COMODO
Creating Trust Online®

COMODO
IT & SECURITY MANAGER

Comodo **Client Security**

Software Version 8.3

User Guide

Guide Version 8.3.052317

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

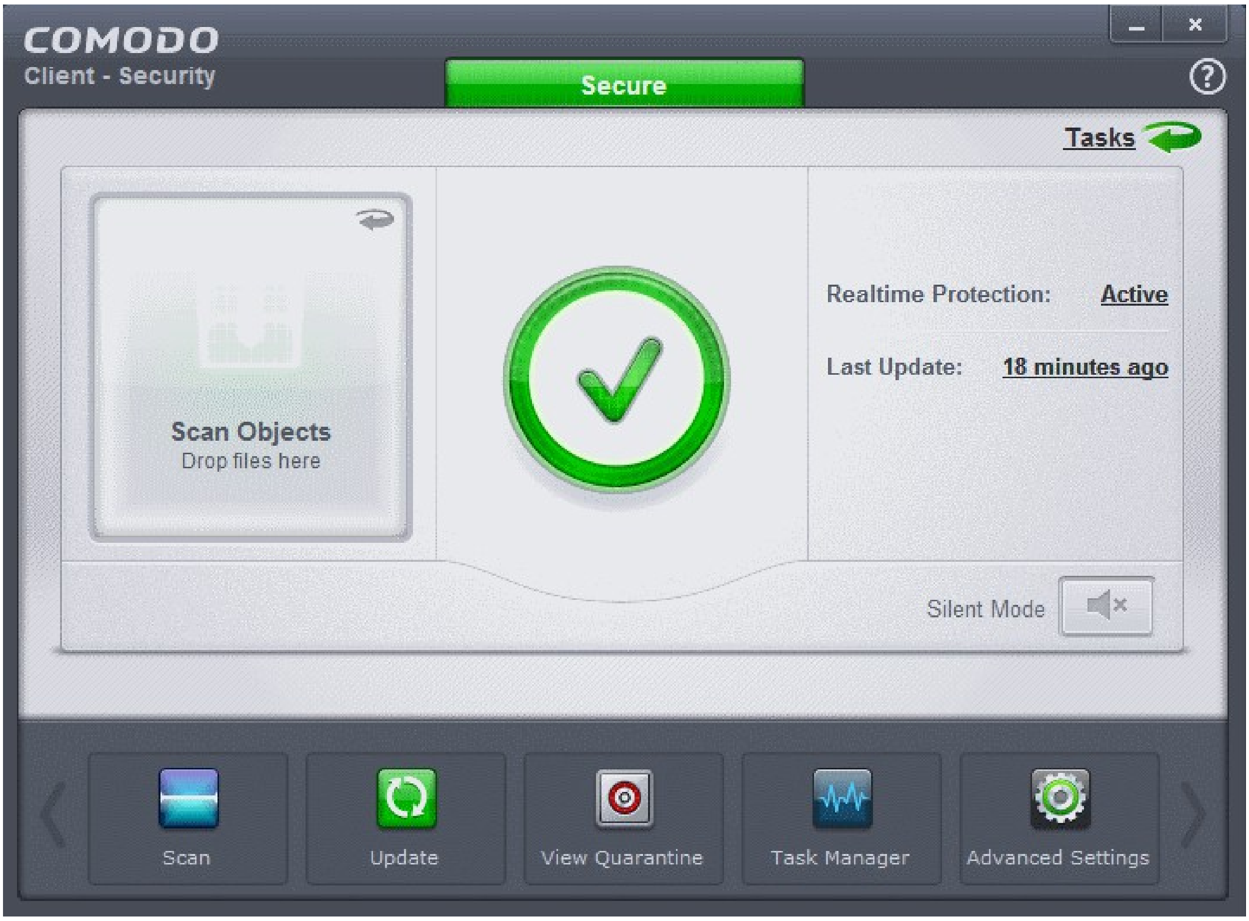
Table of Contents

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 called Advanced Protection.

When used individually, each of the Antivirus, Advanced Protection, Firewall and Containment 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 Comodo IT and Security 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.
- **Advanced Protection** - A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user 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.

    - **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.
    - **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.

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

1.1. Special Features

Containment

- Authenticates the integrity of every program before allowing it to load into your computer's memory
- Automatically runs unknown files inside a secure container which is isolated from the rest of your computer
- Cloud based behavior analysis helps identify zero-day malware before traditional antivirus
- Alerts you every time an unknown or untrusted applications attempts to run or install
- Prevents unauthorized modification of critical operating system files and registry entries

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

- Virtually Bulletproof protection against root-kits, inter-process memory injections, key-loggers and more;

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

Comprehensive Antivirus Protection

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

Intuitive Graphical User Interface

- 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

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

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

Windows XP (Both 32-bit and 64-bit versions)	• 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

CCS rates files appropriately during scanning and submits unrecognized files to Comodo servers for further analysis. In order for the software to submit unknown files to our file rating and Comodo Automated Malware Analysis System (CAMAS) servers, please make sure the following IP addresses and ports are allowed on your network firewall:

- To allow communication with camas.comodo.com
  - IP that needs to be allowed: 199.66.201.30
  - Port that needs to be allowed: port 80 for TCP
  - Direction: Outgoing (Endpoints to CAMAS)
- 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: 4447 UDP and 4448 TCP
  - Direction: Outgoing (Endpoints to FLSs)

1.3. Installing Comodo Client Security

Note - Before beginning installation, please ensure you have uninstalled any other antivirus products that are on your server. 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.

Comodo Client Security is part of Comodo IT and Security Manager (ITSM) and can be deployed onto endpoints via the ITSM management interface. You can subscribe for ITSM as stand-alone application or as a part of the Comodo One (C1) application. If you do not already have an ITSM license, then please see the following links:

- To sign up for Comodo One, see https://one.comodo.com/
- To subscribe for ITSM as stand-alone, visit https://secure.comodo.com/home/purchase.php?pid=98&license=try for the trial version and https://secure.comodo.com/home/purchase.php?pid=98 for the full version.

C1 customers can open ITSM by clicking 'Licensed Applications > 'IT and Security Manager'. Stand-alone customers can access the ITSM interface by entering the URL they were provided with after sign up into any web browser.

The following steps explain how to deploy CCS onto endpoints:

- Step 1 - Enroll Users
- Step 2 – Enroll Devices

- Step 3 – Deploy CCS

Step 1 – Enroll Users

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

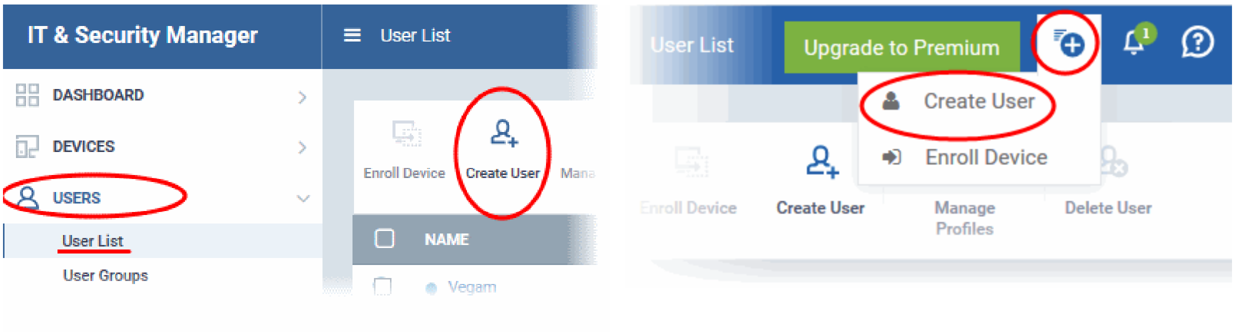
- **Comodo One users** - If you created only one company in C1, then any users you enroll here will be automatically assigned to that company. If you created more than one company, the 'Enroll User' dialog will allow you to choose the company to which you want to assign the user.
- **ITSM Users** - You can add users and enroll their devices without selecting any company. However, If you need the users/devices to be grouped under different companies, you can create companies in ITSM and add device groups.

To add a user

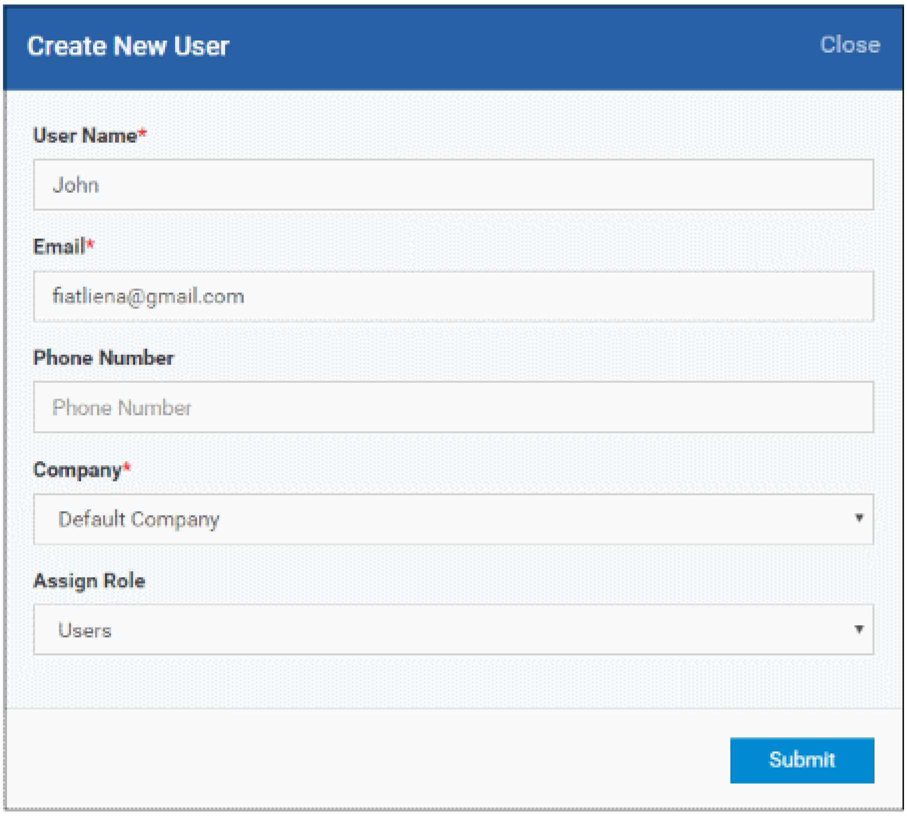
- Click 'Users' on the left then 'User List', then click the 'Create User' button

  or

- Click the 'Add' button ⊕ at the menu bar and choose 'Create User'.



The 'Create new user' form will open.



Create New User Close

User Name*: John

Email*: fiatliena@gmail.com

Phone Number: Phone Number

Company*: Default Company

Assign Role: Users

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- Choose the company (mandatory), from the 'Company' drop-down.
    - Comodo One Users - The drop-down will display the companies added to C1. You can choose the company to which the user belongs. The user will be enrolled under the chosen company.
    - ITSM users - Leave the selection as 'Default Company'.
- Choose a role for the user. A 'role' determines user permissions within the ITSM console itself. ITSM ships with two default roles:
    - **Administrators** - Full administrative privileges in the ITSM 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 ITSM.
- Click 'Submit' to add the user to ITSM.
- Repeat the process to add more number of users.
- New users will be listed in the 'Users' interface (click 'Users' > 'User List')

Step 2 – Enroll Devices

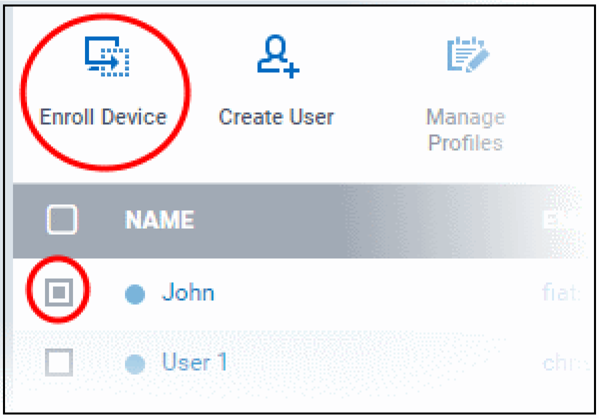
The next step is to enroll users' devices for management.

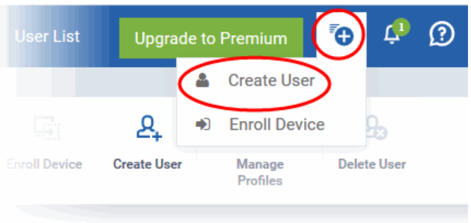
To enroll devices

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

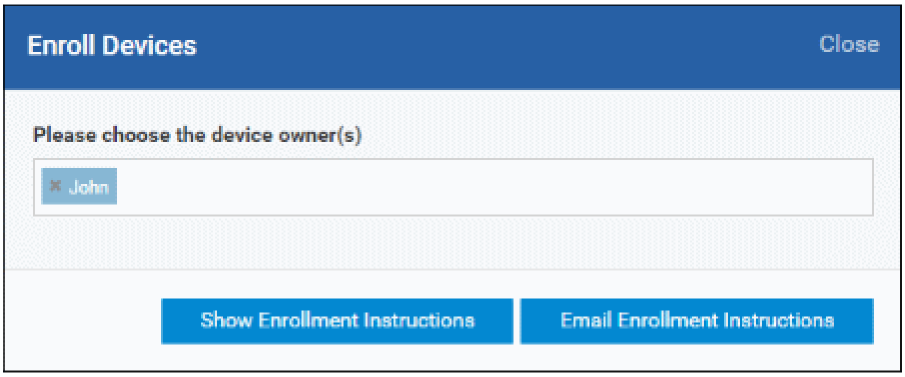
  Or

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



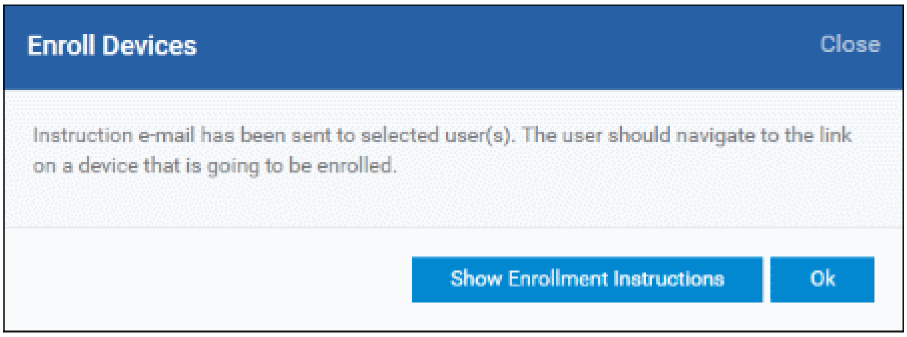


The 'Enroll Devices' dialog will open for the chosen users.


Enroll Devices
Close
Please choose the device owner(s)
John
Show Enrollment Instructions
Email Enrollment Instructions

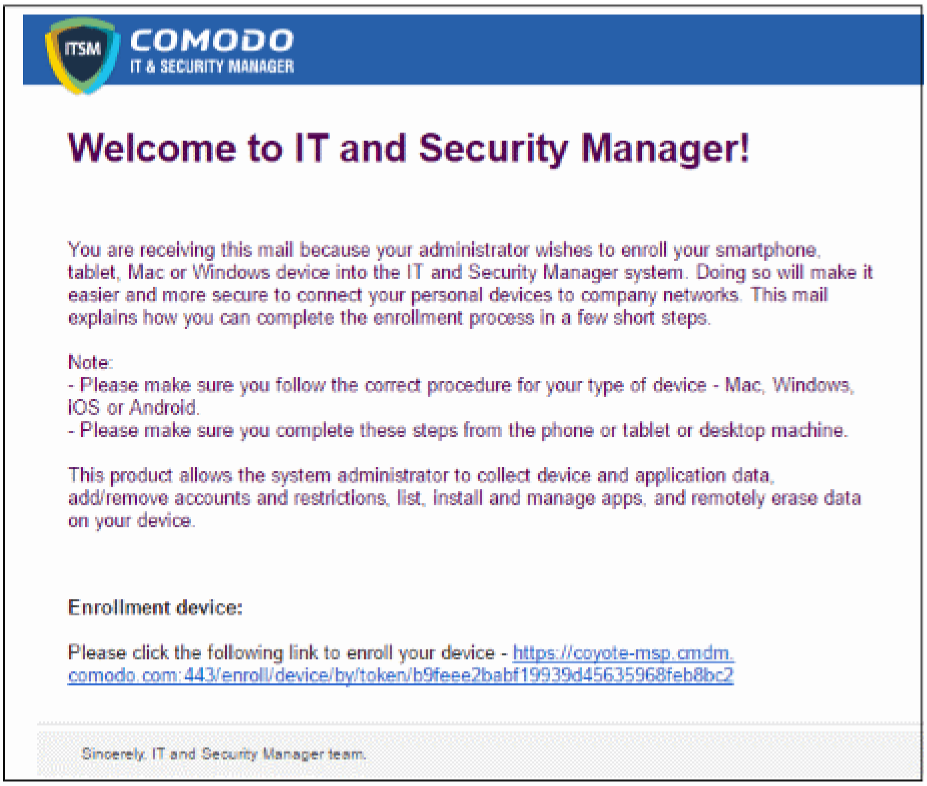
The 'Please choose the device owner(s)' field is pre-populated with any users you selected in the previous step.

- To add more users, start typing first few letters of the username and choose from the results
- If you want to see help on the enrollment process, click 'Show Enrollment Instructions'. This is useful for administrators attempting to enroll their own devices.
- If you want the enrollment instructions to be sent as an email to users, click 'Email Enrollment Instructions'.
- A confirmation dialog will be displayed.



Instruction e-mail has been sent to selected user(s). The user should navigate to the link on a device that is going to be enrolled.

A device enrollment email will be sent to each user. The email contains instructions that will allow them to enroll their device. An example mail is shown below.



COMODO IT & SECURITY MANAGER

Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, Mac or Windows device into the IT and Security 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:
- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

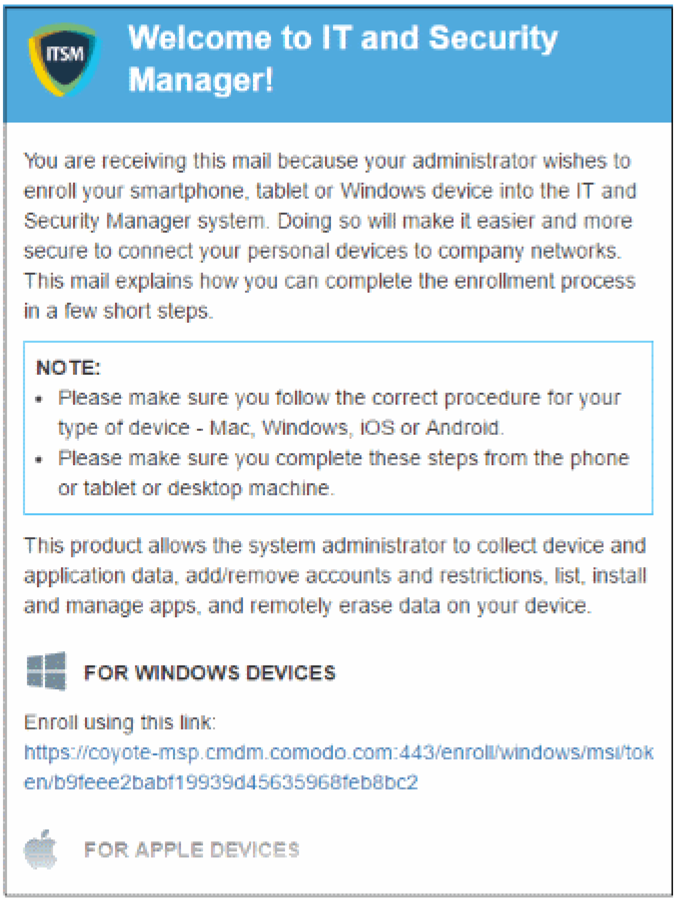
This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

Enrollment device:

Please click the following link to enroll your device - https://coyote-msp.cmdm.comodo.com:443/enroll/device/by/token/b9feee2babf19939d45635968feb8bc2

Sincerely, IT and Security Manager team.

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



Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the IT and Security 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:
- Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.
- Please make sure you complete these steps from the phone or 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://coyote-msp.cmdm.comodo.com:443/enroll/windows/msi/token/b9feee2babf19939d45635968feb8bc2

FOR APPLE DEVICES

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

The ITSM 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 ITSM and a confirmation message will be displayed. Once the device is enrolled, the next step is to install CCS onto the endpoint.

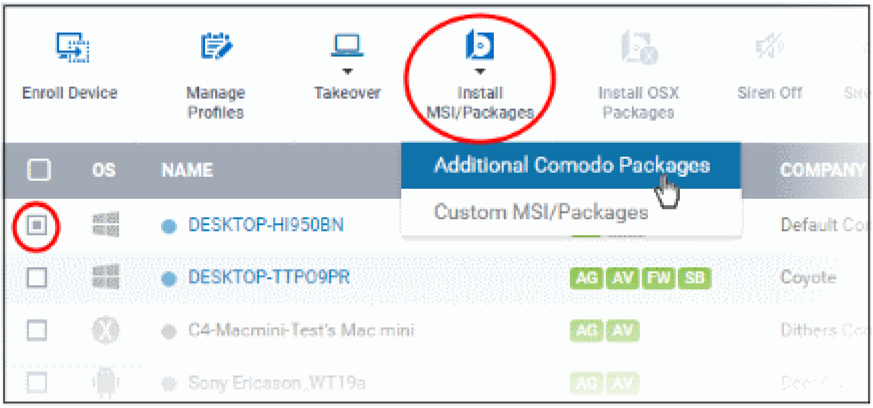
Background Note on ITSM Agent: The ITSM agent is a small application installed on every managed endpoint to facilitate communication between the endpoint and the ITSM central server. The agent is responsible for receiving tasks and passing them to the endpoint's installation of Comodo Security Software (CCS, CAVS or CAV for Mac). 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, endpoint agents can only communicate with the specific instance of the central service which provisioned the agent. This means the agent cannot be reconfigured to connect to any other ITSM service.

Step 3 – Deploy Comodo Client Security

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

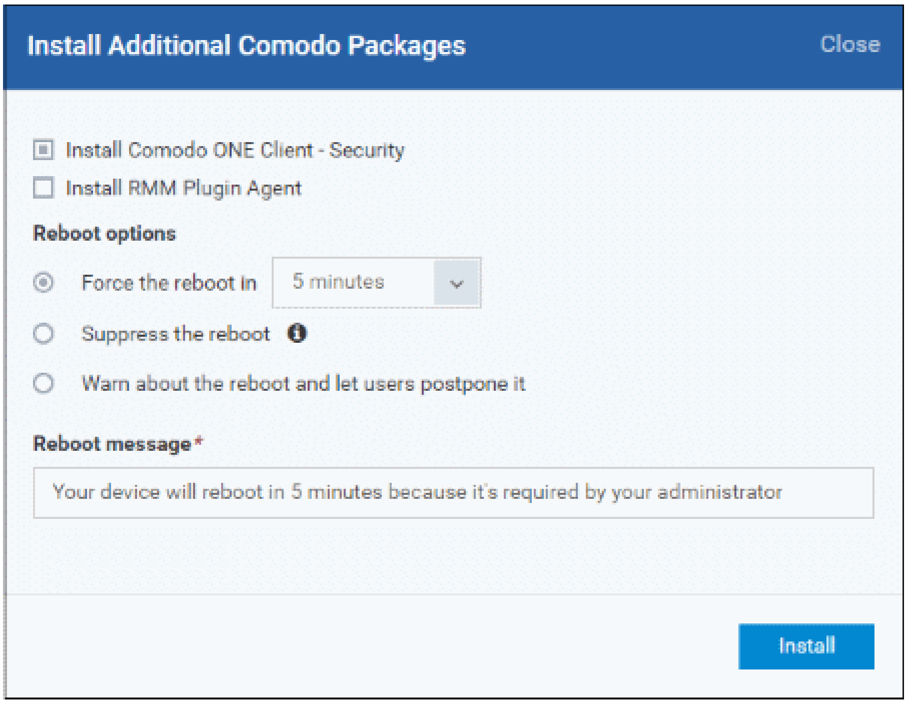
To install CCS

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



	OS	NAME		COMPANY
☒		DESKTOP-HI950BN		Default Co
□		DESKTOP-TTPO9PR	AG AV FW SB	Coyote
□		C4-Macmini-Test's Mac mini	AG AV	Dithers Co
□		Sony Ericsson WT19a	AG AV	

- Click 'Install MSI/Packages' > 'Additional Comodo Packages'


Install Additional Comodo Packages Close

☒ Install Comodo ONE Client - Security
□ Install RMM Plugin Agent

Reboot options

● Force the reboot in 5 minutes
○ Suppress the reboot
○ Warn about the reboot and let users postpone it

Reboot message*

Your device will reboot in 5 minutes because it's required by your administrator

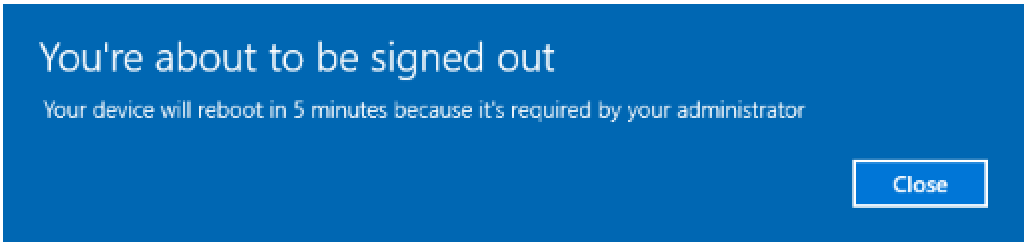
Install

- 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:


You're about to be signed out

Your device will reboot in 5 minutes because it's required by your administrator

Close

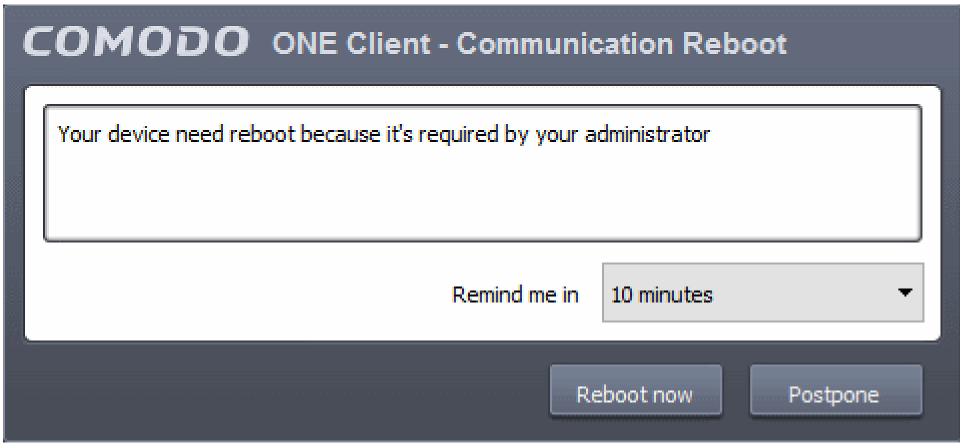
The device will be restarted automatically when the time period elapses.

- 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:



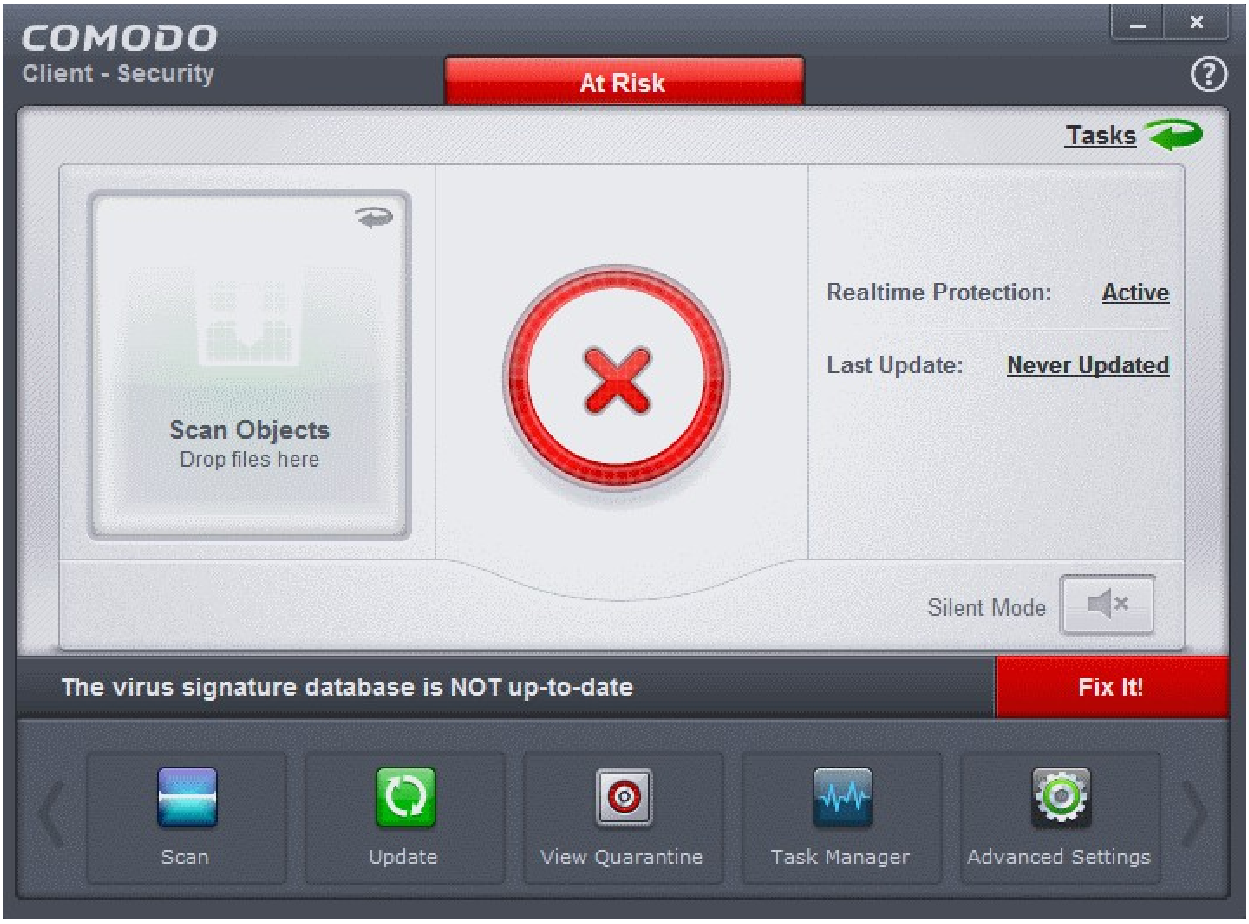
COMODO ONE Client - Communication Reboot

Your device need reboot because it's required by your administrator

Remind me in: 10 minutes

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 ITSM profile.

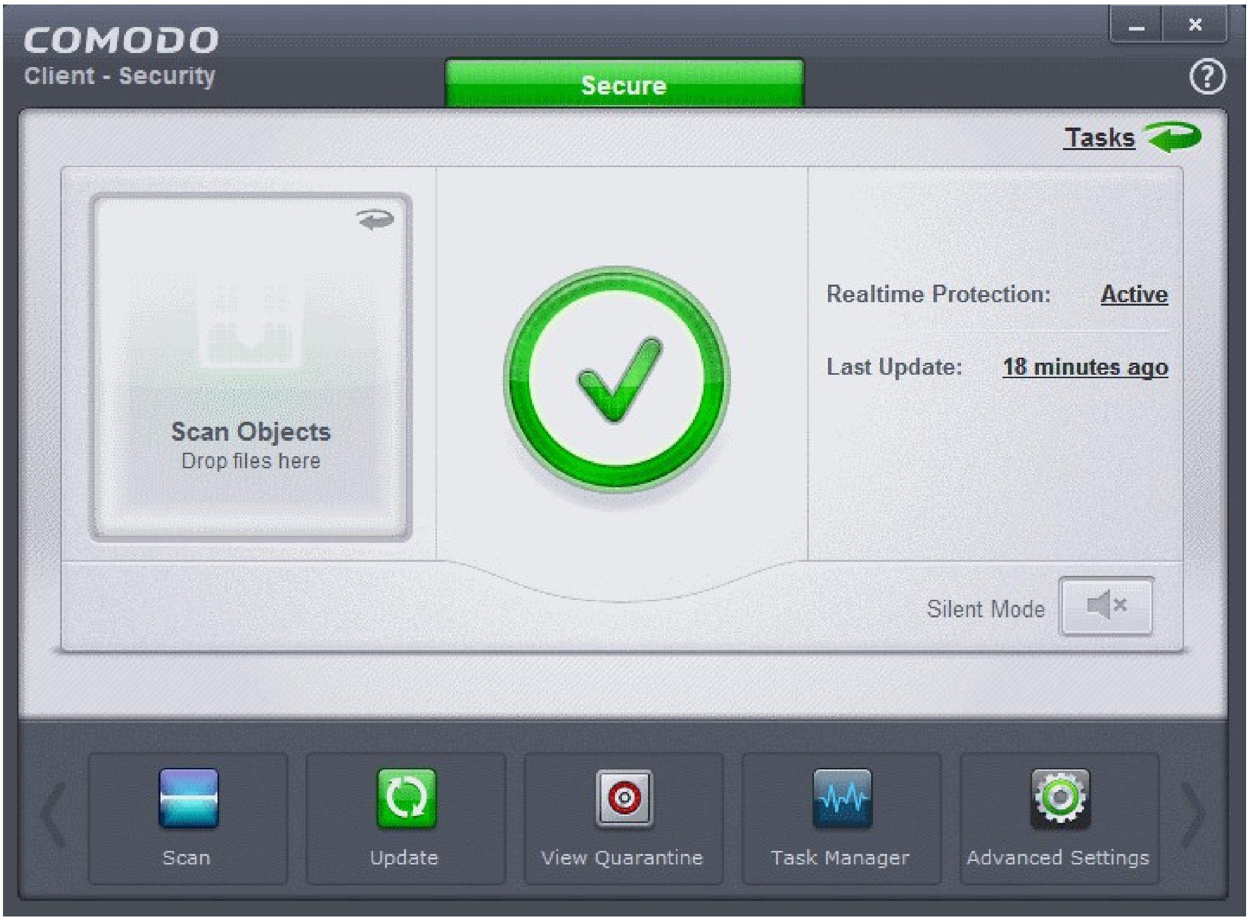


Realtime Protection: Active

Last Update: Never Updated

The virus signature database is NOT up-to-date

The virus database will be updated automatically for the first time after installation.



1.4. Starting 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 4 different ways to access the main interface of Comodo Client Security:

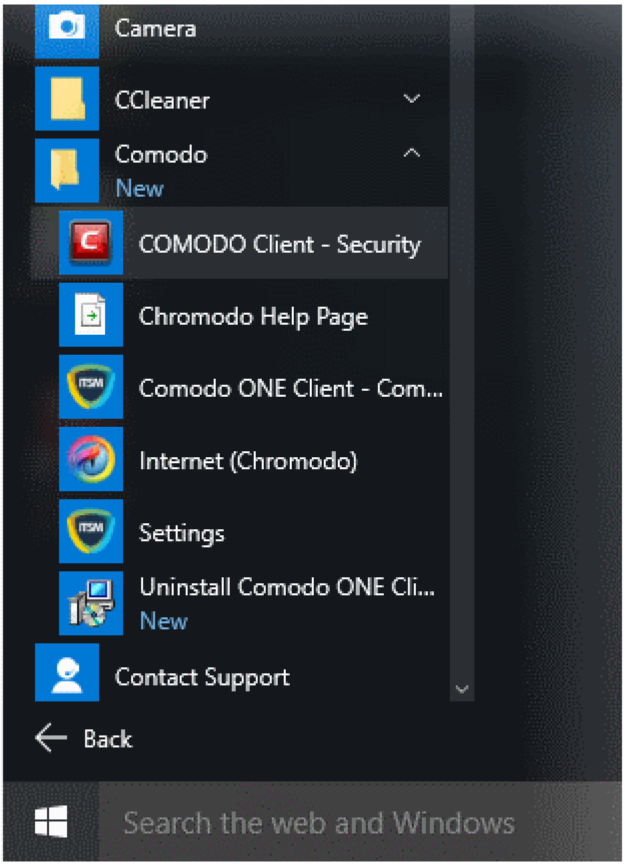
- Windows Start Menu
- Windows Desktop
- Widget
- System Tray Icon

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.)

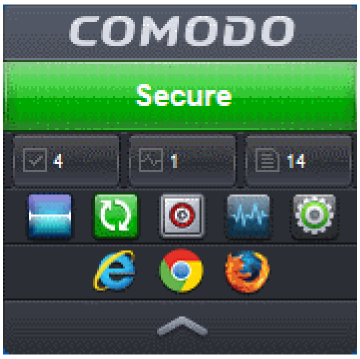


Windows Desktop

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

Widget

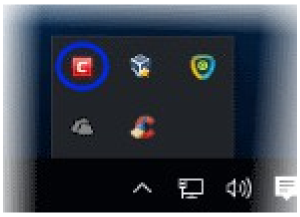
- Just click the information bar in the widget to start CCS.



The widget also contains other useful data and features. Refer to the section '**The Widget**' for more details.

CCS Tray Icon

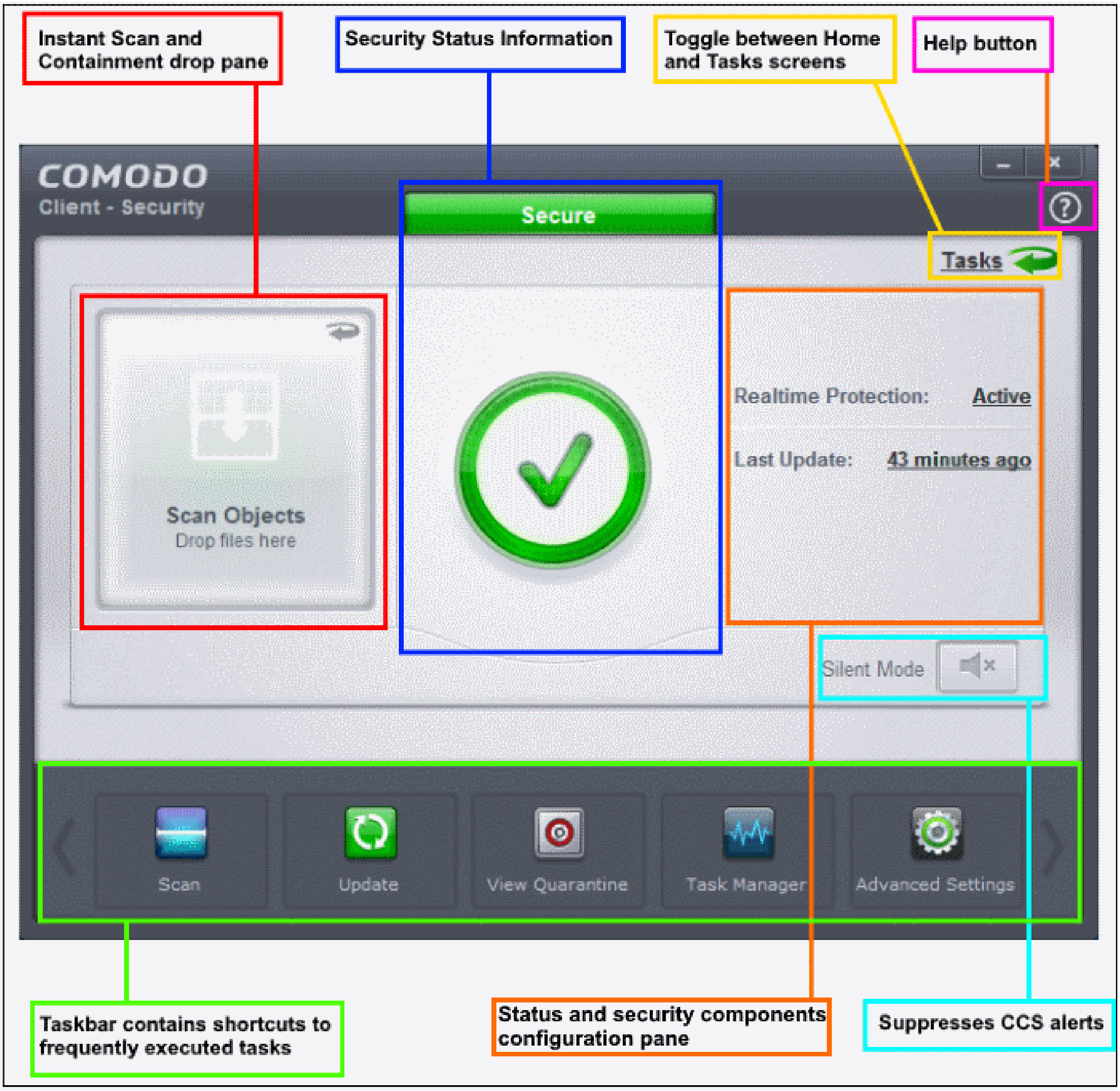
- Just double click the shield icon to start the main interface.



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

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 curved arrow on the upper right lets you switch between the home screen and the more advanced tasks interface. You can instantly run a virus scan on a file or folder by dragging it into the scan box while 'Silent Mode' means you will not be interrupted by CCS messages while you perform other tasks. The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the update checker and the CCS Task Manager.


Instant Scan and Containment drop pane
Security Status Information
Toggle between Home and Tasks screens
Help button
COMODO
Client - Security
Secure
Tasks
Scan Objects
Drop files here
Realtime Protection: Active
Last Update: 43 minutes ago
Silent Mode
Scan
Update
View Quarantine
Task Manager
Advanced Settings
Taskbar contains shortcuts to frequently executed tasks
Status and security components configuration pane
Suppresses CCS alerts

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

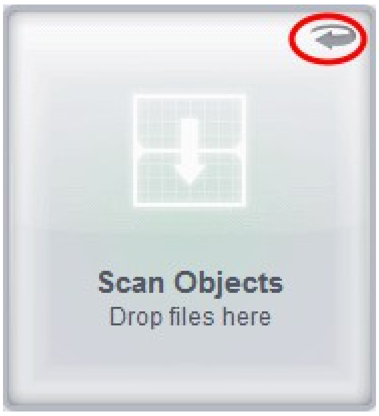
The main interface of CCS can be flipped to display the 'Home' screen or the 'Tasks' interface. Click the curved green arrow at the upper right of the interface to switch between home screen and tasks interface.

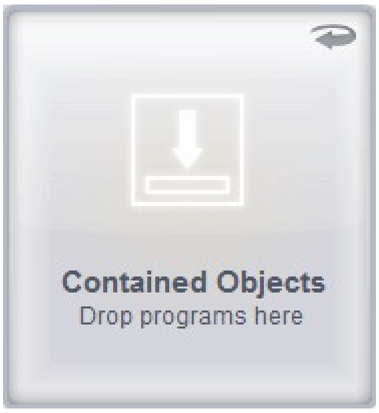
The home screen allows you to carry out various tasks and also provides information about security components. On the left side of the home screen there is an instant virus scan box into which you can drag-and-drop files, folders or drives. If you flip this box, you can drag-and-drop programs here to run them in the container. The pane on the right displays update status and real-time protection status. Clicking on the real-time protection status will flip the pane and allow you to switch individual security components on or off. The Task Bar at the bottom of the home screen allows you to add frequently executed tasks so that you can run any of the tasks with a single mouse click. Click the links below to find out more about the home screen:

- Instantly scan objects / run a program in the container
- Enable or disable security components
- Adding tasks to the Task Bar
- Silent mode
- Get Help

Instantly scan objects / run a program in the container

The pane on the left side of the home screen flips between an instant virus scanner and an instant container:



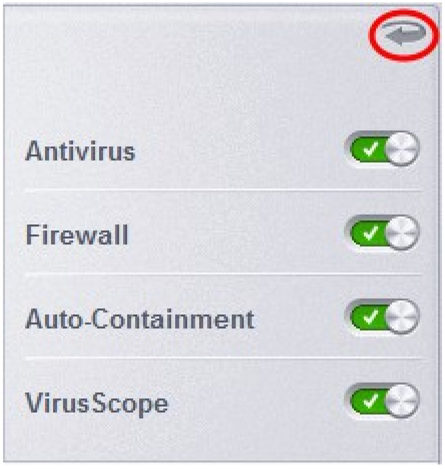


To run an instant scan, navigate to the file/folder you want to scan and drag the file into the 'Scan Objects' box. The virus scan will start immediately. Refer to 'Instantly Scan Individual Files and Folders' for more details.

Click the curved arrow at the top right if you want to quickly run a program in the container instead. Refer to 'Run an application in the Container' for more details.

Enable or disable security components

The flippable pane on the right allows you to selectively enable or disable real-time antivirus, the firewall, auto-containment and/or VirusScope. The other side of the pane displays the status of real-time protection and when the virus database was last updated.

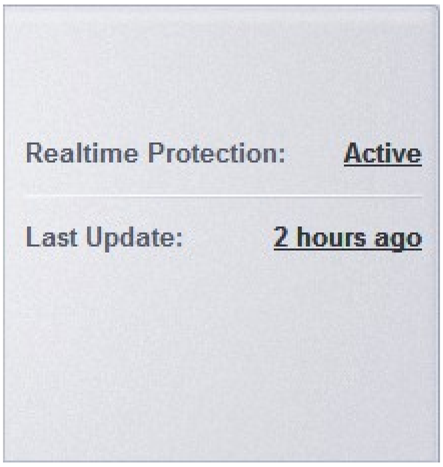


Antivirus

Firewall

Auto-Containment

VirusScope



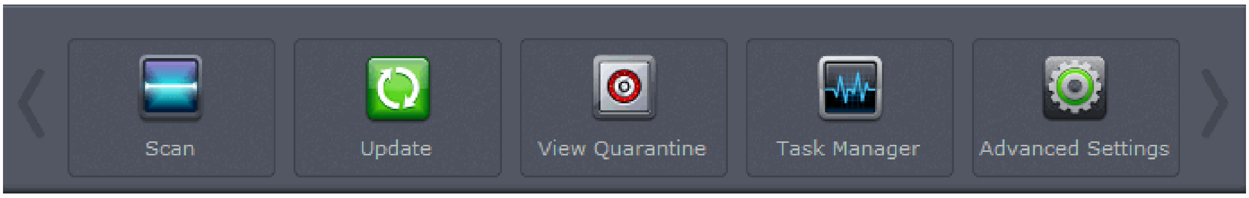
Realtime Protection: Active

Last Update: 2 hours ago

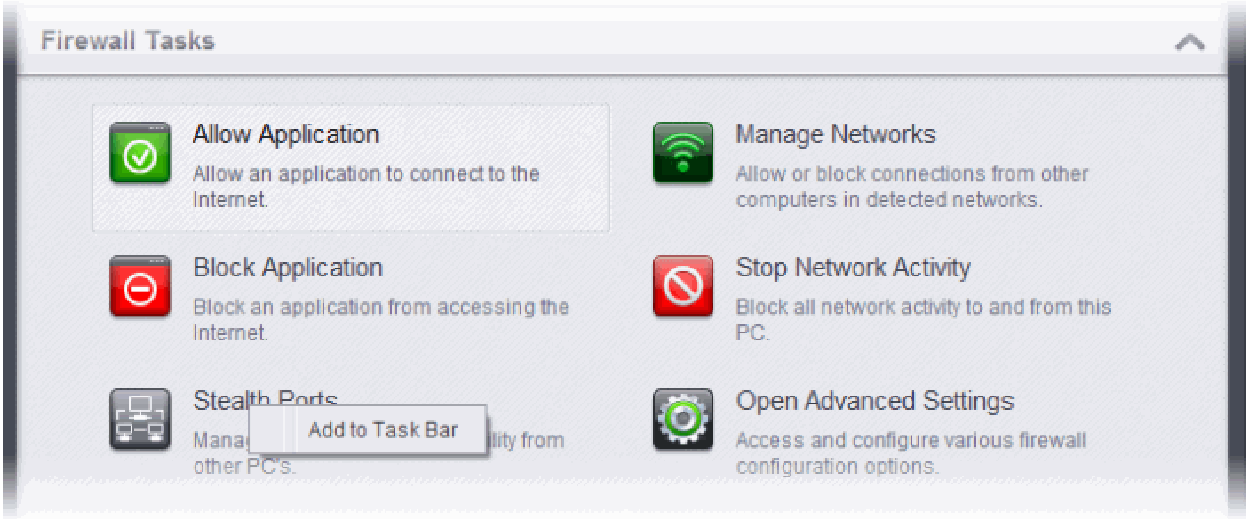
- **Antivirus** – Toggle the switch to enable or disable real-time antivirus scanning. Refer to the section 'Real-time Scanner Settings' for more details.
- **Firewall** - Toggle the switch to enable or disable firewall protection. Refer to the section 'Firewall Behavior Settings' for more details.
- **Auto-Containment** - Toggle the switch to enable or disable automatic containment of unknown files. Refer to the section 'Configuring Rules for Auto-Containment' for more details.
- **Viruscope** - Toggle the switch to enable or disable VirusScope. VirusScope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Refer to the section 'Viruscope' for more details.
- **Realtime Protection** - Displays whether or not real-time protection is enabled. Real-time protection constantly monitors your computer for malicious activity. Clicking the status link will flip the pane.
- **Last Update** - Displays the time of the most recent virus database update. Click on the text link to update the virus database.

Adding tasks to the Task Bar

The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles to the left and right sides to scroll through all tasks.



- To add a task to the Task Bar, first open the tasks interface by clicking the curved arrow:
- Expand any one of the 'General', 'Firewall', 'Containment' or 'Advanced Tasks' menus.
- Right-click on the task you wish to add then click the message 'Add to Task Bar'.



Firewall Tasks

Allow Application
Allow an application to connect to the Internet.

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

Block Application
Block an application from accessing the Internet.

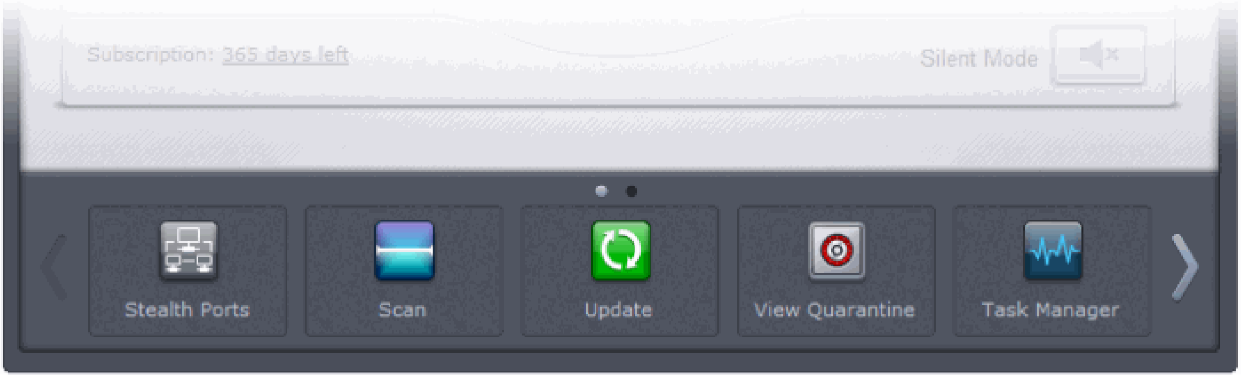
Stop Network Activity
Block all network activity to and from this PC.

Stealth Ports
Mana lity from other PC's.

Add to Task Bar

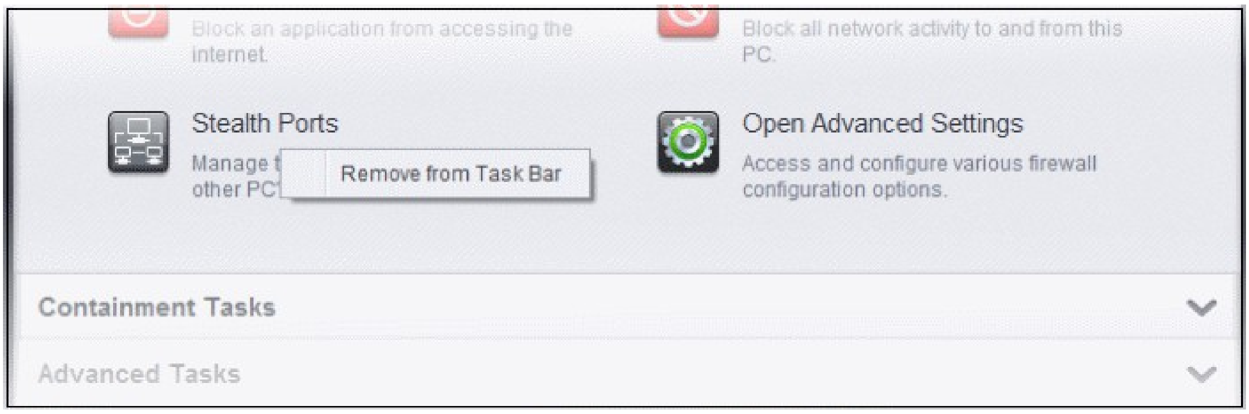
Open Advanced Settings
Access and configure various firewall configuration options.

- The selected task will be added to the Task Bar.



Tip - Many will find it useful to add 'Open Advanced Settings' to the task-bar as it contains several areas important to the configuration of CCS. To do this, click the 'Tasks' arrow at upper-right, click 'Advanced Settings' then right-click on 'Open Advanced Settings' and select 'Add to Task Bar'.

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



Block an application from accessing the internet.

Block all network activity to and from this PC.

Stealth Ports
Manage t other PC

Remove from Task Bar

Open Advanced Settings
Access and configure various firewall configuration options.

Containment Tasks

Advanced Tasks

Silent mode

Silent Mode – Allows you to work without interruption from CCS components. Alerts and updates are either suppressed or postponed.

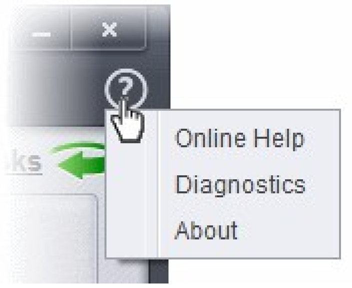
In silent mode:

- Advanced Protection alert is suppressed as if it is in training mode;
- AV database updates and scheduled scans are postponed;
- Automatic containment of unknown applications and real-time virus detection are still functional.

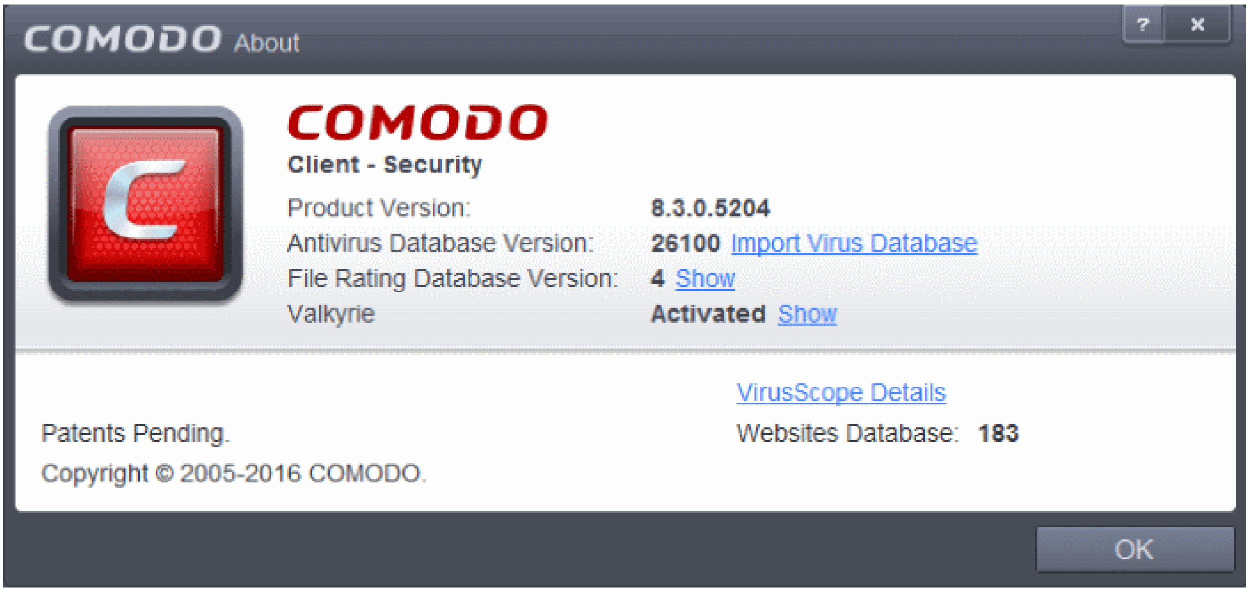
Deactivate silent mode to resume alerts and scheduled scans.

Get Help

The Help button allows you to refer to our online help guide, run a self diagnostics test as well as 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.


COMODO About

COMODO
Client - Security

Product Version:	8.3.0.5204
Antivirus Database Version:	26100 Import Virus Database
File Rating Database Version:	4 Show
Valkyrie	Activated Show

VirusScope Details

Websites Database: 183

Patents Pending.

Copyright © 2005-2016 COMODO.

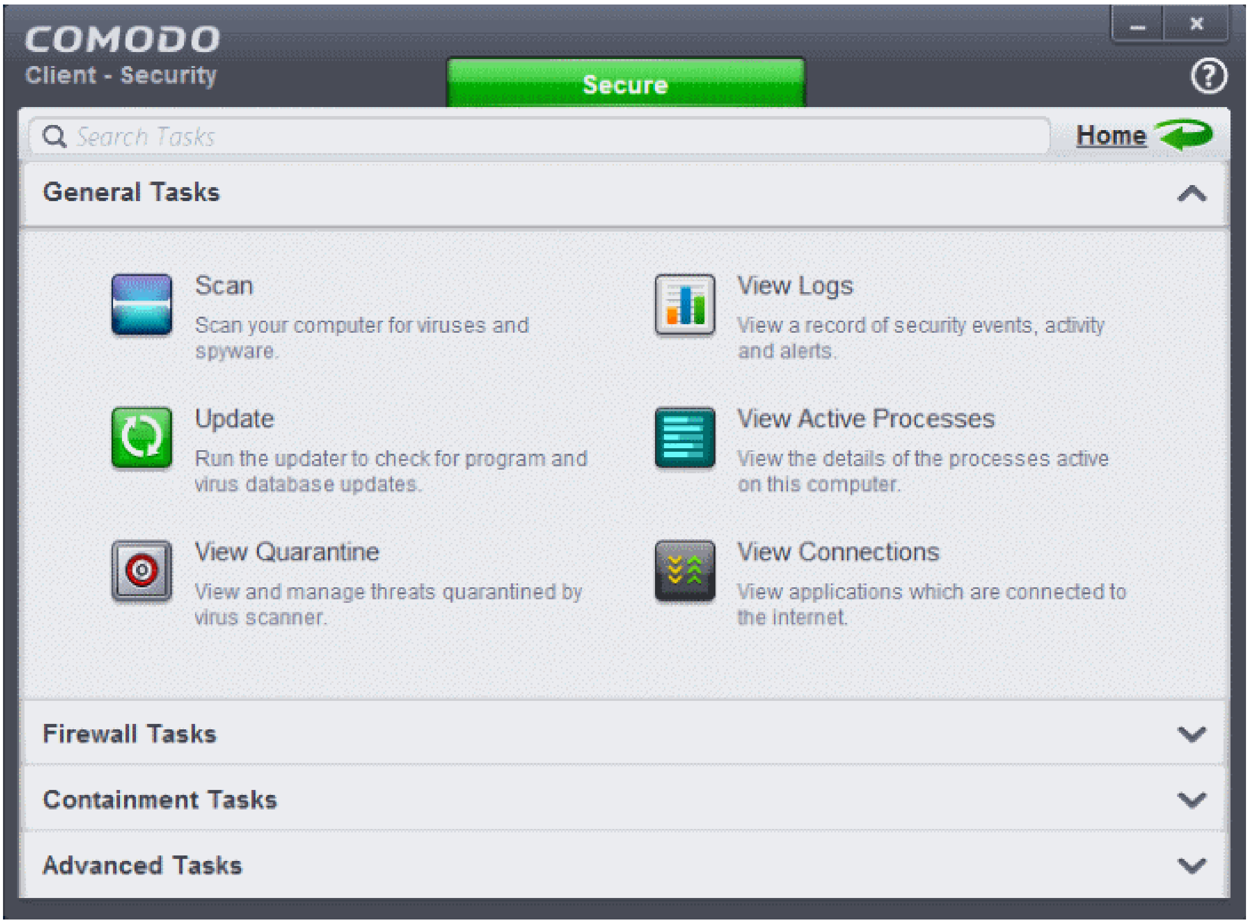
- Click Import Virus Database to import a locally stored virus signature database into CCS.
- Click Show beside 'File Rating Database Version' to view the details file rating database in the ITSM server.

The dialog provides the version number of file rating database in the ITSM server that is managing the endpoint, number of file records in the database and the date it was updated. The file rating can be viewed in ITSM by clicking Security Sub-Systems > Application Control on the left menu.

- Click Show beside Valkyrie to view its activation number for your account.
- Click Viruscope Details to open a dialog which shows the Viruscope Recognizers that are active on your system. Refer to the Viruscope section for more details.

1.5.2. The Tasks Interface

The links in the 'Tasks' interface allows you to configure every aspect of Comodo Client Security.


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
Firewall Tasks
Containment Tasks
Advanced Tasks

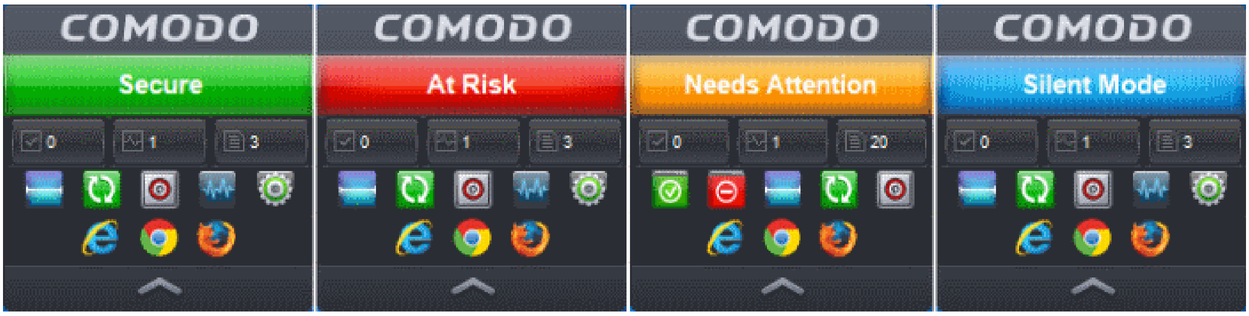
Tasks are broken down into four main sections. Click the following links for more details on each:

- General Tasks - Run antivirus scans, update virus database, view and manage quarantined threats and view logs of security events, activity and alerts. Refer to the section General Tasks for more details.
- Firewall Tasks - Allow or block applications, manage ports, manage networks and configure advanced firewall settings. Refer to the section Firewall Tasks for more details.
- Containment Tasks - Run applications in a virtual environment and configure advanced containment settings. Refer to the section 'Containment Tasks' for more details.
- Advanced Tasks - Create a boot disk to clean up highly infected systems; install other Comodo software like KillSwitch and Cleaning Essentials; submit files to Comodo for analysis and gain access to the 'Advanced Settings' interface. Refer to the section 'Advanced Tasks' for more details.

1.5.3. The Widget

The CCS Widget is a handy control that provides at-a-glance information about the security status, speed of outgoing and incoming traffic and 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 opens a context sensitive menu similar to the one displayed on right clicking the CCS system tray icon. The context sensitive menu allows you to enable or disable CCS components and configure various settings. Refer to section The System Tray Icon for more details.



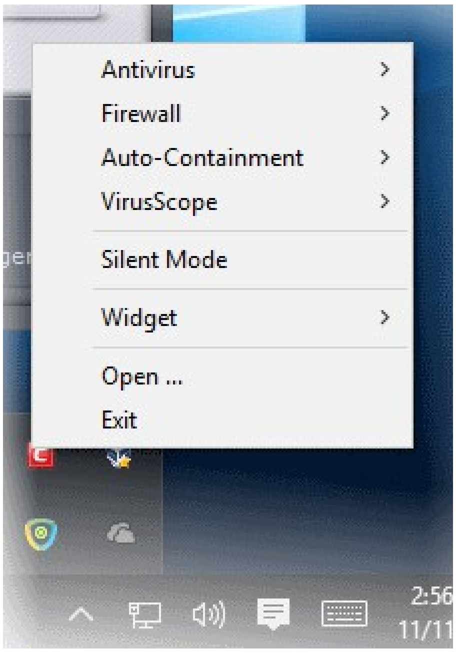
- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' opens the appropriate interface for you to take action immediately.
- The second row tells you current status of the CCS application:
  - The first button ☑ 0 displays the number of programs/processes that are currently running in the container. Clicking the button opens the Active Process List (Contained Only) interface, which allows you to identify and terminate unnecessary processes. Clicking the 'More' button in this interface will open the KillSwitch application. If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the sections View Active Process List and Identify and Kill Unsafe Processes for more details.
  - The second button 0 tells you how many CCS tasks are currently running. Clicking the button opens the Task Manager interface.
  - The third button 1 displays how many files are added as 'Unrecognized' to the Files list and are pending for submission to Comodo for analysis. Clicking on it opens the Files list interface which displays the list of Unrecognized files.

  The status row is displayed only if 'Show Status Pane' is enabled under 'Widget options of CCS tray icon or Widget right click menu. Refer to 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 displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of CCS tray icon or Widget right click menu. Refer to The System Tray Icon for more details. ***(Default = Enabled)***
- The fourth row displays the browsers installed in your computer system. Clicking on a browser icon will 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. Refer to Running an application inside the container for more details. The Browsers row is displayed only if 'Show Browsers Pane' is enabled under 'Widget' options of CCS tray icon or Widget right click menu. Refer to 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

In addition to providing a short cut method to start CCS, the system tray icon also provides short cuts to configure security settings.

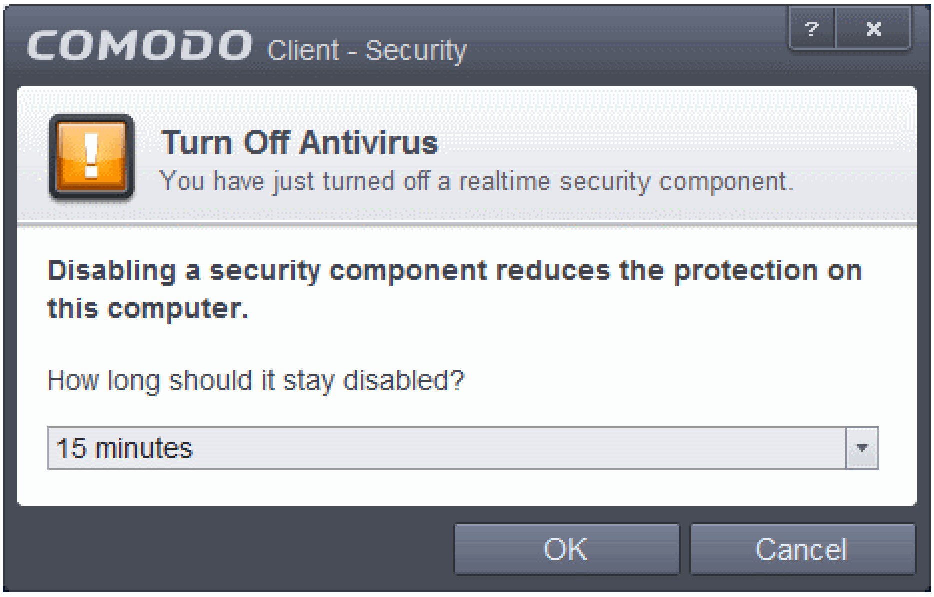
Right-clicking the system tray icon will provide you the option to enable or disable various security settings.



Hover your mouse pointer or click on any of the menus and the following options are available.

- **Antivirus** - You can enable or disable Real-time antivirus scan.

If this setting is disabled, immediately the Security Information in the main task interface and the Widget will turn red alerting you of the status. In addition, a pop-up alert will be displayed.


COMODO Client - Security

Turn Off Antivirus

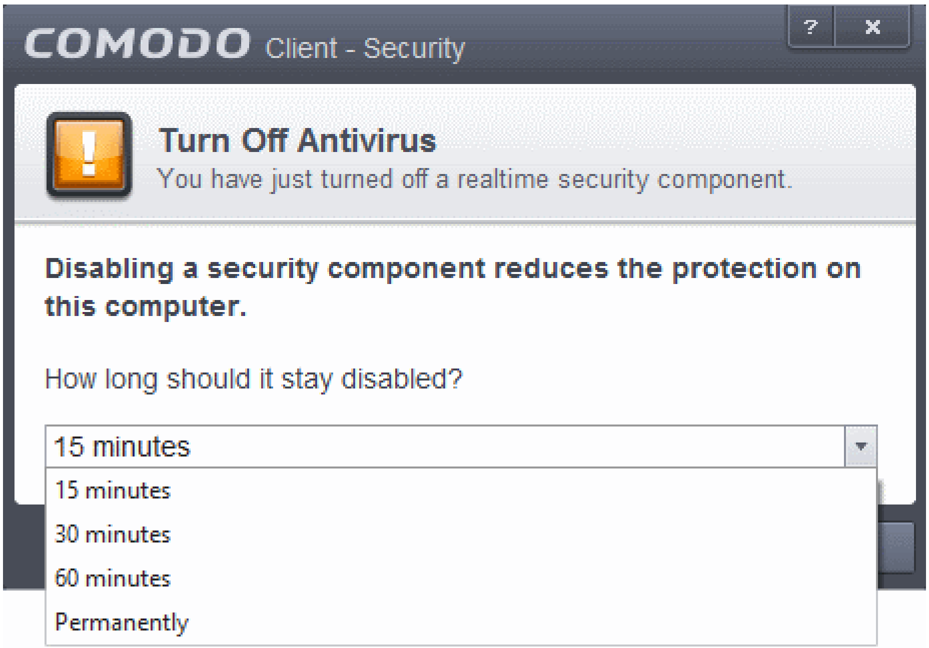
You have just turned off a realtime security component.

Disabling a security component reduces the protection on this computer.

How long should it stay disabled?

15 minutes

You can select the period for which the security should be turned off from the drop-down.



Turn Off Antivirus

You have just turned off a realtime security component.

Disabling a security component reduces the protection on this computer.

How long should it stay disabled?

15 minutes

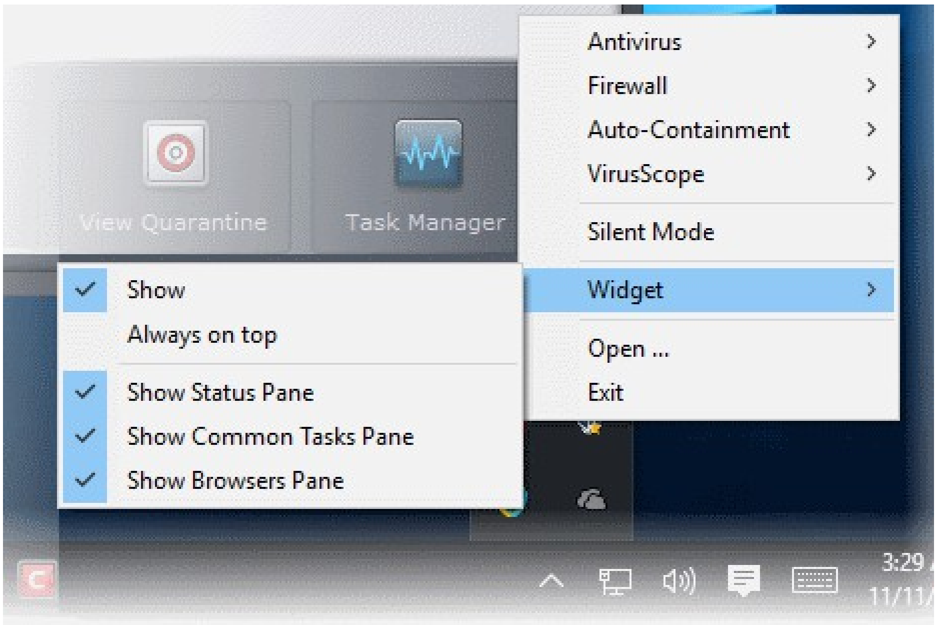
Select the period and click 'OK'. If you have selected any of first three periods, the security component will be enabled automatically after the chosen period.

- **Auto-Containment** - You can enable or disable Auto-Containment. You can create rules for running potentially risky applications on an isolated environment. Refer to the sections Comodo Containment and Configuring Rules for Auto-Containment for more details.
- **Firewall** - You can enable or disable Firewall. Refer to the section 'Firewall Settings' for more details.
- **Viruscope** – You can enable or disable Viruscope. Refer to the section Viruscope for more details.
- **Silent Mode** - Switches CCS to Silent mode to enable you to carry out tasks without any interruptions from various alerts in your computer. The operations that can interfere with users' silent mode experience are either suppressed or postponed.

  In silent mode:
  - Advanced Protection/Firewall alert is suppressed.
  - AV database updates and scheduled scans are postponed until the silent mode is over;
  - Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Silent mode to resume alerts and scheduled scans.

- **Widget** - You can select whether or not the Widget is to be displayed and select the components of it to be displayed.



- **Show**: Toggles the display of widget. (***Default = Disabled***)
- **Always on top**: Displays the widget on top of all windows currently running on your computer. (***Default = Disabled***)
- **Show Status Pane**: Displays the row indicating the current status of CCS in the widget. (***Default = Disabled***)
- **Show Common Tasks Pane**: Displays the row containing shortcuts to common CCS tasks in the widget. (***Default = Enabled***)
- **Show Browsers Pane**: Displays the row containing the shortcuts to browsers in your computer. (***Default = Enabled***)

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

1.6. Understanding Security Alerts

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

Alerts Overview

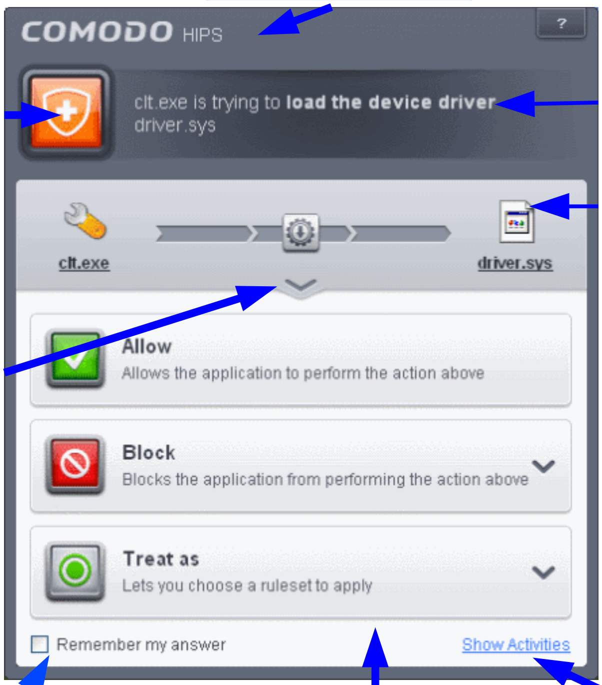
CCS alerts warn you about security related activities and requests at the moment they occur. Each alert contains information about the particular issue so you can make an informed decision about whether to allow or block it. Alerts also let you specify how CCS should behave in future when it encounters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

Type of Alert

Can be Antivirus, Firewall, HIPS, Containment, Viruscope or Cloud Scanner

Color indicates severity of the Alert

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



COMODO HIPS

?

clt.exe is trying to **load the device driver**
driver.sys

clt.exe

driver.sys

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer

Show Activities

Description of activity or connection attempt

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.

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

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

Select this option to create a rule in respective module for the application in question to allow or block as per your choice.

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

Alert Types

Comodo Client Security alerts come in five main varieties, namely:

- 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 other important files, and when an unrecognized file is placed in containment. Containment Alerts will be displayed only if privilege elevation alerts is enabled under Containment Settings.
- Viruscope Alerts - Shown whenever a currently running process attempts to take suspicious actions. Viruscope alerts allow you to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. Viruscope Alerts will be displayed only when Viruscope is enabled under Advanced Protection.

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 generated by the Antivirus, Firewall, HIPS and Auto-Containment components of CCS. For other types of alert, see Comodo Message Center notifications, Notification Messages and Information Messages.

Severity Level

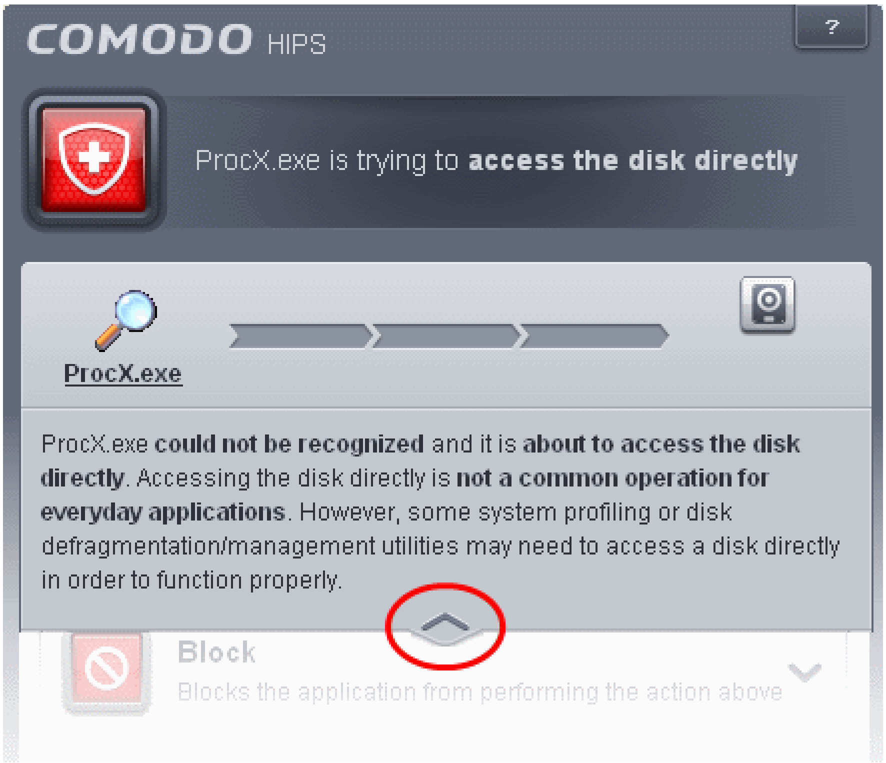
The shield icons at the upper left of each alert are color coded according to the risk level presented by the activity or request. However, it cannot be stressed enough that you should still read the information in order to reach an informed decision on allowing or blocking the activity.

- Yellow Icons - Low Severity - In most cases, you can safely approve these requests. The 'Remember my answer' option is automatically pre-selected for safe requests
- Orange Icons - 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 or activity by a trusted program or an indication of an attack by malware. 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 Icons - 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 and Viruscope alerts are not ranked in this way. They always appear with a red icon.

Alert Description

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



ProcX.exe is trying to **access the disk directly**

ProcX.exe **could not be recognized** and it is **about to access the disk directly**. Accessing the disk directly is **not a common operation for everyday applications**. However, some system profiling or disk defragmentation/management utilities may need to access a disk directly in order to function properly.

Blocks the application from performing the action above

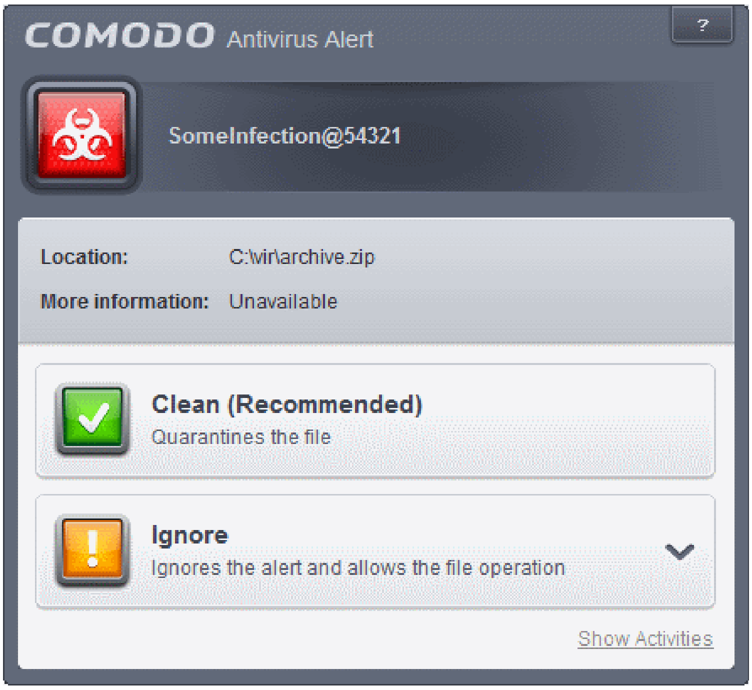
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

Now that we've outlined the basic construction of an alert, lets 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 'Security Settings > Antivirus > Realtime Scan'. Refer to Real-time Scanner Settings for more details.



COMODO Antivirus Alert

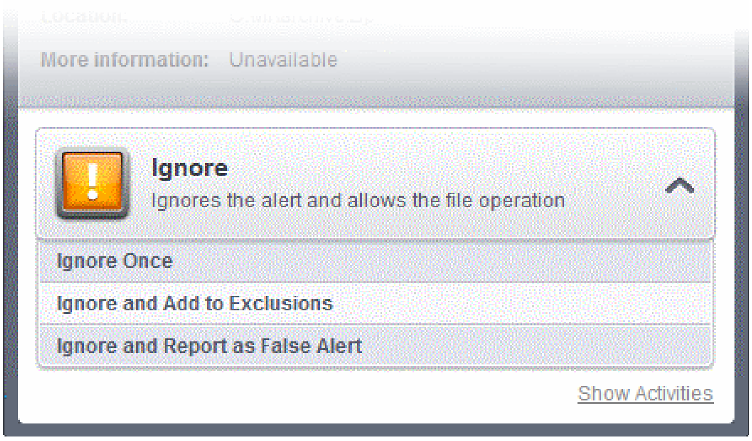
SomeInfection@54321

Location: C:\wir\archive.zip

More information: Unavailable

The following response-options are available:

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



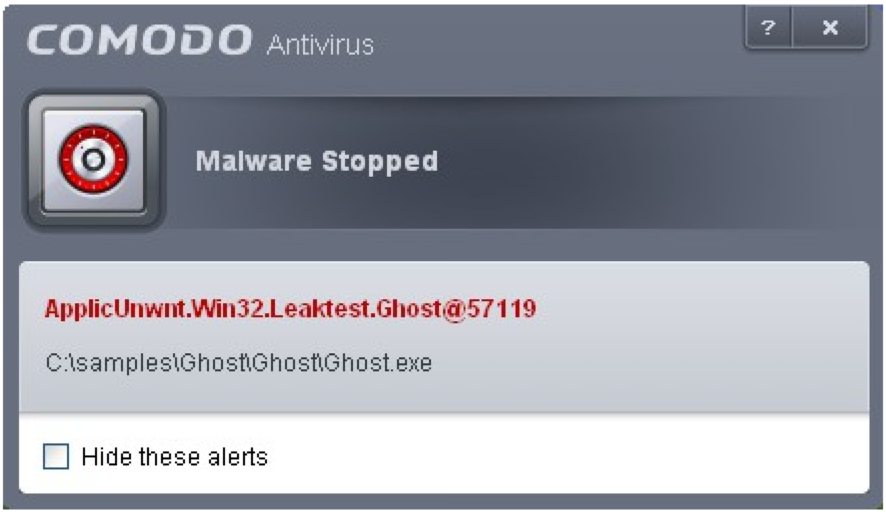
More information: Unavailable

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

- **Ignore Once** -The file is allowed to run this time only. If the file attempts to execute on future occasions, another antivirus alert is displayed.
- **Ignore and Add to Exclusions** - The file is allowed to run and is moved to the Exclusions list - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- **Ignore and Report as a False Alert** - If you are sure that the file is safe, select 'Ignore and Report as a False Alert'. 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 CCS detects a virus or other malware, it will immediately block it and provide you with instant on-screen notification:



COMODO Antivirus

Malware Stopped

ApplicUnwnt.Win32.Leaktest.Ghost@57119

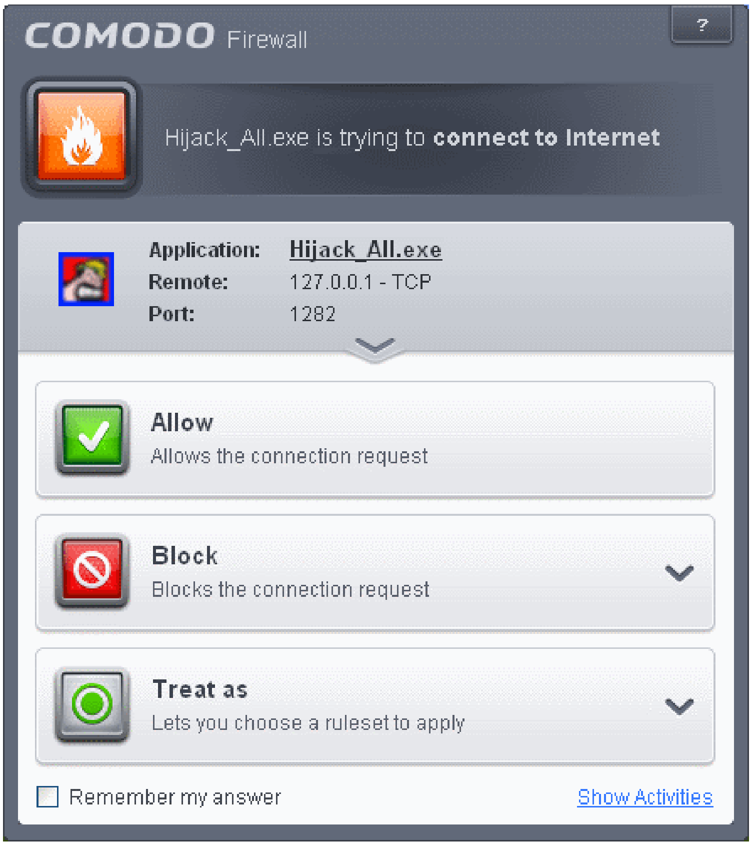
C:\samples\Ghost\Ghost\Ghost.exe

□ Hide these alerts

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 Advanced 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:



COMODO Firewall

Hijack_All.exe is trying to **connect to Internet**

Application: Hijack_All.exe
Remote: 127.0.0.1 - TCP
Port: 1282

Allow — Allows the connection request

Block — Blocks the connection request

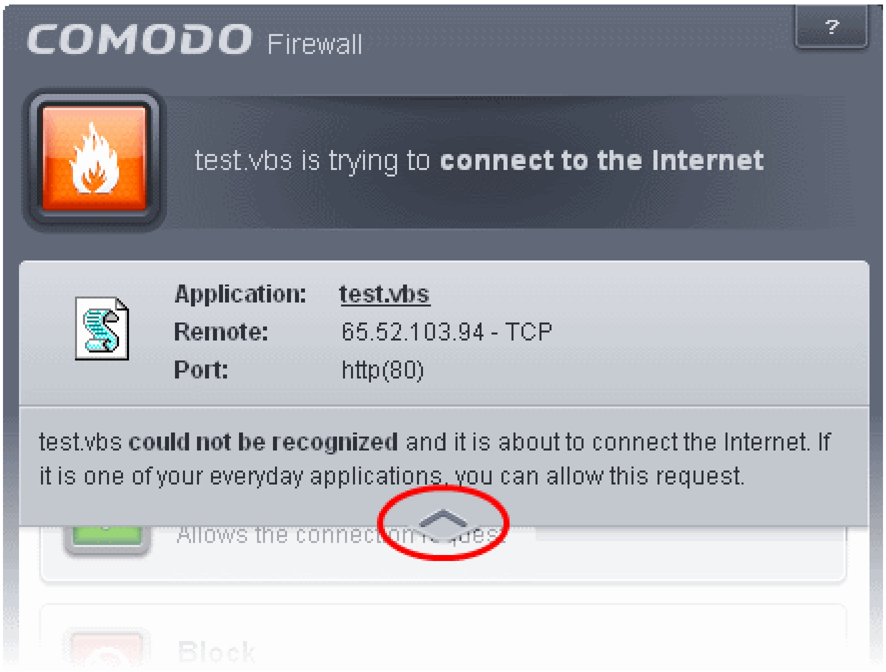
Treat as — Lets you choose a ruleset to apply

□ Remember my answer

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 Viruscope is enabled under Advanced Settings > Advanced Protection > Viruscope. 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 by clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications (for example, Firefox and Outlook are safe applications). If the application is safe, this will be mentioned 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.



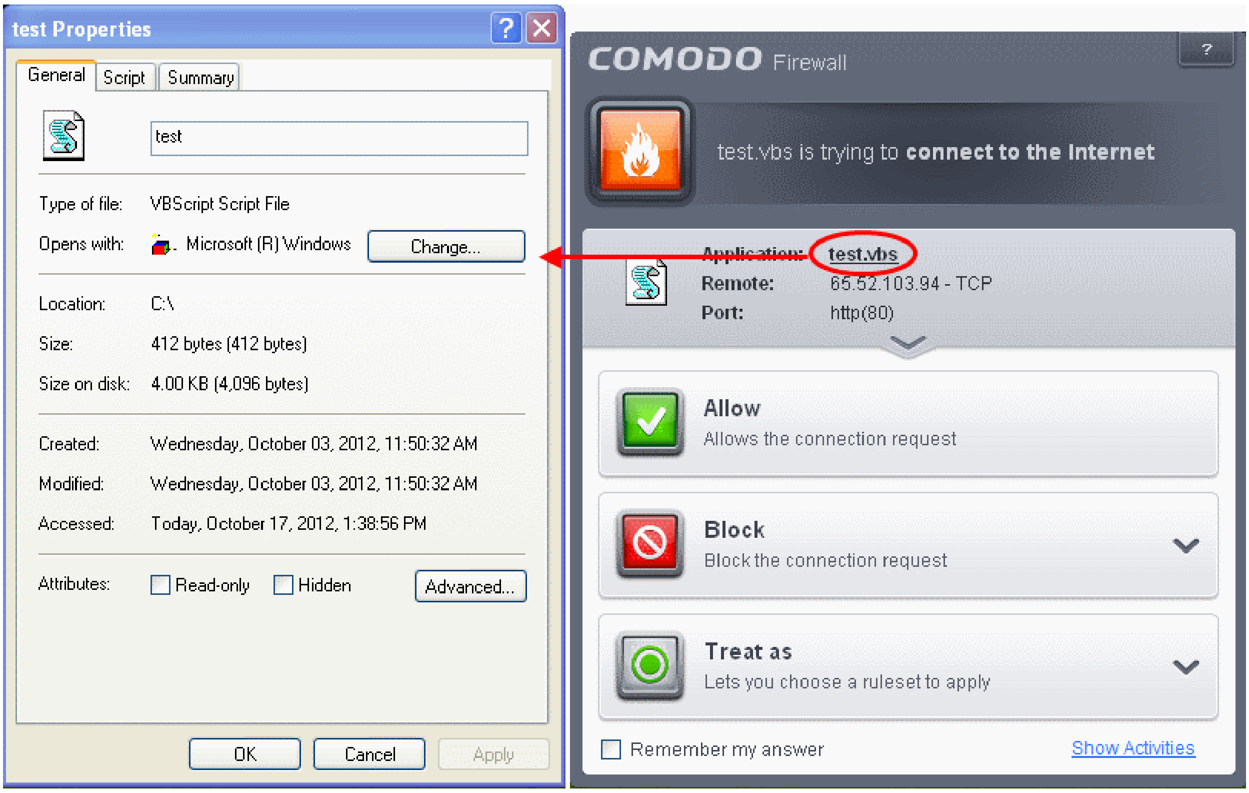
test.vbs is trying to **connect to the Internet**

Application: test.vbs
Remote: 65.52.103.94 - TCP
Port: http(80)

test.vbs **could not be recognized** and it is about to connect the Internet. If it is one of your everyday applications, you can allow this request.

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:



test Properties

General | Script | Summary

test

Type of file: VBScript Script File

Opens with: Microsoft (R) Windows Change...

Location: C:\

Size: 412 bytes (412 bytes)

Size on disk: 4.00 KB (4,096 bytes)

Created: Wednesday, October 03, 2012, 11:50:32 AM

Modified: Wednesday, October 03, 2012, 11:50:32 AM

Accessed: Today, October 17, 2012, 1:38:56 PM

Attributes: □ Read-only □ Hidden Advanced...

OK Cancel Apply

COMODO Firewall

test.vbs is trying to **connect to the Internet**

Application: test.vbs
Remote: 65.52.103.94 - TCP
Port: http(80)

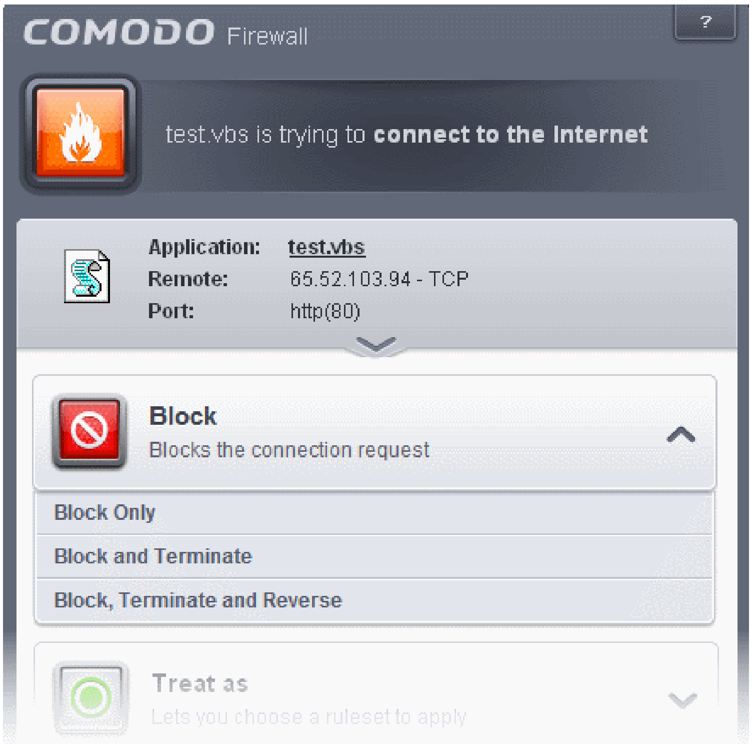
Allow
Allows the connection request

Block
Block the connection request

Treat as
Lets you choose a ruleset to apply

□ Remember my answer Show Activities

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 & 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 and the process/application that has made any changes will be rolled back)



COMODO Firewall

test.vbs is trying to **connect to the Internet**

Application: test.vbs
Remote: 65.52.103.94 - TCP
Port: http(80)

Block
Blocks the connection request

Block Only

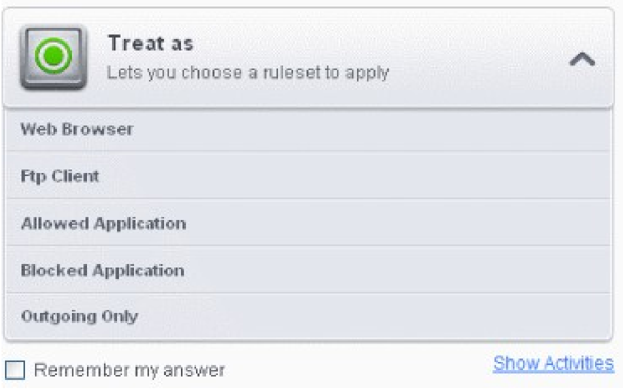
Block and Terminate

Block, Terminate and Reverse

Treat as
Lets you choose a ruleset to apply

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 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application.



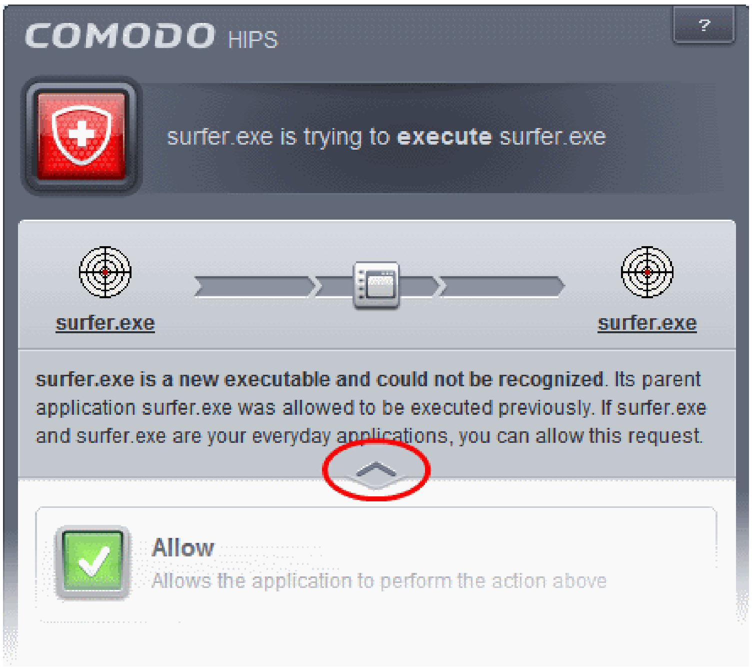
Remember to check the box **Remember My Answer** for the ruleset to be applied in future.

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:

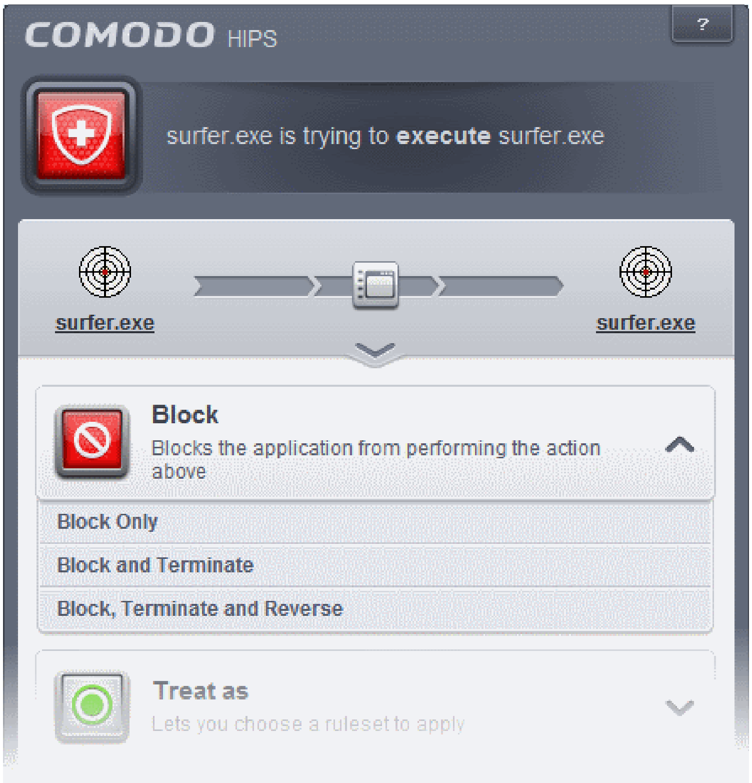
1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Client Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe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


COMODO HIPS
?
surfer.exe is trying to **execute** surfer.exe
surfer.exe
surfer.exe
Allow
Allows the application to perform the action above

surfer.exe is a new executable and could not be recognized. Its parent application surfer.exe was allowed to be executed previously. If surfer.exe and surfer.exe are your everyday applications, you can allow this request.

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

If you don't recognize the application then we recommend you select **Block** the application. You can choose to just block the connection, block & terminate or block, terminate and roll back any changes it may have already done.



COMODO HIPS

surfer.exe is trying to **execute** surfer.exe

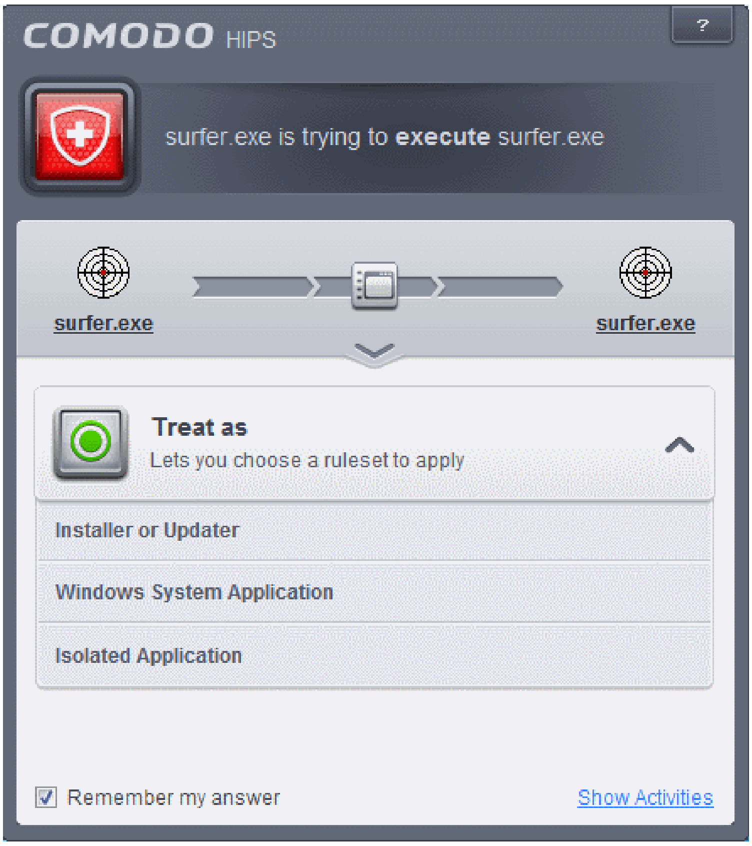
surfer.exe → surfer.exe

Block
Blocks the application from performing the action above

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

Treat as
Lets you choose a ruleset to apply

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.



COMODO HIPS

surfer.exe is trying to **execute** surfer.exe

surfer.exe → surfer.exe

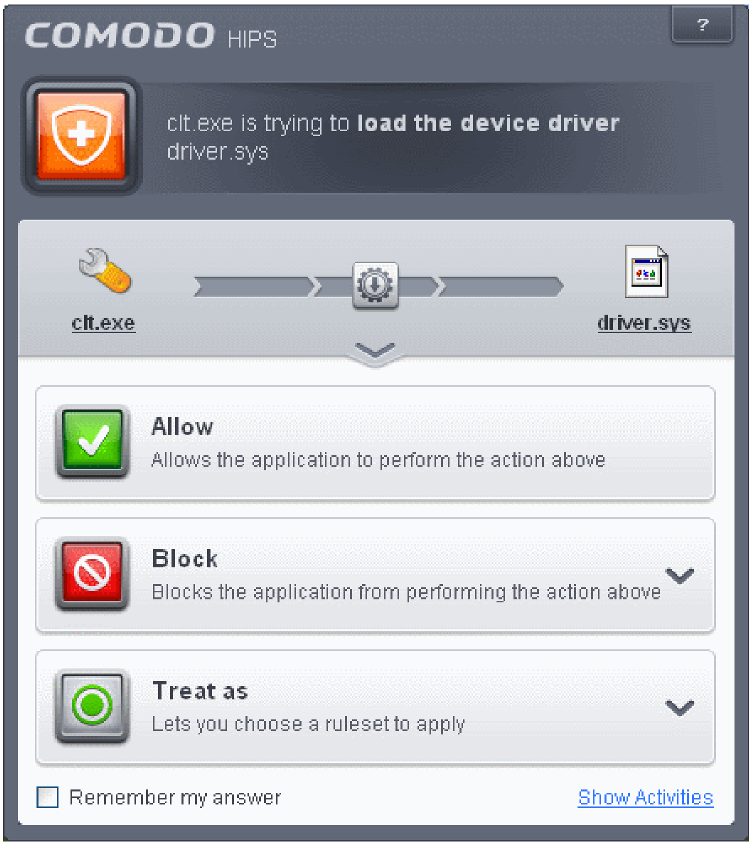
Treat as
Lets you choose a ruleset to apply

- Installer or Updater
- Windows System Application
- Isolated Application

☑ Remember my answer

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

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

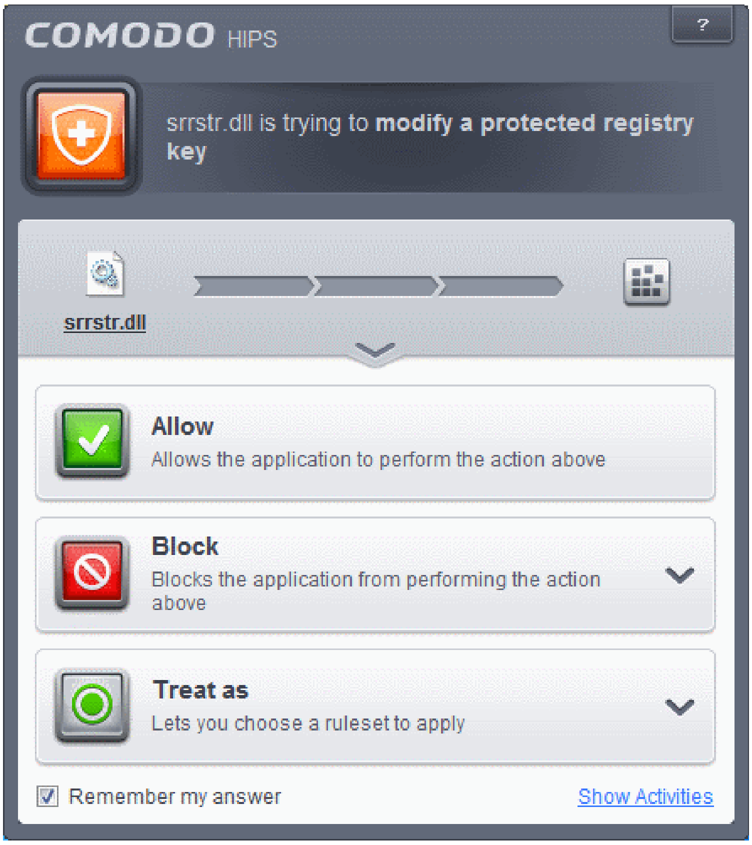


COMODO HIPS

clt.exe is trying to **load the device driver** driver.sys

?
clt.exe
driver.sys
Allow
Allows the application to perform the action above
Block
Blocks the application from performing the action above
Treat as
Lets you choose a ruleset to apply
□ Remember my answer
Show Activities

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



COMODO HIPS

srrstr.dll is trying to **modify a protected registry key**

srrstr.dll

Allow
Allows the application to perform the action above

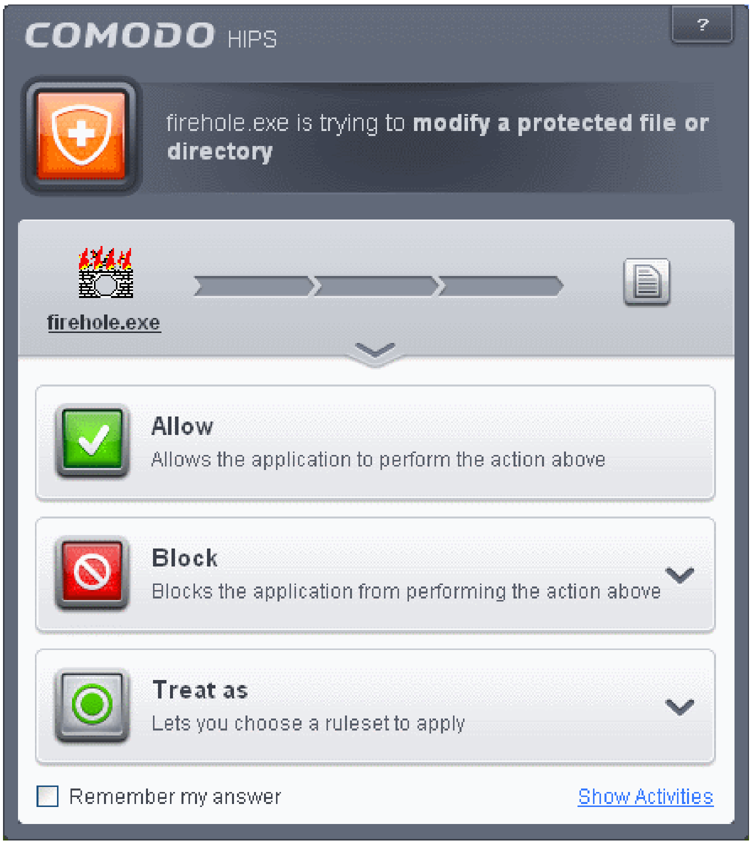
Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

☑ Remember my answer

Show Activities

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



COMODO HIPS

firehole.exe is trying to **modify a protected file or directory**

firehole.exe

Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

□ Remember my answer

Show Activities

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 subdirectories) 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.

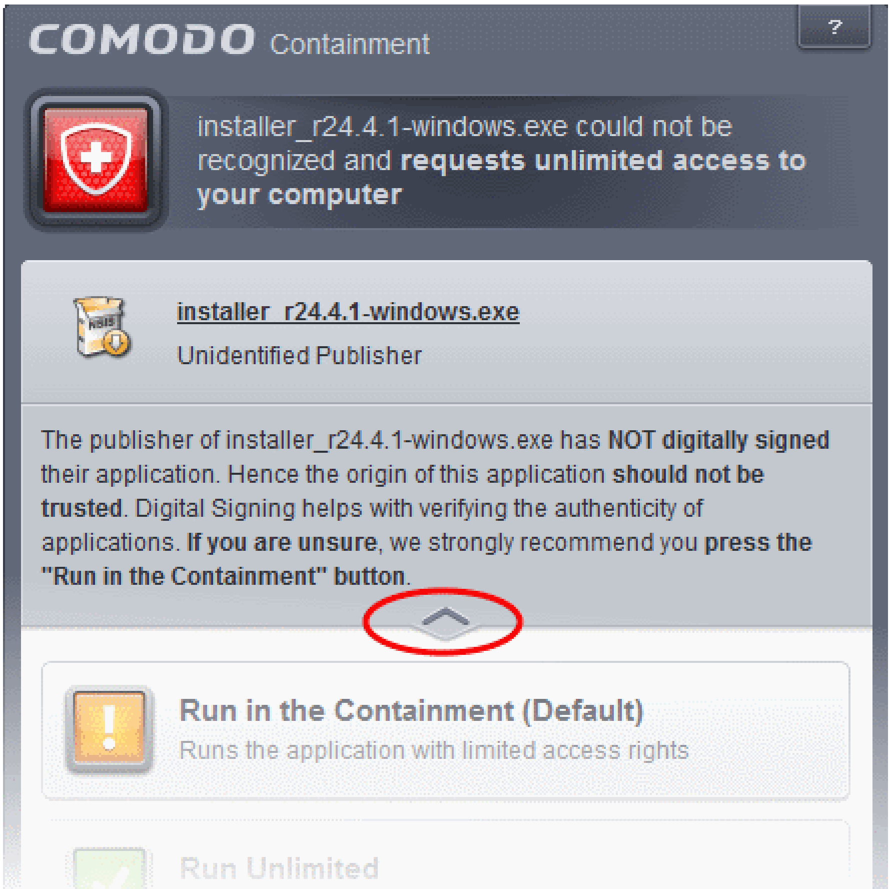
6. If a HIPS alert reports a malware behavior in the security considerations area then you should **Block the request** permanently by selecting **Remember My Answer** option. As this is probably a virus, you should also submit the application in question, to Comodo for analysis.
7. Unrecognized applications 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 Clean PC Mode, you probably are seeing the alerts for any new applications introduced to the system - but not for the ones you have already installed. You may review the files with 'Unrecognized' rating in the '**File List**' interface for your newly installed applications and remove them from the list for them to be considered as clean.
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 containment alerts if an application or a process tries to modify operating system files or critical areas like the Windows Registry, and when it automatically contains 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.



installer_r24.4.1-windows.exe could not be recognized and **requests unlimited access to your computer**

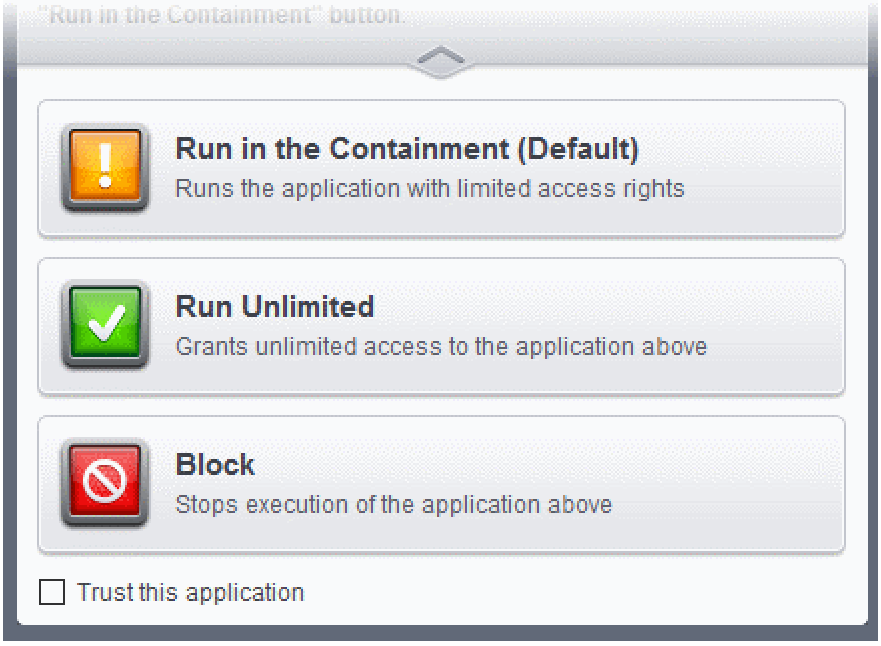
installer_r24.4.1-windows.exe

Unidentified Publisher

The publisher of installer_r24.4.1-windows.exe has **NOT digitally signed** their application. Hence the origin of this application **should not be trusted**. Digital Signing helps with verifying the authenticity of applications. **If you are unsure**, we strongly recommend you **press the "Run in the Containment" button**.

Run in the Containment (Default)
Runs the application with limited access rights
Run Unlimited

- 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 Files List with Trusted status.



"Run in the Containment" button.
Run in the Containment (Default)
Runs the application with limited access rights
Run Unlimited
Grants unlimited access to the application above
Block
Stops execution of the application above
□ Trust this application

- If you are unsure of the safety of the software, then Comodo recommends that you run it with limited privileges by clicking the 'Run in the Containment' button. Refer to 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 Block the application.

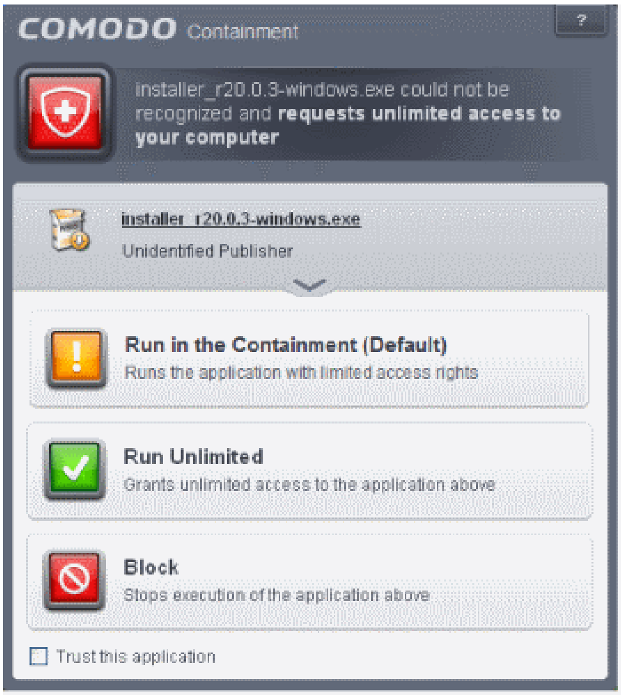
Run with Elevated Privileges Alert

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 in the Containment' 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 assign Trusted Status to this file in the '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 'Do not show privilege alerts but automatically apply the following action' check box is disabled. This can be found in Advanced Settings > Security Settings > Advanced Protection > Configuring Containment Settings'

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



COMODO Containment

installer_r20.0.3-windows.exe could not be recognized and **requests unlimited access to your computer**

installer_r20.0.3-windows.exe
Unidentified Publisher

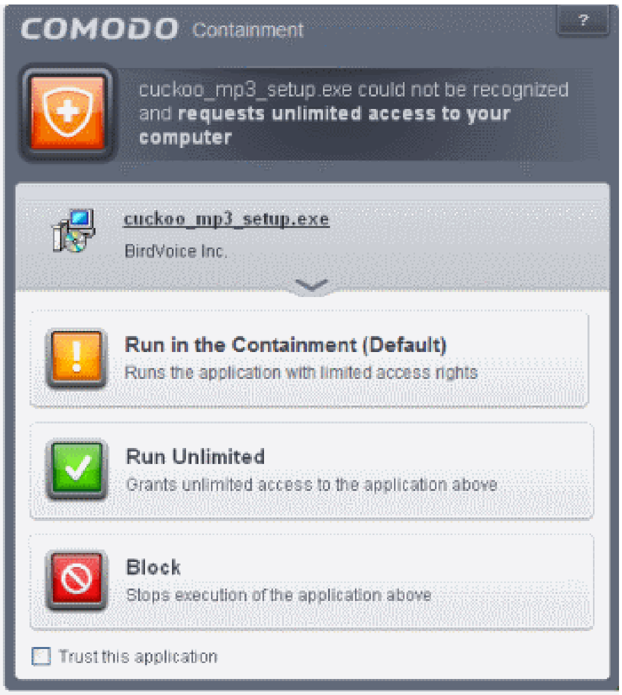
Run in the Containment (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

Unknown and not digitally signed



COMODO Containment

cuckoo_mp3_setup.exe could not be recognized and **requests unlimited access to your computer**

cuckoo_mp3_setup.exe
BirdVoice Inc.

Run in the Containment (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

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

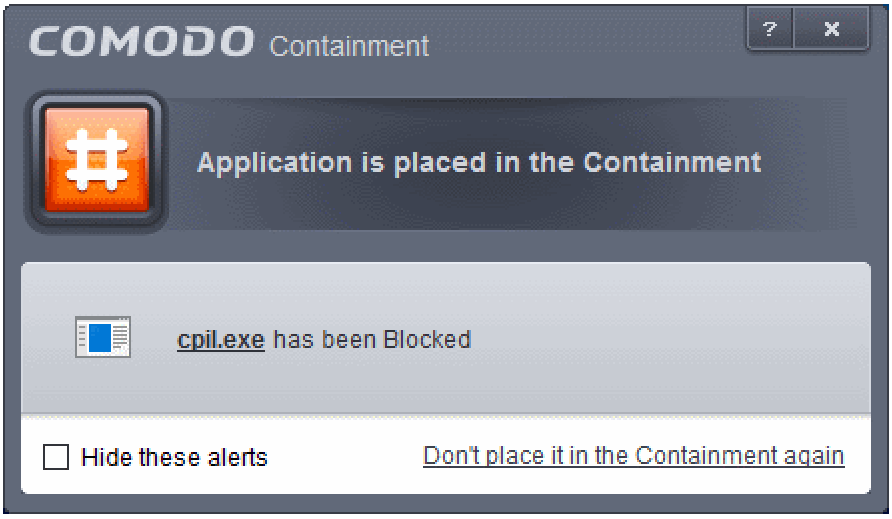
- Unknown and unsigned installers should be either contained or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be contained if you would like to evaluate the behavior of the application.

Also see:

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

Containment Notification

Comodo Containment will display a notification whenever it auto-contains an unknown application:



COMODO Containment

Application is placed in the Containment

cpil.exe has been Blocked

□ Hide these alerts

Don't place it in the Containment again

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

- Clicking the name of the application will open the File List interface with the currently contained application highlighted.
- Clicking Don't place it in the Containment again assigns 'Trusted' status to the file in the File List, so that the application will not be auto-contained in future. Choose this option if you are absolutely sure that the executable is safe.

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:

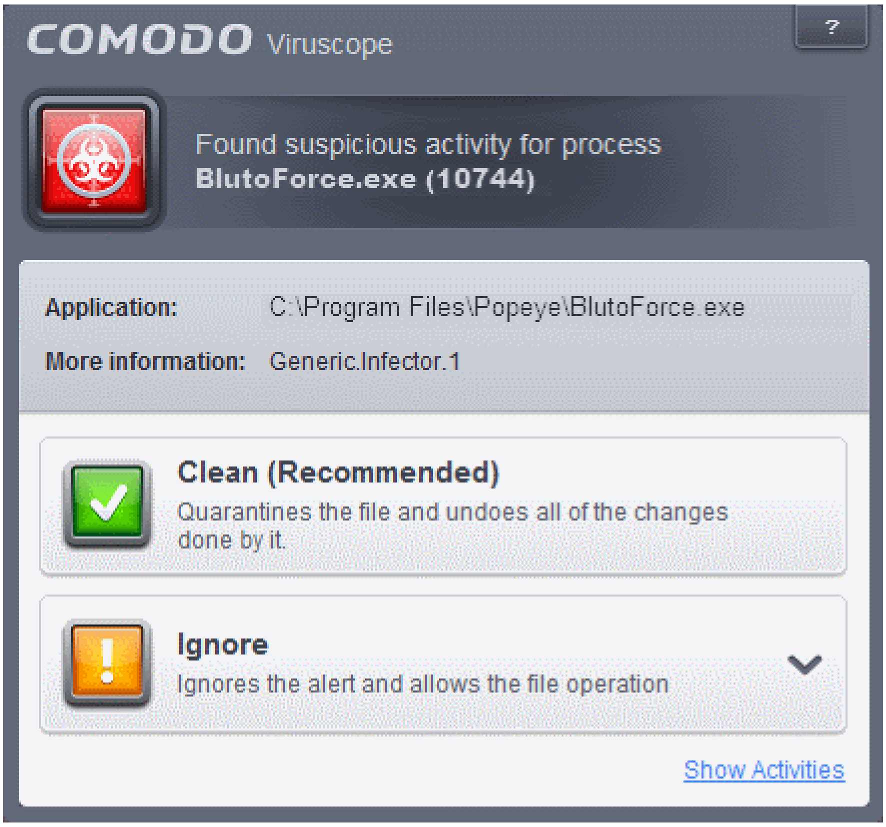
- 'Unknown Files: The Scanning Processes' - to understand process behind how CCS scans files

Answering a Viruscope Alert

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

Please read the following advice before answering a Viruscope alert:

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



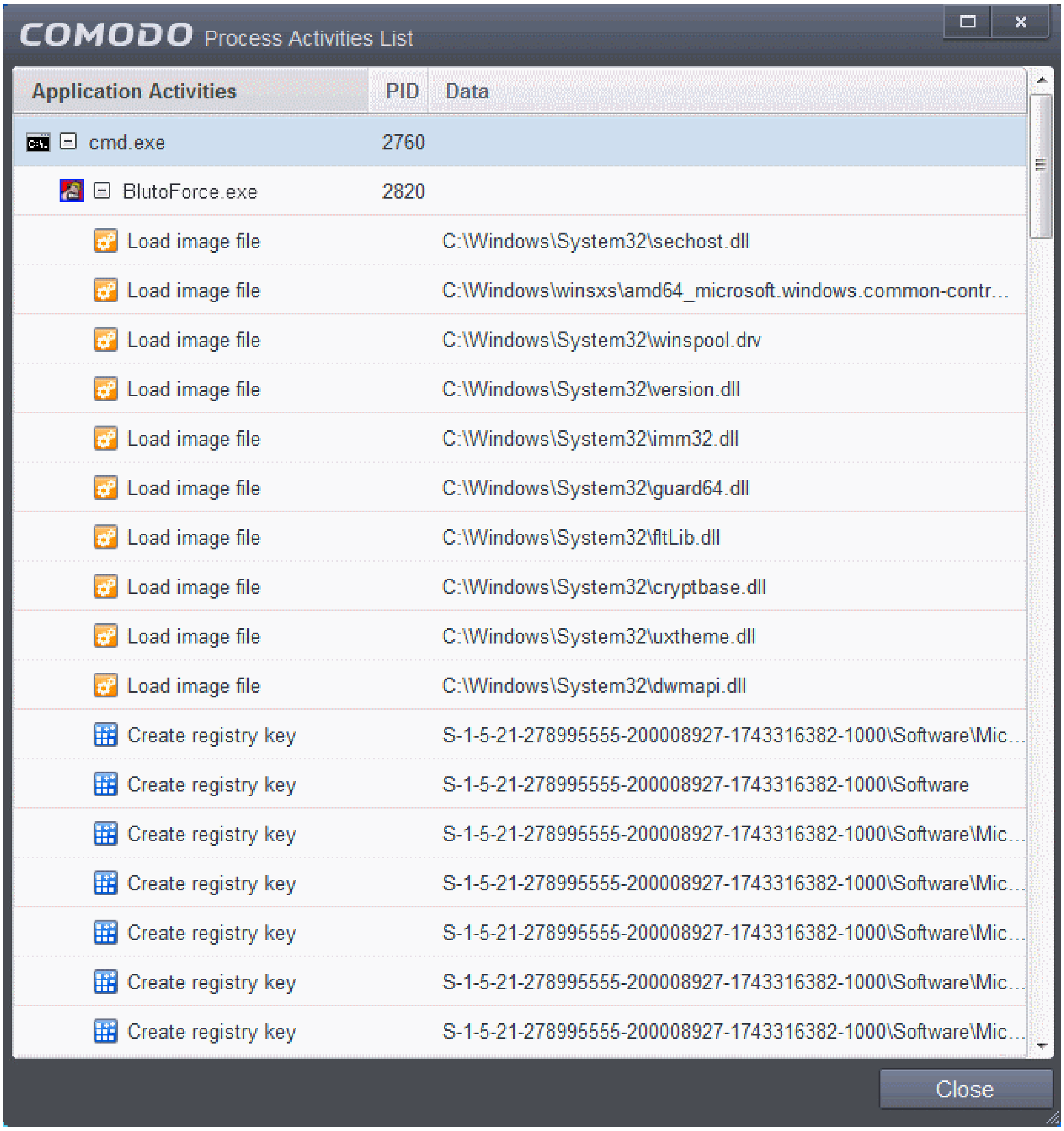
Found suspicious activity for process
BlutoForce.exe (10744)

Application: C:\Program Files\Popeye\BlutoForce.exe

More information: Generic.Infector.1

Clean (Recommended)
Quarantines the file and undoes all of the changes done by it.
Ignore
Ignores the alert and allows the file operation
Show Activities

- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking Ignore and selecting the option from the drop-down.
    - Ignore Once -The process is allowed to run this time only. If the process attempts to execute on future occasions, another Viruscope alert is displayed.
    - Ignore and Add to Trusted Files - The process is allowed to run and and the parent application assigned 'Trusted' status - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- 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.



COMODO Process Activities List

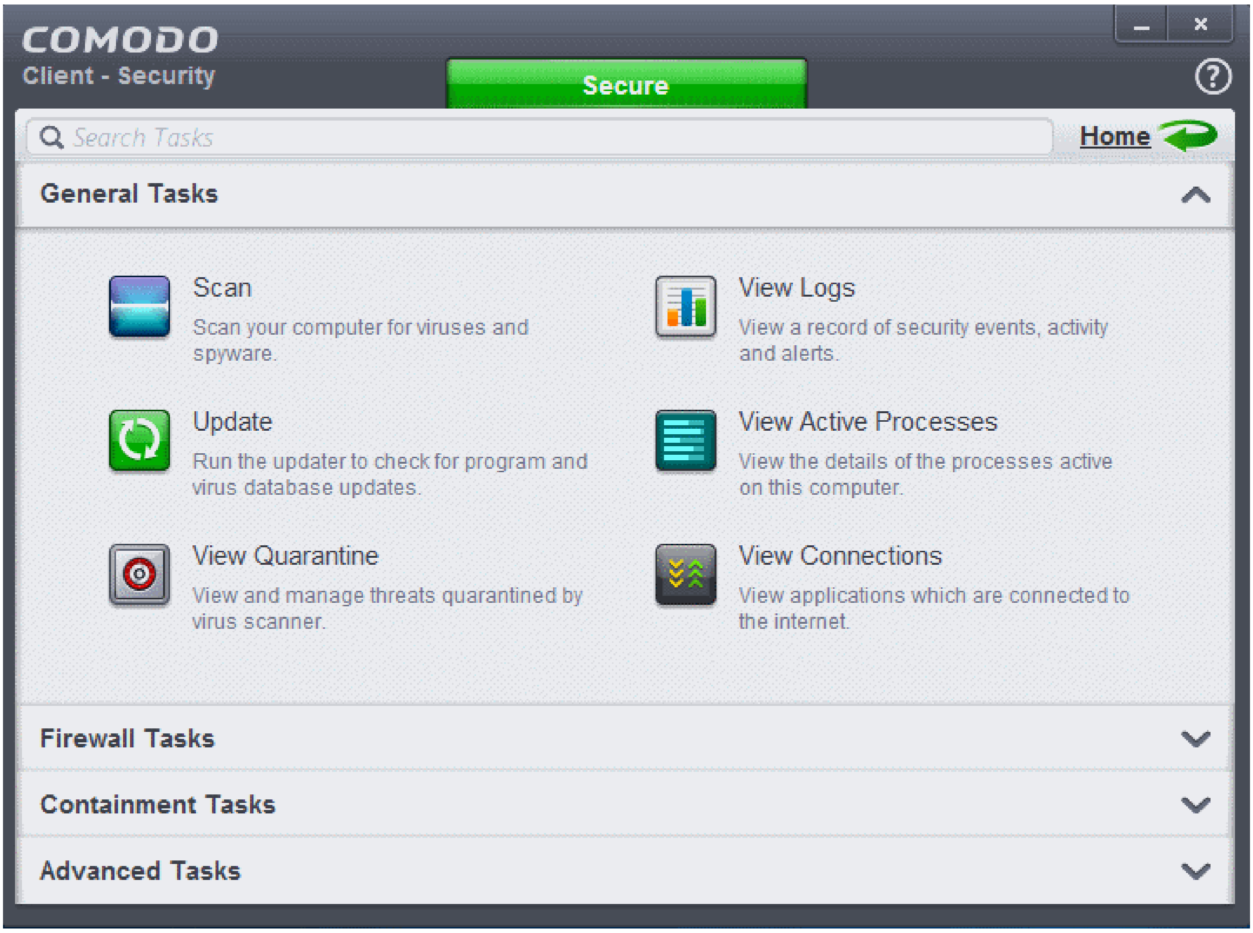
Application Activities	PID	Data
cmd.exe	2760	
BlutoForce.exe	2820	
Load image file		C:\Windows\System32\sechost.dll
Load image file		C:\Windows\winsxs\amd64_microsoft.windows.common-contr...
Load image file		C:\Windows\System32\winspool.drv
Load image file		C:\Windows\System32\version.dll
Load image file		C:\Windows\System32\imm32.dll
Load image file		C:\Windows\System32\guard64.dll
Load image file		C:\Windows\System32\fltLib.dll
Load image file		C:\Windows\System32\cryptbase.dll
Load image file		C:\Windows\System32\uxtheme.dll
Load image file		C:\Windows\System32\dwmapi.dll
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...
Create registry key		S-1-5-21-278995555-200008927-1743316382-1000\Software\Mic...

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.

2. General Tasks - Introduction

The 'General Tasks' interface allows you to quickly perform antivirus scans, update the virus database, manage quarantined files, view event logs and internet connections and manage CCS running tasks.

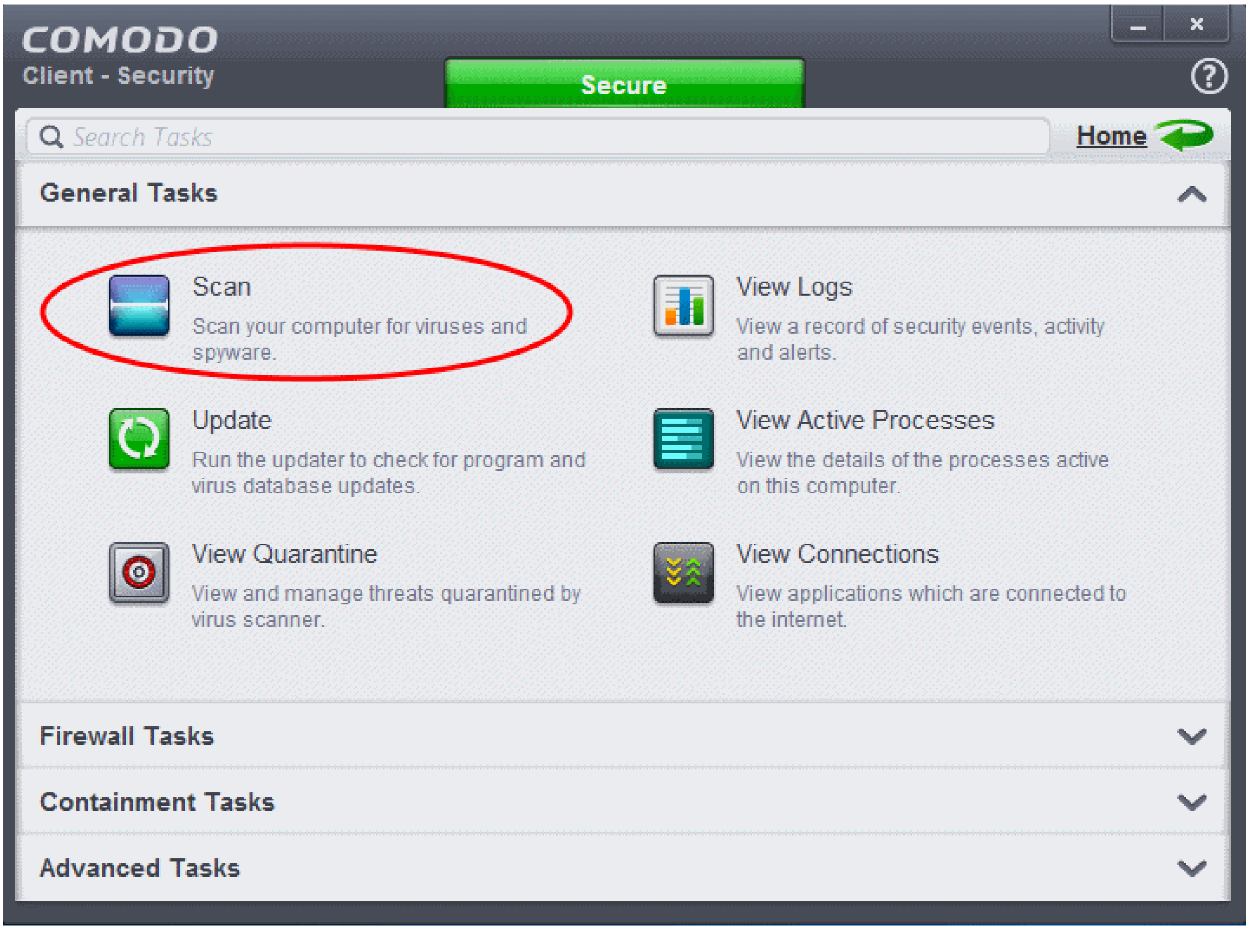

COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
Firewall Tasks
Containment Tasks
Advanced Tasks

'General Tasks' contains the following areas. Click the 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 and Program Updates
- Manage Quarantined Items
- View CCS Logs
- View Active Process List
- View Active Internet Connections

2.1. Scan and Clean Your Computer

Comodo Antivirus leverages multiple technologies, including Real-time/On-Access Scanning and On-Demand Scanning to immediately start cleaning or quarantining suspicious files from your hard drives, shared disks, emails, downloads and system memory. The application also allows users to create custom scan profiles, time-table scheduled scans and features full event logging, quarantine and file submission facilities. When you want to run a virus scan on your system, you can launch an **On-Demand Scan** using the **Scan** option. This executes an instant virus scan on the selected item.



COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
Firewall Tasks
Containment Tasks
Advanced Tasks

There are multiple types of antivirus scan that can be run from the 'Scan' interface. Click the links below to find out more on each:

- 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

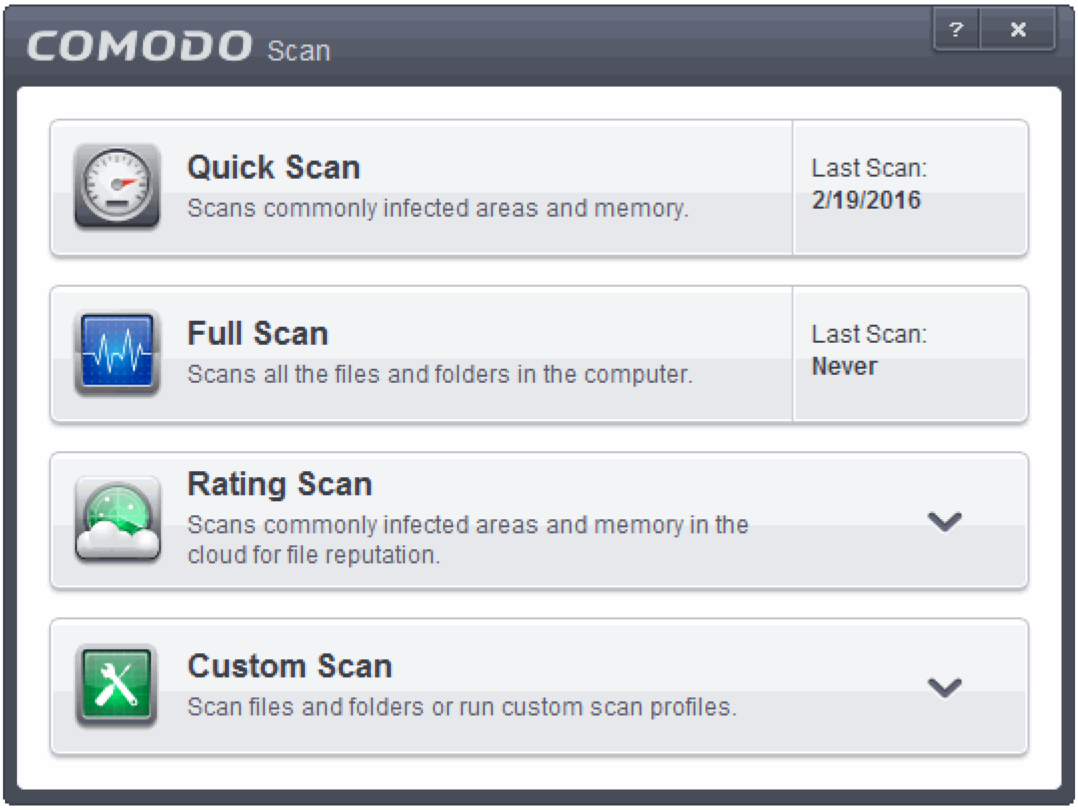
2.1.1. Run a Quick Scan

The 'Quick Scan' profile enables you to quickly scan critical areas of your computer which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of your computer so it is essential to keep them free of infection.

You can customize which items are scanned under a 'Quick Scan' and create a scan schedule from the 'Advanced Tasks' interface. Refer to Antivirus Settings > Scan Profiles Antivirus Settings for more details.

To run a Quick Scan

- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



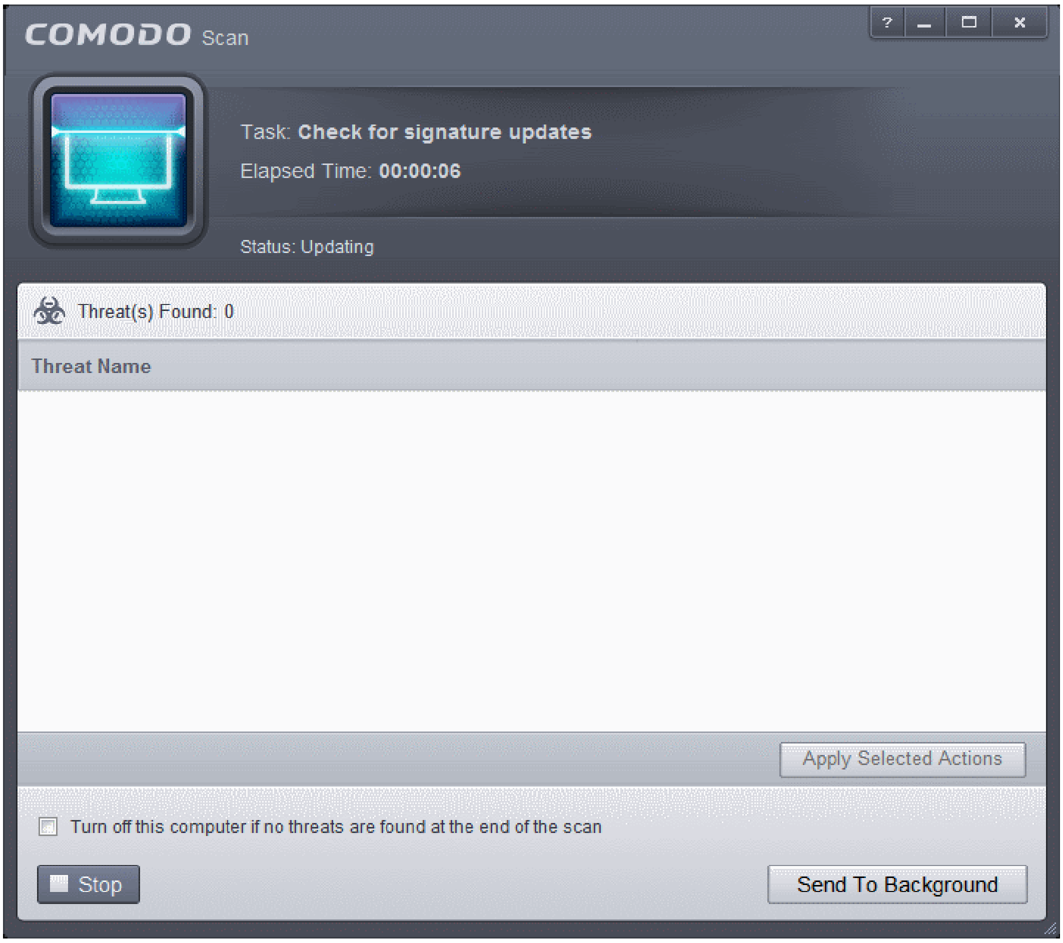
Quick Scan
Scans commonly infected areas and memory.
Last Scan: 2/19/2016

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

Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.

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

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



Task: **Check for signature updates**

Elapsed Time: **00:00:06**

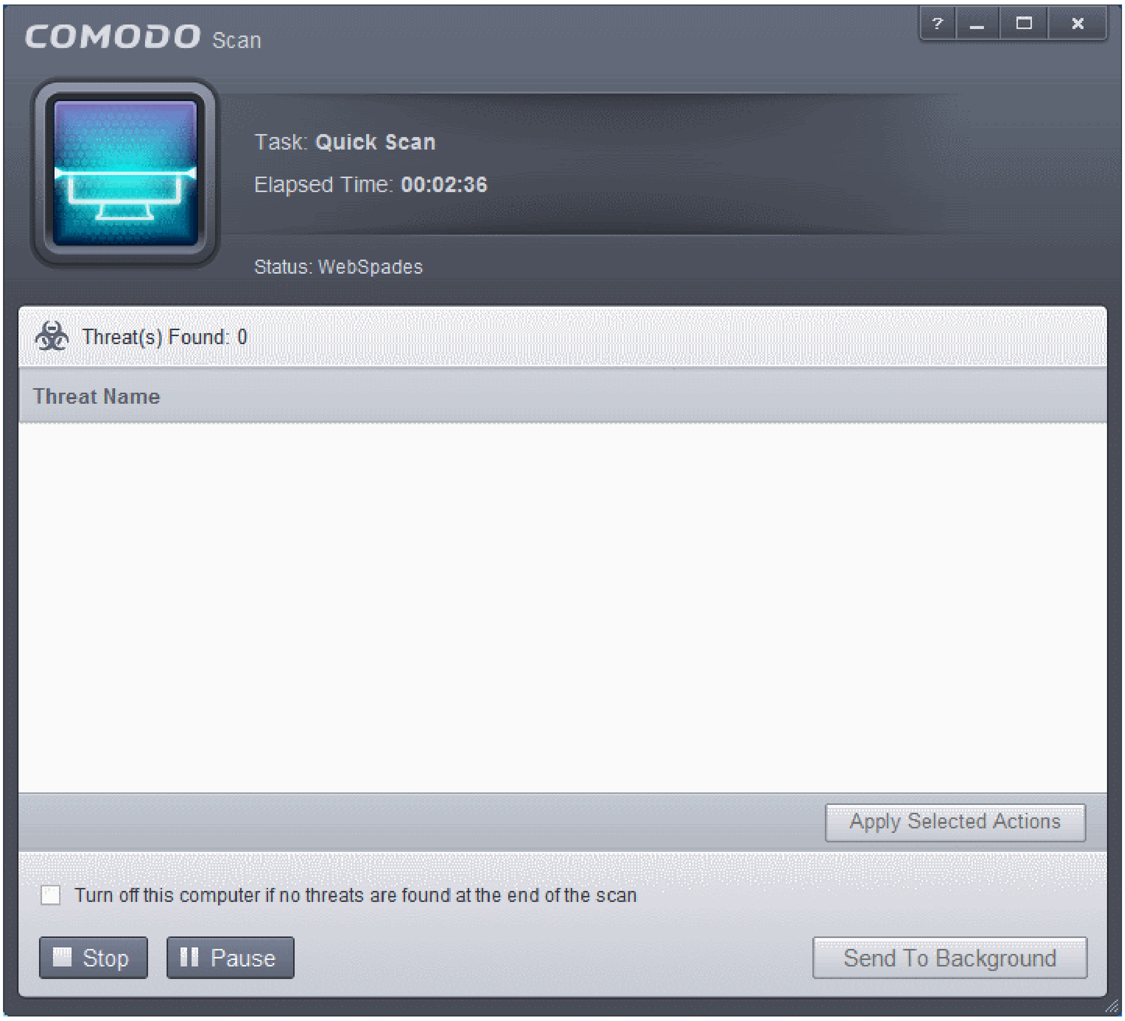
Status: Updating

Threat(s) Found: 0

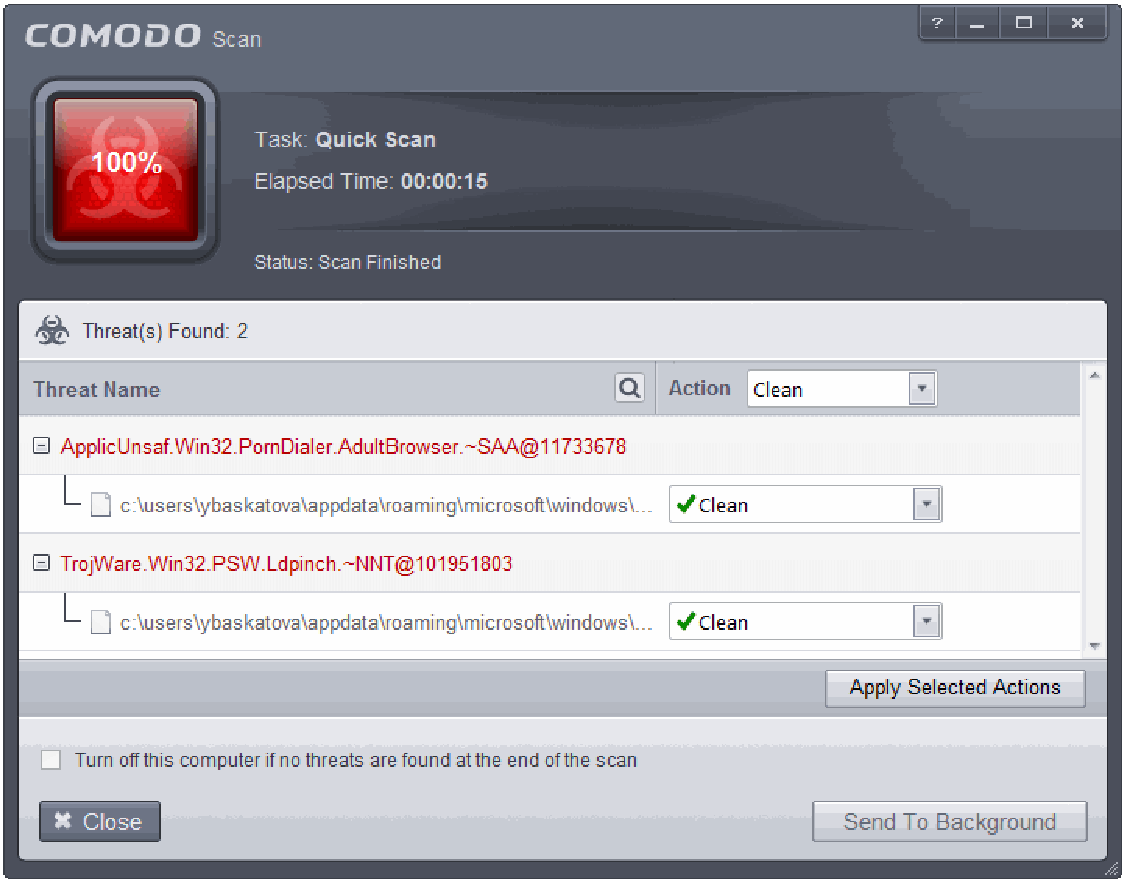
Threat Name

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

If the database is outdated, 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 respective buttons. 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.
- On completion of scanning, the results will be displayed with a list of identified infections
- To open or close the lower panel that shows the list of infected files detected during the course of scan, click the down/up arrow.



Task: Quick Scan

Elapsed Time: 00:00:15

Status: Scan Finished

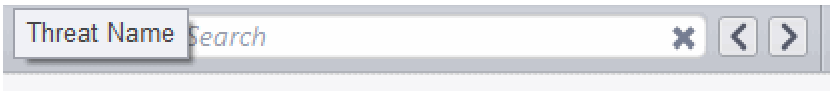
Threat(s) Found: 2

Threat Name	Action: Clean
⊟ ApplicUnsaf.Win32.PornDialer.AdultBrowser.~SAA@11733678	
c:\users\ybaskatova\appdata\roaming\microsoft\windows\...	✓ Clean
⊟ TrojWare.Win32.PSW.Ldpinch.~NNT@101951803	
c:\users\ybaskatova\appdata\roaming\microsoft\windows\...	✓ Clean

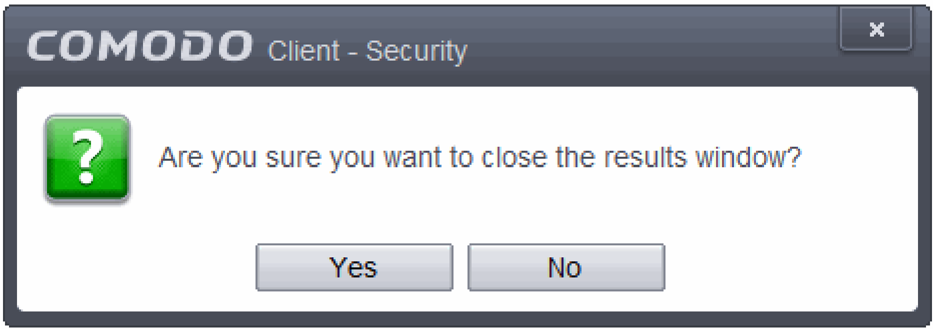
□ Turn off this computer if no threats are found at the end of the scan

You can use the search option to find a specific item in the list.

To use the search option, click the search 🔍 at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.
- Click 'Close' to close the results window



Are you sure you want to close the results window?

- Click 'Yes' in the confirmation window.

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. Refer to Processing the infected files for more details.

2.1.2. Run a Full Computer Scan

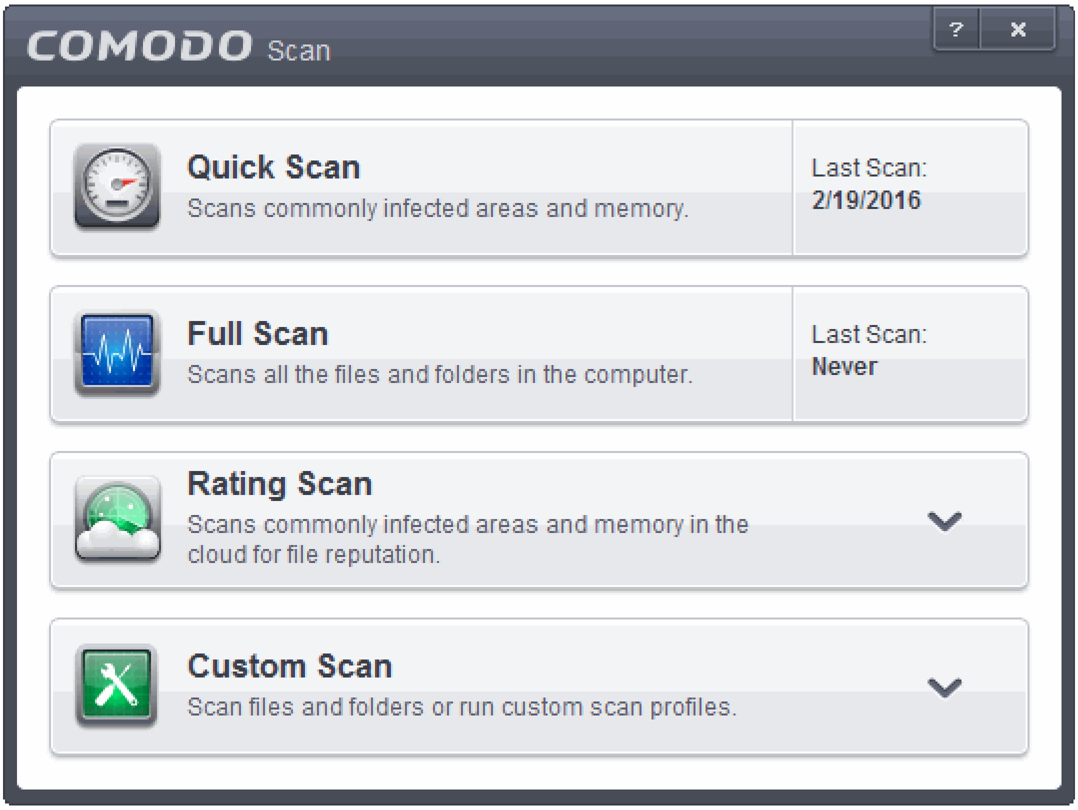
The 'Full System Scan' scans every local drive, folder and file on your system. Any external devices like USB drives, digital camera and so on are also scanned.

You can customize the items scanned during a 'Full System Scan and set-up a scan schedule from the 'Advanced Tasks' interface.

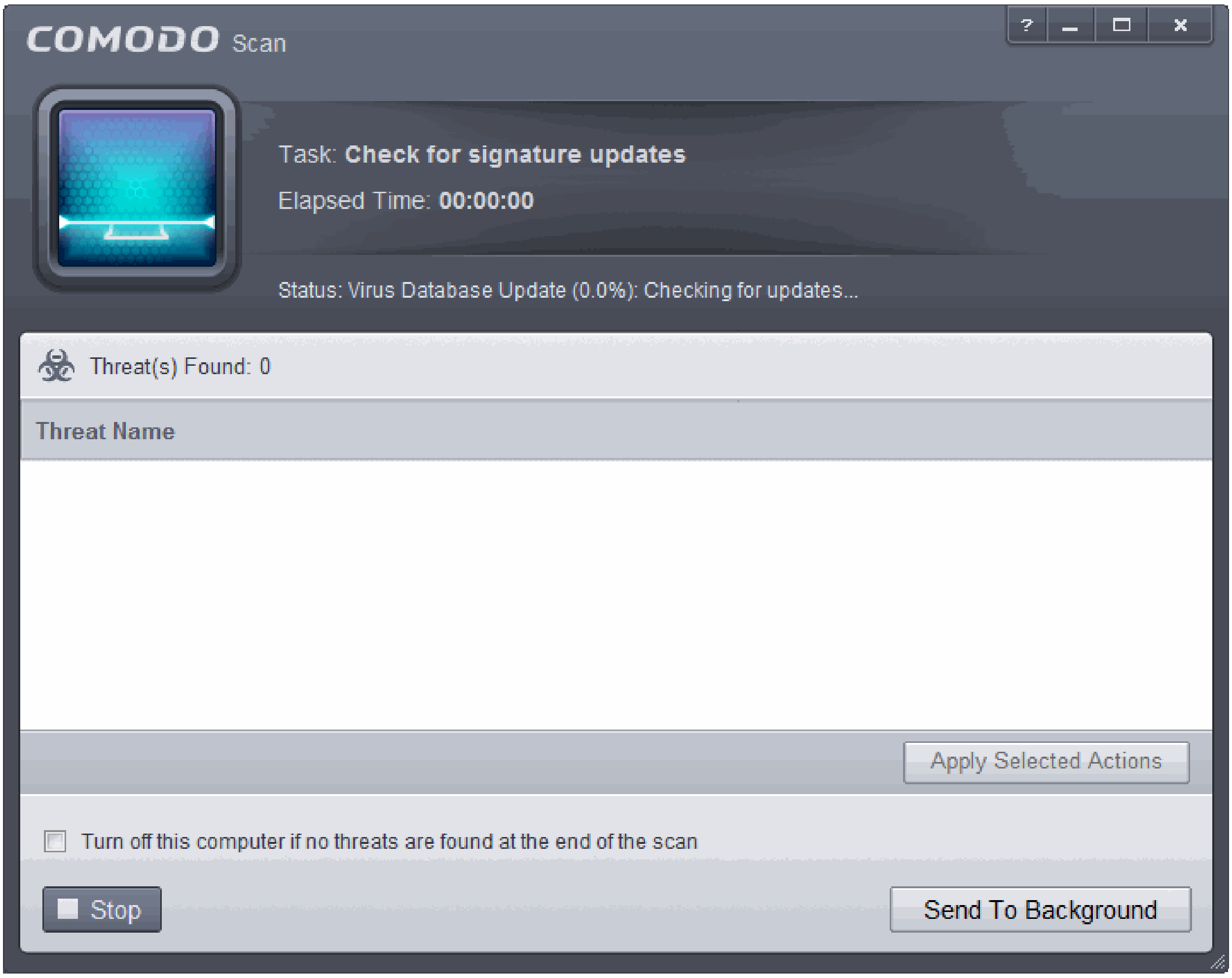
Refer to Antivirus Settings > Scan Profiles for more details.

To run a Full Computer Scan

- Click 'Scan' from the General Tasks interface and click 'Full Scan' from the 'Scan' interface.

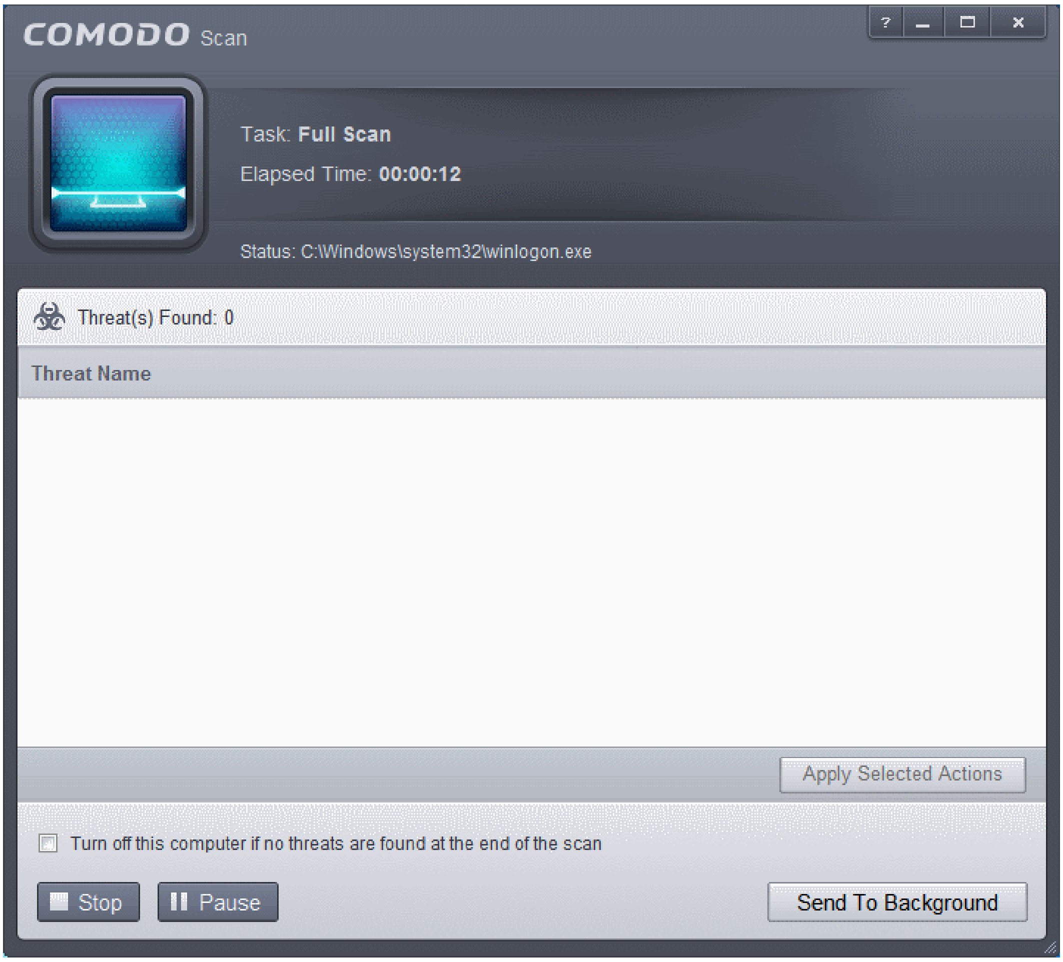

COMODO Scan
?
×
Quick Scan
Scans commonly infected areas and memory.
Last Scan:
2/19/2016
Full Scan
Scans all the files and folders in the computer.
Last Scan:
Never
Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
Custom Scan
Scan files and folders or run custom scan profiles.

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

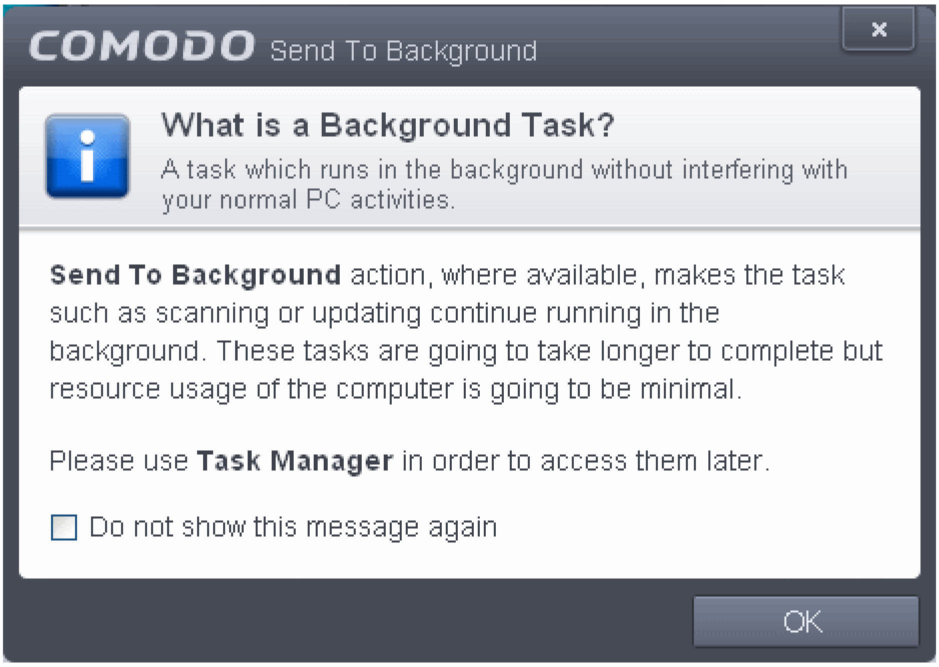


COMODO Scan
Task: Check for signature updates
Elapsed Time: 00:00:00
Status: Virus Database Update (0.0%): Checking for updates...
Threat(s) Found: 0
Threat Name
Apply Selected Actions
□ Turn off this computer if no threats are found at the end of the scan
Stop
Send To Background

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



- You can Pause, Resume or Stop the scan by clicking the respective buttons. If you want to run the scan in the background, click 'Send to Background'.


COMODO Send To Background

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

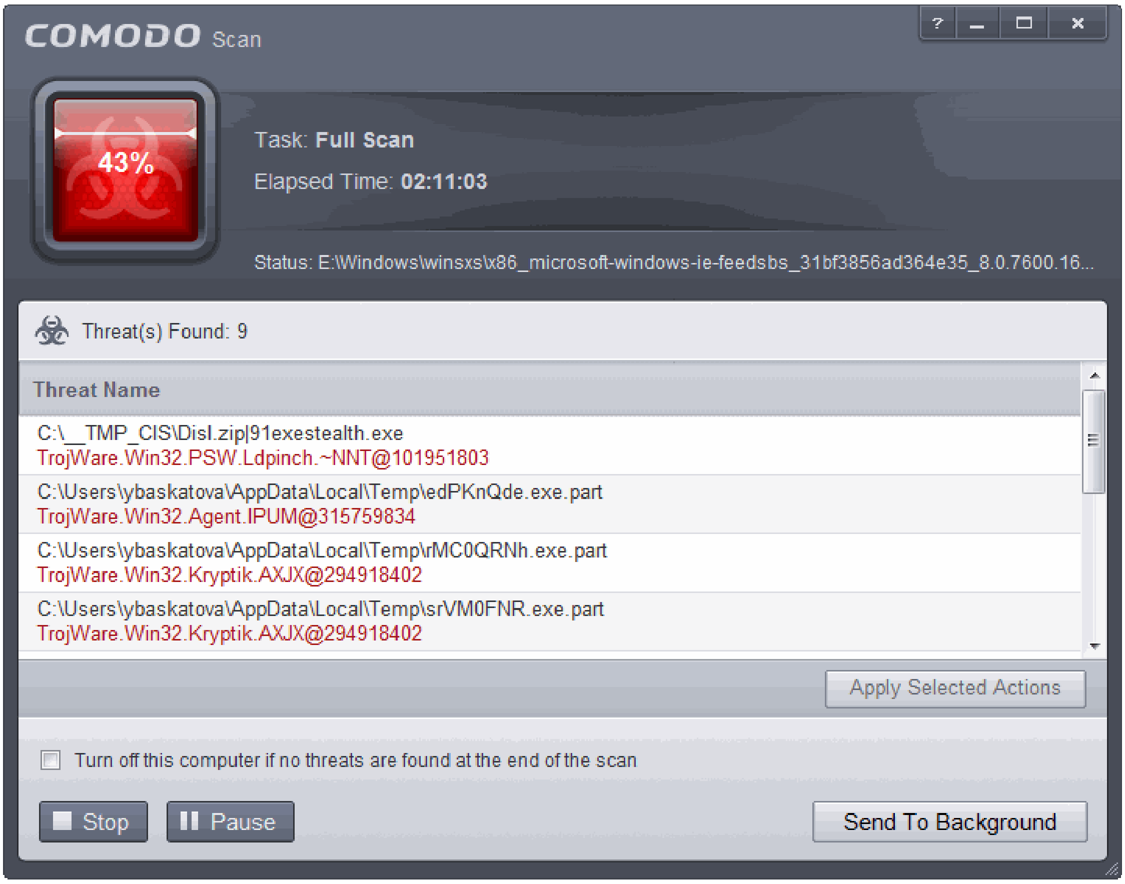
Send To Background action, where available, makes the task such as scanning or updating continue running in the background. These tasks are going to take longer to complete but resource usage of the computer is going to be minimal.

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

☐ Do not show this message again

OK

You can still view scan progress by clicking 'Task Manager' on the home screen.



Task: Full Scan

Elapsed Time: 02:11:03

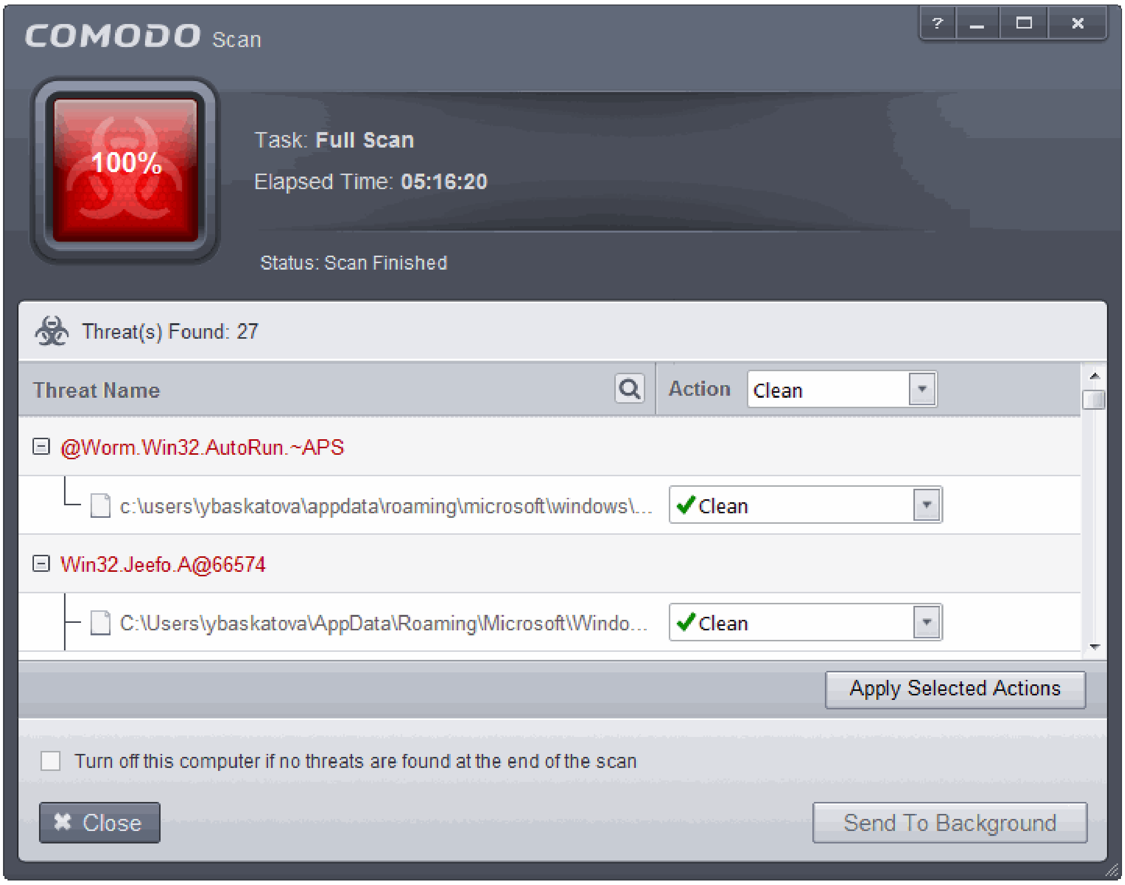
Status: E:\Windows\winsxs\x86_microsoft-windows-ie-feedsbs_31bf3856ad364e35_8.0.7600.16...

Threat(s) Found: 9

Threat Name
C:\__TMP_CIS\Disl.zip|91exestealth.exe TrojWare.Win32.PSW.Ldpinch.~NNT@101951803
C:\Users\ybaskatova\AppData\Local\Temp\edPKnQde.exe.part TrojWare.Win32.Agent.IPUM@315759834
C:\Users\ybaskatova\AppData\Local\Temp\rMC0QRNh.exe.part TrojWare.Win32.Kryptik.AXJX@294918402
C:\Users\ybaskatova\AppData\Local\Temp\srVM0FNR.exe.part TrojWare.Win32.Kryptik.AXJX@294918402

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

- On completion of scanning, if any threats are found, an alert screen will be displayed.



Task: Full Scan

Elapsed Time: 05:16:20

Status: Scan Finished

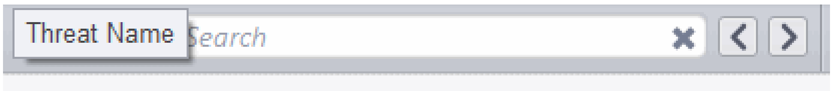
Threat(s) Found: 27

Threat Name	Action: Clean
⊟ @Worm.Win32.AutoRun.~APS	
c:\users\ybaskatova\appdata\roaming\microsoft\windows\...	✓Clean
⊟ Win32.Jeefo.A@66574	
C:\Users\ybaskatova\AppData\Roaming\Microsoft\Windo...	✓Clean

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

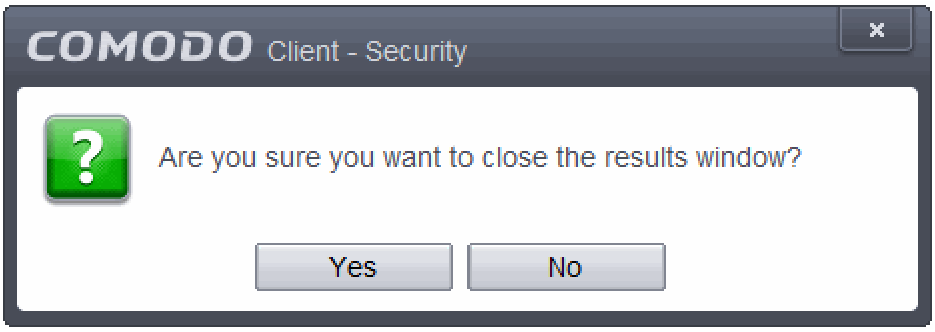
You can use the search option to find a specific item in the list.

To use the search option, click the search 🔍 at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Click 'Close' to close the results window



Are you sure you want to close the results window?

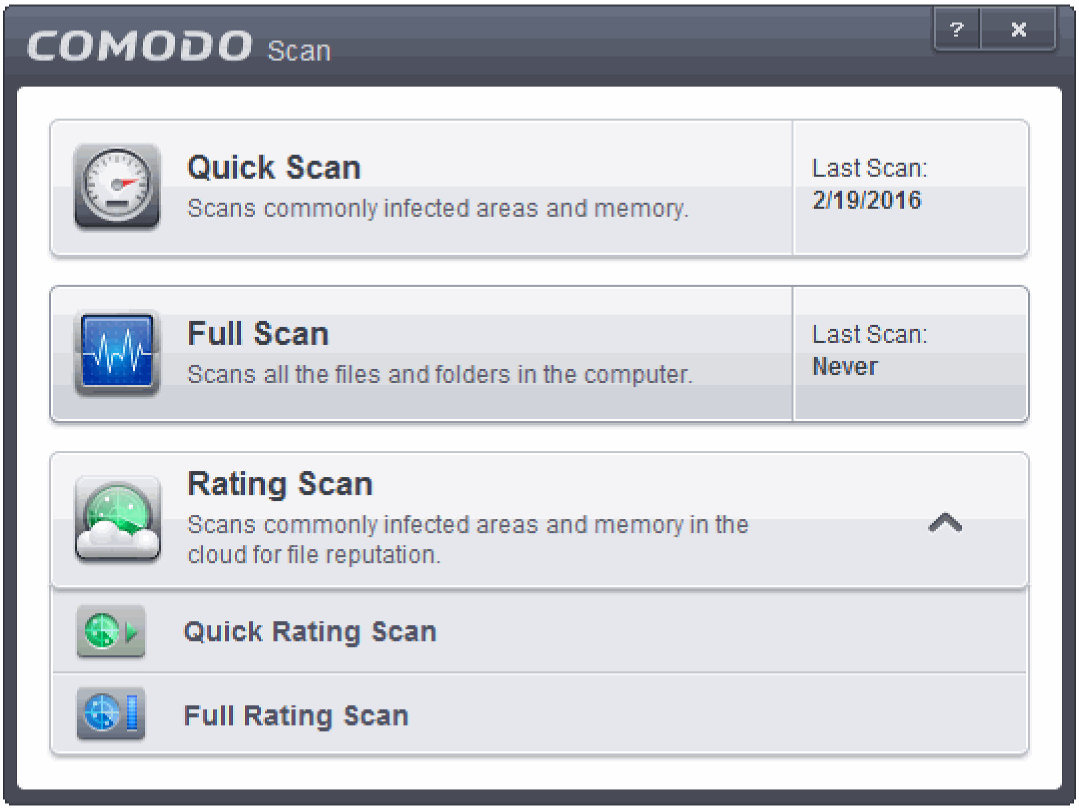
Click 'Yes' in the confirmation window.

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. Refer to Processing the infected files for more details.

2.1.3. Run a Rating Scan

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

To run a Rating Scan click 'Scan' from the 'General Tasks' interface then click 'Rating Scan'. The 'Rating Scan' panel will open:



COMODO Scan

Quick Scan
Scans commonly infected areas and memory.
Last Scan: 2/19/2016

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

Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.

Quick Rating Scan

Full Rating Scan

The 'Rating Scan' panel contains the following scan options. Click the links to jump to the help page for that topic.

- Quick Rating Scan - Obtain a trust assessment of files in key areas of your system
- Full Rating Scan – Run a scan on your entire system and get a trust assessment of all discovered files.

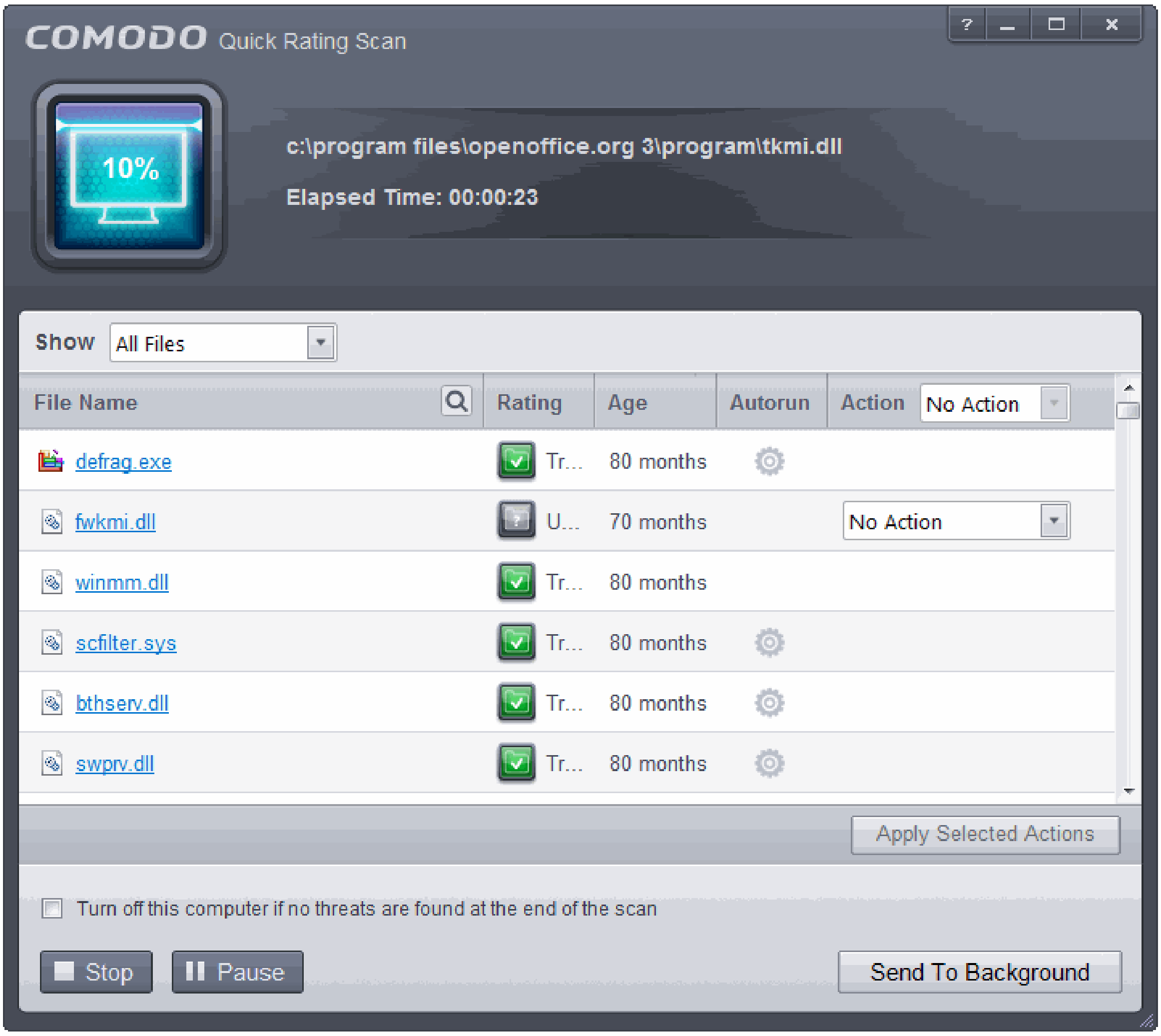
Run a Quick Rating scan

The 'Rating Scan' feature runs a cloud-based assessment areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files.

To run a Rating scan

- Click the curved 'Tasks' arrow on the home screen then click 'General Tasks' > 'Scan' > 'Rating Scan' > 'Quick Rating Scan ':

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



COMODO Quick Rating Scan

10%

c:\program files\openoffice.org 3\program\tkmi.dll

Elapsed Time: 00:00:23

Show: All Files

File Name	Rating	Age	Autorun	Action: No Action
defrag.exe	✓ Tr...	80 months	⚙	
fwkmi.dll	? U...	70 months		No Action
winmm.dll	✓ Tr...	80 months		
scfilter.sys	✓ Tr...	80 months	⚙	
bthserv.dll	✓ Tr...	80 months	⚙	
swprv.dll	✓ Tr...	80 months	⚙	

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

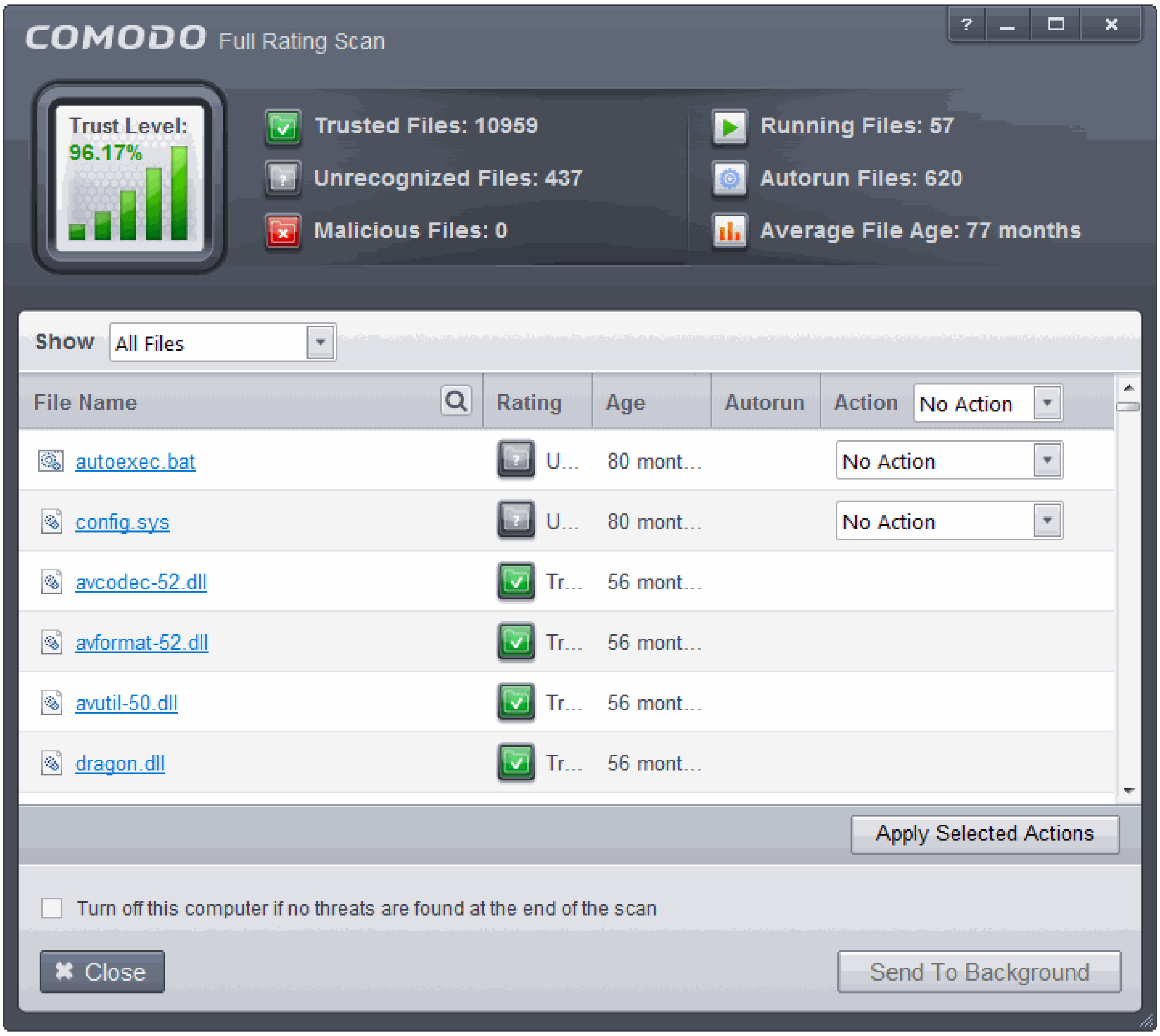
Run a Full Rating scan

The 'Rating Scan' feature runs a cloud-based assessment areas scanned include every local drive, (external devices like USB drives, digital camera are also scanned) folder and file on your system.

To run a Full Computer scan

- Click the curved 'Tasks' arrow on the home screen then click 'General Tasks' > 'Scan' > 'Rating Scan' > 'Full Rating Scan':

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



Trust Level: 96.17%

Trusted Files: 10959

Unrecognized Files: 437

Malicious Files: 0

Running Files: 57

Autorun Files: 620

Average File Age: 77 months

Show: All Files

File Name	Rating	Age	Autorun	Action: No Action
autoexec.bat	U...	80 mont...		No Action
config.sys	U...	80 mont...		No Action
avcodec-52.dll	Tr...	56 mont...		
avformat-52.dll	Tr...	56 mont...		
avutil-50.dll	Tr...	56 mont...		
dragon.dll	Tr...	56 mont...		

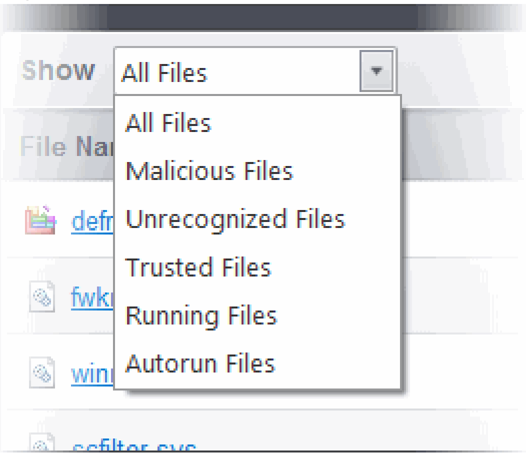
□ Turn off this computer if no threats are found at the end of the scan

- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your computer
- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately.

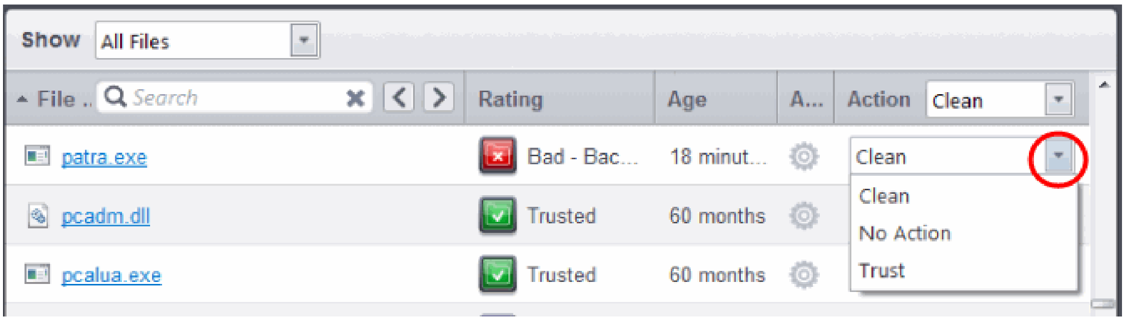
Based on the trustworthiness, the files are rated as:

- Trusted - the file is safe
- Unrecognized - the trustworthiness of the file could not be assessed
- Malicious - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

You can filter the results by rating using the 'Show' drop-down:

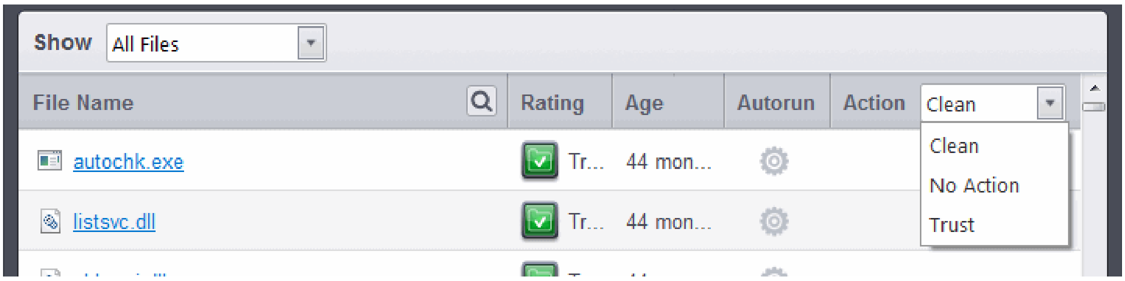


Each file identified as 'Malicious' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

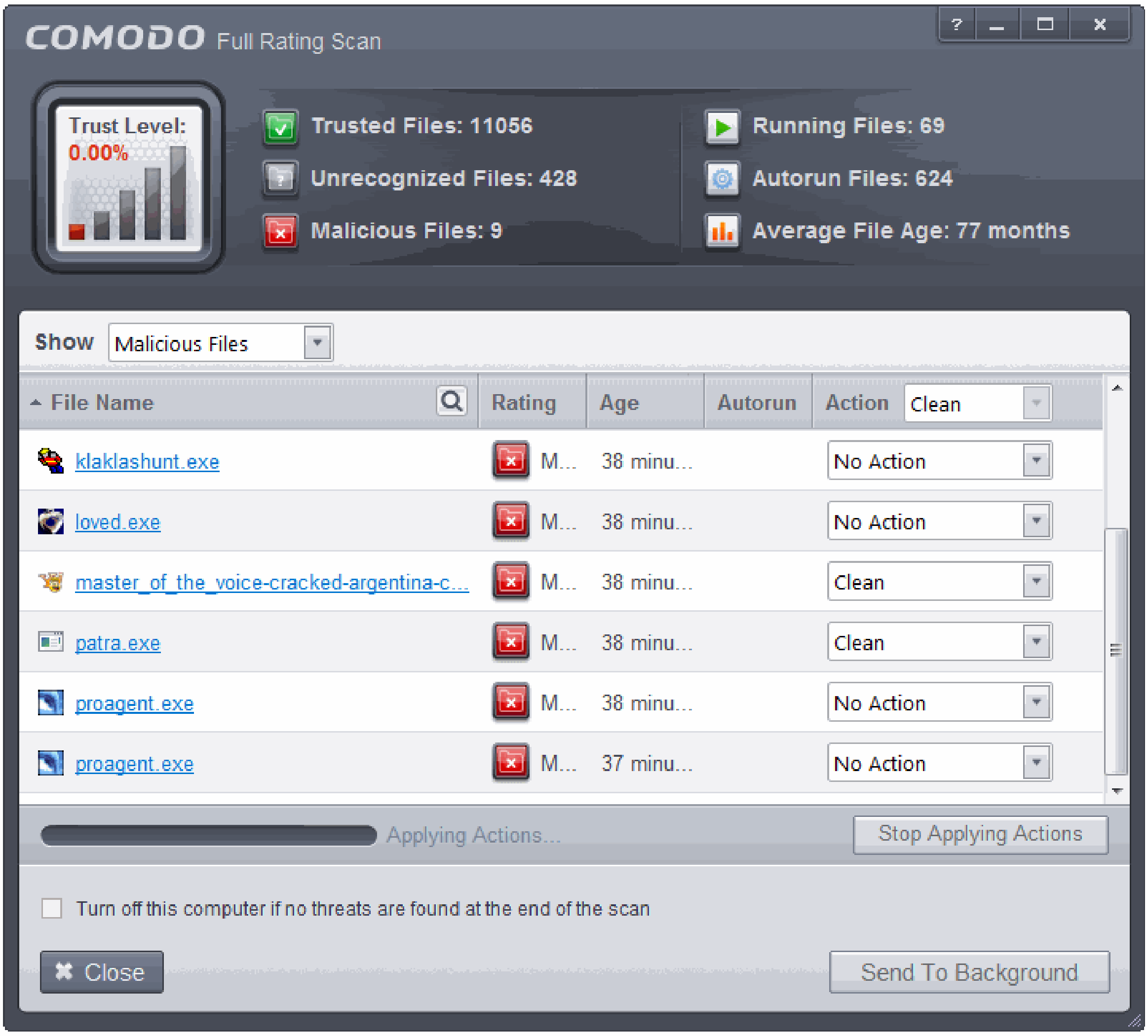


- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See **Manage Quarantined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

For the same action to be applied to all 'Bad' files, make a selection 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:



Trust Level: 0.00%

Trusted Files: 11056
Unrecognized Files: 428
Malicious Files: 9
Running Files: 69
Autorun Files: 624
Average File Age: 77 months

Show: Malicious Files

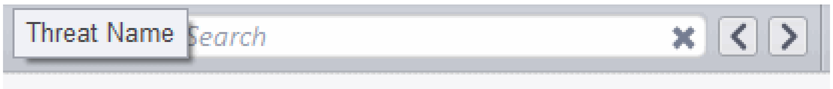
File Name	Rating	Age	Autorun	Action: Clean
klaklashunt.exe	M...	38 minu...		No Action
loved.exe	M...	38 minu...		No Action
master_of_the_voice-cracked-argentina-c...	M...	38 minu...		Clean
patra.exe	M...	38 minu...		Clean
proagent.exe	M...	38 minu...		No Action
proagent.exe	M...	37 minu...		No Action

Applying Actions...

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

You can use the search option to find a specific rule in the list.

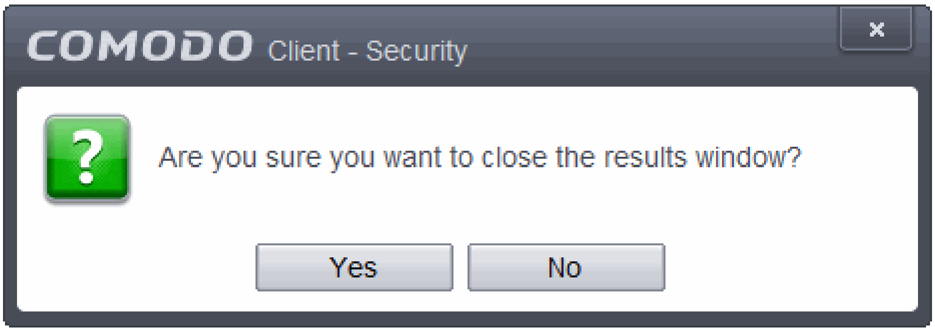
To use the search option, click the search 🔍 at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Click 'Close' to close the results window

- Click 'Close' to exit



COMODO Client - Security

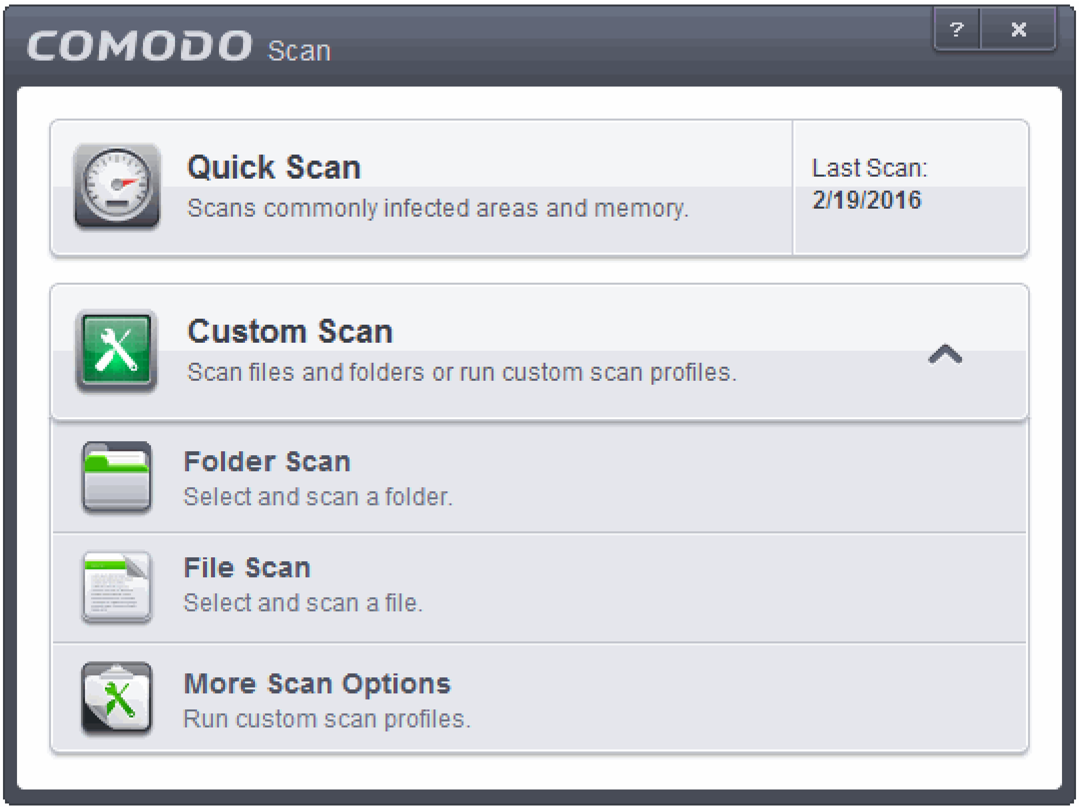
Are you sure you want to close the results window?

Click 'Yes' in the confirmation window.

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 'Scan' from the 'General Tasks' interface then click 'Custom Scan'. The Custom Scan panel will open:



COMODO Scan

Quick Scan
Scans commonly infected areas and memory.

Last Scan:
2/19/2016

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

Folder Scan
Select and scan a folder.

File Scan
Select and scan a file.

More Scan Options
Run custom scan profiles.

The 'Custom Scan' panel contains the following scan options. Click the links to jump to the help page for that topic.

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

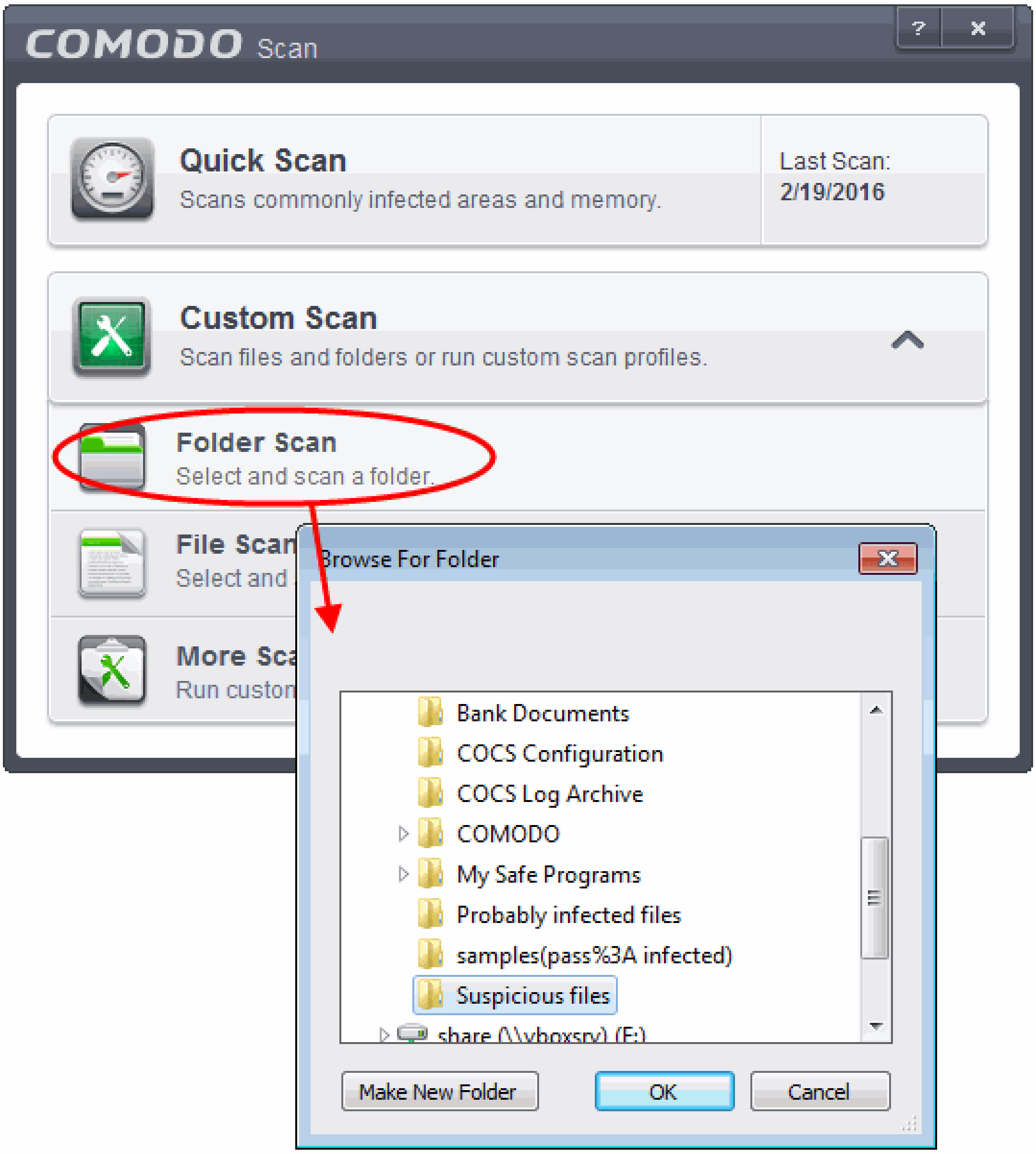
2.1.4.1. Scan a Folder

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

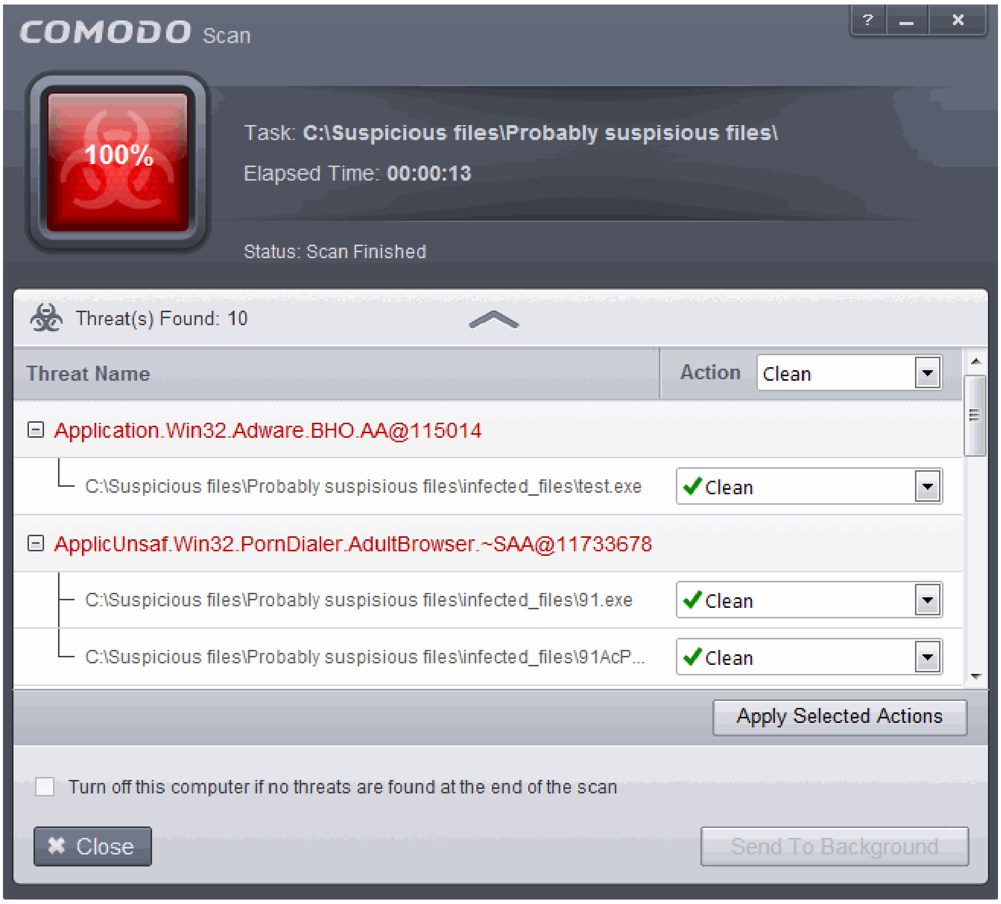
USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan it for viruses and other threats before you open it.

To scan a specific folder

- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'Folder Scan' from the 'Custom Scan' pane
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click 'OK'



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


COMODO Scan

Task: C:\Suspicious files\Probably suspisious files\

Elapsed Time: 00:00:13

Status: Scan Finished

Threat(s) Found: 10

Threat Name	Action: Clean
Application.Win32.Adware.BHO.AA@115014	
C:\Suspicious files\Probably suspisious files\infected_files\test.exe	✓ Clean
ApplicUnsaf.Win32.PornDialer.AdultBrowser.~SAA@11733678	
C:\Suspicious files\Probably suspisious files\infected_files\91.exe	✓ Clean
C:\Suspicious files\Probably suspisious files\infected_files\91AcP...	✓ Clean

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

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

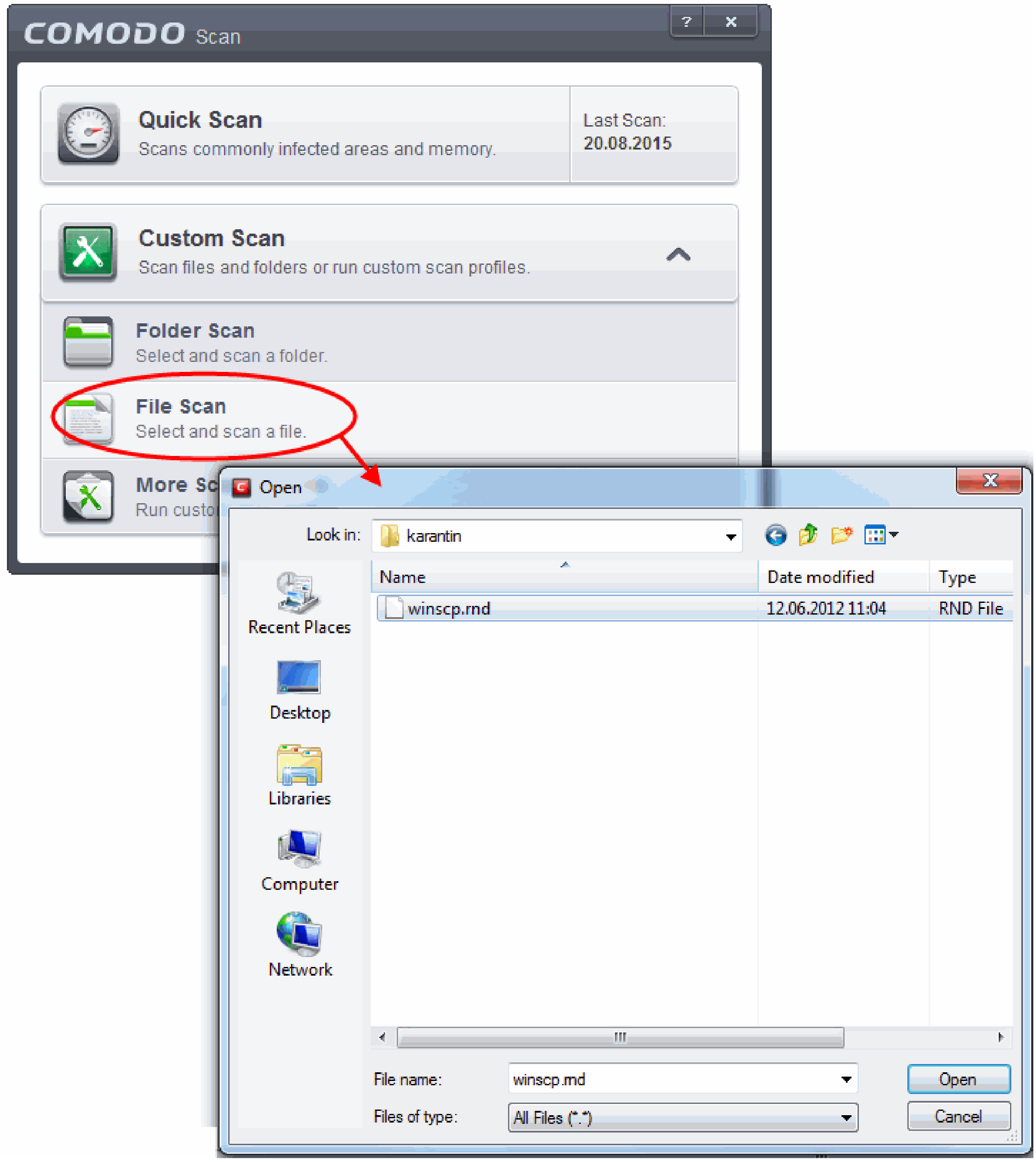
> **Tip**: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CCS interface or by right clicking it. Refer to **Scan Individual File/Folder** for more details.

2.1.4.2. Scan a File

The custom scan allows you to scan a specific file stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have downloaded a file from the Internet or dragged an email attachment onto your desktop and want to scan it for viruses and other threats before you open it.

To scan a specific file

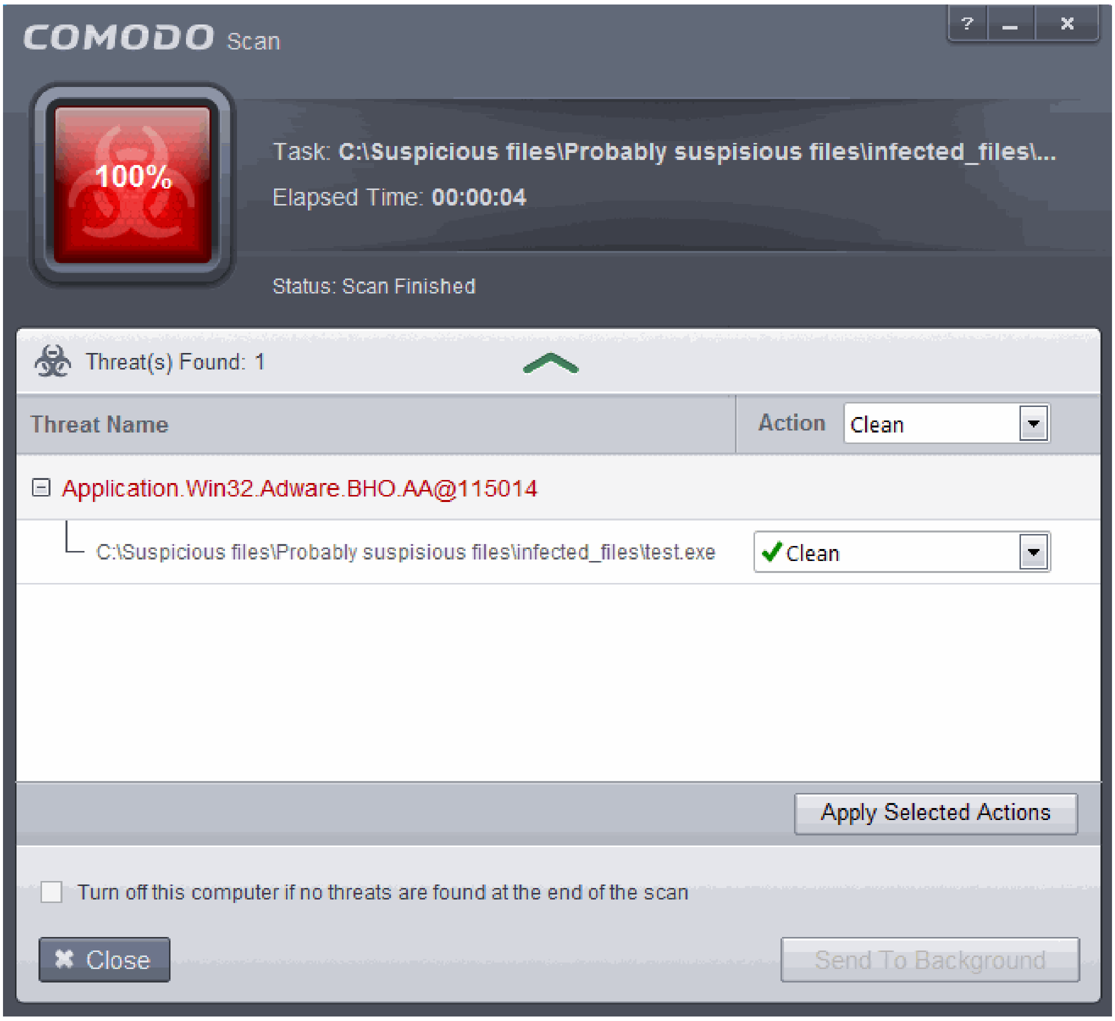
- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'File Scan' from the 'Custom Scan' pane
- Navigate to the file to be scanned in the 'Open' window and click 'Open'



Name	Date modified	Type
winscp.rnd	12.06.2012 11:04	RND File

File name: winscp.rnd

The file will be scanned instantly. On completion of scanning, if any threats are found, an alert screen will be displayed.


COMODO Scan
100%
Task: C:\Suspicious files\Probably suspisious files\infected_files\...
Elapsed Time: 00:00:04
Status: Scan Finished
Threat(s) Found: 1
Threat Name
Action
Clean
Application.Win32.Adware.BHO.AA@115014
C:\Suspicious files\Probably suspisious files\infected_files\test.exe
✓ Clean
Apply Selected Actions
□ Turn off this computer if no threats are found at the end of the scan
Close
Send To Background

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. Refer to Processing the infected files for more details.

Tip: Alternatively, you can perform an express scan on a file by dragging and dropping it onto the CCS interface or by right clicking it. Refer to Scan Individual File/Folder for more details.

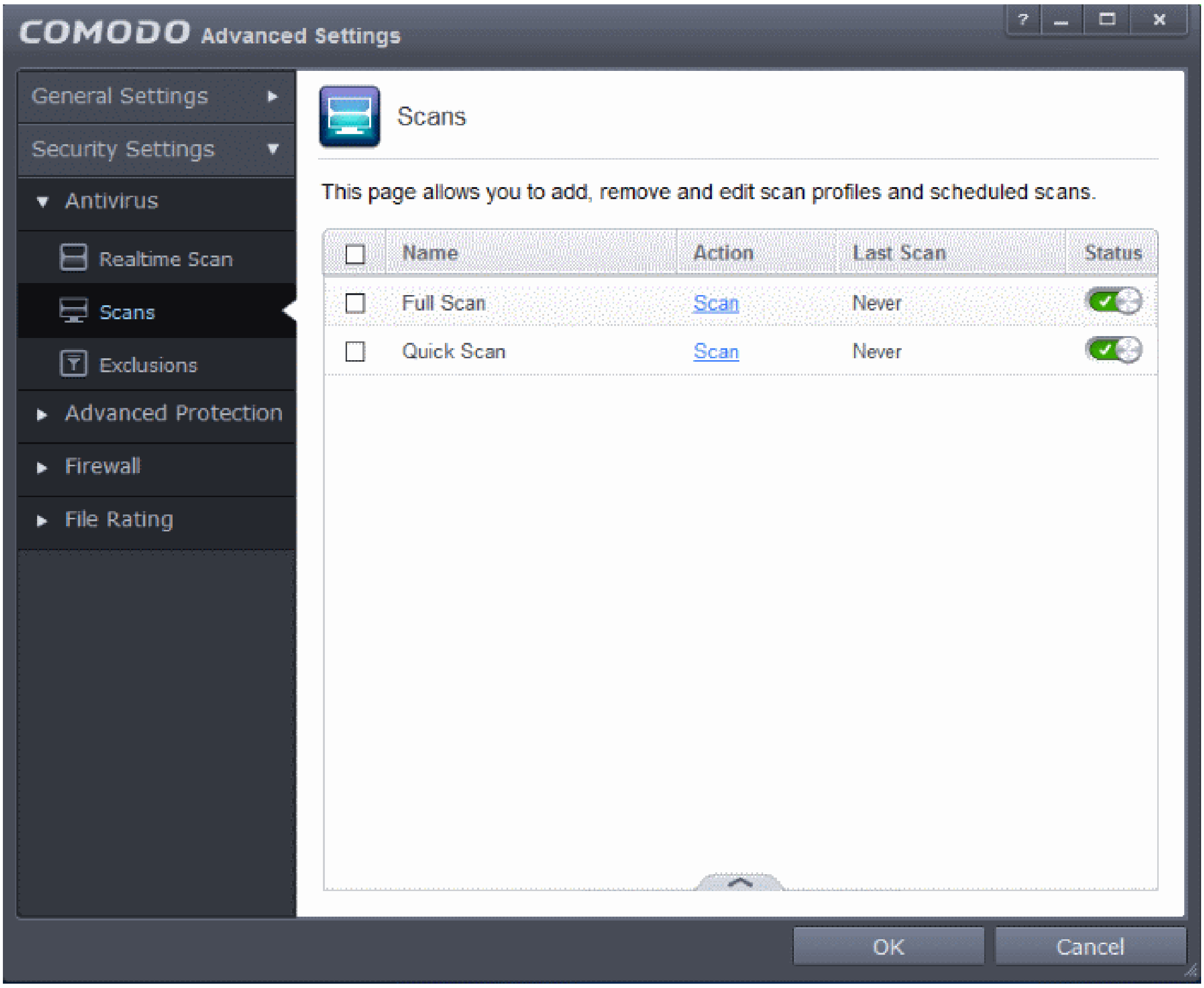
2.1.4.3. Create, Schedule and Run a Custom Scan

By creating a custom scan profile, you can choose exactly which files and folders are scanned, when they are scanned and how they are scanned. Once created and saved, your custom scan profile will appear in the scans interface and can be run, on demand, at any time.

- Creating a Scan Profile
- Running a custom scan

To create a custom profile

- Click the 'Tasks' arrow on the home screen to open the main Tasks menu
- In 'General Tasks', click 'Scan'
- Select 'Custom Scan' then 'More Scan Options'
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened
- Click the handle at the bottom of the interface then select 'Add':



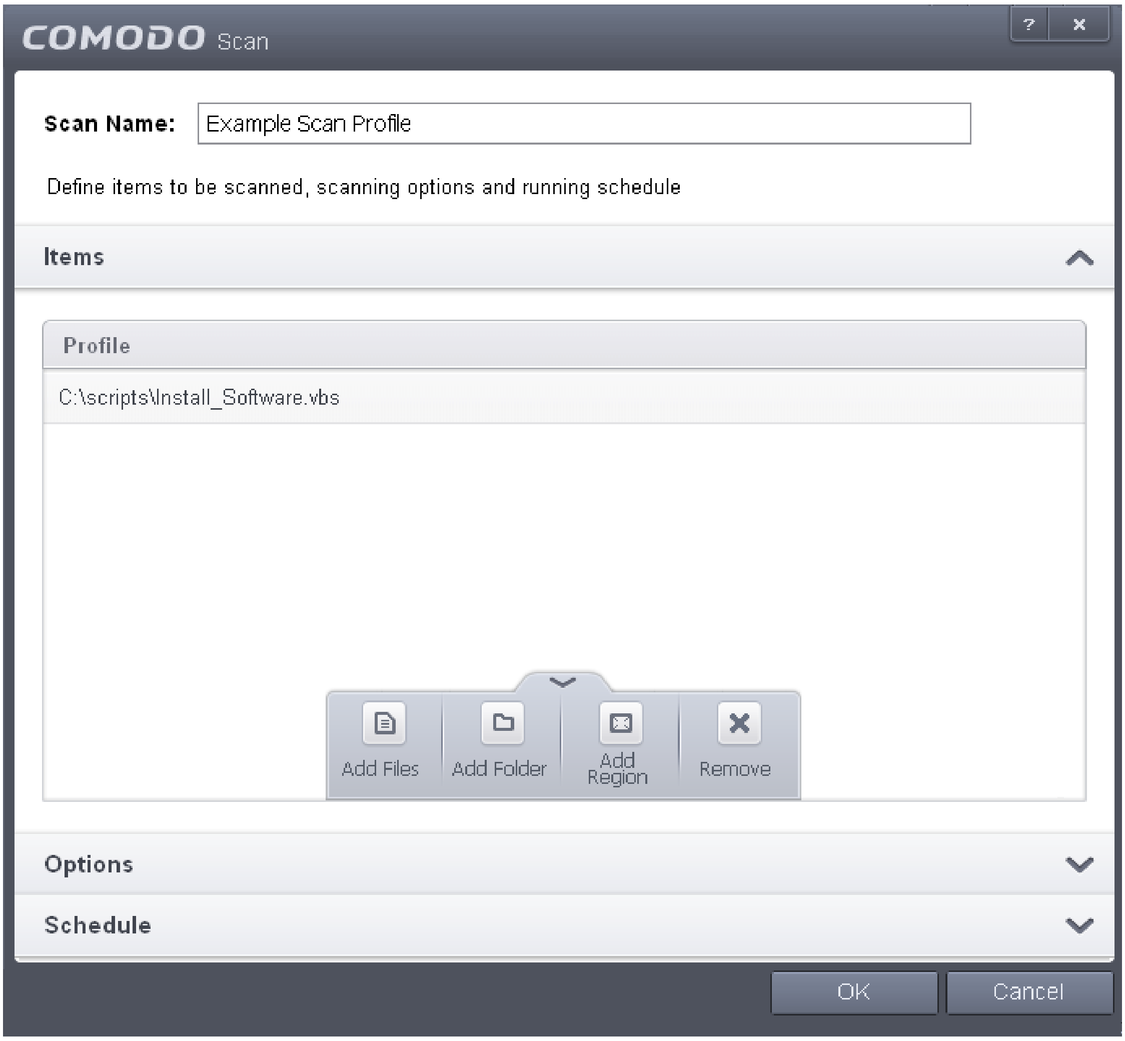
Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	Never	✓

The scan profile interface will be displayed.

- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:

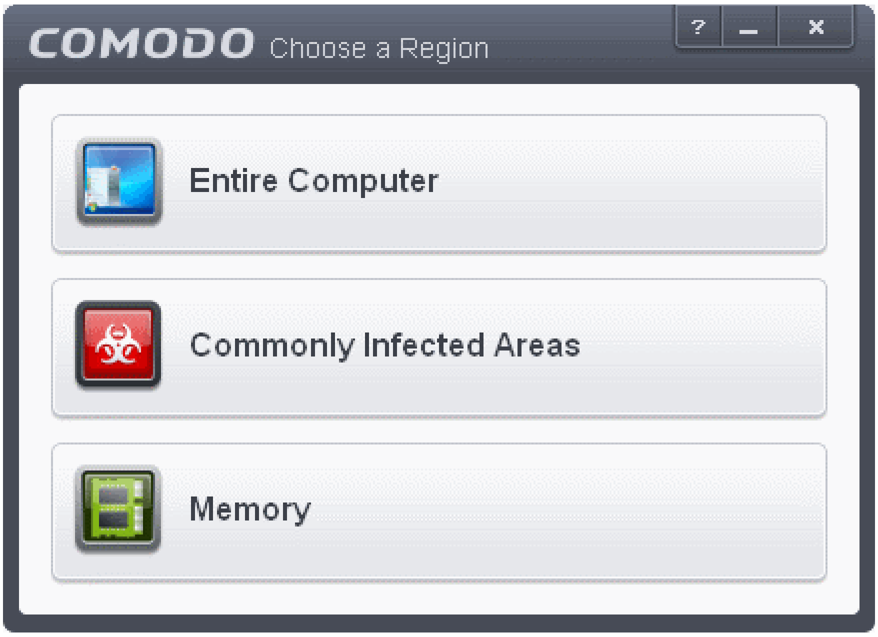


Scan Name: Example Scan Profile

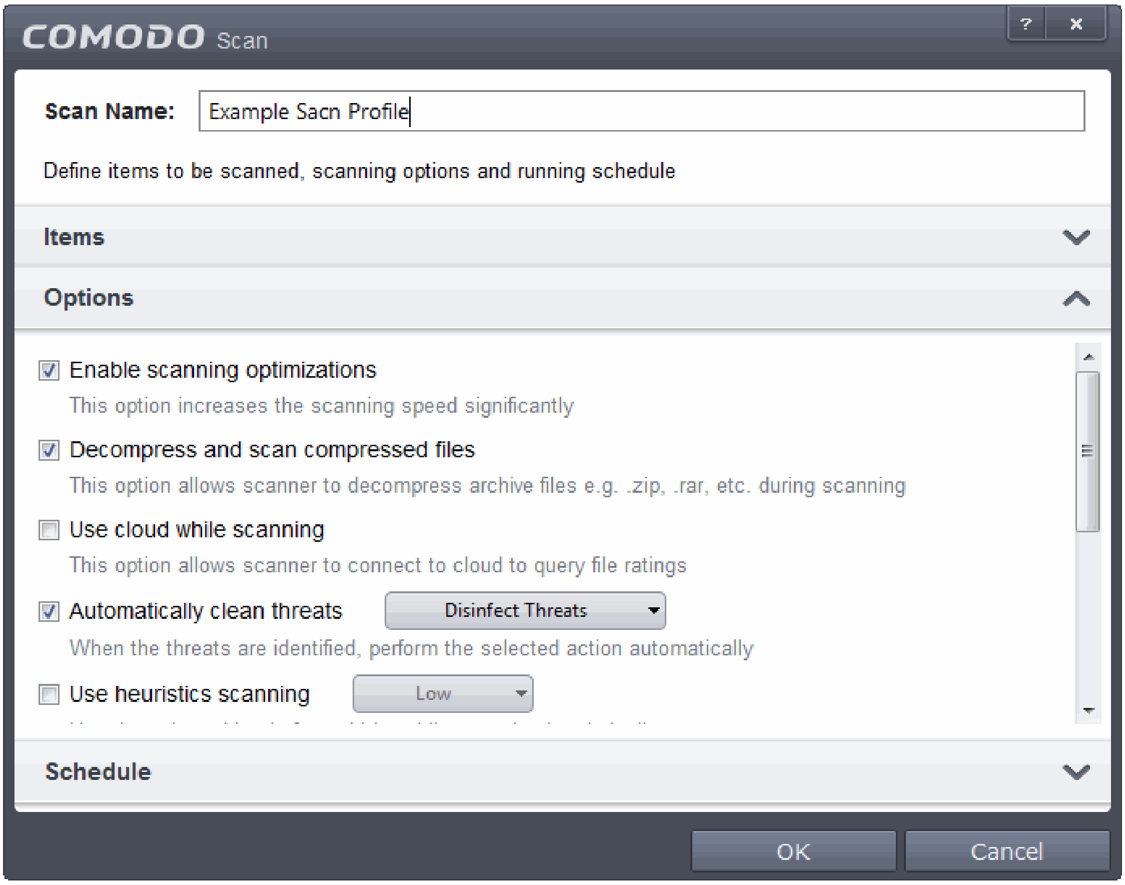
Define items to be scanned, scanning options and running schedule

C:\scripts\Install_Software.vbs

- **Add File** - Allows you to add individual files to the profile.
- **Add Folder** - Allows you to select entire folders to be included in the profile
- **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. Click 'OK' to confirm your choice.
- Next, click 'Options' to further customize the scan:



Scan Name: Example Sacn Profile

Define items to be scanned, scanning options and running schedule

☑ Enable scanning optimizations

This option increases the scanning speed significantly

☑ Decompress and scan compressed files

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

□ Use cloud while scanning

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

☑ Automatically clean threats: Disinfect Threats

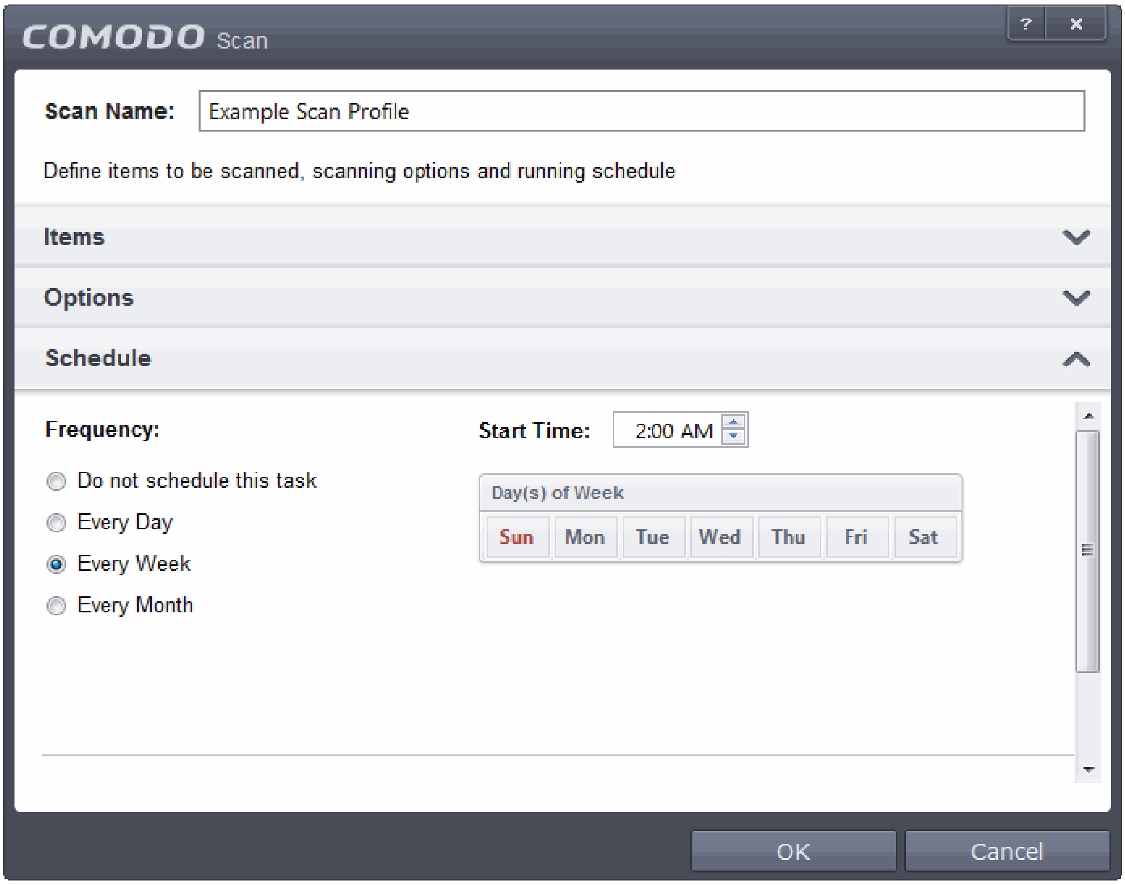
When the threats are identified, perform the selected action automatically

□ Use heuristics scanning: Low

- Options:
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)***
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)***
  - **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antvirus database is out-dated. ***(Default = Enabled)***
  - **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting threats or moving the threats to quarantine ***(Default = Enabled)***
  - **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.

  - **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 how much computer resources should be used for the scan profile. You can select the priority from the drop-down.***(Default = Enabled)***
- **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)***

- If you want the scan to run at specific times, click 'Schedule':



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Frequency:

○ Do not schedule this task
○ Every Day
● Every Week
○ Every Month

Start Time: 2:00 AM

Day(s) of Week

  - **Do not schedule this task -** The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
  - **Every Day -** The Antivirus starts scanning the areas defined in the scan profile every day at the

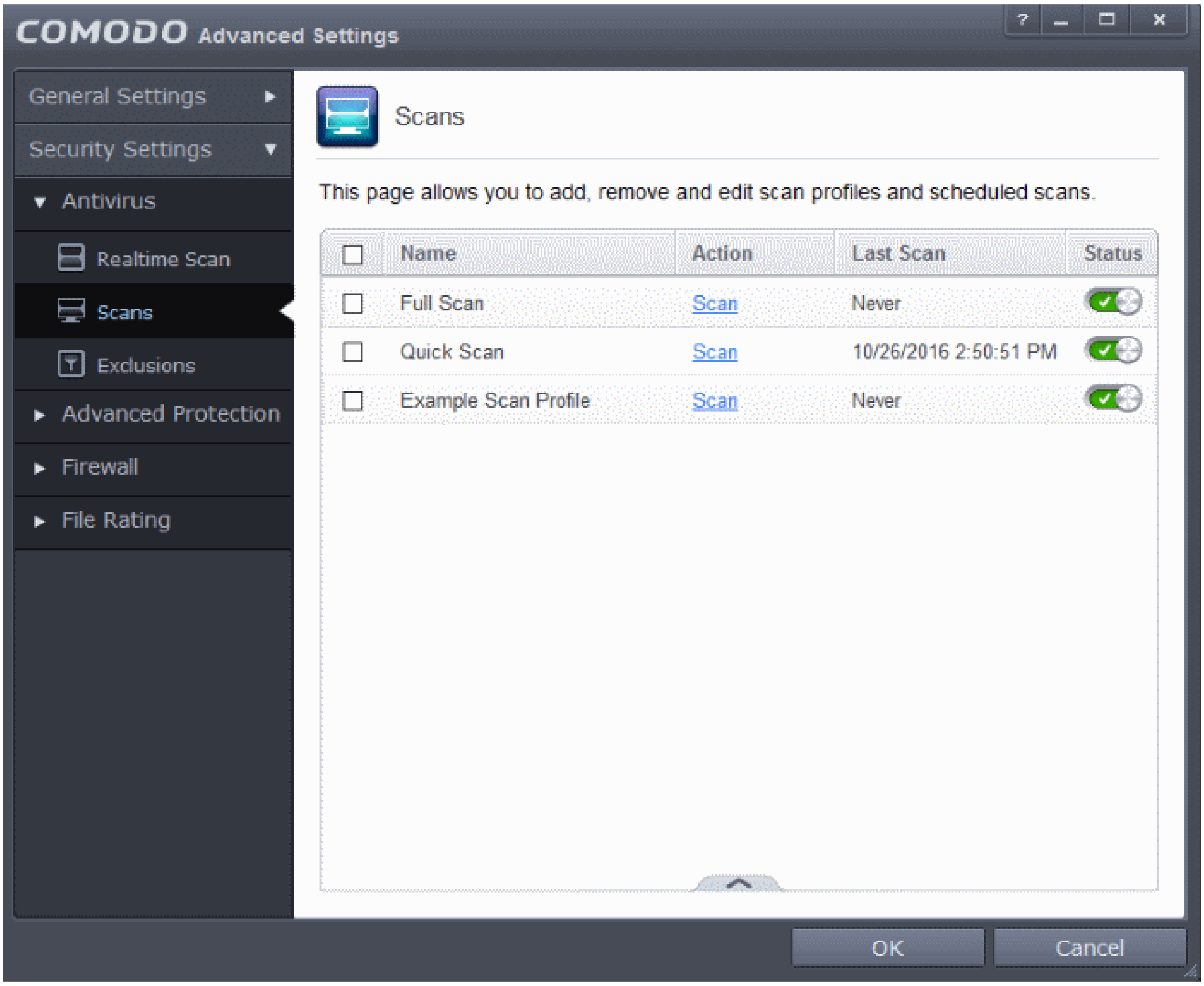
time specified in the Start Time field

- **Every Week** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
- **Run only when computer id IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
- **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 the scans to run at nights.

- Click 'OK' to save the profile.

Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.

The profile will be available for deployment in future.



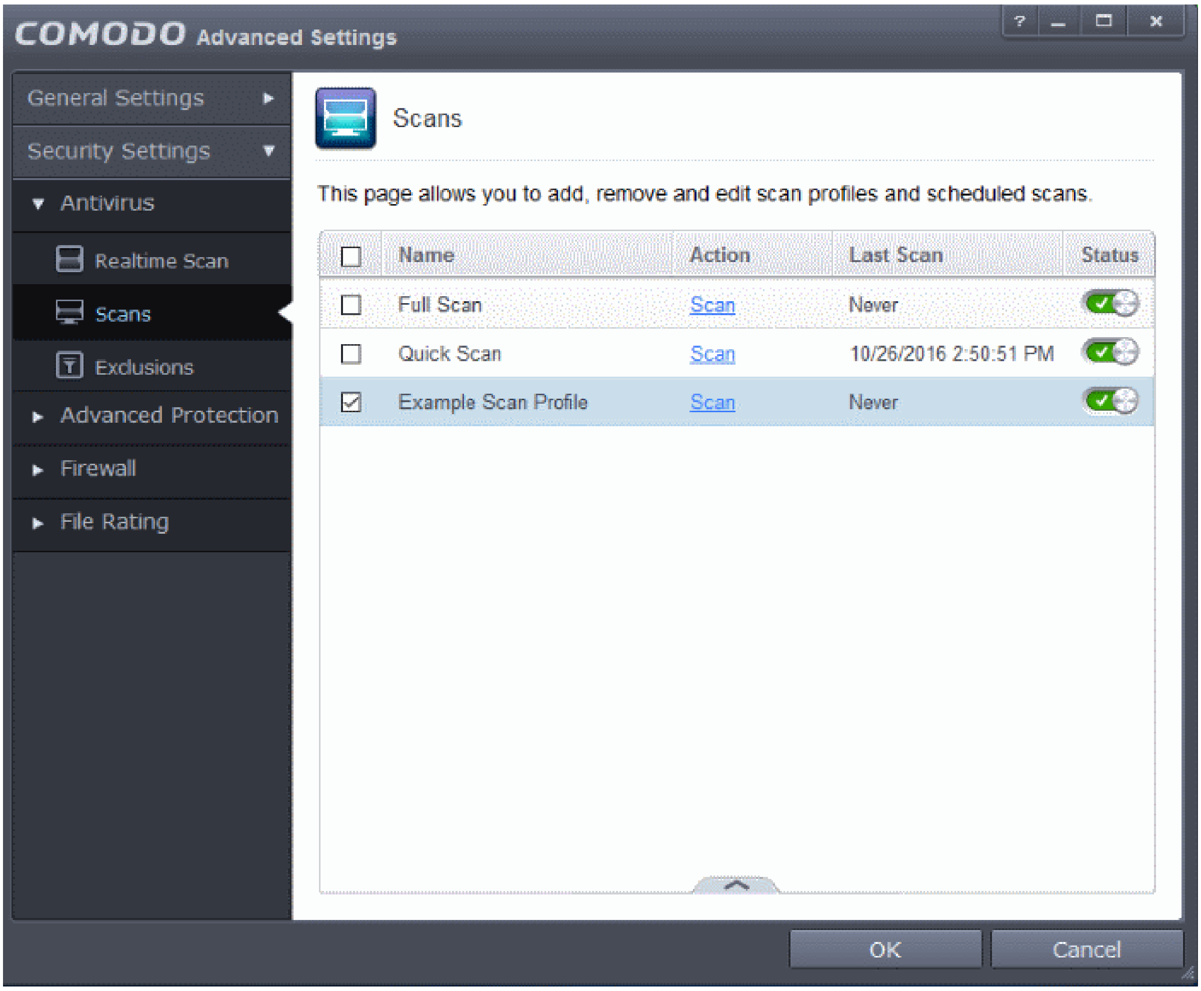
Scans

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

☐	Name	Action	Last Scan	Status
☐	Full Scan	Scan	Never	✓
☐	Quick Scan	Scan	10/26/2016 2:50:51 PM	✓
☐	Example Scan Profile	Scan	Never	✓

To run a custom scan

- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click 'Scan' beside the required scan profile.

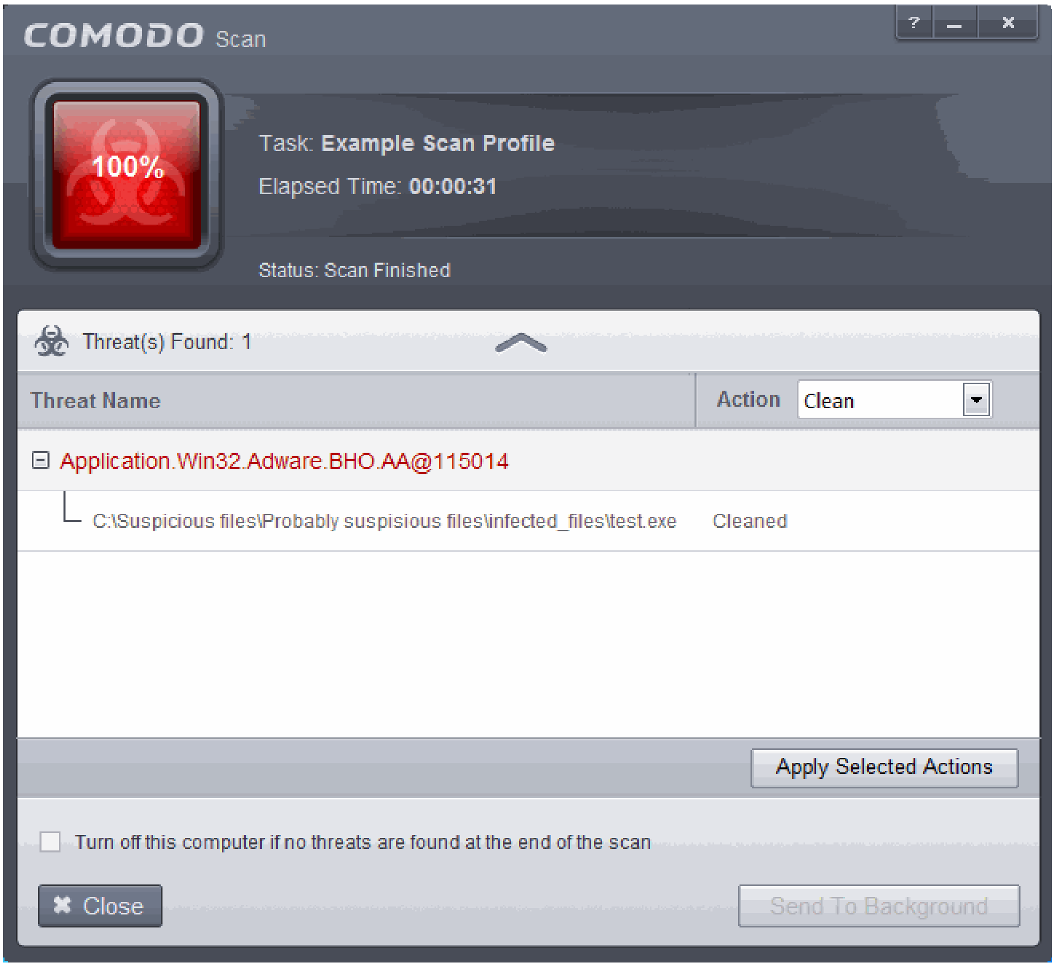


Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	10/26/2016 2:50:51 PM	✓
☑	Example Scan Profile	Scan	Never	✓

- The scan will be started. On completion of scanning, if any threats are found, an alert screen will be displayed.



Task: **Example Scan Profile**

Elapsed Time: **00:00:31**

Status: Scan Finished

Threat(s) Found: 1

Threat Name	Action: Clean
⊟ Application.Win32.Adware.BHO.AA@115014	
C:\Suspicious files\Probably suspisious files\infected_files\test.exe	Cleaned

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

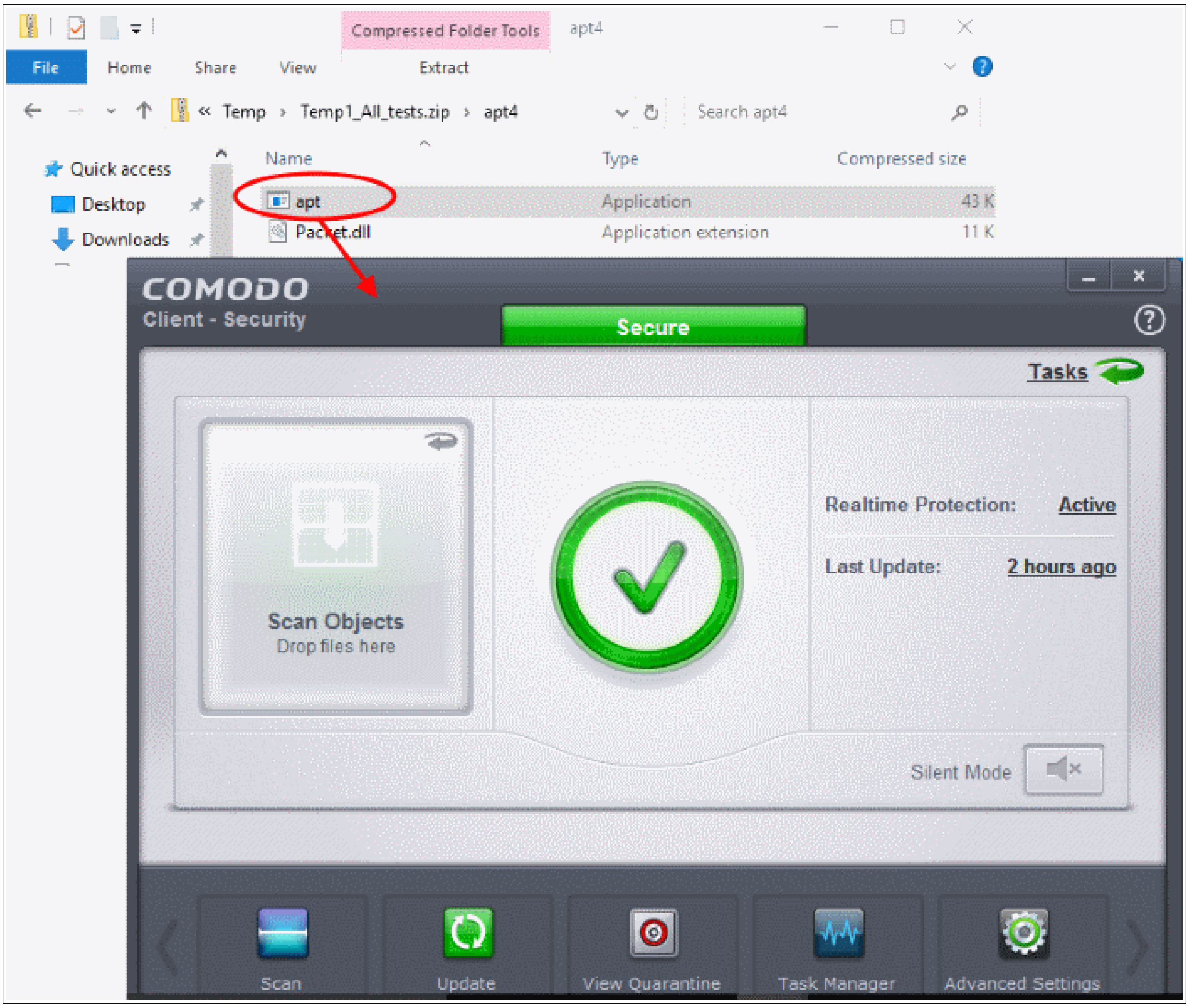
- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

2.2. Instantly Scan Files and Folders

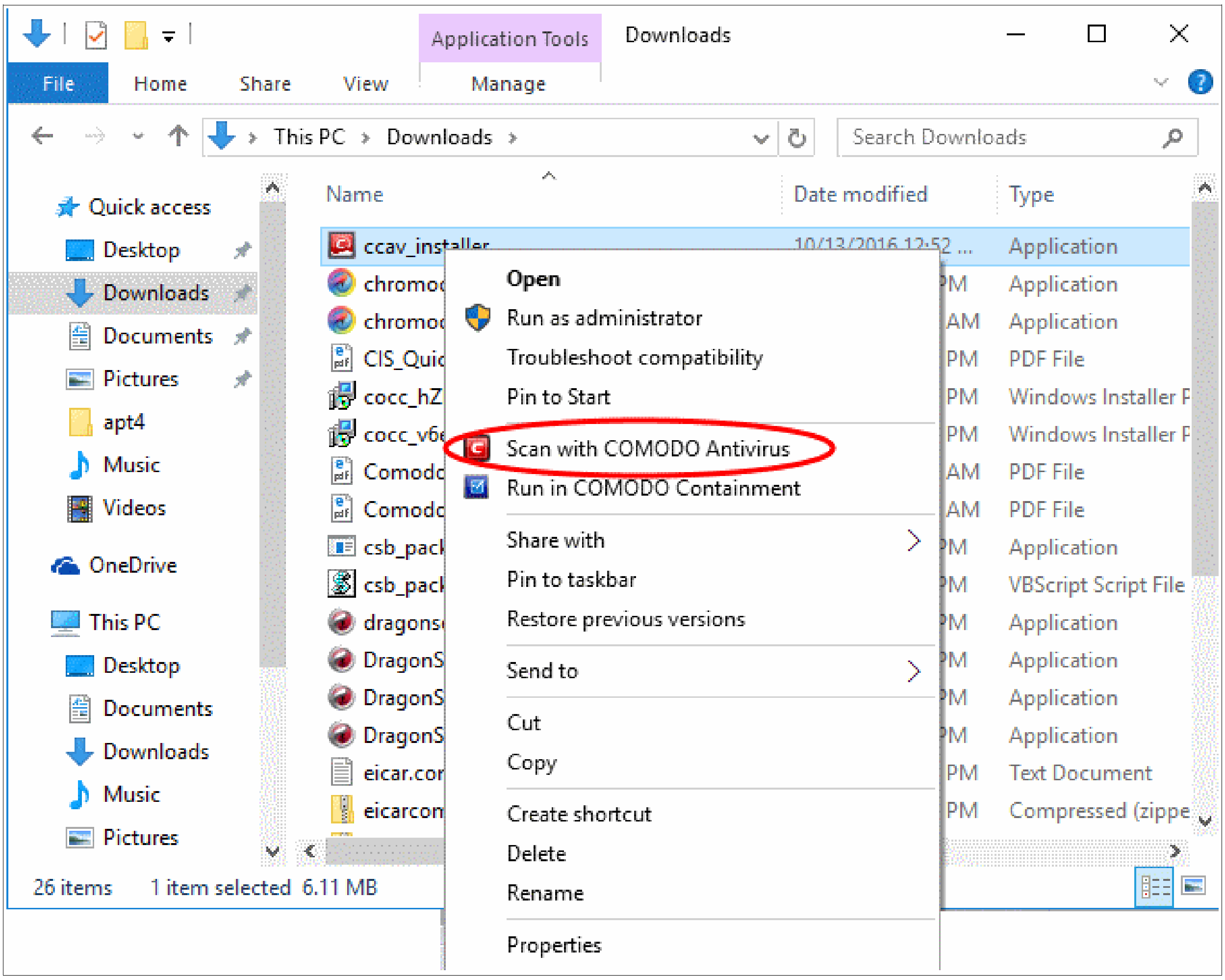
You can scan individual files or folders instantly to check whether they contain any threats or infections.

To instantly scan an item

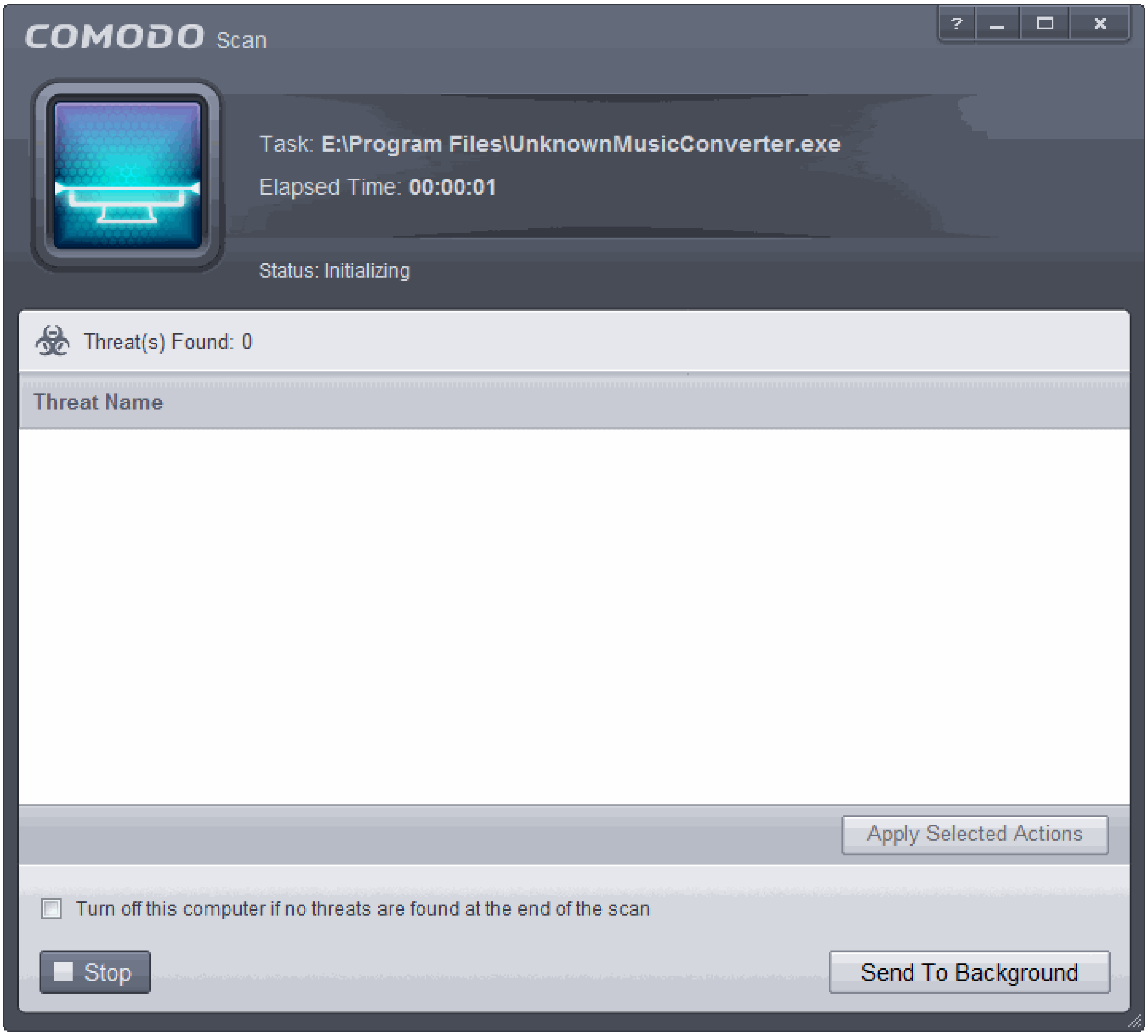
- Drag and drop the item over the area marked 'Scan Objects' in the 'Home' screen of the CCS interface



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



The item will be scanned immediately.



Task: E:\Program Files\UnknownMusicConverter.exe

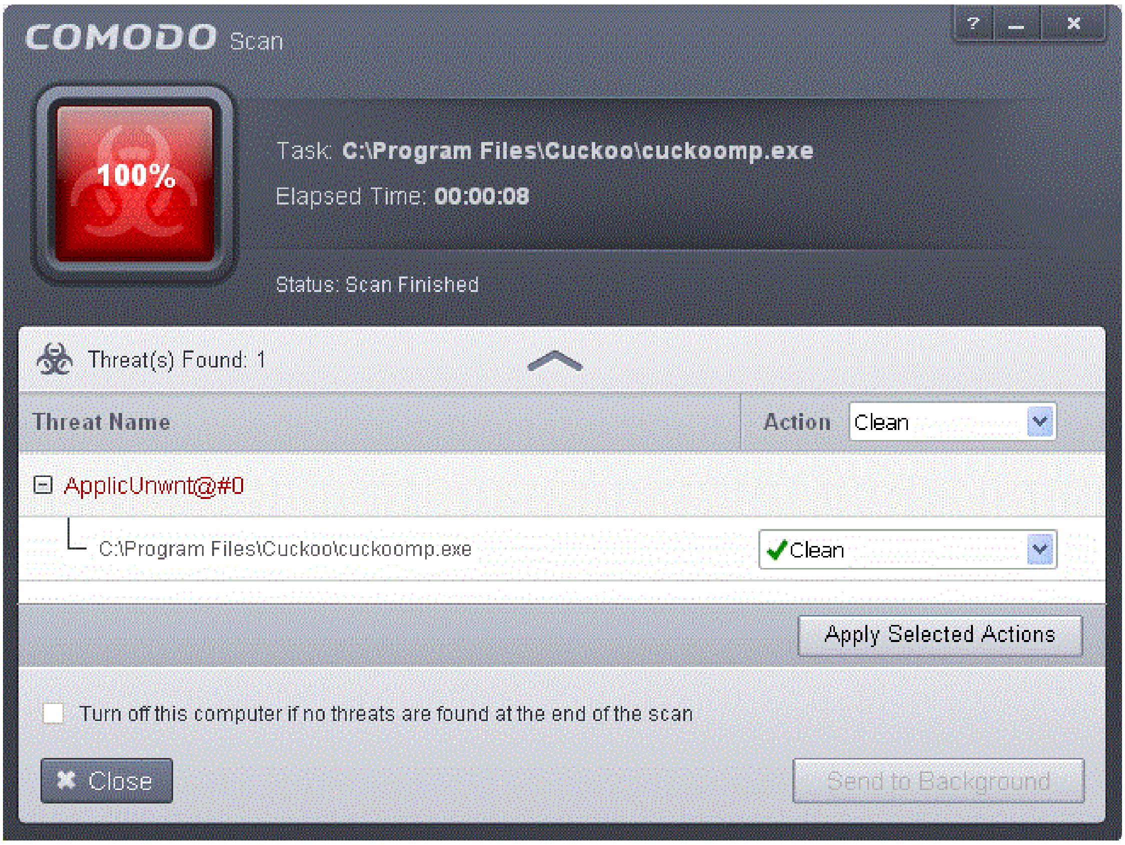
Elapsed Time: 00:00:01

Status: Initializing

Threat(s) Found: 0

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

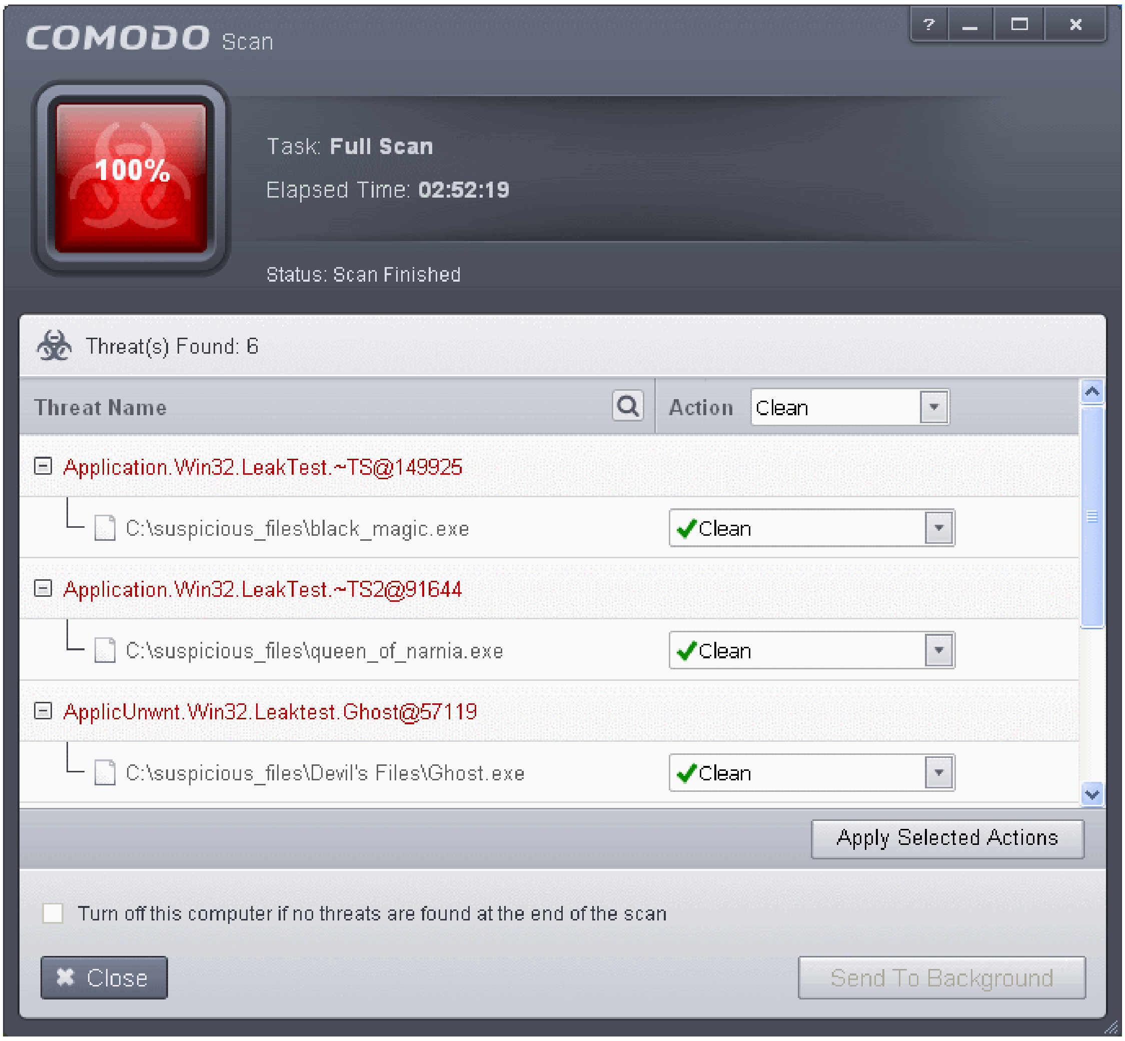
- On completion of scanning, if any threats are found, an alert screen will be displayed.



