Comodo Client Security

Software Version 12.4

User Guide

Guide Version 12.4.071020

Table of Contents

1. Introduction to Comodo Client Security....6
1.1.Special Features....10
1.2.System Requirements....12
1.3.Install Comodo Client Security....13
1.4.Start Comodo Client Security....23
1.5.The Main Interface....27
1.5.1.The Home Screen....28
1.5.2.The Tasks Interface....35
1.5.3.The Widget....36
1.5.4.The System Tray Icon....37
1.6.Understand Security Alerts....40
1.7.Password Protection....62
2. General Tasks - Introduction....63
2.1.Scan and Clean Your Computer....64
2.1.1.Run a Quick Scan....66
2.1.2.Run a Full Computer Scan....68
2.1.3.Run a Rating Scan....72
2.1.4.Run a Custom Scan....76
2.1.4.1.Scan a Folder....76
2.1.4.2.Scan a File....78
2.1.4.3.Create, Schedule and Run a Custom Scan....80
2.1.5.Automatically Scan Unrecognized and Quarantined Files....90
2.2.Instantly Scan Files and Folders....93
2.3.Process Infected Files....95
2.4.Manage Virus Database Updates....99
2.5.Manage Blocked Autoruns....103
2.6.Manage Quarantined Items....106
3. Firewall Tasks - Introduction....110
3.1.Configure internet access rights for applications....111
3.2.Stealth your Computer Ports....113
3.3.Manage Network Connections....115
3.4.Stop all Network Activities....116
3.5.View Active Internet Connections....118
4. Containment Tasks - Introduction....121
4.1.Run an Application in the Container....123
4.2.Reset the Container....126
4.3.Identify and Kill Unsafe Running Processes....128
4.4.Open Shared Space....130
4.5.The Virtual Desktop....131
4.5.1.Start the Virtual Desktop....133
4.5.2.The Main Interface....139

4.5.3.Run Browsers inside the Virtual Desktop....142
4.5.4.Open Files and Run Applications inside the Virtual Desktop....145
4.5.5.Pause and Resume the Virtual Desktop....148
4.5.6.Close the Virtual Desktop....152
4.6.Containment Statistics Analyzer....154
5. DLP Tasks - Introduction....157
5.1.Run Data Loss Prevention Scans....157
5.2.Manage DLP Quarantined Files....163
6.Advanced Tasks - Introduction....165
6.1.Create a Rescue Disk....165
6.1.1.Download and Burn Comodo Rescue Disk....166
6.2.Remove Deeply Hidden Malware....171
6.3.Manage CCS Tasks....174
6.4.View CCS Logs....176
6.4.1.Antivirus Logs....179
6.4.2.VirusScope Logs....180
6.4.3.Firewall Logs....181
6.4.4.HIPS Logs....183
6.4.5.Containment Logs....184
6.4.6.Website Filtering Logs....185
6.4.7.Device Control Logs....186
6.4.8.Autorun Event Logs....187
6.4.9.Alert Logs....188
6.4.10.CCS Tasks Logs....190
6.4.11.File List Changes Logs....191
6.4.12.Vendor List Changes Logs....192
6.4.13.Configuration Change Logs....193
6.4.14.Virtual Desktop Event Logs....194
6.4.15.Data Loss Prevention Event Logs....195
6.4.16.Search and Filter Logs....196
6.5.Submit Files for Analysis to Comodo....216
6.6.View Active Process List....219
7. CCS Advanced Settings....222
7.1.General Settings....224
7.1.1.Customize User Interface....225
7.1.2.Configure Virus Database Updates....230
7.1.3.Log Settings....236
7.1.4.Manage CCS Configurations....239
7.1.4.1.Comodo Preset Configurations....240
7.1.4.2.Personal Configurations....240
7.2.Antivirus Configuration....247
7.2.1.Real-time Scanner Settings....248
7.2.2.Scan Profiles....251

7.3.Firewall Configuration....261
7.3.1.General Firewall Settings....263
7.3.2.Application Rules....267
7.3.3.Global Rules....281
7.3.4.Firewall Rule Sets....283
7.3.5.Network Zones....287
7.3.5.1.Network Zones....288
7.3.5.2.Blocked Zones....294
7.3.6.Port Sets....298
7.4.HIPS Configuration....302
7.4.1.HIPS Settings....303
7.4.2.Active HIPS Rules....309
7.4.3.HIPS Rule Sets....318
7.4.4.HIPS Groups....323
7.4.4.1.Registry Groups....323
7.4.4.2.COM Groups....327
7.5.Protected Objects....332
7.5.1.Protected Objects - HIPS....332
7.5.1.1.Protected Files....333
7.5.1.2.Blocked Files....344
7.5.1.3.Protected Registry Keys....350
7.5.1.4.Protected COM interfaces....353
7.5.2.Protected Objects - Containment....356
7.5.2.1.Protected Files and Folders....356
7.5.2.2.Protected Keys....362
7.6.Data Loss Prevention....364
7.6.1.DLP Monitoring Rules....365
7.6.2.DLP Discovery Rules....366
7.6.3.DLP Keyword Groups....367
7.7.Containment Settings....369
7.7.1.Containment Settings....370
7.7.2.Auto-Containment Rules....379
7.7.3.Virtual Desktop Settings....412
7.7.4.Containment - An Overview....424
7.7.5.Unknown Files: The Scanning Processes....425
7.8.File Rating Configuration....426
7.8.1.File Rating Settings....428
7.8.2.File Groups....432
7.8.3.File List....440
7.8.4.Submitted Files....453
7.8.5.Vendor List....455
7.9.Advanced Protection....471
7.9.1.VirusScope Settings....472

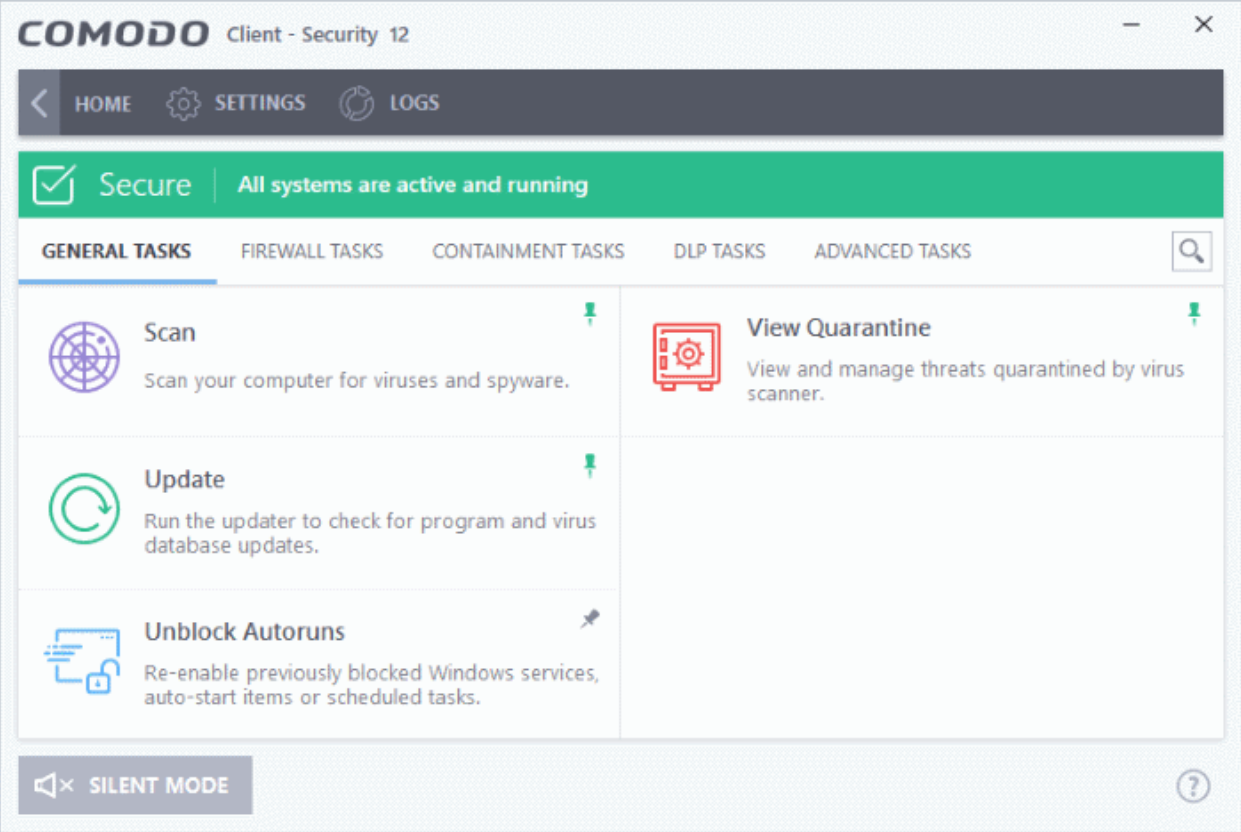
7.9.2.Scan Exclusions....475
7.9.3.Device Control Settings....491
7.9.4.Script Analysis Settings....498
7.9.5.Miscellaneous Settings....505
7.10.Web Filter Settings....509
7.10.1.Website Filtering Rules....511
7.10.2.Website Categories....519
Appendix 1 - CCS How to... Tutorials....525
Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily....525
Set up the Firewall For Maximum Security and Usability....528
Block Internet Access while Allowing Local Area Network (LAN) Access....535
Set up HIPS for Maximum Security and Usability....540
Create Rules to Auto-Contain Applications....542
Run an Instant Antivirus Scan on Selected Items....569
Create an Antivirus Scan Schedule....570
Run Untrusted Programs inside the Container....578
Run Browsers Inside the Container....580
Restore Incorrectly Quarantined Items....582
Submit Quarantined Items to Comodo Valkyrie for Analysis....584
Enable File Sharing Applications like BitTorrent and Emule....586
Block any Downloads of a Specific File Type....591
Disable Auto-Containment on a Per-application Basis....593
Switch Off Automatic Antivirus Updates....598
Suppress CCS Alerts Temporarily....601
Control External Device Accessibility....602
Appendix 2 - Comodo Secure DNS Service....604
Router - Enable or Disable Comodo Secure DNS....605
Windows - Enable Comodo Secure DNS....606

1. Introduction to Comodo Client Security

Overview

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

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



The software is designed to be secure 'out of the box' - so even the most inexperienced users need not have to deal with complex configuration issues after installation.

Comodo Client Security - Key Features:

- **Antivirus** - Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the always-on virus monitor and scheduled scans, you can instantly check any file by right-clicking on it. The antivirus also scans any removable storage plugged-in to your computer.
- **Firewall** - Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.
- **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **Containment** - Authenticates every executable and process running on your computer and prevents them from taking potentially damaging actions. Unrecognized processes and applications will be automatically

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

- **Virtual Desktop** - A sandbox environment in which you can run programs and browse the internet without fear those activities will damage the host computer. Applications in the virtual desktop are isolated from the host operating system, write to a virtual file system, and cannot access user data.
- **Data Loss Prevention (DLP)** - A scanner which lets you identify documents on your computer which contain sensitive data, including credit card numbers and social security numbers. You can move detected documents to another location, quarantine them, ban them from being copied to USB devices, and more.
- **Advanced Protection** - A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
  - **Viruscope** - Monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Using a system of behavior 'recognizers', Viruscope not only detects unauthorized actions but also allows you to completely undo them. Apart from representing another hi-tech layer of protection against malware, this also provides you with the granular power to reverse unwanted actions taken by legitimate software without blocking the software entirely.
- **Rescue Disk -** Built-in wizard that allows you to burn a boot-disk which will run antivirus scans in a pre-Windows / pre-boot environment.
- **Additional Utilities -** The advanced tasks section contains links that allow you to install other, free, Comodo security products - Comodo Cleaning Essentials and KillSwitch.

