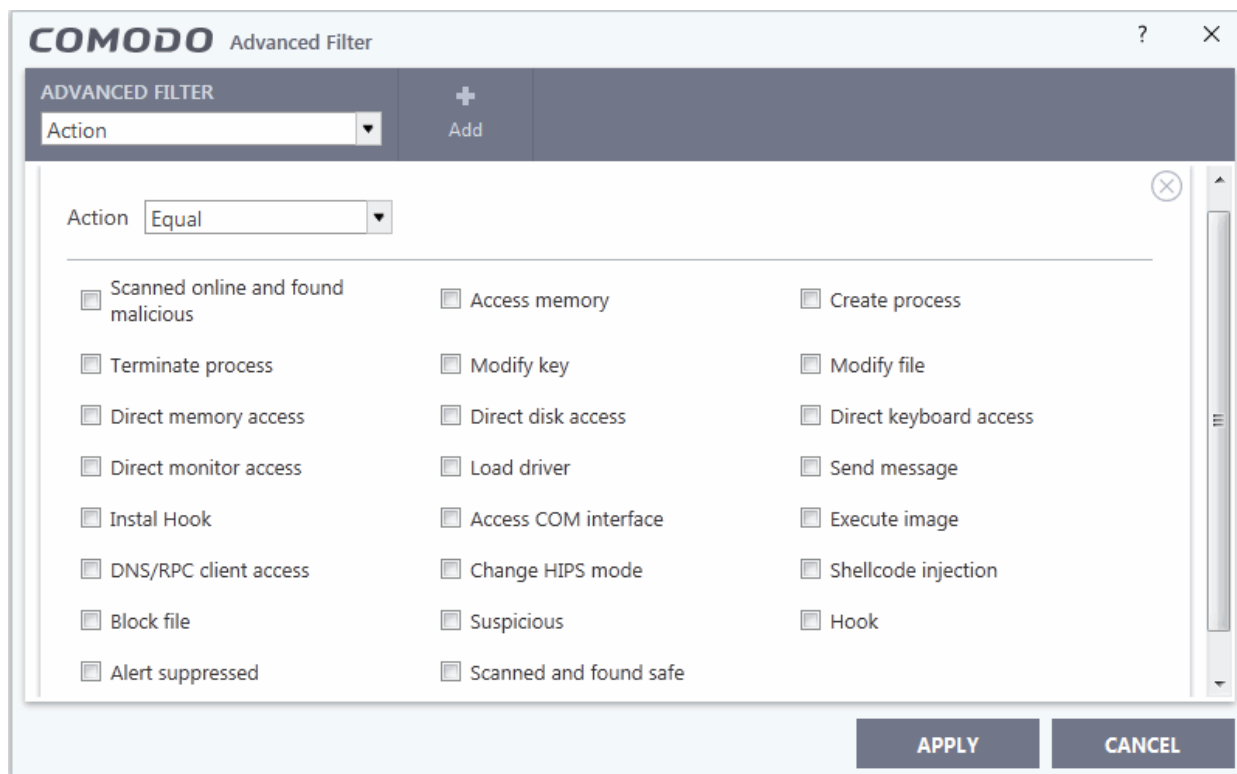
- i. **Application:** The 'Application' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column will be displayed. If you choose 'Does Not Contain' from the drop-down and enter the phrase 'cuckoo', then all events that do not have the entry 'cuckoo' in the 'Application' column will be displayed.

- ii. **Action:** Selecting the 'Action' option displays a drop down menu and a set of filter parameters that can be selected or deselected.



- c. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- d. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Scanned online and found malicious
- Access memory
- Create process
- Terminate process
- Modify key
- Modify file
- Direct memory access
- Direct disk access
- Direct keyboard access
- Direct monitor access
- Load driver
- Send message
- Install Hook
- Access COM interface
- Execute image
- DNS/RPC client access
- Change HIPS Mode
- Shellcode injection

- Block file
- Suspicious
- Hook
- Alert Suppressed
- Scanned and found safe

For example, if you choose 'Equal' and select 'Create process', only events involving the creation of a process by applications will be displayed. If you choose 'Not Equal' and select 'Modify Key', then all events that do not have the entry 'Modify key' in the 'Actions' column will be displayed. You can select more than one action from this interface, as required.

iii. **Target:** Selecting the 'Target' option displays a drop-down menu and text entry field.

- Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' and enter the phrase 'svchost.exe' in the text field, then all events containing the entry 'svchost.exe' in the 'Target' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'svchost.exe', then all events that do not have the entry 'svchost.exe' in the 'Target' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'HIPS' log viewer. Only those HIPS entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

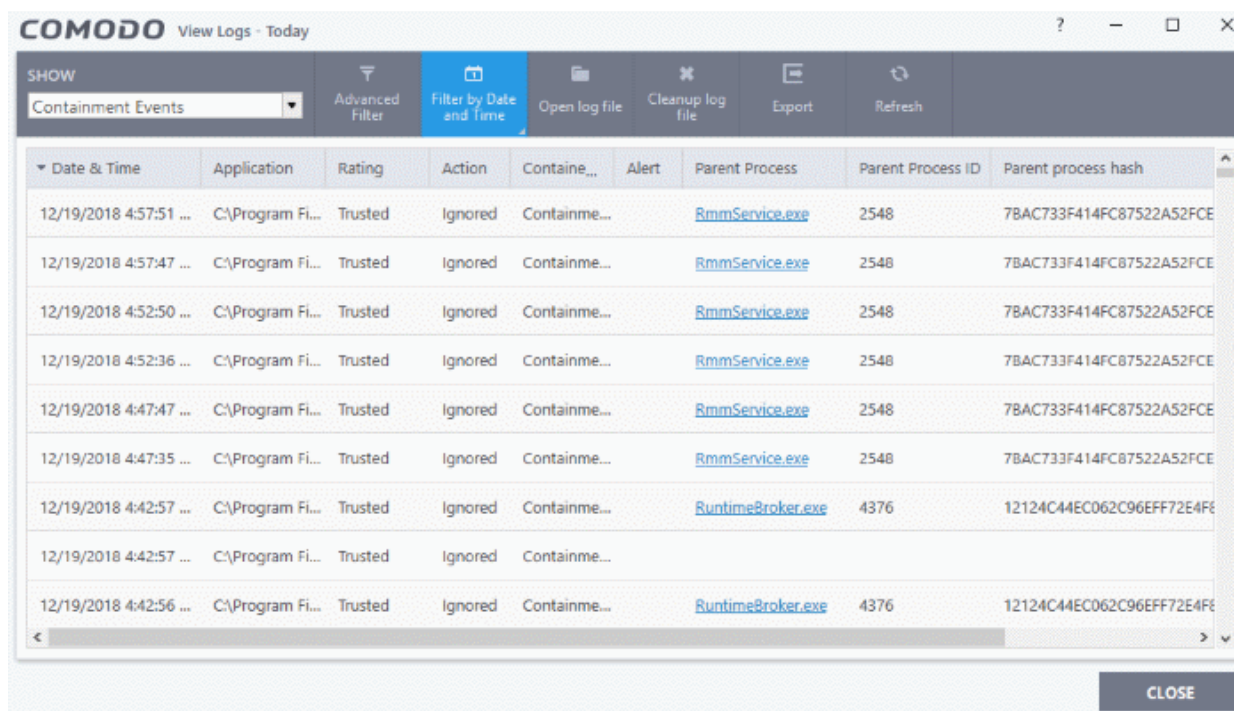
5.4.5. Containment Logs

'Containment Events' are generated whenever an application is placed in containment. Each log provides details about the conditions of the containment operation.

To access containment logs

- Click 'Tasks' at the top-left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs'

- Select 'Containment Events' from the 'Show' drop-down

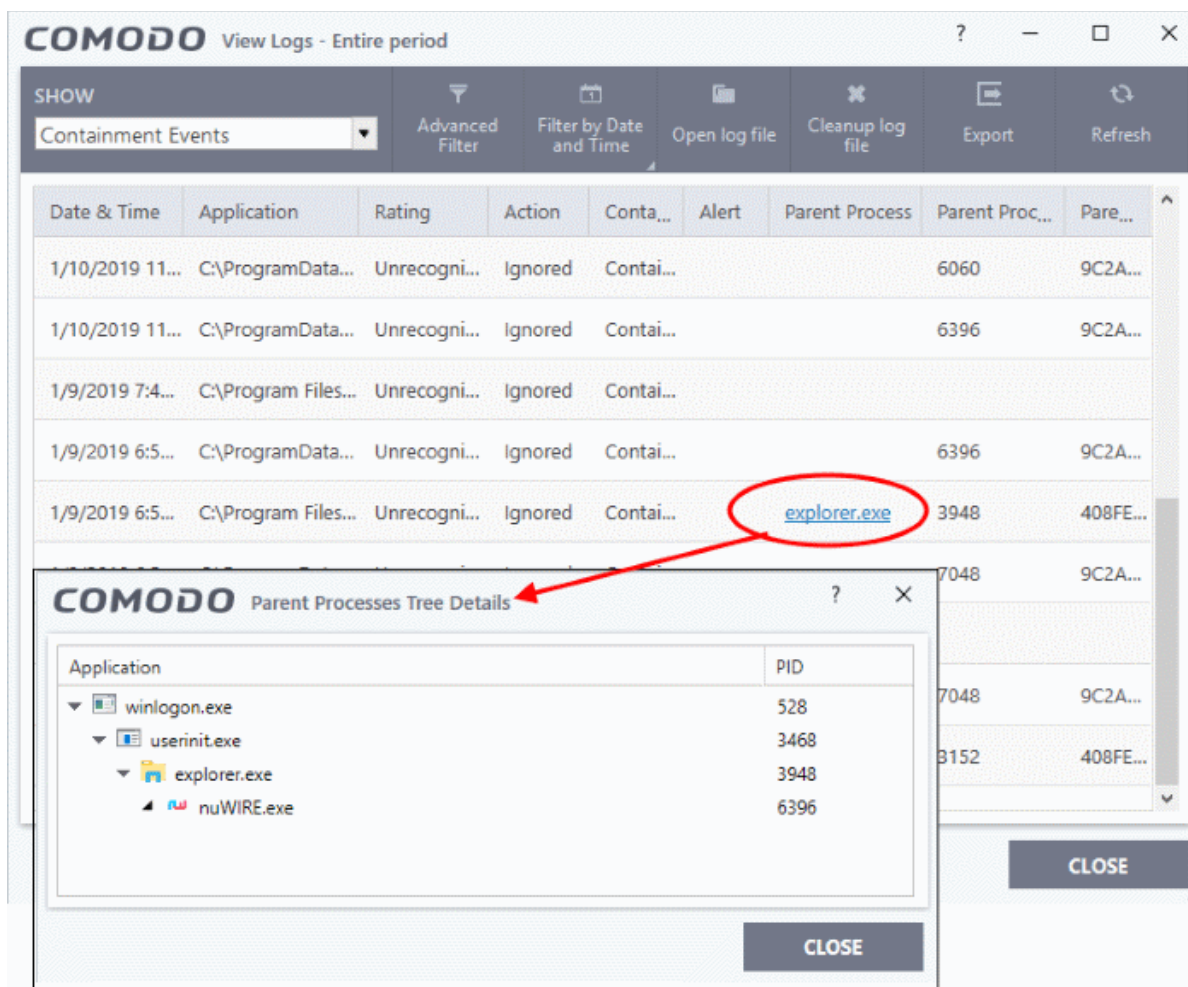


Column Descriptions

1. **Date & Time** - The date and time of the event.
2. **Application** - The location of the program/file/script that was run in the container.
3. **Rating** - The reputation of the file as per Comodo's file rating system. The file can be 'Trusted' (known-safe), 'Malicious' (known-malware) or 'Unrecognized'.
4. **Action** - The restriction level imposed on the contained item.
5. **Contained by** - The CCS component or user that was responsible for placing the item in the container.
6. **Alert** - Click the 'Related Alert' link to view details about the notification shown during the event.
7. **Parent Process** - The program which spawned the contained process.
8. **Parent Process ID** - The unique identifier that points to the process
9. **Parent process hash** - The SHA1 hash value of the program which spawned the contained process.

Note: Containment logs show alerts when the installer of an process ID unknown application requires admin privileges to run. These alerts are shown if 'Do not show privilege elevation alerts' is disabled in containment settings. See **Containment Settings** for more details.

- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
- **'Open log file'** - view a saved log file.
- **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
- **'Cleanup log file'** - Deletes all logs from all modules



You can view the hierarchical order of running processes created by its contained parent application by clicking the link of parent process name

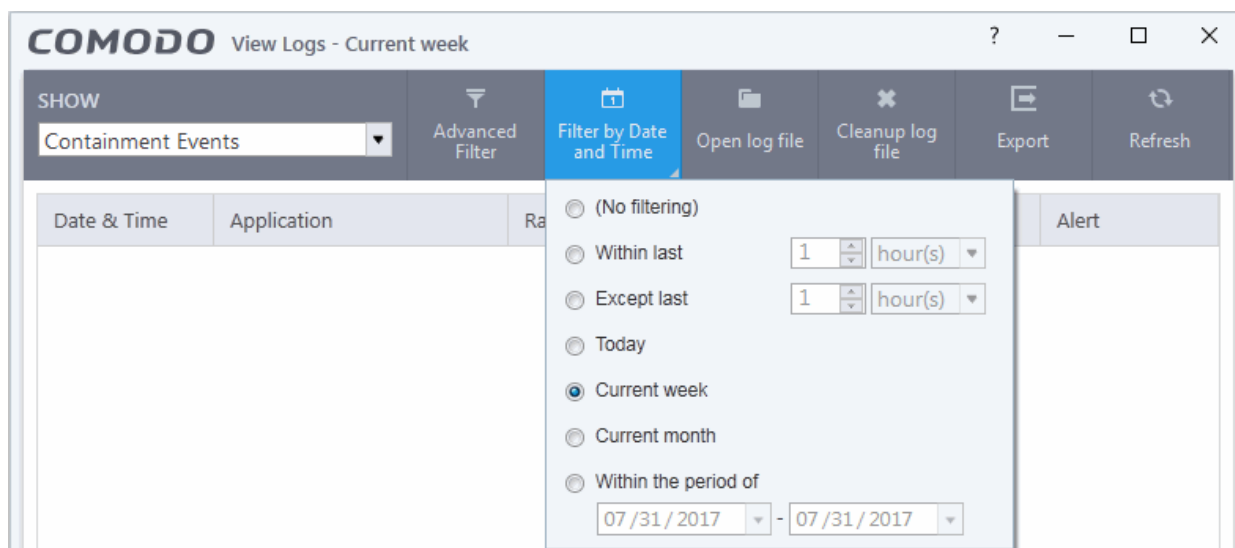
5.4.5.1. Filter Containment Logs

You can create custom event log views according to your preferences. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

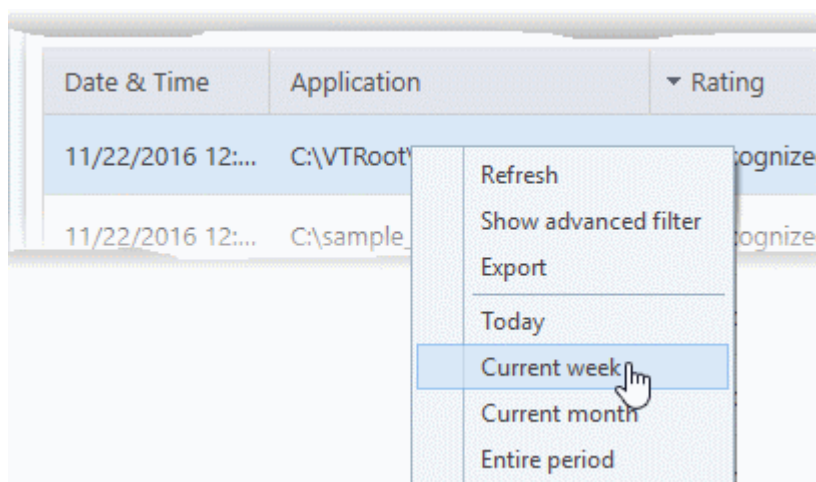
Preset Time Filters:

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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

Having chosen a **time range**, you can further refine events with the following filters:

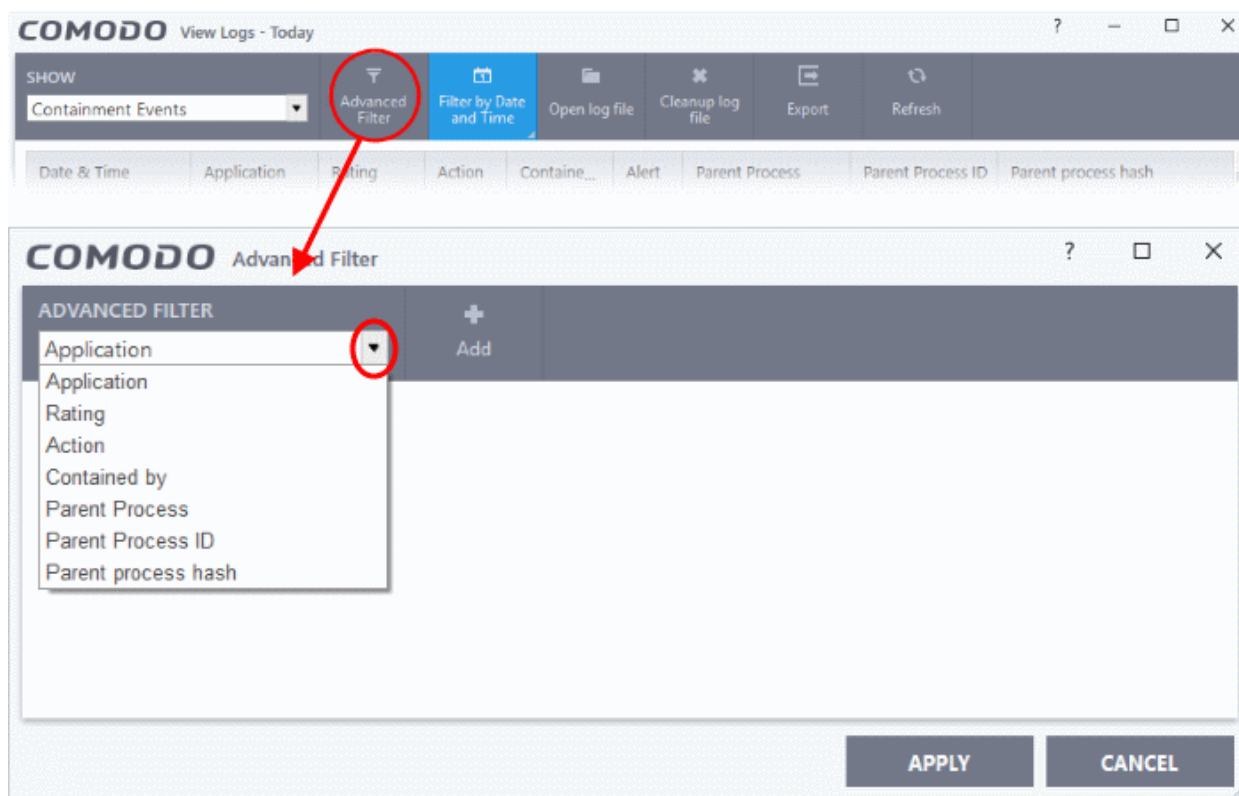
- **Application** - Show events propagated by a specific application
- **Rating** - Show events which concern files that have a specific trust-rating
- **Action** - Show events where a specific action was applied to the file by CCS
- **Contained by** - Show events where the file was contained by a specific module or user

- **Parent process** - Show files contained based on its source process(es)
- **Parent Process ID** – Show events created by a process ID
- **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)

To configure filters for Containment Events

1. Click the 'Advanced Filter' button on the title bar or right-click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

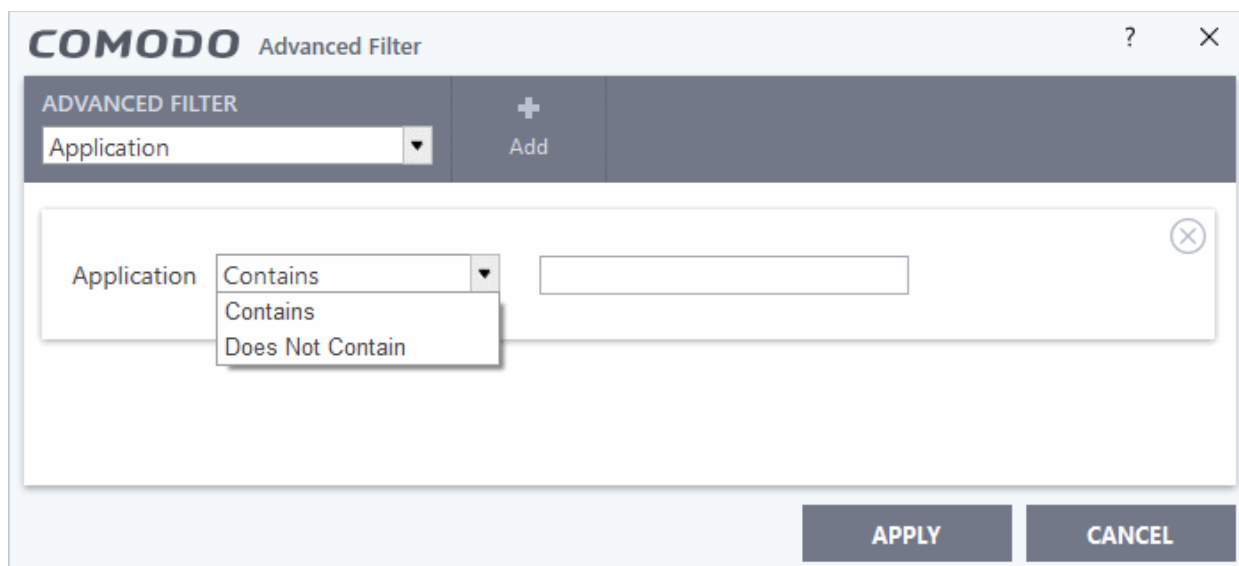
The 'Advanced Filter' interface for containment events will open:



2. Select the filter from the 'Advanced Filter' drop-down then click 'Add' to apply the filter.

There are 6 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

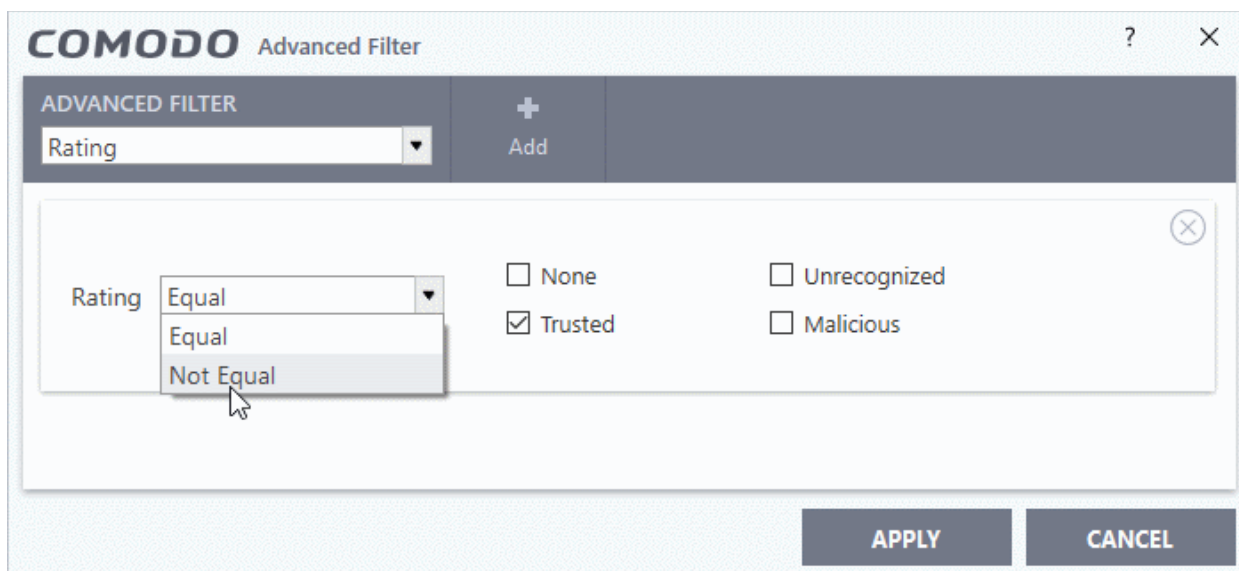
- i. **Application:** Allows you to filter the entries based on name of the contained item. The 'Application' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the search criteria for filtering the logs in the text field.

For example, if you choose 'Contains' and enter the phrase 'pcflank' in the text field, then all events containing the entry 'pcflank' in the 'Application' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'pcflank', then all events that do not have the entry 'pcflank' in the 'Application' column will be displayed.

- c. Repeat the process to add more application filters
- ii. **Rating:** Allows you to filter the entries based on file reputation of the contained item. Selecting the 'Rating' option displays a drop-down menu and set of specific filter parameters that can be selected or deselected.

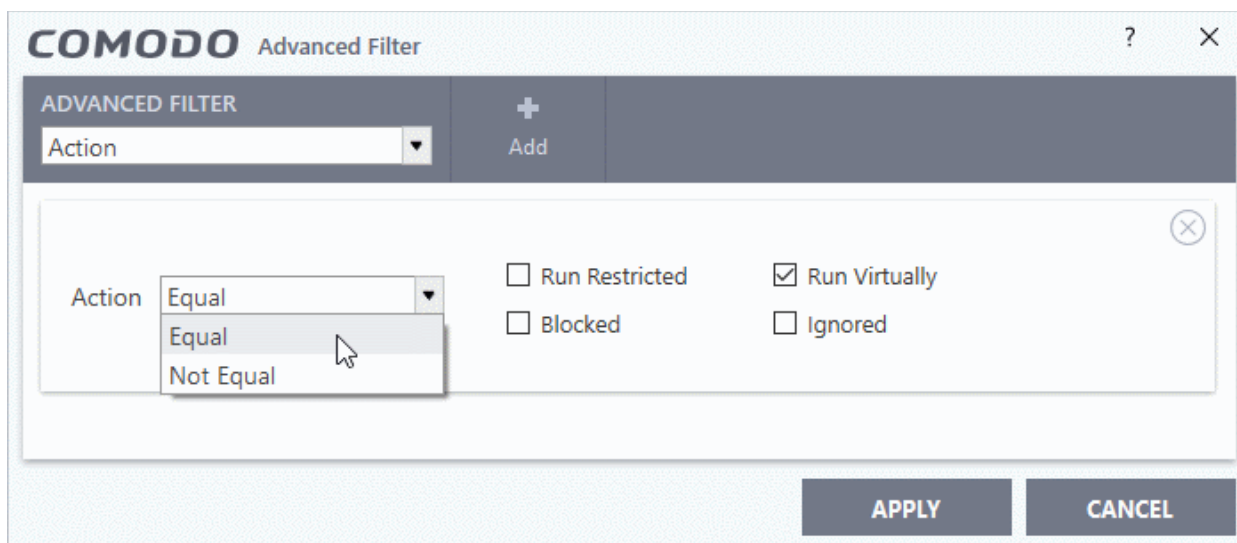


- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - None
 - Unrecognized

- Trusted
- Malicious

For example, if you choose 'Equal' and select the 'Unrecognized' file rating, only the containment events involving applications that are categorized as 'Unrecognized' will be displayed. If you choose 'Not Equal' and choose 'Malicious' file rating, then all events that do not have the entry 'Malicious' in the 'Rating' column will be displayed. You can select more than one file rating from this interface, as required.

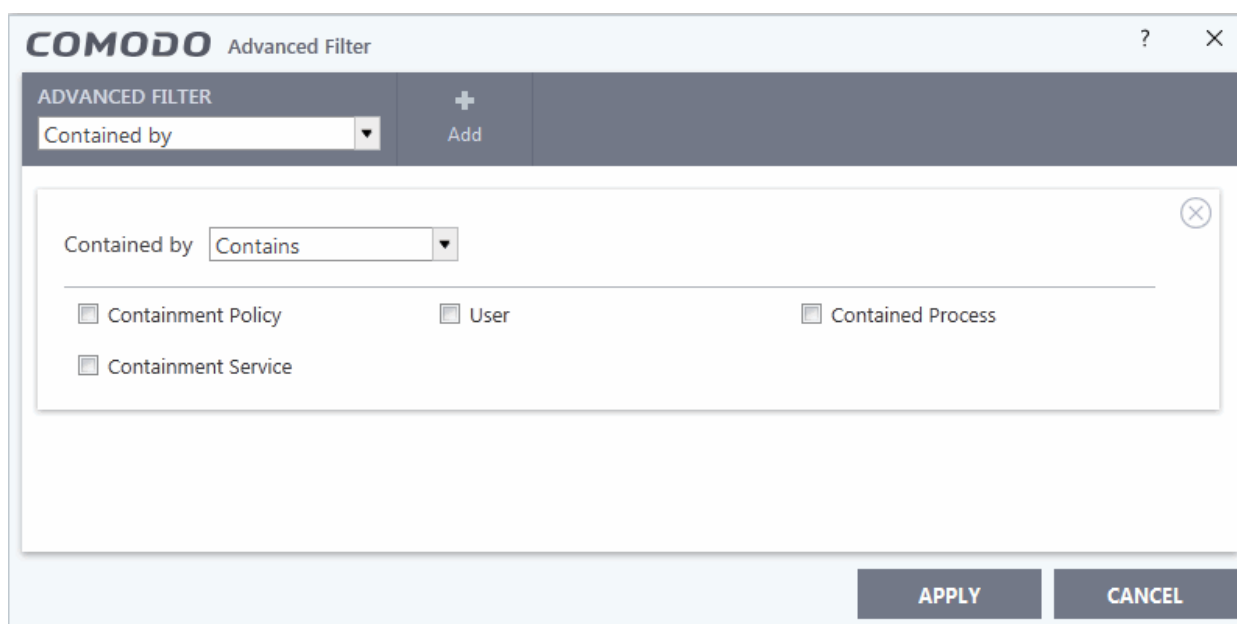
- Repeat the process to add more filters based on file rating
- Action:** Allows you to filter the entries based on containment level imposed on the item. The 'Action' option displays a drop-down menu and a set of specific filter parameters that can be selected or deselected.



- Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- Now select the restriction level(s) applied by the container to the applications, either automatically or as chosen by the user from the alert. The options available are:
 - Run Restricted
 - Run Virtually
 - Blocked
 - Ignored

For example, if you choose 'Equal' from the drop-down and select 'Run Virtually', only the events of applications that are run inside the container will be displayed. If you choose 'Not Equal' and select 'Blocked', then all events that do not have the entry 'Blocked' in the 'Action' column will be displayed. You can select more than one checkbox as required.

- Repeat the process to add more filters based on the action
- Contained by:** Allows you to filter the entries based on CCS service or policy was responsible for running the item inside the containment. Selecting the 'Contained by' option displays a drop-down menu and a set of specific filter parameters that can be selected or deselected.

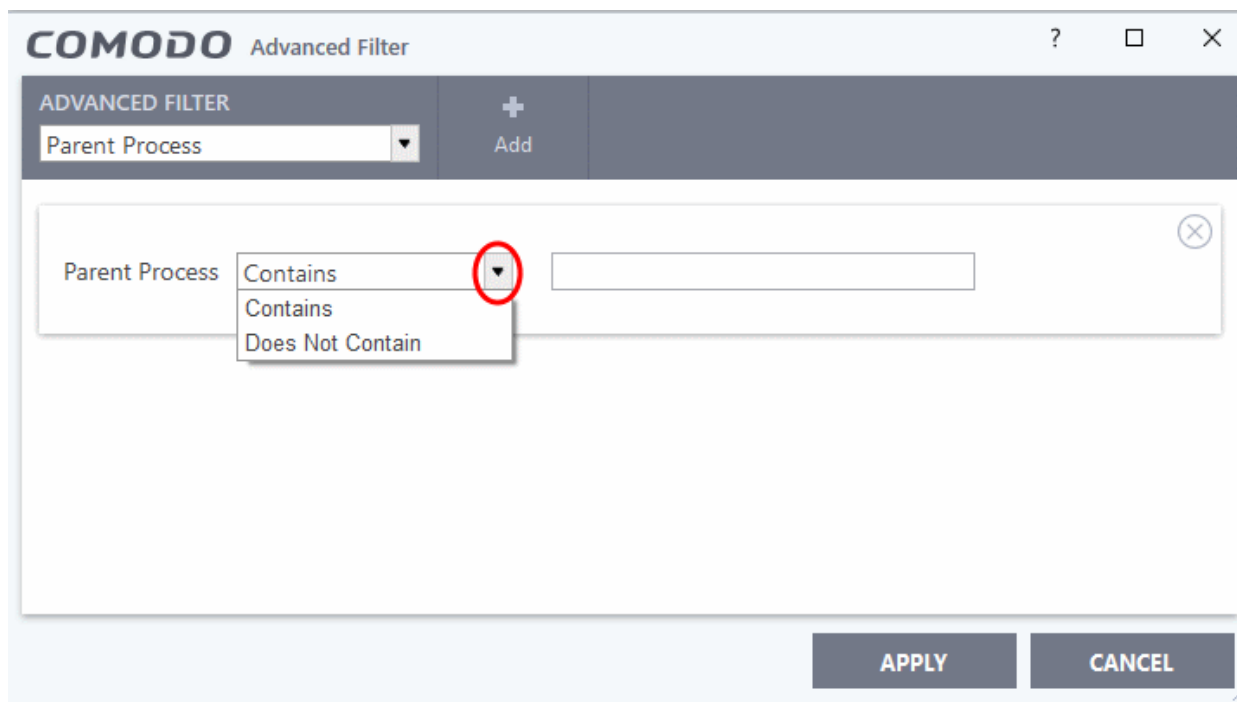


- a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.
- b. To refine your search, select the source(s) by which the applications were contained. The options available are:
 - Containment Policy
 - User
 - Contained Process
 - Containment Service

For example, if you choose 'Contains' and select the 'User' checkbox, then only events involving applications that were manually run inside the container will be displayed. If you choose 'Does Not Contain' and select the 'Containment Policy' checkbox, then all events that do not have the entry 'Containment Policy' in the 'Contained by' column will be displayed. You can select more than one checkbox options from this interface, as required.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

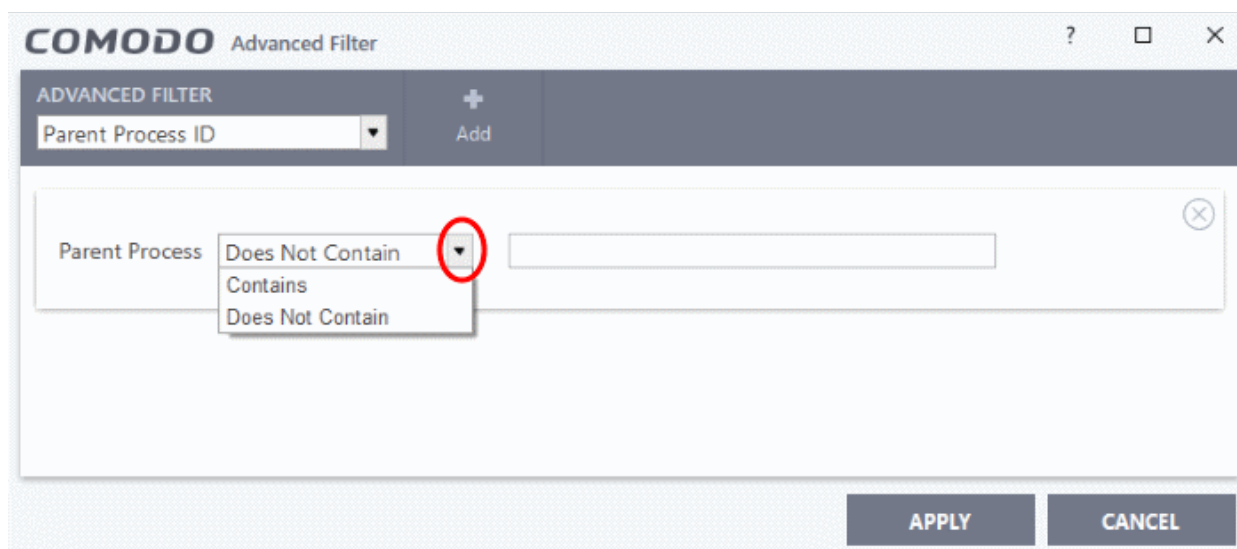
- c. Repeat the process to add more filters based on the CCS service/policy
- v. **Parent process:** Allows you to filter the entries based on the process(es) that launched the contained items. Selecting the 'Parent Process' option displays a drop-down field and text entry field.



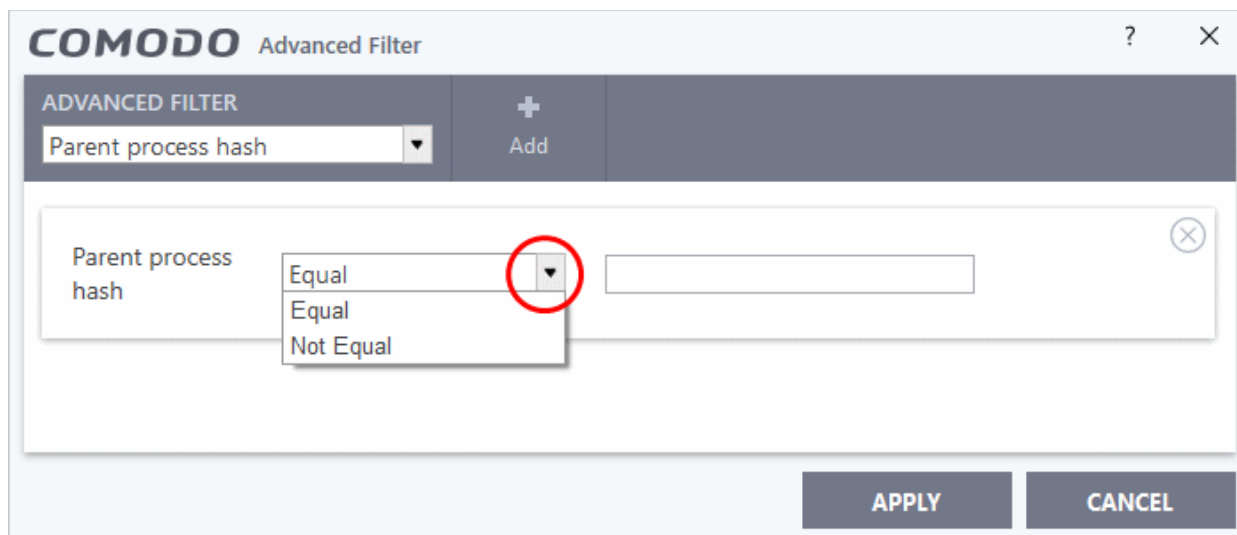
- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the name of the application associated with the process, that launched contained item as the search criteria for filtering the logs in the text field.

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' column will be displayed. If you choose 'Does Not Contain' and enter the phrase 'RuntimeBroker.exe', then all events that do not have the entry 'RuntimeBroker.exe' in the 'Parent Process' column will be displayed.

- c. Repeat the process to add more filters based on the parent process(es).
- vi. **Parent Process ID:** Allows you to filter the entries based on the process(es) ID that launched the contained items. Selecting the 'Parent Process ID' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
- b. Enter the name of the application associated with the process, 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 '2612' in the text field, then all events containing the entry '2612' in the 'Parent Process ID' column will be displayed. If you choose 'Does Not Contain' and enter the phrase '2612', then all events that do not have the entry '2612' in the 'Parent Process ID' column will be displayed.
- c. Repeat the process to add more filters based on the parent process(es).
- vii. **Parent process hash:** Allows you to filter the entries based on the parent process(es) by entering their SHA1 hash values. Selecting the 'Parent process hash' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' from the drop-down menu.
 - b. Enter the SHA1 hash value of the executable file associated with the process, that launched contained item as the search criteria.
 - c. Repeat the process to add more filters based on the parent process(es).
- Click 'Apply' for the filters to be applied to the 'Containment' log viewer. Only those 'Contained' entries selected based on your set filter criteria will be displayed in the log viewer.
 - For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.6. Device Control Logs

The 'Device Control logs' interface lists events related to external devices such as USB drives and optical drives.

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 on how to configure Device control.

Admins can also configure this option in an Endpoint Manager profile. For example, if you want to allow unfettered access to certain devices you can (i) disable device control entirely (ii) remove the device class from the list of controlled types, or (iii) add specific devices to exclusions.

To view 'Device Control' logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs'
- Select 'Device Control Events' from the 'Show' drop-down:

Date	Name	Identifier	Class	State
8/2/2017 3:37:08 PM	USB Input Device	USB\VID_0627&PID_0001\42	745A17A0-74D3-11D0-B6FE-0...	Enabled
8/2/2017 3:37:08 PM	CD-ROM Drive	IDE\CDROMQEMU_QEMU_DVD-ROM_...	4D36E965-E325-11CE-BFC1-0...	Enabled
8/2/2017 3:32:20 PM	USB Input Device	USB\VID_0627&PID_0001\42	745A17A0-74D3-11D0-B6FE-0...	Disabled
8/2/2017 3:32:20 PM	CD-ROM Drive	IDE\CDROMQEMU_QEMU_DVD-ROM_...	4D36E965-E325-11CE-BFC1-0...	Disabled

Column Descriptions

1. **Date** - Date and time of the device control event.
 2. **Name** - The type of task/event.
 3. **Identifier** - Indicates the parameter (like scan type) associated with the task.
 4. **Class** - The device class. Examples include USB, Firewire and Bluetooth.
 5. **State** - Current status of the task.
 6. **Info & Additional Info** - Provides additional information on the task (if available).
- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
 - **'Open log file'** - view a saved log file.
 - **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
 - **'Cleanup log file'** - Deletes all logs from all modules

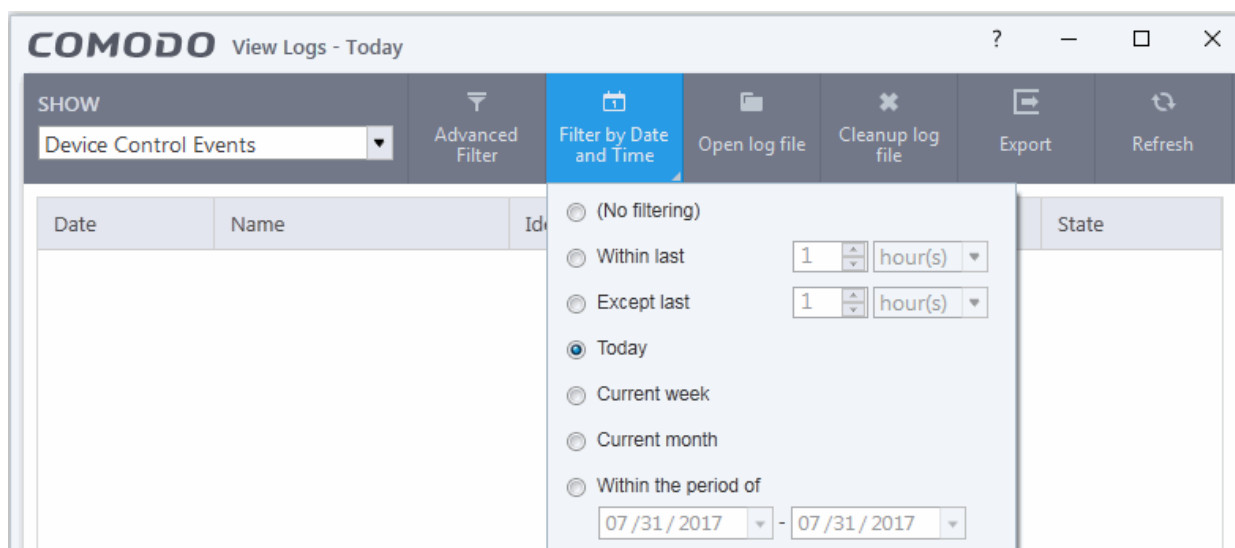
5.4.6.1. Filter 'Device Control' Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

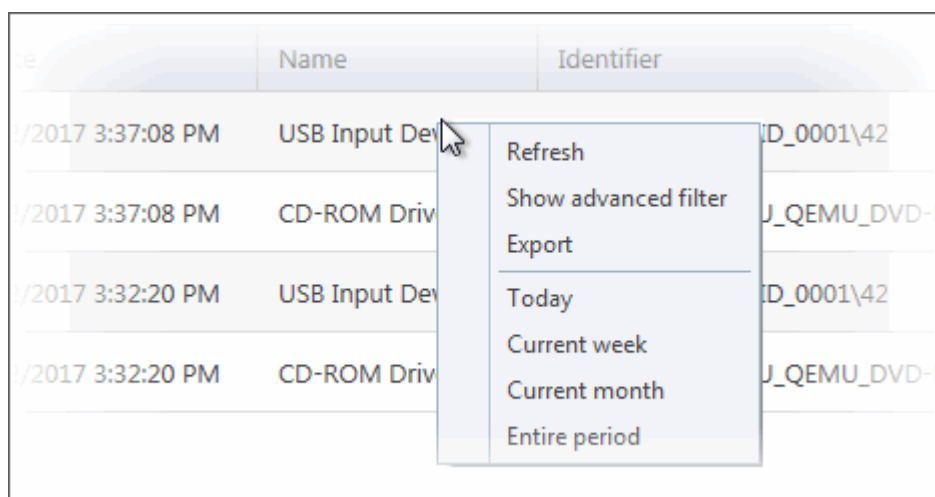
Preset Time Filters

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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

You can further refine the displayed events according to specific filters. Following are available filters for 'Device Control Events' logs and their meanings:

- **Name:** Displays the name of the external device
- **Identifier:** Displays the type of device blocked by CCS
- **Class:** Displays the class of Device such as USB, Firewire and Bluetooth

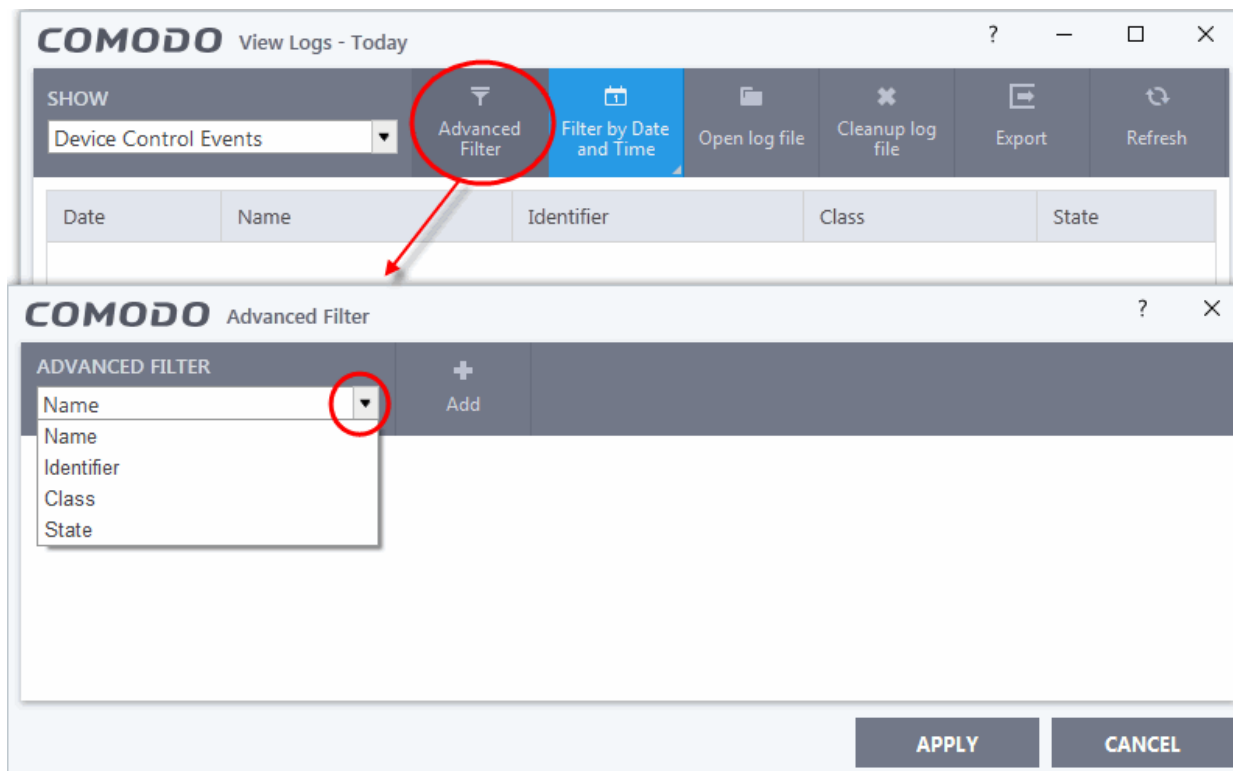
- **State:** Displays the Enabled/Disabled status of Device control

To configure Advanced Filters for Device Control Logs

1. Click the 'Advanced Filter' button from the title bar or right-click inside the log viewer module and choose 'Advanced Filter' from the context sensitive menu.

The 'Advanced Filter' interface for Device control Logs will open:

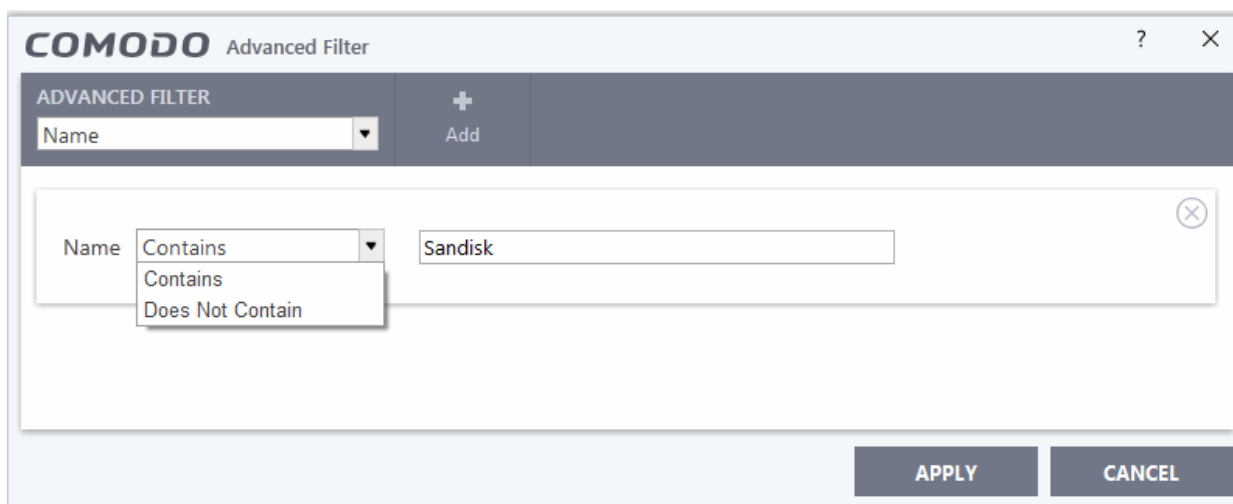
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 3 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

Following are options available in the 'Add' drop-down menu:

- i. **Name:** The 'Name' option enables you to filter log entries related to specific name. Selecting the 'Name' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text of the name that needs to be filtered.

For example, if you select 'Contains' option from the drop-down field and enter 'Sandisk', then all events containing the entry 'Sandisk' in the 'Name' field will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter 'Sandisk' in the text field, then all names that do not have the entry 'Sandisk' in the 'Name' field will be displayed.

- ii. **Identifier:** The 'Identifier' option allows you to filter log entries based on the type/classification of device. Selecting the 'Identifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

The screenshot shows the 'COMODO Advanced Filter' dialog box. At the top, there is a header with the COMODO logo and the text 'Advanced Filter'. Below this, there is a section labeled 'ADVANCED FILTER' with a dropdown menu currently set to 'Identifier'. To the right of this dropdown is a plus sign and the word 'Add'. Below the 'ADVANCED FILTER' section, there is a larger area containing a dropdown menu with 'Contains' selected, and a text input field containing 'USBTOR\DISK'. A dropdown menu is open below the 'Contains' selection, showing 'Contains' and 'Does Not Contain' as options. At the bottom right of the dialog box, there are two buttons: 'APPLY' and 'CANCEL'.

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text of the name that needs to be filtered.

For example, if you select 'Contains' option from the drop-down field and enter 'USBSTORDISK', then all events containing the entry 'USBSTORDISK' in the 'Identifier' field will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter 'USBSTORDISK' in the text field, then all names that do not have the entry 'USBSTORDISK' in the 'Identifier' field will be displayed.

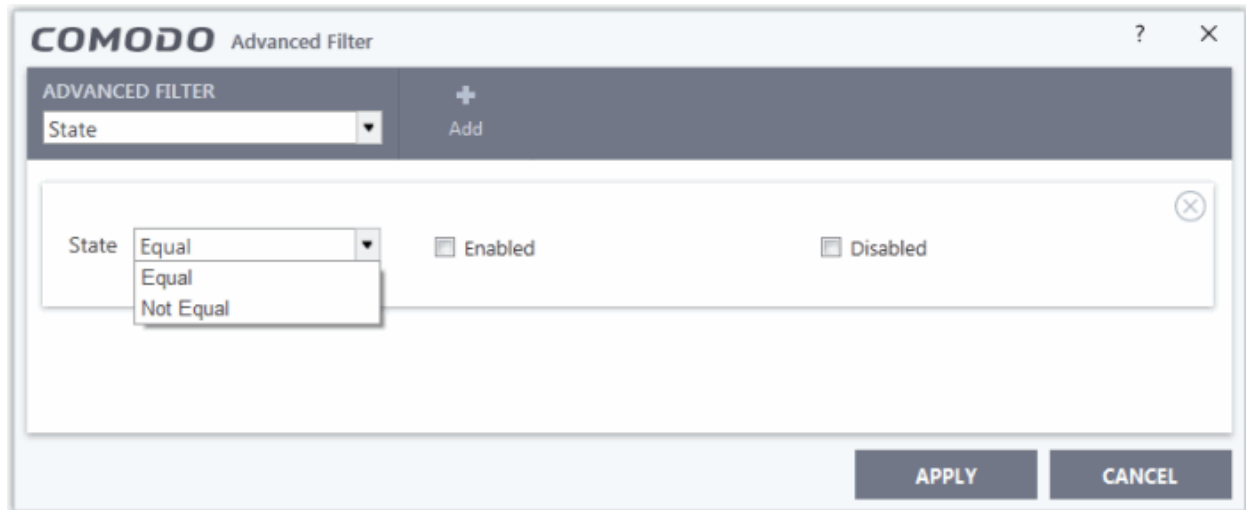
- iii. **Class:** The 'Class' option allows you to filter log entries based on the class of devices. Selecting the 'Class' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

The screenshot shows the 'COMODO Advanced Filter' dialog box. At the top, there is a header with the COMODO logo and the text 'Advanced Filter'. Below this, there is a section labeled 'ADVANCED FILTER' with a dropdown menu currently set to 'Class'. To the right of this dropdown is a plus sign and the word 'Add'. Below the 'ADVANCED FILTER' section, there is a larger area containing a dropdown menu with 'Contains' selected, and a text input field containing '4D36E967'. A dropdown menu is open below the 'Contains' selection, showing 'Contains' and 'Does Not Contain' as options. At the bottom right of the dialog box, there are two buttons: 'APPLY' and 'CANCEL'.

- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text of the name that needs to be filtered.

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 will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter '4D36E967' in the text field, then all names that do not have the entry '4D36E967' in the 'Class' field will be displayed.

iv. **State:** The 'State' option allows you to filter log entries based on the Enabling/Disabling status of the device. Selecting the 'State' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.
- b. Enter the text of the name that needs to be filtered.

For example, if you select 'Contains' option from the drop-down field and enter 'Disabled', then all events containing the entry 'Disabled' in the 'State' field will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter 'Disabled' in the text field, then all names that do not have the entry 'Disabled' in the 'State' field will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Device Control Events' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

5.4.7. Autorun Logs

- The 'Autorun logs' interface shows events where unknown or malicious items were found in registry items for Windows services, auto-start entries and scheduled tasks.

To view 'Autorun Logs' logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs'
- Select 'Auto run Events' from the 'Show' drop-down:

Date & Time	Type	Location	Modifier	Action	Detected By	Status
9/6/2018 3:30:49 PM	Auto Runs	C:\Users\Tester\AppData\Roaming\Microsoft\Windows\Start Menu\Progr...	C:\Windows\explorer.exe	Ignore	Monitor	Success
9/6/2018 3:31:27 PM	Window Services	C:\UnknownApp\UnknownAppUI.exe	C:\Windows\System32\services.exe	Quarantine and Disable	Monitor	Success
9/6/2018 3:32:36 PM	Auto Runs	C:\Users\Tester\AppData\Roaming\Microsoft\Windows\Start Menu\Progr...	Tester	Terminate and Disable	Antivirus Scan	Success
9/6/2018 3:33:22 PM	Scheduled Task	C:\UnknownApp\UnknownAppUI.exe	C:\Windows\System32\svchost.exe	Terminate and Disable	Monitor	Success

- **Date & Time** - Date and time the event occurred.
- **Type** - The category of auto-run event which generated the log. For example, 'Scheduled Task' or 'Windows Service'.
- **Location** - The path of the executable that modified the registry item.
- **Modifier** - Displays change logs made by automatic execution files or a user or an administrator.
- **Action** - The response to the threat as per the settings. The possible actions are:
 - Ignore
 - Terminate
 - Terminate and Disable
 - Quarantine and Disable
- **Detected By** - Security module which identified the threat.
- **Status** - States whether the action was executed successfully or not.

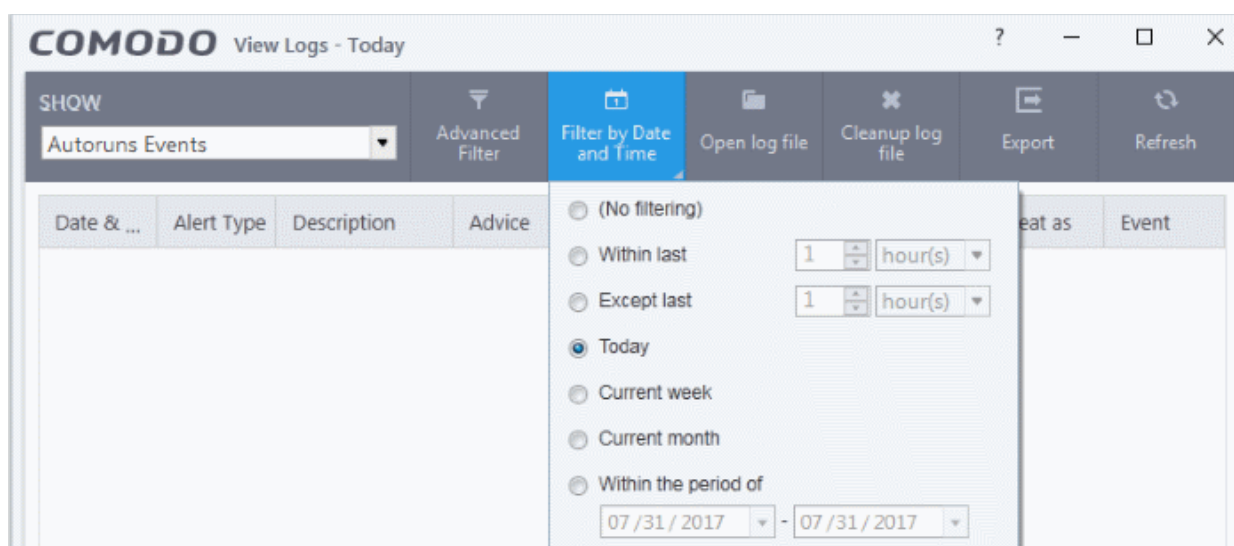
5.4.7.1. Filter 'Autorun' Logs

Comodo Client Security lets you create custom views of all logged events. The following types of filters are available:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

- Click 'Filter by Date and Time' to display logs for a specific time period:

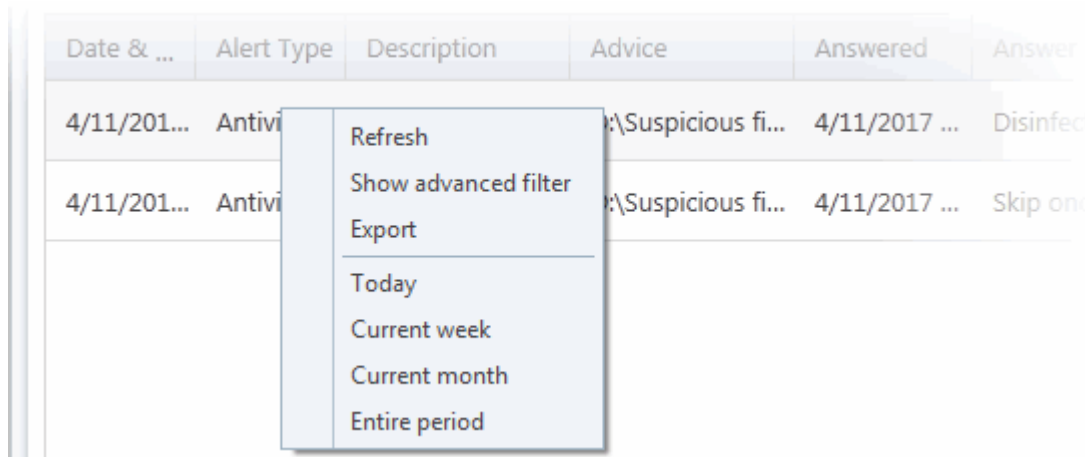


- **No filtering** - Show every event logged since CCS was installed. If you have cleared the logs since

installation, this option shows all logs created since that clearance.

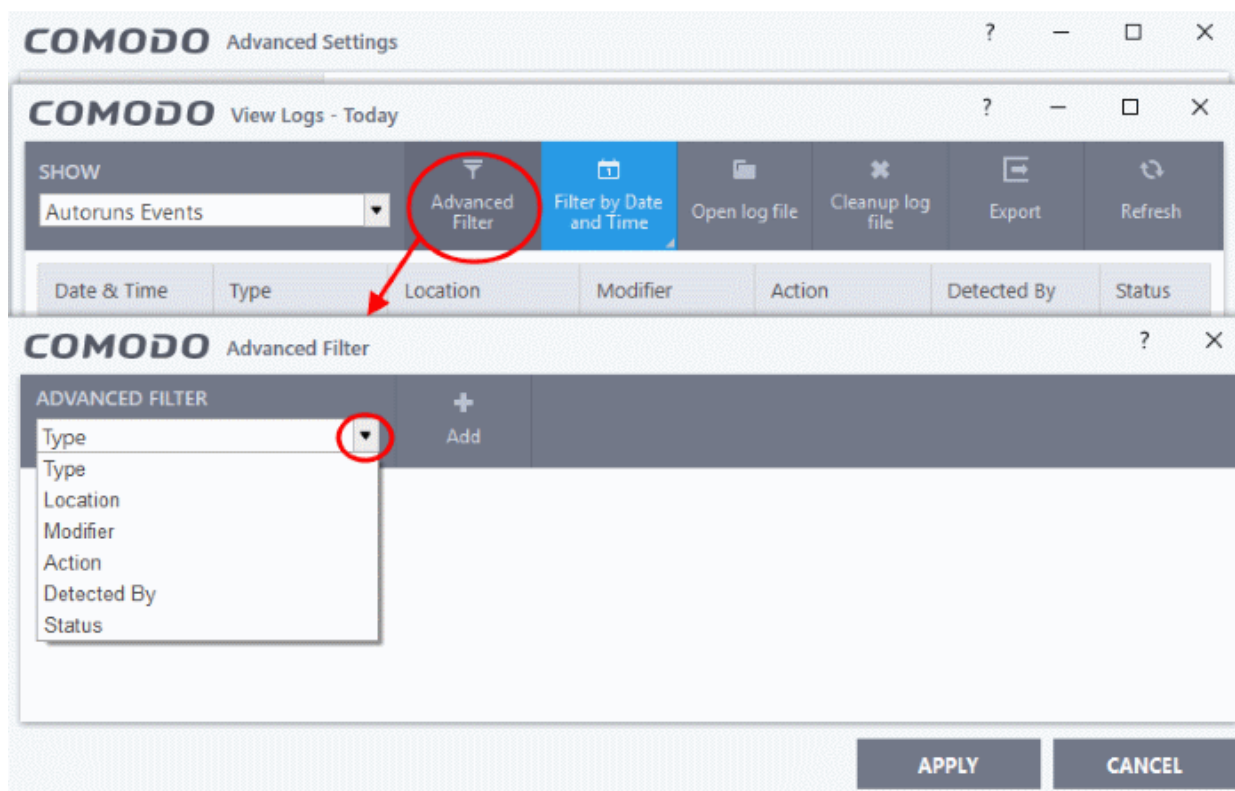
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Show all events logged from 12:00 am today to the current time.
- **Current Week** - Show all events logged 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:



To configure Advanced Filters for Autorun Logs

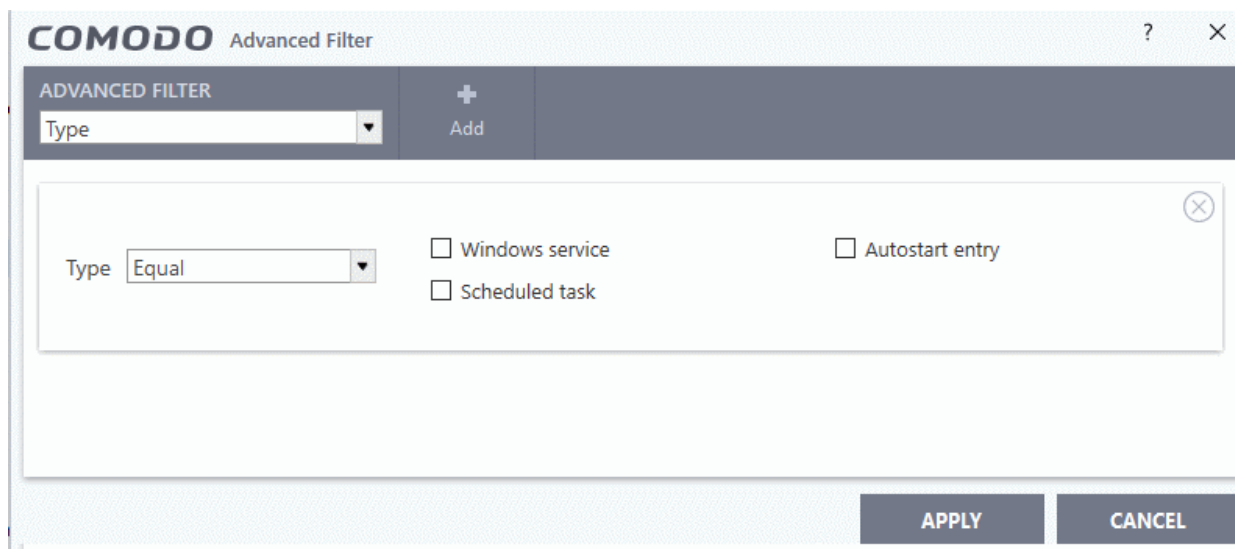
- Click the 'Advanced Filter' button in the title bar OR right-click inside the log viewer module and choose 'Advanced Filter'
- Select the filter you want and click 'Add' to apply it:



- Click the 'Add' button to create a custom filter
- There are 6 categories of filters that you can add. Each of these can be further refined by selecting or deselecting parameters, or by typing a filter string in the field provided.
- You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following are available:

Type: Allows you to filter entries based on the launched tasks. Selecting the 'Type' option displays a drop down box and a set of specific task types that can be selected or deselected.



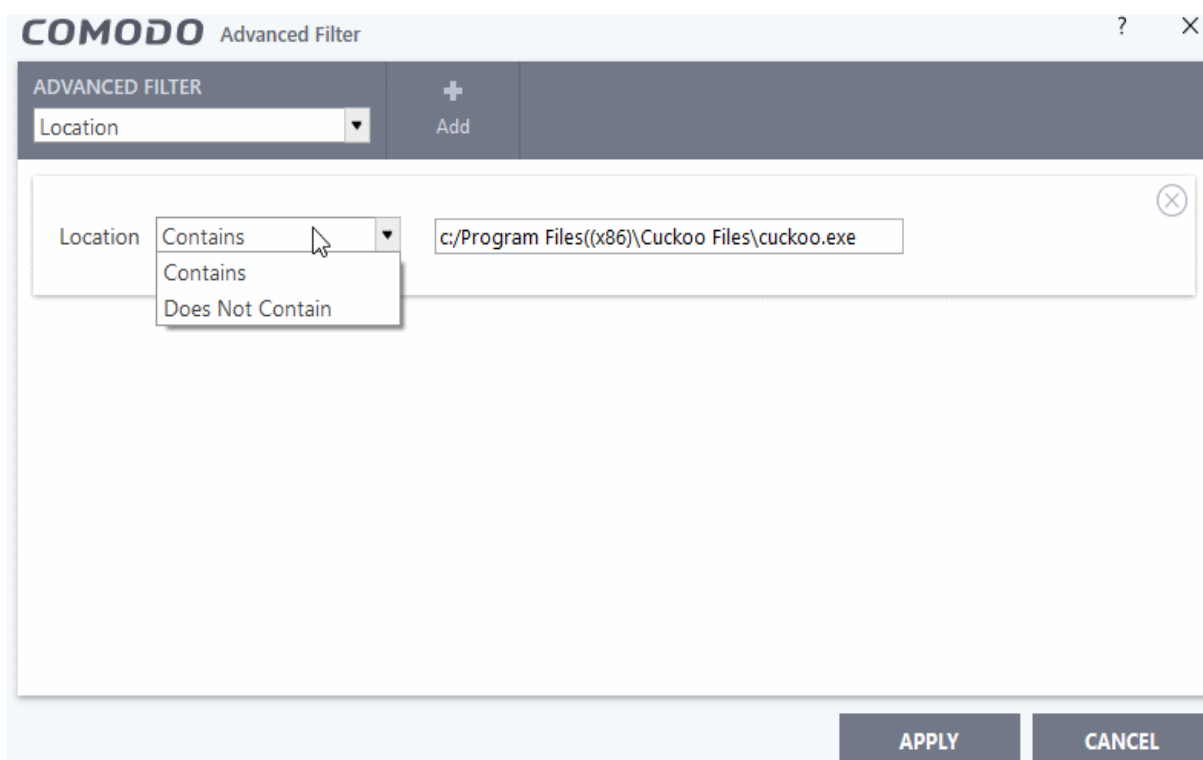
- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Windows Service
 - Autostart entry

- Scheduled task

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

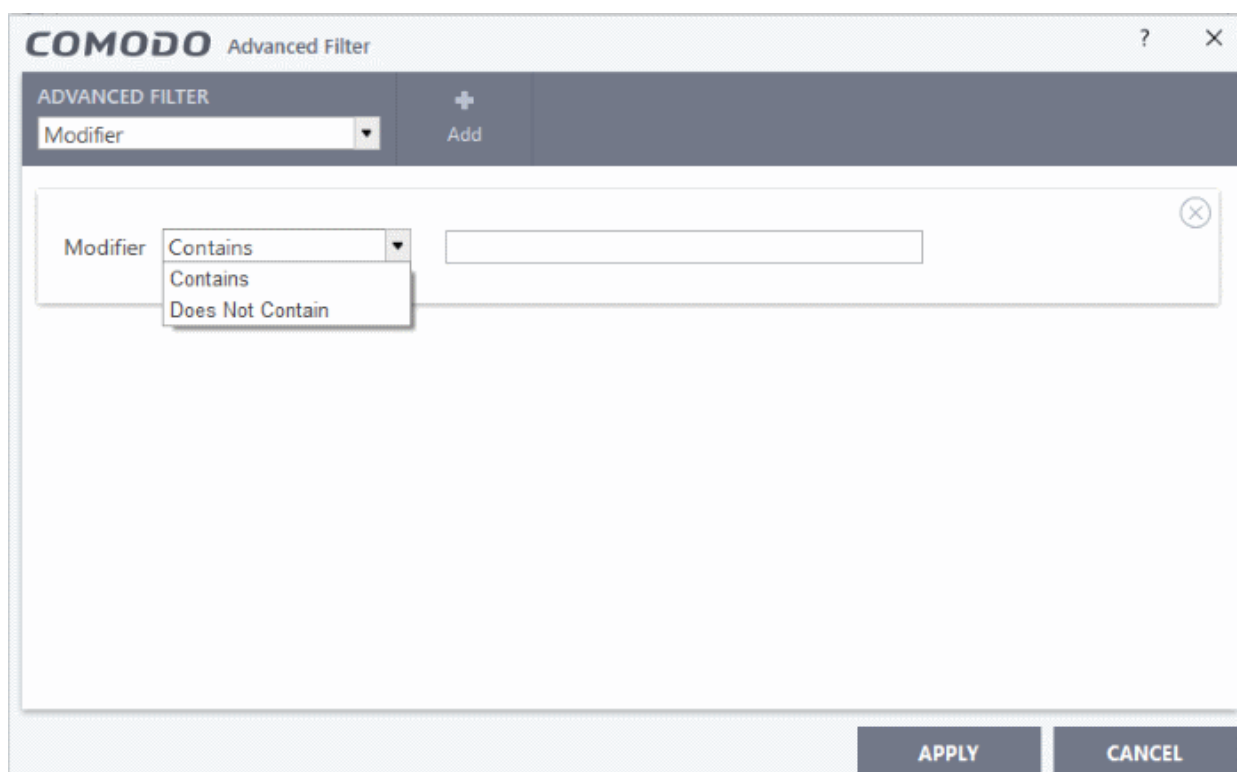
Location: Filter file list changes according to their CCS code. You can view file list changes in the 'Location' column of the log viewer. Selecting the 'Location' option will display drop-down and text entry fields.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Enter the location or a part of it as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'C:/Program Files (x86)/Cuckoo Files/Cuckoo.exe' in the text field, then only log entries with the same value in the 'Path' column will be displayed.

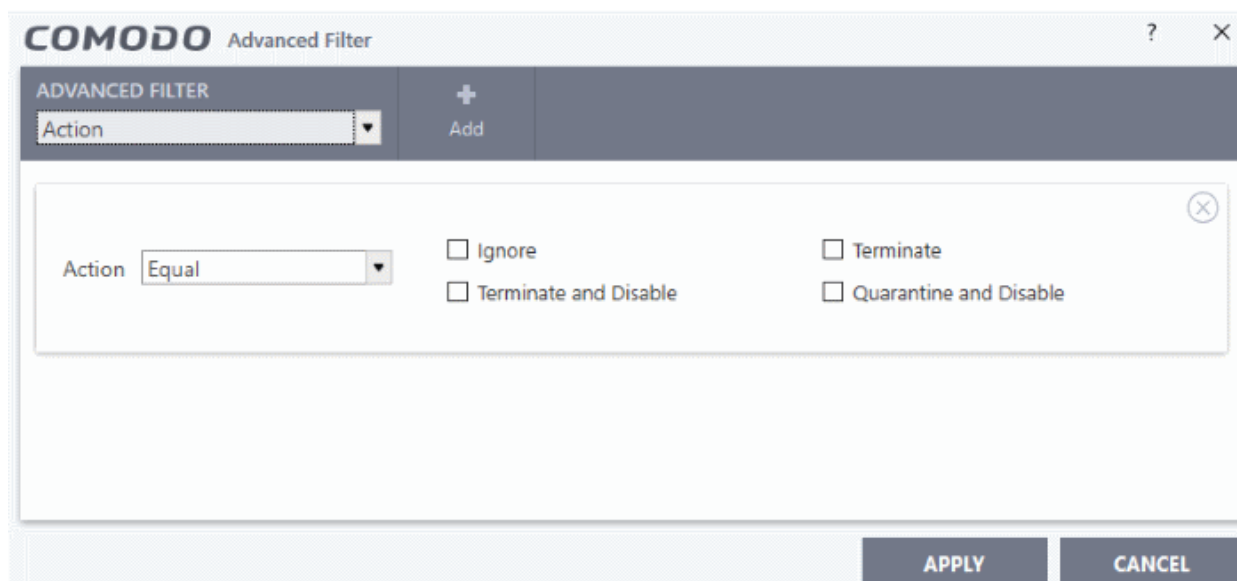
Modifier: Filter log entries based on the file or user that launched the event. Selecting the 'Modifier' option will display drop-down and text entry fields.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Enter the location or a part of it as your filter criteria in the text field.

For example if you 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: The 'Action' option allows you to filter logs based on the actions taken by CCS against the detected threat. To filter logs by CCS action, select 'Action' from the drop-down then click 'Add':

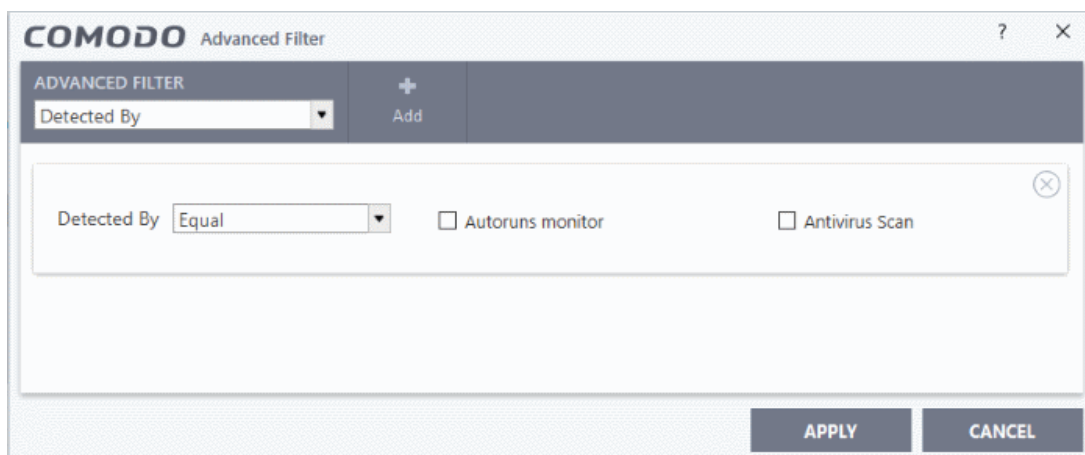


- c. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- d. Now select the check boxes of the specific filter parameters to refine your search. The parameter available

are:

- Ignore - CCS does not take any action
- Terminate - CCS 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, CCS 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, CCS disables the service.

Detected By: The 'Detected By' option allows you to filter logs based on the item that detects or identifies the threat or malware. To filter logs by CCS detected by, select from the drop down box and then choose the detection method.

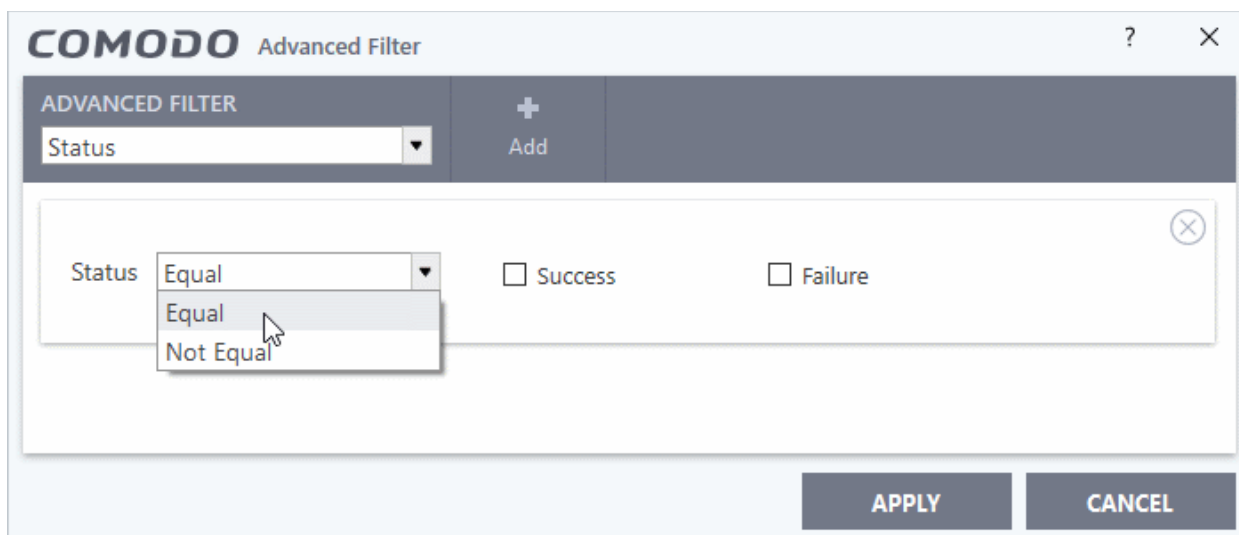


- c) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- d) Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Autorun monitor
 - Antivirus Scan

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

Status: The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by CCS. Selecting the 'Status' option displays a drop-down field and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - Success: Displays events where the actions against the detected threat were successful. For example, the malware was successfully quarantined.
 - Failure: Displays events where the intended actions against the detected threat were not successful. For example, the malware was not disinfected.

Note: Multiple filters can be added in the 'Advanced Filter' pane. After adding a filter, select the next filter type and click 'Add'. You can remove filters by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the VirusScope log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

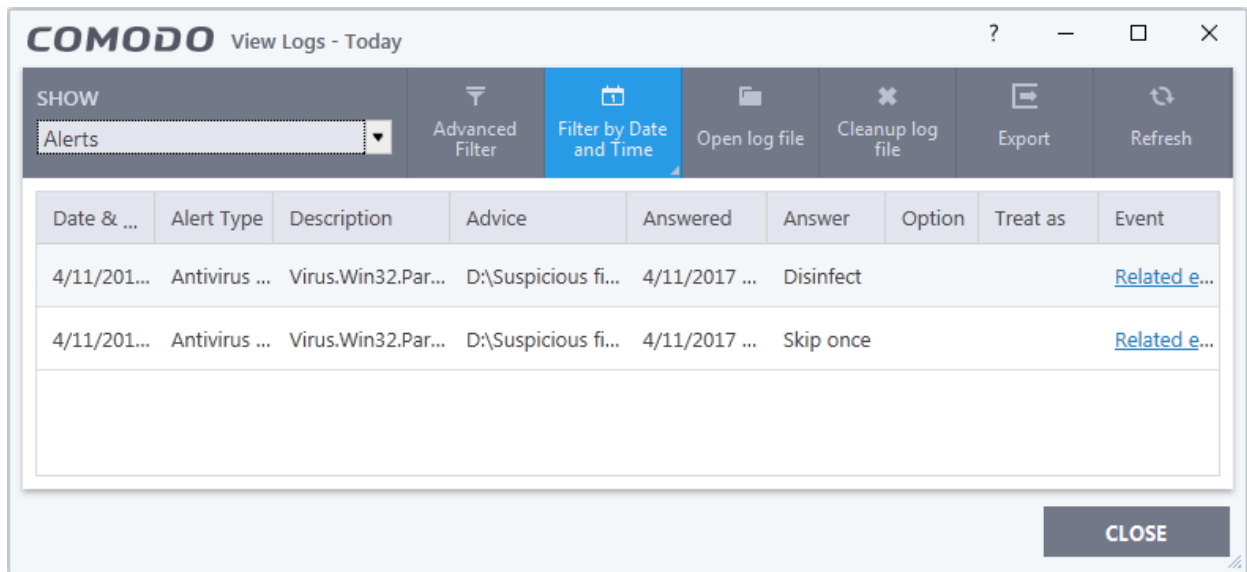
For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.8. 'Alerts' Logs

CCS maintains a history of pop-up security alerts generated by its antivirus and advanced protection components. Each log contains the name of the threat and states how the customer answered the alert.

To view 'Alert' Logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' then select 'View Logs'
- Select 'Alerts' from the 'Show' drop-down:



Column Descriptions

1. **Date & Time** - Date and event time that the alert was generated.
2. **Alert Type** - The type of the alert (antivirus, firewall, HIPS, Containment, VirusScope).
3. **Description** - Brief description of the file or the event that triggered the alert.
4. **Advice** - Advice offered by CCS on how to respond to the alert.
5. **Answered** - Indicates whether the alert has been answered by the user. If answered, you will see the date and time of the response.
6. **Answer** - The response given by the user. For example, allow, block, disinfect, or skip.
7. **Options** - Any additional options chosen by the user at the alert. For example, if the user has chosen 'Remember My Answer' at the alert.
8. **Treat As** - Whether the user told CCS to handle the file in accordance with an application category. For example, treat as a safe application, installer etc.
9. **Event** - Click 'Related Event' link to view details of the event that triggered the alert.
 - **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
 - **'Open log file'** - view a saved log file.
 - **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
 - **'Cleanup log file'** - Deletes all logs from all modules

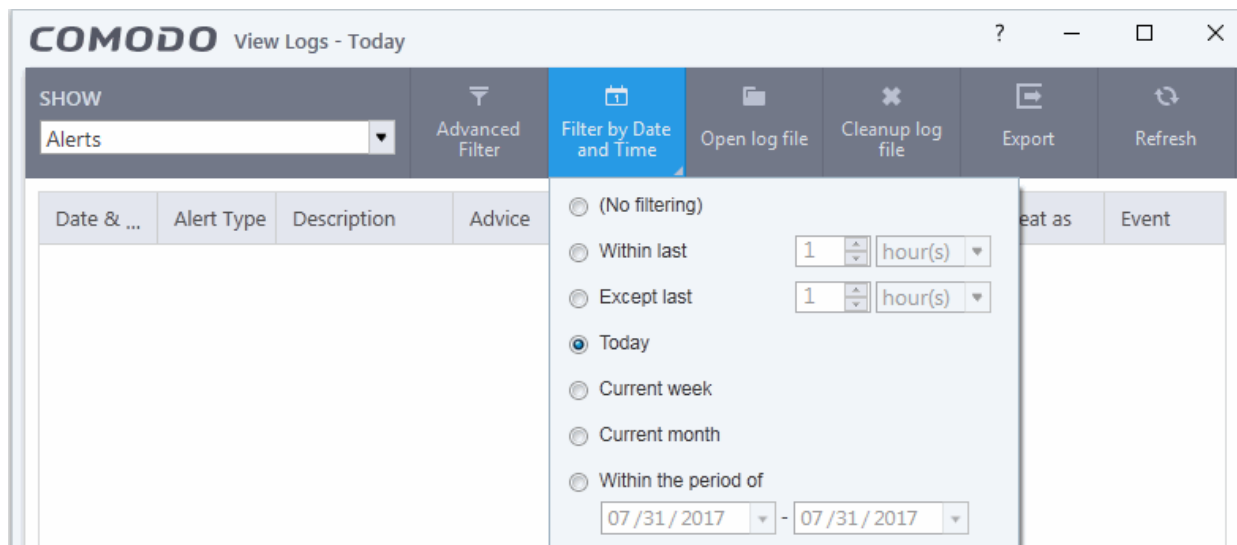
5.4.8.1. Filter 'Alerts' Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

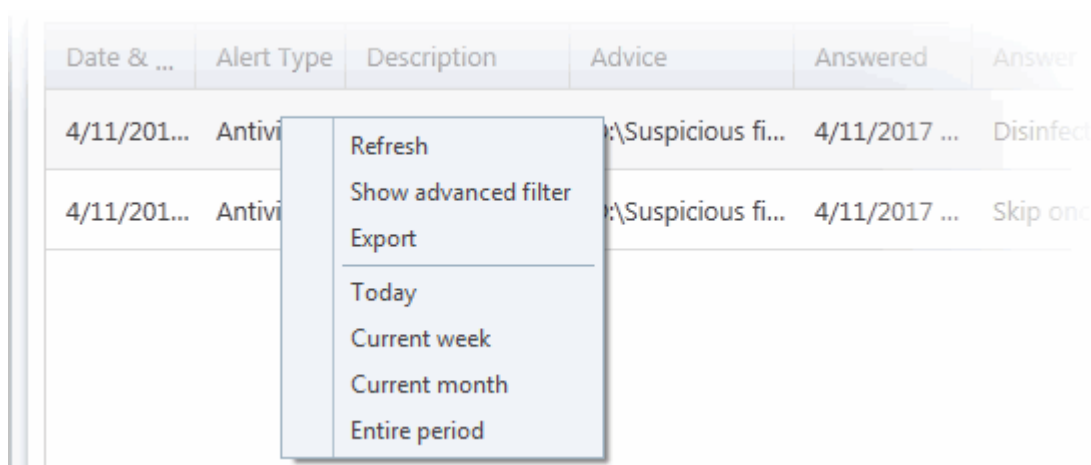
Preset Time Filters

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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

You can further refine which events are displayed according to specific filters. The following filters are available:

- **Advice:** Displays only alerts that match the advice entered.
- **Answer:** Displays only alerts that were answered by the user.

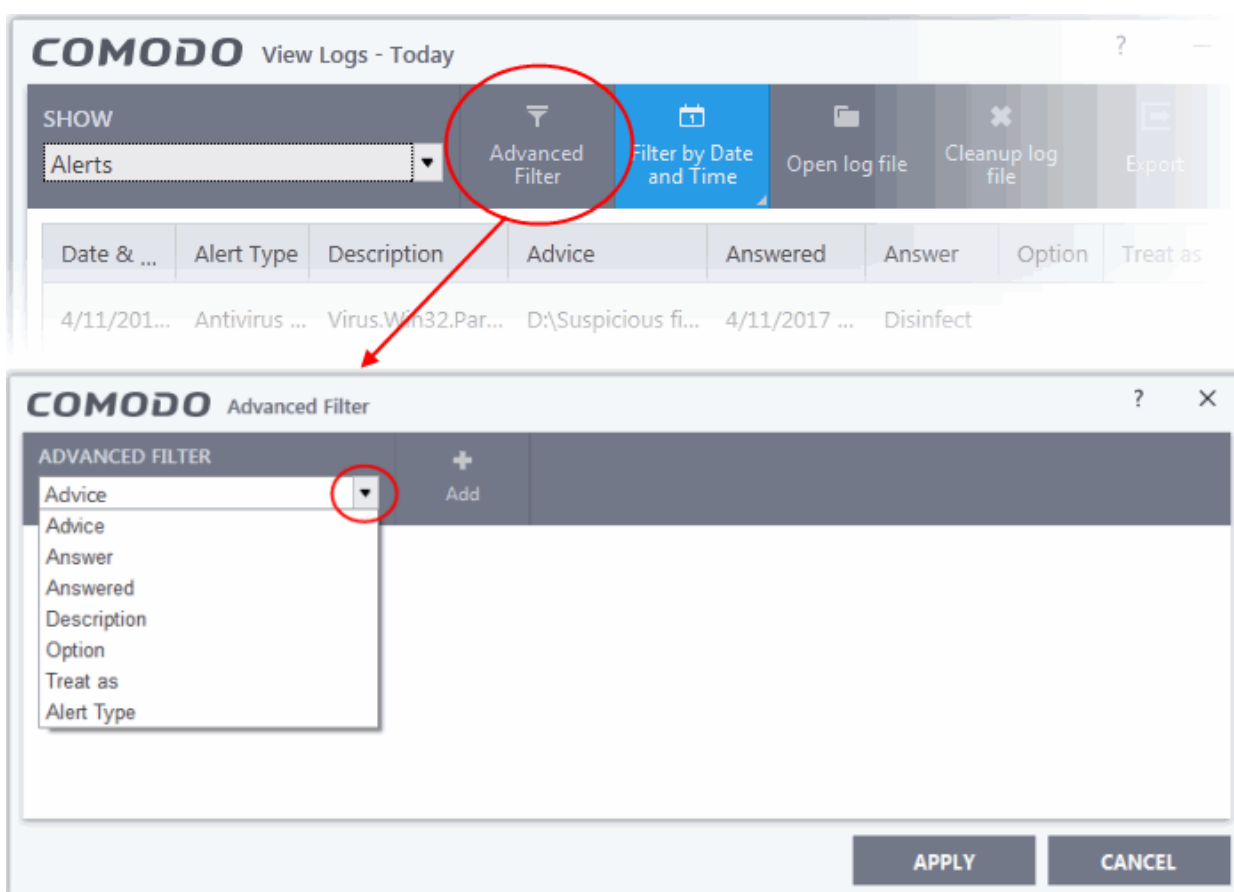
- **Answered:** Displays only alerts that were answered at a specific date and time.
- **Description:** Displays only alerts that match the description entered
- **Option:** Displays only alerts where the user selected an additional option at the alert. Addition options include 'Remember my answer'.
- **Treat As:** Displays only alerts where a 'Treat As' option was chosen by the user. For example, 'treat as a safe application', 'treat as an installer' and so on.
- **Alert Type:** Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope).

To configure Advanced Filters for Alerts Displayed

1. Click the 'Advanced Filter' button on the title bar or right-click inside the log viewer module and choose 'Show advanced filter' from the context sensitive menu.

The 'Advanced Filter' interface for 'Alerts' logs will open:

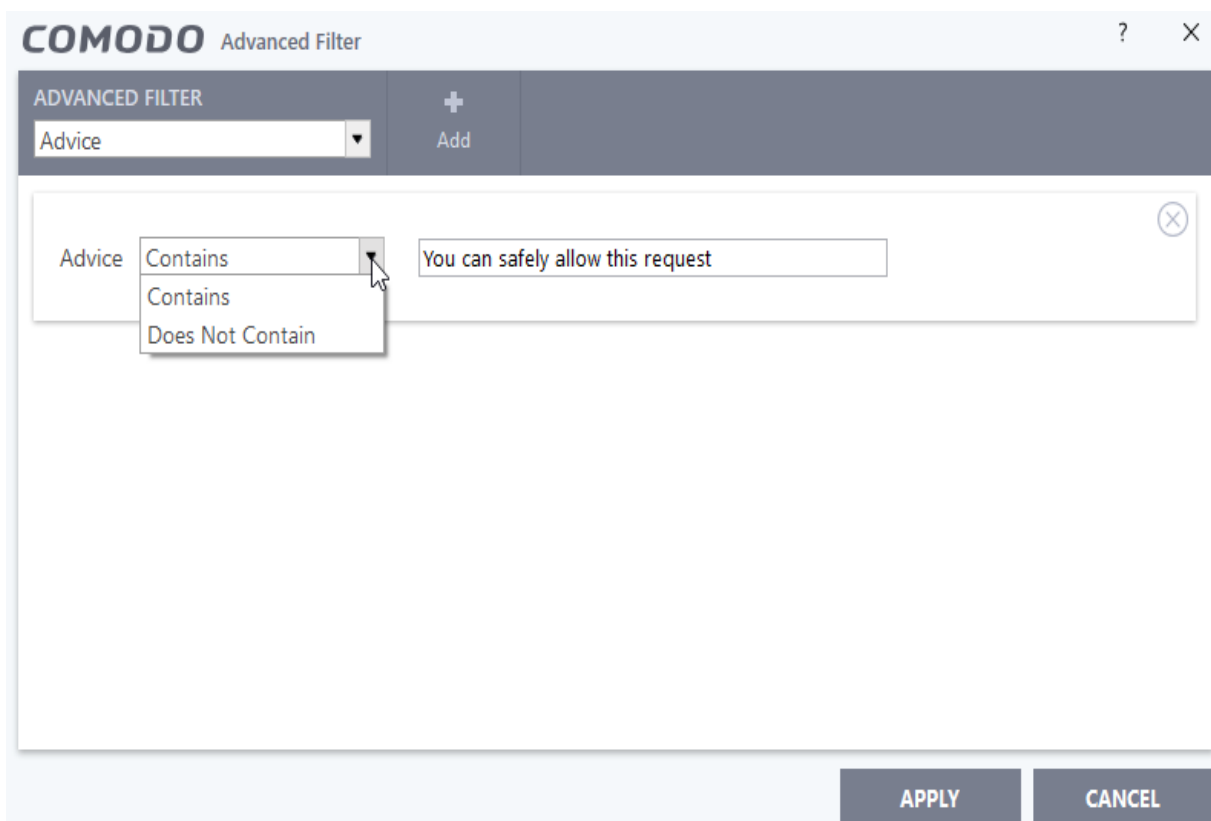
2. Select a filter from the 'Advanced Filter' drop-down and click 'Add'



There are 7 categories of filters that you can add. Each of these categories can be further refined by selecting specific parameters or by typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

The following options available in the 'Add' drop down menu:

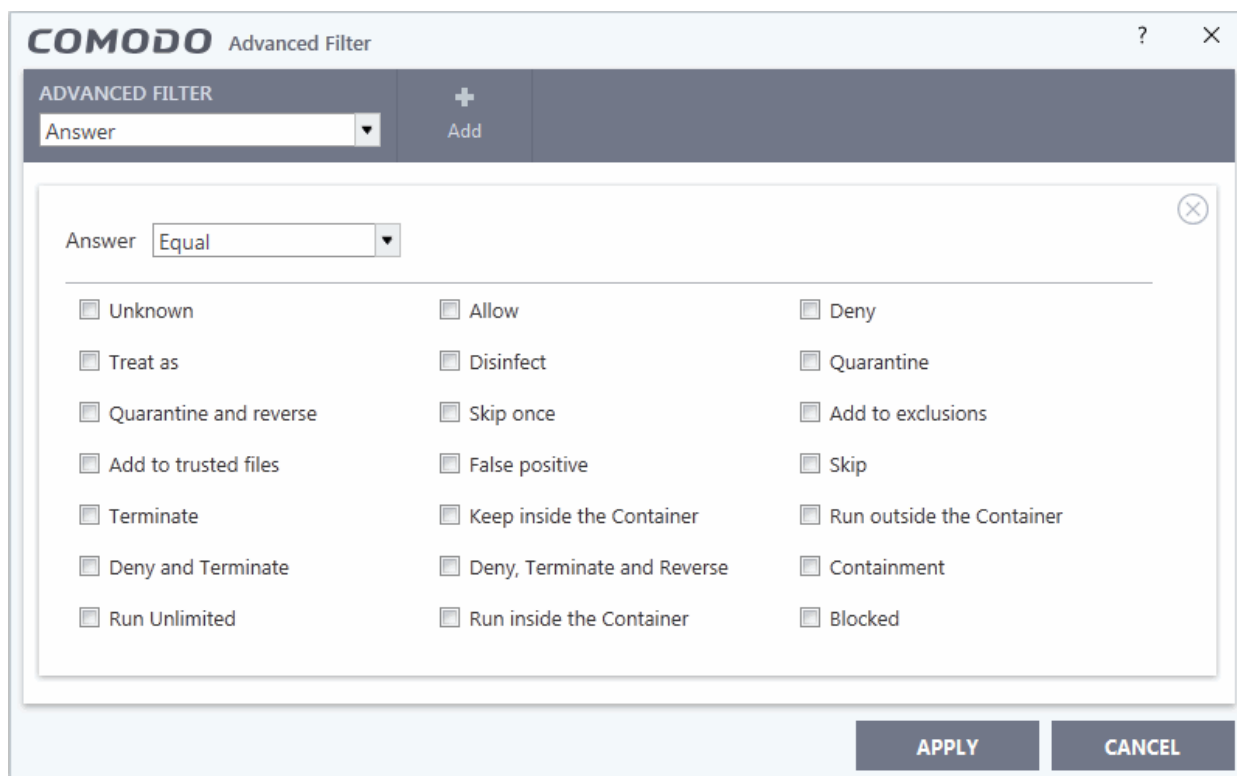
- i. **Advice:** Filter alerts based on the recommendations given by CCS in the alert. Selecting the 'Advice' option will display drop-down and text entry fields.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you choose 'Contains' and enter the phrase 'you can safely allow this request' in the text field, then only entries containing 'you can safely allow this request' in the 'Advice' column will be displayed.

- i. **Answer:** Allows you to filter alerts based on what action the user selected at the alert. Selecting the 'Answer' option displays a drop-down box and a set of answers that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the responses to refine your search. The options available are:
 - Unknown
 - Allow
 - Deny
 - Treat as
 - Disinfect
 - Quarantine
 - Quarantine and reserve
 - Skip once
 - Add to exclusions
 - Add to trusted files
 - False positive
 - Skip
 - Terminate
 - Keep inside the Container
 - Run outside the Container
 - Deny and Terminate
 - Deny, Terminate and Reverse
 - Containment
 - Visit with Secure Browser
 - Run Unlimited
 - Run inside the Container
 - Blocked

For example, if you choose 'Equal' from the drop-down and select the 'Add to exclusions' checkbox, only the alerts where you answered 'Ignore' > 'Ignore and Add to exclusions' will be displayed.

- iii. **Answered:** The 'Answered' option enables you to filter logs based on the date you answered the alerts. Selecting the 'Answered' option displays a drop-down box and date entry field.

The screenshot shows the 'COMODO Advanced Filter' dialog box. It features a title bar with the COMODO logo and window controls. Below the title bar is a dark grey bar containing the text 'ADVANCED FILTER' and an '+ Add' button. A dropdown menu is set to 'Answered'. The main area is white and contains a second dropdown menu set to 'Answered' and a date dropdown set to '07/31/2017'. A calendar for July 2017 is displayed, with the 31st highlighted. At the bottom right, there are 'APPLY' and 'CANCEL' buttons.

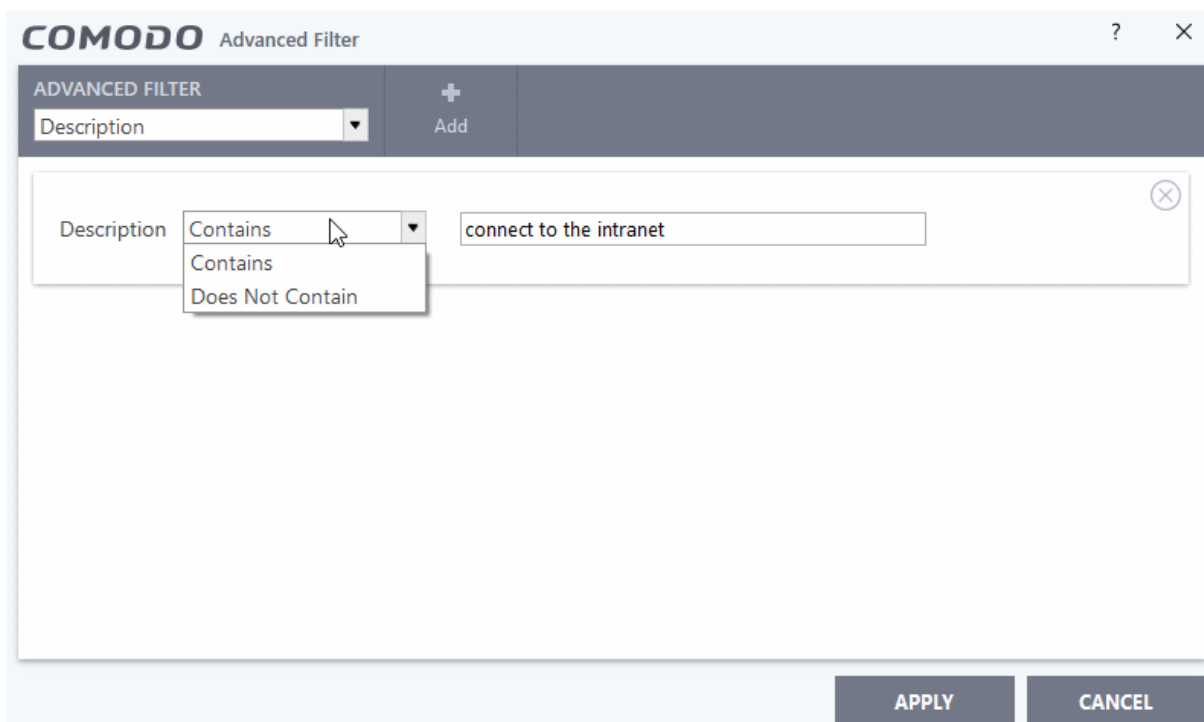
- a. Select any one of the following option the drop-down.

- Equal
- Not Equal

- b. Select the required date from the drop-down calendar.

For example, if you select 'Equal' and select '07/31/2017', only alerts answered on 07/31/2017 will be displayed.

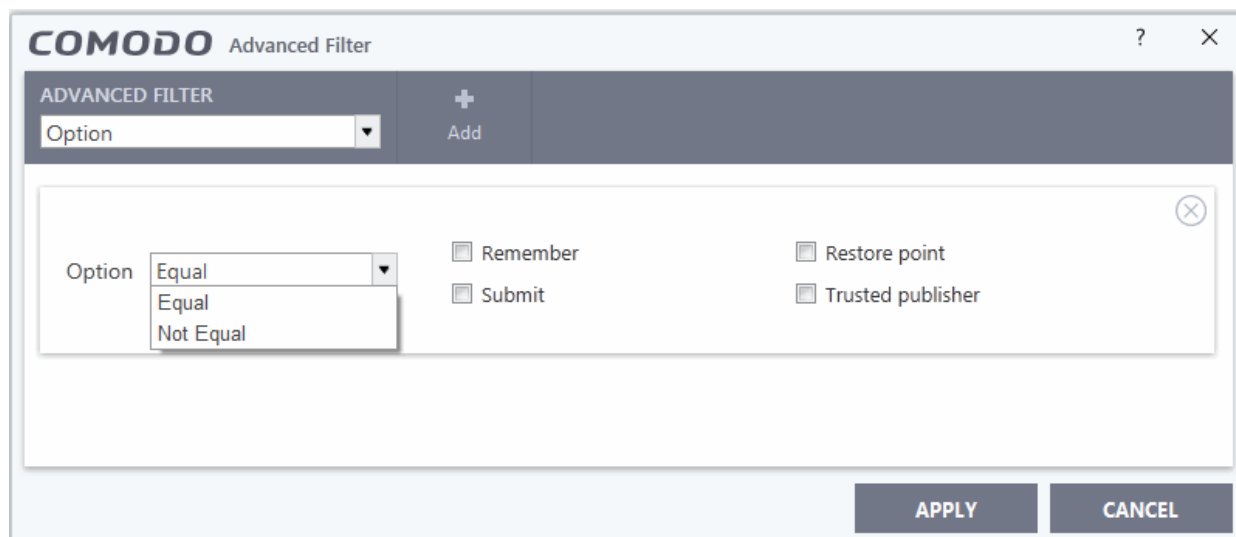
- iv. **Description:** The 'Description' option enables you to filter logs based on the description of the attempt displayed in the alert. Selecting the 'Description' option displays a drop-down field and text entry fields.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you select 'Contains' from the drop-down and enter 'connect to the Internet', only the log entries of Firewall alerts that contain the phrase 'connect to the Internet' in the description, will be displayed.

- v. **Option:** Displays only alerts where the user selected an additional options like 'Remember my answer', 'Submit as False Positive' from the alert.

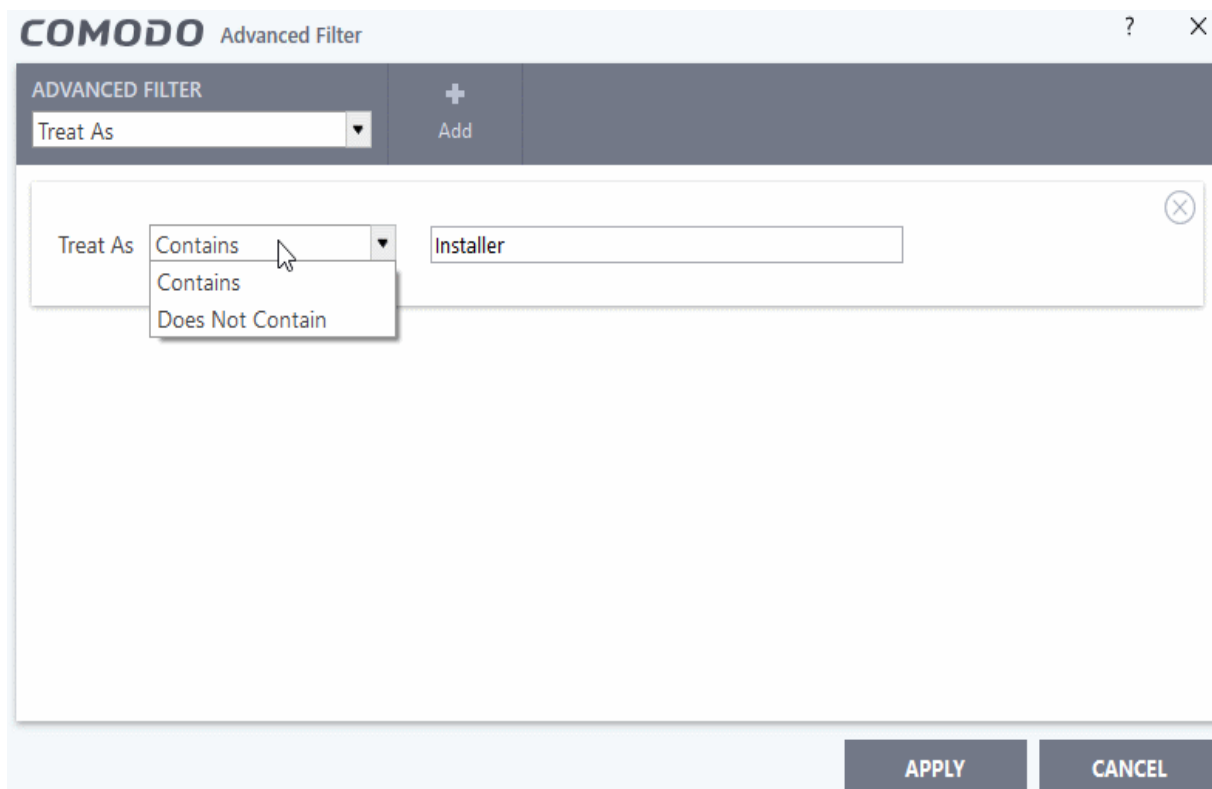


- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Remember
 - Restore point

- Submit
- Trusted publisher

For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected will be displayed.

- vi. **Treat As:** Displays only alerts where a 'Treat As' option was chosen by the user. For example, 'treat as a safe application', 'treat as an installer' and so on.

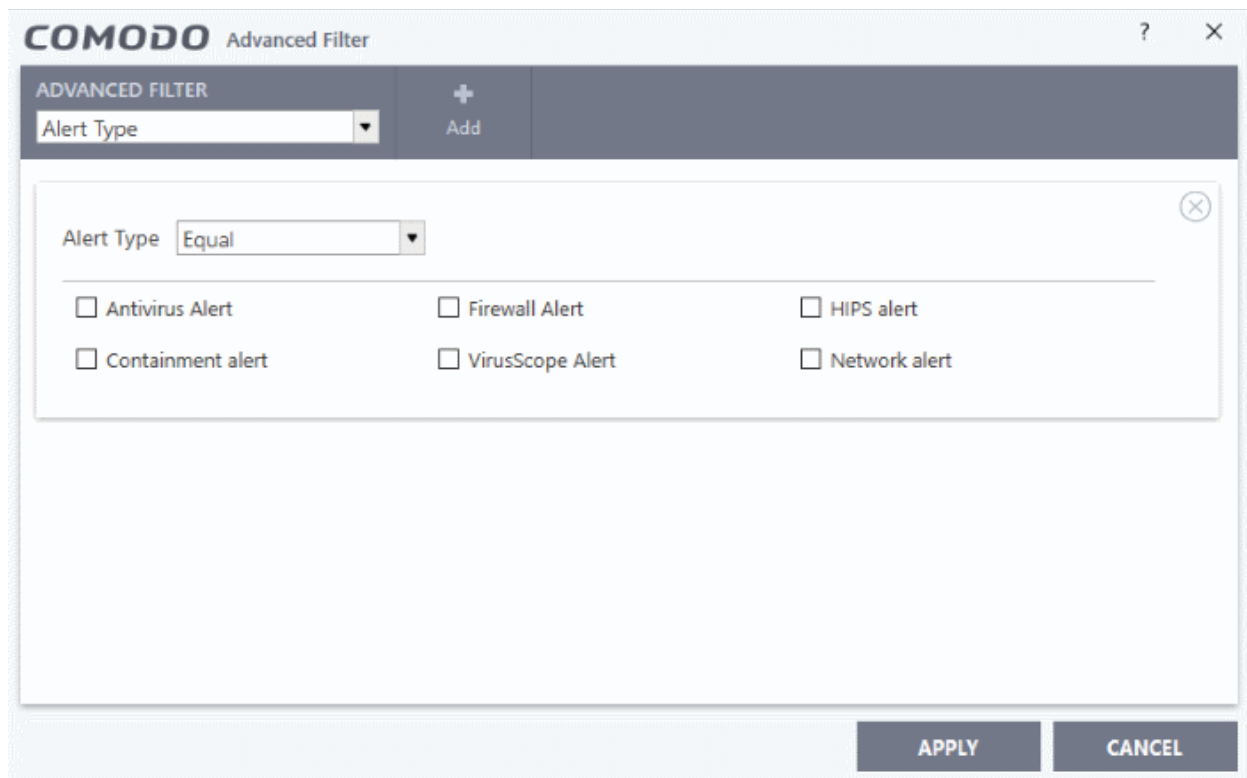


- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu
- b. Enter the text or word as your filter criteria

For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the log entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.

- vii. **Alert Type:** The 'Type' option enables you to filter the entries based on the component of CCS that has triggered the alert. Selecting the 'Type' option displays a drop-down menu and set of specific alert types that can be selected or deselected.

Indicates the type of the alert (antivirus, firewall, HIPS, containment, VirusScope).



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Antivirus Alert
 - Firewall Alert
 - HIPS alert
 - Containment alert
 - VirusScope Alert
 - Network alert

For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of Antivirus alerts will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Alerts' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.9. CCS Tasks Logs

Comodo Client Security keeps a record of all CCS tasks like virus signature database updates, scans run and so on. The 'Tasks' log window displays a list of all tasks launched along with their completion status and other details.

To view 'CCS Task' Logs

- Click 'Tasks' at the top left of the CCS screen

- Click 'Advanced Tasks' > 'View Logs':
- Select 'Tasks' from the 'Show' drop-down:

Date & ...	Type	Parameter	Completed	Code	Info	Additio...
8/1/2017...	Antivirus scan	Quick Scan				
8/1/2017...	Antivirus update		8/1/2017 2:35:30 AM		Old database 2...	New data...
8/1/2017...	Antivirus update		8/1/2017 1:44:48 AM		Old database 2...	New data...
7/31/201...	Antivirus update		7/31/2017 6:41:47 AM		Old database 2...	New data...
7/31/201...	Antivirus update		7/31/2017 5:44:26 AM		Old database 2...	New data...
7/31/201...	Antivirus update		7/31/2017 3:41:47 AM		Old database 2...	New data...
7/31/201...	Antivirus update		7/31/2017 2:43:09 AM		Old database 2...	New data...
7/31/201...	Antivirus update		7/31/2017 2:42:37 AM		Old database 2...	New data...

4. Column Descriptions

1. **Date & Time** - Date and time when the alert was generated.
 2. **Type** - The type of a task.
 3. **Parameter** - Parameter (like scan type) associated with the task.
 4. **Completed** - Date and time that the task finished.
 5. **Code** - Error code generated by Windows operating system for CCS tasks that were not completed successfully. No code will be generated if the tasks that were completed successfully.
 6. **Info & Additional Info** - Additional information about the task. For example, if the task is to update the version of CCS then these fields will show the old version number and the new version number.
- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
 - **'Open log file'** - view a saved log file.
 - **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
 - **'Cleanup log file'** - Deletes all logs from all modules

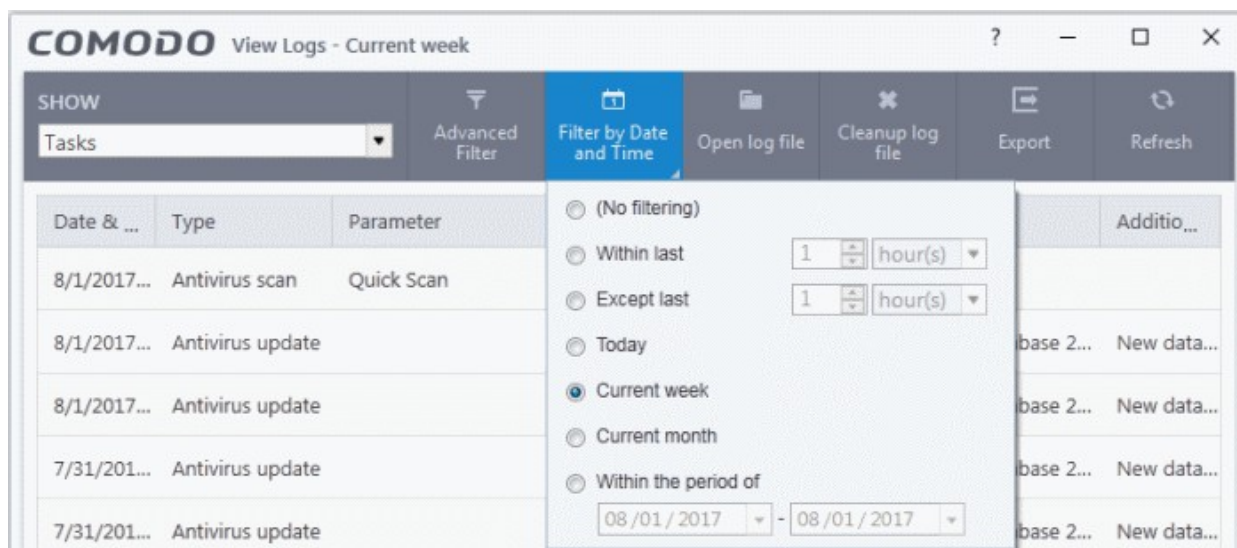
5.4.9.1. Filter 'Tasks' Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

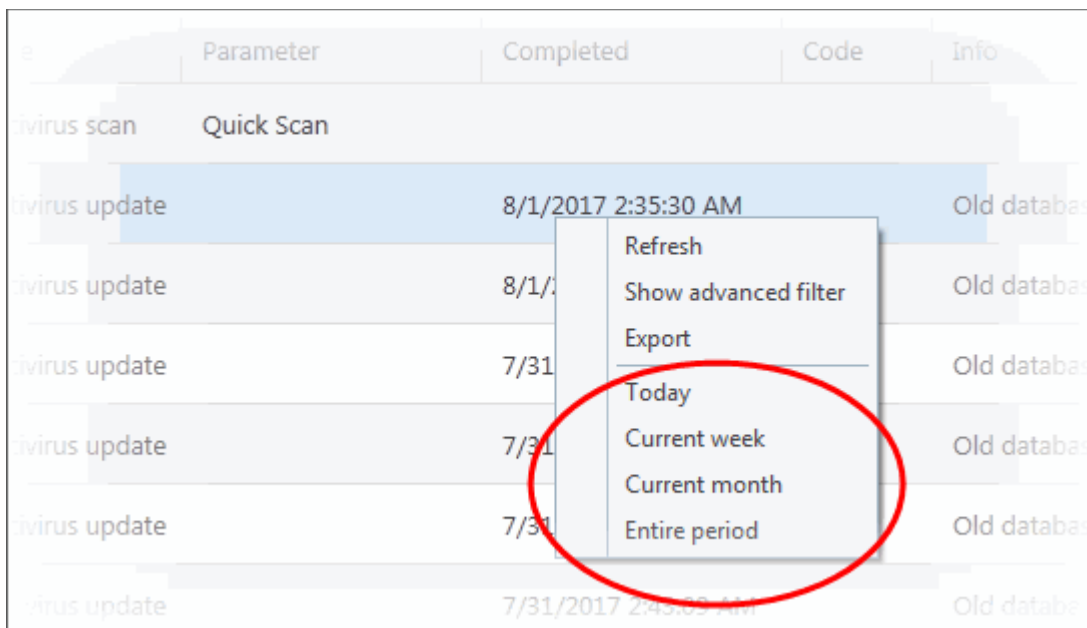
Preset Time Filters

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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.



Parameter	Completed	Code	Info
Quick Scan			
Antivirus update	8/1/2017 2:35:30 AM		Old databases
Antivirus update	8/1/2017 2:35:30 AM		Old databases
Antivirus update	7/31/2017 2:45:00 AM		Old databases
Antivirus update	7/31/2017 2:45:00 AM		Old databases
Antivirus update	7/31/2017 2:45:00 AM		Old databases
Antivirus update	7/31/2017 2:45:00 AM		Old databases
Antivirus update	7/31/2017 2:45:00 AM		Old databases

Advanced Filters

You can further refine which events are displayed according to specific filters. The following additional filters are available:

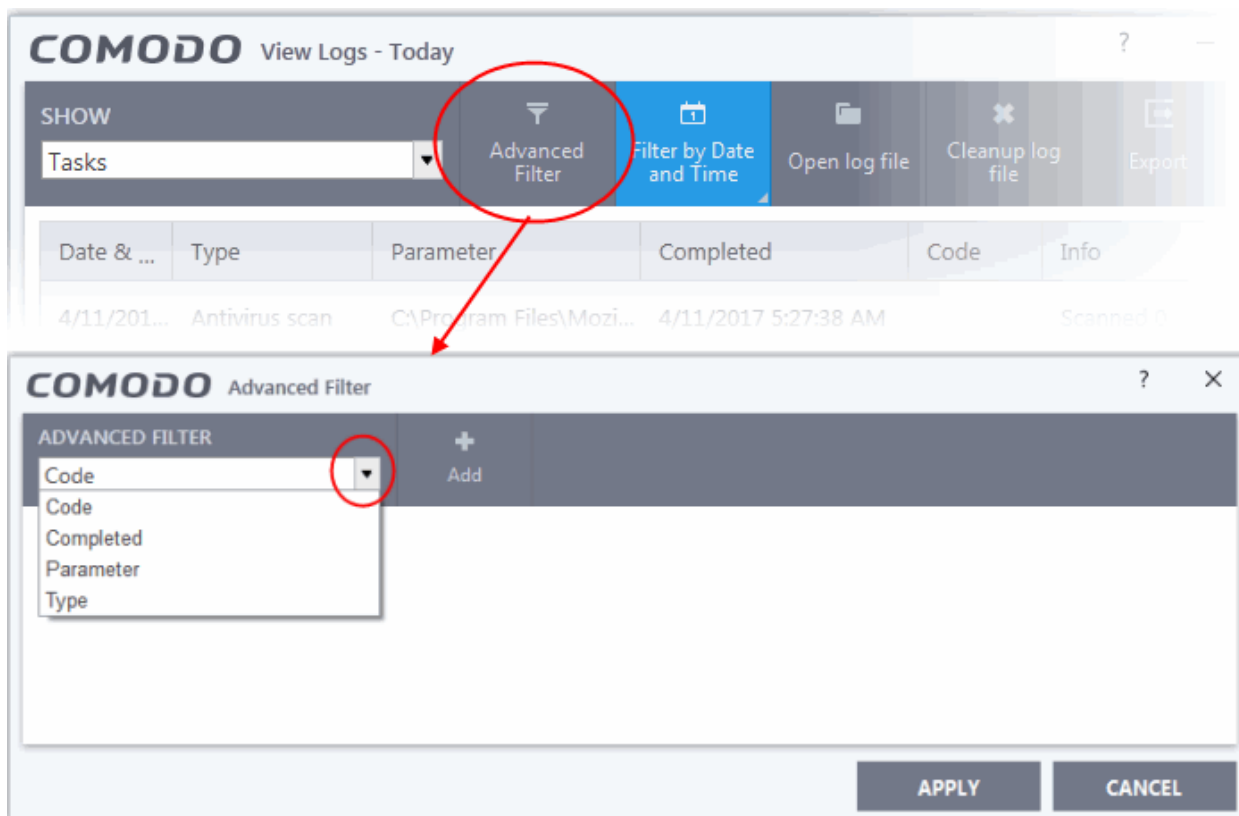
- **Code** - Filters tasks based on specified error code
- **Completed** - Displays only tasks completed on the specified date.
- **Parameter** - Displays only tasks that include the selected parameter. A 'parameter' is a sub-type of the main task type. For example, 'Quick Scan' and 'Rating Scan' are both parameters of the main task type 'Antivirus Scan'.
- **Type** - Displays only tasks of a certain type. Tasks that you can filter for include antivirus updates, antivirus scans, log clearing, warranty activation and more.

To configure Advanced Filters for Tasks logs

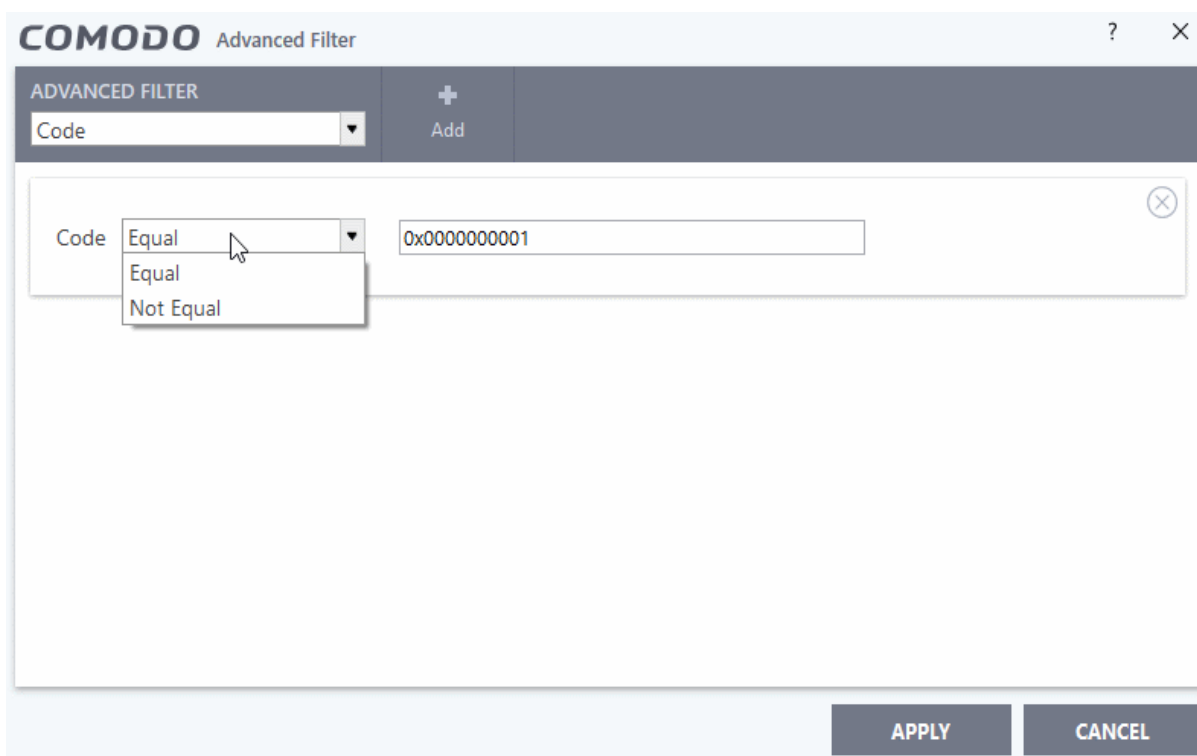
1. Click the 'Advanced Filter' button from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu.

The 'Advanced Filter' interface for 'Tasks' logs will be displayed.

2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



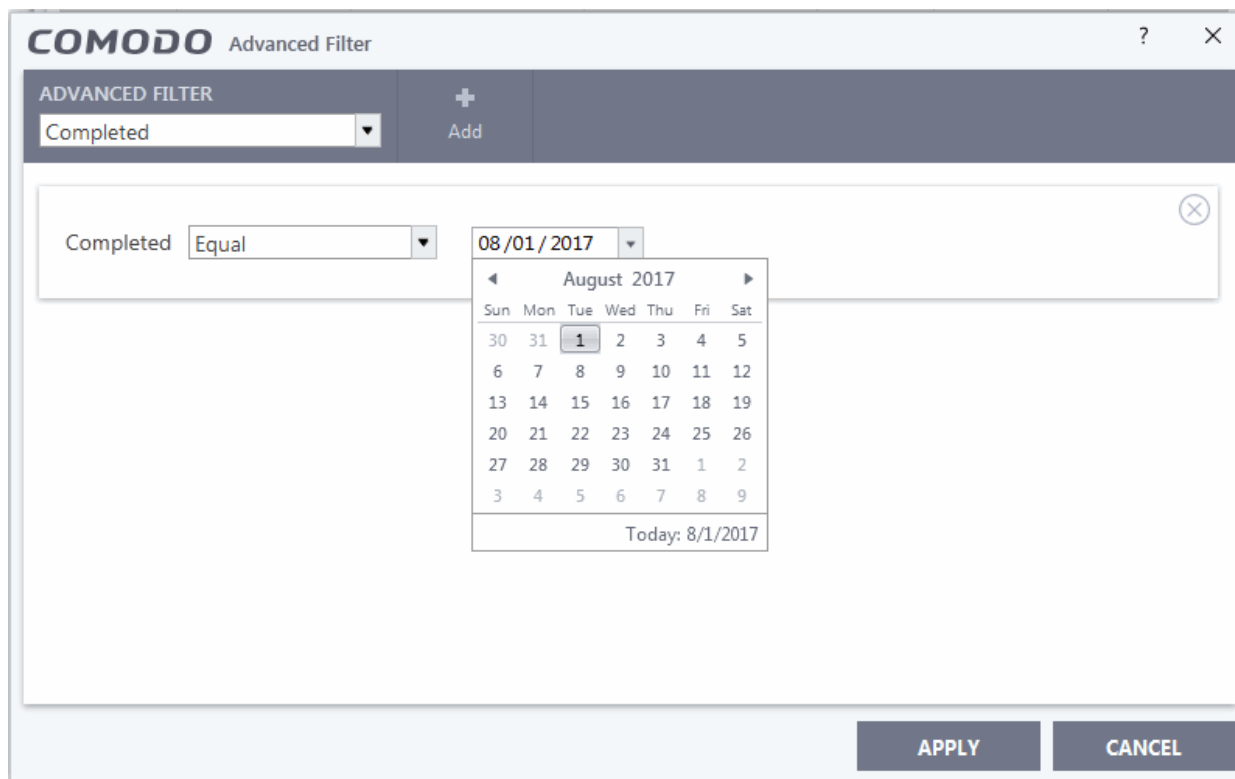
- i. **Code:** Filter incomplete tasks according to their error code generated by Windows. You can view task codes in the 'Code' column of the log viewer. Selecting the 'Code' option will display drop-down and text entry fields.



- a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b. Enter the code or a part of it as your filter criteria in the text field.

For example, if you have select 'Equal' and entered '0x80004004' in the text field, then only entries containing the value '0x80004004' in the 'Code' column will be displayed.

- i. **Completed:** Lets you filter logs based on the completion dates of the Tasks. Selecting the 'Completed' option displays drop-down box and date entry field.



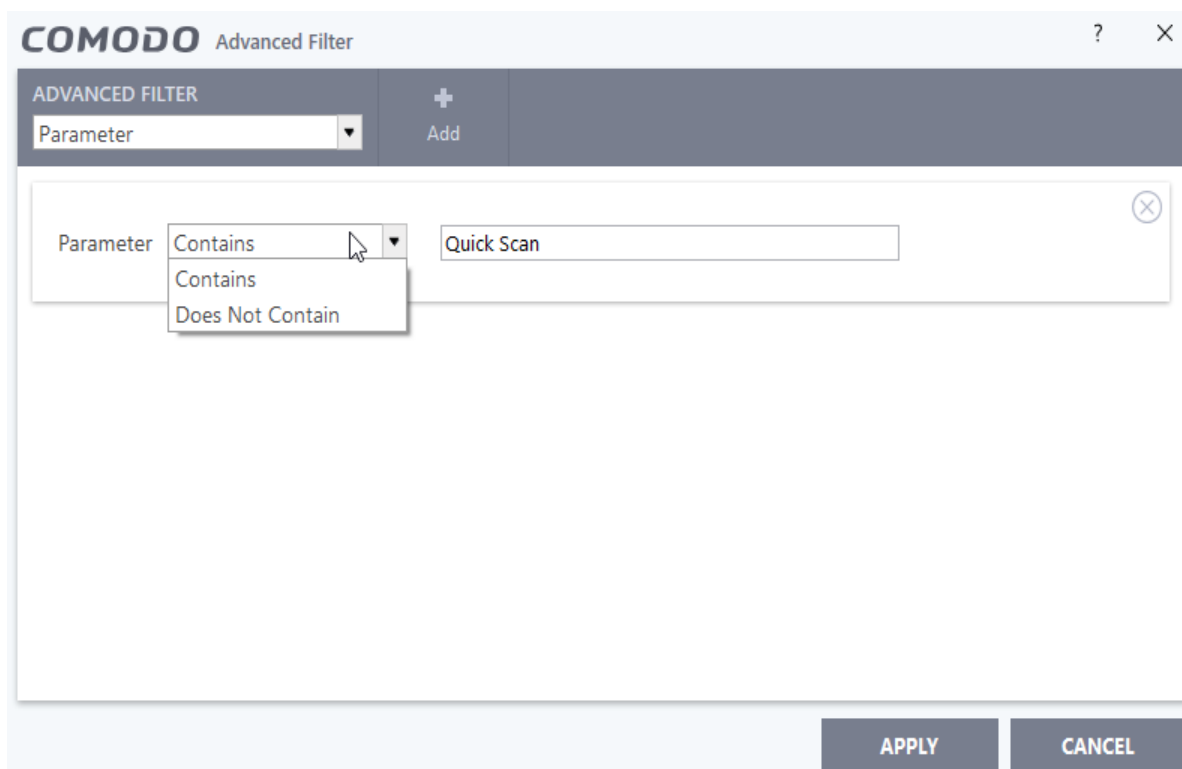
- a. Select any one of the following option the drop-down box.

- Equal
- Not Equal

- b. Select the required date from the date picker.

For example, if you choose 'Equal' and select '08/01/2017', only the logs of tasks completed on 08/01/2017' will be displayed.

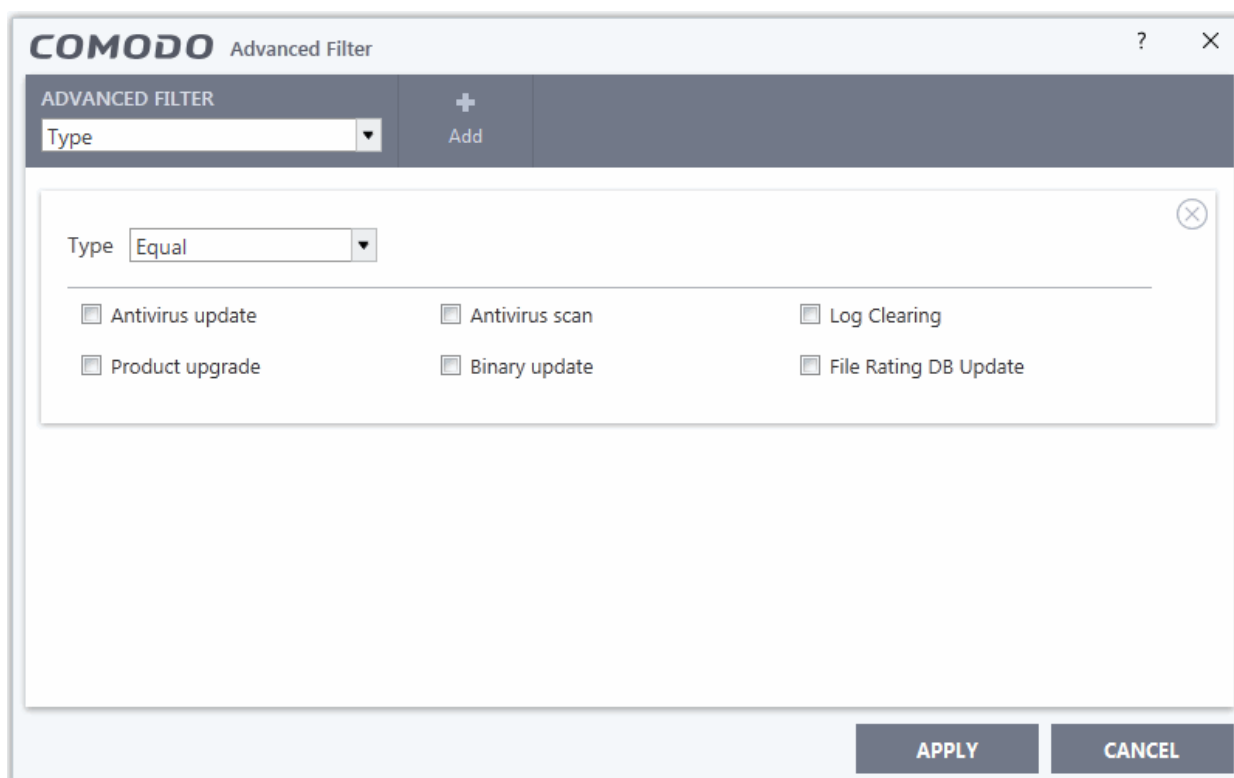
- iii. **Parameter:** The 'Parameter' option lets you filter entries based on the 'Parameter' column of the log viewer. This includes descriptions such as 'Quick Scan' and 'Rating Scan'. Selecting the 'Parameter' option displays drop-down and text entry fields.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
- b. Enter the text or word as your filter criteria.

For example, if you choose 'Contains' 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' will be displayed.

- iv. **Type:** Allows you to filter entries based on type of 'Tasks' launched. Selecting the 'Type' option displays a drop down box and a set of specific task types that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Antivirus update
 - Antivirus scan
 - Log Clearing
 - Product upgrade
 - Binary update
 - File Rating DB Upgrade

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

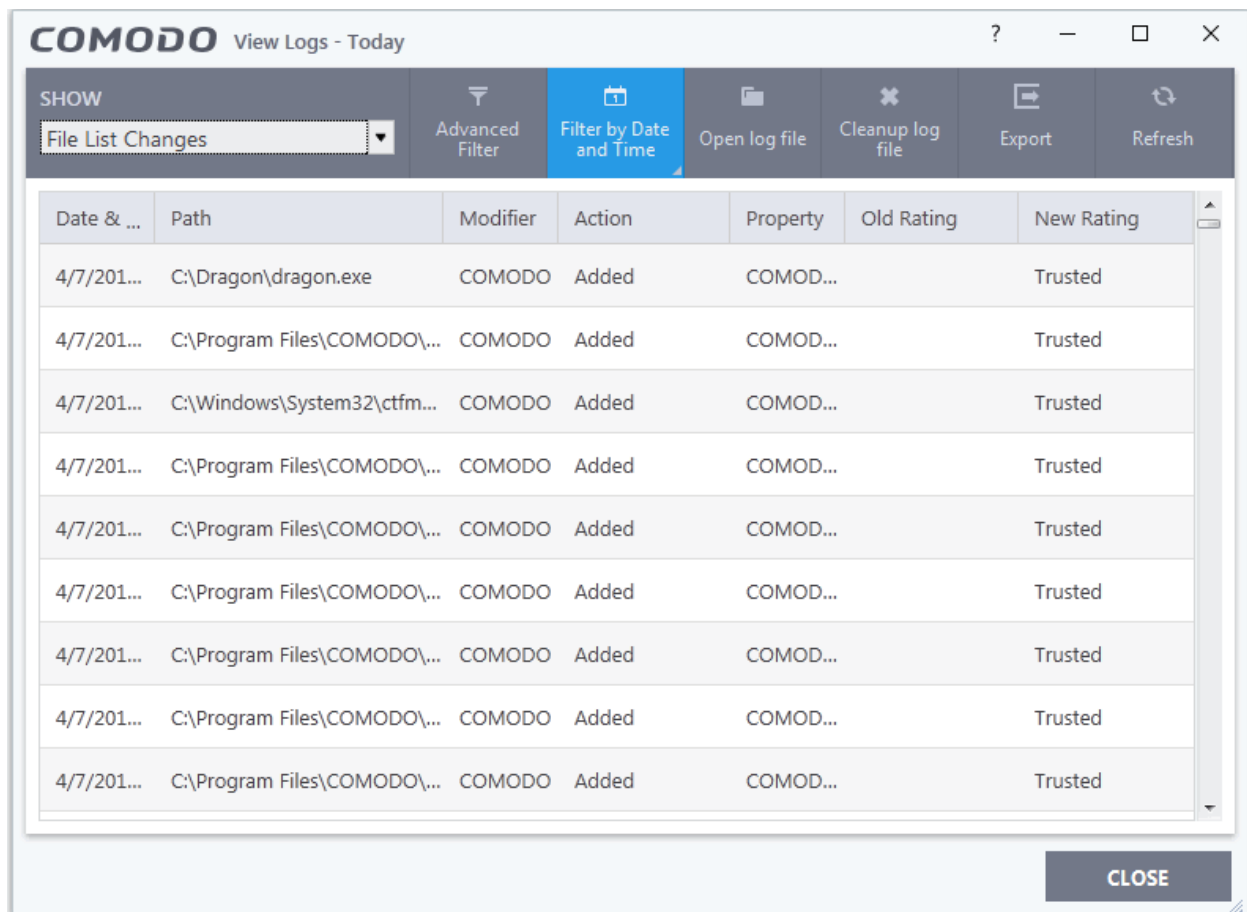
- Click 'Apply' for the filters to be applied to the 'Tasks' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.10. File List Changes Logs

The 'File List Changes' logs is a record of all changes made by CCS to files. For example, this includes adding a new file, removing a file or changing the rating of a file. See "[File List](#)" for more details'.

To access File List Changes Logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs':
- Select 'File List changes' from the 'Show' drop-down:



Column Descriptions

1. **Date & Time** - Date and time when the file list changes was generated.
 2. **Path** - Indicates the file path.
 3. **Modifier** - Indicates who made the changes (User, Administrator or Comodo).
 4. **Action** - Action type done for the file.
 5. **Property** - Indicates the file rating.
 6. **Old Rating** - Indicates the old rating for the file.
 7. **New Rating** - Indicates the new rating for the file.
- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
 - **'Open log file'** - view a saved log file.
 - **'Refresh'** - reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
 - **'Cleanup log file'** - Deletes all logs from all modules

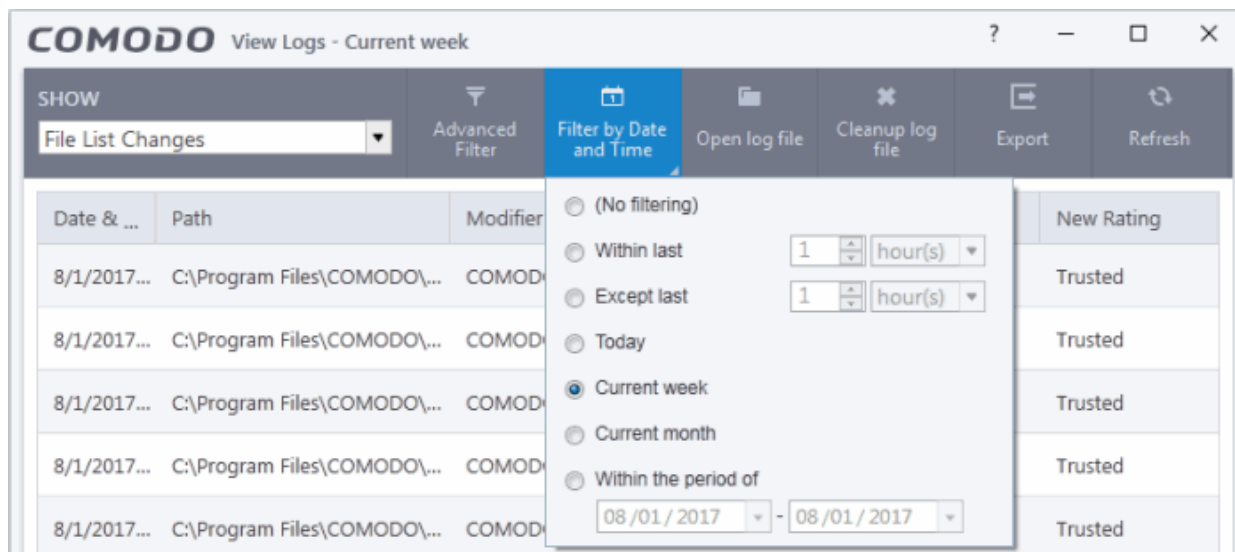
5.4.10.1. Filter 'File List Changes' Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- **Preset Time Filters**
- **Advanced Filters**

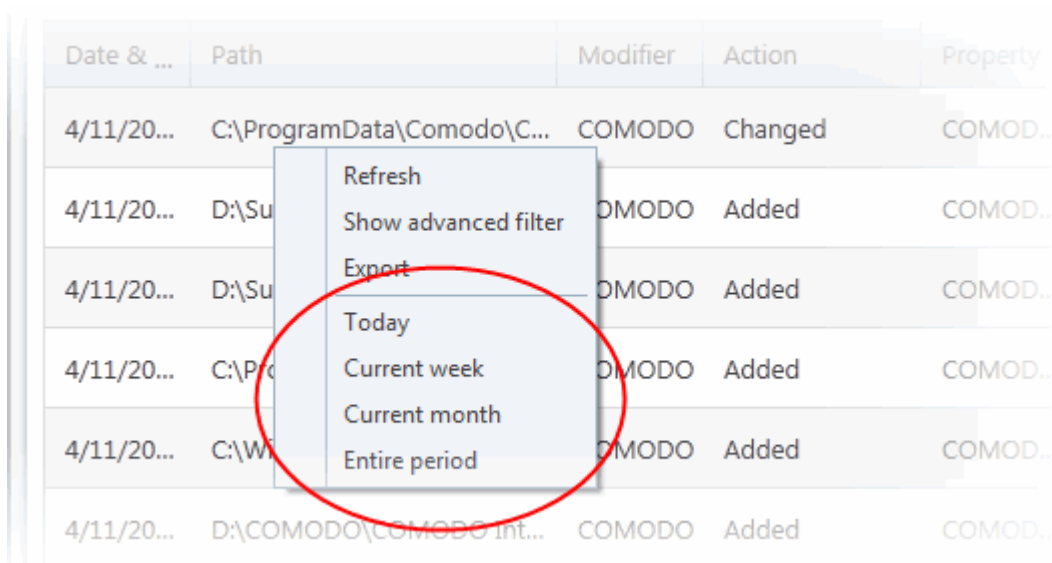
Preset Time Filters

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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

You can further refine which events are displayed according to specific filters. The following additional filters are available:

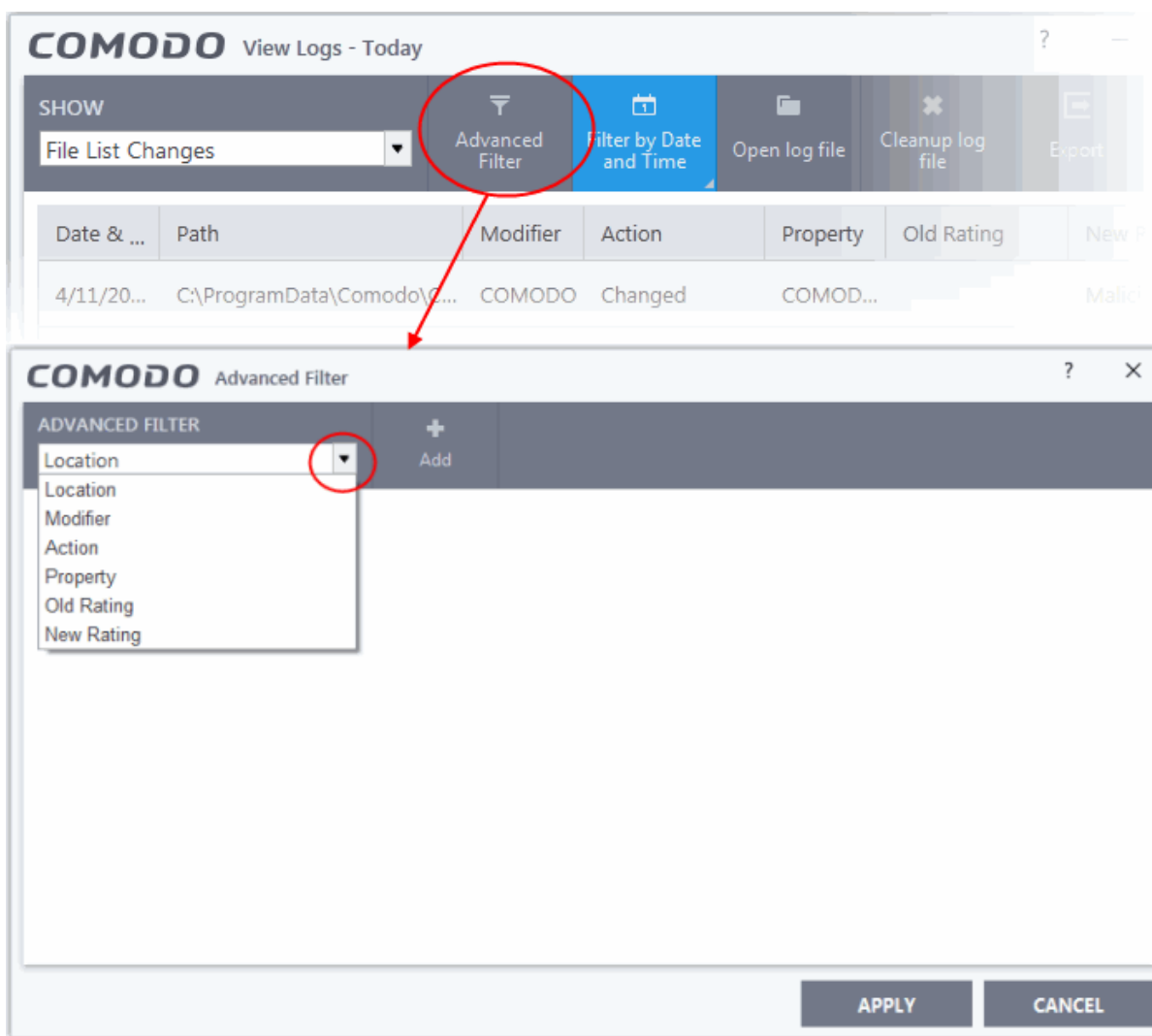
- **Location** - Displays only change logs based on entered file location.
- **Modifier** - Displays only change logs based on change done by such as (User, Administrator, and Comodo).
- **Action** - Displays only change logs for selected actions such as (Added, Removed or Changed).
- **Property** - Displays only change logs based on file rating done by such as (Administrator, User, and Comodo rating).
- **Old Rating** - Displays only change logs based on the old file rating.
- **New Rating** - Displays only change logs based on the new file rating.

To configure advanced filters for File List Changes logs

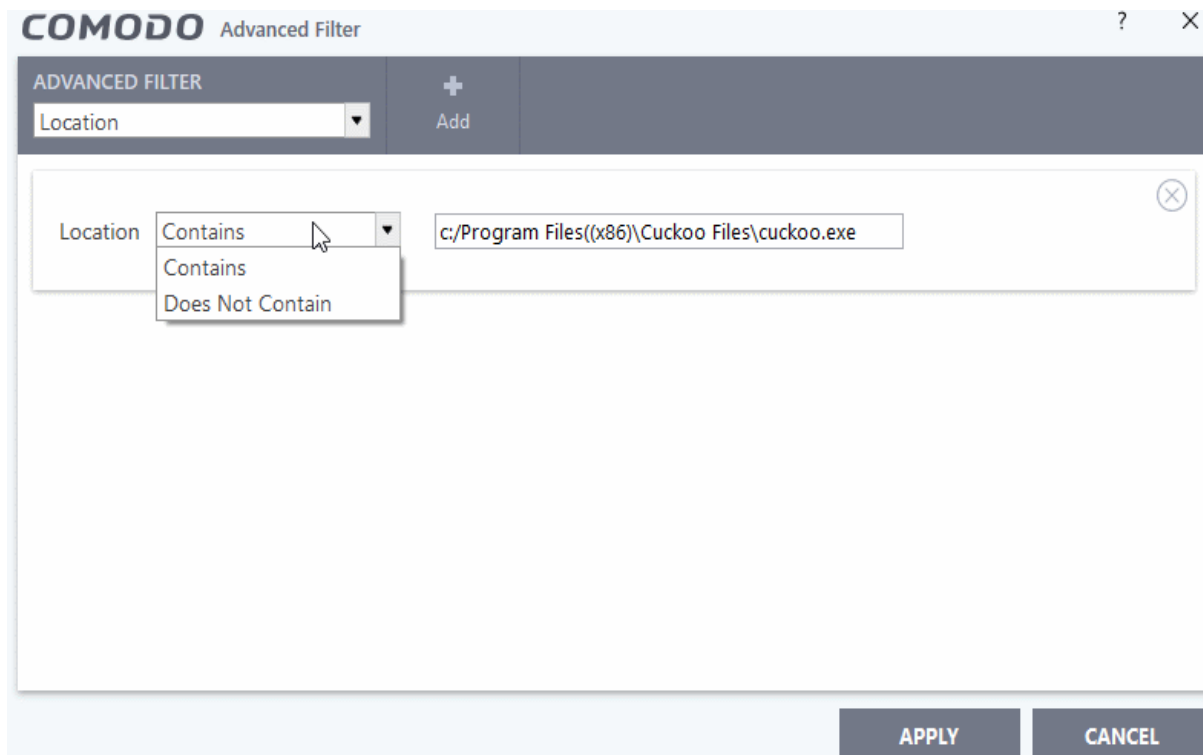
1. Click the 'Advanced Filter' button from the title bar or right-click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu.

The 'Advanced Filter' interface for the 'File List Changes' log viewer will be displayed.

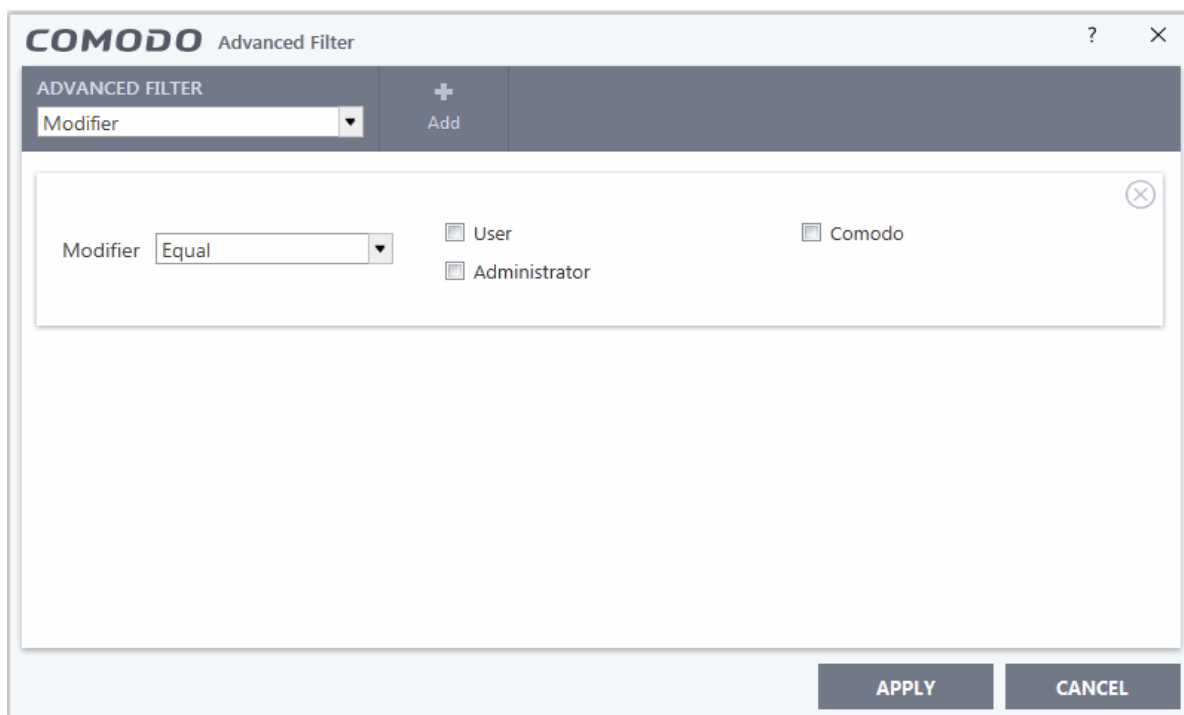
2. Select a filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



- i. **Location:** Filter file list changes according to their CCS code. You can view file list changes in the 'Location' column of the log viewer. Selecting the 'Location' option will display drop-down and text entry fields.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Enter the location or a part of it as your filter criteria in the text field.
For example if you have chosen 'Contains' and entered 'C:/Program Files (x86)/Cuckoo Files/Cuckoo.exe' in the text field, then only log entries with the same value in the 'Path' column will be displayed.
- ii. **Modifier:** The 'Modifier' option enables you to filter the log entries based on who did the file list changes. Selecting the 'Modifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.

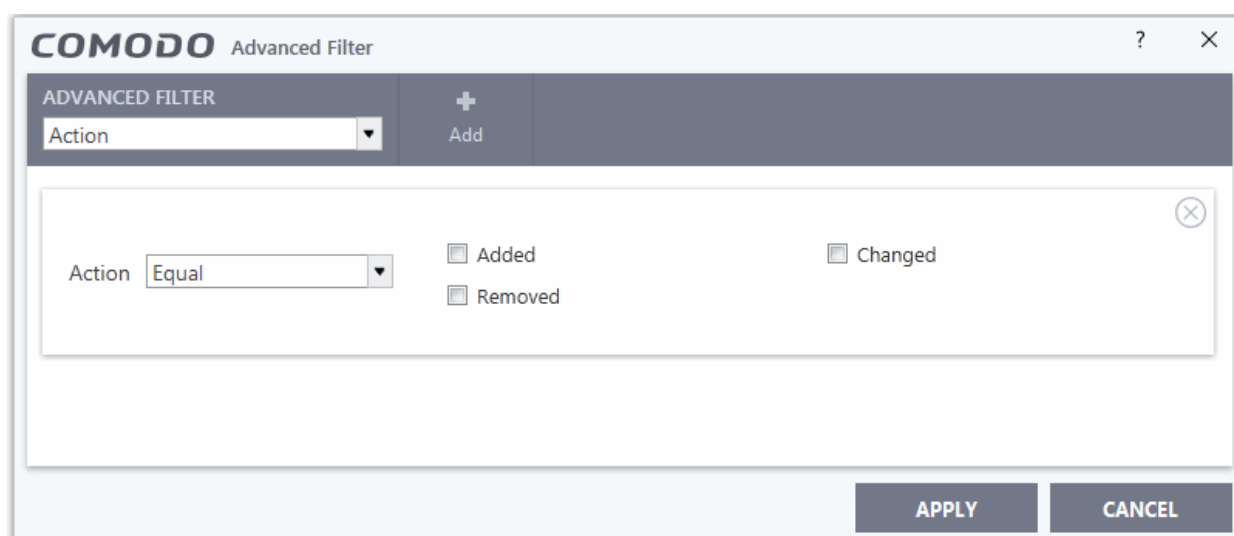


- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- User
- Comodo
- Administrator

For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs changes done by the user will be displayed.

- iii. **Action:** The 'Action' option allows you to filter log entries based on the 'Action' column of the log viewer. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Added
- Changed
- Removed

For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only the logs of files that were removed from the file list will be displayed.

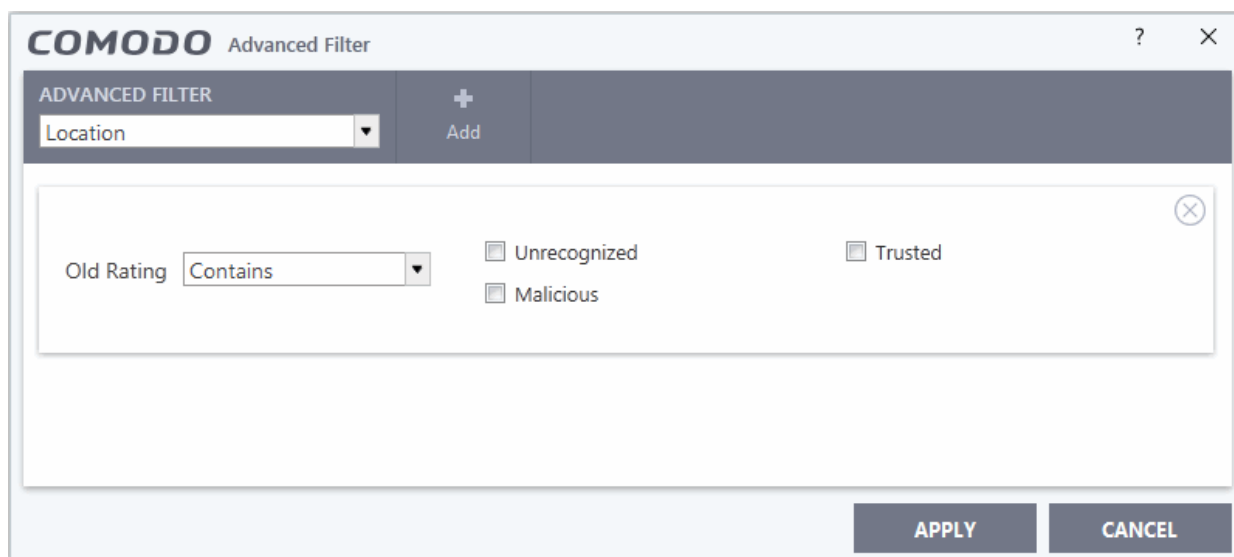
- iv. **Property:** Allows you to filter log entries based on the file rating. Selecting the 'Property' option displays a drop-down box and a set of specific filter parameters.

The screenshot shows the 'COMODO Advanced Filter' dialog box. At the top, there's a title bar with the COMODO logo and the text 'Advanced Filter'. Below the title bar, there's a dark grey header with 'ADVANCED FILTER' and a dropdown menu currently set to 'Property'. To the right of this dropdown is a plus sign and the word 'Add'. The main content area is white and contains a dropdown menu set to 'Property' with 'Contains' selected. To the right of this dropdown are three checkboxes: 'Administrator Rating', 'Comodo Rating', and 'User Rating', all of which are unchecked. A close button (X) is in the top right corner of the main area. At the bottom right are 'APPLY' and 'CANCEL' buttons.

- a. Select 'Contains' or 'Does Not Contain' option from the drop down. 'Does Not Contain' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Administrator Rating
 - User Rating
 - Comodo Rating

For example, if you select 'Equal' from the drop-down and select 'User Rating' checkbox, only the logs of files that were rated by the user will be displayed.

- v. **Old Rating:** Allows you to filter log entries based on old file rating before it's rating was changed. Selecting the 'Old Value' option displays a drop-down and a set of specific filter parameters.



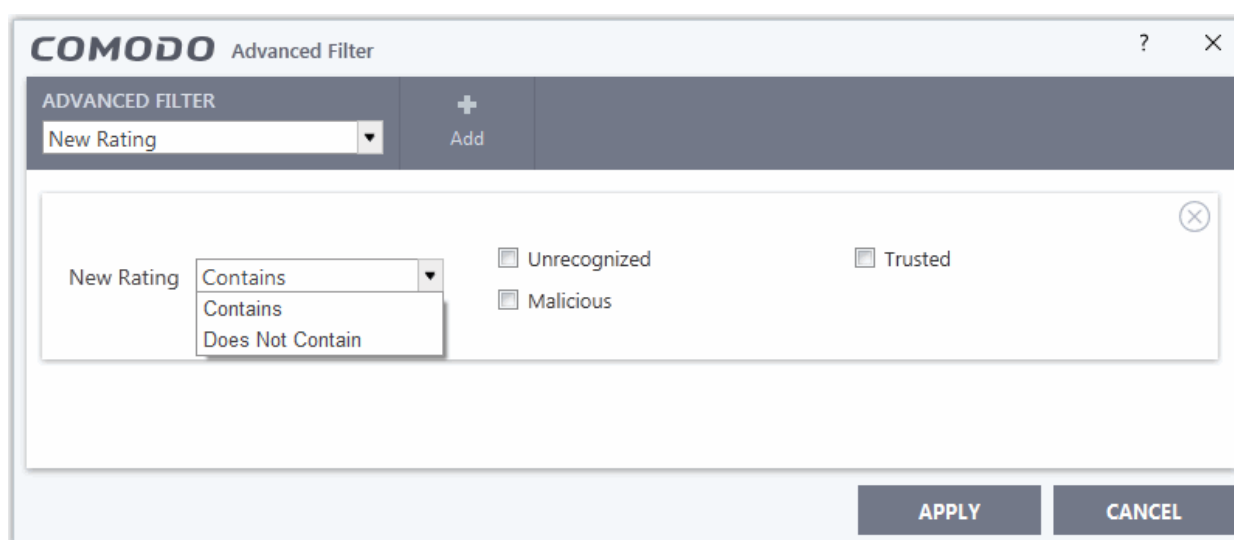
a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.

b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Unrecognized
- Trusted
- Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' under the 'Old Value' column will be displayed.

vi. **New Rating:** Allows you to filter log entries based on new file rating before it's rating was changed.



a. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.

b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:

- Unrecognized

- Trusted
- Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' under the 'New Value' column will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'File List Changes' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

5.4.11. Vendor List Change Logs

- The vendor list is a list of trusted software publishers. Files from trusted vendors are excluded from virus scans.
- Changes to this list are logged in 'Vendor List Changes'.

Open the Vendor List Changes Logs

- Click 'Tasks' at the top-left of the CCS home screen
- Click 'Advanced Tasks' > 'View Logs'
- Click 'Show' > 'Vendor List Changes':

Date & Time	Vendor	Modifier	Action	Property	Old Rating	New Rating
10/8/2018 3:31...	cs@amedtec.de	User	Added	User rating		Unrecognized
10/8/2018 3:29...	OSTOTO CO. LIMITED	User	Changed	User rating	Unrecognized	Malicious
10/8/2018 11:5...	NextInteractiveMedia	COMODO	Changed	COMODO ...	Unrecognized	Trusted
10/5/2018 12:4...	Beijing Huahong Integrated Circ...	COMODO	Added	COMODO ...		Trusted
10/1/2018 4:09...	ABB S.p.A.	User	Changed	User rating	Trusted	Unrecognized

Column Descriptions

1. **Date & Time** - Date the log was generated.
 2. **Vendor** - Name of the software publisher.
 3. **Modifier** - Entity that made the change. Can be 'Admin', 'User' or 'Comodo'.
 4. **Action** - The activity performed on the vendor. For example, 'Removed' or 'Added' to the list.
 5. **Property** - Which entity assigned the rating. Can be 'Admin', 'User' or 'Comodo'.
 6. **Old Rating** - Rating prior to modification. 'Old rating' is populated if the action is 'changed'.
 7. **New Rating** - The modified vendor rating.
- **'Export'** - Generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
 - **'Open log file'** - View a saved log file.
 - **'Refresh'** - Reload the list to view the latest logs
 - Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
 - **'Cleanup log file'** - Deletes all logs from all modules

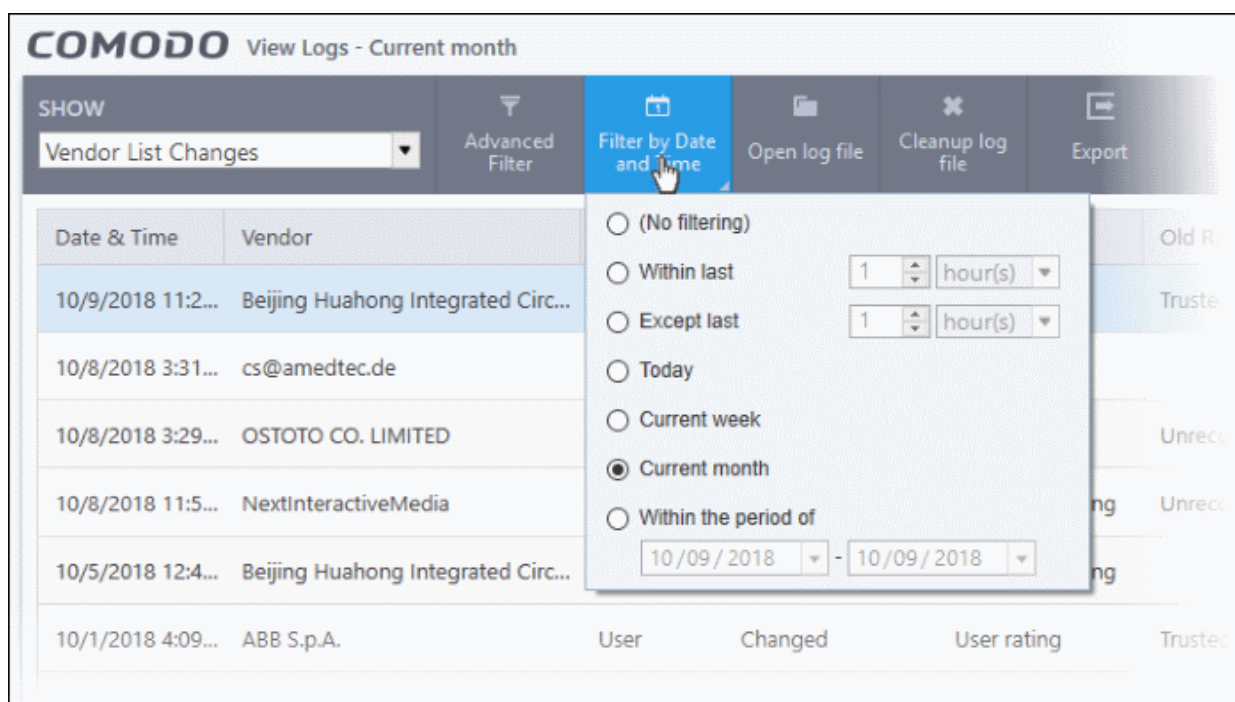
5.4.11.1. Filter 'Vendor List Changes' Logs

You can create filter logged events by various criteria. The following types of filters are available:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

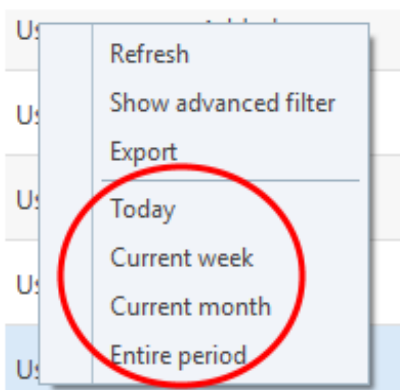
- Click 'Filter by Date and Time' to choose your filters:



- **No filtering** - Show every event logged since CCS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.

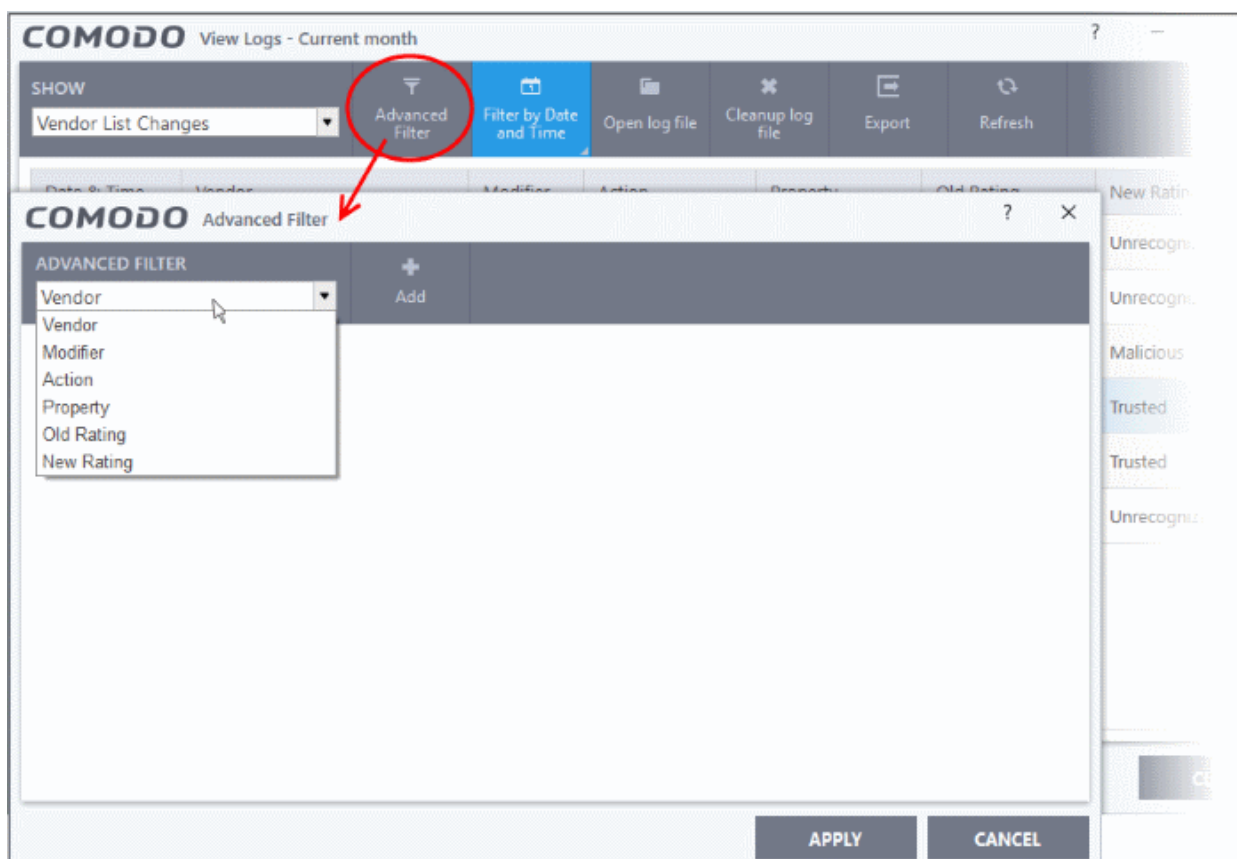
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Show all events logged today, from 12:00 am to the current time.
- **Current Week** - Show all events 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.



Configure 'Advanced Filters'

- Click the 'Advanced Filter' button on the title bar
- Select a filter from the 'Advanced Filter' drop-down and click 'Add'



You can further refine the filter with the following parameters:

- **Vendors** - Show logs related to a specific software publisher
- **Modifier** - Show logs which were modified by a specific entity (user, admin or Comodo)
- **Action** - Show logs which featured a specific activity. For example, object added or removed
- **Property** - Show logs by the entity that provided the rating (admin, user or Comodo)
- **Old Rating** - Show logs which had a specific rating when the vendor was added to the list.
- **New Rating** - Show logs which feature a specific vendor rating after modification.

The rest of this section contains more help to configure advanced filters, if required.

Click 'Add' after selecting a category:

i. **Vendor**: Allows you to filter the change logs based on a software publisher name. Selecting the 'Vendor' option displays a drop-down and text entry fields.

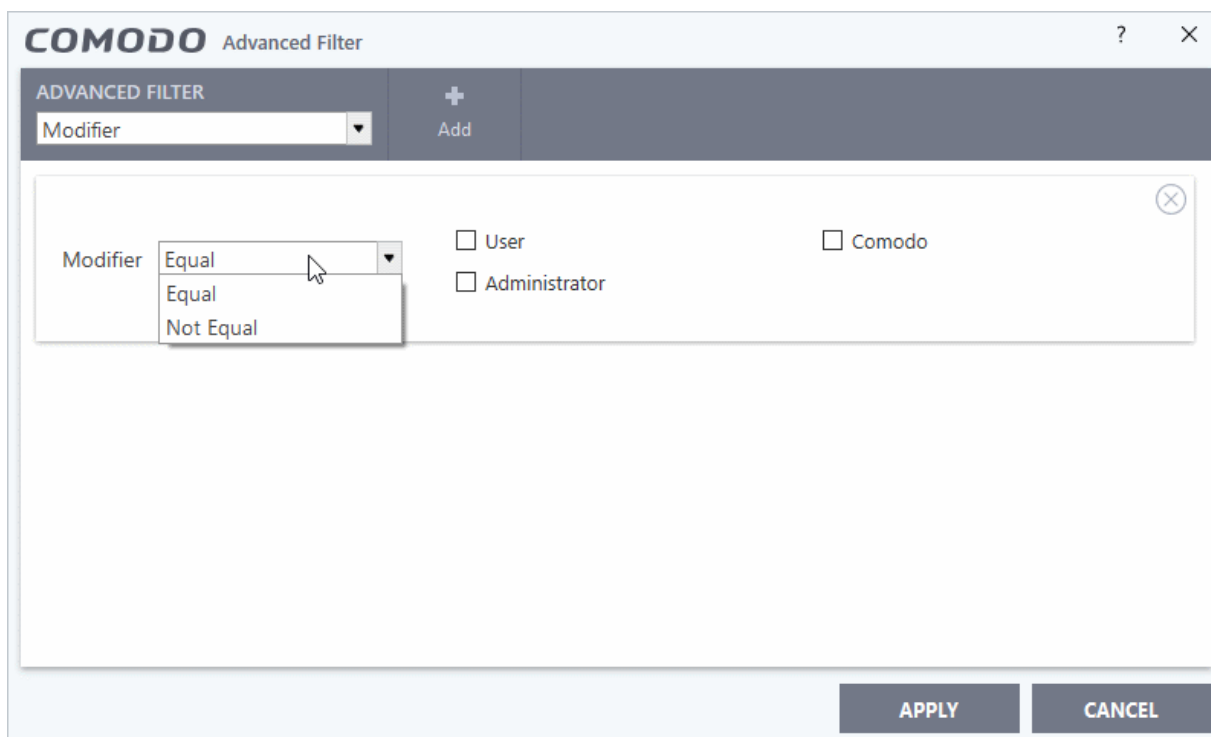
The screenshot shows the 'COMODO Advanced Filter' dialog box. At the top, there's a title bar with the COMODO logo and the text 'Advanced Filter'. Below the title bar is a dark grey header containing 'ADVANCED FILTER' and a dropdown menu currently set to 'Vendor'. To the right of the dropdown is a plus sign and the word 'Add'. Below the header is a main area with a 'Vendor' label, a dropdown menu showing 'Contains', 'Contains', and 'Does Not Contain', and a text input field containing 'Atompark Software'. At the bottom right are 'APPLY' and 'CANCEL' buttons.

a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.

b. Enter the vendor name in full or a part of it as your filter criteria in the text field.

For example if you have chosen 'Contains' and entered 'Atompark Software' in the text field, then only log entries with the same name 'Atompark Software' in the 'Vendors' column will be displayed.

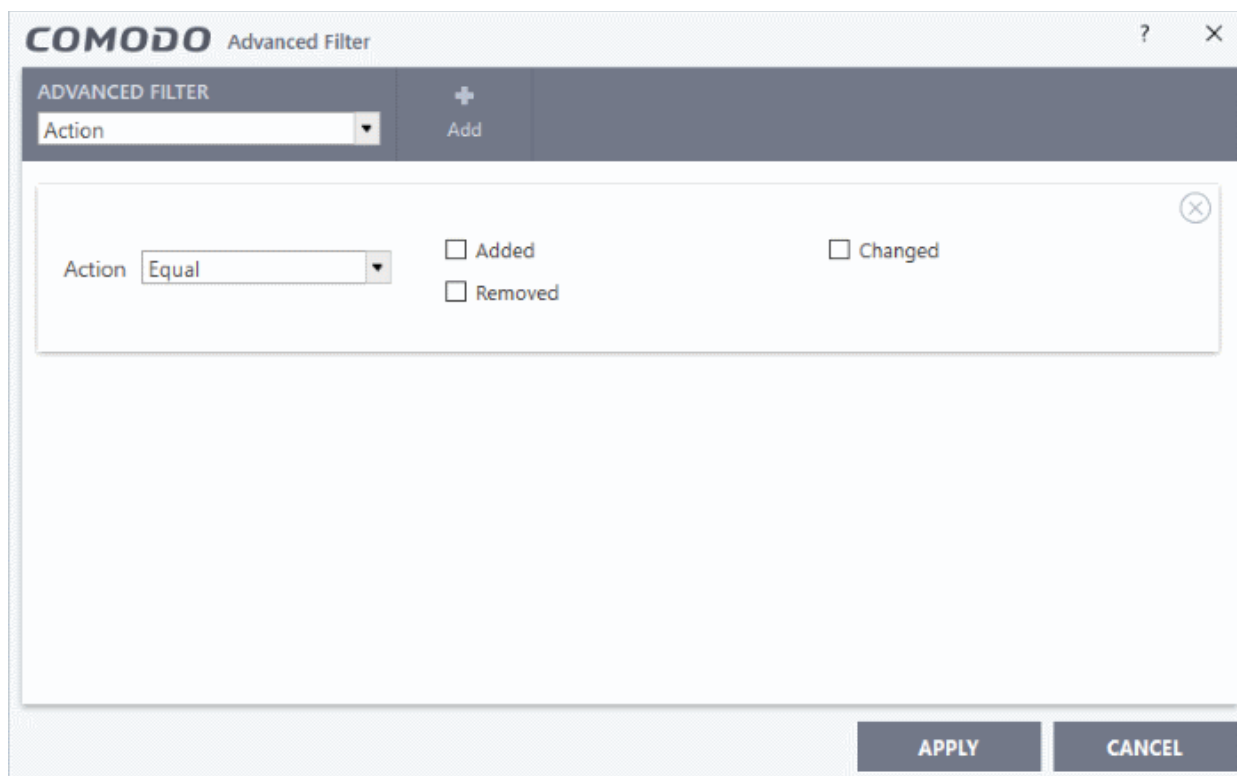
ii. **Modifier**: Allows you to filter logs based on changes done by admin, user or Comodo. Selecting the 'Modifier' option displays drop-down box and a set of specific filter parameters.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - User
 - Comodo
 - Administrator

For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs changes done by the user under 'Modifier' column will be displayed.