You can choose to clean, move to quarantine or ignore the threat based on your assessment. Refer to Processing the infected files for more details.

2.3. Processing Infected Files

An alert screen will be displayed if any threats are found at the end of any on-demand or scheduled scan. The alert will display the number of threats/infections discovered by the scan and provide you with cleaning options.



COMODO Scan

Task: **Full Scan**

Elapsed Time: **02:52:19**

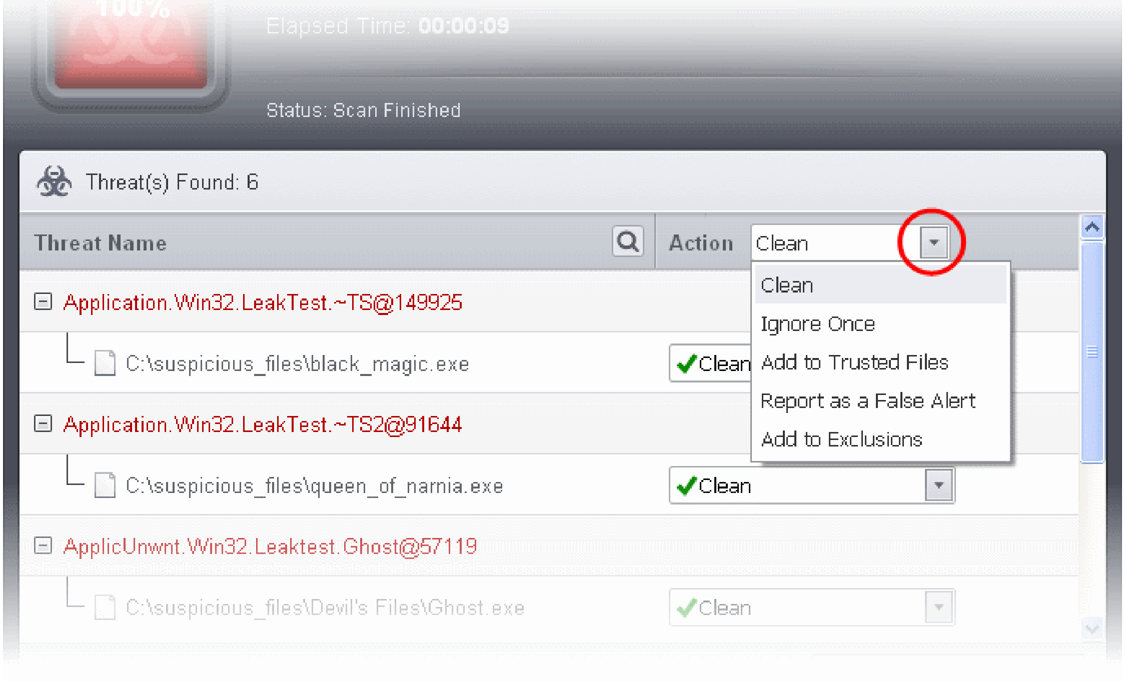
Status: Scan Finished

Threat(s) Found: 6

Threat Name	Action: Clean
⊟ Application.Win32.LeakTest.~TS@149925	
C:\suspicious_files\black_magic.exe	✓Clean
⊟ Application.Win32.LeakTest.~TS2@91644	
C:\suspicious_files\queen_of_narnia.exe	✓Clean
⊟ ApplicUnwnt.Win32.Leaktest.Ghost@57119	
C:\suspicious_files\Devil's Files\Ghost.exe	✓Clean

Apply Selected Actions
□ Turn off this computer if no threats are found at the end of the scan
✖ Close
Send To Background

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



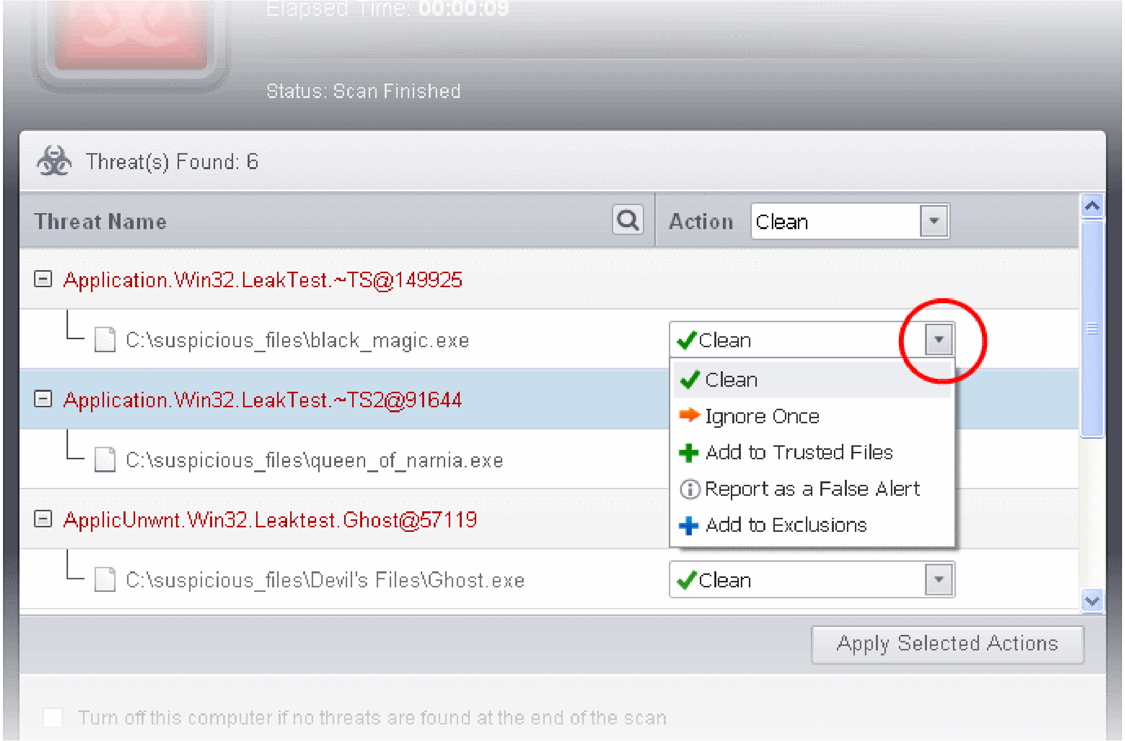
Elapsed Time: **00:00:09**

Status: Scan Finished

Threat(s) Found: 6

Threat Name	Action: Clean
⊟ Application.Win32.LeakTest.~TS@149925	
C:\suspicious_files\black_magic.exe	✓Clean
⊟ Application.Win32.LeakTest.~TS2@91644	
C:\suspicious_files\queen_of_narnia.exe	✓Clean
⊟ ApplicUnwnt.Win32.Leaktest.Ghost@57119	
C:\suspicious_files\Devil's Files\Ghost.exe	✓Clean

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



Elapsed Time: 00:00:09

Status: Scan Finished

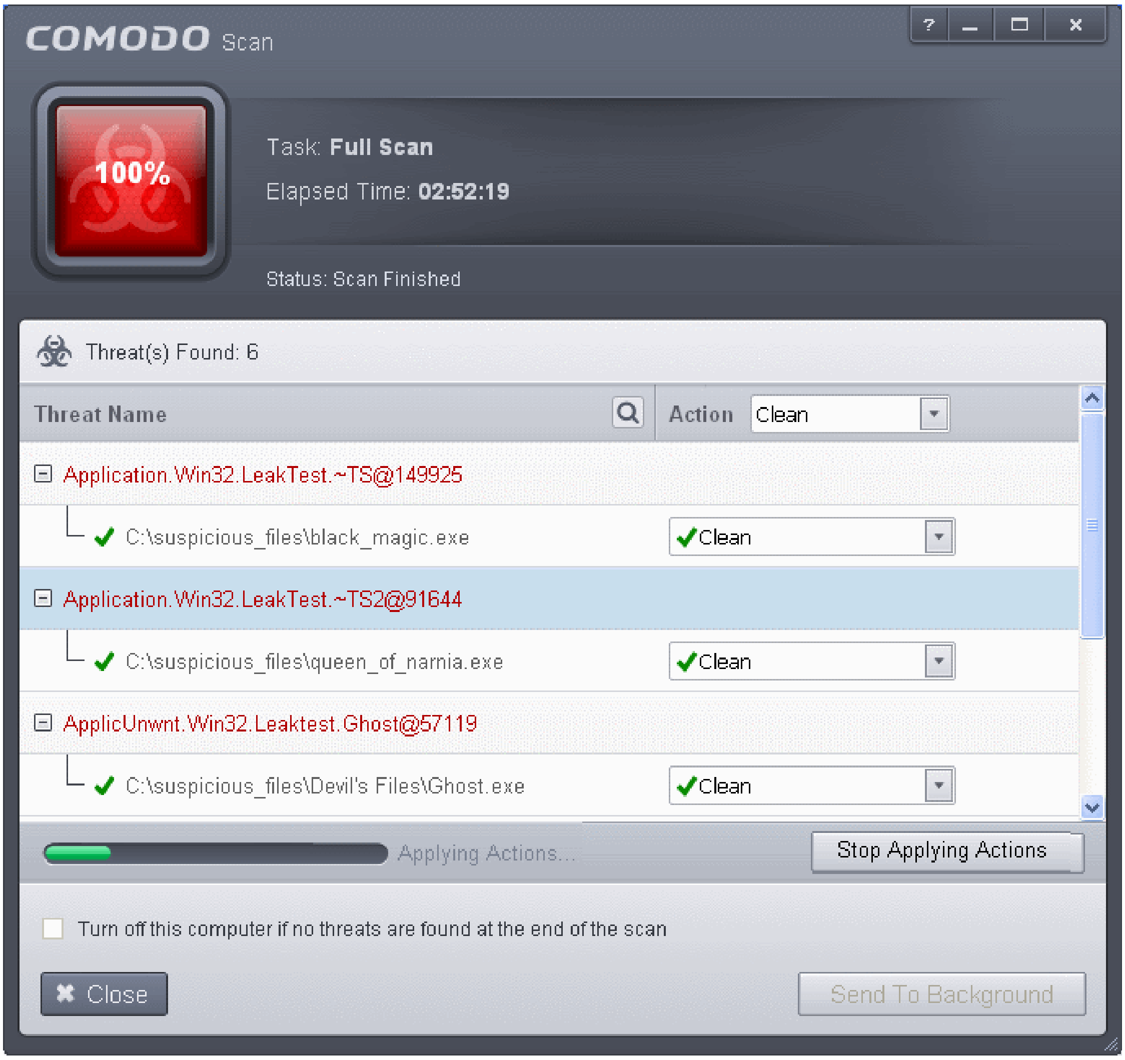
Threat(s) Found: 6

Threat Name	Action: Clean
⊟ Application.Win32.LeakTest.~TS@149925	
C:\suspicious_files\black_magic.exe	✓Clean
⊟ Application.Win32.LeakTest.~TS2@91644	
C:\suspicious_files\queen_of_narnia.exe	
⊟ ApplicUnwnt.Win32.Leaktest.Ghost@57119	
C:\suspicious_files\Devil's Files\Ghost.exe	✓Clean

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

The choices for the actions available are:

- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application safe. If the disinfection routine is not available, Comodo Antivirus will move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to **Manage Quarantined Items**.
- **Ignore Once** - If you want to ignore the threat this time only, select 'Ignore Once'. The file will be ignored only at that time. If the same application invokes again, the Antivirus will report it as a threat.
- **Add to Trusted Files** - If you trust the file, select 'Add to Trusted Files'. The file will be assigned Trusted status in the **File List**. The alert will not generated if the same application invokes again.
- **Report as a False Alert** - If you are sure that the file is safe, select 'Report as a False Alert'. The Antivirus will send the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.
- **Add to Exclusions** - The file will be moved to **Exclusions** list and will not be scanned in future. The alert will not generated if the same application invokes again.
- After selecting the action(s) to be applied, click 'Apply Selected Actions'. The files will be treated as per the action selected and the progress will be displayed.



Task: **Full Scan**

Elapsed Time: **02:52:19**

Status: Scan Finished

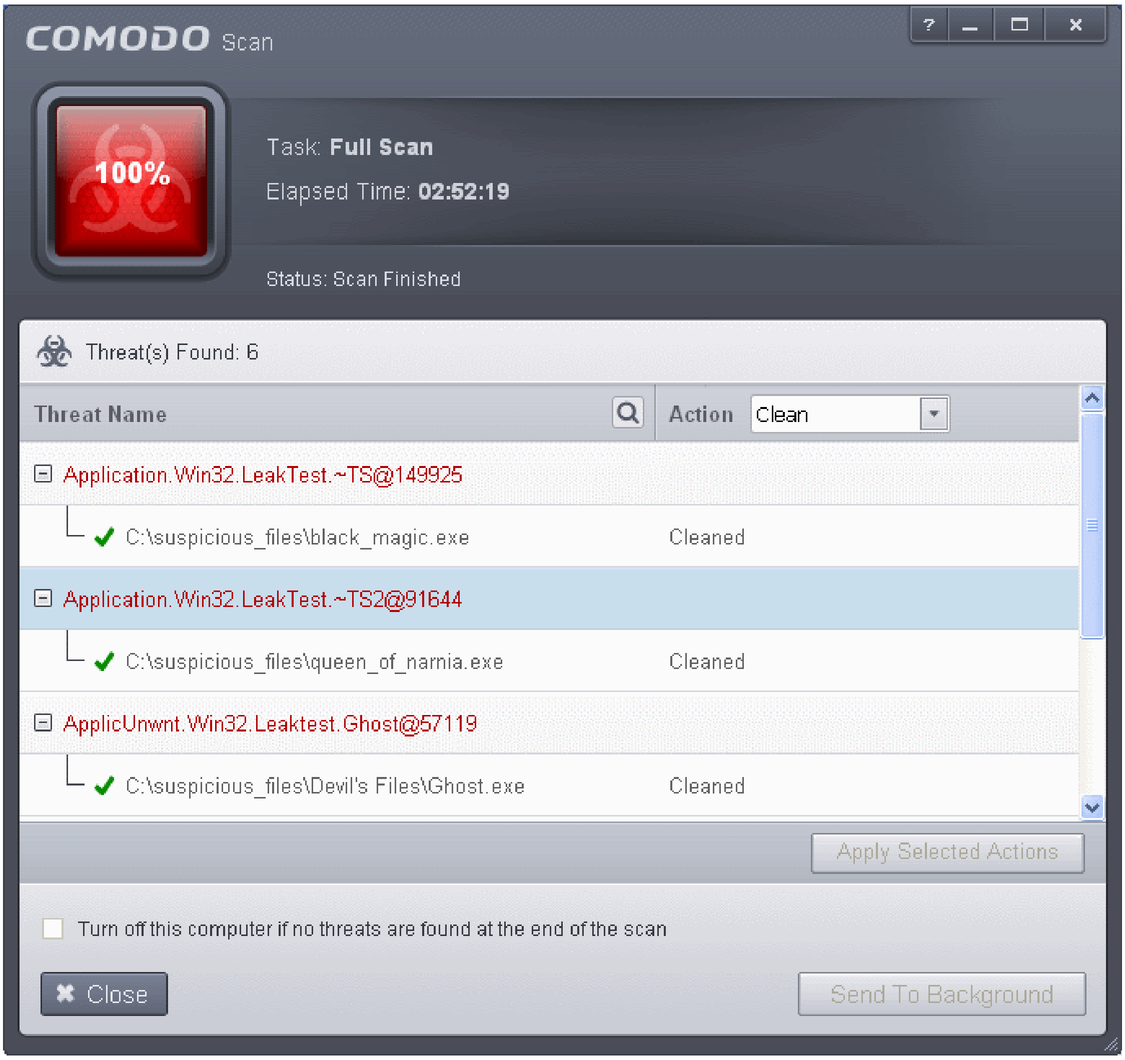
Threat(s) Found: 6

Threat Name	Action: Clean
⊟ Application.Win32.LeakTest.~TS@149925	
✓ C:\suspicious_files\black_magic.exe	✓Clean
⊟ Application.Win32.LeakTest.~TS2@91644	
✓ C:\suspicious_files\queen_of_narnia.exe	✓Clean
⊟ ApplicUnwnt.Win32.Leaktest.Ghost@57119	
✓ C:\suspicious_files\Devil's Files\Ghost.exe	✓Clean

Applying Actions...

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

On completion the action taken against each threat will be displayed.



COMODO Scan

Task: **Full Scan**

Elapsed Time: **02:52:19**

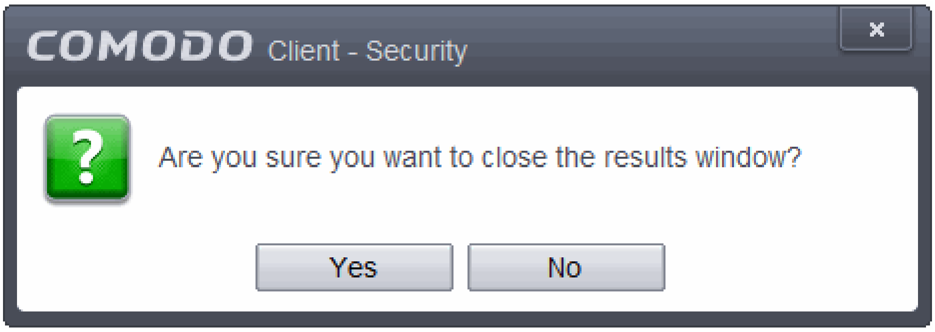
Status: Scan Finished

Threat(s) Found: 6

Threat Name	Action: Clean
Application.Win32.LeakTest.~TS@149925	
✓ C:\suspicious_files\black_magic.exe	Cleaned
Application.Win32.LeakTest.~TS2@91644	
✓ C:\suspicious_files\queen_of_narnia.exe	Cleaned
ApplicUnwnt.Win32.Leaktest.Ghost@57119	
✓ C:\suspicious_files\Devil's Files\Ghost.exe	Cleaned

100%
Apply Selected Actions
□ Turn off this computer if no threats are found at the end of the scan
Close
Send To Background

- Click 'Close' to close the results window.



COMODO Client - Security

Are you sure you want to close the results window?

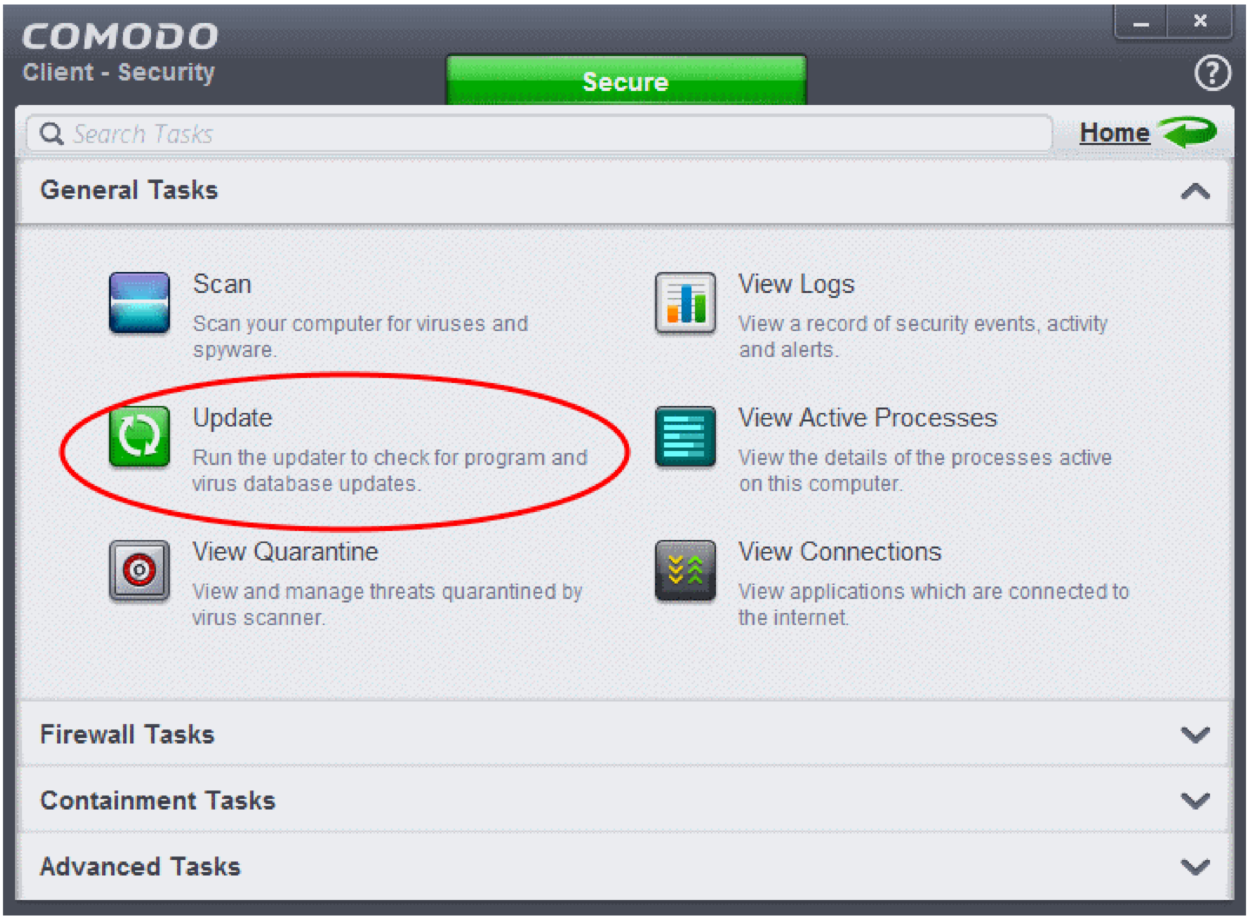
- Click 'Yes' in the confirmation window.

2.4. Manage Virus Database and Program Updates

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

To manually check for the latest virus Database and program updates

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



Scan
Scan your computer for viruses and spyware.

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

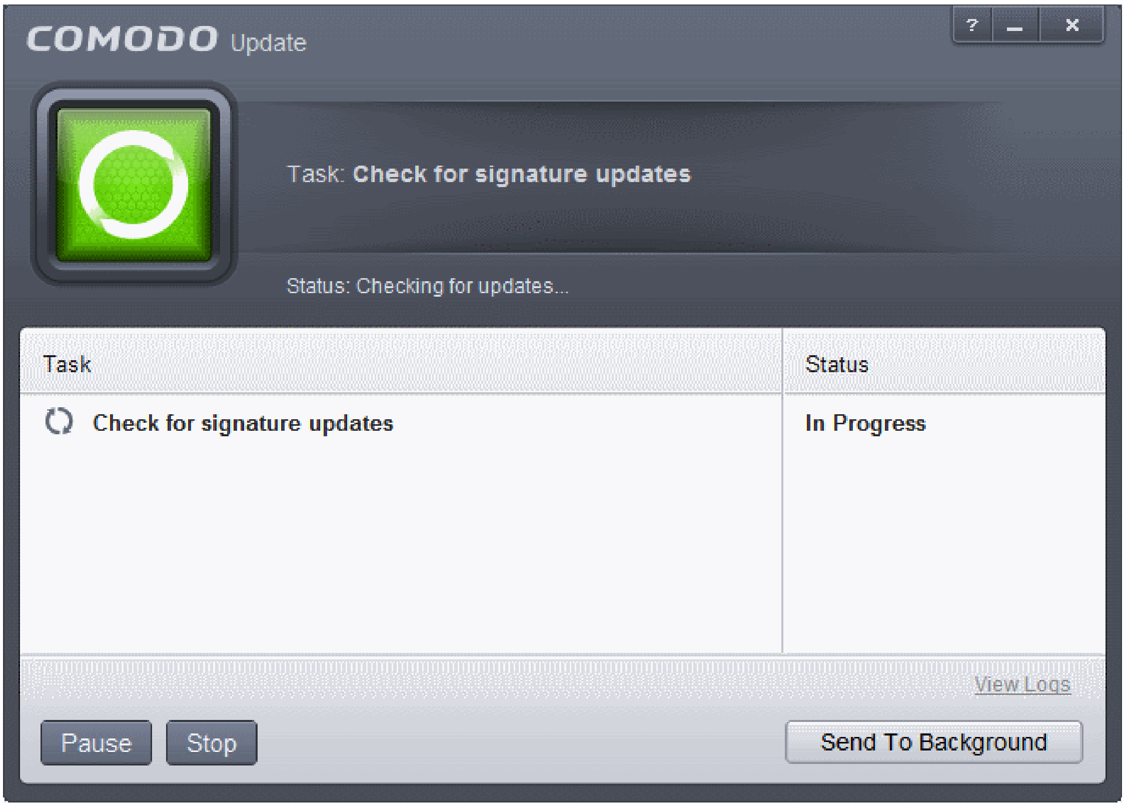
Update
Run the updater to check for program and virus database updates.

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

View Quarantine
View and manage threats quarantined by virus scanner.

View Connections
View applications which are connected to the internet.

The application will check for program and database updates from Comodo Servers.

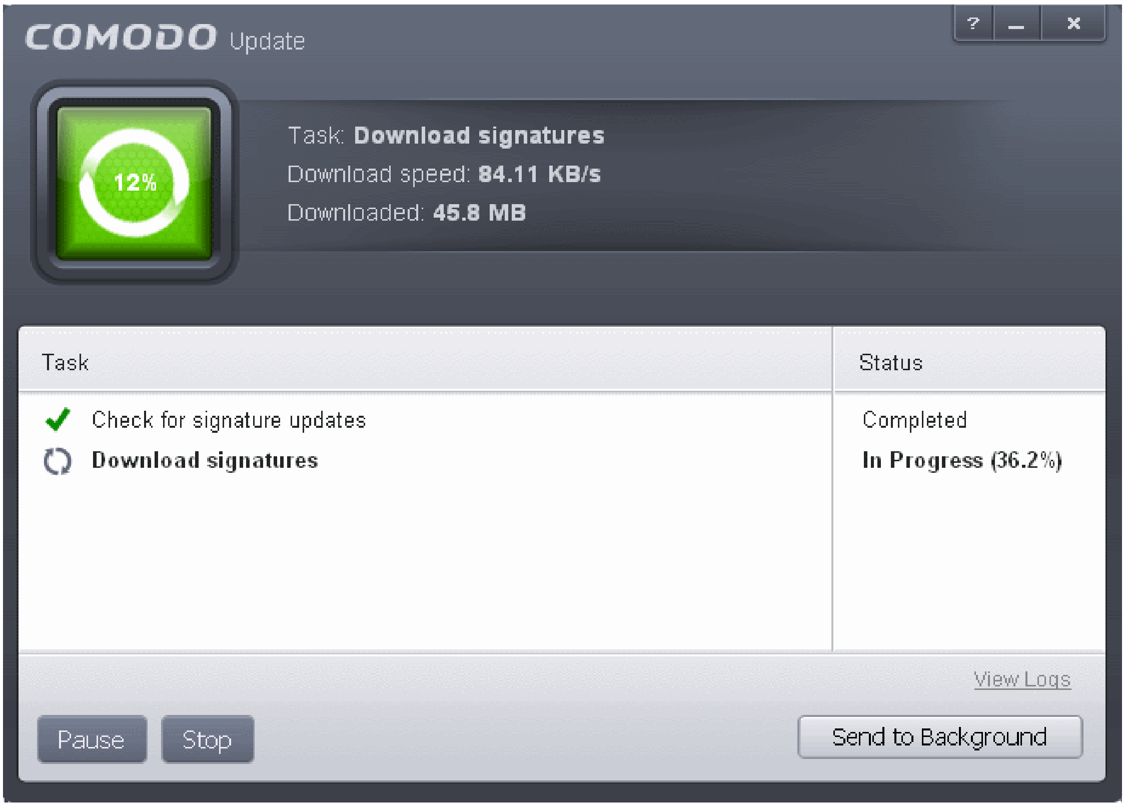


Task: **Check for signature updates**

Status: Checking for updates...

Task	Status
Check for signature updates	In Progress

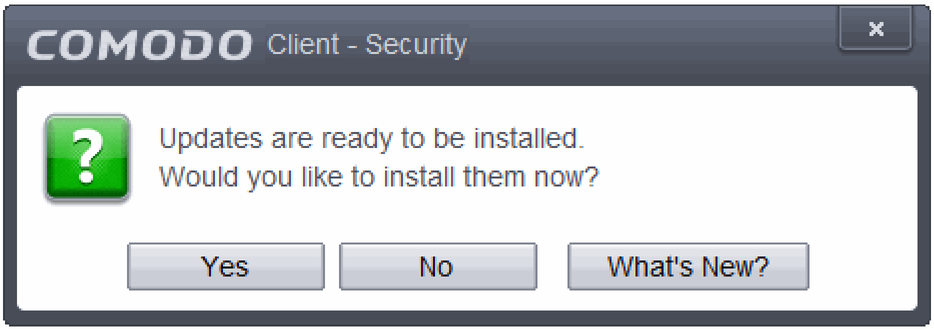
If the updates are available, they will be downloaded.



Task: **Download signatures**
Download speed: **84.11 KB/s**
Downloaded: **45.8 MB**

Task	Status
✓ Check for signature updates	Completed
Download signatures	**In Progress (36.2%)**

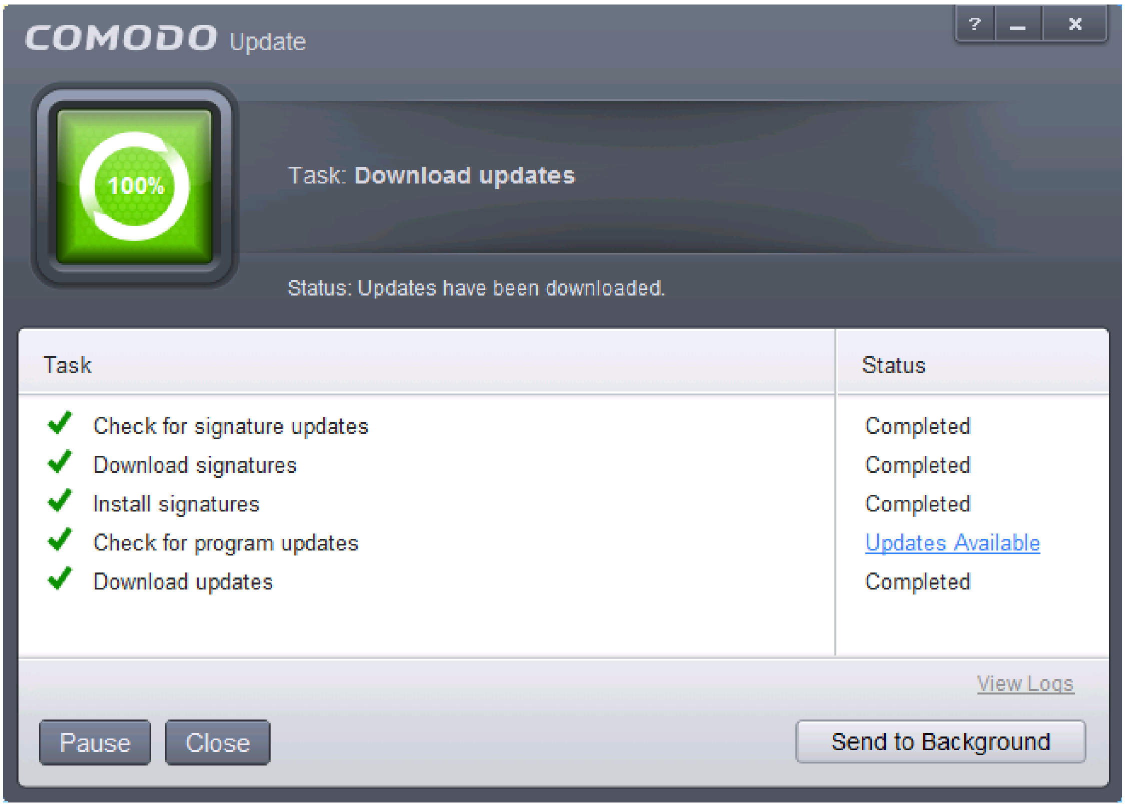
Note: You must be connected to Internet to download the updates.



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

If any program updates are available, they will be downloaded and a confirmation dialog will be displayed before downloading them.

The virus signature database will be updated on completion.



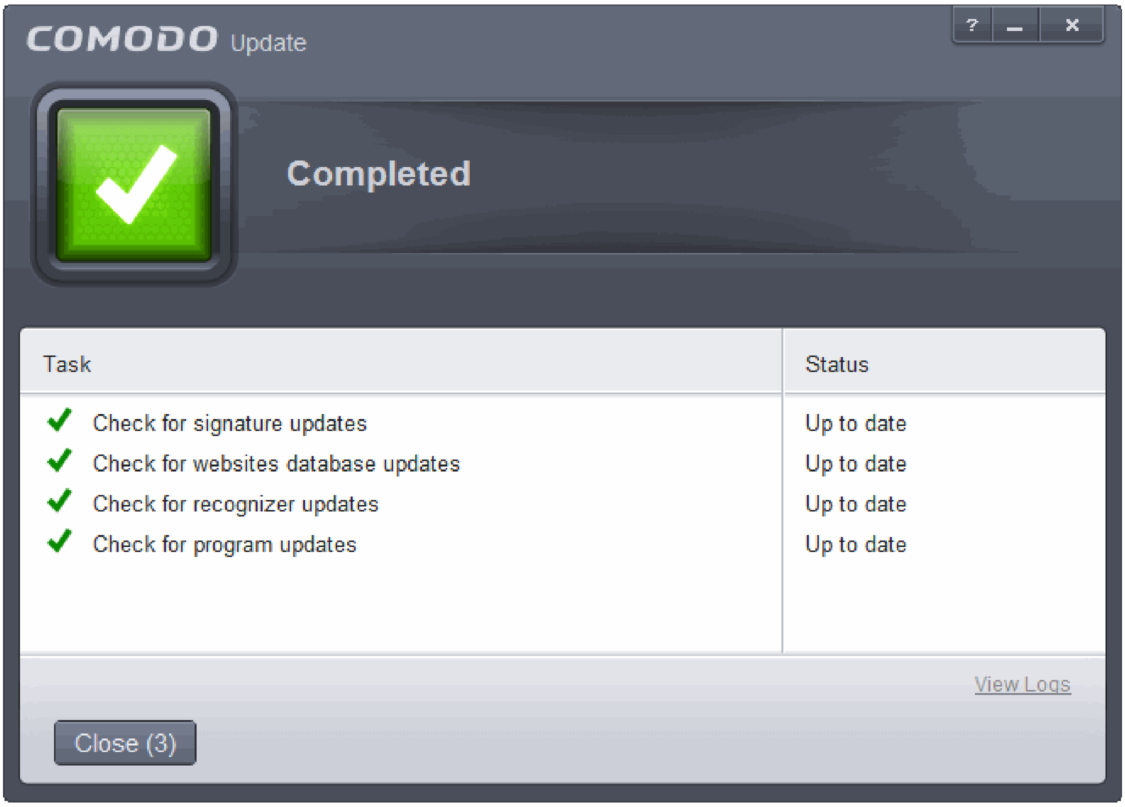
Task: Download updates

Status: Updates have been downloaded.

Task	Status
✓ Check for signature updates	Completed
✓ Download signatures	Completed
✓ Install signatures	Completed
✓ Check for program updates	Updates Available
✓ Download updates	Completed

If any program updates are available, they will be downloaded and a confirmation dialog will be displayed before installing them.

- Click 'Yes' to install the updates and keep your CCS installation up-to-date.

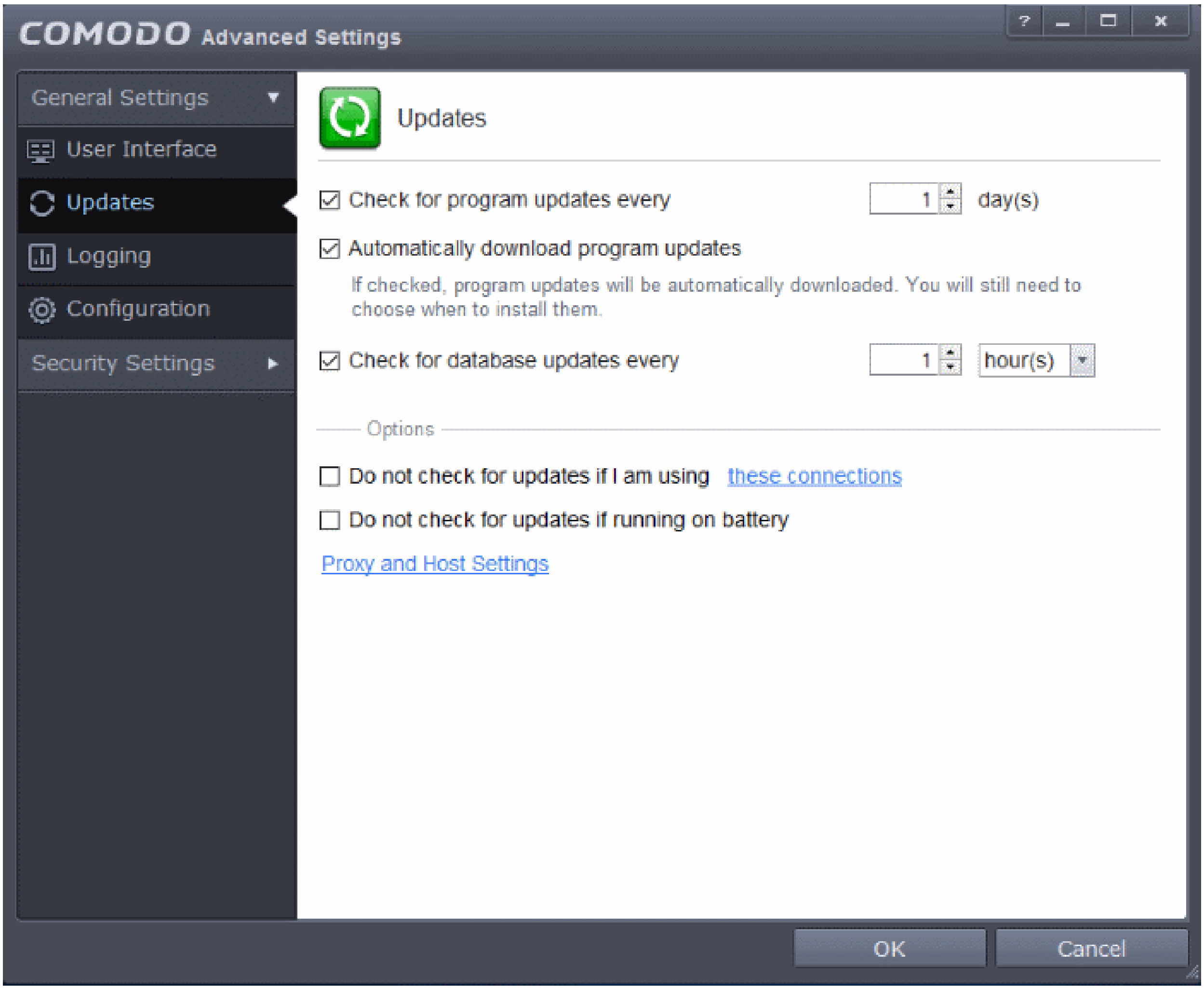


Completed

Task	Status
✓ Check for signature updates	Up to date
✓ Check for websites database updates	Up to date
✓ Check for recognizer updates	Up to date
✓ Check for program updates	Up to date

Automatic Updates

By default, Comodo Antivirus automatically checks for and downloads database updates. You can modify these settings in Advanced Tasks > Advanced Settings > Updates.



☑ Check for program updates every 1 day(s)

☑ Automatically download program updates

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

☑ Check for database updates every 1 hour(s)

Options

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

□ Do not check for updates if running on battery

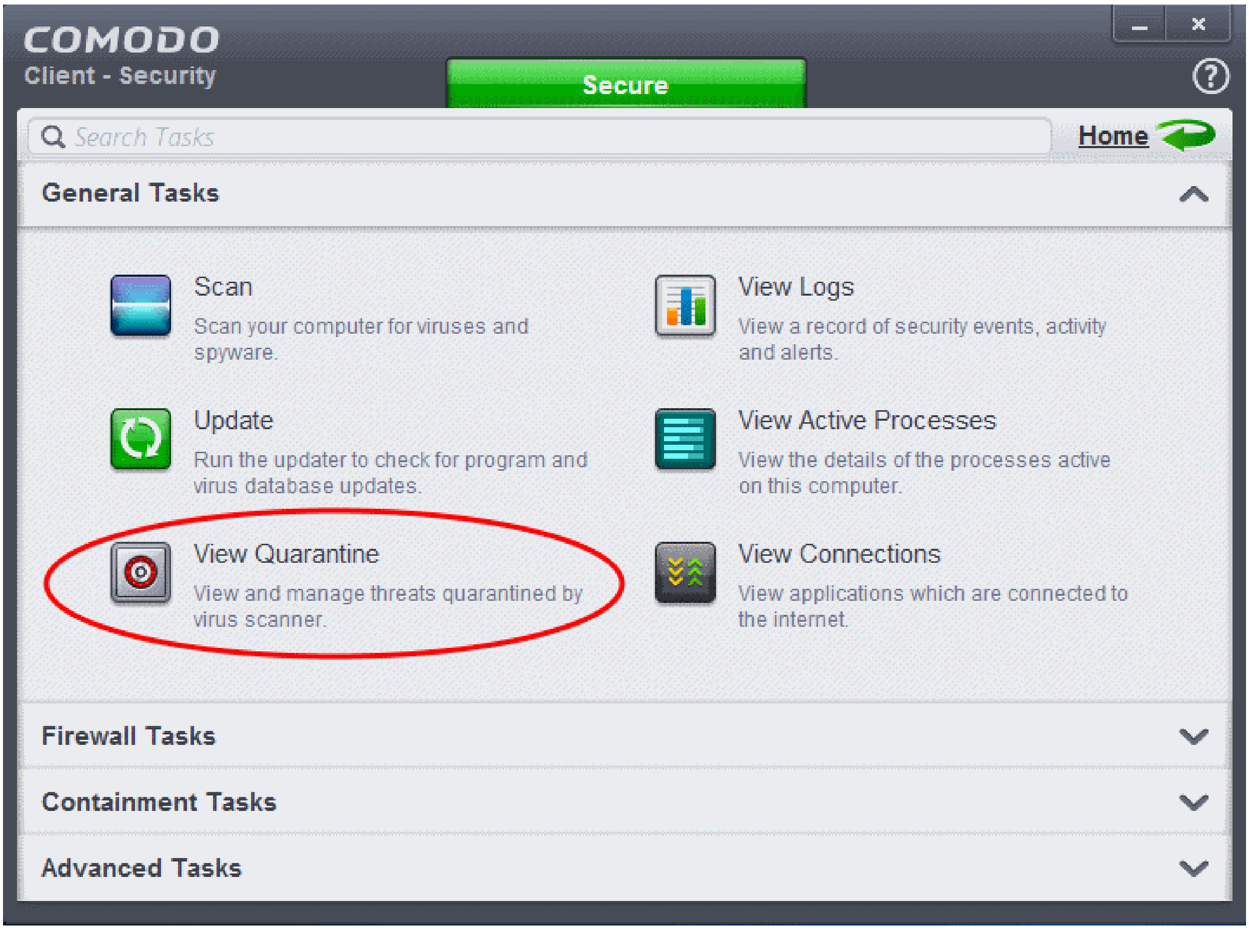
Proxy and Host Settings

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

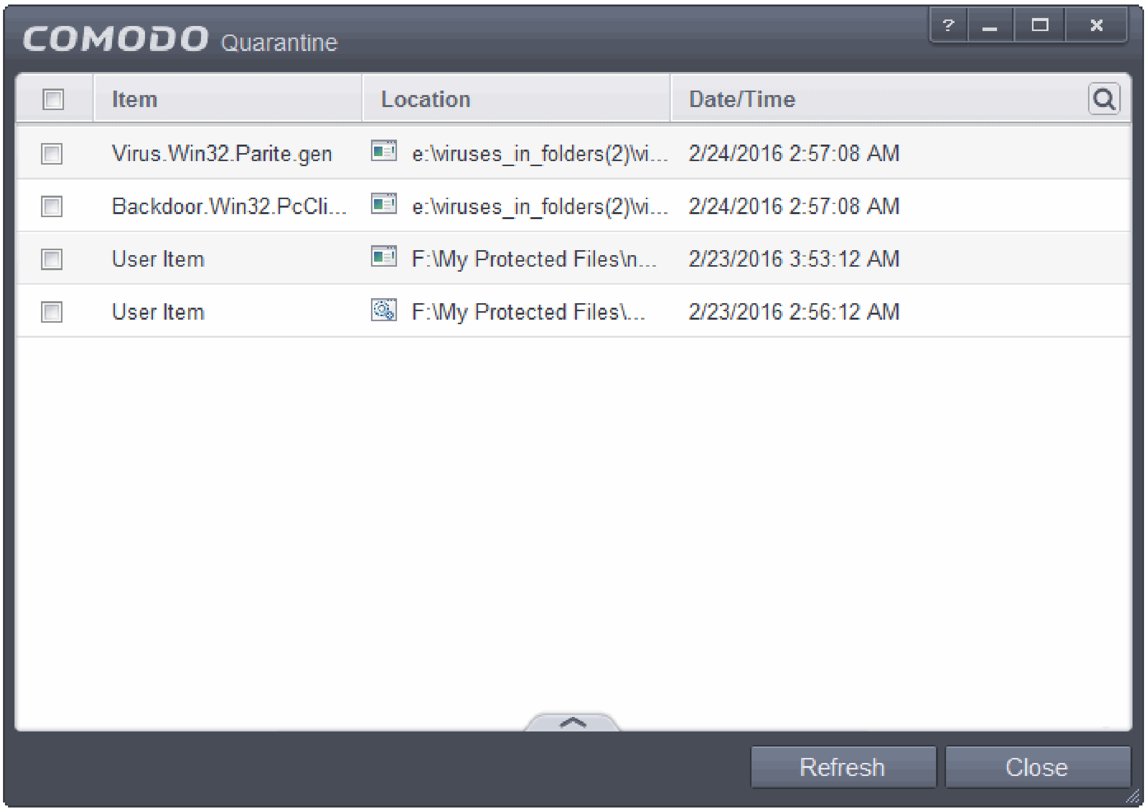
2.5. Manage Quarantined Items

The quarantine facility removes and isolates suspicious files into a safe location before analyzing them for possible infection. Any files transferred in this fashion are encrypted- meaning they cannot be run or executed. This isolation prevents infected files from affecting the rest of your PC. If a file cannot be disinfected, then it provides a reliable safe-house until the virus database is updated- neutralizing the impact of any new virus.

The Quarantine interface can be accessed by clicking View Quarantine from the 'General Tasks' interface.


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
Firewall Tasks
Containment Tasks
Advanced Tasks

The 'Quarantine' interface displays a list of items moved to Quarantine from the results of real-time scanning, on-demand scanning and manually.



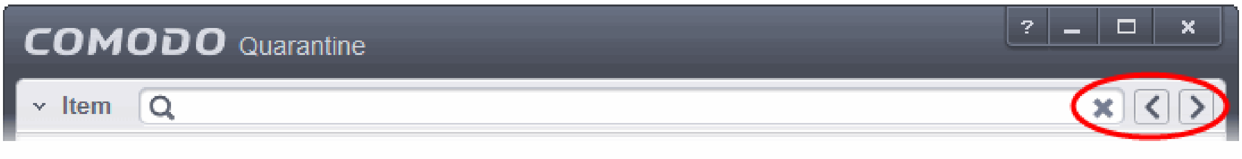
□	Item	Location	Date/Time
□	Virus.Win32.Parite.gen	e:\viruses_in_folders(2)\wi...	2/24/2016 2:57:08 AM
□	Backdoor.Win32.PcCli...	e:\viruses_in_folders(2)\wi...	2/24/2016 2:57:08 AM
□	User Item	F:\My Protected Files\n...	2/23/2016 3:53:12 AM
□	User Item	F:\My Protected Files\...	2/23/2016 2:56:12 AM

Column Descriptions

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

For details on adding executables identified as infected files during on-demand or real time scans to Quarantine, refer to General Tasks > Scan and Clean Your Computer.

You can use the search option to find a specific quarantined item from the list by clicking the search icon 🔍 at the far right in the column header and entering the item name in full or part. You can navigate through the successive results by clicking the left and right arrows.



The Quarantined Items interface also allows you to:

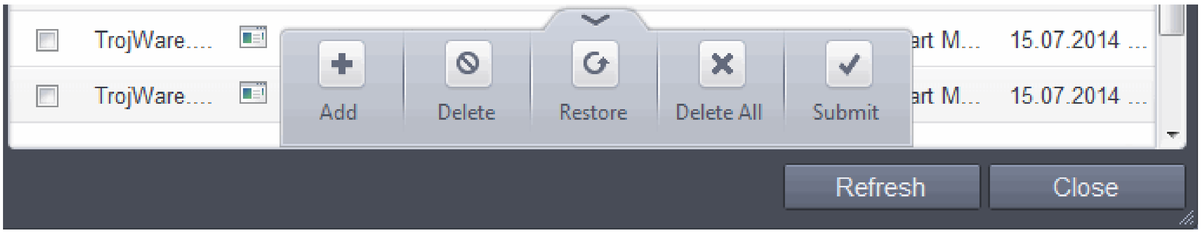
- Manually add applications, executables or other files, that you do not trust, as a Quarantined item
- Delete a selected quarantined item from the system
- Restore a quarantined item to its original location
- Delete all quarantined items
- Submit selected quarantined items to Comodo for analysis

Manually adding files as Quarantined Items

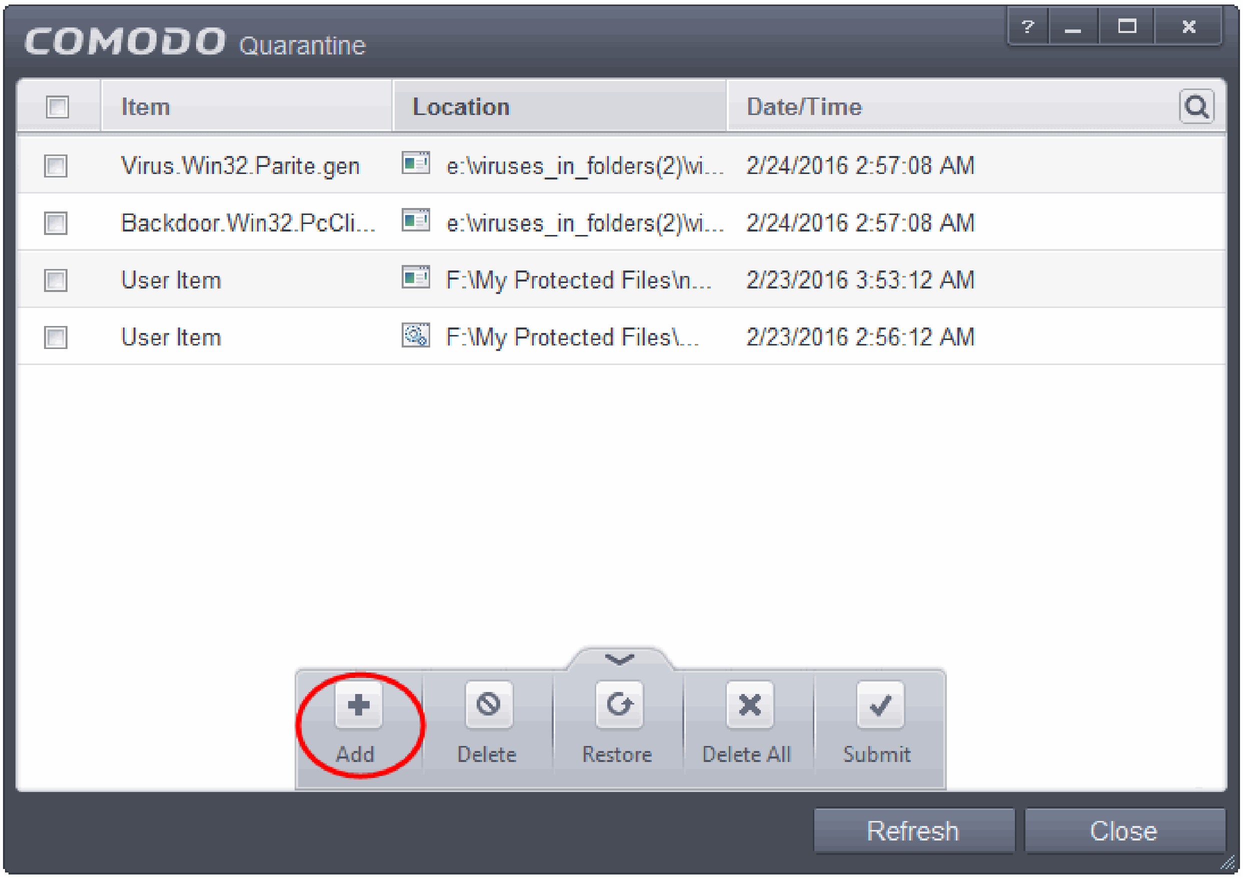
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined Item

1. Click the handle from the bottom of the Quarantine interface

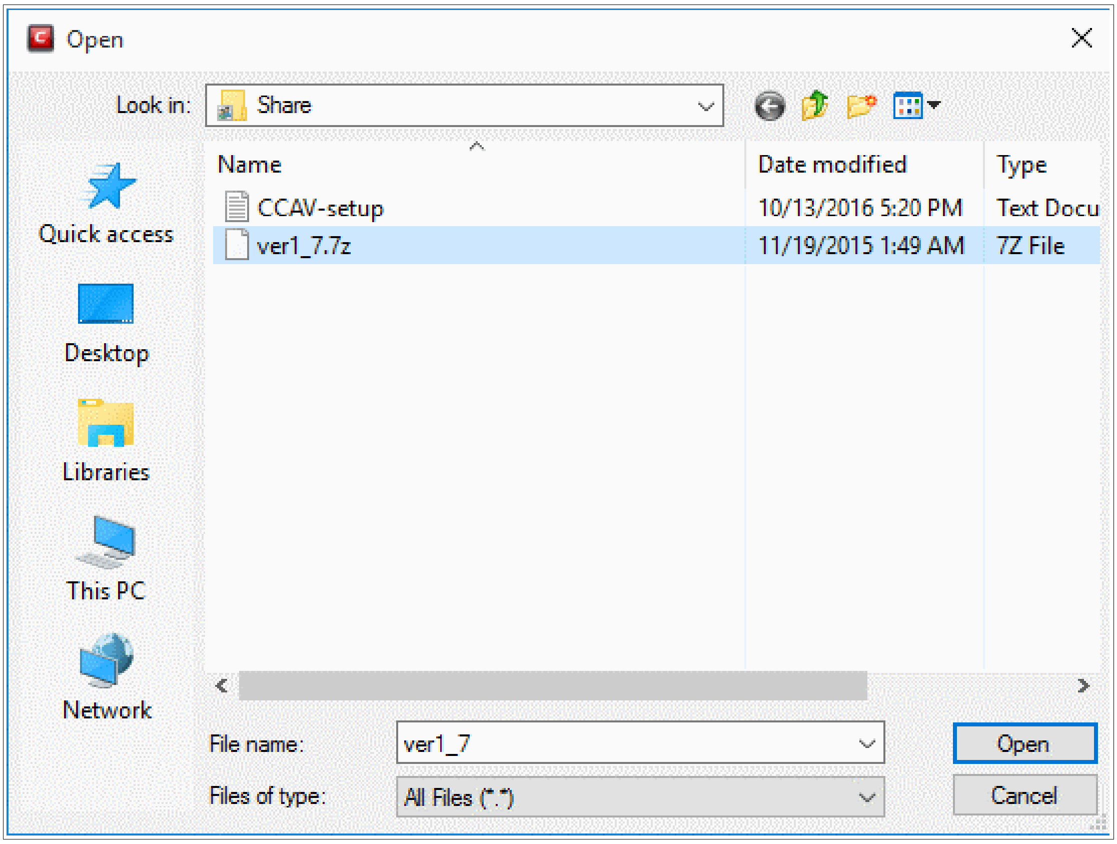


2. Select 'Add' from the options.



□	Item	Location	Date/Time
□	Virus.Win32.Parite.gen	e:\viruses_in_folders(2)\wi...	2/24/2016 2:57:08 AM
□	Backdoor.Win32.PcCli...	e:\viruses_in_folders(2)\wi...	2/24/2016 2:57:08 AM
□	User Item	F:\My Protected Files\n...	2/23/2016 3:53:12 AM
□	User Item	F:\My Protected Files\...	2/23/2016 2:56:12 AM

3. Navigate to the file you want to add to the quarantine and click 'Open'.



Look in: Share

Name	Date modified	Type
CCAV-setup	10/13/2016 5:20 PM	Text Docu
ver1_7.7z	11/19/2015 1:49 AM	7Z File

File name: ver1_7

Files of type: All Files (*.*)

The file will be added to Quarantine. You can even send the file for analysis to Comodo, for inclusion in the white list or black list, by clicking Submit from the options.

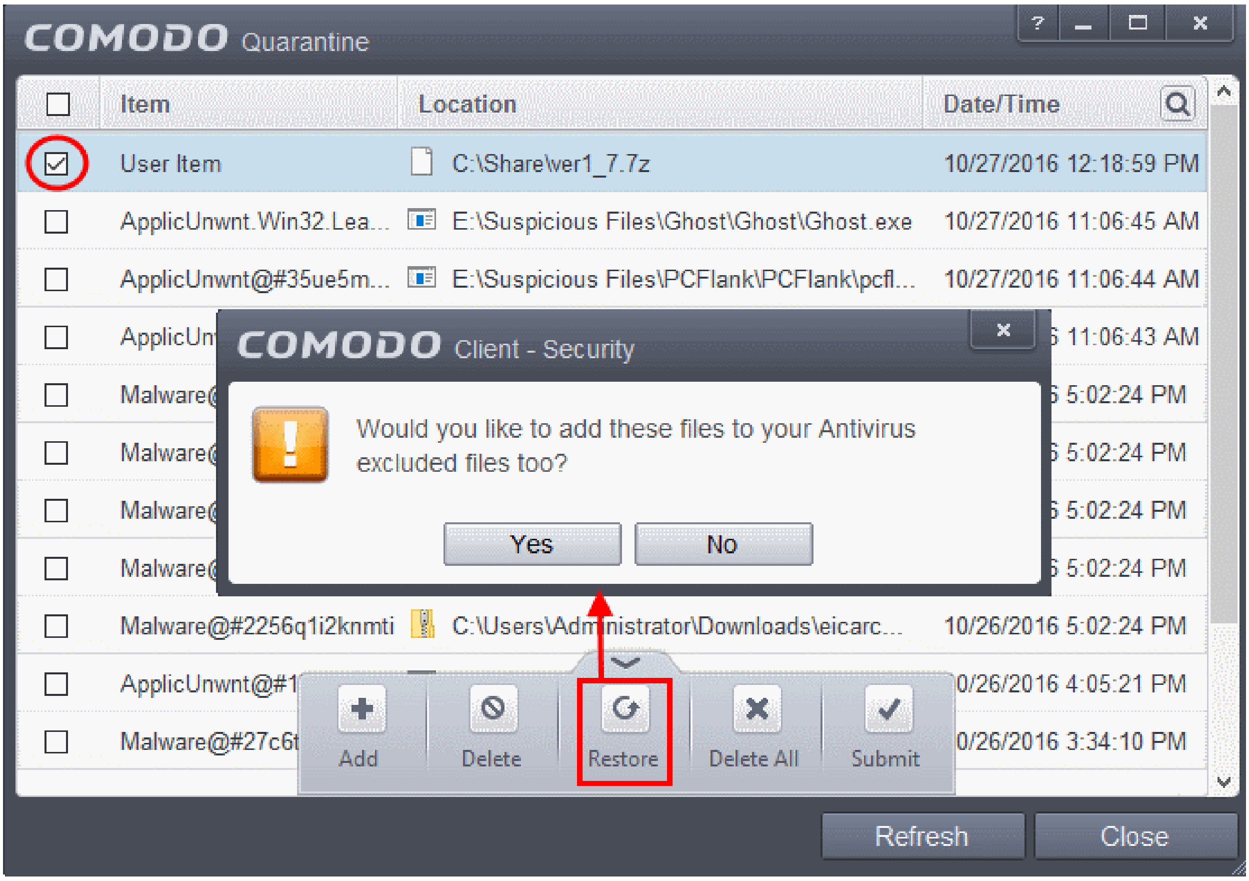
To delete a quarantined item from the system

- Select the item(s) from the 'Quarantine' interface
- Click the handle from the bottom of the interface and select 'Delete' option.

This deletes the file from the system permanently.

To restore a quarantined item to its original location

- Select the item(s) from the 'Quarantine' interface
- Click the handle from the bottom of the interface and select 'Restore' option.



□	Item	Location	Date/Time
☑	User Item	C:\Share\wer1_7.7z	10/27/2016 12:18:59 PM
□	ApplicUnwnt.Win32.Lea...	E:\Suspicious Files\Ghost\Ghost\Ghost.exe	10/27/2016 11:06:45 AM
□	ApplicUnwnt@#35ue5m...	E:\Suspicious Files\PCFlank\PCFlank\pcfl...	10/27/2016 11:06:44 AM
□	ApplicUn		6 11:06:43 AM
□	Malware@		6 5:02:24 PM
□	Malware@		6 5:02:24 PM
□	Malware@		6 5:02:24 PM
□	Malware@		6 5:02:24 PM
□	Malware@#2256q1i2knmti	C:\Users\Administrator\Downloads\eicarc...	10/26/2016 5:02:24 PM
□	ApplicUnwnt@#1		0/26/2016 4:05:21 PM
□	Malware@#27c6t		0/26/2016 3:34:10 PM

COMODO Client - Security

Would you like to add these files to your Antivirus excluded files too?

Yes No

An option will be provided to add the file(s) to **Exclusions** list and if 'Yes' is chosen, 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. However, if it contains malware, it will be detected as a threat immediately by the real-time protection (or during the next scan if real-time protection is disabled).

To remove all quarantined items permanently

- Click the handle at the bottom of the interface and select the 'Delete all' option.

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

To submit selected quarantined items to Comodo for analysis

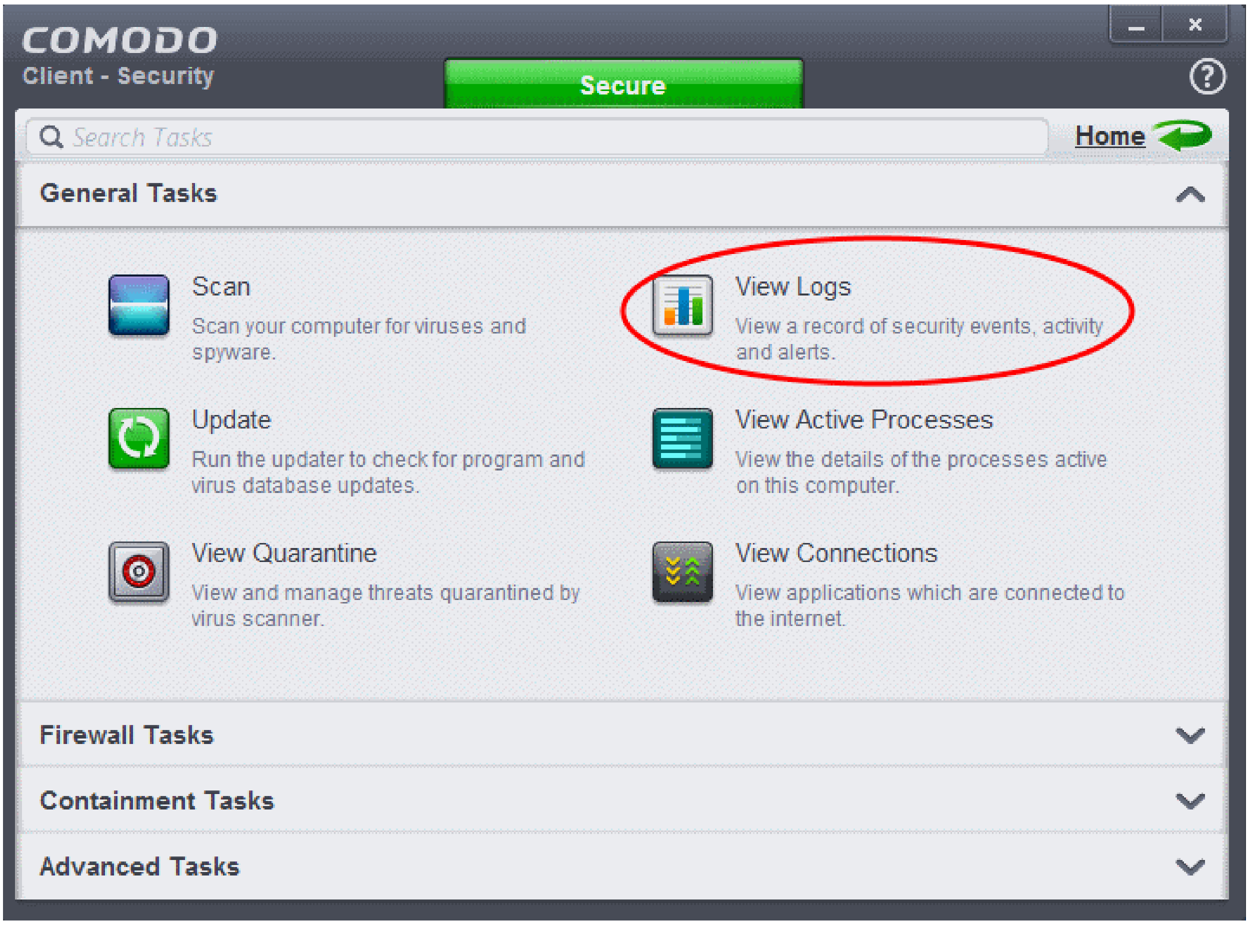
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

You can submit the files which you suspect to be a malware or the files which you consider as safe but identified as malware by Comodo Antivirus (False Positives). 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).

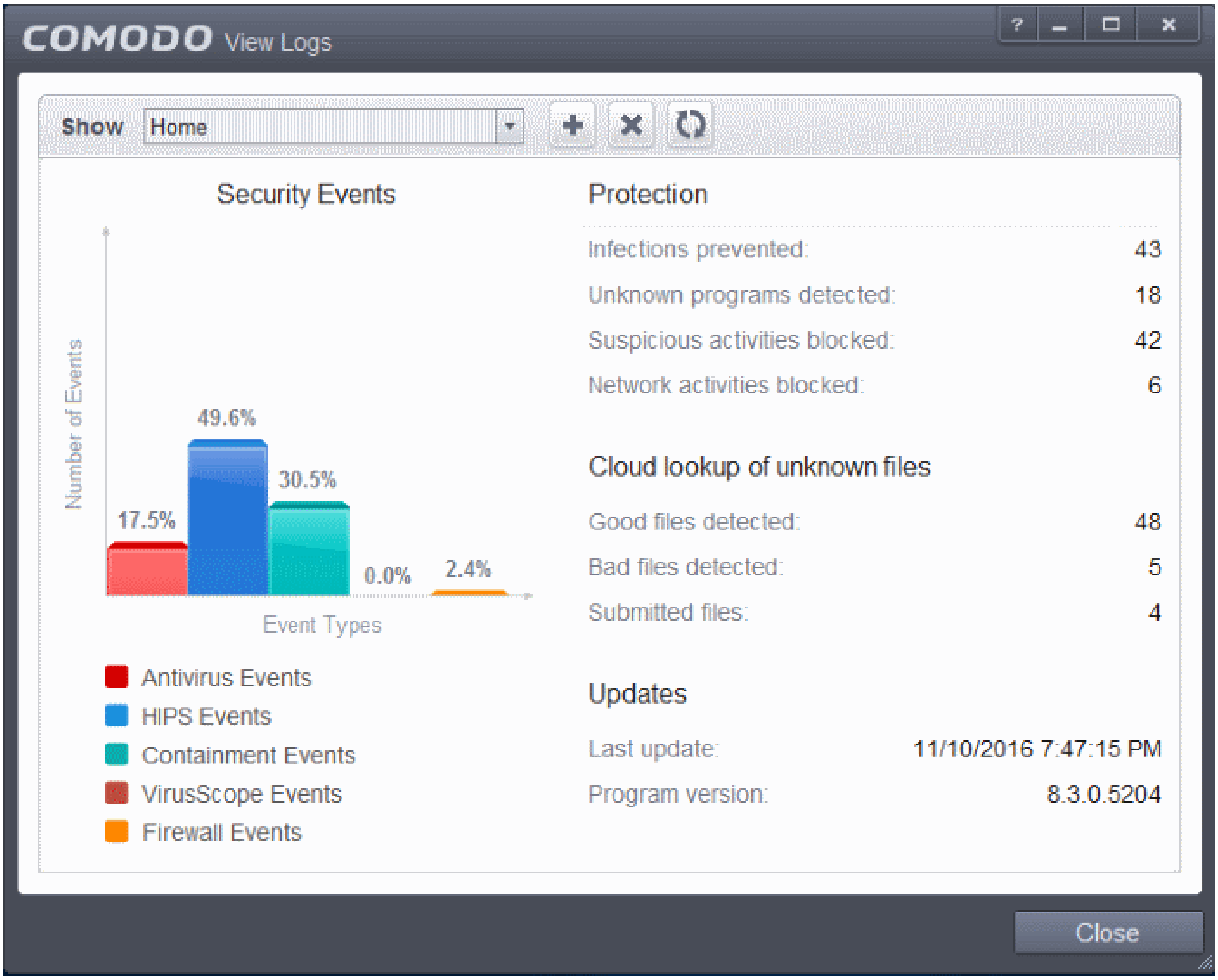
> **Note:** Quarantined files are stored using a special format and do not constitute any danger to your computer.

2.6. View CCS Logs

CCS maintains a log of events which can be viewed at anytime by clicking 'View Logs' from the General Tasks interface.


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
Firewall Tasks
Containment Tasks
Advanced Tasks

The 'Log Viewer' module opens with its home screen displaying a summary of CCS events:



🟥 Antivirus Events
🟦 HIPS Events
🟩 Containment Events
🟥 VirusScope Events
🟧 Firewall Events

Protection

Infections prevented:	43
Unknown programs detected:	18
Suspicious activities blocked:	42
Network activities blocked:	6

Cloud lookup of unknown files

Good files detected:	48
Bad files detected:	5
Submitted files:	4

Updates

Last update:	11/10/2016 7:47:15 PM
Program version:	8.3.0.5204

The left hand side of the home screen displays a bar graph showing a comparison of Antivirus events and Advanced Protection events. The right hand side displays a statistical summary of Antivirus and Advanced Protection events, the results of cloud based scanning of your system and the version and update information of the CCS installation on your system.

- The interface contains a full history of logged events of Advanced Protection and Antivirus modules. Select the module from the 'Show' drop-down at the top left to display that log type in the main window.
- To open a pre-exported/stored log file, click the open button ✚ beside the drop-down and browse to the location where the CCS log file is stored
- To clear the logs, click the clear button ✖
- To refresh the logs, click the 'Refresh' button ⟳

Click the following links for more explanations of the options available for each type of filter:

'Logs per Module':

- Antivirus
- Viruscope
- Firewall
- HIPS
- Containment

'Other Logs':

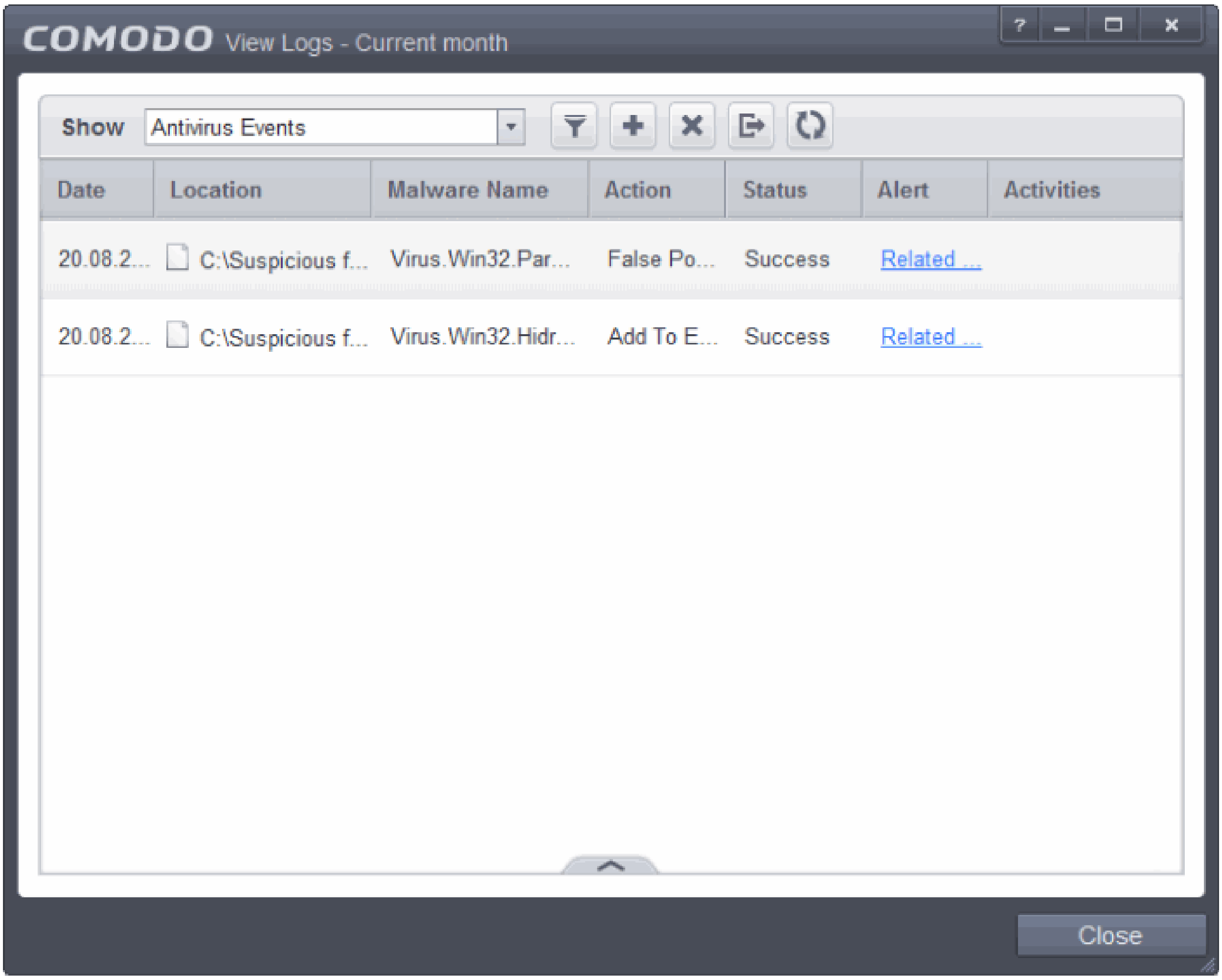
- Website Filtering

- Alerts Displayed
- Tasks Launched
- File List Changes
- Trusted Vendors List
- Configuration Changes
- Device Control

2.6.1. Antivirus Logs

Comodo Antivirus documents the results of all actions performed by it in extensive but easy to understand reports. A detailed scan report contains statistics of all scanned objects, settings used for each task and the history of actions performed on each individual file. Reports are also generated during real-time protection, and after updating the antivirus database and application modules.

The Antivirus logs can be viewed by selecting 'Antivirus Events' from the Show drop-down of the log viewer interface.



Date	Location	Malware Name	Action	Status	Alert	Activities
20.08.2...	C:\Suspicious f...	Virus.Win32.Par...	False Po...	Success	Related ...	
20.08.2...	C:\Suspicious f...	Virus.Win32.Hidr...	Add To E...	Success	Related ...	

Column Descriptions

1. **Date** - Indicates the date of the event.
2. **Location** - Indicates the location where the application detected with a threat is stored.
3. **Malware Name** - Name of the malware event that has been detected.
4. **Action** - Indicates action taken against the malware through Antivirus.
5. **Status** - Gives the status of the action taken. It can be either 'Success' or 'Fail'.

6. **Alert** - Gives the details of the alert displayed for the event
7. **Activities** - Gives the details of activities executed by the processes that are run by the infected application.

- To export the Antivirus logs as a HTML file click the 'Export' button .
- To open a stored CCS log file, click the 'Open' button ✚.
- To refresh the Antivirus logs, click the 'Refresh' button .
- To clear the Antivirus logs click the 'Clear' button ✖.

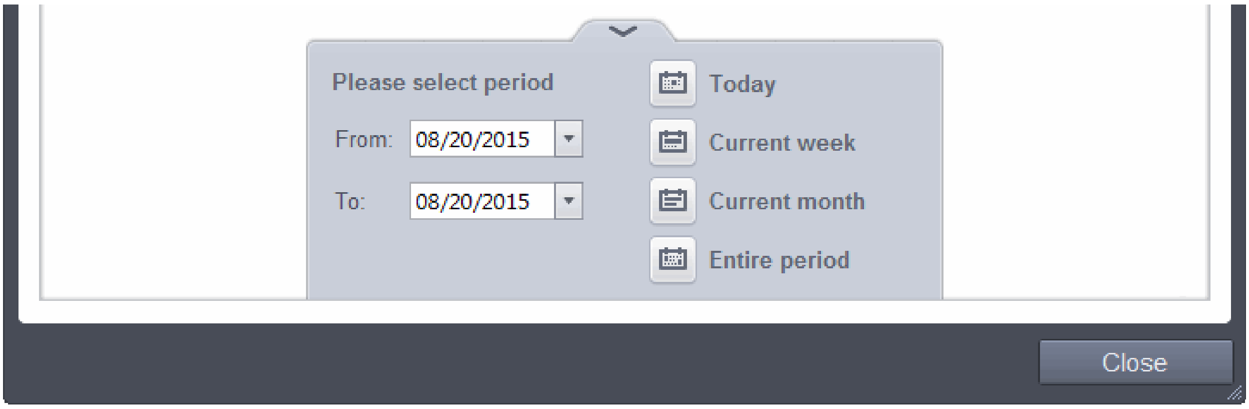
2.6.1.1. Filtering Antivirus Logs

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:

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



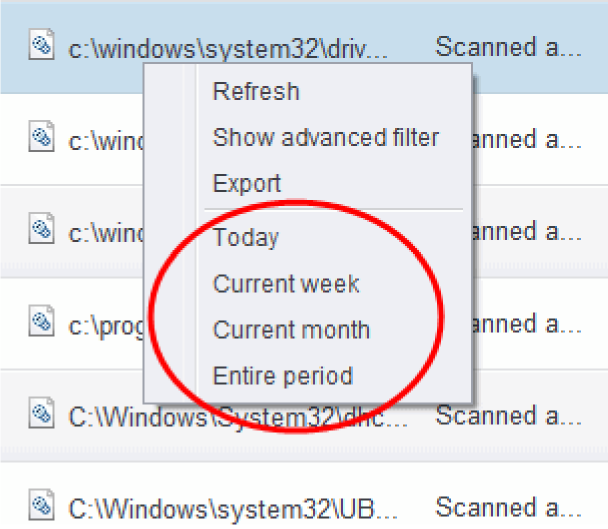
Please select period

From: 08/20/2015

To: 08/20/2015

- **Today -** Displays all logged events for today.
- **Current Week -** Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month -** Displays all logged events during the month that holds the current date.
- **Entire Period -** Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



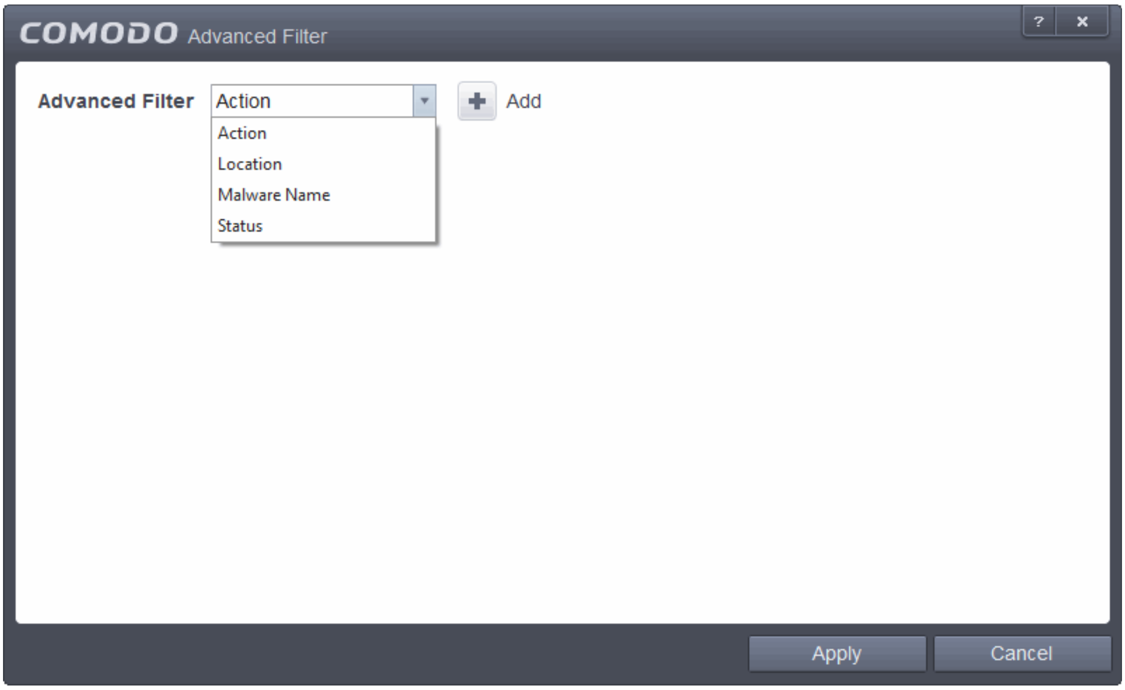
Advanced Filters:

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

- **Action** - Displays events according to the response (or action taken) by the Antivirus
- **Location** - Displays only the events logged from a specific location
- **Malware Name** - Displays only the events logged corresponding to a specific malware
- **Status** - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'

To configure Advanced Filters for Antivirus events

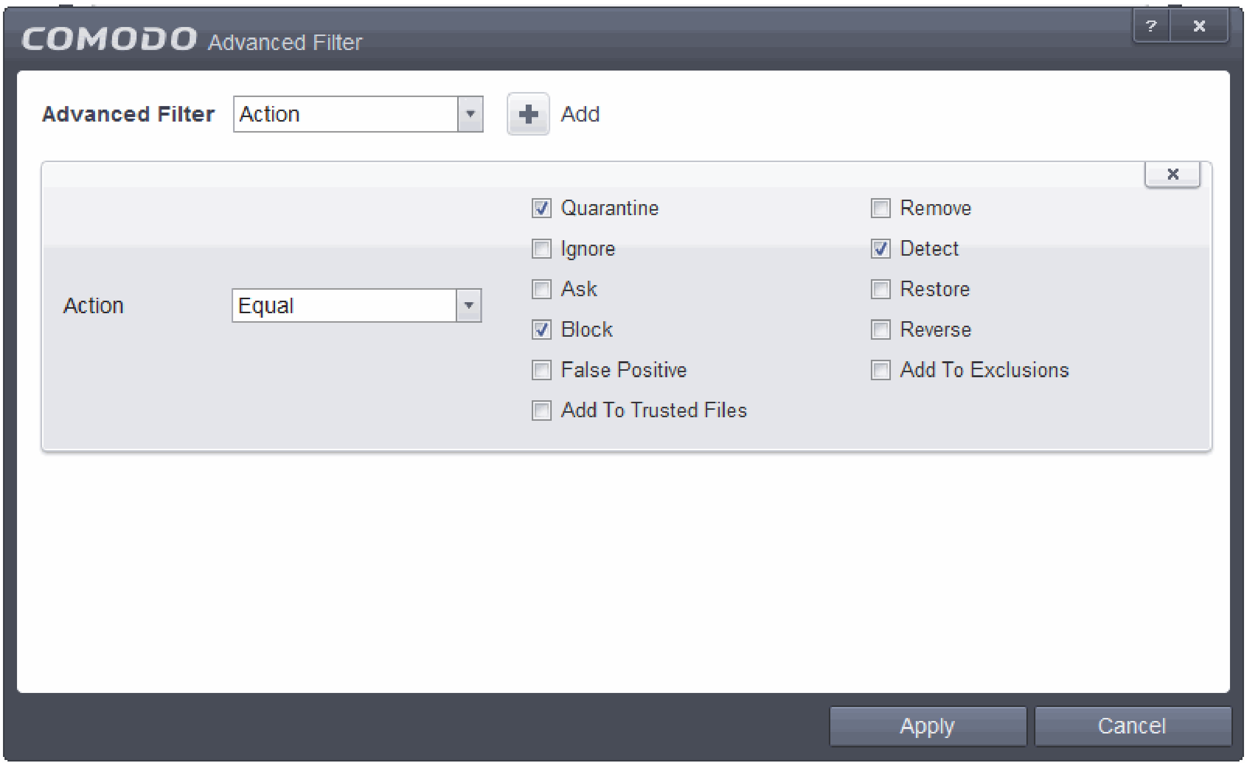
1. Click the funnel button from the title bar. The Advanced Filter interface for AV events will open
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 4 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

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

i. **Action:** The 'Action' option allows you to filter the entries based on the actions taken by CCS against the detected threat. Selecting the 'Action' option displays a drop down field and a set of specific filter parameters that can be selected or deselected.



Advanced Filter: Action

Action: Equal

☑ Quarantine
□ Remove
□ Ignore
☑ Detect
□ Ask
□ Restore
☑ Block
□ Reverse
□ False Positive
□ Add To Exclusions
□ Add To Trusted Files

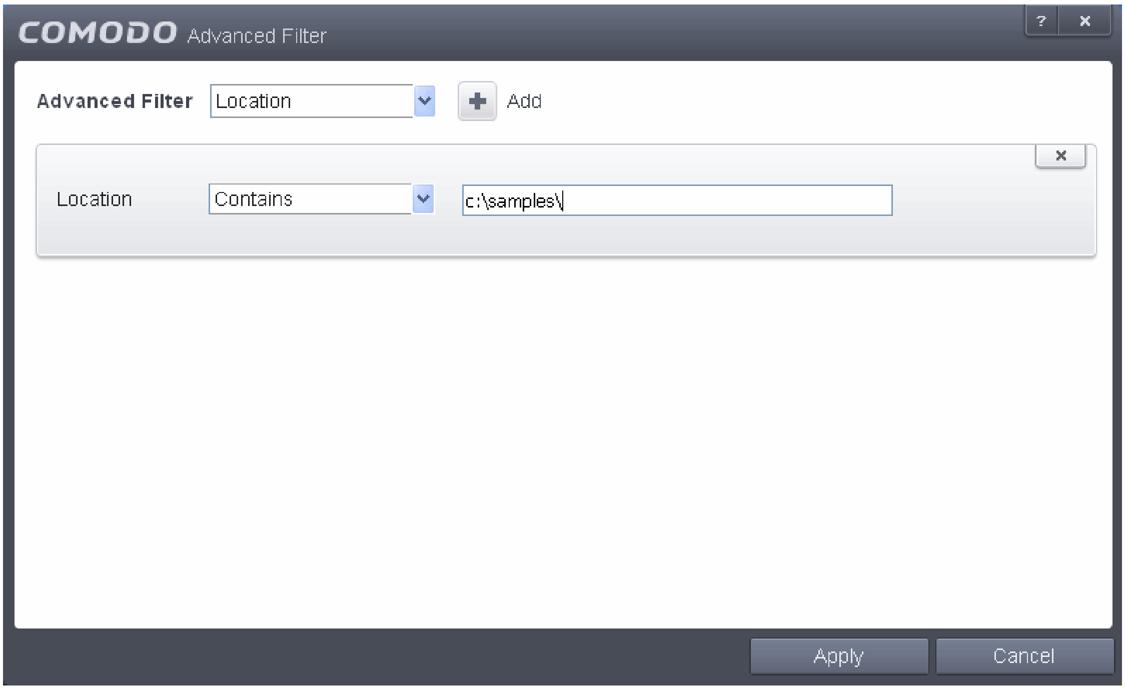
a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- Quarantine: Displays events where the user chose to quarantine a file
- Remove: Displays events where the user chose to delete an item
- Ignore: Displays events where the user chose to ignore an item
- Detect: Displays malware detection events
- Ask: Displays events where the user was asked for a response by an Advanced Protection, Firewall or Antivirus alert
- Restore: Displays events where an executable was quarantined and restored
- Block: Displays events where an application was blocked by CCS
- Reverse: Displays events where an application was reversed by CCS
- False Positive: Displays events where an executable was falsely detected as malicious
- Add To Exclusions: Displays events where an executable was added to the exclusion list
- Add To Trusted Files: Displays events where an executable was added to the trusted list

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

ii. **Location**: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



Advanced Filter: Location

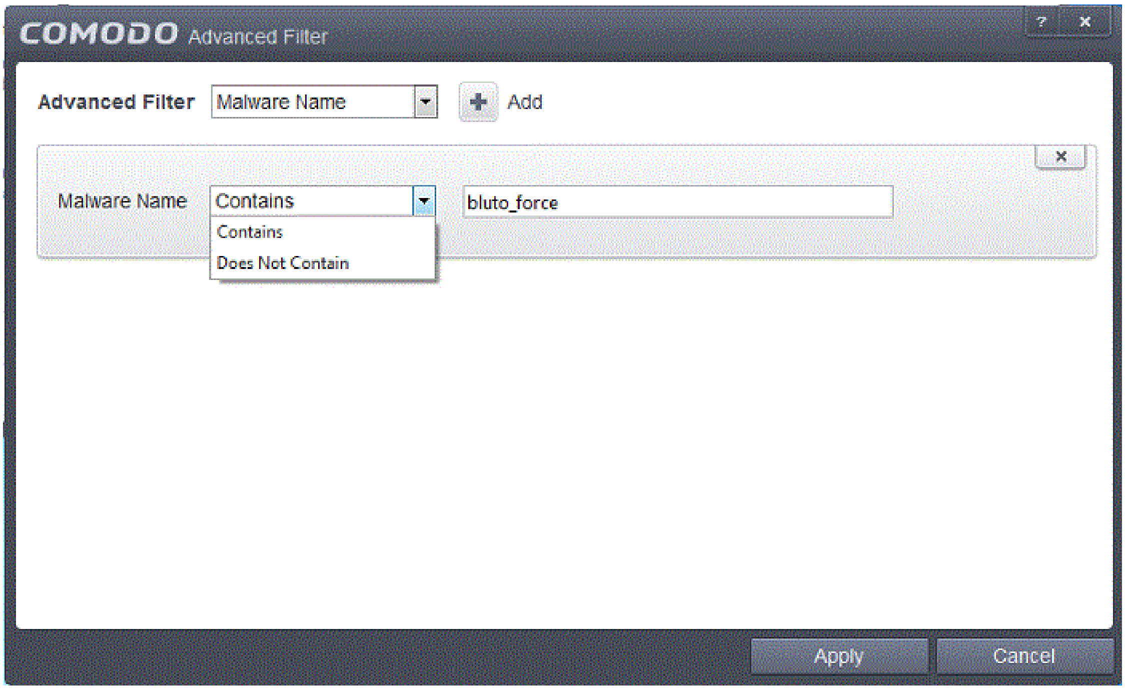
Location: Contains c:\samples\

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



Advanced Filter: Malware Name

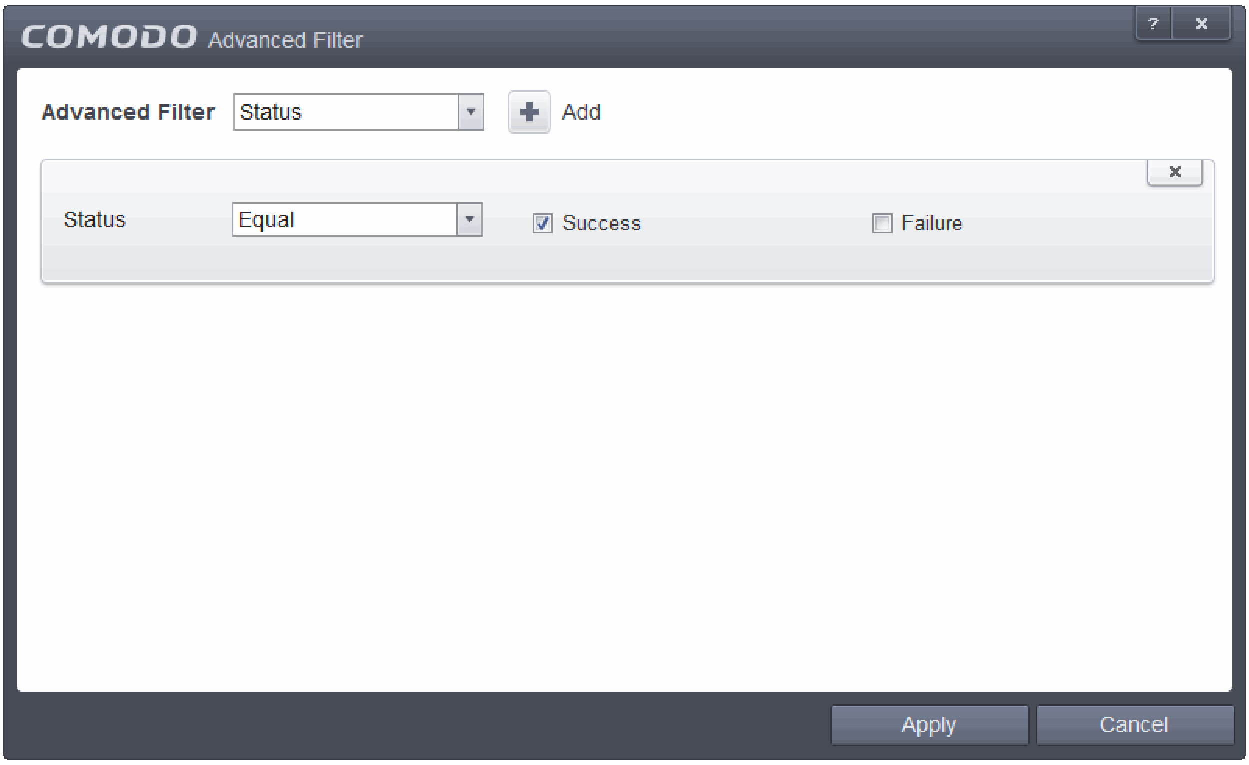
Malware Name: Contains bluto_force

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 select 'Contains' option from the drop-down field and enter the phrase 'bluto-force' in the text field, then all events containing the entry 'bluto-force' in the Malware Name field will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase 'bluto-force' in the text field, then all events that do not have the entry 'bluto-force' 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:

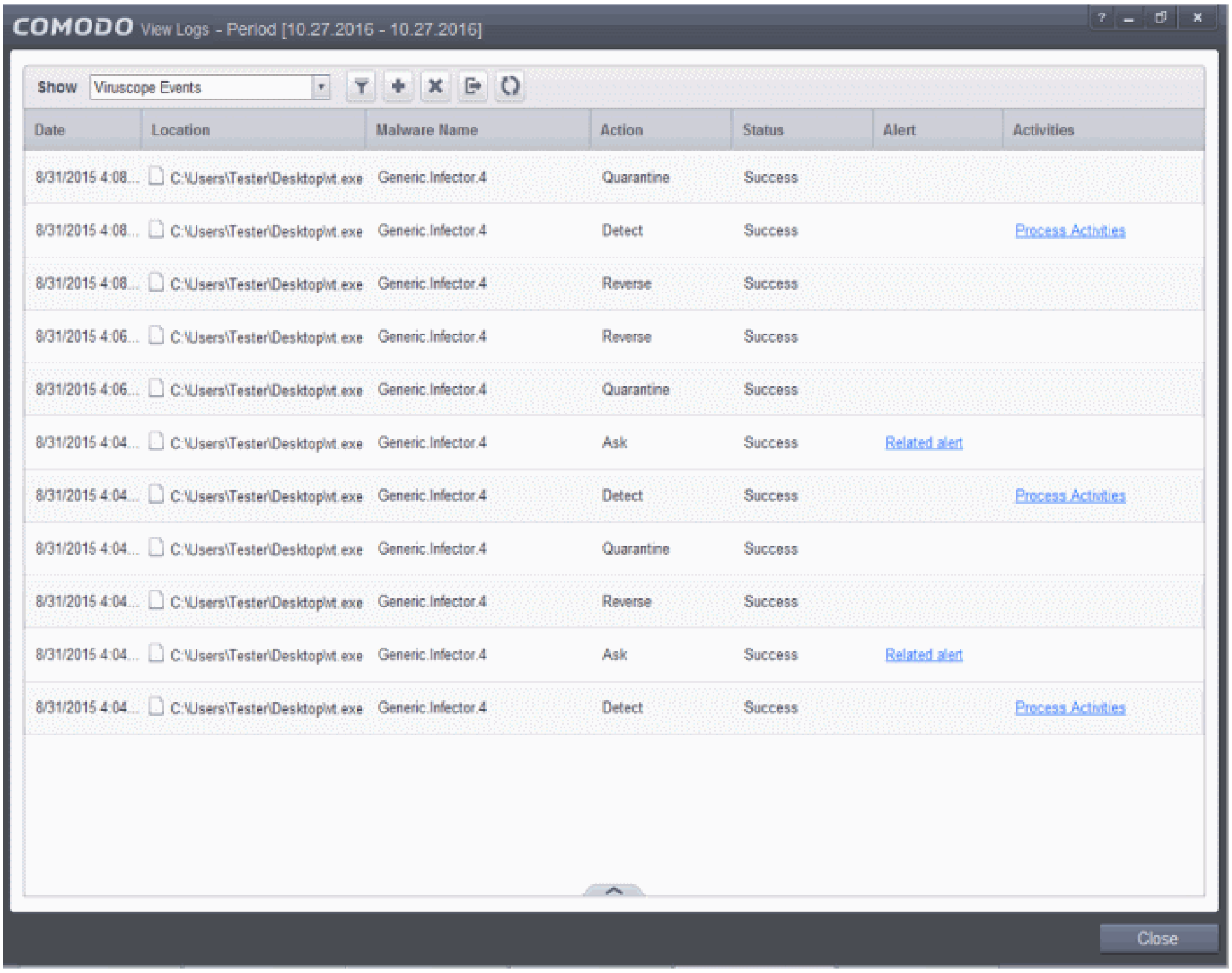
- Success: Displays Events that successfully executed (for example, the malware was successfully quarantined)
- Failure: Displays Events that failed to execute (for example, the database malware was not disinfected)

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.

2.6.2. Viruscope Logs

CCS record the events whenever the Viruscope module detects, blocks or reverses a suspicious activity. Viruscope logs can be viewed by selecting 'Viruscope Events' from the drop-down at the top of the log viewer interface.



Date	Location	Malware Name	Action	Status	Alert	Activities
8/31/2015 4:08...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Quarantine	Success		
8/31/2015 4:08...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Detect	Success		Process Activities
8/31/2015 4:08...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Reverse	Success		
8/31/2015 4:06...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Reverse	Success		
8/31/2015 4:06...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Quarantine	Success		
8/31/2015 4:04...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Ask	Success	Related alert	
8/31/2015 4:04...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Detect	Success		Process Activities
8/31/2015 4:04...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Quarantine	Success		
8/31/2015 4:04...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Reverse	Success		
8/31/2015 4:04...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Ask	Success	Related alert	
8/31/2015 4:04...	C:\Users\Tester\Desktop\vt.exe	Generic.Infector.4	Detect	Success		Process Activities

Column Descriptions

1. **Date** - Indicates the date of the event.
2. **Location** – Indicates where the suspicious executable is stored.
3. **Malware Name** - Name of the detected malware.
4. **Action** – Indicates the action taken by Viruscope in response to the event.
    - Reverse – Viruscope detected suspicious activity and attempted to reverse any changes made to the file system.
    - Quarantine – Viruscope placed the suspicious file into quarantine
    - Detect – Viruscope detected malicious activity but did not quarantine the executable or reverse its changes
    - Ask – Viruscope detected malicious activity and presented a pop-up asking the user whether it should quarantine the executable or reverse the changes.
5. **Status** - Status of the action taken - 'Success' or 'Fail'.
6. **Alert** – If available, this provides further details about the event.
7. **Activities** – Details of activities executed by the suspicious process.

- To export Viruscope logs as a HTML file, click the Export button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a saved CCS log file, click the Open button

- To refresh the Viruscope logs, click the Refresh button ⟳ or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.

- To delete the Viruscope logs click the 'Clear' button ✖.

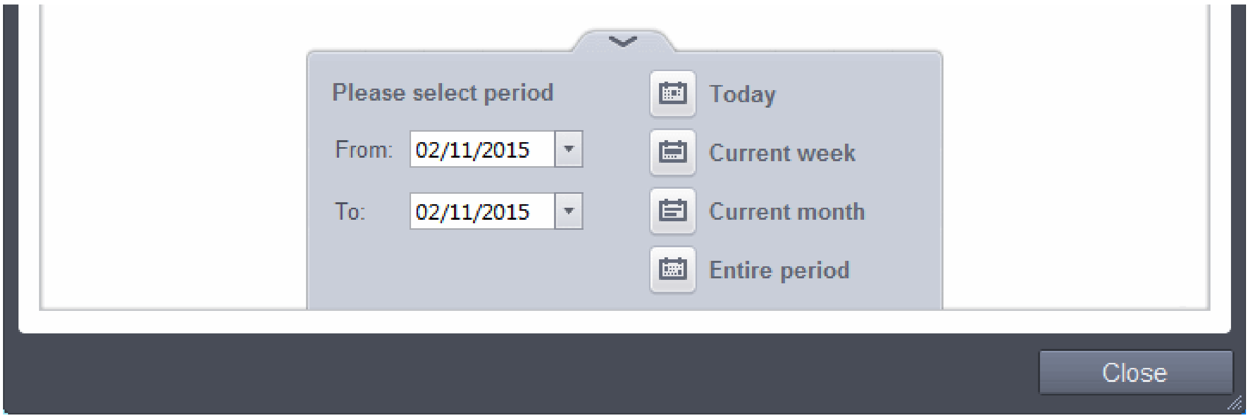
2.6.2.1. Filtering Viruscope Logs

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

- Preset Time Filters
- Advanced Filters

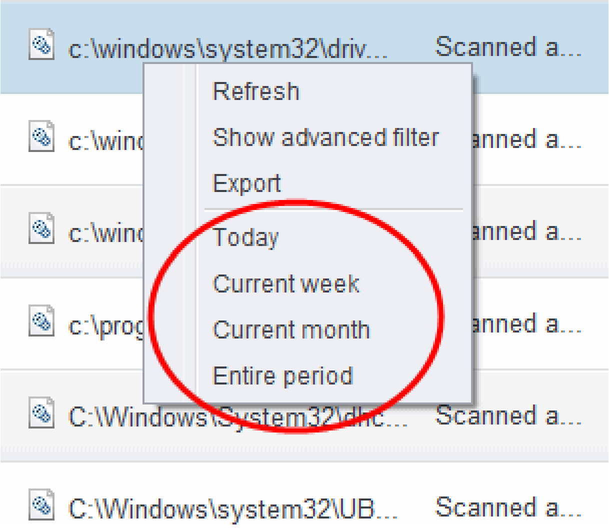
Preset Time Filters:

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** – Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'.

Alternatively, you can right click inside the log viewer module and choose the time period.


c:\windows\system32\driv... Scanned a...
Refresh
Show advanced filter
Export
Today
Current week
Current month
Entire period
c:\winc
c:\winc
c:\prog
anned a...
C:\Windows\System32\dhc... Scanned a...
C:\Windows\system32\UB... Scanned a...

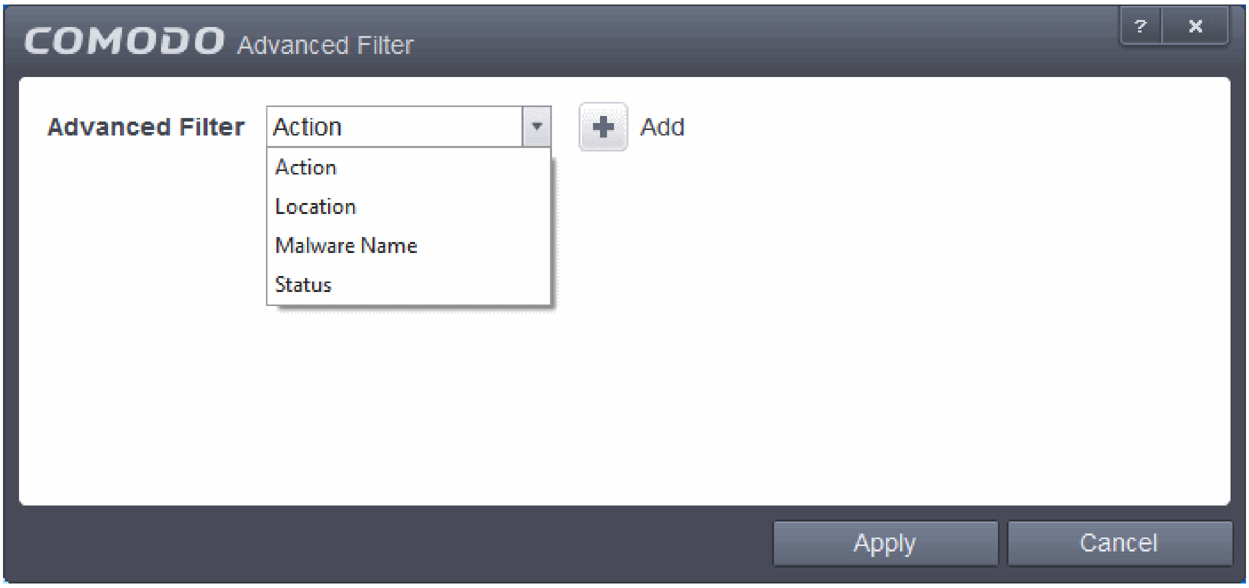
Advanced Filters

Having chosen a **preset time** filter you can further refine the displayed events according to specific filters. You can filter by:

- **Action** - Displays events according to the response (or action taken) by the Viruscope
- **Location** - Displays only the events logged from a specific location
- **Malware Name** - Displays only the events logged corresponding to a specific malware
- **Status** - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'

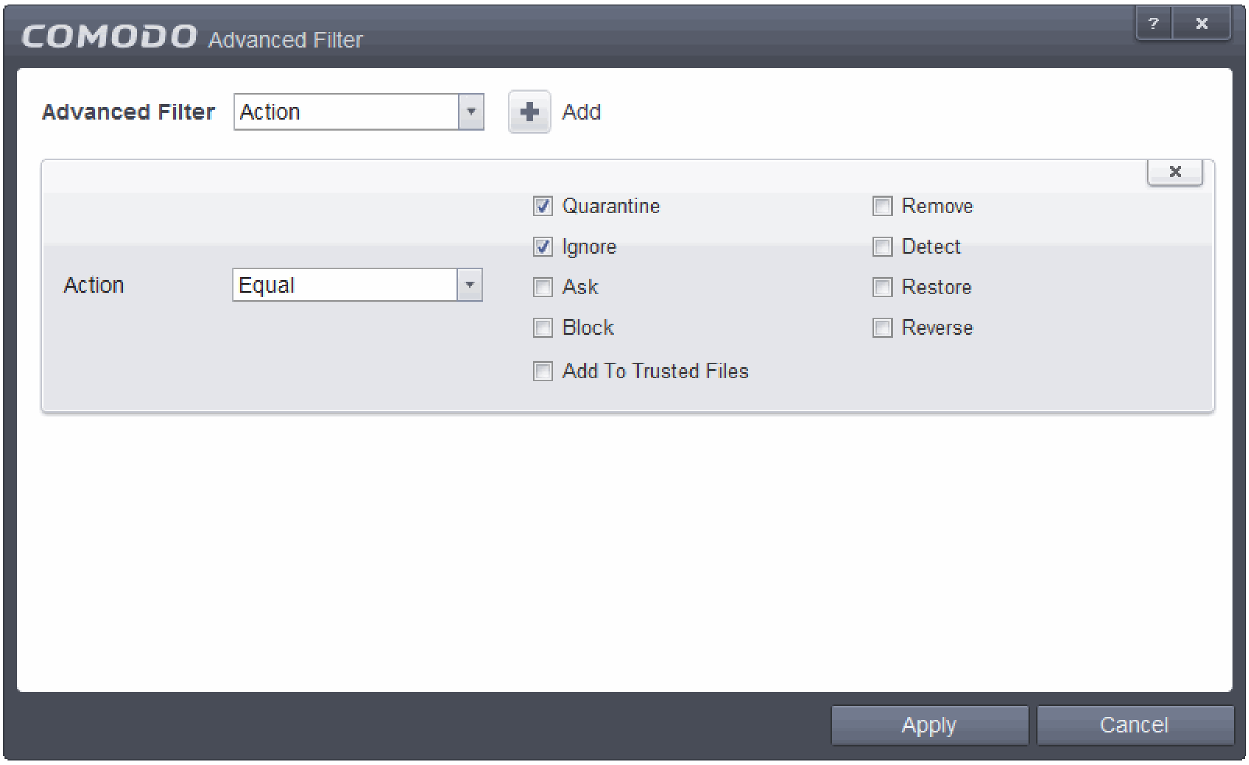
To configure Advanced Filters for Viruscope events

1. Click the funnel button from the title bar. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



Each of these 4 categories can be further refined by either selecting or deselecting specific filter parameters or typing a string into the field provided.

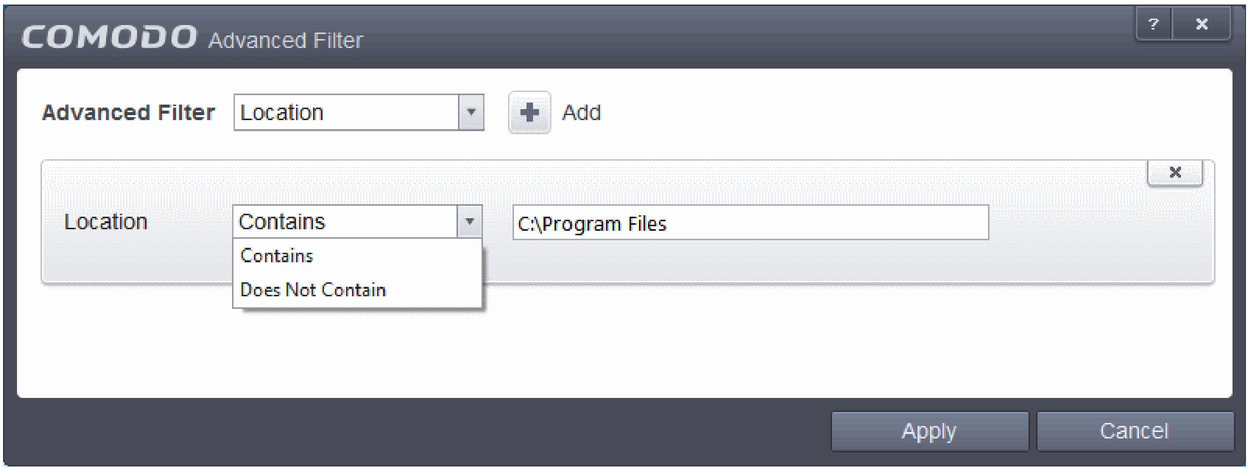
i. **Action**: The 'Action' option allows you to filter the entries based on the actions taken by CCS against the detected threat. Selecting the 'Action' option displays a drop down field and a set of specific filter parameters that can be selected or deselected.



a. Select 'Equal' or 'Not Equal' option from the drop down. '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 where the user chose to quarantine a file
    - Remove: Displays events where the user chose to delete an item
    - Ignore: Displays events where the user chose to ignore an item
    - Detect: Displays events for detection of a malware
    - Ask: Displays events when user was asked by alert concerning some Advanced Protection, Firewall or Antivirus event
    - Restore: Displays events of the applications that were quarantined and restored
    - Block: Displays events of the applications that were blocked
    - Add To Trusted Files: Displays events of the applications that were added to trusted files

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

ii. **Location**: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.

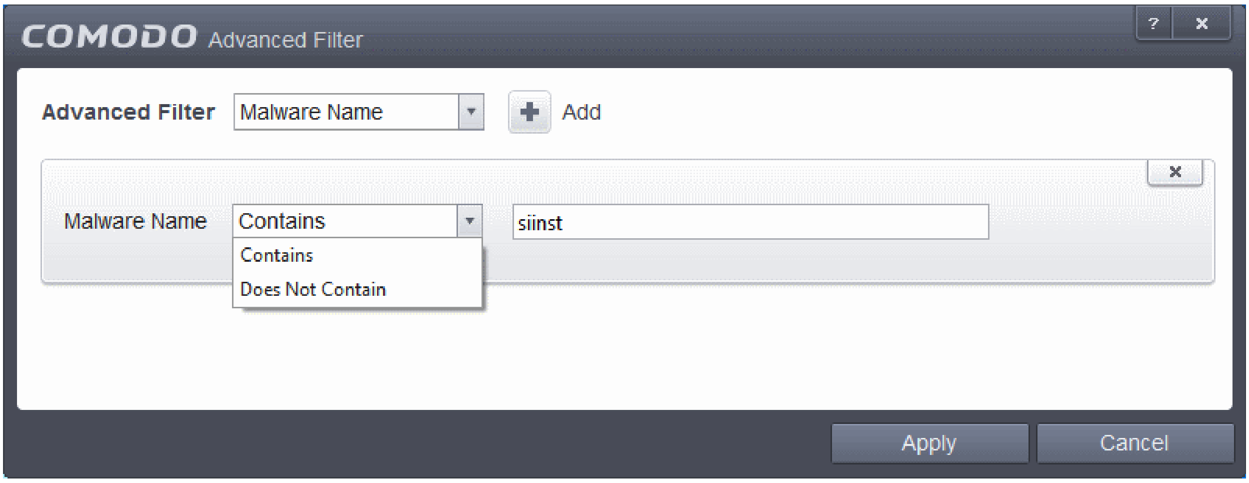


a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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

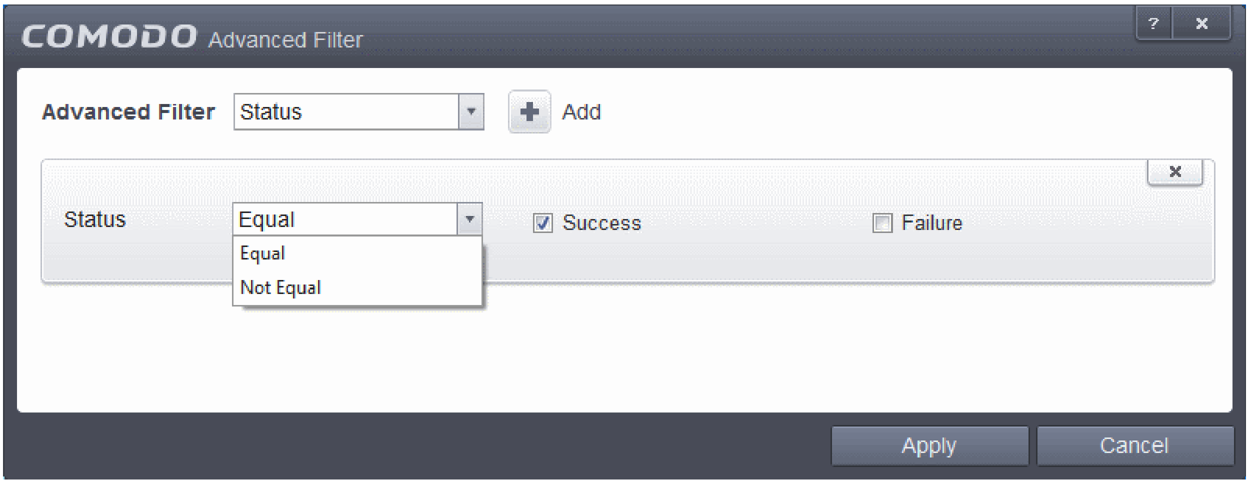
iii. **Malware Name**: The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



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' option from the drop-down and enter the phrase 'Bluto-Force' in the text field, then all events containing the entry 'Bluto-Force' in the Malware Name field will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'Bluto-Force' in the text field, then all events that do not have the entry 'Bluto-Force' 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 that successfully executed (for example, the malware was successfully quarantined)
- Failure: Displays Events that failed to execute (for example, the database malware was not disinfected)

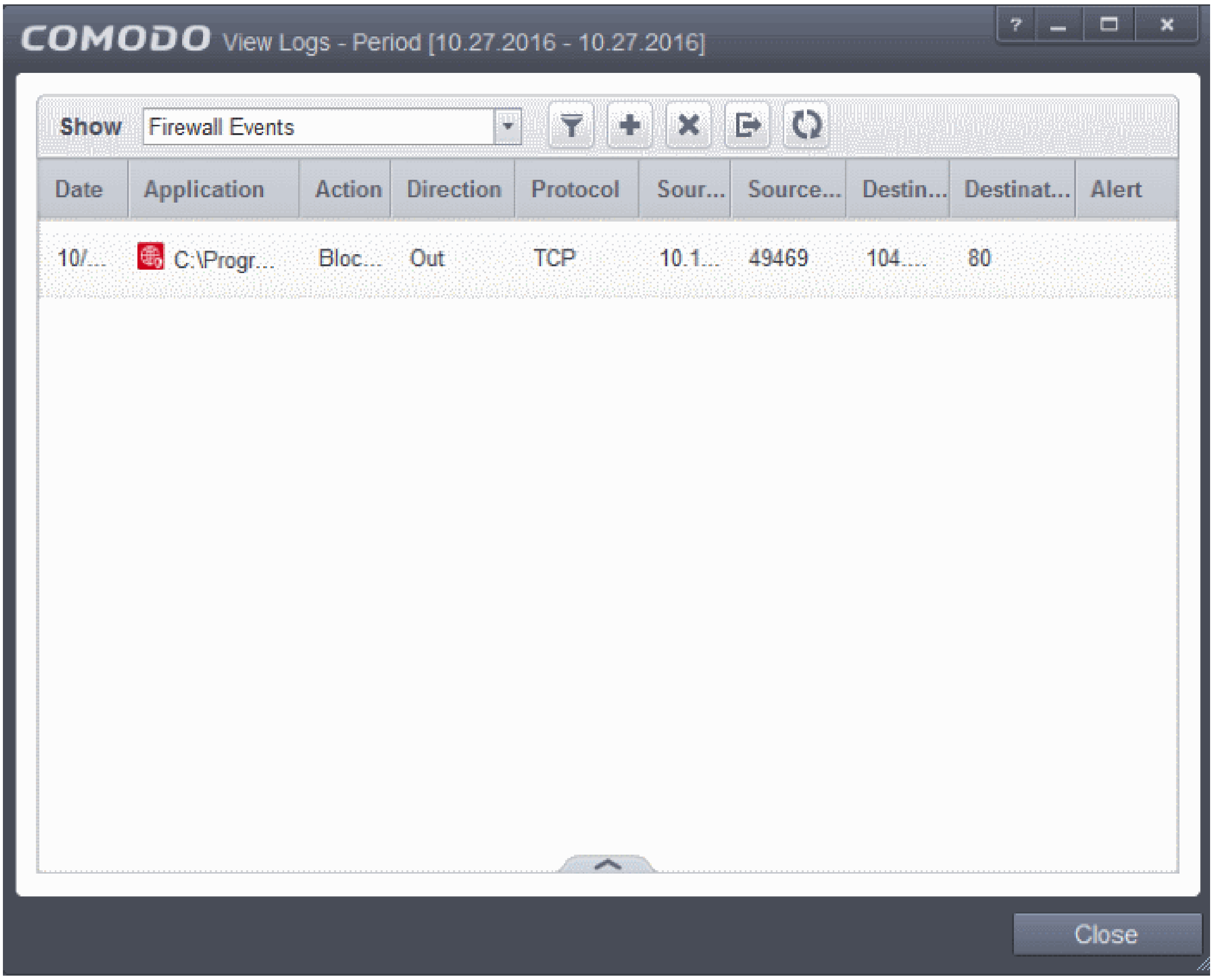
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

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

2.6.3. Firewall Logs

CCS 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.

The Firewall logs can be viewed by selecting 'Firewall Events' from the 'Show' drop-down of the log viewer interface.



COMODO View Logs - Period [10.27.2016 - 10.27.2016]

Show: Firewall Events

Date	Application	Action	Direction	Protocol	Sour...	Source...	Destin...	Destinat...	Alert
10/...	C:\Progr...	Bloc...	Out	TCP	10.1...	49469	104....	80	

Column Descriptions

1. **Date** - Contains precise details of the date and time of the connection attempt.
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** - Contains the actions for the events, indicating how the firewall has reacted to the connection attempt.
4. **Direction** - Indicates whether the connection attempt is inbound or outbound.
5. **Protocol** - Represents the Protocol used by the application that attempted to create the connection. This is usually TCP/IP or UDP - which are the most heavily used networking protocols.
6. **Source IP** - States the IP address of the host that made the connection attempt. This is usually the IP address of your computer for outbound connections.
7. **Source Port** - States the port number on the host at the source IP which was used to make this connection attempt.
8. **Destination IP** - States the IP address of the host to which the connection attempt was made. This is usually the IP address of your computer for inbound connections.
9. **Destination Port** - States the port number on the host at the destination IP to which the connection attempt was made.
10. **Alert** - Gives the details of the alert displayed for the event

- To export the Firewall logs as a HTML file click the Export button.
- To open a stored CCS log file, click the Open button.
- To refresh the Firewall logs, click the Refresh button.
- To clear the Firewall logs click the Clear button.

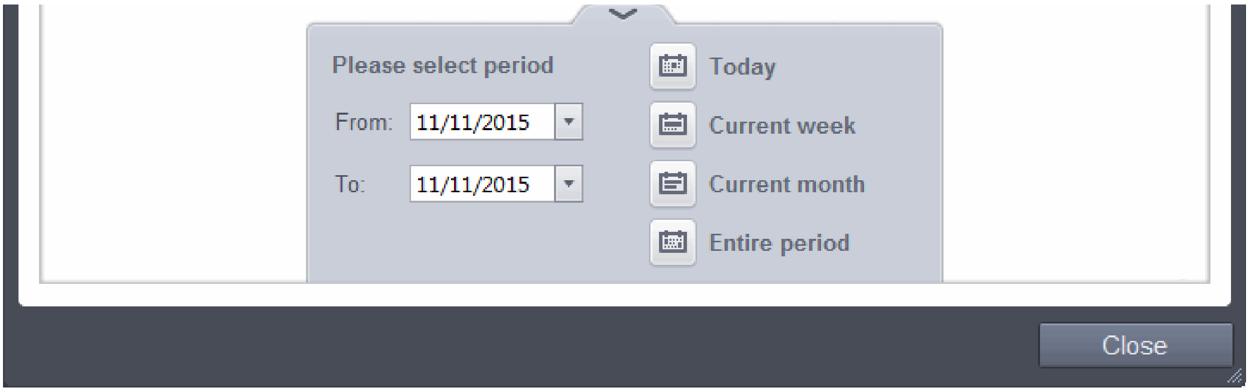
2.6.3.1. Filtering Firewall Logs

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

- Preset Time Filters
- Advanced Filters

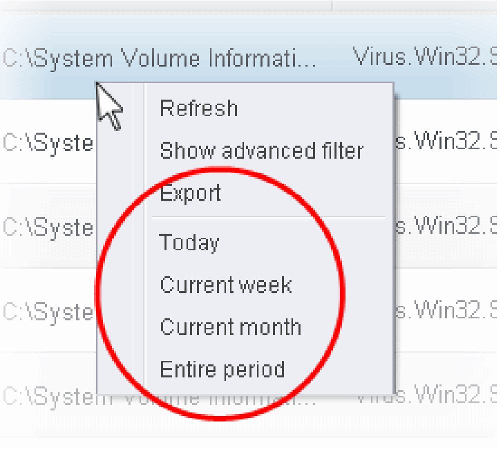
Preset Time Filters:

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since CCS was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



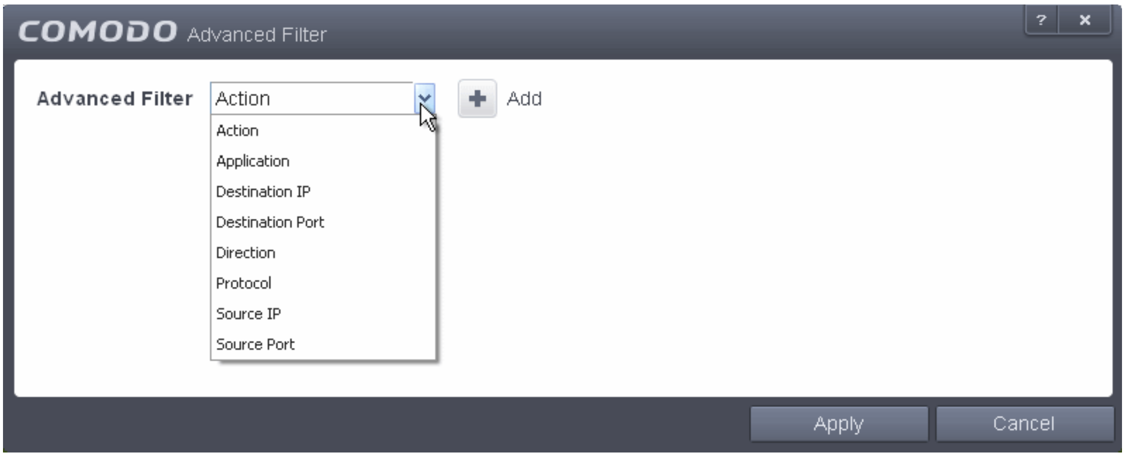
Advanced Filters

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

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

To configure Advanced Filters for Firewall events

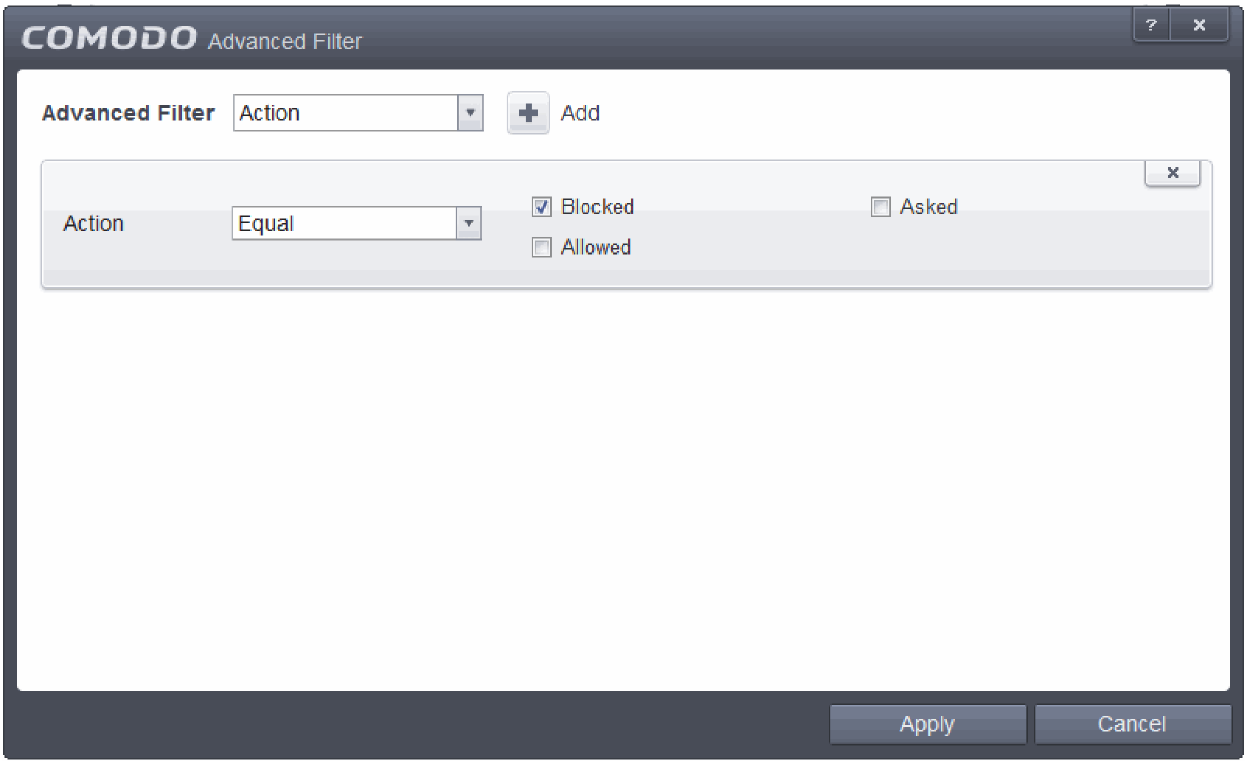
1. Click the funnel button from the title bar. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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



Advanced Filter: Action

Action: Equal

☑ Blocked

□ Allowed

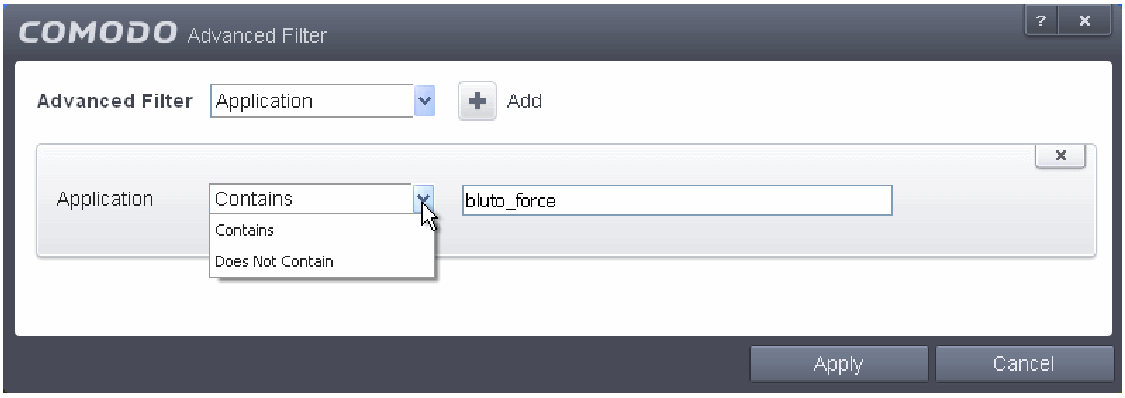
□ Asked

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 list of events that were blocked
- Allowed: Displays list of events that were allowed
- Asked: Displays list of events that were asked to the user

ii. **Application**: Selecting the 'Application' option displays a drop-down box and text entry field.



Advanced Filter: Application

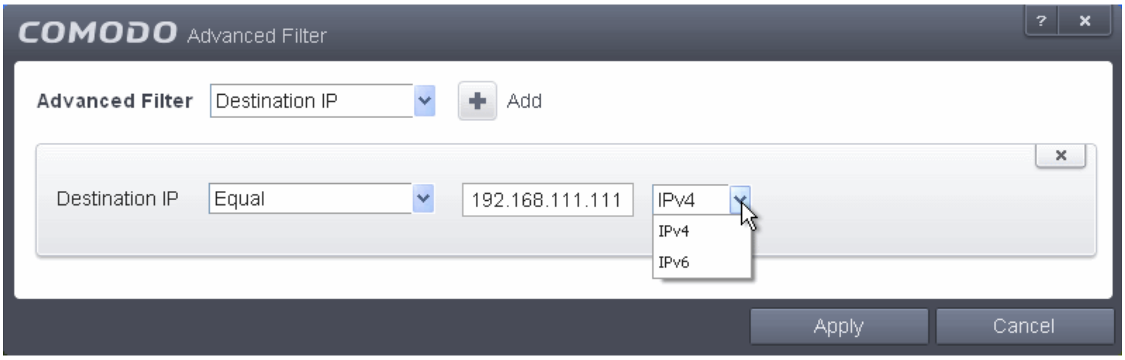
Application: Contains bluto_force

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 select 'Contains' option from the drop-down field and enter the phrase 'bluto-force' in the text field, then all events containing the entry 'bluto-force' in the 'Application' column will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase 'bluto-force' in the text field, then all events that do not have the entry 'bluto-force' in the 'Application' column will be displayed.

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



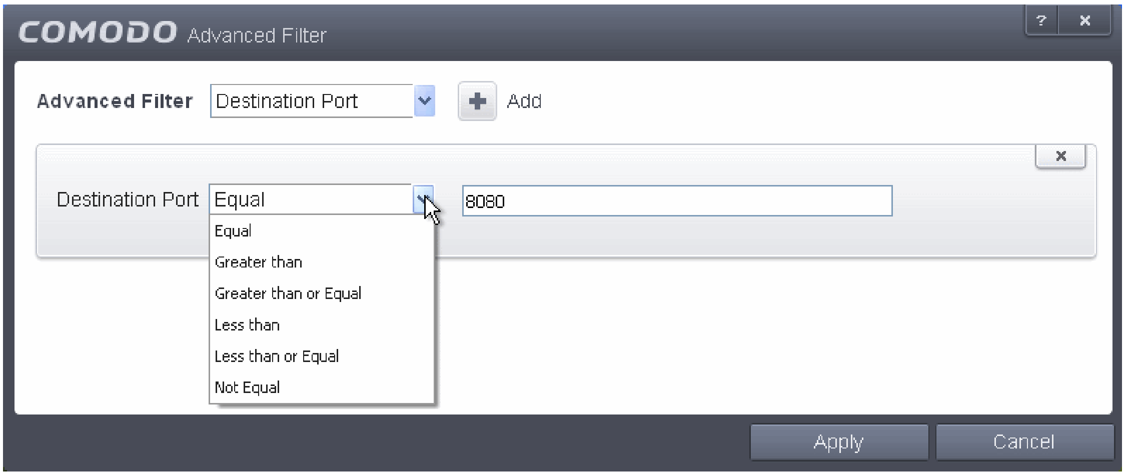
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Select 'IPv4' or 'IPv6' from the drop-down box.

c) Enter the destination system's IP address that needs to be filtered.

For example, if you select 'Contains' option from the drop-down field, select IPv4 and enter 192.168.111.111 in the text fields, then all events containing the entry '192.168.111.111' in the 'Destination IP' column will be displayed.

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



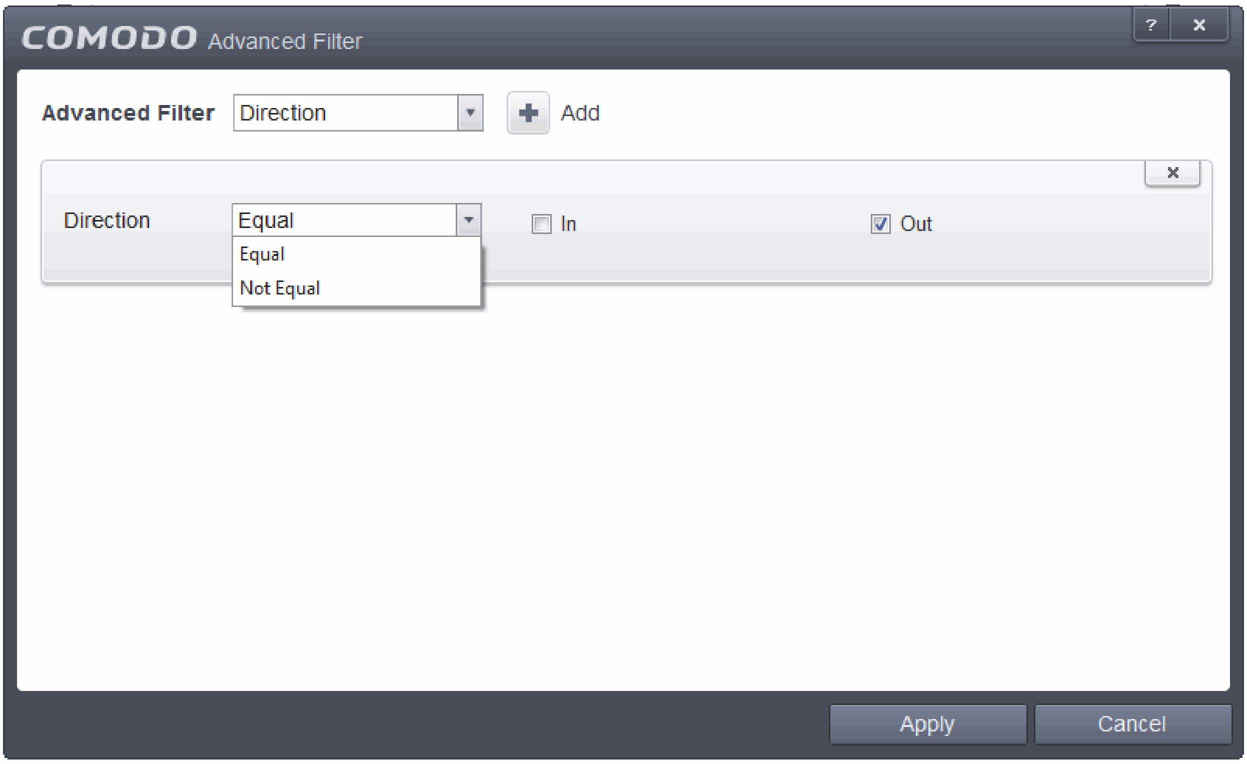
a) Select any one of the following option the drop-down box.

- Equal
- Greater than
- Greater than or Equal
- Less than
- Less than or Equal
- Not Equal

b) Now enter the destination port number in the text entry field.

For example, if you select 'Equal' option from the drop-down field 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.

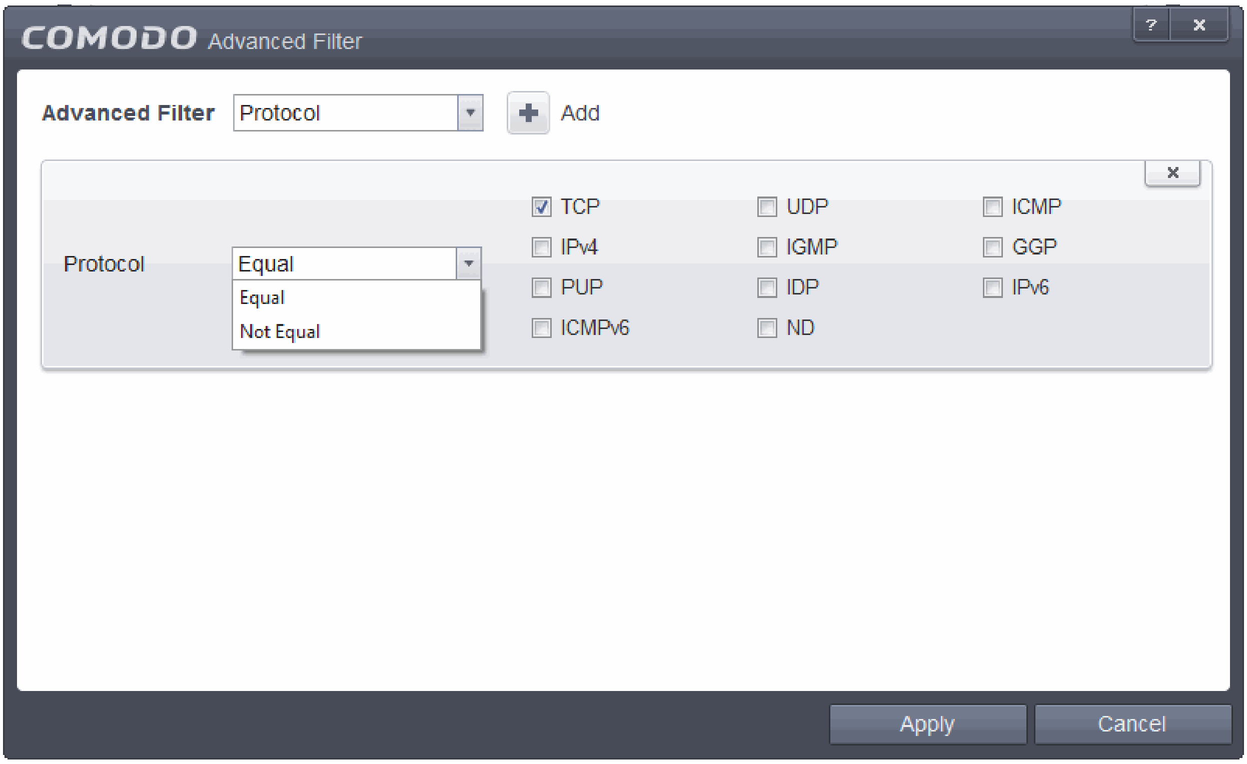


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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 that were directed into the system
- Out: Displays a list of events that were directed out of the system

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

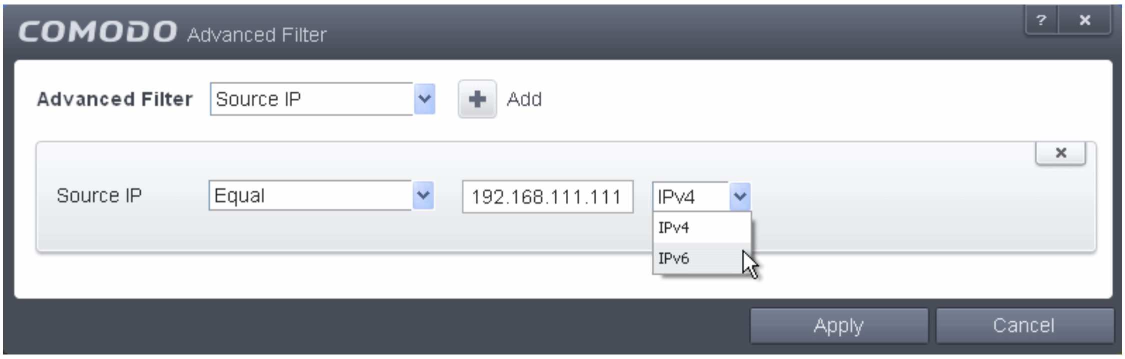


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

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

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

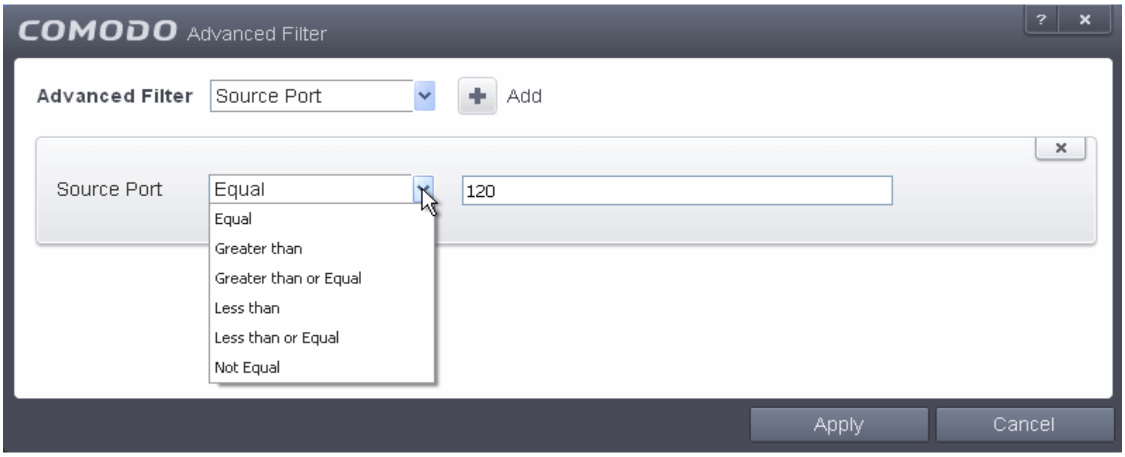


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Select 'IPv4' or 'IPv6' from the drop-down box.

c) Enter the source system's IP address that needs to be filtered.

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.

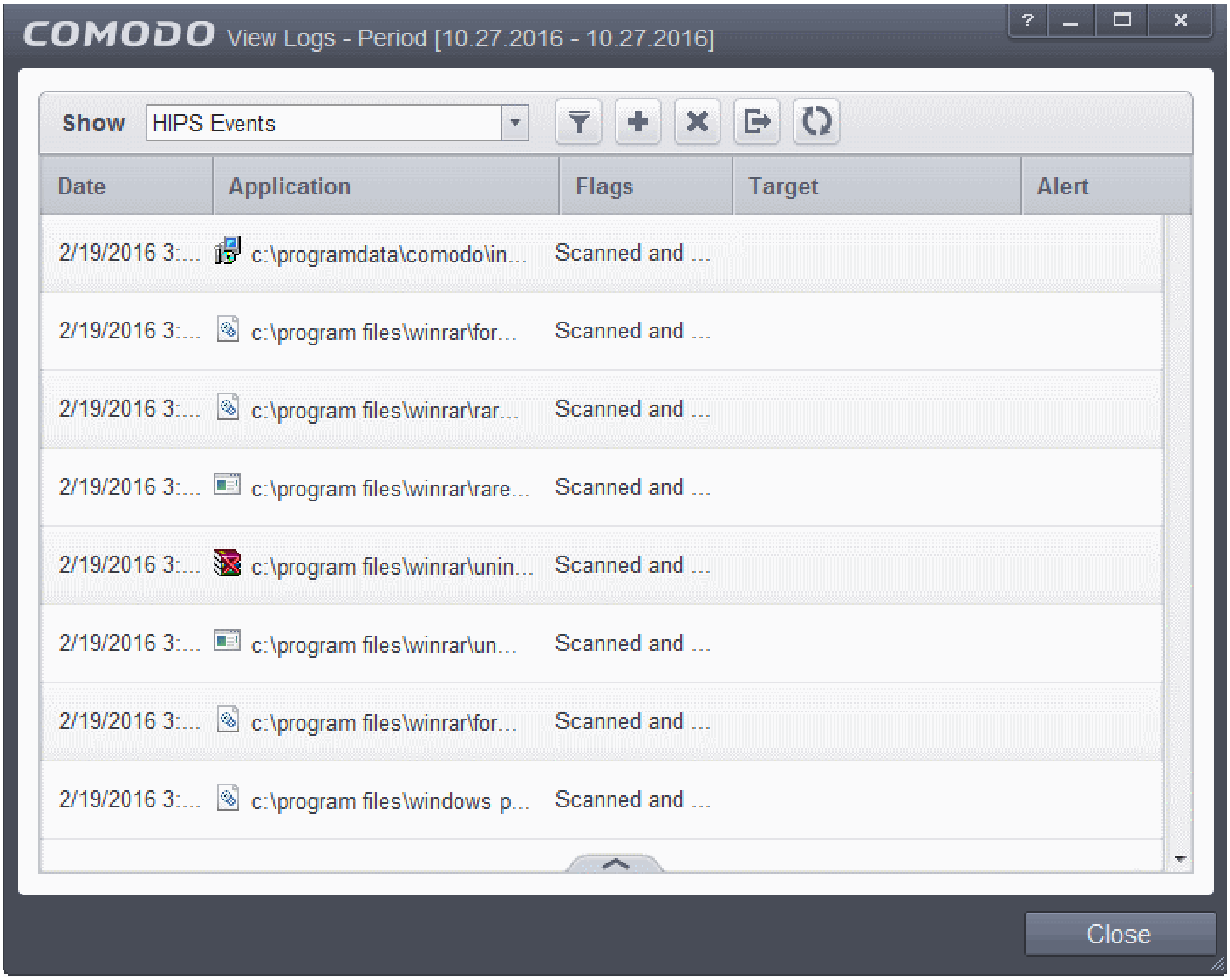
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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.

2.6.4. 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.

The HIPS logs can be viewed by selecting 'HIPS Events' tab from the 'Show' drop-down of the log viewer interface.


COMODO View Logs - Period [10.27.2016 - 10.27.2016]

Show: HIPS Events

Date	Application	Flags	Target	Alert
2/19/2016 3:...	c:\programdata\comodo\in...	Scanned and ...		
2/19/2016 3:...	c:\program files\winrar\for...	Scanned and ...		
2/19/2016 3:...	c:\program files\winrar\rar...	Scanned and ...		
2/19/2016 3:...	c:\program files\winrar\rare...	Scanned and ...		
2/19/2016 3:...	c:\program files\winrar\unin...	Scanned and ...		
2/19/2016 3:...	c:\program files\winrar\un...	Scanned and ...		
2/19/2016 3:...	c:\program files\winrar\for...	Scanned and ...		
2/19/2016 3:...	c:\program files\windows p...	Scanned and ...		

Column Descriptions

1. **Date** - Contains precise details of the date and time of the access attempt.
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. **Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
4. **Target** - Represents the location of the target file.
5. **Alert** - Gives the details of the alert displayed for the event

- To export the HIPS logs as a HTML file click the 'Export' button ⇨.
- To open a stored CCS log file, click the 'Open' button ✚.
- To refresh the HIPS logs, click the 'Refresh' button ⟳.
- To clear the HIPS logs click the 'Clear' button ✖.

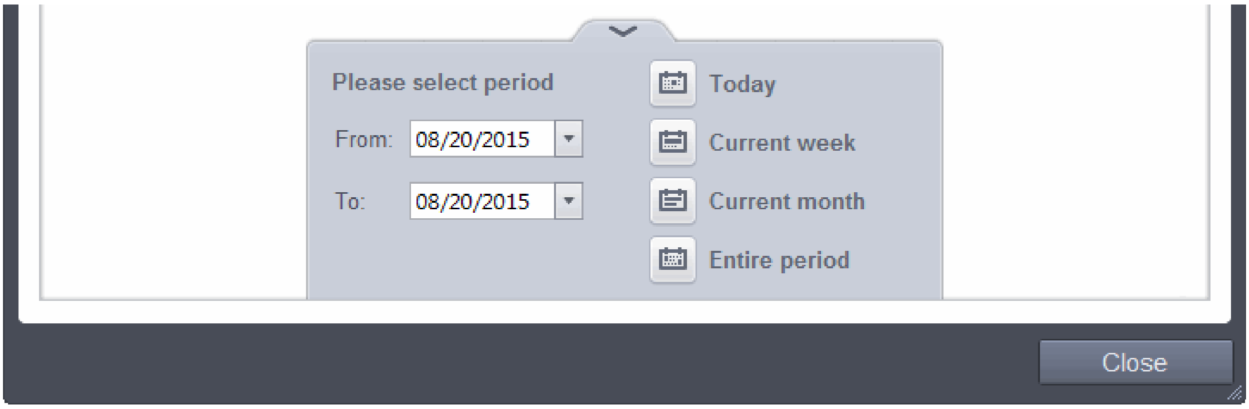
2.6.4.1. Filtering HIPS Logs

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

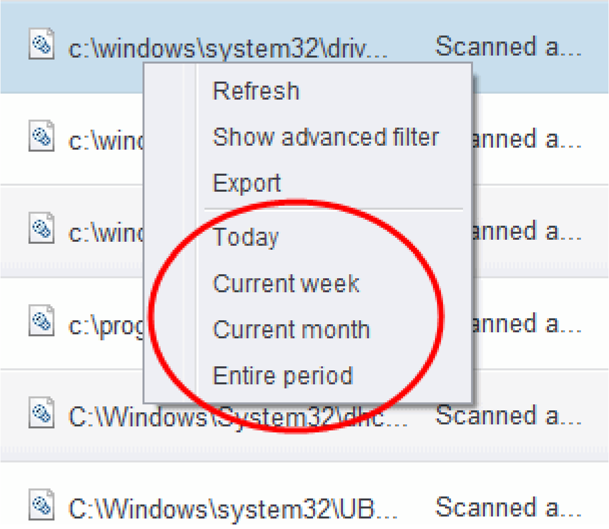
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:


Please select period
From: 08/20/2015
To: 08/20/2015

- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



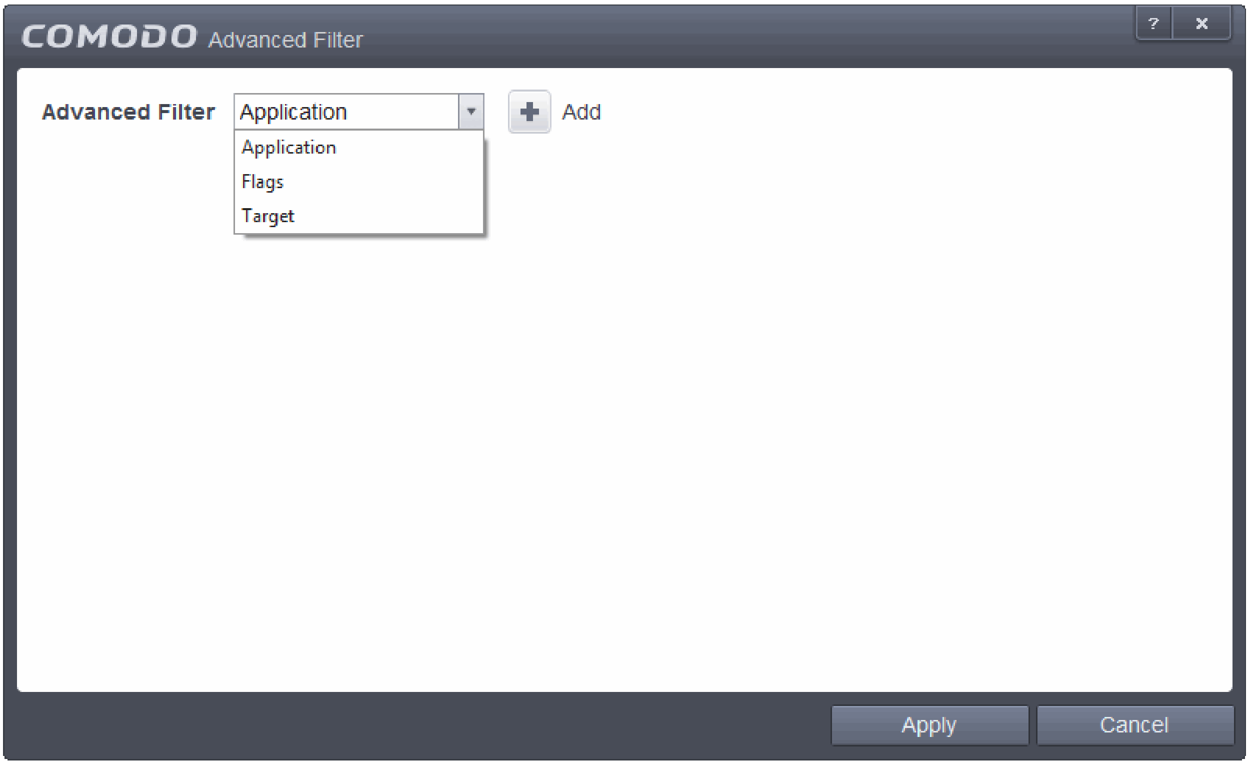
Advanced Filters

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

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

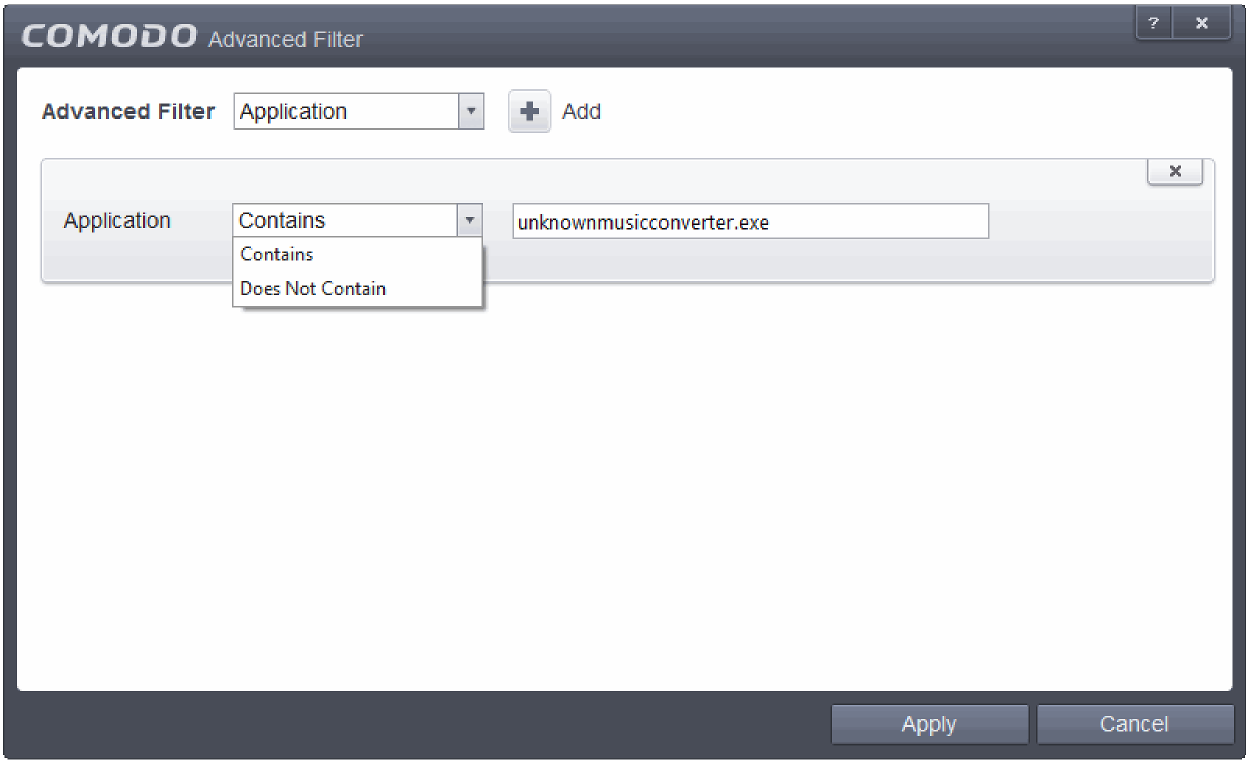
To configure Advanced Filters for HIPS events

1. Click the funnel button from the title bar. The Advanced Filter interface for HIPS events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 3 categories of filter 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. Following are the options available in the 'Advanced Filter' drop-down:

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



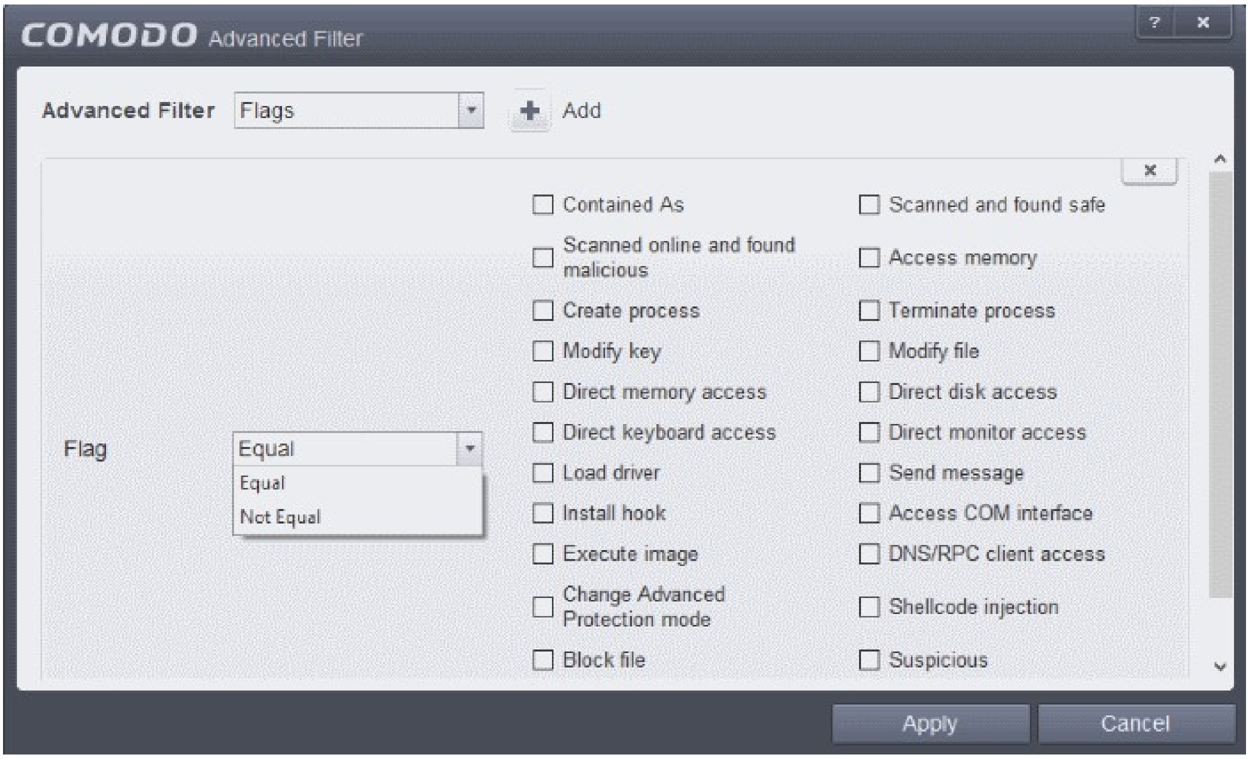
Application: Contains — unknownmusicconverter.exe

a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word that needs to be filtered.

For example, if you select 'Contains' option from the drop-down field and enter the phrase 'cuckoomp3.exe' in the text field, then all events containing the entry 'unknownmusicconverter.exe' in the 'Application' column will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase 'unknownmusicconverter.exe' in the text field, then all events that do not have the entry 'unknownmusicconverter.exe' in the 'Application' column will be displayed.

ii. **Flags**: Selecting the 'Flags' option displays a drop down menu and a set of specific 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.

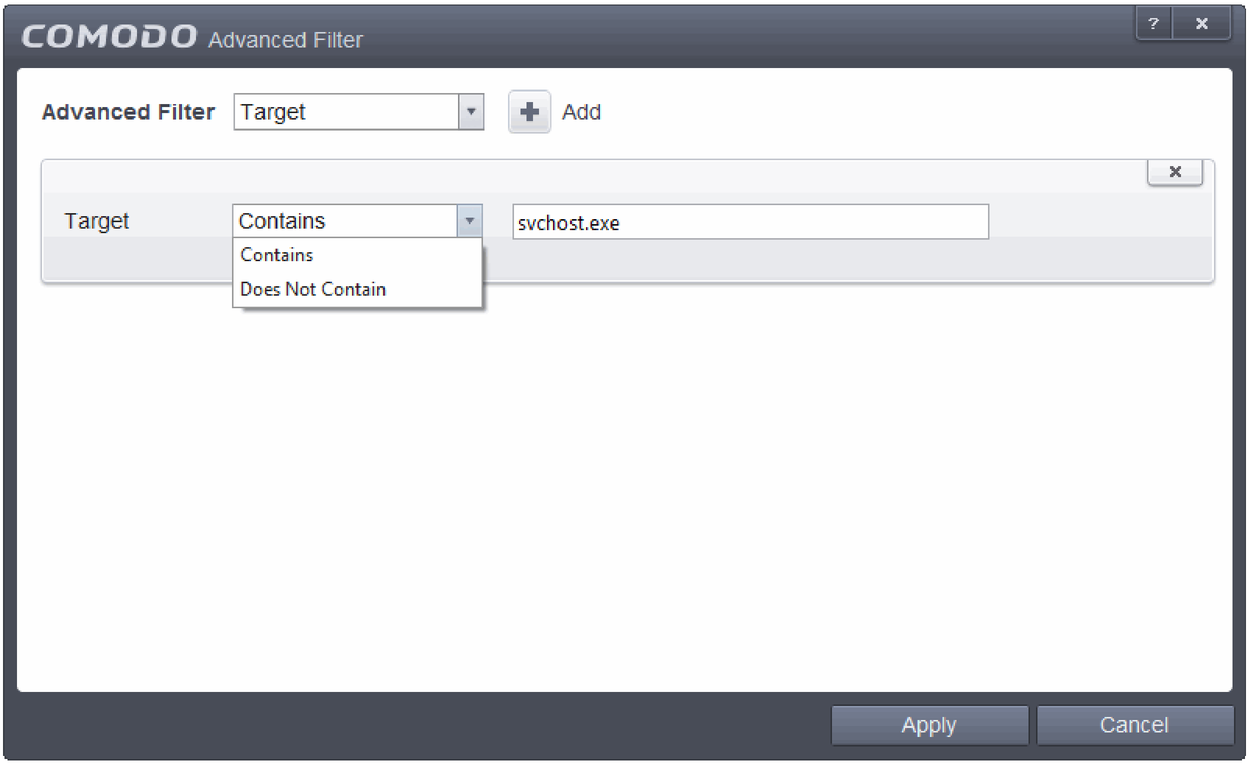
d) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Contained As
- Scanned Online and Found Safe
- 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 Advanced Protection Mode
- Shellcode Injection
- Block File
- Suspicious
- Hook
- Alert Suppressed

For example, if you select 'Equal' option from the drop-down field and select 'Contained as' from the checkboxes, then only events of applications auto-contained by HIPS will be displayed. If you select 'Not Equal' option from the drop-down field and select 'Modify Key' check box, then all events that do not have the entry 'Modify Key' in the 'Flags' column will be displayed. You can select more than one check box options from this interface, as required.

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



svchost.exe

a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word that needs to be filtered from the Target column.

For example, if you select 'Contains' option from the drop-down field 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 select 'Does Not Contain' option from the drop-down field and enter the phrase 'svchost.exe' in the text field, then all events that do not have the entry 'svchost.exe' in the 'Target' column will be displayed.

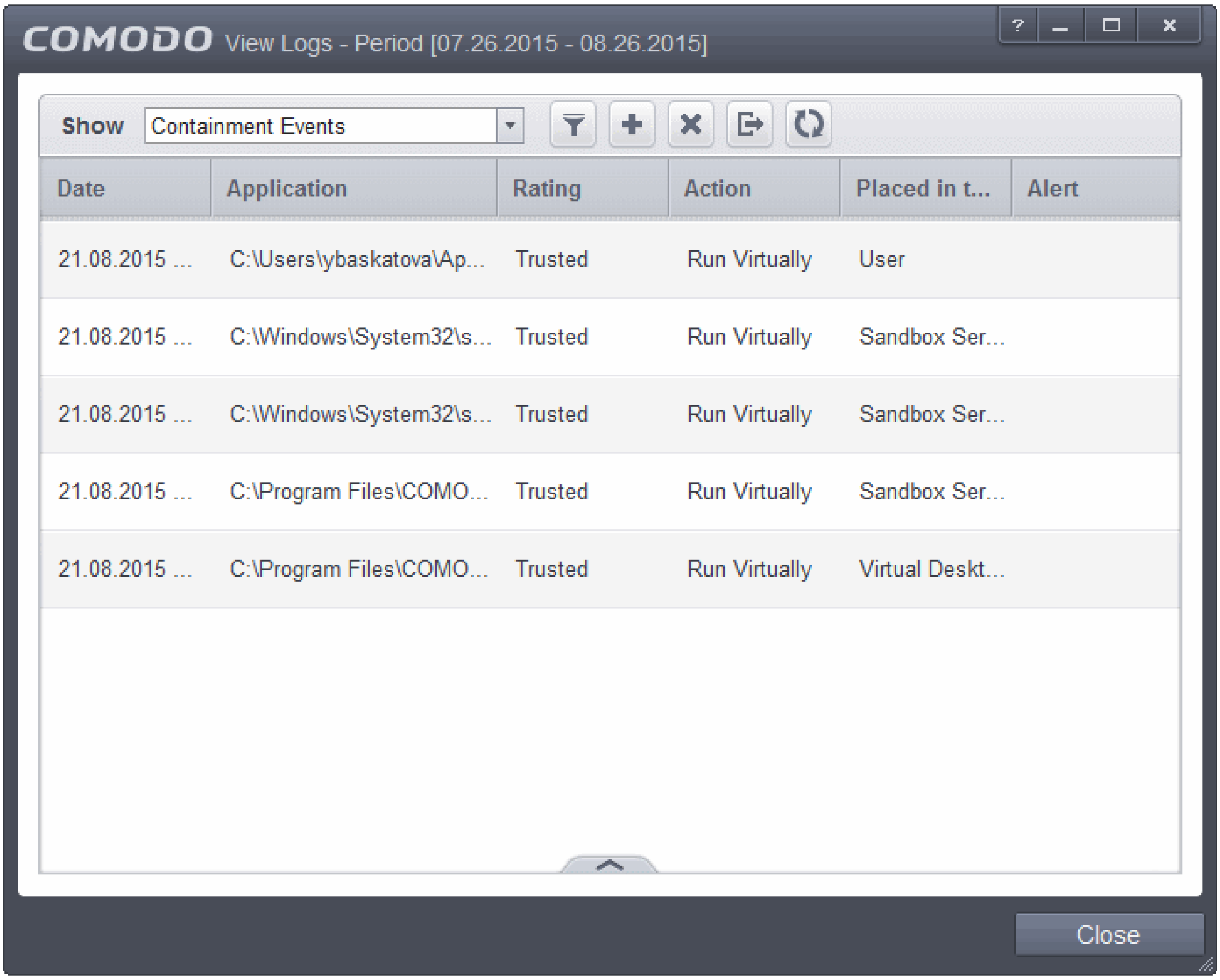
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- 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.

2.6.5. Containment Logs

'Containment Events' are generated whenever an application is placed in containment and provide more details about the conditions of the containment operation.

Containment logs can be viewed by selecting 'Containment Events' from the drop-down at the top of the log viewer interface.



Show: Containment Events

Date	Application	Rating	Action	Placed in t...	Alert
21.08.2015 ...	C:\Users\ybaskatova\Ap...	Trusted	Run Virtually	User	
21.08.2015 ...	C:\Windows\System32\s...	Trusted	Run Virtually	Sandbox Ser...	
21.08.2015 ...	C:\Windows\System32\s...	Trusted	Run Virtually	Sandbox Ser...	
21.08.2015 ...	C:\Program Files\COMO...	Trusted	Run Virtually	Sandbox Ser...	
21.08.2015 ...	C:\Program Files\COMO...	Trusted	Run Virtually	Virtual Deskt...	

Column Descriptions

1. **Date** - Indicates the date 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. **Rating** – Indicates the rating status of application
4. **Action** - Indicates the action taken by Containment in response to the event.
5. **Placed in the Containment by** – Indicates the service or user which implemented the containment operation.
6. **Alert** - Gives the details of the alert displayed for the event

- To export the Containment logs as a HTML file, click the 'Export' button .
- To open a stored CCS log file, click the 'Open' button .
- To refresh the Containment logs, click the 'Refresh' button .

- To clear the Containment logs, click the 'Clear' button ✖.

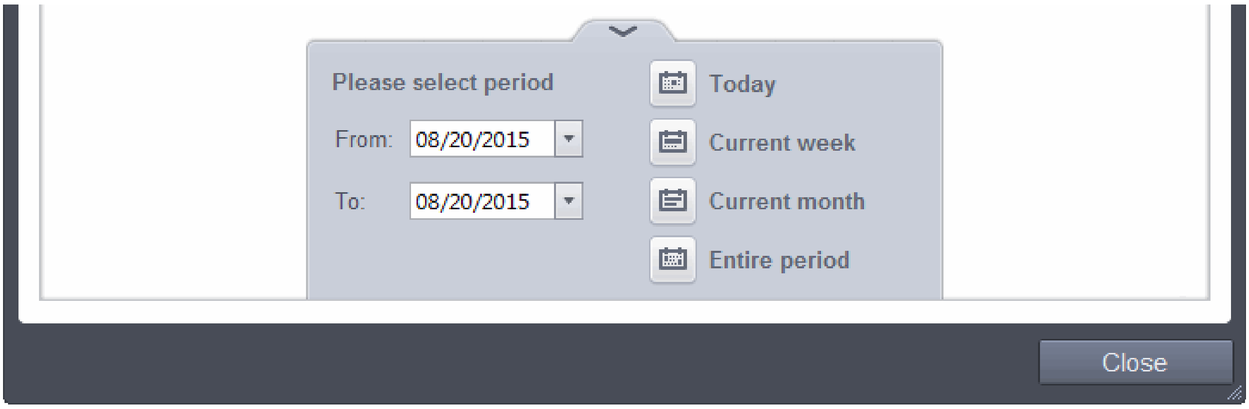
2.6.5.1. Filtering Containment Logs

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

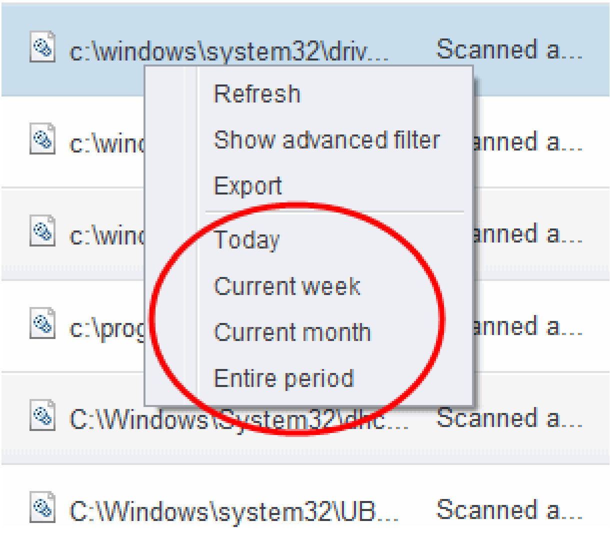
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** – Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'.

Alternatively, you can right click inside the log viewer module and choose the time period.



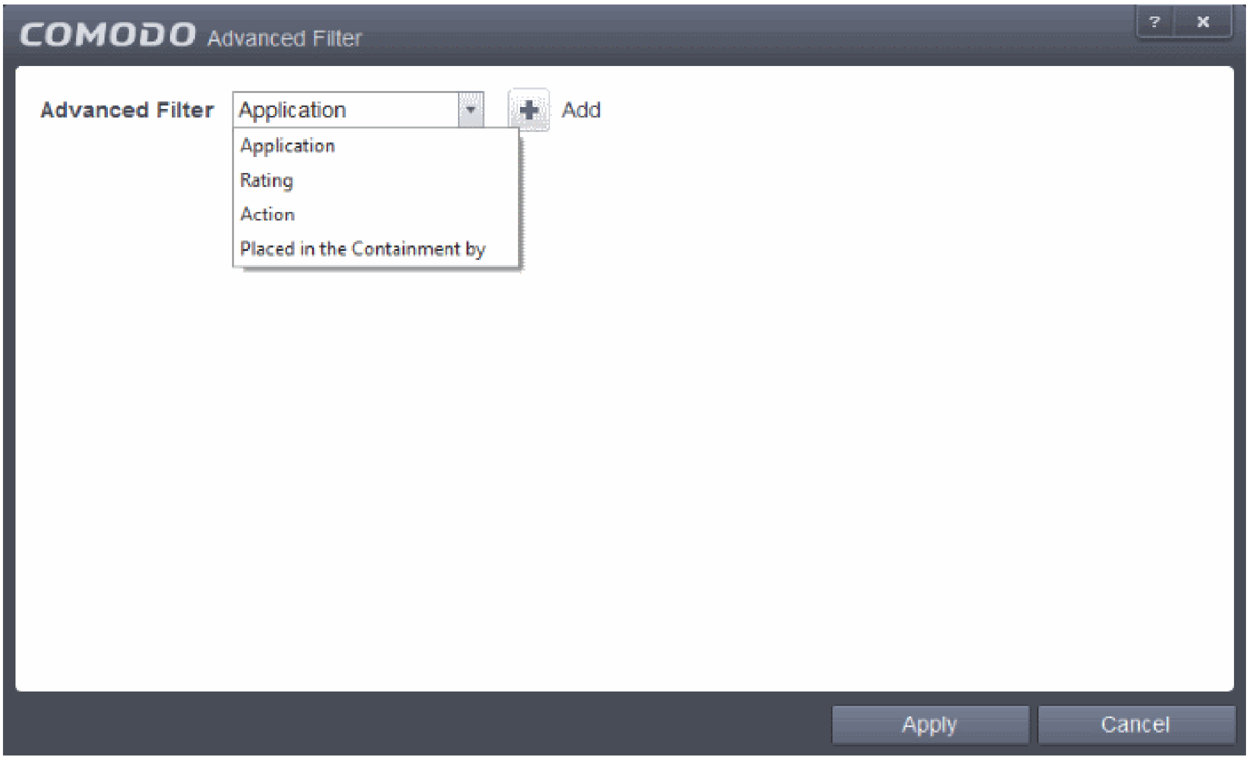
Advanced Filters

You can further refine the displayed events according to specific filters. The following are available for 'Containment' logs:

- **Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used
- **Rating** – Indicates the rating status of application
- **Action** - Indicates the action taken by Containment in response to the event
- **Placed in Containment by** – Indicates which application or process has been placed in containment
- **Alert** - Gives the details of the alert displayed for the event

To configure Advanced Filters for Containment Events

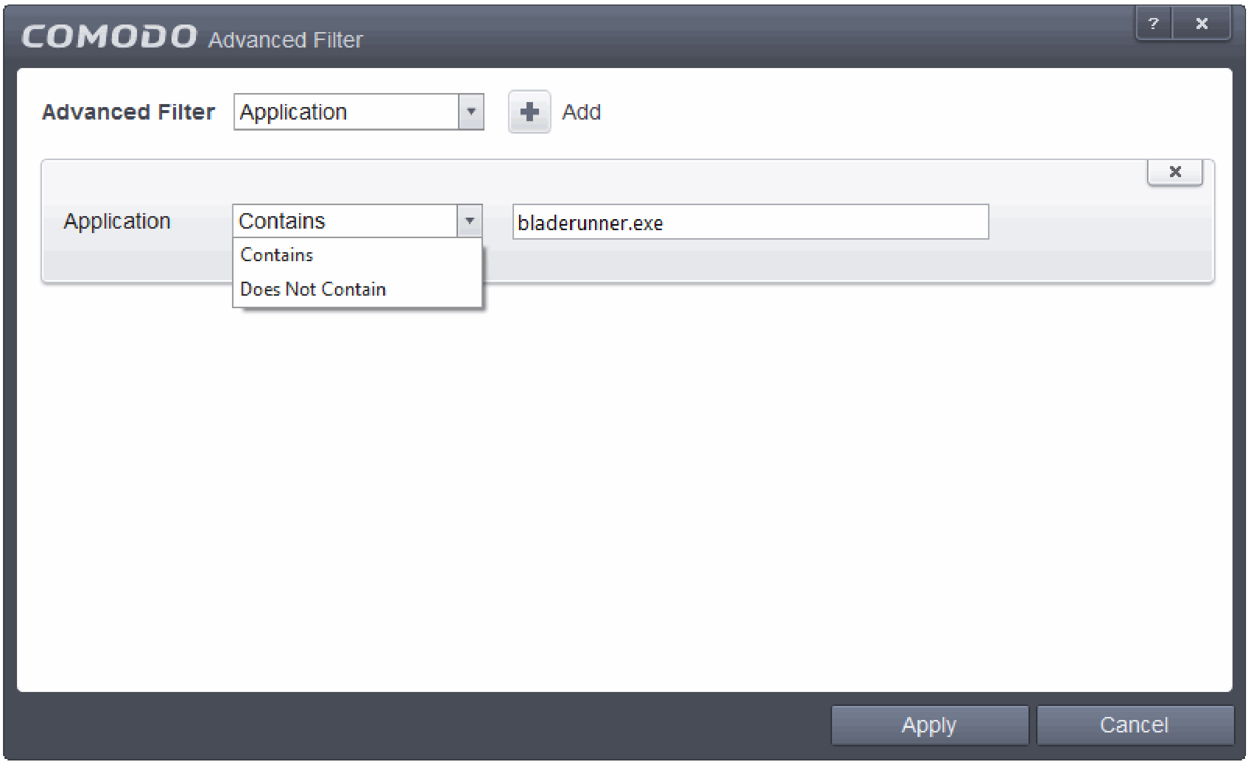
1. Click the funnel button from the title bar. The Advanced Filter interface for 'Containment' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You have 4 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

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

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

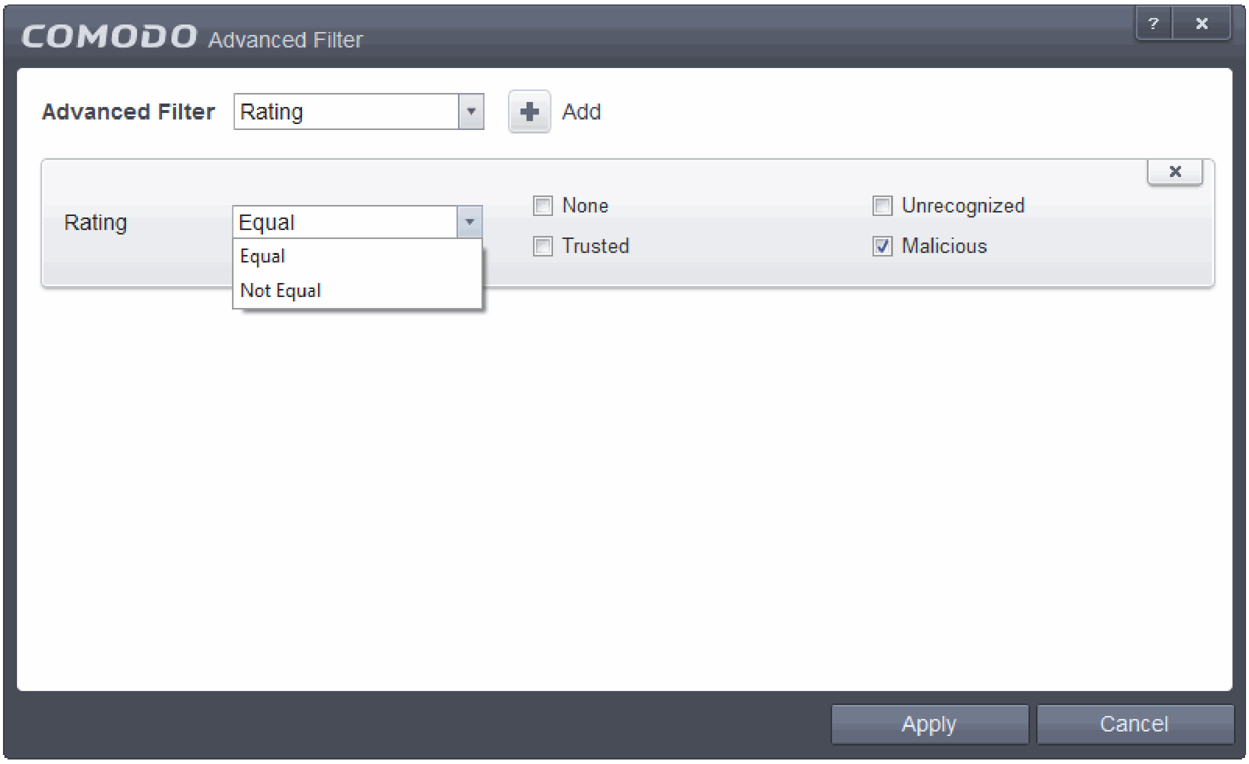


a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b. Enter the text or word that needs to be filtered.

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

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



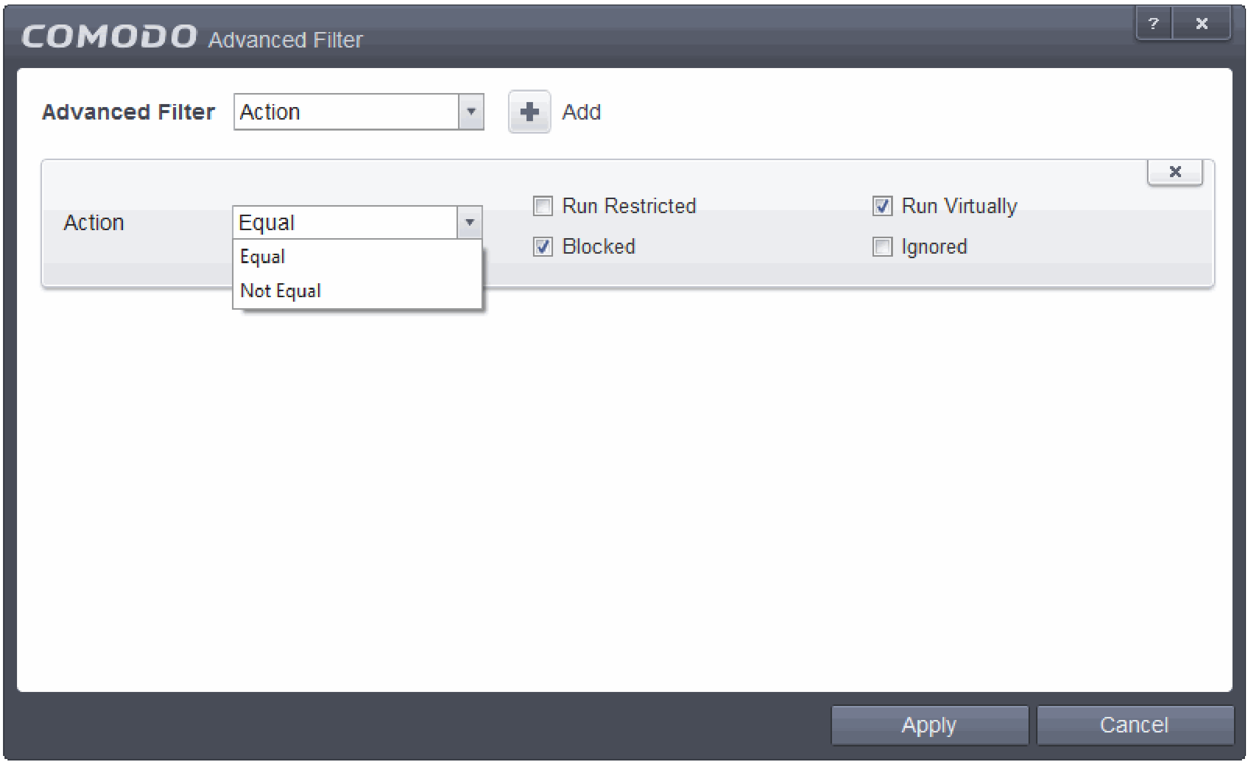
a. Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- None
- Unrecognized
- Trusted
- Malicious

For example, if you select 'Equal' option from the drop-down field and select 'Malicious' from the checkboxes, then only events of applications that are identified as malicious will be displayed. If you select 'Not Equal' option from the drop-down field and checkbox 'Malicious', then all events that do not have the entry 'Malicious' in the 'Rating' column will be displayed. You can select more than one check box options from this interface, as required.

iii. **Action**: The 'Action' option allows you to filter the entries based on privileges that a contained application has to other resources on your computer. Selecting the 'Action' option displays a drop down field and a set of specific filter parameters that can be selected or deselected.



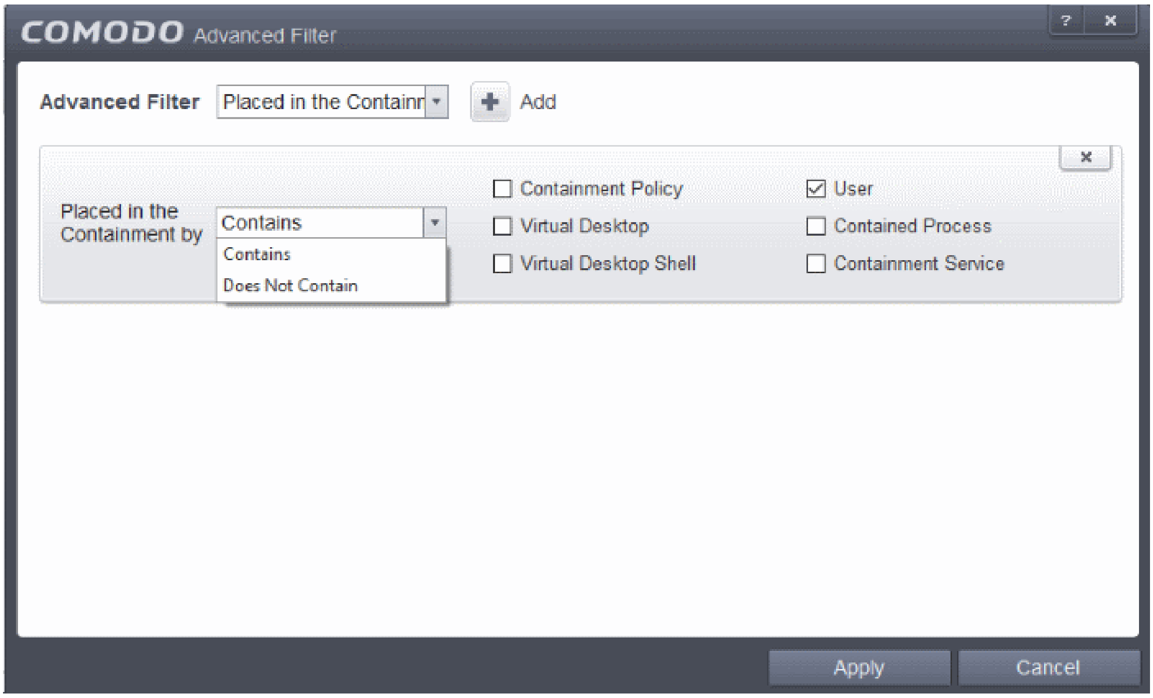
a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

b. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- Run Restricted – Runs in a virtual environment completely isolated from your operating system and files
- Run Restricted - The application is allowed to access very few operating system resources. It is allowed to execute not more than 10 processes at a time and is run with very limited access rights
- Blocked - The application is not allowed to run at all.
- Ignored - The application will not be placed in containment and will be allowed to run normally.

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

iv. **Placed in Containment by**: The 'Placed in Containment by' option allows you to filter the entries based on what placed the application in the container. Selecting the 'Placed in Containment by' option displays a drop down field 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 or word that needs to be filtered. Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- Containment Policy: Displays events where files were contained due to the containment policy.
- User: Displays files that the user placed in containment.
- Virtual Desktop: Displays Virtual desktop files that are placed in containment.
- Contained process: Displays files that are part of a contained process.
- Virtual Desktop Shell: Files placed in containment by the Virtual Desktop Shell.
- Containment Services: Files placed in the container by the containment service.

For example, if you select 'Contains' option from the drop-down field and select 'User' checkbox in the Placed in Containment by, you will see only those Events where Containment Action containing 'User'.

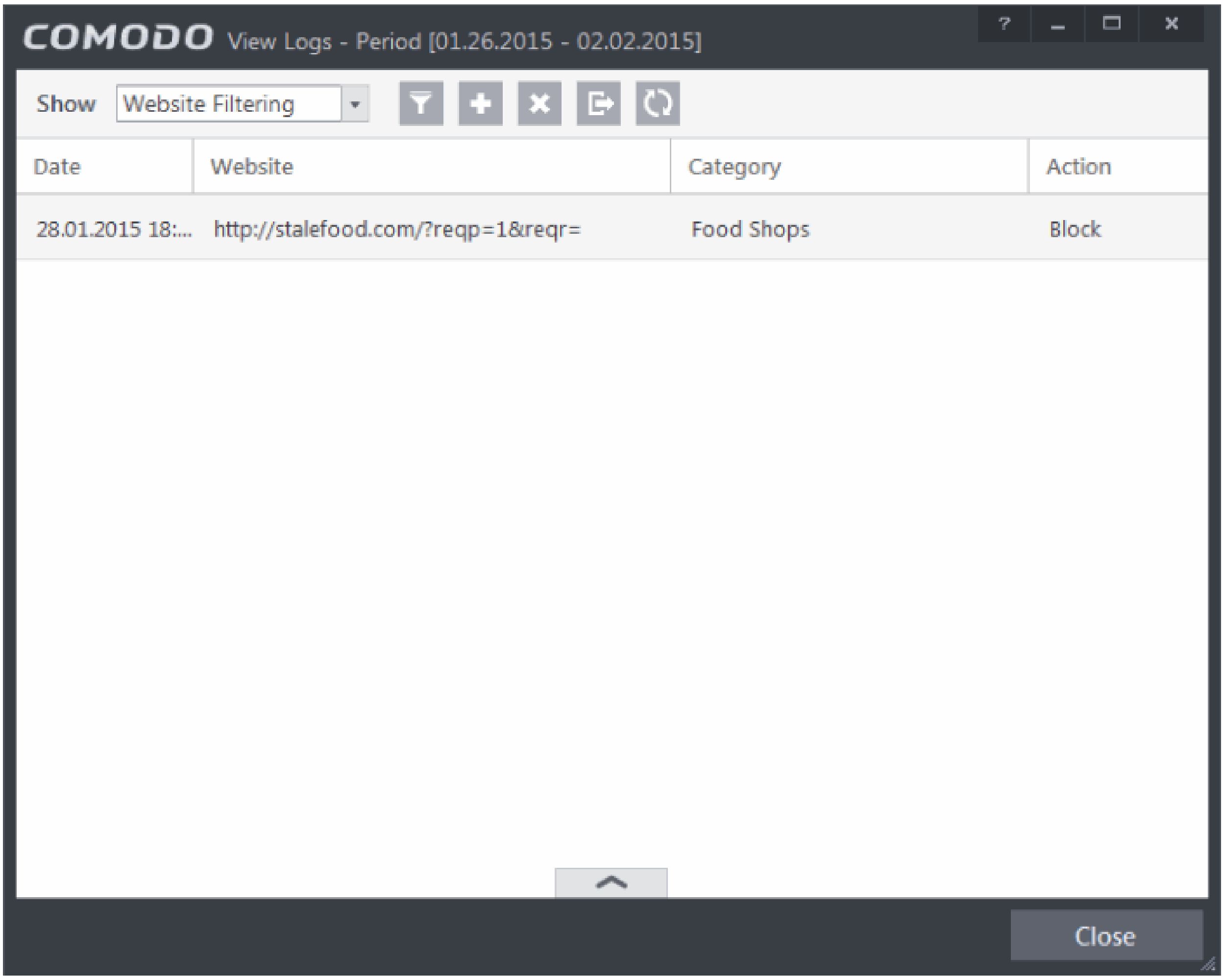
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

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

2.6.6. Website Filtering Logs

Comodo Client Security maintains a log of Websites allowed or blocked to specific users by the 'Website Filter'. You can configure rules to allow or block access to specific websites for particular users of your computer under Advanced Settings > Security Settings > Firewall Settings > Website Filtering. For more details on configuring the Website Filter, refer to the section **Website Filtering**. The Website Filtering log enables you to analyze the attempts made by the other users to access the blocked or allowed websites.

The 'Website Filtering' logs can be viewed by choosing the 'Website Filtering' from the 'Show' drop-down of the log viewer interface.



Date	Website	Category	Action
28.01.2015 18:...	http://stalefood.com/?reqp=1&reqr=	Food Shops	Block

Column Descriptions

1. **Date** - Contains precise details of the date and time of the event.
2. **Website -** Shows the url of the website that was blocked or allowed as per the rules configured in the Website Filtering interface.
3. **Category** - Indicates the predefined category to which the website belongs.
4. **Action -** Indicates whether the access to the website was allowed or blocked to the user.

- To export the 'Website Filtering' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button .
- To refresh the website logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the website logs, click the 'Clear' button

2.6.6.1. Filtering Website Filtering Logs

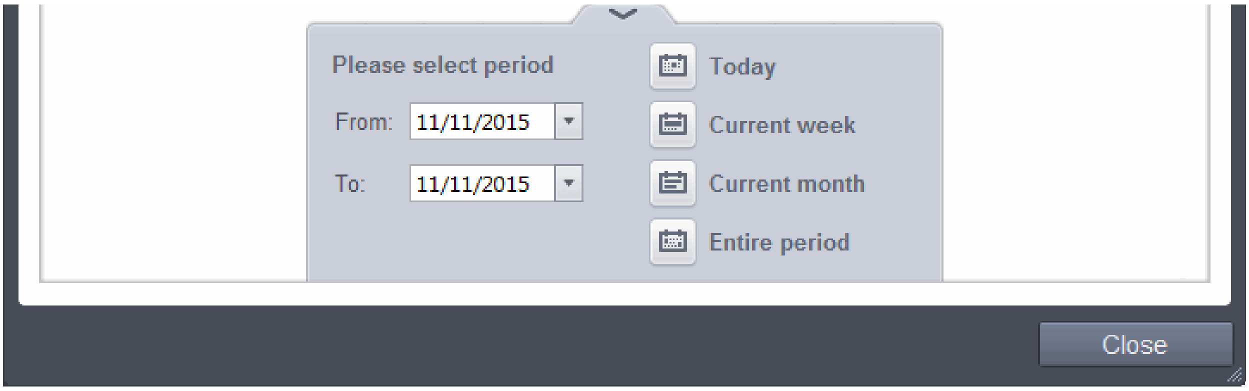
Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters

- Advanced Filters

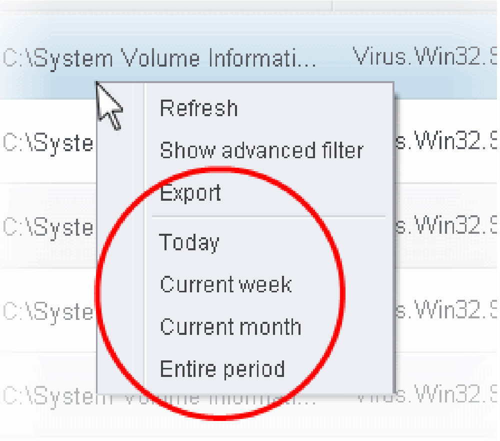
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



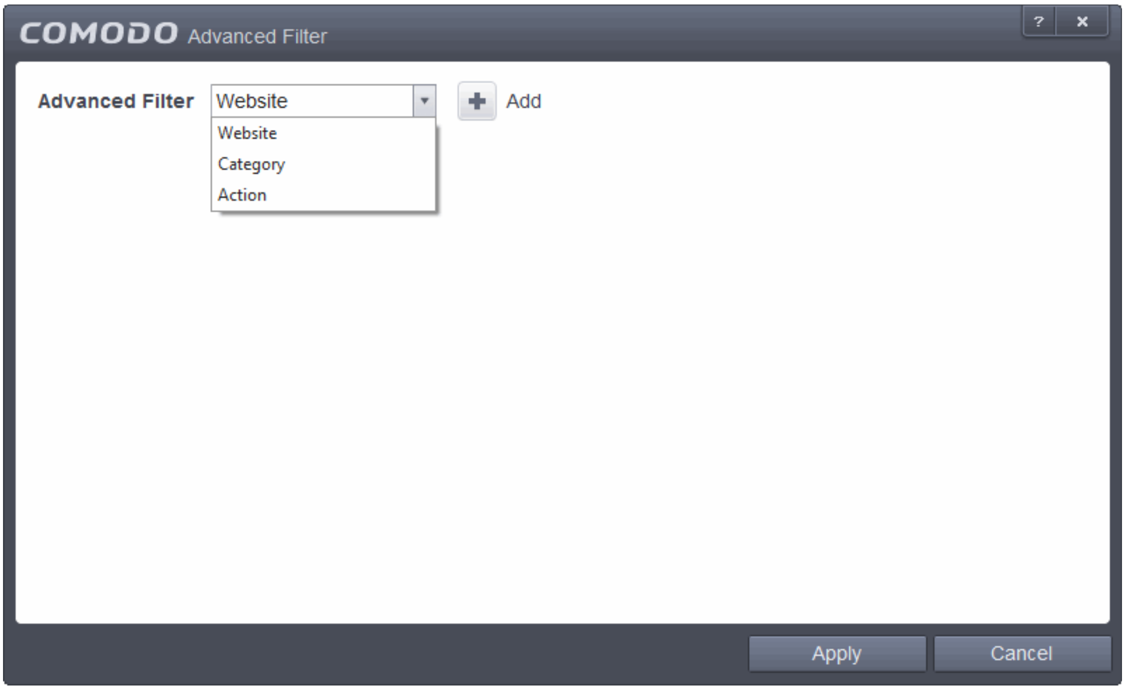
Advanced Filters

Having chosen a preset time filter from the top panel, you can further refine the displayed events according to specific filters. The following filters are available for website logs:

- **Website -** Displays only the events that involve a specific website
- **Category** - Displays only the events that involve attempts to access the websites of the specified category
- **Action -** Displays only the events that involved the specified action

To configure Advanced Filters for Website Filtering events

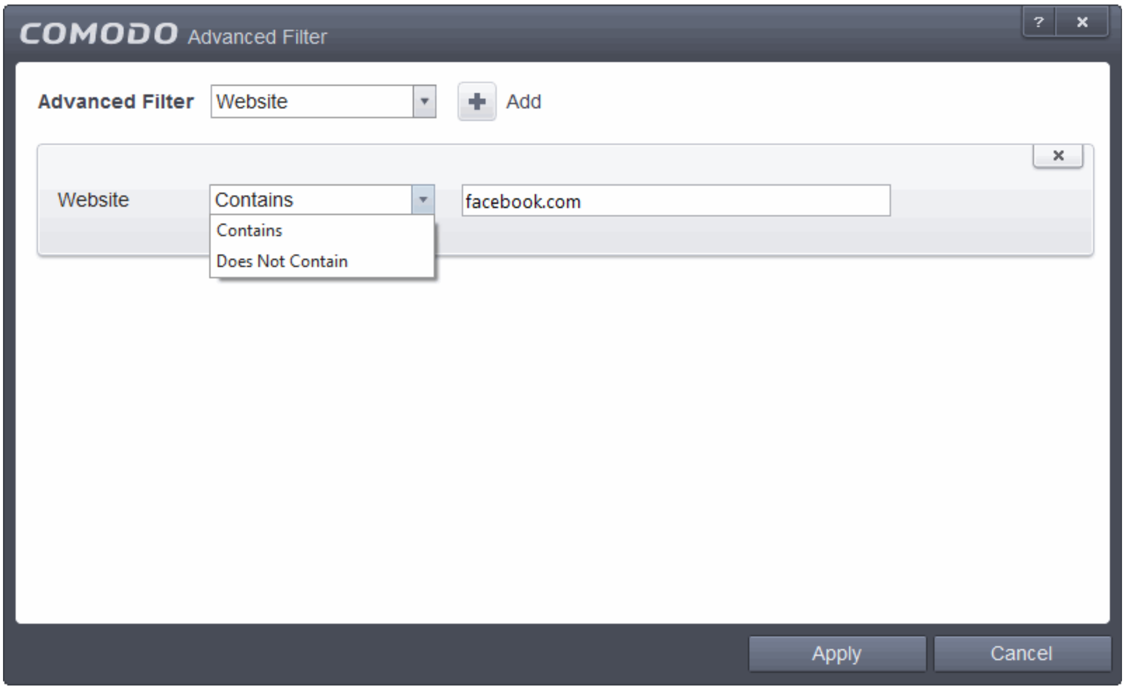
1. Click the funnel button from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Website Filtering' events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add'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



You have 3 categories of filter 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. Following are the options available in the 'Advanced Filter' drop-down:

i. **Website**: Adding the 'Website' option displays a drop-down menu and text entry field.

ii.



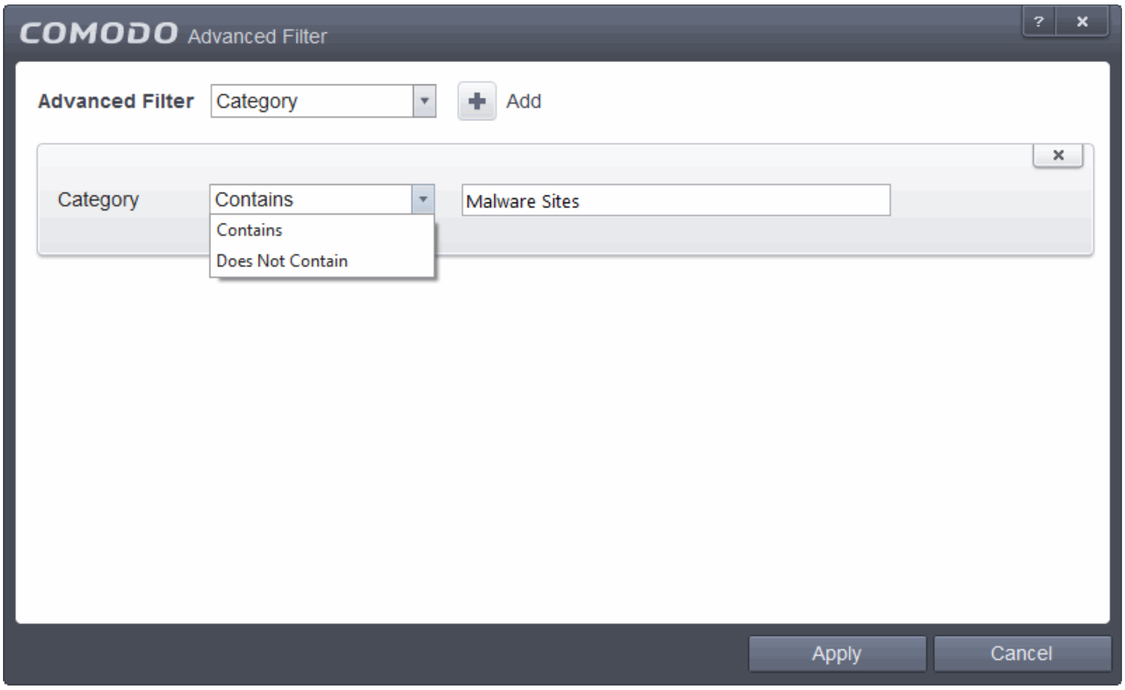
facebook.com

a. Select 'Equal' or 'Not Equal' option from the drop-down menu.

b. Enter the url of the website that needs to be filtered.

For example, if you choose 'Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that involve the website 'facebook.com' in the 'Website' column will be displayed. If you choose 'Not Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that do not involve 'facebook.com' will be displayed.

ii. **Category**: Selecting the 'Category' option displays a drop down menu and text entry field.



Advanced Filter: Category

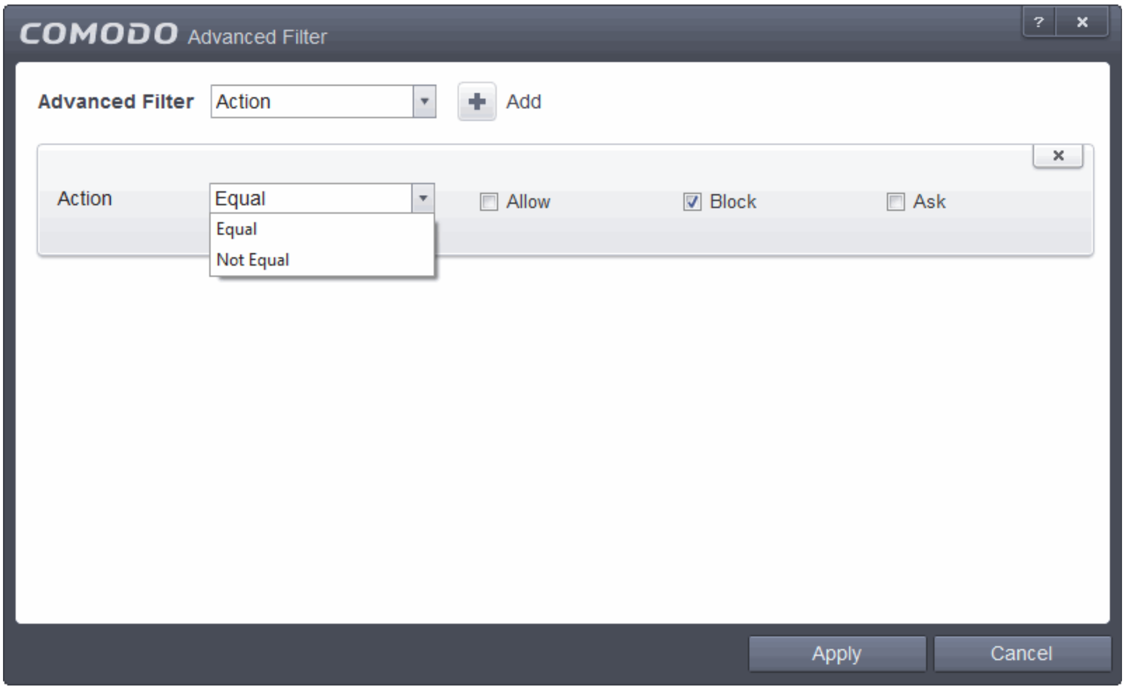
Category: Contains — Malware Sites

a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b. Enter the predefined category of websites that needs to be filtered from the Category column.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Malware Sites' in the text field, then all events that involve the websites falling within the category will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'Malware Sites' in the text field, then all events that do not involve the websites defined within the Malware Sites category will be displayed.

iii. **Action**: Selecting the 'Action' option displays a drop-down menu 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 parameter available are:

- Allow
- Block
- Ask

For example, if you choose 'Equal' option from the drop-down and select 'Block' from the checkboxes, only the events that involve blocking the access to the websites to the users will be displayed. If you choose 'Not Equal' option from the drop-down and select 'Block' check box, all the events that do not involve blocking the websites will be displayed. You can select more than one check box options from this interface, as required.

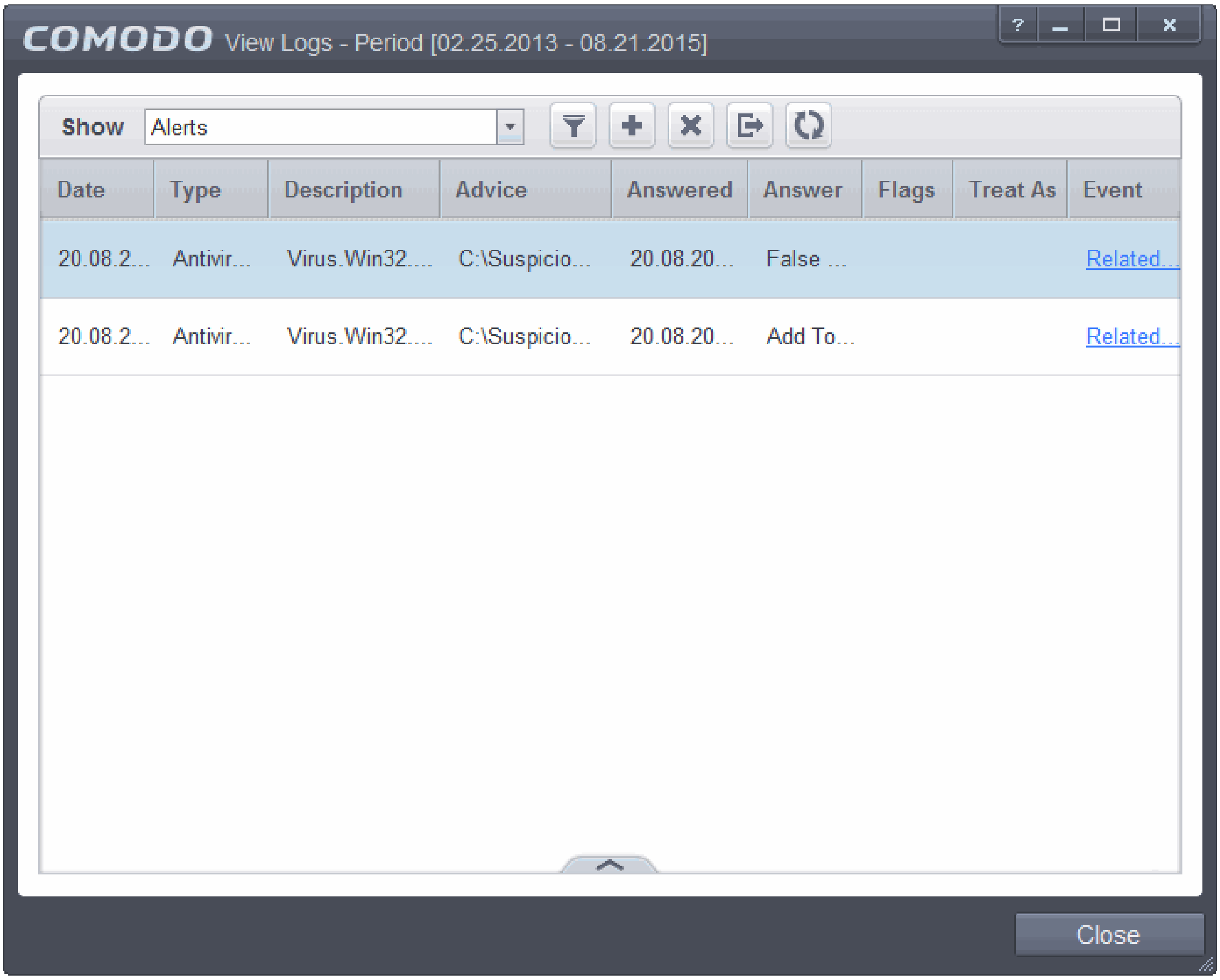
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.7. '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.

The Alerts logs can be viewed by selecting 'Alerts' from the 'Show' drop-down of the log viewer interface.



COMODO View Logs - Period [02.25.2013 - 08.21.2015]

Show: Alerts

Date	Type	Description	Advice	Answered	Answer	Flags	Treat As	Event
20.08.2...	Antivir...	Virus.Win32....	C:\Suspicio...	20.08.20...	False ...			Related...
20.08.2...	Antivir...	Virus.Win32....	C:\Suspicio...	20.08.20...	Add To...			Related...

Column Descriptions

1. **Date** - Contains precise details of the date and time of the alert generation.
2. **Type** - Indicates the type of the alert - Antivirus, Firewall or Advanced Protection (HIPS/Auto-Containment)
3. **Description** - Brief description of the file or the event that triggered the alert.
4. **Advice** - Information offered by CCS on how to respond to the alert.
5. **Answered** - Indicates whether the alert has been answered by the user and if answered, contains precise details of the date and time of response from the user.
6. **Answer** - Indicates the response given by the user.
7. **Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
8. **Treat As** - Based on the response how the file is treated, whether it is treated as a safe application, installer and so on.
9. **Event** - Clicking 'Related Event' opens the details of the event that has triggered the alert.

- To export the Alerts logs as a HTML file click the 'Export' button.
- To open a stored CCS log file, click the 'Open' button ✚.
- To refresh the Alerts logs, click the 'Refresh' button.
- To clear the Alerts logs click the 'Clear' button ✖.

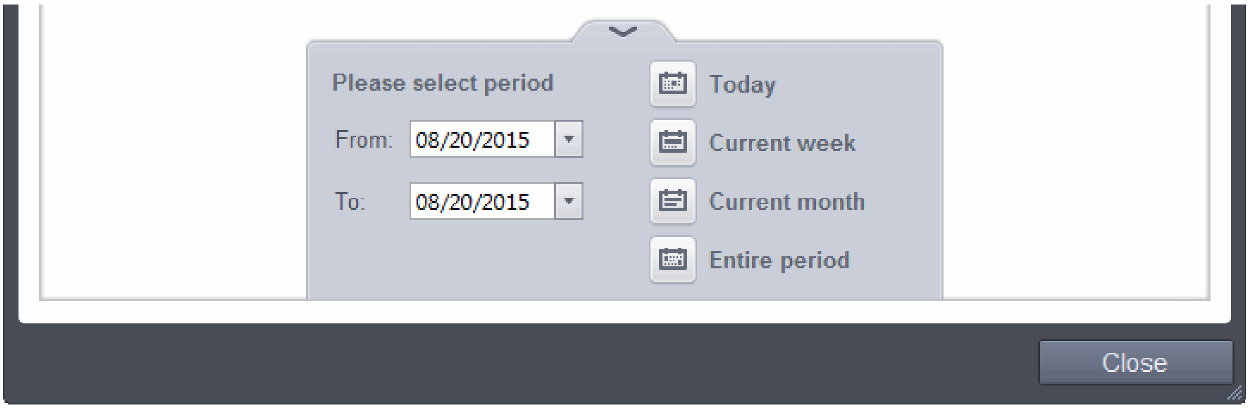
2.6.7.1. Filtering 'Alerts Displayed' Logs

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

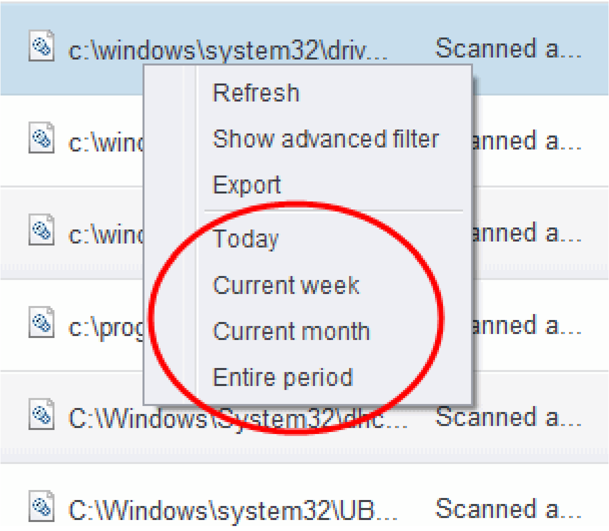
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



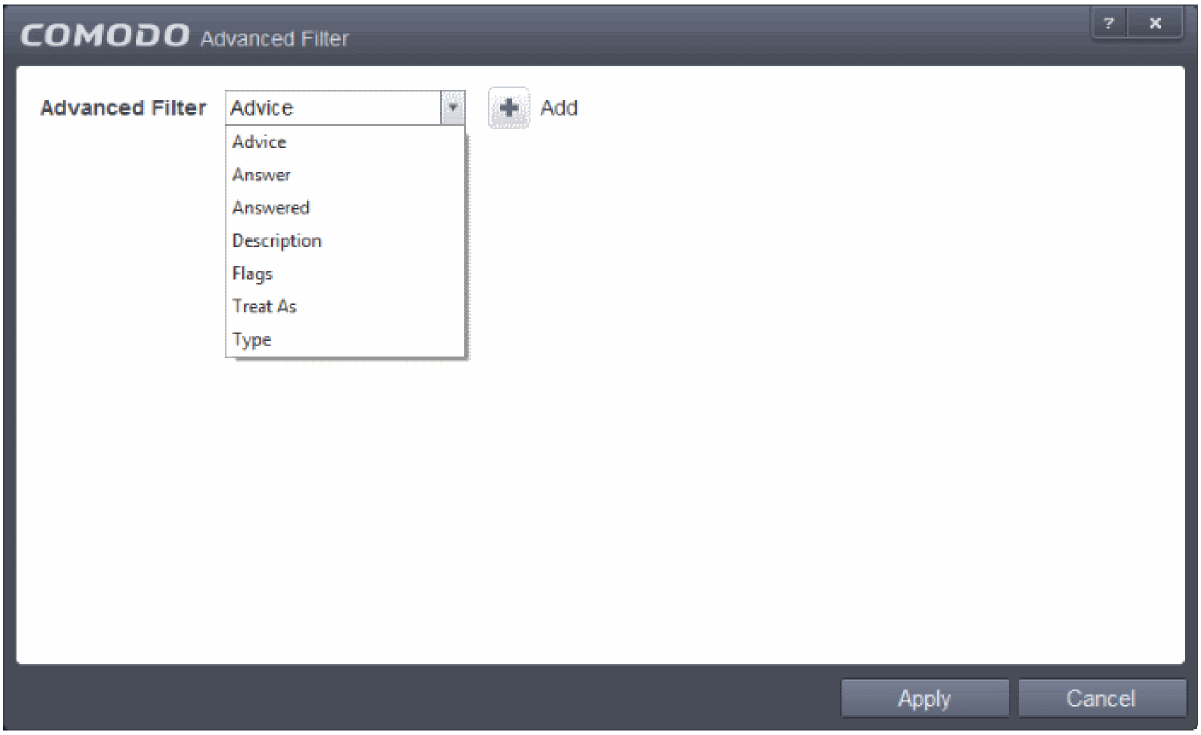
Advanced Filters

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

- **Advice:** Displays only the log of alerts that matches the advice entered
- **Answer:** Displays only the log of alerts that were answered by you with the selected response
- **Answered** Displays only the log of alerts that were answered on a selected date and time
- **Description:** Displays only the log of alerts that matches the description entered
- **Flags:** Displays only the log of alerts based on the selected flags set for the corresponding events
- **Treat As:** Displays only the log of alerts based on their 'Treat As' response you entered in the pop-up alert
- **Type:** Displays only the log of alerts of selected type - Antivirus or Advanced Protection (HIPS/Containment/Auto-Containment).

To configure Advanced Filters for Alerts Displayed

1. Click the funnel button from the title bar. The Advanced Filter interface for 'Alerts' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.

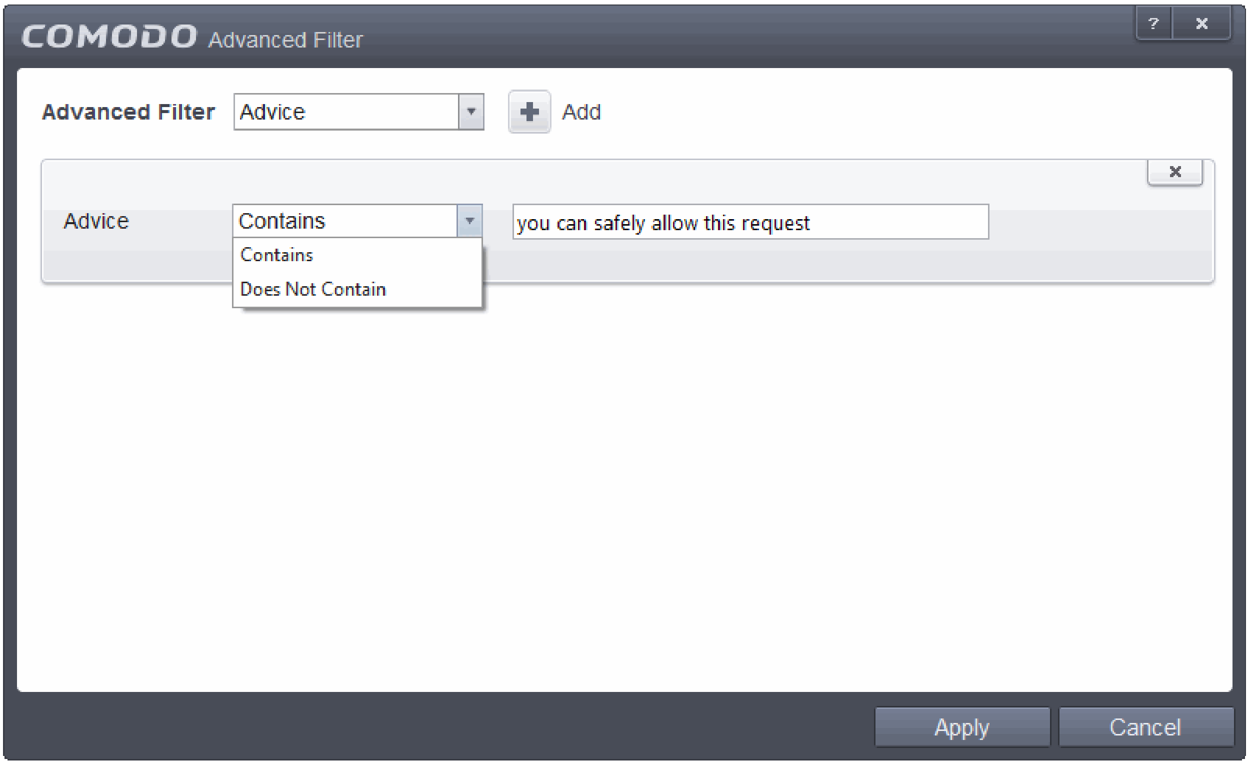


You have 7 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

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

i. **Advice**: The 'Advice' option enables you to filter alerts based on the advice given by CCS in the alert.

Selecting the 'Advice' option displays a drop-down field and text entry field:

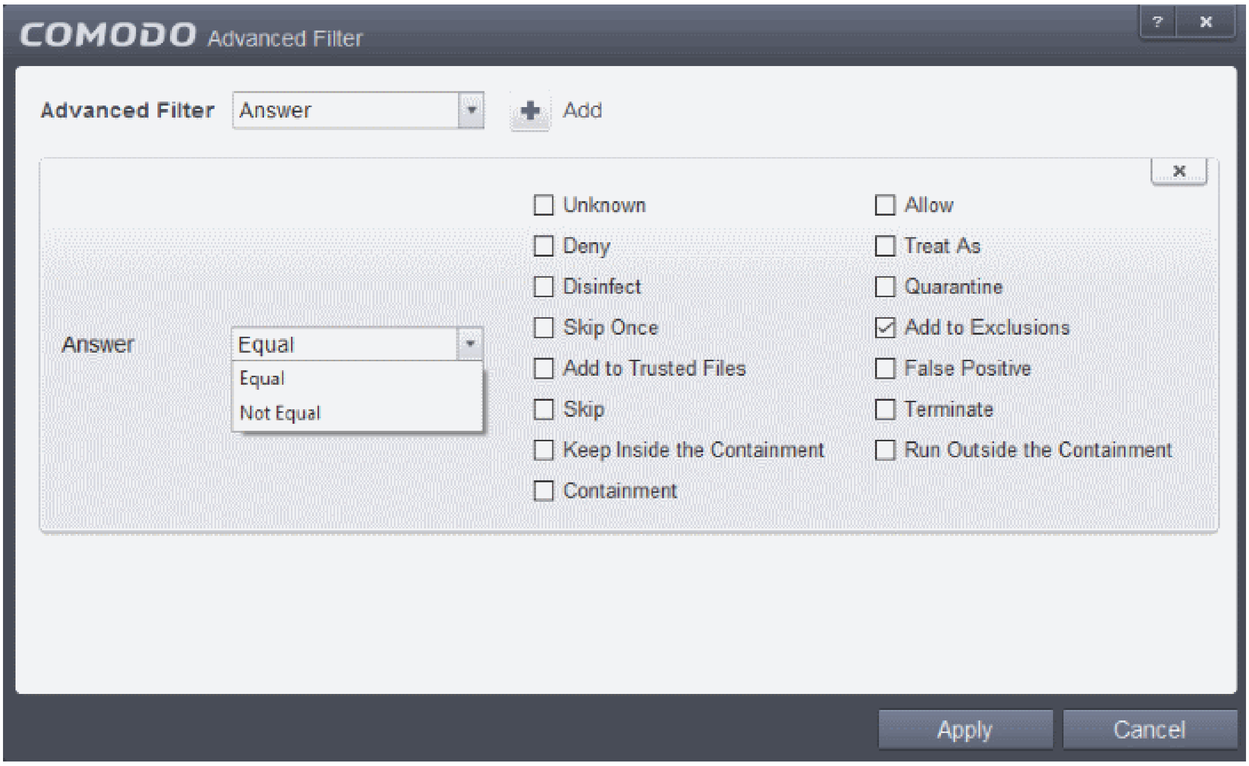


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria.

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

ii. **Answer**: The 'Answer' option enables you to filter the alerts based on how you answered for the alerts. Selecting the 'Answer' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



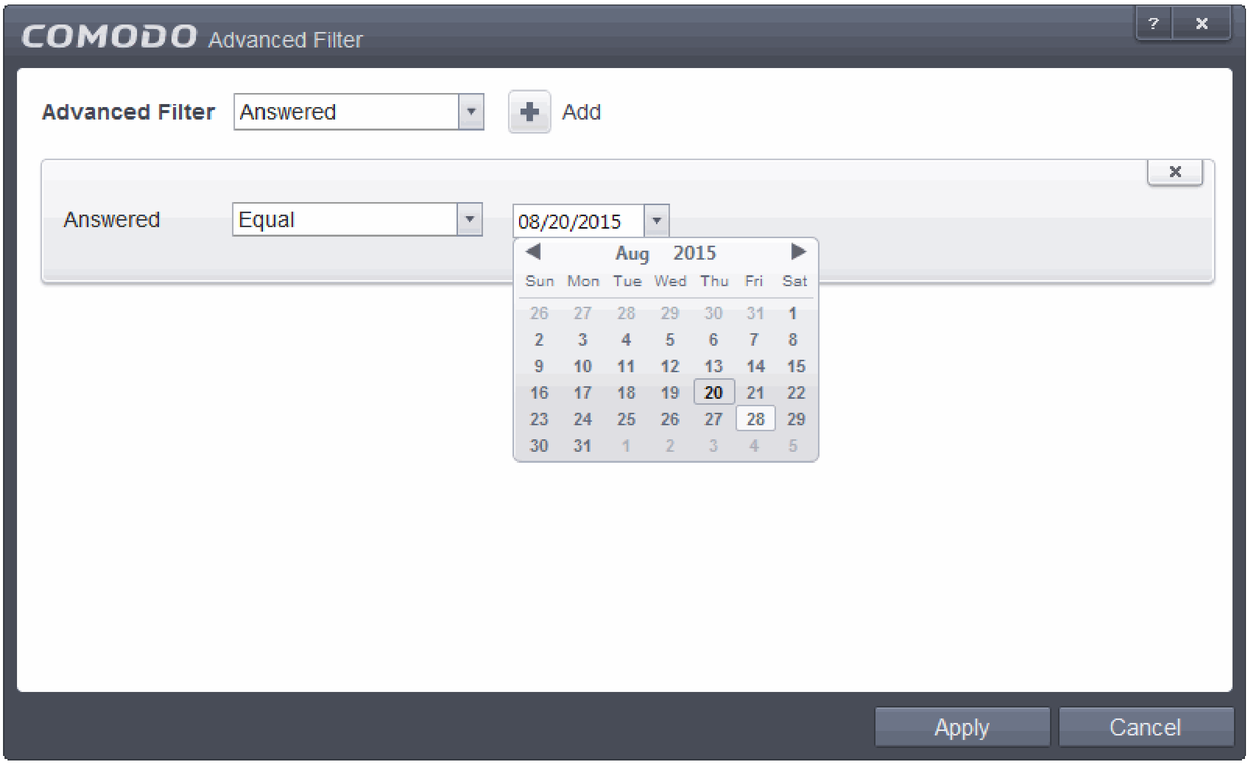
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- Unknown
- Allow
- Deny
- Treat As
- Disinfect
- Quarantine
- Skip Once
- Add to Exclusions
- Add to Trusted Files
- False Positive
- Skip
- Terminate
- Keep Inside the Containment
- Run Outside the Containment
- Containment

For example, if you select 'Equal' from the drop-down and select 'Add to Exclusions' checkbox, only the log of Antivirus alerts for which you answered as 'Ignore' > 'Ignore and Add to Exclusions ' will be displayed.

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



Advanced Filter: Answered

Answered: Equal, 08/20/2015

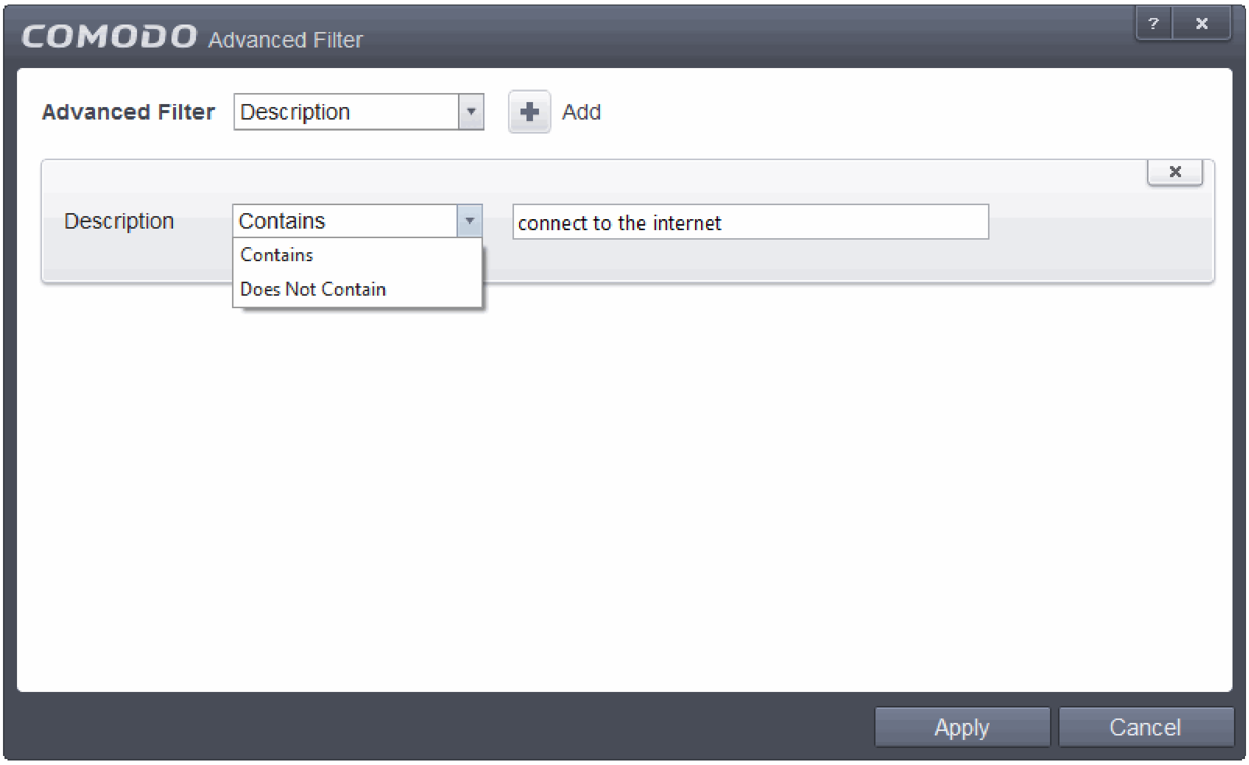
a) Select any one of the following option the drop-down box.

- Equal
- Not Equal

b) Enter the date by selecting it from the calendar displayed by clicking the drop-down arrow.

For example, if you select 'Equal' from the drop-down and select '08/20/2015', only the log of alerts answered on 08/20/2015 will be displayed.

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

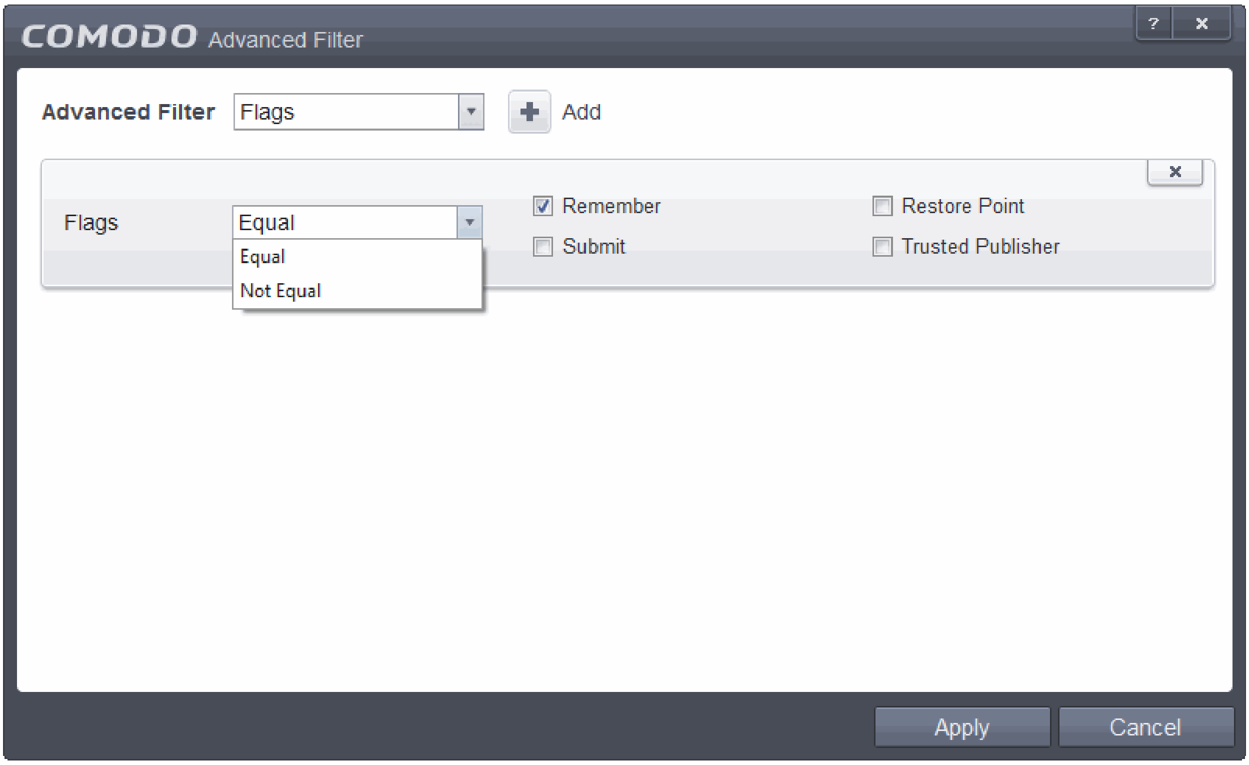


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the 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 containing the phrase alerts 'connect to the Internet' in the description, will be displayed.

v. **Flags**: The 'Flags' option enables you filter the entries based on the flags set for the kinds of actions against the event triggered by the file. Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.

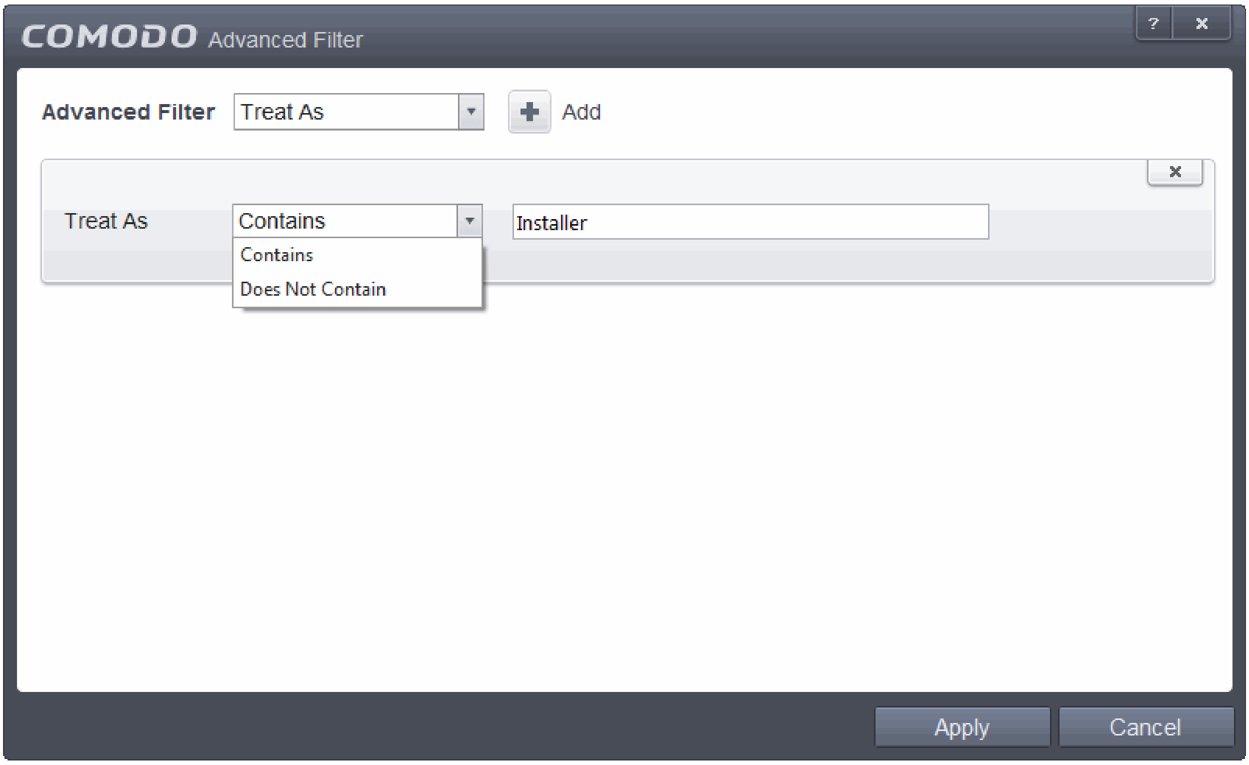


a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- Remember
- Restore Point
- Submit
- Trusted Publisher

vi. **Treat As**: The 'Treat As' enables you to filter the log entries based on their 'Treat As' response you entered in the pop-up alert. Selecting the 'Treat As' option displays a drop-down menu and text entry field.

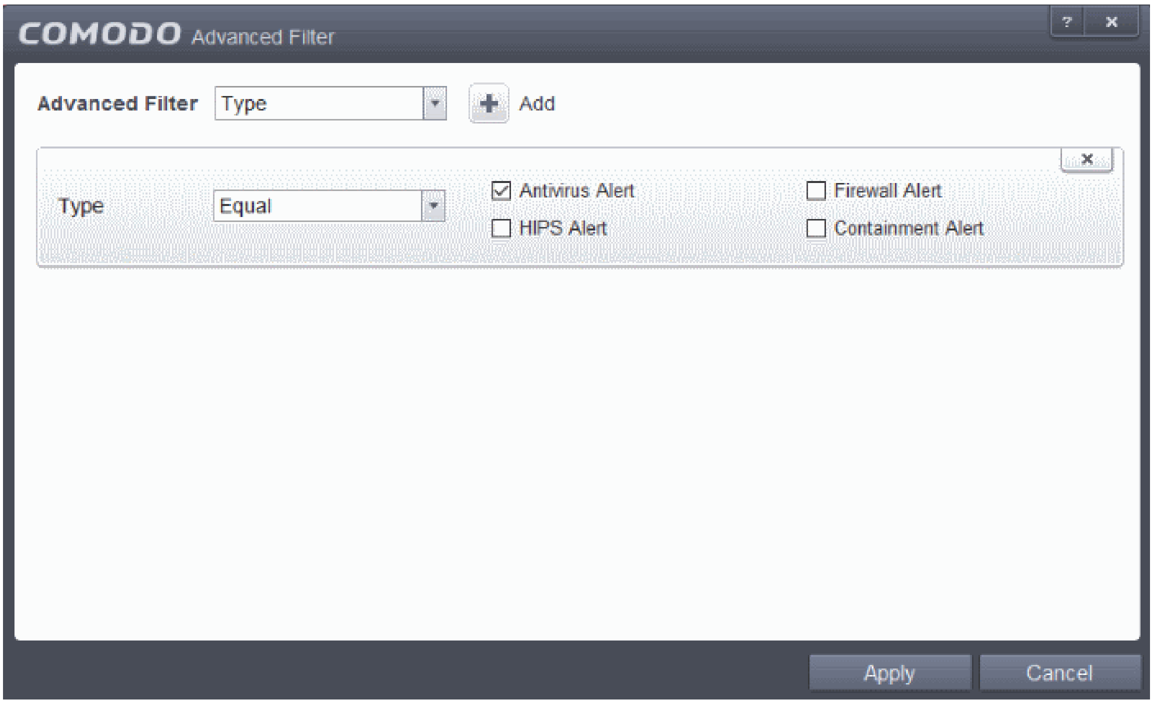


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the 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 entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.

vii. **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 a set of specific alert 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 specific filter parameters to refine your search. The parameters available are:

- Antivirus Alert
- Firewall Alert
- HIPS Alert
- Containment Alert

For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, the logs of Antivirus Alerts alone will be displayed.

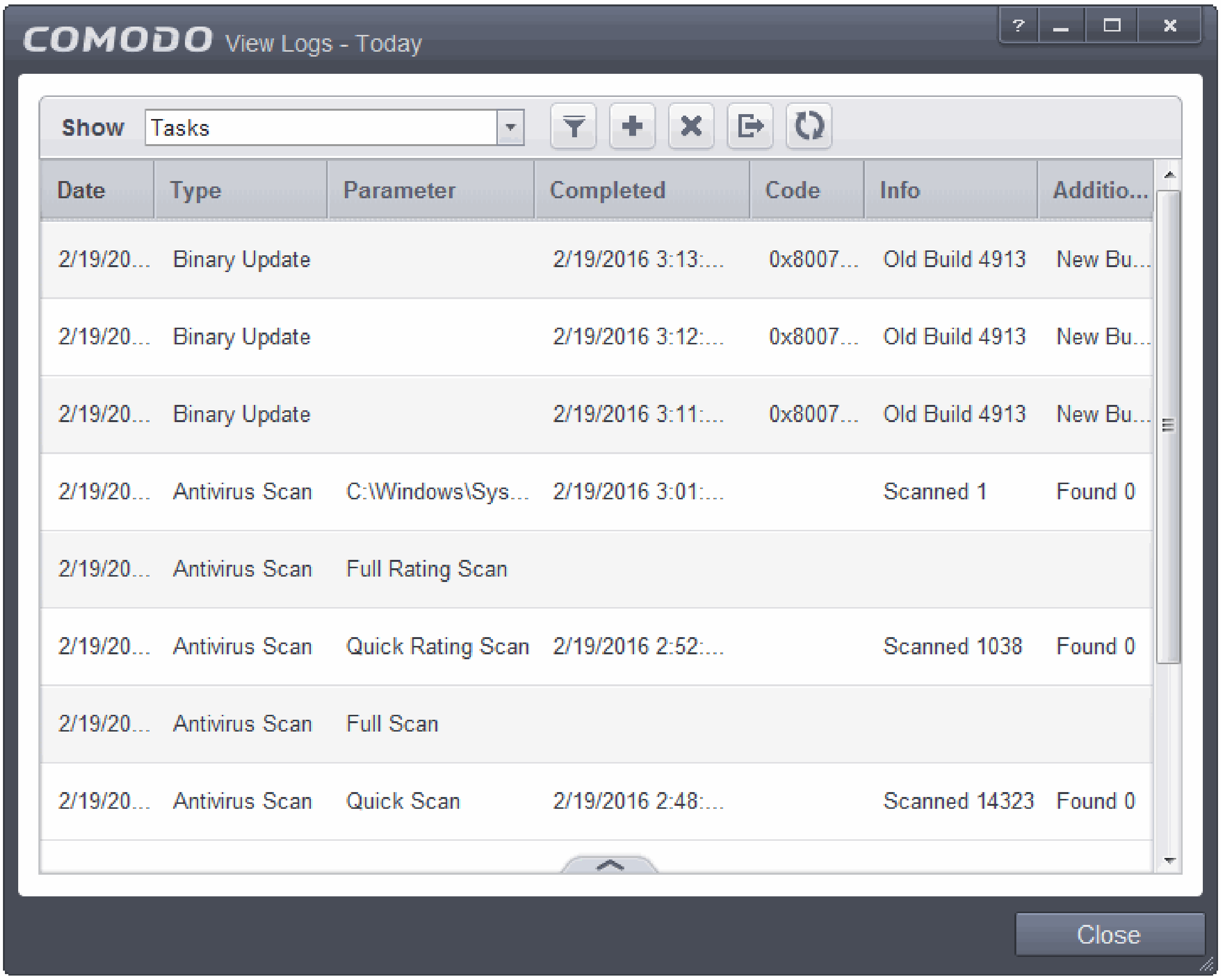
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the '**X**' button at the top right of the filter pane.

- 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.

2.6.8. Tasks

Comodo Client Security records a history of all the CCS tasks like virus signature database updates, scans run and so on. The 'Tasks Launched' log window displays a list of tasks launched at various time points with their completion status and other details.

The 'Tasks' logs can be viewed by selecting 'Tasks' from the 'Show' drop-down of the log viewer interface.



Show: Tasks

Date	Type	Parameter	Completed	Code	Info	Additio...
2/19/20...	Binary Update		2/19/2016 3:13:...	0x8007...	Old Build 4913	New Bu...
2/19/20...	Binary Update		2/19/2016 3:12:...	0x8007...	Old Build 4913	New Bu...
2/19/20...	Binary Update		2/19/2016 3:11:...	0x8007...	Old Build 4913	New Bu...
2/19/20...	Antivirus Scan	C:\Windows\Sys...	2/19/2016 3:01:...		Scanned 1	Found 0
2/19/20...	Antivirus Scan	Full Rating Scan				
2/19/20...	Antivirus Scan	Quick Rating Scan	2/19/2016 2:52:...		Scanned 1038	Found 0
2/19/20...	Antivirus Scan	Full Scan				
2/19/20...	Antivirus Scan	Quick Scan	2/19/2016 2:48:...		Scanned 14323	Found 0

Column Descriptions

1. **Date** - Contains precise details of the date and time when the task is launched.
2. **Type -** Indicates the type of the task.
3. **Parameter -** Indicates the parameter (like scan type) associated with the task.
4. **Completed -** Contains precise details of the date and time of the completion of the task.
5. **Code** - Indicates the code of the task as assigned by CCS.
6. **Info & Additional Info -** Provides additional information of the task.

- To export the Tasks logs as a HTML file, click the 'Export' button .
- To open a stored CCS log file, click the 'Open' button ✚.
- To refresh the Tasks logs, click the 'Refresh' button .
- To clear the Tasks logs, click the 'Clear' button ✖.

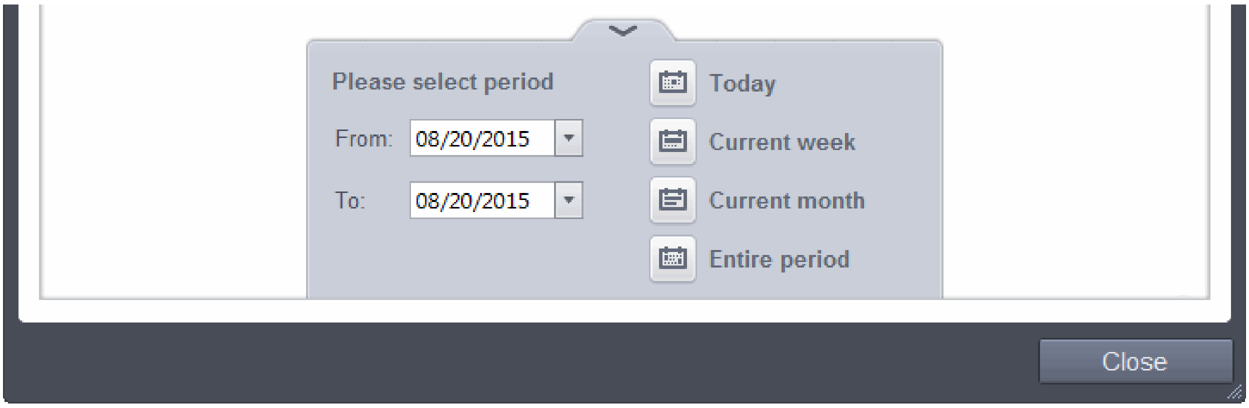
2.6.8.1. Filtering 'Tasks Launched' Logs

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

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:

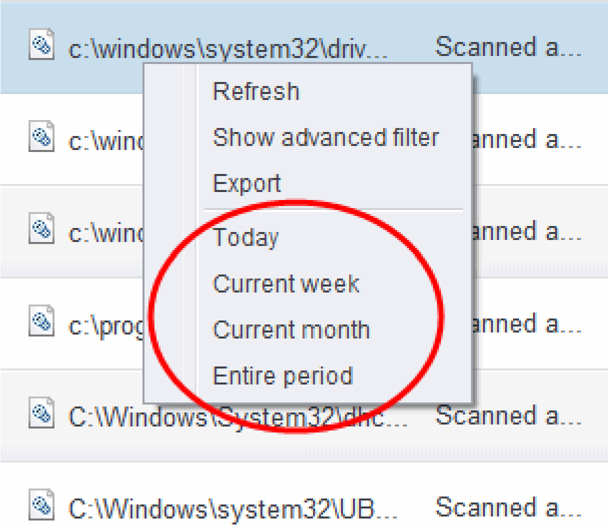

Please select period

From: 08/20/2015

To: 08/20/2015

- **Today** - Displays all logged tasks for today.
- **Current Week** - Displays all logged tasks during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged tasks during the month that holds the current date.
- **Entire Period** - Displays every task logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



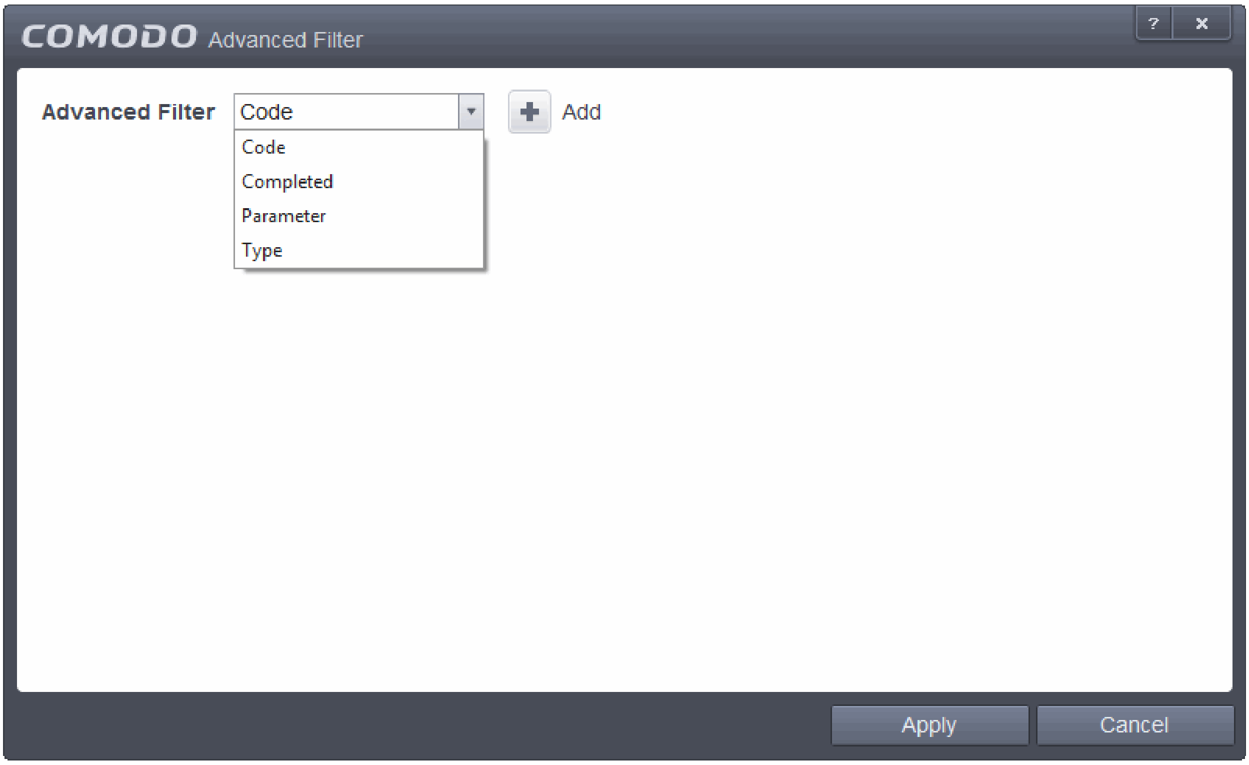
Advanced Filters

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

- **Code** - Displays the tasks based on the code value entered
- **Completed** - Displays tasks completed on the specified date.
- **Parameter** - Displays only the tasks launched that include the selected parameter, like scan profile or the locations scanned during custom scans.
- **Type** - Displays only the selected type of task launched. These can be an AV Update, AV Scan, Clearing logs and Guarantee Activation.

To configure Advanced Filters for 'Tasks' logs

1. Click the funnel button from the title bar. The Advanced Filter interface for Tasks log viewer will open.

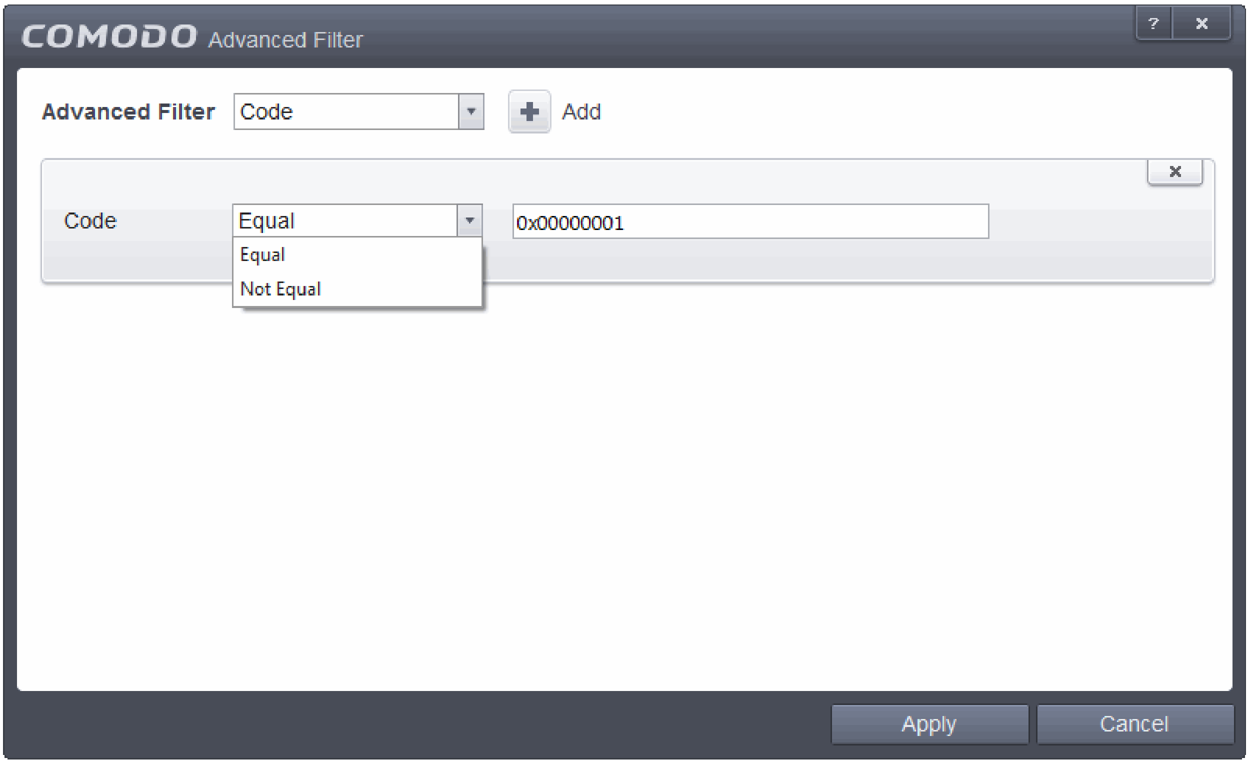


2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.

   You can chose the category of filter from a drop down box. 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.

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

   i. **Code**: The Code option enables you to filter the tasks based on their code value. Selecting the 'Code' option displays a drop-down field and text entry field.