Guide Structure

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

- Introduction
  - Special Features
  - System Requirements
  - Installation
- Start Comodo Client Security
- The Main Interface
- Understand Security Alerts

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

- General Tasks - Introduction
  - Scan and Clean your Computer
    - Run a Quick Scan
    - Run a Full Computer Scan
    - Run a Rating Scan
    - Run a Custom Scan
    - Automatically Scan Unrecognized Files
  - Instantly Scan Files and Folders
  - Processing Infected Files
  - Manage Virus Database Updates
  - Manage Blocked Autoruns
  - Manage Quarantined Items
  - Run Data Loss Prevention Scans
- Firewall Tasks - Introduction

- Configure internet access rights for applications
- Stealth your Computer Ports
- Manage Network Connections
- Stop all Network Activities
- View Active Internet Connections

- Containment Tasks - Introduction
  - Run an Application in the Container
  - Reset the Container
  - Identify and Kill Unsafe Running Processes
  - Open Shared Space
  - The Virtual Desktop
  - Containment Statistics Analyzer
- Advanced Tasks - An Introduction
  - Create a Rescue Disk
  - Remove Deeply Hidden Malware
  - Manage CCS Tasks
  - View CCS Logs
  - Submit Files for Analysis to Comodo
  - View Active Process List
- CCS Advanced Settings
  - General Settings
    - Customize User Interface
    - Configure Virus Database Updates
    - Log Settings
    - Manage CCS Configurations
  - Antivirus Configuration
    - Real-time Scanner Settings
    - Scan Profiles
  - Firewall Configuration
    - General Firewall Settings
    - Application Rules
    - Global Rules
    - Firewall Rule Sets
    - Network Zones
    - Port Sets
  - HIPS Configuration
    - HIPS Settings
    - Active HIPS Rules
    - HIPS Rule Sets
    - Protected Objects - HIPS
    - HIPS Groups
  - Data Loss Prevention
    - DLP Monitoring Rules
    - DLP Discovery Rules

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

1.1. Special Features

Auto-Containment

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

Viruscope

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

Host Intrusion Prevention System

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

Comprehensive Antivirus Protection

- Detects and eliminates viruses from desktops, laptops and workstations;
- Cloud based scans mean you still get 100% protection even if your database is outdated.
- Heuristic techniques identify previously unknown viruses and Trojans;
- Scans registry and system files for possible spyware infection and cleans them;
- Highly configurable on-demand scanner lets you run custom scans on any file, folder or drive;
- Daily, automatic updates of virus definitions;
- Automatically scans external devices when they are plugged in;
- Isolates suspicious files in quarantine preventing further infection;
- Built in scheduler allows you to run scans at a time that suits you;
- Simple to use - install it and forget it - Comodo AV protects you in the background.

Intuitive Graphical User Interface

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

Comodo Client Security - Extended Features

Highly Configurable Security Rules Interface

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

Application Behavior Analysis

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

Cloud Based Behavior Analysis

Comodo Client Security features cloud based analysis of unrecognized files, in which any file that is not recognized and not in Comodo's white-list will be sent to Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it behaves in a malicious manner. If yes, the file is then manually analyzed by Comodo technicians to confirm whether it is a malicious file or not. The results will be sent back to your computer in around 15 minutes.

Event logging

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

Memory Firewall Integration

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

'Training Mode' and 'Clean PC' Mode

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

Application Recognition Database (Extensive and proprietary application safe list)

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

The Firewall is continually updated and currently over 1,000,000 applications are in 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.

Windows boot protection

CCS can identify untrusted DLLs, apps, portable executables (PE) and autoruns that launched before CCS started. These may expose the endpoint to danger if the items are malicious. These items can blocked at the next restart of the endpoint.

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 Endpoints

Windows 10 (32-bit and 64-bit versions) Windows 8 / 8.1 (32-bit and 64-bit versions) Windows IoT	• 512 MB available RAM • 1 GB hard disk space for both 32-bit and 64-bit versions • CPU with SSE2 support • Internet Explorer version 11 or above

Windows XP / Vista

- CCS does not support Windows XP or Vista, period.
- The auto-containment and virtual desktop features simply do not work on XP / Vista, so you cannot take advantage of one of our core protection features.
- Comodo strongly recommends anybody still using XP or Vista to upgrade immediately. Microsoft ceased support for XP/Vista years ago and the number of serious vulnerabilities in these operating systems is almost innumerable. By using them you are exposing yourself to substantial risks which signature-based antivirus cannot protect you against.

Windows 7

- Microsoft ended general support for Windows 7 in January 2020. Devices running Windows 7 will only receive security updates if the user has purchased a 3 year extended security updates (ESU) package from Microsoft.
- Because of this, Windows 7 is no longer an officially supported operating system. Unpatched vulnerabilities introduced by the underlying OS can compromise the protection provided by CCS. For example, a weakness in a Microsoft API that CCS relies on can undermine the protection of CCS.
- Key points:
  - All CCS critical security features will continue to work on Windows 7, including auto-containment, antivirus, and firewall. Similarly, you can also manage Windows 7 devices from Endpoint Manager and deploy security profiles to Windows 7 devices.
  - We will also continue to fix critical and blocker issues for CCS on Windows 7.
  - However, future CCS releases may contain features that are not included/do not work on Windows 7.
- We understand that many customers have clients who still use Windows 7, and hope that this information helps you make an informed decision about transitioning those machines to Windows 10 / 8.1 / 8.

Windows Servers

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

All operating systems

You also need to open some ports on your firewall to allow various services to function correctly:

- USA customers - **Click here** for port information
- EU customers - **Click here** for port information

1.3. Install Comodo Client Security

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

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

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

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

- **Step 1 - Enroll Users**
- **Step 2 - Enroll Devices**

Step 1 - Enroll Users

You must enroll users before you can deploy CCS to your endpoints.

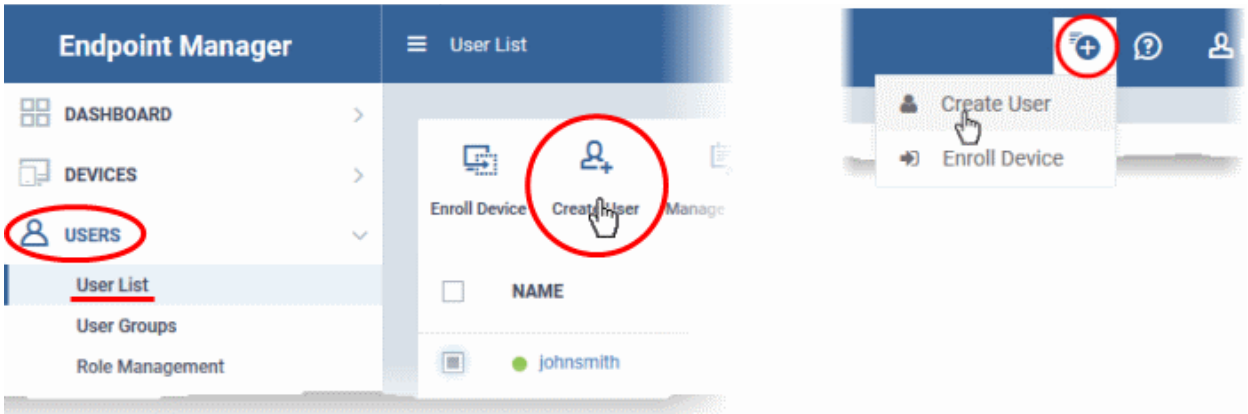
- **ITarian MSP customers** - You can create multiple companies and enroll users to any of them.
- **ITarian Enterprise, and stand-alone Endpoint Manager customers** - All users are enrolled to the default company.

Add a user

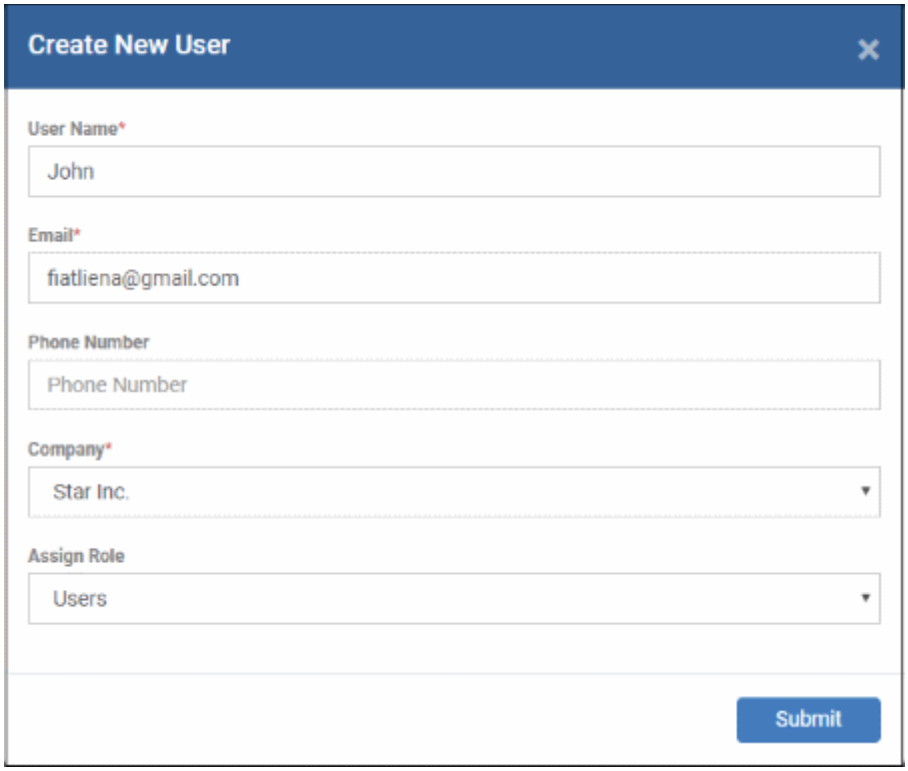
- Click 'Users' > 'User List' > click the 'Create User' button

  or

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



The 'Create new user' form will open.

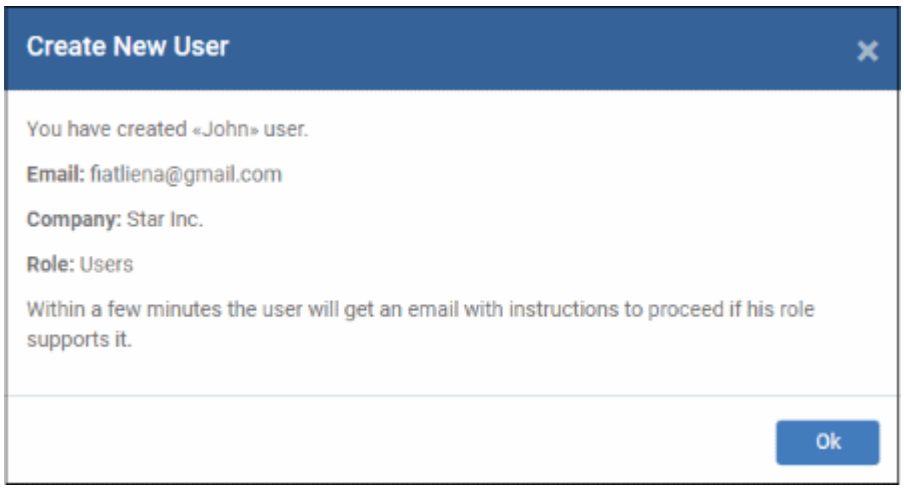


- Type a login username (mandatory), email address (mandatory) and phone number for the user
- **Company** - Choose the organization to which you want to enroll the user.
- **Role**

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

  - **Administrator** - Full privileges in the Endpoint Manager console. The permissions for this role are not editable.
  - **User** - In most cases, a user is simply an owner of a managed device. They should not require access to the Endpoint Manager console. Under default settings, users cannot login to Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

A confirmation message is shown:



- Repeat the process to add more users.
- New users are added to the 'Users' interface (click 'Users' > 'User List')

Tip: You can also bulk import users from a .csv file. See **https://community.itarian.com/help/topic-459-1-1005-14884-Import-Users-from-a-CSV-File.html** for more details.