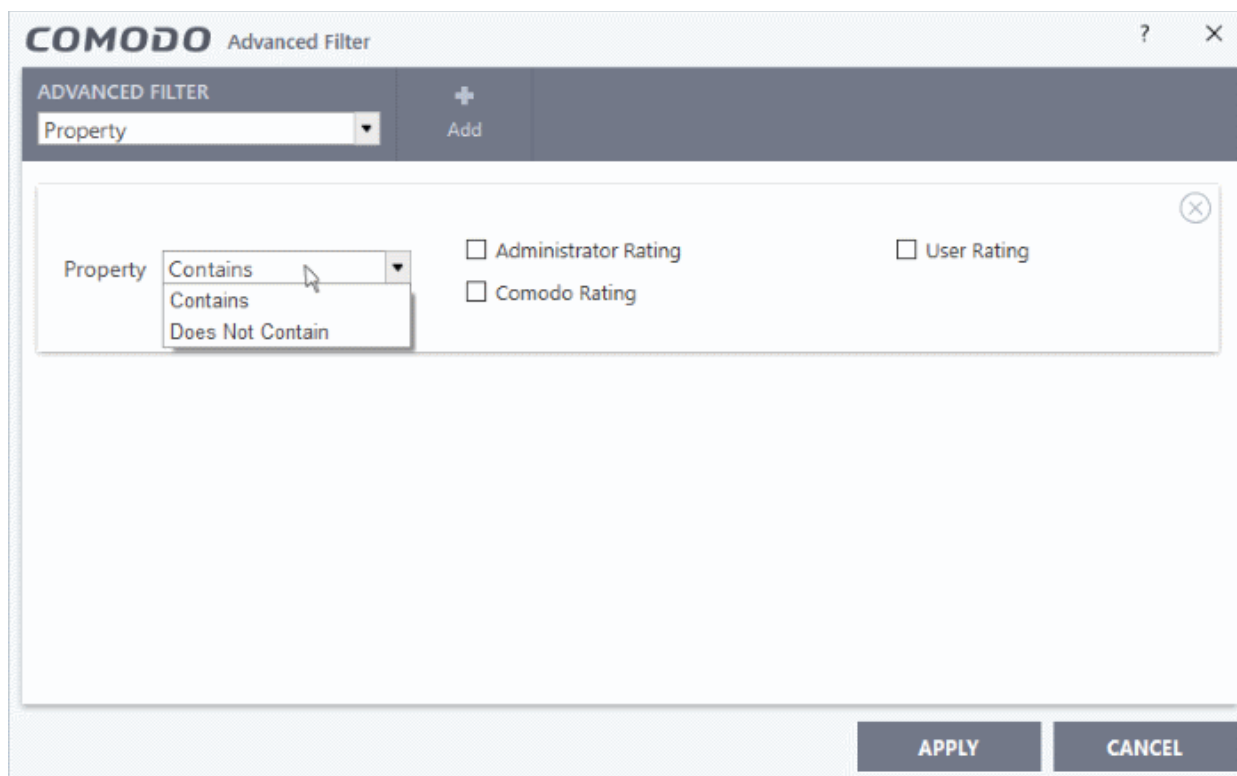
iii. **Action:** Allows you to filter log entries based on the modifications done to the vendor list. Selecting the 'Action' option displays drop-down box and set of specific filter parameters.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Added
 - Removed
 - Changed

For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only logs of vendors that were removed from the list will be displayed.

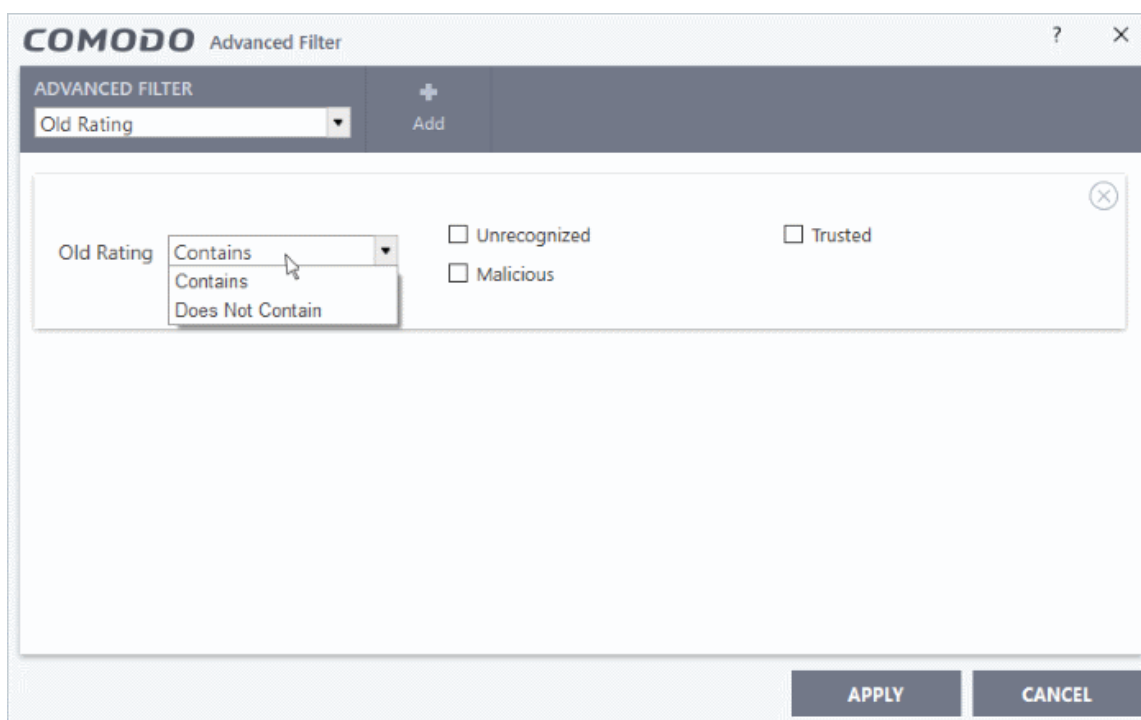
iv. **Property:** Allows you to filter log entries based on the rating provider (admin, user or Comodo) Selecting the 'Property' option displays drop-down box and set of specific filter parameters.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Administrator Rating
 - User Rating
 - Comodo Rating

For example, if you select 'Contains' from the drop-down and select 'Administrator Rating' checkbox, only logs of vendors that were rated by an admin will be displayed.

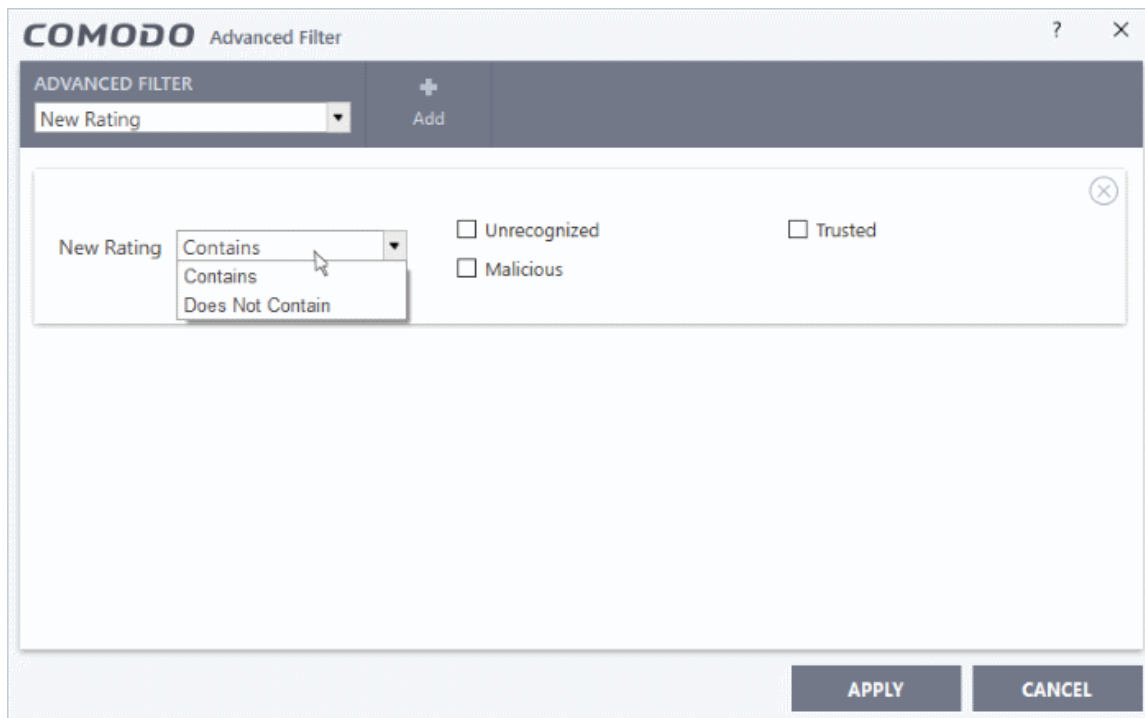
- v. **Old Rating:** Allows you to filter log entries based on the original vendor rating (unrecognized, trusted or malicious). Selecting the 'Old Rating' option displays drop-down box and set of specific filter parameters.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Unrecognized
 - Trusted
 - Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only logs of vendors that were rated as 'Unrecognized' while adding the vendor to the list will be displayed.

vi. **New Rating:** Allows you to filter log entries based on the modified vendor rating (unrecognized, trusted or malicious). Selecting the 'New Rating' option displays drop-down box and set of specific filter parameters.



- a. Select 'Contains' or 'Does Not Contain' option from the drop-down box. 'Does Not Contain' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - Unrecognized
 - Trusted
 - Malicious

For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only logs of vendors whose rating were modified by admin, user or Comodo as 'Unrecognized' will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

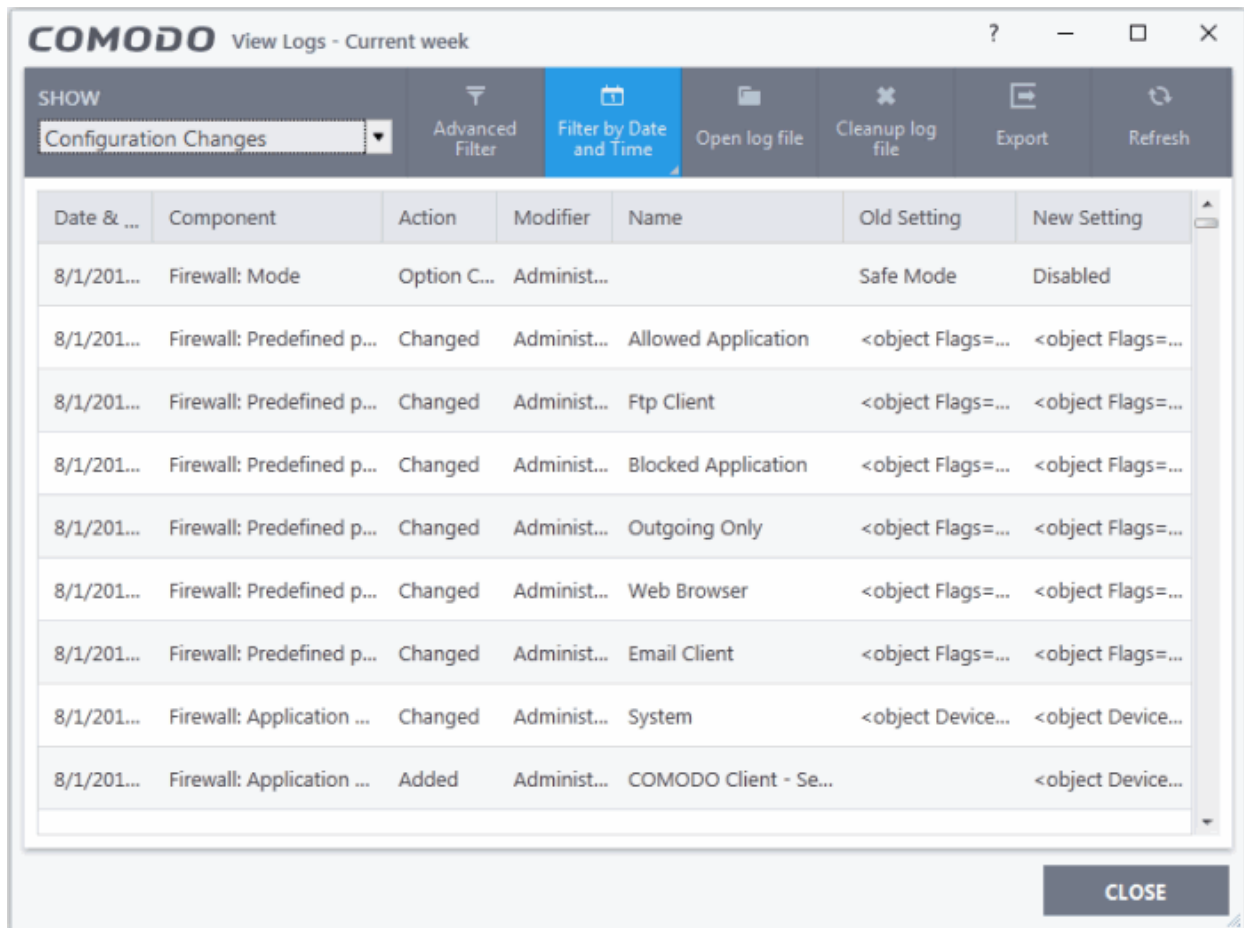
- Click 'Apply' for the filters to be applied to the 'Vendor List Changes' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'

5.4.12. Configuration Changes

The 'Configuration Changes Log' contains CCS records all changes made to its settings since installation.

To access Configuration Changes Logs

- Click 'Tasks' at the top left of the CCS screen
- Click 'Advanced Tasks' > 'View Logs':
- Select 'Configuration Changes' from the 'Show' drop-down



Column Descriptions

1. **Date & Time** - Date and time when the changes occurred.
 2. **Action** - The type of action applied to the component. For example, whether the component was removed, added or changed.
 3. **Modifier** - Indicates who the changes were done by (User, Antivirus Alert, Auto Learn, Firewall Alert, HIPS Alert, Containment Alert, Scheduler, Comodo, and Administrator)
 4. **Name** - The name of the rule, program or the file that has been changed.
 5. **Old Setting** - Parameter value before configuration change.
 6. **New Setting** - Parameter value after configuration change.
- To view full details of a particular configuration change, place your mouse cursor over the entry in the 'Old Settings' or 'New Settings' column

```
<object Name="Suspicious Locations" UID="{A282C320-CBBA-4084-8038-F0672603B83D}"> <Files> <File DeviceName="?:\$\$Recycle.Bin\*" Filename="?:\$\$Recycle.Bin\*" /> <File DeviceName="C:\ProgramData\Comodo\Cis\Quarantine\data\*" Filename="C:\ProgramData\Comodo\Cis\Quarantine\data\*" /> <File DeviceName="C:\Documents and Settings\All Users\Application Data\can.exe\*\*" Filename="C:\Documents and Settings\All Users\Application Data\Comodo\Cis\Quarantine\data\*" /> </Files> </object>
```

- **'Export'** - generate a HTML file of the logs from all modules.
 - Alternatively, right-click inside the log viewer and select 'Export' from the menu
- **'Open log file'** - view a saved log file.
- **'Refresh'** - reload the list to view the latest logs

- Alternatively, right-click inside the log viewer and select 'Refresh' from the menu
- **'Cleanup log file'** - Deletes all logs from all modules

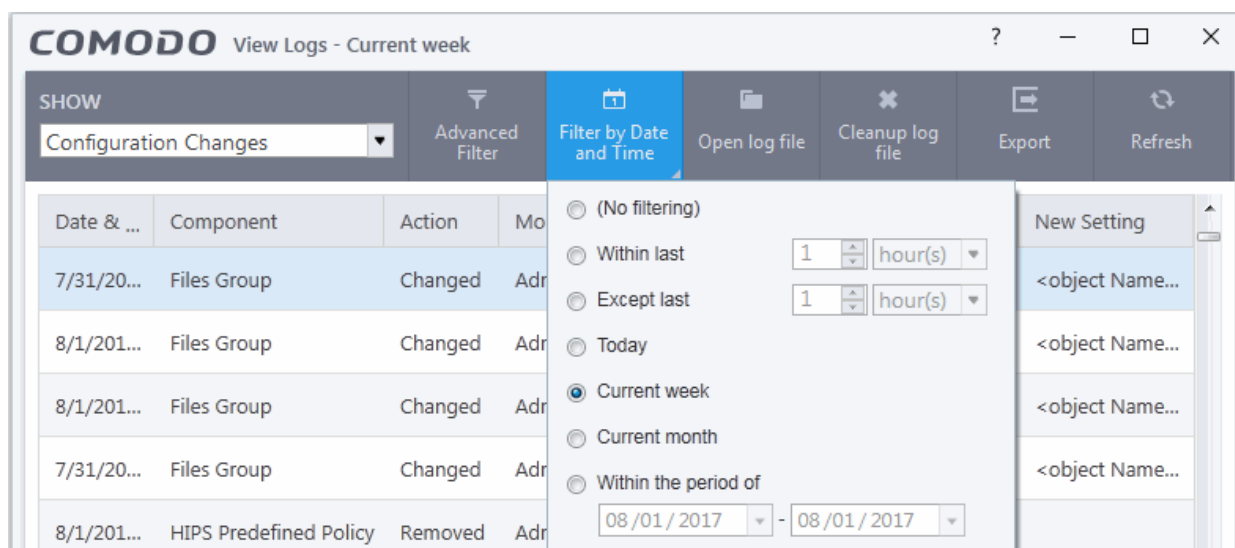
5.4.12.1. Filter 'Configuration Changes' Logs

Comodo Client Security allows you to create custom views of all logged events according to user defined criteria. The following types of filters are:

- **Preset Time Filters**
- **Advanced Filters**

Preset Time Filters

- Click 'Filter by Date and Time' to display logs for a specific time period:



- **No filtering** - Show every event logged since CCS 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.
- **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.

Object	Action	Modifier	Name	Old Setting	New Setting
Group	Changed	Admin		<object Name...	<object Name...
Group	Changed	Admin		<object Name...	<object Name...
Group	Changed	Admin		<object Name...	<object Name...
Group	Changed	Admin		<object Name...	<object Name...
Redefined Policy	Removed	Admin		p...	<object Flags=...
Redefined Policy	Changed	Administ...	Windows System App...	<object Flags=...	<object Name...

Advanced Filters

You can further refine which events are displayed according to specific filters. The following additional filters are available:

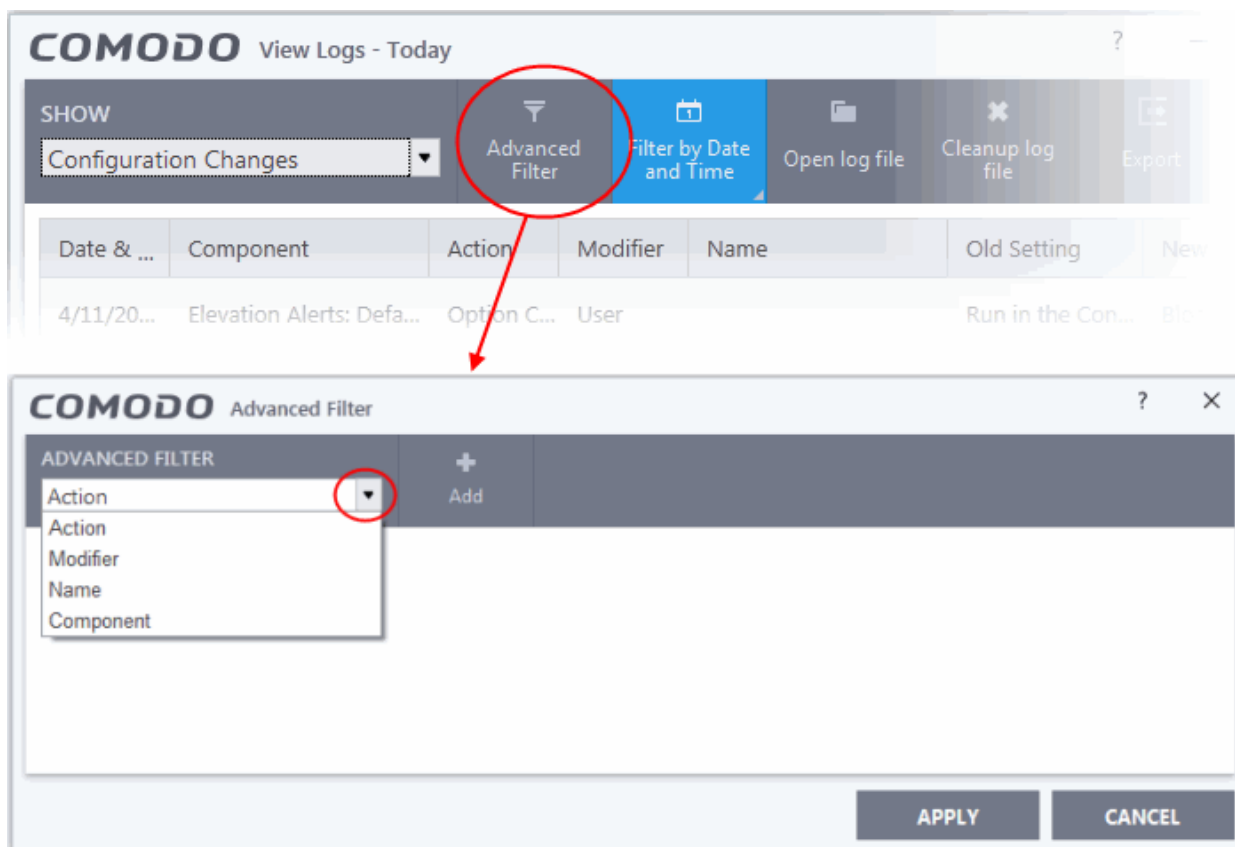
- **Action:** Displays only logs for the selected action(s). Example actions are add, remove and change of rules.
- **Modifier:** Filters logs based on the source of the change. Example sources include the user making a change at an alert, auto-learning, the scheduler, Comodo, Administrator and so on.
- **Name:** Filters logs based on the name of the object.
- **Component:** Filters logs according to changes in selected CCS components and settings

To configure Advanced Filters for Configuration Changes logs

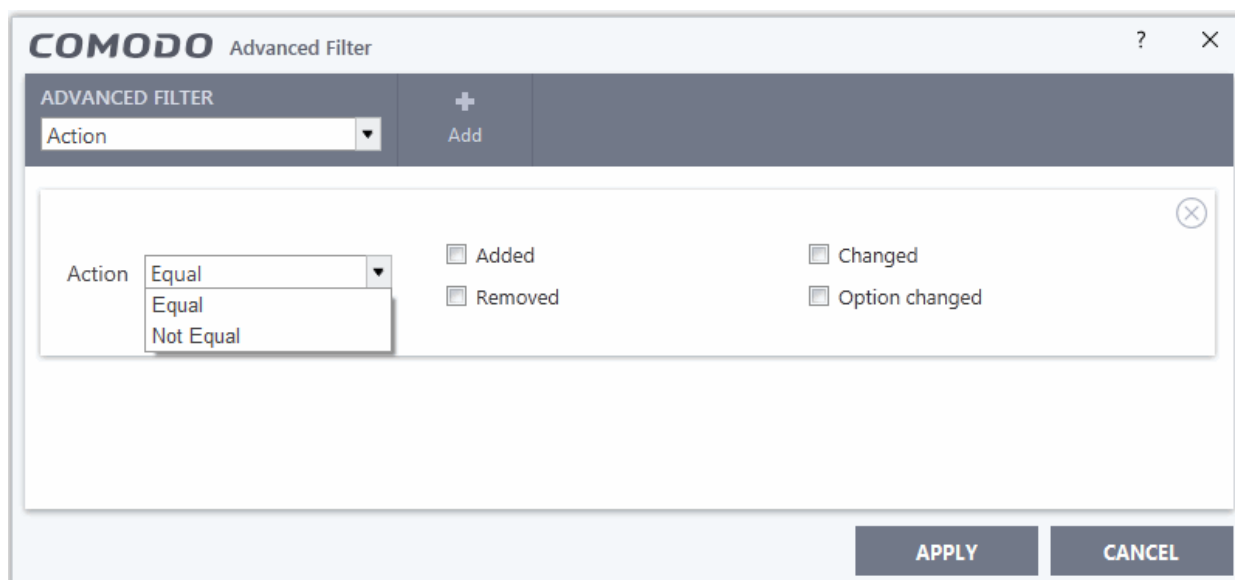
1. Click the 'Advanced Filter' button from the title bar or right-click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu.

The Advanced Filter' interface for 'Configuration Changes' logs will open:

2. Select a filter from the 'Advanced Filter' drop-down and click 'Add'.



- i. **Action:** Allows you to filter log entries based on the actions executed. These include a change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- a. Select 'Equal' or 'Not Equal' option from drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
- Added
 - Changed
 - Removed

- Option changed

For example, if you choose 'Equal' from the drop-down and select 'Added' checkbox, only logs entries with the value 'Added' under 'Action' column will be displayed.

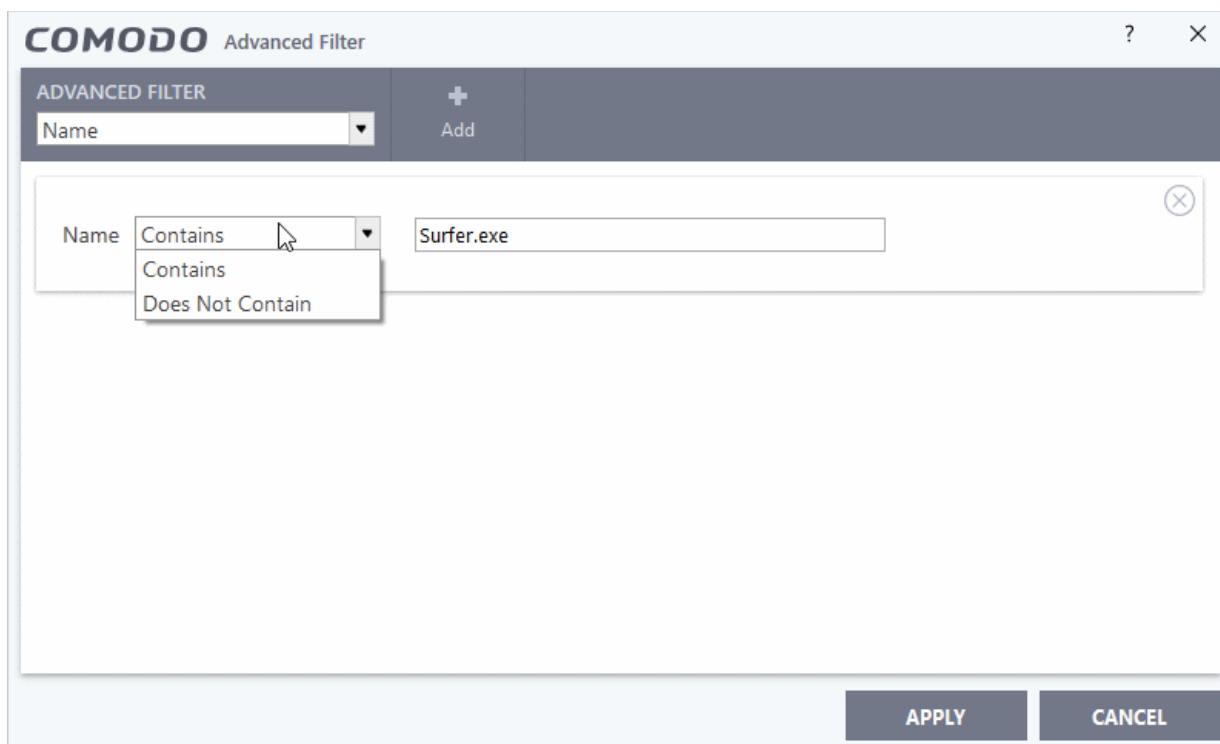
- Modifier:** Allows you to filter log entries based on the entity that is responsible for the configuration change. It can be the user or the response given to an alert. Selecting the 'Modifier' option displays drop-down box and a set of specific filter parameters.

The screenshot shows the 'COMODO Advanced Filter' dialog box. At the top, there's a title bar with the COMODO logo and the text 'Advanced Filter'. Below the title bar is a dark grey bar containing 'ADVANCED FILTER', a plus sign and 'Add' button, and a dropdown menu labeled 'Modifier'. The main area of the dialog is white and contains a 'Modifier' dropdown menu with 'Equal' selected. Below this are several checkboxes for filter parameters: User, Auto learn, Antivirus Alert, Firewall Alert, HIPS alert, Containment alert, Scheduler, Comodo, and Administrator. At the bottom right of the dialog are 'APPLY' and 'CANCEL' buttons.

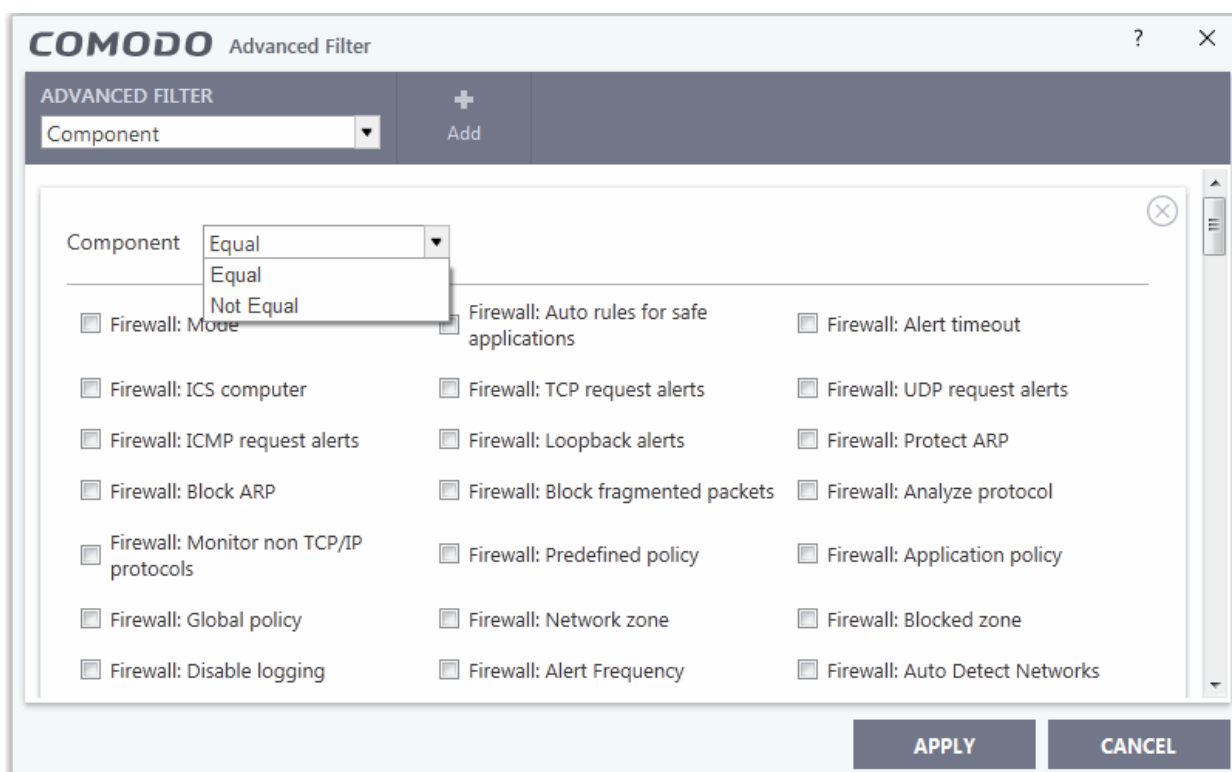
- a. Select 'Equal' or 'Not Equal' option from drop-down box. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific filter parameters to refine your search. The parameters available are:
 - User
 - Auto learn
 - Antivirus Alert
 - Firewall Alert
 - HIPS alert
 - Containment alert
 - Scheduler
 - Comodo
 - Administrator

For example, if you have chosen 'Equal' in the drop-down and selected 'Antivirus Alert' checkbox, then, only logs entries related to the configuration changes effected by responses to 'Antivirus Alerts' will be displayed.

- Name:** The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



- a. Select 'Contains' or 'Does Not Contain' option from drop-down. 'Does Not Contain' will invert your selected choice.
- b. Enter the name of the change, partly or fully as filter criteria in the text box.
For example, if you choose 'Contains' option from the drop-down and enter the phrase 'surfer.exe' in the text field, then only the log entries containing the surfer.exe in the name column will be displayed.
- iv. **Component:** Allows you to filter log entries related to the objects modified during the configuration change. Selecting the 'Object' option displays drop down and the objects of CCS configuration.



- a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b. Now select the check-boxes of the specific objects as filter parameters to refine your search. Scroll down the window to see all the objects.

For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode' checkbox, only the log entries related to the change of Firewall mode will be displayed.

Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Configuration Changes log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- To clear filters, open the 'Advanced Filter' pane and remove each filter by clicking the 'X' button at the top right of each filter pane then click 'Apply'.

5.5. Submit Files for Analysis to Comodo

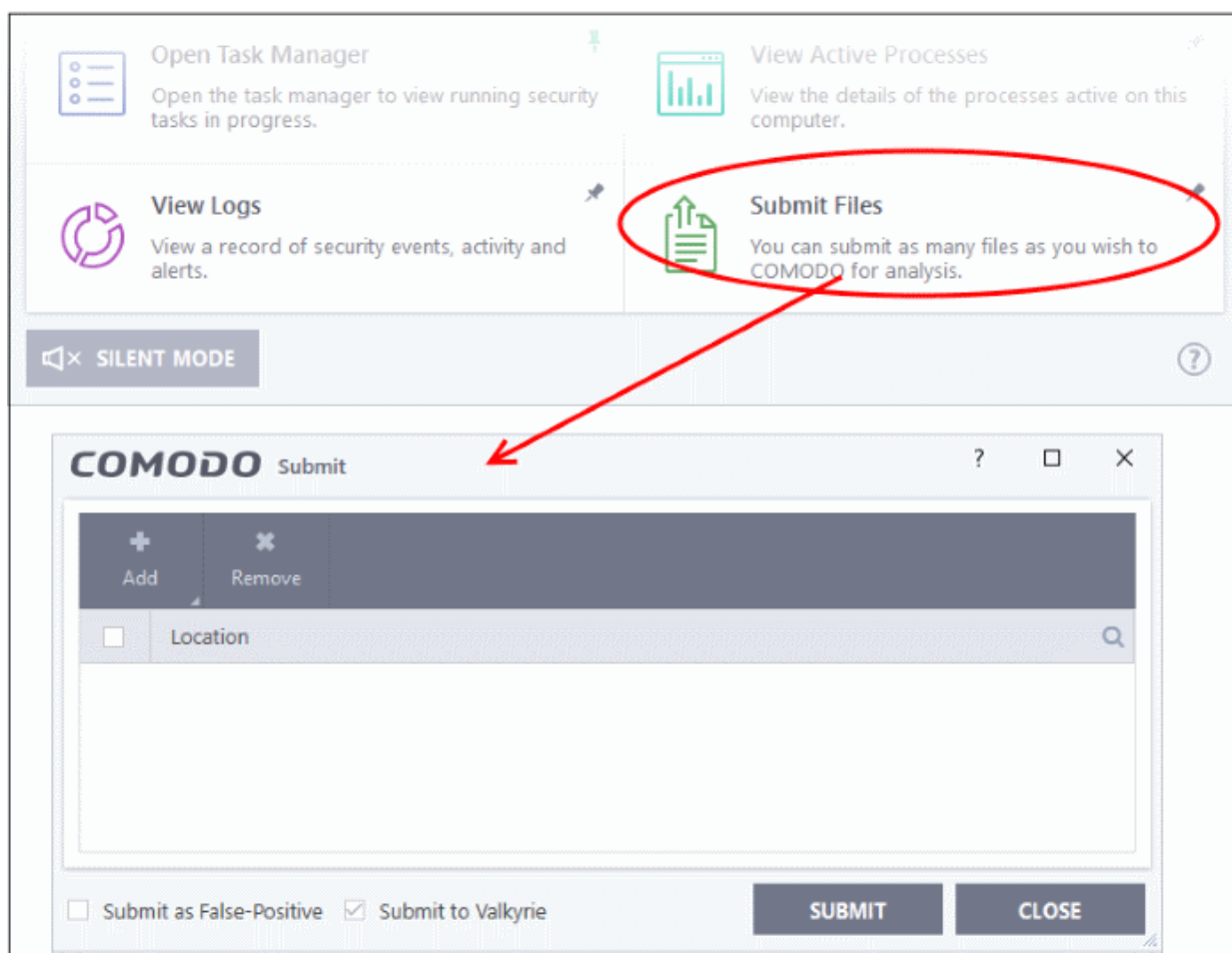
- You can submit files to Valkyrie for analysis in order to confirm their status whether trusted or malicious
- CCS rates a file as either 'trusted', 'malicious' or 'unknown' when it is first run
- Files with no rating at all (by admin, user or Comodo) are automatically uploaded to Valkyrie when executed, or if they are discovered by a **rating scan**.
- Files given an unrecognized rating (by admin, user or Comodo) are *not* uploaded to Valkyrie.
- You can also submit them manually.

The 'Submit Files' interface allows you to send as many files as you wish to Comodo for analysis. Comodo experts analyze them and classify them as either 'Safe' or 'Malicious'. After analysis and classification they will be added to the white or black list accordingly.

You can submit files to Valkyrie from the **Quarantine** and **File List** interfaces. This section explains how you can select files, folders and running processes and submit them manually to Valkyrie for analysis.

To add new file(s) to 'Submit Files' list

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



- Click 'Add' at the top. You can add files to the 'Submit Files' list in three ways:



- **Files** - Navigate to the file or executable of the program you wish to add.
- **Folders** - Navigate to the folder you wish to add. All the files in the folder will be added to the 'Submitted Files' list.
- **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'Submitted Files' list.
- Repeat the process to add more files and to submit them at-once.

To remove the files from 'Submit Files' list

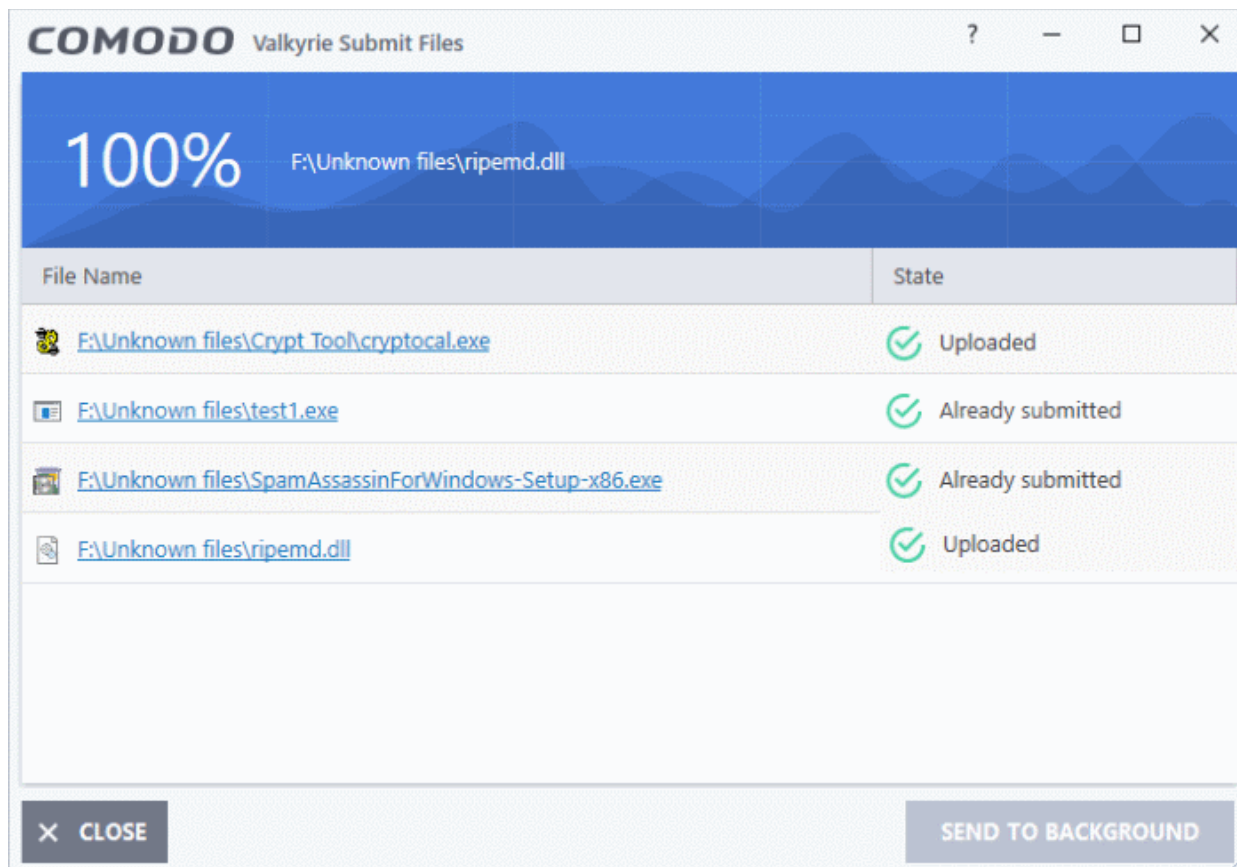
- Select the file from the list and click 'Remove'

To submit files to Valkyrie

After adding the files you want to submit, click the 'Submit' button. Please note the file(s) will be submitted to Valkyrie only by default. The files will be submitted and the progress will be displayed.

You can stop, pause/resume or send the submission process to background by clicking respective buttons.

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen displays these results on completion.



- Uploaded - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- Already submitted - The file has *already* been submitted to our labs by you or by another CCS user.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

The list of files submitted from your computer can be viewed from the **Submitted Files** interface.

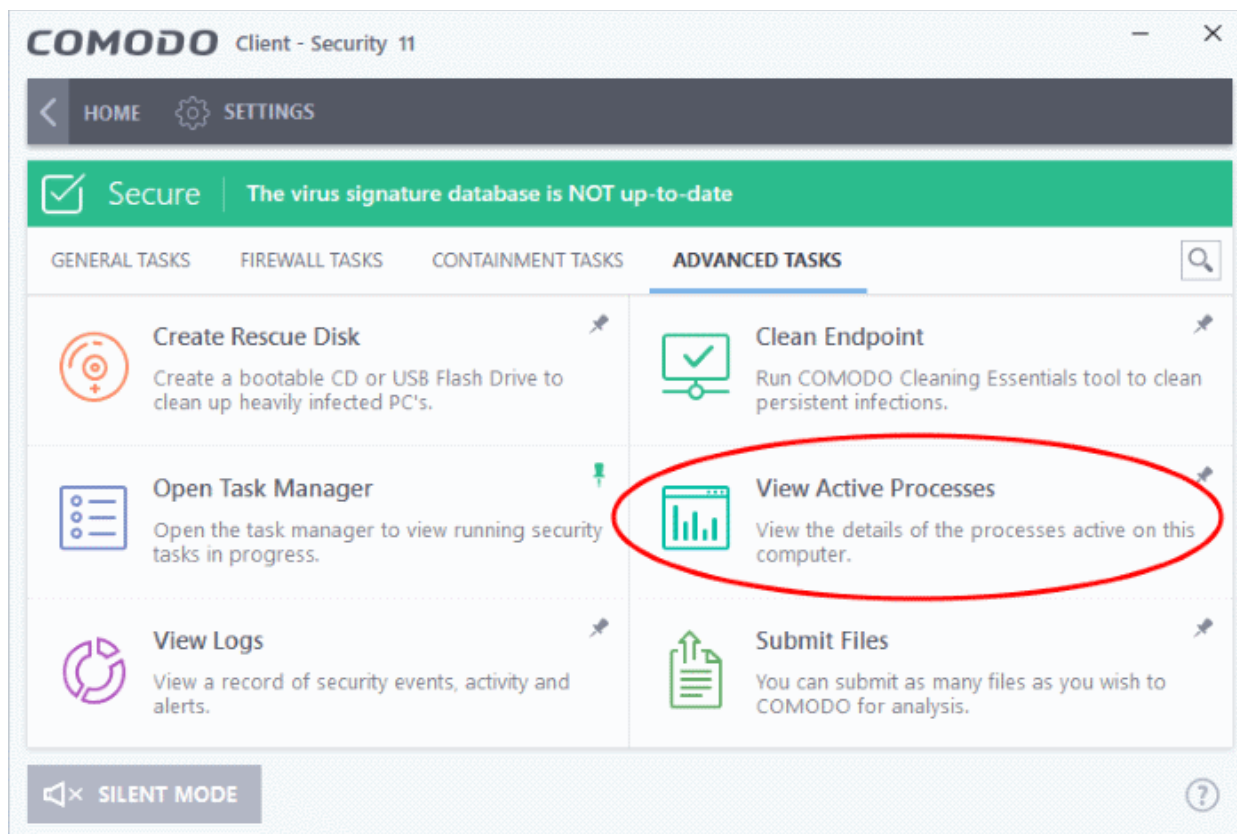
5.6. View Active Process List

- The 'Active Process List' shows all currently running processes started by applications currently running on your system.
- CCS can trace an application's parent process to detect whether a non-trusted application is attempting to spawn a trusted application. CCS can then deny access rights to that trusted application.
- This level of inspection provides the very highest protection against malware and rootkits that try to use trusted software to launch an attack.

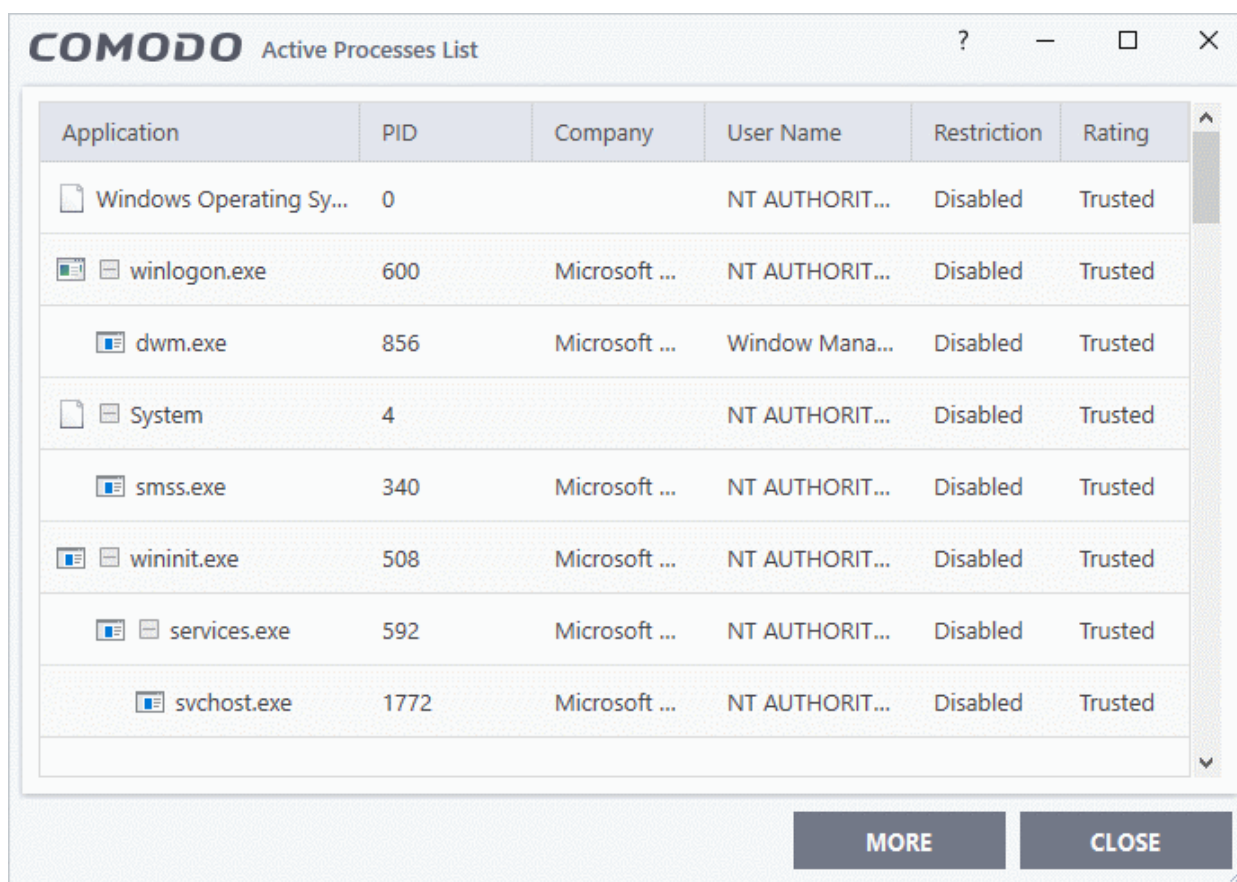
- The interface also lets you run an online lookup on the parent application, so you can check its trust rating on the latest cloud databases. You can also submit an application to Comodo for analysis, kill unwanted processes and more.

View Active Processes

- Open the 'Advanced Tasks' interface then click 'View Active Processes'.



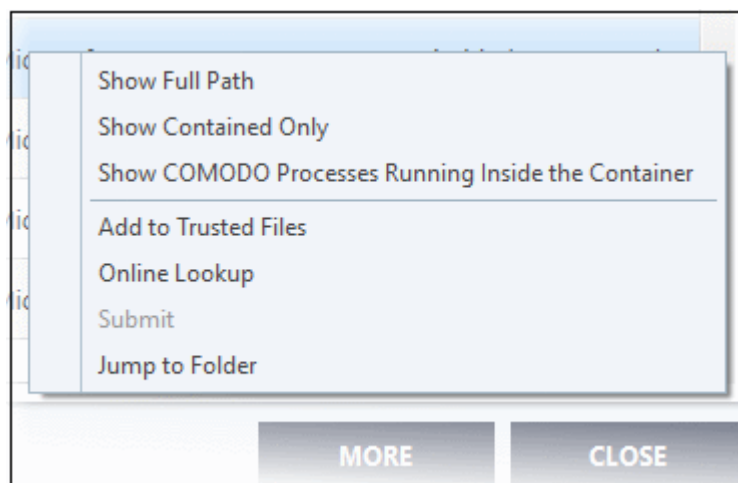
The interface shows all processes currently running on your computer:



Column Descriptions

- **Application** - The name of the running process
- **PID** - Process Identification Number.
- **Company** - Displays the name of the software developer.
- **User Name** - The name of the user that started the process.
- **Restriction** - Displays the level of containment setting selected for the program.
- **Rating** - Displays the rating of the application whether trusted or unknown.

Right-click on any process to:



- **Show full path:** Displays the location of the executable in addition to its name.

- Show Contained Only: Displays the details of the contained programs only.
- Show COMODO Processes Running Inside the Container: Will only show Comodo processes running inside the container.
- Add to Trusted Files: The selected unknown program is added to CCS **File List** with Trusted Status. See **File List** for more details.
- Online Lookup: The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: The folder containing the executable file of the application will open.
- Show Activities: Opens the **Process Activities List dialog**. The Process Activities dialog will display the list activities of the processes run by the application. The 'Show Activities' option is available only if **Viruscope** is enabled under **Advanced Settings > Advanced Protection > Viruscope**.

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

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

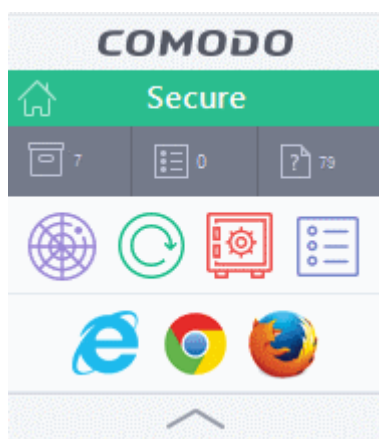
Viewing Active Processes list of Contained Applications

CCS allows you to view only the processes initiated by the applications that are running inside containment, by clicking a shortcut from the CCS widget. These applications include:

- Auto-Containment - Applications that are run inside the containment as per the rules defined for them or by default containment rules. See '**Auto-Containment Rules**' for more details on defining auto-containment rules.
- Run Virtual - Applications that are selected and run in Containment. See '**Run an Application in Containment**' for more details.
- Applications that are run inside the containment using the context sensitive menu - **Click here** for more details.
- Running browsers inside the containment from Widget - **Click here** for more details.
- Programs that are added manually - See '**Auto-Containment Rules**' for more details.

To view Active Process list of contained applications

- Click the first box in the second row in the CCS Widget.



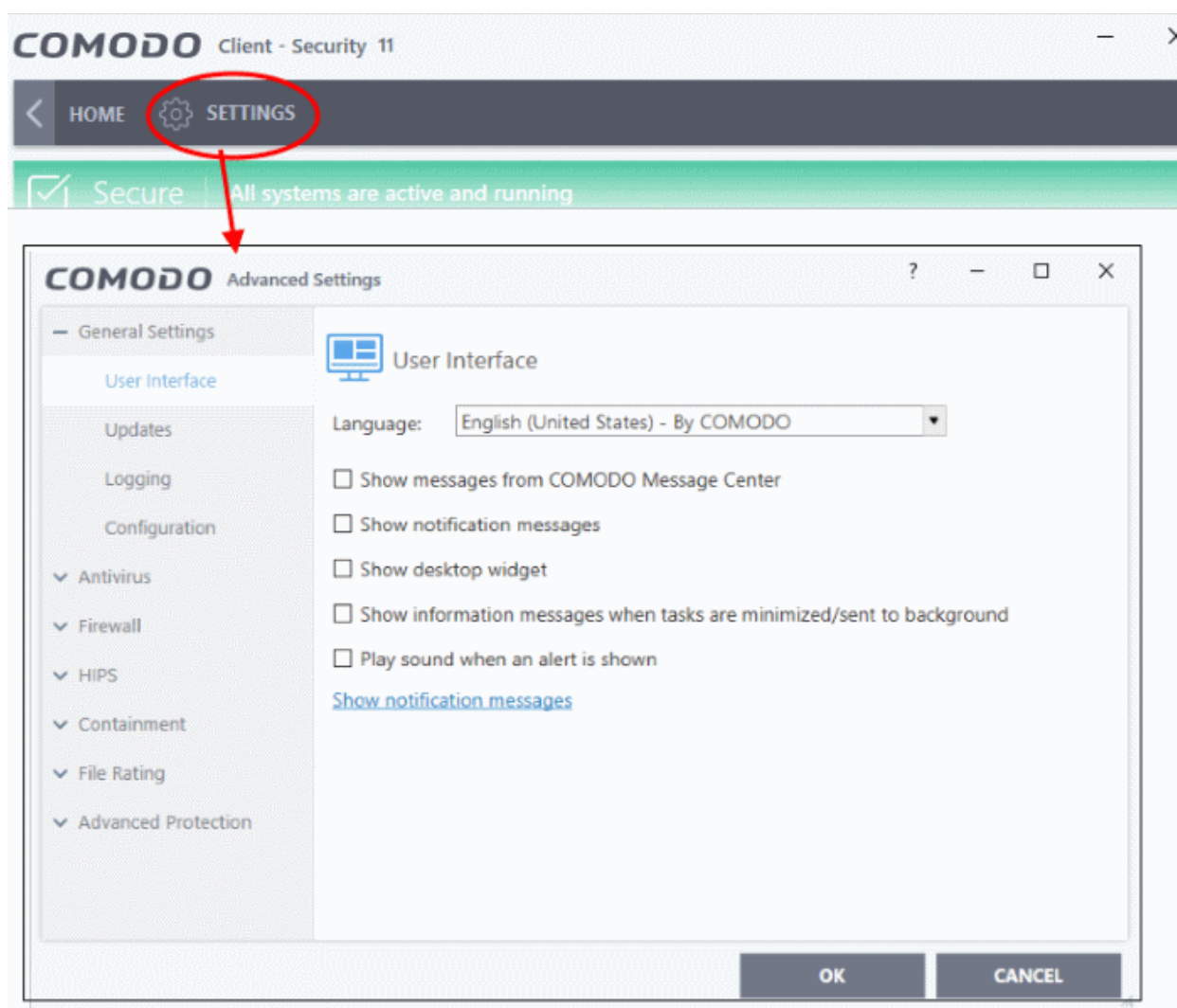
The Active Processes List (Contained Only) screen will be displayed.

Application	PID	Company	User Name	Restriction	Rating
cmdvirth.exe	6816	Comodo Se...	NT AUTHORITY...	Fully Virtu...	Trusted
svchost.exe	2296	Microsoft ...	NT AUTHORITY...	Fully Virtu...	Trusted
svchost.exe	2884	Microsoft ...	NT AUTHORITY...	Fully Virtu...	Trusted
svchost.exe	6788	Microsoft ...	NT AUTHORITY...	Fully Virtu...	Trusted
svchost.exe	2456	Microsoft ...	NT AUTHORITY...	Fully Virtu...	Trusted
firefox.exe	5764	Mozilla Cor...	DESKTOP-HI95...	Fully Virtu...	Trusted

MORE
CLOSE

6. CCS Advanced Settings

- Click 'Settings' on the home screen then 'Advanced Settings'
- The 'Advanced Settings' area lets you configure every aspect of the operation, behavior and appearance of Comodo Client Security.
 - 'General Settings' - Specify top-level preferences regarding the interface, updates and event logging.
 - Advanced users can delve into the granular configuration of each module, including antivirus, firewall, HIPS, containment, file rating and advanced protection.



The left hand menu lets you access the following areas:

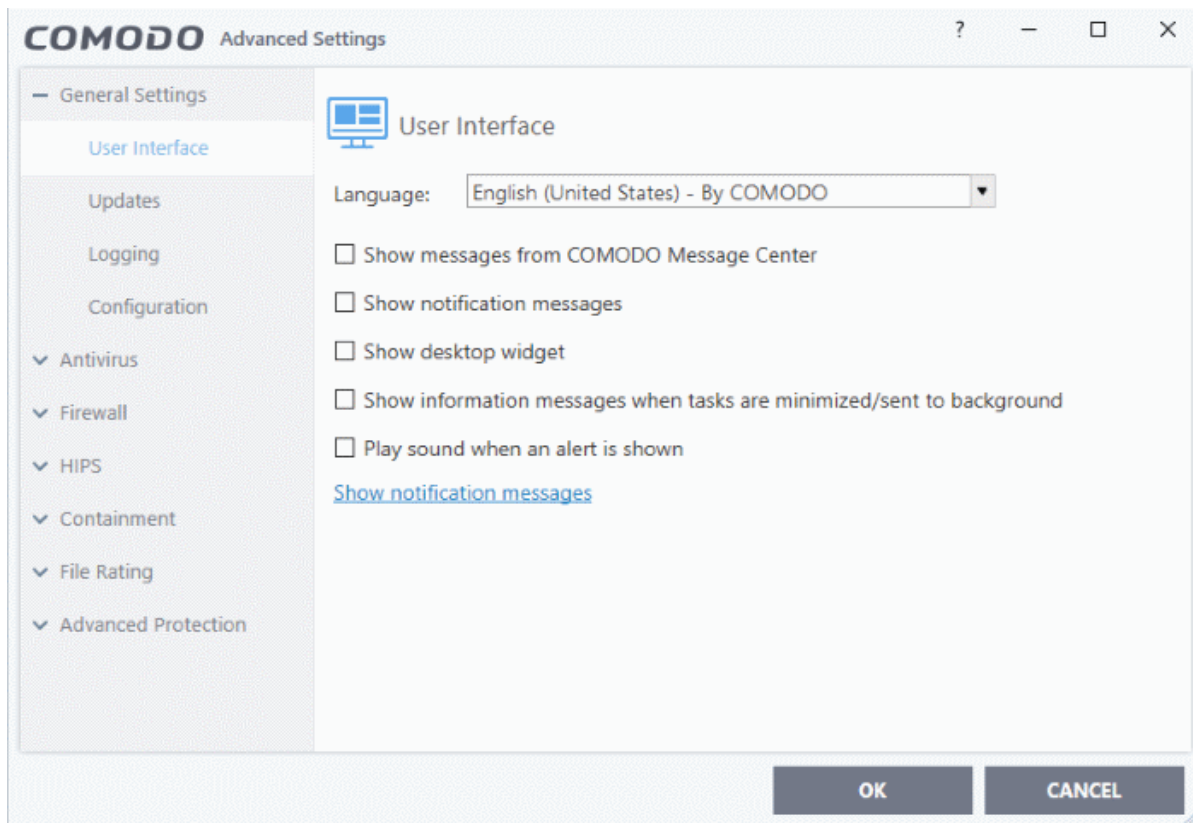
- **General Settings** - Allows you to configure the appearance and behavior of the application
 - **Customize User Interface**
 - **Configure Virus database Updates**
 - **Log Settings**
 - **Manage CCS Configurations**
- **Antivirus Settings**
 - **Real-time Scanner Settings**
 - **Scan Profiles**
 - **Exclusions**
- **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**
- **HIPS Groups**
- **Containment Settings**
 - **Containment - An Overview**
 - **Unknown Files: The Scanning Process**
 - **Containment Settings**
 - **Auto-Containment Rules**
 - **Protected Objects – Containment**
 - **Virtual Desktop Settings**
- **File Ratings**
 - **File Rating Settings**
 - **File Groups**
 - **File List**
 - **Submitted Files**
 - **Vendor List**
- **Advanced Protection**
 - **VirusScope Settings**
 - **Exclusions**
 - **Device Control Settings**
 - **Script Analysis Settings**
 - **Miscellaneous**

6.1. General Settings

This area lets you customize the appearance and overall behavior of Comodo Client Security. You can configure interface language, notification messages, automatic updates, logging and more.

- Click 'Settings' on the CCS home screen
- Click 'General Settings' on the left:



General Settings is broken down into the following areas:

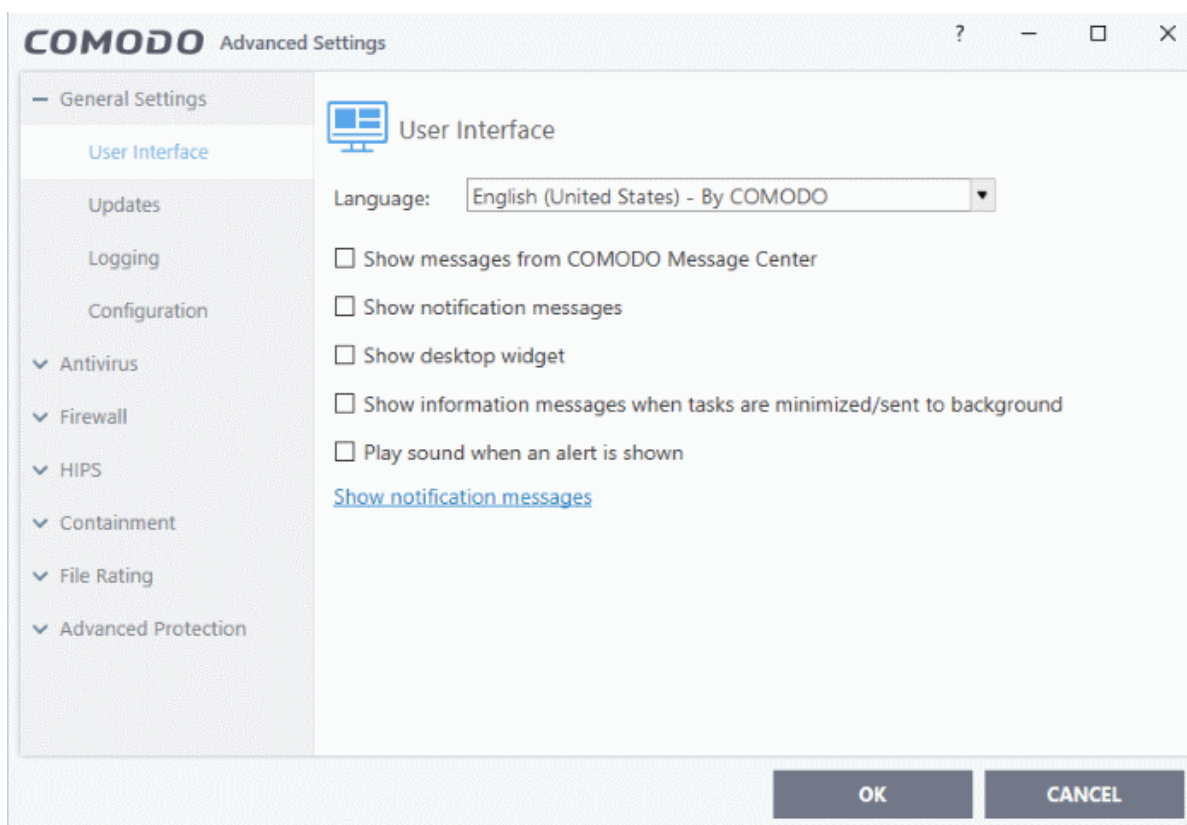
- **User Interface**
- **Updates**
- **Logging**
- **Configuration**

6.1.1. Customize User Interface

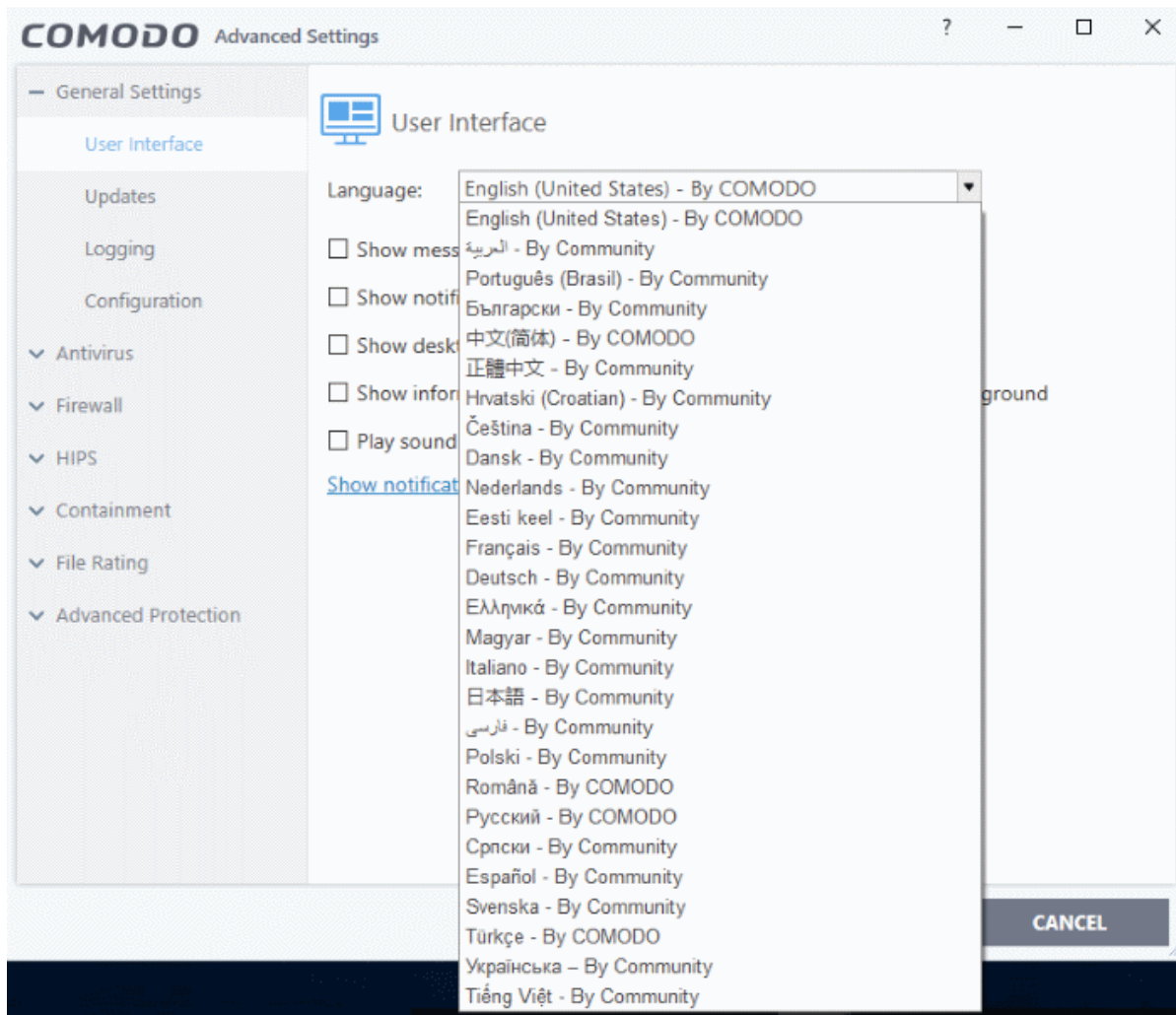
The 'User Interface' tab lets you choose your preferred language and customize the look and feel of the application. You can also configure how messages are displayed and enable password protection of your settings.

Open the user interface screen:

- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'User Interface' on the left:



- **Language Settings** - Comodo Client Security is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (**Default = English (United States)**).

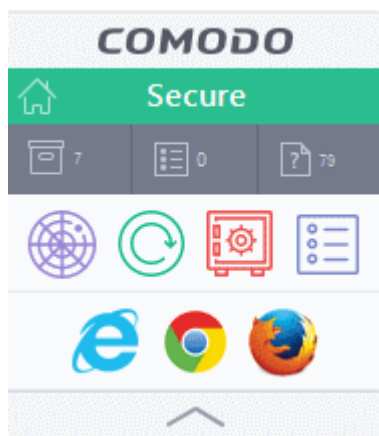


- **Show messages from COMODO Message Center** - If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world.



They contain news about product updates, occasional requests for feedback and info about other Comodo products you may want to try. (**Default = Disabled**).

- **Show Notification Messages** - If enabled, Comodo Client Security displays notification messages on every event that occurs as per CCS rules and settings. (**Default = Enabled**)
- **Show desktop widget** - The widget displays information about your security status, the number of background CCS tasks that are running, and lets you launch your browsers inside the container.

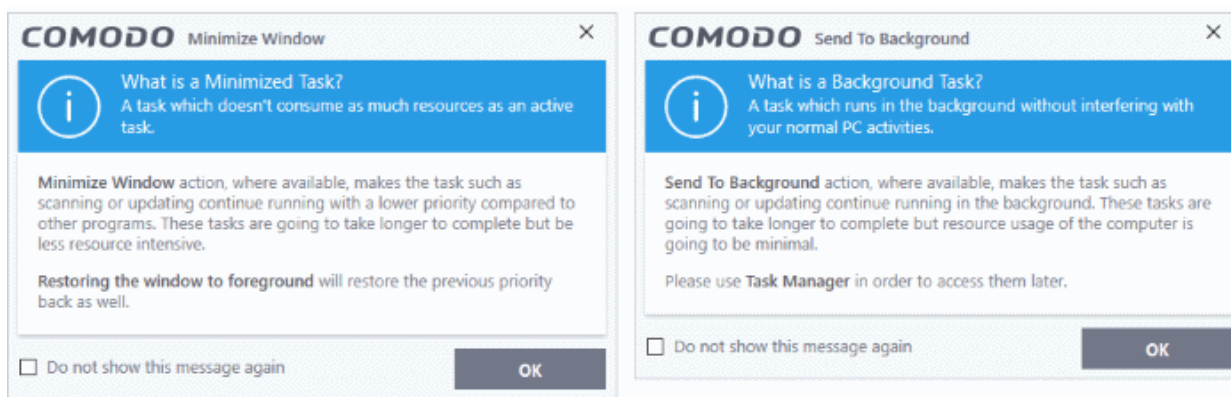


The widget also acts as a shortcut to open the CCS main interface.

Clear this checkbox If you do not want the widget to be displayed on your desktop. (**Default = Disabled**).

Tip: You can disable the widget from the CCS system tray icon. Right click on the CCS system tray icon and deselect the 'Show' option that appears on hovering the mouse cursor on 'Widget'.

- **Show information messages when tasks are minimized/sent to background** - CCS displays messages explaining the effects of minimizing or moving a running task like an AV scan to the background:



If you do not want these messages to be displayed, clear this check-box (**Default = Disabled**).

Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **Play sound when an alert is shown** - CCS generates a chime whenever it raises a security alert to grab your attention. If you do not want the sound to be generated, clear this check box (**Default = Disabled**).
- **Show notification messages** - Clicking this link will take you to the Windows 'Notifications & actions' settings screen for configuration. This is applicable for Windows 10 operating system. For lower versions of Windows, this option will be available as a checkbox.

If enabled, CCS system notices appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CCS is taking and any CCS status updates. For example 'Comodo Firewall is learning' or 'HIPS' is learning' are generated when these modules are learning the activity of previously unknown components of trusted applications (**Default = Disabled**).

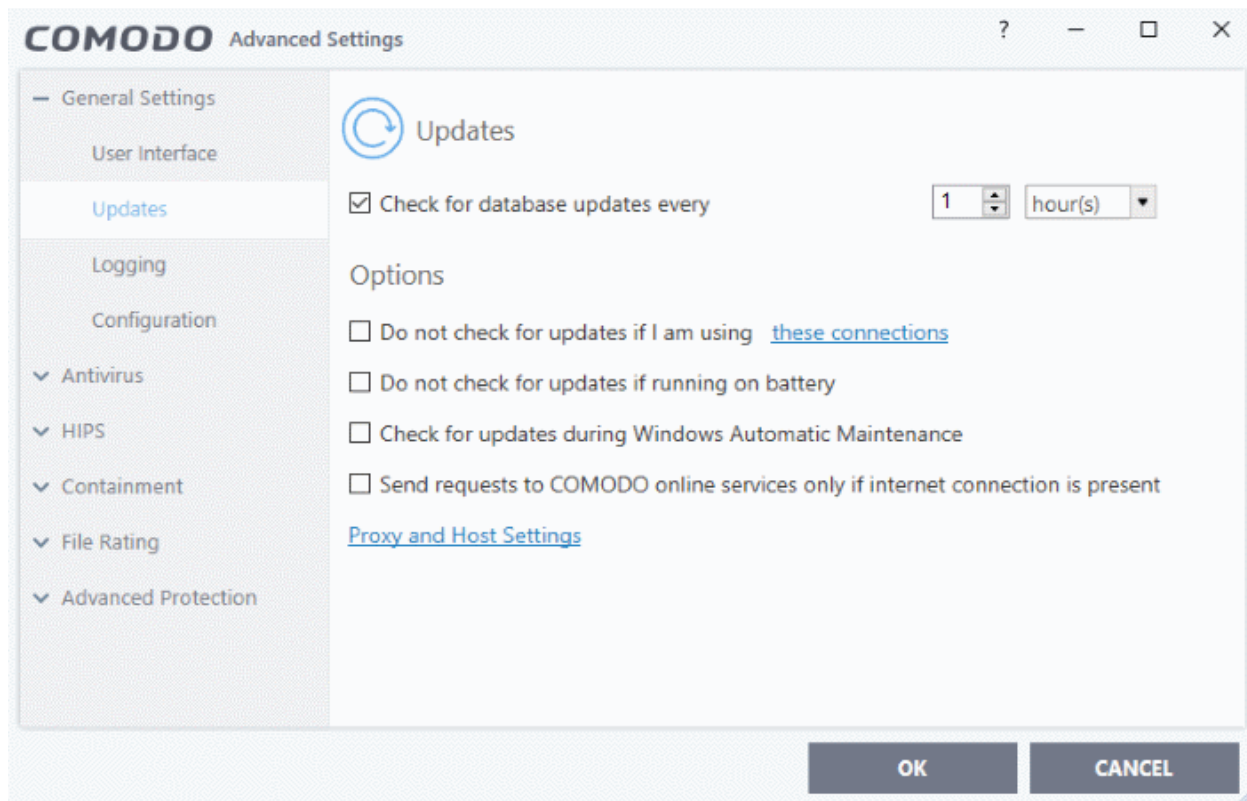
Note: The default settings are governed by the Endpoint Manager profiles applied to Comodo Client Security.

6.1.2. Configure Virus Database Updates

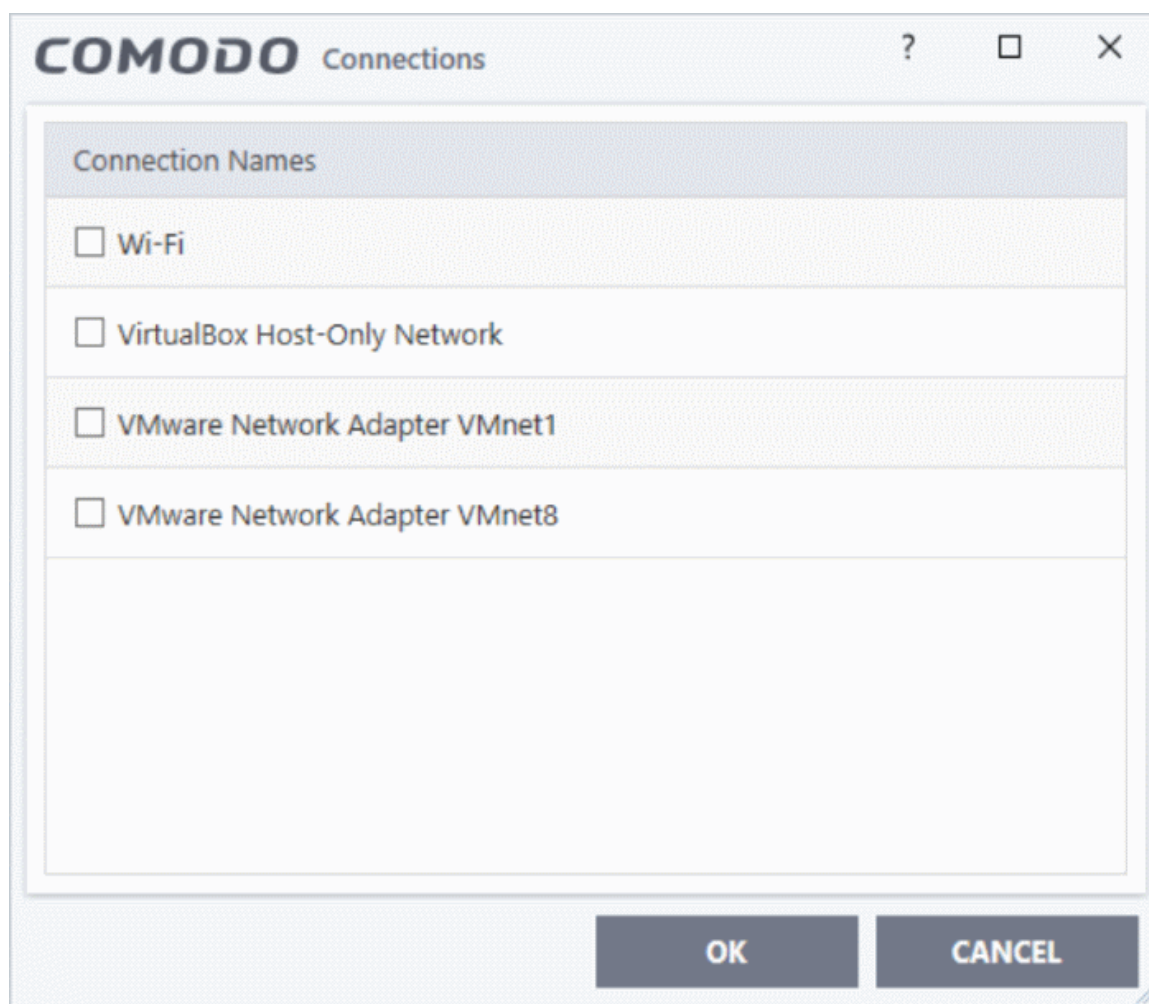
The 'Updates' area lets you configure settings that govern CCS virus database updates.

To open the user interface screen:

- Click 'Settings' on the CCS home \ tasks screen to open the 'Advanced Settings' interface.
- Click 'General Settings' > 'Updates' on the left:



- **Check for database updates every NN hour(s)/day(s)** - Lets you set the interval at which CCS should check for virus database updates. (**Default and recommended = 1 hour**)
- **Do not check updates if am using these connections** - Allows you to stop CCS checking for updates if you are using specific internet connections. For example, you may not wish to check updates if using a wireless connection you know to be slow or not secure (**Default = Disabled**)
- To do this:
 - Select the 'Do not check updates if am using these connections' check-box
 - Then click the 'these connections'. The connections dialog will appear with the list of connections you use.



- Select the connection through which you do not want CCS to check for updates and click OK.
- **Do not check for updates if running on battery** - If enabled, CCS will not download updates if it detects your computer is running on battery power. This is intended to extend battery lifetime on laptops. (**Default = Disabled**).
- **Check for updates during Windows Automatic Maintenance** - If enabled, CCS will check for and download updates when Windows is updating itself.
- **Send requests to COMODO online services only if internet connection is present** – CCS requires an internet connection to connect to Comodo services such as FLS, LVS (Endpoint Manager), download.comodo.com, Valkyrie and so on. (**Default = Disabled**).

This is how CCS will proceed if you enable or disable this setting:

- **Enabled + No internet connection** - CCS will not make requests to Comodo online services. A failure message is shown if users attempt a manual lookup, submit or update.
- **Enabled + Connected to Internet** - CCS will make requests to Comodo online services.
- **Disabled + Connected to Internet** – CCS will make requests to Comodo online services.
- **Disabled + No internet connection** - CCS will make requests to Comodo online services, but will not be able to connect. An error message is shown.
- **Proxy and Host Settings** - Allows you to select the host from which updates are downloaded. By default, CCS will download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CCS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CCS at this proxy/staging

server. This helps to conserve bandwidth and accelerate the update process when a large number of endpoints are involved.

Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from <http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php>

To configure updates via proxy server

- Click 'Proxy and Host Settings' at the bottom of the 'Updates' interface. The 'Proxy and Host Settings' interface will open.

COMODO Proxy and Host Settings

Use proxy

Host:

Port:

Use authentication

Login:

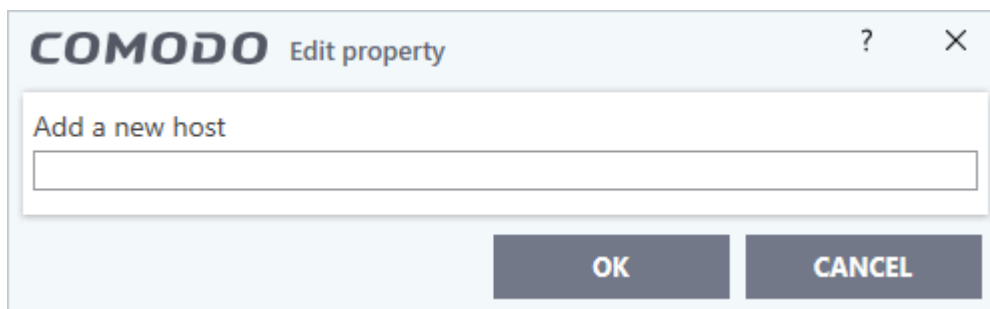
Password:

+ Add ✎ Edit ✕ Remove ↑ Move Up ↓ Move Down

<input type="checkbox"/>	Servers	Status
<input checked="" type="checkbox"/>	http://download.comodo.com/	<input checked="" type="checkbox"/>

OK CANCEL

- Select the 'Use Proxy' checkbox.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- You can add multiple servers from which updates are available. To do this, click 'Add' at the top of the 'Servers' panel then enter the host name in the 'Edit Property' dialog.



- If you specify multiple servers:
 - Activate or deactivate each update server using the 'Active' toggle switch beside it.
 - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CCS will commence downloading from the first server that contains new updates.
- Click 'OK' for your settings to take effect.

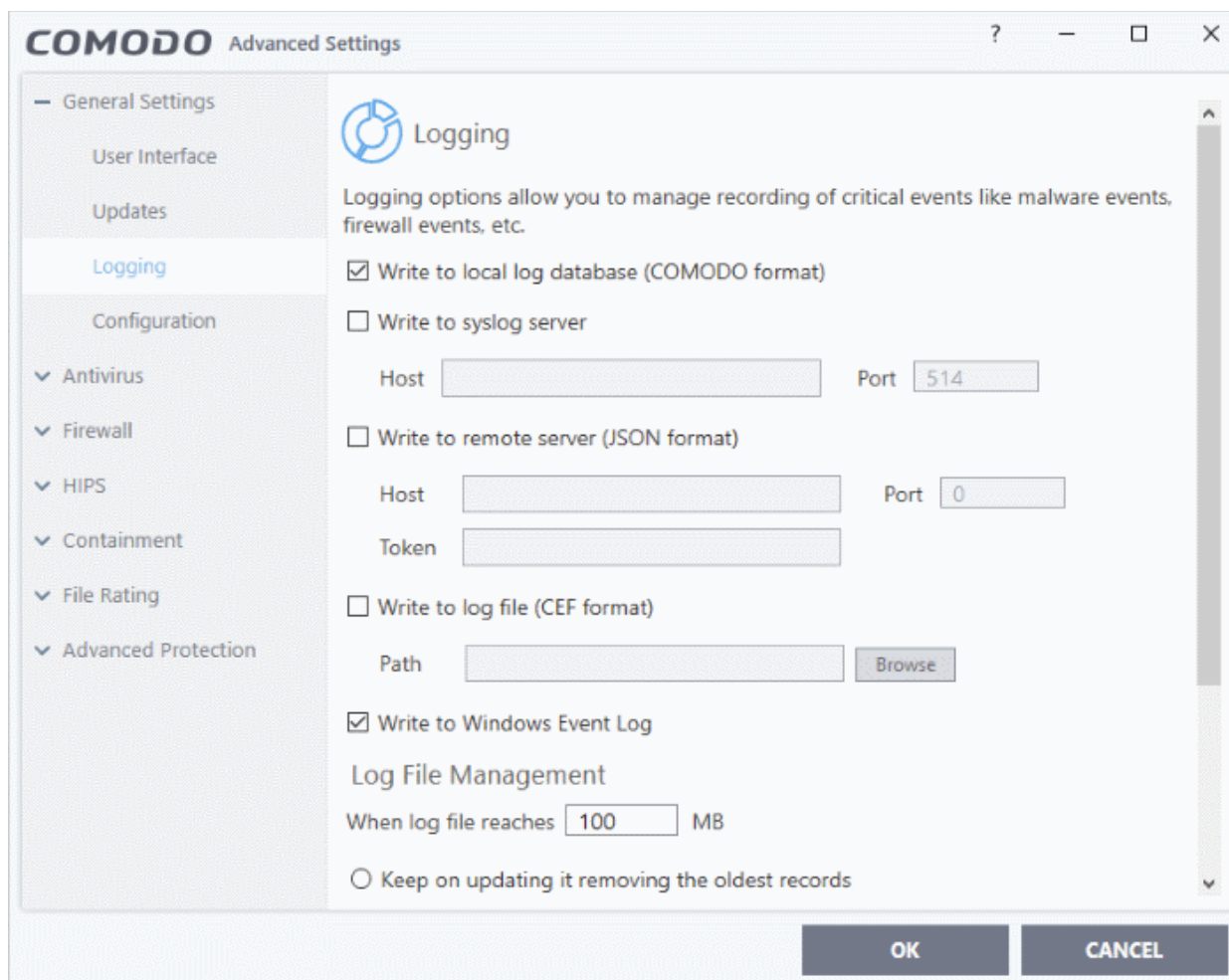
6.1.3. Log Settings

- Comodo Client Security keeps detailed records of all events generated by its security modules.
- The logging interface lets you specify the location to store logs, the maximum size of log files, and how CCS should react if the maximum file size is exceeded.

Note: Click 'Tasks' > 'Advanced Tasks' > 'View Logs' to actually view and manage logs.

Open the logging configuration screen:

- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Logging' on the left:



Logging Options

- **Write to local log database (Comodo format)** - Instructs CCS to store the log files in the local storage of the endpoint in Comodo format so that they can be viewed from Tasks > Advanced Tasks > View Logs interface. See '**View CCS Logs**' for more details. The Log storage depends on the log file management settings configured in the '**Log File Management**' settings area in the same interface. **(Default = Enabled)**.
- **Write to Syslog Server (CEF Format)** - Instructs CCS to forward the log files to an external Syslog Server integrated with the Endpoint Manager (EM) server that remotely manages your CCS installation. Enter the IP address/hostname of the Syslog server in the Host text field and enter the port through which Syslog server listens to EM in the 'Port' field. **(Default = Disabled)**.
- **Write to remote server (JSON format)** - Instructs CCS to forward the log files to HTTPS in JSON format on a remote server integrated with the EM server that remotely manages your CCS installation. Enter the IP address/hostname of the remote server in the Host text field and enter the port through which remote server listens to EM in the 'Port' field. Enter the security token to access the remote server in the Token text field. **(Default = Disabled)**.
- **Write to Log file (CEF) Format** - Instructs CCS to store the log files at a specified location in the local storage or a network storage, in Common Event Format (CEF) format, also known as NCSA Common Log Format, which is standardized text file format. When selecting this option, click 'Browse', select the storage location and navigate to the log file to which the logs are to be added. **(Default = Disabled)**.
- **Write to Windows Event Logs** - Instructs CCS to store the log events to the Windows Event Logs. **(Default = Enabled)**

Log File Management

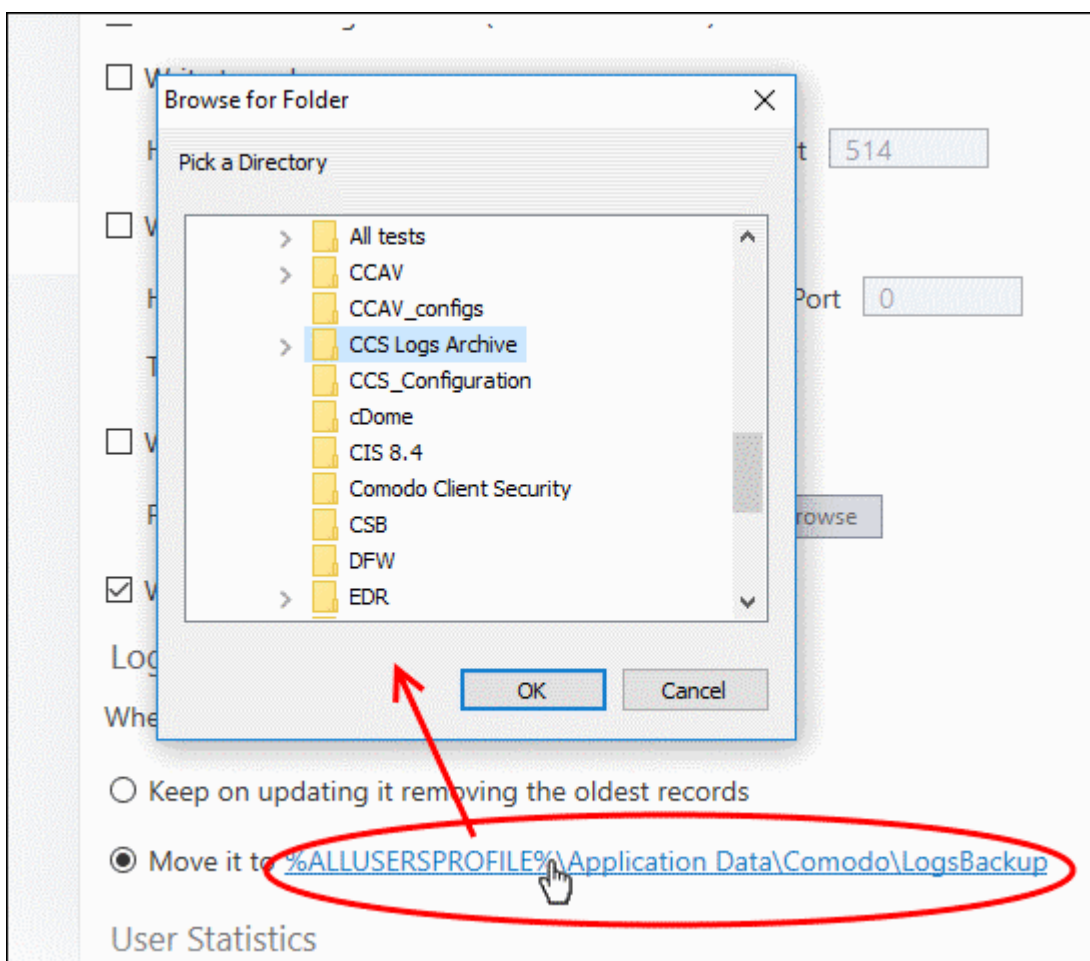
- **If the log file's size exceeds (MB)** - Enables you to specify behavior when the local log database (Comodo format) log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to

discard them depending on your future reference needs and the storage capacity of your hard drive.

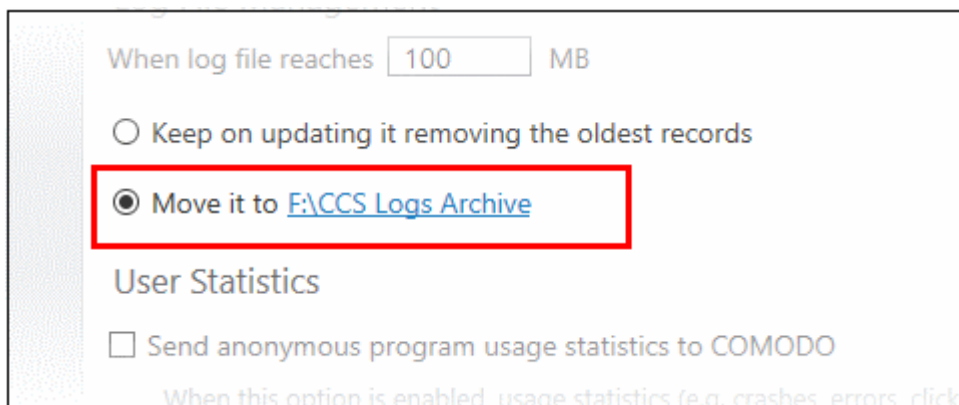
- Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' (**Default = 100MB**).

If you want to discard the log file if it reaches the maximum size, select **'Delete it and create a new one'**. Once the log file reaches the specified maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant (**Default = Enabled**).

If you want to save the log file even if it reaches the maximum size, select **'Move it to'** and select a destination folder for the log file (**Default = Enabled and stored in 'All Users Profile' \Application Data\Comodo\LogsBackup**)



The selected folder path will appear beside 'Move it to'.



Once the log file reaches the maximum size, it will be automatically moved to the selected folder and a new log file

will be created with the log of events occurring from that instant.

User Statistics

- **Send anonymous program usage statistics to Comodo** - Comodo collects usage details so we can analyze how our users interact with CCS. This 'real-world' data allows us to create product improvements which reflect the needs of our users. If you enable this option, CCS 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)**

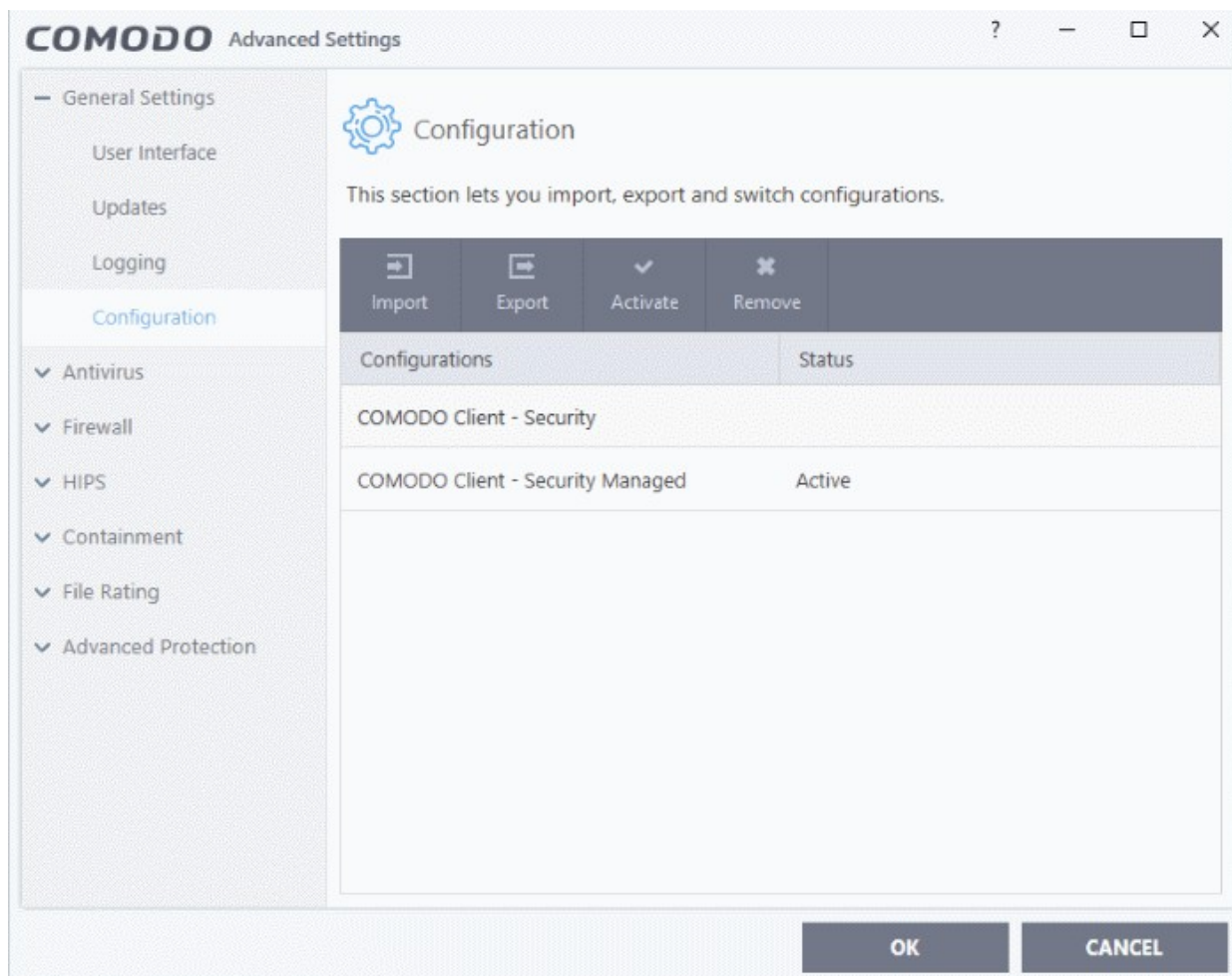
6.1.4. Manage CCS Configurations

- You can save and export your current security settings as a profile. This is especially useful if you are a network admin looking to roll out a standard security configuration across multiple computers.
- Exporting your settings is also useful if you need to uninstall and re-install Comodo Client Security. After re-installation, you can import your previous settings from the profile and avoid having to configure everything over again.

Note: Any changes you make over time will be automatically stored in the currently active profile. If you want to export your current settings then export the 'Active' profile.

To open the CCS configuration screen:

- Click 'Settings' on the CCS home \ tasks screen to open the 'Advanced Settings' interface.
- Click 'General Settings' > 'Configuration' on the left:



The currently active configuration is indicated under the 'Active' column. Click the following links for more details:

- **Comodo Preset Configurations**
- **Importing/Exporting and Managing Personal Configurations**

6.1.4.1. Comodo Preset Configurations

- Comodo preset configurations implement strong security settings on your endpoints.
- CCS ships with two preset configurations - 'Comodo Client Security' and 'Comodo Client Security Managed'.
 - 'Comodo Client Security Managed' is applied to managed endpoints by default.
 - 'Comodo Client Security' is applied to unmanaged endpoints
- Reminder - the active profile is, in effect, your current CCS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time from the 'Configuration' panel.

Comodo Client Security Managed - The default configuration for endpoints managed by Endpoint Manager. Important configuration information:

- HIPS is disabled.
- Auto-Containment is enabled.
- Viruscope is enabled.
- Realtime scan is enabled.
- Traffic filtering (Firewall) is enabled in Safe mode.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Advanced Protection is tuned to prevent infection of the system.
- Alert message notification is disabled.
- Viruscope alert is disabled

Comodo Client Security - The default configuration on standalone (unmanaged) computers. Important configuration information:

- HIPS is disabled.
- Auto-Containment is enabled.
- Viruscope is disabled.
- Realtime scan is enabled.
- Traffic filtering (Firewall) is enabled in Safe mode.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Advanced Protection is tuned to prevent infection of the system.
- Alert message notification is enabled.
- Viruscope alert is disabled

If you wish to switch to Comodo Client - Security option, you can **select** the option from the 'Configuration' panel.

6.1.4.2. Import/Export and Manage Personal Configurations

The CCS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Settings' at the top then 'Configuration' under 'General Settings' in the 'Advanced Settings' interface.

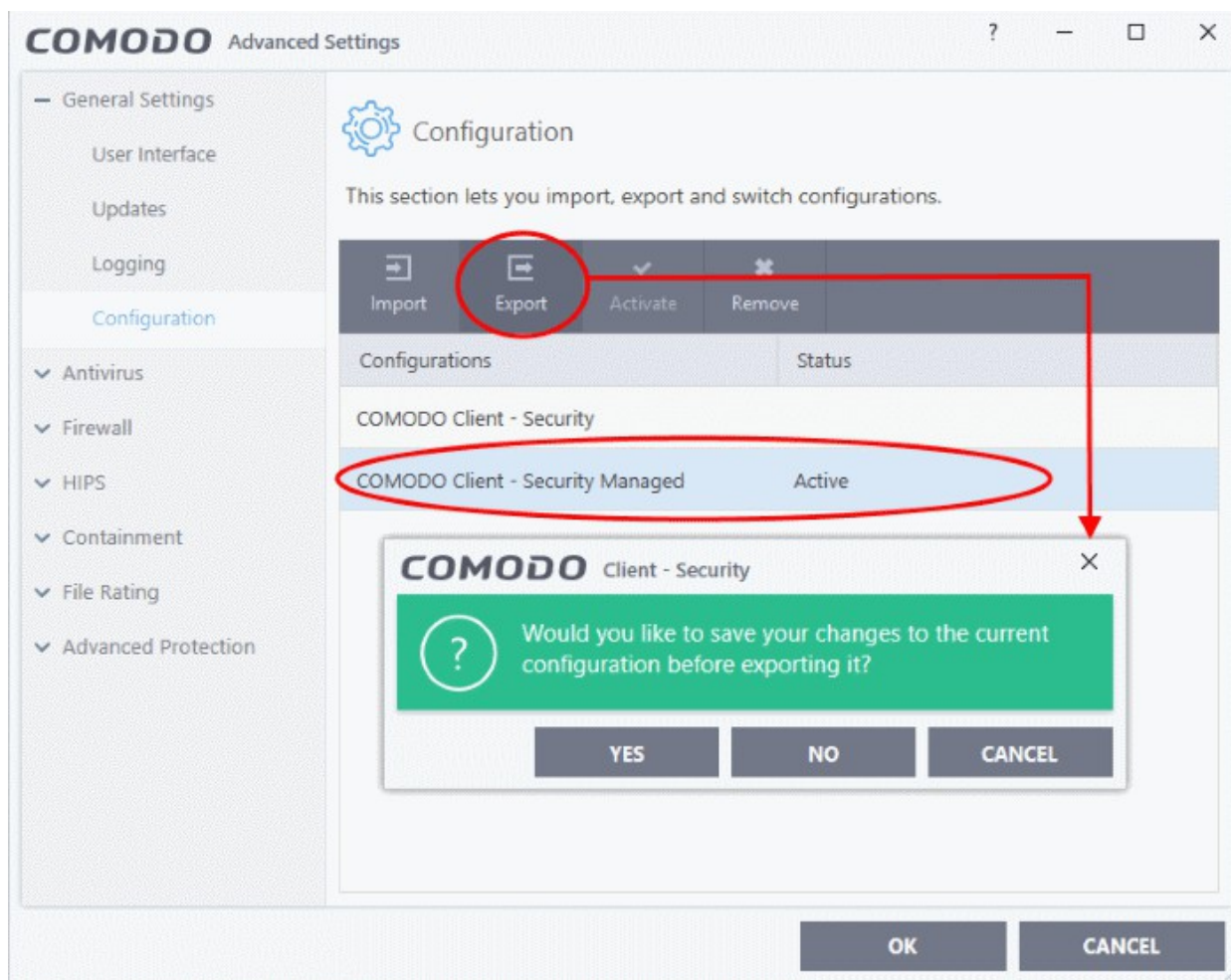
Click the area on which you would like more information:

- **Export a stored configuration to a file**

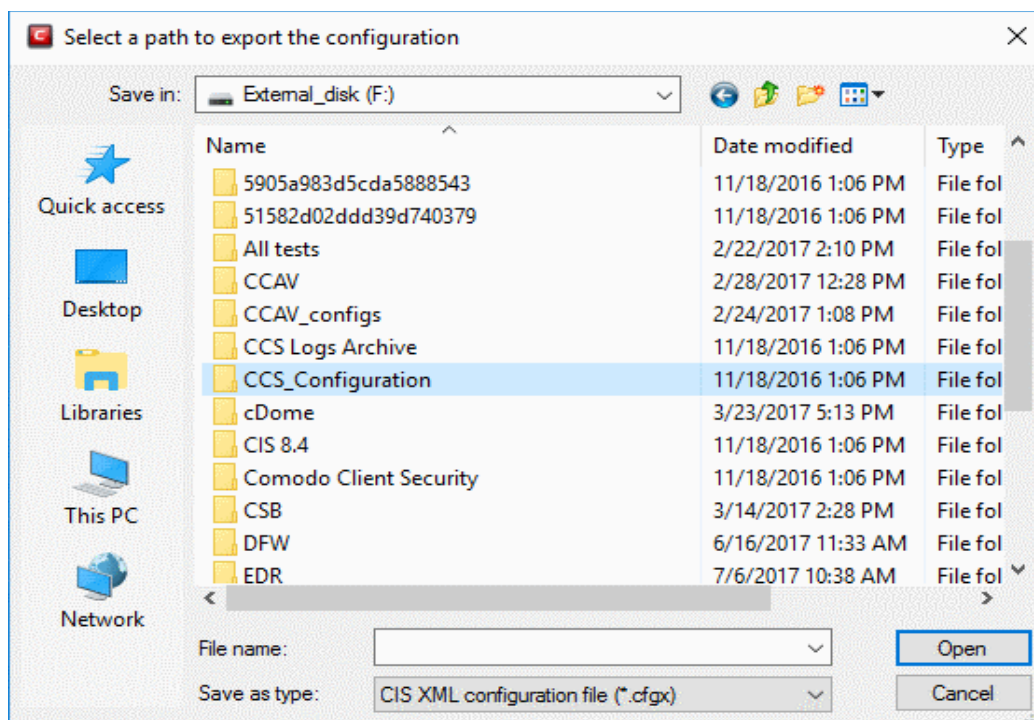
- **Import a saved configuration from a file**
- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

Exporting a stored configuration to a file

1. Open 'Configurations' panel by clicking 'Configuration' under 'General Settings' in the 'Advanced Settings' interface
2. Select the configuration and click 'Export' at the top.

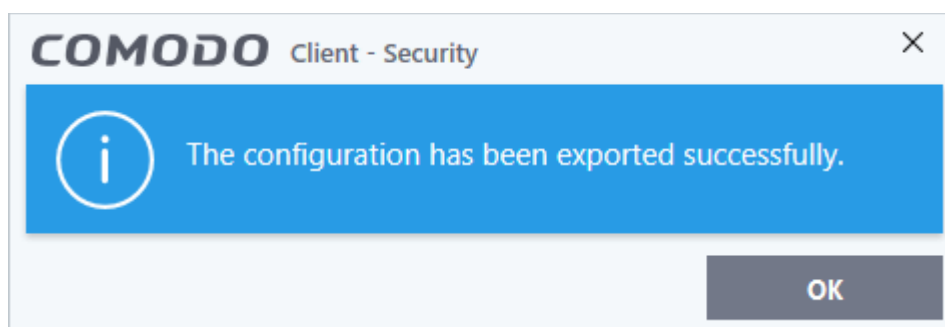


3. Select whether you want to save any changes done to the configuration before exporting it.
4. The Select a path to export the configuration dialog will open.



5. Navigate to the location where you want to save the configuration file, type a name (e.g., 'Default CCS Configuration') for the file to be saved in .cfgx format and click 'Save'.

A confirmation dialog will appear on successful export of the configuration.



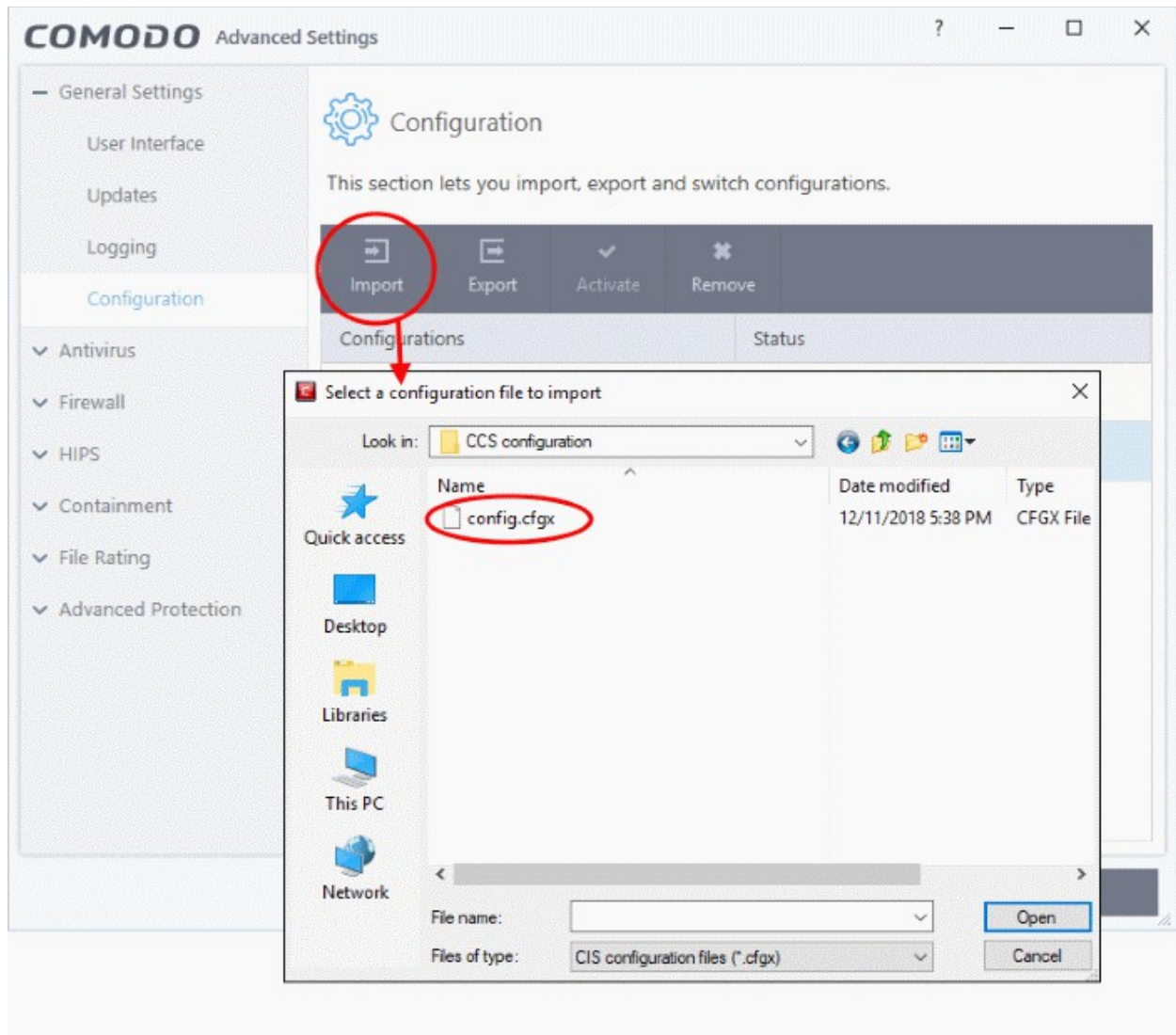
Importing a saved configuration from a file

Importing a configuration profile allows you to store any profile within Comodo Client Security. Any profiles you import do not become active until you **select them for use**.

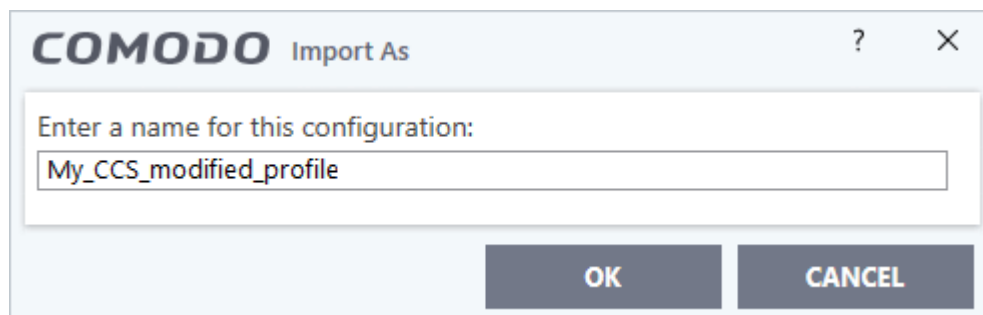
To import a profile

1. Open 'Configurations' panel by clicking 'Configuration' under 'General Settings' in the 'Advanced Settings' interface and click 'Import' at the top.

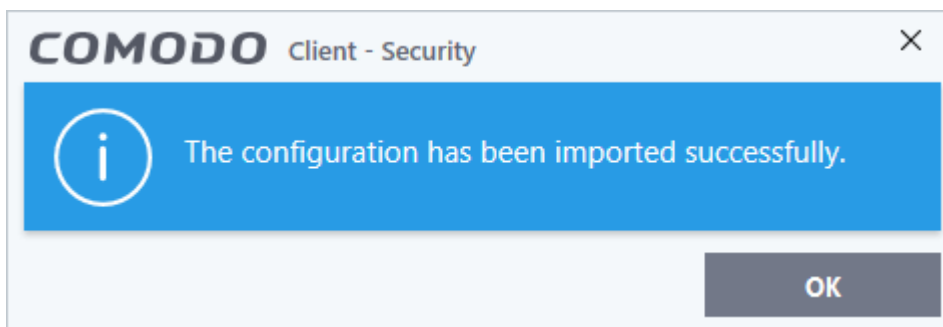
The 'Select a configuration file to import' dialog will open.



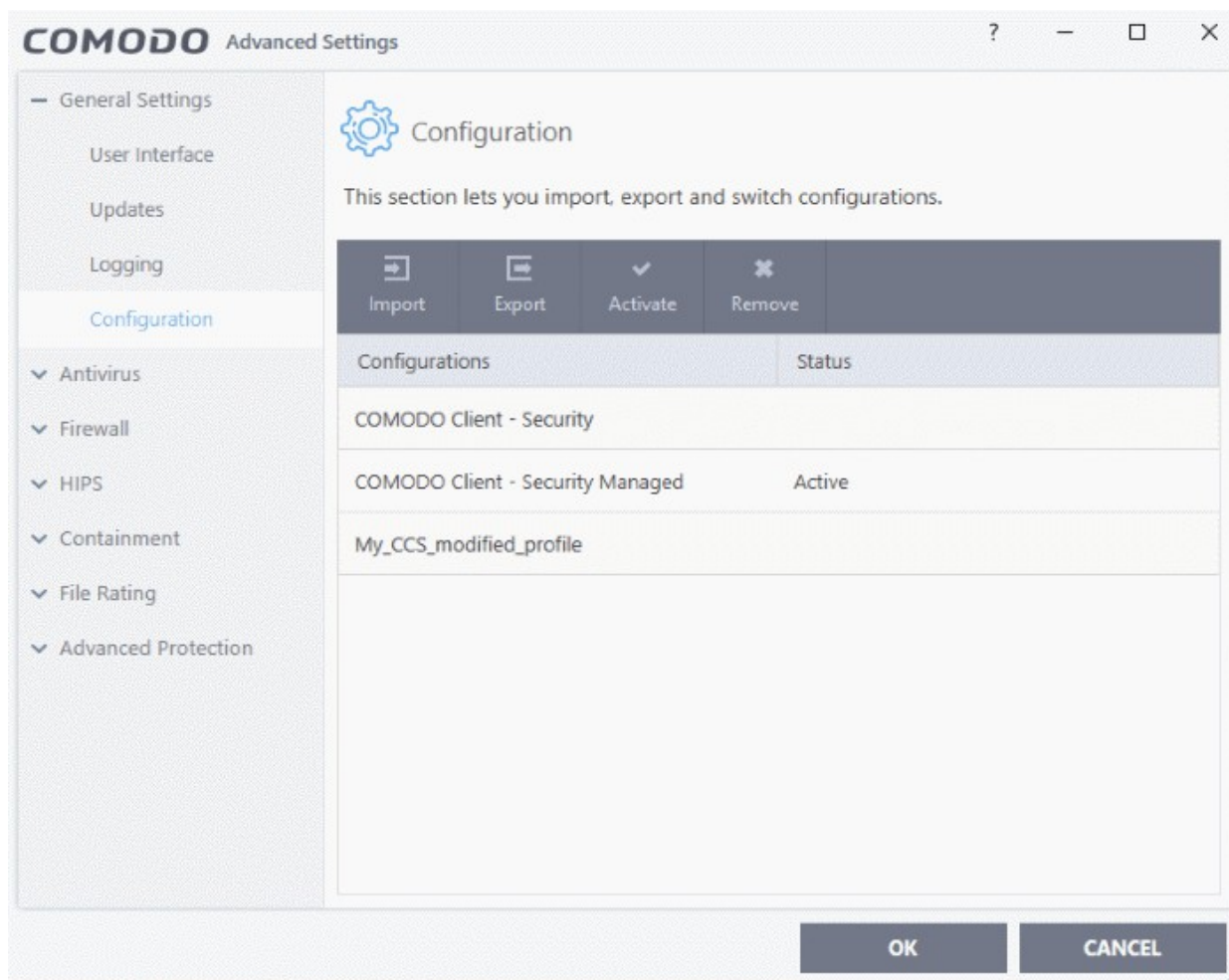
2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



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



Once imported, the configuration profile is available for deployment by **selecting it**.

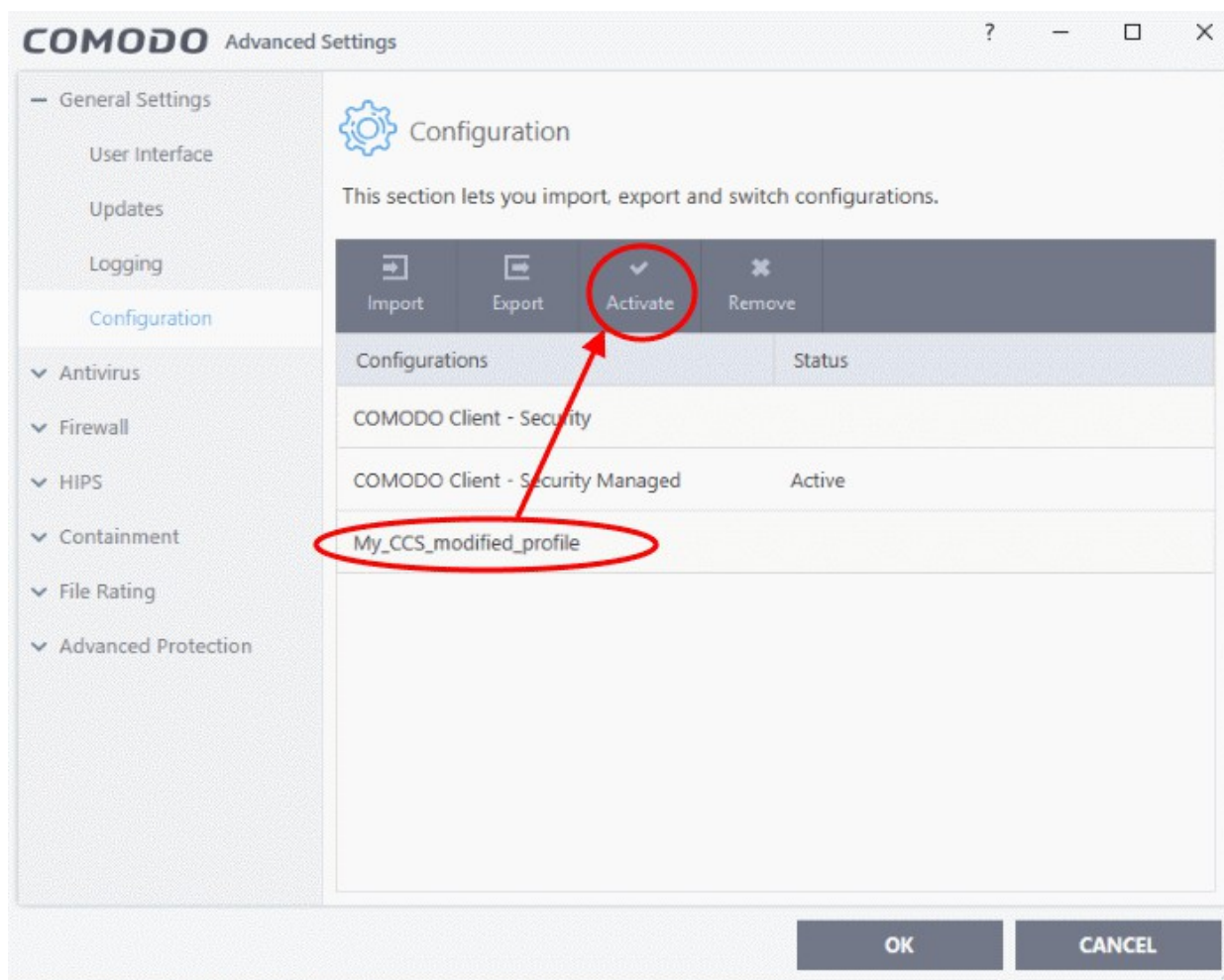


Selecting and Implementing a different configuration profile

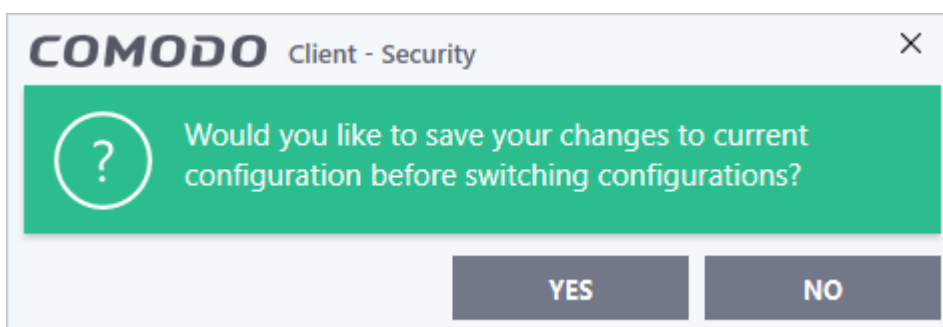
You can change the configuration profile active in CCS at any time from the 'Configurations' panel.

To change the active configuration profile

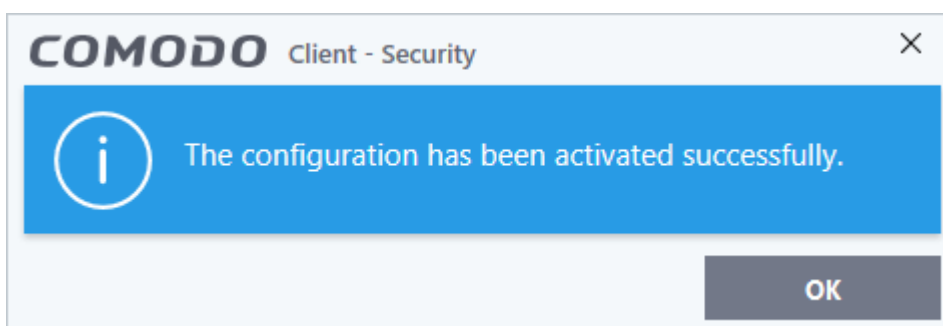
1. Open 'Configurations' panel by clicking 'Configuration' under 'General Settings' in the 'Advanced Settings' interface.
2. Select the configuration profile you want to activate and click 'Activate' at the top.



You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.



3. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

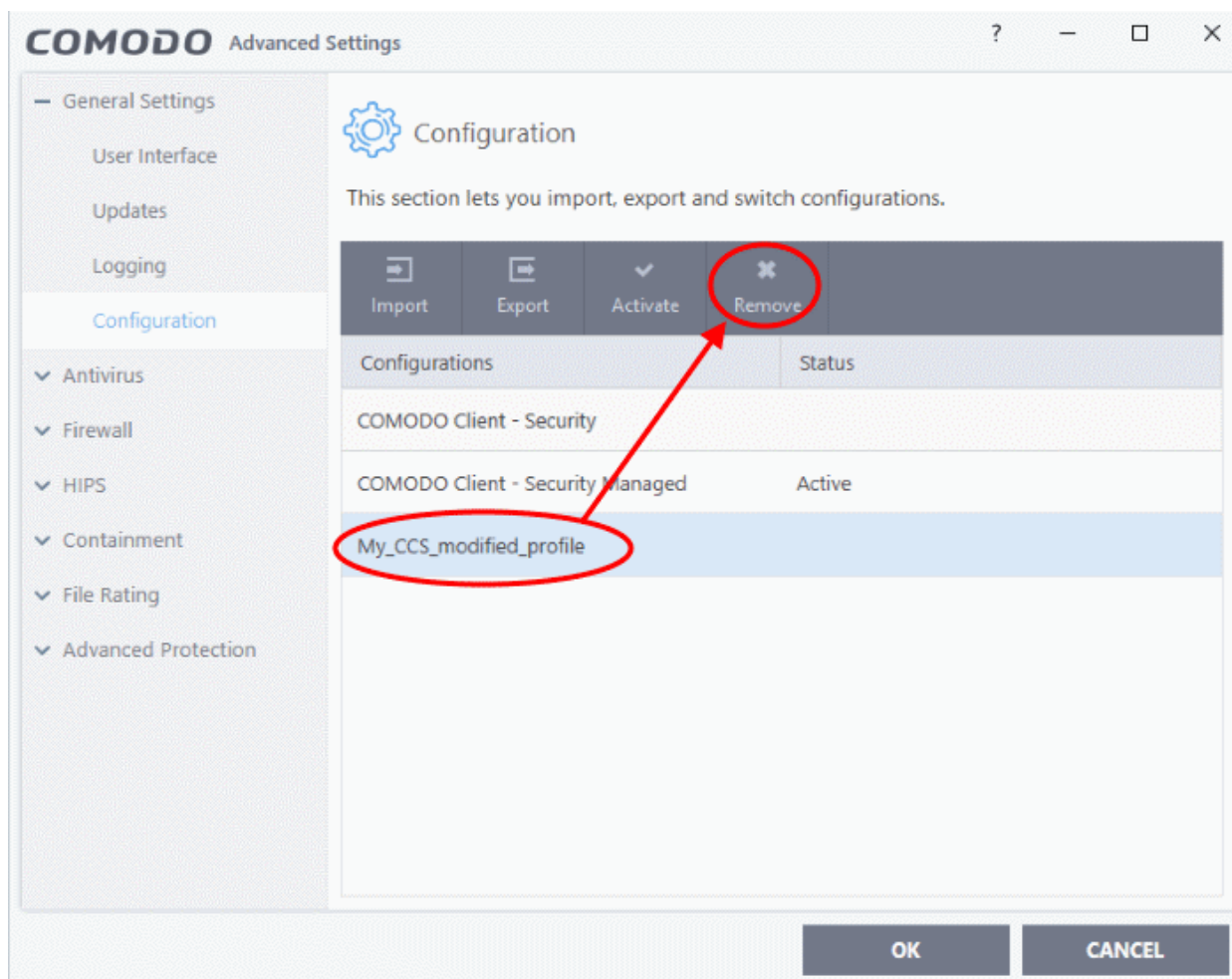


Deleting an inactive configuration profile

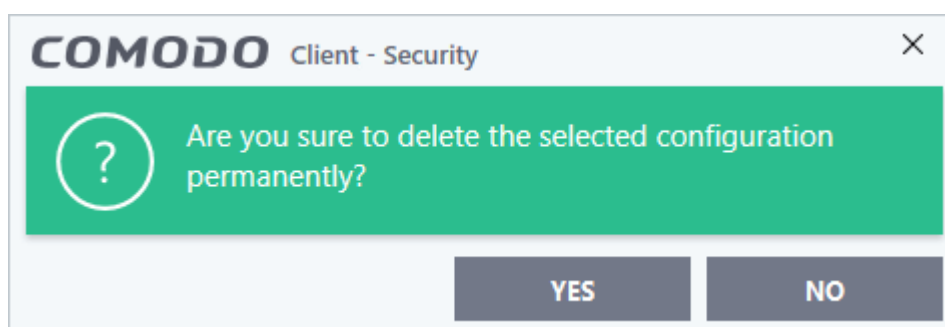
You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that Comodo Client Security is currently using - only the inactive ones. For example if the Comodo Client Security Managed is the active profile, you can only delete the inactive profiles, 'My_CCS_Configuration' and so on.

To remove an unwanted profile

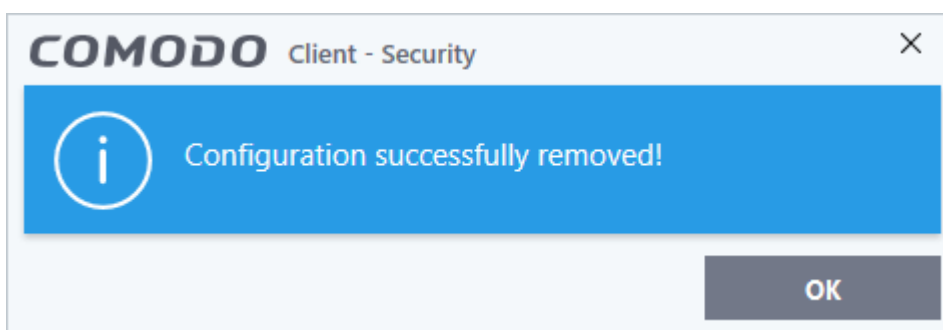
1. Open 'Configurations' panel by clicking 'Configuration' under 'General Settings' in the 'Advanced Settings' interface.
2. Select the configuration profile you want to delete and click 'Remove' at the top.



A confirmation dialog will be displayed.



3. Click 'Yes!'. The configuration profile will be deleted from your computer.

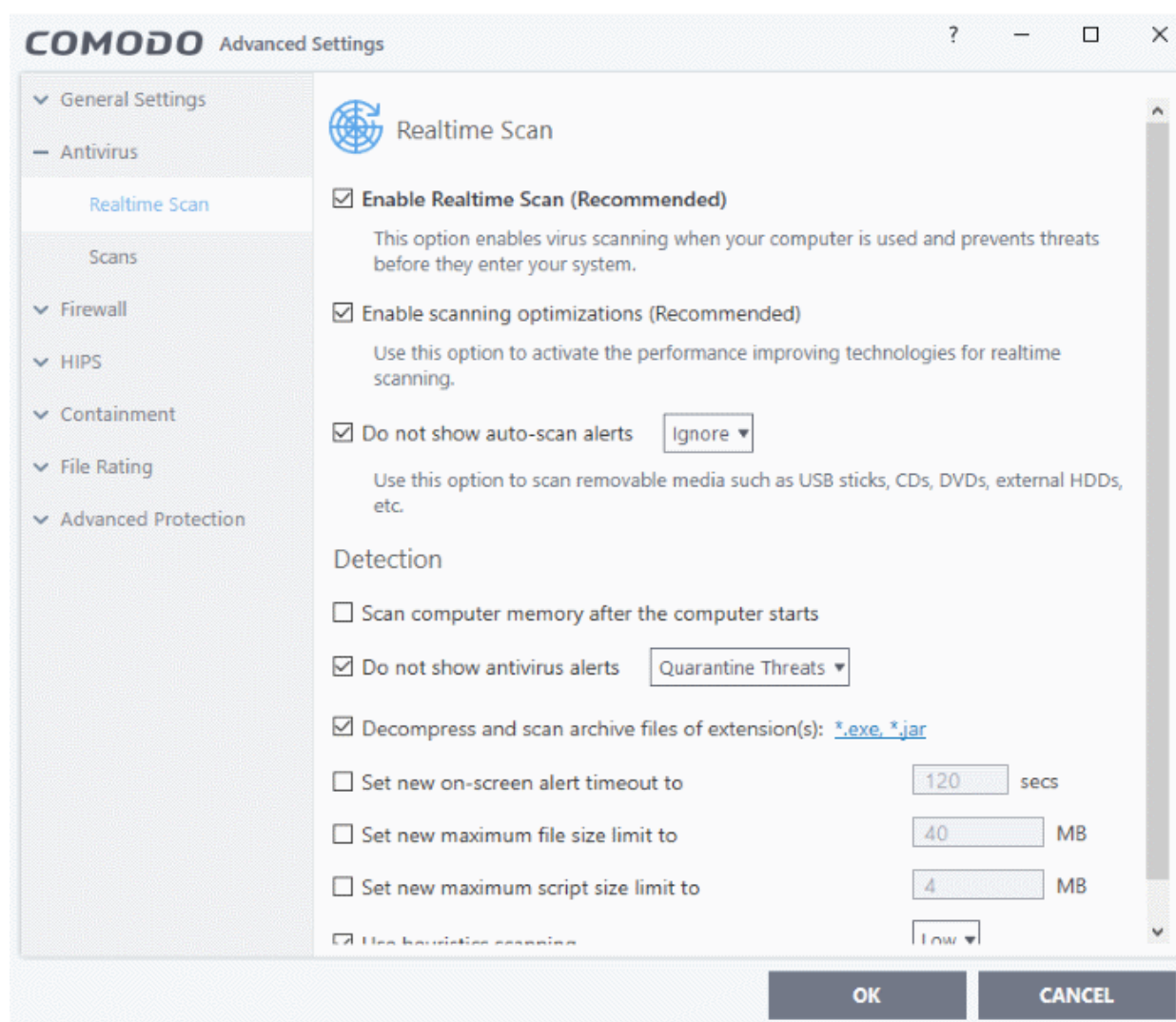


6.2. Antivirus Configuration

The antivirus settings area lets you configure the 'always on' realtime monitor and configure custom scan profiles.

To configure the 'Antivirus' components

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.



- Click 'Antivirus' in the left menu:

The following sections explain about:

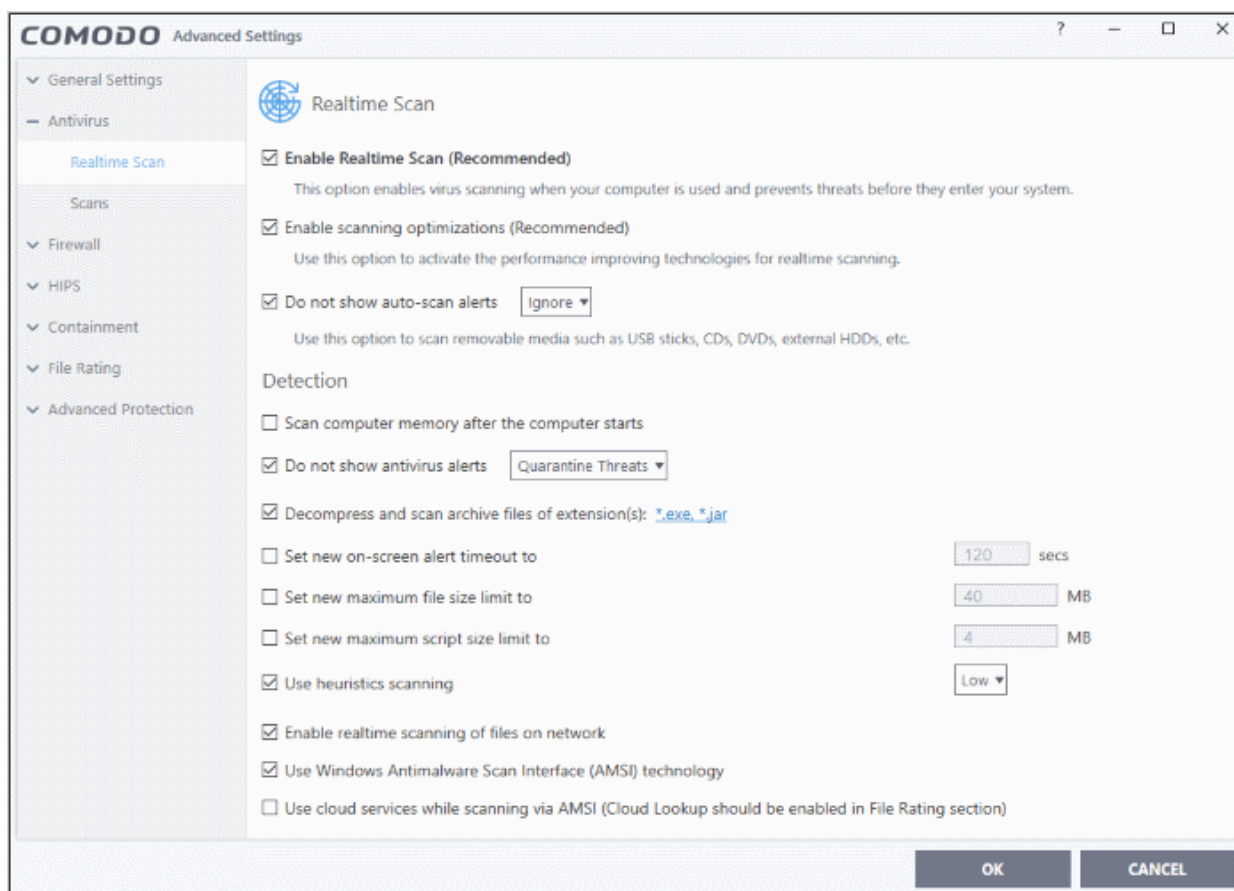
- **Real-time Scan Settings**
- **Custom Scan Profiles**

6.2.1. Real-time Scanner Settings

- The real-time virus scanner constantly monitors your system for threats. It checks files when they are created, opened or copied, and also checks system memory on computer startup.
- You can specify that CCS does not show you alerts when it finds a threat, but automatically deals with the threat. 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.

Open the Real Time Scan settings panel

- Click 'Settings' on the CCS home \ tasks screen to open the 'Advanced Settings' interface.
- Click 'Antivirus' > 'Realtime Scan' on the left:



- **Enable Realtime Scan** – Activate or deactivate real-time virus monitoring. Comodo 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** - Configure whether external devices such as hard drives and USB sticks should be automatically scanned when connected to the endpoint.
 - If you disable alerts, you need to choose a default response that CCS should take:
 - Ignore - The device will not be scanned
 - Scan - The device will be scanned for viruses using the settings in the 'Full Scan' profile
 - If you enable alerts, then a notification is shown to the user when an external device is connected. The user can choose to scan or ignore the device. See '**Auto Scan Alerts**' for more information.

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 but automatically...** - Configure whether or not alerts are shown when malware is encountered. **(Default = Enabled)**.

Choosing 'Do not show...' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CCS should automatically take:

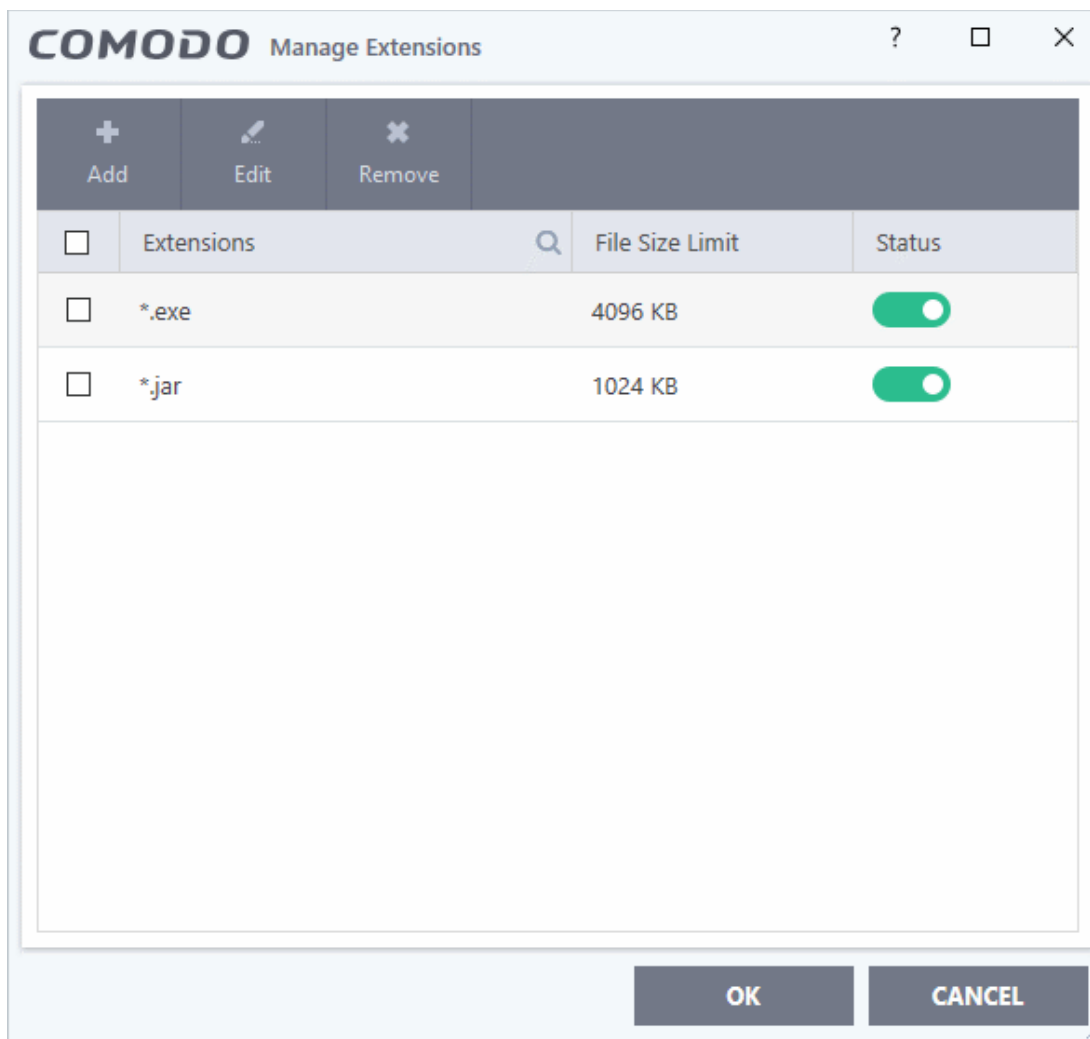
- **Quarantine Threats** - Blocks the threat and moves it to quarantine for your later assessment and action. **(Default)**
- **Block Threats** - Will automatically block and delete the threat.

Note: If you deselect this option then the user is offered the choice to quarantine or block the threat at the alert.

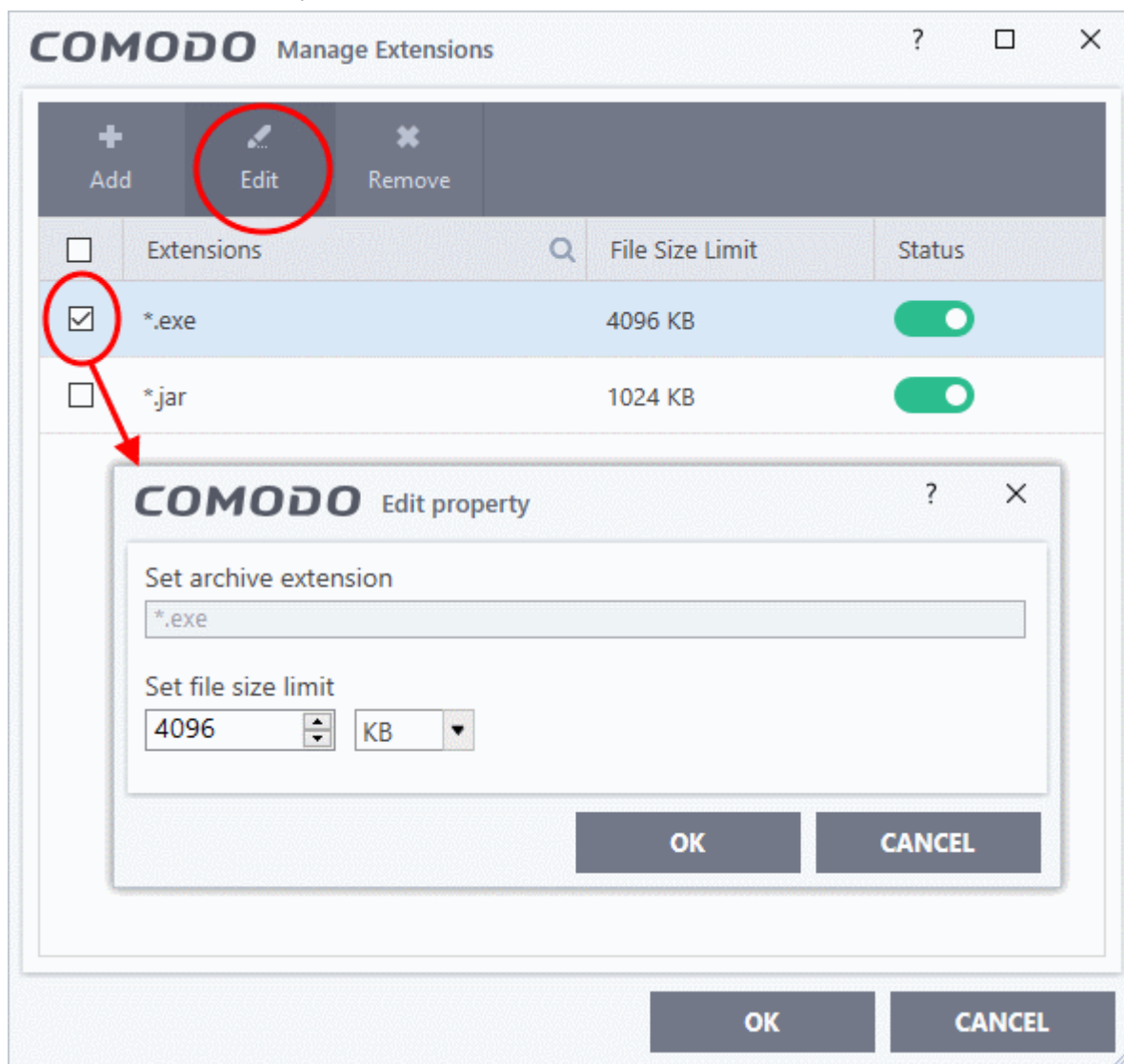
- **Decompress and scan archive files of extension(s)** - If enabled, Comodo Antivirus will scan all types of archive files. Archive file types include .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB files. You will be alerted to the presence of viruses in compressed files before you even open them. **(Default = Enabled)**

You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

- Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.



- To add a 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.
- Set the file size for the extension selected
- Repeat the process to add more extensions
- Click 'OK' in the 'Manage Extensions' dialog
- Set new on-screen alert timeout to** - Set the time period (in seconds) that virus alerts should stay on the screen. (**Default = 120 seconds**)
- Set new maximum file size limit to** - Set the maximum size of files (in MB) that the antivirus should scan. Files larger than the size specified here will not be scanned. (**Default = 40 MB**)
- Set new maximum script size to** - Set the maximum size of scripts (in MB) that the antivirus should scan. Files larger than the size specified here will not be scanned. (**Default = 4 MB**)
- Use heuristics scanning** - Enable or disable heuristics scanning and define scanning level. (**Default = Low**)

Background. Heuristic techniques identify previously unknown malware by analyzing a file to see if it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it

for quarantine. Heuristics is about detecting 'virus-like' attributes rather than looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current virus database.

If enabled, select the level of heuristic scanning from the drop-down:

- **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest alerts. This setting combines a high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (**Default**)
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but also raises the possibility of more false positives.
- **Enable realtime scanning of files on network** - Activate or deactivate automatic scans of files on network drives (**Default = Enabled**)
 - If enabled, the scanner will check all files you interact with on a network drive, even if you do not copy them to your local machine.
 - If disabled, network files are not checked unless you copy them to your local machine.
- **Use Windows Anti-malware Scan Interface (AMSI) technology** – AMSI technology, developed by Microsoft allows 3rd party applications to request AV scans from the installed AV product on the machine. CCS is on the AMSI provider's list. This feature provides enhanced malware protection for users, their data and applications. (**Default = Enabled**)
 - Enabled - CCS will scan on request from an AMSI enabled application.
 - Disabled - CCS removes itself from the local AMSI providers list, and will not respond to scan requests from AMSI enabled apps.
- **Use cloud services while scanning via AMSI** – This option is available if 'Use Windows Anti-malware Scan Interface (AMSI) technology' is enabled. (**Default = Disabled**)
 - Enabled - CCS will check a file's trust rating on our cloud servers as part of the AMSI scan process.
 - Note – Cloud Lookup must also be enabled in '**File Rating Settings**'.

6.2.2. Scan Profiles

An antivirus scan profile is a collection of scanner settings that tell CCS:

- What to scan (which files, folders or drives)
- When to scan (you can create a scan schedule)
- How to scan (you can configure the behavior of the scan engine)

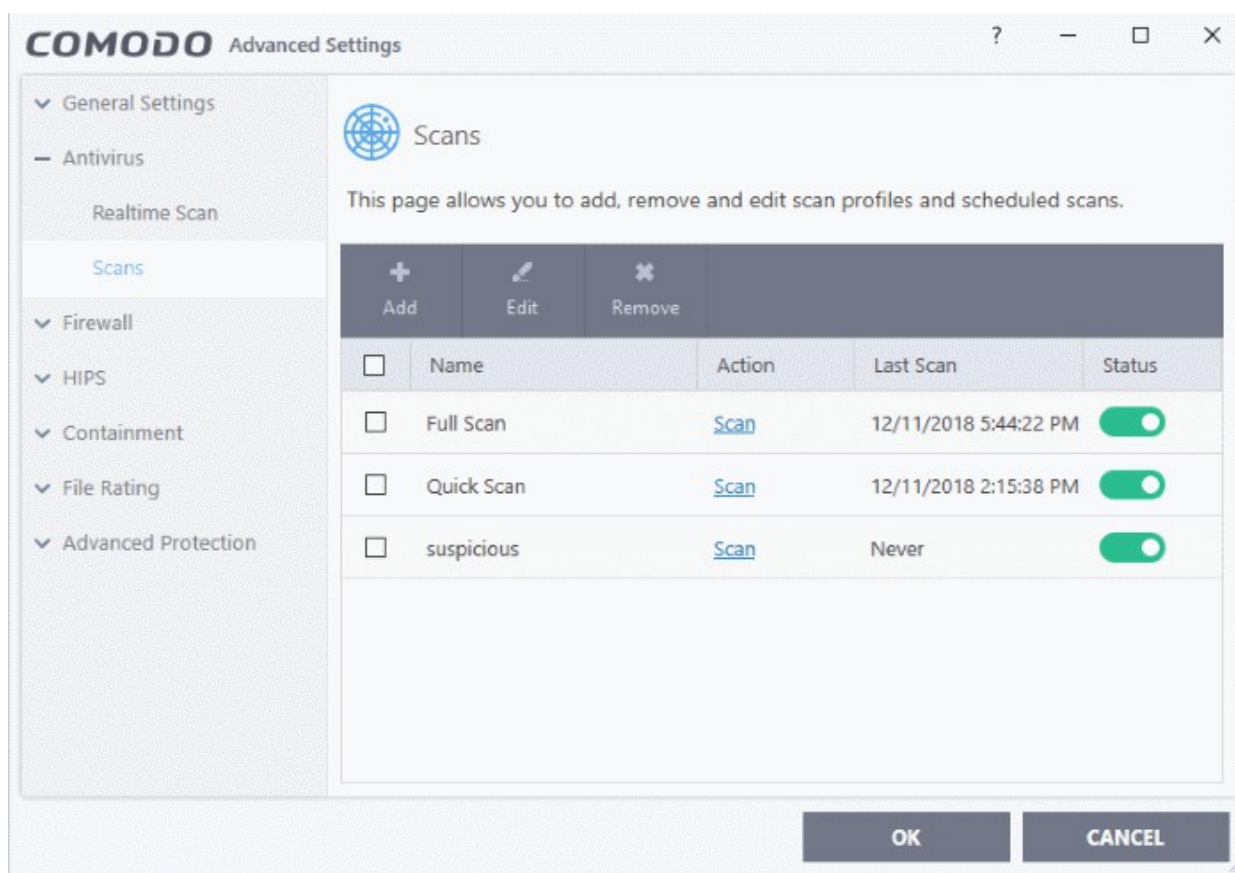
CCS ships with three pre-defined scan profiles and allows you to create custom scan profiles.

- **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 if connected.
- **Quick Scan** - Covers critical areas of your computer which are highly prone to infection and attack. Areas scanned include system memory, auto-run entries, hidden services, boot sectors, 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 clean.

You cannot modify the areas scanned in a pre-defined profile, but you can edit the scan parameters. You can also create custom profiles and scan schedules.

To open the 'Scans' panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Antivirus' > 'Scans' on the left:



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.

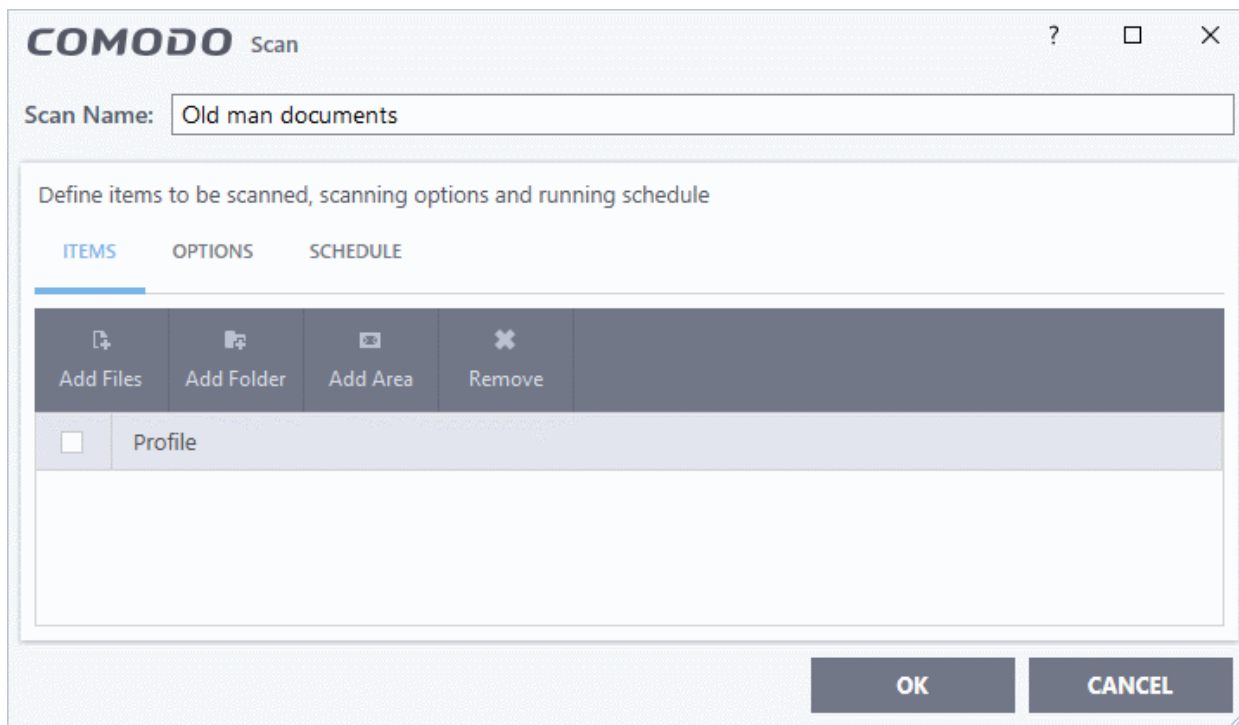
Click the following links for more details about:

- [Create a Scan Profile](#)
- [Run a custom scan](#)

To create a custom profile

- Click 'Settings' at the top-left of the CCS home screen
- Click 'Antivirus' > 'Scans' on the left
- 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:

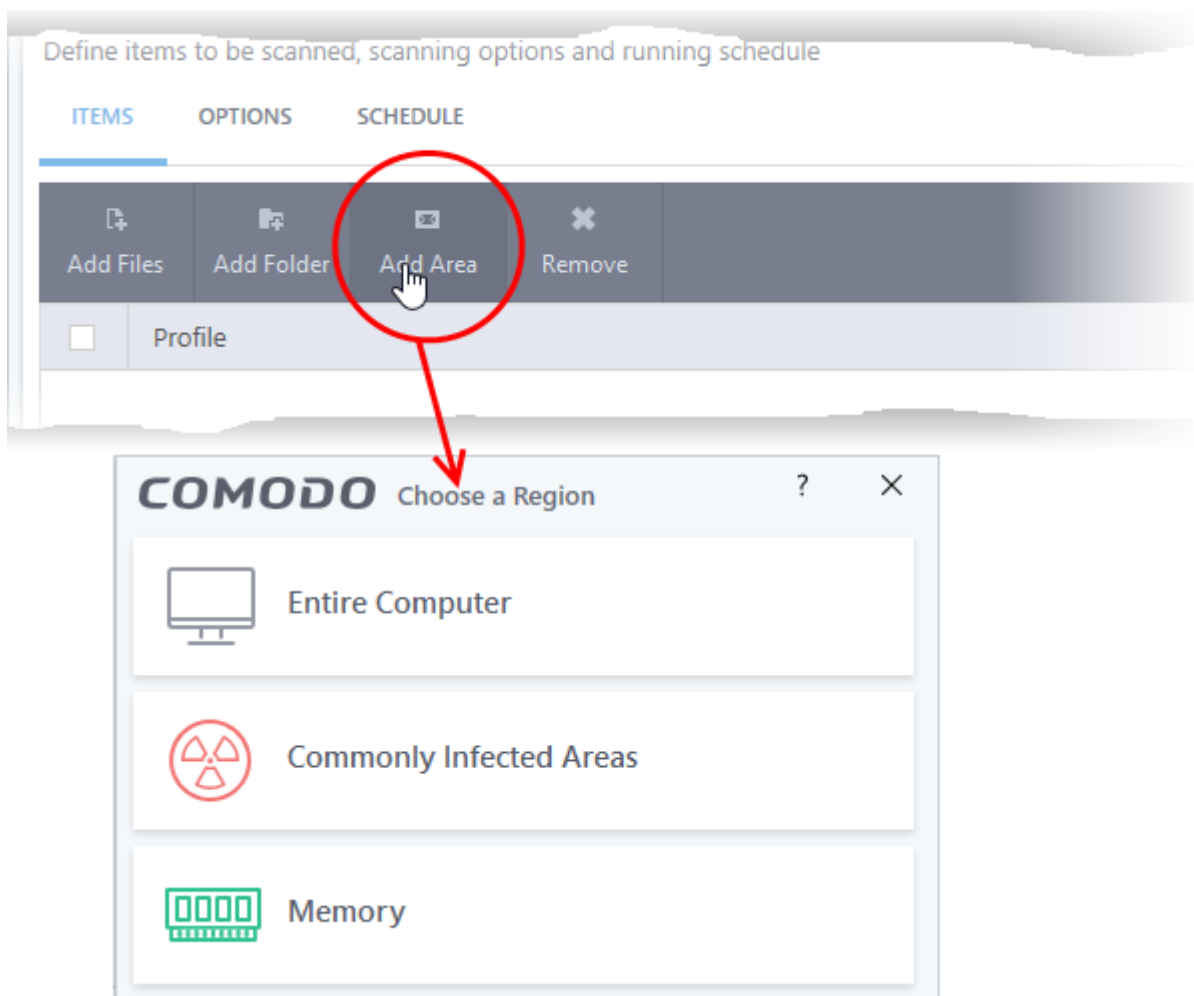
- **Select the items to scan**
- **Configure scan options for the profile**
- **Configure a schedule for the scan**

Select the items to scan

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

The buttons along the top let you add three types of item to the scan. You can add any combination of items.

- **Files** - Add individual files to the profile. Click the 'Add Files' button and navigate to the file you want to include in the scan. Repeat to add more files.
- **Folders** - Add entire folders to the profile. Click the 'Add Folder' button and choose the folder from the 'Browse for Folder' dialog.
- **Areas** - Add pre-defined regions to the profile. Regions include 'Full Computer', 'Commonly Infected Areas' and 'Memory'.



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

Configure Scan Options

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

COMODO Scan

Scan Name:

Define items to be scanned, scanning options and running schedule

ITEMS **OPTIONS** SCHEDULE

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

Use cloud while scanning
This option allows scanner to connect to cloud to query file ratings

Automatically clean threats ▼
When the threats are identified, perform the selected action automatically

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

Use heuristics scanning ▼
Use the selected level of sensitivity while scanning heuristically

Limit maximum file size to MB
While scanning, if a file size is larger than specified, it is not scanned

Run this scan with ▼
Priority of scanner determines how much of the computer resources are used among other tasks

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

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

Apply this action to suspicious autorun processes ▼
The selected action will be automatically applied if unrecognized Windows services, autostart entries or scheduled tasks are detected.

OK **CANCEL**

- **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 CCS can detect the latest malware even if your virus database is out-dated. (**Default = Disabled**).
- **Automatically clean threats** - Choose the automatic action to be taken against detected threats. The options are:
 - **Quarantine Threats** - Infected items will be moved to Quarantine. You can review quarantined items later and remove them or restore them (in case of false positives). See [Manage Quarantined Items](#) for more details on managing quarantined items.
 - **Disinfect Threats** - If a disinfection routine is available, the antivirus will remove the infection and keep the original, safe, file. If not, the item will be moved to 'Quarantine'. (**Default**)
- **Show scan result window** - If selected, you will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.
- **Use heuristics scanning** - Select whether or not heuristic techniques should be used during

scans in this profile. You are also given the opportunity to define the heuristics scan level. (**Default = Enabled**).

Background. Heuristic techniques identify previously unknown malware by analyzing a file to see if it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting 'virus-like' attributes rather than looking for a virus signature which exactly matches a signature on the blacklist. This allows the engine to detect new viruses even if they are not in the current virus database.

If enabled, select the level of heuristic scanning from the drop-down:

- **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest alerts. This setting combines a high level of protection with a low rate of false positives. Comodo recommends this setting for most users. (**Default**)
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but also raises the possibility of more false positives.
- **Limit maximum file size to** - Set the maximum size of files (in MB) that the profile should scan. Files larger than the size specified here will not be scanned. (**Default = 40 MB**)
- **Run this scan with** - Set the Windows priority of the scan process. (**Default = Disabled**). The available options are:
 - High
 - Normal
 - Low
 - Background.
- **Update virus database before running** - Instructs CCS to check for and download the latest virus signatures before starting the scan (**Default = Enabled**) .
- **Detect potentially unwanted applications** - If enabled, the scan will also flag applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars.

Background. PUA's are often bundled as an additional 'utility' when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks your activity on the internet. (**Default = Enabled**).

- **Apply this action to suspicious auto-run processes** - CCS monitors registry records related to Windows services, auto-run entries and scheduled tasks. You can configure the software to stop the creation or modification of unrecognized files and scripts (**Default = Disabled**). The options are:
 - Ignore - CCS does not take any action
 - Terminate - CCS 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, CCS 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, CCS 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**'.

Note 2 - CCS 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**'.

Schedule the scan

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

The screenshot shows the 'COMODO Scan' configuration window with the 'SCHEDULE' tab selected. The window title is 'COMODO Scan'. At the top, there is a 'Scan Name:' field. Below it, the main area is titled 'Define items to be scanned, scanning options and running schedule'. The 'SCHEDULE' tab is active, showing the following options:

Frequency:

- Do not schedule this task
- Every few hours
- Every Day
- Every Week
- Every Month

Additional Options

- Run only when computer is not running on battery
- Run only when computer is IDLE
- Turn off computer if no threats are found at the end of the scan
- Run during Windows Automatic Maintenance

At the bottom right, there are 'OK' and 'CANCEL' buttons.

You have the following options:

- **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** - Scans the areas defined in the profile every 'x' hours. You can specify the number of hours in the 'Repeat scan 'x' hours' field.
- **Every Day** - Run the scan every day at the time specified in the 'Start Time' field.
- **Every Week** - Run the scan on the day(s) specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- **Every Month** - Run the scan on the date(s) specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery** - The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or other mobile device.
- **Run only when computer is IDLE** - The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan** - Will turn off your computer if

no threats are found during the scan. This is useful when you are scheduling scans to run at nights.

- **Run during Windows Automatic Maintenance** - Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time *in addition* to the configured schedule.

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

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

- Click 'OK' to save the profile.

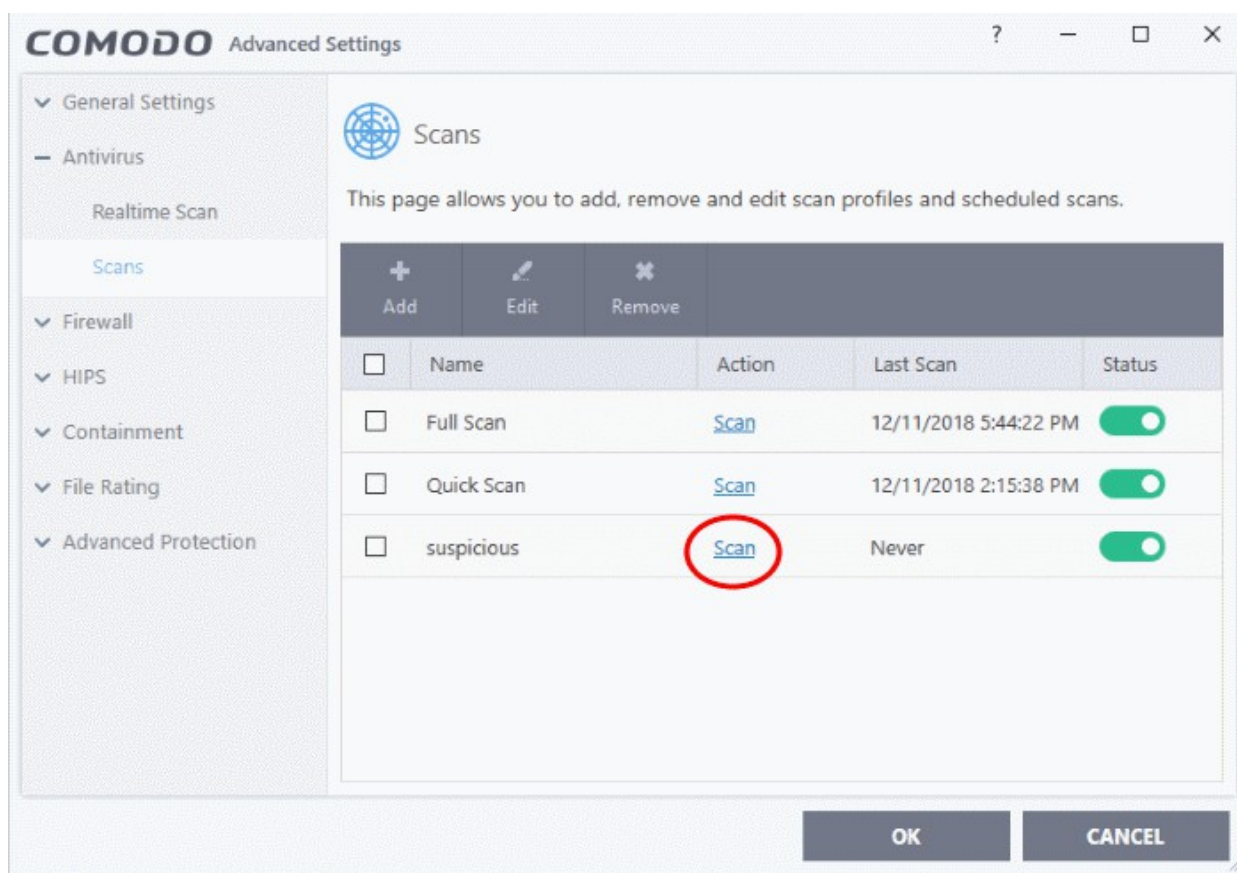
The profile will be available for deployment in future.

Run a saved, custom scan

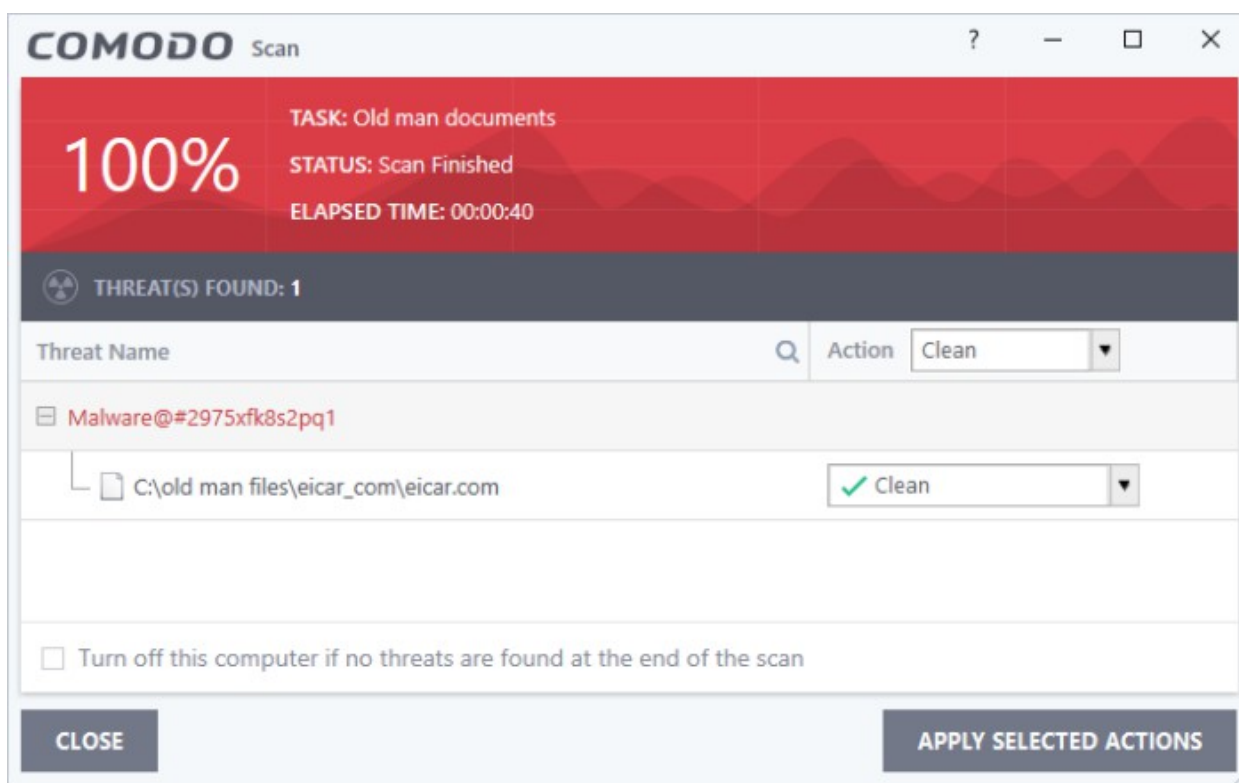
- Click 'General Tasks' on the CCS home screen
- Click 'Scan' > 'Custom Scan'
- Click 'More Scan Options'

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

- Click 'Scan' beside the required scan profile.



The scan will start immediately. Results are shown at the end of the scan:



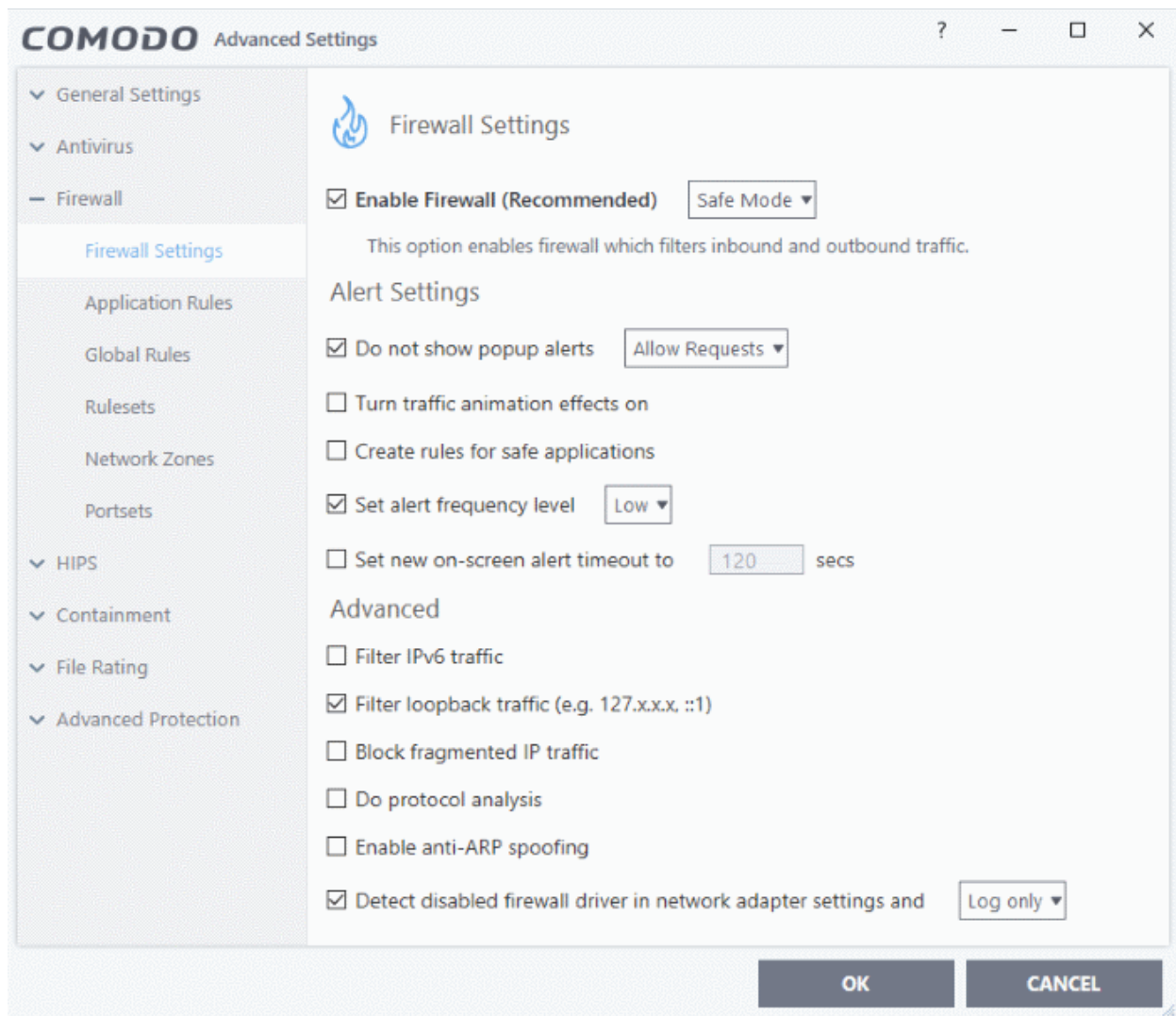
The scan results window displays the number of objects scanned and the number of threats discovered. You can choose to clean, move to quarantine or ignore the threat based on your assessment. See '[Processing infected files](#)' for more details.

6.3. Firewall Configuration

- The firewall component of Comodo Client Security offers the highest levels of security against inbound and outbound threats.
- It checks that all network traffic in and out of your computer is legitimate, hides your computer ports from hackers, and blocks software from transmitting your personal data over the internet.
- The firewall also lets you control which applications are allowed to connect to the internet and will warn you if there is suspicious activity.

Configure the Firewall

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' on the left:



Firewall settings has several sub-sections:

- **General Firewall Settings** - Configure settings that govern the overall behavior of the firewall component.
- **Application Rules** - View, create and modify rules that determine the network access privileges of individual applications or specific types of application
- **Global Rules** - View, create and modify rules that apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Predefined collections of firewall rules that can be applied to internet capable applications such as browsers, email clients and FTP clients.
- **Network Zones** - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Predefined groups of regularly used ports that can be used and reused when creating traffic filtering rules.

Background note on rules: Both application rules and global rules are consulted when the firewall is determining whether to allow or block a connection attempt.

- For Outgoing connection attempts, the application rules are consulted first then the global rules.

- For Incoming connection attempts, the global rules are consulted first then application specific rules.

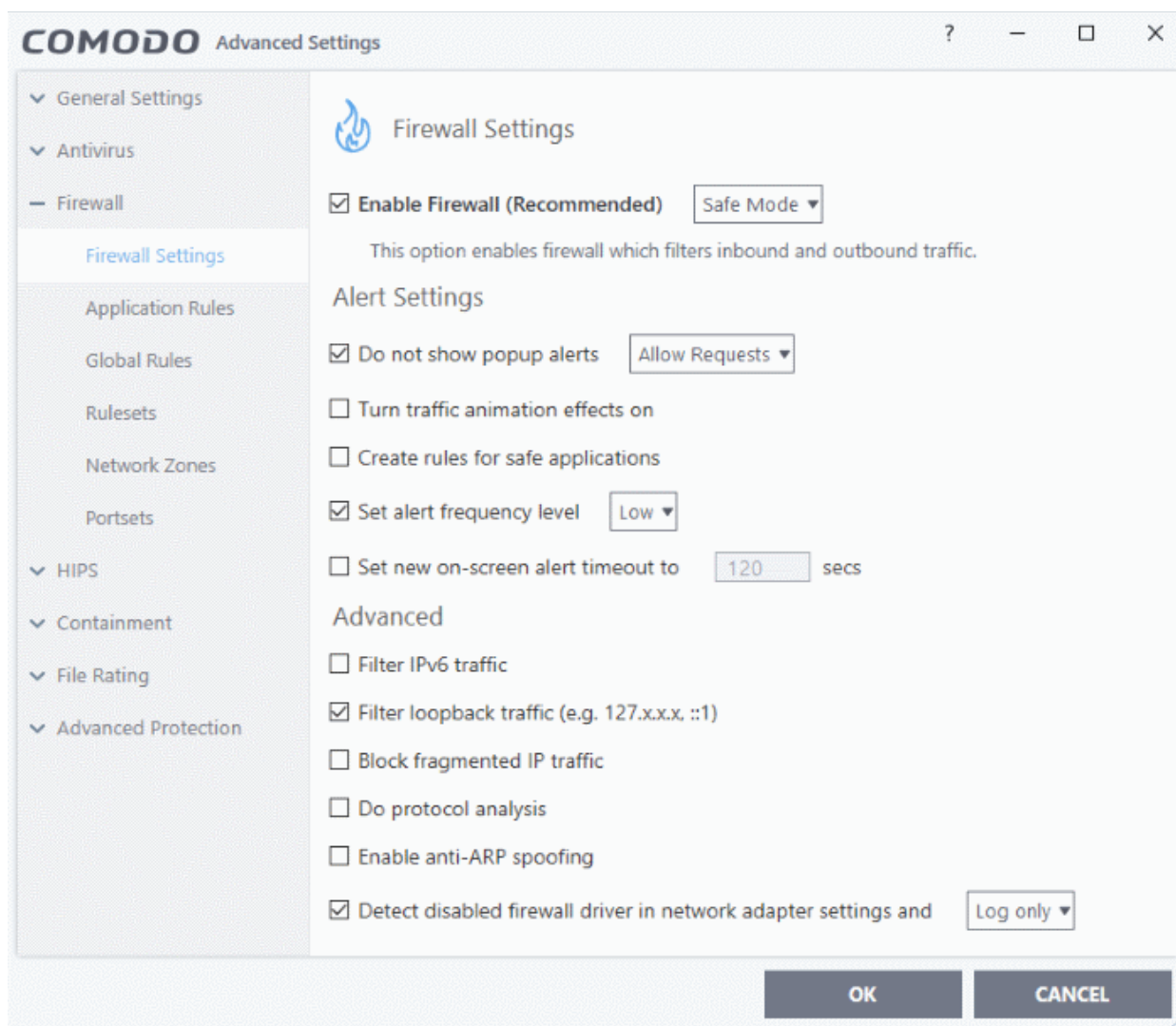
6.3.1. General Firewall Settings

The 'Firewall Settings' panel lets you quickly configure overall firewall behavior. The panel is divided into three areas:

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

Open the 'Firewall Settings' interface

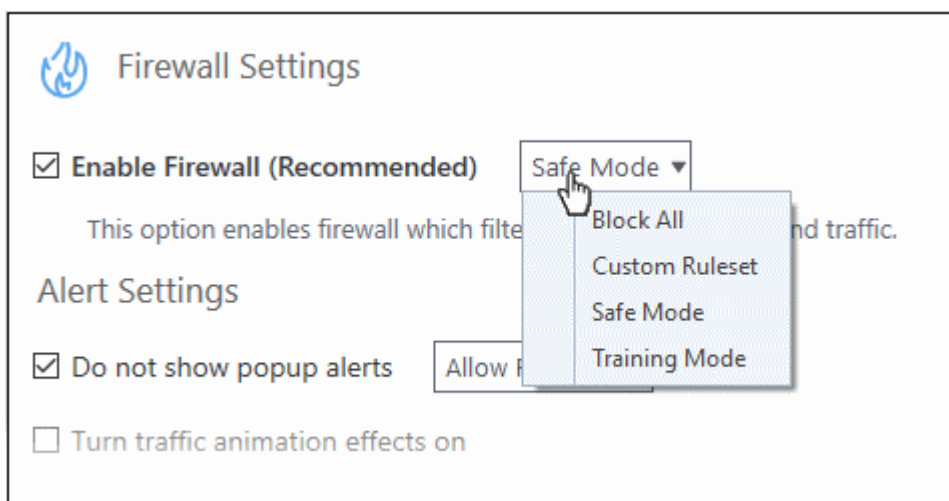
- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Firewall Settings' on the left:



General Settings

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

If enabled, you can also choose the security level from the accompanying drop-down menu:



The choices available are:

- **Block All:** The firewall blocks all traffic in and out of your computer regardless of any user-defined configuration and rules. The firewall does not attempt to learn the behavior of any application and does not automatically create traffic rules for any applications. Choosing this option effectively prevents your computer from accessing any networks, including the internet.
- **Custom Ruleset Mode:** The firewall applies ONLY the custom security configurations and **network traffic rules** specified by the user. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. You will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, you have specified rules and policies that instruct the firewall to trust the application's connection attempt).