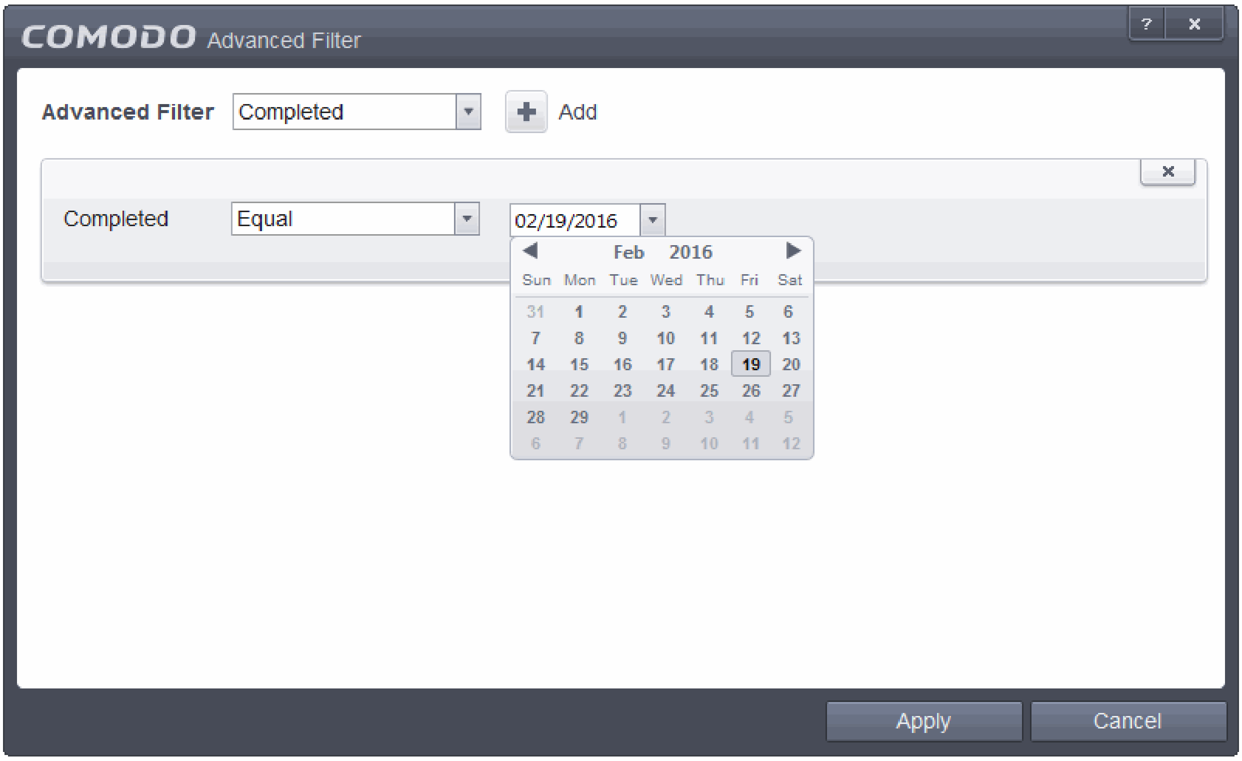


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Enter the code or a part of it as your filter criteria in the text field.

For example if you have chosen 'Equal' from the drop-down and entered '0x00000001' in the text field, then only the log entries with the value 0x00000001 in the code column will be displayed.

ii. **Completed**: The 'Completed' option enables you to filter the log entries based on the completion dates of the Tasks. Selecting the 'Completed' option displays a drop-down box and date entry field.



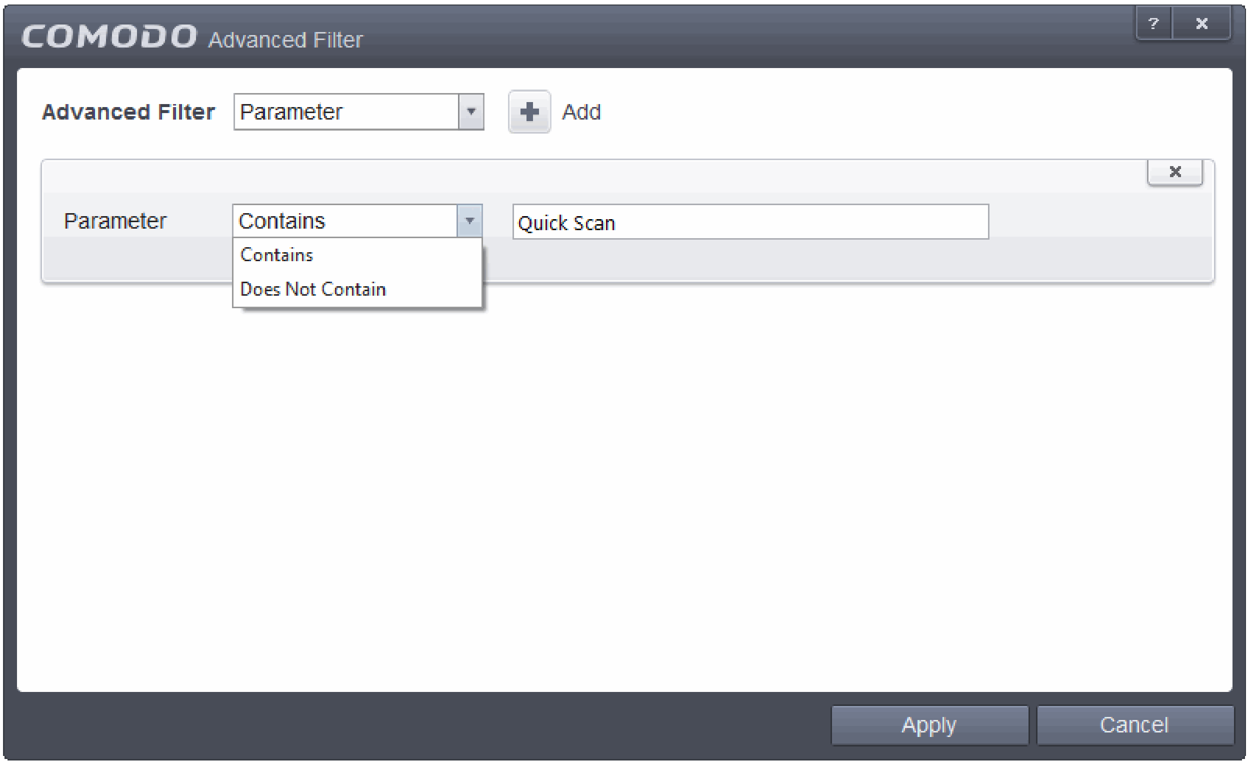
a) Select any one of the following option the drop-down box.

- Equal
- Not Equal

b) Enter the date by selecting it from the calendar displayed by clicking the drop-down arrow.

For example, if you select 'Equal' from the drop-down and select '02/19/2015 ', only the log of Tasks completed on 02/19/2015 will be displayed.

iii. **Parameter**: The Parameter option enables you to filter the entries based on the parameters like scan locations, associated with the Task. Selecting the 'Parameter' option displays a drop-down field and text entry field.

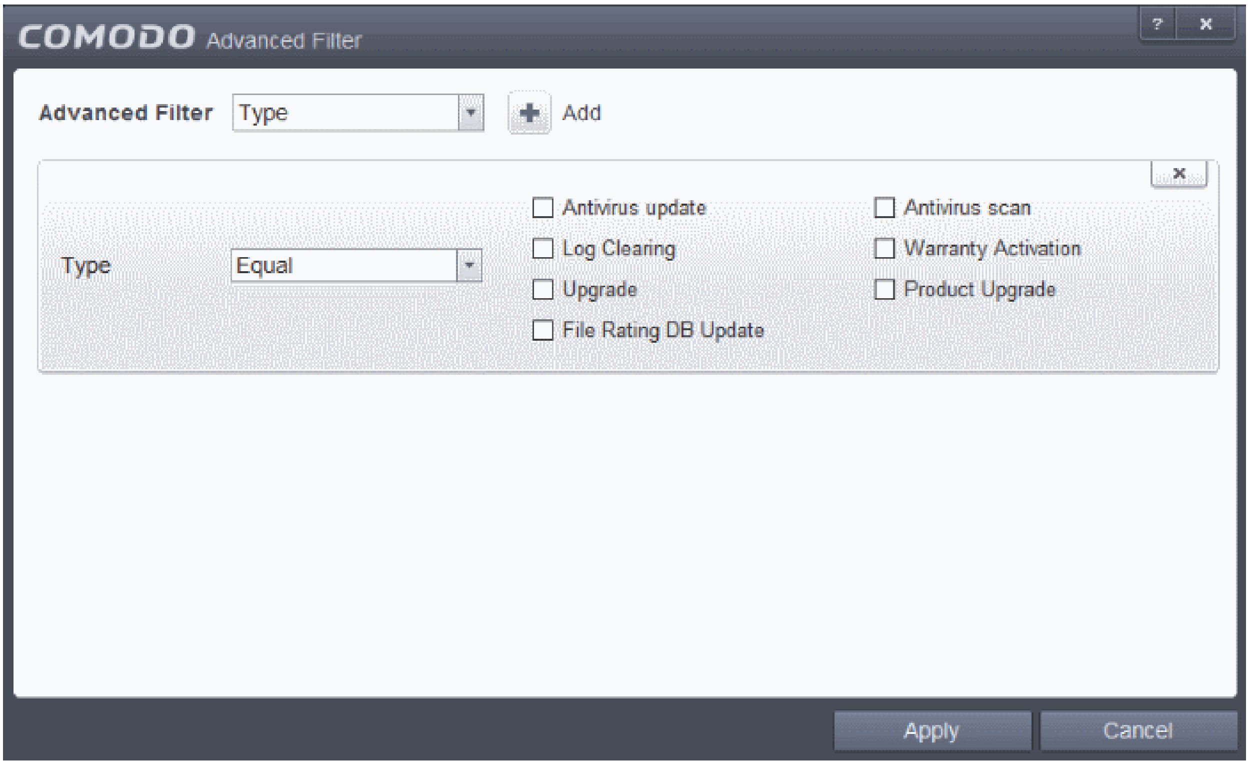


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the text or word as your filter criteria.

For example, if you select 'Contains' option from the drop-down field 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**: The 'Type' option enables you to filter the entries based on the type of Tasks launched. Selecting the 'Type' option displays a drop down menu 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:

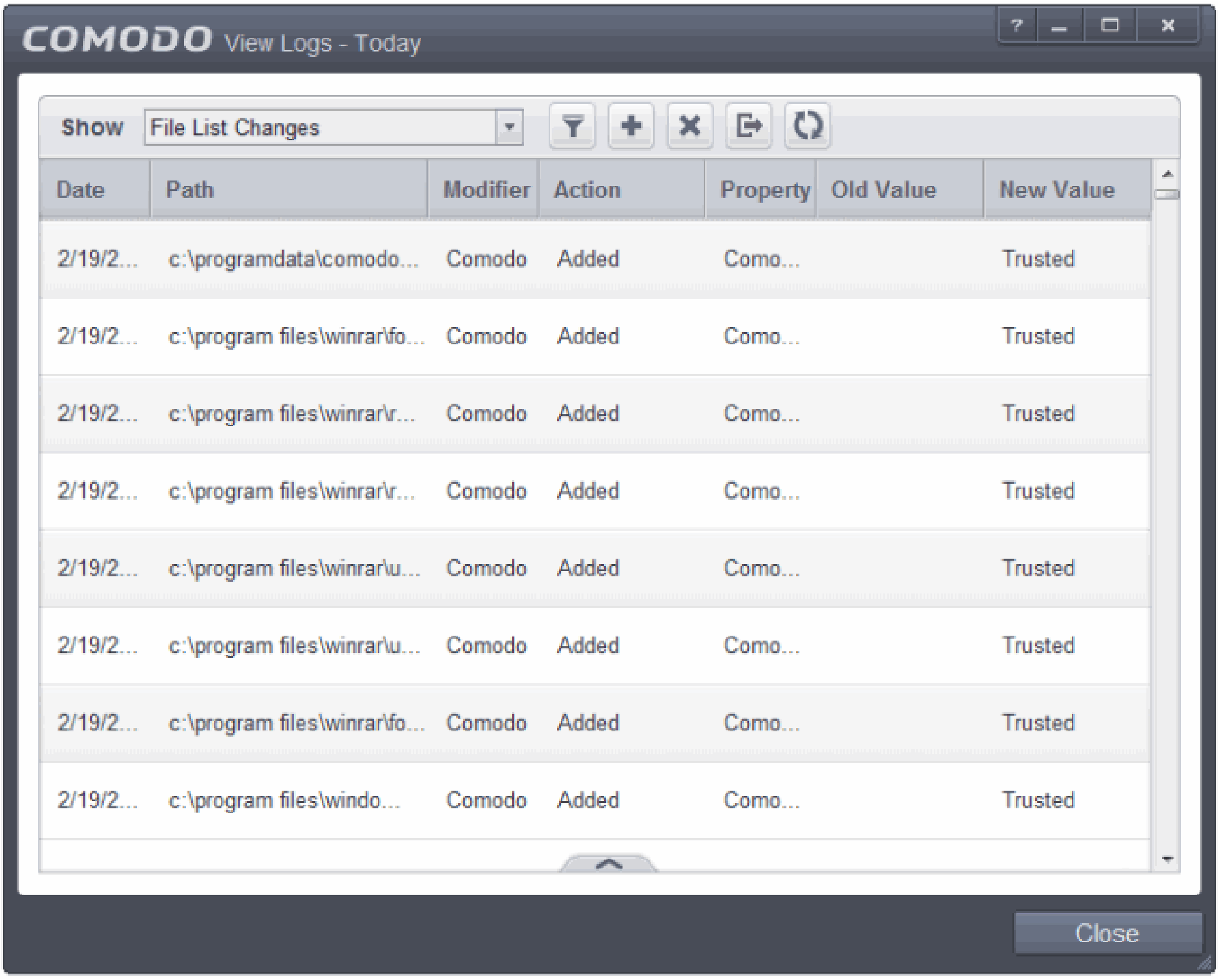
- Antivirus Update
- Antivirus Scan
- Log Clearing
- Warranty Activation
- Upgrade
- Product Upgrade
- File Rating DB Update

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.

2.6.9. File List Changes Logs

The 'File List Changes' logs is a record of all changes made by CCS to endpoint files.



Date	Path	Modifier	Action	Property	Old Value	New Value
2/19/2...	c:\programdata\comodo...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\winrar\fo...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\winrar\r...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\winrar\r...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\winrar\u...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\winrar\u...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\winrar\fo...	Comodo	Added	Como...		Trusted
2/19/2...	c:\program files\windo...	Comodo	Added	Como...		Trusted

'File List Changes' logs can be viewed by selecting 'File List Changes' from the 'Show' drop-down of the log viewer interface.

Column Descriptions

1. **Date** - Contains precise details of the date and time when the changes were made
2. **Path -** Indicates the path or the of executable files, programs and applications
3. **Modifier -** Indicates the user that has made the file change
4. **Action -** Indicates the action taken by File List Changes in response to the event
5. **Property** – Indicates the current rating of the file as per the analysis result from Comodo.
6. **Old Value** – Displays the old value of the files, programs and applications
7. **New Value -** Displays the new value of the files, programs and applications

- To export the 'File List Changes' logs as a HTML file, click the 'Export' button .
- To open a stored CCS log file, click the 'Open' button.
- To refresh the File List Changes logs, click the 'Refresh' button .
- To clear the File List Changes logs, click the 'Clear' button .

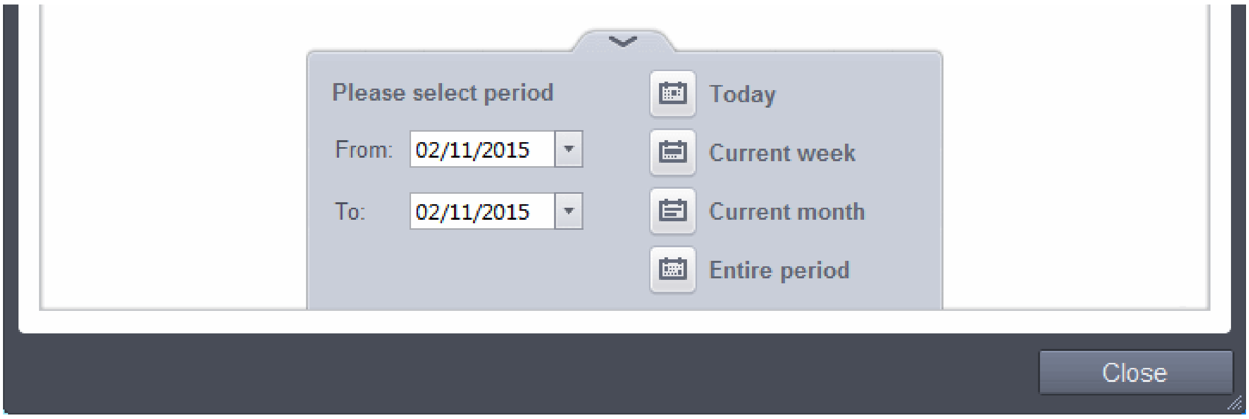
2.6.9.1. Filtering 'File List Changes' Logs

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

- Preset Time Filters
- Advanced Filters

Preset Time Filters:

Clicking on the handle at the bottom enables you to filter the logs for a selected time period:

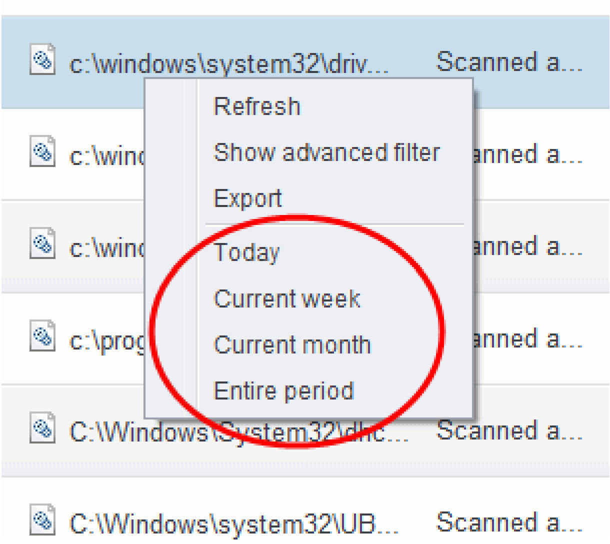


- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have

cleared the log history since installation, this option shows all logs created since that clearance).

- **Custom Filter** – Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'.

Alternatively, you can right click inside the log viewer module and choose the time period.



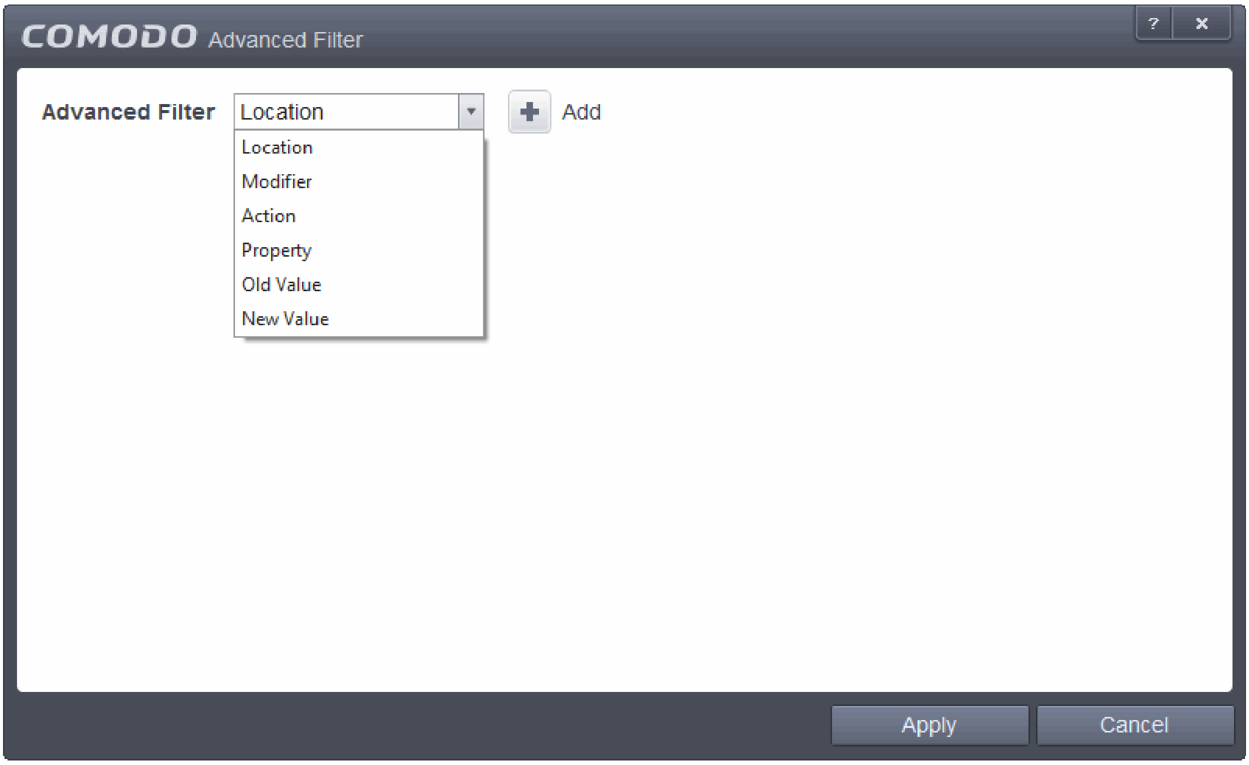
Advanced Filters

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

- **Location -** Displays only the events logged from a specific location
- **Modifier:** Indicates the user that has made the file change
- **Action** - Indicates the action taken by File List Changes in response to the event
- **Property** – Indicates the current rating of the file as per the analysis result from Comodo.
- **Old Value** – Displays the old value of the files, programs and applications
- **New Value** - Displays the new value of the files, programs and applications

To configure Advanced Filters for File List Changes Logs

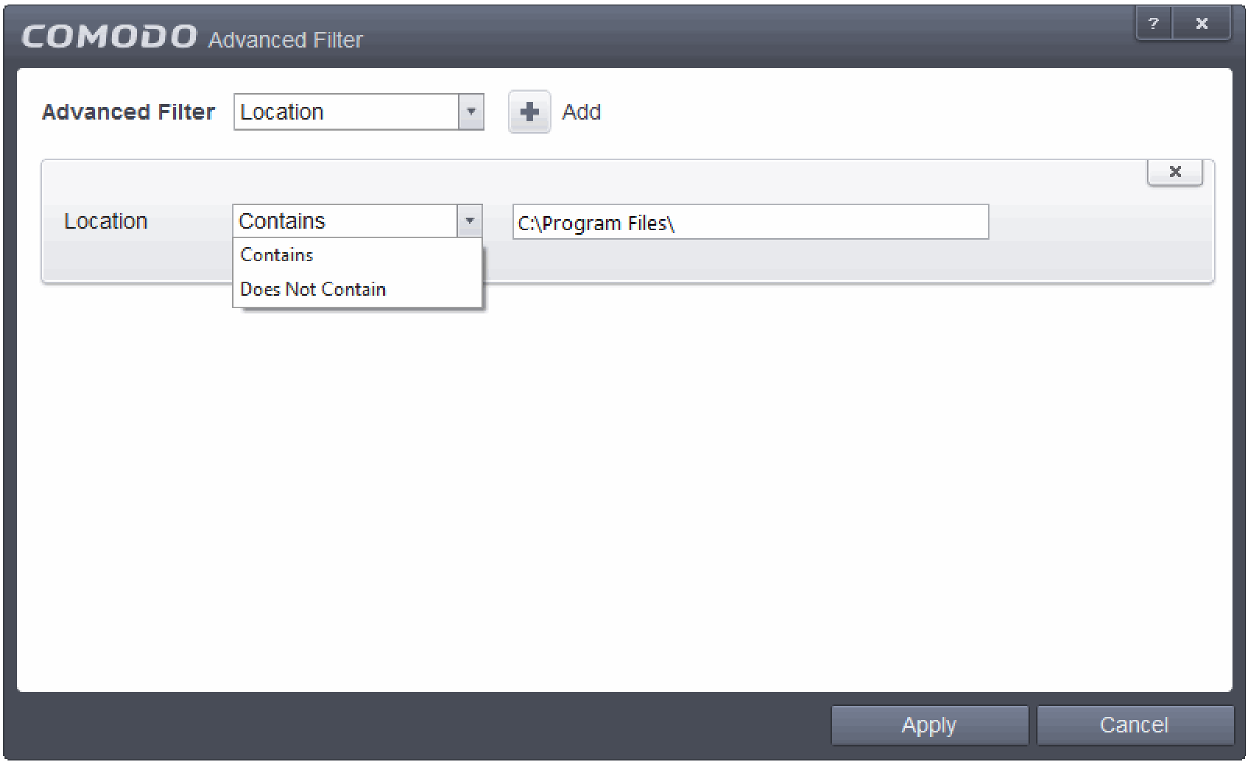
1. Click the funnel button from the title bar. The Advanced Filter interface for 'File List Changes ' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

i. **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.



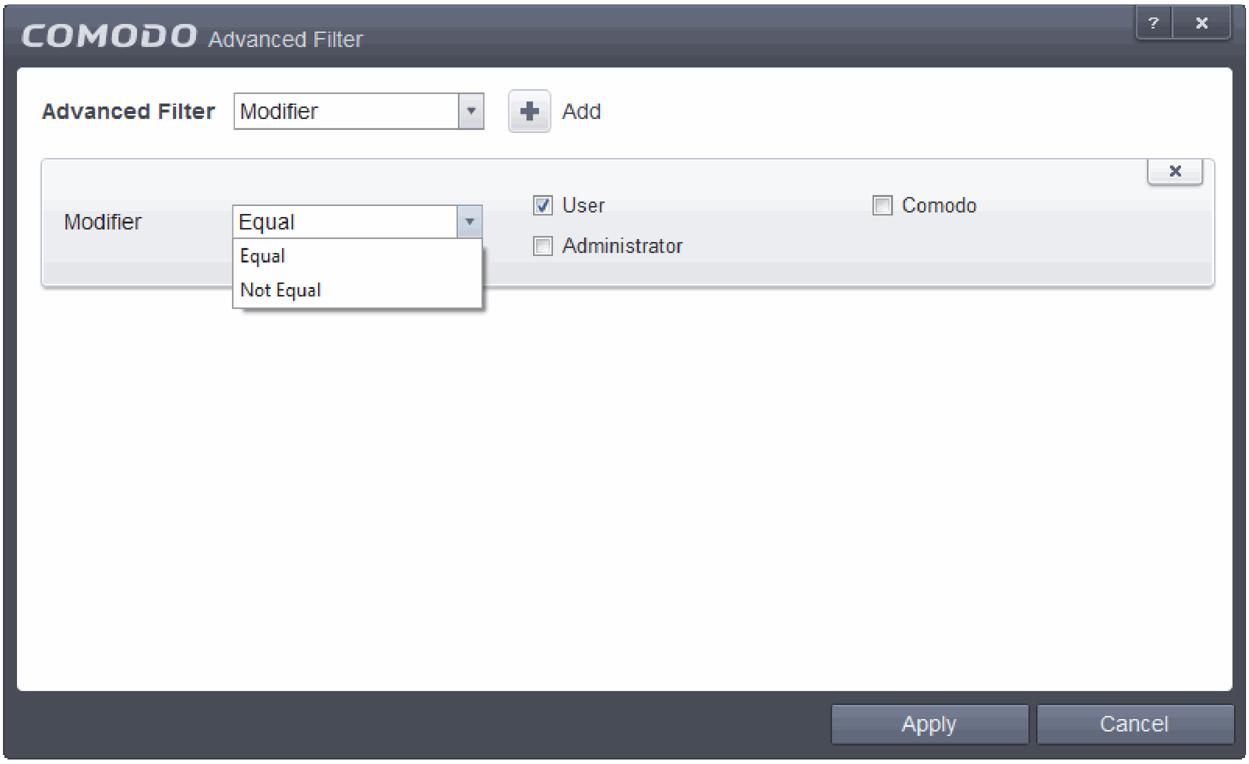
C:\Program Files\

a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b. Enter the text or word that needs to be filtered.

For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:\Program Files\" in the text field, then all events containing the entry 'C:\Program Files\' in the Location field will be displayed. If you select '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.

ii. **Modifier**: The 'Modifier' option allows you to filter the log entries based on the entity that is responsible for the file change. It can be the user, administrator or Comodo. Selecting the 'Modifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



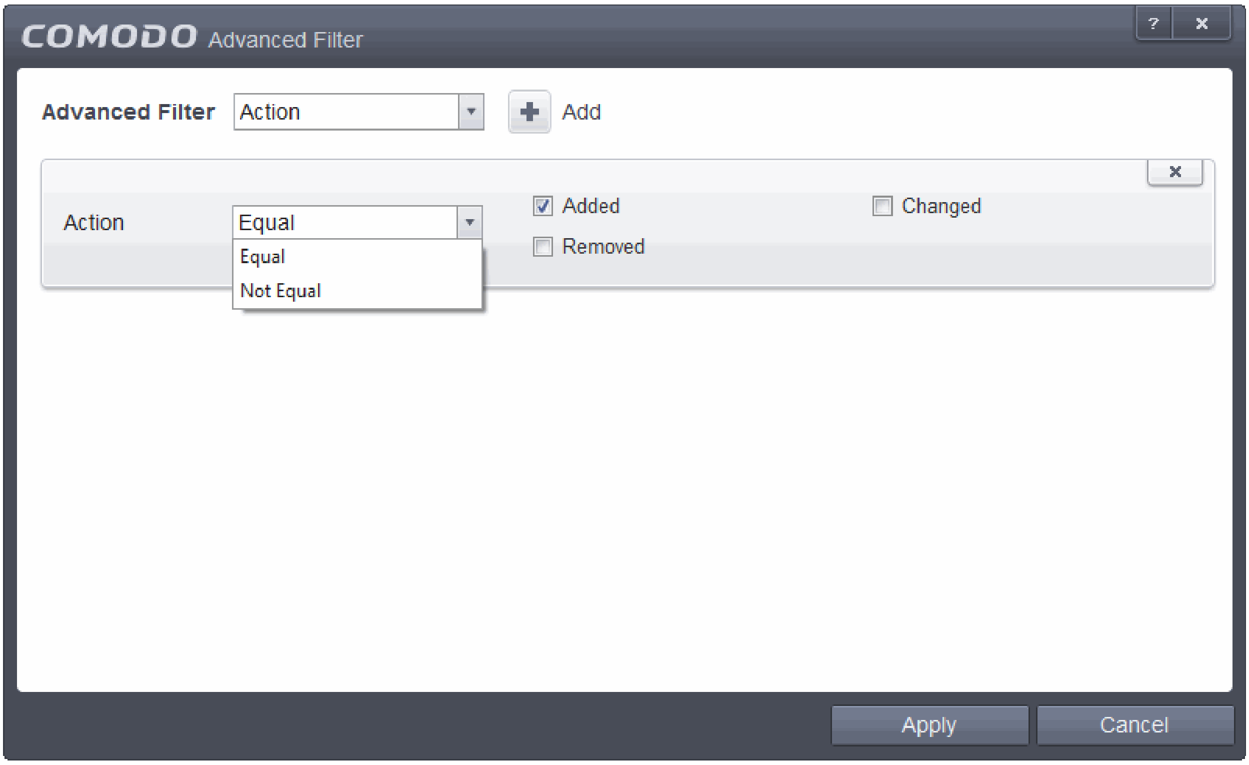
a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b. Select which entities effected the change. The parameters available are:

- User
- Comodo
- Administrator

For example, if you choose 'Equal' in the drop-down and select the 'User' checkbox then only entries related to changes effected by users will be displayed.

iii. **Action**: The 'Action' option allows you to filter the log entries based on the actions executed like removed, added or changes file or applications. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



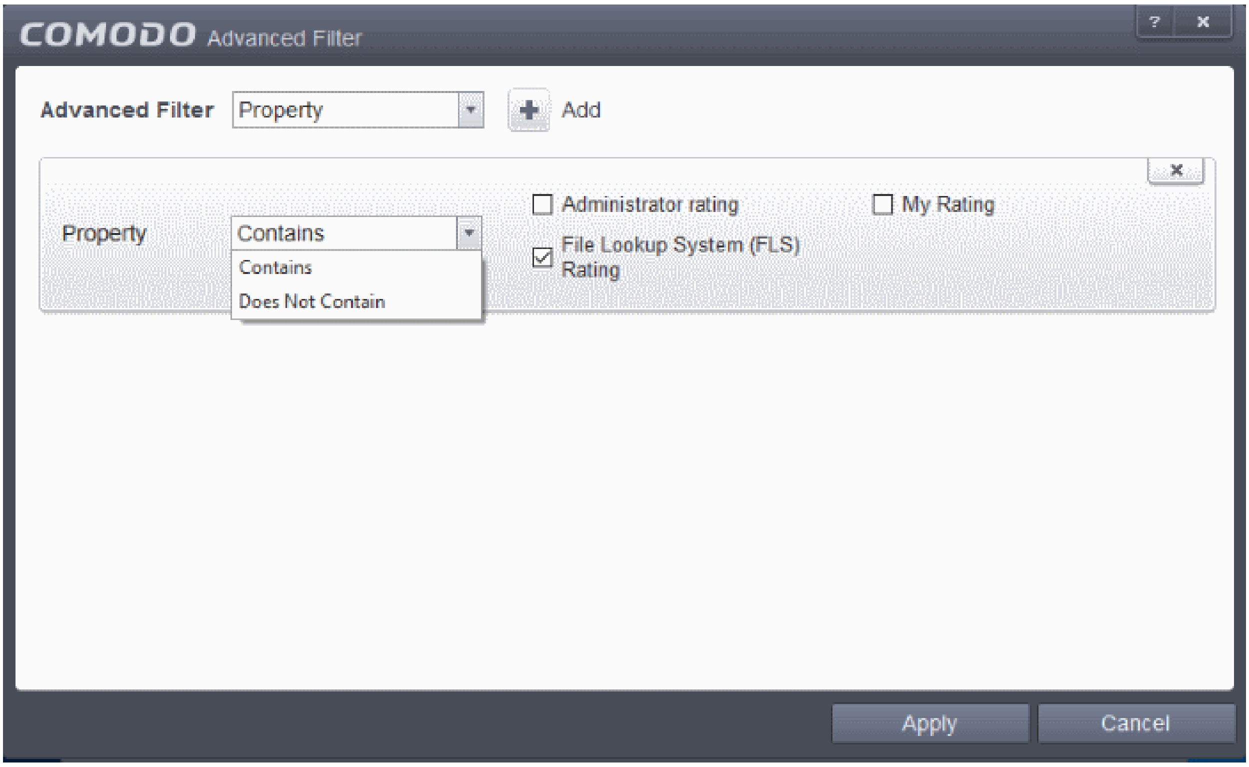
a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

- Added
- Changed
- Removed

For example, if you choose Equal in the drop-down and select 'Added' checkbox, then, only the log entries with the value 'Added' in the 'Action' column will be displayed.

iv. **Property**: The 'Property' option allows you to filter the log entries based on the entity that is responsible for changing the user rating of the file. Selecting the 'Property' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



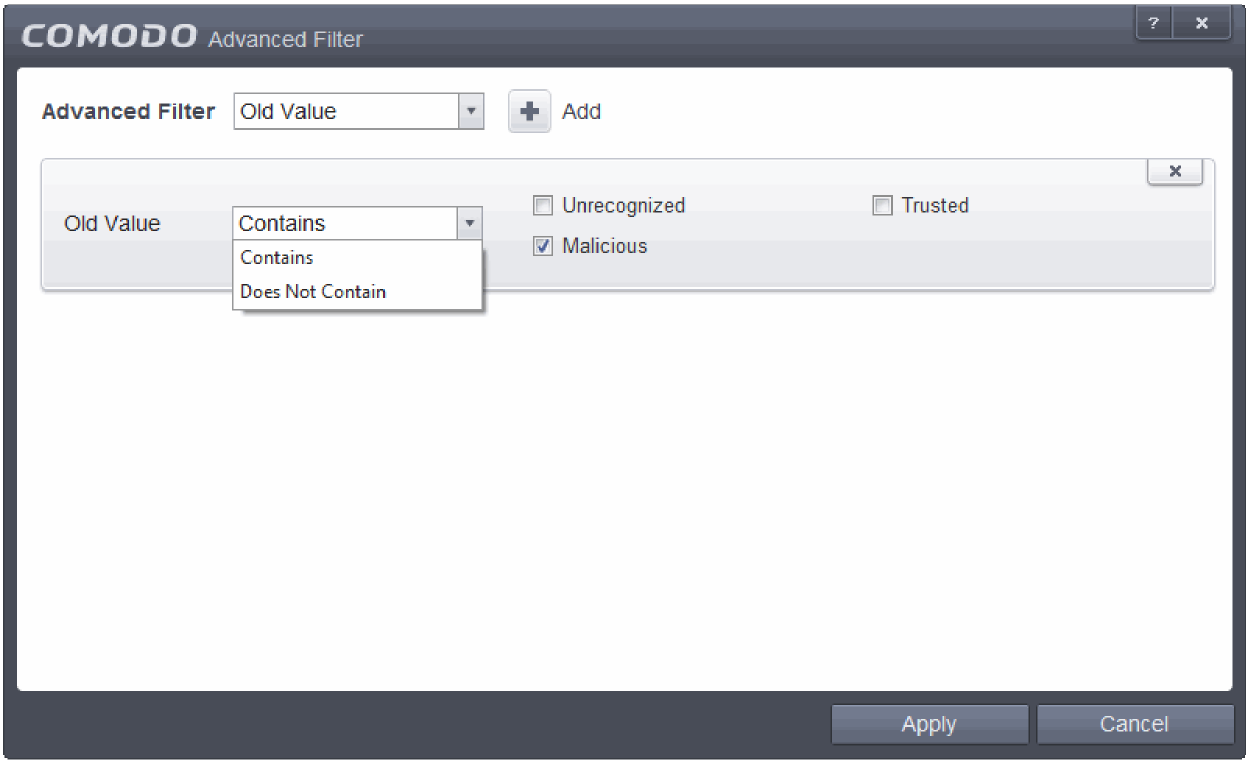
a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b. Enter the name of the change, partly or fully as filter criteria in the text bo

c. x.

For example, if you choose 'Contains' from the drop-down and enter the phrase 'File Lookup System Rating', then only log entries containing the text 'File lookup System Rating' in the name column will be displayed.

v. **Old Value:** The 'Old Value' option allows you to filter the log entries by selecting the value of the parameter changed. Selecting the 'Old Value' option displays a drop-down field and text entry field.

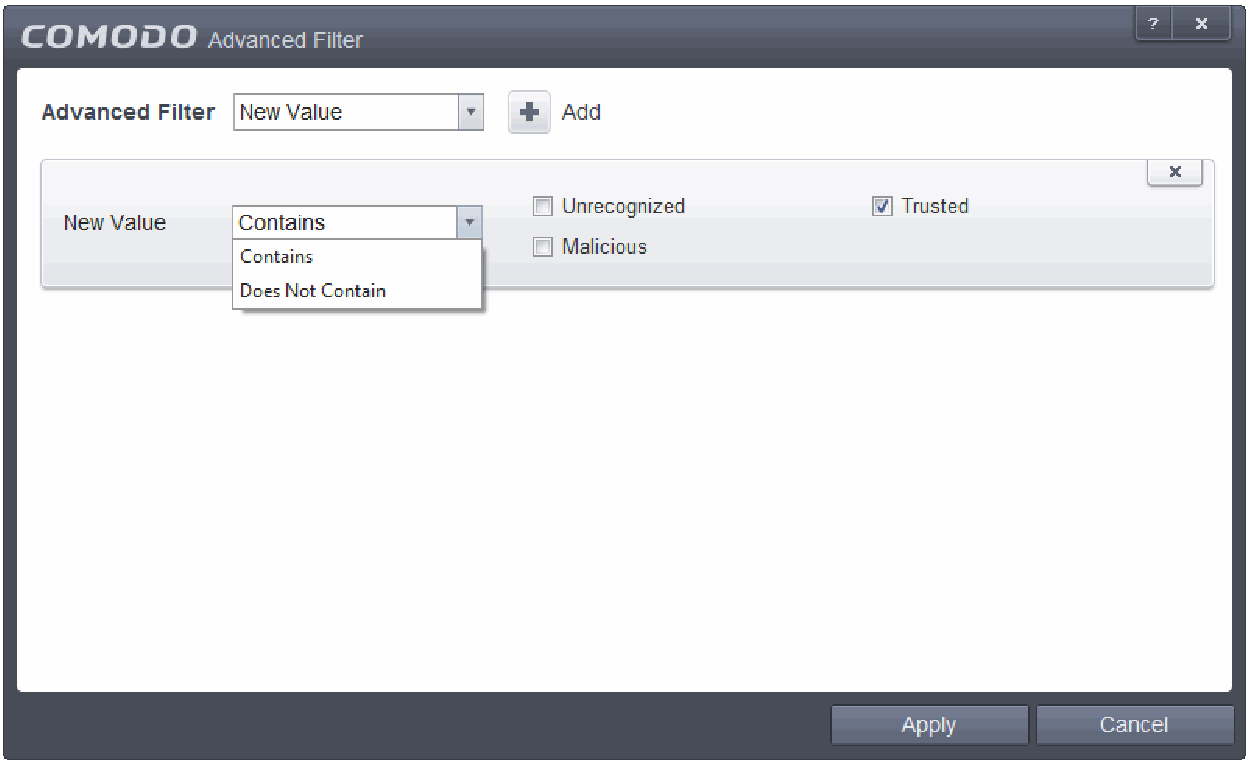


a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b. Enter the 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 selecting 'Malicious' checkbox, only the log entries containing the Malicious in the old value column will be displayed.

vi. **New Value:** The 'New Value' option allows you to filter the log entries by selecting the value of the parameter changed. Selecting the 'New Value' option displays a drop-down field and text entry field.


Advanced Filter: New Value

New Value: Contains

□ Unrecognized

☑ Trusted

□ Malicious

a. Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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 selecting 'Trusted' checkbox, only the log entries containing the Trusted in the new value column will be displayed.

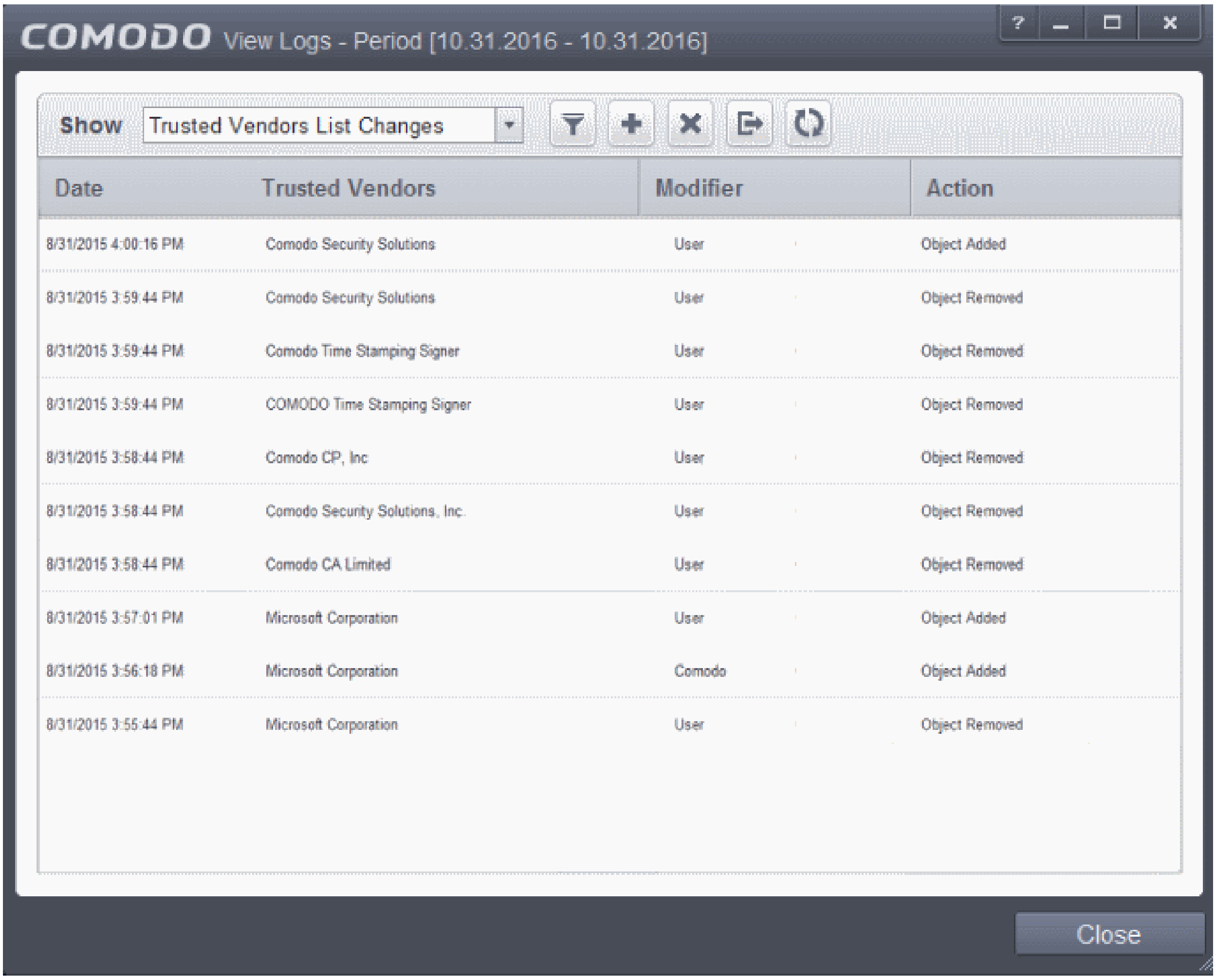
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the **'X'** button at the top right of the filter pane.

- 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.

2.6.10. Trusted Vendors List Changes Logs

Comodo Trusted Vendors List Changes documents the results of all actions performed by it in extensive but easy to understand reports. A detailed scan report contains information of all applications have been treated as safe.

The 'Trusted Vendors List Changes' logs can be viewed by selecting 'Trusted Vendors List Changes' from the 'Show' drop-down of the log viewer interface.


COMODO View Logs - Period [10.31.2016 - 10.31.2016]
Show
Trusted Vendors List Changes
Close

Date	Trusted Vendors	Modifier	Action
8/31/2015 4:00:16 PM	Comodo Security Solutions	User	Object Added
8/31/2015 3:59:44 PM	Comodo Security Solutions	User	Object Removed
8/31/2015 3:59:44 PM	Comodo Time Stamping Signer	User	Object Removed
8/31/2015 3:59:44 PM	COMODO Time Stamping Signer	User	Object Removed
8/31/2015 3:58:44 PM	Comodo CP, Inc	User	Object Removed
8/31/2015 3:58:44 PM	Comodo Security Solutions, Inc.	User	Object Removed
8/31/2015 3:58:44 PM	Comodo CA Limited	User	Object Removed
8/31/2015 3:57:01 PM	Microsoft Corporation	User	Object Added
8/31/2015 3:56:18 PM	Microsoft Corporation	Comodo	Object Added
8/31/2015 3:55:44 PM	Microsoft Corporation	User	Object Removed

Column Descriptions

1. **Date** - Contains precise details of the date and time of the vendors added.
2. **Trusted Vendors** – Lists all trusted vendors that ships to all users with CCS
3. **Modifier** - Indicates the user that has added the application to the trusted and allowed to run
4. **Action** - Indicates action taken by Trusted Vendors in response to the event

- To export the 'Trusted Vendors List Changes' logs as a HTML file click the 'Export' button
- To open a stored CCS log file, click the 'Open' button
- To refresh the 'Trusted Vendors List' logs, click the 'Refresh' button
- To clear the 'Trusted Vendors List' logs click the 'Clear' button

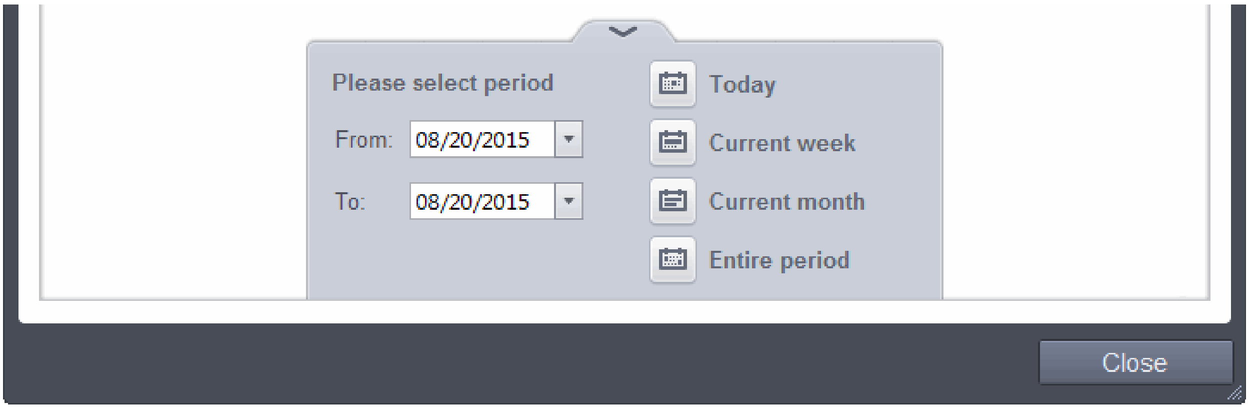
2.6.10.1. Filtering 'Trusted Vendors List Changes' Logs

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

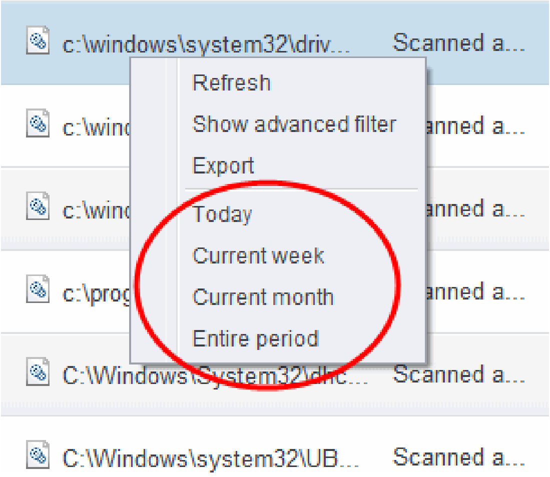
Preset Time Filters

Clicking on the handle at the bottom enables you to filter the log entries for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can 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 'Trusted Vendors List Changes' logs and their meanings:

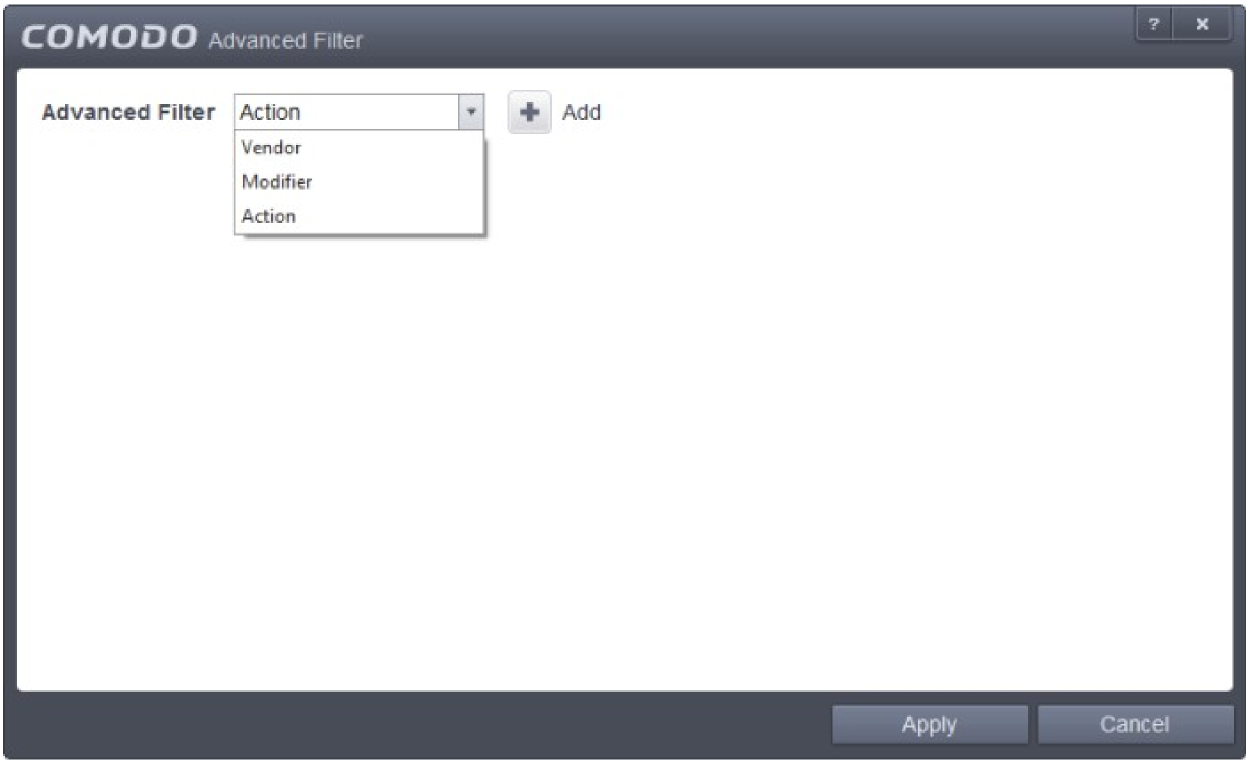
- **Vendors** - Lists all trusted vendors that ships to all users with CCS
- **Modifier** - Indicates the user that has added the application to the trusted list and allowed to run
- **Action** - Indicates action taken by Trusted Vendors in response to the event

To configure Advanced Filters for Trusted Vendors Logs

1. Click the funnel button from the title bar. The Advanced Filter interface for 'Trusted Vendors List

Changes' logs will open.

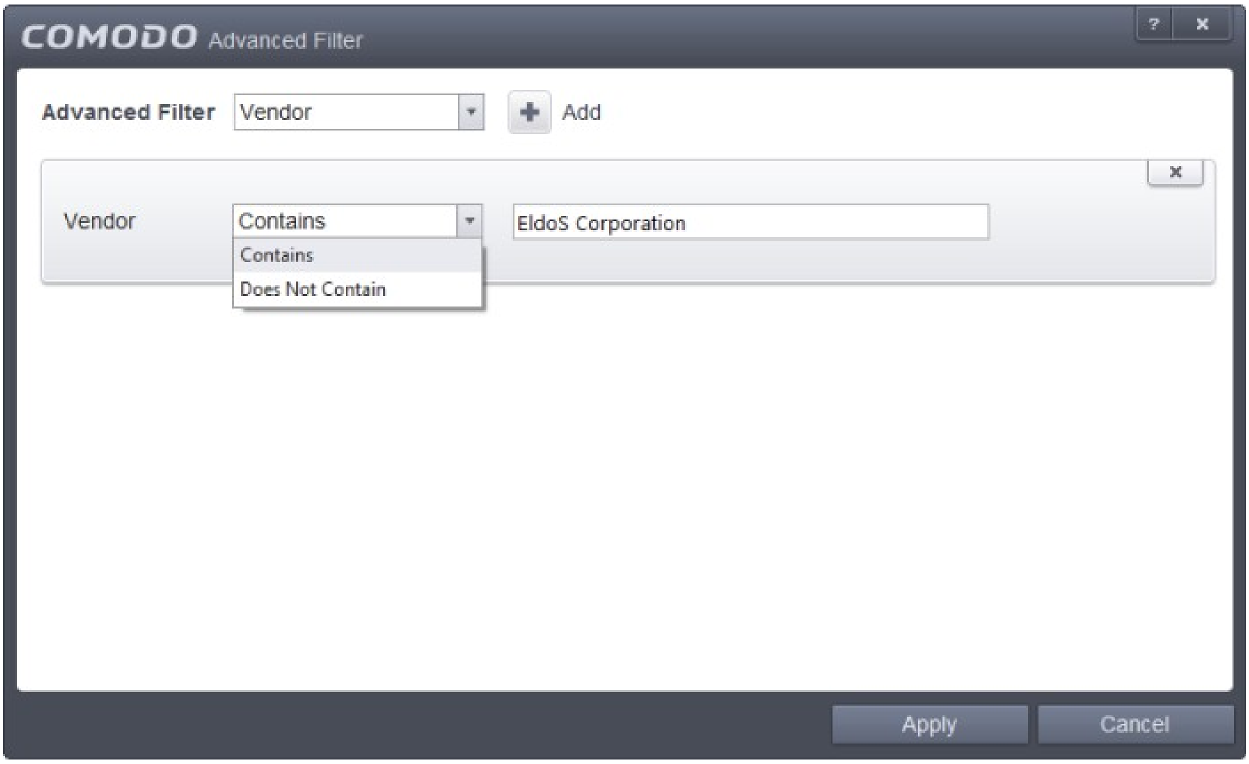
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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



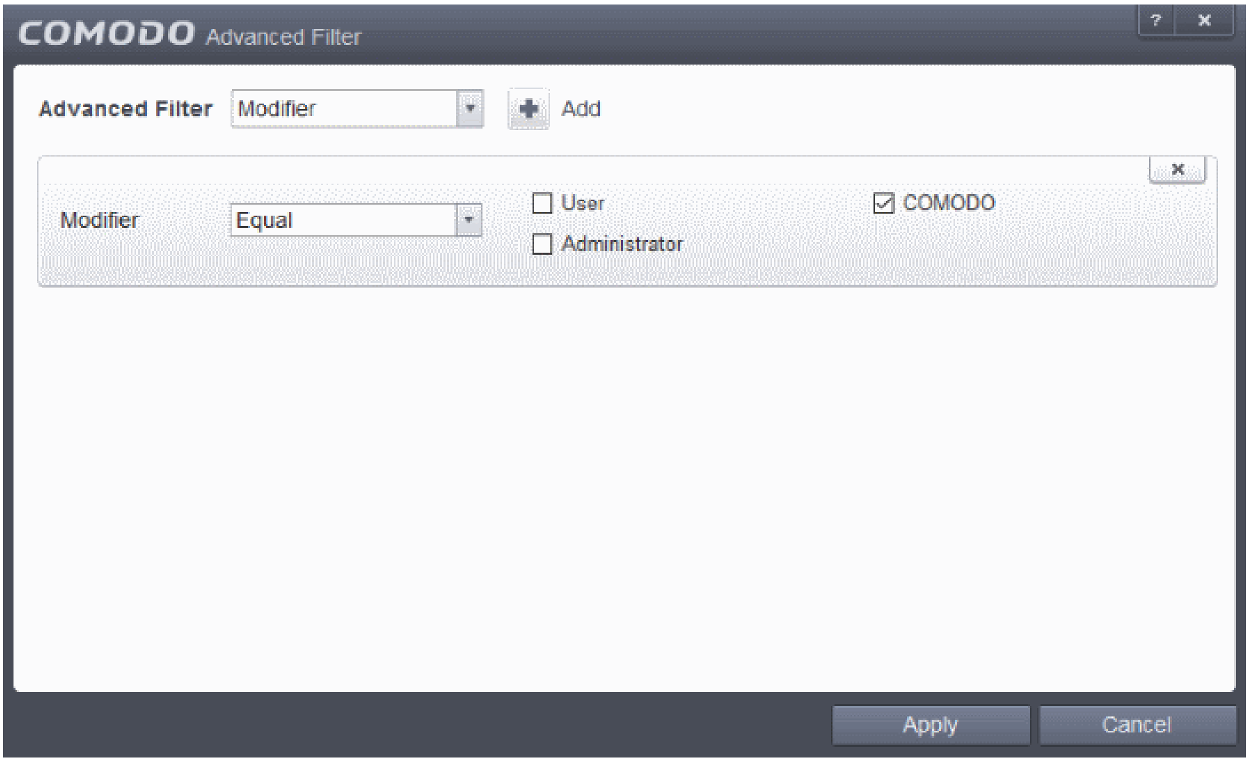
Vendor: Contains — EldoS Corporation

a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

b) Enter the text in the name of the vendor that needs to be filtered.

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

ii. **Modifier:** The 'Modifier' option allows you to filter the log entries based on the entity that is responsible for the trusted vendor. Selecting the 'Modifier' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



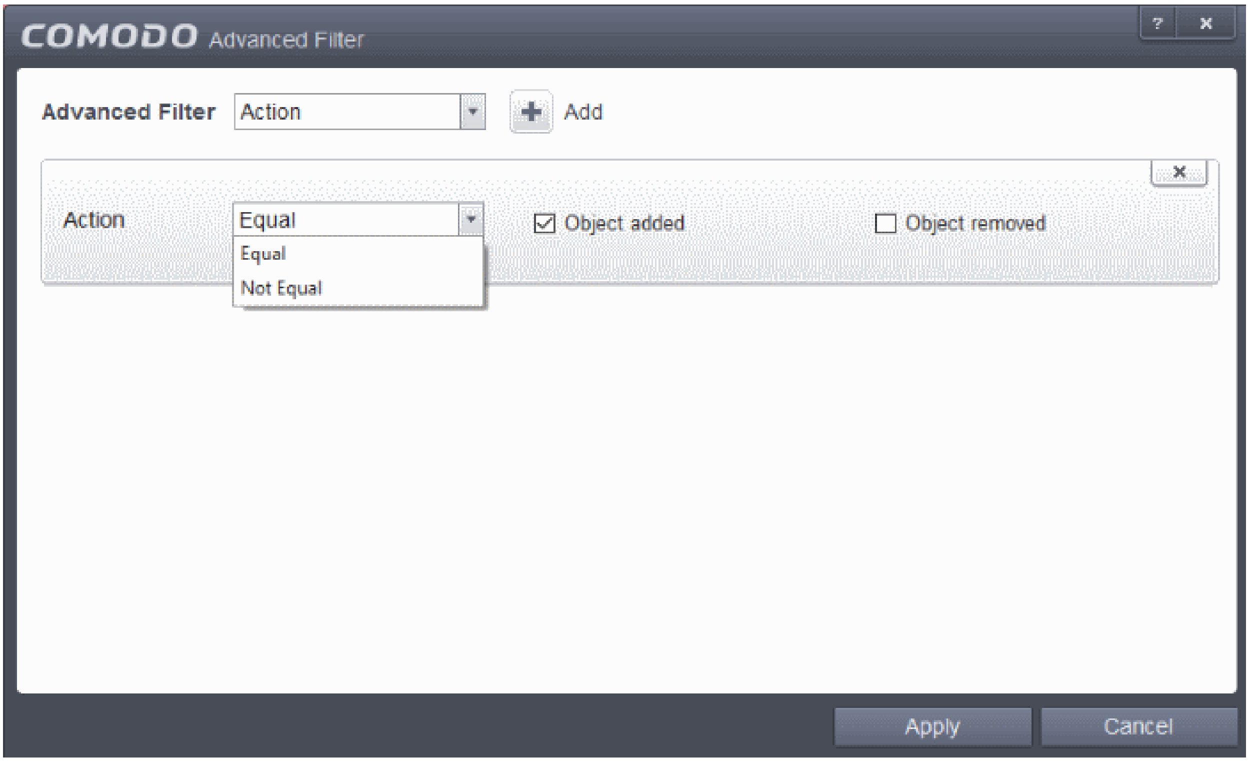
a. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b. Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:

- User
- COMODO
- Administrator

For example, if you have chosen Equal in the drop-down and selected 'User ' checkbox, then, only the log entries related to the vendors effected by responses to 'Trusted Software Vendor List Changes' will be displayed.

iii. **Action:** The 'Action' option allows you to filter the log entries based on the actions executed like change in addition or removal of objects. 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 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:

   - Object added
   - Object removed

   For example, if you choose Equal in the drop-down and select 'Object Added' checkbox, then, only the log entries with the value 'Object Added' in the 'Action' column will be displayed.

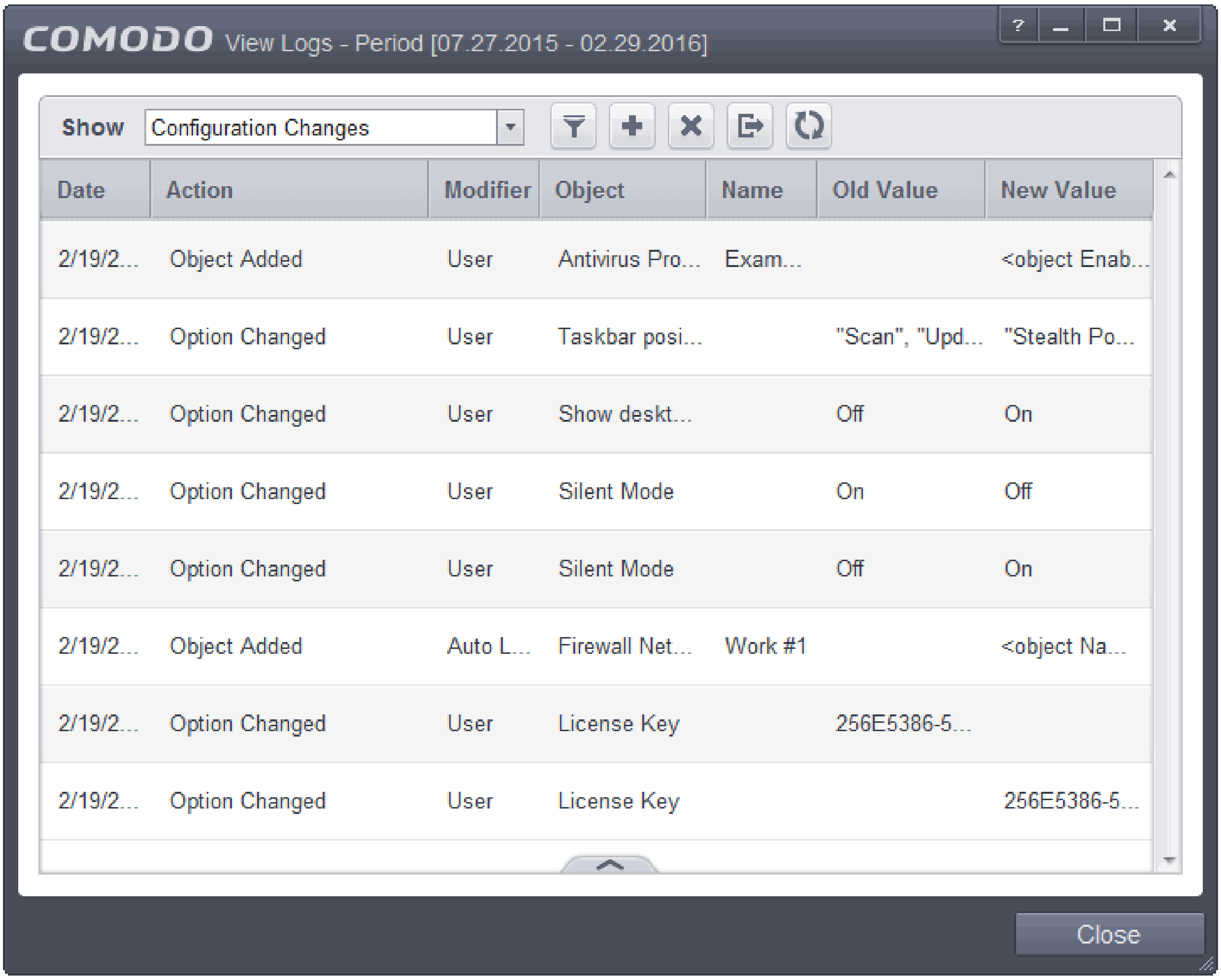
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the **'X'** button at the top right of the filter pane.

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

2.6.11. Configuration Changes

CCS keeps track of all the changes made to its configuration since its installation. The 'Configuration Changes' log viewer displays a list of changes to various options and other configuration changes made to the application.

The 'Configuration Changes' logs can be viewed by selecting 'Configuration Changes' from the 'Show' drop-down of the log viewer interface.



Date	Action	Modifier	Object	Name	Old Value	New Value
2/19/2...	Object Added	User	Antivirus Pro...	Exam...		<object Enab...
2/19/2...	Option Changed	User	Taskbar posi...		"Scan", "Upd...	"Stealth Po...
2/19/2...	Option Changed	User	Show deskt...		Off	On
2/19/2...	Option Changed	User	Silent Mode		On	Off
2/19/2...	Option Changed	User	Silent Mode		Off	On
2/19/2...	Object Added	Auto L...	Firewall Net...	Work #1		<object Na...
2/19/2...	Option Changed	User	License Key		256E5386-5...	
2/19/2...	Option Changed	User	License Key			256E5386-5...

Column Descriptions

1. **Date** - Contains precise details of the date and time of the configuration change.
2. **Action -** Indicates the nature of the configuration change.
3. **Modifier -** Indicates the user that made the configuration change.
4. **Object -** Indicates the CCS object that was affected by the configuration change.
5. **Name** - Indicates the parameter changed.
6. **Old value -** Indicates the value of the parameter before the configuration change.
7. **New value -** Indicates the value of the parameter after the configuration change.

- To export the 'Configuration Changes' logs as a HTML file click the 'Export' button
- To open a stored CCS log file, click the 'Open' button
- To refresh the 'Configuration Changes' logs, click the 'Refresh' button
- To clear the 'Configuration Changes' logs click the 'Clear' button

2.6.11.1. Filtering 'Configuration Changes' Logs

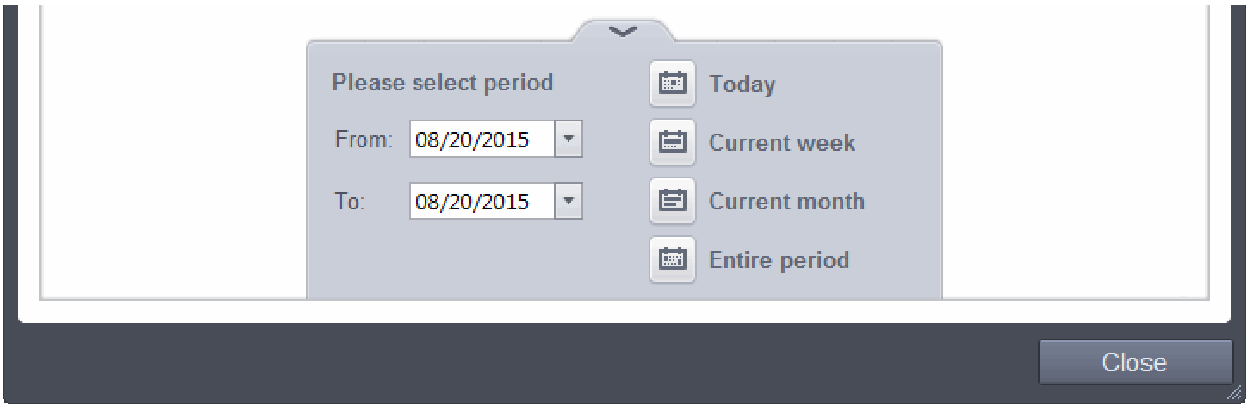
Comodo Client Security allows you to create custom views of all logged events according to user defined criteria.

You can use the following types of filters:

- Preset Time Filters
- Advanced Filters

Preset Time Filters

Clicking on the handle at the bottom enables you to filter the log entries for a selected time period:



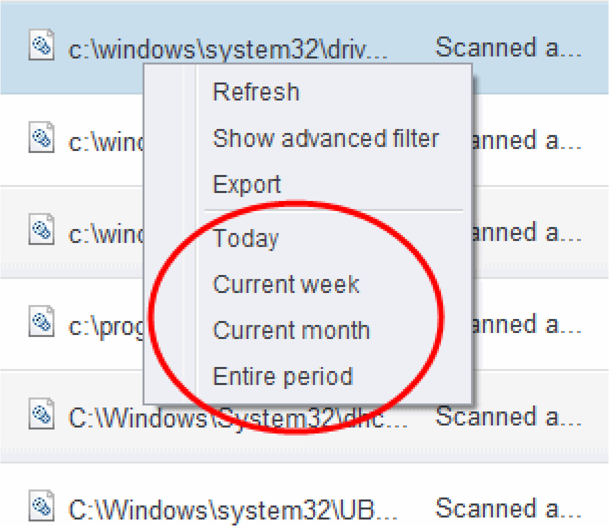
Please select period

From: 08/20/2015

To: 08/20/2015

- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



Advanced Filters

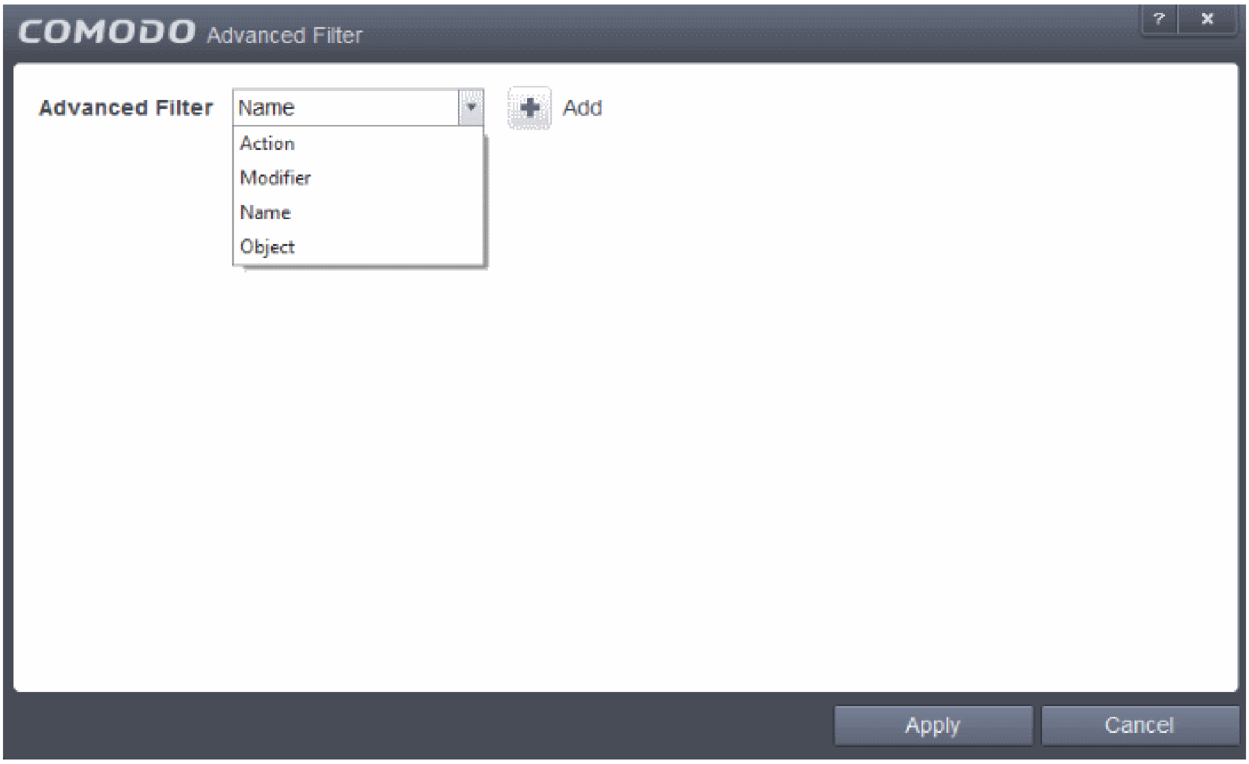
You can further refine the displayed events according to specific filters. Following are available filters for 'Configuration Changes' logs and their meanings:

- **Action:** Displays only the selected type of configuration change(s) like change in options, addition of objects, strings and so on.

- **Modifier**: Displays only the configuration changes effected by the selected entity like the user, response to Antivirus or Advanced protection alerts Alerts and so on.
- **Name**: Displays only the configuration change with the name entered as search criteria.
- **Object:** Displays only the configuration changes on addition or removal of selected objects

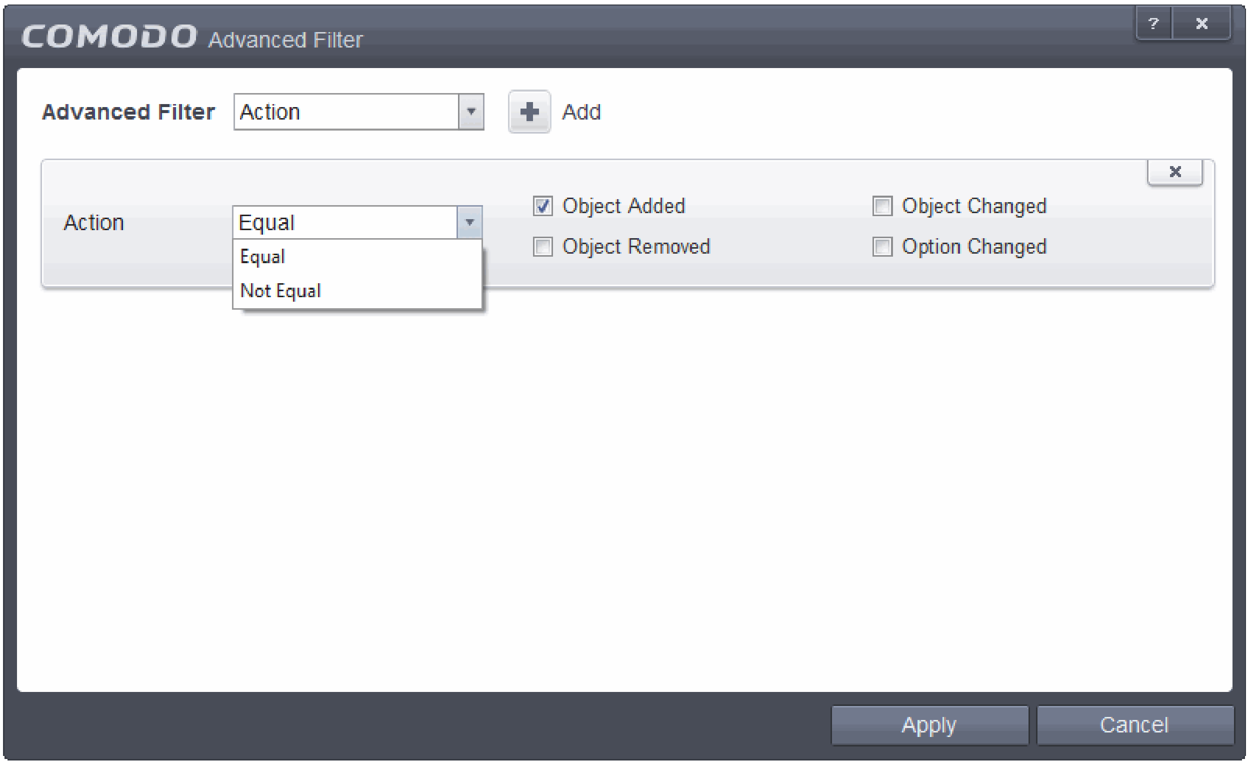
To configure Advanced Filters for Configuration Changes Logs

1. Click the funnel button from the title bar. The Advanced Filter interface for 'Configuration Changes' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You can chose the category of filter from the 'Advanced Filter' drop-down. 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. Following are the options available in the 'Add' drop down menu:

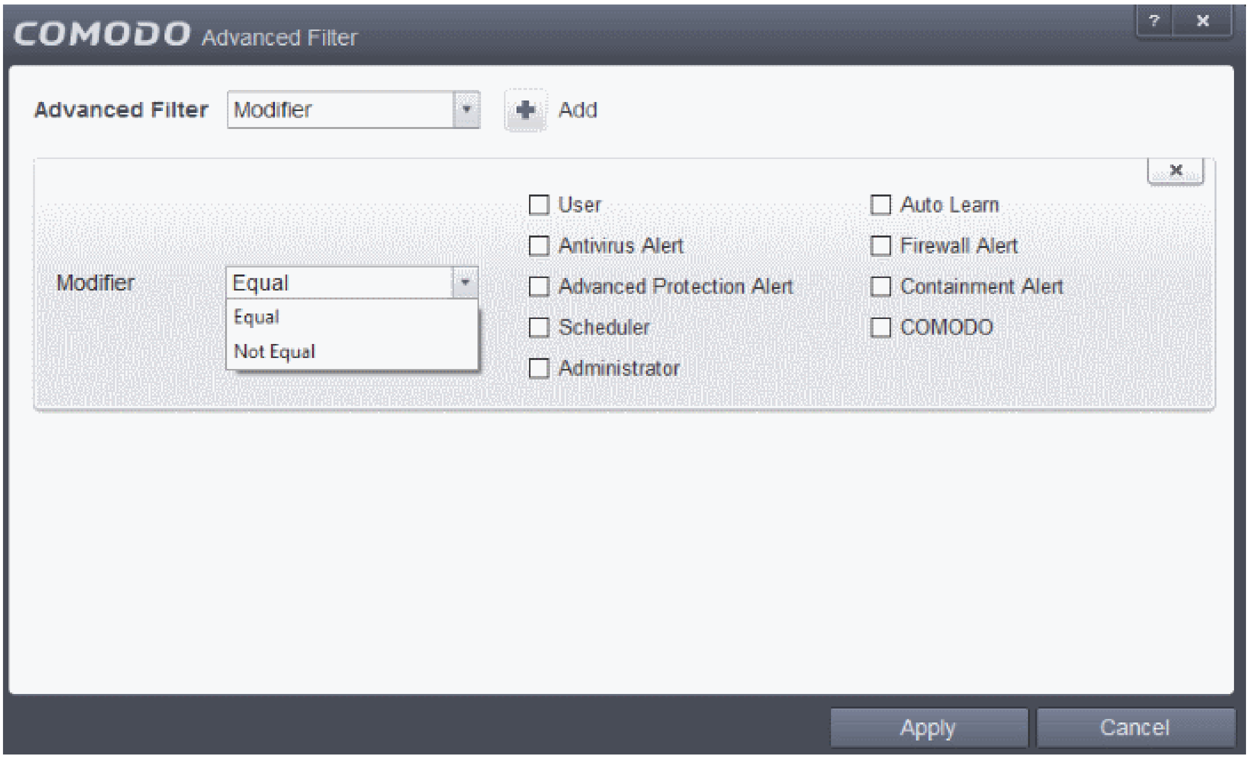
i. **Action**: The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



a) Select 'Equal' or 'Not Equal' option from the drop-down menu.

For example, if you have selected Equal in the drop-down and selected 'Object added' checkbox, then, only the log entries with the value 'Object added' in the 'Action' column will be displayed.

ii. **Modifier**: The 'Modifier' option allows you to filter the 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 a drop-down box and a set of specific filter parameters that can be selected or deselected.



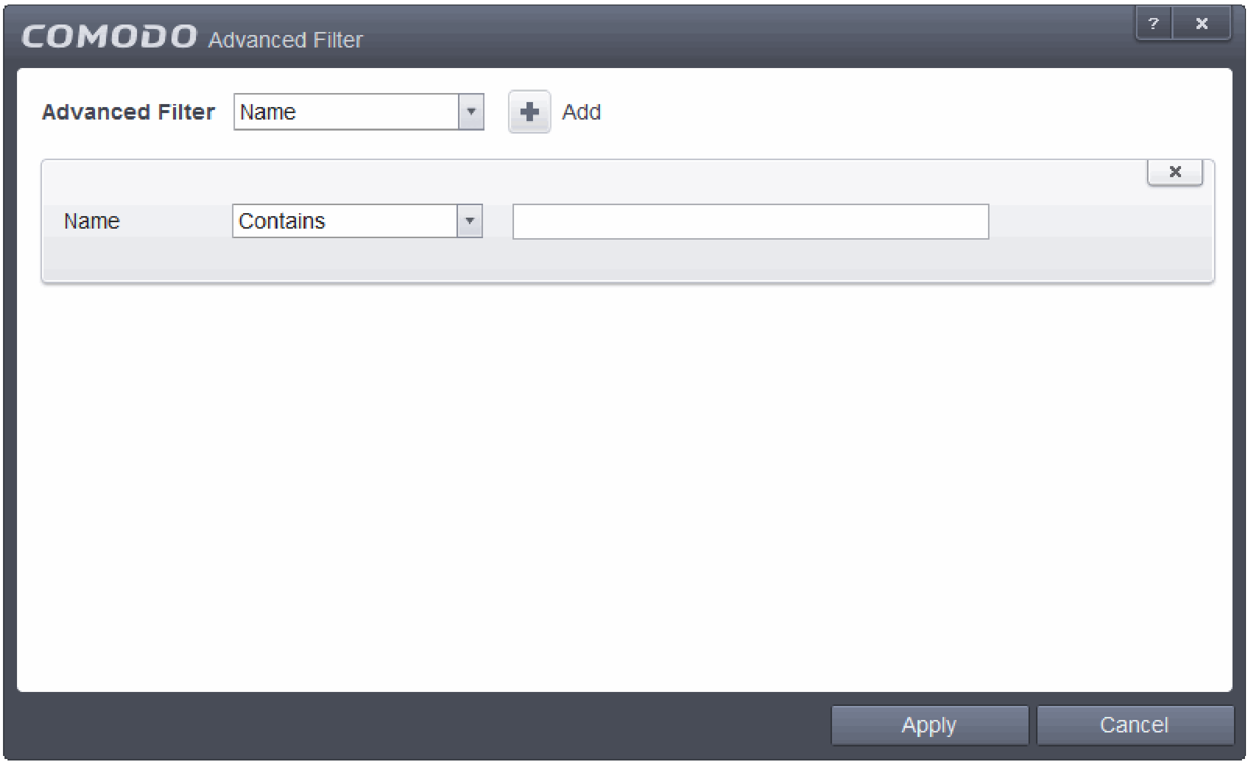
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:

- User
- Auto Learn
- Antivirus Alert
- Firewall Alert
- Advanced Protection Alert
- Containment Alert
- Scheduler
- COMODO
- Administrator

For example, if you have selected Equal in the drop-down and selected 'Antivrius Alert ' checkbox, then, only the log entries related to the configuration changes effected by responses to Antivirus Alerts will be displayed.

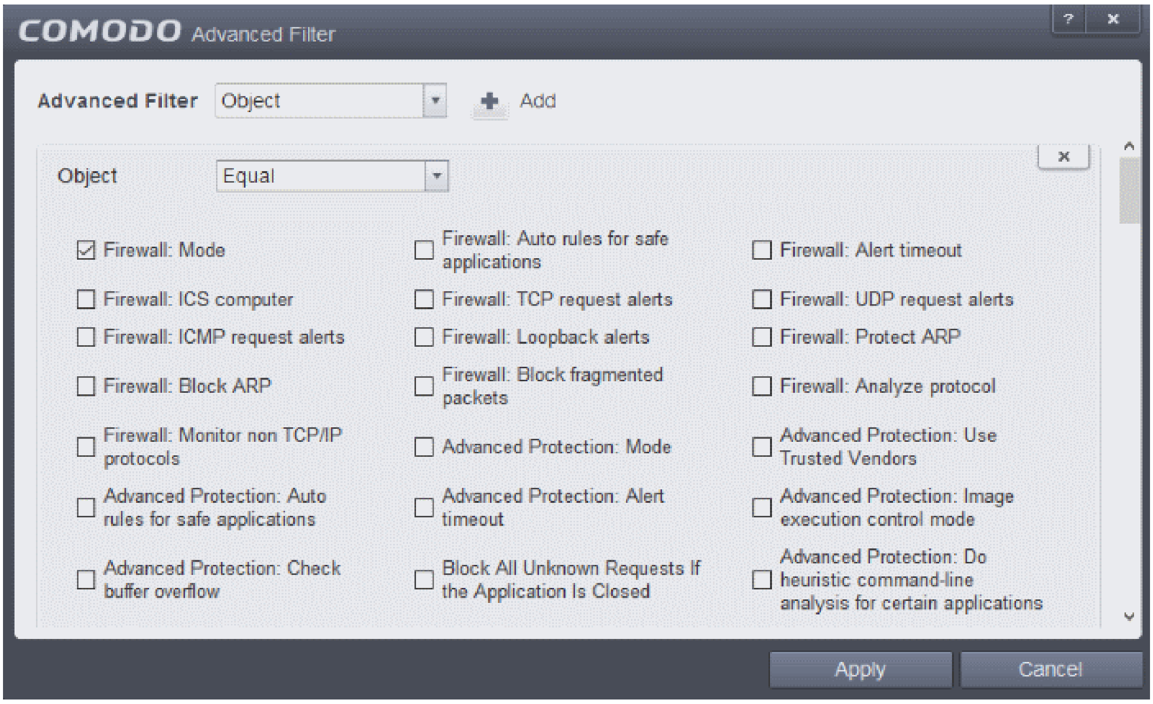
iii. **Name**: The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the name of the change, partly or fully as filter criteria in the text box.

iv. **Object**: The 'Object' option enables you to filter the log entries related to the objects modified during the configuration change. Selecting the 'Object' option displays a drop down menu and the objects of CCS configuration, that can be selected or deselected.



Advanced Filter: Object

Object: Equal

- ☑ Firewall: Mode
- □ Firewall: ICS computer
- □ Firewall: ICMP request alerts
- □ Firewall: Block ARP
- □ Firewall: Monitor non TCP/IP protocols
- □ Advanced Protection: Auto rules for safe applications
- □ Advanced Protection: Check buffer overflow
- □ Firewall: Auto rules for safe applications
- □ Firewall: TCP request alerts
- □ Firewall: Loopback alerts
- □ Firewall: Block fragmented packets
- □ Advanced Protection: Mode
- □ Advanced Protection: Alert timeout
- □ Block All Unknown Requests If the Application Is Closed
- □ Firewall: Alert timeout
- □ Firewall: UDP request alerts
- □ Firewall: Protect ARP
- □ Firewall: Analyze protocol
- □ Advanced Protection: Use Trusted Vendors
- □ Advanced Protection: Image execution control mode
- □ Advanced Protection: Do heuristic command-line analysis for certain applications

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 the window to the right to see all the parameters options.

For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode ' checkbox, only the log entries related to the changes in Firewall mode will be displayed.

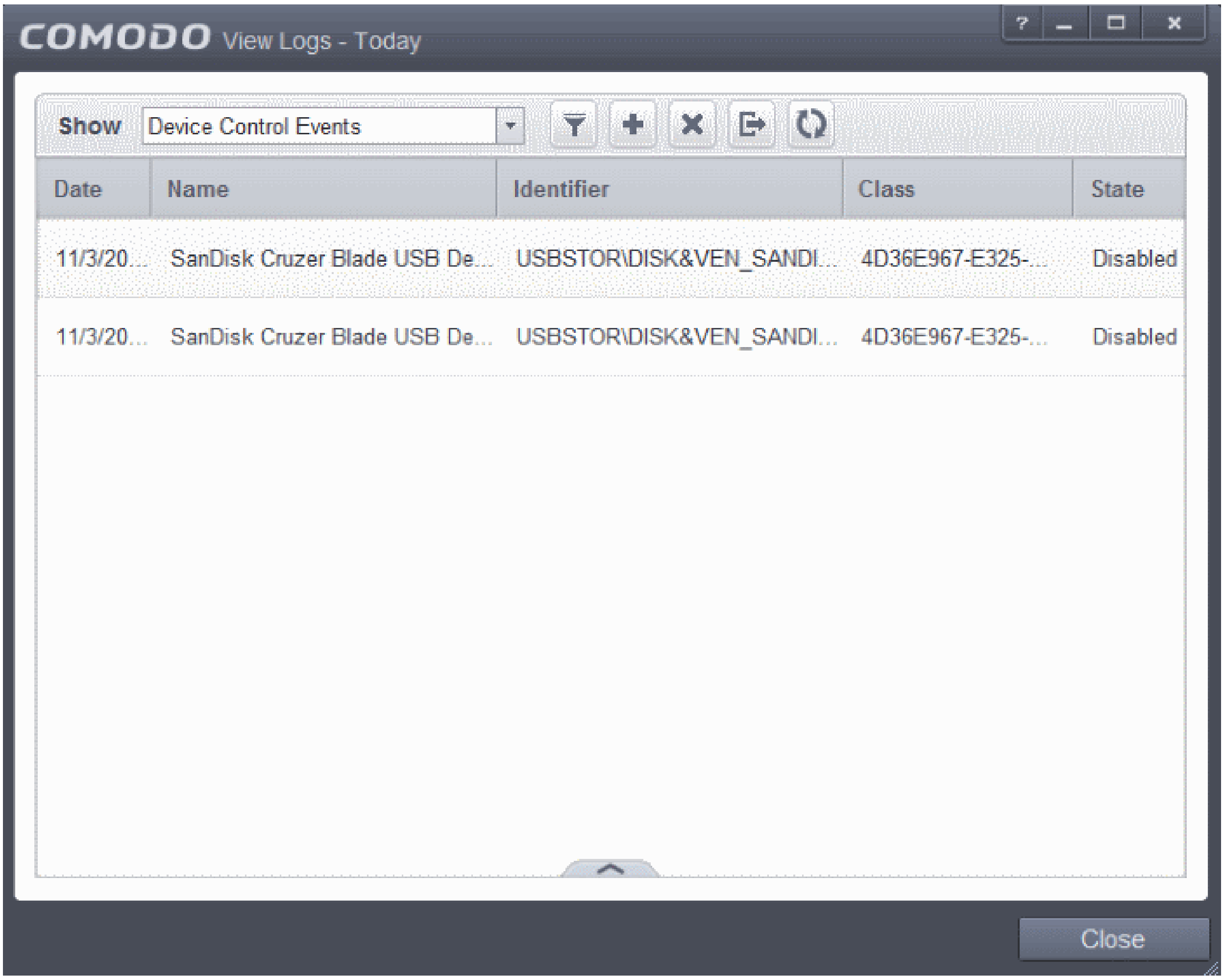
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the **'X'** button at the top right of the filter pane.

- 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.

2.6.12. Device Control Logs

The 'Device Control logs' interface lists events that have taken place on the system once an external device has been detected. Events logged include files copied, deleted and moved. The event of a device being detected is also logged if 'Log detected devices' is enabled.

Device control can be configured in '**Advanced Settings > Device Control Settings'.** Administrators can also configure this option in an ITSM profile. If you need to allow access to certain devices you can disable device control entirely or remove the device class from the list of controlled types or add specific devices to exclusions.



Date	Name	Identifier	Class	State
11/3/20...	SanDisk Cruzer Blade USB De...	USBSTOR\DISK&VEN_SANDI...	4D36E967-E325-...	Disabled
11/3/20...	SanDisk Cruzer Blade USB De...	USBSTOR\DISK&VEN_SANDI...	4D36E967-E325-...	Disabled

Column Descriptions

1. **Date** - Date and time of the device control event.
2. **Name -** Indicates 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** - Indicates the current status of the task.
6. **Info & Additional Info -** Provides additional information on the task (if available).

- To export the Device control logs as a HTML file, click the 'Export' button .
- To open a stored CCS log file, click the 'Open' button .
- To refresh the Device control logs, click the 'Refresh' button .
- To clear the Device control logs, click the 'Clear' button .

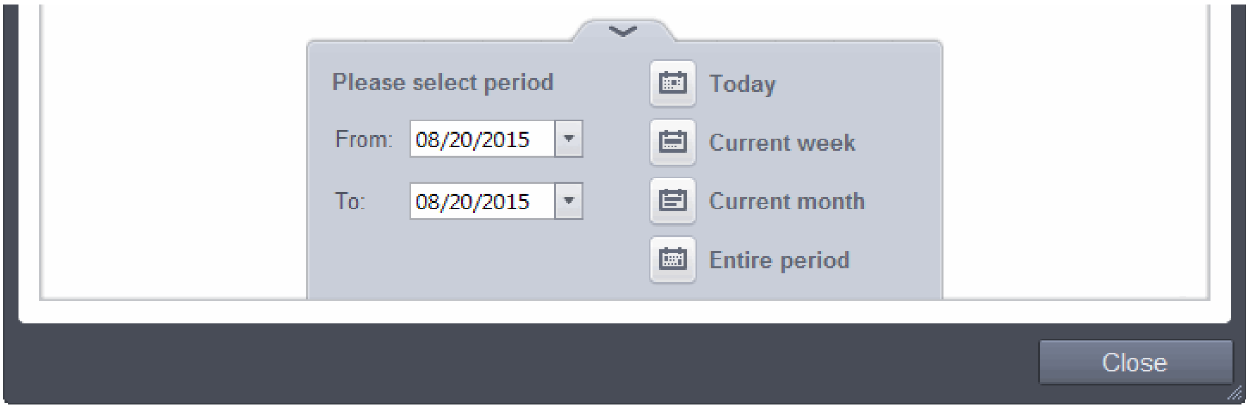
2.6.12.1. Filtering 'Device Control' Logs

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

Clicking on the handle at the bottom enables you to filter the log entries for a selected time period:



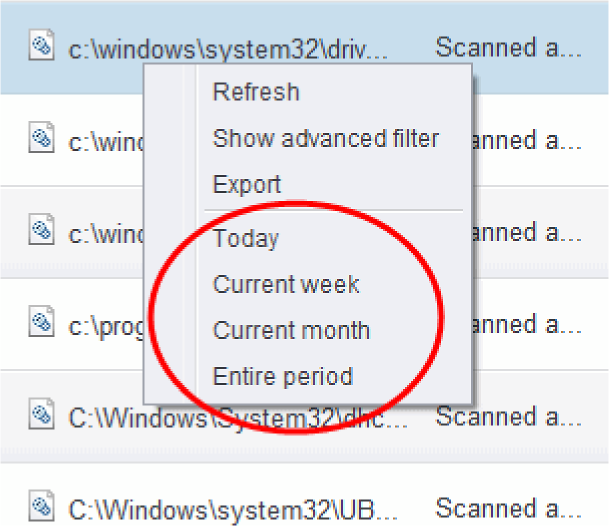
Please select period

From: 08/20/2015

To: 08/20/2015

- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Client Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).
- **Custom Filter** - Enables you to select a custom period by choosing the 'From' and 'To' dates under 'Please Select Period'

Alternatively, you can right click inside the log viewer module and choose the time period.



c:\windows\system32\driv... Scanned a...

c:\wind ... anned a...

c:\wind ... anned a...

c:\prog ... anned a...

C:\Windows\System32\drlc... Scanned a...

C:\Windows\system32\UB... Scanned a...

Advanced Filters

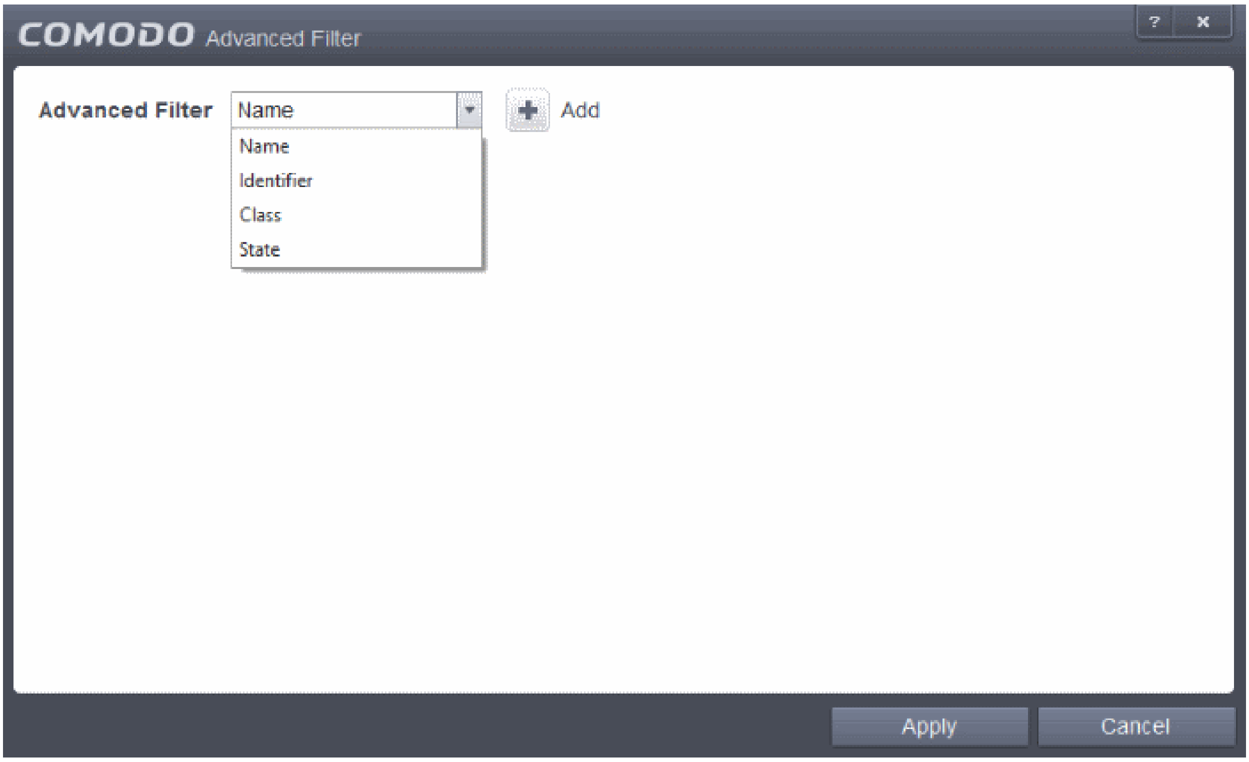
You can further refine the displayed events according to specific filters. Following are available filters for 'Device Control Events' logs and their meanings:

- **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

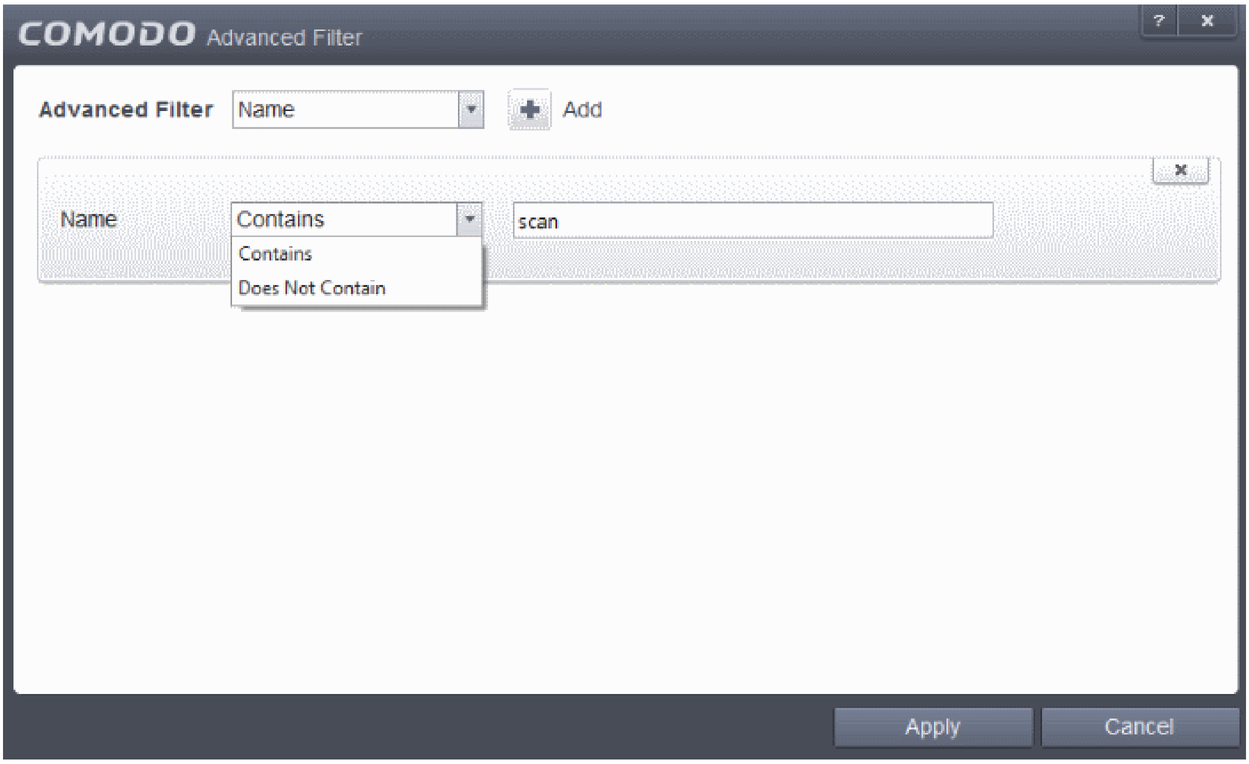
1. Click the funnel button from the title bar. The Advanced Filter interface for 'Device Control Events' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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 the 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.

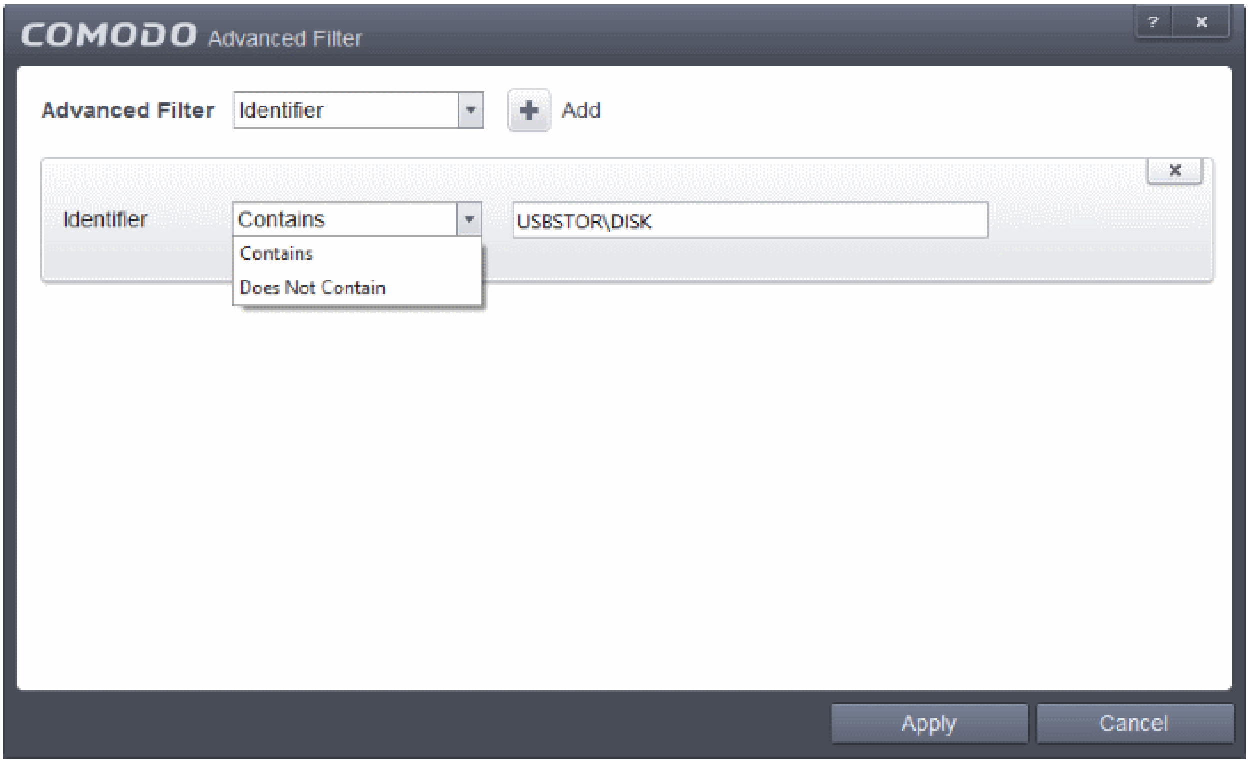


a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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.

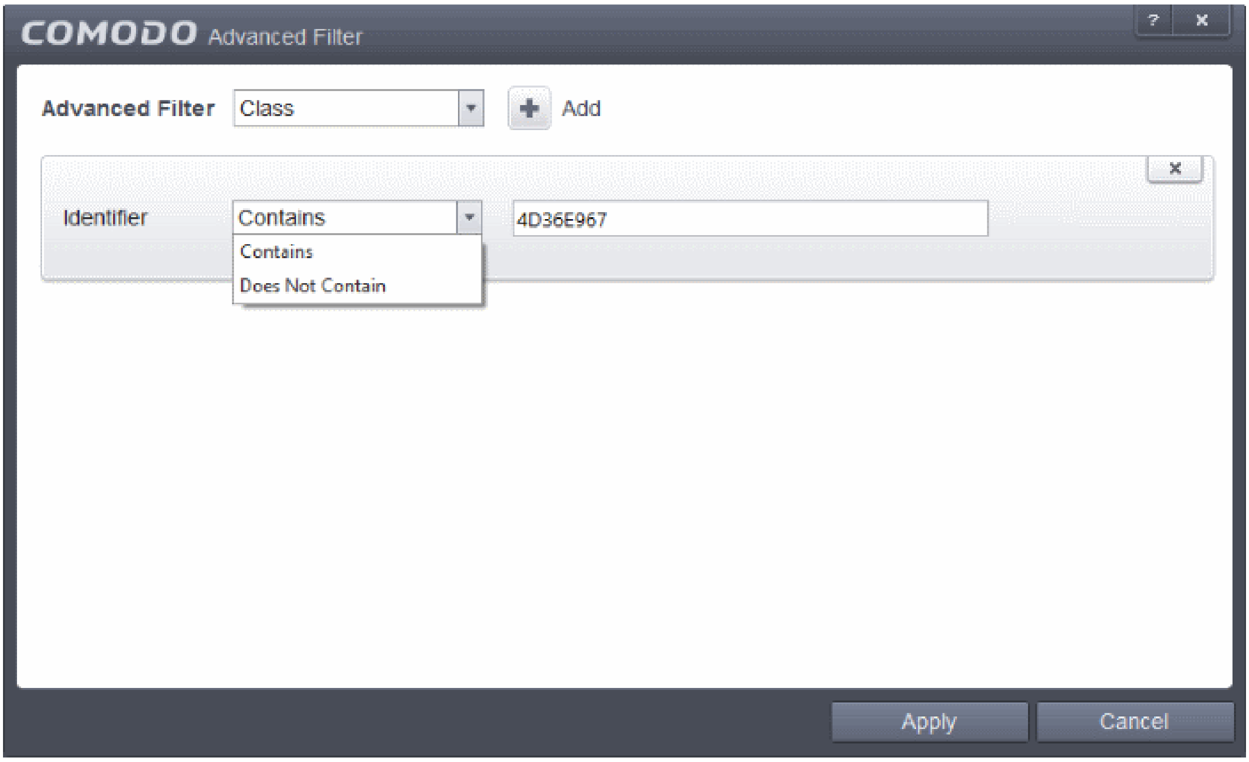


a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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

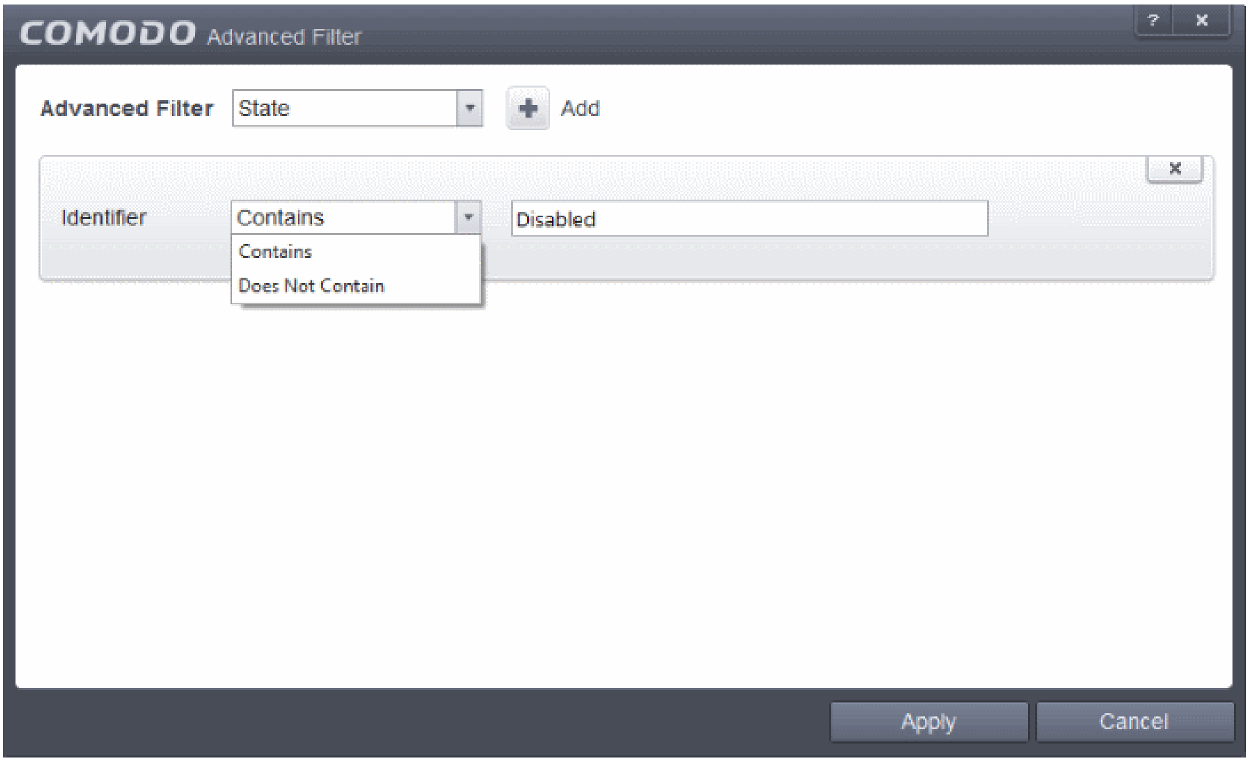


a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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.

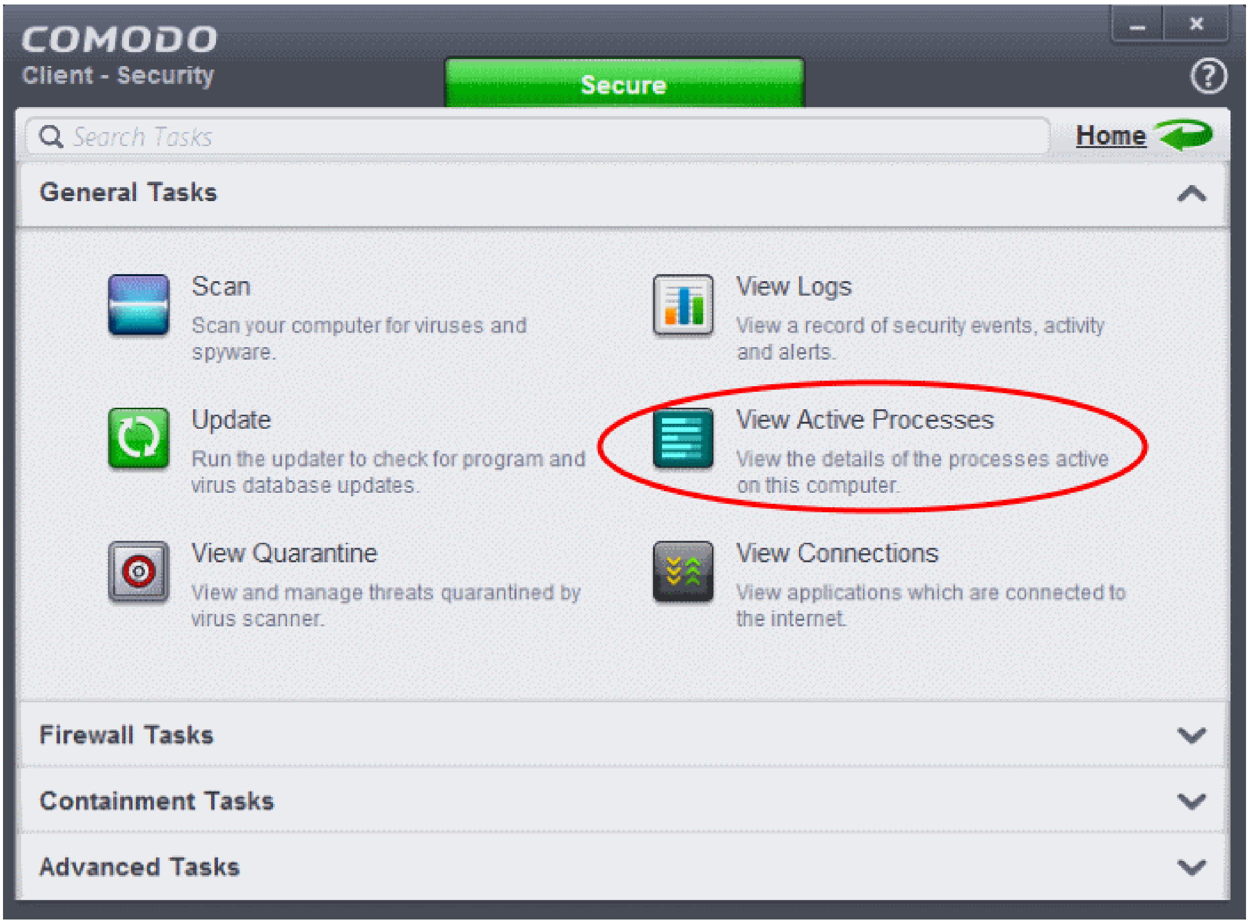
2.7. View Active Process List

The Active Process List interface displays all currently active processes initiated by applications that are currently running in your system. By tracing an application's parent process, CCS can detect whether a non-trusted application is attempting to spawn an already trusted application and thus deny access rights for that trusted application. This system provides the very highest protection against Trojans, malware and rootkits that try to use trusted software to launch an attack.

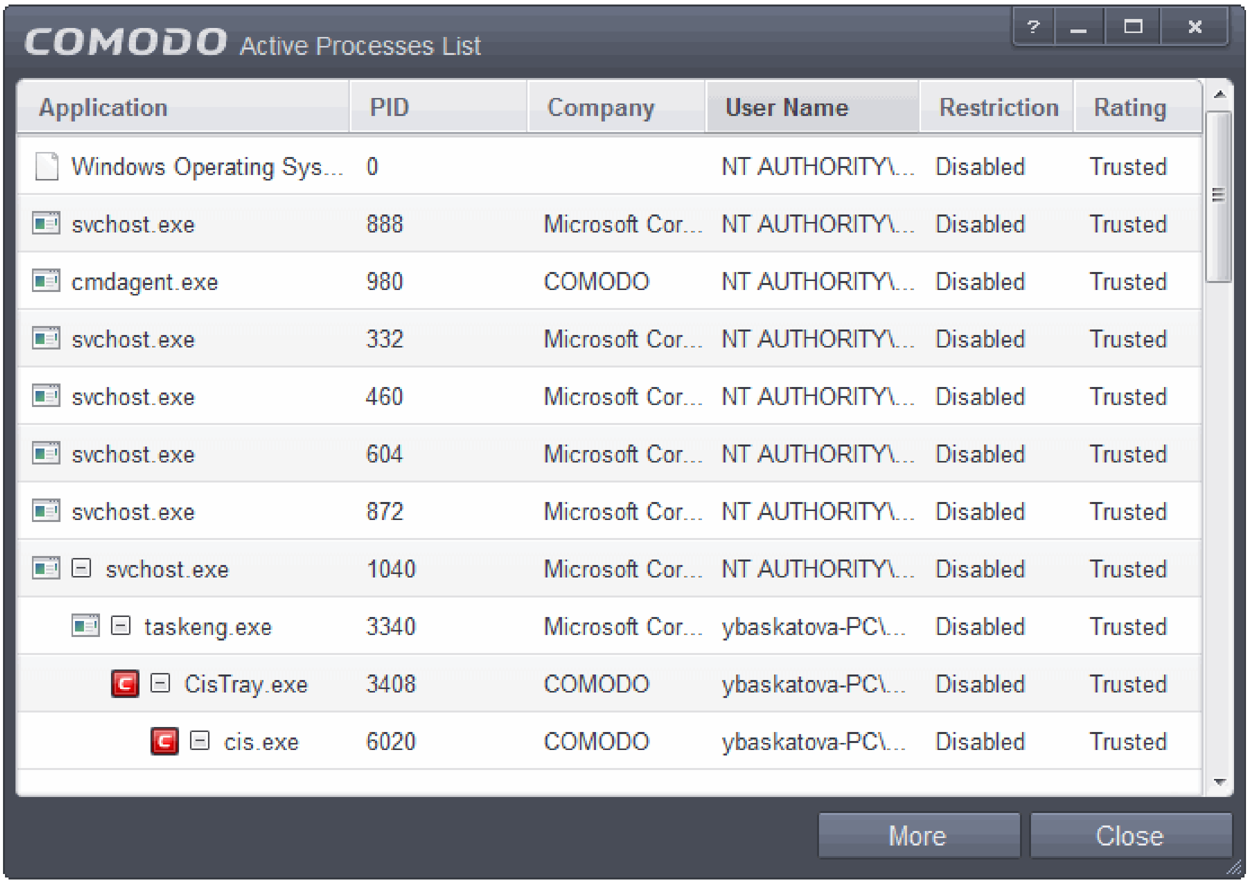
The interface also allows you to perform online lookup for the trustworthiness of the parent application, submit an application to Comodo for analysis, kill unwanted processes and more.

To view Active Process list

- Open the General Tasks interface and click 'View Active Processes'.


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
Firewall Tasks
Containment Tasks
Advanced Tasks

The 'Active Processes List' screen will be displayed.



COMODO Active Processes List

Application	PID	Company	User Name	Restriction	Rating
Windows Operating Sys...	0		NT AUTHORITY\...	Disabled	Trusted
svchost.exe	888	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
cmdagent.exe	980	COMODO	NT AUTHORITY\...	Disabled	Trusted
svchost.exe	332	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
svchost.exe	460	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
svchost.exe	604	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
svchost.exe	872	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
⊟ svchost.exe	1040	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
⊟ taskeng.exe	3340	Microsoft Cor...	ybaskatova-PC\...	Disabled	Trusted
⊟ CisTray.exe	3408	COMODO	ybaskatova-PC\...	Disabled	Trusted
⊟ cis.exe	6020	COMODO	ybaskatova-PC\...	Disabled	Trusted

Column Descriptions

- **Application** – Displays the names of applications that are currently running.
- **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 it's name.
- Show Contained Only: Displays the details of the contained programs only.

Tip: You can open the Active Process List screen that shows only the processes that are currently running inside the containment by clicking the process button from the CCS widget. Refer to the section Viewing Active Processes list of Contained Applications for more details.

- Add to Trusted Files: The selected unknown program is added to CCS File List with Trusted Status. Refer to the section 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. Refer to the section Identify and Kill Unsafe Processes for more details.

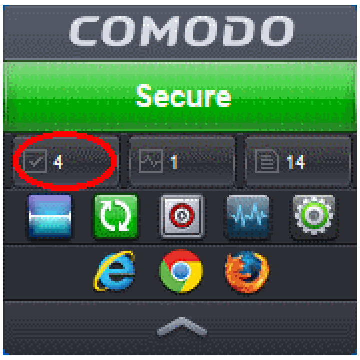
Viewing Active Processes list of Contained Applications

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:

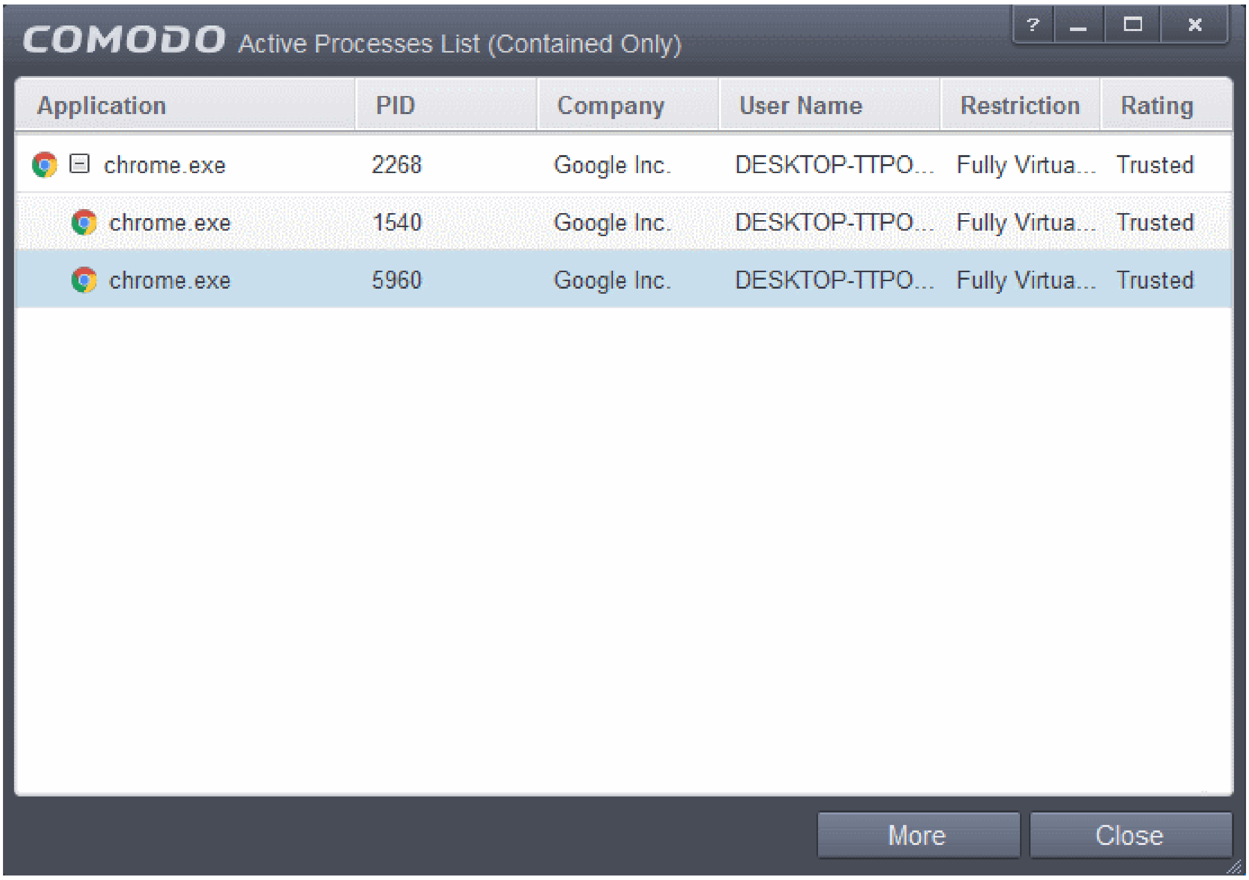
- Auto-Containment - Applications that are run inside the containment as per the rules defined for them or by default containment rules. Refer to the section Configuring Rules for Auto-Containment' for more details on defining auto-containment rules.
- Run Virtual - Applications that are selected and run in Containment. Refer to '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.
- Drag-and-drop applications on to CCS Home Screen - Click here for more details.
- Programs that are added manually - Refer to the section 'Configuring Rules for Auto-Containment' 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.



COMODO Active Processes List (Contained Only)

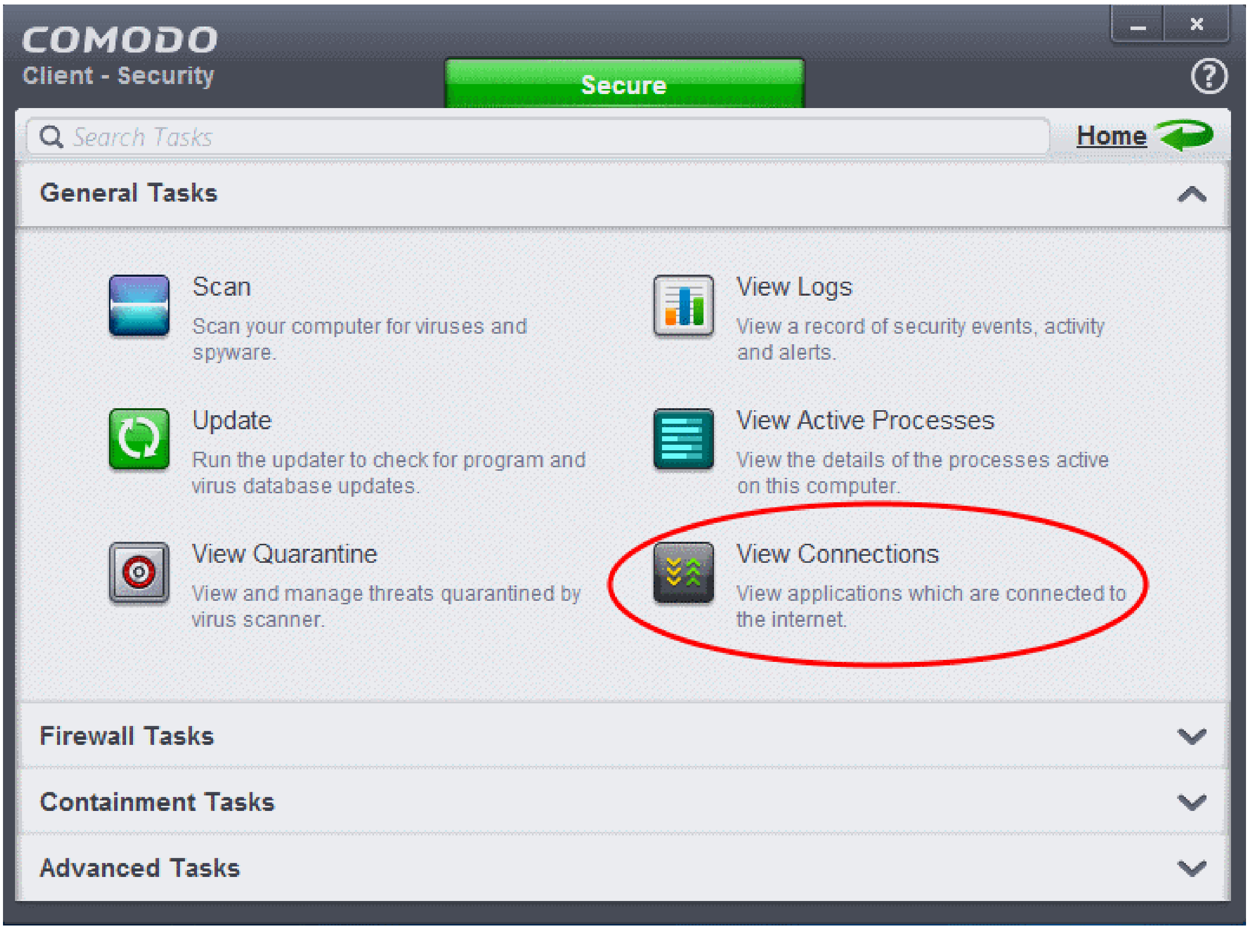
Application	PID	Company	User Name	Restriction	Rating
⊟ chrome.exe	2268	Google Inc.	DESKTOP-TTPO...	Fully Virtua...	Trusted
chrome.exe	1540	Google Inc.	DESKTOP-TTPO...	Fully Virtua...	Trusted
chrome.exe	5960	Google Inc.	DESKTOP-TTPO...	Fully Virtua...	Trusted

2.8. View Active Internet Connections

The 'View Connections' interface displays an 'at-a-glance' summary of all currently active Internet connections per-application. You can view all individual connections that each application is responsible for; the direction of the traffic; the source IP/port and the destination IP/port. You can also view 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 a connection. The 'View Connections' is extremely useful for testing firewall configuration, troubleshooting new firewall rules, monitoring individual applications and for terminating any unwanted connections.

The 'View Connections' interface can be accessed by clicking 'View Connections' from the 'General Tasks' interface.



General Tasks

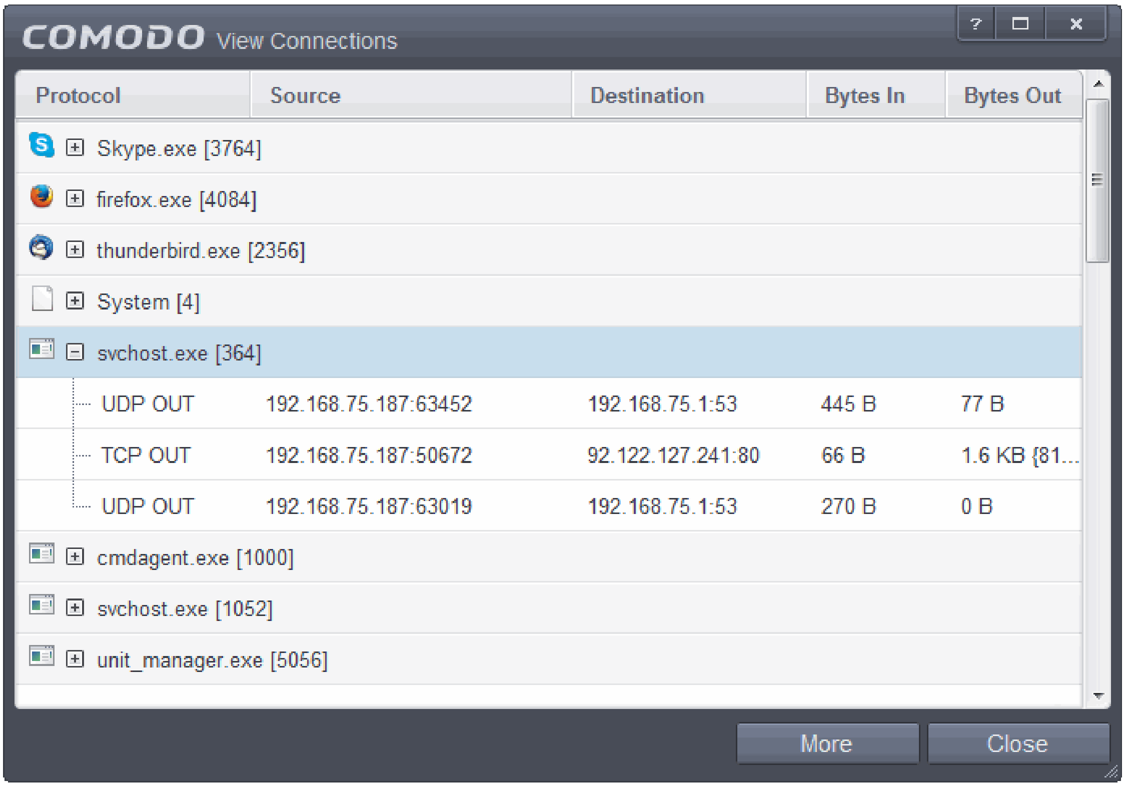
- Scan – Scan your computer for viruses and spyware.
- View Logs – View a record of security events, activity and alerts.
- Update – Run the updater to check for program and virus database updates.
- View Active Processes – View the details of the processes active on this computer.
- View Quarantine – View and manage threats quarantined by virus scanner.
- View Connections – View applications which are connected to the internet.

Firewall Tasks

Containment Tasks

Advanced Tasks

All currently active internet connections are shown in a tree structure:



Protocol	Source	Destination	Bytes In	Bytes Out
⊞ Skype.exe [3764]				
⊞ firefox.exe [4084]				
⊞ thunderbird.exe [2356]				
⊞ System [4]				
⊟ svchost.exe [364]				
UDP OUT	192.168.75.187:63452	192.168.75.1:53	445 B	77 B
TCP OUT	192.168.75.187:50672	92.122.127.241:80	66 B	1.6 KB {81...
UDP OUT	192.168.75.187:63019	192.168.75.1:53	270 B	0 B
⊞ cmdagent.exe [1000]				
⊞ svchost.exe [1052]				
⊞ unit_manager.exe [5056]				

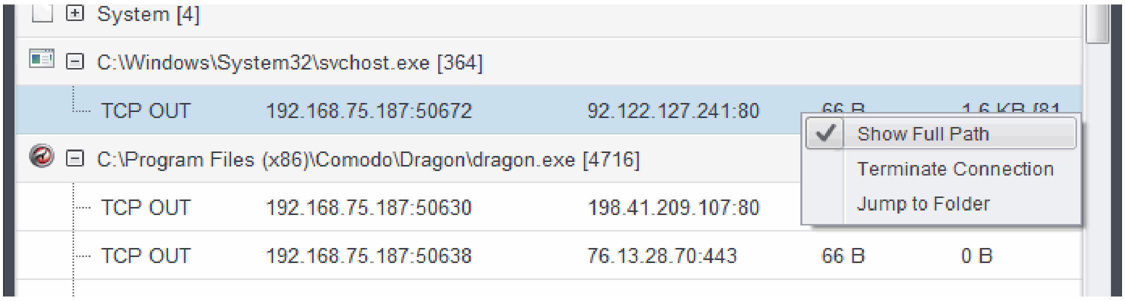
Column Descriptions

- **Protocol** - Shows the application that is connected, the protocol it is using and the direction of traffic. An application may have more than one connection at any time. Clicking + at the left of the application name expands the list of connections created.

- **Source (IP : Port)** - The IP and port that the application is connecting from. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** - The IP and port 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.



```
⊞ System [4]
⊟ C:\Windows\System32\svchost.exe [364]
   TCP OUT   192.168.75.187:50672   92.122.127.241:80    66 B   1.6 KB [81
⊟ C:\Program Files (x86)\Comodo\Dragon\dragon.exe [4716]
   TCP OUT   192.168.75.187:50630   198.41.209.107:80
   TCP OUT   192.168.75.187:50638   76.13.28.70:443      66 B   0 B
```

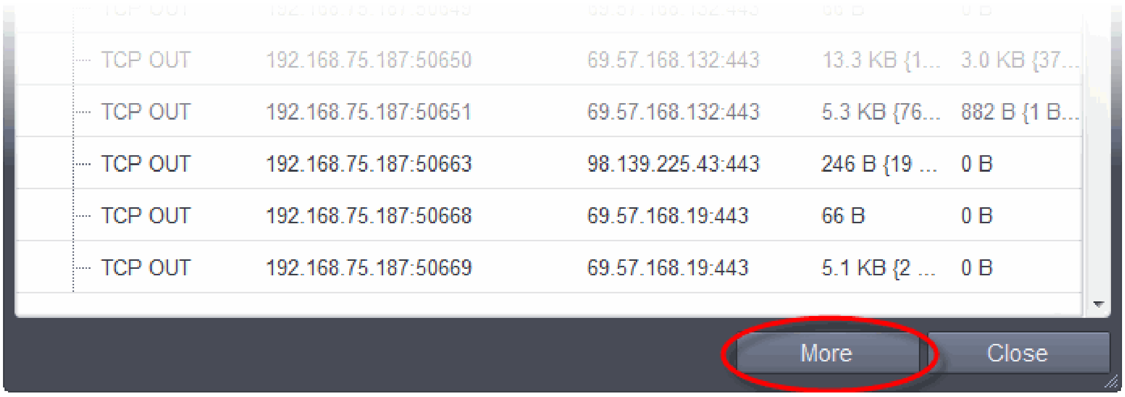
- If you wish to view the full path of the application, right click on the application name and select 'Show Full Path'.
- If you wish to terminate a connection, right click on the specific connection and click 'Terminate Connection'.
- If you wish to open the folder containing the executable file of the application, click 'Jump to Folder'.

Identify and Kill Unsafe Network Connections

KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes and network connections that are running on their system. 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.

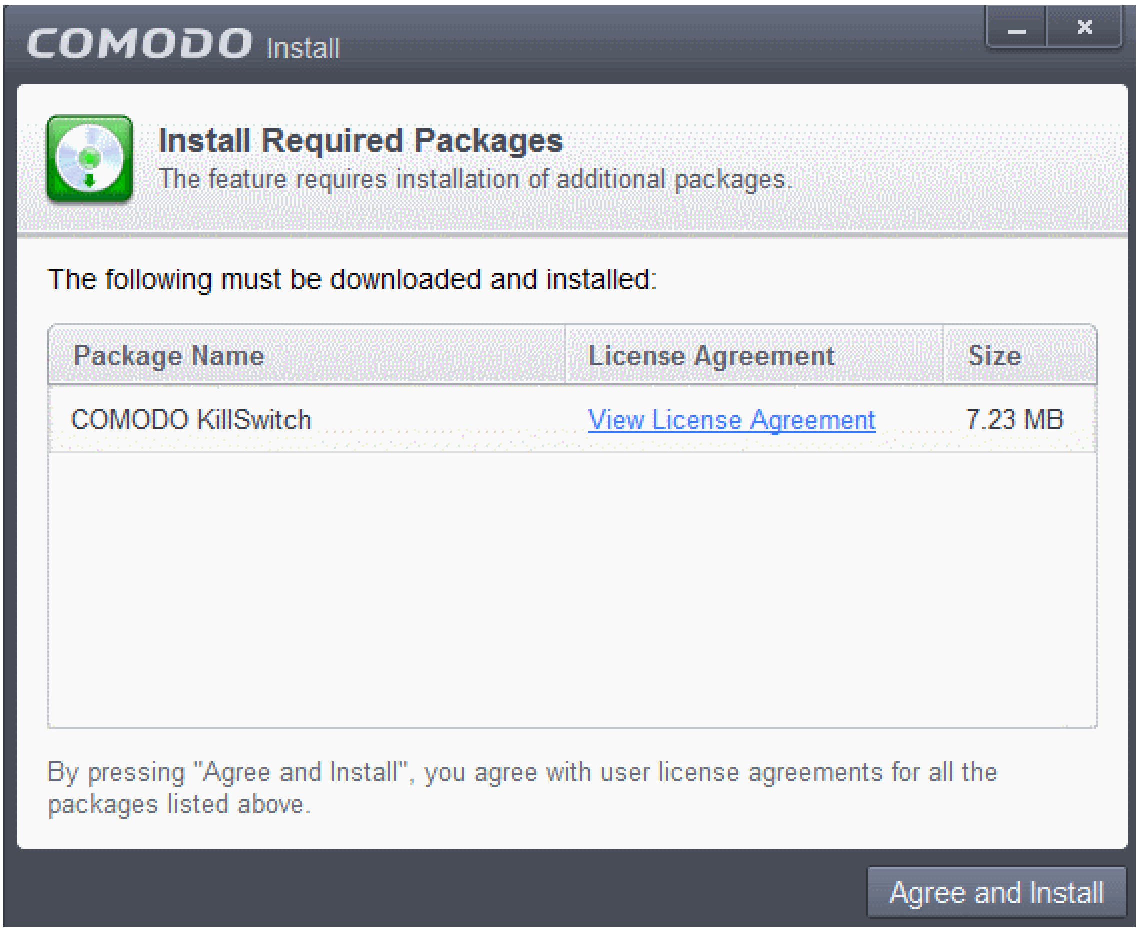
Comodo KillSwitch can show ALL running processes with their granular details– exposing even those that were invisible or very deeply hidden. It allows you to identify which of those running processes are unsafe and shut them all down with a single click. You can also use Killswitch to trace back to the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

Comodo KillSwitch can be directly accessed from the 'View Connections' by clicking the 'More' button.



```
TCP OUT   192.168.75.187:50649   69.57.168.132:443   66 B           0 B
TCP OUT   192.168.75.187:50650   69.57.168.132:443   13.3 KB {1...  3.0 KB {37...
TCP OUT   192.168.75.187:50651   69.57.168.132:443   5.3 KB {76...  882 B {1 B...
TCP OUT   192.168.75.187:50663   98.139.225.43:443   246 B {19 ...  0 B
TCP OUT   192.168.75.187:50668   69.57.168.19:443    66 B           0 B
TCP OUT   192.168.75.187:50669   69.57.168.19:443    5.1 KB {2 ...  0 B
```

If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the Kill switch interface. If not, CCS will download and install Comodo Killswitch.



Install Required Packages

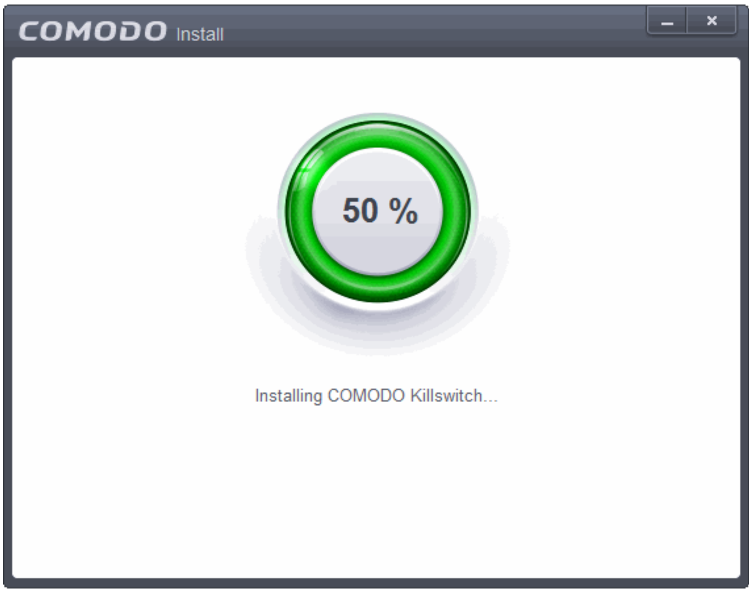
The feature requires installation of additional packages.

The following must be downloaded and installed:

Package Name	License Agreement	Size
COMODO KillSwitch	View License Agreement	7.23 MB

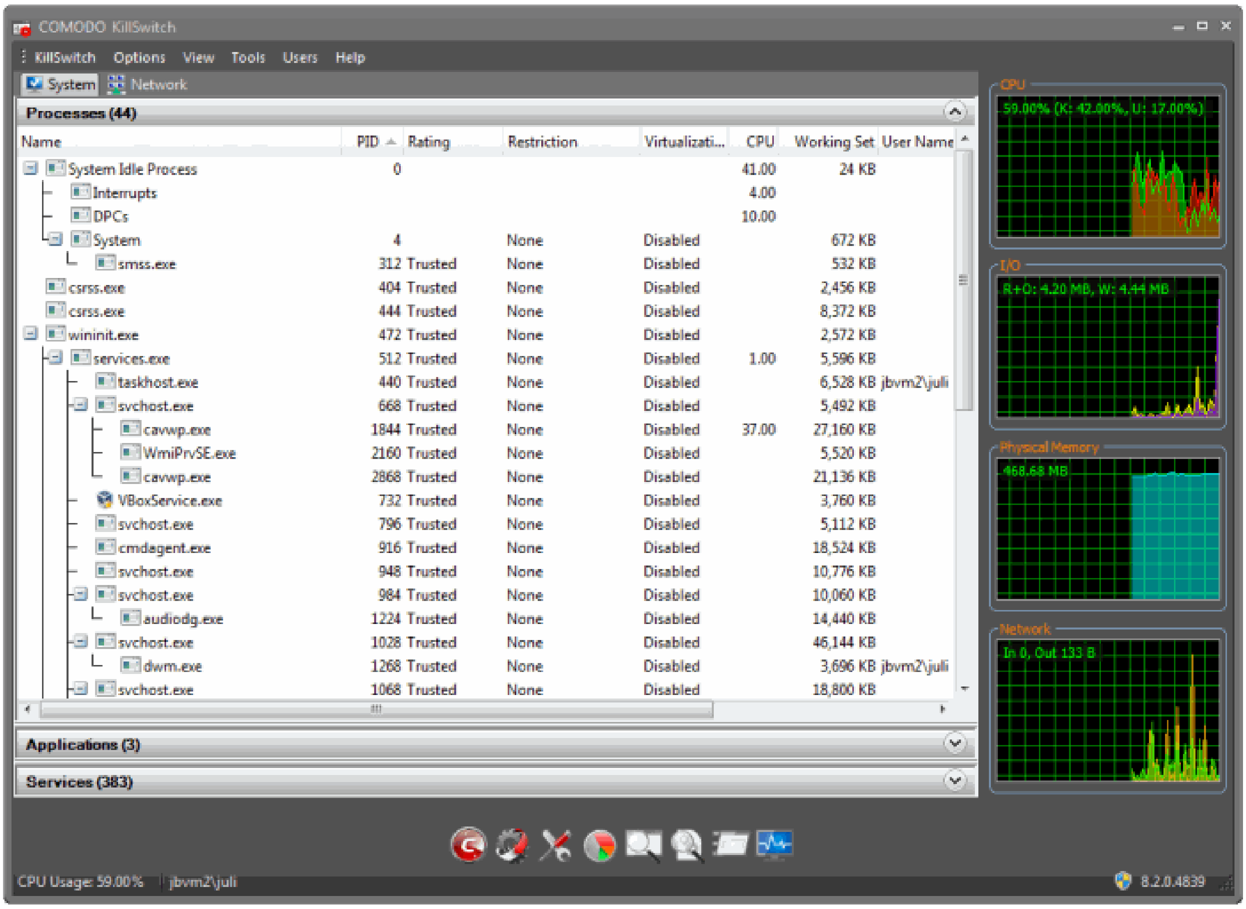
By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

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



Installing COMODO Killswitch...

After installation, the Comodo KillSwitch main interface will open. The main interface contains three panes - Processes, Applications and Services. Clicking the 'Network' tab will display the the Network Connections and Network Utilization panes.



Name	PID	Rating	Restriction	Virtualizati...	CPU	Working Set	User Name
System Idle Process	0				41.00	24 KB	
Interrupts					4.00		
DPCs					10.00		
System	4		None	Disabled		672 KB	
smss.exe	312	Trusted	None	Disabled		532 KB	
csrss.exe	404	Trusted	None	Disabled		2,456 KB	
csrss.exe	444	Trusted	None	Disabled		8,372 KB	
wininit.exe	472	Trusted	None	Disabled		2,572 KB	
services.exe	512	Trusted	None	Disabled	1.00	5,596 KB	
taskhost.exe	440	Trusted	None	Disabled		6,528 KB	jbvm2\juli
svchost.exe	668	Trusted	None	Disabled		5,492 KB	
cavwp.exe	1844	Trusted	None	Disabled	37.00	27,160 KB	
WmiPrvSE.exe	2160	Trusted	None	Disabled		5,520 KB	
cavwp.exe	2868	Trusted	None	Disabled		21,136 KB	
VBoxService.exe	732	Trusted	None	Disabled		3,760 KB	
svchost.exe	796	Trusted	None	Disabled		5,112 KB	
cmdagent.exe	916	Trusted	None	Disabled		18,524 KB	
svchost.exe	948	Trusted	None	Disabled		10,776 KB	
svchost.exe	984	Trusted	None	Disabled		10,060 KB	
audiodg.exe	1224	Trusted	None	Disabled		14,440 KB	
svchost.exe	1028	Trusted	None	Disabled		46,144 KB	
dwm.exe	1268	Trusted	None	Disabled		3,696 KB	jbvm2\juli
svchost.exe	1068	Trusted	None	Disabled		18,800 KB	

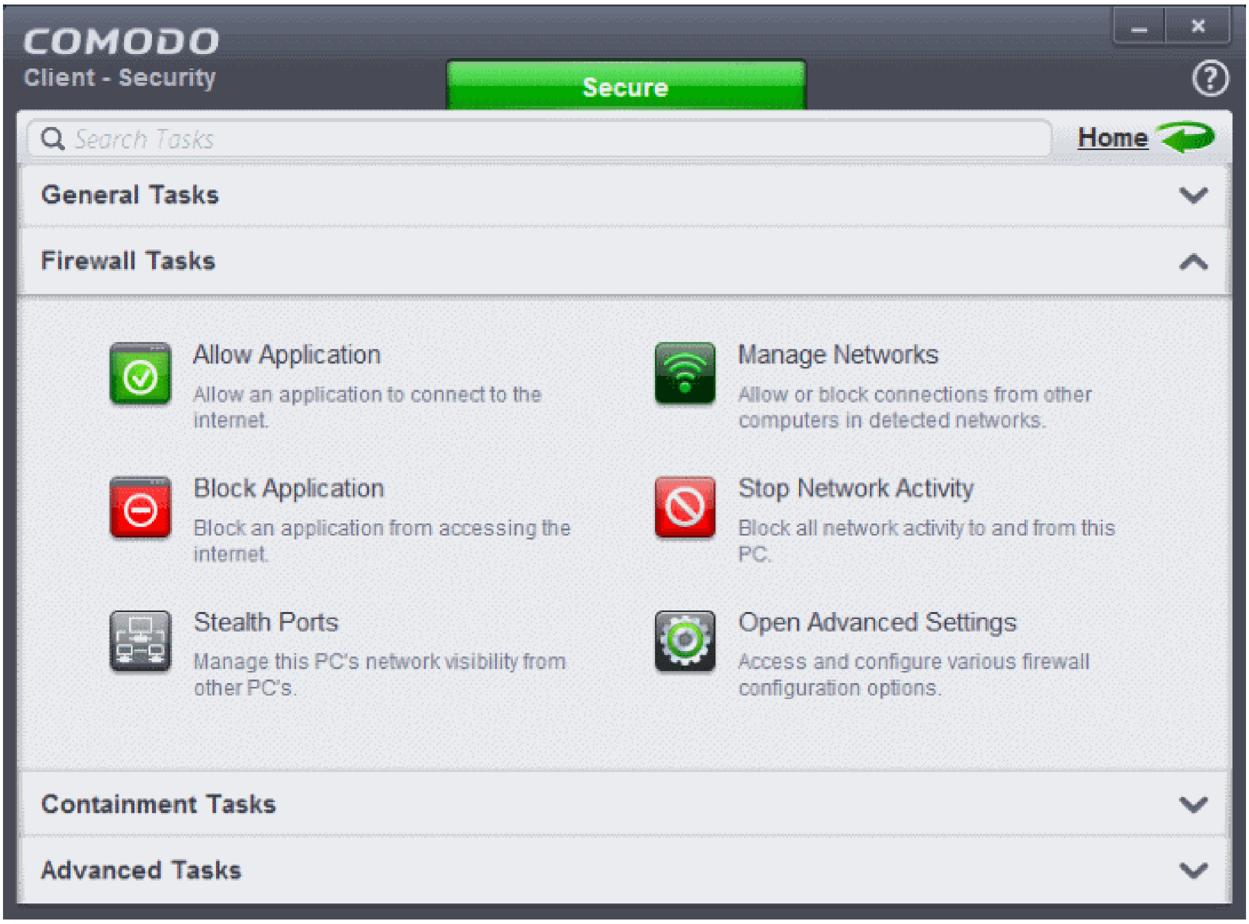
- Details of how to use KillSwitch to identify and terminate unsafe connections can be found at http://help.comodo.com/topic-119-1-328-3577-Viewing-and-Handling-Network-Connections-and-Usage.html.
- The complete user guide for Comodo KillSwitch is available at http://help.comodo.com/topic-119-1-328-3518-Introduction-to-KillSwitch.html.

3.Firewall Tasks - Introduction

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

It can be accessed at all times by clicking on the 'Firewall Tasks' band from the 'Tasks' interface.

The Firewall Tasks area provides easy access to all major features and settings. From here, you can configure Internet access rights per-application, stealth your computer ports, manage available networks and even block all network traffic in and out of your computer. In 'Advanced Settings' you'll be able to specify overall firewall behavior and configure advanced settings such as application rules, rulesets, network zones and port sets.



Allow Application
Allow an application to connect to the internet.

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

Block Application
Block an application from accessing the internet.

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

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

Open Advanced Settings
Access and configure various firewall configuration options.

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

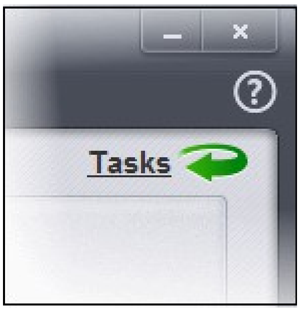
- Allow or block Internet access to applications selectively
- Stealth your computer ports
- Manage network connections
- Stop all network activity
- Advanced firewall settings

3.1. Allow or Block Internet Access to Applications Selectively

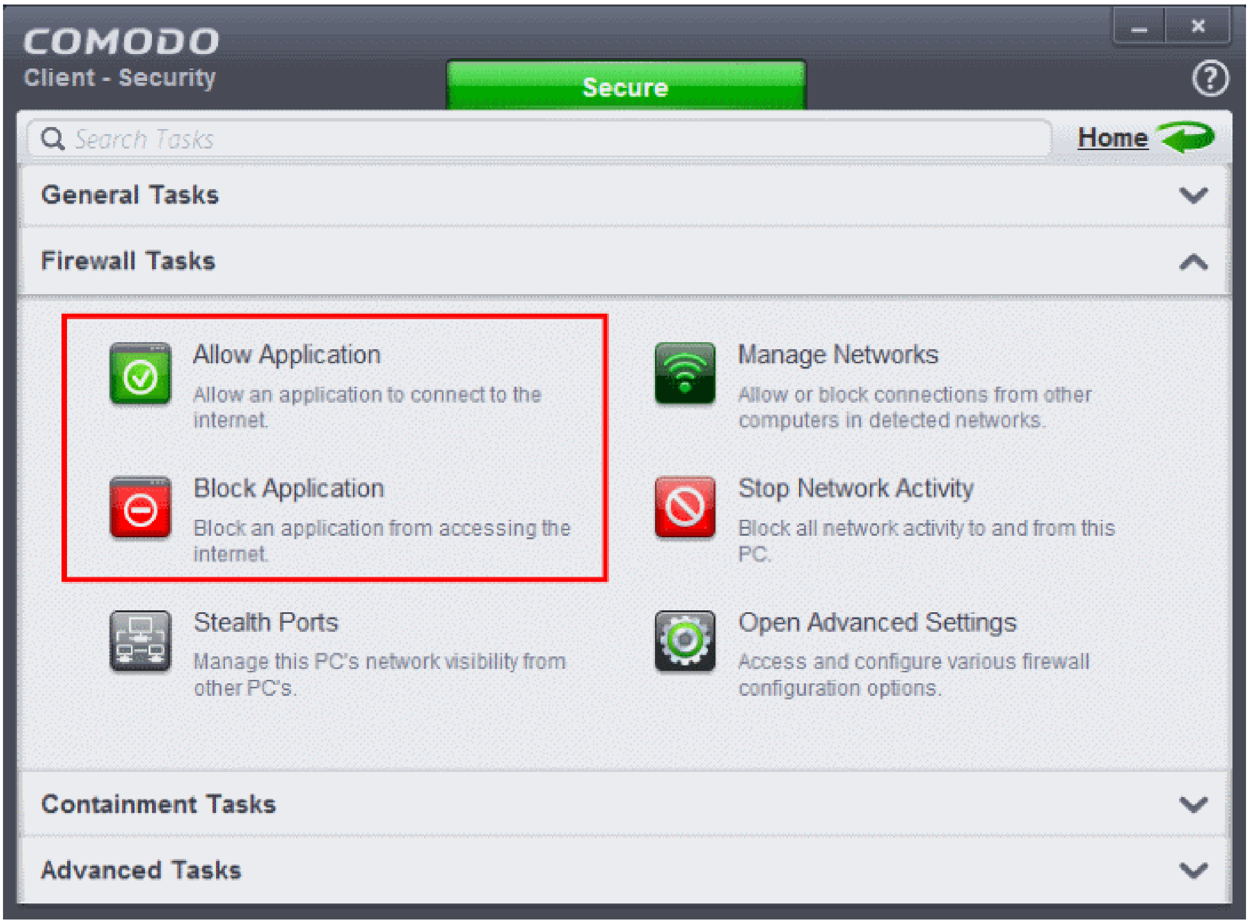
The Firewall Tasks interface allows you to selectively allow or block certain applications from accessing the Internet. These shortcuts represent a convenient way to create an automatic 'Allow Requests' rule or 'Block Requests' rule for individual applications - meaning that inbound and outbound connections are automatically permitted or not permitted to these applications respectively.

To open the 'Firewall Tasks' interface

- Click the 'Tasks' arrow from the CCS home screen:



- Click on the 'Firewall Tasks' band from the 'Tasks' interface:


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Allow Application
Allow an application to connect to the internet.
Block Application
Block an application from accessing the internet.
Stealth Ports
Manage this PC's network visibility from other PC's.
Manage Networks
Allow or block connections from other computers in detected networks.
Stop Network Activity
Block all network activity to and from this PC.
Open Advanced Settings
Access and configure various firewall configuration options.
Containment Tasks
Advanced Tasks

To allow an application to access to the Internet:

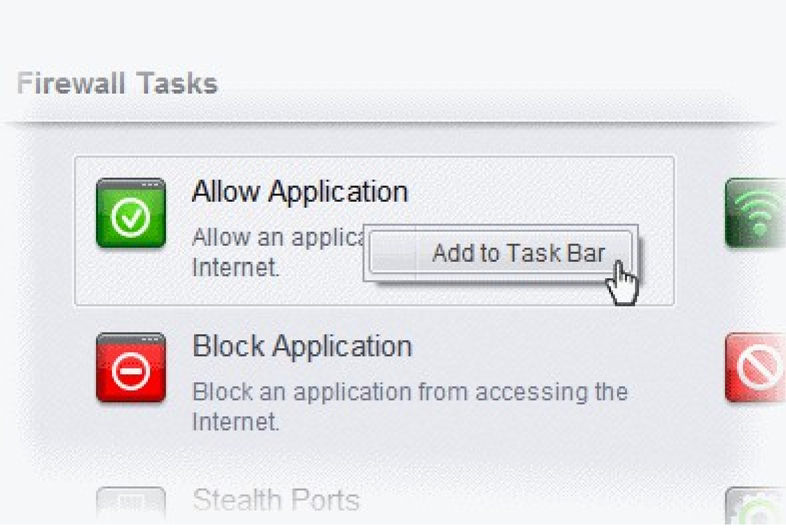
- Click the 'Allow Application' button from the 'Firewall Tasks' interface.
- Navigate to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to allow Internet access to the selected application.

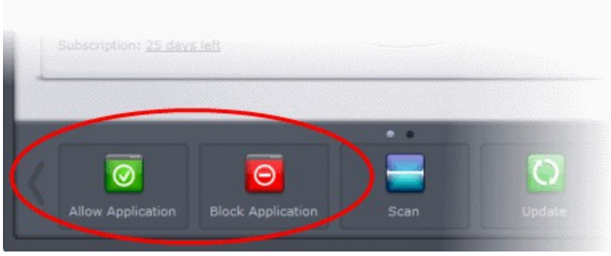
To block an application's Internet access rights

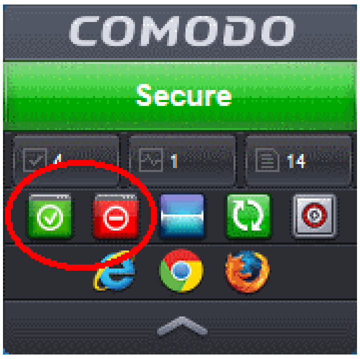
- Click the 'Block Application' button from the 'Firewall Tasks' interface.
- Browse to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to prohibit Internet access to the selected application.

The advanced application rules interface can be accessed by clicking 'Tasks' from the CCS home screen > Firewall Tasks > Open Advanced Settings > Application rules. The application you just allowed or blocked should be listed here. For further information on application rules governing Internet access rights, see Application Rules.

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







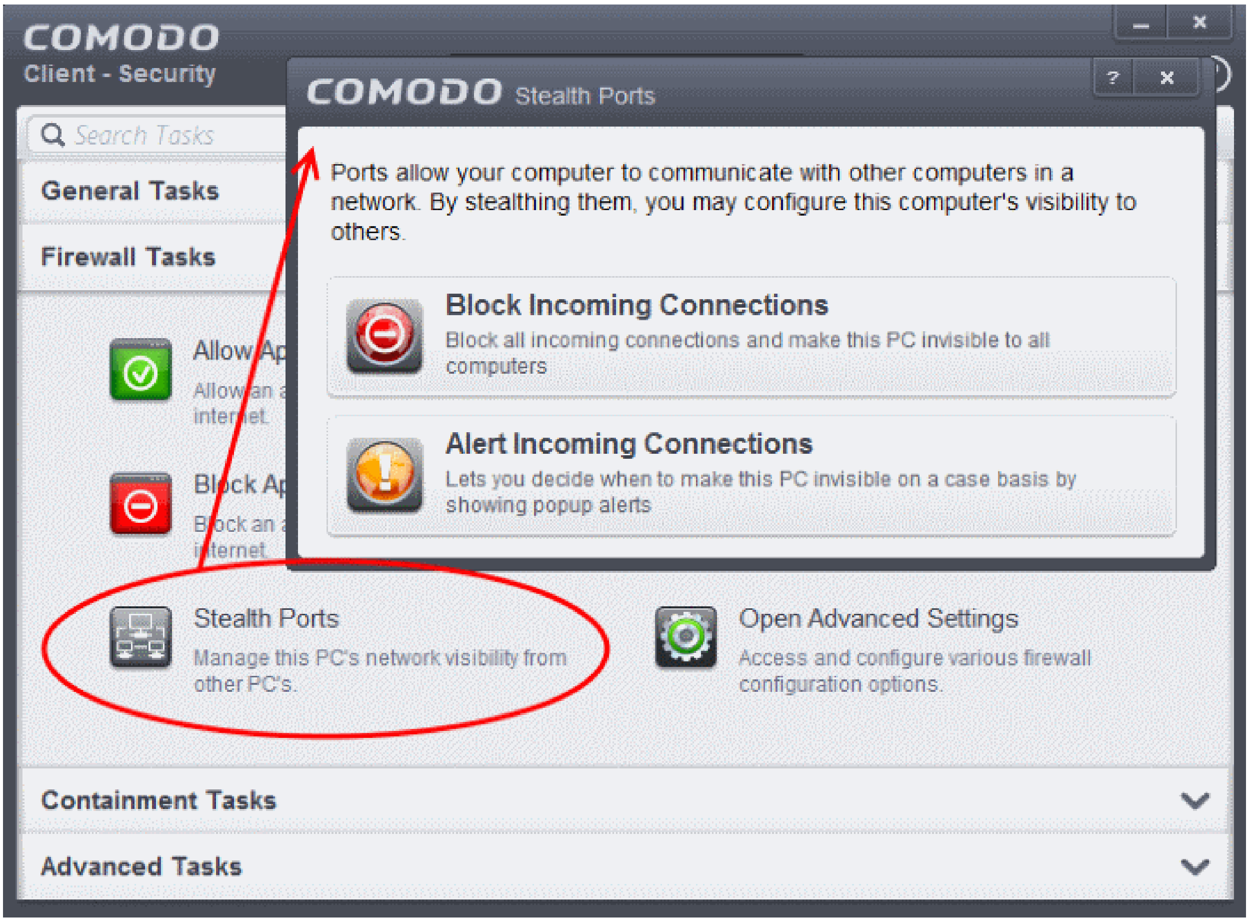
3.2. Stealth your Computer Ports

Port Stealthing is a security feature whereby ports on an Internet connected PC are hidden from sight, evoking no response to opportunistic port scans.

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 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 presumes it is offline and move on to other targets. You can still be able to connect to Internet and transfer information as usual but remain invisible to outside threats.

- Click on 'Stealth Ports' link in Firewall Tasks: \



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

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

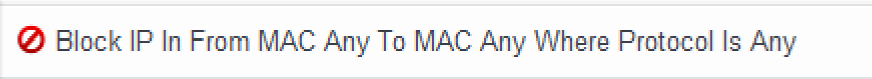
Alert Incoming Connections
Lets you decide when to make this PC invisible on a case basis by showing popup alerts

You have two options to choose from:

Block Incoming Connections

Selecting this option makes your computer's ports 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) finds this option the more convenient and secure. You are not alerted when the incoming connection is blocked, but the rule adds an entry in 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

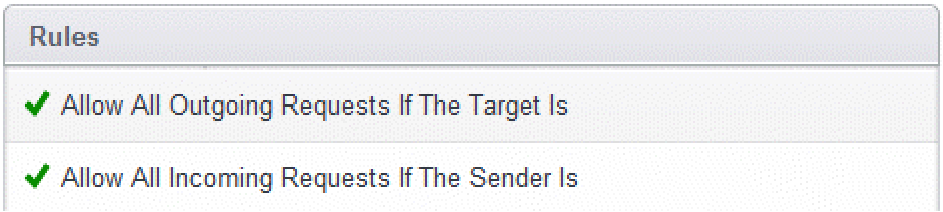
If you would like more information on the meaning and construction of rules, please click here.

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



Rules

✓ Allow All Outgoing Requests If The Target Is

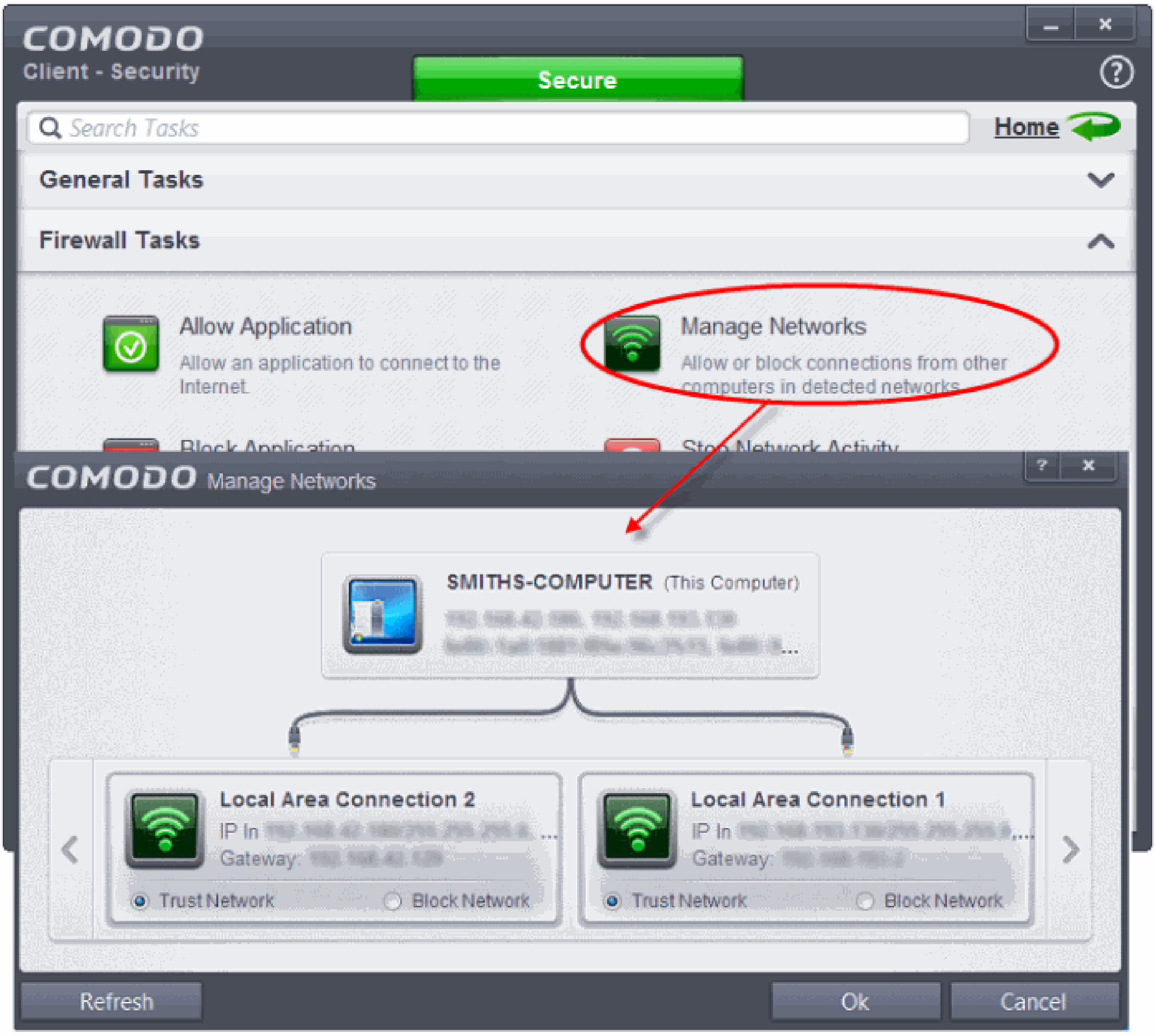
✓ Allow All Incoming Requests If The Sender Is

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.

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

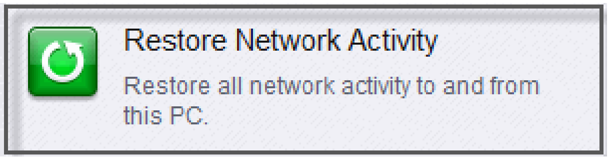


- The 'Manage 'Networks' interface can be opened by clicking 'Tasks > Firewall Tasks > Manage Networks'.

- To view, create or block **Network Zones**, click 'Tasks > Firewall Tasks > Open Advanced Settings > Network Zones'.

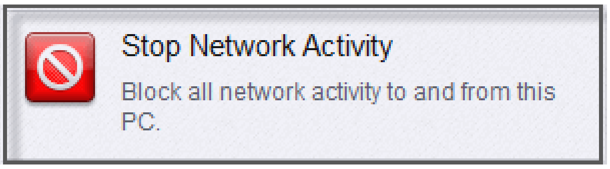
3.4. Stop all Network Activities

As the name suggests, the 'Stop all network activity' button instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and all available networks (including the Internet). Connections will remained 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 to unplug any network cables.



Restore Network Activity

Restore all network activity to and from this PC.



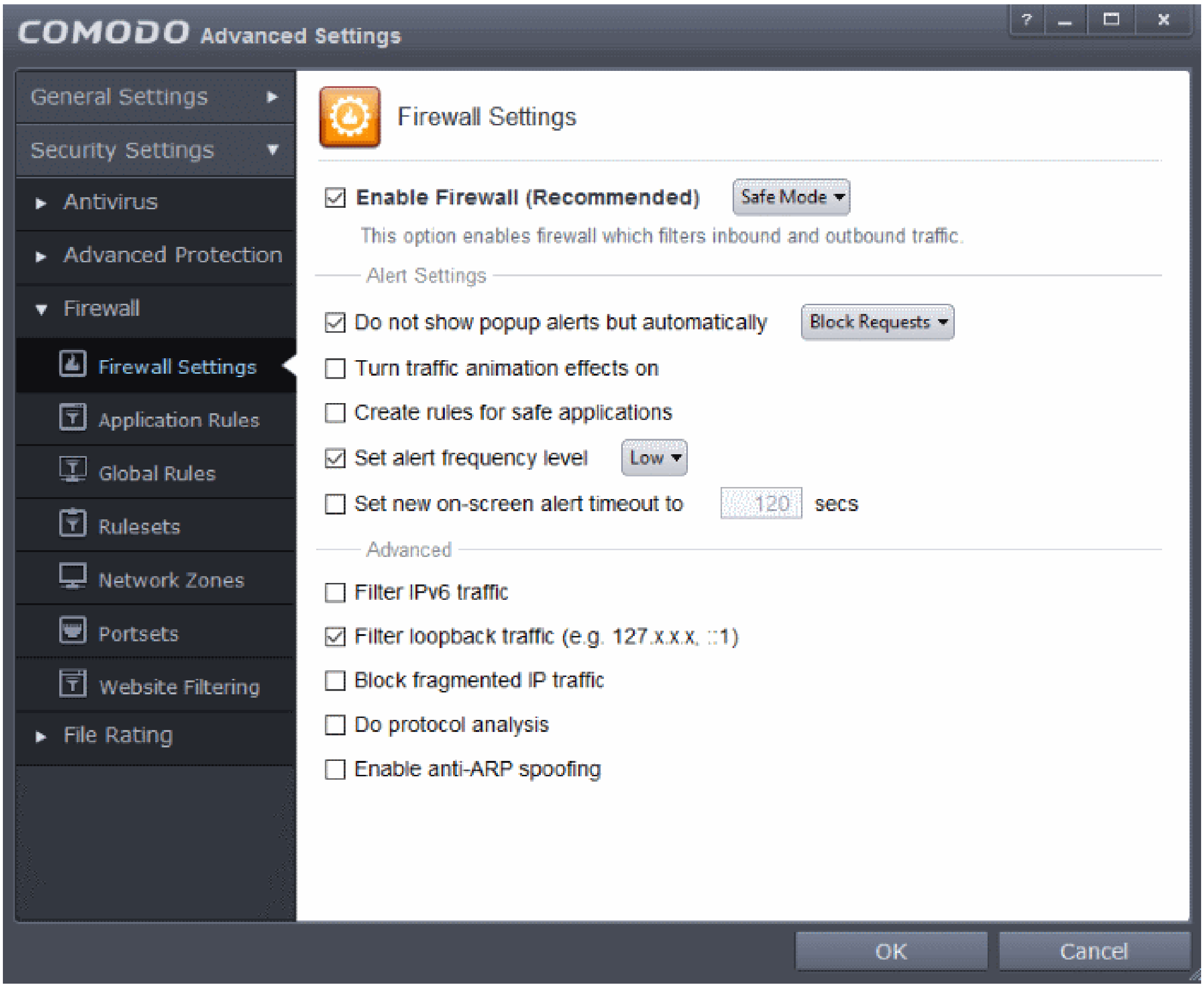
Stop Network Activity

Block all network activity to and from this PC.

- Access the network activity 'on/off' button by clicking Tasks > Firewall Tasks
- Disconnect your computer from all networks by clicking 'Stop All Activity' (button will be red)
- Re-enable connectivity by clicking 'Restore All Activity' (button will be green)
- 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. Advanced Firewall Settings

The 'Advanced Settings' area is the nerve center of Comodo Firewall and allows advanced users to configure and deploy traffic filtering rules and policies on an application specific and global basis. To open the interface, click 'Tasks' on the home screen followed by 'Open Advanced Settings' then 'Firewall Settings':



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do not show popup alerts but automatically Block Requests

□ Turn traffic animation effects on

□ Create rules for safe applications

☑ Set alert frequency level Low

□ Set new on-screen alert timeout to 120 secs

Advanced

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

□ Block fragmented IP traffic

□ Do protocol analysis

□ Enable anti-ARP spoofing

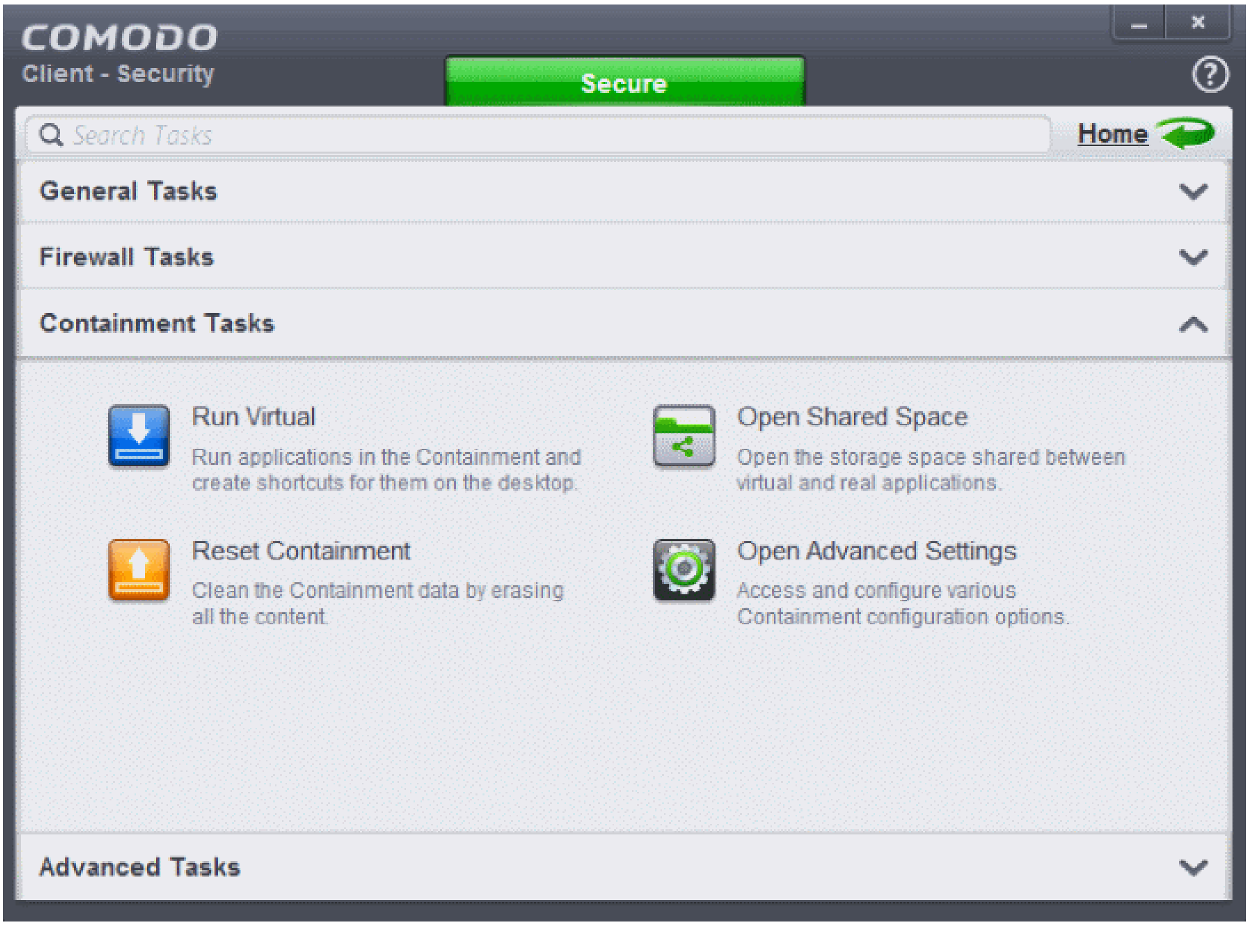
The interface is divided into seven main sections. Click the links below to jump to more details on each section:

- The Firewall Settings area allows you to configure the security of your computer and the frequency of alerts that are generated.
- The Application Rules area allows users to view, manage and define the network and Internet access rights of applications on your system.
- The Global Rules area allows users view, manage and define overall Firewall ruleset that applies to your computer and is independent of application rules.
  - Both application rules and global rules are consulted when the firewall is determining whether or not to allow or block a connection attempt.
  - For Outgoing connection attempts, the application rules are consulted first and then the global rules.
  - For Incoming connection attempts, the global rules are consulted first and then application specific rules.
- The Rulesets area contains a list of preset Firewall rules that can be re-used and applied to multiple applications. For example, there is a 'Browser' rule, an 'Email Client' rule and rules for 'Trusted' and 'Blocked' applications.
- The Network Zones area allows you to group IP addresses and ranges into named zones. Once defined, privileges and rules can be applied to these zones in other areas of CCS. For example, global and application rules can be applied to network zones. This interface also allows you to block network zones.

- The **Portsets** area contains groups of important / regularly used port numbers that can be easily selected as part of a global or application rule.
- The **Website Filtering** area allows you to create website filtering rules which let you determine which sites certain users can or cannot access.

4. Containment Tasks - An Introduction

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


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Containment Tasks
Run Virtual
Run applications in the Containment and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset Containment
Clean the Containment data by erasing all the content.
Open Advanced Settings
Access and configure various Containment configuration options.
Advanced Tasks

The Containment Tasks interface has shortcuts for the following tasks:

- **Run Virual** - Allows you to run individual applications in the container.
- **Reset Containment** - Allows you to clear all data written by programs run inside the container.
- **Open Shared Space** - Opens the folder 'Shared Space' which is shared by your host operating system and the applications running inside the container. The folder is created at the location 'C:\Documents and Settings\All Users\Application Data\Shared Space'.
- **Open Advanced Settings** – Access advanced auto-containment settings interface, add programs that should always run inside the container and create new auto-containment rules. This is covered in the 'Configuring Rules for Auto-Containment' section of 'Advanced Settings'.

4.1. Run an Application in the Container

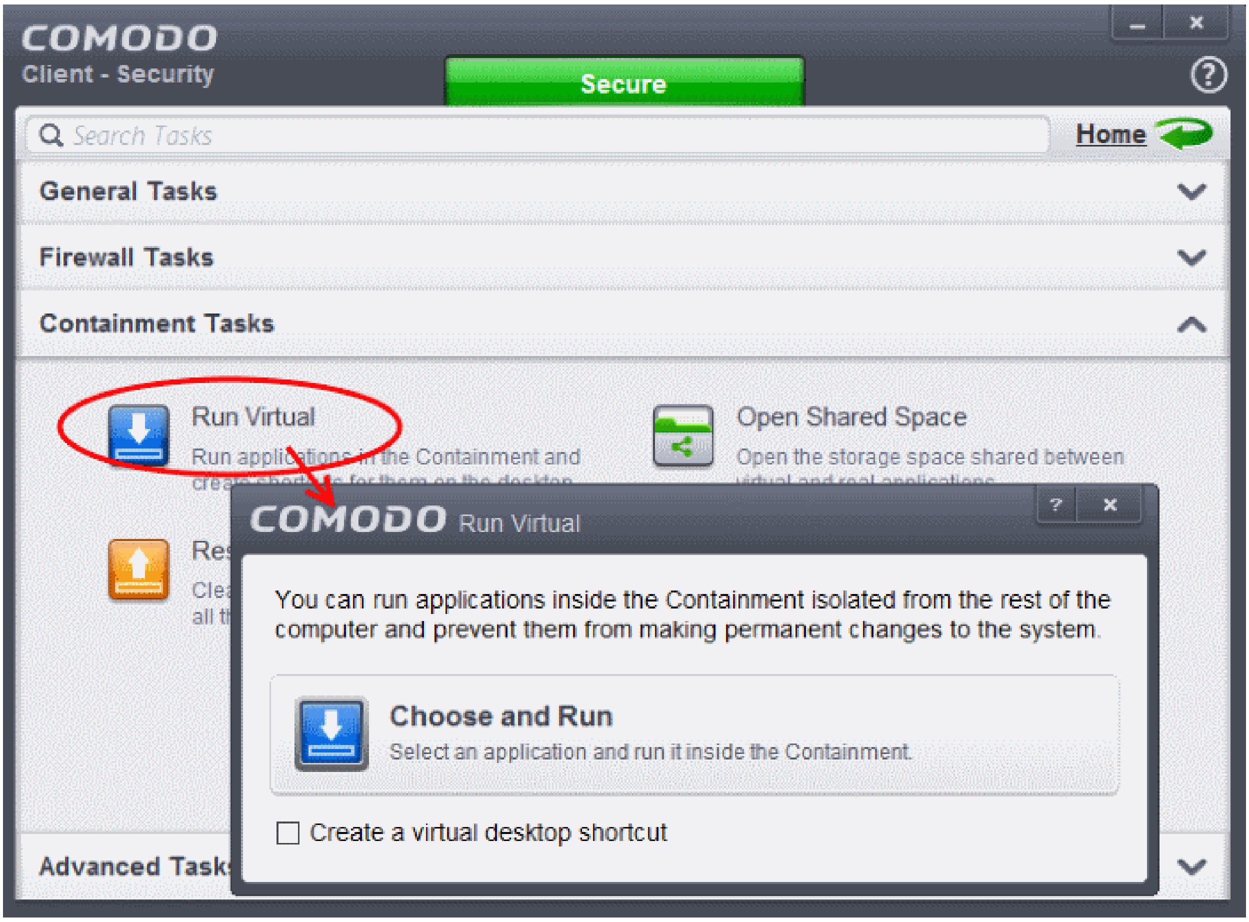
Comodo Client Security allows you to run programs in containment on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. Adding a program in this way means that it will run in the container this time only. On subsequent executions it will not run outside the container (presuming an auto- containment rule has not been created for it).

You can also create a desktop shortcut to run the application inside the containment on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:

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

To run an application in the container

1. Open the 'Containment Tasks' interface and Click 'Run Virtual'.
2. The 'Run Virtual' dialog will be displayed.

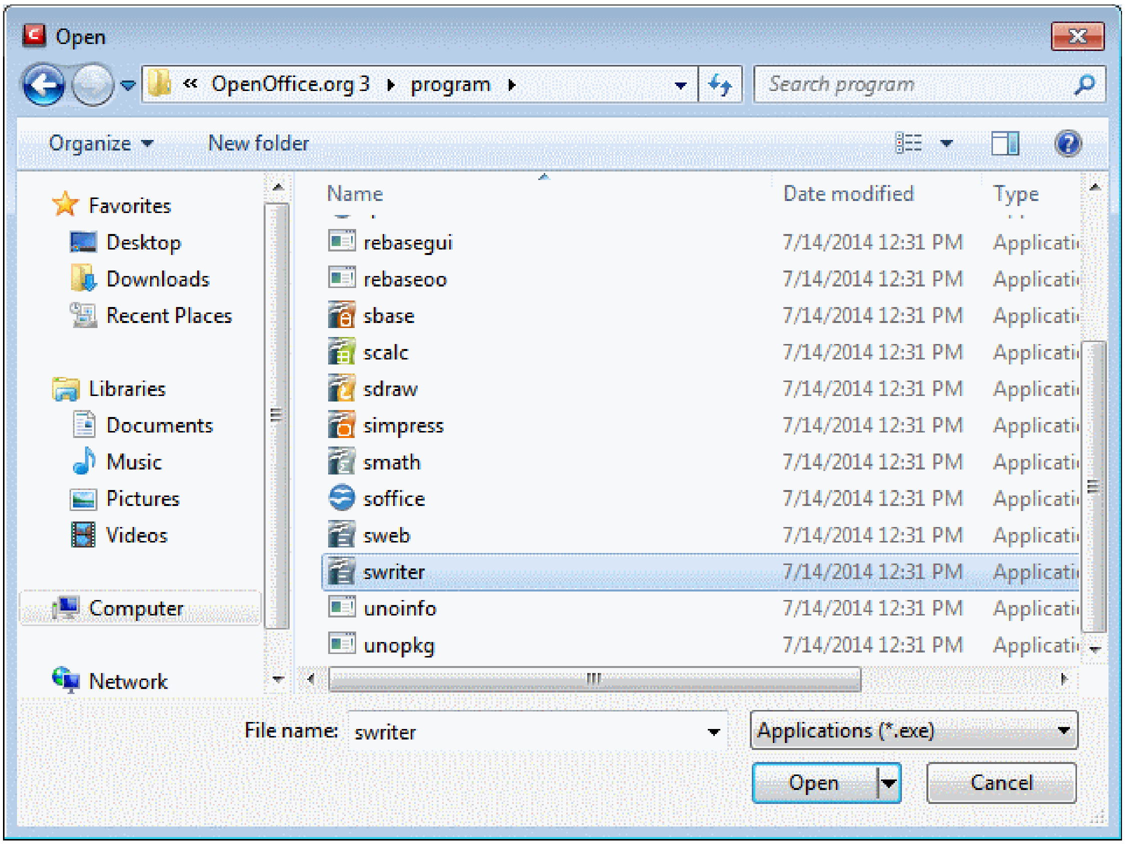


You can run applications inside the Containment isolated from the rest of the computer and prevent them from making permanent changes to the system.

Choose and Run
Select an application and run it inside the Containment.

☐ Create a virtual desktop shortcut

3. To run an application inside the container, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is contained. If you wish to run the application in the container in future, then select 'Create a virtual desktop shortcut'.


Open
« OpenOffice.org 3 ▸ program ▸
Search program
Organize ▾
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
rebasegui 7/14/2014 12:31 PM Applicati
rebaseoo 7/14/2014 12:31 PM Applicati
sbase 7/14/2014 12:31 PM Applicati
scalc 7/14/2014 12:31 PM Applicati
sdraw 7/14/2014 12:31 PM Applicati
simpress 7/14/2014 12:31 PM Applicati
smath 7/14/2014 12:31 PM Applicati
soffice 7/14/2014 12:31 PM Applicati
sweb 7/14/2014 12:31 PM Applicati
swriter 7/14/2014 12:31 PM Applicati
unoinfo 7/14/2014 12:31 PM Applicati
unopkg 7/14/2014 12:31 PM Applicati
File name: swriter
Applications (*.exe)
Open
Cancel

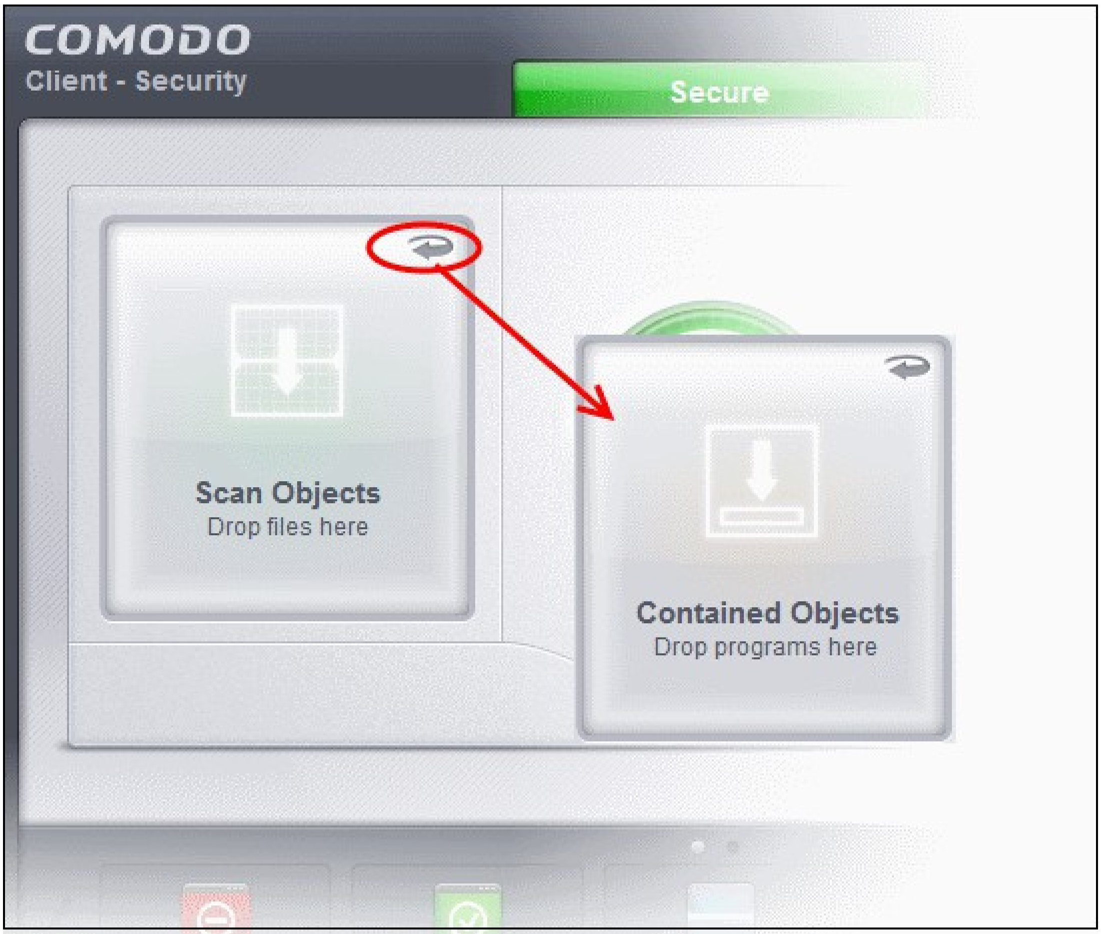
4. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

Alternatively, you can run an application inside the container by the following shortcut methods:

- By dragging-and-dropping the application on to CCS Home screen
- From the context sensitive menu
- Running browsers inside the container

Drag-and-drop the application on to CCS Home Screen

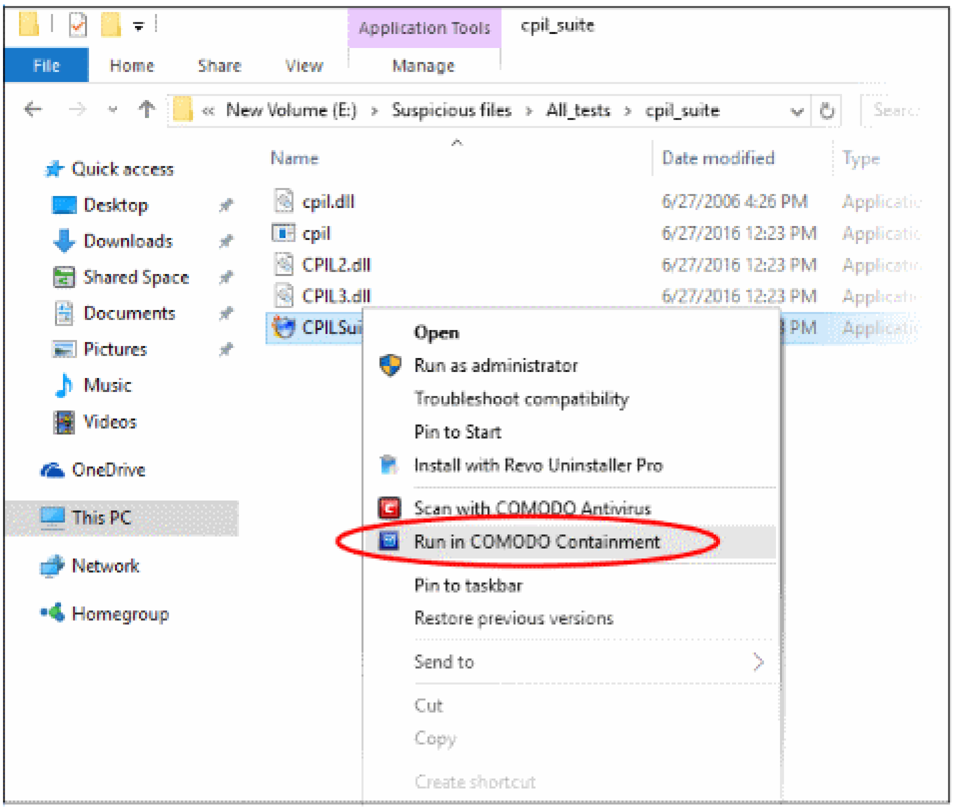
The Home screen of the CCS interface has a flippable pane at the left side allowing you to run instant scans or run a program in the container. To flip the pane to carry out these tasks, just click the curved arrow at the top right side of the pane.



- To run a program in a contained environment, first flip the pane by clicking the curved arrow at the top right side to display 'Contained Objects'.
- Now, navigate to the program in your system that you want to run in contained environment and just drag and drop into the box.

Running a program from the context sensitive menu

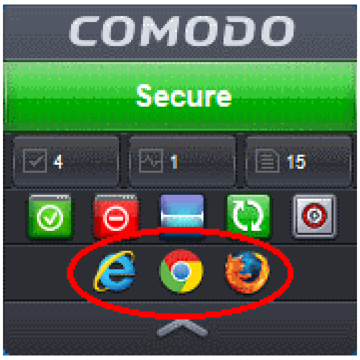
- Navigate to the program in your system that you want to run in contained environment and right click on it



- Choose 'Run in Comodo Containment' from the context sensitive menu.

Running Browsers inside the Container

The CCS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- Clicking on a browser icon will start the browser inside the containment.

The browser will be started and executed inside the container at 'Contained' level. CCS displays a green border around the windows of programs to indicate that they are running inside the contained environment, if the setting 'Show highlight frame for contained applications' is enabled in Configure the Containment Settings

The application will run in the container on this occasion only. If you often want the browser to run inside the contained environment then create a 'virtual shortcut' for the application by selecting the check-box 'Create a virtual desktop shortcut' in step 3. If you wish to run an application in the container on a long-term/permanent basis then Configuring Rules for Auto-Containment.

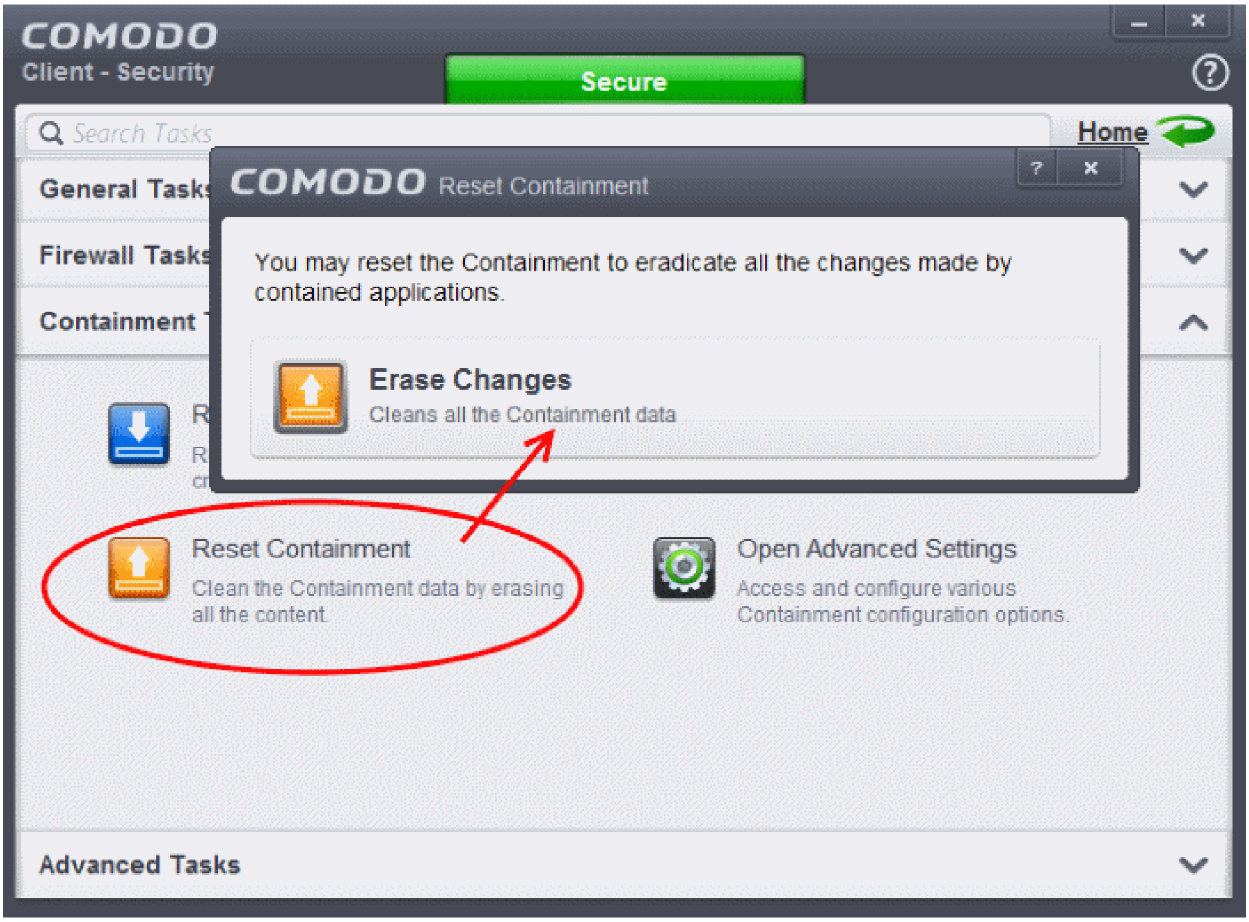
4.2. Reset the Container

Programs running inside the container write all saved data and system changes inside the container itself so they do not affect your real system. Items stored in the container could, depending on your usage patterns, contain malware downloaded from websites or private data in your browsing history. Periodically resetting the container will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time then resetting the container will also help the contained environment operate more smoothly.

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

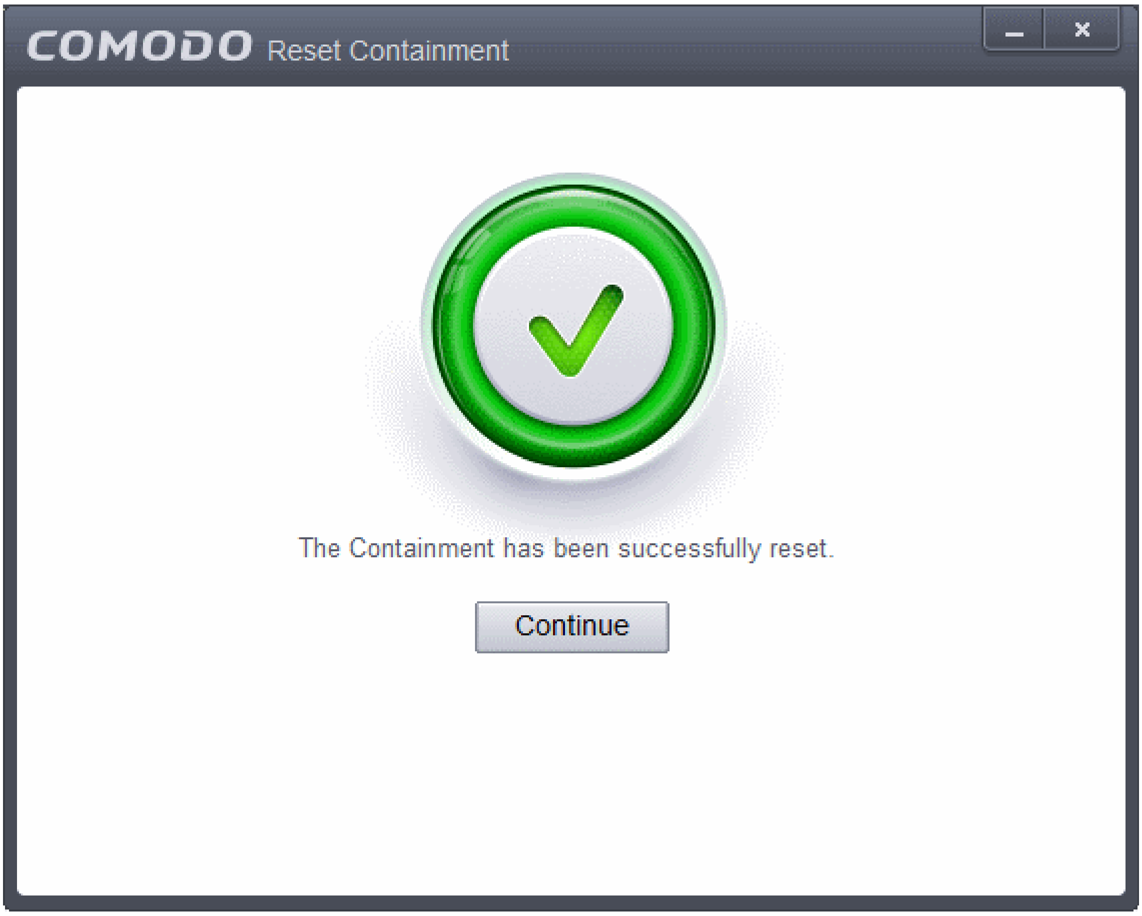
To clear the container

- Click on the 'Containment Tasks' bar from the Tasks interface and then click 'Reset Containment'
- The 'Reset Containment' dialog will appear.



You may reset the Containment to eradicate all the changes made by contained applications.

- Click 'Erase Changes'. The contents in the container will be deleted immediately.

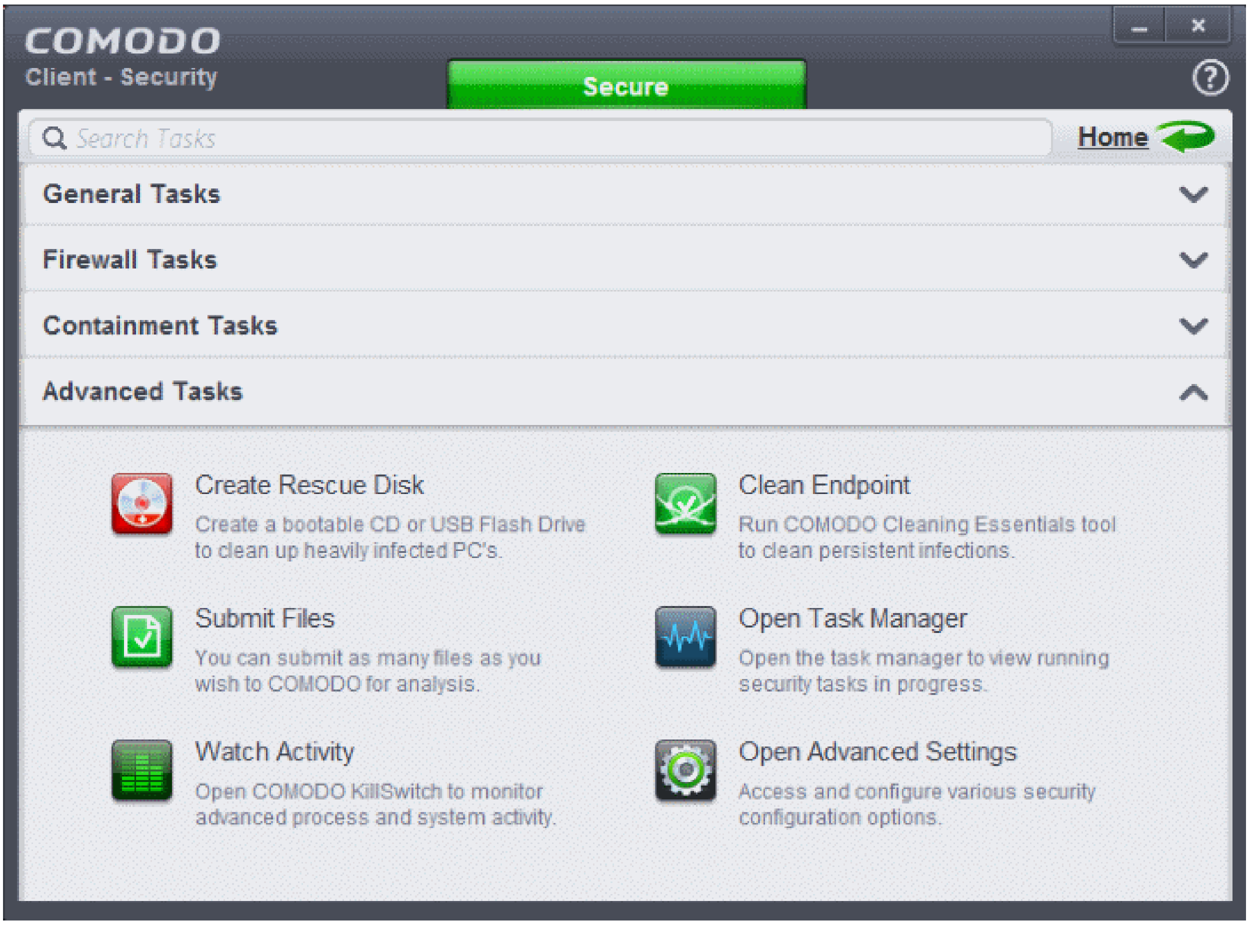


The Containment has been successfully reset.

- Click 'Continue' to close the dialog.

5. Advanced Tasks - Introduction

The 'Advanced Tasks' area allows you modify the overall configuration of CCS and to take advantage of several other Comodo utilities.



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

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

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

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

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

Open Advanced Settings
Access and configure various security configuration options.

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

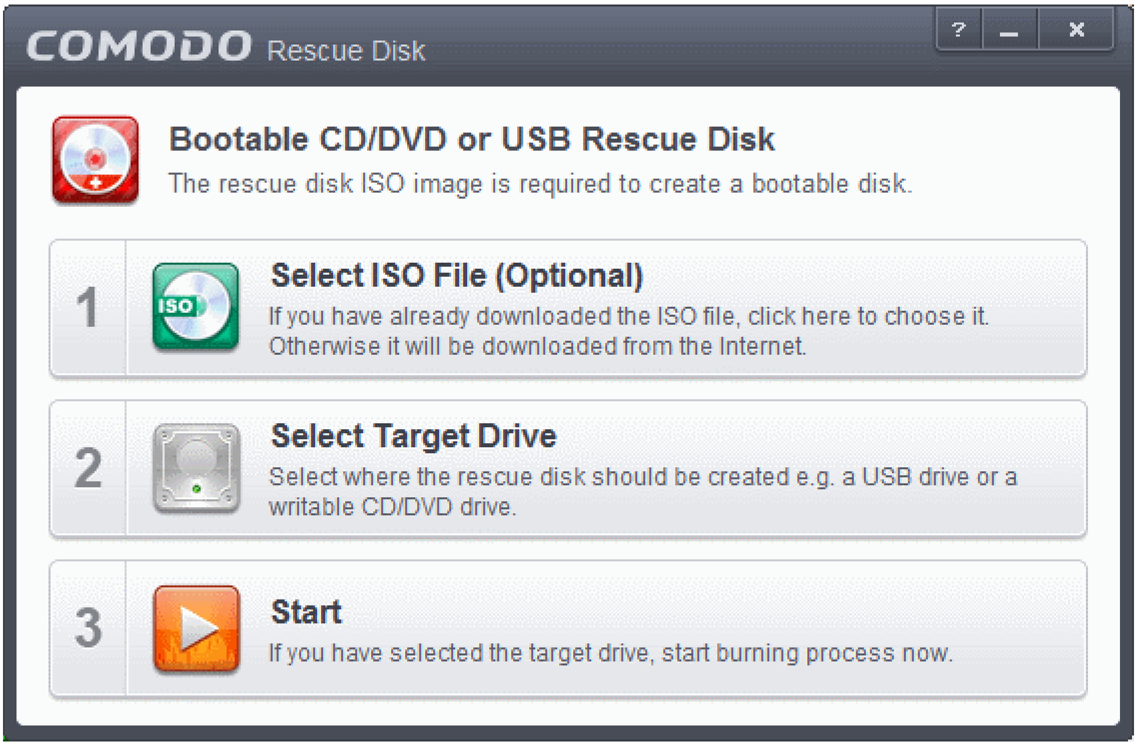
- Create a Rescue Disk - Burn a bootable ISO that lets you run virus scans in pre-boot environments
- Submit Files - Directly Submit unknown/suspicious files to Comodo for analysis
- Identify and Kill Unsafe Running Processes - Use Comodo Killswitch to identify unsafe processes and manage system activity
- Remove Deeply Hidden Malware - Deploy Comodo Cleaning Essentials to eradicate persistent infections from your PC
- Manage CCS Tasks – Manage multiple CCS tasks such as pause a task, resume, reassign and so on
- Advanced Settings - Configure overall behavior, define custom rulesets and much more

Some of these utilities require the download and installation of additional setup files. After installation, the utility will start directly next time you click the button.

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, rootkit scanner and cleaner which works in both GUI and text mode. The tool can provide a more comprehensive and thorough scan than regular malware cleaning applications because it cleans your system before Windows is loaded. CRD is intended to be used when malware embeds itself so deeply into your system that regular AV software cannot remove it. The rescue disk is also very effective at removing infections that are preventing Windows from booting in the first place. Apart from the virus scanner, CRD also provides tools to explore files in your hard drive, take screen-shots and browse web pages.

- Clicking the 'Create Rescue Disk' button in CCS 'Advanced Settings' opens a utility that allows you to download and burn the CRD iso to a CD/DVD, USB or other drive. Click here to jump to a walk-through of this process.



COMODO Rescue Disk

Bootable CD/DVD or USB Rescue Disk

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

1 Select ISO File (Optional)

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

2 Select Target Drive

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

3 Start

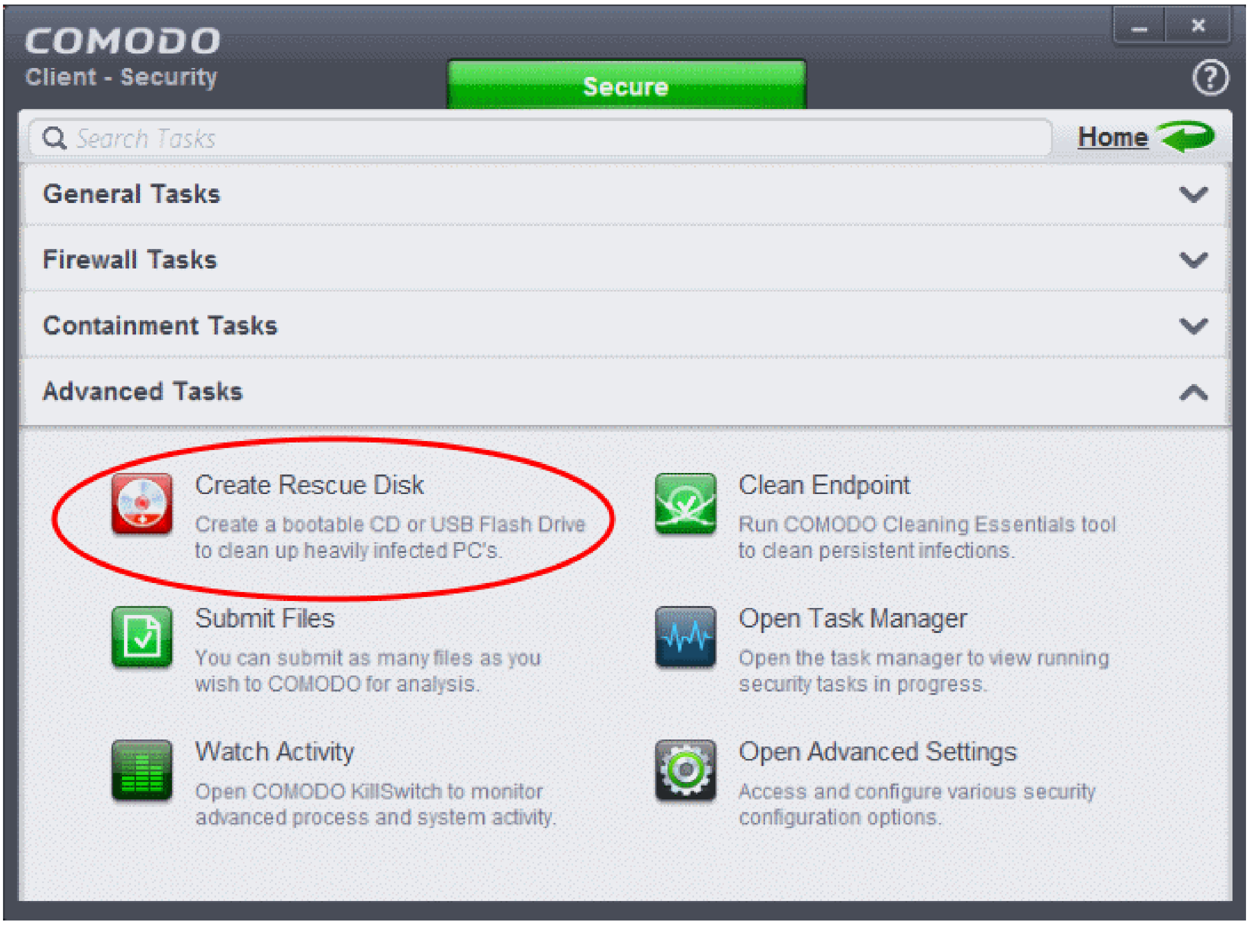
If you have selected the target drive, start burning process now.

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

- Details of how to change boot order on your computer can be found in the Rescue Disk user guide at http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html
- Details of how to initiate CRD after booting can be found at http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html
- Details of how to start running scans on your pre-boot environment are available at 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. Downloading and Burning Comodo Rescue Disk

To create a Comodo Rescue Disk, click 'Create Rescue Disk' button from the Advanced Tasks interface.



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

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

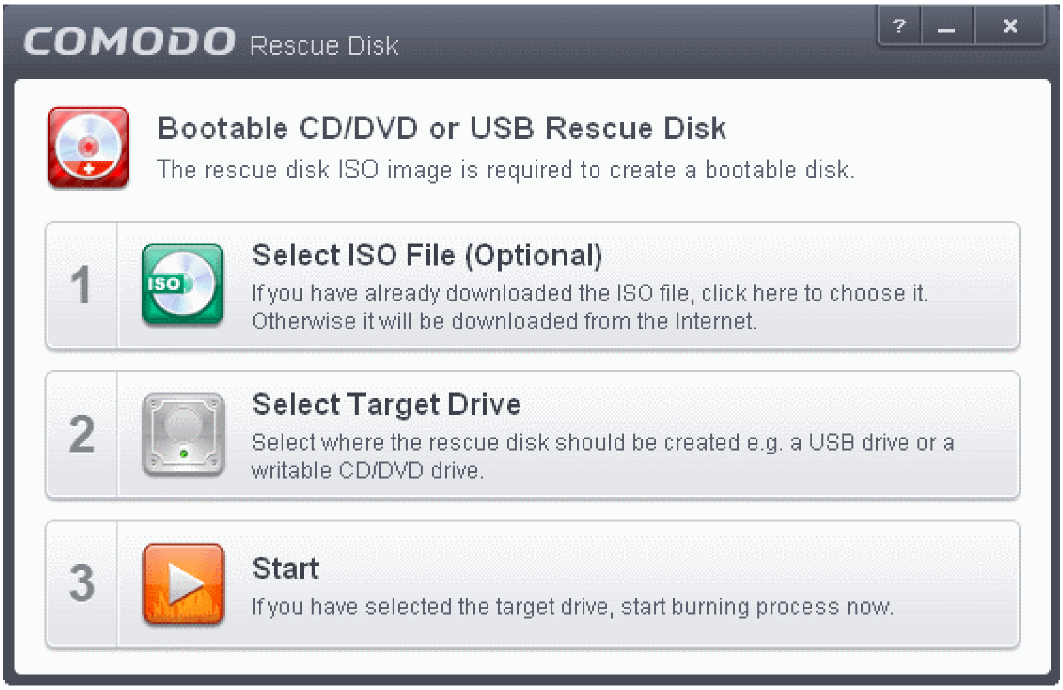
Submit Files
You can submit as many files as you wish to COMODO for analysis.

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

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

Open Advanced Settings
Access and configure various security configuration options.

The 'Comodo Rescue Disk' interface will open.



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

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

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

3 Start
If you have selected the target drive, start burning process now.

The Comodo Rescue Disk interface displays the steps involved in creation of a new Rescue Disk on a CD/DVD or in a USB drive.

Step 1- Select the ISO file

This step allows you to select the Comodo Rescue Disk image file in .iso format stored in your hard drive, if you have already downloaded the same from Comodo servers or copied from another computer. Pre-storing the .iso file and burning the rescue disk from it conserves your Internet connection bandwidth usage. This step is optional. If you haven't downloaded the iso file, it will be automatically downloaded from Comodo Servers prior to execution of Step 3 - Burning the Rescue Disk.

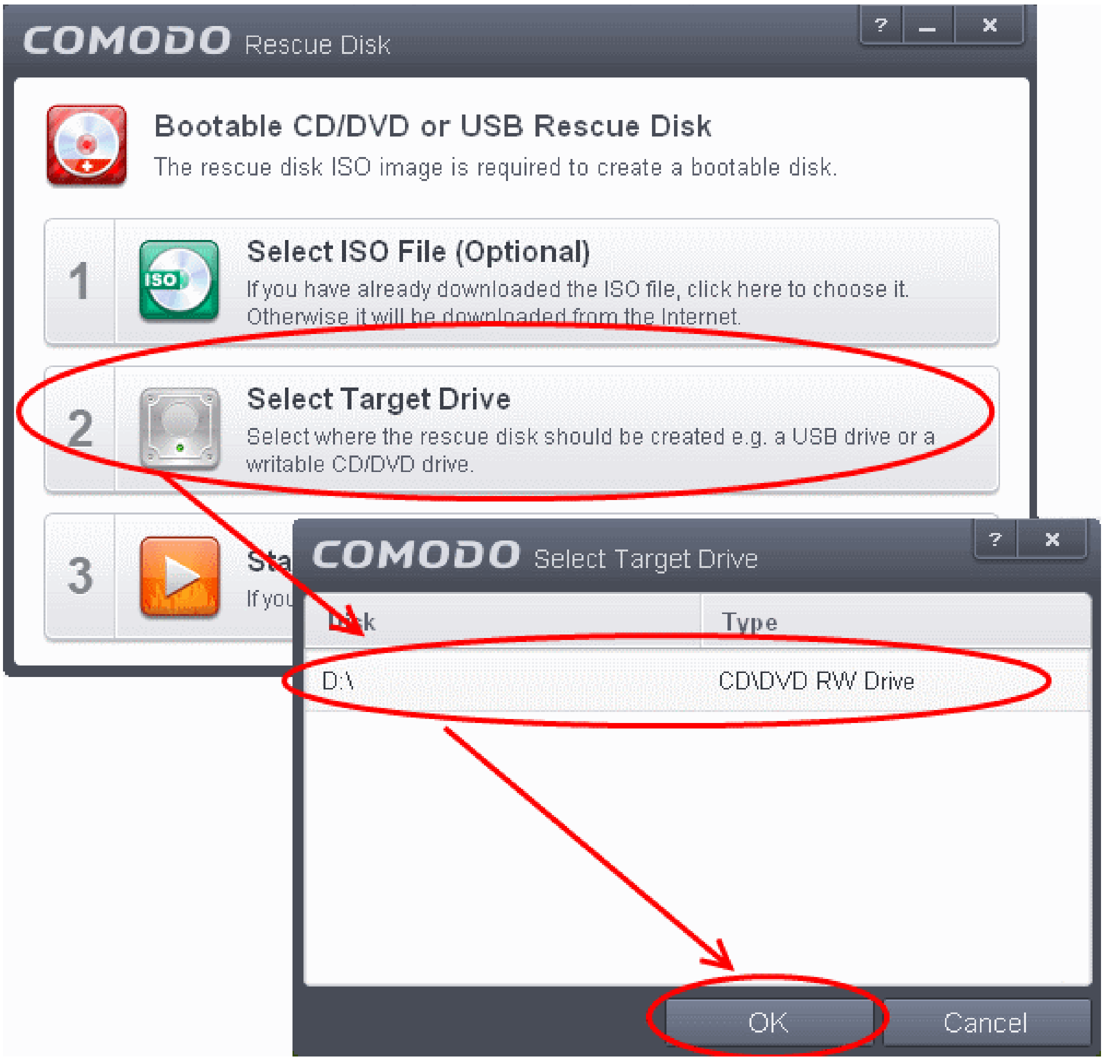
- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

This step allows you to select the CD/DVD drive or the USB drive to burn the Rescue Disk.

To burn the Rescue disk on a CD or a DVD

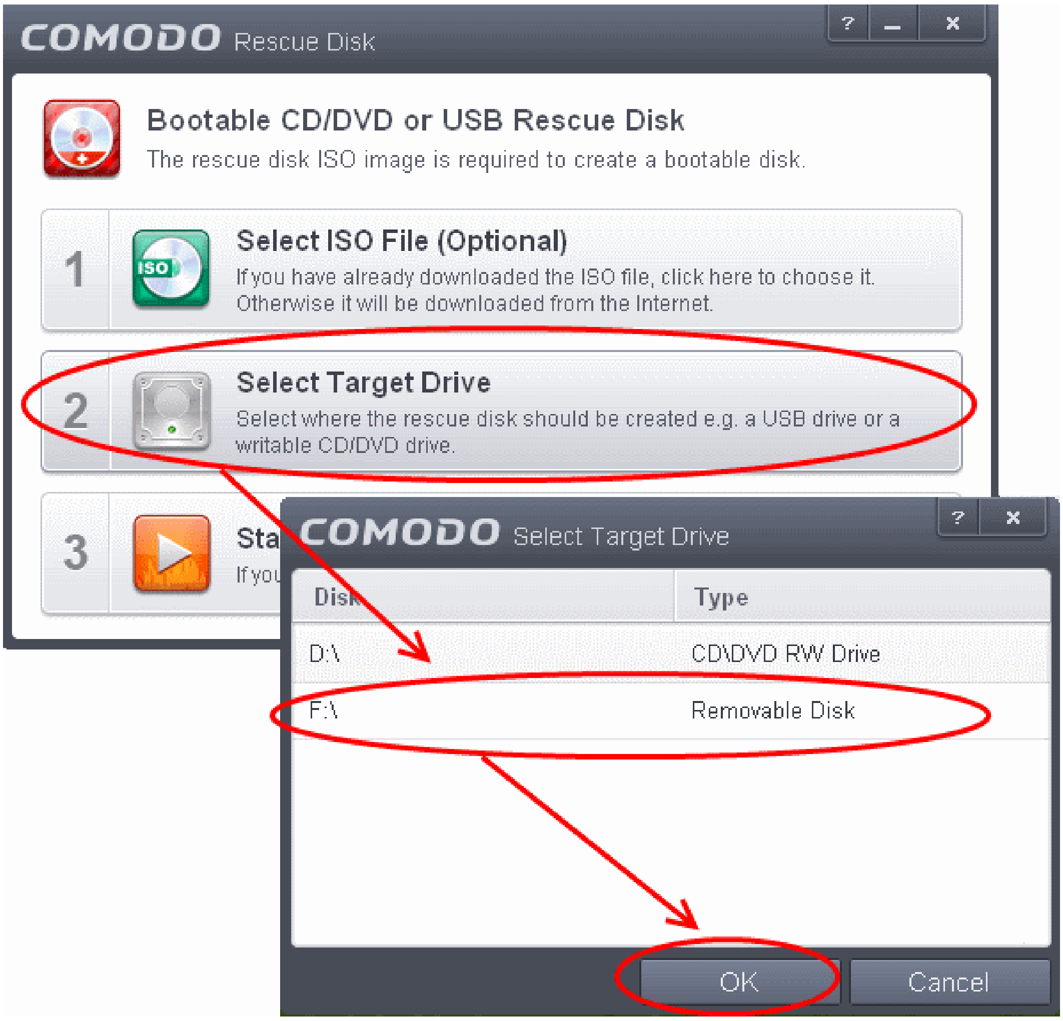
- Label a blank CD or DVD as "Comodo Rescue Disk - Bootable" and load it to the CD/DVD drive in your system
- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the Select Disc dialog


COMODO Rescue Disk
Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.
1
Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.
2
Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.
3
Sta
If you
COMODO Select Target Drive
Disk
Type
D:\
CD\DVD RW Drive
OK
Cancel

To burn the Rescue disk on a USB Drive

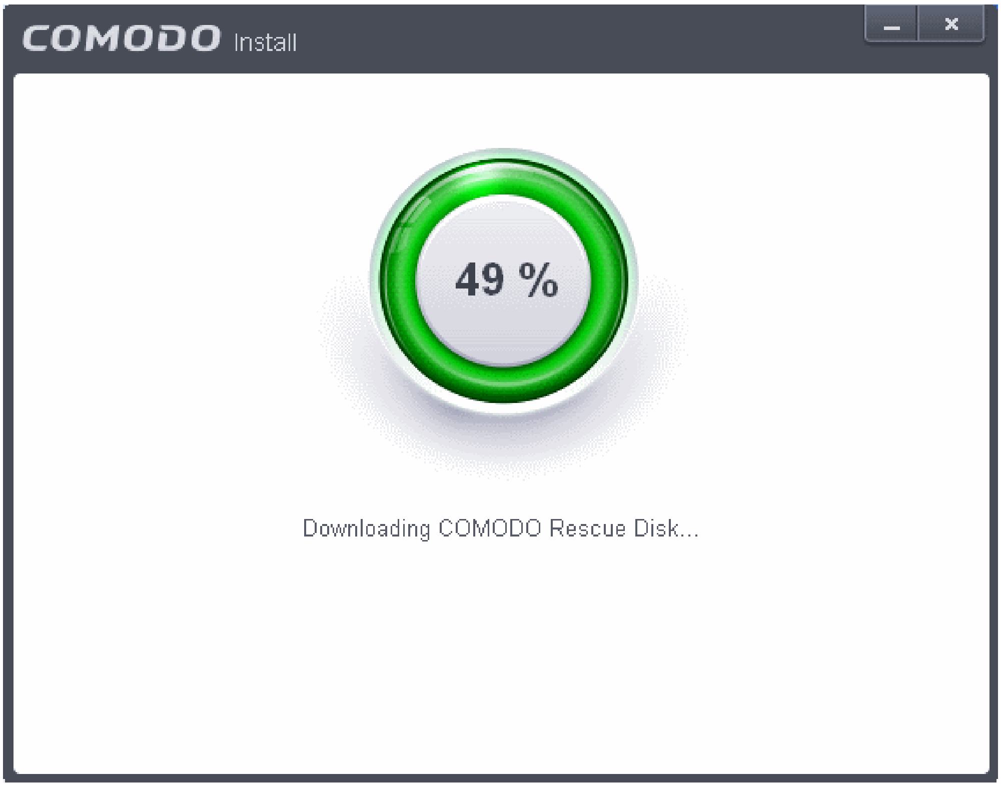
- Insert a formatted USB memory to a free USB port on your computer

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


COMODO Rescue Disk
Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.
1
Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.
2
Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.
3
Sta
If you
COMODO Select Target Drive
Disk
Type
D:\
CD\DVD RW Drive
F:\
Removable Disk
OK
Cancel

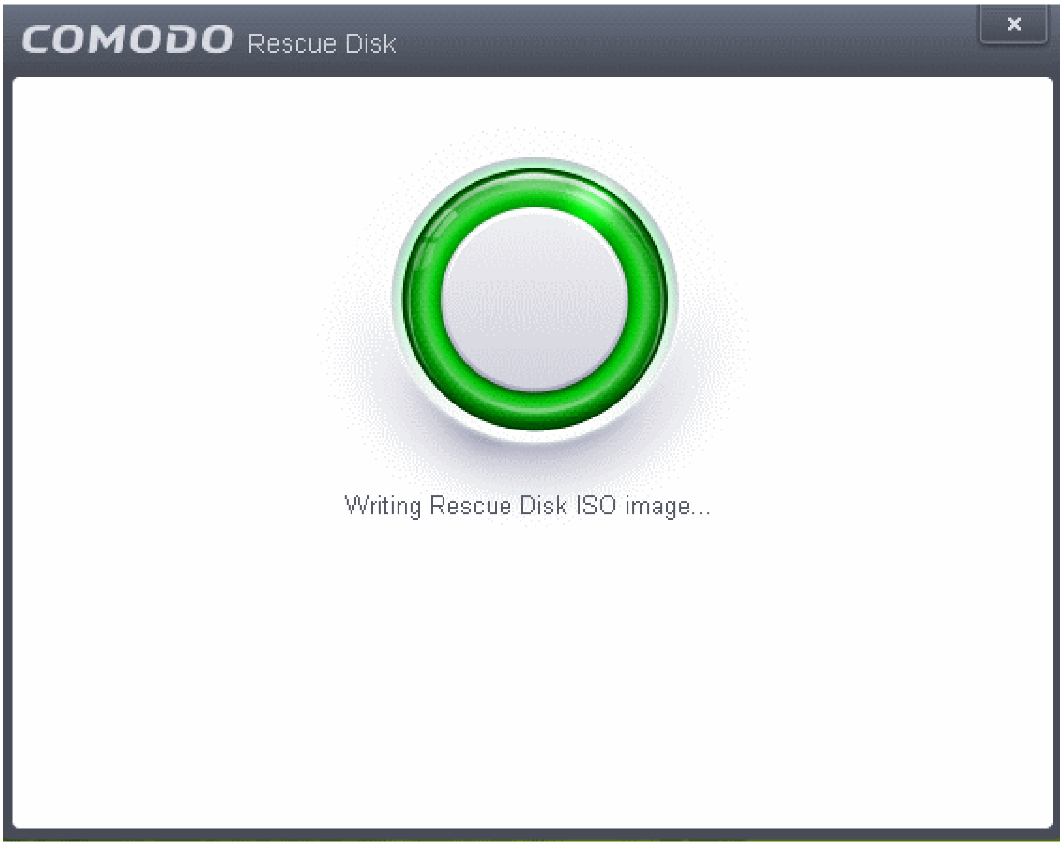
Step 3 - Burn the Rescue Disk

- After you selected the target drive, click 'Start'. If you have selected an .iso file from your hard disk, the burning of the disk will start immediately. Else, the .iso file will be downloaded from Comodo Servers.



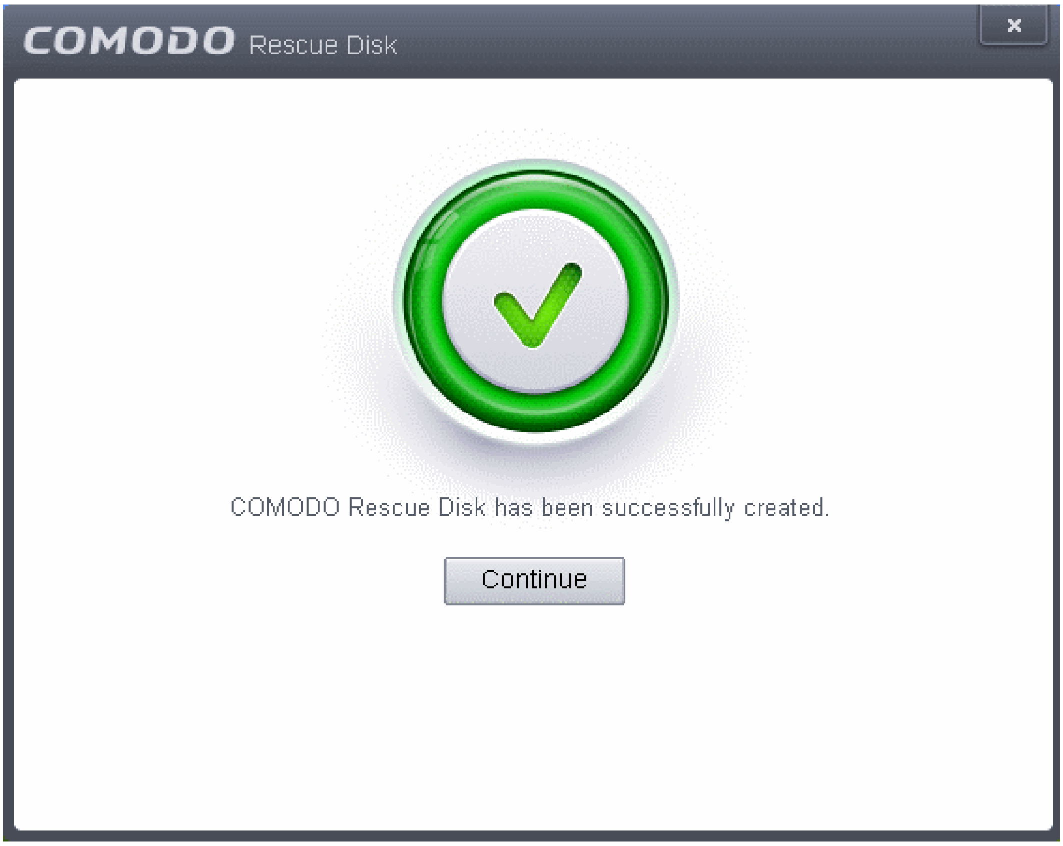
Downloading COMODO Rescue Disk...

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



Writing Rescue Disk ISO image...

- Wait till the completion of the process. Do not eject the CD/DVD or the USB drive. On completion of the process, the CD/DVD will be ejected automatically.



COMODO Rescue Disk has been successfully created.

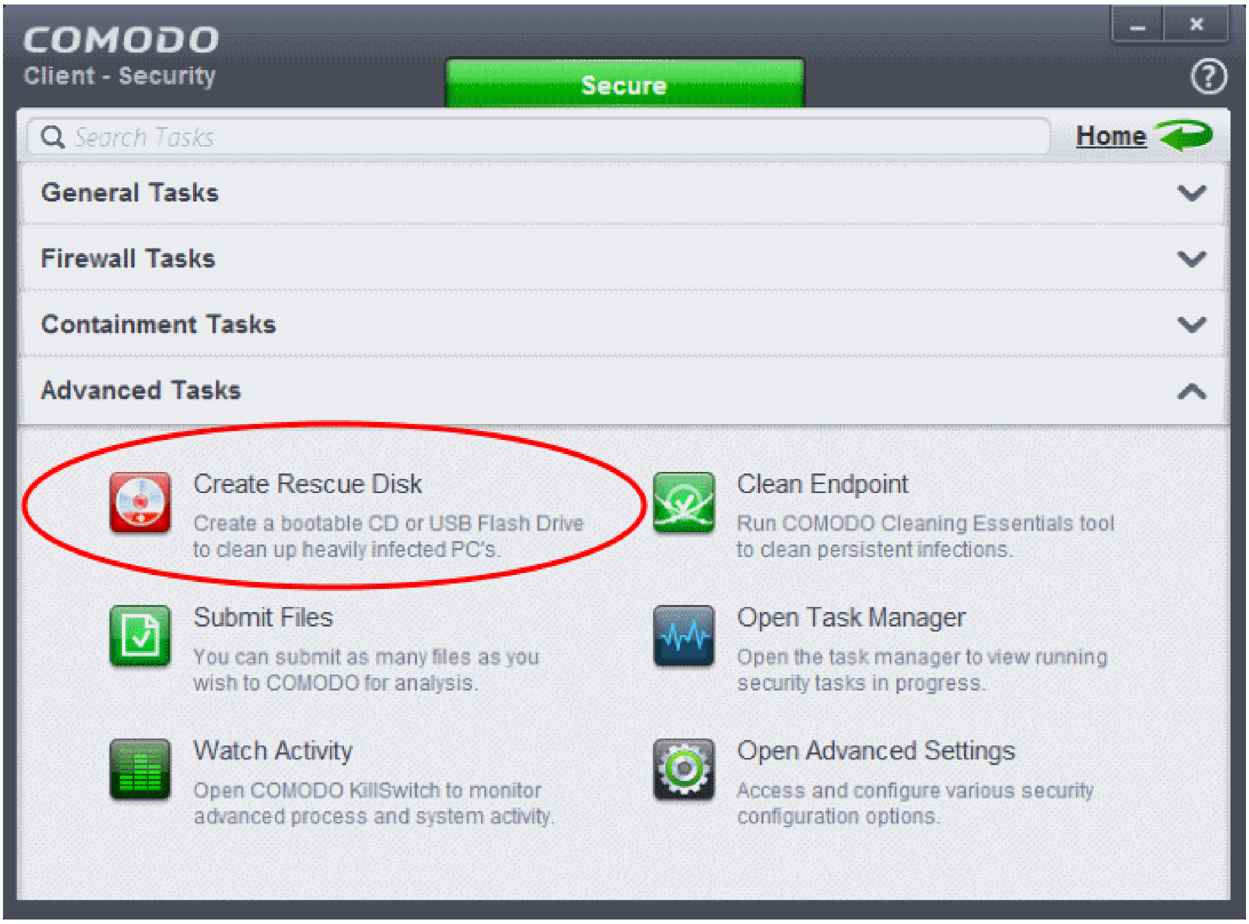
Your Bootable Comodo Rescue Disk is created. Click 'Continue' to go back to CCS interface.

5.2. Submit Files

As the name suggests, the 'Submitted Files' interface allows you to send as many files as you wish to Comodo for analysis. Files which CCS classifies as 'Unknown' or 'Unrecognized' are not in the Comodo safe list but have also not been identified as known malware. By sending these files to Comodo, you allow our team to analyze them and classify them as either 'Safe' or 'Malicious'. You can also submit files you suspect of being 'false positives' (those files that you feel CCS has incorrectly identified as malware). Subsequent to classification, they will be added to the white or black list accordingly.

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

To open the 'Submit Files' interface, click 'Tasks' on the home screen followed by 'Advanced Tasks' > 'Submit Files'



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

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

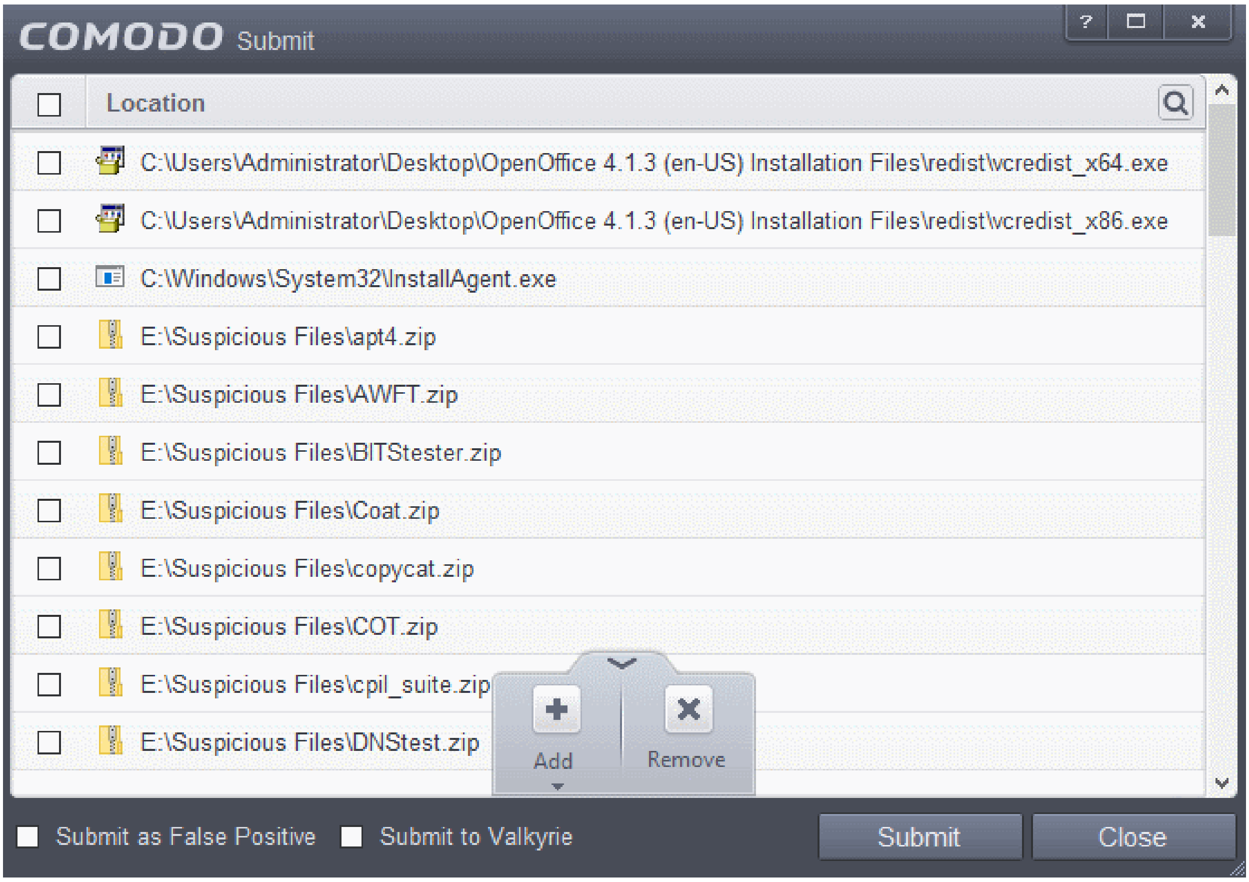
Submit Files
You can submit as many files as you wish to COMODO for analysis.

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

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

Open Advanced Settings
Access and configure various security configuration options.

The 'Submit' interface will open.



□	Location
□	C:\Users\Administrator\Desktop\OpenOffice 4.1.3 (en-US) Installation Files\redist\vcredist_x64.exe
□	C:\Users\Administrator\Desktop\OpenOffice 4.1.3 (en-US) Installation Files\redist\vcredist_x86.exe
□	C:\Windows\System32\InstallAgent.exe
□	E:\Suspicious Files\apt4.zip
□	E:\Suspicious Files\AWFT.zip
□	E:\Suspicious Files\BITStester.zip
□	E:\Suspicious Files\Coat.zip
□	E:\Suspicious Files\copycat.zip
□	E:\Suspicious Files\COT.zip
□	E:\Suspicious Files\cpil_suite.zip
□	E:\Suspicious Files\DNStest.zip

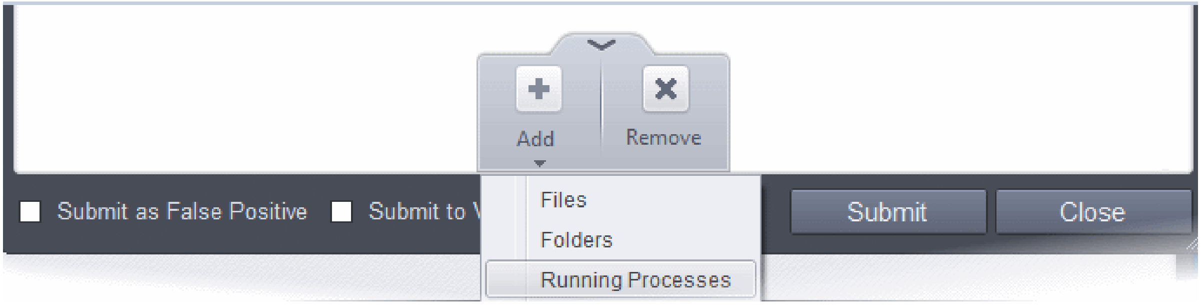
□ Submit as False Positive □ Submit to Valkyrie

Clicking the handle at the bottom center of the panel opens the following options:

- Remove - Allows you to remove files from the 'Submit Files' list
- Add - Allows you to add files to the 'Submit Files' list

To add new file(s) to 'Submit Files' list

- Click the handle from the bottom center and choose 'Add'



You can add files to the Submit Files list by three ways:

- **Files** - Allows you to navigate to the file or executable of the program you wish to add.
- **Folders** - Allows you to 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.

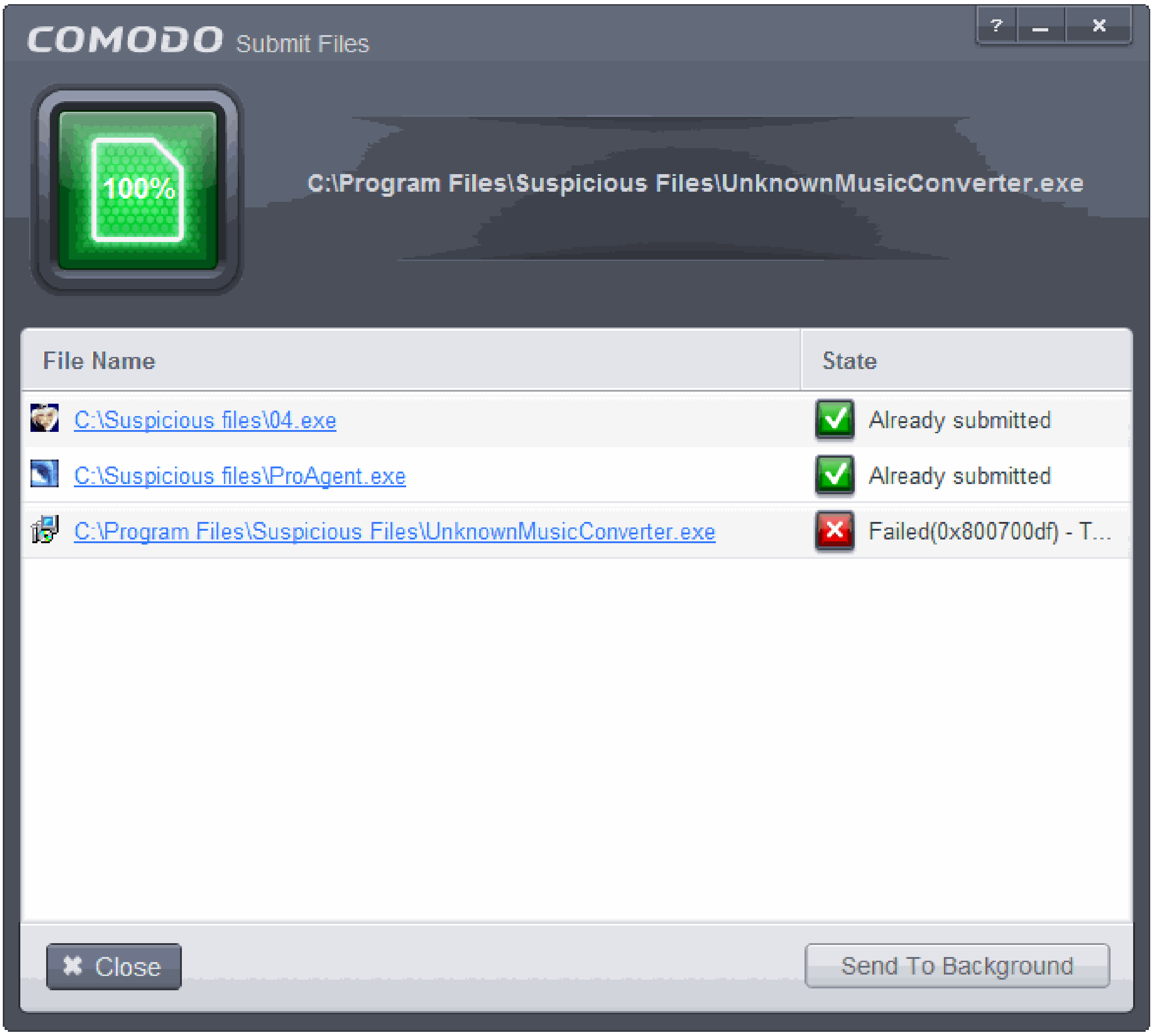
- Repeat the process to add more files and to submit them at-once.

To remove the files from 'Submit Files' list

- Select the file from the list
- Click the handle from the bottom center and select 'Remove'

After adding the files you want to submit, click 'Submit' button. If you want to submit the files as False Positives to Comodo, select the 'Submit as False Positive' check box.

The files will be submitted and the progress will be displayed.



File Name	State
C:\Suspicious files\04.exe	✓ Already submitted
C:\Suspicious files\ProAgent.exe	✓ Already submitted
C:\Program Files\Suspicious Files\UnknownMusicConverter.exe	✗ Failed(0x800700df) - T...

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 another CCS user and was not uploaded from your machine at this time.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

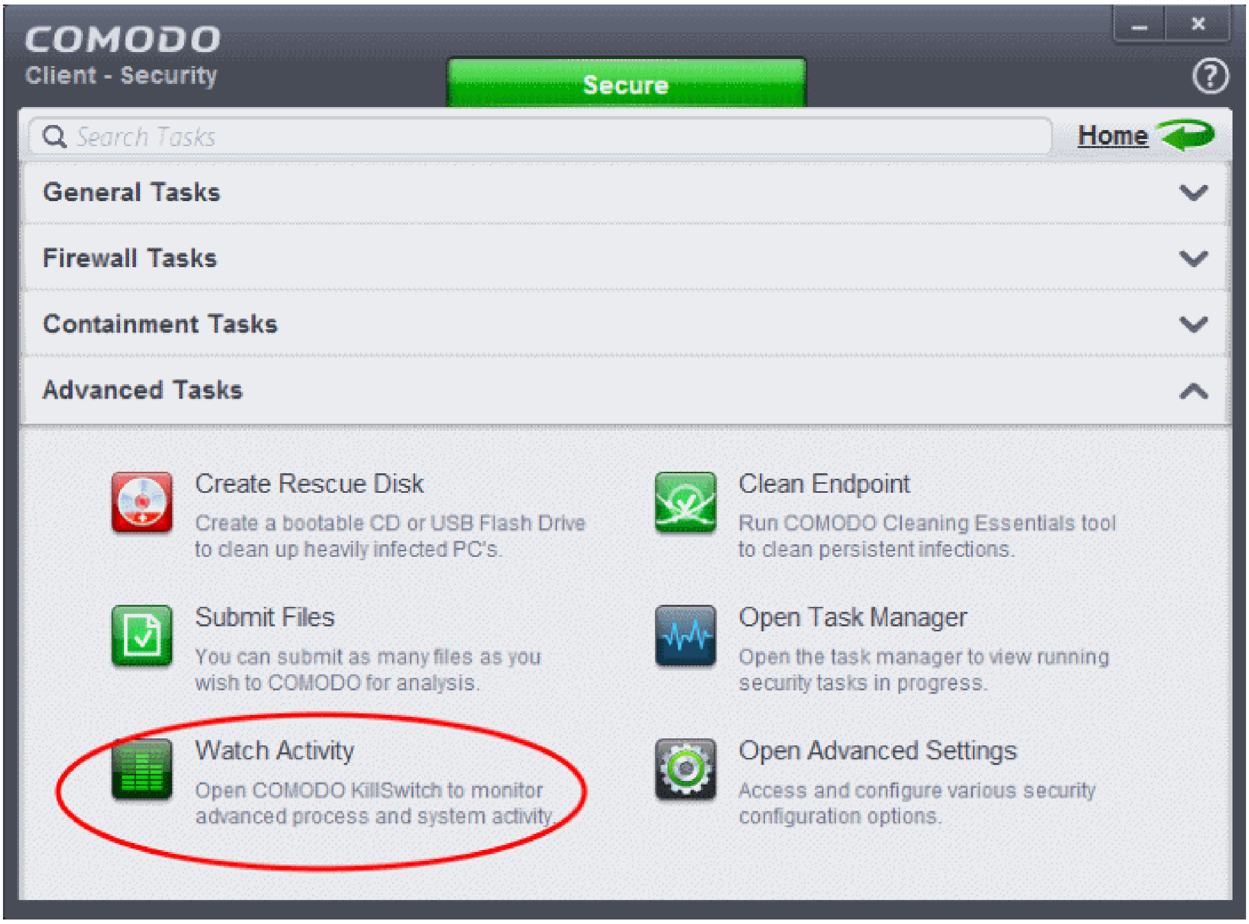
The list of files submitted from your computer can be viewed from the **Submitted Files** interface.

5.3. Identify and Kill Unsafe Running Processes

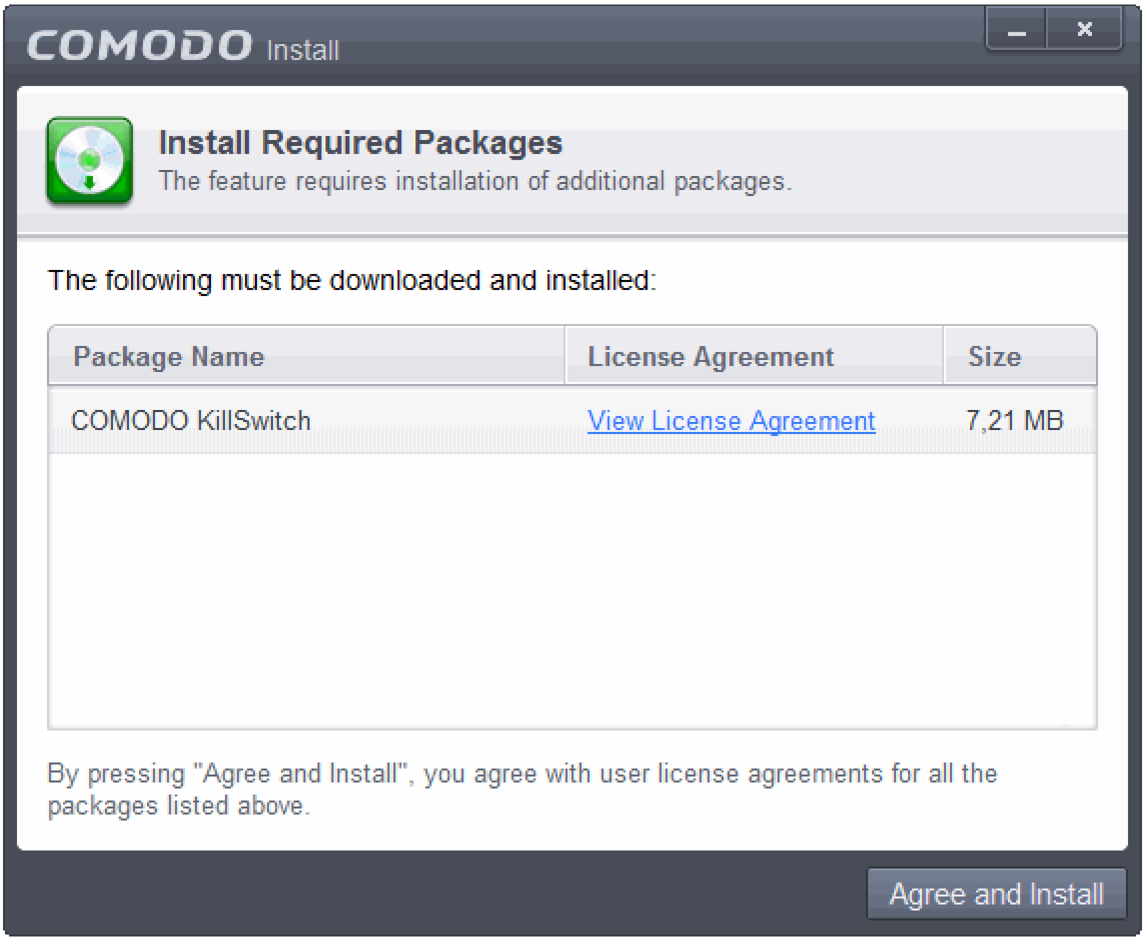
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer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

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


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Containment Tasks
Advanced Tasks
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
Open Task Manager
Open the task manager to view running security tasks in progress.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
Open Advanced Settings
Access and configure various security configuration options.