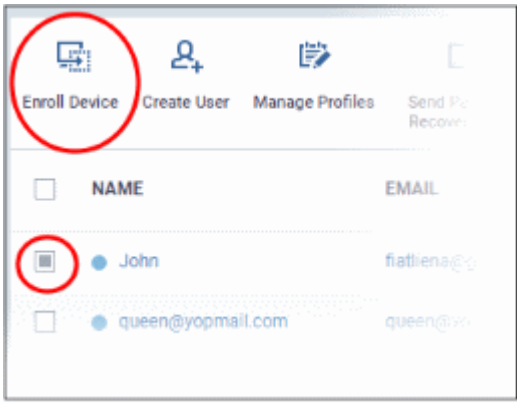
Step 2 - Enroll Devices

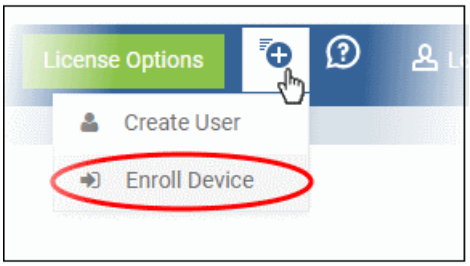
The next step is to add user devices so you can manage them with Endpoint Manager.

- Click 'Users' then 'User List'
- Select the users whose devices you want to add then click 'Enroll Device':

  Or

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

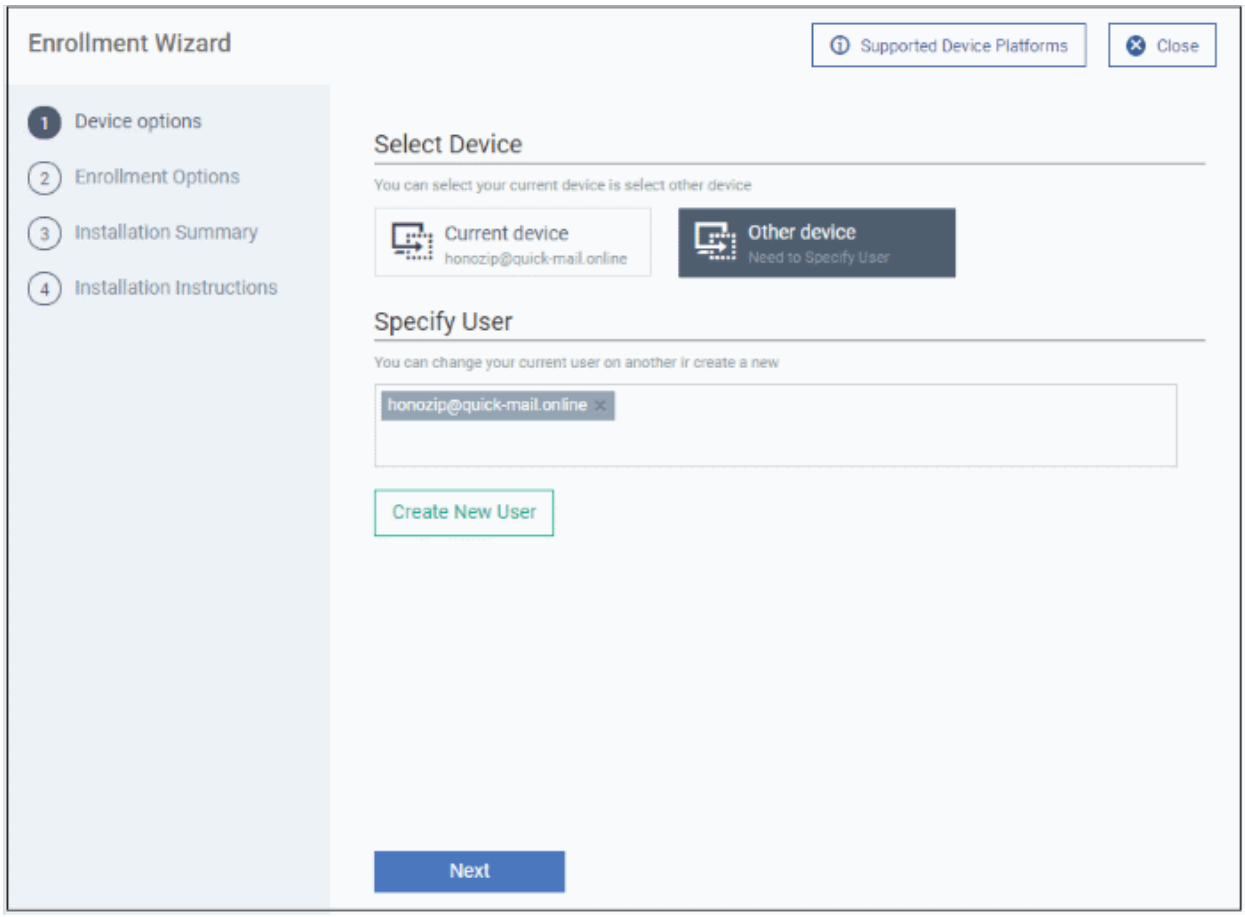




This starts step 1 of the device enrollment wizard:

Step 1 - Device Options

- **Current device -** Enrolls the device you are currently using. You may disregard this option at this stage as we are adding multiple devices with the 'Other device' option.
- **Other device** - Add devices owned by the users you selected previously. Those users should already be listed in the 'Specify User' box:



- You can add additional, existing users by simply typing their email address in the box. Endpoint Manager will auto-suggest users that have already been created.
- **Create New User** - Click if you want to add a new user to Endpoint Manager. You cannot add devices unless you have first added the users that own them.
- Click 'Next' to proceed to step 2.

Step 2 - Enrollment Options

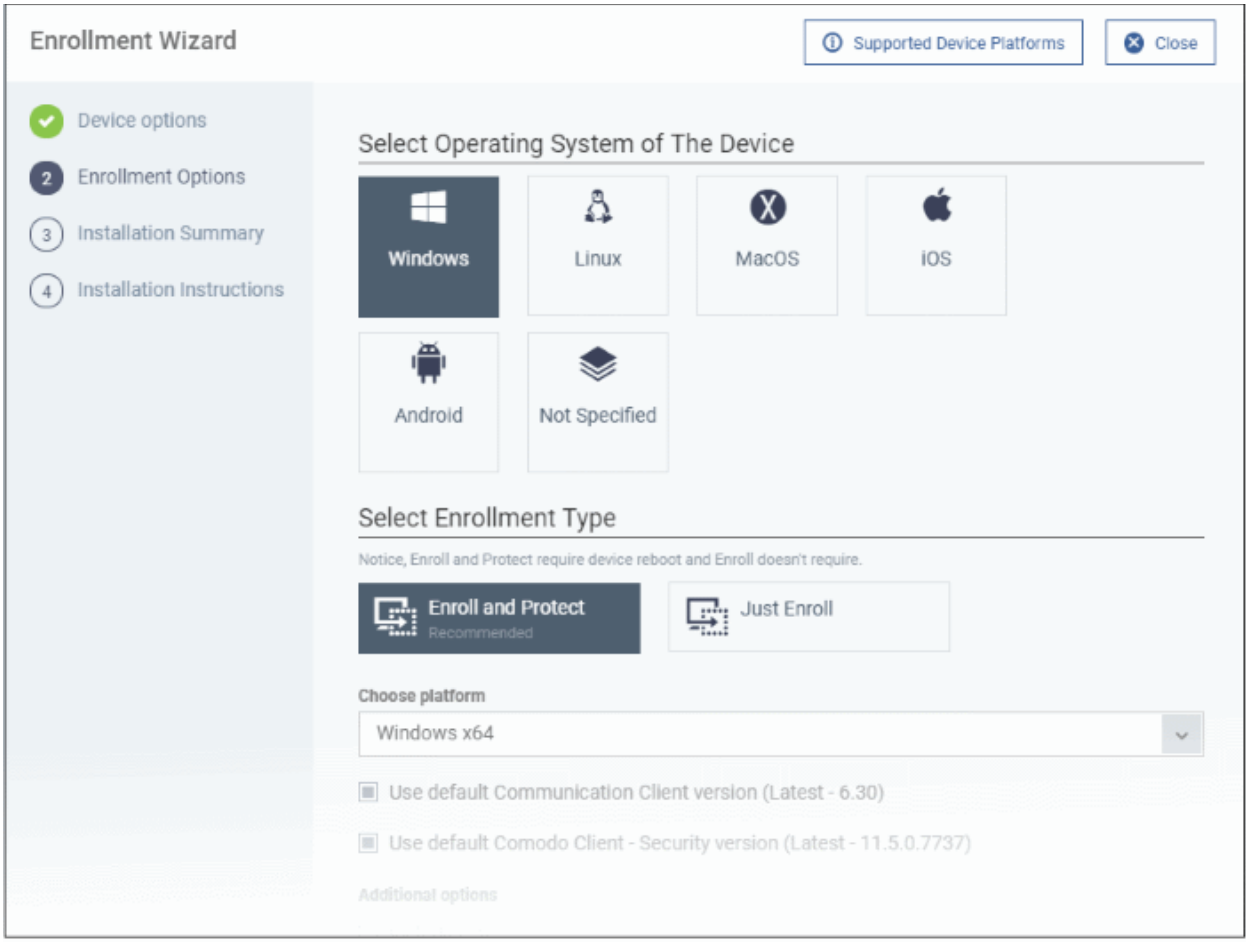
Enrollment Type

Applies to Windows, Mac and Linux devices.

- **Enroll and Protect** - Installs both the communication client and the security client.
- **Just Enroll** - Installs only the communication client

Background. There are two types of client:

- **Communication Client** - Connects the device to Endpoint Manager for central management. It is mandatory to install this client.
- **Security Client** - This is the security software. Depending on the operating system, it includes antivirus, firewall, threat-containment, web-filtering, and more. It is optional to install this client.



TLDR

- Click 'Not Specified' if you only want to install the communication client on target devices. The wizard will detect the target operating system and send the appropriate client to the device user.
- Click one of the operating system tiles if you also want to install the security client. Make sure the target devices use the operating system you selected.

Option 1 - Enroll + Protect - Single Operating System

- Choose this if you want to deploy both communication and security clients
  - Click the Windows OS box. Please make sure all your target devices use this operating system.
  - The wizard will send enrollment mails which *only* contain download links for the Windows clients.
  - You can customize enrollment options as required. You can configure items such as enrollment type, reboot policy, client version, configuration profile and device name.
  - *Note - Please uninstall any other antivirus products from target endpoints before proceeding. Failure to do so could cause conflicts that mean CCS does not function correctly.*

Option 2 - Just Enroll - Multiple Operating Systems

- Choose this if you only want to deploy the communication client. If required, you can install the security client later after enrolling the endpoint.
  - Click 'Devices' > 'Device List'
  - Select the target devices
  - Click the 'Install or Update Package' button > Choose 'Install Comodo Client - Security'.