If any application tries to make a outbound connection, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.

- **Safe Mode (Default):** If **Create rules for safe applications** is enabled then the firewall automatically creates rules to allow traffic by applications certified as 'Safe' by Comodo. For new, unknown applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application internet access by choosing 'Treat this application as a Trusted Application' at the alert. This deploys the **predefined firewall ruleset** 'Trusted Application' onto the application.

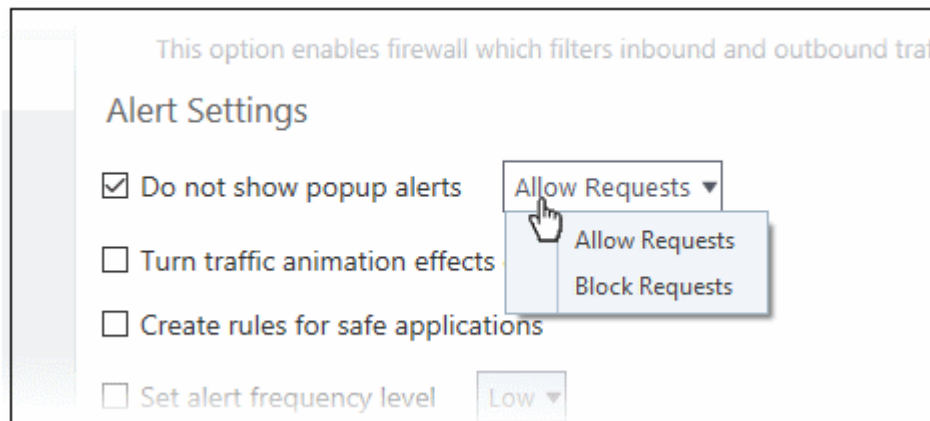
'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.

- **Training Mode:** The firewall monitors network traffic and creates automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the **correct network access rights**.

Alert Settings

- **Do not show popup alerts** - Configure whether or not you want to be notified when the firewall encounters a request for network access. Choosing 'Do not show pop-up alerts' will minimize disturbances but at some loss of user awareness. (**Default = Enabled**)

If you choose this option then you have a choice of default responses that CCS should take - either 'Block Requests' or 'Allow Requests'.



- **Turn traffic animation effects on** - By default, the Comodo Client Security's 'Shield' tray icon displays a small animation whenever traffic moves to or from your computer.



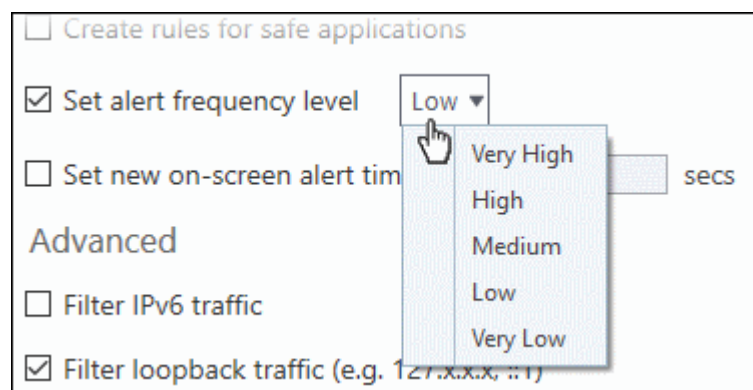
If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the shield. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer. Clear this check box if you would rather not see this animation. **(Default = Disabled)**

- **Create rules for safe applications** - Comodo Firewall trusts the applications if:
 - The application/file is rated as Trusted in the **File List**;
 - The application is from a vendor included in the **Trusted Software Vendors** list
 - The application is included in the extensive and constantly updated Comodo safelist.

By default, CCS does not automatically create 'allow' rules for safe applications. This helps to lower resource usage and simplifies the rules interface. It also reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

Enabling this checkbox instructs CCS 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. The Advanced users can edit/modify the rules as they wish. **(Default = Disabled)**

- **Set alert frequency level** - Configure the amount of alerts generated by the firewall. Please note that this does not affect your security level. Security level is determined by the rules in **Application Rules** and Global Rules. The default setting of 'Low' is perfect for the majority of users - ensuring you are kept informed of any suspicious behavior but are not overwhelmed with alerts about routine connections. **(Default=Enabled)**



The options available are:

- **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application.

This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.

- **High:** The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.
- **Medium:** The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.
- **Low:** The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.
- **Very Low:** The firewall shows only one alert for an application.

The alert frequency settings refer only to connection attempts by applications or from IP addresses that you do not trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.

- **Set new on-screen alert time out to:** Determines how long the Firewall shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced Settings

Advanced detection settings help protect your computer against common types of denial of service (DoS) attack. When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server.

- **Filter IP v6 traffic** - If enabled, the firewall will filter IPv6 network traffic in addition to IPv4 traffic. (**Default = Disabled**)

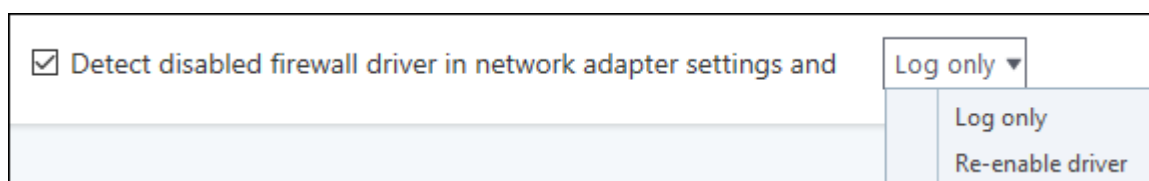
Background Note: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost 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 3.4×10^{38} 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 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 conforms to that 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**)
- **Detect disabled firewall driver in network adapter settings** – The firewall will take action if it discovers its driver is not enabled.



You can choose the following actions if this condition is met:

- **Log only** - Creates an event log but does not notify the administrator.
- **Re-enable Driver** - Attempts to turns the driver back on automatically.

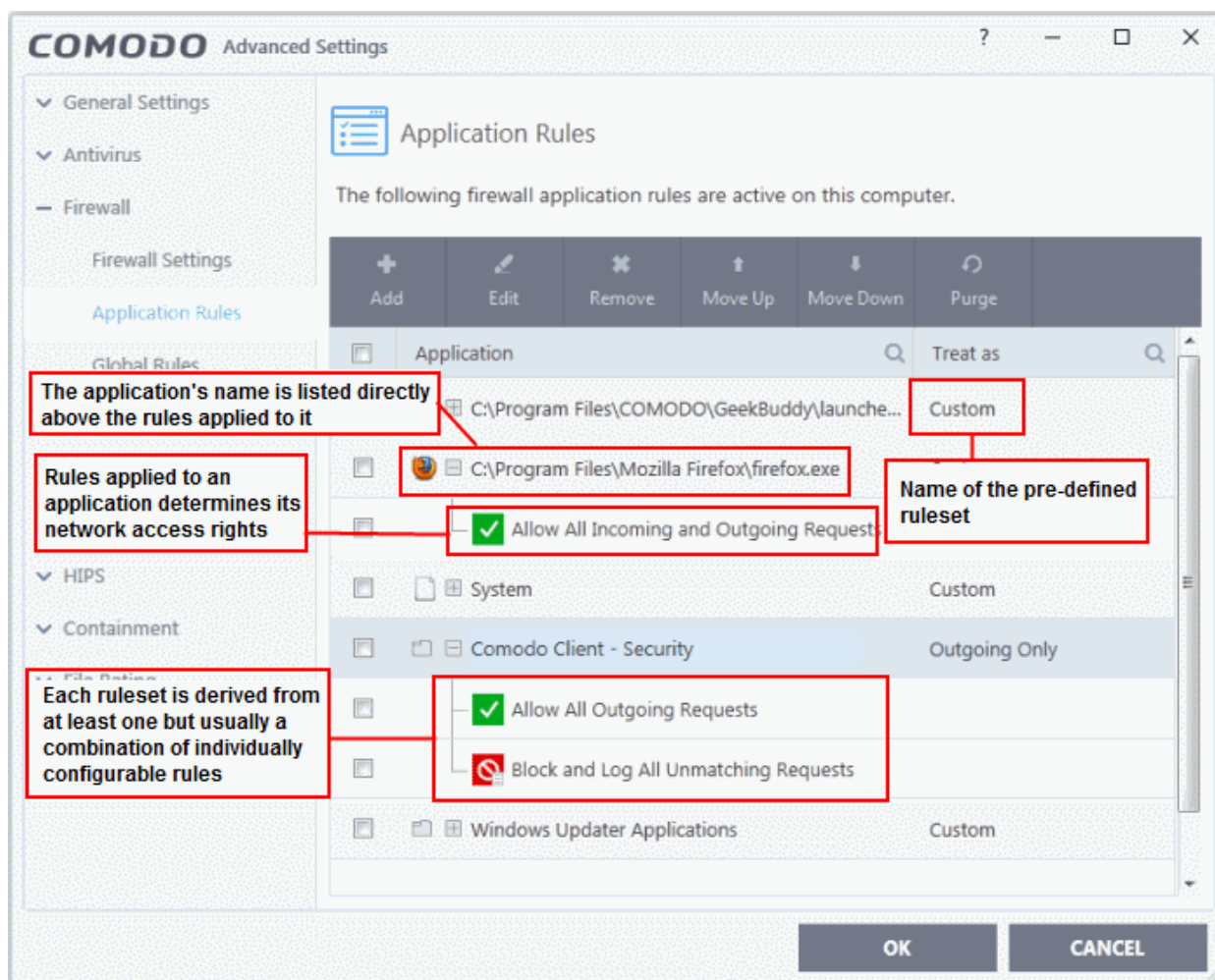
6.3.2. Application Rules

Overview of Rules and Rulesets

- Whenever an application makes a request for internet or network access, the firewall allows or denies the request based on the firewall ruleset specified for the application.
- Firewall rulesets are made up from one or more network access rules. Each access rule contains instructions that determine whether the application should be allowed or blocked, which protocols it is allowed to use, which ports it is allowed to use and so forth.

Open the Application Rules panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Application Rules' on the left:

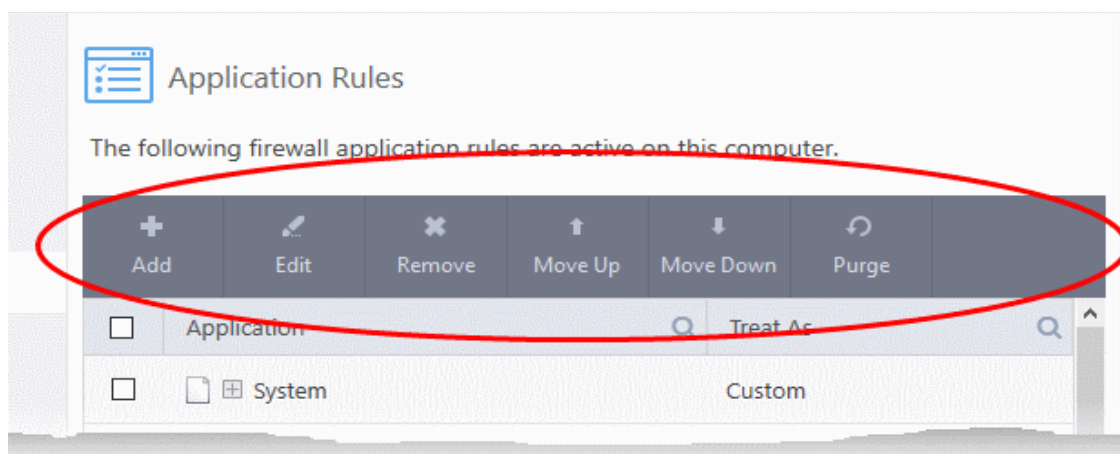


- The first column, **Application**, shows programs for which a firewall ruleset has been created. If the application belongs to a file group, then all member applications assume the ruleset of the file group.
- The second column, **Treat as**, shows the name of the ruleset assigned to the application or group
- Click '+' at the left of the application name to view the individual rules in a ruleset

Click the magnifying glass on the right of the column headers to search for a specific rule.

General Navigation:

The control buttons at the top let you to create and manage application rule sets.



- **Add** - Add a new Application to the list then create a ruleset for it. See **Creating and Modifying**

Firewall Rules and **'Adding and Editing a Firewall Rule'**.

- **Edit** - Allows you to modify the firewall rule or ruleset of the selected application. See the sections **'Creating and Modifying Firewall Rules'** and **'Adding and Editing a Firewall Rule'**.
- **Remove** - Deletes the selected ruleset.
- **Purge** - Runs a check to verify that all applications mentioned in a ruleset are actually installed at the paths specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down** - Rules are prioritized top-to-bottom, with rules at the top of the list having highest priority. The 'Move Up' and 'Move Down' buttons enable you to change the priority of a selected rule.

If you wish to modify the **firewall ruleset** for an application:

- Double click on the application name to begin **'Creating and Modifying Firewall Rules'**

Or

- Select the application name and choose 'Edit' from the options to begin **'Creating and Modifying Firewall Rules'**

If you wish to modify an **individual rule** within the ruleset:

- Double click on the specific rule to begin **'Adding and Editing a Firewall Rule'**

Or

- Select the specific rule and choose 'Edit' at the top to begin 'Adding and Editing a Firewall Rule'

Users can also re-prioritize rulesets by moving them up or down, by selecting them and clicking the 'Move Up' or 'Move Down' buttons.

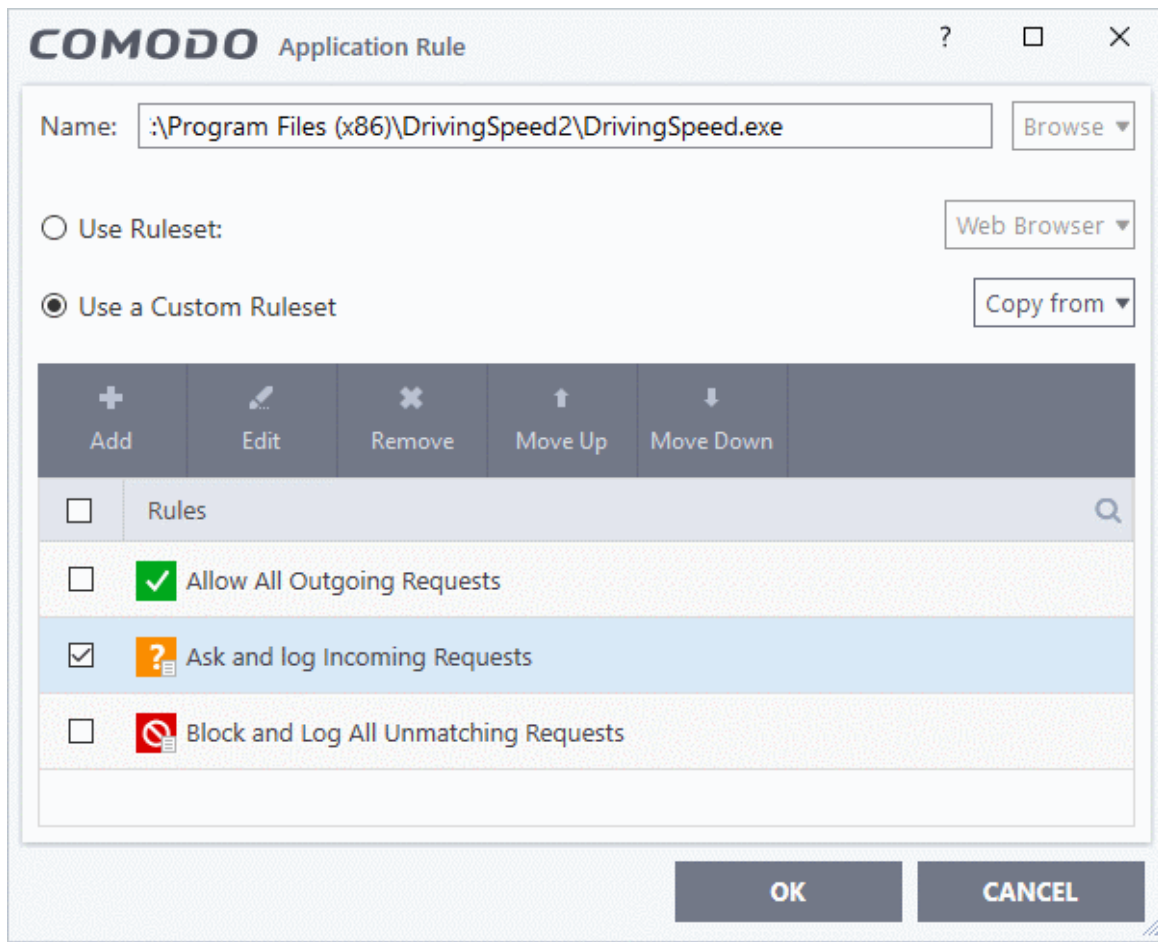
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been designed to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see **Predefined Rule Sets**.

- See **Application Rule interface** for an introduction to the rule setting interface
- See **Creating and Modifying Firewall Rulesets** to learn how to create and edit Firewall rulesets
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration

Application Rule interface

Firewall rules can be added/modified/removed and re-ordered through the Application Rule interface. Any rules created using **Adding and Editing a Firewall Rule** is displayed in this list.

The Application Rule interface is displayed when you click 'Add' or 'Edit' from the options in 'Application Rules' interface.



Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see [Understanding Firewall Rules](#) for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied.

Users can also re-prioritize rulesets by using the 'Move Up' or 'Move Down' buttons. To begin creating Firewall rulesets, first read '[Overview of Rules and Rulesets](#)' then '[Creating and Modifying Firewall Rulesets](#)'

You can search for specific rules by clicking the search icon in the 'Rules' column header and entering the name of the item.

Creating and Modifying Firewall Rulesets

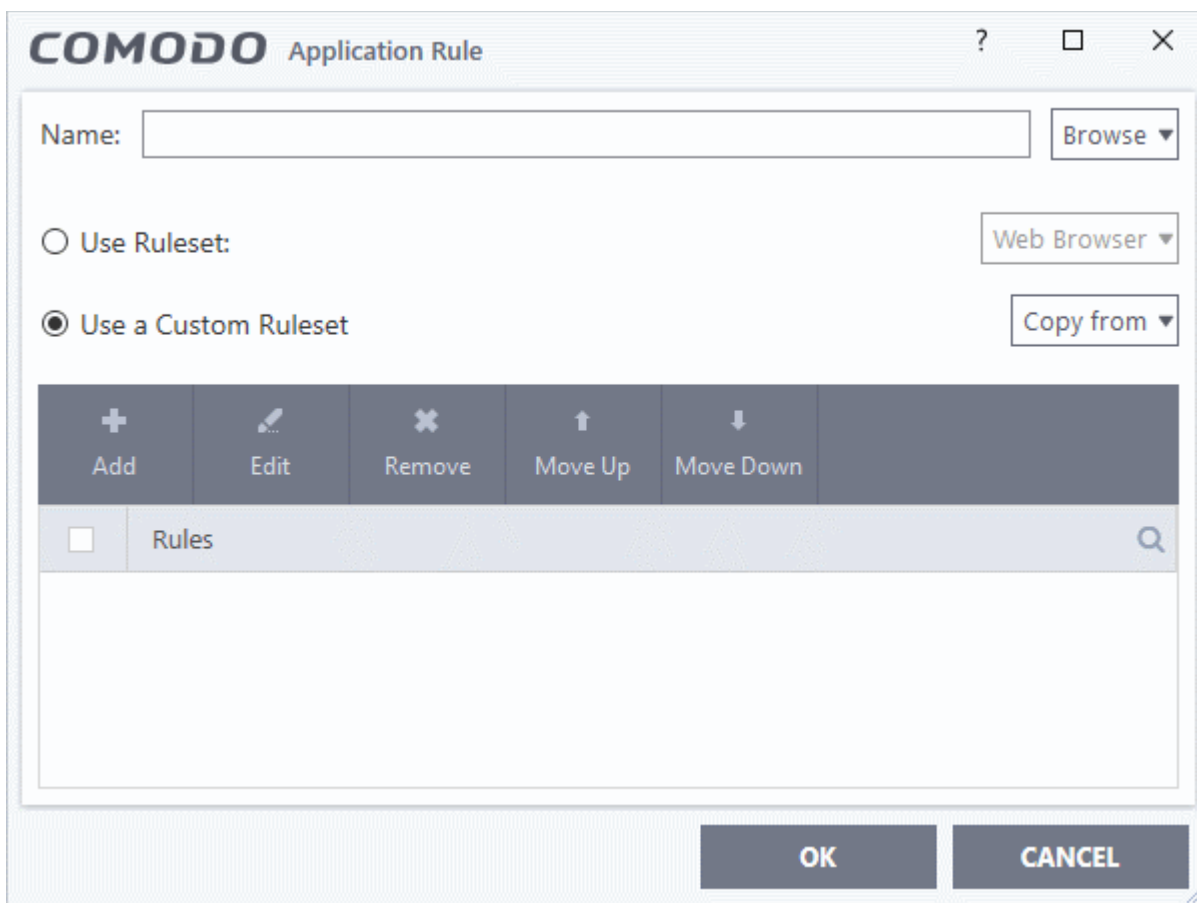
To begin defining an application's Firewall ruleset, you need take two basic steps.

- Step 1 - **Select the application that you wish the ruleset is to be applied.**
- Step2 - **Configure the rules for this application's ruleset.**

Step 1 - Select the application to which you want to apply the ruleset

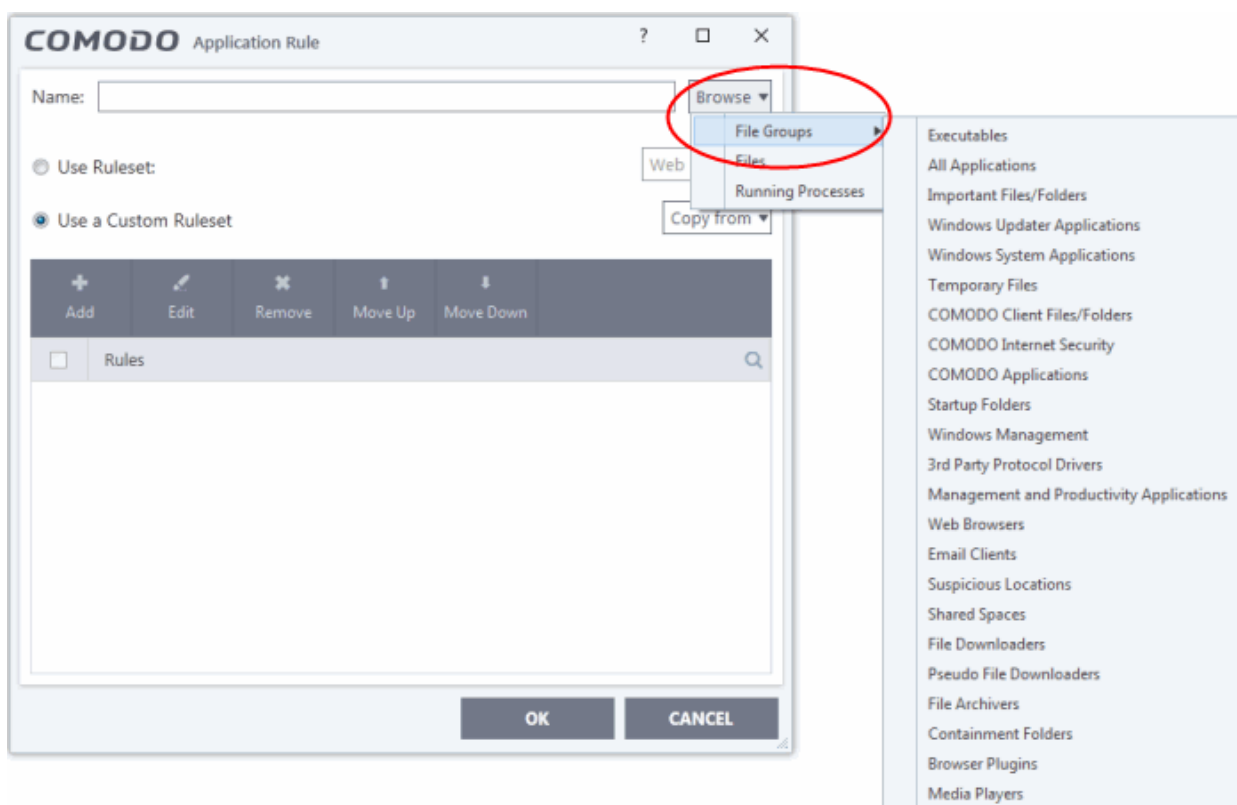
- To define a ruleset for a new application (i.e. one that is not already listed), click the 'Add' button at the top of the list in the [Application Rules interface](#).

The '[Application Rules](#)' interface will open as shown below:



Because this is a new application, the 'Application Path' field is blank. If you are modifying an existing ruleset then the individual rules will be shown.

- Click 'Browse' button beside the 'Name' text box to choose the application file to which this rule set is to be applied.

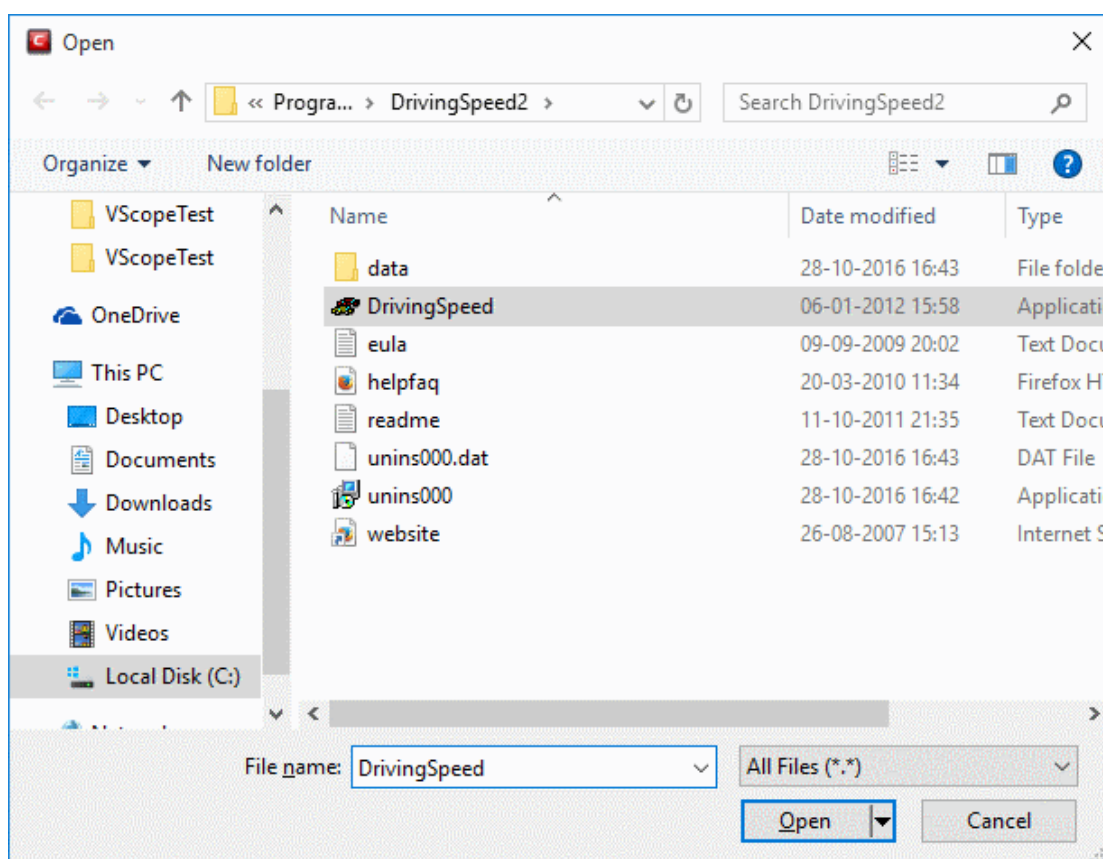


You now have 3 methods available to choose the application for which you wish to create a ruleset - **File Groups**; **Files** and **Running Processes** and

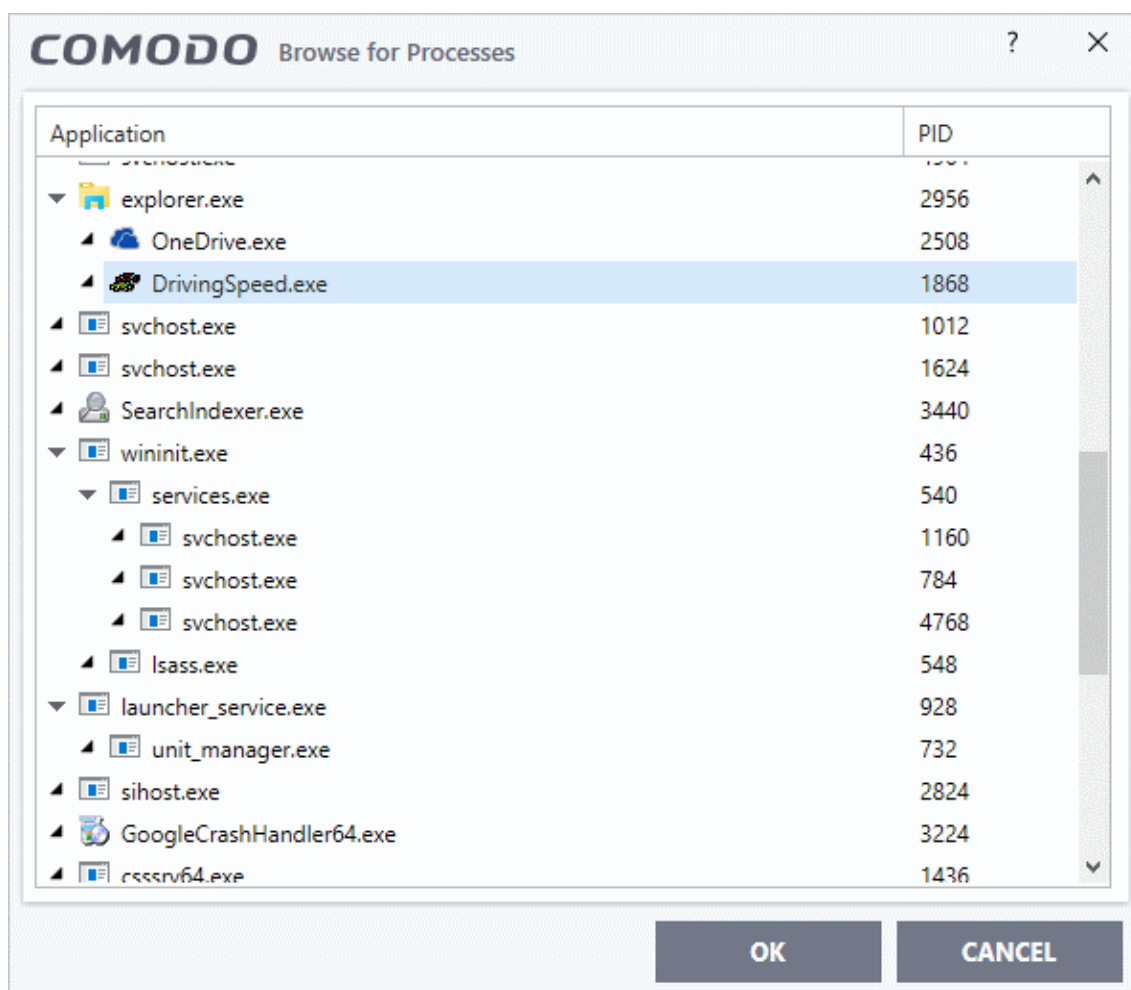
- i. **File Groups** - Allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *cmd.exe, *.bat, *.cmd. Other such categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

CCS ships with a set of pre-defined file groups and also allows you to create your own file groups. You can view and manage the file groups from the 'File Groups' interface accessible from the 'Advanced Settings' interface by clicking 'File Rating' > 'File Groups'. See **File Groups**, for more details on file groups.

- ii. **Files** - this option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the firewall ruleset. In the example shown below, Opera web browser is selected for creating a firewall ruleset.



- iii. **Running Processes** - Displays list of currently running processes in your computer. You can select the process, for whose target application, you wish to deploy a firewall rule.



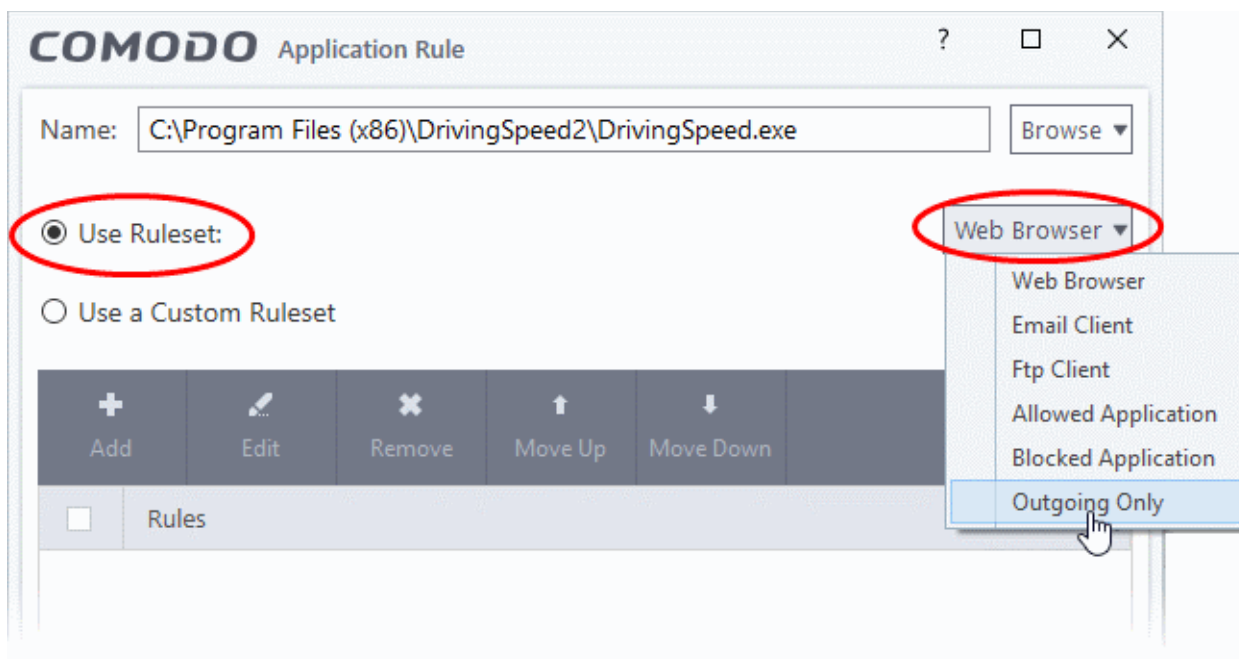
You can choose an individual process or the parent process of a set of running processes. Click 'OK' to confirm your choice.

Having selected the individual application, running process or file group, the next stage is to Configure the rules for this application's Firewall Ruleset.

Step 2 - Configure the rules for this application's ruleset

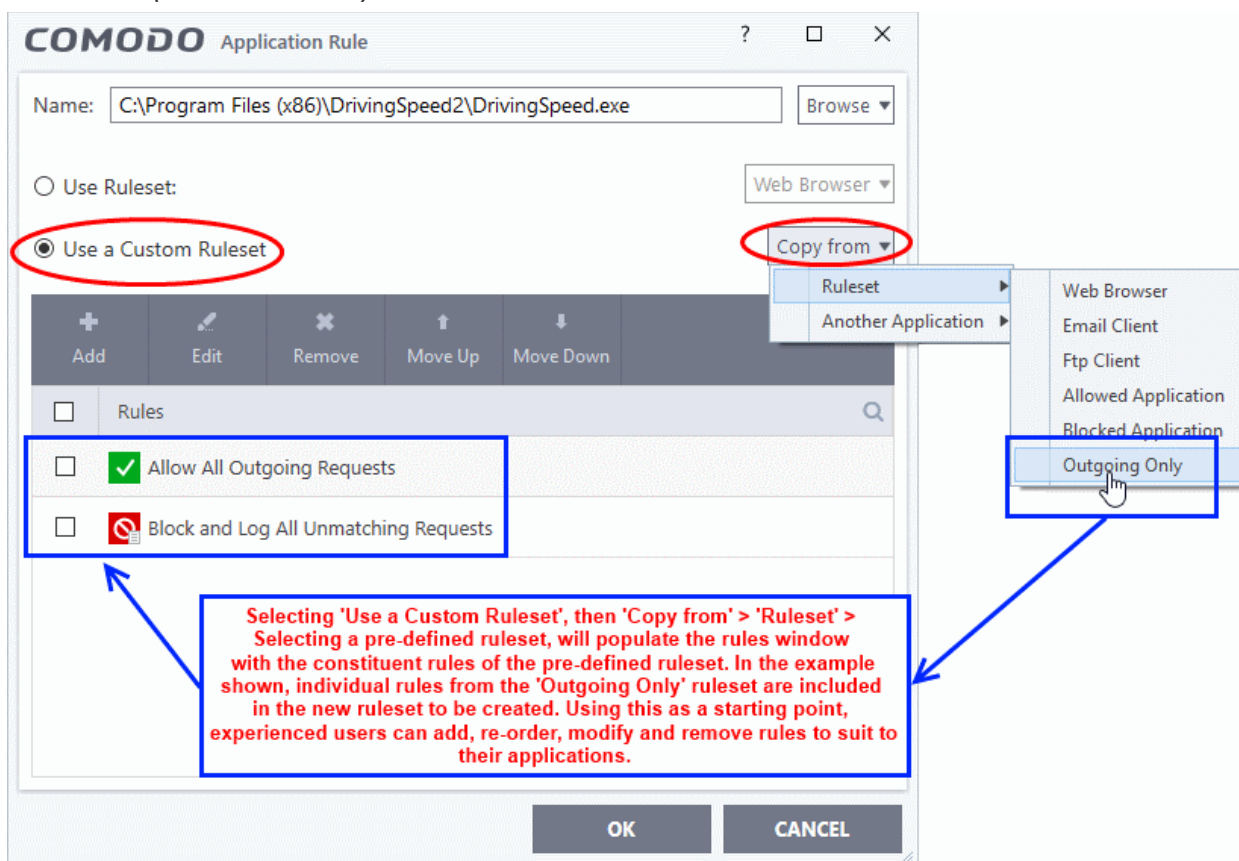
There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- Use a Predefined Ruleset** - Allows you to quickly deploy an existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Opera' browser. The name of the predefined ruleset you choose is displayed in the **Treat As** column for that application in the **interface (Default = Disabled)**.



Note: Predefined Rulesets, once chosen, cannot be modified *directly* from this interface - they can only be modified and defined using the **Rulesets** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - designed for more experienced users, the **Custom Ruleset** option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset (**Default = Enabled**).



You can create an entirely new ruleset or use a predefined ruleset as a starting point by:

- Clicking 'Add' from the top to add individual Firewall rules. See '[Adding and Editing a Firewall Rule](#)' for an overview of the process.
- Use the 'Copy From' button to populate the list with the Firewall rules of a **Predefined Firewall Rule**.
- Use the 'Copy From' button to populate the list with the Firewall rules of another application's ruleset.

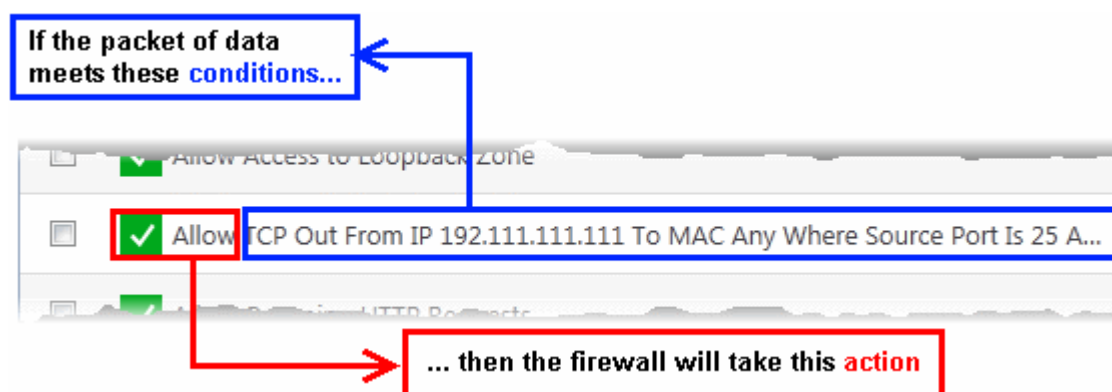
General Tips:

- If you wish to create a reusable ruleset for deployment on multiple applications, we advise you add a new **Predefined Firewall Rules** (or modify one of the existing ones to suit your needs) - then come back to this section and use the '**Ruleset**' option to roll it out.
- If you want to build a bespoke ruleset for maybe one or two specific applications, then we advise you choose the '**Use a Custom Ruleset**' option and create your ruleset either from scratch by adding individual rules or by using one of the built-in rulesets as a starting point.

Understanding Firewall Rules

At their core, each Firewall rule can be thought of as a simple **IF THEN** trigger - a set of **conditions** (or attributes) pertaining to a packet of data from a particular application and an **action** that is enforced if those conditions are met.

As a packet filtering firewall, Comodo Firewall analyzes the attributes of *every single* packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a Firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding Firewall rule, then the connection is automatically blocked until a rule is created.



The actual **conditions** (attributes) you see * on a particular Firewall Rule are determined by the protocol chosen in **Adding and Editing a Firewall Rule**

If you chose 'TCP', 'UDP' or 'TCP and 'UDP', then the rule has the form: **Action** | **Protocol** | **Direction** | **Source Address** | **Destination Address** | **Source Port** | **Destination Port**

If you chose 'ICMP', then the rule has the form: **Action** | **Protocol** | **Direction** | **Source Address** | **Destination Address** | **ICMP Details**

If you chose 'IP', then the rule has the form: **Action** | **Protocol** | **Direction** | **Source Address** | **Destination Address** | **IP Details**

- **Action:** The action the firewall takes when the conditions of the rule are met. The rule shows 'Allow', 'Block' or 'Ask'.**

- **Protocol:** States the protocol that the target application must be attempting to use when sending or receiving packets of data. The rule shows 'TCP', 'UDP', 'TCP or UDP', 'ICMP' or 'IP'
- **Direction:** States the direction of traffic that the data packet must be attempting to negotiate. The rule shows 'In', 'Out' or 'In/Out'
- **Source Address:** States the source address of the connection attempt. The rule shows 'From' followed by one of the following: **IP**, **IP range**, **IP Mask**, **Network Zone**, **Host Name** or **Mac Address**
- **Destination Address:** States the address of the connection attempt. The rule shows 'To' followed by one of the following: **IP**, **IP range**, **IP Mask**, **Network Zone**, **Host Name** or **Mac Address**
- **Source Port:** States the port(s) that the application must be attempting to send packets of data through. Shows 'Where Source Port Is' followed by one of the following: 'Any', 'Port #', 'Port Range' or 'Port Set'
- **Destination Port:** States the port(s) on the remote entity that the application must be attempting to send to. Shows 'Where Source Port Is' followed by one of the following: 'Any', 'Port #', 'Port Range' or 'Port Set'
- **ICMP Details:** States the ICMP message that must be detected to trigger the action. See **Adding and Editing a Firewall Rule** for details of available messages that can be displayed.
- **IP Details:** States the type of IP protocol that must be detected to trigger the action: See **Adding and Editing a Firewall Rule** to see the list of available IP protocols that can be displayed here.

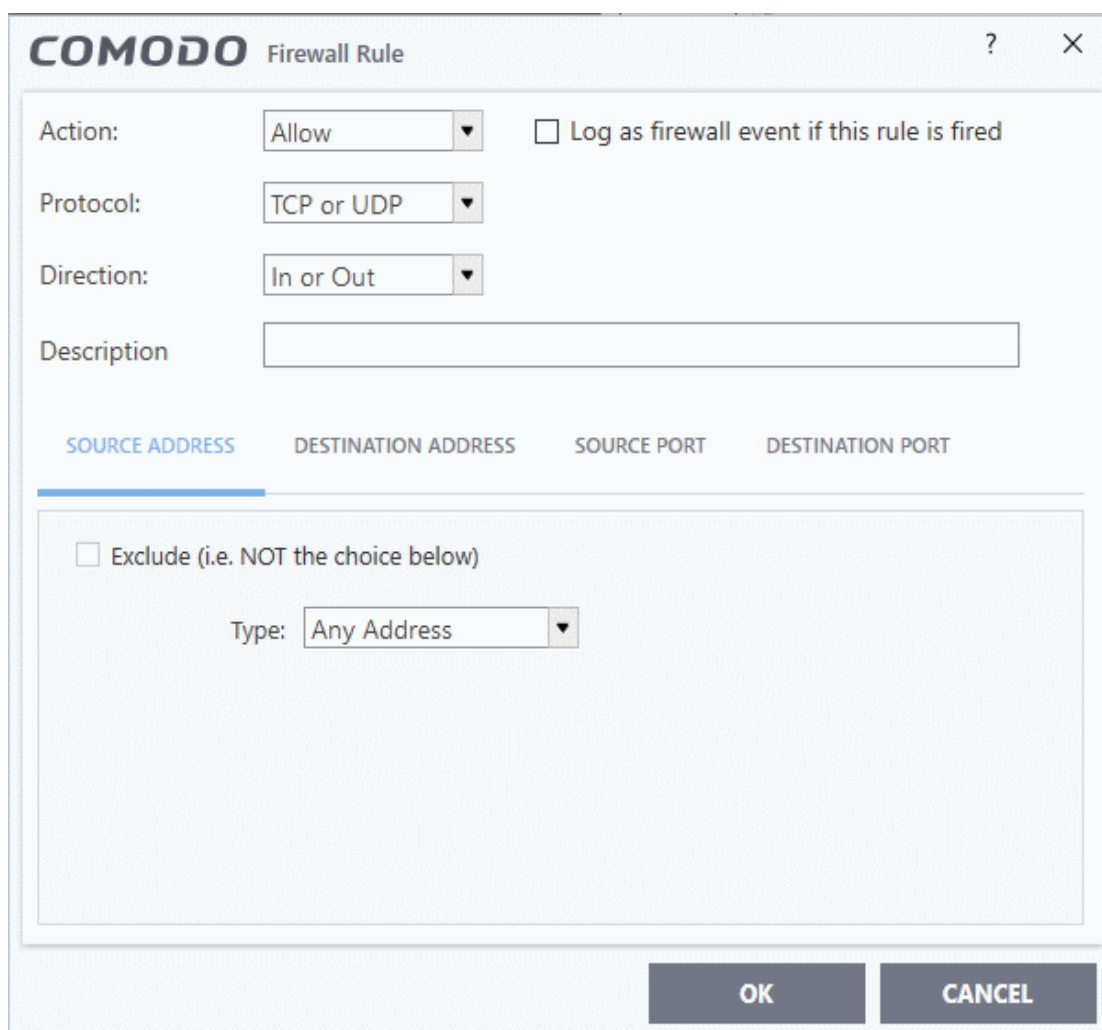
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section '**Global Rules**' to understand the interaction between Application Rules and Global Rules.

** 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)*

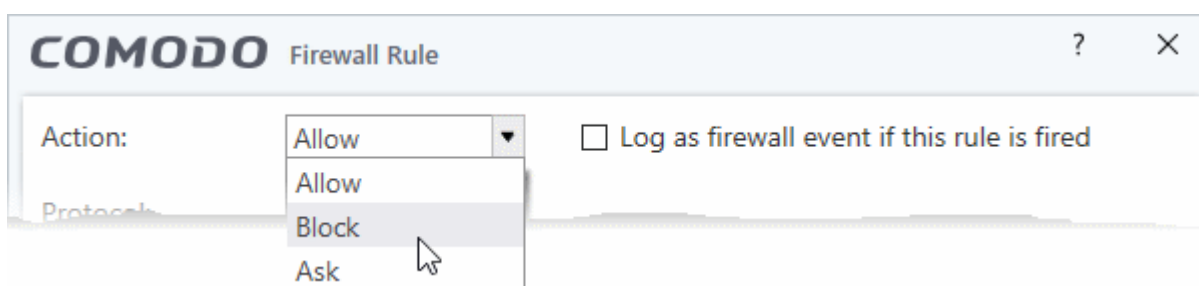
Adding and Editing a Firewall Rule

The Firewall Rule Interface is used to configure the actions and conditions of an individual Firewall rule. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading the sections '**Understanding Firewall Rules**', '**Overview of Rules and Policies**' and '**Creating and Modifying Firewall Rulesets**'.



General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' (*Default*), '**Block**' or '**Ask**'.



- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' (*Default*), '**ICMP**' or '**IP**'.

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

- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are '**In**', '**Out**' or '**In/Out**' (*Default*).
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the **firewall event log viewer** whenever this rule is called into operation. (i.e. when ALL conditions have been met) (*Default = Disabled*).

- **Description:** Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by its intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is displayed to represent instead of the full actions/conditions in the main **Application Rules interface** and the **Application Rule interface**.

Protocol

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

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information.

The screenshot shows a configuration window with a 'Description' text box at the top. Below it are four tabs: 'SOURCE ADDRESS', 'DESTINATION ADDRESS', 'SOURCE PORT', and 'DESTINATION PORT'. The 'SOURCE ADDRESS' tab is selected. Inside this tab, there is a checkbox labeled 'Exclude (i.e. NOT the choice below)'. Below the checkbox is a 'Type:' label followed by a dropdown menu. The dropdown menu is open, showing the following options: 'Any Address', 'Any Address', 'Host Name', 'IPv4 Address Range', 'IPv4 Single Address', 'IPv4 Subnet Mask', 'IPv6 Single Address', 'IPv6 Subnet Mask', 'MAC Address', and 'Network Zone'. At the bottom right of the window are 'OK' and 'CANCEL' buttons.

Source Address and Destination Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.
- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.

DESCRIPTION

SOURCE ADDRESS DESTINATION ADDRESS SOURCE PORT DESTINATION PORT

Exclude (i.e. NOT the choice below)

Type: Any

- A Port Range
- A Set of Ports
- A Single Port
- Any

OK CANCEL

1. You can choose any port number by selecting Any - set by default, 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a predefined **Port Set** by choosing A Set of Ports. If you wish to create a custom port set then please see the section '**Port Sets**'.

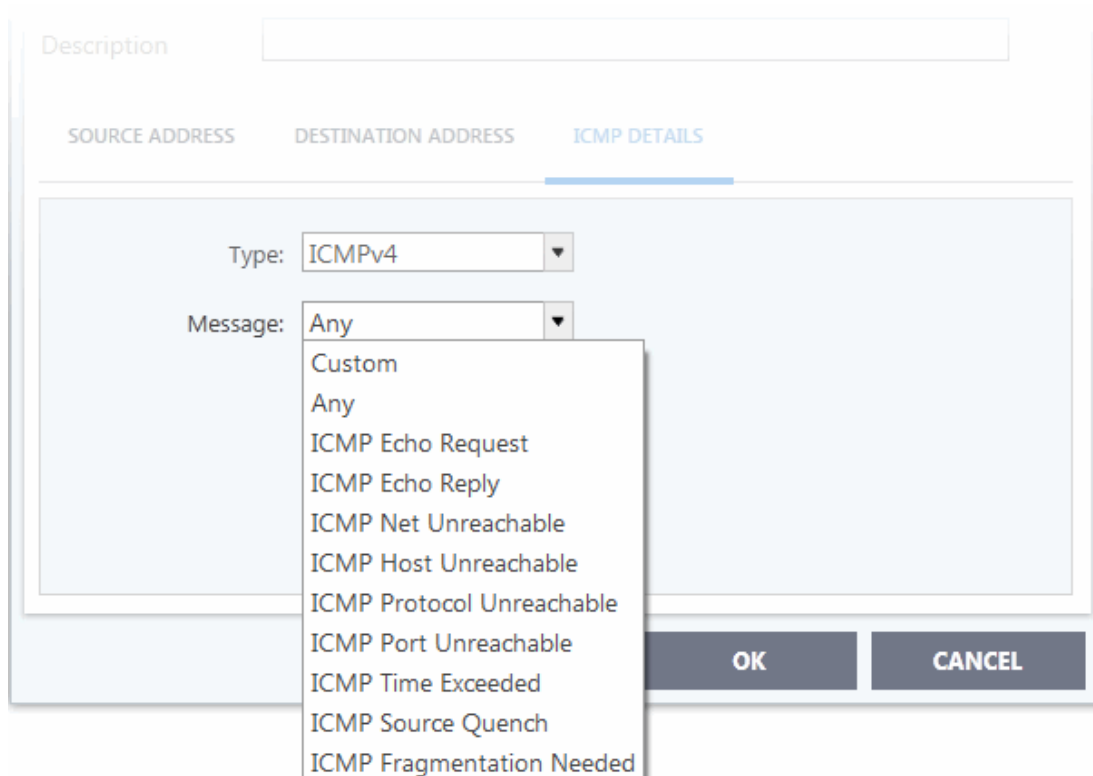
ii. ICMP

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

• ICMP Details

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.



The screenshot shows a configuration window with a 'Description' field at the top. Below it are three tabs: 'SOURCE ADDRESS', 'DESTINATION ADDRESS', and 'ICMP DETAILS'. The 'ICMP DETAILS' tab is selected. Under this tab, there are two dropdown menus: 'Type' (set to 'ICMPv4') and 'Message' (set to 'Any'). The 'Message' dropdown is open, displaying a list of options: 'Custom', 'Any', 'ICMP Echo Request', 'ICMP Echo Reply', 'ICMP Net Unreachable', 'ICMP Host Unreachable', 'ICMP Protocol Unreachable', 'ICMP Port Unreachable', 'ICMP Time Exceeded', 'ICMP Source Quench', and 'ICMP Fragmentation Needed'. At the bottom right of the window are 'OK' and 'CANCEL' buttons.

2. Under the 'ICMP Details' tab, choose the ICMP version from the 'Type' drop-down.
3. Specify ICMP Message, Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.

When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

iii. IP

When you select IP as the protocol in **General Settings**, you are shown a list of IP message type in the 'IP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

Description

SOURCE ADDRESS DESTINATION ADDRESS SOURCE PORT DESTINATION PORT

Exclude (i.e. NOT the choice below)

Type: Any Address ▼

- Any Address
- Host Name
- IPv4 Address Range
- IPv4 Single Address
- IPv4 Subnet Mask
- IPv6 Single Address
- IPv6 Subnet Mask
- MAC Address
- Network Zone

OK CANCEL

- **IP Details**

Select the types of IP protocol that you wish to allow, from the ones that are listed.

Description

SOURCE ADDRESS DESTINATION ADDRESS **IP DETAILS**

IP Protocol: Any ▼

- Custom
- Any
- TCP
- UDP
- ICMPv4
- IGMP
- Raw IP
- PUP
- GGP
- GRE
- RSVP
- ICMPv6

OK CANCEL

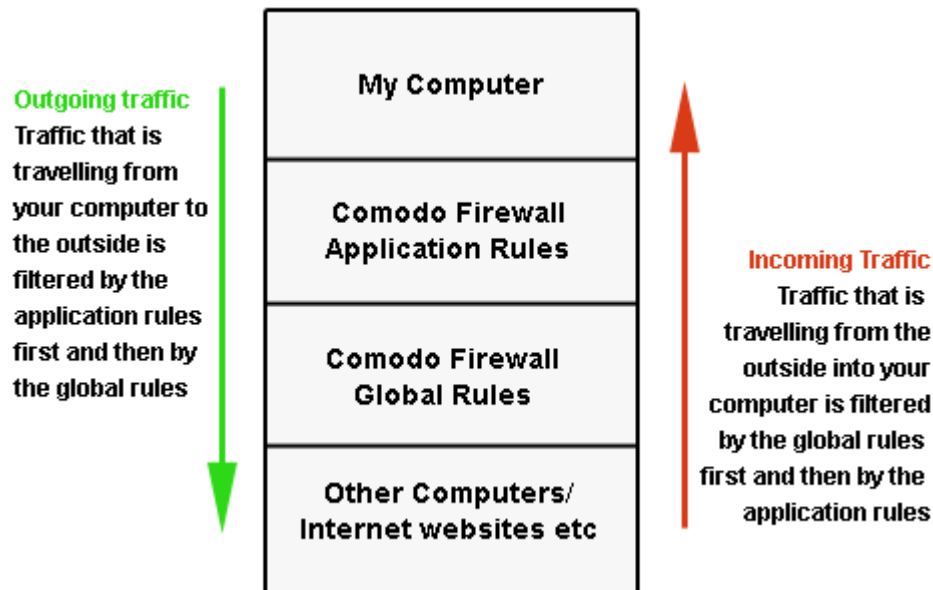
- Click 'OK' to save the firewall rule.

6.3.3. Global Rules

'Global Rules' are applied to *all* traffic traveling in and out of your computer. This makes them different to 'Application Rules', which are applied to and triggered by traffic for a specific application.

Comodo Firewall analyzes every packet of data in and out of your PC using combination of Application and Global Rules.

- Outgoing connection attempts - Application rules are consulted first and the global rules second.
- Incoming connection attempts - Global rules are consulted first and the application rules second.



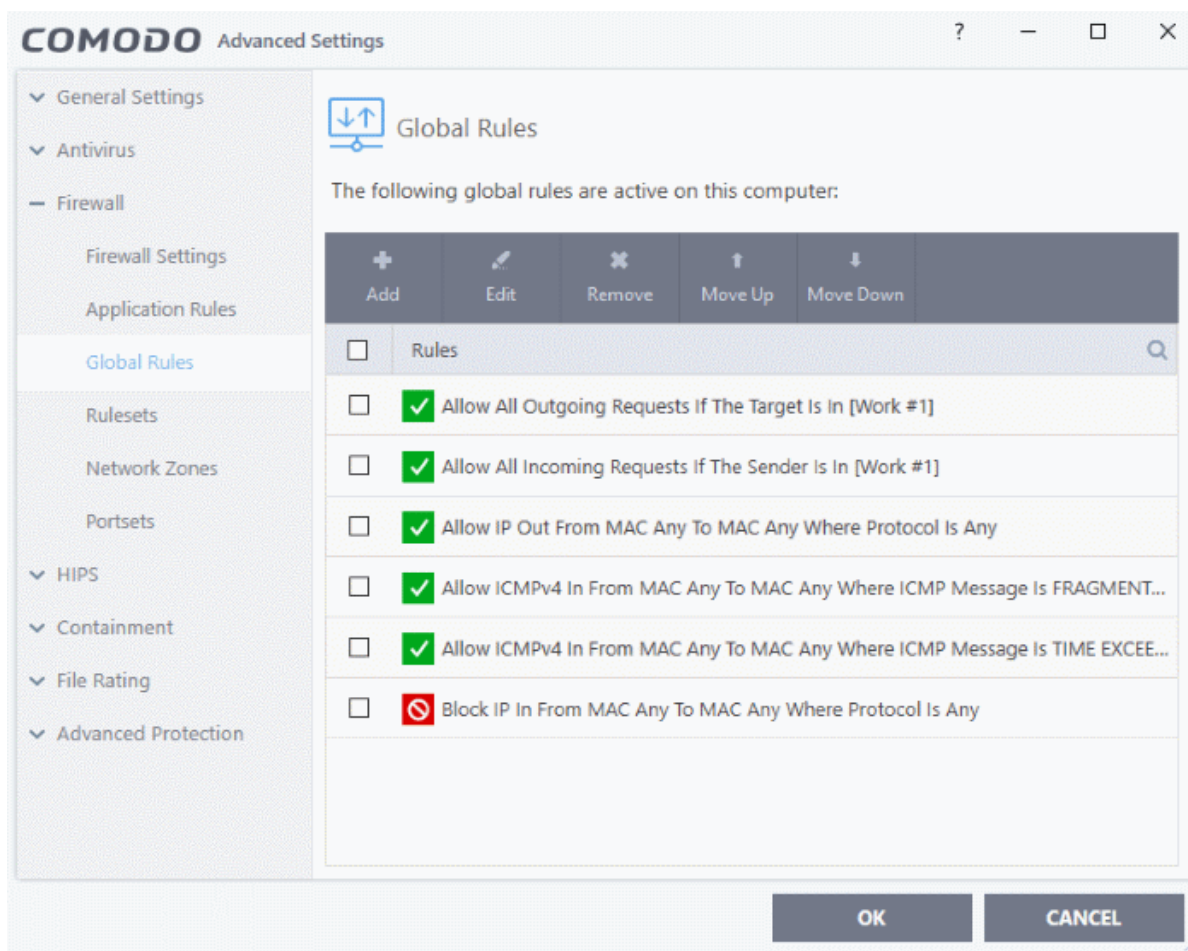
Therefore, outgoing traffic has to pass both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to pass any global rules first then application specific rules that may apply to the packet.

Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

The 'Global Rules' panel in the 'Advanced Settings' interface allows you to view create and manage the global firewall rules.

Open the Global Rules panel

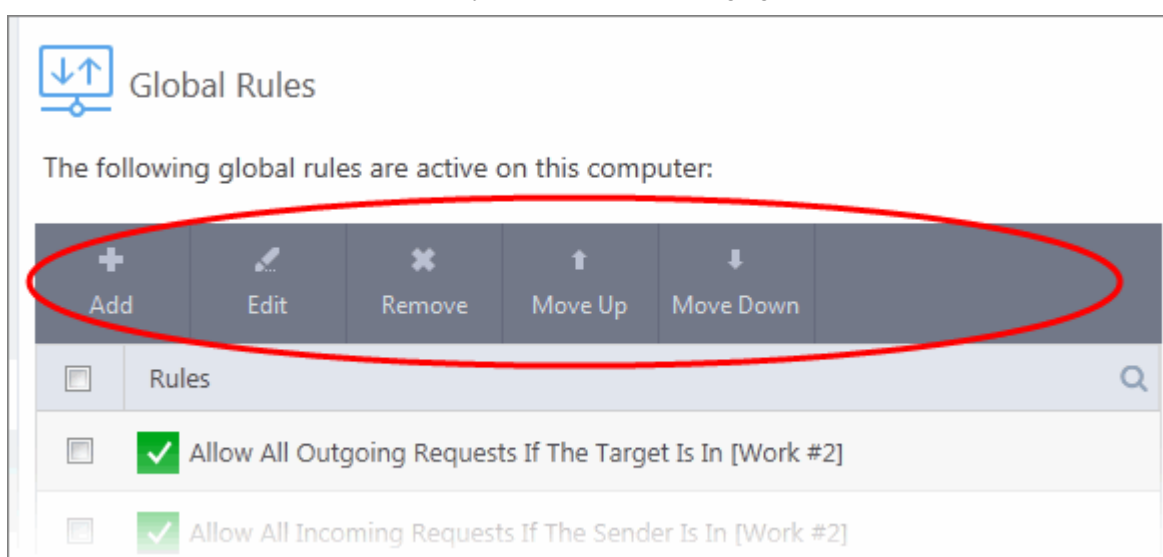
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Global Rules' on the left:



You can search for a specific rule in the list by clicking the search icon on the right and entering the name of the rule in part or full.

General Navigation:

The control buttons at the top of the list enable you to create and manage global rules.



- **Add** - Allows you to add a new global rule. See the section '**Adding and Editing a Firewall Rule**' in the previous section 'Application Rules' for guidance on creating a new rule.
- **Edit** - Allows you to modify the selected global rule. See the section '**Adding and Editing a Firewall Rule**' in the previous section 'Application Rules' for guidance on editing a new rule.

- **Remove** - Deletes the selected rule.
- **Purge** - Runs a system check to verify that all the applications for which rules are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down** - The traffic is filtered by referring to the rules in order from the top. The Move Up and Move Down buttons enable you to change the priority of a selected rule.

To add a global rule, click the 'Add' button. To edit an existing global rule, right click and select 'Edit'. The configuration of Global Rules is identical to that of application rules.

- See **Application Rules** for an introduction to the rule setting interface.
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration.

6.3.4. Firewall Rule Sets

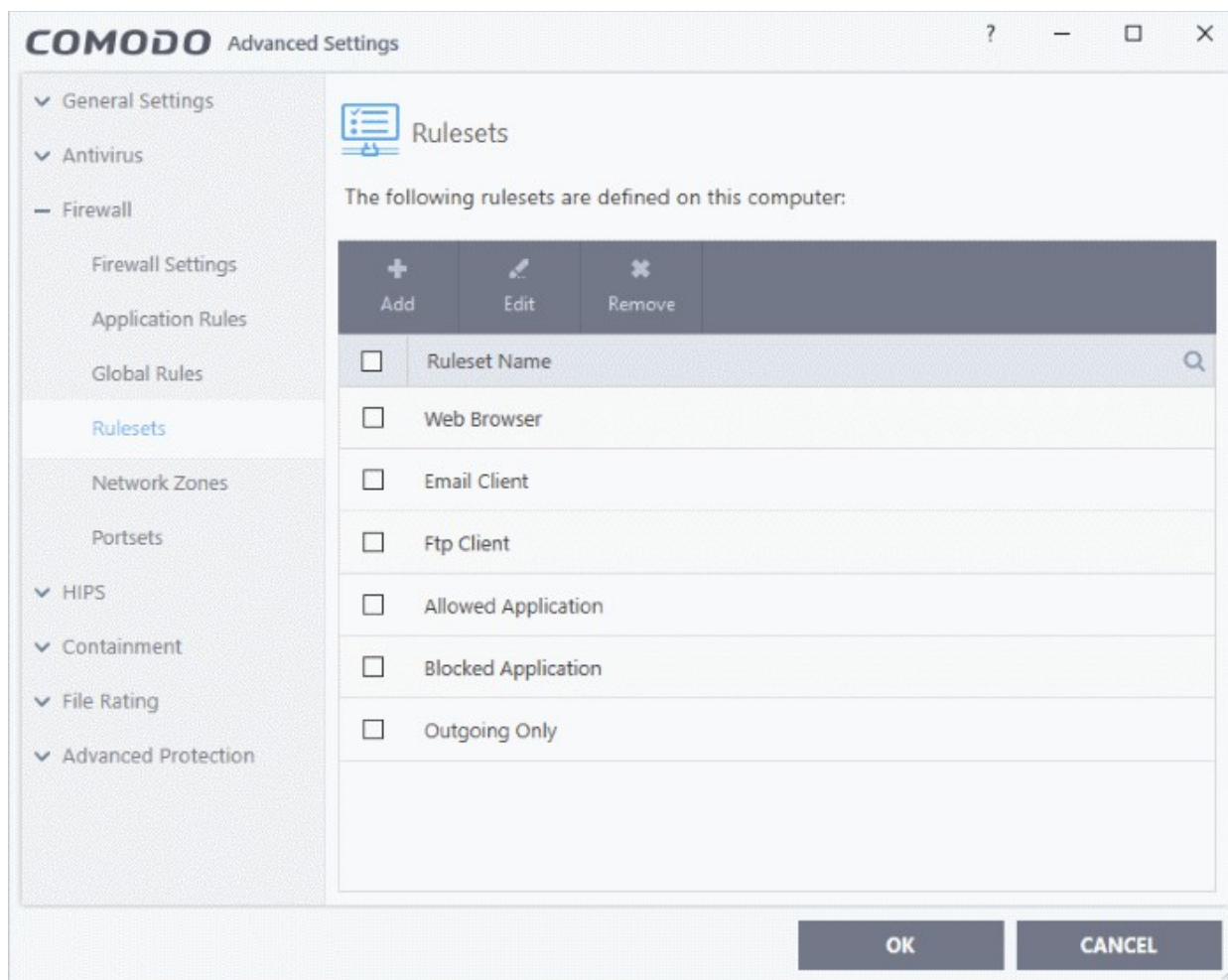
A firewall ruleset is a collection of one or more individual firewall rules which can be deployed on multiple applications. CCS ships with six predefined rulesets and allows you to create custom rulesets.

This section contains advice on the following:

- **Predefined Rulesets**
- **Creating a new ruleset**

To open the Rulesets panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Rulesets' on the left:
- The interface displays a list of pre-defined and custom rulesets. You can search for a specific ruleset by clicking the search icon on the right and entering the name of the ruleset in part or full:



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.

CCS 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. For more details, see [Adding and Editing Firewall Rules](#) in 'Application Rules'.

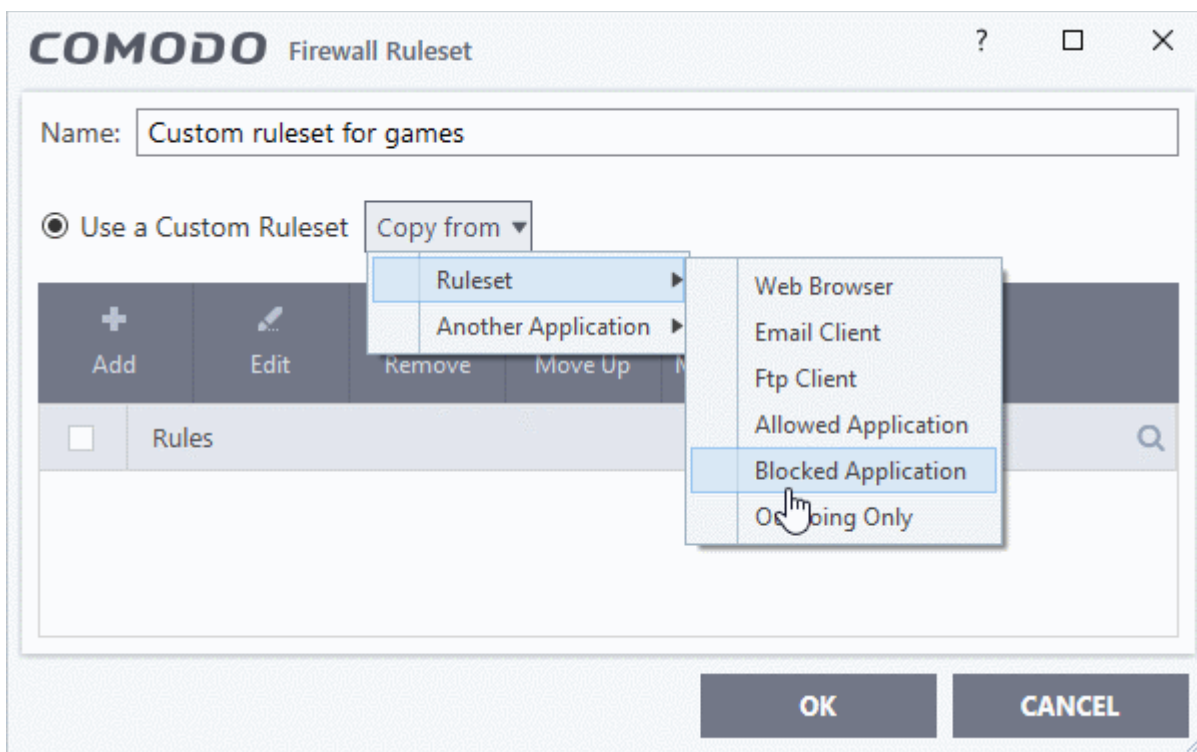
Creating a new ruleset

You can create new rulesets with custom network access control rules as per your requirements. These can then be rolled out to specific applications when [creating a Firewall ruleset](#) for the application.

To add a new Ruleset

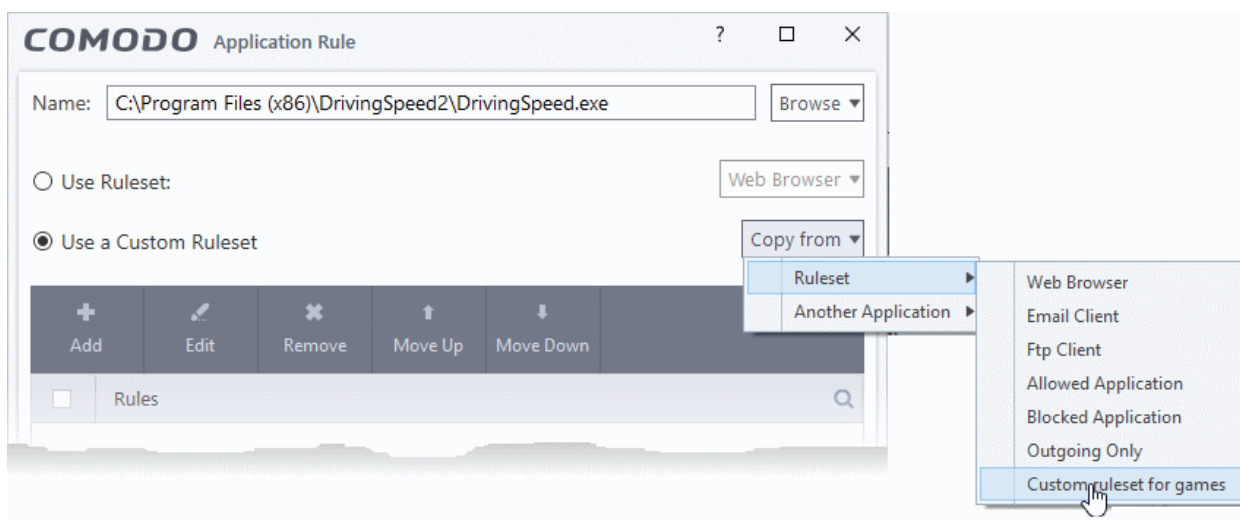
- Click the 'Add' button at the top of the list of rulesets in the 'Rulesets' panel

The 'Firewall Ruleset' interface will open.



- As this is a new ruleset, you need to name it in the text field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for.
- Next you should add and configure the individual rules for this ruleset. You can choose to use an existing ruleset as a starting point and add/edit rules as required. See **'Adding and Editing a Firewall Rule'** for more advice on this.

Once created, this ruleset can be quickly called when **creating or modifying a Firewall ruleset** for an application:



To view or edit an existing predefined Ruleset

- Double click on the ruleset Name in the list

Or

- Select the ruleset name then click the 'Edit' button
- Details of the process from this point on can be found [here](#).

6.3.5. Network Zones

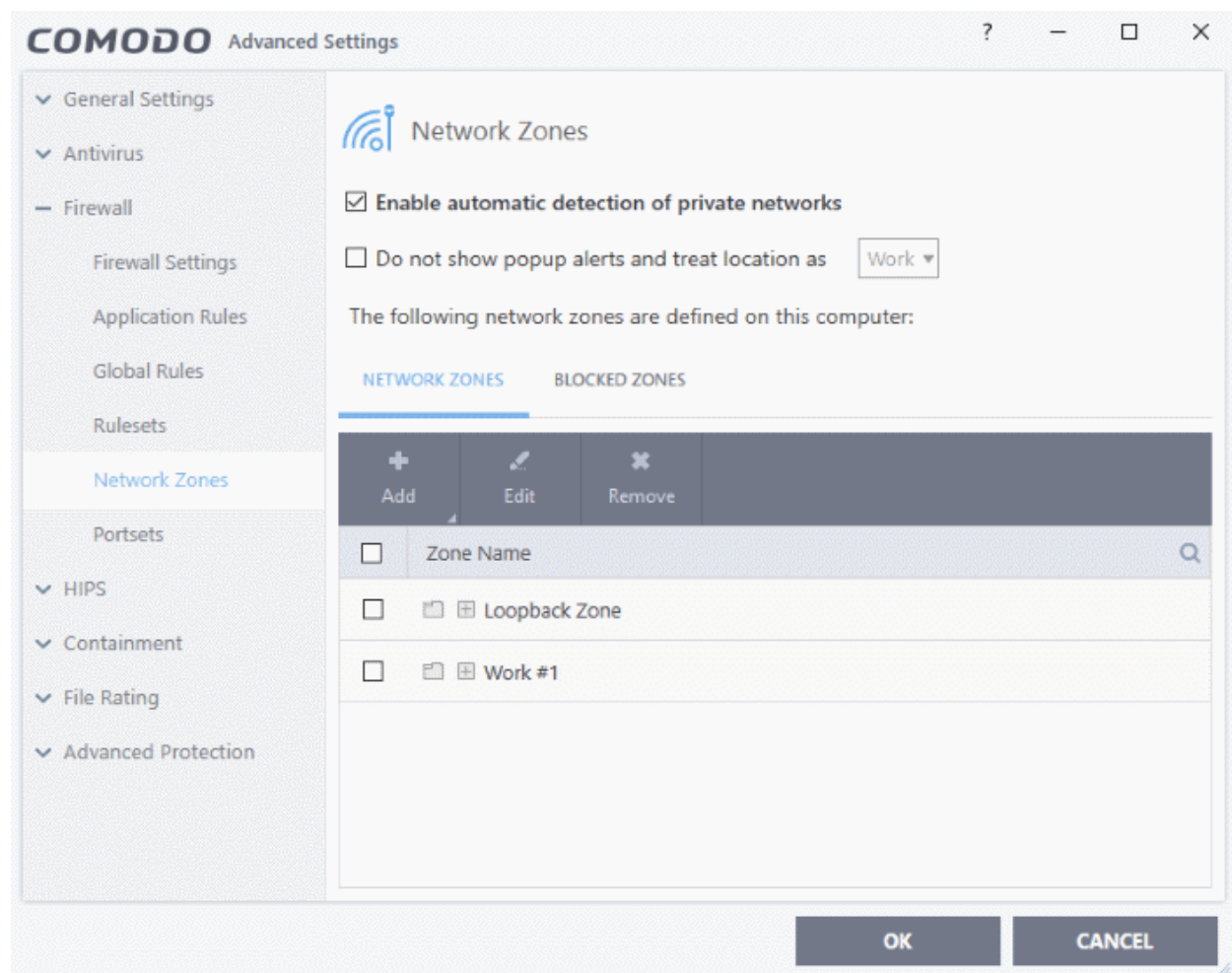
A 'Network Zone' can consist of an individual machine (including a single home computer connected to the internet) or a network of thousands of machines. Access to any network zone can be easily granted or denied in the network zones panel.

The 'Network Zones' panel allows you to:

- Configure automatic detection of new networks (wired or wireless) that your computer connects to
- Configure alerts for network connections
- Define network zones that are trusted and specify access privileges to them
- Define network zones that are untrusted and block access to them

To open the Network Zones panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Network Zones' on the left:

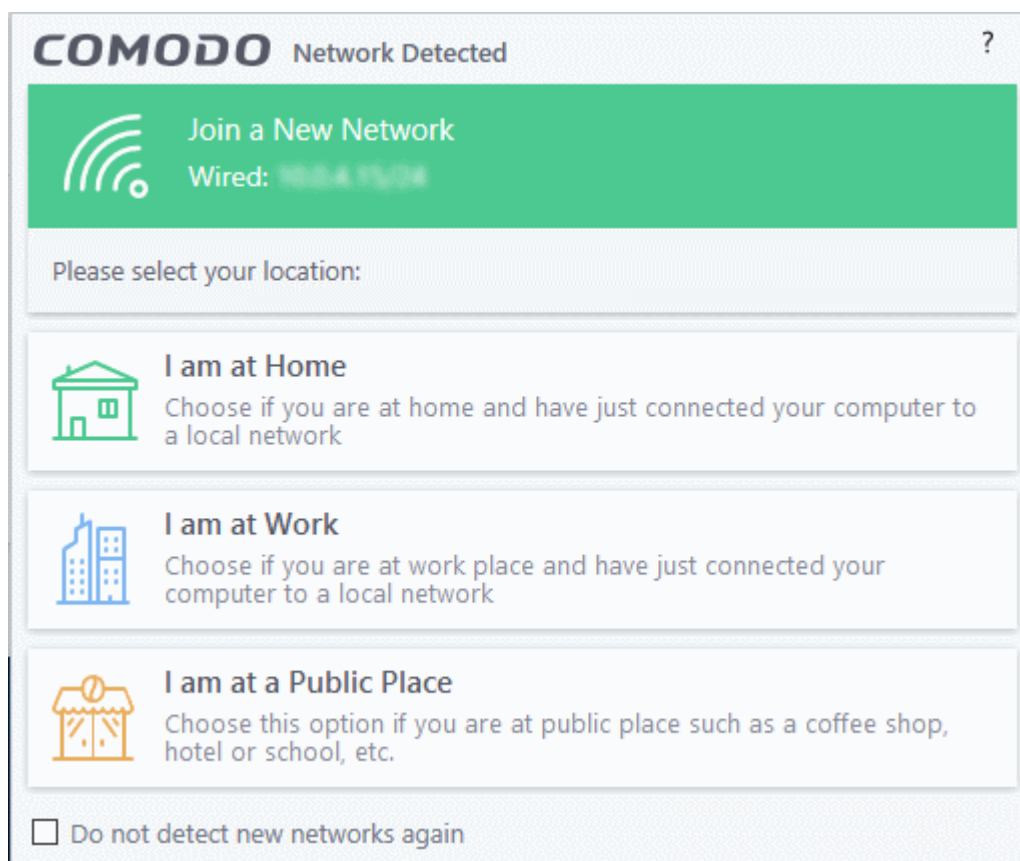


- **Enable automatic detection of private networks** - Instructs Comodo Firewall to monitor for attempted connections to any new wired or wireless network (**Default = Enabled**). Deselect this option if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in **'Network**

Zones' and through the '**Stealth Ports Wizard**').

- **Do not show popup alerts and treat location as** - If enabled, the 'new network connection' alert will not appear and the network location will default to the location selected in the drop-down - Home, Work or Public. (**Default = Disabled**)

If 'automatic detection' is enabled, and 'do not show...' is disabled, then the following alert will be displayed whenever your system tries to connect to a new network:



Select the appropriate network type for your connection. Your firewall configuration will be optimized for security and usability accordingly.

- Select 'Do not automatically detect new networks again' if you are an experienced user that wishes to manually set-up their own trusted networks. This can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**'.

The panel has two tabs:

- **Network Zones** - Allows you to define network zones with specific access rights. Application access privileges are specified through the **Application Rule** interface. See '**Creating or Modifying Firewall Rules**' for more details.
- **Blocked Zones** - Allows you to define trusted networks that are not trustworthy and to block access to them.

6.3.5.1. Network Zones

A 'Network Zone' can consist of an individual machine (including a single home computer connected to internet) or a network of thousands of machines. You can grant or deny access to a network zone as required.

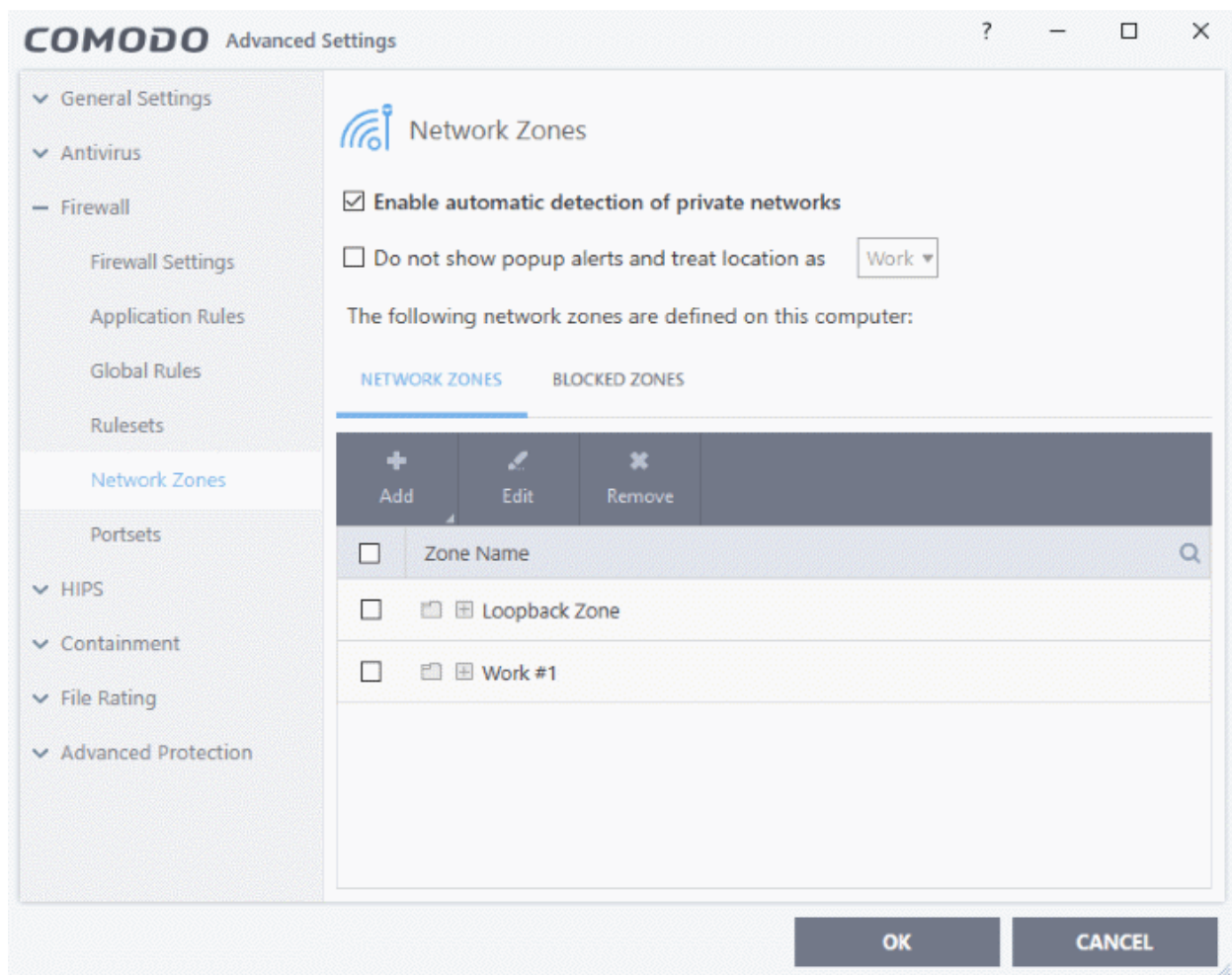
Background Note:

- A computer network is a connection between computers through a cable or some type of wireless connection.

- It enables users to share information and devices between computers and other users within the network.
- Obviously, there are certain computer networks which you need to grant access to, including your home or work network.
- Conversely, there may be other networks with which you want to restrict communication, or even block entirely.

To add and manage network zones

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Network Zones' on the left.
- Click the 'Network Zones' tab:



The 'Network Zones' tab displays a list of zones added to CCS. You can add new zones and manage existing zones.

Note 1: Adding a zone to this area does not, by itself, define any permission levels or access rights to the zone. This area lets you define the zones so you can quickly assign such permissions **in other areas of the firewall**.

Note 2: A network zone can be designated as 'Trusted' and allowed access from the '**Manage Network Connections**' interface. An example would be your home computer or network.

Note 3: A network zone can be designated as 'Blocked' and denied access by using the '**Blocked Zones**' interface. An example would be a known spyware site.

Note 4: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rule** assigned to a zone will inspect all traffic to/from a zone.

Note 5: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc) once you connect to them. This can be disabled by deselecting the option 'Enable automatic detection of private networks' in the

Firewall Settings panel.

You can use search for a specific zone by clicking the search icon and entering the name of the zone in part or full.

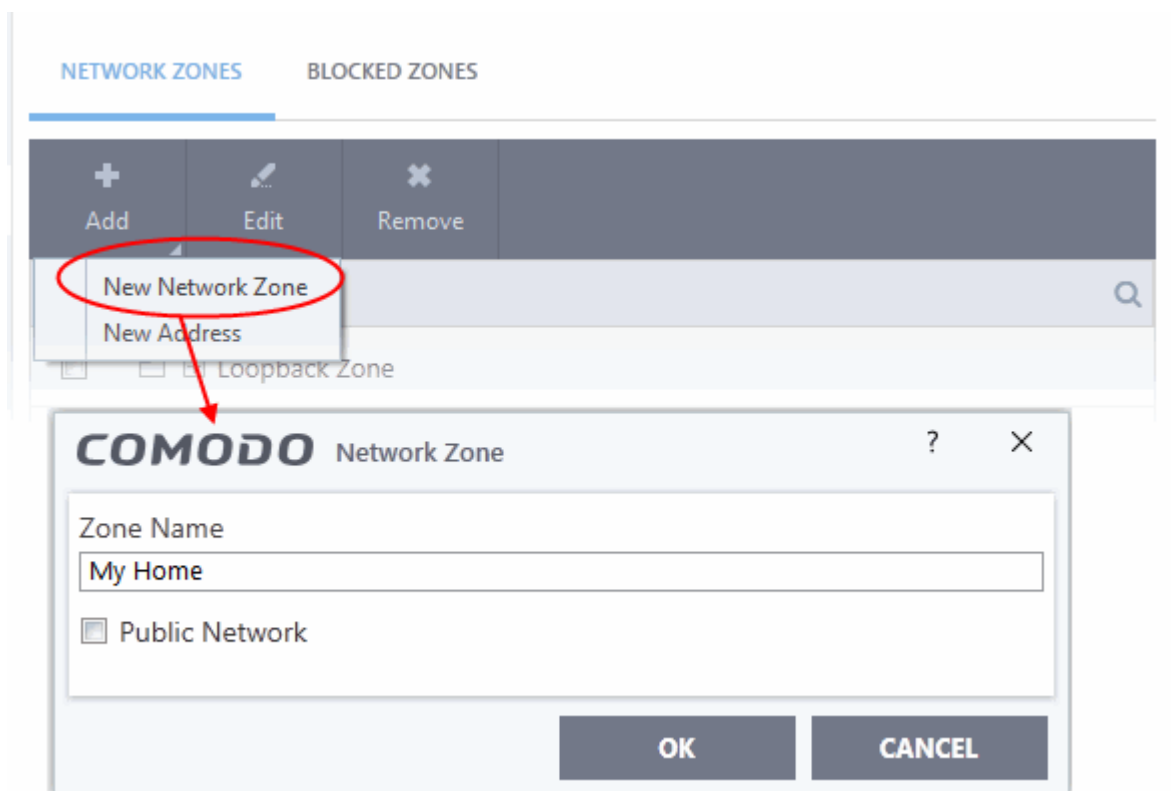
Defining a new Network Zone

To add a new network zone:

- Step 1 - **Define a name for the zone.**
- Step 2 - **Select the addresses to be included in the zone.**

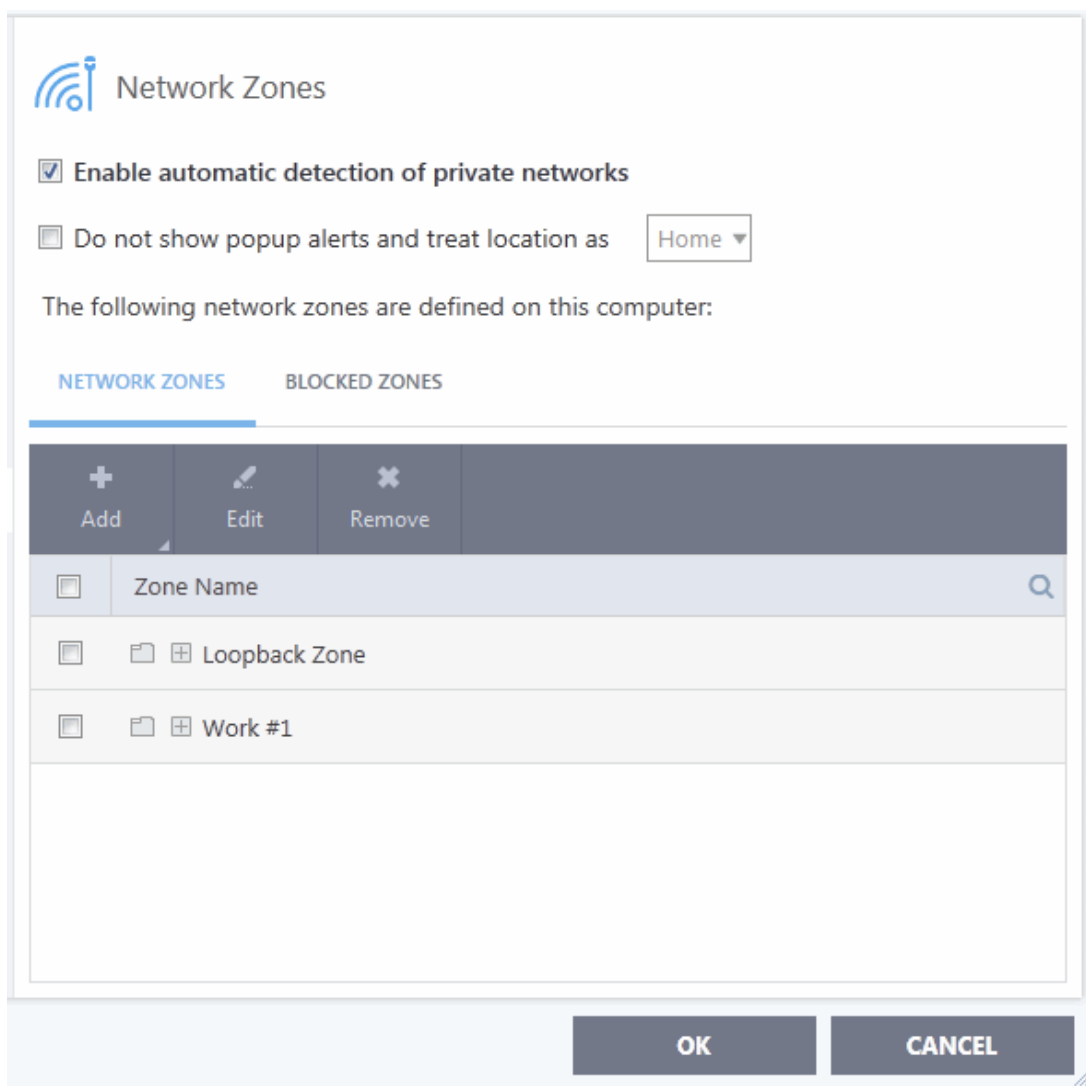
Step 1 - Define a name for the zone

- Click the 'Add' button at the top of the list and choose 'New Network Zone' from the options.



- 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:

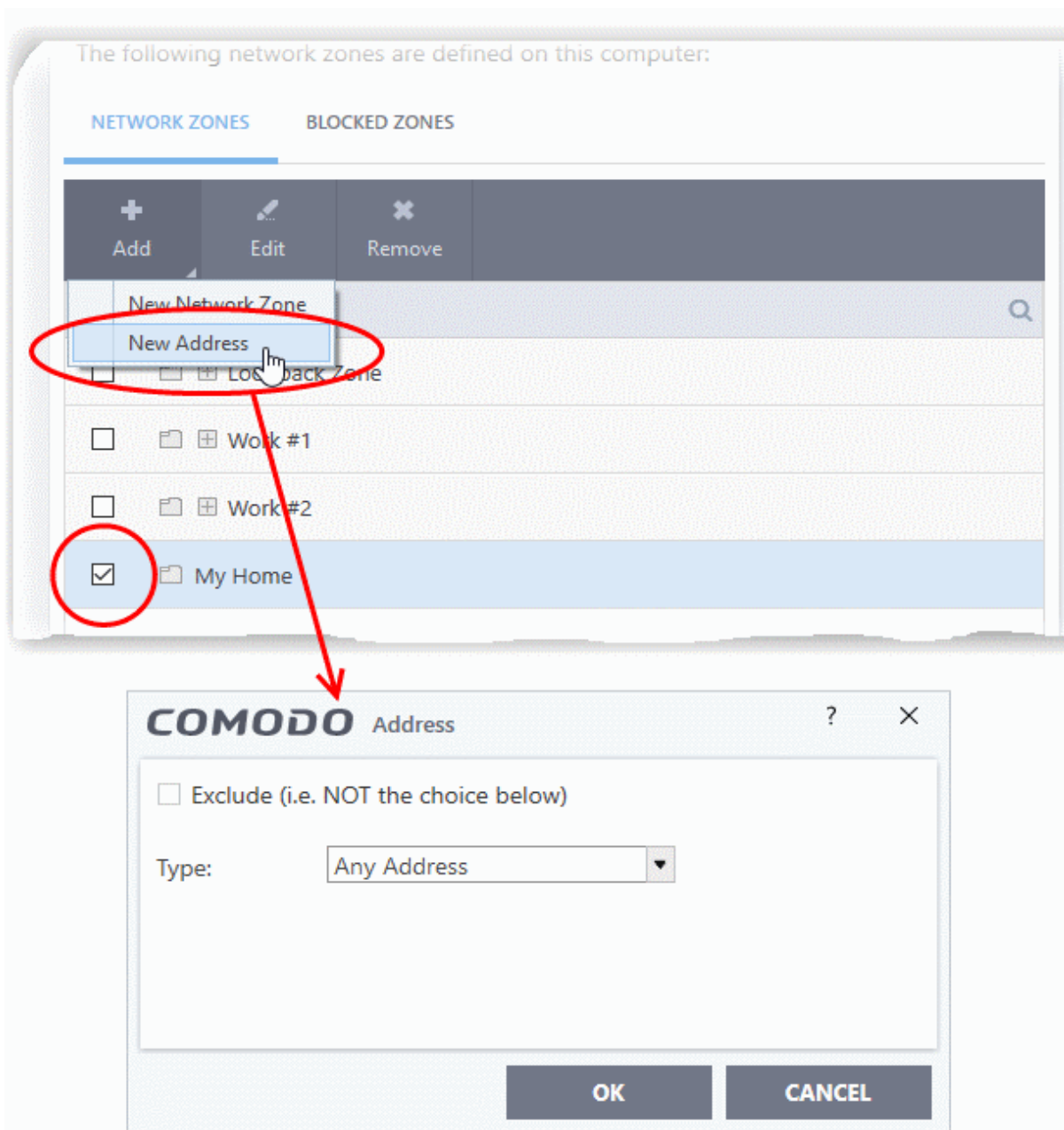


Step 2 - Select the addresses to be included in this zone

- 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 Address - Adds all the IP addresses (0.0.0.0- 255.255.255.255) to the zone.
2. Host Name - Enter a named host which denotes an address on your network.
3. IPv4 Range - Will include all the IPv4 addresses between the values you specify in the 'Start Range' and 'End Range' text boxes.
4. IPv4 Single Address - Enter a single IP address to be added to the zone - e.g. 10.100.100.11.
5. IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and Mask of the network you wish to add to the defined zone.
6. IPv6 Single Address - Enter a single address to be added to the zone - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.

8. MAC Address - Enter a specific MAC address to be added to the zone.
 - Click 'OK' to confirm your choice.
 - Click 'OK' in the 'Network Zones' interface.

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

- Quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**

COMODO Firewall Rule

Action: Log as firewall event if this rule is fired

Protocol:

Direction:

Description:

SOURCE ADDRESS DESTINATION ADDRESS SOURCE PORT DESTINATION PORT

Exclude (i.e. NOT the choice below)

Type:

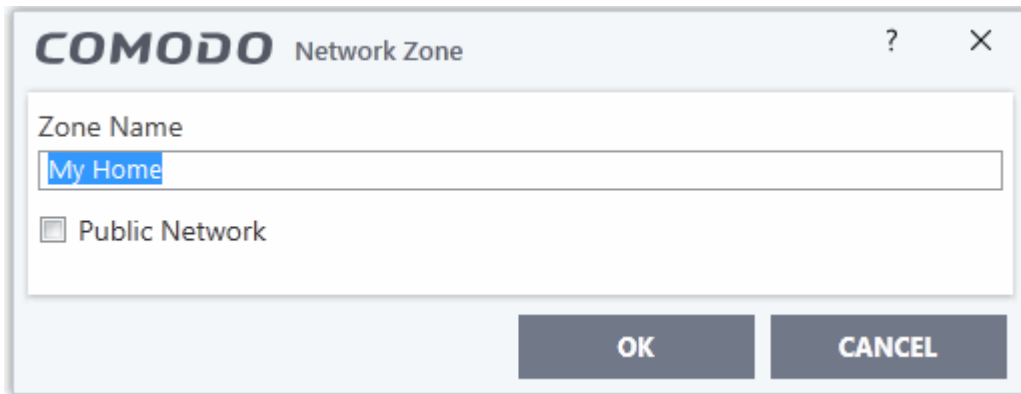
Zone:
Loopback Zone
Work #1
Work #2
Work #3
Work #4
Talkatives Computers
Work #5
My Home

OK CANCEL

- Quickly called and designated as a blocked zone from the '**Blocked Zones**' interface

To edit the name of an existing Network Zone

1. Select the name of the zone in the list (e.g., My Home) and click the 'Edit' button from the top or double click on the network zone name.



2. Edit the name of the zone.

To add more addresses to an existing Network Zone

- Select the network name, click the 'Add' > 'New Address' from the top.
- Add new address from the **'Address' interface**.

To modify or change the existing address in a zone

- Click the + button beside the network zone name to expand the addresses
- Double click on the address to be edited or select the address, click 'Edit' at the top
- Edit the address from the **'Address' interface**.

To remove an existing address in a zone

- Click the '+' button beside the network zone name to expand the addresses
- Select the address and click 'Remove' from the top

6.3.5.2. Blocked Zones

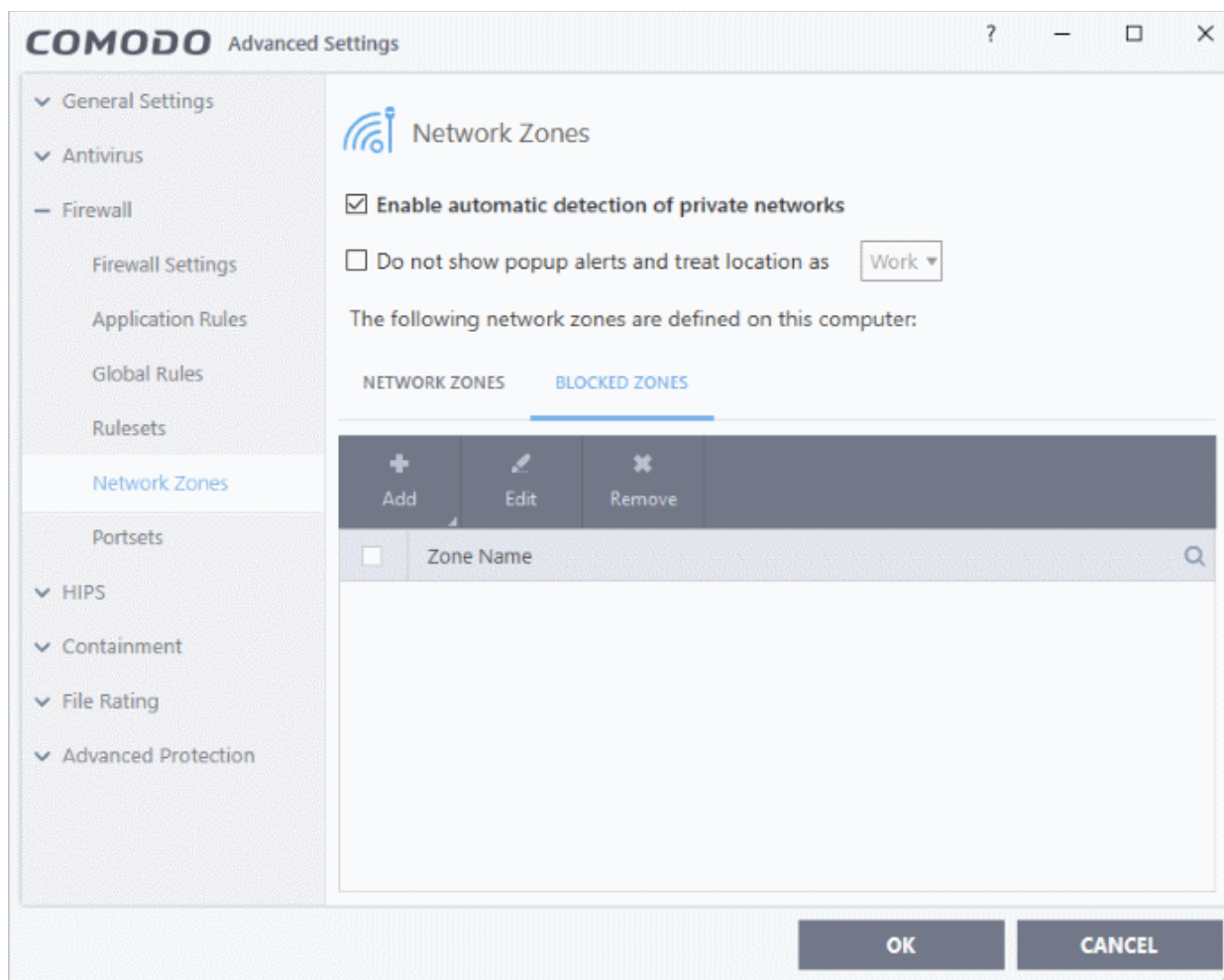
A computer network lets you share information and devices with other users and other computers. There are certain networks that you'll want to 'trust' and grant access to, for example your home or work network. Conversely, there may be other networks that you do not trust and want to restrict communications with or block entirely.

The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not wish to trust.

Note: We advise new or inexperienced users to first read **'Network Zones'**, **'Stealth Ports Wizard'** and **'Application Rules'** before blocking zones using this interface.

To add and manage blocked zones

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Network Zones' on the left.
- Click the 'Blocked Zones' tab:



The 'Blocked Network Zones' tab allows you to:

- **Deny access to an existing network zone**
- **Deny access to a network by manually defining a new blocked zone**

Note 1: You must create a zone before you can block it. There are two ways to do this;

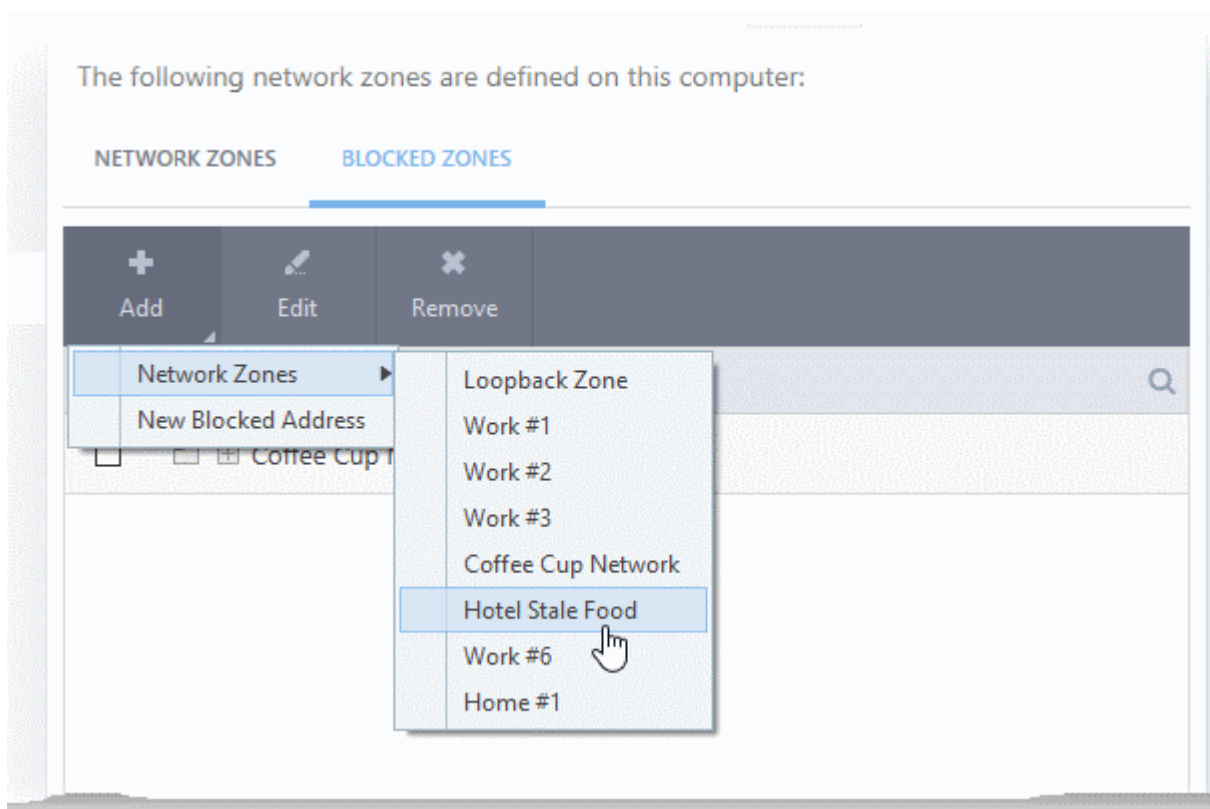
1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

Note 2: You cannot reconfigure *existing* zones from this interface (e.g., to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

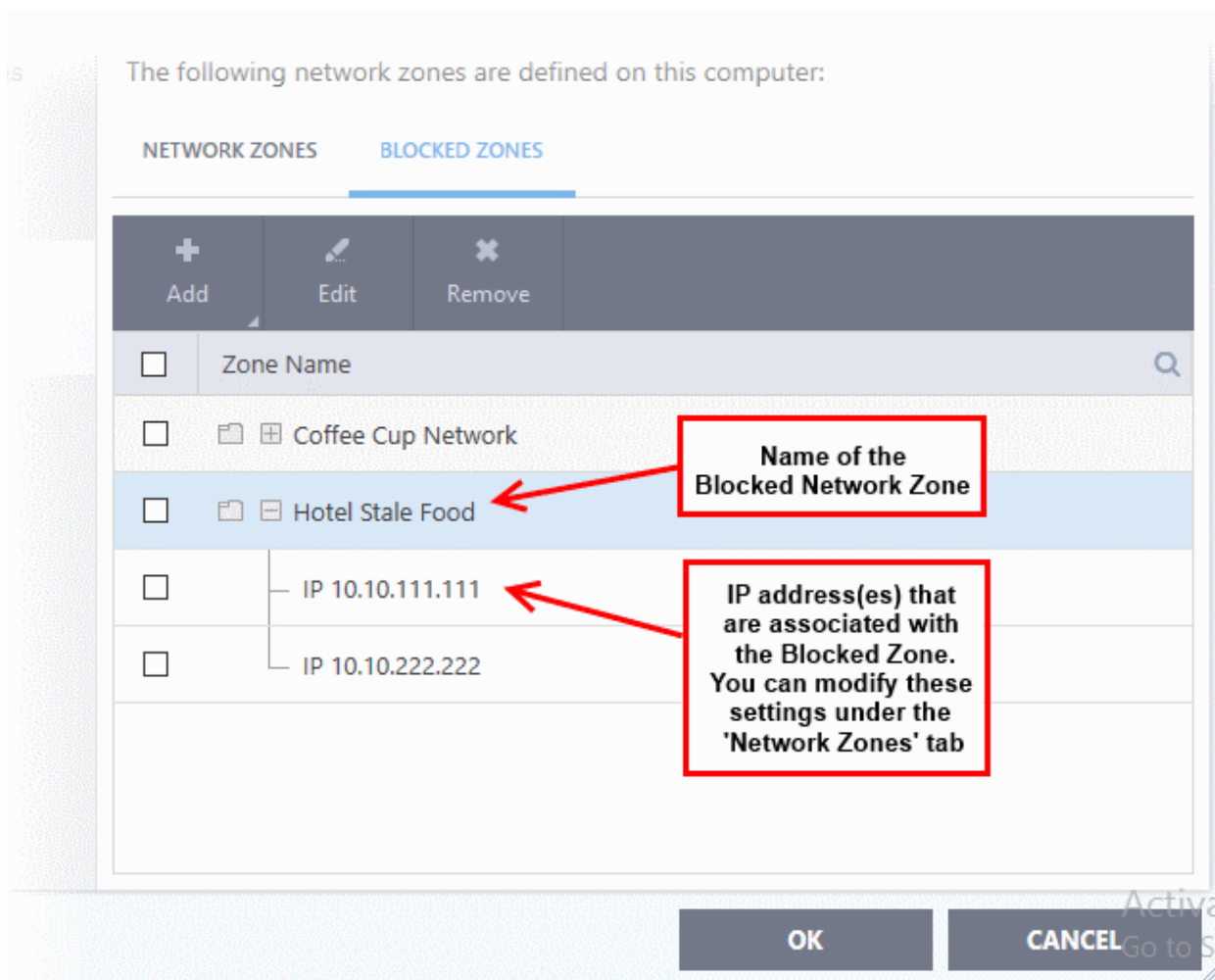
You can search for specific blocked zone by clicking the magnifying glass icon and entering the name of the zone in part or full.

To deny access to an existing network zone

1. Click 'Add' button at the top and choose 'Network Zones' from the options
2. Select the particular zone you wish to block.



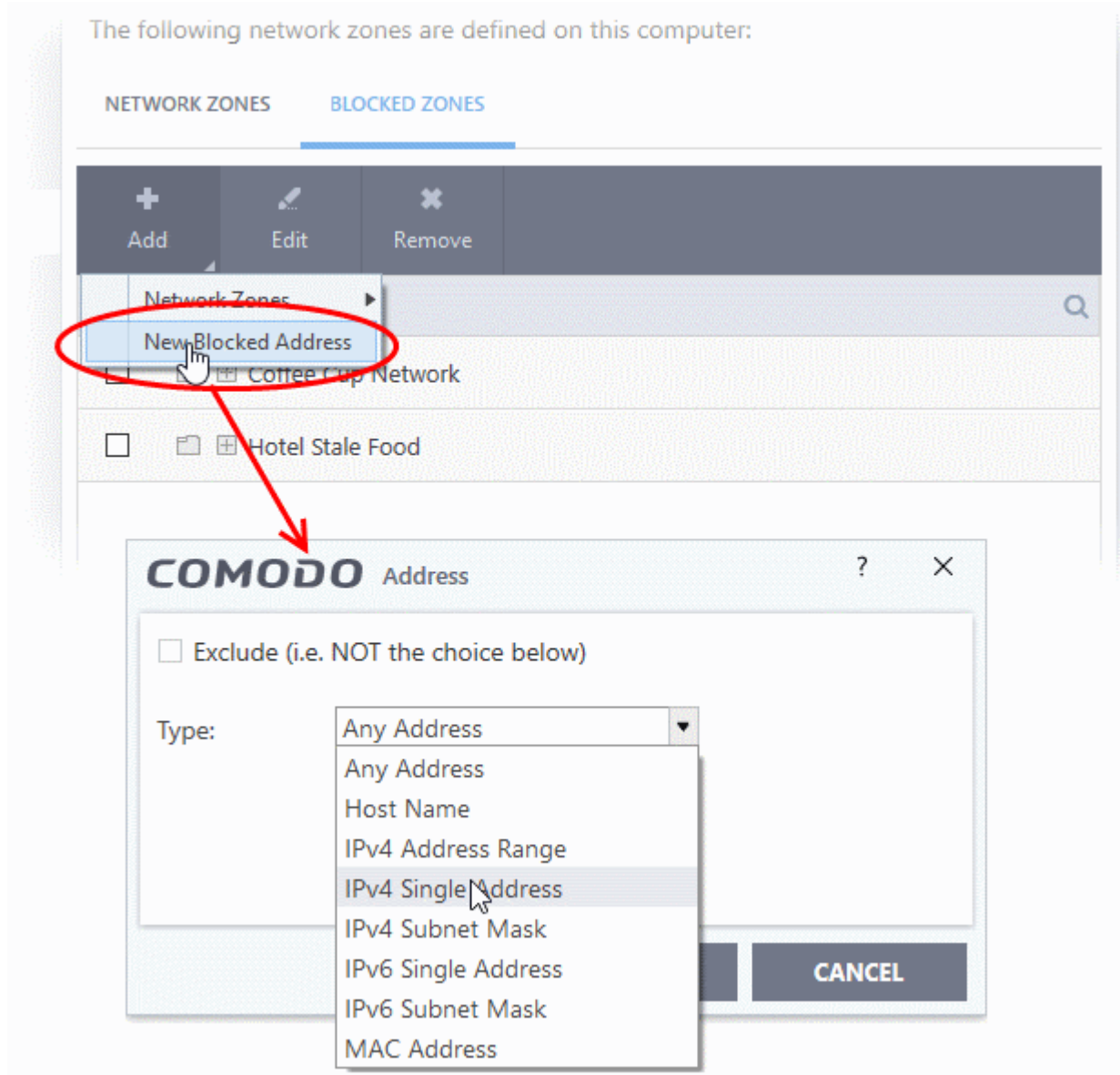
The selected zone will appear in the 'Blocked Zones' interface.



3. Click 'OK' to confirm your choice. All traffic intended for and originating from devices in this zone is now blocked.

To deny access to a network by manually defining a new blocked zone

1. Click the 'Add' button and choose 'New Blocked Address':



Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

Address Types:

- Any Address - Will block connections from all IP addresses (0.0.0.0- 255.255.255.255)
- Host Name- Enter a named host which denotes an address on your network.
- IPv4 Range - Will block access to the IPv4 addresses you specify in the 'Start Range' and 'End Range' text boxes.
- IPv4 Single Address - Block access to a single address - e.g. 192.168.200.113.
- IPv4 Subnet Mask - A subnet mask allows administrators to divide a network into two or more networks by splitting the host part of an IP address into subnet and host numbers. Enter the IP address and

Mask of the network you wish to block.

- IPv6 Single Address -Block access to a single address - e.g. 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
 - IPv6 Subnet Mask. Ipv6 networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
 - MAC Address - Block access to a specific MAC address.
2. Select the address to be blocked and click OK

The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

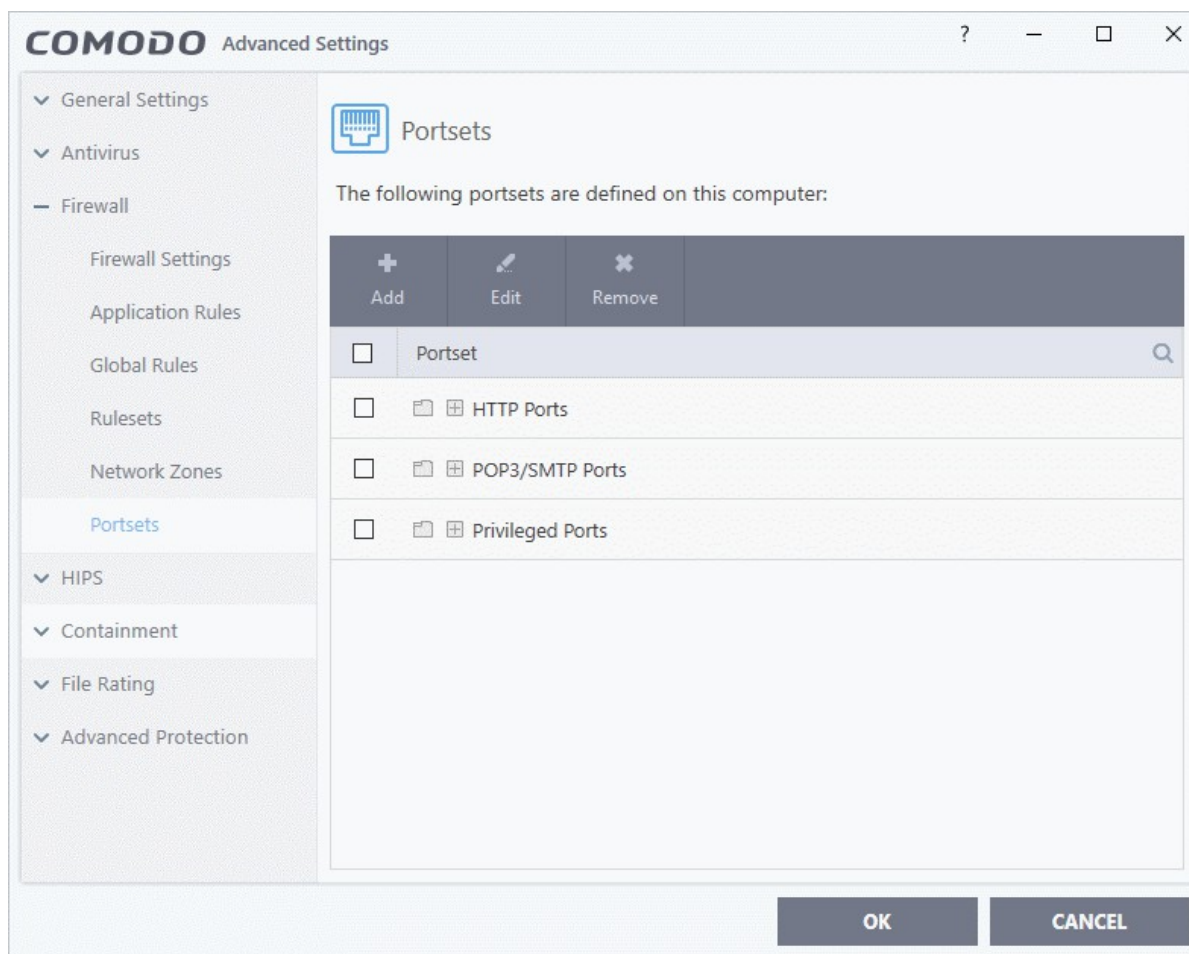
3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from devices in this zone is now blocked.

6.3.6. Port Sets

Port sets are predefined groups of one or more ports that can be used as targets in **Application Rules** and **Global Rules**. The 'Port Sets' panel lets you view and manage pre-defined port sets and to add new port sets.

Open the Portsets panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Firewall' > 'Portsets' on the left:



Port Sets are shown in a tree structure. Click the + button beside a port set name to view ports in the set. CCS ships with three default portsets:

- **HTTP Ports:** 80, 443 and 8080. These are the default ports for http traffic. Your internet browser uses these ports to connect to the internet and other networks.
- **POP3/SMTP Ports:** 110, 25, 143, 995, 465 and 587. These ports are typically used for email communication by mail clients like Outlook and Thunderbird.
- **Privileged Ports:** 0-1023. This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports.

You can search for a specific portset by clicking the search icon and entering the name of the portset in part or full.

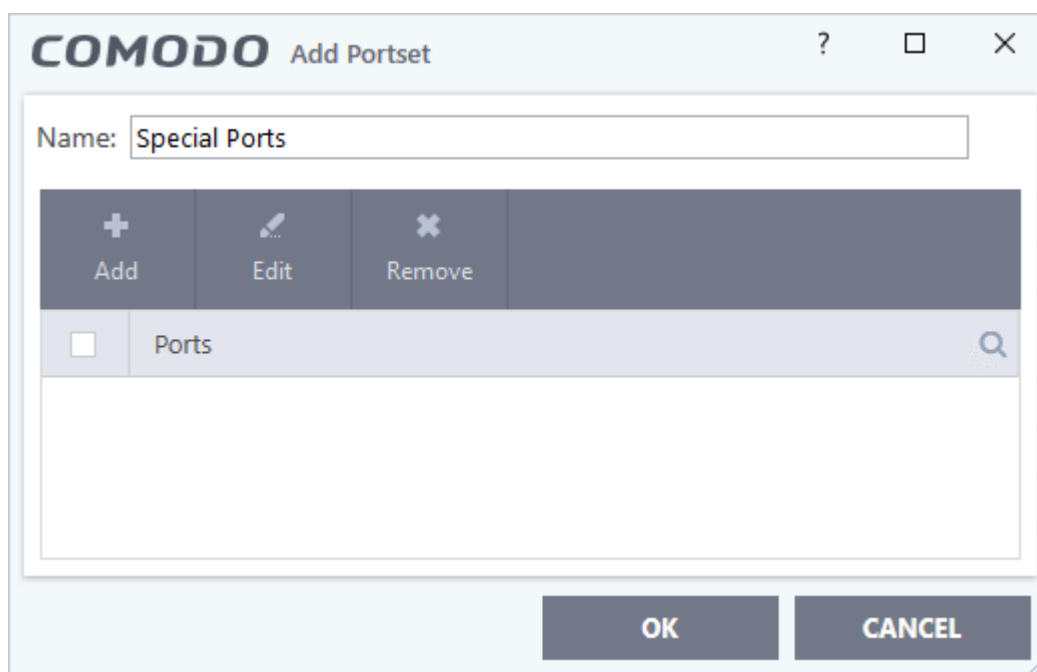
Defining a new Port Set

After defining a new portset you can apply it to applications through the **Application Rule** interface. See '**Creating or Modifying Firewall Rules**' for more details.

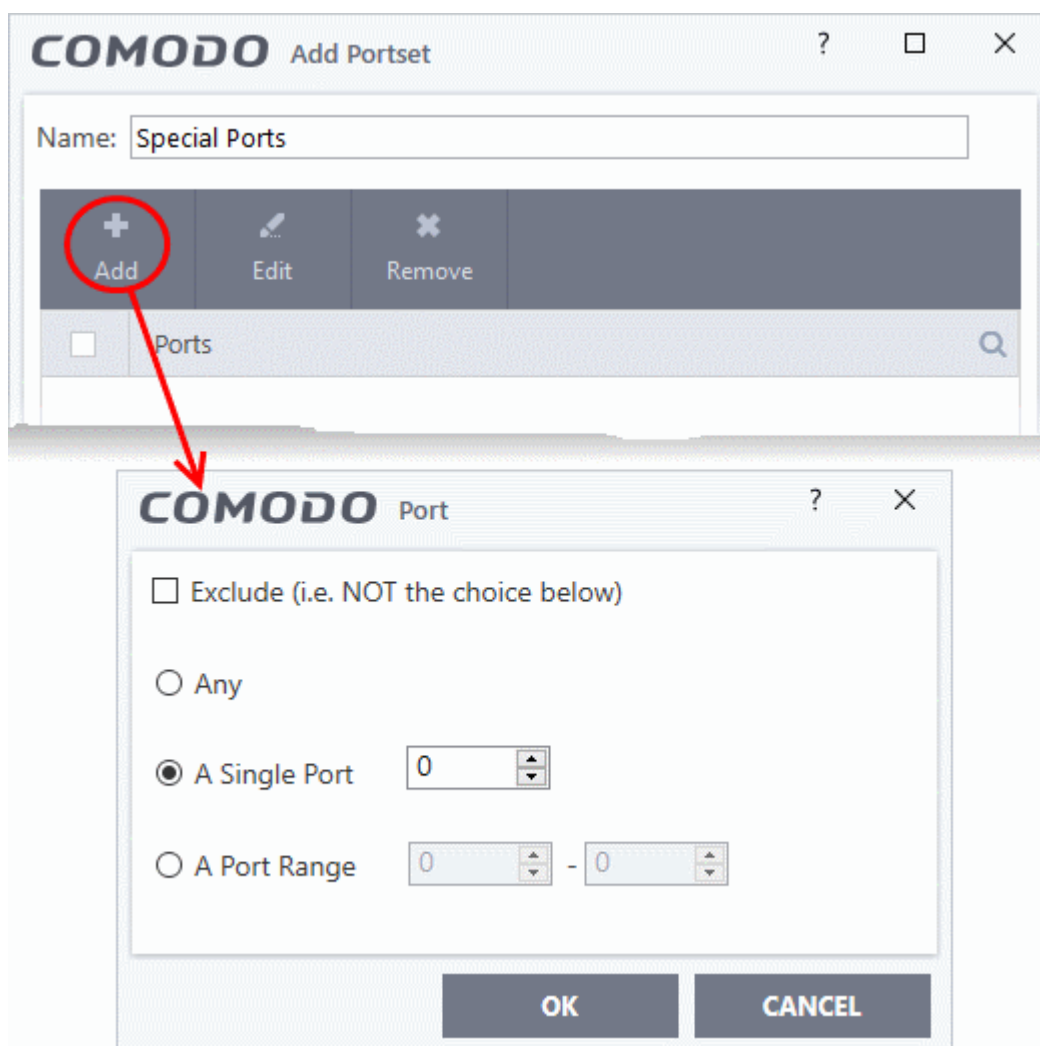
To add a new portset

1. Click the 'Add' button at the top.

The 'Add Portset' dialog will open.



2. Enter a name for the portset in the 'Name' field.
3. Click the 'Add' button to add ports/port ranges to the set:



4. Specify the ports to be included in the new portset:
 - **Any** - to choose all ports
 - **A single port** - Specify the port number
 - **A port range** - Enter the start and end port numbers in the respective combo boxes.
 - **Exclude (i.e. NOT the choice below)**: Means all ports will be included in the portset except the ones you specify here
5. Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Edit Portset' interface.
6. Click 'OK' in the 'Add Portsets' interface to create the new portset.

Once created, a Portset can be quickly called as 'A Set of Ports' when **creating or modifying a Firewall Ruleset**

COMODO Firewall Rule

Action: Log as firewall event if this rule is fired

Protocol:

Direction:

Description:

SOURCE ADDRESS DESTINATION ADDRESS **SOURCE PORT** DESTINATION PORT

Exclude (i.e. NOT the choice below)

Type:

Ports:

- HTTP Ports
- POP3/SMTP Ports
- Privileged Ports
- Special Ports**

OK CANCEL

To edit an existing port set

- Select the portset from the 'Portsets' interface and click the 'Edit' button from the top to bring up the 'Edit Portset' dialog.
- The editing procedure is similar to **adding the portset** explained above.

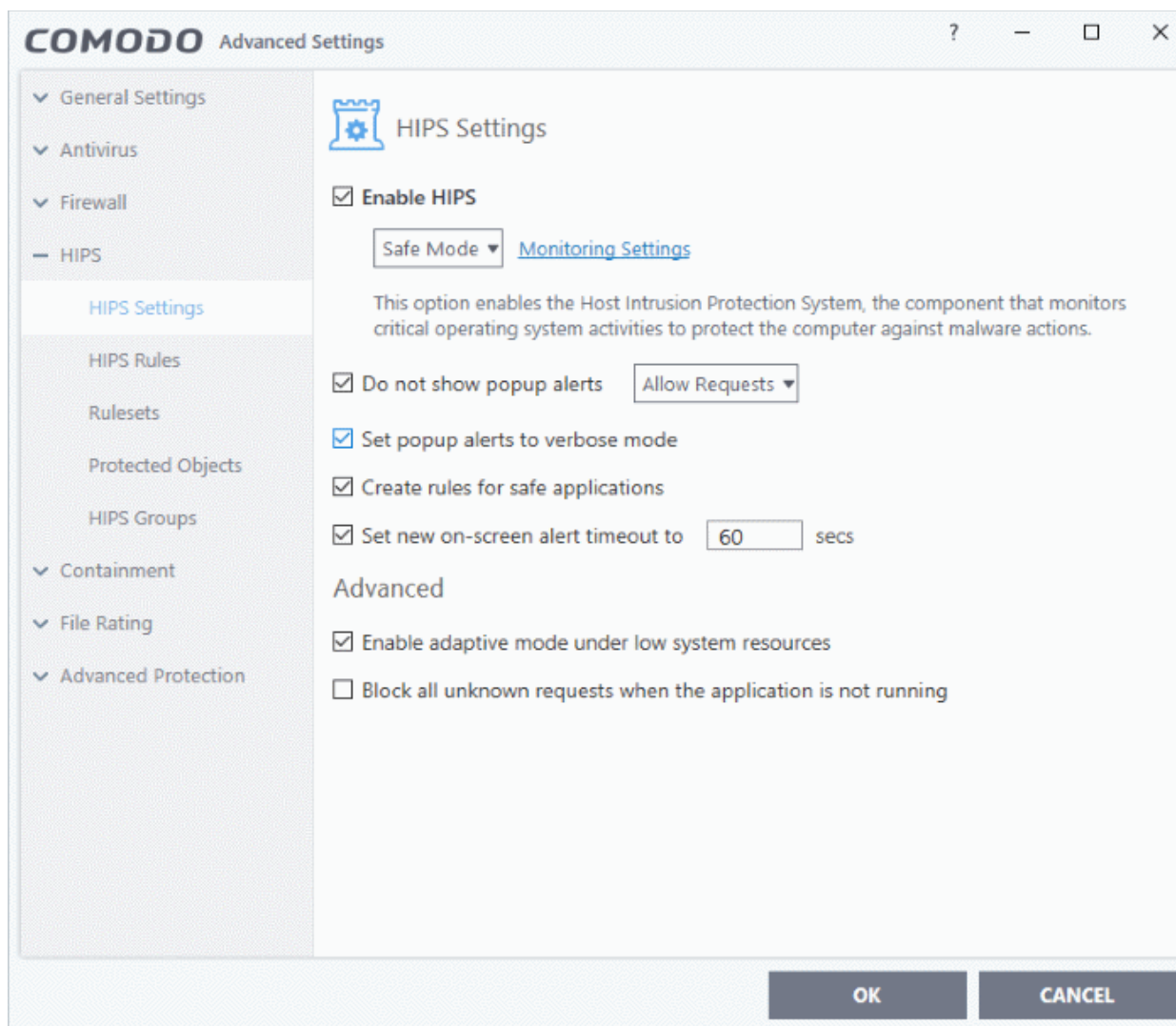
6.4. HIPS Configuration

- The Host Intrusion Protection System (HIPS) constantly monitors system activity and only allows processes to run if they comply with rules enforced by the user.
- Comodo Client Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection.
 - For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications 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 CCS home \ tasks screen to open the 'Advanced Settings' interface.

- Click 'HIPS' on the left:



The 'HIPS' area has sections that allow you to configure the following:

- **HIPS Settings** - Configure settings that govern the overall behavior of the HIPS component.
- **HIPS Rules** - View, create and modify rules that determine how the applications in your system have to be protected.
- **Rulesets** - View predefined rulesets and create new rulesets that can be applied to your applications in your system.
- **Protected Objects** - Define objects to be protected by HIPS such as specific folders, system critical registry keys and so on.
- **HIPS Groups** - View and edit predefined 'Registry Groups' and 'COM Groups', create new groups so as to add them to Protected Objects.

Note for beginners:

- This section often refers to 'executables' (or 'executable files'). An executable is a file that can instruct your computer to perform a task or function.
- Every program, application and device you run on your computer requires an executable file of some kind to start it.
- The most recognizable type of executable file is the '.exe' file. For example, 'winword.exe' is the name of the executable that instructs your computer to start and run Microsoft Word. Other types of executable

files include those with extensions .cpl, .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

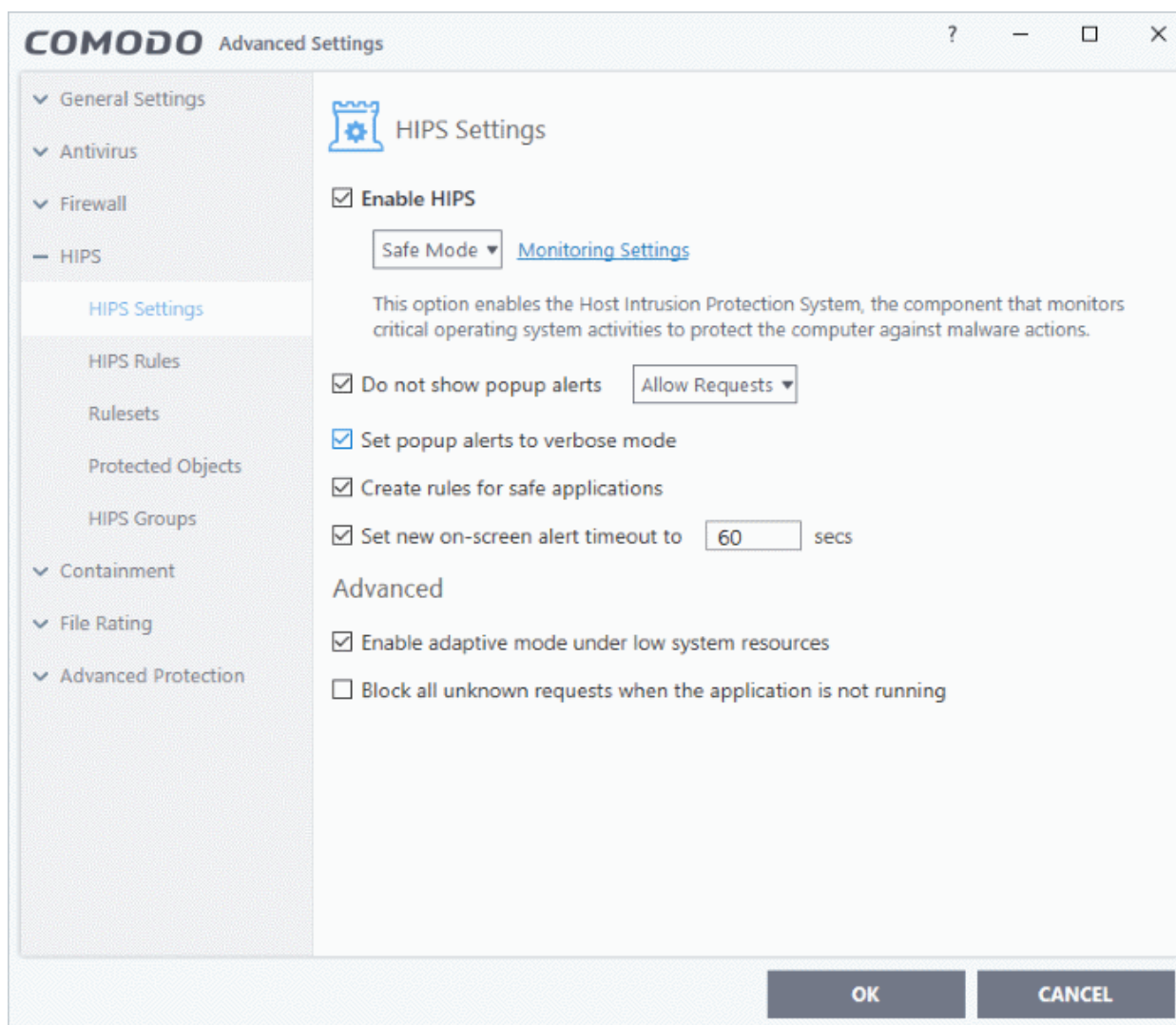
- Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data, steal your identity, corrupt system files, hand control of your PC to a hacker and more. You may also have heard these referred to as Trojans, scripts and worms.

6.4.1. HIPS Settings

The HIPS settings panel allows you to enable/disable HIPS, set HIPS security level and configure HIPS' general behavior.

To open the HIPS Settings panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Settings' on the left:

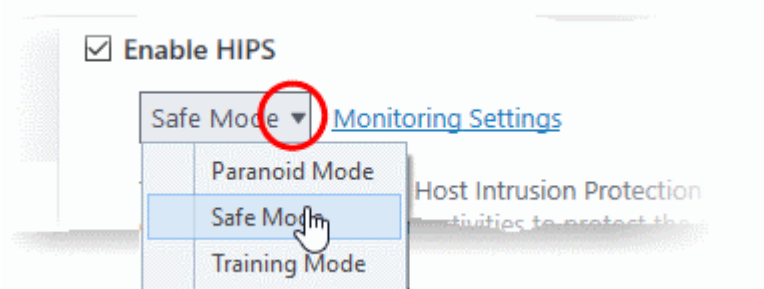


- **Enable HIPS** - Allows you to enable or disable HIPS protection. **(Default=Disabled)**

If enabled, you can configure the HIPS security level and monitoring settings:

Configuring HIPS Security Level

The security level can be chosen from the drop-down under the 'Enable HIPS' check-box:



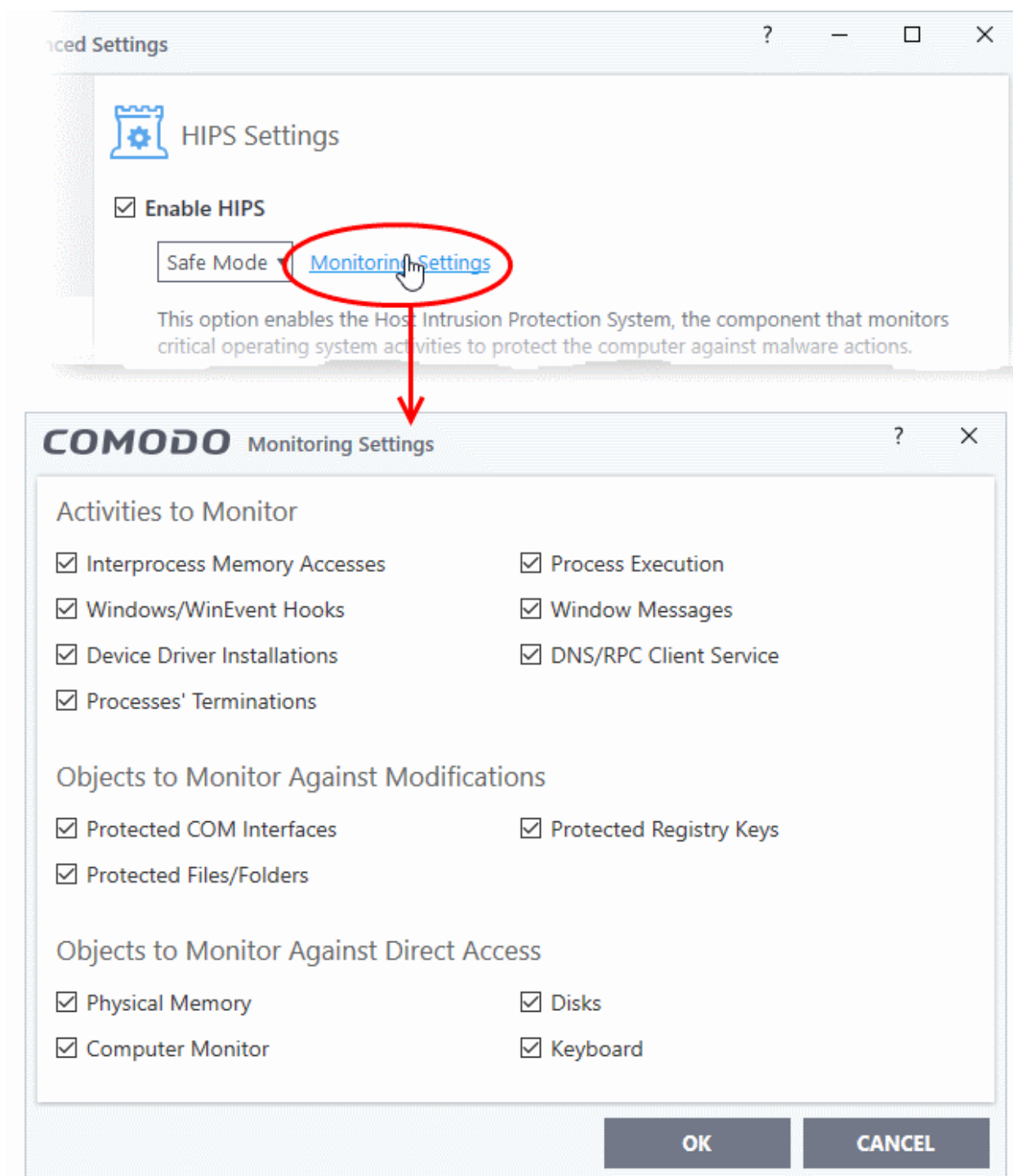
The choices available are:

- **Paranoid Mode:** This is the highest security level setting and means that HIPS monitors and controls all executable files apart from those that you have deemed safe. Comodo Client 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, CCS does not automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their system.
- **Safe Mode:** While monitoring critical system activity, HIPS automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules for these activities, if the checkbox '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the HIPS rules list by choosing 'Treat as' and selecting 'Allowed Application' at the alert with 'Remember my answer' checked. This instructs the HIPS not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Training Mode:** HIPS monitors and learns the activity of any and all executables and creates automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

Configuring Monitoring Settings

The activities 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 or object here, it completely switches off monitoring of that activity on a **global** basis - effectively creating a universal 'Allow' rule for the activity. This 'Allow' setting **over-rules** any specific 'Block' or 'Ask' setting for the activity that you may have created in the '**Access Rights**' and '**Protection Settings**' interfaces.



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 Open VPN GUI process is called 'openvpn.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 Client 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 Client 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

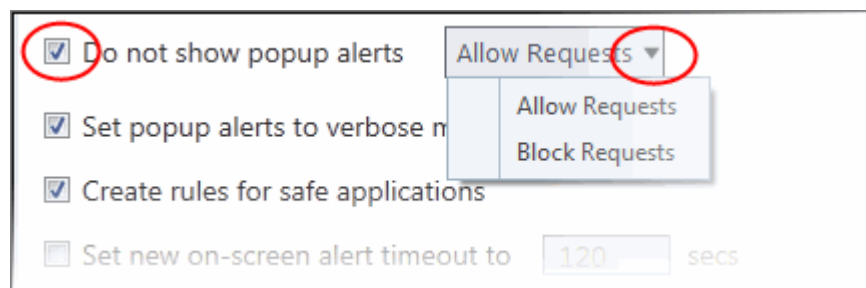
infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:

- **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 Client 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 Client 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 CCS should automatically take - either 'Block Requests' or 'Allow Requests'.



- **Set popup alerts to verbose mode** - Enabling this option instructs CCS to display HIPS alerts in verbose mode, providing more informative alerts and more options for the user to allow or block the requests (**Default = Disabled**).
- **Create rules for safe applications** - Automatically creates rules for safe applications in HIPS Ruleset (**Default = Disabled**).

Note: HIPS trusts the applications if:

- The application/file is rated as 'Trusted' in the **File List**
- The application is from a vendor included in the **Trusted Software Vendors** list
- The application is included in the extensive and constantly updated Comodo safelist.

By default, CCS 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 CCS 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 , CCS 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 CCS 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.

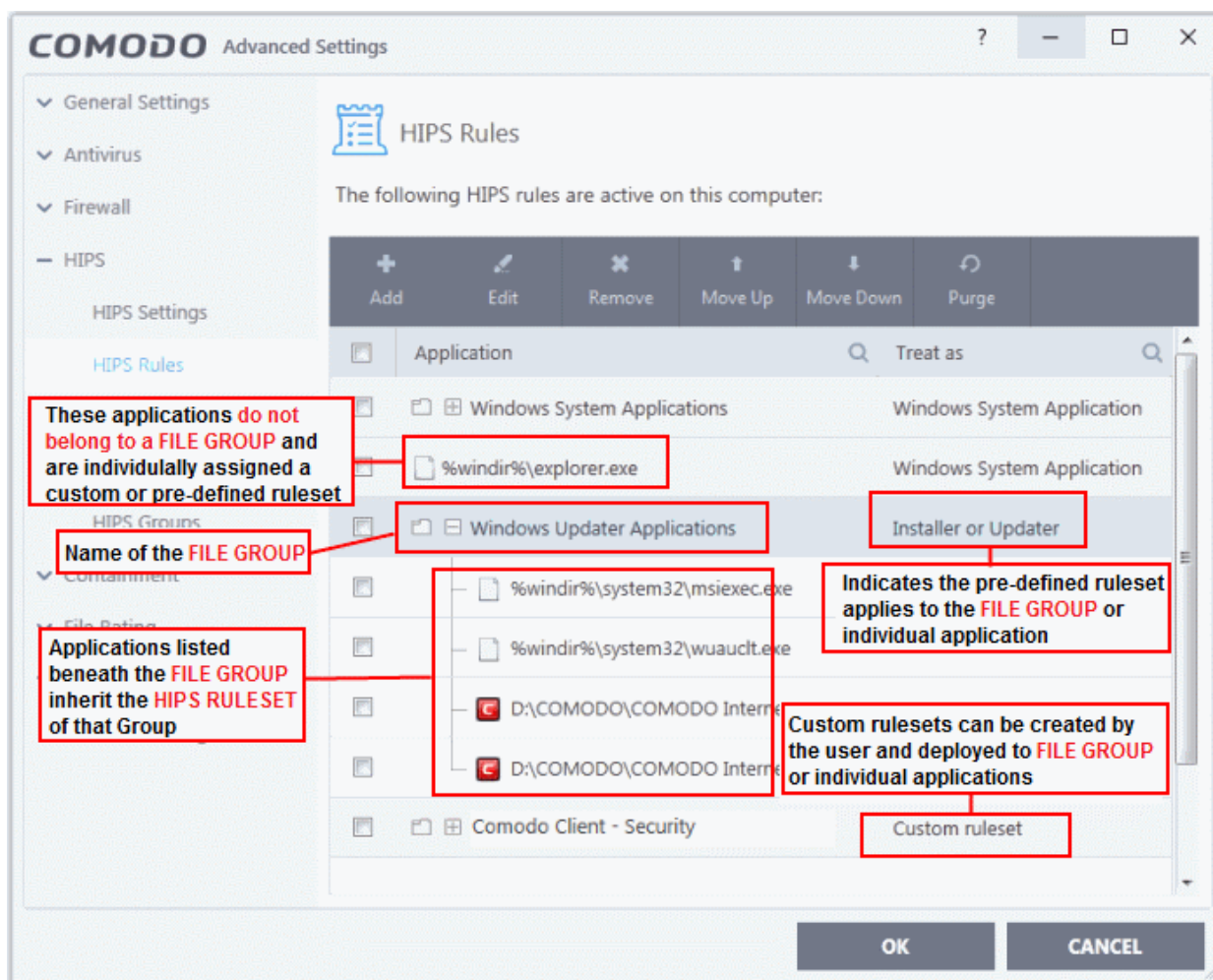
- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CCS functions to fail. With this option enabled, CCS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems (**Default = Disabled**).
- **Block all unknown requests if the application is not running** - Selecting this option blocks all unknown execution requests if Comodo Client 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 CCS security settings then it is OK to leave this box unchecked. (**Default = Disabled**)

6.4.2. Active HIPS Rules

- The 'HIPS Rules' screen shows your installed applications classified into file groups, and the HIPS rulesets which apply 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

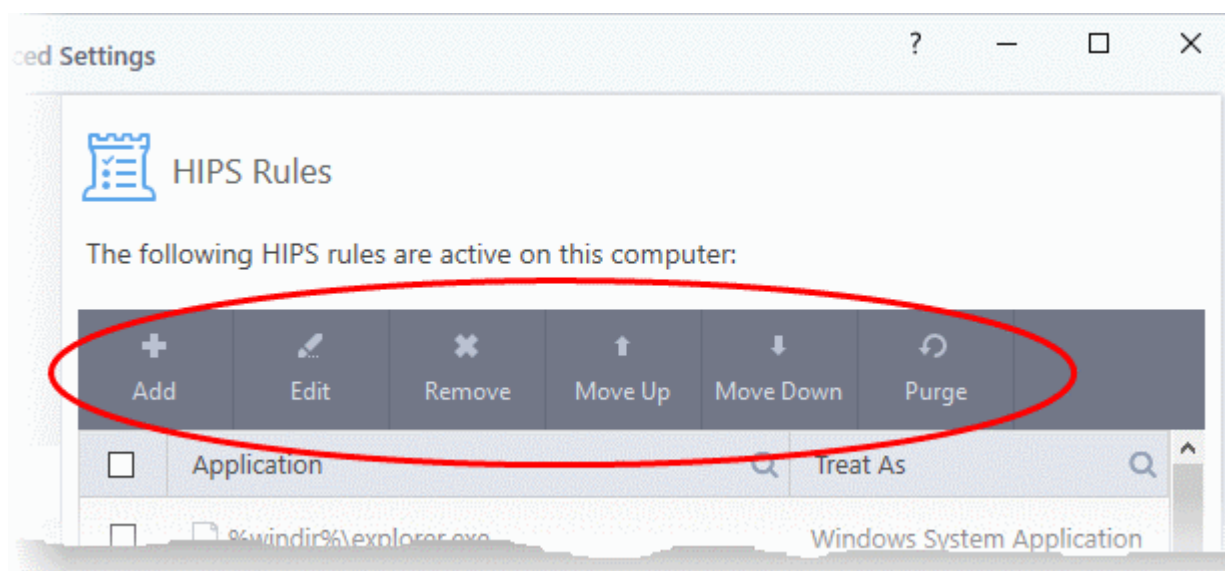
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Rules' on the left:



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 the section '**Creating or Modifying a HIPS Ruleset**'.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **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

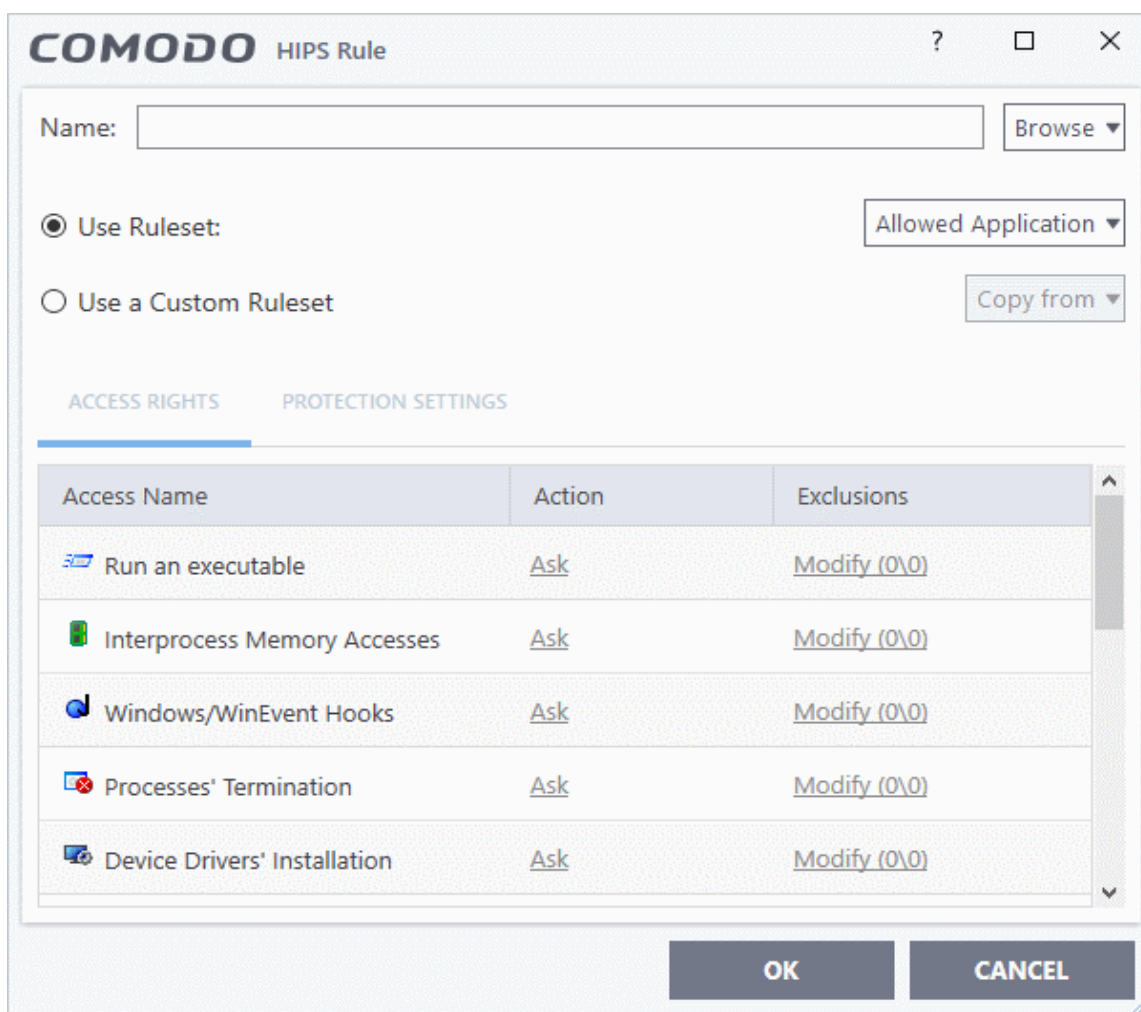
Defining a HIPS Ruleset for an application or File group involves two steps:

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.

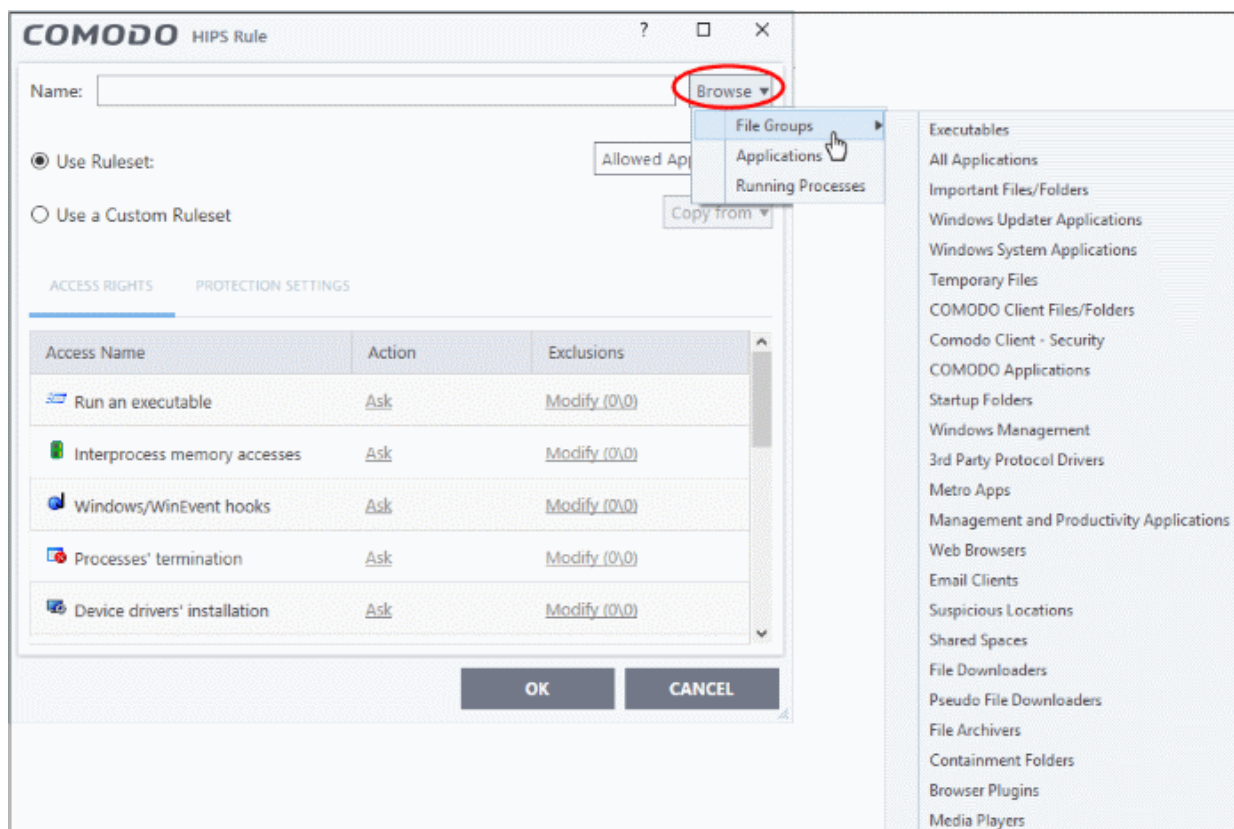


The 'Name' box is blank because you are defining a HIPS rule settings for a new application. If you were editing an existing rule, this field would show the application name and its installation path, or the application group name.

- Click 'Browse' to begin.

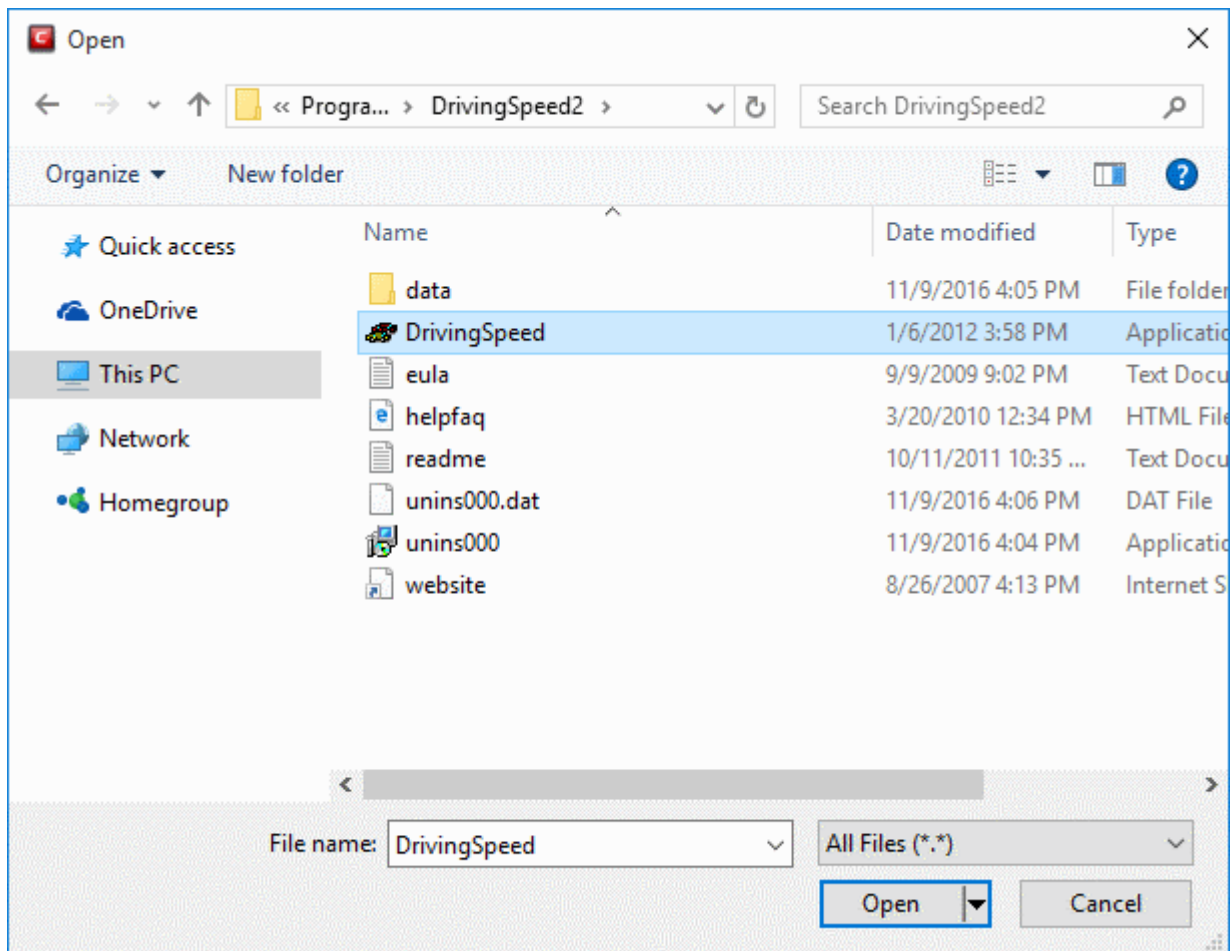
You now have 3 methods available to choose the application for which you wish to create a Ruleset - **File Groups**; **Applications** and **Running Processes**.

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.

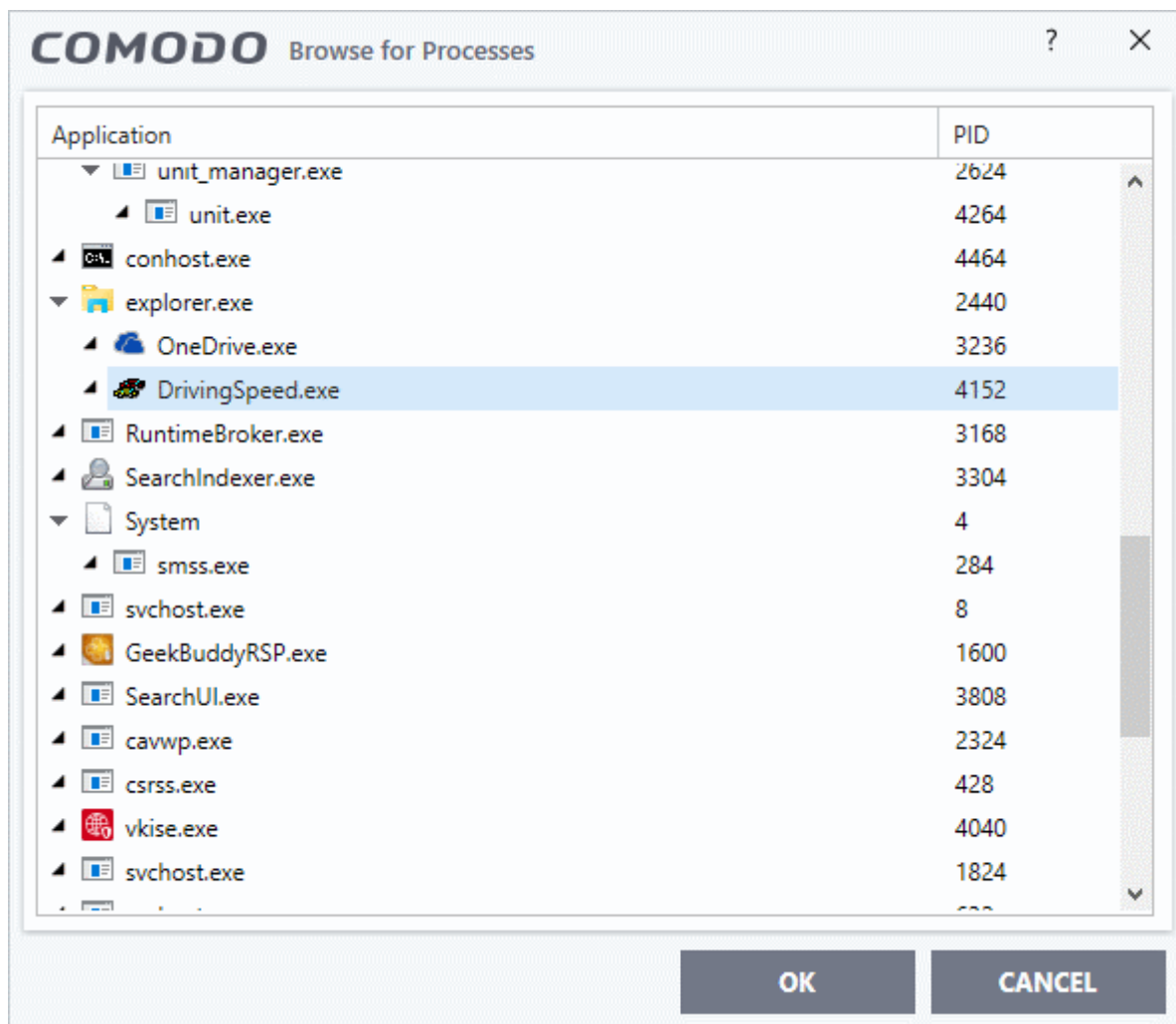


To view the file types and folders that are affected by choosing one of these options, you need to visit the **'File Groups'** interface.

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.

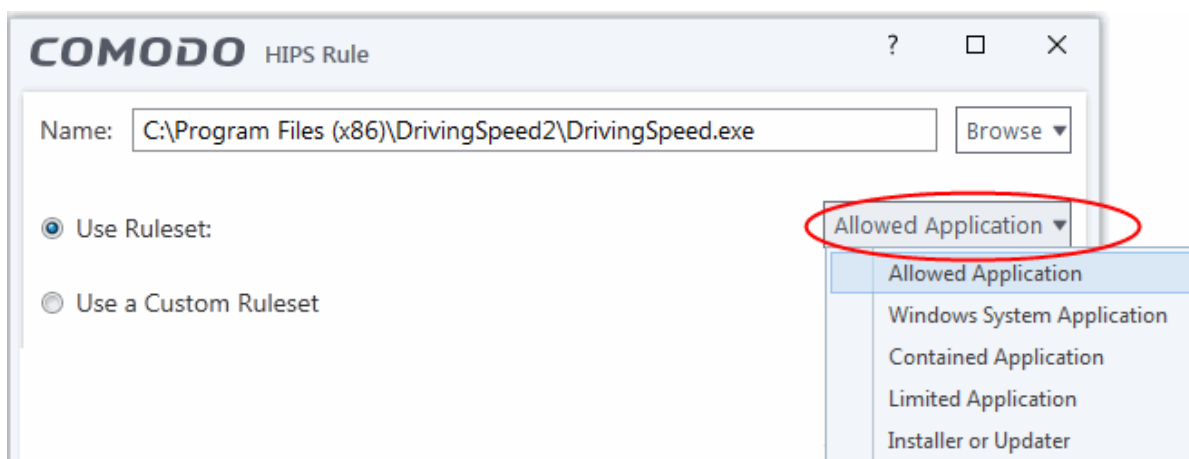


Having selected the individual application, running process or file group, the next stage is to configure the rules for this ruleset.

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.

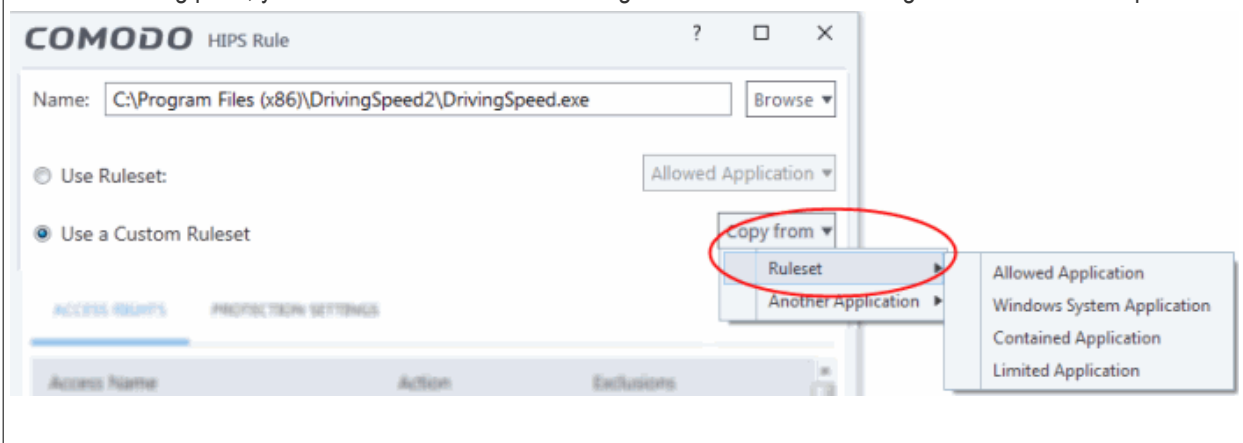
General Note: Predefined Rulesets cannot be modified directly from this interface - they can only be modified and defined using the '**Rulesets**' interface. If you require the ability to add or modify settings for a specific application then you are effectively creating a new, custom ruleset and should 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.

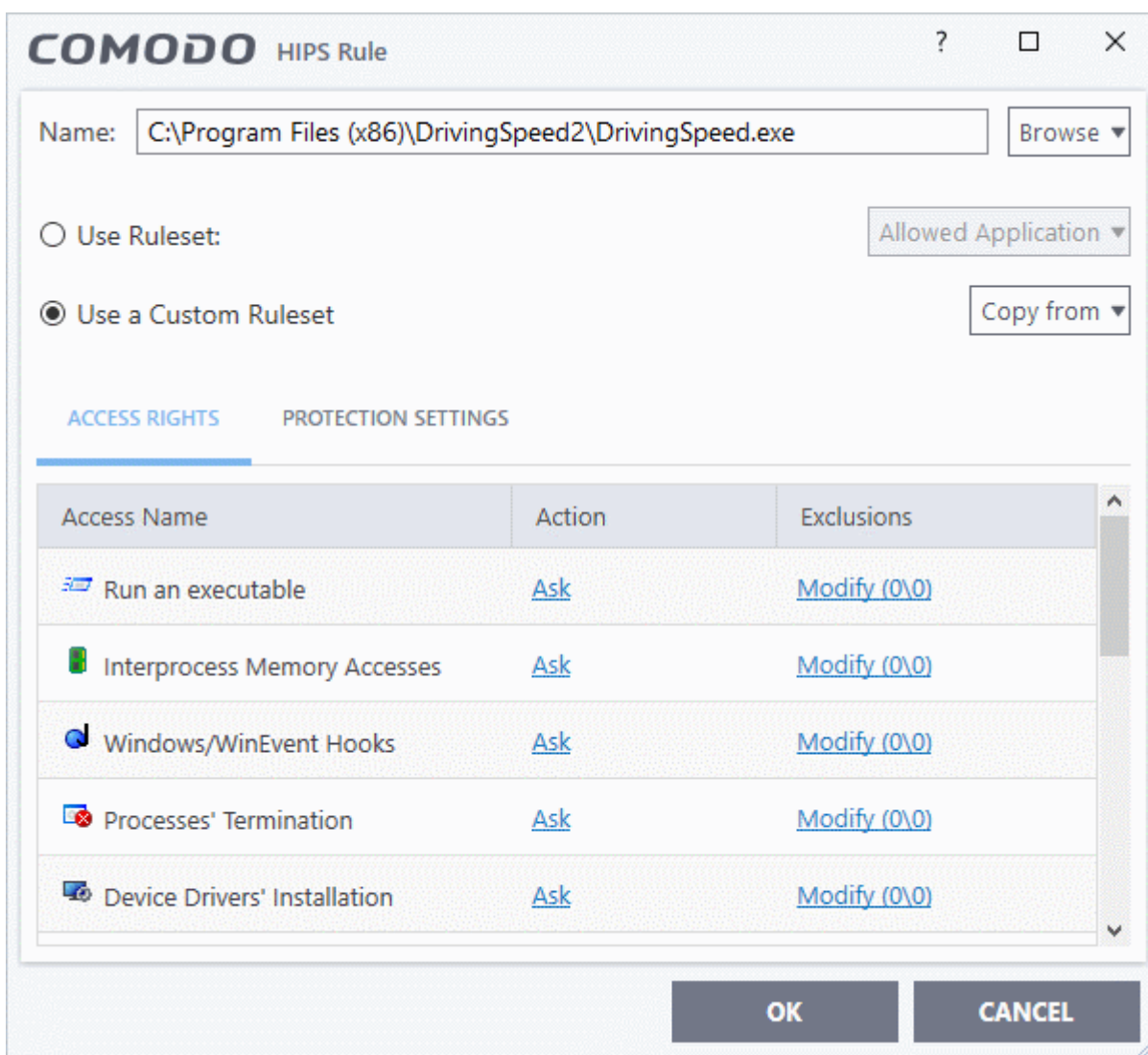
The custom ruleset has two main configuration areas - **Access Rights** and **Protection Settings**.

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.

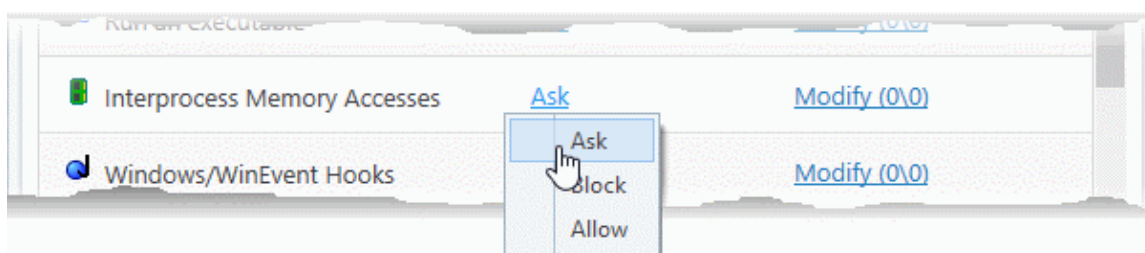
Tip: You can use the 'Copy from' drop-down to choose an existing rule set for an application or file group. Using that as a starting point, you can customize the 'Access Rights' and 'Protection Settings' for the rules as required.



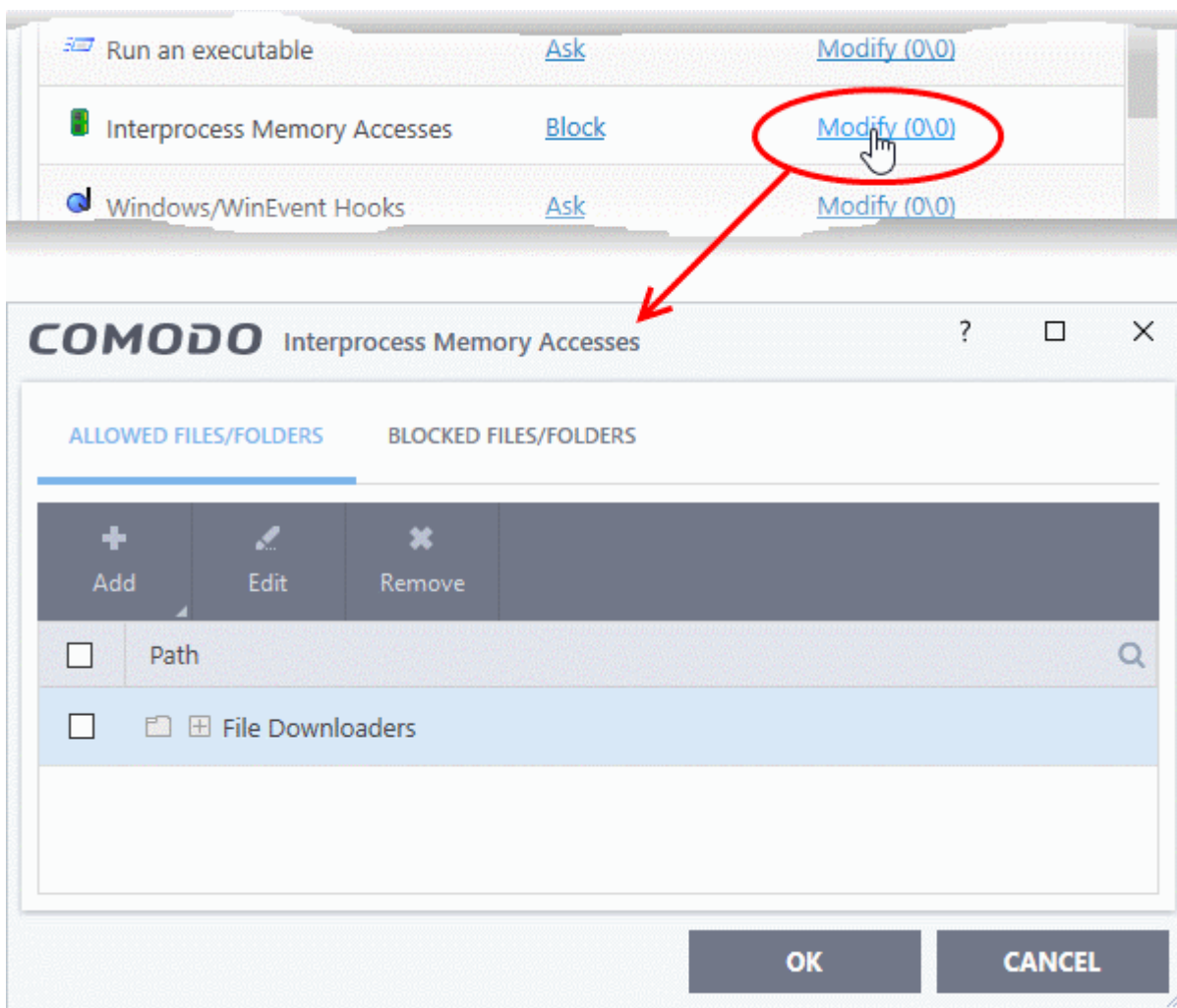
- i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset. These activities are called 'Access Names'.



See **HIPS Settings > Activities to Monitor** to see definitions of the 'Action Names' listed above, and the implications of choosing 'Ask', 'Allow' or 'Block':



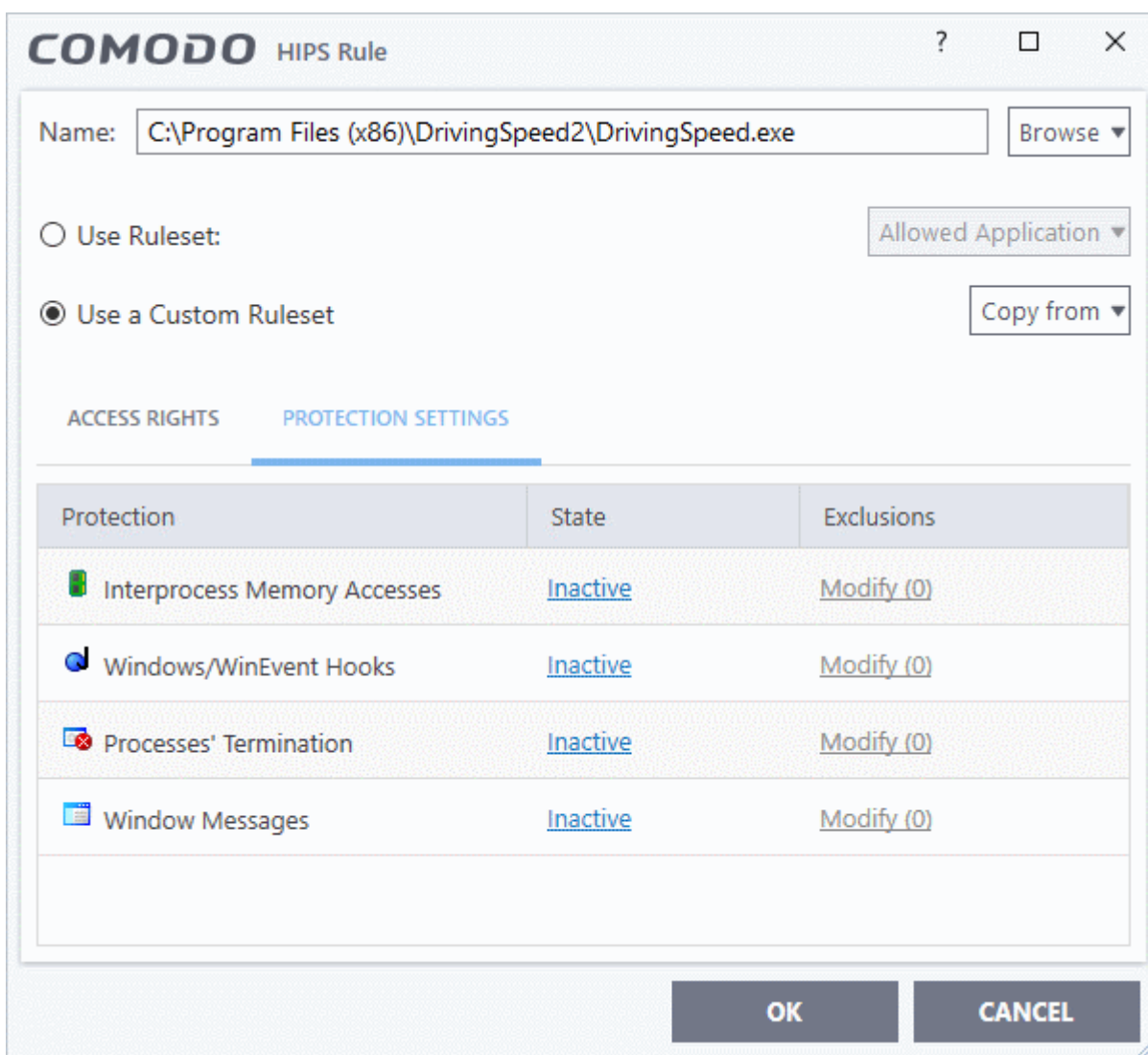
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.