- Clicking the 'Watch Activity' for the first time, CCS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



Install Required Packages

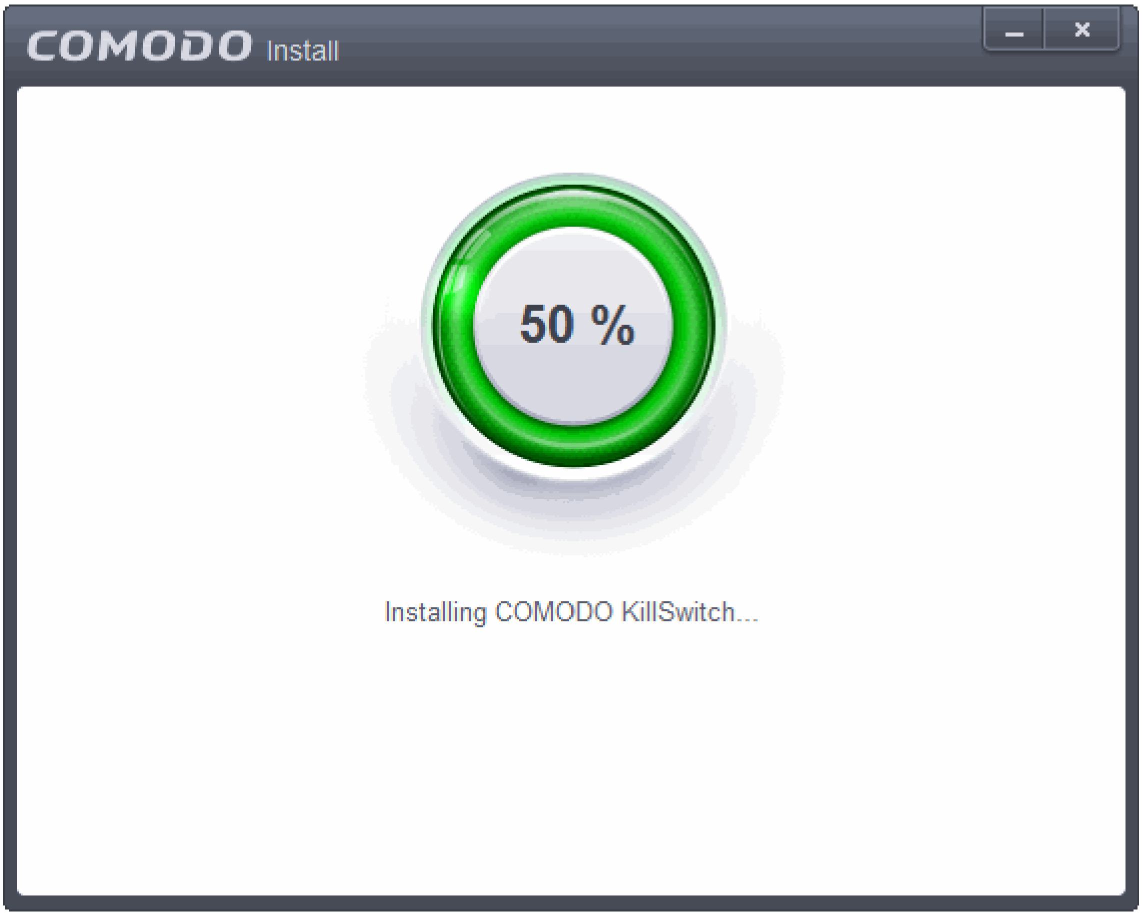
The feature requires installation of additional packages.

The following must be downloaded and installed:

Package Name	License Agreement	Size
COMODO KillSwitch	View License Agreement	7,21 MB

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

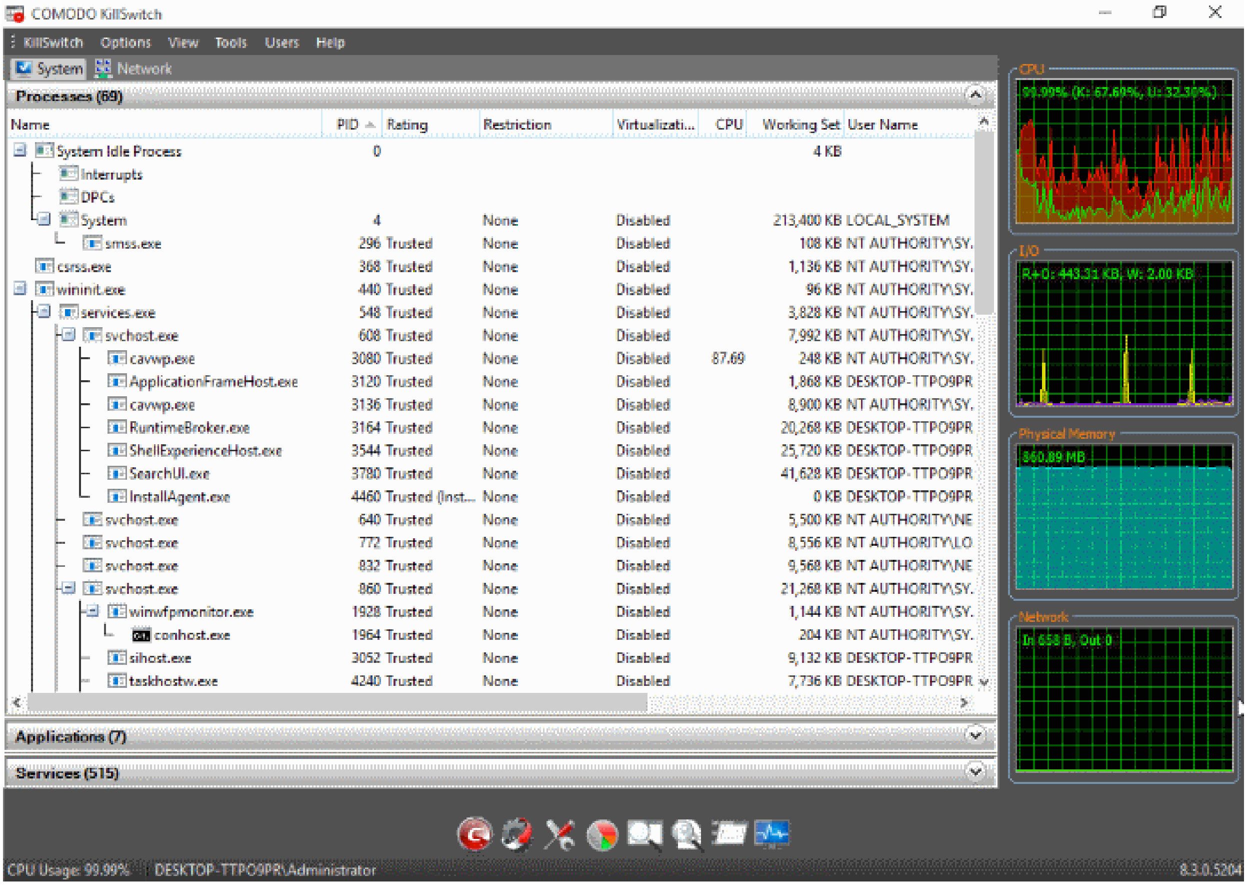
- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CCS will download and install the application.



50 %

Installing COMODO KillSwitch...

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



Name	PID	Rating	Restriction	Virtualizati...	CPU	Working Set	User Name
System Idle Process	0					4 KB	
Interrupts							
DPCs							
System	4		None	Disabled		213,400 KB	LOCAL_SYSTEM
smss.exe	296	Trusted	None	Disabled		108 KB	NT AUTHORITY\SY.
csrss.exe	368	Trusted	None	Disabled		1,136 KB	NT AUTHORITY\SY.
wininit.exe	440	Trusted	None	Disabled		96 KB	NT AUTHORITY\SY.
services.exe	548	Trusted	None	Disabled		3,828 KB	NT AUTHORITY\SY.
svchost.exe	608	Trusted	None	Disabled		7,992 KB	NT AUTHORITY\SY.
cavwp.exe	3080	Trusted	None	Disabled	87.69	248 KB	NT AUTHORITY\SY.
ApplicationFrameHost.exe	3120	Trusted	None	Disabled		1,868 KB	DESKTOP-TTPO9PR
cavwp.exe	3136	Trusted	None	Disabled		8,900 KB	NT AUTHORITY\SY.
RuntimeBroker.exe	3164	Trusted	None	Disabled		20,268 KB	DESKTOP-TTPO9PR
ShellExperienceHost.exe	3544	Trusted	None	Disabled		25,720 KB	DESKTOP-TTPO9PR
SearchUI.exe	3780	Trusted	None	Disabled		41,628 KB	DESKTOP-TTPO9PR
InstallAgent.exe	4460	Trusted (Inst...	None	Disabled		0 KB	DESKTOP-TTPO9PR
svchost.exe	640	Trusted	None	Disabled		5,500 KB	NT AUTHORITY\NE
svchost.exe	772	Trusted	None	Disabled		8,556 KB	NT AUTHORITY\LO
svchost.exe	832	Trusted	None	Disabled		9,568 KB	NT AUTHORITY\NE
svchost.exe	860	Trusted	None	Disabled		21,268 KB	NT AUTHORITY\SY.
winwfpmonitor.exe	1928	Trusted	None	Disabled		1,144 KB	NT AUTHORITY\SY.
conhost.exe	1964	Trusted	None	Disabled		204 KB	NT AUTHORITY\SY.
sihost.exe	3052	Trusted	None	Disabled		9,132 KB	DESKTOP-TTPO9PR
taskhostw.exe	4240	Trusted	None	Disabled		7,736 KB	DESKTOP-TTPO9PR

CPU Usage: 99.99% DESKTOP-TTPO9PR\Administrator 8.3.0.5204

On clicking the 'Watch Activity' button from next time, 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

5.4. 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.

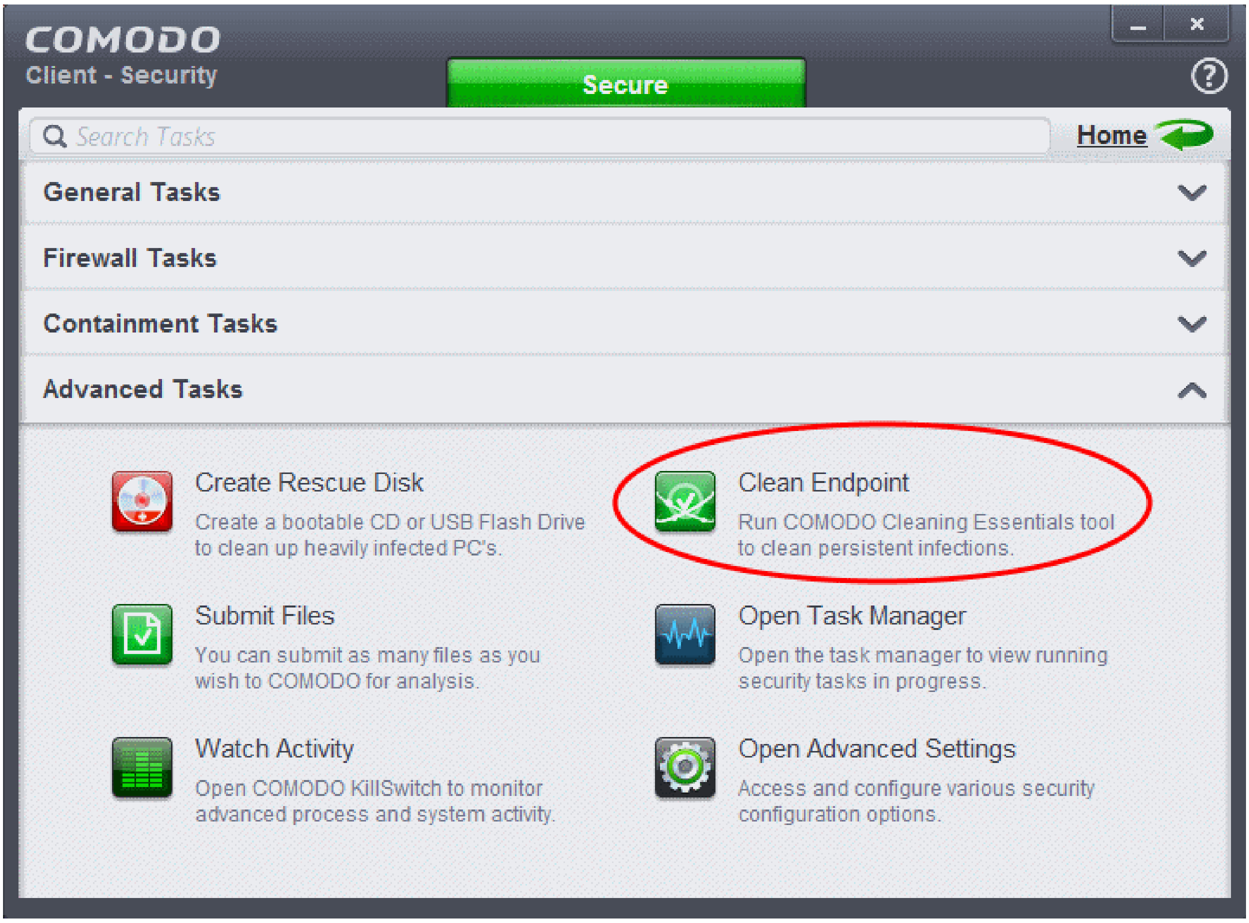
Major features include:

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

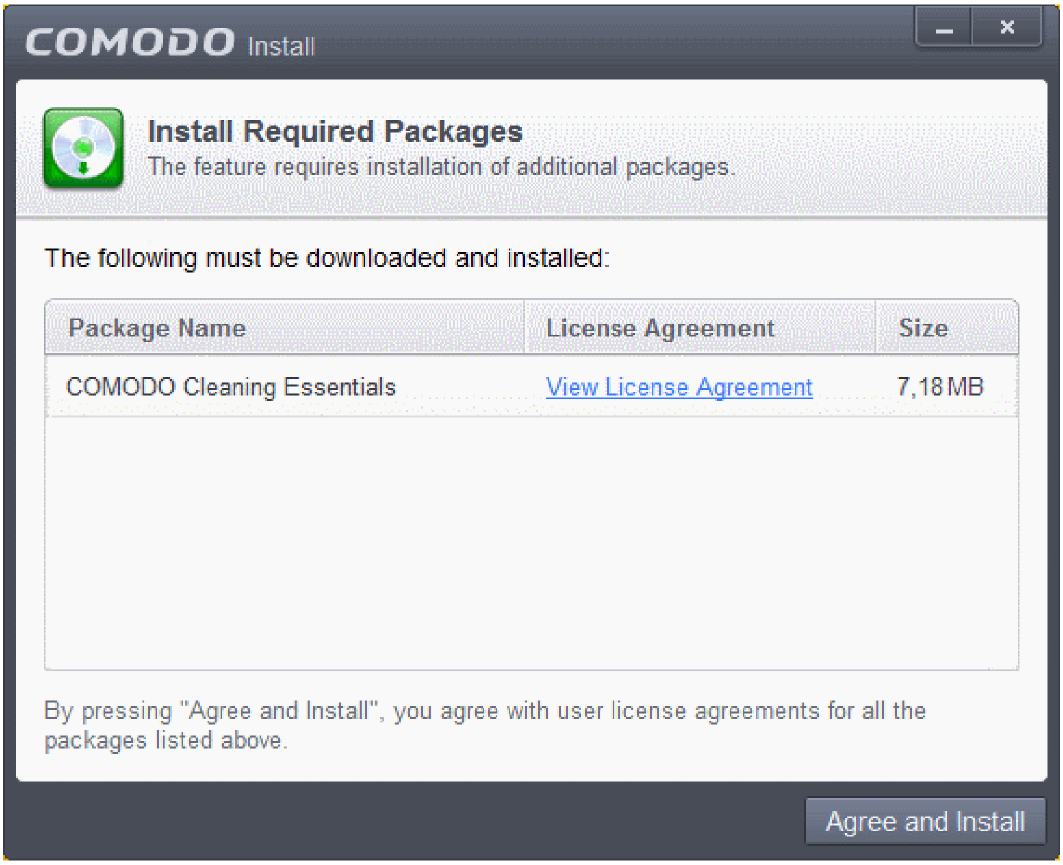
CCE enables home users to quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.

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

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


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Containment Tasks
Advanced Tasks
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
Open Task Manager
Open the task manager to view running security tasks in progress.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
Open Advanced Settings
Access and configure various security configuration options.

- Clicking the 'Clean Endpoint' for the first time, CCS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.



Install Required Packages

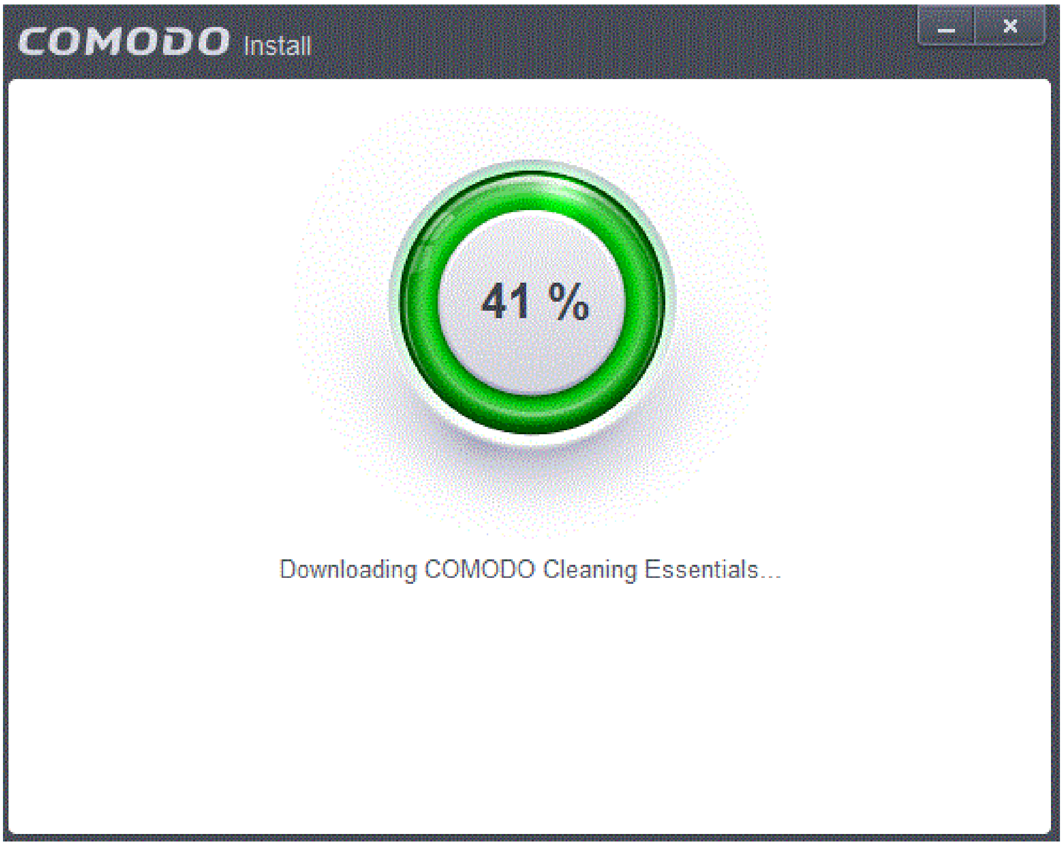
The feature requires installation of additional packages.

The following must be downloaded and installed:

Package Name	License Agreement	Size
COMODO Cleaning Essentials	View License Agreement	7,18 MB

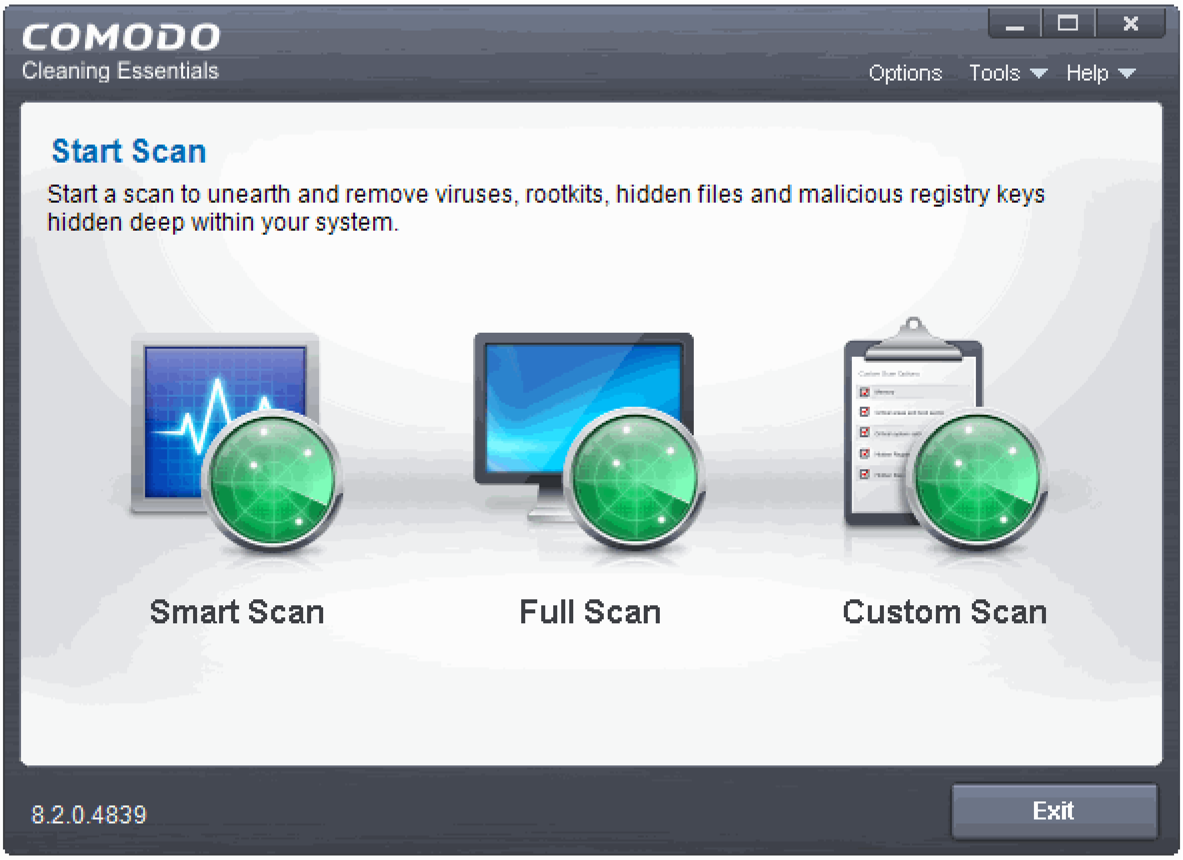
By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

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



Downloading COMODO Cleaning Essentials...

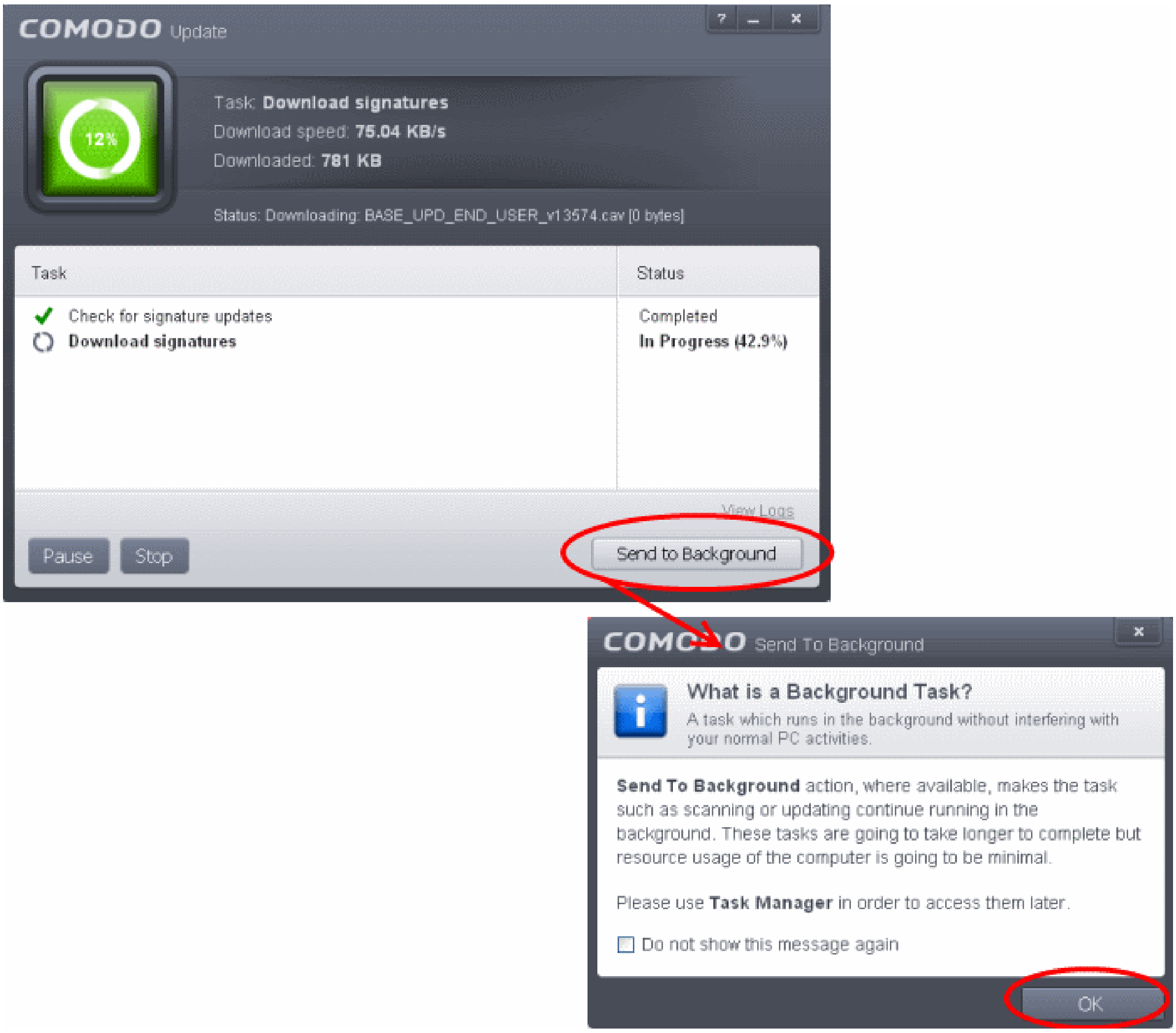
On completion of installation, the Comodo Cleaning Essentials main interface will be opened.


COMODO
Cleaning Essentials
Options
Tools
Help
Start Scan
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.
Smart Scan
Full Scan
Custom Scan
8.2.0.4839
Exit

- 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-119-1-328-3525-The-Main-Interface.html
- On clicking the 'Clean Endpoint' button from the next time, Comodo Cleaning Essentials will be opened.

5.5. Manage CCS Tasks

Comodo Client Security has the ability to concurrently run several tasks like on-demand or scheduled scans, virus signature database updates and so on. The tasks that are currently run, can be sent to background from the progress interface, by clicking 'Send to Background' as shown in the example below.



Task: **Download signatures**
Download speed: **75.04 KB/s**
Downloaded: **781 KB**

Status: Downloading: BASE_UPD_END_USER_v13574.cav [0 bytes]

Task	Status
✓ Check for signature updates	Completed
○ **Download signatures**	**In Progress (42.9%)**

What is a Background Task?

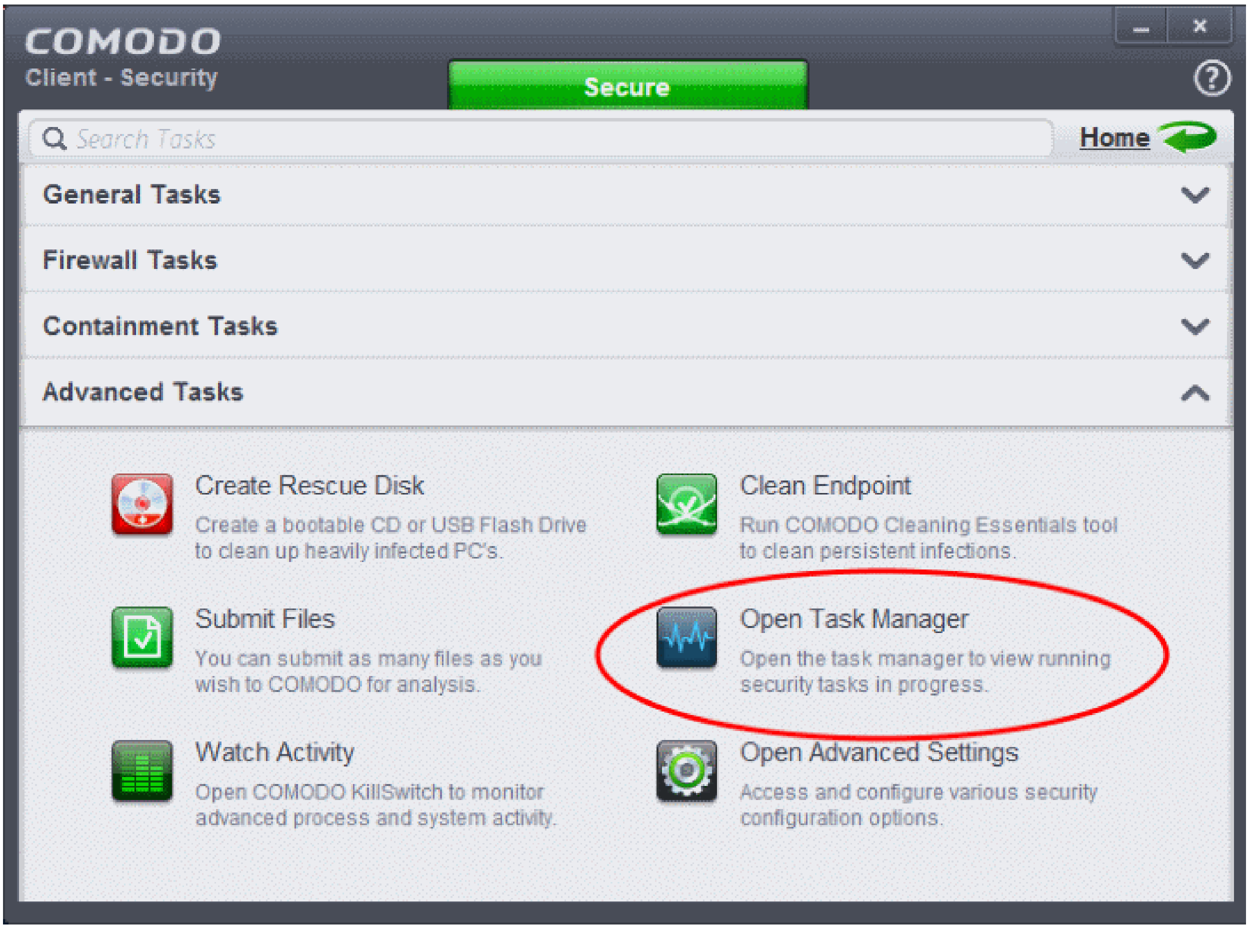
A task which runs in the background without interfering with your normal PC activities.

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

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

□ Do not show this message again

These tasks can be managed, through the Task manager interface that can be accessed anytime by opening Task Manager from the General Tasks interface.



COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Containment Tasks
Advanced Tasks

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

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

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

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

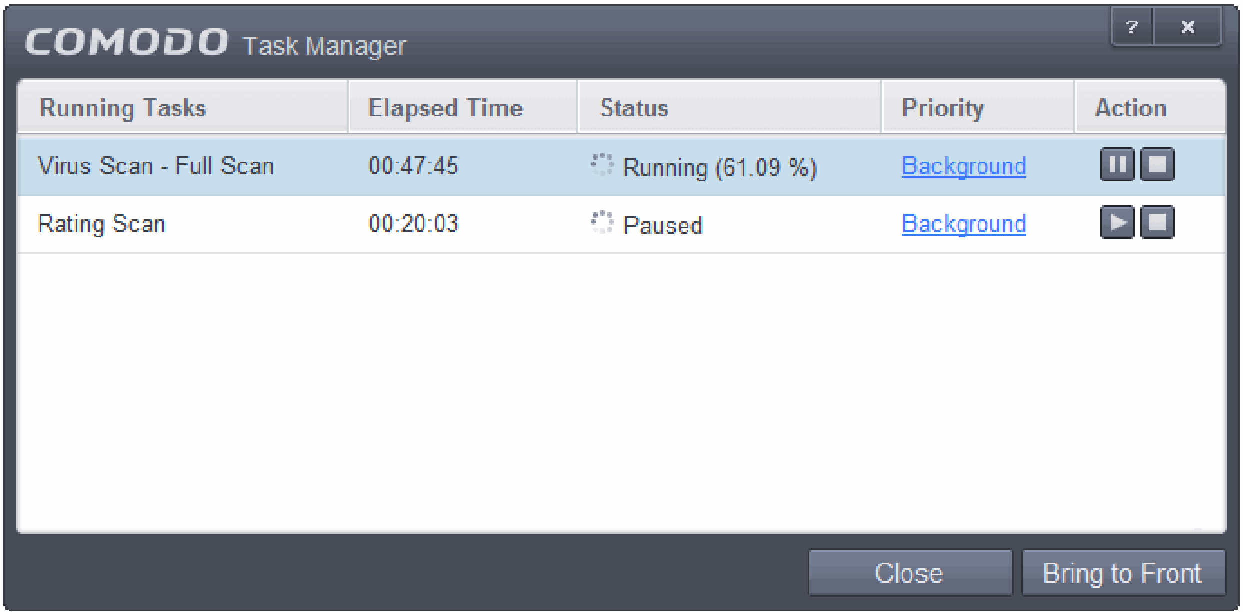
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

Note: The 'What is a Background Task' alert will be displayed only when the setting is enabled in the 'User Interface' screen. Refer to the section 'Customize User Interface' for more details.

Tip: The Task Manager can also be opened by clicking on the center tab in the Status row of the widget, that displays the number of tasks that are currently running.

The Task Manager window displays a list of background tasks that are currently running with the details of time elapsed on each task, status and priority.



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:47:45	Running (61.09 %)	Background	⏸ ⏹
Rating Scan	00:20:03	Paused	Background	▶ ⏹

From the Task Manager interface, you can:

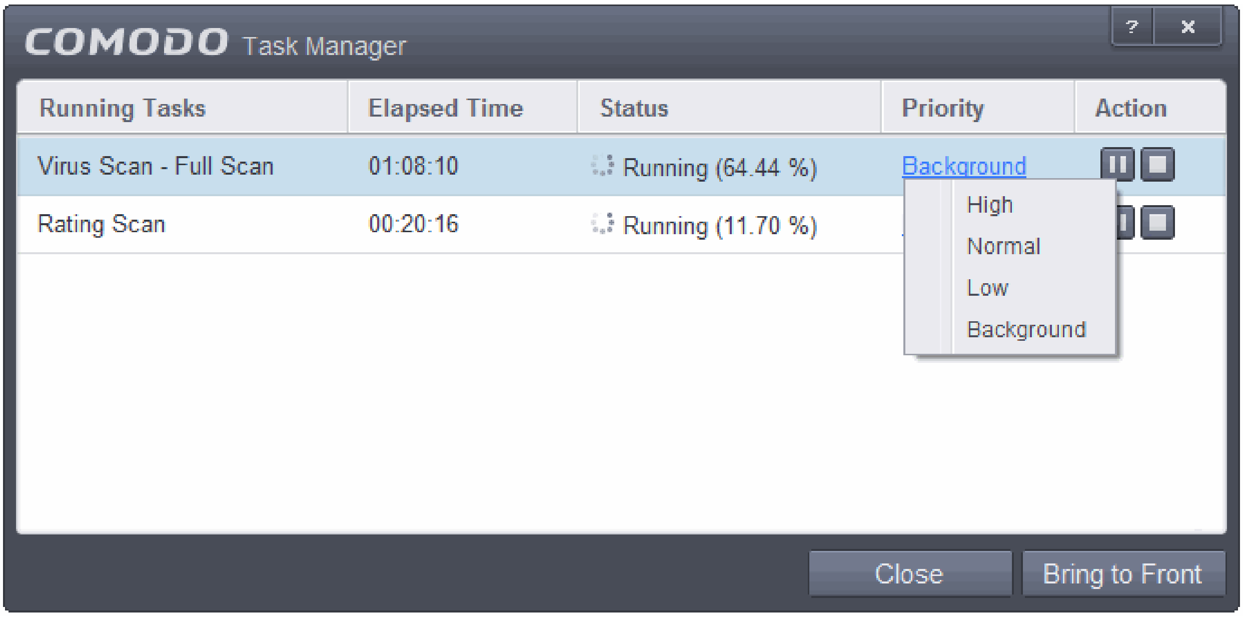
- Reassign priorities to the tasks
- Pause/Resume or Stop a running task
- Bring a selected task to foreground

Reassigning Priorities for a task:

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

To change the priority for a task

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

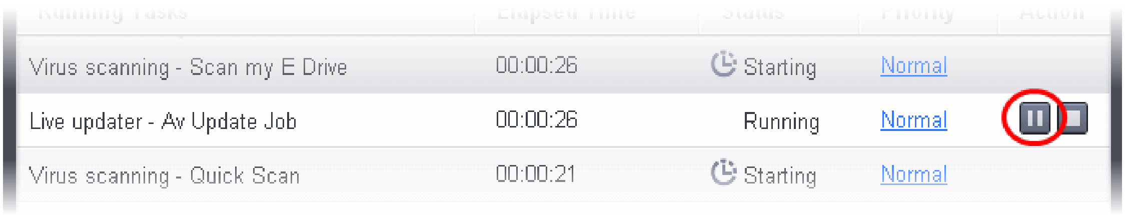


Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	01:08:10	Running (64.44 %)	Background	⏸ ⏹
Rating Scan	00:20:16	Running (11.70 %)		⏸ ⏹

Pausing/Resuming or Stopping running tasks

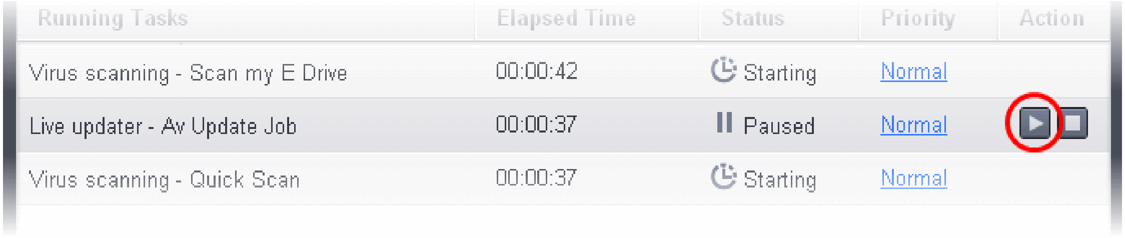
The Action column displays the Pause/Resume and Stop buttons

- To pause a running task, click the Pause button



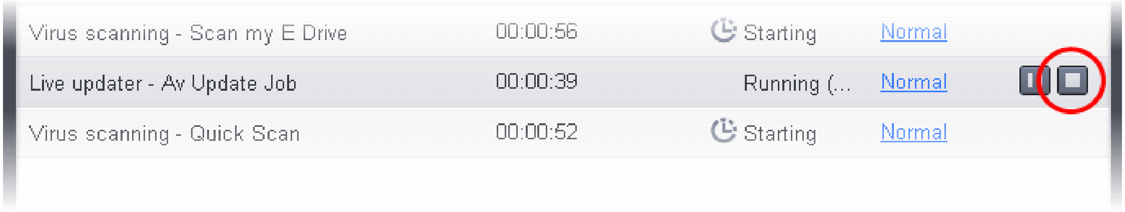
Running Tasks	Elapsed Time	Status	Priority	Action
Virus scanning - Scan my E Drive	00:00:26	Starting	Normal	
Live updater - Av Update Job	00:00:26	Running	Normal	⏸ ■
Virus scanning - Quick Scan	00:00:21	Starting	Normal	

- To resume a paused task, click the Resume button



Running Tasks	Elapsed Time	Status	Priority	Action
Virus scanning - Scan my E Drive	00:00:42	Starting	Normal	
Live updater - Av Update Job	00:00:37	Paused	Normal	▶ ■
Virus scanning - Quick Scan	00:00:37	Starting	Normal	

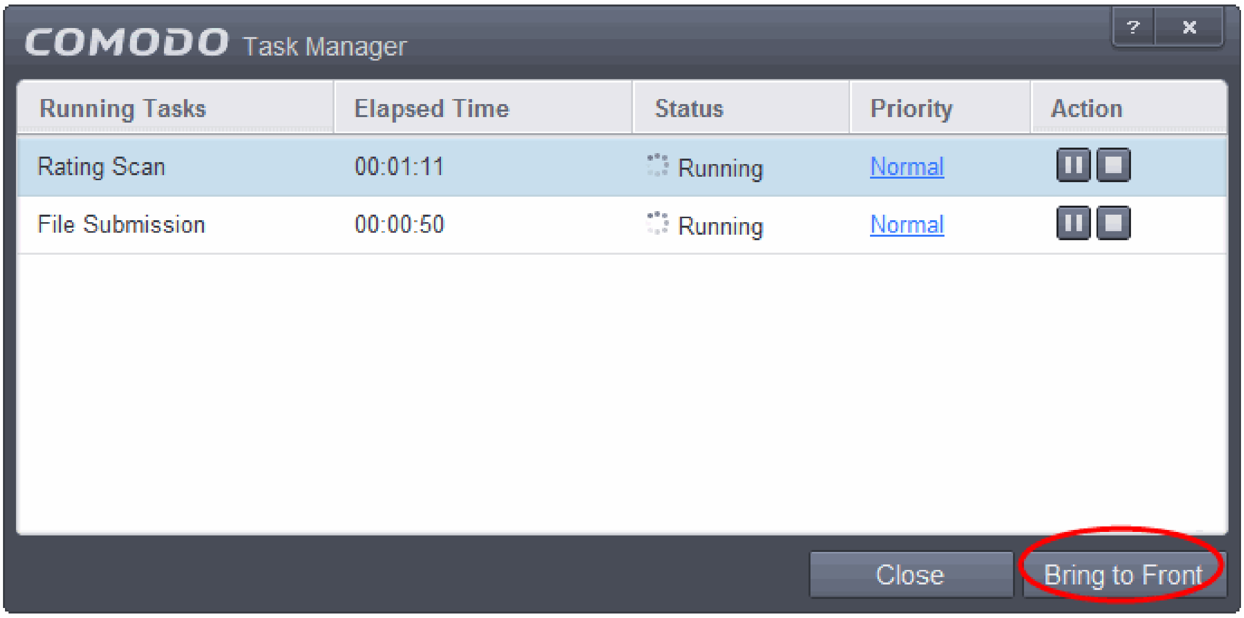
- To stop a running task, click the stop button



Virus scanning - Scan my E Drive	00:00:56	Starting	Normal	
Live updater - Av Update Job	00:00:39	Running (...	Normal	⏸ ■
Virus scanning - Quick Scan	00:00:52	Starting	Normal	

Bringing a running task to foreground

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



Running Tasks	Elapsed Time	Status	Priority	Action
Rating Scan	00:01:11	Running	Normal	⏸ ■
File Submission	00:00:50	Running	Normal	⏸ ■

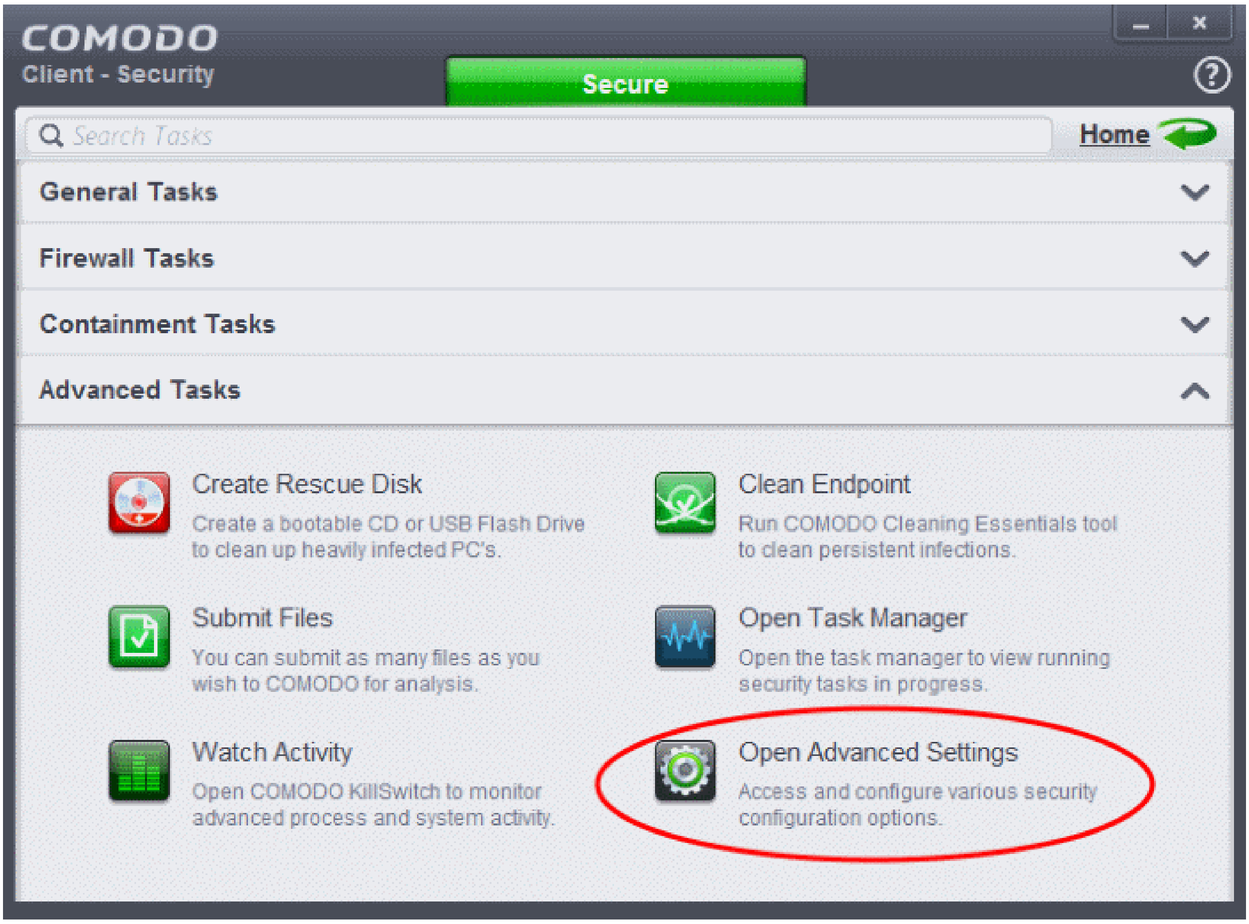
The progress window of the task will be displayed. If the task is completed, the results window will be displayed.

6. Advanced Settings

The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Client Security. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced users delve into granular configuration of the Antivirus, Advanced Protection, Firewall and File Ratings modules. For example, the 'Security Settings' area allows you to create custom virus scan schedules, create virus exclusions, create HIPS rules, modify containment behavior, define network zones and specify how the file rating system deals with trusted and untrusted files.

To open 'Advanced Settings', click the 'Tasks' arrow if you are on the CCS home screen.

- Click 'Advanced Tasks' then 'Open Advanced Settings'



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

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

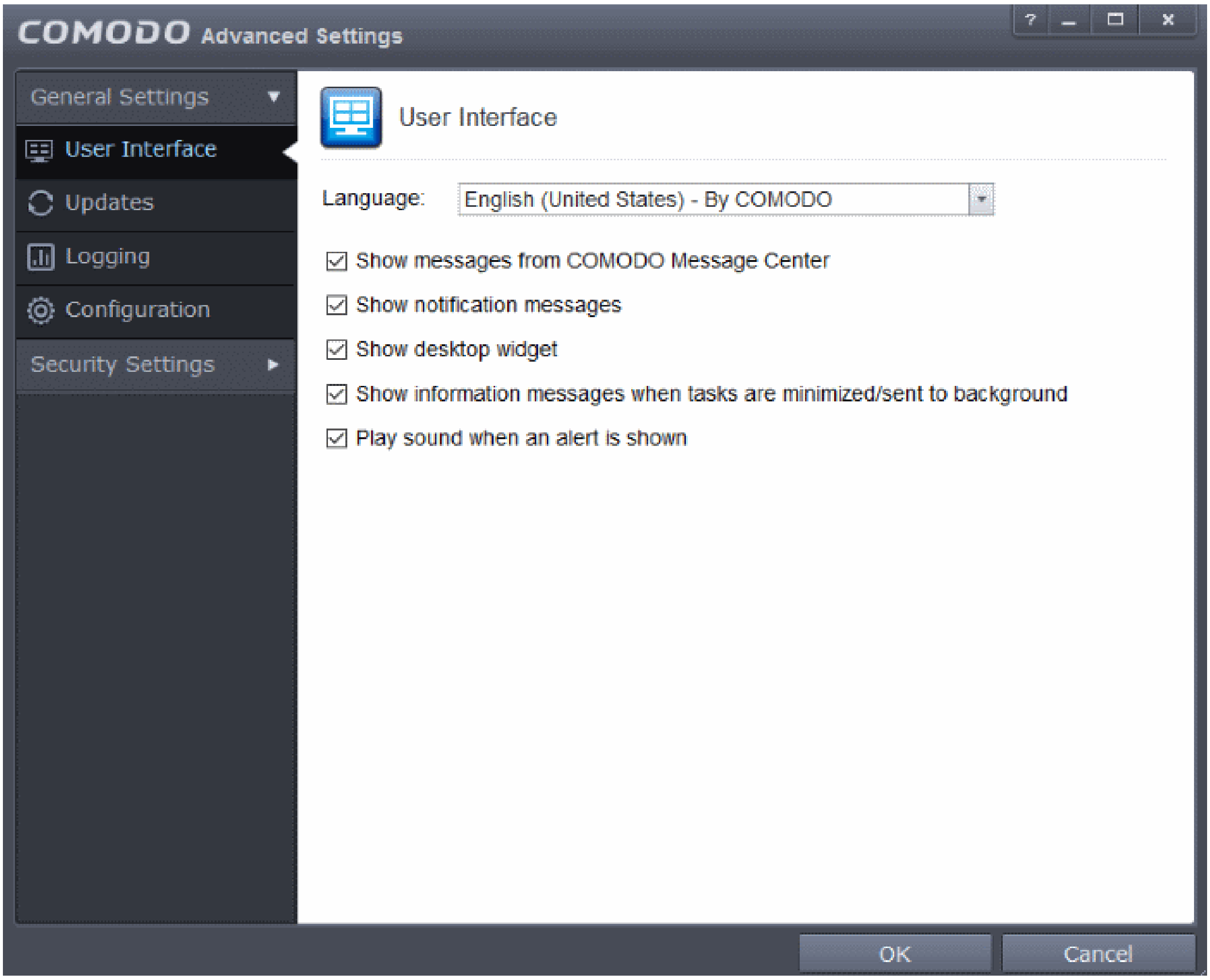
Submit Files
You can submit as many files as you wish to COMODO for analysis.

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

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

Open Advanced Settings
Access and configure various security configuration options.

The 'Advanced Settings' panel will open:



User Interface

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show desktop widget

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

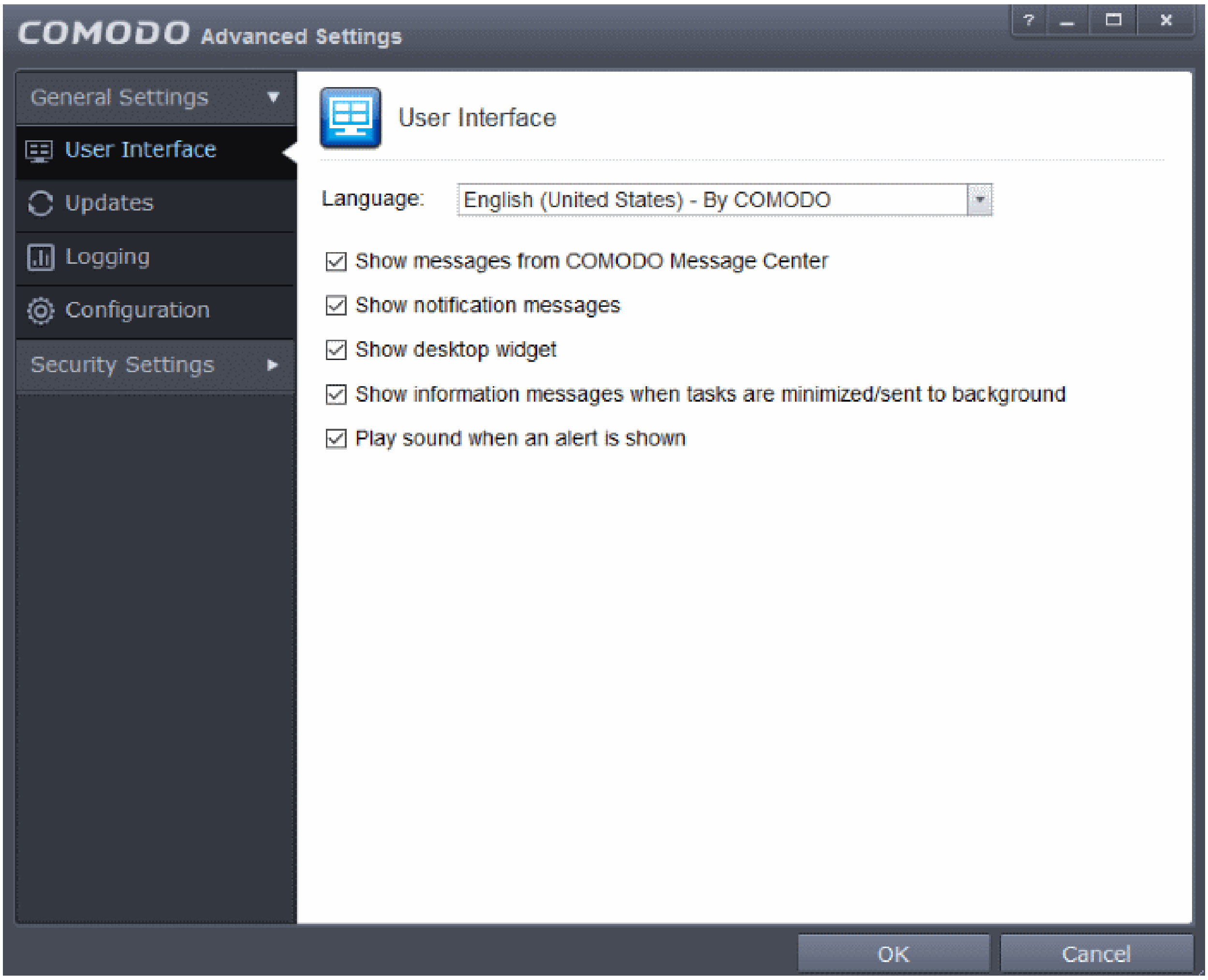
☑ Play sound when an alert is shown

Please refer to the following sections to find out more about setting:

- General Settings - Allows you to configure the appearance and behavior of the application
  - Customize User Interface
  - Configure program and database updates
  - Log Settings
  - Manage CCS Configurations
- Security Settings - Advanced configuration of Antivirus, Advanced Protection, Firewall and File Ratings modules
  - Antivirus Settings
  - Advanced Protection Settings
  - Firewall Settings
  - File Ratings

6.1. General Settings

The 'General Settings' area enables you to customize the appearance and overall behavior of Comodo Client Security. You can configure general properties like the interface language, notification messages, automatic updates, logging and more.



User Interface

Language: English (United States) - By COMODO

☑ Show messages from COMODO Message Center

☑ Show notification messages

☑ Show desktop widget

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

☑ Play sound when an alert is shown

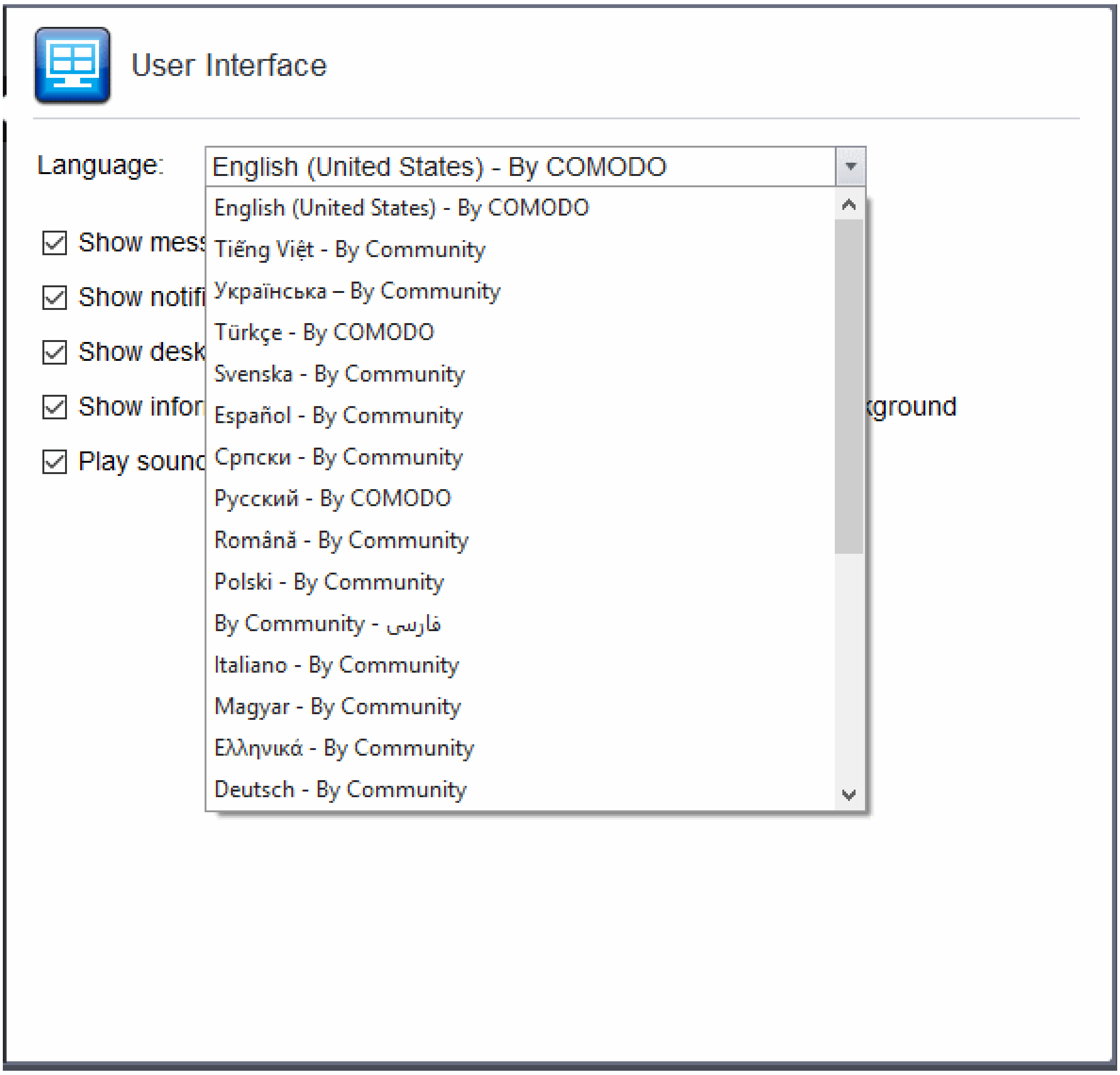
You can configure the following from this interface:

- User Interface
- Updates
- Logging
- Configuration

6.1.1. Customize User Interface

The 'User Interface' tab lets you choose the interface language and customize the look and feel of Comodo Client Security according to your preferences. You can also configure how messages are displayed and enable password protection for your settings.

- **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)***).



User Interface

Language: English (United States) - By COMODO

☑ Show mess

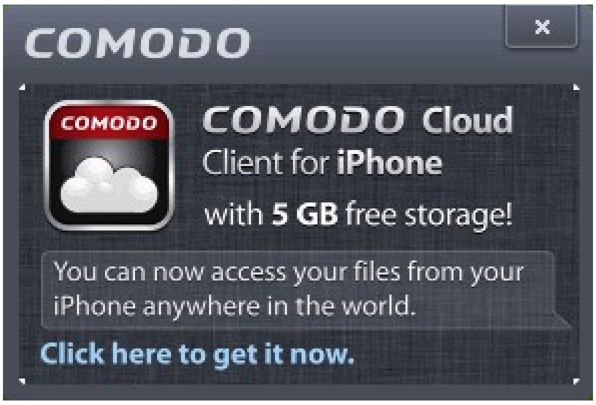
☑ Show notifi

☑ Show desk

☑ Show infor ... kground

☑ Play sound

- **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.

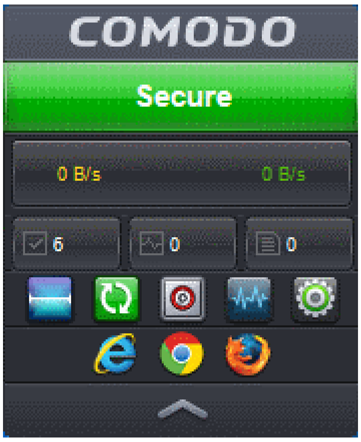


COMODO
COMODO Cloud
Client for iPhone
with 5 GB free storage!
You can now access your files from your iPhone anywhere in the world.
Click here to get it now.

They contain news about product updates, occasional requests for feedback, info about other Comodo products you may be interested to try and other general news. (*Default = Disabled*).

- **Show notification messages -** These are the CCS system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CCS is taking and any CCS status updates. For example 'Advanced Protection is learning ' are generated when these modules are learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in Antivirus > Real-time Scan settings screen. Clear this check box if you do not want to see these system messages *(Default = Disabled for 'CCS Managed' configuration profile and Enabled for CCS configuration profile)*.

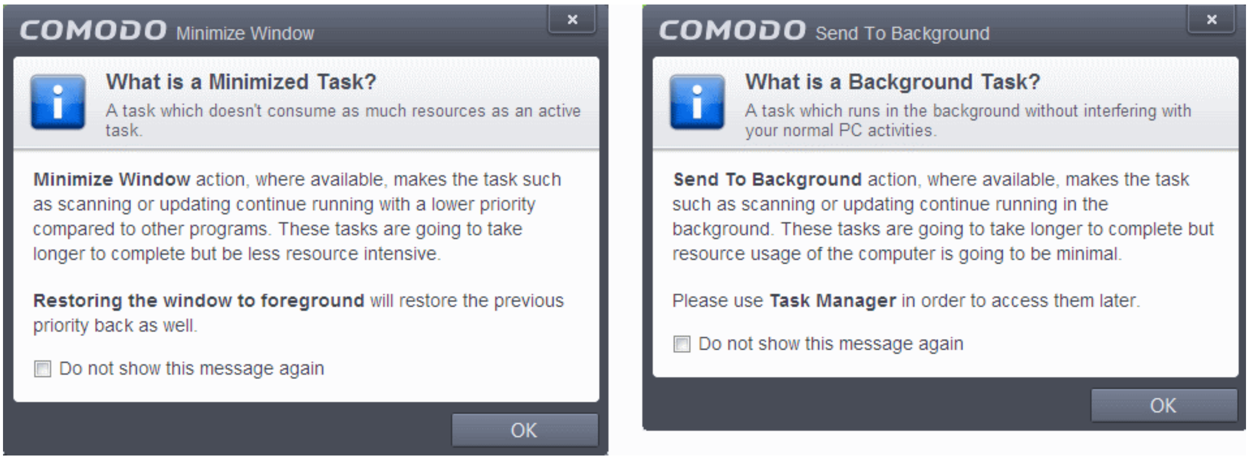
- **Show desktop widget** - The CCS desktop widget displays at-a-glance information about CCS security status, number of background tasks and shortcuts to open browsers inside the container.



The widget also acts as a shortcut to open the CCS main interface, the Task Manager, your browsers and so on. If you do not want the widget to be displayed on your desktop, clear this checkbox. *(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:



What is a Minimized Task?

A task which doesn't consume as much resources as an active task.

Minimize Window action, where available, makes the task such as scanning or updating continue running with a lower priority compared to other programs. These tasks are going to take longer to complete but be less resource intensive.

Restoring the window to foreground will restore the previous priority back as well.

□ Do not show this message again

What is a Background Task?

A task which runs in the background without interfering with your normal PC activities.

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

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

□ Do not show this message again

If you do not want these messages to be displayed, clear this check-box *(Default = Disabled).*

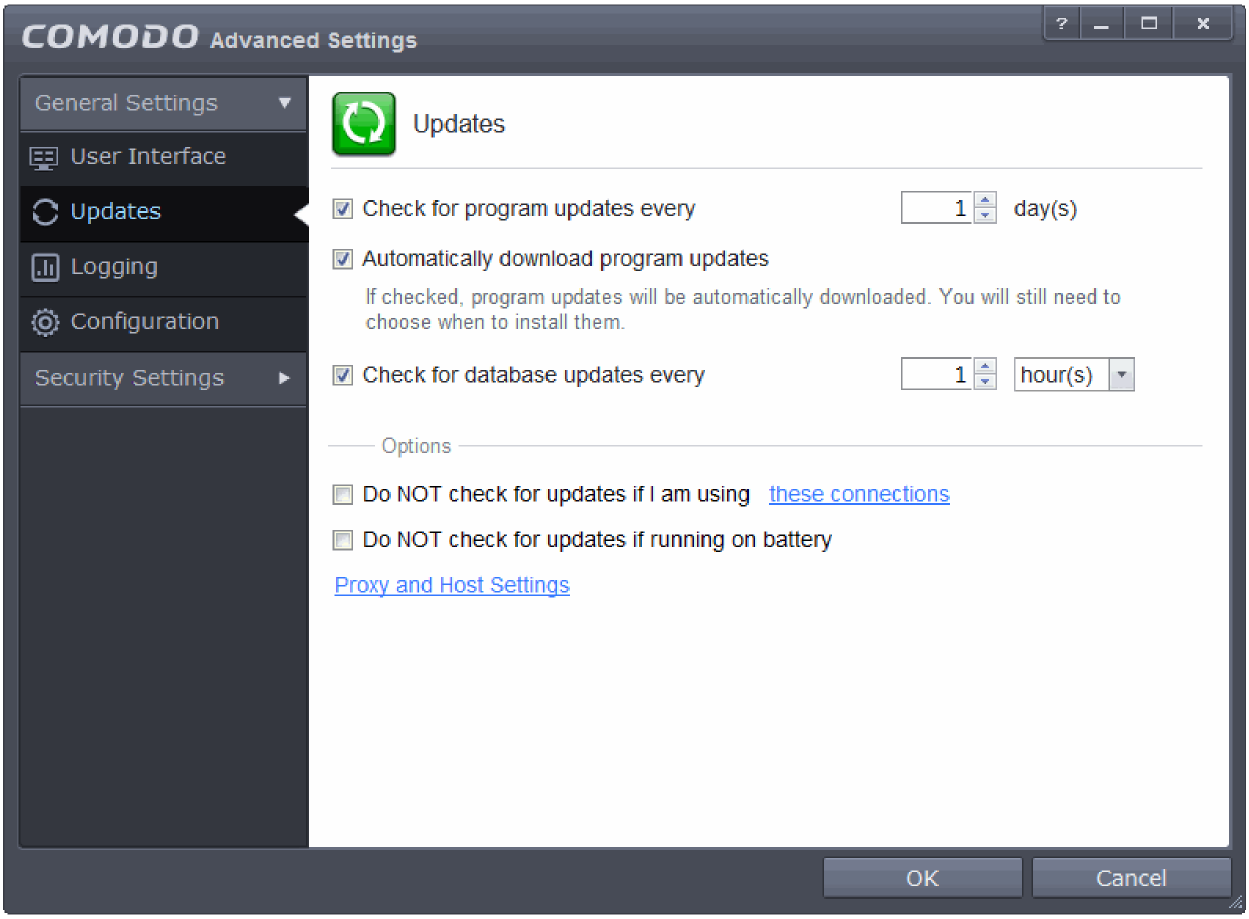
Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **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).*

6.1.2. Configure Program and Virus Database Updates

The 'Updates' area allows you to configure settings that govern CCS program and virus database updates.

This screen can be accessed by clicking 'Updates' under the 'General Settings' section of 'Advanced Settings':



Updates

☑ Check for program updates every 1 day(s)

☑ Automatically download program updates

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

☑ Check for database updates every 1 hour(s)

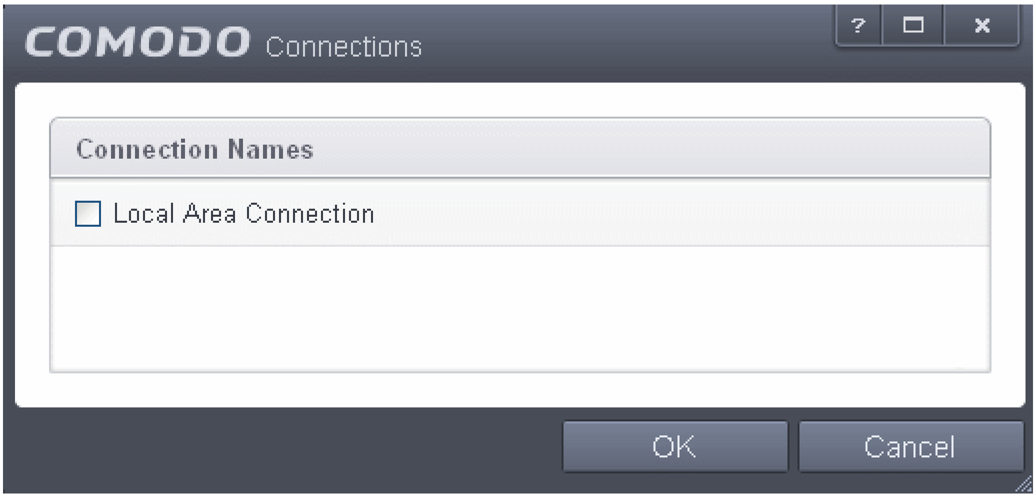
Options

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

□ Do NOT check for updates if running on battery

Proxy and Host Settings

- **Check program updates every NN day(s)** - Enables you to set the interval at which CCS will check for program updates. Select the interval in days from the drop-down combo box. ***(Default = Disabled)***
- **Automatically download program updates** - Instructs CCS to automatically download virus database updates as soon as they are available then notify you that they are ready for installation. (***Default=Enabled***)
- **Check for database updates every NN hour(s)/day(s)** - Enables you to set the interval at which CCS will check for virus signature database updates. 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 hour***)
- **Do NOT check updates if am using these connections** - Enables you to restrict CCS from checking for updates if you use certain types of Internet connection. 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.



☐ Local Area Connection

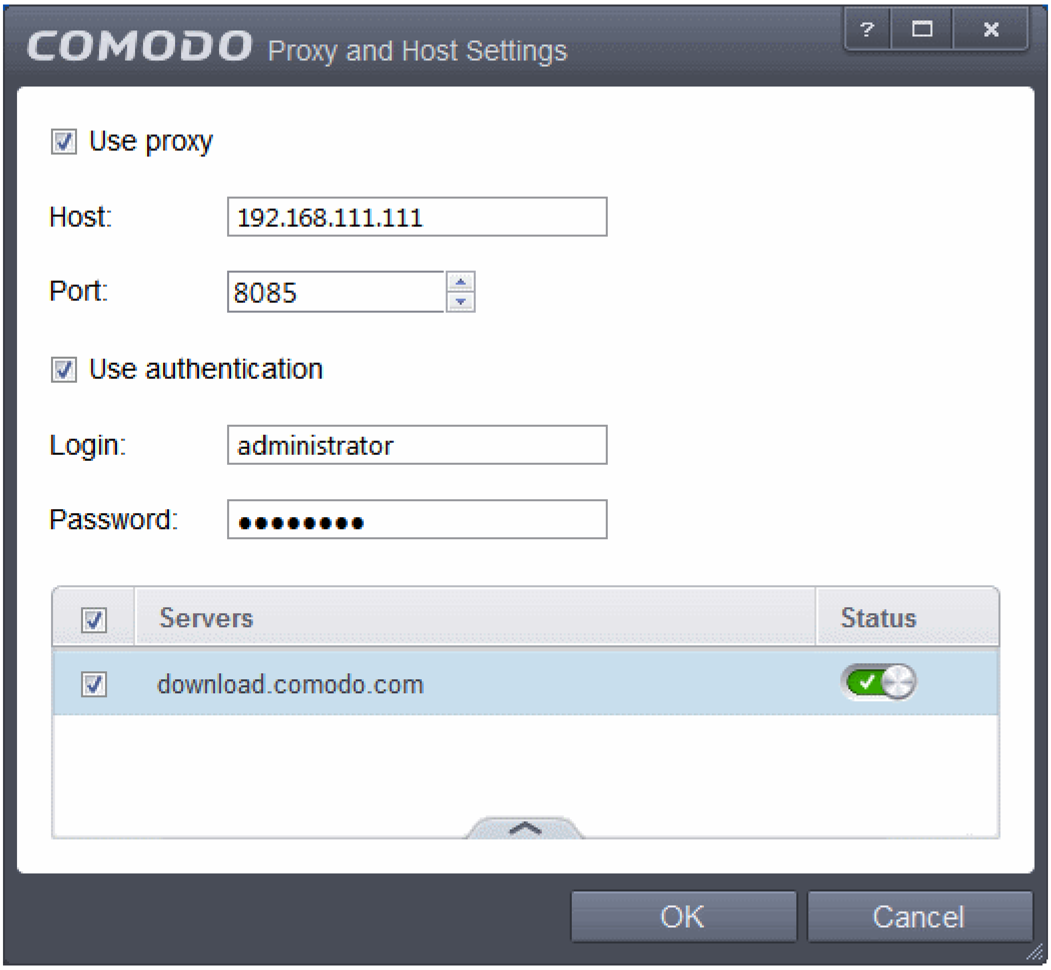
- Select the connection through which you do not want CCS to check for updates and click OK.

- **Do NOT check for updates if running on battery -** If enabled, CCS will not download updates if it detects your computer is running from battery power. This is intended to extend battery lifetime on laptops. (***Default = Disabled***)
- **Proxy and Host Settings -** Allows you to select the host from which updates are downloaded. By default, CCS will directly 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 conserve overall bandwidth consumption and accelerates the update process when 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.



☑ Use proxy

Host: 192.168.111.111

Port: 8085

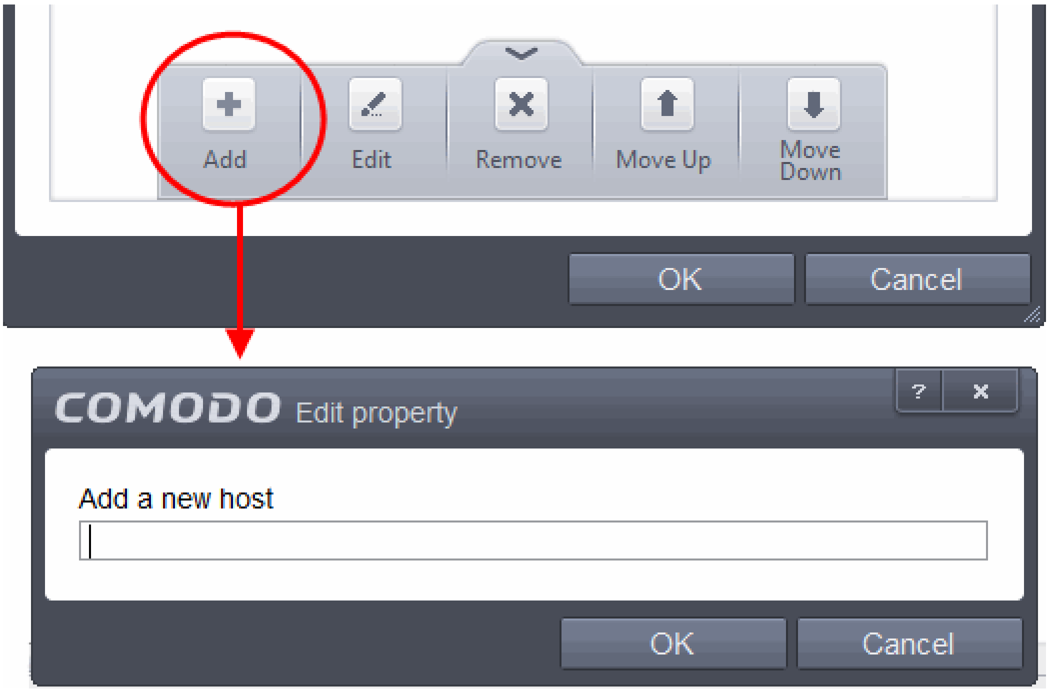
☑ Use authentication

Login: administrator

Password: ●●●●●●●●●

☑	Servers	Status
☑	download.comodo.com	✓

- 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 the handle at the bottom center of the 'Servers' panel, click the 'Add' button then enter the host name in the 'Edit Property' dialog.



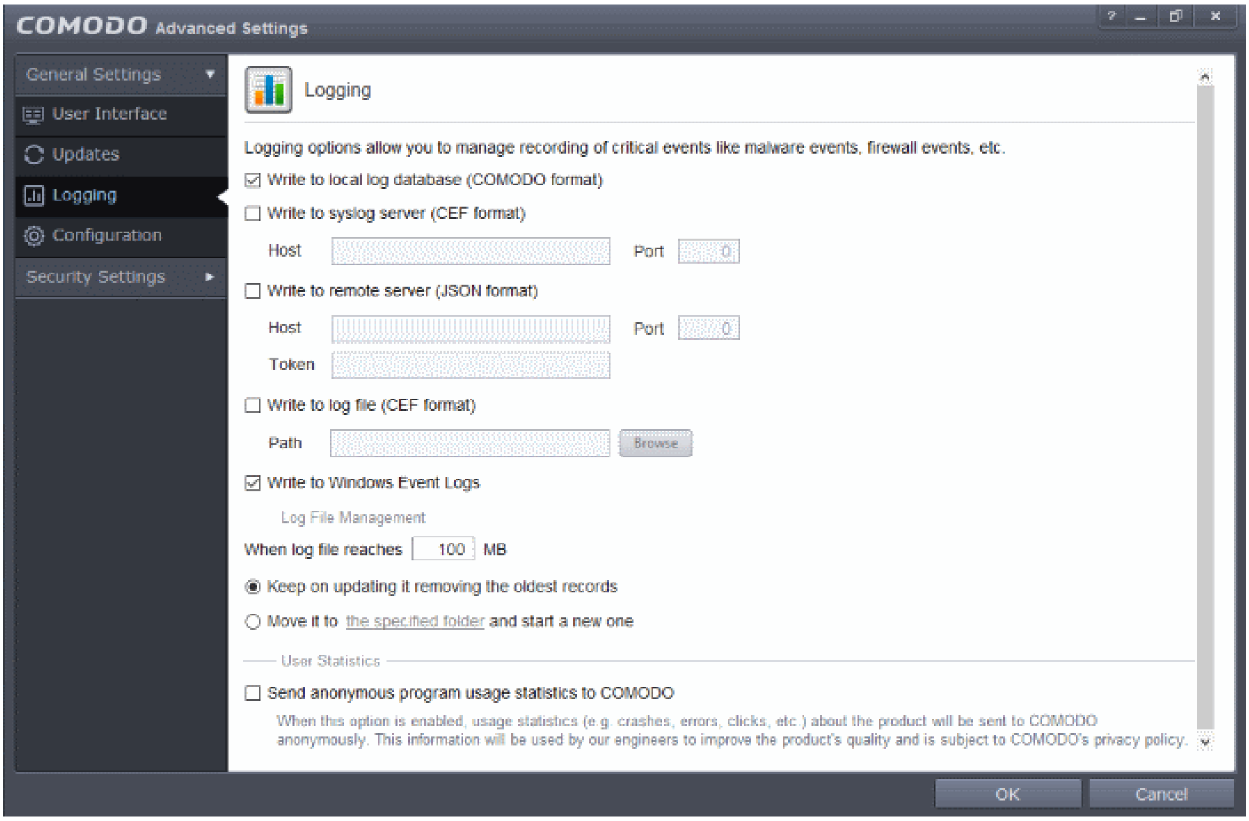
- If you specify multiple servers:
  - Activate or deactivate each update server using the 'Active' toggle switch beside it.
  - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CCS will commence downloading from the first server that contains new updates.
- Click 'OK' for your settings to take effect.

6.1.3. Log Settings

By default, Comodo Client Security maintains detailed logs of all Antivirus, HIPS, Containment, VirusScope and Firewall events. Logs are also created for 'Website Filtering', 'Device Control Events', 'Alerts Displayed', 'Tasks' 'File List Changes, Trusted Vendors List Changes 'and 'Configuration Changes'.

- The 'Logging' interface allows you to specify the locations for storing log file, maximum size of the log file in local storage and how CCS should react if the maximum file size is exceeded.

Note: If you wish to actually view, manage and export logs, then you need to open the 'View Logs' interface under 'General Settings' (Tasks > General Settings > View Logs)



Logging

Logging options allow you to manage recording of critical events like malware events, firewall events, etc.

☑ Write to local log database (COMODO format)

□ Write to syslog server (CEF format)

Host Port 0

□ Write to remote server (JSON format)

Host Port 0

Token

□ Write to log file (CEF format)

Path Browse

☑ Write to Windows Event Logs

Log File Management

When log file reaches 100 MB

● Keep on updating it removing the oldest records

○ Move it to the specified folder and start a new one

User Statistics

□ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, errors, clicks, etc.) about the product will be sent to COMODO anonymously. This information will be used by our engineers to improve the product's quality and is subject to COMODO's privacy policy.

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 > General Settings > View Logs interface. Refer to the section '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 ITSM 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 ITSM 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 ITSM 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 ITSM 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***)

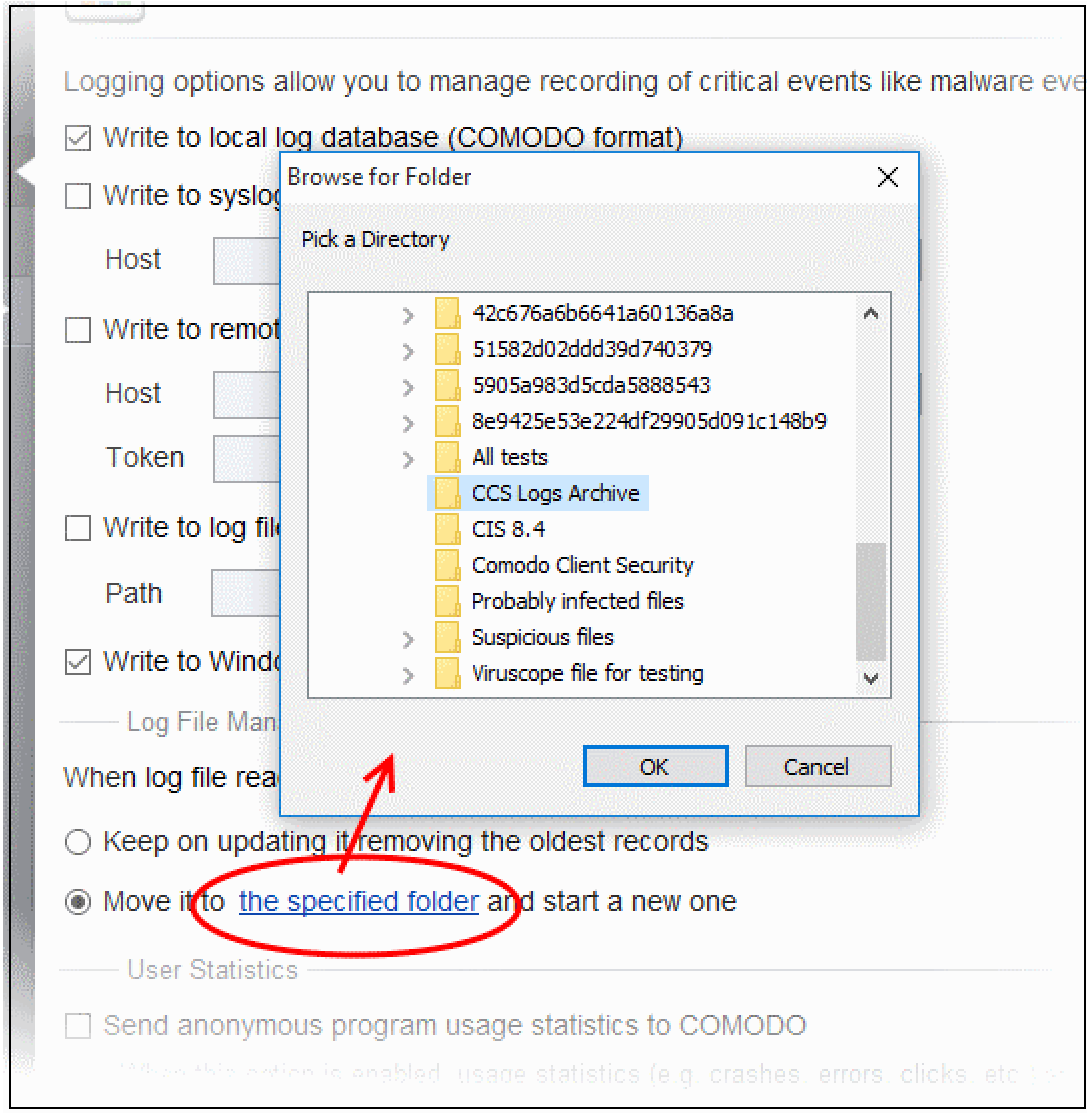
Log File Management

- **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 = Disabled).*



Logging options allow you to manage recording of critical events like malware eve

☑ Write to local log database (COMODO format)

□ Write to syslog

Host

□ Write to remot

Host

Token

□ Write to log fil

Path

☑ Write to Windo

Log File Man

When log file rea

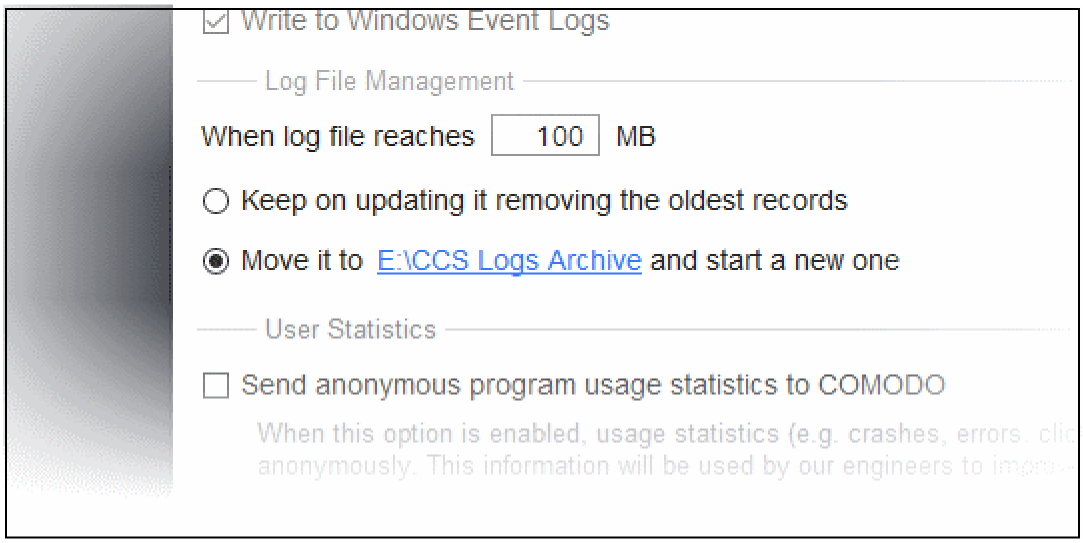
○ Keep on updating it removing the oldest records

● Move it to the specified folder and start a new one

User Statistics

□ Send anonymous program usage statistics to COMODO

The selected folder path will appear beside 'Move it to'.



☑ Write to Windows Event Logs

Log File Management

When log file reaches 100 MB

○ Keep on updating it removing the oldest records

● Move it to E:\CCS Logs Archive and start a new one

User Statistics

□ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, errors, cli anonymously. This information will be used by our engineers to impro

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

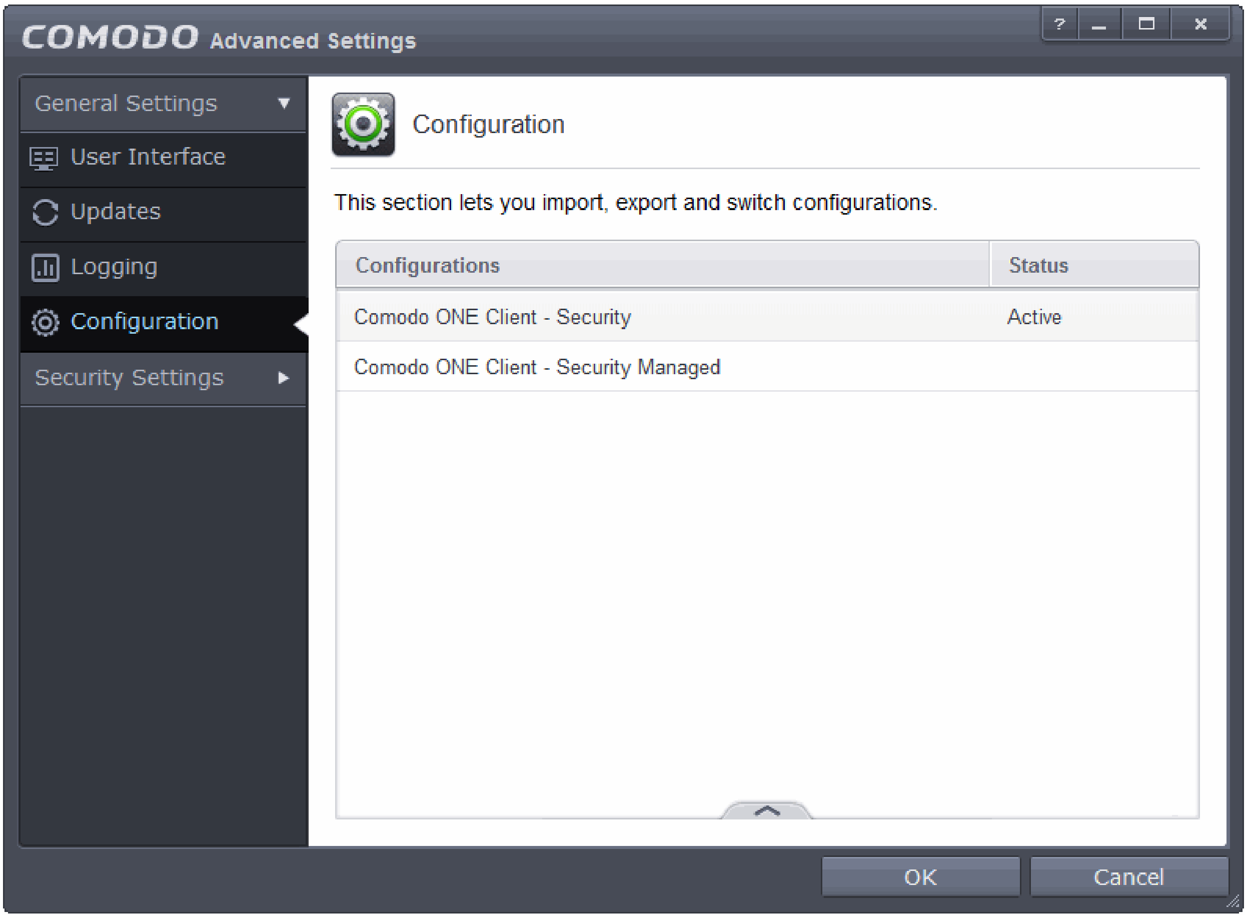
- **Send anonymous program usage statistics to Comodo -** Comodo collects the usage details from millions of CCS users to analyze their usage statistics (e.g. clicks, crashes, errors etc) to Comodo in order to improve the product's quality - for the continual enhancement of the product. Your CCS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. ***(Default = Disabled)***

6.1.4. Manage CCS Configurations

Comodo Client Security allows you to maintain, save and export a configuration of your security settings as configuration profiles. This is especially useful if you are a network administrator looking to roll out a standard security configuration across multiple computers. If you are upgrading your system and there is a need to uninstall and re-install Comodo Client Security then it can be great time-saver to export your configuration settings beforehand. After re-installation, you can import your previous settings and avoid having to configure everything over again.

Note: Any changes you make over time will be automatically stored in the currently active profile. If you want to export your current settings then export the 'Active' profile.

This panel can be accessed by clicking 'Configuration' under the 'General Settings' section of 'Advanced Settings':



This section lets you import, export and switch configurations.

Configurations	Status
Comodo ONE Client - Security	Active
Comodo ONE Client - Security Managed	

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

CCS is shipped with two present configurations, 'Comodo Client Security' and 'Comodo Client Security Managed' configurations. By default, the endpoints that are managed by ITSM will be applied 'Comodo One Client – Security Managed' configuration automatically and standalone endpoints (that are not managed by ITSM) with CCS will be applied 'One Client - Security' configuration. 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 - This configuration is activated by default on endpoints that are managed by ESM/ITSM and important default CCS configuration is given below:

- HIPS is disabled.
- Auto-Sandbox (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 - This configuration is activated by default on standalone computers, that is, computers not managed by ESM/ITSM, and important default CCS configuration is given below:

- HIPS is disabled.
- Auto-Sandbox (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 enabled.
- Viruscope alert is enabled

If you wish to switch to Comodo Client - Security option, you can **select** the option from the 'Configuration' panel.

6.1.4.2. Importing/Exporting and Managing Personal Configurations

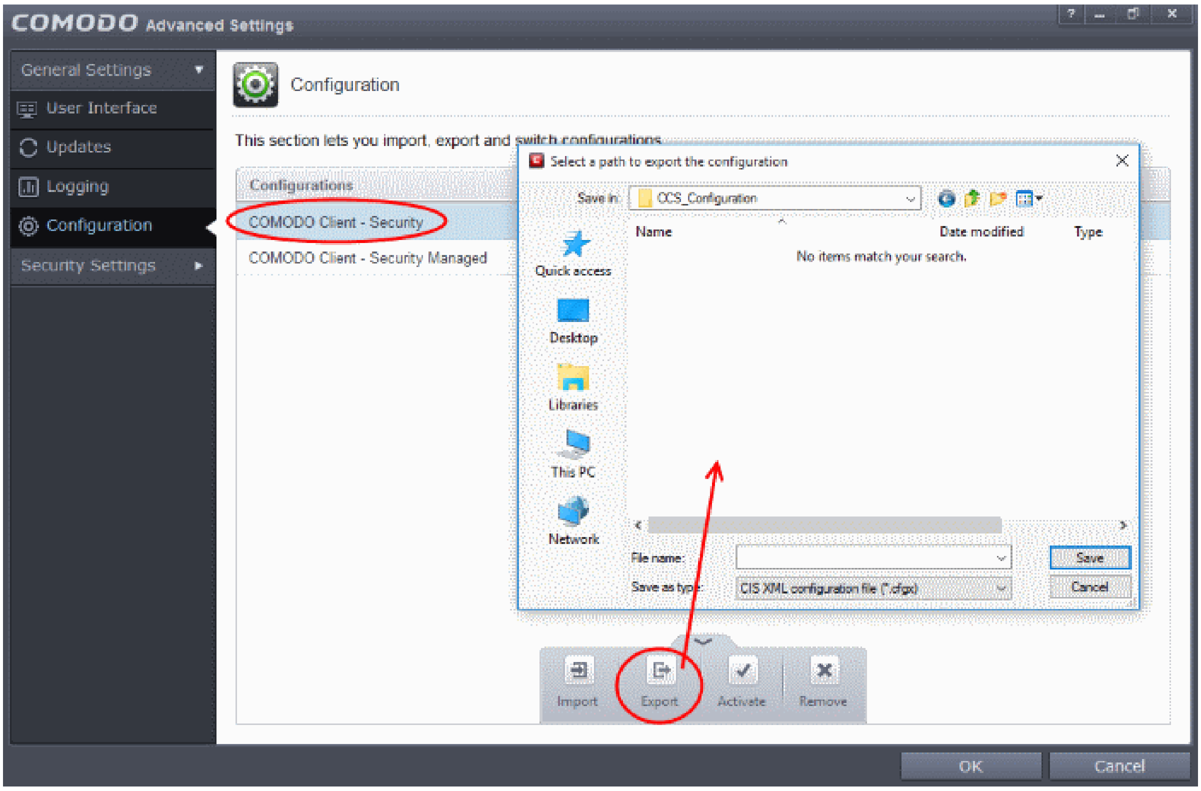
The CCS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Configuration' tab under 'General Settings' in 'Advanced Settings' interface.

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

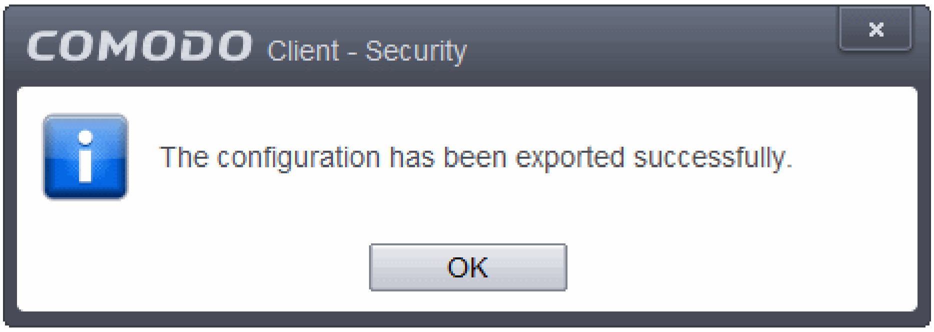
Exporting a stored configuration to a file

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration, click the handle from the bottom and choose 'Export'. The Select a path to export the configuration dialog will open.



3. 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.



The configuration has been exported successfully.

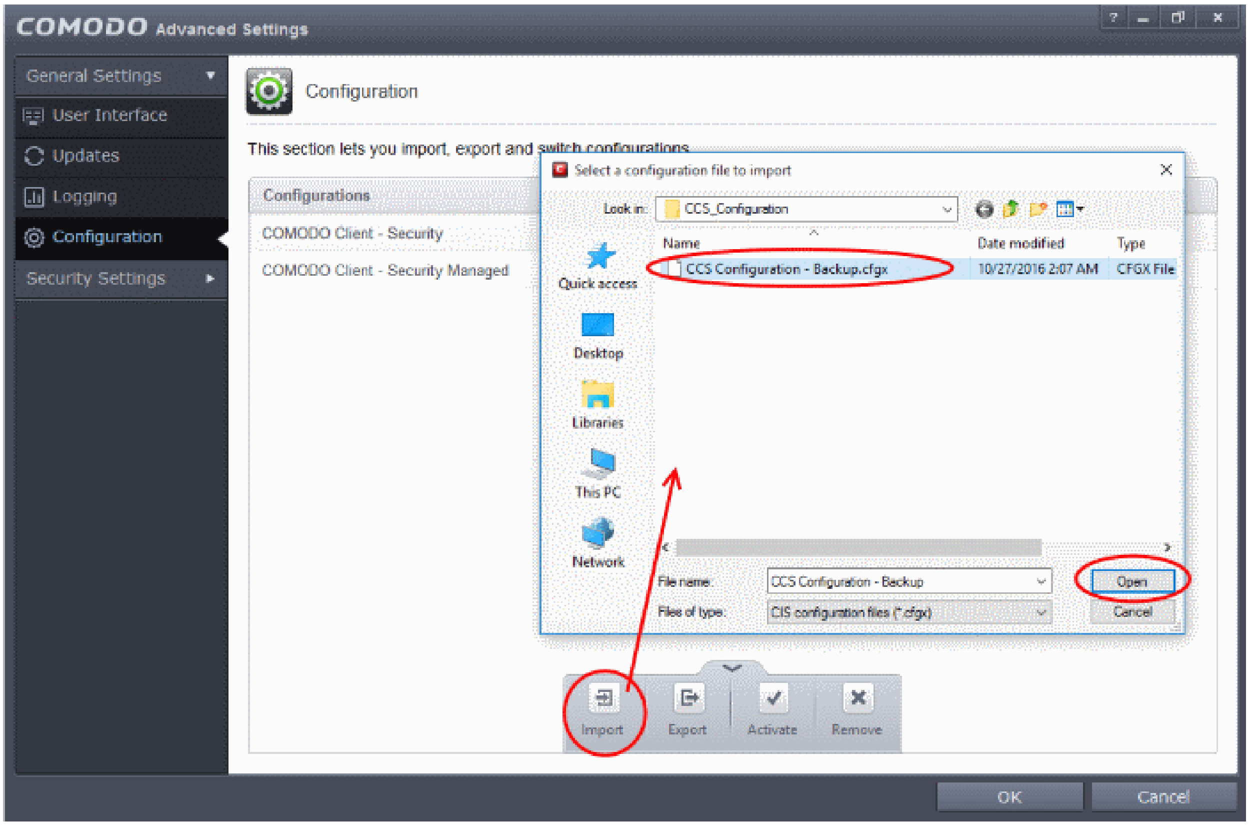
Importing a saved configuration from a file

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 'Advanced Tasks' interface, click the handle from the bottom and choose Import from the options.

The 'Select a configuration file to import' dialog will open.



This section lets you import, export and switch configurations.

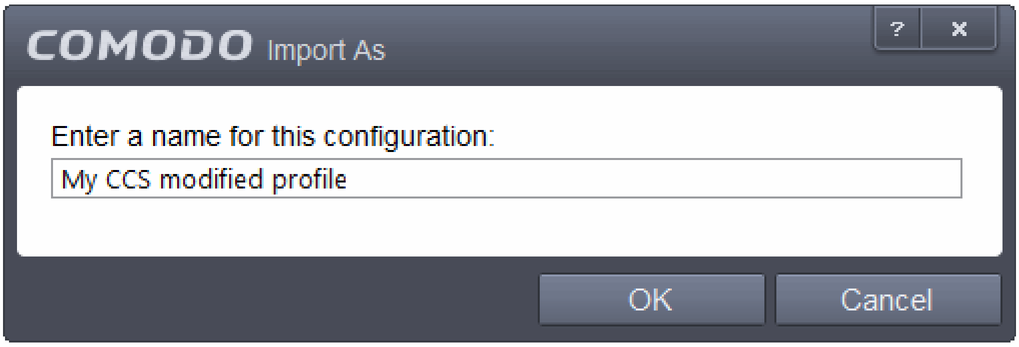
CCS Configuration - Backup.cfgx 10/27/2016 2:07 AM CFGX File

File name: CCS Configuration - Backup

Files of type: CIS configuration files (*.cfgx)

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

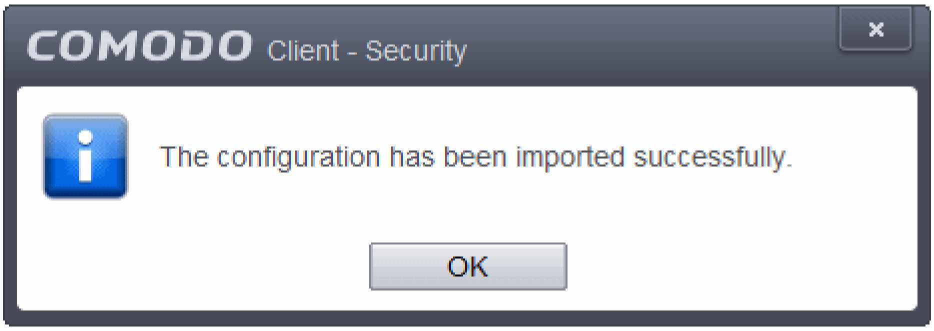
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



Enter a name for this configuration:

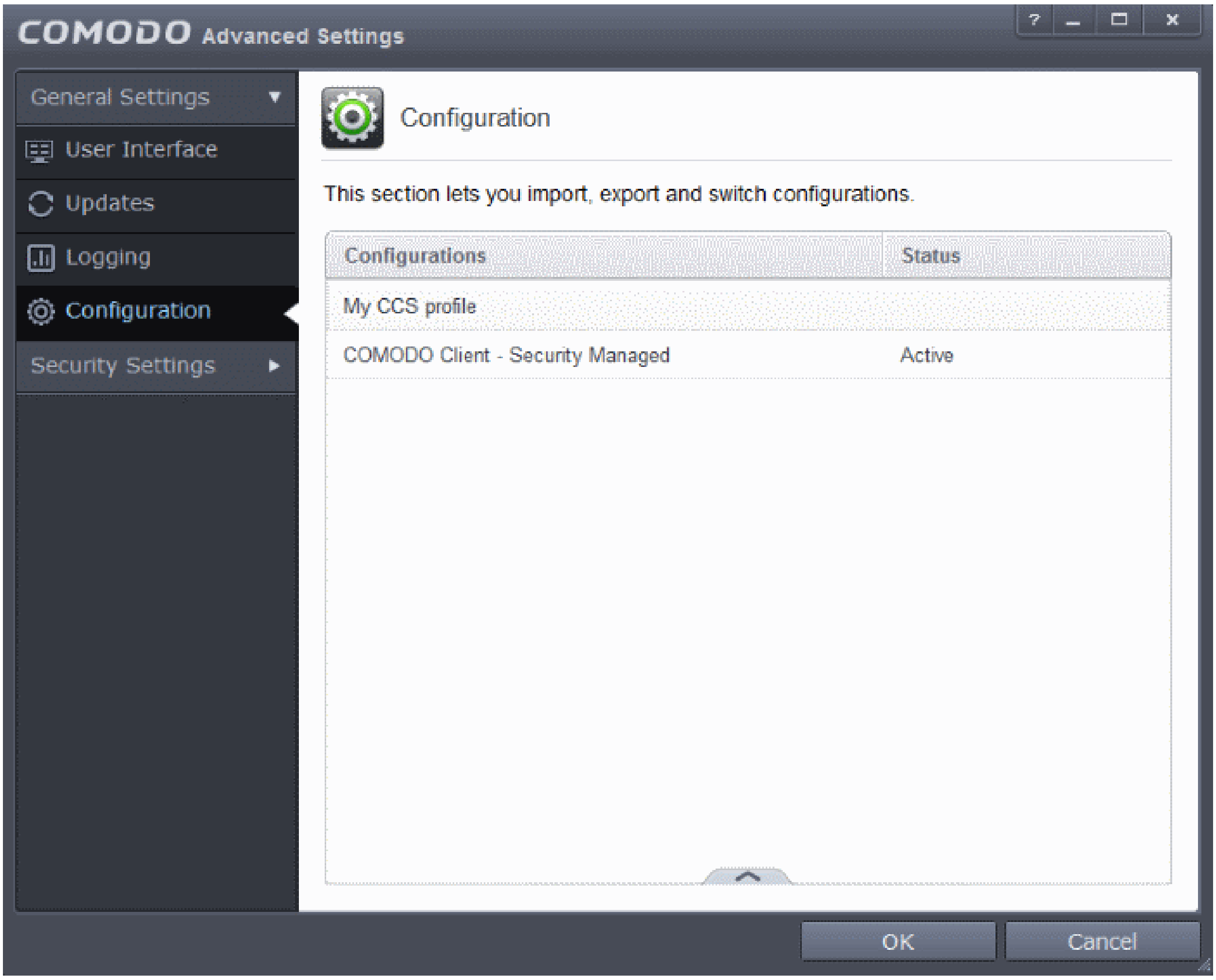
My CCS modified profile

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



The configuration has been imported successfully.

Once imported, the configuration profile is available for deployment by selecting it.



This section lets you import, export and switch configurations.

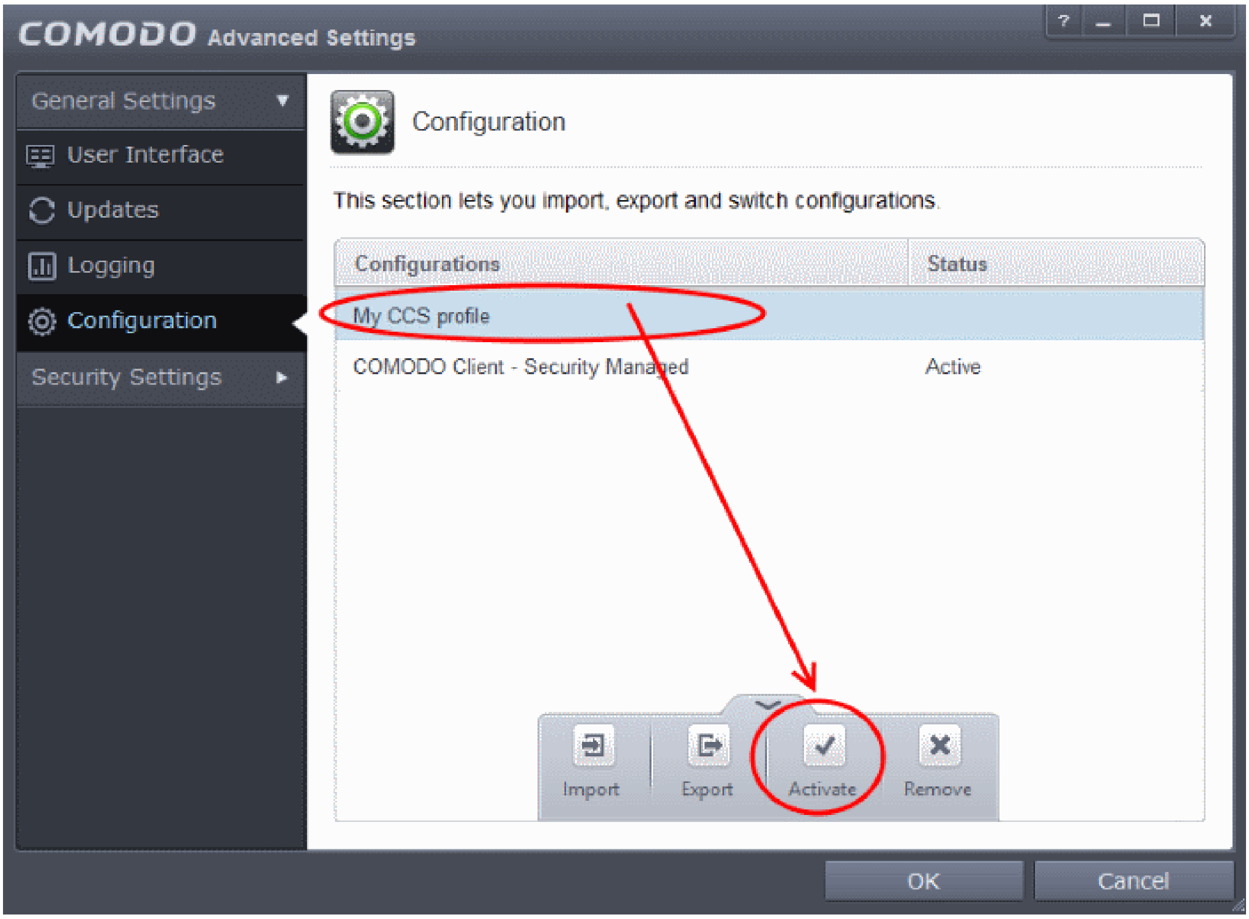
Configurations	Status
My CCS profile	
COMODO Client - Security Managed	Active

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 'Advanced Tasks' interface
2. Select the configuration profile you want to activate, click the handle from the bottom and choose Activate from the options.

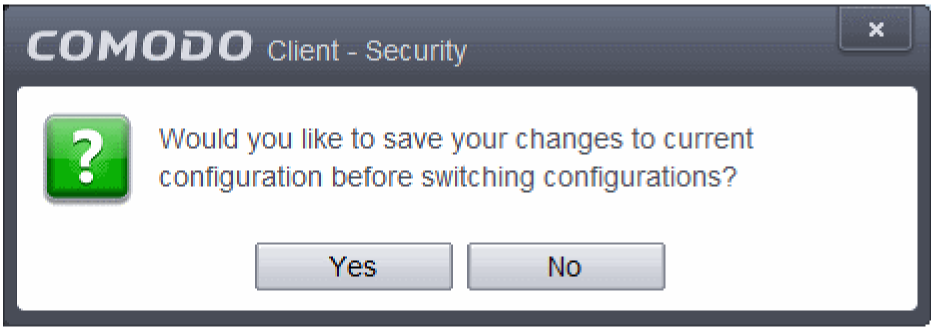


Configuration

This section lets you import, export and switch configurations.

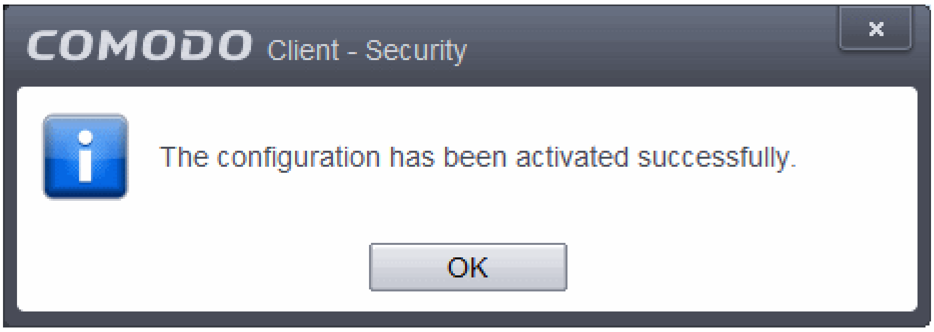
Configurations	Status
My CCS profile	
COMODO Client - Security Managed	Active

You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.



Would you like to save your changes to current configuration before switching configurations?

3. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.



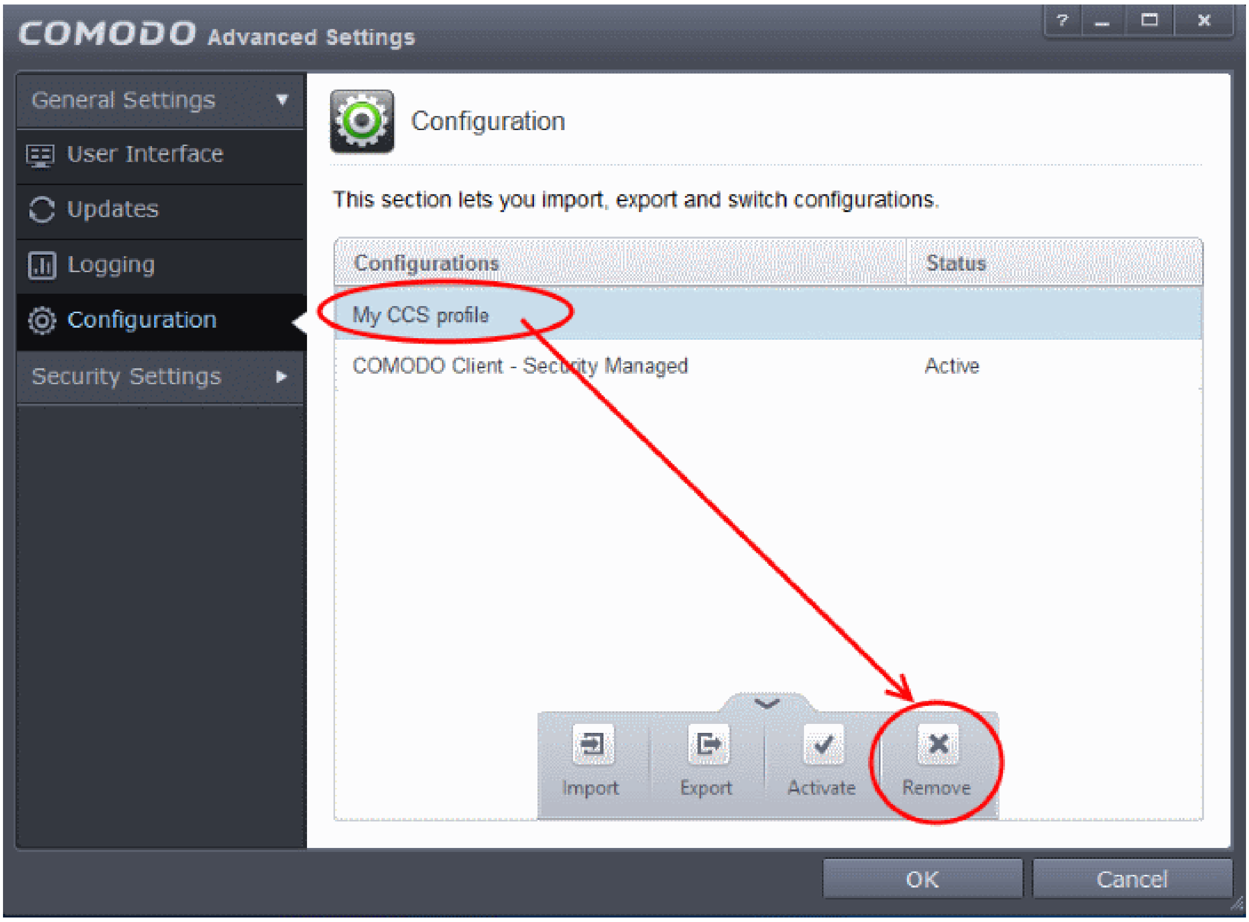
The configuration has been activated successfully.

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 'Advanced Tasks' interface
2. Select the configuration profile you want to delete, click the handle from the bottom and choose 'Remove' from the options.



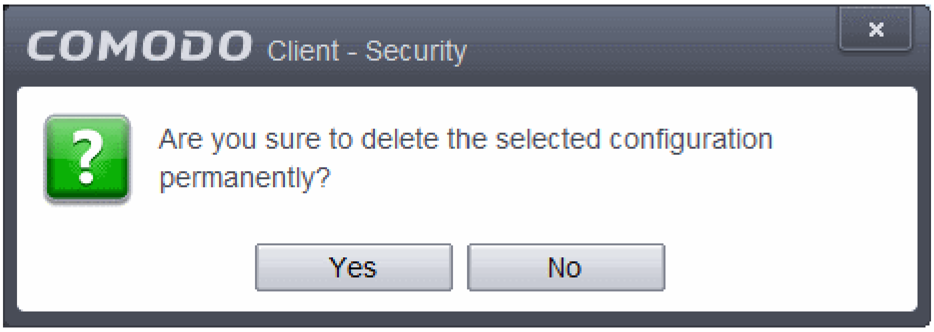
COMODO Advanced Settings

Configuration

This section lets you import, export and switch configurations.

Configurations	Status
My CCS profile	
COMODO Client - Security Managed	Active

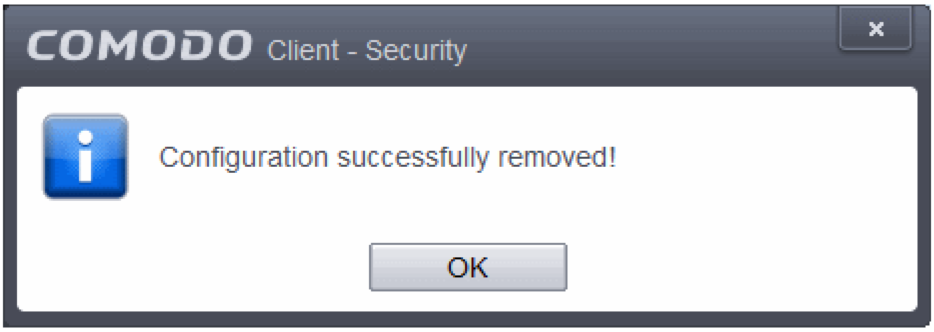
A confirmation dialog will be displayed.



COMODO Client - Security

Are you sure to delete the selected configuration permanently?

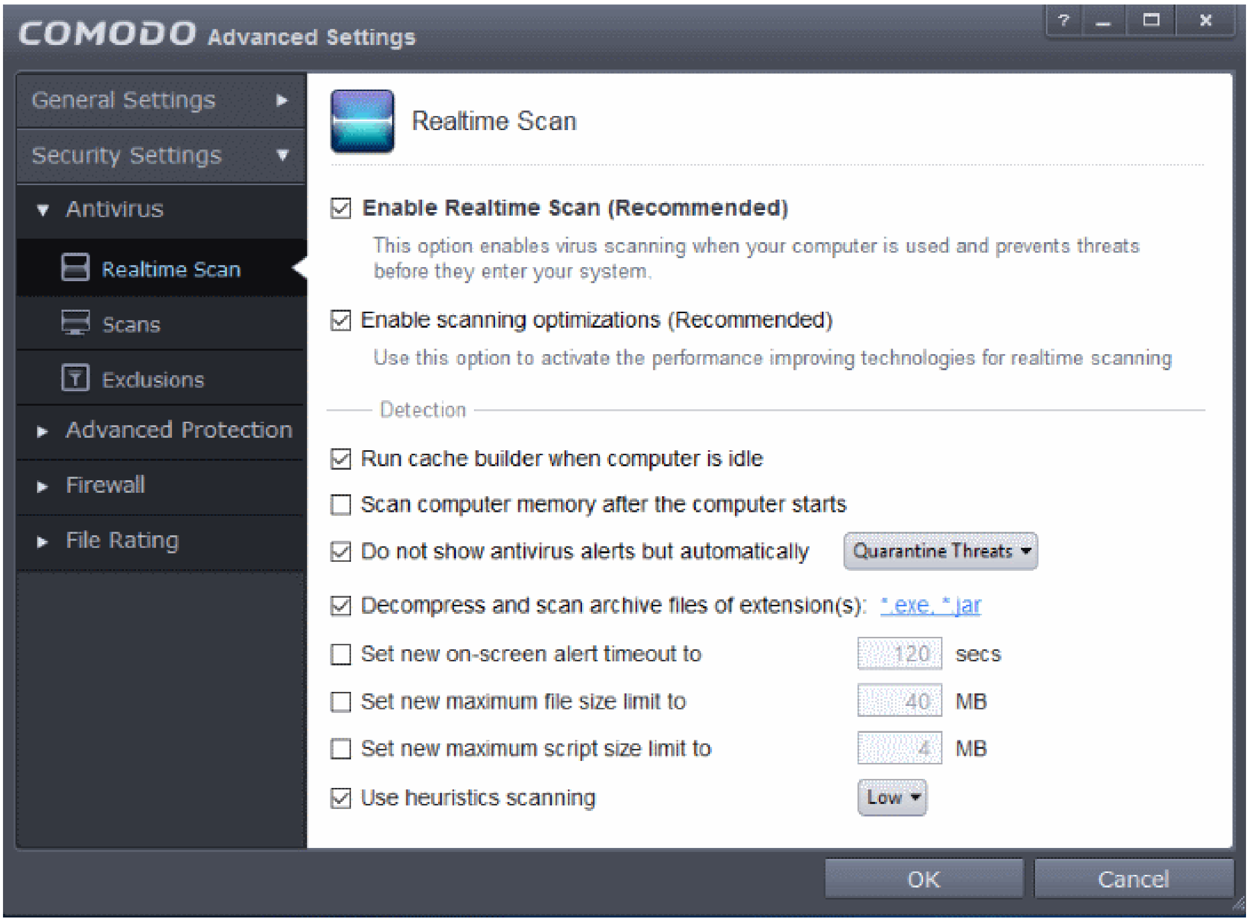
3. Click 'Yes'. The configuration profile will be deleted from your computer.



Configuration successfully removed!

6.2. Security Settings

The Security Settings area enables you to perform granular configuration of the Antivirus, Advanced Protection, Firewall and File ratings components. These settings play a large part in governing the level of security offered by the application. Comodo Client Security ships with secure defaults for all major settings so provides 'out-of-the-box' protection for all users.



Realtime Scan

☑ Enable Realtime Scan (Recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning

Detection

☑ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☑ Do not show antivirus alerts but automatically Quarantine Threats

☑ Decompress and scan archive files of extension(s): *.exe, *.jar

□ Set new on-screen alert timeout to 120 secs

□ Set new maximum file size limit to 40 MB

□ Set new maximum script size limit to 4 MB

☑ Use heuristics scanning Low

Click the following links to go straight to the topic that explains the respective settings screen:

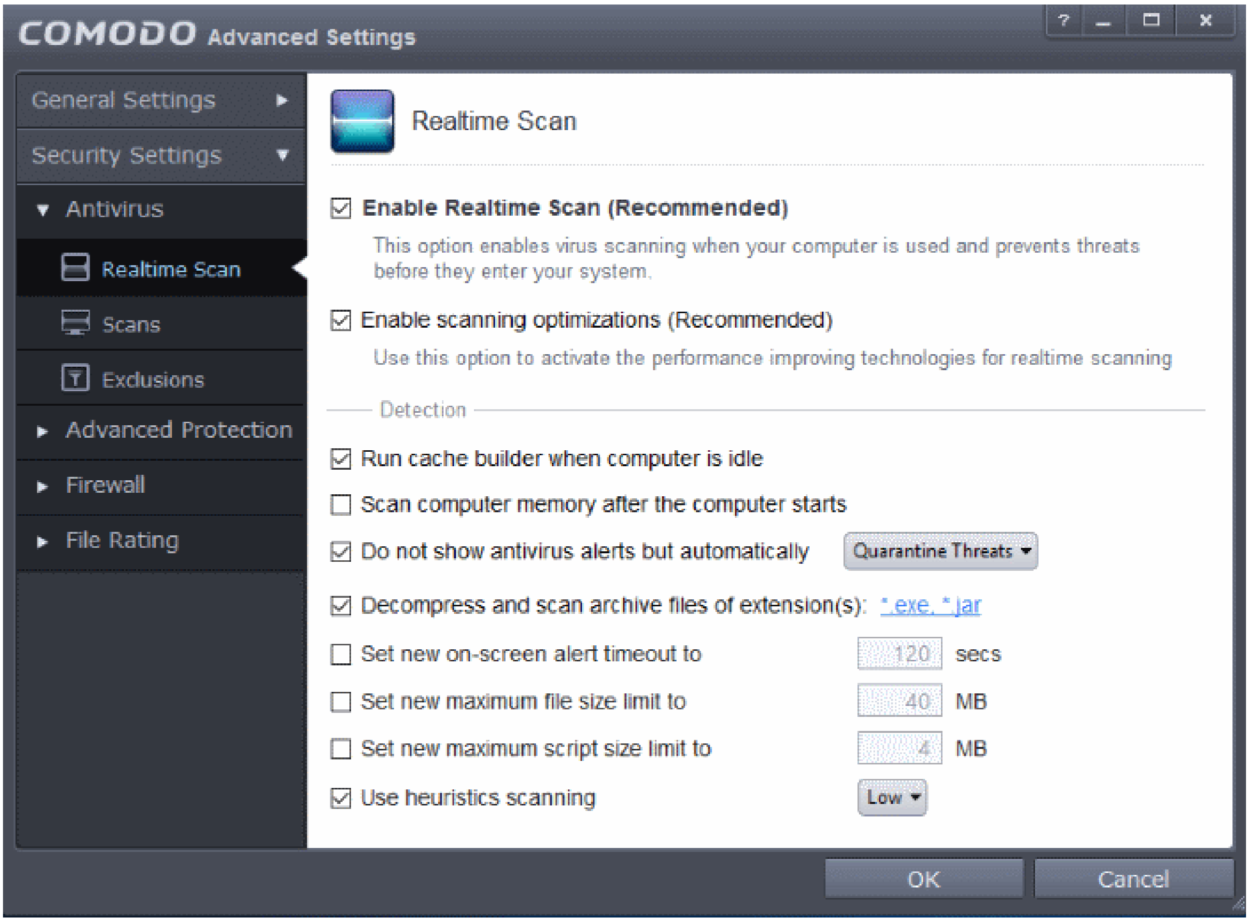
- Antivirus Settings
    - Real-time Scanner Settings
    - Custom Scan Settings
    - Exclusions
- Advanced Protection Settings

- HIPS Behavior Settings
- Active HIPS Rules
- Predefined HIPS Rule Sets
- Protected Objects
- HIPS Groups
- Comodo Containment
- Containment Settings
- Configuring Rules for Auto-Containment
- Viruscope
- Device Control Settings

- Firewall Settings
  - Firewall Behavior Settings
  - Application Rules
  - Global Rules
  - Firewall Rule Sets
  - Network Zones
  - Port Sets
  - Website Filtering
- Manage File Rating
  - File Rating Settings
  - File Groups
  - File List
  - Submitted Files
  - Trusted Vendors

6.2.1. Antivirus Settings

The Antivirus Settings category has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe).



Realtime Scan

☑ Enable Realtime Scan (Recommended)

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning

Detection

☑ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☑ Do not show antivirus alerts but automatically [Quarantine Threats]

☑ Decompress and scan archive files of extension(s): *.exe, *.jar

□ Set new on-screen alert timeout to 120 secs

□ Set new maximum file size limit to 40 MB

□ Set new maximum script size limit to 4 MB

☑ Use heuristics scanning [Low]

Click the following links to jump to each section:

- Real Time Scan - To set the parameters for on-access scanning;
- Custom Scan - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans;
- Exclusions- To see the list of ignored threats and to set the parameters for Exclusions.

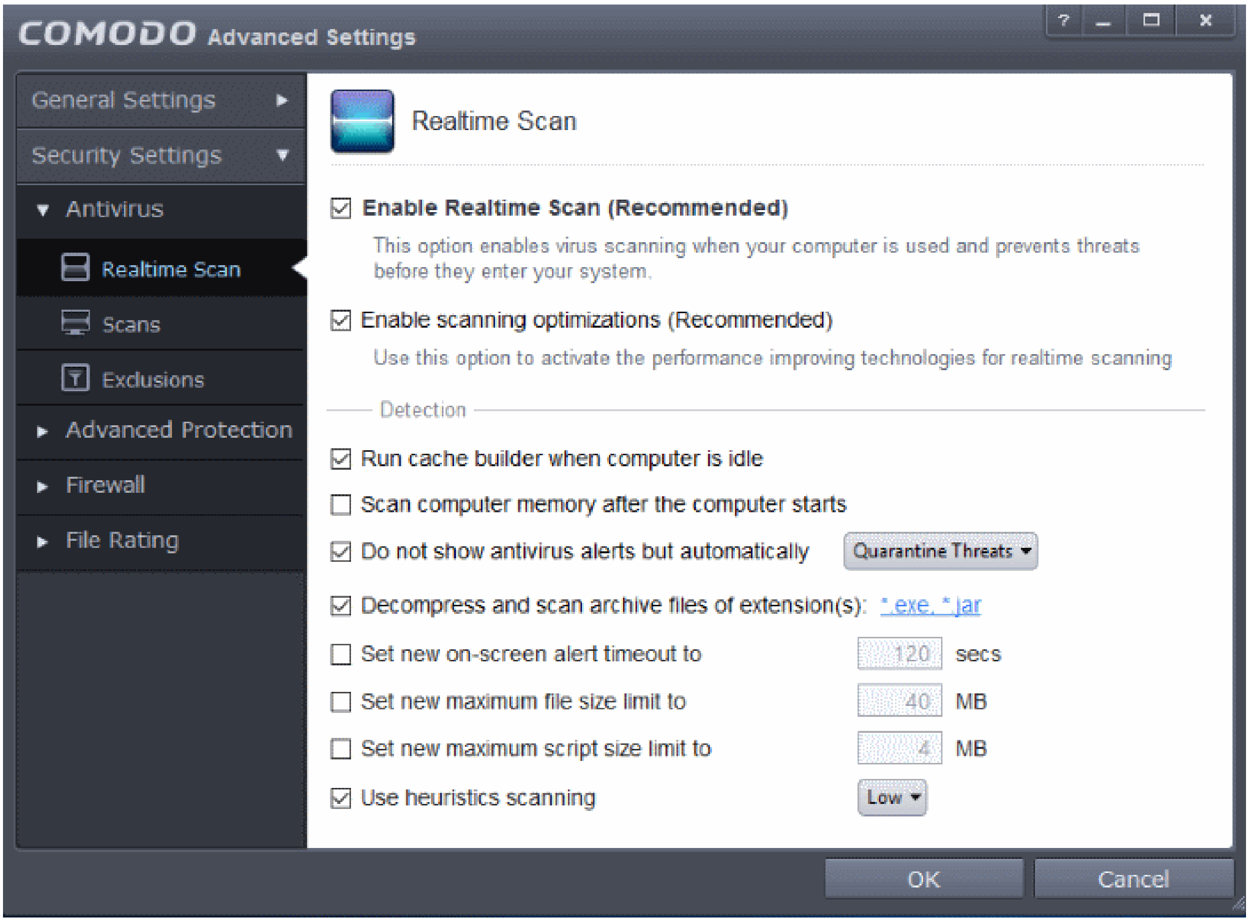
6.2.1.1. Real-time Scanner Settings

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

The real-time scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, however, you can specify that CCS does not show you alerts if viruses are found but automatically deals with them (choice of auto-quarantine or auto-block/delete). It is highly recommended that leave the Real Time Scanner enabled to ensure your system remains continually free of infection.

To open the Real Time Scan settings panel

- Click 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Antivirus > Realtime Scan':



Realtime Scan

☑ **Enable Realtime Scan (Recommended)**

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning

Detection

☑ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☑ Do not show antivirus alerts but automatically [Quarantine Threats]

☑ Decompress and scan archive files of extension(s): *.exe, *.jar

□ Set new on-screen alert timeout to 120 secs

□ Set new maximum file size limit to 40 MB

□ Set new maximum script size limit to 4 MB

☑ Use heuristics scanning [Low]

- **Enable Realtime Scan** - Allows you to enable or disable real-time scanning. Comodo recommends to leave this option selected (***Default=Enabled***)
- **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to reduce consumption of system resources and speed-up the scanning process ***(Default = Enabled)***

Detection Settings

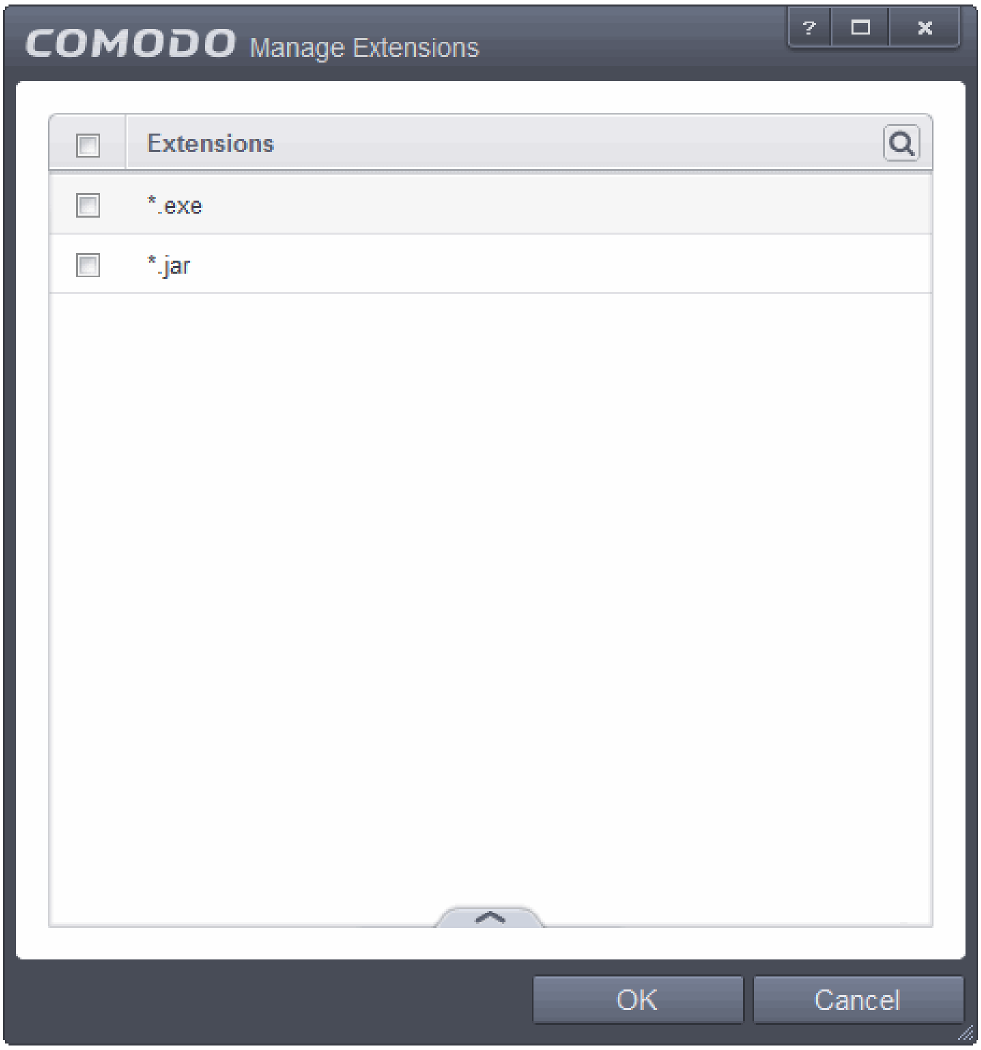
- **Run cache builder when computer is idle** - CCS runs the Antivirus Cache Builder whenever the computer is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (***Default = Enabled***)
- **Scan computer memory after the computer starts** - When this check box is selected, the Antivirus scans the system memory during system start-up ***(Default = Disabled)***
- **Do not show antivirus alerts but automatically** - Allows you to configure whether or not to show antivirus alerts when malware is encountered. Choosing 'Do not show antivirus alerts but automatically' 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 - either 'Block Threats' or 'Quarantine Threats'. (***Default = Enabled***)
  - **Quarantine Threats** - Moves the detected threat(s) to quarantine for your later assessment and action. (***Default***)
  - **Block Threats** - Stops the application or file from execution, if a threat is detected in it.

Note: If you deselect this option and thus enable alerts then your choice of quarantine/block is presented within the alert itself.

- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default = Enabled)***

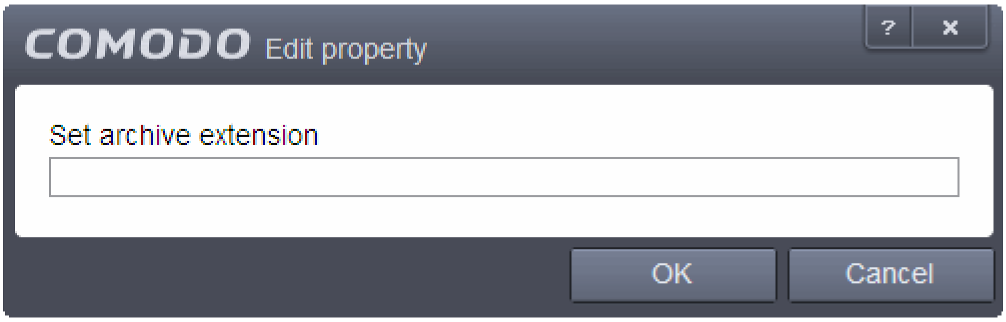
You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

- Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.



☐	Extensions
☐	*.exe
☐	*.jar

- To add a file type, click the handle at the bottom center and click 'Add'.



Set archive extension

- Enter the extension (e.x.: rar, msi, zip, 7z, cab and so on) to be included in the 'Edit property' dialog and click 'OK'.
- Repeat the process to add more extensions
- Click 'OK' in the 'Manage Extensions' dialog

- **Set new on-screen alert timeout to -** This box allows you to set the time period (in seconds) for which the alert message should stay on the screen. (***Default = 120 seconds***)

- **Set new maximum file size limit to -** This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned. (***Default = 40 MB***)
- **Set new maximum script size to -** This box allows you to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (***Default = 4 MB***)
- **Use heuristics scanning -** Allows you to enable or disable Heuristics scanning and define scanning level. (***Default = Low***)

  Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether 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 behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  Leave this option selected to keep Heuristics scanning enabled. Else, deselect this checkbox. If enabled, you can select the level of 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.

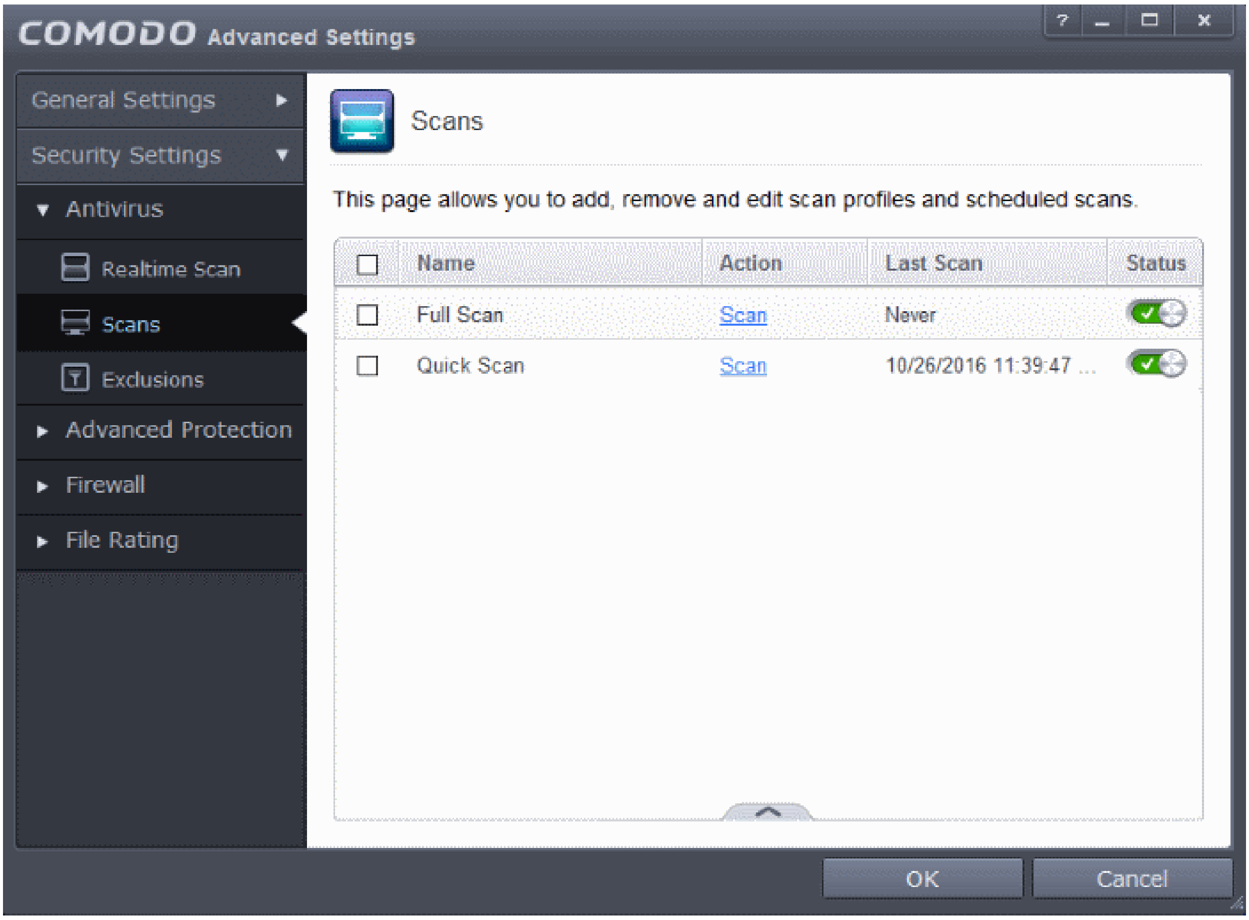
6.2.1.2. Scan Profiles

The Scan Profiles area allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CCS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)
- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To open the panel

- Click Security Settings > Antivirus > 'Scans' tab in the 'Advanced Settings' panel.



Scans

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

☐	Name	Action	Last Scan	Status
☐	Full Scan	Scan	Never	✓
☐	Quick Scan	Scan	10/26/2016 11:39:47 ...	✓

CCS ships with two predefined scan profiles:

- **Full Scan** - Covers every local drive, folder and file on your system.
- **Quick Scan** - Covers critical areas in your system which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of your computer and keeping them clean is essential.

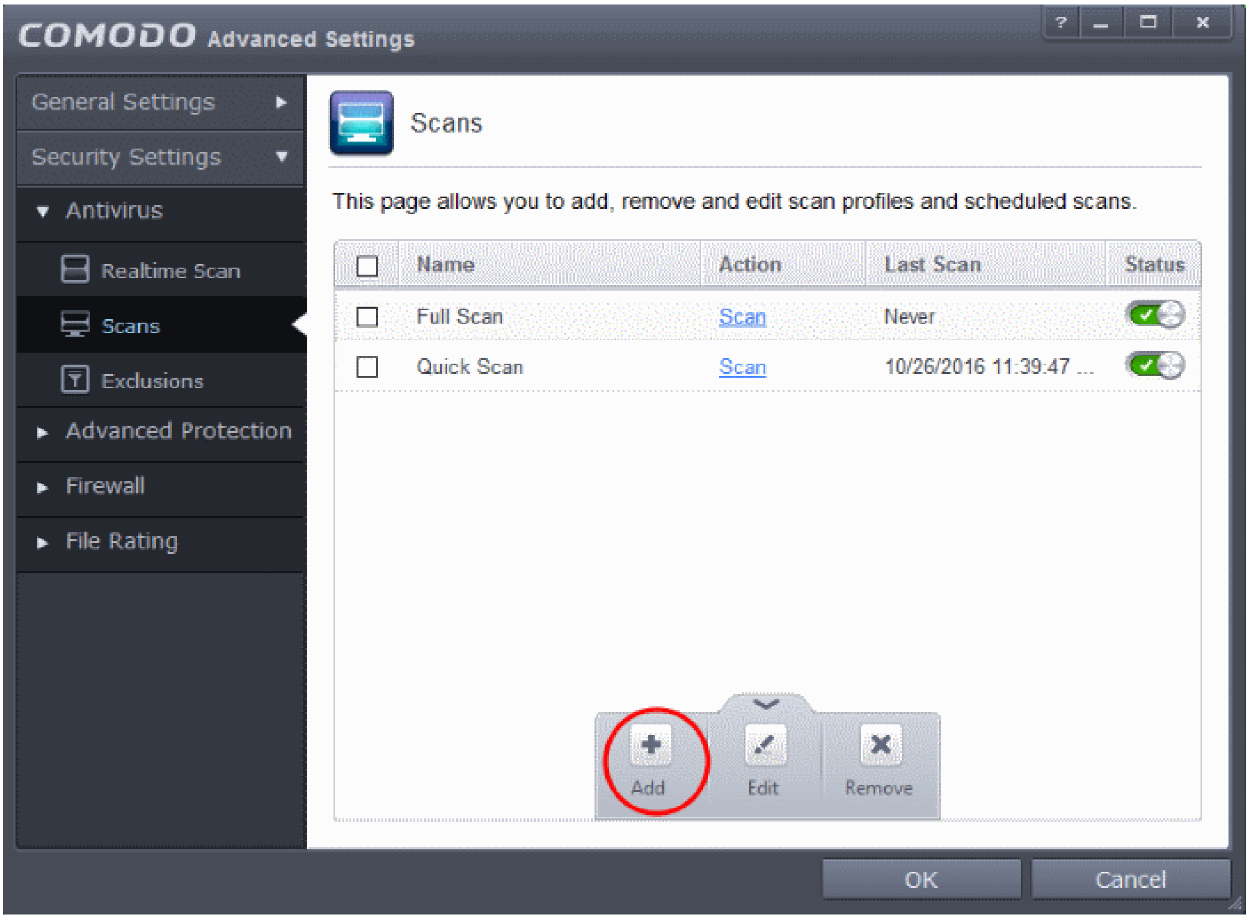
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

- Creating a Scan Profile
- Running a custom scan

To create a custom profile

- Click the handle at the bottom of the interface then click the 'Add' button:

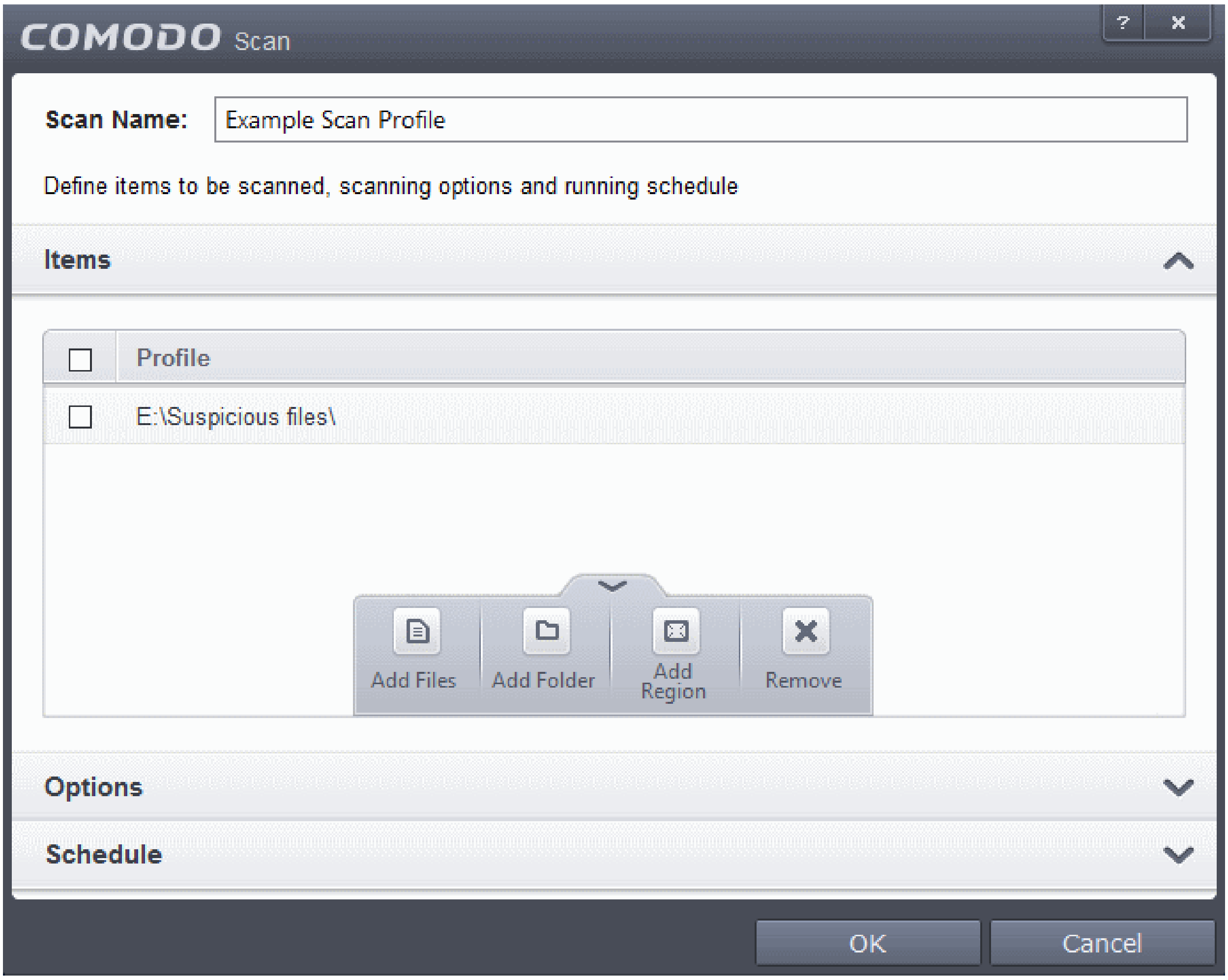


This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	10/26/2016 11:39:47 ...	✓

The scan profile interface will be displayed.

- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items that should be included in the profile

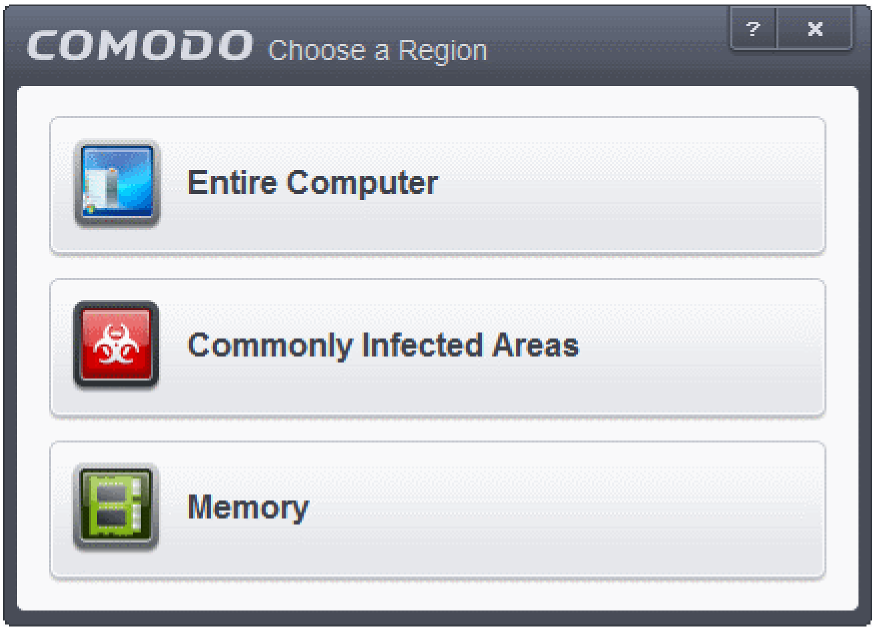


COMODO Scan

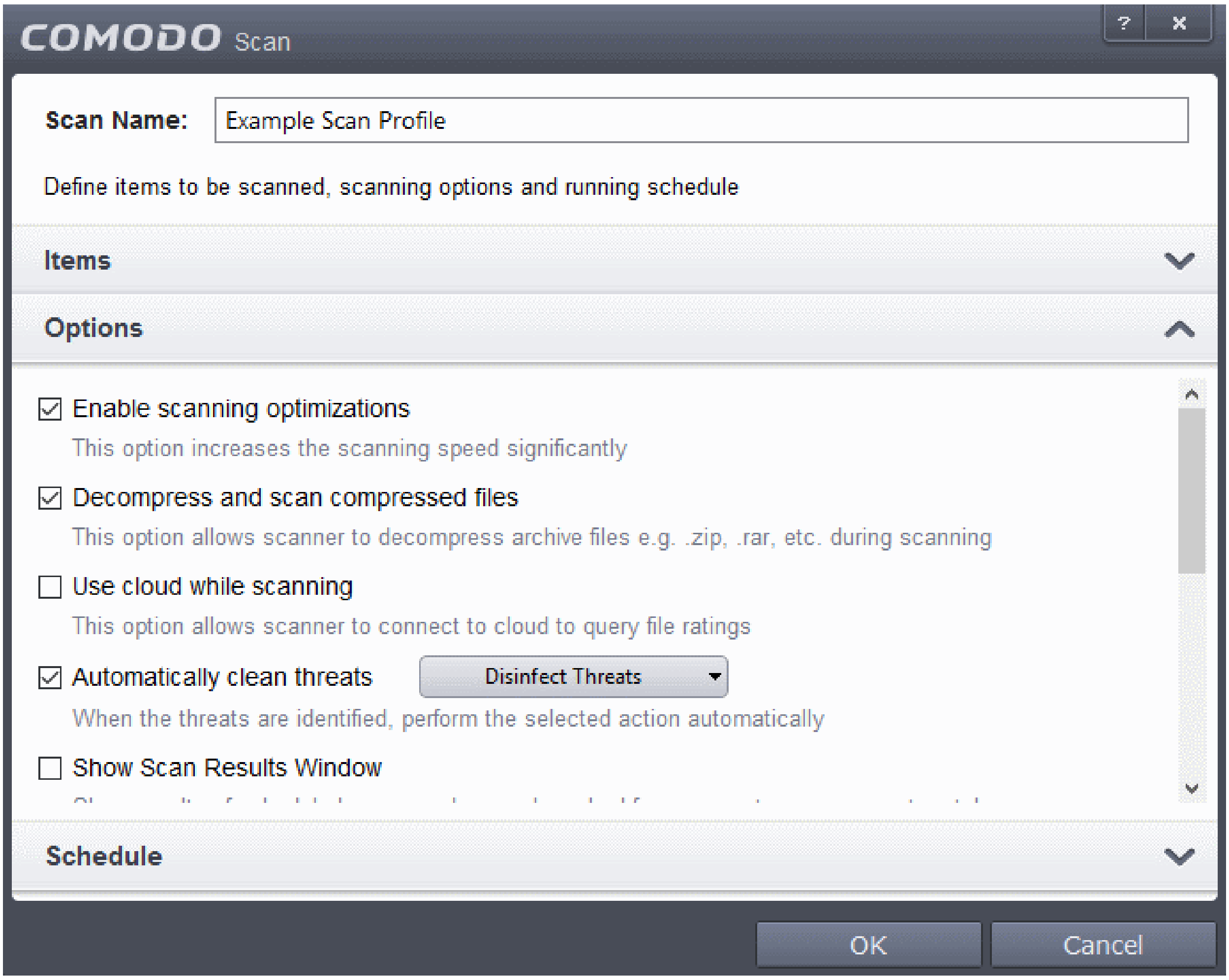
Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

- **Add Files** - Allows you to navigate to specific files that you wish to add to the profile
- **Add Folder** - Opens the 'Browse For Folder' window and allows you to select entire folders
- **Add Region** - Allows you to add predefined regions to the profile. For example, 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.



- Repeat the process to add more items into the profile
- Click 'Options' to further customize the scan



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

☑ Enable scanning optimizations
This option increases the scanning speed significantly

☑ Decompress and scan compressed files
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

□ Use cloud while scanning
This option allows scanner to connect to cloud to query file ratings

☑ Automatically clean threats — Disinfect Threats
When the threats are identified, perform the selected action automatically

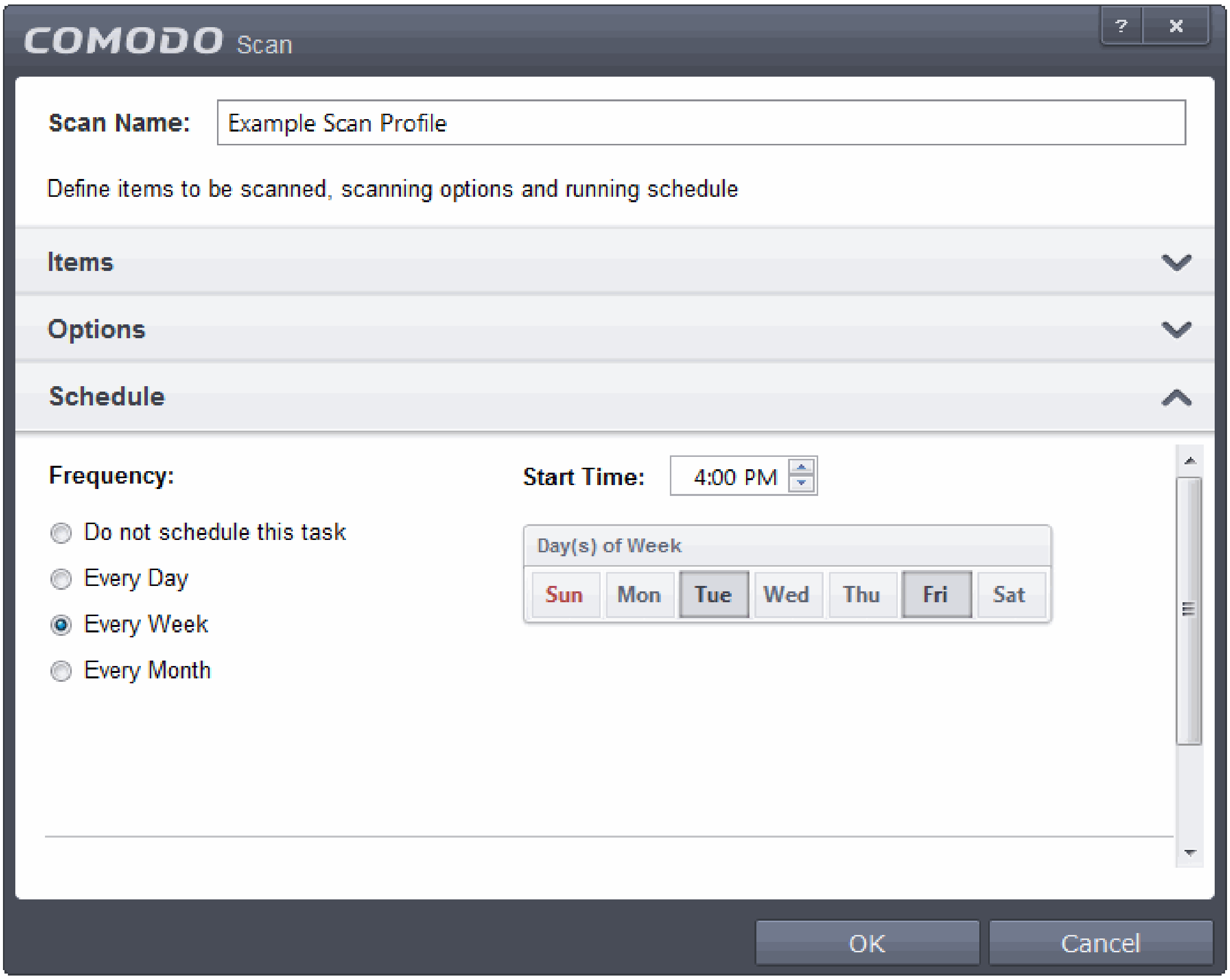
□ Show Scan Results Window

- **Options**:
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)*** .
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
  - **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local anitvirus database is out-dated. ***(Default = Disabled)***.
  - **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine. ***(Default = Enabled with Disinfect Threats option)***
  - **Show Scan Results Window** – If enabled, the results of custom scans and scans that are launched from ITSM will be displayed. ***(Default = Disabled)***
  - **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 = Disabled).***

    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.

        - **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 scanning from High to Low and to run at background. ***(Default = Disabled)***
    - **Update virus database before running** - Selecting this option makes CCS to check for virus database updates and if available, update the database before commencing the scan. ***(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***).
- If you want the scan to be performed periodically, set a Schedule for the custom scan by clicking 'Schedule'



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Frequency:

○ Do not schedule this task

○ Every Day

● Every Week

○ Every Month

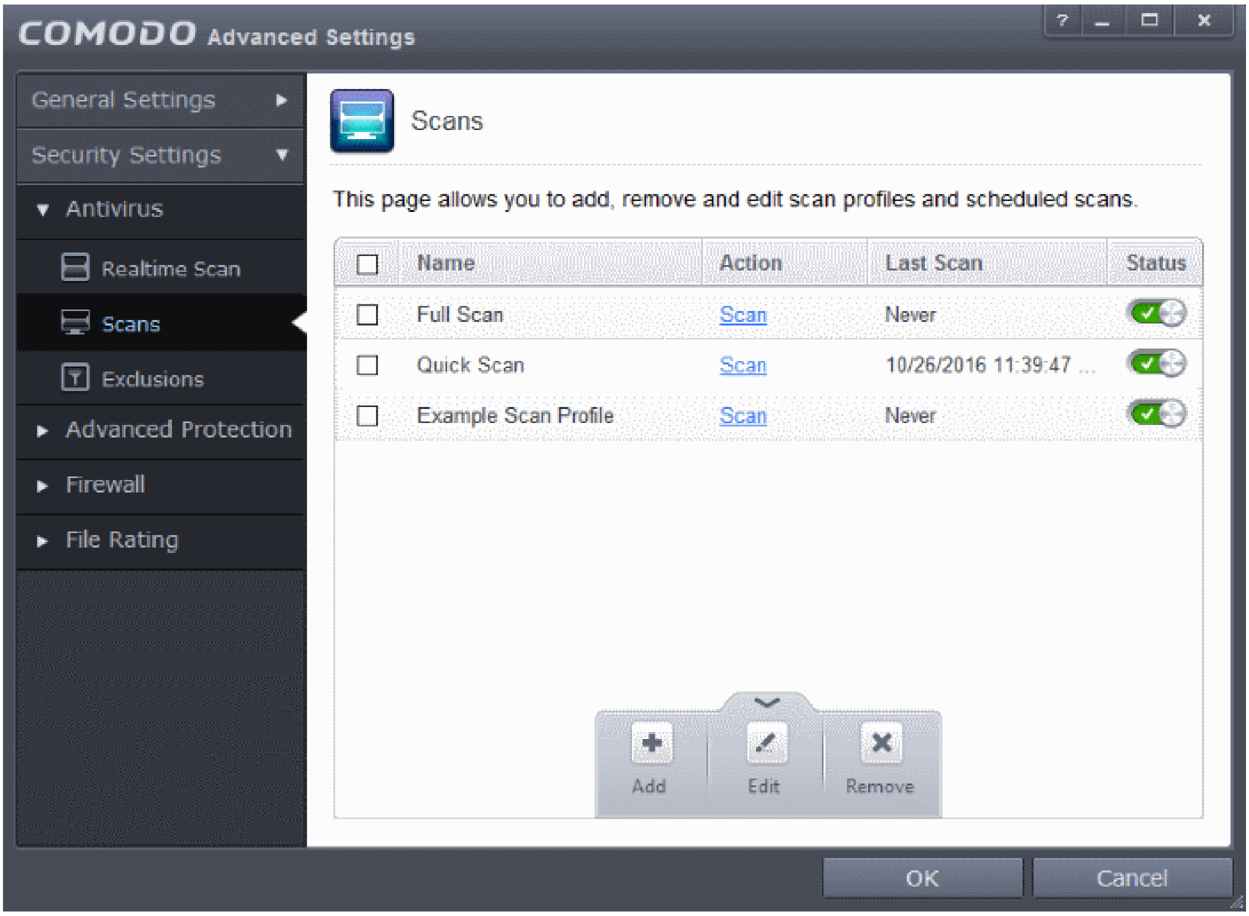
Start Time: 4:00 PM

Day(s) of Week: Sun Mon **Tue** Wed Thu **Fri** Sat

- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - Runs the scan every day at the time specified
- **Every Week** - Scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - Scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
- **Run only when computer is idle** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
- **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 the scans to run at nights.

- Click 'OK' to save the profile.

Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.



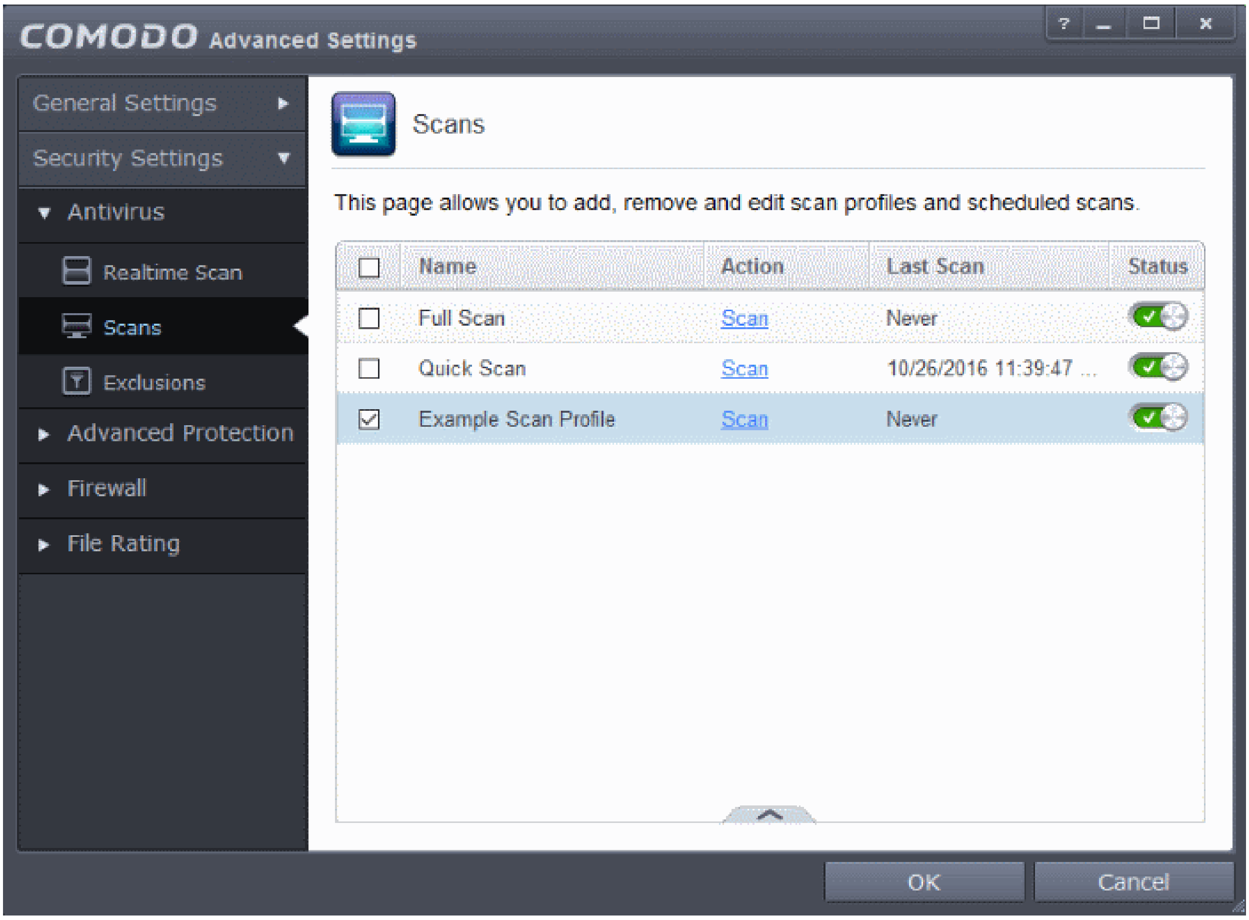
Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	10/26/2016 11:39:47 ...	✓
□	Example Scan Profile	Scan	Never	✓

To run a custom scan as per scan profile

- 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 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click Scan beside the required scan profile.

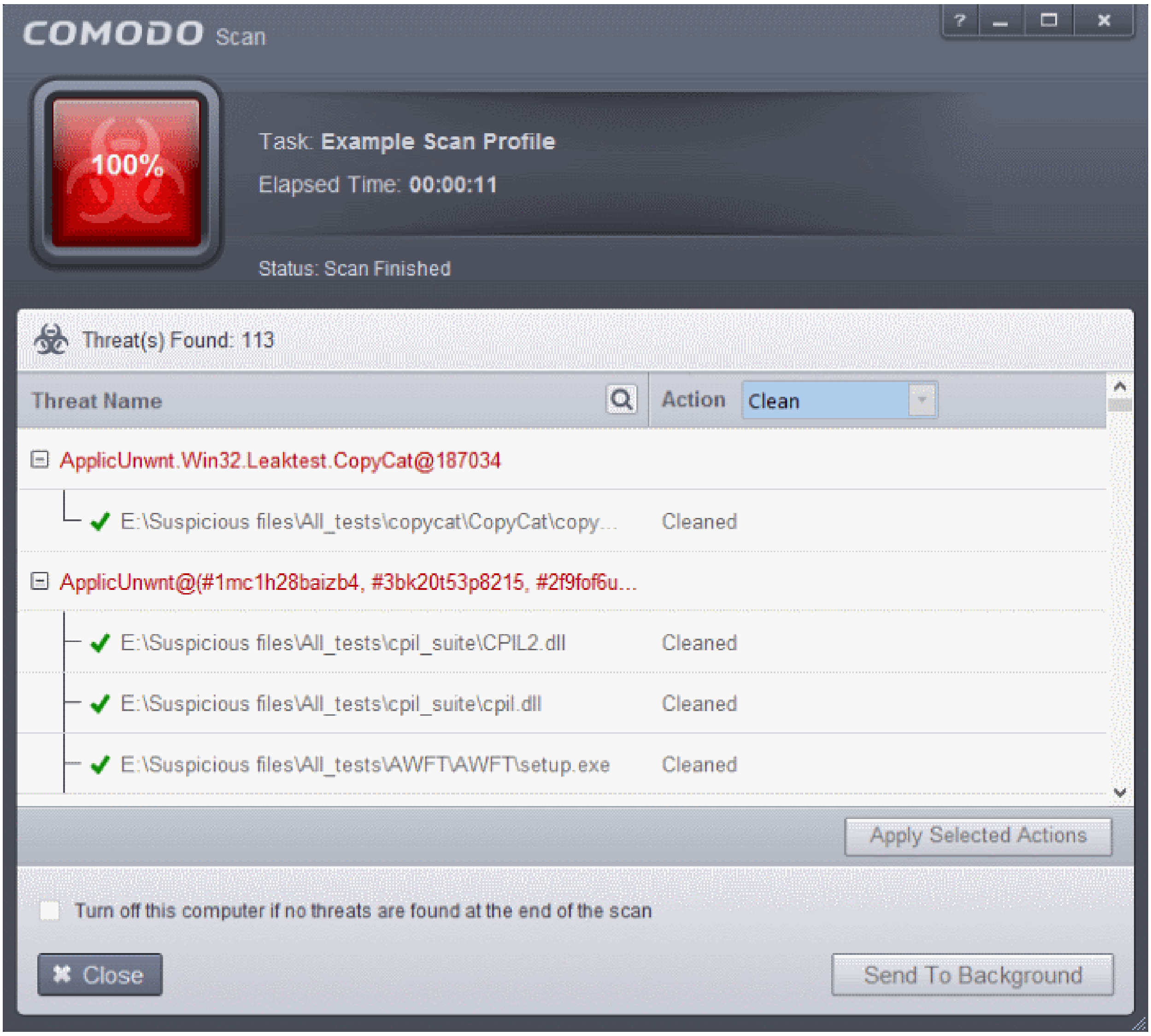


Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	10/26/2016 11:39:47 ...	✓
☑	Example Scan Profile	Scan	Never	✓

- The scan will be started and on completion the results will be displayed.



Task: **Example Scan Profile**

Elapsed Time: **00:00:11**

Status: Scan Finished

Threat(s) Found: 113

Threat Name	Action: Clean
⊟ ApplicUnwnt.Win32.Leaktest.CopyCat@187034	
✓ E:\Suspicious files\All_tests\copycat\CopyCat\copy...	Cleaned
⊟ ApplicUnwnt@(#1mc1h28baizb4, #3bk20t53p8215, #2f9fof6u...	
✓ E:\Suspicious files\All_tests\cpil_suite\CPIL2.dll	Cleaned
✓ E:\Suspicious files\All_tests\cpil_suite\cpil.dll	Cleaned
✓ E:\Suspicious files\All_tests\AWFT\AWFT\setup.exe	Cleaned

Apply Selected Actions
☐ Turn off this computer if no threats are found at the end of the scan
Close
Send To Background

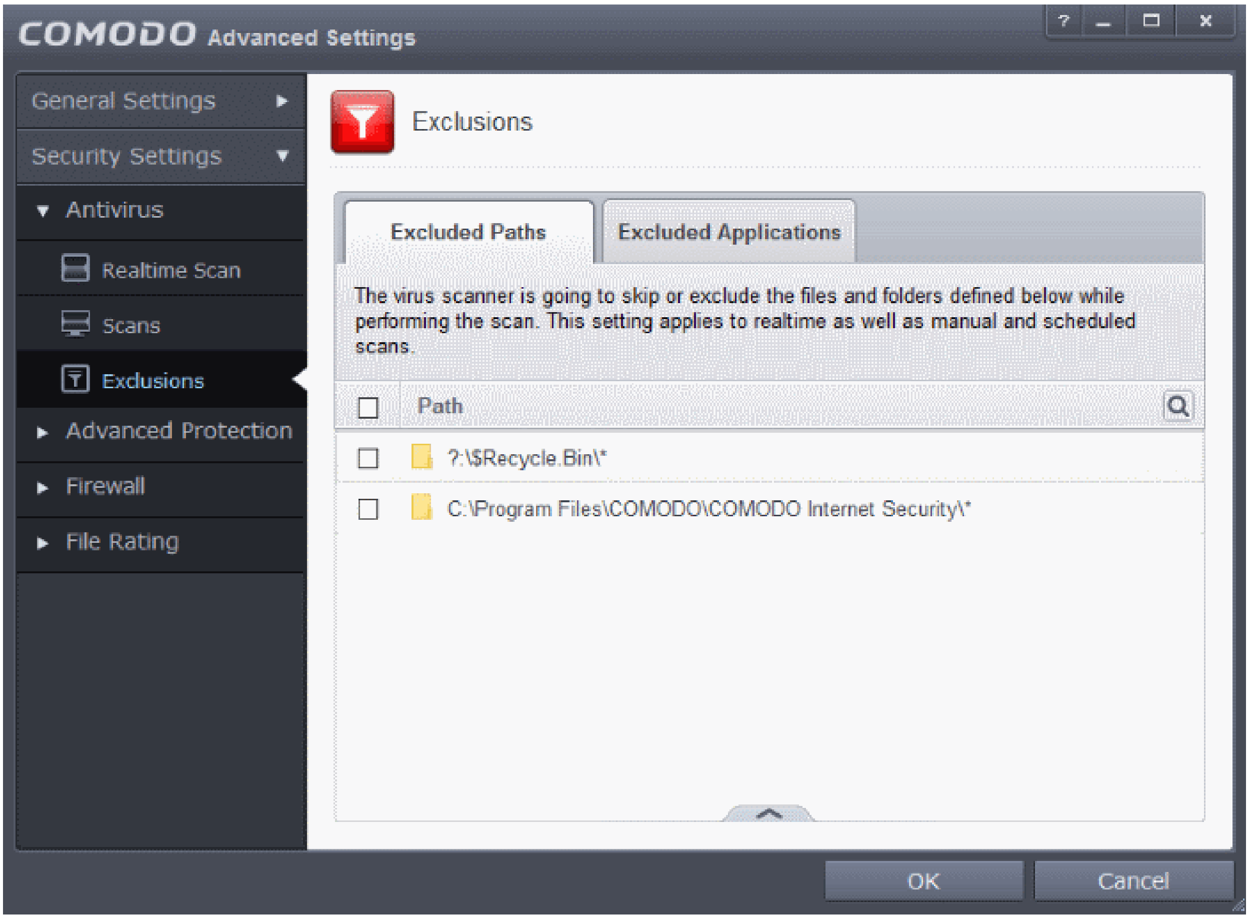
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

6.2.1.3. Exclusions

The 'Exclusions' panel displays a list of paths and files for which you have selected 'Ignore' from the Scan Results window, or have added as an exclusion from an antivirus alert.

To open the Exclusions panel

- Click Security Settings > Antivirus > 'Exclusions' tab in the 'Advanced Settings' panel.



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

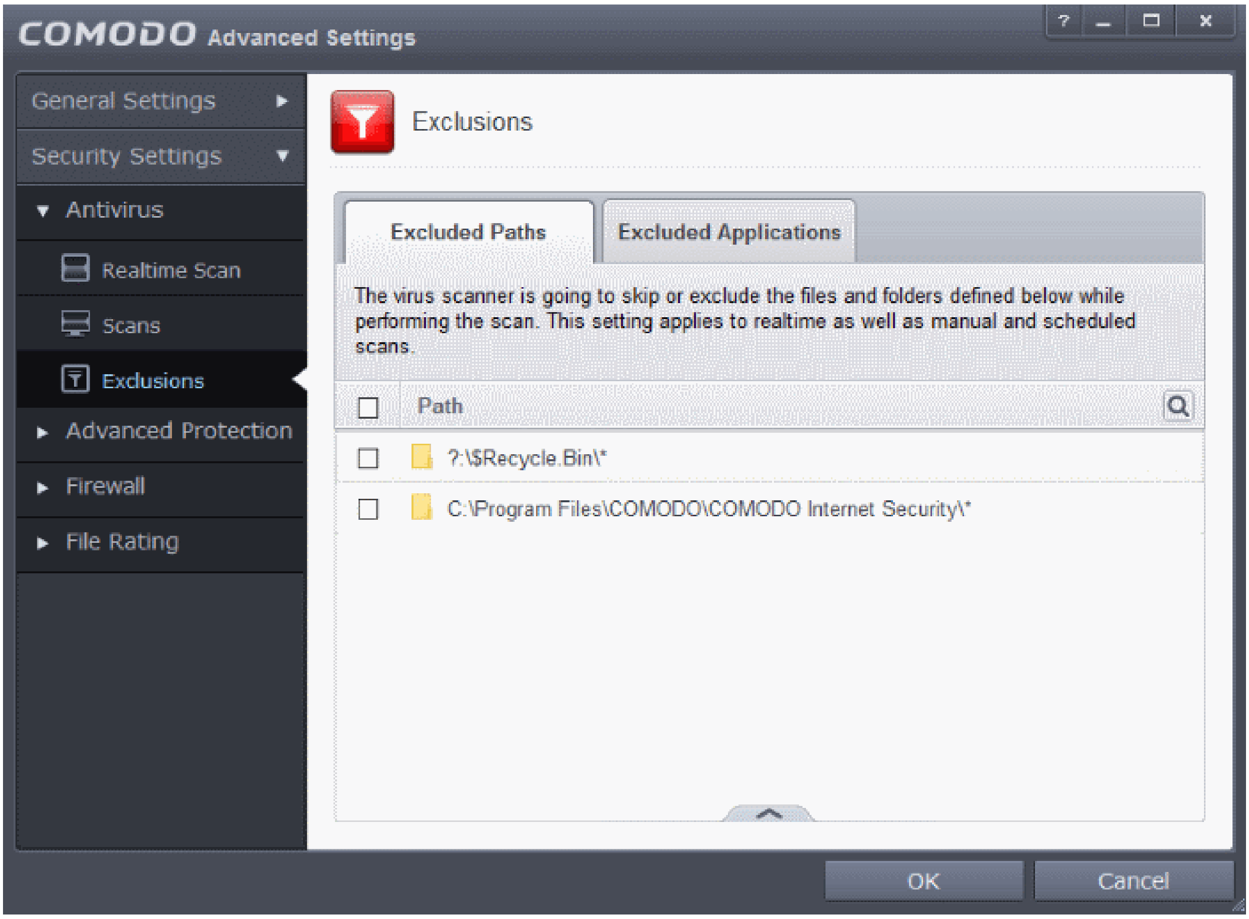
□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*

The 'Exclusions' panel has two tabs:

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

Excluding Drives/Folders/Files from all types of scans

You can exclude a drive partition, a folder, a sub-folder or a file from both the real-time and on-demand/custom scheduled antivirus scans at any time, by adding them to Excluded Paths.



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

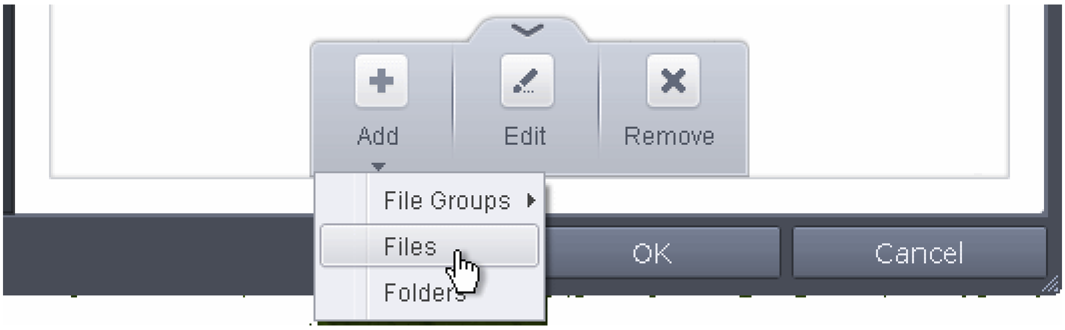
	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*

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

- Enter the path, folder name or file name to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

To add item(s) to excluded paths

- Click the handle from the bottom center and click on 'Add' from the options



You can choose to add a:

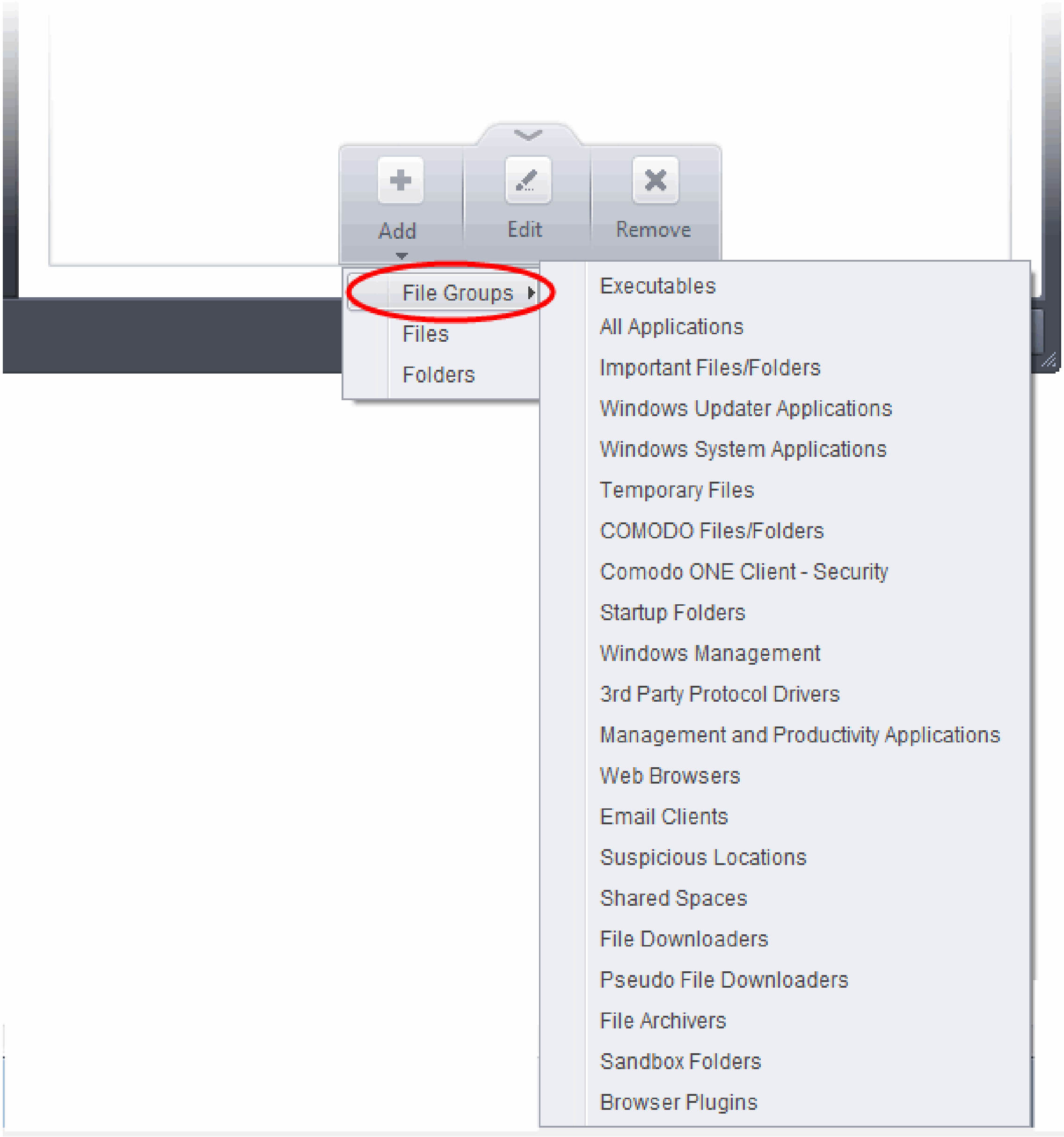
- File Group
- Drive partition/Folder

or

- an individual file

Adding a File Group

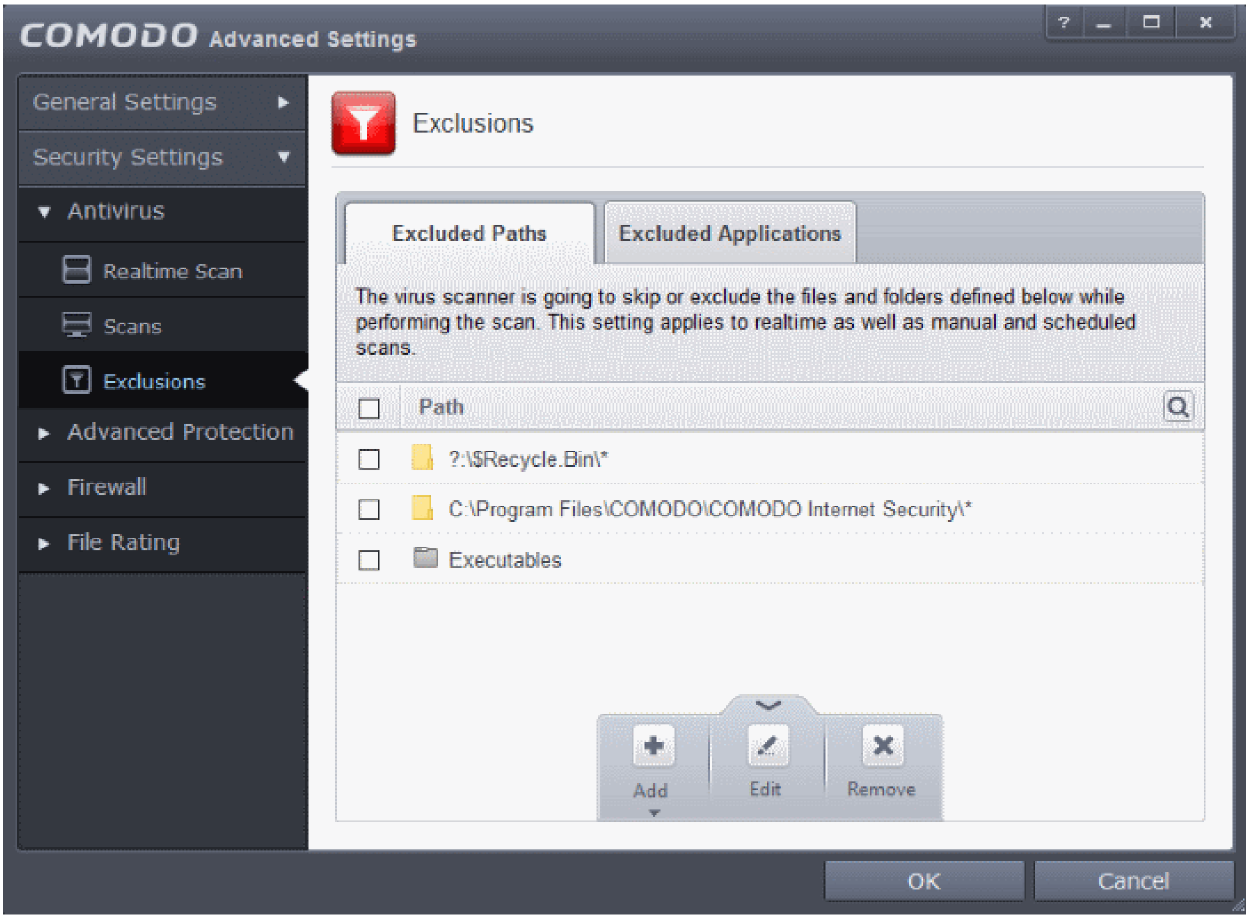
- Choosing File Groups allows you to exclude a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows 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 predefined File Groups and can be viewed in Advanced Settings > File Rating > File Groups. You can also add new file groups here which will be displayed in the predefined list.

To add a file group to Excluded Paths, click 'Add '> File Groups and select the type of File Group from the list.

The file group will be added to Excluded Paths.



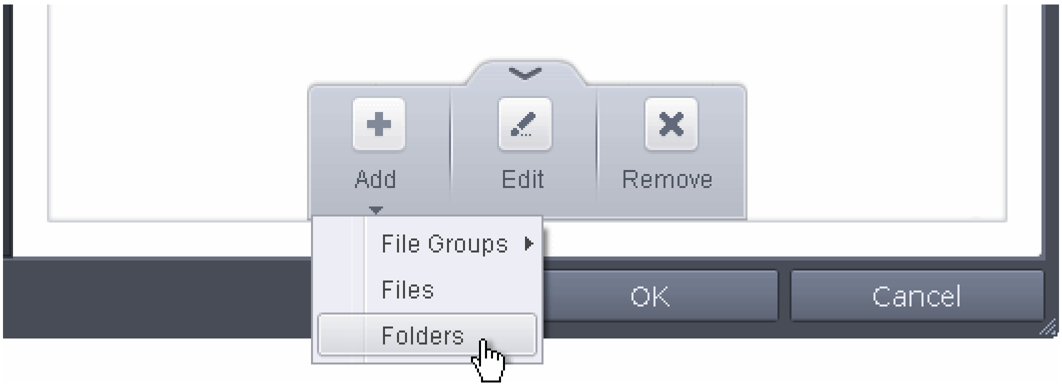
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	Executables

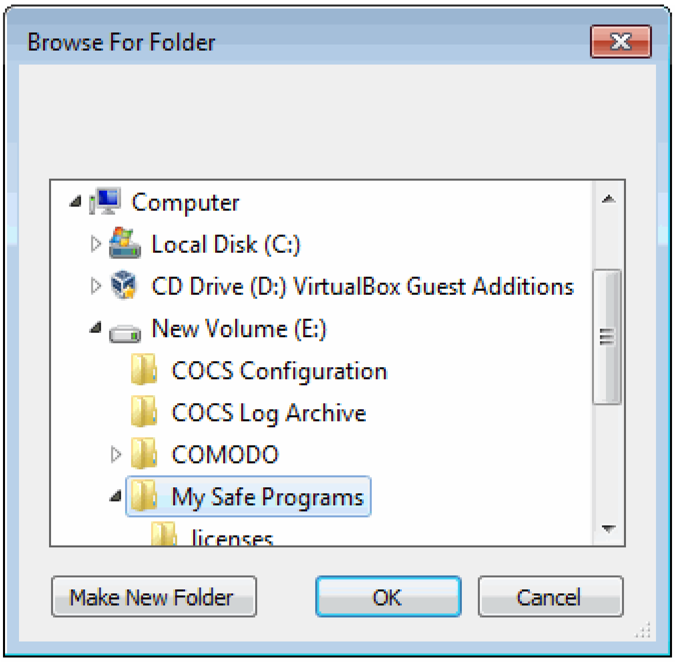
- Repeat the process to add more file groups. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding a Drive Partition/Folder

- To add a folder, choose 'Folders' from the 'Add' drop-down.

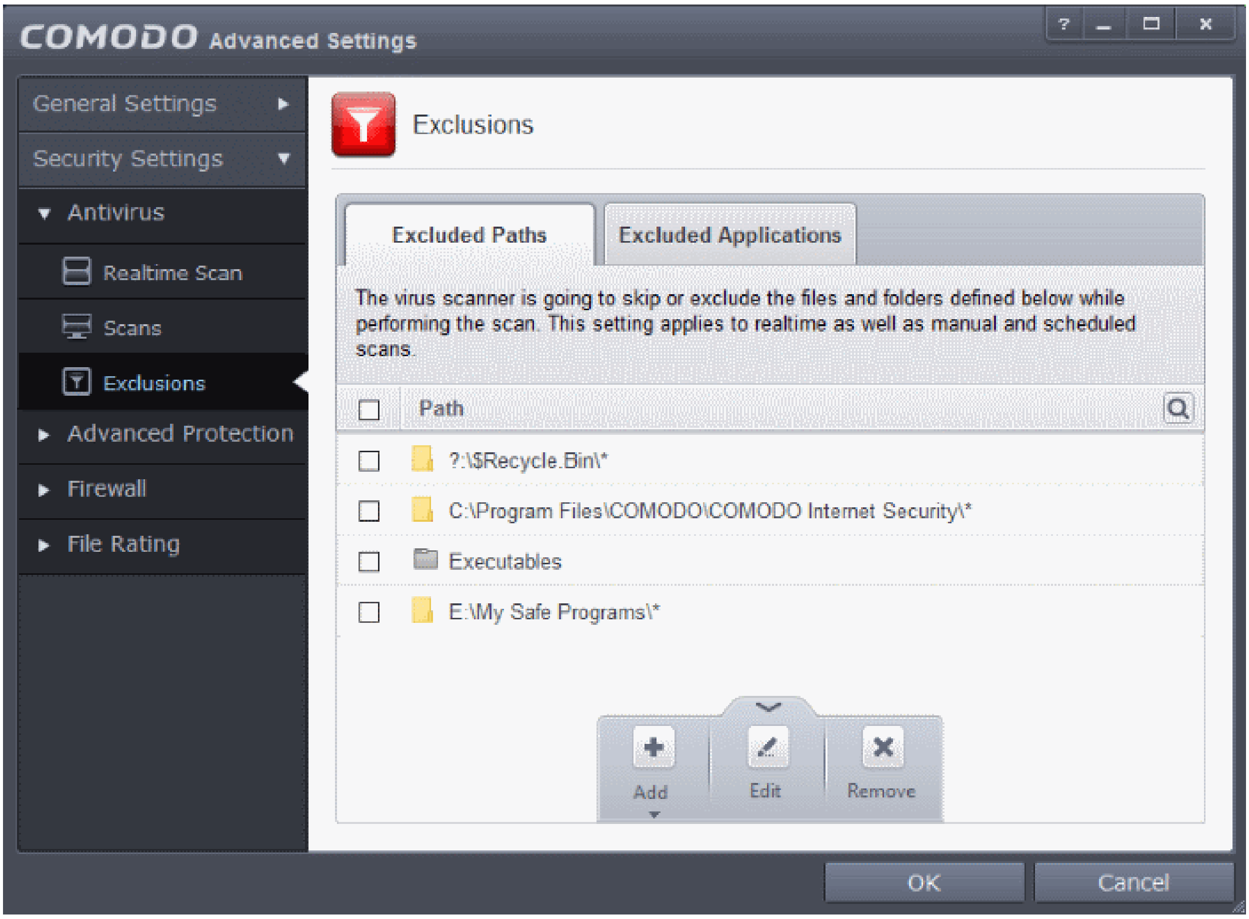


The 'Browse for Folder' dialog will appear.



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

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



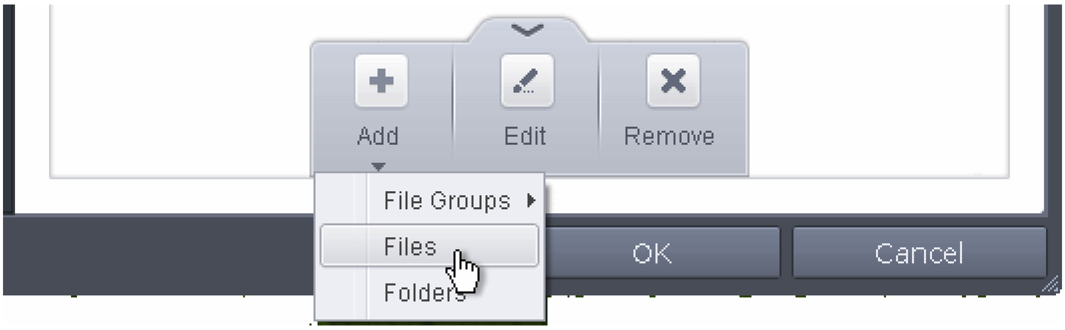
The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	Executables
□	E:\My Safe Programs*

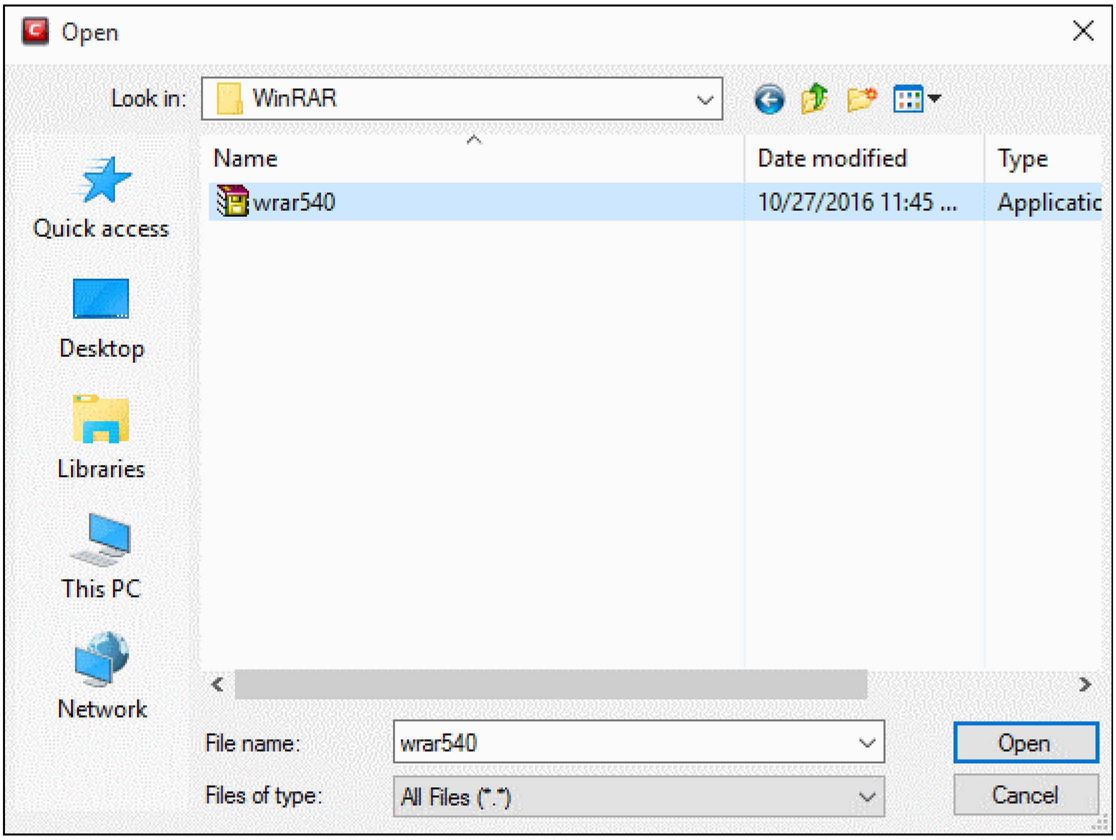
- Repeat the process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding an individual File

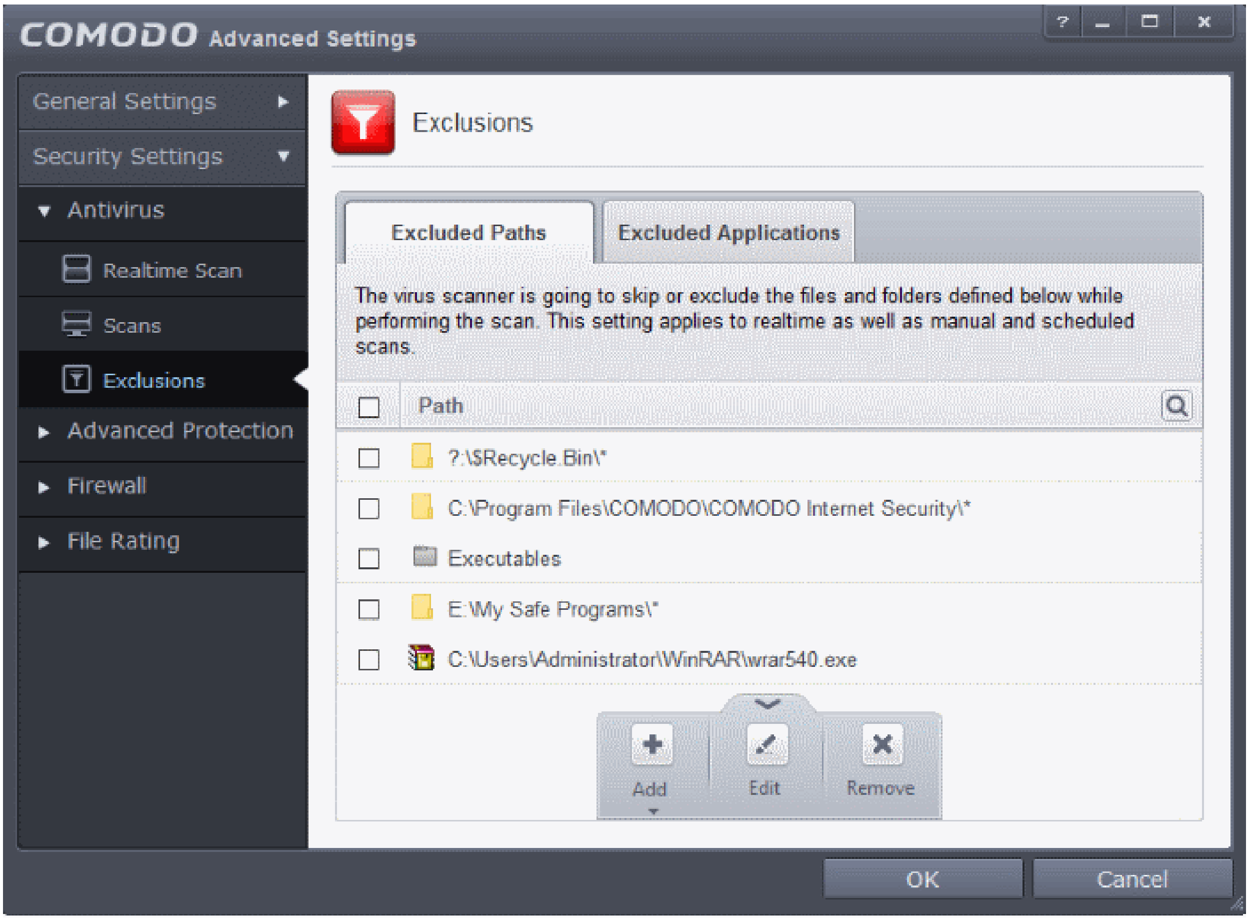
- Choose 'Files' from the 'Add' drop-down.



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



The file will be added to 'Excluded Paths'.



The virus scanner is going to skip or exclude the files and folders defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

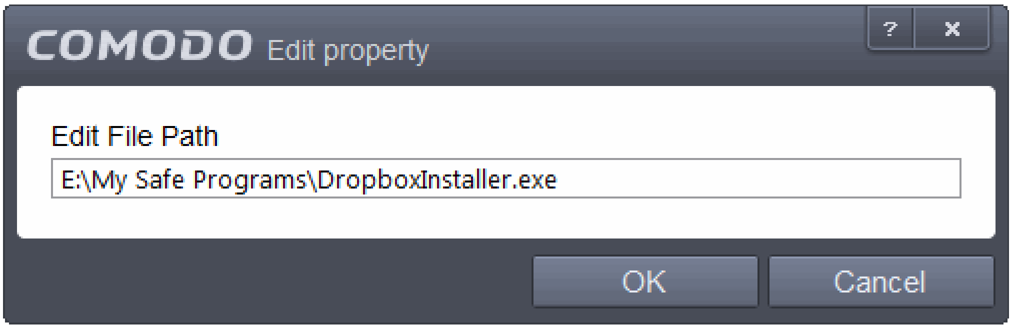
□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	Executables
□	E:\My Safe Programs*
□	C:\Users\Administrator\WinRAR\wrar540.exe

- Repeat the process to add more paths. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Note: Choosing the option 'Add to Exclusions' action from the Scan Results window, the selected items are automatically added to Excluded Paths.

To edit the path of an added item

- Select the item, click the handle from the bottom and select 'Edit'.



Edit File Path

E:\My Safe Programs\DropboxInstaller.exe

- Make the required changes for the file path in the 'Edit Property' dialog.

To remove an item from the Excluded Paths

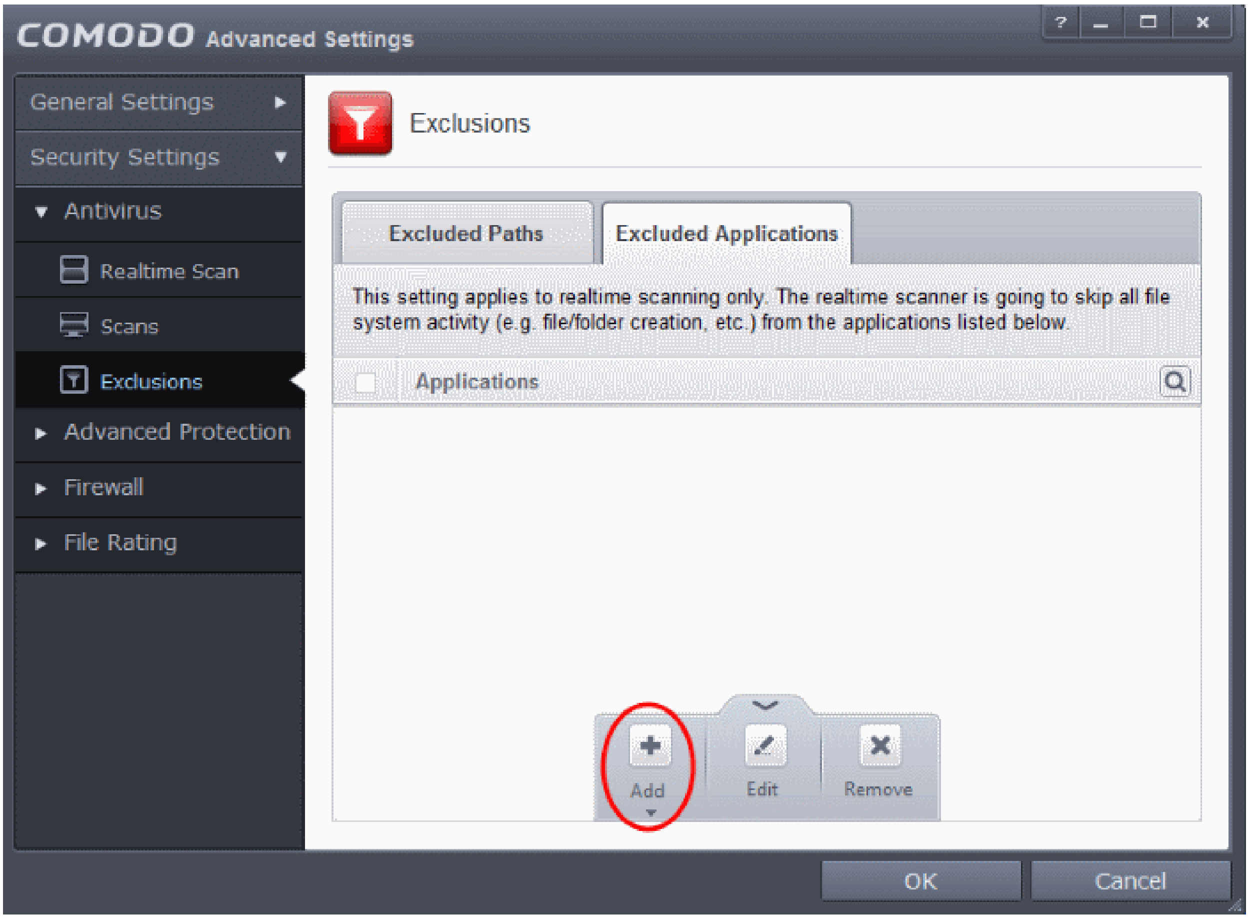
- Select the item, click the handle from the bottom and select 'Remove'.
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

You can manually add programs, applications of files to Excluded Applications list for excluding them from real-time scans. Also you can remove the items from Excluded Applications that were added by mistake.

To add an item to Excluded Applications

- Click the handle from the bottom and click on 'Add' from the options



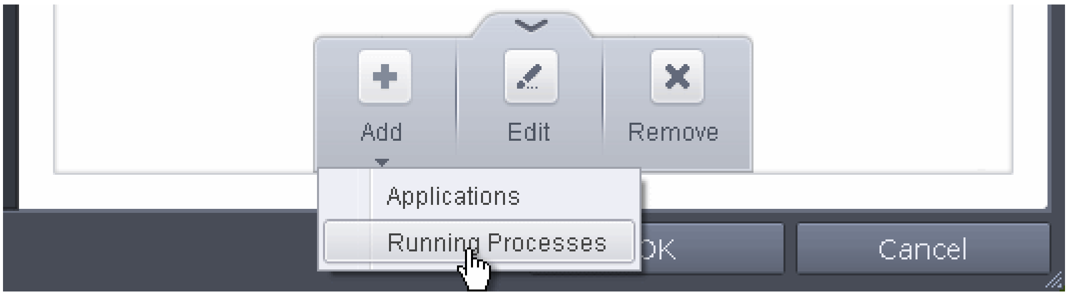
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

You can choose to add an application 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 the files which you want to exclude from a virus scan.

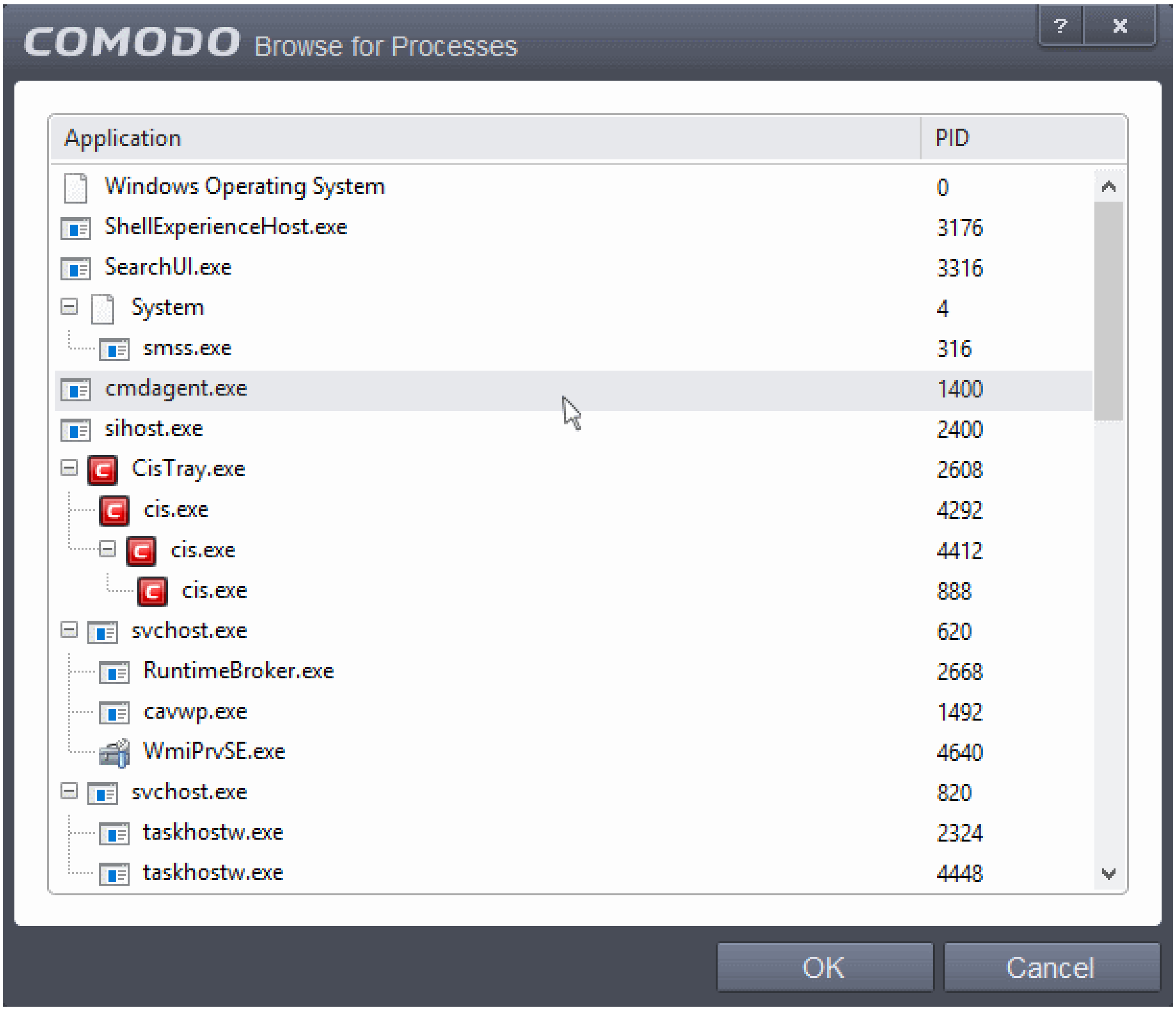
Adding an application from a running processes

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



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

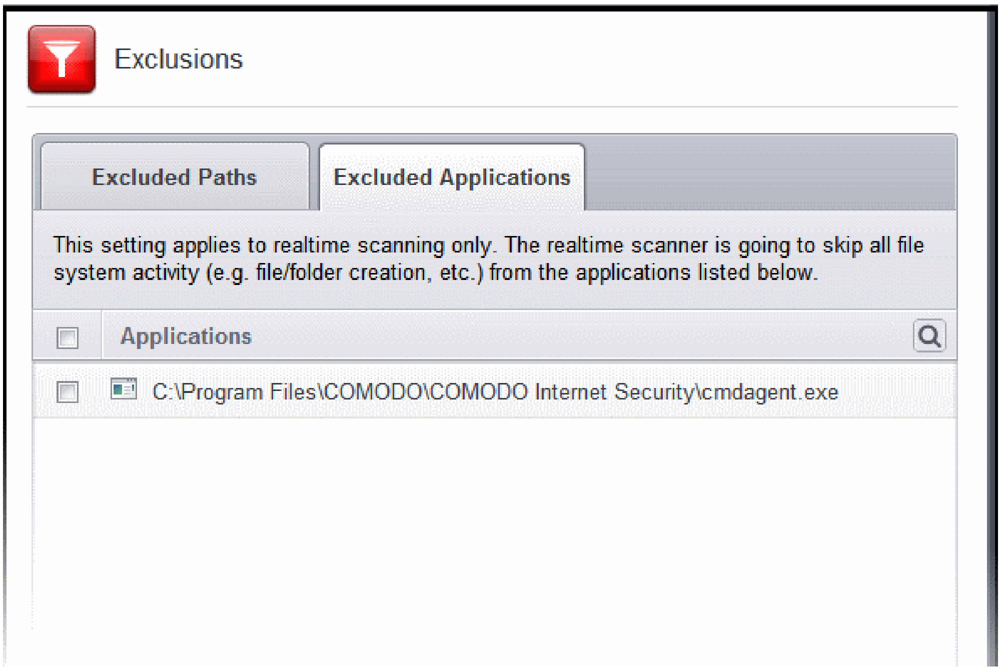
- Select the process, whose target application is to be added to excluded applications and click OK from the Browse for Process dialog.



COMODO Browse for Processes

Application	PID
Windows Operating System	0
ShellExperienceHost.exe	3176
SearchUI.exe	3316
System	4
smss.exe	316
cmdagent.exe	1400
sihost.exe	2400
CisTray.exe	2608
cis.exe	4292
cis.exe	4412
cis.exe	888
svchost.exe	620
RuntimeBroker.exe	2668
cavwp.exe	1492
WmiPrvSE.exe	4640
svchost.exe	820
taskhostw.exe	2324
taskhostw.exe	4448

The application will be added to Excluded Applications.



Exclusions

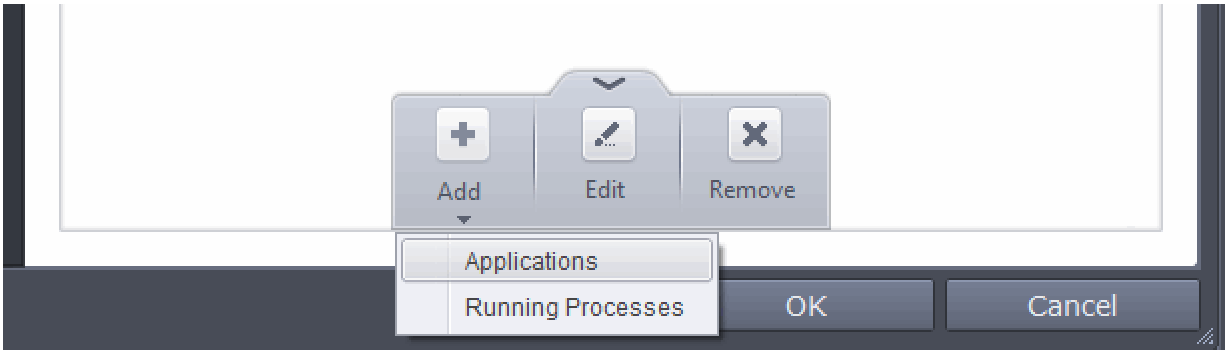
Excluded Paths | Excluded Applications

This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

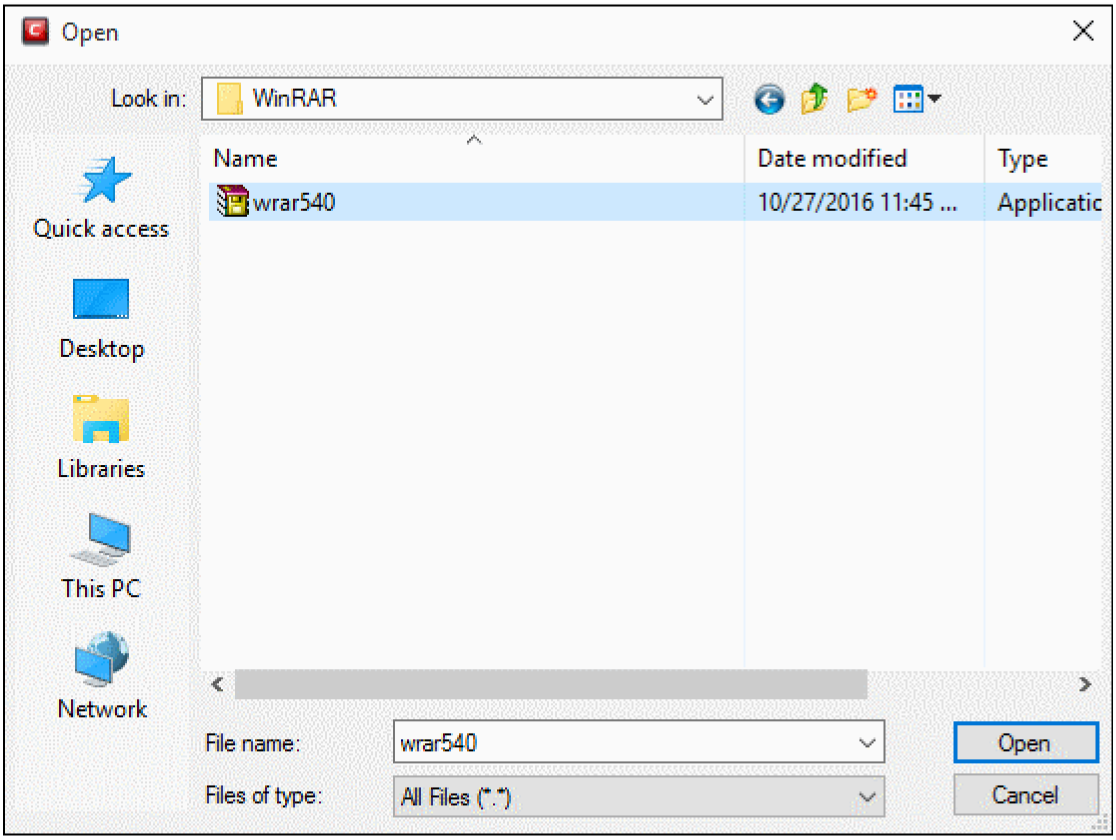
□	Applications
□	C:\Program Files\COMODO\COMODO Internet Security\cmdagent.exe

Browsing to the Application

- Choose 'Applications' from the 'Add' drop-down



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

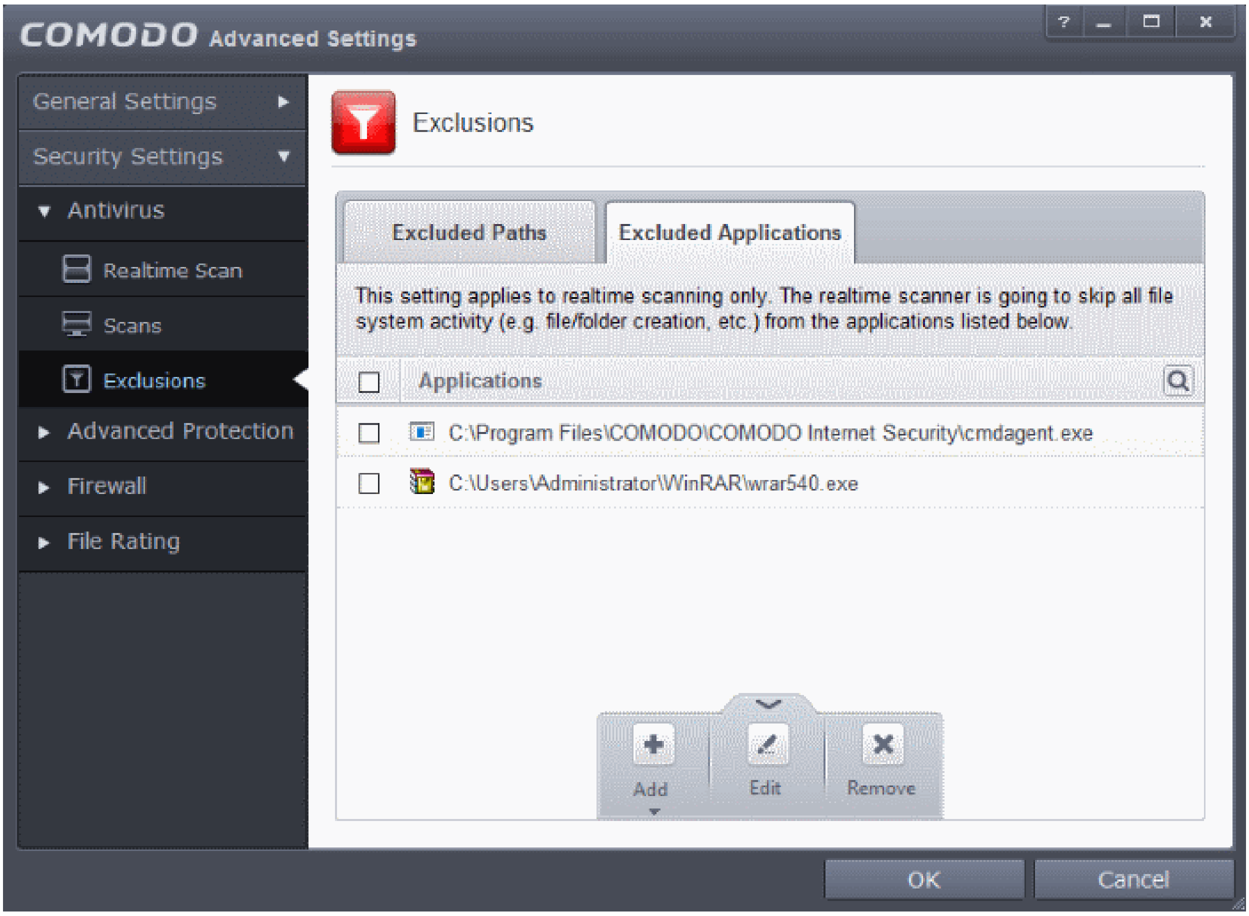


Name	Date modified	Type
wrar540	10/27/2016 11:45 ...	Applicatic

File name: wrar540

Files of type: All Files (*.*)

The file will be added to 'Excluded Applications'.



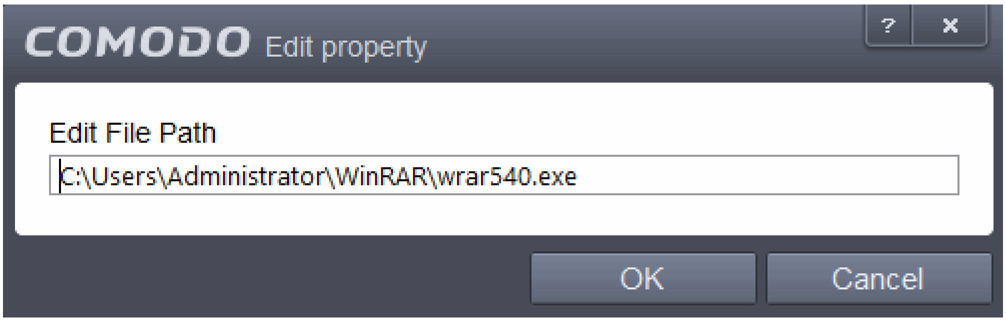
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

□	Applications
□	C:\Program Files\COMODO\COMODO Internet Security\cmdagent.exe
□	C:\Users\Administrator\WinRAR\wrar540.exe

- Repeat the process to add more items. The items will be skipped from future real-time scans.

To edit the path of the application added to Excluded Application

- Select the application, click the handle from the bottom and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



Edit File Path

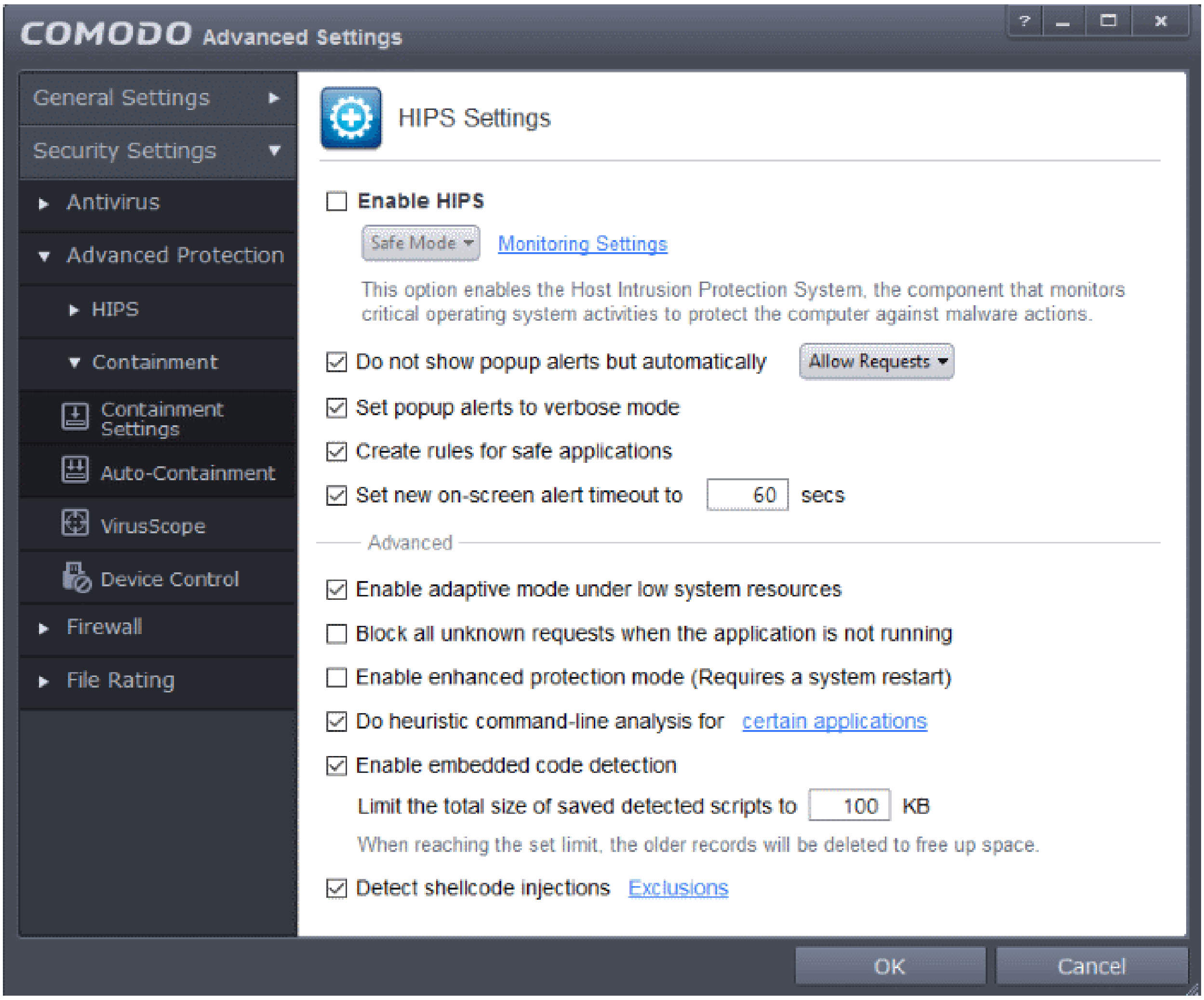
C:\Users\Administrator\WinRAR\wrar540.exe

To remove an item from the Excluded Applications

- Select the item, click the handle from the bottom and select 'Remove'.
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

6.2.2. Advanced Protection Settings

Advanced Protection is a collective term that covers the Host Intrusion Prevention (HIPS), Containment, VirusScope and Device Control components of Comodo Client Security. Together, these technologies ensure all applications, processes and services on your PC behave in a secure manner - and are prevented from taking actions that could damage your computer or your data.



HIPS Settings

☐ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do not show popup alerts but automatically Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

Advanced

☑ Enable adaptive mode under low system resources

☐ Block all unknown requests when the application is not running

☐ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Enable embedded code detection

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Detect shellcode injections Exclusions

The Advanced Protection settings area allows you to configure the following:

- HIPS
  - HIPS Behavior Settings
  - Active HIPS Rules
  - Predefined HIPS Rule Sets
  - Protected Objects
  - HIPS Groups
- Comodo Containment
  - Containment Settings
  - Rules for Auto-Containment
- Viruscope
- Device Control Settings

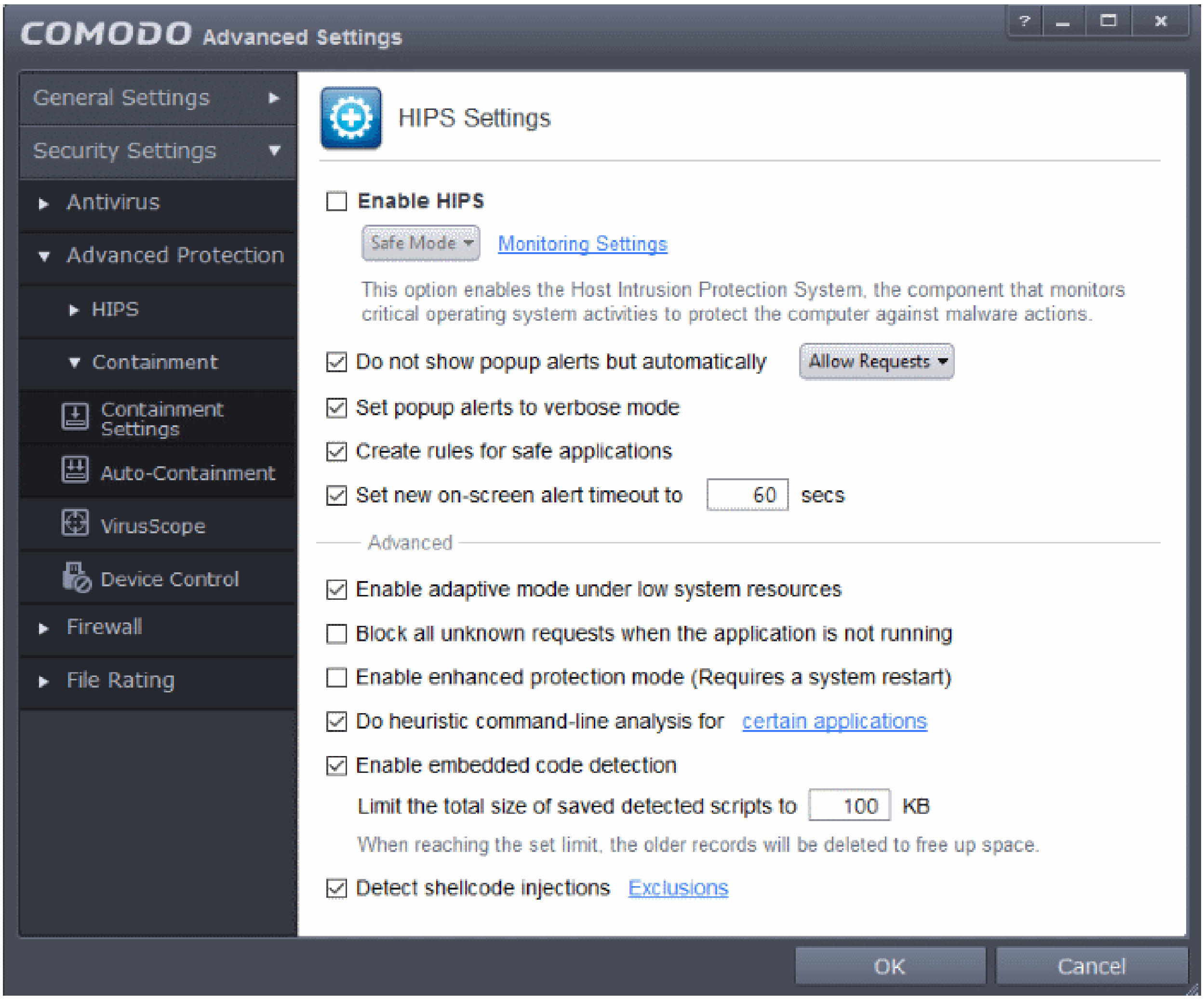
6.2.2.1. HIPS Behavior Settings

HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo Client Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized 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.

Note for beginners: This page often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your computer to perform a task or function. Every program, application and device you run on your computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. (e.g., when you start Microsoft Word, the executable file 'winword.exe' instructs your computer to start and run the Word application). Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data; steal your identity; corrupt system files; give control of your PC to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms.

- The HIPS Settings panel allows you to enable/disable HIPS, set its security level and configure its general behavior.
- The HIPS Settings panel can be accessed by clicking 'Advanced Settings' > 'Security Settings' > 'Advanced Protection' > 'HIPS' > 'HIPS Settings'



HIPS Settings

□ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do not show popup alerts but automatically Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

Advanced

☑ Enable adaptive mode under low system resources

□ Block all unknown requests when the application is not running

□ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Enable embedded code detection

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

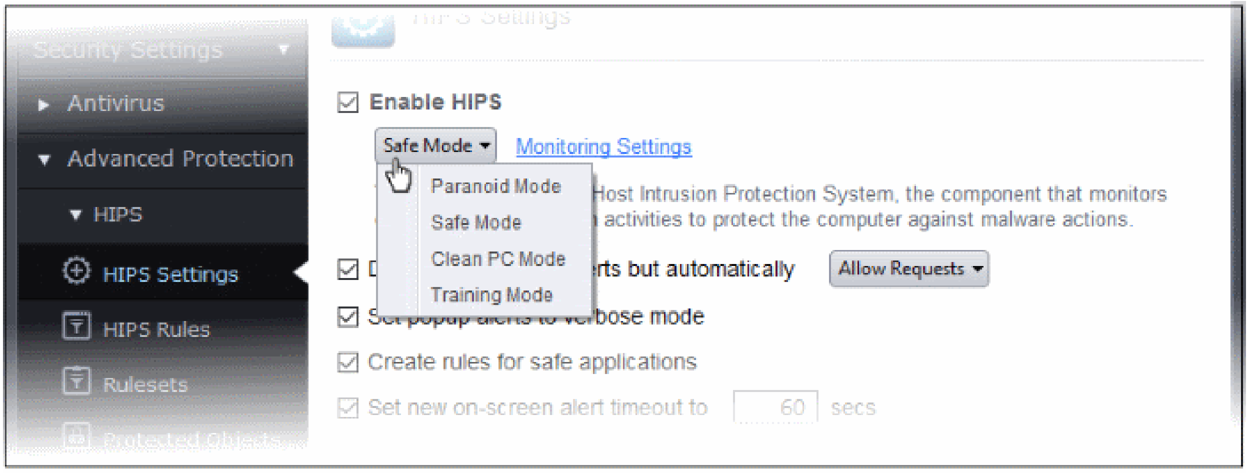
☑ Detect shellcode injections Exclusions

- **Enable HIPS -** Allows you to enable/disable the HIPS protection. (*Default=Disabled*)

If enabled, you can choose the security level and configure the monitoring settings for the HIPS component.

Configuring Security Level of HIPS

The security level can be chosen from the drop-down that becomes active only on enabling HIPS:



☑ Enable HIPS

Safe Mode ▾ Monitoring Settings

Host Intrusion Protection System, the component that monitors activities to protect the computer against malware actions.

☑ D...rts but automatically Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

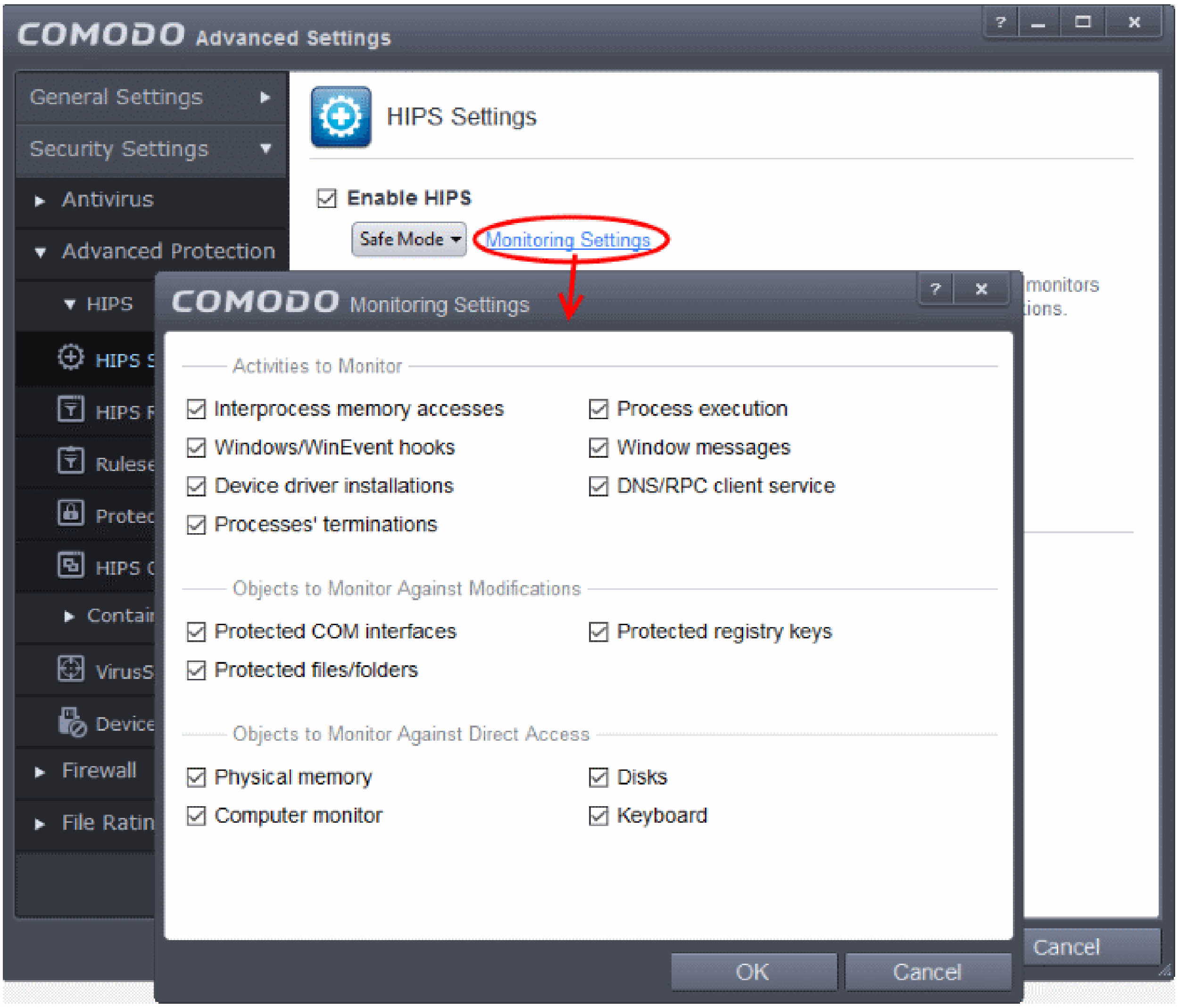
The choices available are:

- **Paranoid Mode**: This is the highest security level setting and means that 'Advanced Protection' 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, the Comodo Client Security does 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, 'Advanced Protection' automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules 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 safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs 'Advanced Protection' 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 as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Clean PC Mode:** From the time you set the slider to 'Clean PC Mode', 'Advanced Protection' learns the activities of the applications currently installed on the computer while all new executables introduced to the system are monitored and controlled. This patent-pending mode of operation is the recommended option on a new computer or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files with 'Unrecognized' rating in the '**File List**' are excluded from being considered as clean and are monitored and controlled.
- **Training Mode**: 'Advanced Protection' monitors and learn the activity of any and all executables and create 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 the Monitoring Settings

The activities, entities and objects that should monitored by HIPS can be configured by clicking the Monitoring Settings link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a ***global*** basis - effectively creating a universal '**Allow**' rule for that activity. This 'Allow' setting ***over-rules*** any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the '**Access Rights**' and '**Protection Settings**' interface.



☑ Enable HIPS

Activities to Monitor

☑ Interprocess memory accesses
☑ Windows/WinEvent hooks
☑ Device driver installations
☑ Processes' terminations
☑ Process execution
☑ Window messages
☑ DNS/RPC client service

Objects to Monitor Against Modifications

☑ Protected COM interfaces
☑ Protected files/folders
☑ Protected registry keys

Objects to Monitor Against Direct Access

☑ Physical memory
☑ Computer monitor
☑ Disks
☑ Keyboard

Activities To Monitor:

- **Interprocess Memory Access -** Malware programs use memory space modification to inject malicious code for numerous types of attacks, including recording your keyboard strokes; modifying the behavior of the invaded application; stealing confidential data by sending confidential information from one process to another process etc. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of the invaded process, or '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 (messages, mouse actions, keystrokes) *before* they reach an application. The function can act on 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; take over control of your mouse and keyboard to remotely administer 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 a hardware device on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable

damage to your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application ***(Default = Enabled)***

- **Processes' Terminations -** A process is a running instance of a program. (for example, the Comodo Client Security process is called 'CCS.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, 'Advanced Protection' monitors and alerts you to all attempts by an untrusted application to close down another application ***(Default = Enabled)***.
- **Process Execution** - Typical malware like rootkits, keylogger etc. would often invoke by itself and runs its process mostly at the background. These processes, invisible at the foreground will act as agents for infecting your computer and to steal your confidential and sensitive information like your credit card details and passwords and pass to hackers. With this setting enabled, the 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 an malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' pc's which are sending out these requests without the 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 translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever you type a domain name, your Internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to your computer, 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 Protected COM 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 a 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 an 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

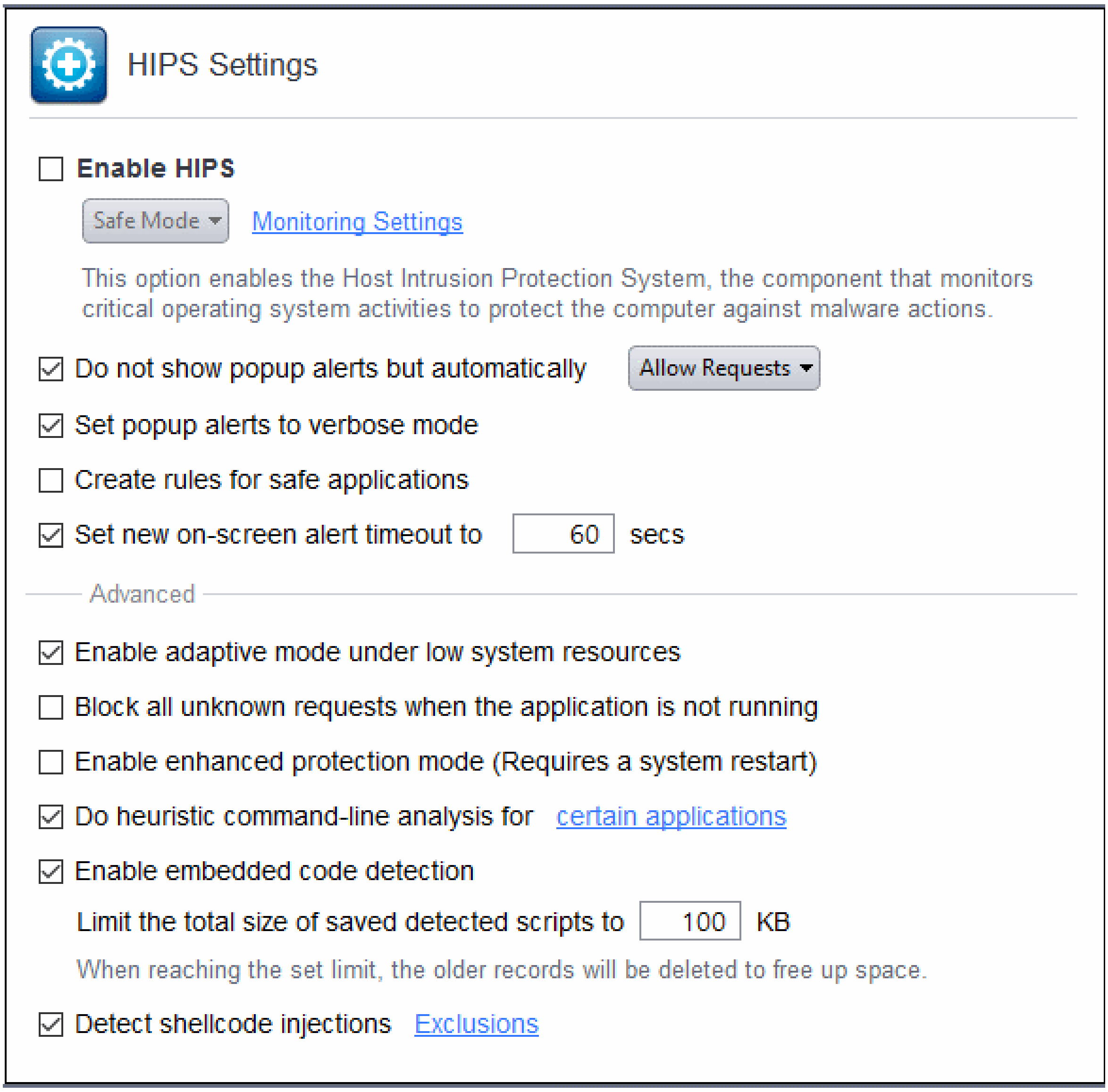
computer monitor. Although legitimate applications sometimes require this access, there is also an emerging category of spyware programs that use such access to monitor users' activities. (for example, to take screen shots of your current desktop; to record your browsing activities etc) ***(Default = 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 a malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness. (***Default = Enabled***)

  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'.



HIPS Settings

□ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do not show popup alerts but automatically Allow Requests ▾

☑ Set popup alerts to verbose mode

□ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

Advanced

☑ Enable adaptive mode under low system resources

□ Block all unknown requests when the application is not running

□ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Enable embedded code detection

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Detect shellcode injections Exclusions

- **Set popup alerts to verbose mode** - Enabling this option instructs CCS to display HIPS Alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests

(Default = Enabled).

- **Create rules for safe applications -** Automatically creates rules for safe applications in HIPS Ruleset *(Default = Enabled).*

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 saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, 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 the 'Allow' rules. These rules are listed in the HIPS Rules interface. The Advanced users can edit / modify the rules as they wish.

Background Note: CCS automatically adds an allow rule for 'safe' files to the rules interface. This allows advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also takes a toll on system resources. In this version, '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.

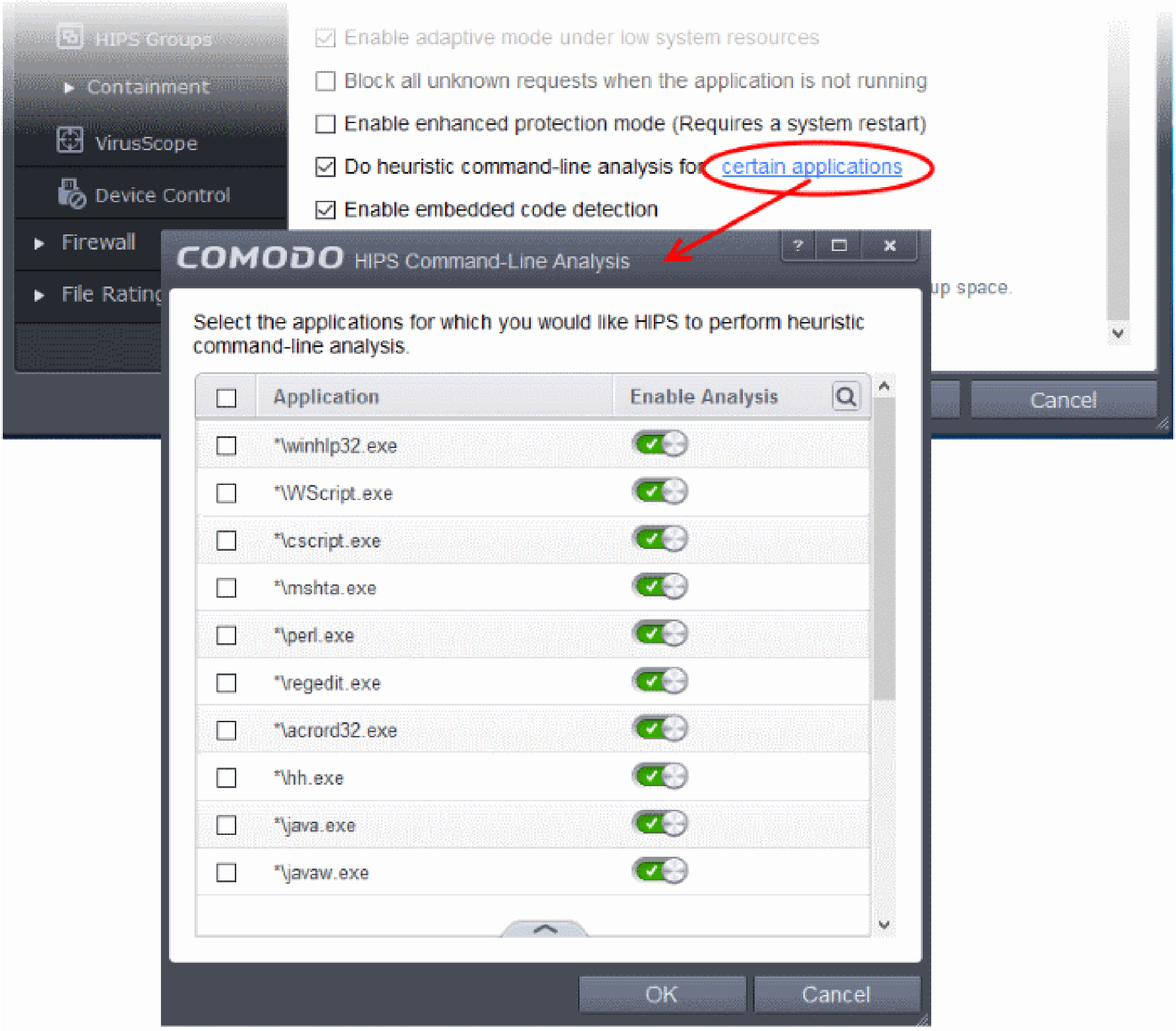
- **Set new on-screen alert timeout to:** Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 60 seconds. You may adjust this setting to your own preference.

Advanced HIPS Settings

- **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, the cost of enabling this option may be reduced performance in even lightly loaded systems. ***(Default = Enabled)***
- **Block all unknown requests when 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)***
- **Enable enhanced protection mode -** On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures. Because of limitations in Windows 7/8 x64 systems, 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. CCS requires a system restart for enabling enhanced protection mode. ***(Default = Disabled)***
- **Do heuristic command-line analysis for certain applications –** If enabled, CCS will perform heuristic analysis on programs that are capable of executing code. Code that is executed includes visual basic scripts and java applications. Example programs that are affected by this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscipt.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, 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. ***(Default = Enabled)***
- If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the Internet'.

Background note: 'Heuristics' describes the method of analyzing a file to ascertain whether it contains codes typical of a virus. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. This helps to identify previously unknown (new) viruses.

Click the 'certain applications' link to view the list of programs that are included by default:



☑ Enable adaptive mode under low system resources

☐ Block all unknown requests when the application is not running

☐ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Enable embedded code detection

COMODO HIPS Command-Line Analysis

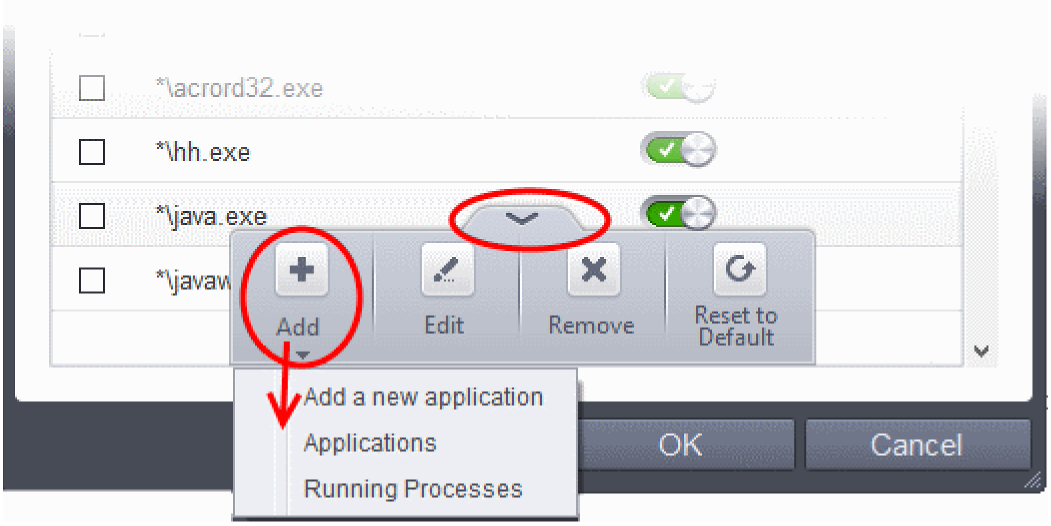
Select the applications for which you would like HIPS to perform heuristic command-line analysis.