Click 'Next' to **skip to step 3** if you are happy with your choices thus far

OR

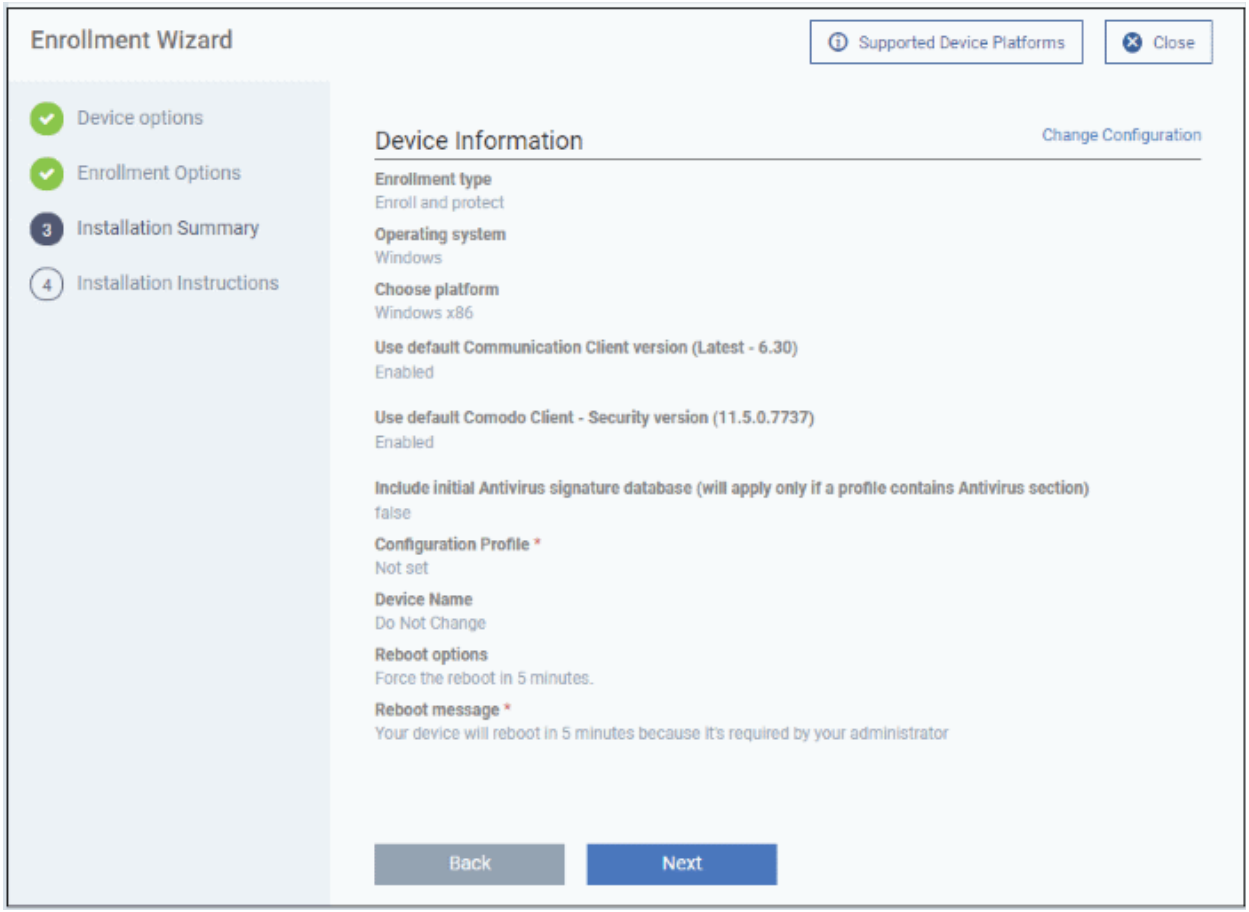
See the tables below for more information about the options on this page

Setting	Description
Choose platform	Select Window OS version. 64 bit, 32 bit, or hybrid. The hybrid package will auto-detect and install the correct version.
Use default Communication Client version	This client enrolls the endpoint for central management. • You can only change the CCC version if enabled in **portal settings**. If the option is not enabled then the 'Default version' is deployed.
Use default Communication Client Security version	This client installs security software such as antivirus, firewall and auto-containment. • You can only change the CCS version if enabled in **portal settings**. If the option is not enabled then the 'Default version' is deployed.
Additional options	**AV Database** - Choose whether to include the latest virus database with the installation package. This increases the size of the package. If disabled, the client will download the latest database anyway when you run the first virus scan.
Configuration Profile	A configuration profile is a collection of settings which specify a device's network access rights, security settings, antivirus scan schedule, and more. The default is 'Windows - Security Level 1' profile. Choose a different profile if required. • The default profile is recommended for most users and can always be changed later if required. • If you want to change it, type the first few characters of a profile name and choose from the suggestions that appear. • You can view the settings in a profile at 'Configuration Templates' > 'Profiles'.
Set Reboot Options	Endpoints need to be restarted to complete CCS installation. You have the following restart options: • **Force the reboot in**... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message is shown to the user prior to the restart. • **Suppress reboot** - Endpoint is not auto-restarted. The installation is finalized when the user next restarts the endpoint. • **Warn about reboot and let users postpone it** - Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens. Optional. Type a custom message in the 'Reboot Message' field.
Device Name Options	• Do Not Change - The device's existing name is used to identify the device in Endpoint Manager. • Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.

- Click 'Next' to proceed to step 3

Step 3 - Installation Summary

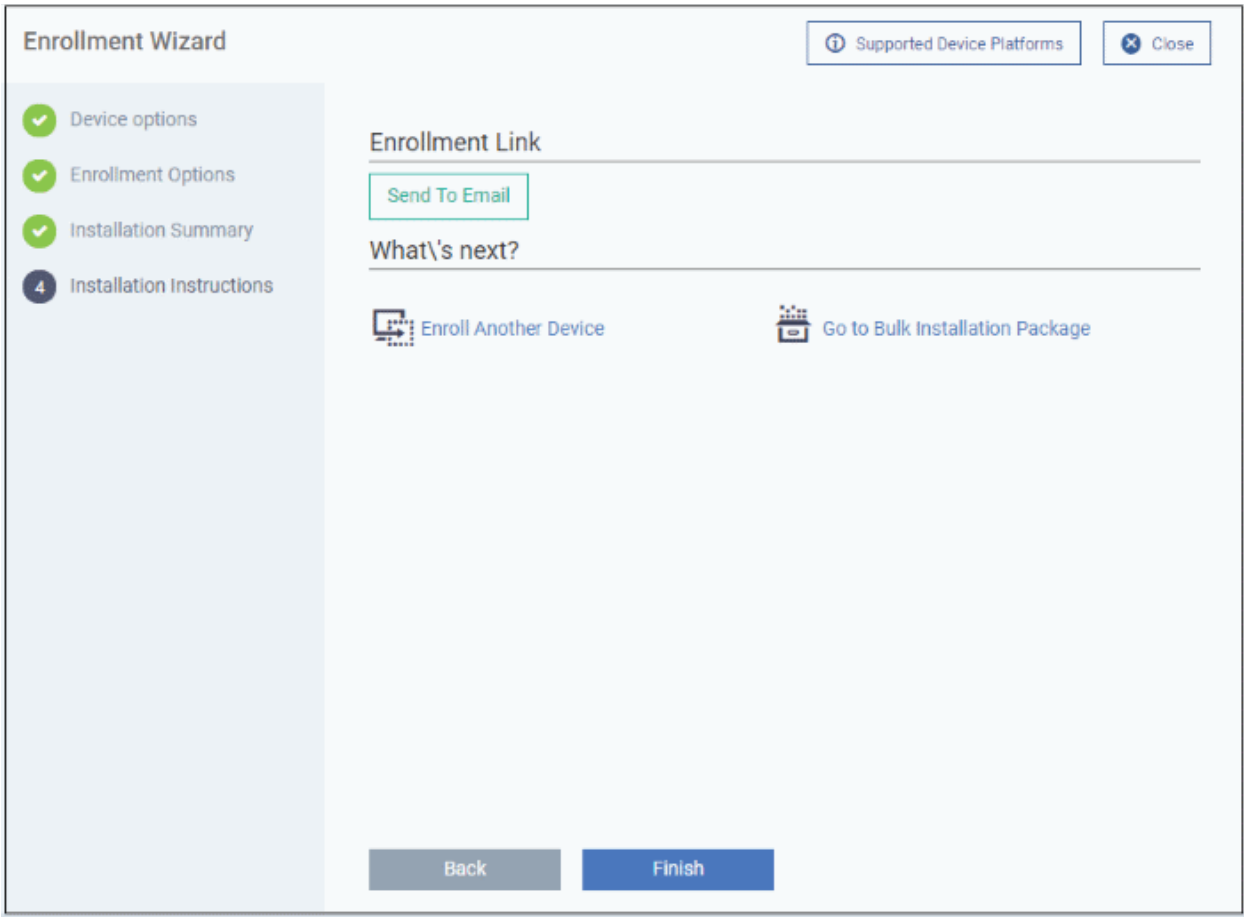
Review your choices so far.



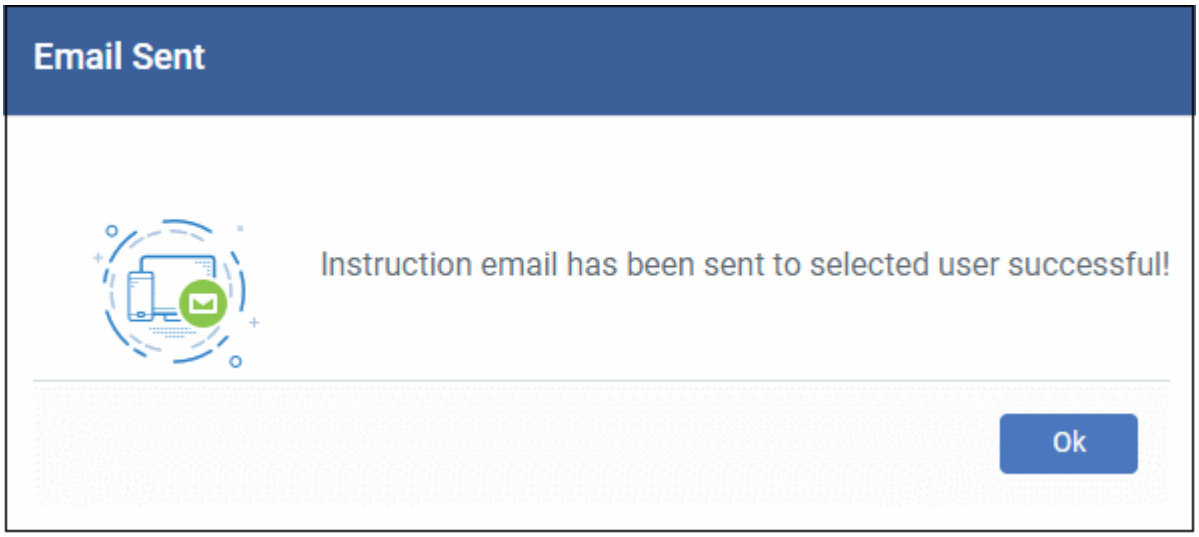
- Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
- Click 'Next' to proceed to step 4

Step 4 - Installation Instructions

The final step is to send out the enrollment emails to the device owners:



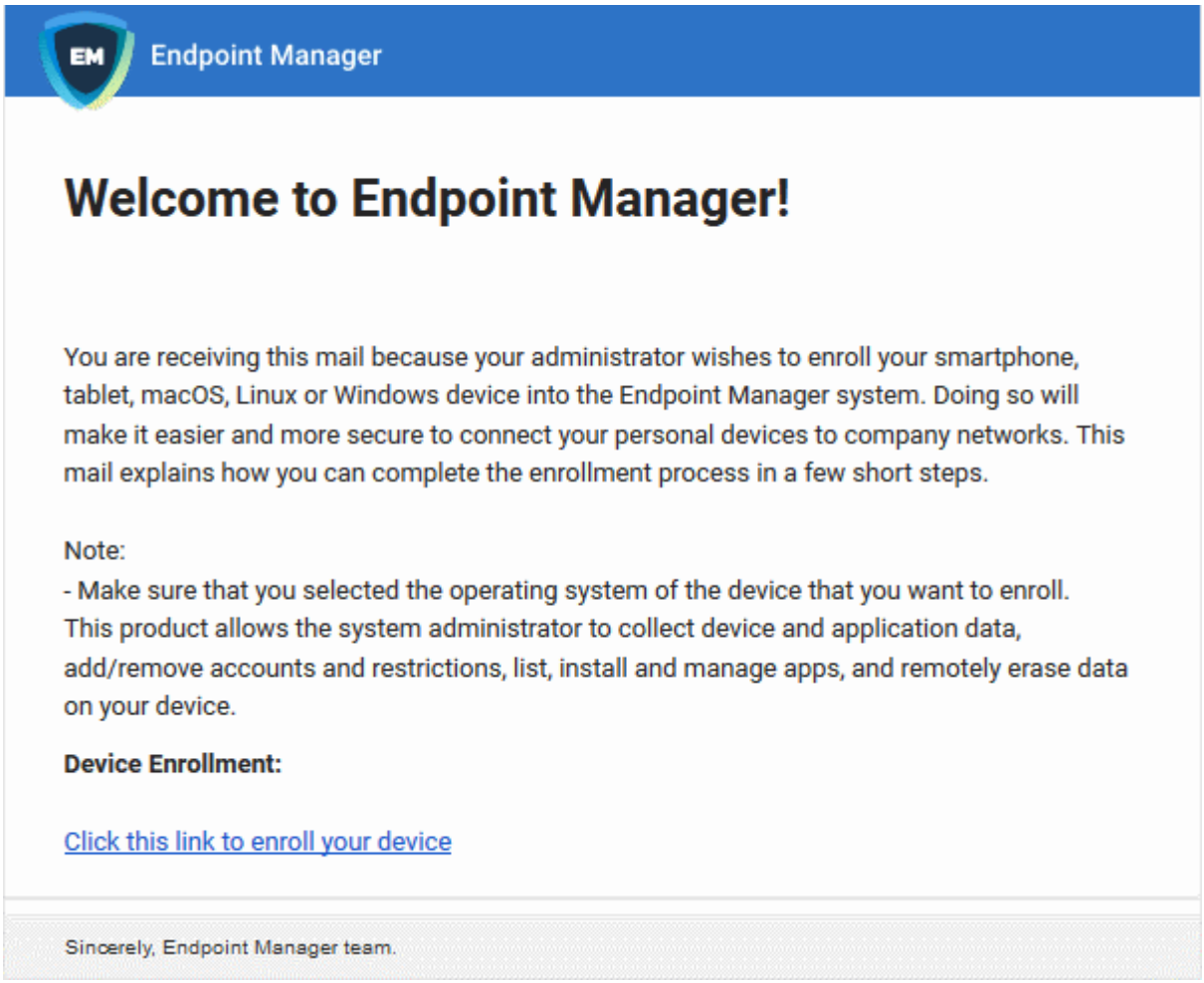
- **Send To Email** - Click this to send enrollment mails to users with the settings you choose in steps 1 - 3.



- **Enroll Another Device** - Takes you back to step 1
- **Go to Bulk Installation Package** - Takes you to bulk installation package screen to configure and enroll users in bulk. See '**Bulk Enrollment of Devices**'

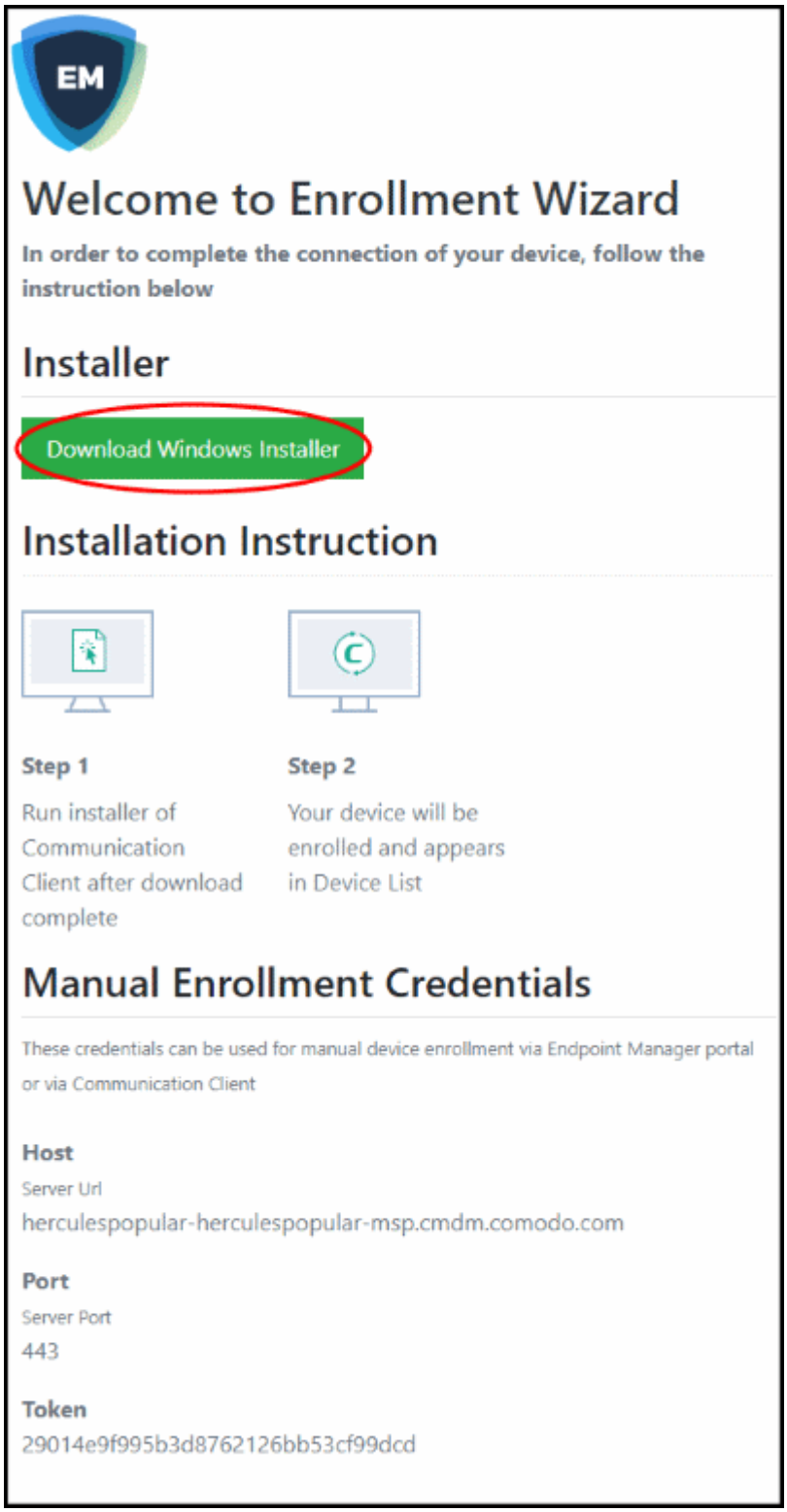
- Click 'Finish' to close the window.

An example mail is shown below:



The user experience is as follows:

- User opens the email on the Windows endpoint you want to enroll.
- Click the enrollment link in the email to open the device enrollment page
- Click the 'Download Windows Installer' button:



- The EM client setup file gets downloaded.
- Run the setup file to install the client on the endpoint.
- The device is automatically added to Endpoint Manager once installation is complete. The EM communication client icon appears at the bottom-right of the endpoint screen.
- If the client is not automatically enrolled after installation, you can manually enroll the device at a later time. This might happen if, for example, there are connectivity issues.
- You will need to enter the host, port and token ID to manually enroll. You can find these items at the end of the device enrollment page.

- Protection is effective immediately after the computer restarts.

An Endpoint Manager (EM) security profile is applied to the device.

- If the user is already associated with a configuration profile in EM, then those profiles will be applied to the device. See **Assign Configuration Profile(s) to User Devices** and **Assign Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user then the default Windows profile(s) will be applied to the device. See **Manage Default Profiles** for more details.

The device can now be remotely managed from the EM console.

1.4. Start Comodo Client Security

After installation, Comodo Client Security automatically starts whenever you start Windows.

CCS has two modes:

- **Normal Mode** - Allows you to access the entire CCS interface.
- **Virtual Desktop Only Mode** - You can only open the Virtual Desktop and Virtual Desktop settings.

The mode available to you depends on the Endpoint Manager (EM) profile active on the device.

Normal Mode

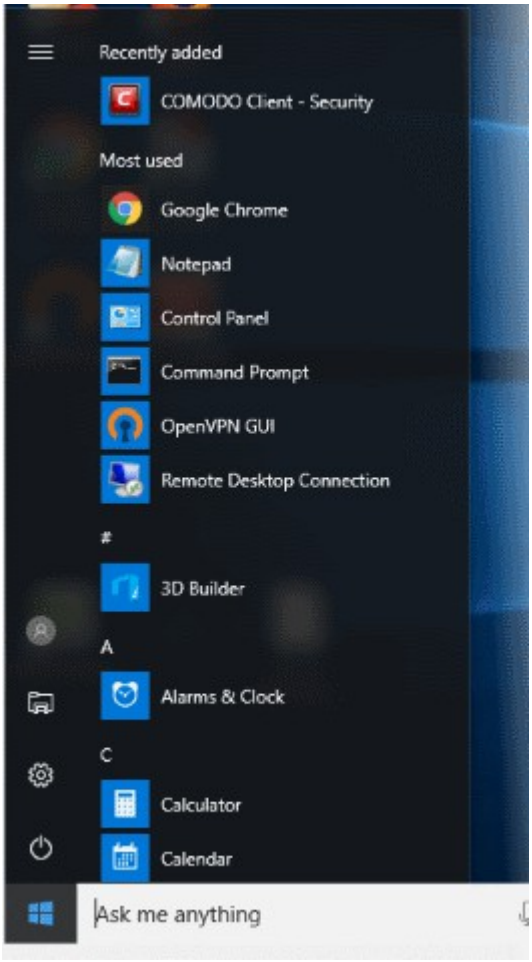
There are 5 different ways to open CCS if it is in normal mode:

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

Start Menu

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

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

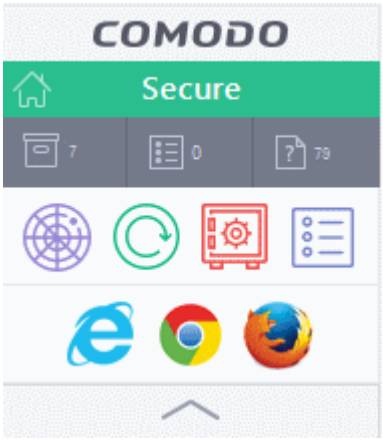


Windows Desktop

- Double-click the desktop shortcut to start Comodo Client Security. The shortcut is only visible if 'Show Desktop Shortcut' is enabled in the Endpoint Manager profile active on the endpoint.

Widget

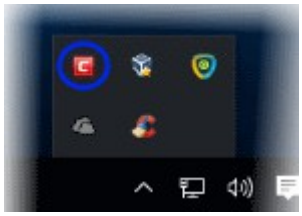
- Click the information bar in the widget to start CCS. The shortcut is only visible if 'Show Widget' is enabled in the Endpoint Manager profile active on the endpoint.



The widget also contains other useful data and features. See '**The Widget**' for more details.