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

- A ruleset is a collection of **access rights and protection settings** that can be deployed to control applications or application groups.
- Each ruleset consists of a number of rules, and each of these rules is defined by a set of conditions and parameters. Rulesets govern an application's rights to access memory, other programs, the registry etc.

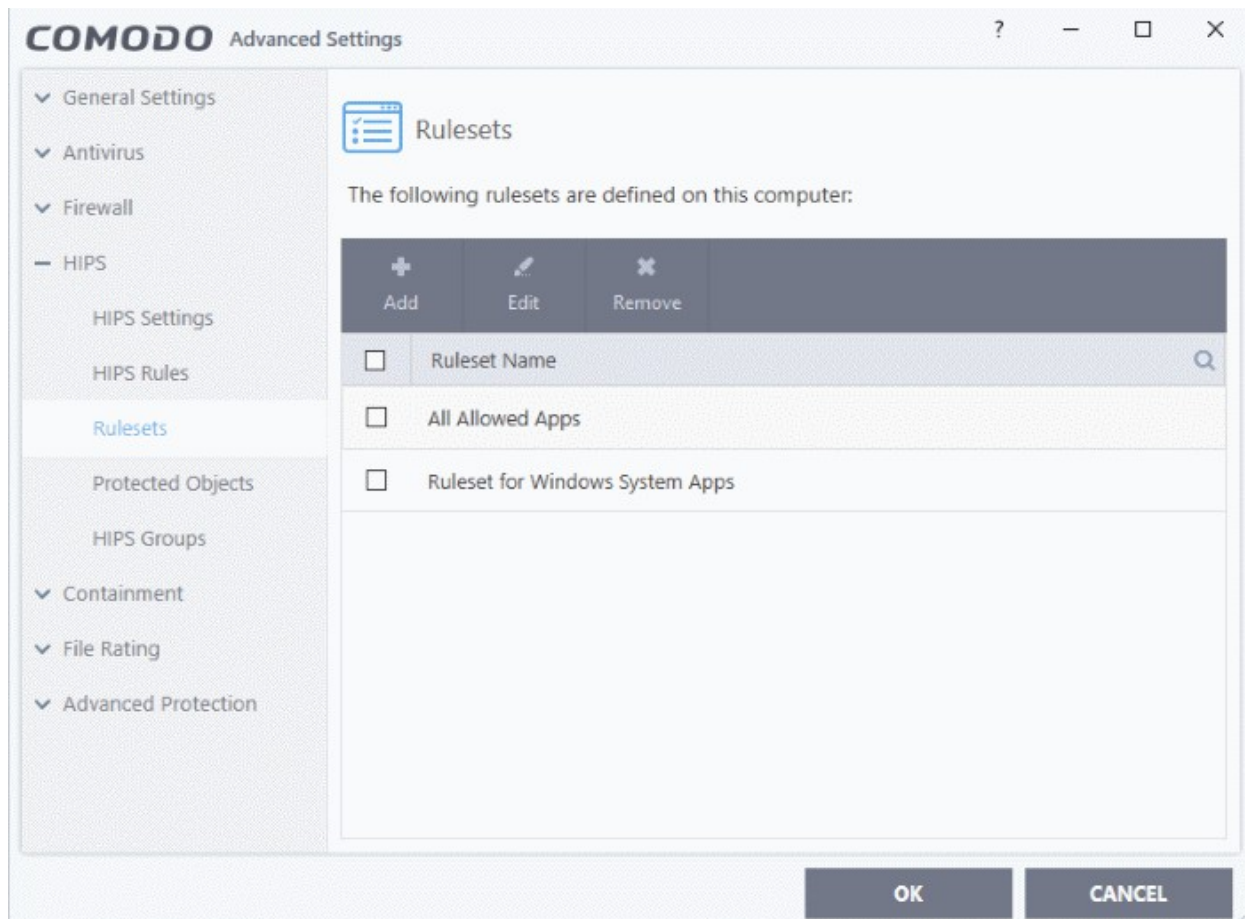
Note: This section is for advanced users. If you are new CCS user, we advise you first read the **Active HIPS Rules** section in this help guide.

- Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice would prove time consuming if it had to be performed for every single program on your system.

- For this reason, Comodo Client Security contains a selection of pre-defined rulesets which implement optimal security settings for a range of application types. Users can, of course, modify these predefined rulesets to suit their requirements.

To view the list of HIPS Rulesets

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'Rulesets' on the left:



You can search for a specific ruleset by clicking the search icon and typing the rulesets name in full or part.

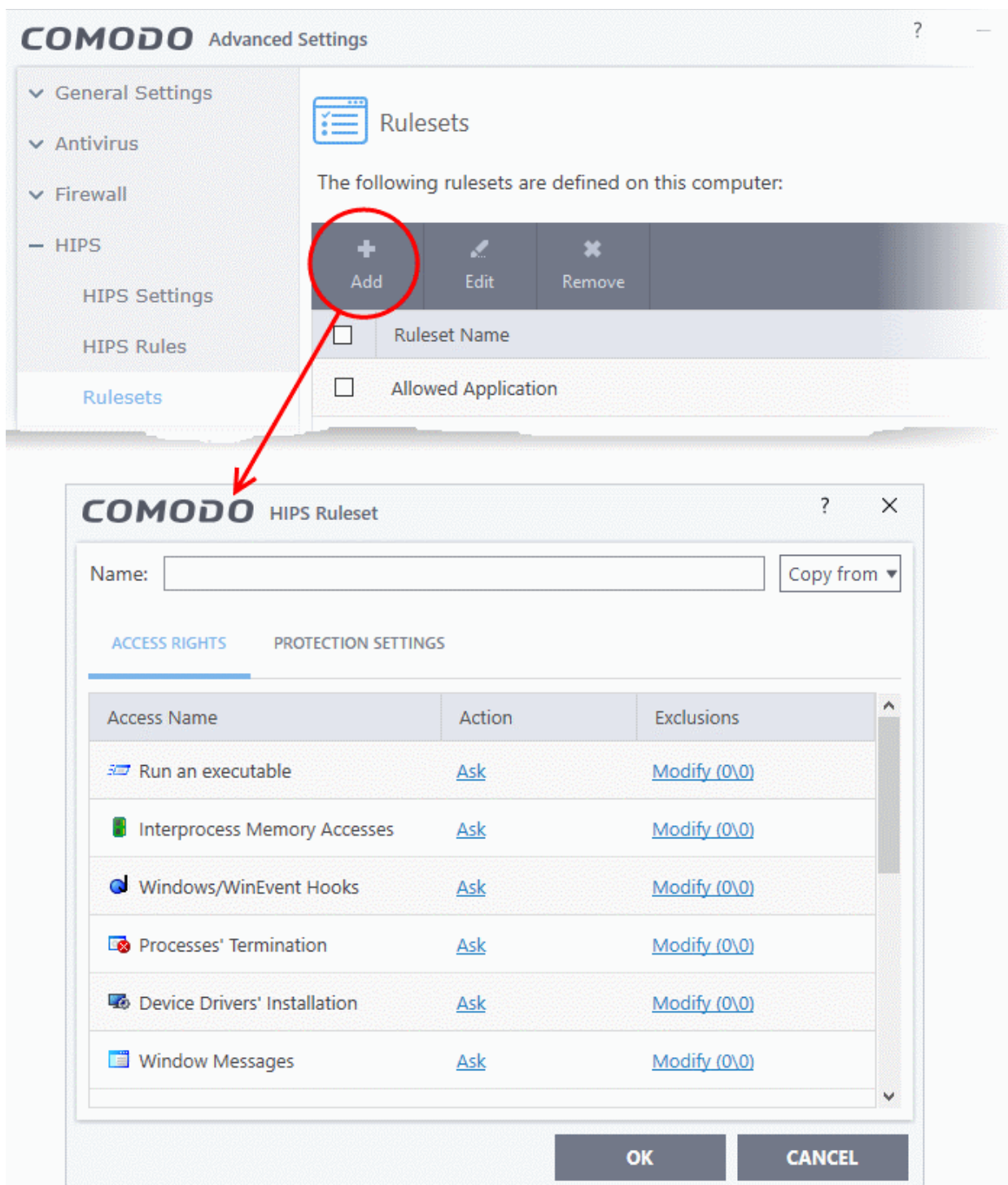
To view or edit a ruleset

- Double click on the 'Ruleset' in the list
- or
- Select the 'Ruleset' and click the 'Edit' button at the top of the interface

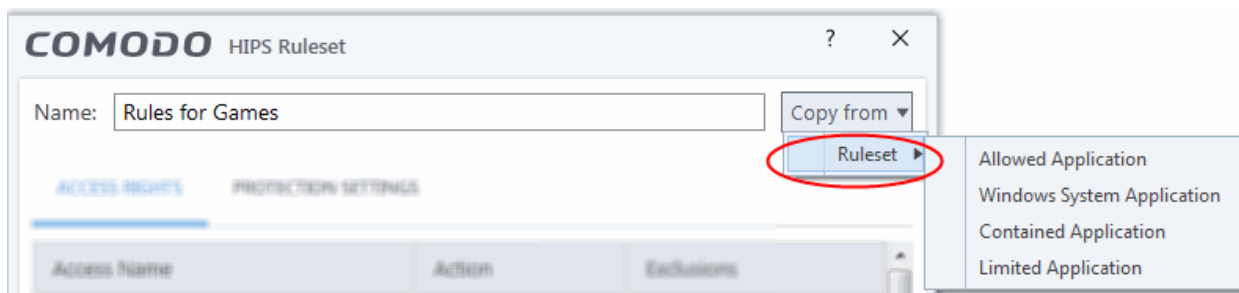
From here, you can make changes to its **'Access Rights'** and **'Protection Settings'**. Any changes you make here are automatically rolled out to all applications that are covered by the ruleset.

To create a new ruleset

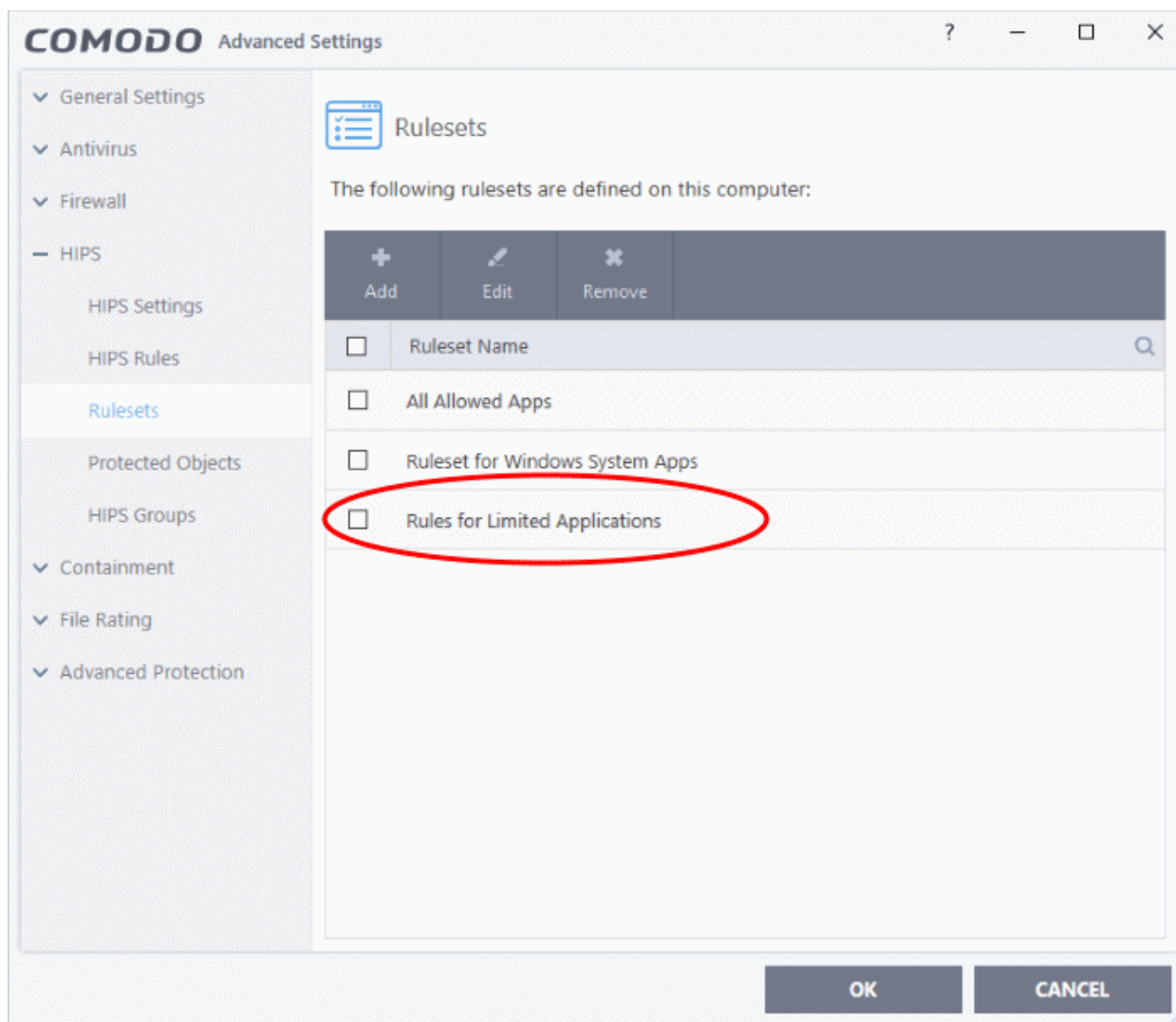
- Click the 'Add' button at the top of the interface



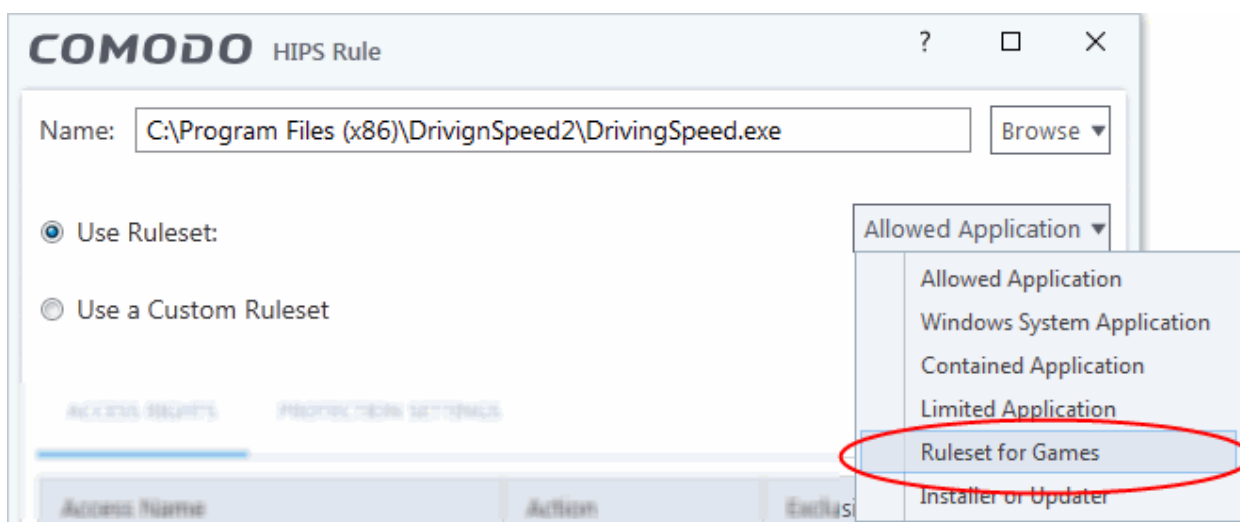
- Enter a name for the new ruleset.
- To copy the **Access Rights** and **Protection Settings** from an existing ruleset, click 'Copy From' and choose the ruleset from the drop-down.



- 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.

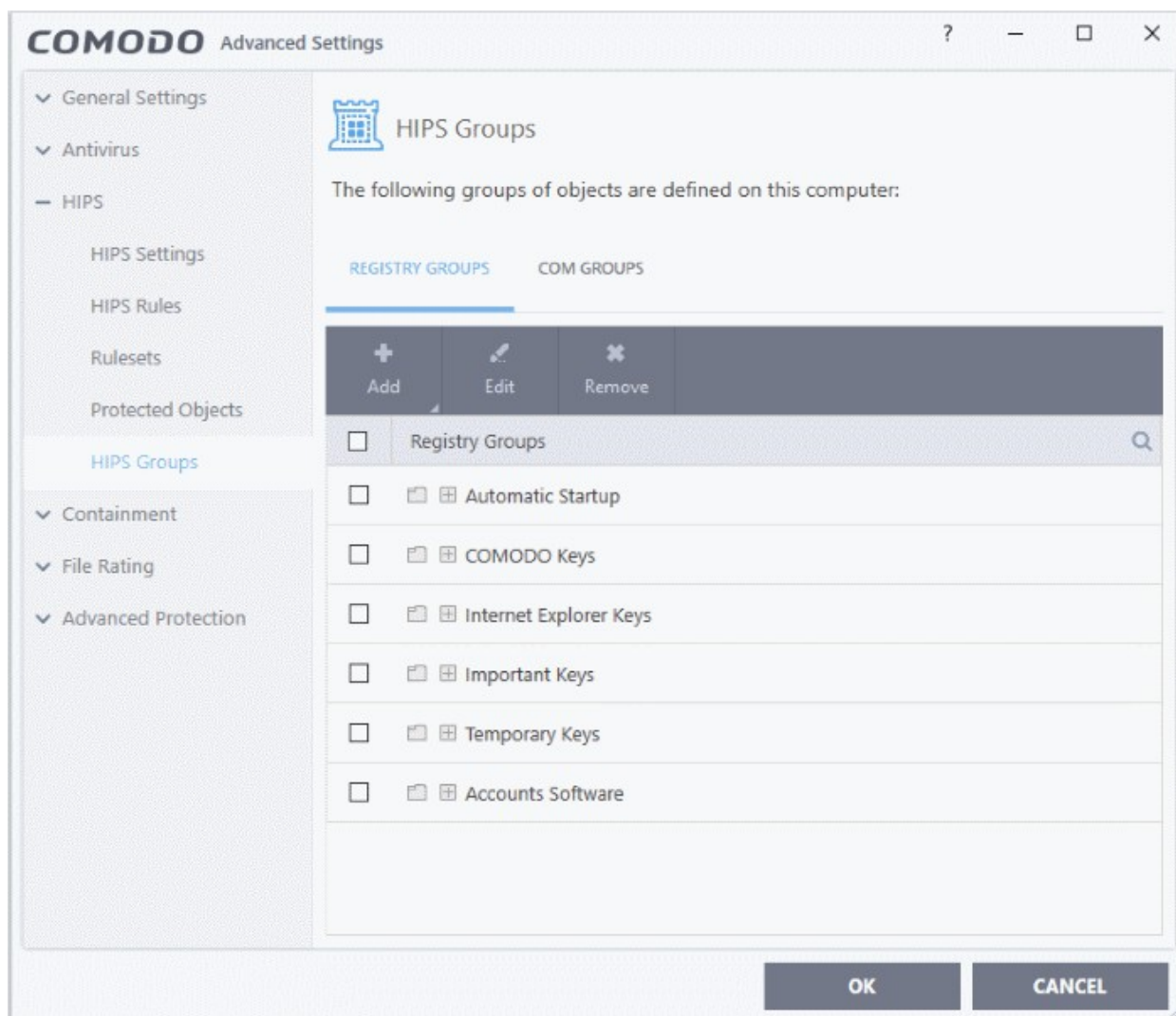


6.4.4. HIPS Groups

- 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**.
- CCS 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' on the CCS 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. You need to select the group in the **Protected Objects** interface to actually apply the protections.

The panel has two sections:

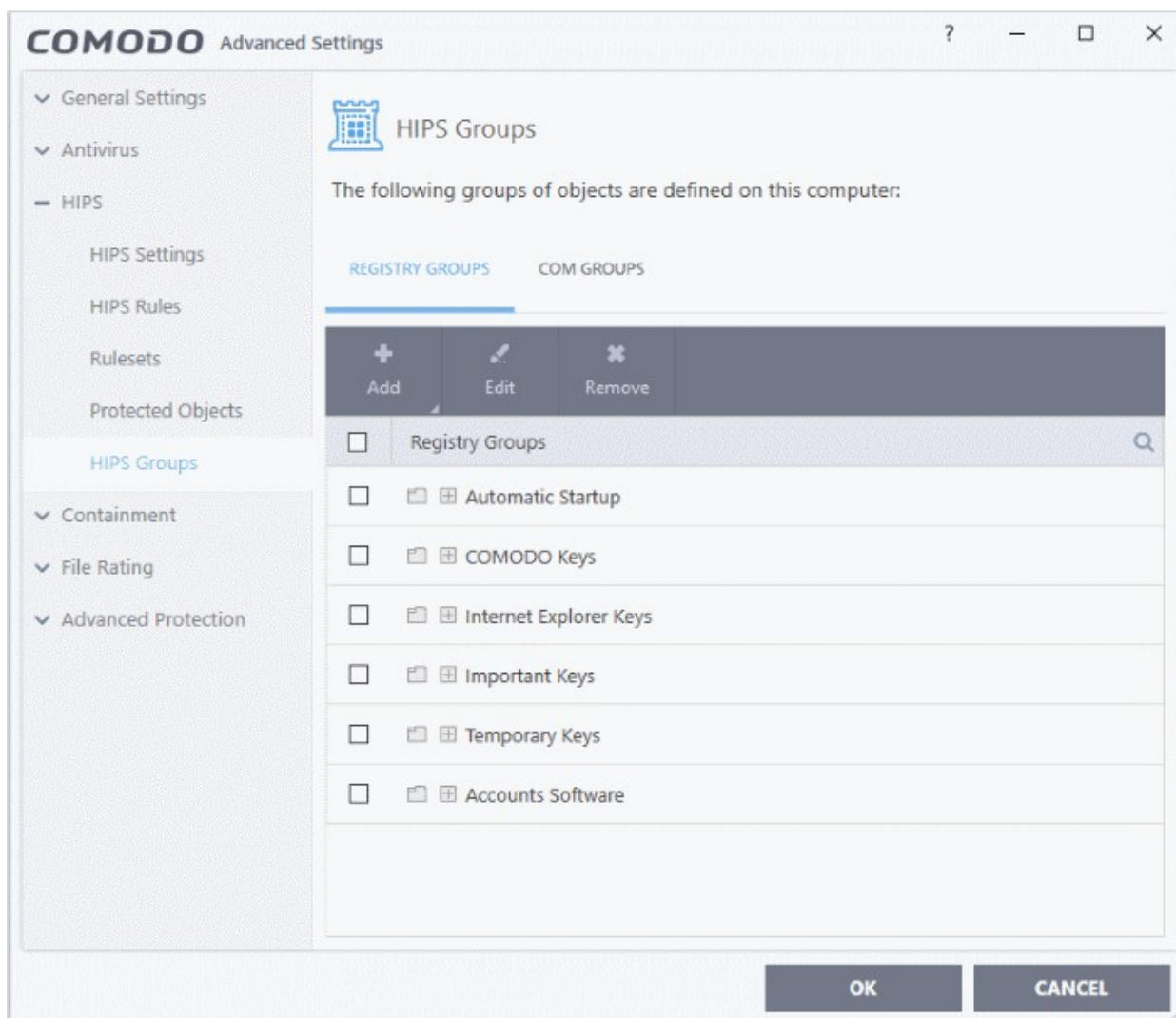
- **Registry Groups** - View, edit and create groups of registry keys which you want to protect from changes.
- **COM Groups** - View, edit and create groups of COM interfaces which you want to protect from changes.

6.4.4.1. Registry Groups

- Registry groups are predefined batches of one or more registry keys.
- Comodo Client Security ships with a set of important registry groups: 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.
- Creating a registry group allows you to quickly add it to the list of protected keys. See '**Protected Registry Keys**' for help with this.

To open the 'Registry Groups' section

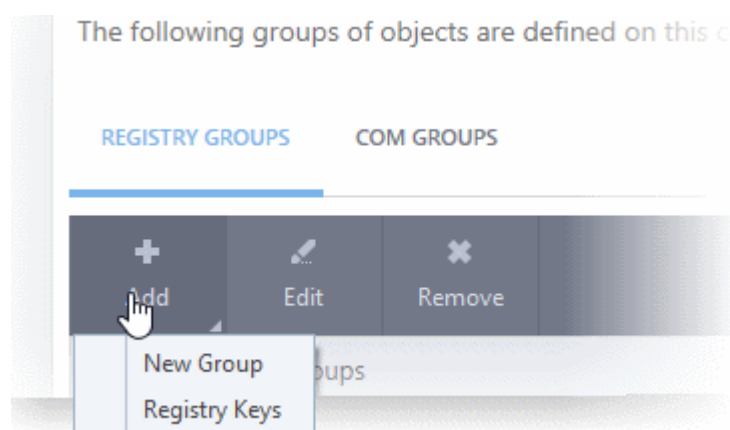
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left.
- Click the 'Registry Groups' tab:



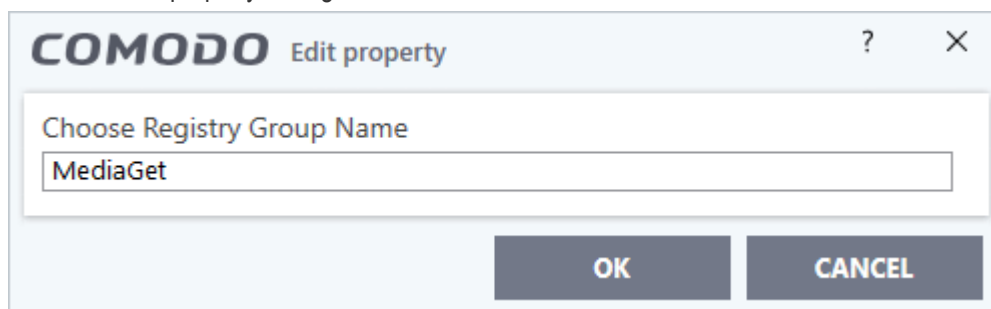
- Click the search icon on the right to find a specific item. You can enter a full or partial name.

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

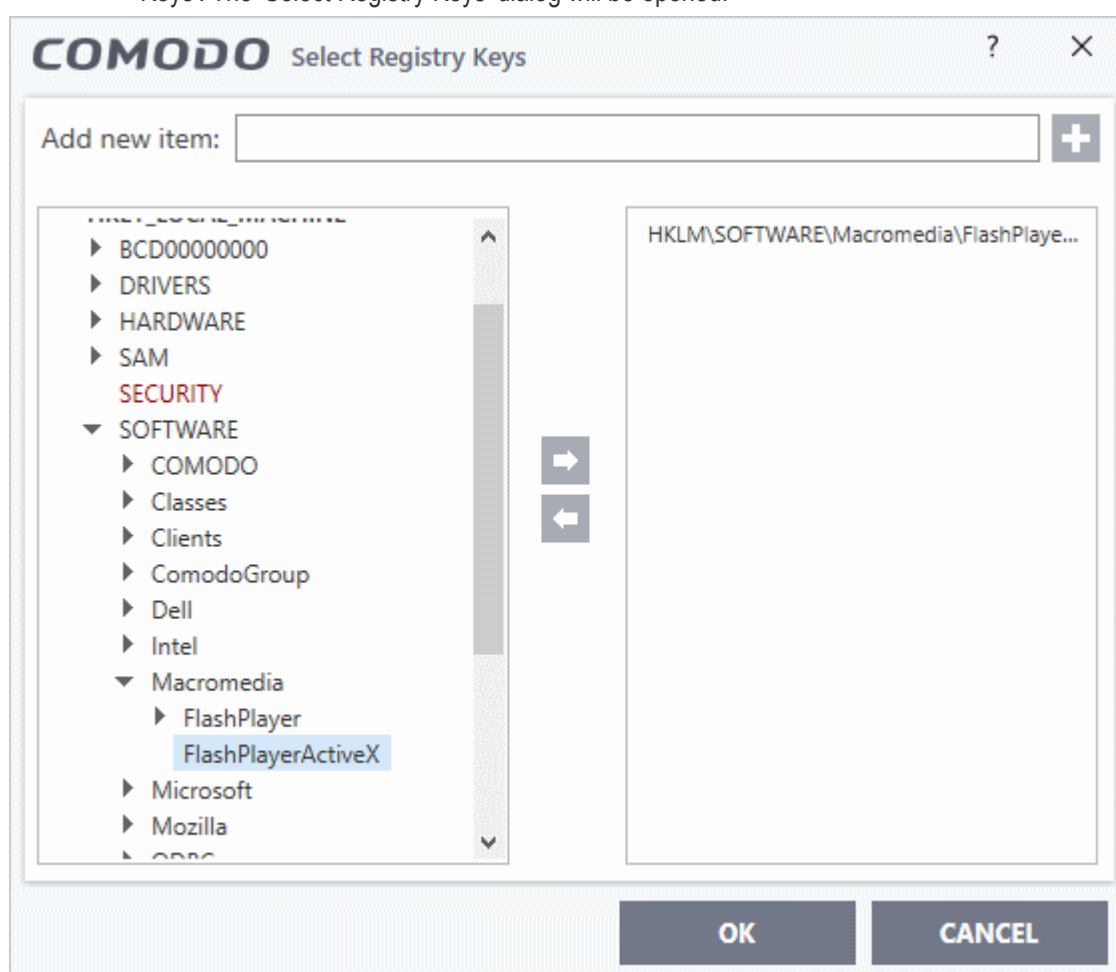


- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.

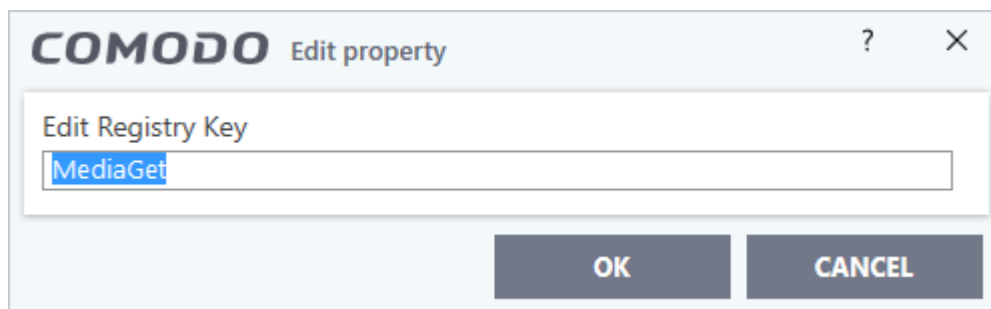


The group will be added to the list.

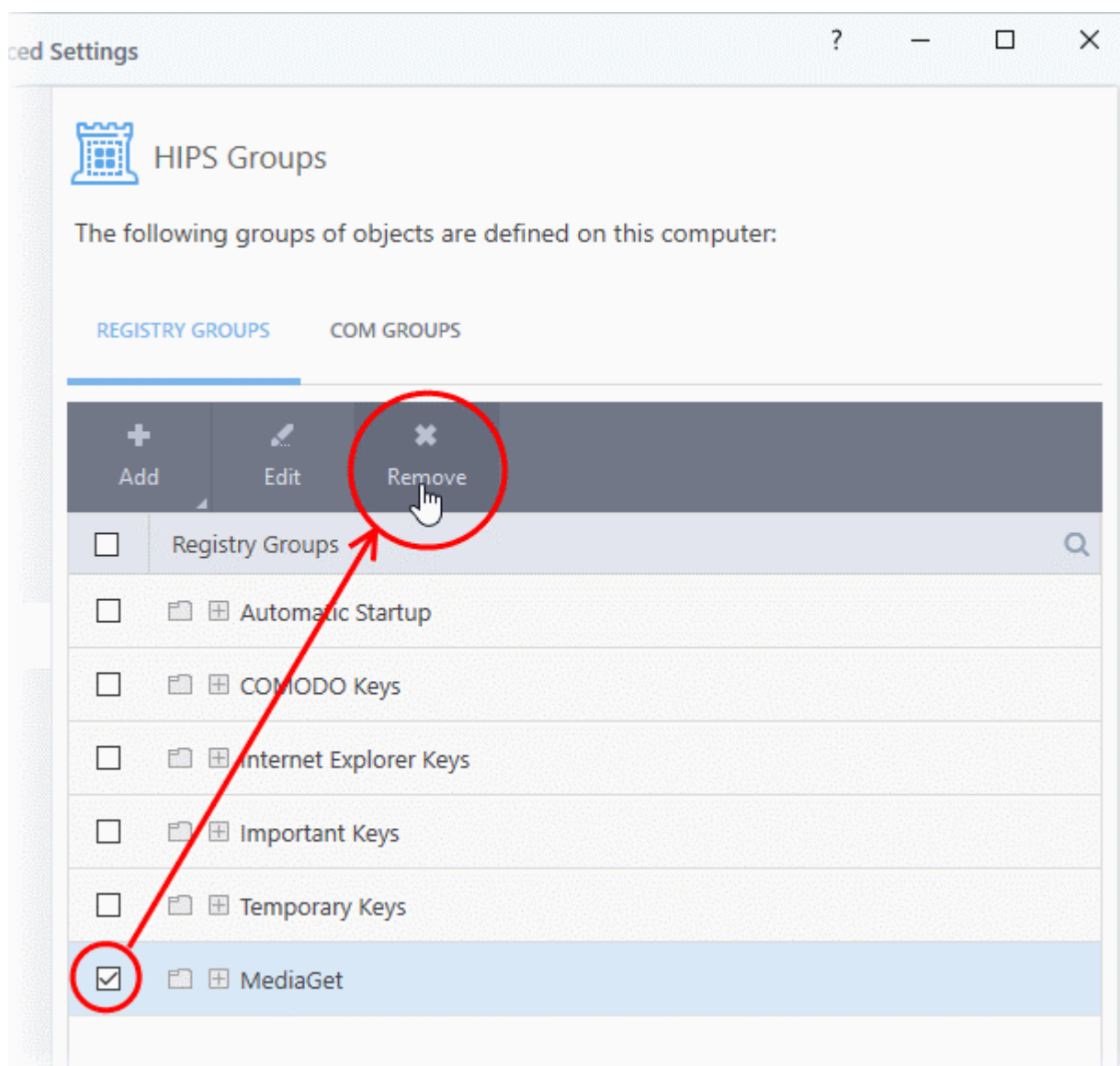
- **Add keys to a group** - Select the group from the list, click 'the Add' button and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



- 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.

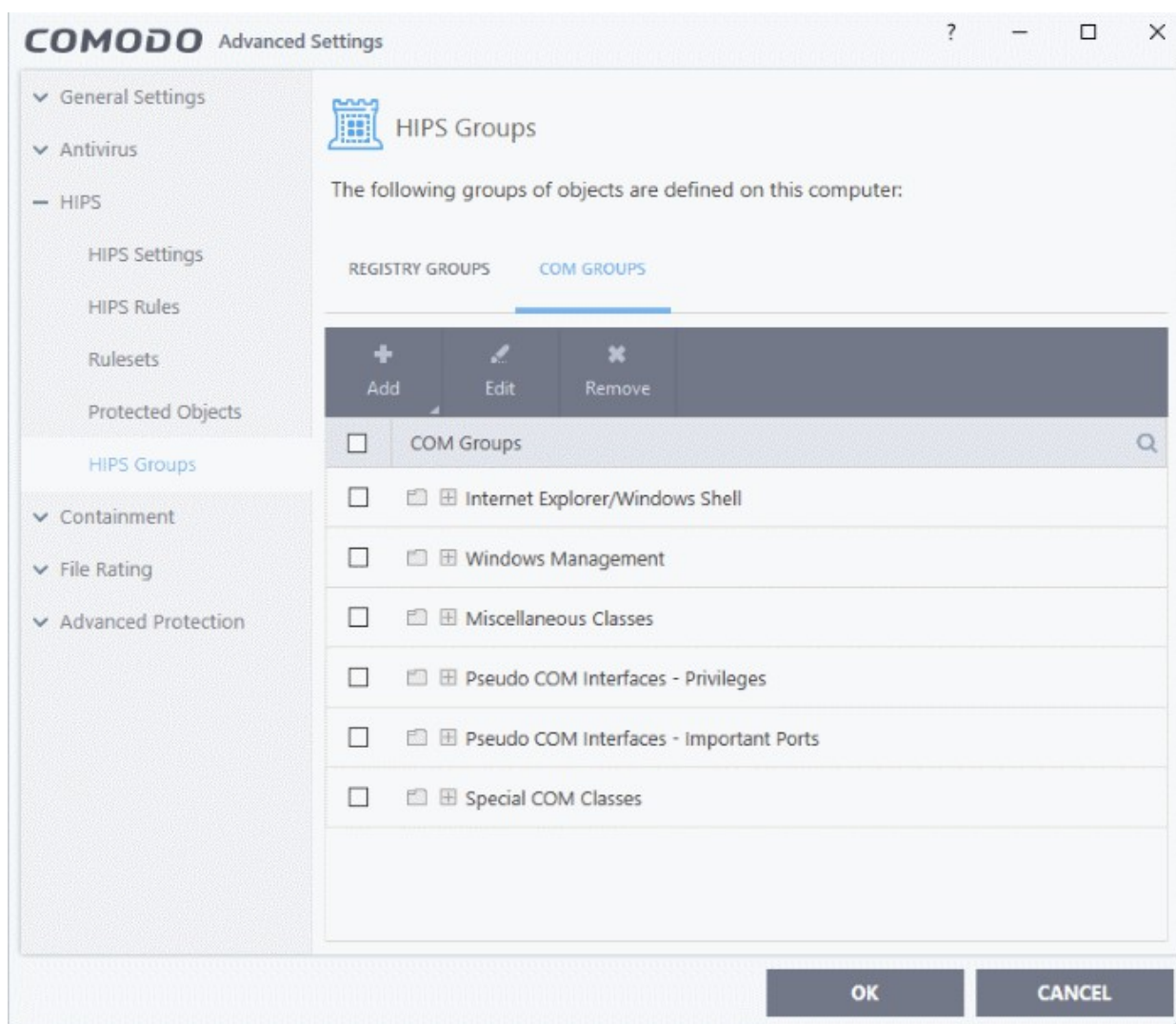
6.4.4.2. COM Groups

- COM groups are predefined groups of COM interfaces. COM interfaces are used by Windows to define how objects interact within a single application or between applications.

- COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks. It is therefore essential that COM interfaces are protected.
- Comodo Client Security ships with the following, important COM groups: 'Internet Explorer/Windows Shell', 'Windows Management', 'Miscellaneous Classes', 'Pseudo COM Interfaces - Privileges' and 'Pseudo COM Interfaces - Important Ports'.
- Creating a COM group allows you to quickly add it to the 'COM' protection list. See '**Protected COM Interfaces**' for more details.

To open the 'COM Groups' section

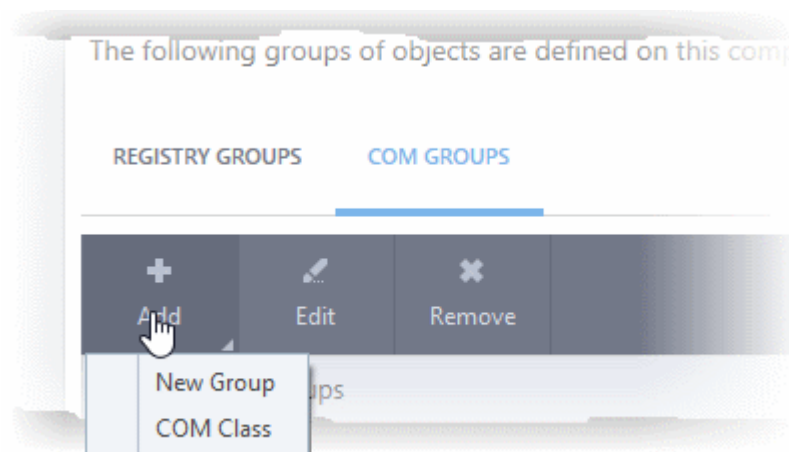
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left.
- Click the 'COM Groups' tab:



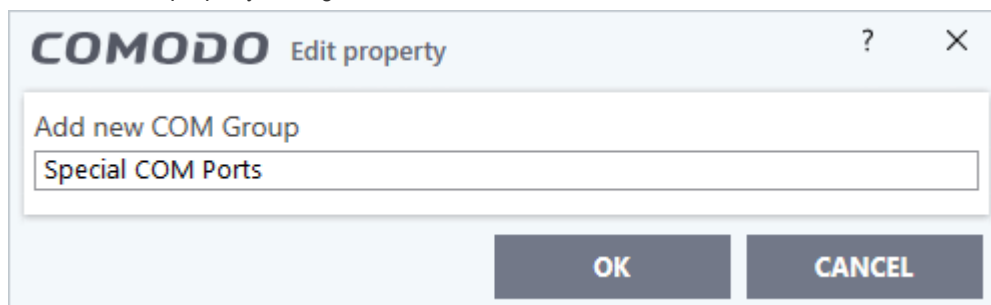
- Click the search icon on the right to find a specific item. You can enter full or partial names.

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

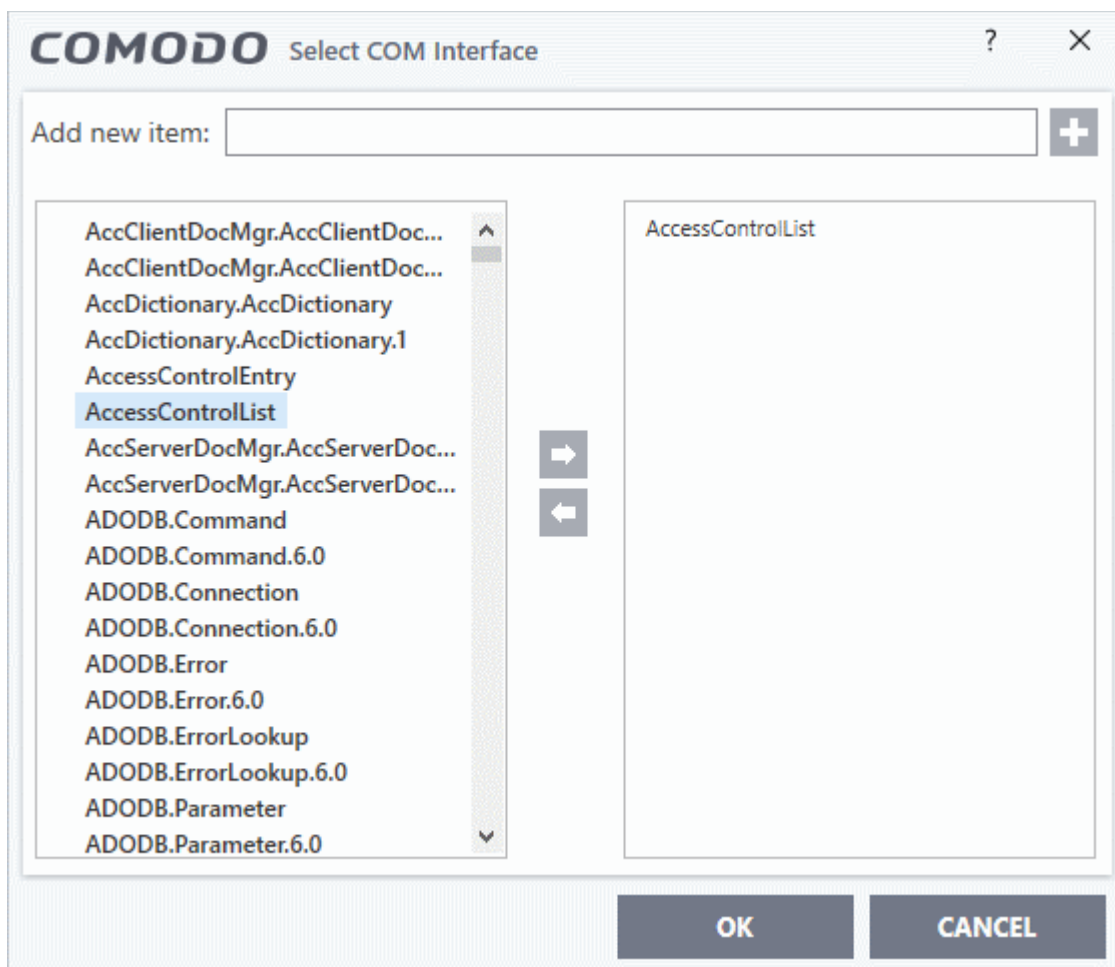


- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.



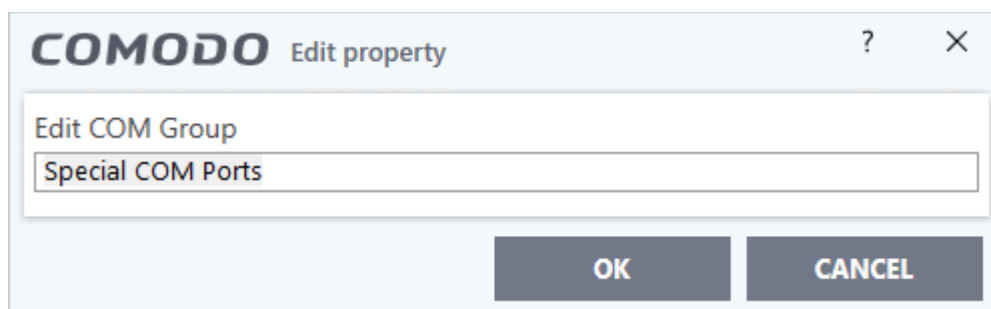
The group will be added to the list.

- **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.

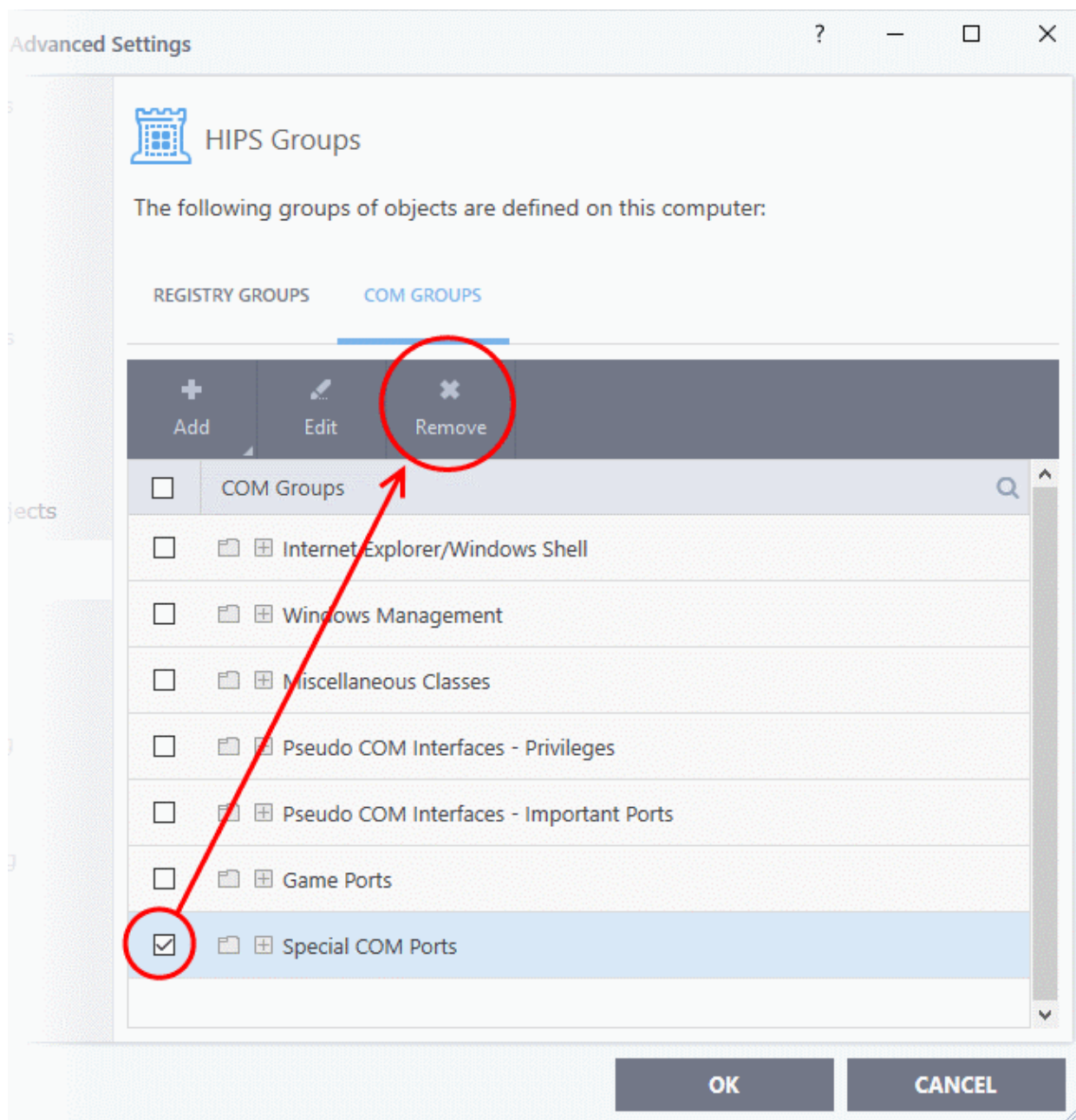


You can add new items by selecting them on the left and clicking the right arrow button. To add items manually, type their name in the 'Add new item' field and press the '+' button.

- 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. Protected Objects

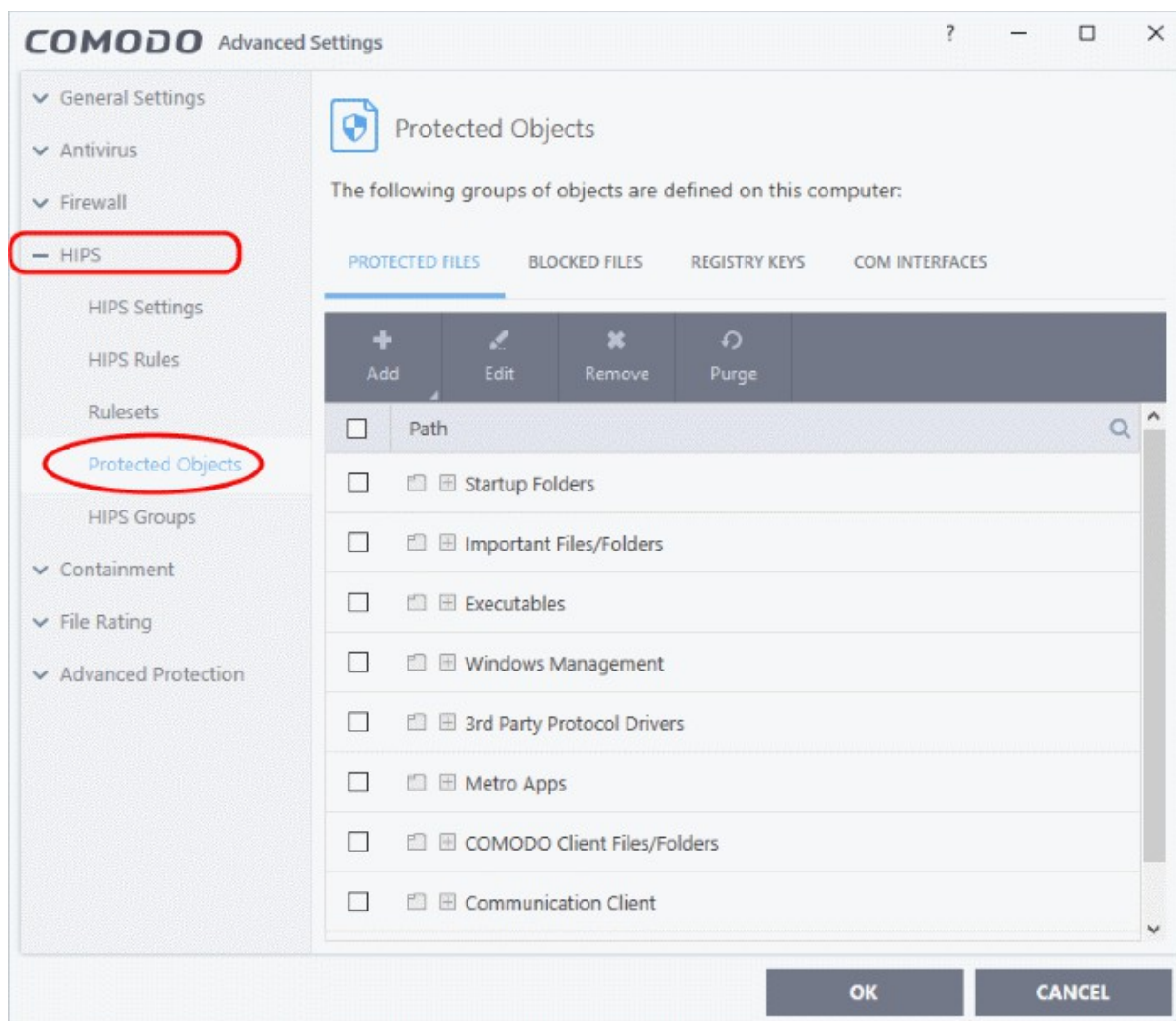
- The protected objects area lets you protect files, folders, registry keys and COM interfaces against access or modification by unauthorized processes.

There are two basic options you can choose:

- **Read access only** - Processes can access but not modify the protected item
 - Click 'Advanced Settings' > 'HIPS' > 'Protected Objects'.
 - See '**Protected Objects – HIPS**' for more help
- **Deny all** – Applications in the container cannot read or modify the protected item
 - Click 'Advanced Settings' > 'Containment' > 'Protected Objects'
 - See 'Protected Objects – Containment' for more help

6.5.1. Protected Objects – HIPS

- This area lets you protect specific files, folders, registry keys and COM interfaces against modification by unauthorized processes.
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'Protected Objects' on the left:



The interface has the following sub-sections:

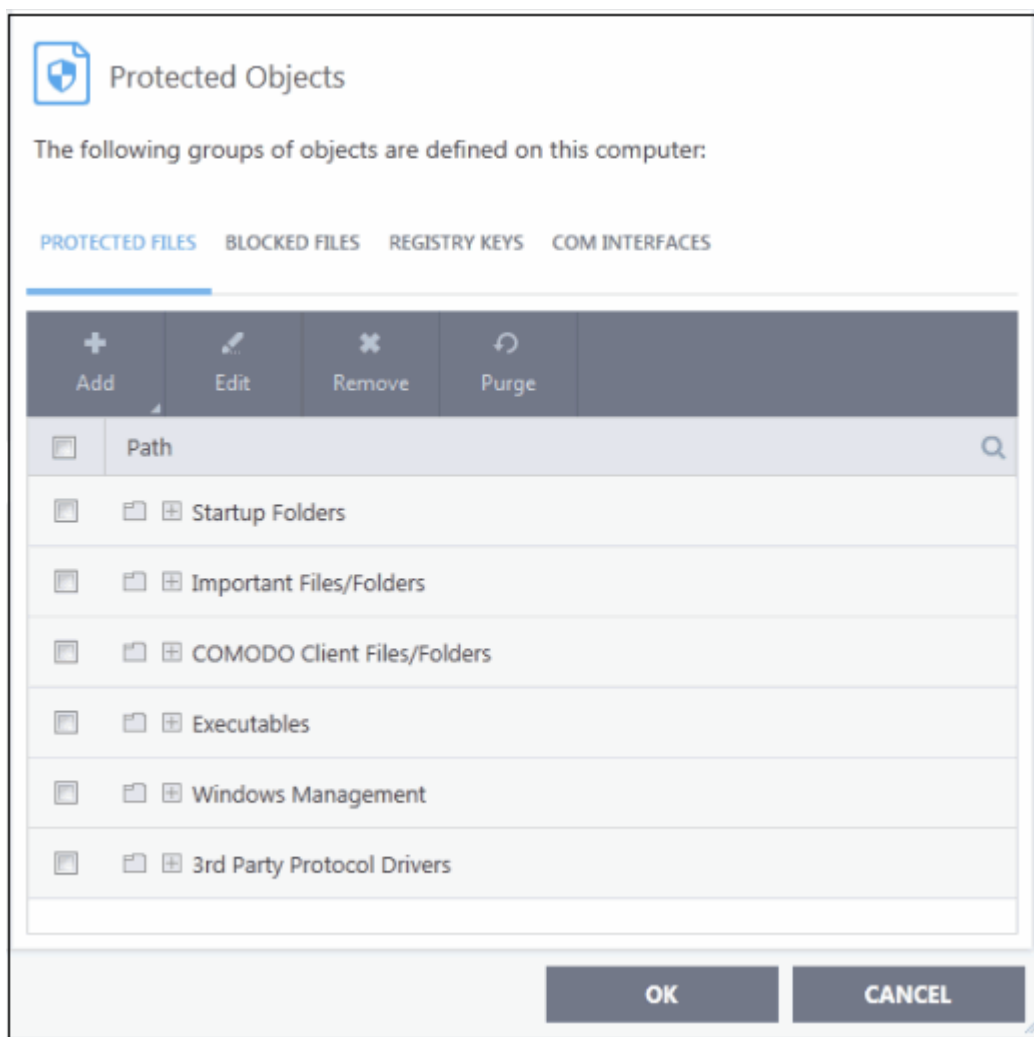
- **Protected Files** – Applications and files which are protected from modification by other processes
- **Blocked Files** - Applications and files that are prevented from running
- **Registry Keys** - Registry keys that are protected from modification by other processes
- **COM Interfaces** - COM interfaces that are protected from modification

6.5.1.1. Protected Files

- The protected files screen shows file groups that are protected from access by other programs.
- Files in this area are 'read only'. They can be accessed and read by other programs, but not modified.
- This prevents malicious programs from hijacking important files. It is also useful for safeguarding valuable files (spreadsheets, databases, documents) against accidental or deliberate sabotage.
- A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Adding your host file to this area will allow web browsers to use the file as normal, but will block any attempt to modify it.
- You can create exceptions if you want to allow a trusted application to access a protected file. See **Exceptions** for more details about how to allow access to files placed in 'Protected Files'.

Open the 'Protected Files' area

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Protected Files' tab:



The buttons at the top provide the following options:

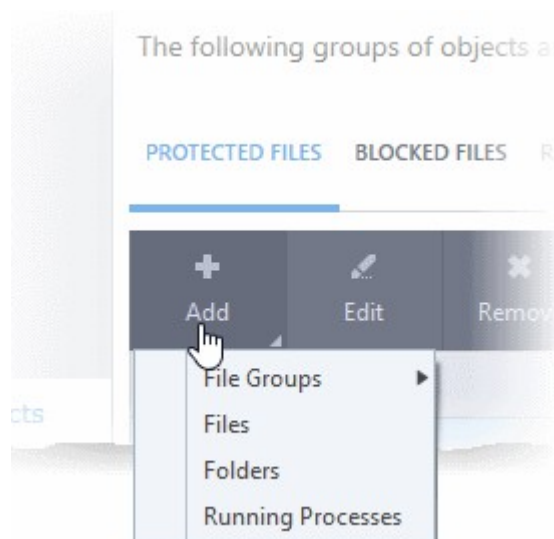
- **Add** – Select files/folders that you want to protect
- **Edit** – Modify the path of the file or group
- **Remove** - Delete the currently highlighted item
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the item is removed (purged) from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

Manually add protected items

You can protect individual files, folders, file groups or processes:

- Click the 'Add' button above the list:

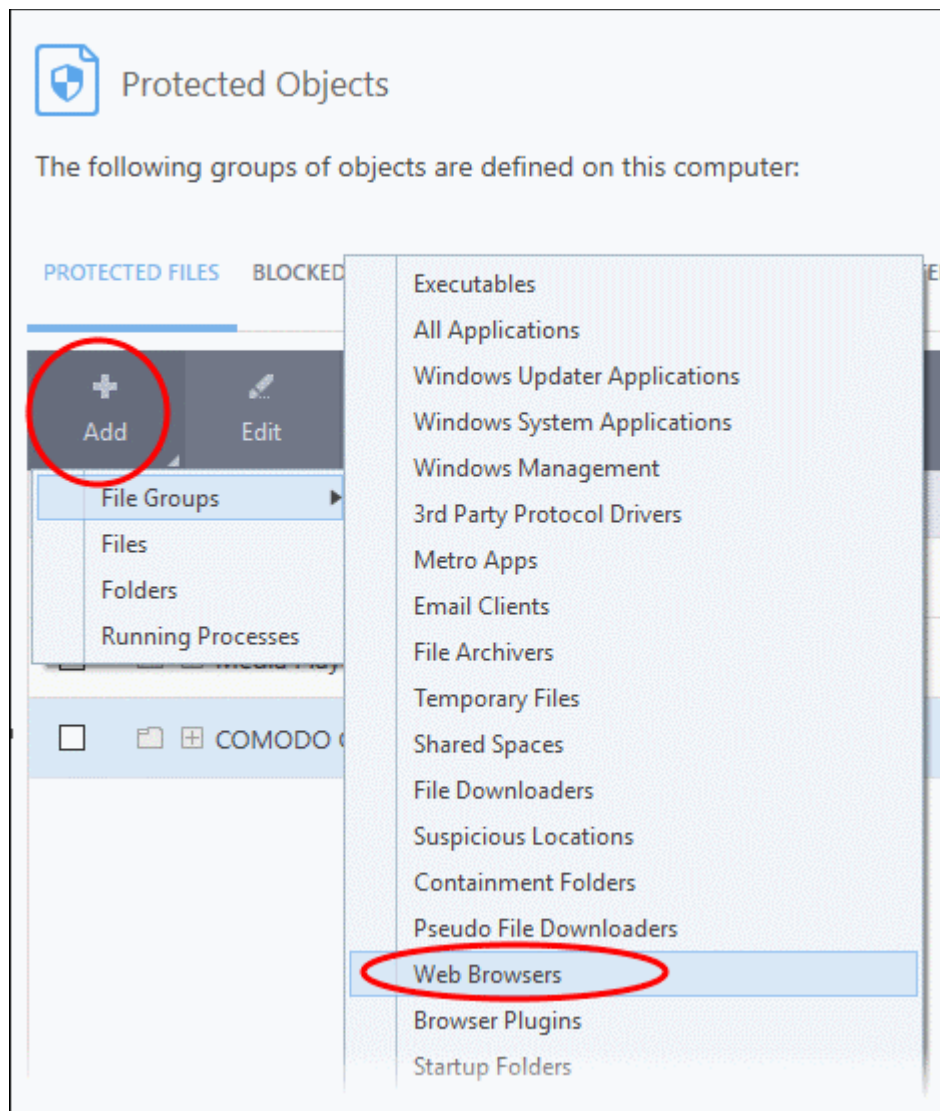


You can add items using any of the following methods:

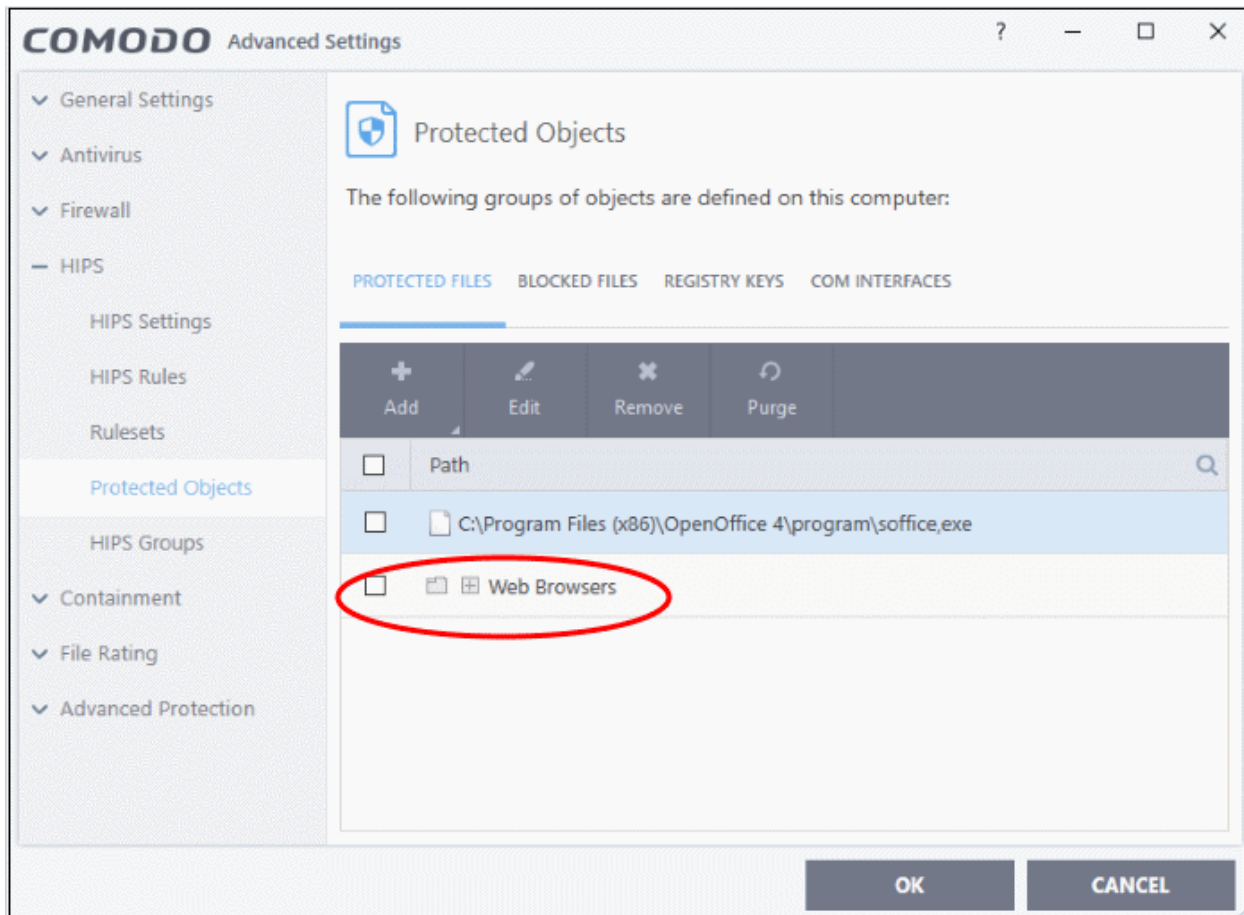
- **Select from File Groups**
- **Browse to a File**
- **Browse to a Folder**
- **Select from currently running processes**

Add a File Group

- Choosing 'File Groups' allows you to protect a category of pre-set files or folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.
 - Background - CCS ships with a set of predefined 'File Groups' which can be viewed in 'Settings' > 'File Rating' > **'File Groups'**. You can also add your own file groups if required.
- Click 'Add' > 'File Groups' and select the type of 'File Group' from the list:

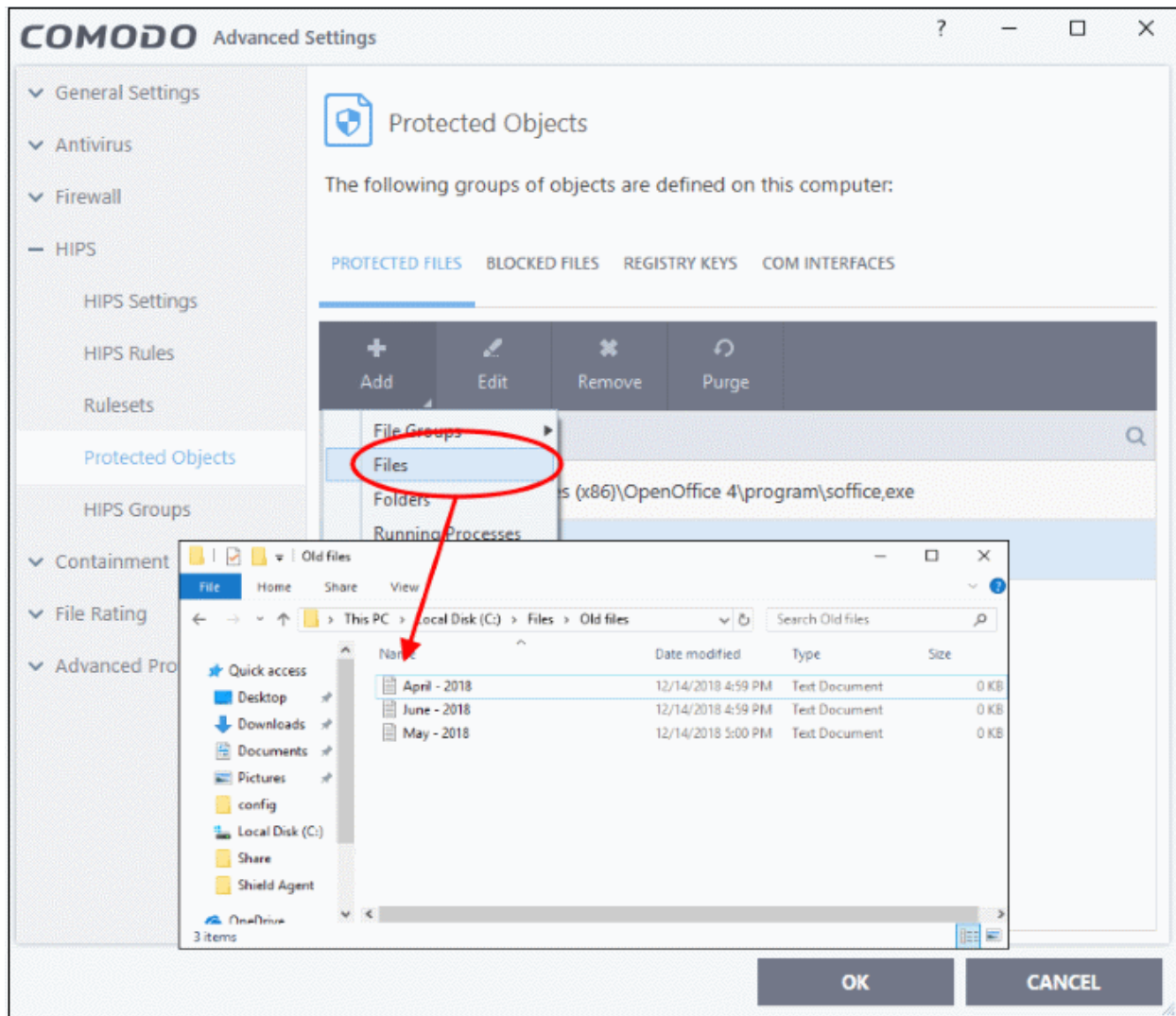


The selected group will be added to the 'Protected Files' list:

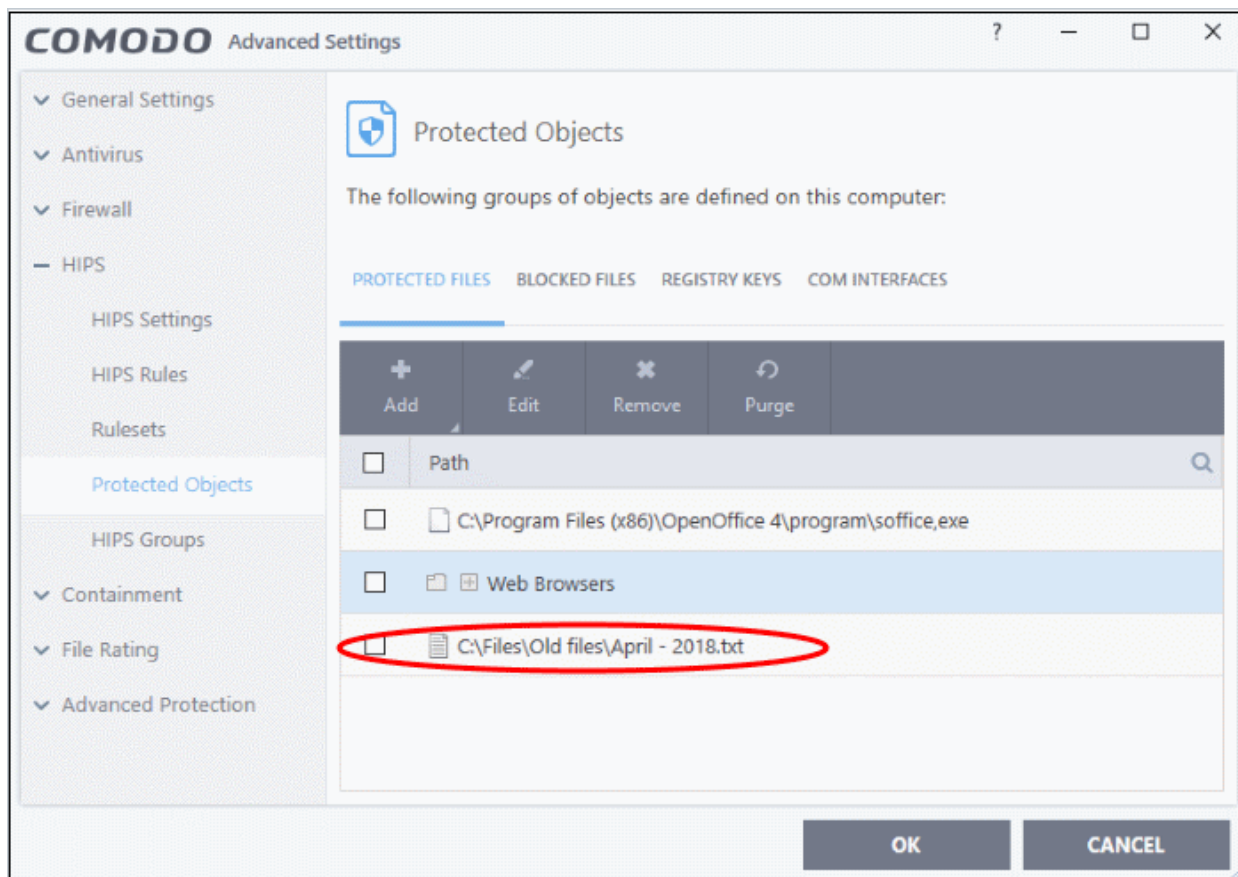


Add an individual file

- Click 'Add' and choose 'Files' from the options:

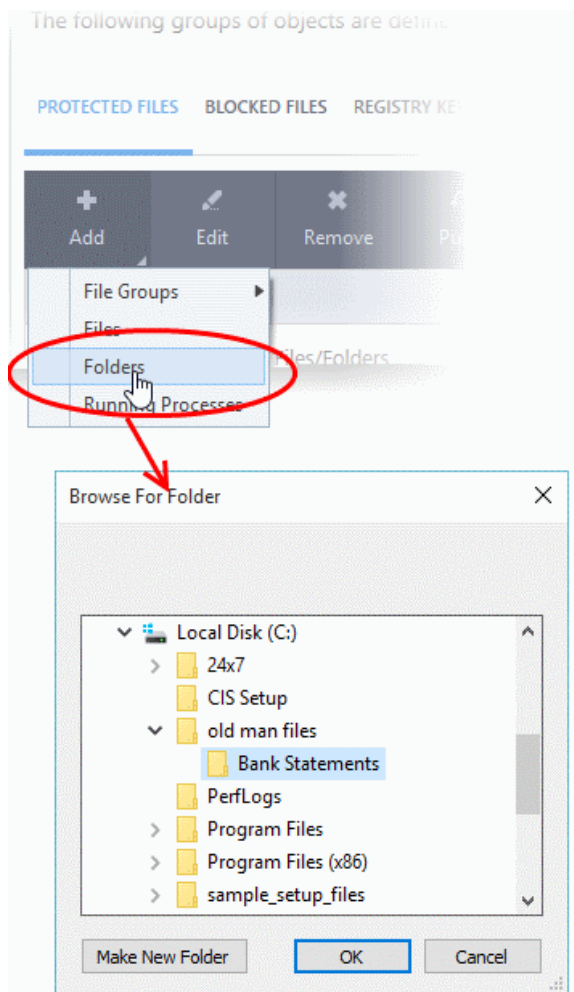


- Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open' The file will be added to 'Protected Files'.



Add a Drive Partition/Folder

- Click 'Folders' from the 'Add' drop-down.

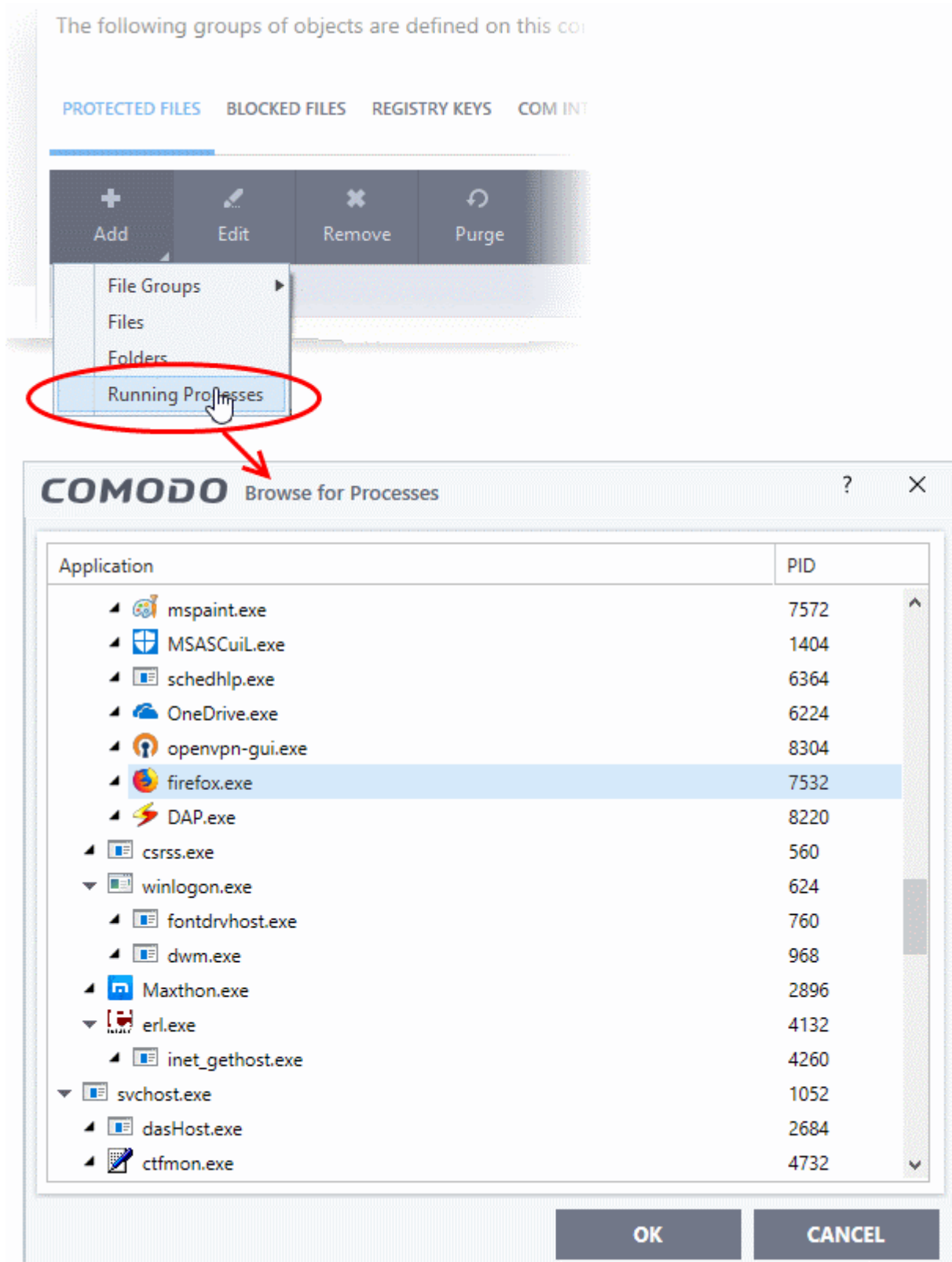


The 'Browse for Folder' dialog will appear.

- Select the folder/drive and click 'OK'. Repeat the process to add more items.

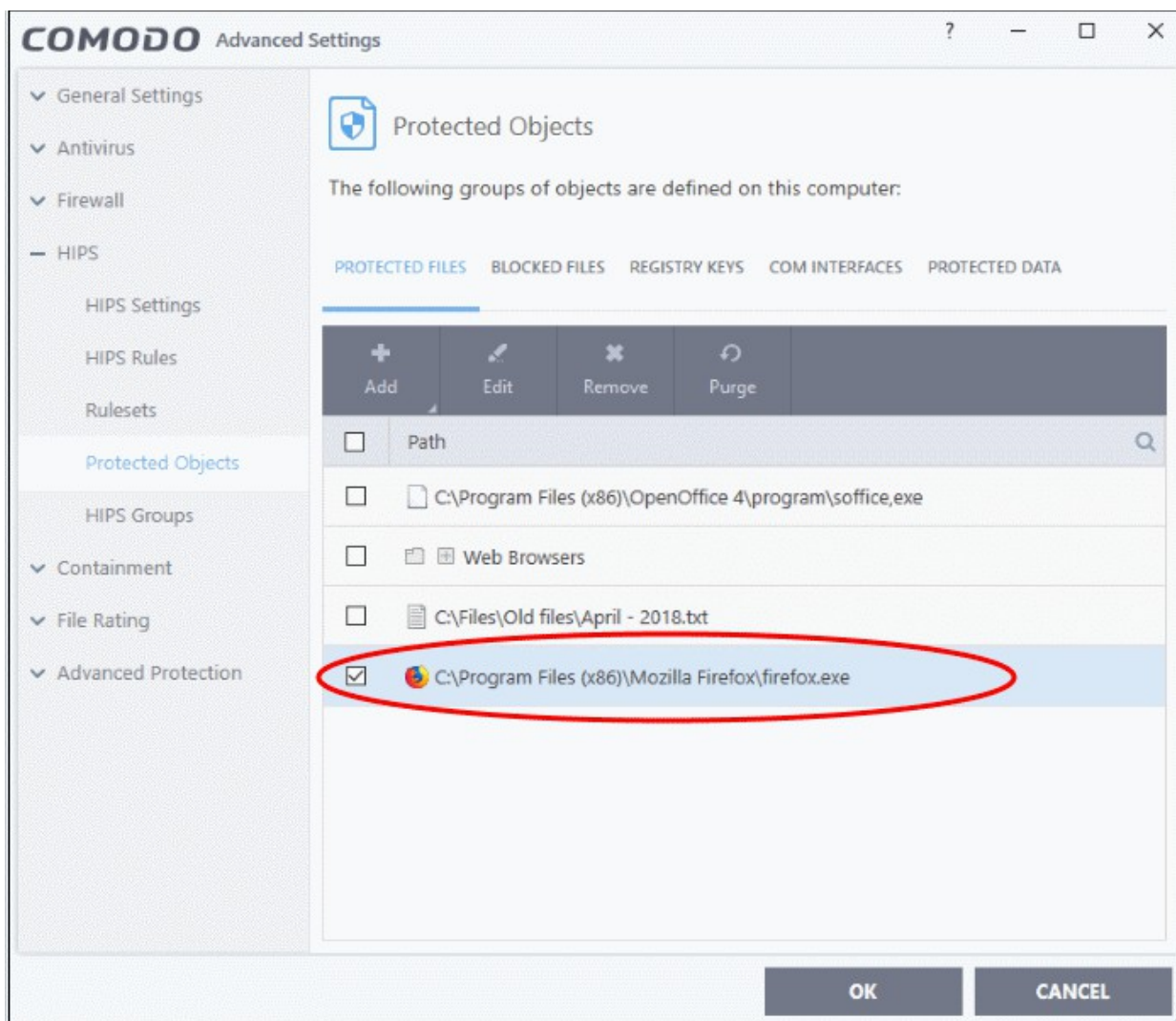
Add an application from a running process

- Choose 'Running Processes' from the 'Add' drop-down
- This will open a list of processes that are currently running on your computer:



- Select the process you want to protect
- Click 'OK'

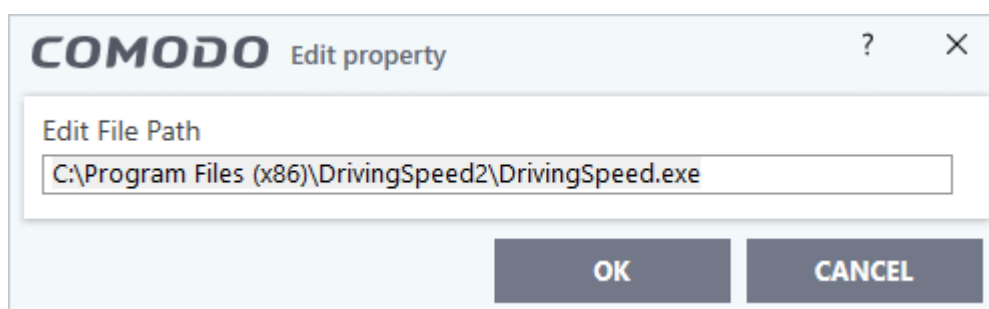
The parent application will be added to the 'Protected Files' list:



- Repeat the process to add more files. The items added to the 'Protected Files' will be protected from access by other programs.

To edit an item in the Protected Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click 'OK'

To delete an item from Protected Files list

- Select the item from the list and click the 'Remove' button

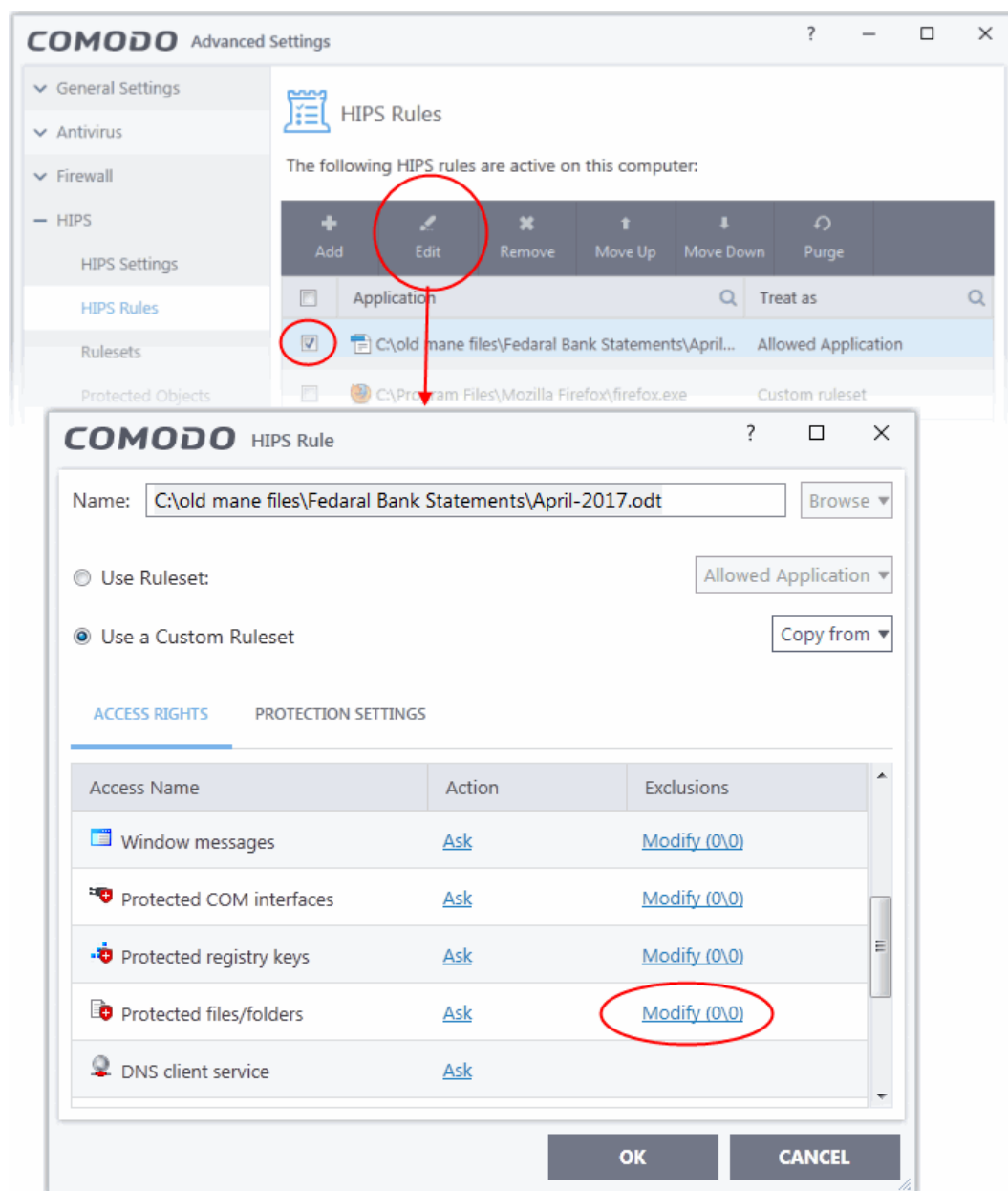
The selected item will be deleted from the protected files list. CCS will not generate alerts, if the file or program is subjected to unauthorized access.

Exceptions

Users can selectively allow another application (or file group) to modify a protected file by affording the appropriate 'Access Right' in '**Active HIPS Rules**' interface.

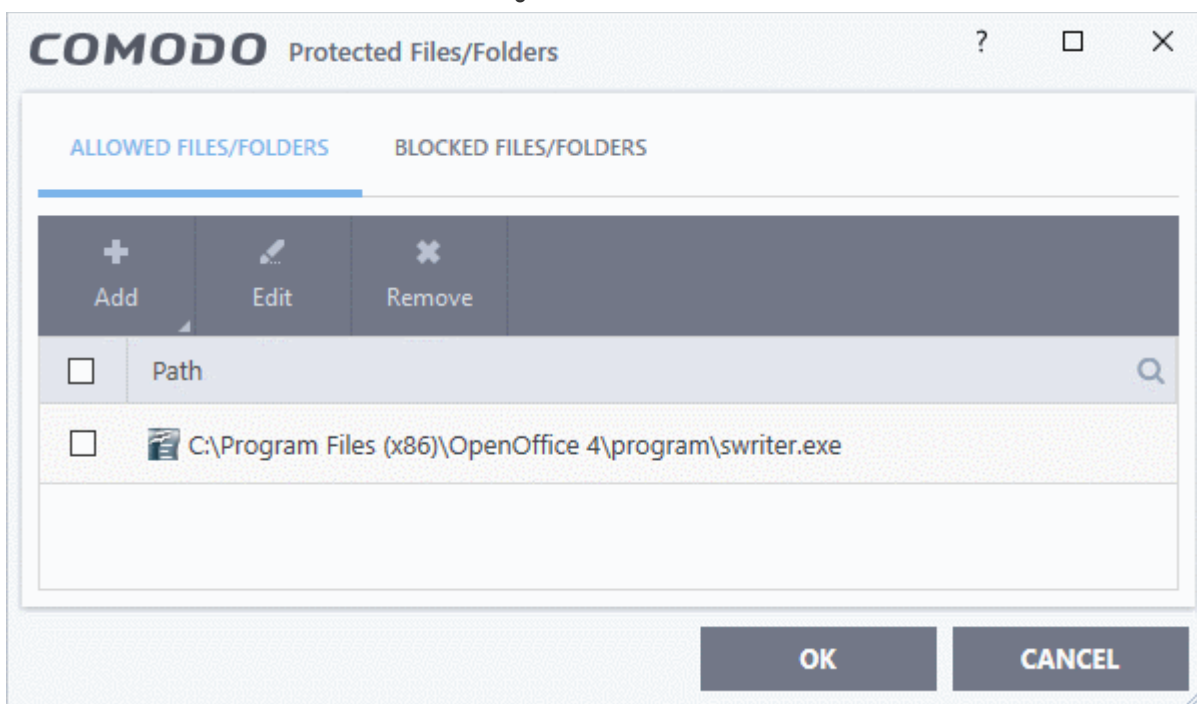
A simple example would be the imaginary file 'April - 2018.odt'. You would want the 'Open Office Writer' program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potentially malicious program. You would first **add** the document to the 'Protected Files' area. Once added to 'Protected Files', you would go into '**Active HIPS Rules**' and create an exception for 'swriter.exe' so that it alone could modify 'June - 2016.odt'.

- First add 'April - 2017.odt' to 'Protected Files'
- Then go to the 'HIPS Rules' interface and add it to the list of applications.
- Click the 'Edit' button after selecting 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'.



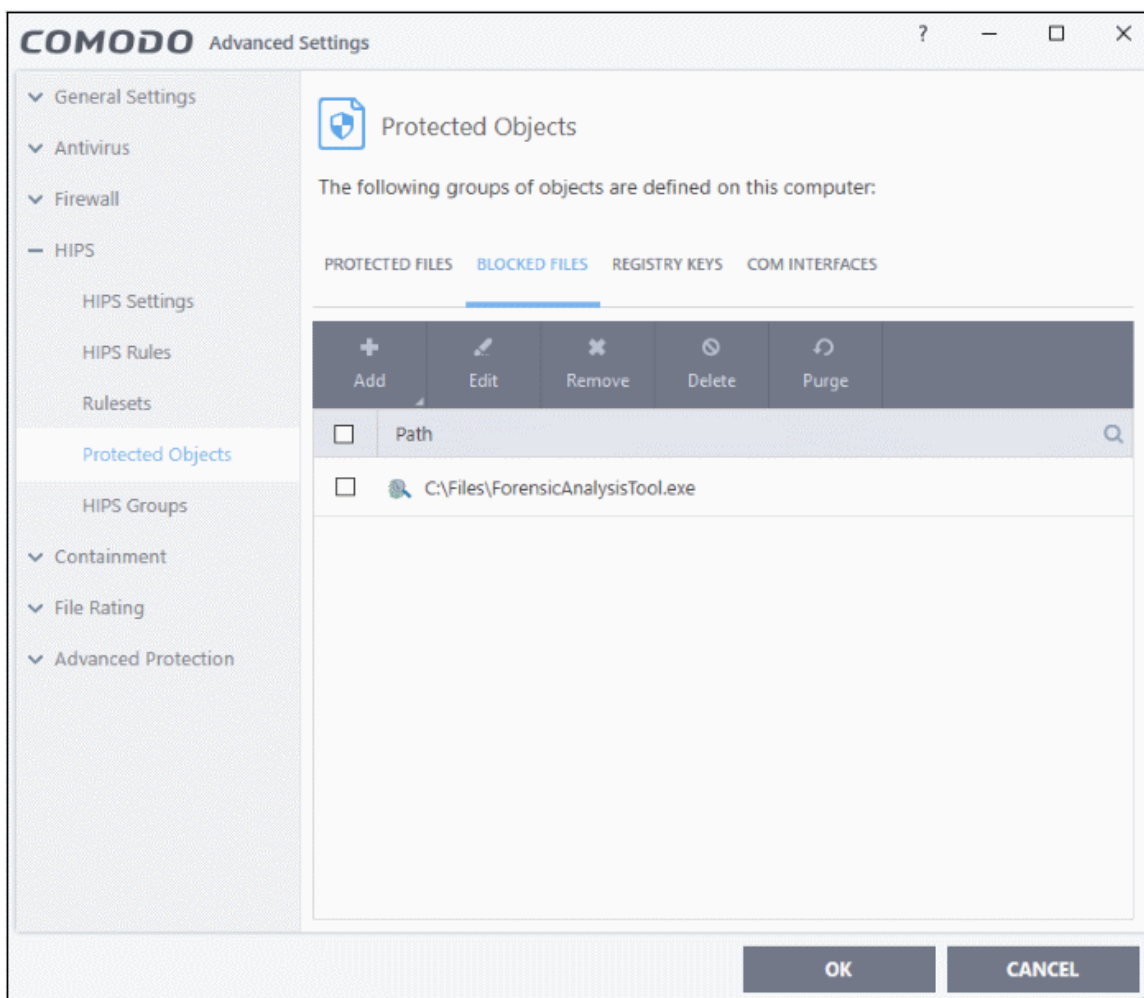
Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

6.5.1.2. Blocked Files

- CCS allows you to lock-down files and folders by denying all access rights to them from other processes or users - effectively cutting them off from the rest of your system.
- If the file you block is an executable, then neither you nor anything else is able to run that program.
- Unlike files in 'Protected Files', users cannot selectively allow access to a blocked file.

Open the blocked files section

- Click 'Settings' on the CCS home screen.
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Blocked Files' tab:



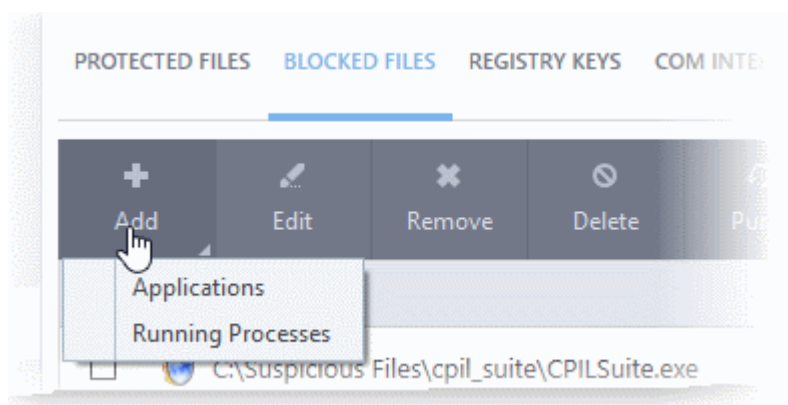
The buttons at the top provide the following options:

- **Add** - Select files/folders that you want to block
- **Edit** - Modify the path of the file or group
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the item is removed (purged) from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

Manually add an item to the block list

- Click the 'Add' button:

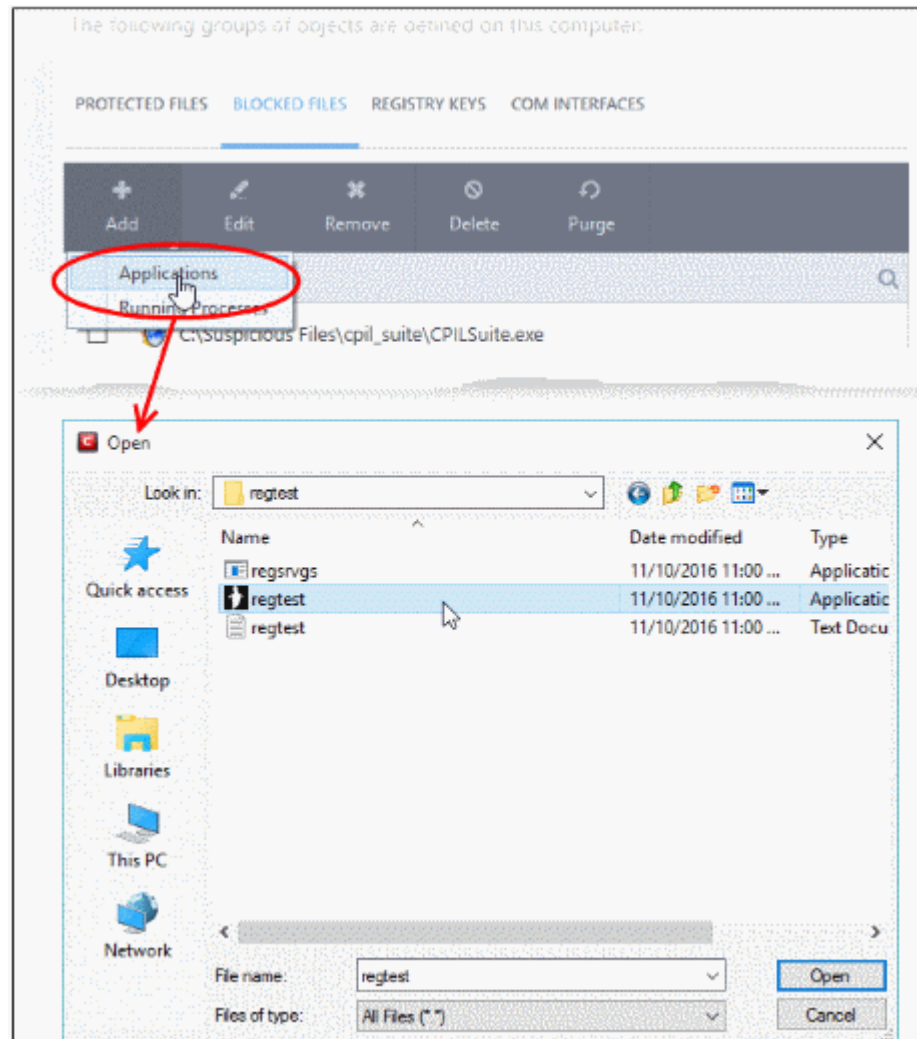


You can add the files by following methods:

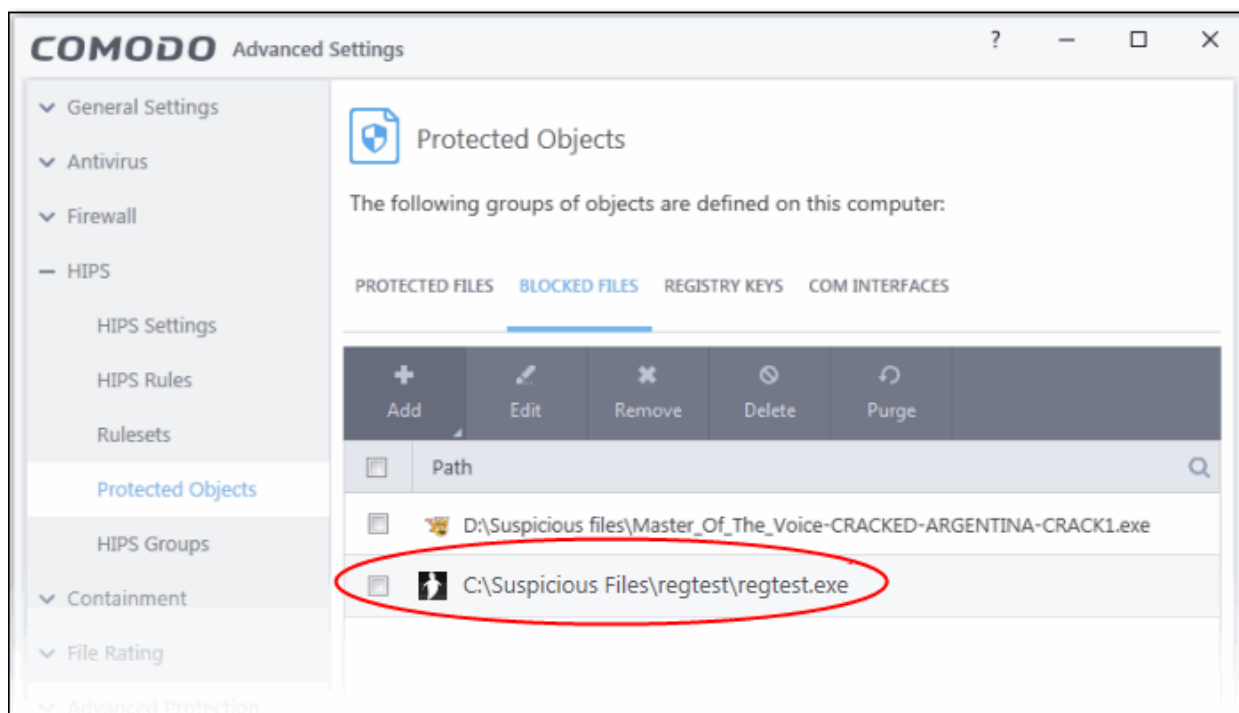
- **Select a file**
- **Select a currently running process**

Add a File

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



The file will be added to 'Blocked Files' list.



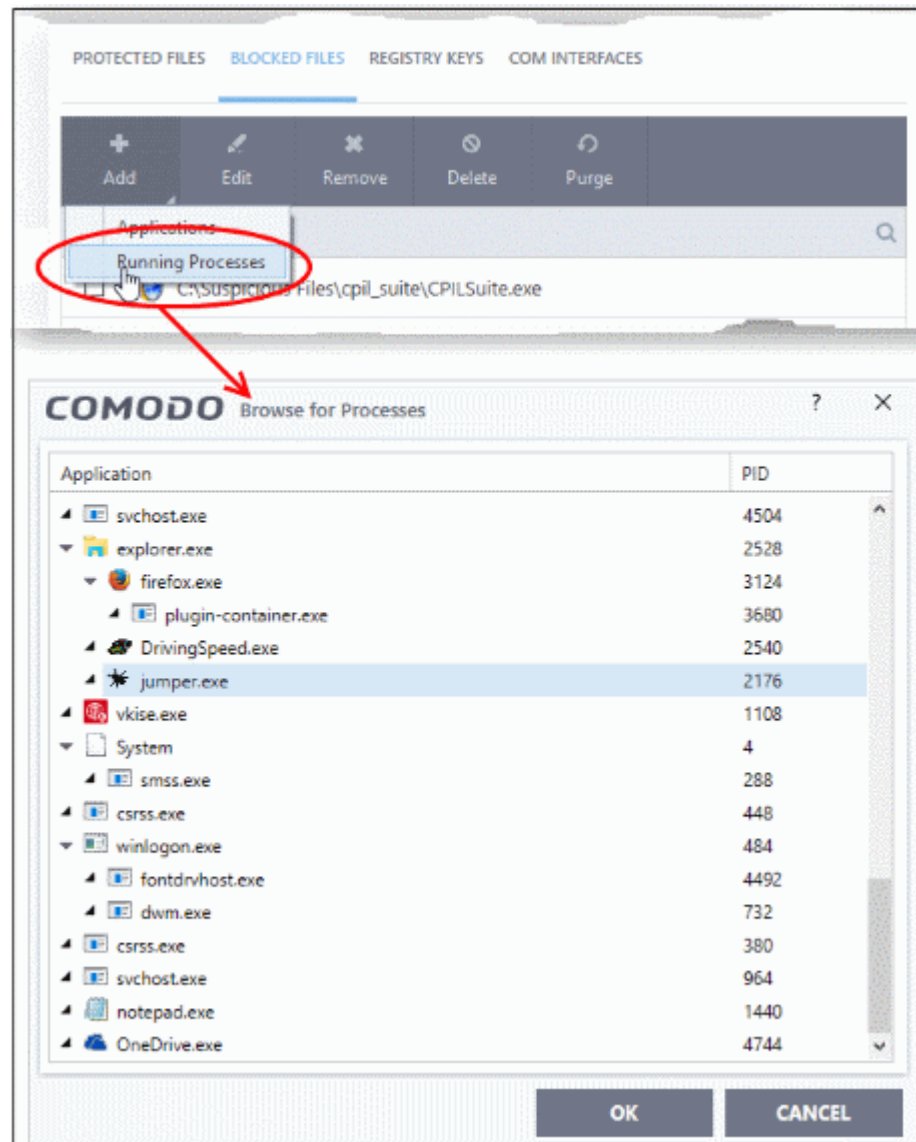
- Repeat the process to add more files.

Add a running process

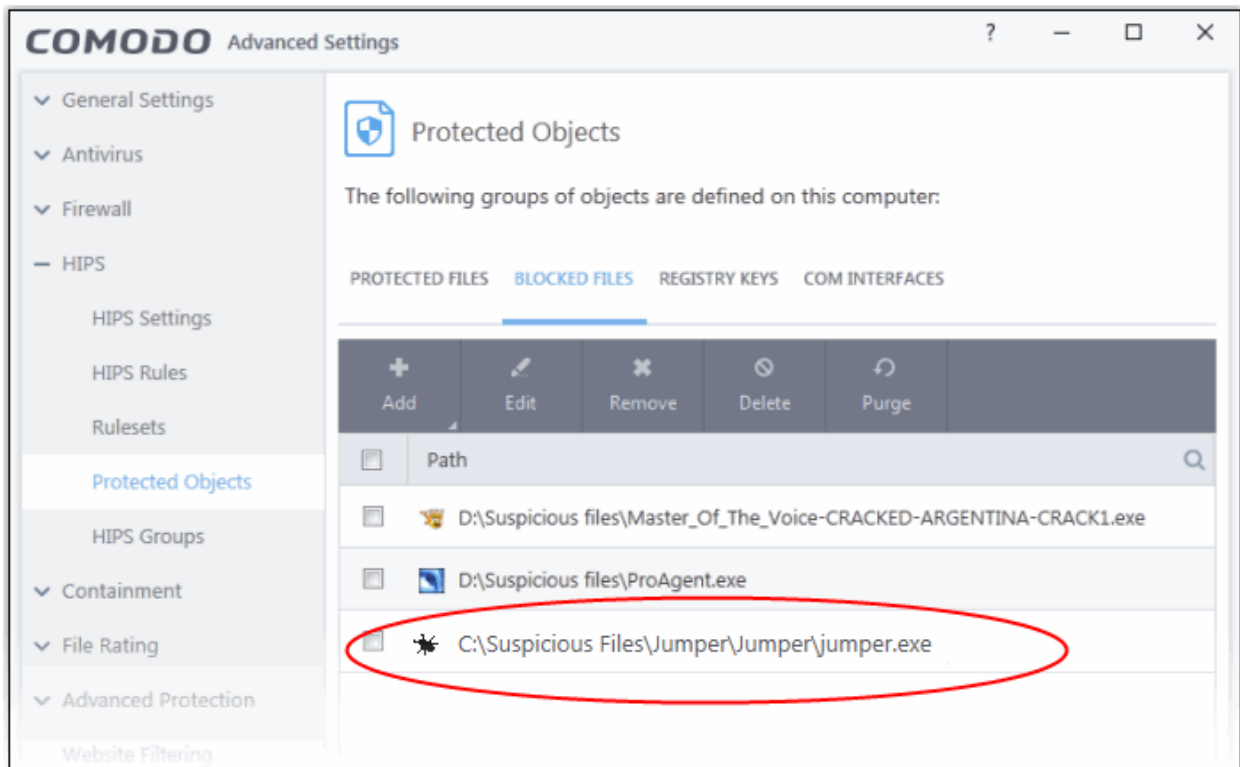
- Choose 'Running Processes' from the 'Add' drop-down

This will open a list of processes that are currently running on your computer:

- Select the process you want to protect
- Click 'OK'



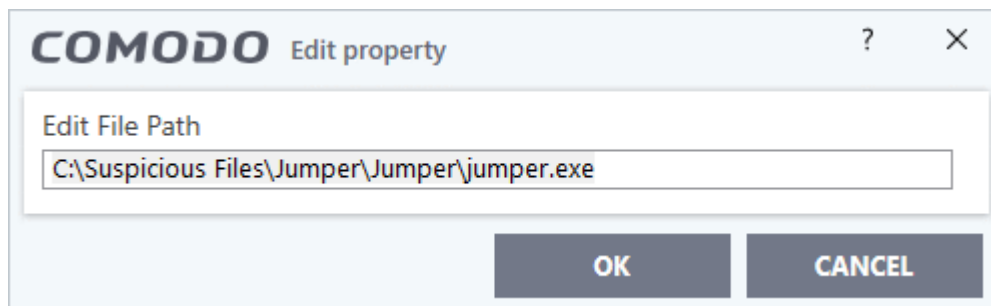
The parent application will be added to the 'Protected Files' list:



- Repeat the process to add more files.

To edit an item in the Blocked Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click 'OK'

To release an item from Blocked Files list

- Select the item from the list and click the 'Remove' button

The selected item will be removed from the 'Blocked Files' list. CCS will not block the application or file from execution or opening then onwards.

To permanently delete a blocked file from your system

- Select the item from the list and click the 'Delete' button

The selected item will be deleted from your computer immediately.

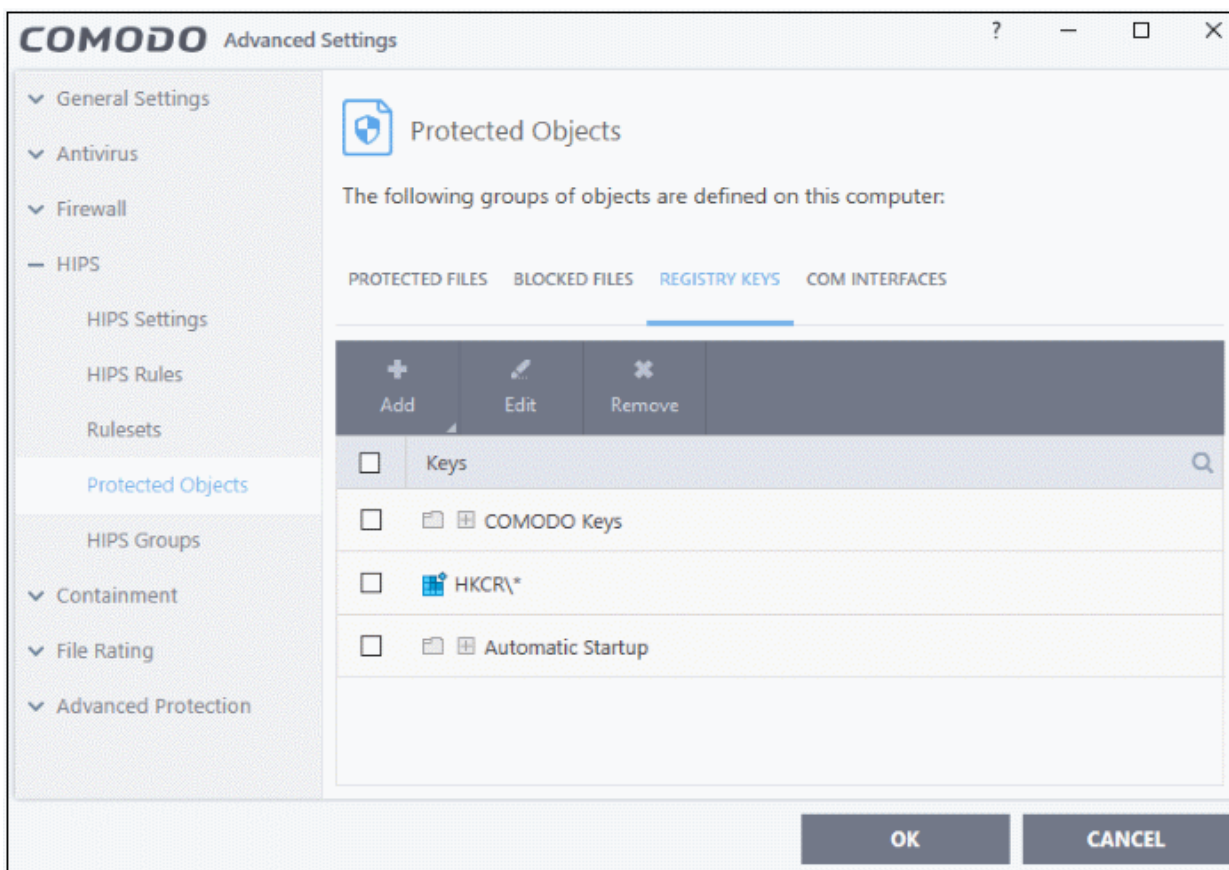
Warning: Deleting a file from from the 'Blocked Files' interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

6.5.1.3. Protected Registry Keys

The 'Registry Keys' area lets you define system critical registry keys which should be protected against modification. 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 CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Registry Keys' tab:



The buttons at the top provide the following options:

- **Add** – Select registry groups or individual keys that you want to protect
- **Edit** - Modify the path of the key or key group
- **Remove** - Delete the currently highlighted item
- Click the magnifying glass on the right to search for a specific item.

Manually add individual keys or registry groups

- Click the 'Add' button

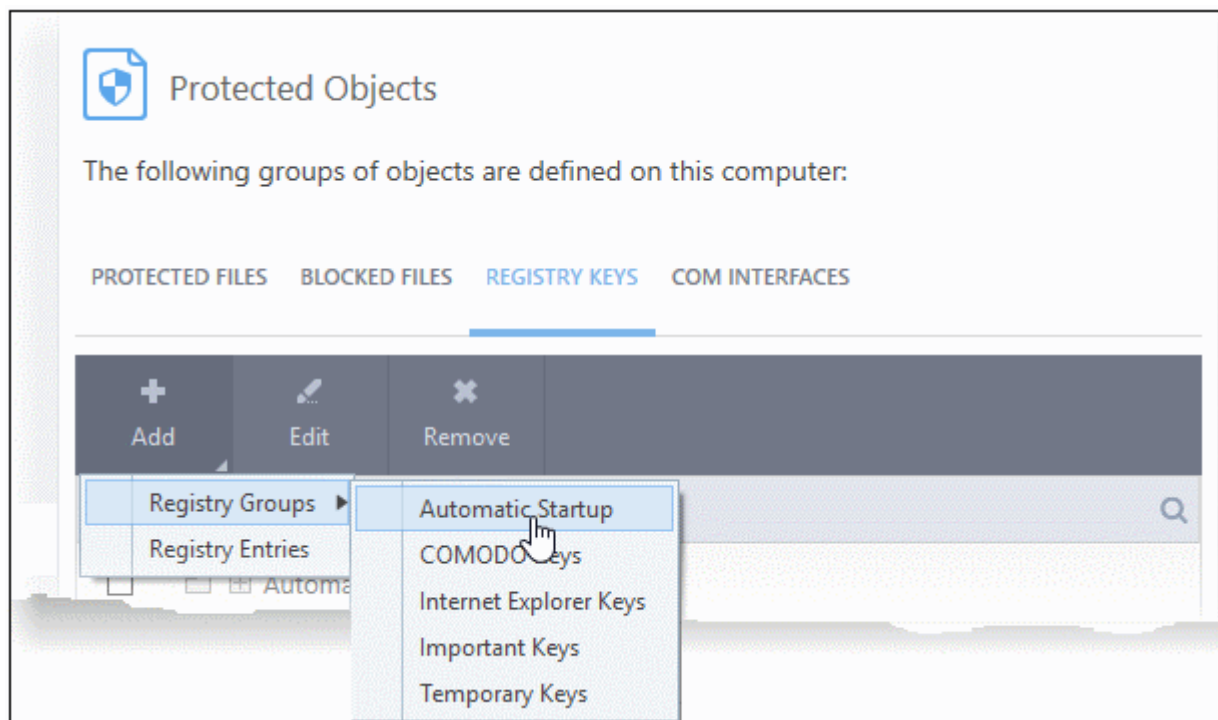
You can add keys individually or by registry group:

- **Add Registry Groups** - Adding a registry group allows you to batch select and import groups of important registry keys. Comodo Client Security provides the following, pre-defined groups - 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.

You can also create custom registry groups containing keys you wish to protect.

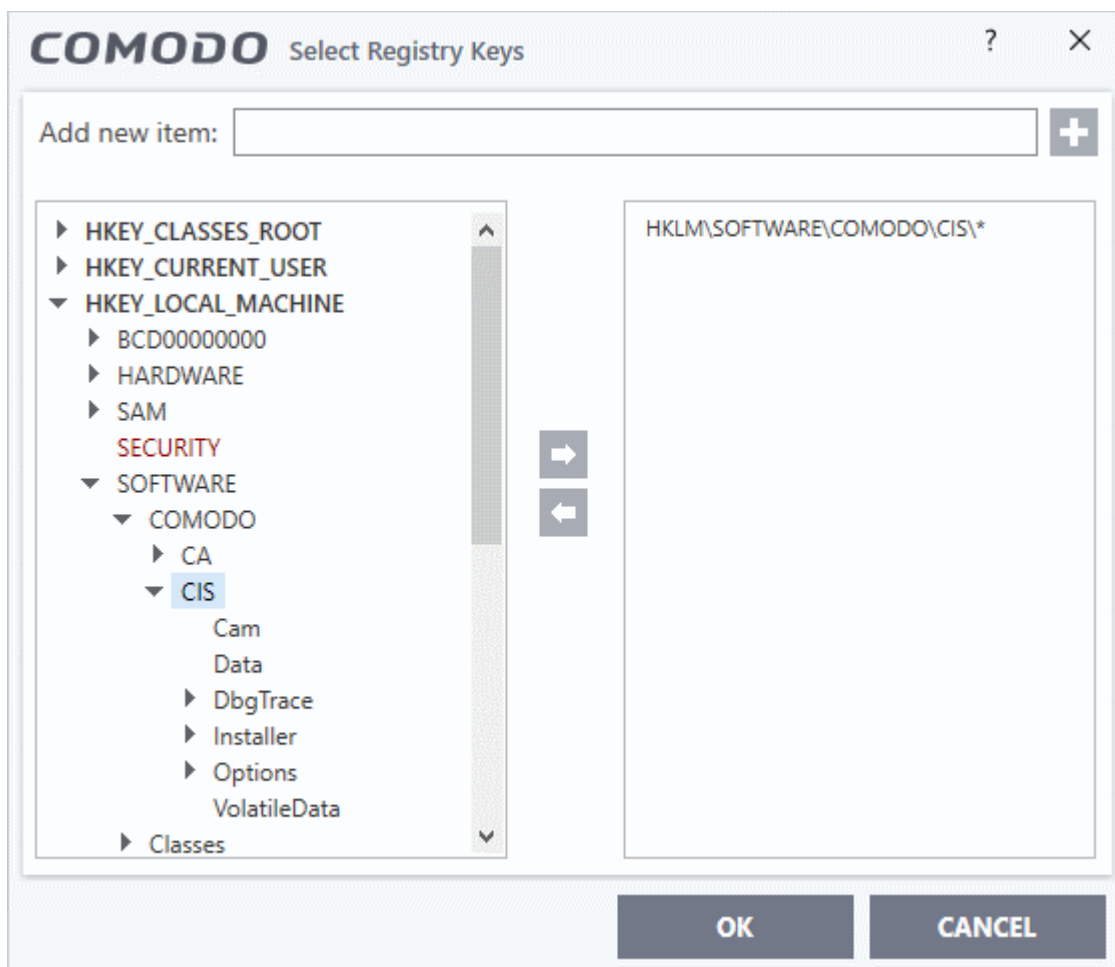
- To add a new group, click the 'Add' button > 'Registry Groups' and select the predefined group

from the list and click 'OK'



See **Registry Groups** in the **HIPS Groups** section if you want to read more on this interface.

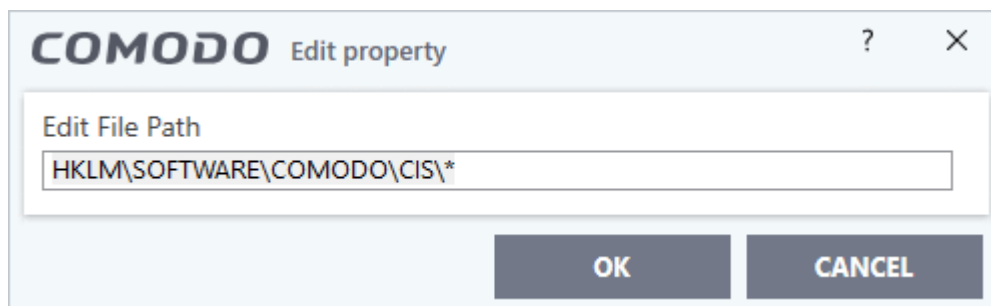
- **Add individual Registry Keys -**
 - Click the 'Add' button and then select 'Registry Entries'
 - Choose a key on the left then click the right arrow to add it to the protected list:



- Alternatively, you can type the key name in the field at the top then click '+'.

Edit an item in the Registry Protection list

- Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the key path, if you have relocated the key and click 'OK'.

Note: The 'Registry Groups' cannot be edited from this interface. You can edit only from **Registry Groups** in **HIPS Groups** section.

To delete an item from Registry Protection list

- Select the item from the list and click the 'Remove' button.

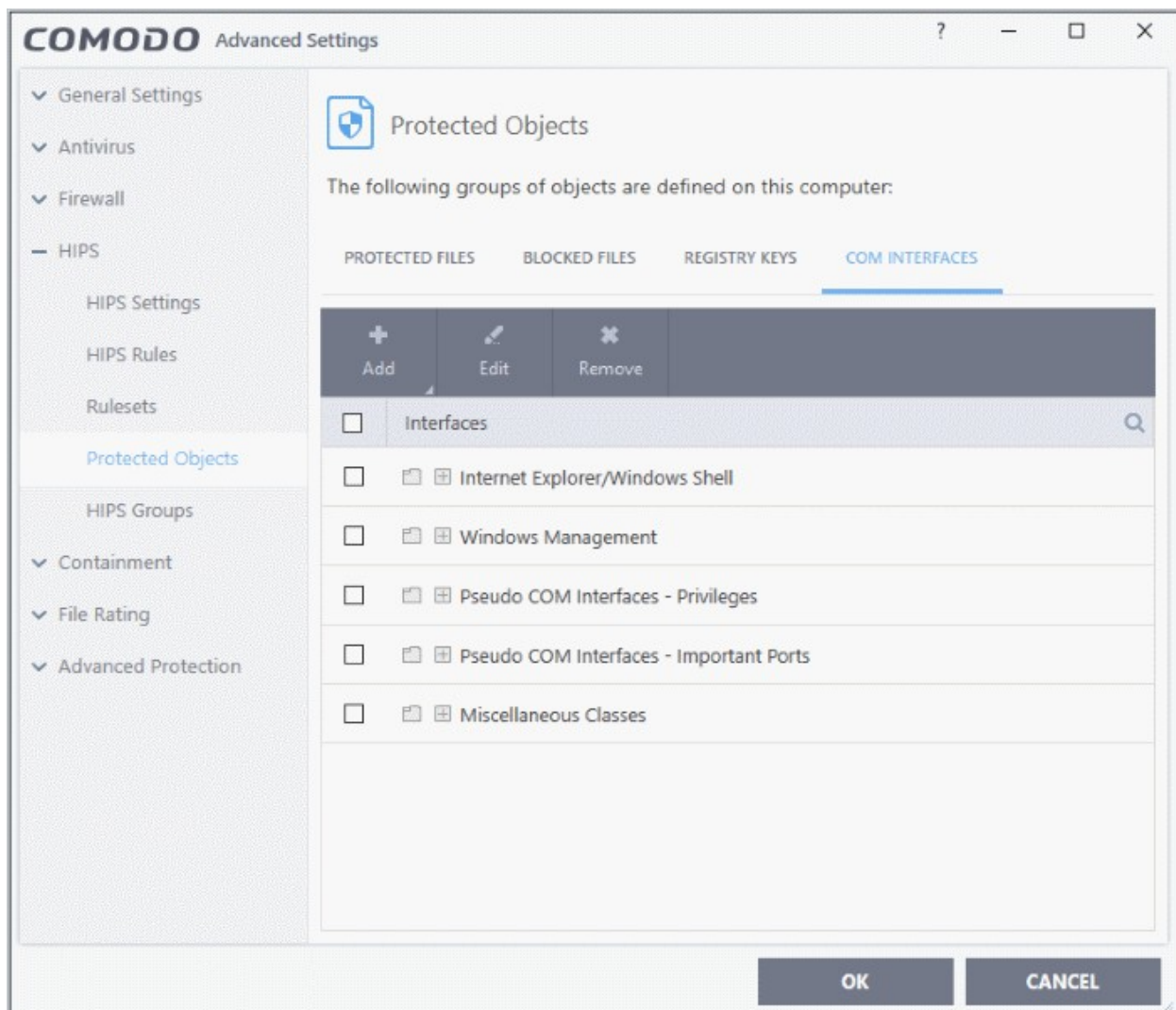
The selected item will be deleted from the 'Registry Keys' protection list. CCS will not generate alerts, if the key or the group is modified by other programs.

6.5.1.4. Protected COM interfaces

- The Component Object Model (COM) is Microsoft's object-oriented programming model. It defines how objects interact within a single application, or between applications.
- COM is used as the basis for Active X and OLE - two favorite targets of hackers and malware for launching attacks on your computer.
- Comodo Client Security automatically protects COM interfaces against modification and manipulation by malicious processes.
- 'Protected Objects' > 'COM Interfaces' lets you view, add and edit these protected interfaces.
 - Background - CCS ships with a set of COM groups - category based collections of COM interface components.
 - Click 'Settings' > 'HIPS Groups' > 'COM Groups' if you want to view these groups. You can create custom groups if required. See [COM Groups](#) for the help page on this area.

Open the protected COM interfaces area

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'COM Interfaces' tab:



The buttons at the top provide the following options:

- **Add** - Select COM groups or individual components that you want to protect
- **Edit** - Edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or COM component.

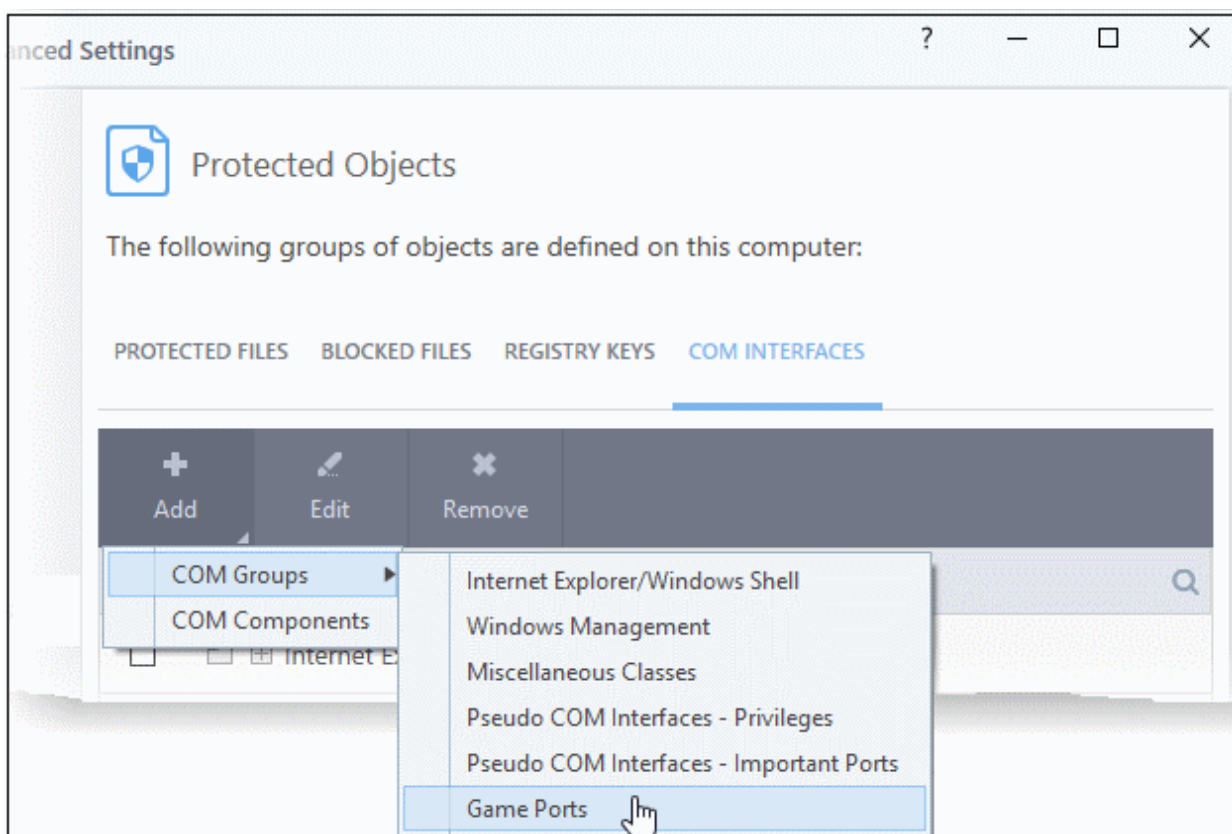
You can search for a specific interface by clicking the magnifying glass icon at the far right of the column header.

Manually add a COM group or individual component

- Click the 'Add' button

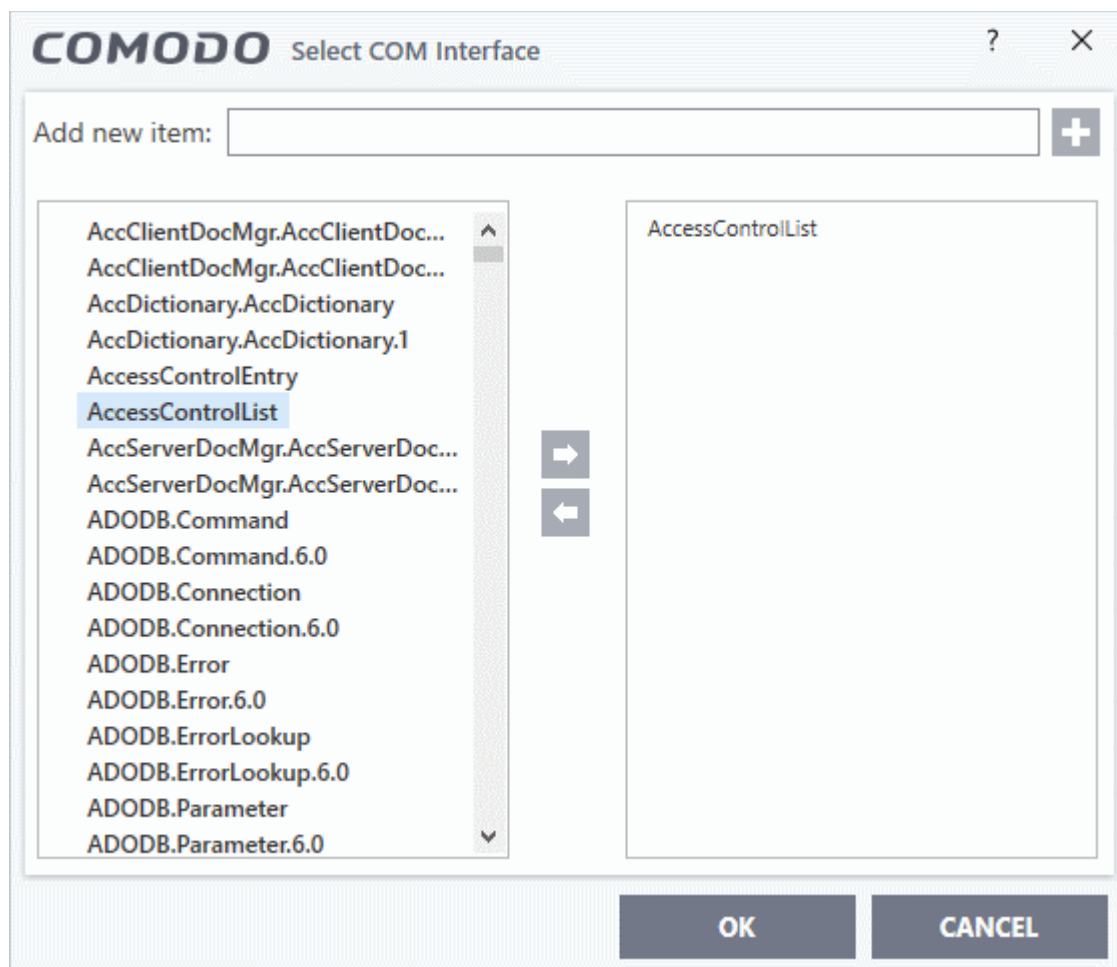
You can add items as follows:

- **Add COM Groups** - Batch select and import predefined groups of important COM components.
 - Click 'Add' > 'COM Groups'
 - Select the group you want to add
 - Click 'OK'



For explanations on editing existing 'COM Groups' and creating new groups, see [COM Groups](#).

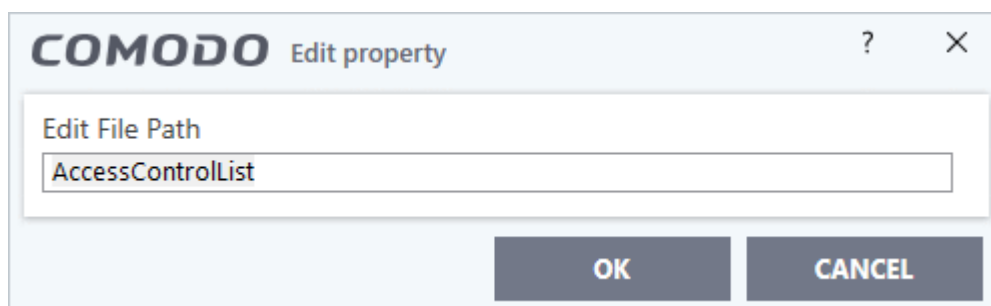
- **Add individual components**
 - Click the 'Add' button then 'COM Components'.
 - Select a component on the left
 - Click the right arrow to add it to the protected list:



- Click 'OK' to add the items to the list

Edit an item in the COM Interfaces protection list

- Select the COM component from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the COM Class file path and click 'OK'

Note: The COM Groups cannot be edited from this interface. You can edit only from **COM Groups** in **HIPS Groups** section.

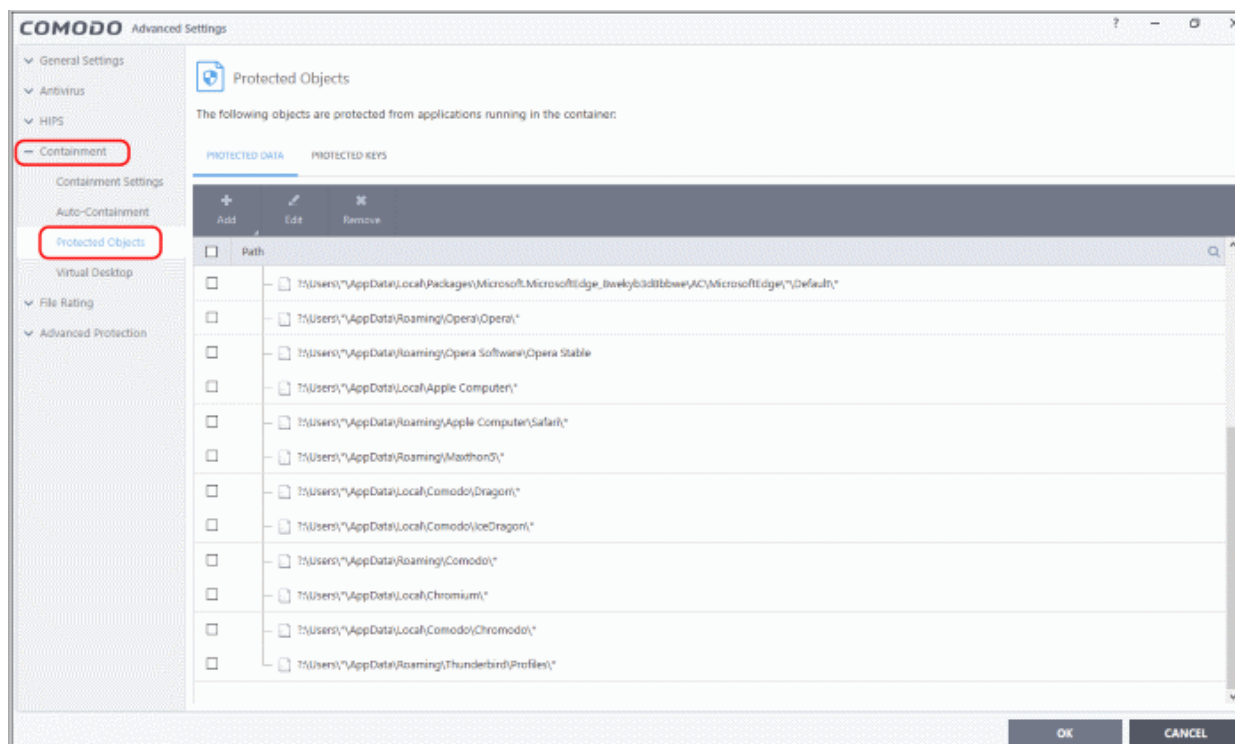
To delete an item from COM Interfaces protection list

- Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the 'COM Interfaces' protection list. CCS will not generate alerts, if the COM component or the group is modified by other programs or processes.

6.5.2. Protected Objects - Containment

- Items that you add to this area cannot be read or modified by applications running in the container.
- Examples items you can add are files, folders and registry keys.
- This prevents unknown/untrusted applications from causing damage to, or stealing data from, important items
- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Protected Objects' on the left:



Click the following links for more details:

- [Protected Data Folders](#)
- [Protected Keys](#)

6.5.2.1. Protected Data Folders

Files inside a 'Protected Data Folder' cannot be seen, accessed or modified by applications running inside the container.

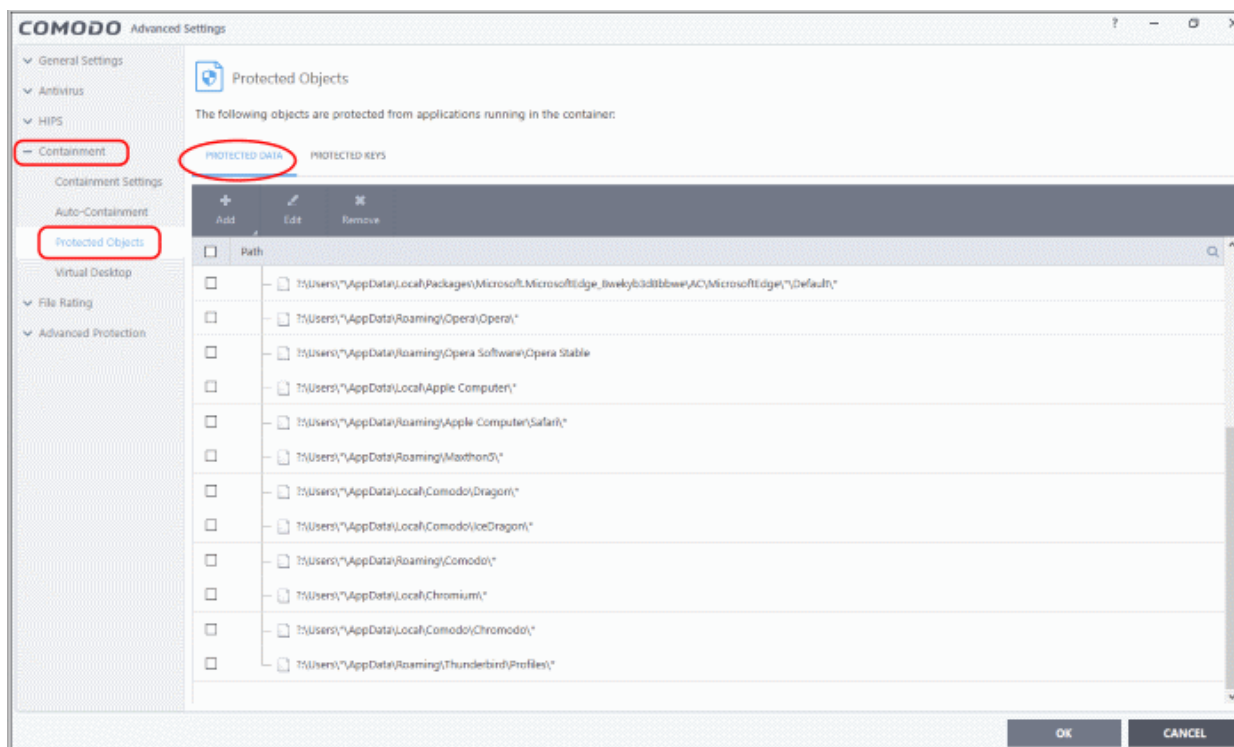
Tip:

- Files and folders added to 'Advanced Settings' > 'HIPS' > 'Protected Objects' > '**Protected Files**' permit read access by other programs, but cannot be modified. This contrasts to files/folders in 'Protected Data folders' in this interface, which are totally hidden to contained programs.
- If you want a file to be read by other programs but protected from modifications, then add it to '**Protected Files**' list.

Open the 'Protected Data Folders' section

- Click 'Settings' on the CCS home screen

- Click 'Containment' > 'Protected Objects' on the left.
- Click the 'Protected Data Folders' tab:



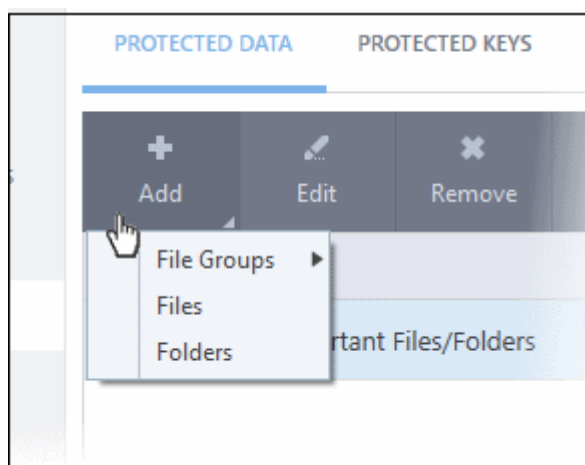
The buttons at the top provide the following options:

- **Add** - Select files/folders that you want to protect
- **Edit** - Modify the path of the file or group.
- **Remove** - Delete the currently highlighted item

You can use the search option to find a specific name in the list by clicking the search icon at the far right of the column header and entering the name in full or part.

Manually add a file, folder or file group

- Click the 'Add' button



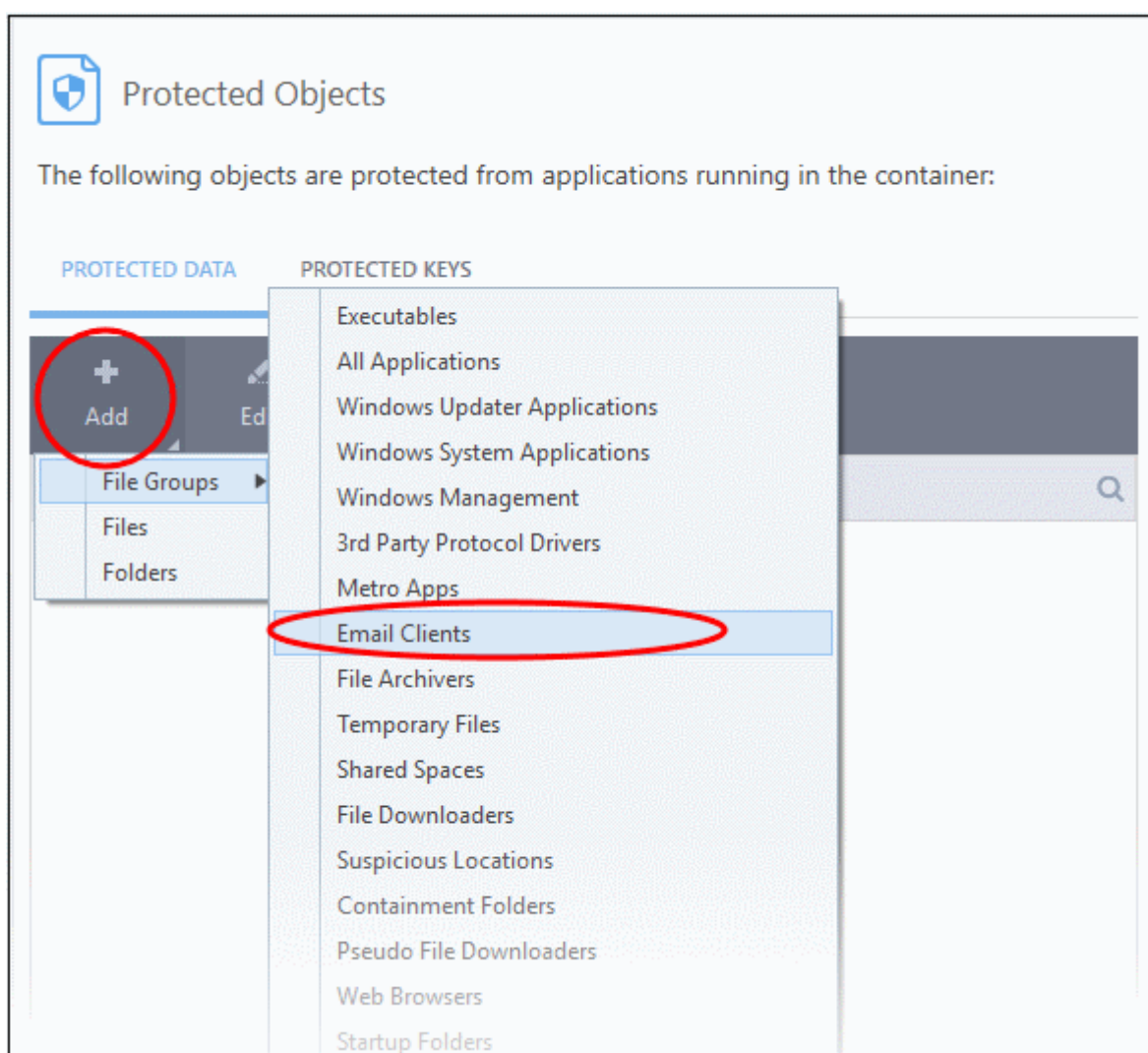
You can add items using any of the following methods:

- **Select from File Groups**
- **Browse to a File**

- **Browse to a Folder**

Add a File Group

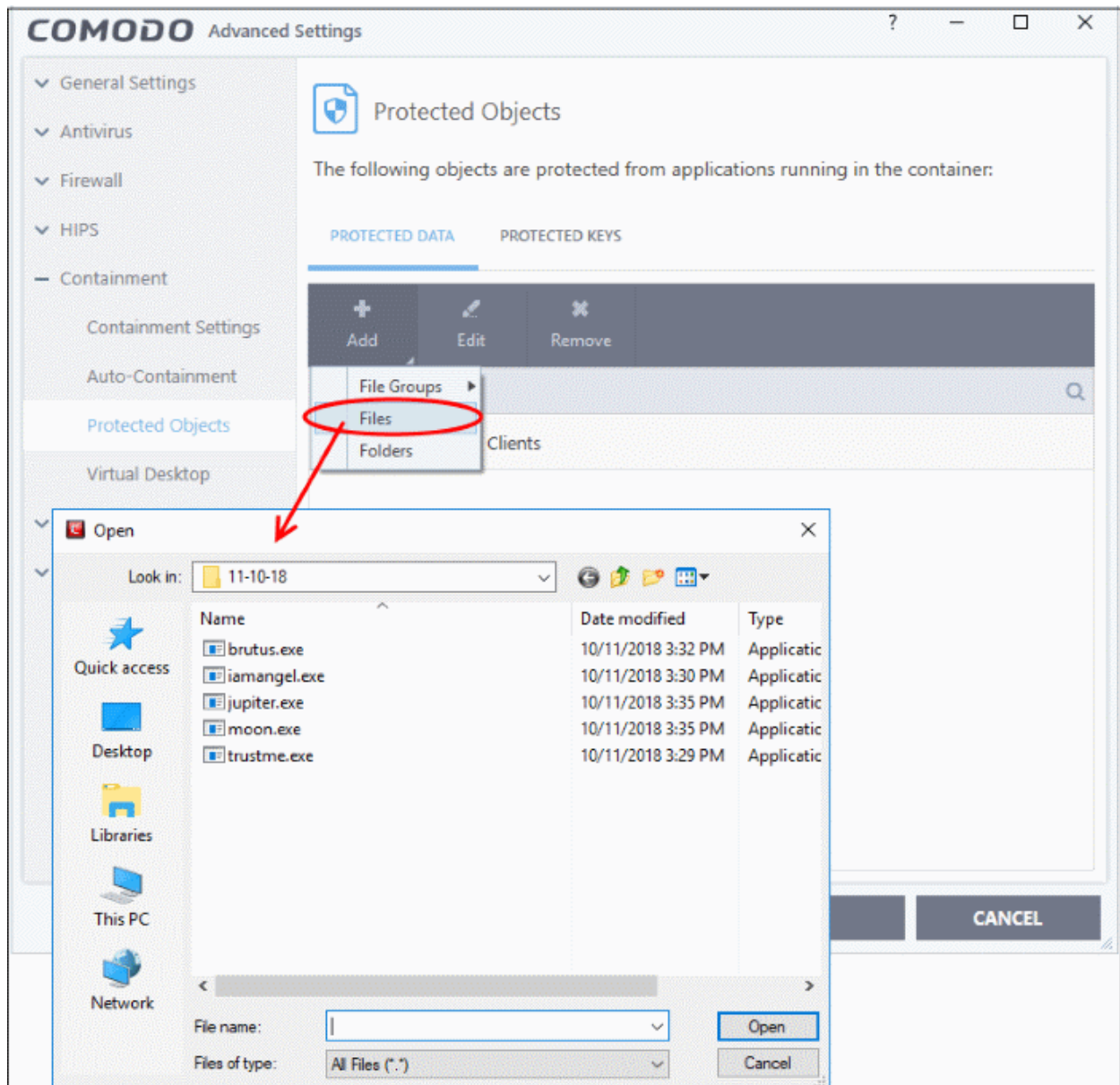
- Choosing 'File Groups' allows you to protect a category of pre-set files or folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.
 - Background - CCS ships with a set of predefined 'File Groups' which can be viewed in 'Settings' > 'File Rating' > **'File Groups'**. You can also add your own file groups if required.
- Click 'Add' > 'File Groups' and select the type of 'File Group' from the list:



The selected group will be added to the 'Protected Files' list:

Add an Individual File

- Click 'Add' and choose 'Files' from the options:

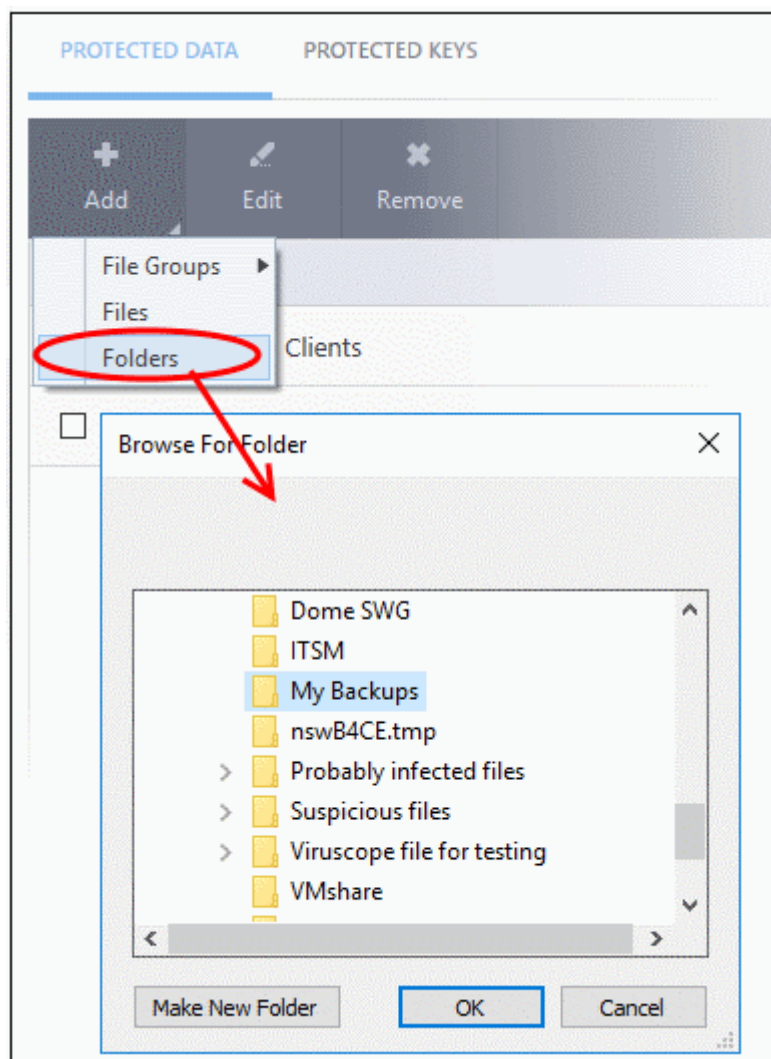


- Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open'

The file will be added to 'Protected Files'.

Add a Drive Partition / Folder

- Click 'Folders' from the 'Add' drop-down.

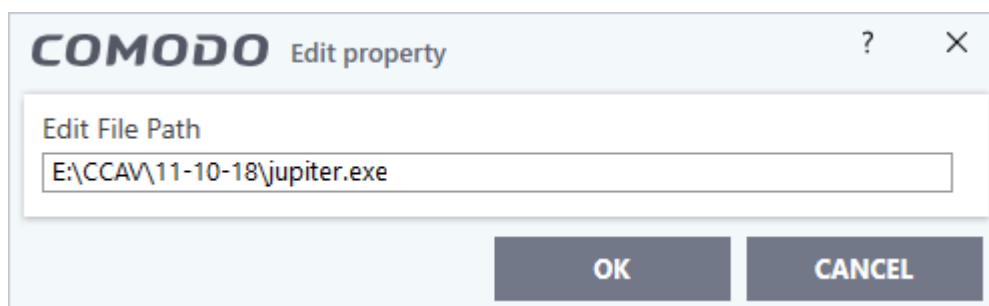


The 'Browse for Folder' dialog will appear.

- Select the folder/drive and click 'OK'. Repeat the process to add more items. The items added to the 'Protected Files' will be protected from programs that are contained.

To edit an item in the Protected Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Update as required and click 'OK'

To delete an item from Protected Files list

- Select the item from the list and click the 'Remove' button

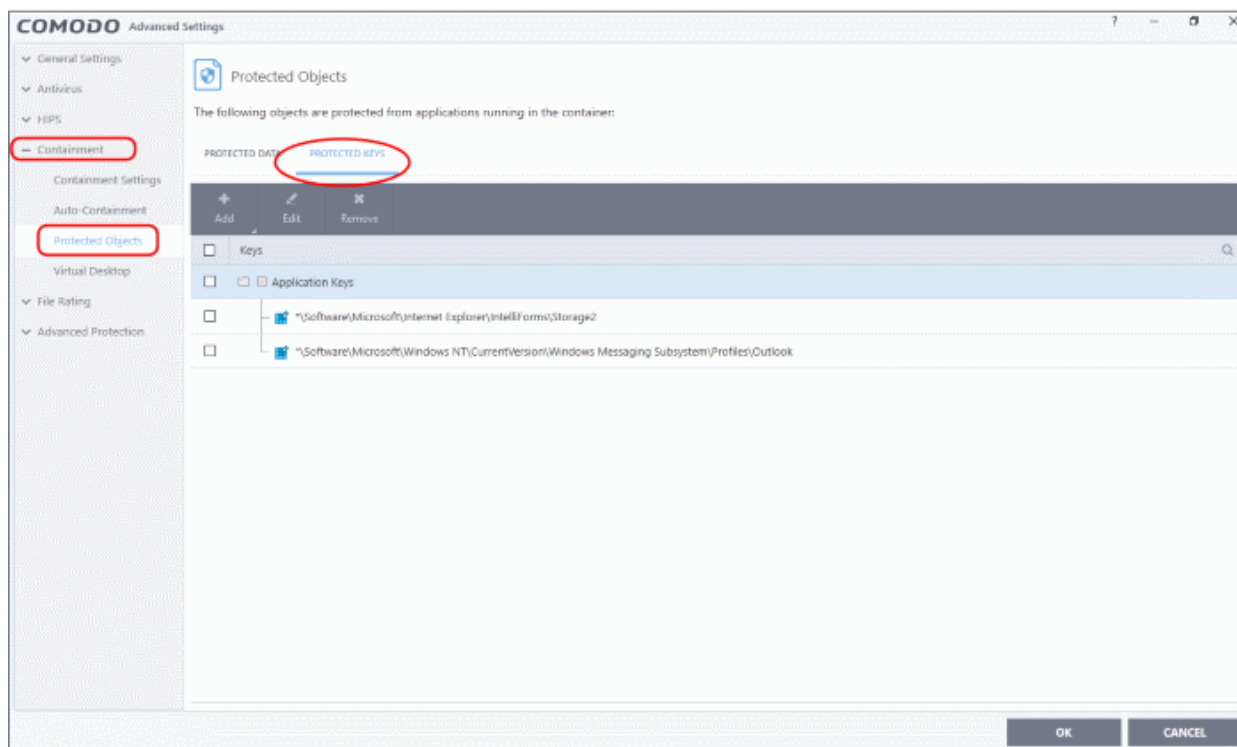
The selected item will be deleted from the protected files list.

6.5.2.2. Protected Keys

- The 'Protected Keys' area lets you define system critical registry keys which should be protected against modification from programs running inside the container
- Applications in the container cannot read or modify registry keys added here

Open the 'Protected Keys' section

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Protected Objects' on the left.
- Click the 'Protected Keys' tab:

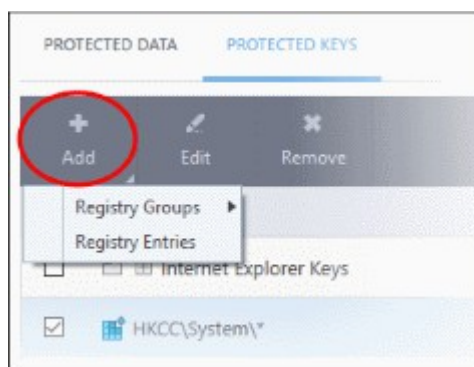


The buttons at the top provide the following options:

- **Add** - Select registry groups or individual keys that you want to protect
- **Edit** - Modify the path of the key or key group
- **Remove** - Delete the currently highlighted item
- Click the magnifying glass on the right to search for a specific item.

Manually add individual keys or registry groups

- Click the 'Add' button

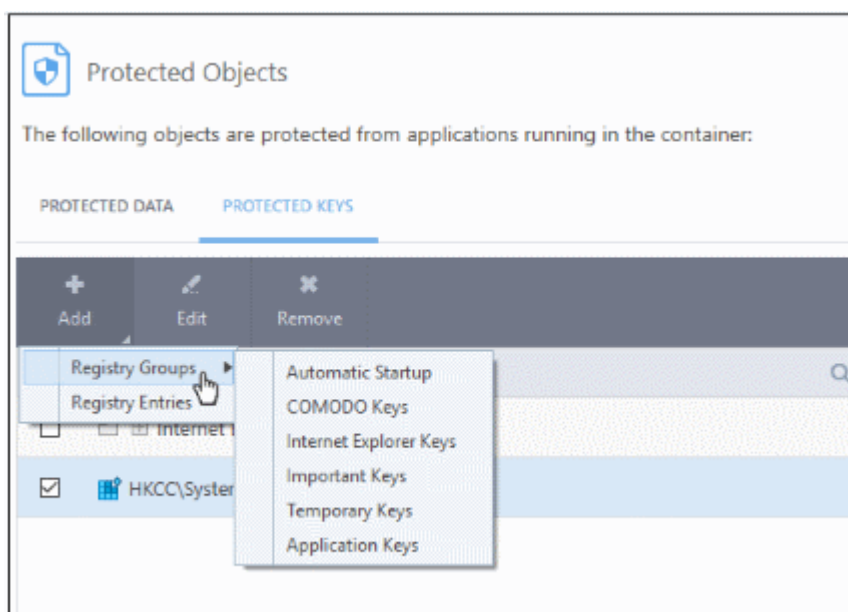


You can add keys individually or by registry group:

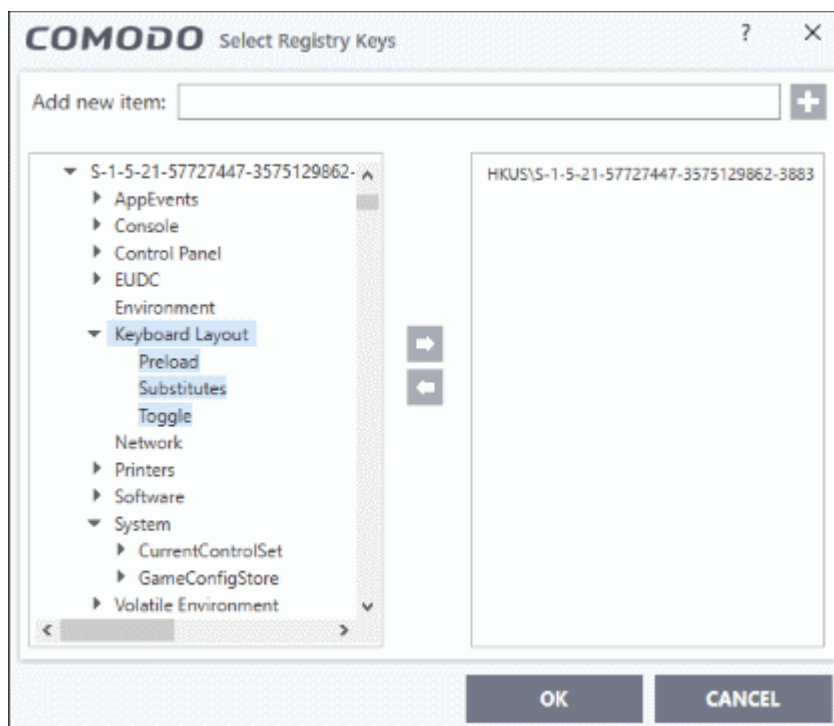
- **Add Registry Groups** - Adding a registry group allows you to batch select and import groups of important registry keys. Comodo Client Security provides the following, pre-defined groups - 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.

You can also create custom registry groups containing keys you wish to protect. See **Registry Groups** in the **HIPS Groups** section if you want to read more on this interface.

- To add a new group, click the 'Add' button > 'Registry Groups' and select the predefined group from the list and click 'OK'



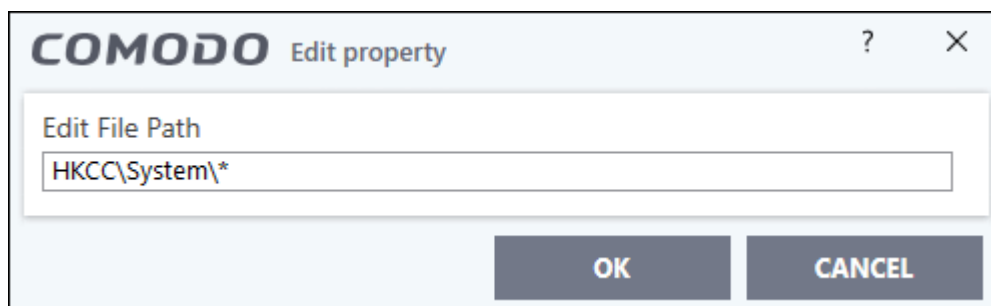
- **Add individual Registry Keys**
 - Click the 'Add' button and then select 'Registry Entries'
 - Choose a key on the left then click the right arrow to add it to the protected list:



- Alternatively, you can type the key name in the field at the top then click '+' and click 'OK'

Edit an item in the Registry Protection list

- Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Update as required and click 'OK'

Note: The 'Registry Groups' cannot be edited from this interface. You can edit only from **Registry Groups** in **HIPS Groups** section.

To delete an item from Registry Protection list

- Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the protected register list.

6.6. Containment Configuration

- If CCS encounters a file that has a trust status of 'Unknown' then you have the option to automatically run that file in the container. 'Unknown' files are those that are not rated as malware (not blacklisted), but also not rated as safe (not whitelisted).
- Files running in the container are isolated from the rest of your computer. This eliminates the possibility of them causing damage or accessing your data.
- The containment configuration section lets you define what level of restriction is applied to such 'Unknown' files. You can choose from:
 - Run with restricted access to operating system resources
 - Run completely isolated from your operating system and files on your computer
 - Completely prevent it from running
 - Allow to run outside the containment environment without restriction

See '[Auto-Containment Rules](#)' for more information about defining containment rules.

Applications running in the container are not allowed to write or save files to your local system. CCS creates a special folder called 'Shared Space' at 'C:/Program Data/Shared Space' so you can pass files between the container and your real system. This data can also be accessed by non-contained applications.

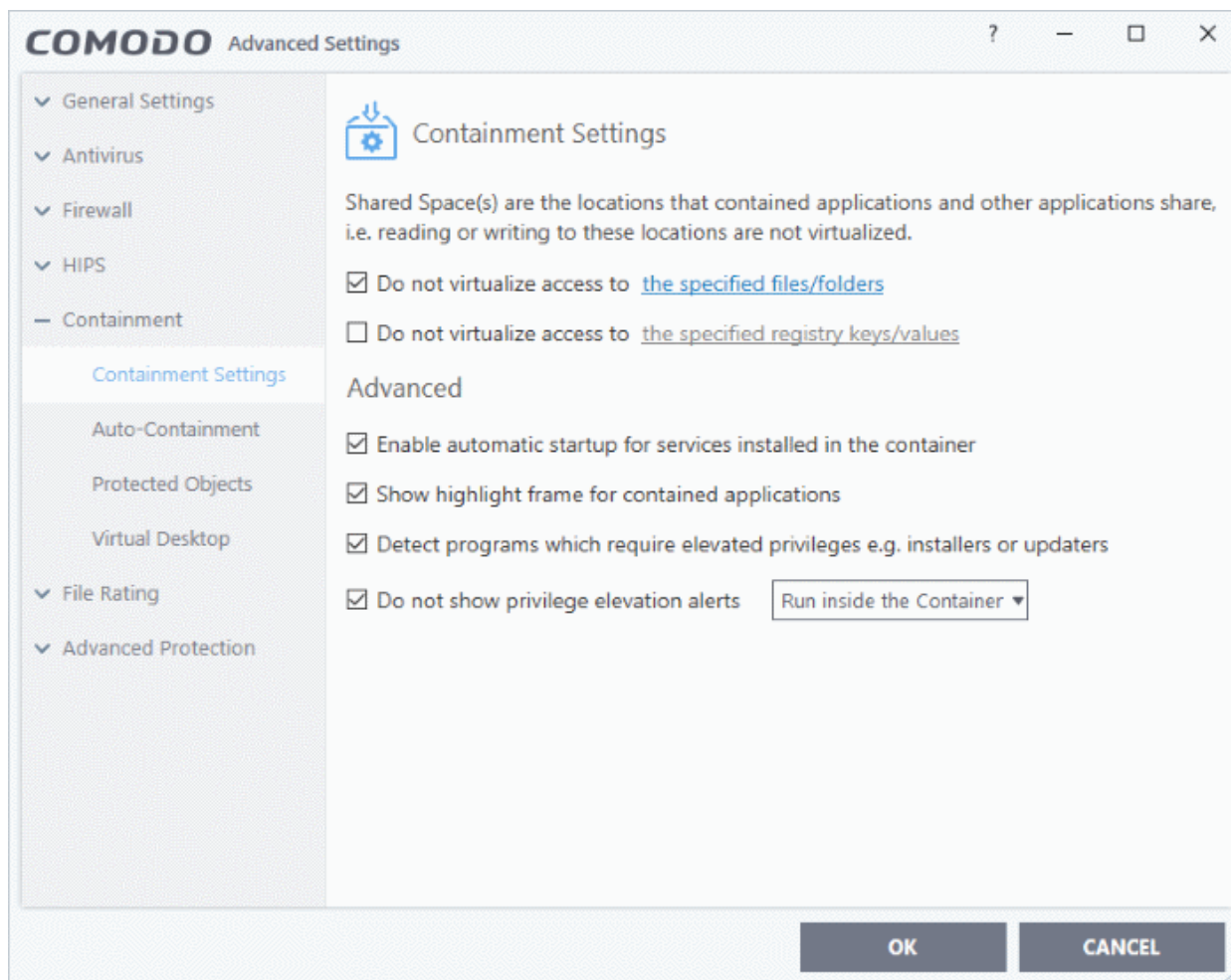
- See '[Containment - An Overview](#)' for background information about the containment process.
- See '[Unknown Files: The Scanning Processes](#)' for more information about how CCS determines the reputation of a file.

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

- Windows XP 64 bit
- Windows Server 2003 64 bit

To open the containment interface:

- Click 'Settings' on the CCS home \ tasks screen to open the 'Advanced Settings' interface.
- Click 'Containment' on the left:



The 'Containment Settings' and 'Auto-Containment' options allow you to quickly configure overall containment behavior and create rules for auto-contained selected programs.

See the following sections for more details:

- [Containment - An Overview](#)
- [Unknown Files: The Scanning Processes](#)
- [Configuring the Containment Settings](#)
- [Configuring Rules for Auto-Containment](#)
- [Protected Objects – Containment](#)
- [Virtual Desktop Settings](#)

6.6.1. Containment - An Overview

- The container is an isolated operating environment for unknown and untrusted applications.
- Running an application in the container means that it cannot make changes to other processes, programs or data on your local computer. Applications in the container are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of your real system.

- This delivers a smooth user experience by letting unknown applications run as normal while denying them the potential to cause damage.
- After an unknown application has been placed in the container, CCS also submits it to Valkyrie for behavior analysis. Valkyrie tests include:
 - Static analysis
 - Dynamic analysis
 - Valkyrie plugins and embedded detectors
 - Signature based detections
 - Trusted vendor and certificate validation
 - Reputation system
 - Human expert analysis
- If Valkyrie discovers that a file is malicious then it is added to the antivirus black list. The file is quarantined on the local machine and the user is alerted.
- Users can print documents from within the container. This is useful, for example, if a suspicious PDF has valid information that should be printed.

By uniquely deploying 'containment as security', CCS offers improved security, fewer pop-ups and greater ease of use than ever before.

6.6.2. Unknown Files: The Scanning Processes

- When an executable is first run it passes through the following CCS 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 CCS (and therefore not 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**
 - Because the software publisher is rated as 'Trusted' in the **Vendor List**.
 - By the user granting the installer elevated privileges (CCS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CCS regards the installer and all files generated by the installer as safe)
- Additionally, a file is not 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**
 - Step 1 - Comodo File Look-up Server (FLS)**
 - In order to try to establish whether a file is safe or not, CCS will first consult Comodo's File Look-Up Server (FLS) to check the 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 CCS
- 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 CCS
 - 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'.

Step 2 - Vendor Rating

- If a file is still 'unrecognized' after FLS check up, CCS checks the rating of the software publisher.
 - **'Trusted' vendor rating** - CCS will award trusted status to the file.
 - **'Malicious' vendor rating** - CCS will award malicious status to the software file and place it in quarantine.
 - **'Unrecognized' vendor rating** - The file will keep its unknown status and is run in the container. The file is also sent to Valkyrie for analysis.

Step 3 - Valkyrie Analysis

- Applications that have neither file rating nor vendor rating are first contained then submitted to Valkyrie for analysis.
- Unrecognized files uploaded to Valkyrie undergo a battery of static and dynamic analysis. At the end of the automated tests, files are analyzed by human experts for confirmation.
- Valkyrie returns its verdicts to CCS which will quarantine, allow or contain the file as appropriate.
- [Click here](#) to view Valkyrie online help guide

Important Note: In order for the software to submit unknown files to our file rating and malware analysis servers, please make sure the following IP addresses and ports are allowed on your network firewall:

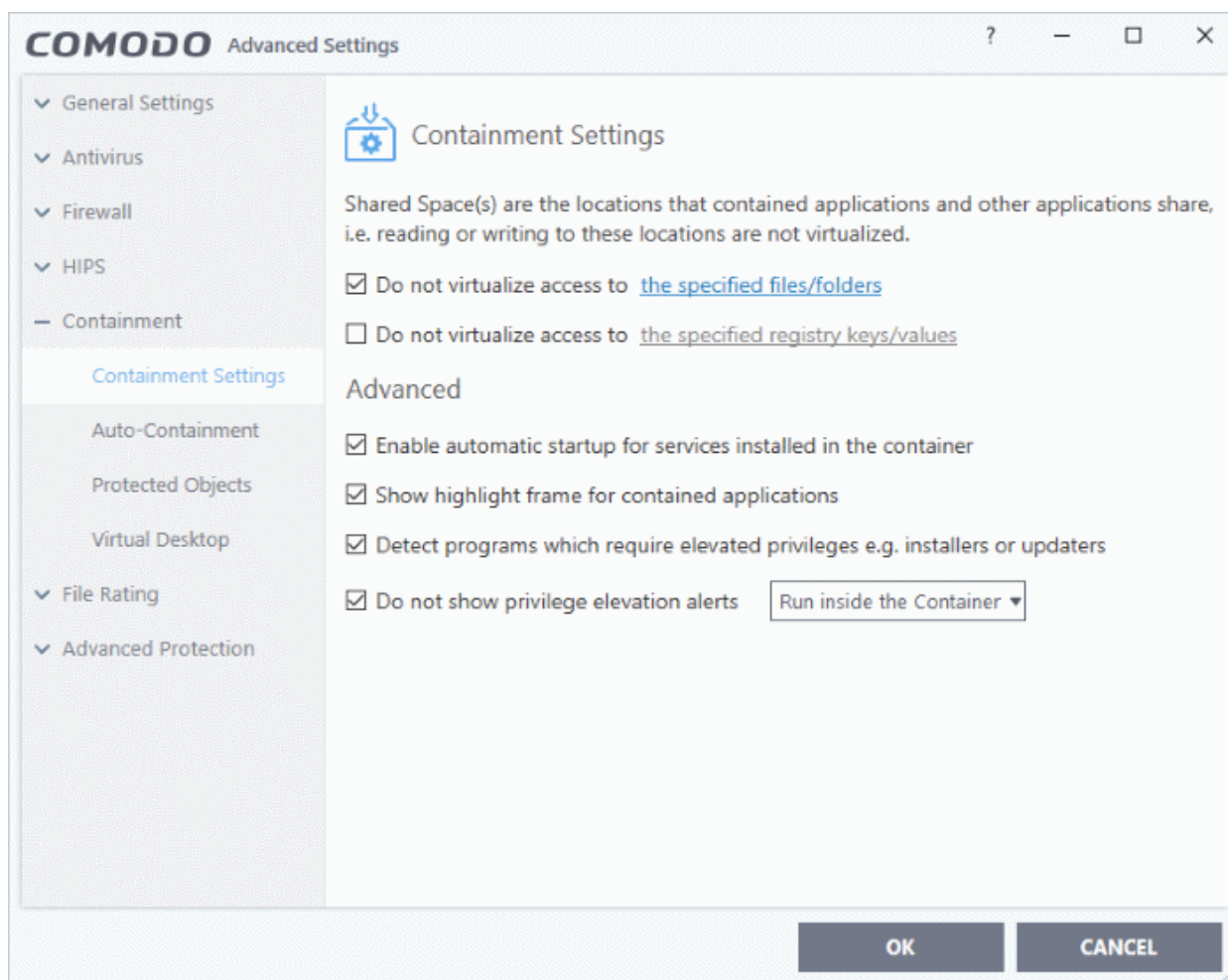
- To allow communication with our FLSs:
 - IPs that need to be allowed:
 - 91.209.196.27
 - 91.209.196.28
 - 199.66.201.20
 - 199.66.201.21
 - 199.66.201.22
 - 199.66.201.25
 - 199.66.201.26
 - Ports that need to be allowed: 53 UDP and 80 TCP
 - Direction: Outgoing (Endpoints to FLSs)

6.6.3. Containment Settings

The 'Containment Settings' panel lets you configure how proactive the auto-containment feature should be, and which types of files it should check.

Open the 'Containment Settings' section

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Containment' > 'Containment Settings' on the left:



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

- **Shared Space Settings** - Shared space lets you swap files between the container and your real computer. Files downloaded or generated by contained applications that you wish to access from your real system should be downloaded to the shared space.
- **Advanced Settings** - Configure containment alert settings and enable automatic startup services for programs in the container.

Shared Space Settings:

'Shared Space' is a dedicated area on your local drive which contained applications are allowed to write to. Files in shared space can also be accessed by non-contained applications. For example, any files or programs you download via a contained browser that you wish to be able to access from your real system should be downloaded to the shared space. This folder is located by default at 'C:/Program Data/Shared Space'.



The desktop shortcut provides quick access to shared space:

You can also access shared space via the CCS interface by clicking 'Tasks' > 'Containment Tasks' > 'Open Shared Space'.

Exclusions

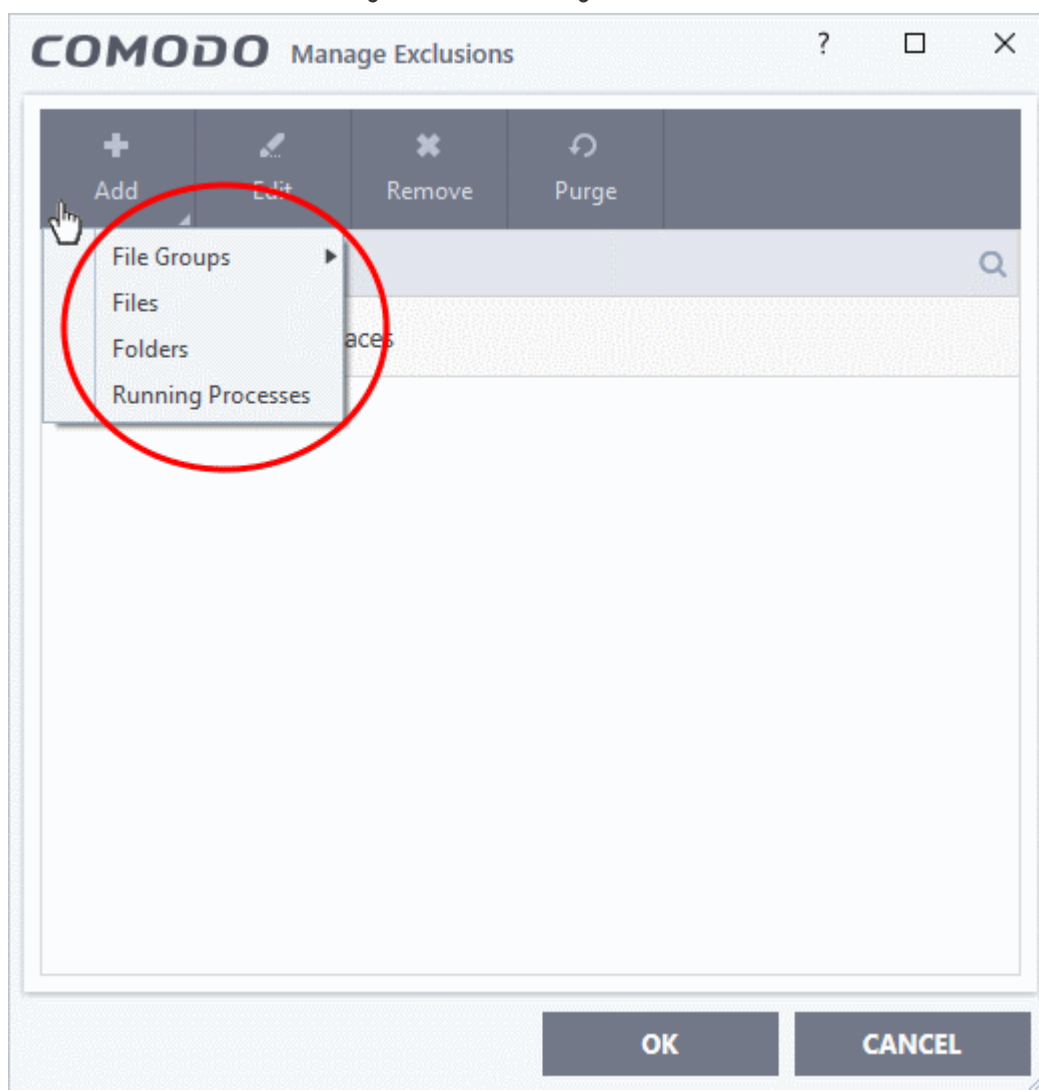
By default, contained applications can access folders and files on your 'real' system but cannot modify them. However, you can define exclusions to this rule by using the 'Do not virtualize access to...' links.