☐	Application	Enable Analysis
☐	*\winhlp32.exe	✓
☐	*\WScript.exe	✓
☐	*\cscript.exe	✓
☐	*\mshta.exe	✓
☐	*\perl.exe	✓
☐	*\regedit.exe	✓
☐	*\acrord32.exe	✓
☐	*\hh.exe	✓
☐	*\java.exe	✓
☐	*\javaw.exe	✓

- Application - List of applications which will be analyzed, including defined custom applications.
- Enable Analysis – Enable\disable command-line analysis for a particular application(s)

To manually add a new application to the list for analysis

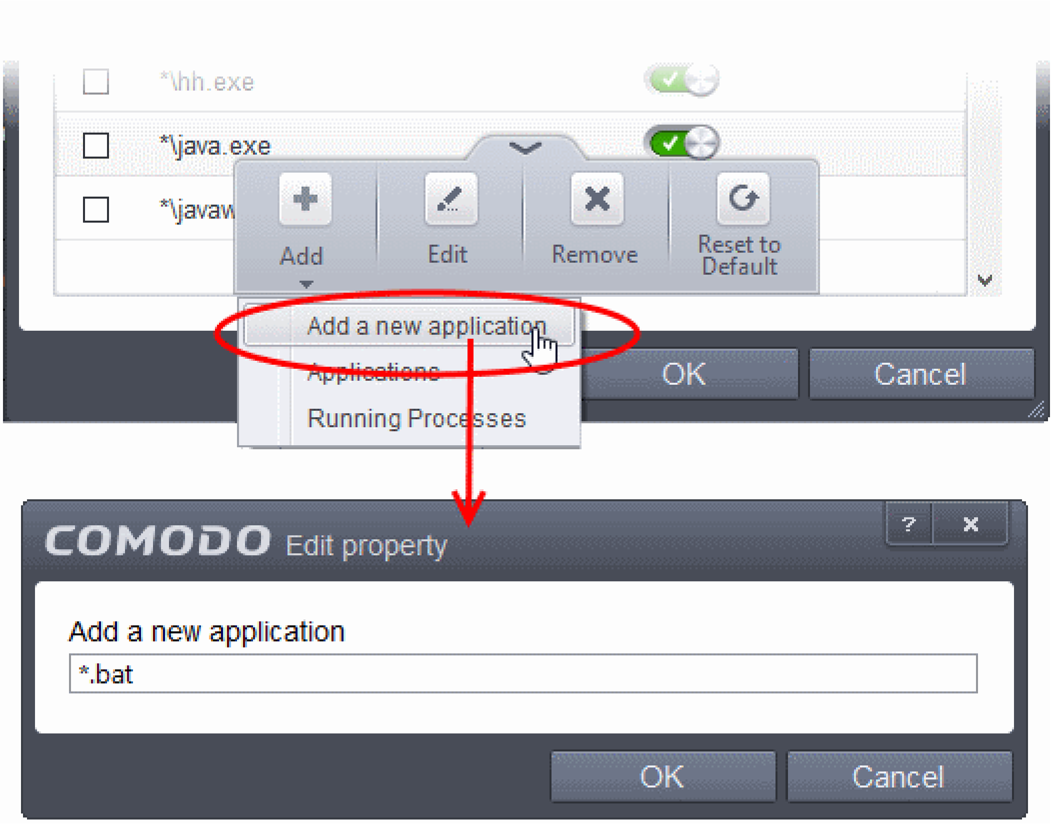
- Click the handle at the bottom



- You can add an application using any of the following methods:
- Add a new application
- Add a current application
- Add application from the currently running processes

Adding a new application

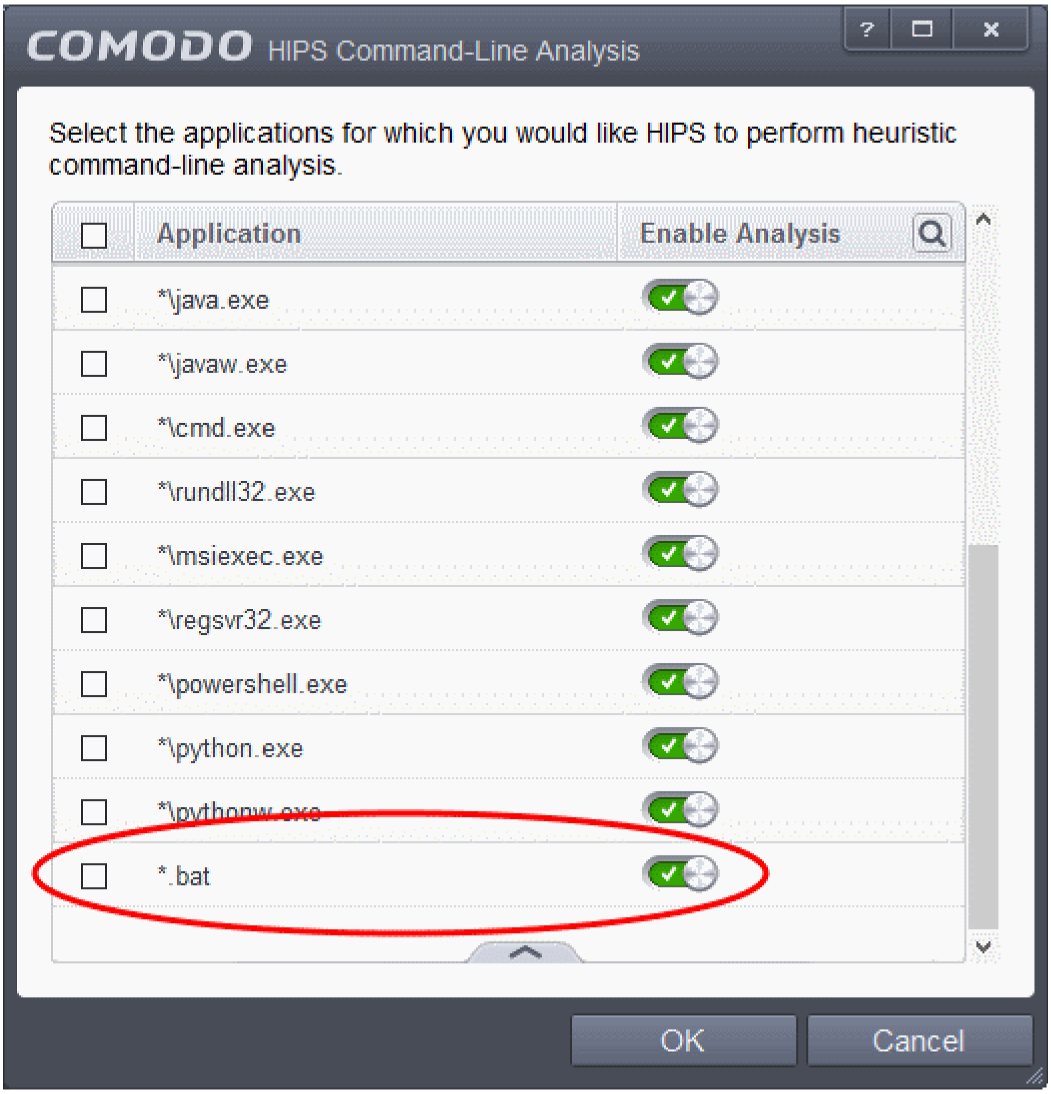
- Click the 'Add' button at the bottom of the list then select 'Add new application'
- Type the name of the application or extension in the 'Edit Property'
- Click 'OK' to apply your changes



Add a new application

*.bat

The application will be added and displayed in the list:



Select the applications for which you would like HIPS to perform heuristic command-line analysis.

□	Application	Enable Analysis
□	*\java.exe	✓
□	*\javaw.exe	✓
□	*\cmd.exe	✓
□	*\rundll32.exe	✓
□	*\msiexec.exe	✓
□	*\regsvr32.exe	✓
□	*\powershell.exe	✓
□	*\python.exe	✓
□	*\pythonw.exe	✓
□	*.bat	✓

Add a current application

- Click the 'Add' button at the bottom of the list then select 'Applications'
- 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

- Click the 'Add' button at the bottom of the list then select 'Running Applications'
- A list of processes currently running on your computer will be displayed
- Select the process whose parent application you wish to add for analysis
- Click 'OK' to confirm your choice
- The application will be added to the list
  - Use the slider beside an application to enable or disable analysis.
  - Click the 'Edit' button to update the details of an application.
  - To remove an application, select it from the list, click the handle at the bottom then 'Remove'
  - Click the handle at the bottom then 'Reset to Default' to revert the list to the default, predefined,

applications.

- Click 'OK' at the bottom to apply your changes.

- **Enable embedded code detection** – If enabled, CCS will also scan for embedded codes (scripts) to provide 'Fileless Malware' protection.

  The total size of saved scripts can be limited. Enter the total size to be saved in the 'Limit the total size of saved detected scripts to' field. When the limit is reached, the older records will be deleted to free up space.

- **Detect shellcode injections (i.e. Buffer overflow protection)** - Enabling this setting turns-on the Buffer over flow protection.

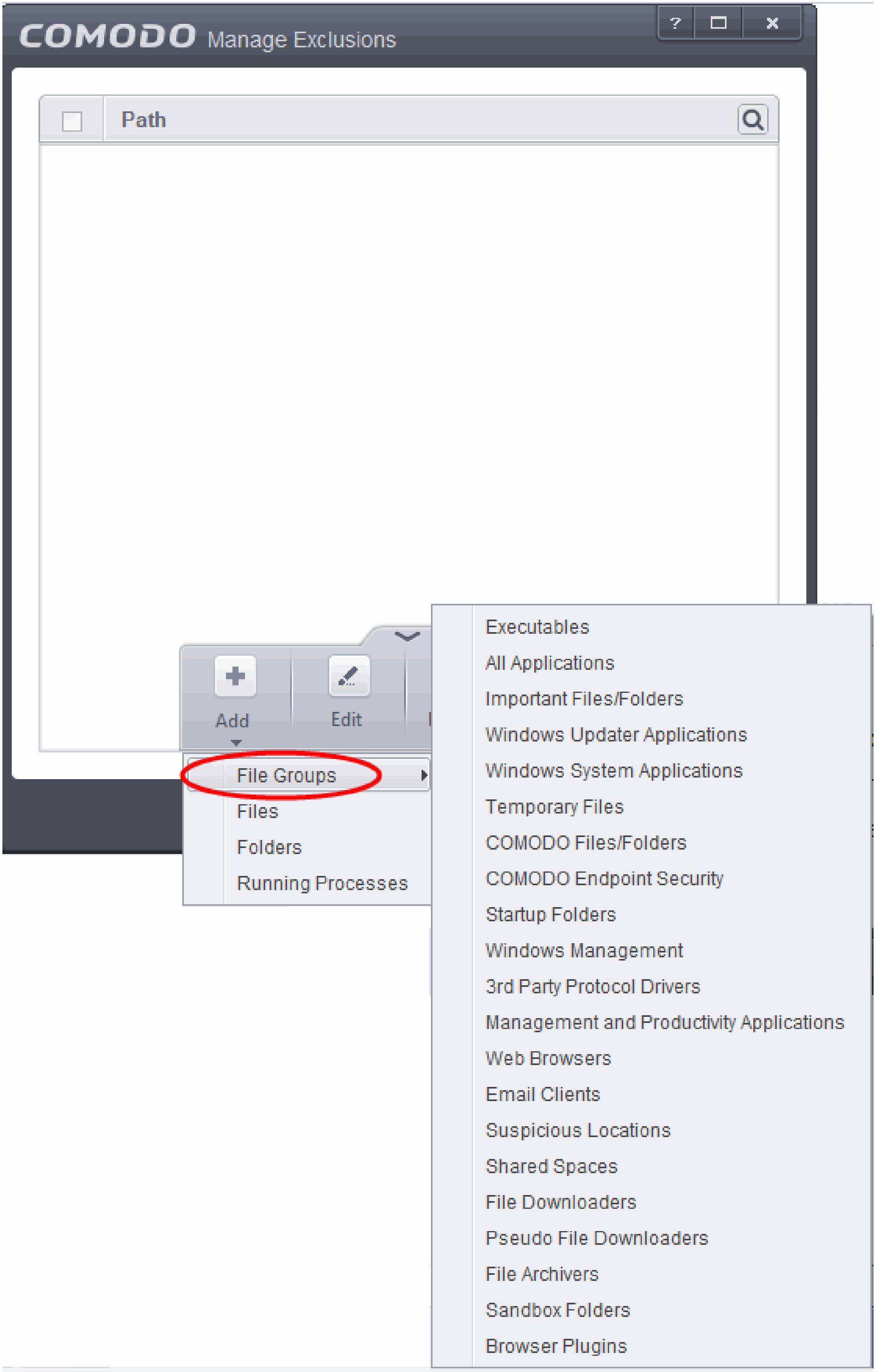
  Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

  Turning-on buffer overflow protection instructs the Comodo Client Security to raise pop-up alerts in every event of a possible buffer overflow attack. You can allow or deny the requested activity raised by the process under execution depending on the reliability of the software and its vendor.

  Comodo recommends that this setting to be maintained selected always. ***(Default = Enabled)***

  To exclude some of the file types from being monitored under Detect Shellcode injections.

  - Select the 'Detect shellcode injections' checkbox and click the Exclusions link. The 'Manage Exclusions' dialog will appear.
  - Click the handle from the bottom of the interface and choose 'Add'
  - You can add items by selecting the required option from the drop-down:



- **File Groups** - Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. For more details on file groups, refer to the section File Groups.

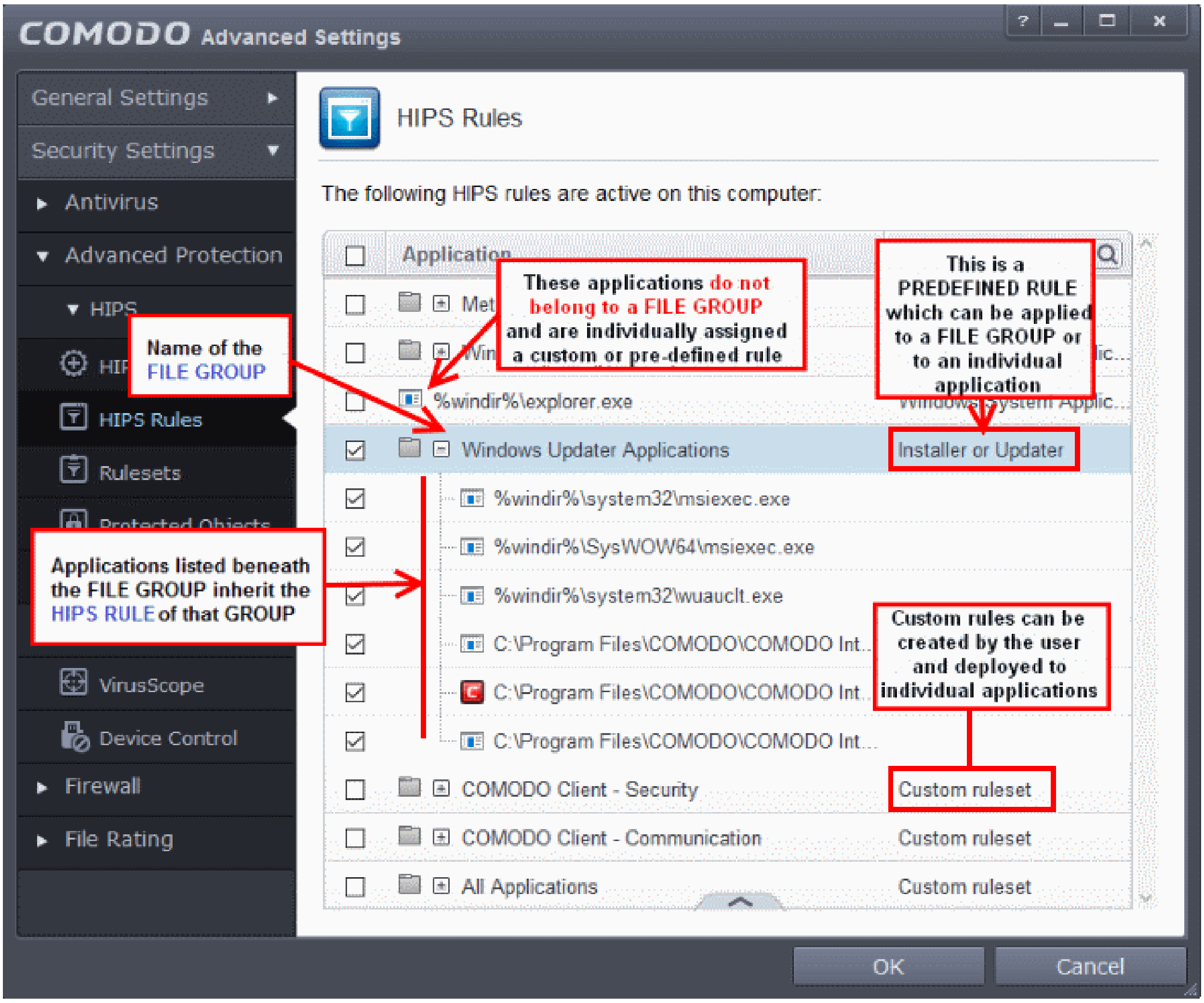
- **Running Processes** - As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.
- **Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
- **Files** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.

Note: These settings are recommended for advanced users only.

- Click 'OK' to implement your settings.

6.2.2.2. Active HIPS Rules

The HIPS rules tab lists the different groups of applications installed in your system and the Rulesets applied to them. You can change the ruleset applied to selected applications and also create custom rulesets to be applied to selected applications.



The following HIPS rules are active on this computer:

☐	Application	
☐	⊞ Met...	
☐	⊞ Win...	...ic...
☐	%windir%\explorer.exe	Windows System Applic...
☑	⊟ Windows Updater Applications	Installer or Updater
☑	%windir%\system32\msiexec.exe	
☑	%windir%\SysWOW64\msiexec.exe	
☑	%windir%\system32\wuauclt.exe	
☑	C:\Program Files\COMODO\COMODO Int...	
☑	C:\Program Files\COMODO\COMODO Int...	
☑	C:\Program Files\COMODO\COMODO Int...	
☐	⊞ COMODO Client - Security	Custom ruleset
☐	⊞ COMODO Client - Communication	Custom ruleset
☐	⊞ All Applications	Custom ruleset

Name of the FILE GROUP

These applications do not belong to a FILE GROUP and are individually assigned a custom or pre-defined rule

This is a PREDEFINED RULE which can be applied to a FILE GROUP or to an individual application

Applications listed beneath the FILE GROUP inherit the HIPS RULE of that GROUP

Custom rules can be created by the user and deployed to individual applications

The first column, **Application Name**, displays a list of the applications on your system for which a HIPS ruleset has been deployed. If the application belongs to a file group, then all member applications assume the ruleset of the file group. The second column, **Treat as**, column displays the name of the HIPS ruleset assigned to the application or group of applications in column one.

General Navigation:

Clicking the handle at the bottom of the interface opens an option panel:

- **Add** - Allows the user to Add a new Application to the list then create it's 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 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.

Users can re-order the priority of rules by simply selecting the application name or file group name in question, clicking the handle at the bottom 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.

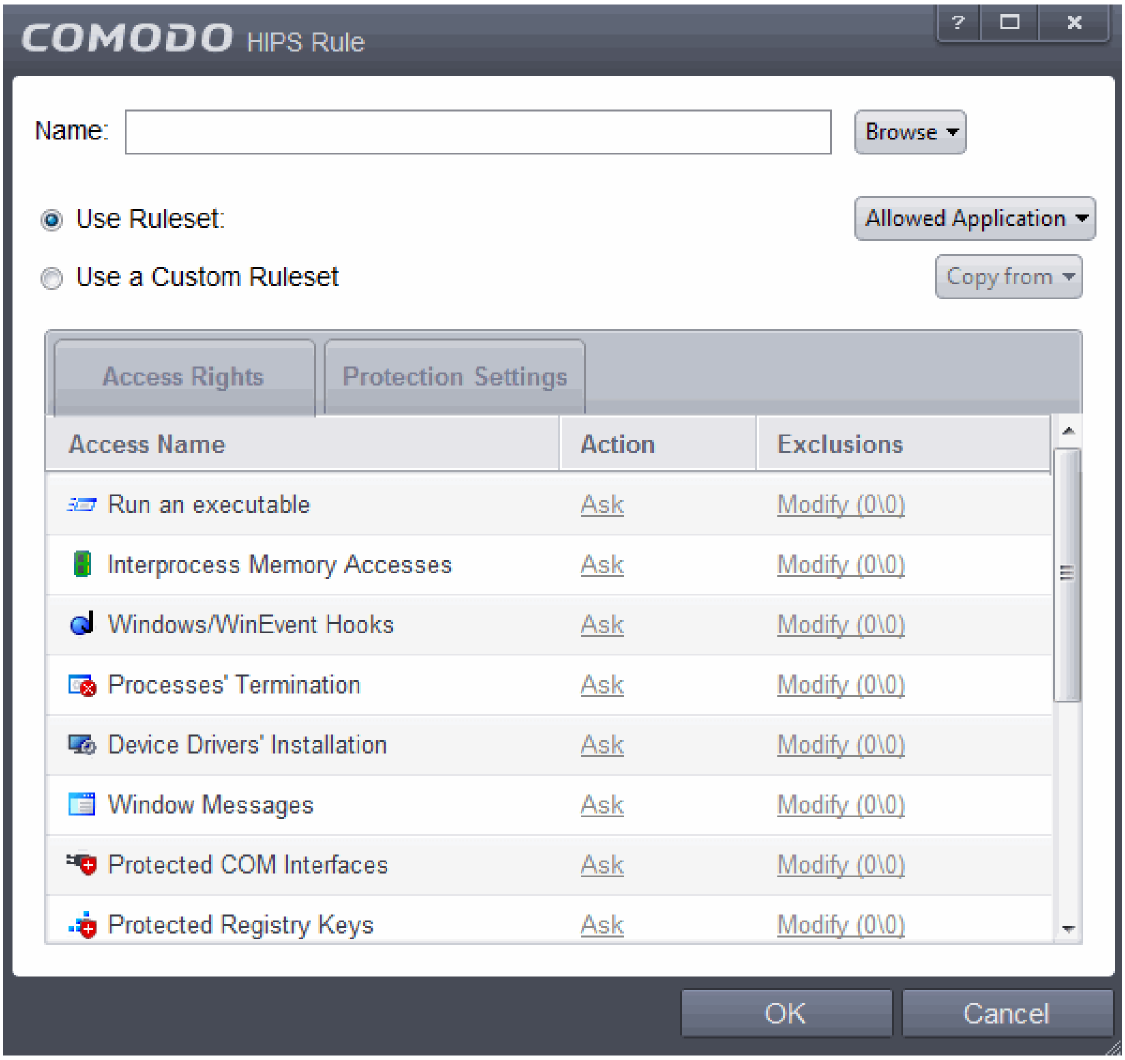
Creating or Modifying a HIPS Ruleset

To begin defining an application's HIPS Ruleset

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

If you wish to define a rule for a new application (i.e. one that is not already listed), click the handle from the **HIPS Rules pane** and select 'Add'. This brings up the 'HIPS Rule' interface as shown below.



Name:

● Use Ruleset: Allowed Application

○ Use a Custom Ruleset

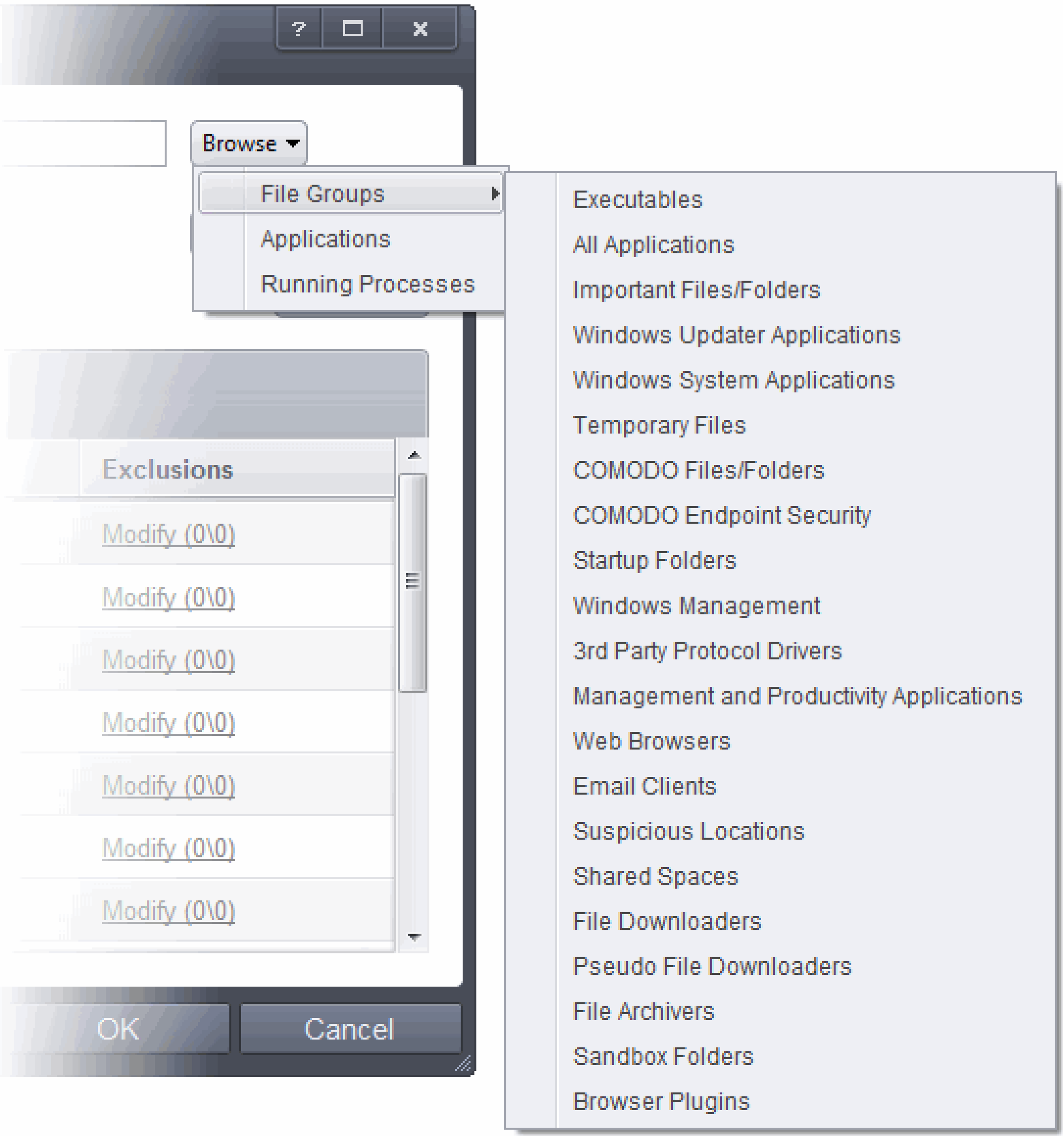
Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (0\0)

Because you are defining the HIPS rule settings for a new application, you can notice that the 'Name' box is blank. (If you were editing an existing rule instead, then this interface would show that application's name with installation path or application group's name.)

- Click 'Browse' to begin.

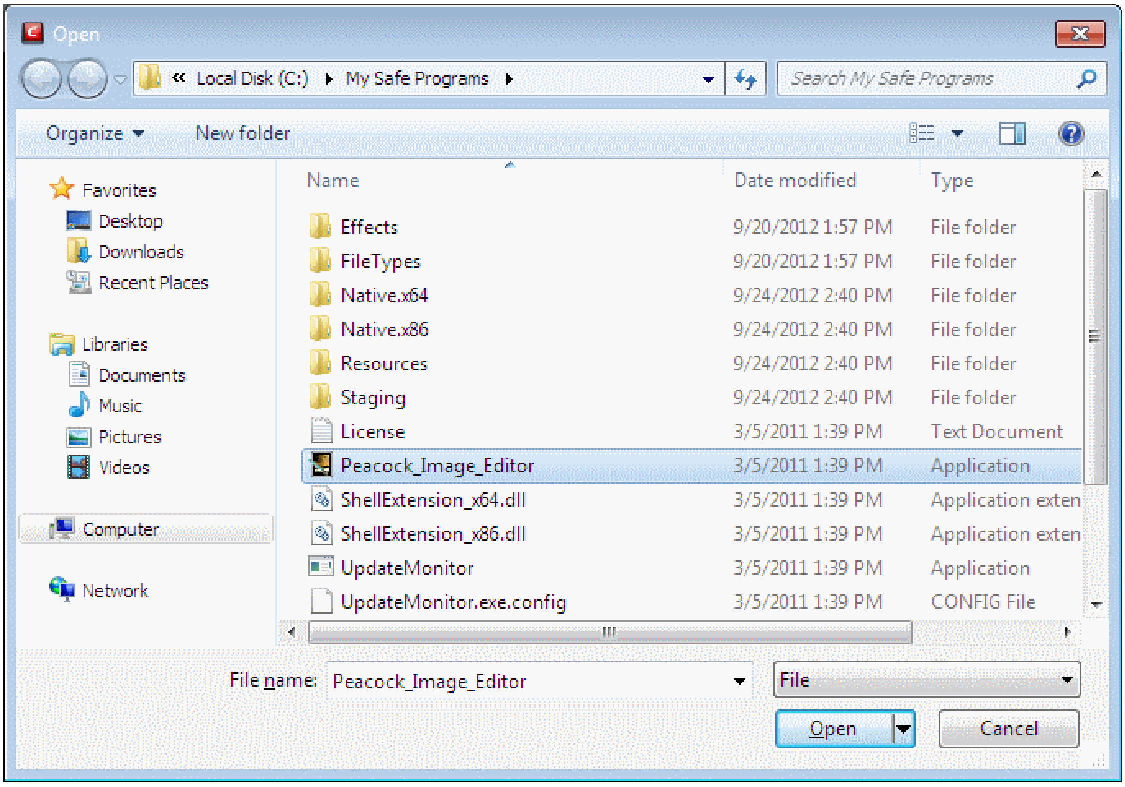
You now have 3 methods available to choose the application for which you wish to create a Ruleset - File Groups; Applications and Running Processes.

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 . 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.

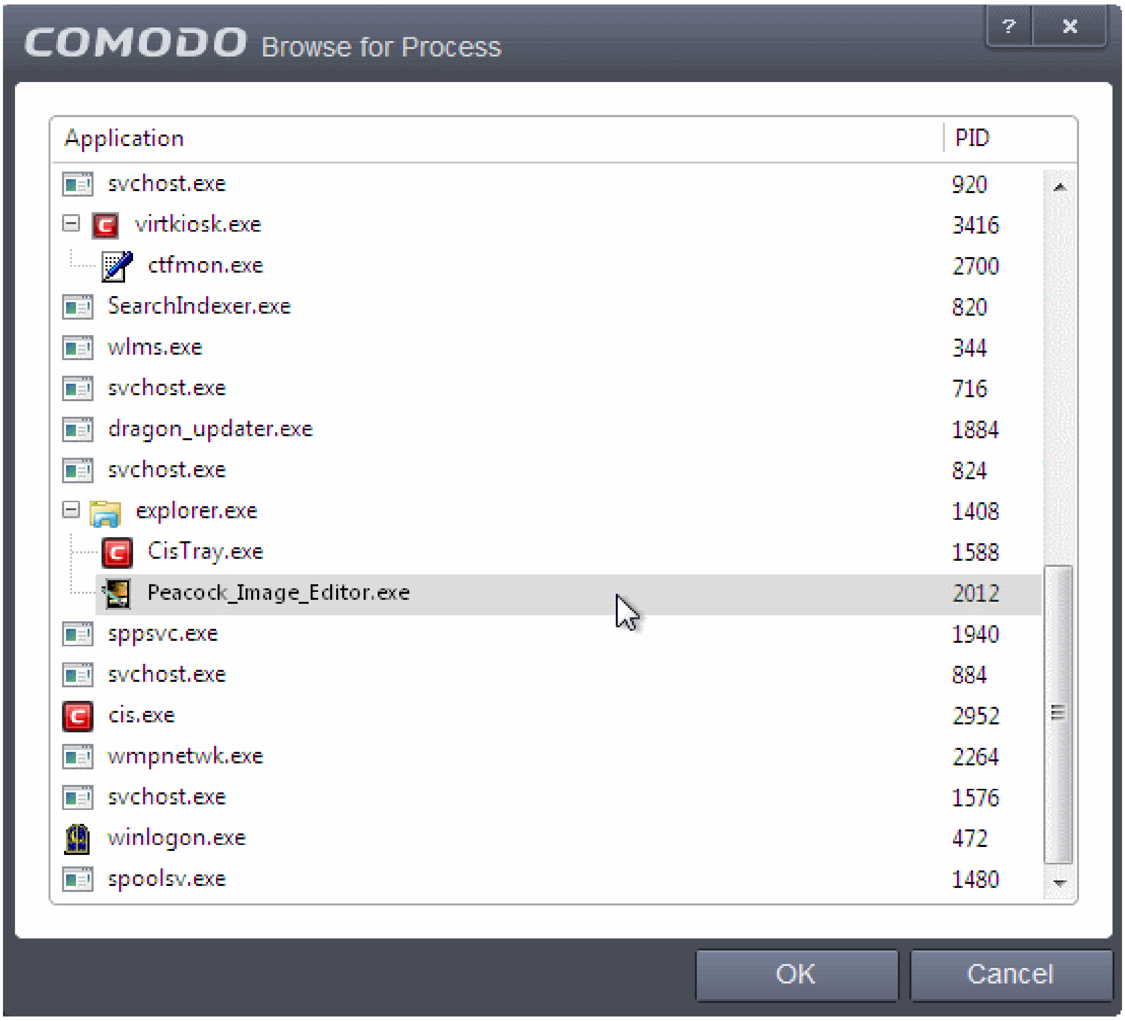


Name	Date modified	Type
Effects	9/20/2012 1:57 PM	File folder
FileTypes	9/20/2012 1:57 PM	File folder
Native.x64	9/24/2012 2:40 PM	File folder
Native.x86	9/24/2012 2:40 PM	File folder
Resources	9/24/2012 2:40 PM	File folder
Staging	9/24/2012 2:40 PM	File folder
License	3/5/2011 1:39 PM	Text Document
Peacock_Image_Editor	3/5/2011 1:39 PM	Application
ShellExtension_x64.dll	3/5/2011 1:39 PM	Application exten
ShellExtension_x86.dll	3/5/2011 1:39 PM	Application exten
UpdateMonitor	3/5/2011 1:39 PM	Application
UpdateMonitor.exe.config	3/5/2011 1:39 PM	CONFIG File

File name: Peacock_Image_Editor

File

3. **Running Processes -** as the name suggests, this option allows you to create and deploy a ruleset for any process that is currently running on your PC.



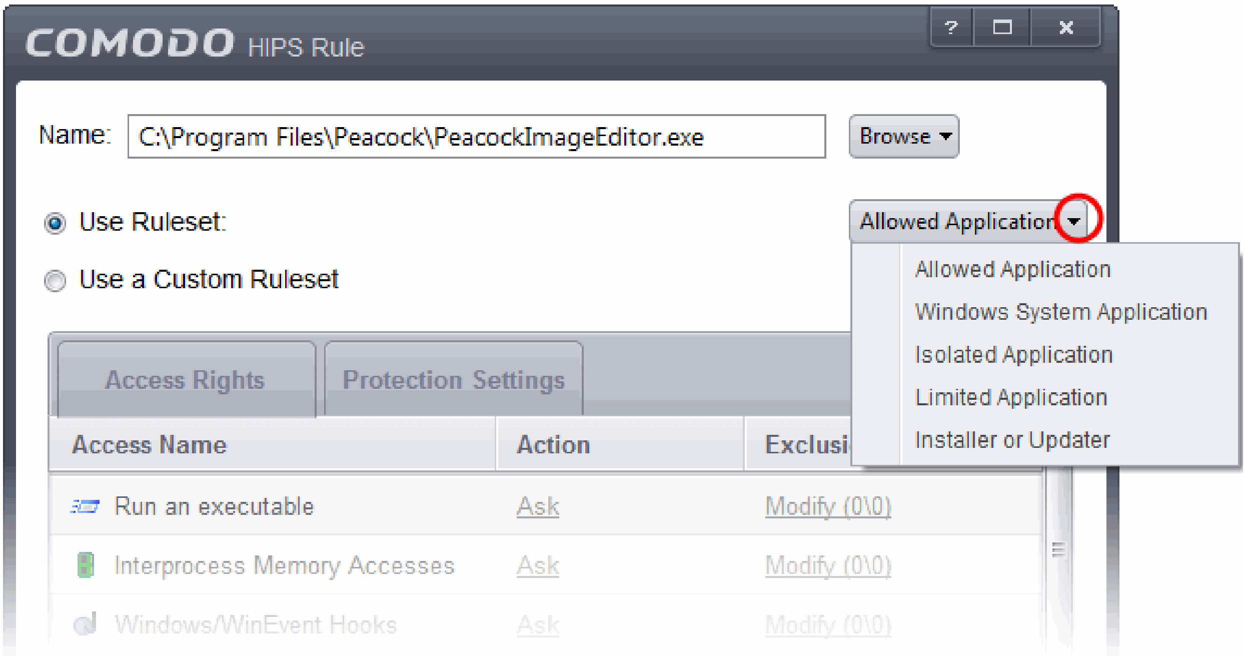
Application	PID
svchost.exe	920
⊟ virtkiosk.exe	3416
ctfmon.exe	2700
SearchIndexer.exe	820
wlms.exe	344
svchost.exe	716
dragon_updater.exe	1884
svchost.exe	824
⊟ explorer.exe	1408
CisTray.exe	1588
Peacock_Image_Editor.exe	2012
sppsvc.exe	1940
svchost.exe	884
cis.exe	2952
wmpnetwk.exe	2264
svchost.exe	1576
winlogon.exe	472
spoolsv.exe	1480

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 the user to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the HIPS Rules interface *(Default = Enabled).*



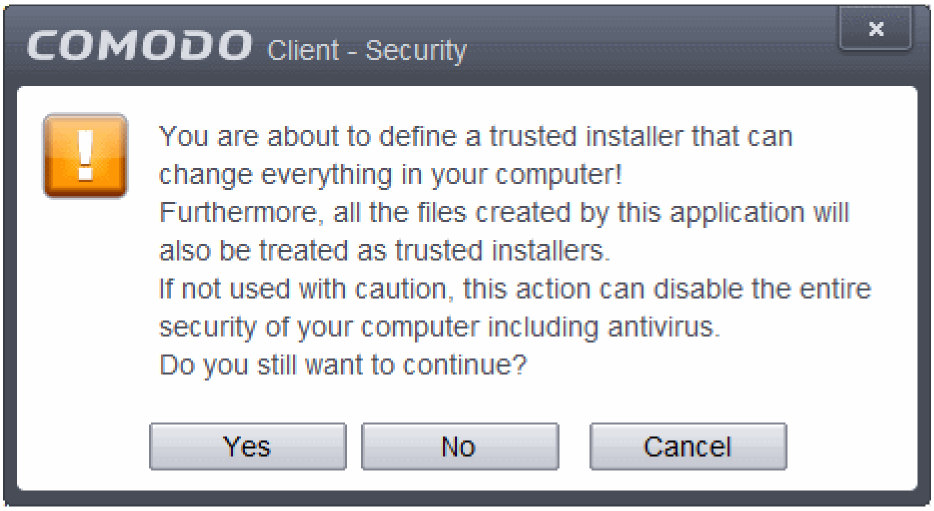
Name: C:\Program Files\Peacock\PeacockImageEditor.exe

● Use Ruleset: Allowed Application

○ Use a Custom Ruleset

Access Name	Action	Exclusi
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)

Note on 'Installer or Updater' Rule: Applying the Predefined Ruleset 'Installer or Updater' for an application defines it as a trusted installer and all files created by the application will also be considered as trusted files. 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.



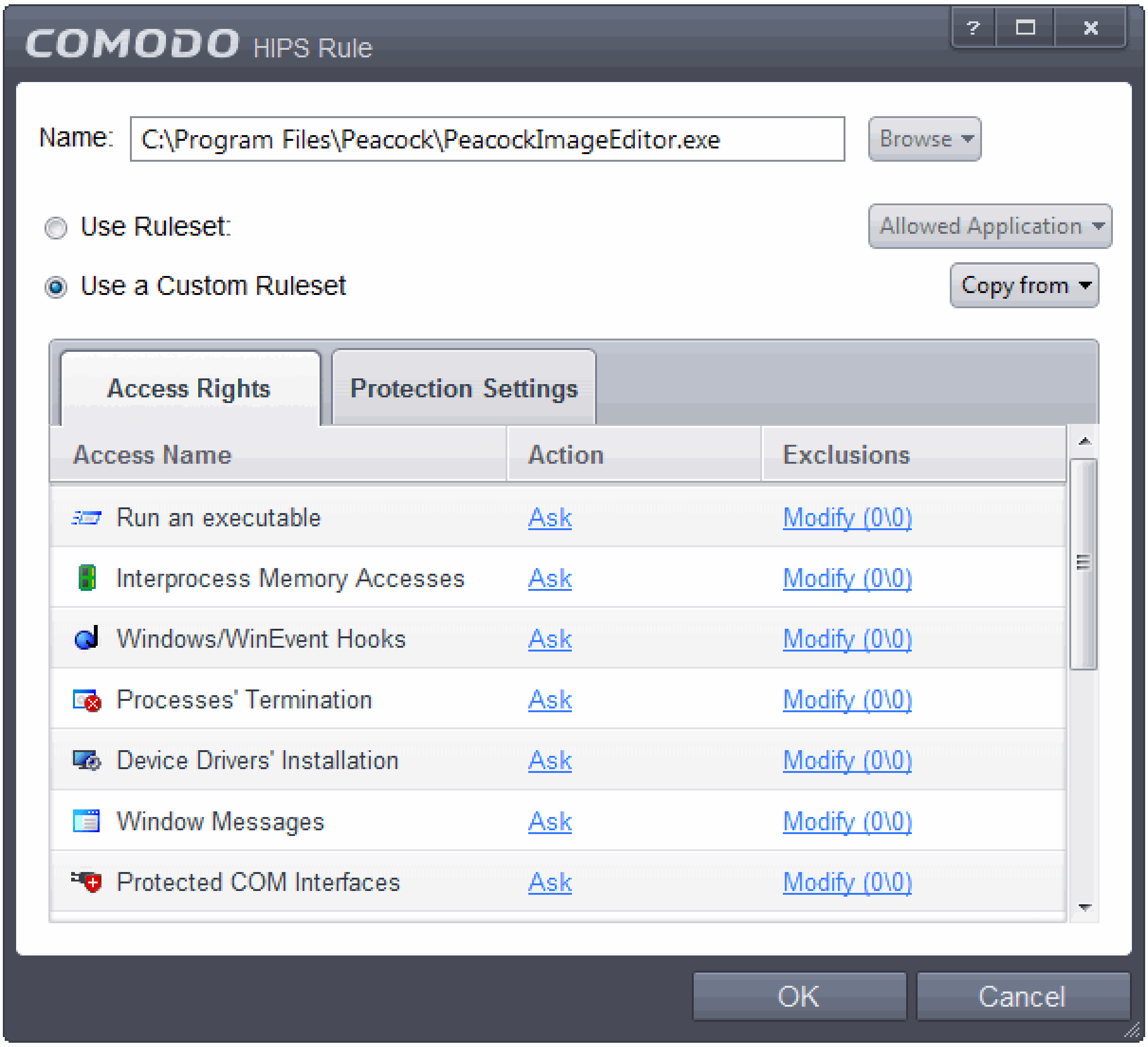
You are about to define a trusted installer that can change everything in your computer!
Furthermore, all the files created by this application will also be treated as trusted installers.
If not used with caution, this action can disable the entire security of your computer including antivirus.
Do you still want to continue?

General 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 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 enables full control over the configuration specific security ruleset and the parameters of each rule within that ruleset. The Custom ruleset has two main configuration areas - Access Rights and Protection Settings *(Default = Disabled).*

   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.

   i. **Access Rights** - The Process Access Rights tab allows you to determine what activities the applications in your custom ruleset are allowed to execute. These activities are called 'Access Names'.



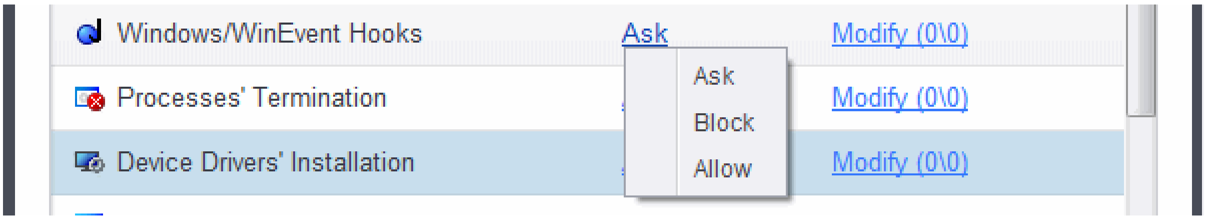
Name: C:\Program Files\Peacock\PeacockImageEditor.exe

○ Use Ruleset:

● Use a Custom Ruleset

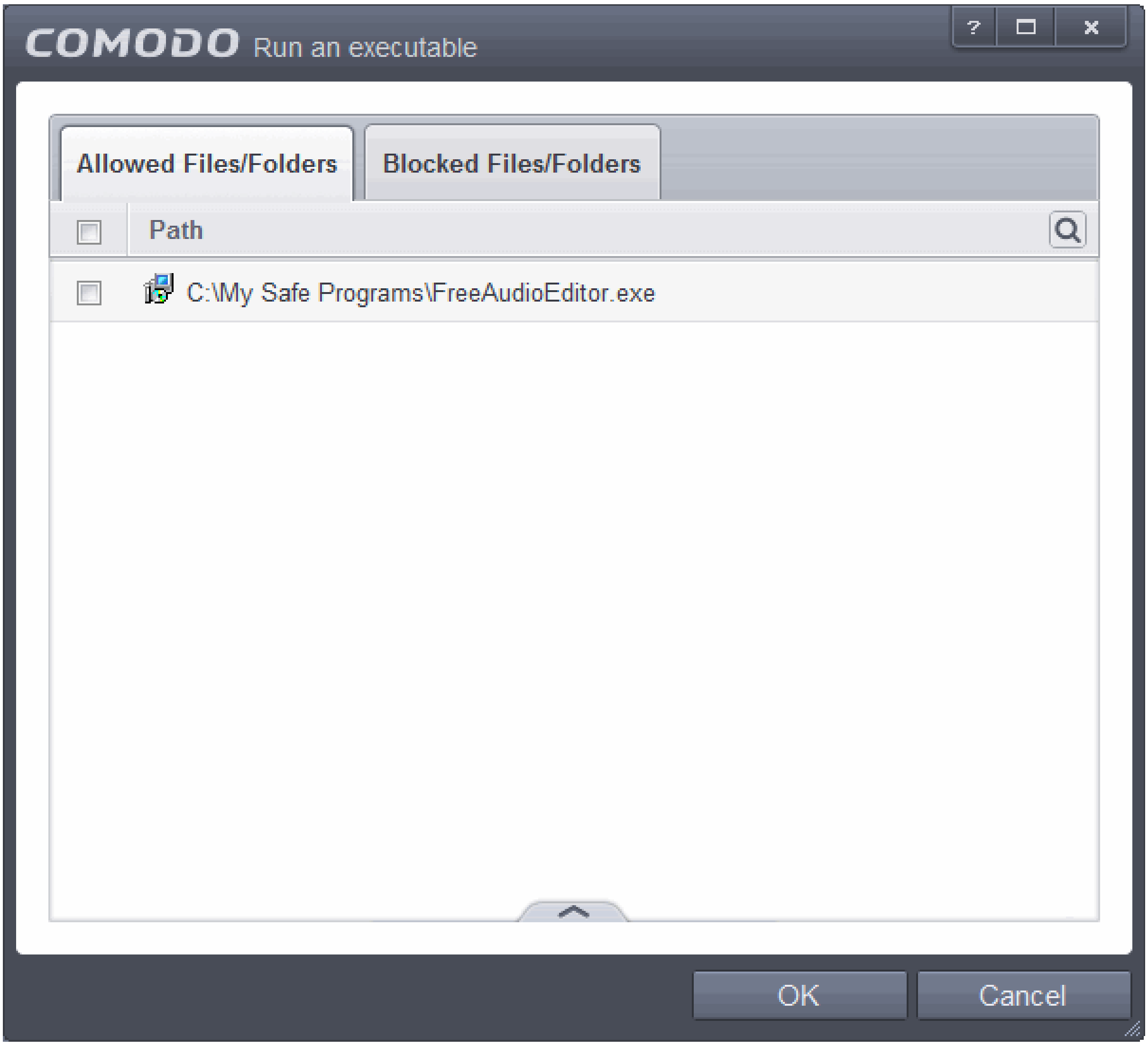
Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify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

Refer to the section HIPS Behavior Settings > Activities to Monitor to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:



Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination		Modify (0\0)
Device Drivers' Installation		Modify (0\0)

- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.

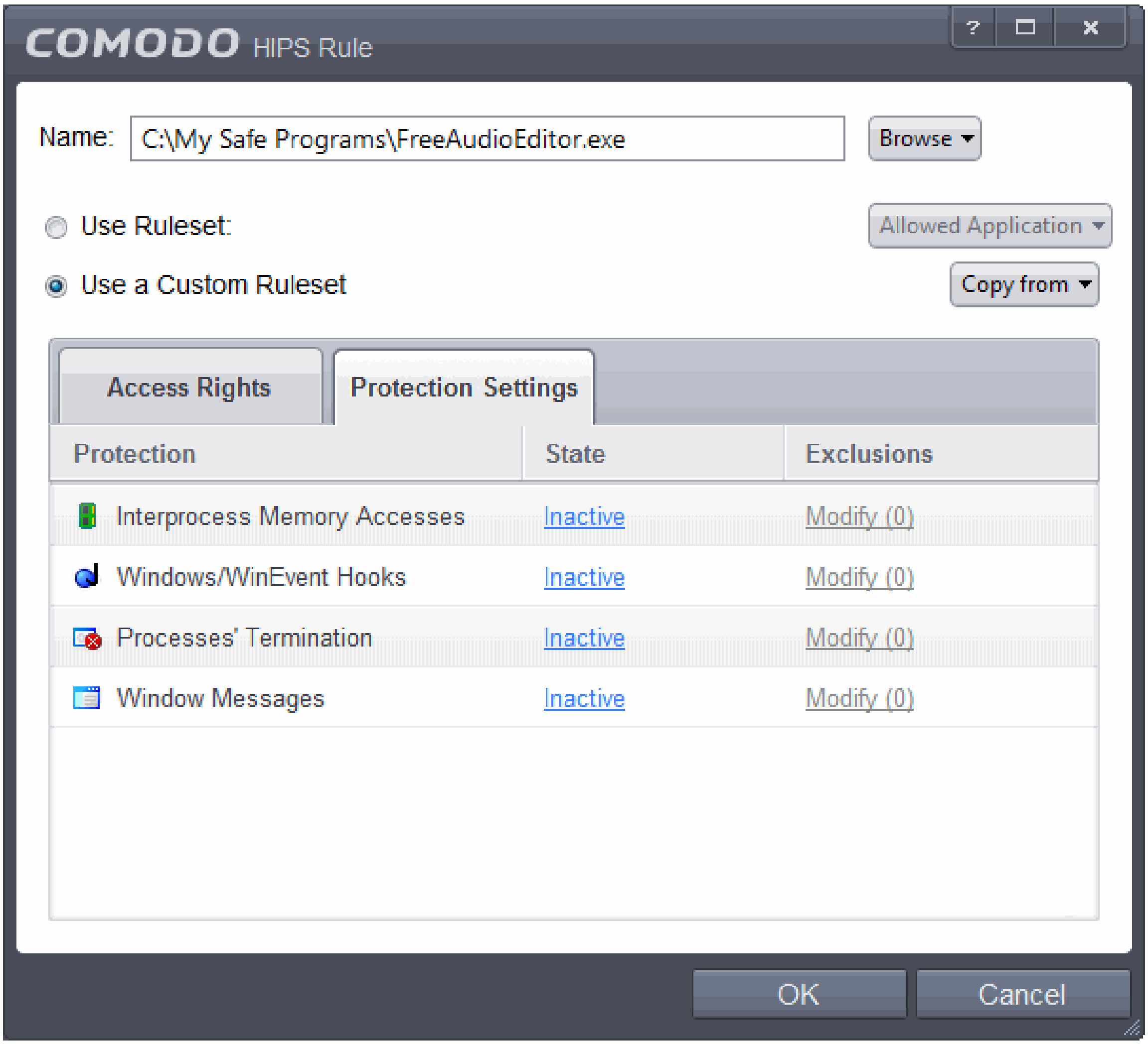


□	Path
□	C:\My Safe Programs\FreeAudioEditor.exe

Clicking the handle and selecting 'Add' 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 '*Ask*'. This means HIPS will generate an alert asking your permission if 'Peacock_Image_Editor.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'opera.exe' to the 'Allowed Applications' tab creates an exception to this rule. Peacock_Image_Editor.exe can now modify the memory space of firefox.exe.

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



Name: C:\My Safe Programs\FreeAudioEditor.exe

○ Use Ruleset: Allowed Application
● Use a Custom Ruleset

Protection	State	Exclusions
Interprocess Memory Accesses	Inactive	Modify (0)
Windows/WinEvent Hooks	Inactive	Modify (0)
Processes' Termination	Inactive	Modify (0)
Window Messages	Inactive	Modify (0)

- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection Type' 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.

6.2.2.3. HIPS Rule Sets

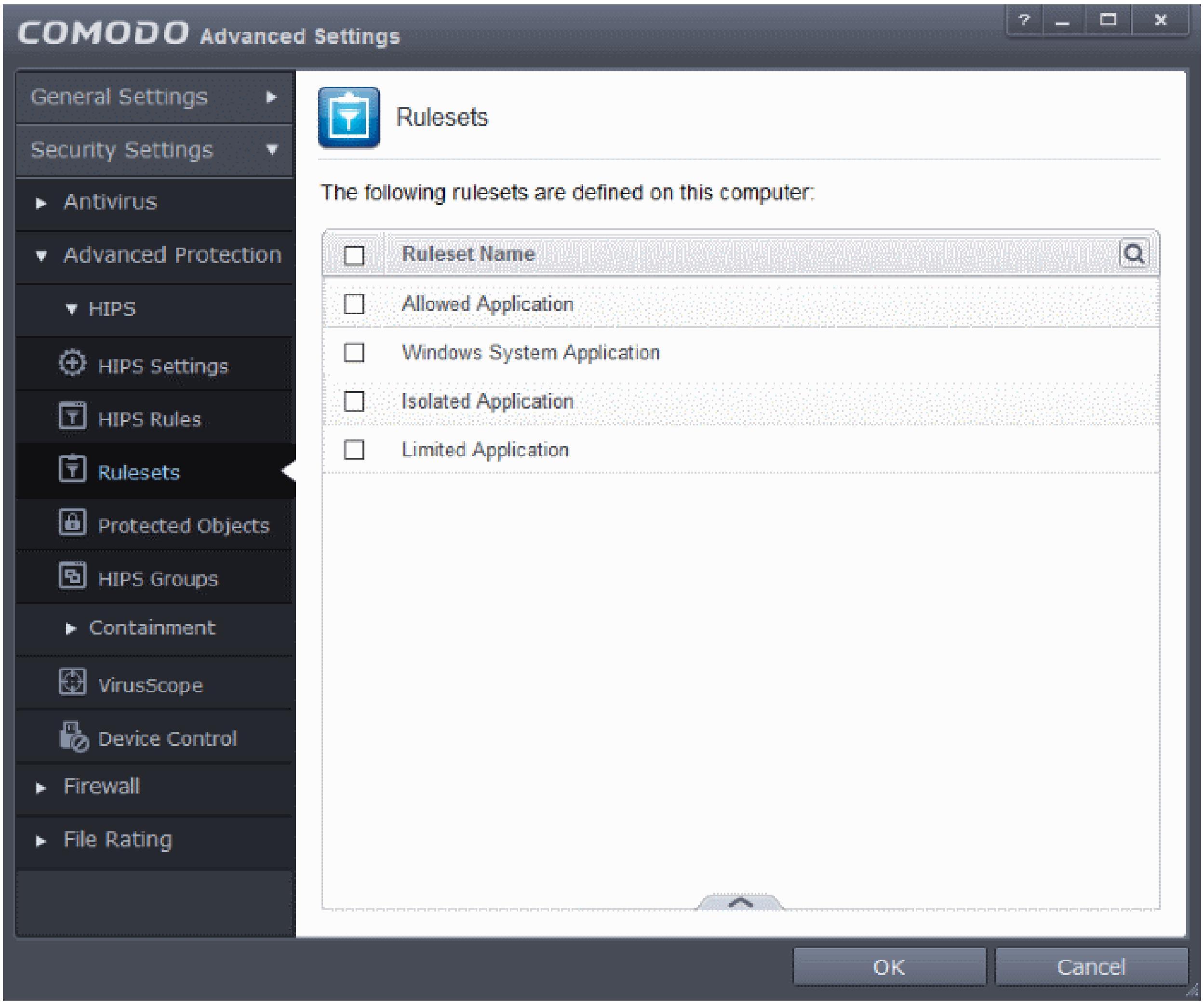
A Pre-defined ruleset is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined rulesets' is a set of rulesets that concern an application's access rights to memory, other programs, the registry etc.

> Note: This section is for advanced and experienced users. If you are a novice user to Comodo Client Security, we advise you first read the **Active HIPS Rules** section in this help guide if you have not already done so.

Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Client Security contains a selection of rulesets according to broad application categories. Each predefined ruleset has been specifically designed by Comodo 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.

To configure this category

- Navigate to: Advanced Tasks > Security Settings >Advanced Protection > HIPS > Rulesets. There are four default Rulesets listed under the 'Ruleset Name' column.



Rulesets

The following rulesets are defined on this computer:

□	Ruleset Name
□	Allowed Application
□	Windows System Application
□	Isolated Application
□	Limited Application

To view or edit an existing predefined ruleset

- Double click on the Ruleset in the list

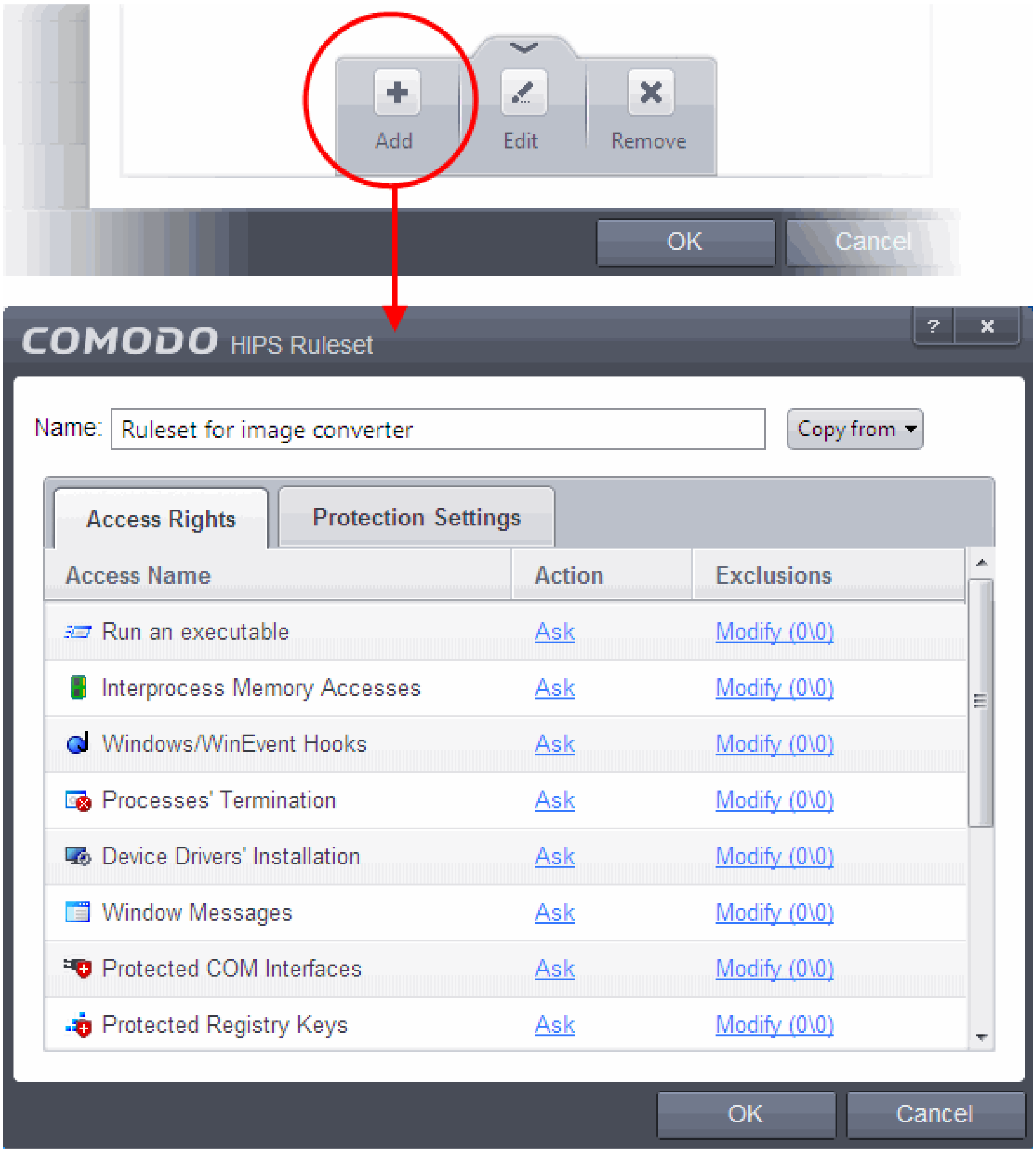
  or

- Select the Ruleset, click the handle at the bottom of the interface and choose 'Edit' from the options.

From here, you can modify a ruleset and, if desired, make changes to its 'Access Rights' and 'Protection Settings'. Any changes you make here are automatically rolled out to all applications that are currently applied with the ruleset.

To create a new predefined ruleset

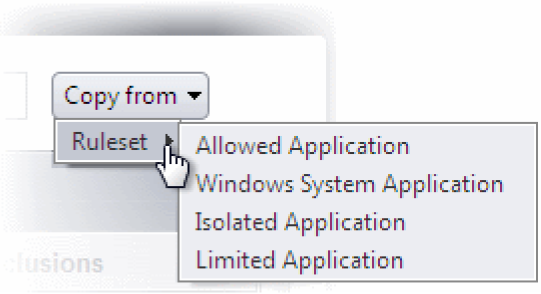
- Click up arrow at the bottom of the interface and choose 'Add' from the options.

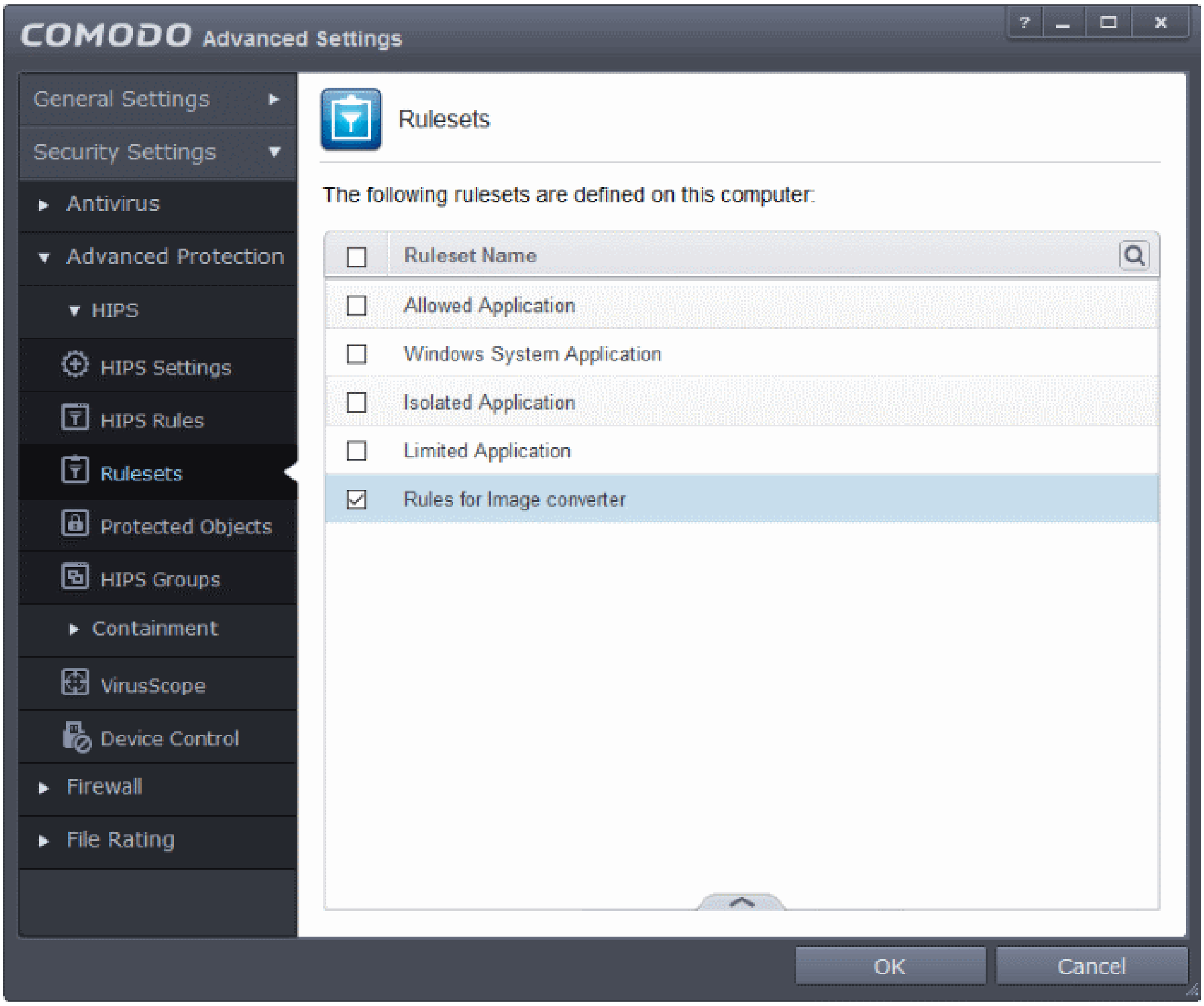


Name: Ruleset for image converter

Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (0\0)

- Enter a name for the new ruleset.
- To copy the Access Rights and Protection Settings from another pre-existing ruleset, click 'Copy From' and select the ruleset from the drop-down
- To customize the Access Rights and Protection Settings as per the requirements of this new rule set, follow the procedure explained in the section Use a Custom Ruleset.
- Click 'OK' to save the new ruleset.





Rulesets

The following rulesets are defined on this computer:

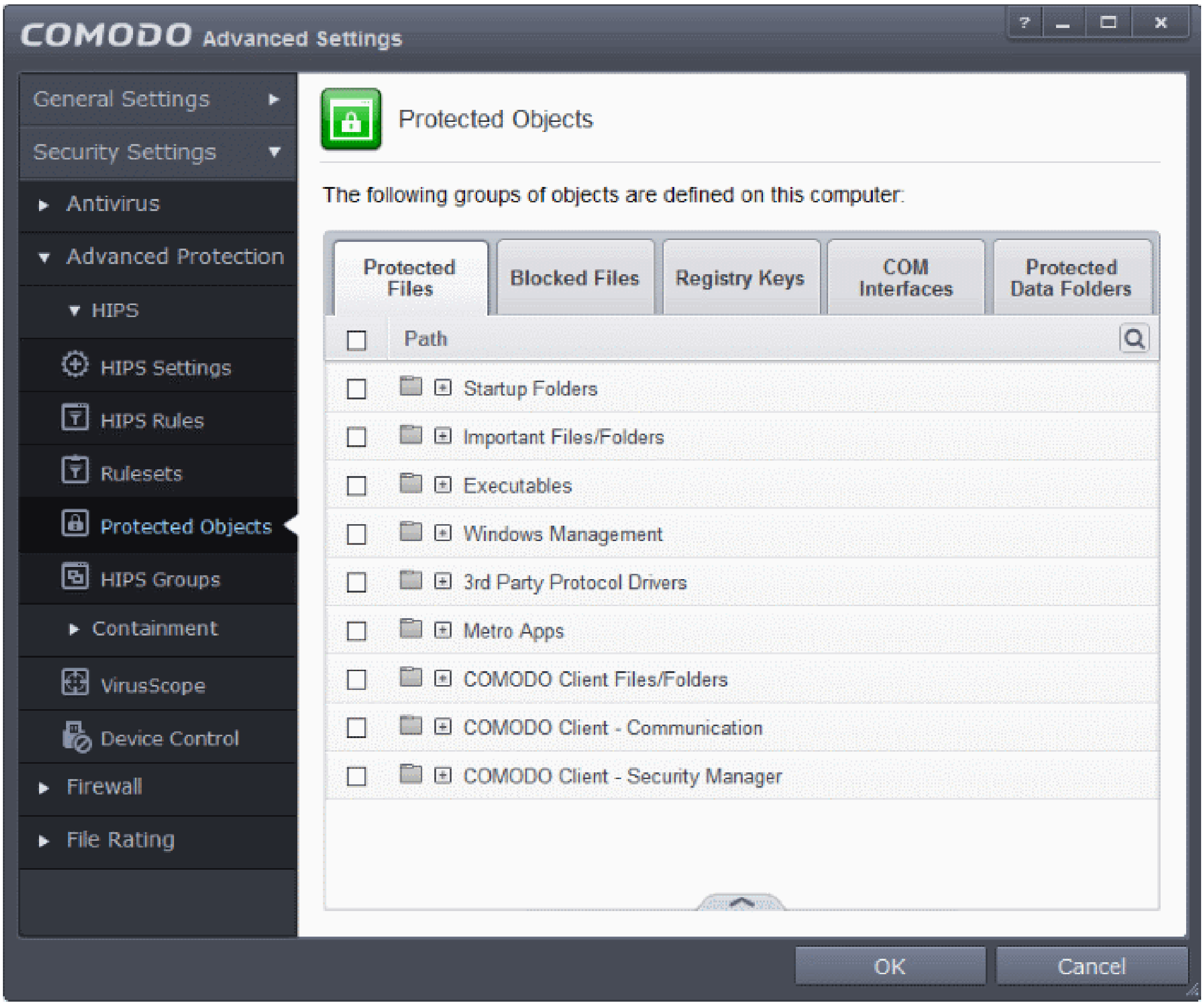
□	Ruleset Name
□	Allowed Application
□	Windows System Application
□	Isolated Application
□	Limited Application
☑	Rules for Image converter

Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.

6.2.2.4. Protected Objects

The Protected Objects panel allows you to protect specific files and folders, system critical registry keys and COM interfaces against access or modification by unauthorized processes and services. You can also add files to Protected Data Folders so that contained programs will be blocked from accessing them.

The File Protection panel can be accessed by clicking Security Settings > Advanced Protection > HIPS > Protected Objects from the Advanced Settings interface.



Protected Objects

The following groups of objects are defined on this computer:

□	Path
□	⊞ Startup Folders
□	⊞ Important Files/Folders
□	⊞ Executables
□	⊞ Windows Management
□	⊞ 3rd Party Protocol Drivers
□	⊞ Metro Apps
□	⊞ COMODO Client Files/Folders
□	⊞ COMODO Client - Communication
□	⊞ COMODO Client - Security Manager

The panel has five tabs:

- Protected Files - Allows you to specify programs, applications and files that are to be protected from changes
- Blocked Files - Allows you to specify programs, applications and files that are to be blocked from execution and opening
- Registry Keys - Allows you to specify registry keys that are to be protected from changes
- COM Interface - Allows you to specify COM interfaces that are to be protected from changes
- Protected Data Folders - Allows you to specify folders containing data files that are to be protected from changes by the contained programs

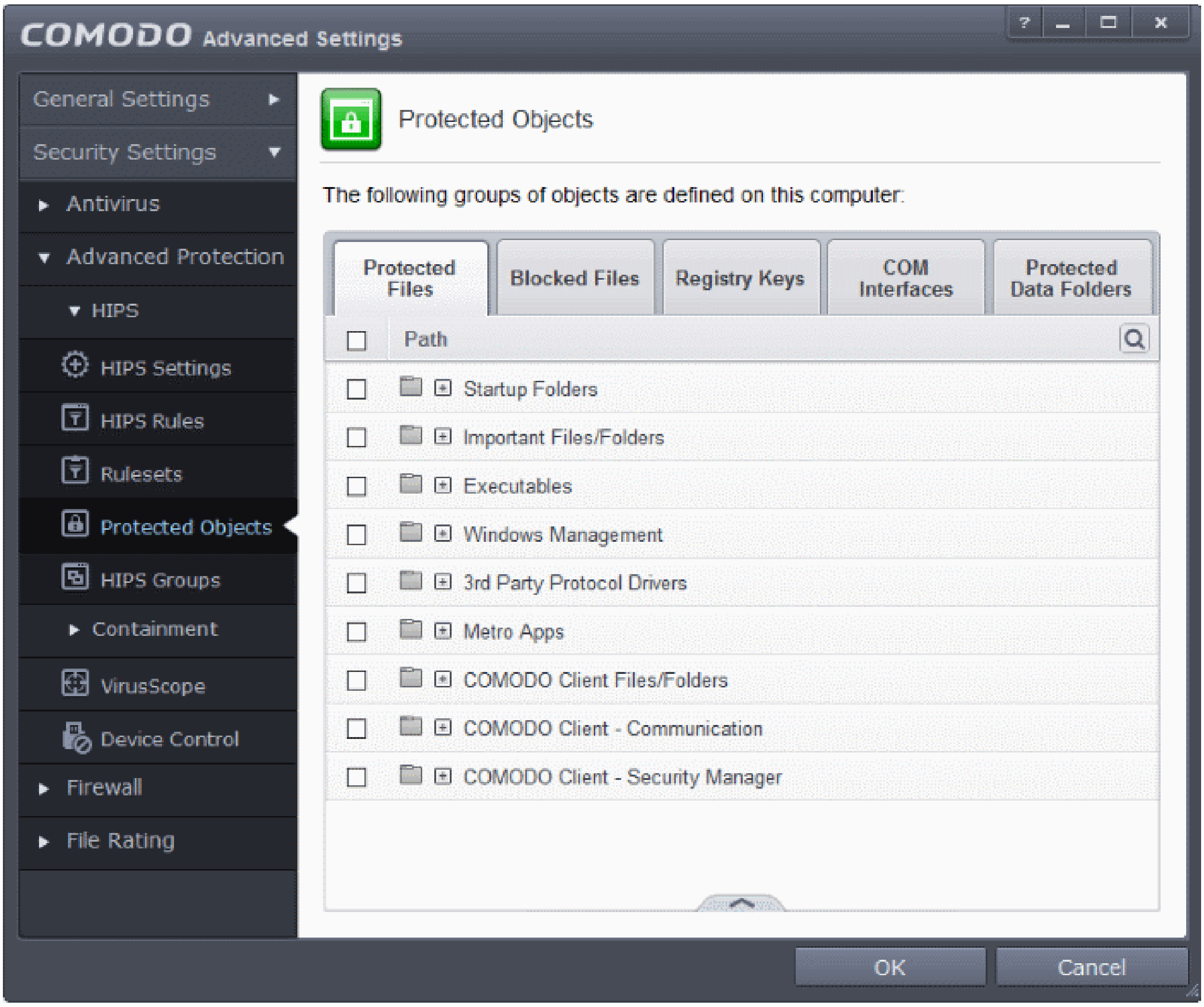
6.2.2.4.1. Protected Files

The Protected Files tab displays a list of files and file groups that are protected from access by other programs, especially malicious programs such as virus, Trojans and spyware. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying anyone and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is the your 'hosts' file. (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Client Security blocks this attempt and produce a 'Protected File Access' pop-up alert.

If you add a file to Protected Files, but want to allow trusted application to access it, then rules can be defined in HIPS Rulesets. Refer to the section Exceptions for more details about how to allow access to files placed in

Protected Files.

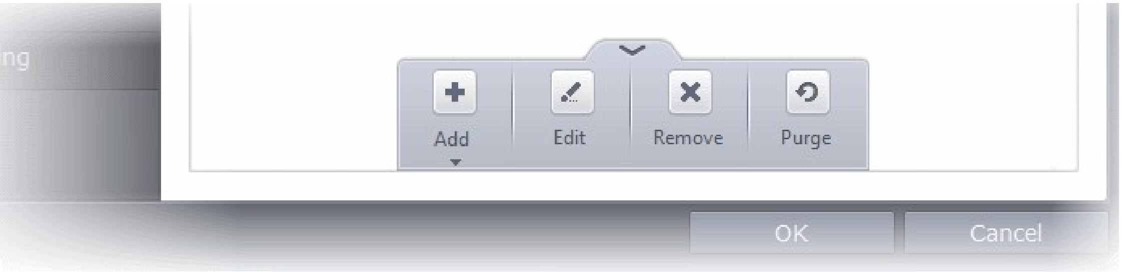
To open the 'Protected Files' screen, click 'Security Settings' > 'Advanced Protection' > 'Protected Objects' > then click the 'Protected Files' tab.



The following groups of objects are defined on this computer:

□ Path
□ Startup Folders
□ Important Files/Folders
□ Executables
□ Windows Management
□ 3rd Party Protocol Drivers
□ Metro Apps
□ COMODO Client Files/Folders
□ COMODO Client - Communication
□ COMODO Client - Security Manager

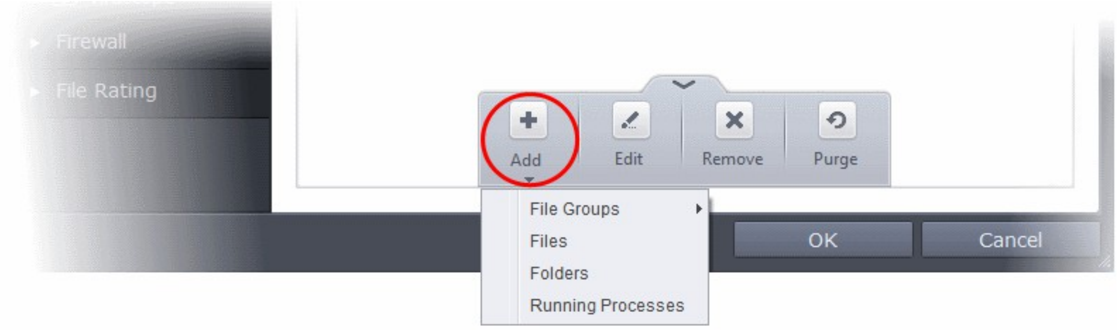
Clicking the handle at the bottom of the interface opens an options panel:



- Add - Allows you to add individual files, folders, programs, applications to Protected Files.
- Edit - Allows you to edit the path of the file or group of a selected item in the Protected Files interface.
- Remove - Deletes the currently highlighted file or file group.
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

To manually add an individual file, folder, file group or process

- Click the handle from the bottom center and select 'Add'.

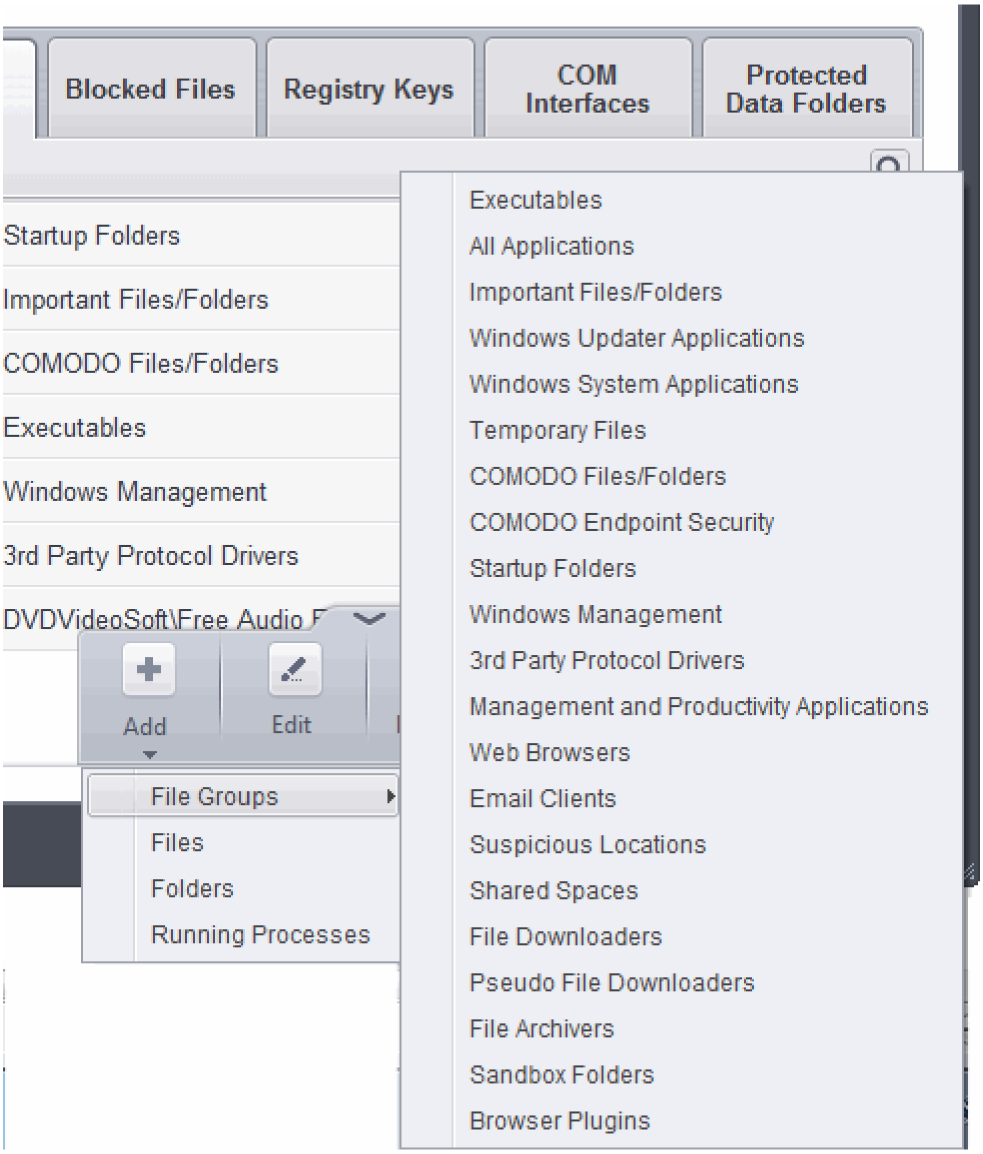


You can add the files by following methods:

- Selecting from File Groups
- Browsing to a Folder
- Browsing to a File
- Selecting from currently running Processes

Adding a File Group

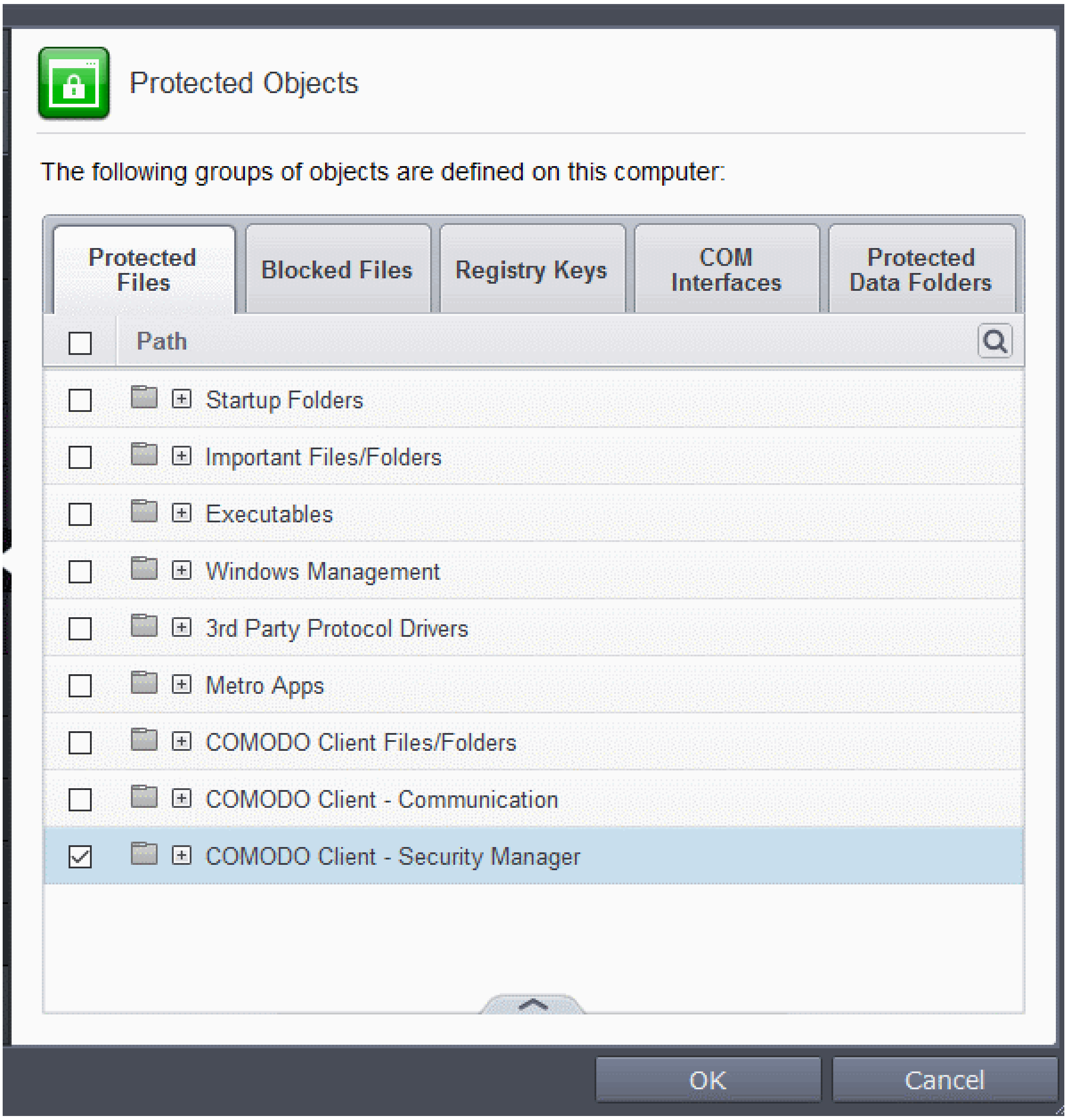
Choosing File Groups allows you to add a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' and so on - 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 predefined File Groups and can be viewed in Advanced Settings > File Rating > File Groups. You can also add new file groups here which will be displayed in the predefined list.

To add a file group to Protected Files, click Add > File Groups and select the type of File Group from the list.

The file group will be added to Protected Files.



Protected Objects

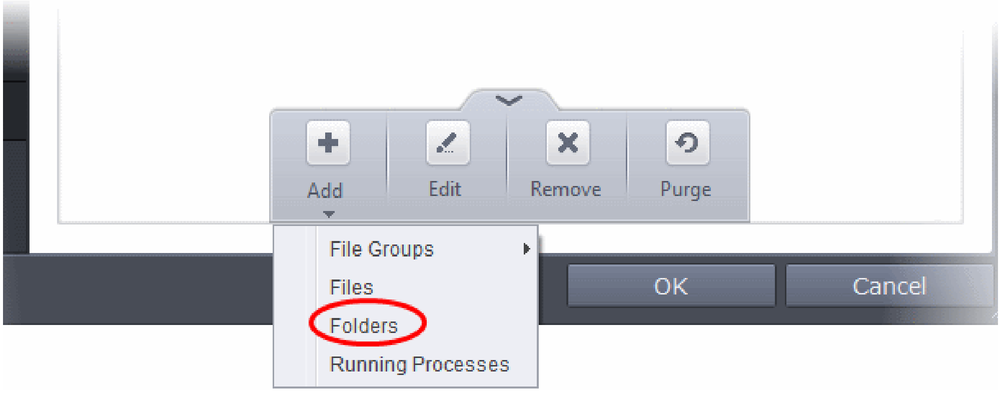
The following groups of objects are defined on this computer:

□	Path
□	Startup Folders
□	Important Files/Folders
□	Executables
□	Windows Management
□	3rd Party Protocol Drivers
□	Metro Apps
□	COMODO Client Files/Folders
□	COMODO Client - Communication
☑	COMODO Client - Security Manager

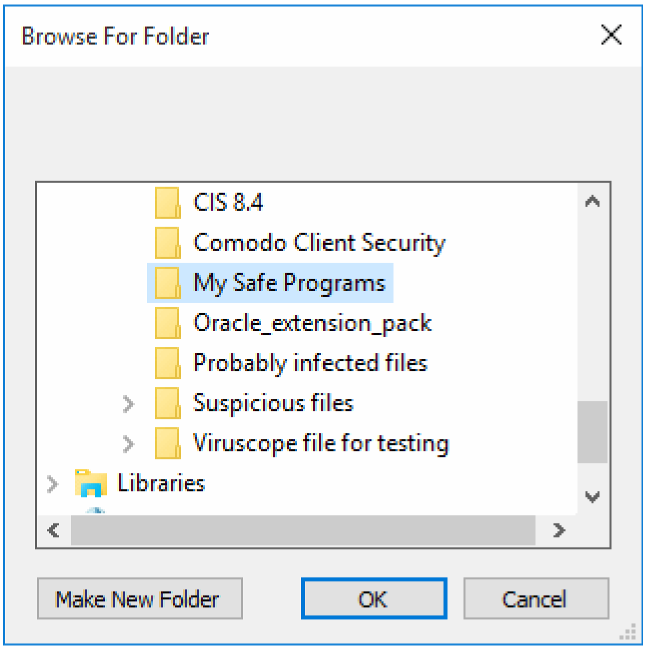
- Repeat the process to add more file groups. The items added to the Protected Files will be protected from access by other programs.

Adding a Drive Partition/Folder

- To add a folder, choose 'Folders' from the 'Add' drop-down.

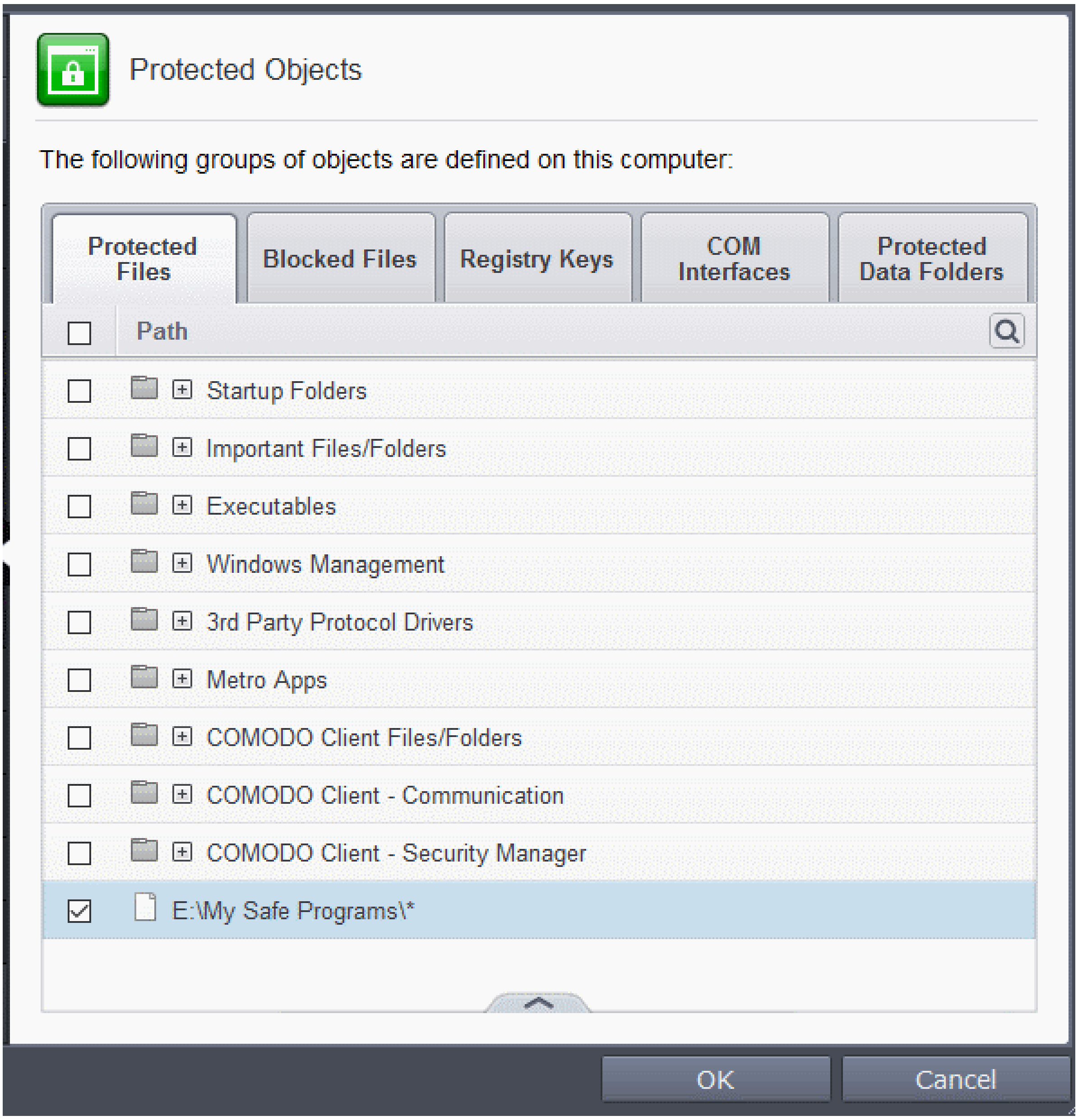


The 'Browse for Folder' dialog will appear.



- Navigate to the drive partition or folder you want to add to Protected Files and click 'OK'

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



Protected Objects

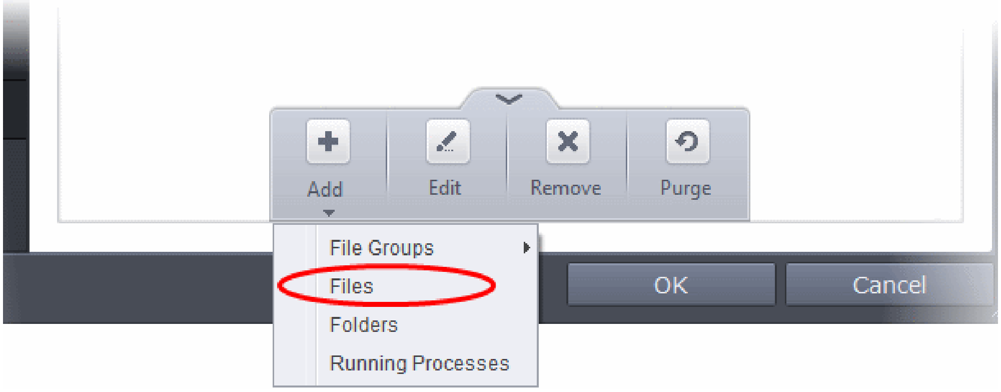
The following groups of objects are defined on this computer:

	Path
□	Startup Folders
□	Important Files/Folders
□	Executables
□	Windows Management
□	3rd Party Protocol Drivers
□	Metro Apps
□	COMODO Client Files/Folders
□	COMODO Client - Communication
□	COMODO Client - Security Manager
☑	E:\My Safe Programs*

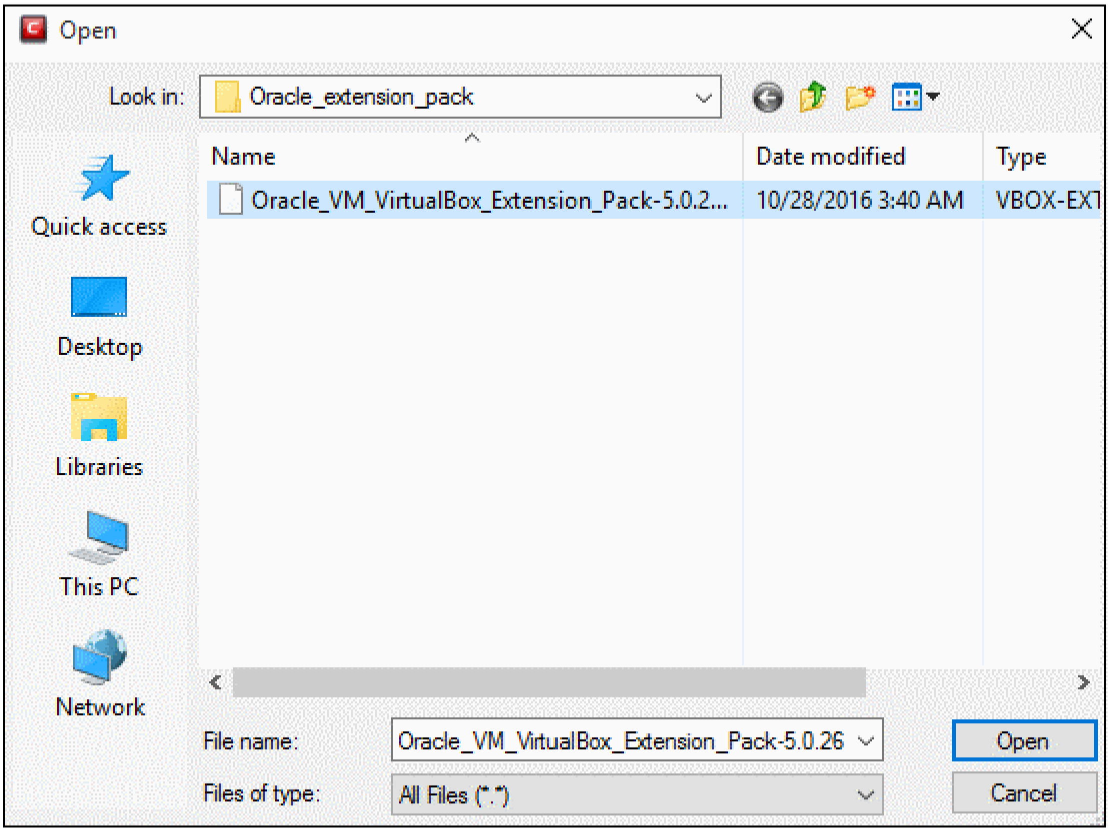
- Repeat the process to add more folders. The items added to the Protected Files will be protected from access by other programs.

Adding an individual File

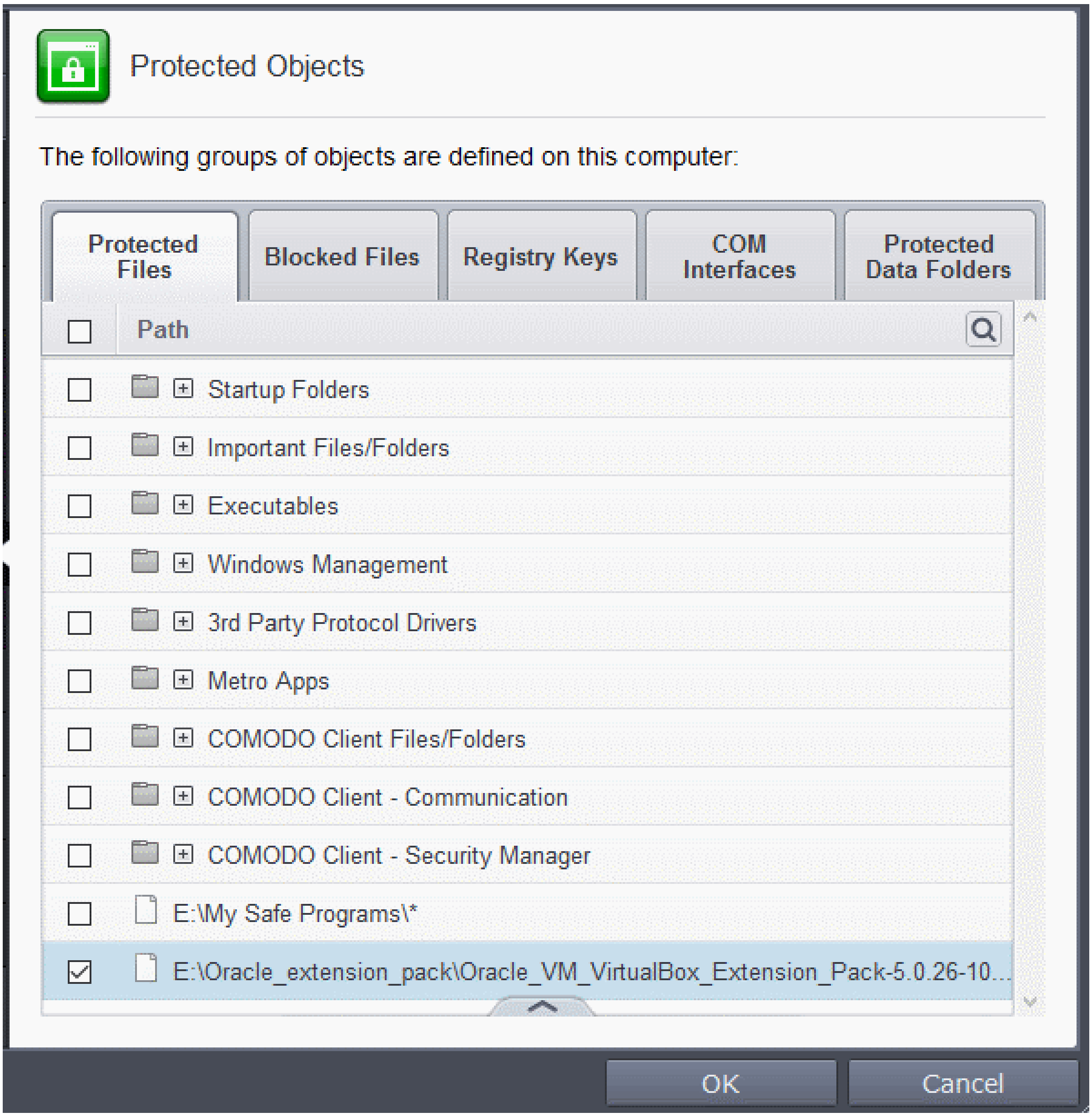
- Choose 'Files' from the 'Add' drop-down.



- Navigate to the file you want to add to Protected Files in the 'Open' dialog and click 'Open'


Open
Look in: Oracle_extension_pack
Quick access
Desktop
Libraries
This PC
Network
Name
Date modified
Type
Oracle_VM_VirtualBox_Extension_Pack-5.0.2...
10/28/2016 3:40 AM
VBOX-EXT
File name: Oracle_VM_VirtualBox_Extension_Pack-5.0.26
Files of type: All Files (*.*)
Open
Cancel

The file will be added to 'Protected Files'.



Protected Objects

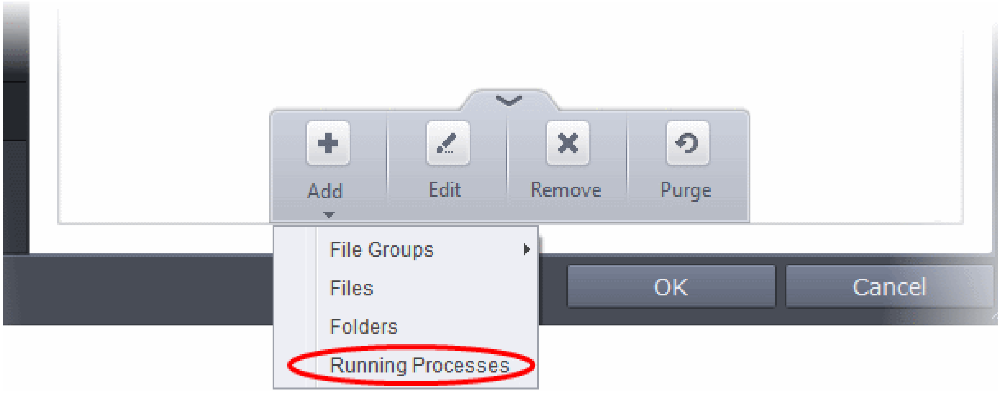
The following groups of objects are defined on this computer:

☐	Path
☐	⊞ Startup Folders
☐	⊞ Important Files/Folders
☐	⊞ Executables
☐	⊞ Windows Management
☐	⊞ 3rd Party Protocol Drivers
☐	⊞ Metro Apps
☐	⊞ COMODO Client Files/Folders
☐	⊞ COMODO Client - Communication
☐	⊞ COMODO Client - Security Manager
☐	E:\My Safe Programs*
☑	E:\Oracle_extension_pack\Oracle_VM_VirtualBox_Extension_Pack-5.0.26-10...

- Repeat the process to add more files. The items added to the Protected Files will be protected from access by other programs.

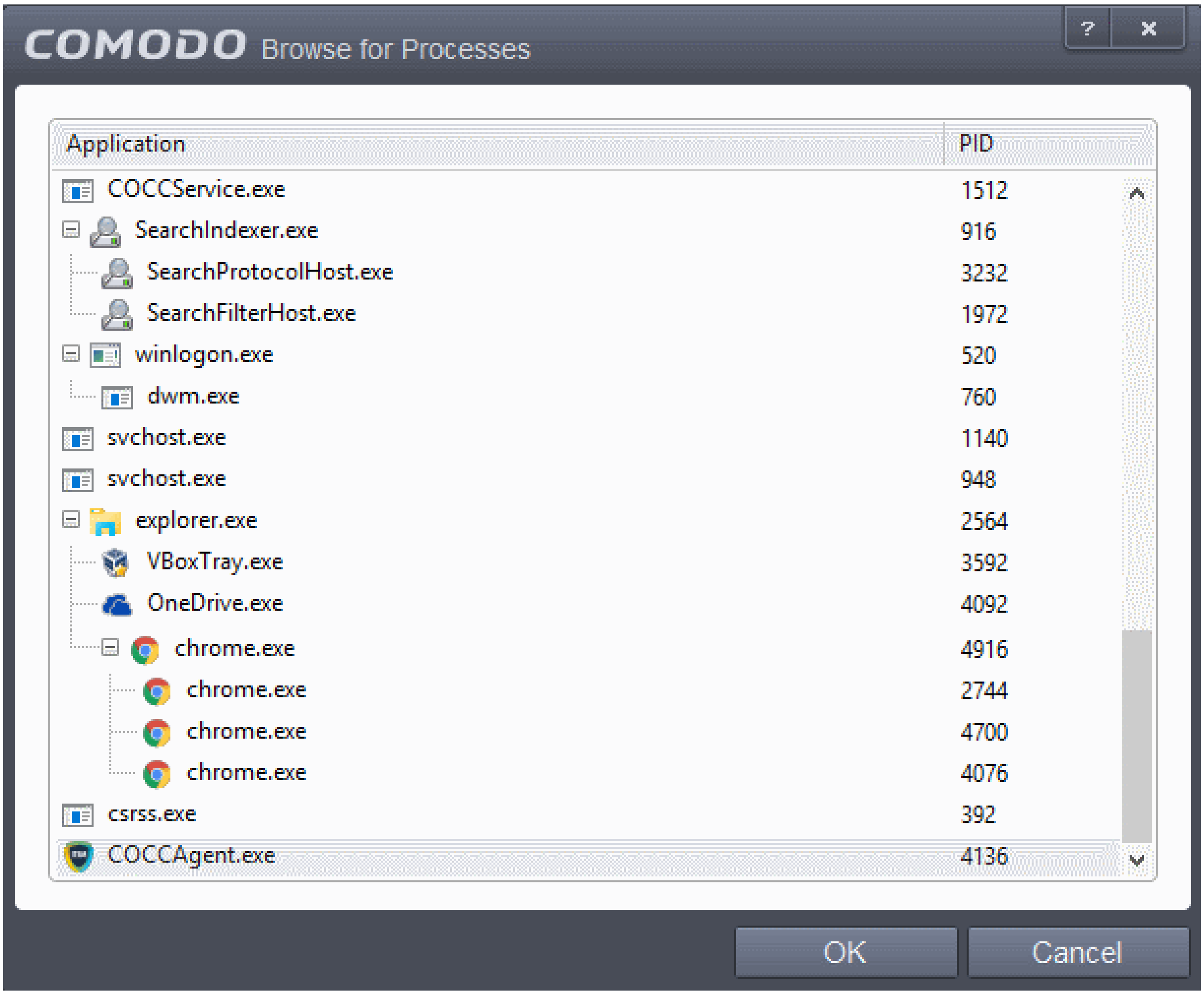
Adding an application from a running processes

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



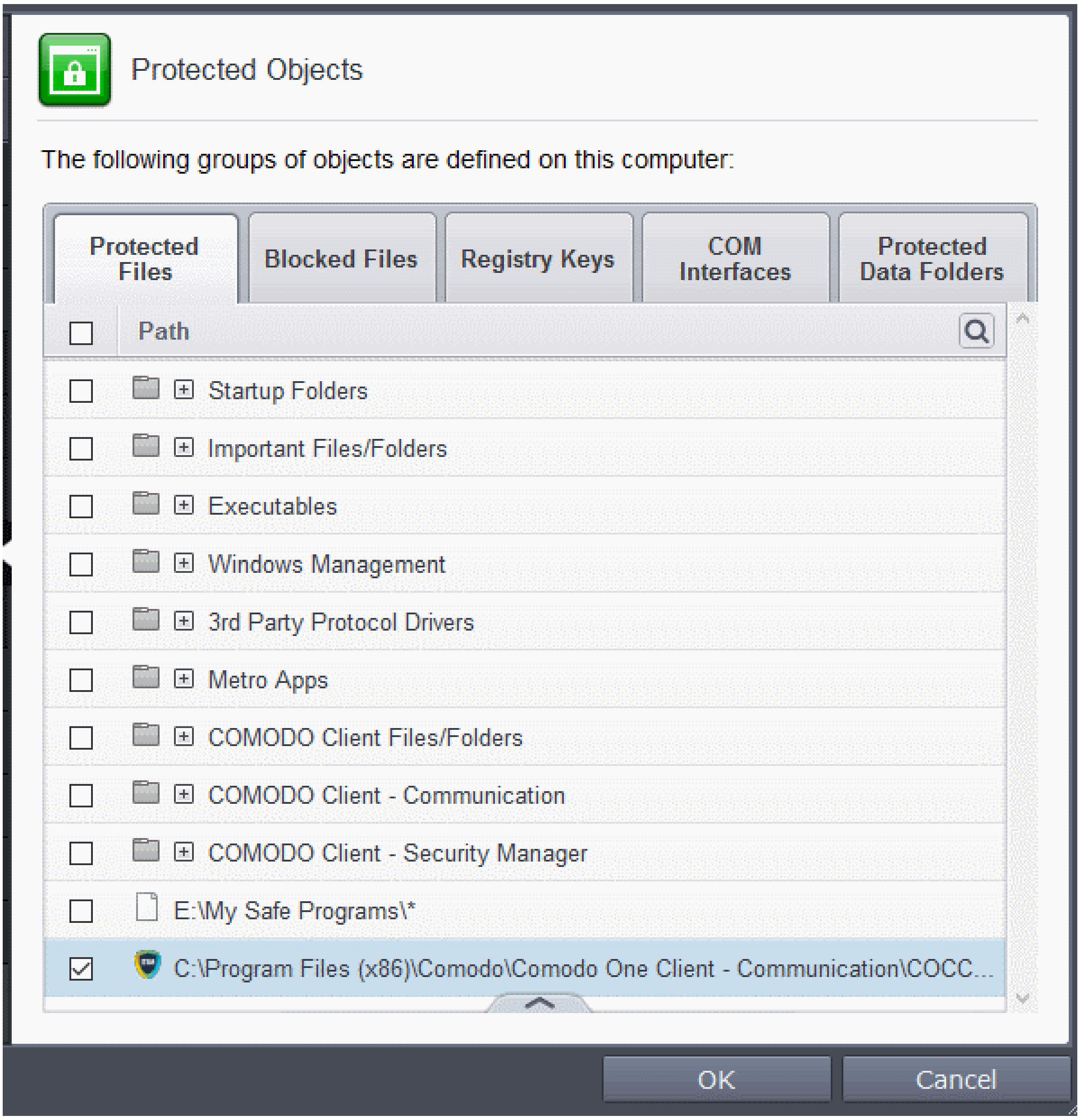
A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to Protected Files and click OK from the Browse for Process dialog.



Application	PID
COCCService.exe	1512
SearchIndexer.exe	916
SearchProtocolHost.exe	3232
SearchFilterHost.exe	1972
winlogon.exe	520
dwm.exe	760
svchost.exe	1140
svchost.exe	948
explorer.exe	2564
VBoxTray.exe	3592
OneDrive.exe	4092
chrome.exe	4916
chrome.exe	2744
chrome.exe	4700
chrome.exe	4076
csrss.exe	392
COCCAgent.exe	4136

The application will be added to 'Protected Files'.



Protected Objects

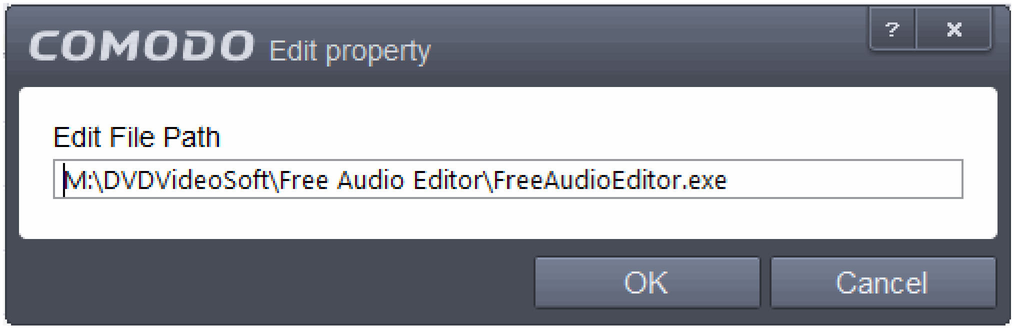
The following groups of objects are defined on this computer:

□	Path
□	⊞ Startup Folders
□	⊞ Important Files/Folders
□	⊞ Executables
□	⊞ Windows Management
□	⊞ 3rd Party Protocol Drivers
□	⊞ Metro Apps
□	⊞ COMODO Client Files/Folders
□	⊞ COMODO Client - Communication
□	⊞ COMODO Client - Security Manager
□	E:\My Safe Programs*
☑	C:\Program Files (x86)\Comodo\Comodo One Client - Communication\COCC...

- 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, click the up arrow from the bottom and select Edit. The 'Edit Property' dialog will appear.



COMODO Edit property

Edit File Path

M:\DVDVideoSoft\Free Audio Editor\FreeAudioEditor.exe

- Edit the file path, if you have relocated the file and click 'OK'

To delete an item from Protected Files list

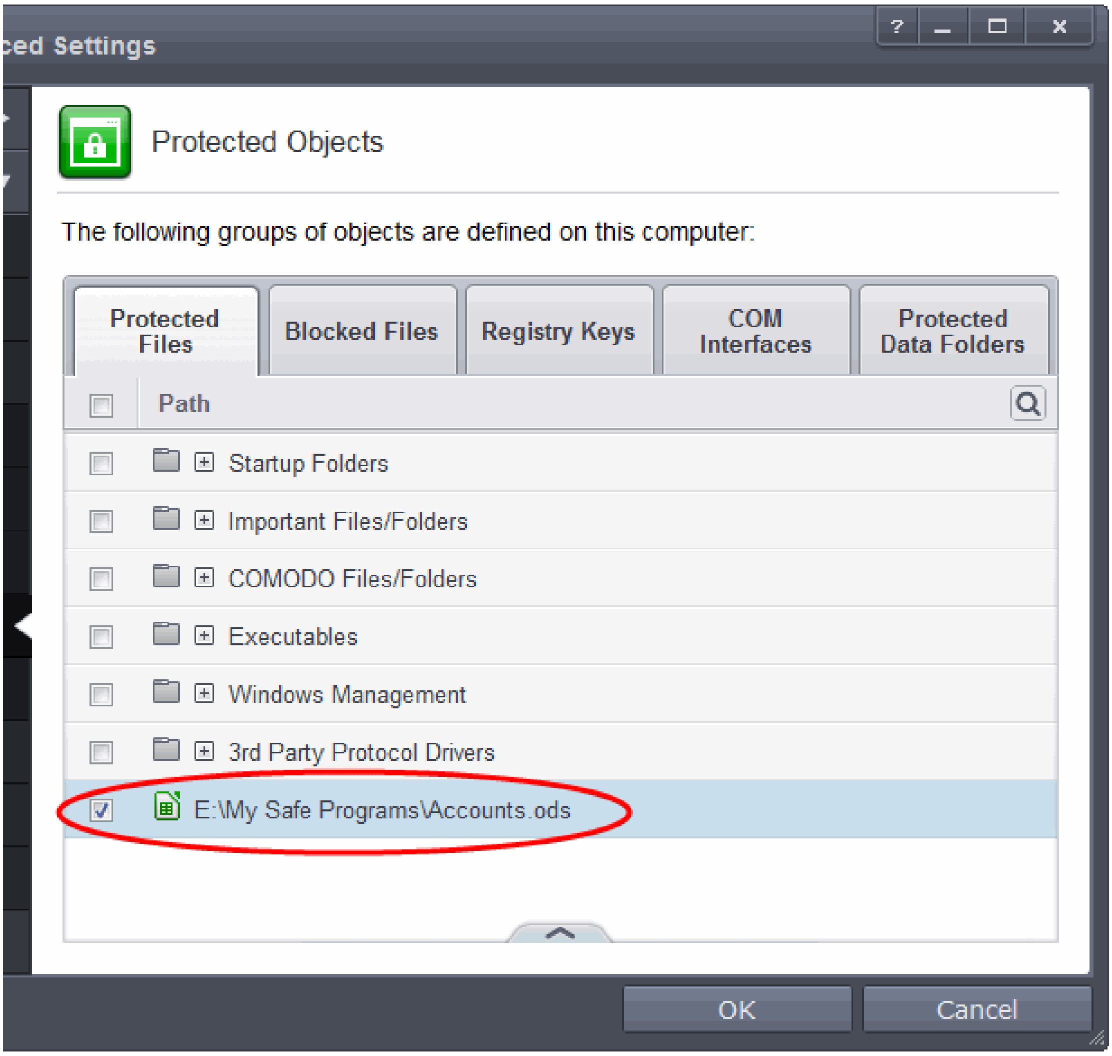
- Select the item from the list, click the up arrow from the bottom and select 'Remove'.

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.

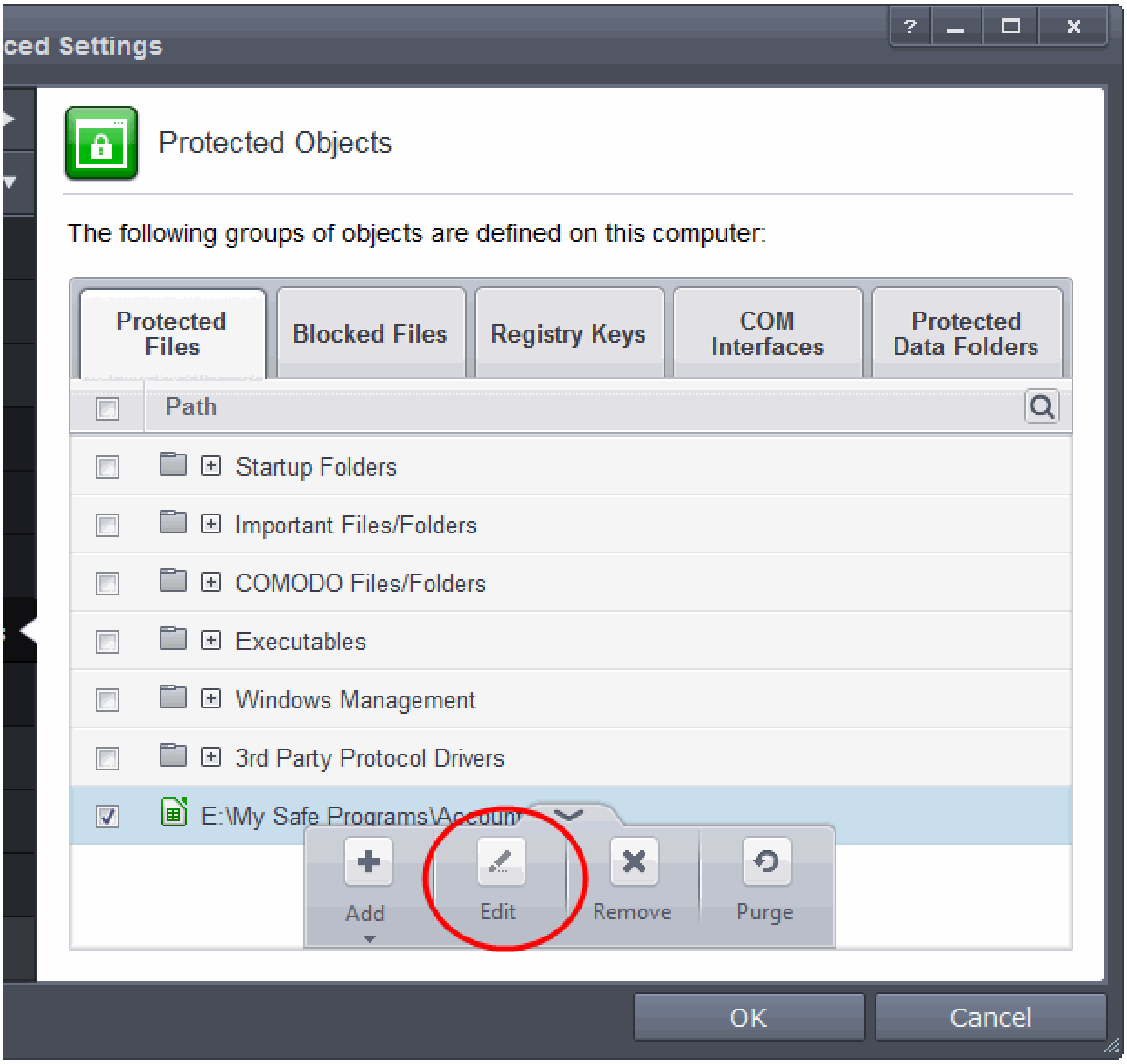
Exceptions

Users can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate Access Right in 'Active HIPS Rules' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the Open Office Calc 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 potential malicious program. You would first add the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into 'Active HIPS Rules' and create an exception for 'scalc' so that it alone could modify 'Accounts.ods'.

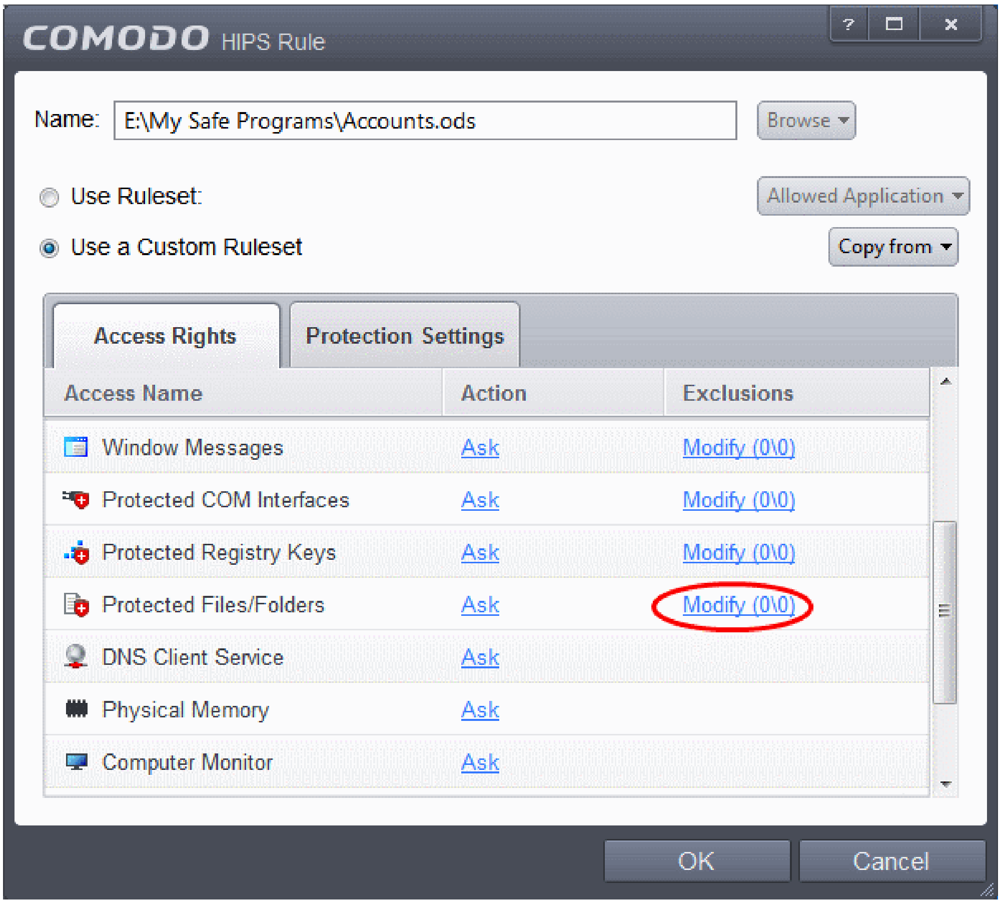
- First add 'Accounts.ods' to Protected Files area.



- Then go to HIPS Rules interface and add it to the list of applications (Click Add > select User Ruleset > Allowed Application > Browse and select the file).



- Select the file, click the up arrow and choose 'Edit'.
- In the HIPS Rule interface, select 'Use a custom ruleset'.



Name: E:\My Safe Programs\Accounts.ods

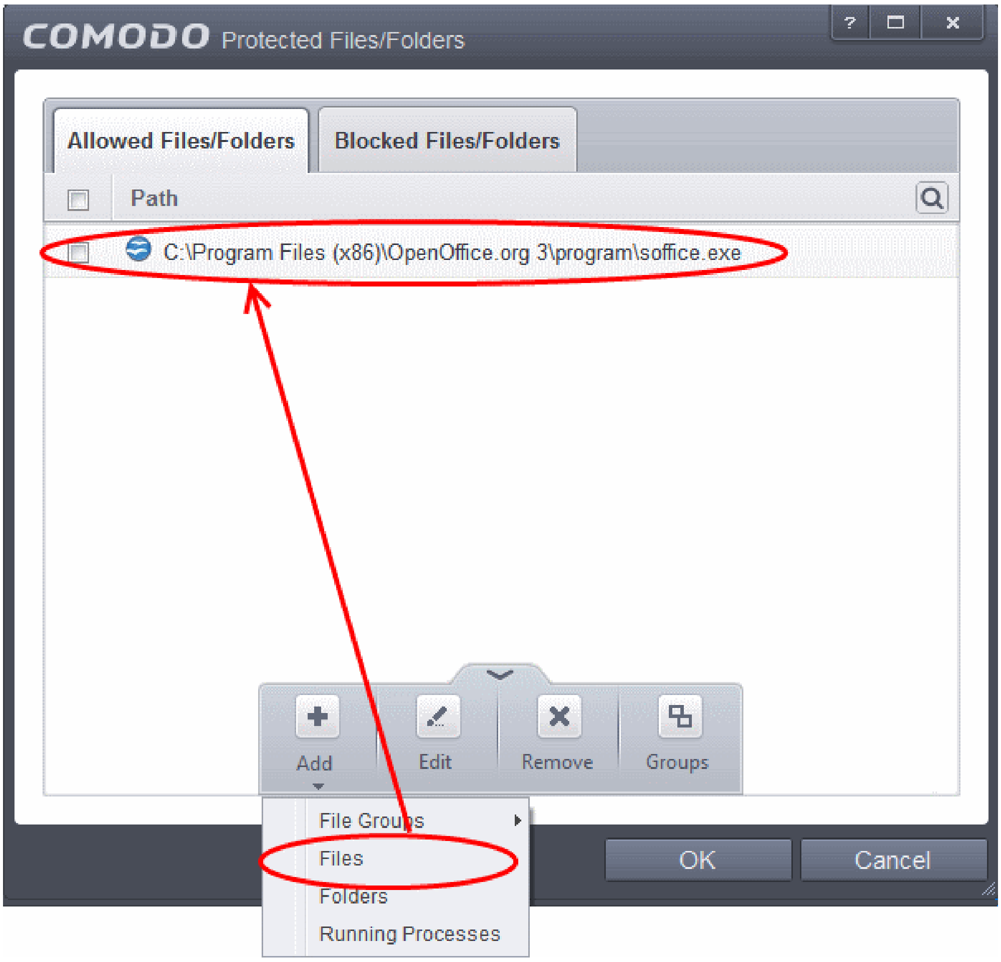
○ Use Ruleset:

● Use a Custom Ruleset

Access Rights | Protection Settings

Access Name	Action	Exclusions
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (0\0)
Protected Files/Folders	Ask	Modify (0\0)
DNS Client Service	Ask	
Physical Memory	Ask	
Computer Monitor	Ask	

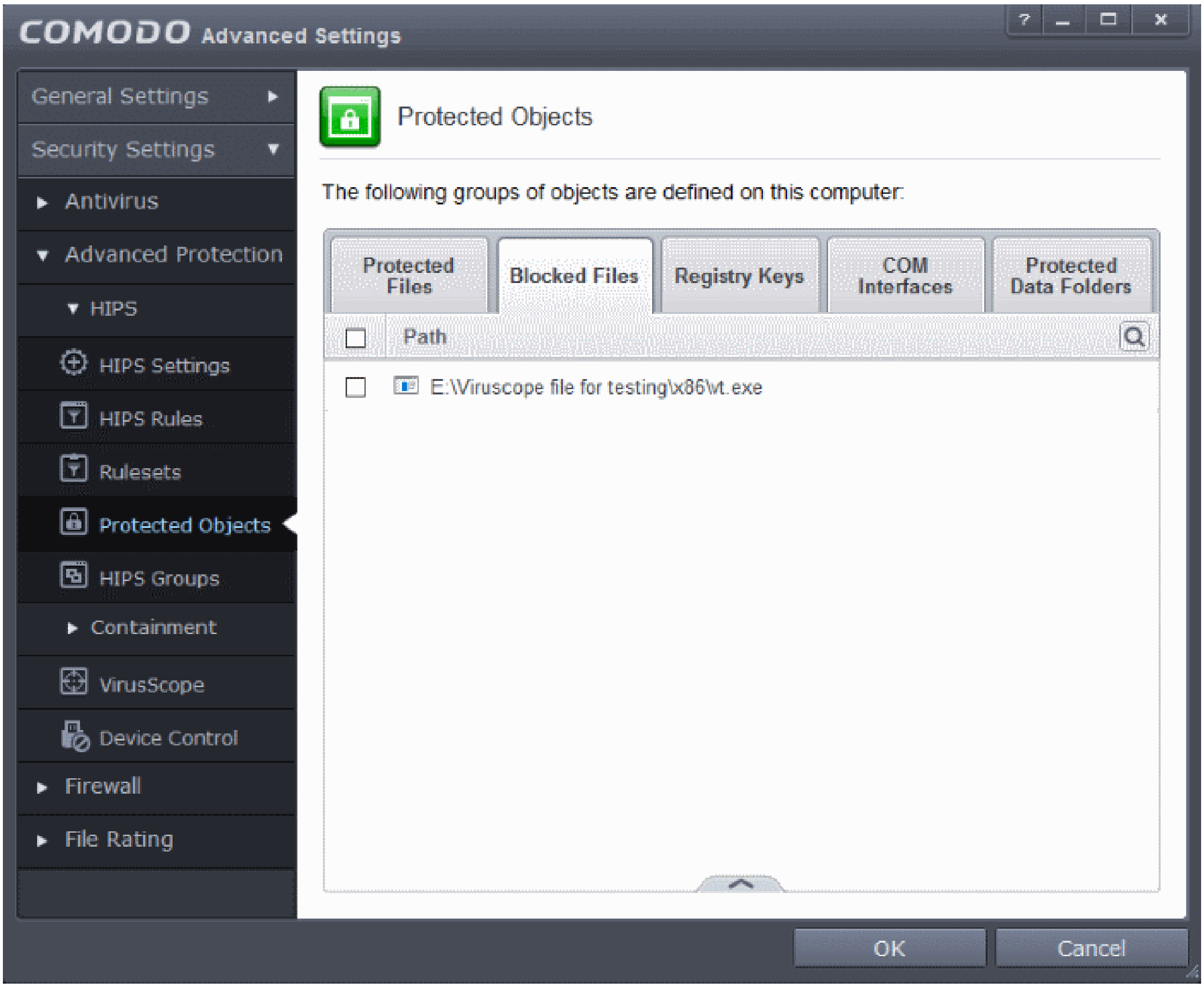
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the '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.

6.2.2.4.2. Blocked Files

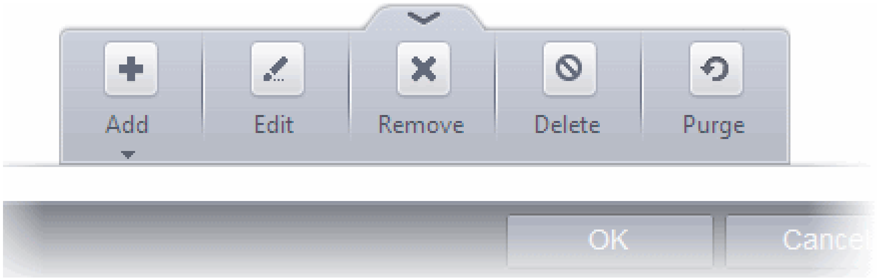
The 'Blocked Files' component of 'Protected Objects' allows you to lock-down files by all denying access rights to them from other processes or users. This effectively cuts them off from the rest of your system. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files that are placed in 'Protected Files', users cannot selectively allow any process access to a blocked file.



The following groups of objects are defined on this computer:

□ E:\Viruscope file for testing\x86\wt.exe

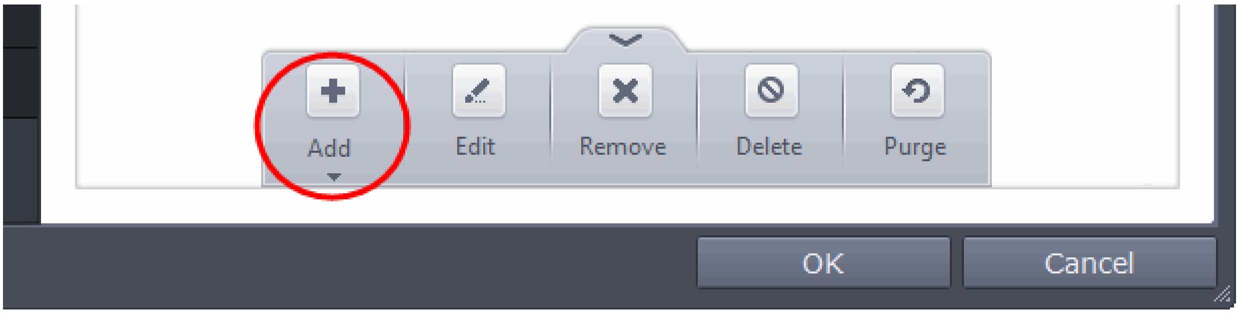
Clicking the handle at the bottom of the interface opens an options panel:



- Add - Allows you to add individual files, programs, applications to Blocked Files.
- Edit - Allows you to edit the path of the file.
- Remove - Releases the currently highlighted file from the blocked files list.
- Delete - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

To manually add an individual file or application

- Click the handle from the bottom and select 'Add'.

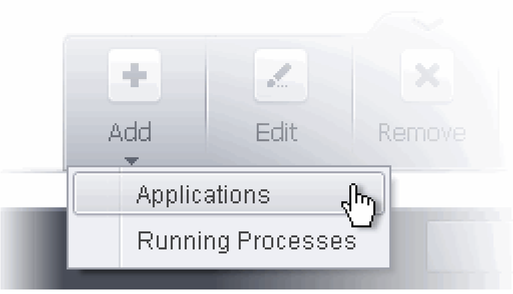


You can add the files by following methods:

- Selecting a File
- Selecting from currently running Processes

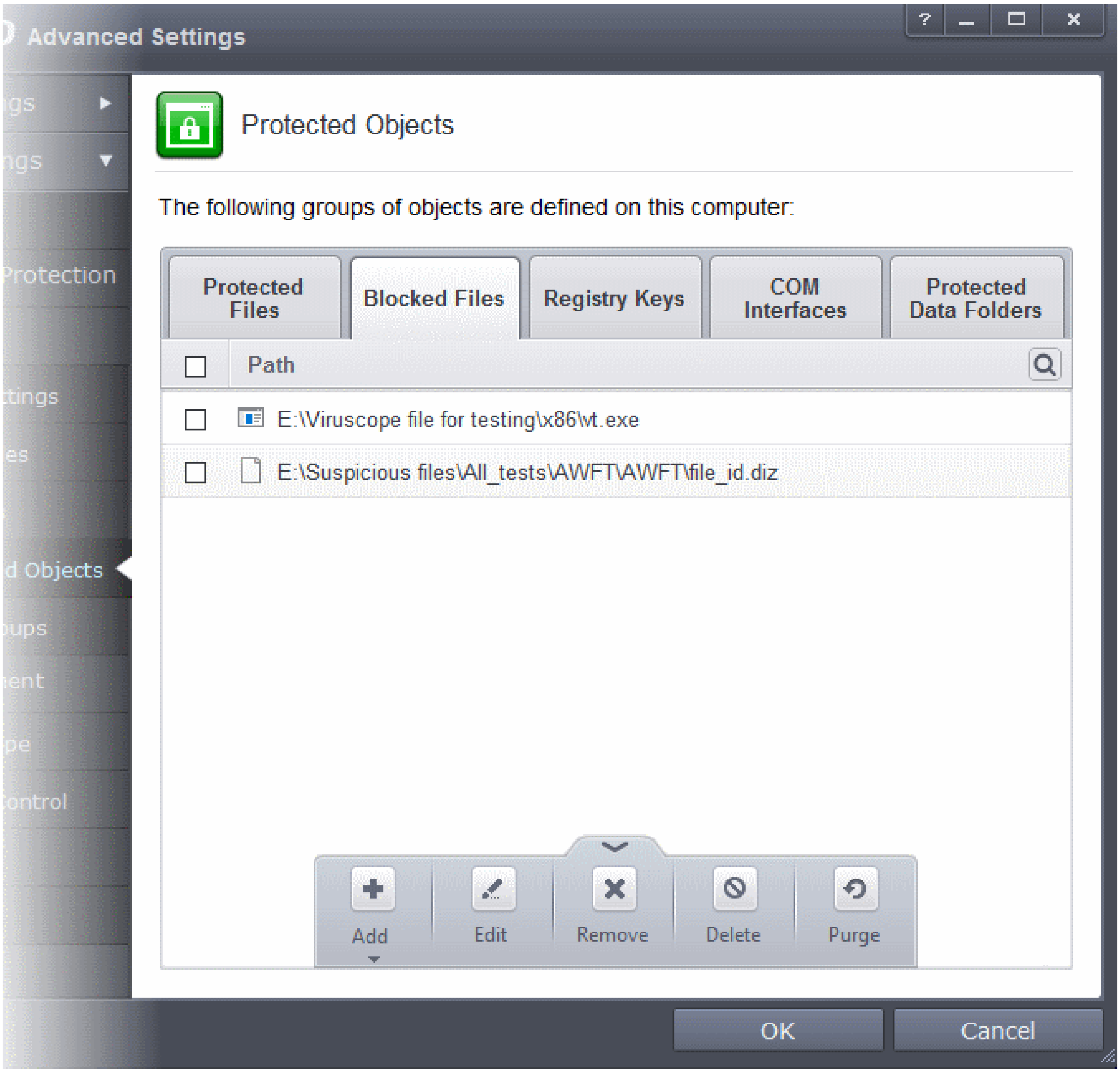
Adding a File

- Choose 'Applications' from the 'Add' drop-down.



- Navigate to the file you want to add to Blocked Files in the 'Open' dialog and click 'Open'

The file will be added to 'Blocked Files'.

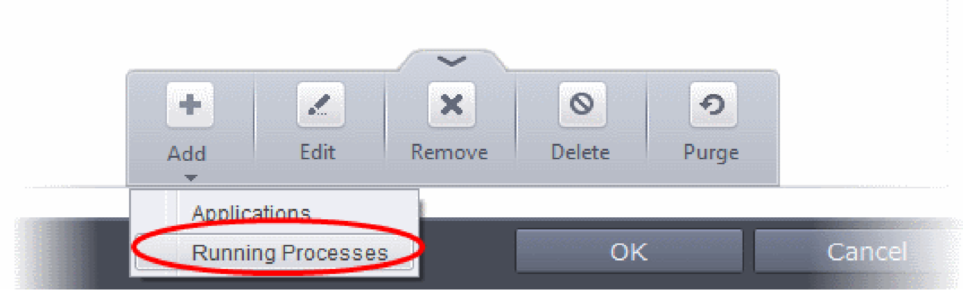


☐	Path
☐	E:\Viruscope file for testing\x86\vt.exe
☐	E:\Suspicious files\All_tests\AWFT\AWFT\file_id.diz

- Repeat the process to add more files.

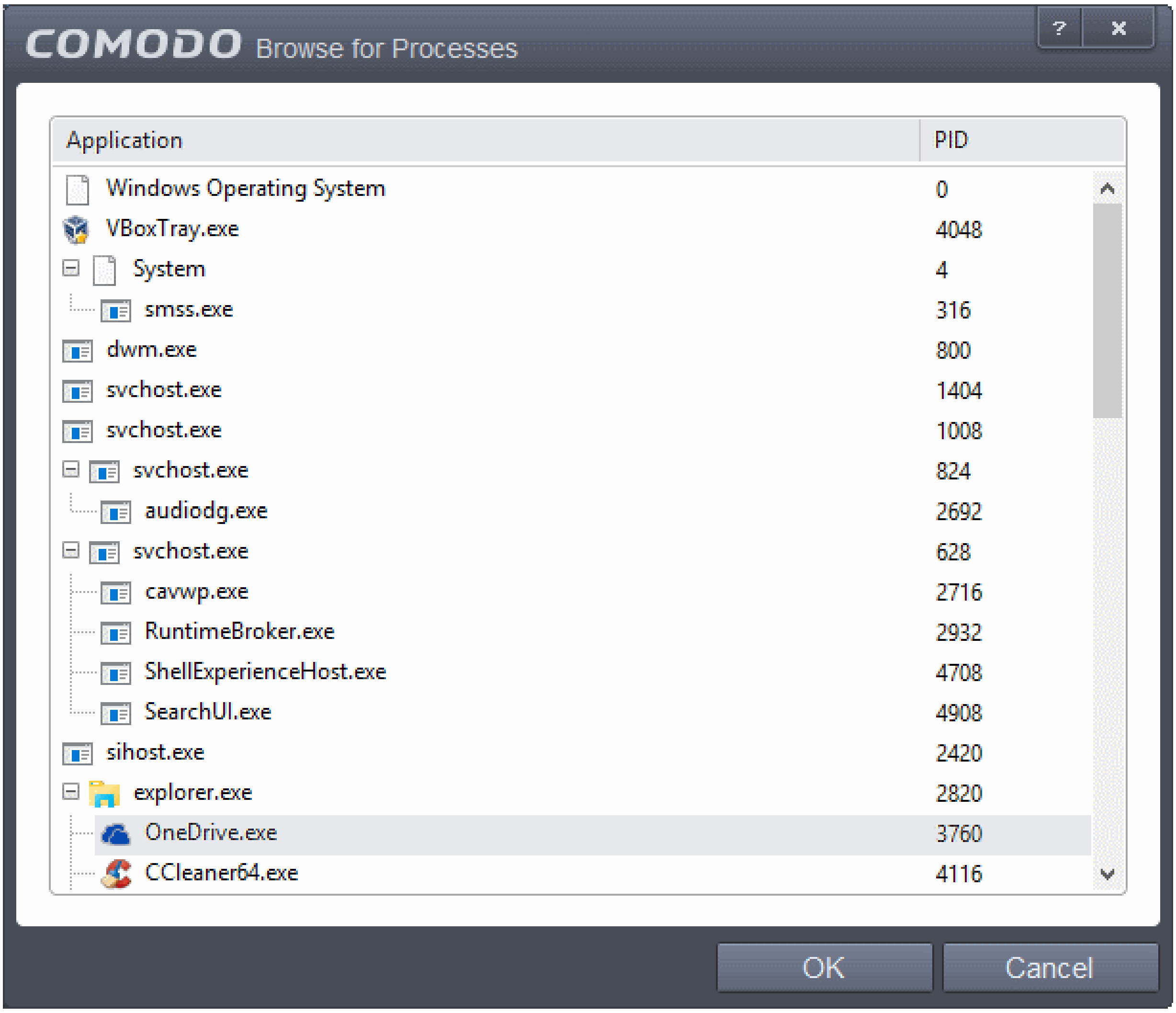
Adding an application from a running processes

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



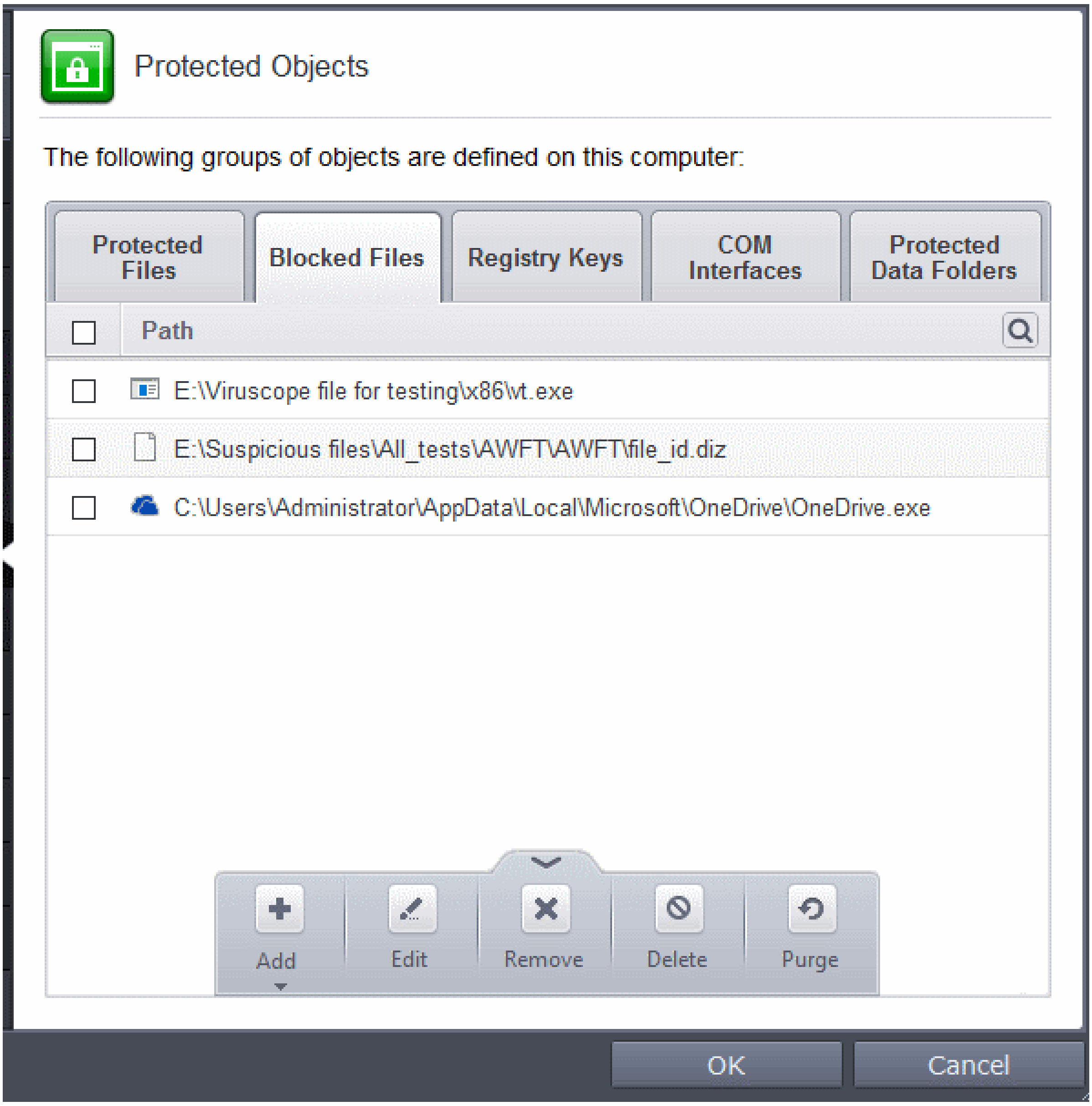
A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to Blocked Files and click OK from the Browse for Process dialog.



Application	PID
Windows Operating System	0
VBoxTray.exe	4048
System	4
smss.exe	316
dwm.exe	800
svchost.exe	1404
svchost.exe	1008
svchost.exe	824
audiodg.exe	2692
svchost.exe	628
cavwp.exe	2716
RuntimeBroker.exe	2932
ShellExperienceHost.exe	4708
SearchUI.exe	4908
sihost.exe	2420
explorer.exe	2820
OneDrive.exe	3760
CCleaner64.exe	4116

The application will be added to 'Blocked Files'.



Protected Objects

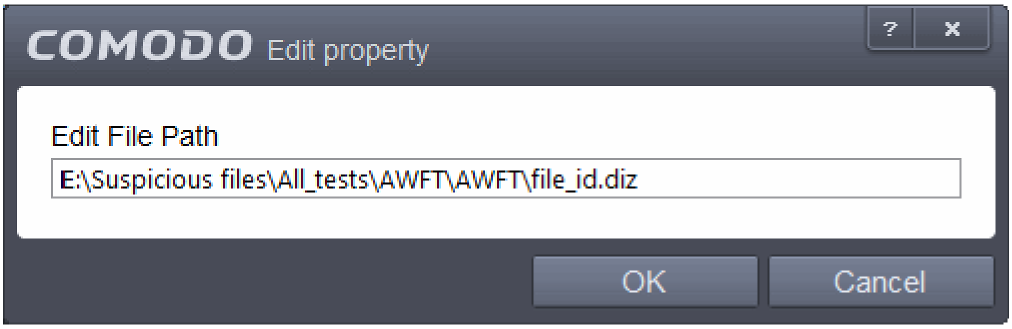
The following groups of objects are defined on this computer:

□	Path
□	E:\Viruscope file for testing\x86\wt.exe
□	E:\Suspicious files\All_tests\AWFT\AWFT\file_id.diz
□	C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe

- Repeat the process to add more files.

To edit an item in the Blocked Files list

- Select the item from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



Edit File Path

E:\Suspicious files\All_tests\AWFT\AWFT\file_id.diz

- 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, click the handle from the bottom and select 'Remove'.

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, click the up arrow from the bottom and select 'Delete'.

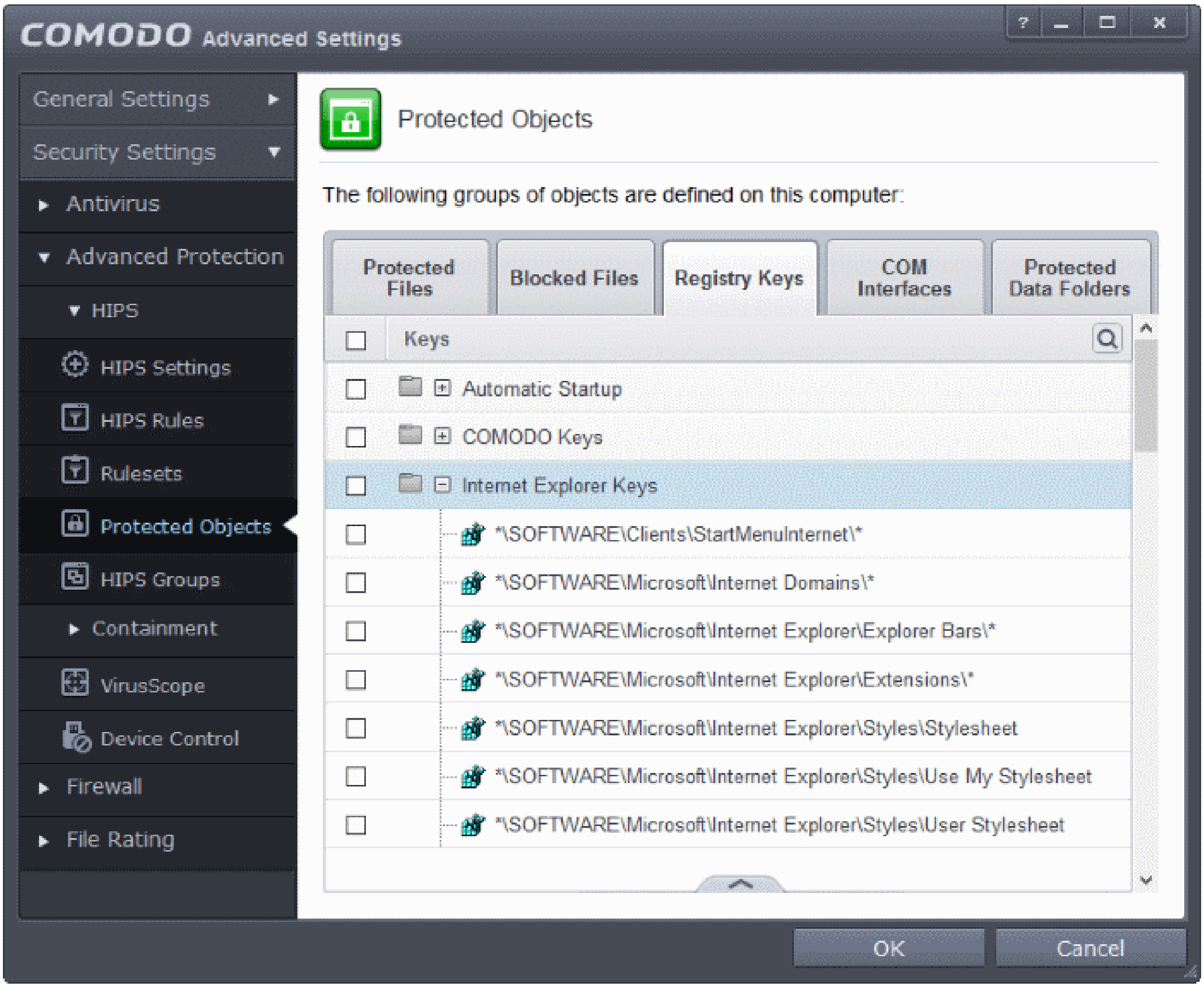
The selected item will be deleted from your computer immediately.

Warning: Deleting a file from from the Blocked Files interface will permanently delete the file from your system. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

6.2.2.4.3. Protected Registry Keys

The 'Registry Protection' panel allows you to protect system critical registry keys against modification. It is essential that registry keys are protected against attack because irreversible damage can be caused if important keys are corrupted or modified. CCS protects important registry keys by default. This interface allows you to add and remove keys from protection.

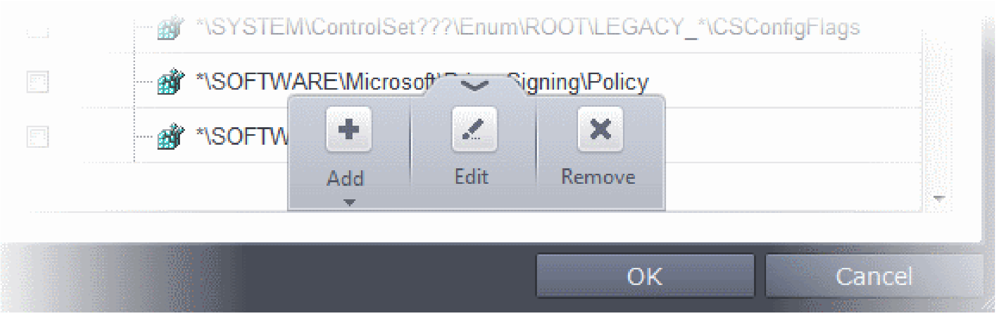
Click the 'Registry Keys' tab in the Protected Objects interface.



The following groups of objects are defined on this computer:

- □ ⊞ Automatic Startup
- □ ⊞ COMODO Keys
- □ ⊟ Internet Explorer Keys
  - □ *\SOFTWARE\Clients\StartMenuInternet\*
  - □ *\SOFTWARE\Microsoft\Internet Domains*
  - □ *\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars*
  - □ *\SOFTWARE\Microsoft\Internet Explorer\Extensions\*
  - □ *\SOFTWARE\Microsoft\Internet Explorer\Styles\Stylesheet
  - □ *\SOFTWARE\Microsoft\Internet Explorer\Styles\Use My Stylesheet
  - □ *\SOFTWARE\Microsoft\Internet Explorer\Styles\User Stylesheet

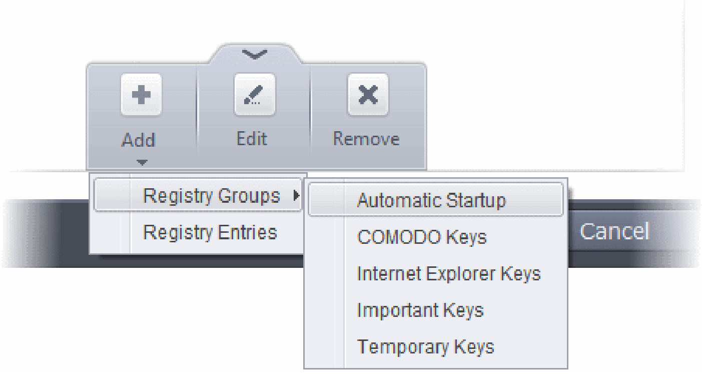
Clicking the handle at the bottom of the interface opens an options panel:


*\SYSTEM\ControlSet???\Enum\ROOT\LEGACY_*\CSConfigFlags
*\SOFTWARE\Microsoft\...Signing\Policy
*\SOFTW
Add
Edit
Remove
OK
Cancel

- Add - Allows you to add Registry groups or individual registry keys/entries to Registry Protection list.
- Edit - Allows you to edit the path of the Registry group or individual registry keys/entries of the selected item in the Registry Protection interface.
- Remove - Deletes the currently highlighted Registry group or individual registry key from the Registry Protection list.

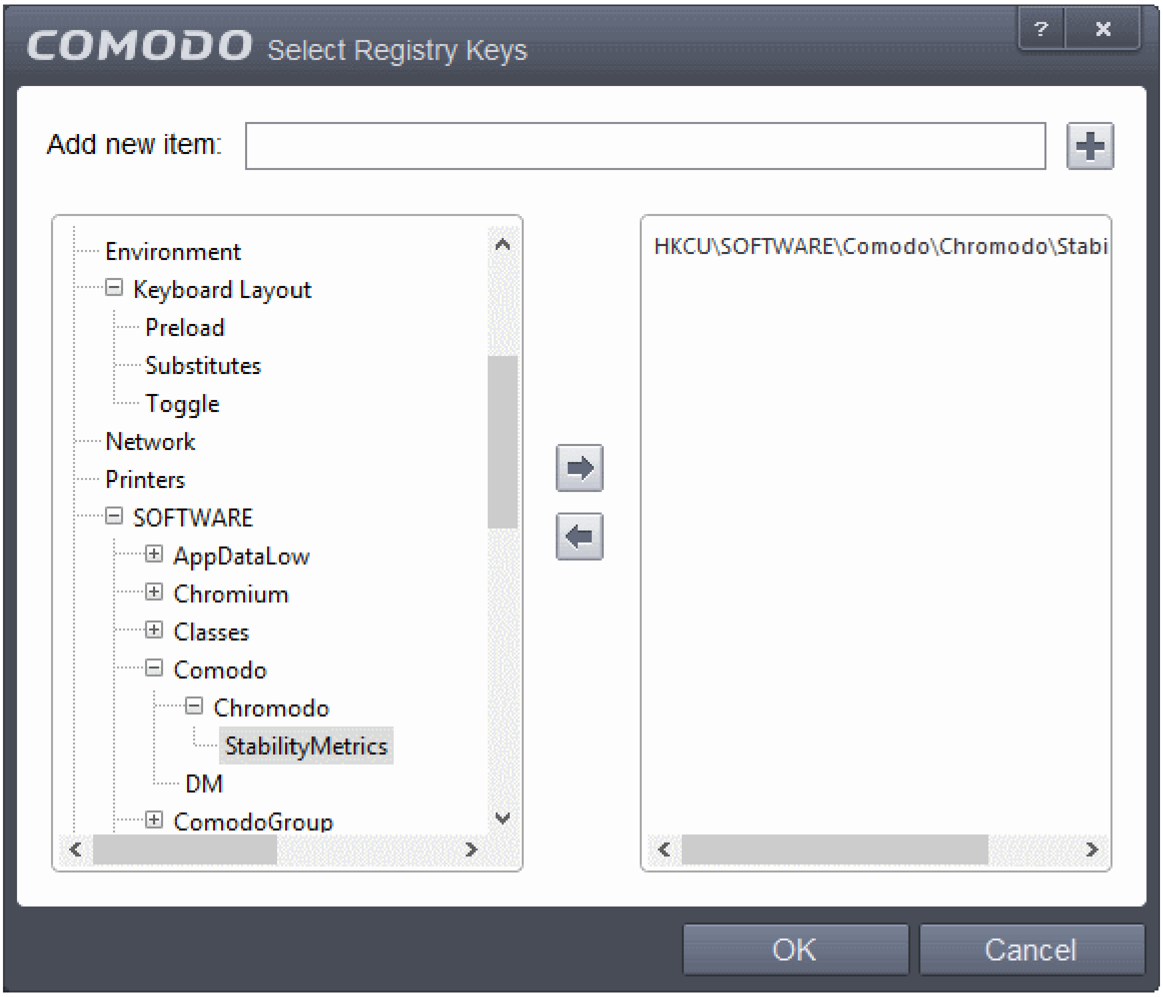
To manually add an individual Registry key or Registry Group

- Click the handle from the bottom and select 'Add'.



You can add the items by following methods:

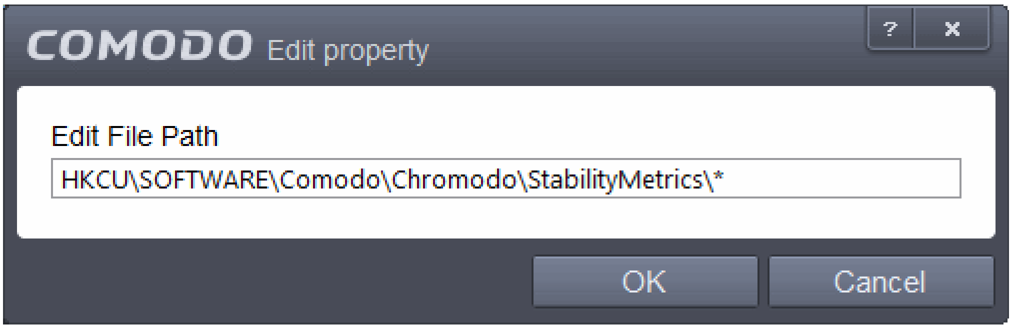
- **Adding Registry Groups** - Selecting Registry Groups allows you to batch select and import predefined groups of important registry keys. Comodo Client Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'. For explanations on editing existing registry groups and creating new groups refer to Registry Groups in HIPS Groups section.
- **Adding individual Registry Keys** - Selecting 'Registry Entries' opens the 'Select Registry Keys'.



You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the Registry Protection list

- Select the key from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



Edit File Path

HKCU\SOFTWARE\Comodo\Chromodo\StabilityMetrics\*

- Edit the key path, if you have relocated the file and click OK.

Note: The Registry Groups cannot be edited from this interface. You can edit Registry Groups from the Manage Registry Groups interface. Refer to Registry Groups in HIPS Groups section.

To delete an item from Registry Protection list

- Select the item from the list, click the up arrow from the bottom and select 'Remove'.

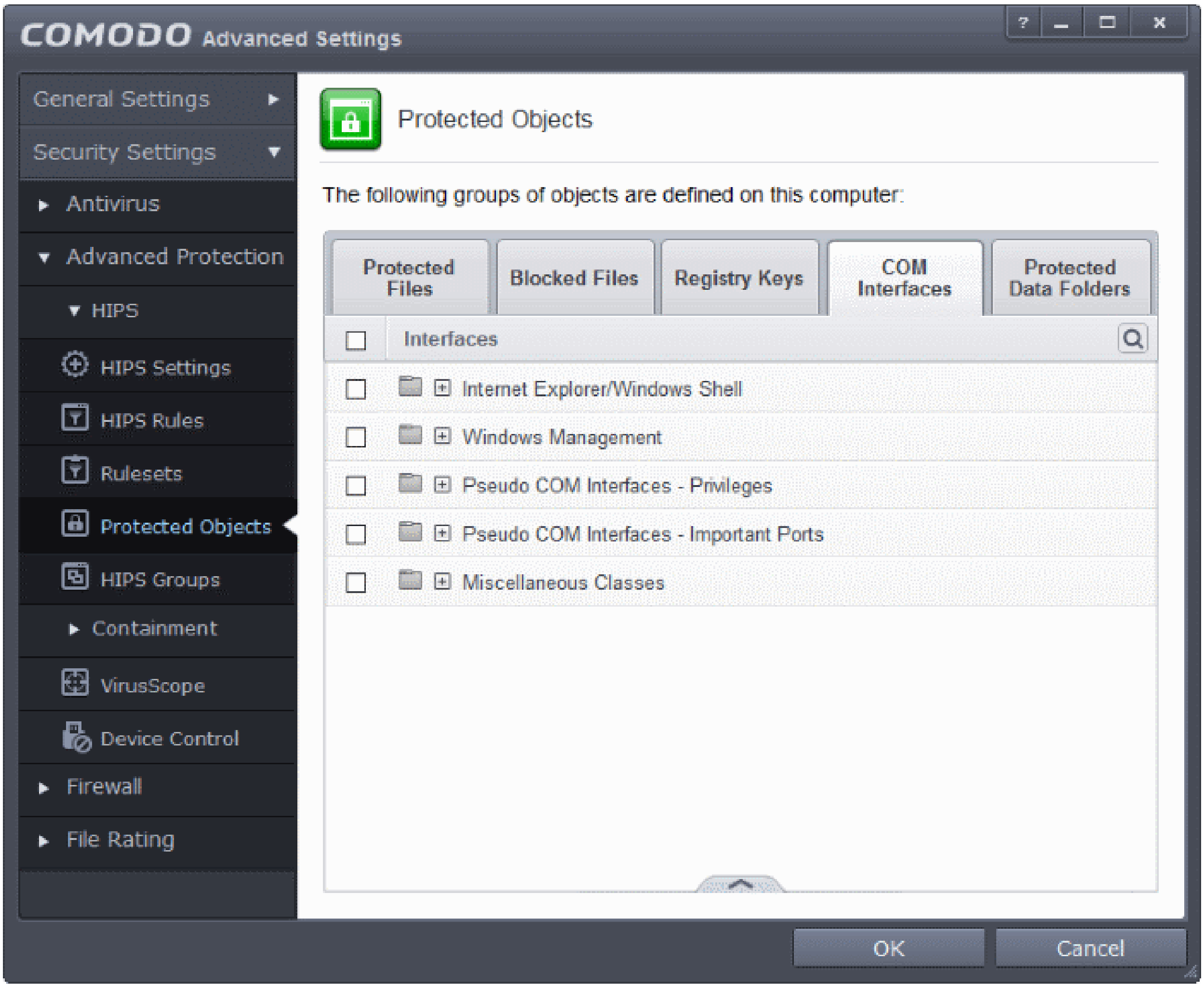
The selected item will be deleted from the Registry Protection list. CCS will not generate alerts, if the key or the group is modified by other programs.

6.2.2.4.4. Protected COM interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malware to launch attacks on your computer. It is a critical part of any security system to restrict processes from accessing the Component Object Model - in other words, to protect the COM interfaces.

Comodo Client Security automatically protects COM interfaces against against modification, corruption and manipulation by malicious processes. The predefined COM Interface groups can be accessed by clicking the HIPS Groups tab.

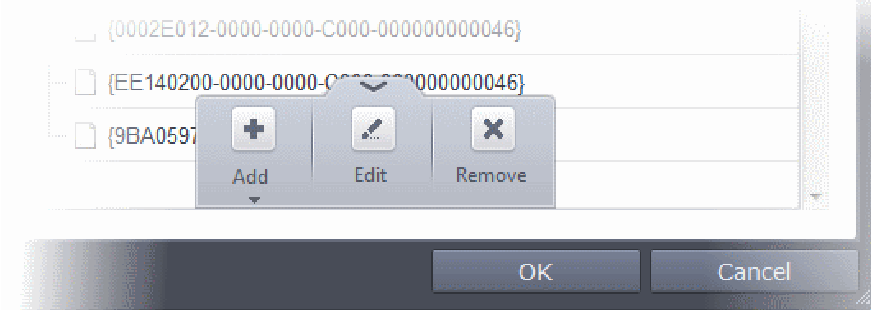
The 'COM Protection' panel allows you to view the list of predefined COM Interface groups protected by CCS, edit them and to add new COM interface components to the list. This screen can be accessed by clicking the 'COM Interfaces' tab in the Protected Objects interface.



The following groups of objects are defined on this computer:

□ Interfaces
- □ ⊞ Internet Explorer/Windows Shell
- □ ⊞ Windows Management
- □ ⊞ Pseudo COM Interfaces - Privileges
- □ ⊞ Pseudo COM Interfaces - Important Ports
- □ ⊞ Miscellaneous Classes

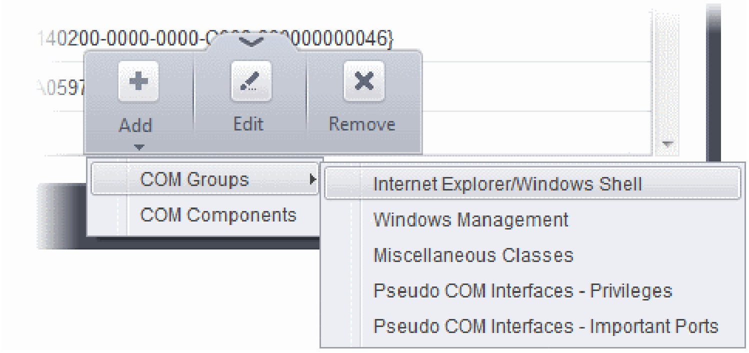
Clicking the handle at the bottom of the interface opens an options panel:


{0002E012-0000-0000-C000-000000000046}
{EE140200-0000-0000-C000-000000000046}
{9BA0597
Add
Edit
Remove
OK
Cancel

- Add - Allows you to add COM groups or individual COM components to COM Protection list.
- Edit - Allows you to edit the COM Class.
- Remove - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.

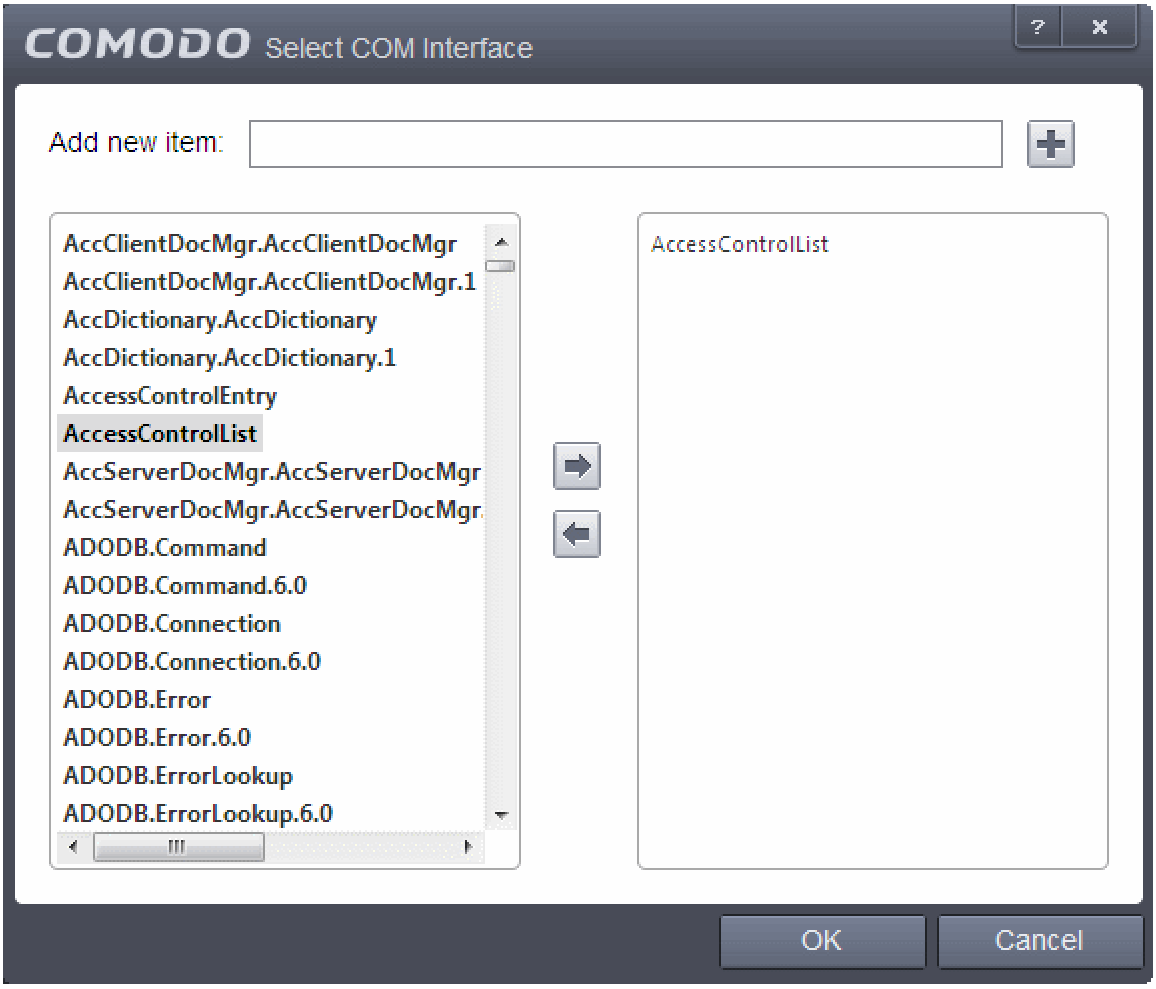
To manually add a COM Group or individual COM component

- Click the handle from the bottom and select 'Add'.


Add
Edit
Remove
COM Groups
COM Components
Internet Explorer/Windows Shell
Windows Management
Miscellaneous Classes
Pseudo COM Interfaces - Privileges
Pseudo COM Interfaces - Important Ports

You can add the items by following methods:

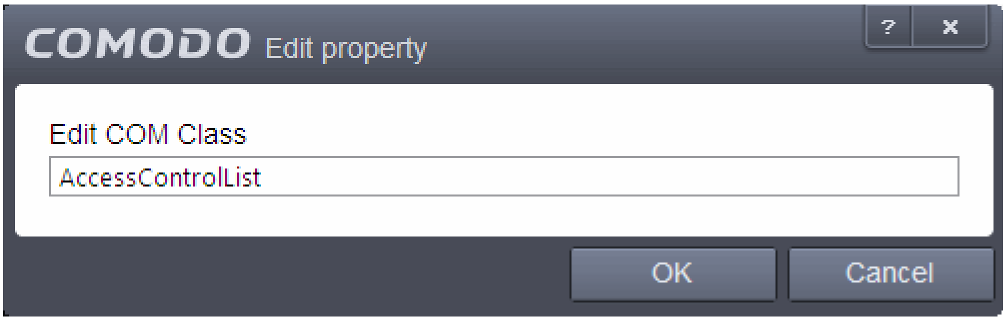
- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section COM Groups.
- **Adding COM Components** - Selecting 'COM components' opens the 'Select COM Interfaces' dialog.


COMODO Select COM Interface
Add new item:
AccClientDocMgr.AccClientDocMgr
AccClientDocMgr.AccClientDocMgr.1
AccDictionary.AccDictionary
AccDictionary.AccDictionary.1
AccessControlEntry
AccessControlList
AccServerDocMgr.AccServerDocMgr
AccServerDocMgr.AccServerDocMgr.
ADODB.Command
ADODB.Command.6.0
ADODB.Connection
ADODB.Connection.6.0
ADODB.Error
ADODB.Error.6.0
ADODB.ErrorLookup
ADODB.ErrorLookup.6.0
AccessControlList
OK
Cancel

You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the COM Protection

- Select the COM component from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



Edit COM Class: AccessControlList

- Edit the COM Class and click 'OK'

Note: The COM Groups cannot be edited from this interface. You can edit COM Groups from the Manage COM Groups interface. Refer to the section COM Groups for more details.

To delete an item from COM Protection list

- Select the item from the list, click the handle from the bottom and select 'Remove'.

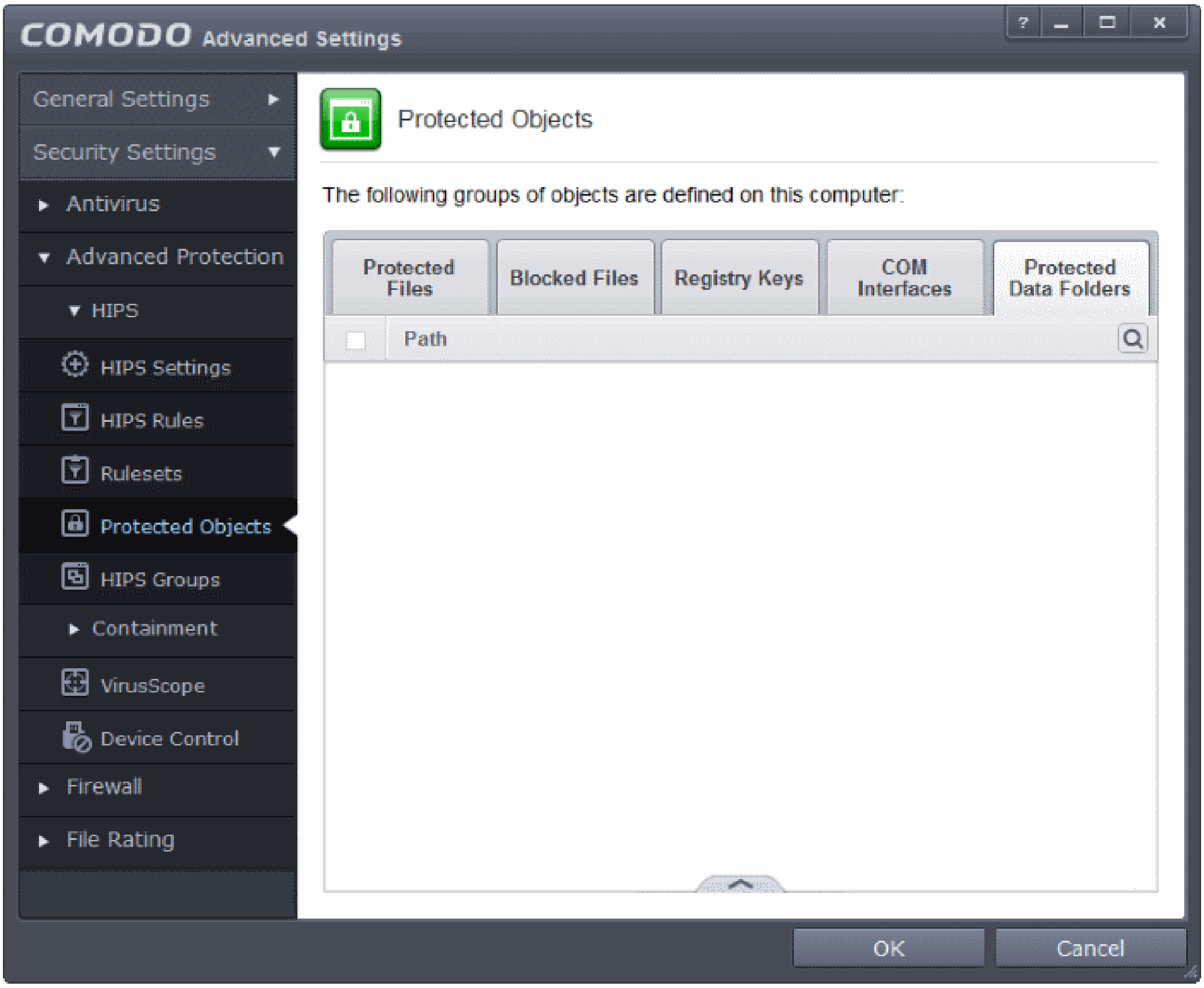
The selected item will be deleted from the COM Protection list. CCS will not generate alerts, if the COM component or the group is modified by other programs or processes.

6.2.2.4.5. Protected Data Folders

The contents of folders listed in the 'Protected Data Folders' area cannot be seen, accessed or modified by any known or unknown application that is running inside the Comodo Container.

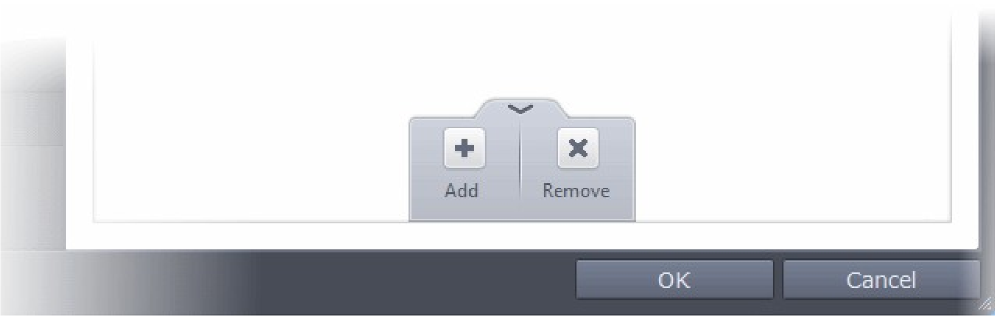
Tip: Files and folders that are added to 'Protected Files' interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to contained programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all contained programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

To open the 'Protected Data Folders' interface, click the 'Protected Data Folders' tab in the Protected Objects interface:



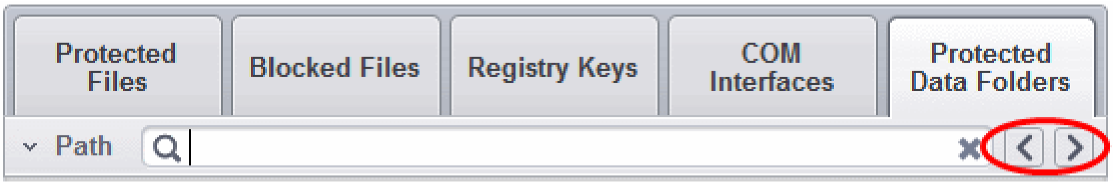
The following groups of objects are defined on this computer:

Clicking the handle at the bottom of the interface opens an options panel:



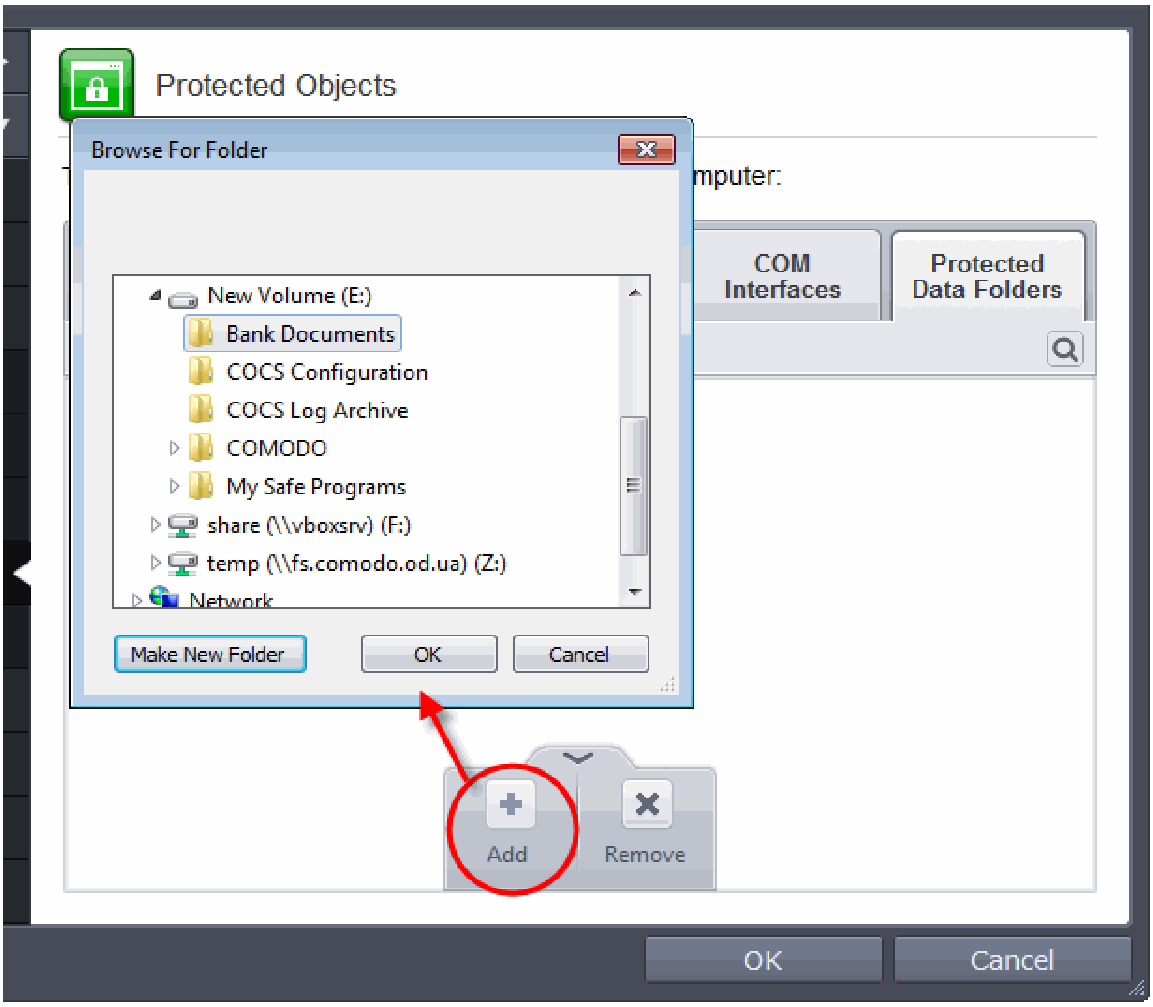
- Add - Allows you to add folders to Protected Data Folders list.
- Remove - Deletes the currently selected folder.

You can use the search option to find a specific folder by clicking the search icon 🔍 at the far right of the column header. You can search by entering the folder name in full or part. You can navigate through the successive results by clicking the left and right arrows.

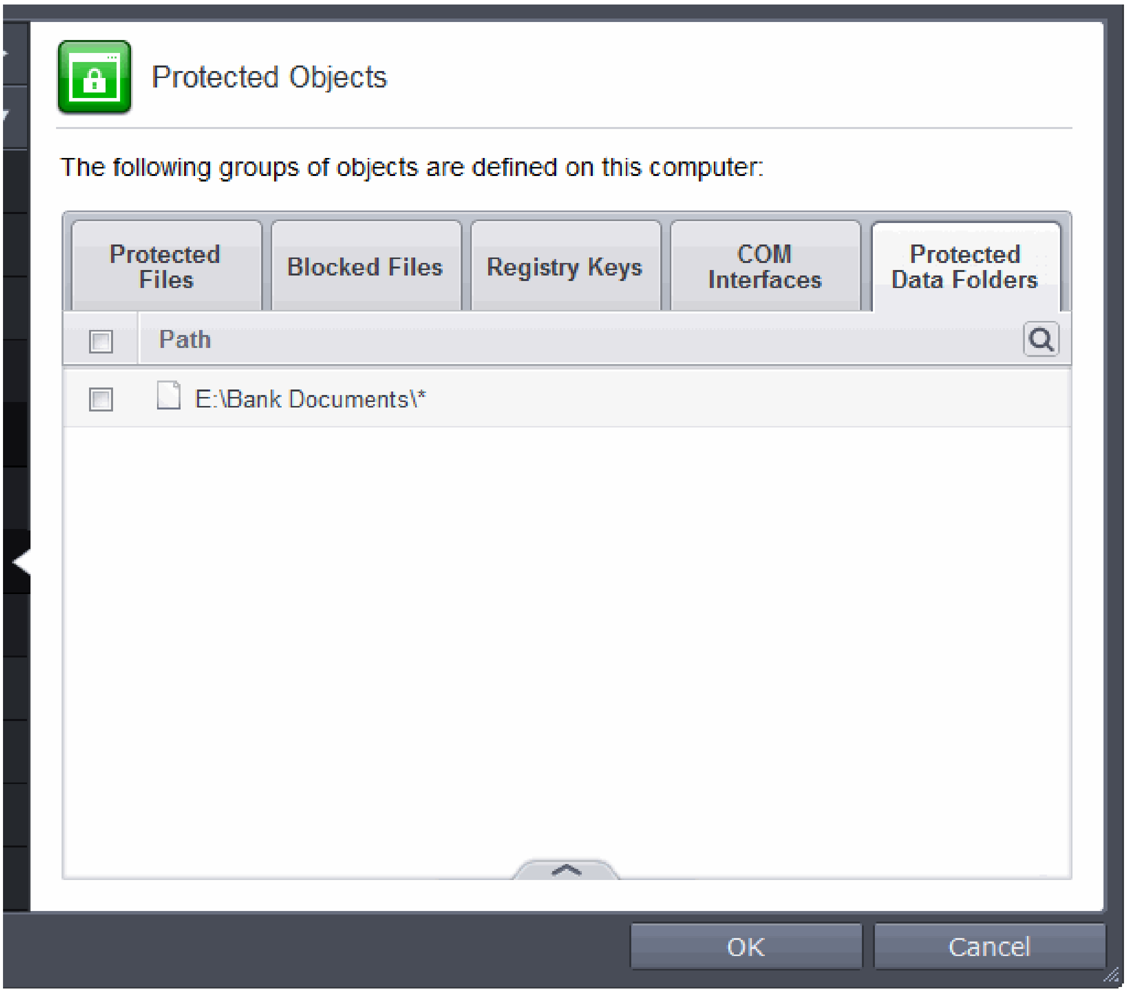


To add a folder to be protected

- Click the handle from the bottom and select 'Add'.



- Navigate to the folder to be added and click 'OK'.



Protected Objects

The following groups of objects are defined on this computer:

□ E:\Bank Documents*

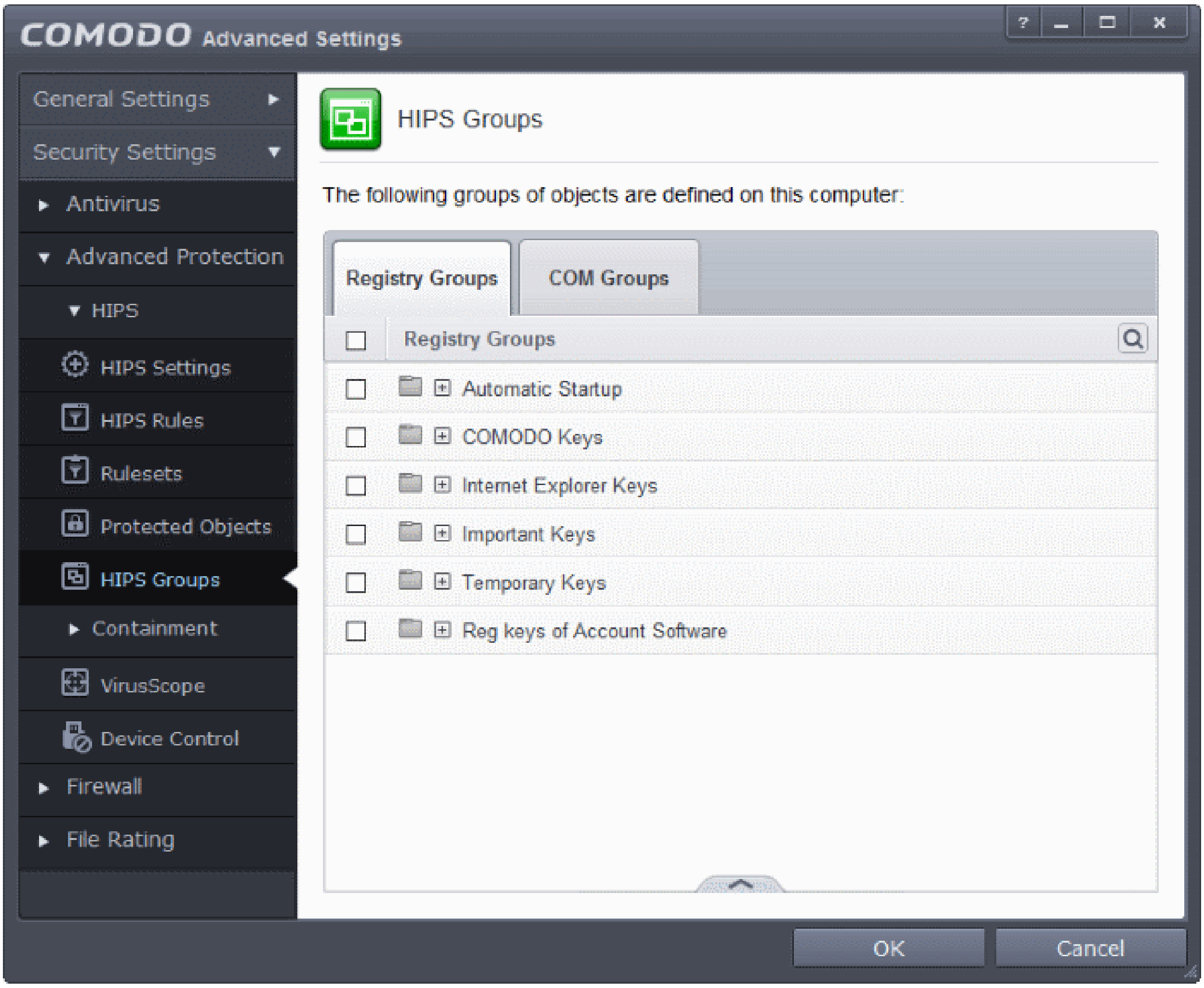
To remove an item from Protected Data Folders list

- Select the folder from the list, click the handle from the bottom and choose 'Remove'.
- The selected folder will be removed from the protected folders list. CCS will not generate alerts, if the folder is subjected to unauthorized access.

6.2.2.5. HIPS Groups

The HIPS Groups panel allows you to add, edit or remove predefined Registry and COM Groups. CCS ships with some important predefined Registry and COM Groups and this interface allows you to add new groups. New groups will also become available for selection in the Registry Keys and COM Interfaces for protection.

The 'HIPS Groups' panel can be accessed by clicking Security Settings > Advanced Protection > HIPS > HIPS Groups from the Advanced Settings interface.



The following groups of objects are defined on this computer:

Registry Groups
Automatic Startup
COMODO Keys
Internet Explorer Keys
Important Keys
Temporary Keys
Reg keys of Account Software

The panel has two tabs:

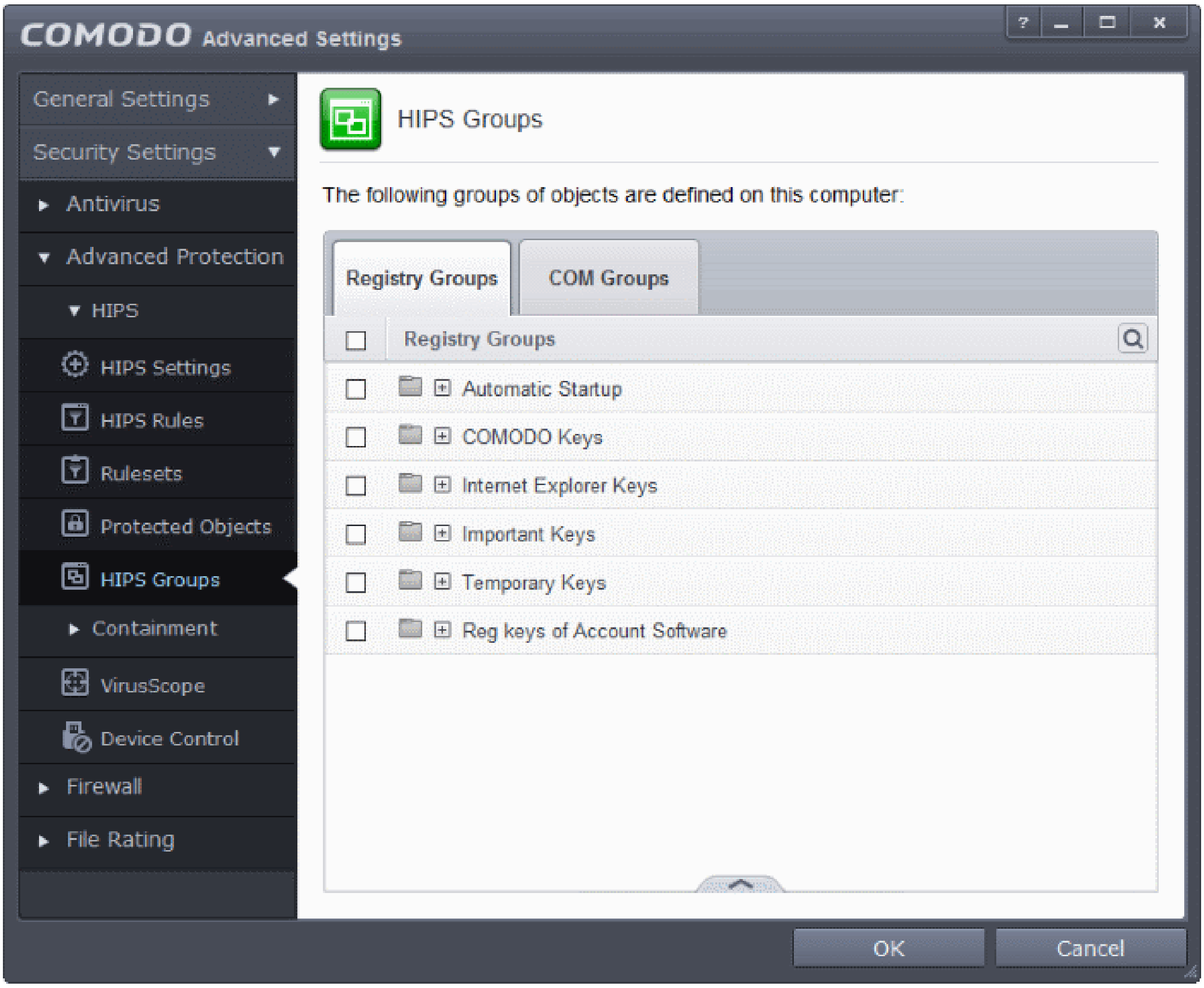
- **Registry Groups**- Allows you to create new groups and add registry keys to groups that are to be protected from changes
- **COM Groups** - Allows you to create new COM groups and add COM classes to groups that are to be protected from changes

6.2.2.5.1. Registry Groups

Registry groups are predefined batches of one or more registry keys. Creating a registry group allows you to quickly add it to Registry Protection list.

To open the Registry Groups interface

- In the Advanced Settings screen, click Security Settings > Advanced Protection > HIPS > HIPS Groups and select the Registry Groups tab.



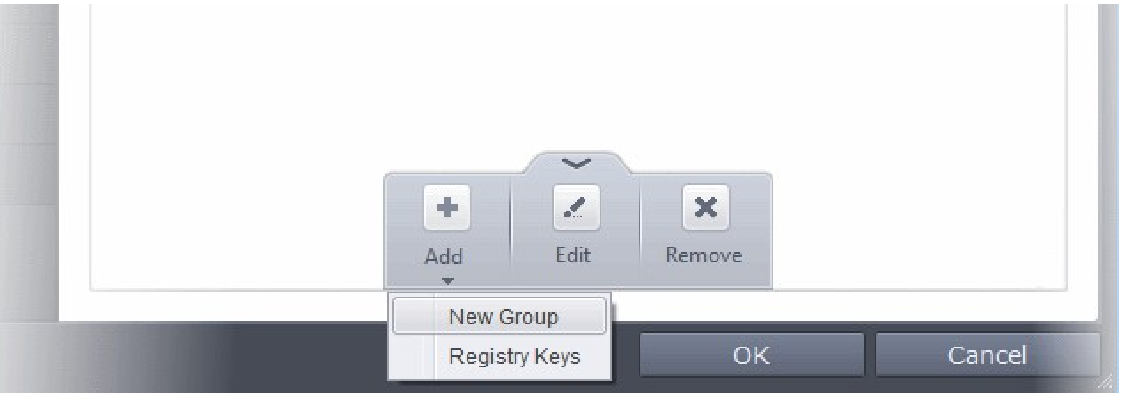
The following groups of objects are defined on this computer:

- □ Registry Groups
- □ Automatic Startup
- □ COMODO Keys
- □ Internet Explorer Keys
- □ Important Keys
- □ Temporary Keys
- □ Reg keys of Account Software

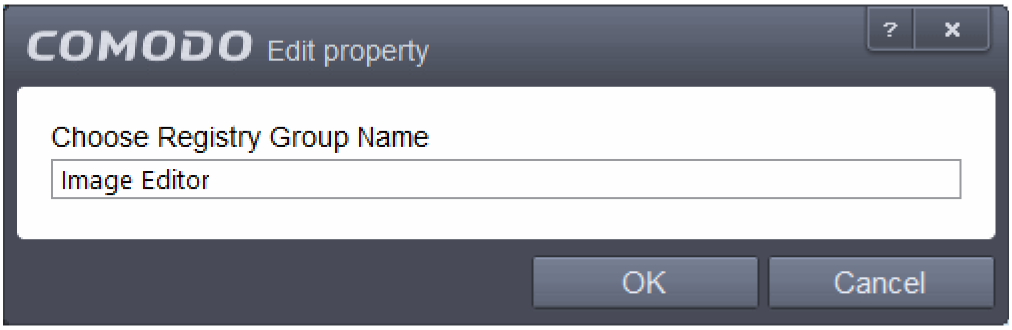
This interface allows you to

- 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 handle from the bottom and click 'Add'.



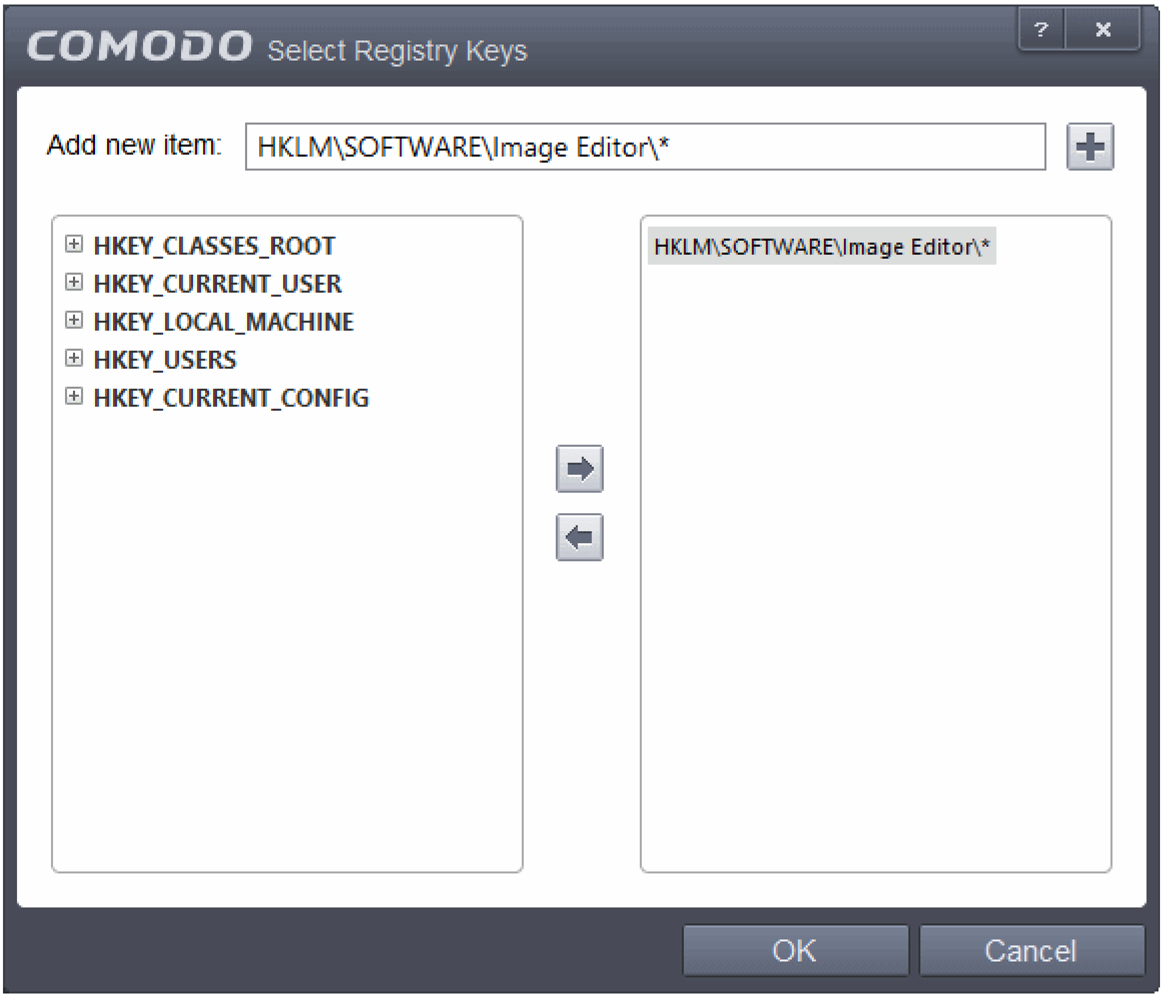
- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'


COMODO Edit property

Choose Registry Group Name

Image Editor

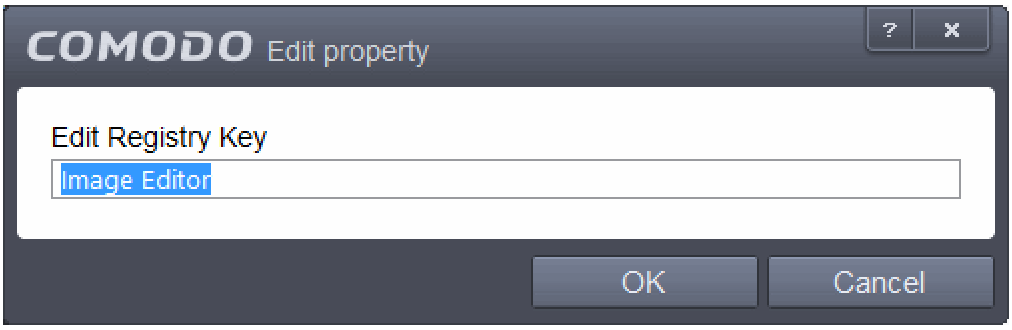
- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.


COMODO Select Registry Keys

Add new item: HKLM\SOFTWARE\Image Editor*

You can add items by browsing the registry tree in the left hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



Edit Registry Key

Image Editor

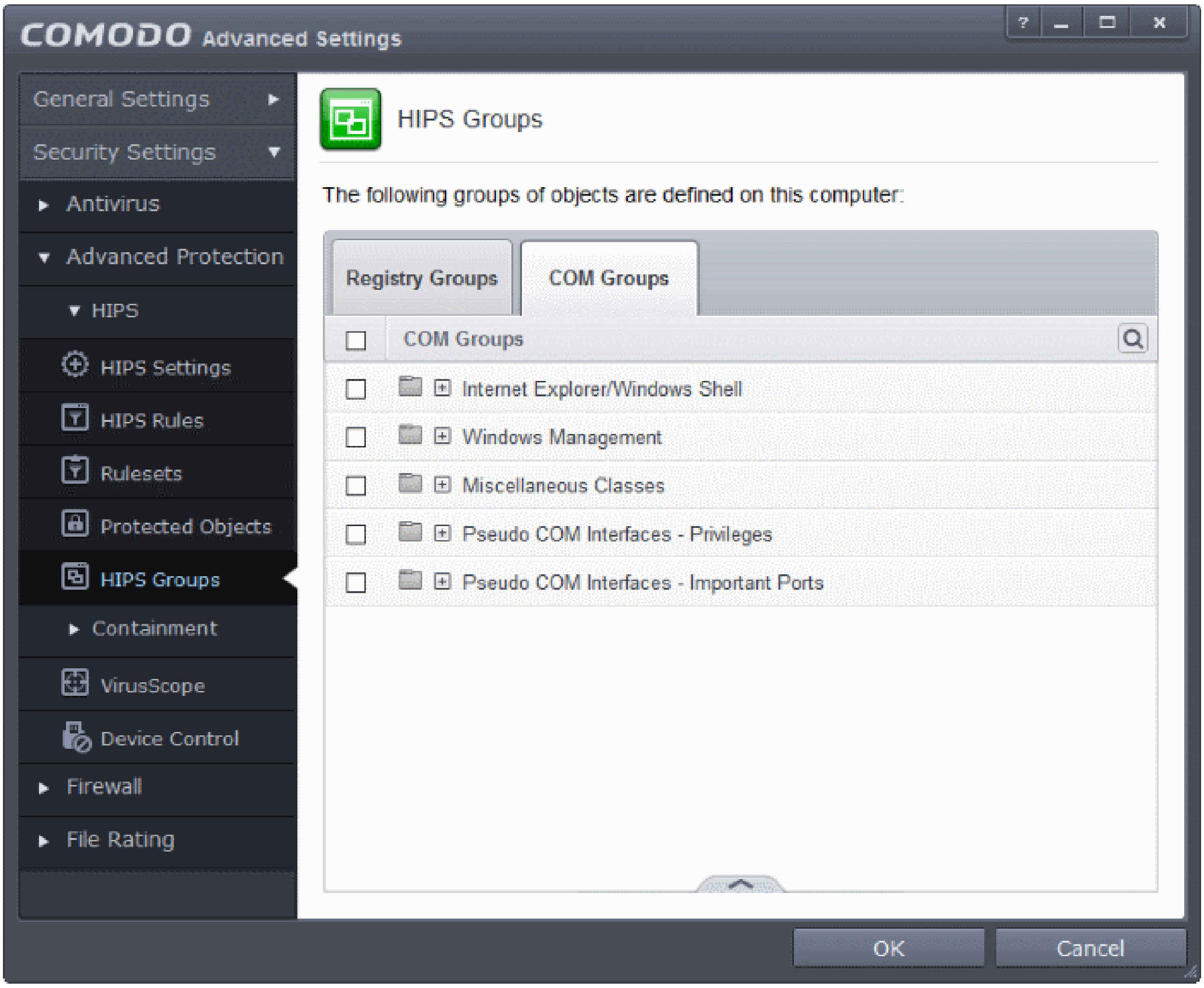
- To remove a group, select the group, click the handle and choose 'Remove'.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.5.2. COM Groups

COM groups are handy, predefined groupings of COM interfaces. Creating a COM group allows you to quickly add it to COM Protection list.

To open the COM Groups interface

- In the Advanced Settings screen, click Security Settings > Advanced Protection > HIPS > HIPS Groups and select the 'COM Groups' tab.



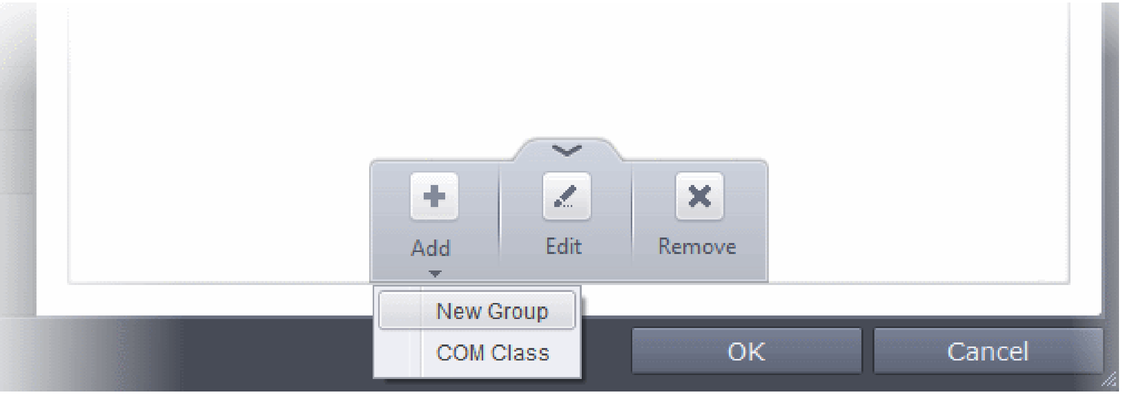
The following groups of objects are defined on this computer:

	COM Groups
□	Internet Explorer/Windows Shell
□	Windows Management
□	Miscellaneous Classes
□	Pseudo COM Interfaces - Privileges
□	Pseudo COM Interfaces - Important Ports

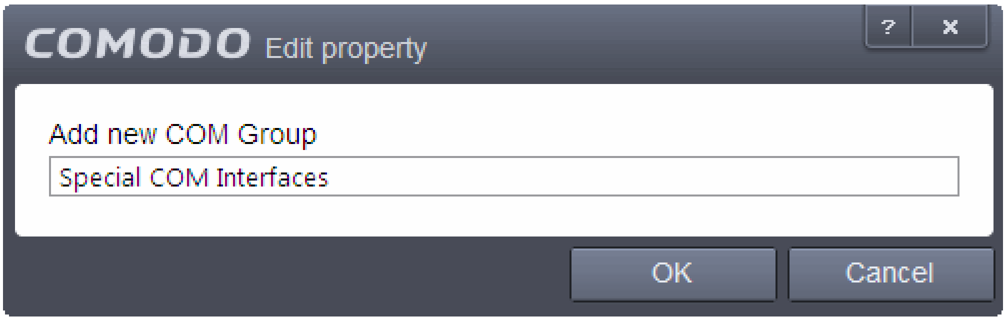
This interface allows you to:

- 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 handle from the bottom and click 'Add'.



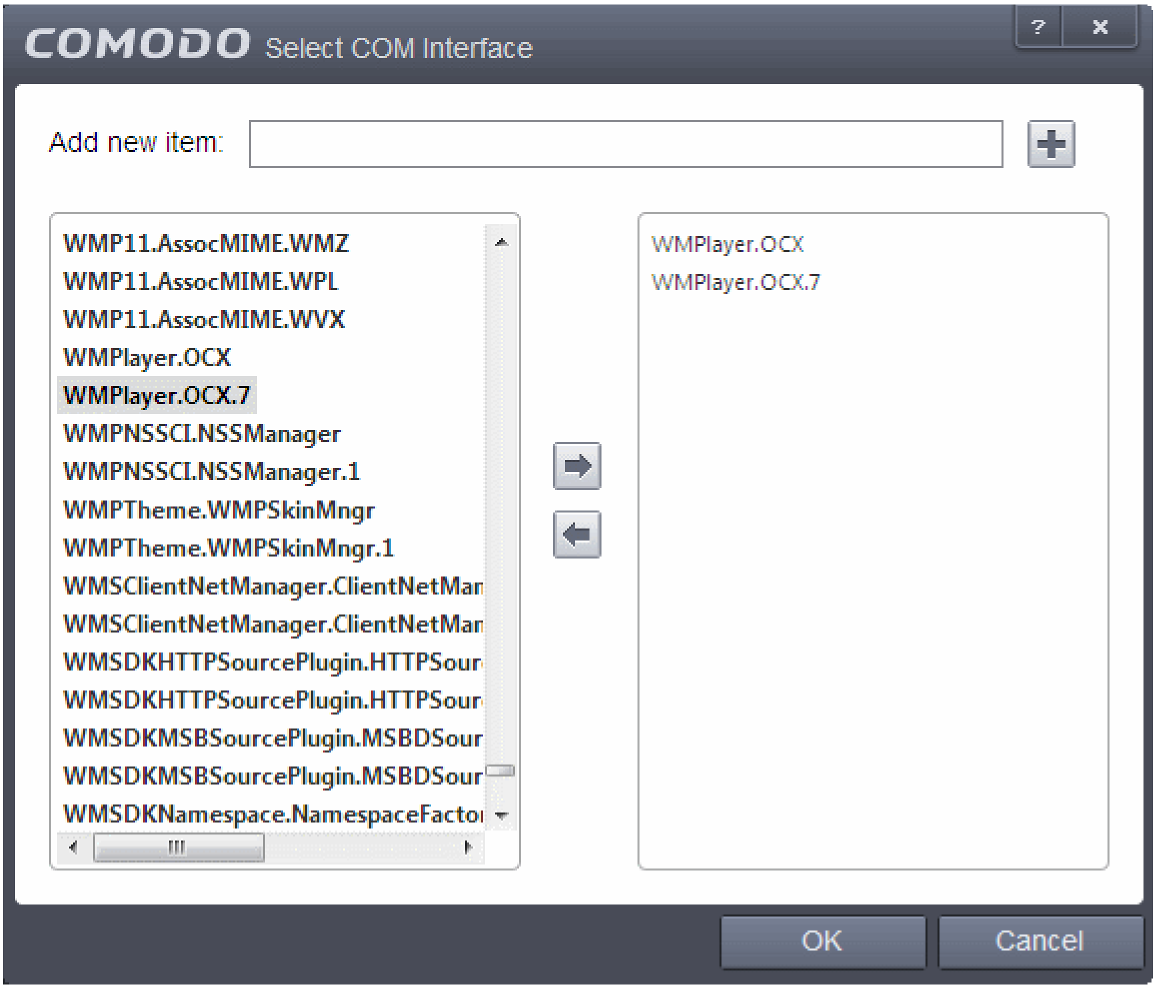
- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.



Add new COM Group

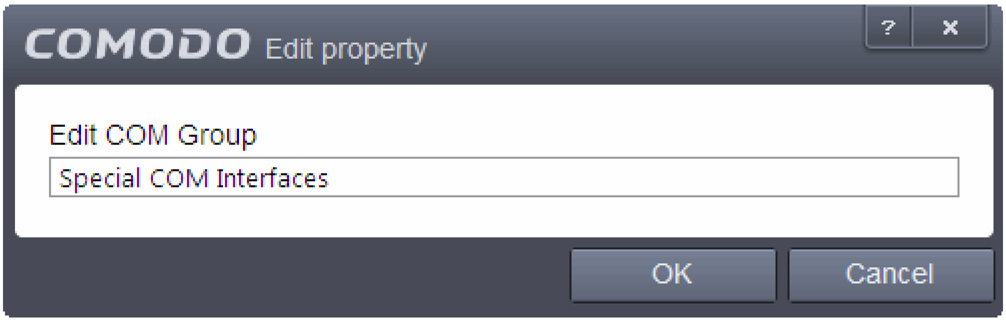
Special COM Interfaces

- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class. The 'Select COM Interface' dialog will be opened.


COMODO Select COM Interface
Add new item:
WMP11.AssocMIME.WMZ
WMP11.AssocMIME.WPL
WMP11.AssocMIME.WVX
WMPlayer.OCX
WMPlayer.OCX.7
WMPNSSCI.NSSManager
WMPNSSCI.NSSManager.1
WMPTheme.WMPSkinMngr
WMPTheme.WMPSkinMngr.1
WMSClientNetManager.ClientNetMan
WMSClientNetManager.ClientNetMan
WMSDKHTTPSourcePlugin.HTTPSour
WMSDKHTTPSourcePlugin.HTTPSour
WMSDKMSBSourcePlugin.MSBDSour
WMSDKMSBSourcePlugin.MSBDSour
WMSDKNamespace.NamespaceFactoi
WMPlayer.OCX
WMPlayer.OCX.7
OK
Cancel

You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the 'Edit Property' dialog



Edit COM Group

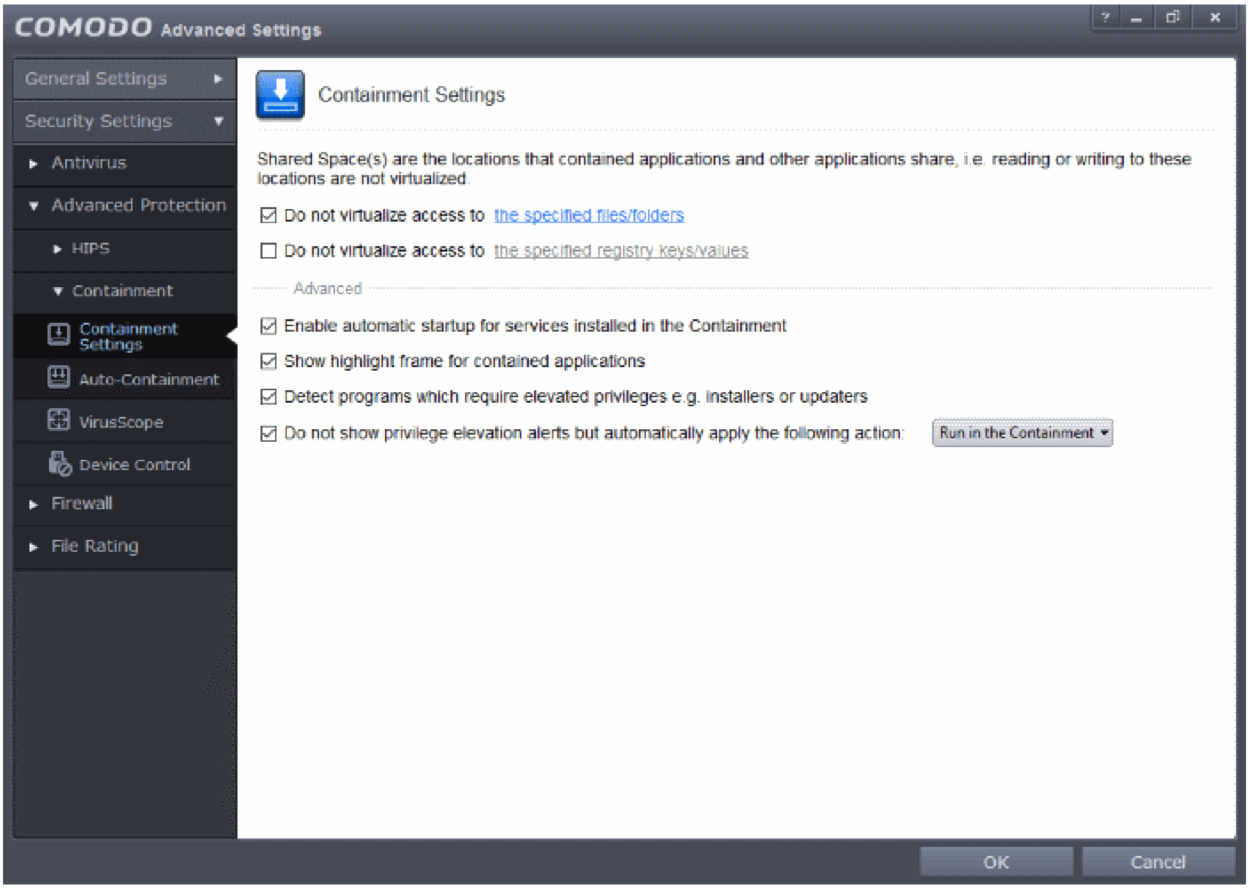
Special COM Interfaces

- To remove a group, select the group, click the handle and choose 'Remove'.
- 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, click the handle and choose 'Remove'.

6.2.2.6. Comodo Containment

Comodo Containment protects your computer by isolating unknown and potentially unsafe applications in a security hardened virtual environment to prevent them causing any damage.

- See Configuring Containment Settings for details on how to configure shared space settings and other general containment settings.
- You can define rules which control how much access a contained application should have. For more information, refer to Configuring Rules for Auto-Containment.
- For more background information about Comodo Containment, see The Container – An Overview.
- For more information about how the Advanced Protection engine determines the reputation of a file, refer to Unknown Files: The Scanning Processes



Containment Settings

Shared Space(s) are the locations that contained applications and other applications share, i.e. reading or writing to these locations are not virtualized.

☑ Do not virtualize access to the specified files/folders

□ Do not virtualize access to the specified registry keys/values

Advanced

☑ Enable automatic startup for services installed in the Containment

☑ Show highlight frame for contained applications

☑ Detect programs which require elevated privileges e.g. installers or updaters

☑ Do not show privilege elevation alerts but automatically apply the following action: Run in the Containment

6.2.2.6.1. The Container - An Overview

Comodo Containment is an isolated operating environment for unknown and untrusted applications. Running an application in the container means that it cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have integrated containment technology directly into the security architecture of Comodo Client Security to complement and strengthen the Firewall, Advanced Protection, File Rating and Antivirus modules.

Applications in the container are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of the real system. This delivers the smoothest user experience possible by allowing unknown applications to run and operate as they normally would while denying them the potential to cause lasting damage. Users can also print documents from within the container. This is useful, for example, if a suspicious PDF has valid information that should be printed.

After an unknown application has been placed in the container, CCS also automatically queues it for submission to Comodo Cloud Scanners for automatic behavior analysis. Firstly, the files undergo another antivirus scan on our servers. If the scan discovers the file to be malicious, then it is designated as malware, the result is sent back to the local installation of CCS and the local black-list is updated. If the scan does not detect that the file is malicious then its behavior will be monitored by running it in a virtual environment within Comodo's Instant Malware Analysis (CIMA) servers and all its activities are recorded. If these behaviors are found to be malicious then the file is manually analyzed by Comodo technicians to confirm whether it is a malicious file or not. If found to be malicious, the executable is then added to the antivirus black list, the results sent back to the local installation of CCS, file quarantined and the user alerted.

By uniquely deploying 'containment as security', CCS offers improved security, fewer pop-ups and greater ease of use than ever before.

6.2.2.6.2. 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**
  - 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**

  Files and processes that pass the security inspections above but are not yet recognized as 'safe' (white-listed) are 'Unrecognized' files and contained automatically. In order to try to establish whether a file is safe or not, CCS will first consult Comodo's File Look-Up Server (FLS) to check the very latest signature databases:
  - A digital hash of the unrecognized process or file is created.
  - These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all known malware and a white list of the signatures of the 'safe' files.
    - First, our servers check these hashes against the latest available black-list
    - If the hash is discovered on this blacklist then it is malware
    - The result is sent back to the local installation of 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'.
  - Unrecognized files are simultaneously uploaded to Comodo's Instant Malware Analysis servers [a.k.a Comodo Automated Malware Analysis System (CAMAS)] for further checks:
  - Firstly, the files undergo another antivirus scan on our servers.
    - If the scan discovers the file to be malicious (for example, heuristics discover it is a brand new variant) then it is designated as malware. This result is sent back to the local installation of

CCS and the local and global black-list is updated.

- If the scan does not detect that the file is malicious then it passes onto the the next stage of inspection - behavior monitoring.
- The behavior analysis system is a cloud based service that is used to help determine whether a file exhibits malicious behavior. Once submitted to the system, the unknown executable will be automatically run in a virtual environment and all actions that it takes will be monitored. For example, processes spawned, files and registry key modifications, host state changes and network activity will be recorded.
- If these behaviors are found to be malicious, the file is submitted to our technicians for further manual checks and confirmation. If the manual testing confirms it as a malware, then it will be added to the global blacklist which will benefit all users. The results will be sent back to local installation of CCS, file will be quarantined and the user alerted.
- If the manual analysis confirms the file as safe, then it will be added to global whitelist and results sent back to local installation of CCS.

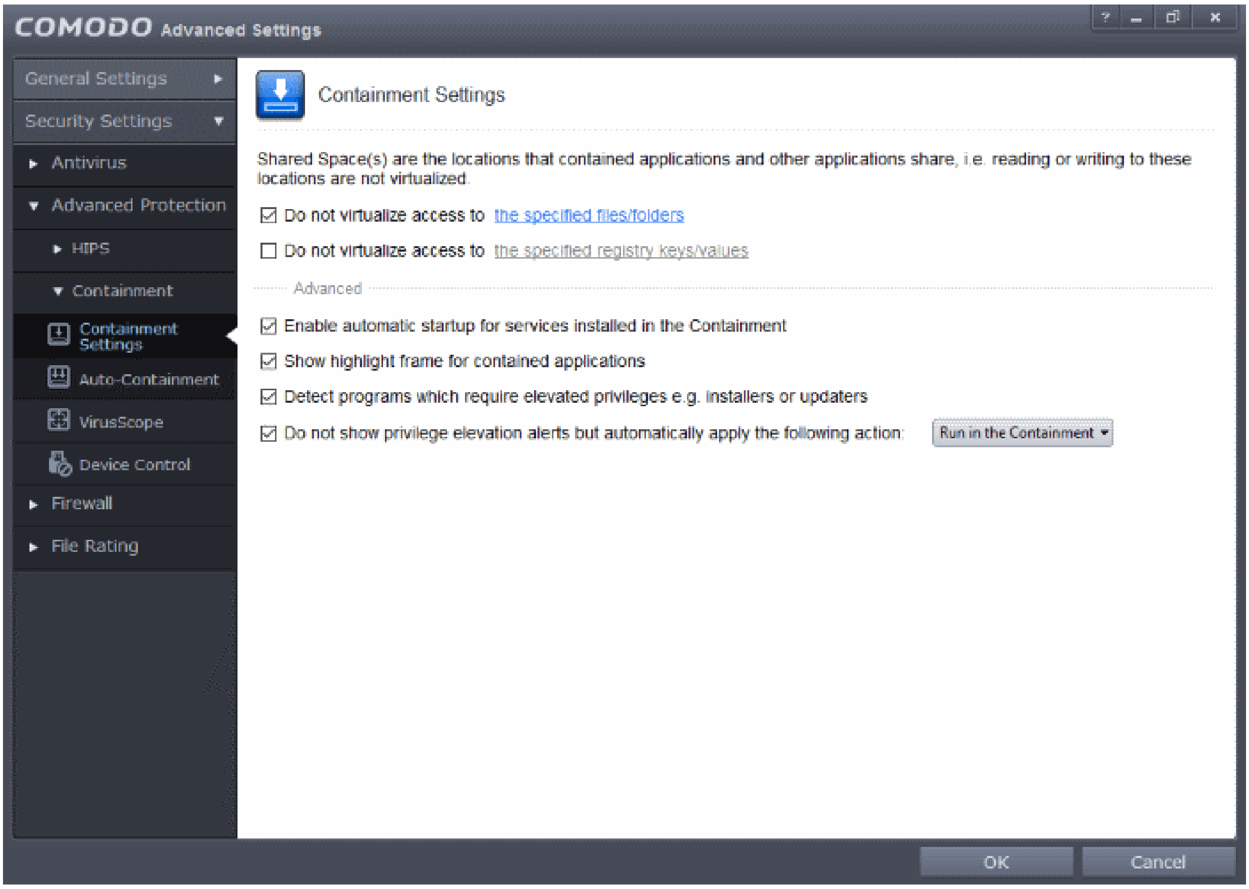
Important Note: In order for the software to submit unknown files to our file rating and malware analysis servers (CAMAS), please make sure the following IP addresses and ports are allowed on your network firewall:

- To allow communication with camas.comodo.com
  - IP that needs to be allowed: 199.66.201.30
  - Port that needs to be allowed: port 80 for TCP
  - Direction: Outgoing (Endpoints to CAMAS)
- 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: 4447 UDP and 4448 TCP
  - Direction: Outgoing (Endpoints to FLSs)

6.2.2.7. Configuring Containment Settings

The 'Containment Settings' section of 'Advanced Settings' allows you to configure settings that determine how proactive the containment should be and which types of files it should check.

- The 'Containment Settings' panel can be accessed by clicking 'Tasks > Open Advanced Settings > Security Settings > Advanced Protection > Containment > Containment Settings



Containment Settings

Shared Space(s) are the locations that contained applications and other applications share, i.e. reading or writing to these locations are not virtualized.

☑ Do not virtualize access to the specified files/folders

☐ Do not virtualize access to the specified registry keys/values

Advanced

☑ Enable automatic startup for services installed in the Containment

☑ Show highlight frame for contained applications

☑ Detect programs which require elevated privileges e.g. installers or updaters

☑ Do not show privilege elevation alerts but automatically apply the following action: Run in the Containment

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

- Shared Space Settings - Files downloaded or generated by contained applications that you wish to be able to access from your real system should be downloaded to the shared space
- Advanced Settings – Allows you to configure alert settings for containment as well as to enable automatic startup services for programs installed in the container.

Shared Space Settings:

'Shared Space' is a dedicated area on your local drive that the contained applications are permitted to write to and which can also be accessed by non-contained applications (hence the term 'Shared Space'). 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 is located by default at 'C:/Program Data/Shared Space'.

You can access the shared space folder in the following ways:

- Clicking the 'Shared Space' shortcut on your computer desktop
- Clicking 'Shared Space' button on the CCS interface
- Opening 'Containment Tasks' from the Tasks interface then clicking 'Open Shared Space'
- By default, contained applications can access folders and files on your 'real' system but cannot save any changes to them. However, you can define exceptions to this rule by using the 'Do not virtualize access to...' links.

To define exceptions for files and folders

- Enable the 'Do not virtualize access to the specified files/folders' check-box then click on the words the specified files/folders. The 'Manage Exclusions' dialog will appear.
  - Click the handle at the bottom to open the tools menu then click 'Add.

  i. **Files** - Allows you to specify files or applications that contained applications are able to access

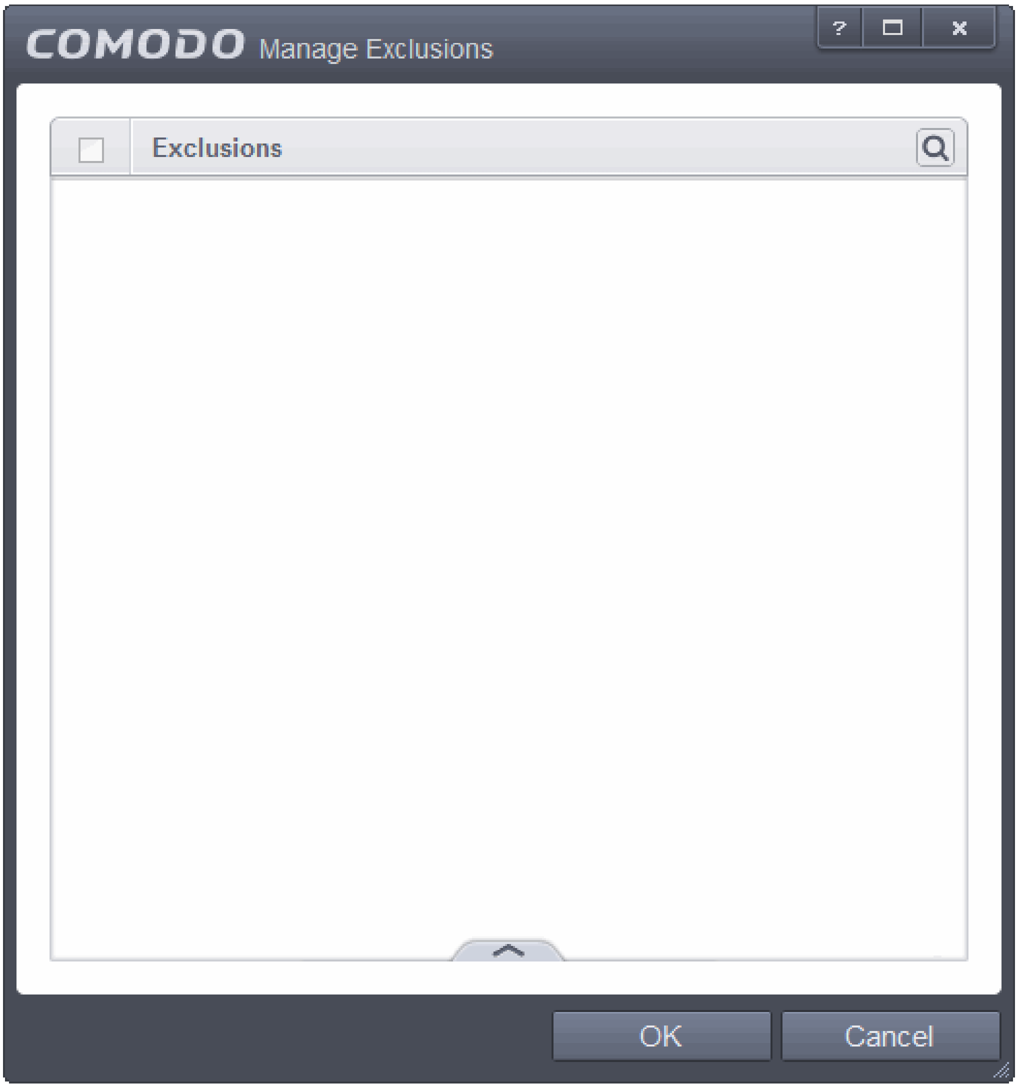
  ii. **Folders** - Specify a folder that can be accessed by contained applications

  iii. **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. For more details on file groups, refer to the section File Groups.

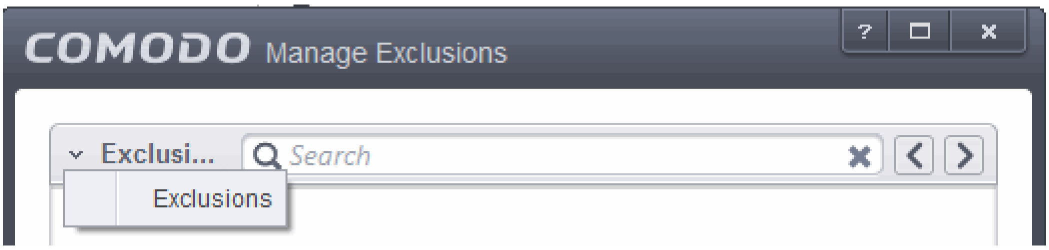
  iv. **Running Processes** - Allows you to add a program that contained applications are able to access
- To edit an exception, select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Change file or folder location path and click 'OK'
- Click 'OK' to implement your settings
- To manage file groups, click 'File Groups' on the left under 'File Rating'. The 'File Groups' screen allows you to view, add and edit file groups. Please refer to the section File Groups if you need more information with this area.

To define exceptions for specific Registry keys and values

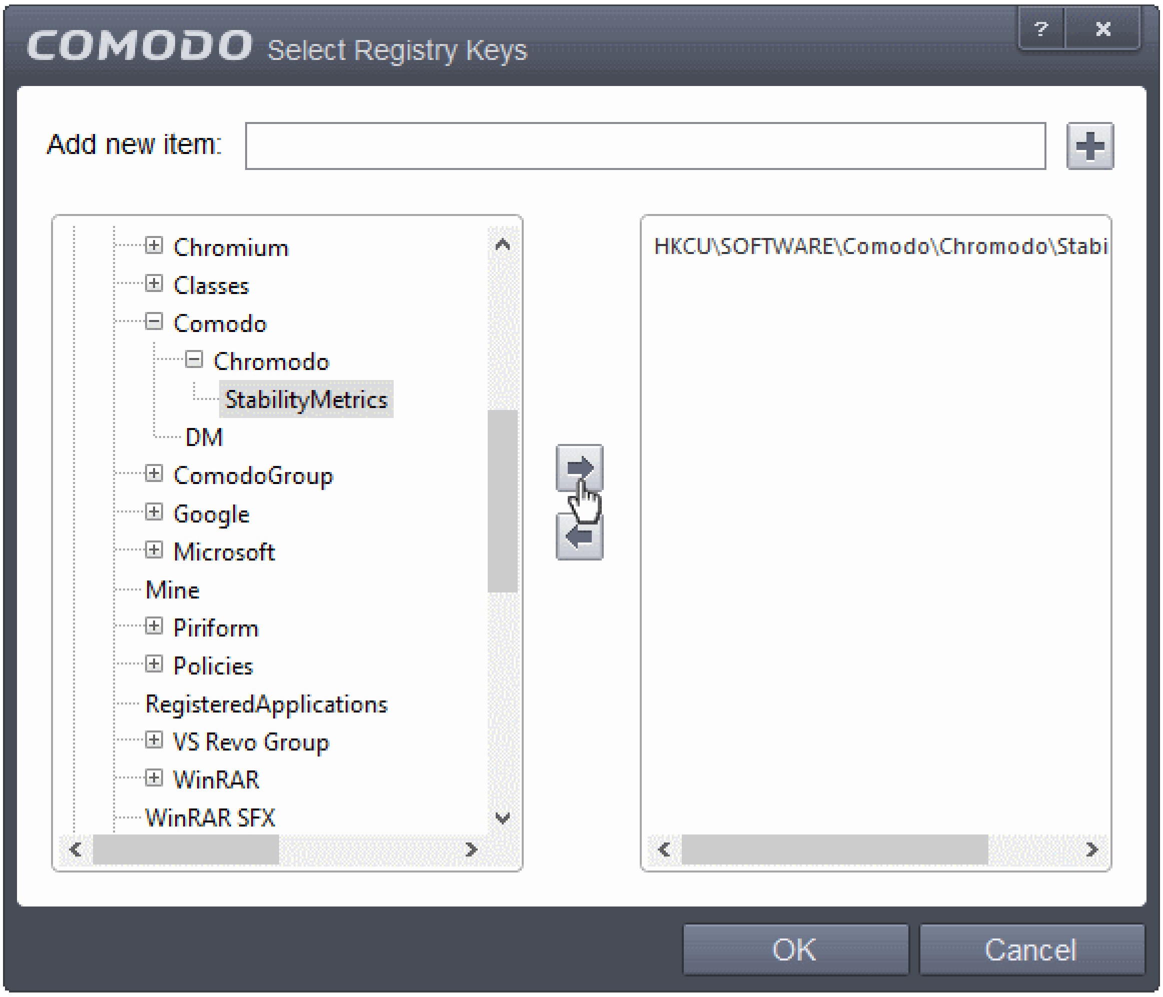
- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the words 'the specified registry keys/values'. The 'Manage Exclusions' dialog will appear.



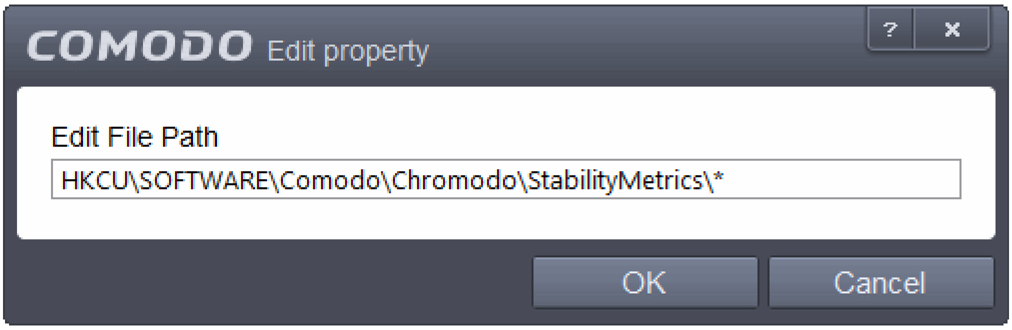
You can search for specific excluded Registry Keys or Values from the list by clicking the search icon 🔍 at the far right in the column header and entering the name of the key/value in full or part. You can navigate through the successive results by clicking the left and right arrows.



- Click the handle at the bottom to open the tools menu then click 'Add'.
  - **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exceptions. For an explanation of CCS registry groups, refer to the section **Registry Groups**.
  - **Registry Entries** - Opens an interface that allows you to quickly browse Windows registry keys and add them as exceptions:



  - 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'.

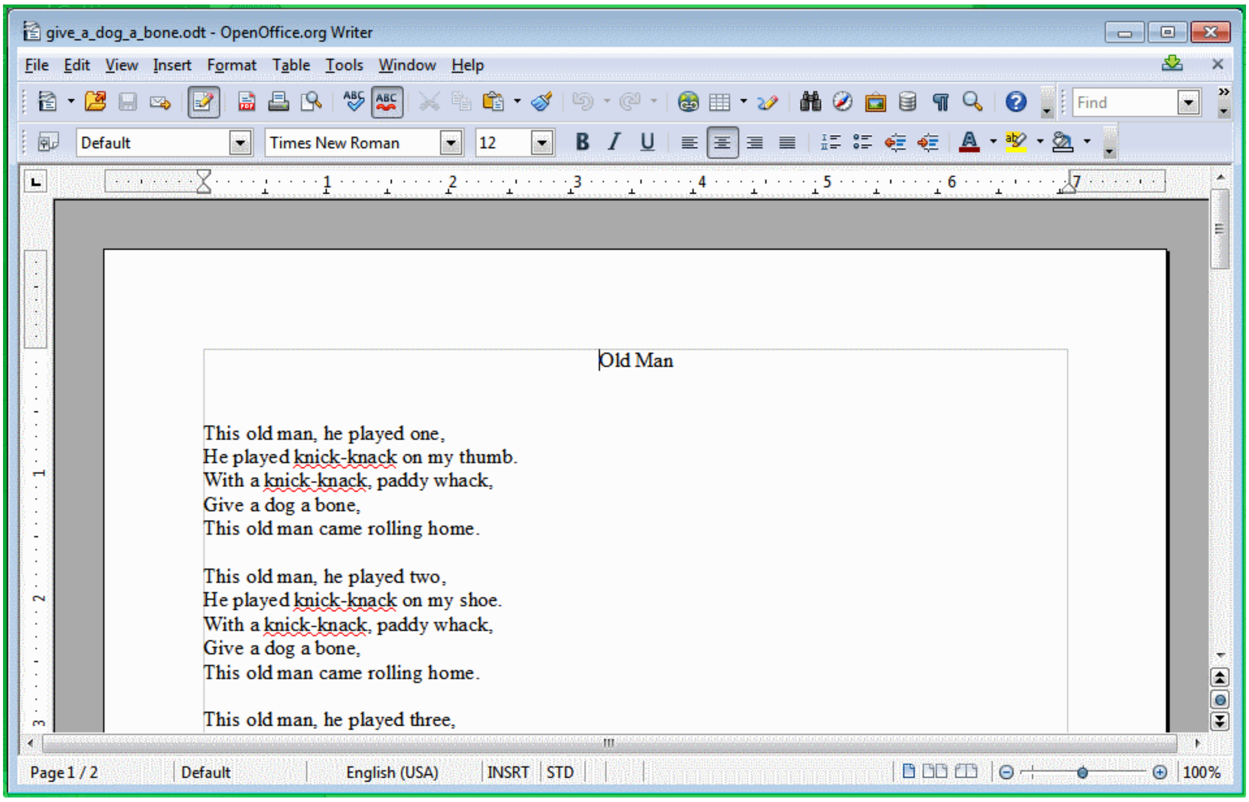


HKCU\SOFTWARE\Comodo\Chromodo\StabilityMetrics\*

Advanced Settings:

- **Enable automatic startup for services installed in the Containment -** By default, CCS does not permit contained services to run at Windows startup. Select this check-box to allow them to do so. (***Default = Enabled***)
- **Show highlight frame for contained programs -** 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 version OpenOffice Writer:


give_a_dog_a_bone.odt - OpenOffice.org Writer
File Edit View Insert Format Table Tools Window Help
Find
Default
Times New Roman
12
Page 1 / 2
Default
English (USA)
INSRT
STD
100%

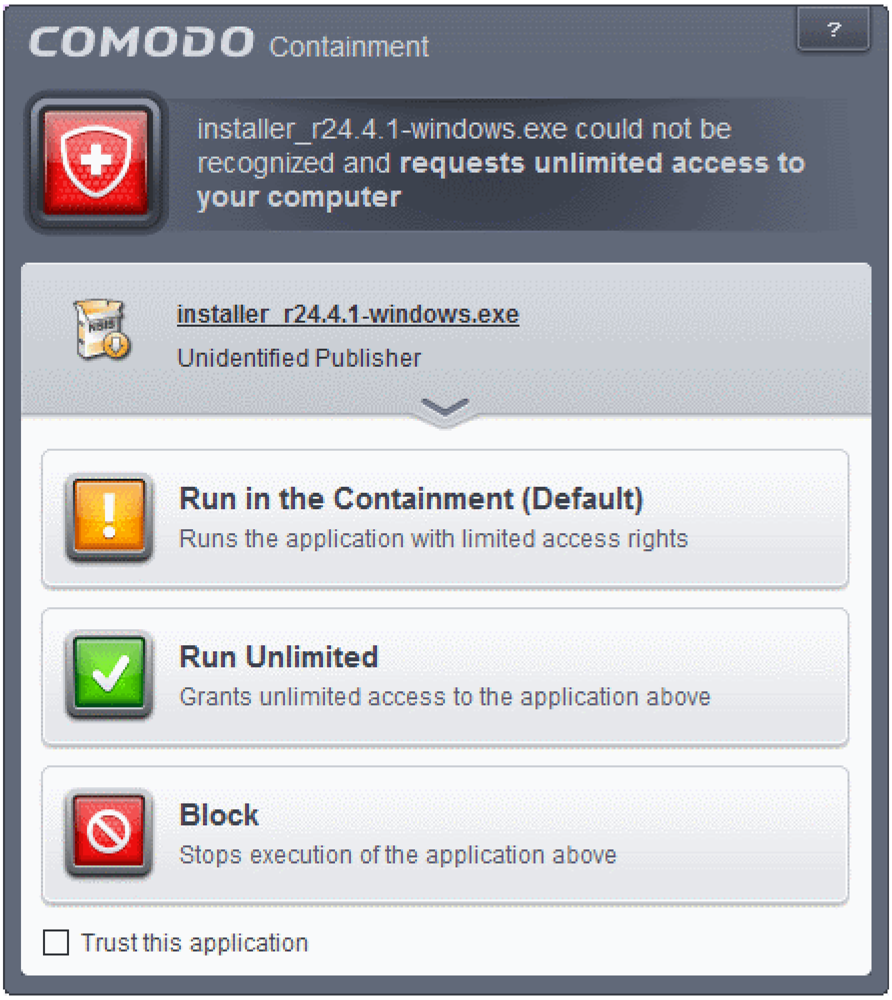
Old Man

This old man, he played one,
He played knick-knack on my thumb.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played two,
He played knick-knack on my shoe.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played three,

- **Detect programs which require elevated privileges e.g. installers or updaters:** Allows you to instruct the container to display alerts when an installer or updater requires administrator or elevated privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry. Refer to the section Understanding Security Alerts for more details.



installer_r24.4.1-windows.exe could not be recognized and **requests unlimited access to your computer**

installer_r24.4.1-windows.exe
Unidentified Publisher

Run in the Containment (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

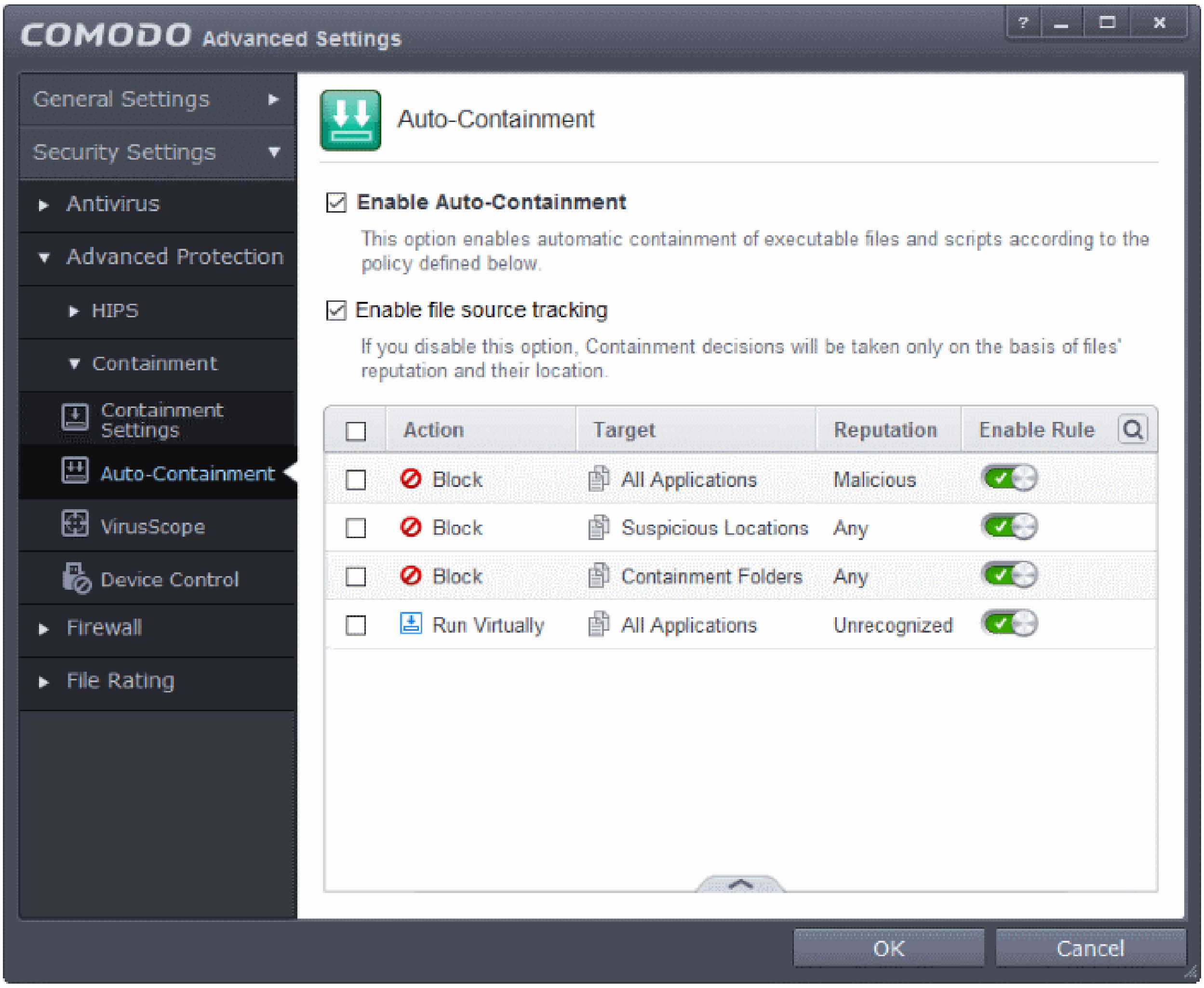
You can decide on whether or not to allow the installer or update based on your assessment, from the alert itself. (*Default=Enabled*)

- **Do not show privilege elevation alerts but automatically apply the following action:** If disabled, allows you to instruct the container to display alerts when a new or unrecognized program, application or executable requires administrator or elevated privileges to run. You can decide on whether or not to allow the unknown application based on your assessment, from the alert itself. (*Default=Enabled and Run in the Containment*)

6.2.2.8. Configuring Rules for Auto-Containment

The 'Auto-Containment' interface allows you to add and define rules for programs that should be run in the contained environment. A contained application has much less opportunity to damage your computer because it is run isolated from your operating system and your files. This allows you to safely run applications that you are not 100% sure about. Auto-Containment rules allow you to determine whether programs should be allowed to run with full privileges, ignored, run restricted or run in fully virtualized environment. For easy identification, Comodo Client Security will show a green border around programs that are running in the container.

- The 'Auto-Containment' panel can be accessed by clicking 'Tasks' > 'Containment Tasks' > 'Open Advanced Settings' > 'Security Settings' > 'Containment' > 'Auto-Containment'



Auto-Containment

☑ **Enable Auto-Containment**

This option enables automatic containment of executable files and scripts according to the policy defined below.

☑ Enable file source tracking

If you disable this option, Containment decisions will be taken only on the basis of files' reputation and their location.

□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malicious	✓
□	Block	Suspicious Locations	Any	✓
□	Block	Containment Folders	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓

- **Enable Auto-Containment -** Allows you to enable or disable automatic containment of unrecognized/unknown files. If enabled, unknown applications are run inside the container as per the rules defined. (***Default = Enabled***)
- **Enable file source tracking –** If enabled, the source parameter of a containment rule will be considered. Specifying a source in a rule allows you to create granular custom rules. For example, if you wanted to only auto-contain all files downloaded from the internet, then the 'internet' is your source. If this setting is disabled then the source parameter will be disregarded and only the reputation and location parameters will be considered. More information about sources can be found here ***(Default = Enabled)***

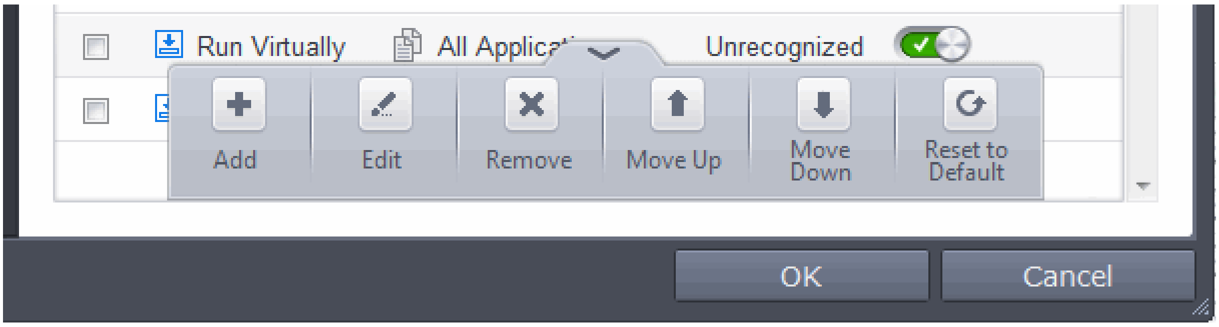
Each rule has the following attributes:

- **Action –** Displays the operation that the container should perform on the target file if the rule is triggered.
- **Target –** The file types, groups or locations on which the rule will be executed.
- **Reputation –** The trust status of the files to which the rule should apply. Can be 'Malware', 'Trusted' or 'Unrecognized'.
- **Enable Rule –** Allows you to enable or disable the rule.

CCS ships with a set of pre-defined auto-containment rules that are configured to provide maximum protection for your system. The following table tells you settings of these pre-defined rules:

Rule	Action	Target	Restriction Level	Rating	Source			Log Action	Limit Maximum memory	Limit Program Execution Time	Quarantine
					Created by	Located on	Downloaded from				
1	Block	File Group - All Applications	N/A	Malware	Any	Any	Any	On	N/A	N/A	On
2	Block	File Group - Suspicious Locations	N/A	Any	Any	Any	Any	On	N/A	N/A	Off
3	Block	File Group – Containment Folders	N/A	Any	Any	Any	Any	On	N/A	N/A	Off
4	Run Virtually	File Group – All Applicatiouns	Off	Unrecognized	Any	Any	Any	On	Off	Off	N/A

Clicking the handle at the bottom of the interface opens a rule configuration panel:



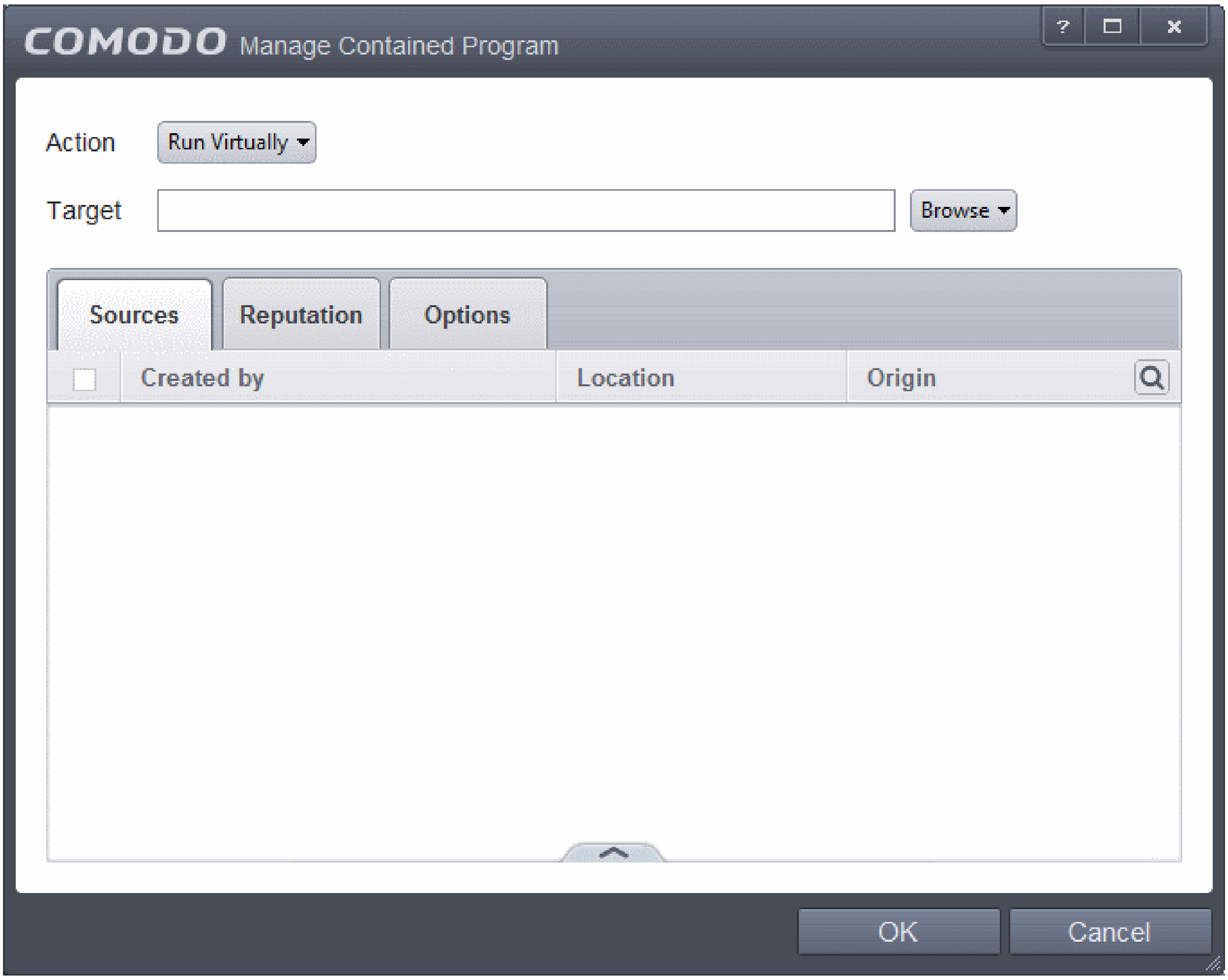
- **Add** - Allows you to add a new containment rule. See the section **Adding an Auto-Containment Rule** for guidance on creating a new rule.
- **Edit** - Allows you to modify the selected containment rule. See the section '**Editing an Auto-Containment Rule**' for more details.
- **Remove** - Deletes the selected rule.
- **Reset to Default** – Resets to default the rule.

Users can also re-prioritize the containment rules by using the 'Move Up' and 'Move Down' buttons.

Adding an Auto-Containment Rule

Auto-containment rules can be created for a single application, for all applications in a folder or file group, from running processes or for applications based on their file or process hash. ‘Source’, ‘Reputation’ and ‘Options’ allow you to add detailed filters to your rule. These are, however, optional, so you can create a very simple rule to run an application in the container just by specifying the action and the target application.

- Click the 'Add' button from the options.

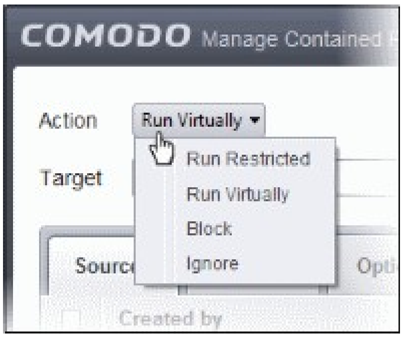


The Manage Contained Program screen will be displayed.