CCS Tray Icon

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

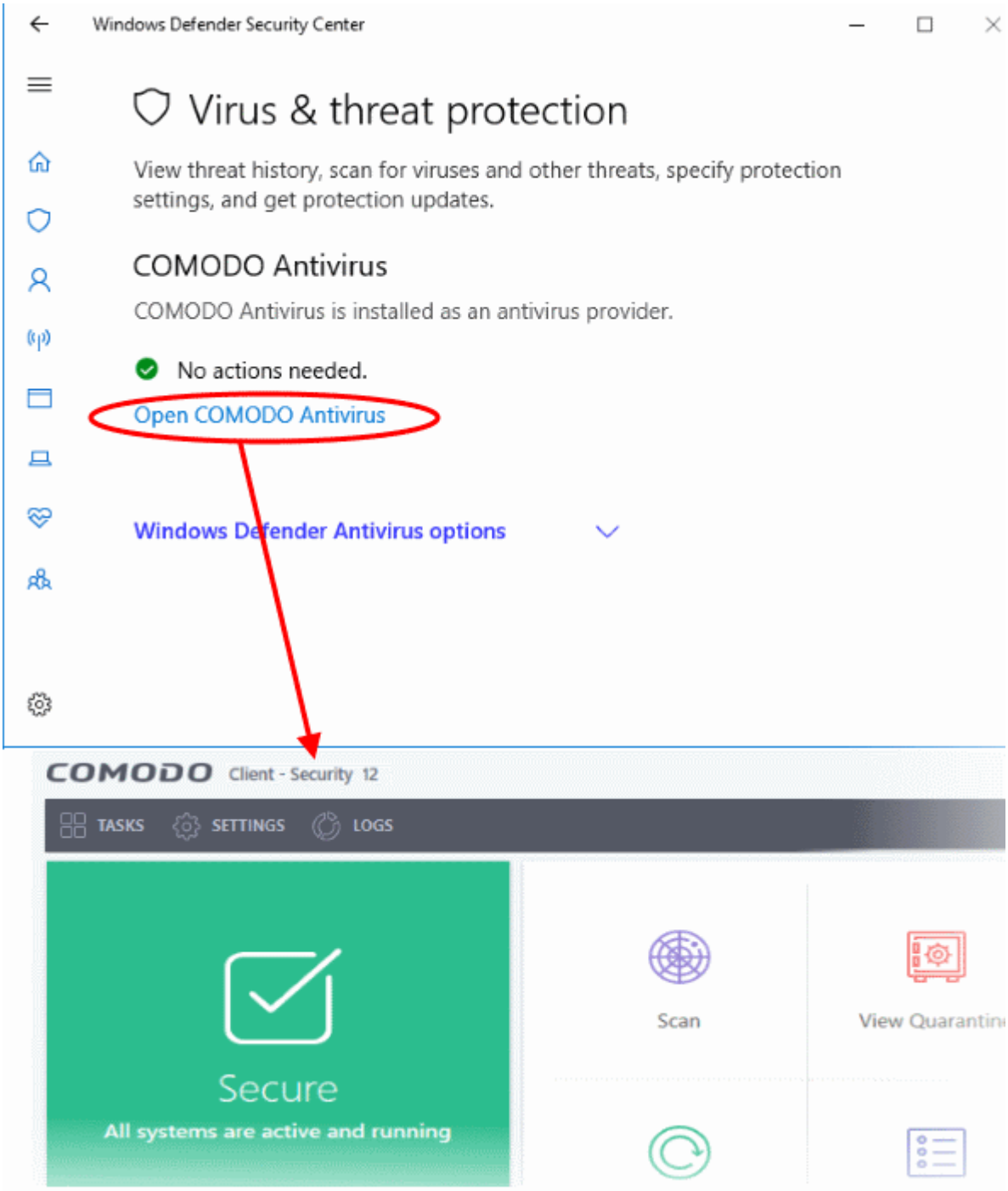


You can also right-click on the tray icon and select 'Open...'.

Windows Defender

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

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



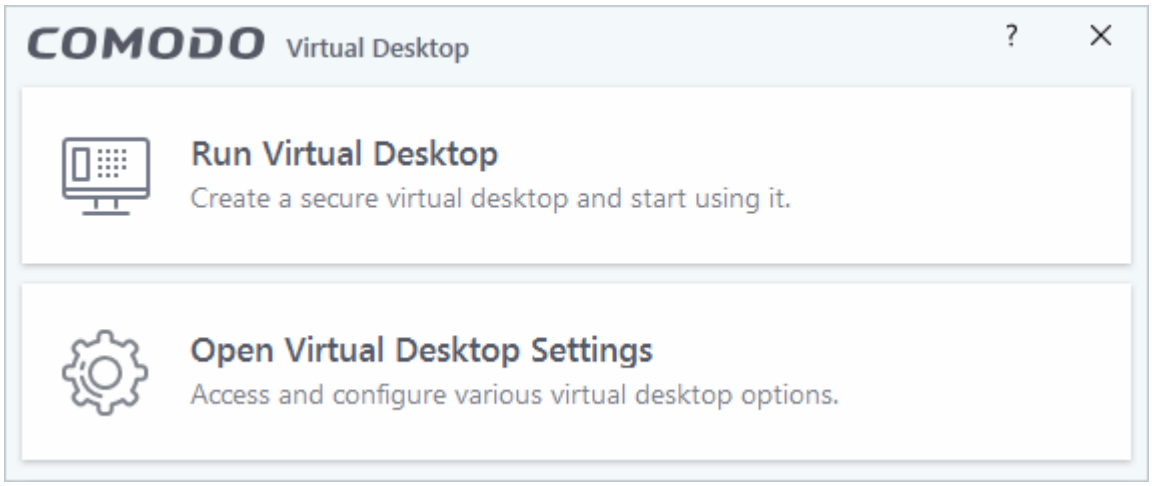
Virtual Desktop Only mode

- This mode means you can only open the Virtual Desktop and access Virtual Desktop settings. You cannot access any other areas of the CCS interface.
    - Endpoint Manager admins - You can enable or disable this setting in the 'UI Settings' section of a profile.
    - See **https://community.itarian.com/help/topic-459-1-1005-14932-Communication-Client-and-Comodo-Client---Security-Application-UI-Settings.html** if you want to read more on this.

In 'Virtual Desktop Only' mode:

- The system tray icon and the desktop widget are hidden

- The CCS desktop shortcut and Windows start menu entry lead to the following menu:



- **Run Virtual Desktop** - Opens the virtual desktop. See **The Virtual Desktop** for more help on this.
- **Open Virtual Desktop Settings** - Opens the virtual desktop settings area in CCS. See **Virtual Desktop Settings** for help with these settings.

End-users cannot access any other area of CCS.

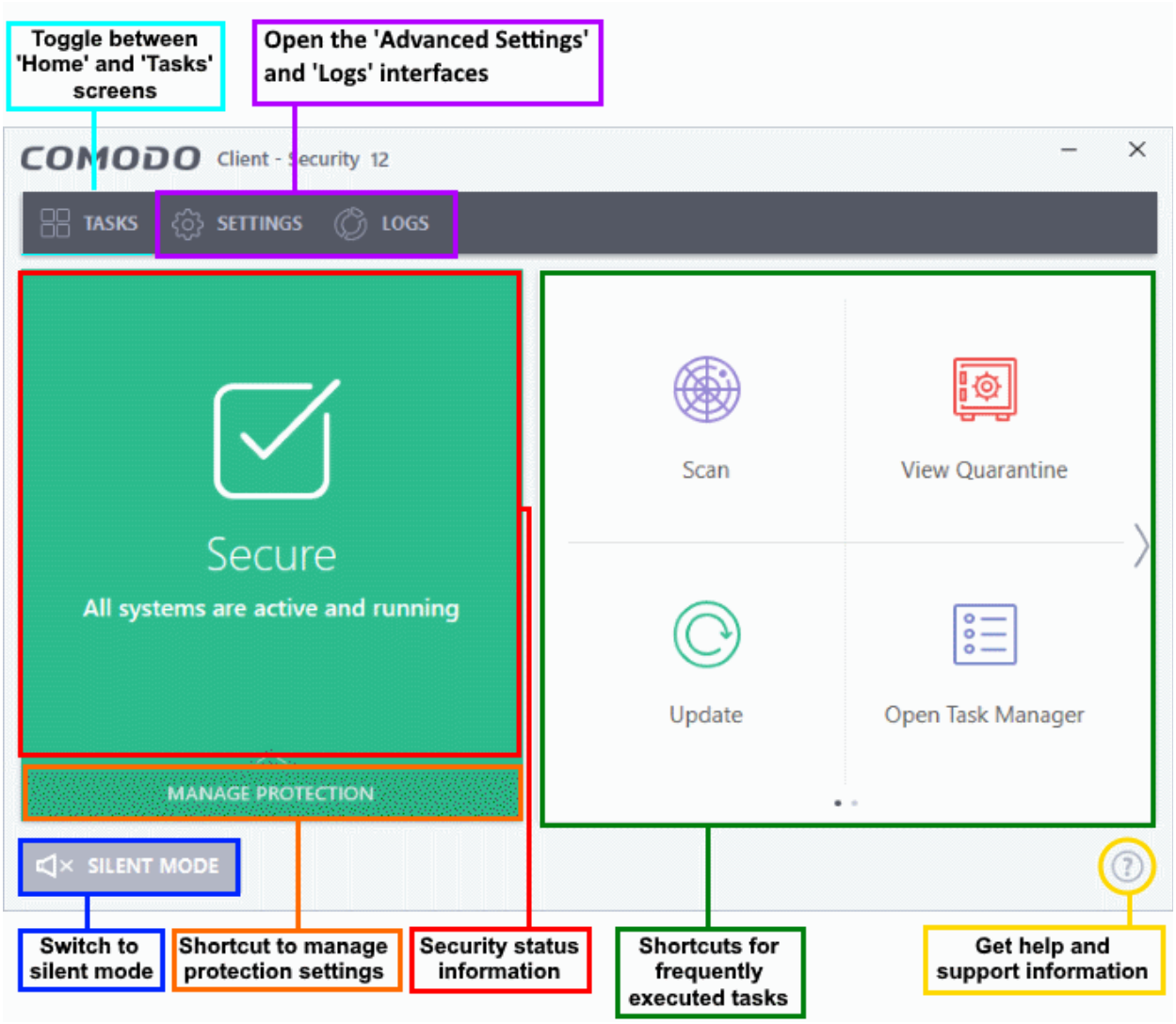
What is an Endpoint Manager profile?

- Endpoint Manager (EM) is a product which allows admins to manage Comodo Client Security on network endpoints.
- An EM profile is a template which contains all the security settings and privileges that the admin wants to implement on the endpoint.
- Admins can allow local changes to CCS by activating 'Enable local user to override profile configuration'. See **https://community.itarian.com/help/topic-459-1-1005-14934-Client-Access-Control.html** for help with this.

1.5. The Main Interface

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

- Click the 'Home/Tasks' button at the upper-left to switch between the **'home screen'** and the **'tasks' interface**.
- Switch on 'Silent Mode' to make sure nothing interrupts you while you are on an important task.
- The tiles on the right give you one-click access to important features, including the antivirus scanner, updates, task manager and more.