To define exclusions for files and folders

- Enable 'Do not virtualize access to the specified files/folders' then click the 'specified files/folders' link.

The 'Manage Exclusions' dialog will appear with a list of defined exclusions. You can search for a specific item from the list by clicking the search icon at the far right of the column header and entering the name of the item in part or full.

- Click the 'Add' button in the 'Manage Exclusions' dialog.



- **Files** - Allows you to specify files or applications that contained applications are able to access
- **Folders** - Specify a folder that can be accessed by contained applications
- **File Groups** - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exception for all files

with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd. See **'File Groups'**, for more details on file groups.

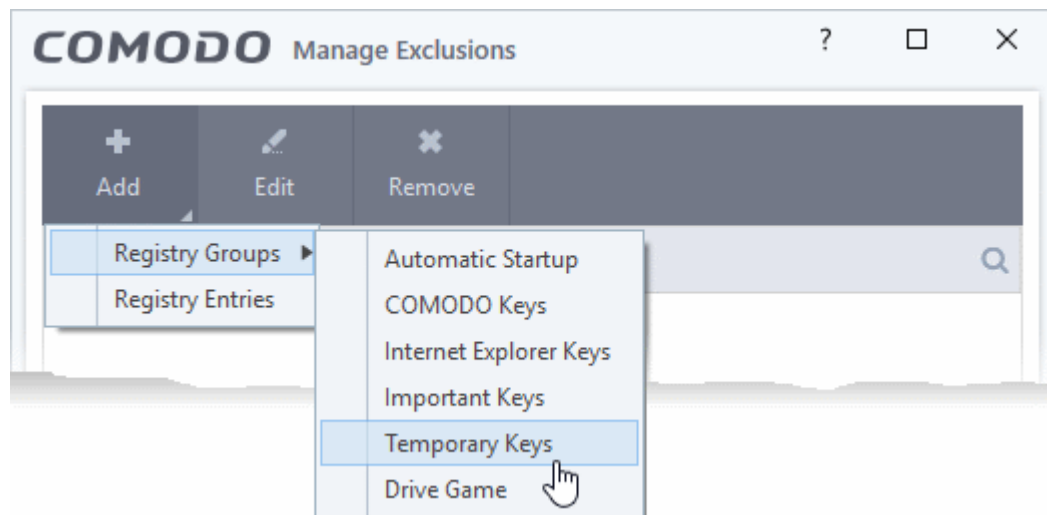
- **Running Processes** - Allows you to choose a process from the list of currently running processes. The parent application of the process will be added as an exclusion.
- To edit an exception, select it from the list, click the handle to open the tools menu then select 'Edit'.
 - Change file or folder location path and click 'OK'
- Click 'OK' to implement your settings

To define exclusions for specific Registry keys and values

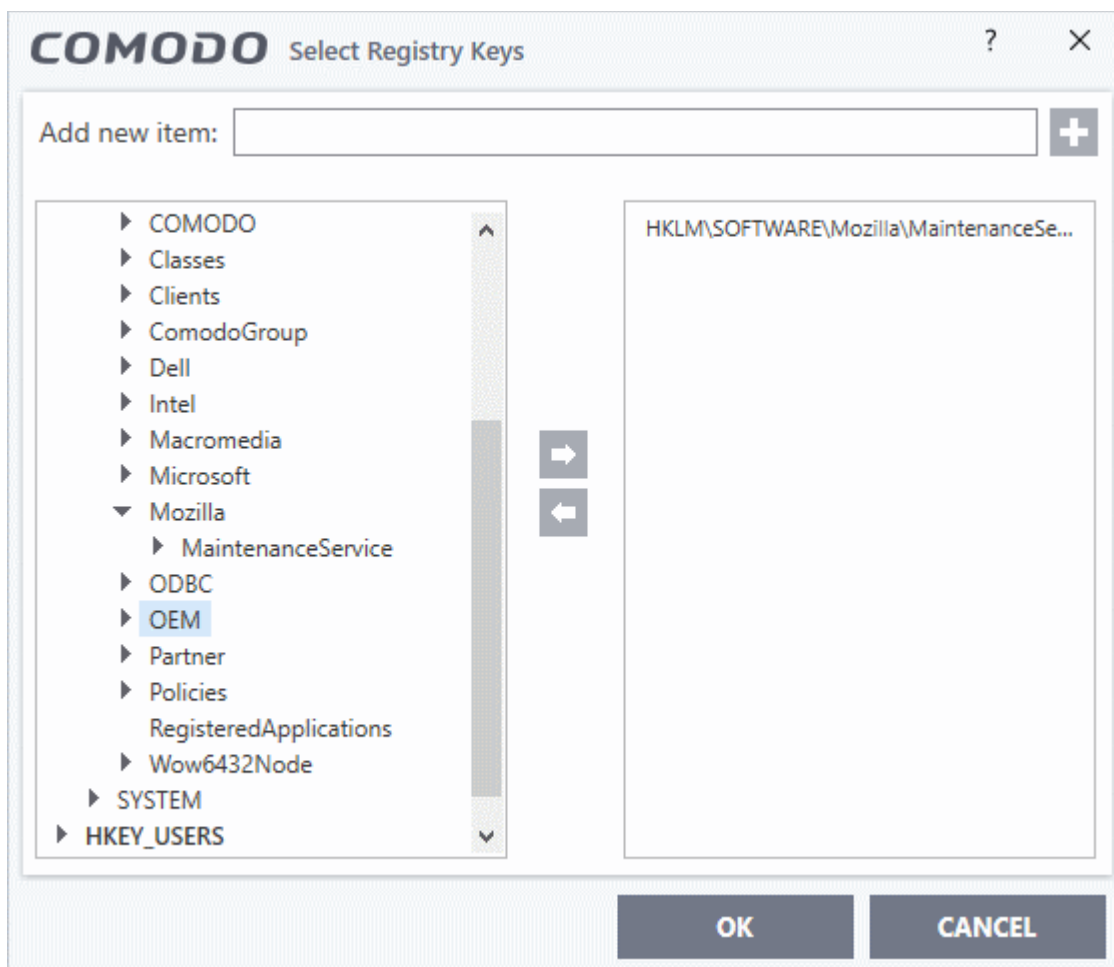
- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the link 'the specified registry keys/values'.

The 'Manage Exclusions' dialog will appear with the list of excluded registry keys and values. You can search for a specific item from the list by clicking the search icon at the far right of the column header and entering the name of the item in part or full.

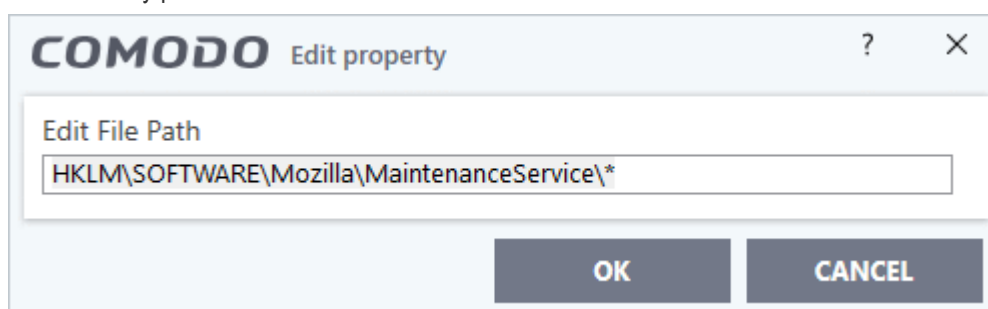
- Click the 'Add' button in the 'Manage Exclusions' dialog.



- **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exclusions. See **'Registry Groups'** to find out more about CCS registry groups.
- **Registry Entries** - Opens an interface that allows you to quickly browse Windows registry keys and add them as exclusions:



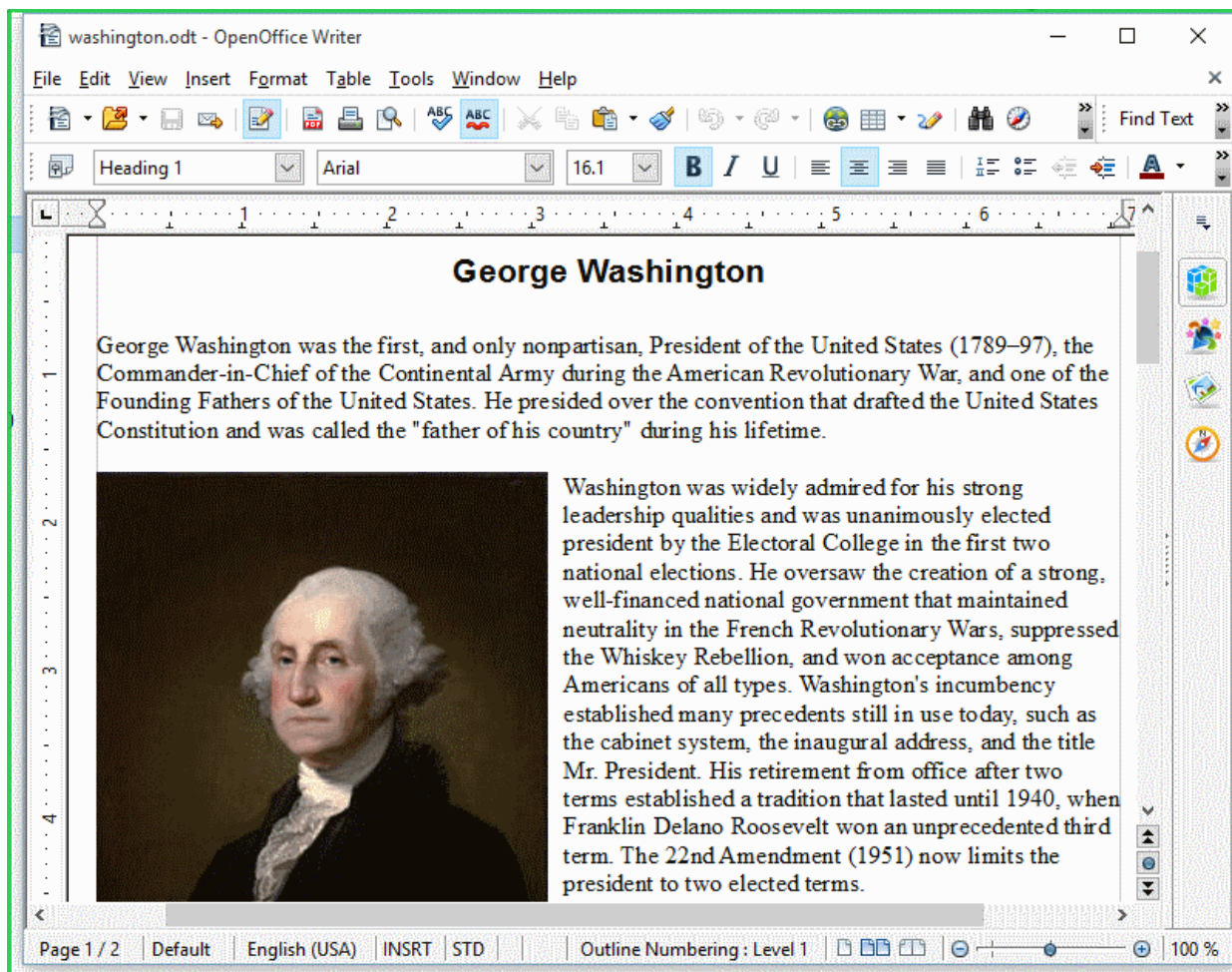
- Click 'OK' to implement your settings.
- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.
- Edit the key path and click 'OK'.



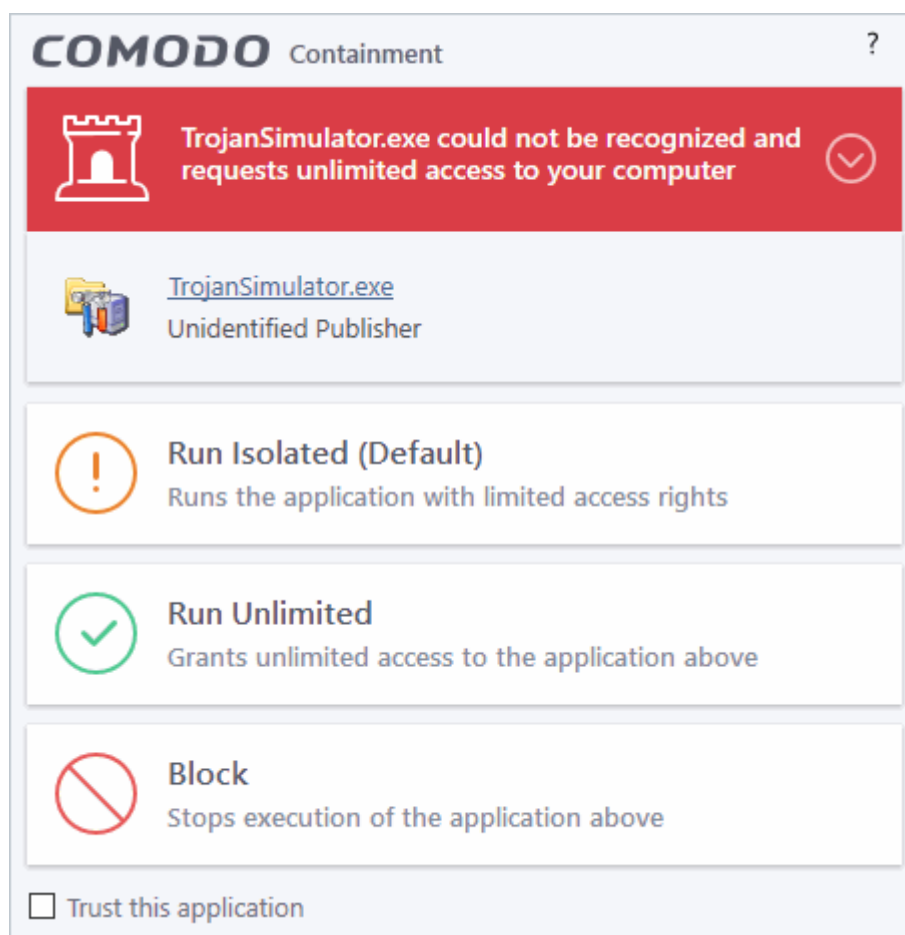
Advanced Settings:

- **Enable automatic startup for services installed in the container** - CCS permits contained services to run at Windows startup only if this option is enabled. Clear this check-box if you do not want those services to run at Windows Startup. (**Default = Enabled**)
- **Show highlight frame for contained applications** - If enabled, CCS displays a green border around the windows of programs that are running inside the container. (**Default = Enabled**)

The following example shows an .odt document opened with a contained instance of OpenOffice Writer:



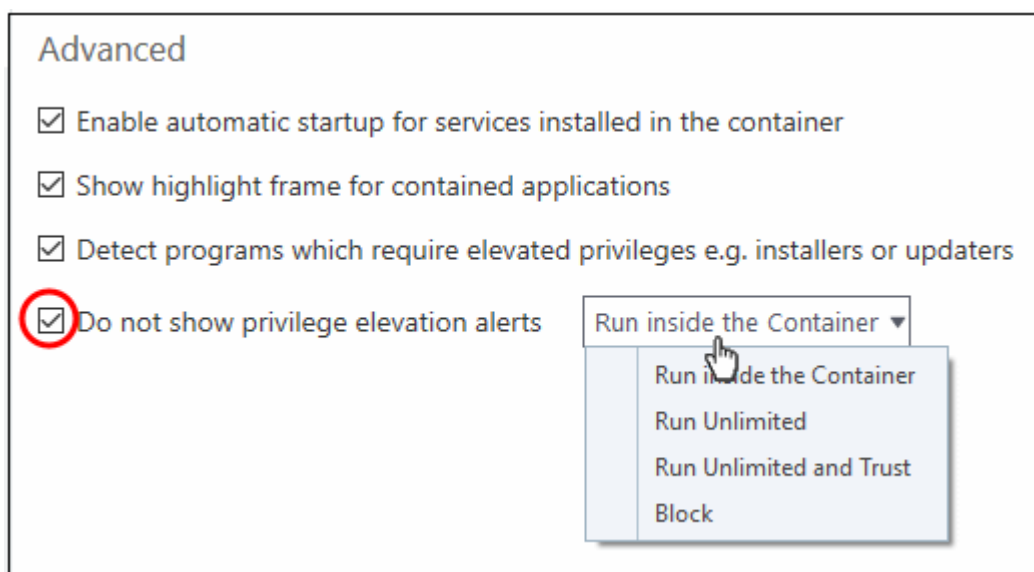
- **Detect programs which require elevated privileges, e.g., installer or updaters:** Instruct the container to show alerts when an installer or updater requires admin privileges to run. An installer that is allowed to run with admin privileges is permitted to make changes to important areas of your computer such as the registry. See '[Understanding Security Alerts](#)' for more details.



You can decide whether or not to allow the installer/updater from the options in the alert.
(Default=Enabled)

- **Do not show privilege elevation alerts:** CCS will not show alerts (as shown above) when a new or unrecognized application requires admin privileges to run.

On selecting this option, you need to choose the action to be taken by the container from the drop-down.
(Default=Disabled)

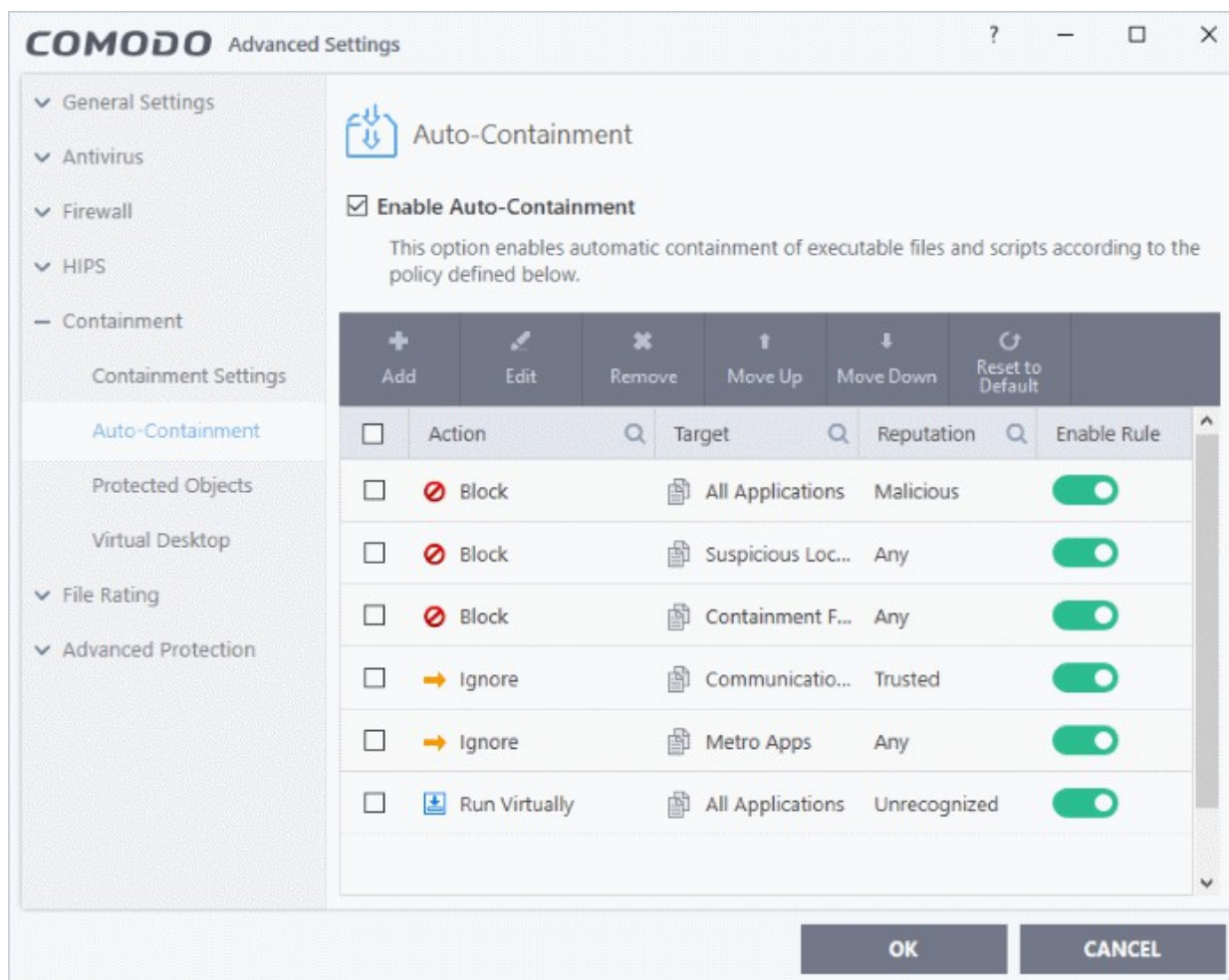


6.6.4. Auto-Containment Rules

- The 'Auto-Containment' panel lets you add and define rules for programs that run in the container.
- Auto-containment rules let you specify whether programs should be blocked, ignored (allowed to run normally), run restricted, or run virtually (contained).
- A contained application has much less opportunity to damage your computer because it is isolated from your operating system, important files and personal data. This allows you to safely run applications that you are not 100% sure about.
- Programs running in the container have a green border around them.
- CCS ships with a set of pre-configured containment rules which provide maximum protection against unknown, potentially malicious applications. You can also create your own.

Open the Auto-Containment panel

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'Containment' > 'Auto-Containment' on the left:



The 'Auto-Containment' panel contains configuration options and a list of currently defined auto-contained rules. You can add new rules and manage existing rules from this panel.

General Settings

- **Enable Auto-Containment** - Allows you to enable or disable the Containment. If enabled, the applications are run inside the container as per the rules defined. (**Default = Enabled**)

Containment Rules

Containment Rules - Column Descriptions	
Column Header	Description
Action	The operation that the container should perform on the 'Target' if the rule is triggered.
Target	The files, file groups or specified locations on which the rule will be executed.
Reputation	The trust status of the 'Target' files to which the rule will apply. Can be 'Malware', 'Trusted' 'Unrecognized' or 'Any'.
Enable Rule	Allows you to enable/disable the rule.

- CCS ships with a set of pre-defined rules designed to provide maximum protection for your system.
- The following table show the setting for these pre-defined rules:

Predefined Rule no.			1	2	3	4	5	6
Action			Block	Block	Block	Ignore	Ignore	Run Virtually
Target			File Group - All Applications	File Group - Suspicious Locations	File Group - Contained Folders	File Group - Comodo Client - Communication	File Group - Metro Apps	File Group - All Applications
File Reputation			Malicious	Any	Any	Trusted	Any	Unrecognized
File origin	Source of file creation	Application(s)						Any
		Process(s)	Any	Any	Any	Any	Any	Any
		user(s)	Any	Any	Any	Any	Any	Any
	Downloaded from	Any	Any	Any	Any	Any	Any	Any
Age of file			Any	Any	Any	Any	Any	Any
Log Action			On	On	On	On	On	On
Restriction Level			N/A	N/A	N/A	N/A	N/A	Off
Limit Maximum Memory			N/A	N/A	N/A	N/A	N/A	Off
Limit Program Execution Time			N/A	N/A	N/A	N/A	N/A	Off
Quarantine			On	Off	Off	N/A	N/A	N/A
Exclude child processes from the action			N/A	N/A	N/A	Off	Off	N/A

- CCS will consult the containment rules every time you open an application.
- Rules are prioritized from the top of the list downwards. The rule nearer the top will prevail in the event of a conflict in settings.
- You can re-prioritize rules using the 'Move Up' and 'Move Down' buttons at the top of the list.

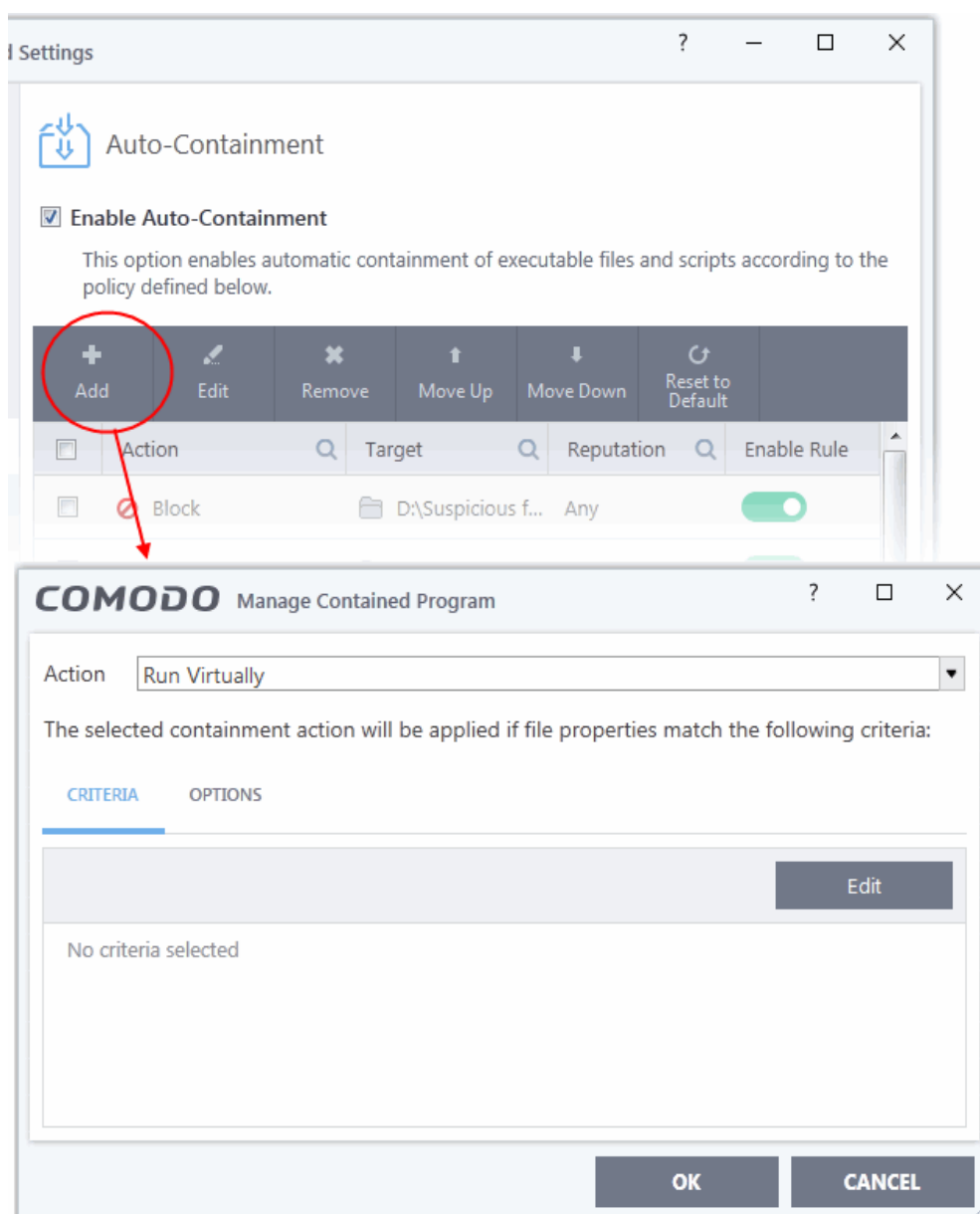
Add an Auto-Containment Rule

Auto-containment rules can be created for:

- A single application,
- For all applications in a folder or file group
- For running processes
- For applications based on their file or process hash.

You can specify the action to be taken on the contained file. You can create filters to target very specific file types, or create a simple rules to run a particular application in the container.

- 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:

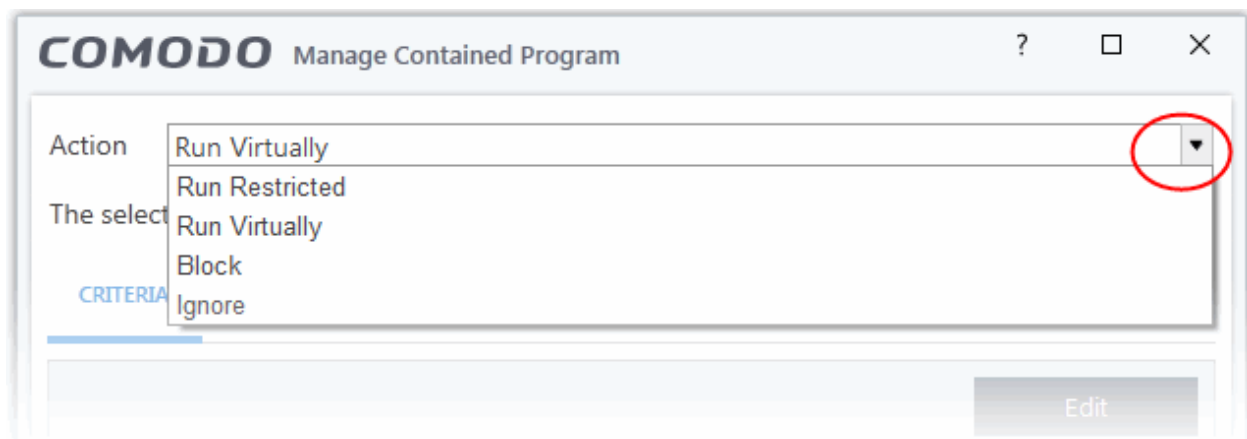
- **Criteria** - Allows you to define conditions upon which the rule should be applied.
- **Options** - Allows you to configure additional actions like logging, setting memory usage and execution time restrictions.

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 for the target files

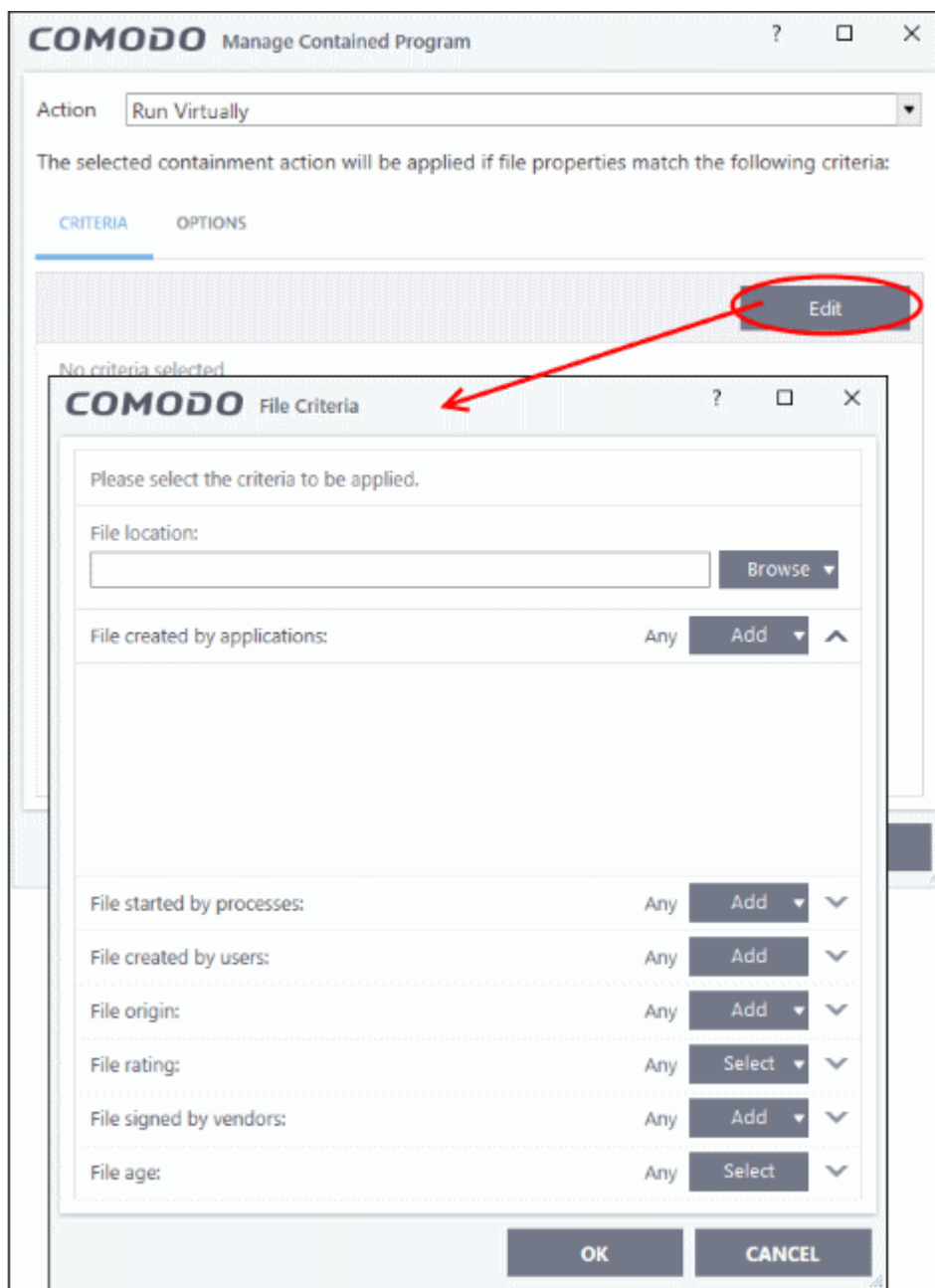
- The next step is to select the targets and configure filter parameters.
- You can apply filters to a target so the action applies only to specific files. For example, you can specify 'All executables' as the target and add a filter so it only affects executables downloaded from the internet.
- Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target and 'File created by specific user' as the filter criteria.

To select the target and set the filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- To add new target and filter criteria, click the 'Edit' button at the far right

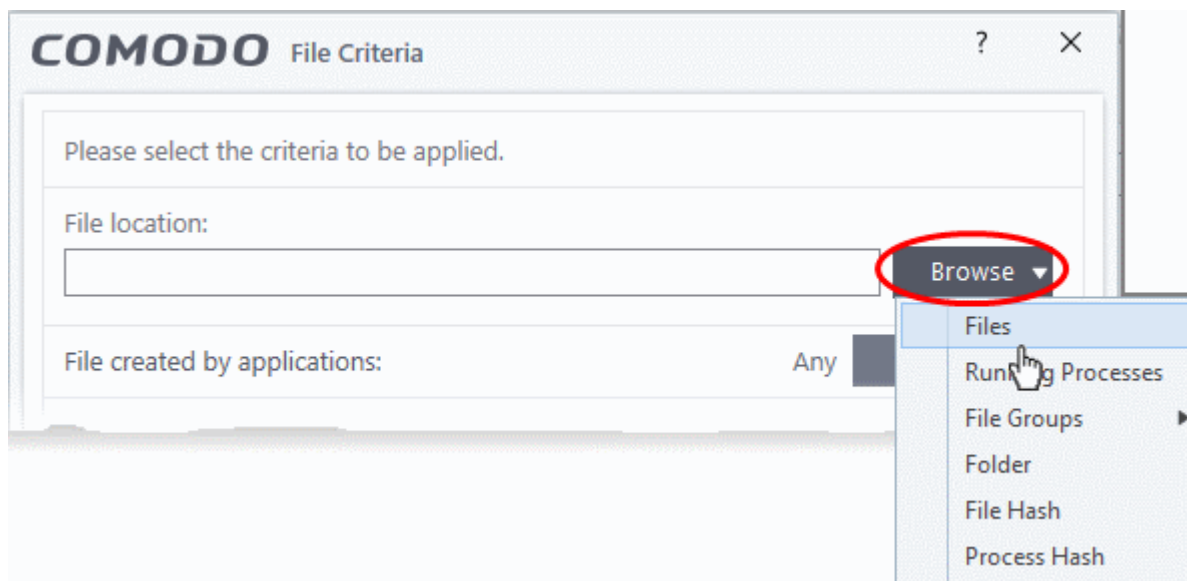


The 'File Criteria' dialog will open. The file criteria dialog allows you:

- **Select the target**
- **Configure the filter criteria**

Select the target

- To select the target, click the 'Browse' button beside the 'File Location' field

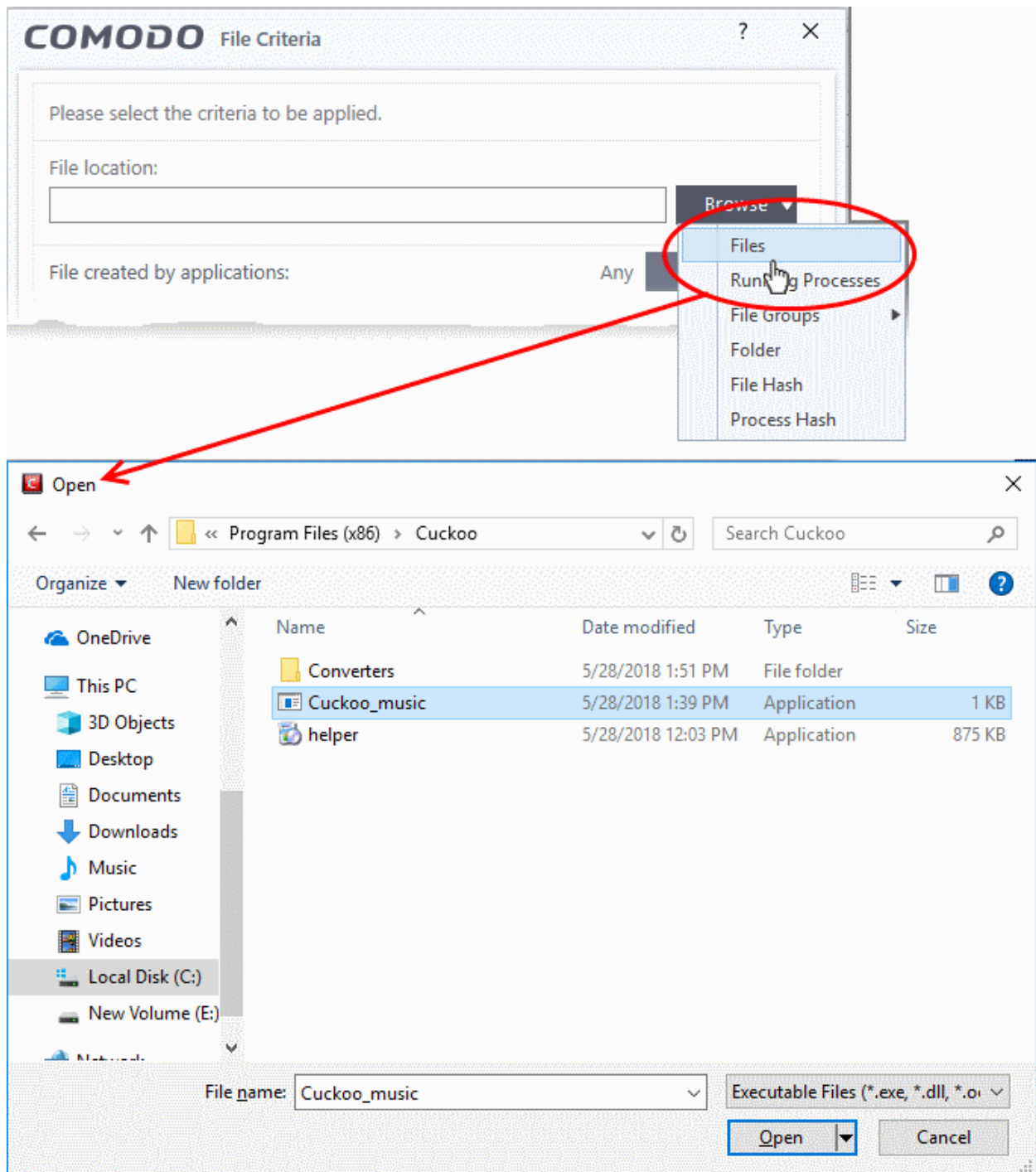


There are six types of target you can add:

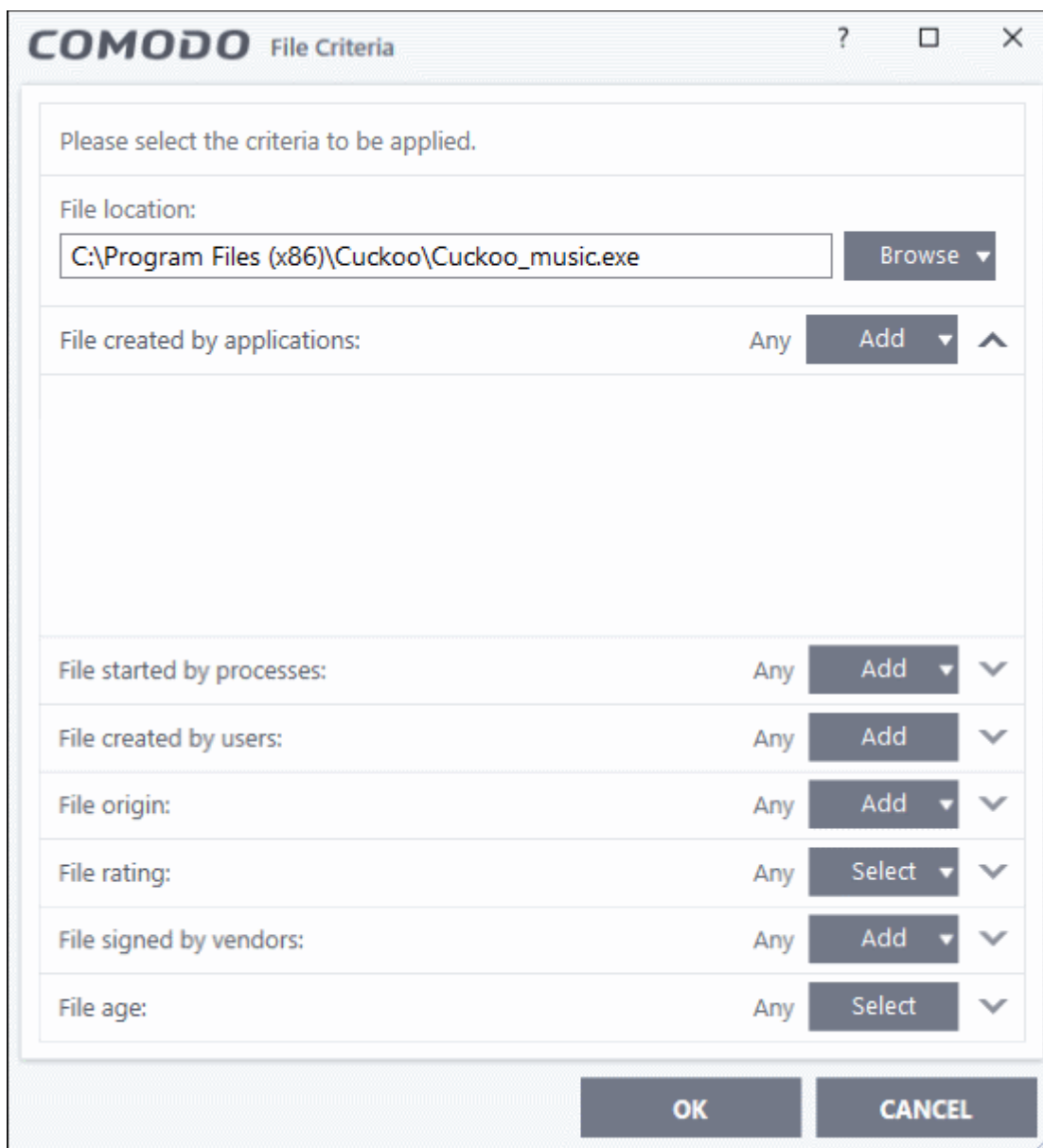
- **Files** – Apply the rule to specific files.
- **Running Processes** – Apply the rule to a process that is currently running on your computer.
- **File Groups** – Apply the rule to predefined file groups. See **File Groups** for help to add or modify a file group.
- **Folder** – Apply the rule to a folder or drive.
- **File Hash** – Create a hash value from a file and use it as the rule target.
- **Process Hash** – Create a hash value of a process and use it as the rule target.

Add an individual File

- Choose 'Files' from the 'Browse' drop-down.



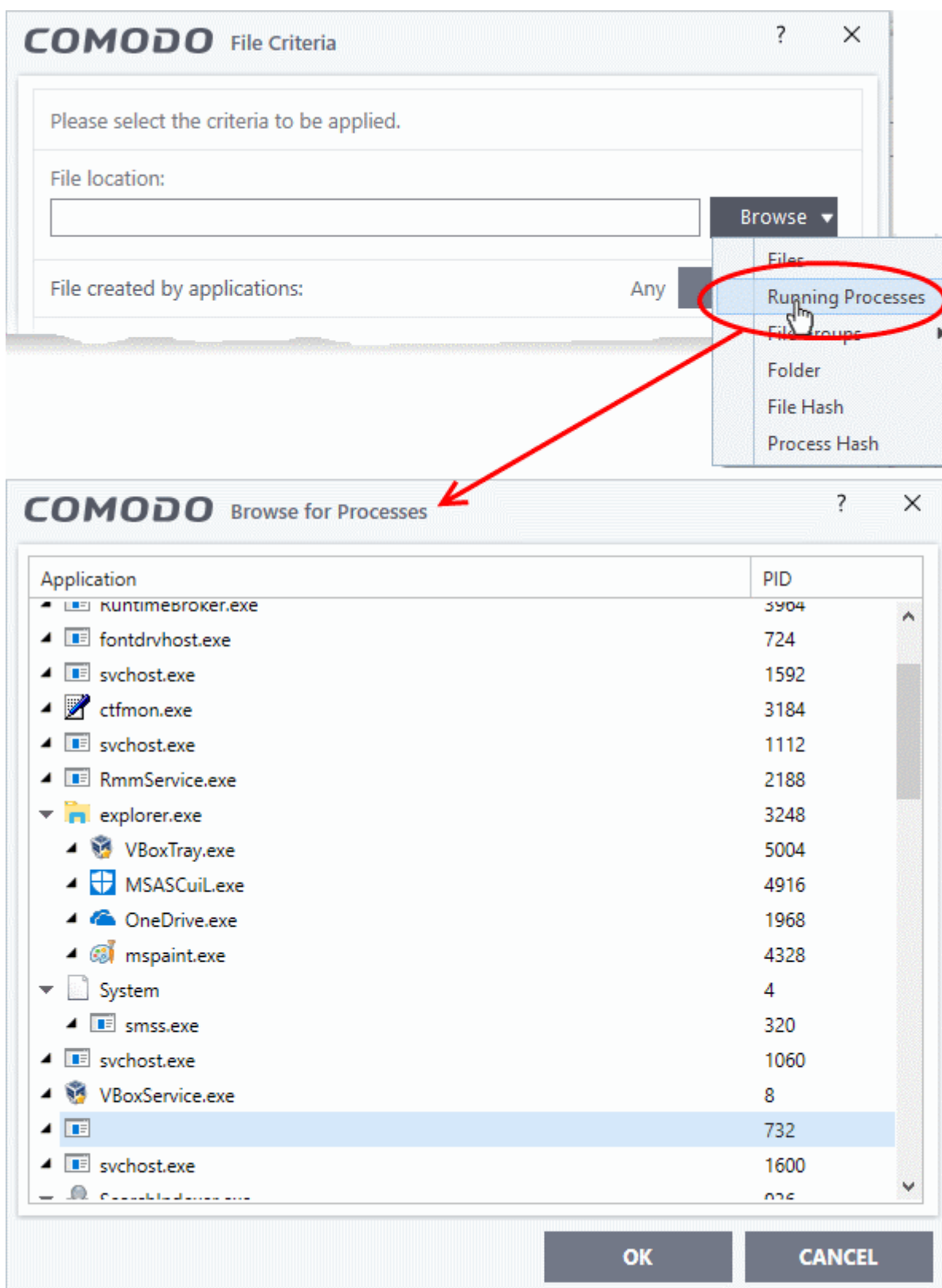
- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'
- The file will be added as target and will be run as per the action chosen in **Step 1**.



- If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'.
- The default values for filter criteria and file rating will be 'Any', and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Add a currently running application by choosing its process

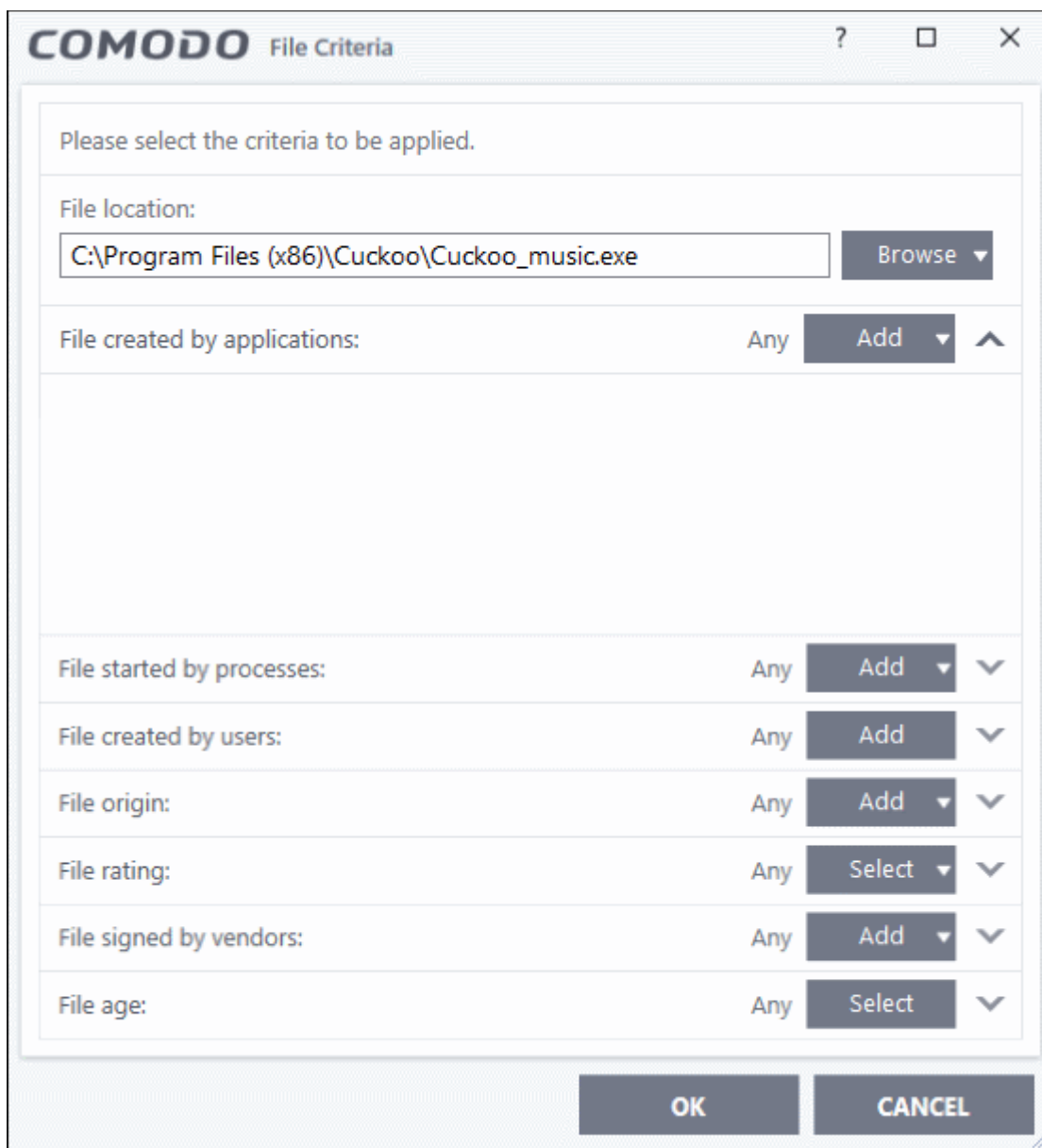
- Choose 'Running Processes' from the 'Browse' drop-down.



This will open a list of all processes running on your computer.

- Select the process you want to add as a target and click 'OK'.

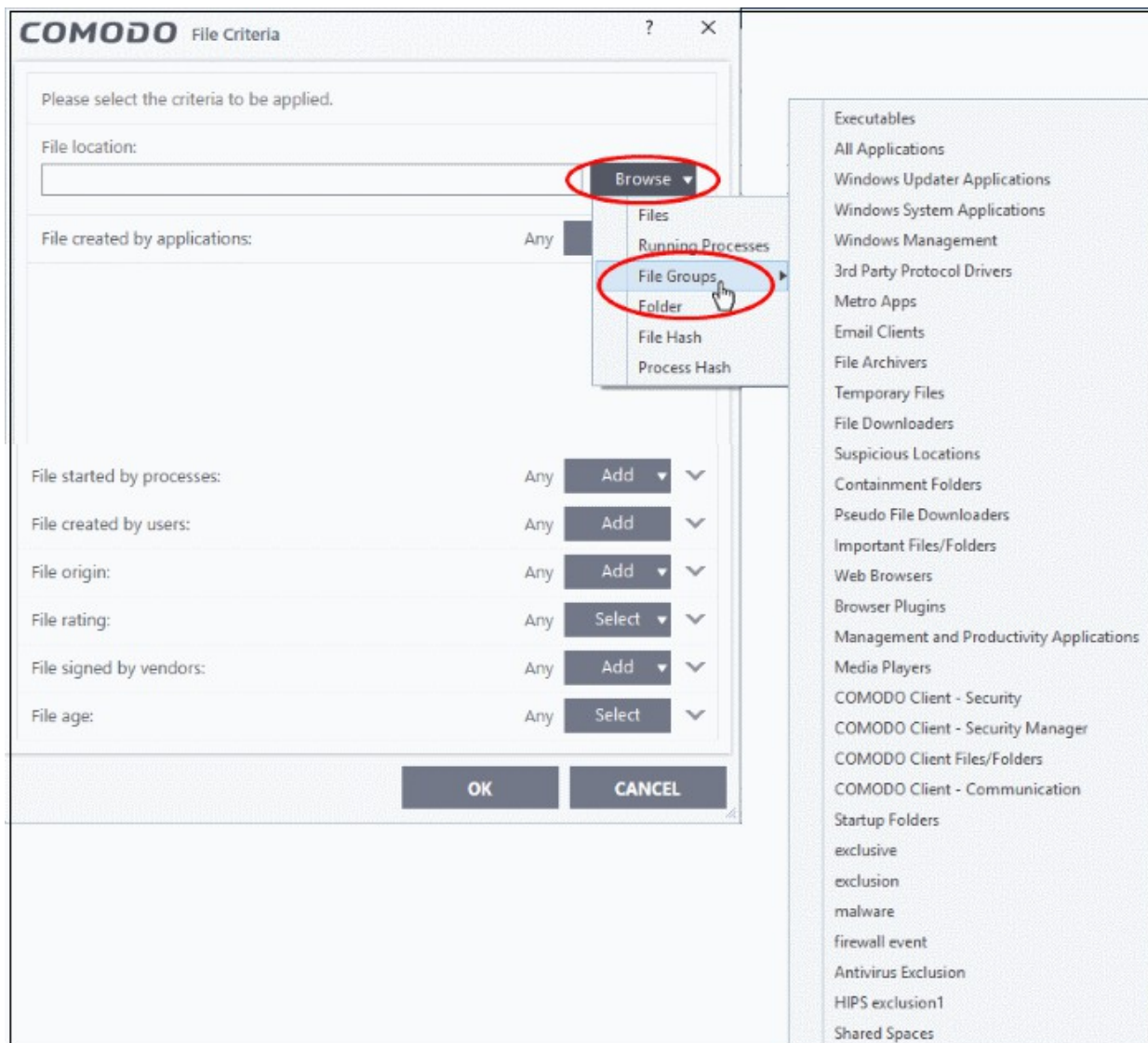
The file will be added as the target. The action chosen in **Step 1** will be applied to the process.



- If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'.
- The default values for filter criteria and file rating will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

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.



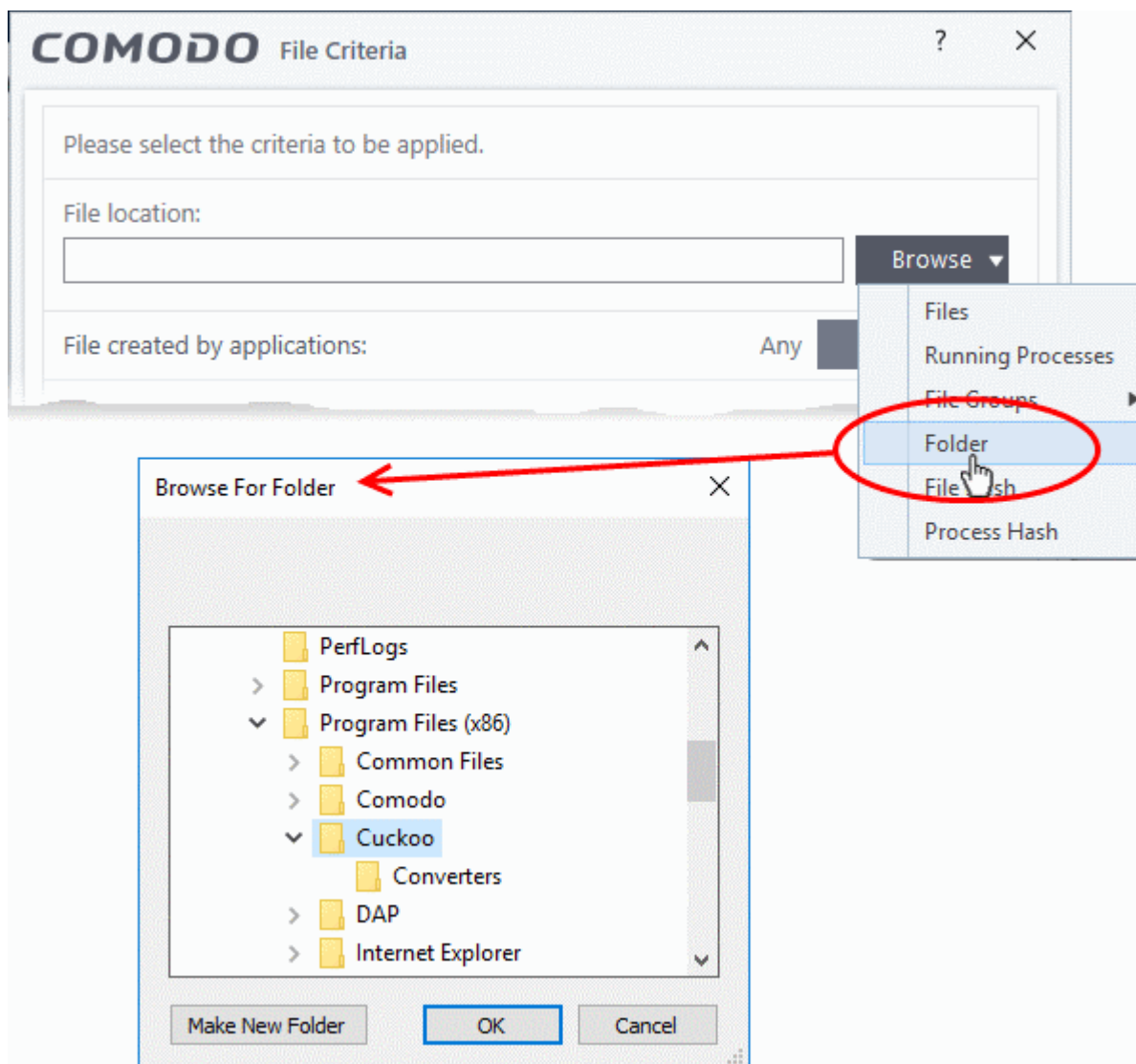
- Select the file group from the drop-down.

The file group will be added as target and will be run as per the action chosen in **Step 1**.

If you want to just add the applications in the file group for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Add a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.



The 'Browse for Folder' dialog will appear.

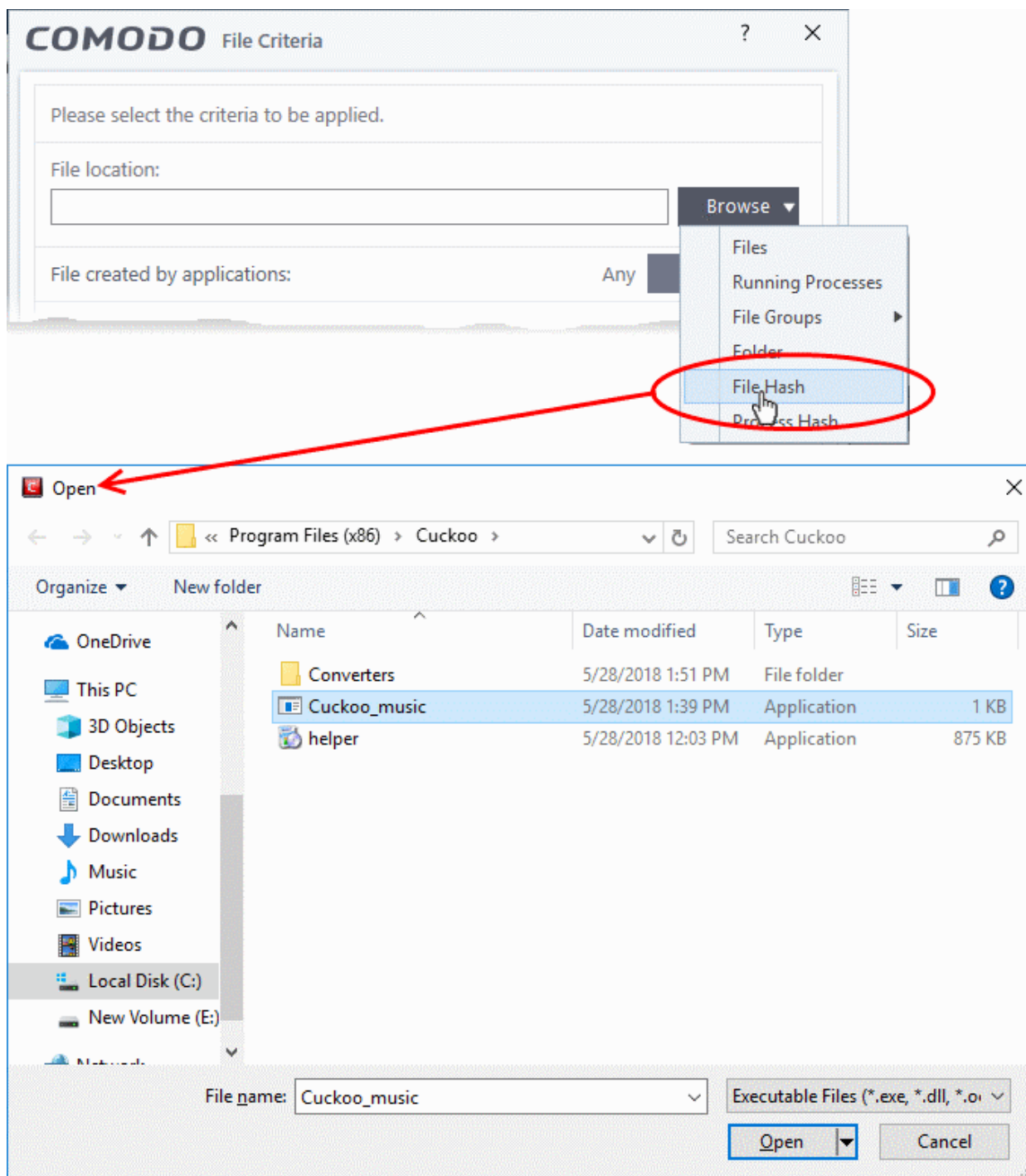
- Navigate to the drive partition or folder you want to add as target and click 'OK'

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**.

If you want to just add the applications in the folder/partition for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Adding a file based on its hash value

- Choose 'File Hash' from the 'Browse' drop-down



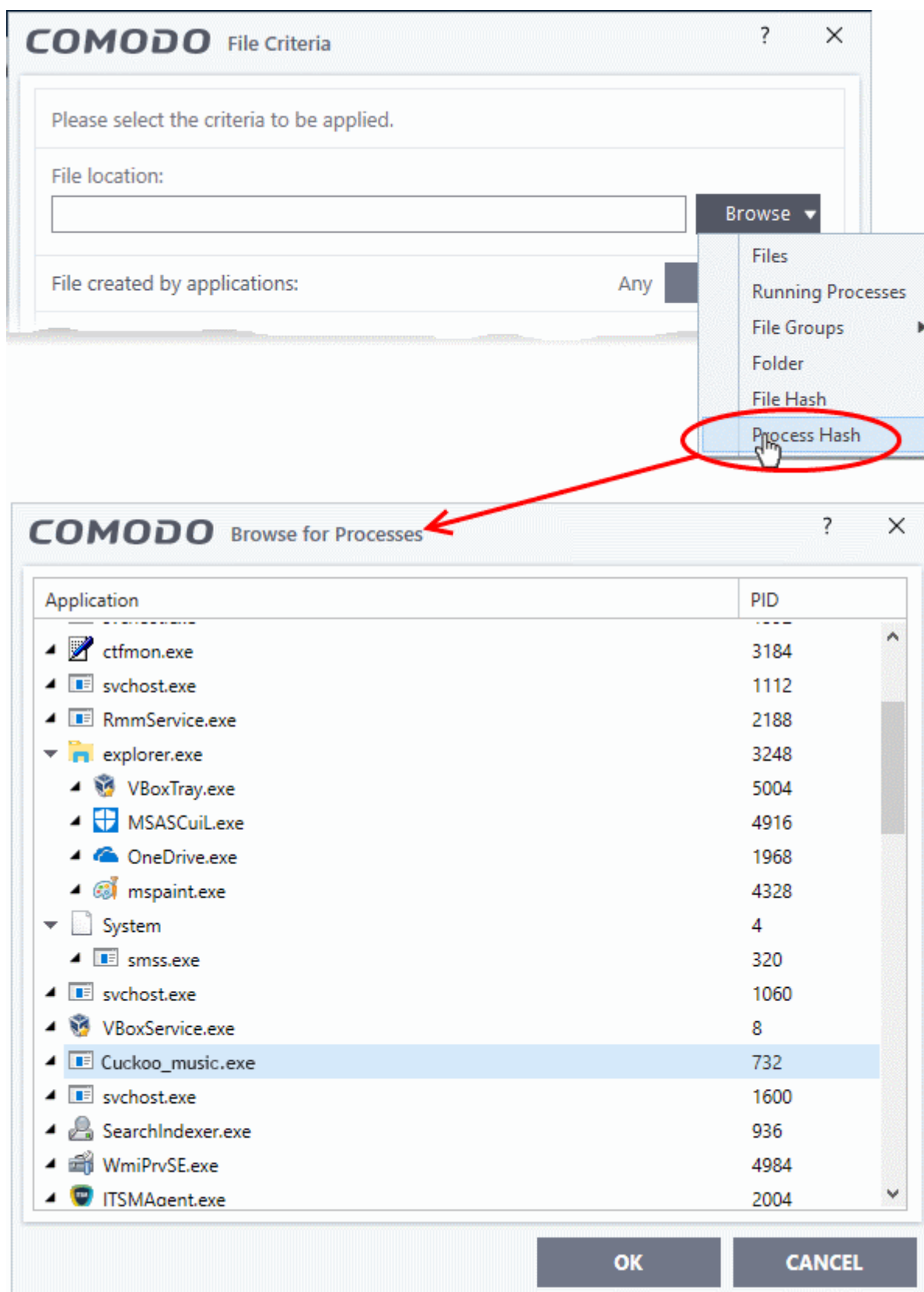
- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'

The file will be added as target and will be run as per the action chosen in **Step 1**.

If you want to just add an application for a particular action as selected in Step 1 without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for **Options** it will be 'Log' when this action is performed'. If required you can configure filter criteria and file rating and Options for the rule.

Adding an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



This will open a list of all processes running on your computer.

- Select the process whose hash you want to add as a target and click 'OK'.

The hash value of the parent executable will be added as the target. The action chosen in **Step 1** will be applied when CCS detects a program with this hash.

If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or

options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for options it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Configure the Filter Criteria and File Rating

You can apply an action to a file if the file's properties match certain criteria.

The available filter criteria are:

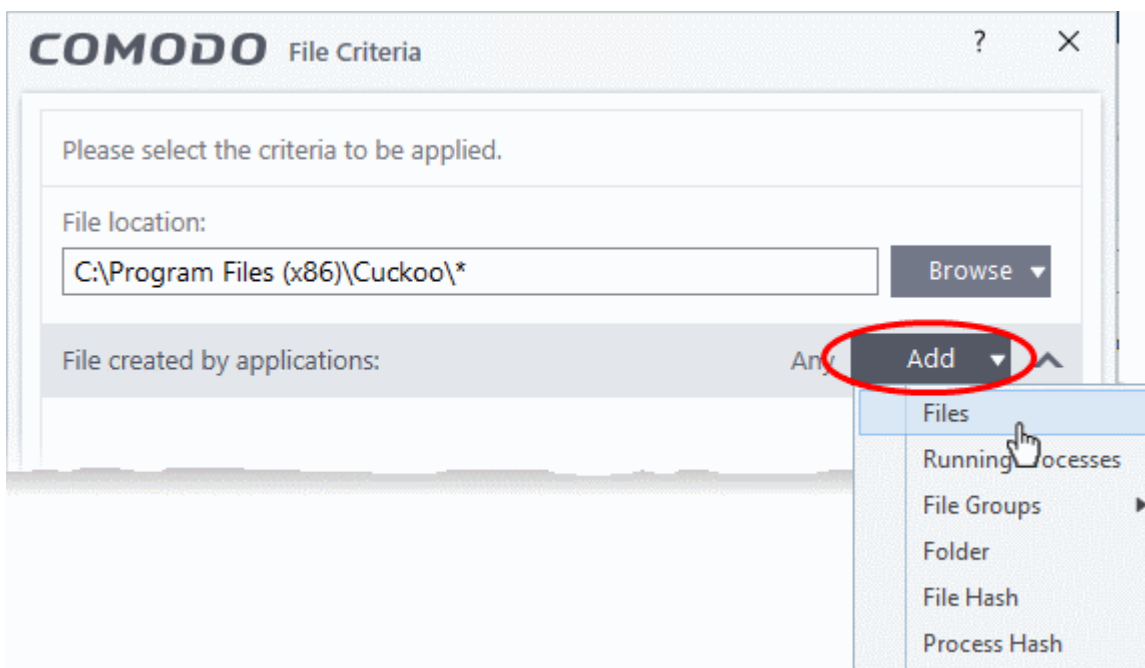
- **Application(s) that created the file**
- **Process(es) that created the file**
- **User(s) that created the file**
- **The origin from which the file was downloaded**
- **The file rating**
- **The file signed by vendors**
- **The age of the file**

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)

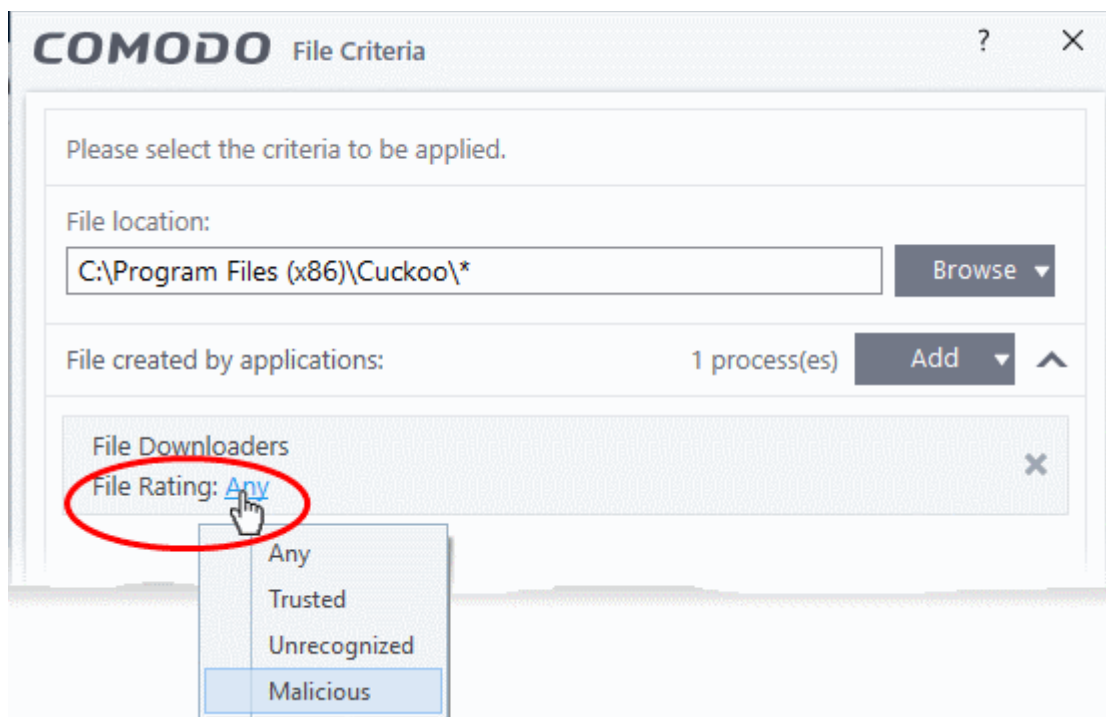
- Click the 'Add' button in the 'File Created by applications' stripe.



- 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



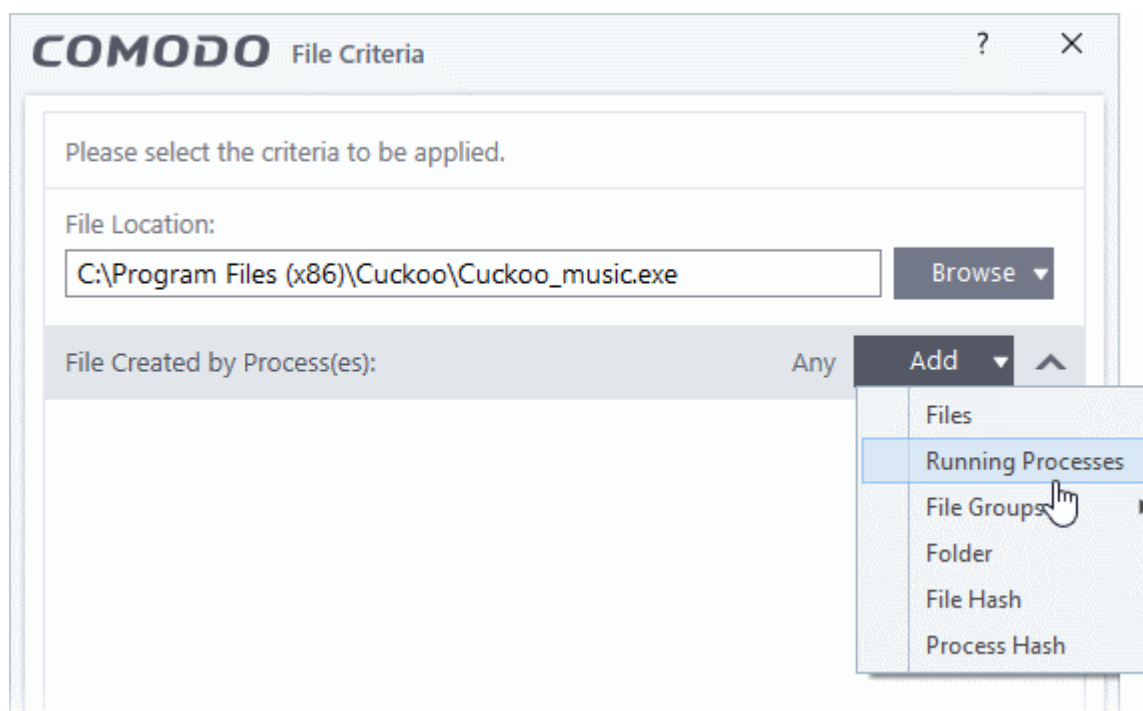
- Repeat the process to add more applications or groups/folders.

Auto-contain a File if it was created by a Specific Process

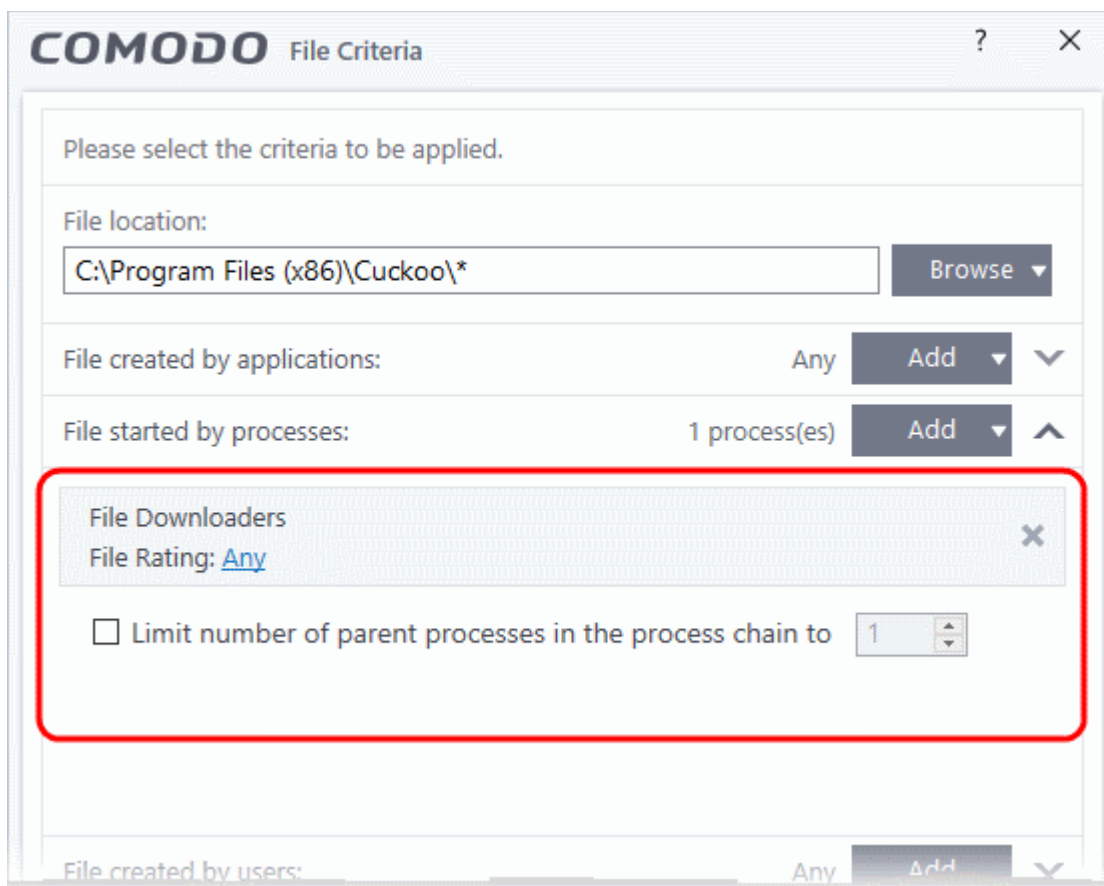
- You can create a filter to apply an action to a file based on its source process.
- Optionally, you can also specify:
 - The file rating of the source. The rule will then only contain a file if its parent process has a certain trust rating.
 - The number of levels in the process chain that should be inspected.

To specify source process(es)

- Click the 'Add' button in the 'File Created by Process(es)' stripe.

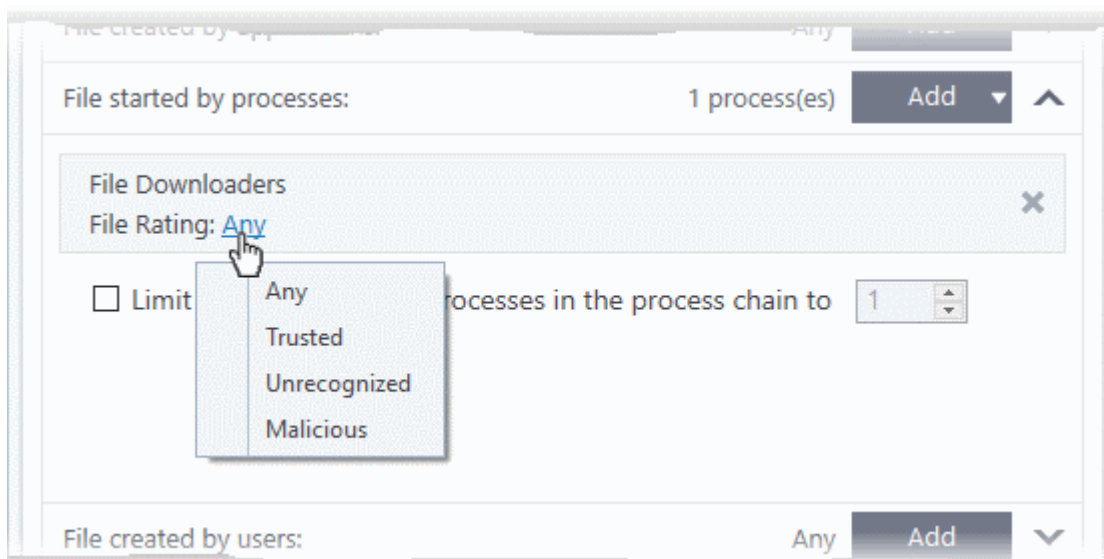


- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.



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



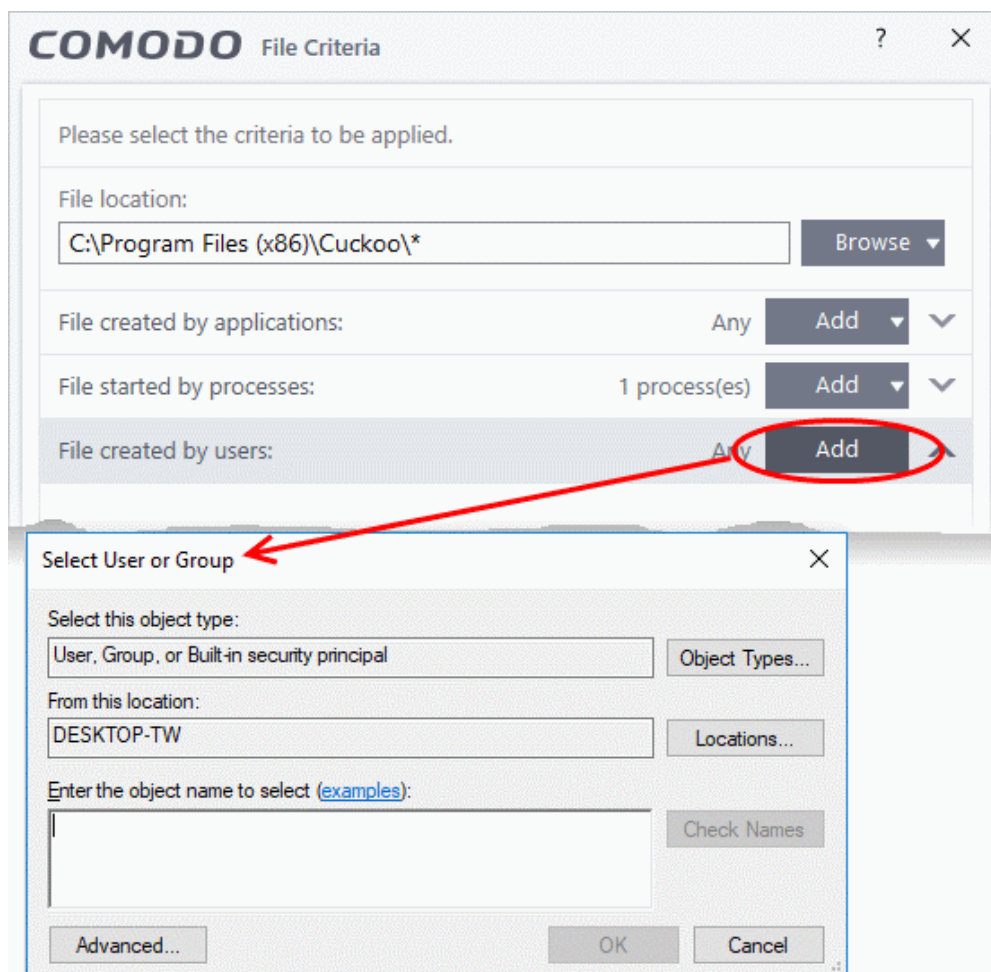
- **'Limit number of parent process(es) in the process chain to'** - Specify how far up the process tree CCS should check when inspecting the file's sources. 1 = will only check the file's parent process. 2 = will check the parent process and the grand-parent process, etc., etc.



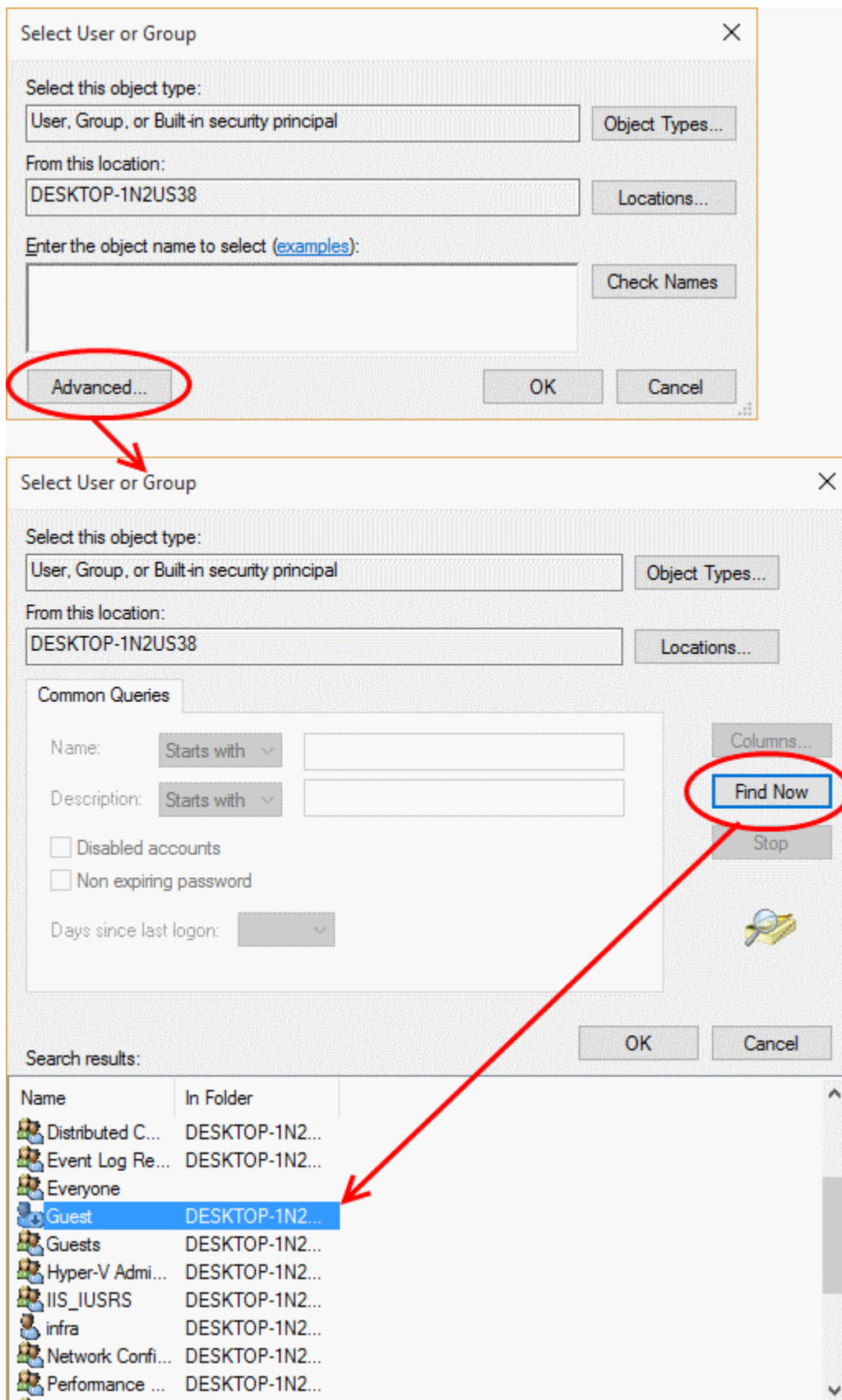
- Repeat the process to add more process(es)

Auto-contain a file if it was created by specific user(s)

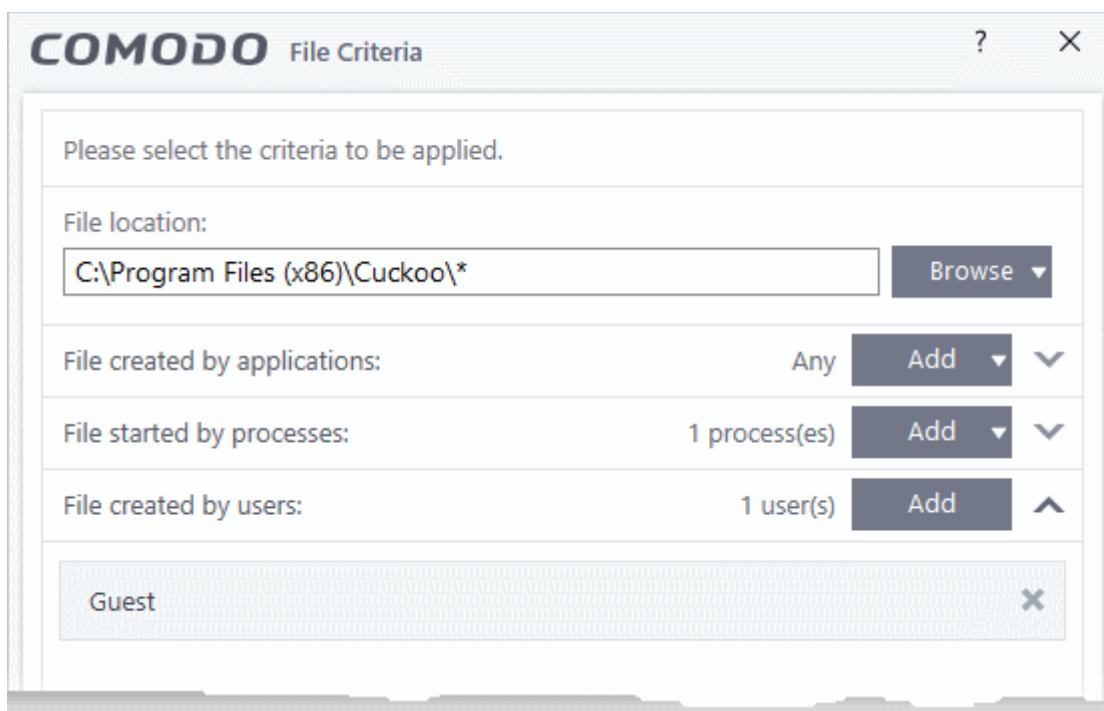
- Click the 'Add' button in the 'File Created by User(s)' stripe.



- The 'Select User or Group' dialog will appear.
 - Type the names of the users to be added to the rule. 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.



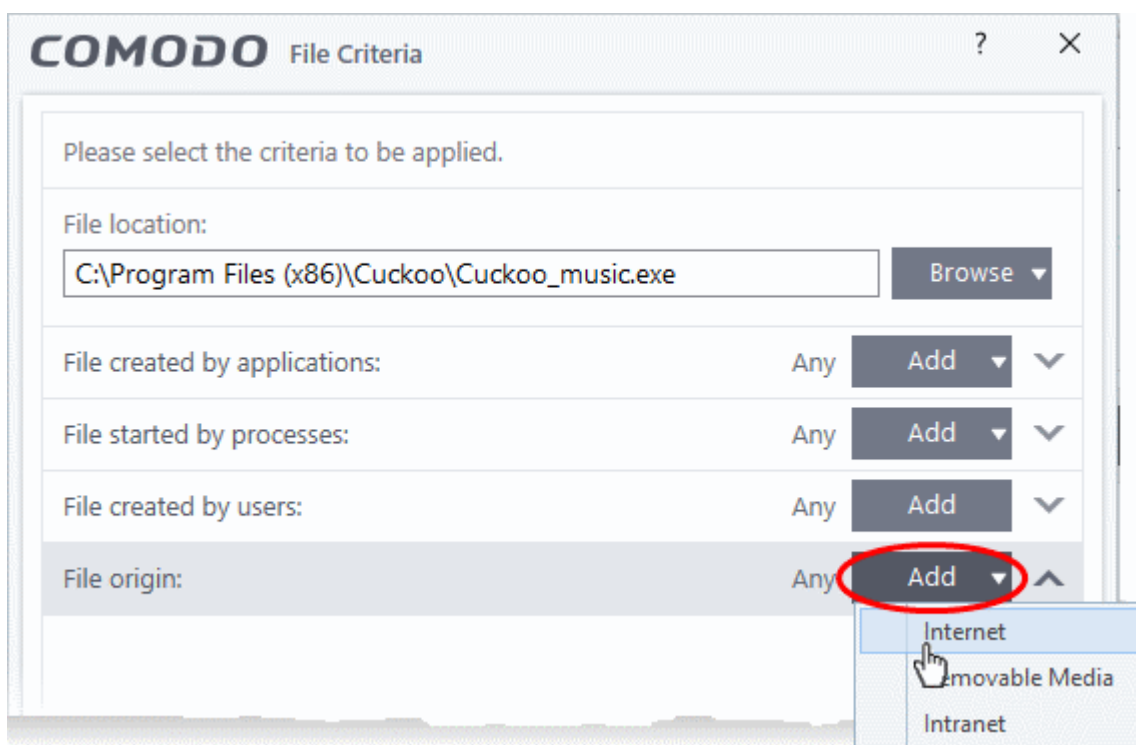
The user will be added to the list.



- 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(s)' stripe.
- Choose the source from the options:

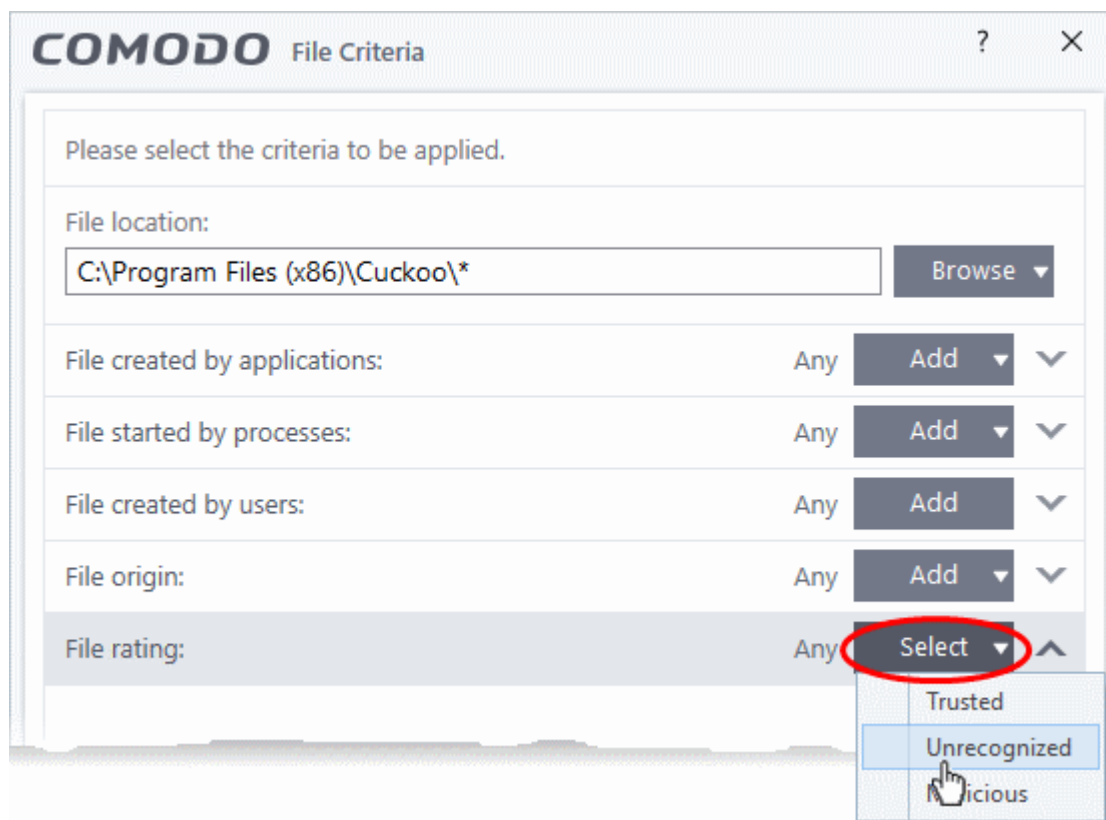


- Internet - The rule will only apply to files that were downloaded from the internet.

- Removable Media - The rule will only apply to items copied to the computer from removable devices like a USB drive, CD/DVD or external storage.
- 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

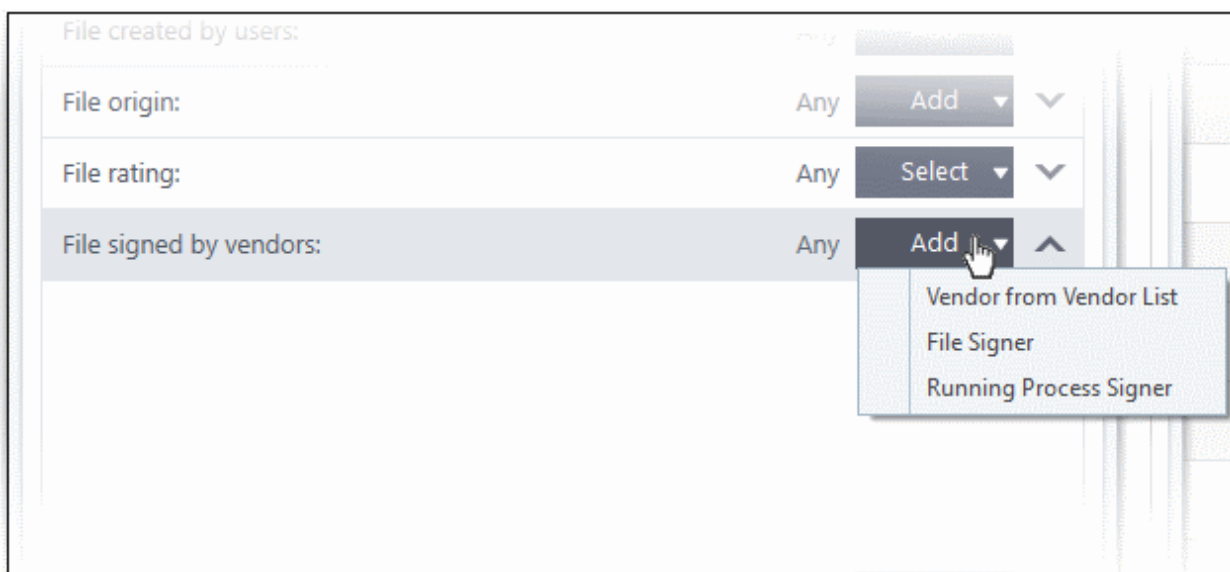
- Click the 'Select' button in the 'File Rating' stripe



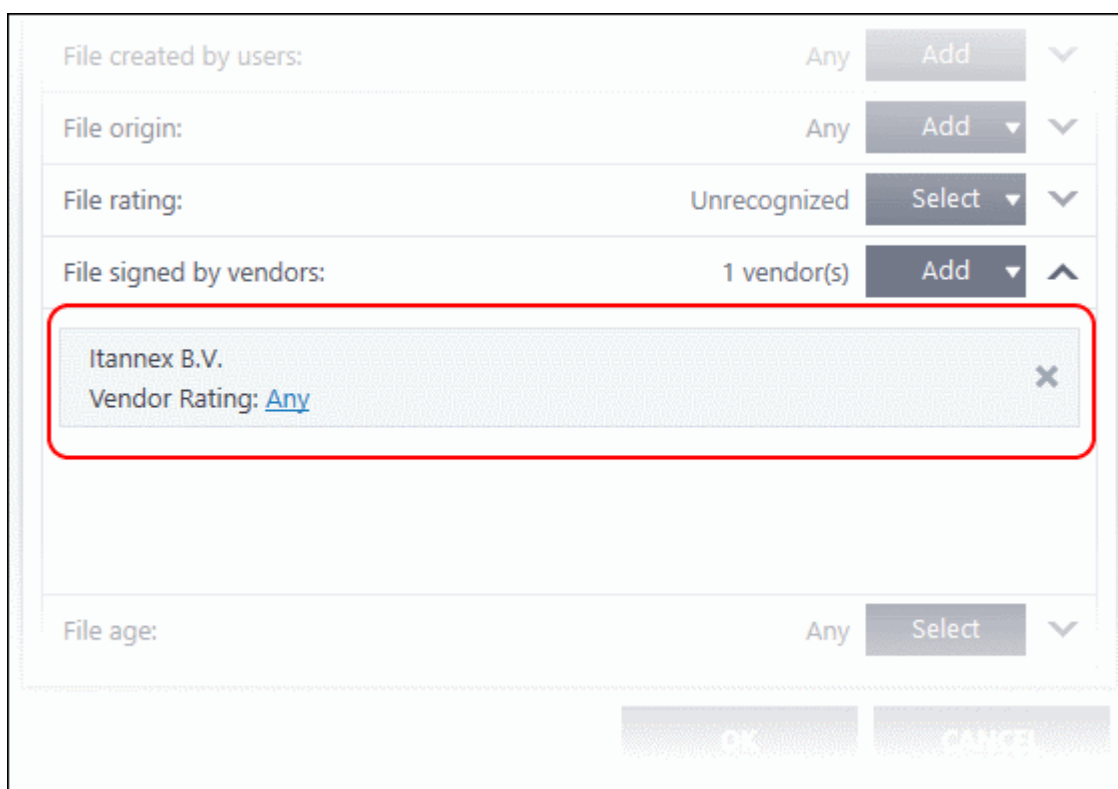
- Choose the source from the options:
 - **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by CCS. See [File Rating Settings](#) for more information.
 - **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. See [File List](#) for more information.
 - **Malicious** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. See [Unknown Files - The Scanning Process](#) for more information.
- Repeat the process to add more file ratings

Auto-contain a file based on software vendor

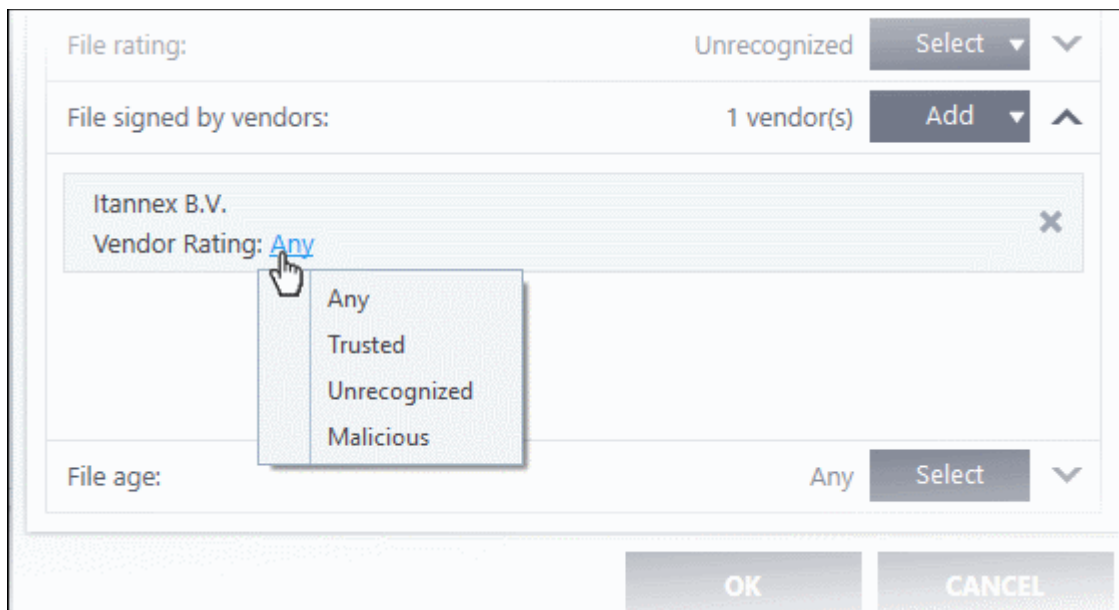
- Click the 'Add' button in the 'File signed by vendors' stripe.



- Choose the software vendor source from the options
 - **Vendor from Vendor List** - Select a vendor from the list to contain all files by a specific publisher. See 'Vendor List' for more information about managing software vendors.
 - **File Signer** - Browse to the file location, select the file and click open. The software vendor of the file will be added as a filter criteria.
 - **Running Process Signer** - Click this and in the 'Browse for Processes' dialog, select the process and click 'OK'. The software vendor of the file that created the process will be added as a filter criteria.



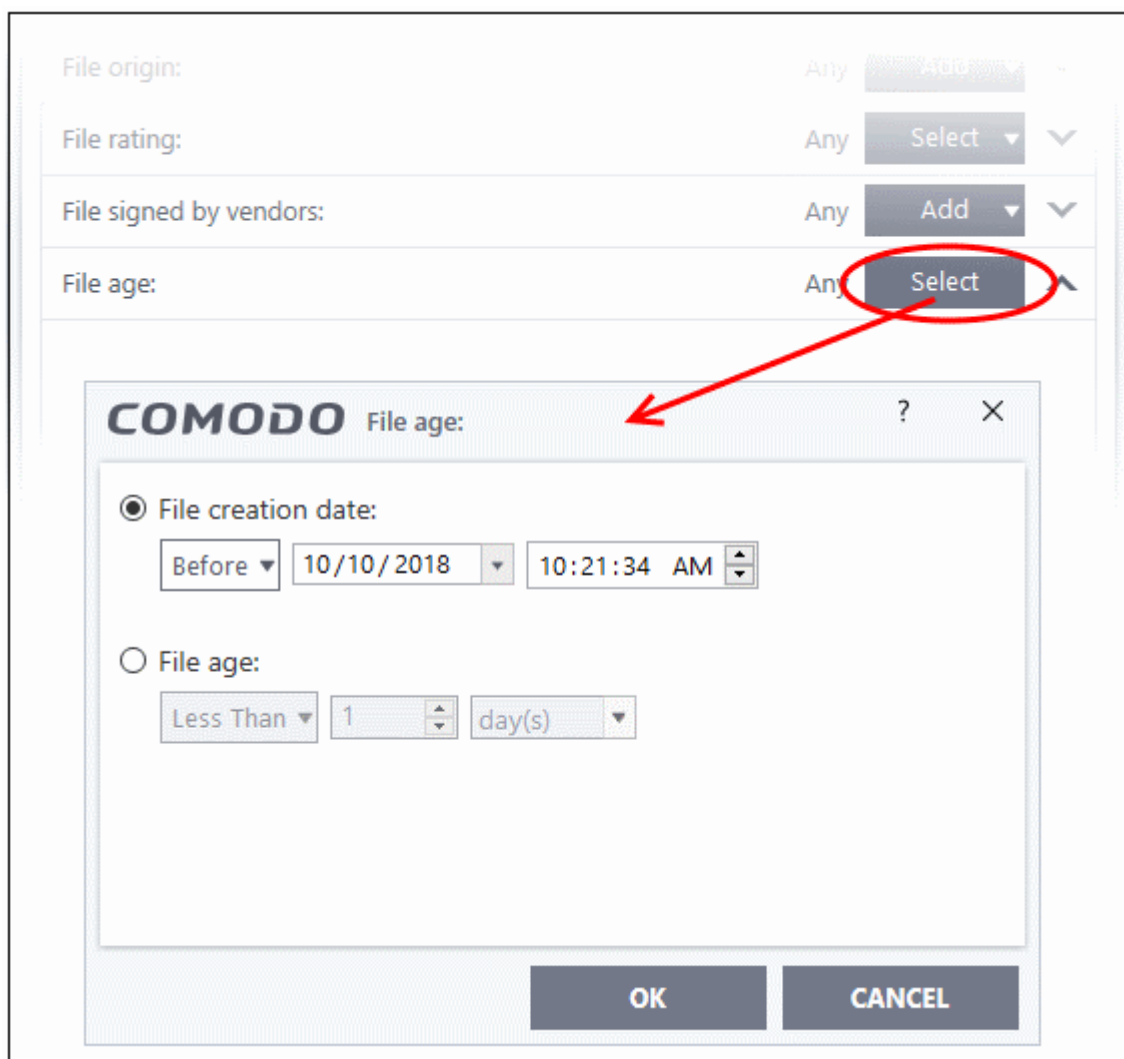
- Vendor rating - Click 'Any' to choose a specific file rating. Use this if you only want the rule to apply to vendor files which have a specific rating.



- Repeat the process to add more vendors

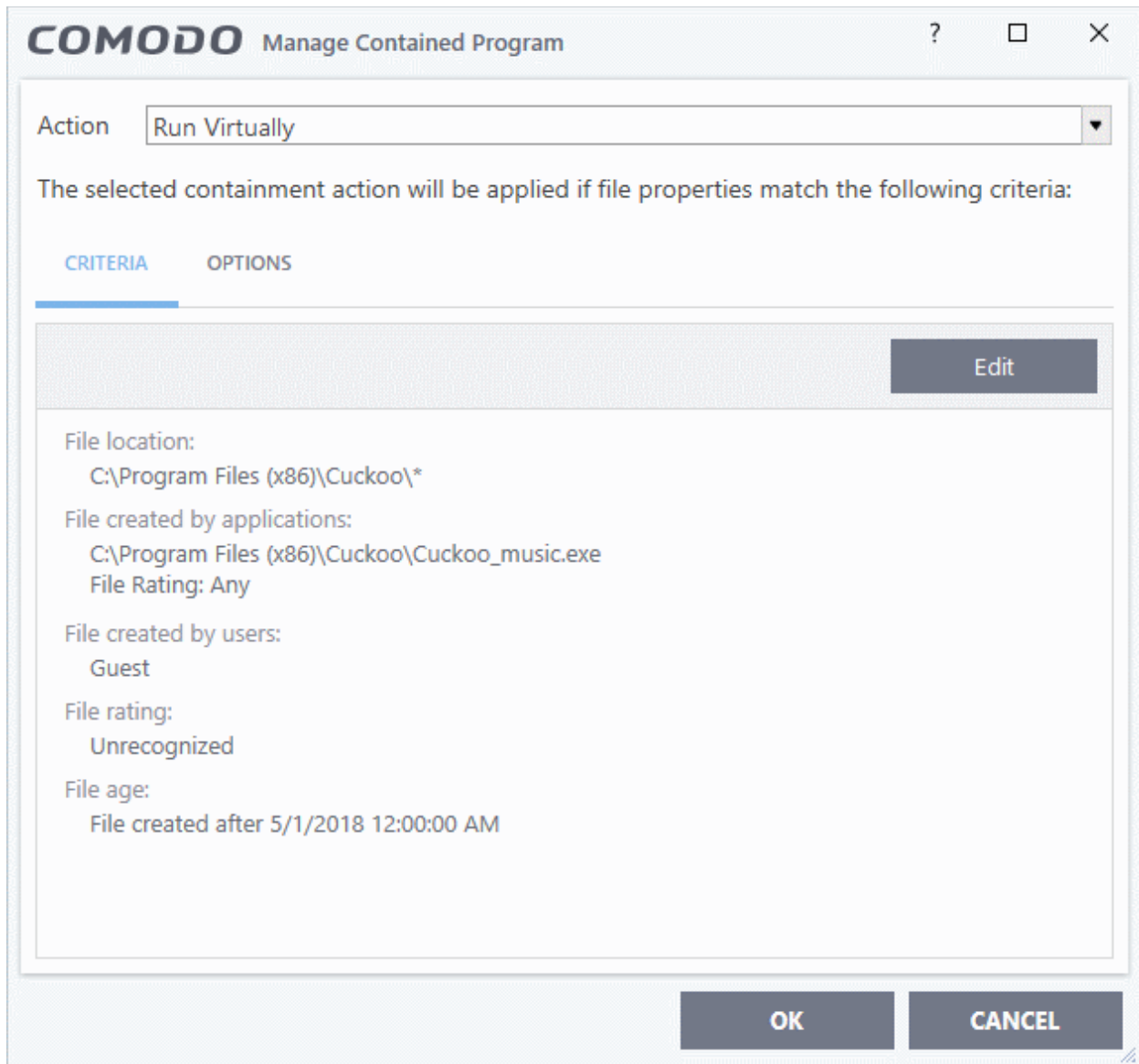
Set the file age as filter criteria

- 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** - CCS 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** - CCS 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.

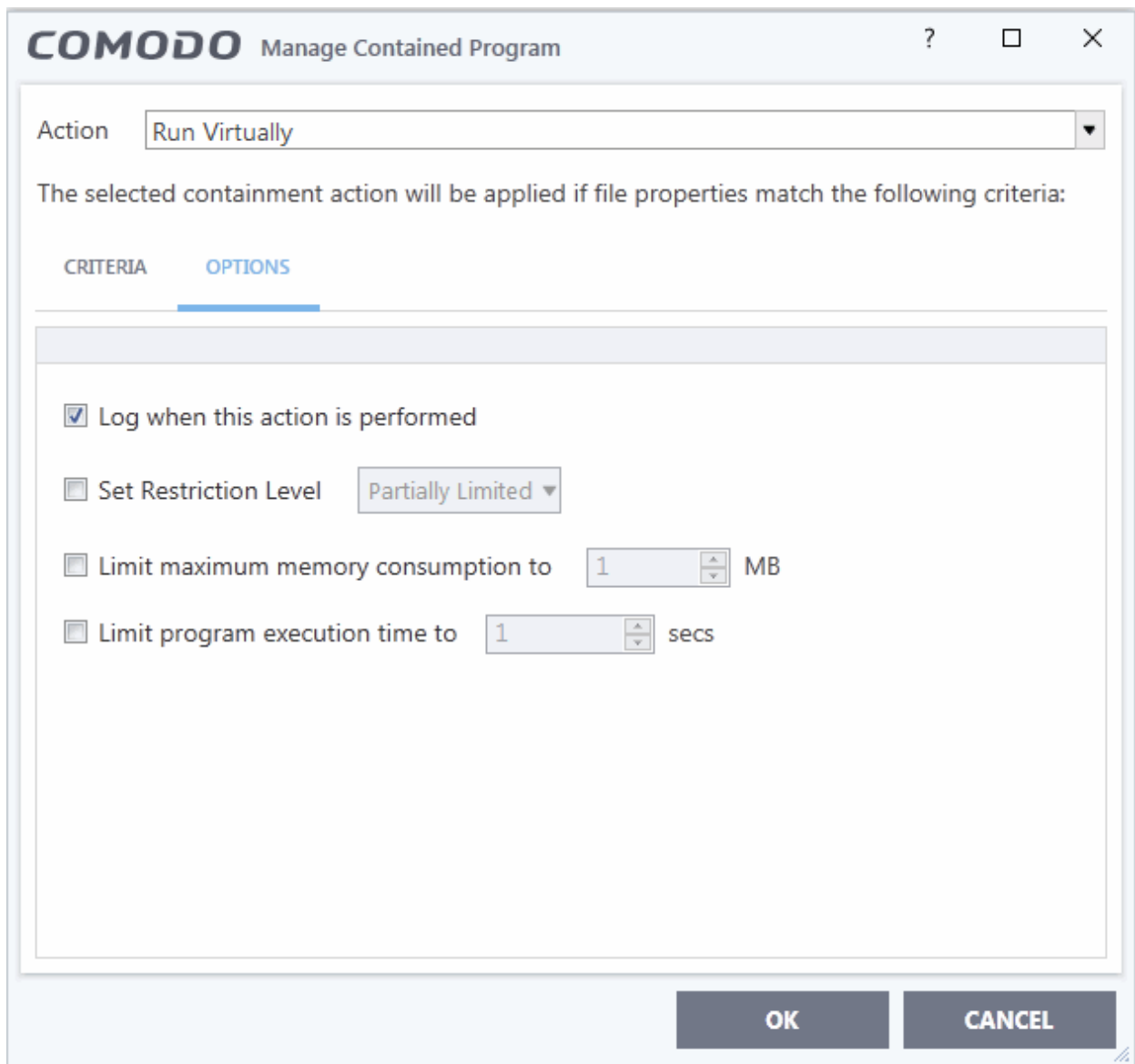


Step 3 - Select the Options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

To select the options

- Click the 'Options' tab.



The options will be displayed, depending on the 'Action' chosen in **Step 1**.

The options available for **'Ignore'** action are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be added to CCS Containment logs.
- **Don't apply the selected action to child processes** - Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CCS treats all the child processes as individual processes and forces them to run as per the file rating and the Containment rules.
 - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
 - If this option is selected, then the ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Containment rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the 'Ignore' action only.

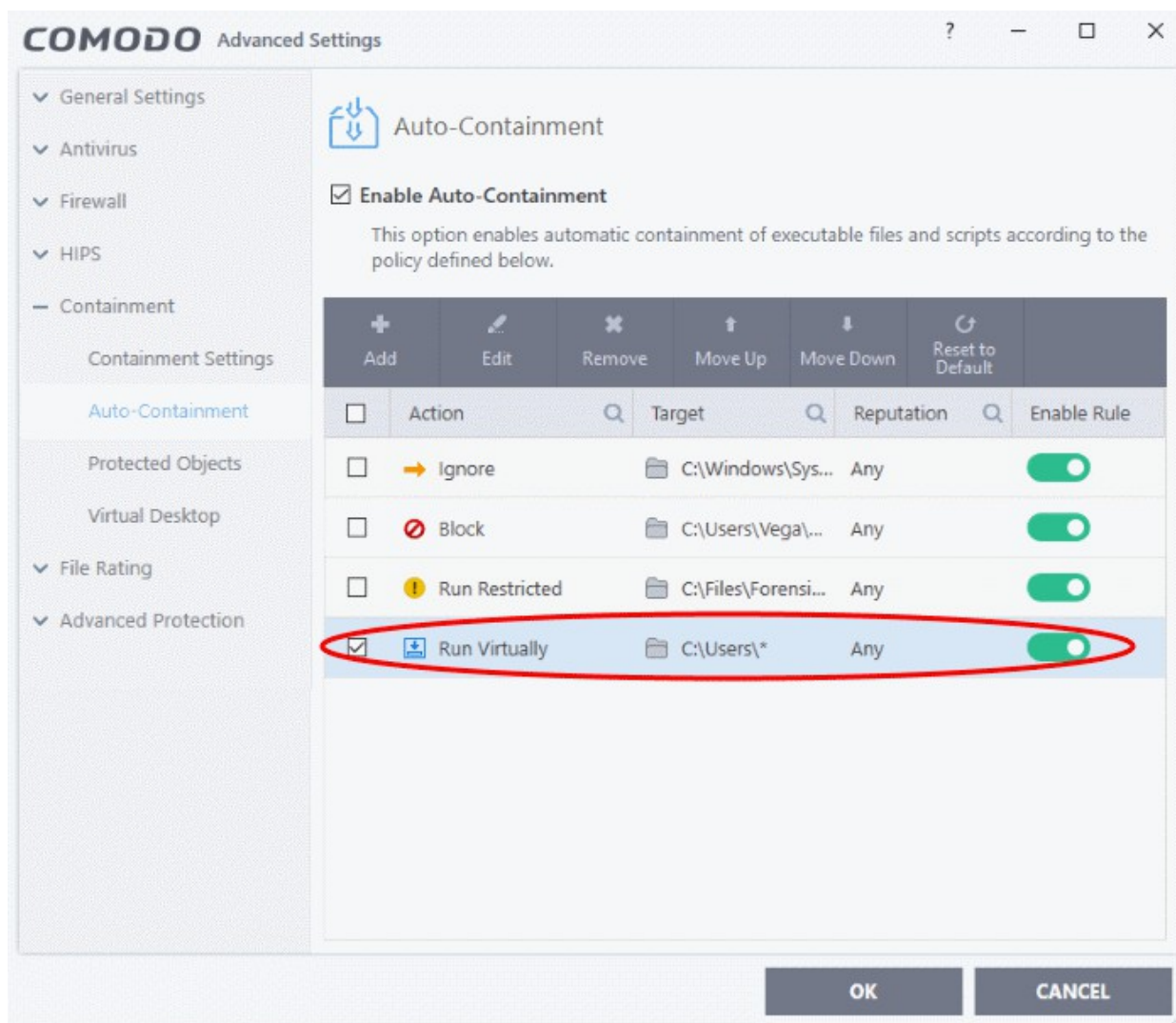
The options available for **'Run Restricted'** and **'Run Virtually'** actions are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be added to CCS 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. 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 options available for 'Blocked' action are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be added to CCS Containment logs.
- **Quarantine program** - If checked, the programs 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 depending on the priority to be given to it, with respect to the other rules.

Editing an Auto-Containment Rule

- To edit an auto-containment rule, select it from the list in the Auto-Containment panel and click 'Edit' from the top.

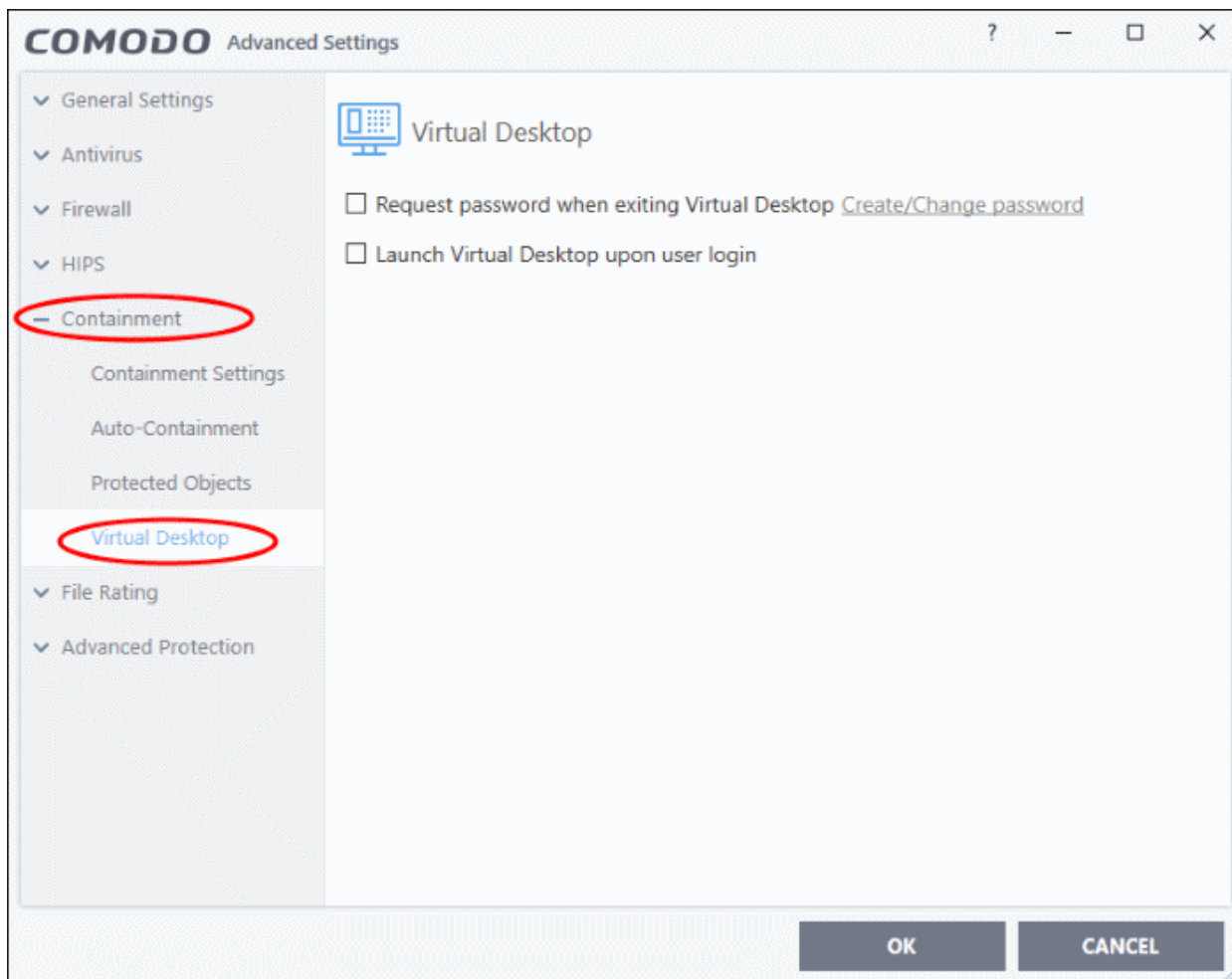
The 'Manage Contained Program' dialog will be displayed. The procedure is similar to **Adding an Auto-Containment Rule**.

- Click 'OK' to save the changes to the rule.

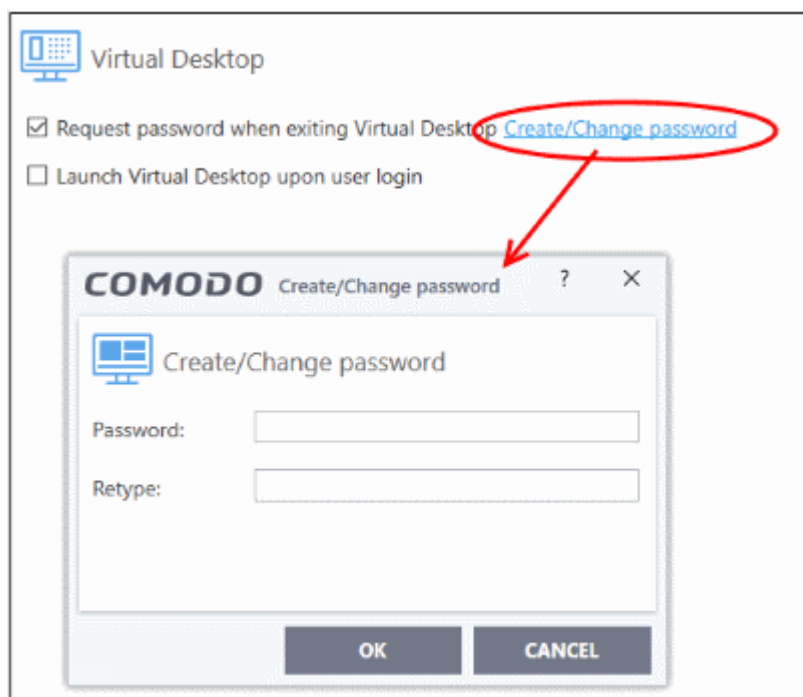
Important Note: Please make sure the auto-containment rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail. You can restore the rules to default rules at any time by clicking the 'Reset to Default' button at the top.

6.6.5. Virtual Desktop Settings

- The settings area lets you password protect the **Virtual Desktop**. Once set, the password has to be entered in order to close the virtual desktop. This lets admins and parents prevent users from closing the virtual session and accessing the host computer.
- You can also configure CCS to launch the virtual desktop automatically when a user logs on.
- Click 'Settings' > 'Containment' > 'Virtual Desktop' to open the interface:



- **Launch Virtual Desktop upon user login** – Will automatically run the **Virtual Desktop** when a user logs in to the system. **(Default = Disabled)**
- **Request password when exiting Virtual Desktop** – Configure an exit password. The exit password is a security measure to prevent guests or younger users from closing the virtual desktop and potentially exposing the computer to danger. **(Default = Disabled)**



- Type a password that cannot easily be guessed. It should be at least 8 characters long and contain a combination of uppercase and lowercase letters, numbers and special characters.
- Re-enter the password in the 'Retype' field then click 'OK'.

You will now be asked for a password every time you exit the virtual desktop.

6.7. File Rating Configuration

- The CCS file rating system is a cloud-based file look-up service (FLS) that attempts to ascertain the reputation of files on your computer by consulting a global database.
- Whenever a file is first accessed, CCS will check the file against our master whitelist and blacklists and will award it trusted status if:
 - The application/file has a 'Trusted' status in the CCS **File List**
 - The application is from a trusted vendor in the **Vendor List**
 - The application is included on the Comodo safelist.
- Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource consumption.
- On the other hand, files which are identified as harmful are given a status of 'Malicious' and quarantined or deleted automatically.
- Files which could not be recognized by the rating system are awarded 'Unrecognized' status.
- You can review unrecognized files in the **File List** interface and manually trust/block/delete them.
- You can also submit them to Comodo for further analysis or run an on-demand file-lookup.

Important Note: In order for the software to submit unknown files to our file rating and malware analysis servers, please make sure the following IP addresses and ports are allowed on your network firewall:

- To allow communication with our File Lookup Servers (FLSs):
 - IPs that need to be allowed:
 - 91.209.196.27

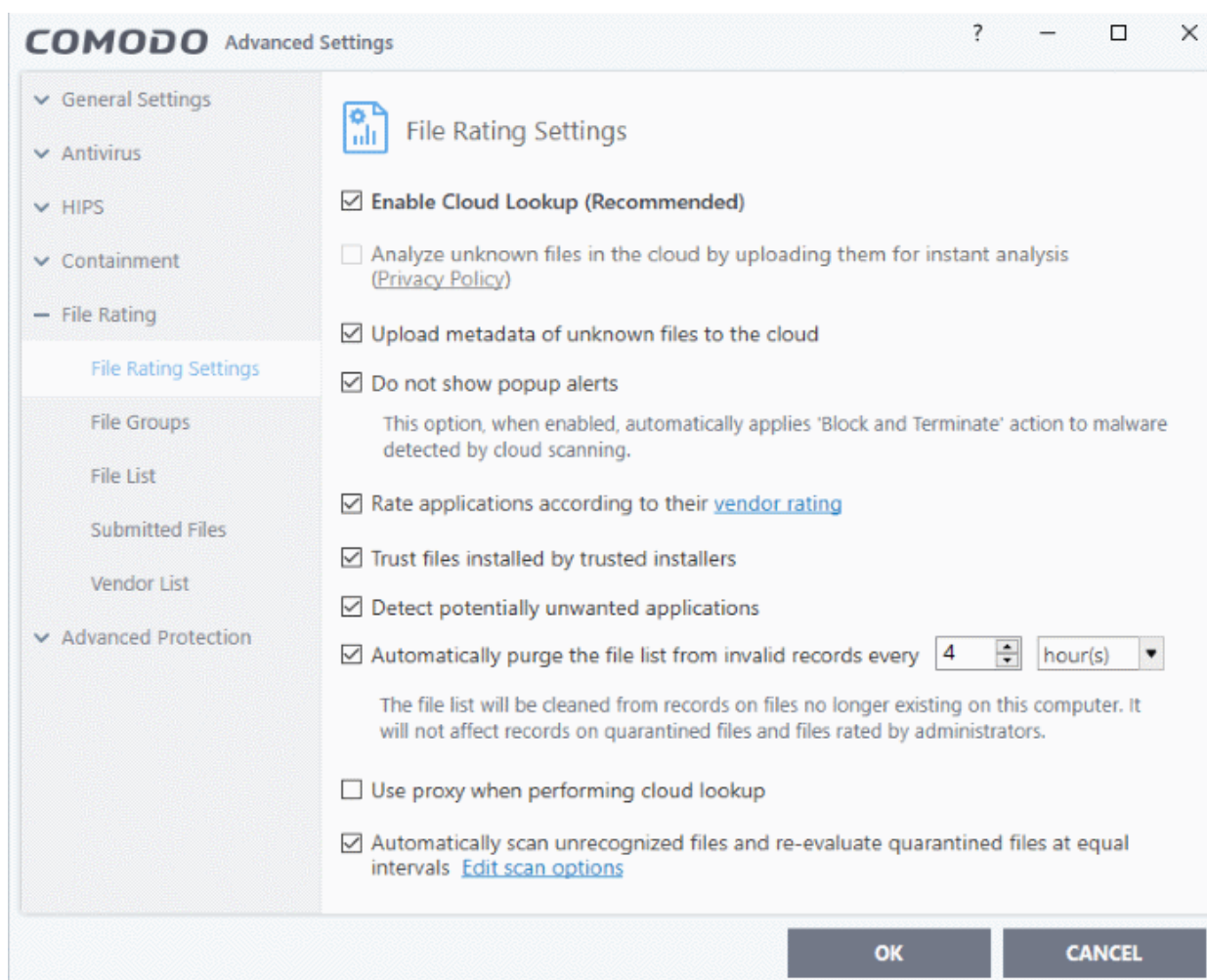
- 91.209.196.28
- 199.66.201.20
- 199.66.201.21
- 199.66.201.22
- 199.66.201.25
- 199.66.201.26
- Ports that need to be allowed: 53 UDP and 80 TCP
- Direction: Outgoing (Endpoints to FLSs)

The 'File Rating' area allows you to view and manage the list of 'Trusted Files', Malicious Files, and 'Unrecognized Files' and also allows you to:

- Manually add files and executable to 'Trusted Files' list.
- Submit 'Unrecognized Files' for look-up and view the list of files you have submitted previously.
- View and manage the 'Trusted Software Vendor' list.

Open the 'File Rating' section,

- Click 'Settings' in the top left of the CCS home screen
- Select 'File Rating' > 'File Rating Settings':



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

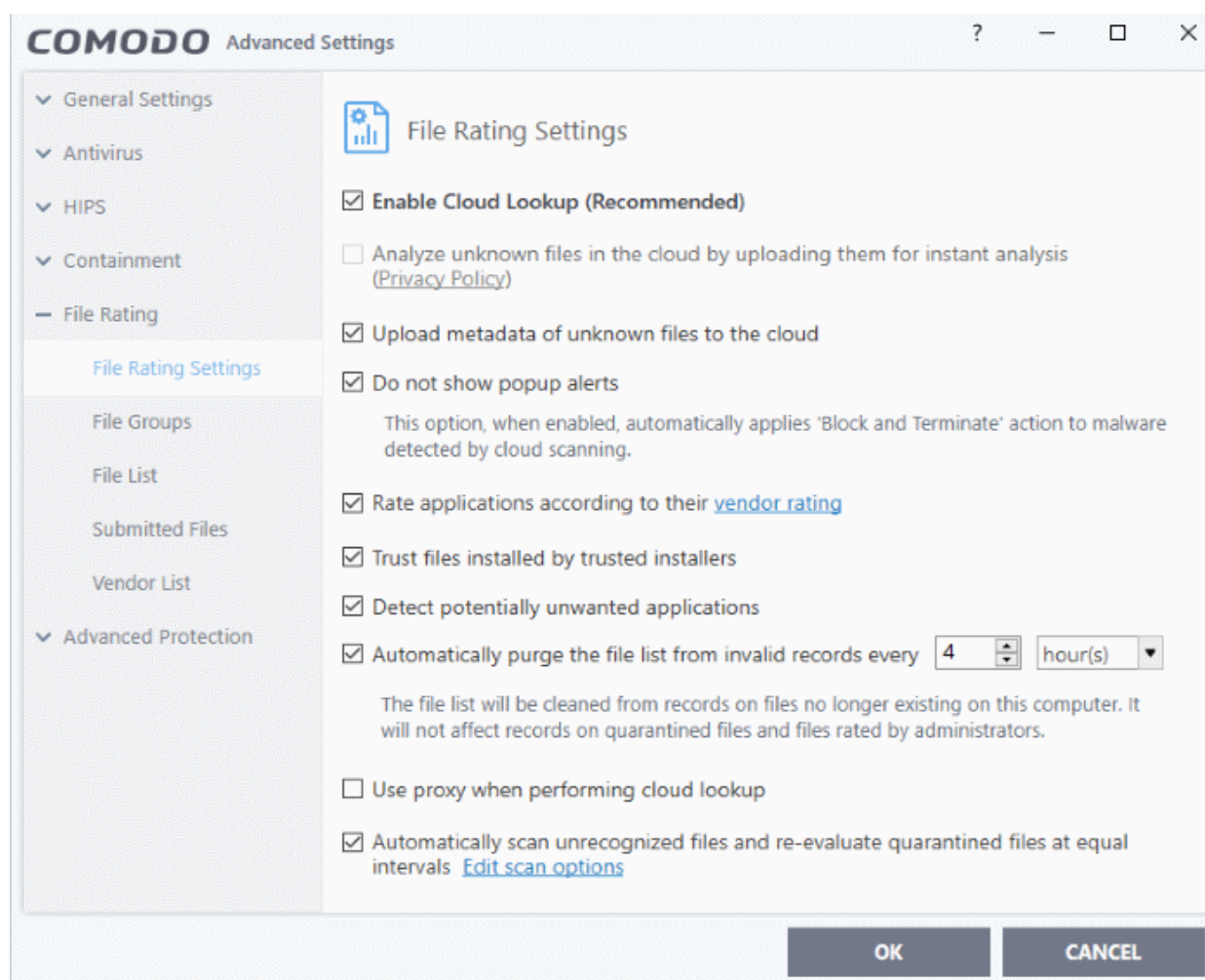
- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **File Groups** - Create predefined groups of one or more file types.
- **File List** - View, manage and investigate executable files on your computer and their current trust rating.
- **Submitted Files** - View any files already submitted to Comodo for analysis.
- **Vendor List** - View the list of software vendors and manually add vendors.

6.7.1. File Rating Settings

- A file rating determines how CCS interacts with a file.
 - 'Trusted' files are safe and are allowed to run normally.
 - 'Untrusted' files are malware so they get quarantined or deleted.
 - 'Unknown' files are run in the container until they are classified as trusted or untrusted.
- Especially in the case of 'unknown' files, the rating of a file can change over time. For example, an 'unknown' file might be re-classified as 'trusted' or 'untrusted' after it has been tested.
- You can also configure whether CCS should upload unknown files to Comodo cloud for instant analysis

Open File Rating Settings

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File Rating Settings' on the left:



- **Enable Cloud Lookup** - If enabled, CCS will check a file's trust rating on our cloud servers as part of the

scan process. **(Default and recommended =Enabled)**

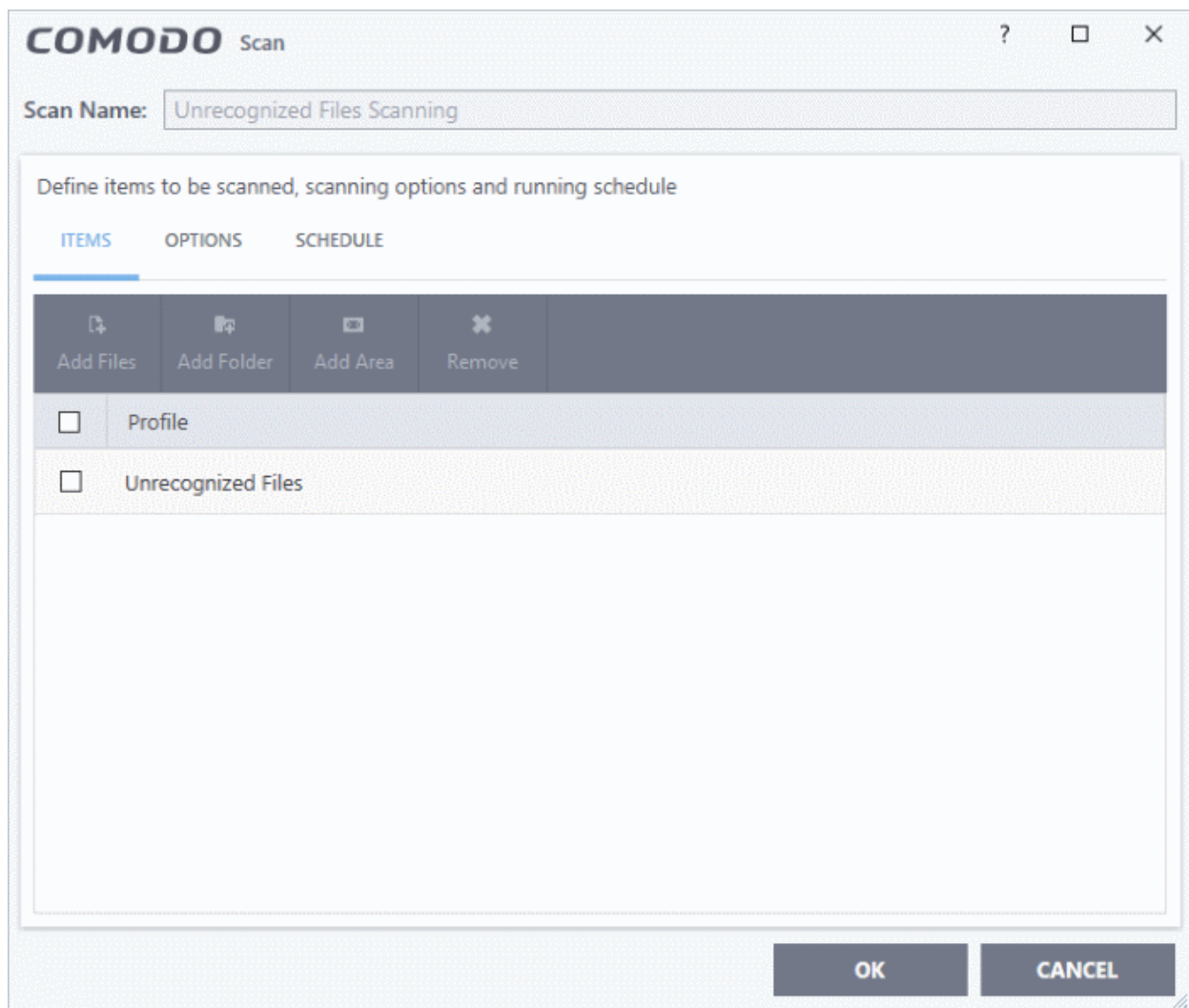
- **Analyze unknown files in the cloud by uploading them for instant analysis** – Files which do not have a trust rating in our online database will be uploaded to Comodo for further testing. The files undergo a range of automated and manual behavior tests to try and determine whether they are safe or not. They will be added to the global whitelist or blacklist once a verdict is reached. **(Default = Disabled)**
- **Upload metadata of unknown files to the cloud** - If enabled, information about unknown files will be uploaded to Comodo servers. Metadata is basic file information such as file source, author, date of creation. **(Default =Enabled)**
- **Do not show popup alerts** - This option allows you to configure whether or not to show malware alerts when malware is encountered. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show popup alerts then you have a choice of default responses that CCS should automatically take - either 'Block Requests' or 'Allow Requests'. **(Default =Enabled)**
- **Rate applications according to their vendor rating** - Determines whether CIS should award applications the same trust rating as the application publisher (vendor).

For example, if CCS detects an unknown file then it will check the rating of the vendor and apply the same rating to the file. If disabled, CCS will not apply the vendor rating but will instead run the file in the container. **(Default =Enabled)**

- Vendor ratings are listed in the '**Vendor List**' interface.
- CCS ships with a predefined list of trusted vendors. Click the words 'vendor rating' to open the '**Vendor List**' panel.
- Admins and users can add vendors to the list and rate them accordingly.
- Vendors rated by Comodo also can be re-rated by admins and users.
- The vendor rating priority is shown below:
 - Admin
 - User
 - Comodo
- See '**Vendor List**' for more information.
- **Trust files installed by trusted installers** - If enabled, CCS will trust files created by applications that are covered by the 'Installer or Updater' rule in **HIPS Rules**. **(Default = Enabled)**
- **Detect potentially unwanted applications** - When this option is selected the antivirus will also scan for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional 'utility' when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the internet. **(Default = Enabled)**.
- **Automatically purge unrecognized files every NN hour(s)** - Comodo Client Security will remove from the ratings interface all entries for unrecognized files which have actually been deleted. Select the interval in days from the drop-down combo box. **(Default = Enabled)**
- **Use proxy when performing Cloud Lookup** - If enabled, CCS will submit files to FLS for analysis through a proxy. The proxy server is same one that is defined for program and database updates. See '**Configure Program and Virus Database Updates**' for more details. **(Default = Disabled)**
- **Automatically scan unrecognized files at equal intervals** - Comodo Client Security will periodically run file-lookup checks on unrecognized files to obtain their trust rating from the latest cloud database. 'Edit scan options' allows you to configure various scanning options for the unrecognized items. **(Default = Enabled)**

To do this:

- Select the 'Edit scan options' link



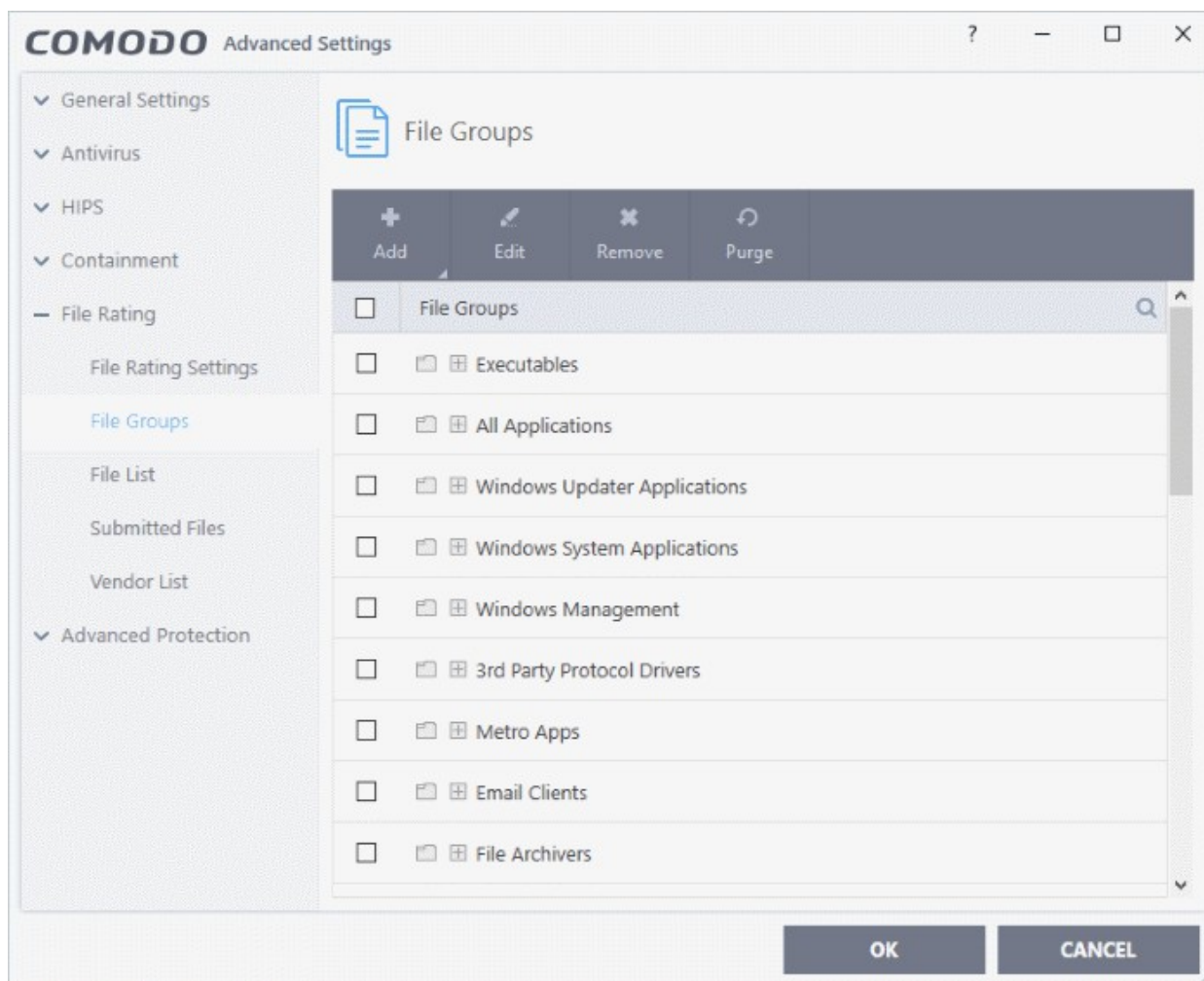
- Scan Name - The scan name is pre-configured as 'Unrecognized Files Scanning' and cannot be edited.
- Items - The profile is pre-configured for unrecognized and quarantined files and cannot be edited.
- Scan Options - This is same as explained for a custom scan. [Click here](#) to view.
- Schedule - This is set to scan every 4 hours by default. This is same as explained for a custom scan. [Click here](#) to view
- See '[Automatically Scan Unrecognized Files](#)' for more information.

6.7.2. File Groups

- As the name suggests, a file group is a collection of one or more file types.
- Once created, file groups can be referenced from other areas of CCS, making it easy to add an entire class of files to exclusions, HIPS rules, containment rules and more.
- CCS ships with a set of predefined file groups. You can also create your own file groups and edit existing groups as required.

To open the 'File Groups' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File Groups' on the left:



Use the search option on the right to look for a specific group.

The buttons at the top provide the following options:

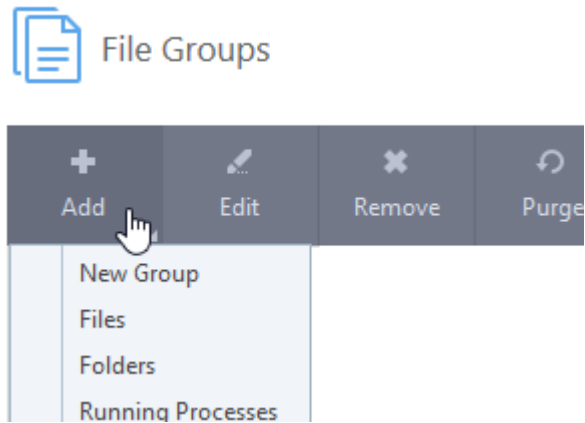
- **Add** - Create a new groups
- **Edit** - Rename a group or change the file path of items in a group.
- **Remove** - Delete an entire group or individual items.
- **Purge** - Run a check to verify that all files listed are still installed on the host at the path specified. If not, the item is removed from the list.

This interface allows you to:

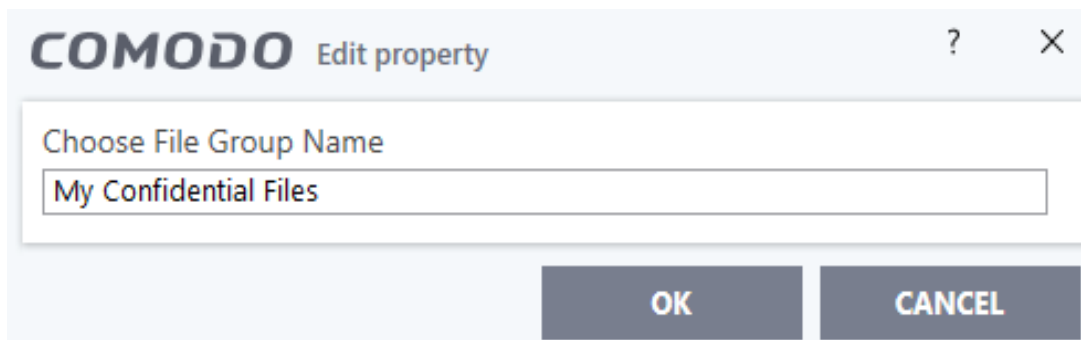
- **Create a new File Group**
- **Edit the names of an Existing File Group**
- **Add a file to an existing file group**
- **Remove existing file group(s) or individual file(s) from existing group**

Add a File Group

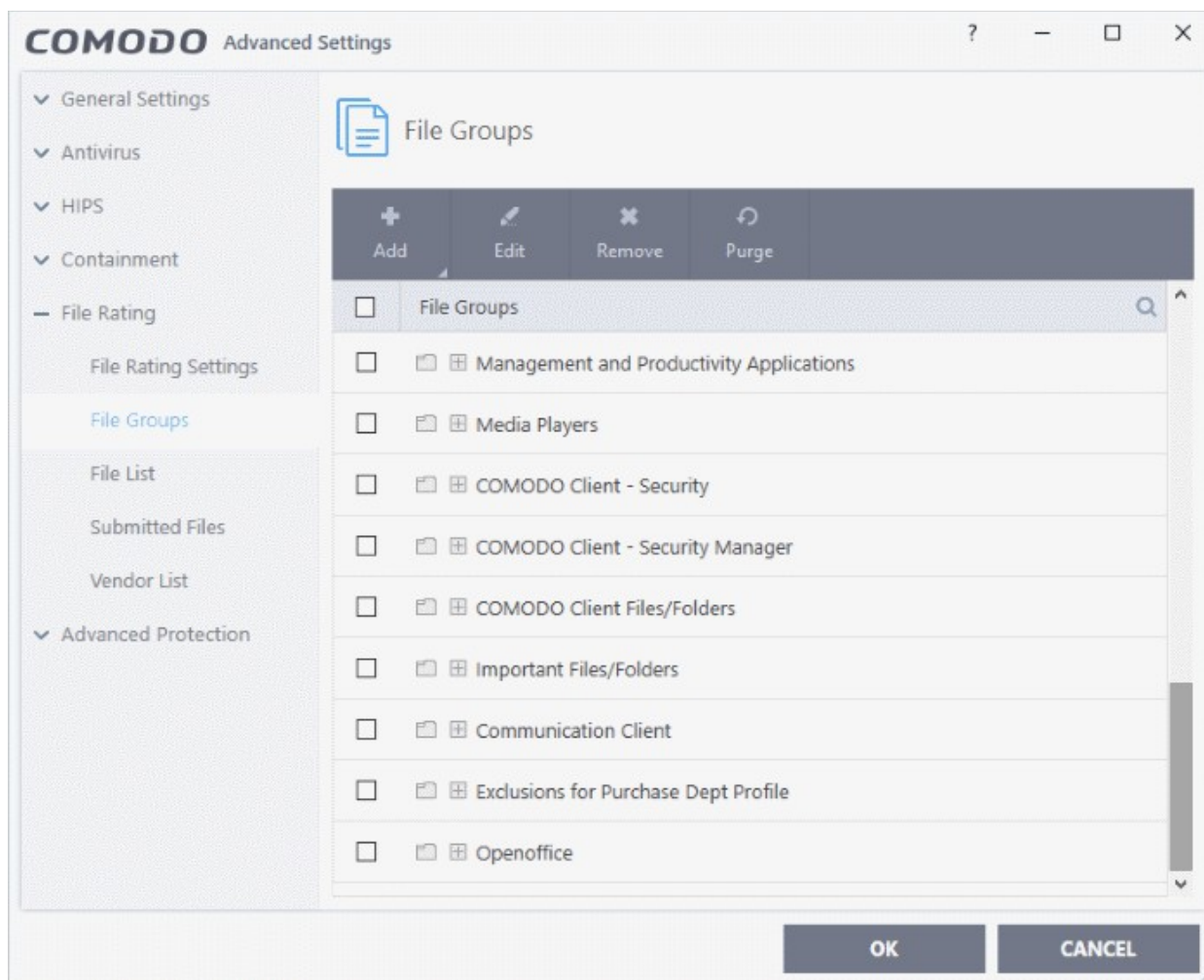
- To add a new 'File Group', click the 'Add' button from 'File Groups Pane'.



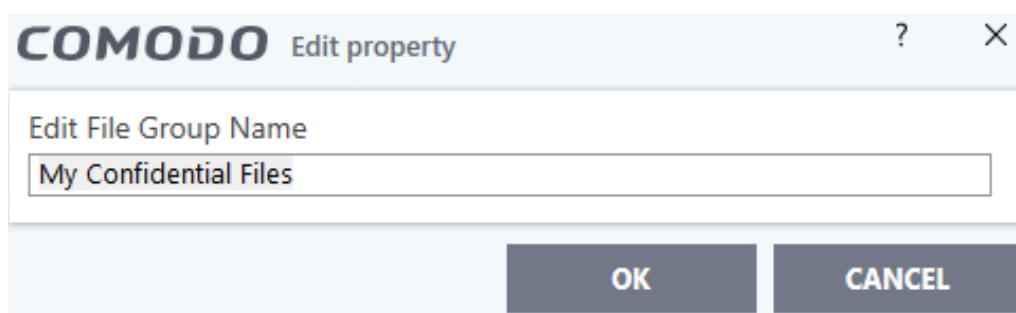
- Select 'New Group' from the 'Add' drop-down menu.
- Enter a 'File Group Name' in the 'Edit property' dialog and click 'OK'.



The 'File Group' will be added and displayed in the list.



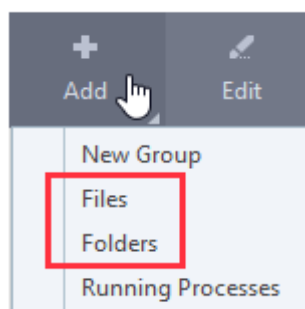
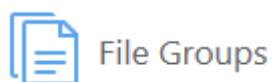
- To edit the name of an existing group, select it from the 'File Groups' list and click the 'Edit' button.



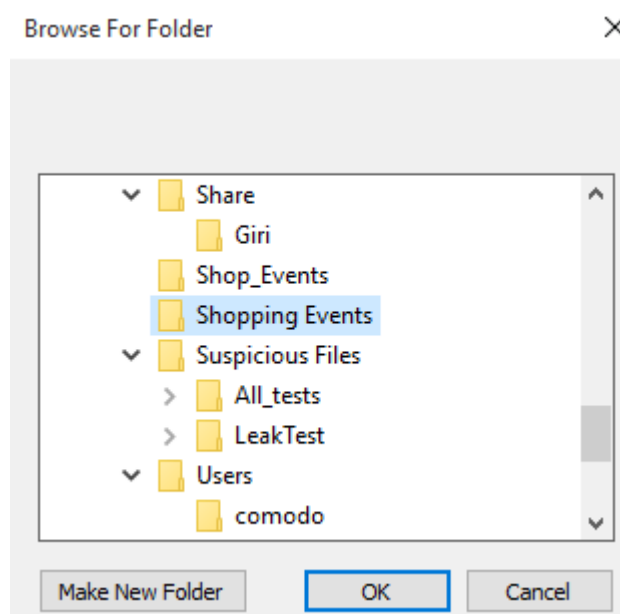
- Edit the 'File Group Name' in the 'Edit property' dialog and click 'OK'.

Add individual files or folder to a group

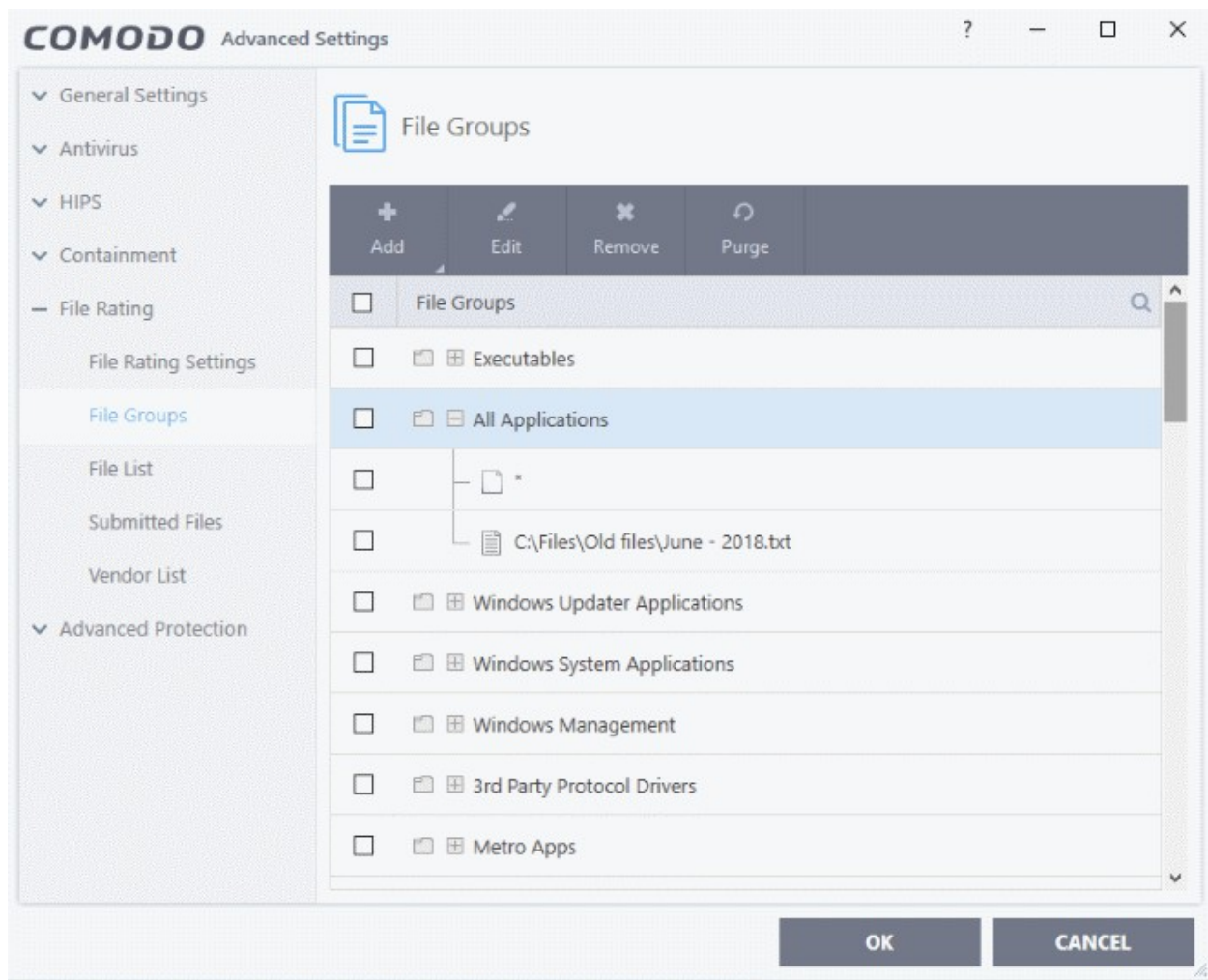
- Select the group from the list and click the 'Add' button. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes.
 - To add a file or folder, choose 'Files' or 'Folders' from the 'Add' drop-down menu.



The 'Browse' dialog will be displayed:



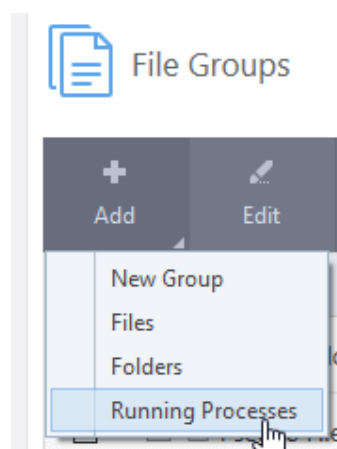
- Navigate to the file or folder you want to add to add to the group and click 'OK'



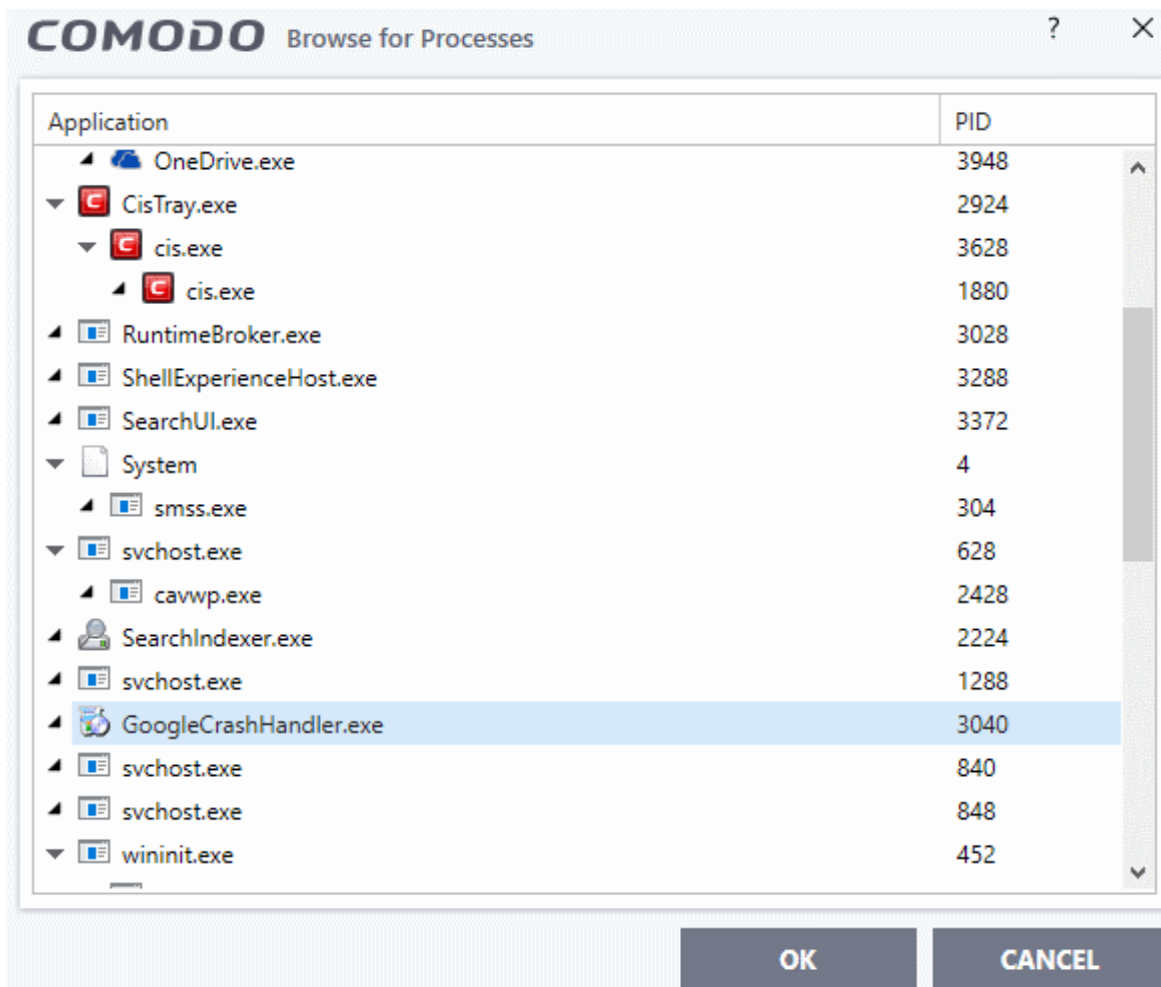
The drive file/folder will be added to 'File Groups'. Repeat the process to add more individual files or folders.

Add an application from a running processes

Click the 'Add' button then select 'Running Processes':



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

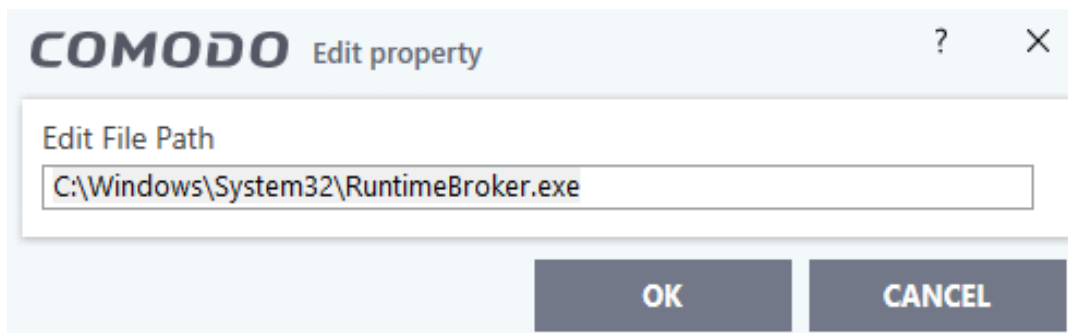


- Select the process, whose target application is to be added to 'Files Groups' and click 'OK' from the 'Browse for Process' dialog.

The application will be added to the selected group.

To edit an item in the Files Groups list

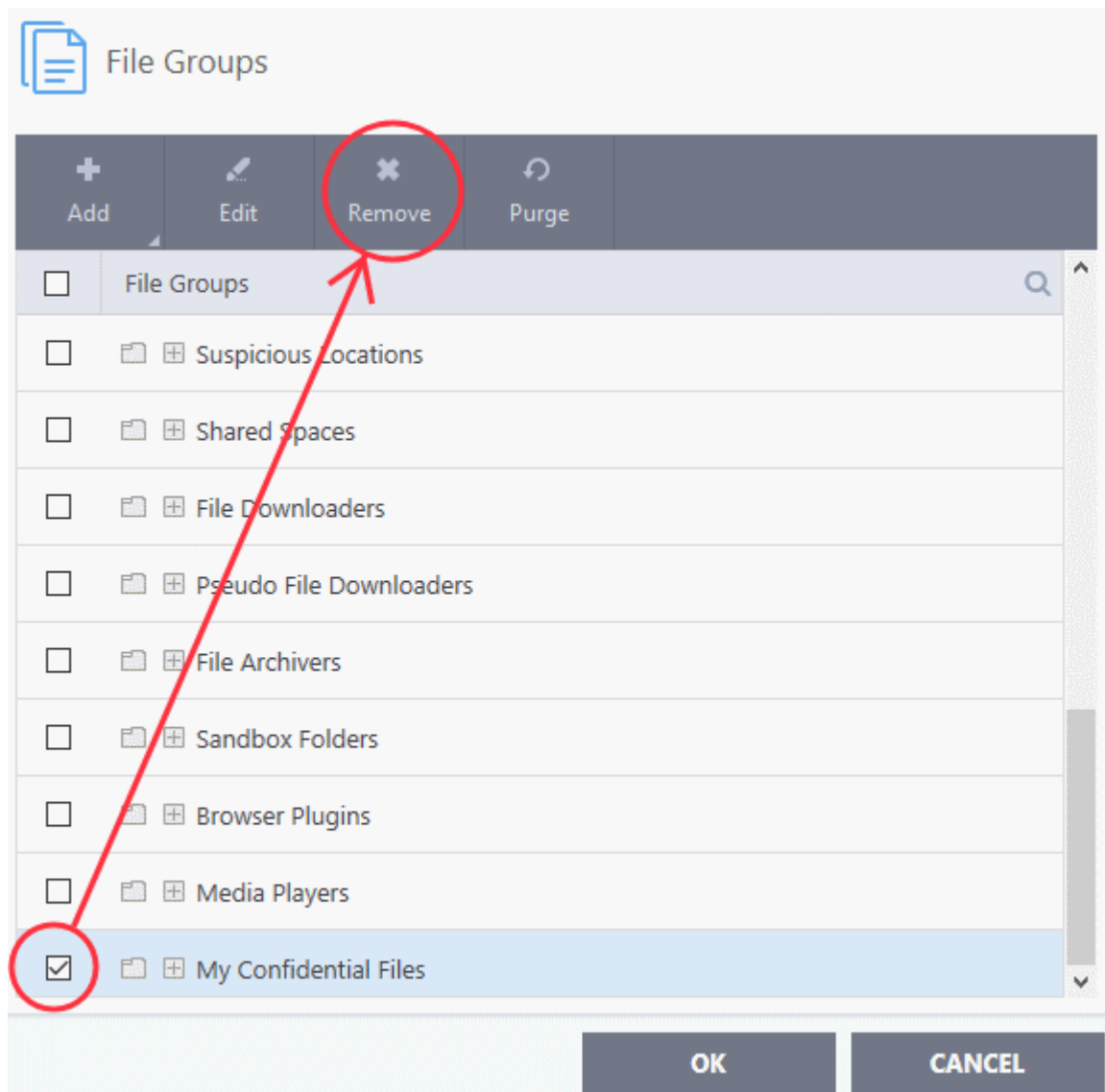
- Select the item from the list and click the 'Edit' button. The 'Edit property' dialog will be displayed:



- Edit the file path if required and click 'OK'.

To delete existing file group(s) individual file(s) from existing group

- To remove a file group, select it from the list and click the 'Remove' button.



- To remove an individual file from a group - expand the group by clicking '+' at the left of the group, select the file to be removed and click the 'Remove' button.
- Alternatively, right-click on a file and choose remove from drop-down menu.

6.7.3. File List

- Click 'Settings' > 'File Rating' > 'File List' to open the file list
- The file list is an inventory of executables and applications on your computer. Details about each file include the vendor, the date it was discovered and the file's trust rating.
- Files are scanned and assigned a trust rating when they first run on an endpoint.

CCS rates files as:

- **Trusted** - the file is safe to run outside the container.
- **Unrecognized** - no trust-rating was found for the file, so it will be run in the container.
- **Malicious** - the file is known malware and will be quarantined or deleted.

Trusted Files

'Trusted' files are considered safe to run outside the container. Files can be awarded trusted status as follows:

- **File rating** - When a file is first opened, CCS will contact our FLS servers to see if it has an existing trust rating. CCS will trust the file locally if it has a trusted rating on our FLS.
- **Vendor Rating** - If a file does not have a trust rating, then CCS will next check whether the publisher of the file has a rating. The file inherits the vendor (publisher) rating. CCS will trust the file if the vendor is rated as 'Trusted'.
 - Trusted publishers can be found in the **Vendors List**
- **Administrator rating** - Admins can elect to trust files on a local endpoints and networks. Only applies if your CCS installation is remotely managed by an administrator.
- **User Rating** - You can provide 'Trusted' status to your files in the following ways:
 1. Choose 'Treat this file as a Trusted Application' at a HIPS alert.
If an executable is unknown then it, and all its active components, generate a HIPS alert when they run. You can choose to trust files at these alerts.
 2. Assign 'Trusted' rating to a file or folder in the 'Files List' interface.
Click 'Settings' > 'File Rating' > 'File List'. It is often more convenient to classify entire directories of files as 'Trusted' rather than individually them individually at an alert. See **changing the file rating** in **File Details** for more information.

For files assigned 'Trusted' status by a user, CCS generates a hash of the file and saves it in its database as 'Trusted'. When you open any file, CCS creates a hash of the file in real-time and compares it with the list of saved hashes. This way, the file retains its 'Trusted' status even if you change the filename because the hash remains the same.

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

Unrecognized Files

- Every new executable file is first scanned against the virus blacklist (known 'bad' files) and the file whitelist (known 'good' files).
- If the file isn't on either list it is given a rating of 'Unrecognized'. Any executables that are modified are also given 'Unrecognized' status. This helps safeguard against malware changing the behavior of a previously trusted application.

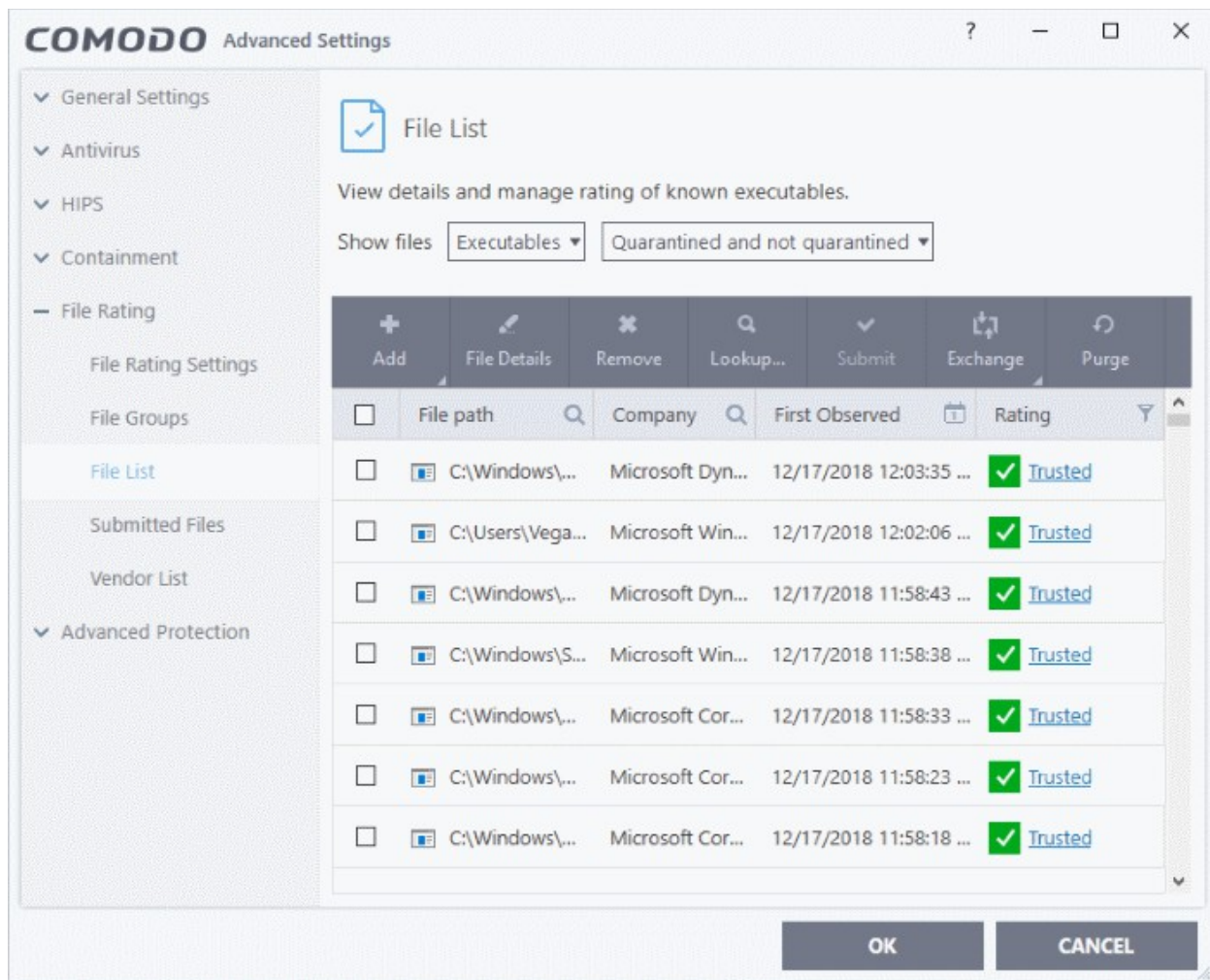
You can review pending files to determine whether or not they should be trusted. If they are trustworthy, they can be given a 'Trusted' rating. See **changing the file rating** for more details. You can also submit the files to Comodo for analysis. Experts at Comodo will analyze the files and add them to global white-list or black-list accordingly.

Malicious Files

Files identified as malware are given a 'Malicious' rating and are not allowed to run.

To open the 'File List' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File List' on the left:



The file list shows executable and non-executable files discovered on your computer.

- **Show files** - Choose the type of files shown in the interface.
 - The first drop-down lets you choose the type of files that are shown. The options available are:
 - Executables
 - Non-executables
 - All types
 - The second drop-down lets you choose file by status. The options are:
 - Quarantined
 - Not quarantined
 - Quarantined and not quarantined
 - You can combine these two filters. For example, select 'Executables' in the first drop-down and 'Quarantined' in the second drop-down to view executables that are quarantined.