- Step 1 – Select the Action
- Step 2 – Select the Target
- Step 3 – Select the Sources
- Step 4 – Select the File Reputation
- Step 5 – Select the Options

Step 1 – Select the Action

The options under the 'Action' drop-down button combined with the 'Set Restriction Level' setting in the 'Options' tab determine the amount of privileges a contained application has to access other software and hardware resources on your computer.



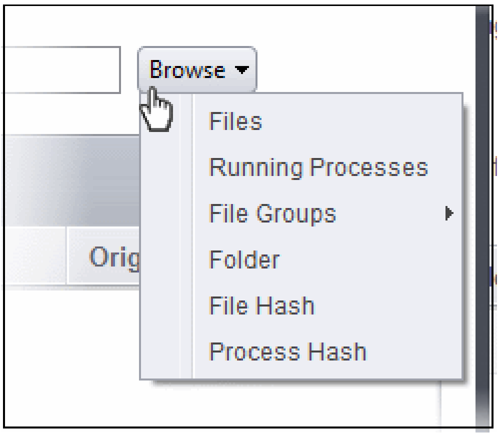
The options available are:

- **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 is allowed to run with all privileges.

Select the action from the options.

Step 2 – Select the Target

The next step is to select the target to which the auto-containment rule should be applied. Click the 'Browse' button beside the Target field.

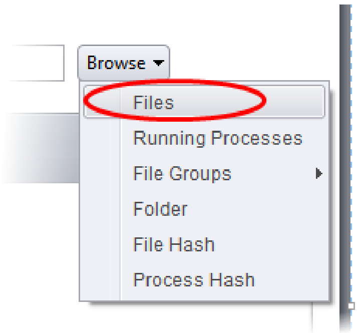


You have six options available to add the target path.

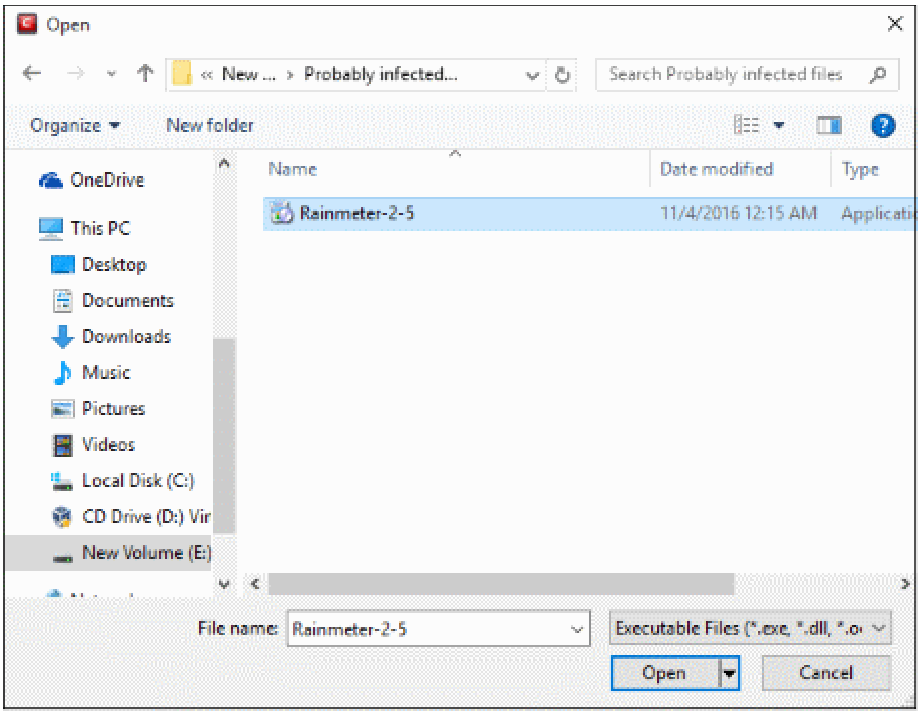
- Files – Specify individual files as targets of the rule.
- Running Processes – Add any process that is currently running on your computer as a target of the rule.
- File Groups – Add predefined file groups as the rule target. For information about creating or modifying a predefined file group, refer to File Groups
- 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 a target based on its hash value

Adding an individual File

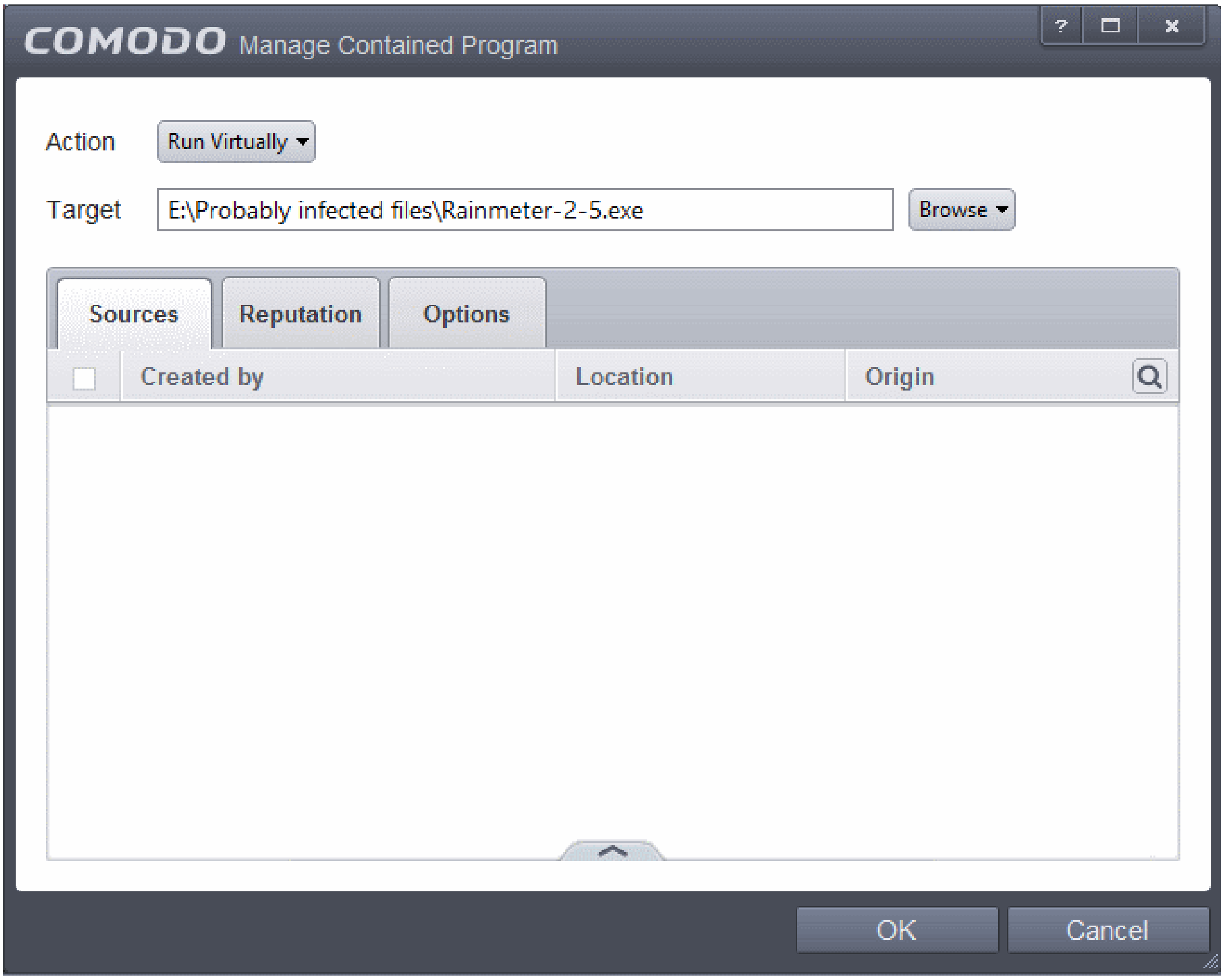
- Choose 'Files' from the 'Browse' drop-down.



- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'



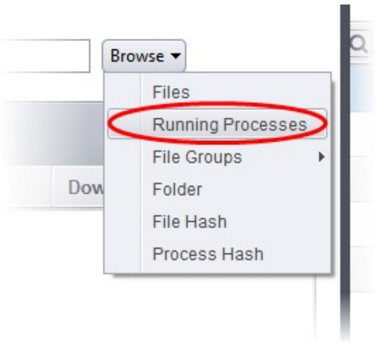
The file will be added as target and will be run as per the action chosen in Step 1.



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 Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Source and Reputation filters and Options for the rule.

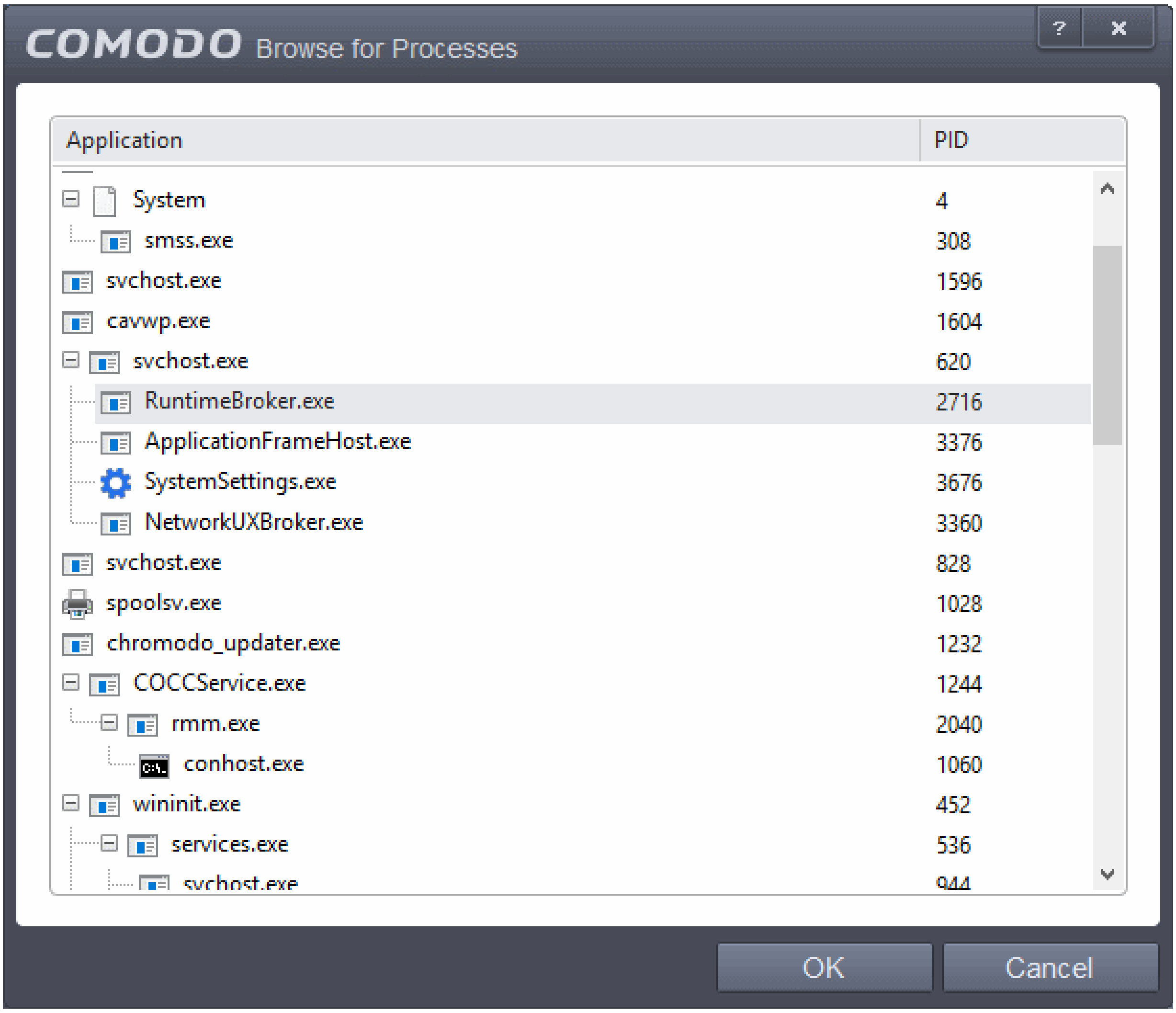
Adding an application from a running processes

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



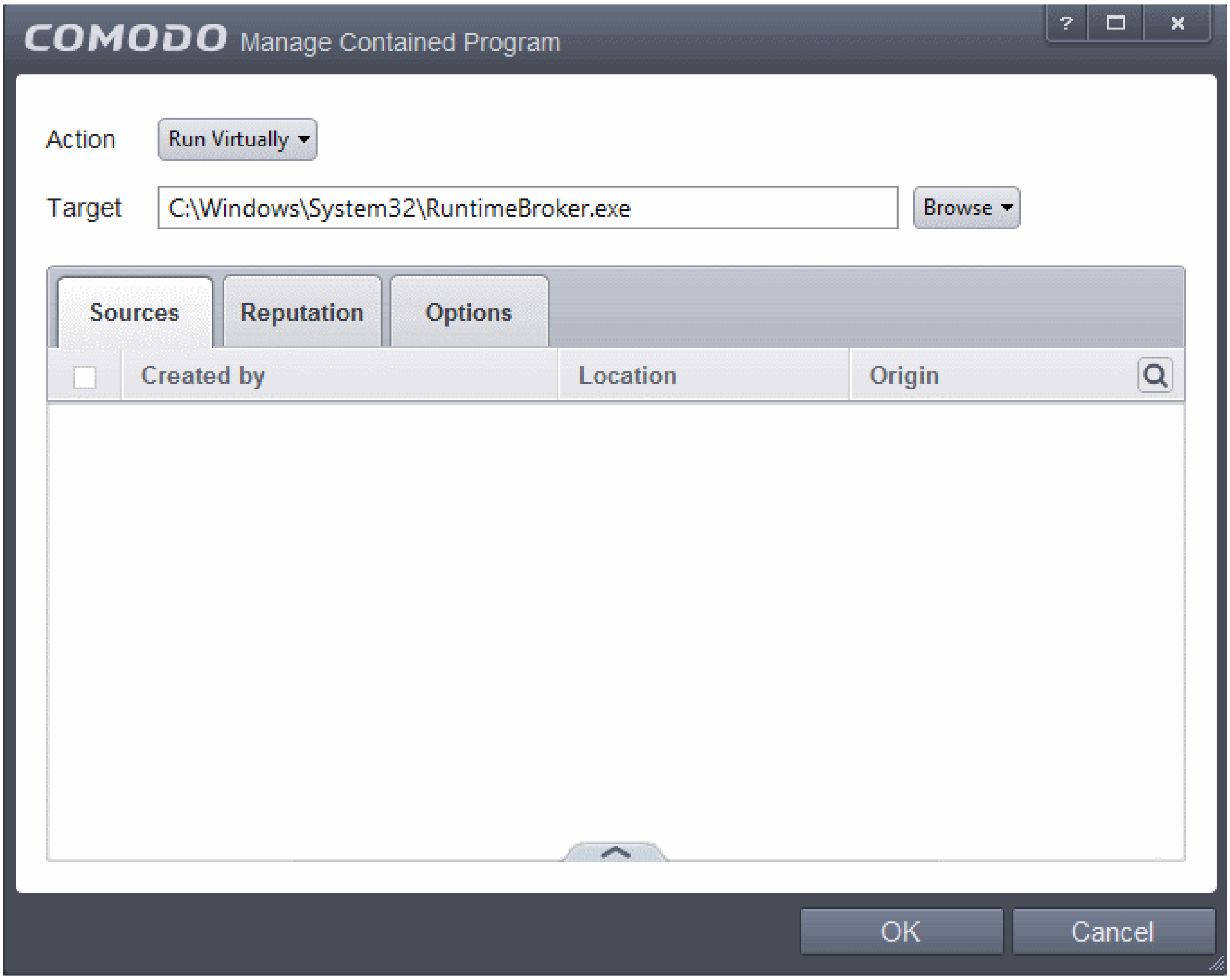
A list of currently running processes in your computer will be displayed.

- Select the process, whose target application is to be added to target and click 'OK' from the Browse for Process dialog.



Application	PID
System	4
smss.exe	308
svchost.exe	1596
cavwp.exe	1604
svchost.exe	620
RuntimeBroker.exe	2716
ApplicationFrameHost.exe	3376
SystemSettings.exe	3676
NetworkUXBroker.exe	3360
svchost.exe	828
spoolsv.exe	1028
chromodo_updater.exe	1232
COCCService.exe	1244
rmm.exe	2040
conhost.exe	1060
wininit.exe	452
services.exe	536
svchost.exe	944

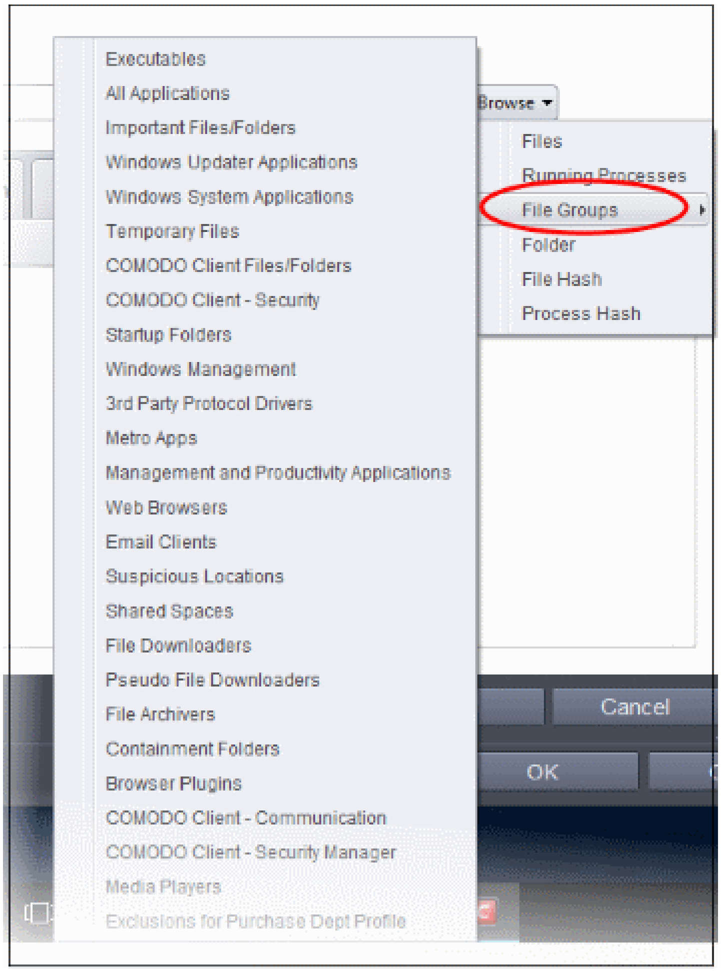
The file will be added as target and will be run as per the action chosen in Step 1.



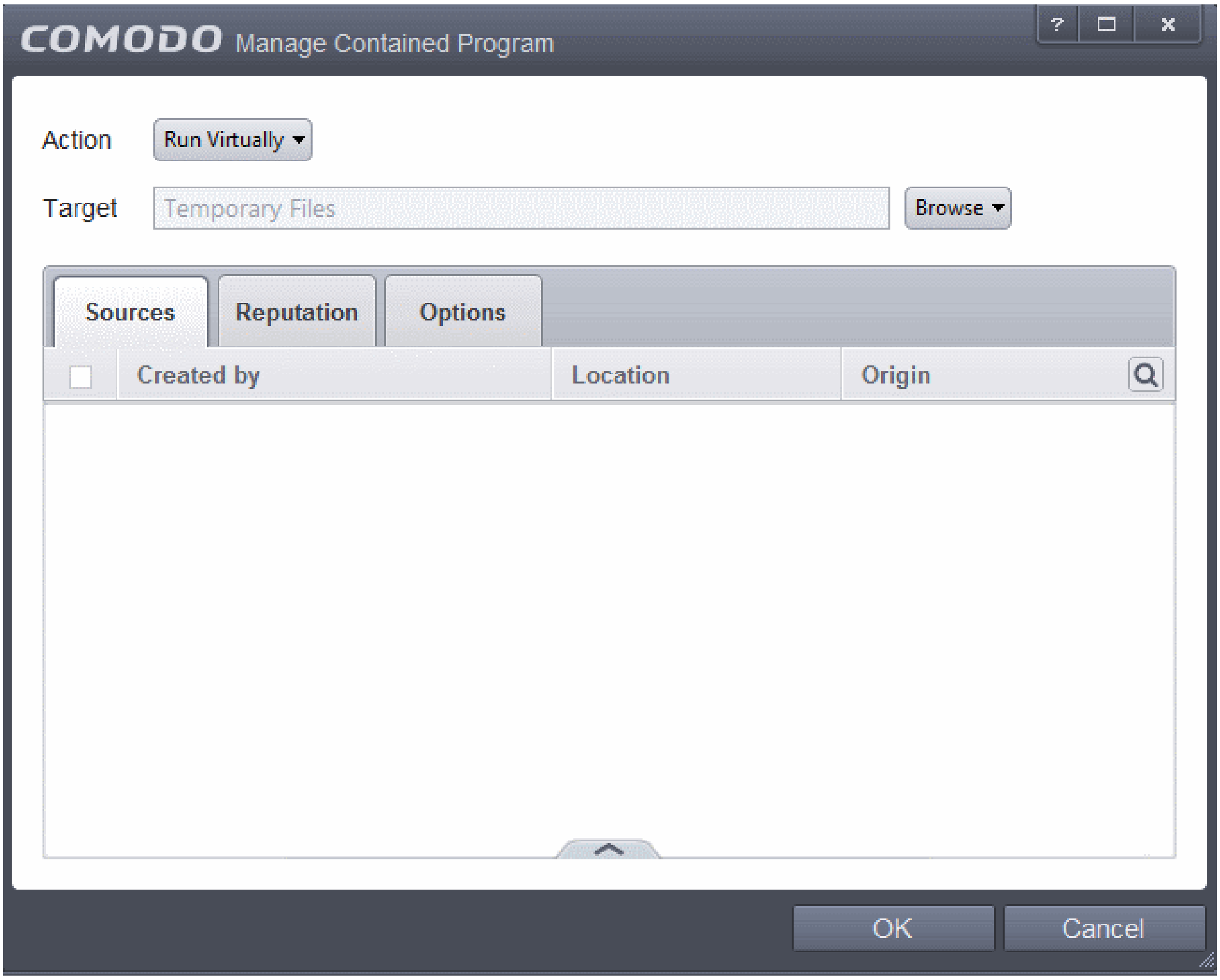
If you want to just add an application for a particular action as selected in Step 1 without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Source and Reputation filters and Options for the rule.

Adding a File Group

- Choose 'File Groups' from the 'Browse' drop-down. Choosing File Groups allows you to include a category of pre-set files or folders. For more details on how to manage file groups refer to the section File Groups.



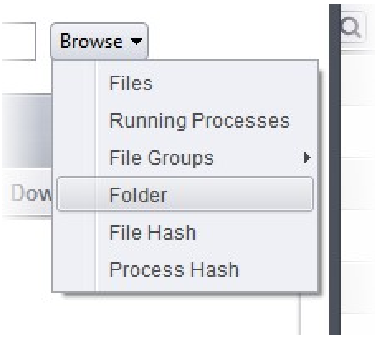
- Select the preset file group from the options.
- The file group will be added as target and the applications inside it will be run as per the action chosen in Step 1.



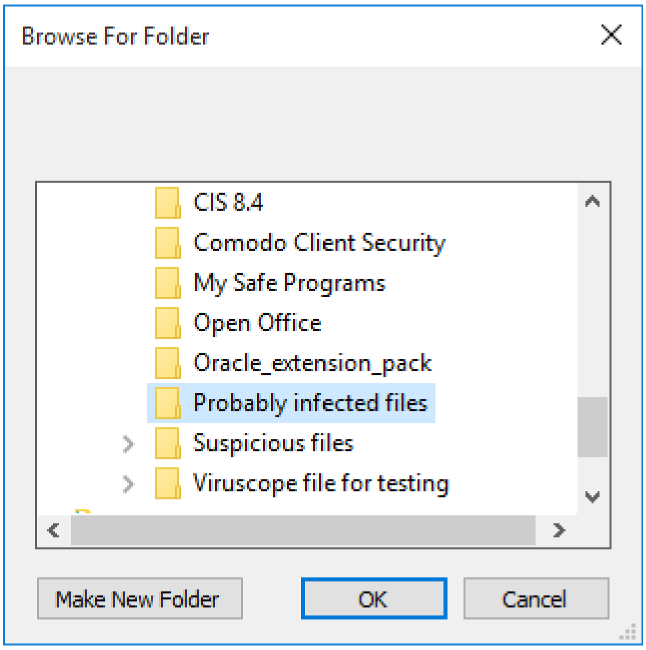
If you want to just add the applications in the file group for a particular action as selected in Step 1 without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Source and Reputation filters and Options for the rule.

Adding a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.

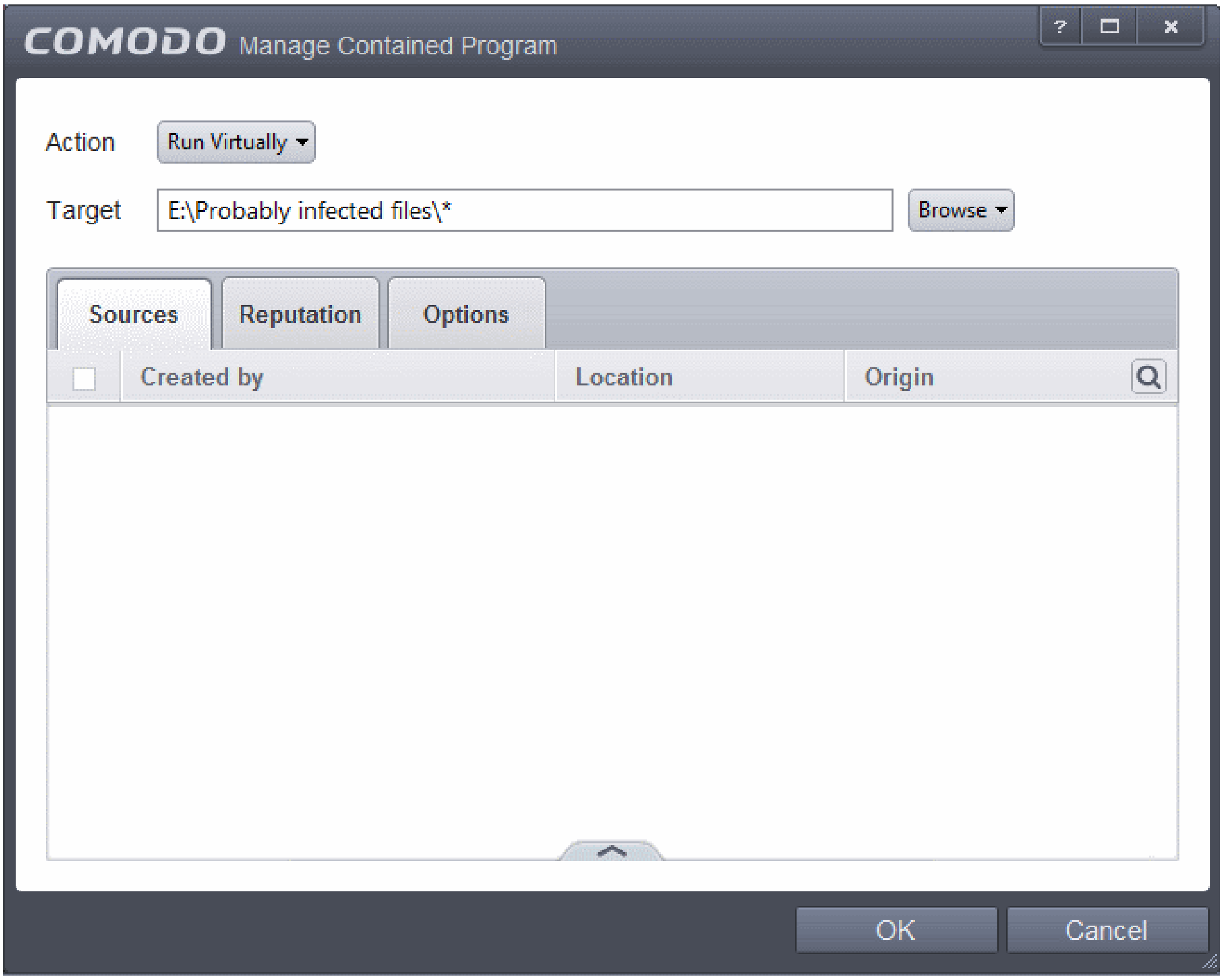


The 'Browse for Folder' dialog will appear.



- Navigate to the drive partition or folder you want to add as target and click 'OK'

The drive partition/folder will be added as target and will be run as per the action chosen in **Step 1**.



Action: Run Virtually

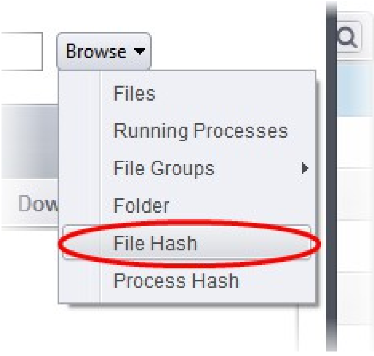
Target: E:\Probably infected files*

Browse

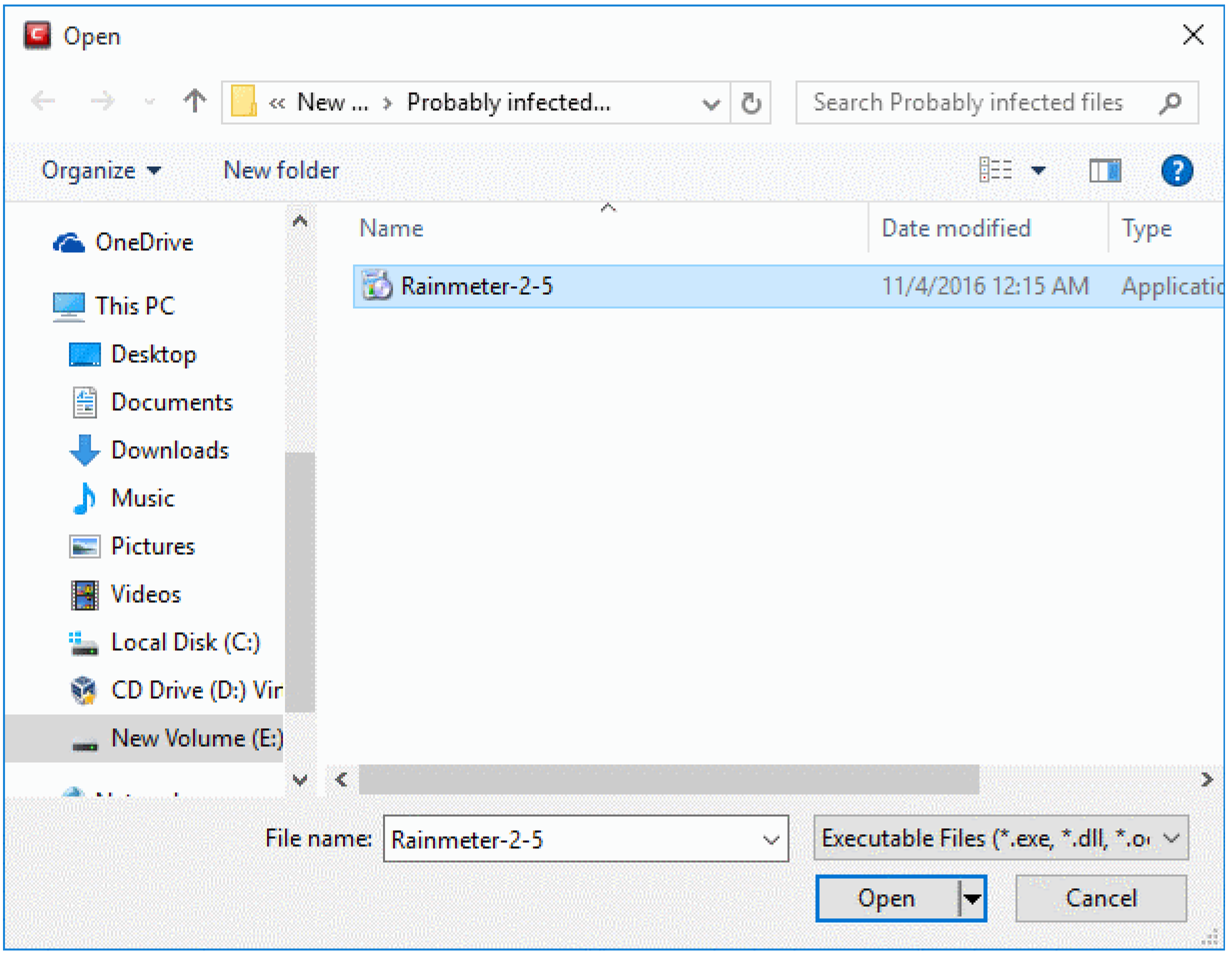
If you want to just add the applications in the drive partition/folder for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Source and Reputation filters and Options for the rule.

Adding a file based on its hash value

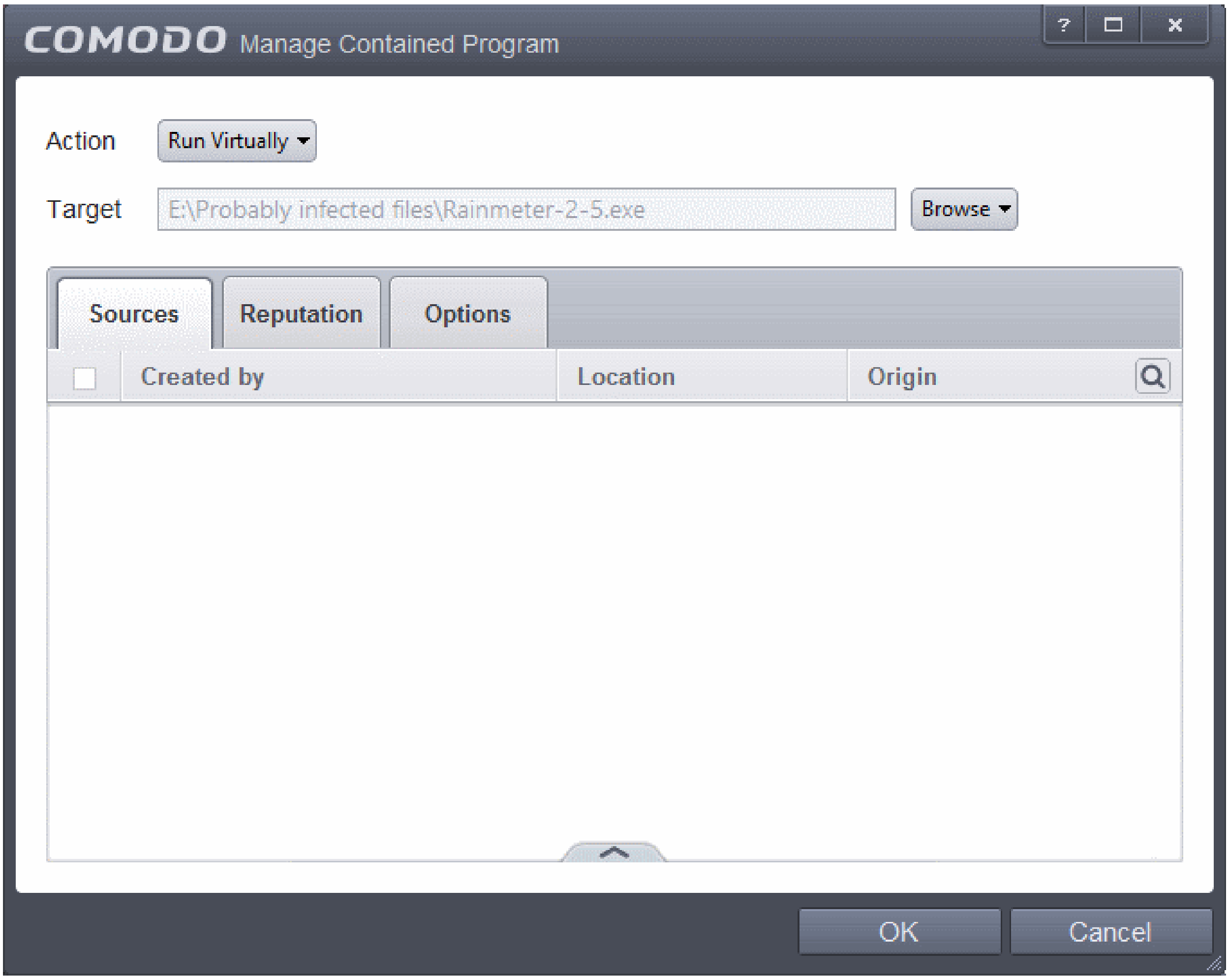
- Choose 'File Hash' from the 'Browse' drop-down.



- 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.



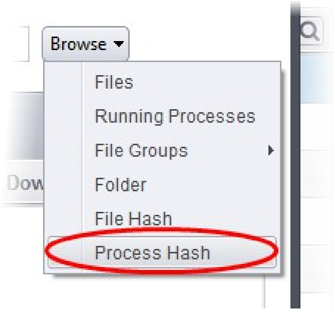
Action: Run Virtually

Target: E:\Probably infected files\Rainmeter-2-5.exe

If you want to just add the hash value of an application for a particular action as selected in Step 1 without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Source and Reputation filters and Options for the rule.

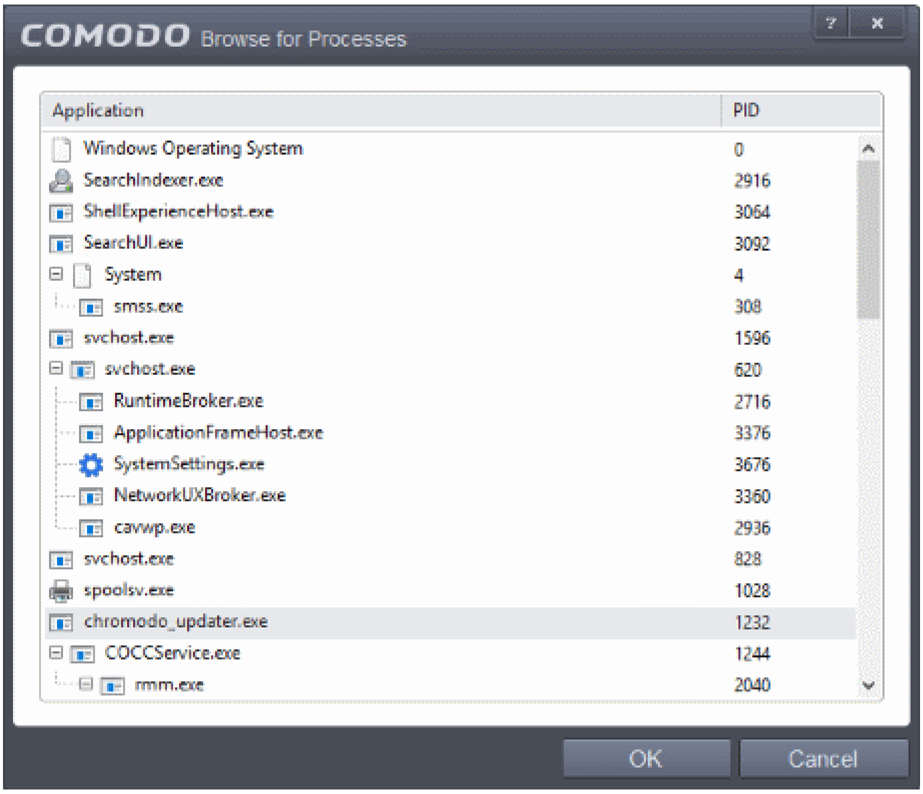
Adding an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



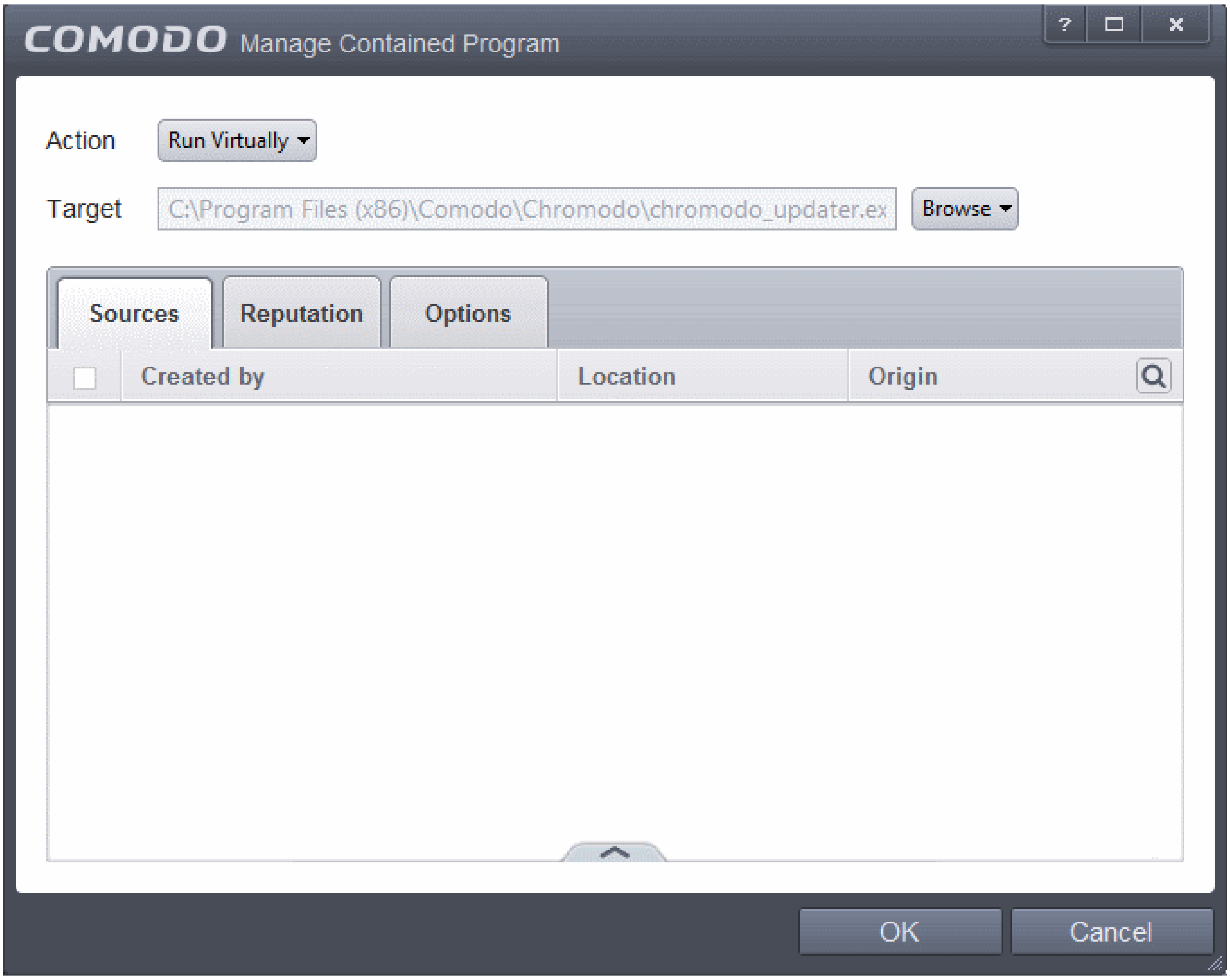
A list of currently running processes in your computer will be displayed.

- Select the process, whose hash value of the target application is to be added to target and click 'OK' from the Browse for Process dialog.



Application	PID
Windows Operating System	0
SearchIndexer.exe	2916
ShellExperienceHost.exe	3064
SearchUI.exe	3092
⊟ System	4
smss.exe	308
svchost.exe	1596
⊟ svchost.exe	620
RuntimeBroker.exe	2716
ApplicationFrameHost.exe	3376
SystemSettings.exe	3676
NetworkUXBroker.exe	3360
cavwp.exe	2936
svchost.exe	828
spoolsv.exe	1028
chromodo_updater.exe	1232
⊟ COCCService.exe	1244
⊟ rmm.exe	2040

The file will be added as target and will be run as per the action chosen in **Step 1**.



Action: Run Virtually

Target: C:\Program Files (x86)\Comodo\Chromodo\chromodo_updater.ex

Browse

If you want to just add the process hash value of an application for a particular action as selected in Step 1 without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Source and Reputation filters and Options for the rule.

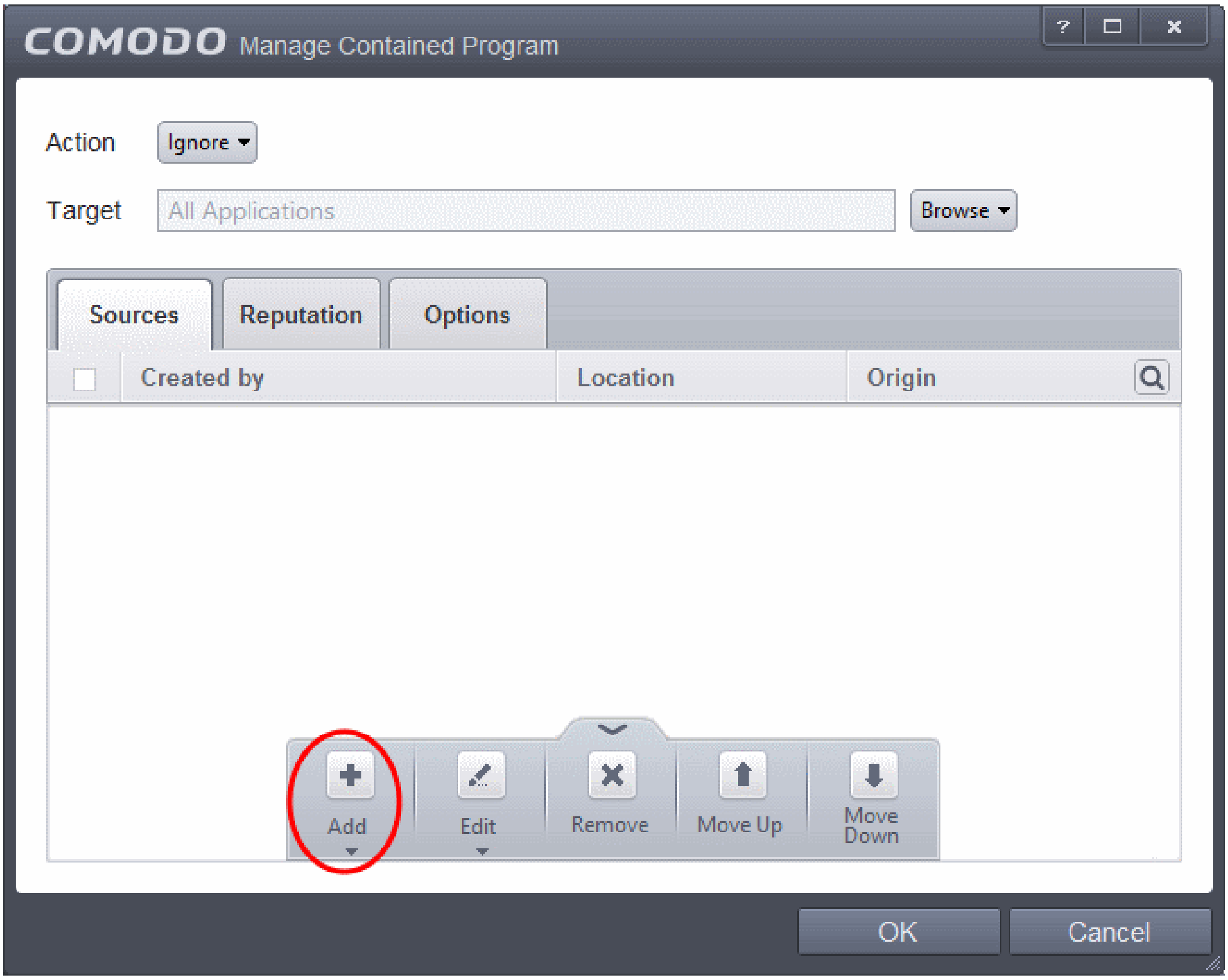
Step 3 – Select the Sources

If you want to include a number of items in a rule but want the rule to be applied only in certain conditions, then you can do so in this step. For example, if you want your target to be executables downloaded from the internet, then you would add 'All Applications' then apply a filter in 'Sources' tab. Another example is you want to exclude from containment any unrecognized files from your internal network share. You could create an ignore rule with 'All Applications' set as the target and specify your source as your intranet.

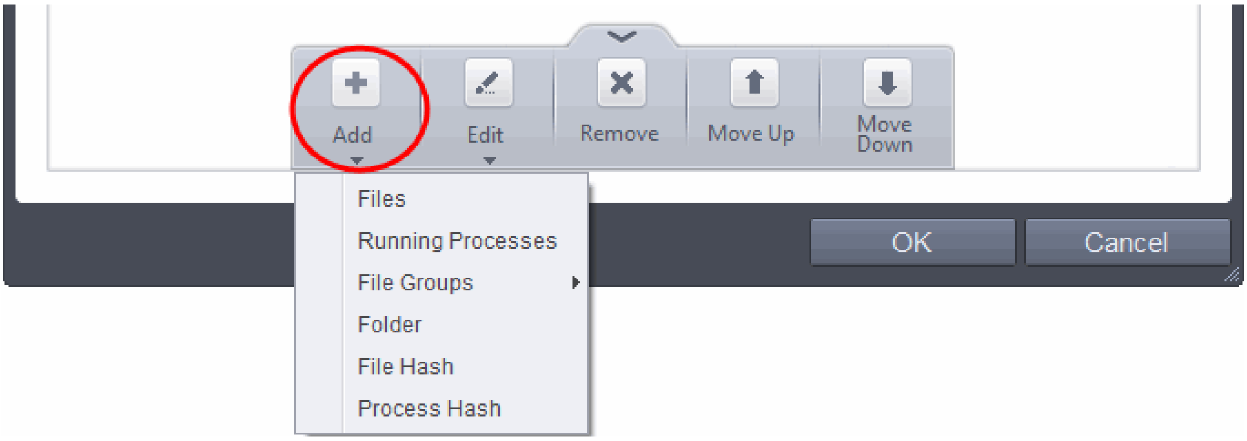
Please note that the 'Enable file source tracking' check box should be enabled in the 'Auto-Containment' screen for the source parameter to be taken account in the rule. If this is not enabled then the source parameter will be ignored and the rule will be applied based on the other parameters.

To add a source

- Click the handle at the bottom and then click Add from the options.

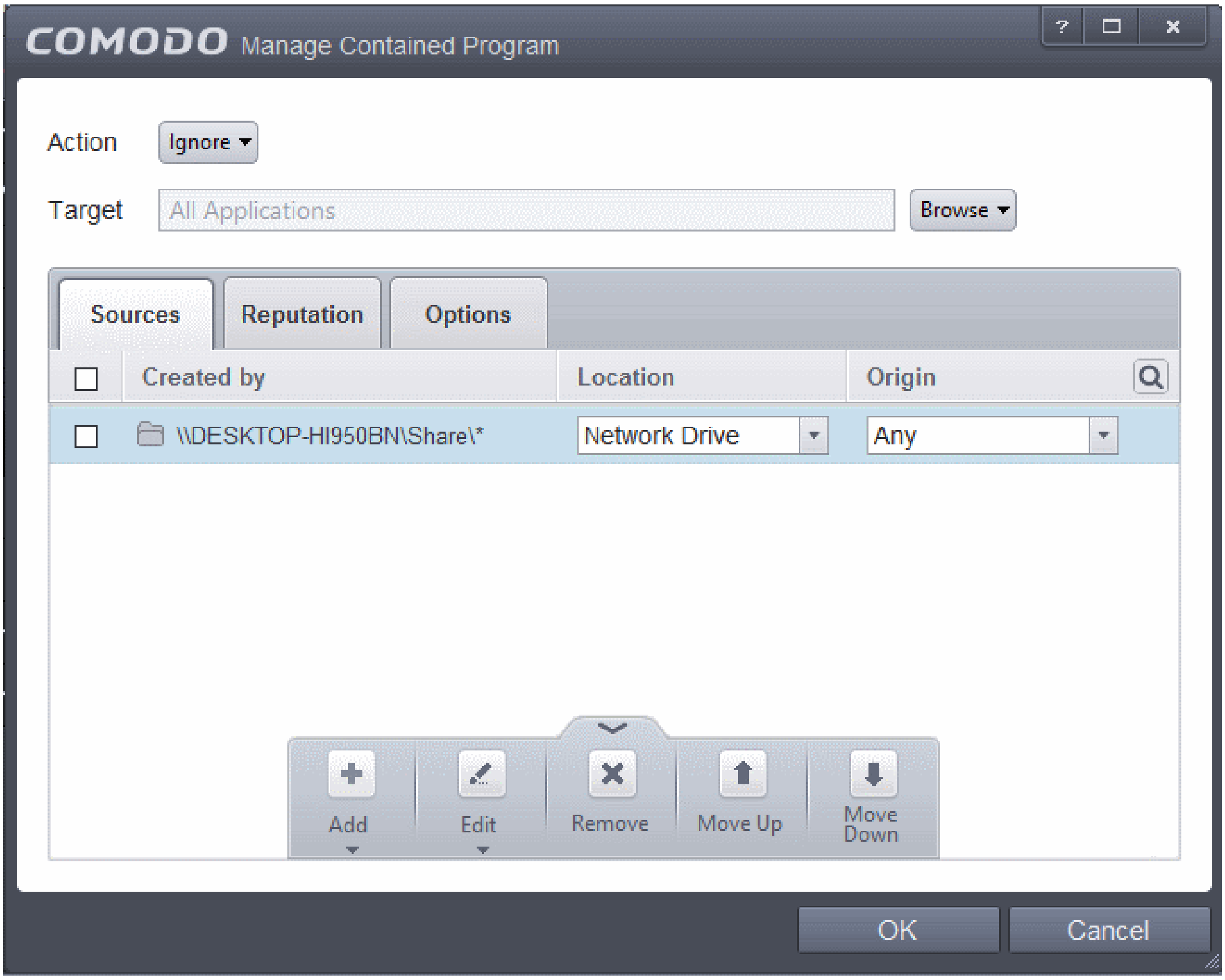


The options available are available are same as explained in Step 2.



The following example describes how to add an 'Ignore' rule for Unrecognized files from a network source:

- In Step 1, select the action as Ignore
- In Step 2, select the Target as File Groups > All Applications
- In Step 3, click the 'Add' button and select 'Folder'. Navigate to the source folder on the network and click 'OK'.



Action: Ignore

Target: All Applications

□	Created by	Location	Origin
□	\\DESKTOP-HI950BN\Share\*	Network Drive	Any

The selected network source folder will be added under the 'Created by' column and the screen displays the options to specify the location and from where the files were downloaded.

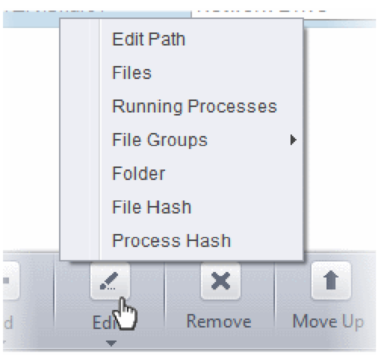
- **Location** – Apply the rule to files found in one of the following locations:
  - Any
  - Local Drive
  - Removable Drive
  - Network Drive

Since the source is located in a network, select Network Drive from the options.

- **Origin** – The options available are:
  - Any – The rule will apply to files that were downloaded to the source folder from both Internet and Intranet.
  - Internet – The rule will apply to files that were downloaded to the source folder from Internet only.
  - Intranet – The rule will apply to files that were downloaded to the source folder from Intranet only.

Repeat the process to add more source folders.

- Click the Edit button to change the source path from the options:



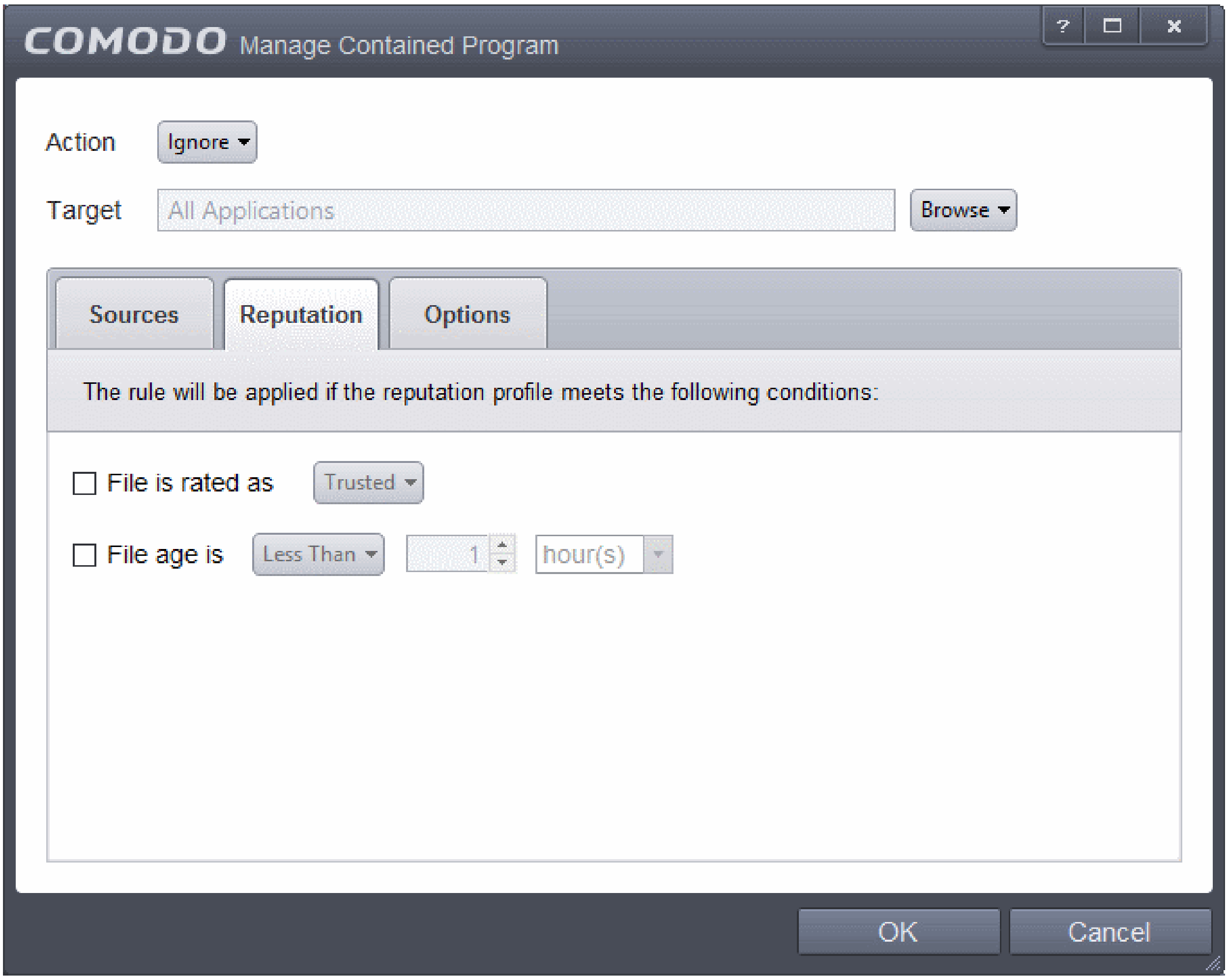
- To remove a source from the list, select it and click the Remove button.
- Use the 'Move Up' and 'Move Down' buttons to specify the order of source path.

If you want to just add the Sources for a particular action as selected in Step 1 without specifying rating of the file or options, then click 'OK'. The default values for Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure Reputation filters and Options for the rule.

Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options in Step 4.

Step 4 – Select the File Reputation

- Click the Reputation tab in the 'Manage Contained Program' interface.



Action: Ignore

Target: All Applications

The rule will be applied if the reputation profile meets the following conditions:

☐ File is rated as Trusted

☐ File age is Less Than 1 hour(s)

By default, the file rating is not selected meaning the rating could be Any. The options available are:

- **Trusted** – Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by CCS. Refer to the sections File Rating Settings and File List for more information.

- **Unrecognized** – Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section File List for more information.
- **Malware** – Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. Refer the section Unknown Files – The Scanning Process for more information.

By default, file age is not selected, so the age could be Any. The options available are:

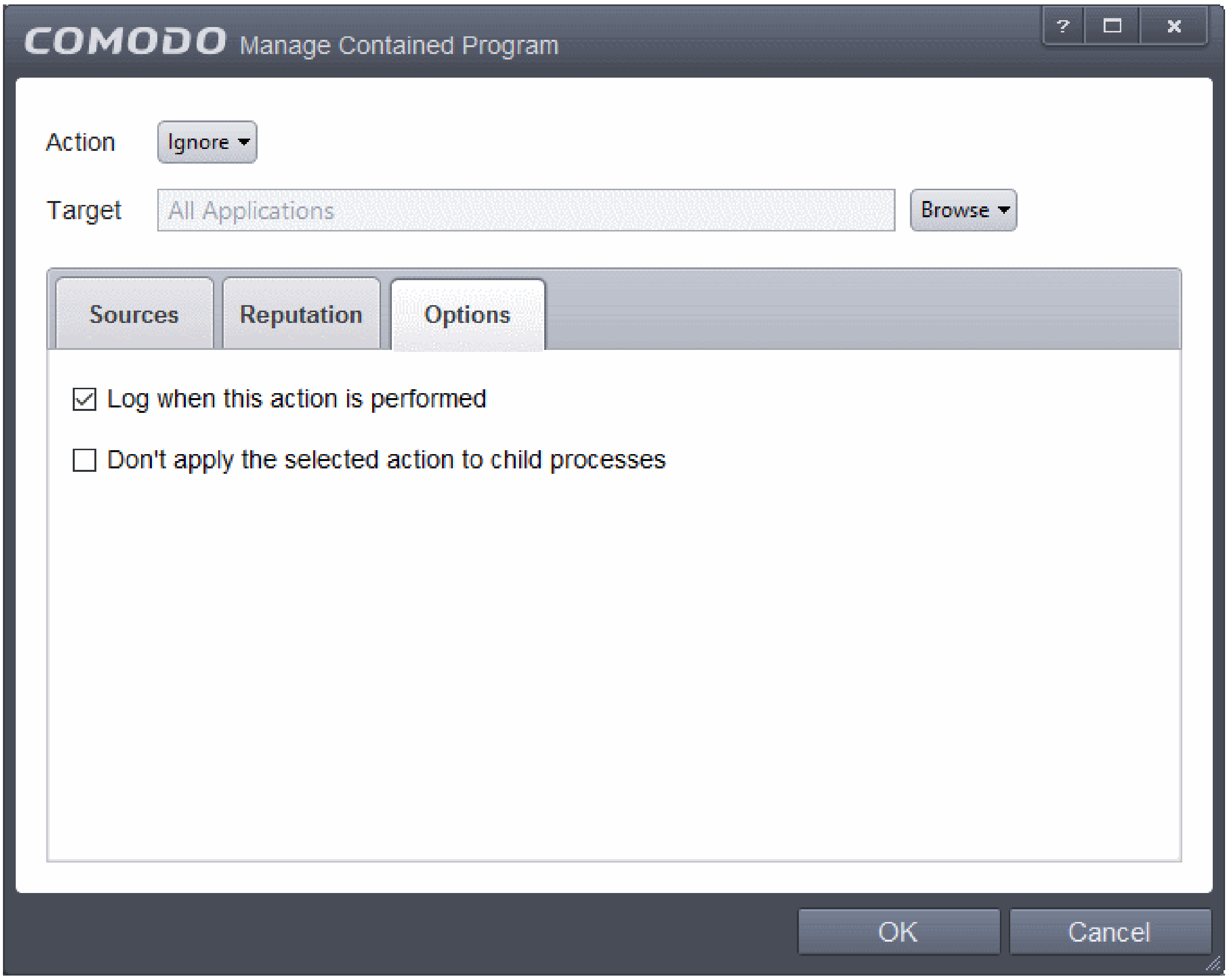
- Less Than – CCS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (*Default and recommended = 1 hour)*
- More Than - CCS will check for reputation if a 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 hour)*

Select the category from the options. Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options.

If you want to just add the Sources and Reputation for a particular action as selected in Step 1 without specifying the options, then click 'OK'. The default values for Options will be 'Log when this action is performed'. If required you can configure Options for the rule.

Step 5 – Select the Options

- Click the Options tab in the 'Manage Contained Program' interface.



Action: Ignore

Target: All Applications

Browse

☑ Log when this action is performed

□ Don't apply the selected action to child processes

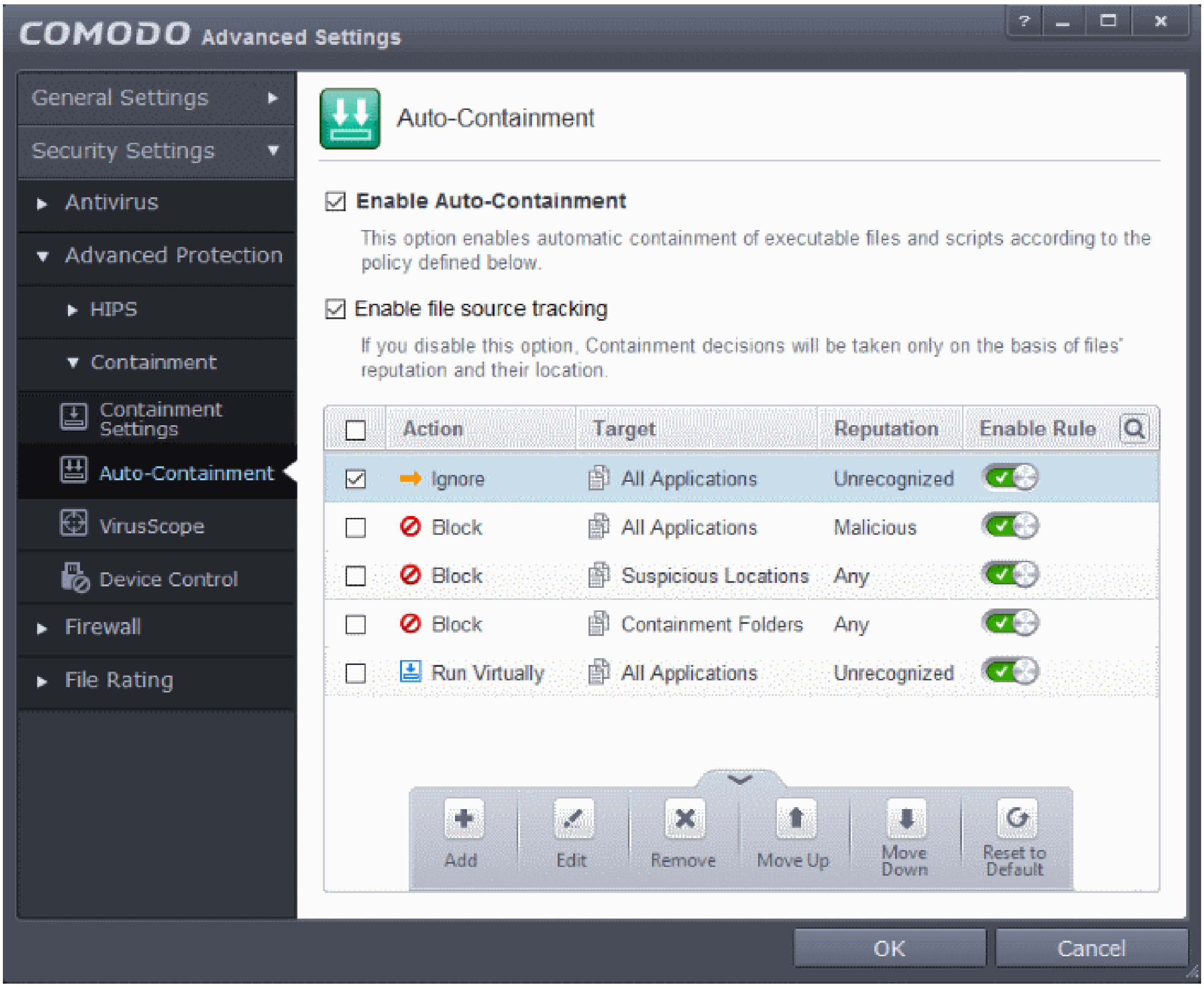
By default, the 'Log when this action is performed' The options available for Ignore action are:

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** – Child processes are the processes initiated by the applications. For example, the process may launch another app or plugin. CCS treats all child processes as individual processes and forces them to run as per their file rating and the containment rules.
    - This option is disabled by default, so the ignore rule will usually be applied to all child process of the target application(s).
    - If this option is enabled, then the Ignore rule will be applied only to the target application. All child processes will be checked individually and containment rules applied as per the child's file rating.
    - The 'Don't apply to child processes' option is available only for the 'Ignore' action. For 'Run Restricted' and 'Run Virtually', the following options are available:
- **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. Refer to the section Manage Quarantined Items for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



Auto-Containment

☑ **Enable Auto-Containment**

This option enables automatic containment of executable files and scripts according to the policy defined below.

☑ Enable file source tracking

If you disable this option, Containment decisions will be taken only on the basis of files' reputation and their location.

□	Action	Target	Reputation	Enable Rule
☑	Ignore	All Applications	Unrecognized	✓
□	Block	All Applications	Malicious	✓
□	Block	Suspicious Locations	Any	✓
□	Block	Containment Folders	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓

Editing an Auto-Containment Rule

- To edit an auto-containment rule, select it from the list and click 'Edit' from the options.

The Manage Contained Program interface will be displayed. The procedure is similar to adding Adding an Auto-Containment Rule.

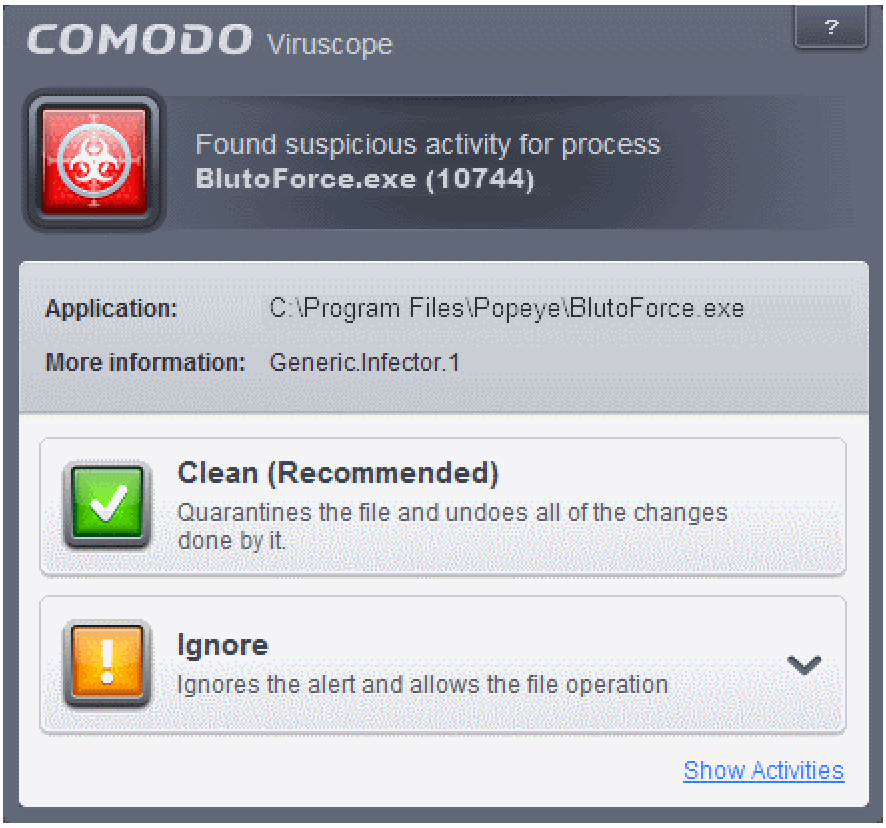
- Click 'OK' to save the changes to the rule.

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.

6.2.2.9. Viruscope

Viruscope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Viruscope represents a valuable addition to the core process-monitoring functionality of CCS by introducing the ability to undo the potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented in order to run correctly.

Viruscope alerts give you the opportunity to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer.



Found suspicious activity for process
BlutoForce.exe (10744)

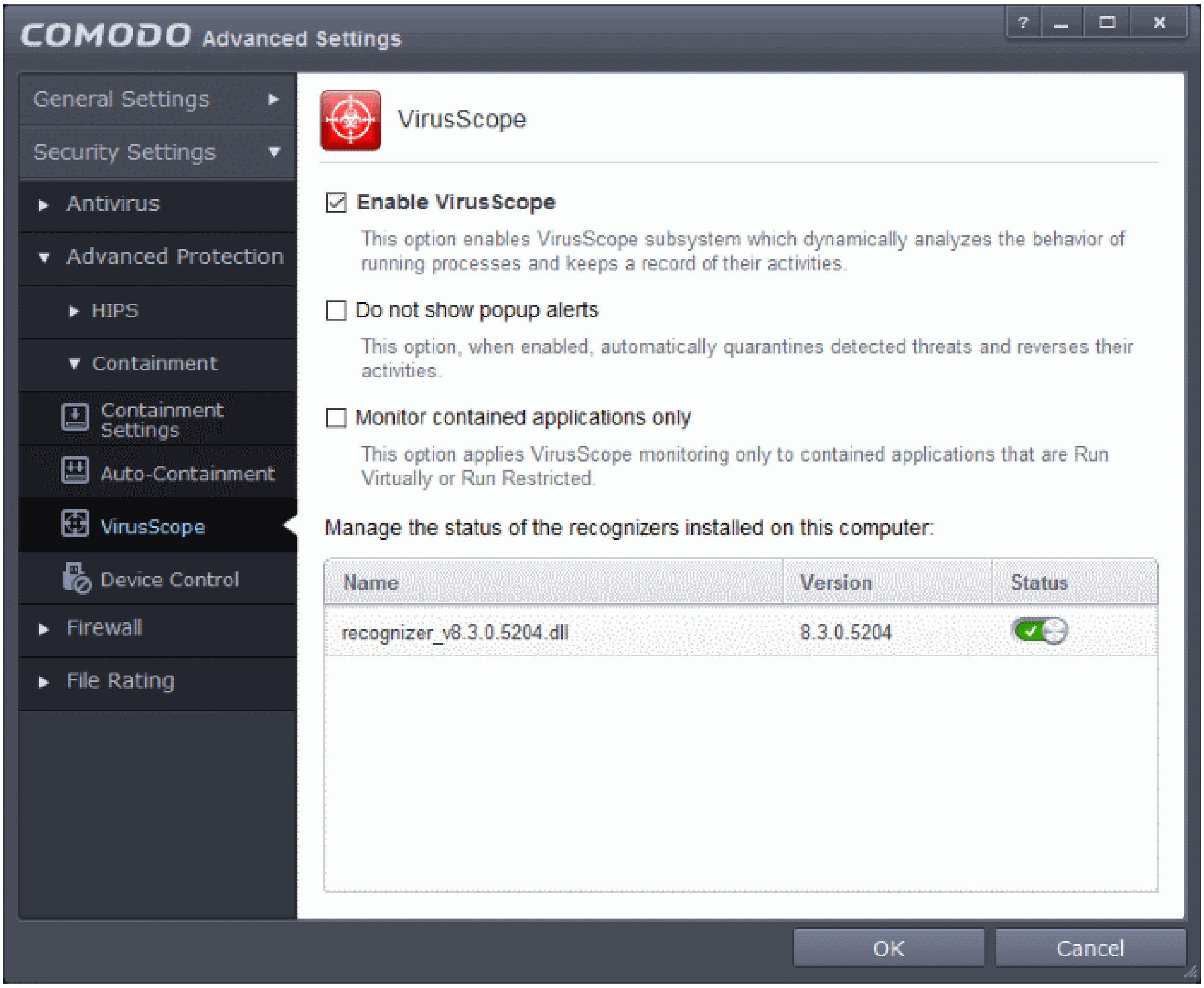
Application: C:\Program Files\Popeye\BlutoForce.exe

More information: Generic.Infector.1

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

Ignore
Ignores the alert and allows the file operation

The 'Viruscope' configuration panel can be accessed by clicking 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Advanced Protection > Viruscope'.



VirusScope

☑ Enable VirusScope

This option enables VirusScope subsystem which dynamically analyzes the behavior of running processes and keeps a record of their activities.

□ Do not show popup alerts

This option, when enabled, automatically quarantines detected threats and reverses their activities.

□ Monitor contained applications only

This option applies VirusScope monitoring only to contained applications that are Run Virtually or Run Restricted.

Manage the status of the recognizers installed on this computer:

Name	Version	Status
recognizer_v8.3.0.5204.dll	8.3.0.5204	✓

Viruscope Settings

Viruscope monitors the activities of all processes, regardless of whether they are running normally or inside the container. If suspicious activity is detected, Viruscope will generate a pop-up alert that allows you to block or allow the activity.

- **Enable Viruscope** - Allows you to enable or disable Viruscope. If enabled, the Viruscope monitors the activities of all the running processes and generates alerts on suspicious activities. ***(Default = Enabled)***
- **Do not show popup alerts** - Allows you to configure whether or not to show Viruscope alerts when a suspicious activity is recognized. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed. (***Default = Enabled***)
- **Monitor contained applications only** – If enabled, Viruscope will only monitor the processes of contained applications. It will not monitor processes running directly on the host. ***(Default = Enabled***)

Manage the status of recognizers installed on this computer

Viruscope detects zero-day malware by analyzing the behavior and actions of an application using the periodically updated 'Viruscope Recognizer' files.

Each 'recognizer' file installed on your system during periodical program updates of CCS, contains the sets of behaviors that Viruscope needs to look out for. If you disable a particular recognizer, then Viruscope will no longer raise an alert if an application exhibits the behaviors referenced in the file. 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 Viruscope false positives.

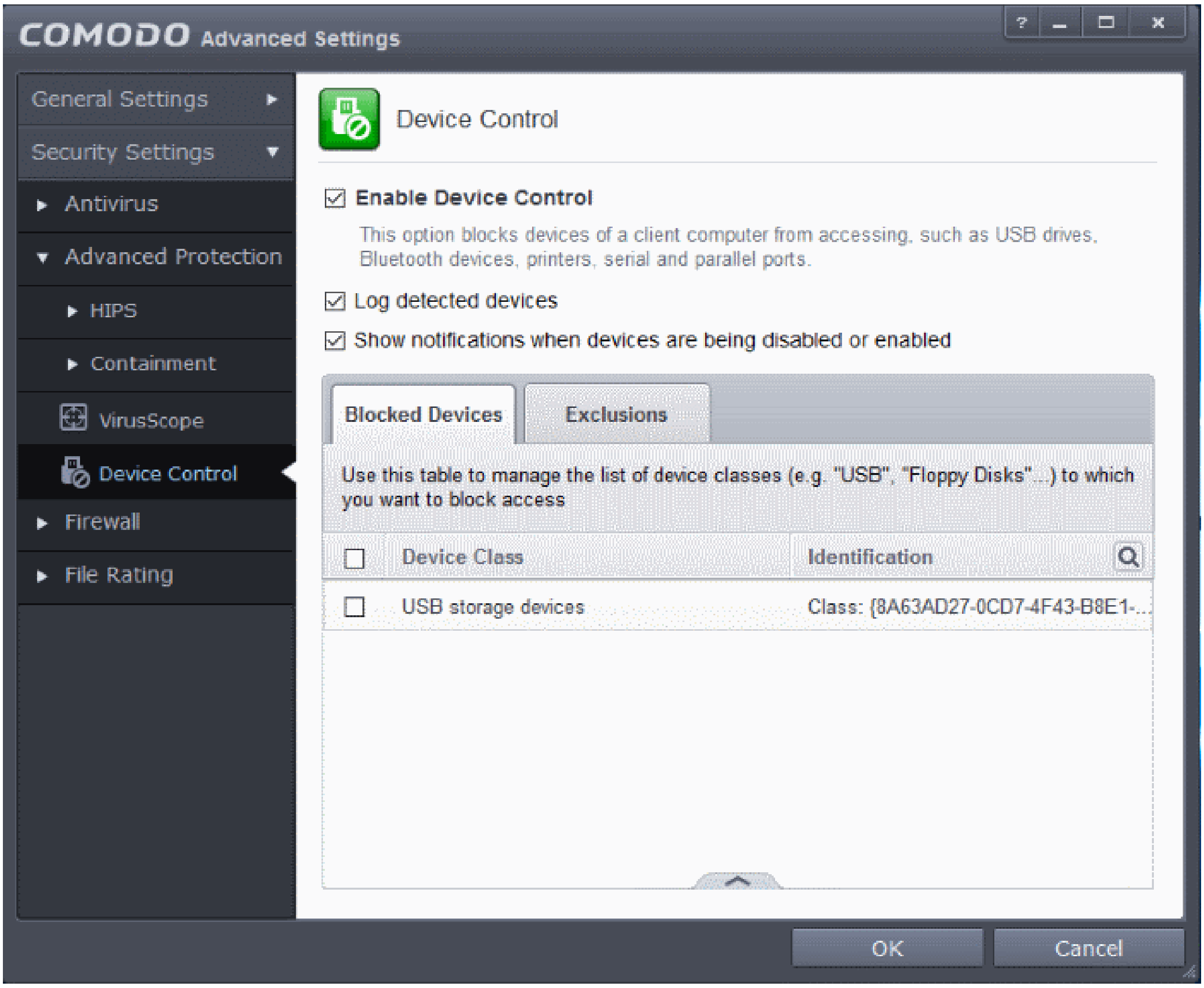
The table below the 'Manage the status of recognizers installed on this computer' displays the list of recognizer file available on your system with their version details.

- To disable a recognizer, use the toggle switch in 'Status' column.

6.2.2.10. Device Control Settings

The 'Device Control Settings' section allows you to configure which types of external devices are allowed to connect to an endpoint. Device Control Settings can also be configured as part of an ITSM profile.

- To open device control, click: Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Advanced Protection > Device Control:



☑ Enable Device Control

This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, serial and parallel ports.

☑ Log detected devices

☑ Show notifications when devices are being disabled or enabled

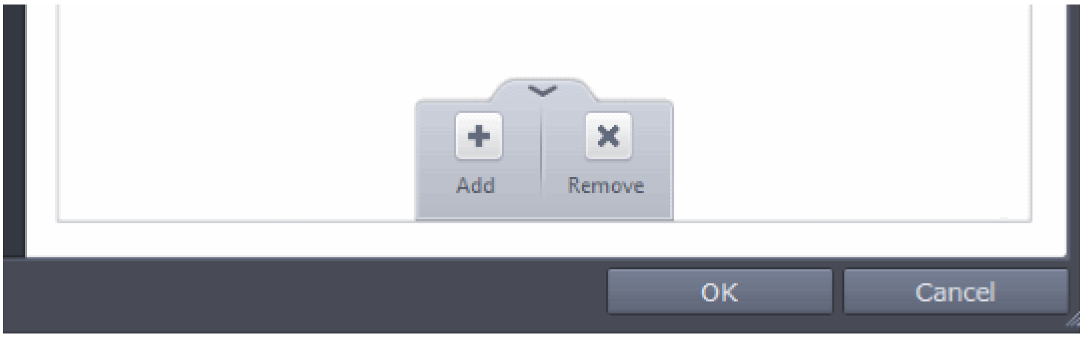
Use this table to manage the list of device classes (e.g. "USB", "Floppy Disks"...) to which you want to block access

□	Device Class	Identification
□	USB storage devices	Class: {8A63AD27-0CD7-4F43-B8E1-...

- **Enable Device Control** - Enable or disable device control functionality. If enabled you should specify banned device types in the 'Blocked Devices' section ***(Default = Enabled)***
- **Log Detected Devices** – If enabled, CCS will log events by external devices (Default = Disabled)
- **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.

General Navigation:

Clicking the handle at the bottom of the interface opens the following controls:

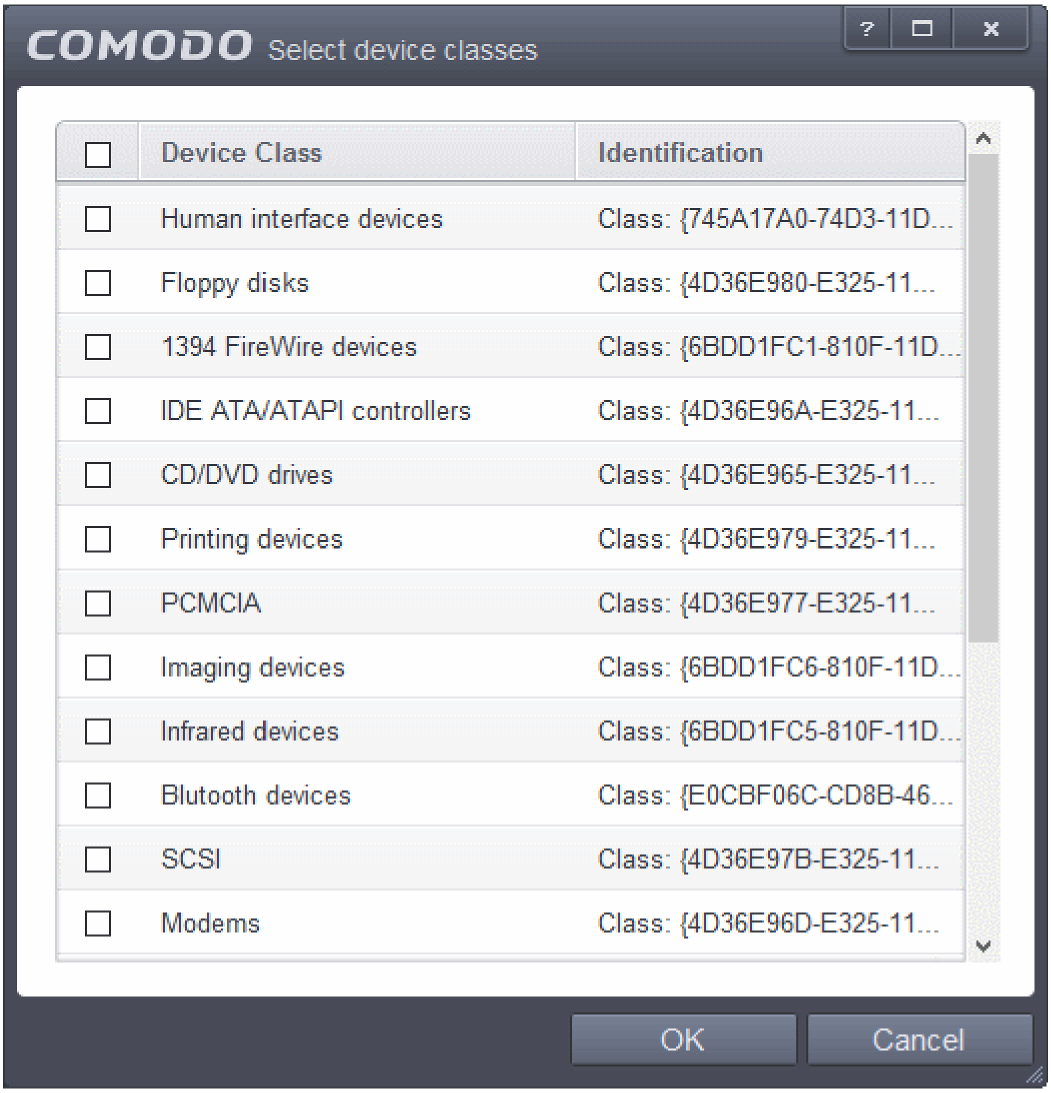


- **Add** - Allows the user to Add a new device or device class.
- **Remove** – Deletes the selected device or device class.

- Click 'OK' to save your settings.

To block a device class and specify exceptions:

- Click the handle at the bottom of the interface and then click the 'Add' button.
- This will open the 'Select device classes' screen:


COMODO Select device classes

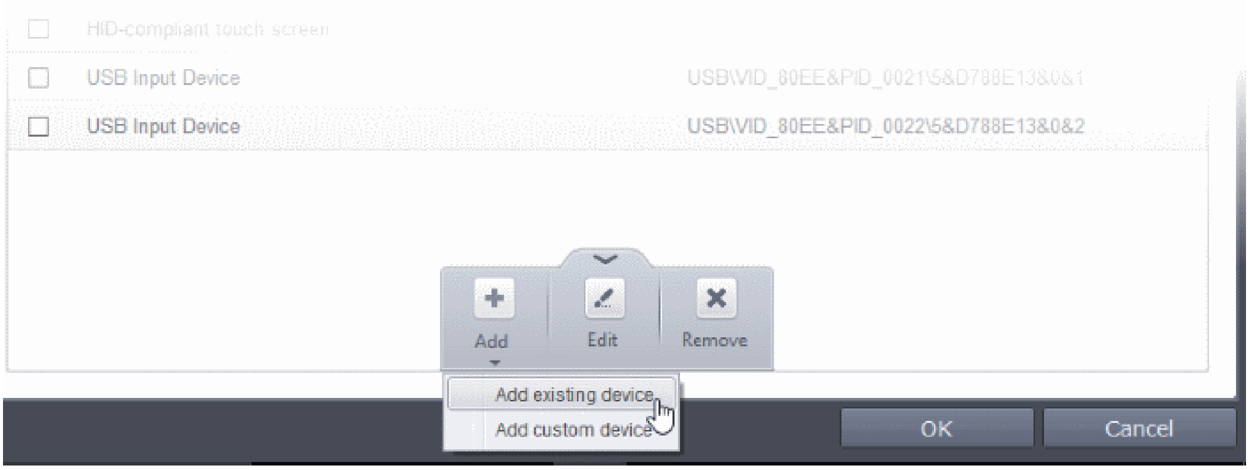
□	Device Class	Identification
□	Human interface devices	Class: {745A17A0-74D3-11D...
□	Floppy disks	Class: {4D36E980-E325-11...
□	1394 FireWire devices	Class: {6BDD1FC1-810F-11D...
□	IDE ATA/ATAPI controllers	Class: {4D36E96A-E325-11...
□	CD/DVD drives	Class: {4D36E965-E325-11...
□	Printing devices	Class: {4D36E979-E325-11...
□	PCMCIA	Class: {4D36E977-E325-11...
□	Imaging devices	Class: {6BDD1FC6-810F-11D...
□	Infrared devices	Class: {6BDD1FC5-810F-11D...
□	Blutooth devices	Class: {E0CBF06C-CD8B-46...
□	SCSI	Class: {4D36E97B-E325-11...
□	Modems	Class: {4D36E96D-E325-11...

- Choose the type of device you wish to block. For example, USB devices, Bluetooth devices or firewire devices.

- Click 'OK'

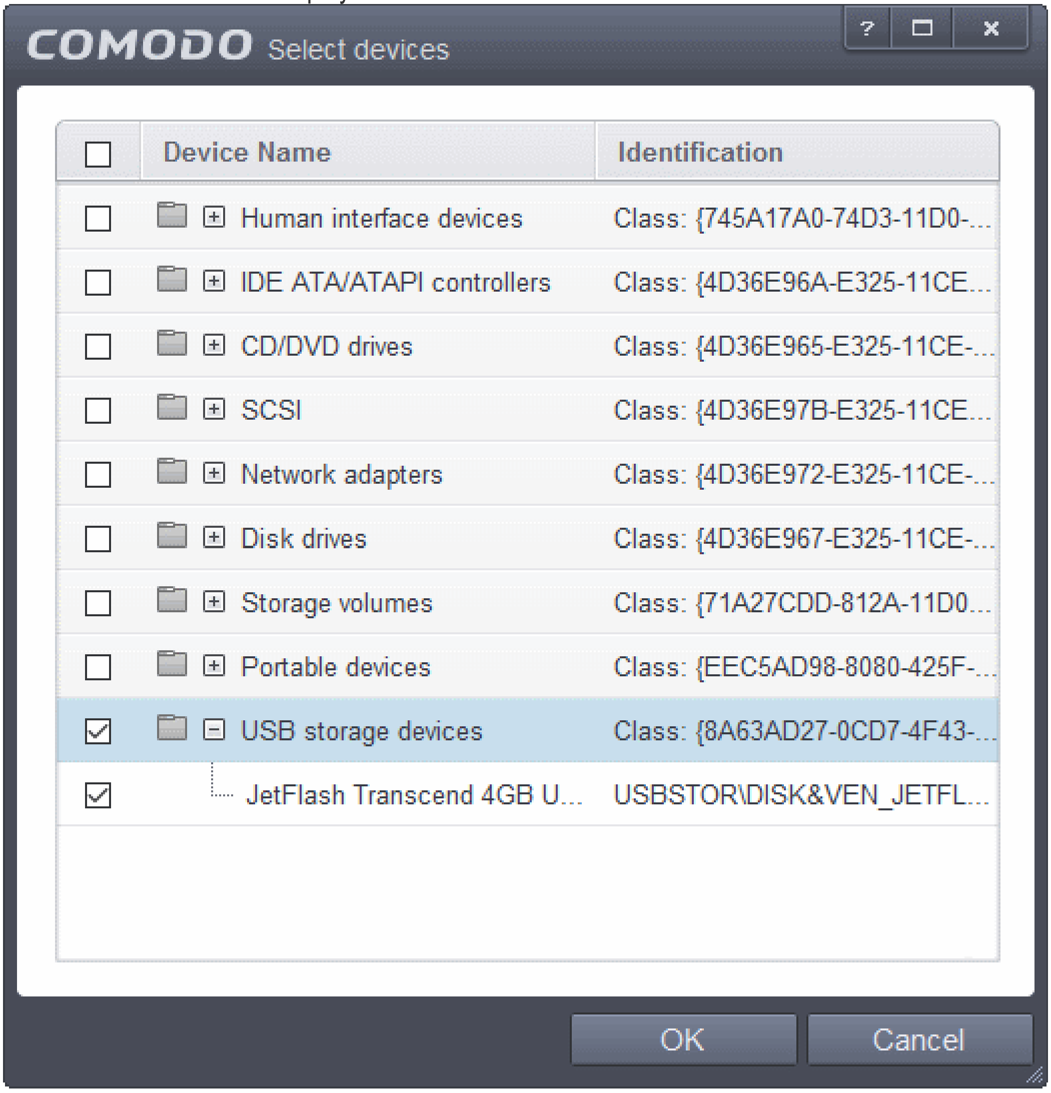
If you want to allow access to specific devices that fall within a blocked device class:

- Make sure the external device is connected to the computer
- Click the 'Exclusions' tab
- Click the handle at the bottom then 'Add'


HID-compliant touch screen
USB Input Device
USBVID_80EE&PID_0021\5&D788E13&0&1
USB Input Device
USBVID_80EE&PID_0022\5&D788E13&0&2
Add
Edit
Remove
Add existing device
Add custom device
OK
Cancel

- Click 'Add existing device' from the options

The 'Select devices' screen will be displayed:

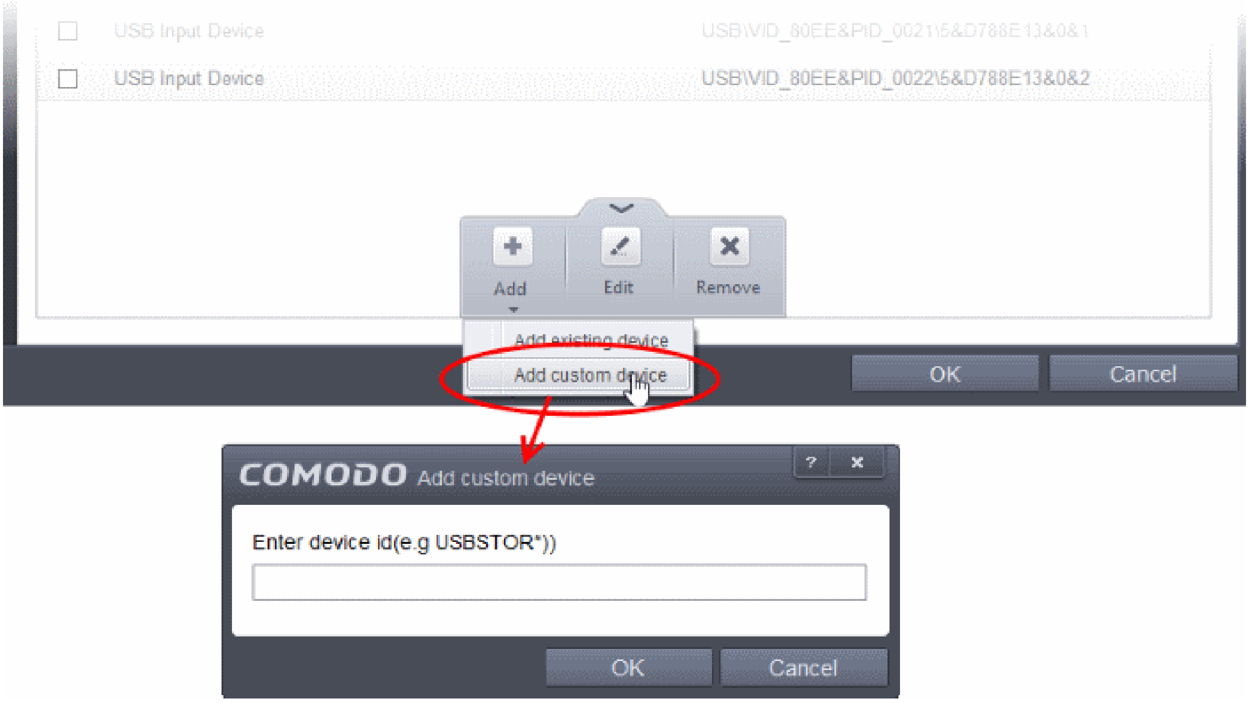


□	Device Name	Identification
□	⊞ Human interface devices	Class: {745A17A0-74D3-11D0-...
□	⊞ IDE ATA/ATAPI controllers	Class: {4D36E96A-E325-11CE...
□	⊞ CD/DVD drives	Class: {4D36E965-E325-11CE-...
□	⊞ SCSI	Class: {4D36E97B-E325-11CE...
□	⊞ Network adapters	Class: {4D36E972-E325-11CE-...
□	⊞ Disk drives	Class: {4D36E967-E325-11CE-...
□	⊞ Storage volumes	Class: {71A27CDD-812A-11D0...
□	⊞ Portable devices	Class: {EEC5AD98-8080-425F-...
☑	⊟ USB storage devices	Class: {8A63AD27-0CD7-4F43-...
☑	JetFlash Transcend 4GB U...	USBSTOR\DISK&VEN_JETFL...

  - 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 a specific type of SANDISK devices that is 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 handle at the bottom then 'Add' from the options:

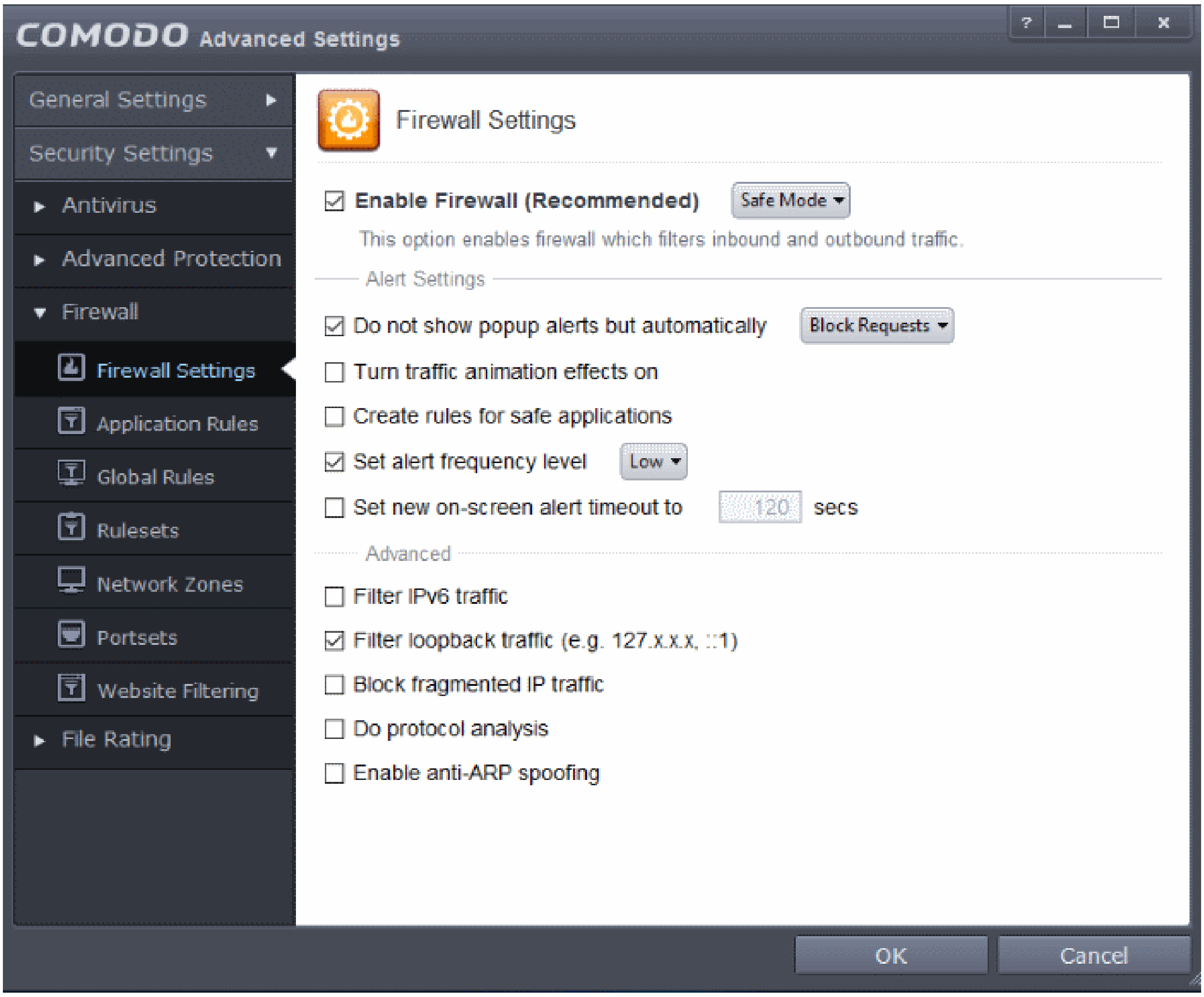


□ USB Input Device USB\VID_80EE&PID_0021\5&D788E13&0&1
□ USB Input Device USB\VID_80EE&PID_0022\5&D788E13&0&2
Add
Edit
Remove
Add existing device
Add custom device
OK
Cancel
COMODO Add custom device
Enter device id(e.g USBSTOR*))
OK
Cancel

- 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.

6.2.3. Firewall Settings

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. It hides your computer's ports from hackers and it helps stop malware from transmitting your confidential data over the internet. Comodo Firewall also makes it easy for you to specify exactly which applications are allowed to connect to the internet and immediately warns you when there is suspicious activity.



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do not show popup alerts but automatically Block Requests

☐ Turn traffic animation effects on

☐ Create rules for safe applications

☑ Set alert frequency level Low

☐ Set new on-screen alert timeout to 120 secs

Advanced

☐ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☐ Block fragmented IP traffic

☐ Do protocol analysis

☐ Enable anti-ARP spoofing

The 'Firewall Settings' area has several sub-sections that allow you to configure overall firewall behavior; configure network zones and portsets and (for advanced users) to configure traffic filtering rules on an application specific and global basis.

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

- Firewall Behavior Settings - Configure settings that govern the overall behavior of the firewall component.
- Application Rules - View, create and modify rules that determine the network access privileges of individual applications or specific types of application
- Global Rules - View, create and modify rules that apply to all traffic flowing in and out of your computer.
- Rule Sets - Predefined collections of firewall rules that can be applied, out-of-the-box, to Internet capable applications such as browsers, email clients and FTP clients.
- Network Zones - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- Portsets - Predefined groups of regularly used ports that can used and reused when creating traffic filtering rules.
- Website Filtering – Create website filtering rules which let you determine which sites certain users can or cannot access.

Background note on rules: Both application rules and global rules are consulted when the firewall is determining whether or not to allow or block a connection attempt.

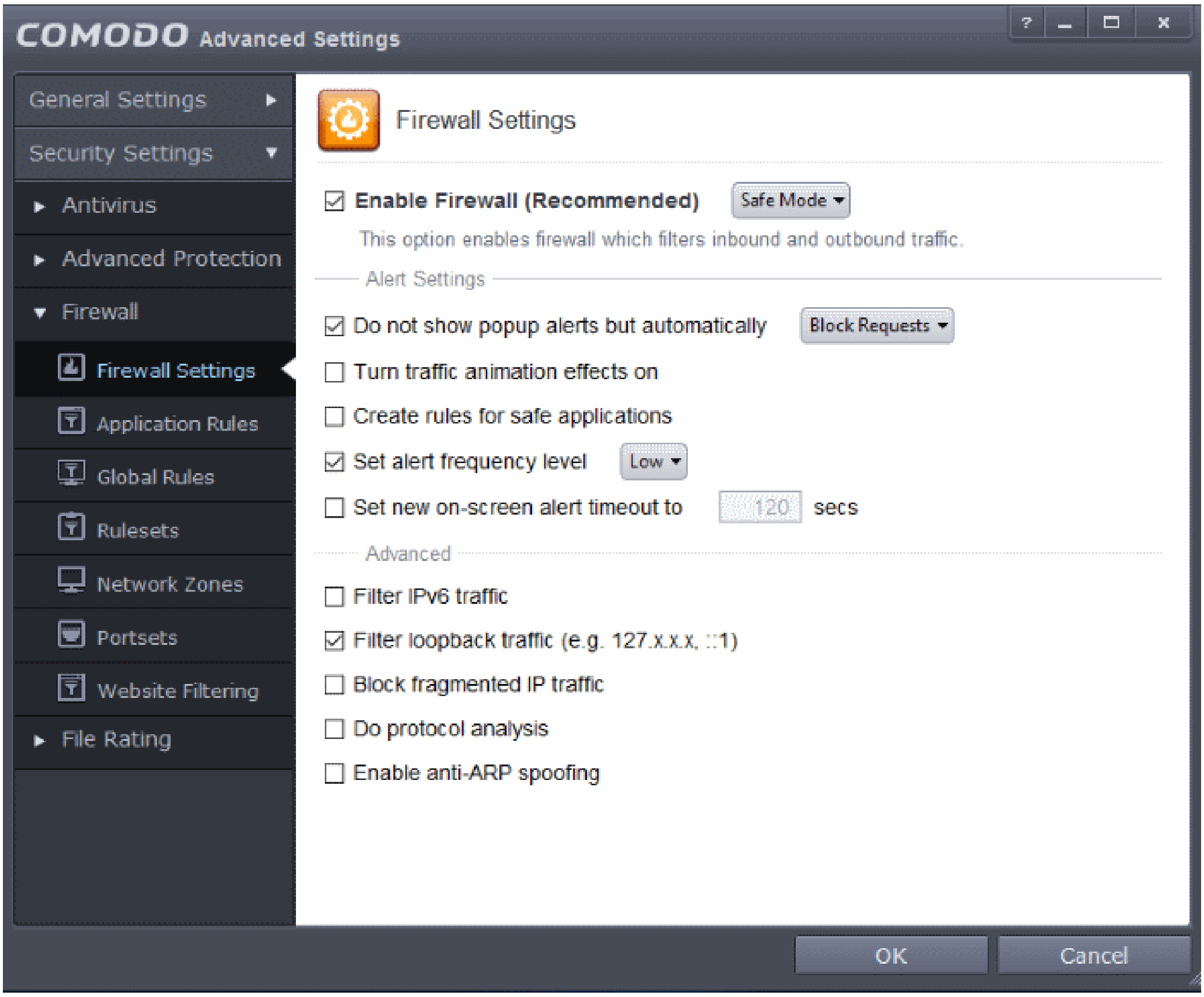
- For Outgoing connection attempts, the application rules are consulted first then the global rules.

- For Incoming connection attempts, the global rules are consulted first then application specific rules.

6.2.3.1. Firewall Behavior Settings

The 'Firewall Settings' panel allows you to quickly configure overall Firewall behavior and is divided into three main areas:

- General Settings
- Alert Settings
- Advanced Settings



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do not show popup alerts but automatically Block Requests

□ Turn traffic animation effects on

□ Create rules for safe applications

☑ Set alert frequency level Low

□ Set new on-screen alert timeout to 120 secs

Advanced

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

□ Block fragmented IP traffic

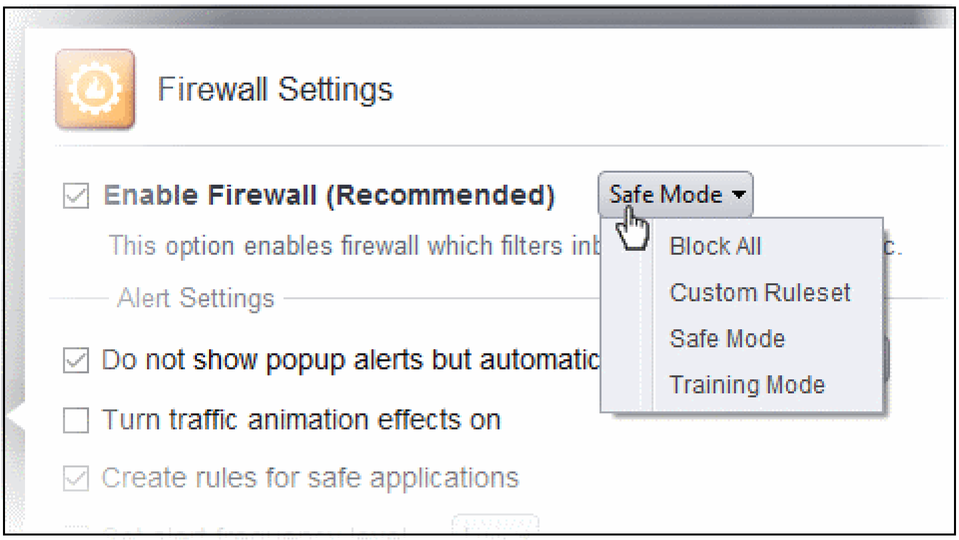
□ Do protocol analysis

□ Enable anti-ARP spoofing

General Settings

- **Enable Firewall** - Allows you to enable or disable Firewall protection.(***Default and recommended = Enabled***)

If enabled, you can also choose the security level from the accompanying drop-down menu:



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode ▾

This option enables firewall which filters inb c.

Alert Settings

☑ Do not show popup alerts but automatic

□ Turn traffic animation effects on

☑ Create rules for safe applications

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).

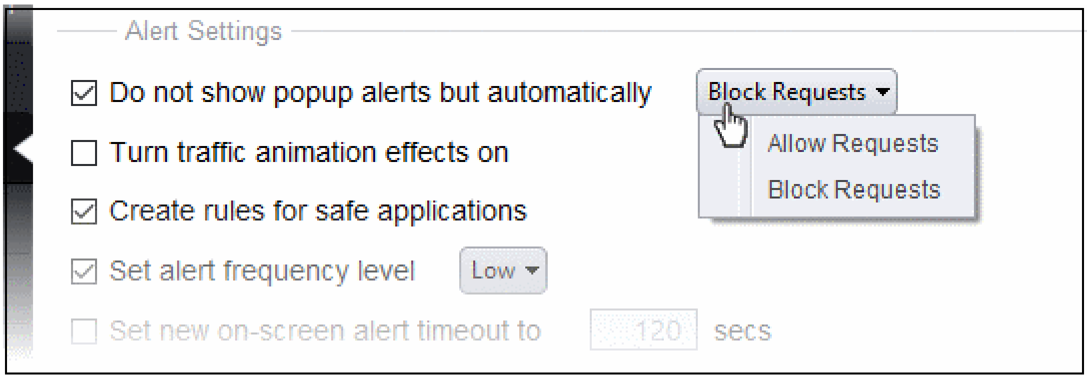
  If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This 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)***: While filtering network traffic, the firewall automatically creates rules that allow all traffic for the components of applications certified as 'Safe' by Comodo, if the checkbox Create rules for safe applications is selected. 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 deploys the predefined firewall ruleset 'Trusted Application' onto the application.

  'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.
- **Training Mode** : The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the correct network access rights.

Alert Settings

- **Do not show popup alerts but automatically** - 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 but automatically' will minimize disturbances but at some loss of user awareness. (***Default = Enabled***)

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'.



Alert Settings

☑ Do not show popup alerts but automatically

☐ Turn traffic animation effects on

☑ Create rules for safe applications

☑ Set alert frequency level Low

☐ Set new on-screen alert timeout to 120 secs

- **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.

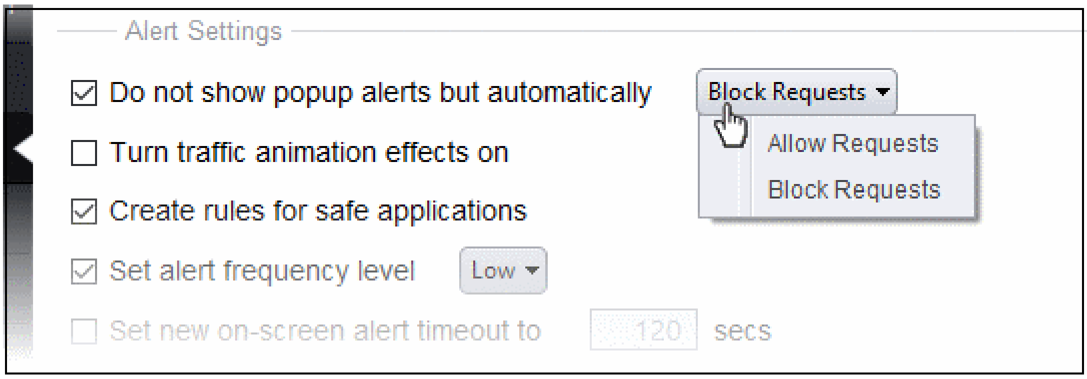
If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the shield. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer. Clear 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 under File Rating Settings;
  - 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 saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, 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 the '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** - Enabling this option allows you to configure the amount of alerts that Comodo Firewall generates, from the drop-down. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages. (***Default=Enabled***)



Alert Settings

☑ Do not show popup alerts but automatically

☐ Turn traffic animation effects on

☑ Create rules for safe applications

☑ Set alert frequency level Low

☐ Set new on-screen alert timeout to 120 secs

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 have not (yet) decided to 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

Comodo Firewall features advanced detection settings to 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 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

- **Filter loopback traffic**: Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately received by it. This involves no connection outside your computer to the Internet or a local network. The IP address of the loopback network is 127.0.0.1, which you might have heard referred to, under its domain name of 'http://localhost', i.e. 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 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

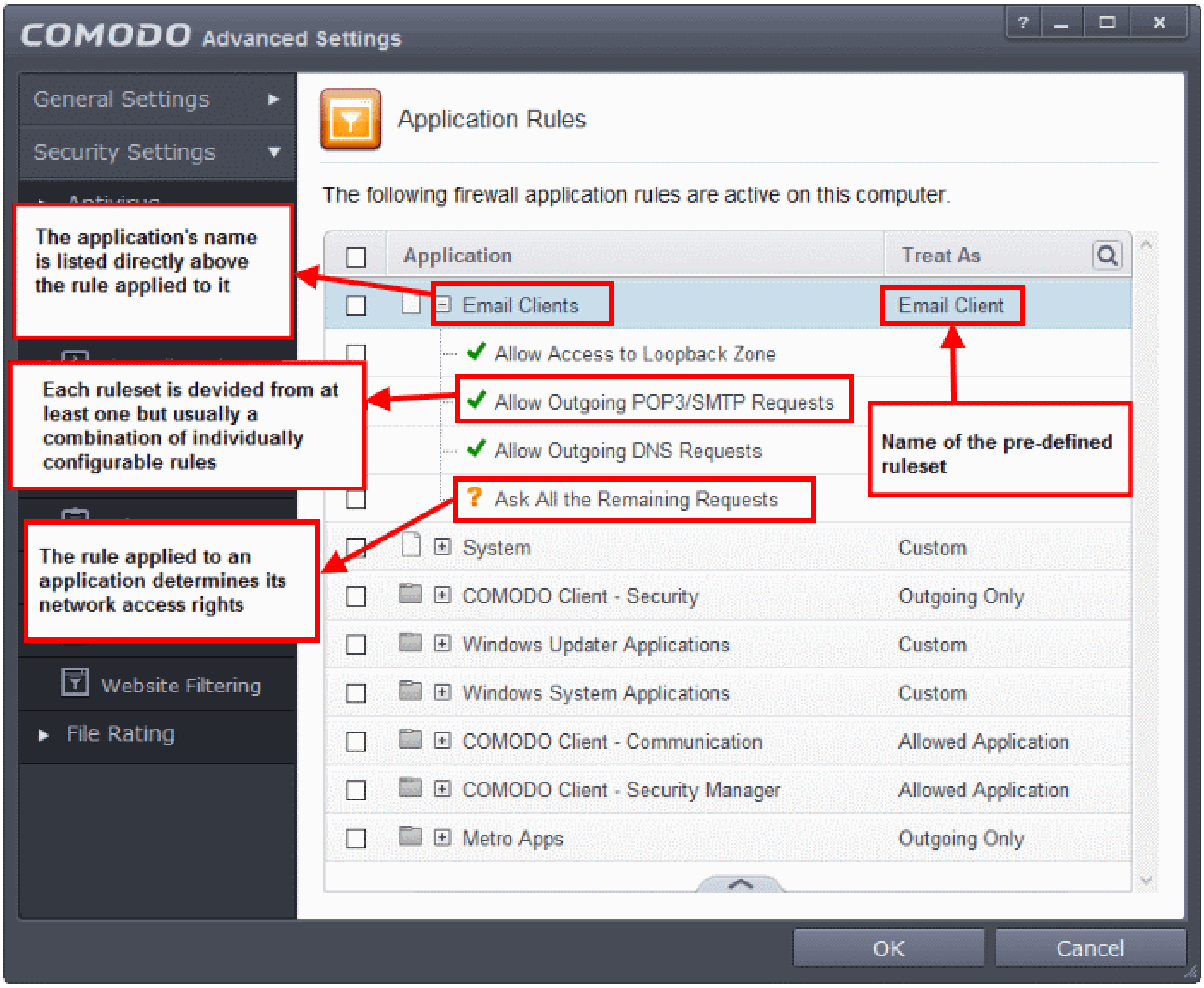
IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time. (***Default = Disabled***)

- **Do Protocol Analysis** - Protocol Analysis is key to the detection of fake packets used in denial of service attacks. Checking this option means Comodo Firewall checks 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***)

6.2.3.2. Application Rules

Overview of Rules and Rulesets

Whenever an application makes a request for internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Ruleset that has been specified for the application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual network 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.



The following firewall application rules are active on this computer.

Application	Treat As
⊟ Email Clients	Email Client
✓ Allow Access to Loopback Zone	
✓ Allow Outgoing POP3/SMTP Requests	
✓ Allow Outgoing DNS Requests	
? Ask All the Remaining Requests	
⊞ System	Custom
⊞ COMODO Client - Security	Outgoing Only
⊞ Windows Updater Applications	Custom
⊞ Windows System Applications	Custom
⊞ COMODO Client - Communication	Allowed Application
⊞ COMODO Client - Security Manager	Allowed Application
⊞ Metro Apps	Outgoing Only

The application's name is listed directly above the rule applied to it

Each ruleset is devided from at least one but usually a combination of individually configurable rules

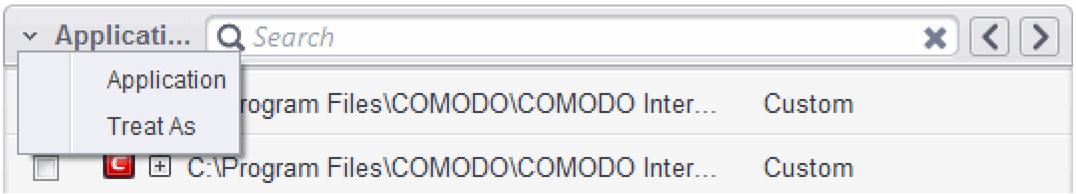
The rule applied to an application determines its network access rights

Name of the pre-defined ruleset

The first column, **Application**, displays a list of the applications on your system for which a Firewall ruleset has been deployed. If the application belongs to a file group, then all member applications assume the ruleset of the file group. The second column, **Treat as**, column displays the name of the Firewall ruleset assigned to the application or group of applications in column one.

You can use the search option to find a specific name in the list.

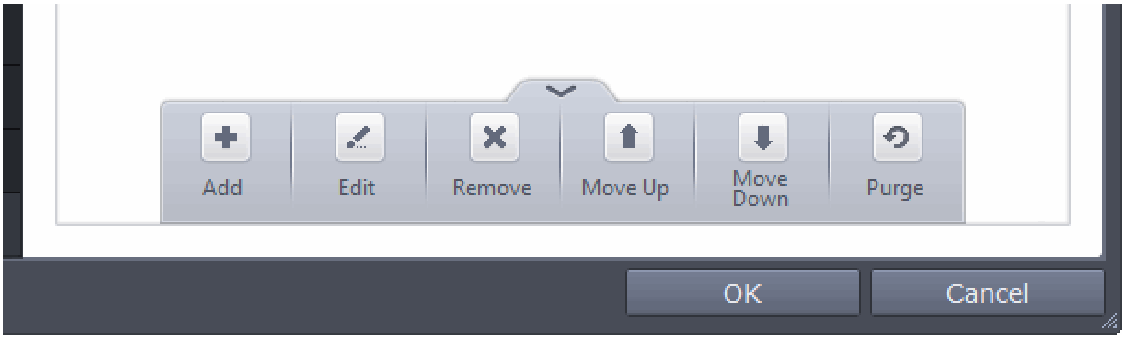
To use the search option, click the search icon 🔍 at the far right in the column header.


Applicati...
Search
Application
Treat As
rogram Files\COMODO\COMODO Inter... Custom
C:\Program Files\COMODO\COMODO Inter... Custom

- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

General Navigation:

Clicking the handle at the bottom of the interface opens an option panel:



- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the sections 'Creating or Modifying Firewall Rules' and 'Adding and Editing a Firewall Control Rule'.
- **Edit** - Allows the user to modify the Firewall rule or ruleset of the selected application. See the sections 'Creating or Modifying Firewall Rules' and 'Adding and Editing a Firewall Rule'.
- **Remove** - Deletes the selected ruleset.
- **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.

If you wish to modify the firewall ruleset for an application:

- Double click on the application name to begin 'Creating or Modifying Firewall Rules'
- Select the application name click the handle at the bottom right and choose 'Edit' from the options to begin 'Creating or Modifying Firewall Rules'

If you wish to modify an individual rule within the ruleset:

- Double click on the specific rule to begin 'Adding and Editing a Firewall Rule'

or

- Select the specific rule and click the handle at the bottom center and choose 'Edit' from the options to begin 'Adding and Editing a Firewall Rule'

Users can also re-prioritize rulesets by clicking the handle at the bottom and select 'Move Up' or 'Move Down' from the options.

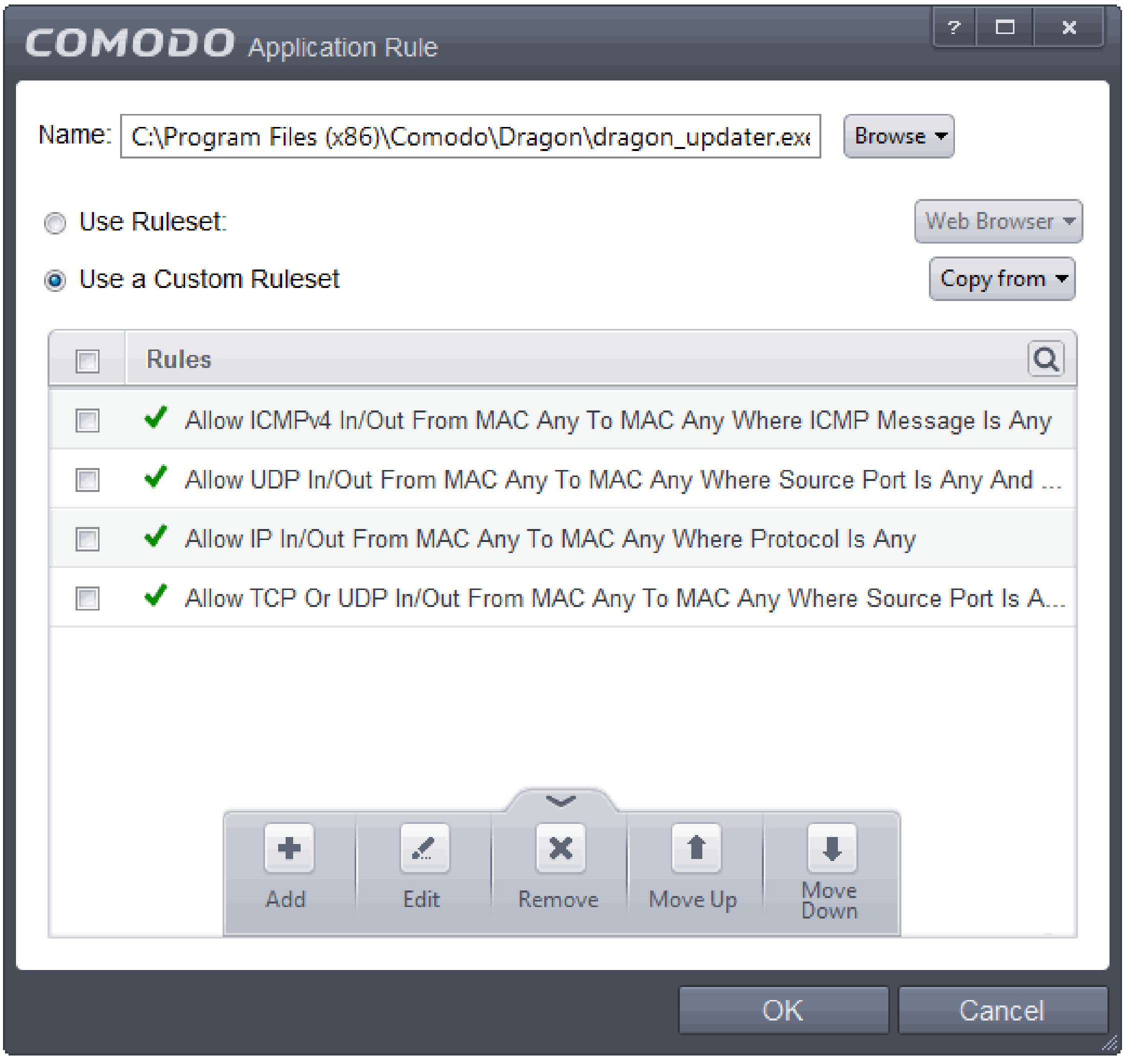
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. 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 Application Rule

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

○ Use Ruleset: Web Browser

● Use a Custom Ruleset — Copy from

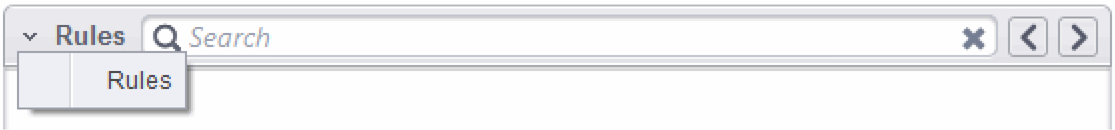
□	Rules
□	✓ Allow ICMPv4 In/Out From MAC Any To MAC Any Where ICMP Message Is Any
□	✓ Allow UDP In/Out From MAC Any To MAC Any Where Source Port Is Any And ...
□	✓ Allow IP In/Out From MAC Any To MAC Any Where Protocol Is Any
□	✓ Allow TCP Or UDP In/Out From MAC Any To MAC Any Where Source Port Is A...

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 clicking the handle at the bottom center and select 'Move Up' or 'Move Down' from the options. To begin creating Firewall rulesets, first read 'Overview of Rules and Rulesets' then 'Creating and Modifying Firewall Rulesets'

You can use the search option to find a specific rule in the list.

To use the search option, click the search icon 🔍 at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option

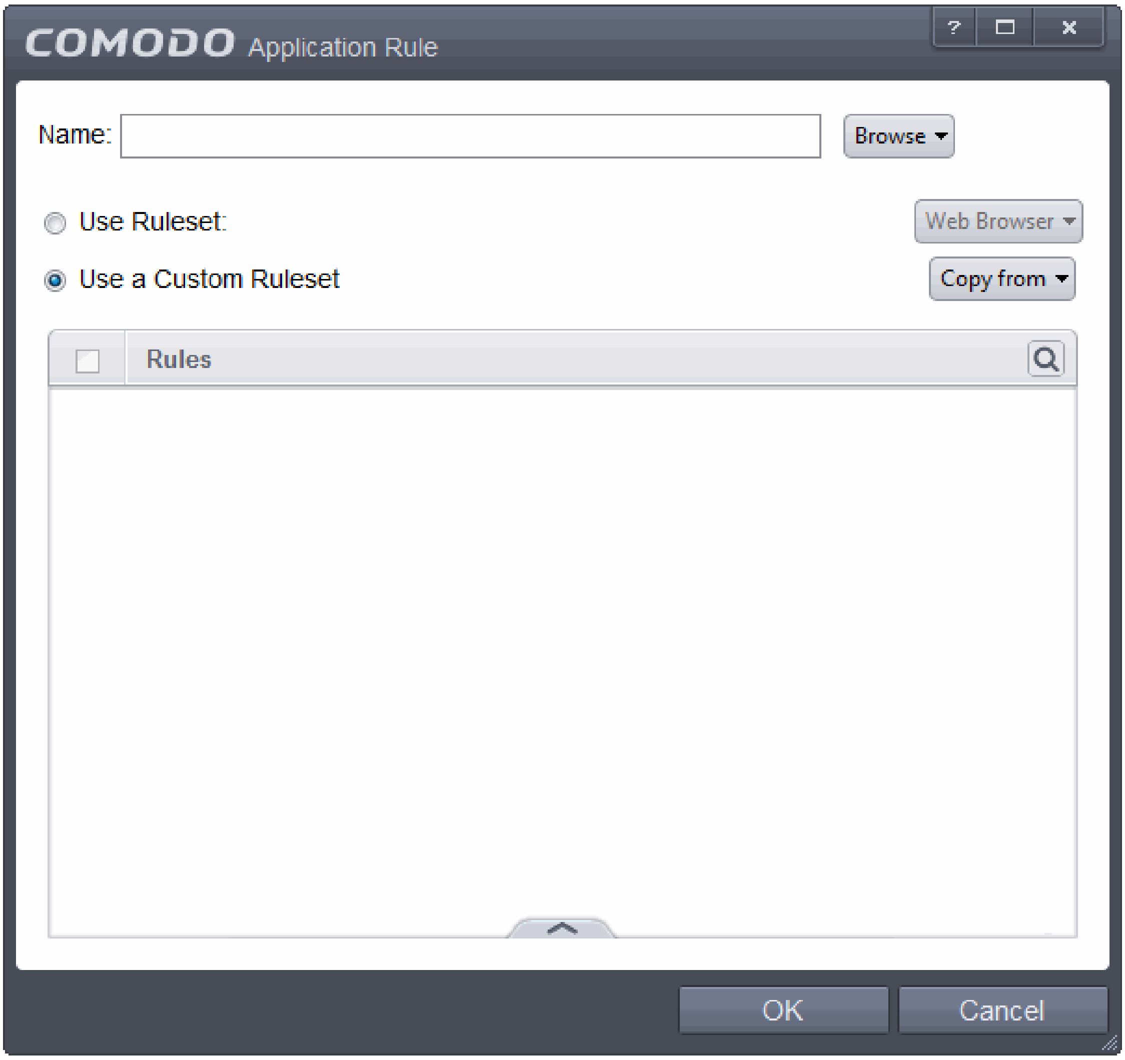
Creating and Modifying Firewall Rulesets

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.

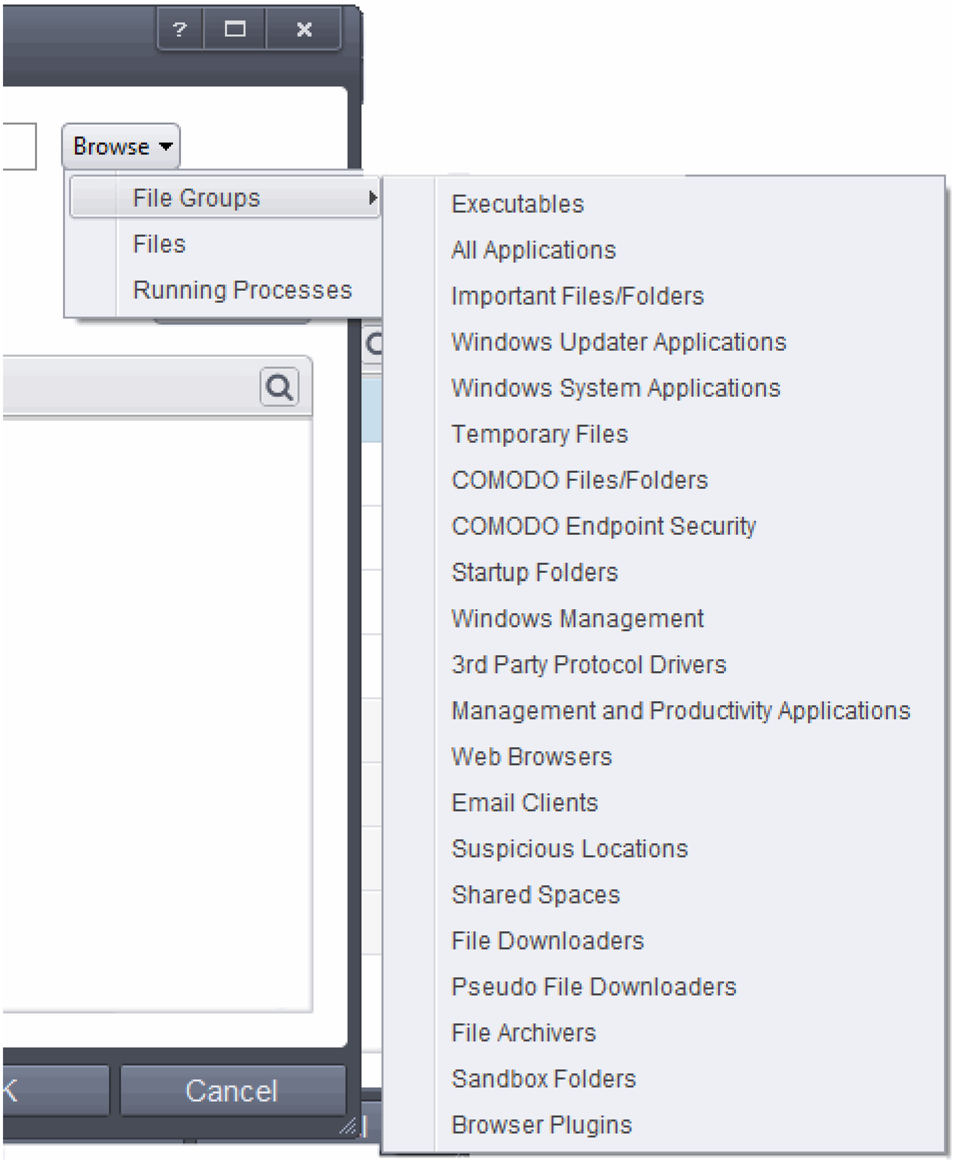
Step 1 - Select the application that you wish the ruleset is to be applied

If you wish to define a ruleset for a new application (i.e. one that is not already listed) then click the handle from the Application Rules interface and select 'Add' from the options. This brings up the 'Application Rule' interface shown below:



Because this is a new application, the 'Application Path' field is blank. (If you are modifying an existing ruleset, then this interface shows the individual rules for that application's ruleset).

- Click 'Browse' button.

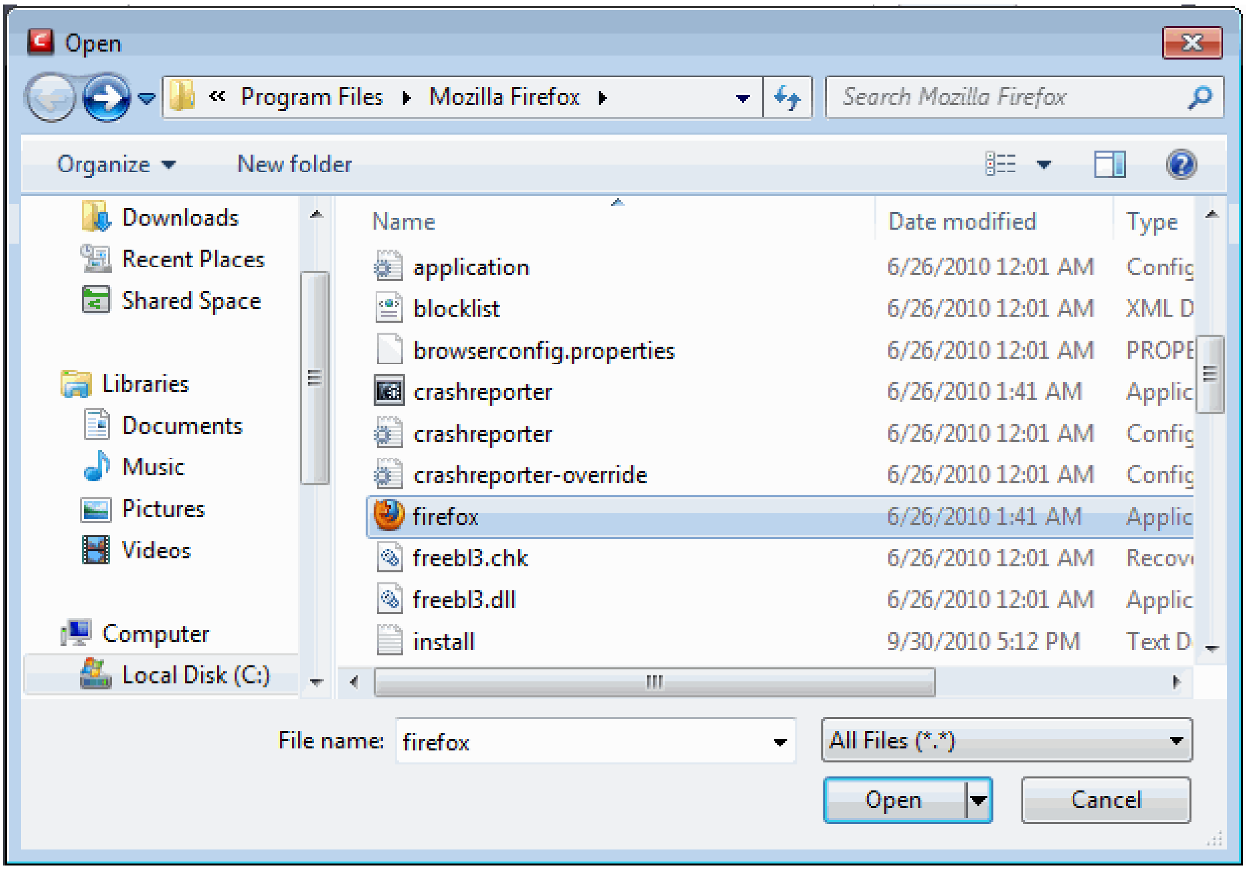


You now have 3 methods available to choose the application for which you wish to create a ruleset - File Groups; Files and Running Processes and

i. **File Groups** - choosing this option 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 . 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.

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 below, we have decided to create a firewall ruleset for the Opera web browser.

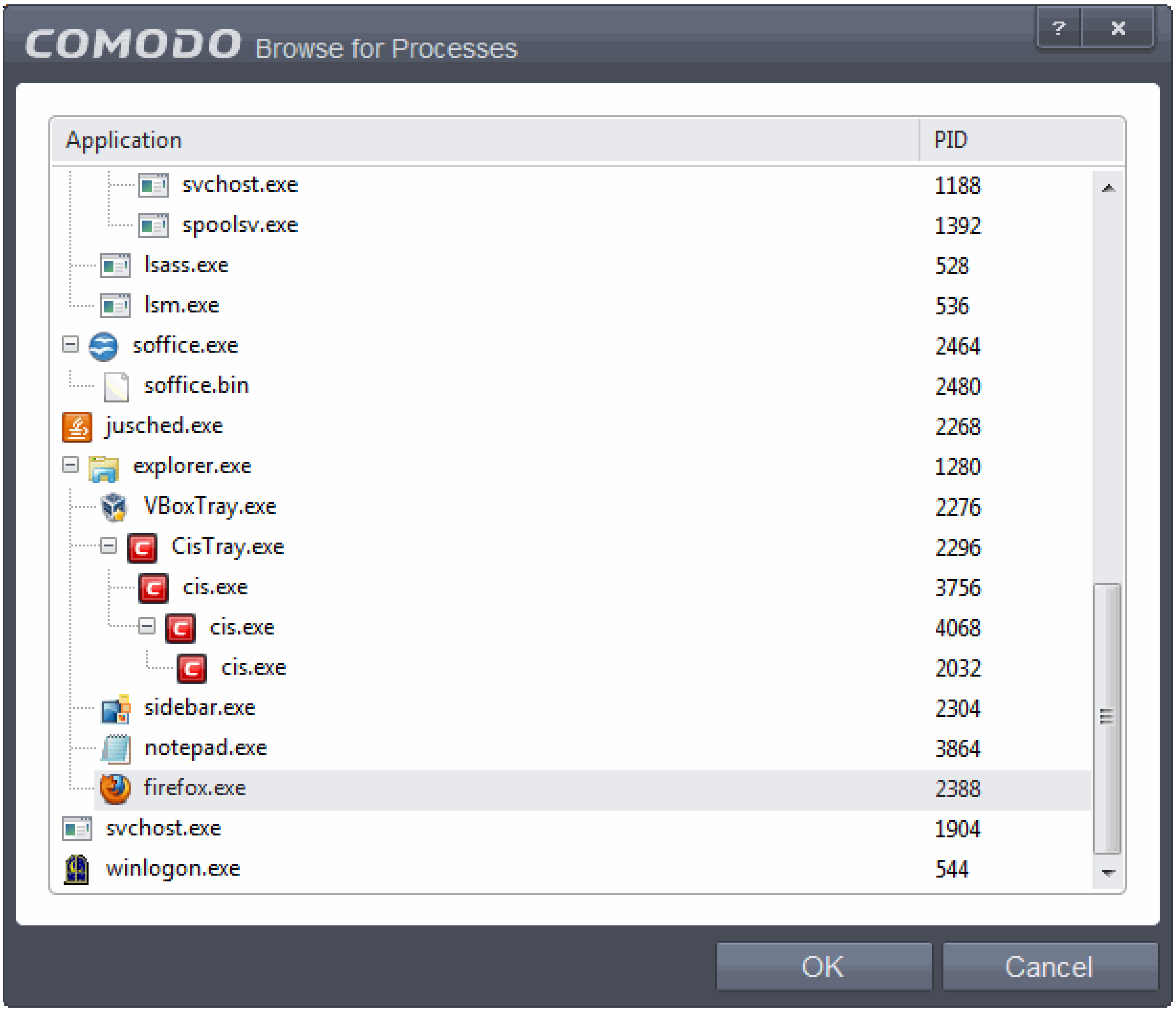


Name	Date modified	Type
application	6/26/2010 12:01 AM	Config
blocklist	6/26/2010 12:01 AM	XML D
browserconfig.properties	6/26/2010 12:01 AM	PROPE
crashreporter	6/26/2010 1:41 AM	Applic
crashreporter	6/26/2010 12:01 AM	Config
crashreporter-override	6/26/2010 12:01 AM	Config
firefox	6/26/2010 1:41 AM	Applic
freebl3.chk	6/26/2010 12:01 AM	Recov
freebl3.dll	6/26/2010 12:01 AM	Applic
install	9/30/2010 5:12 PM	Text D

File name: firefox

All Files (*.*)

iii. **Running Processes -** as the name suggests, this option allows you to create and deploy firewall ruleset for any process that is currently running on your PC.



COMODO Browse for Processes

Application	PID
svchost.exe	1188
spoolsv.exe	1392
lsass.exe	528
lsm.exe	536
soffice.exe	2464
soffice.bin	2480
jusched.exe	2268
explorer.exe	1280
VBoxTray.exe	2276
CisTray.exe	2296
cis.exe	3756
cis.exe	4068
cis.exe	2032
sidebar.exe	2304
notepad.exe	3864
firefox.exe	2388
svchost.exe	1904
winlogon.exe	544

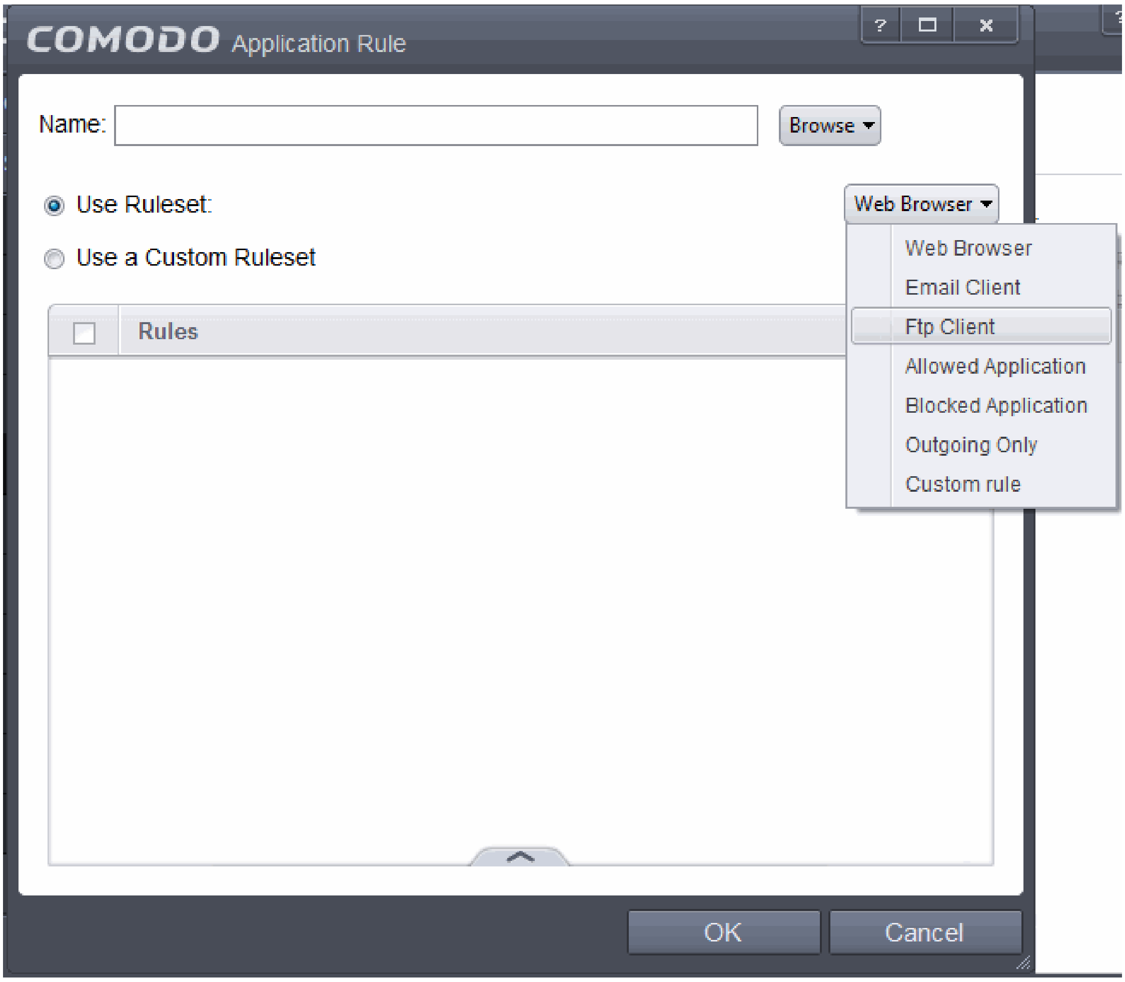
You can choose an individual process (shown above) or the parent process of a set of running processes. Click 'OK' to confirm your choice.

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

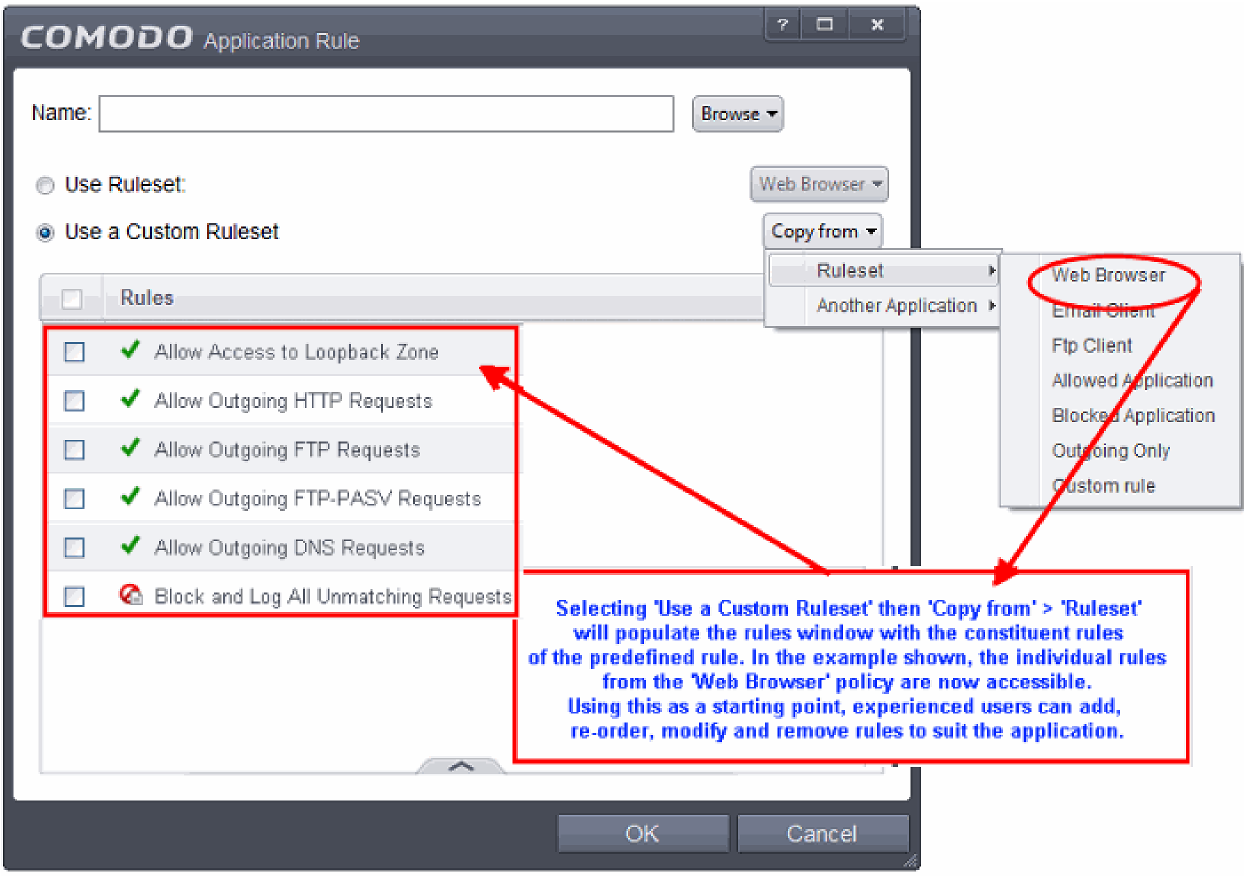
There are two broad options available for creating a ruleset that applies to an application - Use a Predefined Ruleset or Use a Custom Ruleset.

- **Use a Predefined Ruleset** - Selecting this option allows the user to quickly deploy a 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 **Predefined Rulesets** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - designed for more experienced users, the **Custom Ruleset** option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset. *(Default = Enabled)*



Selecting 'Use a Custom Ruleset' then 'Copy from' > 'Ruleset' will populate the rules window with the constituent rules of the predefined rule. In the example shown, the individual rules from the 'Web Browser' policy are now accessible. Using this as a starting point, experienced users can add, re-order, modify and remove rules to suit the application.

You can create an entirely new ruleset or use a predefined ruleset as a starting point by:

- Clicking the handle from the bottom right and choosing 'Add' from the options 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.

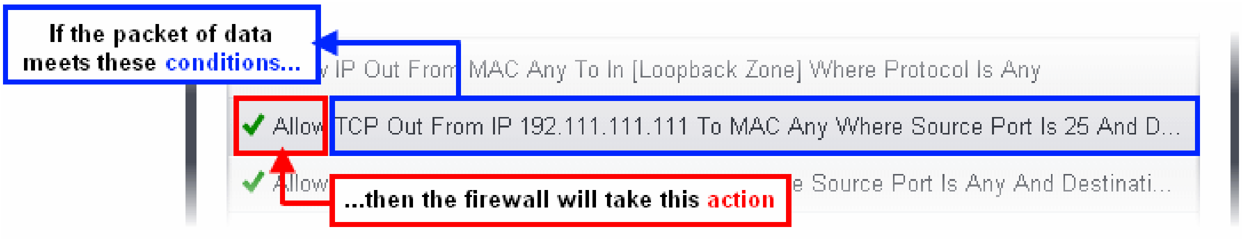
General Tips:

- 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 can be thought of as a simple **IF THEN** trigger - a set of conditions (or attributes) pertaining to a packet of data from a particular application and an action it that is enforced if those conditions are met.

As a packet filtering firewall, Comodo Firewall analyzes the attributes of *every single* packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a Firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding Firewall rule, then the connection is automatically blocked until a rule is created.


If the packet of data meets these conditions...
...then the firewall will take this action

Allow IP Out From MAC Any To In [Loopback Zone] Where Protocol Is Any
✓ Allow TCP Out From IP 192.111.111.111 To MAC Any Where Source Port Is 25 And D...
✓ Allow ... Source Port Is Any And Destinati...

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.

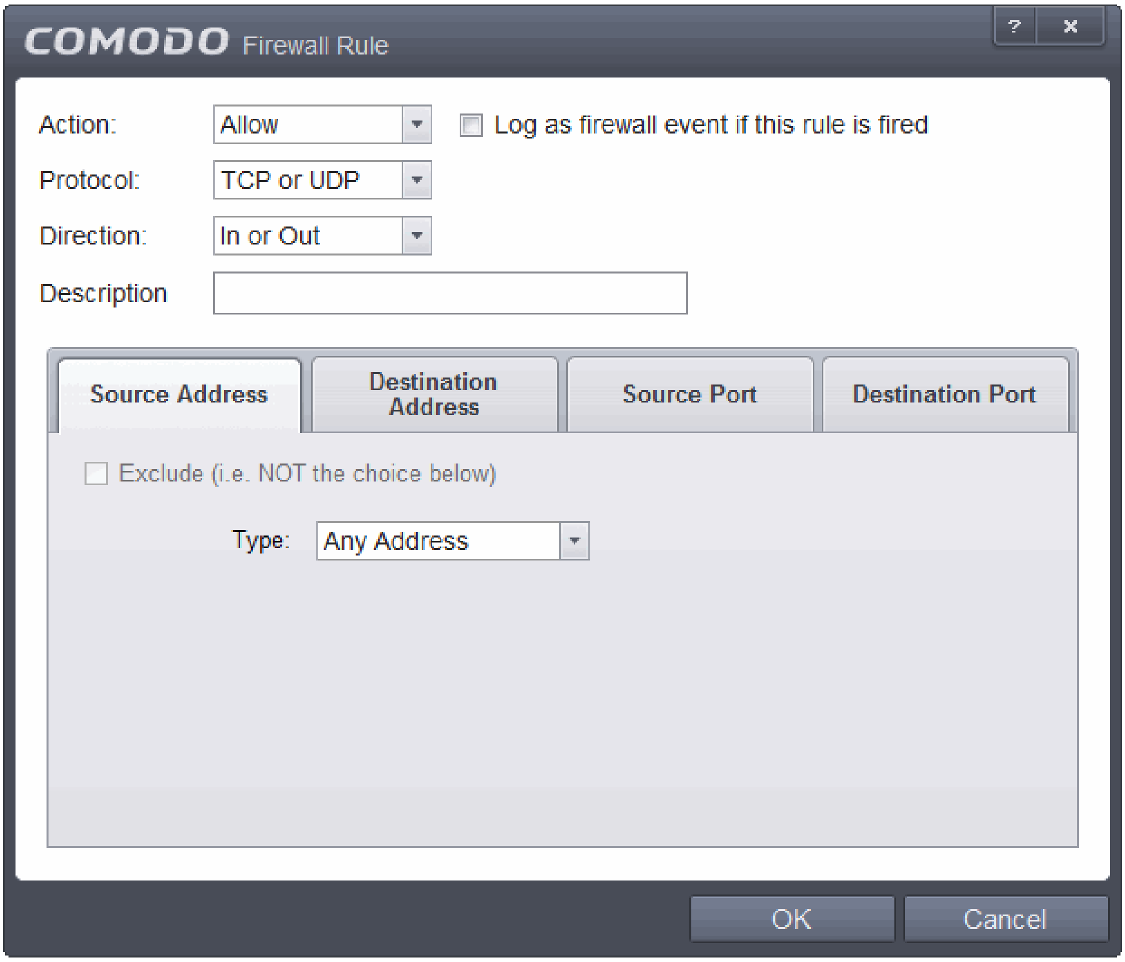
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section 'Global Rules' to understand the interaction between Application Rules and Global Rules.

** 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'



Action: Allow

□ Log as firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description

□ Exclude (i.e. NOT the choice below)

Type: Any Address

General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' ***(Default)***, '**Block**' or '**Ask**'.
- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' ***(Default)***, '**ICMP**' or '**IP**' .

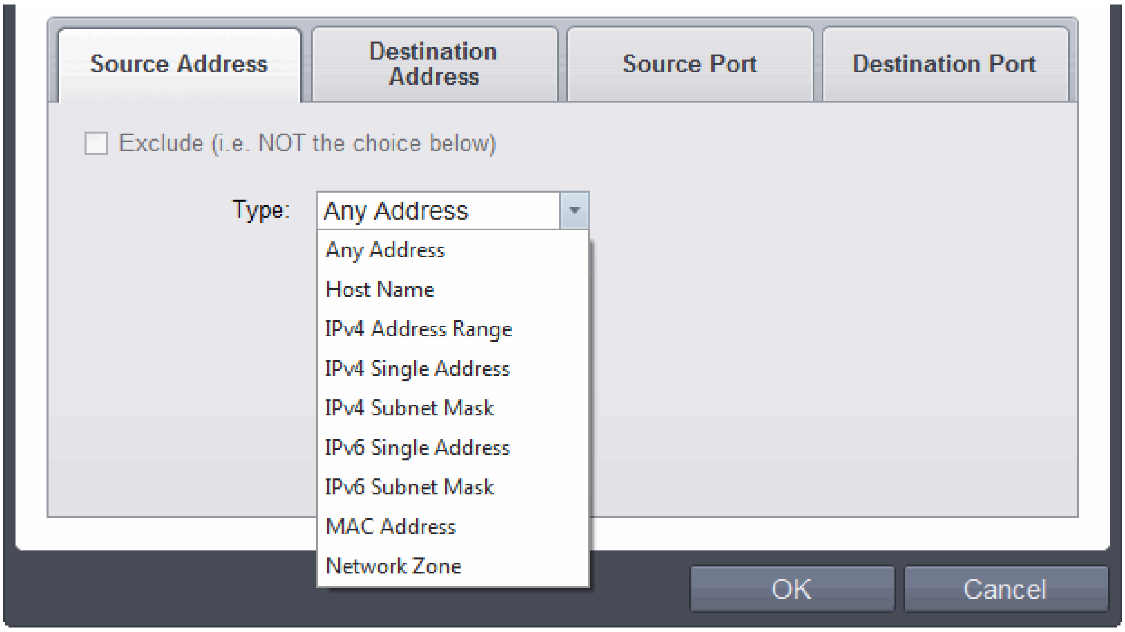
Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the **firewall event log viewer** whenever this rule is called into operation. (i.e. when ALL conditions have been met) ***(Default = Disabled).***
- **Description**: Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is displayed to represent instead of the full actions/conditions in the main Application Rules interface and the Application Rule interface.

Protocol

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

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information.



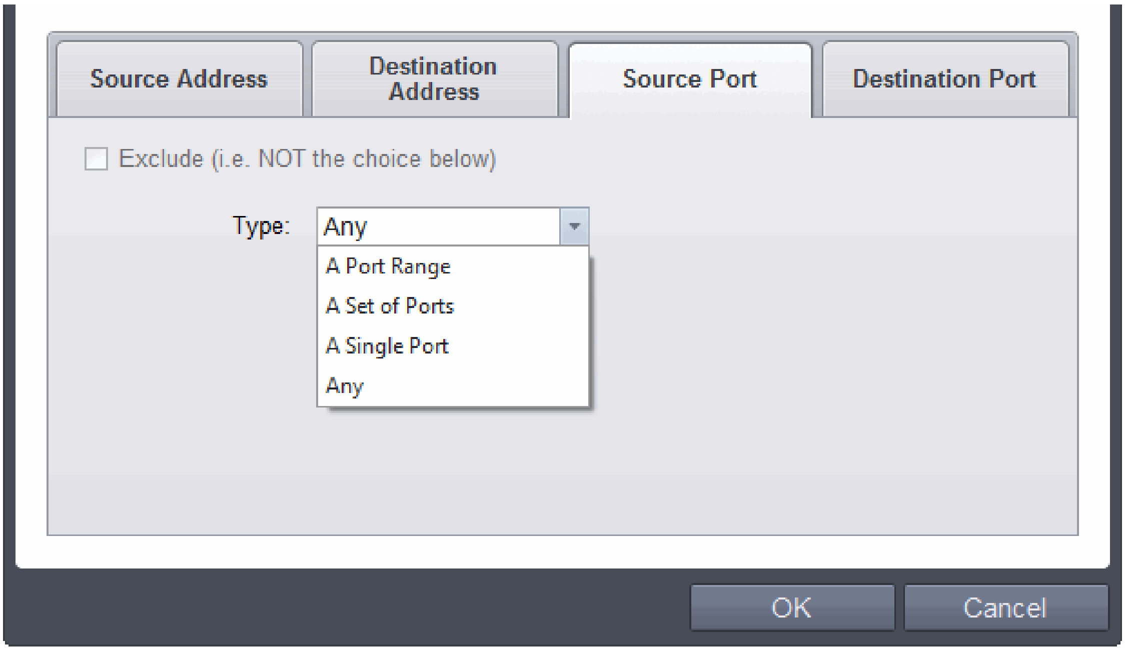
Source Address and Destination Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.
9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the 'Network Zones' area.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.



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 Sets by choosing A Set of Ports. If you wish to create a port set then please see the section 'Port Sets'.

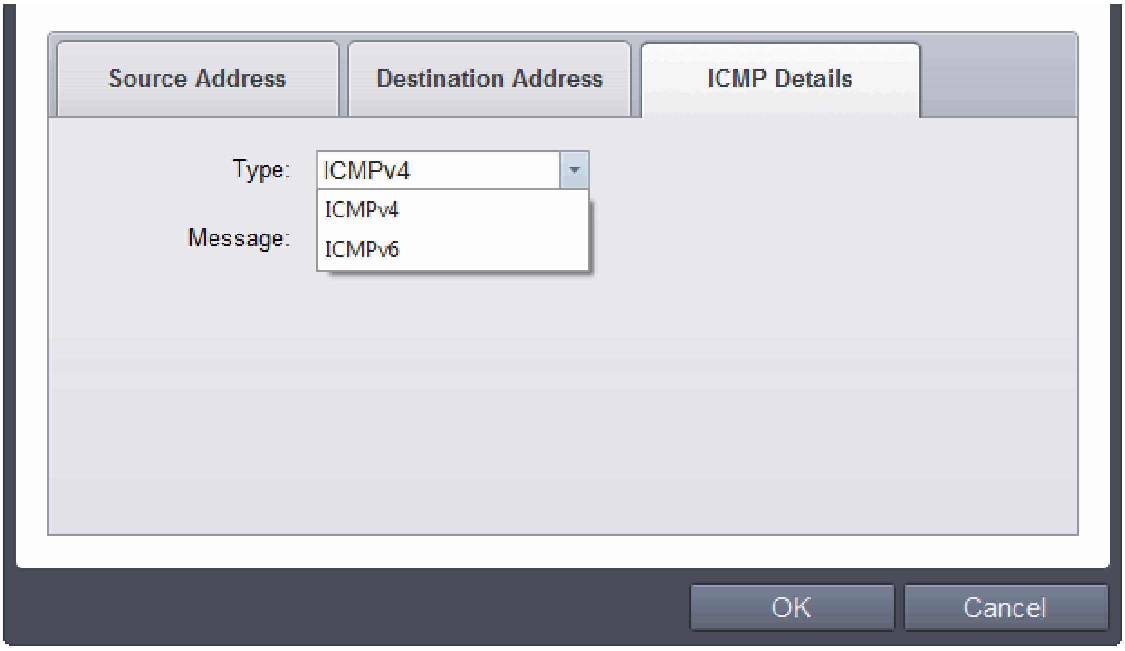
ii. **ICMP**

When you select ICMP as the protocol in General Settings, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the Destination Address tabs. The last two tabs are configured identically to the explanation above. You cannot see the source and destination port tabs.

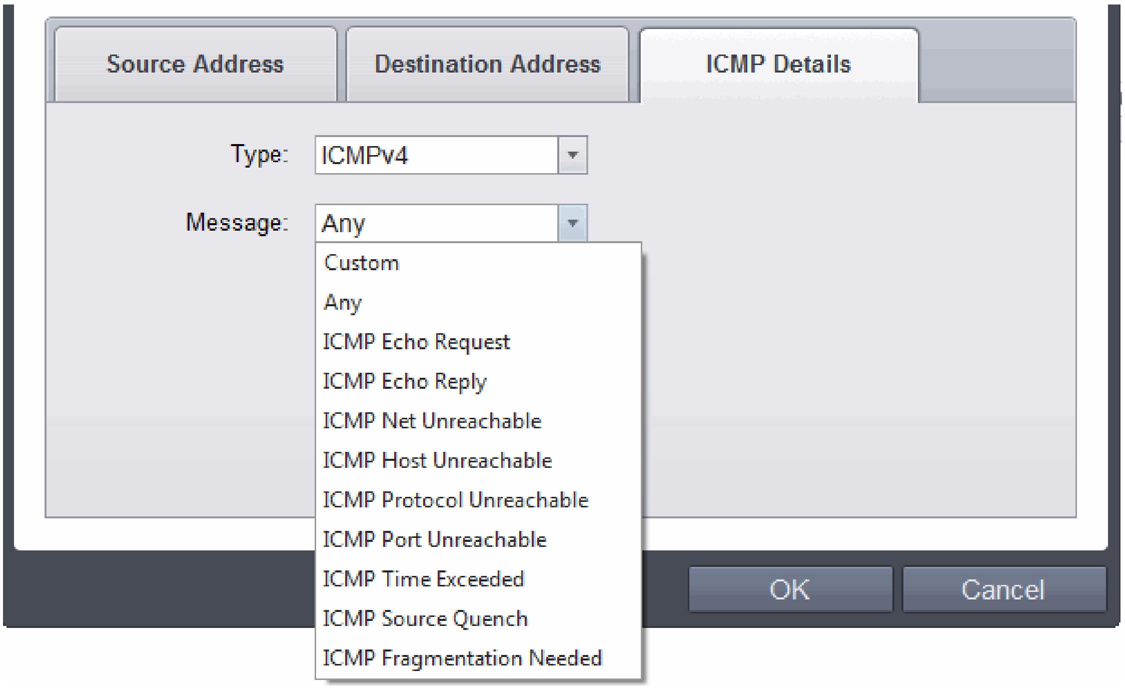
- **ICMP Details**

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.
2. 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.



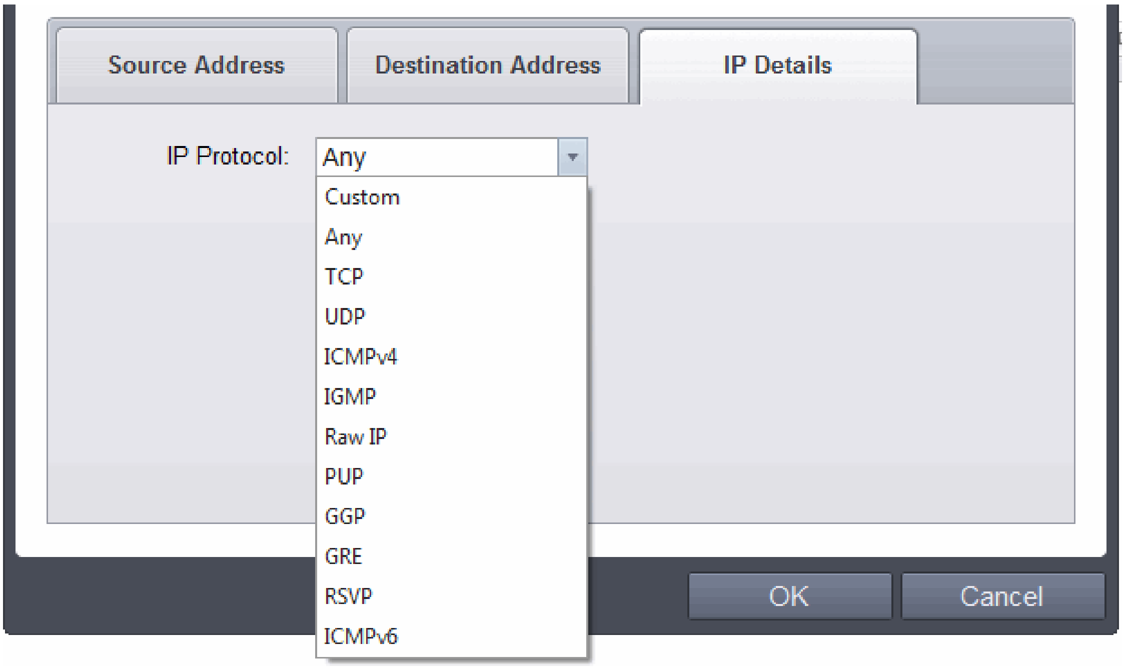
4. Specify ICMP Message, Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.



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.



- **IP Details**

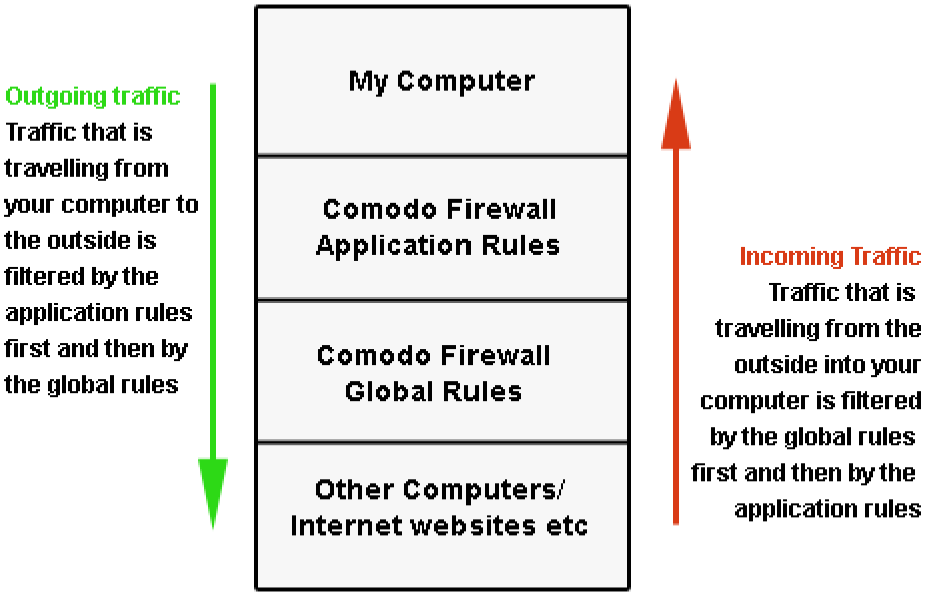
  Select the types of IP protocol that you wish to allow, from the ones that are listed.

6.2.3.3. Global Rules

Unlike Application rules, which are applied to and triggered by traffic relating to a specific application, Global Rules are applied to all traffic traveling in and out of your computer.

Comodo Firewall analyzes every packet of data in and out of your PC using combination of Application and Global Rules.

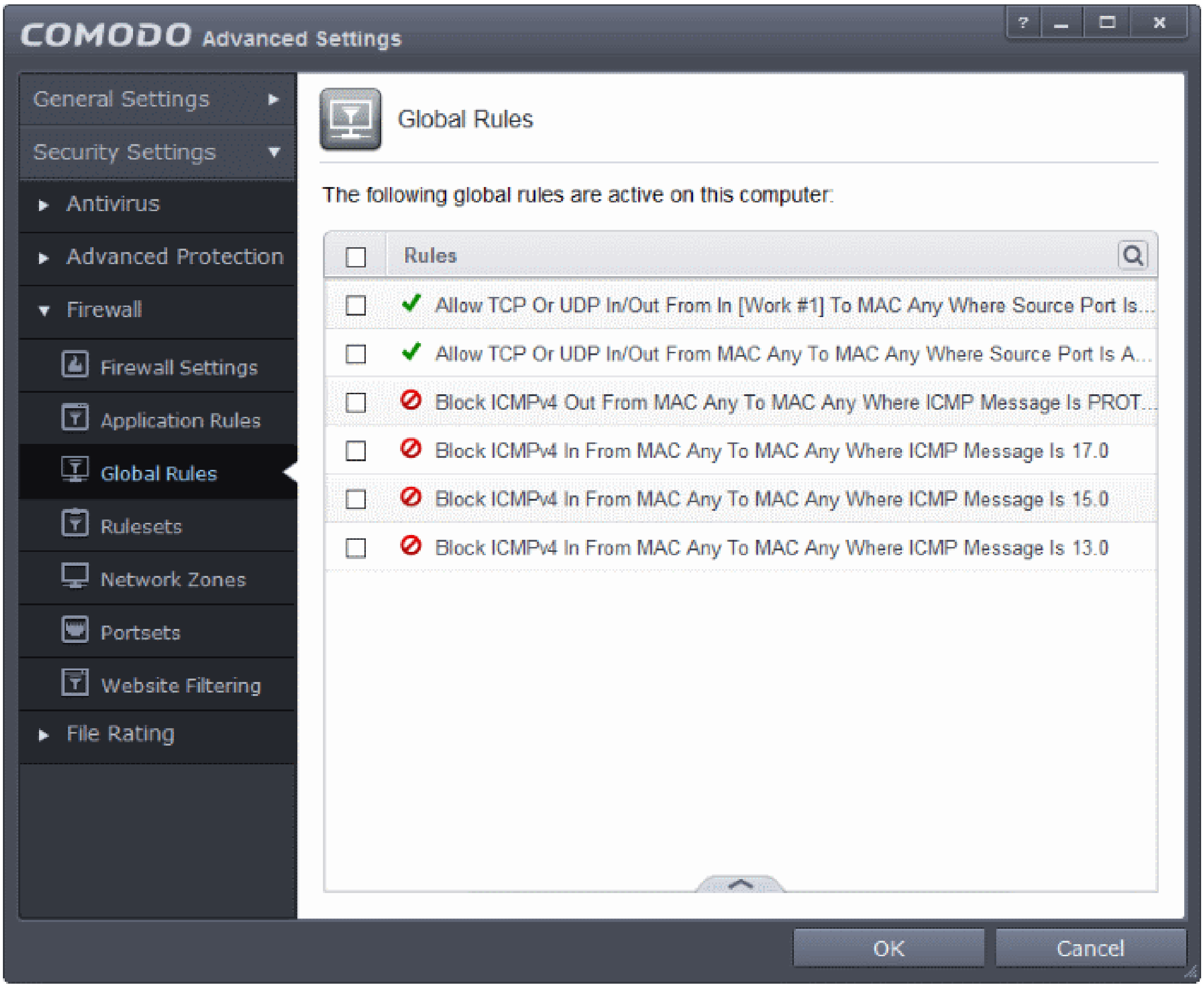
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.


Outgoing traffic
Traffic that is travelling from your computer to the outside is filtered by the application rules first and then by the global rules
My Computer
Comodo Firewall Application Rules
Comodo Firewall Global Rules
Other Computers/ Internet websites etc
Incoming Traffic
Traffic that is travelling from the outside into your computer is filtered by the global rules first and then by the application rules

Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.

Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

- The Global Rules panel, accessible by clicking Security Settings > Firewall > Global rules tab from the Advanced tasks interface, allows you to view, add and manage the rules

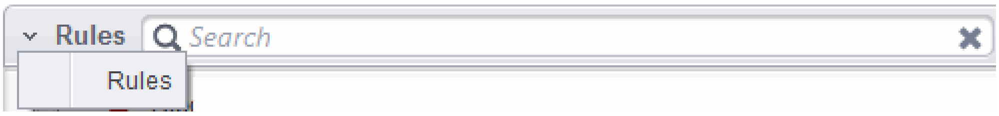


The following global rules are active on this computer:

□	Rules
□	✓ Allow TCP Or UDP In/Out From In [Work #1] To MAC Any Where Source Port Is...
□	✓ Allow TCP Or UDP In/Out From MAC Any To MAC Any Where Source Port Is A...
□	⊘ Block ICMPv4 Out From MAC Any To MAC Any Where ICMP Message Is PROT...
□	⊘ 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

You can use the search option to find a specific rule in the list.

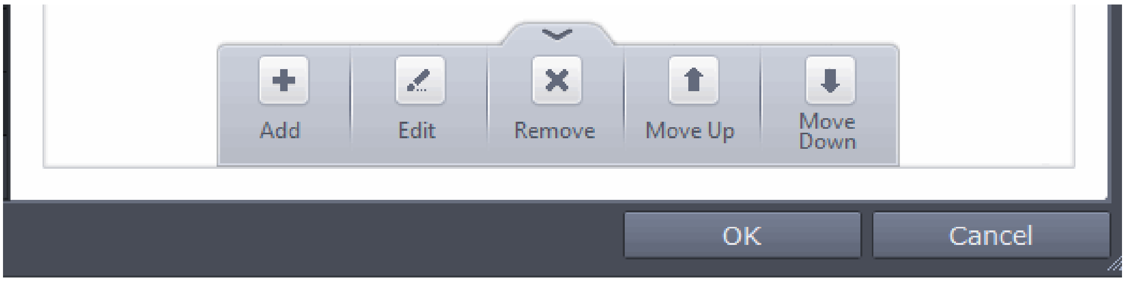
To use the search option, click the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

General Navigation:

Clicking the handle at the bottom center of the interface opens an option panel with the following options:



- **Add** - Allows you to add a new global rule. See the section 'Adding and Editing a Firewall Rule' 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' for guidance on editing a new rule.
- **Remove** - Deletes the selected rule.

Users can also re-prioritize rulesets by clicking the handle at the bottom center and select 'Move Up' or 'Move Down' from the options.

The configuration of Global Rules is identical to that for application rules. To add a global rule, click the 'Add...' button on the right. To edit an existing global rule, right click and select 'edit'.

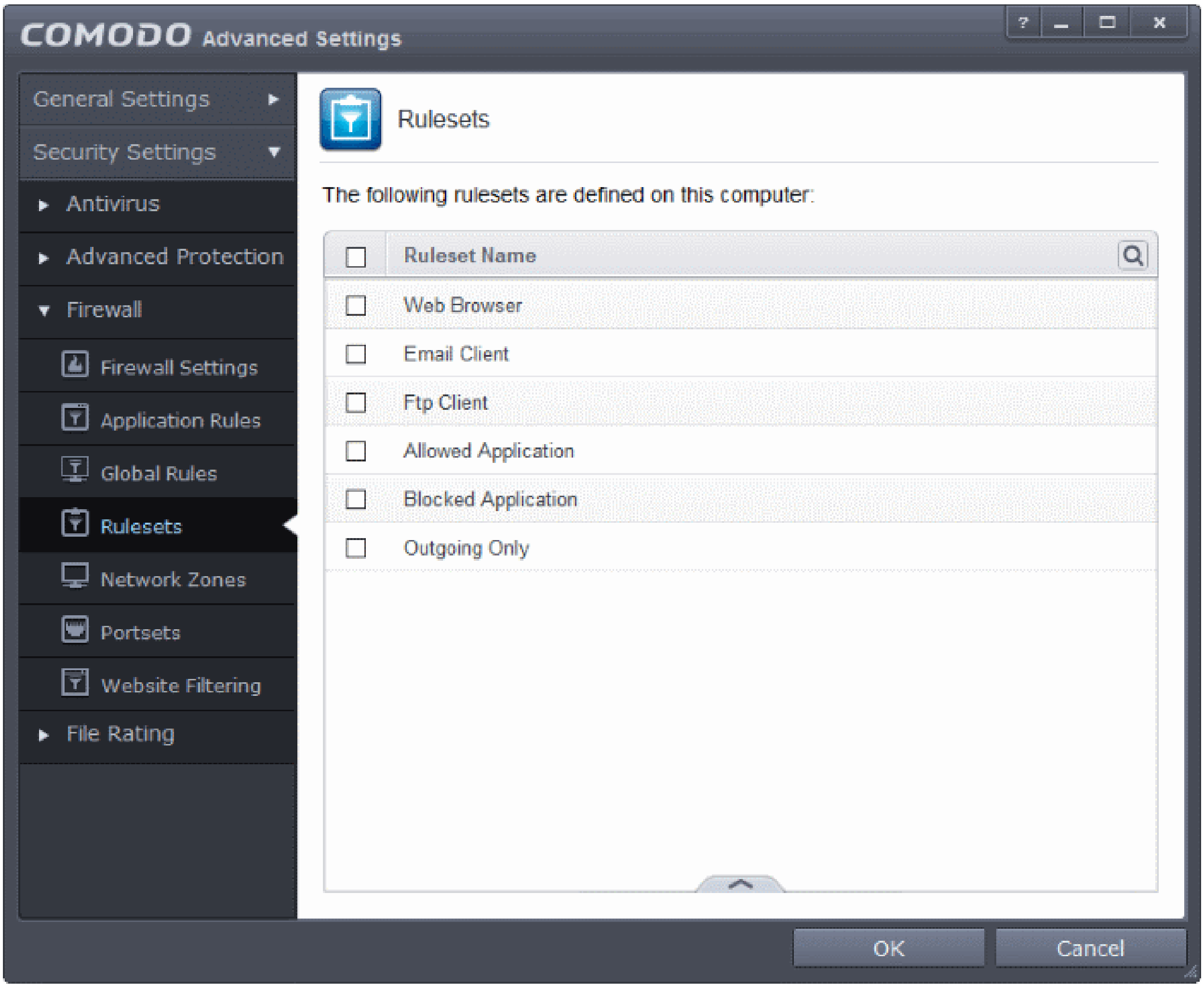
- See Application Rules for an introduction to the rule setting interface.
- See Understanding Firewall Rules for an overview of the meaning, construction and importance of individual rules.
- See Adding and Editing a Firewall Rule for an explanation of individual rule configuration.

6.2.3.4. Firewall Rule Sets

As the name suggests, a firewall Ruleset is a set of one or more individual Firewall rules that have been saved and which can be re-deployed on multiple applications. This section contains advice on the following:

- Predefined Rulesets
- Creating a new ruleset

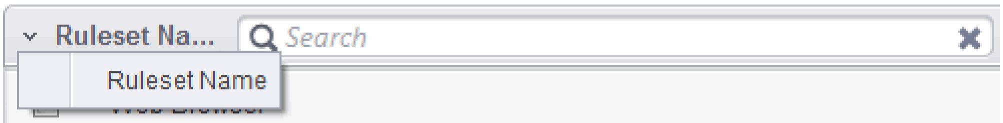
The Predefined rulesets interface can be accessed by clicking Security Settings > Firewall > Rulesets from the 'Advanced Settings' interface.



The following rulesets are defined on this computer:

□	Ruleset Name
□	Web Browser
□	Email Client
□	Ftp Client
□	Allowed Application
□	Blocked Application
□	Outgoing Only

You can use the search option to find a specific ruleset in the list by clicking the search icon 🔍 at the far right in the column header.



- Enter the name of the item to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Predefined Rulesets

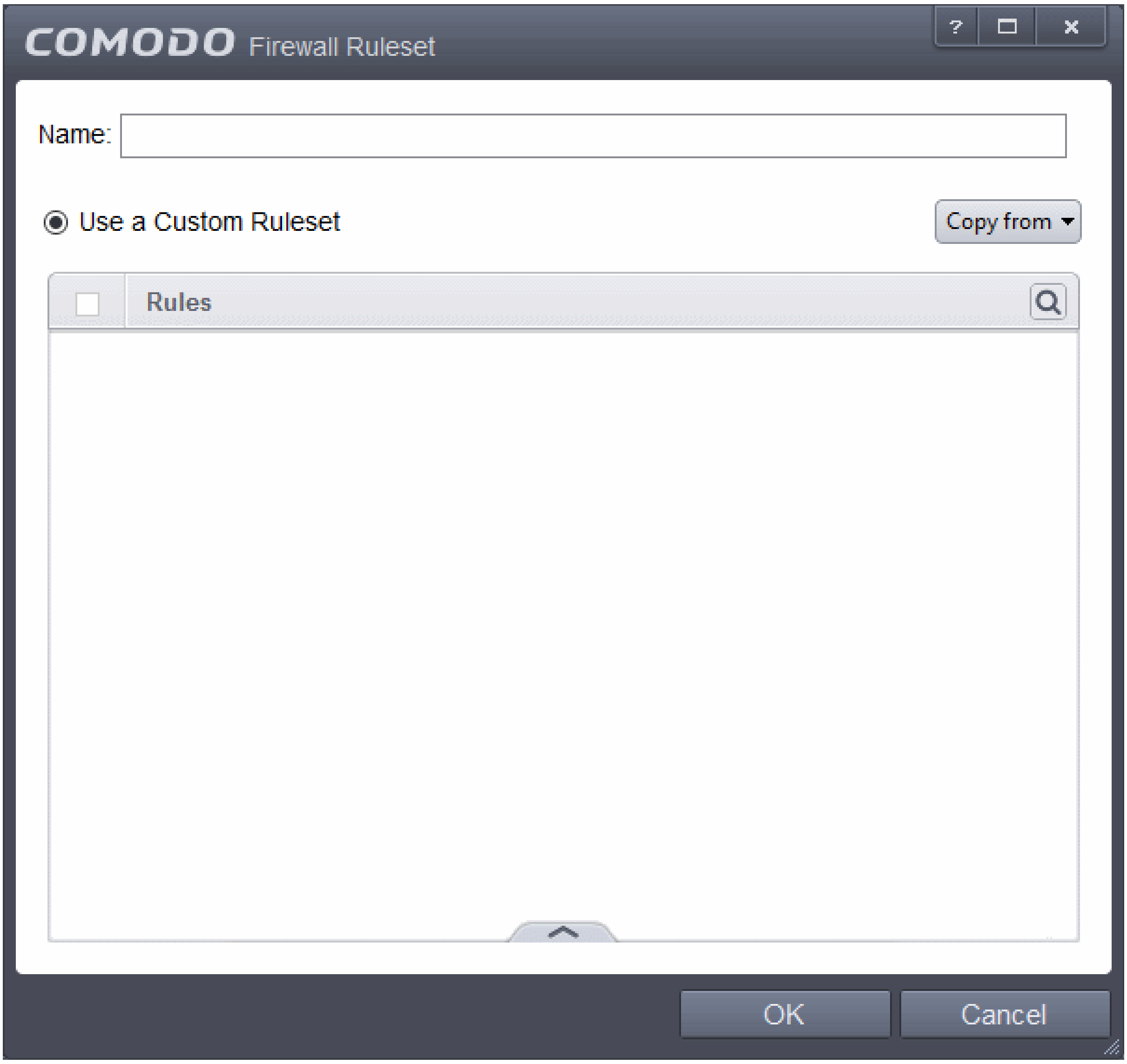
Although each application's firewall ruleset *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined 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 it rules).

Creating a new ruleset

You can create new rulesets with network access control rules customized as per your requirements and can roll out them to required applications while creating Firewall ruleset for the applications individually.

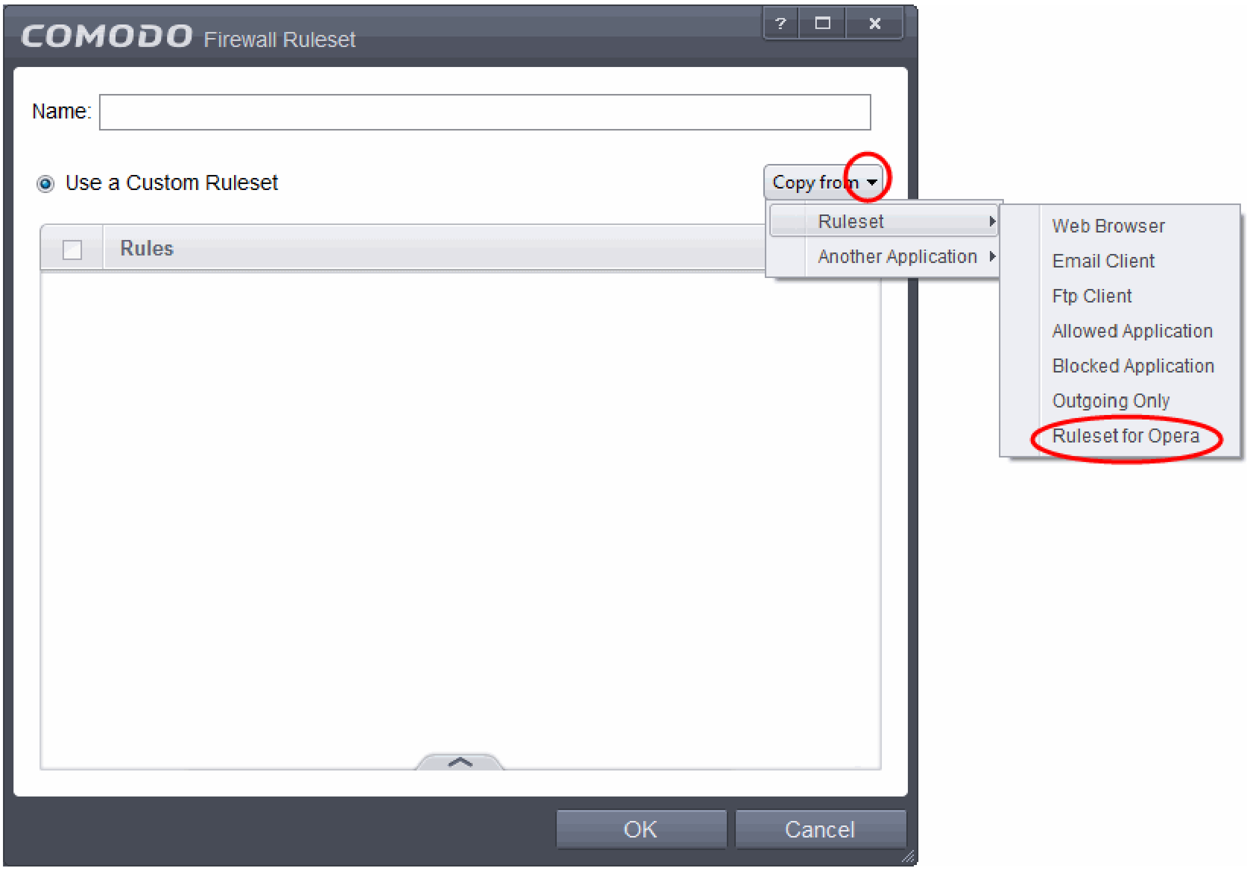
To add a new Ruleset

- Click the handle from the bottom center and select 'Add' from the options



- 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. See 'Adding and Editing a Firewall Rule' for more advice on this.

  Once created, this ruleset can be quickly called from 'Use Ruleset' when creating or modifying a Firewall ruleset.



To view or edit an existing predefined Ruleset

- Double click on the Ruleset Name in the list

  or

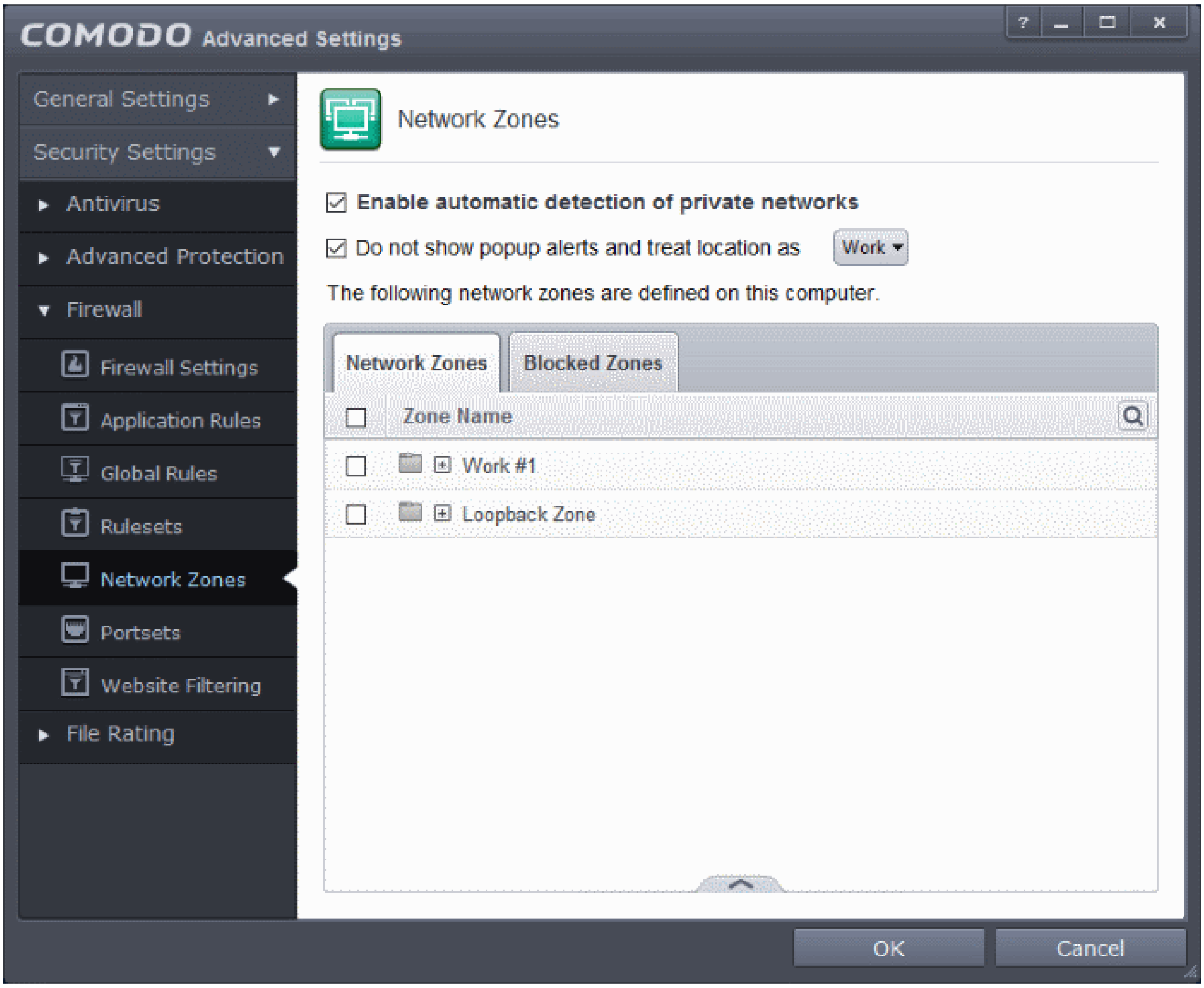
- Select the Ruleset Name, click the handle from the bottom and select Edit from the options
- Details of the process from this point on can be found here.

6.2.3.5. Network Zones

The Network Zones panel allows you to:

- Configure automatic detection of new networks (wired or wireless) that your computer can connect to.
- Configure alerts for network connections
- Define network zones that are trusted and specify access privileges to them
- Define network zones that are untrusted and block access to them

The Network Zones panel can be accessed by clicking Security Settings > Firewall > Network Zones from the 'Advanced Settings' interface.



Network Zones

☑ **Enable automatic detection of private networks**

☑ Do not show popup alerts and treat location as Work

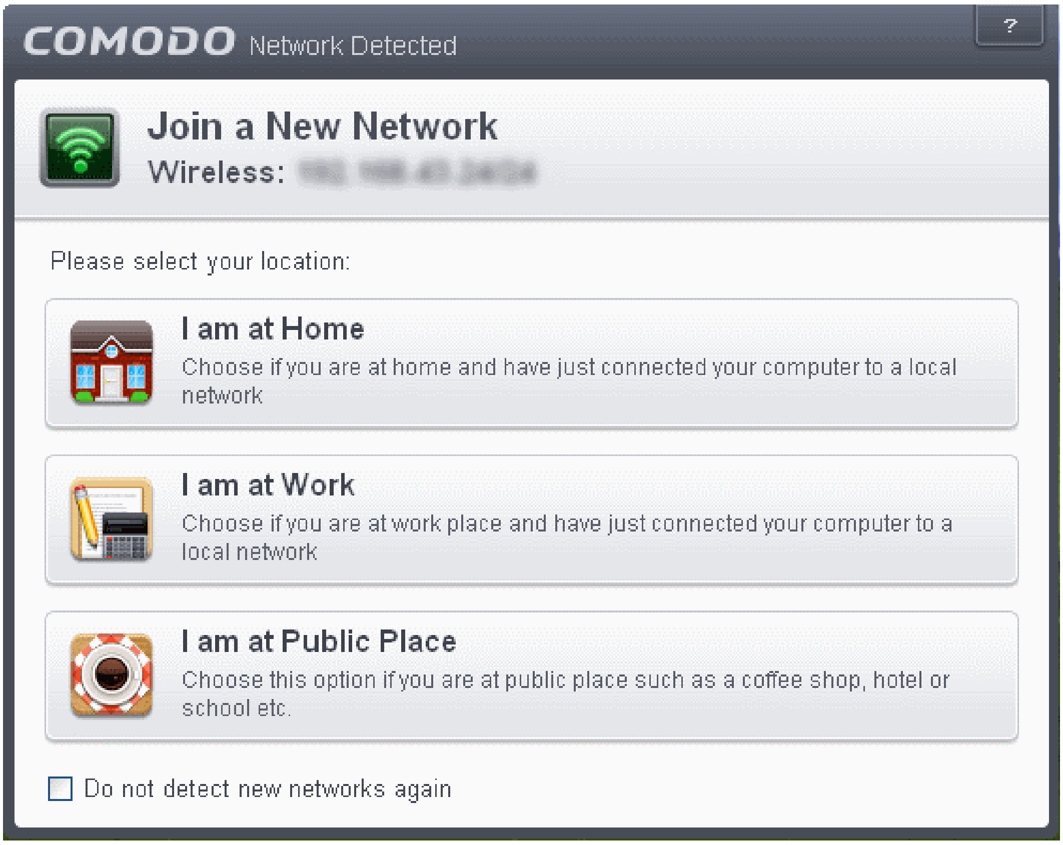
The following network zones are defined on this computer.

Network Zones | Blocked Zones

□	Zone Name
□	Work #1
□	Loopback Zone

- **Enable automatic detection of private networks** - Instructs Comodo Firewall to keep monitoring whether your computer is connected 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 be displayed and the network location will be saved as selected from the drop-down options – Home, Work and Public. *(Default = Enabled with location as Work)*

If automatic detection of new networks is enabled and pop up alert is disabled, then the following alert will be displayed whenever your system is trying to connect to any new wired or wireless network.



COMODO Network Detected

?

Join a New Network

Wireless: [redacted]

Please select your location:

I am at Home

Choose if you are at home and have just connected your computer to a local network

I am at Work

Choose if you are at work place and have just connected your computer to a local network

I am at Public Place

Choose this option if you are at public place such as a coffee shop, hotel or school etc.

□ Do not detect new networks again

You can select the type of new network you are connected to, so that the firewall configuration is optimized for the type of connection.

- Select 'Do not detect new networks again' if you are an experienced user that wishes to manually set-up your own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

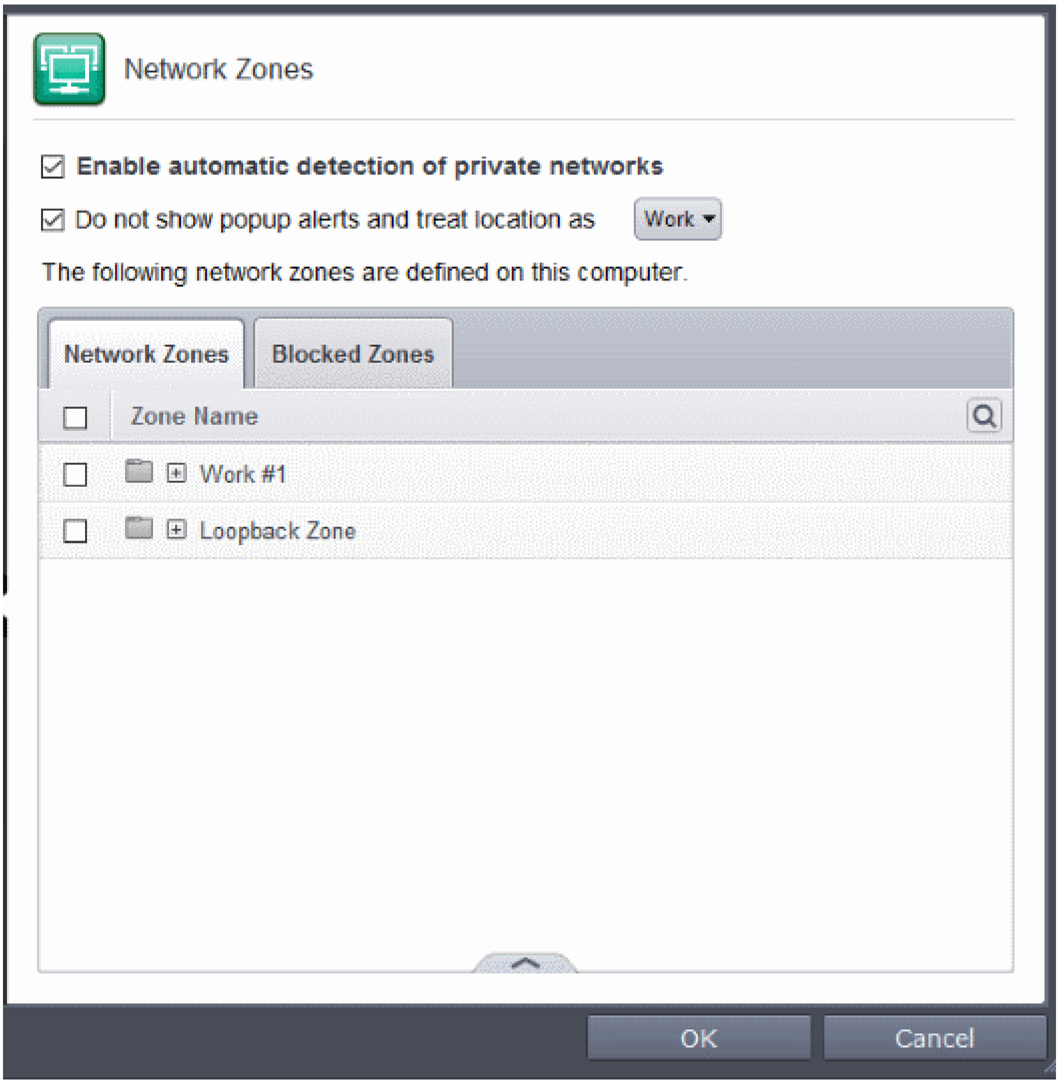
The Network Zone panel has two tabs:

- Network Zones - Allows you to define network zones and to allow access to them for applications, with the access privileges specified through Application Rule interface. Refer to '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.

6.2.3.5.1. 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 to which access can be granted or denied.

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 that you need to grant access to, including your home or work network. Conversely, there may be other networks that you want to restrict communication with - or even block entirely.



Network Zones

☑ Enable automatic detection of private networks

☑ Do not show popup alerts and treat location as Work

The following network zones are defined on this computer.

Note 1: Adding a zone to this area does not, in itself, define any permission levels or access rights to the zone. This area allows you to *define* the zones so you can quickly assign such permissions in other areas of the firewall.

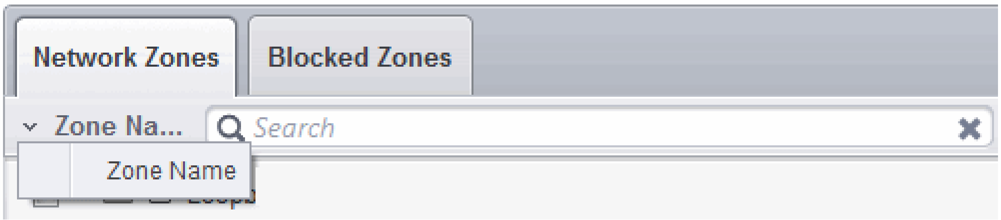
Note 2: A network zone can be designated as 'Trusted' and allowed access from the 'Manage Network Connections' interface. For example, your home computer or network.

Note 3: A network zone can be designated as 'Blocked' and denied access by using the 'Blocked Zones' interface. For example, 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 can be assigned to a network zone to handle all activity from a zone.

Note 5: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc) when 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 the search option to find a network zone in the list by clicking the search icon 🔍 at the far right in the column header.



- Enter the name of the item to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

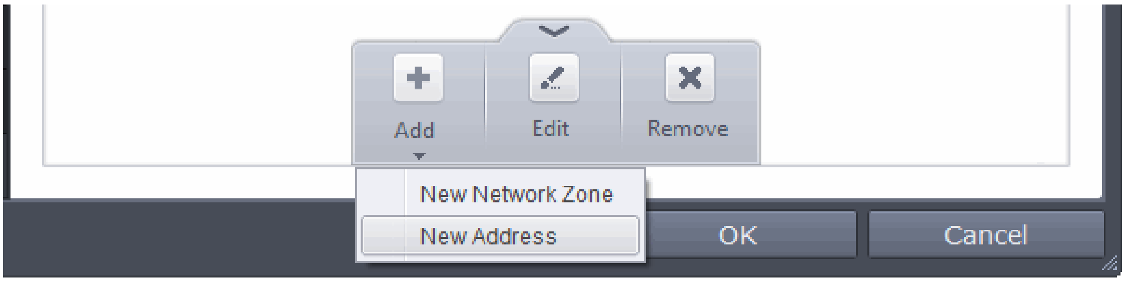
Defining a new Network Zone

To add a new network zone:

- Step 1 - Define a name for the zone.
- Step 2 - Select the addresses to be included in this zone.

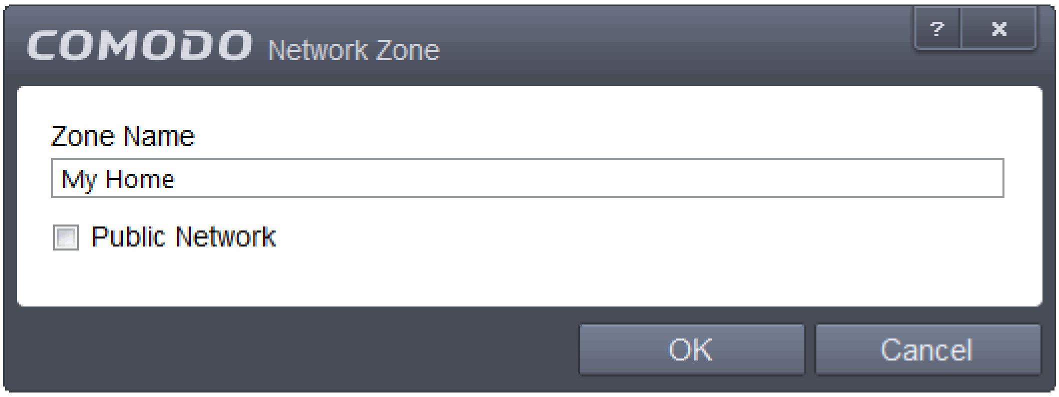
Step 1 - Define a name for the zone

1. Click the handle from the bottom center select 'Add' > 'New Network Zone'.



A dialog box will appear, prompting you to specify a name for the new zone.

2. Choose a name that accurately describes the network zone you are creating.

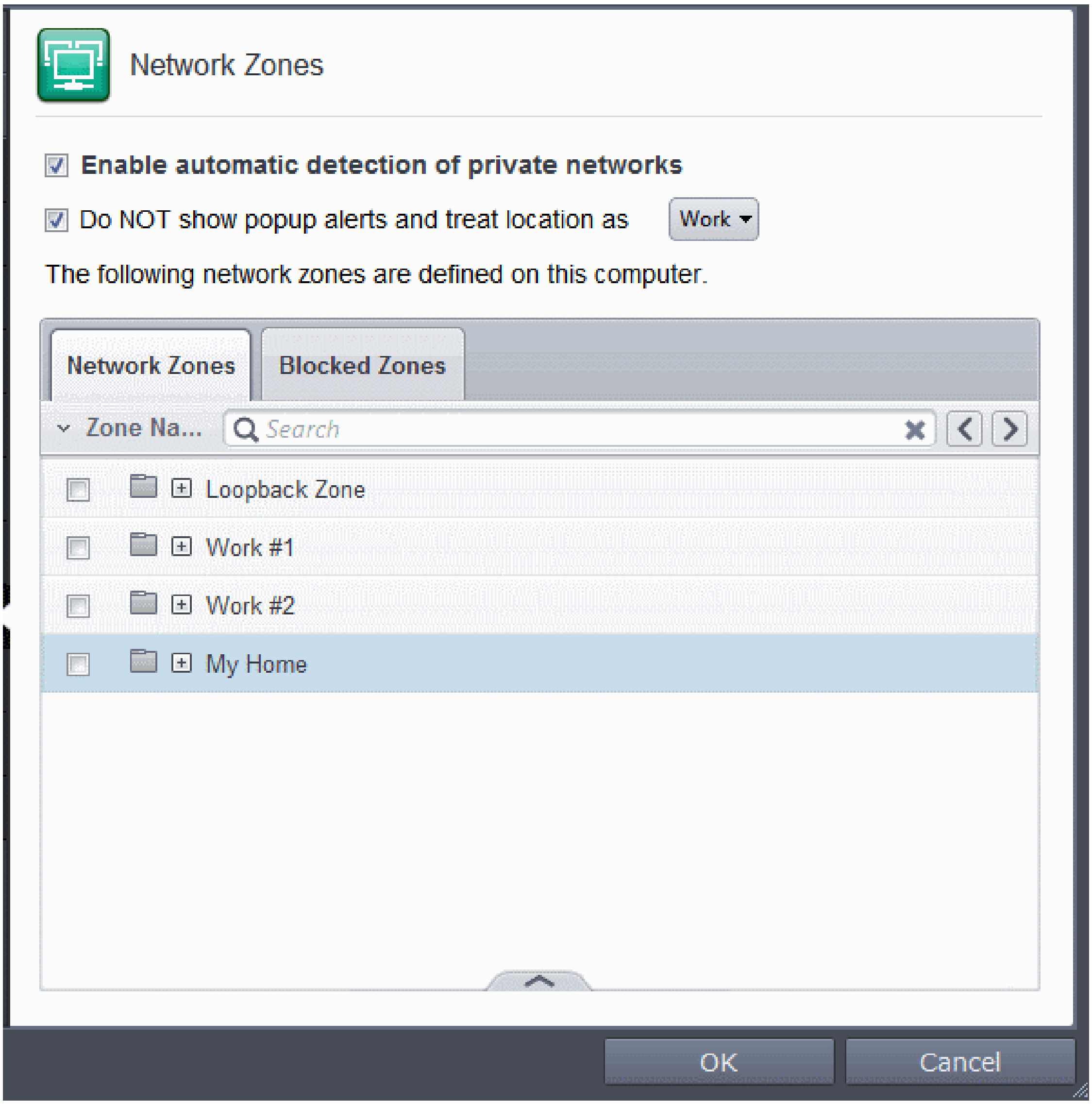


Zone Name: My Home

□ Public Network

3. Select the checkbox '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., so that Comodo Firewall will optimize the configuration accordingly.
4. Click 'Apply' to confirm your zone name.

   This adds the name of your new zone to the Network Zones list.



Network Zones

☑ Enable automatic detection of private networks

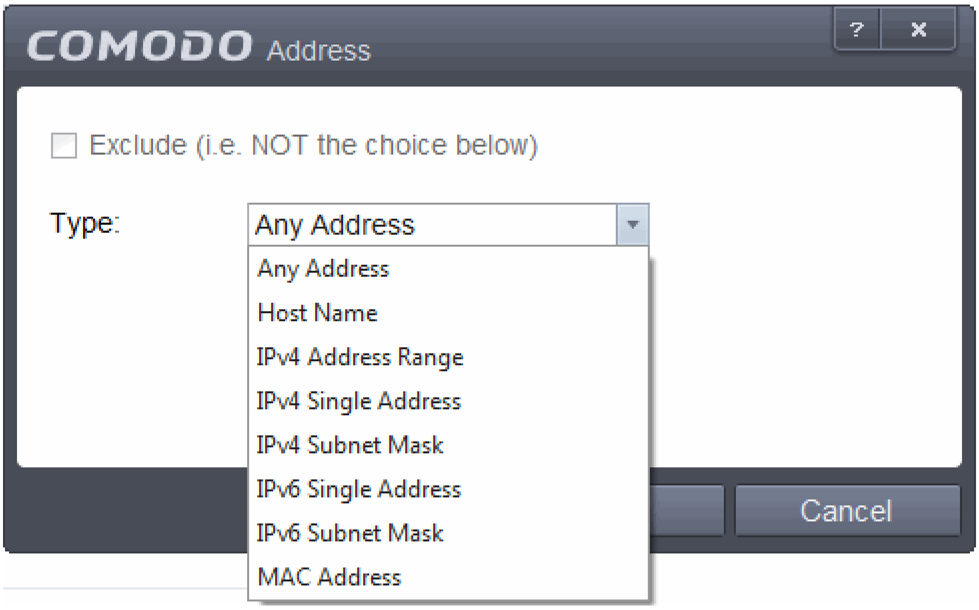
☑ Do NOT show popup alerts and treat location as Work

The following network zones are defined on this computer.

Step 2 - Select the addresses to be included in this zone

1. Select the network name, click the handle at the bottom and choose 'Add' > 'New Address' from the options or click the + button beside the new network zone name and double click on '(add addresses here)'

   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 be enabled only if any other choice is selected from the drop-down box.



Select 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.

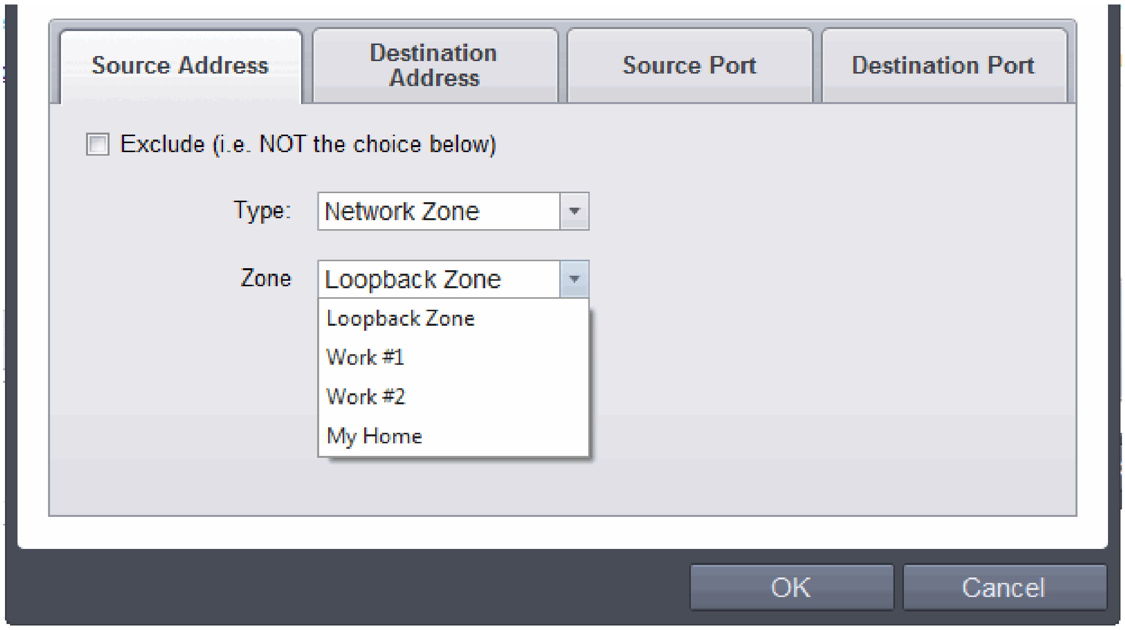
- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

2. Click 'OK' to confirm your choice.
3. Click 'OK' in the 'Network Zones' interface.

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

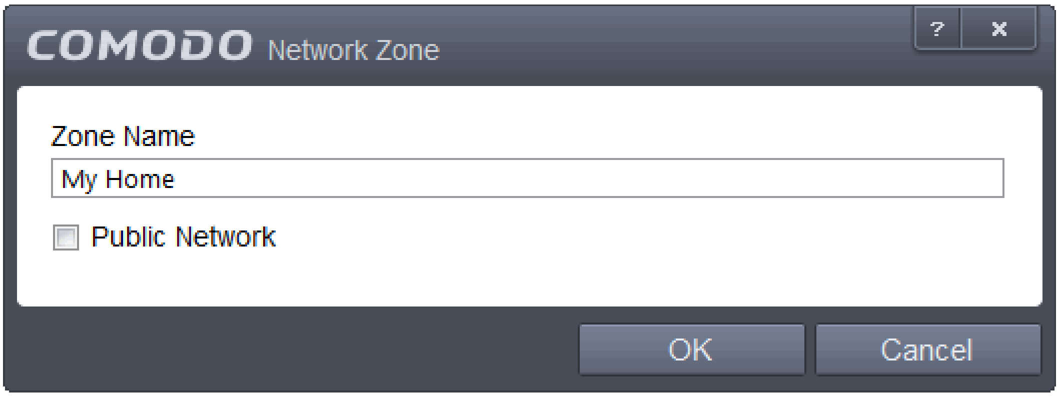
- Quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**



- Quickly called and designated as a blocked zone from the 'Blocked Zones' interface

To edit the name of an existing Network Zone

1. Select the name of the zone in the list (e.g. My Home), click the handle at the bottom center and choose 'Edit' from the options or double click on the network zone name.



Zone Name

My Home

□ Public Network

2. Edit the name of the zone.

To add more addresses to an existing Network Zone

- Select the network name, click the handle at the bottom center and choose 'Add > A new Address' from the options
- Add new address from the 'Address' interface.

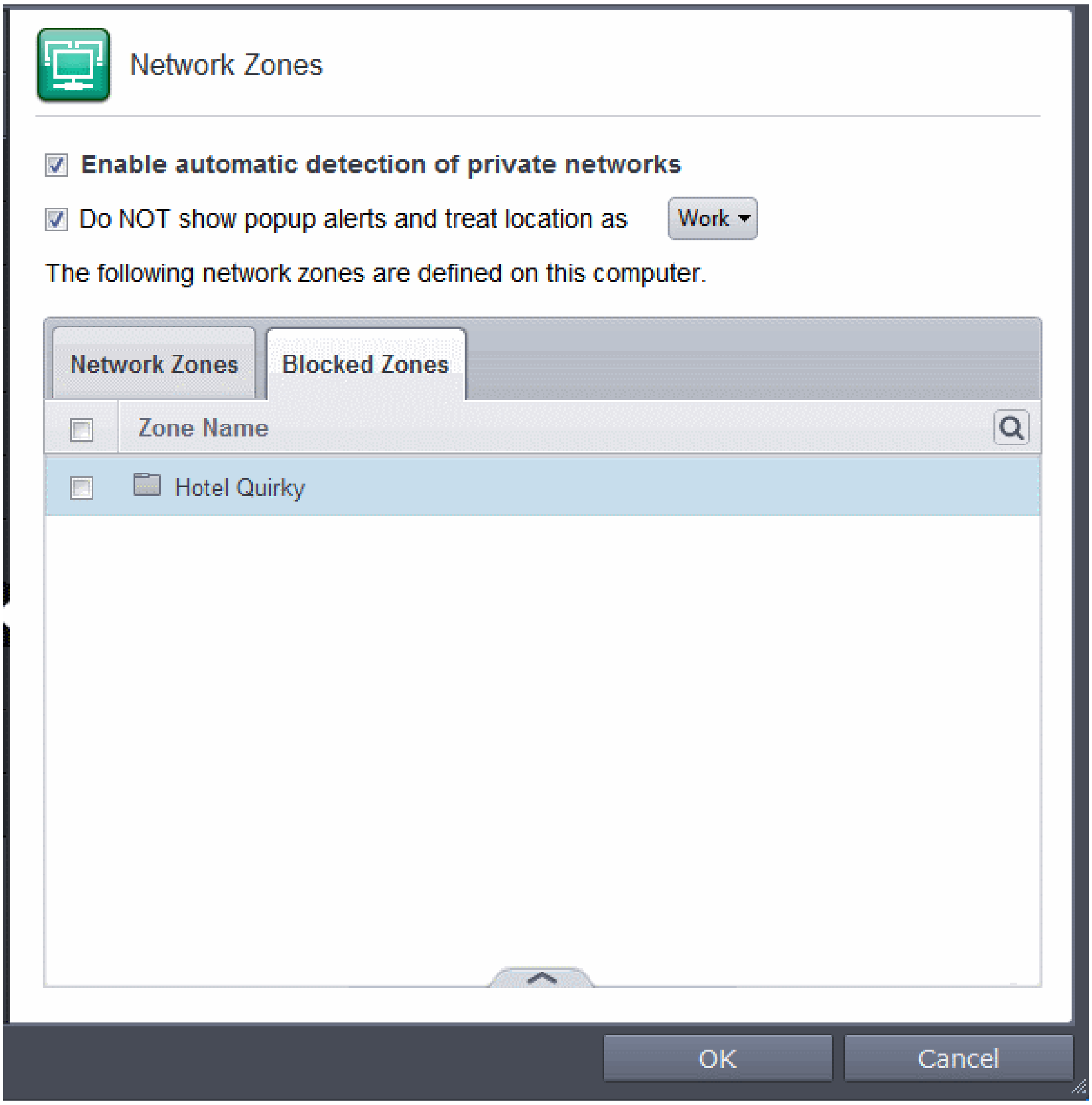
To modify or change the existing address in a zone

- 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 the handle from the bottom center and choose Edit from the options
- Edit the address from the 'Address' interface.

6.2.3.5.2. Blocked Zones

A network enables users to share information and devices with other computers and users in the network. Obviously, there are certain computer networks that you need to 'trust' and grant access to - for example your home or work network. Unfortunately, there may be other, untrustworthy networks that you want to restrict communication with - or even block entirely.

Note: We advise new or inexperienced users to first read 'Network Zones' , 'Stealth Ports Wizard' and 'Application Rules' before blocking zones using this interface.



Network Zones

☑ Enable automatic detection of private networks

☑ Do NOT show popup alerts and treat location as Work

The following network zones are defined on this computer.

□	Zone Name
□	Hotel Quirky

The 'Blocked Network Zones' tab allows you to:

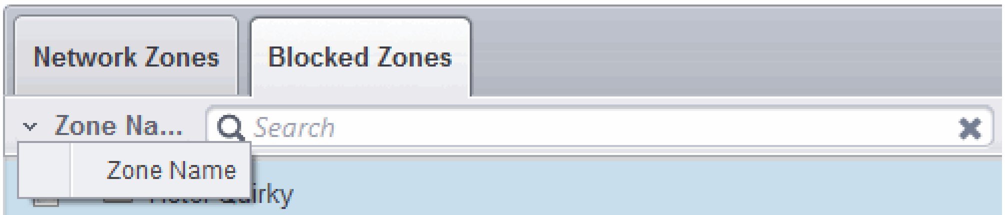
- Deny access to a specific network by selecting a pre-existing network zone and designating it as blocked
- Deny access to a specific network by manually defining a new blocked zone

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 *pre-existing* network 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.

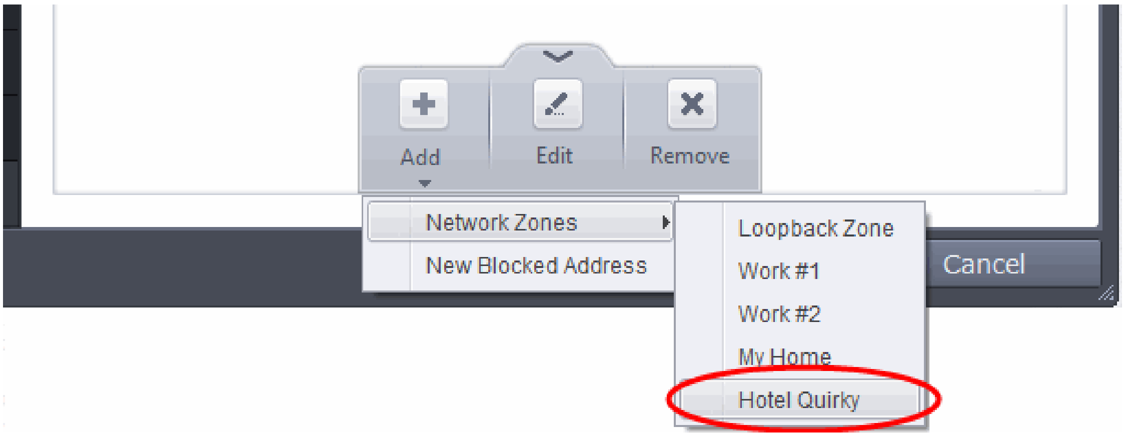
You can use the search option to find a blocked zone in the list by clicking the search icon 🔍 at the far right in the column header.



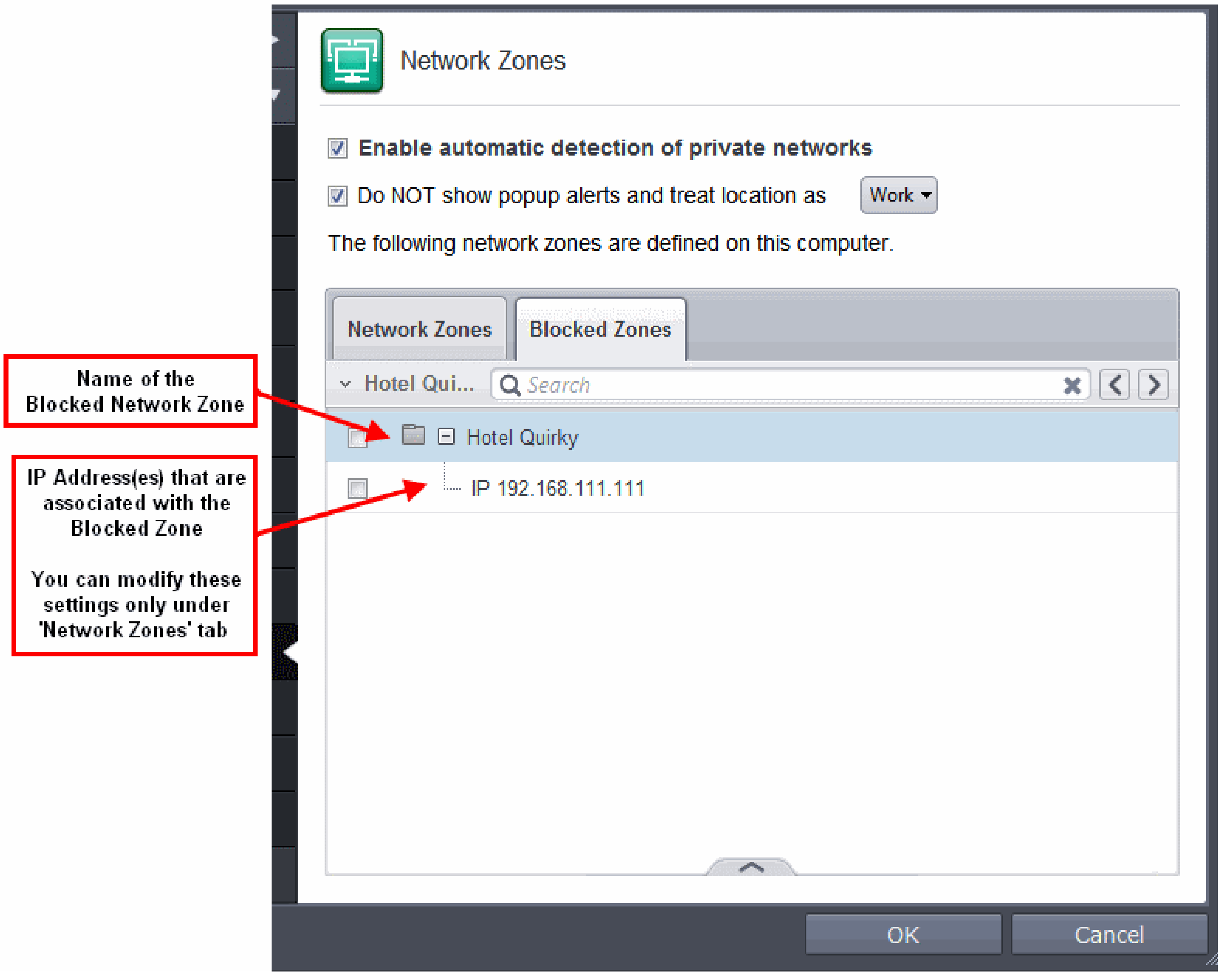
- Enter the name of the zone to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

To deny access to a specific network by selecting a pre-existing network zone and designating it as blocked

1. Click the handle from the bottom center and choose 'Add' > 'Network Zones' from the options
2. Select the particular zone you wish to block.



The selected zone will appear in the 'Blocked Zones' interface.



Network Zones

☑ Enable automatic detection of private networks

☑ Do NOT show popup alerts and treat location as Work

The following network zones are defined on this computer.

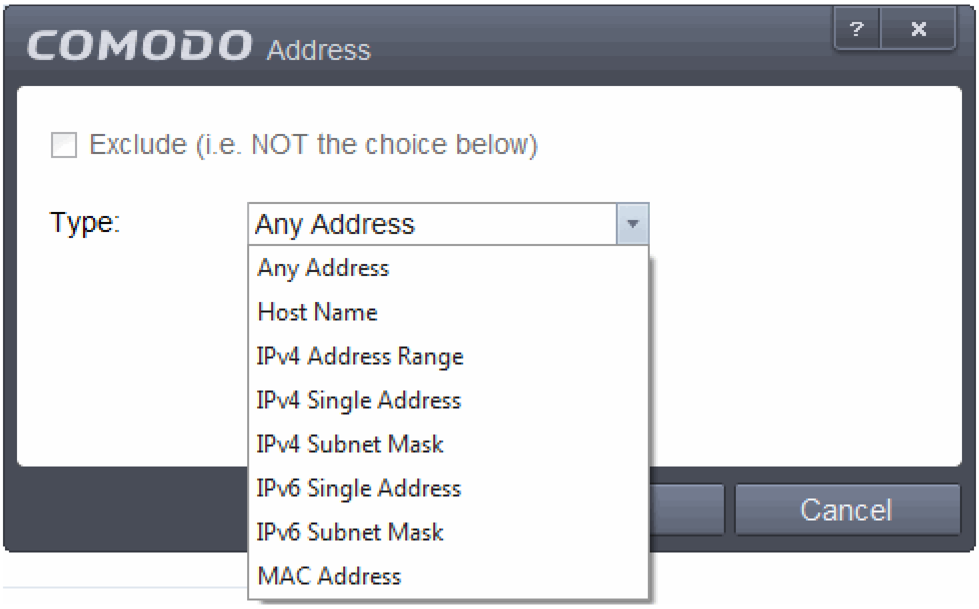
Network Zones
Blocked Zones
Hotel Qui...
Search
Hotel Quirky
IP 192.168.111.111
OK
Cancel
Name of the Blocked Network Zone
IP Address(es) that are associated with the Blocked Zone
You can modify these settings only under 'Network Zones' tab

3. Click 'OK' to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

To deny access to a specific network by manually defining a new blocked zone

1. Click the handle from the bottom and choose 'Add' > 'New Blocked Address' from the options.

The Address dialog will appear. The 'Address' dialog allows you to select an address from the Type drop-down box shown below *(Default = Any Address)*.



COMODO Address

□ Exclude (i.e. NOT the choice below)

Type: Any Address

Select 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.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

2. Select the address to be blocked and click OK

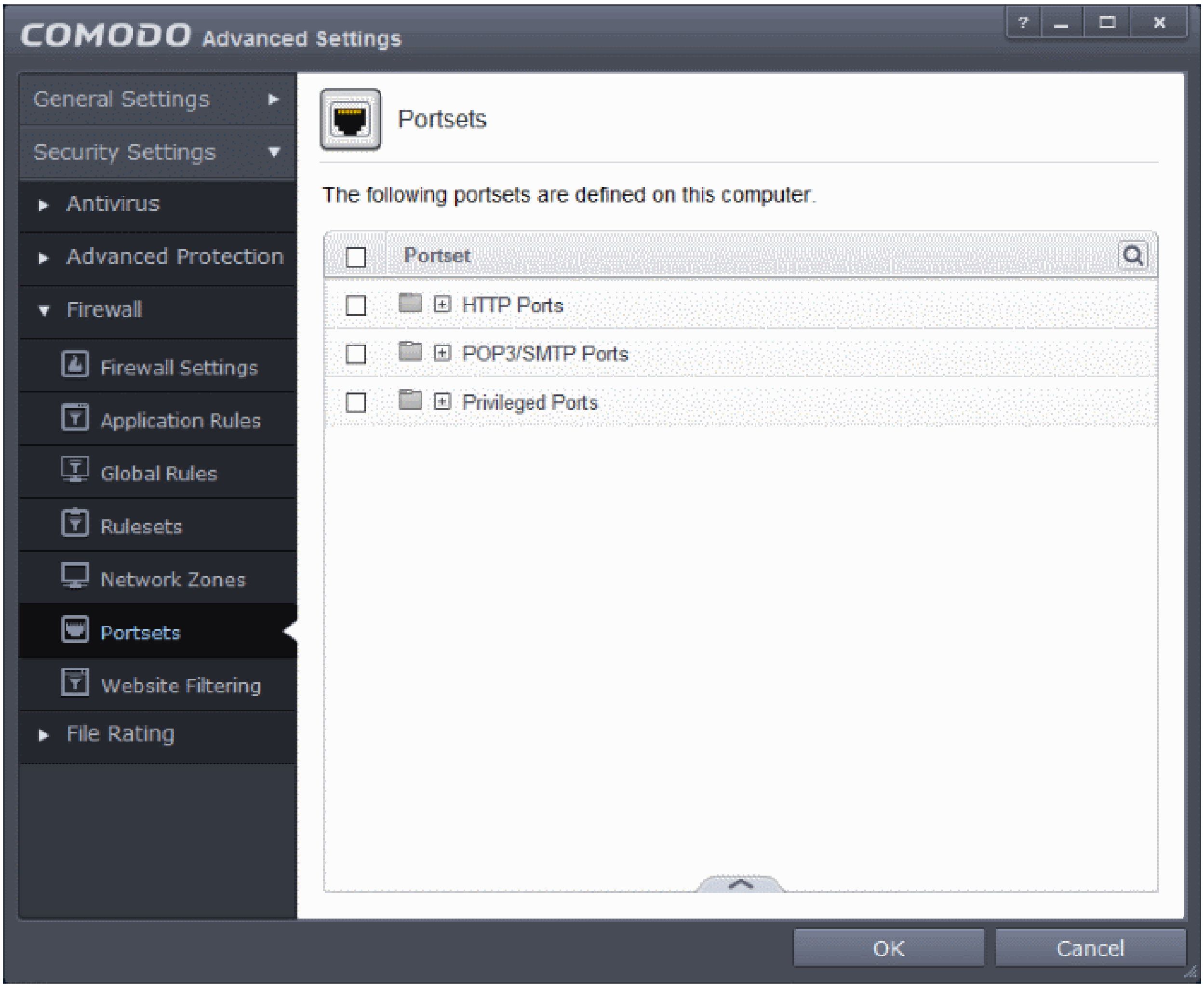
The address(es) you blocked will appear under the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

6.2.3.6. Port Sets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple Application Rules and Global Rules.

- The 'Port Sets' panel allows you to view and manage pre-defined port sets and to add new port sets
- The panel can be accessed by clicking Security Settings > Firewall > Portsets from the 'Advanced Tasks' interface



Portsets

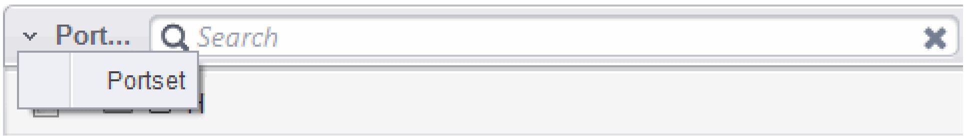
The following portsets are defined on this computer.

□	Portset
□	⊞ HTTP Ports
□	⊞ POP3/SMTP Ports
□	⊞ Privileged Ports

Port Sets are displayed in a tree structure. Click the + button beside a port set name to view ports contained in the set. The default port sets shipped with Comodo Client Security are:

- **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, 993, 995, 465 and 587. These are the ports that are typically used by mail clients like Outlook Express and WinMail for communication using the POP3, SMTP and IMAP protocols.
- **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 use the search option to find a specific port set in the list by clicking the search icon 🔍 at the far right in the column header.



- Enter the name of the port set to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.

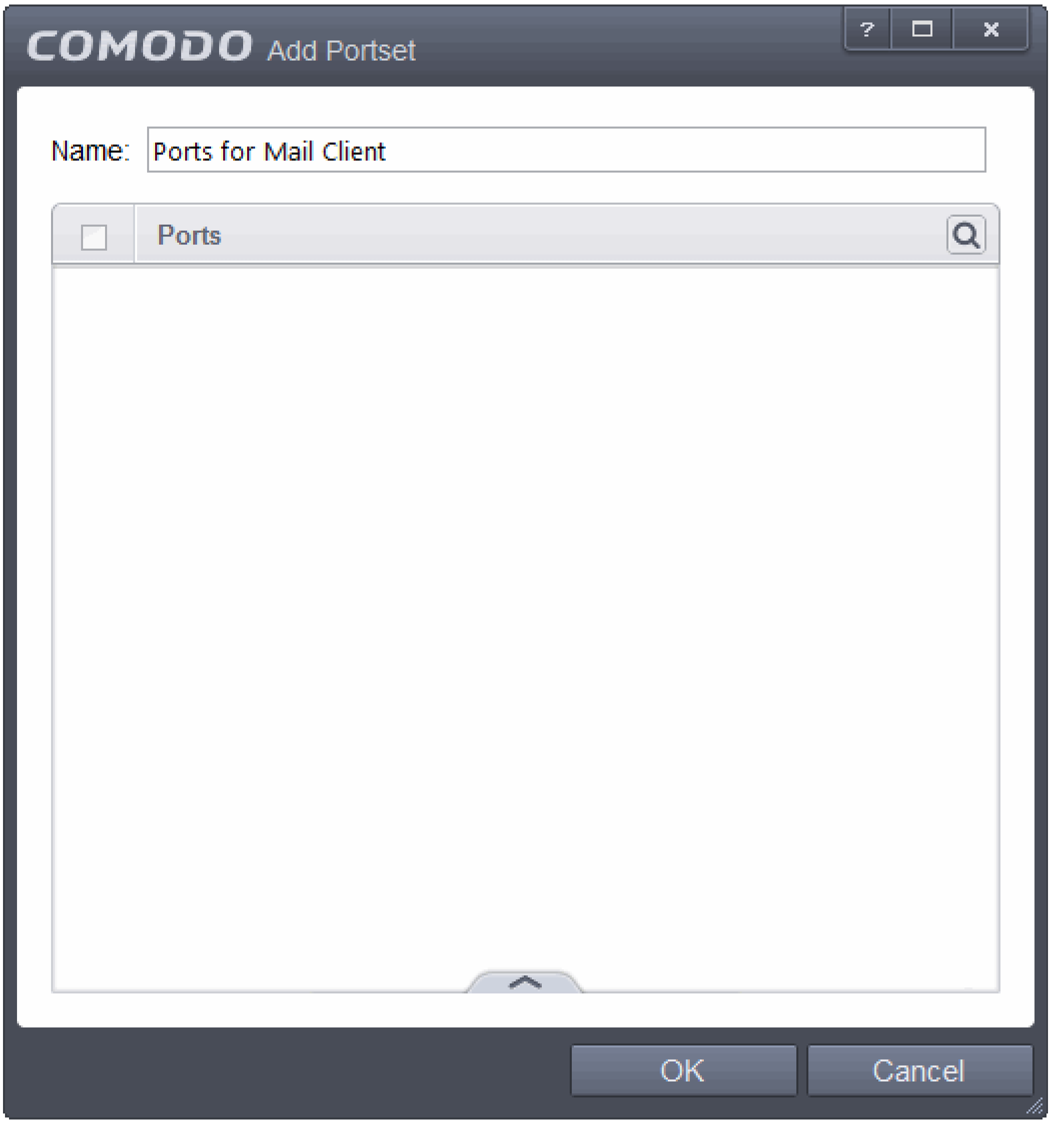
- Click the ✕ icon in the search field to close the search option.

Defining a new Port Set

You can create new portsets and allow applications to access them through the Application Rule interface. Refer to 'Creating or Modifying Firewall Rules' for more details.

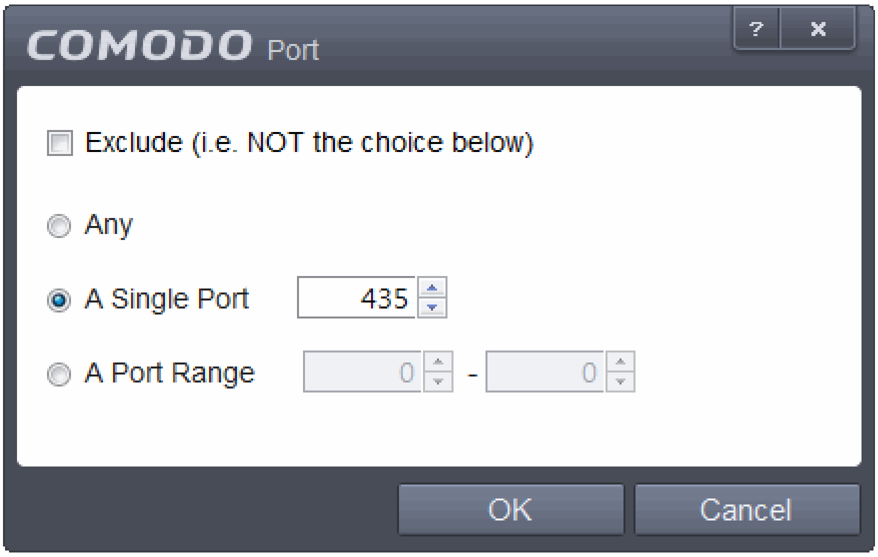
To add a new portset

1. Click the handle at the bottom of the Portsets interface and select 'Add' from the options. The 'Add Portset' dialog will open.



Name: Ports for Mail Client

2. Enter a name for the new portset in the Name field.
3. To add ports to the new portset, click the handle at the bottom and choose Add from the 'Add Portset' dialog.



□ Exclude (i.e. NOT the choice below)

○ Any

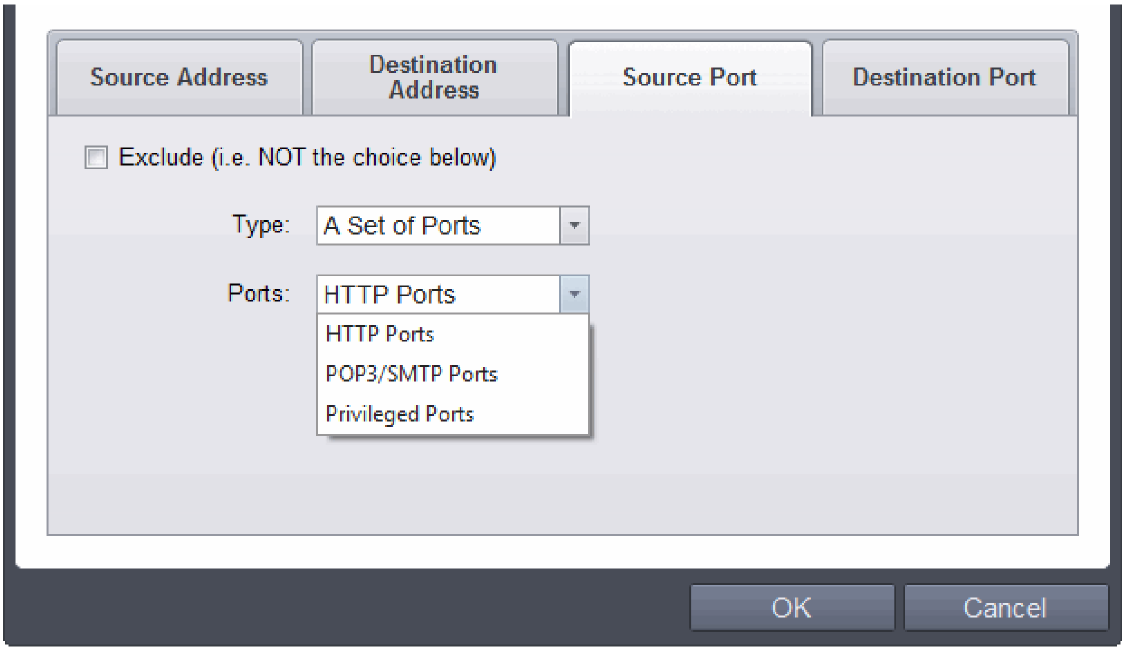
● A Single Port 435

○ A Port Range 0 - 0

4. Specify the ports to be included in the new portset:
   - **Any -** to choose all ports;
   - **A single port -** Define the port number in the combo box beside;
   - **A port range -** Enter the start and end port numbers in the respective combo boxes.
   - Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.
5. Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Add 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



□ Exclude (i.e. NOT the choice below)

Type: A Set of Ports

Ports: HTTP Ports

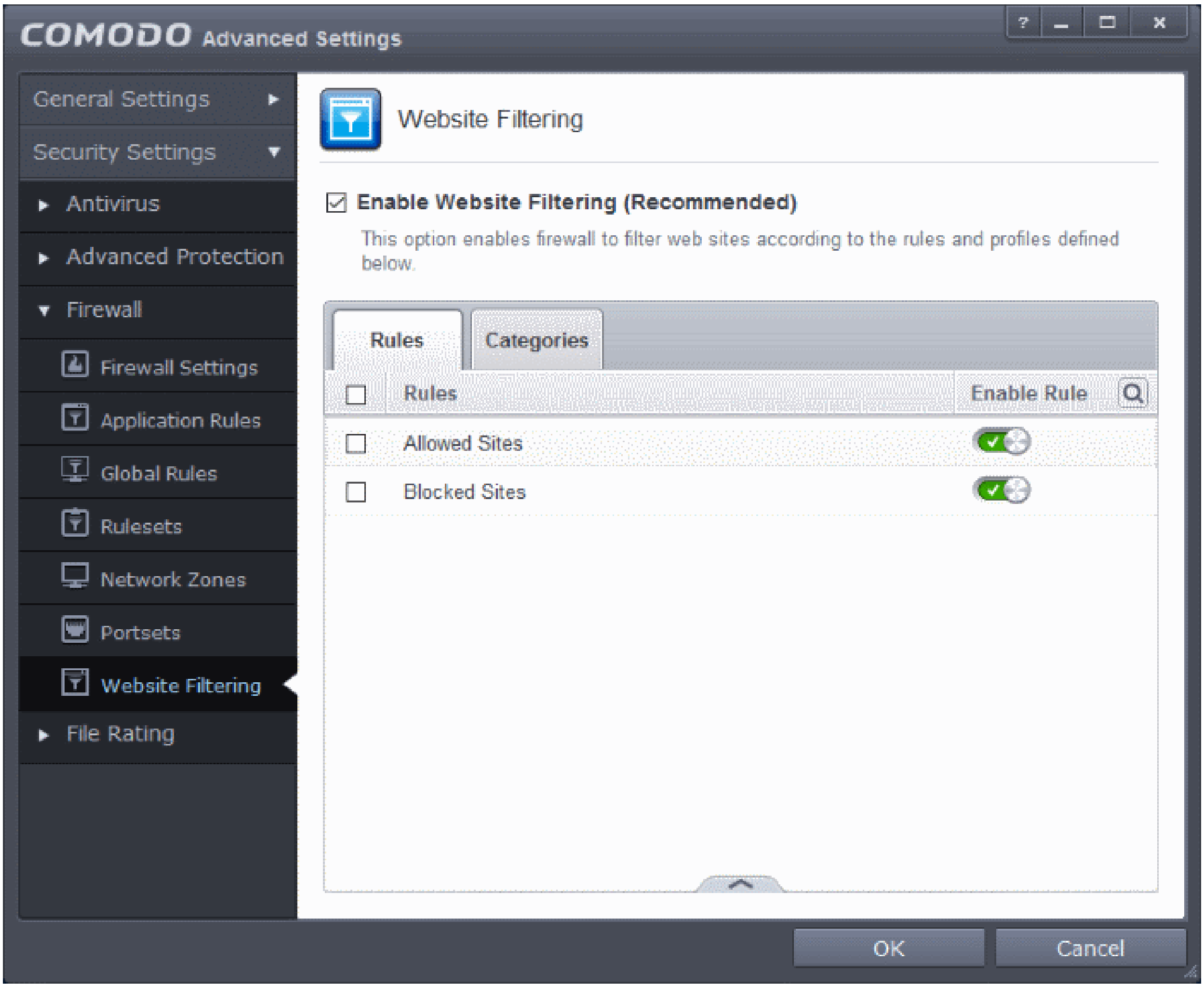
To edit an existing port set

- Select the portset from the 'Portsets' interface, click the handle from the bottom center and select 'Edit' to bring up the 'Edit Portset' dialog.
- The editing procedure is similar to adding the portset explained above.

6.2.3.7. Website Filtering

The Website filtering interface allows you to set up rules to allow or block access to specific websites. Rules can be created for particular users of your computer, which makes this feature very useful for both home and work environments. For example, parents can block juvenile users from visiting inappropriate websites while companies can prevent employees from visiting social networking sites during working hours. You also have the option to create a log event whenever a user tries to visit a website which is in conflict with a rule.

The Website Filtering panel can be accessed by clicking Security Settings > Firewall > Website Filtering tab from 'Advanced Settings' interface.



☑ **Enable Website Filtering (Recommended)**

This option enables firewall to filter web sites according to the rules and profiles defined below.

□	Rules	Enable Rule
□	Allowed Sites	✓
□	Blocked Sites	✓

Brief overview:

- Rules are constructed from one or more 'categories'.
- A category is a collection of one or more URL 'patterns'.
- A URL pattern can be a straight list of domain names and/or filtered terms (for example 'contains', 'starts with', 'equal to', etc.)
- You must set a rule to be 'Allow', 'Block' or 'Ask' and must specify to which users it should apply.

CCS ships with four preset categories of Websites which can be added to rules that you create. Three of these are non-modifiable lists which are managed by Comodo. These are 'Comodo Safe category', 'Comodo Phishing category' and 'Comodo Malware category'. The fourth preset, 'Exclusions', is empty by default but allows you to specify websites that should be allowed. You should add URLs to the 'Exclusions' category over time if you find you require access to a website which is blocked by a category.

CCS also ships with two predefined rules, 'Allowed Sites' and 'Blocked sites', both of which are modifiable. If switched on, the 'Blocked sites' rule will proactively block access to websites in the 'Comodo defined Malware sites'

and 'Comodo defined Phishing Sites' categories. If you wish, you can add other categories to this rule to expand its coverage. The 'Allowed Sites' rule will permit access to websites in the Comodo 'Safe Sites' category and 'Exclusions' categories.
To set up a new rule of your own, click the 'Rules' tab, click 'Add', name your rule, add categories to the rule, specify to which users it should apply and whether it should be 'Allow', 'Block' or 'Ask'.

The 'Website Filtering' panel has two tabs:

- Rules - Allows you to define Website Filtering Rules and assign to required users. Refer to the section 'Creating or Modifying Website Filtering Rules' for more details.
- Categories - Allows you to define categories of Websites to be allowed or blocked in Website filtering rules. Refer to the section 'Defining or Modifying website Categories' for more details.

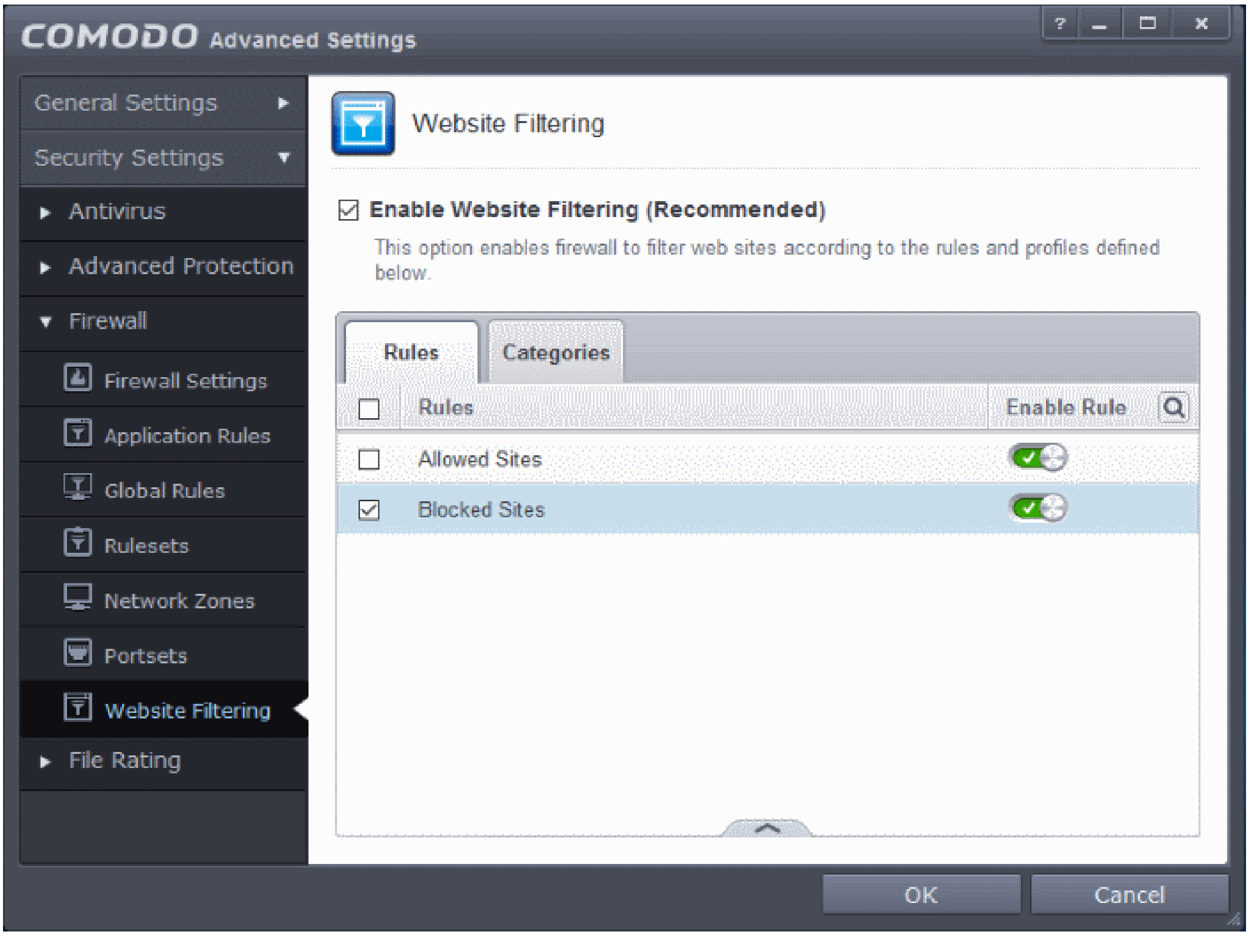
General Advice:

- It is the 'Categories' section where you specify the website(s) you wish to block or allow, not the 'Rules' section. A rule is mainly for specifying the user(s) for whom a category of URLs should be filtered and whether those categories should be allowed or blocked.
- When creating a new rule, you will be required to specify which categories should be included. You can elect to use just the pre-defined Comodo categories but, if you wish to filter specific websites, you will need to create your own category.
- For example, if you wanted to create a category to block youtube.com and certain other leisure websites, you would click 'Categories' > 'Add Category' > *Type name for category* > *Select your new category in list* > 'Add Website' > *Type www.youtube.com.* Click 'Add Website' again to add more sites. You will now be able to select this category when creating a rule for a user(s).
- Refer to the section 'Defining or Modifying Website Categories' for more details on specifying Website categories.

6.2.3.7.1. Creating and Modifying Website Filtering Rules

The 'Rules' tab allows you to create, view, edit and specify exceptions to your website filtering rules. The powerful rule-configuration interface lets you create rules which are as sweeping or as granular as you require. Rules can be created on a per-user basis, allowing you to control exactly which websites certain people can or cannot visit. You can also disable or enable a rule as required at any time.

Comodo Firewall implements rules for the currently logged-in user based on the order they are in this list. Should a conflict exist between individual rules, then the rules at the top takes priority. Click the handle and use the 'Move Up' or 'Move Down' buttons to change a rule's priority.

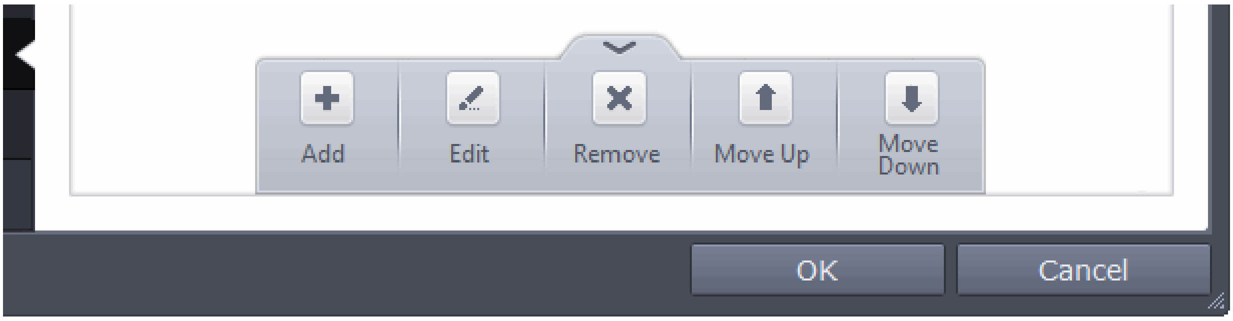


☑ Enable Website Filtering (Recommended)

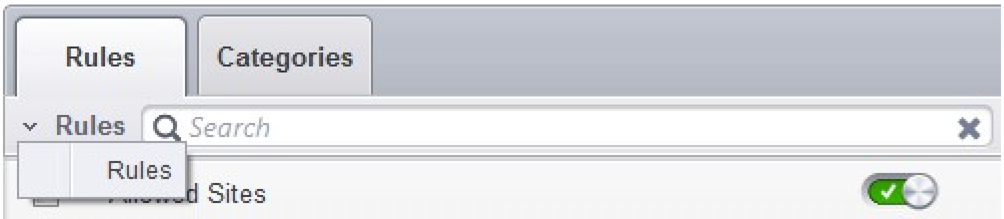
This option enables firewall to filter web sites according to the rules and profiles defined below.

□ Rules	Enable Rule
□ Allowed Sites	✓
☑ Blocked Sites	✓

- The switches in the 'Enable Rule' column enable you to quickly turn a rule on or off
- The check-boxes next to a rule name allow you to select it for editing, removing or re-prioritizing using the controls at the bottom of the interface:



You can search for a specific rule by clicking the search icon at the far right in the column header.