Click the following links for more information:

- **The Home Screen**
- **The Tasks Interface**
- **The Widget**
- **The System Tray Icon**

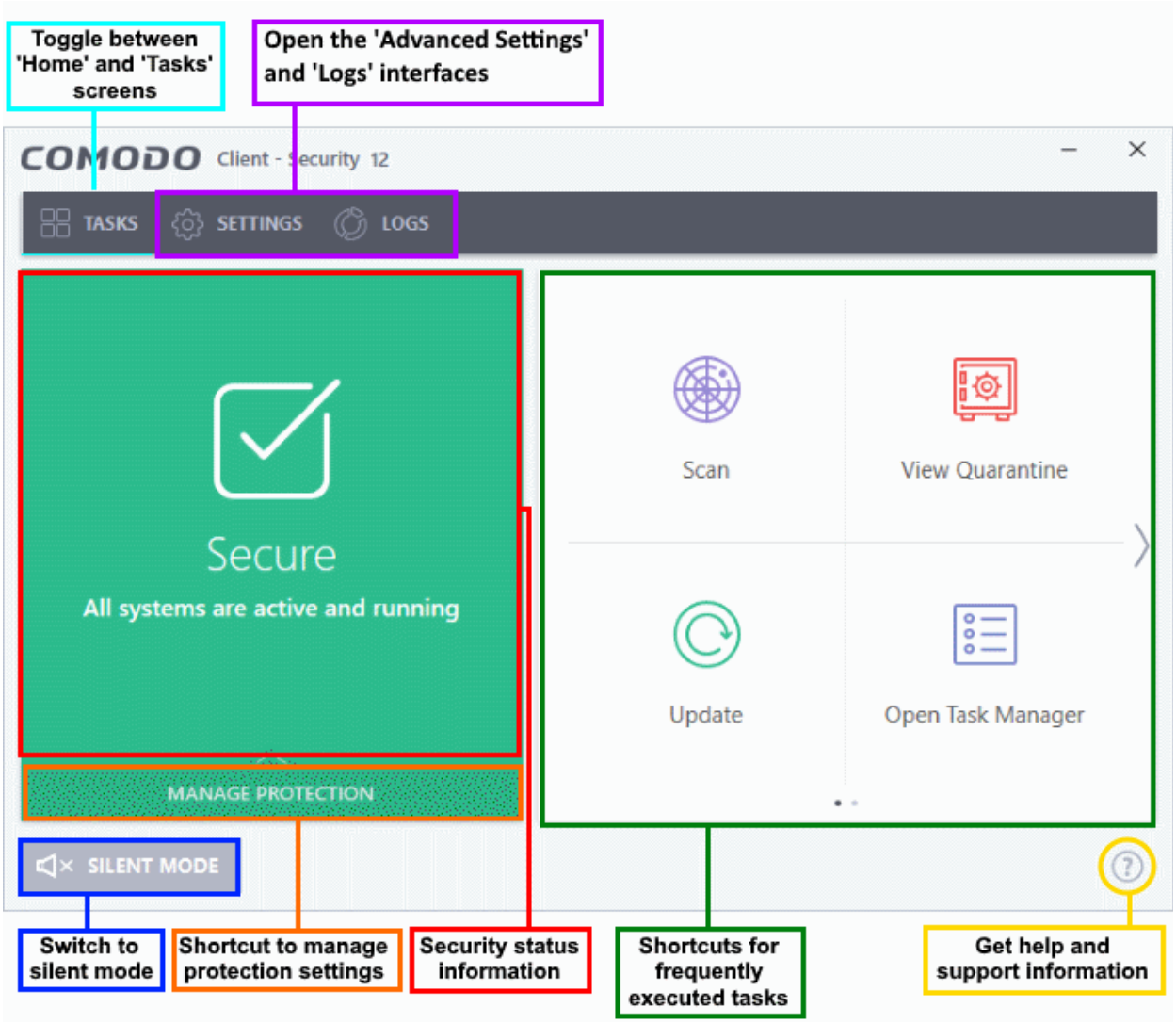
1.5.1. The Home Screen

You can switch between the home and tasks screens by clicking the 'Home/Tasks' button at the top-left of the interface:

- The home screen has an easy to use interface that lets you quickly run common tasks and manage program settings.
- The large 'security information' tile on the left shows your overall security level and lets you quickly deal with

any threats.

- The 'Manage Protection' button lets you turn security components on or off and open advanced settings.



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

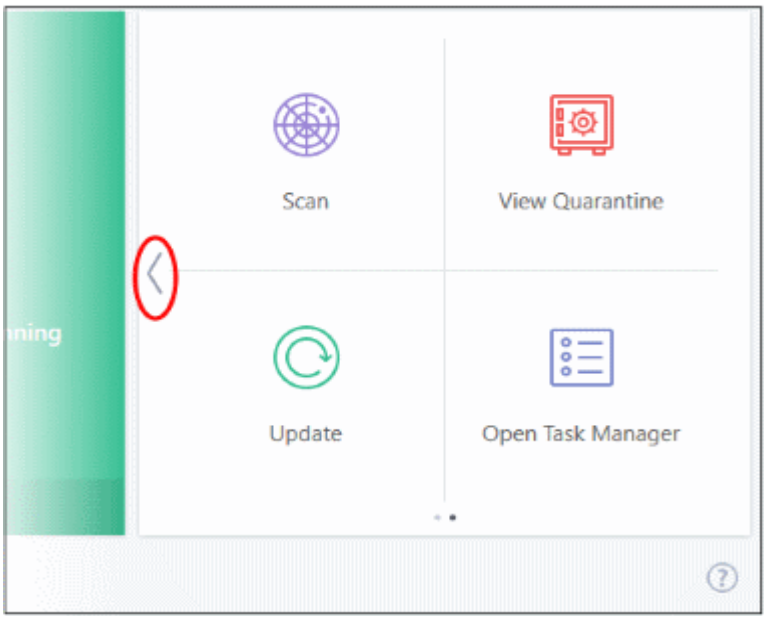
You can easily rectify the issue by clicking the 'FIX IT' button. '**Silent Mode**' and '**Help Window**' are common to both home and tasks screen.

From the home screen you can:

- **Add shortcuts tasks**
- **Manage protection settings**
- **Set CCS to silent mode**
- **View the help options**

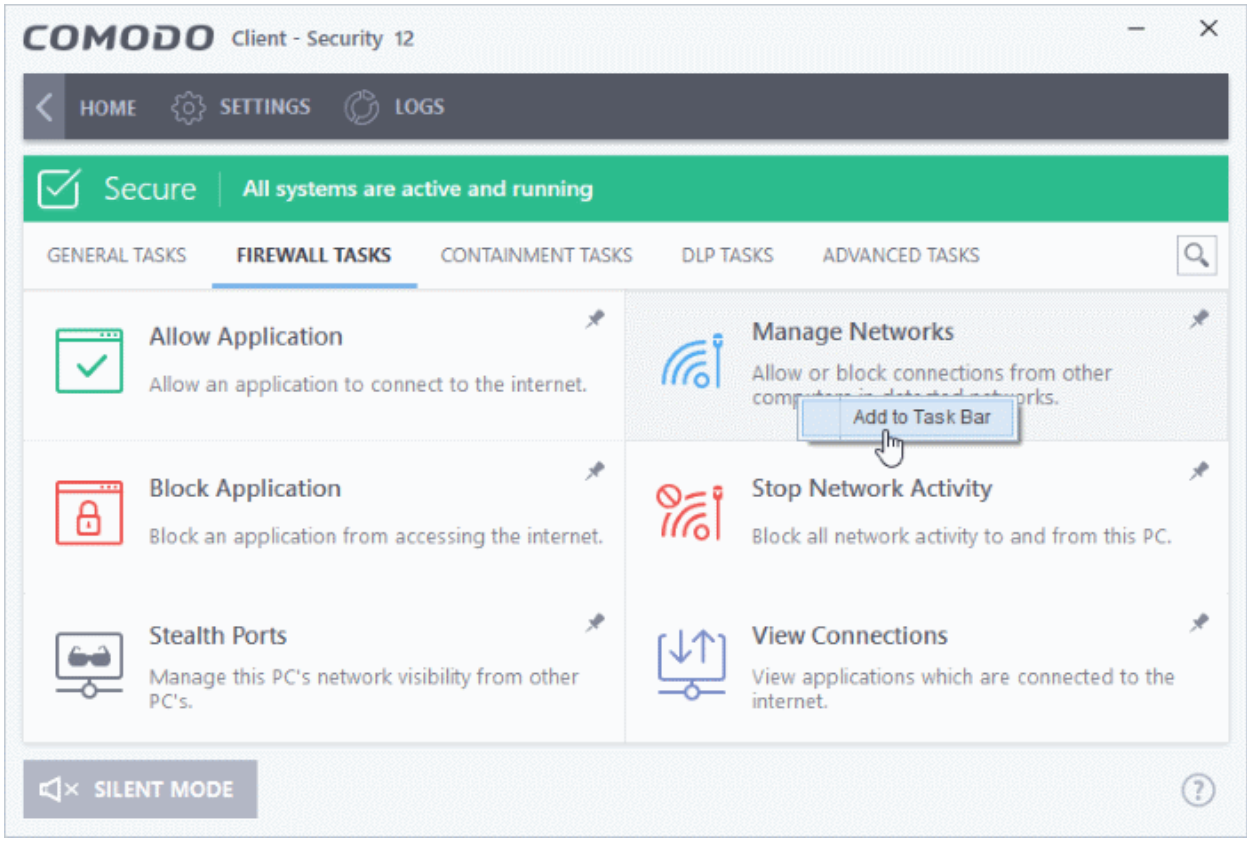
Add tasks to the home screen

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

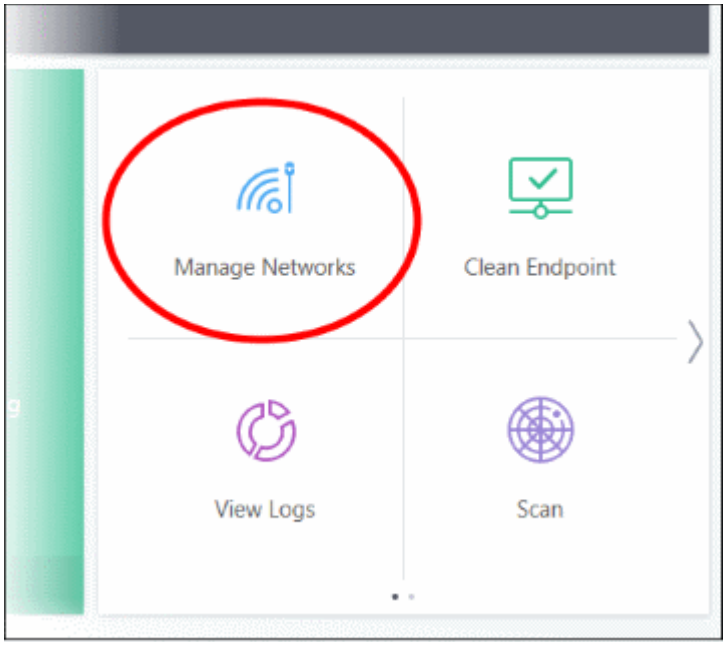


You can add tasks to this pane as follows:

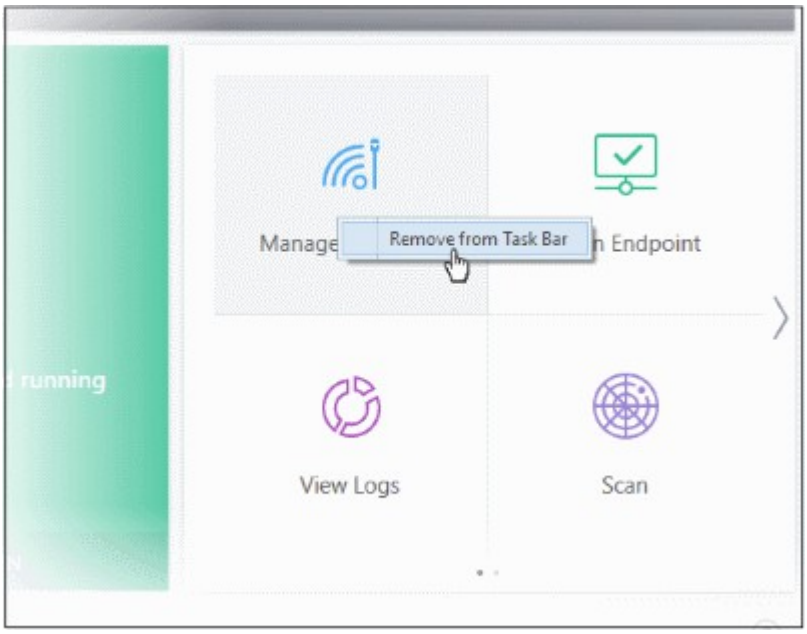
- Open the 'Tasks' interface (click the button at top left to switch between the tasks and home screens).
- Click any of the 'General', 'Firewall', 'Containment' or 'Advanced' tabs
- Right-click on the task you wish to add then click 'Add to Task Bar':



- Alternatively, you can add task shortcuts to the home screen by clicking the 'pin' button at the top-right of any tile.
- The selected task will be added to the tasks pane.