Column Descriptions:

- **File Path**- Indicates installation or storage path of the file;
- **Company** - Shows the publisher of the file;
- **First Observed** - Indicates date and time at which the file was first discovered by CCS. For the files installed or stored before the installation of CCS, it shows the first execution time of CCS, when the file was discovered. For the files installed or stored after installation of CCS, it shows when the file was stored.
- **Rating** - Indicates the current CCS rating of the file. The possible values are:

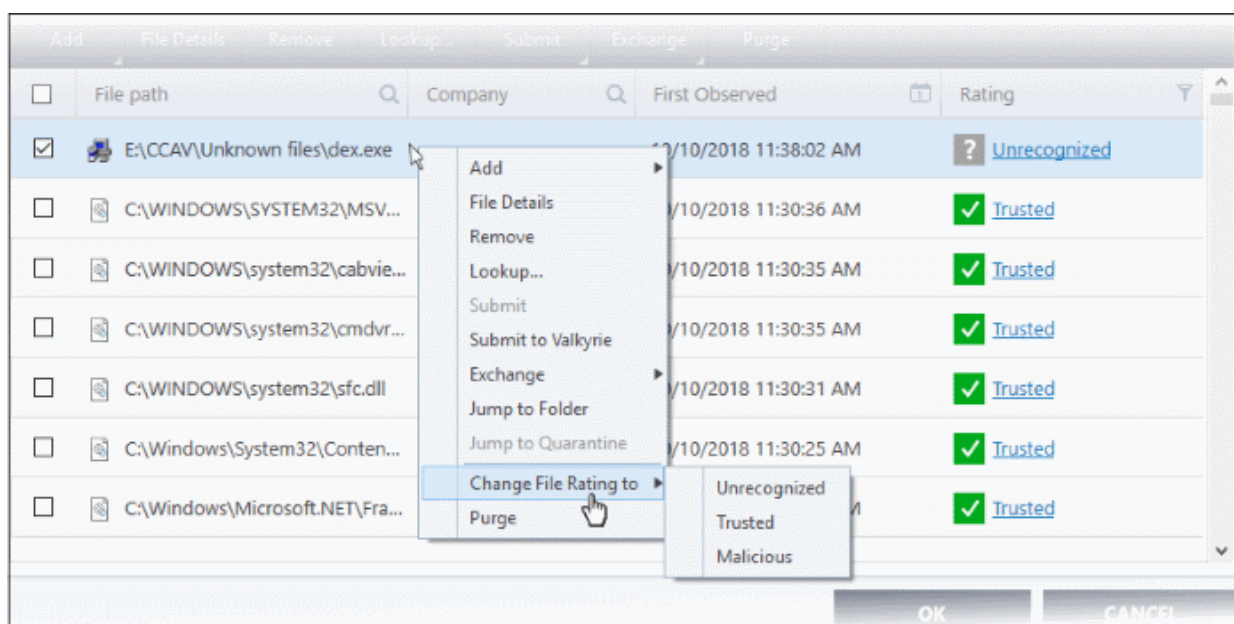
- **Trusted**
- **Unrecognized**
- **Malicious**

Files can be rated by an administrator, by an end-user or by the file-lookup system. CCS will prioritize ratings as follows:

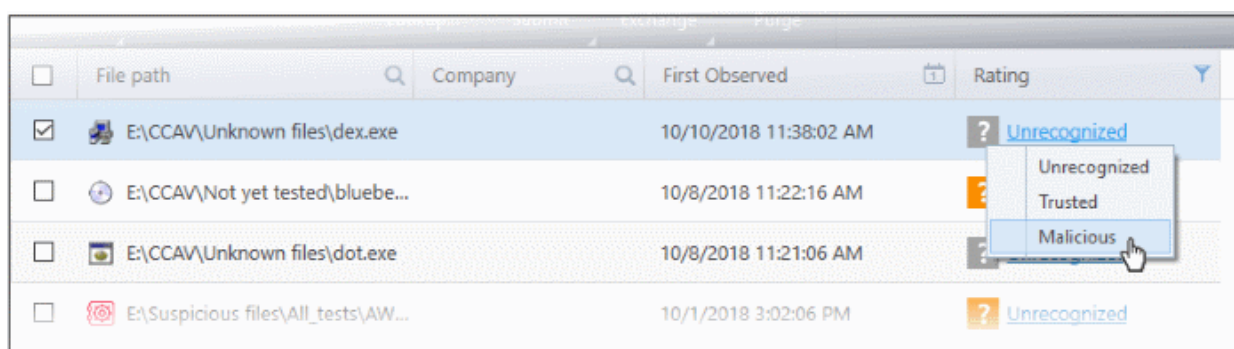
1. Administrator rating (applies if CCS is remotely managed by an Endpoint Manager admin).
2. User rating (rating set by the CCS end-user)
3. FLS (Comodo) rating (rating set by the online file-lookup system)

File rating can be modified by the user in three ways:

- By clicking on the displayed rating in the row of the desired file and choosing the rating from the context sensitive menu.



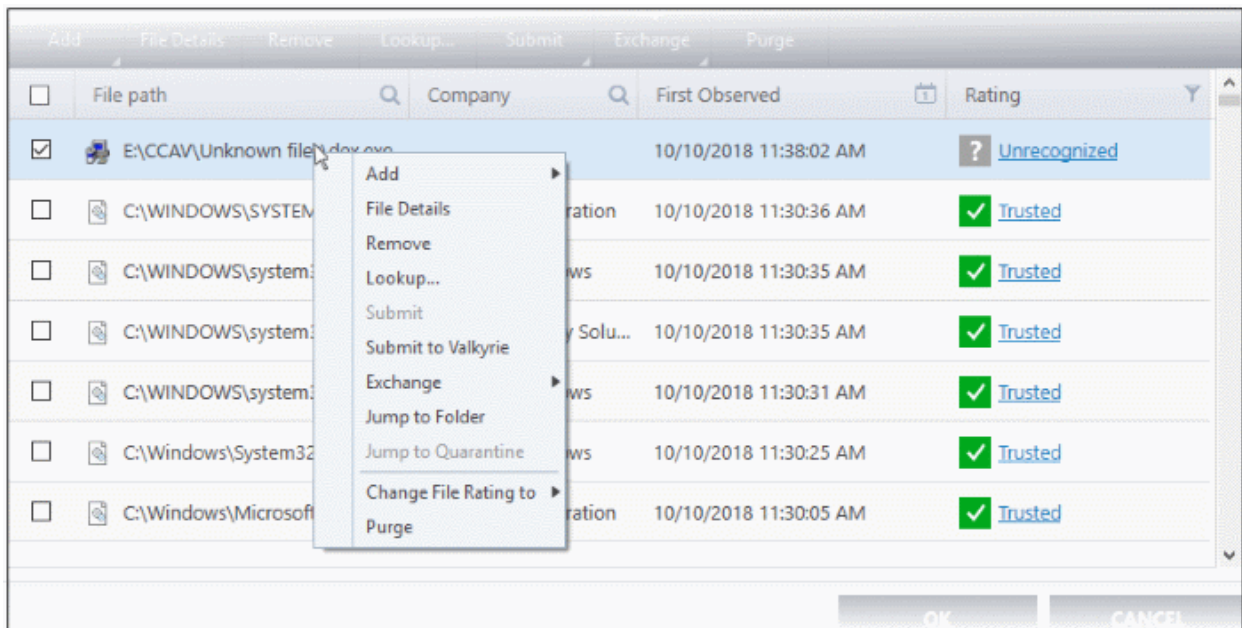
- By clicking on the rating of a file in the 'Rating' column and choosing a new rating from the options



- From the 'File Details' dialog. Select a file and click the 'File Details' button at the top. See **changing the file rating** in **File Details** for more details.

Context Sensitive Menu

Right-clicking on a file opens a context sensitive menu that allows you to view the 'File Details' dialog, remove the file from the list, submit the file to Comodo for analysis and more.



- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo FLS safelist if any details are available.
- **Submit to Valkyrie** - Upload the file to Valkyrie, Comodo's file analysis system.
- **Exchange** - Consists of two options (**Import** and **Export**).
 - **Import** - Import a .xml list of files and file ratings
 - **Export** - Export the current file list and ratings to an .xml file
- **Jump to Folder** - Opens the folder containing the file in Windows Explorer.
- **Jump to Quarantine** - Opens the CCS quarantined files interface.
- **Change File Rating to** - Enables you to change the file rating to: Trusted, Unrecognized, Malicious
- **Purge** - CCS checks whether a listed file is still installed at the path specified, and removes it if it isn't. The default schedule is every four hours. You can also manually remove non-existent files from the file list by clicking 'Purge'.

Sorting, searching and filtering options

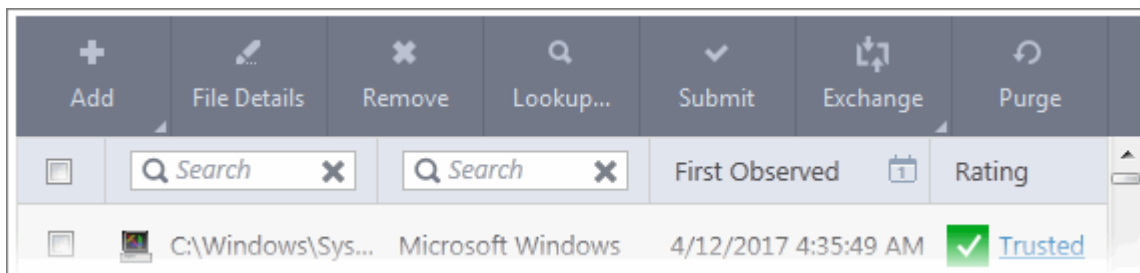
Sorting option

You can sort the items in alphabetical / ascending / descending order by clicking on the respective column headers.

Searching option

You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and 'File rating'.

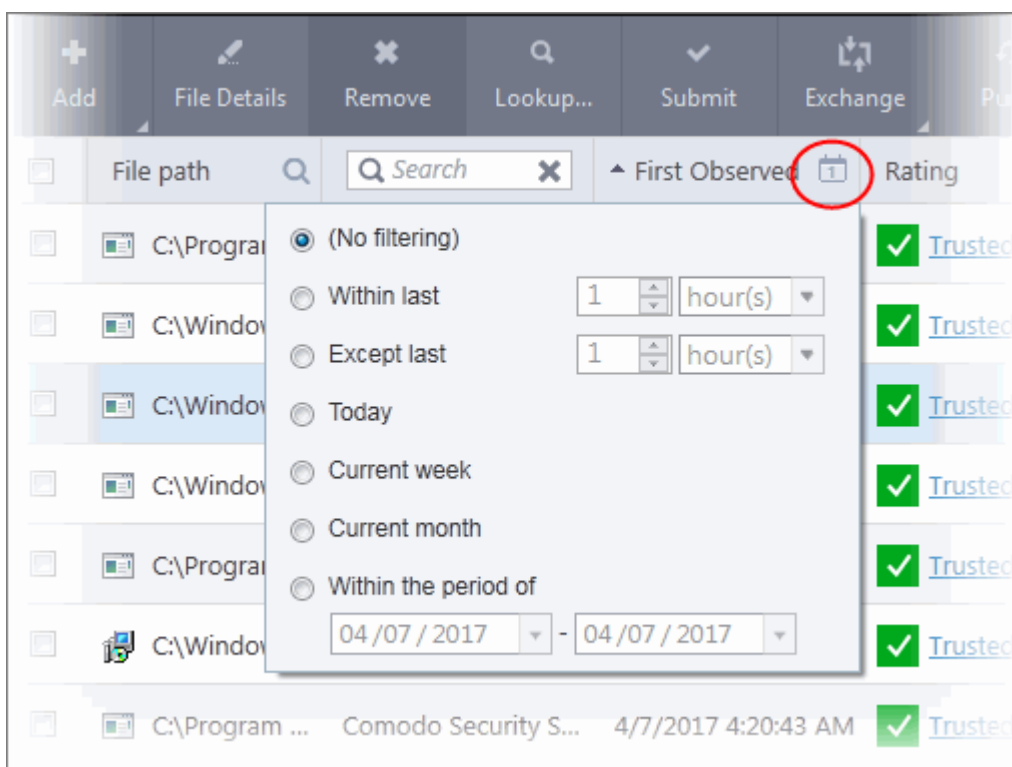
To use the search option, click the search icon at the far right in the 'File path' and/or 'Company' column header.



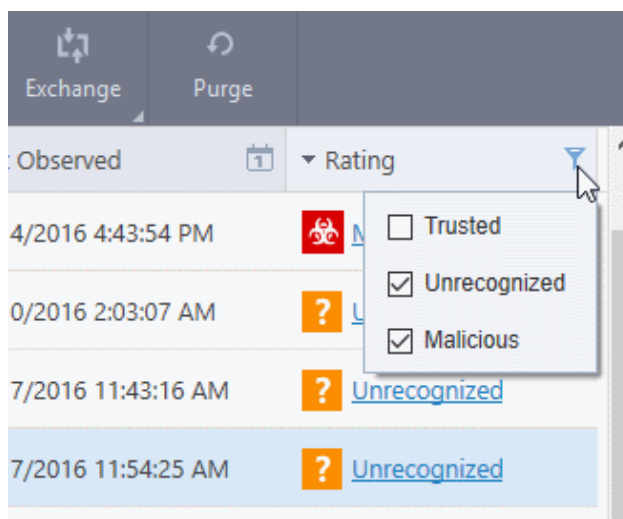
- Enter the file path and/or the name of company in part or full as per the selected criteria in the search field. The result for the entered criteria will be listed automatically within a few moments. Click the 'X' icon to clear the search criteria and display all the items again in the list.

Filtering option

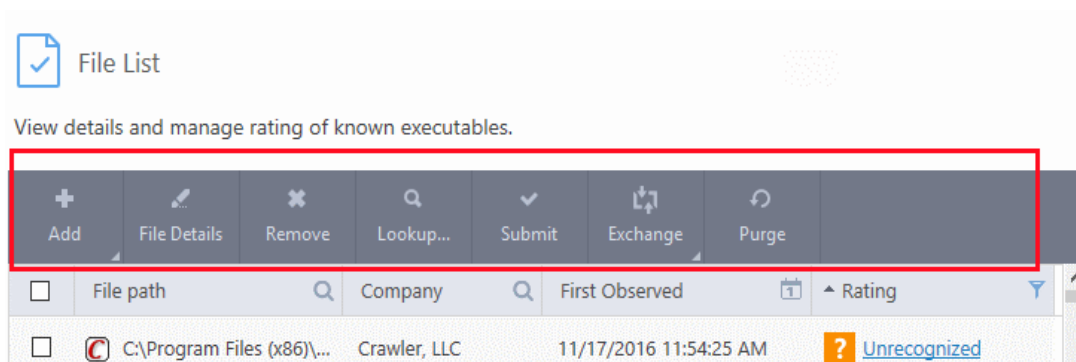
- To filter the list based on the date of installation or storage of the files, click the calendar icon at the right of the 'First Observed' column header and choose the time/date/period.



- To filter the list based on the file rating, click the funnel icon at the right of the 'File Rating' column header and select the specific ratings to display the files.



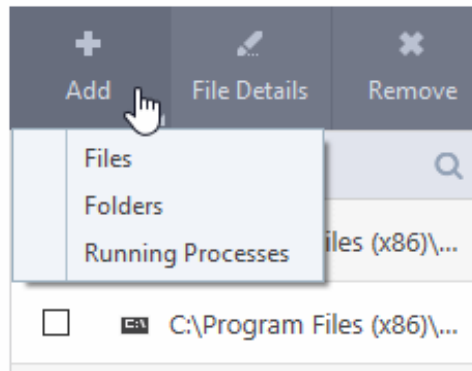
The buttons at the top provide the following options:



- **Add** - Allows you to manually add files, folders and running processes to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup...** - Starts the online lookup of selected file with the master Comodo FLS safelist if any details are available
- **Submit to Valkyrie** - Upload selected files to Valkyrie for behavior analysis.
- **Exchange** - Consists of two options (**Import** and **Export**).
 - **Import** - Allows you to import a file list from an XML file
 - **Export** - Allows you to export the current file list and ratings to an XML file
- **Purge** - Runs a check to verify the listed applications are still installed on the host machine at the stated location. If not, the rule is removed, or 'purged', from the list.

To manually add files to 'File list'

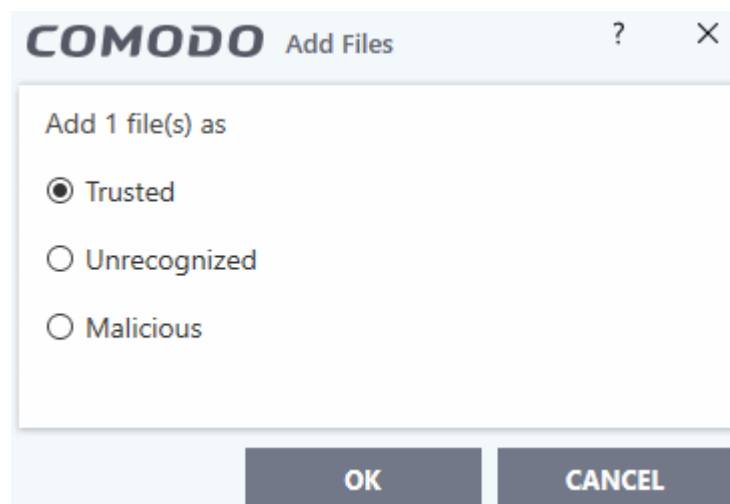
- Click the 'Add' button at the top



Tip: Alternatively, right click inside the File List page and choose 'Add' from the context sensitive menu.

- You can add files to the file list by three ways:
 - **Files** - Allows you to navigate to the file or executable of the program you wish to add and assign a rating.
 - **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'File List' with the rating you assign.
 - **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'File List' with the rating you assign.

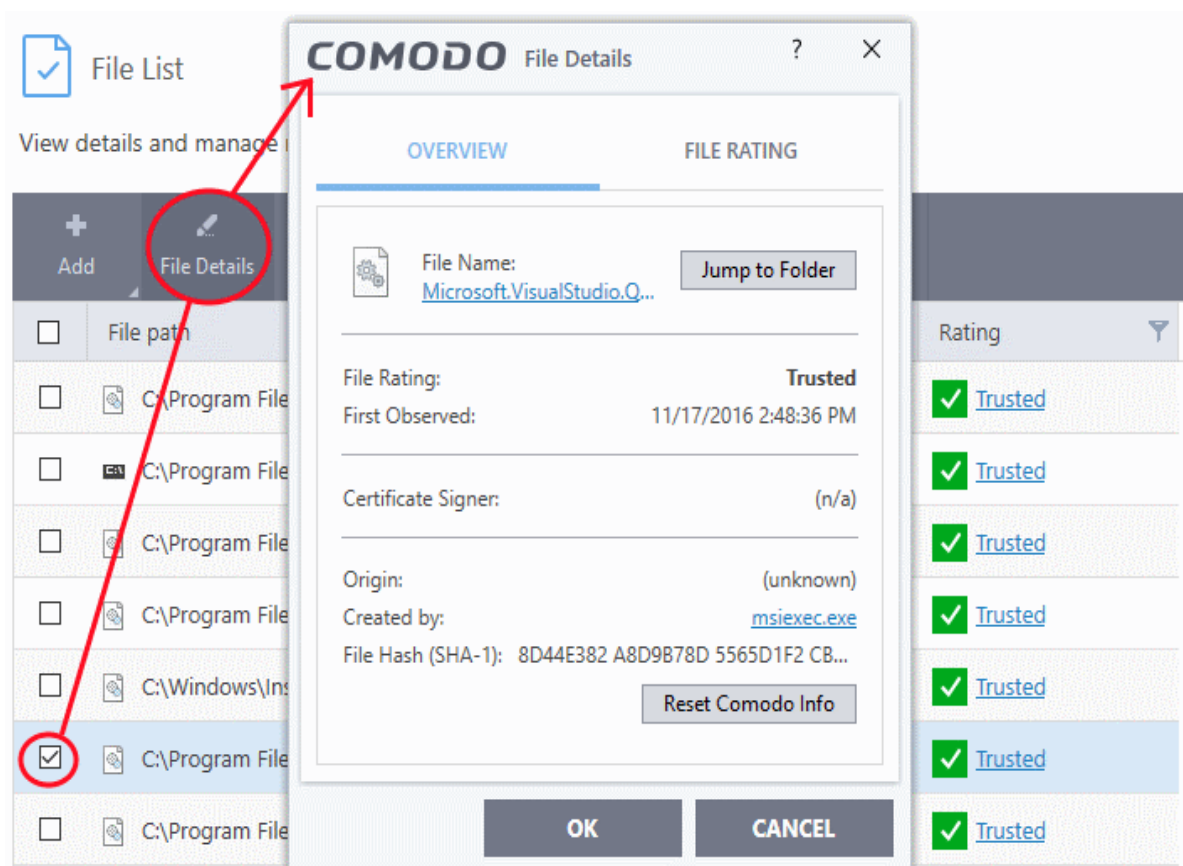
Once you have chosen the file(s) or the folder, you can assign the rating for the file(s) to be added.



- Choose the rating to be assigned to the file(s). The available options are:
 - **Trusted** - The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
 - **Unrecognized** - The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
 - **Malicious** - The file will not be allowed to run.
- Click 'OK' in the 'Add Files' dialog
- Click 'OK' in the 'Advanced Settings' for your changes to take effect.

To view the 'File Details' and change the rating

- Choose the file to view its details and click the 'File Details' button on the 'File List' pane.



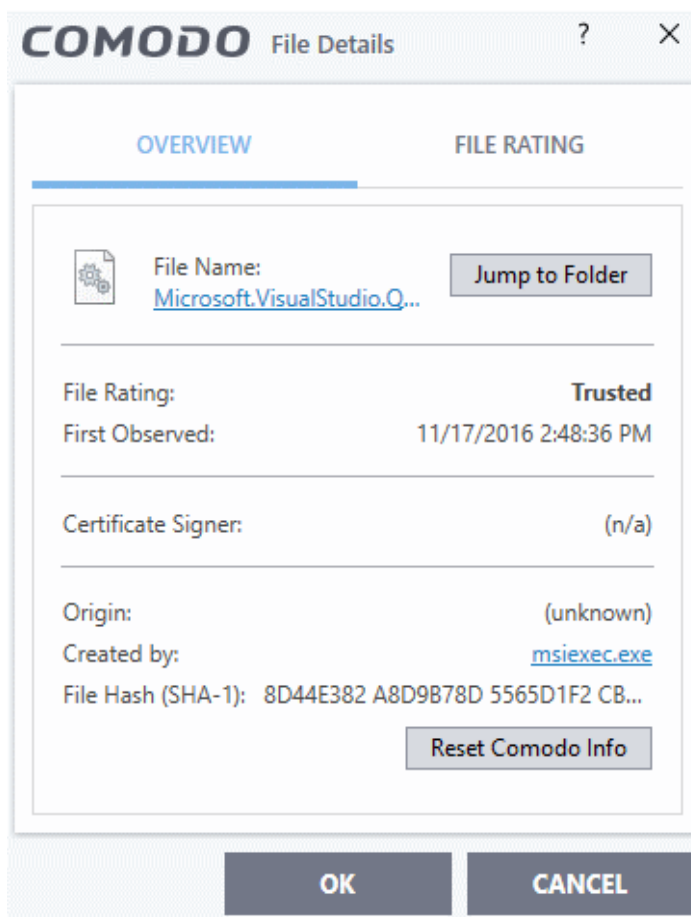
Tip: Alternatively, right click on the selected file inside the File List page and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog contains two tabs:

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

Overview

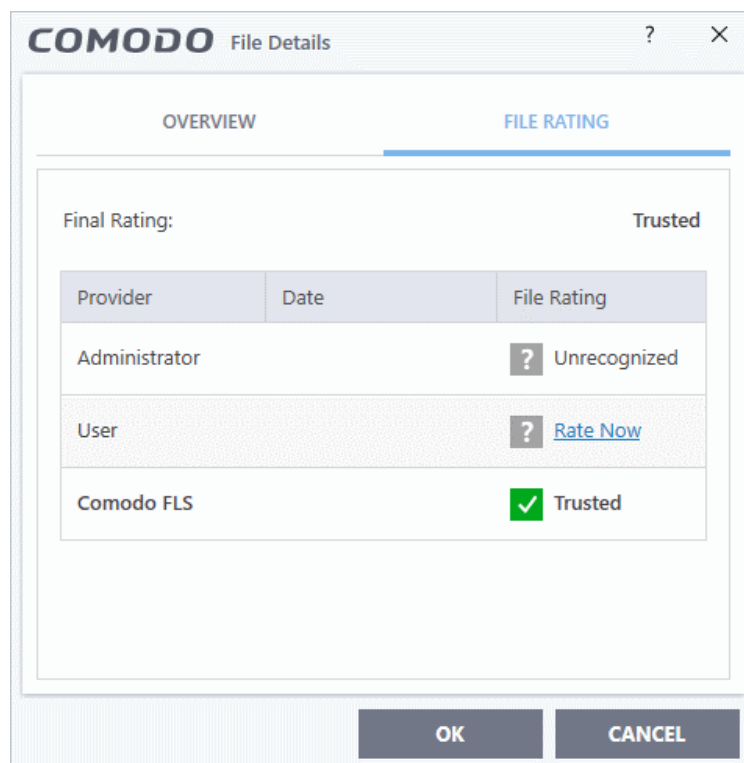
The Overview tab displays the general details of the file and the publisher details.



- Clicking the file name opens the Windows 'File Properties' dialog.
- Clicking 'Jump to folder' opens the folder containing the file in Windows Explorer, with the respective file selected.

File Rating

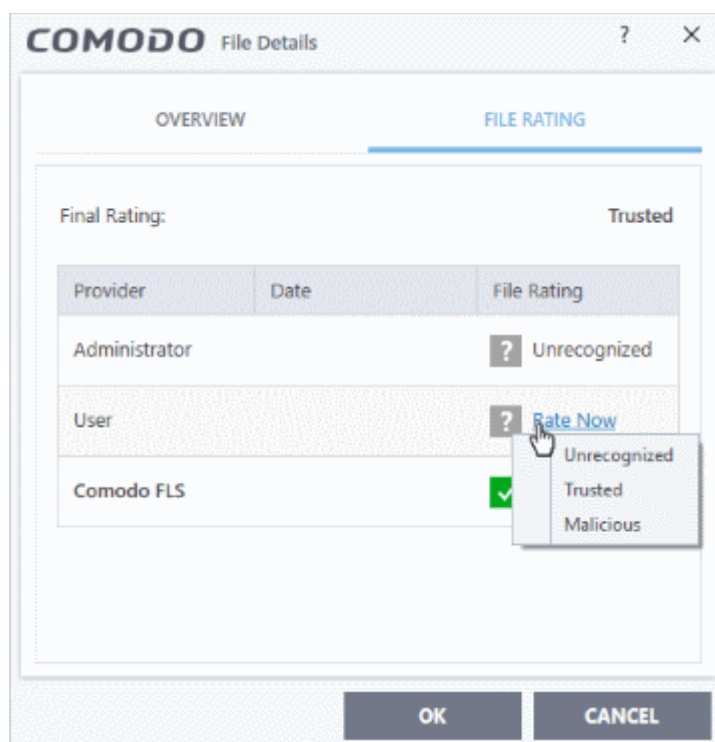
The 'File Rating' tab enables you to change the current rating of the file and displays the current rating as per the analysis result from Comodo.



Note: If the CCS installation is remotely managed by the CESM/Endpoint Manager server on your network, your Administrator's file rating for individual file will override your user file rating.

To change the user rating of the file

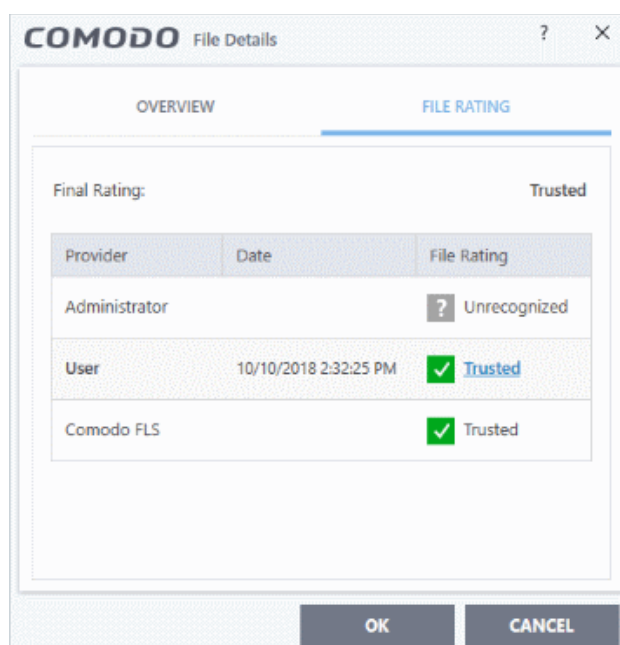
- Select the file from the 'File List' pane and click the 'File Details' button
- Click the 'File Rating' tab
- Click the 'Rate Now' link and choose the rating from the drop-down:



The options available are:

- **Trusted** - The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- **Unrecognized** - The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- **Malicious** - The file will be deleted or placed in quarantine and will not be allowed to run.

Once you chose a rating for a file it will be displayed in the 'User' rating row.



- Click 'OK' in the 'Files Details' dialog

Tip: Alternatively, right click on a selected file, then choose 'Change File Rating to' from context sensitive menu and select the rating.

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

To remove files from the file list

- Select the files you want to remove from in the 'File List' pane.
- Click 'Remove' at the top. This removes the file from the the list but does not delete it from your system.

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Remove' from the context sensitive menu.

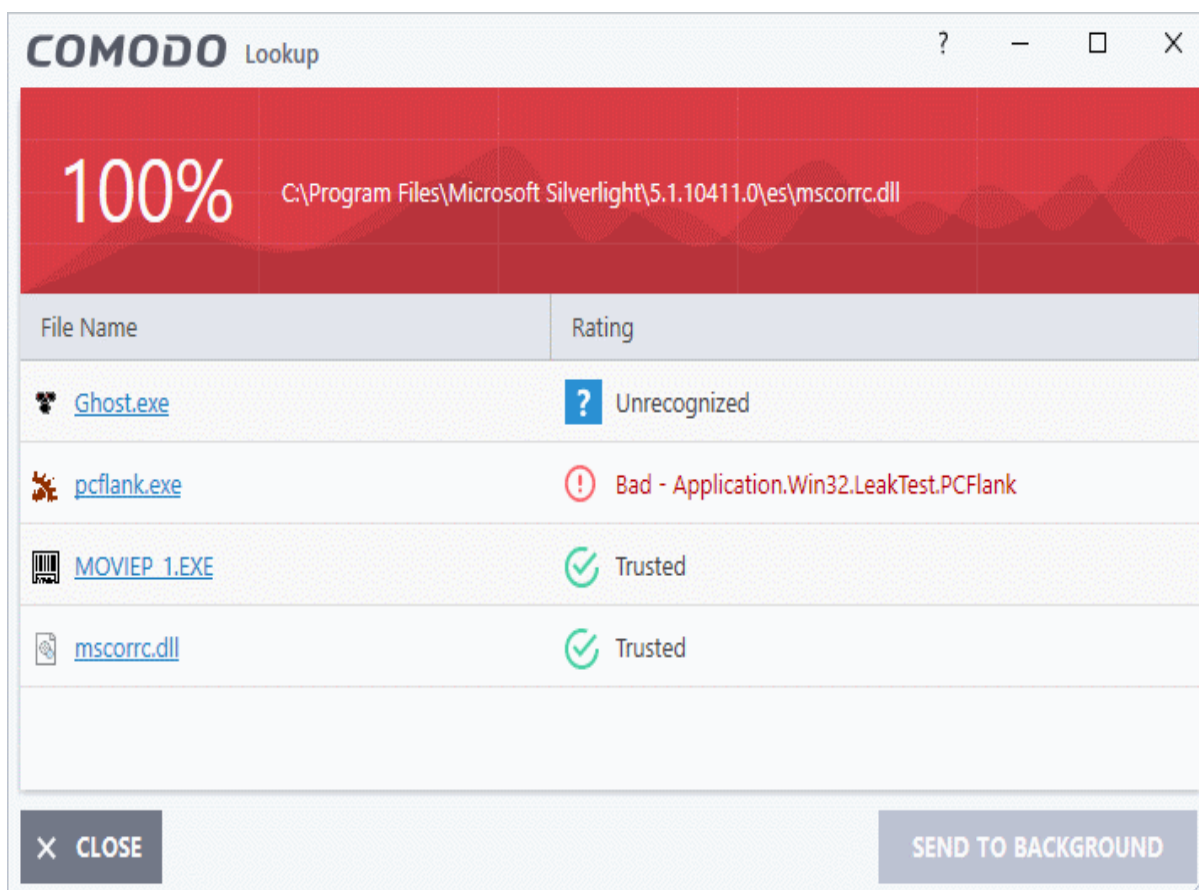
- Click 'OK' for your changes to take effect.

To perform an online lookup for files

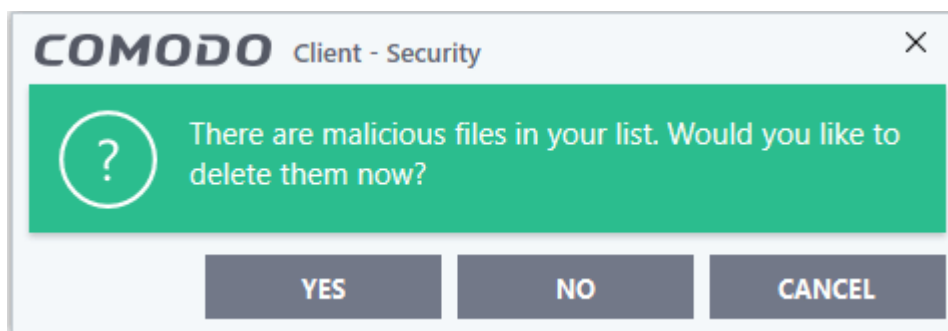
- Select the files to be checked from the 'File list' pane. You can select several entries at once by marking the check-boxes beside the entries.
- Click the 'Lookup...' button at the top from the 'File list' pane.

Tip: Alternatively, right click on a selected file inside the 'File List' page and 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 the description of **changing the file rating** under the section **File Details** for more details.
- If no information is available, it will be indicated as 'Needs to be submitted' with a yellow icon. You can submit the file to Comodo for analysis from the dialog that appears on closing the 'Lookup' dialog. See **explanation below** for more details.

Manually submit files to Valkyrie

Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.

- Click 'Settings' > 'File Rating' > 'File List' to open the file list
- Use the checkboxes to select the files you want to submit. You can send several files at once.
- Click 'Submit' > 'Submit to Valkyrie' in the top-menu. The files will be immediately sent to Valkyrie for analysis.

Tip: Alternatively, right click on a file then choose 'Submit to Valkyrie' from the 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 export the list of files with their currently assigned file ratings to an XML file and store the list on a safe place. This is useful to restore your 'File List', in case you are reinstalling the CCS application for some reasons.

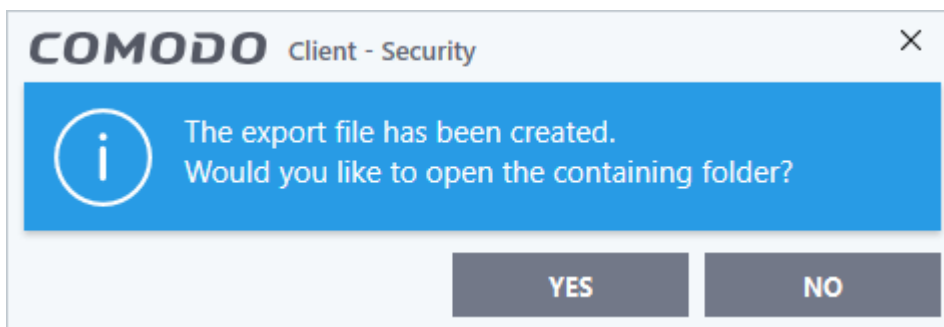
To export the File List

- Click the 'Exchange' button at the top of the 'File List' pane then select 'Export' from the menu

Tip: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Export'

- Navigate to where you want to store the exported list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.



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'.

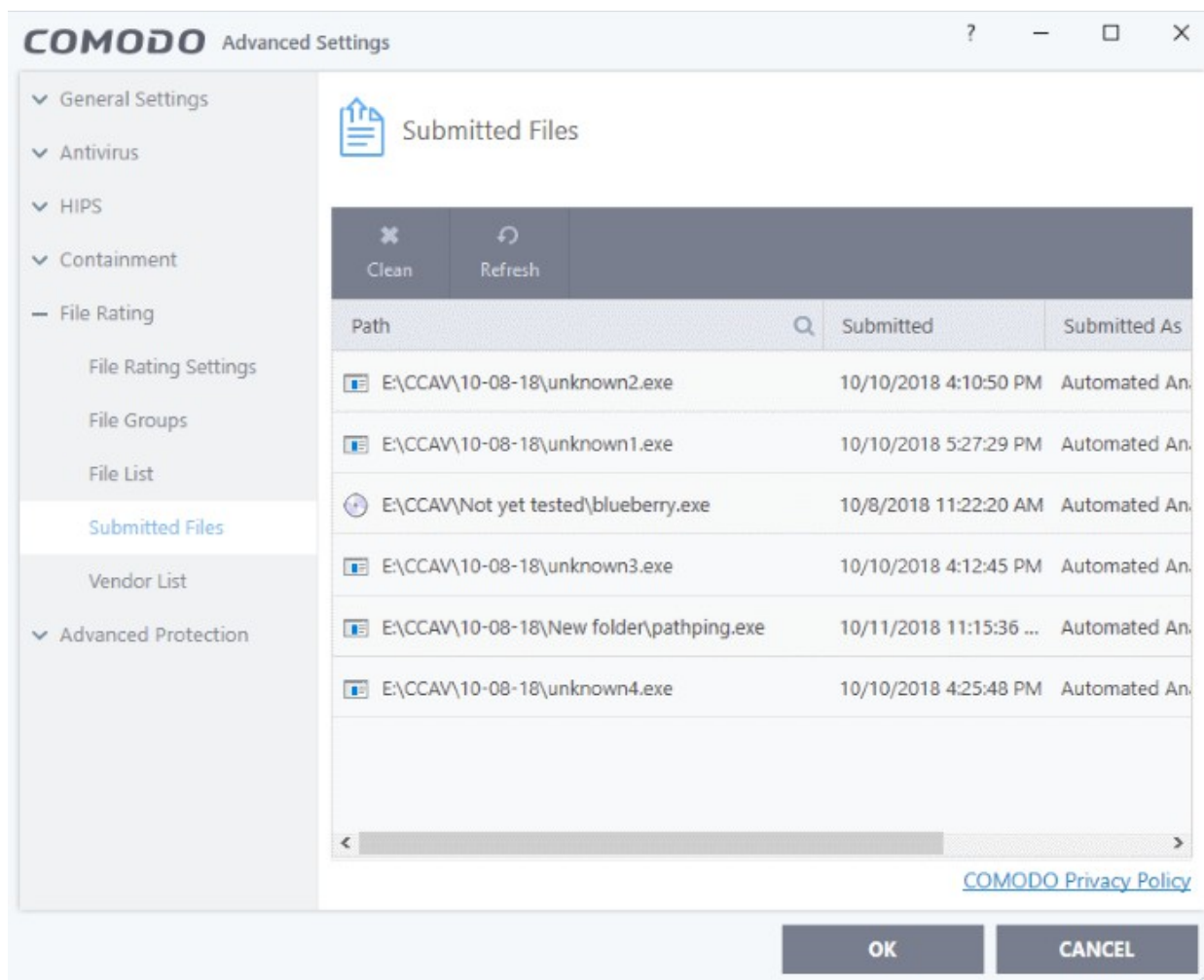
The 'File List' will be populated as per the imported 'File List'.

6.7.4. Submitted Files

- The 'Submitted Applications' area lets you manage files that you have uploaded to Valkyrie for analysis.
- You can submit suspicious files, files with an 'unknown' trust rating, or false-positive files (those files you feel CCS has incorrectly identified as malware).
- Once uploaded, the files will undergo a series of automated tests to establish whether or not they are trustworthy. After manual classification by Valkyrie, they will be added to global white or black list accordingly.

To open the 'Submitted Files' interface

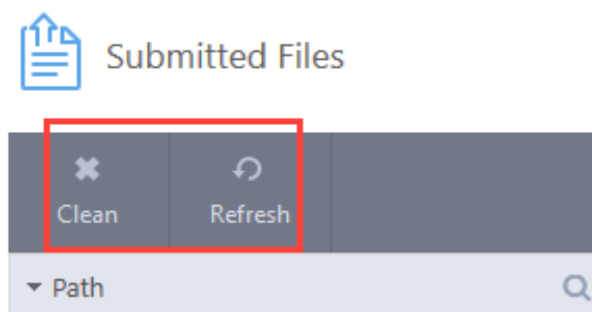
- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'Submitted Files' on the left:



Column Descriptions:

- Path - The location of the file on your computer
- Submitted - Date and time the file was uploaded for analysis;
- Submitted As - The label under which the file was uploaded. Examples include 'automated' and 'contained'.
- Cloud Service - The name of the Comodo cloud service to which the files were submitted. This is usually the Valkyrie analytic system operated by Comodo.

The buttons at the top provide the following options:



- **Clean** - Clears the list
- **Refresh** - Reloads the list to add items that are submitted recently

6.7.5. Vendor List

- Click 'Settings' > 'File Rating' > 'Vendor List' to open this interface

There are three basic methods in which an application can be treated as safe.

- It is on the Comodo safe list (a global white-list of trusted software).
- The file was manually added to 'Trusted Applications' by the user
- It is digitally signed by a trusted vendor in the vendor list

Unknown files are handled as follows:

- If the file vendor has a 'Trusted' rating AND '**Rate applications according to their vendor rating**' is enabled, then the application is trusted and allowed to run.

The vendor rating priority is as follows:

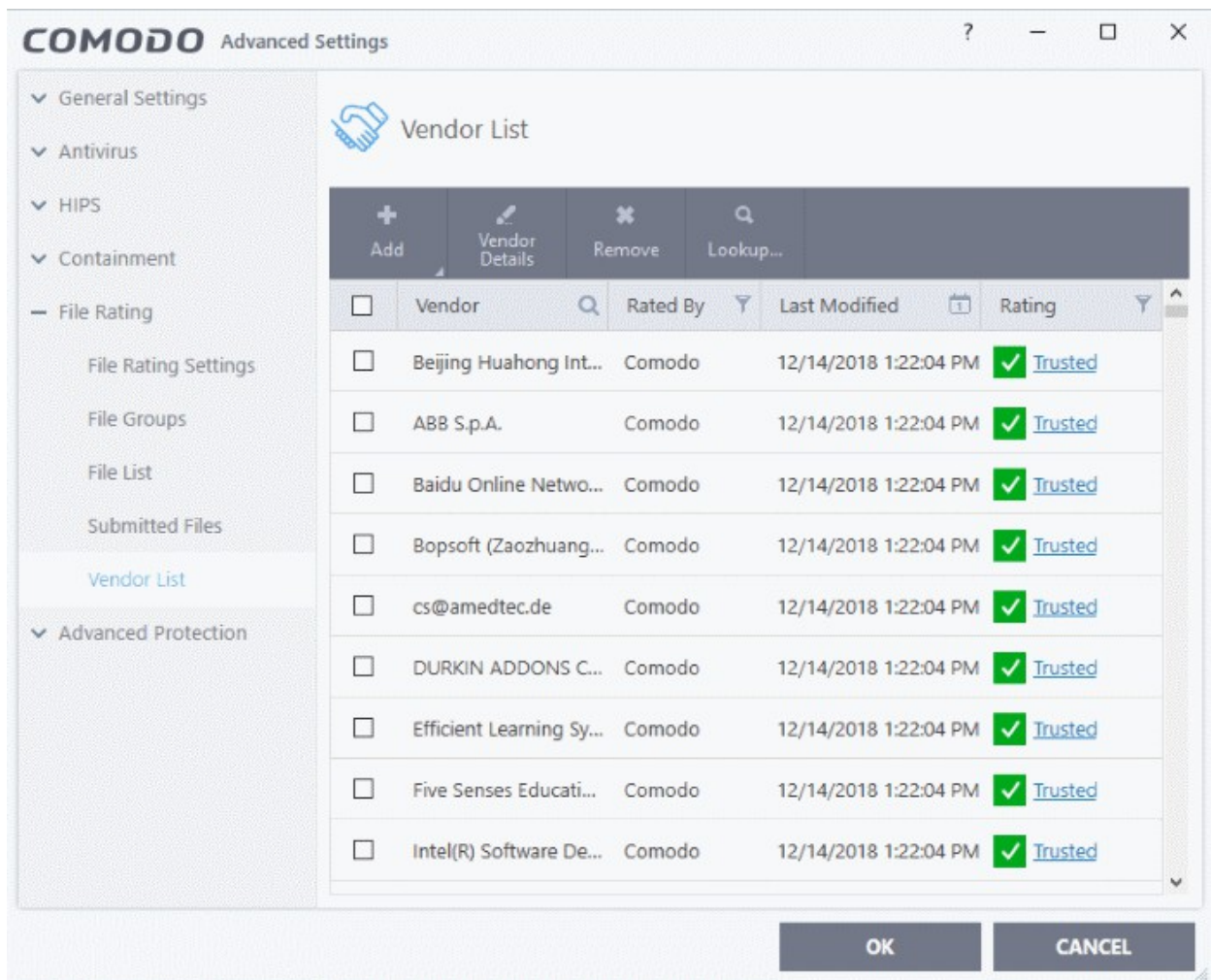
- Admin
 - User
 - Comodo
- If the file vendor is not on the vendor list OR '**Rate applications according to their vendor rating**' is disabled, then the application is run in the container.

If the application in question is an installer then CCS will generate an elevated privilege alert.

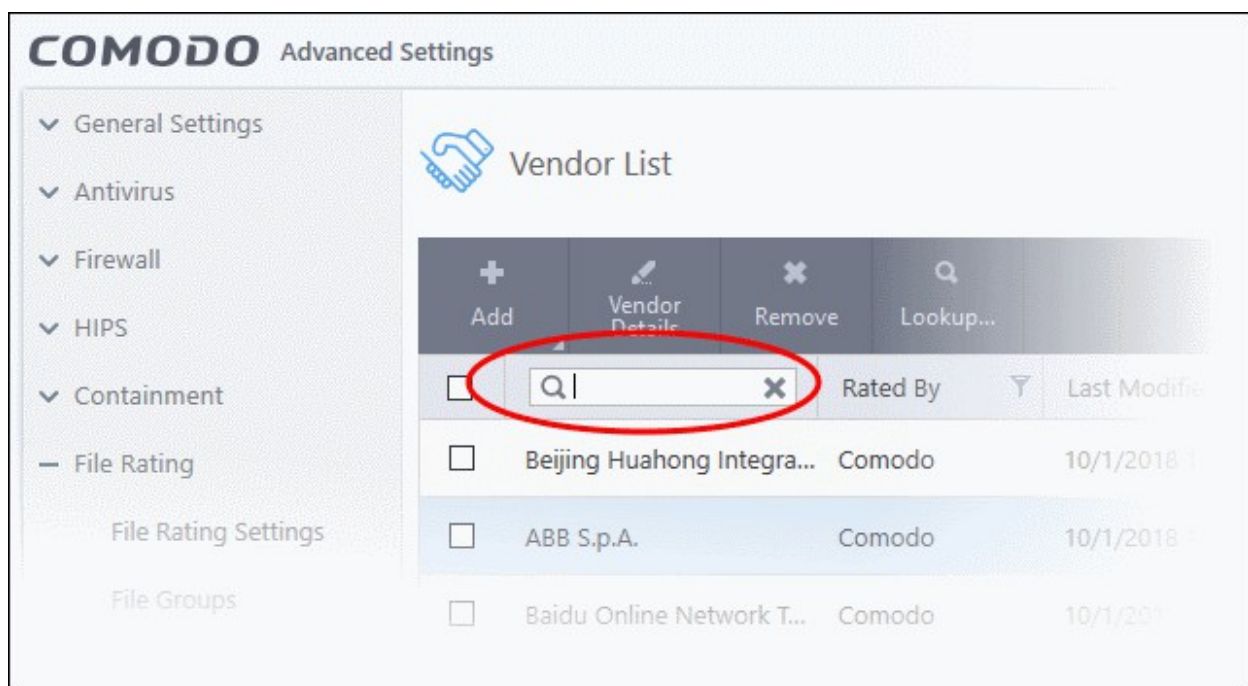
CCS ships with a list of trusted software publishers. Vendors can get their signatures added to this list by contacting Comodo with their software details. [Click here](#) to read more about this.

You can view the vendor list as follows:

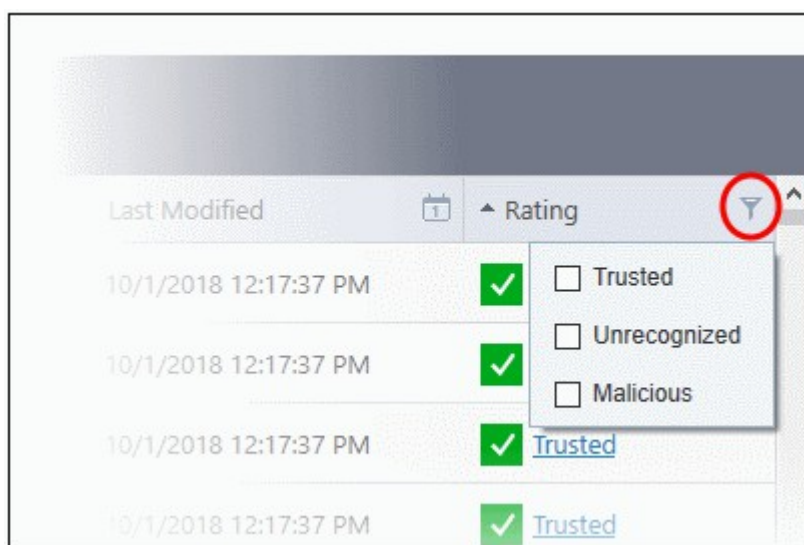
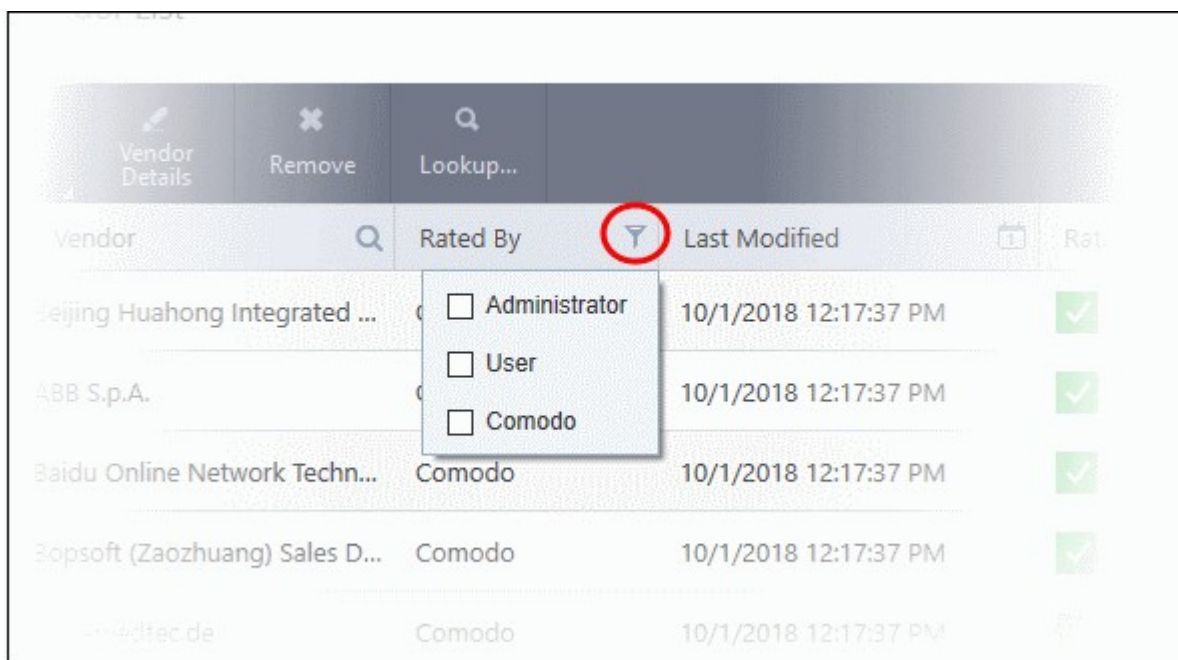
- Click 'Settings' > 'File Rating' > 'Vendor List' to open the interface



- Click the magnifying glass in the vendor column to search for a specific vendor:



- Click the funnel icons in the 'Rated by' or 'Rating' columns to apply further filters:



- [Click here for background information on digitally signing software](#)
- [Software Vendors - click here to get your software whitelisted](#)

The interface allows you to:

- **Re-rate a software vendor**
- **Add \ define a locally trusted vendor**
- **View vendor details and reset user rating**
- **View Comodo rating of software vendors**

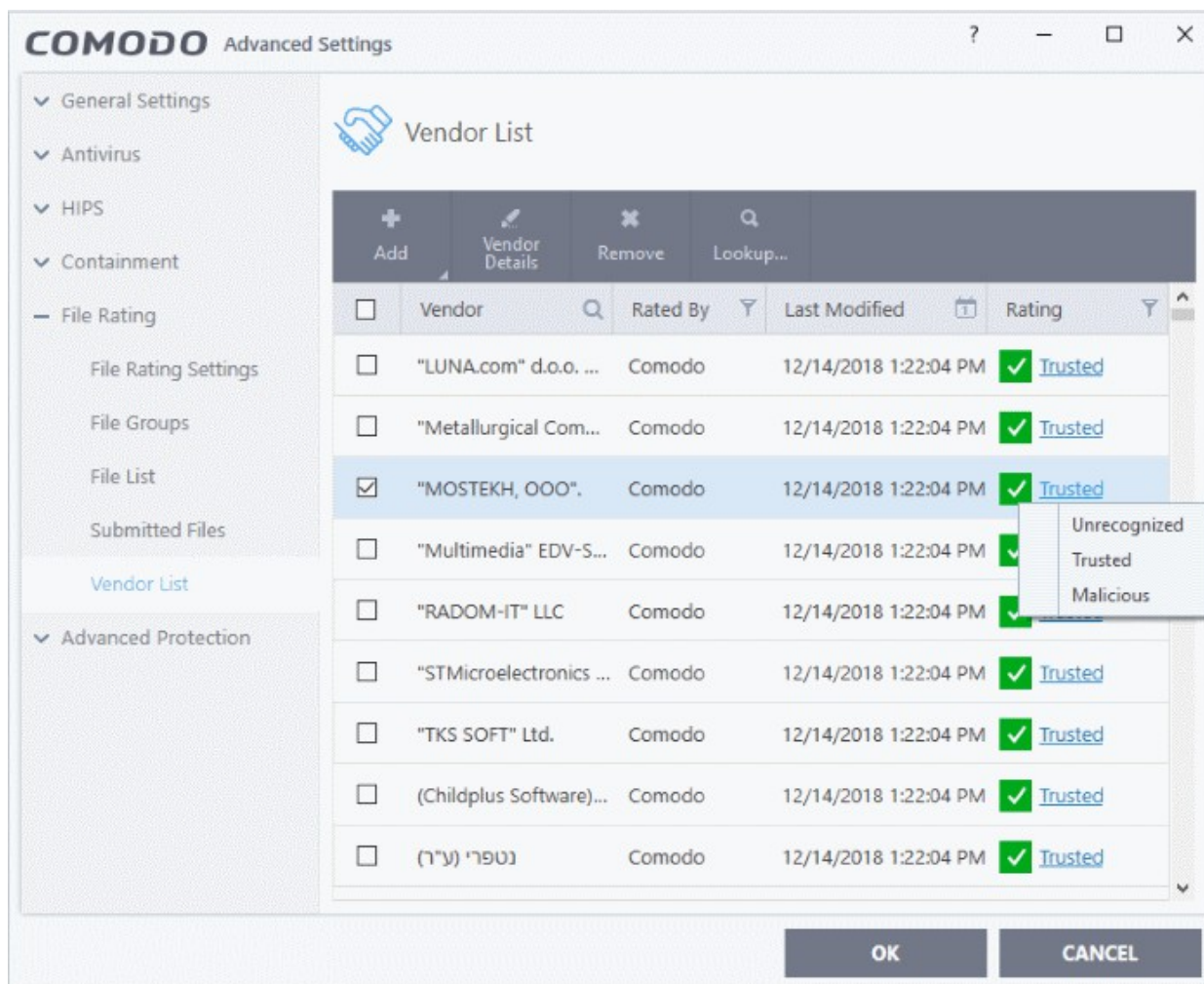
Re-rate a Software Vendor

- CCS ships with a list of trust-rated software vendors. You can re-rate vendors as required.
- Vendor rating priority is as follows:

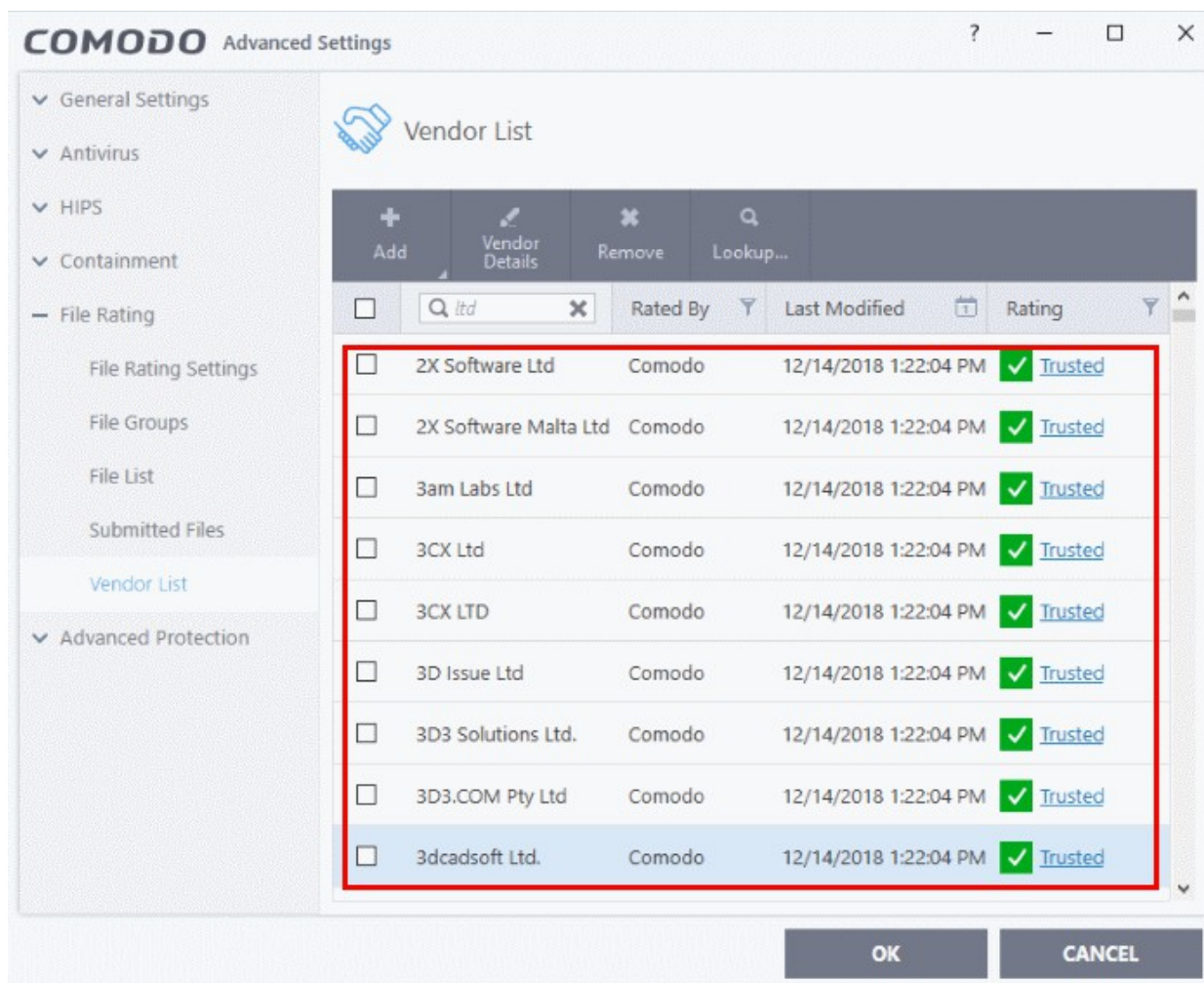
- Admin rating > User rating > Comodo rating

To re-rate a software vendor

- Click 'Settings' > 'File Rating' > 'Vendor List'
- Select a vendor from the list then click the link in the 'Rating' column:



- Select the new rating from the options.
- Click 'OK' to save your changes.
- CCS will obey ratings in the following order - Admin rating > User rating > Comodo rating
 - An application can have multiple ratings



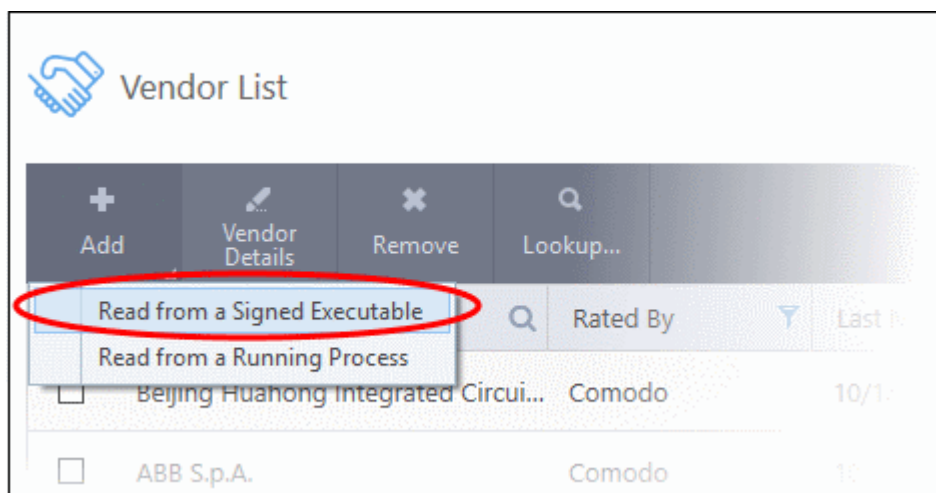
Add \ Define a Locally Trusted Vendor

A software vendor can be added to the local vendor list in two ways:

- **By reading the vendor's signature from an executable file on your local drive**
- **By reading the vendor's signature from a running process**

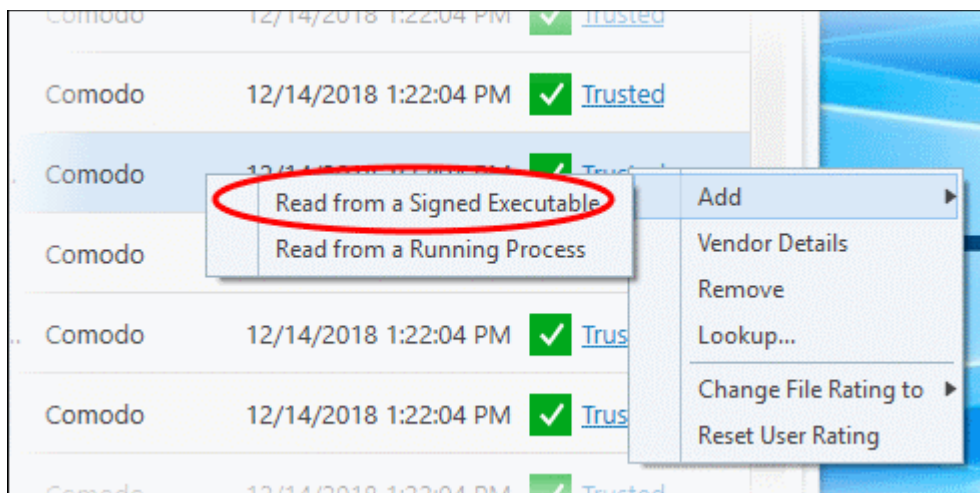
To add a trusted vendor by reading the vendor's signature from an executable

- Click 'Settings' > 'File Rating' > 'Vendor List'
- Click the 'Add' button at the top and select 'Read from a signed executable':



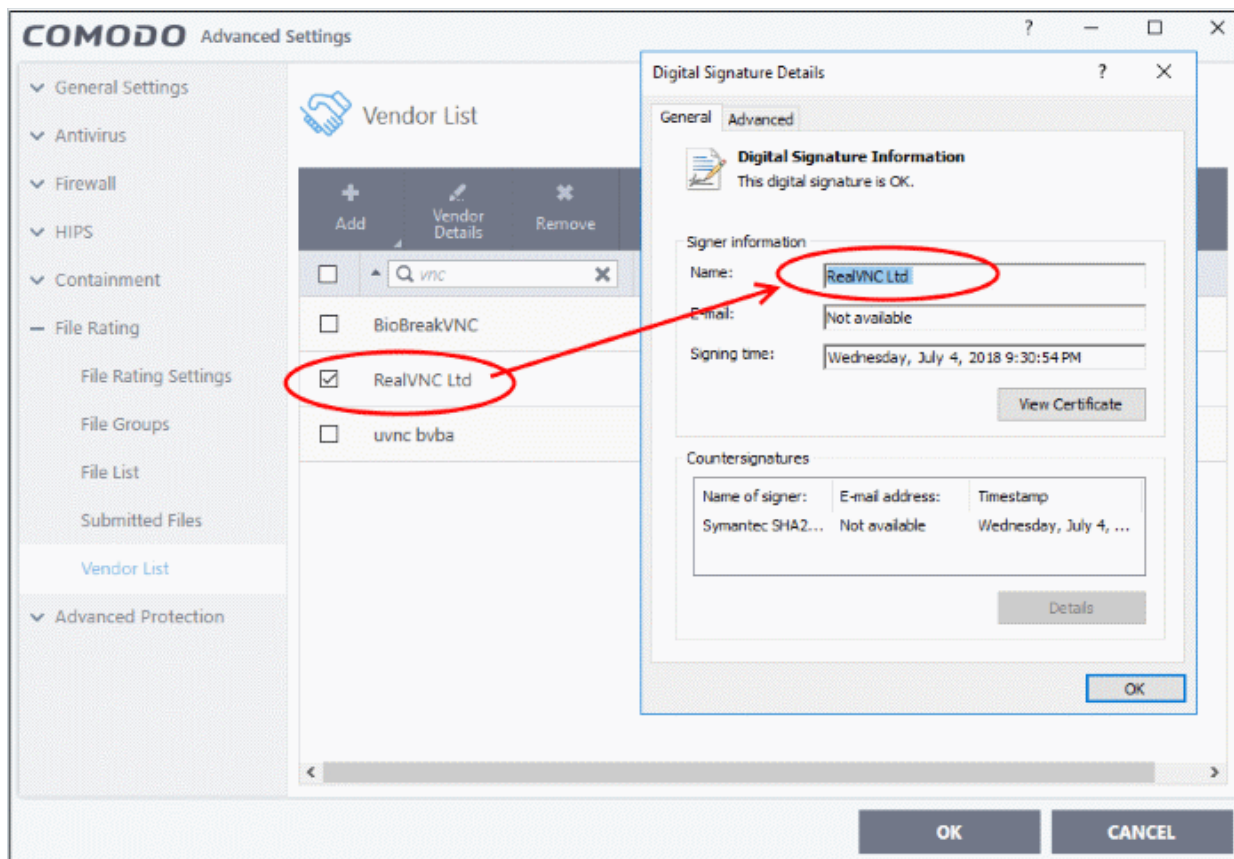
OR

- Right-click on the vendor and select 'Read from a signed executable':



- Browse to the location of the executable your local drive. In the example below, we are adding the executable 'vncviewer.exe'.

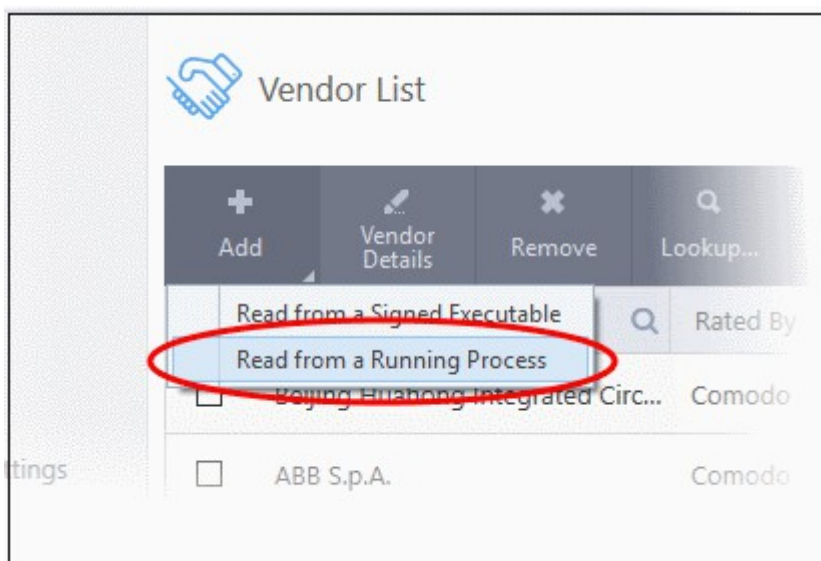
Comodo Client Security checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the local trusted vendor list (TVL):



- In the example above, Comodo Client Security was able to verify the signature on vncviewer.exe because it had been counter-signed by the trusted CA 'Symantec'.
- The signer of the software, 'RealVNC Ltd', is now a trusted software vendor. All future software signed by 'RealVNC Ltd' is automatically trusted UNLESS you change this **setting** in 'File Rating Settings'.

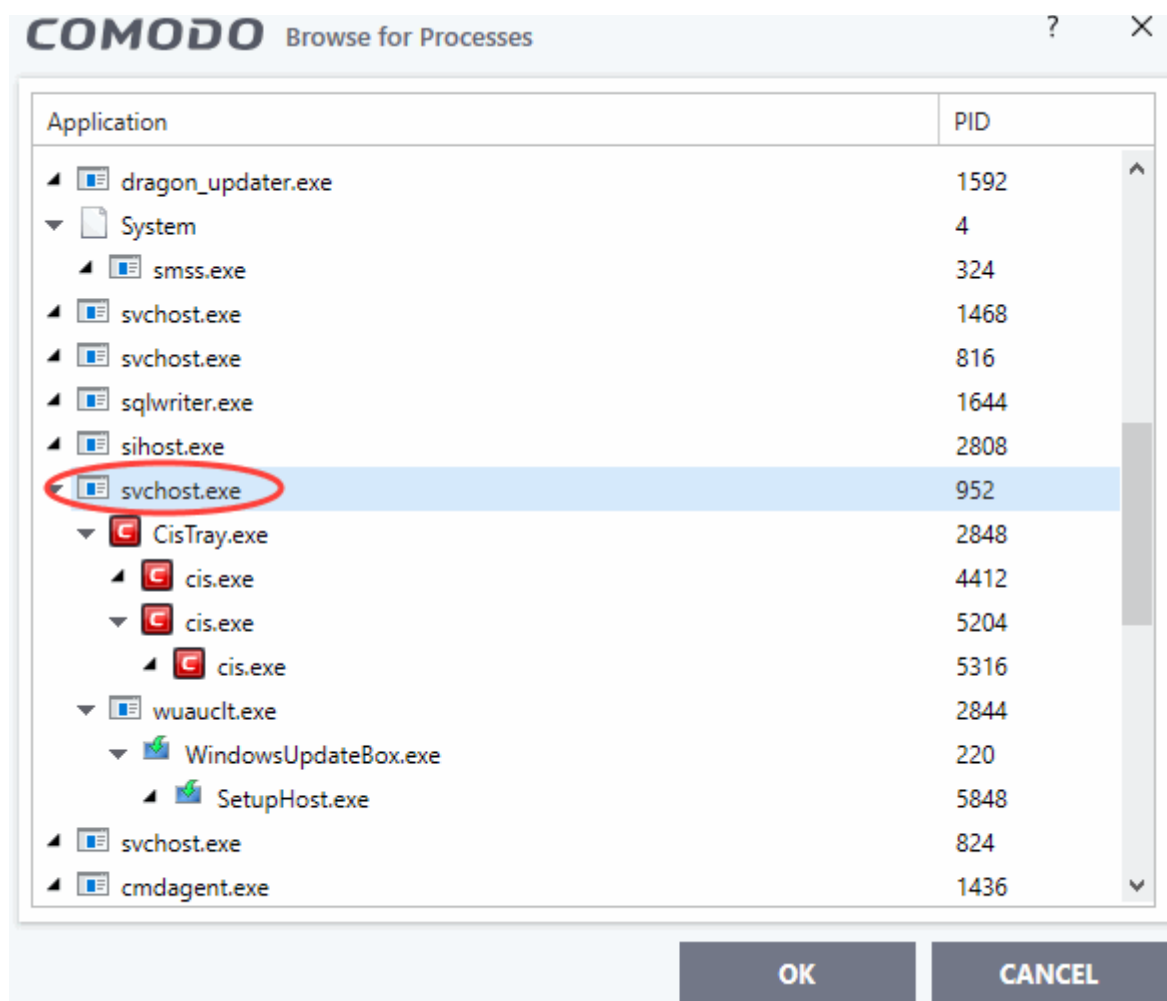
To add a trusted vendor from a currently running process

- Click the 'Add' button at the top and select 'Read from a running process'



OR

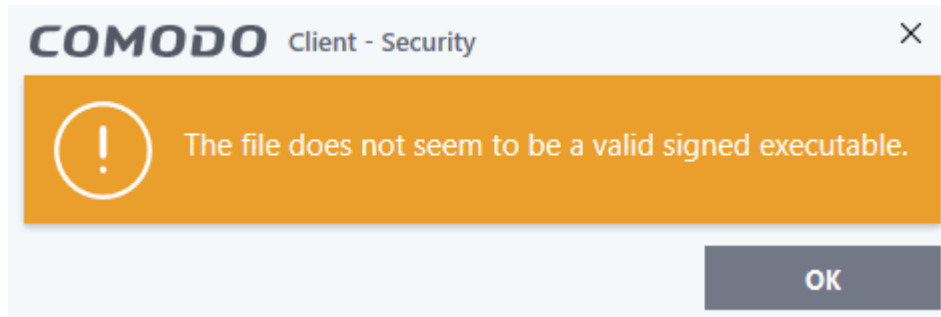
- Right-click on the vendor and select 'Read from a Running Process':
- Select the signed executable that you want to trust and click the 'OK' button.



Comodo Client Security performs the same certificate check as described above. If the parent application of the selected process is signed, CCS adds the vendor to the list as trusted.

If CCS cannot verify that the software's certificate is counter-signed by a trusted CA then it does not add the vendor to the list. You will see the following error message.

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

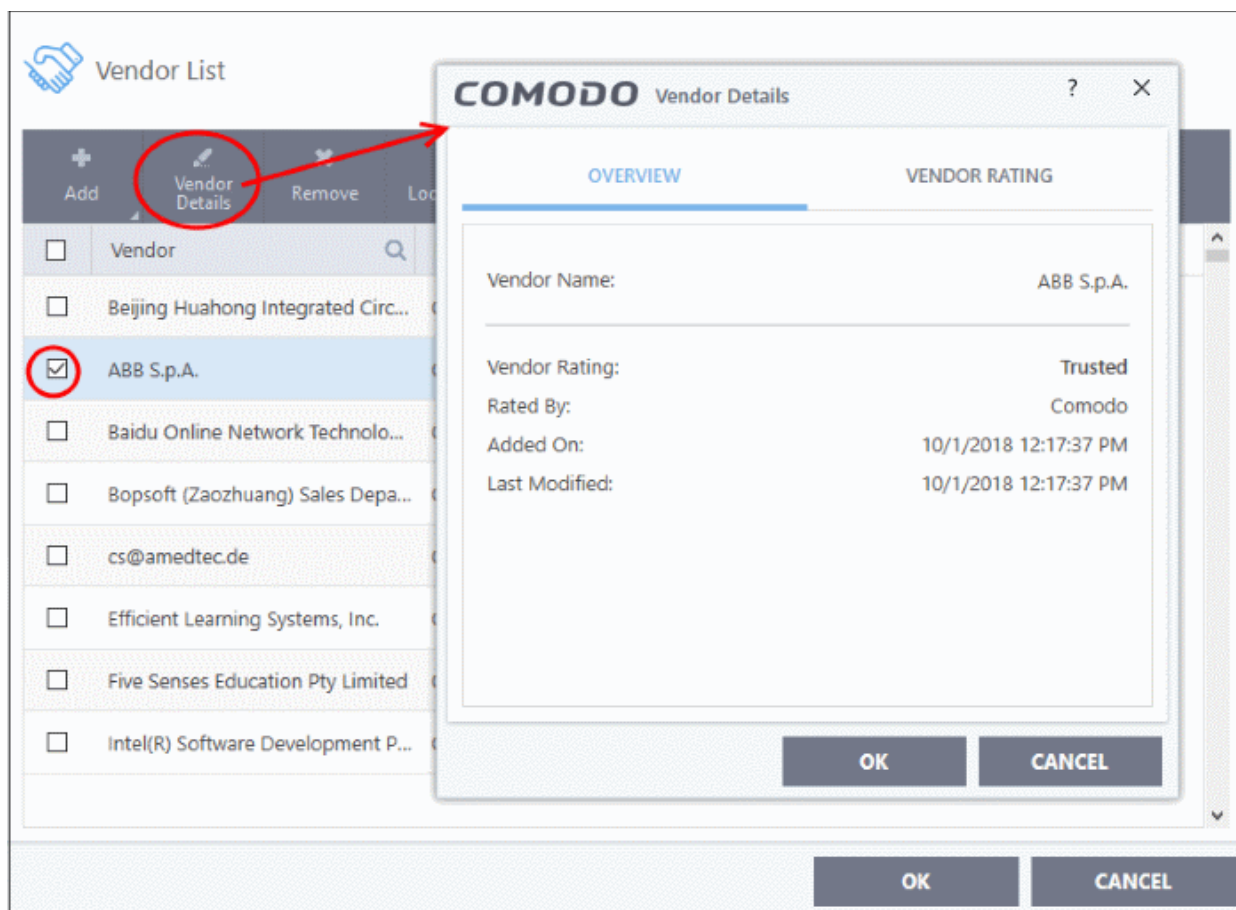


- User defined trusted software vendors - As the name suggests, these are added by the user via one of the two methods outlined earlier. These vendors can be removed by the user by selecting and clicking the 'Remove' button.
- Comodo defined trusted software vendors - These are the vendors that Comodo,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

View Vendors Details and Reset User Rating

The 'Vendor Details' dialog provides information about the software published. Details include its rating by the admin, user and Comodo and so on.

- Click 'Settings' > 'File Rating' > 'Vendor List'
- Select the vendor and click 'Vendor Details'



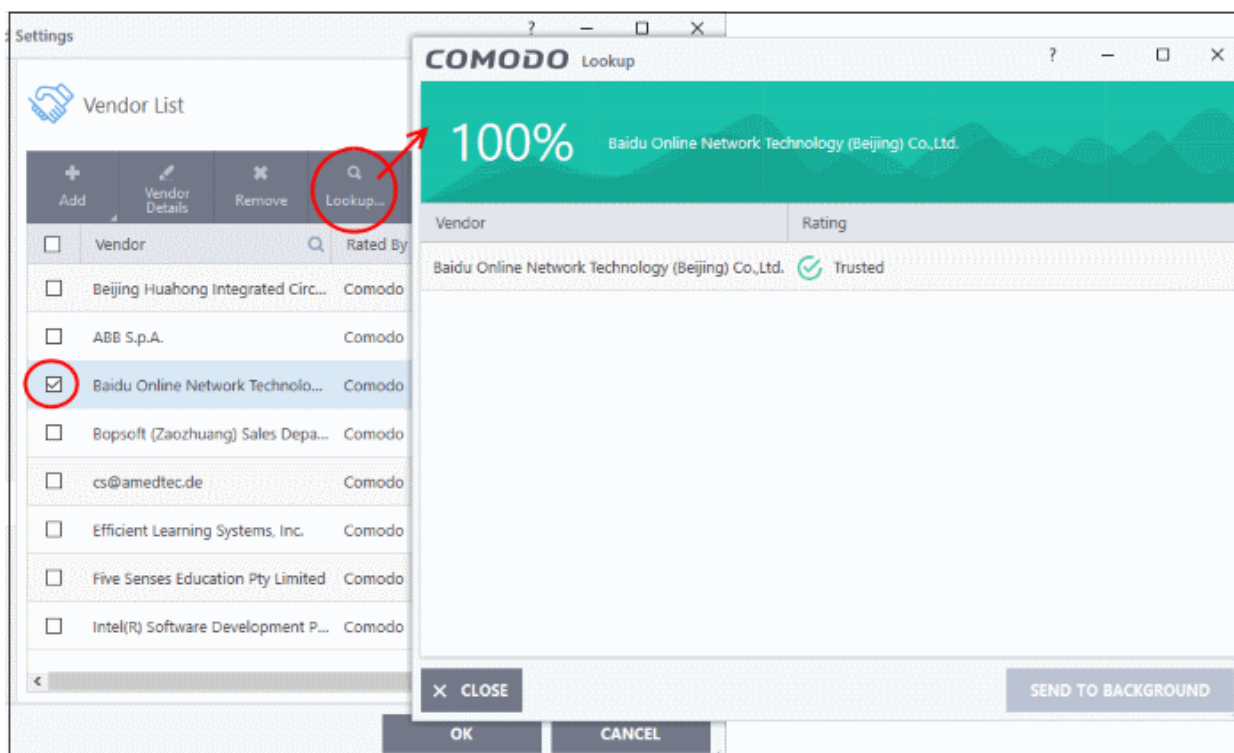
OR

- Right-click on the vendor and select 'Vendor Details/ Reset User Rating':
- **Overview** - General information about the vendor
- **Vendor Rating** - Shows rating by the admin, user and Comodo. Click the 'Rate Now' link beside 'User' to change the vendor rating.

View Comodo Rating of Software Vendors

You can check the rating of the vendors online to view the latest rating from Comodo servers.

- Select the vendor from the list and click 'Lookup...'



OR

- Right-click on the vendor and select 'Lookup':
- CCS will check with Comodo servers and provide the latest vendor rating.

Background information on digitally signing software

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

- Content Source:** The software they are downloading and are about to install *really comes from the publisher that signed it.*
 - Content Integrity:** That the software they are downloading and are about to install *has not be modified or corrupted since it was signed.*
- In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with. They know they are downloading and installing the genuine software.
 - The 'Vendors' that digitally sign their software are the software publishers. These are the company names you see listed in the graphic above.
 - However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Certificate Authority' (CA).
 - 'Comodo CA Limited' and 'Verisign' are two example CAs who are authorized to counter-sign 3rd party software.
 - The counter-signature is critical to the trust process. A CA only counter-signs a certificate after it has conducted detailed background checks on the publisher.

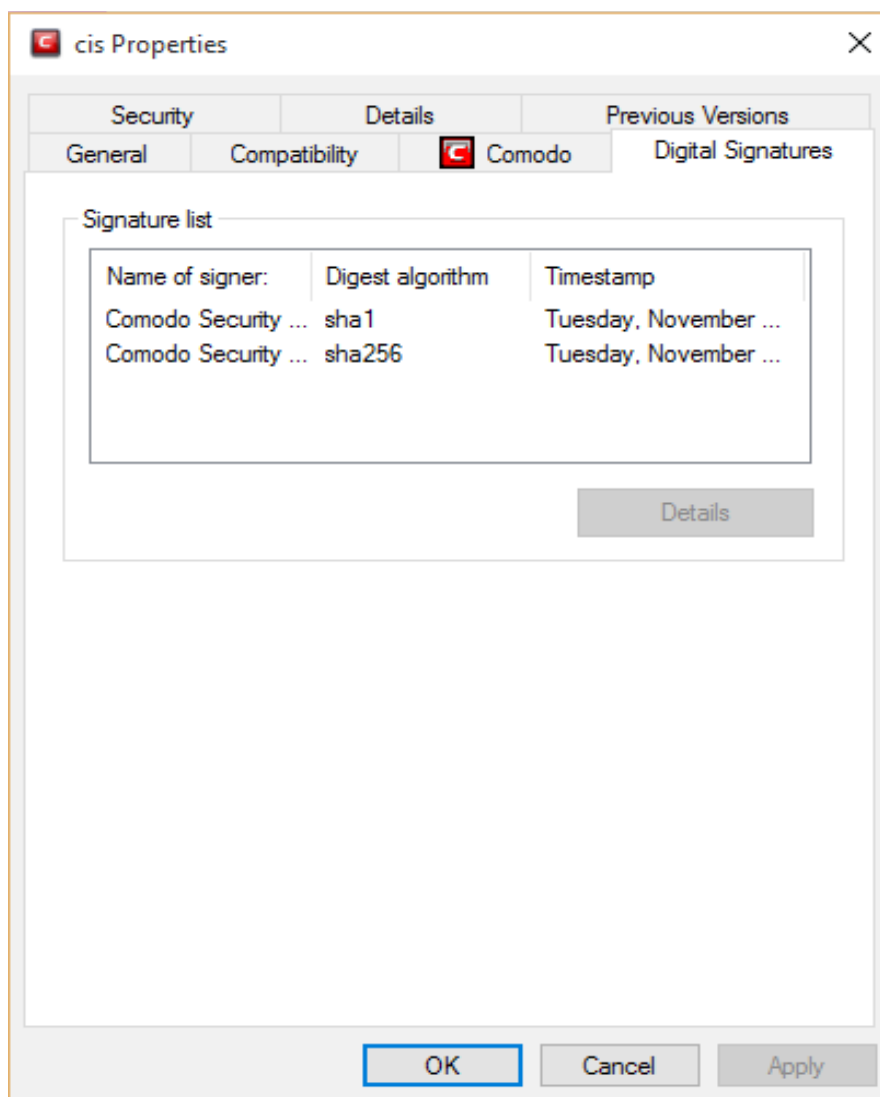
If a file is signed by a 'Trusted Software Vendor' and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Client Security (if you would like to read more about code signing certificates, see <http://www.instantssl.com/code-signing/>).

- One of the methods of identifying whether an executable file has been digitally signed is by checking the properties of the .exe file in question.
- For example, the main program executable for Comodo Client Security is called 'ccs.exe' and has been

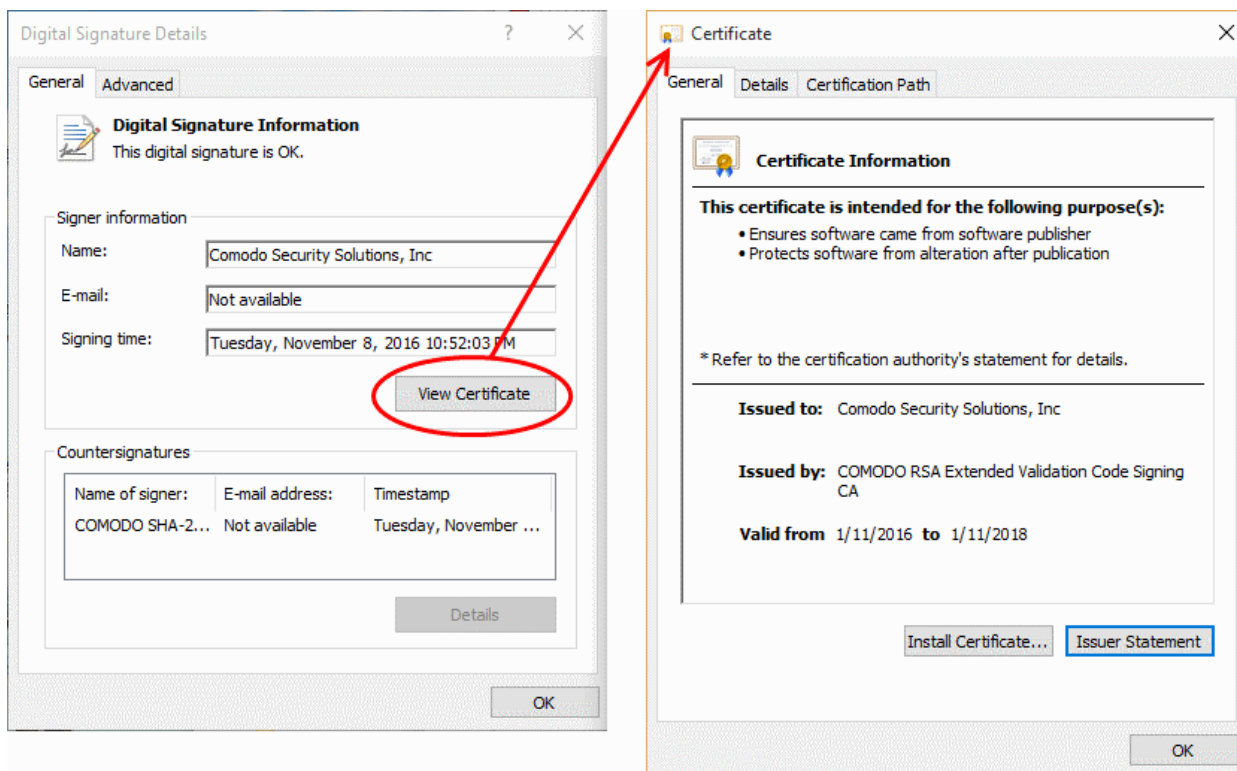
digitally signed.

- Browse to the (default) installation directory of Comodo Client Security.
- Right click on the file ccs.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 'ccs.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different. See [this example](#) for more details.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default 'Vendor List' as trusted that is shipped with Comodo Client Security. This service is free of cost and is also open to vendors who have used code signing certificates from any Certificate Authority. Upon adding the software to the vendor list as trusted, CCS 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 Vendors list as trusted 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 Vendor list as trusted of the next release of CCS.

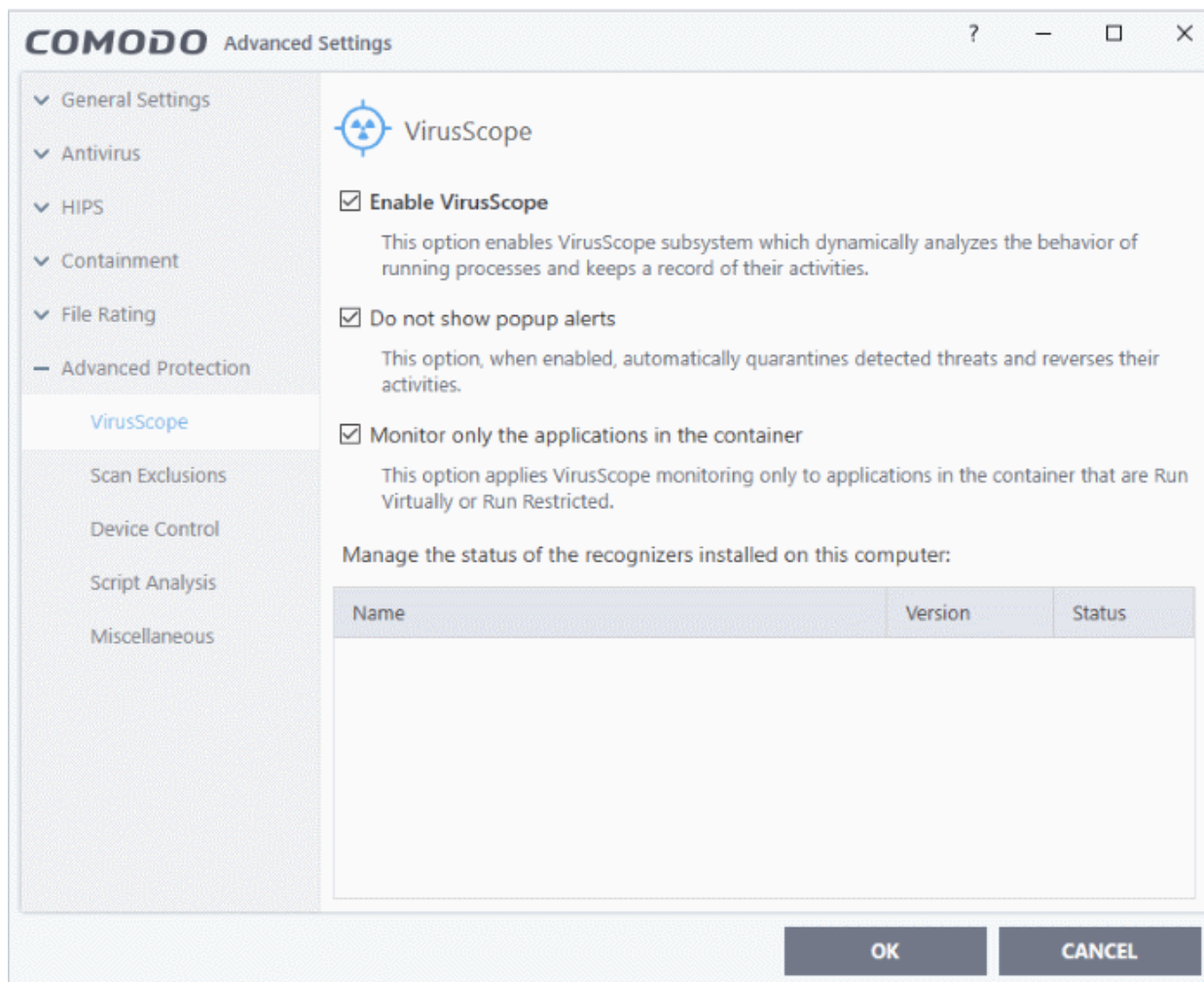
More details are available at <http://internetsecurity.comodo.com/trustedvendor/overview.php>

6.8. Advanced Protection

The 'Advanced Protection' section lets you view and configure VirusScope, device control, script analysis and other miscellaneous settings.

To open the 'Advanced Protection' area:

- Click 'Settings' on the CCS home screen then 'Advanced Protection' on the left:

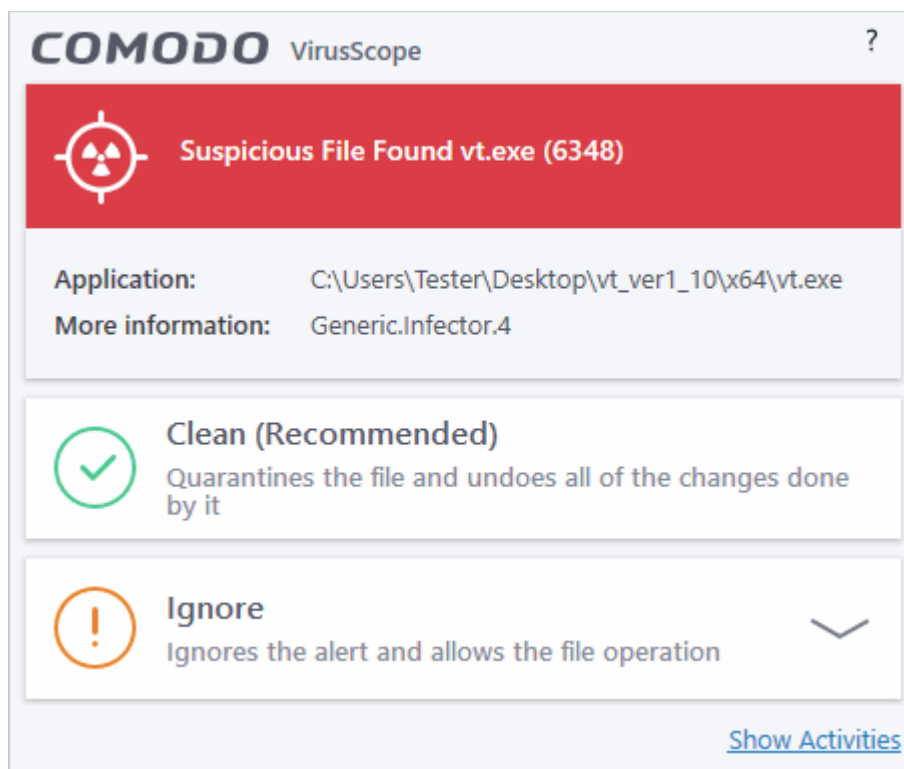


Click the following links to jump to the section you need help with:

- **VirusScope Settings** - Configure VirusScope behavior
- **Scan Exclusions** - Select items which should be skipped during real-time, on-demand and scheduled virus scans.
- **Device Control Settings** - Settings which determine whether endpoints can access USB drives, blue-tooth devices, printers etc.
- **Script Analysis** - Configure heuristic command line analysis for applications and auto-run entries.
- **Miscellaneous Settings** - View and configure analysis of executed code, monitor file types against buffer overflows and set alerts when programs try to modify your browser settings

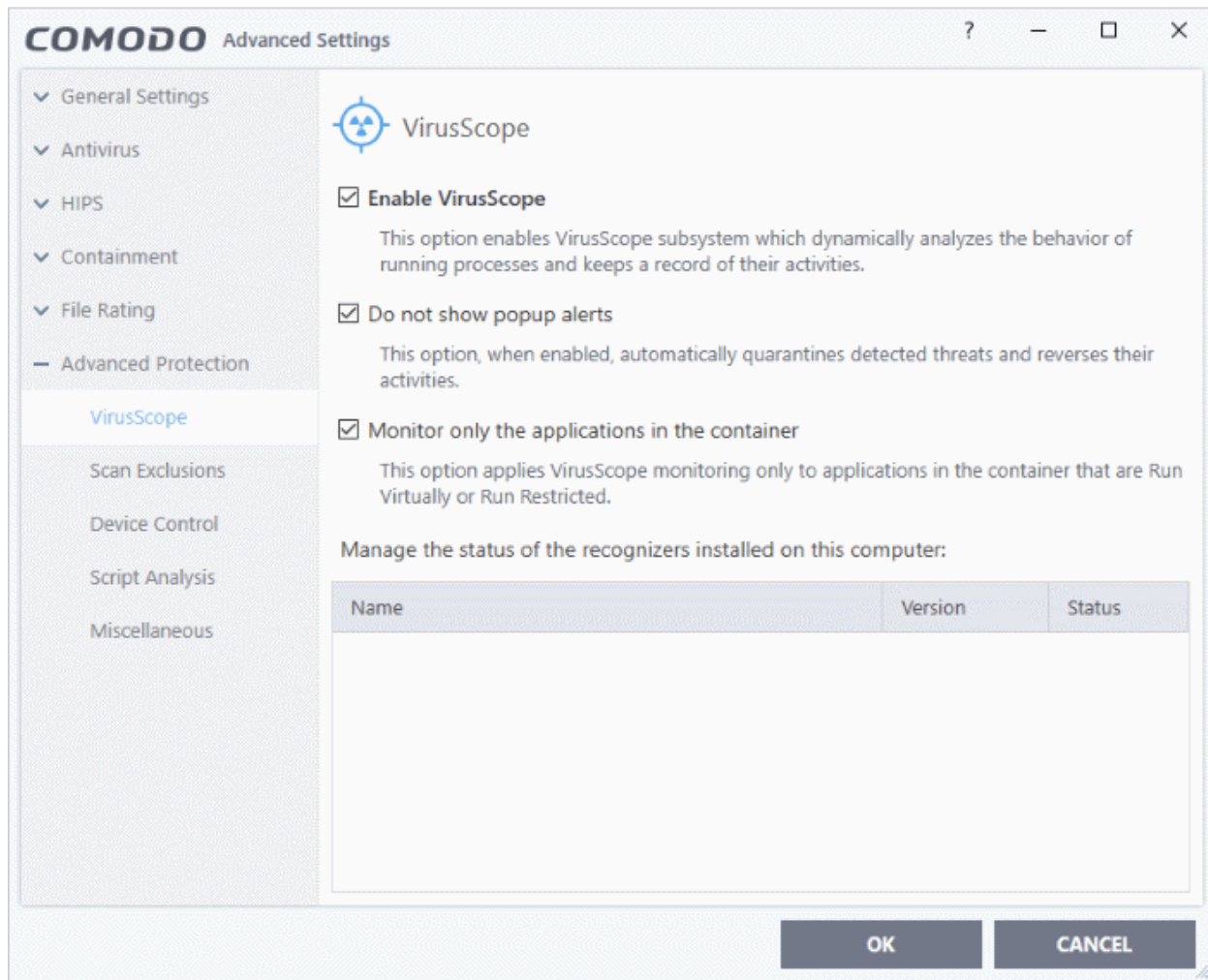
6.8.1. VirusScope Settings

- VirusScope monitors the activities of processes running on your computer and alerts you if they take actions that could threaten your privacy 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' at the top left of the CCS home screen
- Click 'Advanced Protection' > 'VirusScope':



VirusScope Settings

VirusScope monitors all running processes and generates alerts if it discovers malicious activity.

- **Enable VirusScope** - Enable or disable VirusScope. If enabled, VirusScope monitors the activities of running processes and generates alerts if suspicious activity is detected. **(Default = Enabled)**
- **Do not show pop-up alerts** - Configure whether or not CCS should show an alert if VirusScope detects suspicious activity.
 - Choosing 'Do not show pop-up alerts' will minimize disturbances but at some loss of user awareness.
 - If you choose not to show alerts then threats are automatically quarantined and their activities are reversed. **(Default = Disabled)**
- **Monitor only applications in the container** - Choose whether VirusScope should monitor the activities of all running processes, or only processes which are contained. **(Default = Enabled)**

Manage the status of recognizers

- VirusScope detects zero-day malware by analyzing the behavior and actions of an application.
- If the detected behavior corresponds to that of known malware, then VirusScope will generate an alert which allows you to quarantine the application and reverse any changes that it made.
- A 'recognizer' file contains the sets of behaviors that VirusScope needs to look out for.
- If you disable a recognizer, VirusScope will no longer show an alert if an application exhibits behavior described by the recognizer.
- We recommend most users to leave the 'Status' of recognizers at their default settings.

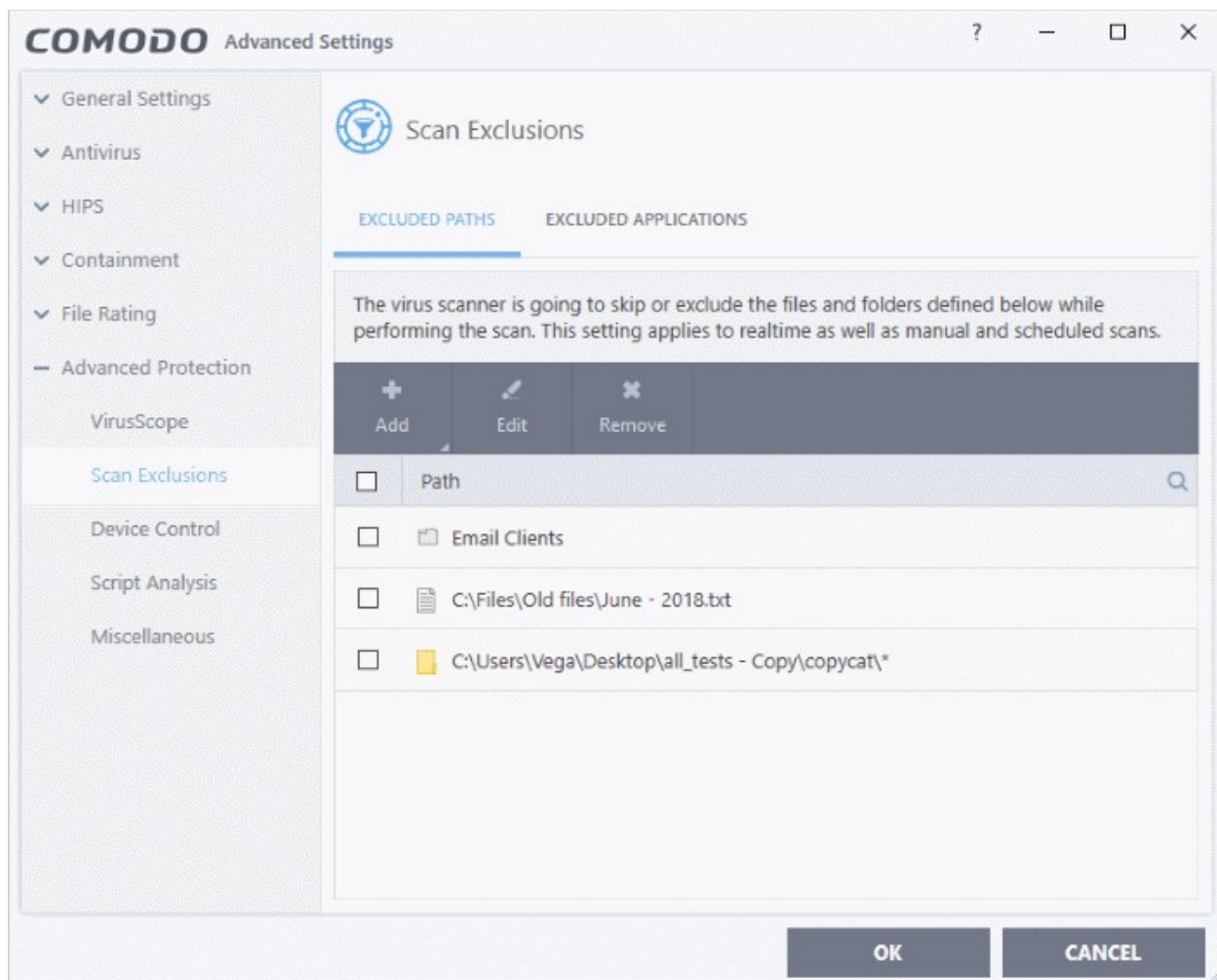
- Advanced users, however, may want to try disabling recognizers if they are experiencing a large number of VirusScope false positives.

6.8.2. Exclusions

- The 'Scan Exclusions' panel shows items you have chosen to ignore in the **results window** shown at the end of a virus scan.
- You may also have chosen to ignore them at an antivirus alert.

To open the Exclusions panel

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions' on the left:



The 'Scan Exclusions' panel has two tabs:

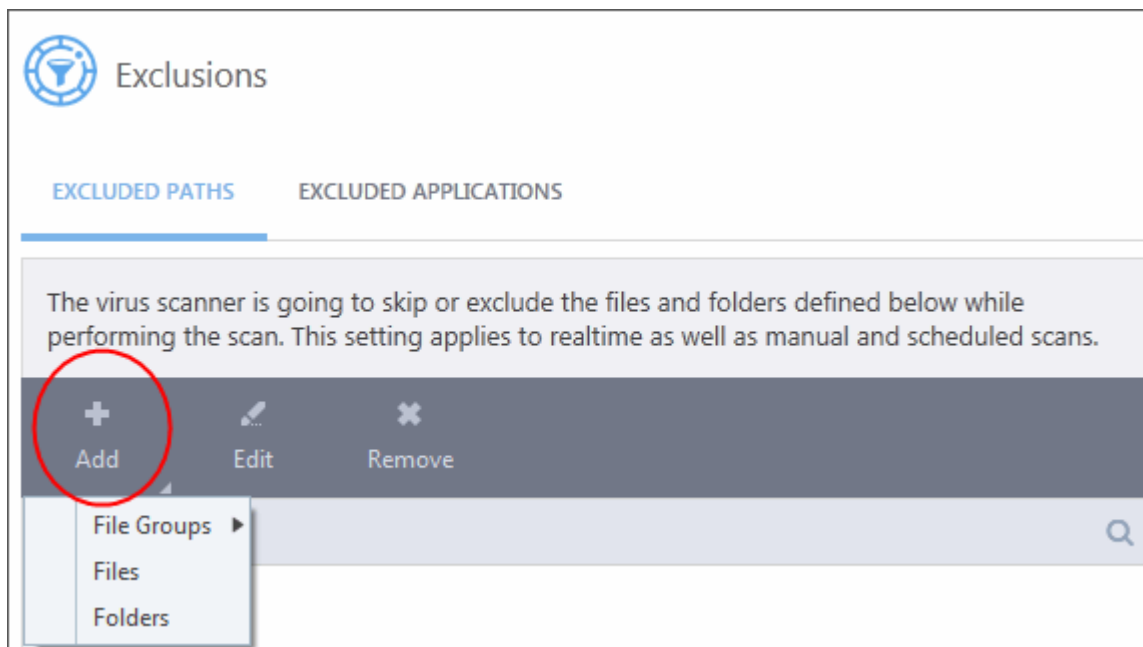
- **Excluded Paths** - A list of paths/folders/files on your computer which are excluded from real-time, on-demand and scheduled antivirus scans. See '[Excluding Drives/Folders/Files from all types of scans](#)' for more details.
- **Excluded Applications** - A list of applications which are excluded from real-time antivirus scans. Items can be excluded by clicking 'Ignore' in the virus '**Scan Results**', or by clicking 'Ignore' at an **Antivirus Alert**, or by excluding it manually. Note - excluded items are skipped by the real-time scanner but will be scanned during on-demand scans. See '[Excluding Programs/Applications from real-time scans](#)' for more details.

Excluding Drives/Folders/Files from all types of scans

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

To add item(s) to excluded paths

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions' on the left
- Select the 'Excluded Paths' tab
- Click the 'Add' button:

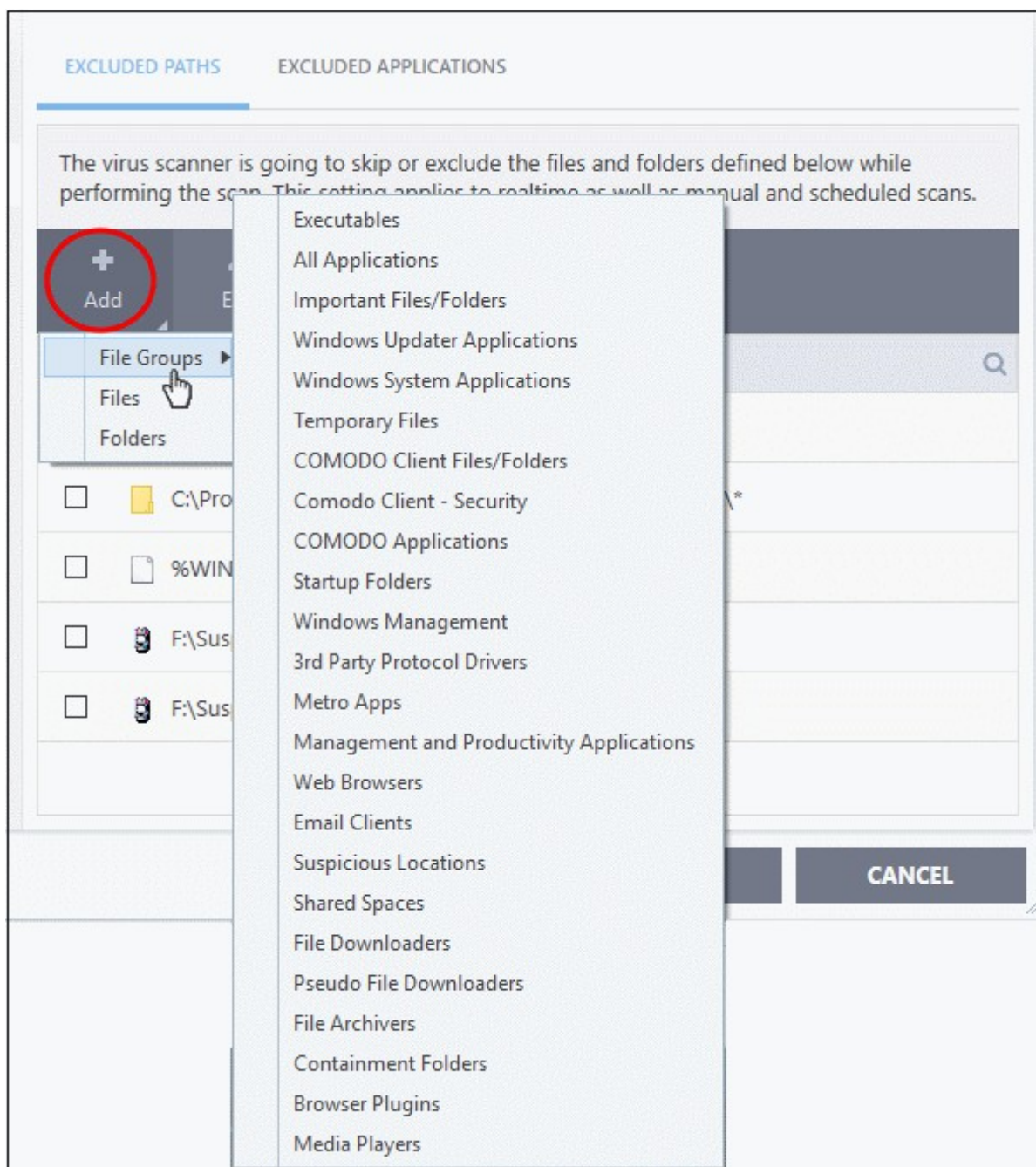


You can add a:

- **File Group**
 - **Drive partition/Folder**
- or
- **Individual file**

Adding a File Group

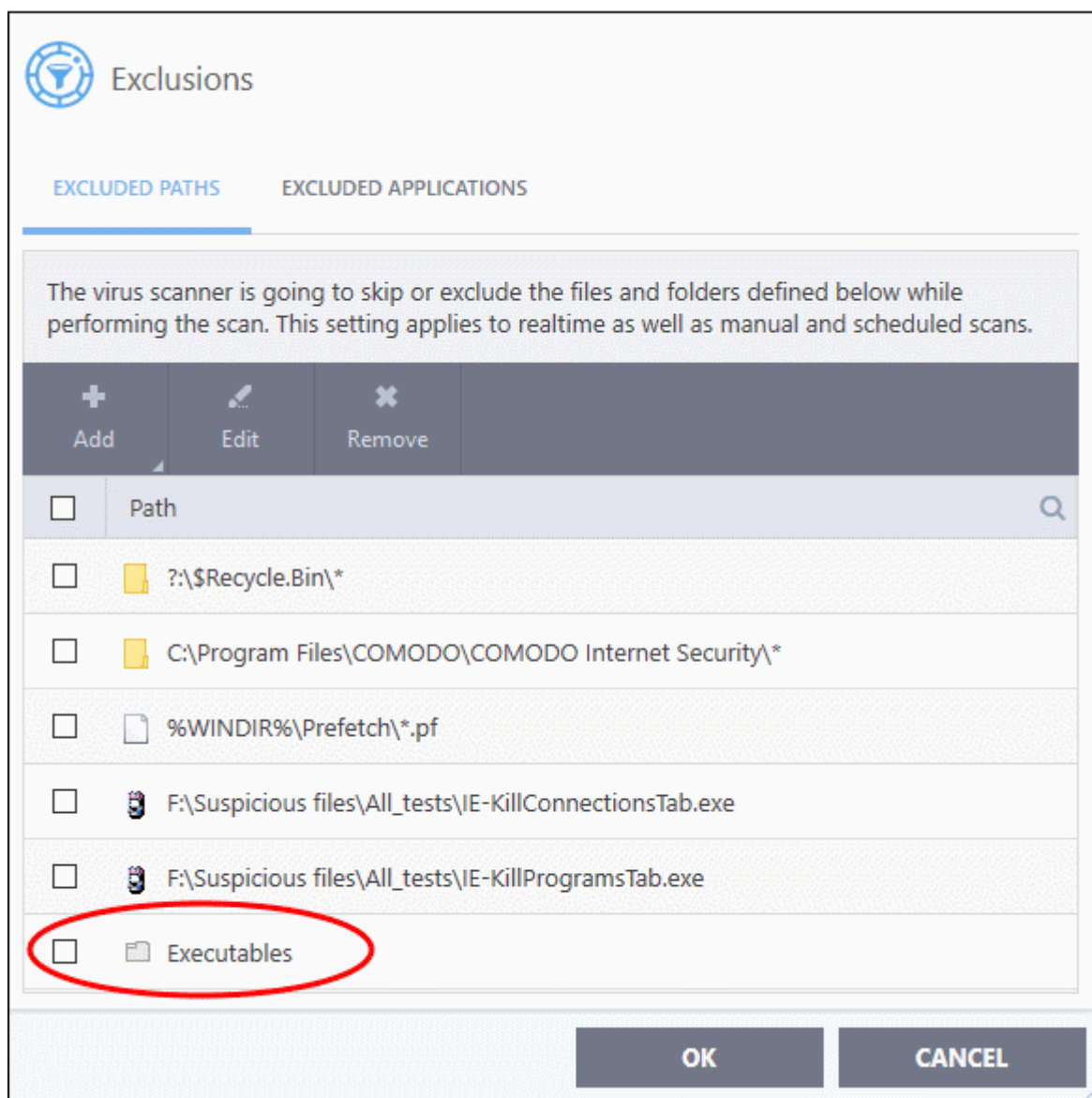
- Choosing 'File Groups' allows you to exclude a pre-set category of files or folders. This provides a convenient way to apply a generic ruleset to important files and folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl *cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications' and 'Start Up Folders'.



CCS ships with a set of predefined file groups which can be viewed in 'Advanced Settings' > 'File Rating' > **File Groups**.

To add new file groups:

- Click 'Add' > 'File Groups' and select the type of 'File Group' from the list:

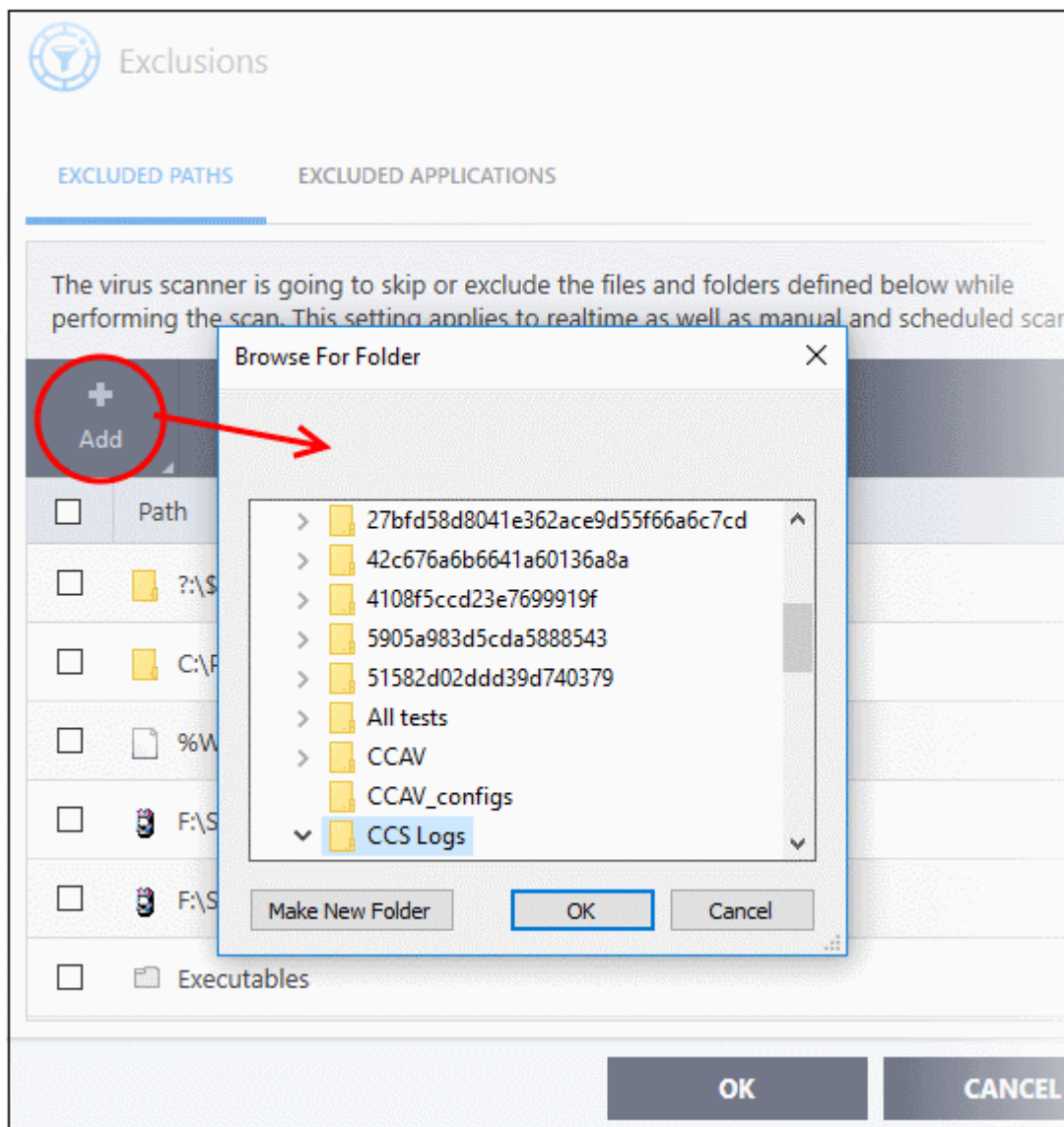


The file groups will be added to 'Excluded Paths'.

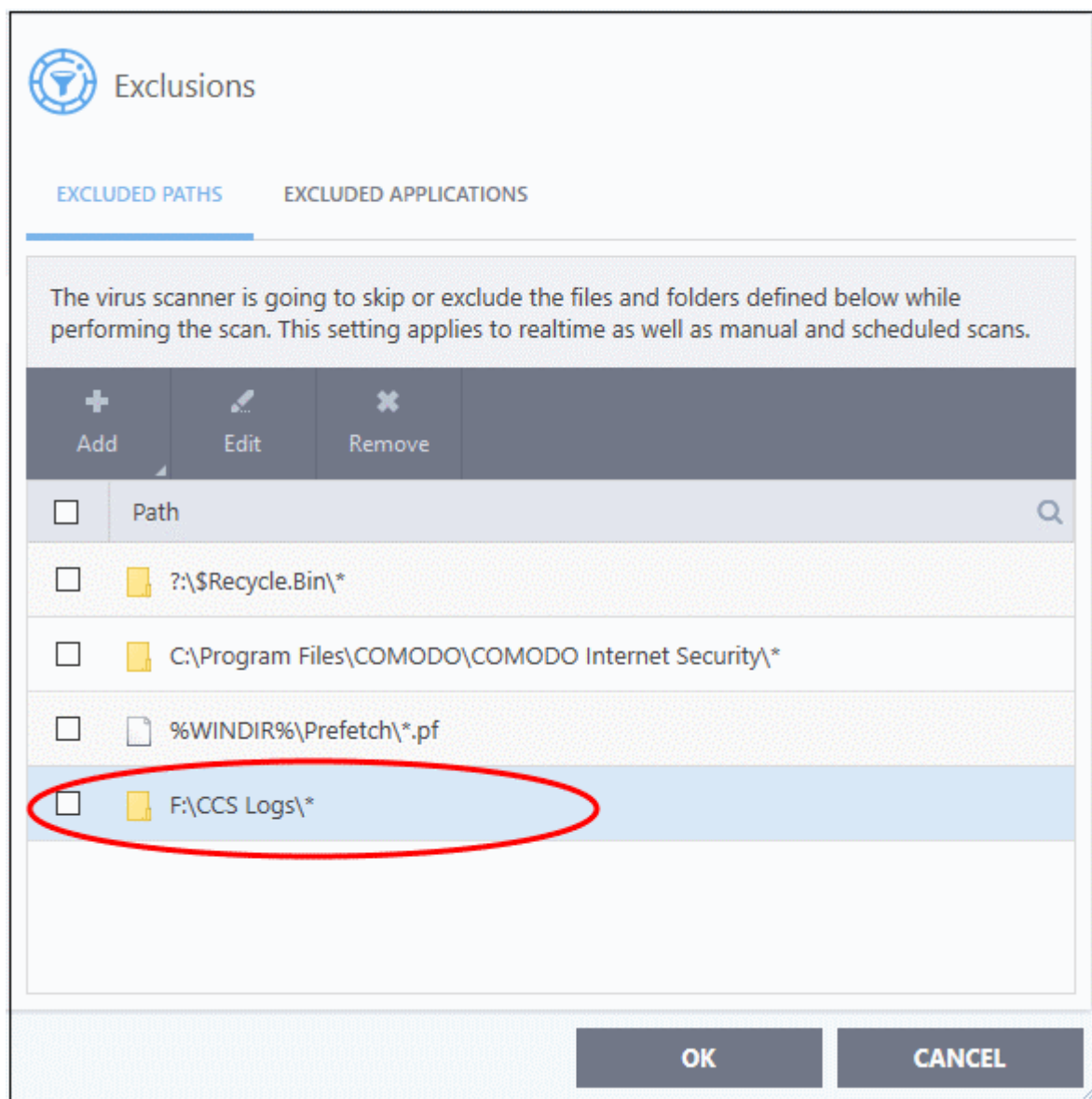
- Repeat the process to add more file groups. Items added to the 'Excluded Paths' will be omitted from all types of future Antivirus scans.

Adding a Drive Partition/Folder

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions' on the left
- Select 'Excluded Paths'
- 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:

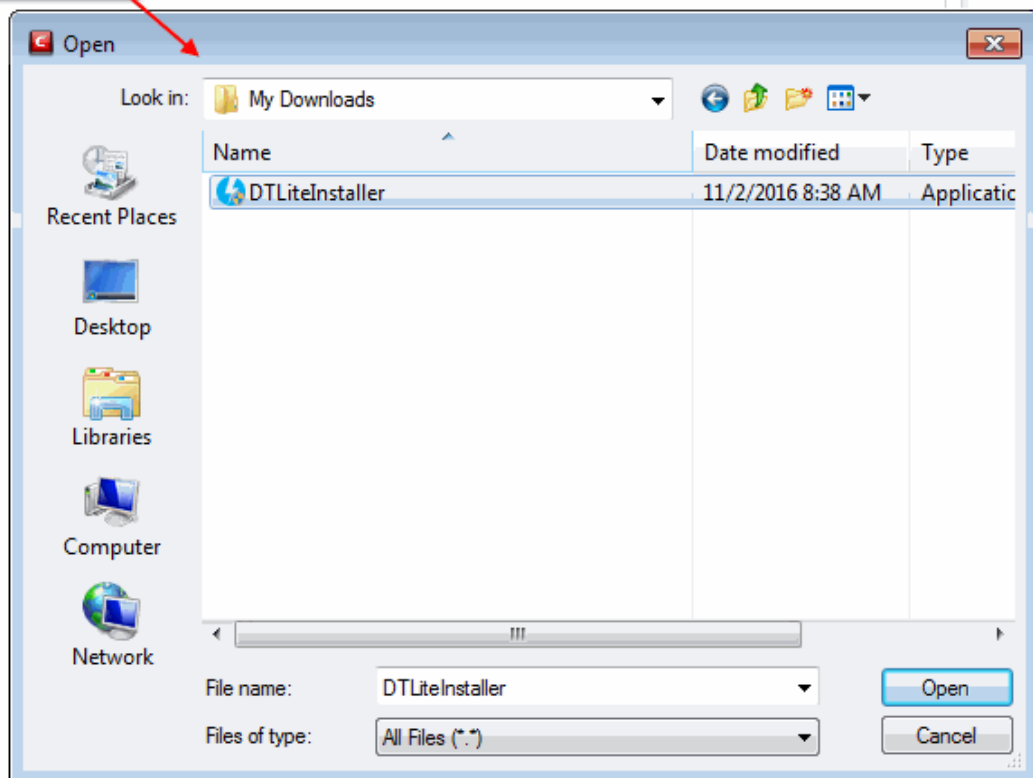
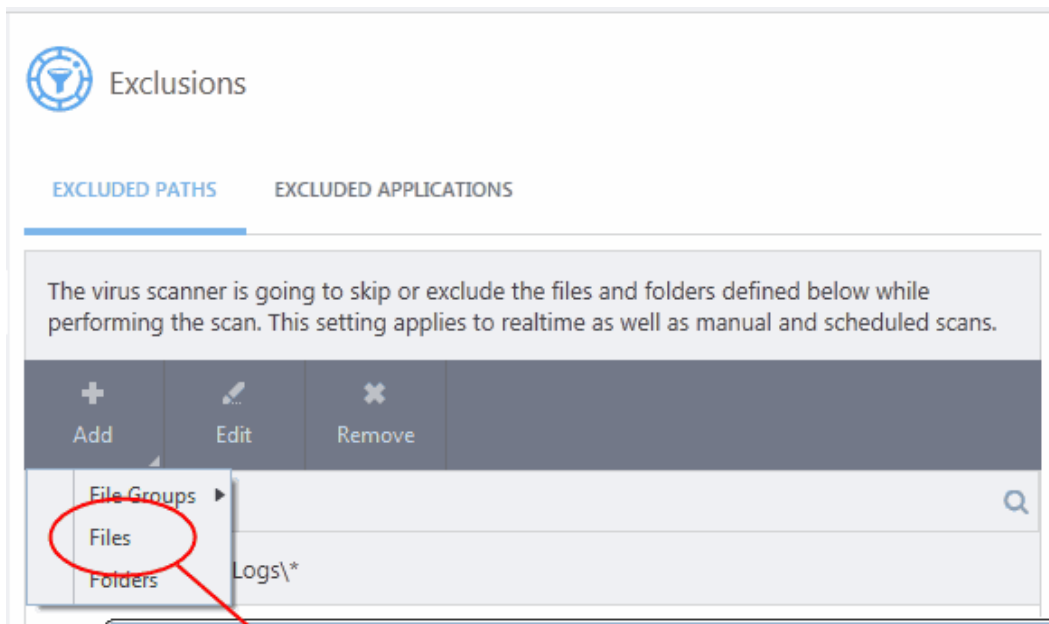


- Repeat the process to add more folders. Items added to 'Excluded Paths' will be omitted from all types of antivirus scans in future.

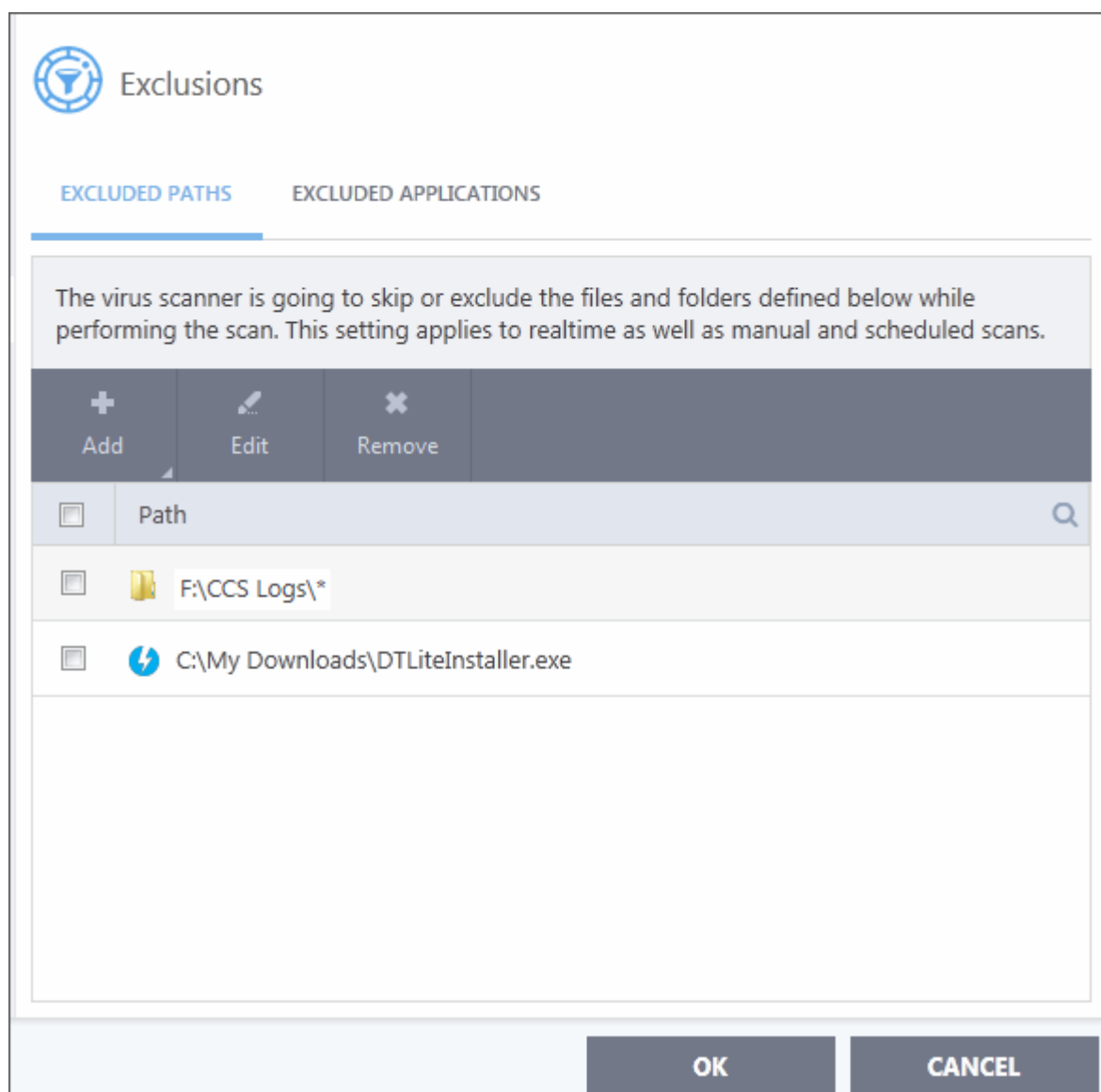
Add an individual file

You can specify individual files as excluded path.

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions' on the left
- Select 'Excluded Paths'
- Click 'Add' > 'Files'
- Navigate to the file you want to add to excluded paths and click 'OK'.



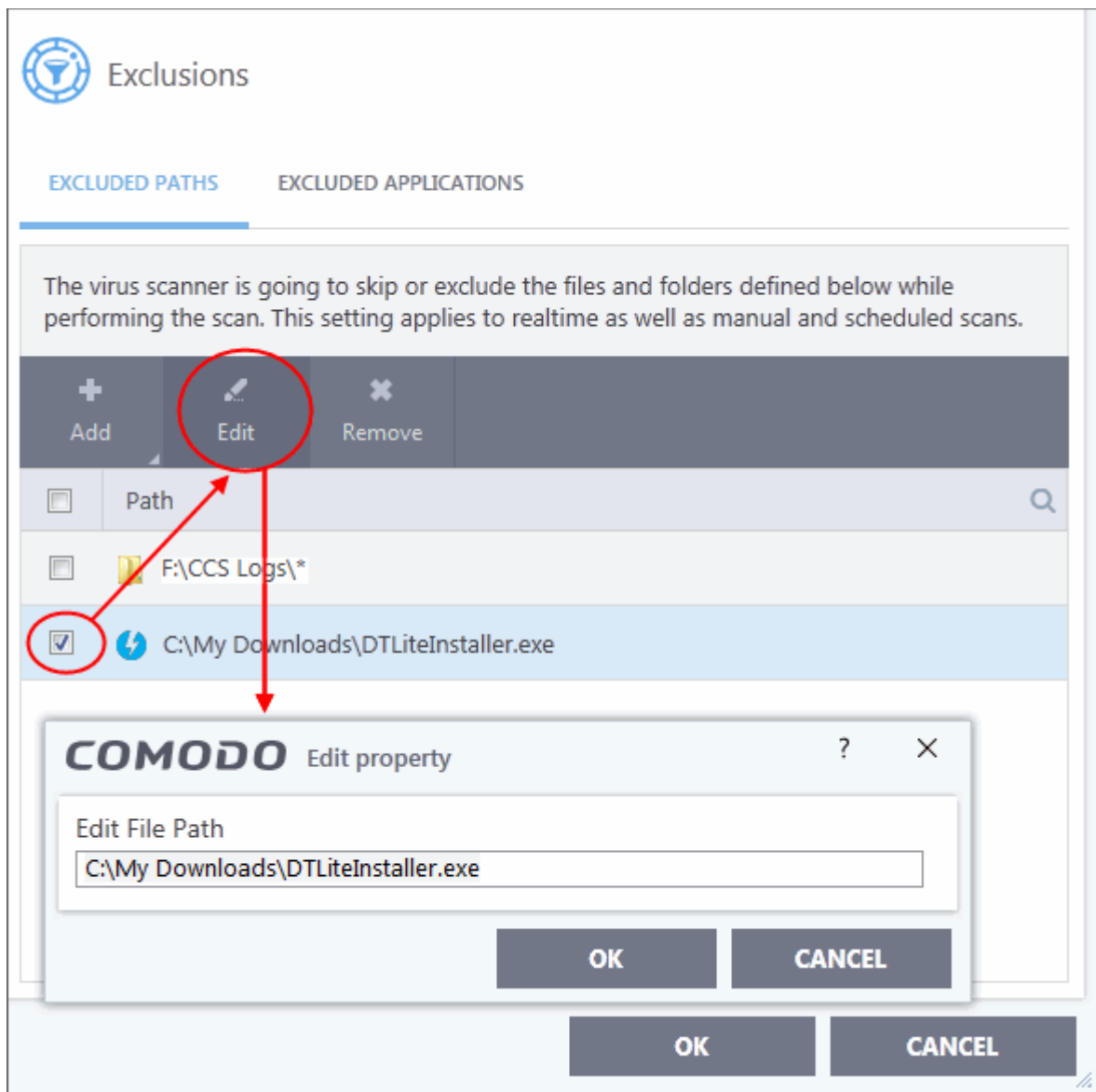
- The file will be added to excluded paths:



- Repeat the process to add more paths.
- Items added to 'Excluded Paths' will be omitted from all types of virus scan in the future.

To edit the path of an added item

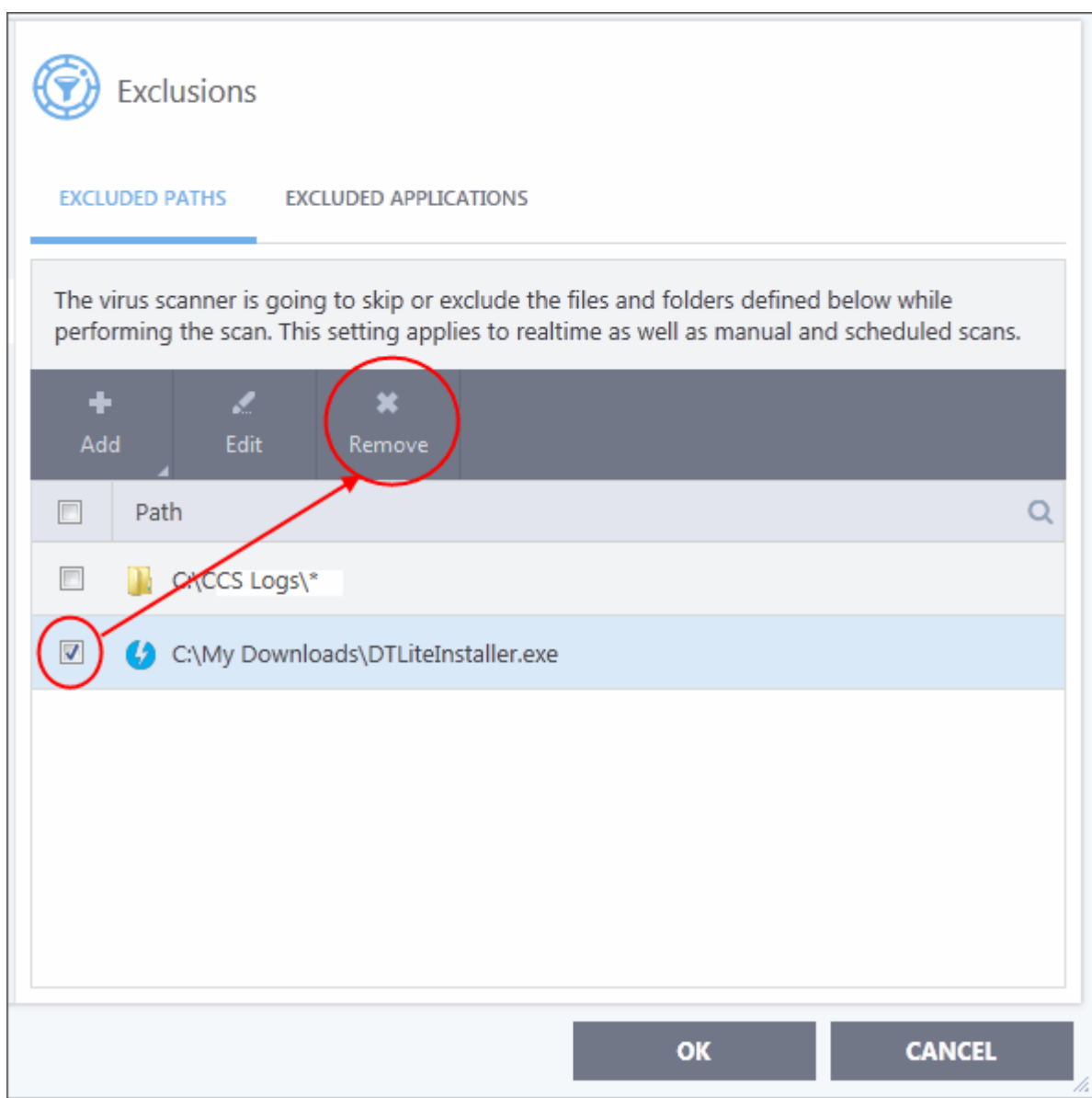
- Select the target item and click 'Edit':



- Modify the file-path as required and click 'OK'.

Remove an item from 'Excluded Paths'

- Select the target item and click 'Remove':



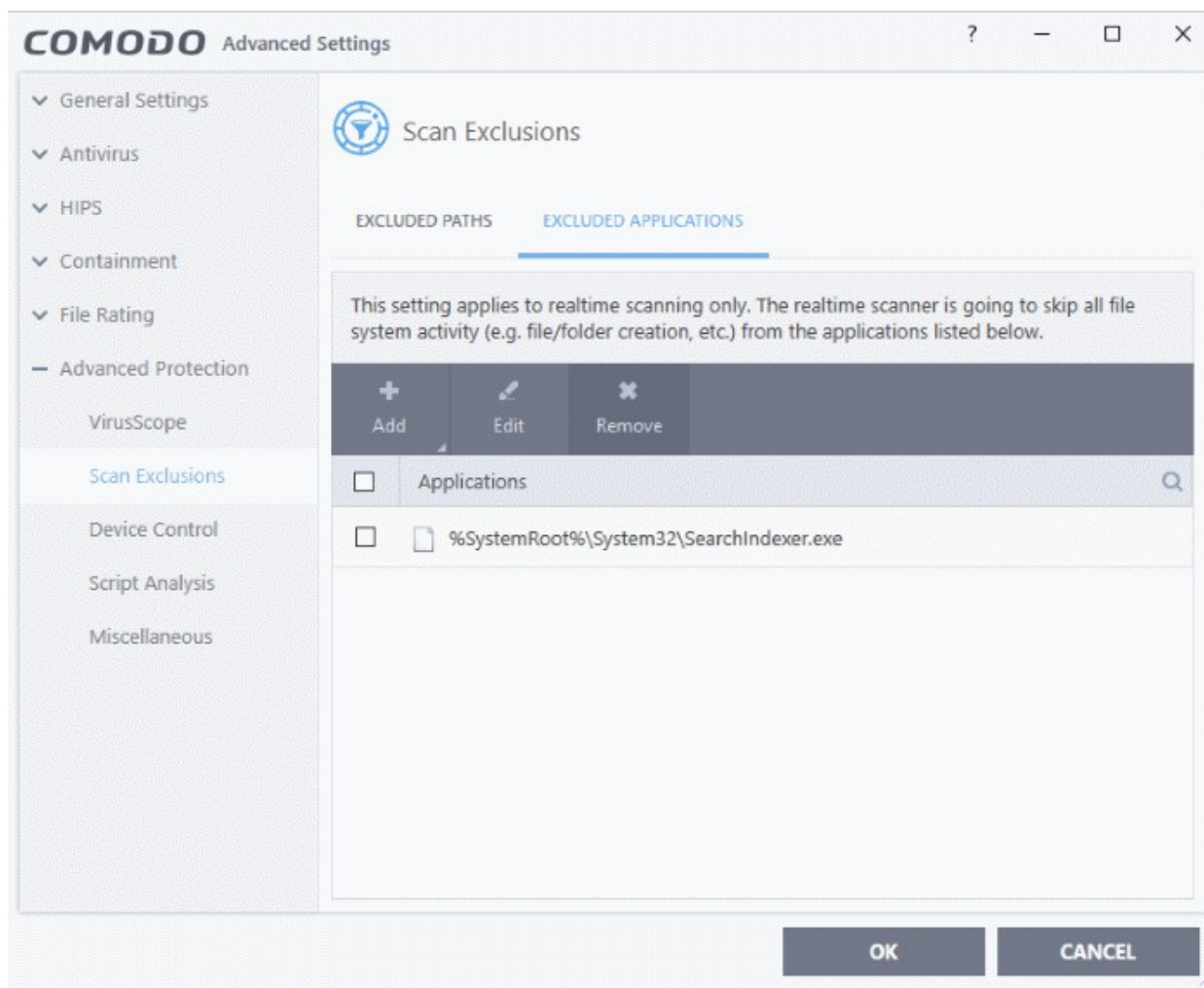
- Click 'OK' for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

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

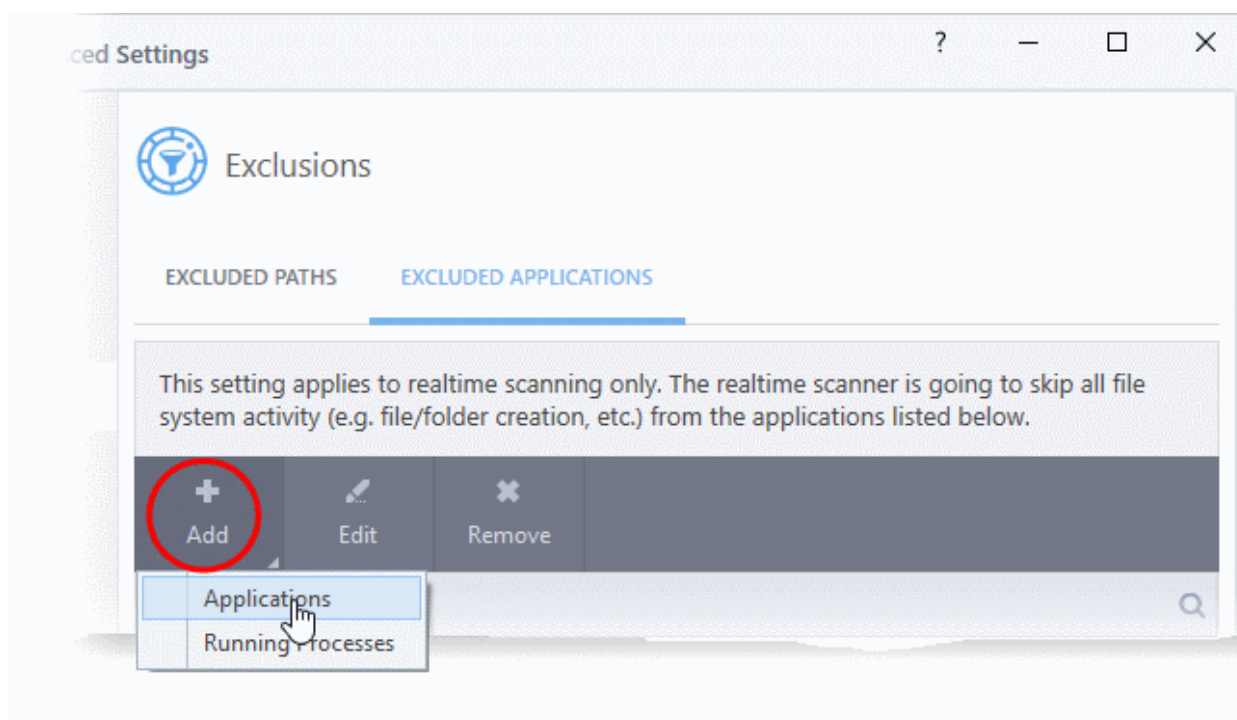
To open 'Excluded Applications':

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions' on the left
- Select the 'Excluded Applications' tab:



To add an item to Excluded Applications

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

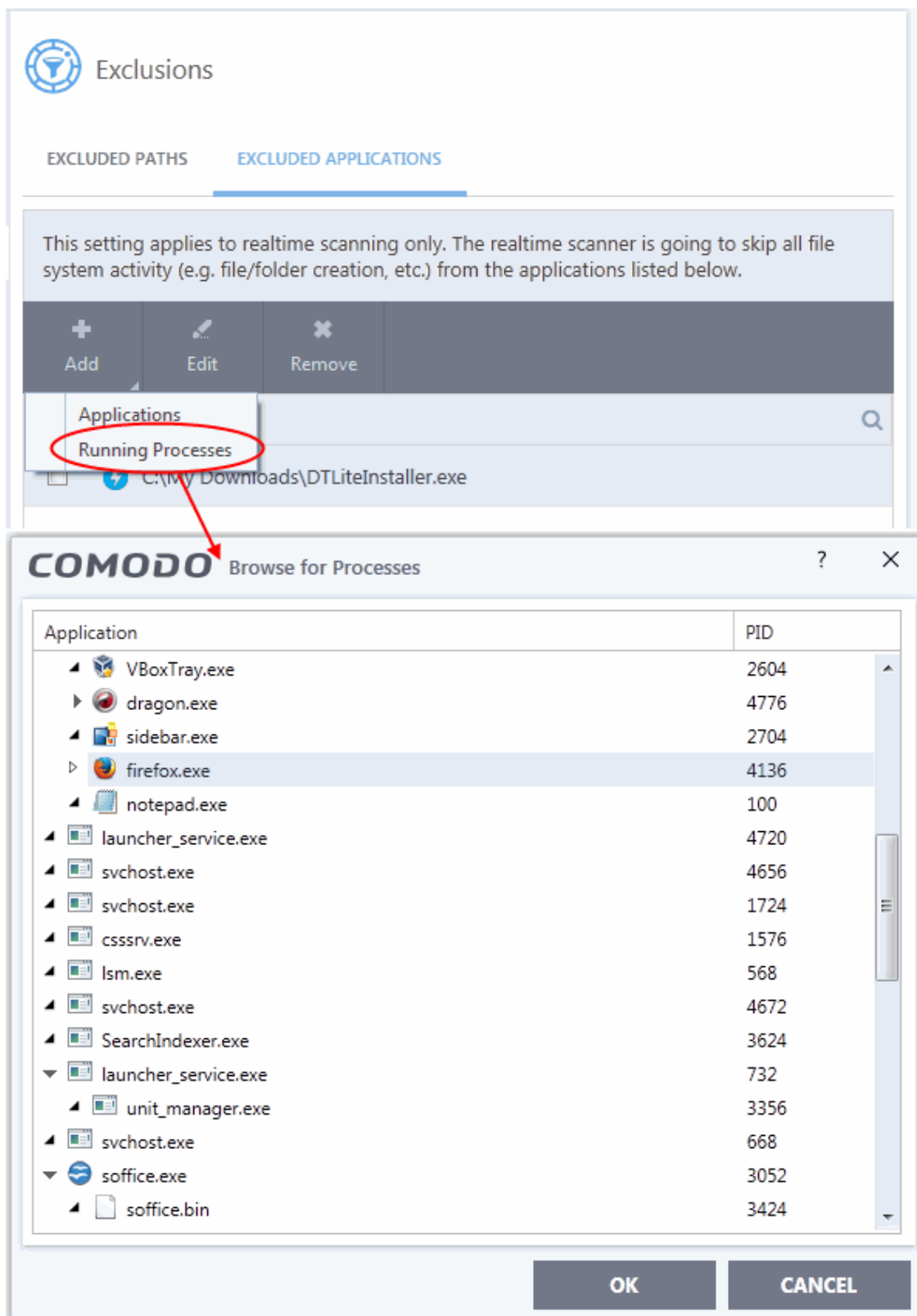


You can choose to add an applications by:

- **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.

Adding an application from a running processes

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



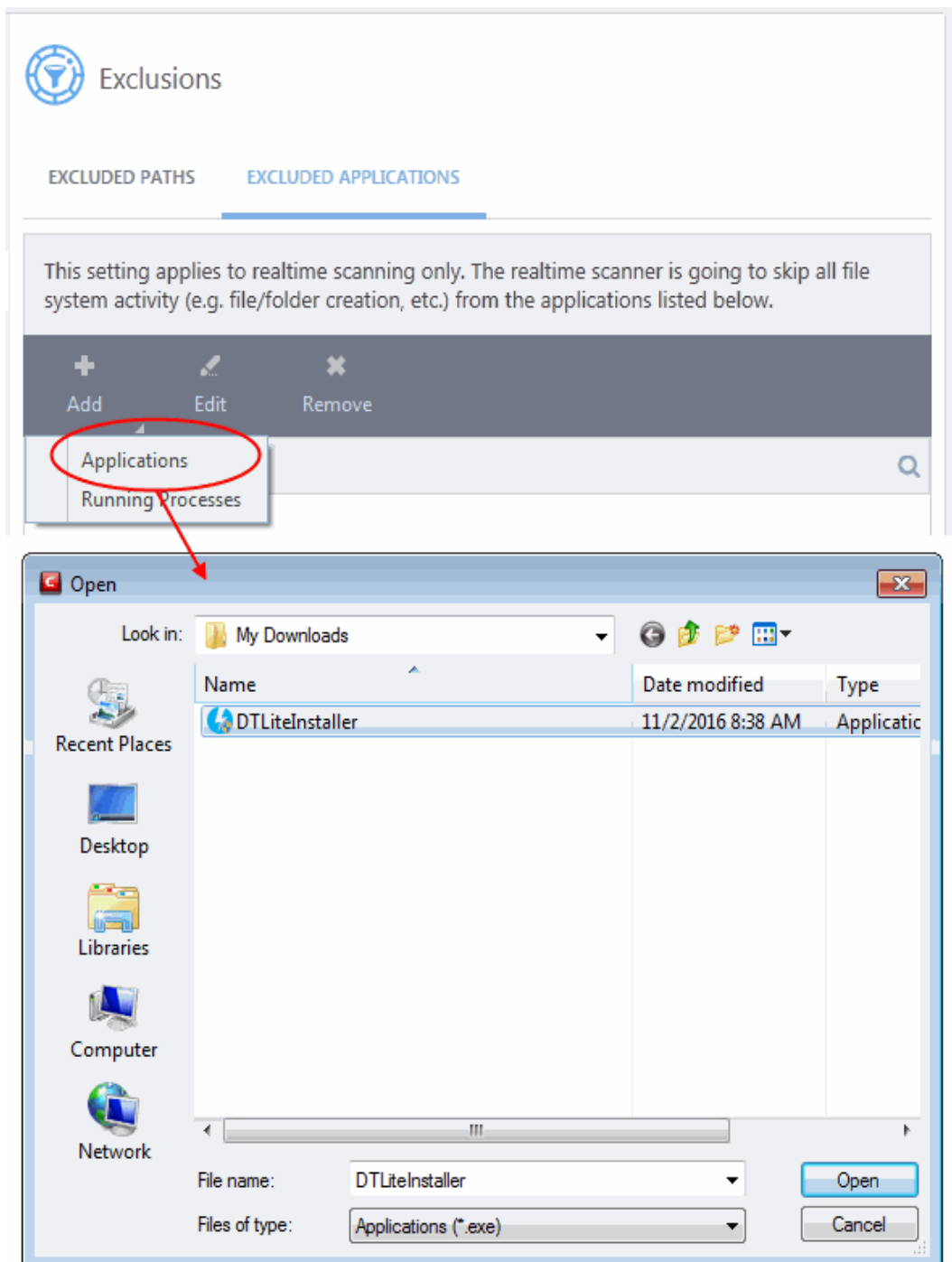
A list of currently running processes in your computer will be displayed:

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

The application will be added to 'Excluded Applications'.

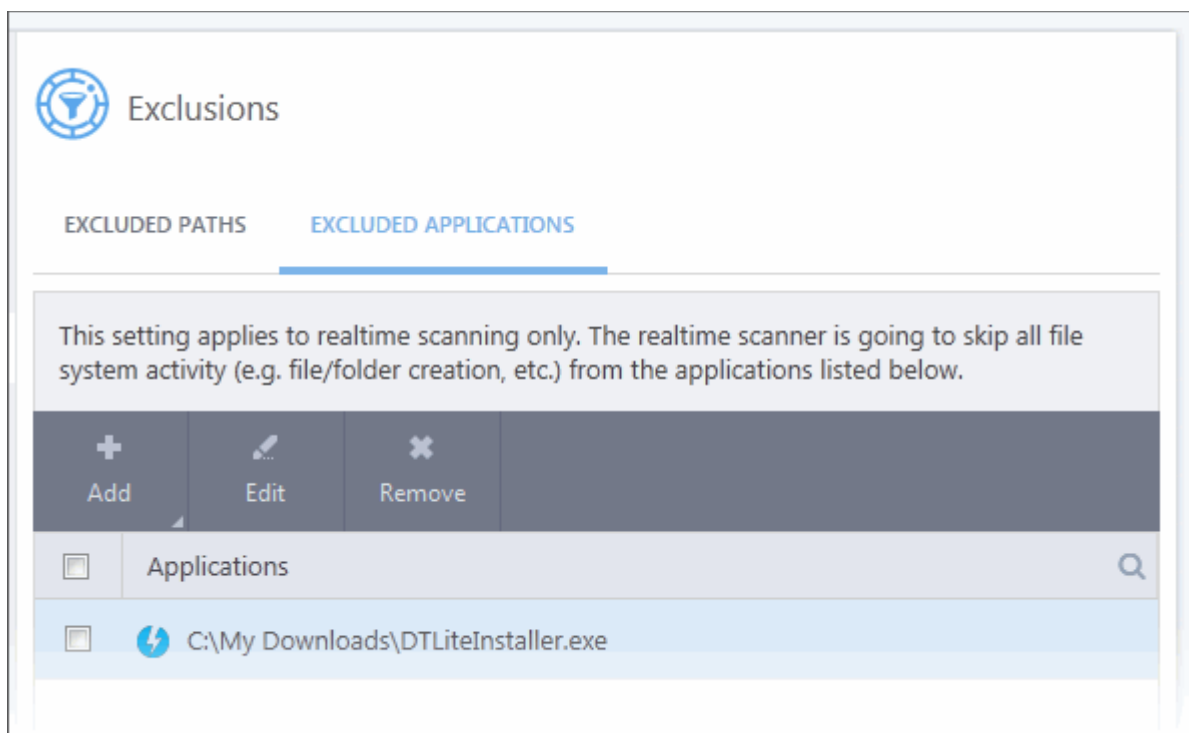
Browsing to the Application

- Choose 'Applications' from the 'Add' drop-down



- Navigate to the file you want to exclude and click 'Open'.

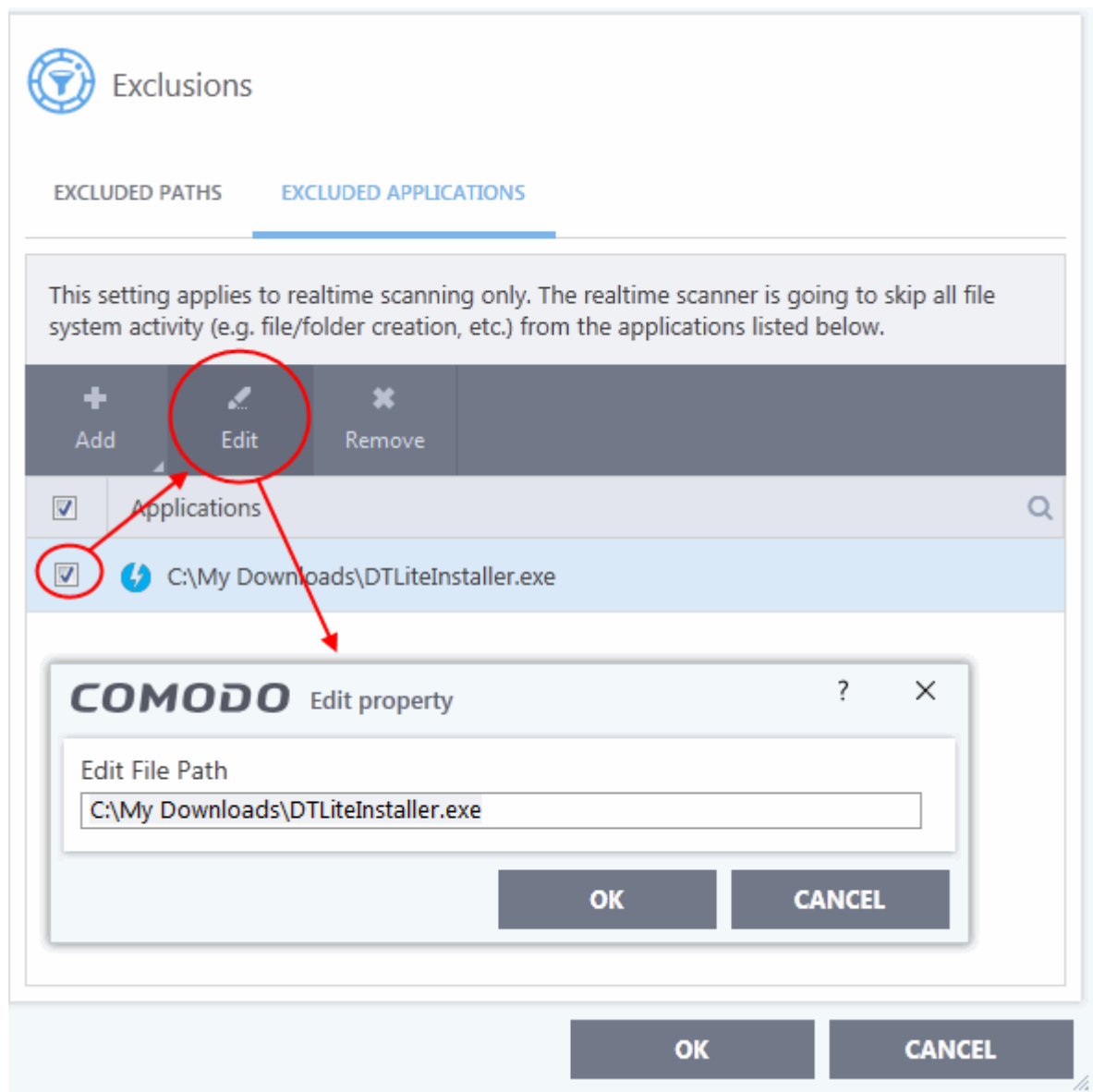
The file will be added to 'Excluded Applications'.



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

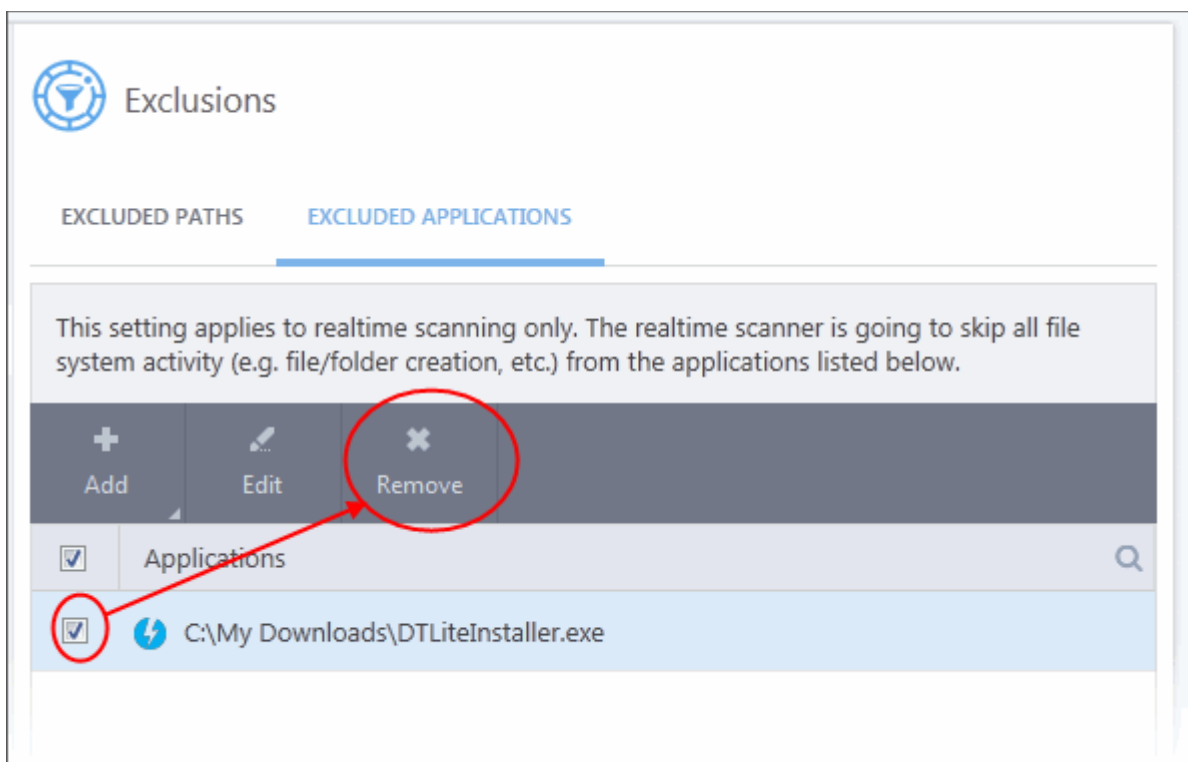
To edit the path of the application added to Excluded Application

- Select the application and click 'Edit' at the top.
- Make the required changes to the file path in the 'Edit Property' dialog.



To remove an item from the Excluded Applications

- Select the item and click 'Remove' at the top:



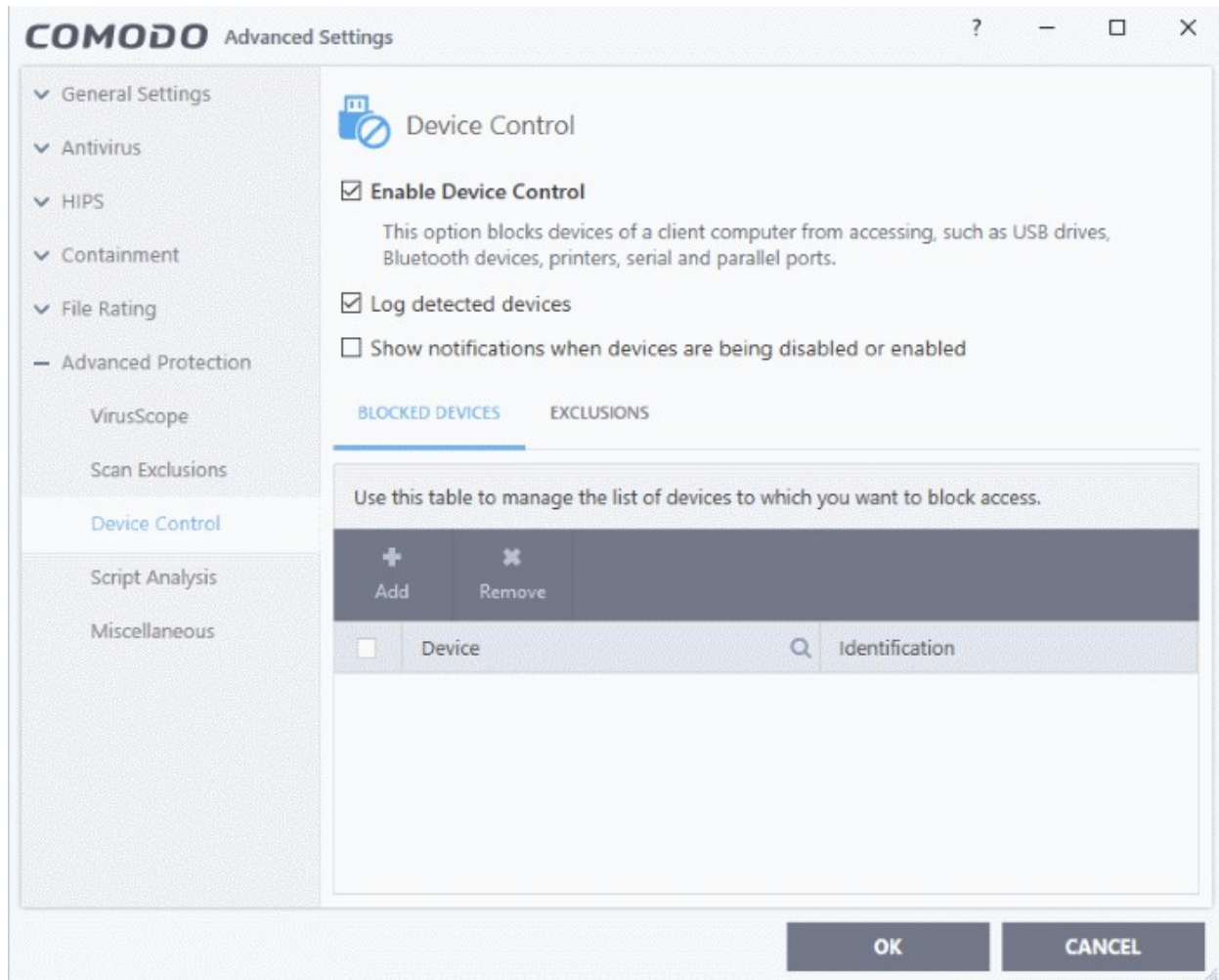
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

6.8.3. Device Control Settings

The 'Device Control Settings' section let you configure which types of external devices are allowed to connect to an endpoint.

Open the Device Control panel

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control' on the left:



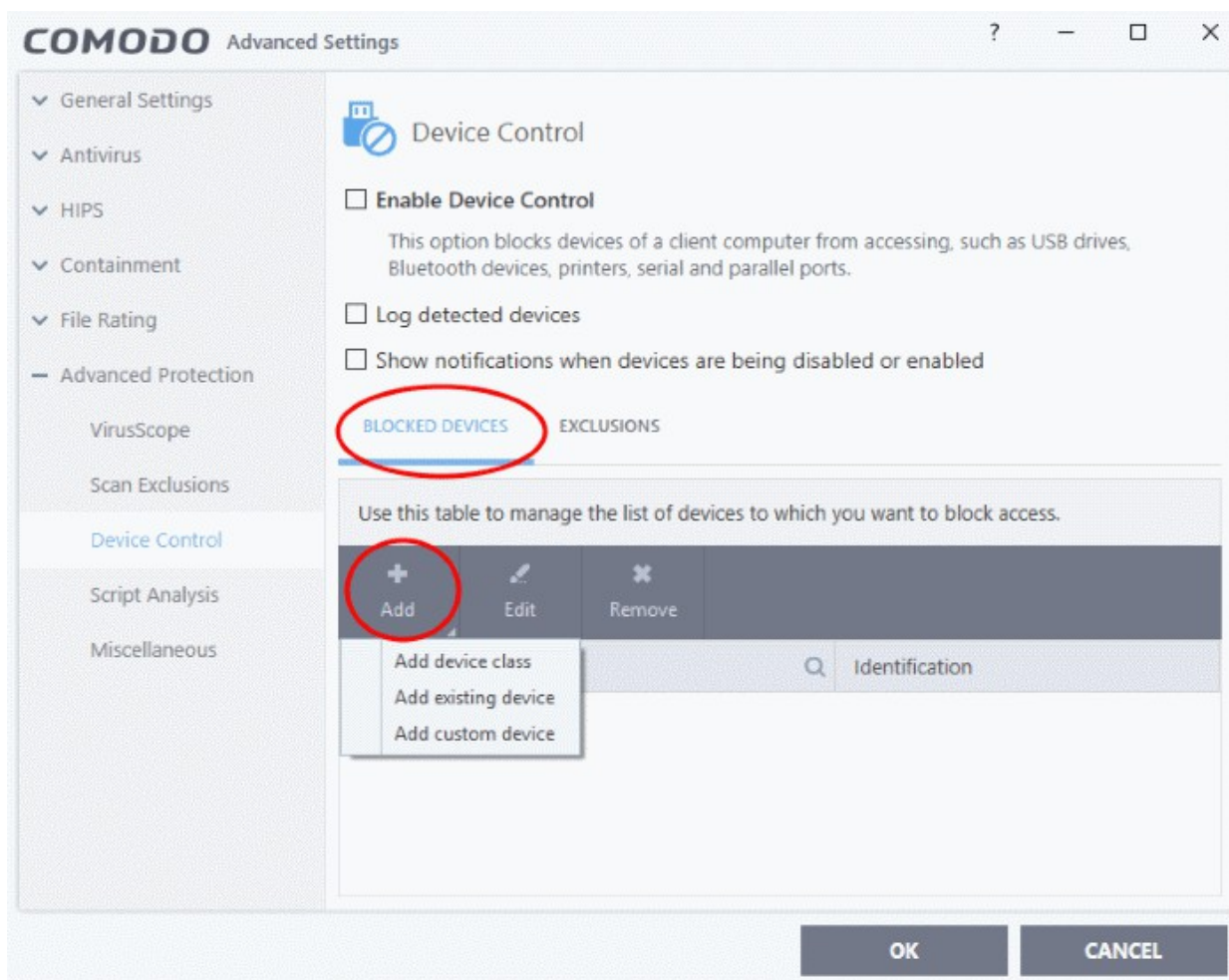
- **Enable Device Control** - Enable or disable device control functionality. If enabled you should specify banned device types in the 'Blocked Devices' section of this dialog (**Default = Enabled**)
- **Log Detected Devices** - If enabled, CCS will log events by external devices (**Default = Enabled**)
- **Show Notifications when devices are being disabled or enabled** - Will show an alert whenever an external device is connected or disconnected. (**Default = Disabled**)
- **Blocked Devices** - Lists 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** - Allows you to add specific devices which are 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:

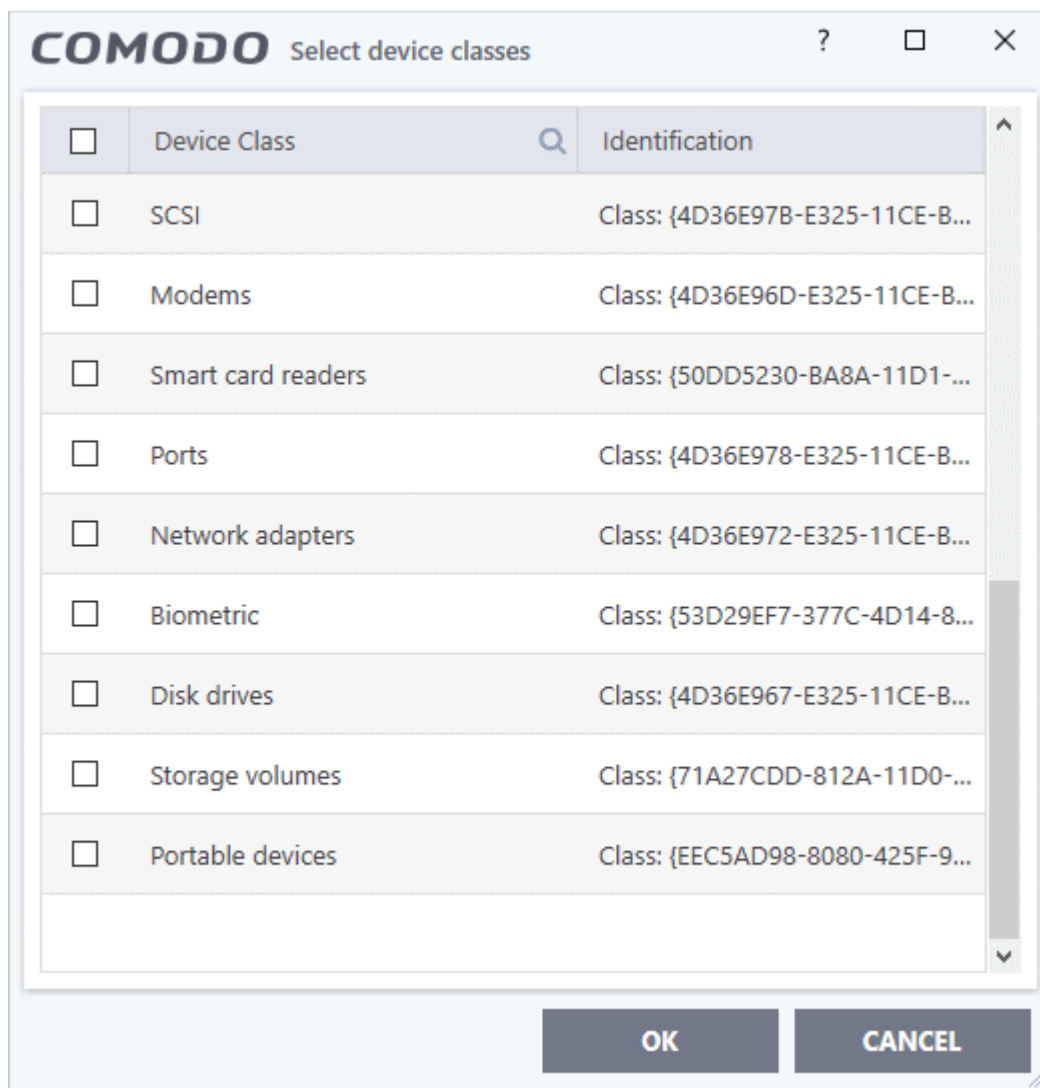
- [Block devices](#)
- [Specify exclusions](#)

Block a device class

- Click the 'Blocked Devices' tab then the 'Add' button
- Click 'Add device class' from the options:



- 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.

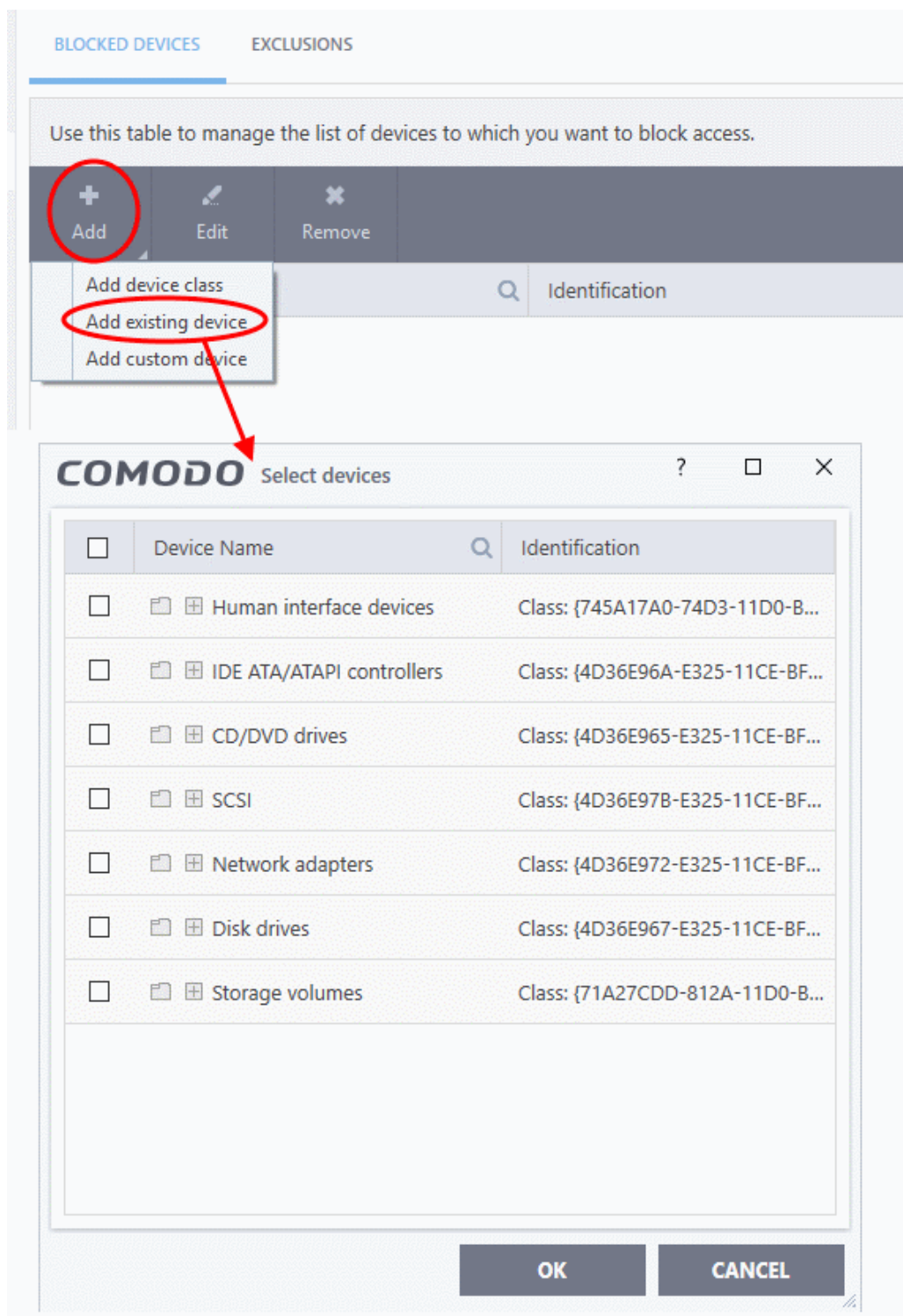


- Select the device(s) you wish to block
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

To add existing devices:

- Click 'Add existing device' from the options

The 'Select devices' screen will be displayed:

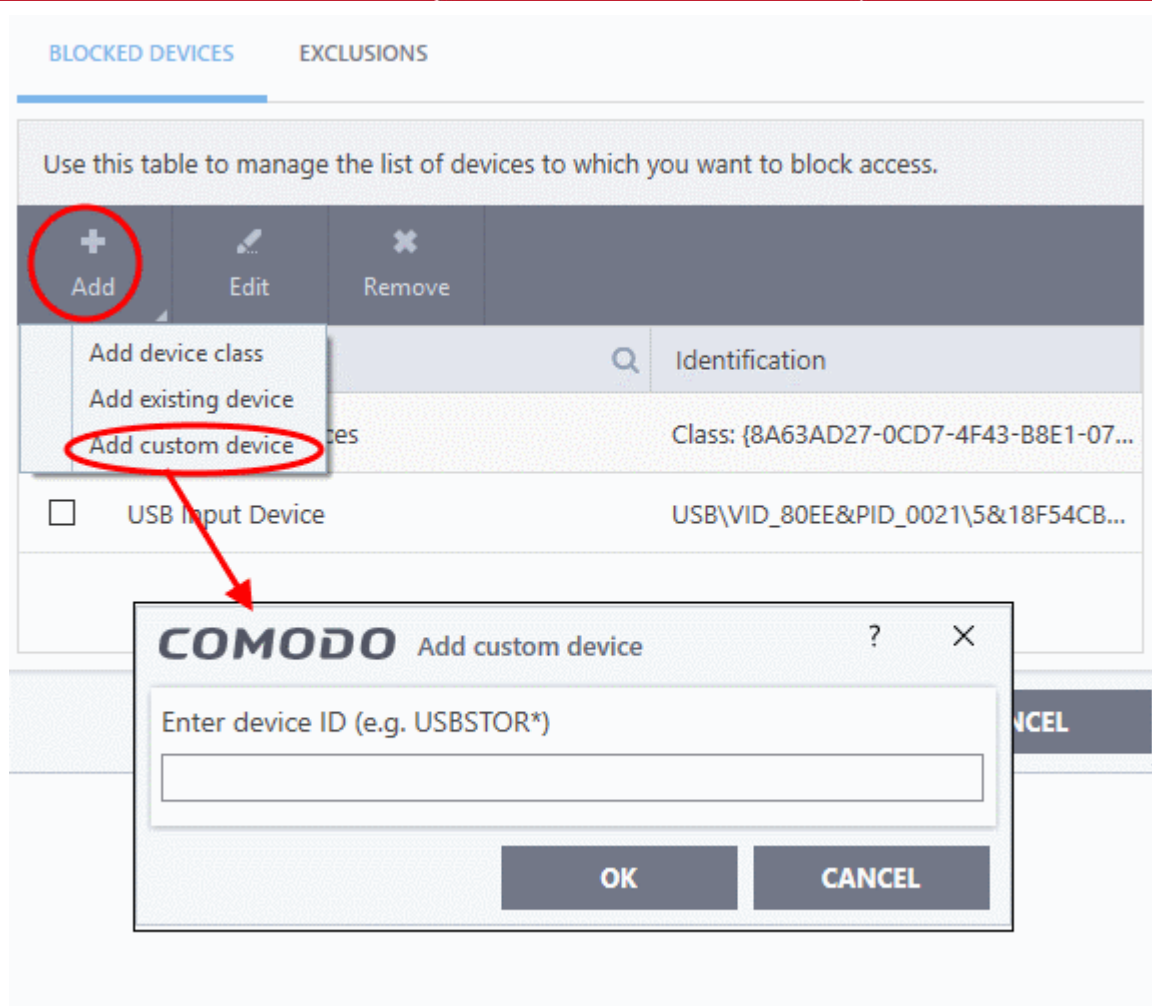


- Choose the device class you wish to block. For example, Network adaptor devices, CD/DVD drives, Storage devices or Disk drives.
- Click the '+' sign of the class to which your device belongs
- Select the device(s) you wish to block
- Click 'OK' and again click 'OK' in the 'Device Control' panel.