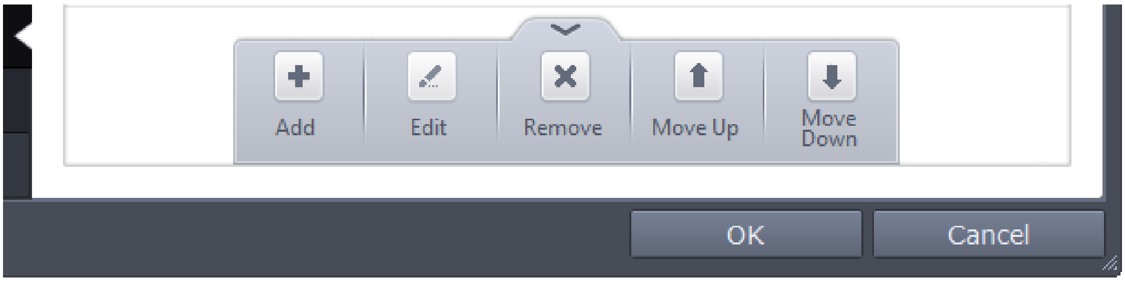
- Enter full or part of the name of the rule in the search field.
- Click the right or left arrow at the far right to begin the search.
- Click the ✖ icon in the search field to close the search option.

The Rules interface allows you to:

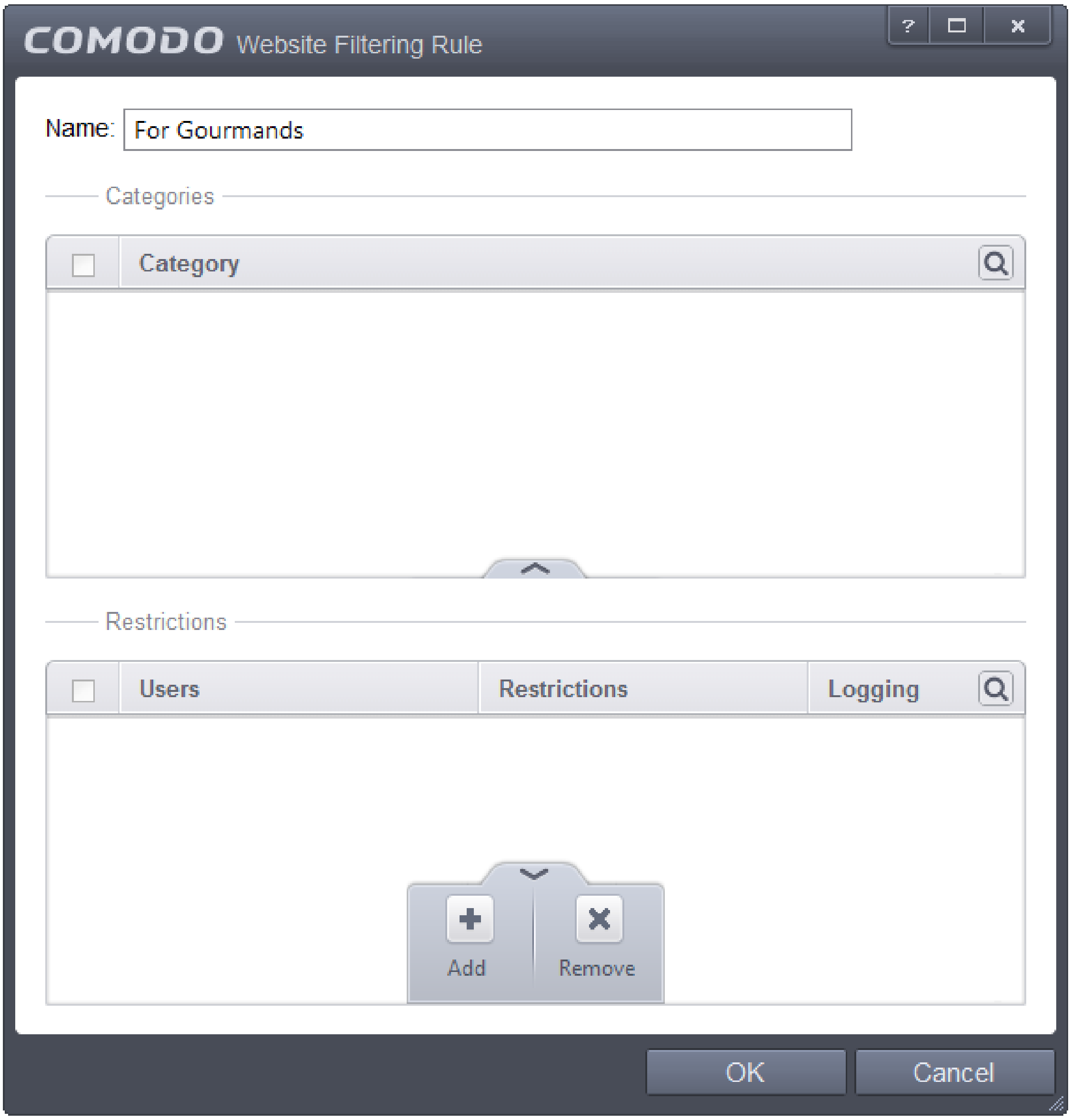
- Create new URL filtering Rules
- Edit existing rules
- Change priority of the rules
- Remove unwanted rules

To create a new Website filtering rule

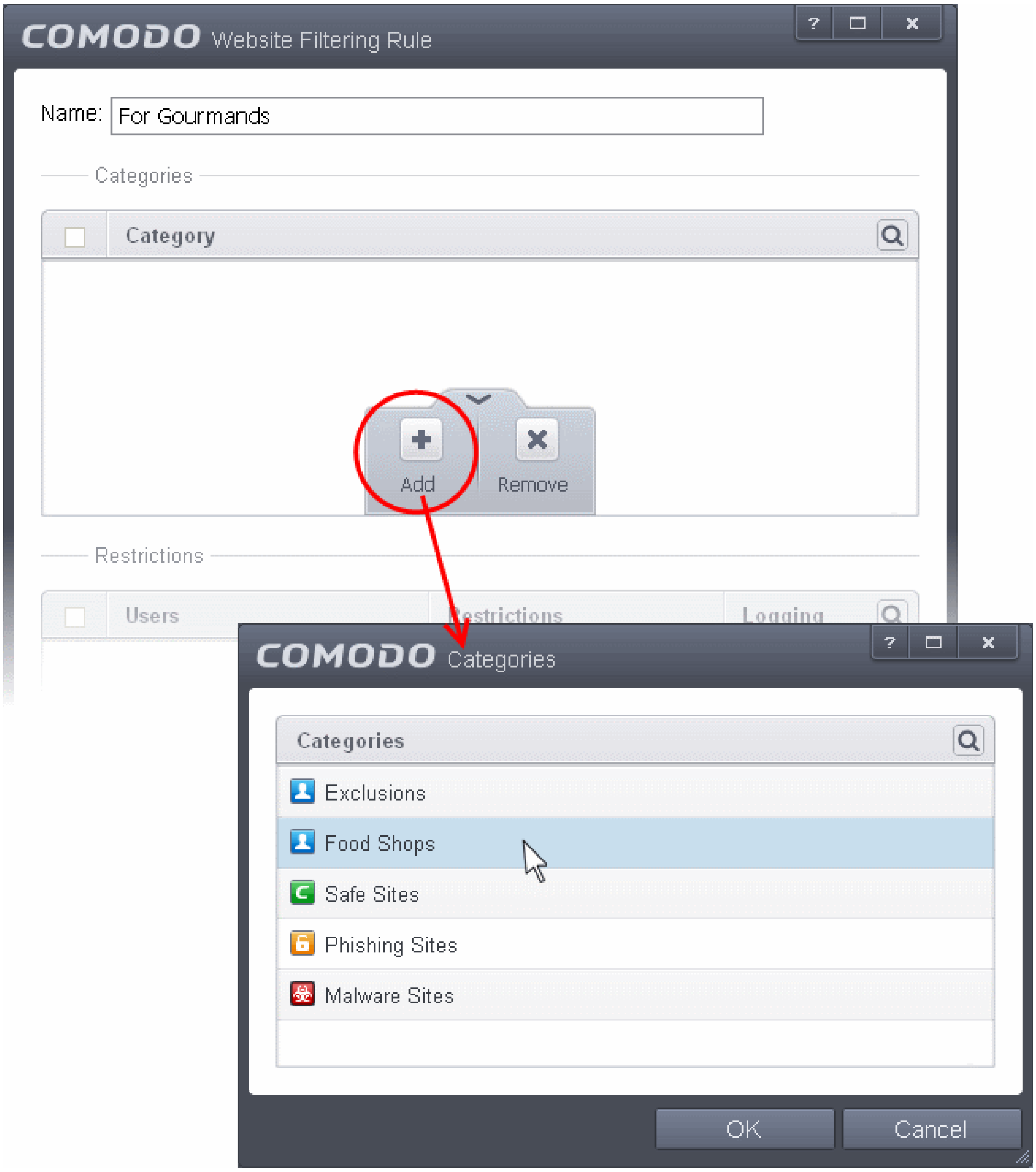
1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' from the 'Advanced Settings' interface
2. Click the handle at the bottom of the Rules interface and select 'Add':



3. Enter a name for your new filter.



4. Select the categories that should be added to the filter:
    - Click the handle at the bottom of the 'Category' pane and choose 'Add'.



COMODO Website Filtering Rule

Name: For Gourmands

Categories

COMODO Categories

Categories
Exclusions
Food Shops
Safe Sites
Phishing Sites
Malware Sites

Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

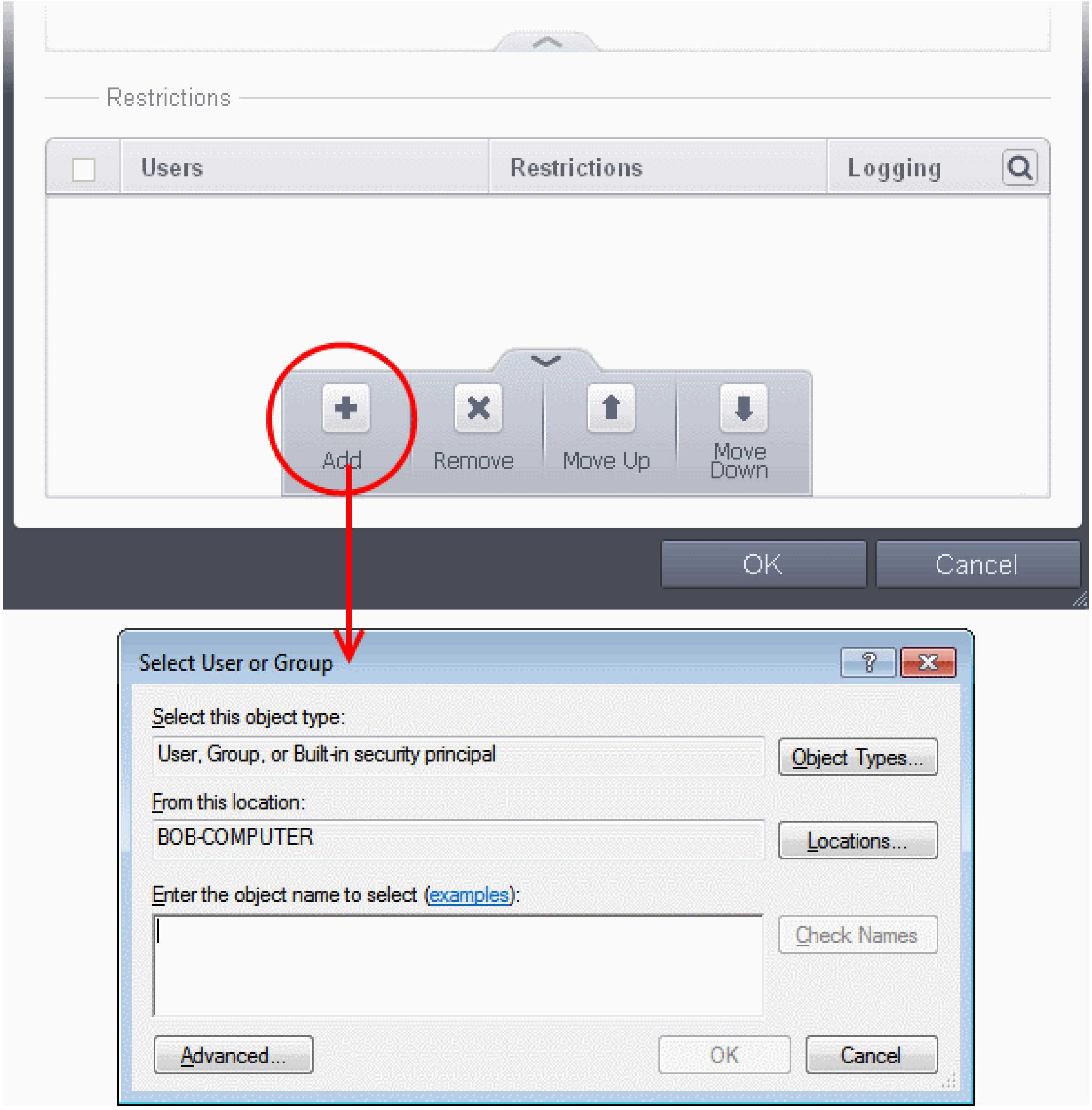
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Comodo Safe Category** - URLs of websites that are considered safe according to global whitelist
- **Comodo Phishing Category** - URLs of websites that lead to phishing websites, as per dynamically updated Comodo Blacklist
- **Comodo Malware Category** - URLs of websites that may inject malware into your system, as per dynamically updated Comodo Blacklist

For more details on creating and modifying user specified categories, Refer to the section **Defining or Modifying Website Categories**

5. Add Users or User Groups to whom the rule should be applied:

- Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:

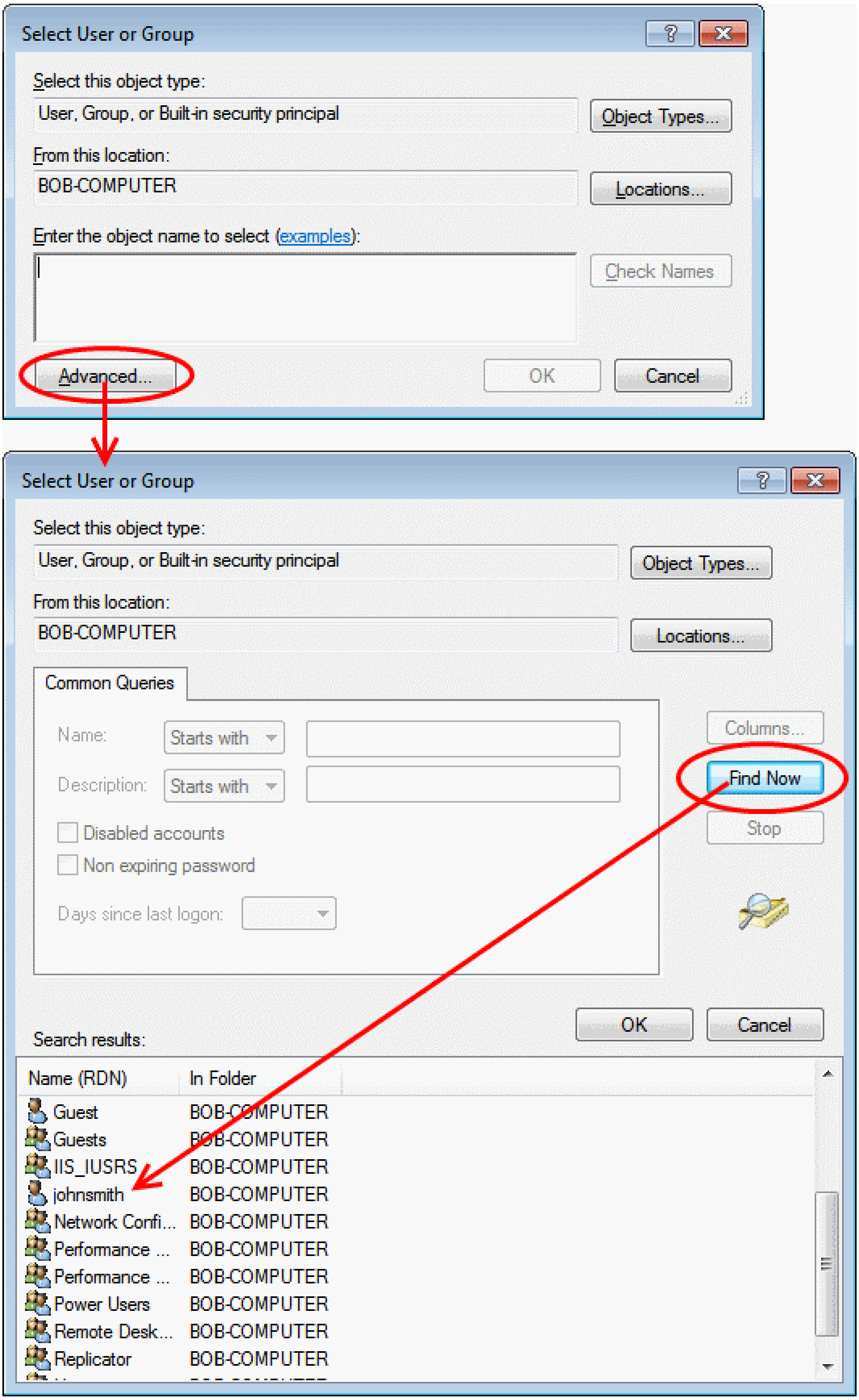


Select this object type:
User, Group, or Built-in security principal

From this location:
BOB-COMPUTER

Enter the object name to select (examples):

- Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format \ or @. Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



Select this object type: User, Group, or Built-in security principal

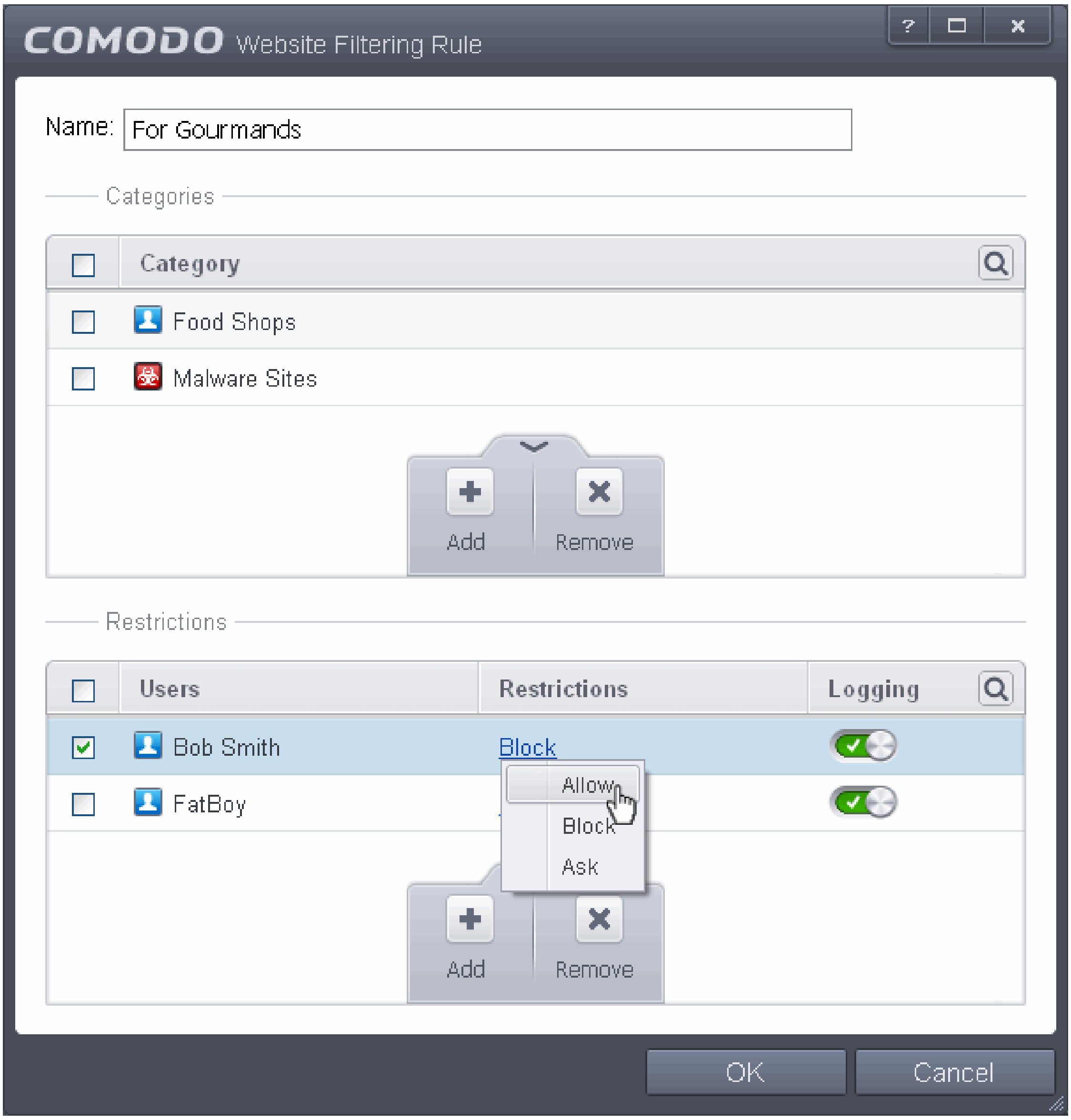
From this location: BOB-COMPUTER

□ Disabled accounts

□ Non expiring password

Name (RDN)	In Folder
Guest	BOB-COMPUTER
Guests	BOB-COMPUTER
IIS_IUSRS	BOB-COMPUTER
johnsmith	BOB-COMPUTER
Network Confi...	BOB-COMPUTER
Performance ...	BOB-COMPUTER
Performance ...	BOB-COMPUTER
Power Users	BOB-COMPUTER
Remote Desk...	BOB-COMPUTER
Replicator	BOB-COMPUTER

After adding target users or groups, you next need to specify whether those users should be allowed or blocked from viewing the websites in the category or they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:



COMODO Website Filtering Rule

Name: For Gourmands

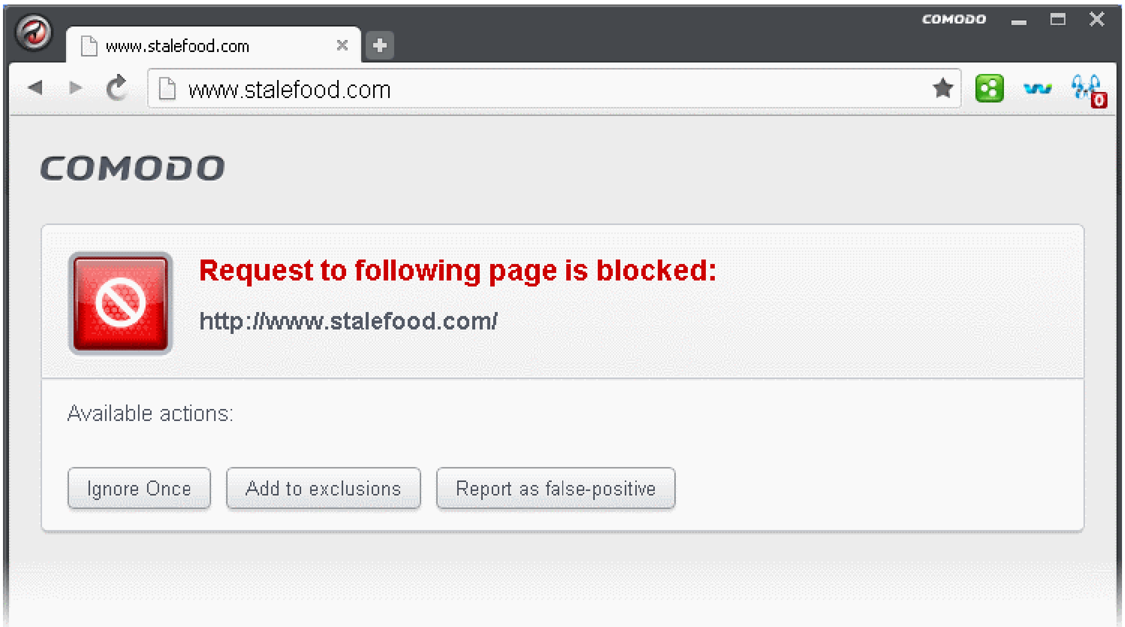
Categories

□	Category
□	Food Shops
□	Malware Sites

Restrictions

□	Users	Restrictions	Logging
☑	Bob Smith	Block	✓
□	FatBoy		✓

- **Allow** - The websites in the categories can be accessed by the user.
- **Block** - The websites in the categories cannot be accessed by the user.
- **Ask** - An alert will be displayed in the browser (shown below) if the user tries to access any of the websites in the category. The user can decide whether or not to continue.



Request to following page is blocked:

http://www.stalefood.com/

Available actions:

6. Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.
7. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
8. Make sure that the rule is enabled using the toggle switch under the Enable Rule column for the rule to take effect.

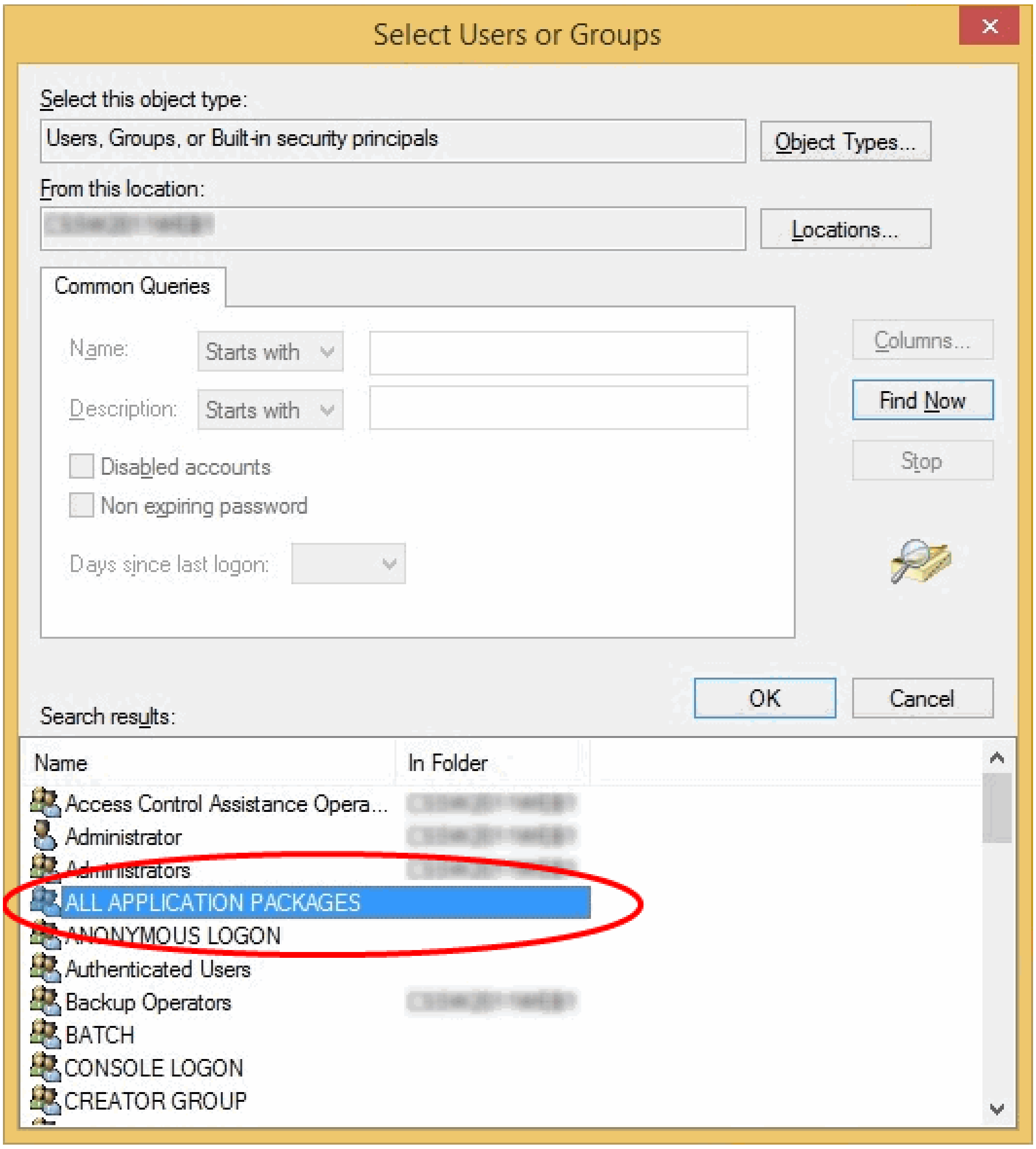
    - You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Important Note to Windows 8 and Windows 8.1 users: If you are using Internet Explorer 11 version 11.0.9600.16384, it is mandatory to add the user group 'ALL APPLICATION PACKAGES' to the Restrictions list in addition to the intended users for each rule you create.

If you or other users access websites using Internet Explorer 11 on Windows 8/8.1, then you must add this user group or your rules will have no effect. For example, users will still be able to access blocked websites.

To add 'ALL APPLICATION PACKAGES' to the restrictions list

- Click 'Advanced' in the 'Select User or Group' dialog
-



Select Users or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
[redacted]

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

□ Non expiring password

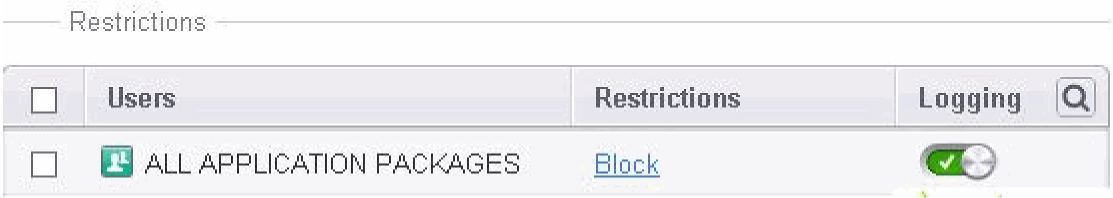
Days since last logon:

Search results:

Name	In Folder
Access Control Assistance Opera...	[redacted]
Administrator	[redacted]
Administrators	[redacted]
ALL APPLICATION PACKAGES	
ANONYMOUS LOGON	
Authenticated Users	
Backup Operators	[redacted]
BATCH	
CONSOLE LOGON	
CREATOR GROUP	

Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom

- Click 'OK '



Restrictions

□	Users	Restrictions	Logging
□	ALL APPLICATION PACKAGES	Block	✓

To edit existing rules

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface

2. Choose the Website Filtering Rule to be edited under the 'Rules' tab by selecting the checkbox beside the rule.

3. Click the handle from the bottom center of the Rules interface and choose 'Edit' from the options.

The ' Website Filtering Rule' interface for the selected rule will open. You can add/remove categories, add/remove users or change the restriction for selected users from this interface. Refer to **To create a new Website Filtering Rule** for more details on this interface.

To remove a Website Filtering Rule

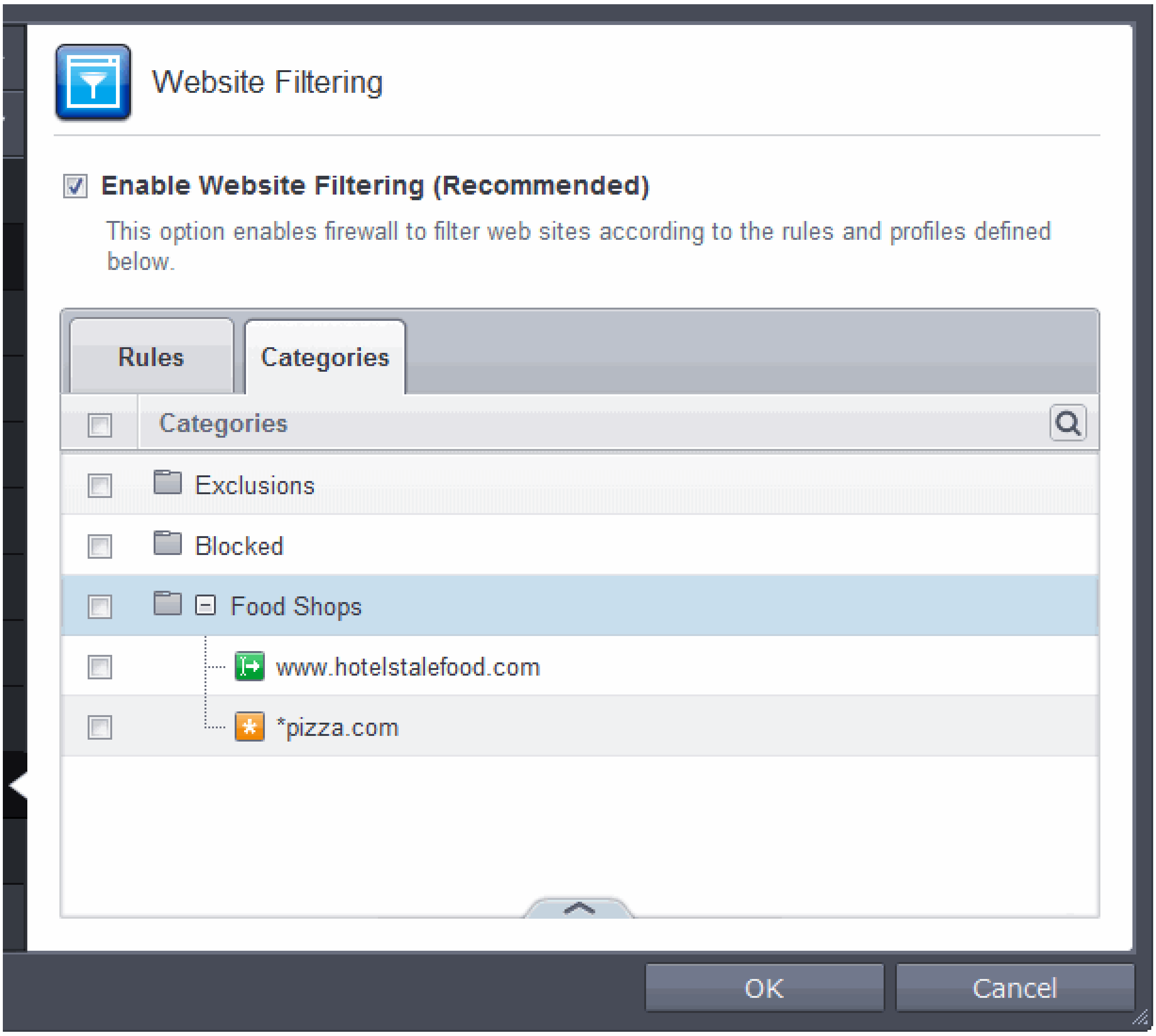
1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule(s) to be removed under the 'Rules' tab by selecting the checkbox(es) beside them.
3. Click the handle from the bottom center of the Rules interface and choose 'Remove' from the options.

To change the priority of Website Filtering Rules

1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule to be moved under the 'Rules' tab by selecting the check box beside the rule.
3. Click the handle from the bottom center of the Rules interface and choose 'Move Up' or 'Move Down' option to change the order of the rules in the interface.

6.2.3.7.2. Defining or Modifying Website Categories

The Categories pane displays a list of user defined Website categories that can be applied in the Website Filtering Rules. A Category can contain a full URL and/or part of URL with wildcard character of the each of the websites to be included in it.



Website Filtering

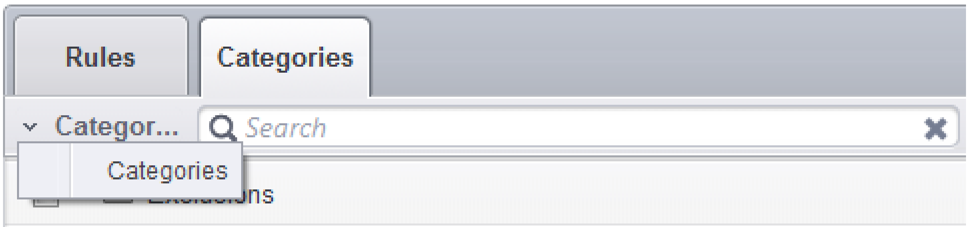
☑ **Enable Website Filtering (Recommended)**

This option enables firewall to filter web sites according to the rules and profiles defined below.

The 'Categories' pane allows you to:

- Add a new category of Website
- Rename a Category
- Remove unwanted Website from category
- Remove a Category

You can search for a specific category by clicking the search 🔍 at the far right in the column header.



- Enter full or part of the name of the category in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

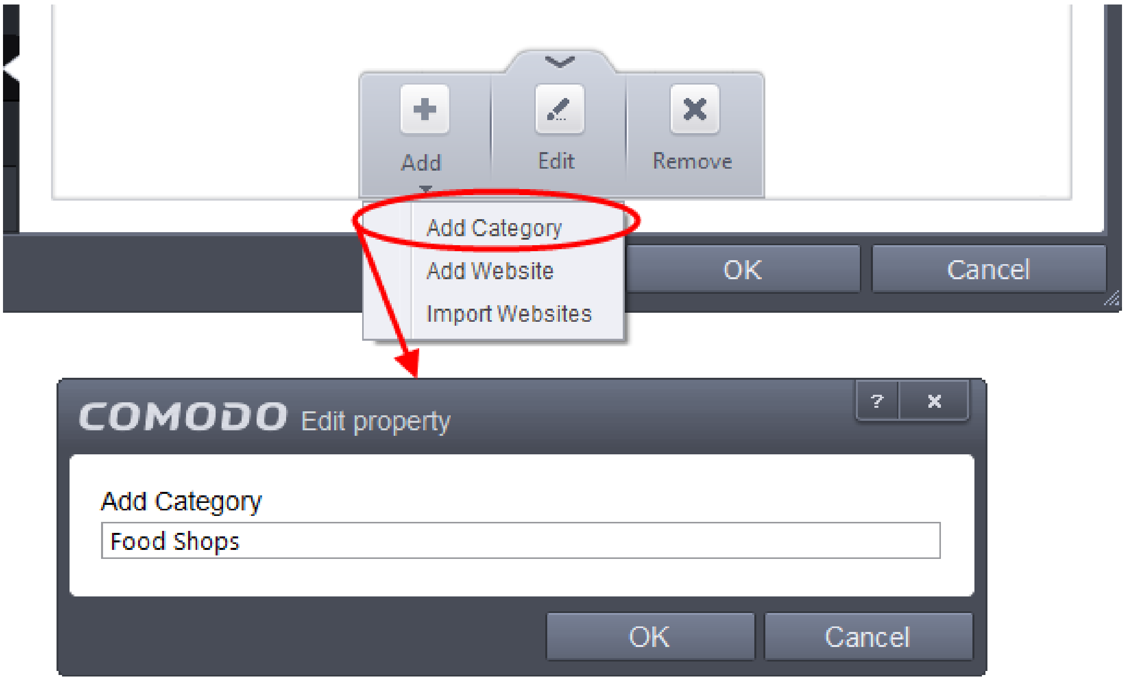
Adding a New Category of Website

Adding a new category involves two steps:

- Step 1 - Define a name for the category
- Step 2 - Add Website to be included to the category

Step 1 - Define a name for the category

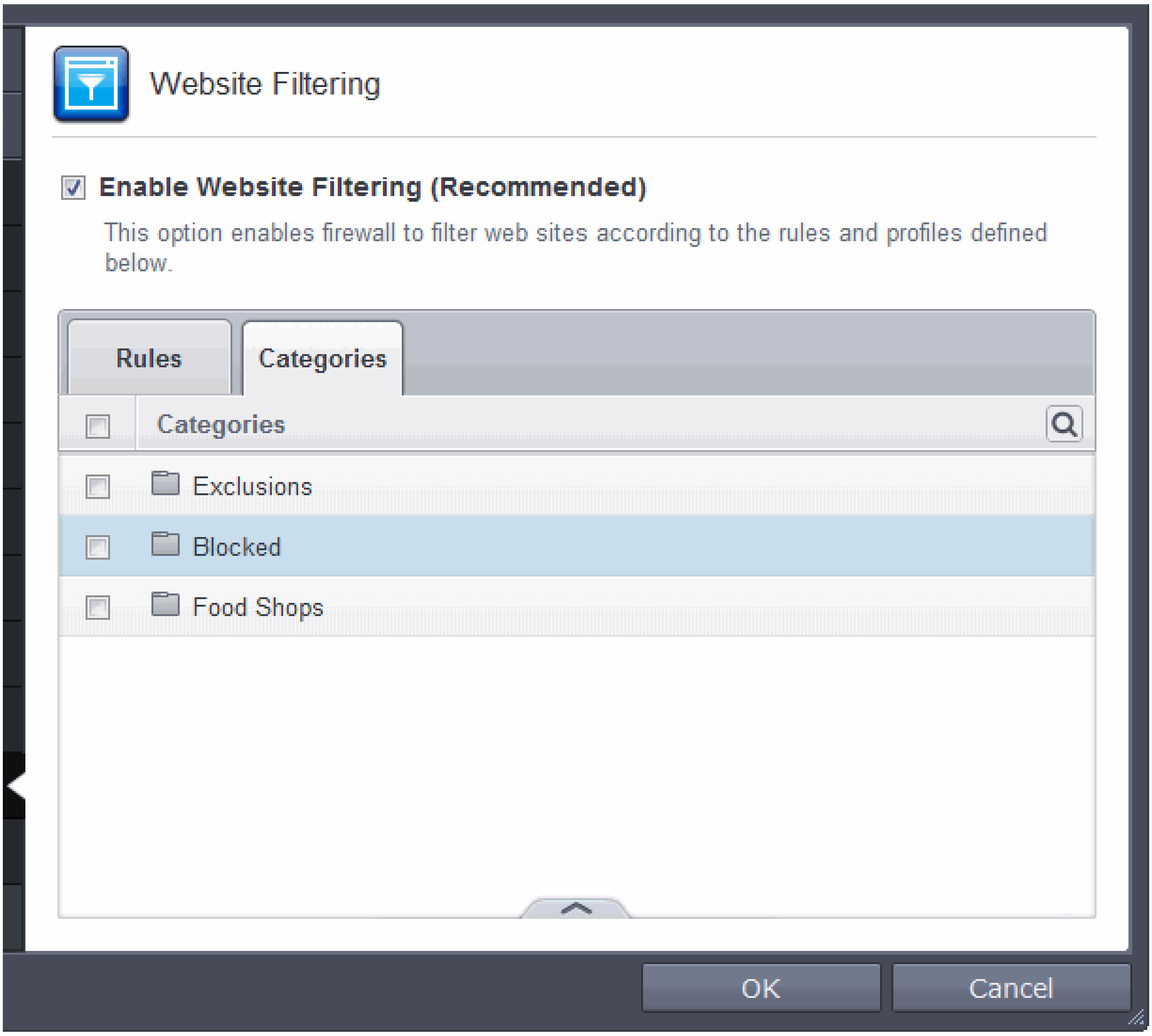
1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Click the handle from the bottom center of the 'Categories' pane, click 'Add' from the options and choose 'Add Category' from the drop-down. The 'Edit Property' dialog will open.



Add Category
Food Shops

4. Enter a name for the category and click 'OK'

The new category will be created and added under the 'Categories' tab.



Website Filtering

☑ Enable Website Filtering (Recommended)

This option enables firewall to filter web sites according to the rules and profiles defined below.

You can add URLs of websites to be included in the category.

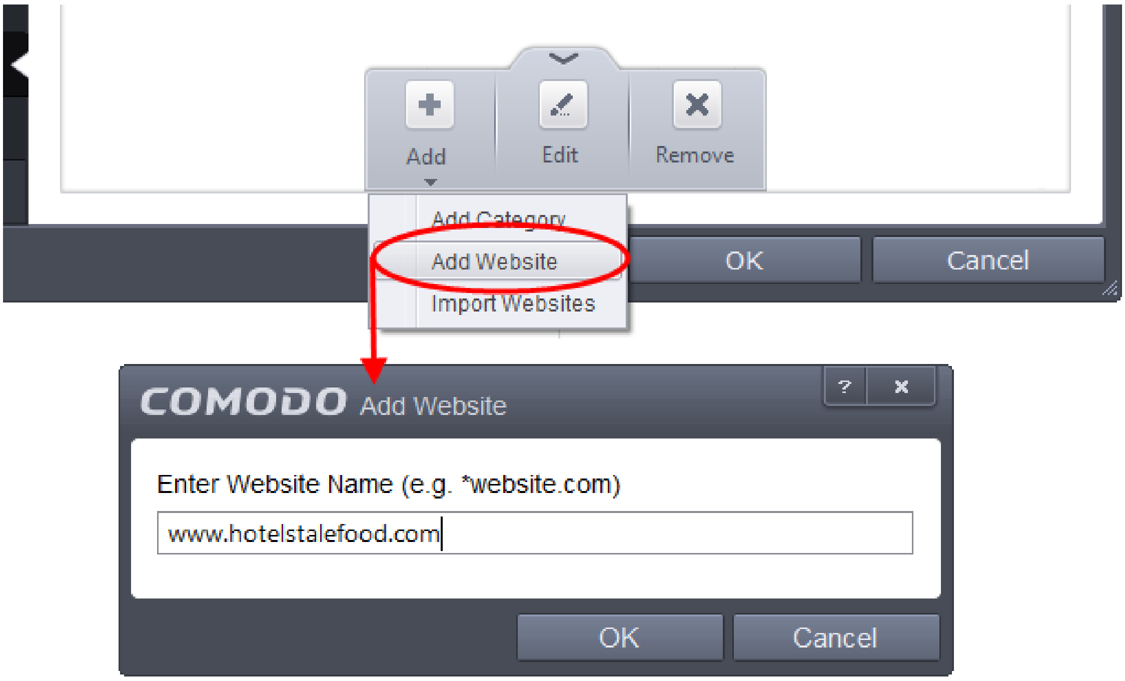
Step 2 - Add URLs to be included to the category

You can add websites to a category in two ways:

- Manually Specify Websites one by one
- Upload Websites from a text file

To manually specify URLs

1. Select the Category under the 'Categories' tab.
2. Click the handle from the bottom of the 'Categories' pane, click 'Add' from the options and choose 'Add Website' from the drop-down. The 'Add Website' dialog will open.



Enter Website Name (e.g. *website.com)

www.hotelstalefood.com

3. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.

To add a specific website/webpage, enter the full URL of the website/webpage

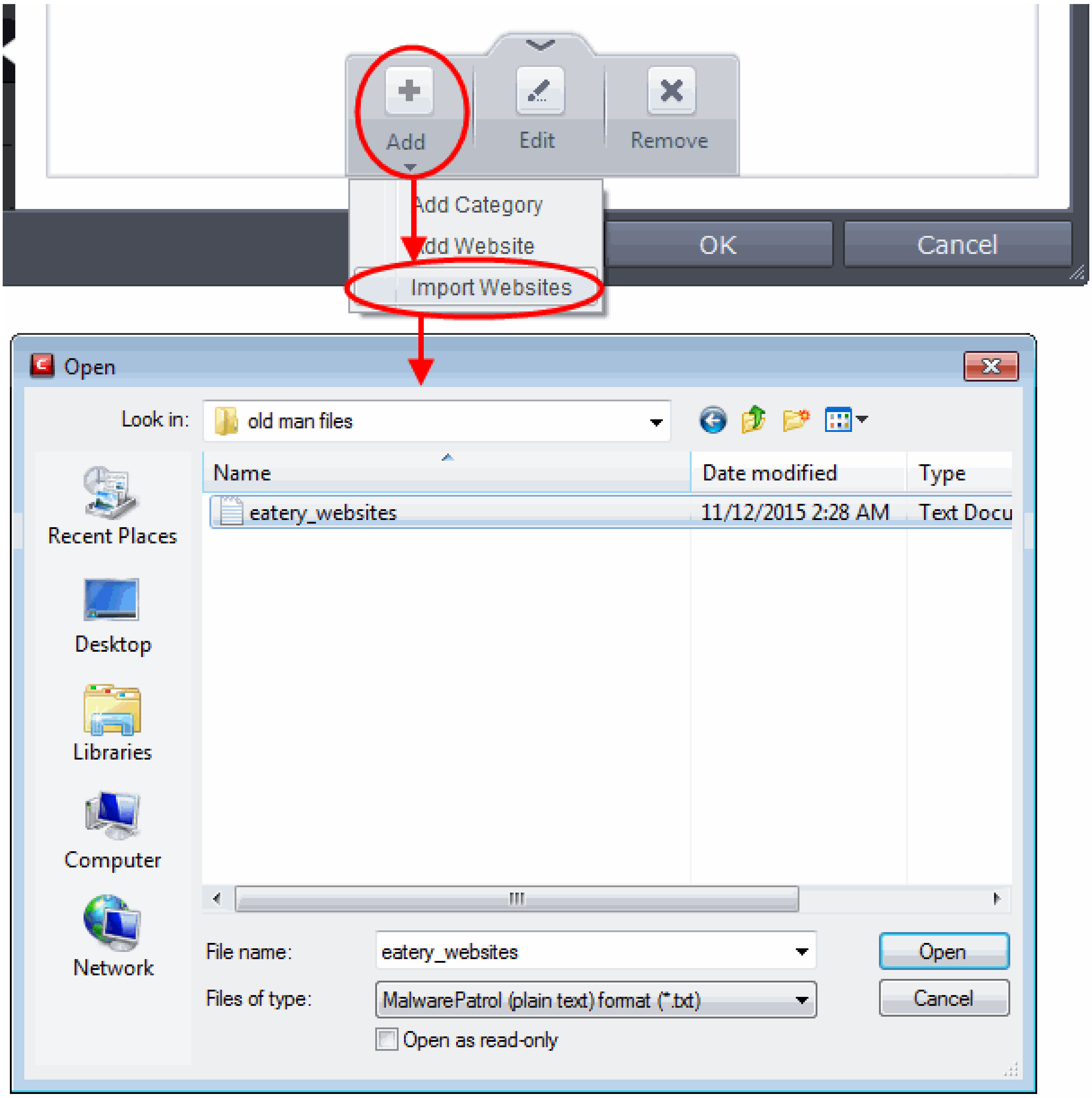
- To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
- To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, “pizza*” will cover 'pizzahut.com', pizzacorner.com, and so on.
- To include all the websites with URLs that contain a specific string, add the wildcard character befor and after the string. For example, “*pizza*” will cover hotpizza.com, spicypizza.com and so on.

The website will be added to the category.

4. Repeat the process to add more websites.

To upload the list of websites from a text file

1. Select the Category under the 'Categories' tab.
2. Click the handle from the bottom of the 'Categories' pane, click 'Add' from the options and choose 'Import Websites' from the drop-down.
3. Navigate to the file containing the list of URLs of the Websites to be added to the category.



Look in: old man files

eatery_websites 11/12/2015 2:28 AM Text Docu

File name: eatery_websites

Files of type: MalwarePatrol (plain text) format (*.txt)

□ Open as read-only

Note: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.

4. Click 'Open'.

CCS will automatically add the websites specified in the text file into the selected category.

To rename a category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Select the category to be renamed.
4. Click the handle from the bottom of the 'Categories' pane and choose 'Edit' from the options. The 'Edit Property' dialog will open.
5. Enter the new name for the category and click 'OK'

The category will be renamed immediately both under the Categories tab and in the Website Filtering Rules to which it is applied.

To remove a Website from a category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Click the + button beside the category to be edited to expand the website list
4. Select the Website(s) to be removed
5. Click the handle from the bottom of the 'Categories' pane and choose 'Remove' from the options.

To remove a Category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Select the Category to be removed
4. Click the handle from the bottom of the 'Categories' pane and choose 'Remove' from the options.

Note: You cannot remove a category which is currently applied in a Website Filtering Rule. Before removing a category, make sure you remove the category from the rules to which it is applied.

6.2.4. Manage File Rating

The file rating system is a cloud-based file lookup service (FLS) that ascertains the reputation of files on your computer. Whenever a file is first accessed, CCS will check the file against Comodo's master white and blacklists.

The file will be awarded trusted status if:

- The application/file is in the trusted local 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.

Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource consumption. On the other hand, files which are identified as malicious will be awarded 'Malicious' status and denied all access rights from other processes or users - effectively cutting them off from the rest of your system. Files which could not be recognized by the rating system are awarded 'Unrecognized' status'. You can review files on the unrecognized list and manually choose to trust/block/delete them or investigate further by sending them to Comodo for analysis/running another file lookup. Refer to the section File List for more details.

Important Note: In order for the software to submit unknown files to our file rating and malware analysis servers (CAMAS), please make sure the following IP addresses and ports are allowed on your network firewall:

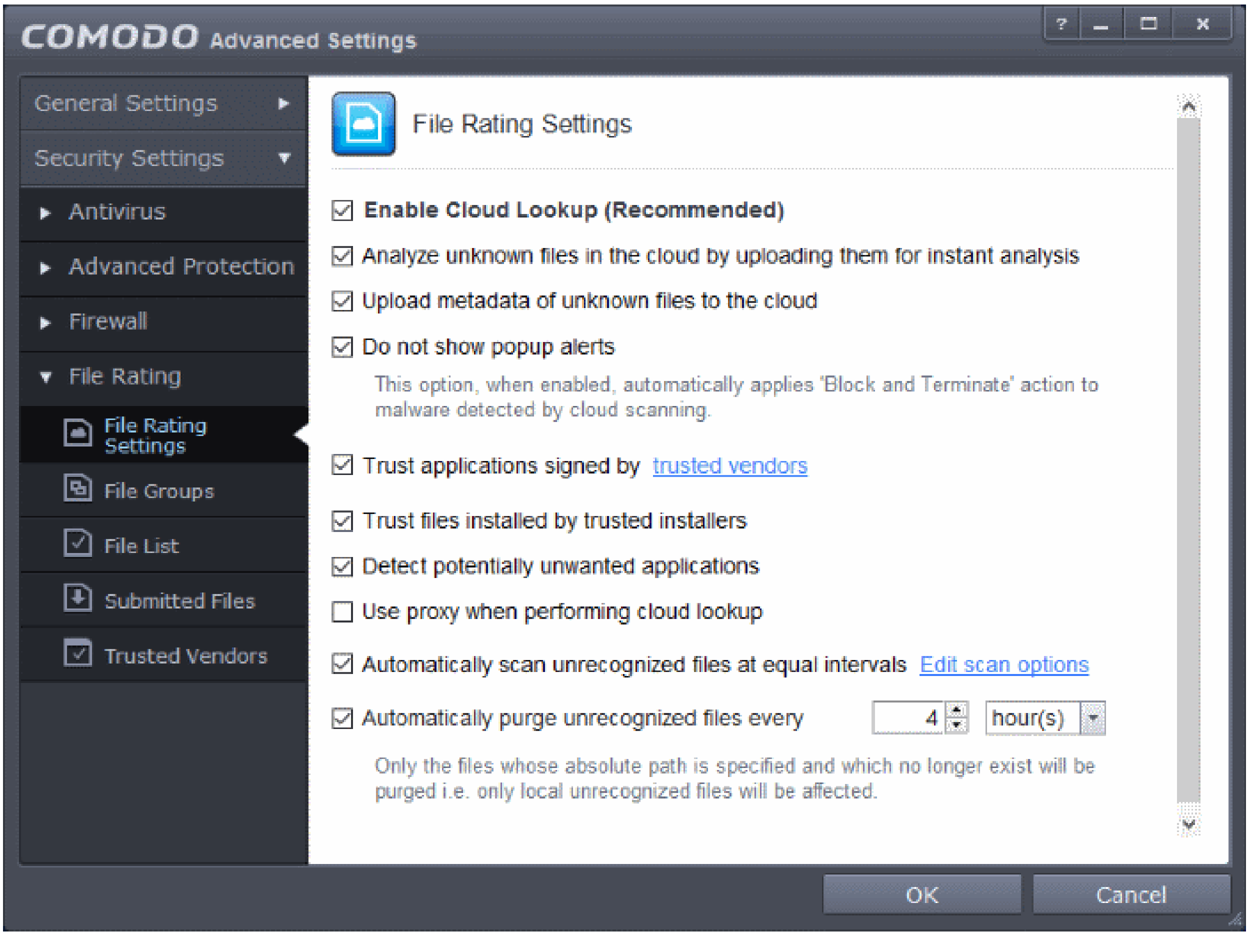
- To allow communication with camas.comodo.com
  - IP that needs to be allowed: 199.66.201.30
  - Port that needs to be allowed: port 80 for TCP
  - Direction: Outgoing (Endpoints to CAMAS)
- To allow communication with our File Lookup Servers (FLSs):
  - IPs that need to be allowed:
    - 91.209.196.27
    - 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: 4447 UDP and 4448 TCP
- Direction: Outgoing (Endpoints to FLSs)

The 'Manage File Rating' area allows you to view and manage the list of programs, applications and executable files discovered from your computer with their assigned file rating. You can also:

- Manually add files and executables to 'Files List' and assign status;
- Submit unrecognized files and view the list of files you submitted;
- View and manage Trusted Software Vendor list;



File Rating Settings

☑ Enable Cloud Lookup (Recommended)

☑ Analyze unknown files in the cloud by uploading them for instant analysis

☑ Upload metadata of unknown files to the cloud

☑ Do not show popup alerts

This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

☑ Detect potentially unwanted applications

☐ Use proxy when performing cloud lookup

☑ Automatically scan unrecognized files at equal intervals Edit scan options

☑ Automatically purge unrecognized files every 4 hour(s)

Only the files whose absolute path is specified and which no longer exist will be purged i.e. only local unrecognized files will be affected.

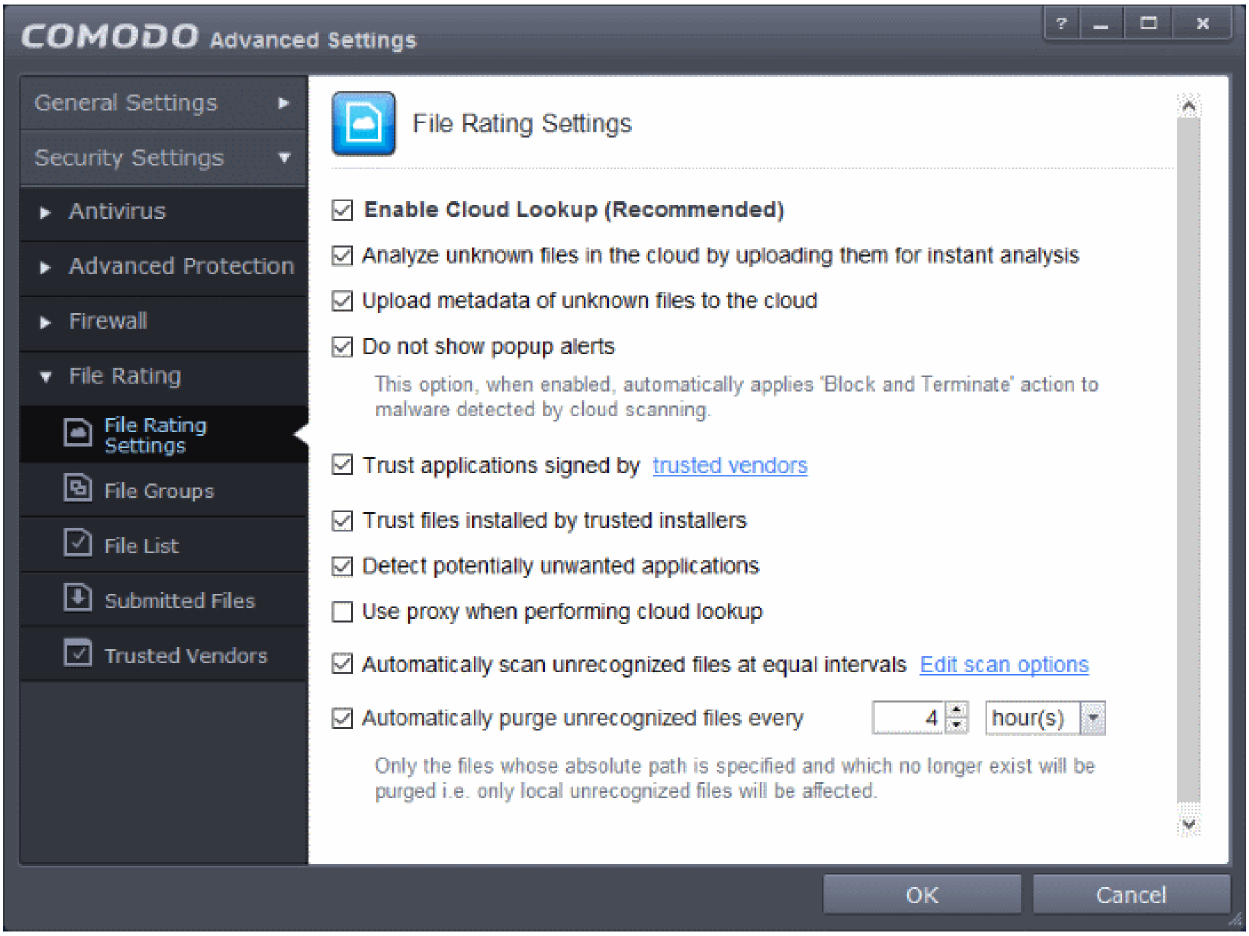
Click the following links to jump to the section you need help with:

- 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 the list of programs. Applications and executable files in your computer with their file rating and manually add files to it
- Submitted Files - View the list of files submitted for analysis to Comodo.
- Trusted Vendors - View the list of trusted software vendors and manually add vendors

6.2.4.1. File Rating Settings

The 'File Rating Settings' panel allows you to configure the overall behavior of the file rating feature.

- The panel can be accessed by opening Advanced Settings > Security Settings > File Rating > File Rating Settings



File Rating Settings

☑ Enable Cloud Lookup (Recommended)

☑ Analyze unknown files in the cloud by uploading them for instant analysis

☑ Upload metadata of unknown files to the cloud

☑ Do not show popup alerts

This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

☑ Detect potentially unwanted applications

☐ Use proxy when performing cloud lookup

☑ Automatically scan unrecognized files at equal intervals Edit scan options

☑ Automatically purge unrecognized files every 4 hour(s)

Only the files whose absolute path is specified and which no longer exist will be purged i.e. only local unrecognized files will be affected.

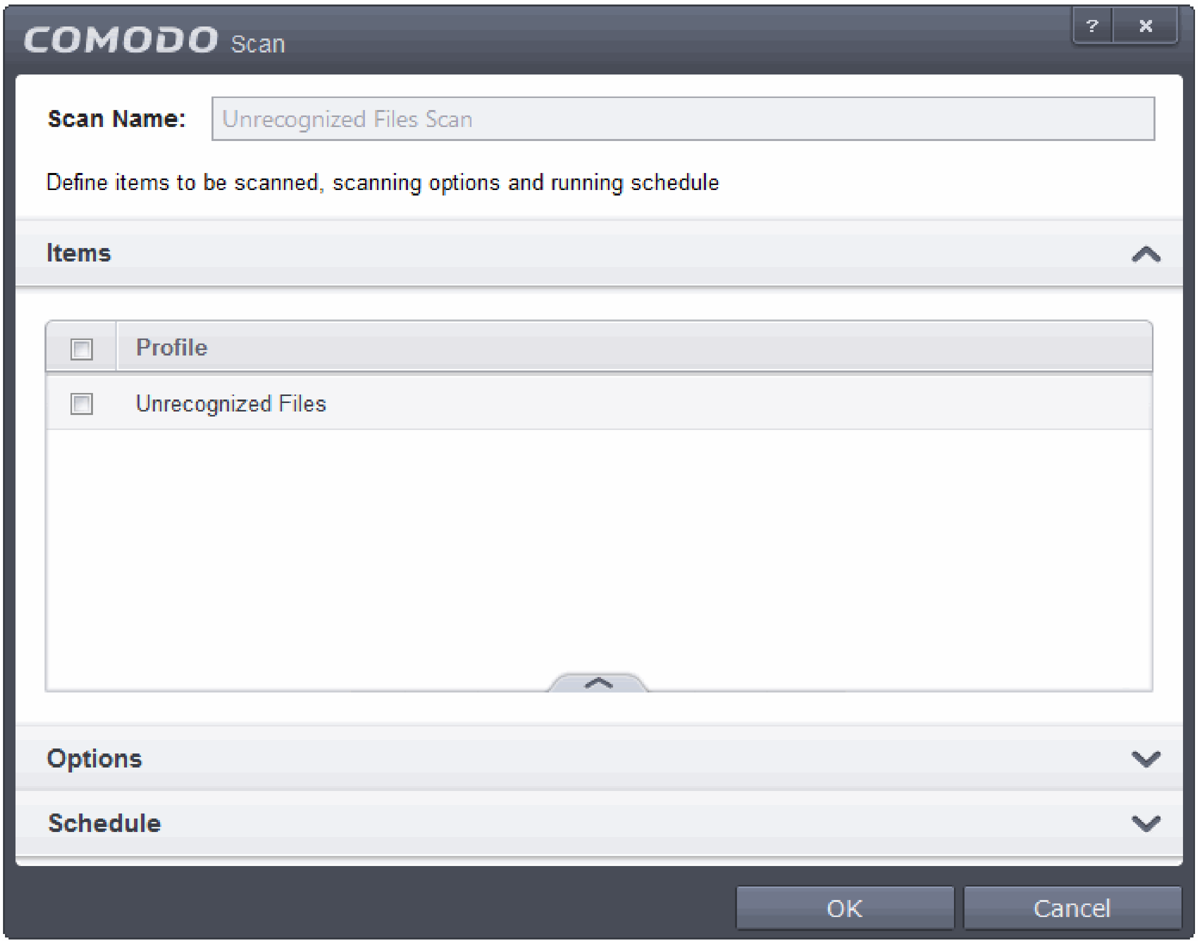
- **Enable Cloud Lookup** - Allows you to enable or disable File Rating.(***Default and recommended =Enabled***)
- **Analyze unknown files in the cloud by uploading them for instant analysis** - Instructs CCS to upload files whose trustworthiness could not be assessed by cloud lookup to Comodo for analysis immediately. The experts at Comodo will analyze the file and add to the whitelist or blacklist according to the analysis. (***Default =Enabled***)
- **Upload metadata of unknown files to the cloud** - If enabled, information about the 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 firewall 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)***
- **Trust applications signed by trusted vendors** - When this option is enabled, CCS will award trusted status to the executables and files that are digitally signed by vendors in the Trusted Vendors list using their code signing certificates. Click the words 'trusted vendors' will open the Trusted Vendors List panel. (***Default =Enabled***)
- **Trust files installed by trusted installers** - When this option is enabled, CCS will consider the executable and files stored by applications that are assigned with Installer or Updater rule under HIPS Rules or the applications. (***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***).

- **Use proxy when performing Cloud Lookup** - When this check box is selected, CCS will submit files to CAMAS for analysis through proxy. (***Default = Disabled***)
- **Automatically scan unrecognized files at equal intervals** - Comodo One 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 choose which files and folders are scanned, when they are scanned and how they are scanned. ***(Default = Enabled)***

  To do this:

  - Select the 'Edit scan options' link
  - Click the handle at the bottom of the interface and select items to be included in the profile:



Scan Name: Unrecognized Files Scan

Define items to be scanned, scanning options and running schedule

□	Profile
□	Unrecognized Files

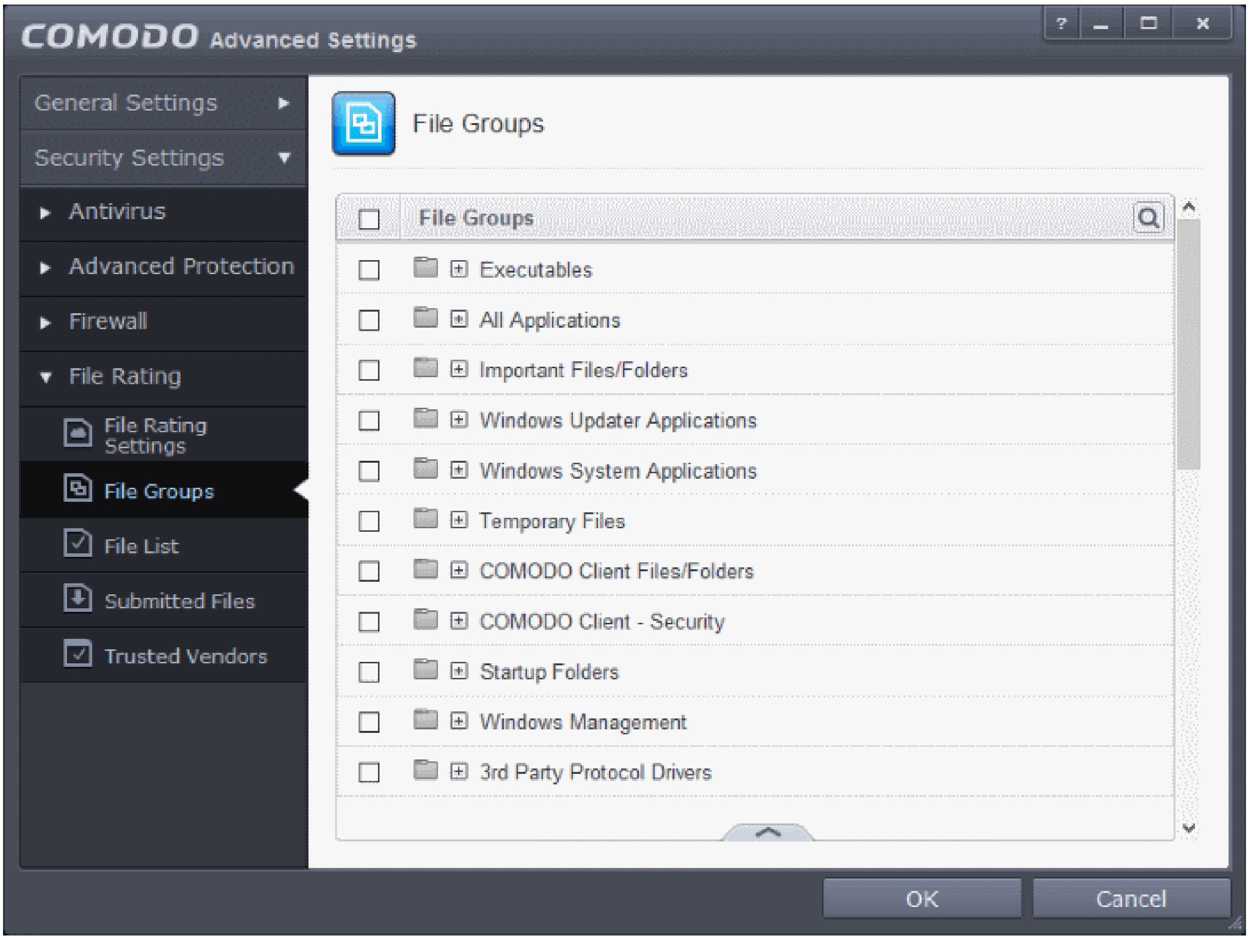
Refer to Scan Profiles for a guide that explains how to create a custom profile for unrecognized files.

- **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***)

6.2.4.2. File Groups

File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various CCS functions such as adding them to Exclusions, HIPS Rules, Auto-Containment and so on. CCS ships with a set of predefined File Groups and if required users can add new File Groups, edit and manage all the groups.

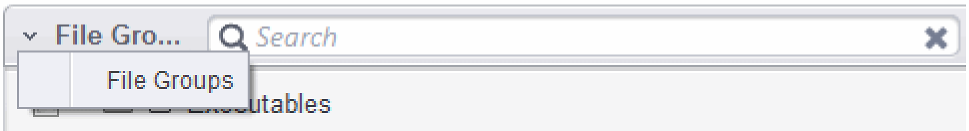
- The 'File Groups' panel can be accessed by clicking Security Settings > File Rating > File Groups from the Advanced Tasks interface.



□	File Groups
□	Executables
□	All Applications
□	Important Files/Folders
□	Windows Updater Applications
□	Windows System Applications
□	Temporary Files
□	COMODO Client Files/Folders
□	COMODO Client - Security
□	Startup Folders
□	Windows Management
□	3rd Party Protocol Drivers

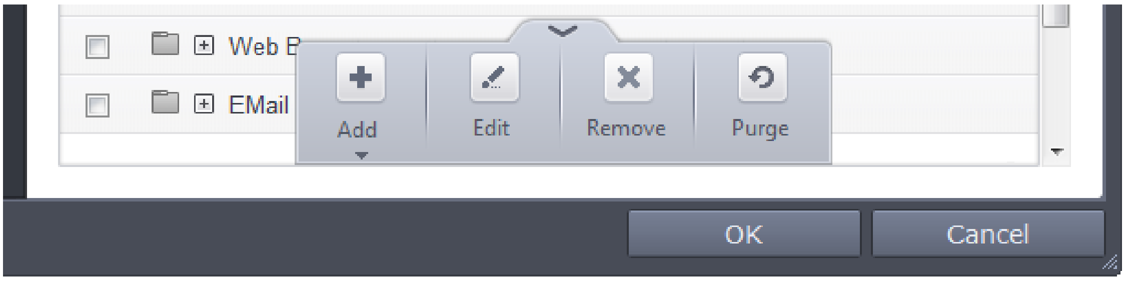
You can use the search option to find a specific name in the list.

To use the search option, click the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Clicking the handle at the bottom of the interface opens an options panel:



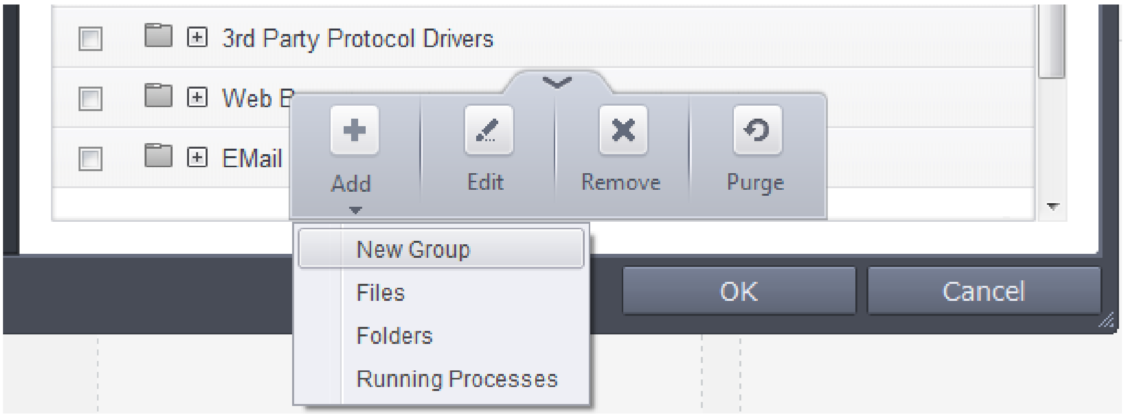
- **Add** – Allows you to add new groups, add individual files ,folders or running process to File Groups.
- **Edit** – Allows you to edit the name of file groups and edit file path of items under a file group.
- **Remove** – Allows you to delete a File Group or item(s) under a file group.
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

This interface allows you to

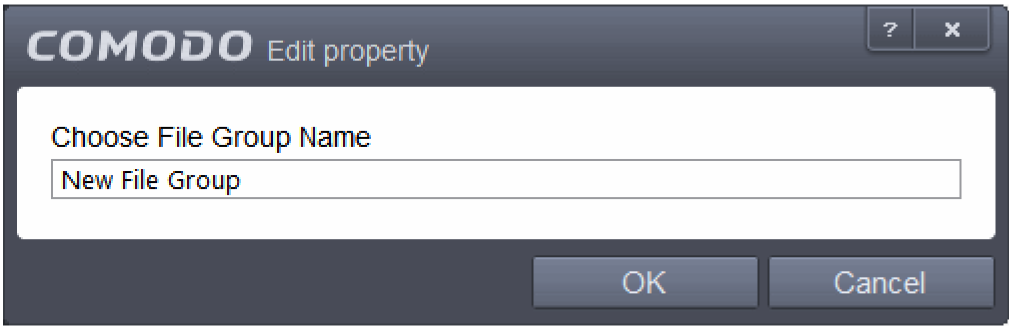
- Create a new File Group
- Edit the names of an Existing File Group
- Add a file to an existing file group
- Remove existing file group(s) or individual file(s) from existing group

Adding a File Group

- To add a new File group or add files to an existing group, click the handle from the bottom and click 'Add'.



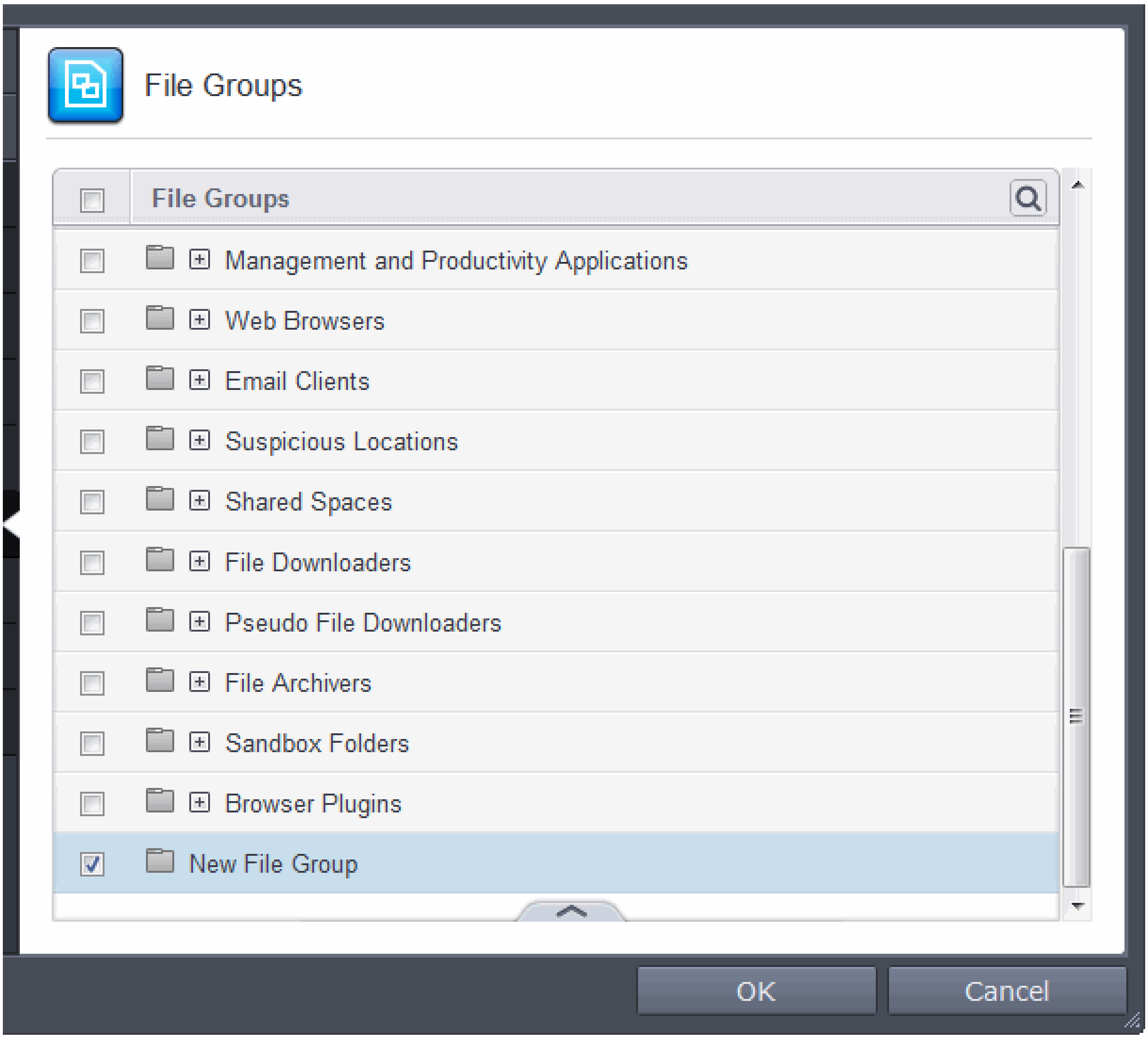
- Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'



Choose File Group Name

New File Group

The 'File Group' will be added and displayed in the list.

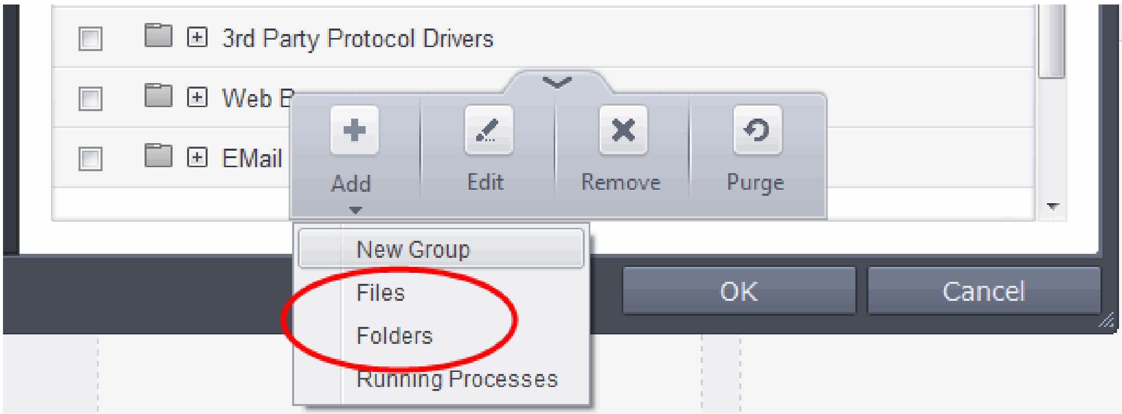


- □ File Groups
- □ Management and Productivity Applications
- □ Web Browsers
- □ Email Clients
- □ Suspicious Locations
- □ Shared Spaces
- □ File Downloaders
- □ Pseudo File Downloaders
- □ File Archivers
- □ Sandbox Folders
- □ Browser Plugins
- ☑ New File Group

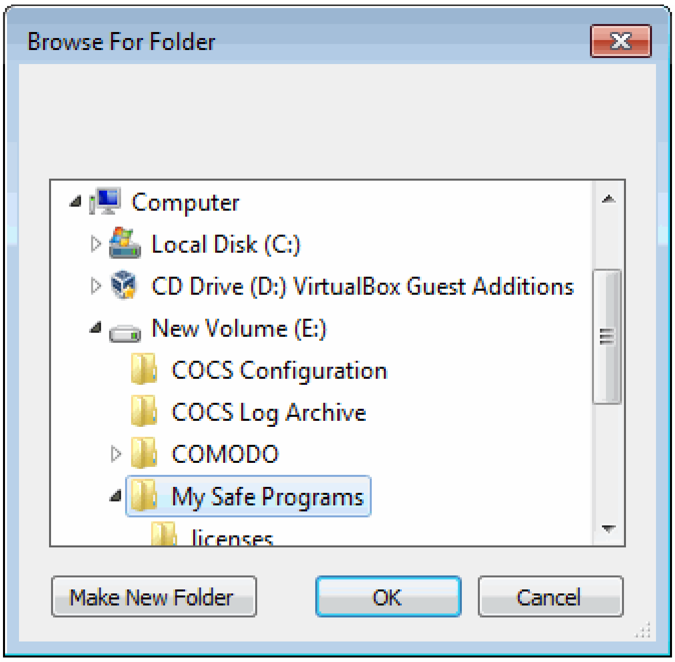
- To edit the name of an existing group, select the group, click the handle and choose 'Edit'. Edit the name of the group in the 'Edit Property' dialog.

Add individual files or folder to a group

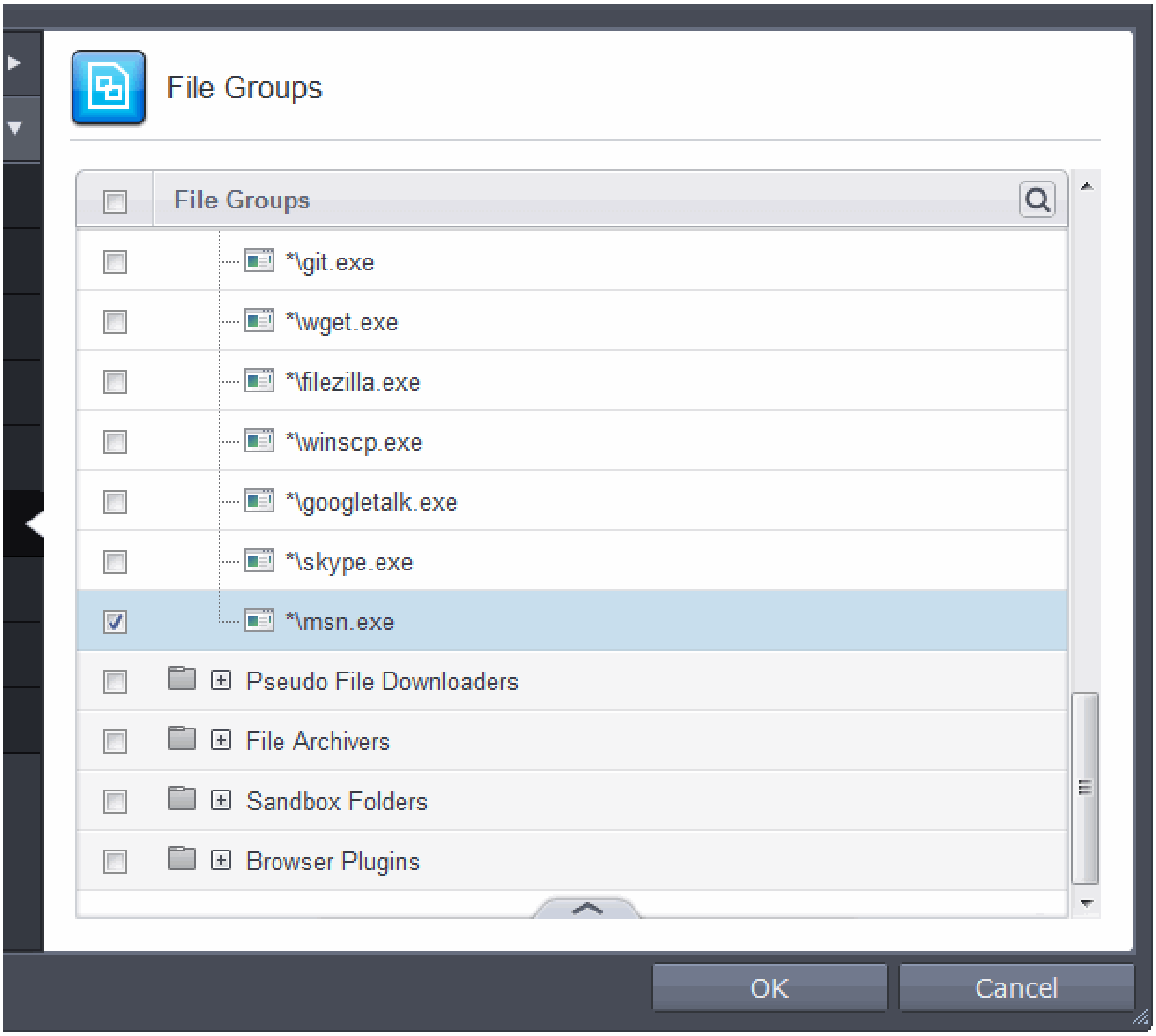
- Select the Group, click the handle and click 'Add'. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes.
  - To add a file or folder, choose 'Files' or 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will open.



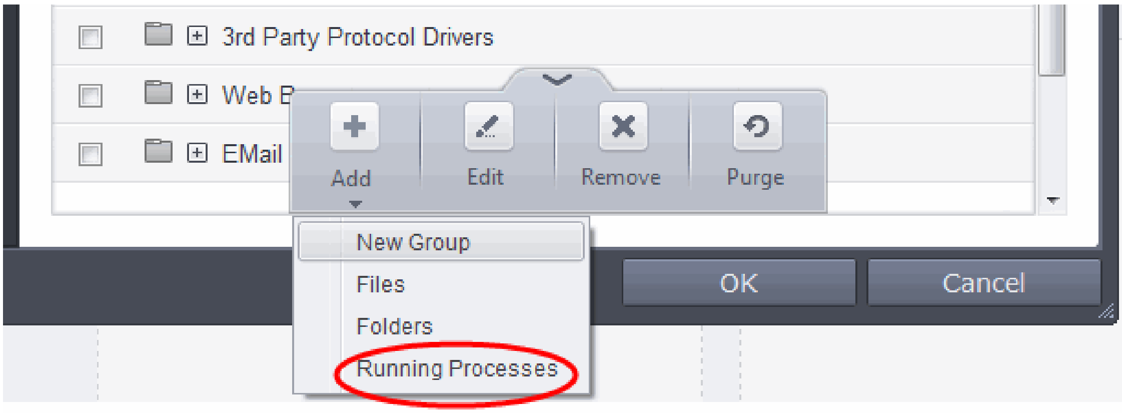
- Navigate to the individual file or folder you want to add to 'Files Groups' and click 'OK'



The drive file/folder will be added to 'File Groups'. Repeat the process to add more individual files or folders.

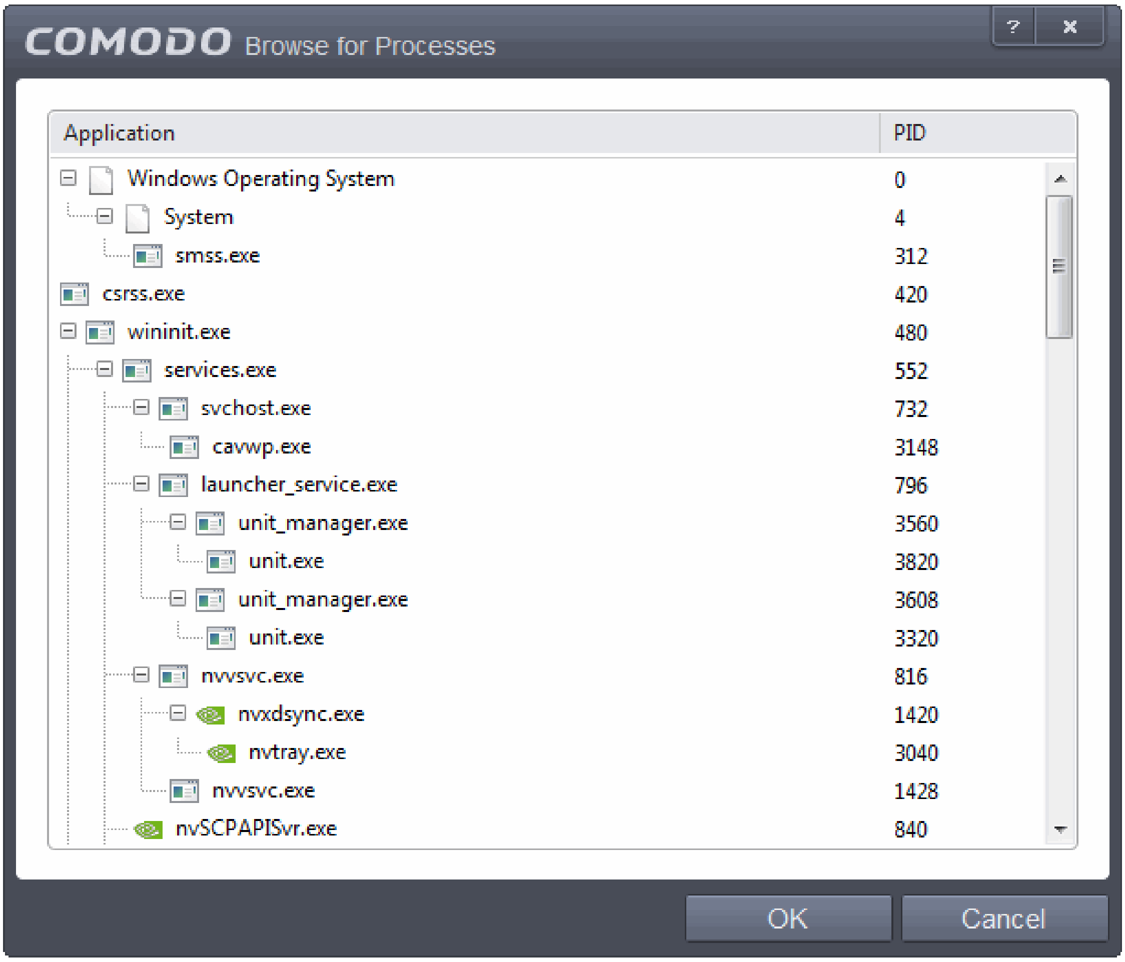
Add an application from a running processes

- 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 is to be added to Files Groups and click 'OK' from the Browse for Process dialog.

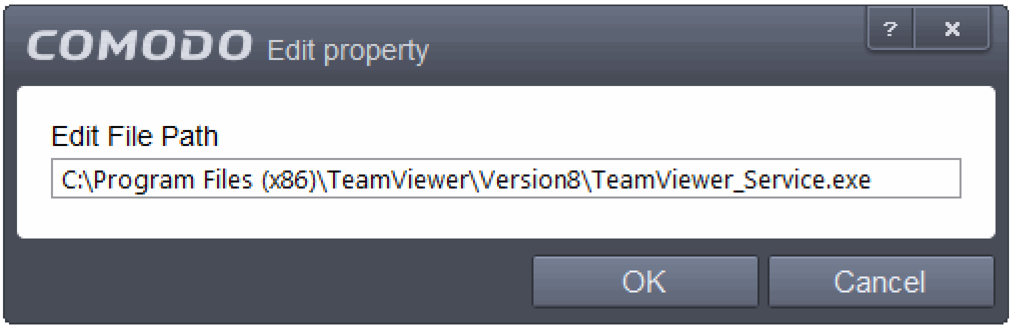


Application	PID
Windows Operating System	0
System	4
smss.exe	312
csrss.exe	420
wininit.exe	480
services.exe	552
svchost.exe	732
cavwp.exe	3148
launcher_service.exe	796
unit_manager.exe	3560
unit.exe	3820
unit_manager.exe	3608
unit.exe	3320
nvvsvc.exe	816
nvxdsync.exe	1420
nvtray.exe	3040
nvvsvc.exe	1428
nvSCPAPISvr.exe	840

The application will be added to File Groups.

To edit an item in the Files Groups list

- Select the item from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



Edit File Path

C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe

- Edit the file path, if you have relocated the file and click 'OK'

To delete existing file group(s) individual file(s) from existing group

- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the file to be removed, click the handle and choose 'Remove'.

6.2.4.3. File List

The 'File List' pane displays a list of executable files and applications discovered on your system along with their file rating. CCS file ratings include:

- Trusted
- Unrecognized
- Malicious

Trusted Files

Files with 'Trusted' rating are considered safe to run outside the container. Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - 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 is from a vendor included in the Trusted Software Vendors list;
    - The application is included in the extensive and constantly updated Comodo safelist.
- Administrator rating (Applicable only if your CCS installation is remotely managed by your CESM/ITSM administrator).
- User Rating – You can assign 'Trusted' rating to any file from the Files List interface. Refer to the description of changing the file rating under the section File Details for more details. Users may also trust a file from an antivirus or containment alert.

    Background note. For files that are trusted by the user, CCS generates a hash or a digest of the file using a pre-defined algorithm which it saves in its database. When accessing the file in future, a digest is created instantly and compared against the list of stored hashes. In this way, even if the file name is changed later, it will retain its Trusted status as the hash remains 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

CCS watches all file system activity on your computer. Every new executable file introduced to your computer is first scanned against the Comodo white and black lists. If they are not on either list they are neither known-safe nor known-bad) then they are awarded an 'Unrecognized' file rating. Any executables that are modified are also given the 'Unrecognized' status.

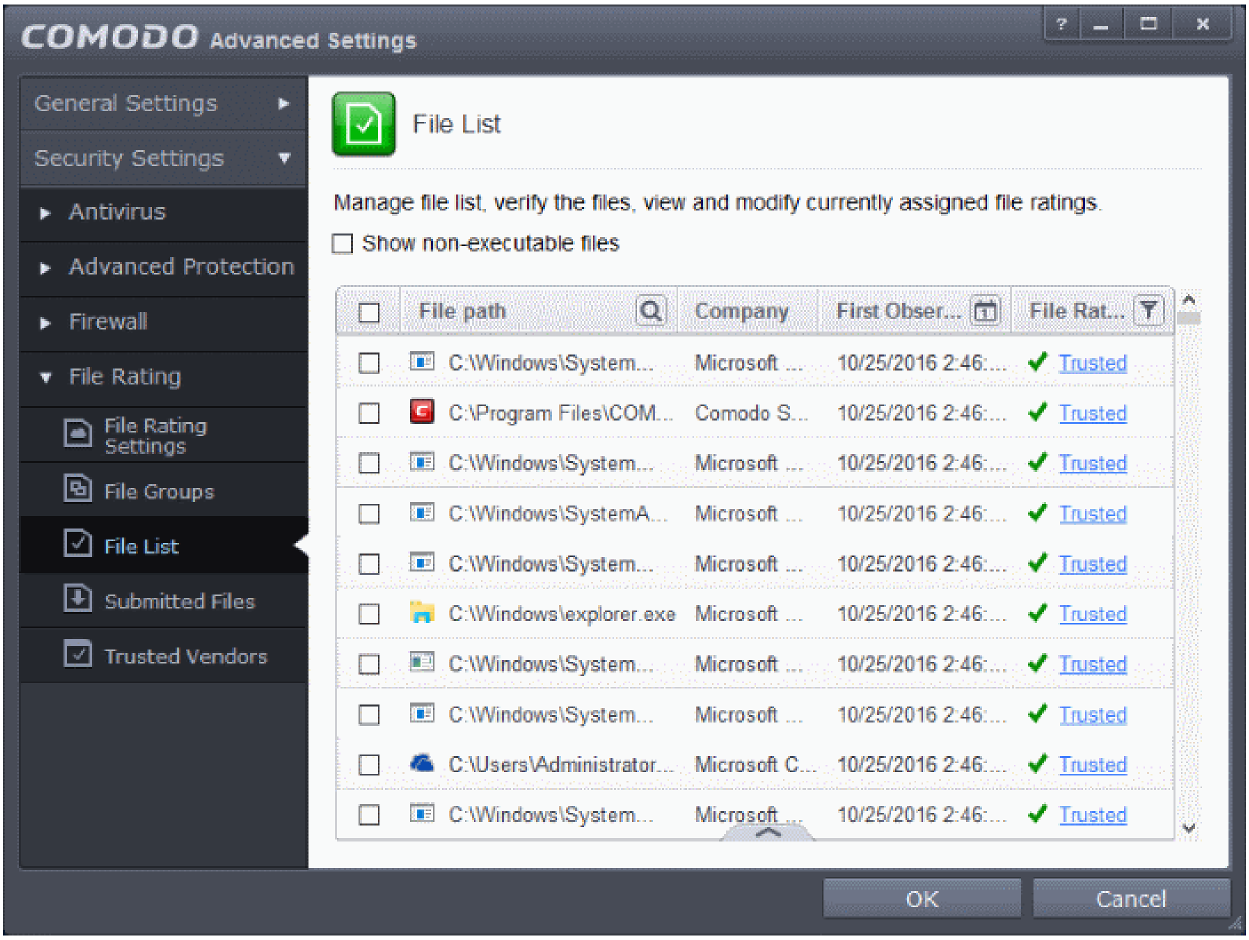
You can assess these unrecognized files to determine whether or not they are to be trusted. If they are trustworthy, they can be given the 'Trusted' rating. Refer to the description of changing the file rating for more details. You can also submit the files to Comodo for analysis. Experts at Comodo will analyze the files and add them to global white-list or black-list accordingly.

'Unrecognized Files' is specifically important while HIPS is in 'Clean PC Mode'. In Clean PC Mode, the files in 'Unrecognized Files' are NOT considered safe. For more information, please check 'Clean PC Mode' on the HIPS settings page.

Malicious Files

Files that are identified as malicious from the FLS will be given 'Malicious' rating and will not be allowed to run by default.

The Trusted Files panel can be accessed by clicking 'Security Settings' > 'File Rating' > 'File List' from the Advanced Settings interface.



File List

Manage file list, verify the files, view and modify currently assigned file ratings.

□ Show non-executable files

□	File path	Company	First Obser...	File Rat...
□	C:\Windows\System...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Program Files\COM...	Comodo S...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\System...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\SystemA...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\System...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\explorer.exe	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\System...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\System...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted
□	C:\Users\Administrator...	Microsoft C...	10/25/2016 2:46:...	✓ Trusted
□	C:\Windows\System...	Microsoft ...	10/25/2016 2:46:...	✓ Trusted

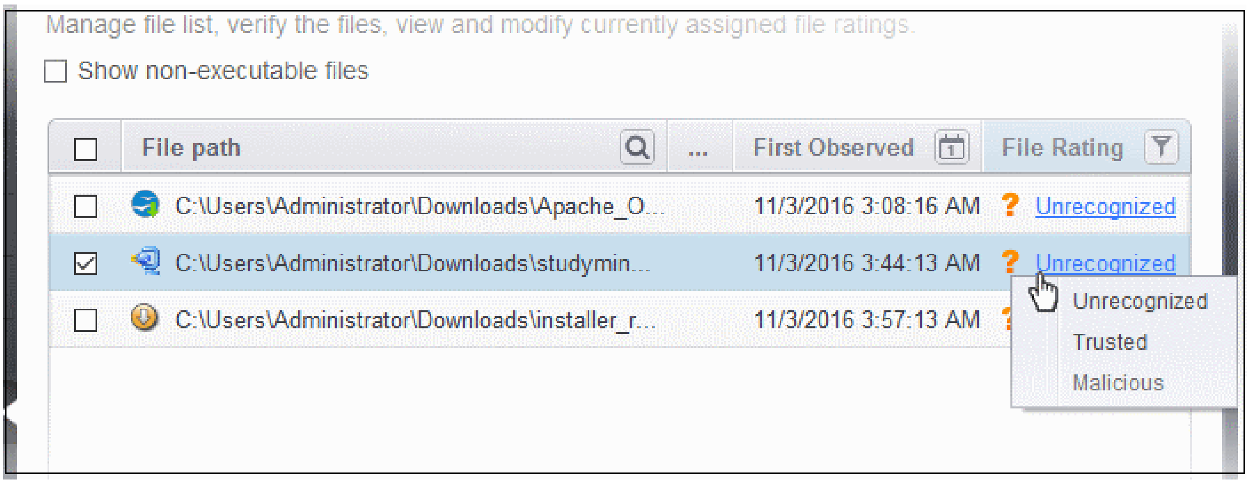
The pane displays the list of applications, programs and executable files discovered on your computer.

- **Show non-executable files** – If enabled, the list of files will also include non executable files. For example files with file extensions like .bat and so on.

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.
- **File Rating** - Indicates the current CCS rating of the file. The possible values are:
    - **Trusted**
    - **Unrecognized**
    - **Malicious**
    - The files are rated based on the following, in order of priority:

1. Administrator rating (Applicable only if your CCS installation is remotely managed by your CESM/ITSM administrator).
2. User rating (Rating as set by the user, if modified from the default rating)
3. FLS rating
    - The File rating can be modified by the user in two ways:
    - By clicking on the displayed rating in the row of the desired file and choosing the rating from the context sensitive menu.



Manage file list, verify the files, view and modify currently assigned file ratings.

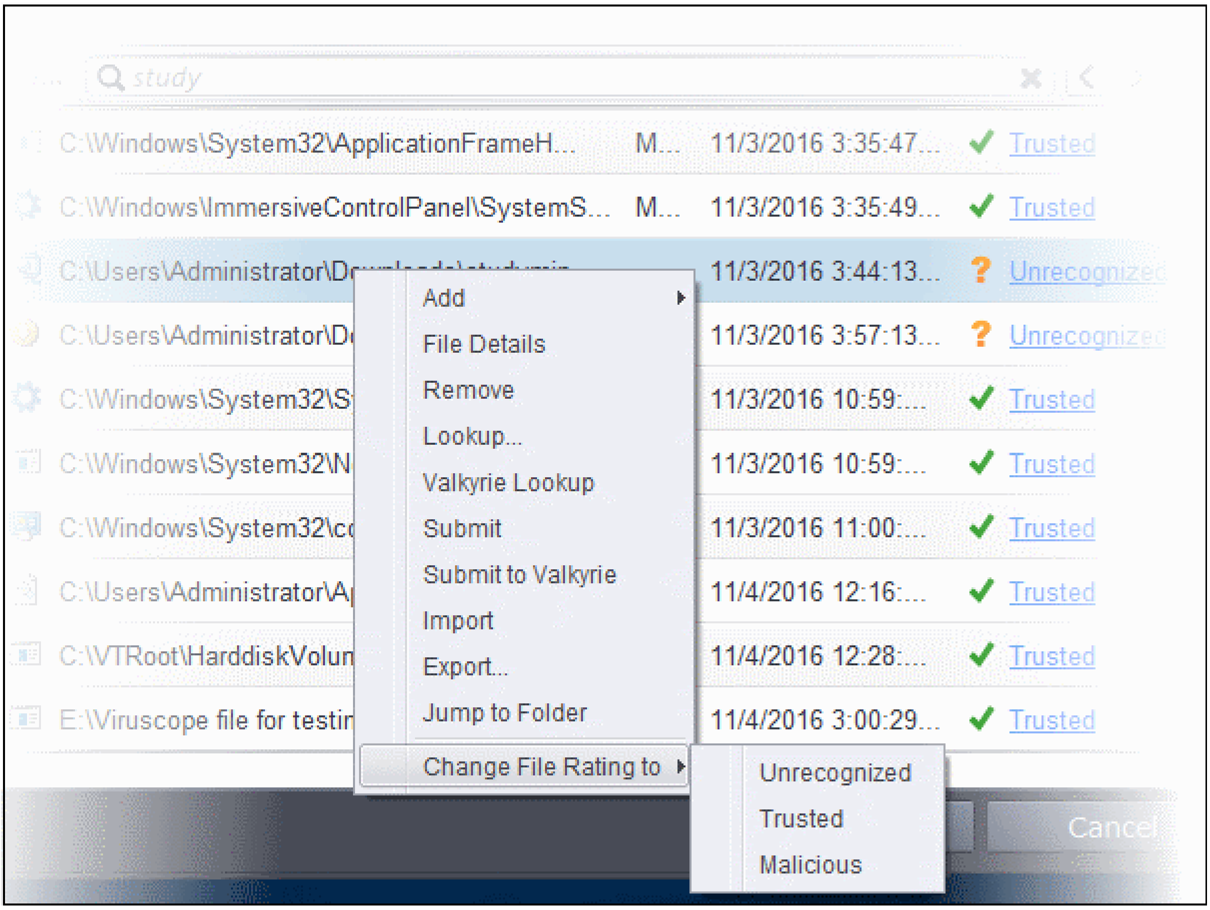
□ Show non-executable files

□	File path	...	First Observed	File Rating
□	C:\Users\Administrator\Downloads\Apache_O...		11/3/2016 3:08:16 AM	? Unrecognized
☑	C:\Users\Administrator\Downloads\studymin...		11/3/2016 3:44:13 AM	? Unrecognized
□	C:\Users\Administrator\Downloads\installer_r...		11/3/2016 3:57:13 AM	?

- From the 'File Details' dialog of the desired file by selecting it, clicking the handle from the bottom and choosing 'File Details' from the options. Refer to the description of changing the file rating under the section 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.



study

File path		First Observed	File Rating
C:\Windows\System32\ApplicationFrameH...	M...	11/3/2016 3:35:47...	✓ Trusted
C:\Windows\ImmersiveControlPanel\SystemS...	M...	11/3/2016 3:35:49...	✓ Trusted
C:\Users\Administrator\D...		11/3/2016 3:44:13...	? Unrecognized
C:\Users\Administrator\D...		11/3/2016 3:57:13...	? Unrecognized
C:\Windows\System32\S...		11/3/2016 10:59:...	✓ Trusted
C:\Windows\System32\N...		11/3/2016 10:59:...	✓ Trusted
C:\Windows\System32\c...		11/3/2016 11:00:...	✓ Trusted
C:\Users\Administrator\A...		11/4/2016 12:16:...	✓ Trusted
C:\VTRoot\HarddiskVolun...		11/4/2016 12:28:...	✓ Trusted
E:\Viruscope file for testin...		11/4/2016 3:00:29...	✓ Trusted

- Add - Allows you to manually add files to the 'File List' with user defined rating
- File Details - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- Remove - Allows you to remove files from 'File List'.
- Lookup - Starts the online lookup of selected file with the master Comodo FLS safelist if any details are

available.

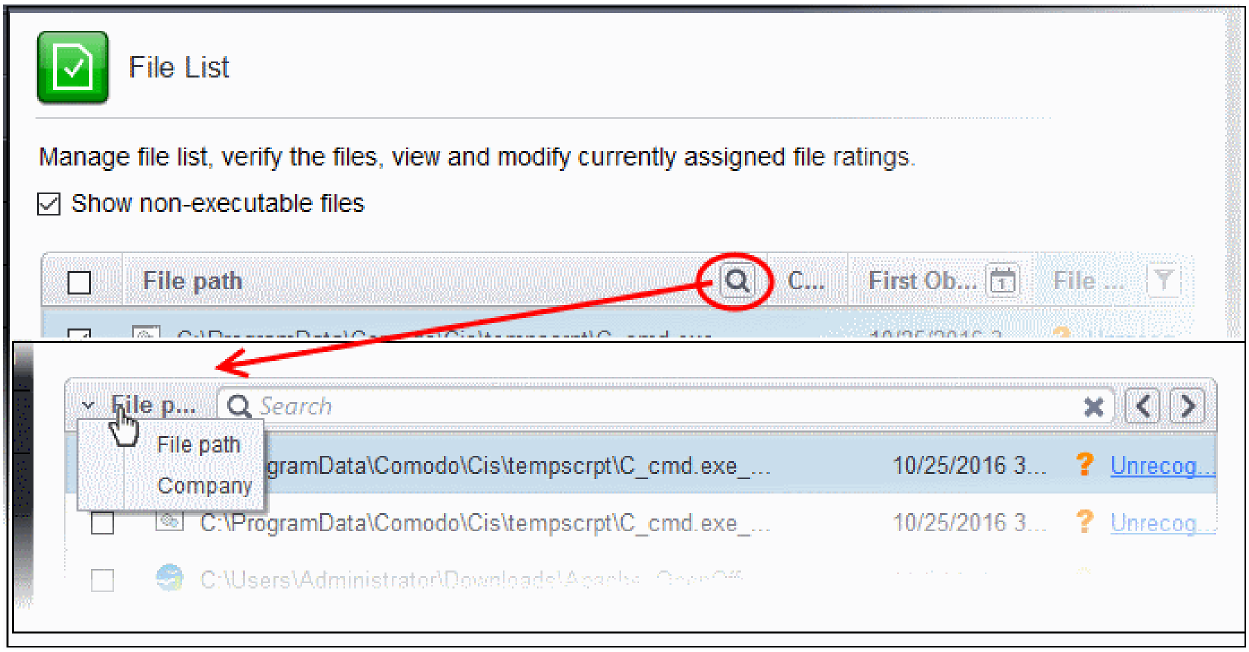
- Valkyrie Lookup – Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. The results of these file tests are stored on the Valkyrie servers to improve the effectiveness of the service for all CCS users. Clicking Valkyrie Lookup will search the file rating of the selected file from the Valkyrie analysis results.
- Submit - Begins the file submission process to CAMAS.
- Submit to Valkyrie – Begins the file submission process to Valkyrie analysis.
- Import - Enables you import a file list from an XML file
- Export - Enables you export the current file list with existing ratings to an XML file
- **Jump to Folder** – Opens the folder containing the file in Windows Explorer.
- Change File Rating to – Enables you to change the file rating to: Trusted, Unrecognized, Malicious

Searching and Filtering options

You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and File rating.

To use the search option, click the search icon 🔍 at the far right in the 'File path' column header.

- Click the chevron on the left side of the column header and select the search criteria from the drop-down.



File List

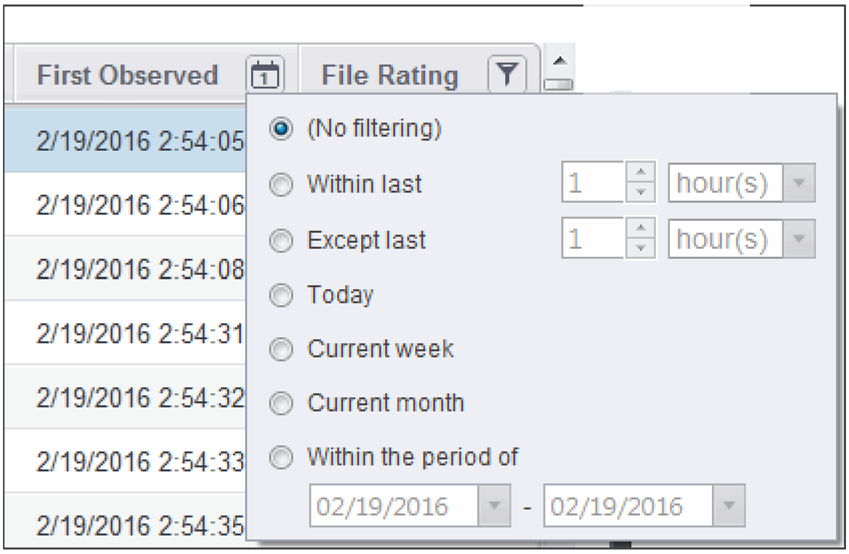
Manage file list, verify the files, view and modify currently assigned file ratings.

☑ Show non-executable files

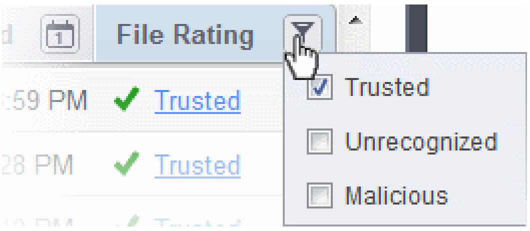
□	File path	C...	First Ob...	File ...
□	C:\ProgramData\Comodo\Cis\tempscrpt\C_cmd.exe_...		10/25/2016 3...	? Unrecog...
□	C:\ProgramData\Comodo\Cis\tempscrpt\C_cmd.exe_...		10/25/2016 3...	? Unrecog...
□	C:\Users\Administrator\Downloads\Acrobat_OpenOff...			

  - Enter the file path or the name of company in part or full as per the selected criteria in the search field and press 'Enter' to begin the search.

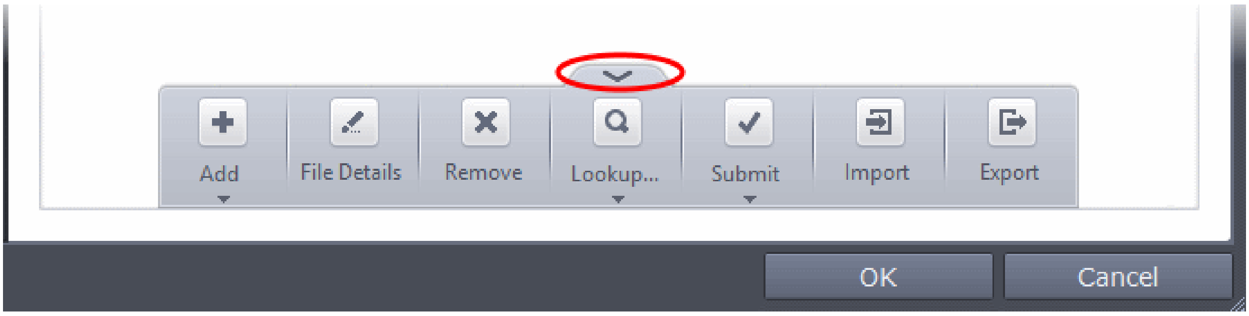
- To filter the list based on the date of installation or storage of the files, click the calendar icon at the right of the 'First Observed' column header and choose the time/date/period.



- 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 ratings to display only the files with the selected rating(s).



Clicking the handle at the bottom of the panel opens the following options:



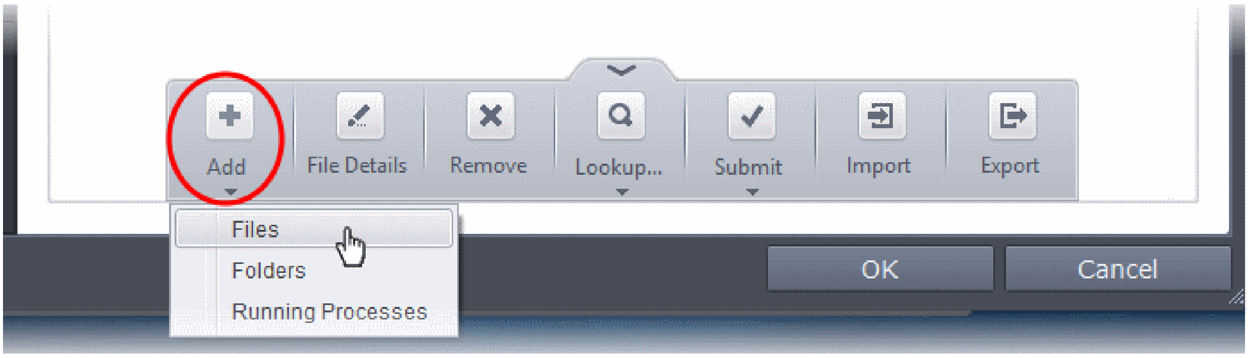
- **Add** - Allows you to manually add files, folders and running processes to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- Lookup... - Allows to you lookup of selected file with Comodo FLS safelist and Valkyrie analysis results.
  - **Lookup...** - Starts the online lookup of selected file with the master Comodo FLS safelist if any details are available
  - **Valkyrie Lookup** – Starts the Valkyrie lookup of the selected file from the Valkyrie analysis results.
- **Submit**
  - **Submit** - Begins the file submission process to Comodo file analysis engines.

- **Submit to Valkyrie** - Begins the file submission process to Valkyrie analysis.

- **Import** - Enables you import a file list from an XML file
- **Export** - Enables you export the current file list with existing ratings to an XML file

To manually add files to 'File list'

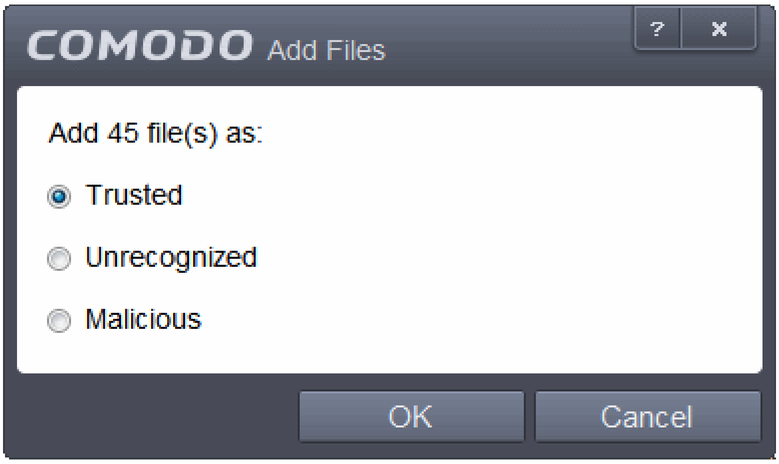
- Click the handle from the bottom and choose 'Add'



Tip: Alternatively, right click inside the File List page and choose 'Add' from the context sensitive menu.

- You can add files to the File list by three ways:
  - **Files** - Allows you to navigate to the file or executable of the program you wish to add and assign a rating.
  - **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'File List' with the rating you assign.
  - **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'File List' with the rating you assign.

Once you have chosen the file(s) or the folder, you can assign the rating for the file(s) to be added.



Add 45 file(s) as:

● Trusted

○ Unrecognized

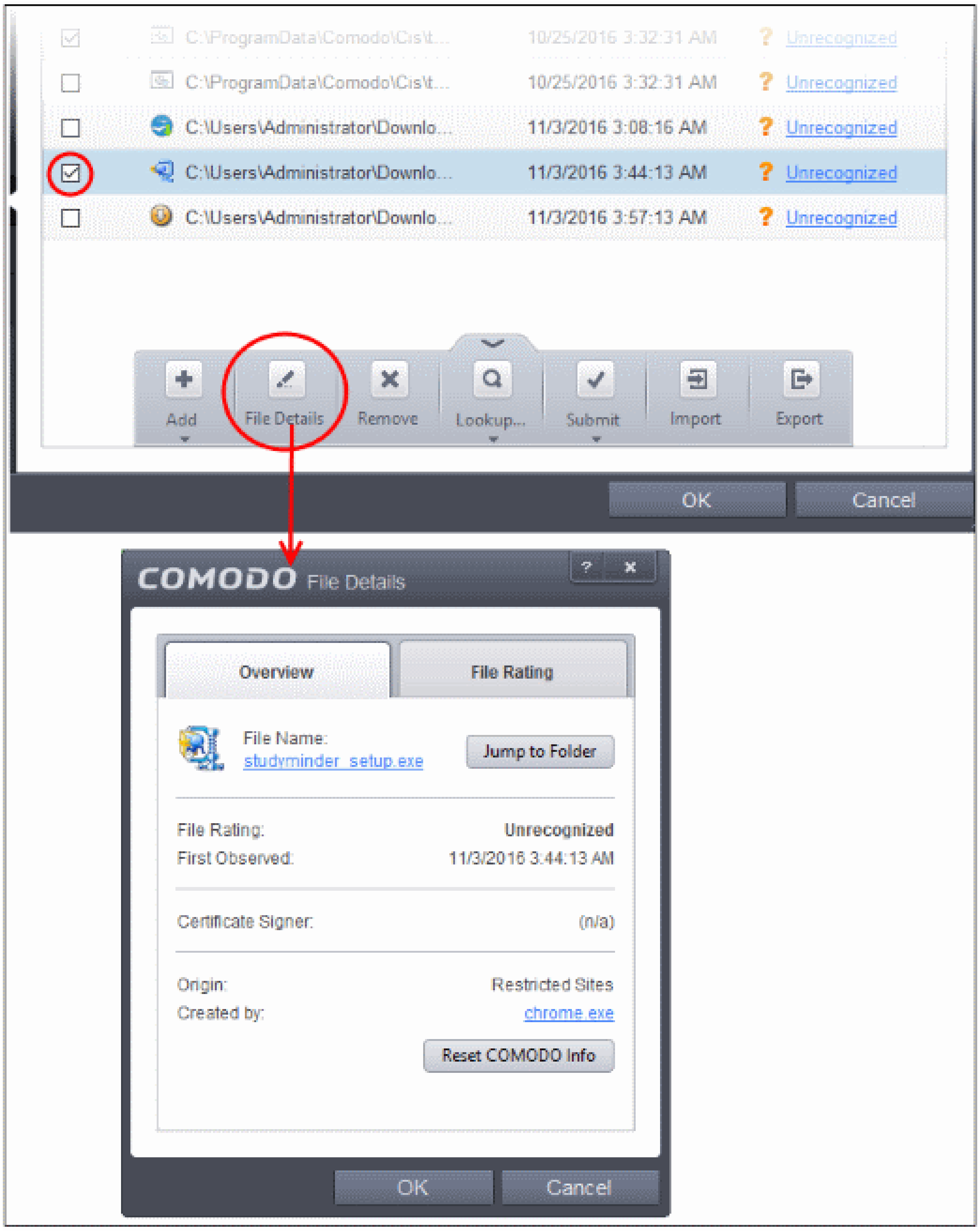
○ Malicious

- Choose the rating to be assigned to the file(s). The available options are:
  - Trusted – The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
  - Unrecognized – The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
  - Malicious – The file will not be allowed to run.

  - Click 'OK' in the 'Add Files' dialog
- Click 'OK' in the 'Advanced Settings' for your changes to take effect.

To view the 'File Details' and change the rating

- Choose the file to view its details
- Click the handle from the bottom and choose 'File Details'



☑	C:\ProgramData\Comodo\Cis\t...	10/25/2016 3:32:31 AM	? Unrecognized
□	C:\ProgramData\Comodo\Cis\t...	10/25/2016 3:32:31 AM	? Unrecognized
□	C:\Users\Administrator\Downlo...	11/3/2016 3:08:16 AM	? Unrecognized
☑	C:\Users\Administrator\Downlo...	11/3/2016 3:44:13 AM	? Unrecognized
□	C:\Users\Administrator\Downlo...	11/3/2016 3:57:13 AM	? Unrecognized

File Name: studyminder_setup.exe

File Rating: Unrecognized

First Observed: 11/3/2016 3:44:13 AM

Certificate Signer: (n/a)

Origin: Restricted Sites

Created by: chrome.exe

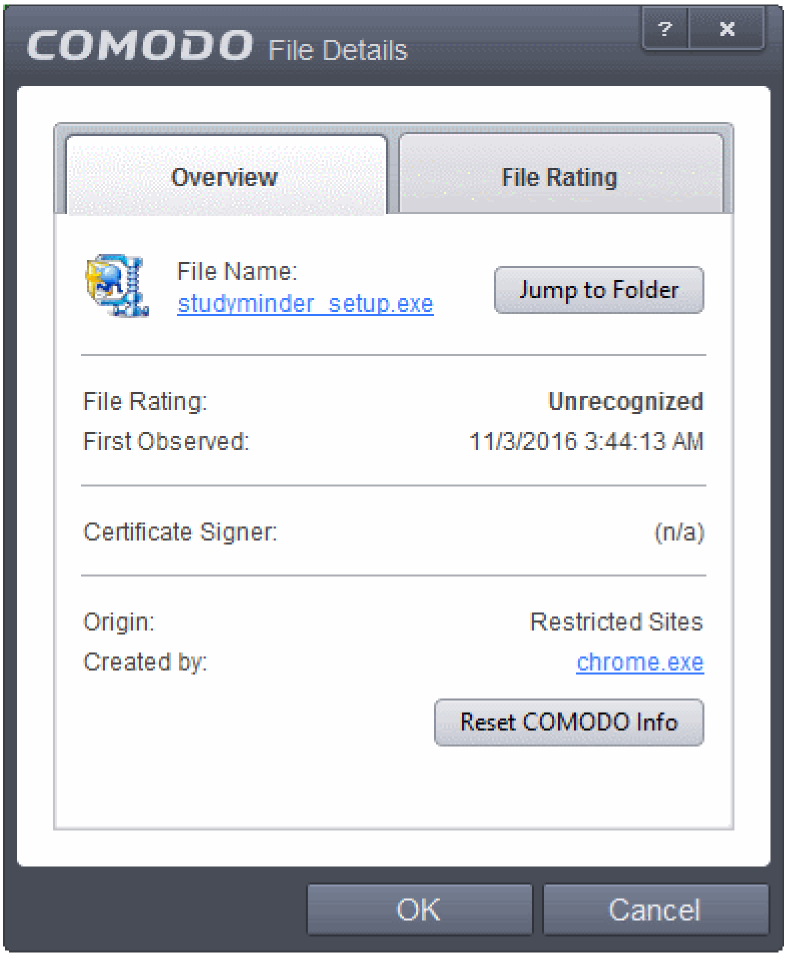
Tip: Alternatively, right click on the selected file inside the File List page and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog contains two tabs:

- Overview
- File Rating

Overview

The Overview tab displays the general details of the file and the publisher details.



File Name: studyminder_setup.exe

File Rating: Unrecognized

First Observed: 11/3/2016 3:44:13 AM

Certificate Signer: (n/a)

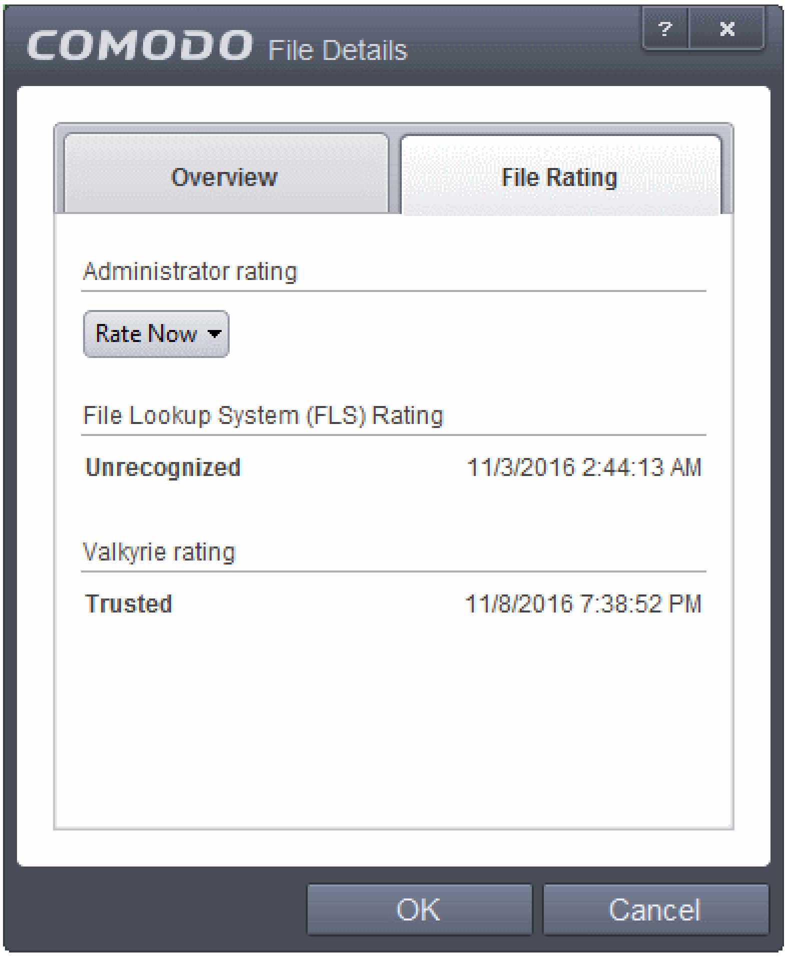
Origin: Restricted Sites

Created by: chrome.exe

- 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 servers and Valkyrie (if submitted to Valkyrie).


COMODO File Details

Overview | File Rating

Administrator rating

Rate Now

File Lookup System (FLS) Rating

Unrecognized 11/3/2016 2:44:13 AM

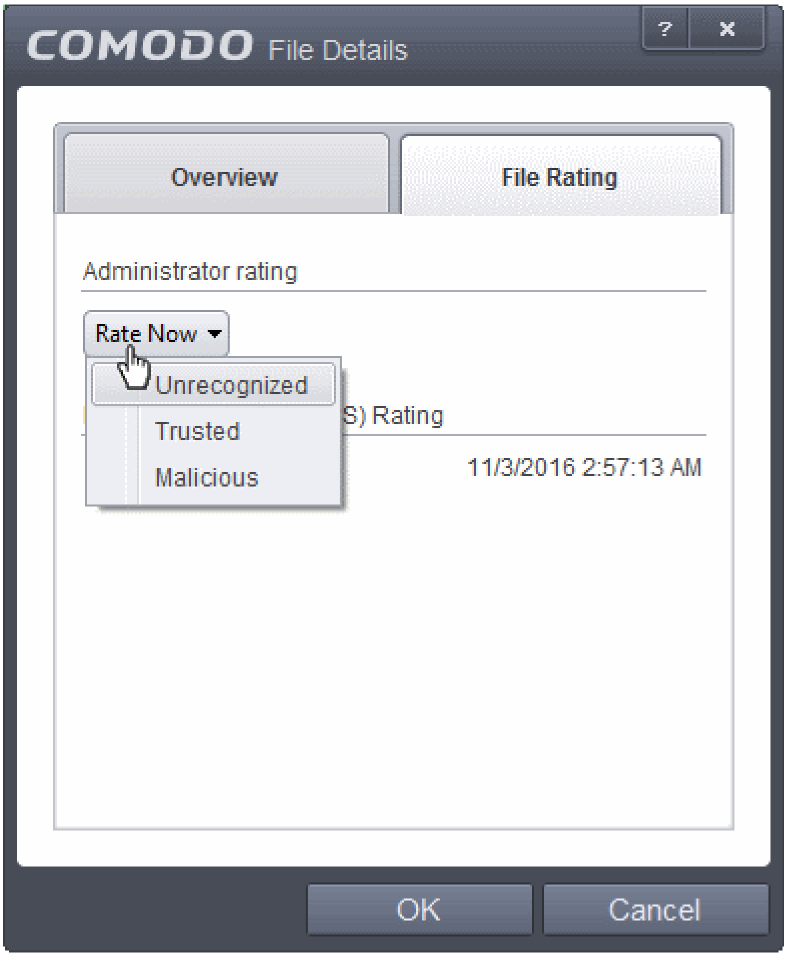
Valkyrie rating

Trusted 11/8/2016 7:38:52 PM

Note: If the CCS installation is remotely managed by the CESM/ITSM 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, click the handle from the bottom and choose File Rating from the options
- Click the File Rating tab from the File Details tab
- Click 'Rate Now' and choose the rating from the drop-down



The options available are:

- Trusted – The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- Unrecognized – The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- Malicious – The file will not be allowed to run.

- Click 'OK' in the 'Files Details' dialog

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

To remove files(s) from the File list

- Select the file(s) to be removed from the 'File List' pane. You can select several entries to be removed at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Remove'. The file is only removed from the list and not deleted from your system.

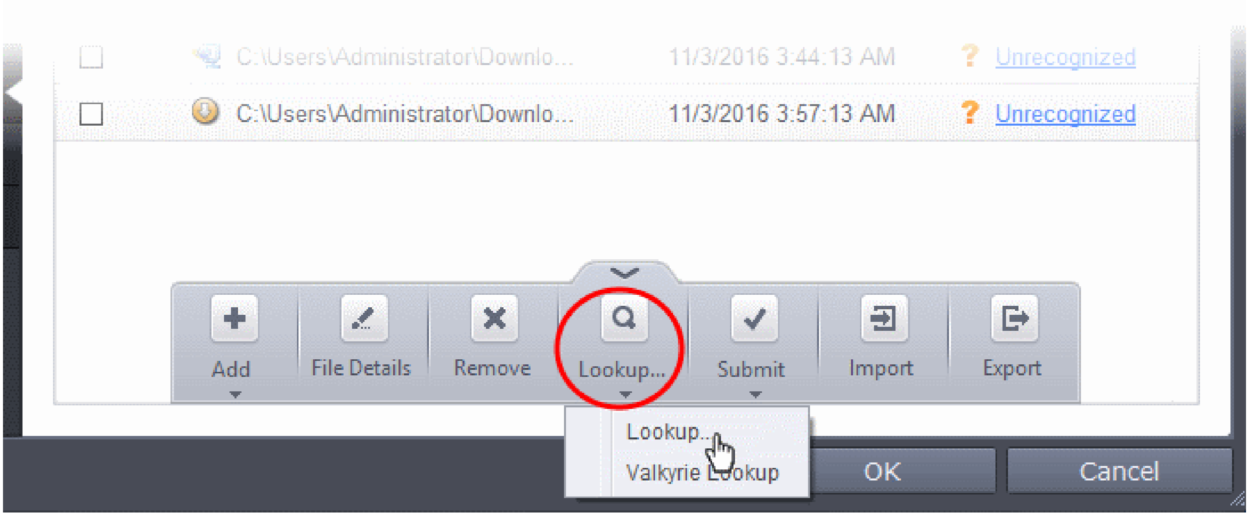
Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Remove' from the context sensitive menu.

- Click 'OK' for your changes to take effect.

To perform Comodo FLS lookup for files

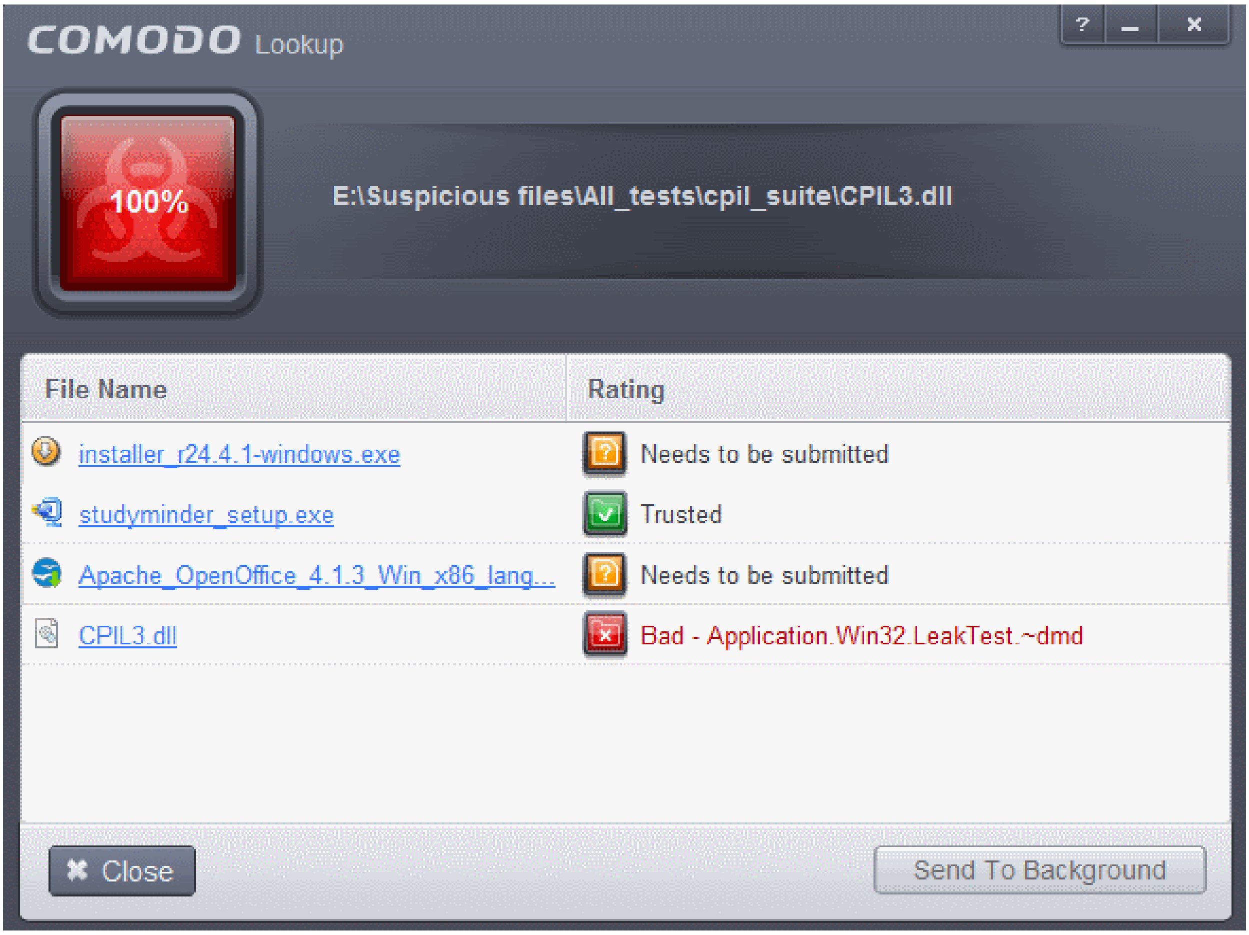
- Select the files to be checked from the 'File list' pane. You can select several entries at once by marking the check-boxes beside the entries.

- Click the handle from the bottom and click 'Lookup...' then 'Lookup...' from the options.


C:\Users\Administrator\Downlo... 11/3/2016 3:44:13 AM ? Unrecognized
C:\Users\Administrator\Downlo... 11/3/2016 3:57:13 AM ? Unrecognized
Add
File Details
Remove
Lookup...
Submit
Import
Export
Lookup...
Valkyrie Lookup
OK
Cancel

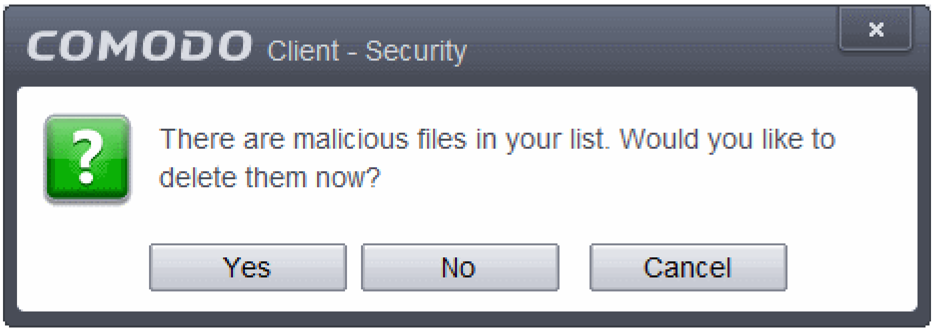
Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Lookup' from the context sensitive menu.

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.



File Name	Rating
installer_r24.4.1-windows.exe	Needs to be submitted
studyminder_setup.exe	Trusted
Apache_OpenOffice_4.1.3_Win_x86_lang...	Needs to be submitted
CPIL3.dll	Bad - Application.Win32.LeakTest.~dmd

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.

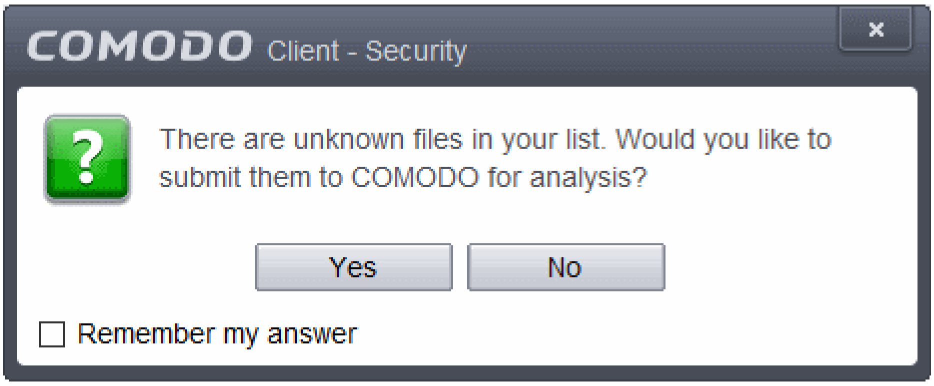


COMODO Client - Security

There are malicious files in your list. Would you like to delete them now?

- Click 'Yes' to permanently delete the malicious file(s) from your computer.

- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. Refer to 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. Refer to the explanation below for more details.



COMODO Client - Security

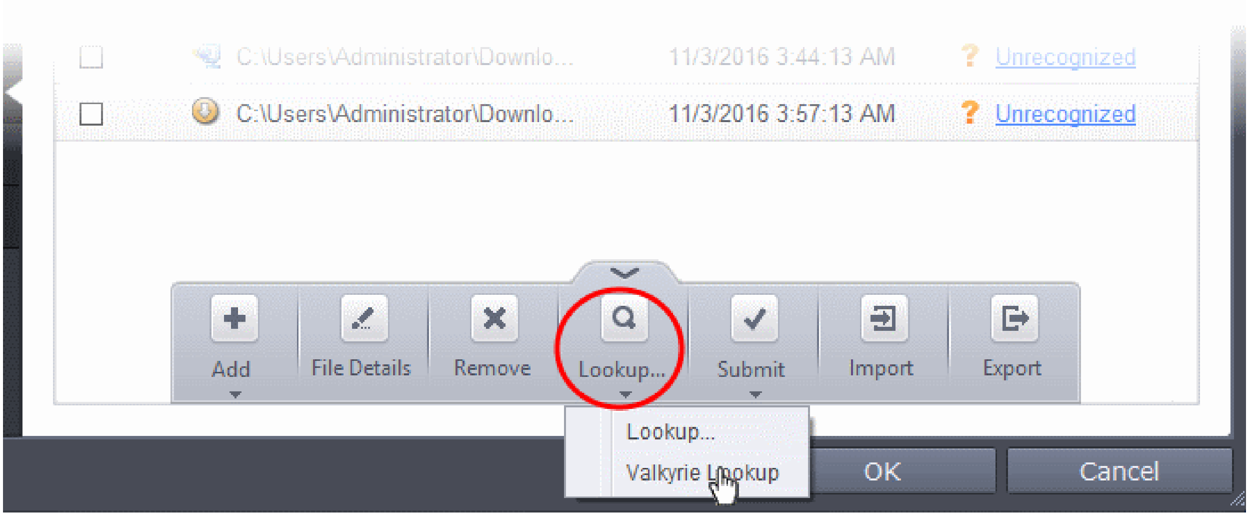
There are unknown files in your list. Would you like to submit them to COMODO for analysis?

□ Remember my answer

To perform Valkyrie lookup of files

Valkyrie is a cloud-based file analysis service that tests unknown files with a range of static and behavioral checks in order to identify those that are malicious. The Valkyrie results are stored in Comodo Valkyrie servers for references.

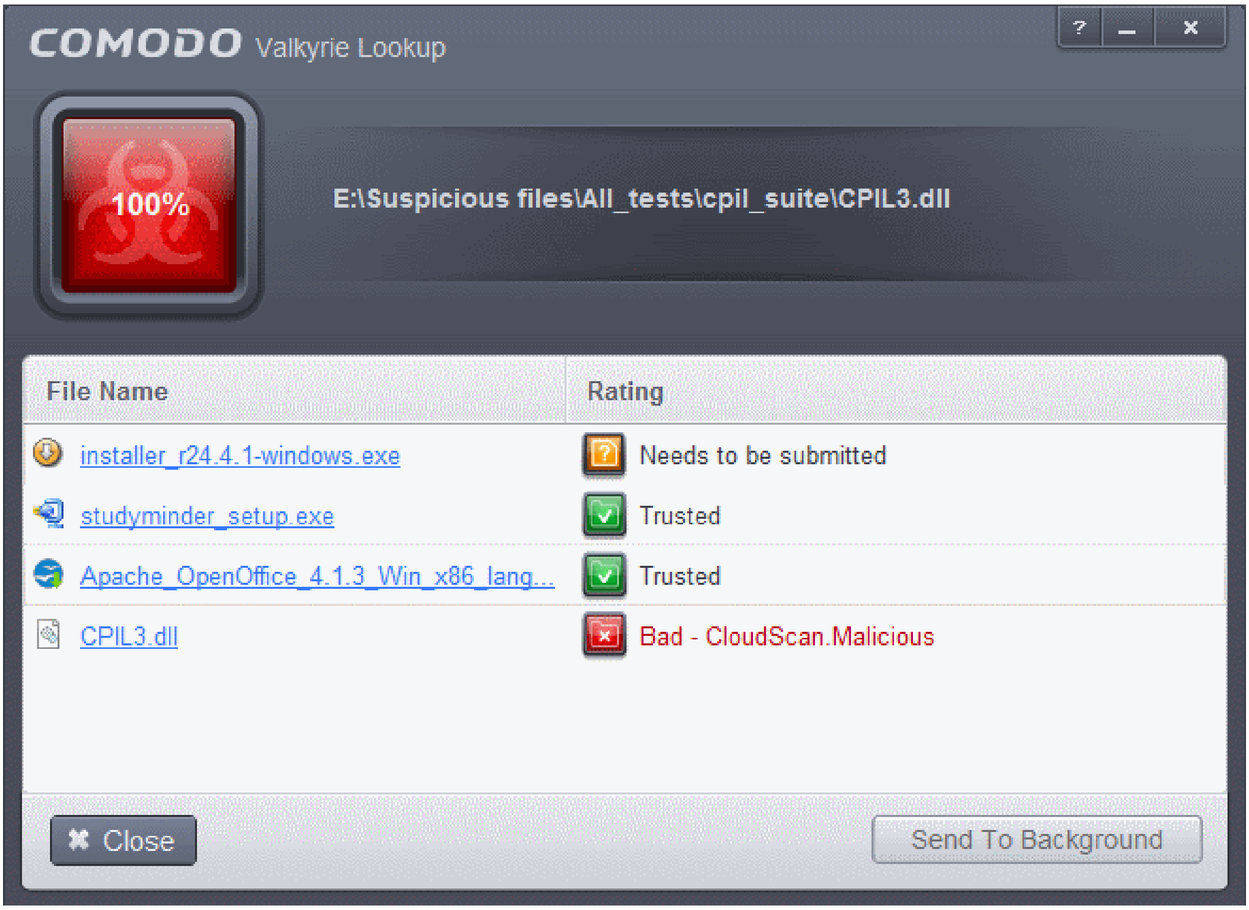
- Select the files to be checked from the 'File list' pane. You can select several entries at once by marking the check-boxes beside the entries.
- Click the handle from the bottom and click 'Lookup...' then 'Valkyrie Lookup' from the options.



□	C:\Users\Administrator\Downlo...	11/3/2016 3:44:13 AM	? Unrecognized
□	C:\Users\Administrator\Downlo...	11/3/2016 3:57:13 AM	? Unrecognized

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Valkyrie Lookup' from the context sensitive menu.

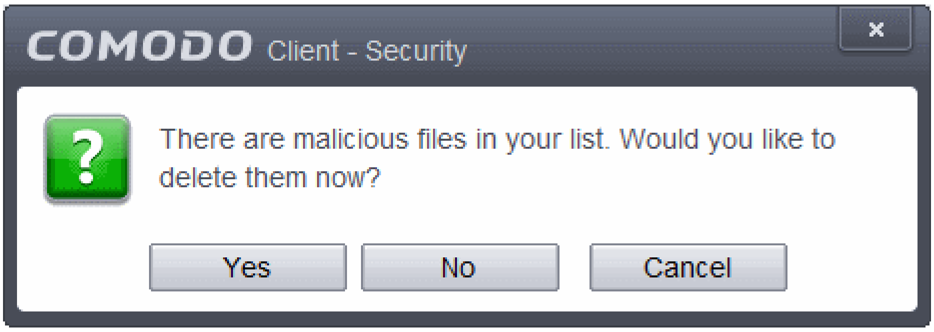
Comodo Valkyrie servers will be contacted immediately to conduct a search in the database to check if any information is available about the files in question and the results will be displayed.



E:\Suspicious files\All_tests\cpil_suite\CPIL3.dll

File Name	Rating
installer_r24.4.1-windows.exe	Needs to be submitted
studyminder_setup.exe	Trusted
Apache_OpenOffice_4.1.3_Win_x86_lang...	Trusted
CPIL3.dll	Bad - CloudScan.Malicious

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.

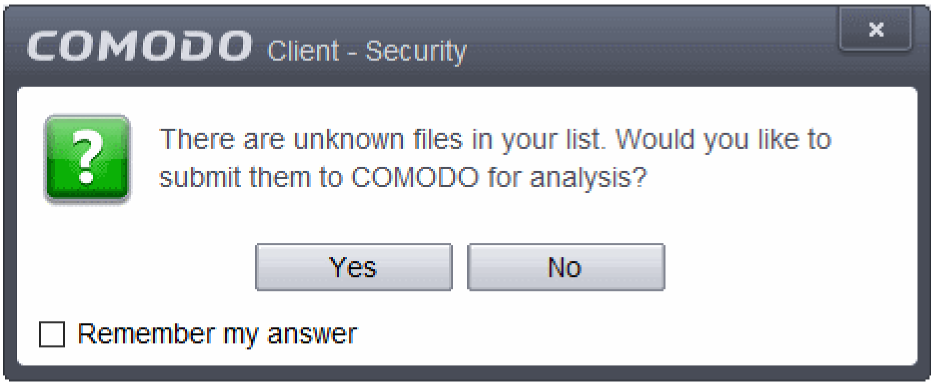


COMODO Client - Security

There are malicious files in your list. Would you like to delete them now?

- Click 'Yes' to permanently delete the malicious file(s) from your computer.

- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. Refer to 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 'Unknown' with a yellow icon. You can submit the file to Comodo Valkyrie for analysis from the dialog that appears on closing the 'Lookup' dialog. Refer to the **explanation below** for more details.



COMODO Client - Security

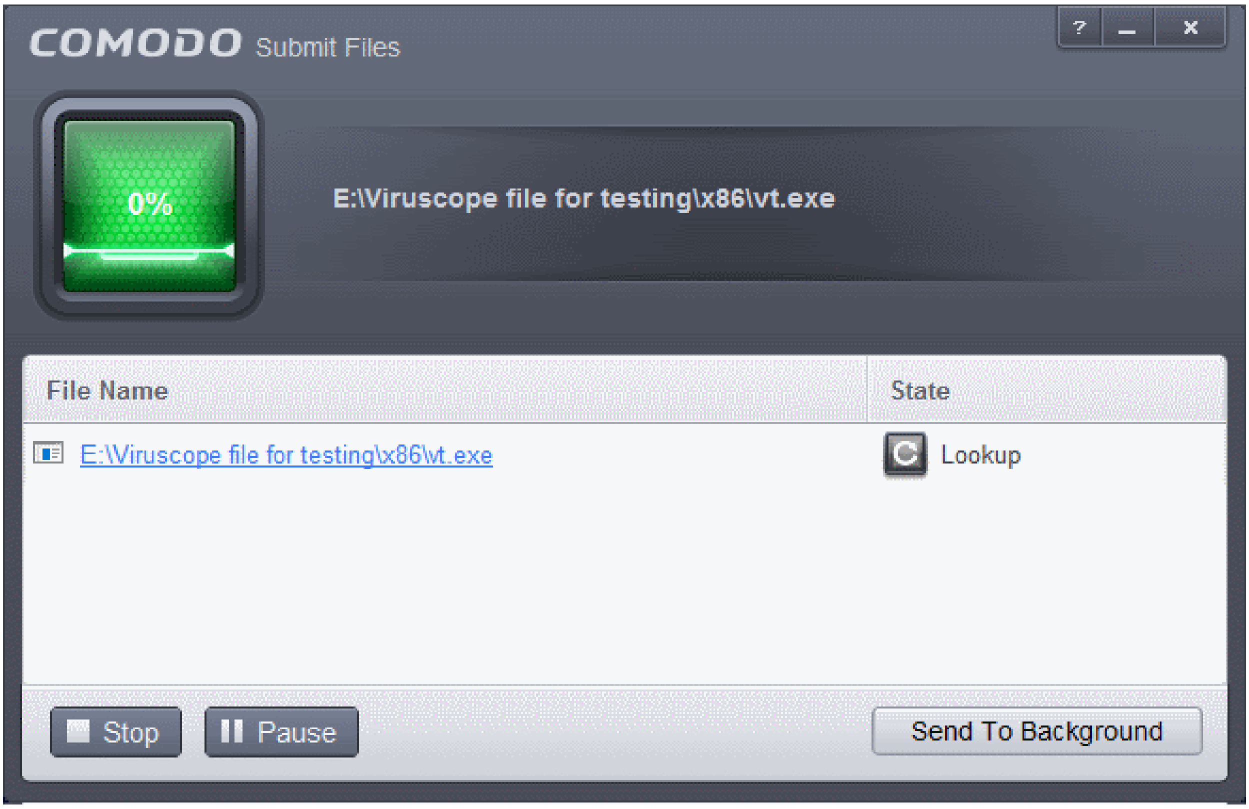
There are unknown files in your list. Would you like to submit them to COMODO for analysis?

□ Remember my answer

To manually submit files to CAMAS

- Select the file(s) to be submitted from the 'File List' pane. You can select several entries to be sent at once by marking the check-boxes beside the entries.
- Click the handle from the bottom and click 'Submit', then 'Submit' from the options. The file(s) will be immediately sent to Comodo Automated Malware Analysis System .

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Submit' from the context sensitive menu or click 'Yes' in the submit unknown files dialog from the '**Lookup...**' feature.



E:\Viruscope file for testing\x86\vt.exe

File Name	State
E:\Viruscope file for testing\x86\vt.exe	Lookup

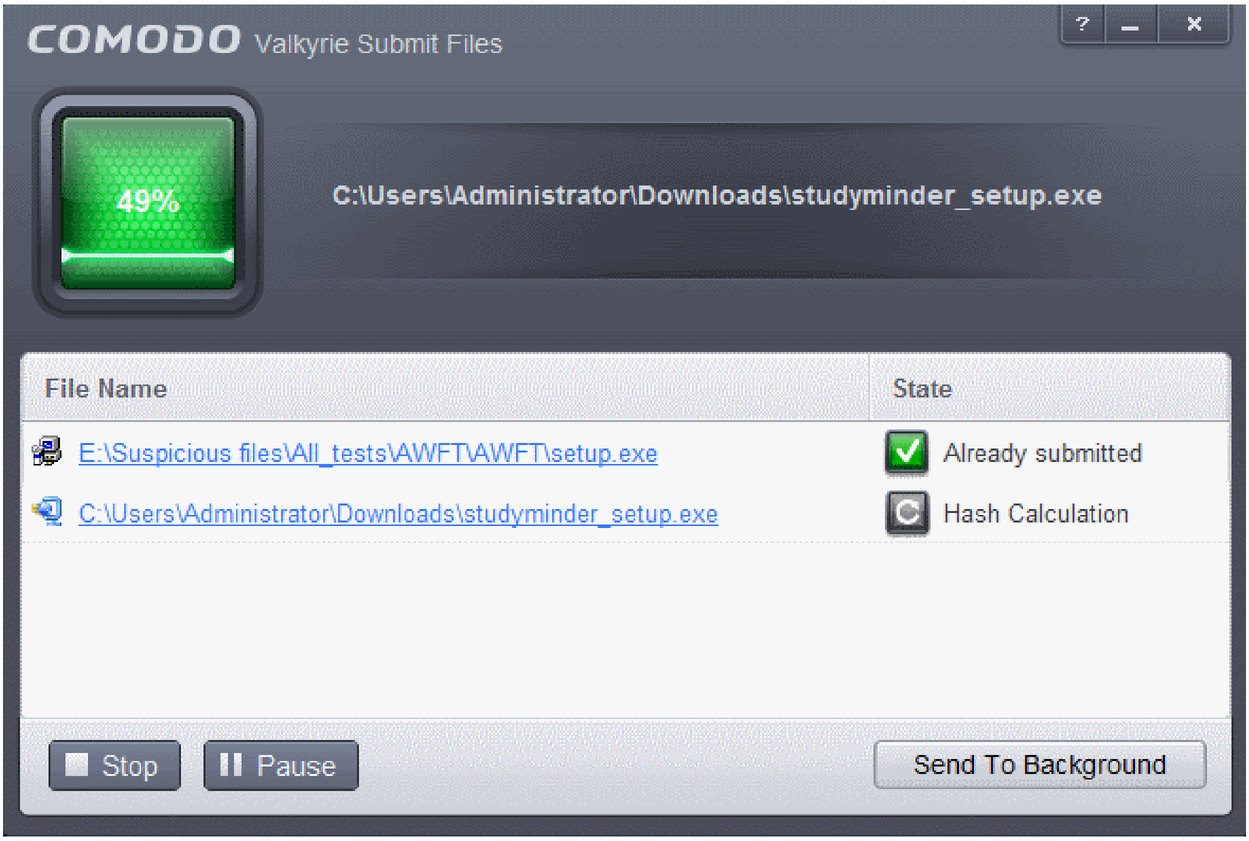
You can view the list of files you submitted so far, from the **Submitted Files** panel.

To submit files for Valkyrie analysis

Valkyrie is a online file verdict system that tests submitted files with a range of static and behavioral checks in order to identify those that are malicious.

- Select the file(s) to be submitted from the 'File List' pane. You can select several entries to be sent at once by marking the check-boxes beside the entries.
- Click the handle from the bottom and click 'Submit', then 'Submit to Valkyrie' from the options. The file(s) will be immediately sent to Comodo Valkyrie.

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Submit' from the context sensitive menu or click 'Yes' in the submit unknown files dialog from the ' **Valkyrie Lookup...**' feature.



C:\Users\Administrator\Downloads\studyminder_setup.exe

File Name	State
E:\Suspicious files\All_tests\AWFT\AWFT\setup.exe	✓ Already submitted
C:\Users\Administrator\Downloads\studyminder_setup.exe	Hash Calculation

You can view the list of files you submitted so far, from the '**Submitted Files** ' panel.

Exporting and Importing the File List

You can export the list of files with their currently assigned file ratings to an XML file and store the list on a safe place. This is useful to restore your File List, in case you are reinstalling the CCS application for some reasons.

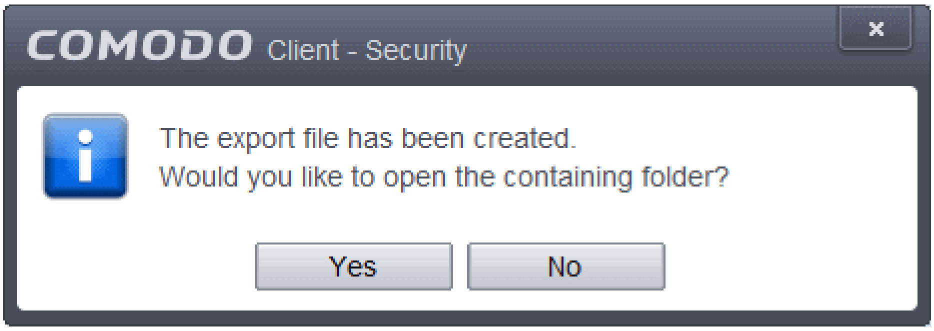
To export the File List

- Click the handle from the 'File List' pane and choose 'Export' from the options

Tip: Alternatively, right click inside the 'File List' page and choose 'Export' from the context sensitive menu.

- Navigate to the location to store the XML file containing the file list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.



The export file has been created.
Would you like to open the containing folder?

To import a saved file list

- Click the handle from the 'File List' pane and choose 'Import' from the options

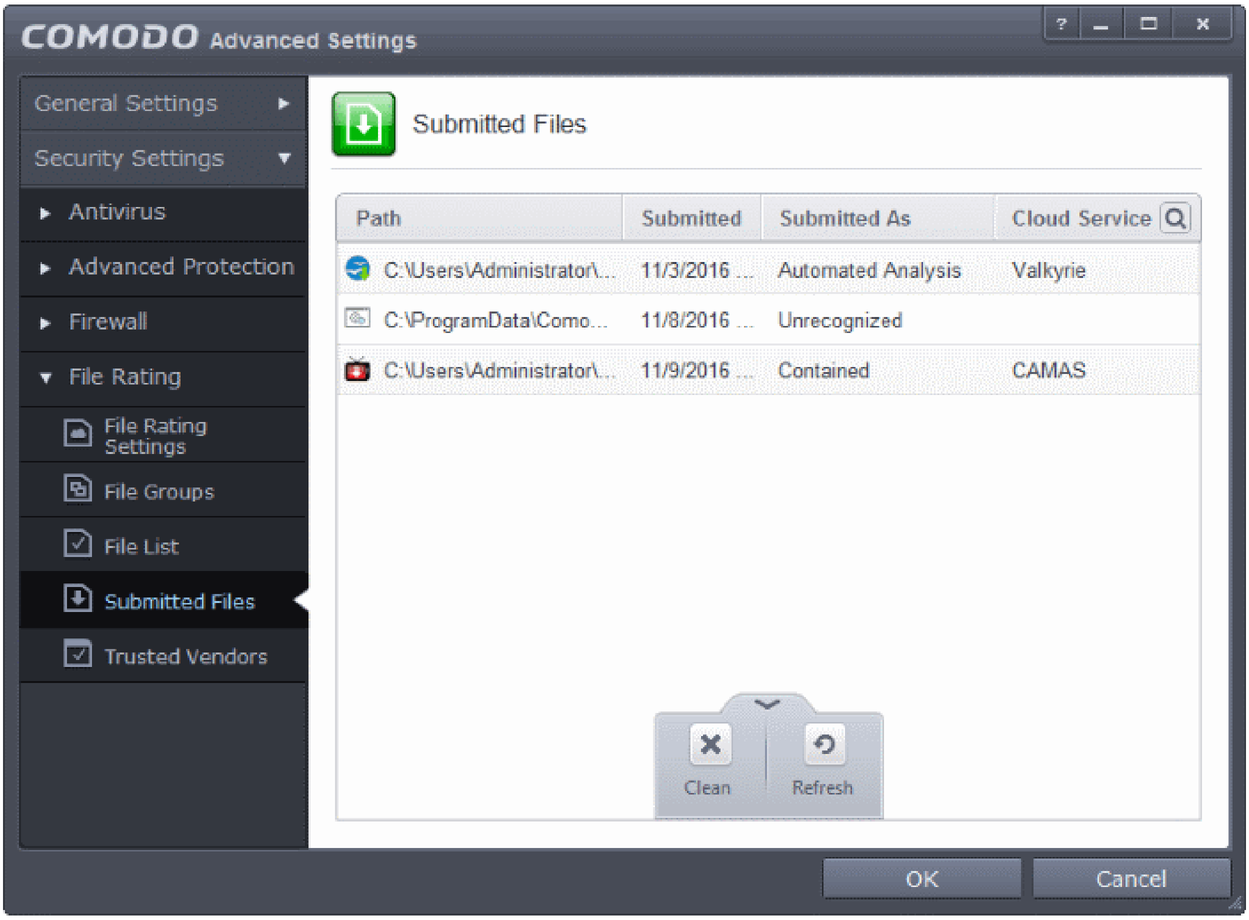
Tip: Alternatively, right click inside the 'File List' page and choose 'Import' from the context sensitive menu.

- 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'.

6.2.4.4. Submitted Files

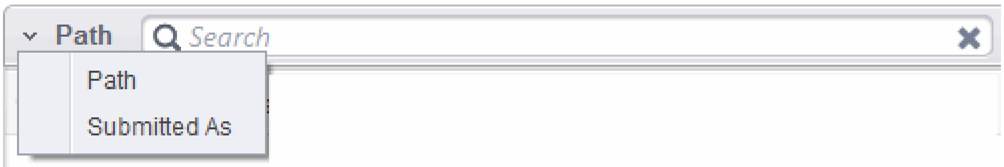
The Submitted Files panel displays a list of files you have submitted so far for analysis to CAMAS and Comodo Valkyrie.



Path	Submitted	Submitted As	Cloud Service
C:\Users\Administrator\...	11/3/2016 ...	Automated Analysis	Valkyrie
C:\ProgramData\Como...	11/8/2016 ...	Unrecognized	
C:\Users\Administrator\...	11/9/2016 ...	Contained	CAMAS

You can use the search option to find a specific file in the list.

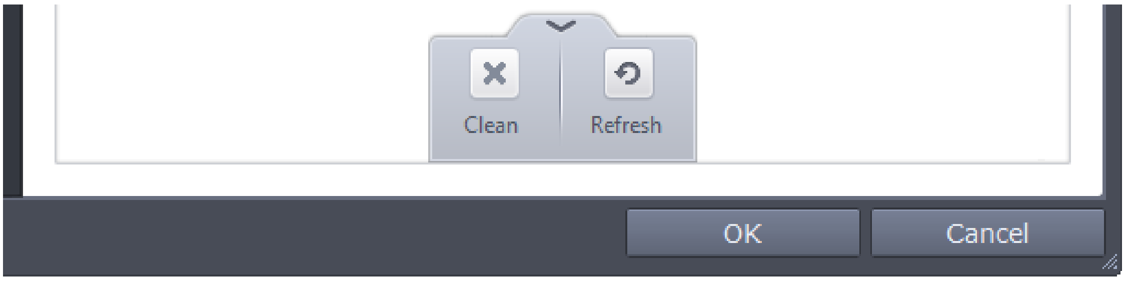
To use the search option, click the search icon 🔍 at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the file path or the submitted status as per the selected criteria in the search field.

- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Clicking the handle at the bottom of the panel opens the following options:



- **Clean** - Clears the list
- **Refresh** - Reloads the list to add items that are submitted recently

6.2.4.5. Trusted Vendors List

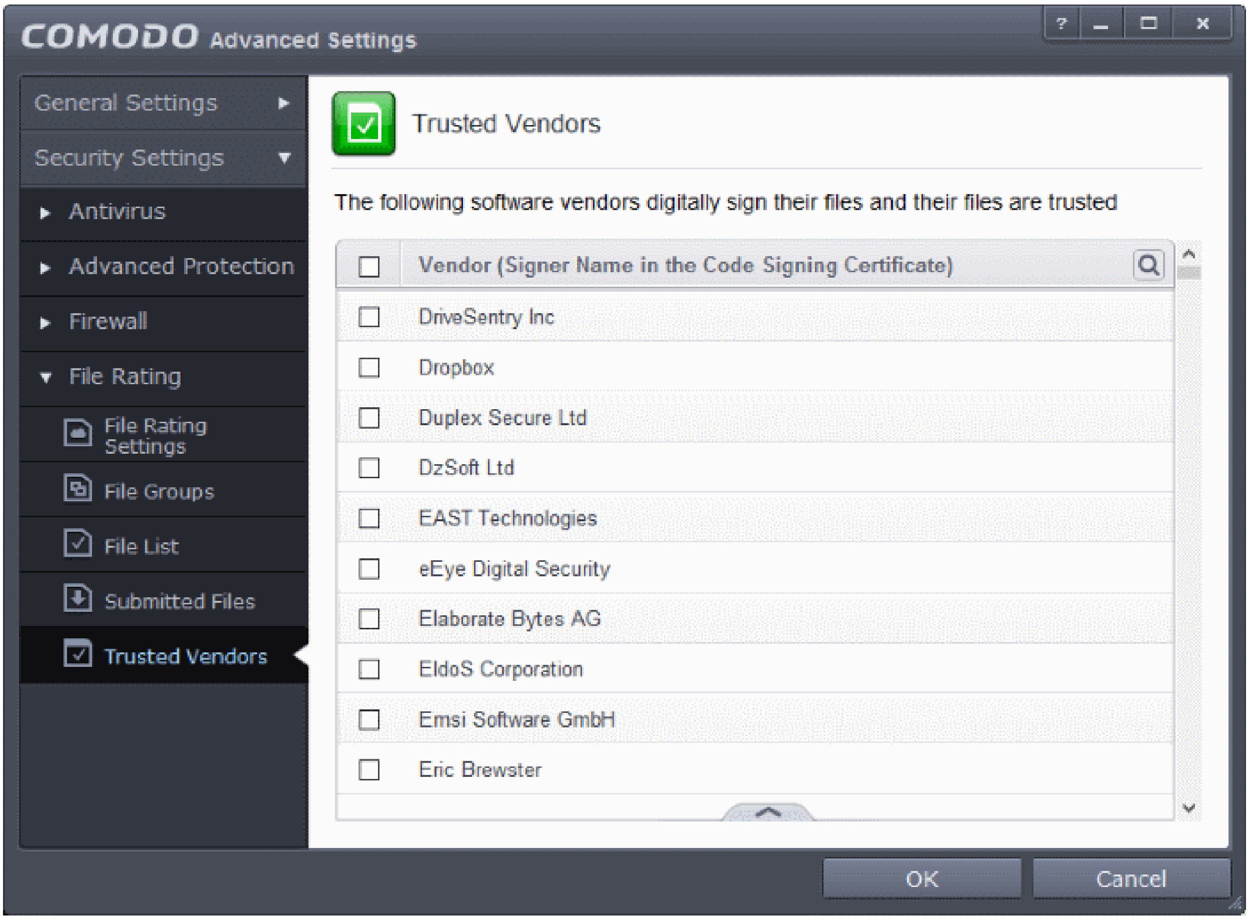
In Comodo Client Security, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Vendor' list.

From this point:

- IF the vendor is on the Trusted Software Vendor List AND the user has enabled '**Trust Applications signed by Trusted Vendors**' in the File rating Settings panel, THEN the application will be trusted and allowed to run.
- IF the vendor is not on the Trusted Software Vendor List OR the user has not enabled 'Trust Applications signed by Trusted Vendors' THEN the application will be contained. If the application in question is an installer then CCS will generate an elevated privilege alert.

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

The 'Trusted Vendors' panel can be opened by clicking Security Settings > File Rating > Trusted Vendors.



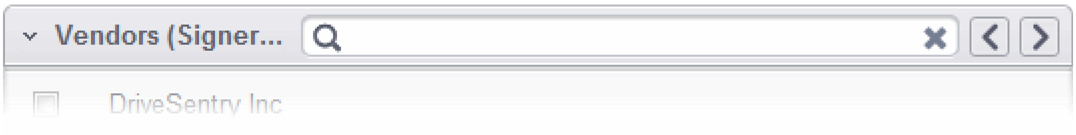
Trusted Vendors

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

□	Vendor (Signer Name in the Code Signing Certificate)
□	DriveSentry Inc
□	Dropbox
□	Duplex Secure Ltd
□	DzSoft Ltd
□	EAST Technologies
□	eEye Digital Security
□	Elaborate Bytes AG
□	EldoS Corporation
□	Emsi Software GmbH
□	Eric Brewster

You can use the search option to find a specific vendor in the list.

To use the search option, click the search icon 🔍 at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the vendor's name in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Click here to read background information on digitally signing software

Click here to learn how to Add / Define a user-trusted vendor

Software Vendors - click here to find out about getting your software added to the list

Background

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

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

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

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

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

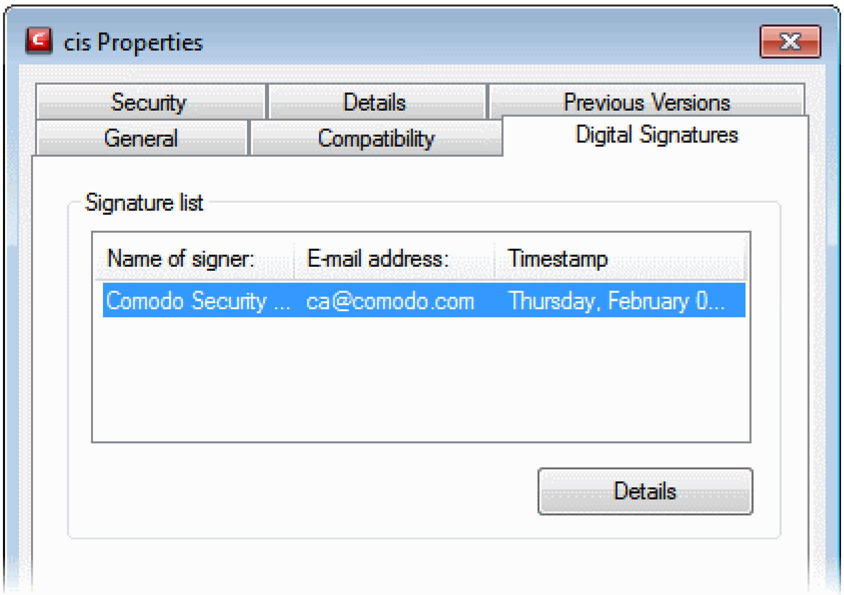
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign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

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Client Security (if you would like to read more about code signing certificates, see http://www.instantssl.com/code-signing/).

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

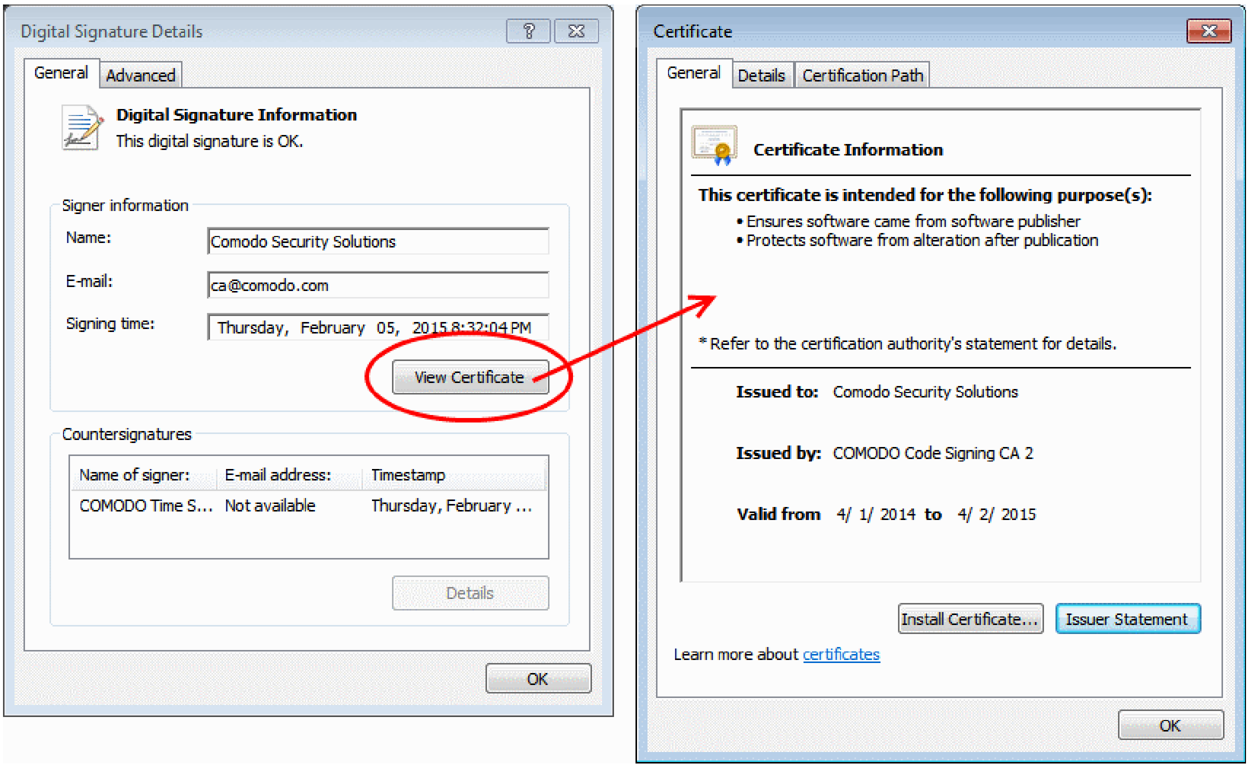
- Browse to the (default) installation directory of Comodo Client Security.
- Right click on the file CCS.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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



Name of signer:	E-mail address:	Timestamp
Comodo Security ...	ca@comodo.com	Thursday, February 0...

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



Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information
Name: Comodo Security Solutions
E-mail: ca@comodo.com
Signing time: Thursday, February 05, 2015 8:32:04 PM

Countersignatures

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

Certificate

General | Details | Certification Path

Certificate Information

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

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

Issued to: Comodo Security Solutions

Issued by: COMODO Code Signing CA 2

Valid from 4/ 1/ 2014 **to** 4/ 2/ 2015

Learn more about certificates

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

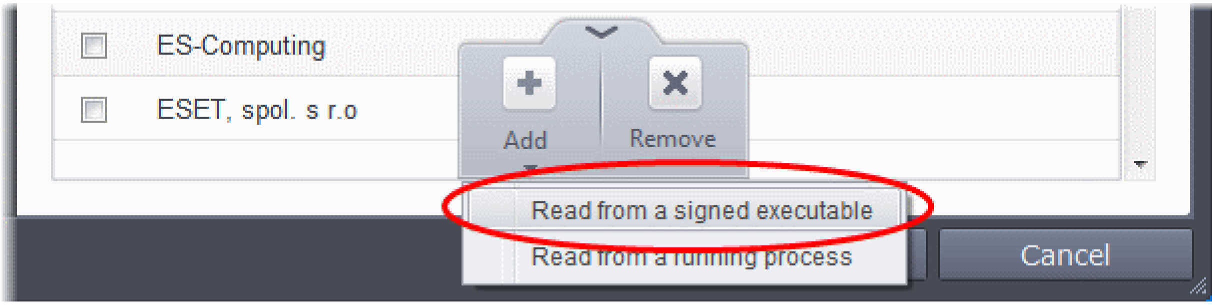
Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

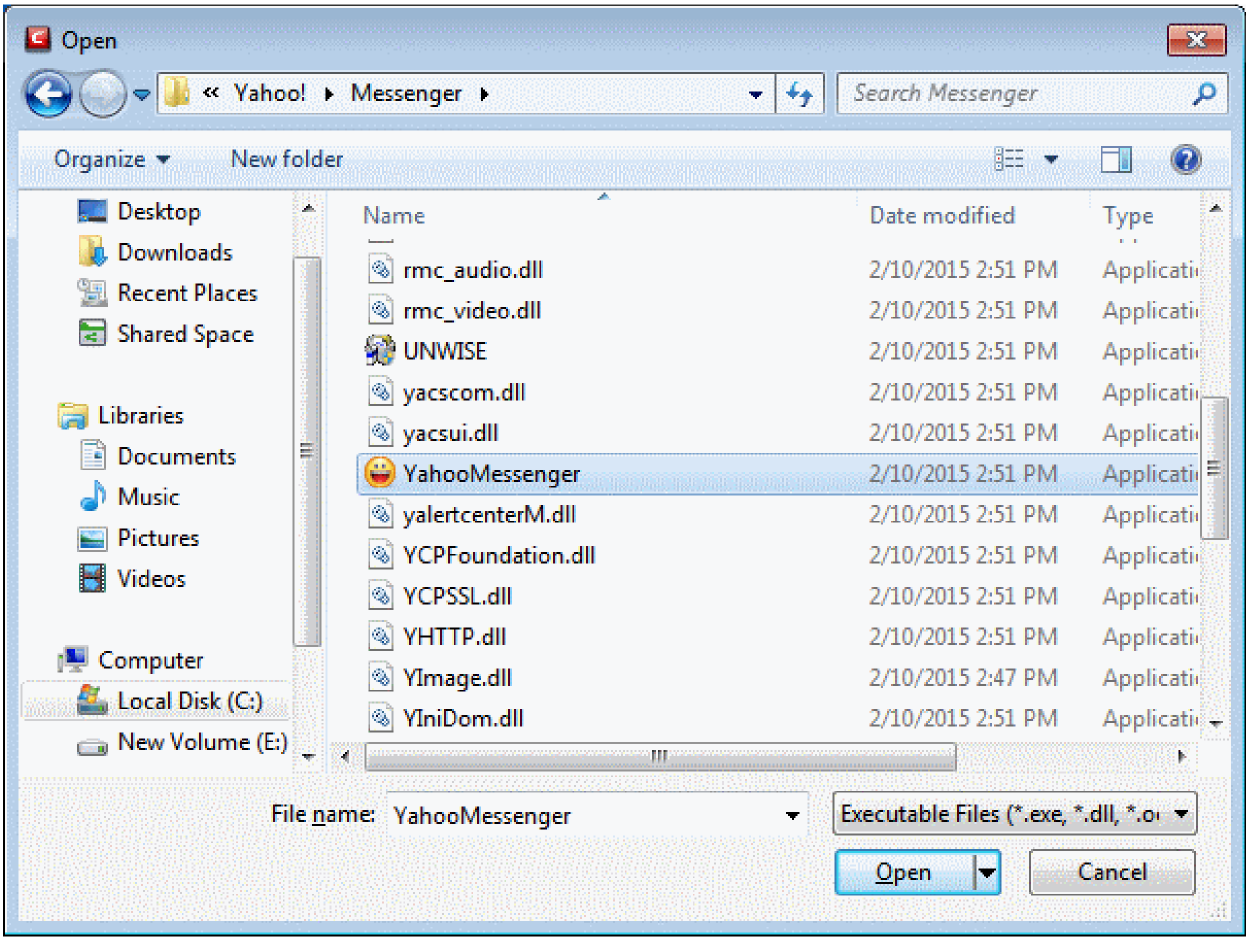
- By reading the vendor's signature from an executable file on your local drive
- By reading the vendor's signature from a running process

To add a trusted vendor by reading the vendor's signature from an executable

- Click the handle from the bottom and choose 'Add' > 'Read from a signed executable'



- Browse to the location of the executable your local drive. In the example below, we are adding the executable 'YahooMessenger.exe'.

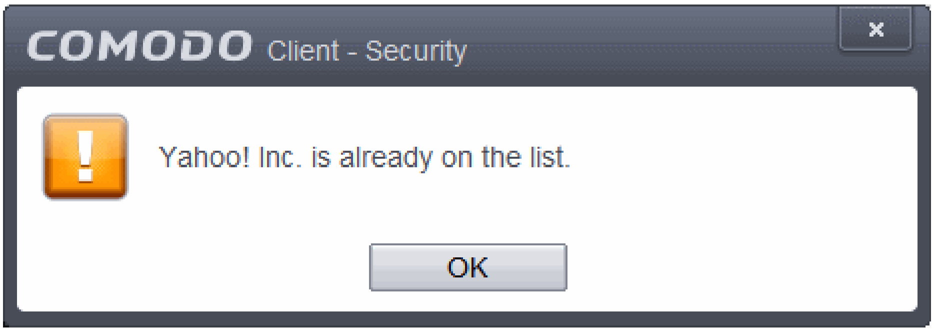


Name	Date modified	Type
rmc_audio.dll	2/10/2015 2:51 PM	Applicati
rmc_video.dll	2/10/2015 2:51 PM	Applicati
UNWISE	2/10/2015 2:51 PM	Applicati
yacscom.dll	2/10/2015 2:51 PM	Applicati
yacsui.dll	2/10/2015 2:51 PM	Applicati
YahooMessenger	2/10/2015 2:51 PM	Applicati
yalertcenterM.dll	2/10/2015 2:51 PM	Applicati
YCPFoundation.dll	2/10/2015 2:51 PM	Applicati
YCPSSL.dll	2/10/2015 2:51 PM	Applicati
YHTTP.dll	2/10/2015 2:51 PM	Applicati
YImage.dll	2/10/2015 2:47 PM	Applicati
YIniDom.dll	2/10/2015 2:51 PM	Applicati

File name: YahooMessenger

Executable Files (*.exe, *.dll, *.o

On clicking 'Open', 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 Trusted Vendor list (TVL). If the file is already in the list, you will be notified.

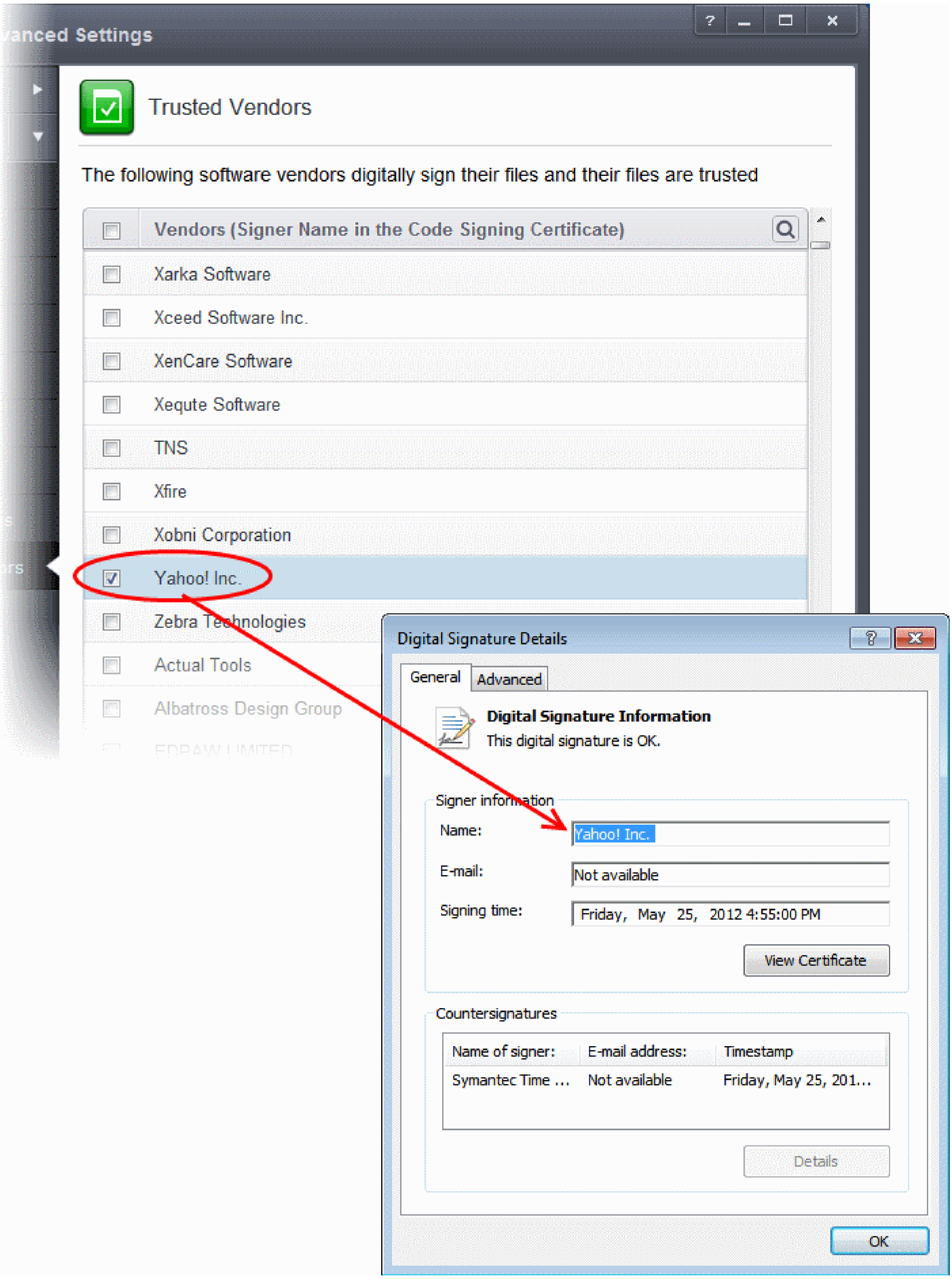


Yahoo! Inc. is already on the list.

To verify the signer

- Navigate to the installation location of the executable
- Right click on the executable file
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).
- From the 'Digital Certificate Details' dialog, click 'View Certificate'.

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



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

☐	Vendors (Signer Name in the Code Signing Certificate)
☐	Xarka Software
☐	Xceed Software Inc.
☐	XenCare Software
☐	Xequte Software
☐	TNS
☐	Xfire
☐	Xobni Corporation
☑	Yahoo! Inc.
☐	Zebra Technologies
☐	Actual Tools
☐	Albatross Design Group
☐	EDRAW LIMITED

Digital Signature Details

Digital Signature Information
This digital signature is OK.

Signer information

Name: Yahoo! Inc.

E-mail: Not available

Signing time: Friday, May 25, 2012 4:55:00 PM

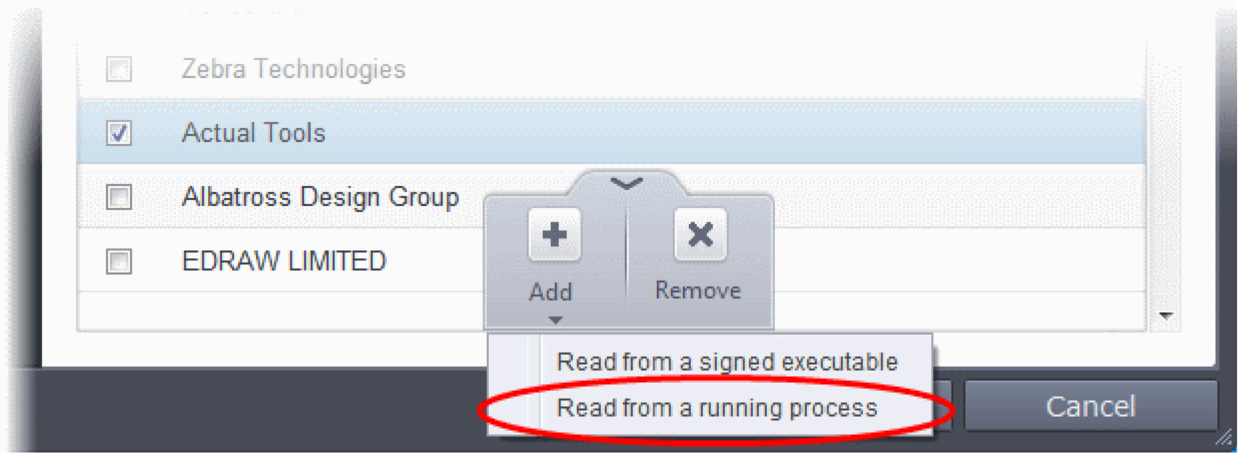
Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	Friday, May 25, 201...

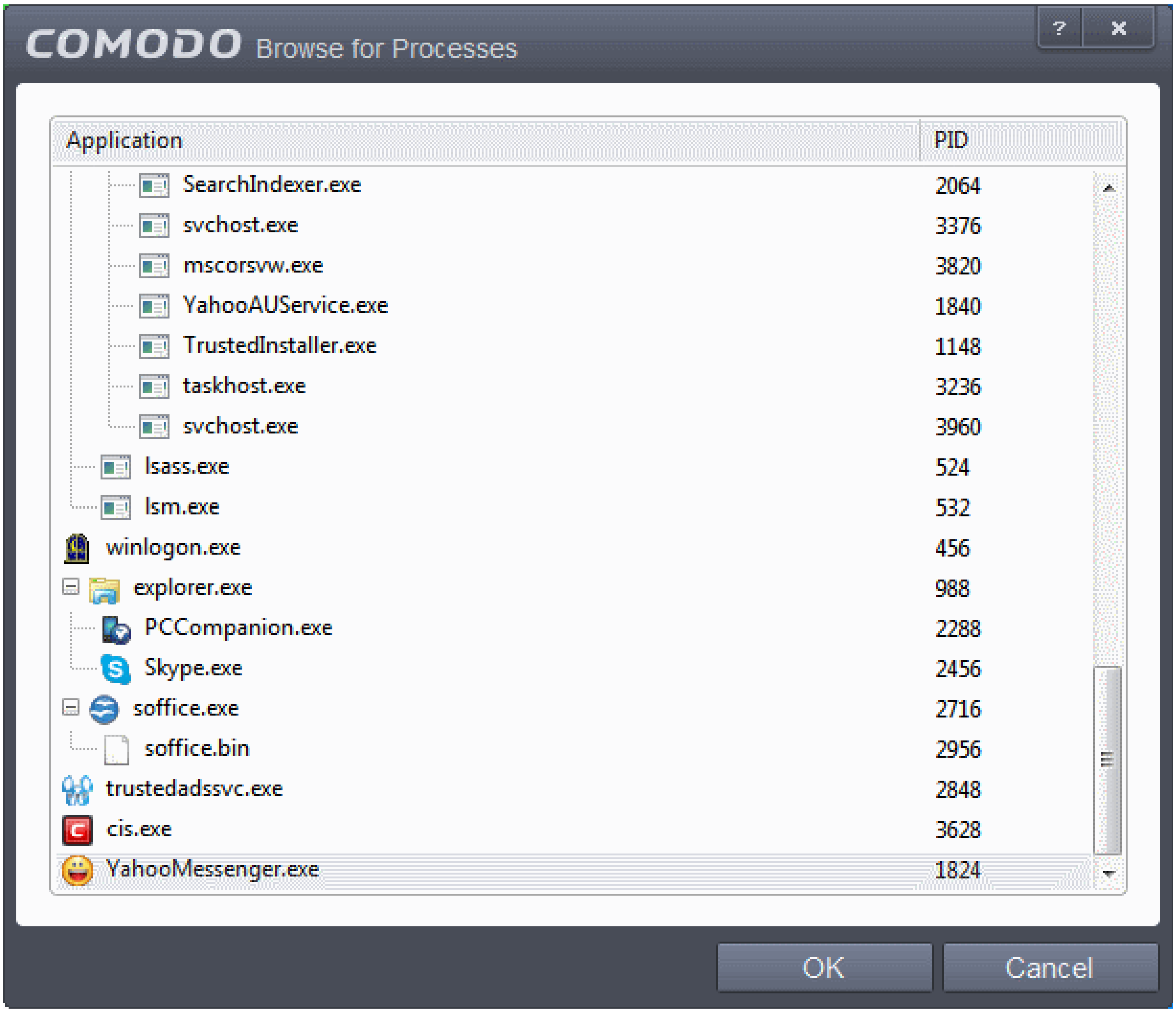
In the example above, Comodo Client Security was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to the list. All future software that is signed by the vendor 'Yahoo! Inc.' is automatically added to the Comodo Trusted Vendor list UNLESS you change this setting in File Rating Settings.

To add a trusted vendor from a currently running process

- Click the handle from the bottom and choose 'Add' > 'Read from a running process'



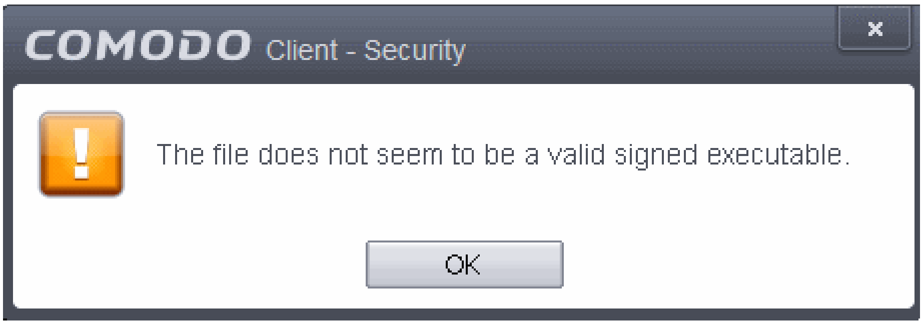
- Select the signed executable that you want to trust and click the 'OK' button.


COMODO Browse for Processes

Application	PID
SearchIndexer.exe	2064
svchost.exe	3376
mscorsvw.exe	3820
YahooAUService.exe	1840
TrustedInstaller.exe	1148
taskhost.exe	3236
svchost.exe	3960
lsass.exe	524
lsm.exe	532
winlogon.exe	456
explorer.exe	988
PCCompanion.exe	2288
Skype.exe	2456
soffice.exe	2716
soffice.bin	2956
trustedadssvc.exe	2848
cis.exe	3628
YahooMessenger.exe	1824

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 Trusted Software Vendors list.

If Comodo Client Security cannot verify that the software certificate is signed by a Trusted CA then it does not add the software vendor to the list of 'Trusted Vendors'. In this case, you can see the following error message.



The file does not seem to be a valid signed executable.

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 it's capacity as a Trusted CA, has independently validated as legitimate companies. If the user needs to remove any of these vendors from the list, it can be done by selecting the vendor, clicking 'Remove' and restarting the system. Please note that the removal will take effect only on restarting the system.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default Trusted Vendor List that is shipped with Comodo Client Security. This service is free of cost and is also open to vendors that have used code signing certificates from any Certificate Authority. Upon adding the software to the Trusted Vendor list, 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 Trusted Vendors list through the sign-up form at http://internetsecurity.comodo.com/trustedvendor/signup.php and make sure that the software can be downloaded by our technicians. Our technicians check whether:

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

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

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

Appendix 1 - CCS How to... Tutorials

The 'How To...' section of the guide contains guidance on key tasks of Comodo Client Security. Use the links below to go to each tutorial's page.

How to...:

- Enabling / Disabling AV, Firewall, Auto-Containment and Viruscope Easily- Guidance on changing the current enabled/disabled states of Antivirus, Firewall and Advanced Protection.
- Set up the Firewall For Maximum Security and Usability - A brief outline of the setting up a secure connection to Internet
- Block Internet Access while Allowing Local Area Network (LAN) Access - Guidance on configuring the Firewall to allow only Intranet or LAN connection and to block Internet connection
- Block/allow Websites Selectively to Users of Your Computer - Guidance on configuring website filtering rules for different users to selectively allow or block specific websites to them.
- Setup HIPS for maximum security and usability - A brief outline of how to set Host intrusion Protection for the optimum balance between security and usability
- Create Rules for Auto-Containing Applications - A brief outline of how to set create auto-containment rules for the maximum security against untrusted applications
- Run an instant Antivirus scan on selected items - Guidance on initiating a manual scan on selected folders/files to check for viruses and other malware.
- Create an Antivirus scanning schedule - Guidance on time-table scheduling of antivirus scans to be run on selected items at selected intervals
- Run an untrusted program inside the container - Guidance on executing a program that you do not trust to be safe, inside the container to protect any harmful effects of the program upon your system.
- Run browsers inside the container - Guidance on running your browser, inside the container when you plan to visit untrusted websites.
- Restore incorrectly quarantined item(s) - Help to restore files and executables that were moved to quarantine by mistake
- Submit quarantined items to Comodo for analysis - Advice on how to send suspicious files/executables to Comodo for analysis
- Enable File Sharing Applications like BitTorrent and Emule - Explains how to configure Comodo Firewall for file sharing through popular software
- Block any downloads of a specific file type - Explains how to configure Advanced Protection to block downloads of files of a specific type
- Disable Auto-Containment on a Per-application Basis - Explains how to exclude specific files or file types from the auto-containment process
- Switch Off Automatic Antivirus and Software Updates - Explains how to stop automatic software and virus updates
- Suppressing CCS Alerts Temporarily - Helps you to switch off CCS pop-up alerts to avoid interruptions while configuring the application
- Control External Device Accessibility – Explains how to restrict access to external devices such as USB pen drive on the endpoints.

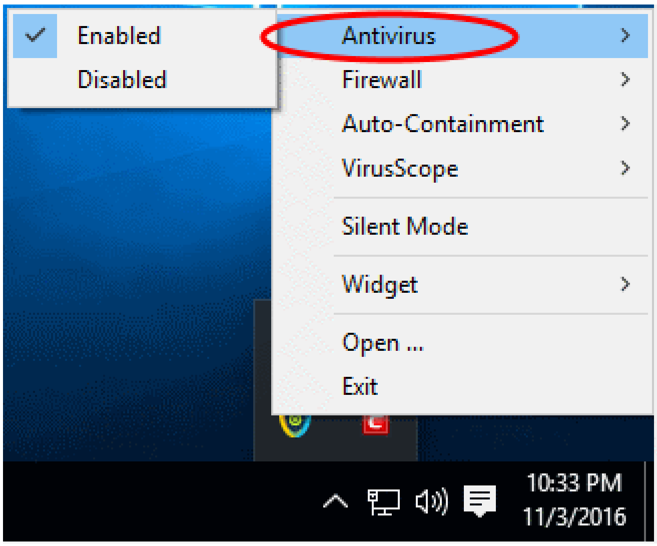
Enabling / Disabling AV, Firewall, Auto-Containment and Viruscope Easily

Comodo Client Security allows users to quickly switch the Enabled/Disabled states of Antivirus, Firewall, Auto-Containment and Viruscope by right clicking on the system tray icon.

Antivirus

To enable/disable the Antivirus

1. Right click on the system tray icon
2. Move the mouse cursor over 'Antivirus'



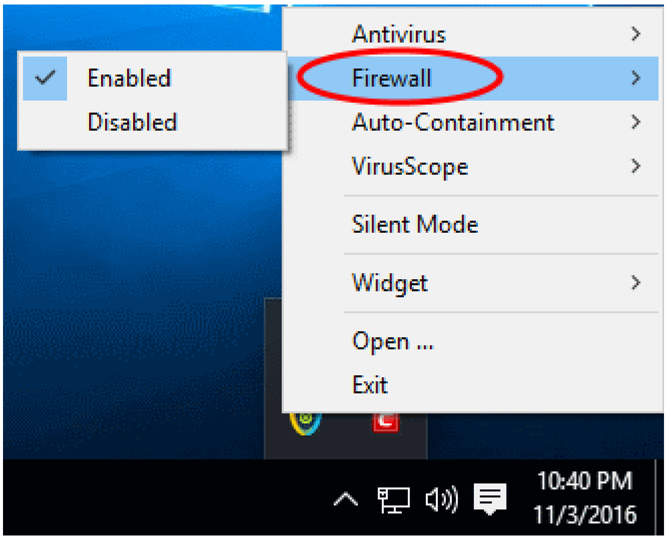
3. Choose 'Enabled or Disabled' as per your choice

You can also set the security level from the Home Screen

Firewall

To enable/disable the Firewall

1. Right click on the system tray icon
2. Move the mouse cursor over 'Firewall'



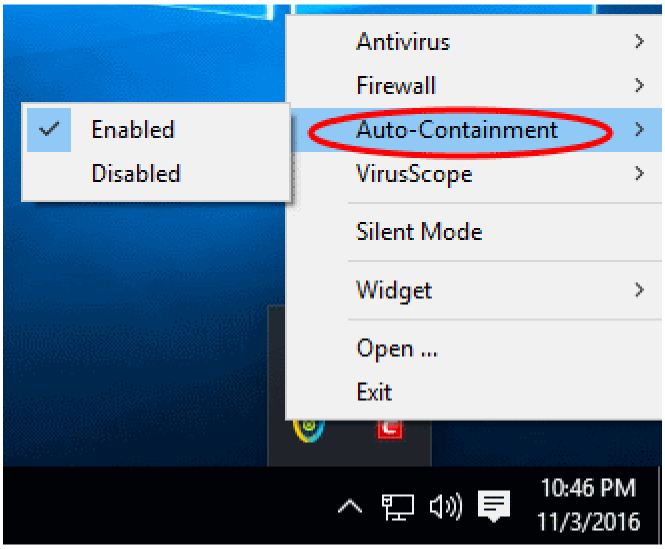
4. Choose 'Enabled or Disabled' as per your choice

You can also set the security level from the Home Screen.

Auto-Containment

To enable/disable the Auto-Containment

- Right click on the system tray icon
- Move the mouse cursor over 'Auto-Containment'

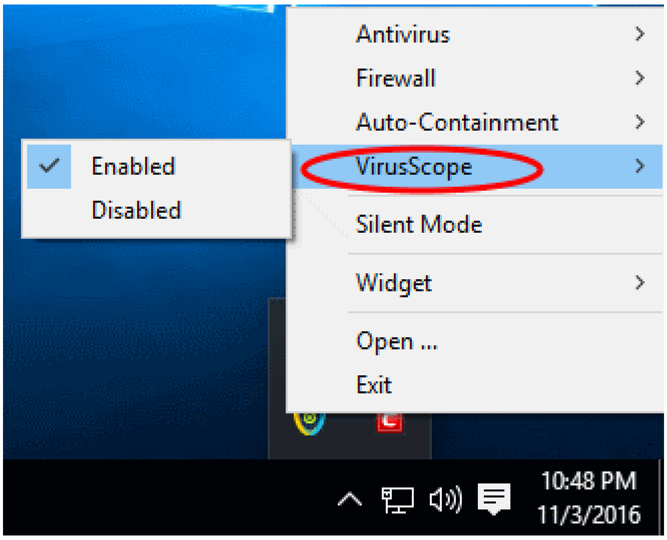


- Choose 'Enabled or Disabled' as per your choice

You can also set the security level from the Home Screen.

To enable/disable the Viruscope

1. Right click on the system tray icon
2. Move the mouse cursor over 'Viruscope'



3. Choose 'Enabled' or 'Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

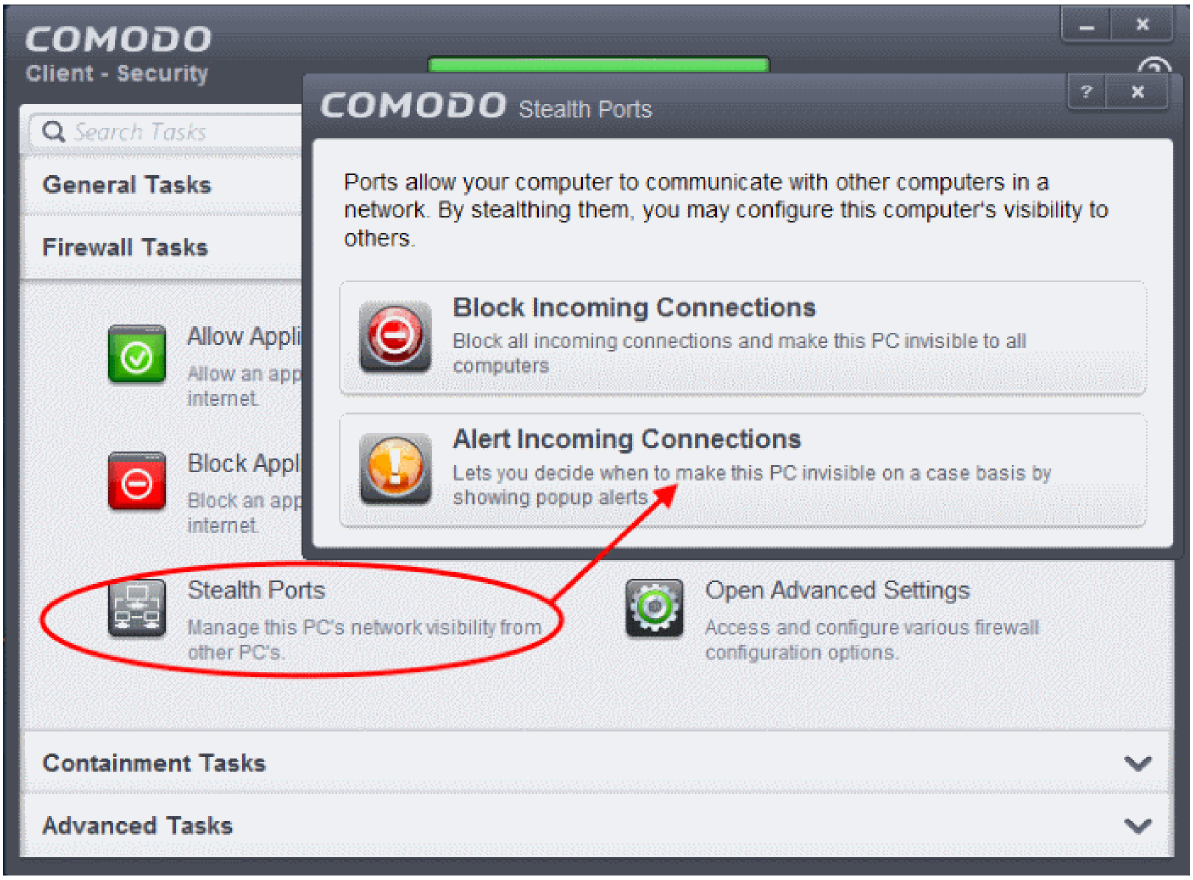
Set up the Firewall For Maximum Security and Usability

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. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface
3. Open Stealth Ports interface by clicking the 'Stealth Ports' icon from the Firewall Tasks panel



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

COMODO Client - Security
Search Tasks
General Tasks
Firewall Tasks
Allow Appli
Allow an app internet
Block Appl
Block an app internet
Stealth Ports
Manage this PC's network visibility from other PC's.
Open Advanced Settings
Access and configure various firewall configuration options.
Containment Tasks
Advanced Tasks
COMODO Stealth Ports
Block Incoming Connections
Block all incoming connections and make this PC invisible to all computers
Alert Incoming Connections
Lets you decide when to make this PC invisible on a case basis by showing popup alerts

4. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

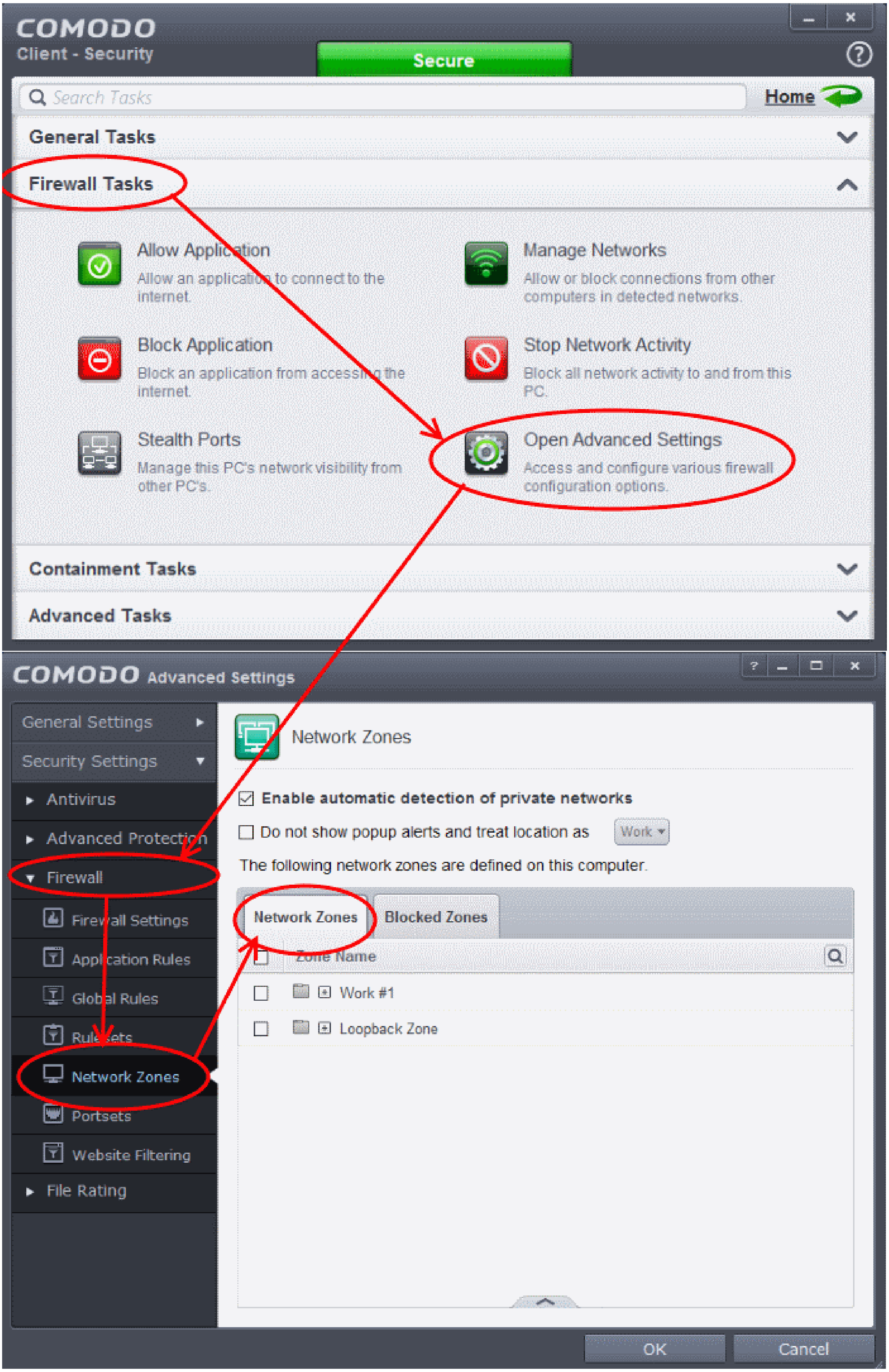
Click here for more details on Stealthing your Computer Ports

Network Zones Settings

The 'Network Zones' settings allow you to configure the protection level for network connection to a Router/home network. (This is usually done **automatically** for you).

To view the configurations

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Network Zones' under Firewall from the left hand side pane
4. Click 'Network Zones' tab from the 'Network Zones' interface



☑ Enable automatic detection of private networks

□ Do not show popup alerts and treat location as Work

The following network zones are defined on this computer.

Check the Loopback zone and Local Area Network #1. **In most cases**, the loopback zone IP address should be *127.0.01/255.0.0.0*
In most cases, the IP address of the auto detected Network zone should be *192.168.1.100/255.255.255.0 .*

5. Check these addressees and click 'OK'.

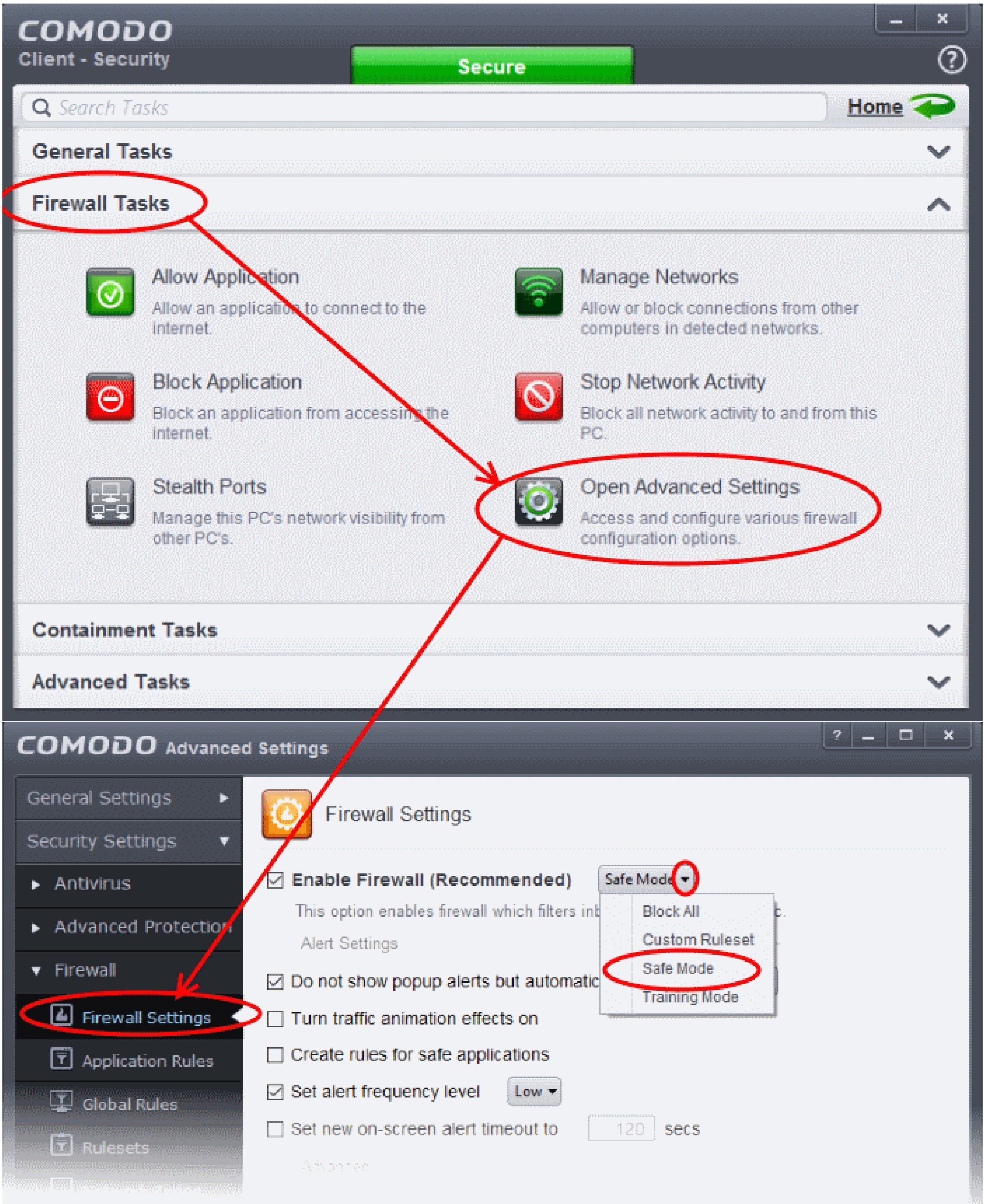
Click here for more details on Network Zones settings

Firewall Behavior Settings

The Firewall Behavior Settings option allows you to configure the protection level for your Internet connection and the frequency of alerts generated.

To open Firewall Behavior Settings panel

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Firewall Settings' under Firewall from the left hand side pane
4. Ensure that 'Enable Firewall' is selected and choose **Safe mode** from the drop-down beside it.



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filters inb

Alert Settings

☑ Do not show popup alerts but automatic

☐ Turn traffic animation effects on

☐ Create rules for safe applications

☑ Set alert frequency level Low

☐ Set new on-screen alert timeout to 120 secs

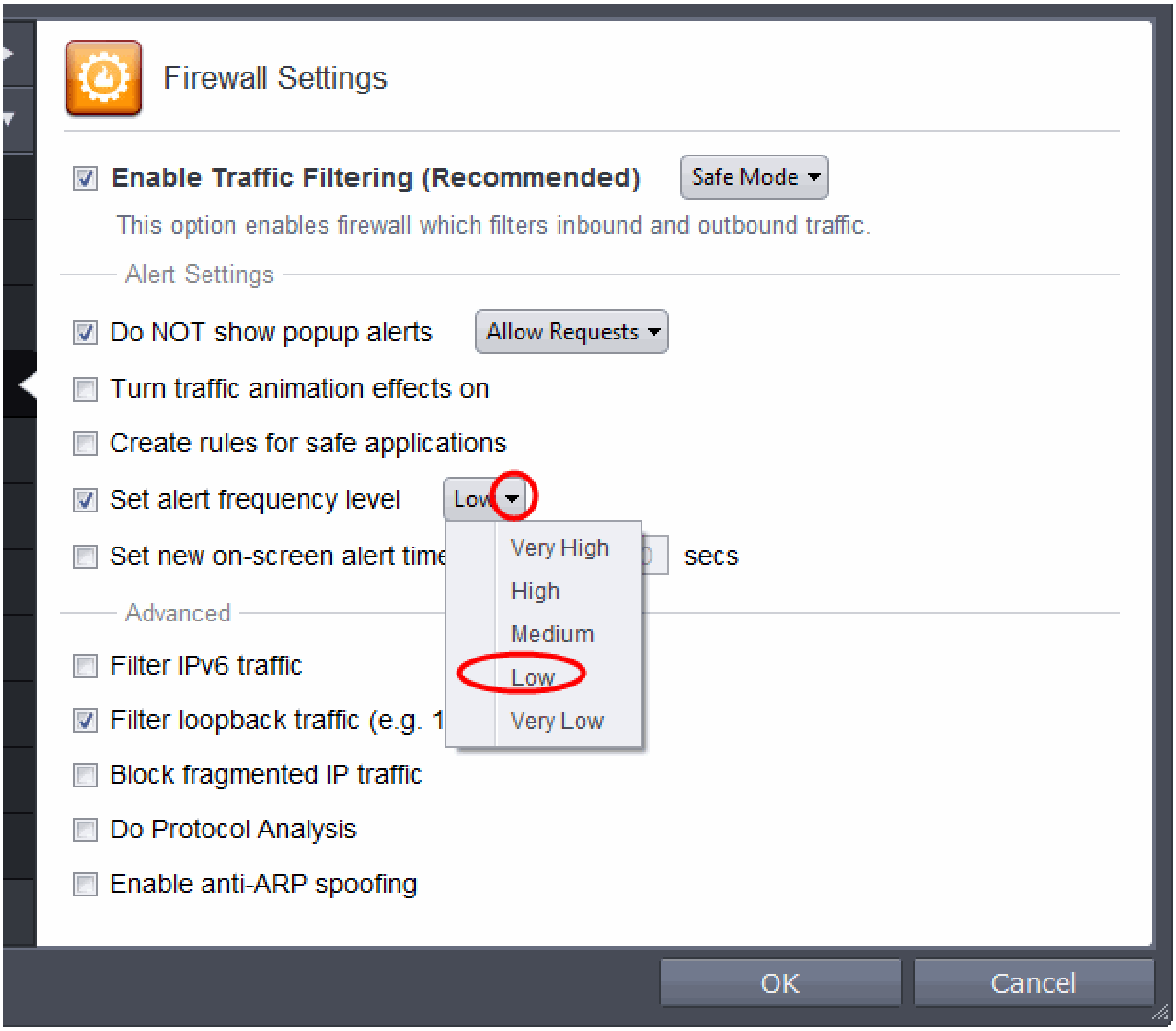
Safe Mode: While filtering network traffic, the firewall will automatically create rules that allow all traffic for the components of applications certified as 'Safe' by Comodo. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

Under 'Alert Settings' in the same interface:

- Deselect Do not show popup alerts

- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.



Firewall Settings

☑ **Enable Traffic Filtering (Recommended)** Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do NOT show popup alerts Allow Requests

□ Turn traffic animation effects on

□ Create rules for safe applications

☑ Set alert frequency level Low

□ Set new on-screen alert time secs

Advanced

□ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 1

□ Block fragmented IP traffic

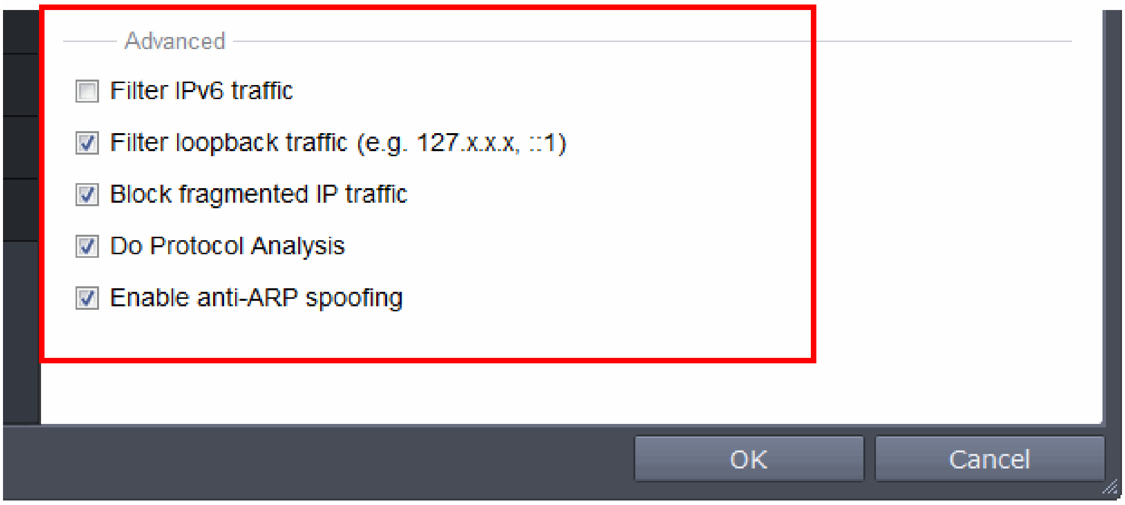
□ Do Protocol Analysis

□ Enable anti-ARP spoofing

Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- Select **Filter loopback traffic**
- Ensure that the **Block fragmented IP traffic** is selected
  - **Block fragmented IP traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time.
- Select the '**Do Protocol Analysis'** checkbox to detect fake packets used in denial of service attacks
- Select '**Enable anti-ARP spoofing'**



Advanced

☐ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☑ Block fragmented IP traffic

☑ Do Protocol Analysis

☑ Enable anti-ARP spoofing

5. Click 'OK' for your settings to take effect.

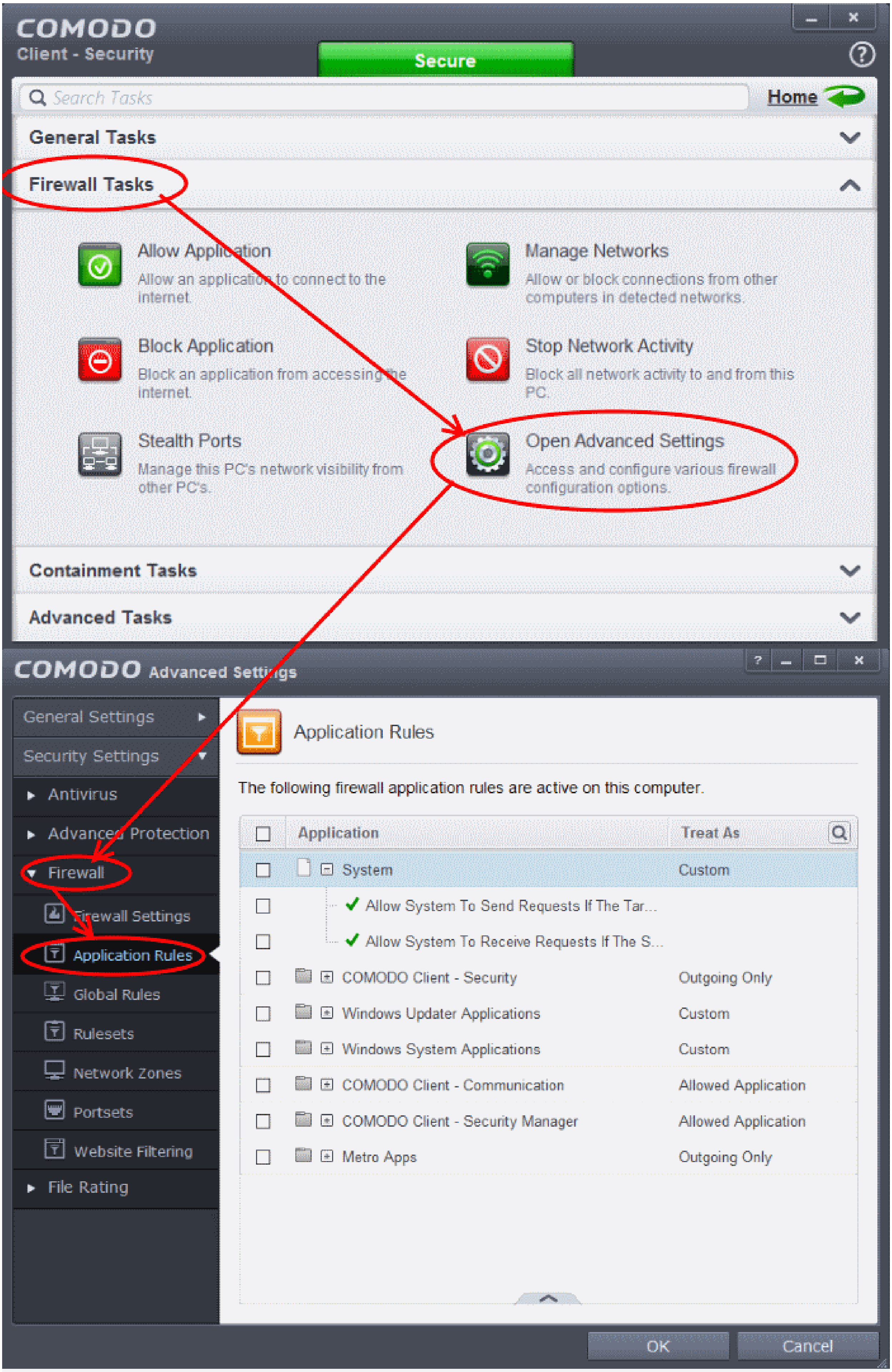
Click here for more details on Firewall Behavior Settings

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 and predefined firewall rulesets.

To view the Application Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Application Rules' under Firewall from the left hand side pane



Allow Application
Allow an application to connect to the internet.

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

Block Application
Block an application from accessing the internet.

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

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

Open Advanced Settings
Access and configure various firewall configuration options.

Application Rules

The following firewall application rules are active on this computer.

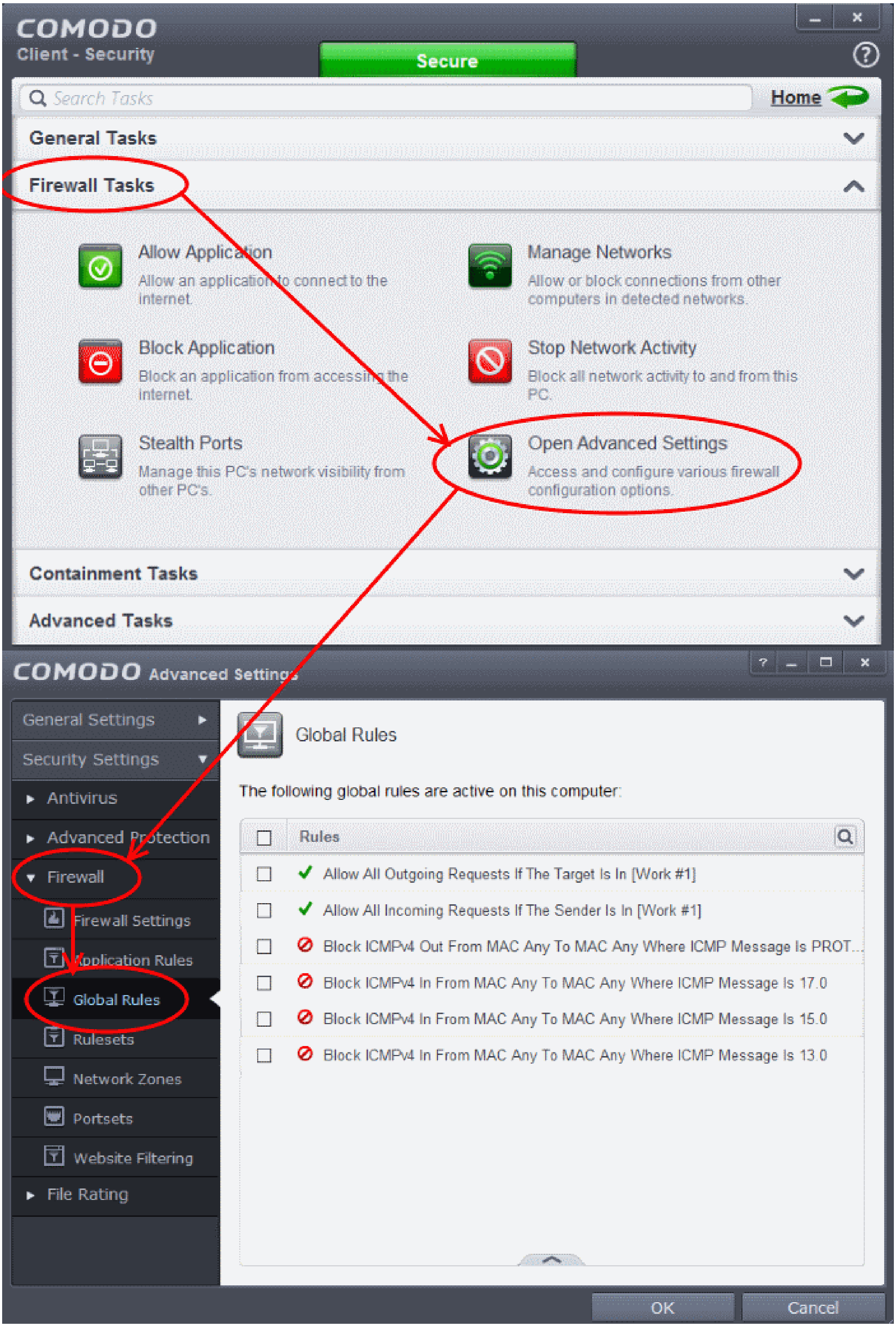
□	Application	Treat As
□	⊟ System	Custom
□	✓ Allow System To Send Requests If The Tar...	
□	✓ Allow System To Receive Requests If The S...	
□	⊞ COMODO Client - Security	Outgoing Only
□	⊞ Windows Updater Applications	Custom
□	⊞ Windows System Applications	Custom
□	⊞ COMODO Client - Communication	Allowed Application
□	⊞ COMODO Client - Security Manager	Allowed Application
□	⊞ Metro Apps	Outgoing Only

4. Click the handle from the bottom and 'Add' or 'Edit' rules for specific applications manually or remove them.

Click here for more details on Application Rules

To view the Global Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Global Rules' under Firewall from the left hand side pane



COMODO Client - Security

Secure

Search Tasks

Home

General Tasks

Firewall Tasks

Allow Application

Allow an application to connect to the internet.

Manage Networks

Allow or block connections from other computers in detected networks.

Block Application

Block an application from accessing the internet.

Stop Network Activity

Block all network activity to and from this PC.

Stealth Ports

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

Open Advanced Settings

Access and configure various firewall configuration options.

Containment Tasks

Advanced Tasks

COMODO Advanced Settings

- General Settings
- Security Settings
  - Antivirus
  - Advanced Protection
  - Firewall
    - Firewall Settings
    - Application Rules
    - Global Rules
    - Rulesets
    - Network Zones
    - Portsets
    - Website Filtering
  - File Rating

Global Rules

The following global rules are active on this computer:

☐	Rules
☐	✓ Allow All Outgoing Requests If The Target Is In [Work #1]
☐	✓ Allow All Incoming Requests If The Sender Is In [Work #1]
☐	⊘ Block ICMPv4 Out From MAC Any To MAC Any Where ICMP Message Is PROT...
☐	⊘ 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

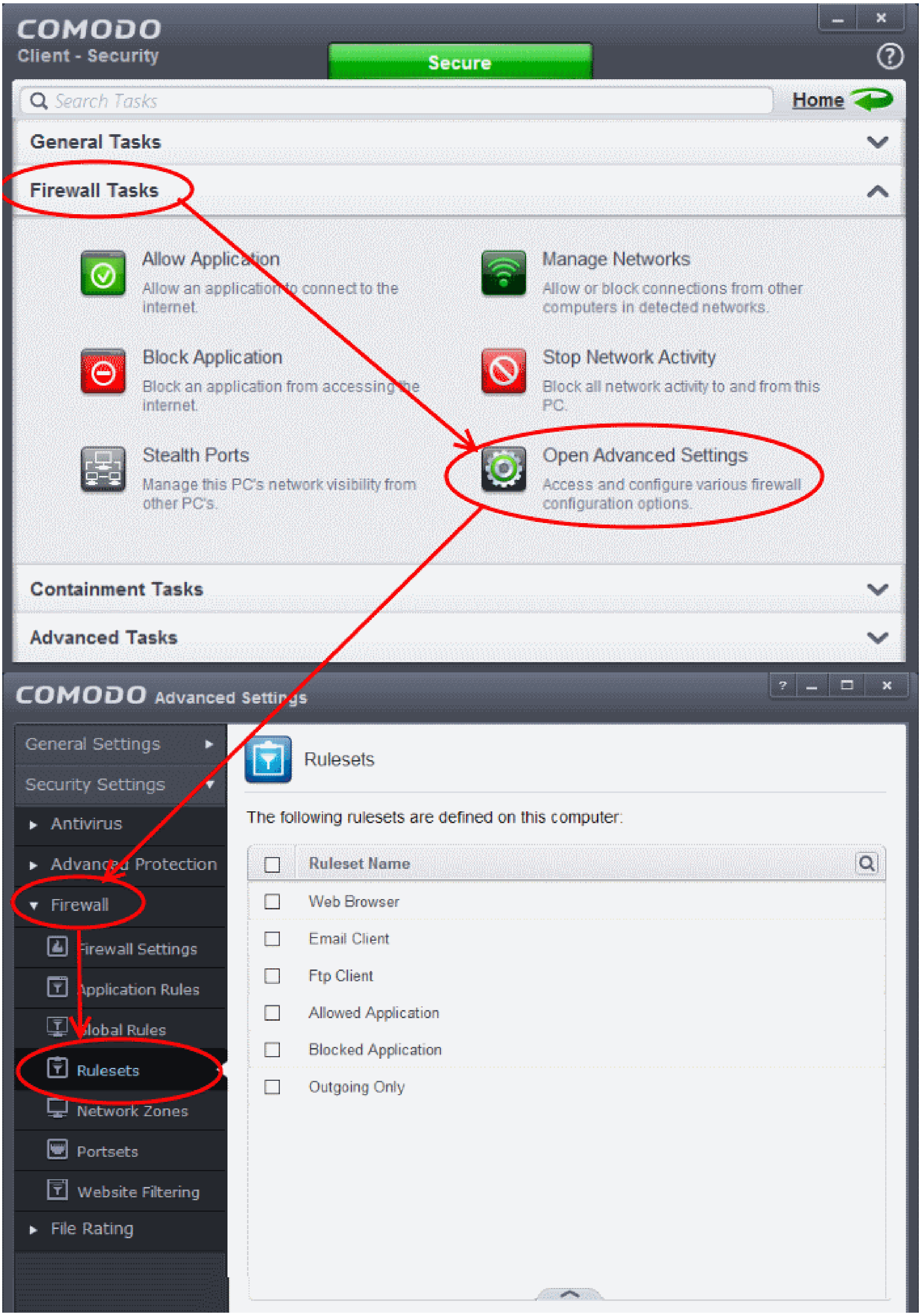
OK Cancel

4. Click the handle from the bottom and add or edit global rules manually or remove them.

Click here for more details on Global Rules

To view Predefined Firewall rulesets

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Rulesets' under Firewall from the left hand side pane



Allow Application
Allow an application to connect to the internet.

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

Block Application
Block an application from accessing the internet.

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

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

Open Advanced Settings
Access and configure various firewall configuration options.

Rulesets

The following rulesets are defined on this computer:

□	Ruleset Name
□	Web Browser
□	Email Client
□	Ftp Client
□	Allowed Application
□	Blocked Application
□	Outgoing Only

4. Click the handle from the bottom to Add, Edit or remove rulesets.

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 free connections to an internal network (intranet or LAN).

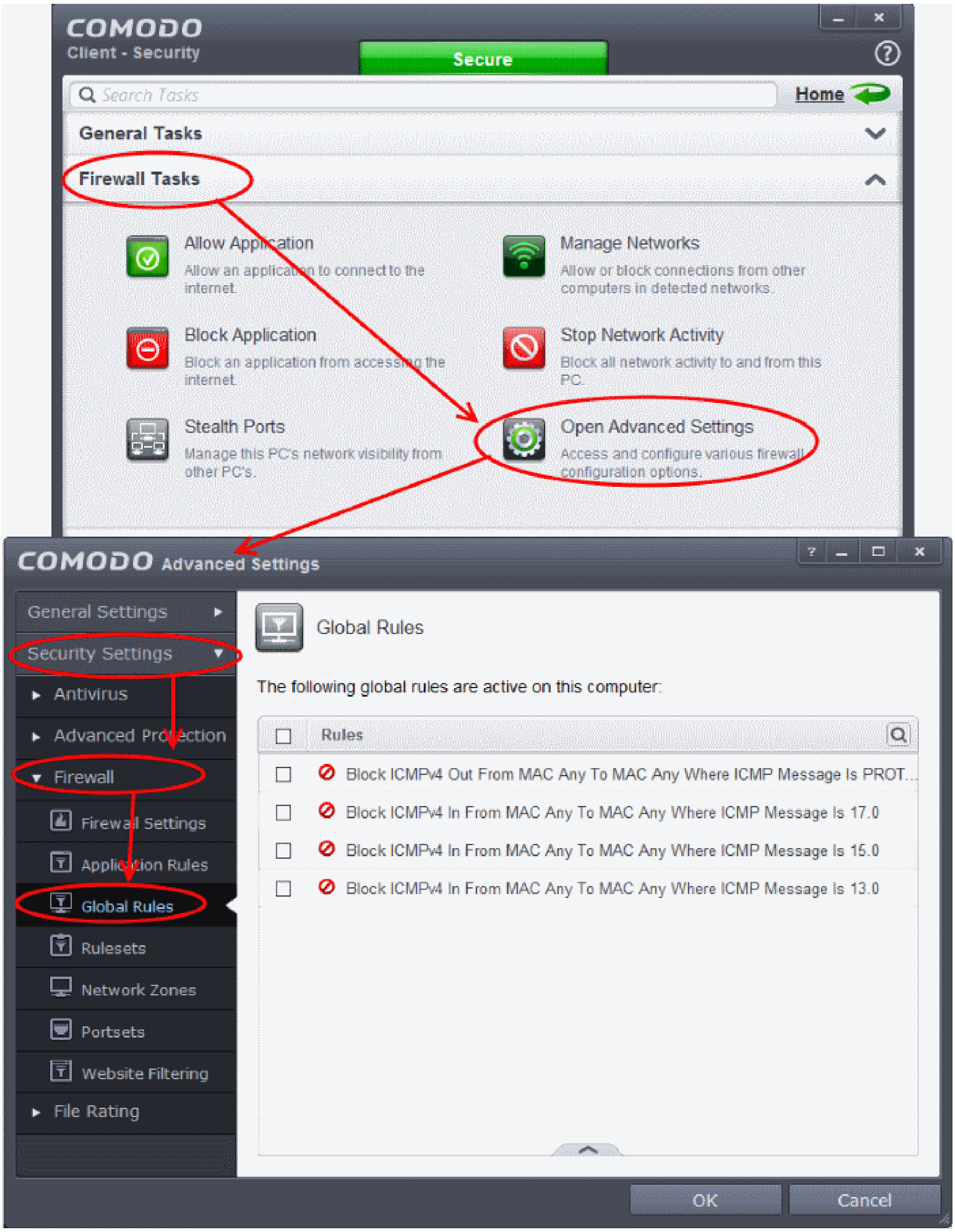
Example scenarios:

- In your network at home, you want your child's computer to connect to other computers at home but disable internet access for safety reasons
- In your corporate network, you want your employee's computers to connect to your local network machines but disable internet access for bandwidth reasons

To block the internet while allowing connections to an internal network you need to create a 'Global Rule' under 'Advanced Firewall Settings'. You should also password protect your configuration to prevent others from altering it.

To create a Global Rule

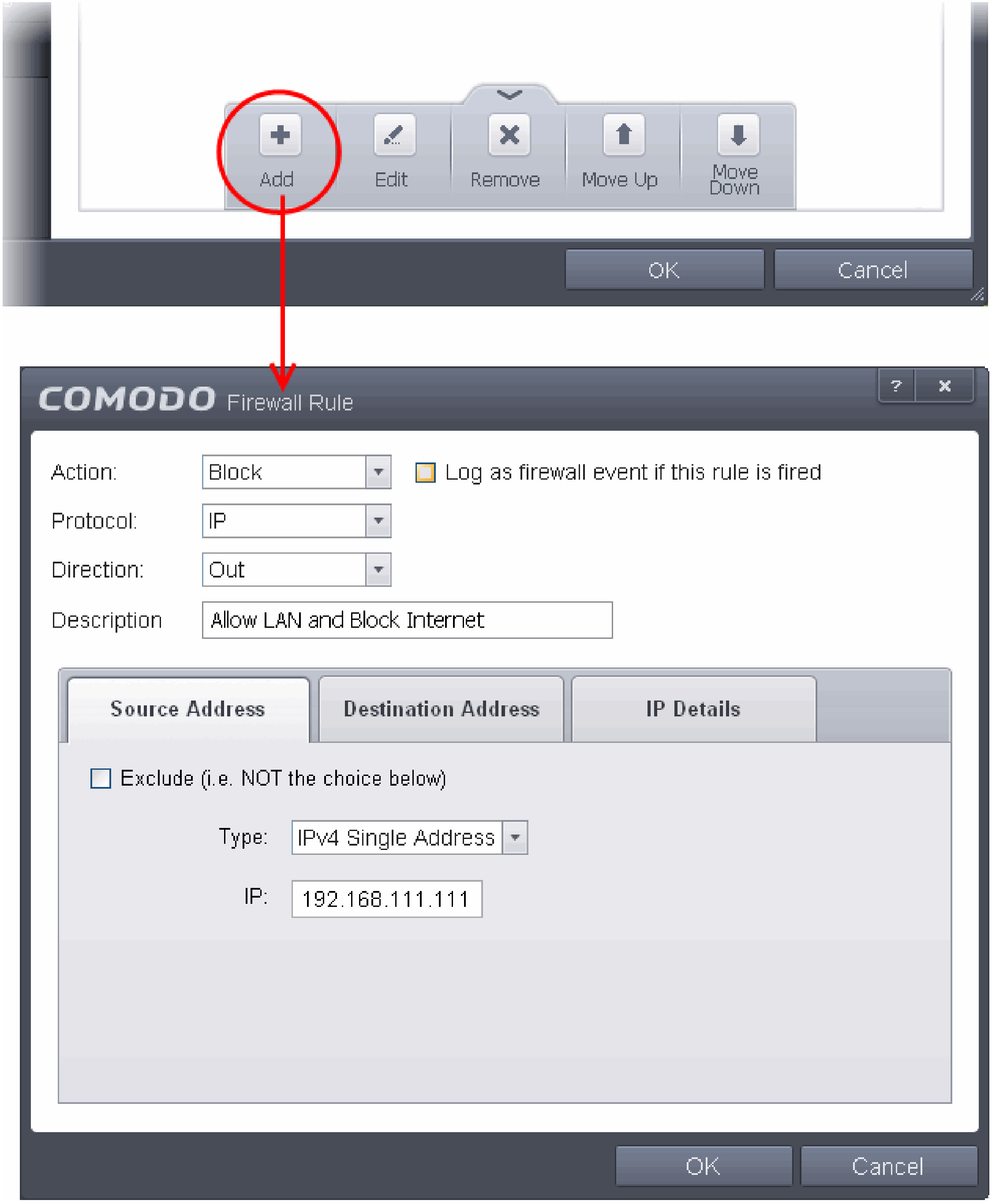
1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' then click 'Open Advanced Settings'.
3. Click 'Global Rules' under 'Firewall' on the left hand menu:



The following global rules are active on this computer:

□	Rules
□	⊘ Block ICMPv4 Out From MAC Any To MAC Any Where ICMP Message Is PROT...
□	⊘ 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

4. Click the handle from the bottom and choose 'Add' from the options. The Firewall Rule interface will open.



Action: Block

□ Log as firewall event if this rule is fired

Protocol: IP

Direction: Out

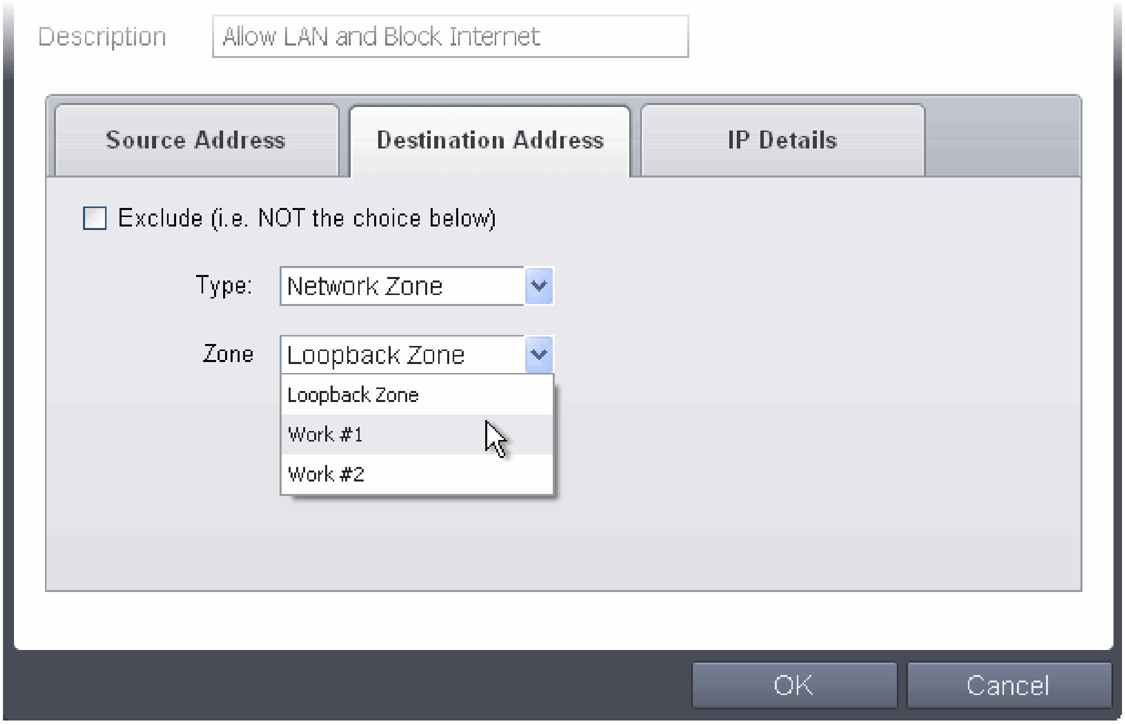
Description: Allow LAN and Block Internet

□ Exclude (i.e. NOT the choice below)

Type: IPv4 Single Address

IP: 192.168.111.111

5. Choose the following options from the drop-down menus:
   - Action = Block
   - Protocol = IP
   - Direction = Out
6. Enter a description for the new rule in the Description text box.
7. 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.
8. Click the 'Destination Address' tab, choose 'Network Zone' from the Type drop-down and choose your local area network from the 'Zone' drop-down.



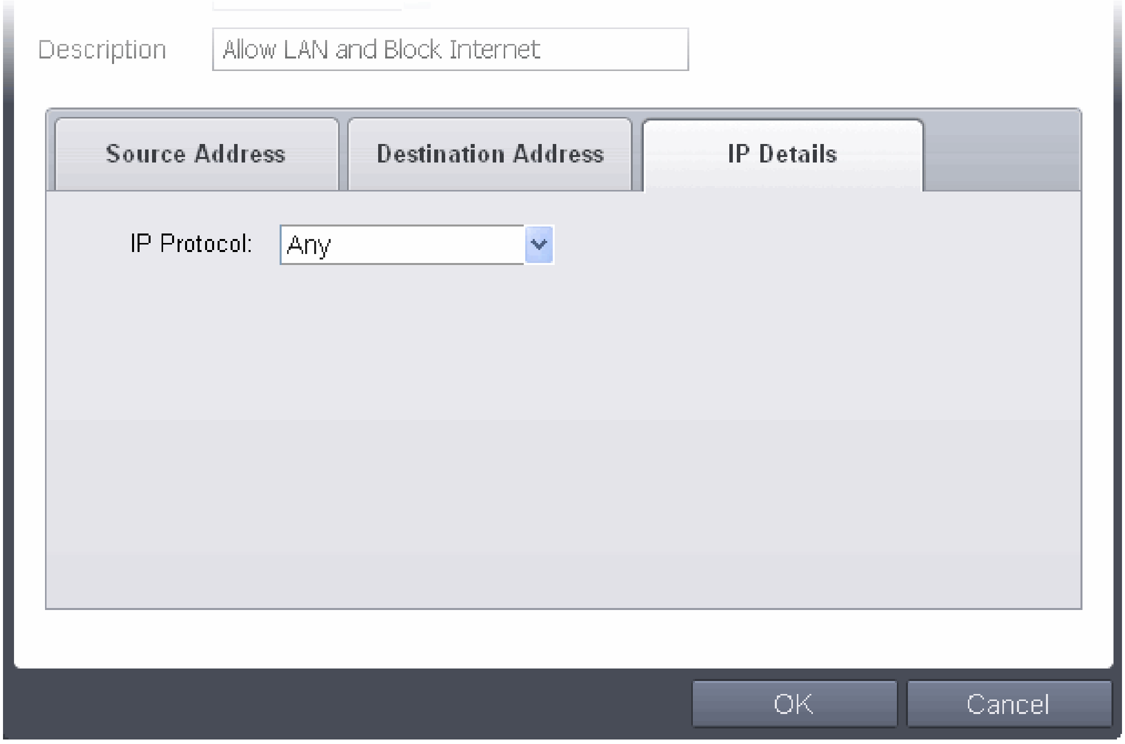
Description: Allow LAN and Block Internet

□ Exclude (i.e. NOT the choice below)

Type: Network Zone

Zone: Loopback Zone

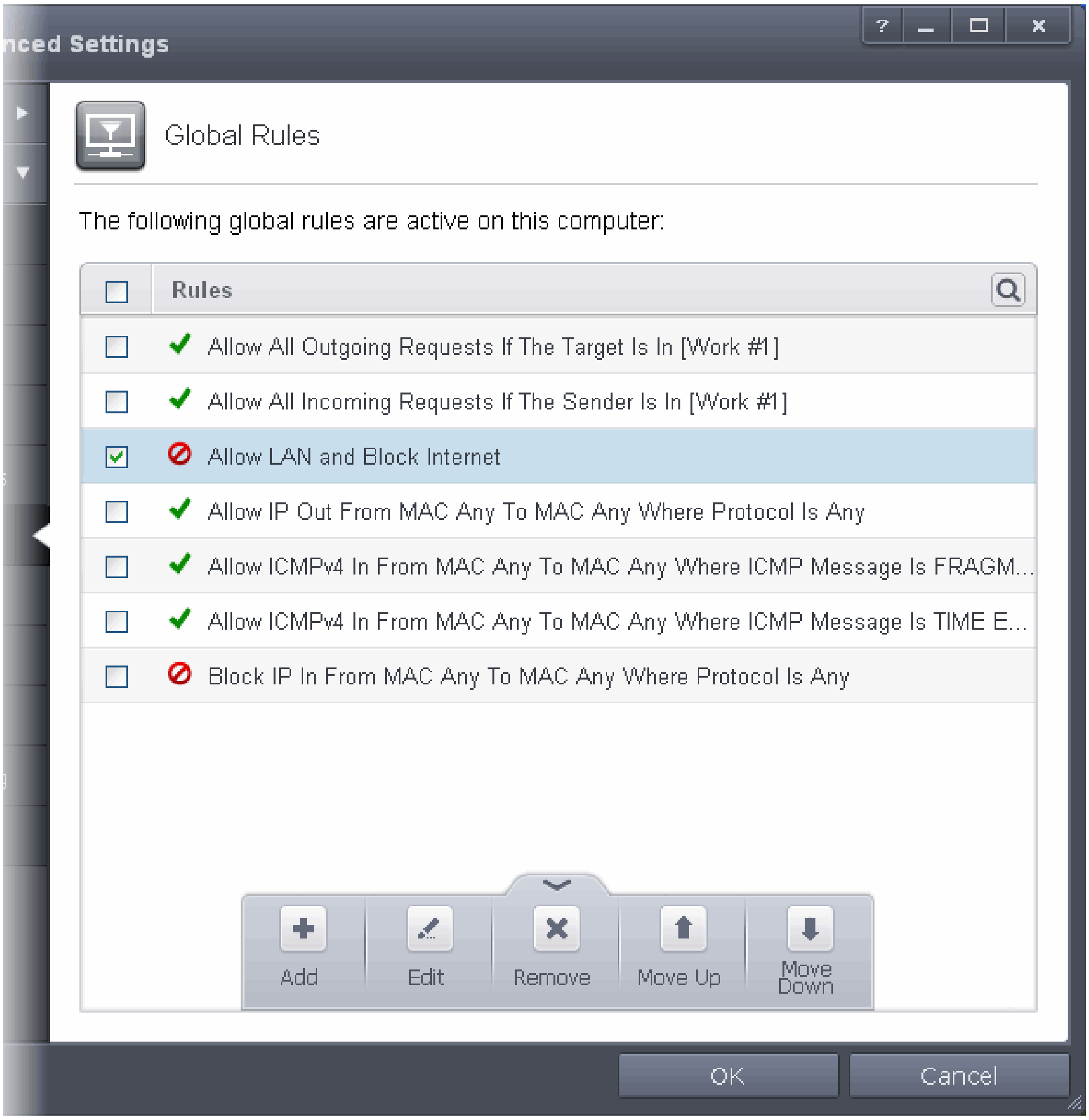
9. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.



Description: Allow LAN and Block Internet

IP Protocol: Any

10. Click 'OK'. The created policy will be added to the list of Global Rules.
11. Select the rule, click the handle from the bottom and click 'Move Up' repeatedly until the rule moves to the first position.



The following global rules are active on this computer:

□	Rules
□	✓ Allow All Outgoing Requests If The Target Is In [Work #1]
□	✓ Allow All Incoming Requests If The Sender Is In [Work #1]
☑	⊘ Allow LAN and Block Internet
□	✓ Allow IP Out From MAC Any To MAC Any Where Protocol Is Any
□	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is FRAGM...
□	✓ Allow ICMPv4 In From MAC Any To MAC Any Where ICMP Message Is TIME E...
□	⊘ Block IP In From MAC Any To MAC Any Where Protocol Is Any

12. Click 'OK' for your configuration to take effect.

Your Firewall is now configured to allow access to internal network but to block Internet access. Now you need to password protect this configuration to prevent others from changing it.

Block/Allow Websites Selectively to Users of Your Computer

Comodo Client Security allows you block or permit access to websites and website categories on a per-user basis.

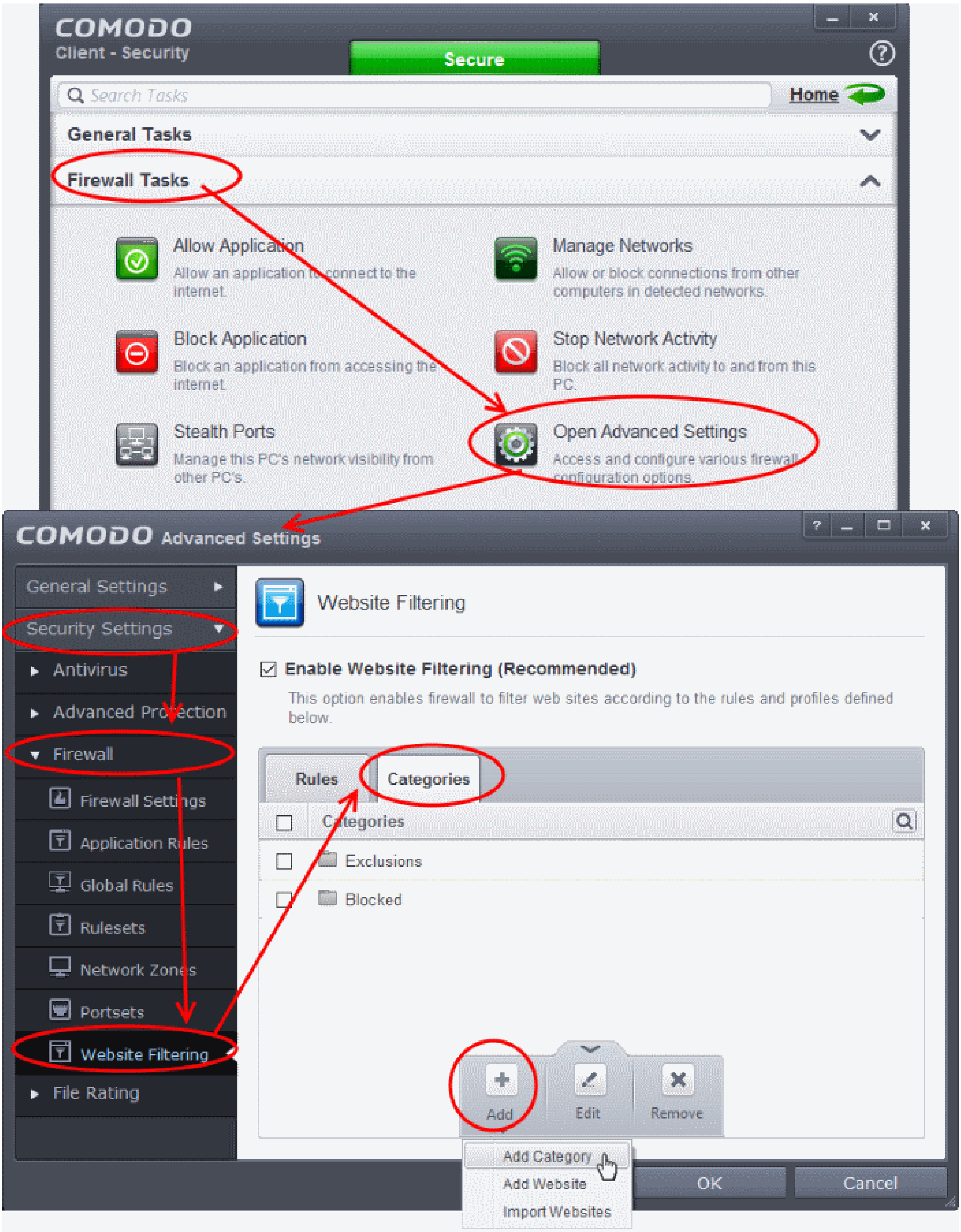
Configuring the website filtering involves two steps:

- Define Website Categories and add websites
- Create Firewall rules for allowing or blocking website categories to selected users

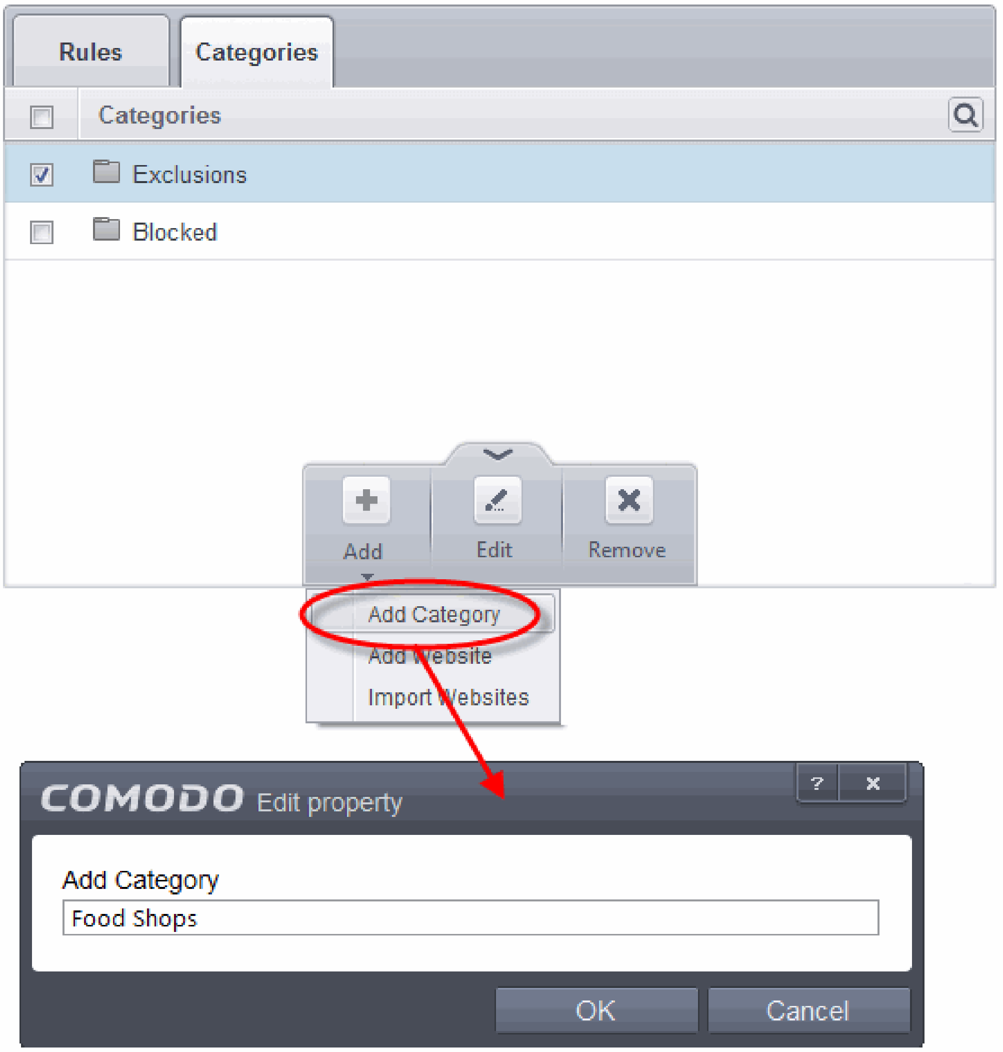
To define website categories

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen.
2. Open 'Firewall Tasks' then click 'Open Advanced Settings'.
3. Click 'Firewall' then 'Website Filtering' on the left hand menu.
4. Ensure that the 'Enable Website Filtering Filtering' checkbox is selected.

5. Click the 'Categories' tab from the 'Website Filtering' interface.



6. Click the handle at the bottom of the 'Categories' pane then click 'Add' and choose 'Add Category'. The 'Edit Property' dialog will open.

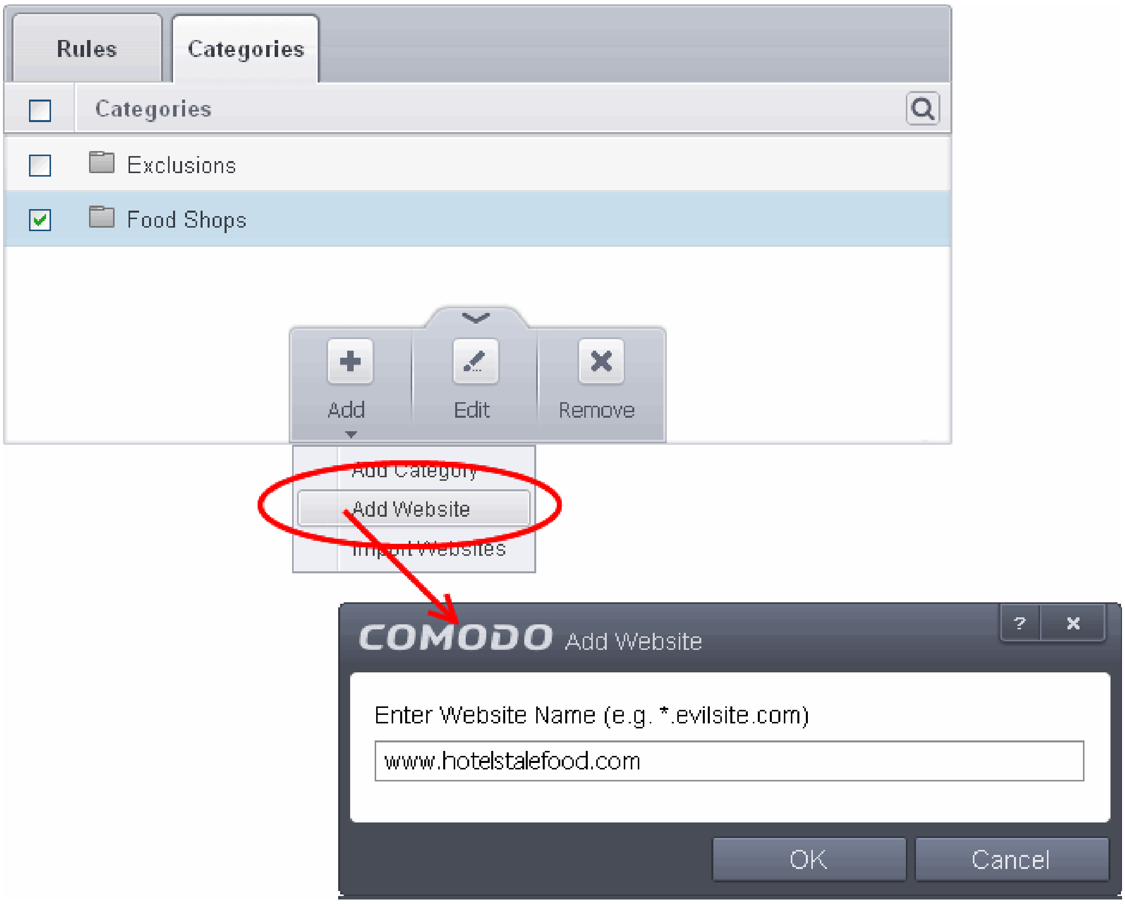


Add Category

Food Shops

7. Enter a name for the category and click OK. The new category will be created and added under the 'Categories' tab.

8. Select the category, click the handle at the bottom of the 'Categories' pane, click 'Add' then choose 'Add Website' from the drop-down menu. The 'Add Website' dialog will open:



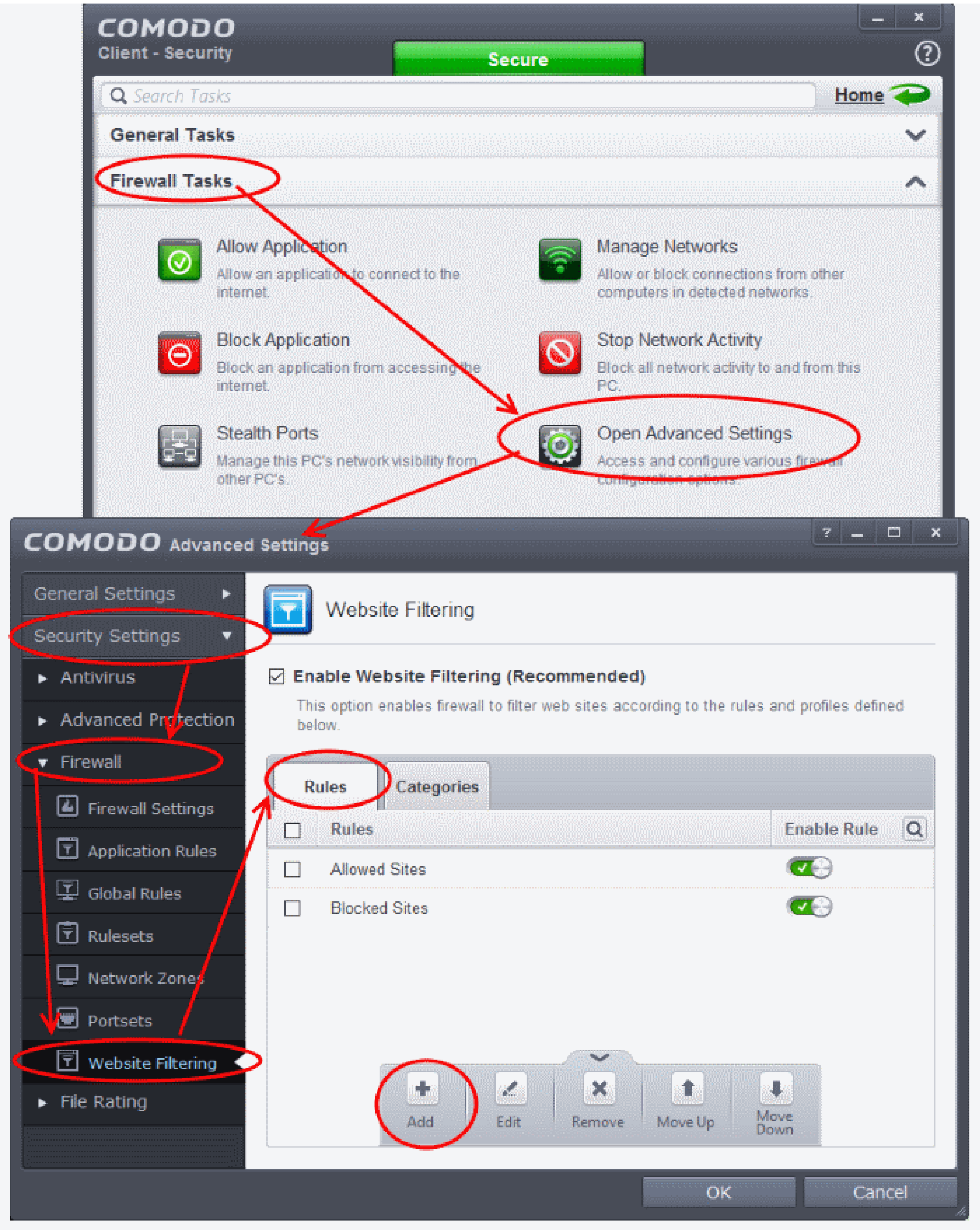
9. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
   - To add a specific website/webpage, enter the full URL of the website/webpage
   - To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
   - To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, pizza* will cover 'pizzahut.com', pizzacorner.com, and so on.
   - To include all the websites with URLs that contain a specific string, add the wildcard character before and after the string. For example, *pizza* will cover hotpizza.com, spicypizza.com and so on.

The website(s) will be added to the category.

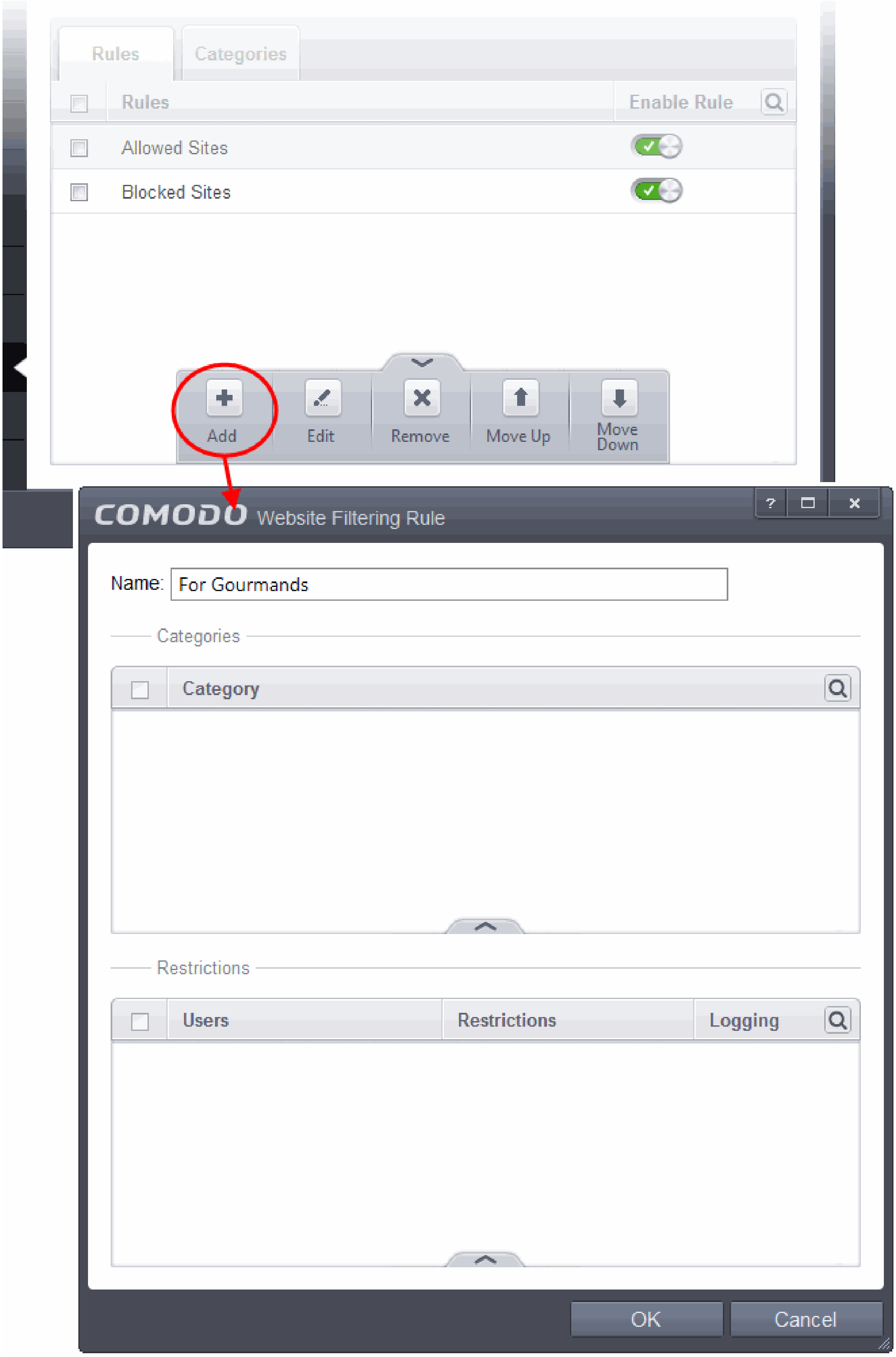
10. Repeat the process to add more websites.
11. Click 'OK' in the 'Advanced Settings' interface to save your settings

To create rules for selectively blocking or allowing websites to users

1. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
2. Click 'Website Filtering' under Firewall from the left hand side pane.
3. Click 'Rules' tab from the 'Website Filtering' interface.
4. Click the handle at the bottom of the Rules interface and select 'Add':

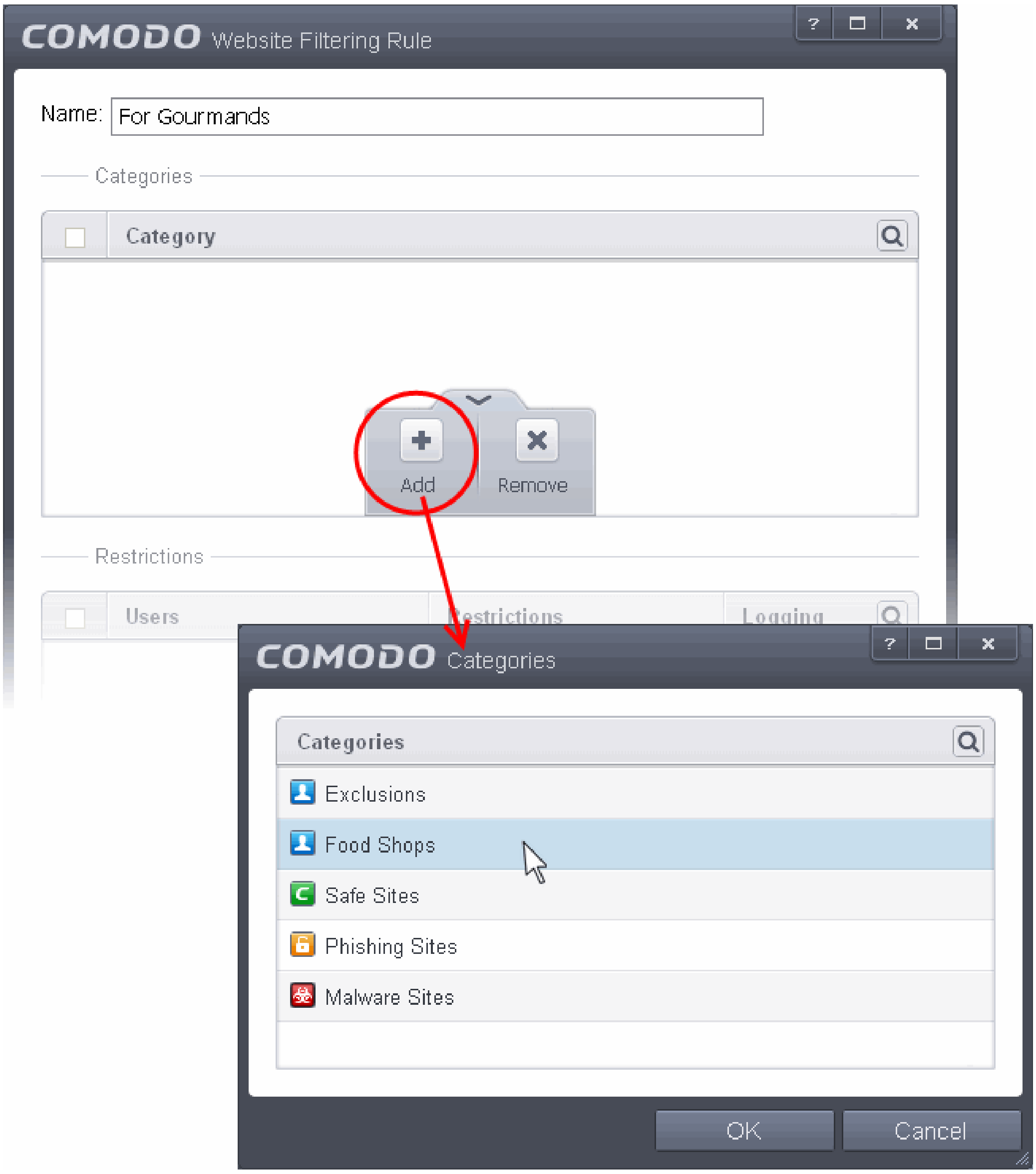


5. Enter a name for your new filter in the 'Website Filtering Rule' dialog.



Name: For Gourmands

6. Select the categories that should be added to the filter:
   - Click the handle at the bottom of the 'Category' pane and choose 'Add'.



Website Filtering Rule

Name: For Gourmands

Categories

Categories
Exclusions
Food Shops
Safe Sites
Phishing Sites
Malware Sites

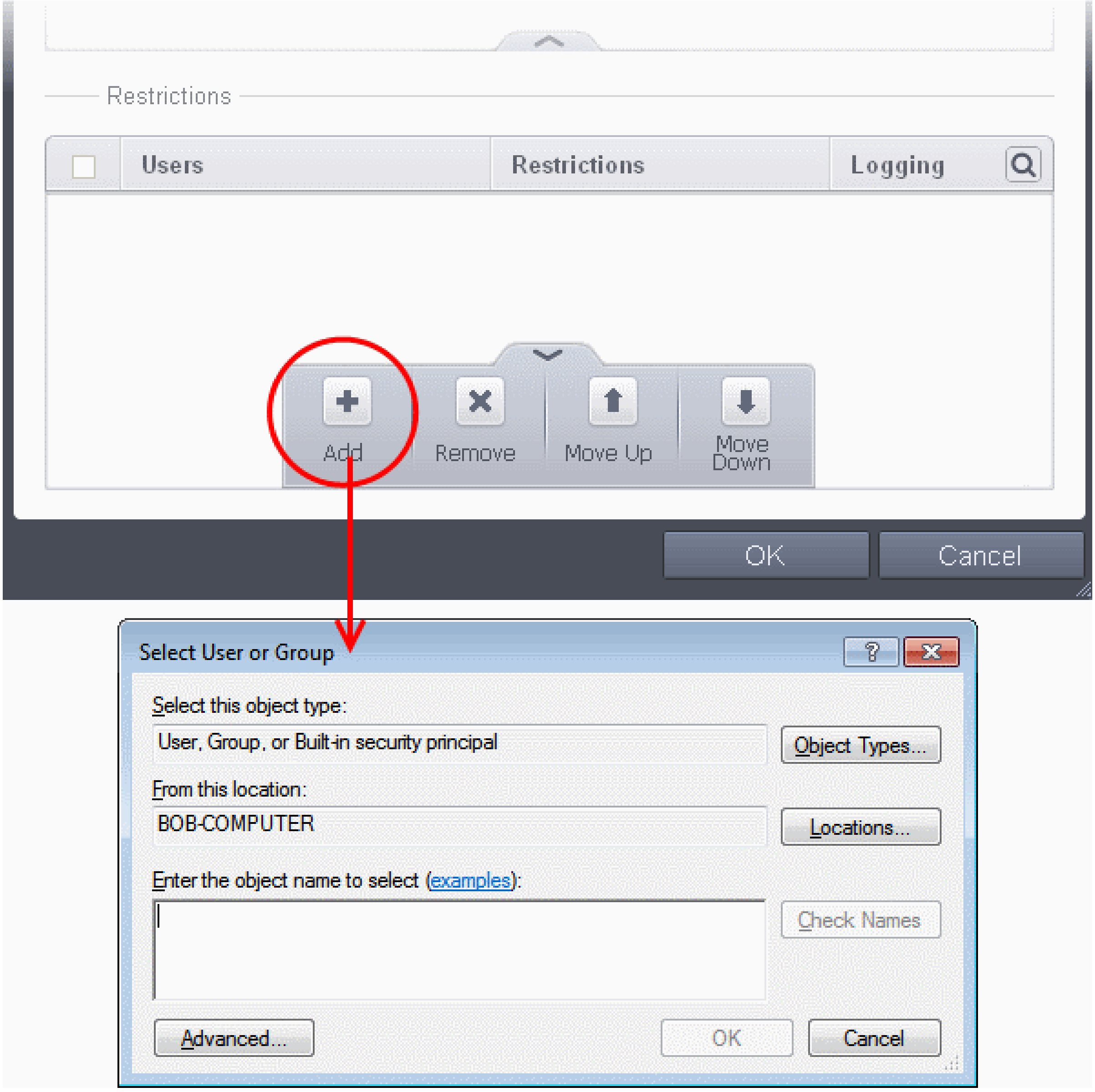
- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Comodo Safe Sites** - Websites that are considered safe according to global whitelist
- **Comodo Phishing Sites** - Websites that lead to phishing websites, as per dynamically updated Comodo Blacklist
- **Comodo Malware Sites** - Websites that may inject malware into your system, as per dynamically updated Comodo Blacklist

For more details on creating and modifying user specified categories, Refer to the section **Defining or Modifying Website Categories**

7. Add Users or User Groups to whom the rule should be applied:
   - Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:

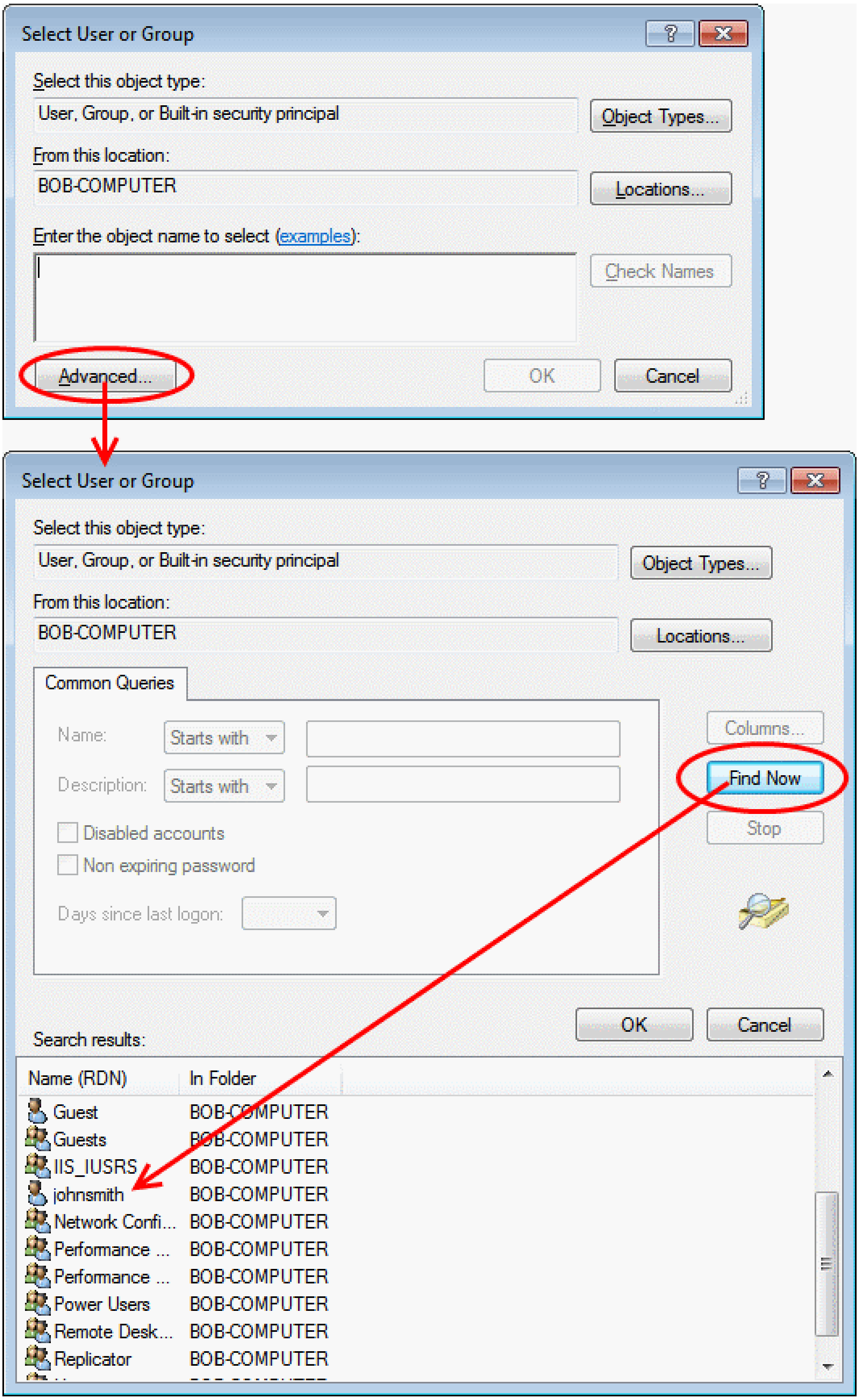


Select this object type:
User, Group, or Built-in security principal

From this location:
BOB-COMPUTER

Enter the object name to select (examples):

- Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format or @. Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



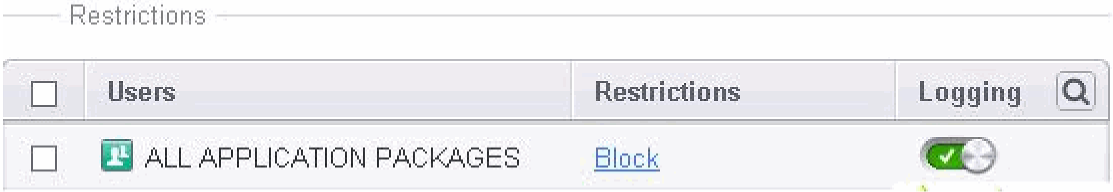
Select this object type: User, Group, or Built-in security principal

From this location: BOB-COMPUTER

Search results:

Name (RDN)	In Folder
Guest	BOB-COMPUTER
Guests	BOB-COMPUTER
IIS_IUSRS	BOB-COMPUTER
johnsmith	BOB-COMPUTER
Network Confi...	BOB-COMPUTER
Performance ...	BOB-COMPUTER
Performance ...	BOB-COMPUTER
Power Users	BOB-COMPUTER
Remote Desk...	BOB-COMPUTER
Replicator	BOB-COMPUTER

Important Note to IE 11 users: If you are using Internet Explorer 11 and above, it is mandatory to add the user group 'ALL APPLICATION PACKAGES' to the Restrictions list in addition to the added users for each rule you create.



Restrictions

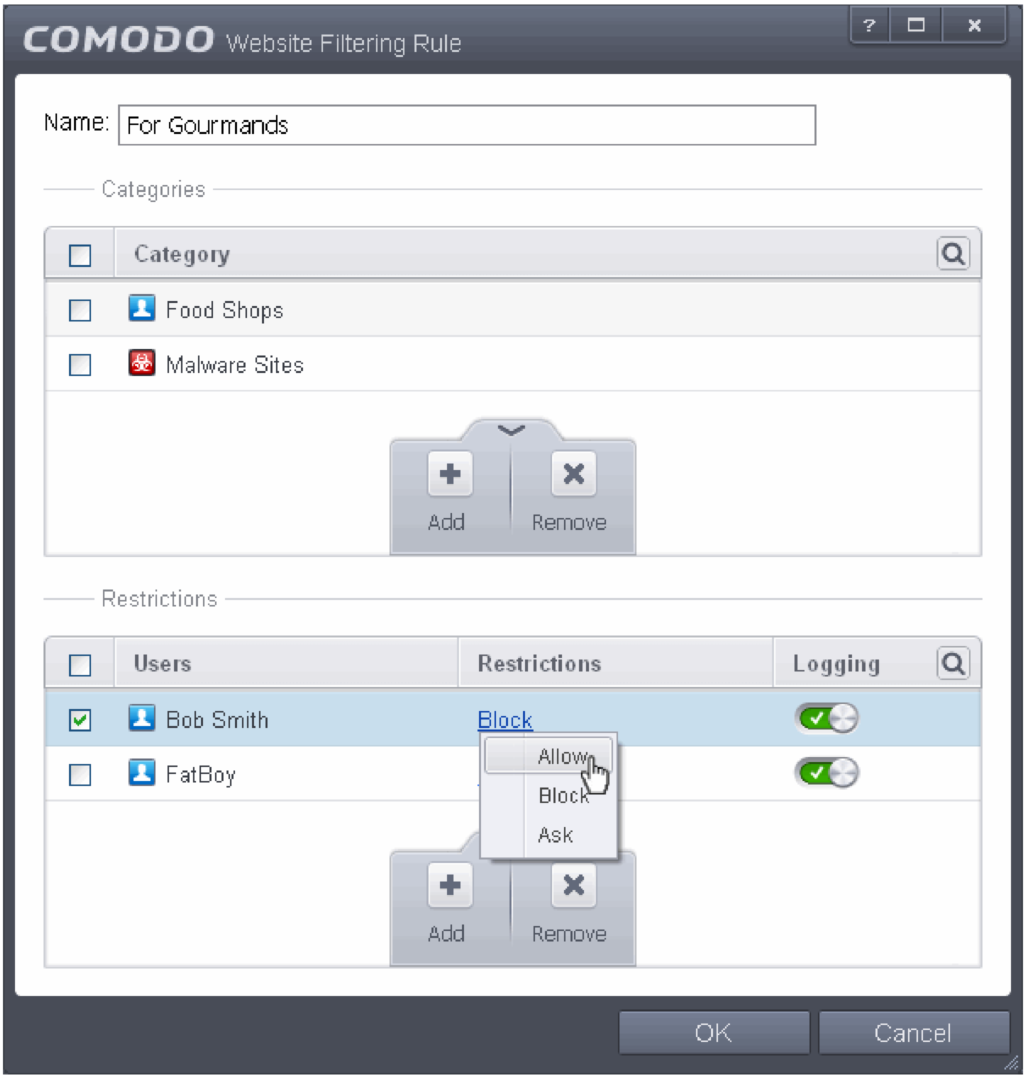
□	Users	Restrictions	Logging
□	ALL APPLICATION PACKAGES	Block	✓

The rule will take full effect only after adding this user group.

To add 'ALL APPLICATION PACKAGES' to the restrictions list

- Click 'Advanced' in the 'Select User or Group' dialog
- Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom
- Click 'OK'

- After adding target users or groups, you next need to specify whether those users should be allowed or blocked from viewing the websites in the category or they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:



COMODO Website Filtering Rule

Name: For Gourmands

Categories

□	Category
□	Food Shops
□	Malware Sites

Restrictions

□	Users	Restrictions	Logging
☑	Bob Smith	Block	✓
□	FatBoy		✓

  - **Allow-** The websites in the categories can be accessed by the user.
  - **Block -** The websites in the categories cannot be accessed by the user.
  - **Ask-** An alert will be displayed in the browser if the user tries to access any of the websites in the category. The user can decide whether or not to continue.
- Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.

8. Click 'OK' to save your new rule. The rule will become effective immediately.

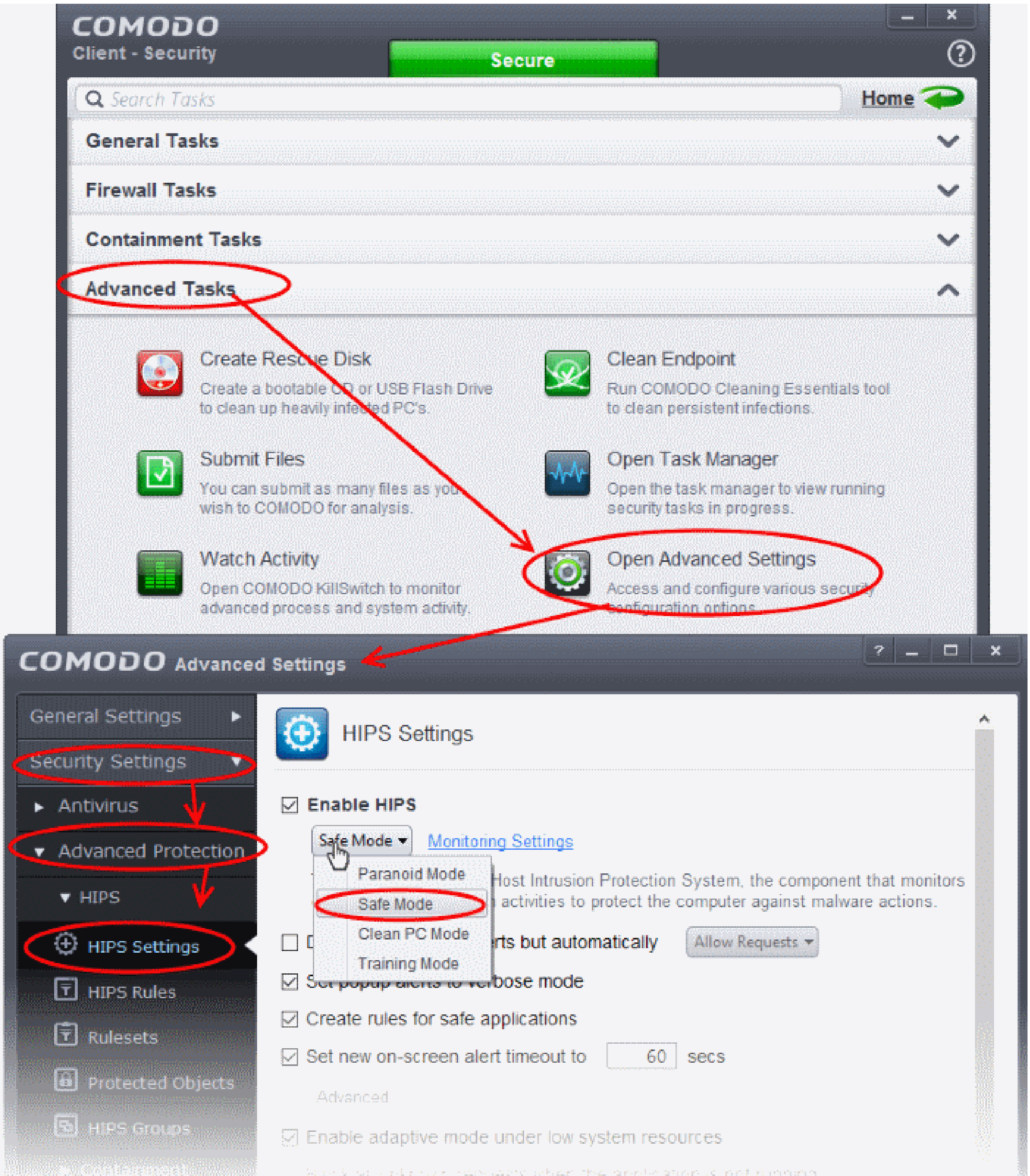
You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Setting up HIPS for Maximum Security and Usability

This page explains how to configure the Host Intrusion Prevention System (HIPS) to provide maximum security from malware and unsafe processes.

To configure HIPS

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' then click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Advanced Protection' > 'HIPS' > 'HIPS Settings' on the left hand pane


COMODO Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Containment Tasks
Advanced Tasks
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
Open Task Manager
Open the task manager to view running security tasks in progress.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
Open Advanced Settings
Access and configure various security configuration options.
COMODO Advanced Settings
General Settings
Security Settings
Antivirus
Advanced Protection
HIPS
HIPS Settings
HIPS Rules
Rulesets
Protected Objects
HIPS Groups
Containment
HIPS Settings
Monitoring Settings
Paranoid Mode
Safe Mode
Clean PC Mode
Training Mode
Host Intrusion Protection System, the component that monitors activities to protect the computer against malware actions.
Allow Requests
Advanced

☑ Enable HIPS

Safe Mode

□ D...rts but automatically Allow Requests

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

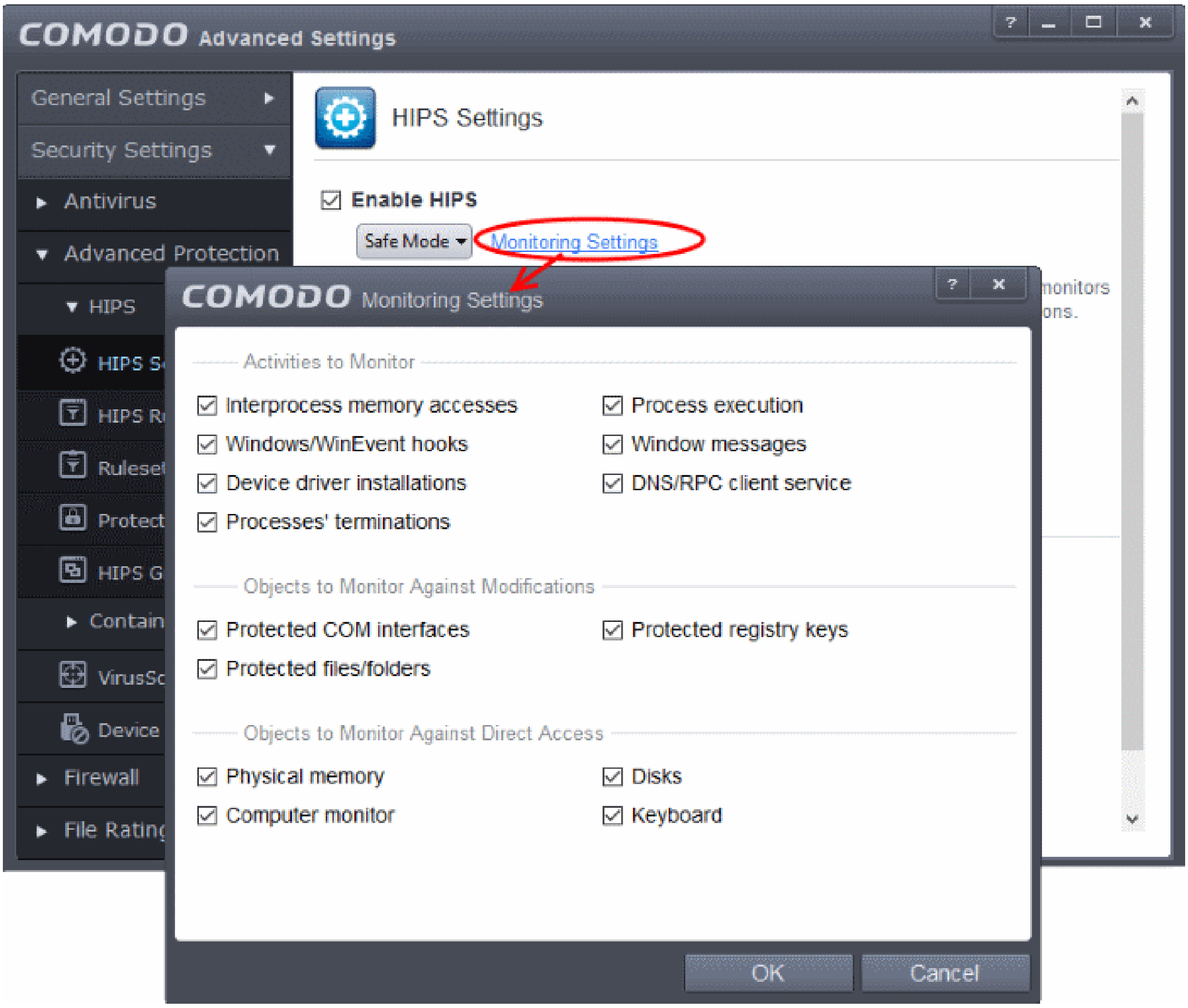
☑ Enable adaptive mode under low system resources

4. Check the 'Enable HIPS' checkbox

5. Choose 'Safe Mode' from the drop-down. Refer to **HIPS Behavior Settings** if you want more details about the various security levels on offer here.

Monitoring Settings

6. Click '[Monitoring Settings](#)' from the HIPS Settings interface



☑ Enable HIPS

COMODO Monitoring Settings

Activities to Monitor

☑ Interprocess memory accesses

☑ Process execution

☑ Windows/WinEvent hooks

☑ Window messages

☑ Device driver installations

☑ DNS/RPC client service

☑ Processes' terminations

Objects to Monitor Against Modifications

☑ Protected COM interfaces

☑ Protected registry keys

☑ Protected files/folders

Objects to Monitor Against Direct Access

☑ Physical memory

☑ Disks

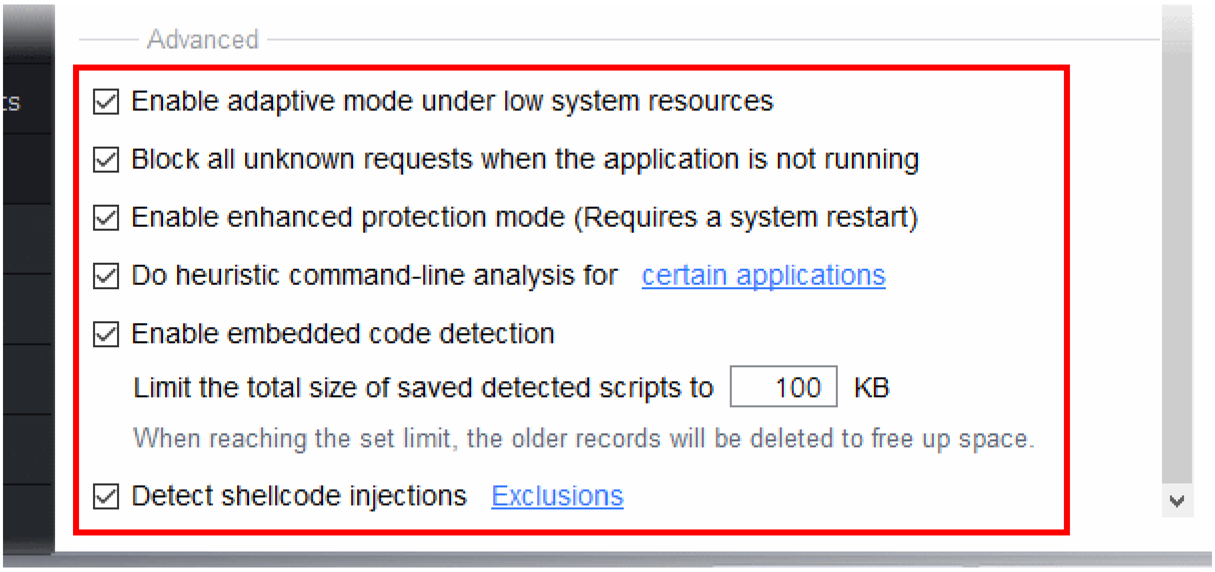
☑ Computer monitor

☑ Keyboard

7. Make sure that all check boxes are selected and click 'OK'

Advanced Settings

8. Enable the following settings under Advanced in the 'HIPS Settings' interface



☑ Enable adaptive mode under low system resources

☑ Block all unknown requests when the application is not running

☑ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Enable embedded code detection

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Detect shellcode injections Exclusions

- Optional – Enable '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.
- If you are using a 64-bit system it is important to select 'Enable enhanced protection mode (requires a system restart)'. Enabling this mode will activate additional intrusion prevention techniques to counter sophisticated malware that tries to exploit limitations in 64 bit Windows systems.

Click here for more details on HIPS Behavior Settings

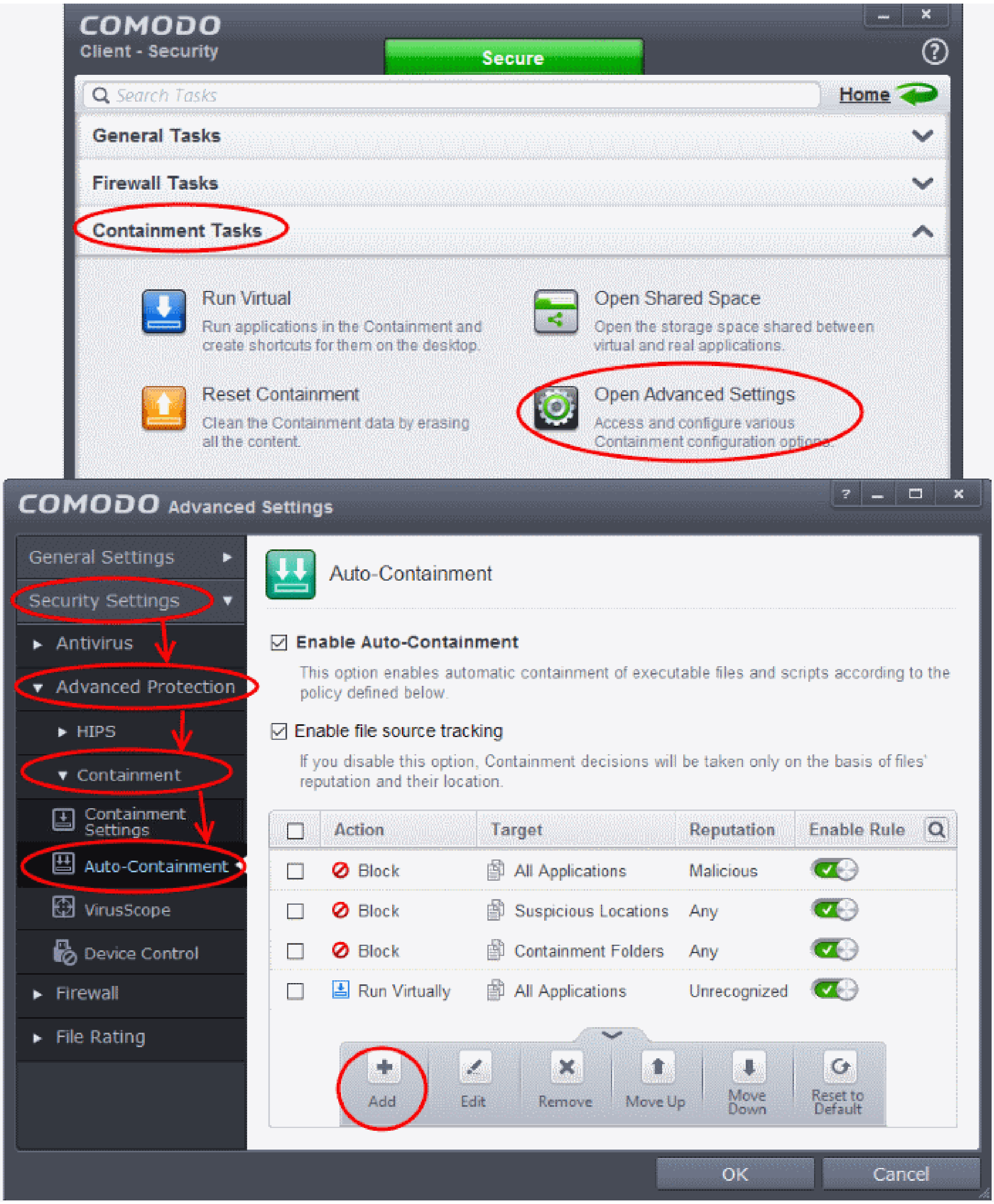
Create Rules for Auto-Containing Applications

You can define rules for programs that should be run in the contained environment. A contained application has much less opportunity to damage your computer because it is run isolated from your operating system and your files.

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 requirement is met by the default rules. Refer to the section Configuring Rules for Auto-Containment for more details.

To create auto-containment rules

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Containment Tasks' then click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Advanced Protection' > 'Containment' > 'Auto-Containment' on the left hand menu.
4. Click the handle at the bottom of the interface to open the option panel:



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

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

Reset Containment
Clean the Containment data by erasing all the content.

Open Advanced Settings
Access and configure various Containment configuration options.

Auto-Containment

☑ Enable Auto-Containment

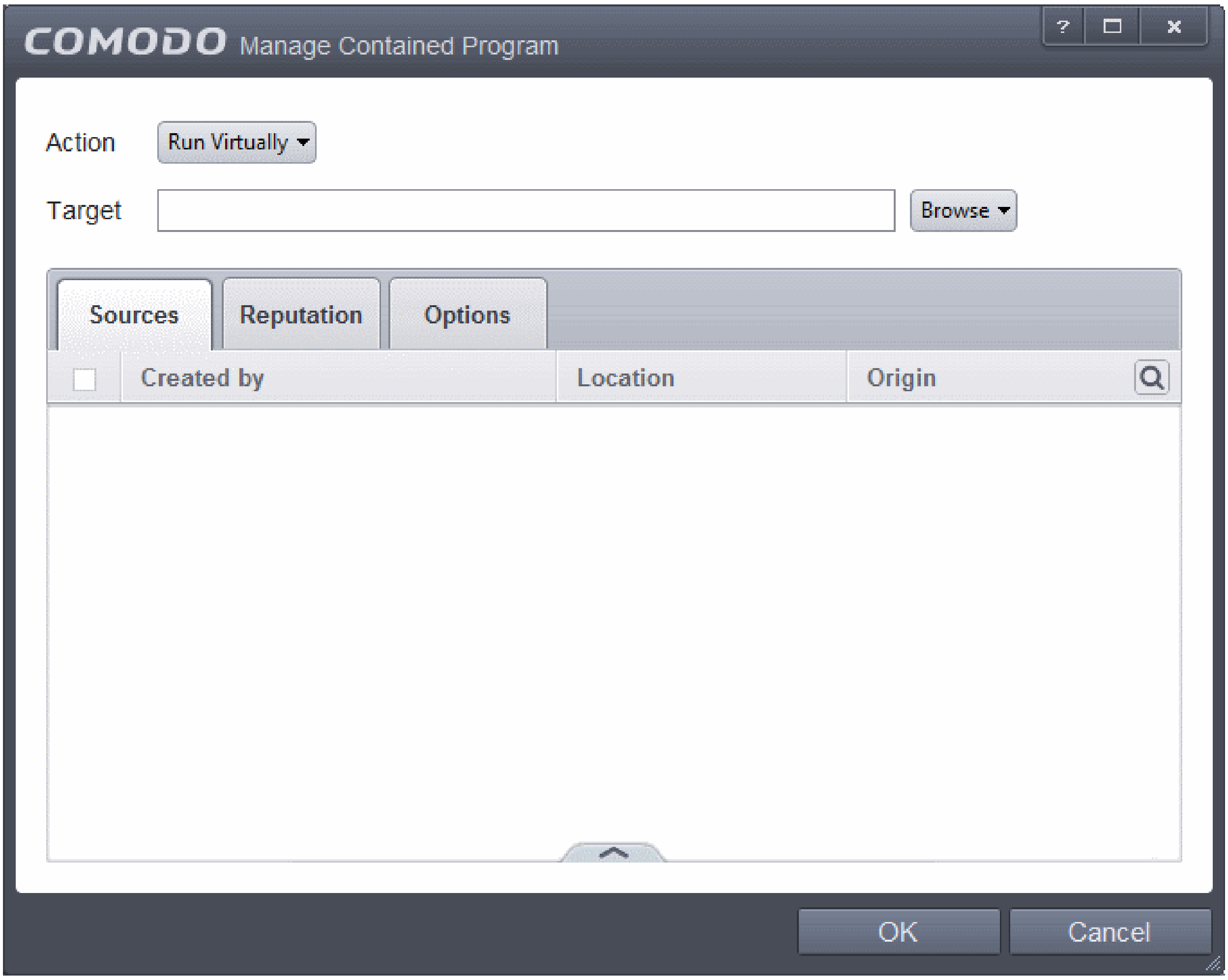
This option enables automatic containment of executable files and scripts according to the policy defined below.

☑ Enable file source tracking

If you disable this option, Containment decisions will be taken only on the basis of files' reputation and their location.

□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malicious	✓
□	Block	Suspicious Locations	Any	✓
□	Block	Containment Folders	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓

5. Click the 'Add' button

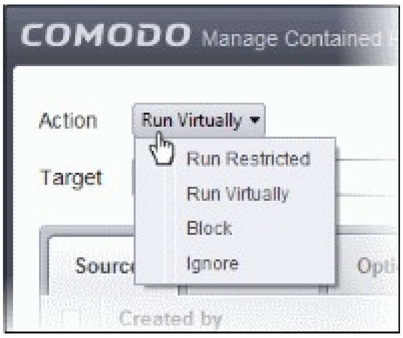


The 'Manage Contained Program' screen will appear:

- Step 1 – Select the Action
- Step 2 – Select the Target
- Step 3 – Select the Sources
- Step 4 – Select the File Reputation
- Step 5 – Select Options

Step 1 – Select the Action

The options in the 'Action' drop-down combined with the 'Set Restriction Level' setting in the 'Options' tab determine the privileges a contained application has to access other software and hardware resources on your computer.

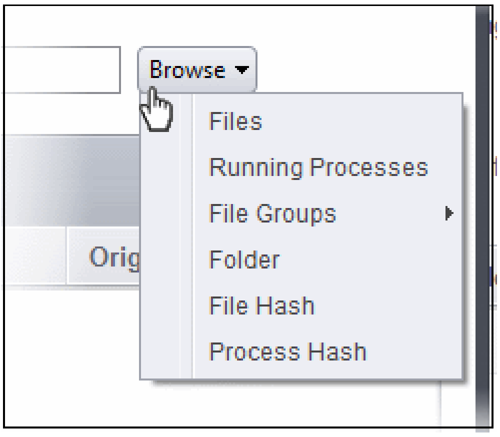


The options available are:

- **Run Virtually** - The application will be run in the container, 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 is allowed to run with all privileges.

Step 2 – Select the Target

The next step is to select the target to which the auto-containment rule should be applied. Click the 'Browse' button beside the 'Target' field.



You have six options available to add the target path:

- Files – Specify individual files as targets of the rule.
- Running Processes – Add any process that is currently running on your computer as a target of the rule.
- File Groups –Add predefined file groups as the rule target. For information about creating or modifying a predefined file group, refer to File Groups
- 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 a target based on its hash value

Click here to know more about adding each of the options.

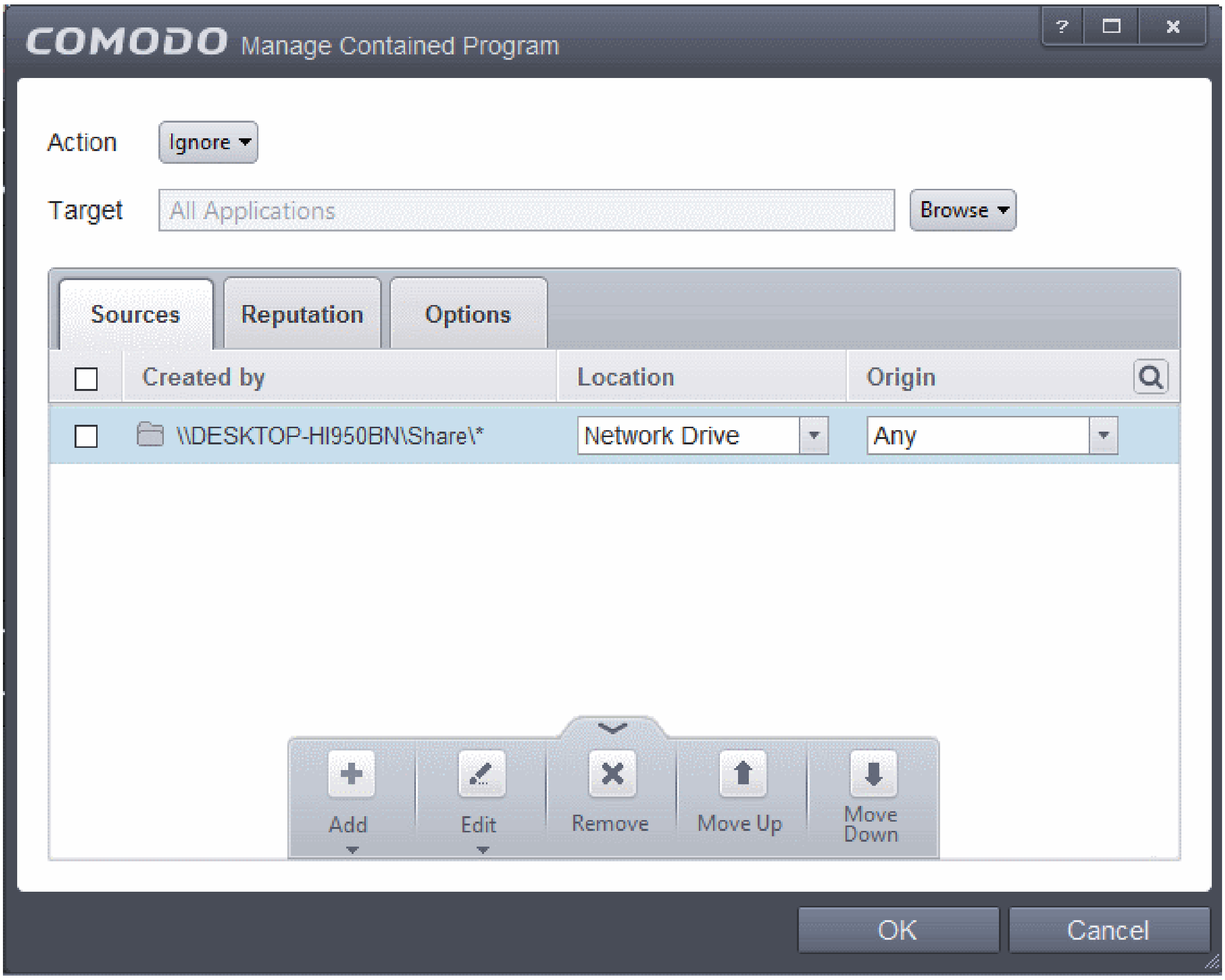
Step 3 – Select the Sources

If you want to include a number of items in a rule but want the rule to be applied only in certain conditions, then you can do so in this step. For example, if you want your target to be executables downloaded from the internet, then you would add 'All Applications' then apply a filter in 'Sources' tab. Another example is you want to exclude from containment any unrecognized files from your internal network share. You could create an ignore rule with 'All Applications' set as the target and specify your source as your intranet.

Please note that the 'Enable file source tracking' check box should be enabled in the 'Auto-Containment' screen for the source parameter to be taken account in the rule. If this is not enabled then the source parameter will be ignored and the rule will be applied based on the other parameters.

The following example describes how to add an 'Ignore' rule for Unrecognized files from a network source:

- In Step 1, select the action as Ignore
- In Step 2, select the Target as File Groups > All Applications
- In Step 3, click the 'Add' button and select 'Folder'. Navigate to the source folder on the network and click 'OK'.



Action: Ignore

Target: All Applications

□	Created by	Location	Origin
□	\\DESKTOP-HI950BN\Share\*	Network Drive	Any

The selected network source folder will be added under the 'Created by' column and the screen displays the options to specify the location and from where the files were downloaded.

- **Location** – Apply the rule to files found in one of the following locations:
  - Any
  - Local Drive
  - Removable Drive
  - Network Drive

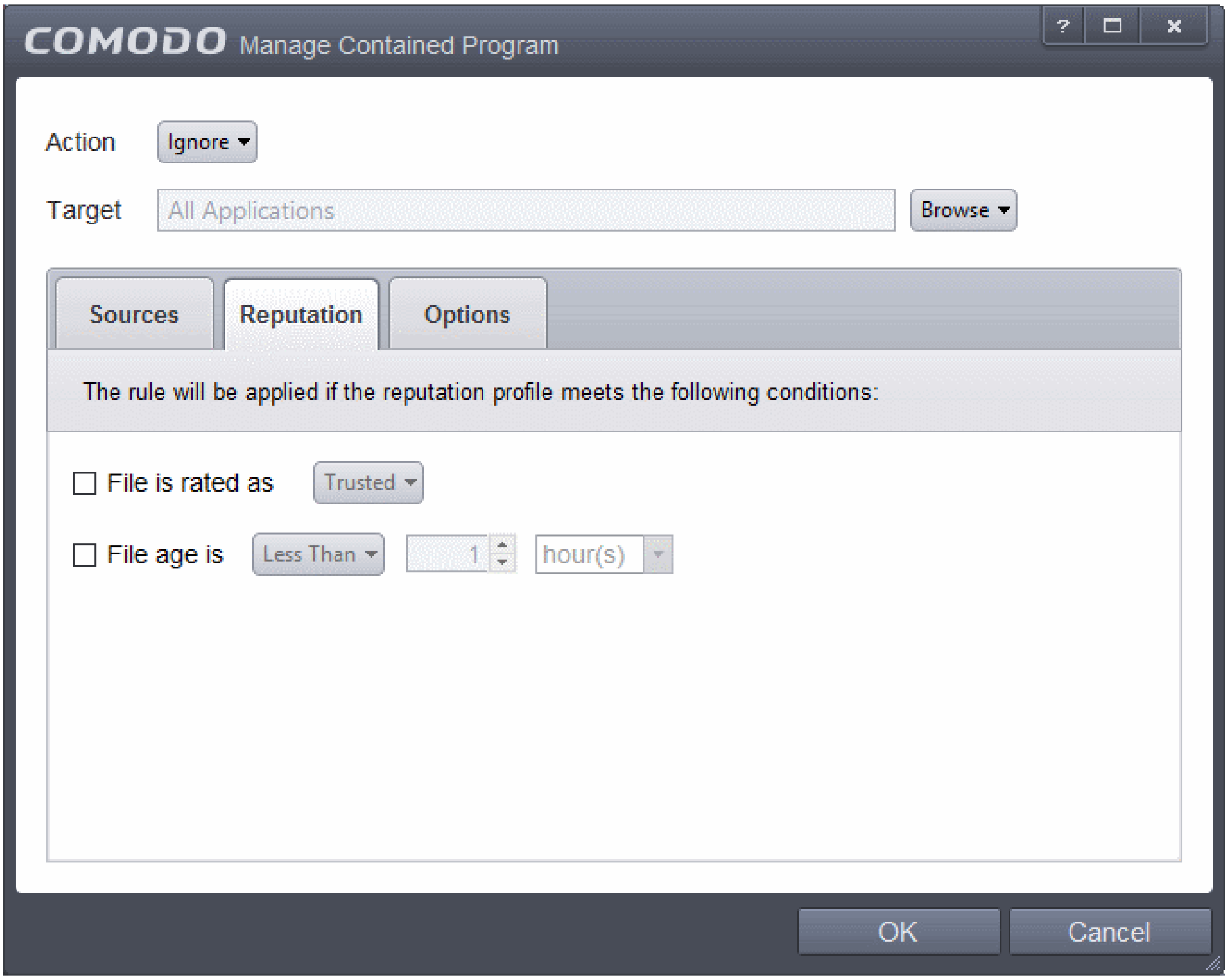
Since the source is located in a network, select Network Drive from the options.

- **Origin** – The options available are:
  - Any – The rule will apply to files that were downloaded to the source folder from both Internet and Intranet.
  - Internet – The rule will apply to files that were downloaded to the source folder from Internet only.
  - Intranet – The rule will apply to files that were downloaded to the source folder from Intranet only.

Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options in Step 4.

Step 4 – Select the File Reputation

- Click the Reputation tab in the 'Manage Contained Program' interface.



The rule will be applied if the reputation profile meets the following conditions:

□ File is rated as Trusted

□ File age is Less Than 1 hour(s)

By default, the file rating is not selected meaning the rating could be Any. The options available are:

- **Trusted** – Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by CCS. Refer to the sections File Rating Settings and File List for more information.
- **Unrecognized** – Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section 'File List' for more information.
- **Malware** – Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. Refer the section Unknown Files – The Scanning Process for more information.

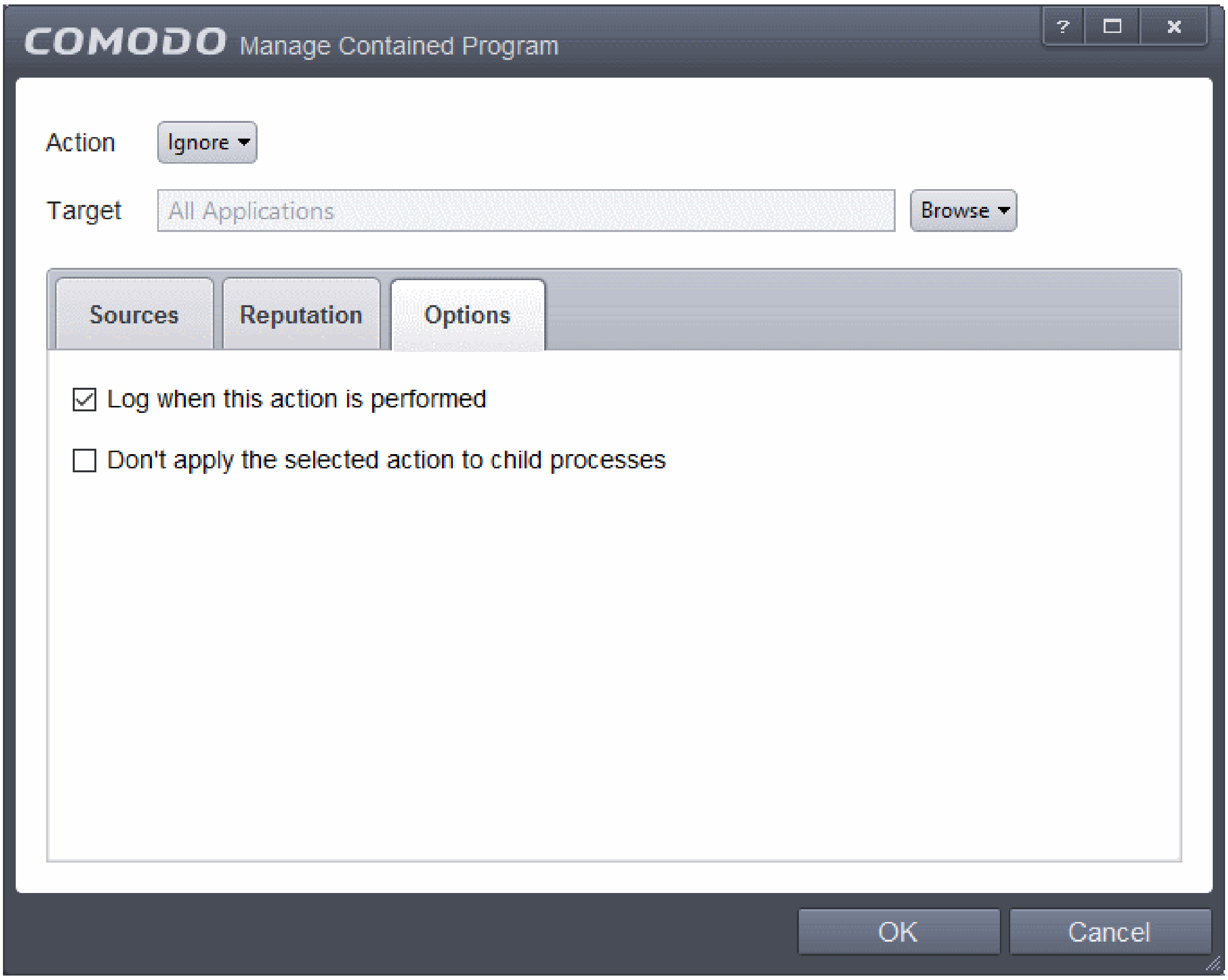
By default, file age is not selected, so the age could be Any. The options available are:

- **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)***

Select the category from the options. Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options.

Step 5 – Select the Options

- Click the Options tab in the 'Manage Contained Program' interface.



☑ Log when this action is performed

☐ Don't apply the selected action to child processes

By default, the 'Log when this action is performed' The options available for Ignore action are:

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** – Child processes are the processes initiated by the applications. For example, the process may launch another app or plugin. CCS treats all child processes as individual processes and forces them to run as per their file rating and the containment rules.
  - This option is disabled by default, so the ignore rule will usually be applied to all child process of the target application(s).
  - If this option is enabled, then the Ignore rule will be applied only to the target application. All child processes will be checked individually and containment rules applied as per the child's file rating.
  - The 'Don't apply to child processes' option is available only for the 'Ignore' action. For 'Run Restricted' and 'Run Virtually', the following options are available:
- **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.

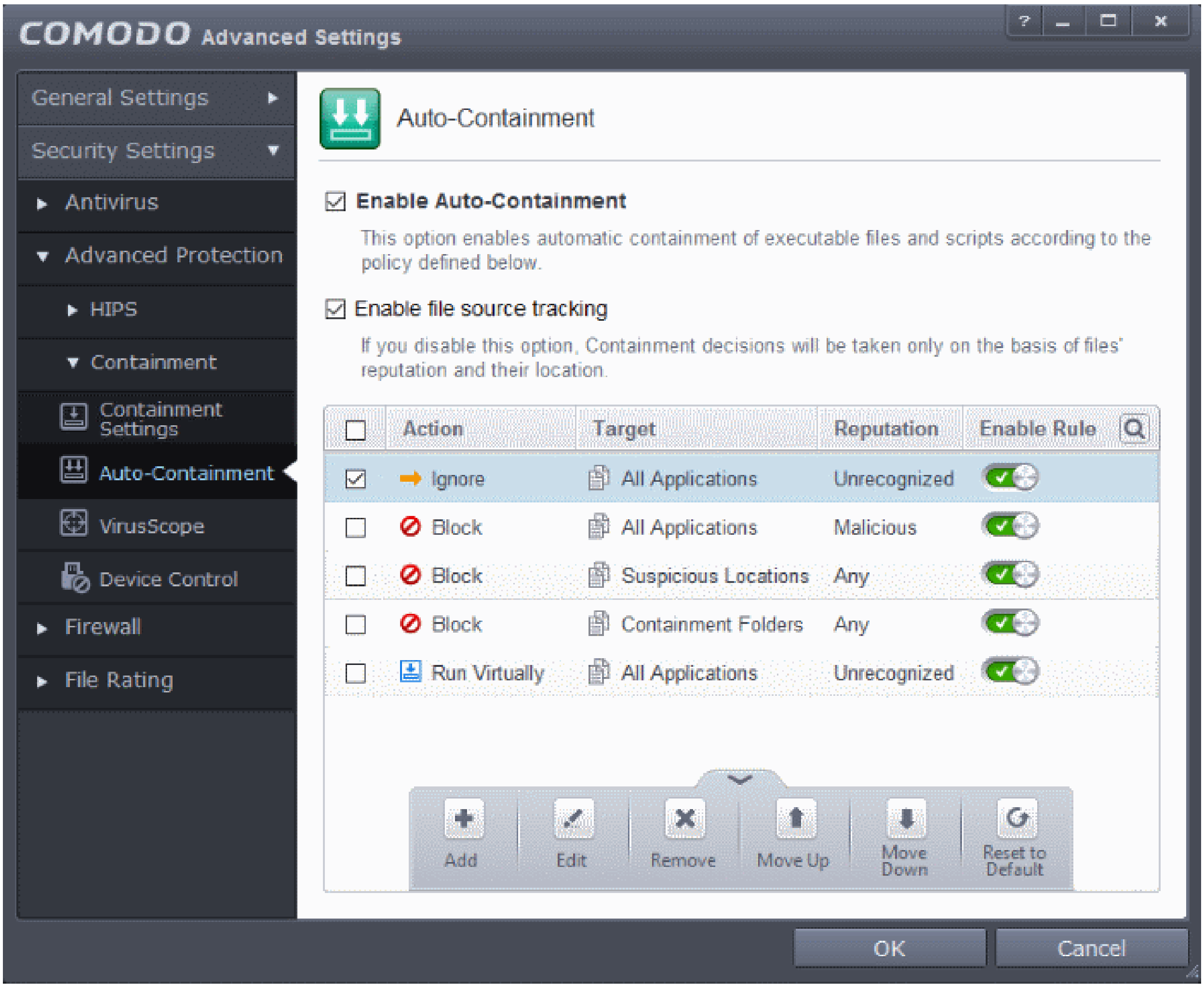
  - **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
  - **Untrusted -** 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. Refer to the section Manage Quarantined Items for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



Auto-Containment

☑ Enable Auto-Containment

This option enables automatic containment of executable files and scripts according to the policy defined below.

☑ Enable file source tracking

If you disable this option, Containment decisions will be taken only on the basis of files' reputation and their location.

□	Action	Target	Reputation	Enable Rule
☑	Ignore	All Applications	Unrecognized	✓
□	Block	All Applications	Malicious	✓
□	Block	Suspicious Locations	Any	✓
□	Block	Containment Folders	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓

That's it. You have created an Ignore auto-containment rule for unrecognized files with a Network drive as source.

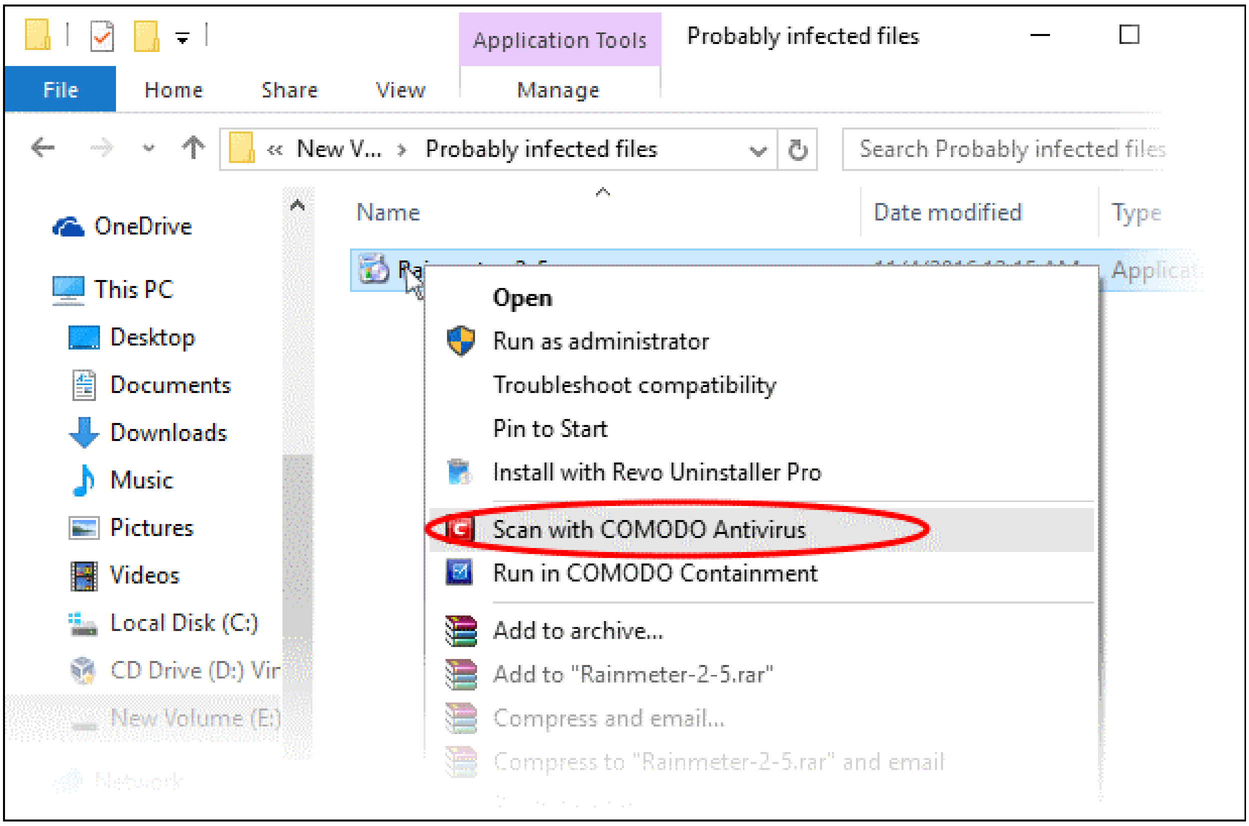
Running an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders files etc. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives, digital cameras - even your iPod and mobile phones too!!! This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from the Internet.

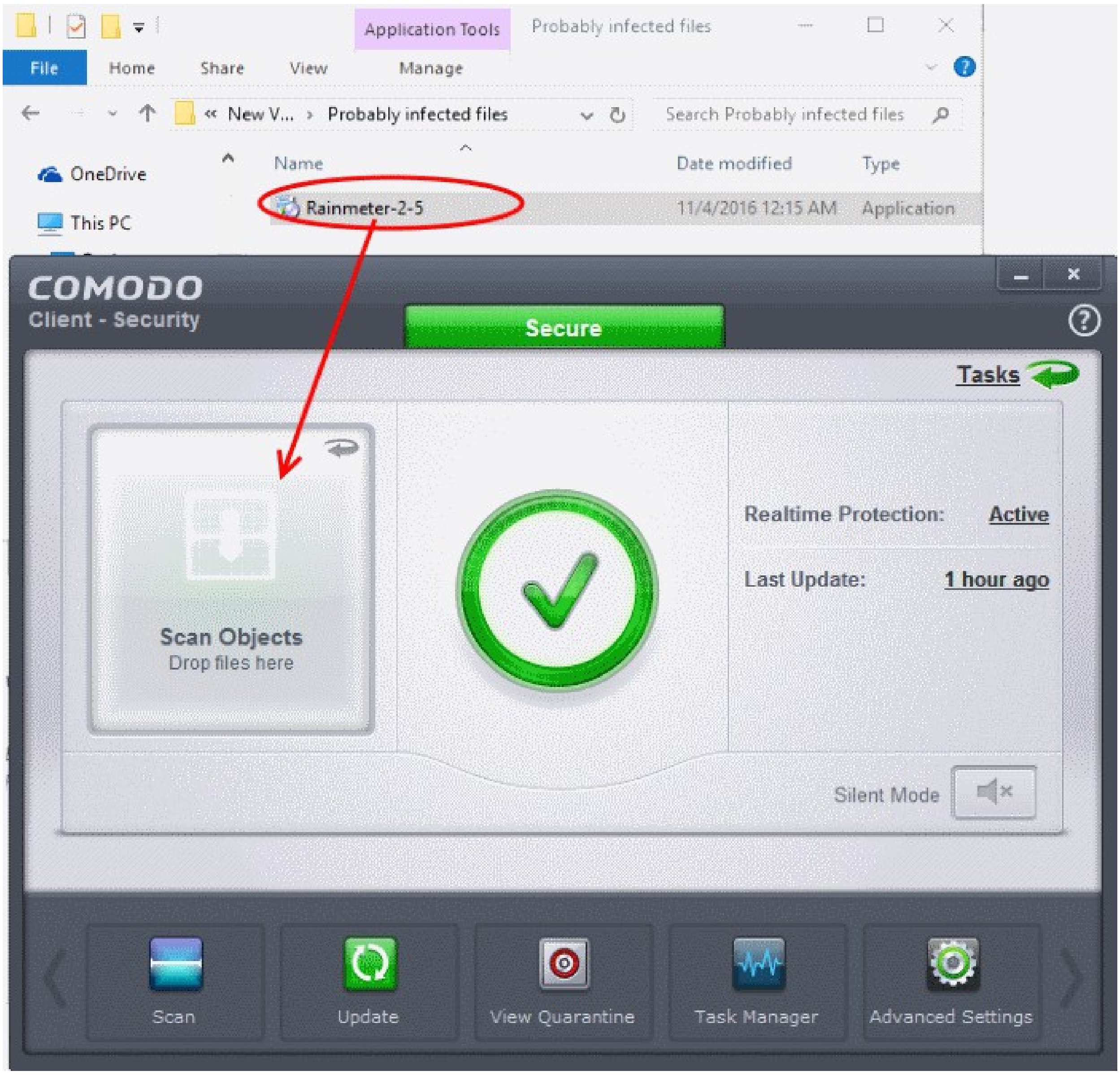
Click here for more details on running on-demand scans.

To instantly scan an item

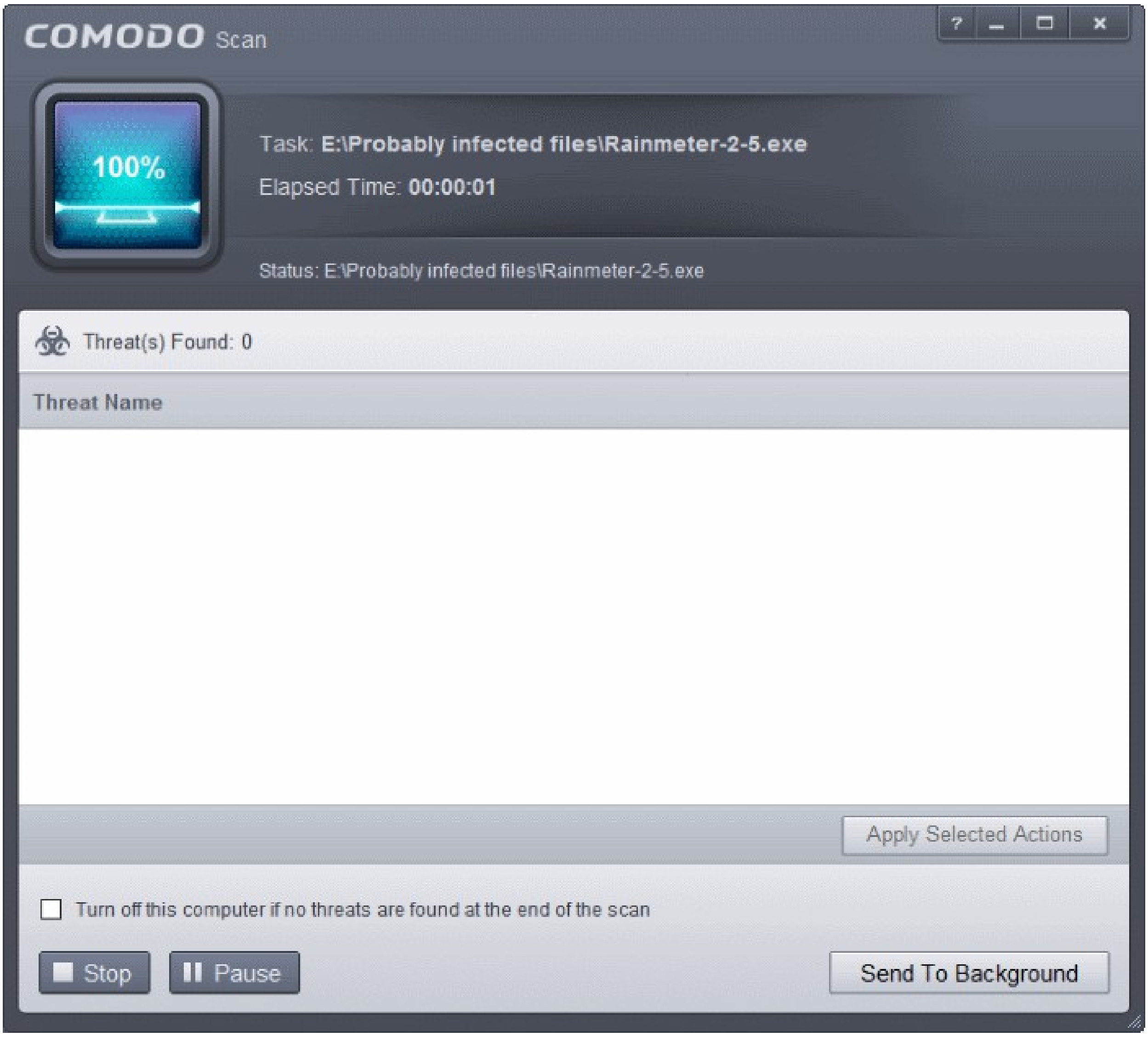
Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu.



- Alternatively drag and drop the item over the area marked 'Scan Objects' in the 'Home' screen of the CCS interface



The item will be scanned immediately.



Task: E:\Probably infected files\Rainmeter-2-5.exe

Elapsed Time: 00:00:01

Status: E:\Probably infected files\Rainmeter-2-5.exe

Threat(s) Found: 0

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

...and on completion of scanning, the scan finished dialog be displayed with the number of threats found.

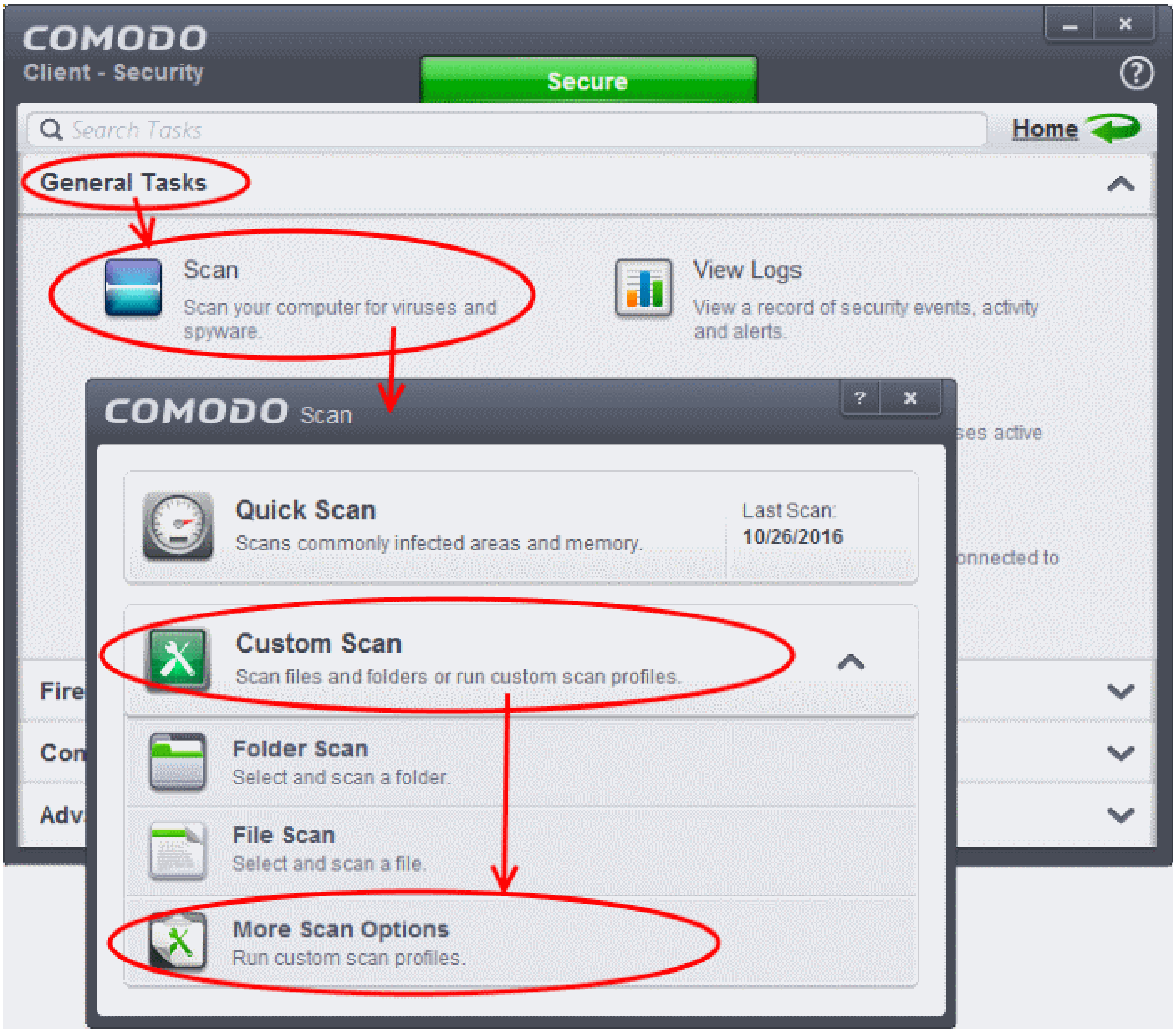
Click here for more details to take action on the infected item(s).

Creating an Antivirus Scanning Schedule

Comodo Client Security allows you to schedule Antivirus scans on your entire system or on specific areas according to your preferences. You can create a custom scan profile defining exactly which files and folders are to be scanned, when they are to be scanned and how they are to be scanned.

To create an antivirus scanning schedule

- Click the 'Tasks' arrow on the home screen to open the main Tasks menu
- In 'General Tasks', click 'Scan'
- Select 'Custom Scan' then 'More Scan Options'

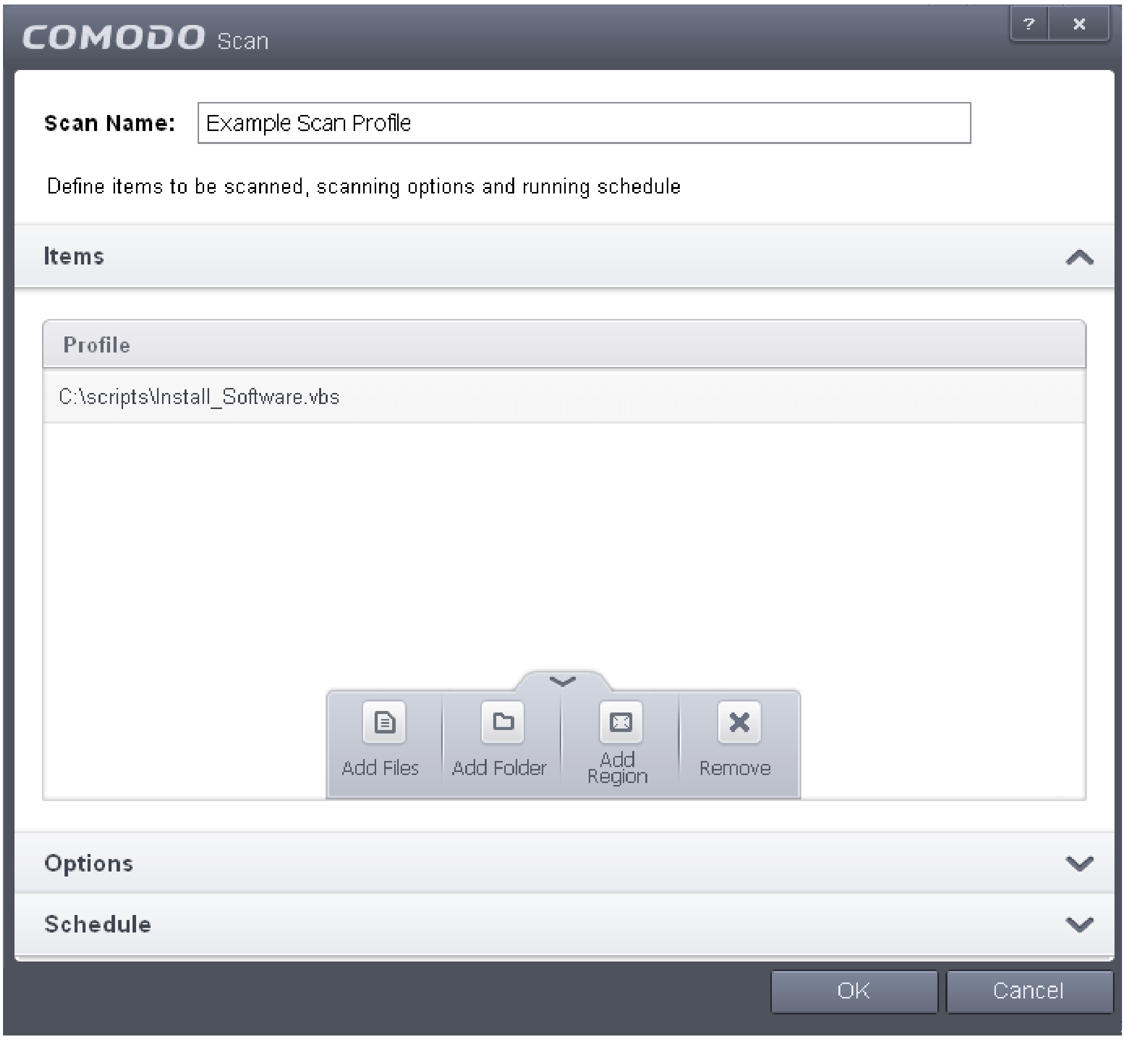

COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
COMODO Scan
Quick Scan
Scans commonly infected areas and memory.
Last Scan:
10/26/2016
Custom Scan
Scan files and folders or run custom scan profiles.
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.
More Scan Options
Run custom scan profiles.
Fire
Con
Adv

The 'Advanced Settings' interface will be displayed with 'Scans' panel opened

- Click the handle at the bottom of the interface then select 'Add'

The scan profile interface will be displayed.

- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:

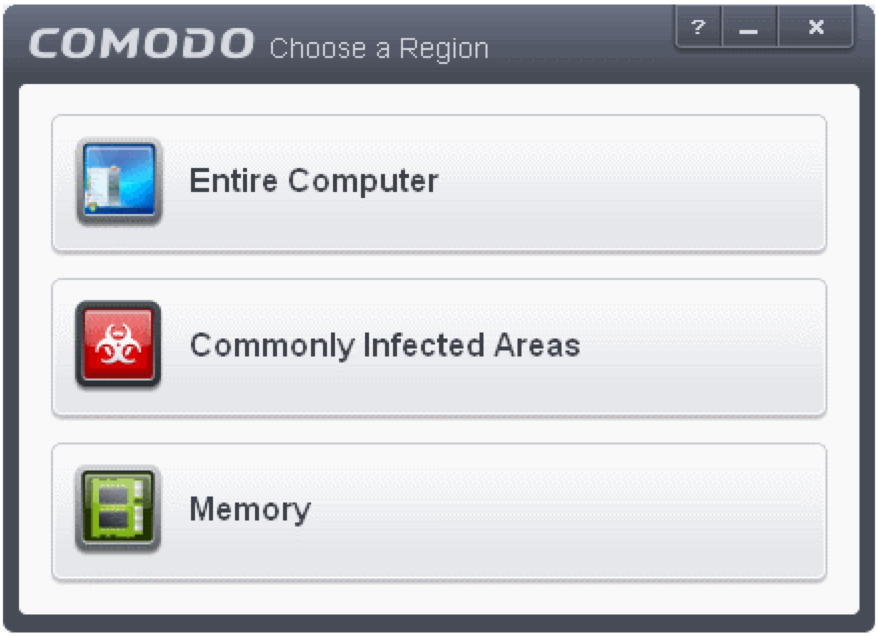


Scan Name: Example Scan Profile

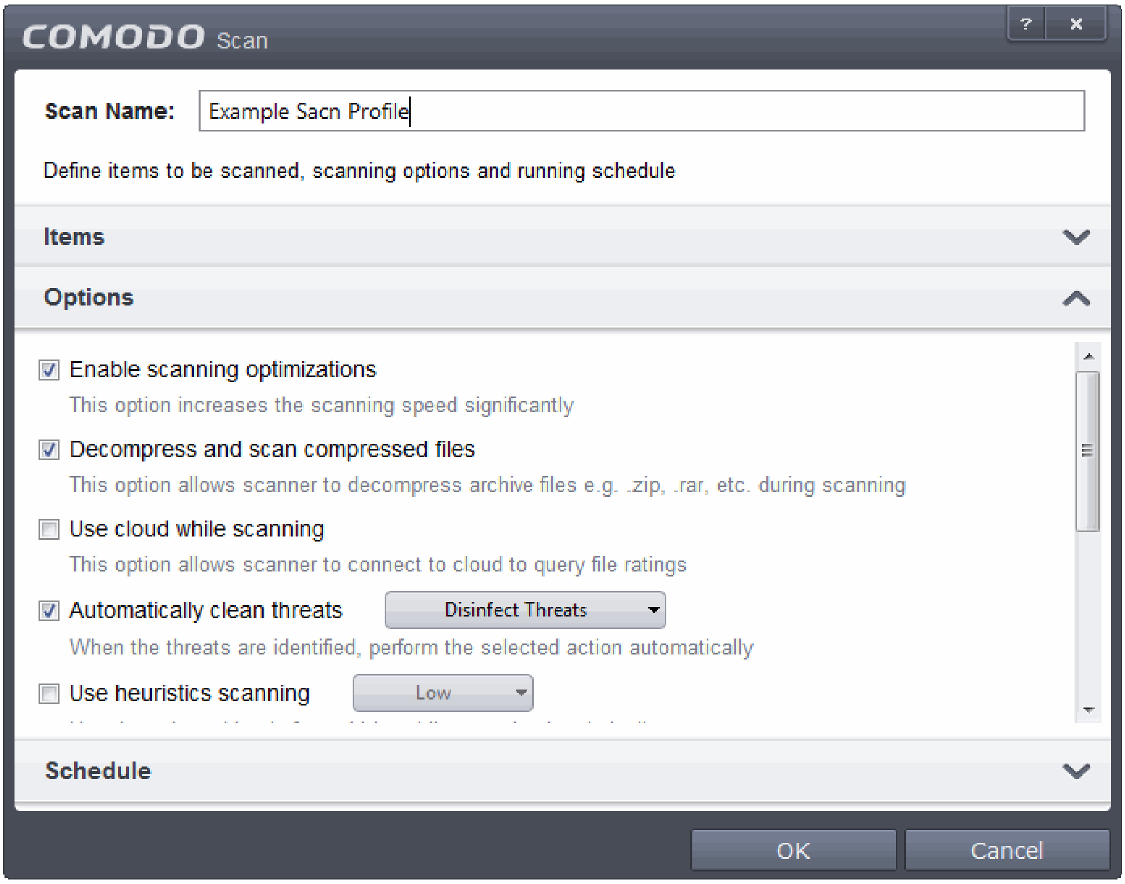
Define items to be scanned, scanning options and running schedule

C:\scripts\Install_Software.vbs

- **Add File -** Allows you to add individual files to the profile.
- **Add Folder -** Allows you to select entire folders to be included in the profile
- **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. Click 'OK' to confirm your choice.
- Next, click 'Options' to further customize the scan:



Scan Name: Example Sacn Profile

Define items to be scanned, scanning options and running schedule

☑ Enable scanning optimizations
This option increases the scanning speed significantly

☑ Decompress and scan compressed files
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

☐ Use cloud while scanning
This option allows scanner to connect to cloud to query file ratings

☑ Automatically clean threats — Disinfect Threats
When the threats are identified, perform the selected action automatically

☐ Use heuristics scanning — Low

- **Options:**
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)*** .
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP

ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .

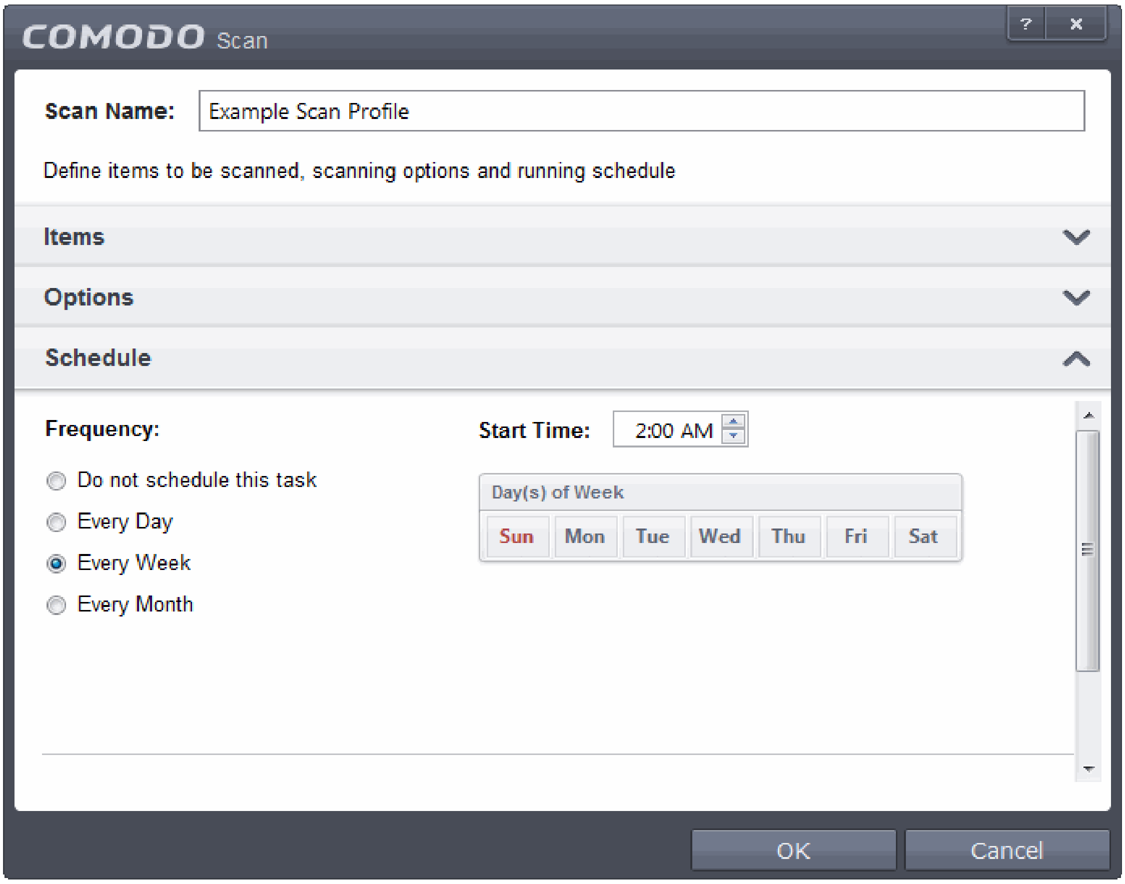
- **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. ***(Default = Disabled)***.
- **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine. ***(Default = Enabled).***
- **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 = Disabled).***

  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.

  - **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. You can select the priority from the drop-down.(***Default = Disabled and Backgraund***).
- **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)***

- To schedule the scan to run at set intervals, click 'Schedule':



COMODO Scan
? ×
Scan Name: Example Scan Profile
Define items to be scanned, scanning options and running schedule
Items
Options
Schedule
Frequency:
○ Do not schedule this task
○ Every Day
● Every Week
○ Every Month
Start Time: 2:00 AM
Day(s) of Week
Sun Mon Tue Wed Thu Fri Sat
OK
Cancel

  - **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
  - **Every Day** - The Antivirus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
  - **Every Week** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
  - **Every Month** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
  - **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
  - **Run only when computer id IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
  - **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 the scans to run at nights.
- Click 'OK' to save the profile.

The profile will be saved and the selected areas will be scanned repeatedly as per the set schedule.

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 to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. You can also create a desktop shortcut to run the application inside the container on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:

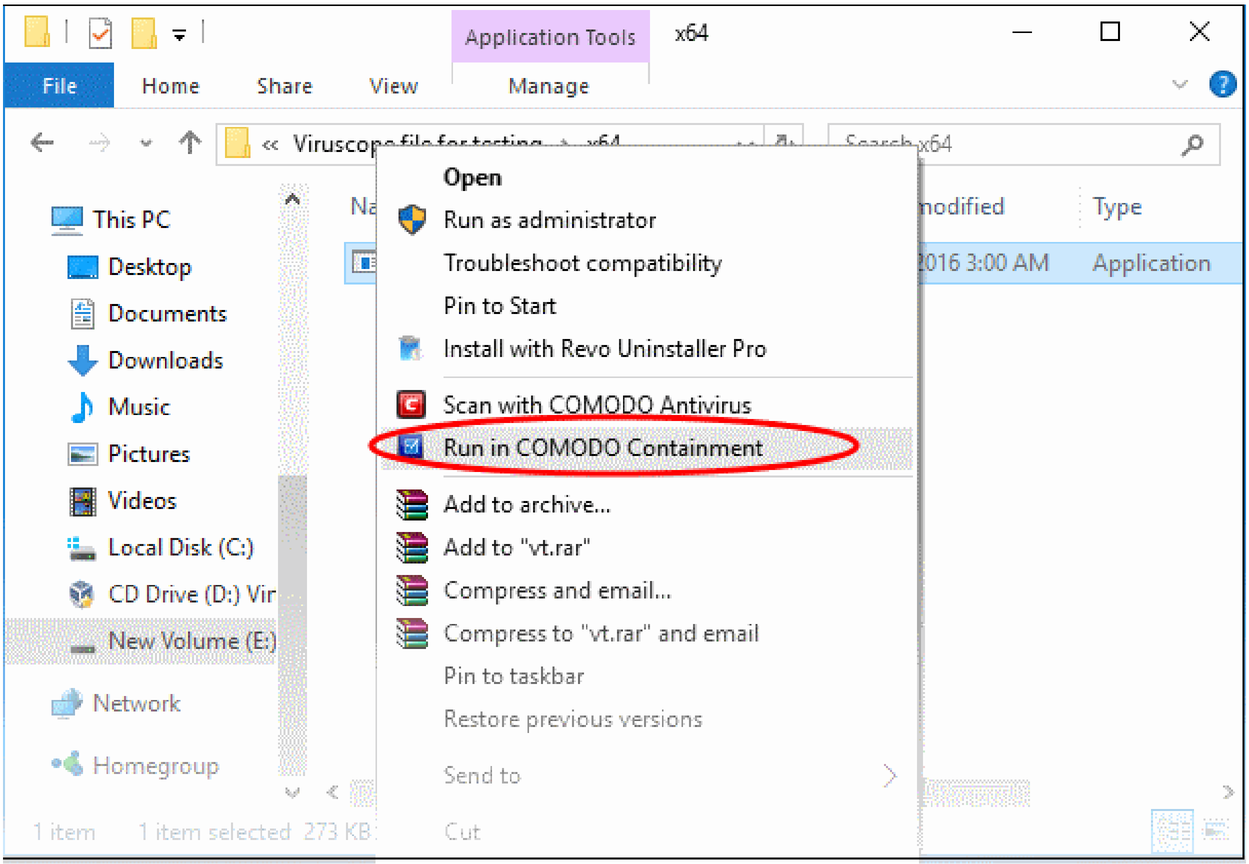
Comodo Client Security allows you to run a program in the container:

- From the right click options
- By dragging-and-dropping the application on to CCS Home screen
- From the Containment Tasks interface

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

Run a program inside the container through right click options

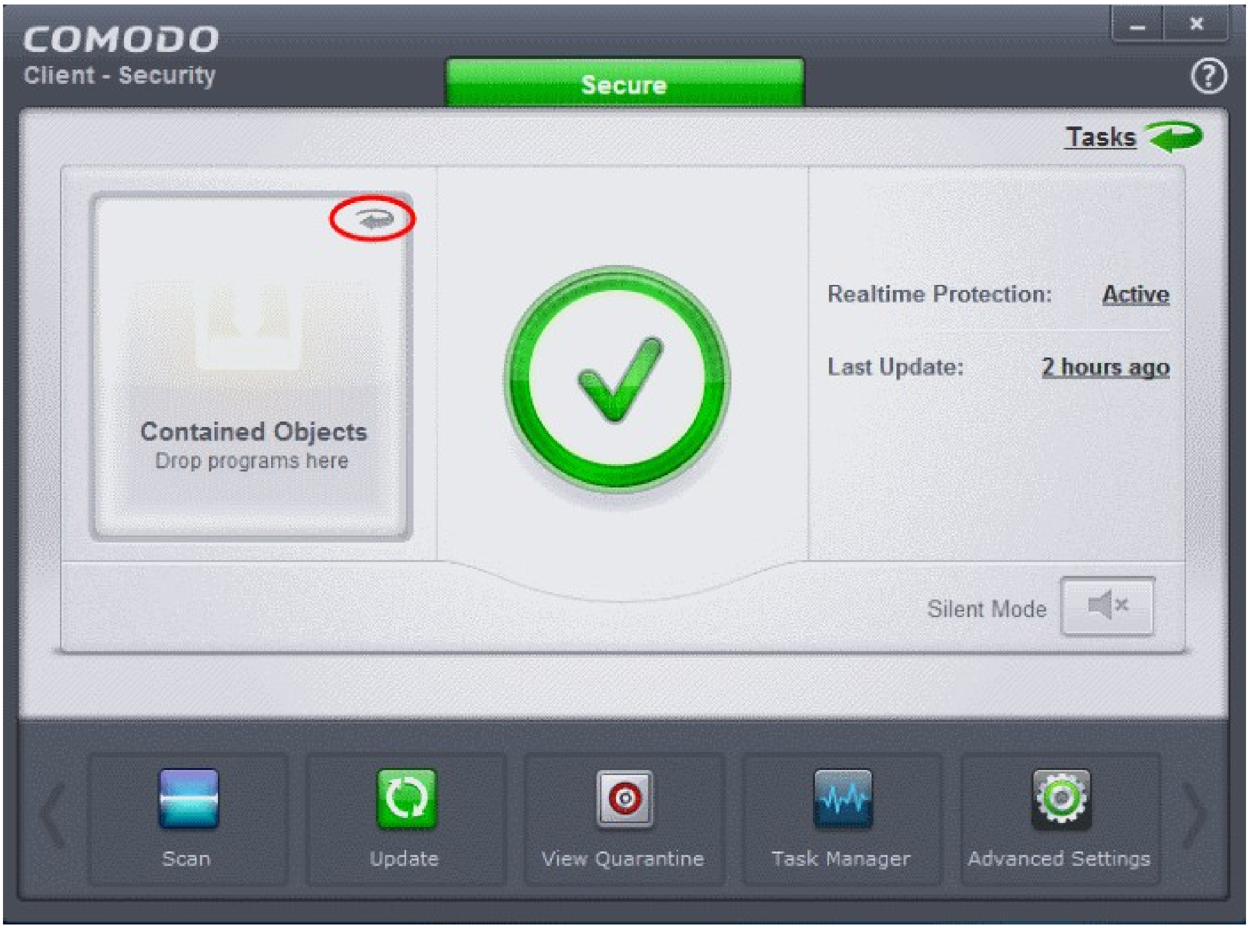
1. Browse to the installation folder of the .exe file through Windows Explorer
2. Right click on the program that you want to run inside the container



3. Choose 'Run in COMODO Containment' from the context sensitive menu

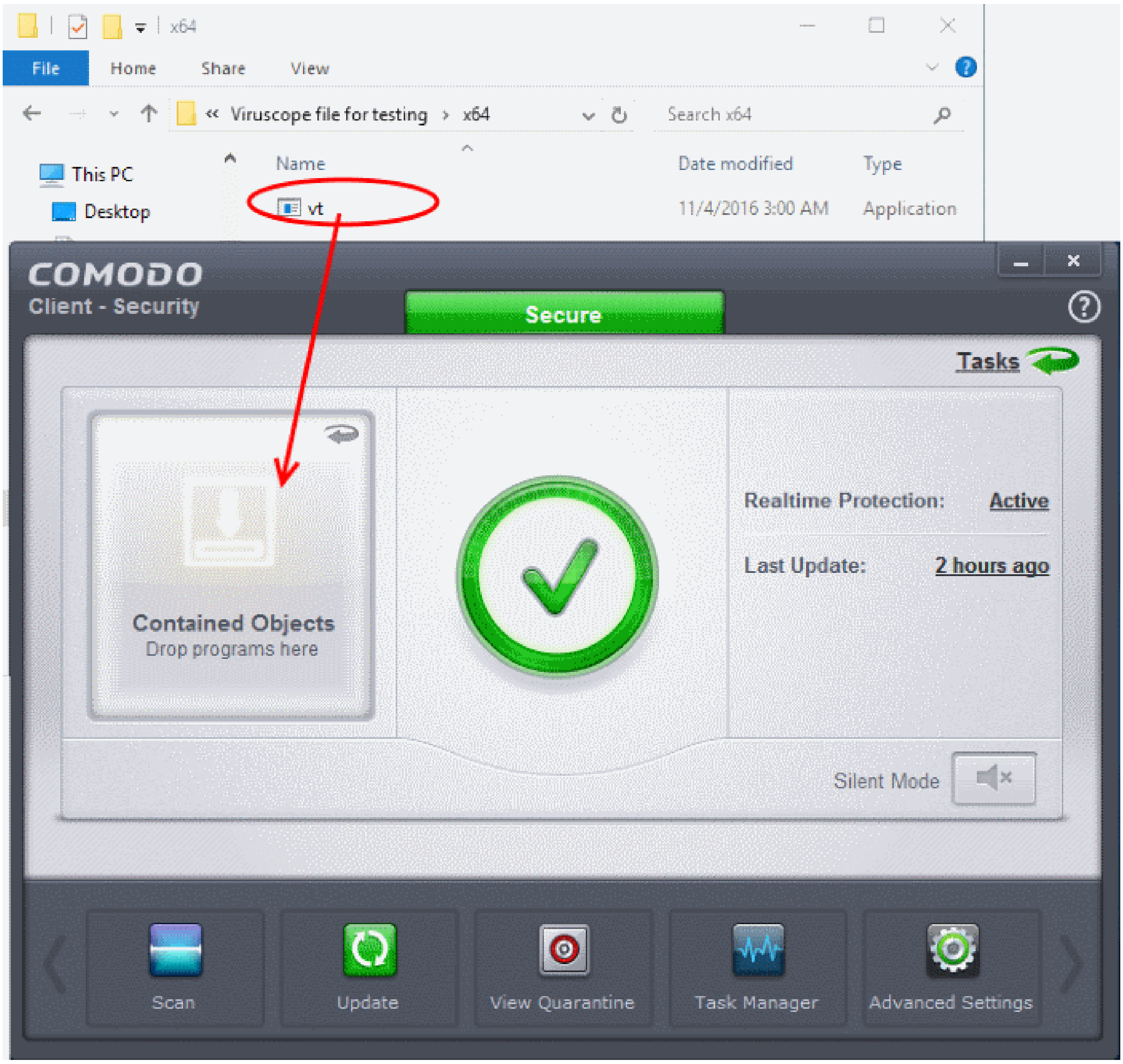
Drag-and-drop the application on to CCS Home Screen

The Home screen of the CCS interface has a flippable pane at the left side allowing you to run instant scans or run a program in the container. To flip the pane to carry out these tasks, just click the curved arrow at the top right side of the pane.



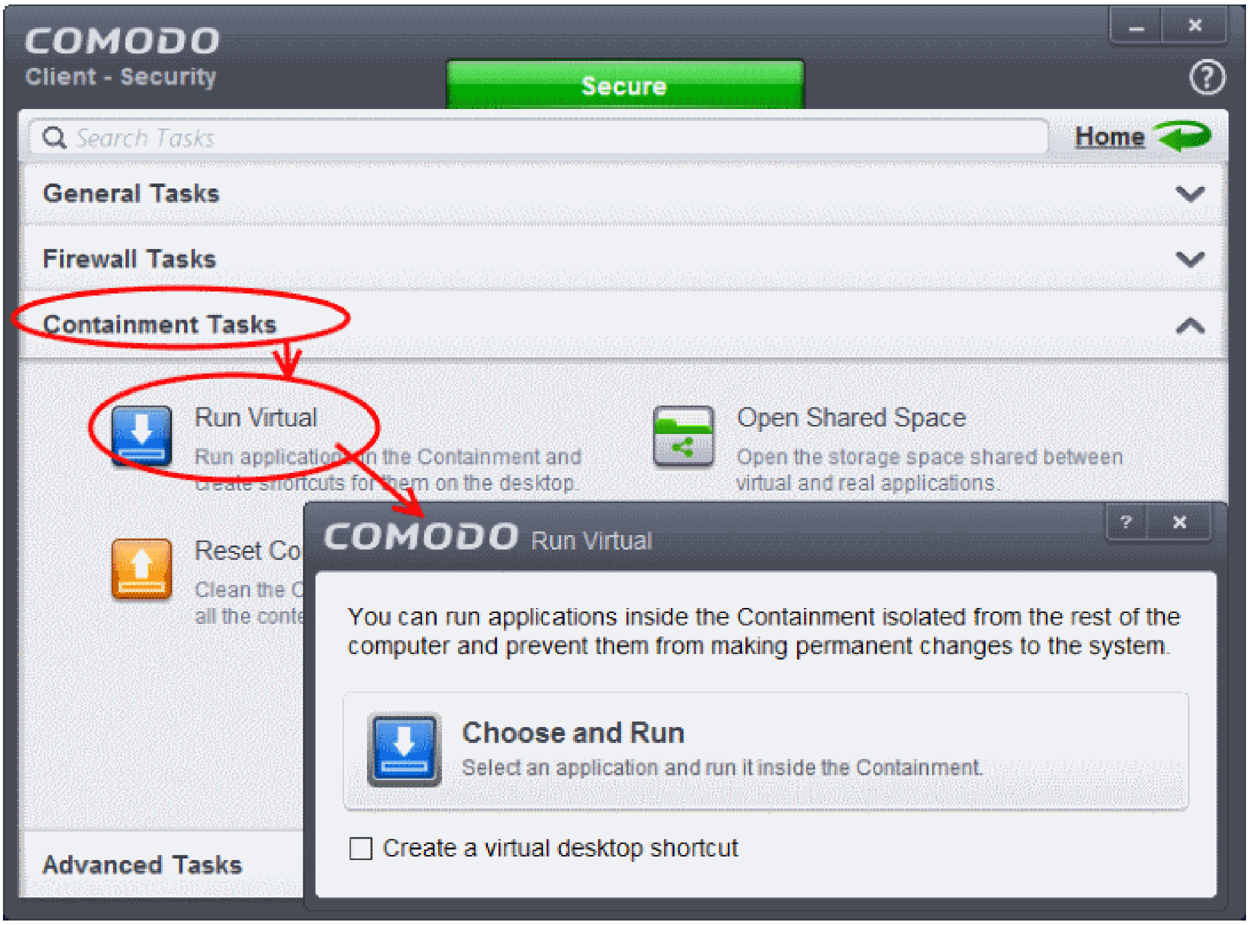
To run a program in the container

1. Flip the pane by clicking the curved arrow at the top right side to display 'Contained Objects'.
2. Navigate to the program in your system that you want to run in the container through Windows Explorer and just drag and drop into the box.



Run a program in the container from Containment Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Containment Tasks' and click 'Run Virtual'



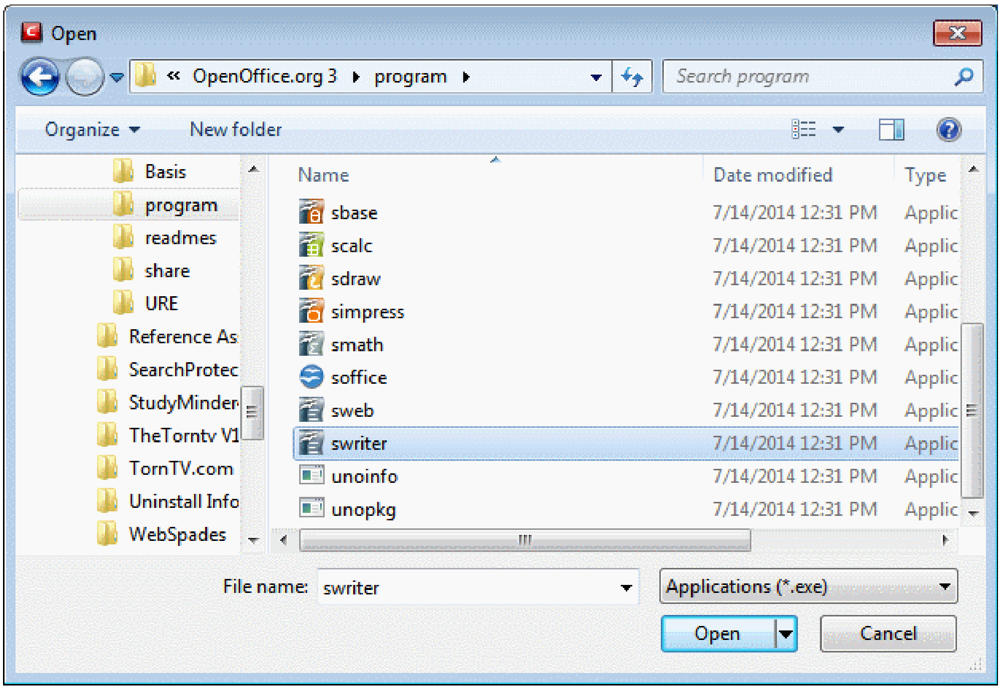
You can run applications inside the Containment isolated from the rest of the computer and prevent them from making permanent changes to the system.

Choose and Run
Select an application and run it inside the Containment.

□ Create a virtual desktop shortcut

The 'Run Virtual' dialog will be displayed.

3. To run an application inside the container, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is contained. If you wish to run the application in the container in future, then select 'Create a virtual desktop shortcut' check box.

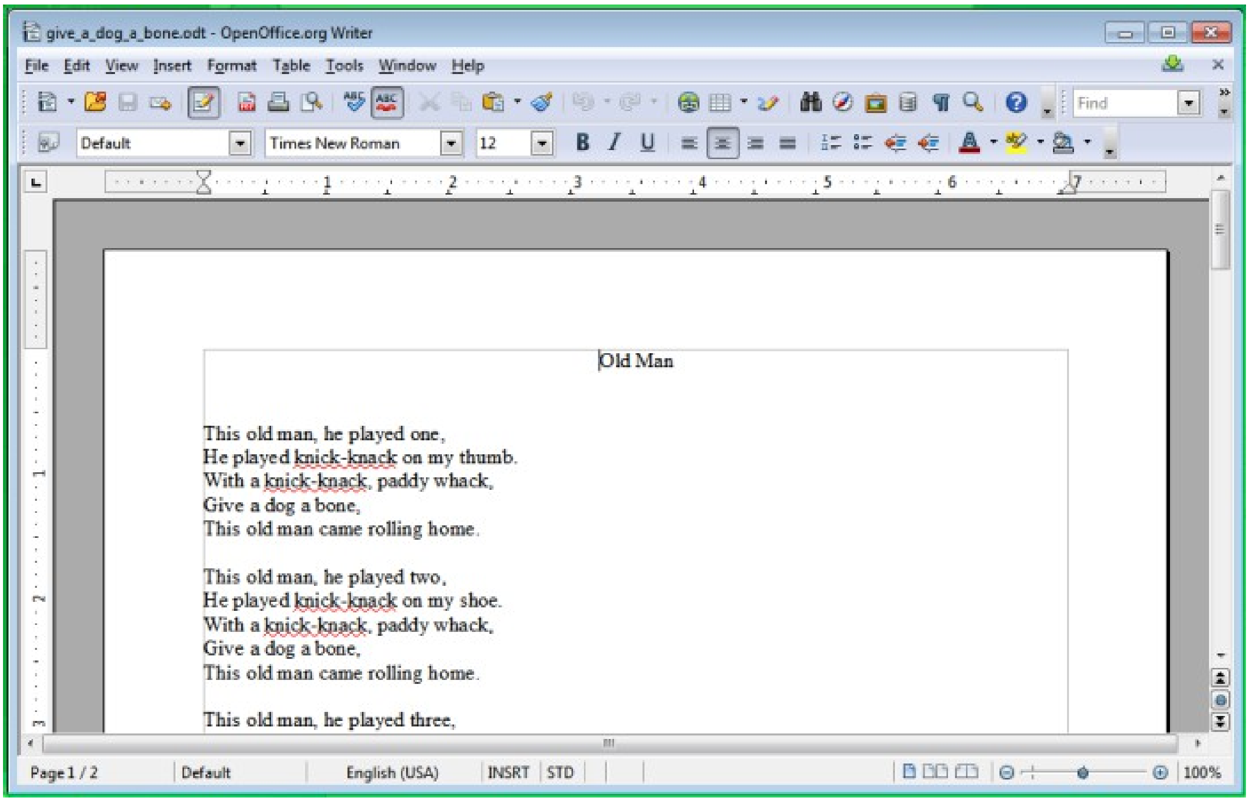


Name	Date modified	Type
sbase	7/14/2014 12:31 PM	Applic
scalc	7/14/2014 12:31 PM	Applic
sdraw	7/14/2014 12:31 PM	Applic
simpress	7/14/2014 12:31 PM	Applic
smath	7/14/2014 12:31 PM	Applic
soffice	7/14/2014 12:31 PM	Applic
sweb	7/14/2014 12:31 PM	Applic
swriter	7/14/2014 12:31 PM	Applic
unoinfo	7/14/2014 12:31 PM	Applic
unopkg	7/14/2014 12:31 PM	Applic

File name: swriter

4. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

The application will run in the container on this occasion only. If you often want a desktop short cut to the contained application, then select the check-box 'Create a virtual desktop shortcut' in step 2. If you wish to run an application in the container on a long-term/permanent basis then add the file to the container.


give_a_dog_a_bone.odt - OpenOffice.org Writer
File Edit View Insert Format Table Tools Window Help
Find
Default
Times New Roman
12
Page 1 / 2
Default
English (USA)
INSRT
STD
100%

Old Man

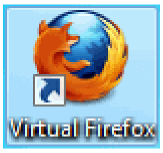
This old man, he played one,
He played knick-knack on my thumb.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played two,
He played knick-knack on my shoe.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played three,

Run Browsers Inside the Container

This page explains how to run your Internet browser inside the container. Surfing the internet with a contained browser is the same as normal, with the benefit that any malicious files you inadvertently download cannot do 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:

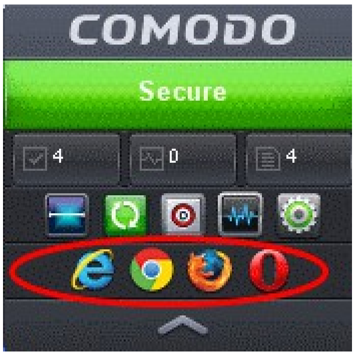


Comodo Client Security allows you to run a browser in the container:

- From the desktop widget
- From the Containment Tasks interface
- From CCS Protocol Handlers

Starting a browser from the desktop widget

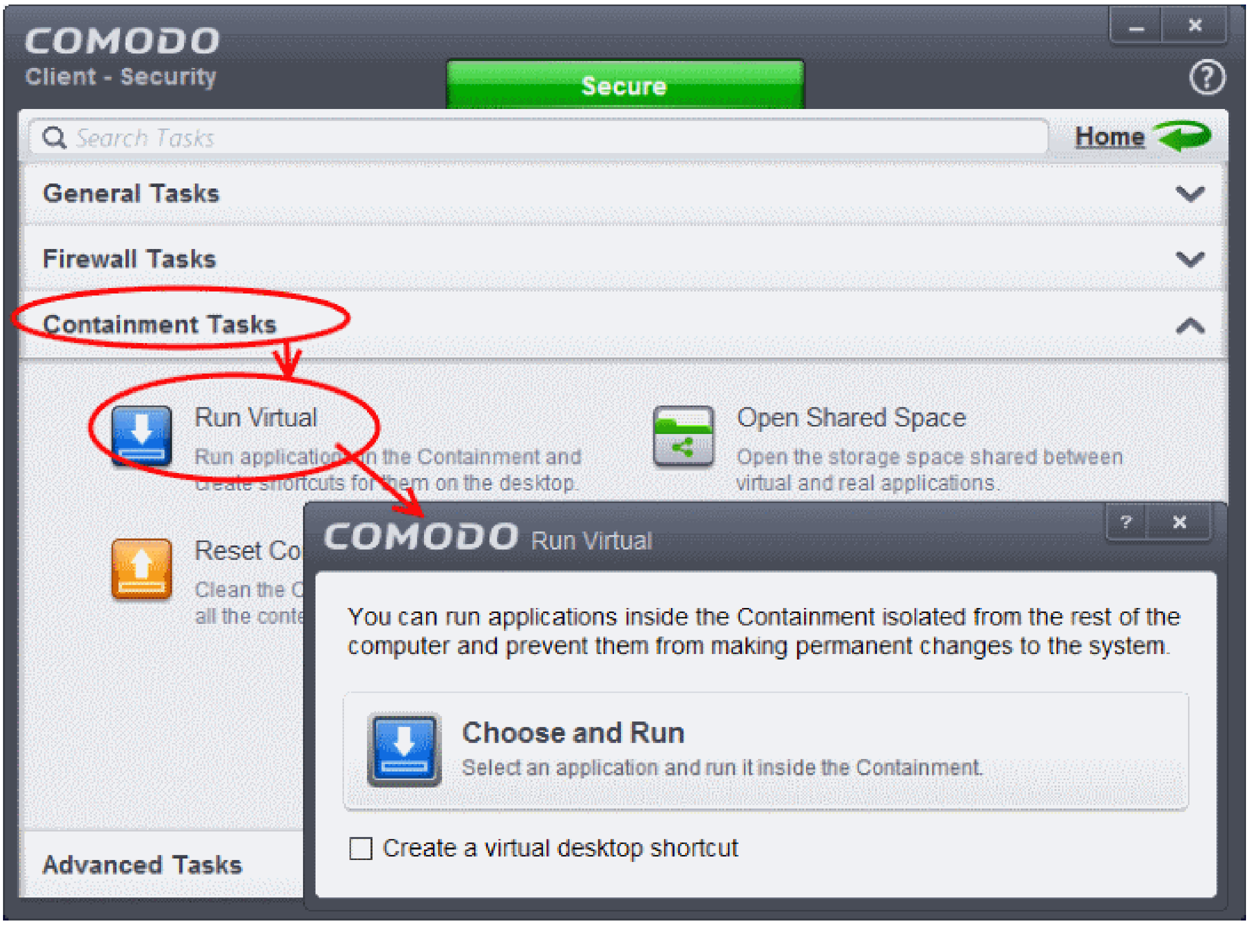
The CCS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- To start a browser inside the container, click on the browser icon.

Starting a browser from the Containment Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Containment Tasks' and click 'Run Virtual'



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

Choose and Run

Select an application and run it inside the Containment.

☐ Create a virtual desktop shortcut

The 'Run Virtual' dialog will be displayed.

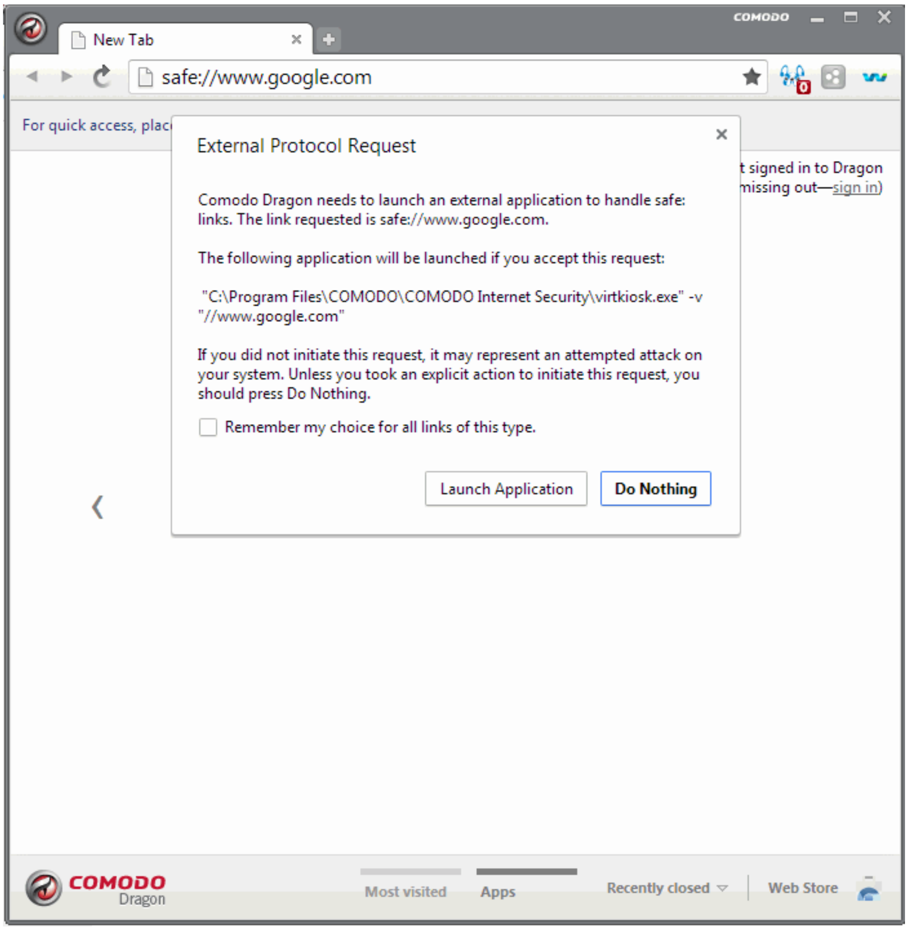
3. To run a browser inside the container, click 'Choose and Run', navigate to the installation location of the browser and select the exe file of the browser. If you wish to create a desktop shortcut to run the browser in the container in future, then select 'Create a virtual desktop shortcut'.

The browser will run with a green border indicating that it is contained.

Starting a browser from the CCS protocol handlers

safe://

This protocol is used to open any URL with a contained browser. For example: *safe://www.google.com*



External Protocol Request

Comodo Dragon needs to launch an external application to handle safe: links. The link requested is safe://www.google.com.

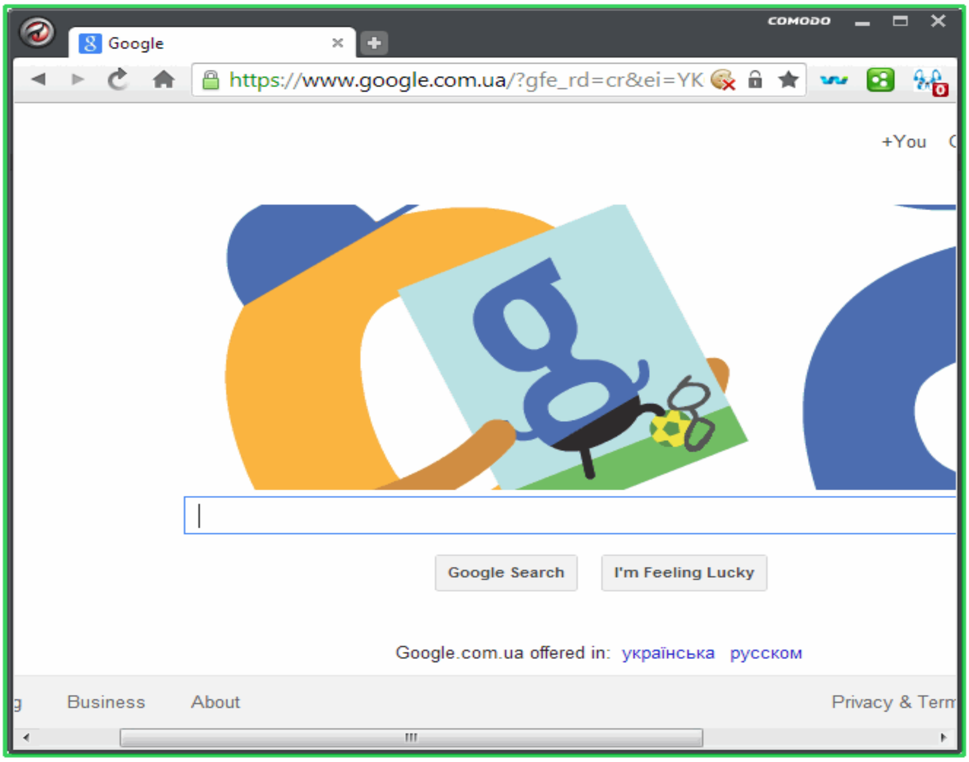
The following application will be launched if you accept this request:

"C:\Program Files\COMODO\COMODO Internet Security\virtkiosk.exe" -v "//www.google.com"

If you did not initiate this request, it may represent an attempted attack on your system. Unless you took an explicit action to initiate this request, you should press Do Nothing.

□ Remember my choice for all links of this type.

The browser will run with a green border indicating that it is contained.



Google
https://www.google.com.ua/?gfe_rd=cr&ei=YK
+You
Google Search
I'm Feeling Lucky
Google.com.ua offered in: українська русском
Business
About
Privacy & Term

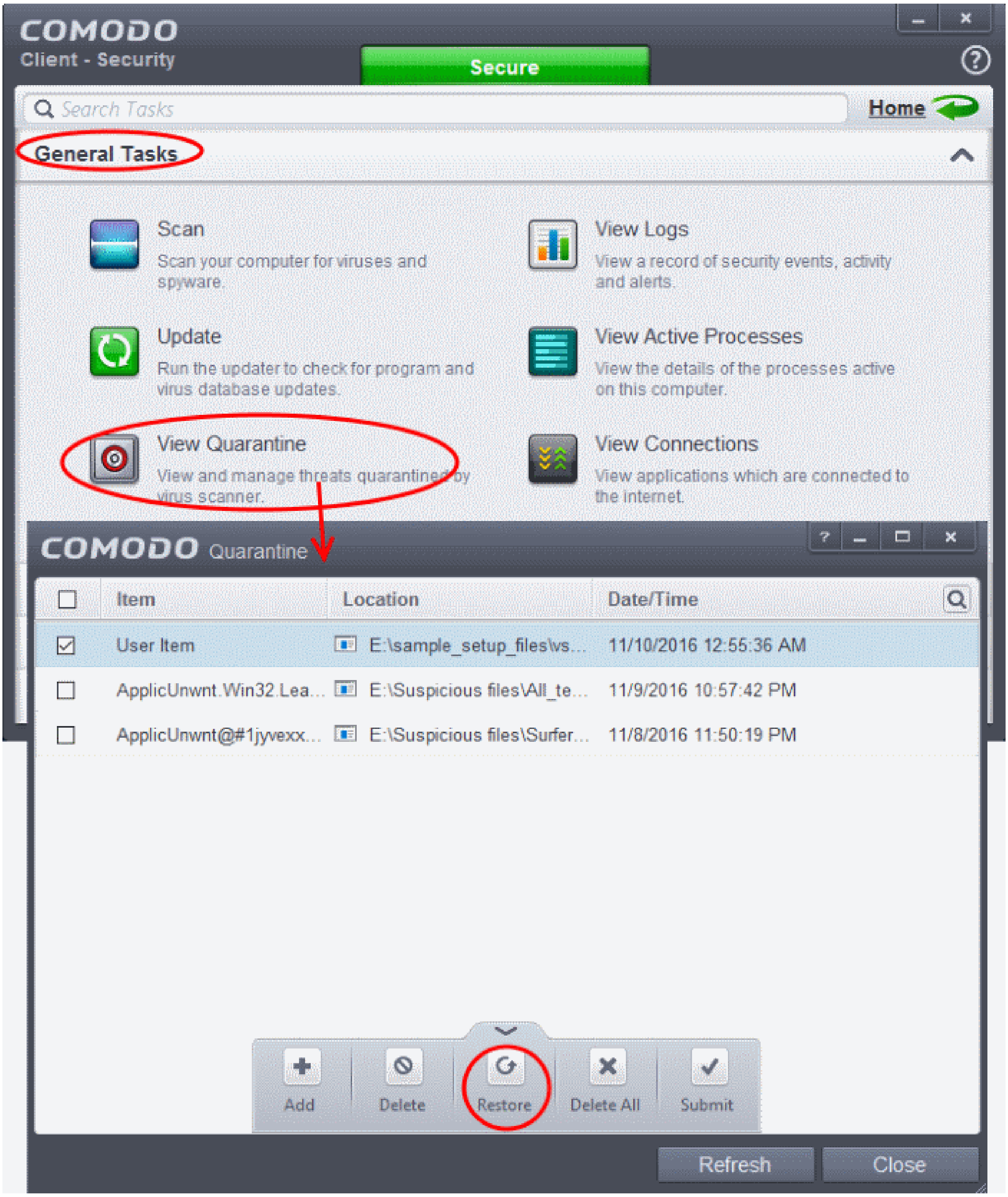
Restore Incorrectly Quarantined Item(s)

If you have incorrectly quarantined item(s) or you feel an item has been incorrectly quarantined by the application (a false positive) then you can restore it/them using the following procedure:

To submit Quarantined items

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

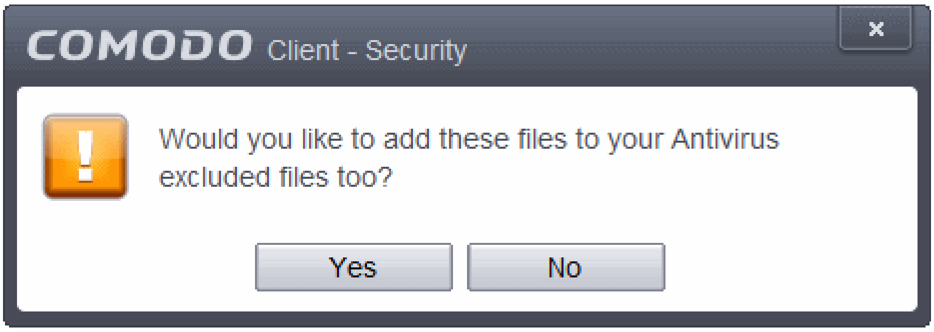
The 'Quarantine' interface will open. The interface displays a list of items moved to Quarantine manually, from the results of real-time scanning, on-demand scanning and scheduled scans.


COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
COMODO Quarantine
Add
Delete
Restore
Delete All
Submit
Refresh
Close

□	Item	Location	Date/Time
☑	User Item	E:\sample_setup_files\vs...	11/10/2016 12:55:36 AM
□	ApplicUnwnt.Win32.Lea...	E:\Suspicious files\All_te...	11/9/2016 10:57:42 PM
□	ApplicUnwnt@#1jyvexx...	E:\Suspicious files\Surfer...	11/8/2016 11:50:19 PM

3. Choose the items to be restored by selecting the checkbox beside them.
4. Click the handle from the bottom and choose 'Restore'.

An option to add the selected items to AV excluded files will open.



Would you like to add these files to your Antivirus excluded files too?

If you select 'Yes', these items will not be included for AV scans. If you select' No', these items will be included for AV scans and quarantined during the next scanning.

All the selected files will be restored to their original locations immediately.

5. Click 'Close' button to exit.

Click here for more details on the Quarantined Items.

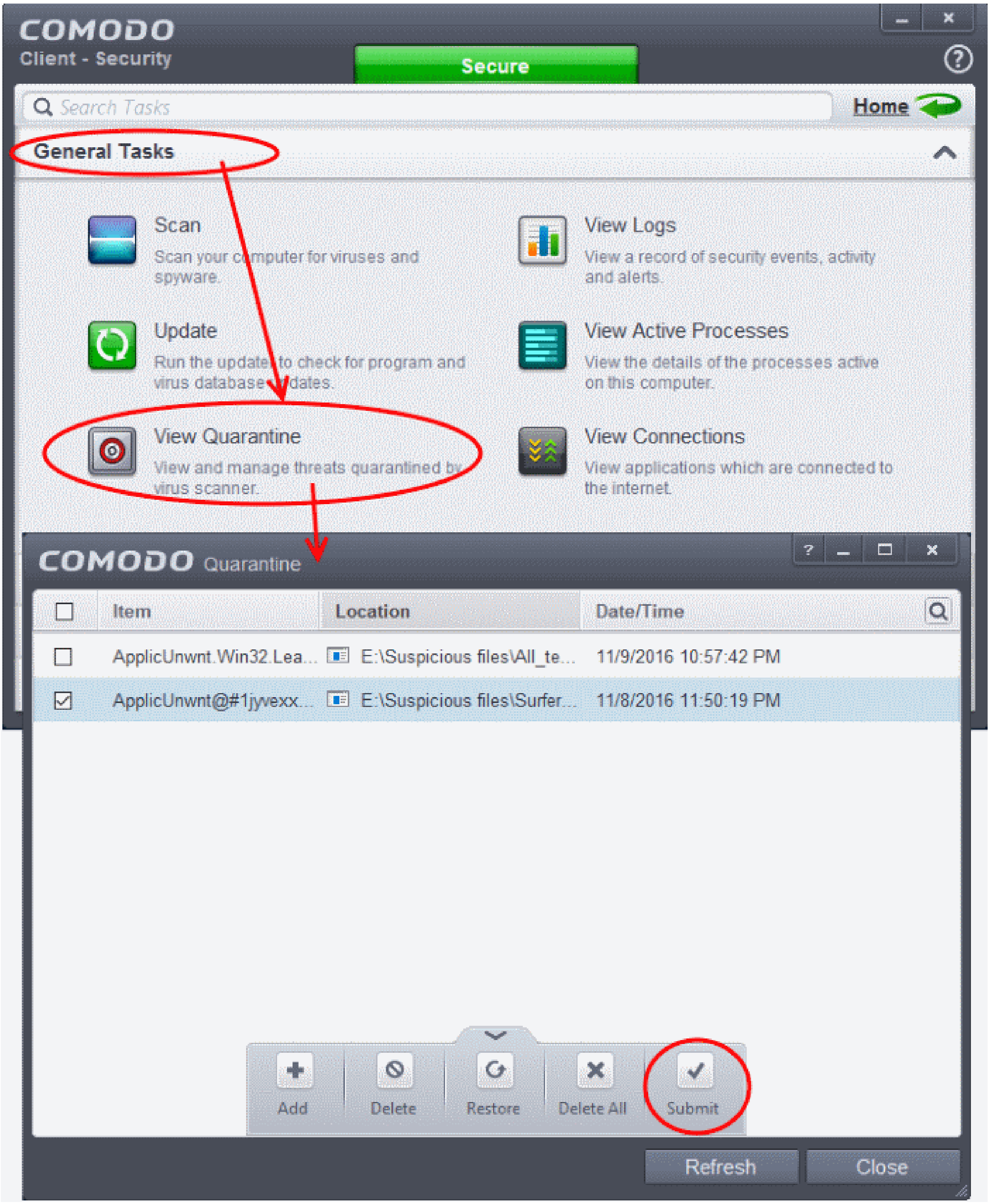
Submit Quarantined Items to Comodo for Analysis

Items which have been quarantined as a result of an On Access, On Demand or Scheduled Scans, can be sent to Comodo for Analysis. After the analysis, if the submitted item is found to be a False Positive, it will be added to Comodo Safe List. Conversely, if it is found to be a malware, it will be added to the anti-malware Black list. This helps Comodo to enhance its virus signature database and helps millions of other CCS users to benefit out of it. Click here for more details on Quarantined Items.

To submit Quarantined items

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

The 'Quarantine' interface will open. The interface displays a list of items moved to Quarantine manually, from the results of real-time scanning, on-demand scanning and scheduled scans.



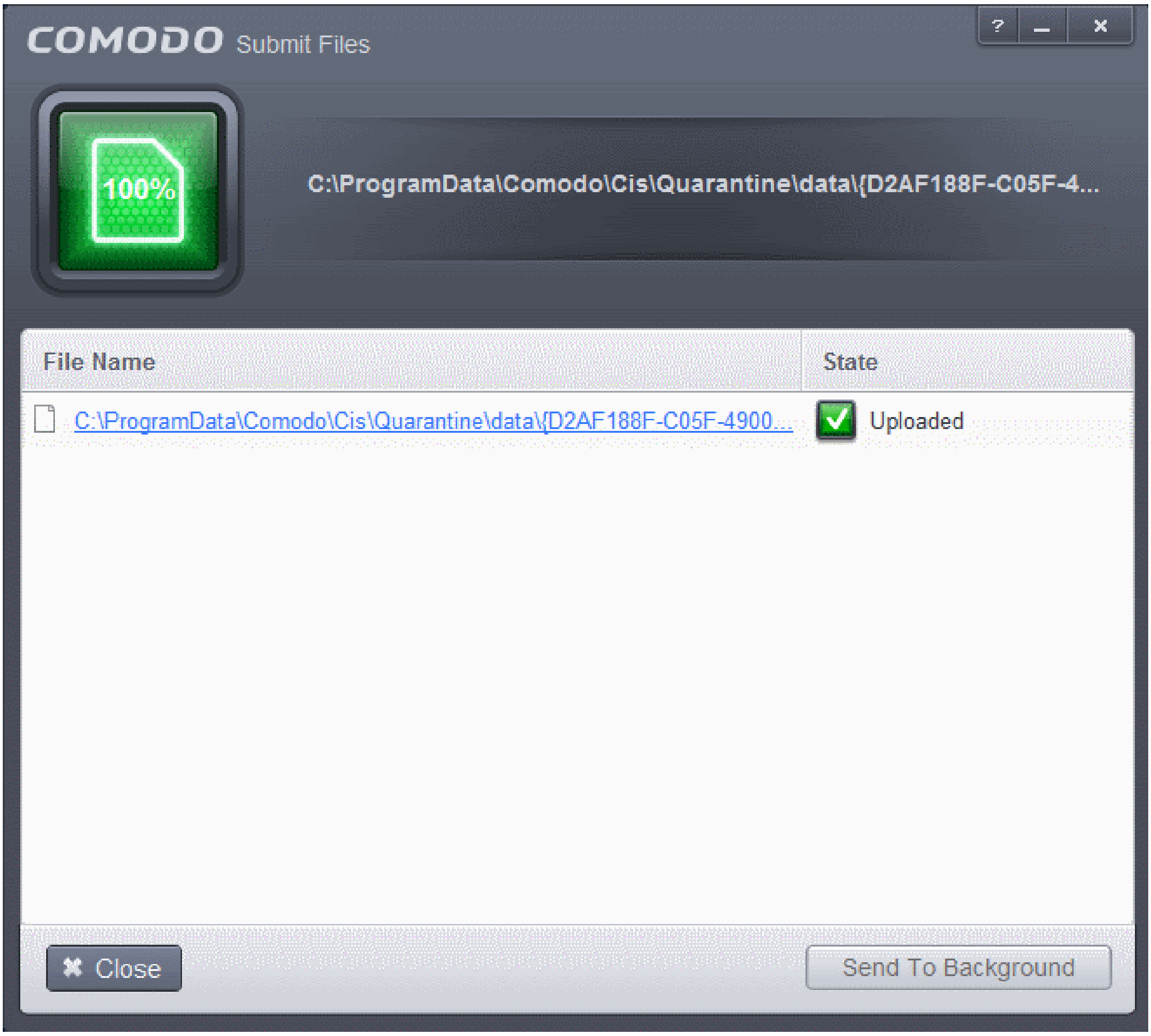
COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Active Processes
View the details of the processes active on this computer.
View Quarantine
View and manage threats quarantined by virus scanner.
View Connections
View applications which are connected to the internet.
COMODO Quarantine
Add
Delete
Restore
Delete All
Submit
Refresh
Close

□	Item	Location	Date/Time
□	ApplicUnwnt.Win32.Lea...	E:\Suspicious files\All_te...	11/9/2016 10:57:42 PM
☑	ApplicUnwnt@#1jyvexx...	E:\Suspicious files\Surfer...	11/8/2016 11:50:19 PM

3. Choose the items to be submitted to Comodo for analysis by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Submit'.

The submission progress will be indicated.

On completion, the submission results will be displayed, indicating whether the file is successfully submitted or already submitted by other users and is pending for analysis.


COMODO Submit Files
100%
C:\ProgramData\Comodo\Cis\Quarantine\data\{D2AF188F-C05F-4...
Close
Send To Background

File Name	State
C:\ProgramData\Comodo\Cis\Quarantine\data\{D2AF188F-C05F-4900...	✓ Uploaded

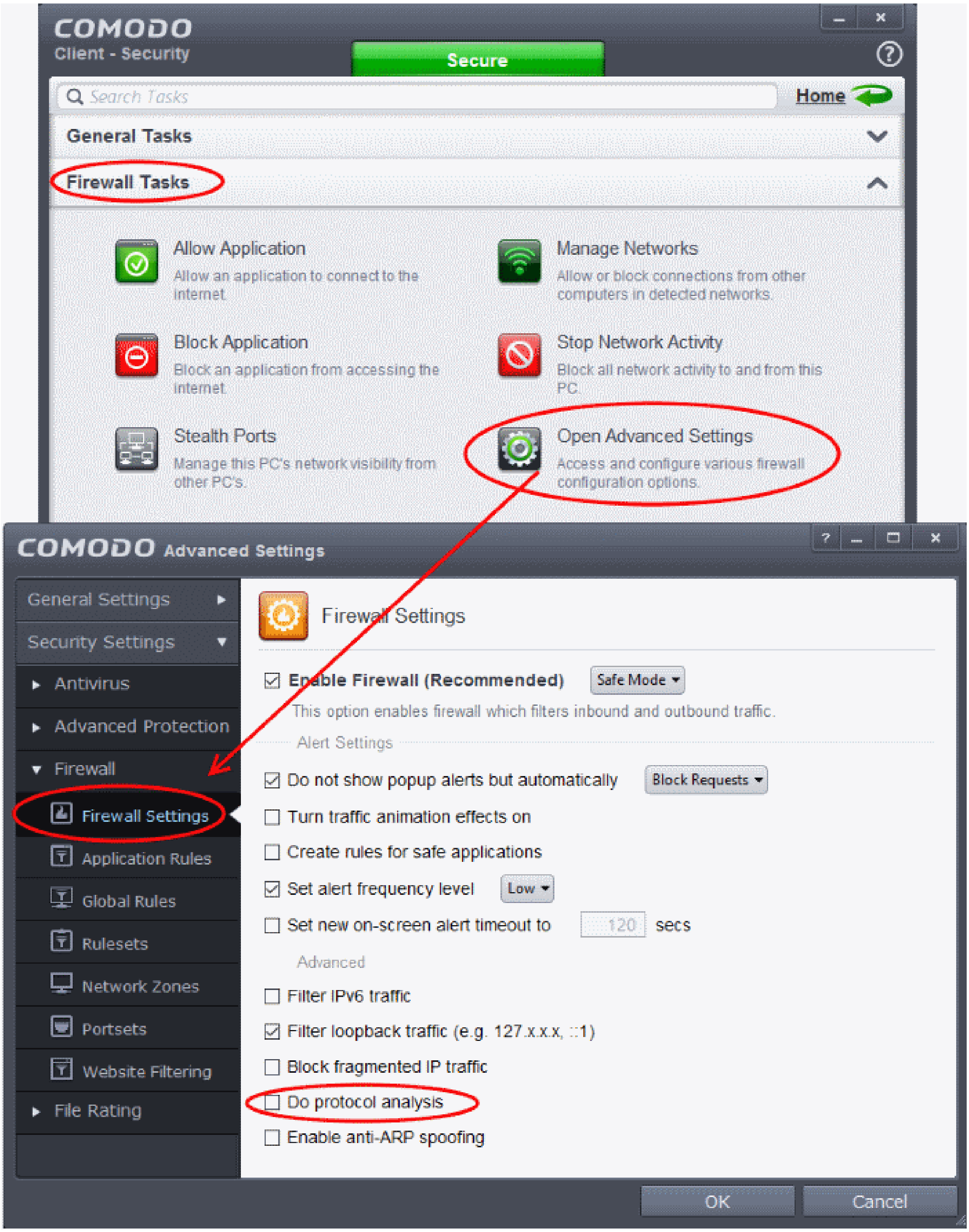
Enable File Sharing Applications like BitTorrent and Emule

This topic explains how to configure Comodo Firewall for file sharing applications like Shareaza/Emule and BitTorrent/UTorrent. To allow these file sharing applications, you must:

- Disable 'Do Protocol analysis' *(disabled, by default)*
- Create a 'Predefined Firewall Ruleset' for Shareaza/Emule
- Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent

To Disable 'Do Protocol analysis'

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.



Firewall Settings

☑ Enable Firewall (Recommended) Safe Mode

This option enables firewall which filters inbound and outbound traffic.

Alert Settings

☑ Do not show popup alerts but automatically Block Requests

☐ Turn traffic animation effects on

☐ Create rules for safe applications

☑ Set alert frequency level Low

☐ Set new on-screen alert timeout to 120 secs

Advanced

☐ Filter IPv6 traffic

☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)

☐ Block fragmented IP traffic

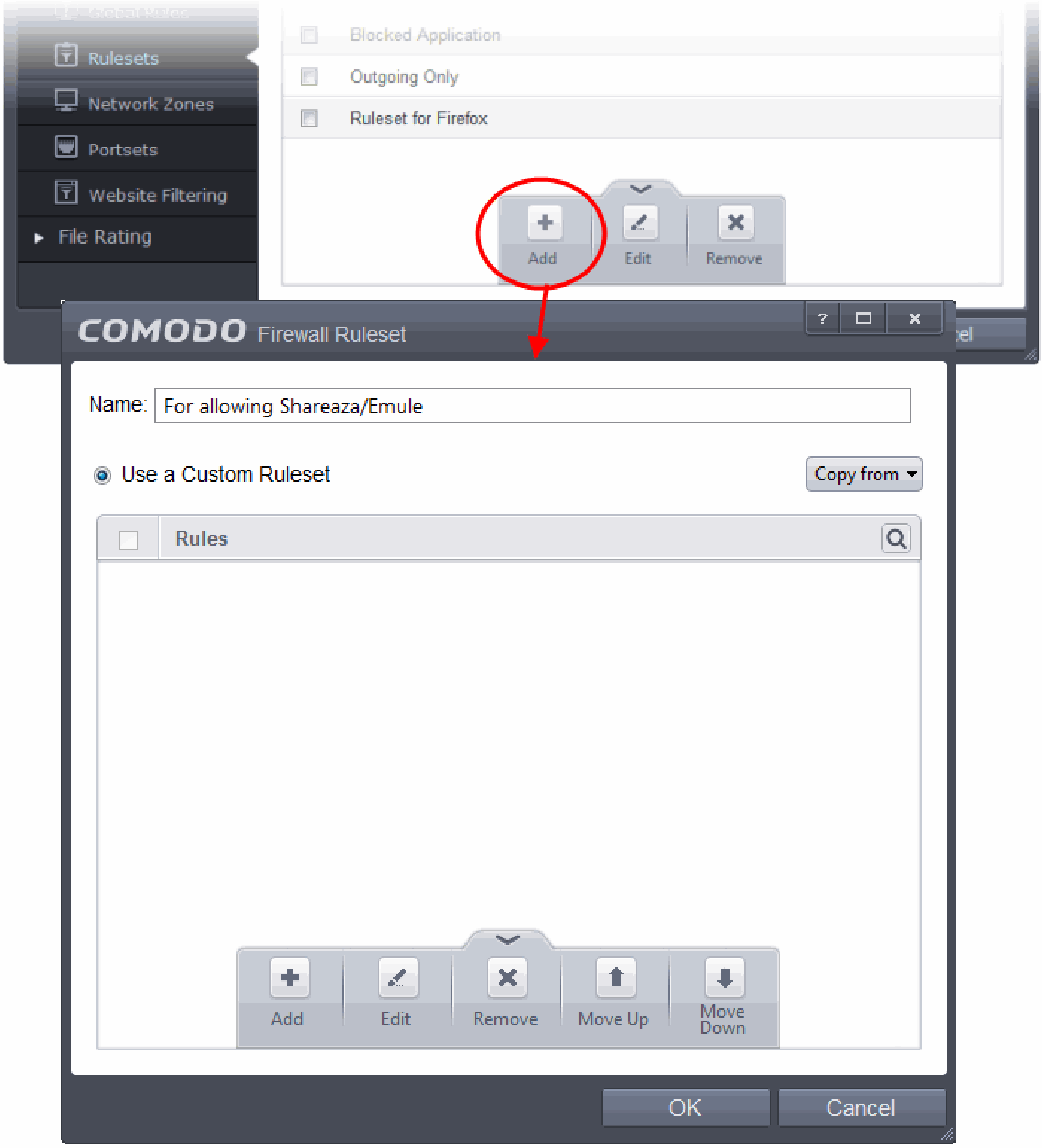
☐ Do protocol analysis

☐ Enable anti-ARP spoofing

3. Ensure that 'Do Protocol Analysis' checkbox is not selected.

To create a 'Predefined Firewall Ruleset' for Shareaza/Emule

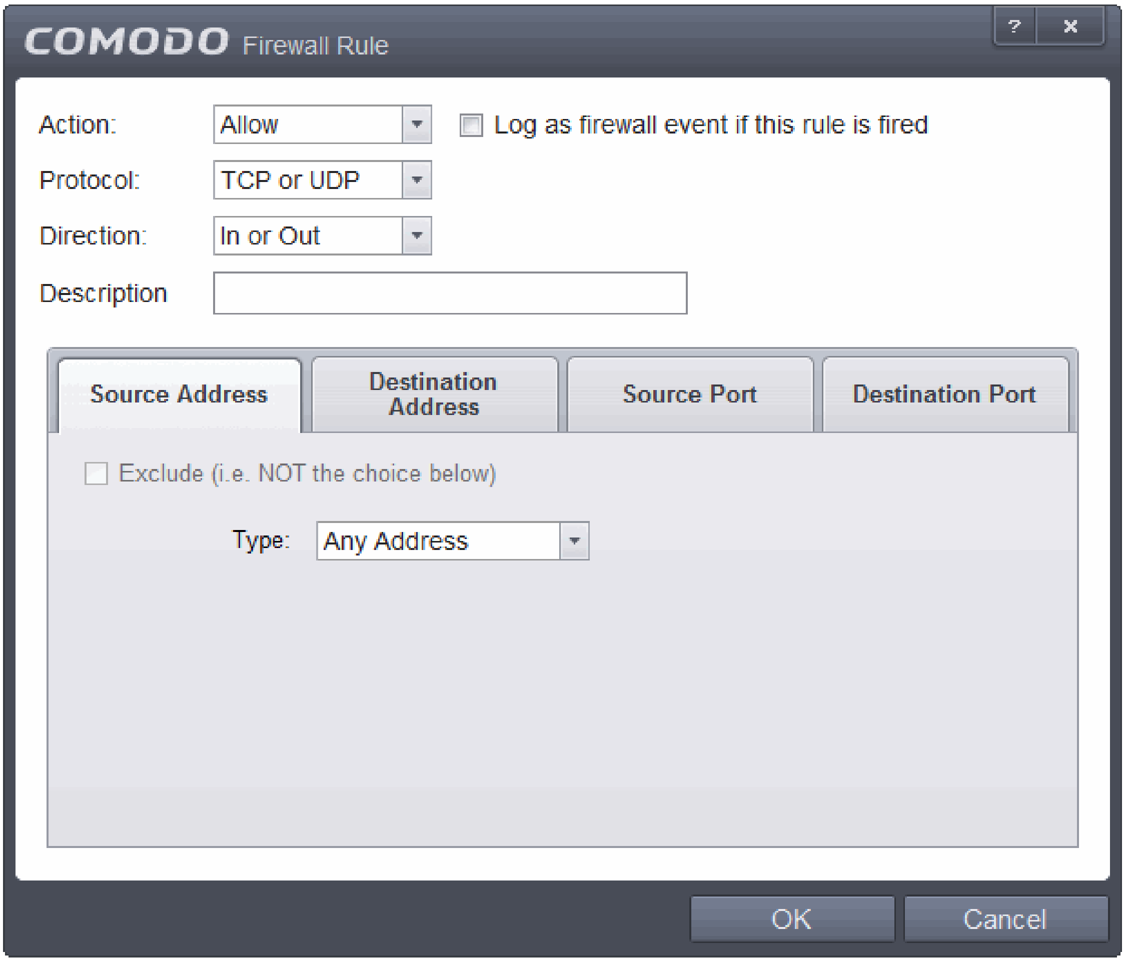
1. Click 'Rulesets' under 'Firewall' from the LHS navigation pane of 'Advanced Settings' interface to open 'Rulesets' panel
2. Click the handle from the bottom of the panel and choose 'Add'



Name: For allowing Shareaza/Emule

The 'Firewall Ruleset' interface will open for creating a new set of rules.

3. Click the handle from the bottom and choose 'Add'
4. Enter a descriptive name for the new ruleset to be created in the 'Description' text box (for example: For allowing Shareaza/Emule).
5. Now you need to create six rules for the newly created ruleset. To do so, click 'Add'. The 'Firewall Rule' interface will appear. For creating each rule, select the check box and choose the drop-down options under each tab as given below. After creating each rule, click 'OK' for the rule to be added. Click handle in the 'Firewall Ruleset' interface and choose 'Add' to create the next rule.



COMODO Firewall Rule

Action: Allow ☐ Log as firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description:

☐ Exclude (i.e. NOT the choice below)

Type: Any Address

Rule 1

- Action : Allow
- Protocol : TCP
- Direction : In
- Description : Rule for incoming TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1025 / 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 = 1025 / 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 = 1025 / end port = 65535)
- Destination port : A port range : (start port = 1025 / 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 = 1025 / 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.

The new ruleset will be created and added as a Predefined ruleset. Start Shareaza or Emule. When Comodo raises a pop-up alert, choose 'Treat this application as', select the descriptive name you gave for this rule (e.g. For allowing Shareaza/Emule) from the options and select 'Remember my answer'.

To create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Rulesets' under 'Firewall' from the LHS navigation pane of 'Advanced Settings' interface to open 'Rulesets' panel

2. Click the handle from the bottom of the panel and choose 'Add'

The 'Firewall Ruleset' interface will open for creating a new set of rules.

3. Click the handle from the bottom and choose 'Add'
4. Enter a descriptive name for the new ruleset to be created in the 'Description' text box (for example: For allowing BitTorrent/Utorrent).
5. Now you need to create six rules for the newly created ruleset. To do so, click 'Add'. The 'Firewall Rule' interface will appear. For creating each rule, select the check box and choose the drop-down options under each tab as given below. After creating each rule, click 'OK' for the rule to be added. Click handle in the 'Firewall Ruleset' interface and choose 'Add' to create the next rule.

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 = 1025 / 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 = 1025 / End port = 65535)
- Destination port : A Port Range : (Start port = 1025 / 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 = 1025 / 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 = 1025 / 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.

The new ruleset will be created and added as a Predefined Firewall ruleset. Start BitTorrent or Utorrent. When Comodo raises a pop-up alert, choose 'Treat this application as', select the descriptive name you gave for this rule (e.g. For allowing

BitTorrent/Utorrent) from the options and select 'Remember my answer'.

Block any Downloads of a Specific File Type

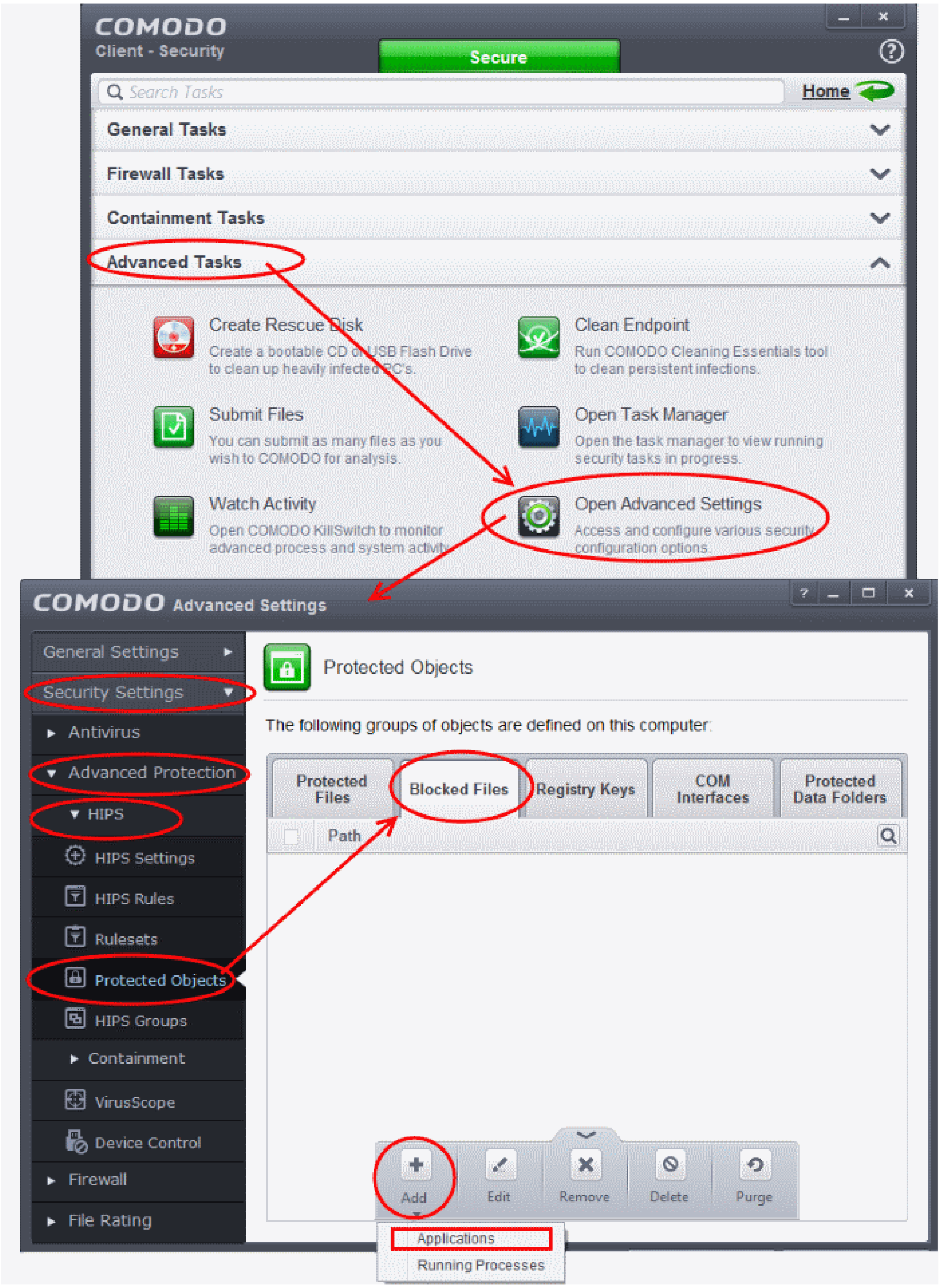
Comodo Client Security can be configured to block downloads of specific types of file. Example scenarios:

- You want to avoid downloading media files like audio files (e.g. files with extensions .wma, .mp3, .wav, .midi), video files (e.g. files with extensions .wmv, .avi, .mpeg, .swf) or image files (e.g. files with extensions .bmp. .jpg, .png) for your disk space restrictions.

To selectively block downloading of specific file type, you need to configure Advanced Protection component of CCS to block the specific file type from the default download folder of your browser.

- 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 in intent then these commands could include the installation of key logging programs, initiation of buffer overflow attacks or 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.

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Advanced Protection' > 'HIPS' > 'Protected Objects' from the left hand side pane
4. Click 'Blocked Files' tab
5. Click the handle from the bottom and choose 'Add' > 'Applications'.
6. Browse to the default download folder for that particular file type of your Internet Browser from the Open dialog



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

Run COMODO Cleaning Essentials tool to clean persistent infections.

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

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

Open COMODO KillSwitch to monitor advanced process and system activity

Access and configure various security configuration options.

The following groups of objects are defined on this computer:

- For example, the default download locations for some file types in Internet Explorer are given below:
  - Executable files - C:\Documents and Settings\user name\Local Settings\Temporary Internet Files\
  - Document files - C:\Documents and Settings\user name\My Documents\
  - Image files - C:\Documents and Settings\user name\My Documents\My Pictures\
  - Music files - C:\Documents and Settings\user name\My Documents\My Music\
  - Video files - C:\Documents and Settings\user name\My Documents\My Videos\

7. Select file from the folder and click 'Open'

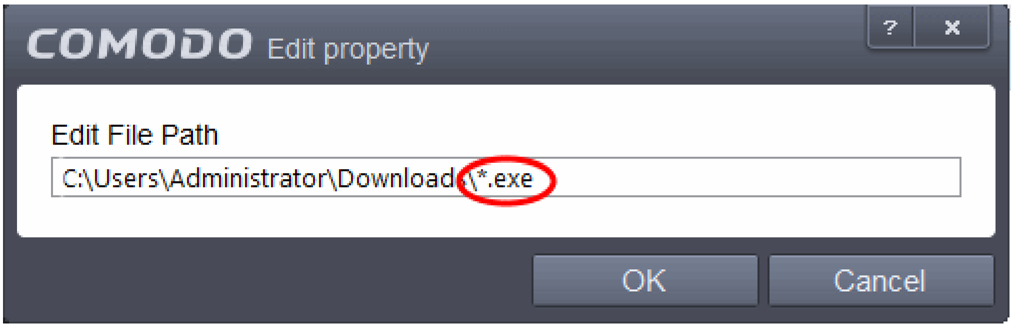
The file will be added to blocked files list. The next step is to edit the file path by adding a wildcard character to the file name in order to block the specific file type from downloading.

To edit an item in the Blocked Files list

1. Select the entry from the Blocked Files interface, click the handle from the bottom and choose 'Edit'

The 'Edit Property' dialog will appear.

2. Change the file name at the end of the file path to *.file_extension” (e.g. *.exe, *.jpg)



Edit File Path

C:\Users\Administrator\Downloads\*.exe

3. Click 'OK' in the 'Edit Property' dialog
4. Click 'OK' in the Advanced Settings interface to save your settings

The download of the specific file type to the specified folder through the browser will be blocked. If you have more than one browser, repeat the same for the other browsers too.

Note: Blocking files in this way will only block the downloads of the specific file types in the specified folders. If you change the download destination while downloading a file through your web browser, the download will be allowed.

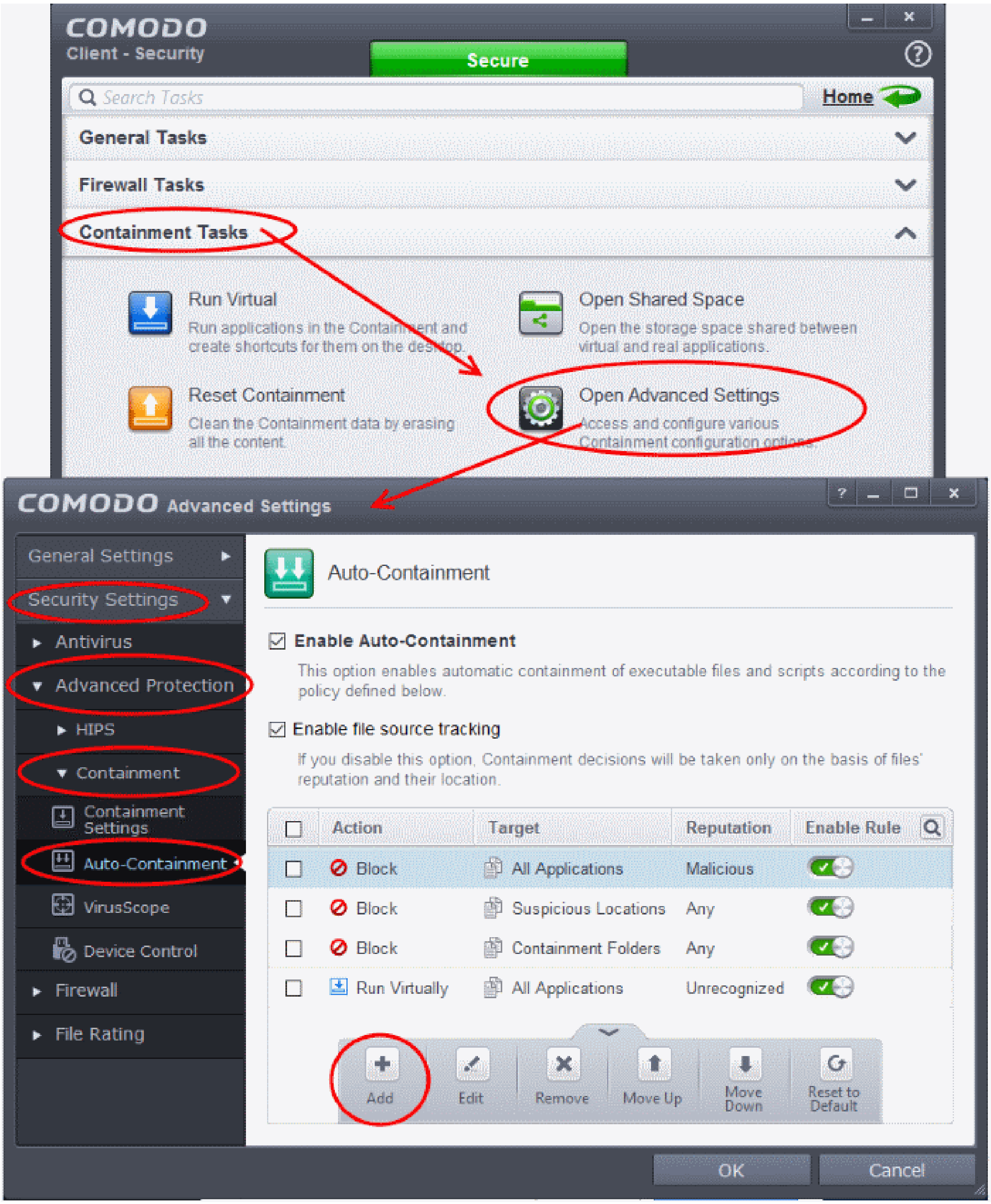
Tip: To unblock the download go to Advanced Settings > Advanced Protection > HIPS > Protected Objects > Blocked Files, select the file path, click the handle from the bottom and choose 'Remove'.

Disable Auto-Containment on a Per-application Basis

The default auto-containment rules will run unknown executables in the container and queue them for submission to Comodo Cloud scanners for behavior analysis. Users do, however, have the option to exclude specific files or file types from this auto-containment process by creating a rule. This is particularly useful for developers that are creating new applications which, by their nature, are as yet unknown to the Comodo safe list.

To disable the auto-containment selectively

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Containment Tasks' and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Advanced Protection' > 'Containment' > 'Auto-Containment' from the left hand side pane
4. Click the handle at the bottom of the interface and open the option panel



Auto-Containment

☑ **Enable Auto-Containment**

This option enables automatic containment of executable files and scripts according to the policy defined below.

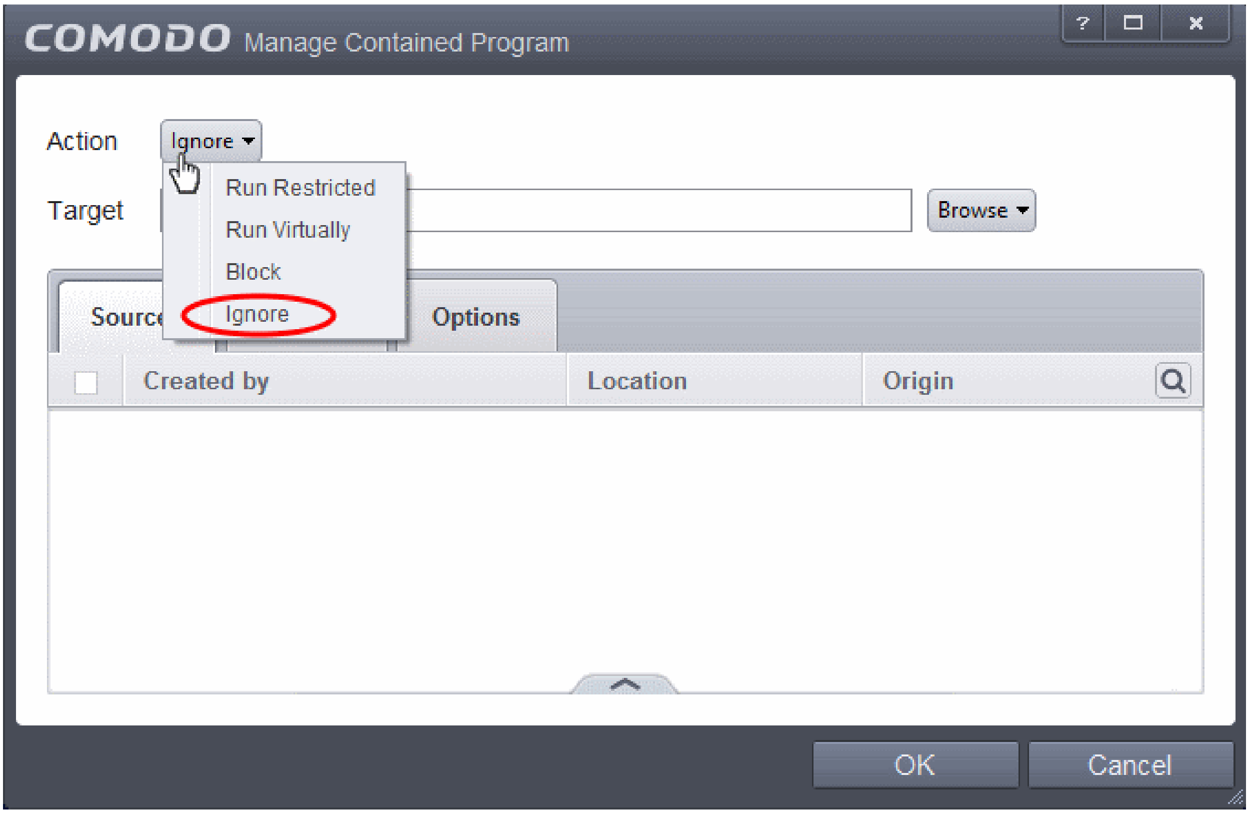
☑ Enable file source tracking

If you disable this option, Containment decisions will be taken only on the basis of files' reputation and their location.

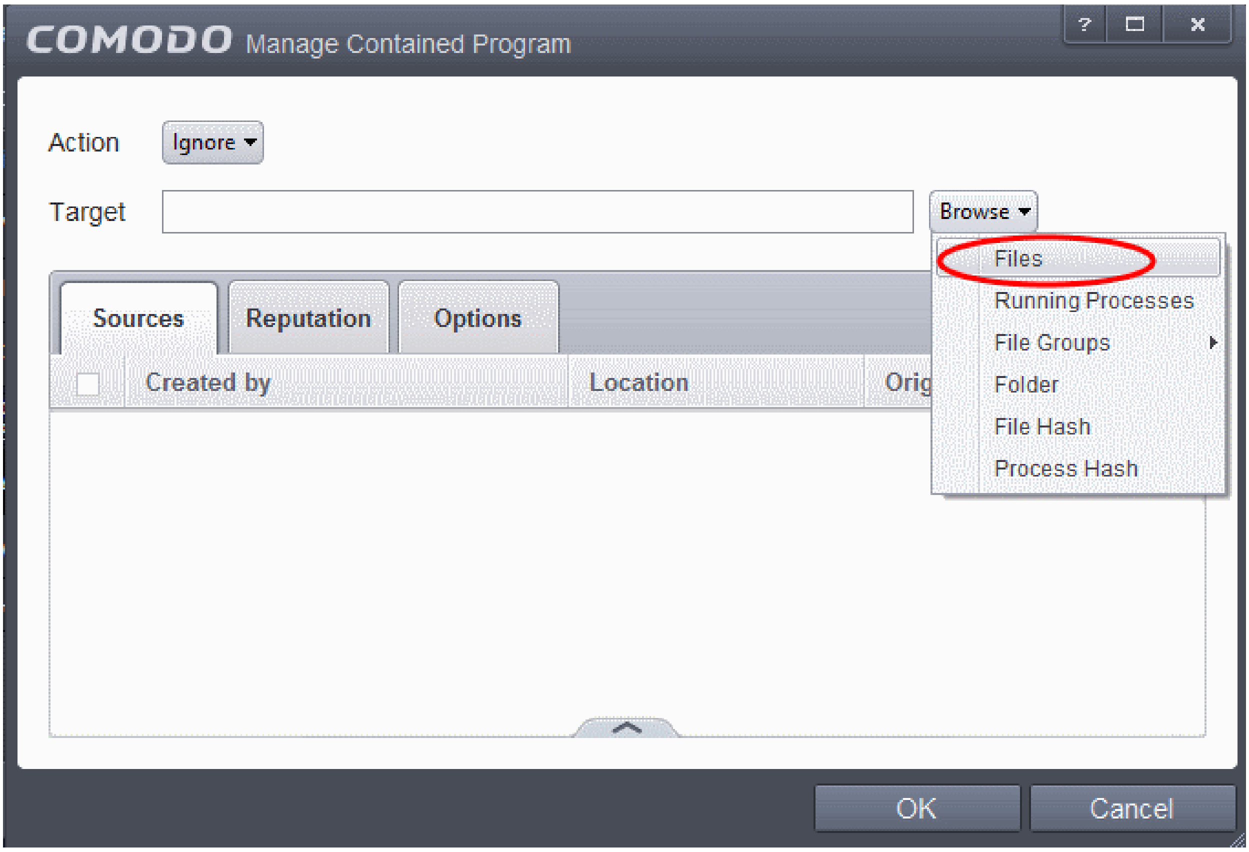
□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malicious	✓
□	Block	Suspicious Locations	Any	✓
□	Block	Containment Folders	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓

Make sure 'Enable Auto-Containment' and 'Enable file source tracking' check boxes are selected.

5. Click the 'Add' button
6. In the 'Manage Contained Program' interface, select 'Ignore' from the 'Action' drop-down options:

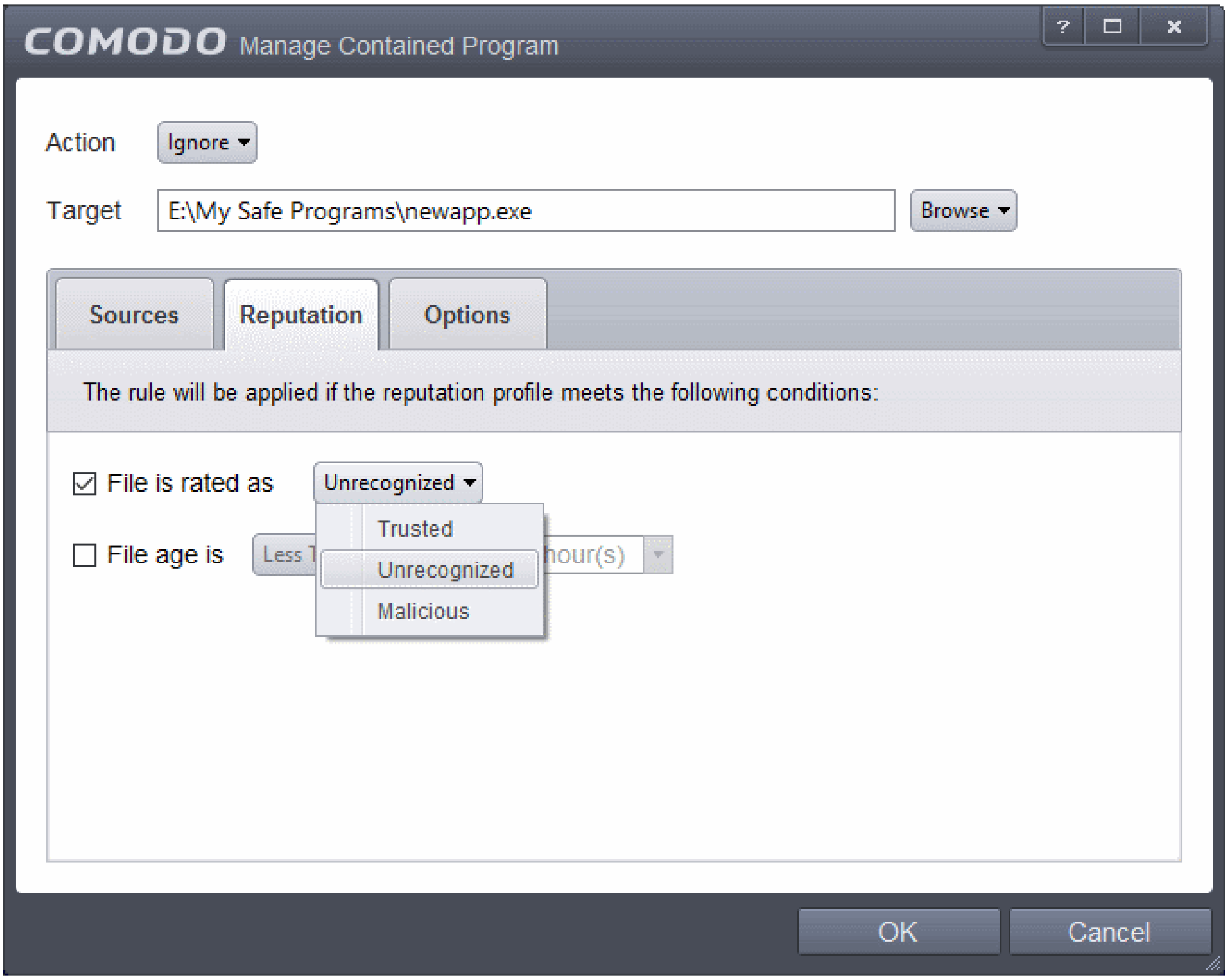


7. By default the Source tab will be selected. Click the Browse button beside the Target field then click Files from the options.



8. Navigate to the location where is the application is installed or stored, select it and click 'Open'. Click here for details about adding to target from other options.

9. Click the Reputation tab, select the checkbox beside 'File is rated as' and click 'Unrecognized' from the drop-down options.



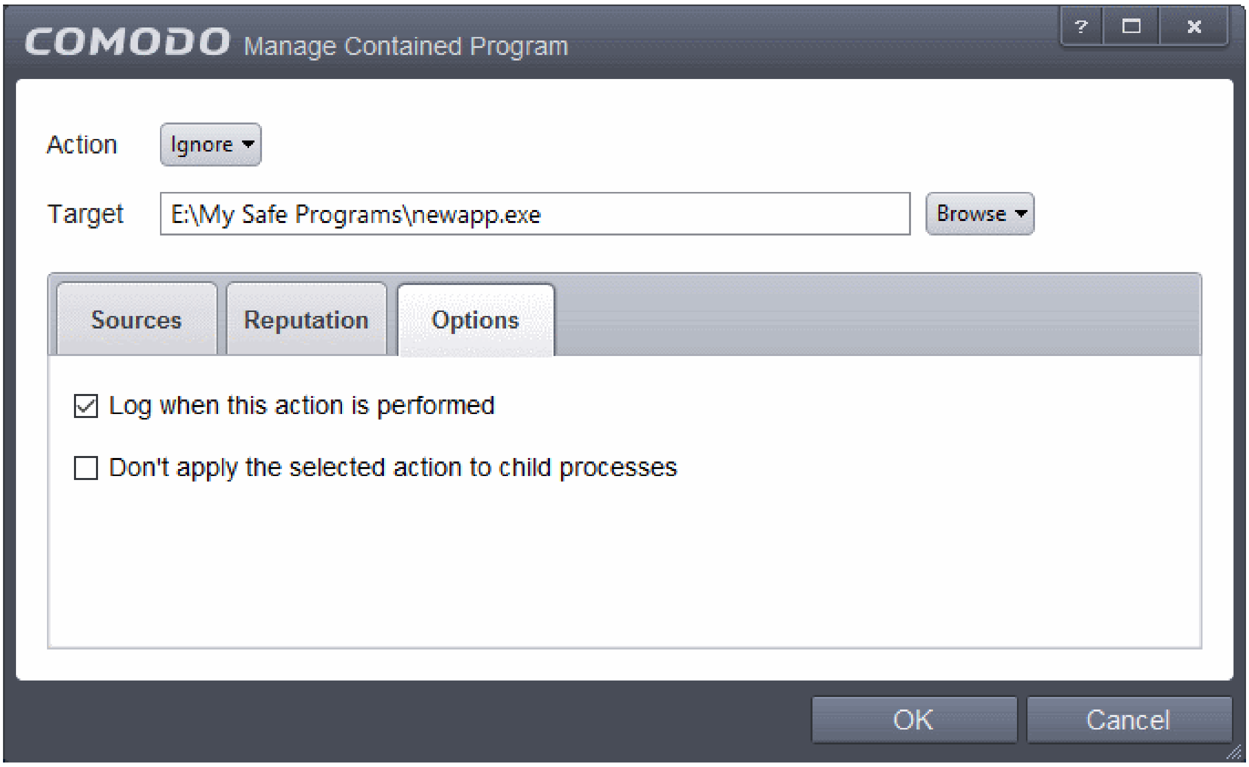
E:\My Safe Programs\newapp.exe

The rule will be applied if the reputation profile meets the following conditions:

☑ File is rated as Unrecognized

□ File age is

10. Click the 'Options' tab.



E:\My Safe Programs\newapp.exe

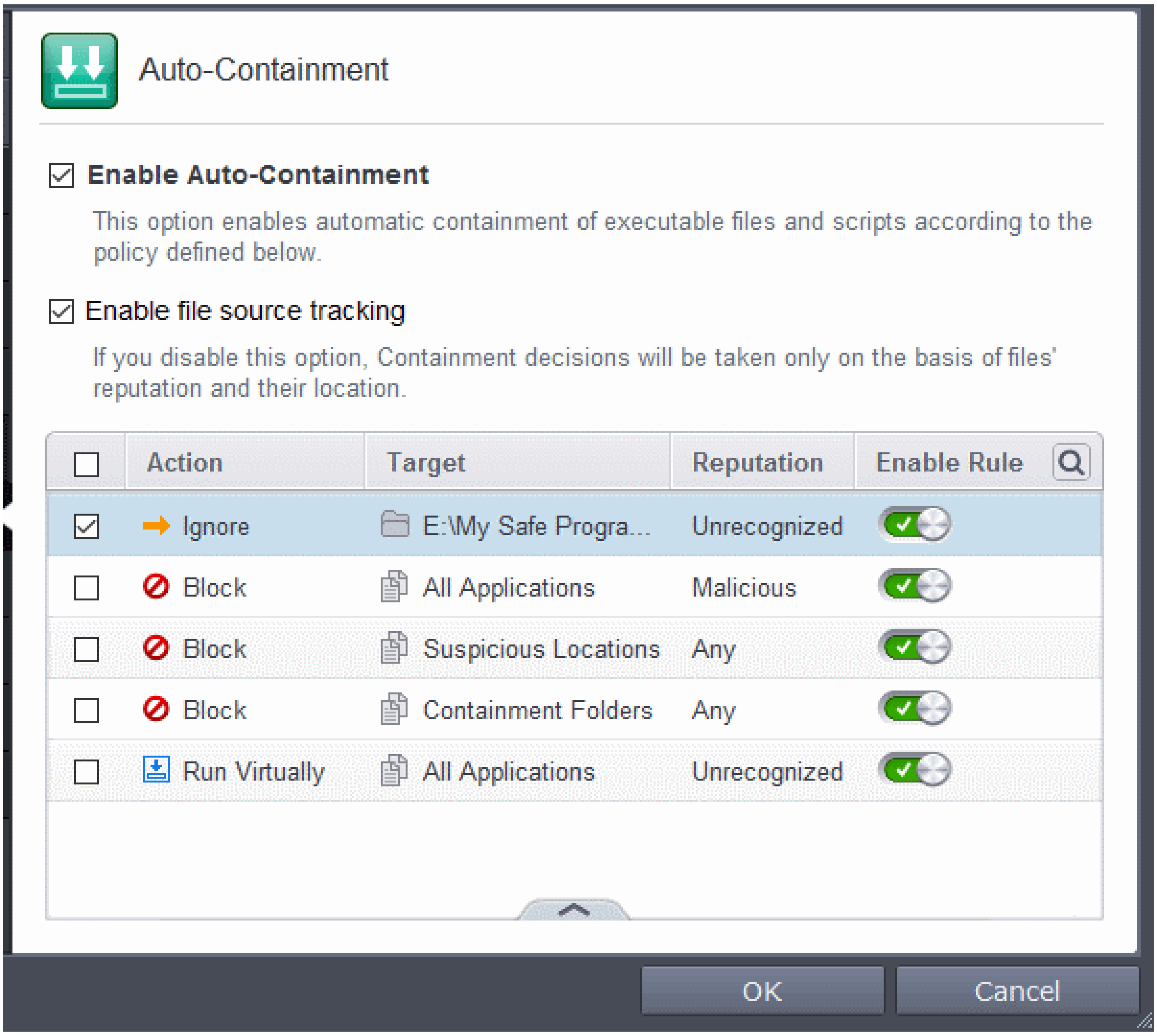
☑ Log when this action is performed

□ Don't apply the selected action to child processes

By default, 'Log when this action is performed' will be selected.

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **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.

11. Select the options as required and click 'OK'.



Auto-Containment

☑ **Enable Auto-Containment**

This option enables automatic containment of executable files and scripts according to the policy defined below.

☑ Enable file source tracking

If you disable this option, Containment decisions will be taken only on the basis of files' reputation and their location.

□	Action	Target	Reputation	Enable Rule
☑	Ignore	E:\My Safe Progra...	Unrecognized	✓
□	Block	All Applications	Malicious	✓
□	Block	Suspicious Locations	Any	✓
□	Block	Containment Folders	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓

The Ignore rule will be saved for the specified application and displayed in the Auto-Containment' screen. Make sure to keep this rule above all other rules for unrecognized files.

Alternatively...

1. Assign Trusted rating to the file from 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 **Trusted Software Vendors** list

3. Disable Auto-Containment by de-selecting the 'Enable Auto-Containment' check box in the Auto-Containment settings panel. *Not recommended*.

For more details on creating rules for auto-containment, refer to the section Configuring Rules for Auto-Containment.

Switch Off Automatic Antivirus and Software Updates

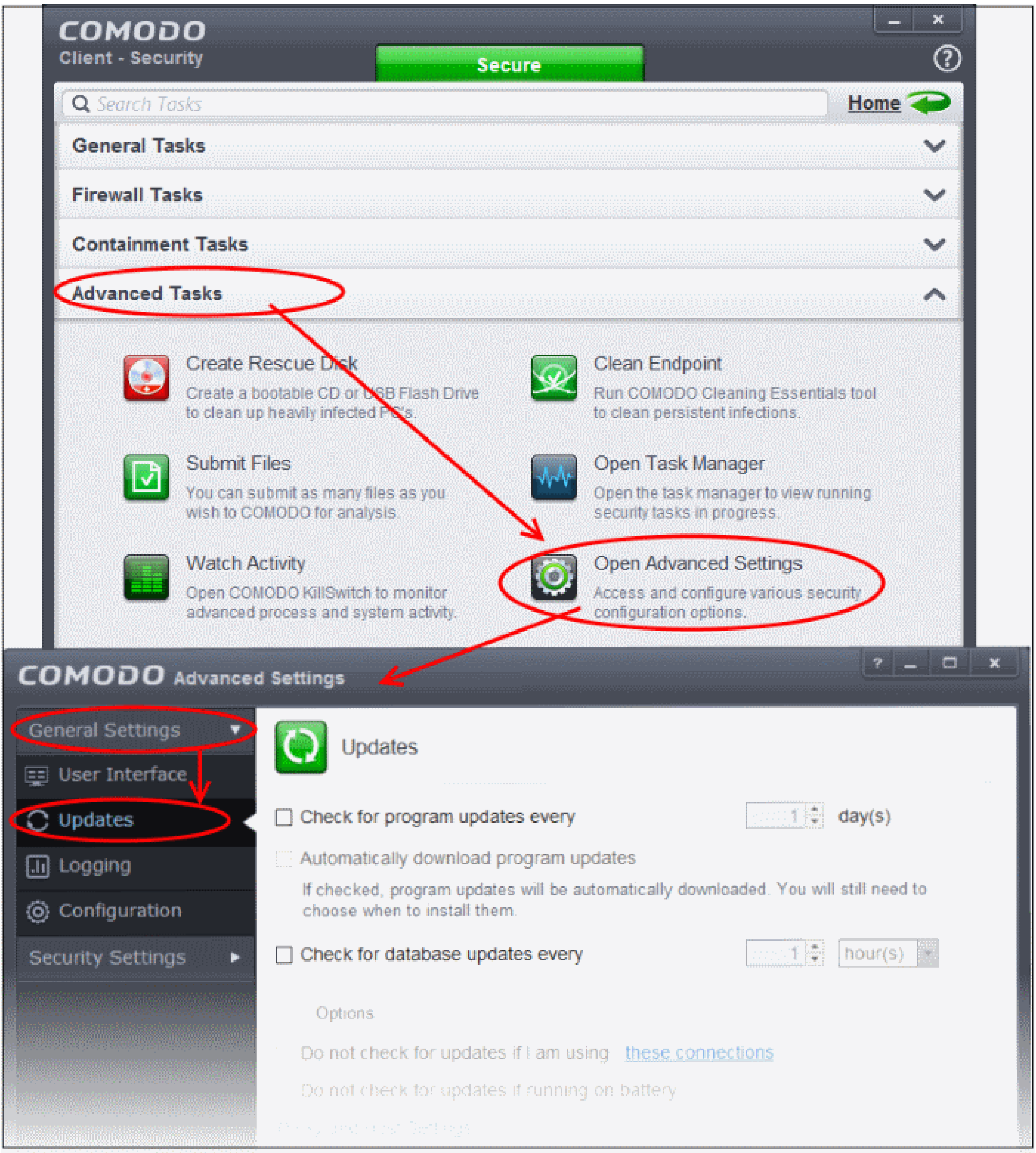
By default, Comodo Client Security will automatically check for software and Antivirus database updates. However, some users like to have control over what gets downloaded and when it gets downloaded. For example, network administrators may not wish to automatically download because it will take up to much bandwidth during the day. Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.

CCS provides full control over virus and software updates. Click the appropriate link below to find out more:

- Switch off automatic software and virus signature database updates entirely
- Switch off automatic software and virus signature database selectively
- Switch off automatic virus signature database updates prior to Antivirus Scans

To switch off automatic updates entirely:

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' then click 'Open Advanced Settings'
3. Click 'General Settings' > 'Updates' on the left menu
4. Deselect the check boxes 'Check for program updates every xxx day(s)' and 'Check for database updates every xxx hour(s)'



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

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

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

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

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

Open Advanced Settings
Access and configure various security configuration options.

☐ Check for program updates every 1 day(s)

☐ Automatically download program updates

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

☐ Check for database updates every 1 hour(s)

Options

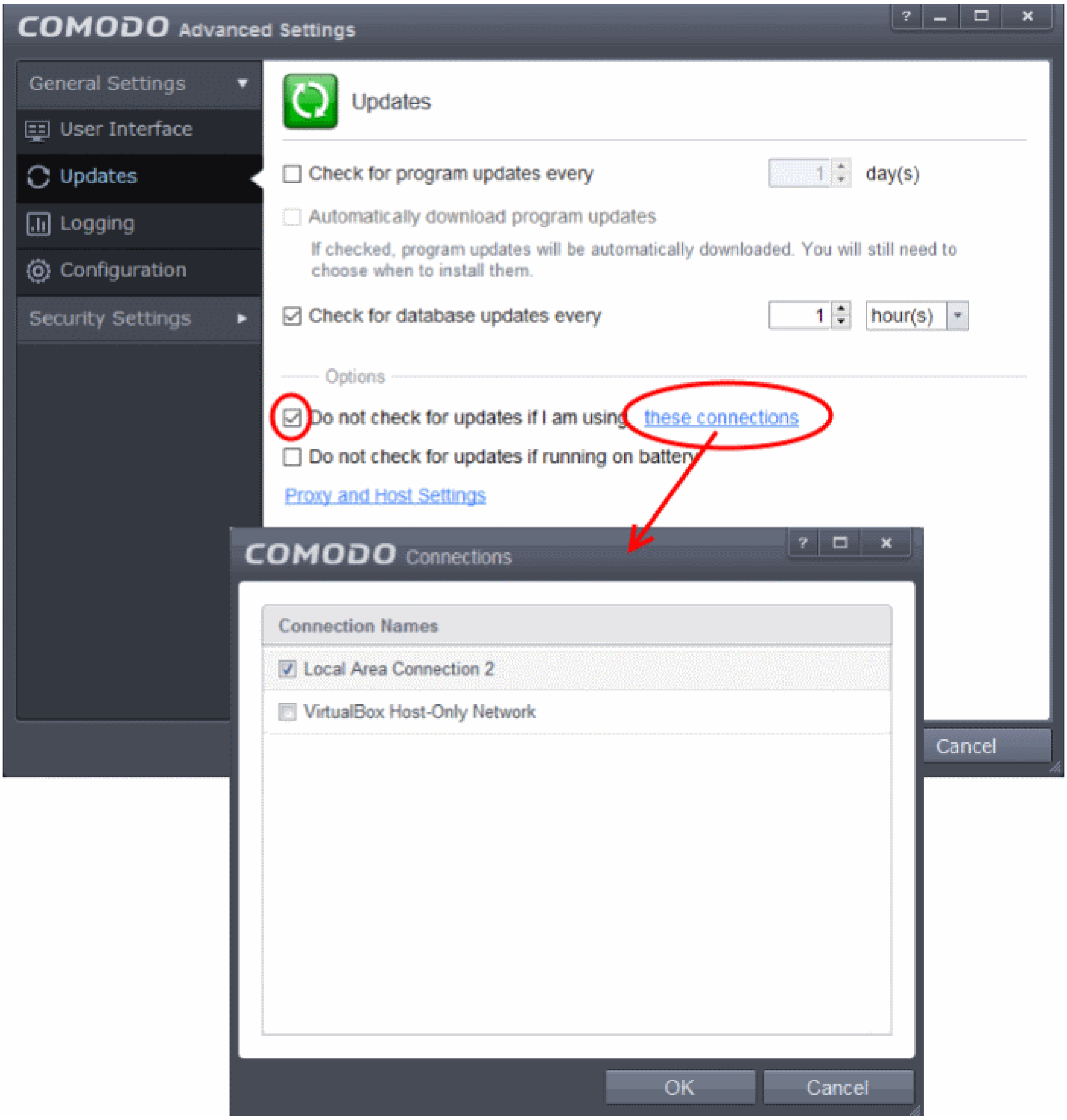
Do not check for updates if I am using these connections

Do not check for updates if running on battery

5. Click 'OK' in the 'Advanced Settings' panel.

To switch off automatic updates selectively:

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' then click 'Open Advanced Settings'
3. Click 'General Settings' > 'Updates' on the left menu



Updates

☐ Check for program updates every 1 day(s)

☐ Automatically download program updates

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

☑ Check for database updates every 1 hour(s)

Options

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

☐ Do not check for updates if running on battery

Proxy and Host Settings

Connection Names

☑ Local Area Connection 2

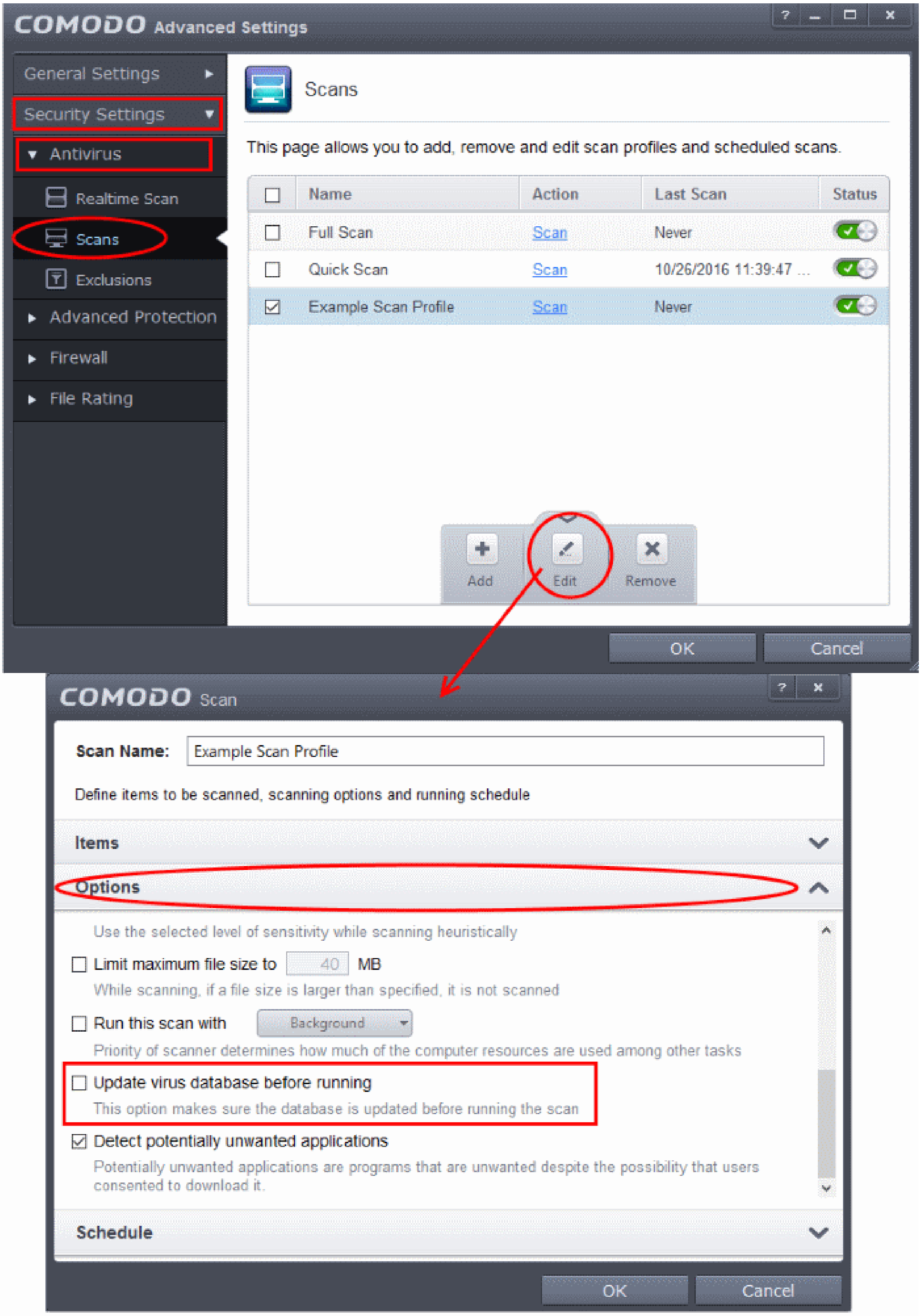
☐ VirtualBox Host-Only Network

- 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' link. 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' check box

To switch off automatic virus signature database updates prior to AV Scans:

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' then click 'Open Advanced Settings'
3. Click 'Security Settings' > Antivirus' > 'Scans'. A list of defined scan profiles will appear.

4. Select the scan profile for which you do not want the automatic virus database updates prior to the scan
5. Click the handle at the bottom of the interface and select 'Edit'



Scans

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

☐	Name	Action	Last Scan	Status
☐	Full Scan	Scan	Never	✓
☐	Quick Scan	Scan	10/26/2016 11:39:47 ...	✓
☑	Example Scan Profile	Scan	Never	✓

Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Use the selected level of sensitivity while scanning heuristically

☐ Limit maximum file size to 40 MB

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

☐ Run this scan with Background

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

☐ Update virus database before running

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

☑ Detect potentially unwanted applications

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

6. In the 'Scan' interface, click 'Options' and deselect 'Update virus database before running' check box.
7. Click 'OK' on the 'Scan' interface.
8. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

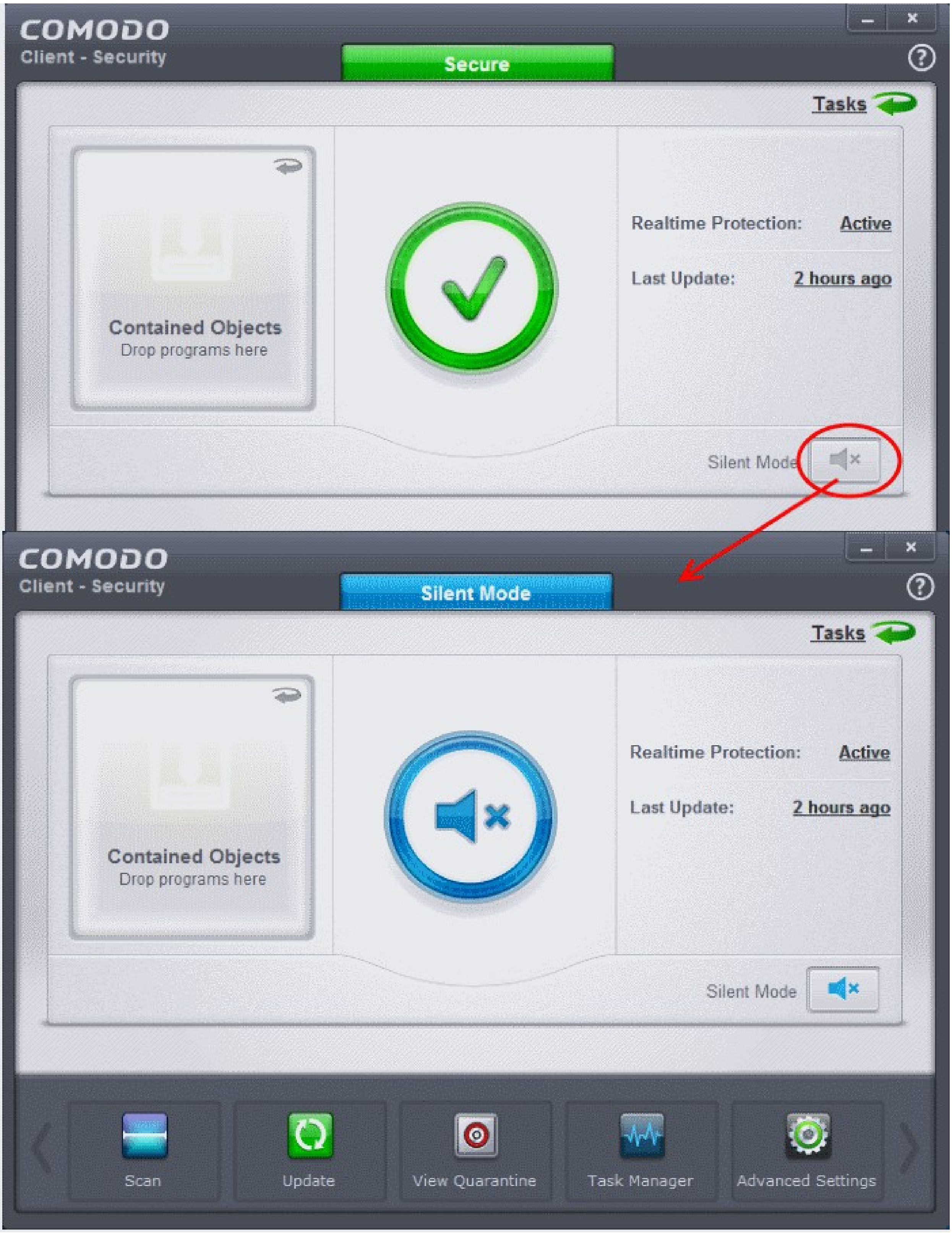
Suppressing CCS Alerts Temporarily

Because of continuous monitoring of all your system activities in granular level for implementing Default-Deny Protection, Comodo Client Security generates pop-up alerts whenever it identifies any event appearing to be a malicious activity or execution of programs that require privileges like Internet access and file access rights. Each alert provides information and options that enable you to make an informed decision on whether you want to allow or block a request or activity. Alerts also to allow you to instruct Comodo Client Security on how it should behave in future when it encounters activities of the same type.

But at times when you are involved in activities that require undisturbed environment, you can temporarily stop them from being displayed. During this time, the operations that can interfere with users' workflow experience are either suppressed or postponed.

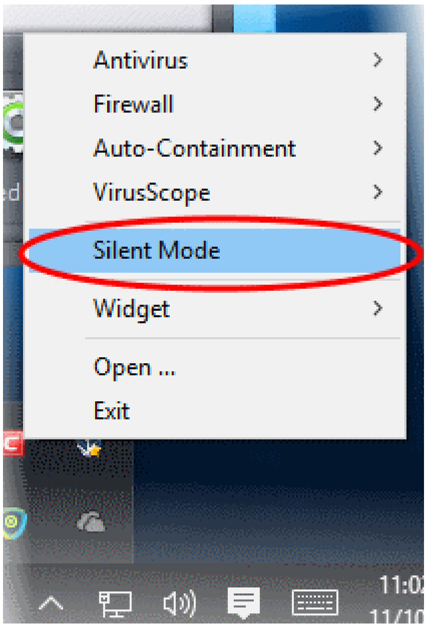
To temporarily stop pop-up alerts

- Click 'Silent Mode' button from CCS Home screen



OR

- Right click on the CCS System Tray icon and select 'Silent Mode' from the options.

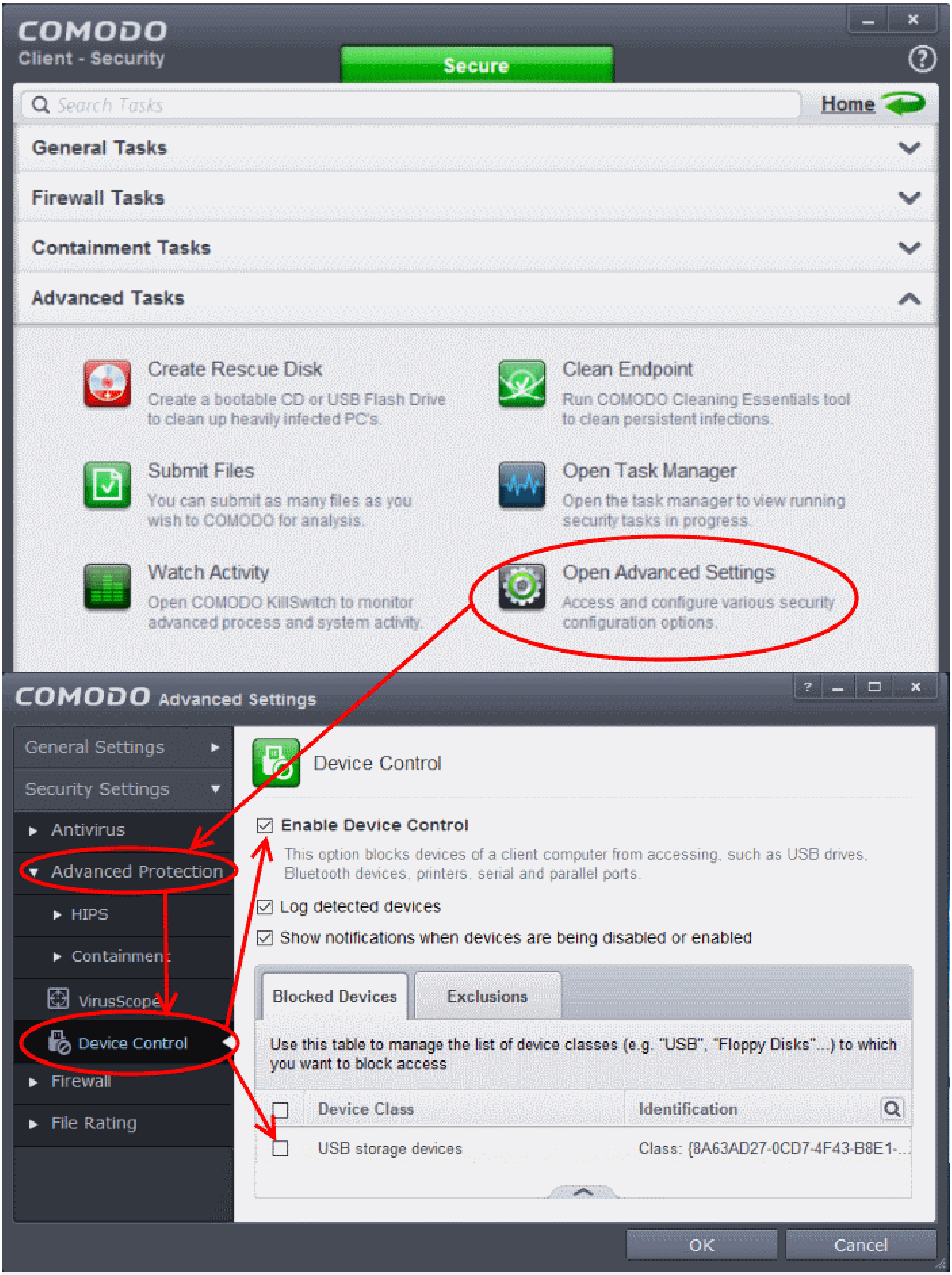


The alerts are now suppressed. To resume alerts and scheduled scans, just de-activate Silent Mode from the home screen or the system tray icon right click options.

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, click: Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Advanced Protection > Device Control:



COMODO
Client - Security
Secure
Search Tasks
Home
General Tasks
Firewall Tasks
Containment Tasks
Advanced Tasks
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
Open Task Manager
Open the task manager to view running security tasks in progress.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
Open Advanced Settings
Access and configure various security configuration options.
COMODO Advanced Settings
General Settings
Security Settings
Antivirus
Advanced Protection
HIPS
Containment
VirusScope
Device Control
Firewall
File Rating
Blocked Devices
Exclusions
OK
Cancel

Device Control

☑ Enable Device Control

This option blocks devices of a client computer from accessing, such as USB drives, Bluetooth devices, printers, serial and parallel ports.

☑ Log detected devices

☑ Show notifications when devices are being disabled or enabled

Use this table to manage the list of device classes (e.g. "USB", "Floppy Disks"...) to which you want to block access

□	Device Class	Identification
□	USB storage devices	Class: {8A63AD27-0CD7-4F43-B8E1-...

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 Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Router by modifying the DNS settings accessible through DNS Server settings of your router. Comodo recommends making the change on your router so that with one change, all the computers on your network can benefit from Comodo Secure DNS.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Primary DNS : 8.26.56.26

Secondary DNS : 8.20.247.20

To stop Comodo Secure DNS service

- Modify the DNS server IP address to your previous settings.

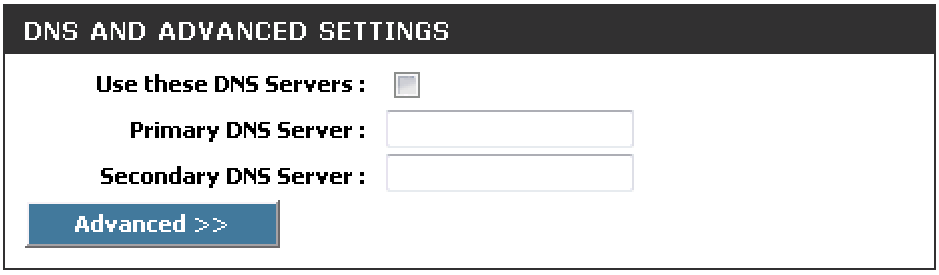
To modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

   http://192.168.0.1
   http://192.168.1.1
   http://192.168.10.1

   If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).



DNS AND ADVANCED SETTINGS

Use these DNS Servers : □

Primary DNS Server :

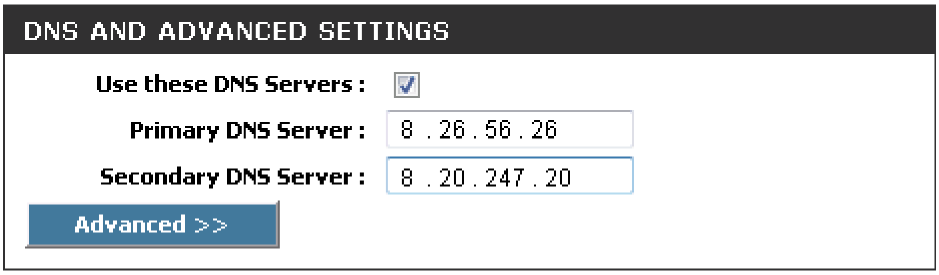
Secondary DNS Server :

3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

   Primary DNS server address for Comodo Secure DNS is: 8.26.56.26

   Secondary DNS server address for Comodo Secure DNS is: 8.20.247.20

   When you are done, the above example would look like this.



DNS AND ADVANCED SETTINGS

Use these DNS Servers : ☑

Primary DNS Server : 8 . 26 . 56 . 26

Secondary DNS Server : 8 . 20 . 247 . 20

You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.

Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Windows XP computer by modifying the DNS settings accessible through Control Panel > Network Connections.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Preferred DNS : 8.26.56.26

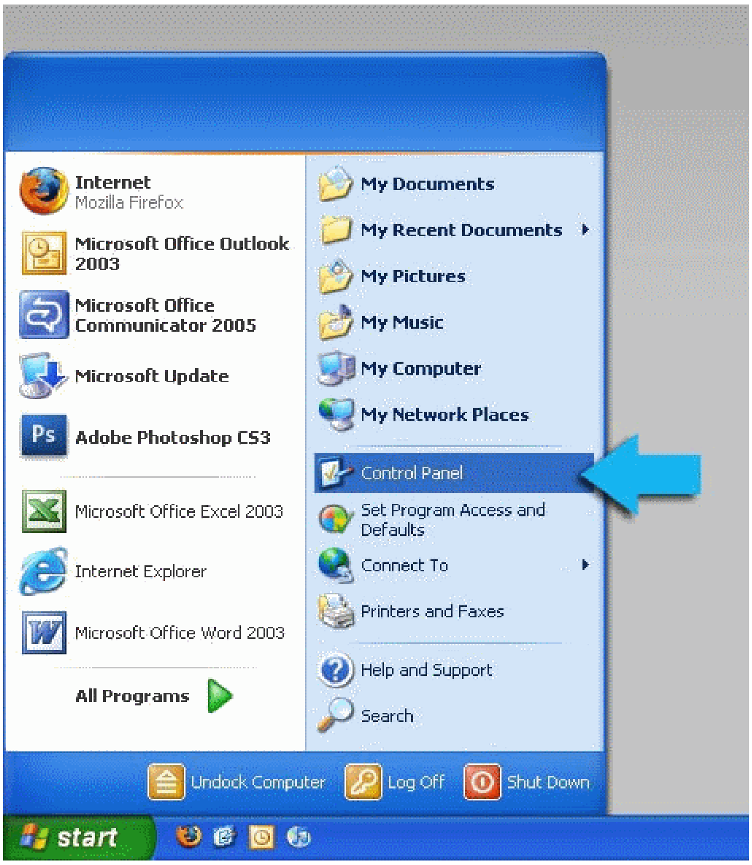
Alternate DNS : 8.20.247.20

To stop Comodo Secure DNS service

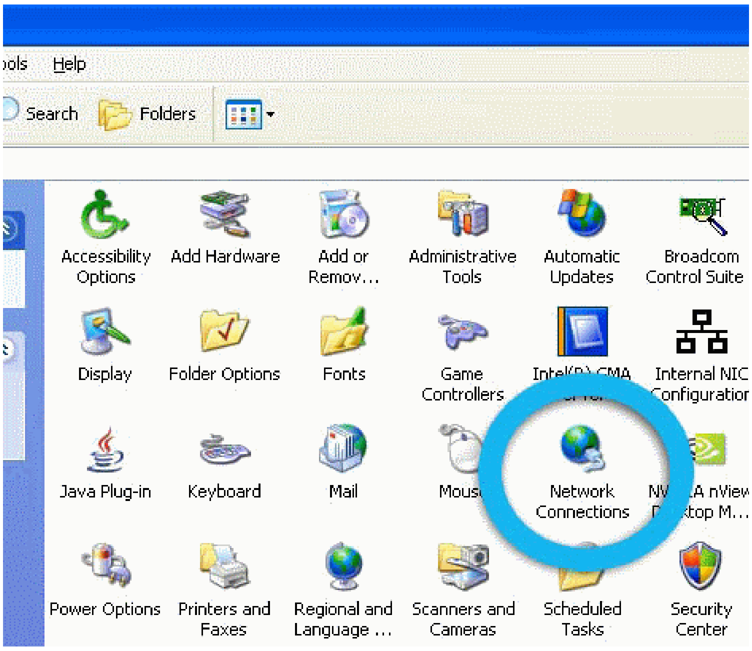
- Modify the DNS server IP address to your previous settings.

To modify the DNS settings

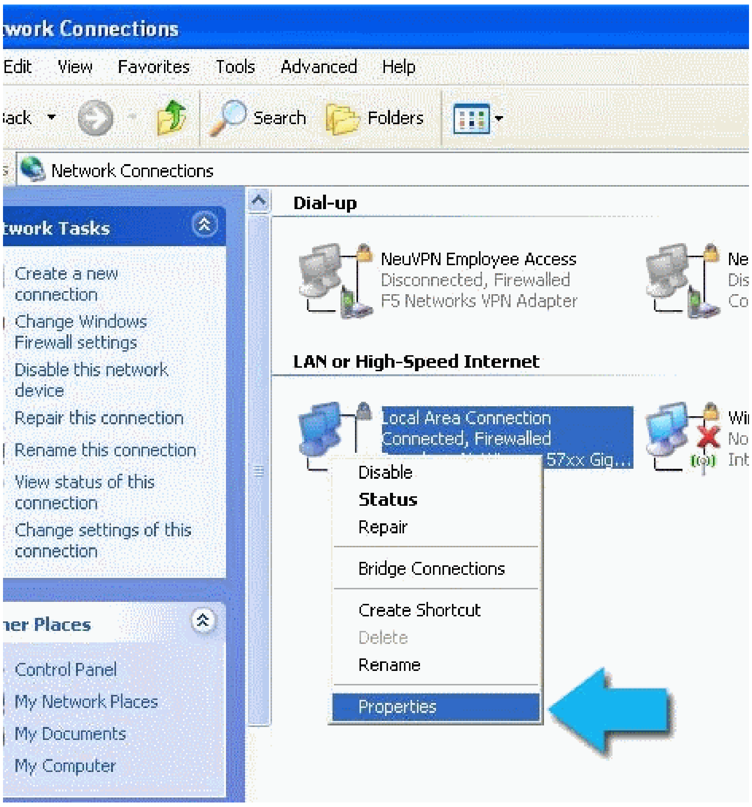
1. Select the 'Control Panel' from the Start Menu.



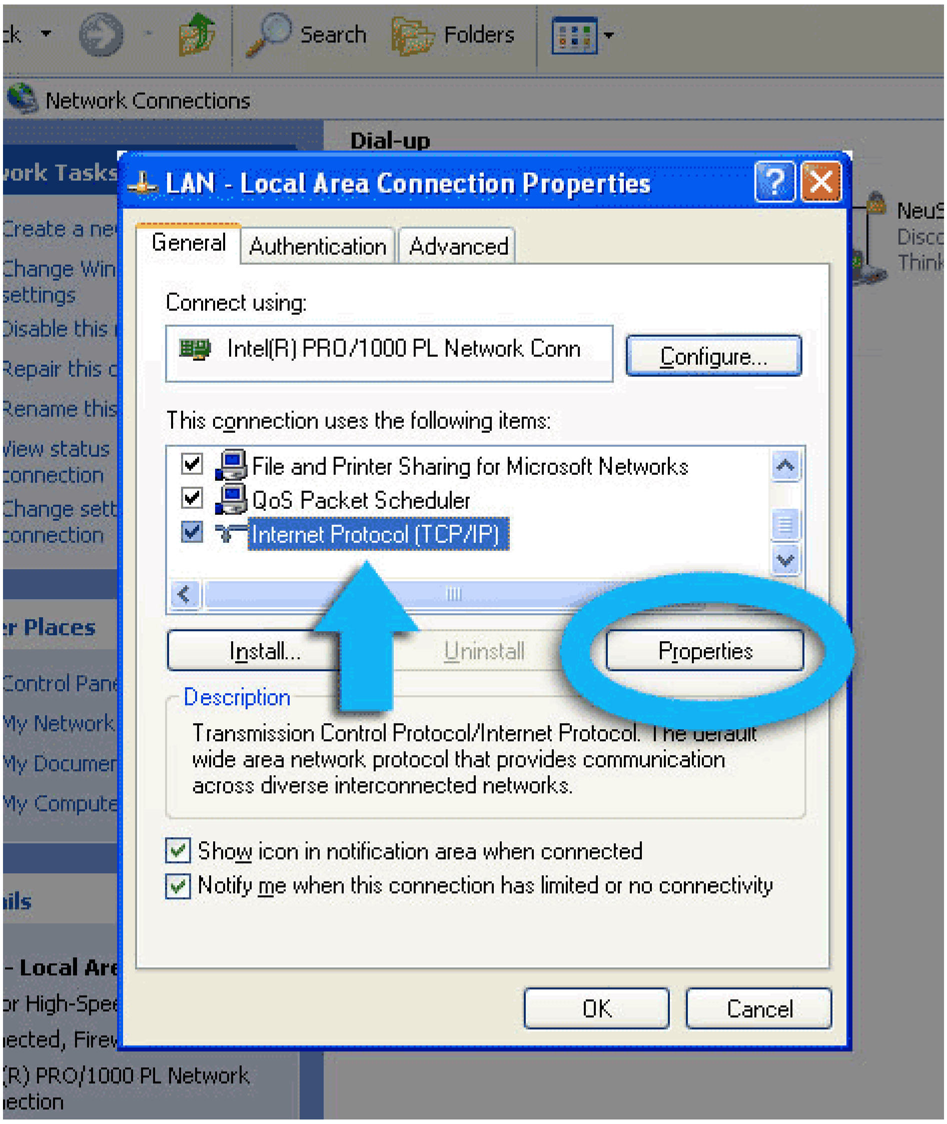
2. Click 'Network Connections' from the Control Panel options.



3. Right click on your connection from the Network Connections window and click 'Properties'.



4. Select 'Internet Protocol (TCP/IP)' and click 'Properties'.



LAN - Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Intel(R) PRO/1000 PL Network Conn

Configure...

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

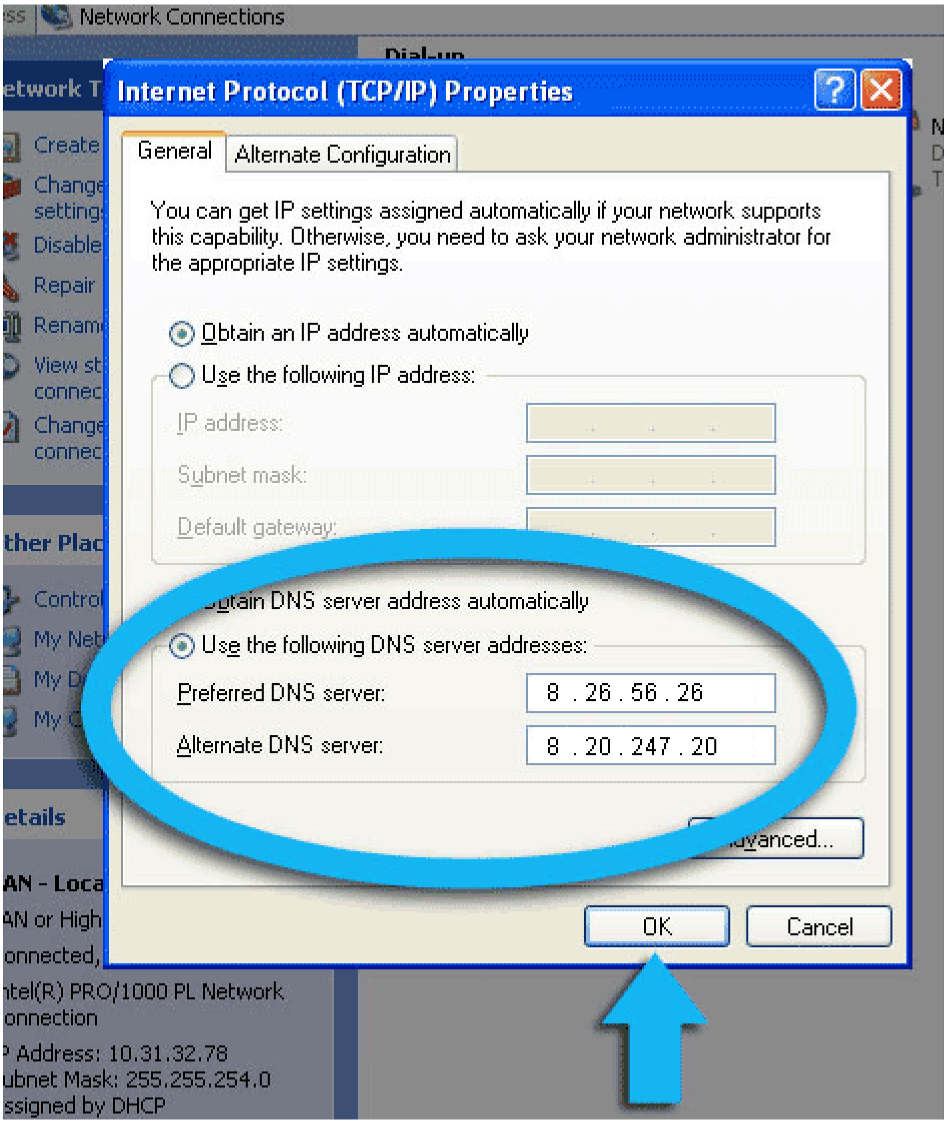
OK | Cancel

5. Click the radio button Use the following DNS server addresses and type in Comodo Secure DNS addresses in the Preferred DNS server and Alternate DNS server fields.

   Please note down your current DNS settings before switching to Comodo Secure DNS, in case you want to return to your old settings for any reason.

   Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26

   Alternate DNS server address for Comodo Secure DNS is: 8.20.247.20



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 26 . 56 . 26

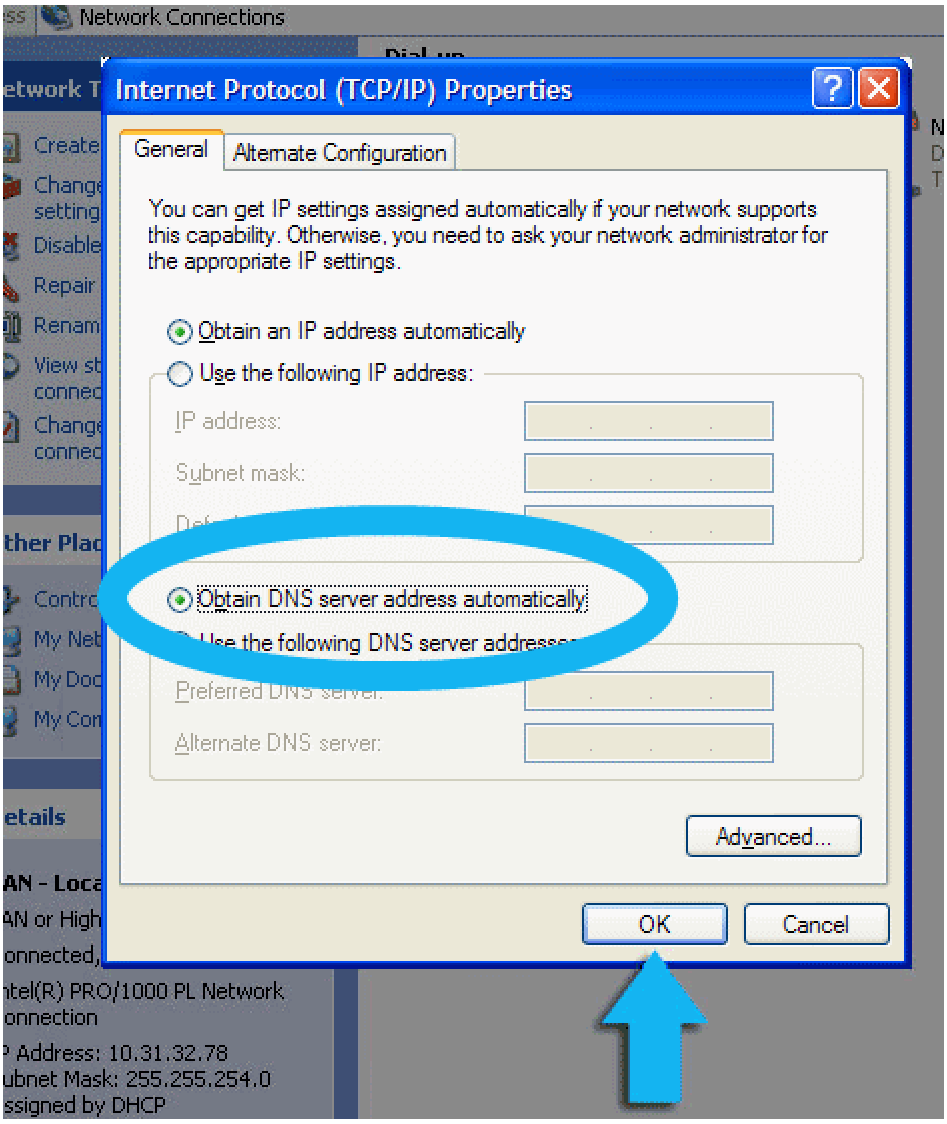
Alternate DNS server: 8 . 20 . 247 . 20

You can disable Comodo Secure DNS by:

- Selecting 'Obtain DNS server address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable the Comodo Secure DNS service by changing your DNS server addresses to:

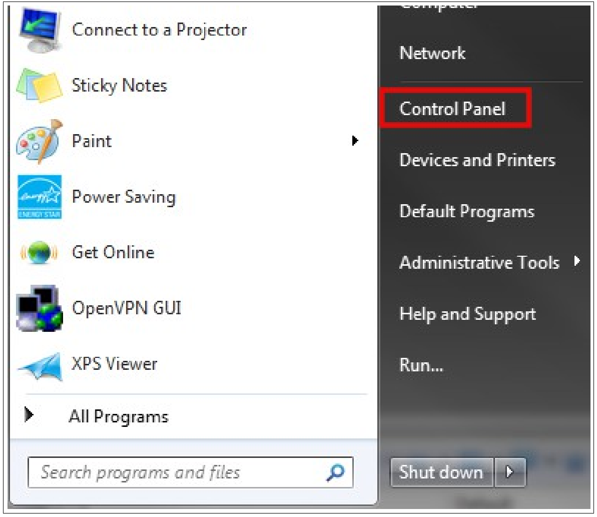
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

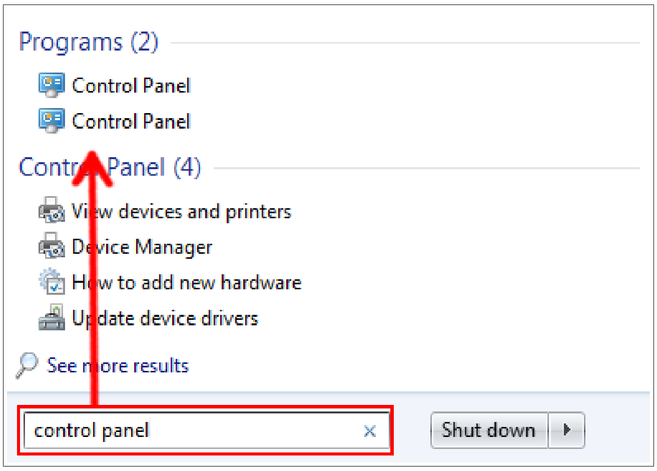
Enabling Comodo DNS in Windows 7 / Vista

Disabling Comodo DNS in Windows 7 / Vista

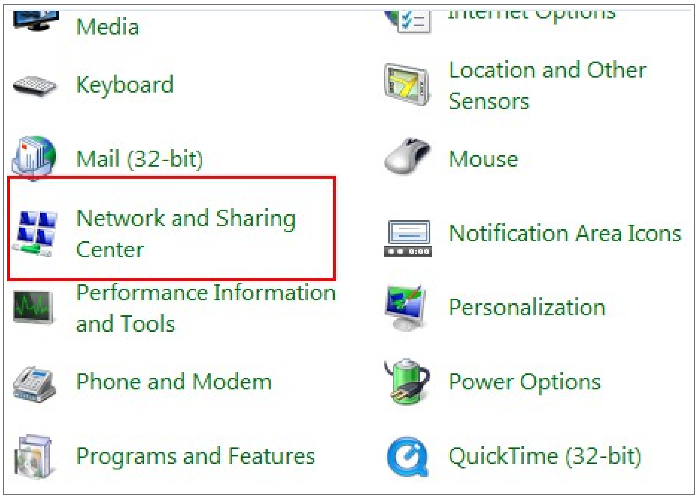
Enabling Comodo DNS in Windows 7 / Vista

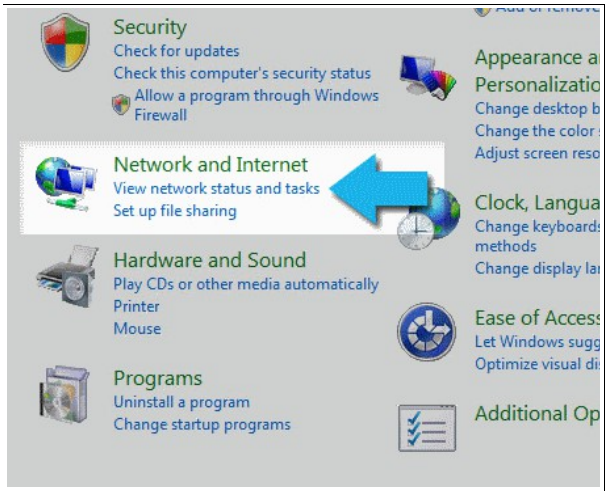
1. Open the control panel by either selecting it from the Windows 'Start' menu or by typing 'control panel' into the search box then clicking the program name.



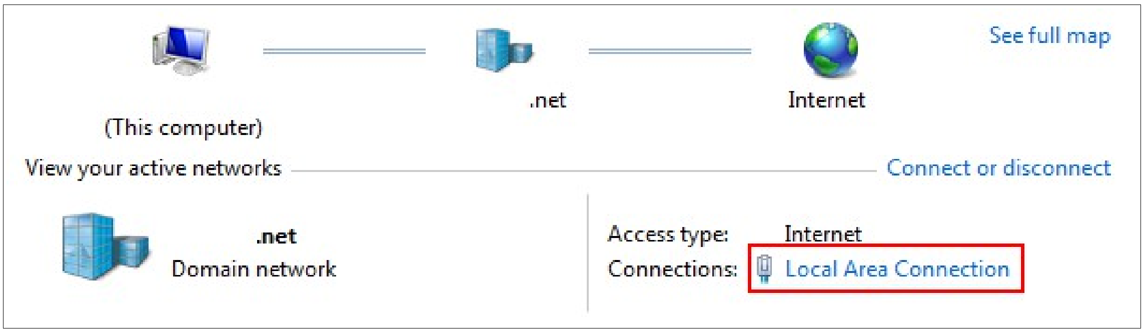


2. From the control panel menu, select 'Network and Sharing Center' (Windows 7) or 'Network and Internet (Vista):

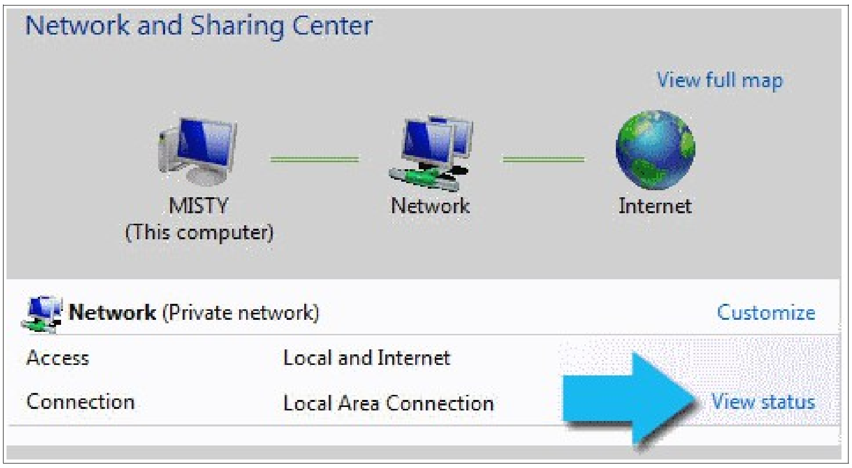




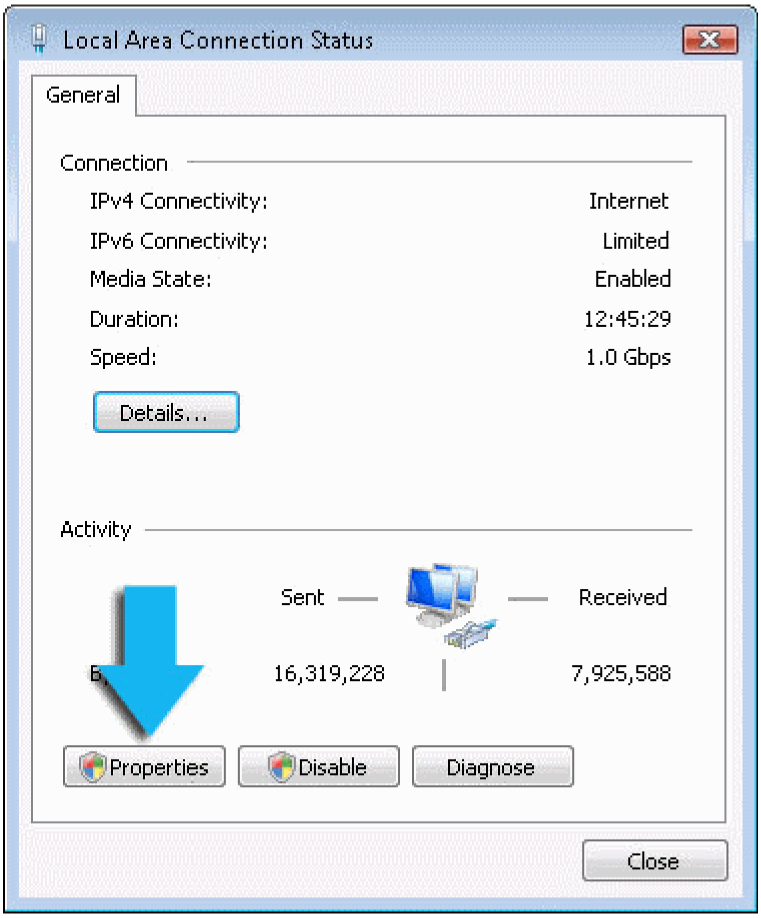
3. In the Network and Sharing center, click the connection type next to 'Connections' (Windows 7):



or 'View Status' (Vista):

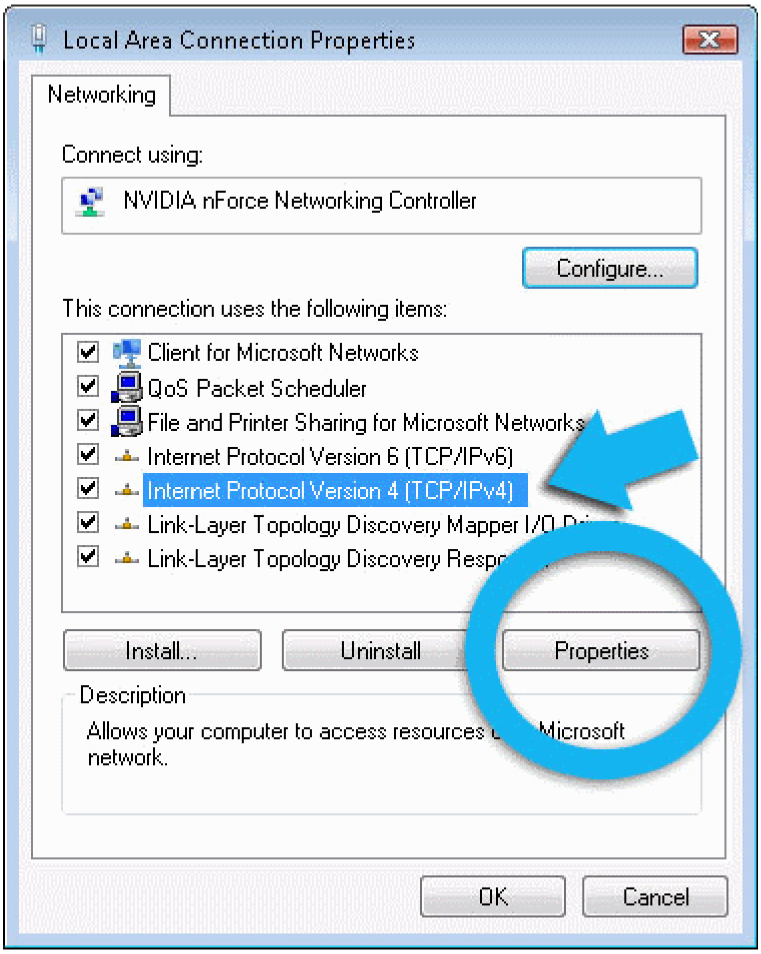


4. This will open the 'Local Area Connection Status' dialog. Click the 'Properties' button:



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:



Local Area Connection Properties

Networking

Connect using:

NVIDIA nForce Networking Controller

This connection uses the following items:

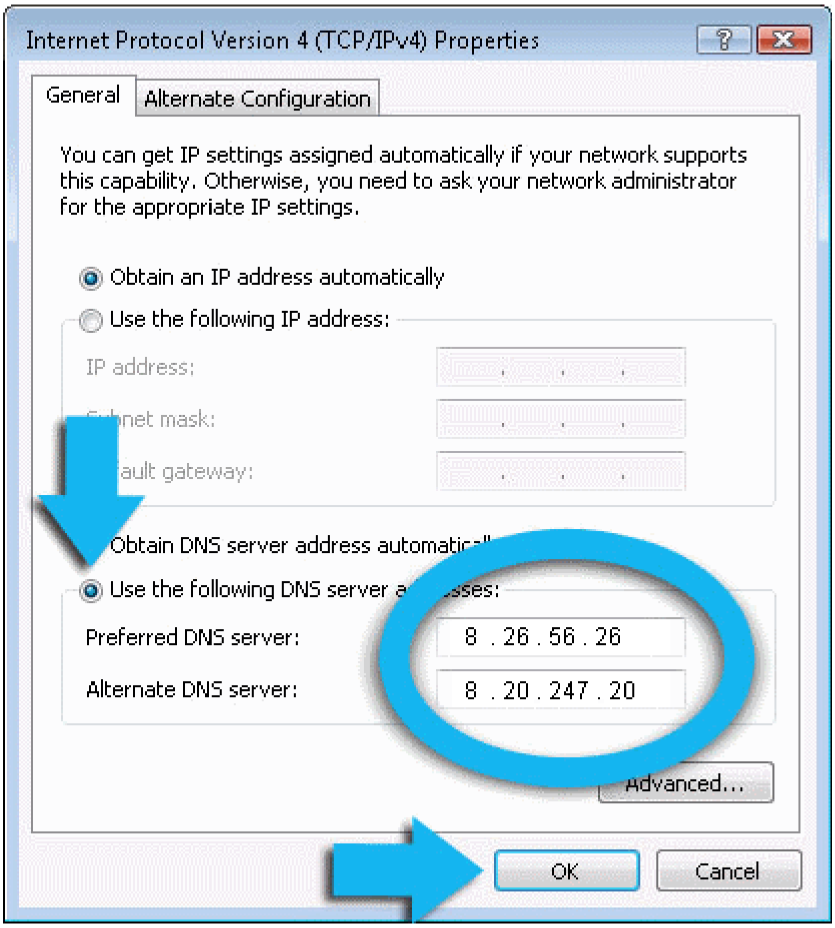
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Dri
☑ Link-Layer Topology Discovery Respo

Description

Allows your computer to access resources o Microsoft network.

6. Enable 'Use the following DNS server addresses'. Doing so will allow you to enter the addresses of Comodo DNS servers in the fields provided. Enter the addresses listed below then click 'OK' to activate your settings:

   - Preferred DNS : 8.26.56.26
   - Alternate DNS : 8.20.247.20



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 26 . 56 . 26

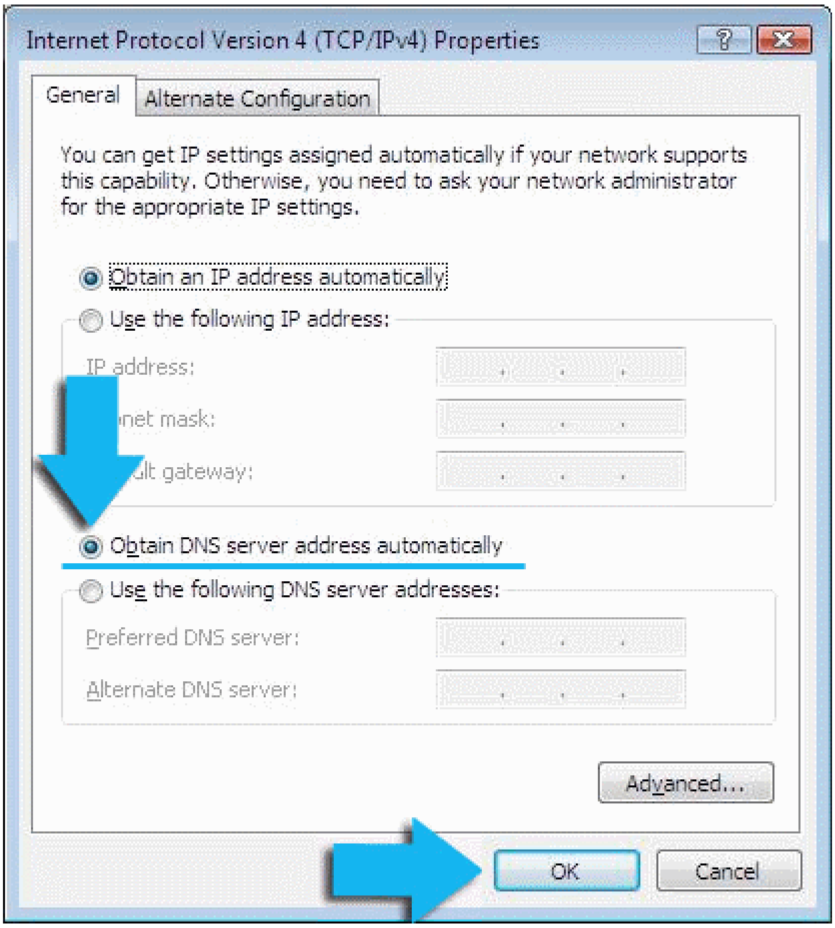
Alternate DNS server: 8 . 20 . 247 . 20

Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the Internet.

Disabling Comodo DNS in Windows 7 / Vista

To disable Comodo DNS, you need to instruct Windows to automatically obtain the address of a DNS server. Doing so means you will use the DNS server provided by your ISP. To do this:

- Follow steps 1 to 7 of the '**Enabling Comodo DNS in Windows 7 / Vista**' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

About Comodo

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

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

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