To add custom devices:

- Click 'Add custom device' from the options

The 'Select custom device' screen will be displayed:

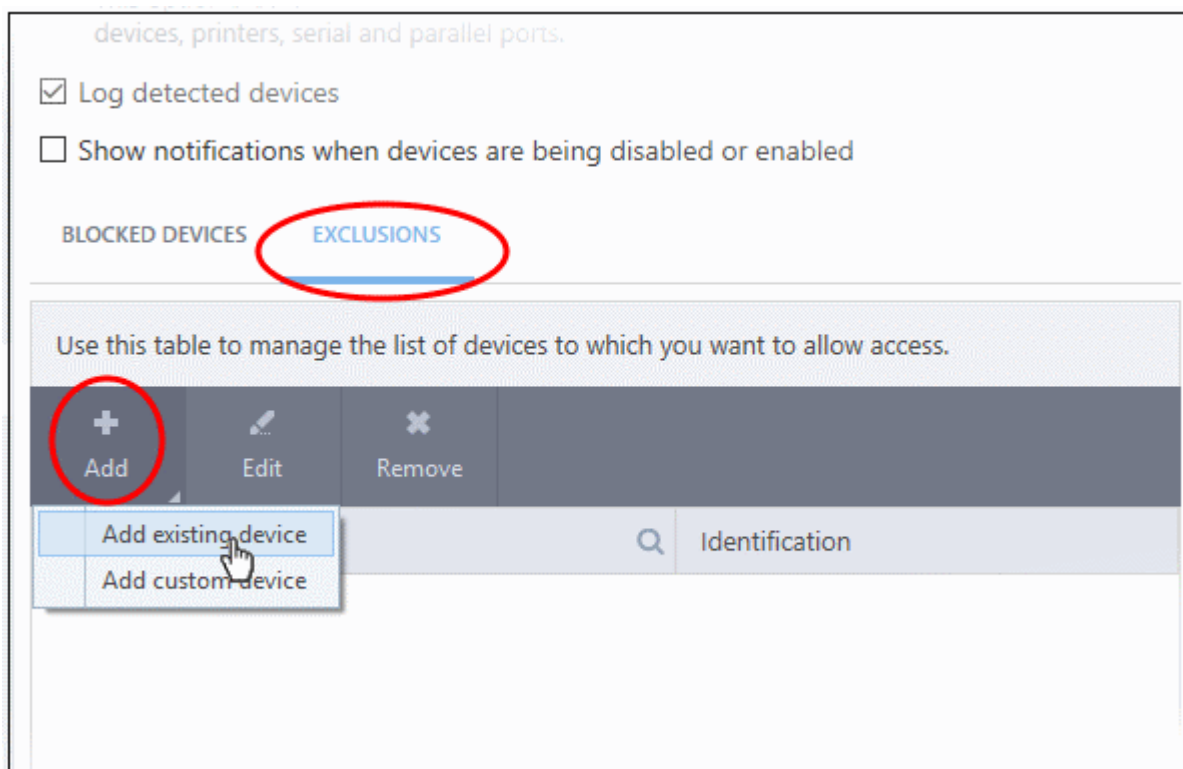


- Enter the device ID and click 'OK'

Specify exclusions

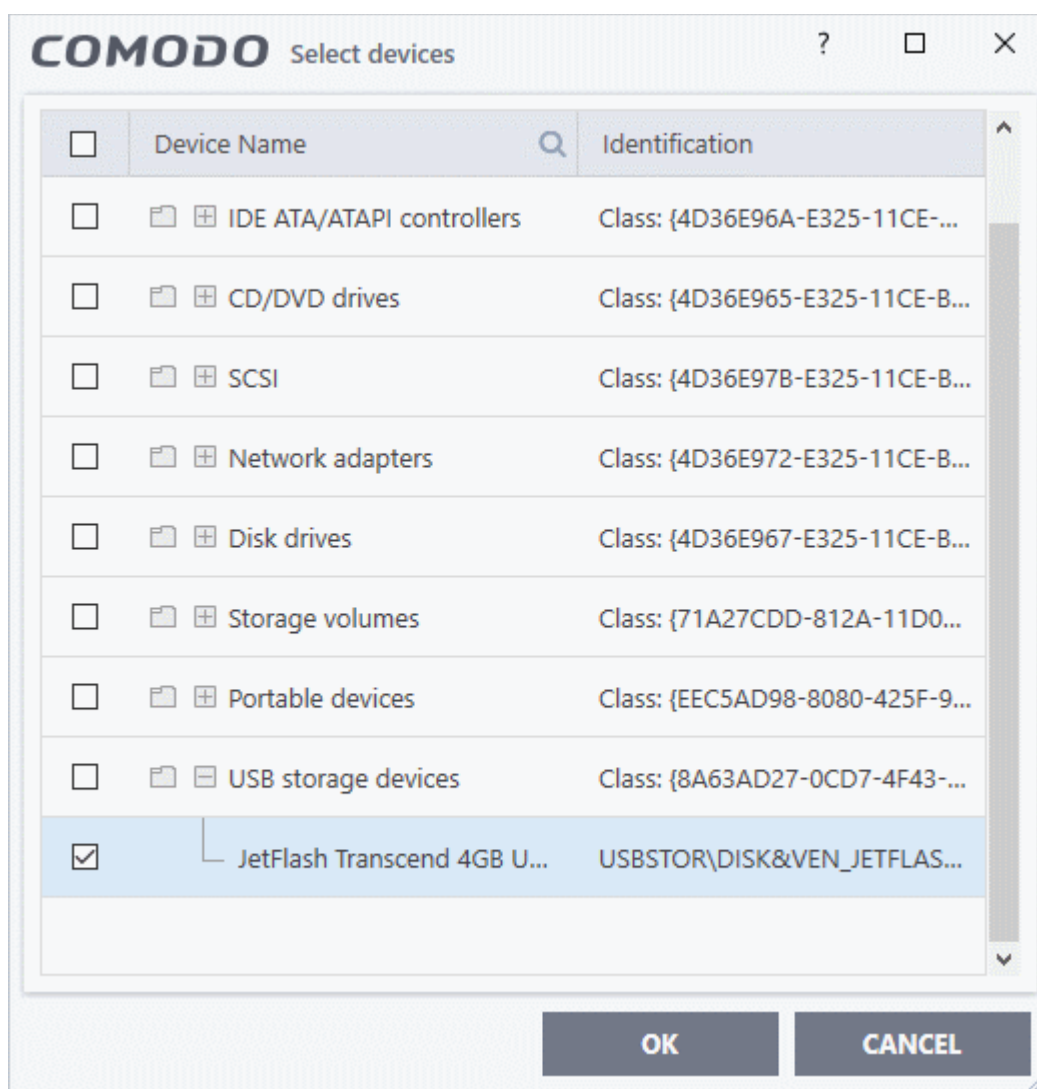
If you want to allow access to specific devices that fall within a blocked device class:

- Add the device to the exclusion list *before* blocking the device class
- Make sure the external device is connected to the computer
- Click the 'Exclusions' tab then 'Add':



- Click 'Add existing device' from the options

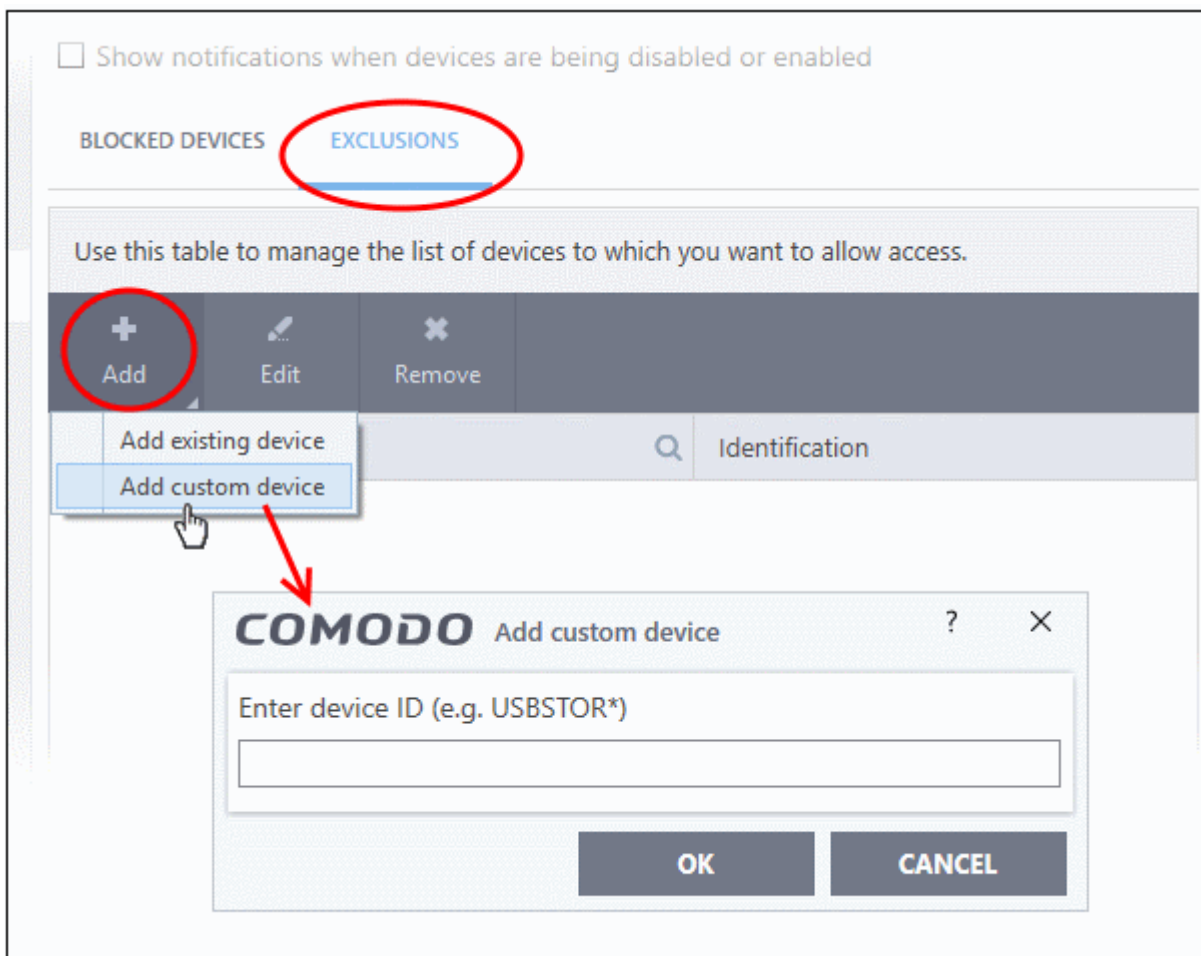
The 'Select devices' screen will be displayed:



- 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.

You can also add exclusions by using the wildcard character - '*'. For example, say you wanted 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*'.

- To add exclusions by using wildcard characters, click the 'Exclusions' tab
- Click the 'Exclusions' tab then 'Add':



- Click '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.

6.8.4. Script Analysis Settings

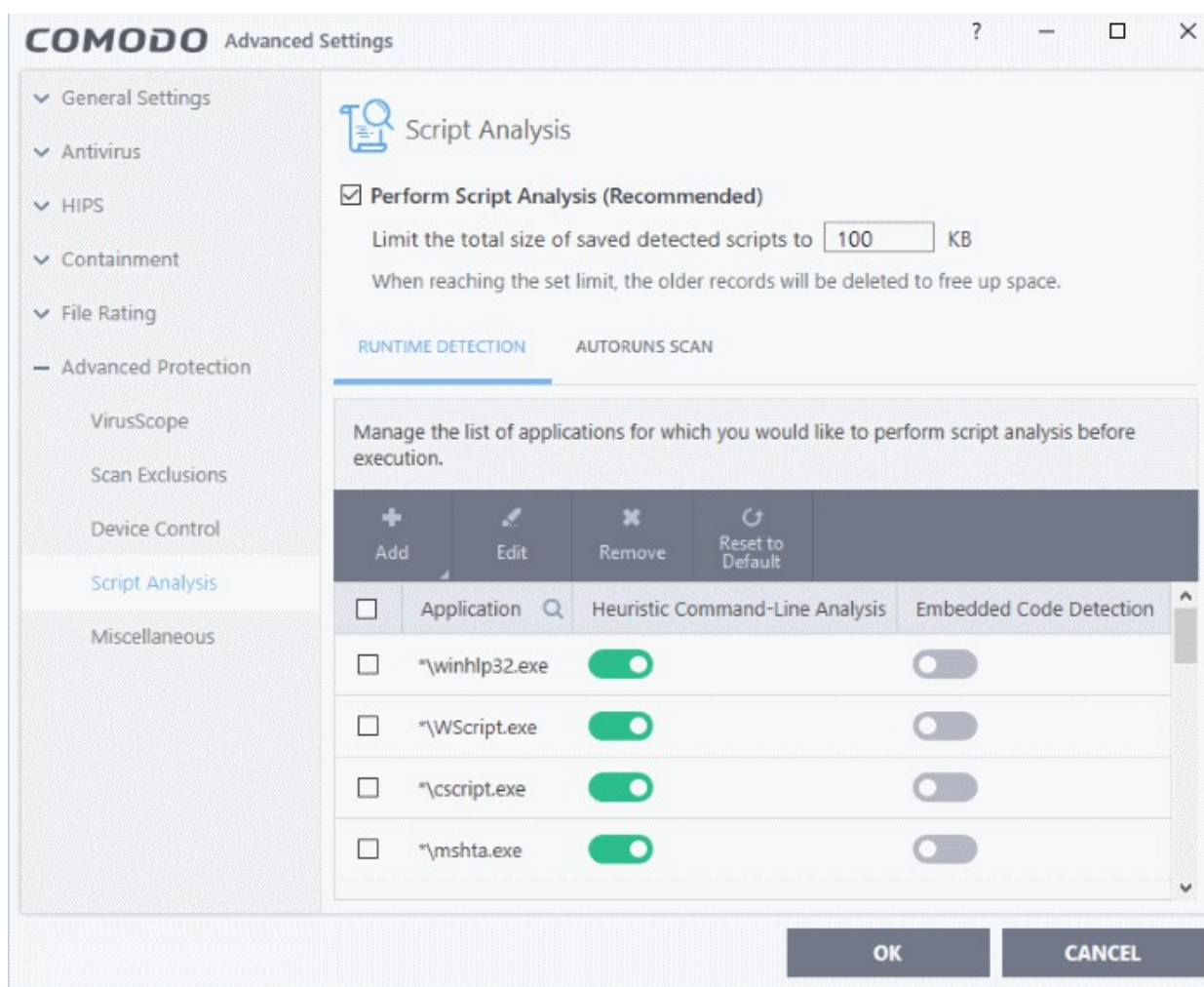
The script analysis settings panel lets you:

- 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 CCS home screen
- 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 - CCS stores the list of executing scripts that are run by the managed applications. 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.

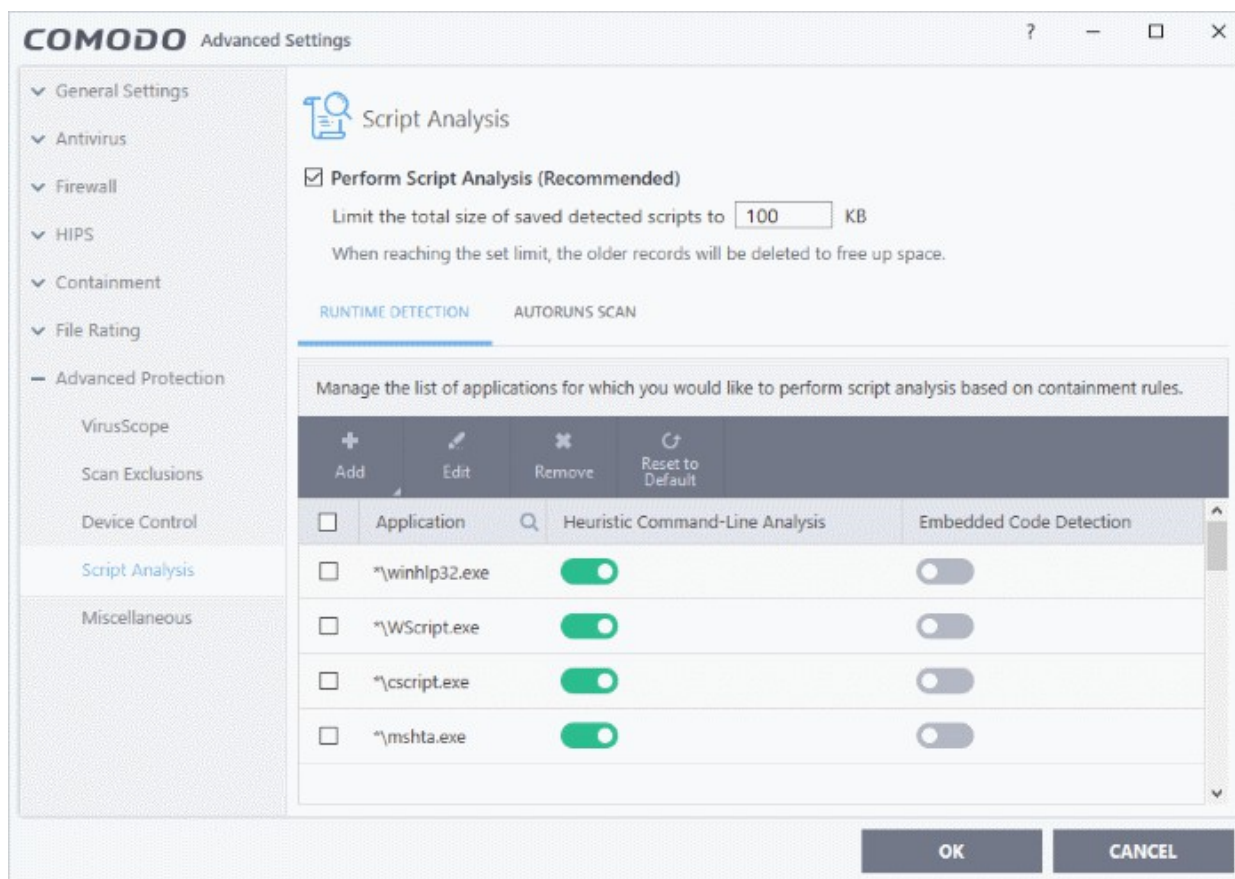
The interface has two tabs:

- **Runtime Detection**
- **Autoruns Scans**

Runtime Detection

CCS 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.

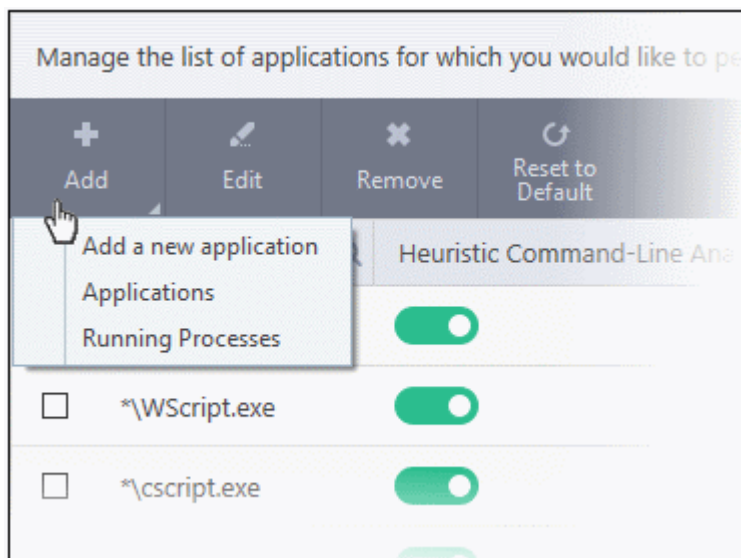
- For example, the program wscript.exe can be made to execute Visual Basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'.
- If this option is selected, CCS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs 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	Names 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

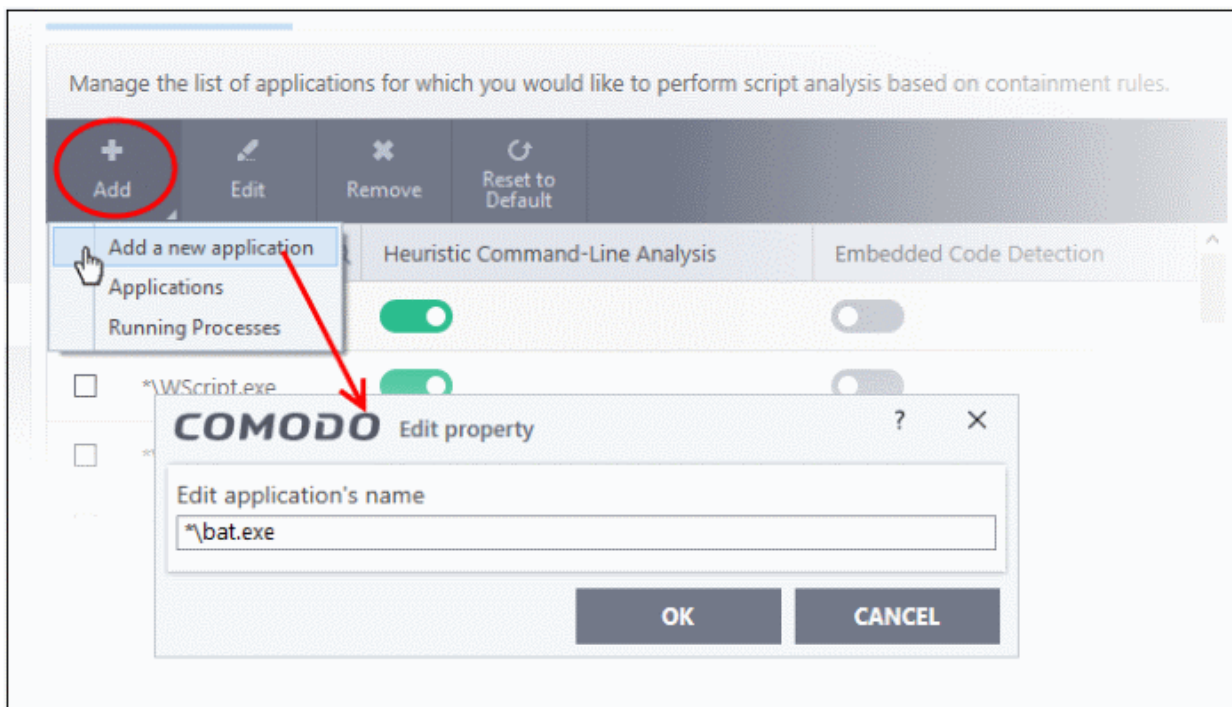


You can add an application by following methods:

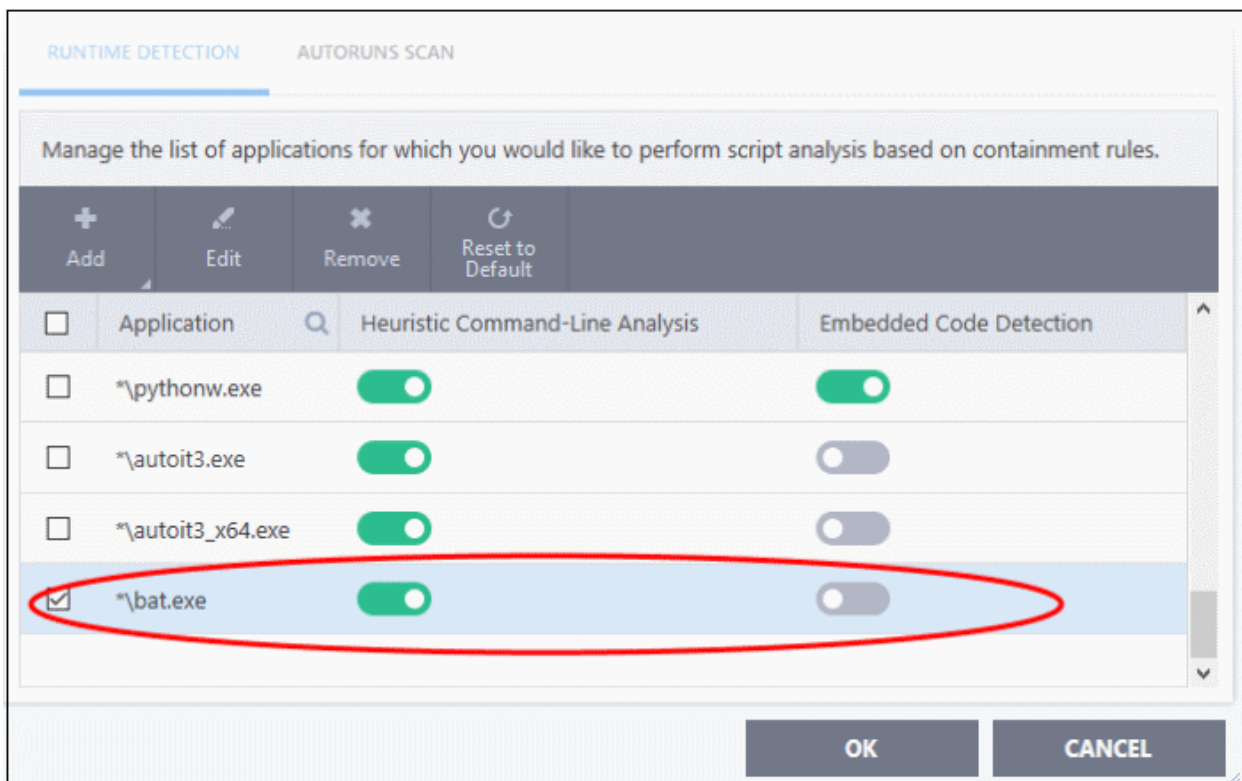
- **Add a new application**
- **Add a current application**
- **Add application from the currently running processes**

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 slider beside the applications to enable/disable them for analysis.
 - Click the 'Edit' button to update the details of an application.
 - To remove an application, select it from the list and choose 'Remove' at the top.
 - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

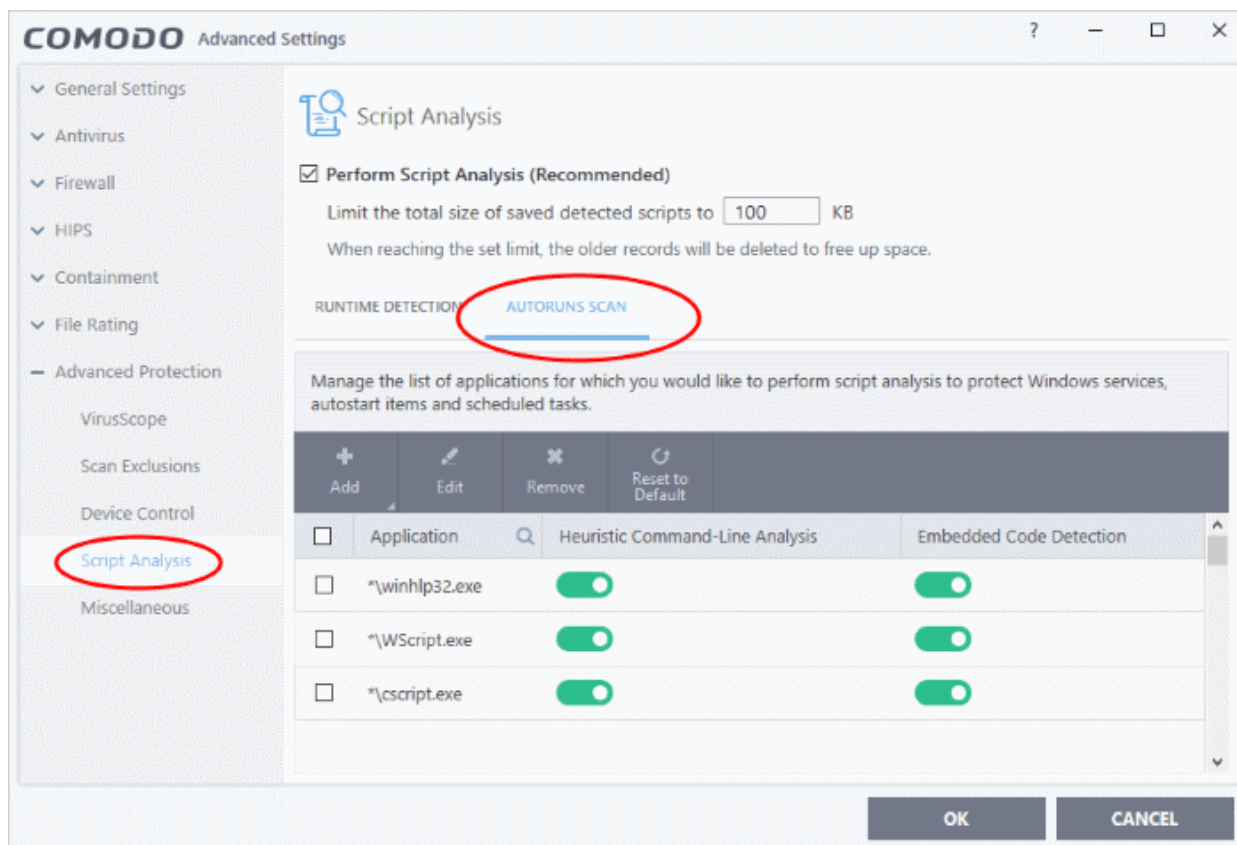
Autoruns Scans

- 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.
- CCS 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)

To open the 'Autoruns Scans' interface

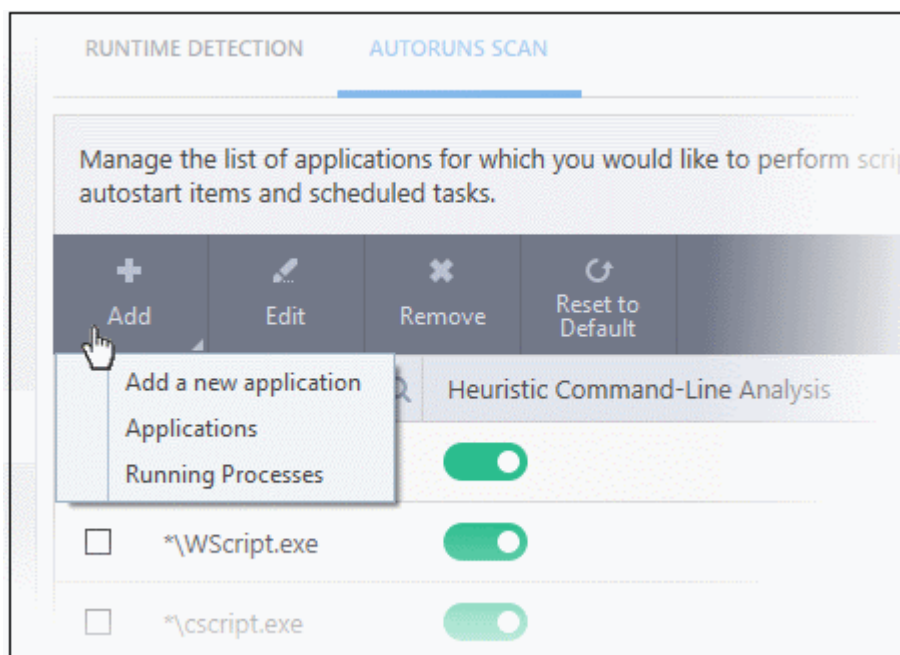
- Click 'Settings' on the CCS home \ tasks screen to open the 'Advanced Settings' interface.
- Click 'Advanced Protection' > 'Script Analysis' on the left then 'Autoruns Scan' tab



Autoruns Scans - Column Descriptions	
Column Header	Description
Application	Names 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

To manually add a new application to the list for analysis

- Click 'Add' at the top

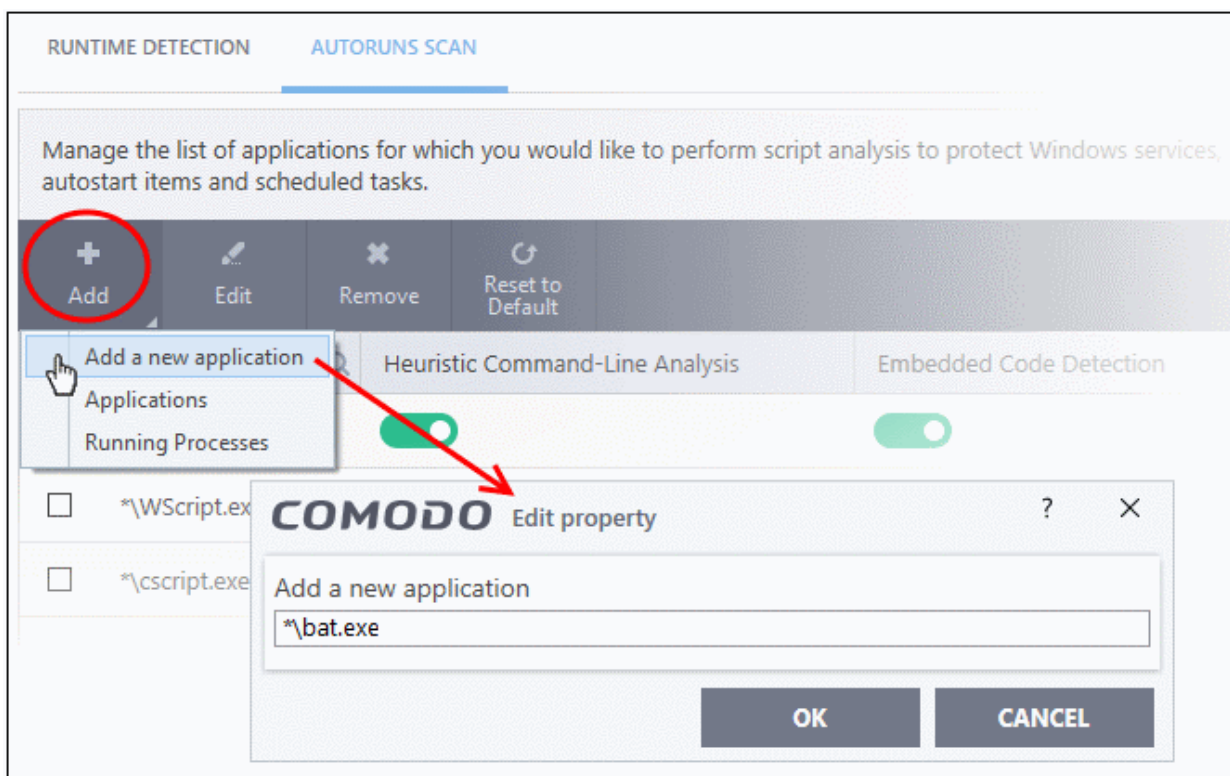


You can add an application by following methods:

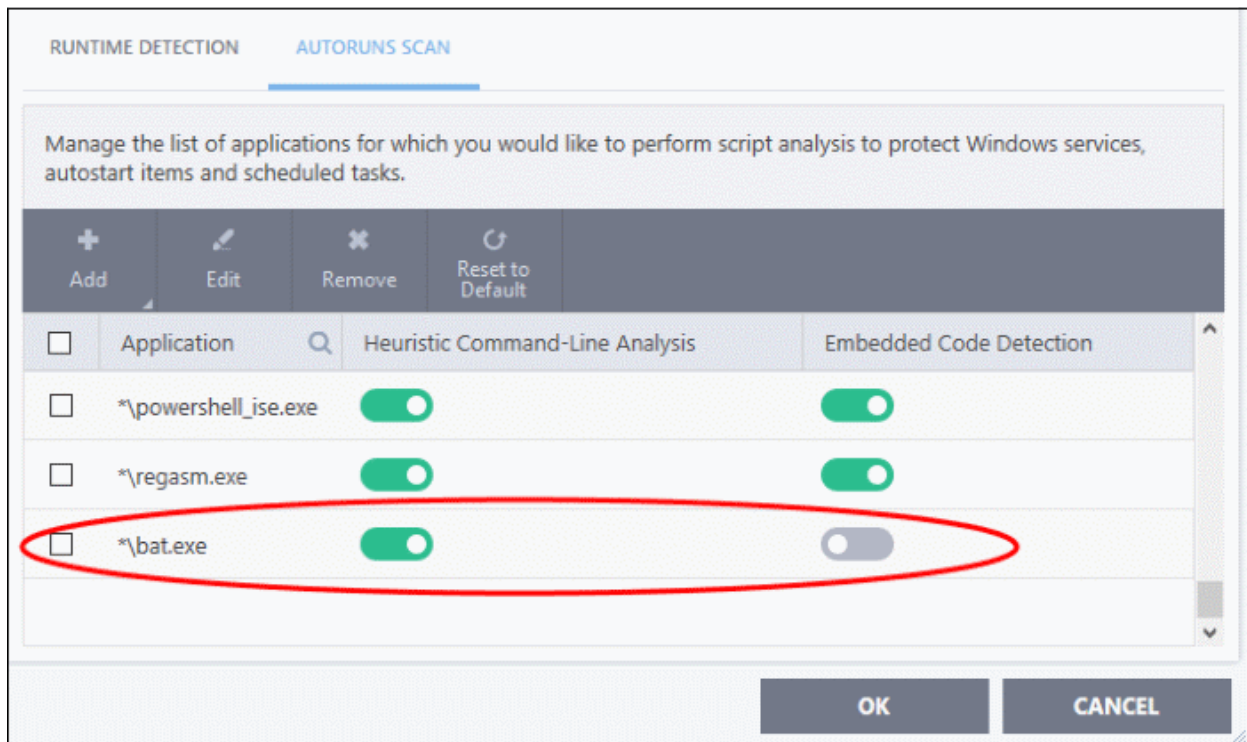
- **Add a new application**
- **Add a current application**
- **Add application from the currently running processes**

Adding 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 slider beside the applications to enable/disable them for analysis.
 - Click the 'Edit' button to update the details of an application.
 - To remove an application, select it from the list and choose 'Remove' at the top.
 - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

6.8.5. Miscellaneous Settings

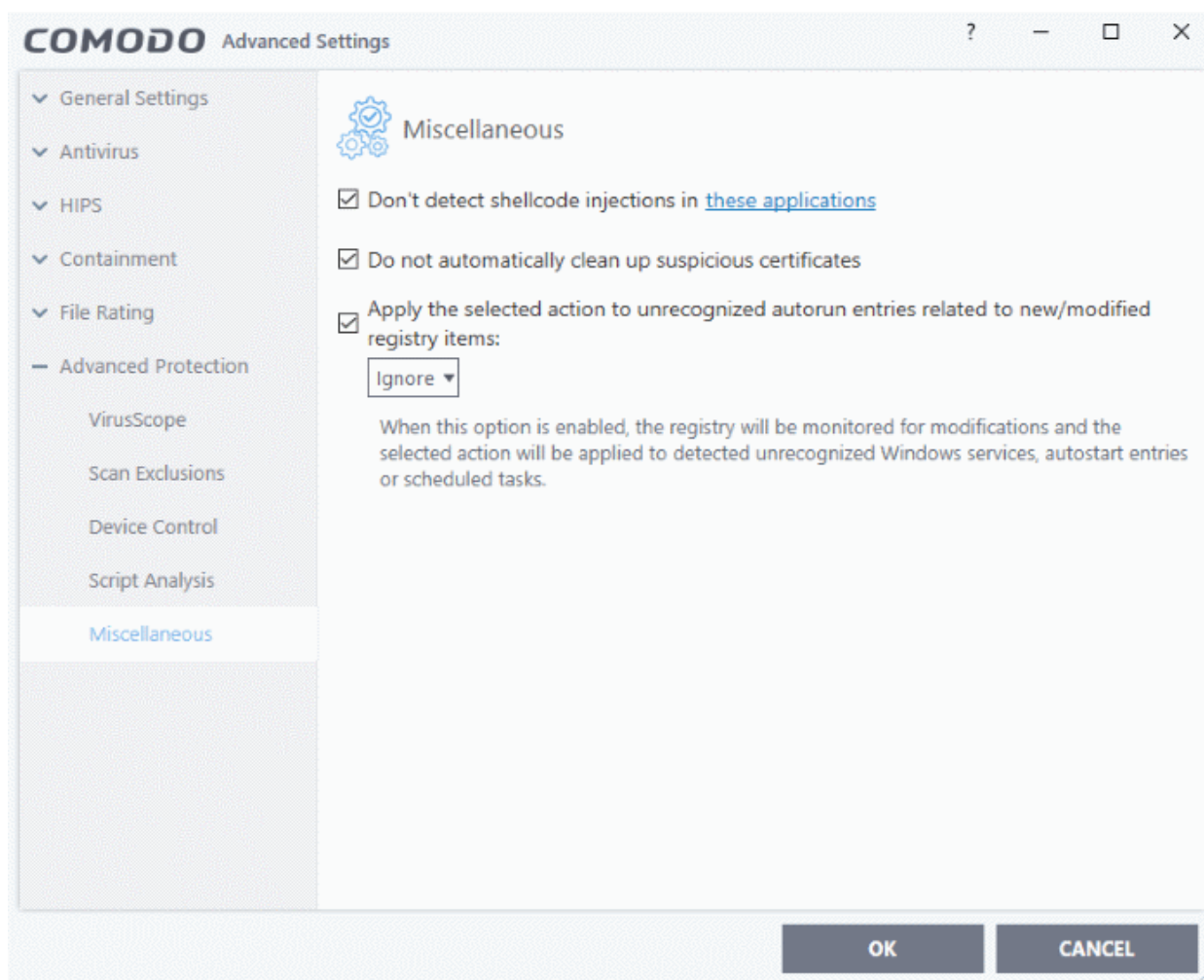
The miscellaneous settings panel allows you to:

- Configure heuristic command line analysis for certain applications
- Configure protection against shellcode injections (buffer overflow attacks)
- Specify what actions are taken if CCS detects unrecognized auto-start entries or scheduled tasks

- Skip automatic cleanup of suspicious certificates.

To open the 'Miscellaneous' settings interface:

- Click 'Settings' on the CCS home \ tasks screen to open the 'Advanced Settings' interface.
- Click 'Advanced Protection' > 'Miscellaneous'



This interface allows you to:

- **Disable shellcode injection detection for certain applications**
- **Define actions to be taken on unrecognized auto-start entries/scheduled tasks**
- **Skip automatically clean-up of suspicious certificates**

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:

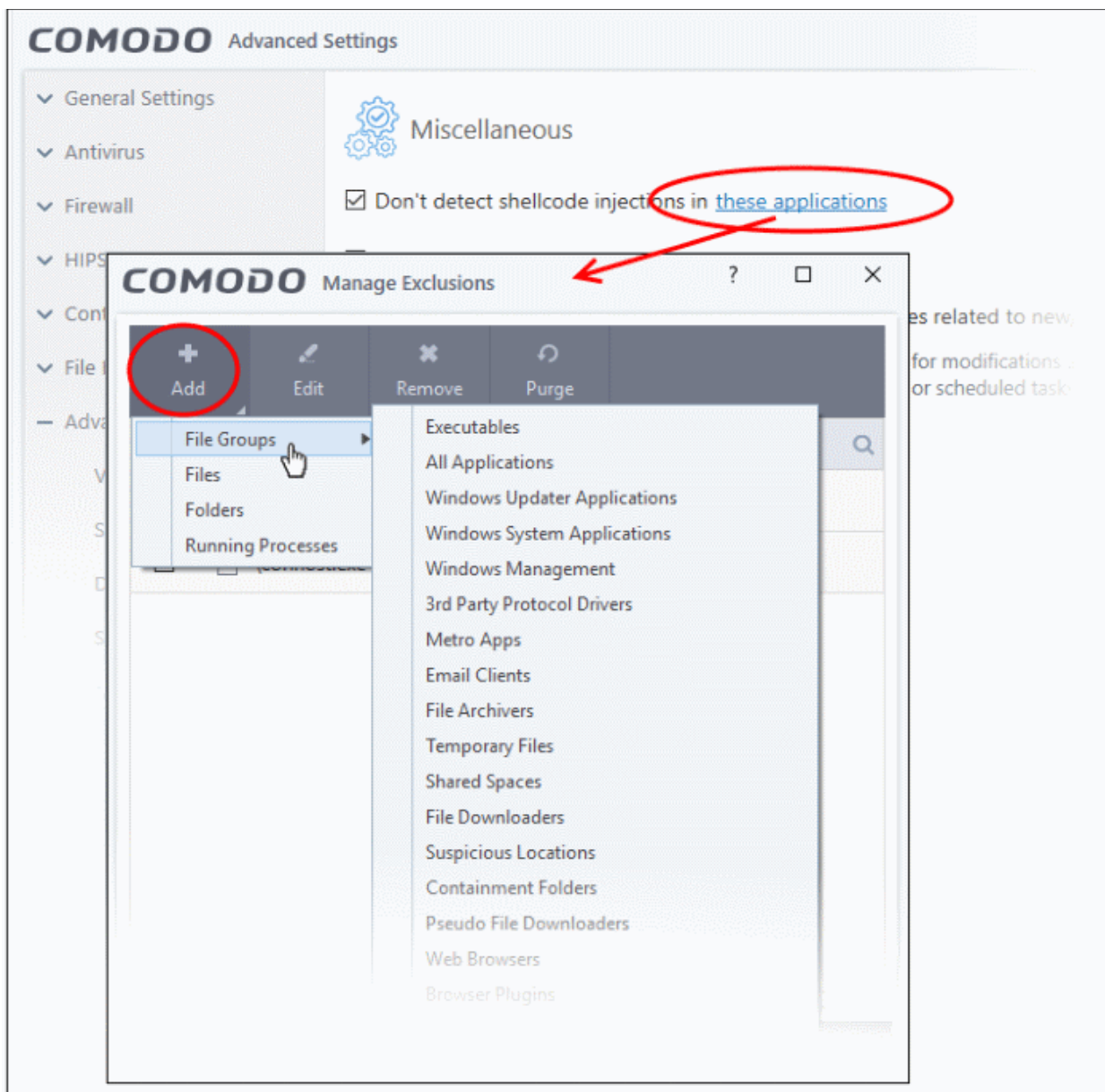
- Shellcode injection is a malicious technique which allows an attacker to cause a buffer overflow on your system.
- A buffer overflow occurs when a process attempts to store data beyond the boundaries of a fixed-length buffer. A buffer is an area of memory designed to hold a specific amount of data.
- 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.

To exclude certain applications from shellcode injection protection

- Make sure 'Don't detect shellcode injections' checkbox is enabled and click the 'these applications' link. The 'Manage Exclusions' dialog will appear.
- Click the 'Add' button at the top

You can add items by selecting the required option from the drop-down:



- **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. See **File Groups**, for more details on file groups.
- **Running Processes** - As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.
- **Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.

- **Files** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.

Click 'OK' to implement your settings.

Define actions to be taken on unrecognized auto-start entries/scheduled tasks

Specify what CCS should do if the managed applications in **Scrip Analysis > Autoruns Scans** try to create or modify one of the following registry items:

- Windows services
- Auto-start entries
- Scheduled tasks

The options are:

- Ignore - CCS does not take any action
- Terminate - CCS 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, CCS disables the service. **(Default)**
- Quarantine and Disable - Auto-start processes are quarantined and the corresponding auto-start entry removed. In the case of a service, CCS disables the service.
- Click 'OK' to save your settings.

Skip automatic cleanup of suspicious certificates

- If disabled, CCS automatically deletes any root certificates that were not signed by a trusted certificate authority.

Background:

- SSL certificates are used by websites to encrypt the connection between your browser and the website.
- This ensures nobody can intercept the traffic sent between you and the website. 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. You will also notice that the website address begins with https:// (the 's' stands for 'secure').
- SSL certificates are issued to website owners by an organization known as a 'Certificate Authority' (CA). The certificate authority checks the applicant, the website owner, is a legitimate business before they will issue a certificate to them.
- Root certificates are embedded in your browser and are used to check that the SSL certificate used by a website is legitimate. That it was indeed signed by a certificate authority.
- A fake root certificate would, therefore, bypass this check of legitimacy. It could tell you to trust a website run by a hacker.
- CCS detects whether you have any fake root certificates in your browser and warns you if you do. Disable this option if you also want CCS to delete fake root certificates automatically.

Appendix 1 - CCS How to... Tutorials

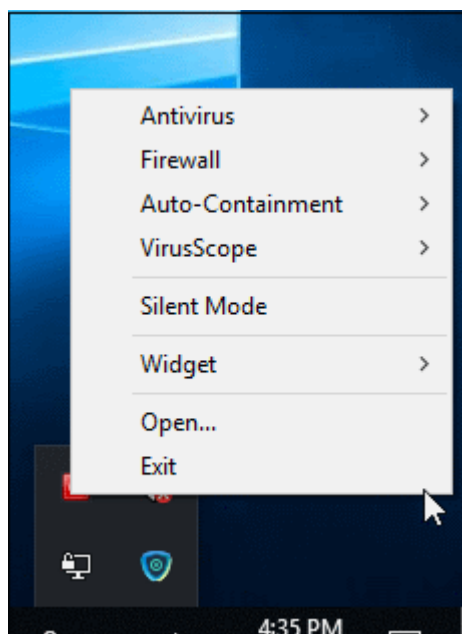
The 'How To...' section of the guide contains guidance on key tasks in Comodo Client Security. Use the links below to go to each tutorial's page.

How to...:

- **Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily** - How to quickly enable or disable various CCS 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
- **Set up HIPS for Maximum Security and Usability** - How to set up Host Intrusion Protection for the optimum balance between security and usability
- **Create Rules to Auto-Contain Applications** - How to set auto-containment rules for maximum security against untrusted applications
- **Run an instant Antivirus scan on selected items** - Run a manual scan on selected folders/files to check for viruses and other malware
- **Create an Antivirus scan 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** - Run your browser inside the container when you plan to visit untrusted websites
- **Restore incorrectly quarantined item(s)** - Restore files and executables that had been moved to quarantine by mistake
- **Submit quarantined items to Comodo for analysis** - Send suspicious files/executables to Comodo for analysis
- **Enable file sharing applications like BitTorrent and Emule** - Configure Comodo Firewall for file sharing through popular software
- **Block any downloads of a specific file type** - Configure HIPS to block downloads of files of a specific type
- **Disable Auto-Containment on a Per-application Basis** - Exclude specific files or file types from the auto-containment process
- **Switch Off Automatic Antivirus Updates** - Stop automatic virus updates
- **Suppress alerts when playing games** - Switch off CCS pop-up alerts to avoid interruptions while playing games
- **Control External Device Accessibility** - Restrict access to external devices such as USB pen drive on the endpoints.

Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily

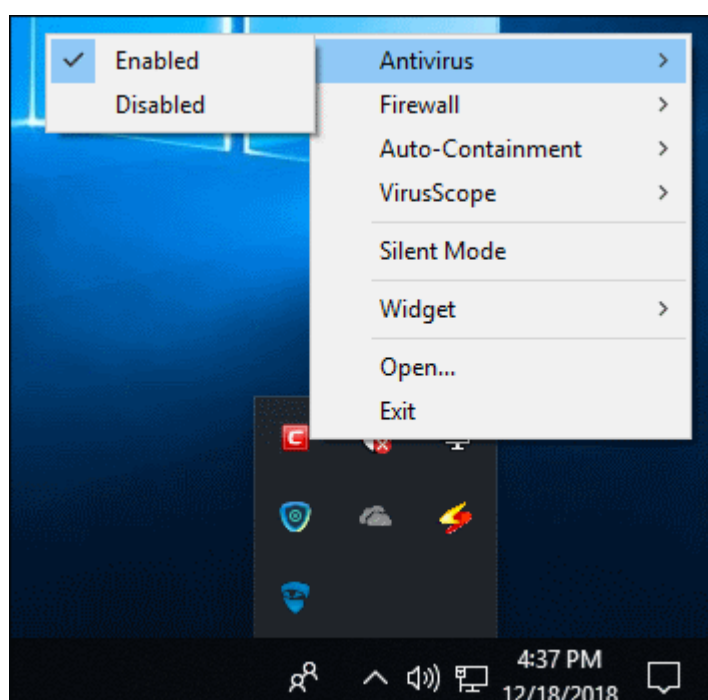
Right-click on the CCS tray icon to quickly switch **Antivirus**, **Firewall**, **Auto-Containment** or **VirusScope** on or off.



Antivirus

To enable/disable Antivirus

1. Right-click on the system tray icon
2. Move your mouse over 'Antivirus'



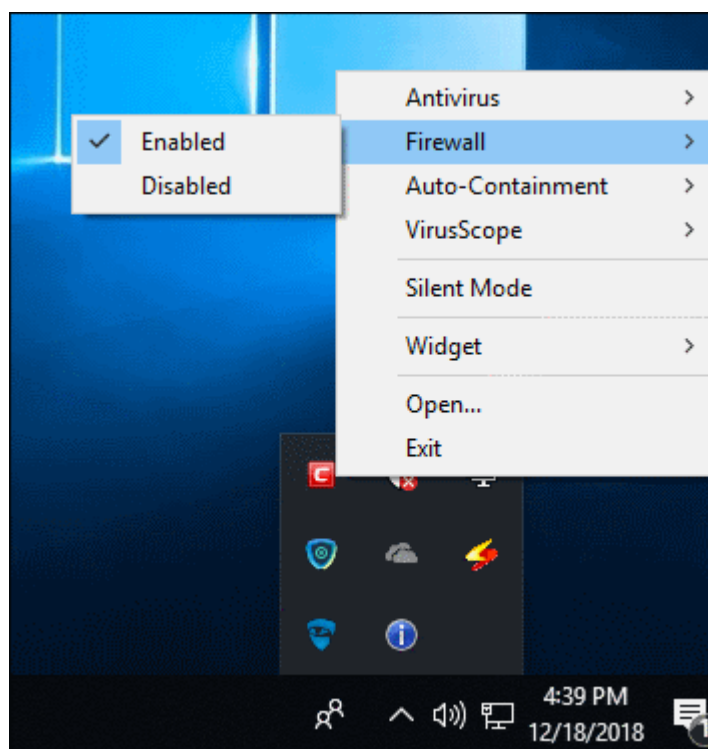
3. Choose 'Enabled' or 'Disabled' as required
You can also set security level in **the Home Screen**.

Firewall

To Enable/Disable Firewall

1. Right-click on the system tray icon
2. Move your mouse over 'Firewall'

3. Choose 'Enabled' or 'Disabled' as required

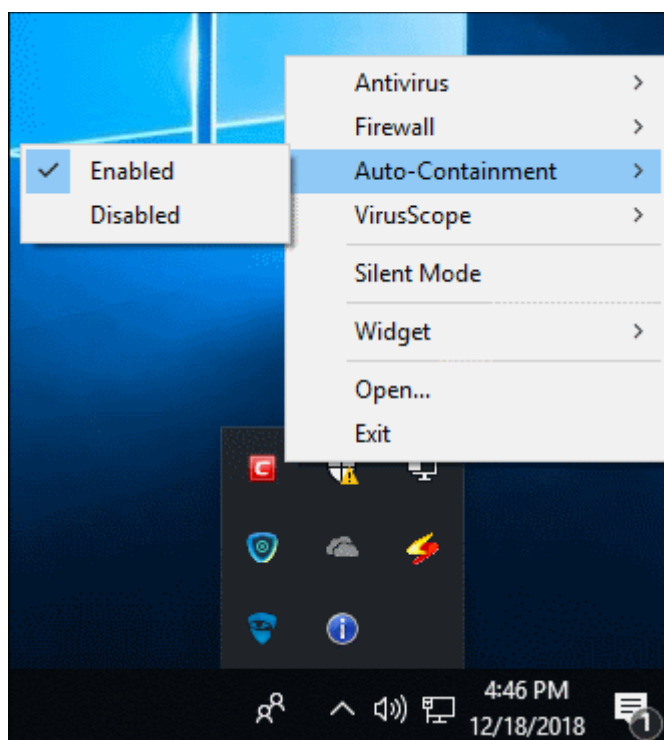


You can also set security level in **the Home Screen**.

Auto-Containment

To enable/disable the Auto-Containment

1. Right-click on the system tray icon
2. Move your mouse over 'Auto-Containment'

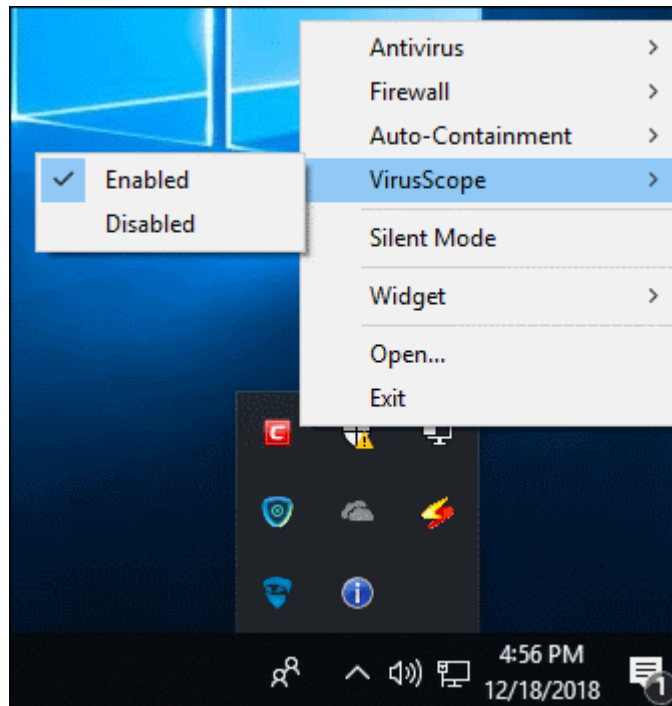


3. Choose 'Enabled' or 'Disabled' as required

You can also set security level in **the Home Screen**.

To enable/disable the VirusScope

1. Right-click on the system tray icon
2. Move your mouse over 'VirusScope'



3. Choose 'Enabled' or 'Disabled' as required

You can also set security level from **the Home Screen**.

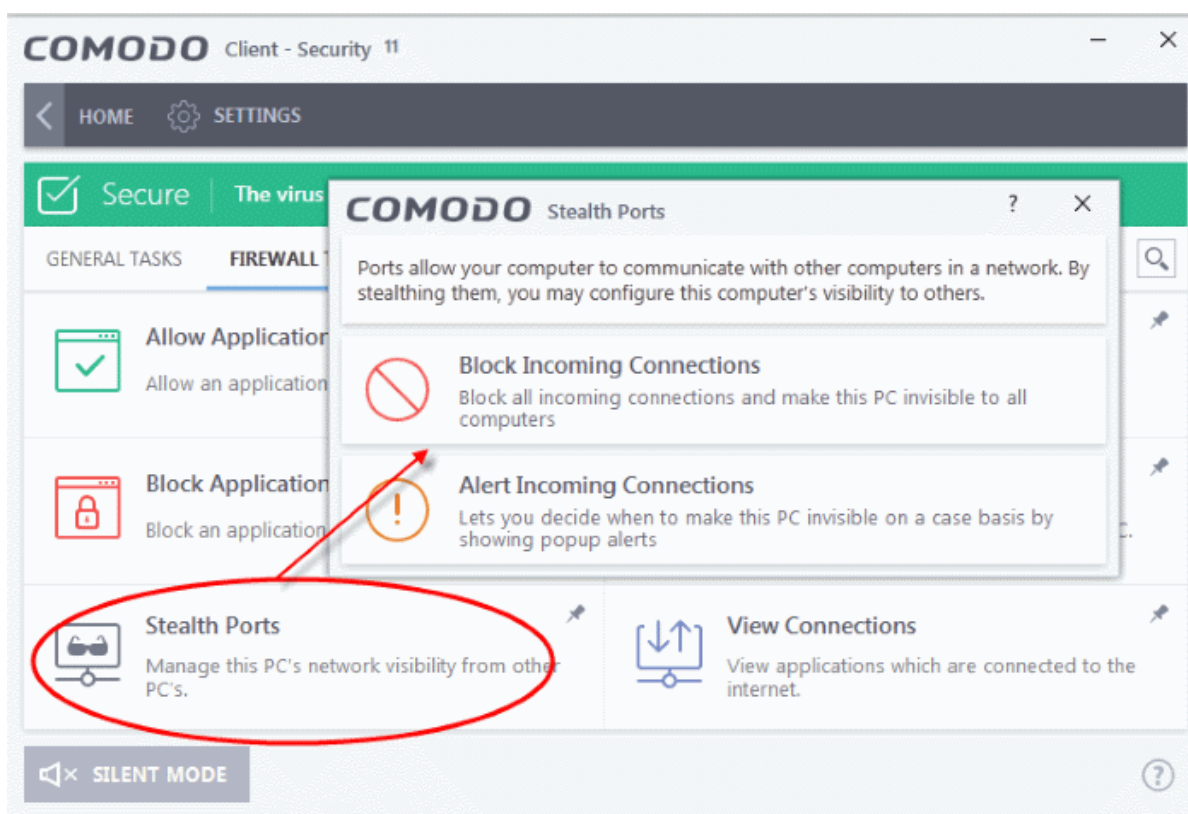
Set up the Firewall For Maximum Security and Usability

This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the internet.

Stealth Ports Settings

Port stealthing is a security feature whereby ports on an internet connected PC are hidden from sight, sending no response to opportunistic port scans.

1. Click 'Tasks' at the top-left of the CCS screen
2. Click 'Firewall Tasks' tab > 'Stealth Ports'



3. Select 'Block Incoming Connections' to make your computer's ports are invisible to all networks

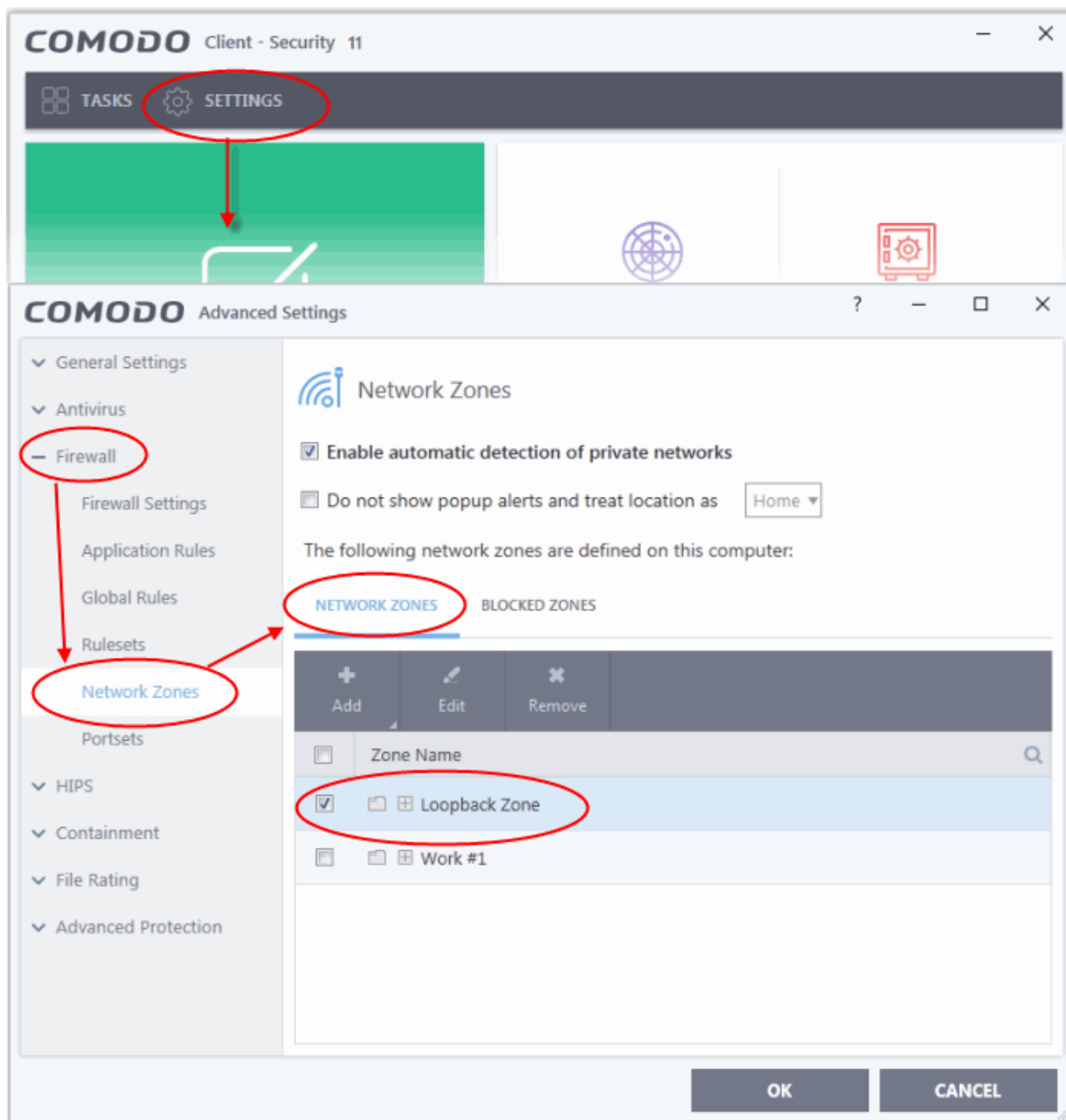
[Click here for more information about port stealthing](#)

Network Zones Settings

'Network Zones' settings allow you to configure the protection level for connections to a router/home network (this is usually done **automatically** for you).

To view the configurations

1. Click 'Settings' at the top of the CCS home screen
2. Select 'Firewall' > 'Network Zones'
3. Click 'Network Zones' tab in the 'Network Zones' interface



4. Inspect the 'Loopback zone' and 'Local Area Network #1' (exact name may vary) by clicking the '+' button beside the zone name
 - **In most cases**, the loopback zone IP address should be 127.0.0.1/255.0.0.0
 - **In most cases**, the IP address of the auto-detected Network zone should be 10.nnn.nnn.nnn/255.255.255.0
5. Click 'OK'.

[Click here for more details on Network Zones settings](#)

Firewall Settings

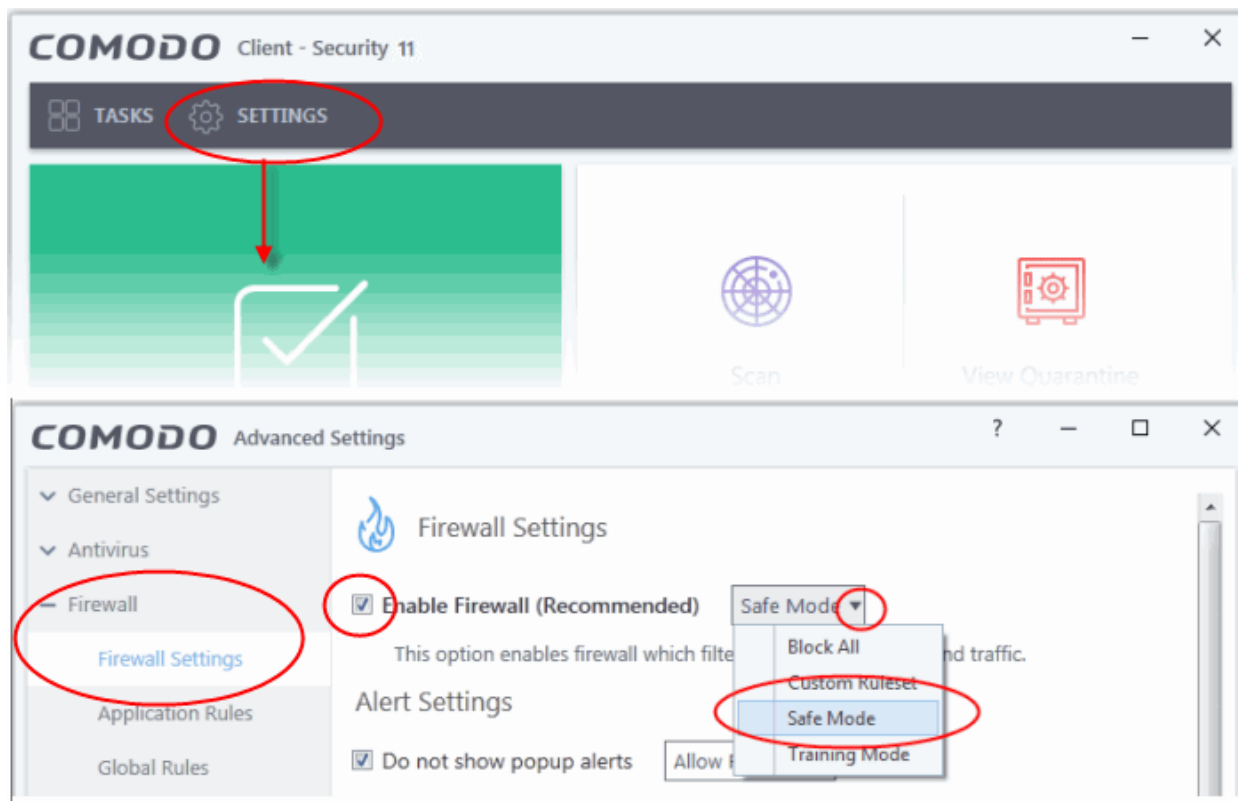
The Firewall settings option lets you configure the protection level for your internet connection and the frequency of alerts generated.

To open the Firewall settings panel

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Firewall' > 'Firewall Settings' on the left

3. Select 'Enable Firewall' and choose 'Safe Mode' from the drop-down

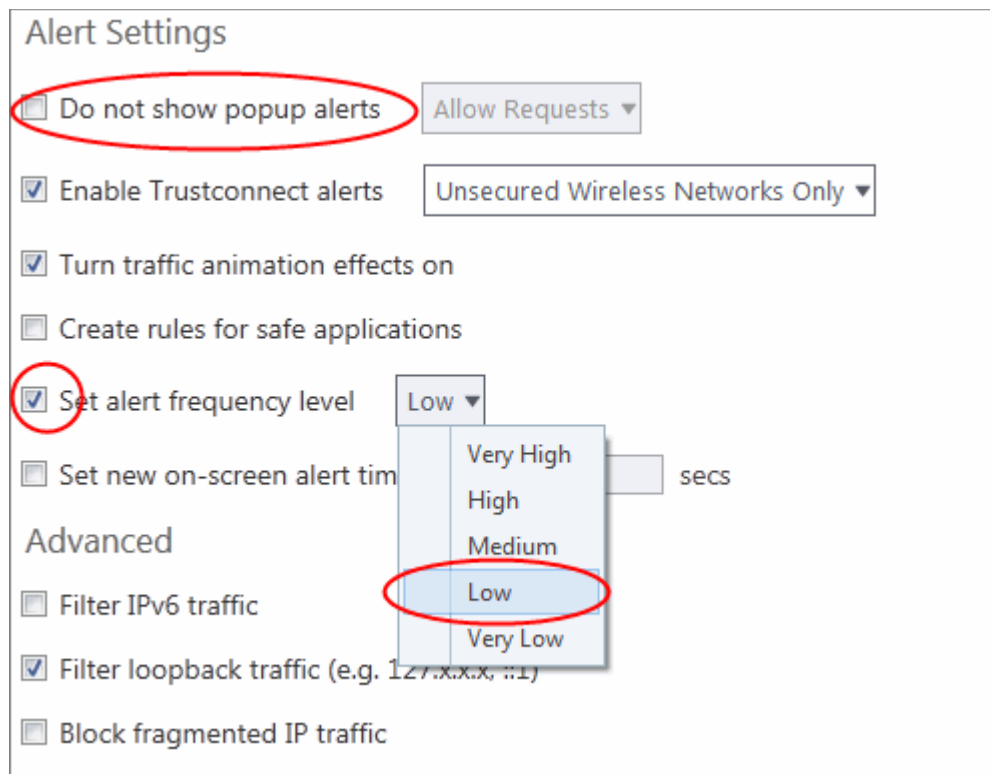
Safe Mode: While filtering network traffic, the firewall will automatically create rules which allow traffic for application components certified as 'Safe' by Comodo. For non-certified, new, applications, you will receive an alert whenever that application attempts to access the network. Should you choose, 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:

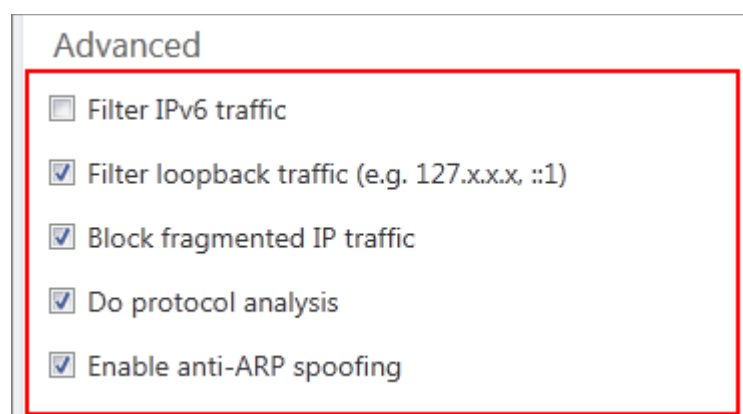
- Deselect 'Do not show pop-up alerts'
- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority 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 '**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.

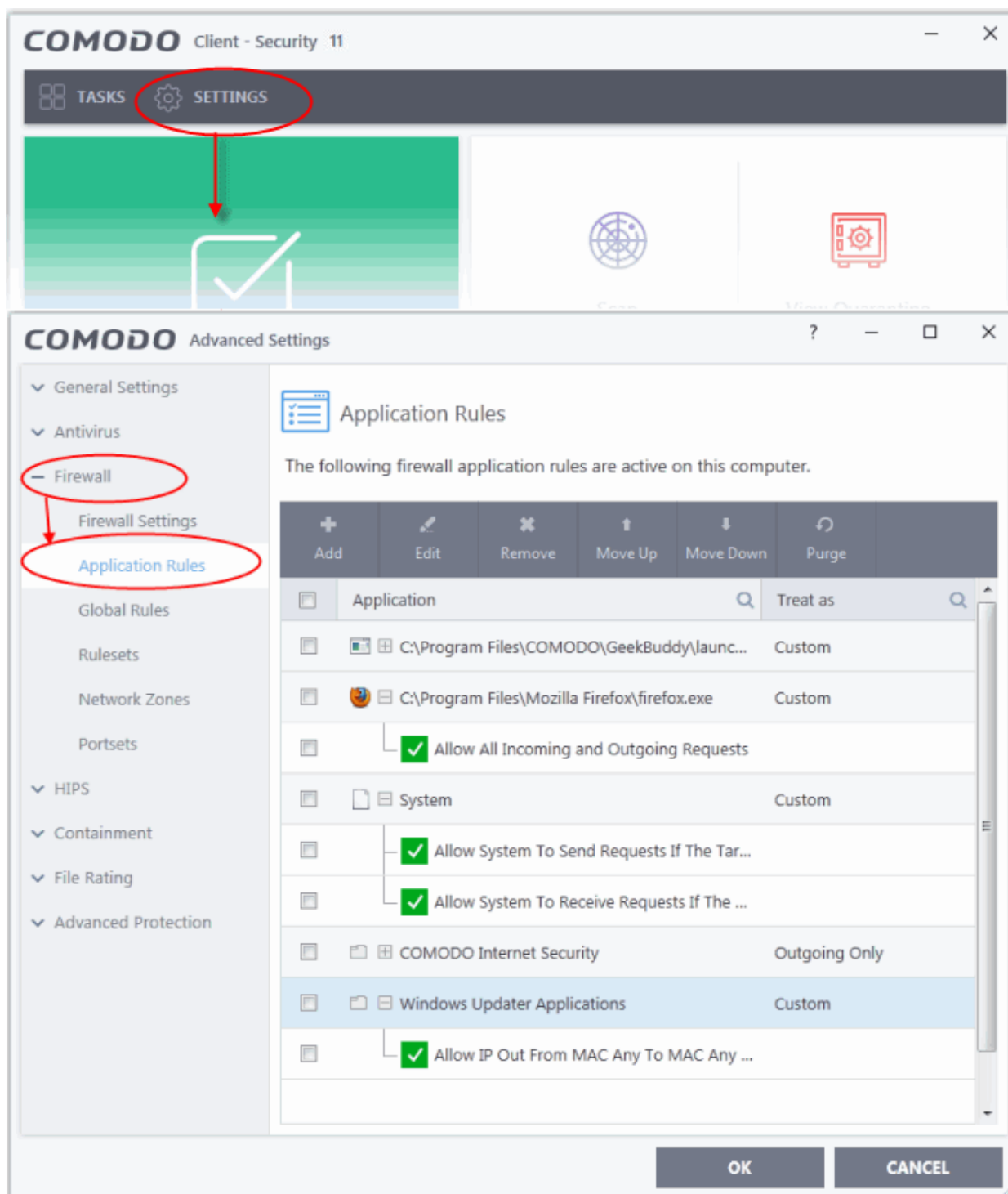
[Click here for more details on Firewall Settings](#)

Setting-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules and policies on an application-specific and global basis.

To view the Application Rules

1. Click 'Settings' at the top of CCS home screen
2. Click 'Firewall > 'Application Rules' on the left

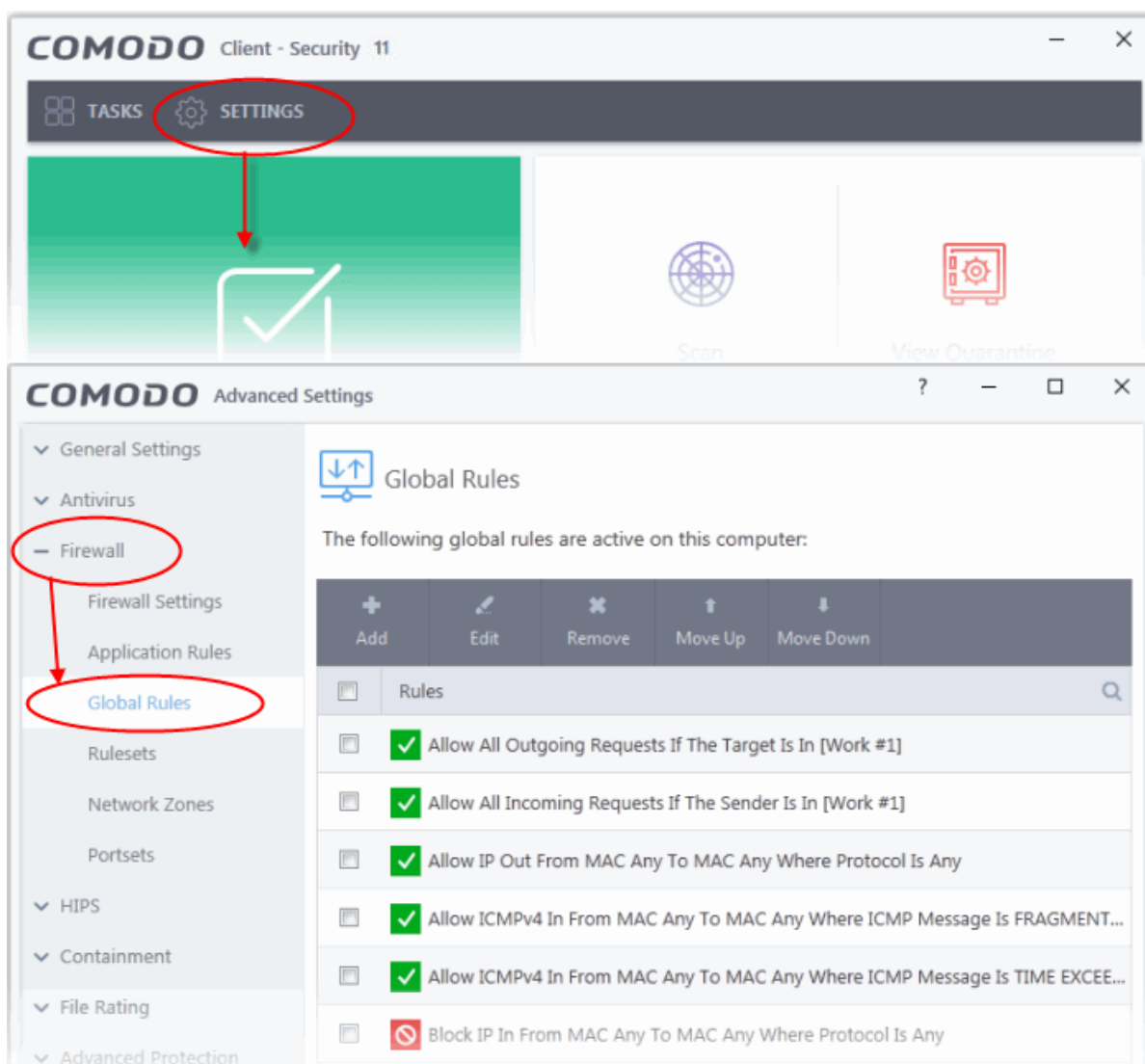


3. Click 'Add' to add a new application rule
4. Select a rule and click 'Edit' to edit the rules for a specific application manually or click 'Remove' to remove them
5. Click 'OK' for your settings to take effect

[Click here for more details on Application Rules](#)

To view the Global Rules

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Firewall' > 'Global Rules' on the left

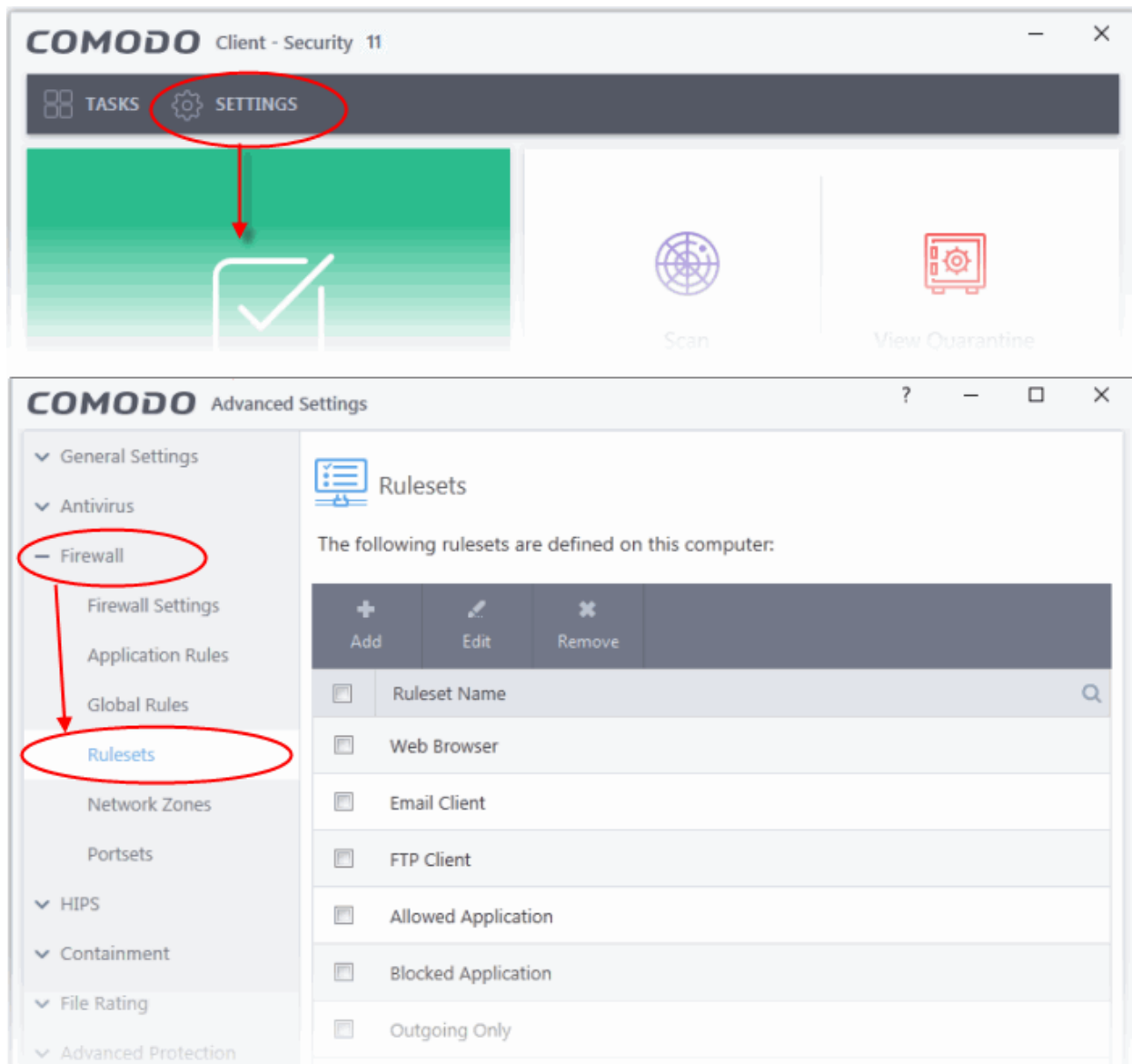


3. Click 'Add' to add a new global rule
4. Select a rule and click 'Edit' to edit the a rule manually or click 'Remove' to remove them
5. Click 'OK' for your settings to take effect

[Click here for more details on Global Rules](#)

To view Predefined Firewall rulesets

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Firewall' > 'Rulesets' on the left



3. Click 'Add' to add a new ruleset
4. Select a ruleset and click 'Edit' to edit the rules manually or click 'Remove' to remove them
5. Click 'OK' for your settings to take effect

Note: You need not make your own rulesets, the defaults are usually enough.

[Click here for more details on pre-defined firewall rulesets](#)

Block Internet Access while Allowing Local Area Network (LAN) Access

You can configure Comodo Firewall to block internet access while allowing connections to an internal network (intranet or LAN).

Example scenarios:

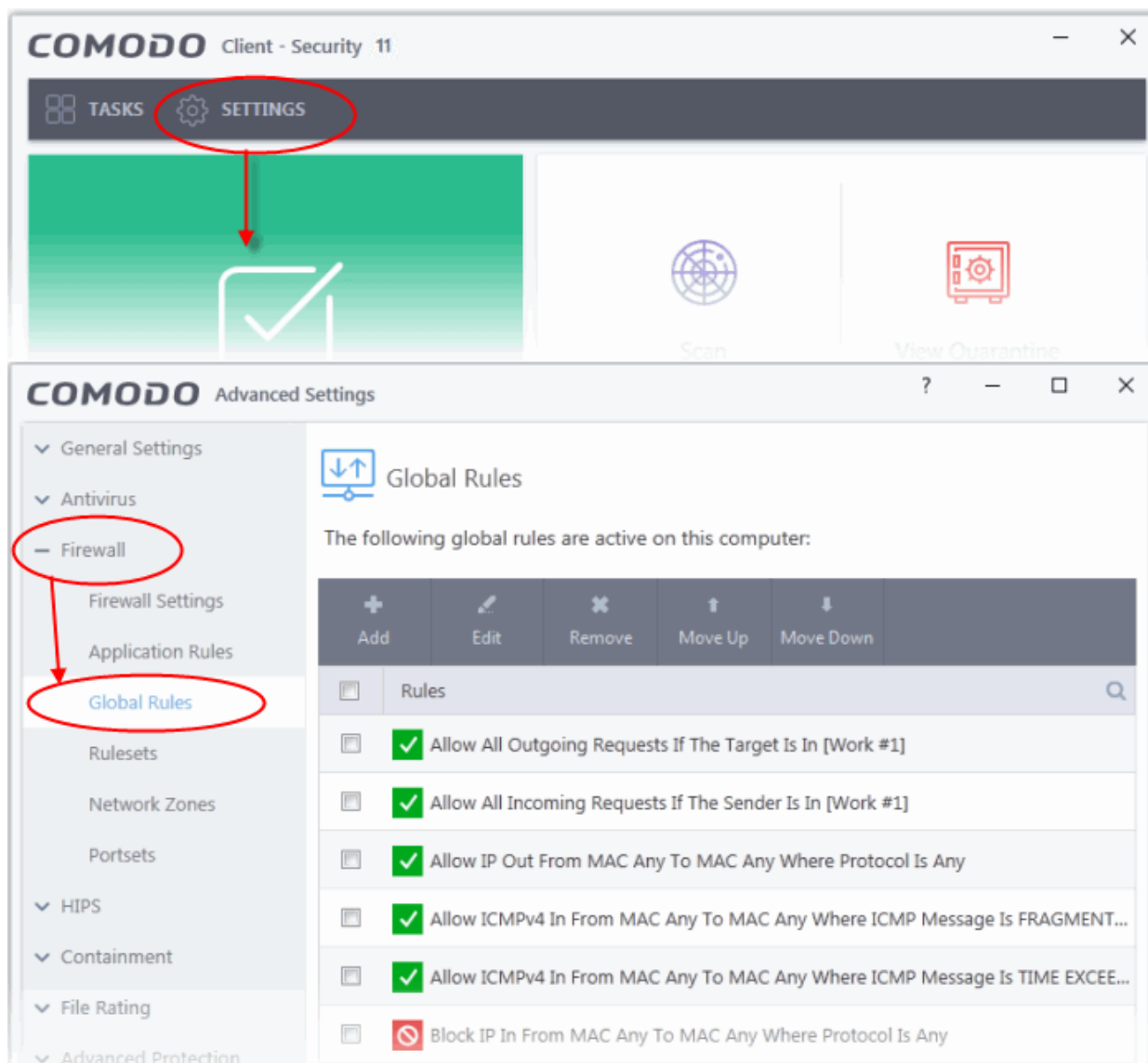
- In your network at home, you want your child's computer to connect to other computers at home but disable their internet access for safety reasons
- In your corporate network, you want your employee's computers to connect to your network machines but disable internet access for bandwidth reasons

*Side note. If you just want to block access to certain websites, see **'Block/allow websites selectively to users of your computer'** instead.*

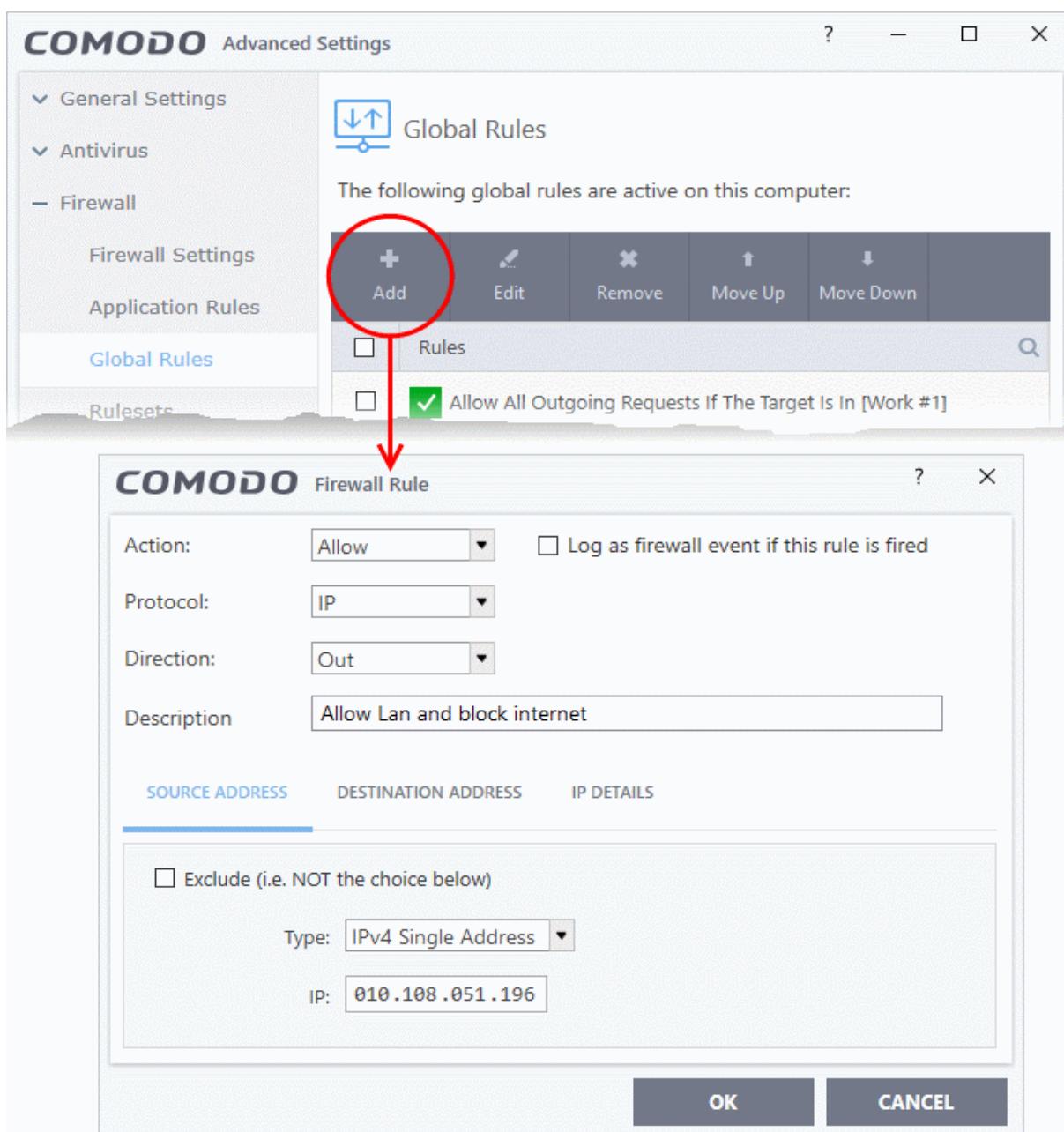
To block internet access while allowing connections to an internal network, you need to create a 'Global Rule' under firewall settings. You should also password protect your configuration to prevent others from altering it.

To create Global Rules

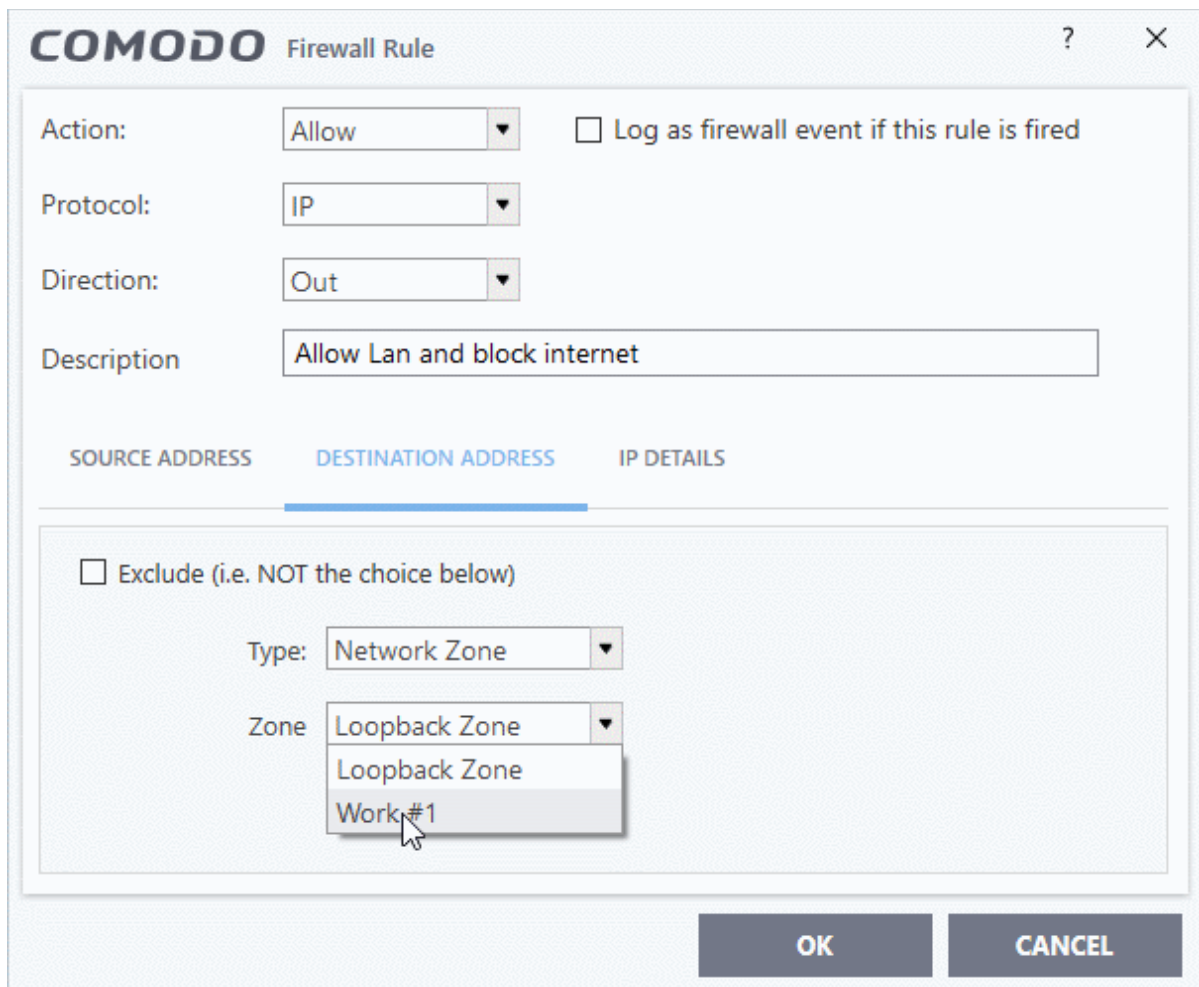
1. Click 'Settings' at the top of the CCS home screen
2. Click 'Global Rules' under 'Firewall' on the left



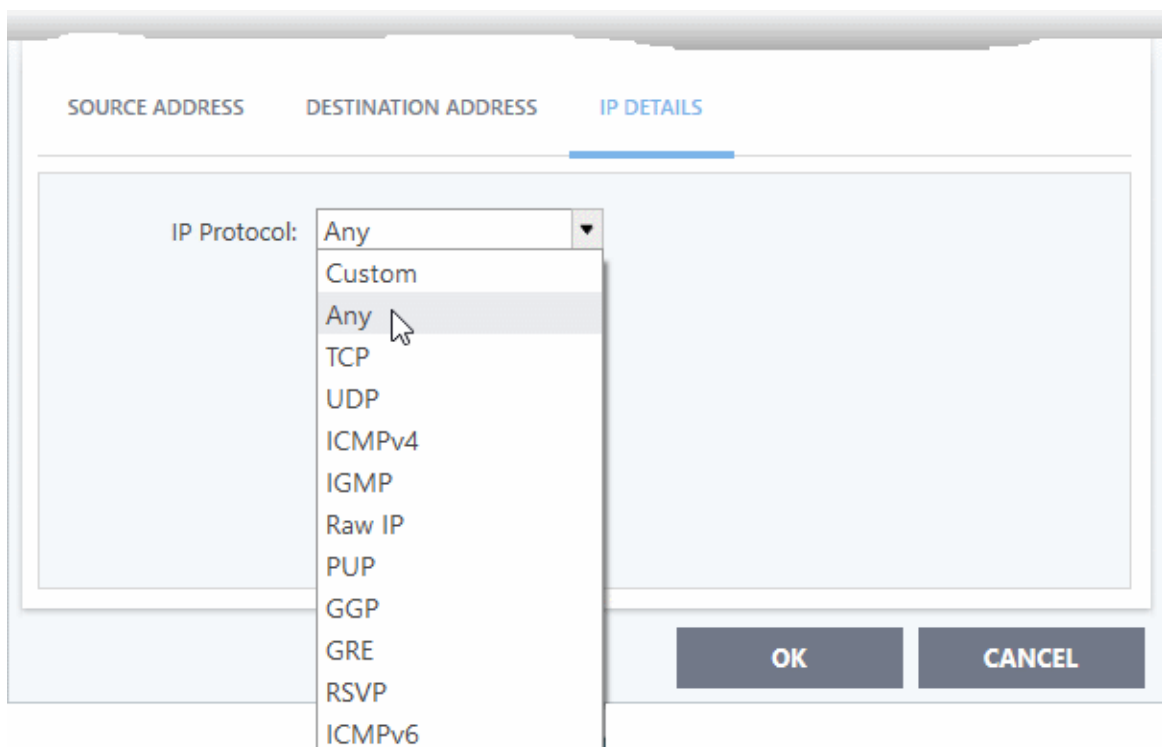
3. Choose 'Add' from the options at the top. The 'Firewall Rule' interface will open.



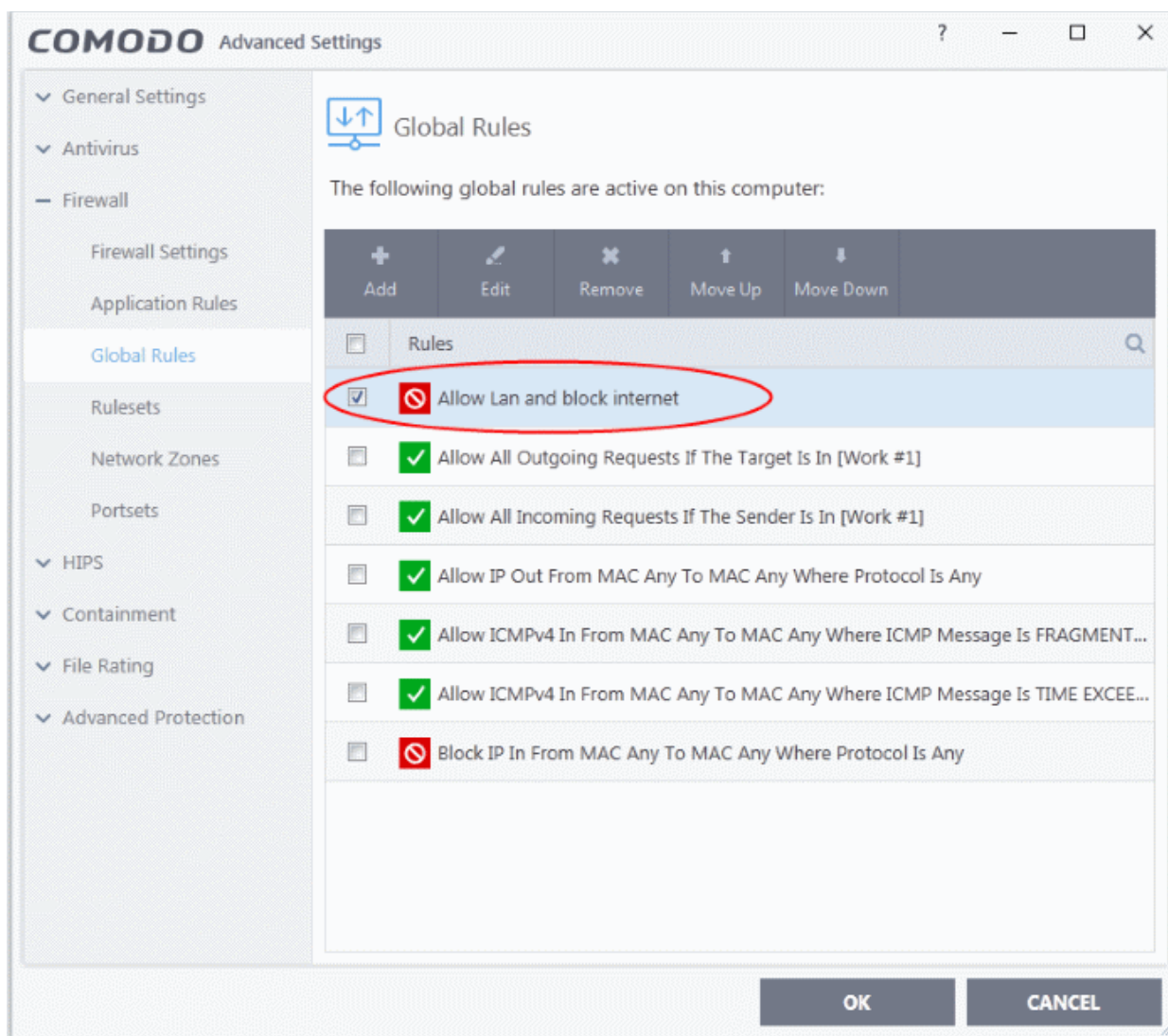
4. Choose the following options from the respective drop-downs:
 - Action = 'Block';
 - Protocol = 'IP';
 - Direction = 'Out'.
5. Enter a description for the new rule in the 'Description' text box.
6. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network 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.

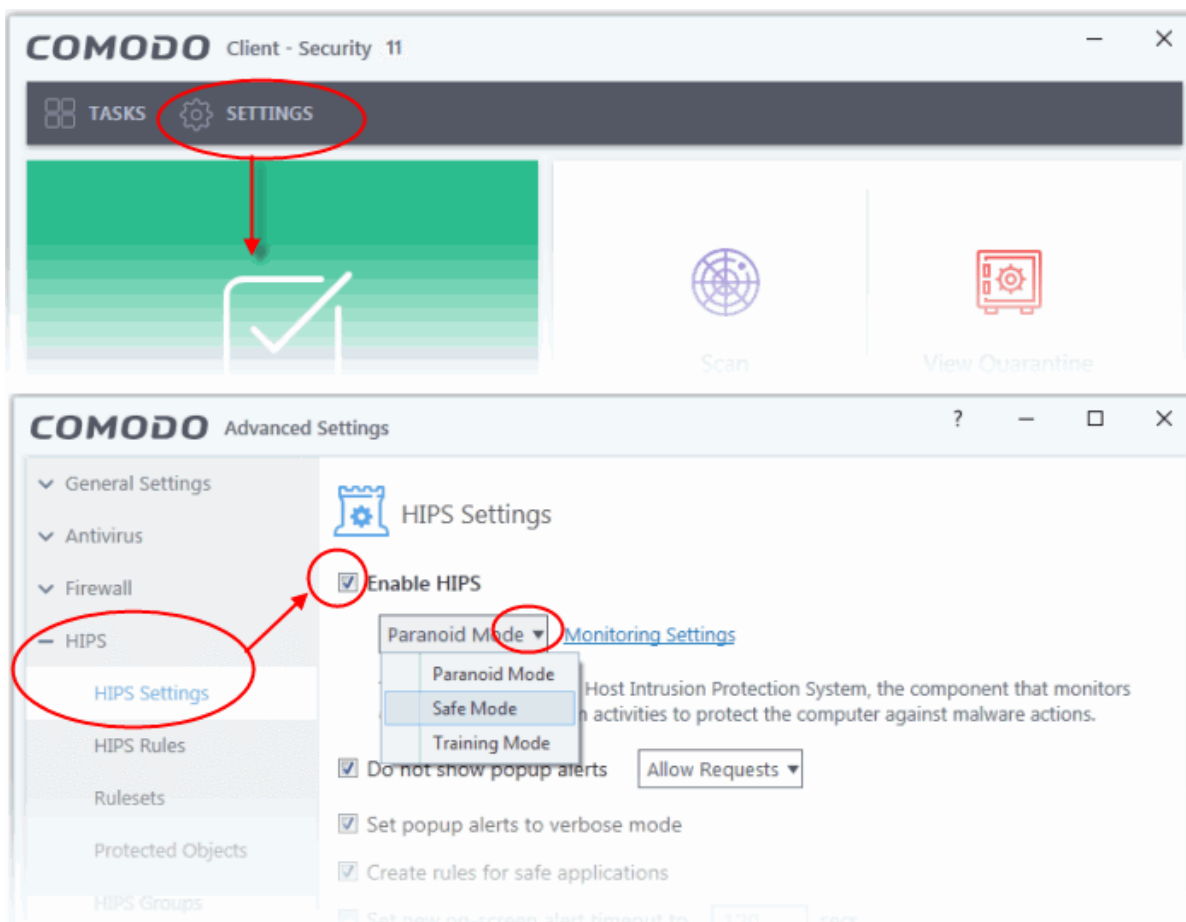
Your firewall is now configured to allow access to the internal network but to block internet access. Now you need to password protect this configuration to prevent others from changing it.

Set up HIPS for Maximum Security and Usability

This page explains how to configure the Host Intrusion Prevention System (HIPS) component to provide maximum security against malware and hackers.

To configure HIPS

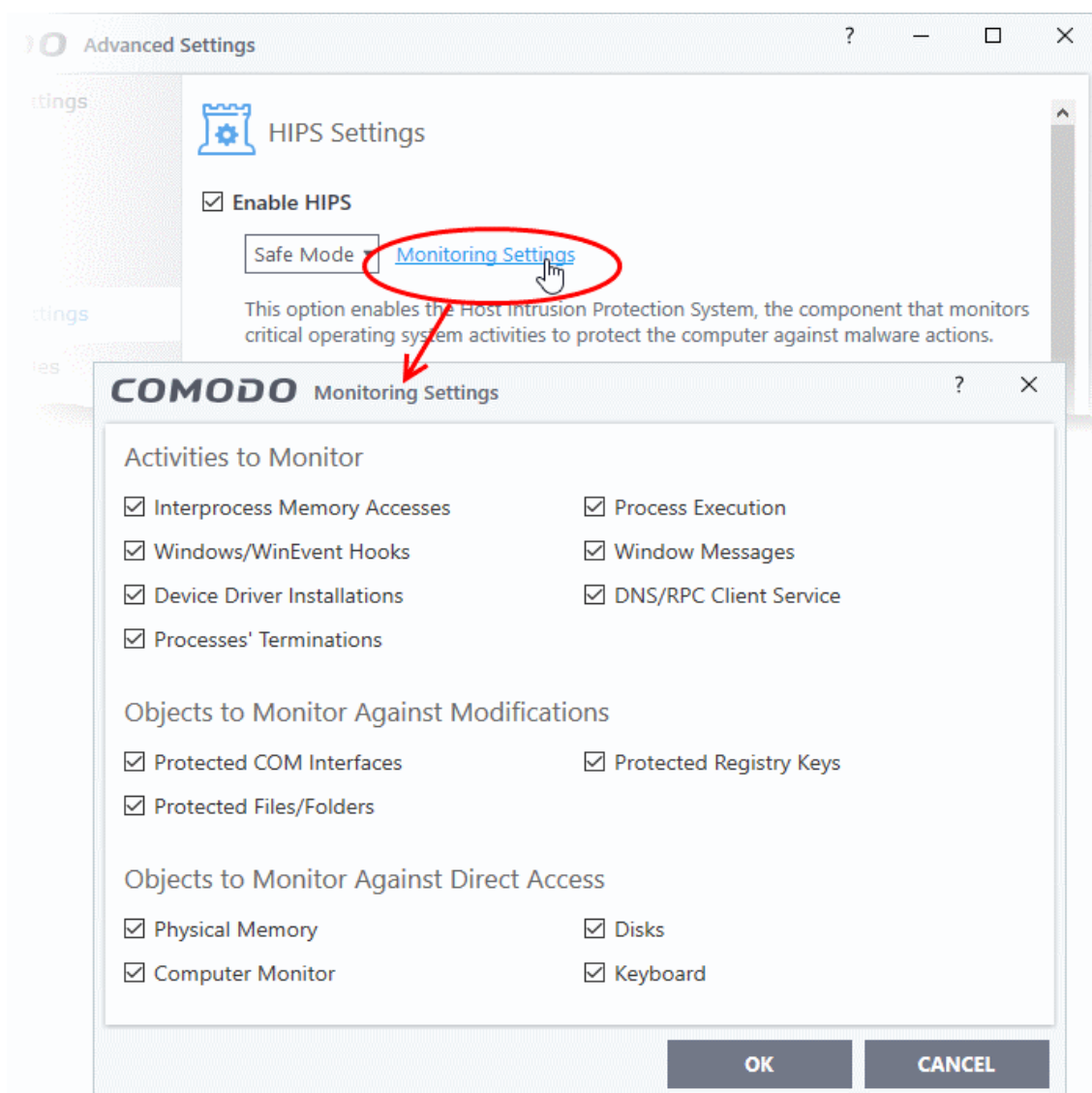
1. Click 'Settings' at the top of the CCS home screen
2. Click 'HIPS' > 'HIPS Settings' the left
3. Enable the checkbox 'Enable HIPS'



4. Choose 'Safe Mode' from the drop-down. See [HIPS Settings](#) for more details.

Monitoring Settings

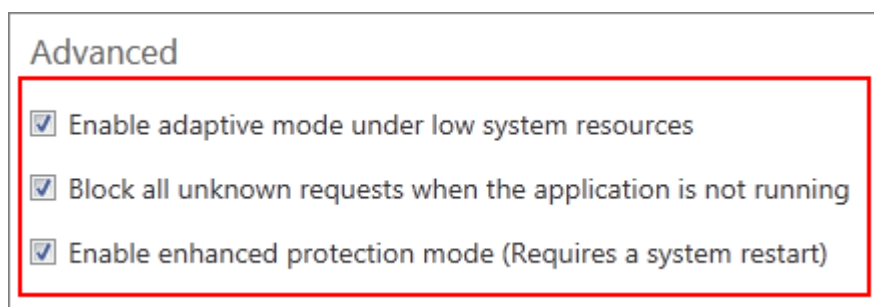
1. Click the 'Monitoring Settings' link in the 'HIPS Settings' interface



2. Make sure that all the check boxes are selected then click 'OK'

Advanced Settings

1. Enable the following settings in the 'Advanced' area of the HIPS Settings interface:



- Enable 'Block all unknown requests if the application is not running' (Optional) - Selecting this option blocks all unknown execution requests if Comodo Client 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 CCS security settings, then it is 'OK' to leave this box unchecked.

- Select 'Enable enhanced protection mode (Requires a system restart)' - If you are using a 64-bit system, in order to maximize the security, it is important to enable this mode to activate additional host intrusion prevention techniques in HIPS to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures.
- Because of limitations in Windows 7 x64, some HIPS functions in previous versions of CCS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS functionality.

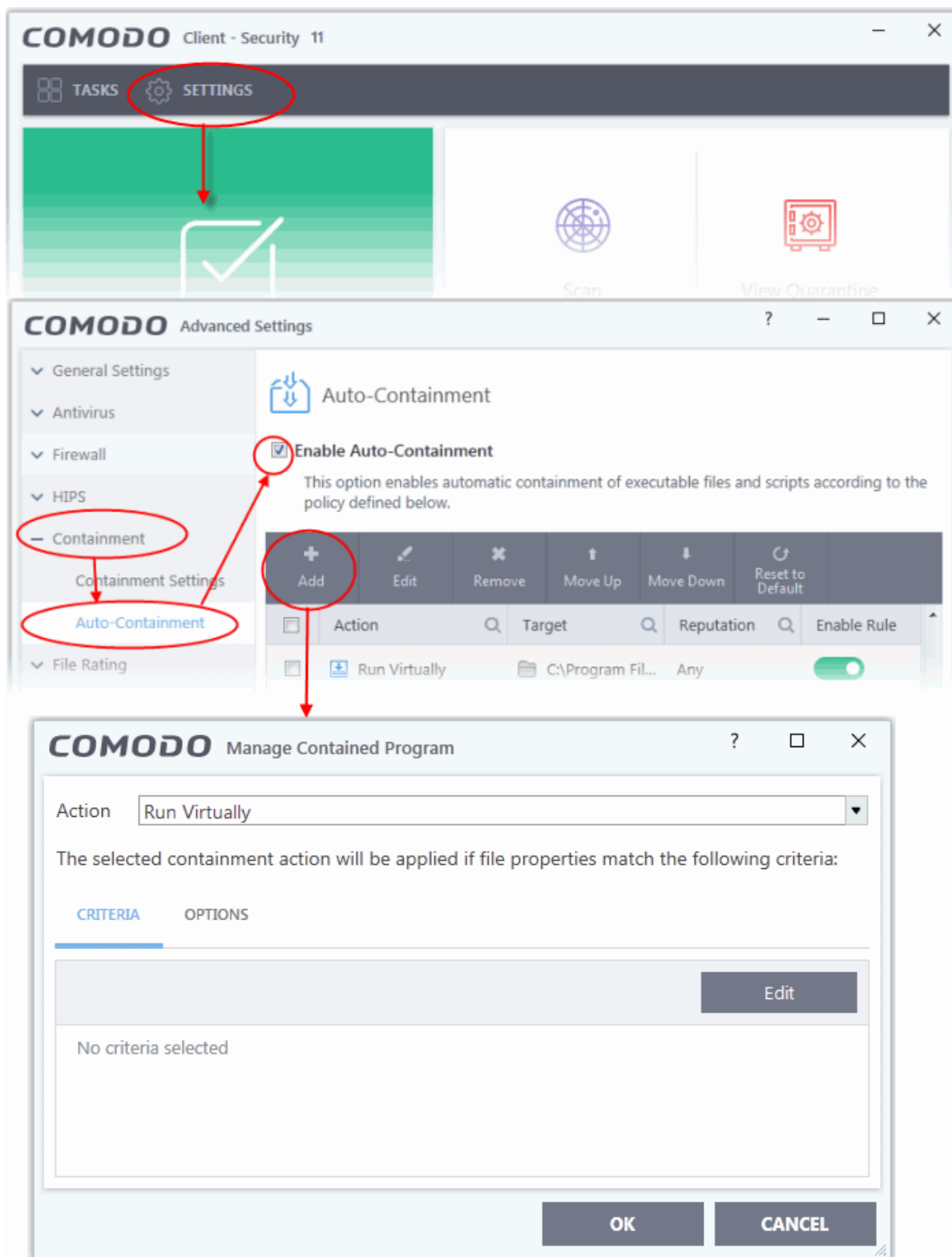
[Click here for more details on HIPS Settings](#)

Create Rules to Auto-Contain Applications

- Auto-containment rules let you determine whether programs should be blocked, ignored (allowed to run normally), run restricted, or run virtually (run in the container).
- You can contain files based on various criteria, including location and file source.
- A contained application cannot damage your computer because it is isolated from your operating system and your files.
- Comodo Client Security shows a green border around programs that are running in the container.
- CCS ships with a set of pre-defined auto-containment rules that are configured to provide maximum protection for your system.
- Before creating a rule, first check if your requirements are met by the default rules. See [Auto-Containment Rules](#) for more details.

To create auto-containment rules

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Containment' > 'Auto-Containment' on the left
3. Ensure that 'Enable Auto-Containment' is selected
4. Click 'Add'



The 'Manage Contained Program' dialog will open. It contains two tabs:

- **Criteria** - Allows you to define conditions upon which the rule should be applied
- **Options** - Allows you to configure additional actions like logging, memory usage and execution time restrictions

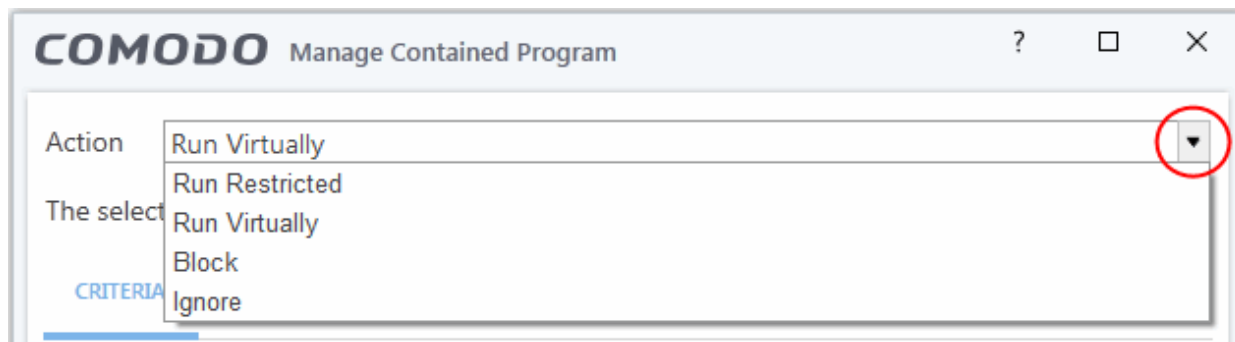
You can create new containment rules from the 'Manage Contained Program' interface in three steps:

- **Step 1 - Choose the action**

- **Step 2 - Select the target file/group and set the filter criteria for the target files**
- **Step 3 - Select the options**

Step 1 - Select the Action

The 'Action', in combination with the restriction level in the 'Options' tab, determine the privileges an auto-contained application has to access other resources on your computer.



The options available in 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 limited operating system resources. The application is not allowed to execute more than 10 processes at a time and has few access rights. Some applications, like computer games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be contained and allowed to run with all privileges.
- Choose the action from the options.

Step 2 - Select the target file/group and set the filter criteria for the target files

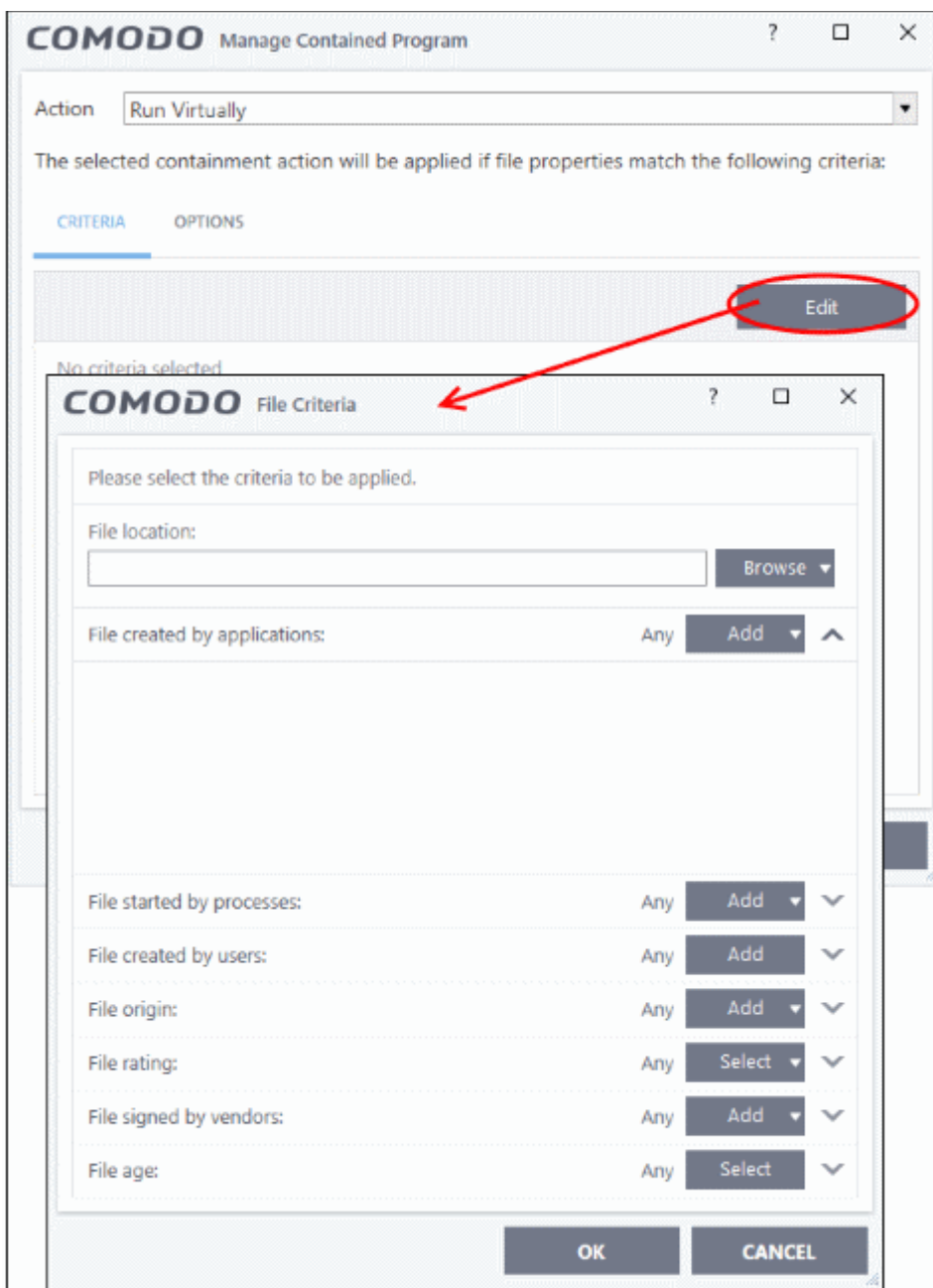
- The next step is to select the targets and configure filter parameters.
- You can apply filters to a target so the action applies only to specific files. For example, you can specify 'All executables' as the target and add a filter so it only affects executables downloaded from the internet.
- Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target and 'File created by specific user' as the filter criteria.

To select the target and set the filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- To add new target and filter criteria, click the 'Edit' button at the far right

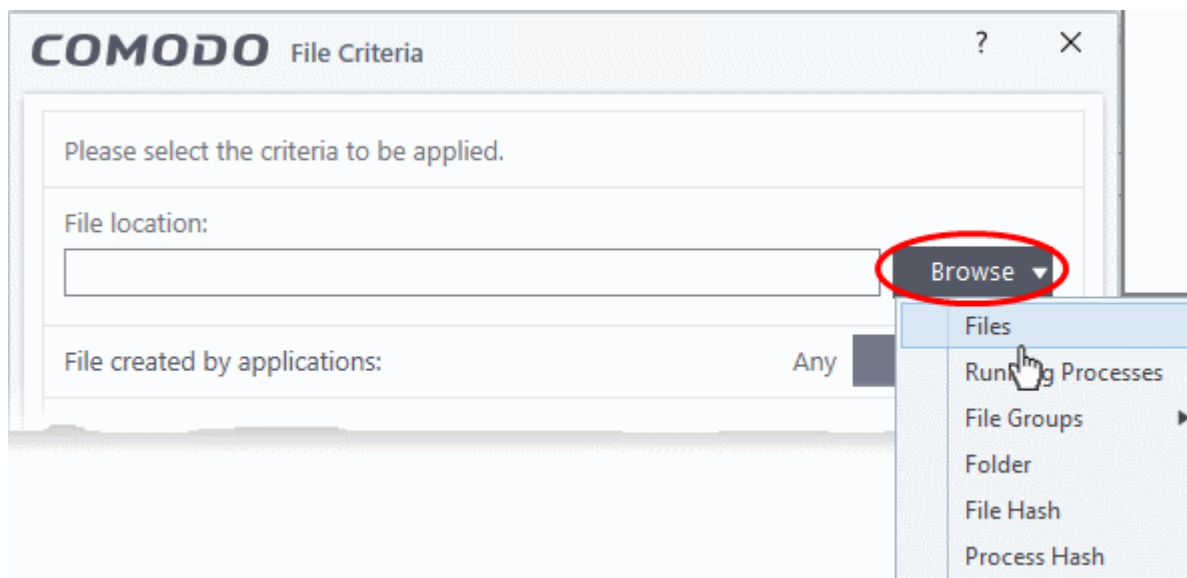


The 'File Criteria' dialog will open. The file criteria dialog allows you:

- **Select the target**
- **Configure the filter criteria**

Select the target

- To select the target, click the 'Browse' button beside the 'File Location' field

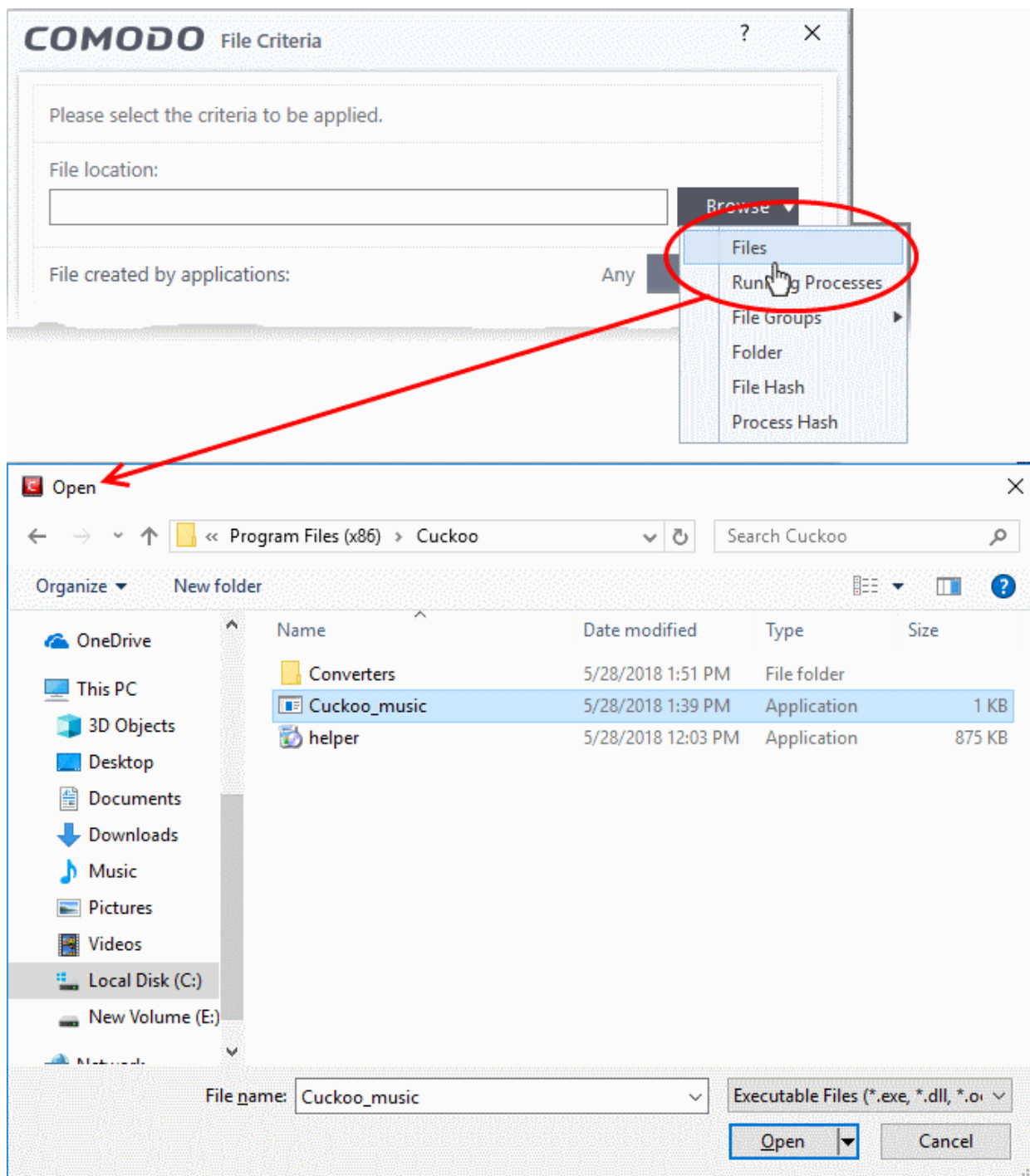


You have six options available to add the target path:

- **Files** - Allows you to add individual files as target.
- **Running Processes** - As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** - Allows to add predefined File Groups as target. To add or modify a predefined file group see **File Groups** for more details.
- **Folder** - Allows you to add a folder or drive as the target
- **File Hash** - Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

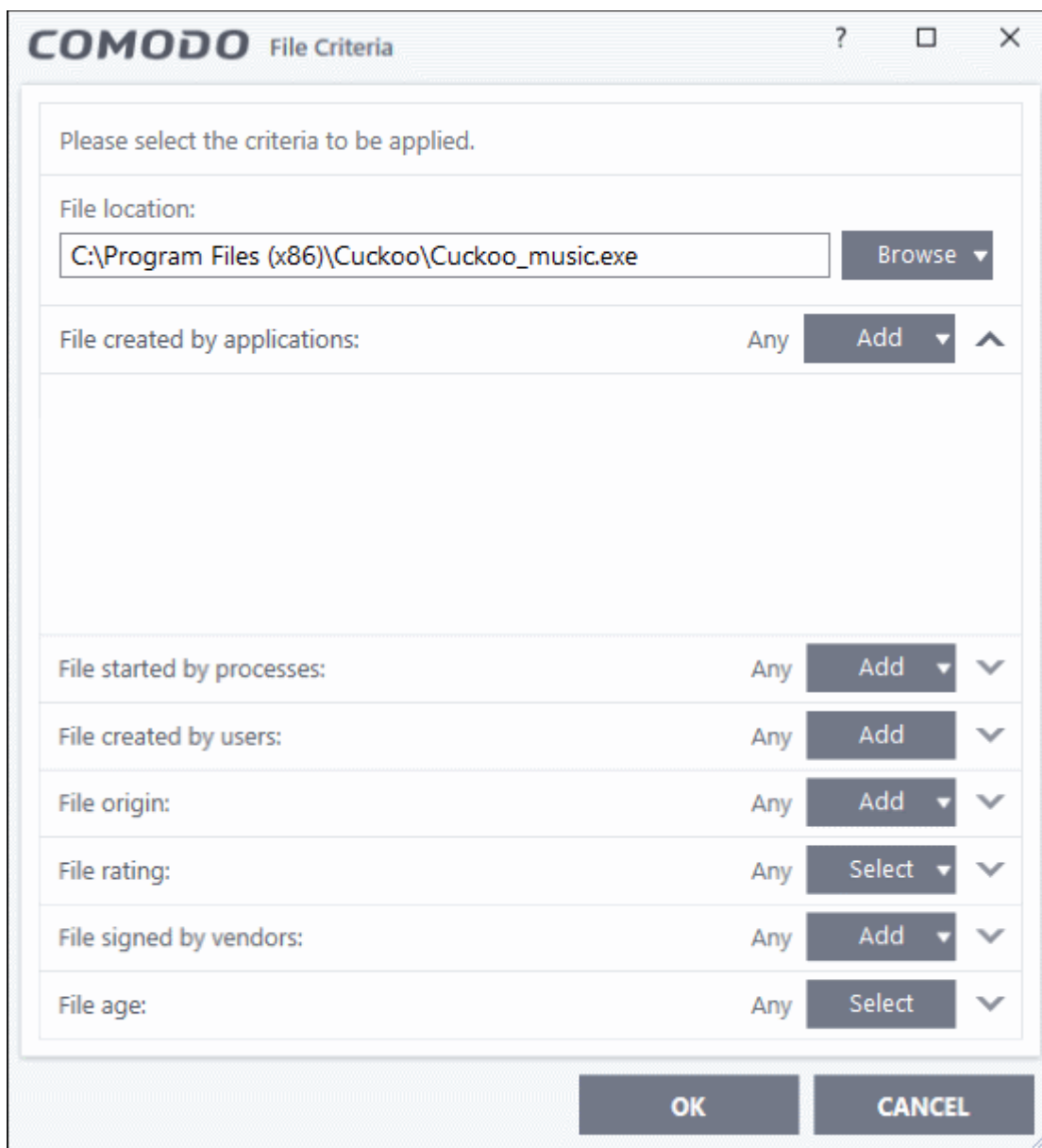
Add an individual File

- Choose 'Files' from the 'Browse' drop-down.



- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'

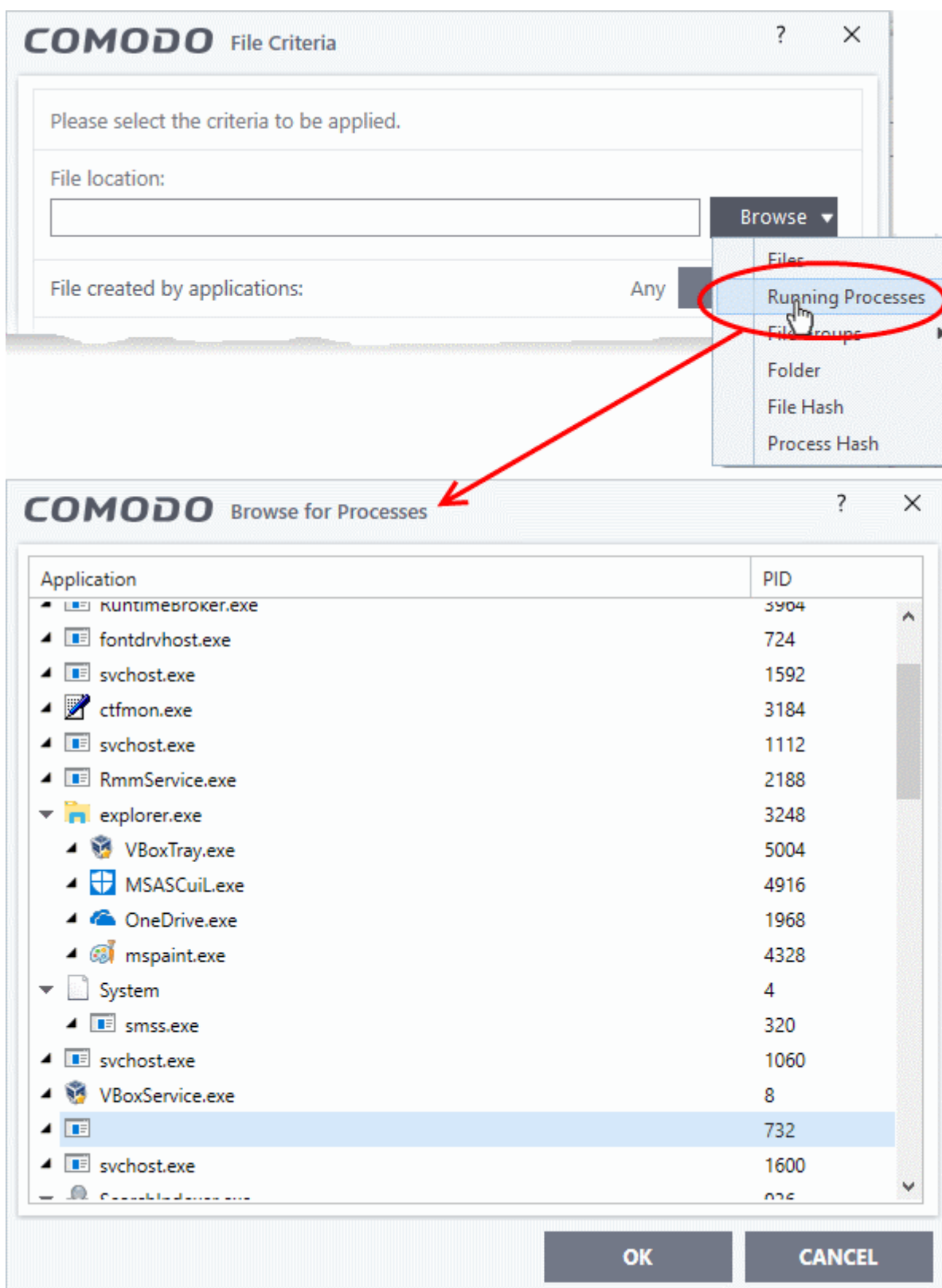
The file will be added as target and will be run as per the action chosen in **Step 1**.



- If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'.
- The default values for filter criteria and file rating will be 'Any', and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

Add a currently running application by choosing its process

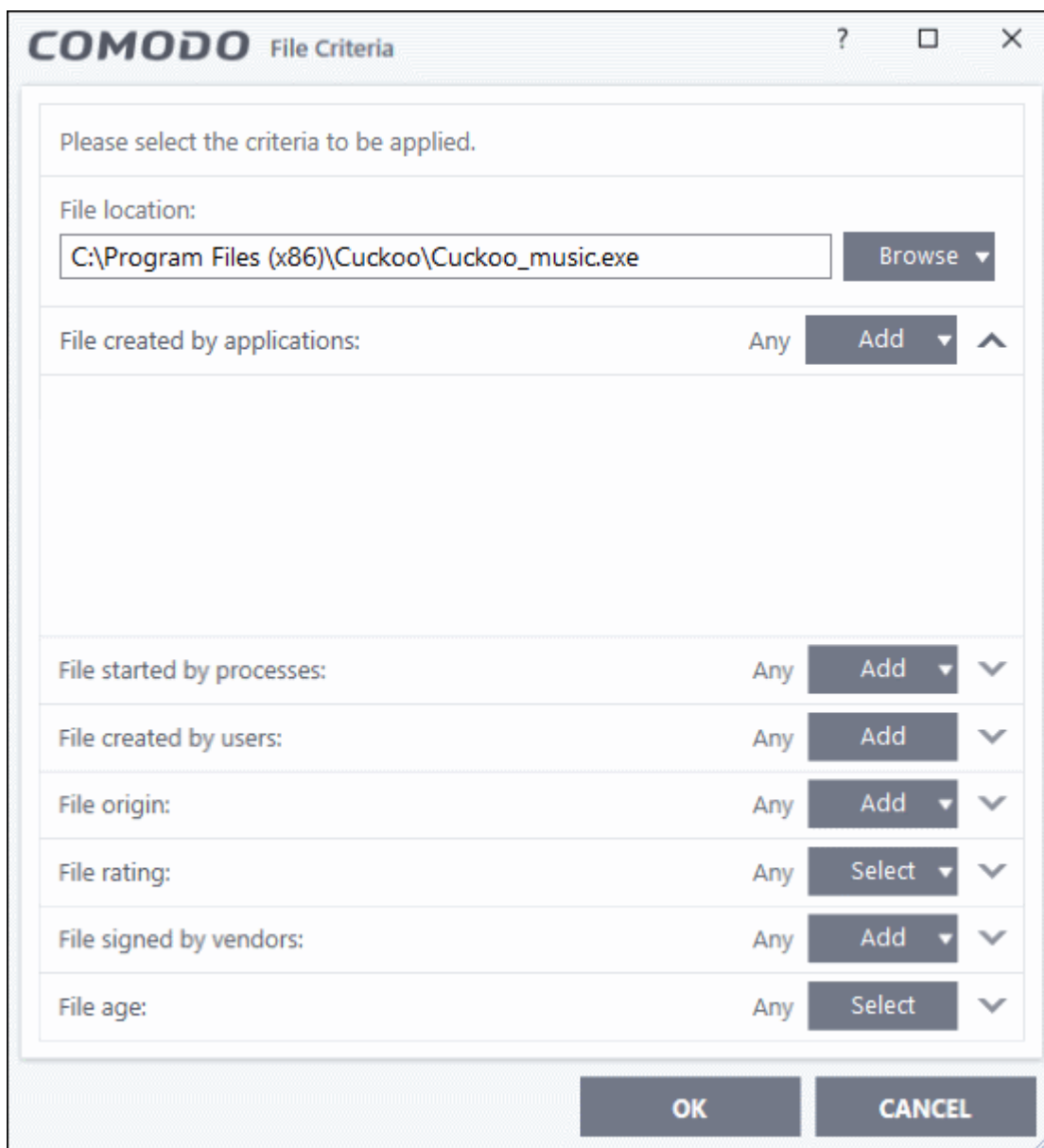
- Choose 'Running Processes' from the 'Browse' drop-down



This will open a list of all processes running on your computer.

- Select the process you want to add as a target and click 'OK'.

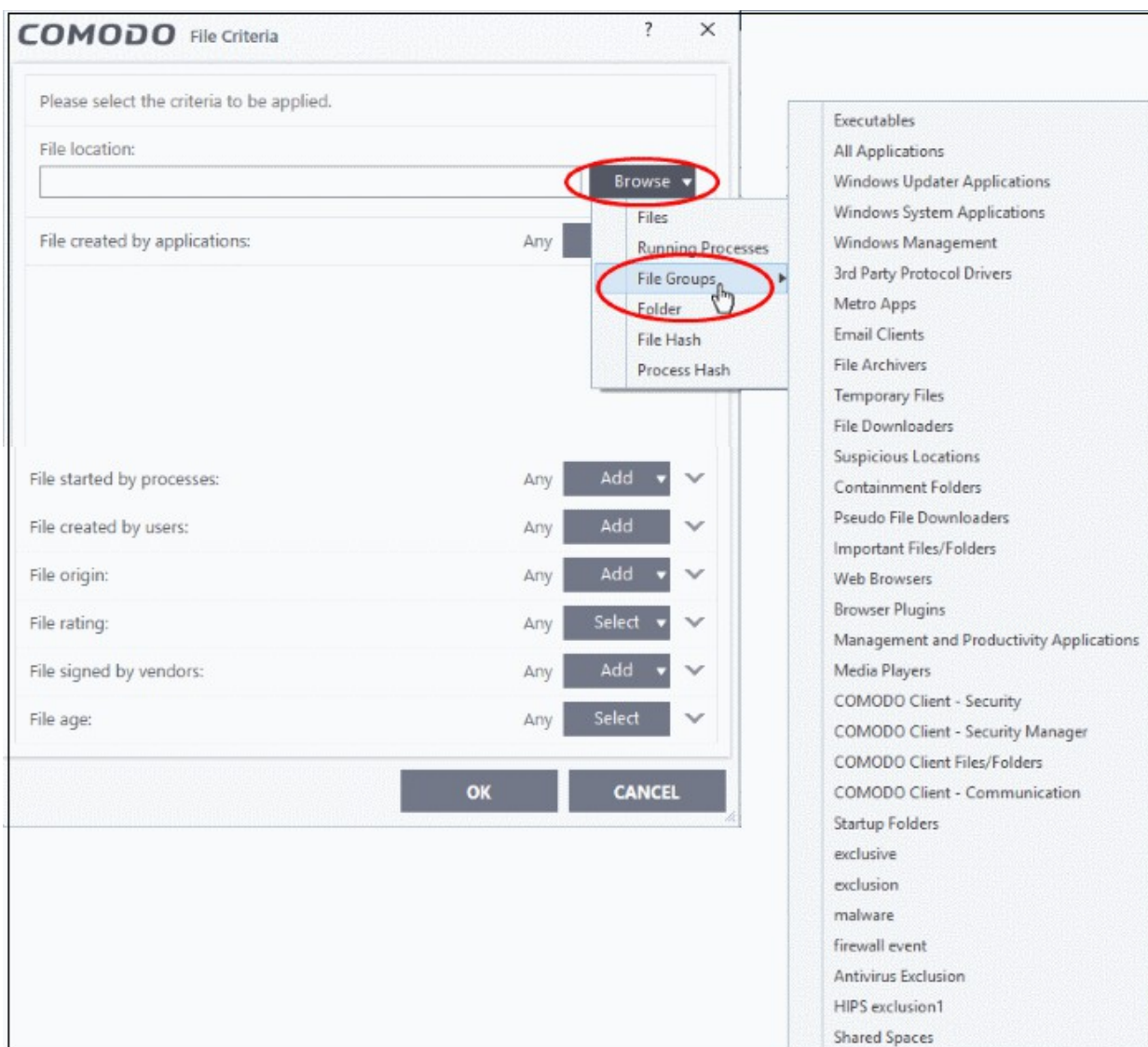
The file will be added as the target. The action chosen in **Step 1** will be applied to the process.



- If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'.
- The default values for filter criteria and file rating will be 'Any', and for 'Options' it will be 'Log when this action is performed'. If required you can **configure filter criteria and file rating** and **Options** for the rule.

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



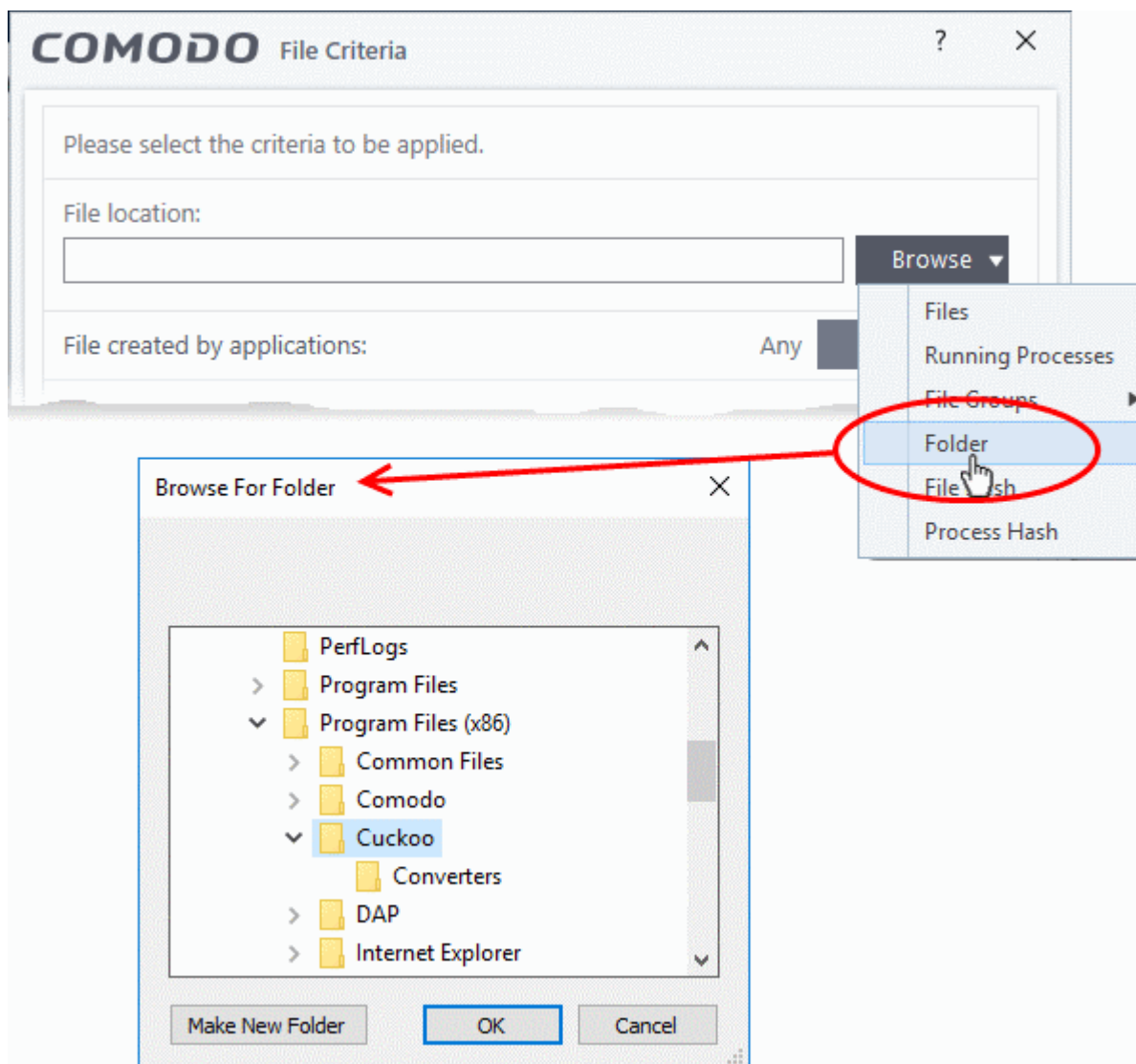
- Select the file group from the drop-down.

The file group will be added as target and will be run as per the action chosen in **Step 1**.

If you just want to add the applications for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for 'filter criteria' and 'file rating' will be 'Any'. For 'Options' it will be 'Log when this action is performed'. If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Add a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.



The 'Browse for Folder' dialog will appear:

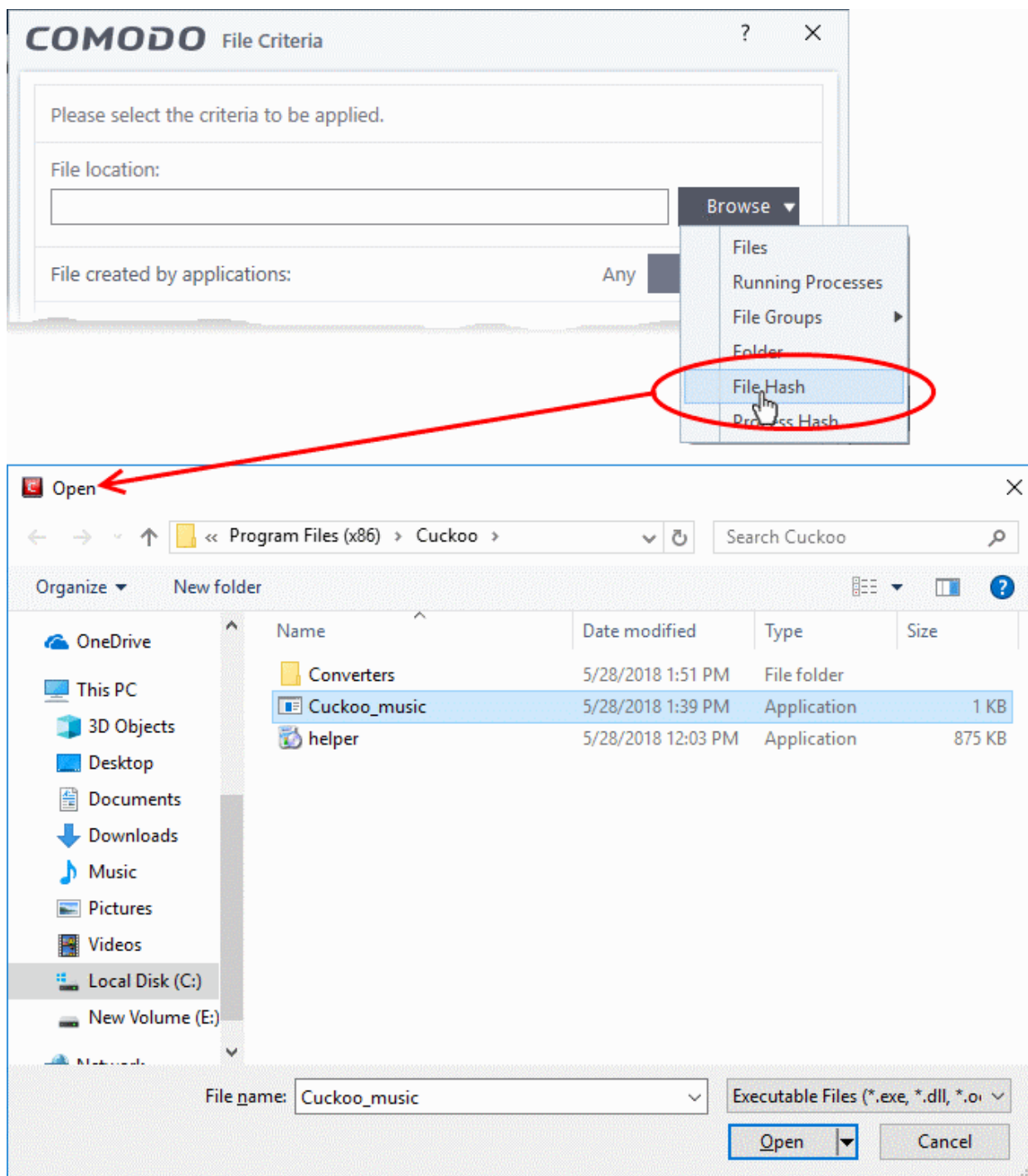
- Navigate to the drive partition or folder you want to add as target and click 'OK'

The drive partition/folder will be added as the target. All executable files in the folder will be run as per the action chosen in **Step 1**.

If you just want to add the application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'. If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Add a file based on its hash value

- Choose 'File Hash' from the 'Browse' drop-down.



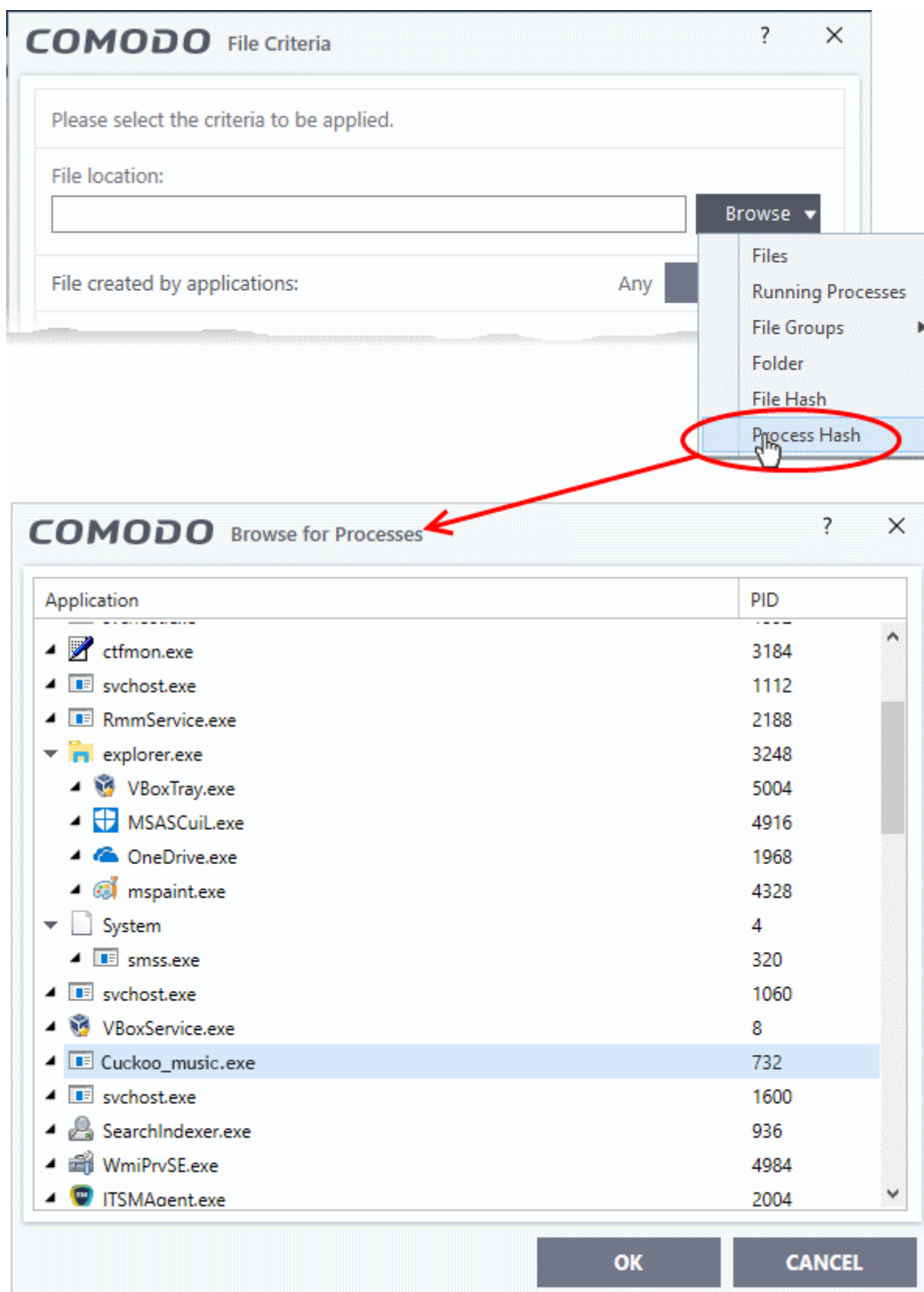
- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'

The file will be added as target and will be run as per the action chosen in **Step 1**.

If you want to add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for 'filter criteria' and 'file rating' will be 'Any'. For 'Options' it will be 'Log when this action is performed'. If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Add an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



This will open a list of all processes running on your computer.

- Select the process whose hash you want to add as a target and click 'OK'.

The hash value of the parent executable will be added as the target. The action chosen in **Step 1** will be applied when CCS detects a program with this hash.

If you just want to add an application for a particular action as selected in **Step 1** without specifying any filters or

options, then click 'OK'. The default values for 'filter criteria' and 'file rating' will be 'Any'. For 'Options' it will be 'Log when this action is performed'. If required, you can **configure filter criteria and file rating** and **Options** for the rule.

Configure the Filter Criteria and File Rating

You can apply an action to a file if the file's properties match certain criteria.

The available filter criteria are:

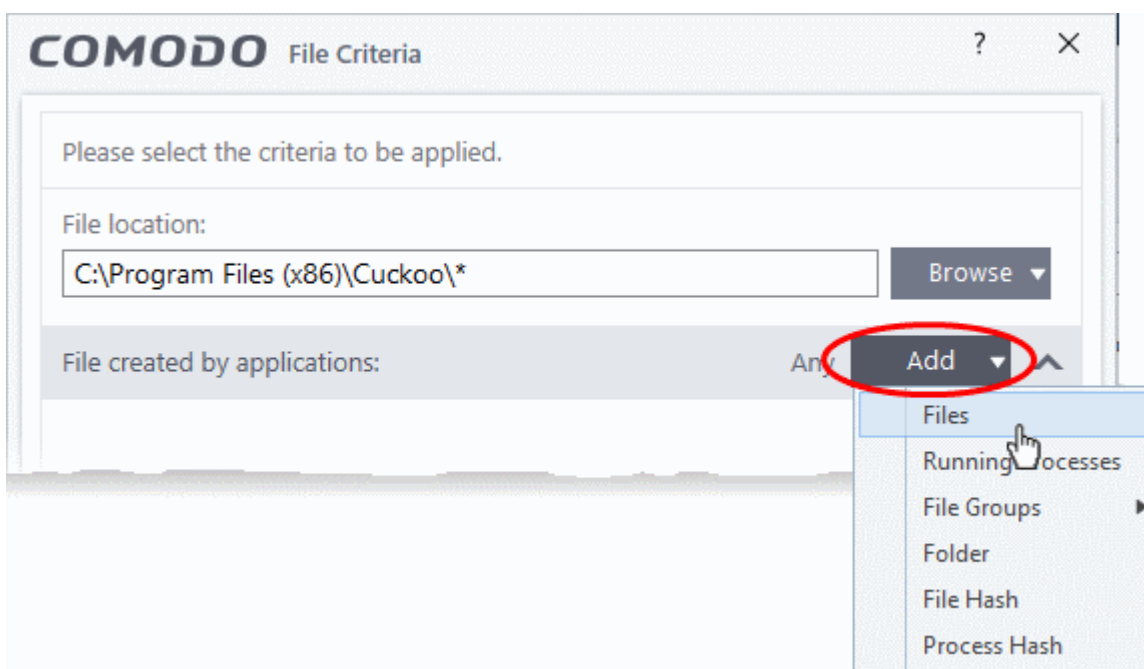
- **Application(s) that created the file**
- **Process(es) that created the file**
- **User(s) that created the file**
- **The origin from which the file was downloaded**
- **The file rating**
- **The file signed by vendors**
- **The age of the file**

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)

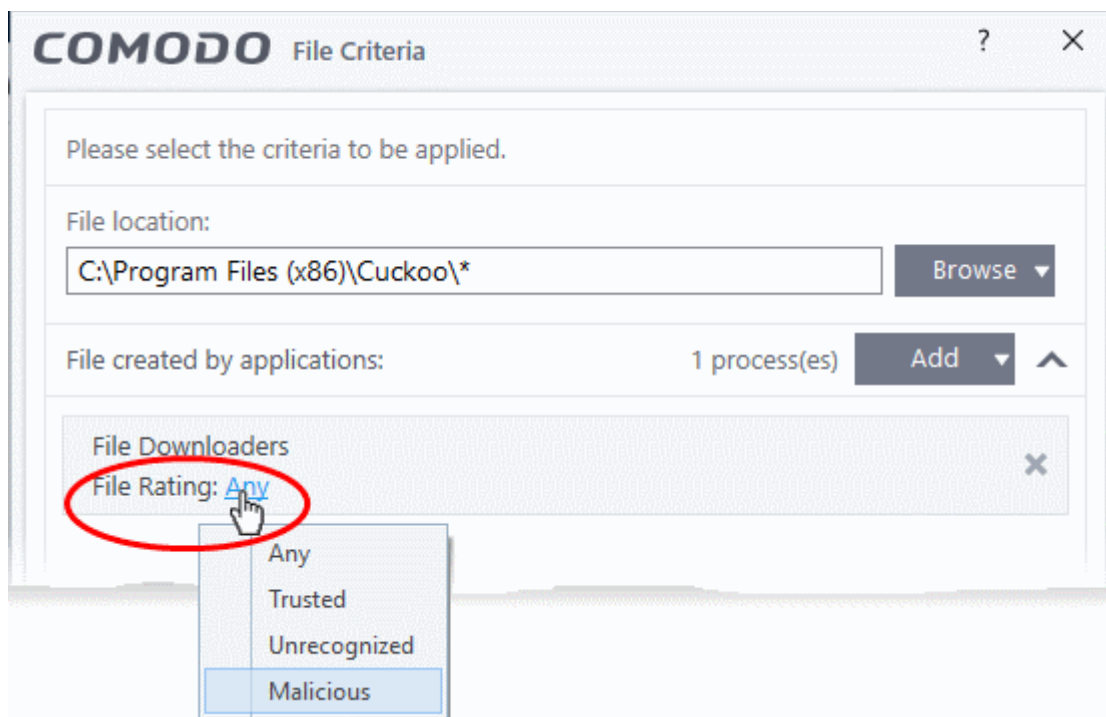
- Click the 'Add' button in the 'File Created by applications' stripe.



- 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



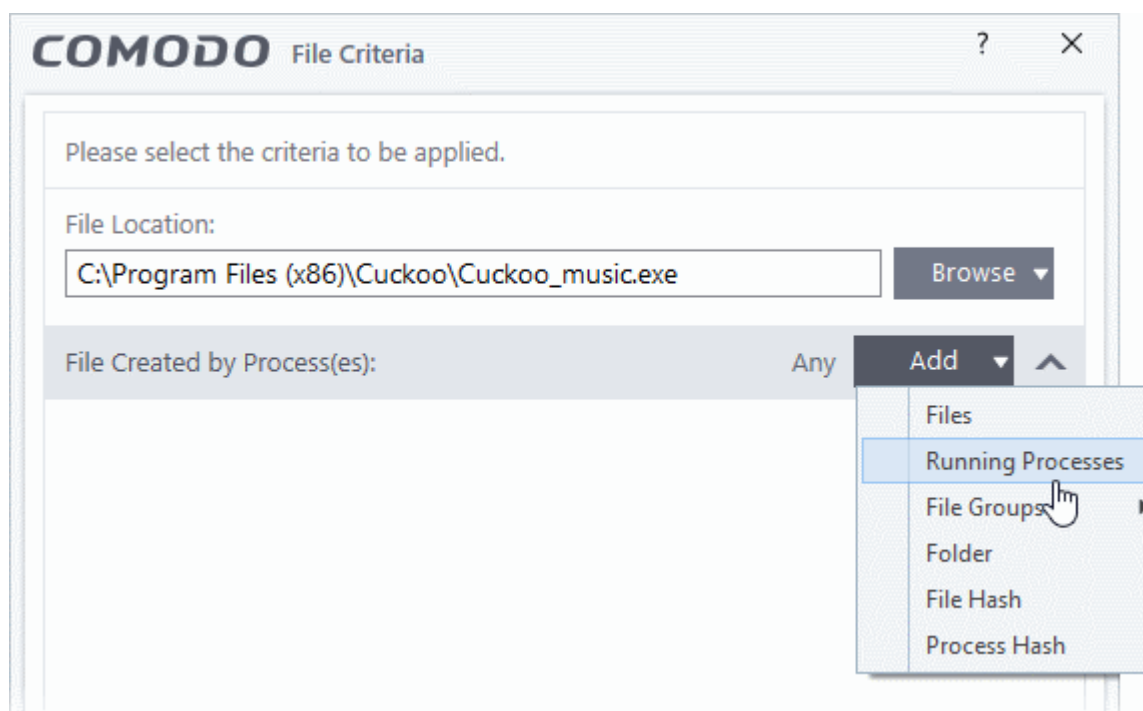
- Repeat the process to add more applications or groups/folders.

Auto-contain a File if it was Created by a Specific Process

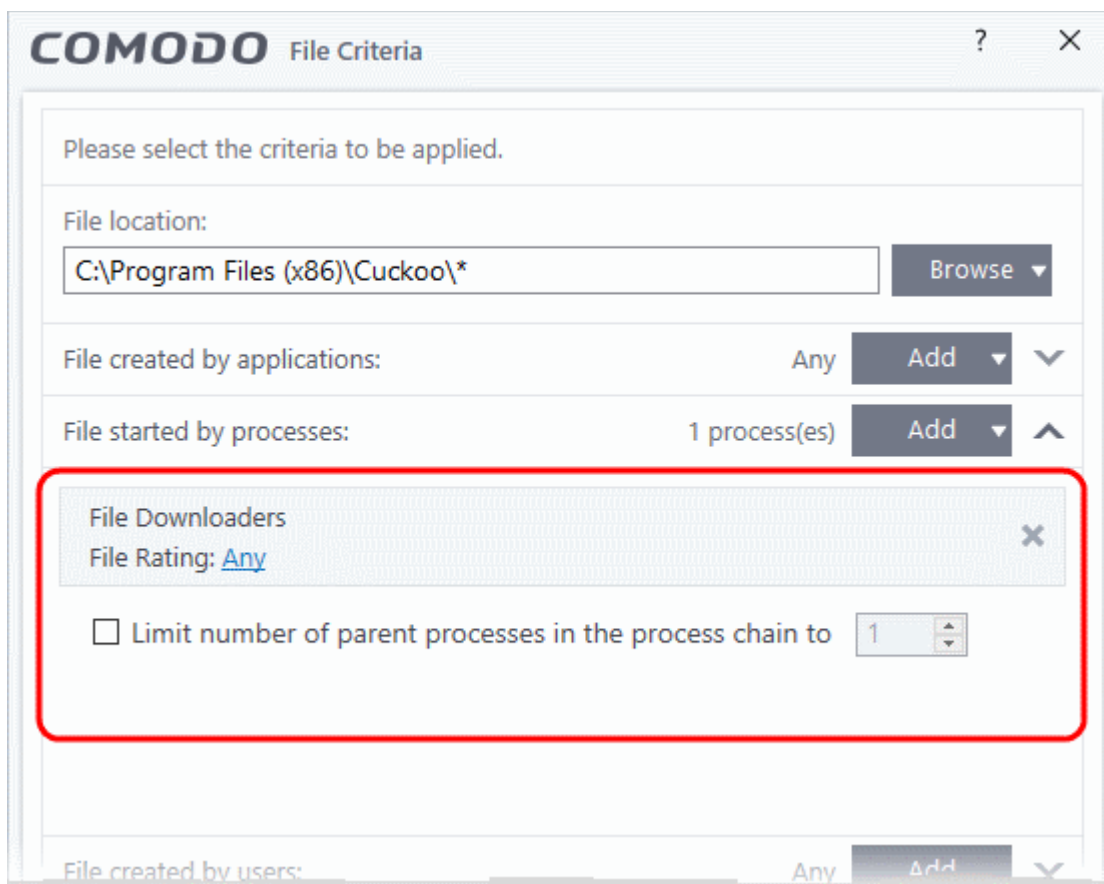
- You can create a filter to apply an action to a file based on its source process.
- Optionally, you can also specify:
 - The file rating of the source. The rule will then only contain a file if its parent process has a certain trust rating.
 - The number of levels in the process chain that should be inspected.

To specify source process(es)

- Click the 'Add' button in the 'File Created by Process(es)' stripe.

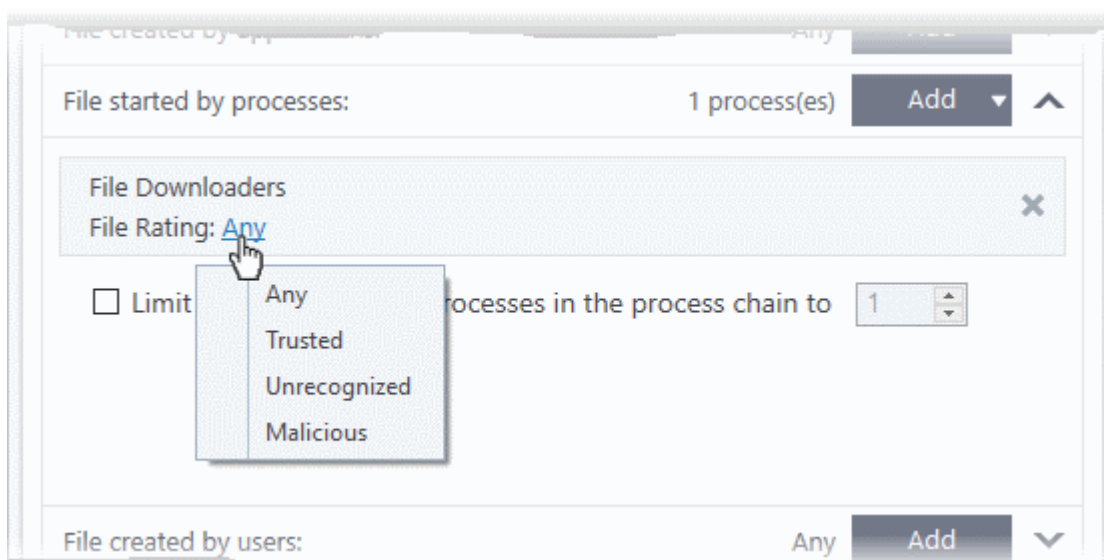


- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.



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



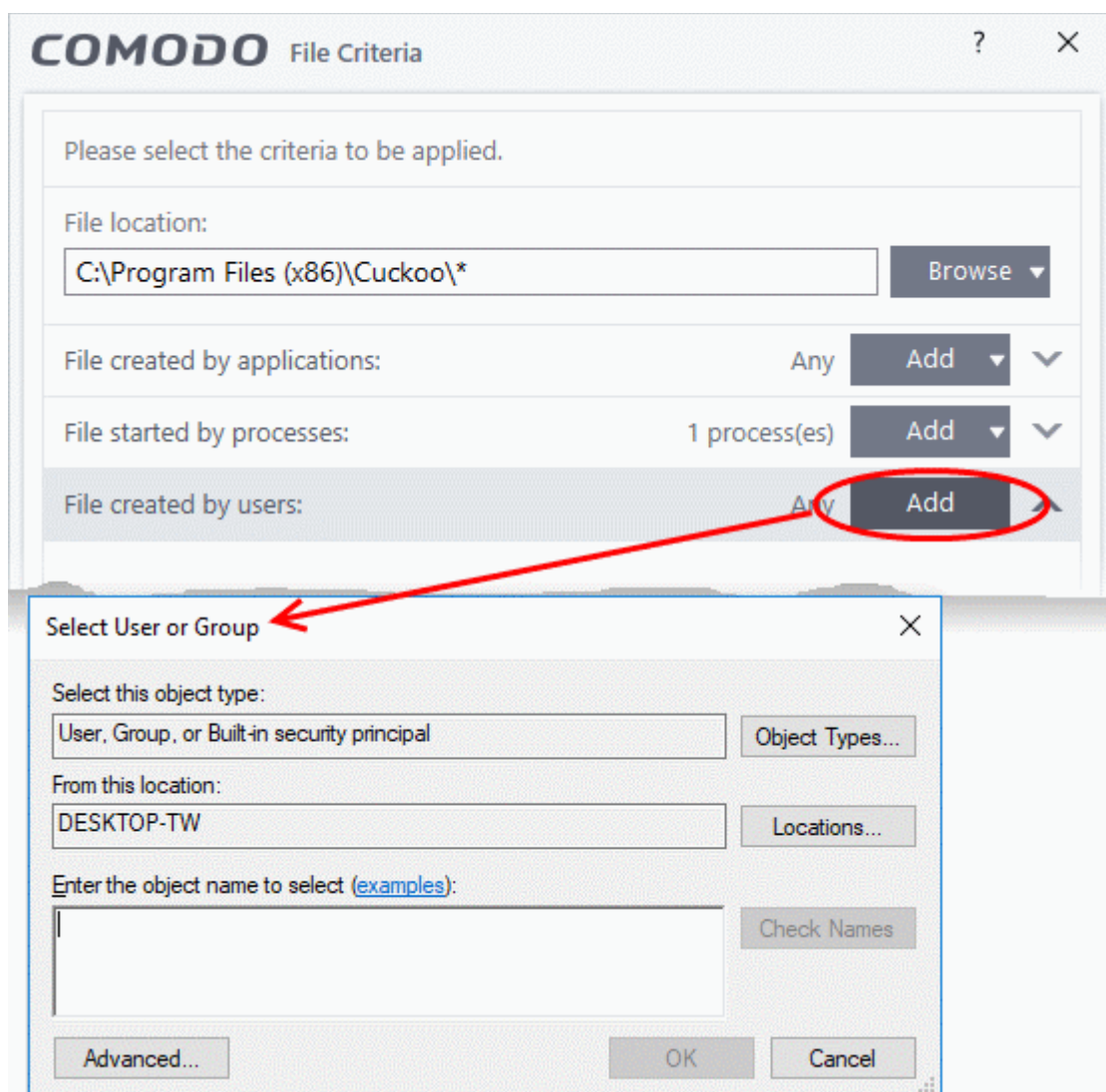
- **'Limit number of parent process(es) in the process chain to'** - Specify how far up the process tree CCS should check when inspecting the file's sources. 1 = will only check the file's parent process. 2 = will check the parent process and the grand-parent process, etc., etc.



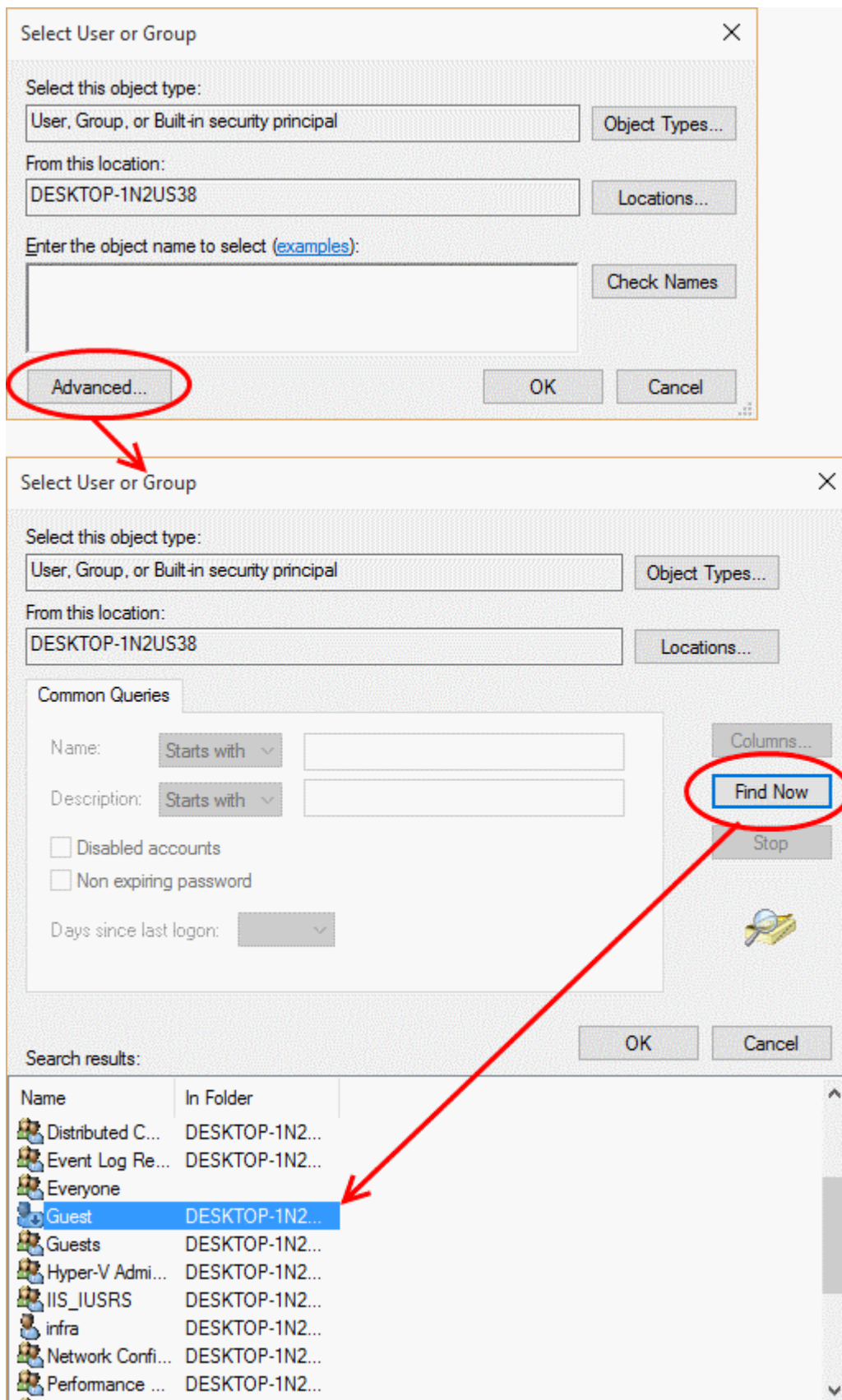
- Repeat the process to add more process(es)

Auto-contain a file if it was created by specific user(s)

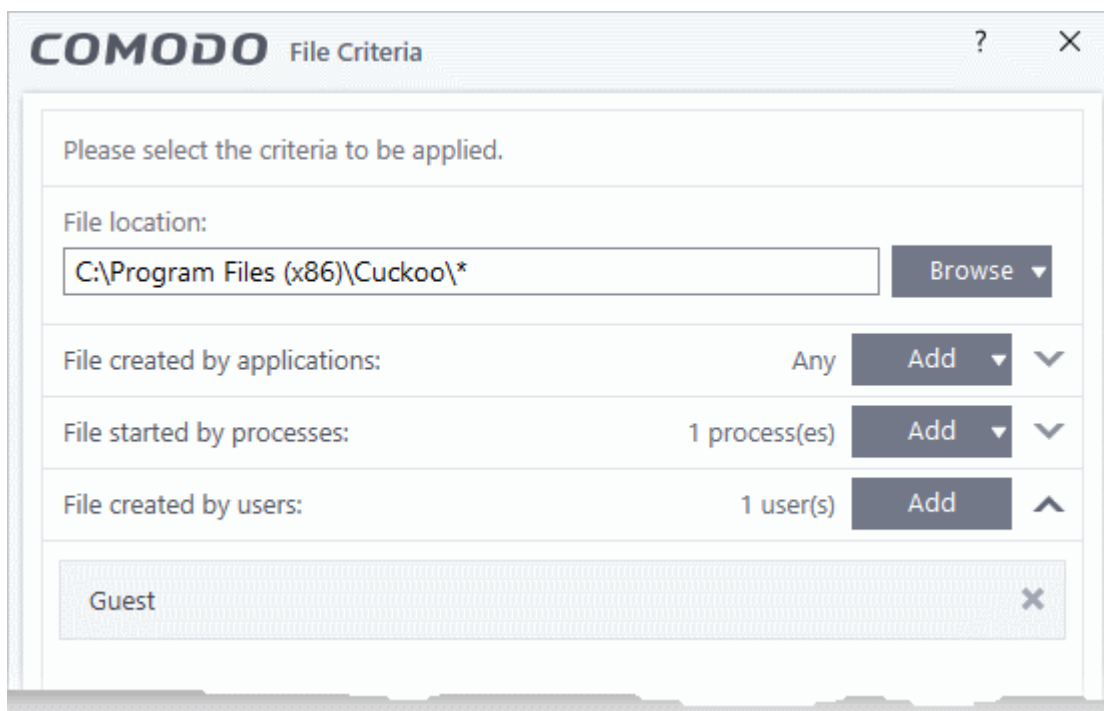
- Click the 'Add' button in the 'File Created by User(s)' stripe.



- The 'Select User or Group' dialog will appear.
 - Type the names of the users to be added to the rule. 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.



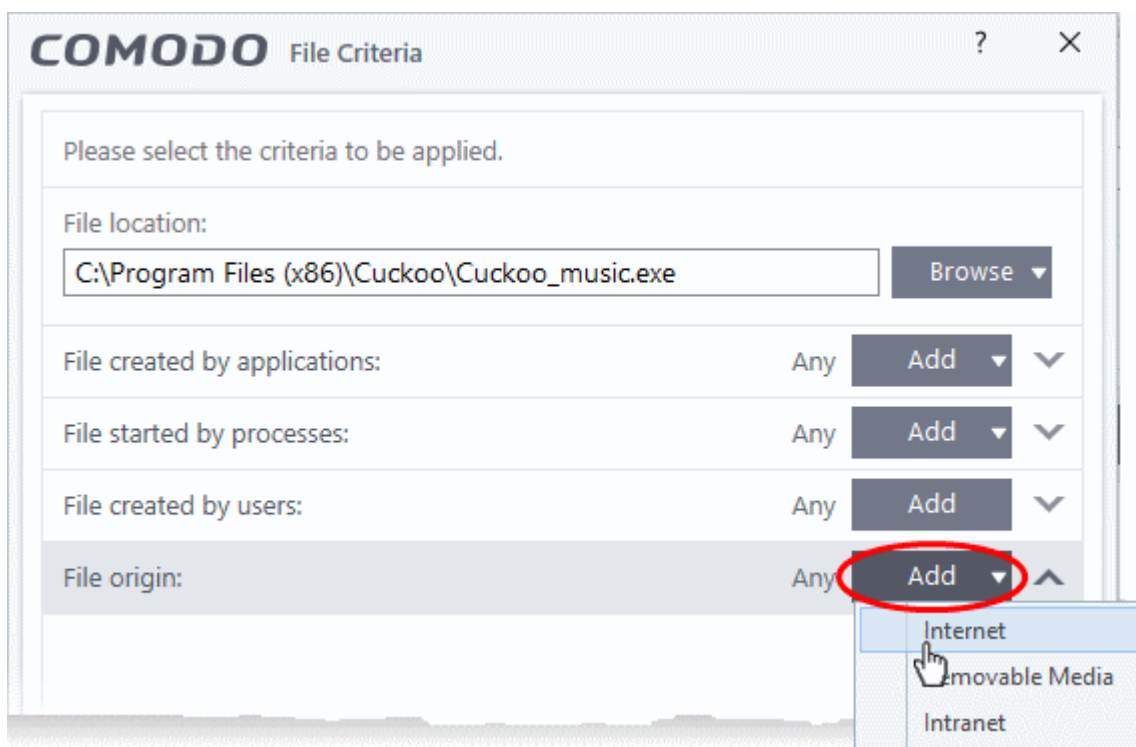
The user will be added to the list.



- 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(s)' stripe.
- Choose the source from the options:



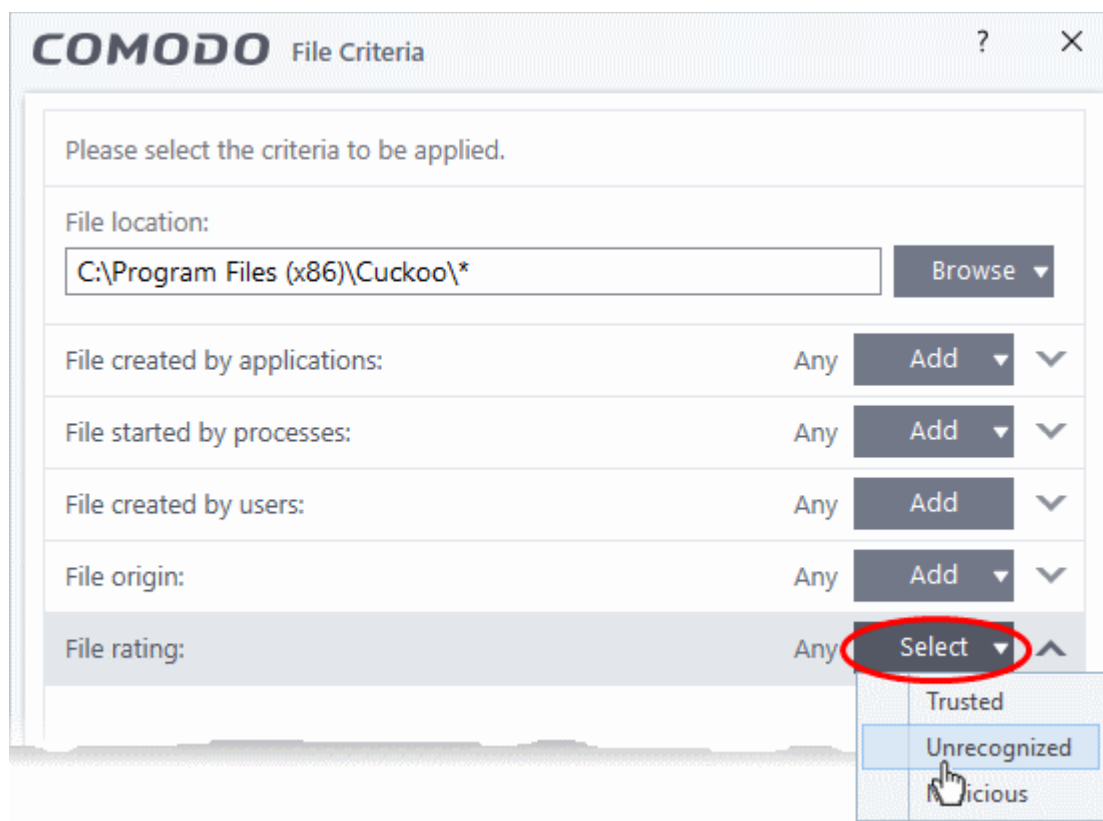
- Internet - The rule will only apply to files that were downloaded from the internet.
- Removable Media - The rule will only apply to items copied to the computer from removable

devices like a USB drive, CD/DVD or external storage.

- 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

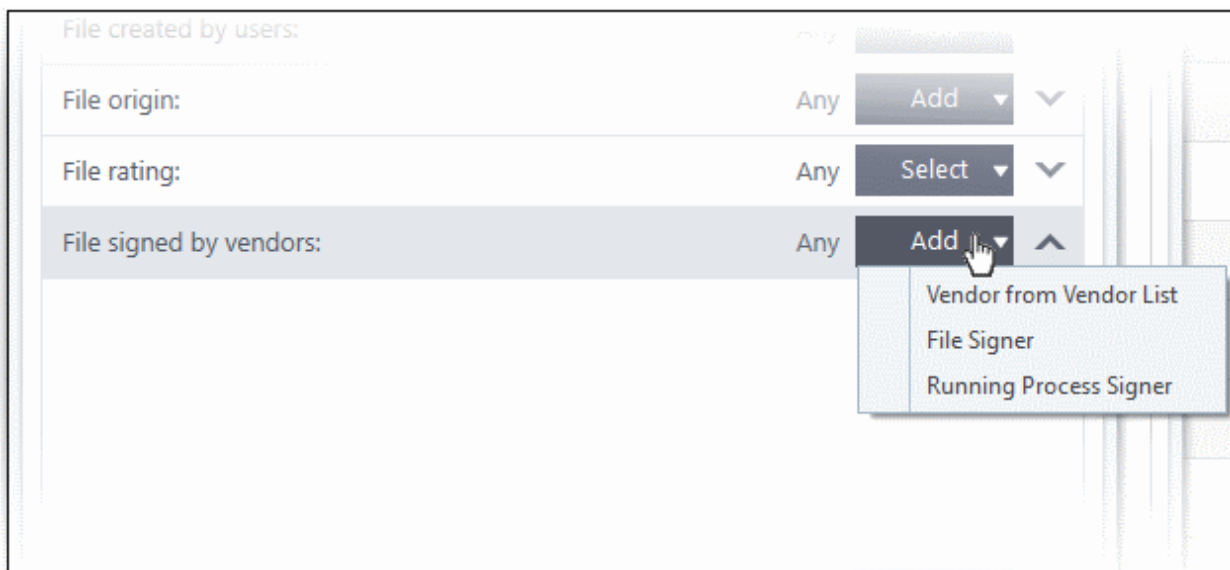
- Click the 'Select' button in the 'File Rating' stripe



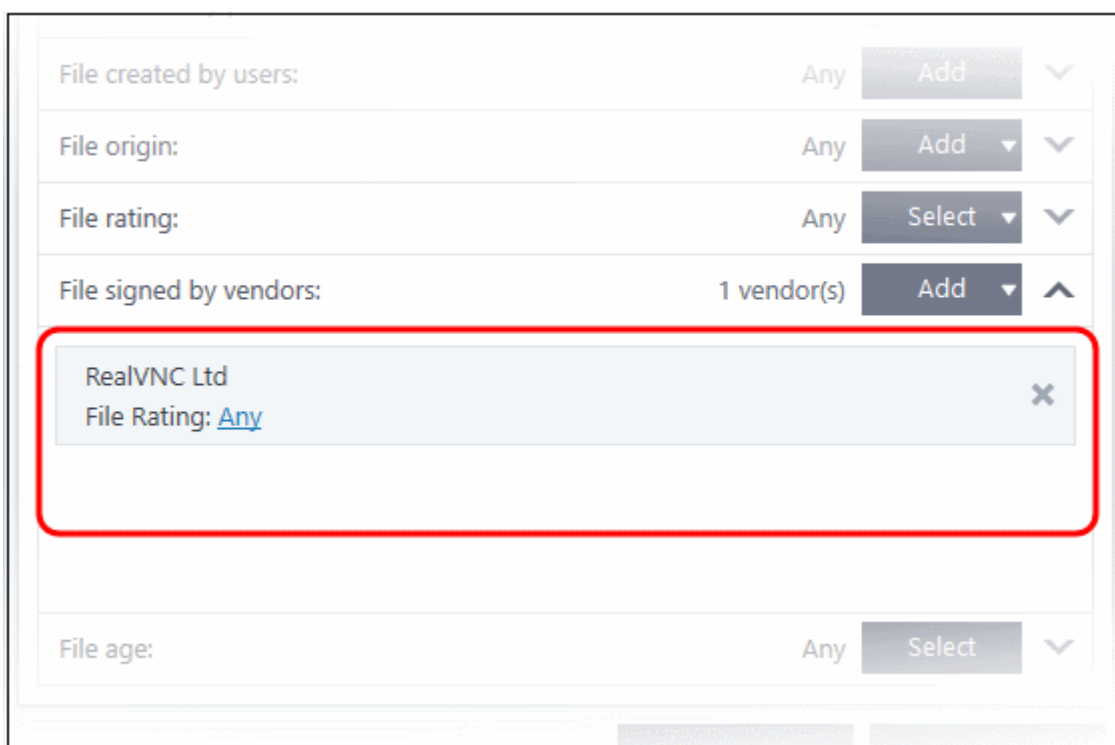
- Choose the source from the options:
 - **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by CCS. See [File Rating Settings](#) for more information.
 - **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. See [File List](#) for more information.
 - **Malicious** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. See [Unknown Files - The Scanning Process](#) for more information.
- Repeat the process to add more file ratings

Auto-contain a file based on software vendor

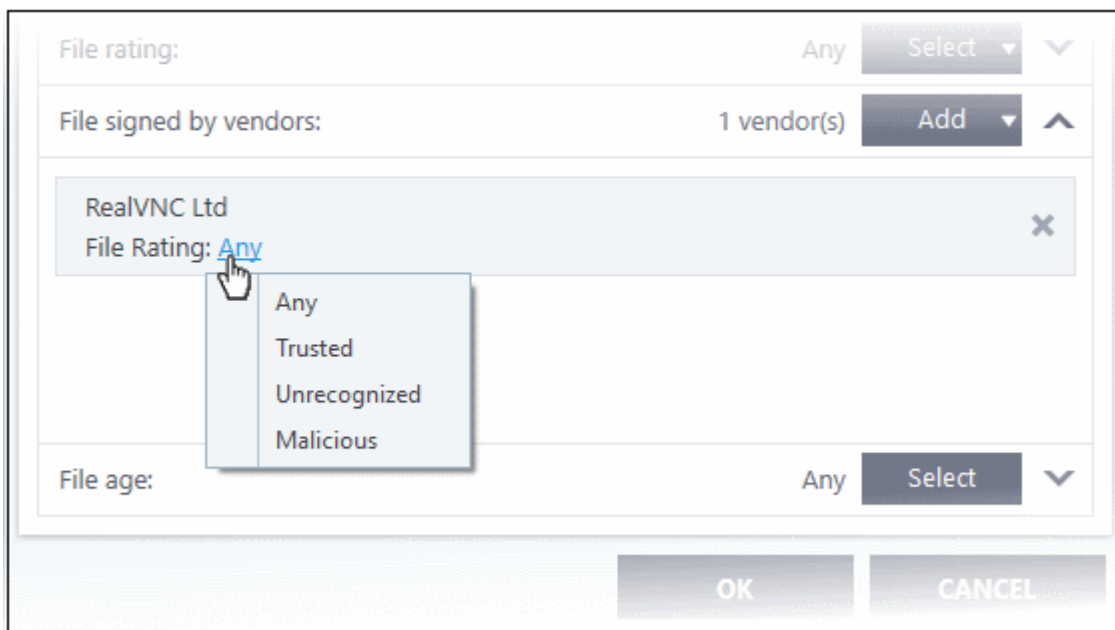
- Click the 'Add' button in the 'File signed by vendors' stripe.



- Choose the software vendor source from the options
 - **Vendor from Vendor List** - Select a vendor from the list to contain all files by a specific publisher. See **'Vendor List'** for more information about managing software vendors.
 - **File Signer** - Browse to the file location, select the file and click open. The software vendor of the file will be added as a filter criteria.
 - **Running Process Signer** - Click this and in the 'Browse for Processes' dialog, select the process and click 'OK'. The software vendor of the file that created the process will be added as a filter criteria.



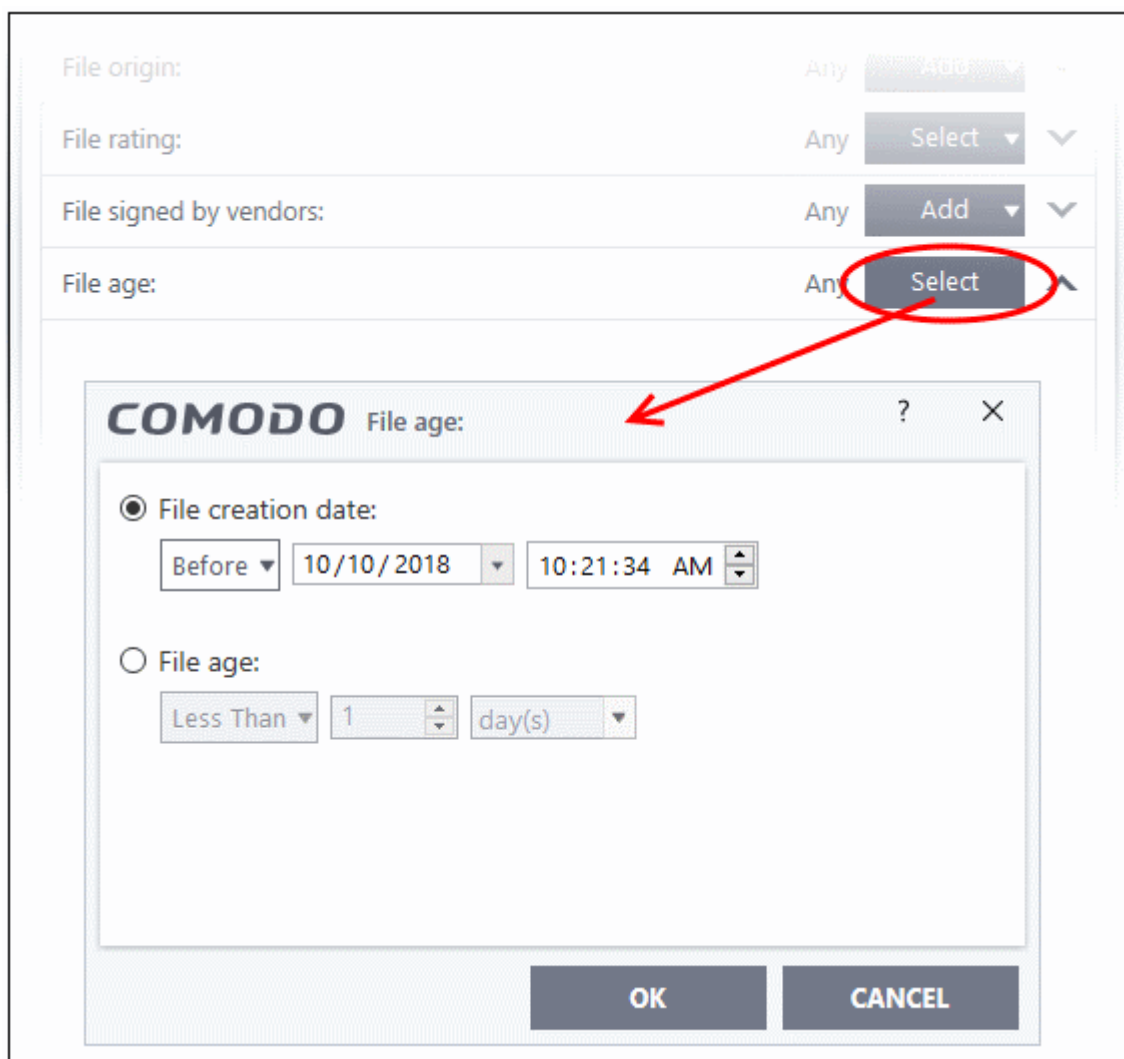
- Click the 'Any' link beside 'File Rating' and select the file rating of the source



- Repeat the process to add more vendors

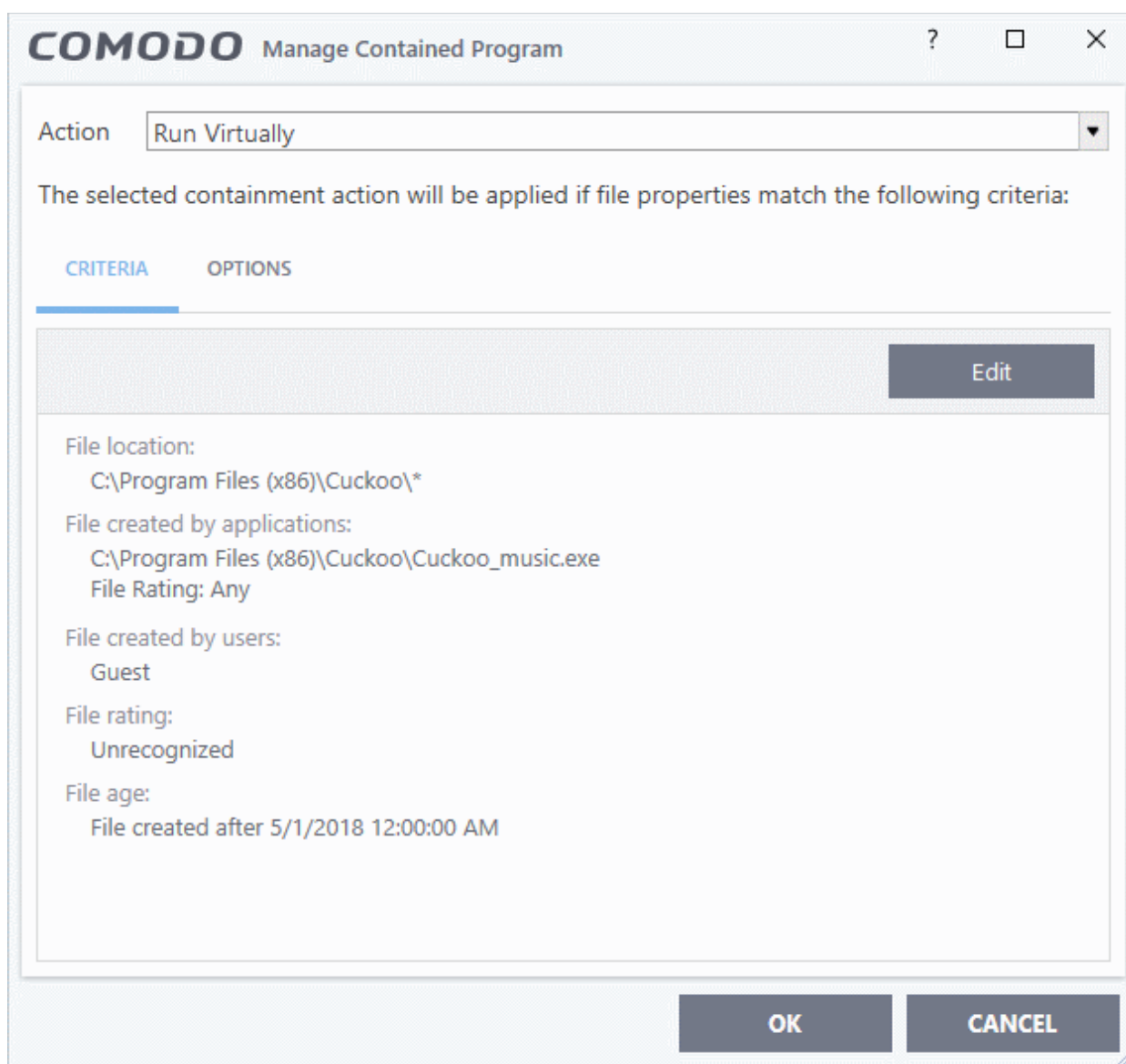
Set the file age as filter criteria

- 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** - CCS 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** - CCS 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.

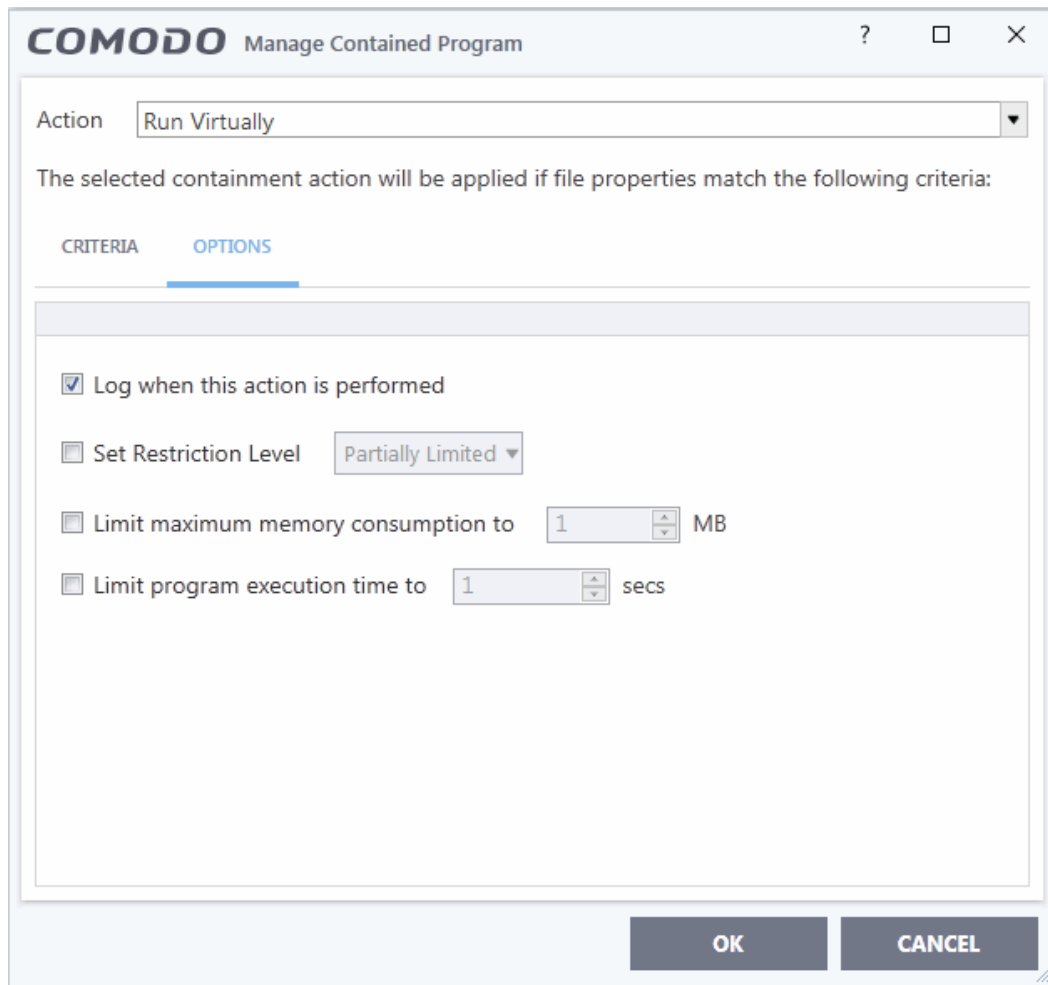


Step 3 - Select the Options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

To select the options

- Click the 'Options' tab.



The options will be displayed, depending on the 'Action' chosen in **Step 1**.

The options available for 'Ignore' action are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be added to CCS Containment logs.
- **Don't apply the selected action to child processes** - Child processes are those initiated by a parent application. Unwanted child processes can include launching another app or third party browser plugin. CCS treats all child processes as individual processes and forces them to run as per the file rating and the Containment rules.
 - By default, this option is not enabled and the 'Ignore' rule will also apply to child process of the target application(s).
 - If this option is enabled then the 'Ignore' rule will be applied only to the target application. Any child processes will be checked and Containment rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the 'Ignore' action only.

The options available for 'Run Restricted' and 'Run Virtually' actions are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Set Restriction Level** - When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
 - **Partially Limited** - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. **(Default)**
 - **Limited** - Only selected operating system resources can be accessed by the application. The

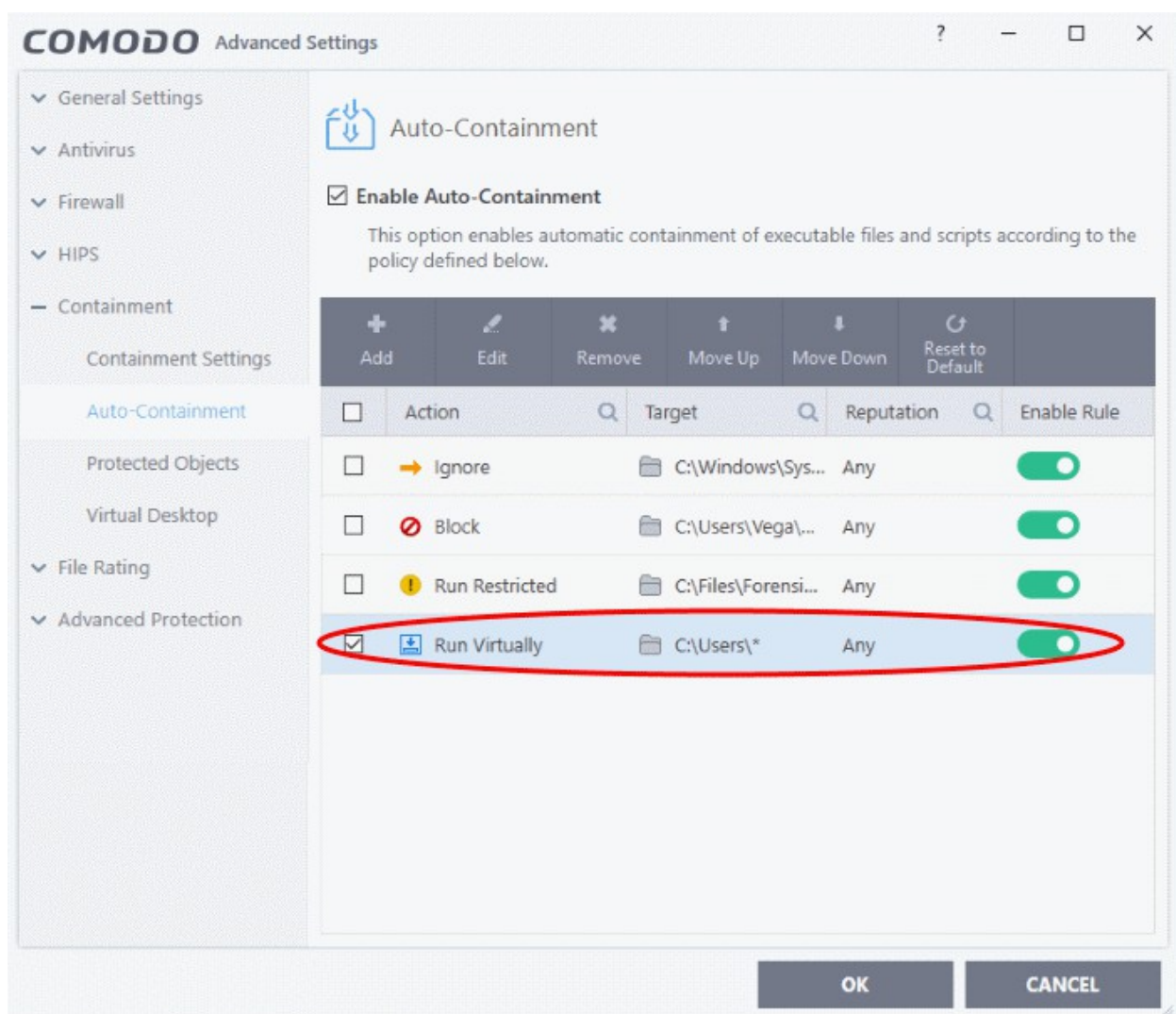
application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.

- **Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Untrusted** - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
- **Limit maximum memory consumption to** - Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** - Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For 'Block' action, the following options are available:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Quarantine program** - If checked, the programs will be automatically quarantined. See [Manage Quarantined Items](#) for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.

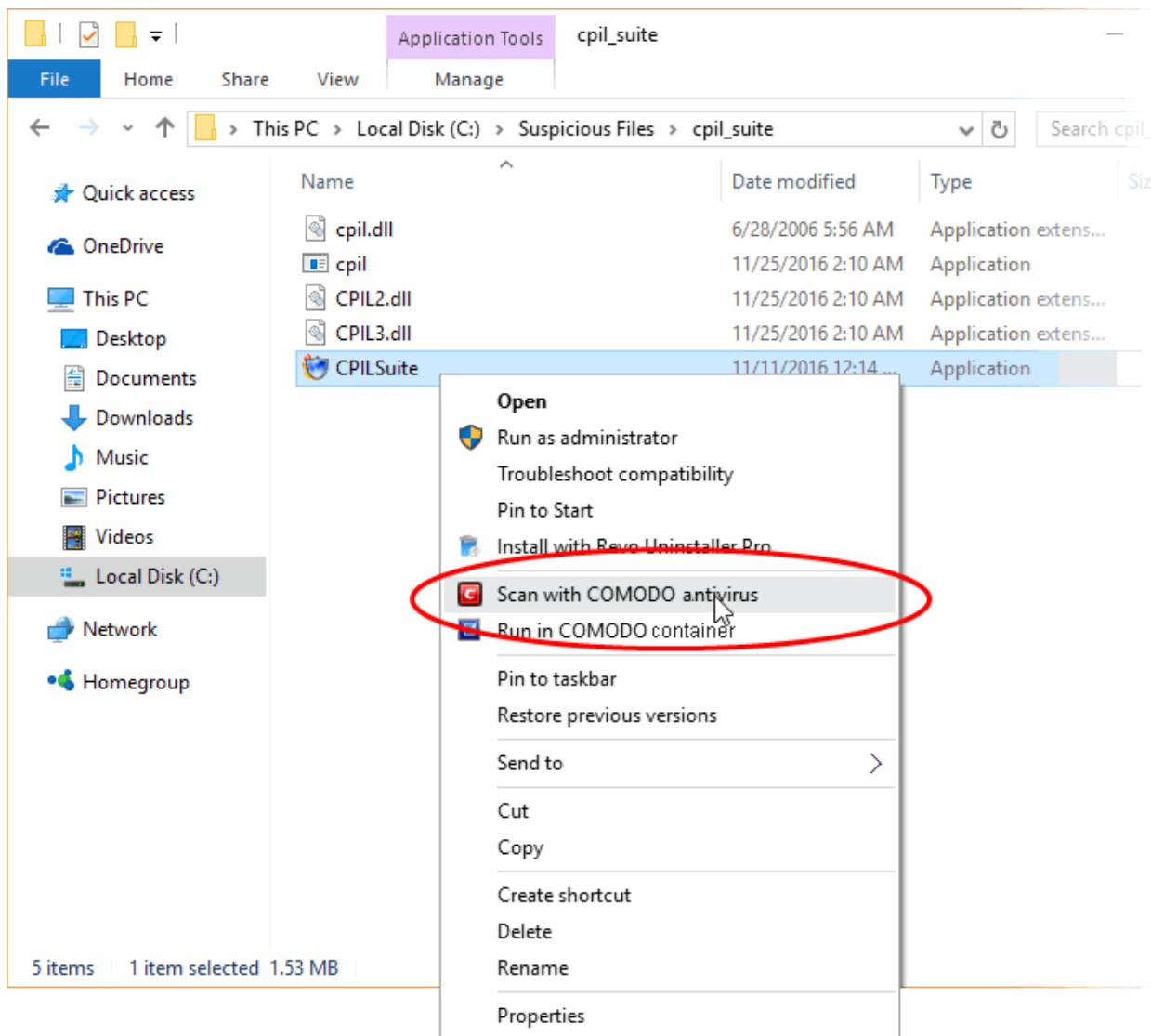


Run an Instant Antivirus Scan on Selected Items

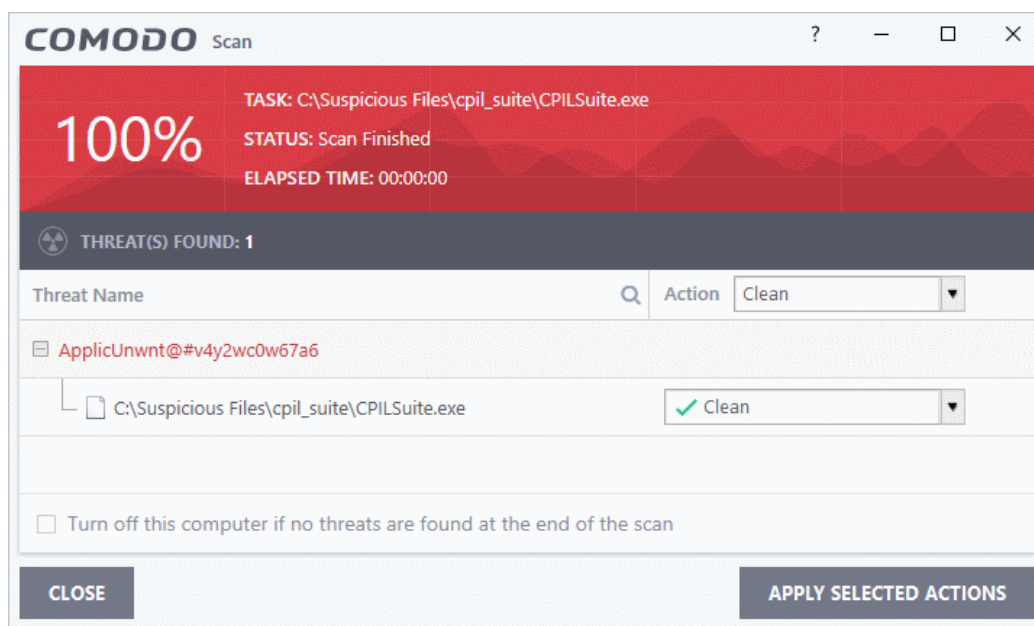
You can run an instant virus scan on files, folders and entire drives. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives and digital cameras.

To instantly scan an item

- Right-click on the item and select 'Scan with COMODO Antivirus' from the context sensitive menu



The item will be scanned immediately. Any threats found will be shown at the end of the scan:



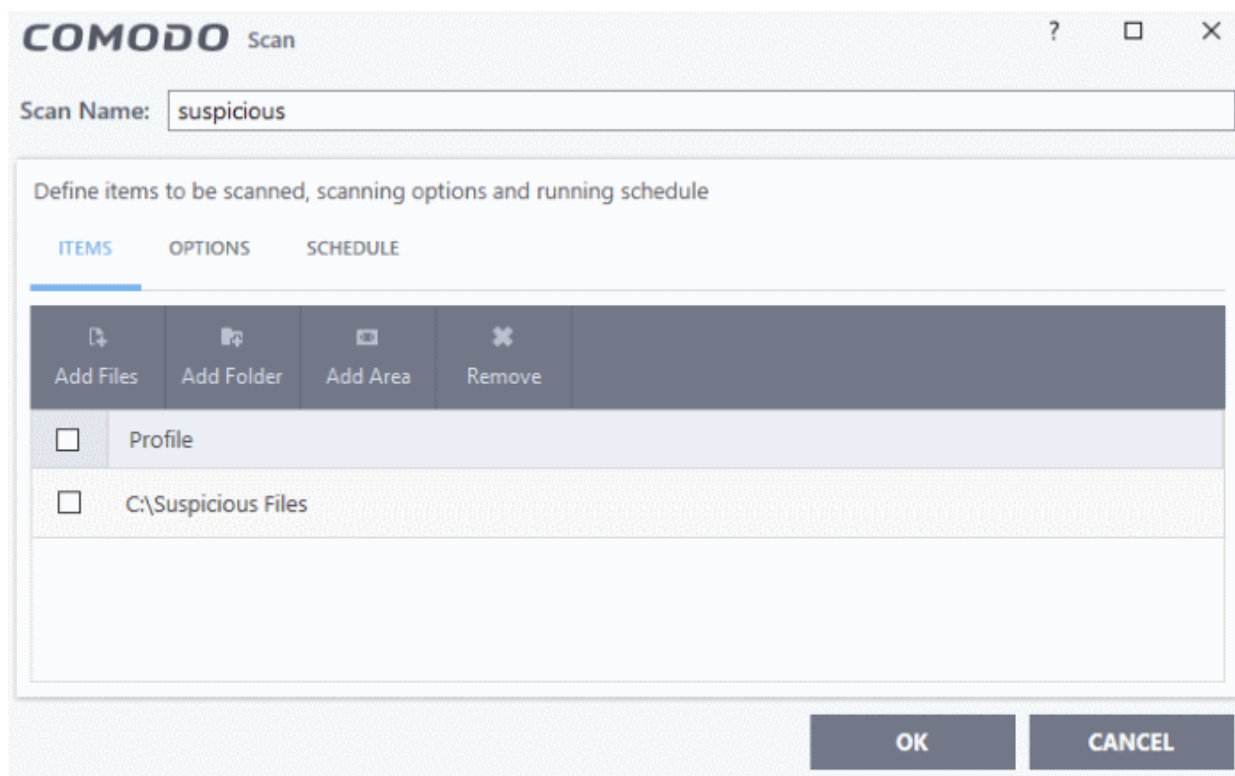
[Click here](#) for more details to take action on the infected item(s).

Create an Antivirus Scan Schedule

- Comodo Client Security lets you schedule virus scans on your entire system or specific areas.
- You can create a profile which defines exactly which files and folders are scanned, when they are scanned, and how they are scanned.

To create a scan schedule

- Click 'Tasks' at the top left of the CCS home screen
- Click 'Tasks' > 'General Tasks' interface
- Click 'Scan' > 'Custom Scan' > 'More Scan Options'
- Click 'Add' at the top to create a new custom scan profile



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

The next steps are to:

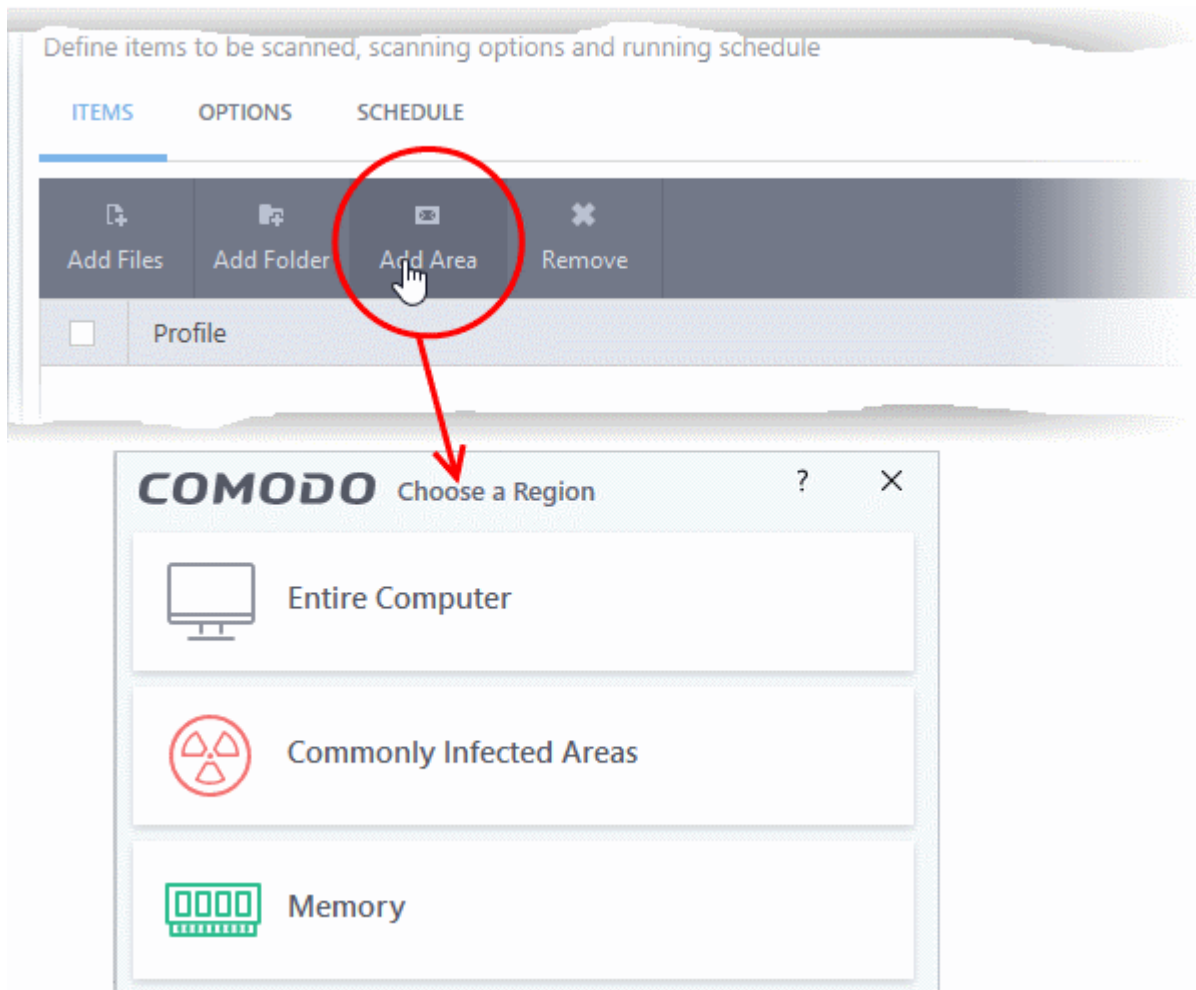
- **Select the items to be scanned**
- **Configure the scanning options for the profile (Optional)**
- **Configure a schedule for the scan to run periodically (Optional)**

To select the items to be scanned

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

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

- **Add File** - Allows you to add individual files to the profile. Click the 'Add Files' button and navigate to the file to be scanned in the 'Open' dialog and click 'Open'.
- **Add Folder** - Allows you to select entire folders to be included in the profile. Click the 'Add Folder' button and choose the folder from the 'Browse for Folder' dialog.
- **Add Region** - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas' and 'System Memory')

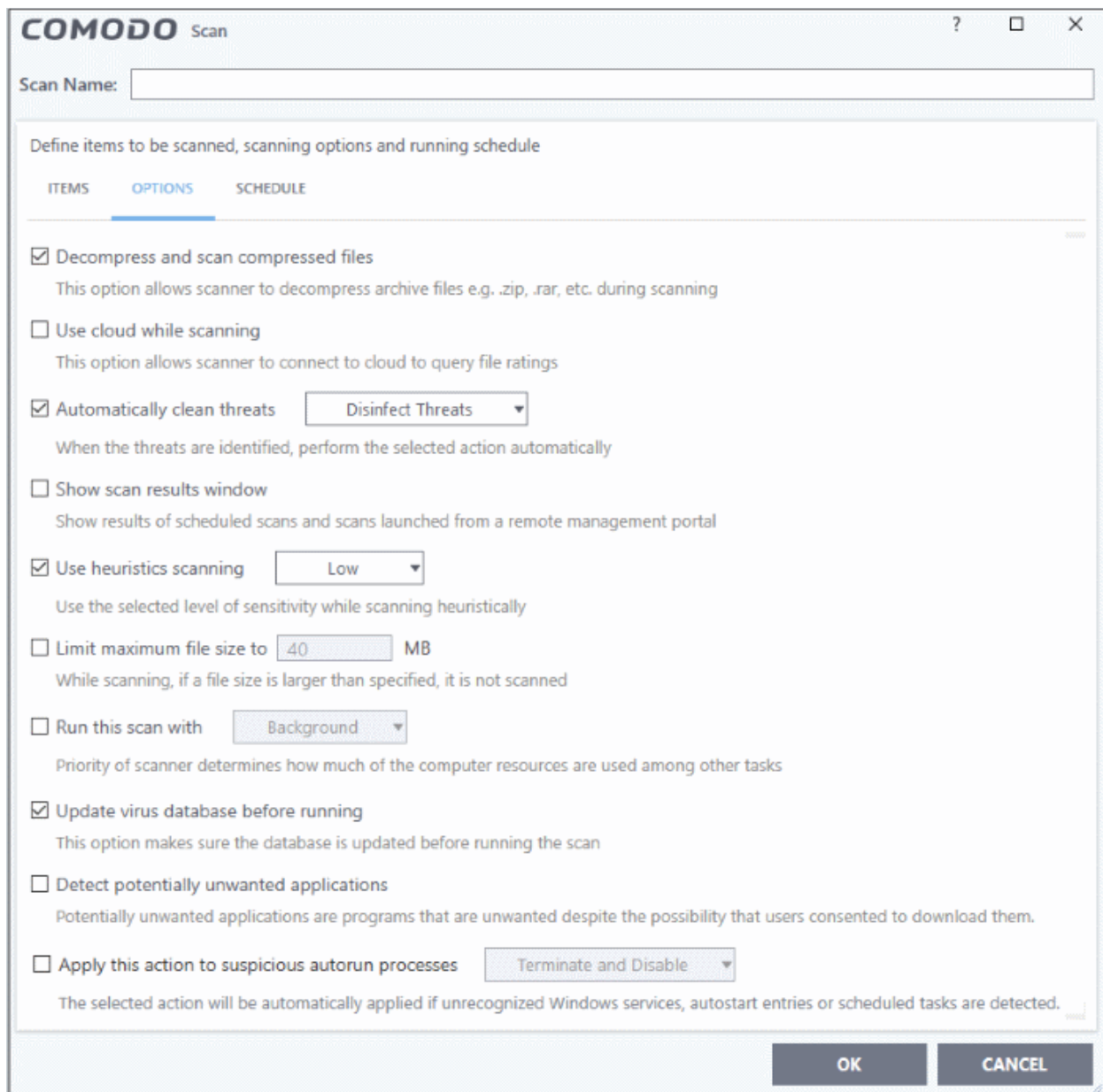


- Repeat the process to add more items to the profile
- To remove an item, select it and click 'Remove'

To configure Scanning Options

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

The options to customize the scan will open:



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

The available options are:

- **Quarantine Threats** - Malicious items will be moved to quarantine. You can view the items in the quarantine and choose to remove them or restore them (in case of false positives). See **Manage Quarantined Items** for more details on viewing and managing items moved to quarantine.
- **Disinfect Threats** - If a disinfection routine is available for the detected threat, the antivirus will remove the threat from the infected file and retain the application safe. Otherwise the item will be moved to 'Quarantine'.
- **Show scan results window** - If selected, displays the number of objects scanned and the number of

threats found by local and remotely run scans.

- **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. **(Default = Enabled)**

Background Info:

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

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

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

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

Note 2 - CCS 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'**.

To schedule the scan to run at specified times

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

The screenshot shows the 'COMODO Scan' dialog box with the 'SCHEDULE' tab selected. The 'Scan Name' field is empty. The 'Define items to be scanned, scanning options and running schedule' section has three tabs: 'ITEMS', 'OPTIONS', and 'SCHEDULE'. Under 'Frequency', the 'Do not schedule this task' option is selected. Other options include 'Every few hours', 'Every Day', 'Every Week', and 'Every Month'. The 'Additional Options' section contains four unchecked checkboxes: 'Run only when computer is not running on battery', 'Run only when computer is IDLE', 'Turn off computer if no threats are found at the end of the scan', and 'Run during Windows Automatic Maintenance'. 'OK' and 'CANCEL' buttons are at the bottom right.

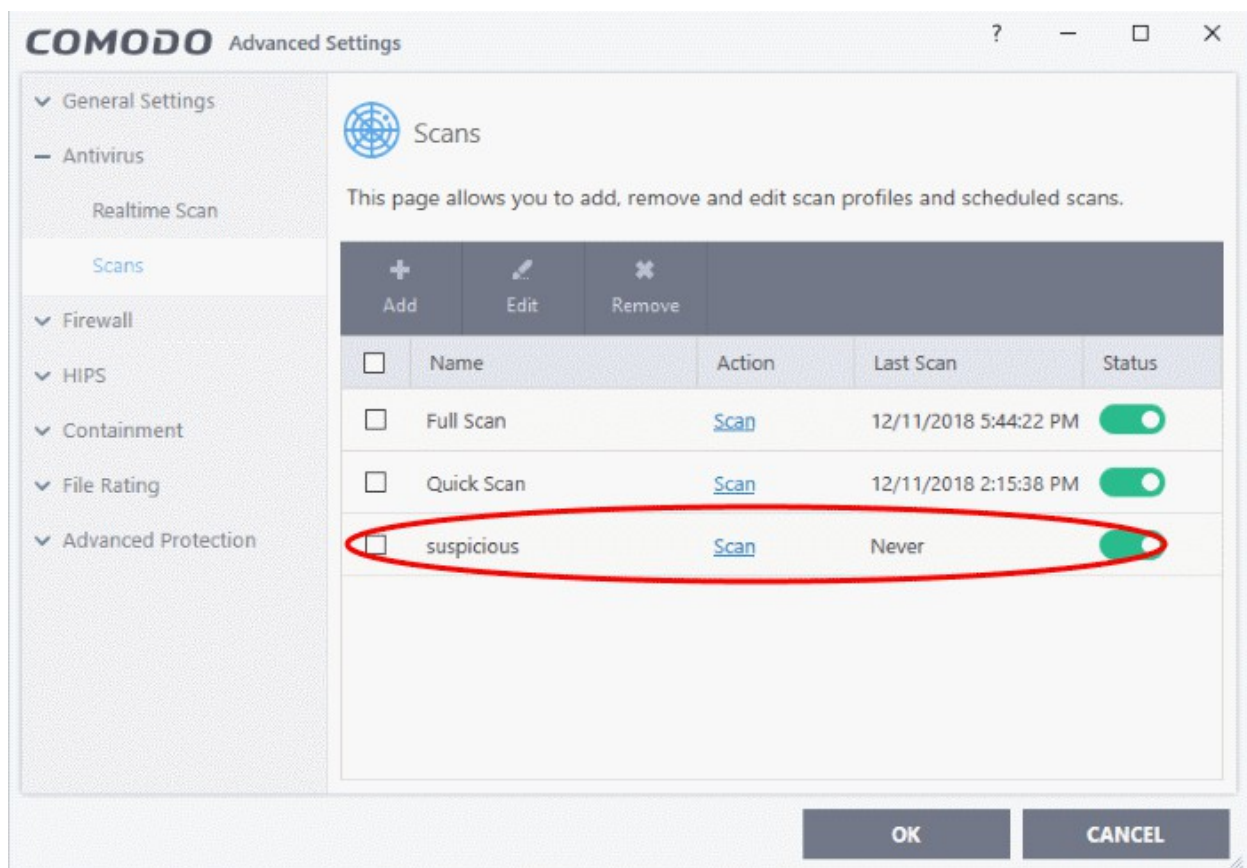
- **Do not schedule this task** - The scan profile will be created but will not run automatically. The profile will be available for manual, on-demand scans.
- **Every few hours** - Scans the areas defined in the profile every 'x' hours. You can specify the number of hours in the 'Repeat scan 'x' hours' field.
- **Every Day** - Scans the areas defined in the profile every day at the time specified in the 'Start Time' field.
- **Every Week** - Scans the areas defined in the profile on the day(s) specified in 'Days of the Week' field at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.

- **Every Month** - Scans the areas defined in the profile on the date(s) specified in 'Days of the month' field at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Run only when computer is not running on battery** - The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or any other battery driven portable computer.
- **Run only when computer is IDLE** - The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- **Run during Windows Maintenance** - Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time in addition to the configured schedule.
- The option 'Run during Windows Maintenance' will be available only if 'Automatically Clean Threats' is enabled for the scan profile under the 'Options' tab. See **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 Untrusted Programs inside the Container

Comodo Client Security allows you to run programs inside the Container on a 'one-off' basis. This is helpful for testing new programs you have downloaded, for applications that you are not sure that you trust, and for running beta software. You can also create a desktop shortcut to run the application inside the container on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



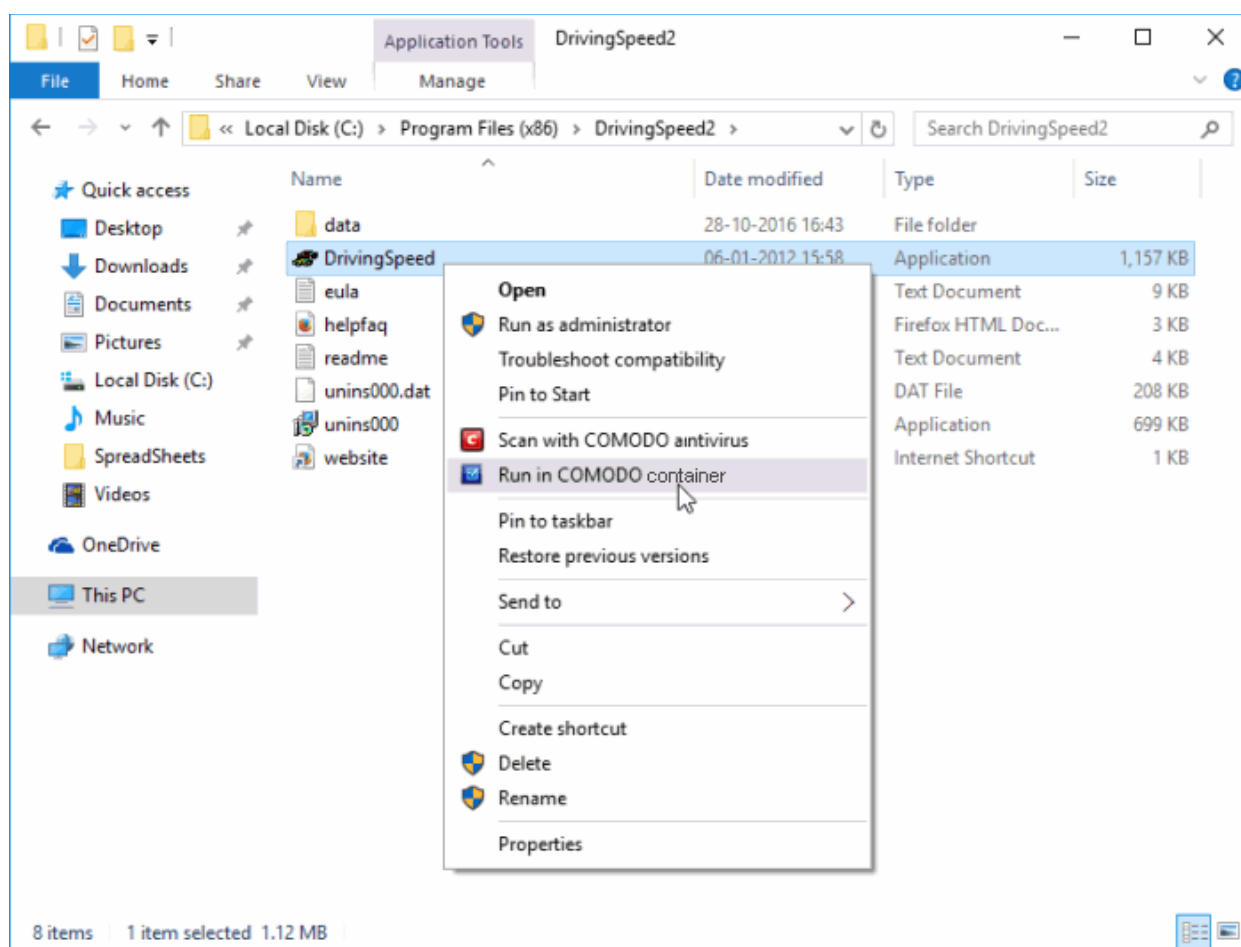
You can run a program in the container:

- **From the right click options**
- **From the Containment Tasks interface**
- **Running browsers inside the container**

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

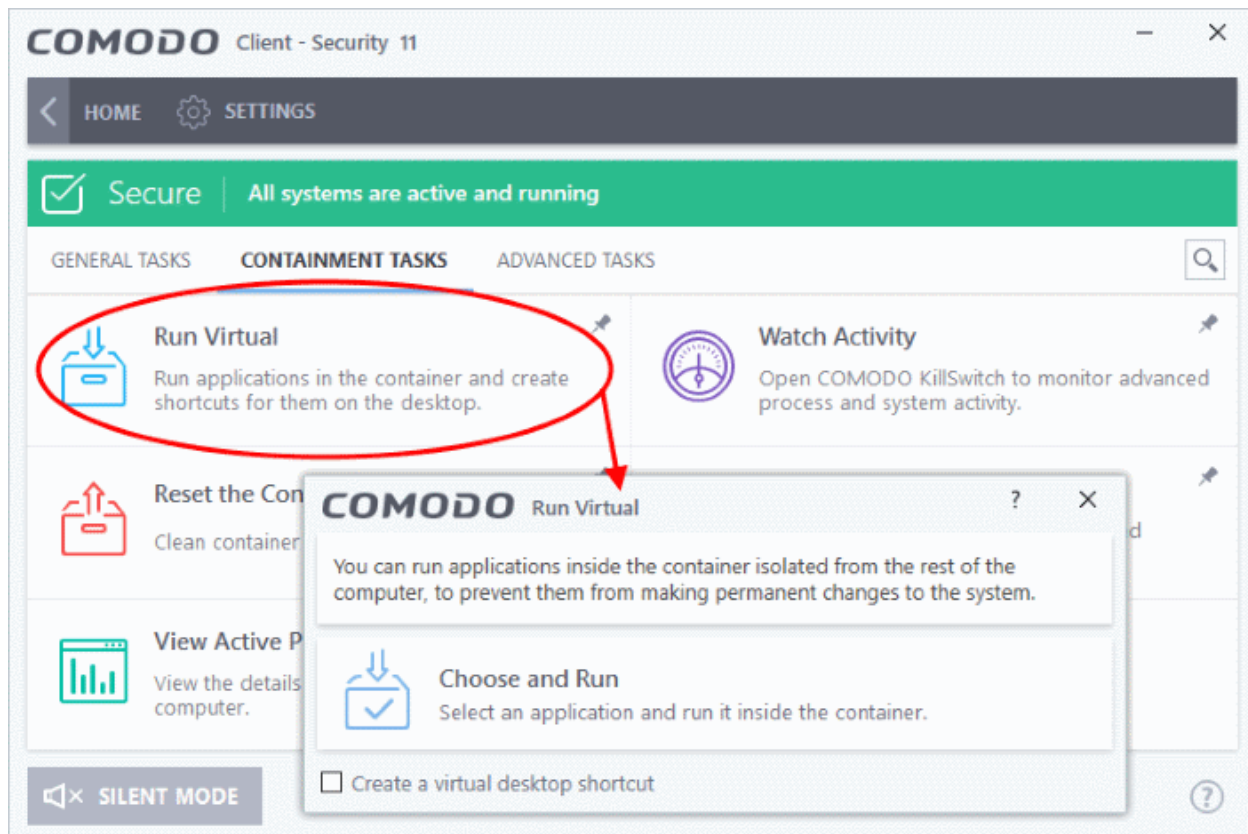
Right-click menu

1. Open Windows Explorer and navigate to the program you want to run in the container
2. Right-click on the program
3. Choose 'Run in COMODO container' from the context sensitive menu:



From the Containment Tasks interface

1. Click 'Tasks' at the top left of the CCS home screen
2. Click the 'Containment Tasks' tab
3. Click 'Run Virtual' from the 'Containment Tasks' interface

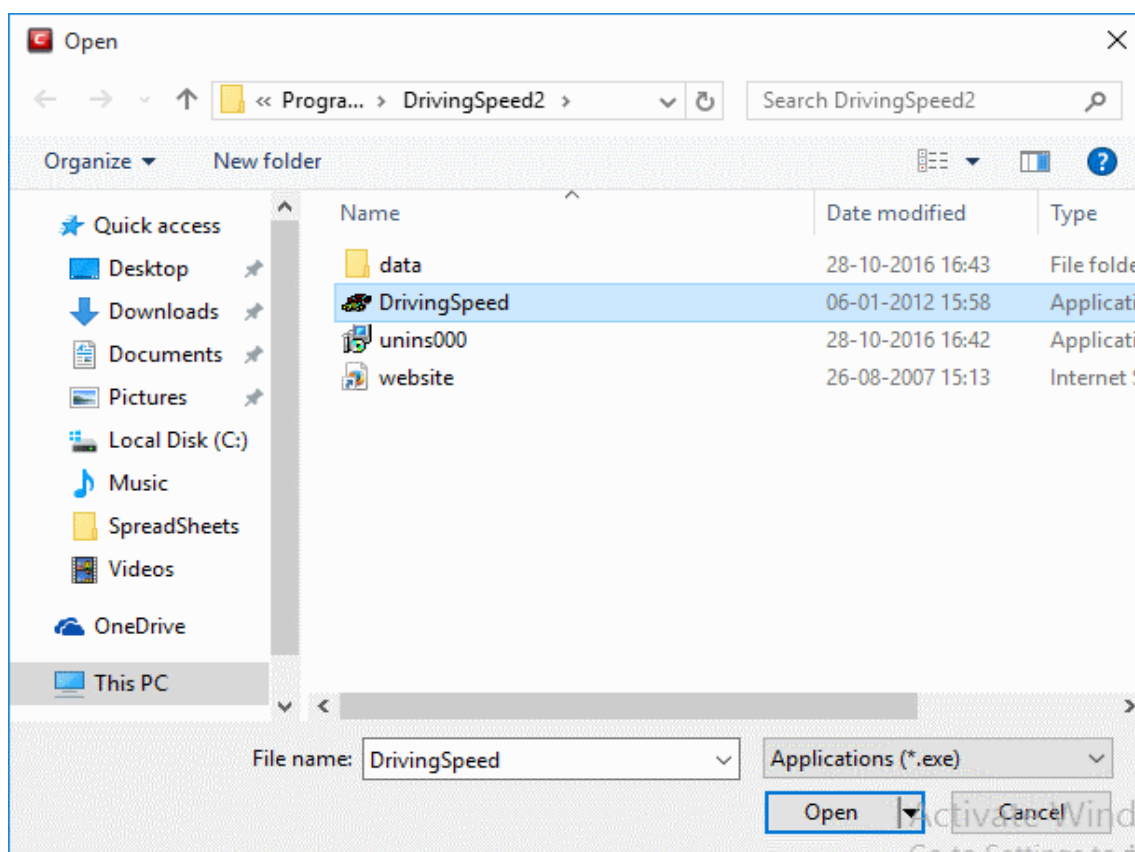


The 'Run Virtual' dialog will be displayed.

4. To run an application inside the container, click 'Choose and Run' then browse to the application.

The contained application will run with a green border around it.

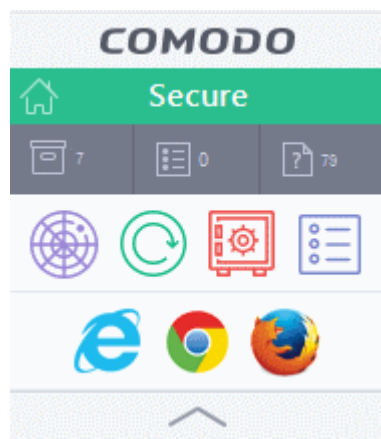
- Select 'Create a virtual desktop shortcut' if you wish to run the application in the container in future



5. Browse to the application and click 'Open'.

Running browsers inside the Container

The CCS Desktop Widget contains shortcuts that open the browsers installed on your computer. Browser opened in this way will run inside the container.



- Click a browser icon to start the browser inside the container
- The application will run in the container on this occasion only.
- You can create a desktop 'virtual shortcut' for the browser by selecting 'Create a virtual desktop shortcut' in step 3 (above). This will allow you to quickly launch a containerized instance of the browser in future.
- If you wish to run an application in the container on a long-term/permanent basis then **add the file to the Container.**

Run Browsers Inside 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:

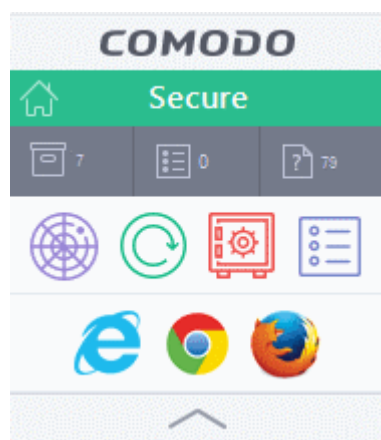


There are two ways to run a browser in the container:

- **From the desktop widget**
- **From the Containment Tasks interface**

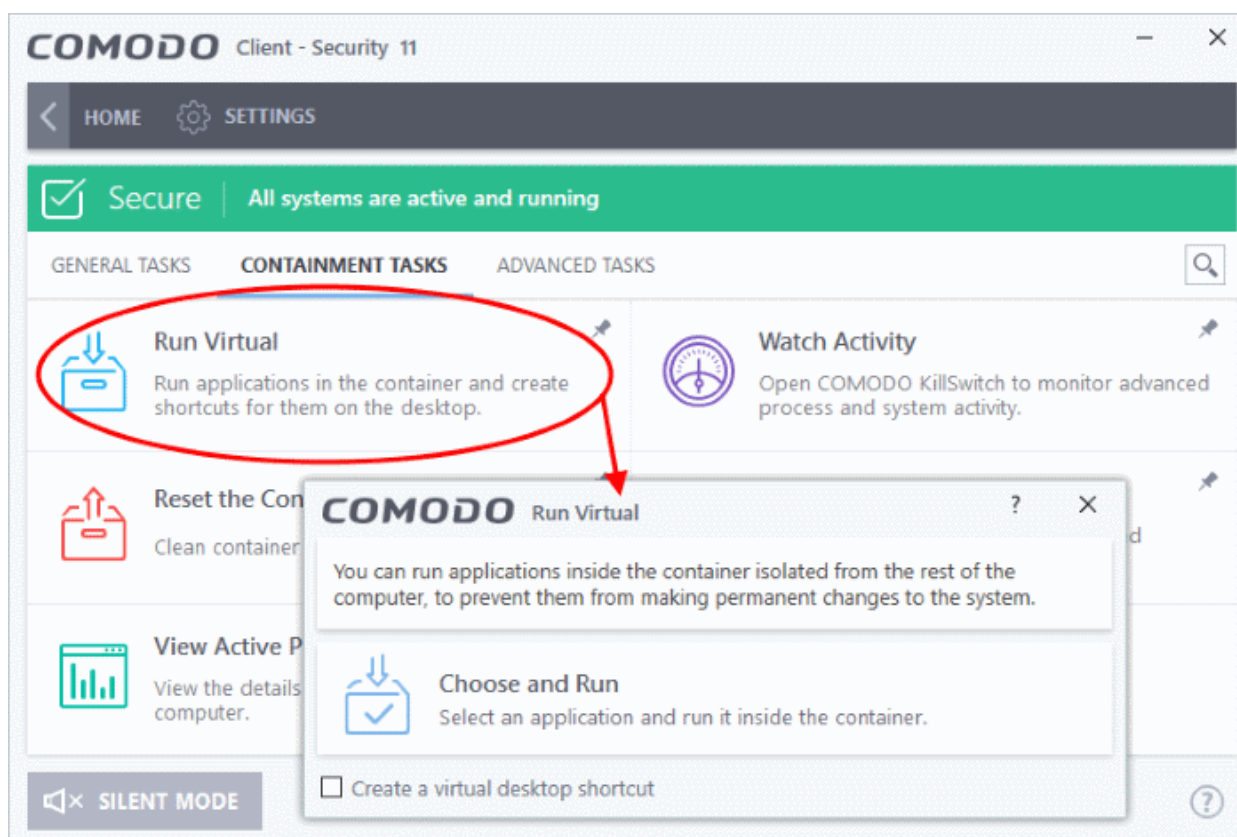
To start a browser from the desktop widget

- The CCS Desktop Widget contains shortcuts to browsers installed on your computer.
- Click one of these icons to launch your browser inside the secure container:



To start a browser from the Containment Tasks interface

1. Click 'Tasks' at the top left of the CCS home screen
2. Click the 'Containment Tasks' tab
3. Click 'Run Virtual'

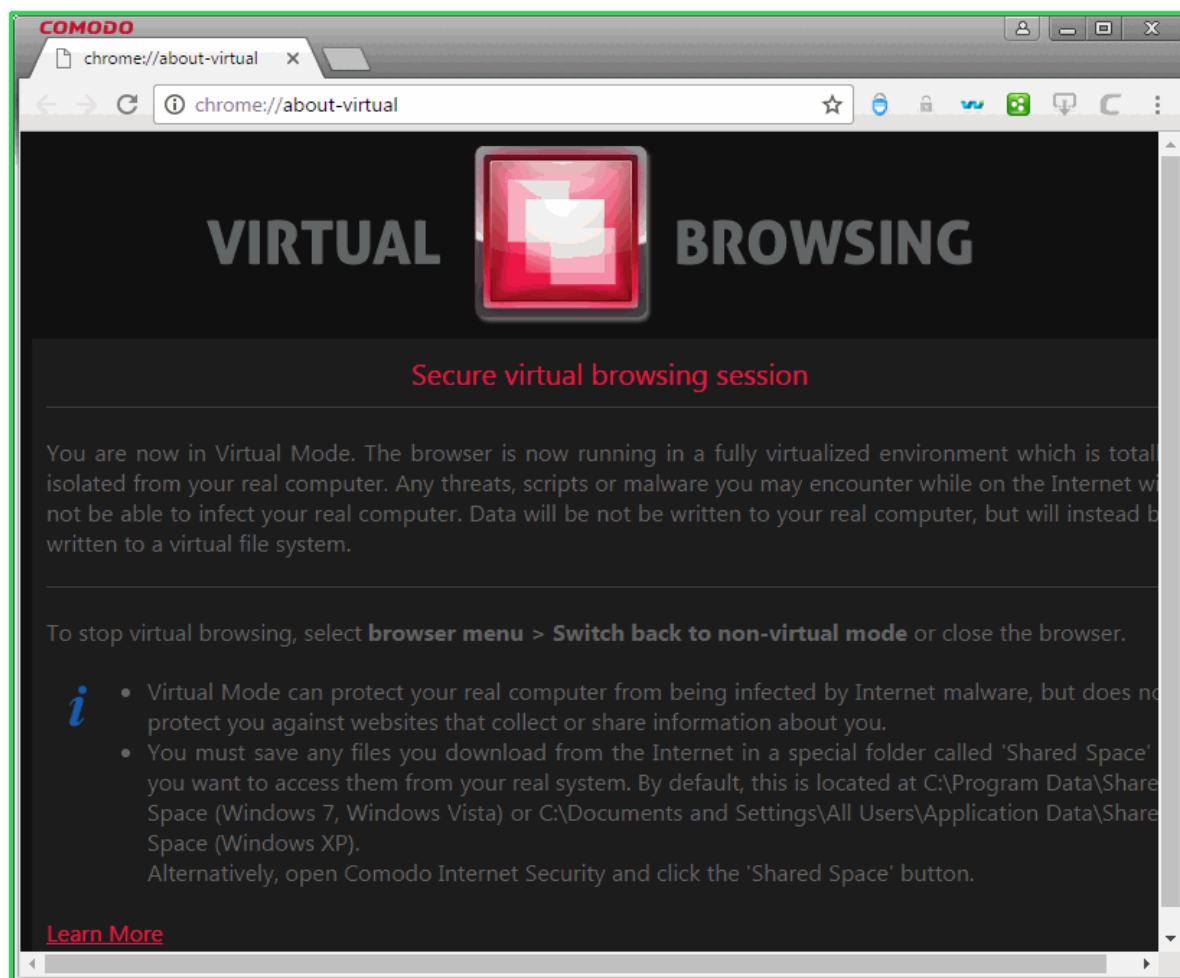


4.

The 'Run Virtual' dialog will open:

5. To run a browser inside the container, click 'Choose and Run'.
6. Navigate to the installation location of the browser and select the .exe file of the browser.
7. If you wish to create a desktop shortcut to run the browser in the container in future, select 'Create a virtual desktop shortcut'

The browser will run with a green border indicating that it is contained:

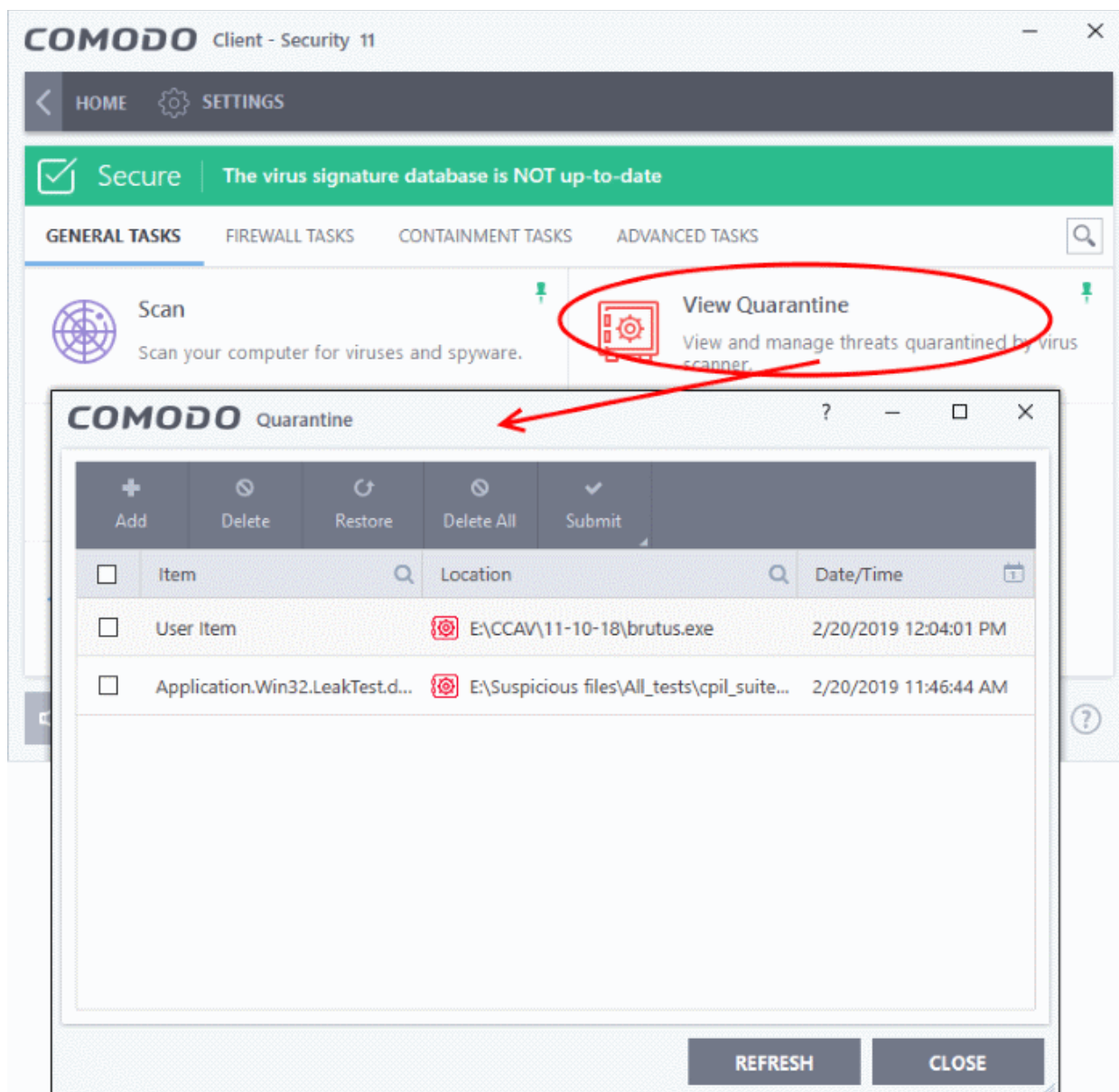


Restore Incorrectly Quarantined Item(s)

If you have incorrectly quarantined an item then you can restore it as follows:

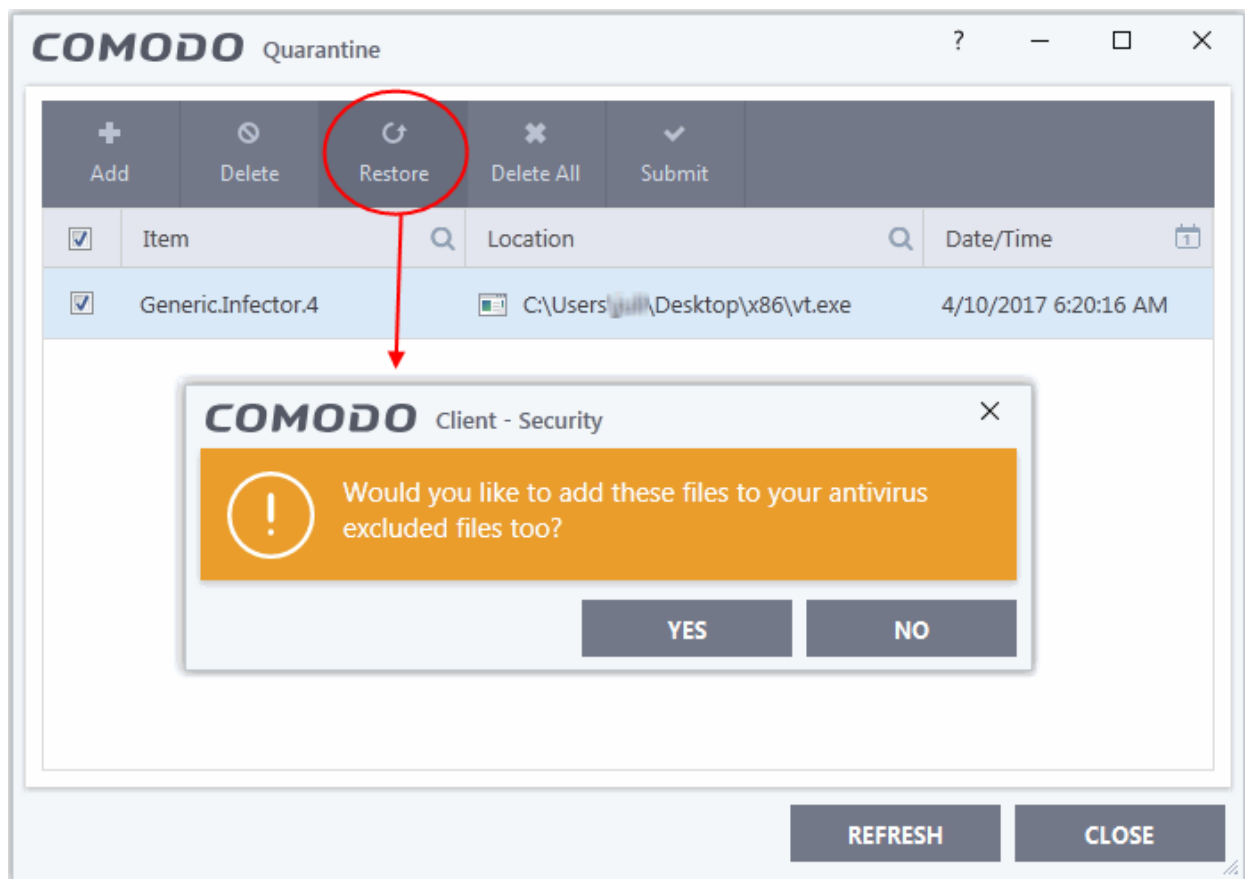
- Click 'Tasks' at the top left of the CCS home screen
- Click the 'General Tasks' tab
- Click 'View Quarantine'

The 'Quarantine' interface will open:



The interface lists items moved to quarantine by the antivirus system and those that were manually quarantined.

1. Select item(s) from the 'Quarantine' interface and click 'Restore' at the top.
2. 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:



- If you choose 'Yes', the selected files will be restored to their original locations and will be added to the antivirus exclusion list. These files will be skipped during future scans.
 - If you choose 'No', the items will be restored to their original locations BUT may still be flagged by future antivirus scans.
3. See **Submit Quarantined Items to Comodo for Analysis** for related information on this topic.
 4. Click 'Close' to exit.

[Click here](#) for more details on the quarantined items.

Submit Quarantined Items to Comodo for Analysis

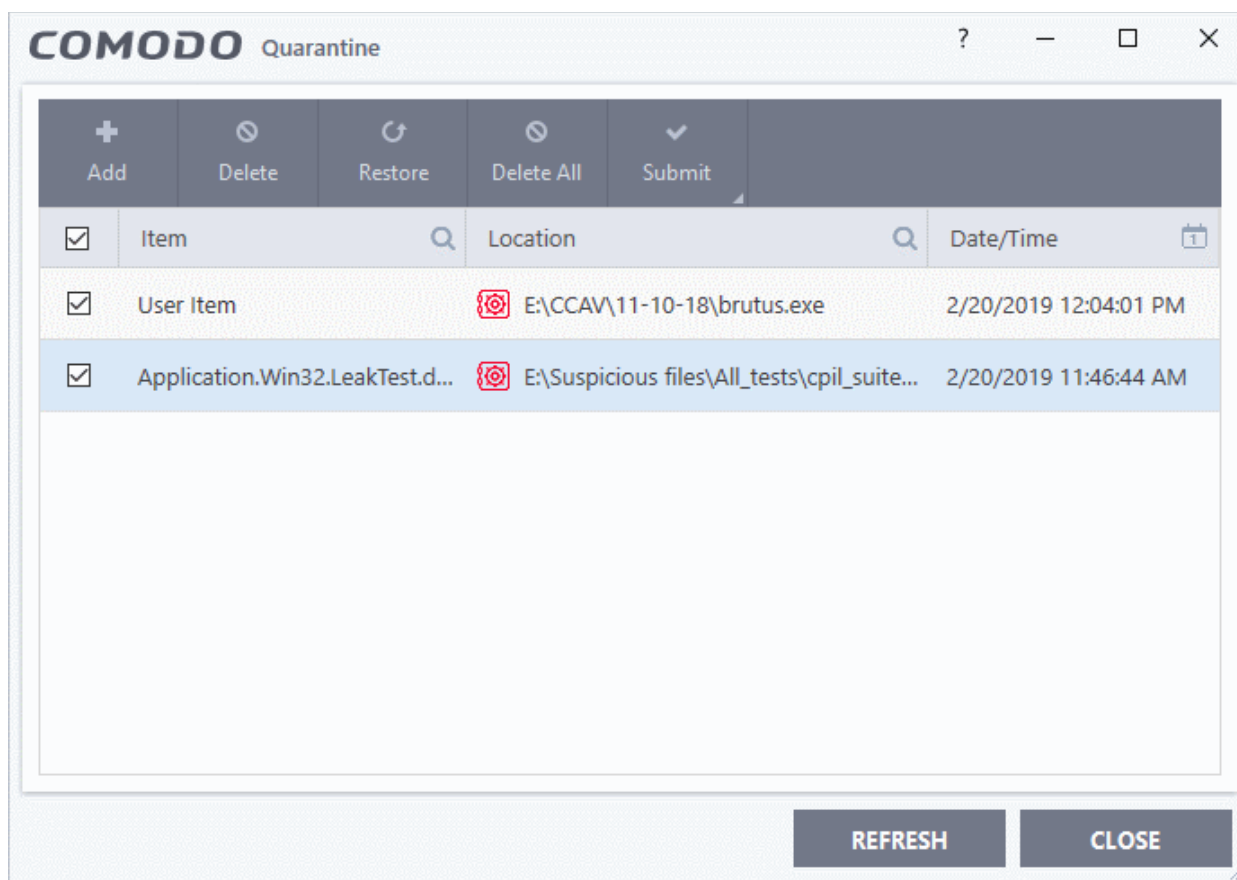
- Items which have been quarantined as a result of an antivirus scan can be sent to Valkyrie for analysis.
- Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.
- If the submitted item is found to be a false positive, it will be added to the Comodo white-list.
- If it is found to be malware, it will be added to the virus black-list.
- Submitting files helps Comodo enhance its virus signature database and benefits millions of CCS users. See **Quarantined Items** for more detailed information on the quarantine system.

To submit quarantined items

1. Click 'Tasks' at the top left of the CCS home screen
2. Click the 'General Tasks' tab
3. Click 'View Quarantine'

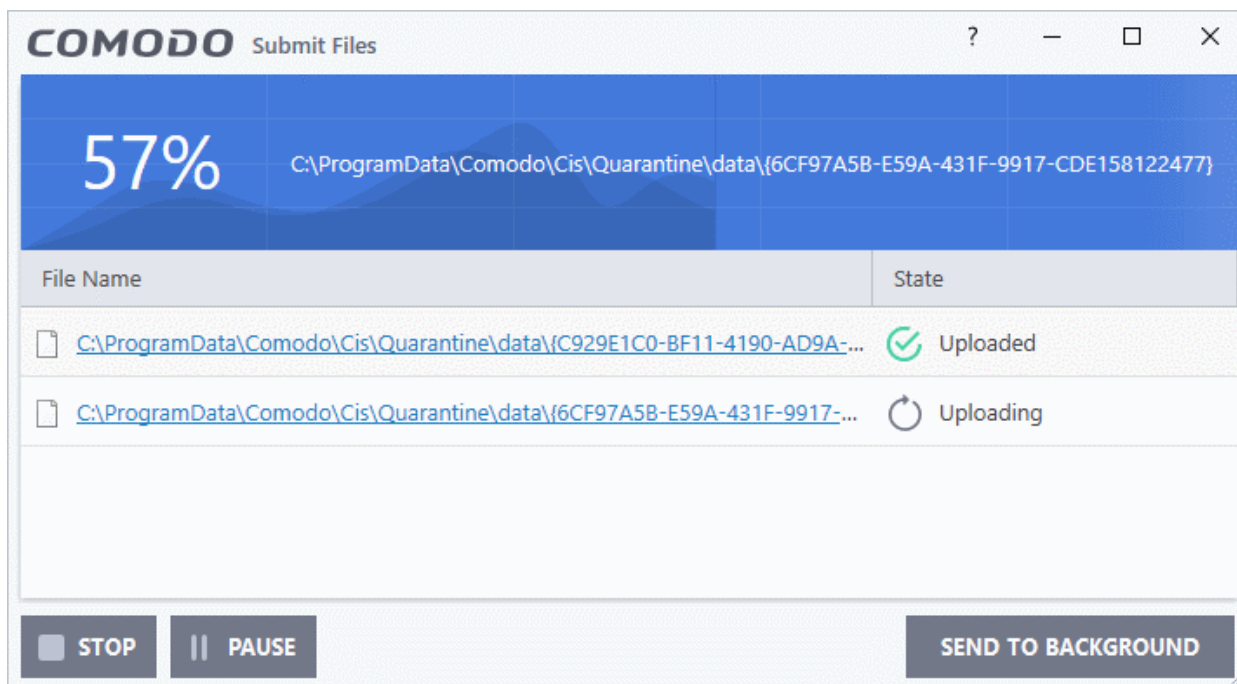
The 'Quarantine' interface will open. The interface lists files moved to quarantine by the antivirus scanner and files

that were manually moved to quarantine.



4. Select the item(s) you wish to send for analysis and click 'Submit' > 'Submit to Valkyrie'

The submission progress will start:



The results will state whether the file was successfully submitted or whether it was already submitted by other users

and is pending analysis.

Enable File Sharing Applications like BitTorrent and Emule

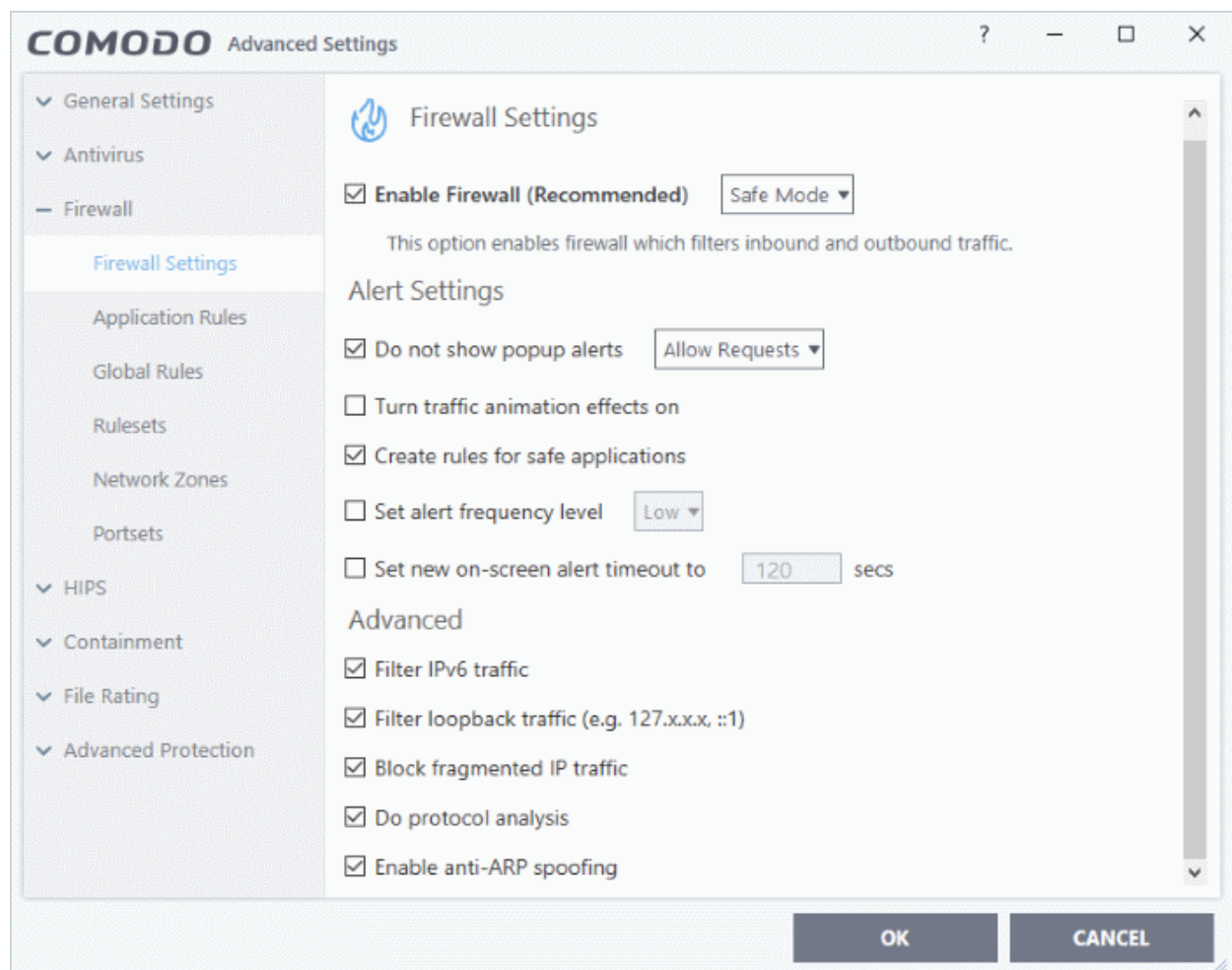
This topic explains how to configure Comodo Firewall to work with file sharing applications like Shareaza/Emule and BitTorrent/UTorrent.

To allow file sharing applications:

- **Disable 'Do Protocol analysis' (disabled, by default)**
- **Create a 'Predefined Firewall Ruleset' for Shareaza/Emule**
- **Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent**

Disable 'Do Protocol analysis'

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Firewall' > 'Firewall Settings' on the left



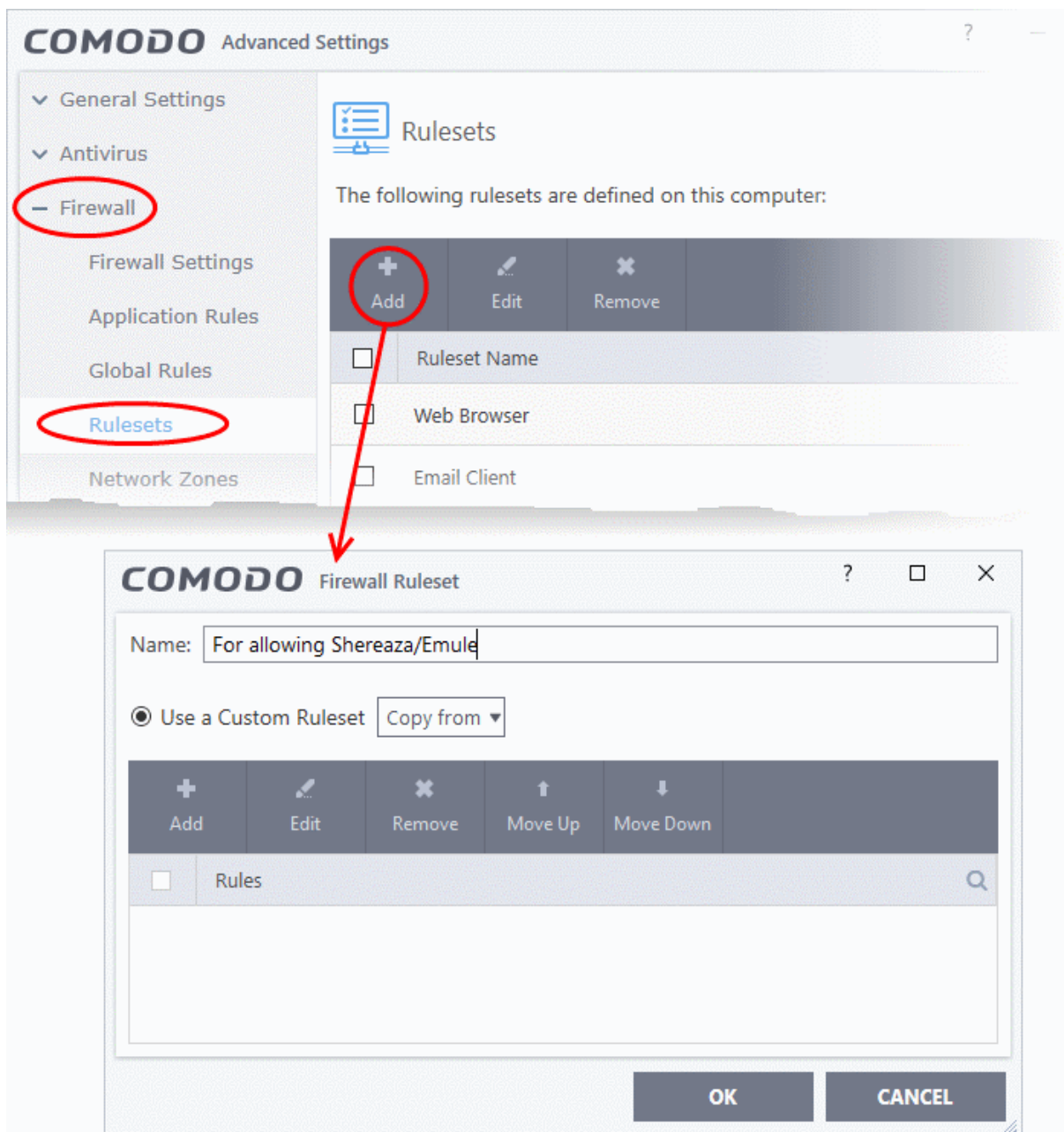
3. Disable 'Do not Show popup alerts' so CCS will generate alerts when you open Shareaza or Emule.
4. Disable 'Do Protocol Analysis'
5. Click 'OK' to save your settings.

Create a 'Predefined Firewall Ruleset' for Shareaza/Emule

1. Click 'Settings' at the top of the CCS home screen

2. Click 'Rulesets' under 'Firewall' on the left
3. Click 'Add' from the options at the top.

The 'Firewall Ruleset' interface will open:



6. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing Shareaza/Emule'.
7. Now you need to create six rules for the newly created 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

COMODO Firewall Rule ? X

Action: Log as firewall event if this rule is fired

Protocol:

Direction:

Description:

SOURCE ADDRESS DESTINATION ADDRESS SOURCE PORT DESTINATION PORT

Exclude (i.e. NOT the choice below)

Type:

OK CANCEL

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 CCS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'For allowing Shareaza/Emule')
- Select 'Remember my answer'.

To create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Settings' on the CCS home screen to open 'Advanced Settings'
2. Click 'Rulesets' under 'Firewall' on the left

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

The 'Firewall Ruleset' interface will open, allowing you to create a new ruleset:

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

- Click 'OK' in the 'Firewall Ruleset' interface.
- Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start BitTorrent or Utorrent. When CCS raises an alert:

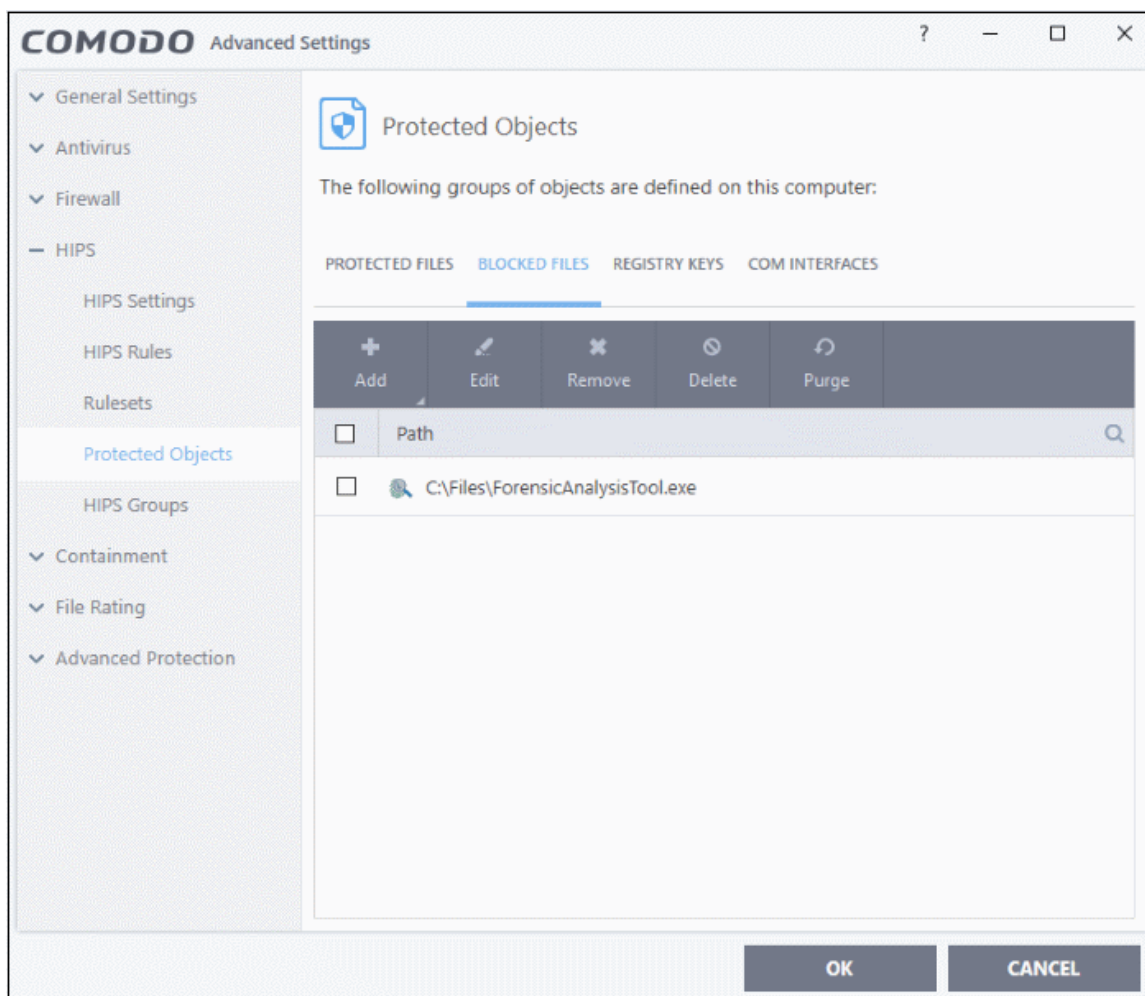
- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'BitTorrent/Utorrent')
- Select 'Remember my answer'.

Block any Downloads of a Specific File Type

Comodo Client Security can be configured to block downloads of specific types of file.

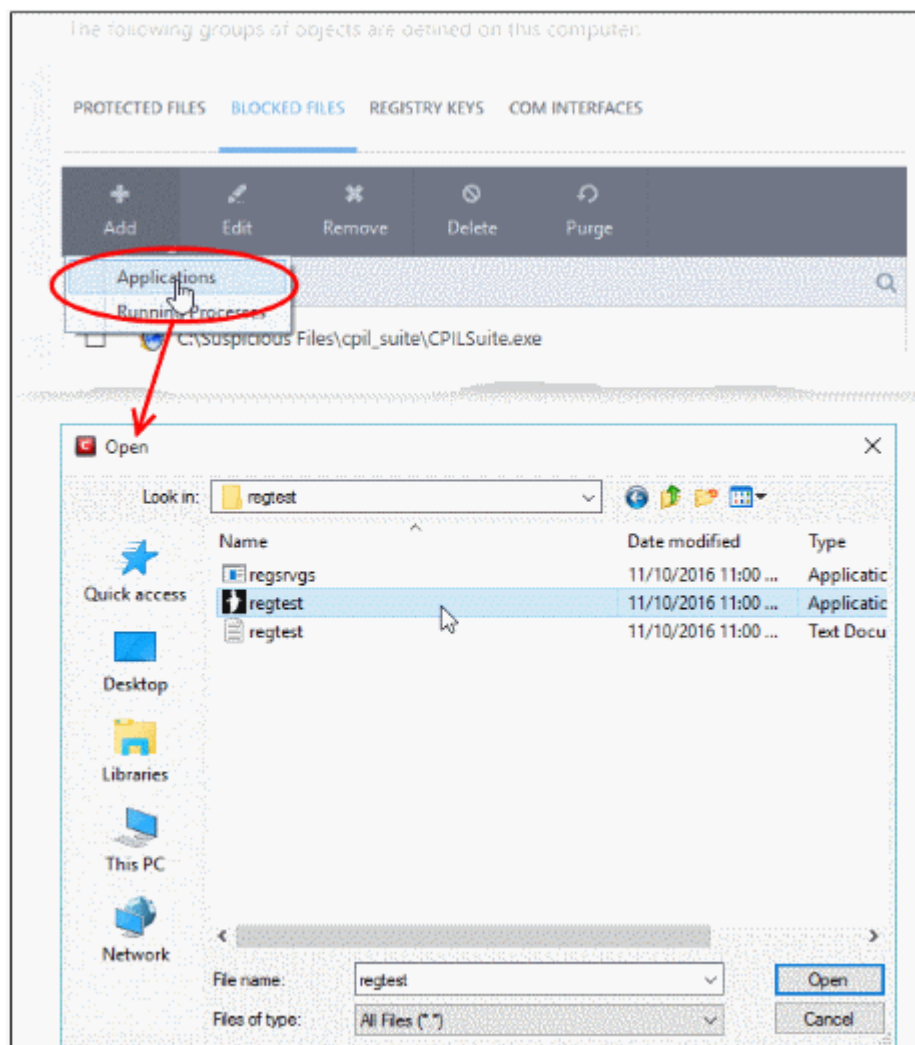
Example scenarios:

- Some malicious websites try to push downloads of malware in .exe file format. .exe files are programs which can execute commands on your computer. If the .exe is malicious then these commands could install a virus, initiate a buffer overflow attack or could contain code to turn your PC into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You may want to block the download of audio files (.wma, .mp3, .wav, .midi), video files (.wmv, .avi, .mpeg, .swf) or image files (.bmp, .jpg, .png) for various reasons.
- To block downloads of a specific file type in the HIPS section:
 1. Click 'Settings' on the CCS home screen
 2. Click 'HIPS' > 'Protected Objects' on the left
 3. Click the 'Blocked Files' tab:



4. Click 'Add' > 'Applications'.
5. Navigate to the file you want to add and click 'Open'.
6. Select any file from the folder and click 'Open'.

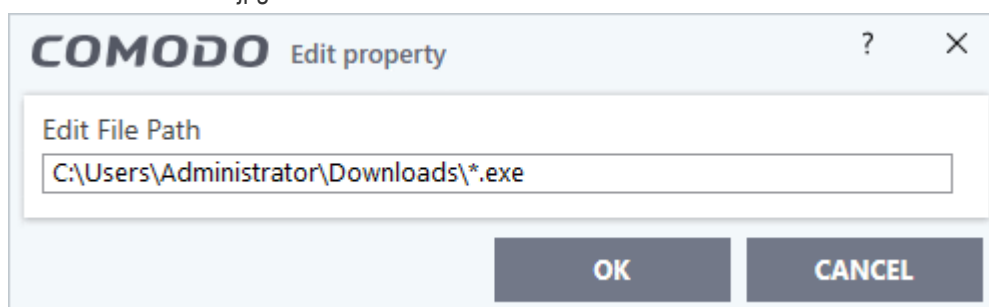
The file will be added to the 'Blocked Files' list.



7. Select the entry from the 'Blocked Files' interface and click 'Edit' at the top.

The 'Edit Property' dialog will open:

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' 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.

To unblock the download, go to

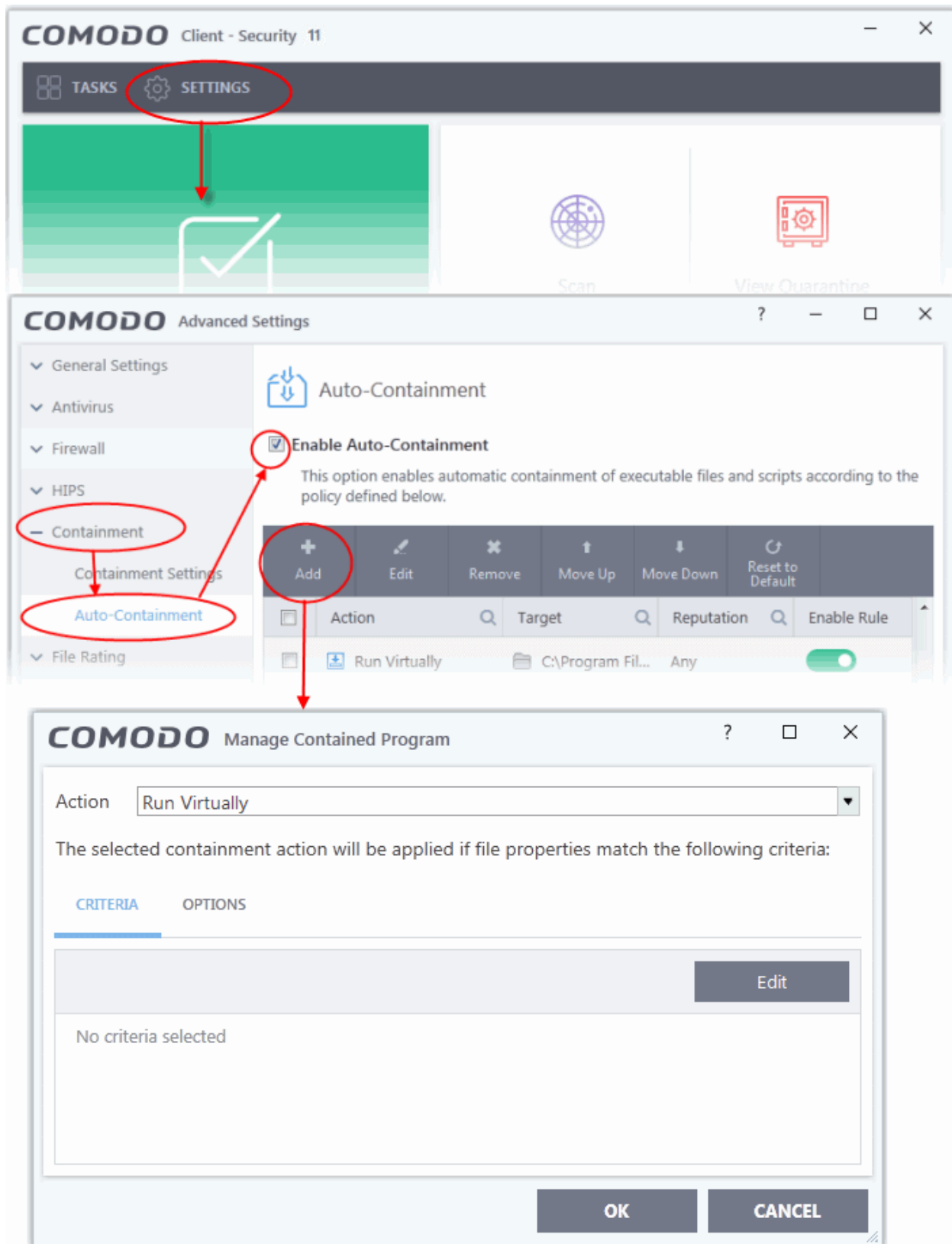
- 'HIPS' > 'Protected Objects' > 'Blocked Files'
- Select the file path and choose 'Remove'

Disable Auto-Containment on a Per-application Basis

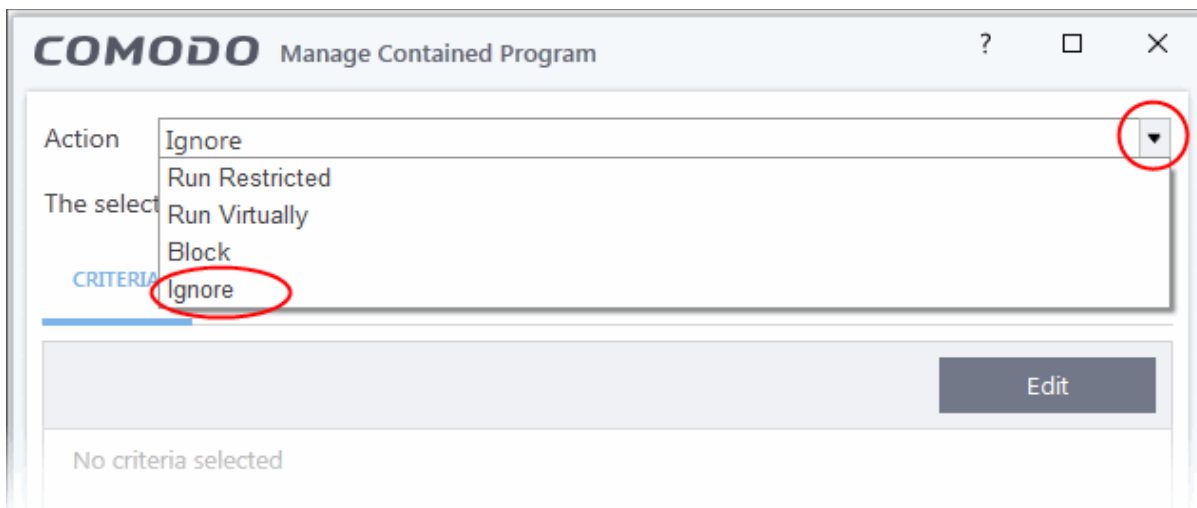
- The default auto-containment rules will run all unknown executables in the container and queue them for submission to Comodo for behavior analysis.
- Comodo recommends most users leave this setting intact to ensure the highest protection levels.
- Should you wish, you can create an 'Ignore' rule to exclude certain files or file types from containment.
- This could be useful for developers testing new applications which, by their nature, are unknown to the Comodo safe list.

To create an auto-containment exception

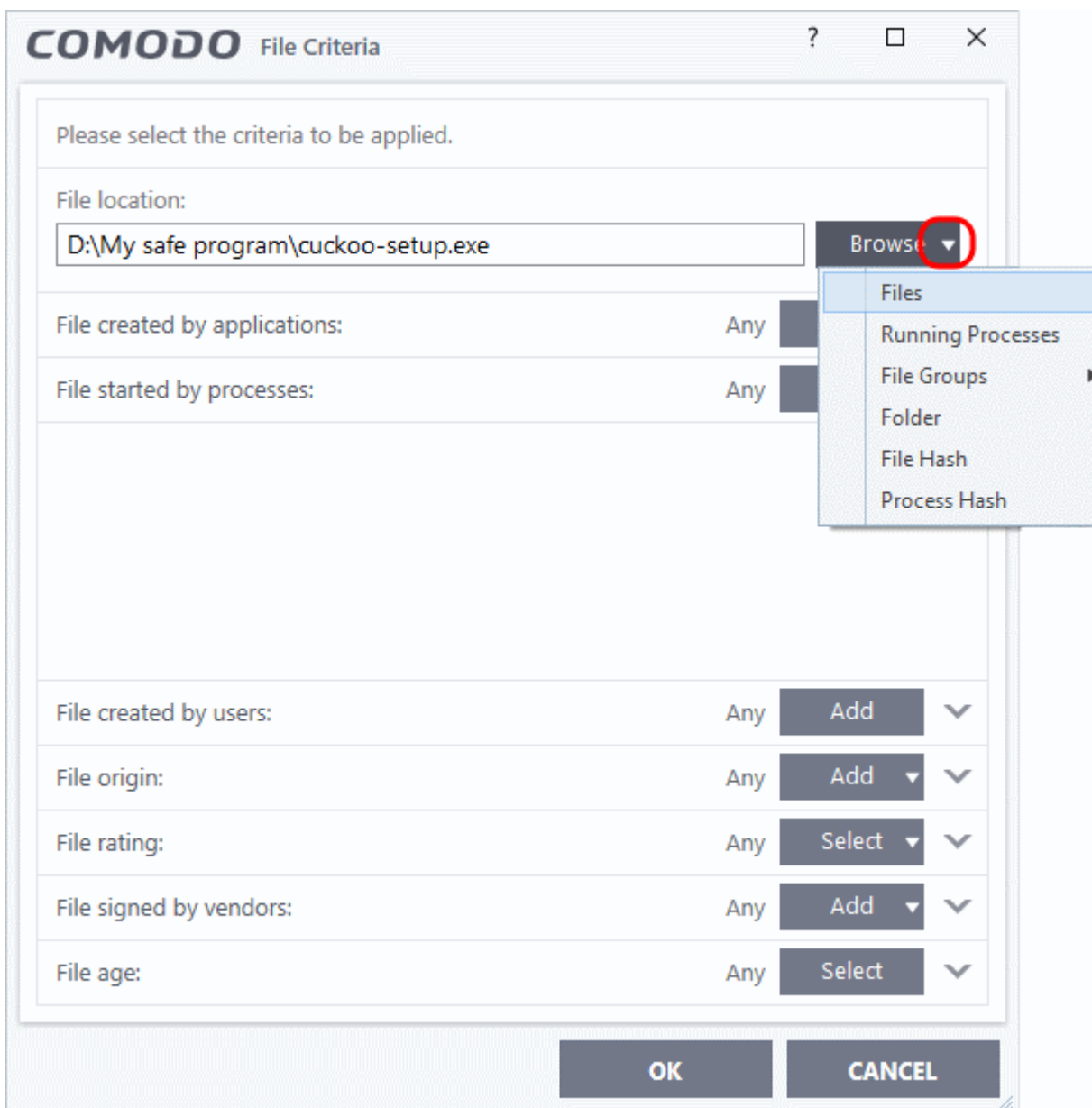
1. Click 'Settings' on the CCS home screen
2. Click 'Containment' > 'Auto-Containment' on the left
3. Ensure that 'Enable Auto-Containment' is selected
4. Click 'Add' to create a new rule:



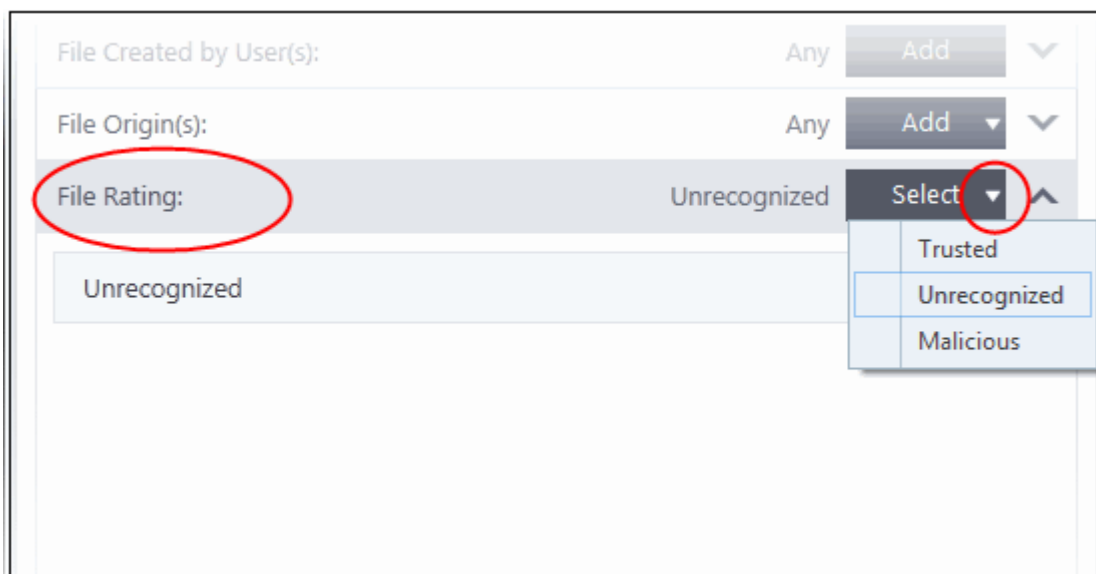
5. Select 'Ignore' from the 'Action' drop-down:



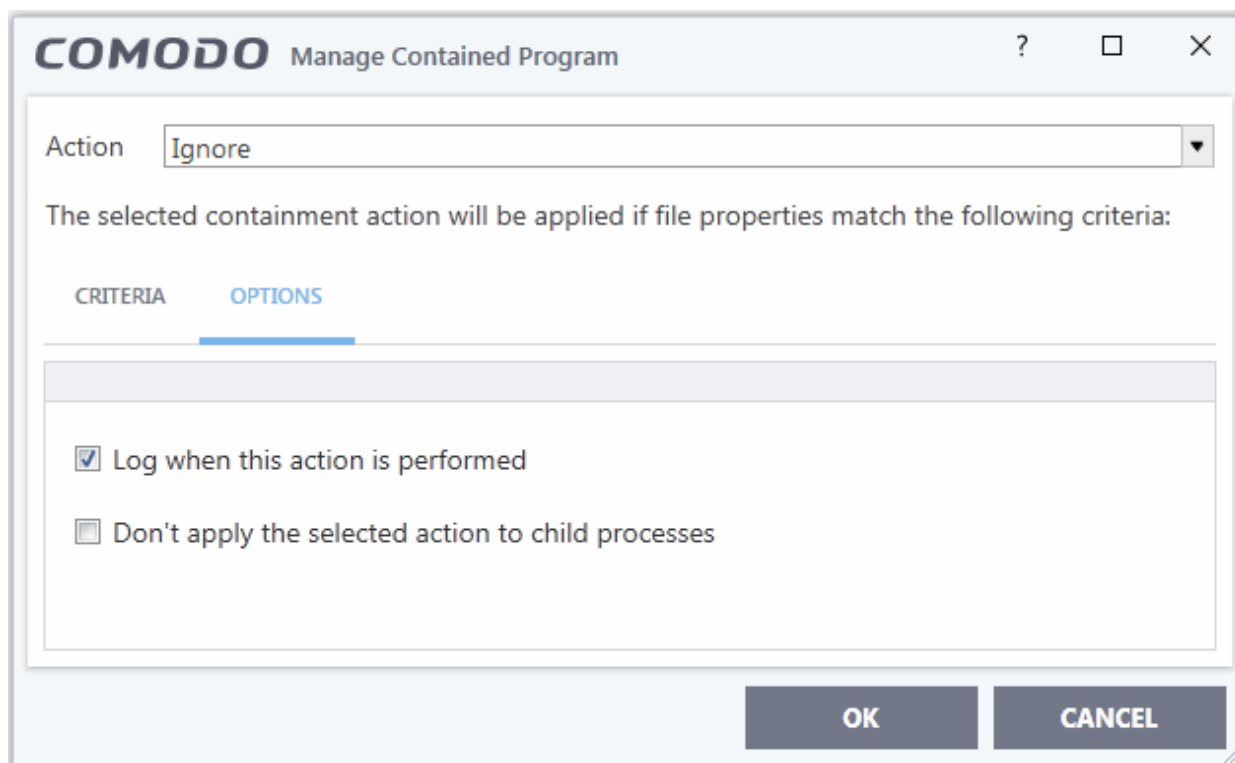
6. Make sure the 'Criteria' tab is open and click the 'Edit' button
7. Click 'Browse' to specify the type of item you wish to exclude:



8. You can select individual files, folders, processes, file groups or hashes. Click 'Open' when you have made your selection.
9. Click 'Select' at the end of the 'File Rating' row and select 'Unrecognized' from the drop-down:

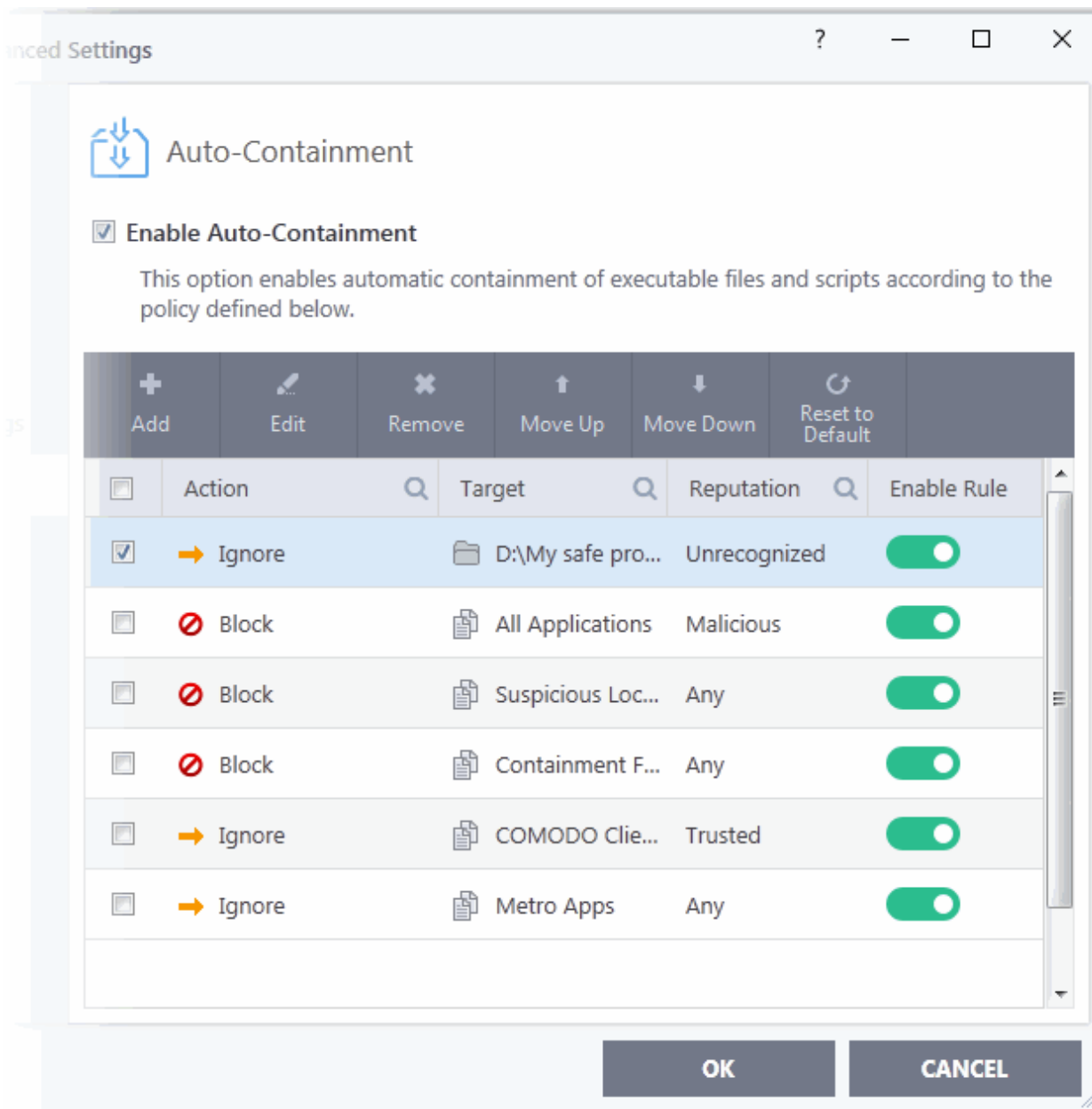


10. Next, click the 'Options' tab.



- **Log when this action is performed** - Optional. Will log events where this rule is triggered.
- **Don't apply the selected action to child processes** - Child processes are processes spawned by a parent application. By default, CCS treats all child processes individually.
 - Disabled - The ignore rule will apply to the target application and all child processes that it spawns. All will be allowed to run outside the container.

- Enabled - The ignore rule will apply only to the target application. All child processes will be inspected and possibly contained as per their file rating.
11. Select options as required and click 'OK'.



The new rule will be listed in the 'Auto-Containment' screen. Make sure to keep this rule above all other rules for unrecognized files.

Alternatively...

1. Assign a 'Trusted' rating to the file in the **File List** interface
2. Digitally sign your files with a code signing certificate from a trusted CA then manually add your organization to the **Vendors List** as trusted.
3. Disable auto-containment by de-selecting the 'Enable Auto-Containment' check box in the 'Auto-containment' settings panel. *Not recommended*

See **Unknown Files: The Scanning Processes**, for more details on Auto-Containment process.

Switch Off Automatic Antivirus Updates

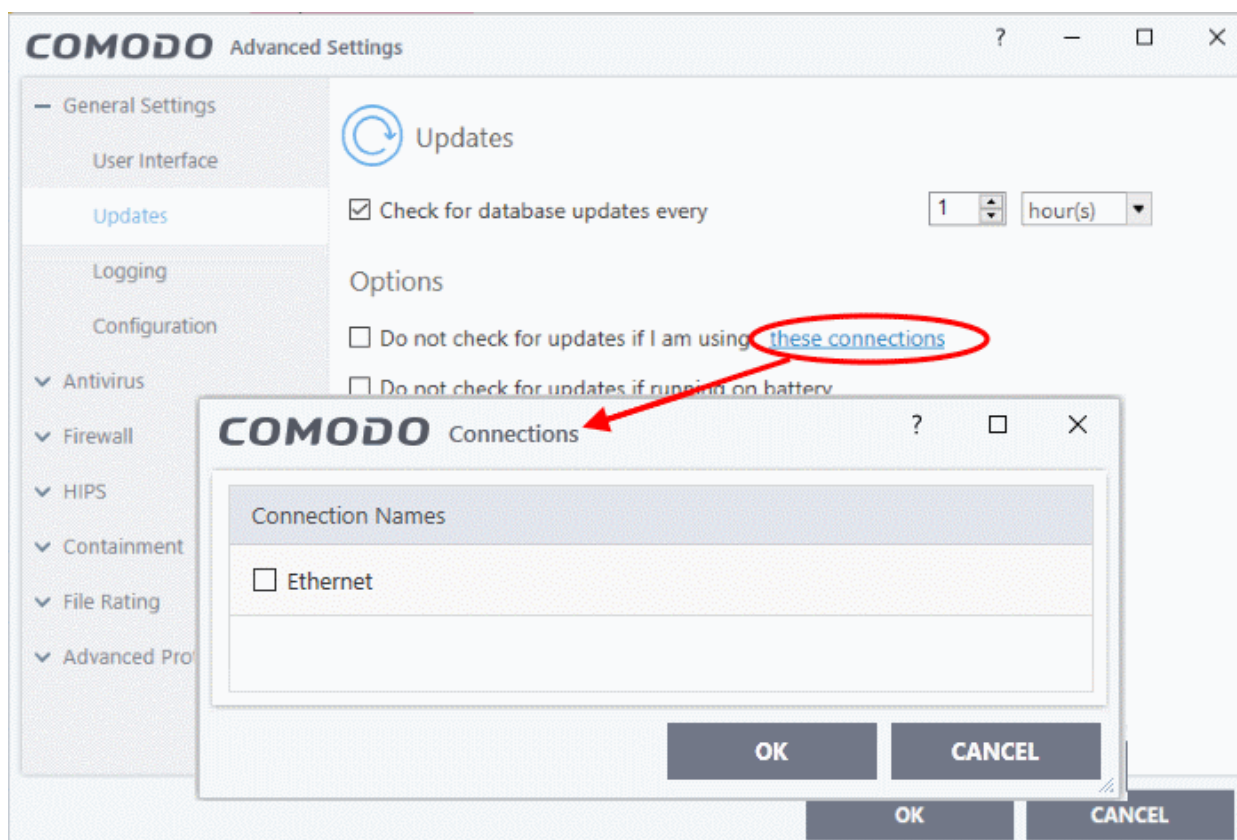
- By default, Comodo Client Security automatically checks for Antivirus database updates. However, some users like have control over when updates are downloaded.
 - For example, network administrators may not wish to automatically download because it will take up too much bandwidth during the day.
- Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.
- CCS provides full control over virus updates.

Click the appropriate link below to find out more:

- [Switch off automatic virus updates selectively](#)
- [Switch off automatic virus signature database updates prior to Antivirus Scans](#)

To switch off automatic updates selectively

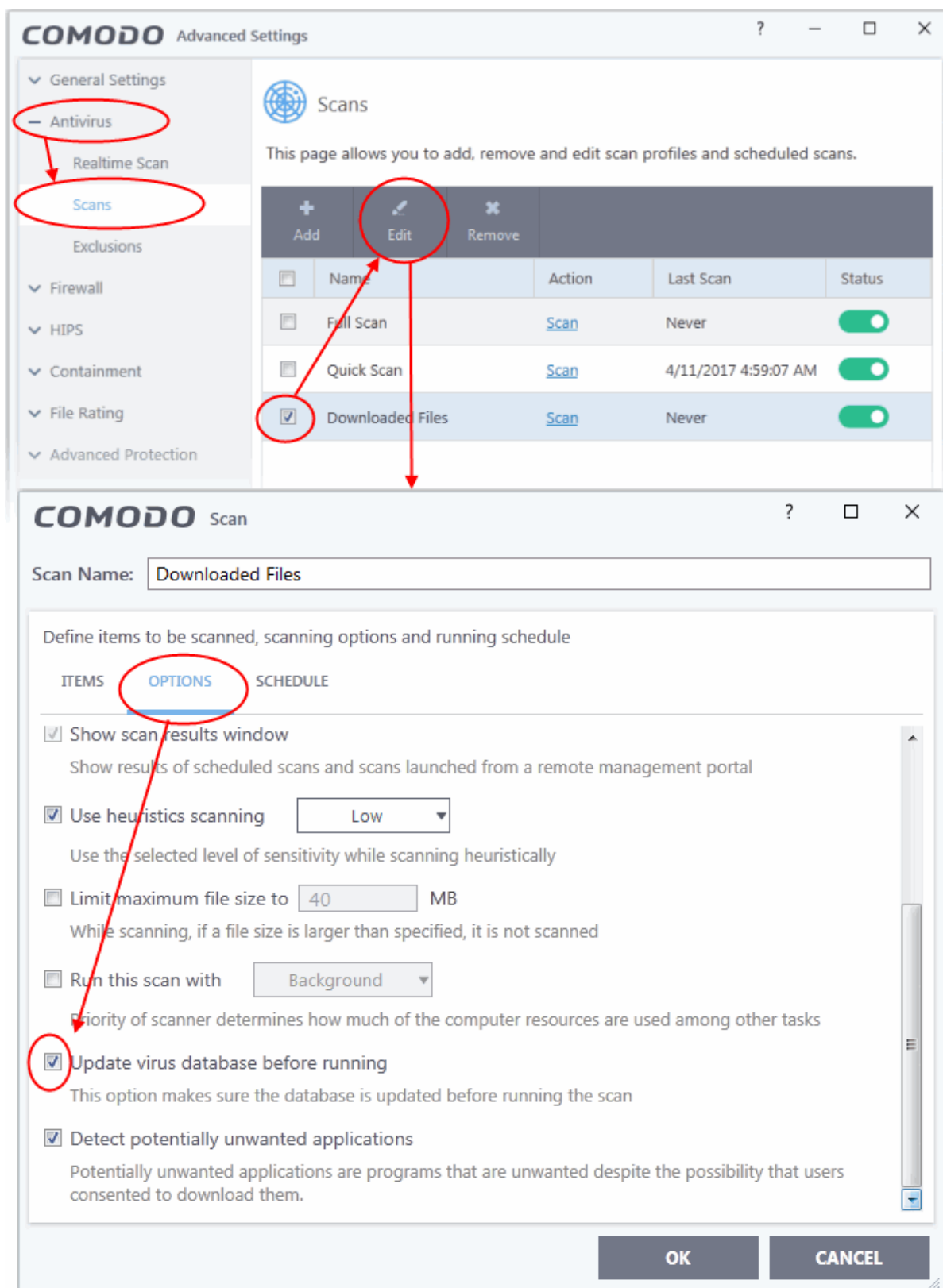
1. Click 'Settings' at the top of the CCS home screen
2. Click 'Updates' under 'General Settings' on the left



- If you want to suppress automatic updates when you are connected to internet through certain networks:
 - Select the 'Do not check updates if am using these connections' check-box.
 - Then click the 'these connections'. The 'Connections' dialog will appear with the list of connections you use.
 - Select the connection through which you do not want CCS to check for updates and click 'OK'.
- If you want to suppress automatic updates when your computer is running on battery:
 - Select the 'Do NOT check for updates if running on battery' checkbox.

To switch off automatic virus signature database updates prior to AV Scans

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Antivirus' > 'Scans'
A list defined scan profiles will be displayed.
3. Select the scan profile for which you do want the automatic virus database updates prior to the scan.



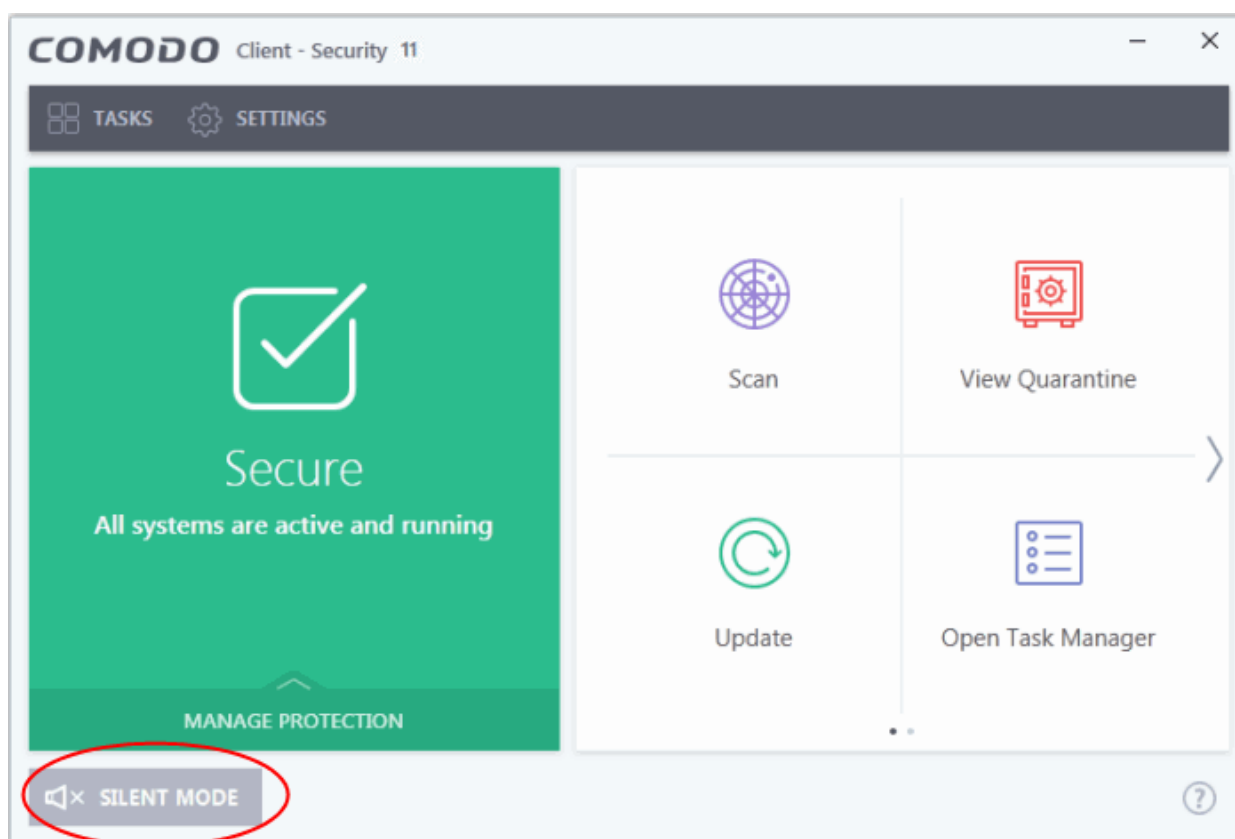
4. Click 'Edit' from the options at the top.
5. Click 'Options' > scroll down and deselect 'Update virus database before running' checkbox.
6. Click 'OK' on the 'Scan' interface.
7. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

Suppress CCS Alerts Temporarily

- CCS generates alerts if it discovers a potential security threat and also shows alerts for general system messages.
- 'Silent mode' lets you temporarily disable alerts so they don't interrupt you while playing a game or running a presentation/product demo etc.
- During this time, operations that can interfere with the user experience are either suppressed or postponed. All protection components are still 100% active in silent mode.

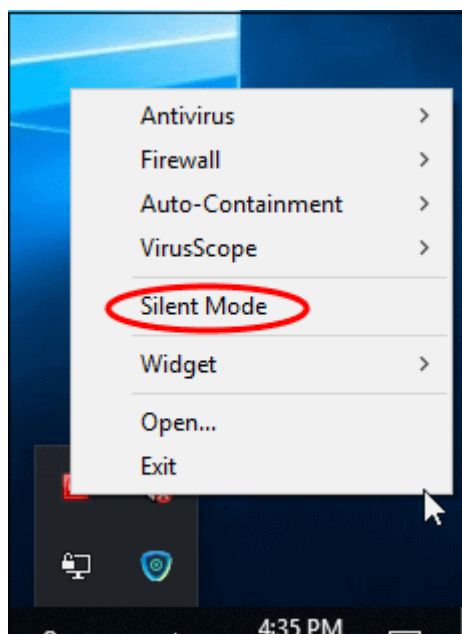
To temporarily stop pop-up alerts

- Click the 'Silent Mode' button from CCS Home screen



OR

- Right-click on the CCS system tray icon and select 'Silent Mode' from the options



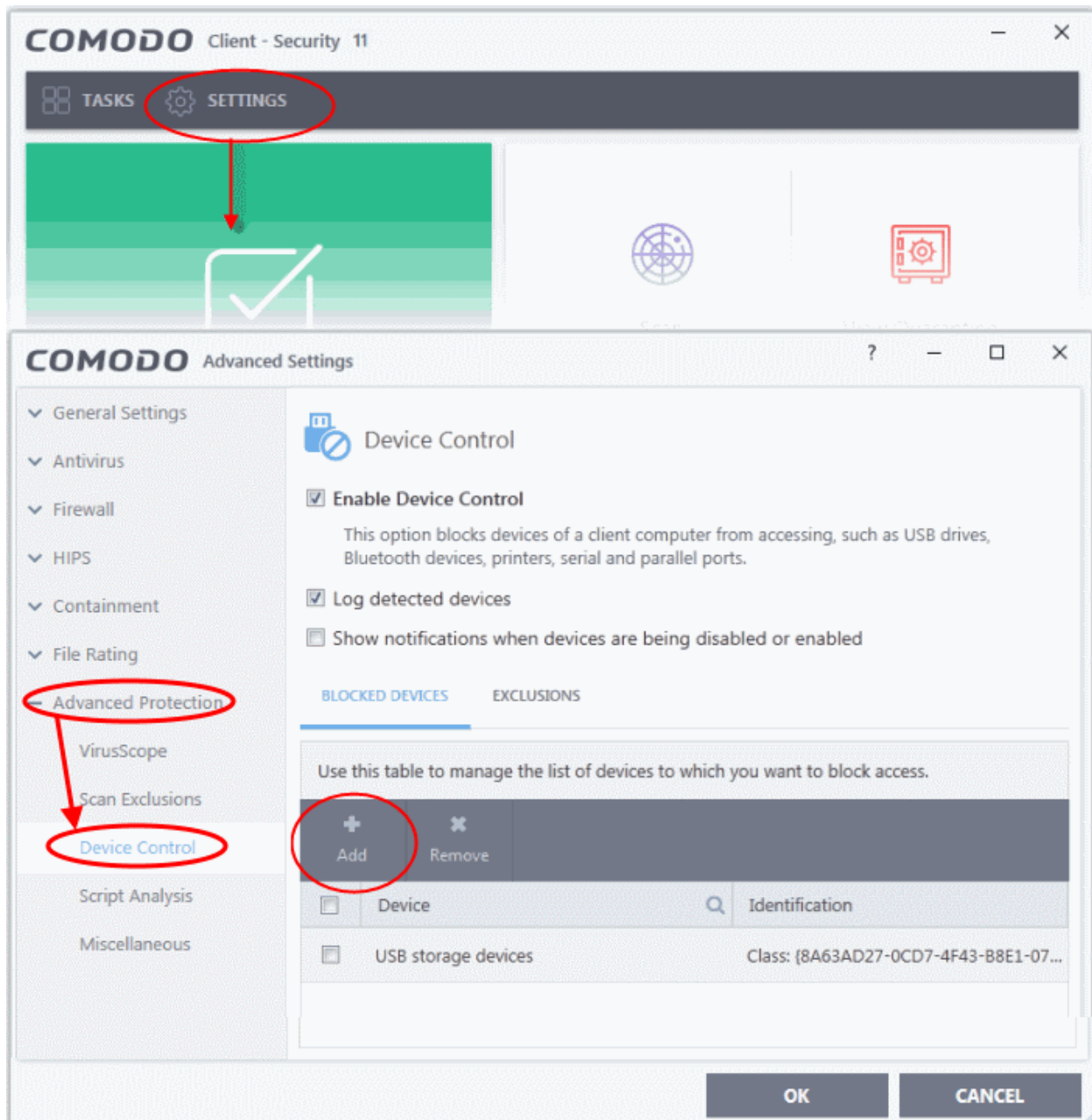
The alerts are now suppressed. To resume alerts and scheduled scans, just de-activate 'Silent Mode' from the 'Home' screen or the system tray icon right-click options.

Control External Device Accessibility

CCS helps you block external devices connected to your computer. You can block an external device by checking the 'Enable Device Control' option and then add the device class which you want to block. If you need a particular device to be given access, then you need to add the name of that device to Exclusions.

To block an external device

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Advanced Protection' > 'Device Control' on the left
3. Click 'Add' at the top to add an external device



[Click here for more details on controlling device access](#)

Appendix 2 - Comodo Secure DNS Service

Introduction

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Most of the networks use recursive DNS services that are provided by their ISP or that reside on their own set of small DNS servers but it becomes essential to have a secure and broadly distributed DNS service to have a faster and safe DNS resolution.

Background Note: Every device on the Internet is uniquely identified by a 32-bit number (IPv4) or a 128-bit number (IPv6). While this is perfectly satisfactory for computers, humans are far more comfortable remembering names rather than a string of numbers. The Domain Name System (DNS) provides the translation between those names and numbers. Virtually every piece of software, device, and service on the Internet utilizes DNS to communicate with one another. DNS also makes this information available across the entire span of the Internet, allowing users to find information remotely.

Comodo Secure DNS is a broadly distributed Recursive DNS service that gives you full control to determine how your clients interact with the Internet. It requires no hardware or software and provides reliable, faster, smarter and safer Internet experience.

- **Reliable** - Comodo Secure DNS Directory Services Platform currently spans across five continents around the world. This allows us to offer you the most reliable fully redundant DNS service anywhere. Each node has multiple servers, and is connected by several Tier 1 carriers to the Internet.
- **Faster** - Our strategically placed nodes are located at the most optimal intersections of the Internet. Unlike most DNS providers, Comodo Secure DNS Directory Services Platform uses Anycast routing technology - which means that no matter where you are located in the world, your DNS requests are answered by the closest available Comodo Secure DNS set of servers. Combine this with our huge cache and we can get the answers you seek faster and more reliably than anyone else. Furthermore, our "name cache invalidation" solution signals the Comodo Secure DNS recursive servers anytime one of our authoritative customers or partners updates a DNS record, fundamentally eliminating the concept of a TTL.
- **Smarter** - Comodo's highly structured search and guide pages get you where you want to be, when you inadvertently attempt to go to a site that doesn't exist.
- **Safer** - As a leading provider of computer security solutions, Comodo is keenly aware of the dangers that plague the Internet today. Secure DNS helps users keep safe online with its malware domain filtering feature. Secure DNS references a real-time block list (RBL) of harmful websites (i.e. phishing sites, malware sites, spyware sites, excessive advertising sites, etc.) and will warn you whenever you attempt to access a site containing potentially threatening content. Additionally, our 'name cache invalidation' solution signals the Comodo Secure DNS recursive servers whenever a DNS record is updated - fundamentally eliminating the concept of a TTL. Directing your requests through highly secure servers can also reduce your exposure to the DNS Cache Poisoning attacks that may affect everybody else using your ISP.

To start Comodo Secure DNS service the DNS settings of your computer has to be modified to point to our server's IP addresses. Comodo Client Security automatically modifies the DNS settings of your system during its installation to get the services. You can also modify the DNS settings of your system manually, if you haven't selected the option during installation. You can also revert to the previous settings if you want, at anytime.

Click the following links to get the instructions for manually modifying the DNS settings on your router or on your computer.

- [Router](#)
- [Windows XP](#)

- **Windows 7/ Windows Vista**

Router - Manually Enable or Disable 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:

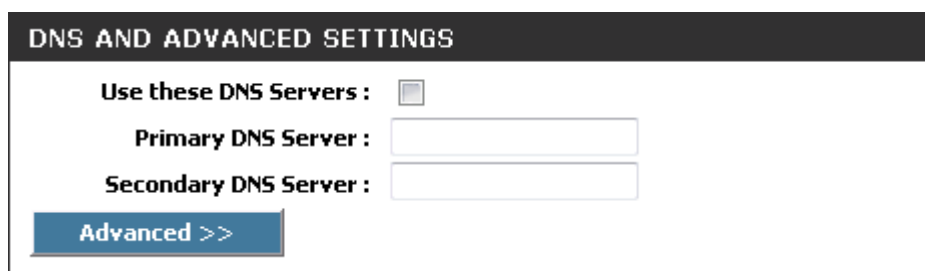
http://192.168.0.1

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).

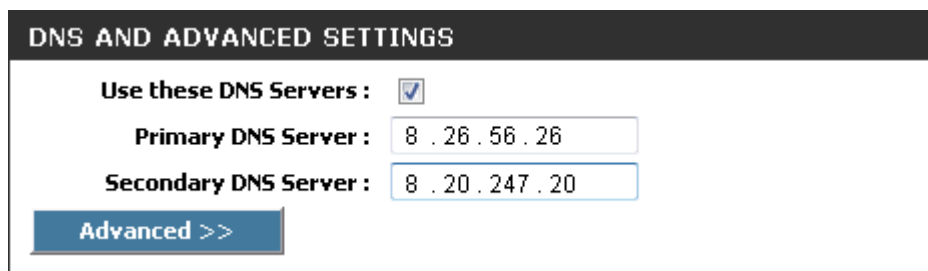


3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

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.



DNS AND ADVANCED SETTINGS

Use these DNS Servers :

Primary DNS Server : 8 . 26 . 56 . 26

Secondary DNS Server : 8 . 20 . 247 . 20

Advanced >>

You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

OR

- Entering different preferred and alternate DNS server IP addresses.

Windows XP - Manually Enable or Disable Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Windows XP computer by modifying the DNS settings accessible through Control Panel > Network Connections.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Preferred DNS : 8.26.56.26

Alternate DNS : 8.20.247.20

To stop Comodo Secure DNS service

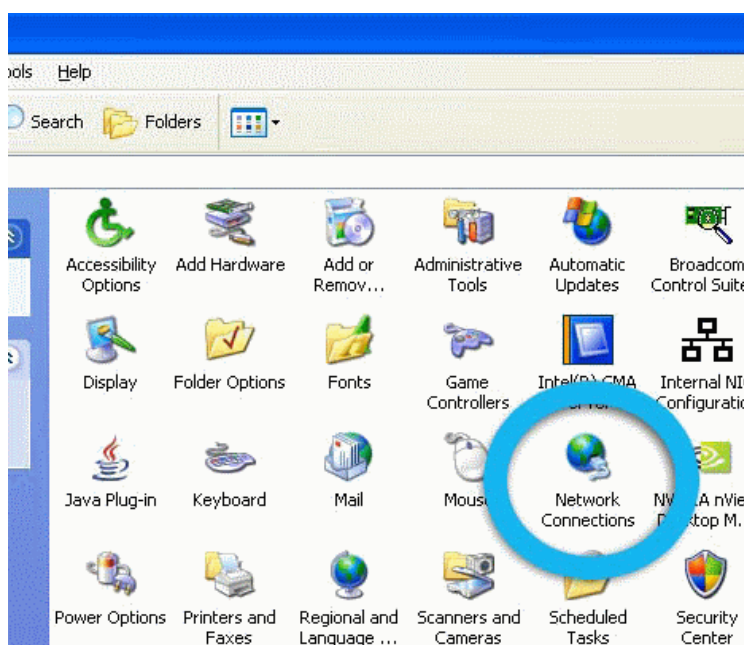
- **Modify the DNS server IP address to your previous settings.**

To modify the DNS settings

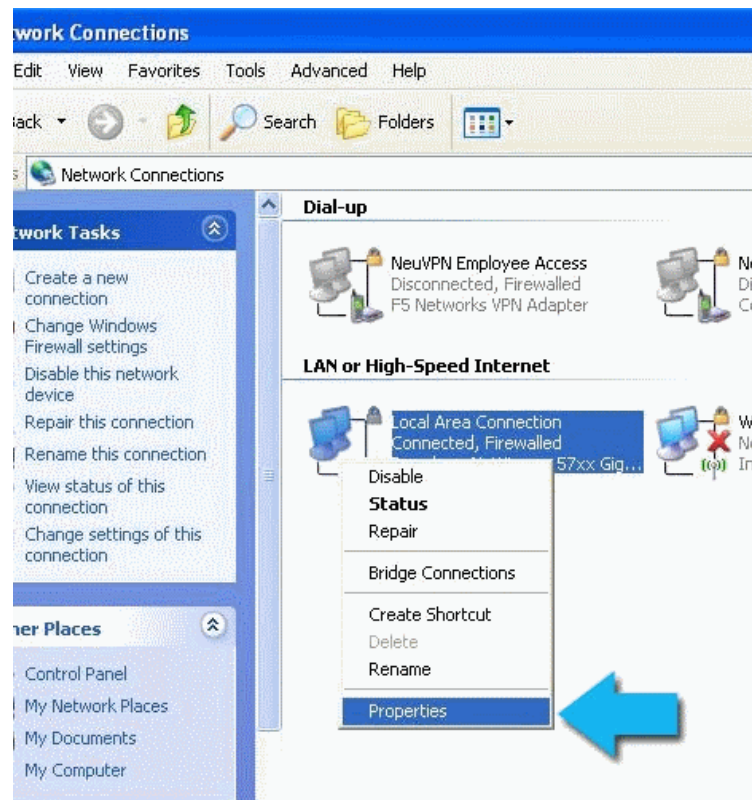
1. Select the 'Control Panel' from the Start Menu.



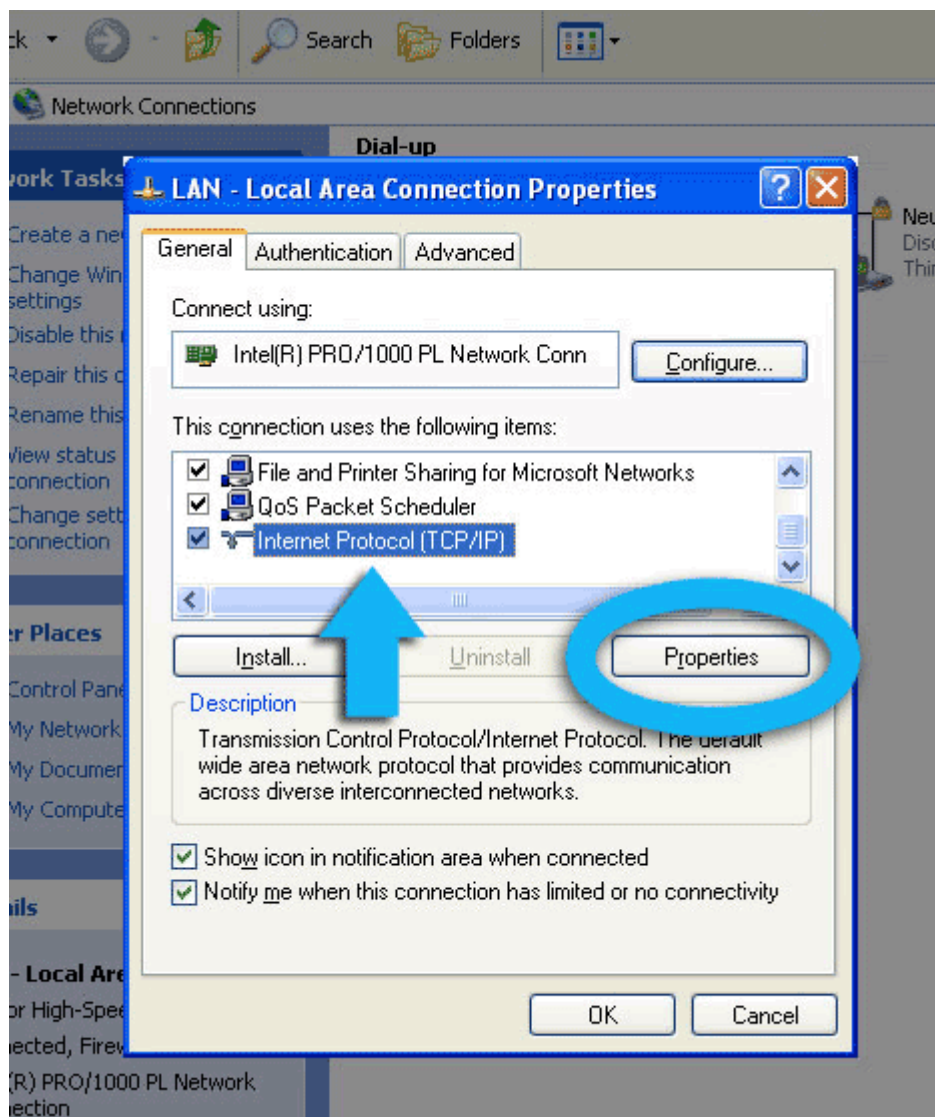
2. Click 'Network Connections' from the Control Panel options.



3. Right click on your connection from the Network Connections window and click 'Properties'.



4. Select 'Internet Protocol (TCP/IP)' and click 'Properties'.

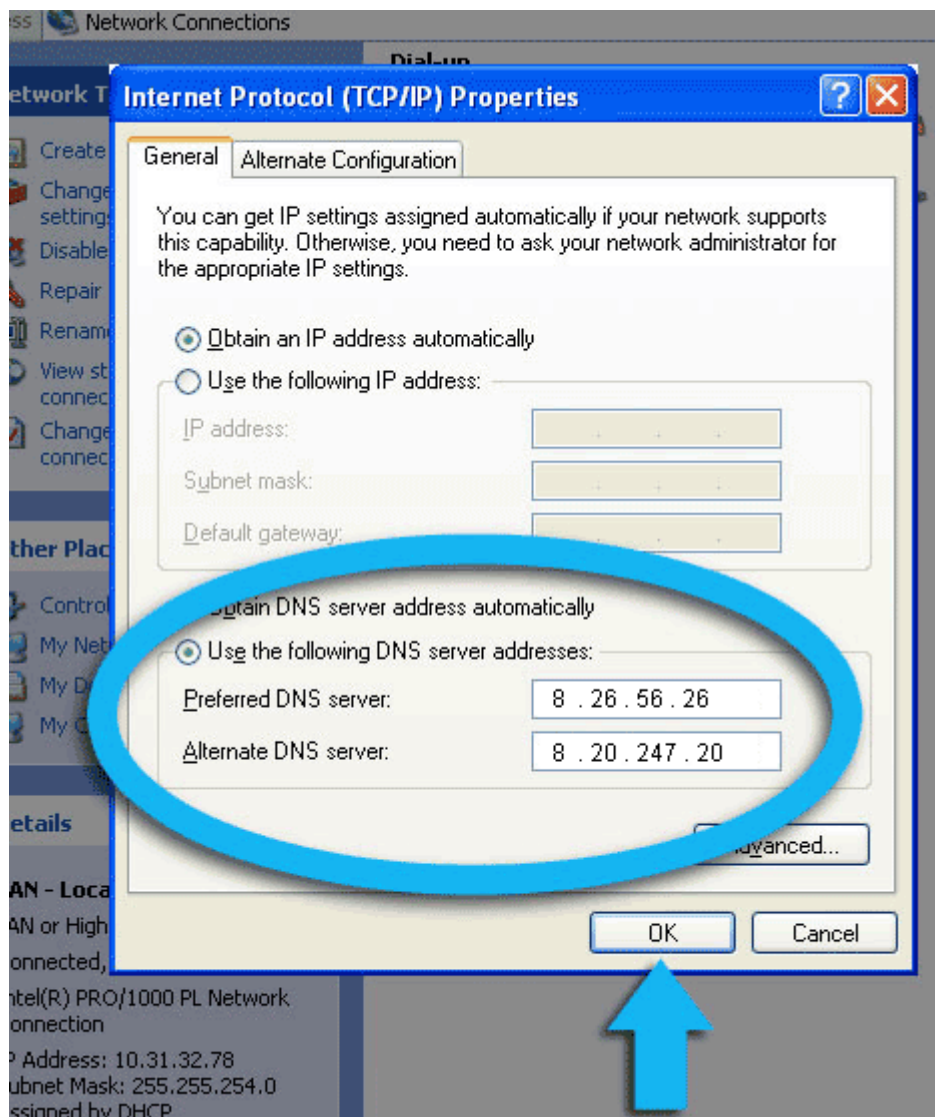


5. Click the radio button Use the following DNS server addresses and type in Comodo Secure DNS addresses in the Preferred DNS server and Alternate DNS server fields.

Please note down your current DNS settings before switching to Comodo Secure DNS, in case you want to return to your old settings for any reason.

Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26

Alternate DNS server address for Comodo Secure DNS is: 8.20.247.20

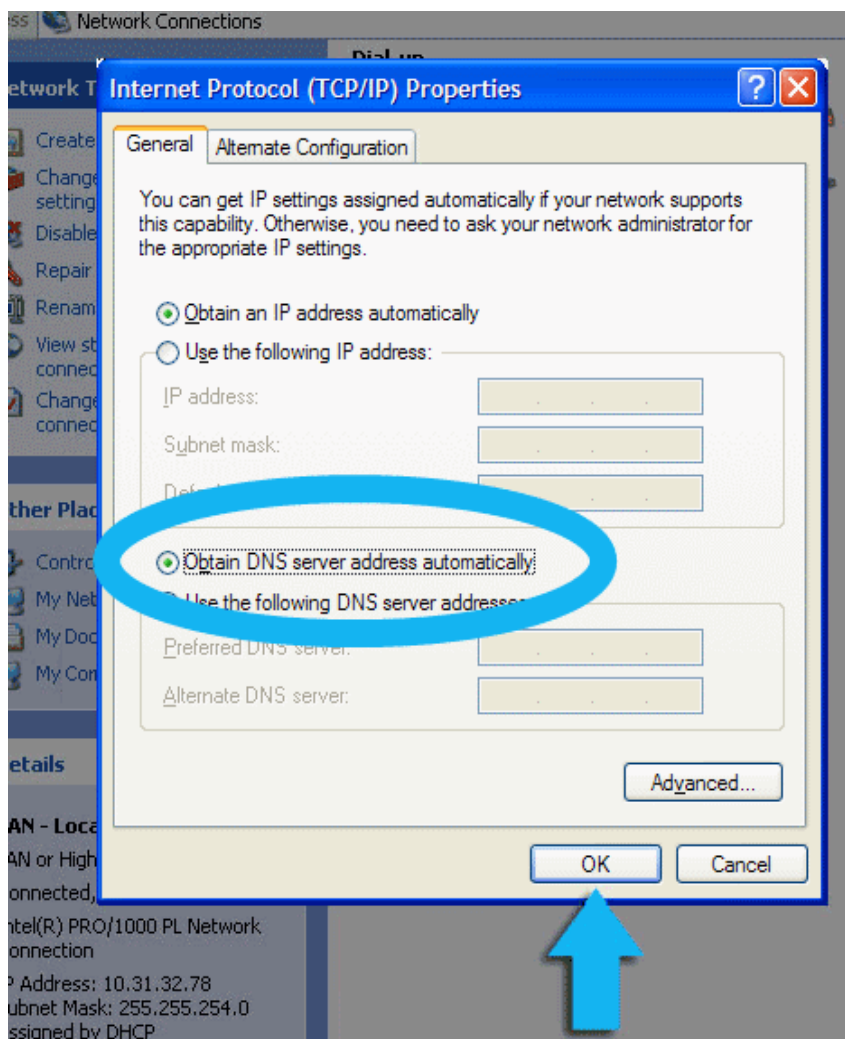


You can disable Comodo Secure DNS by:

- Selecting 'Obtain DNS server address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

OR

- Entering different preferred and alternate DNS server IP addresses.



Windows 7 / Vista - Manually Enable or Disable Comodo Secure DNS Service

You can manually enable or disable the Comodo Secure DNS service by changing your DNS server addresses to:

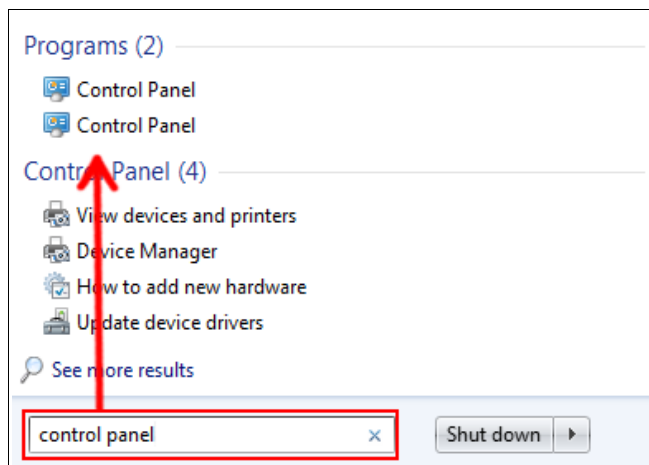
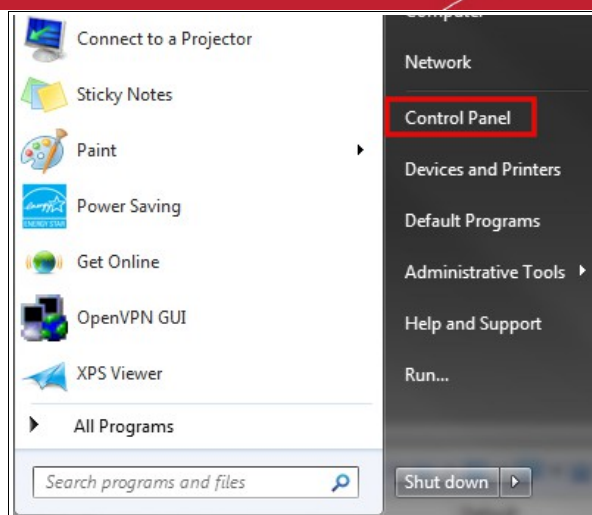
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

Enabling Comodo DNS in Windows 7 / Vista

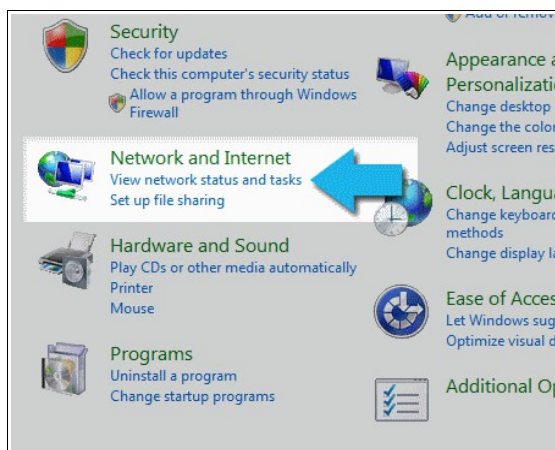
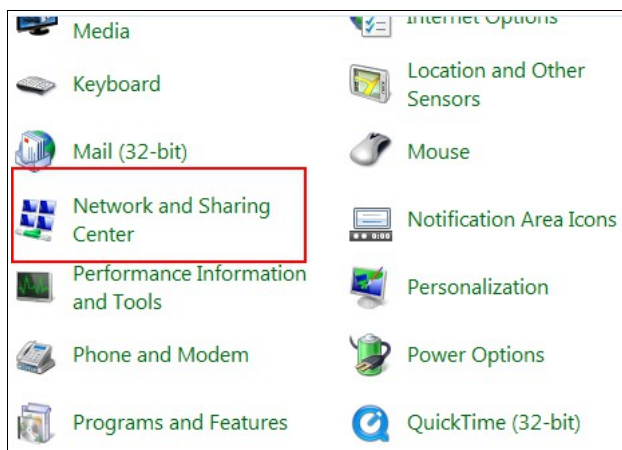
Disabling Comodo DNS in Windows 7 / Vista

Enabling Comodo DNS in Windows 7 / Vista

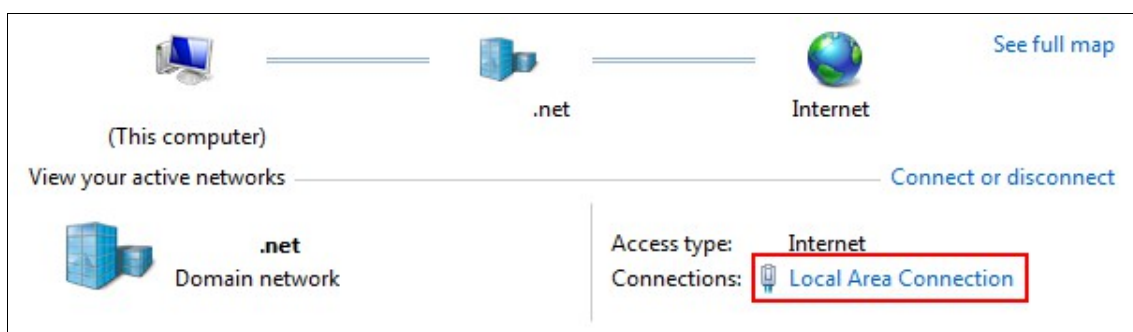
1. Open the control panel by either selecting it from the Windows 'Start' menu or by typing 'control panel' into the search box then clicking the program name.



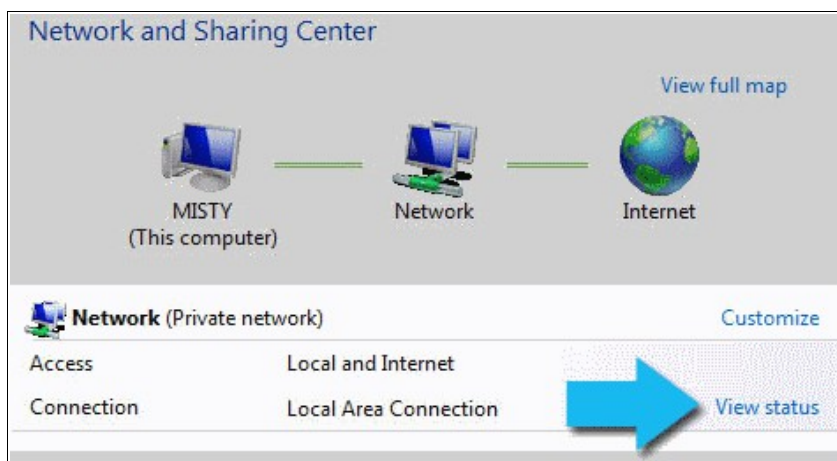
2. From the control panel menu, select 'Network and Sharing Center' (Windows 7) or 'Network and Internet' (Vista):



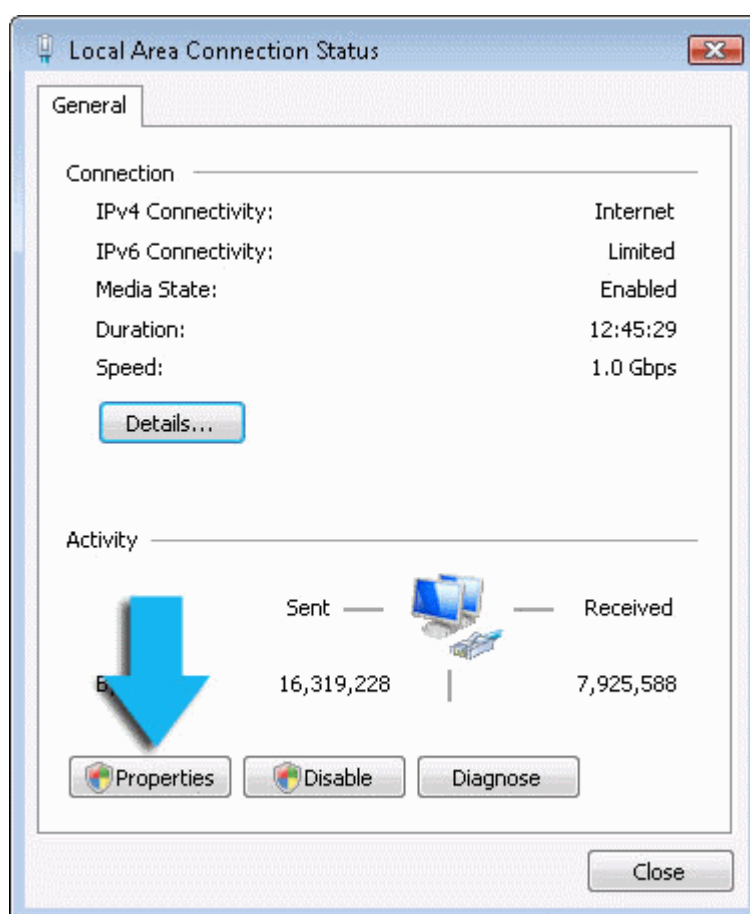
3. In the Network and Sharing center, click the connection type next to 'Connections' (Windows 7):



or 'View Status' (Vista):

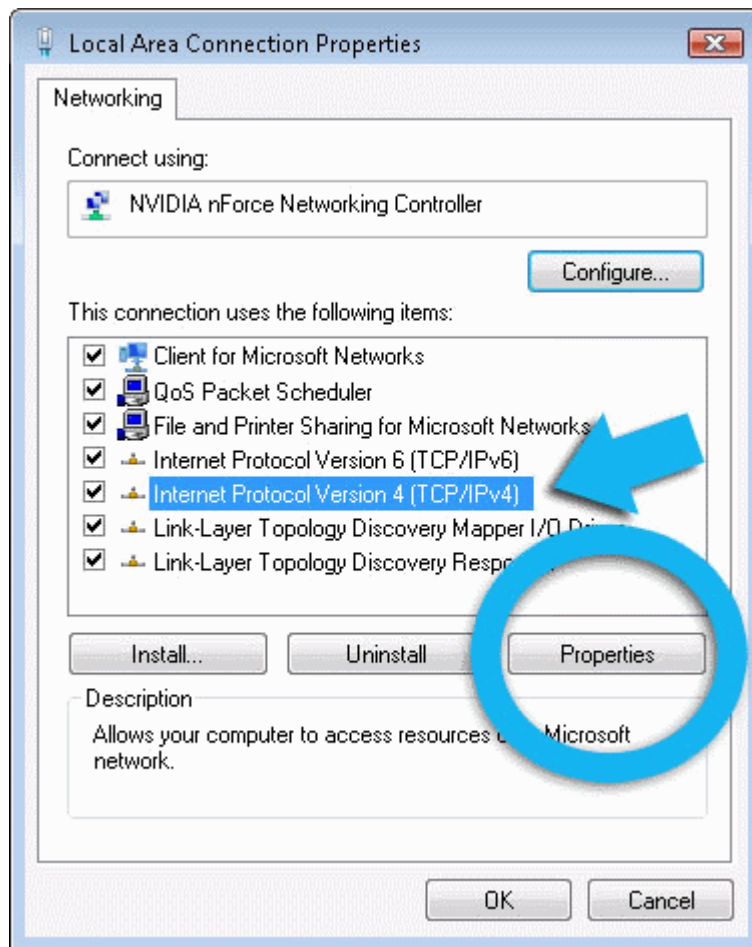


4. This will open the 'Local Area Connection Status' dialog. Click the 'Properties' button:

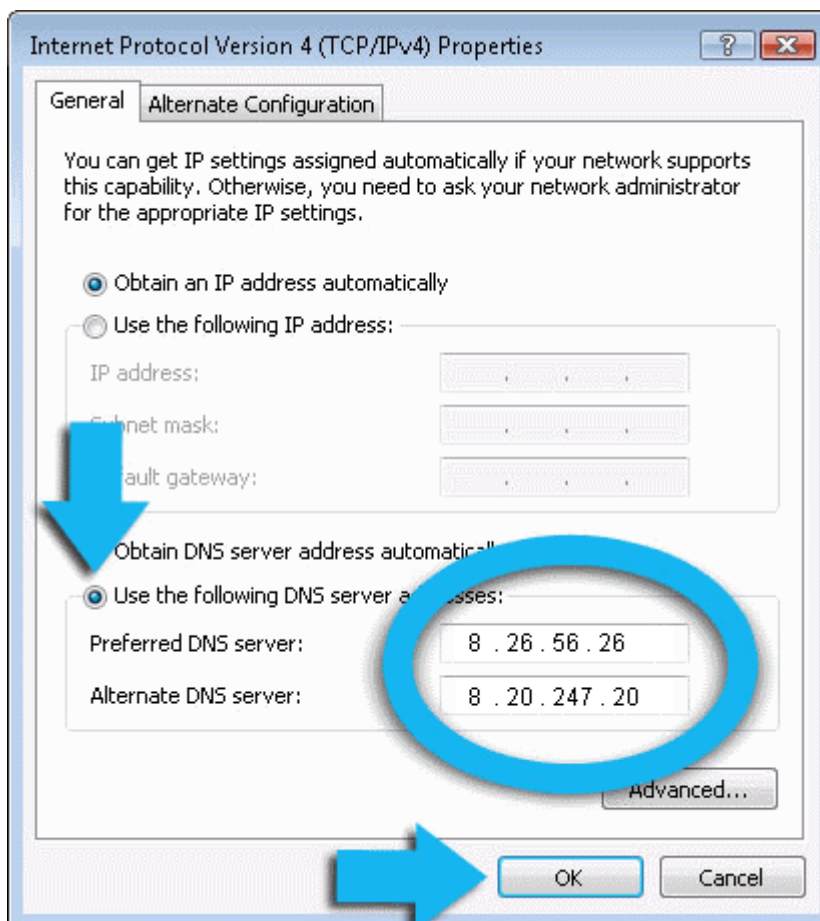


At this point, Windows might ask for your permission to continue or request that you enter an Administrator password.

5. Once you have granted permission/entered an admin password, you will be presented with the 'Local Area Connection Properties' dialog. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button:



6. Enable 'Use the following DNS server addresses'. Doing so will allow you to enter the addresses of Comodo DNS servers in the fields provided. Enter the addresses listed below then click 'OK' to activate your settings:
 - Preferred DNS : 8.26.56.26
 - Alternate DNS : 8.20.247.20

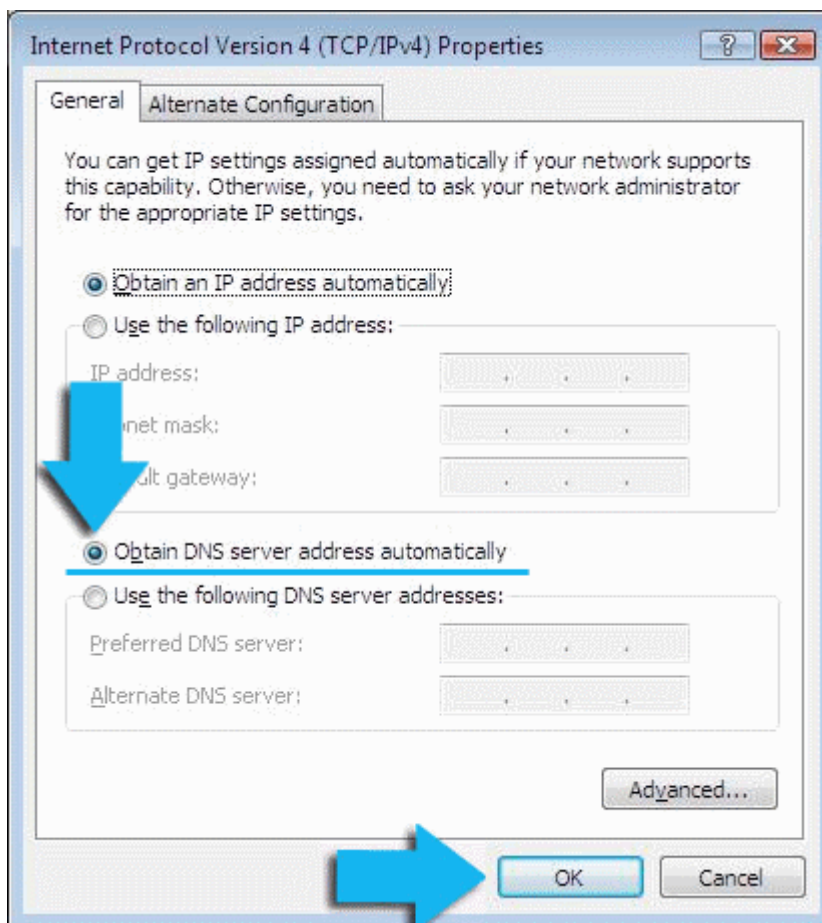


Your computer will now use Comodo DNS as its default domain name resolution service for all applications that connect to the Internet.

Disabling Comodo DNS in Windows 7 / Vista

To disable Comodo DNS, you need to instruct Windows to automatically obtain the address of a DNS server. Doing so means you will use the DNS server provided by your ISP. To do this:

- Follow steps 1 to 7 of the '[Enabling Comodo DNS in Windows 7 / Vista](#)' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

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](https://www.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