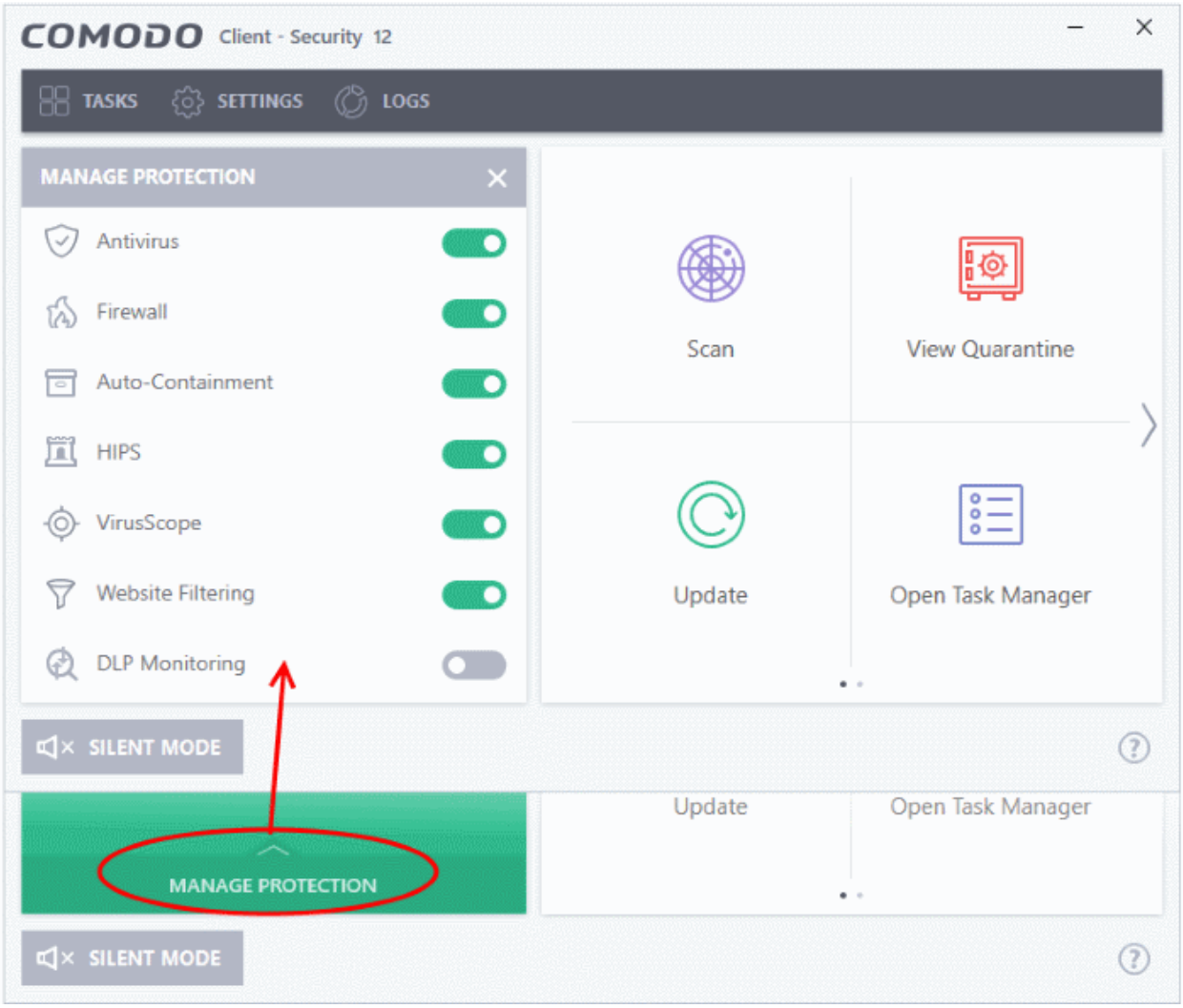


- To remove a task shortcut from the pane, right click on it and choose 'Remove from Task Bar'.



Manage Protection Settings

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



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

- **Antivirus Configuration**
- **Firewall Configuration**
- **Auto-Containment**
- **HIPS Configuration**
- **VirusScope Configuration**
- **Website Filtering**
- **DLP Monitoring**

Silent mode

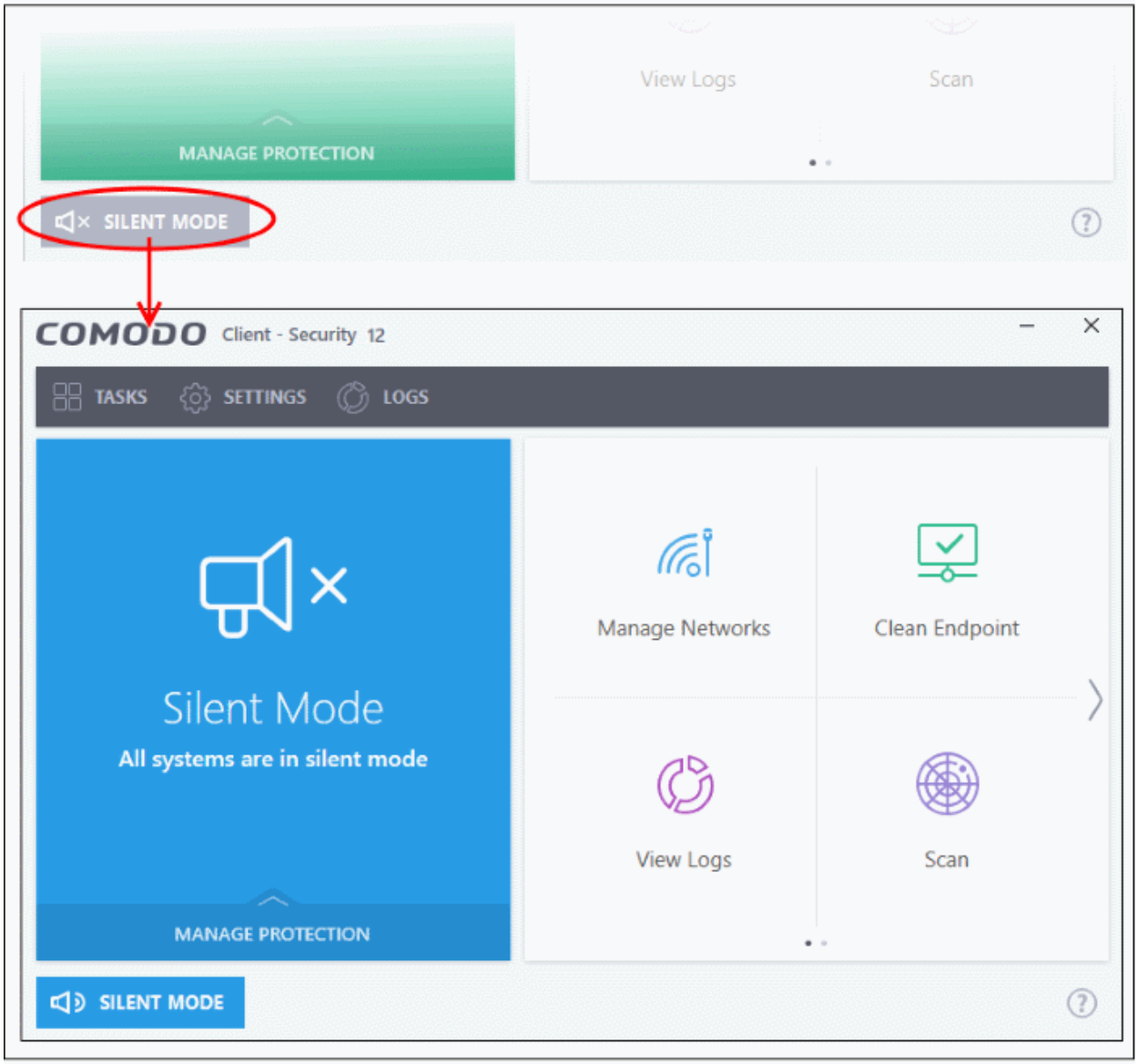
Silent mode lets you use your computer without interruptions from CCS. Operations that could interfere with your work are either suppressed or postponed.

In silent mode:

- All protection components remain 100% active
- HIPS/Firewall alerts are suppressed.
- AV updates and scheduled scans are postponed

Switch to Silent mode

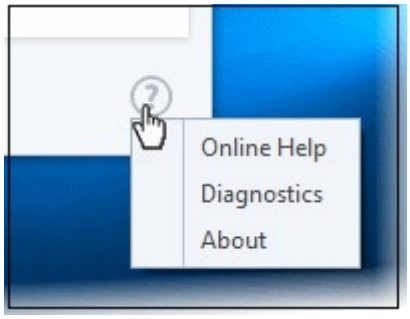
- Click the 'Silent Mode' button at the bottom-left of the home screen



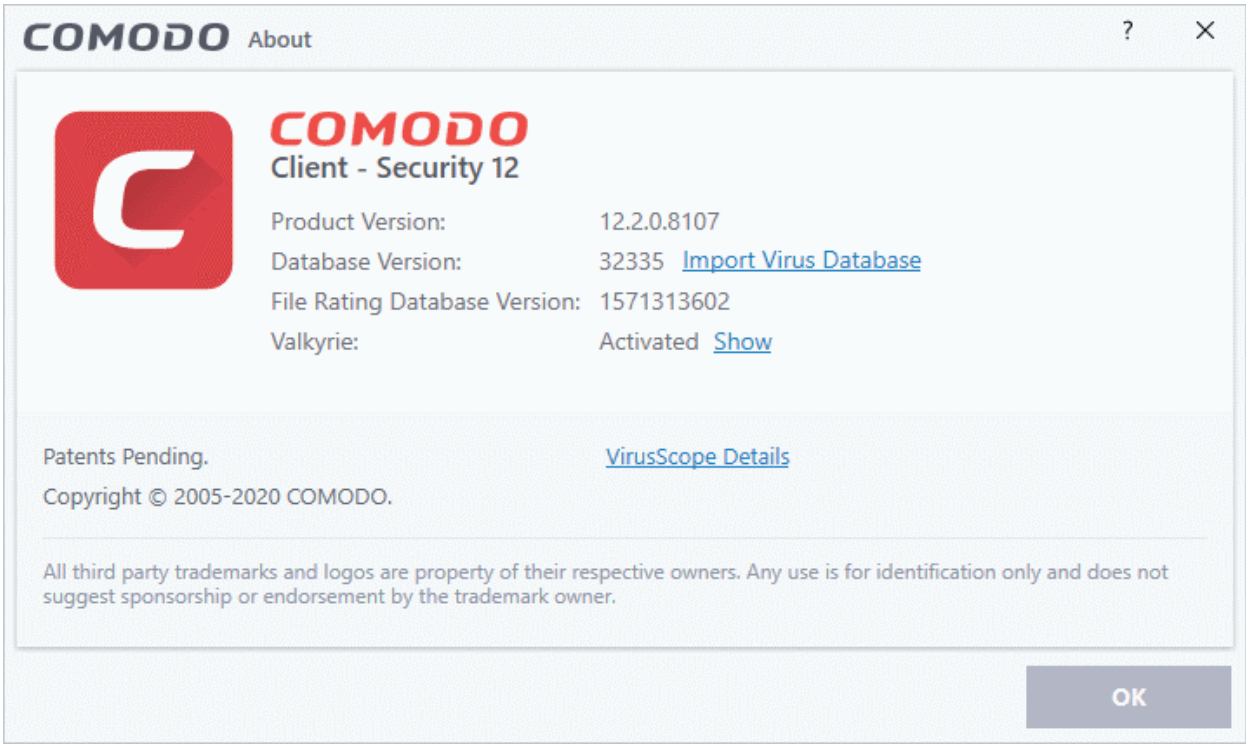
- Deactivate 'Silent Mode' to resume alerts and notifications.

Help Options

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



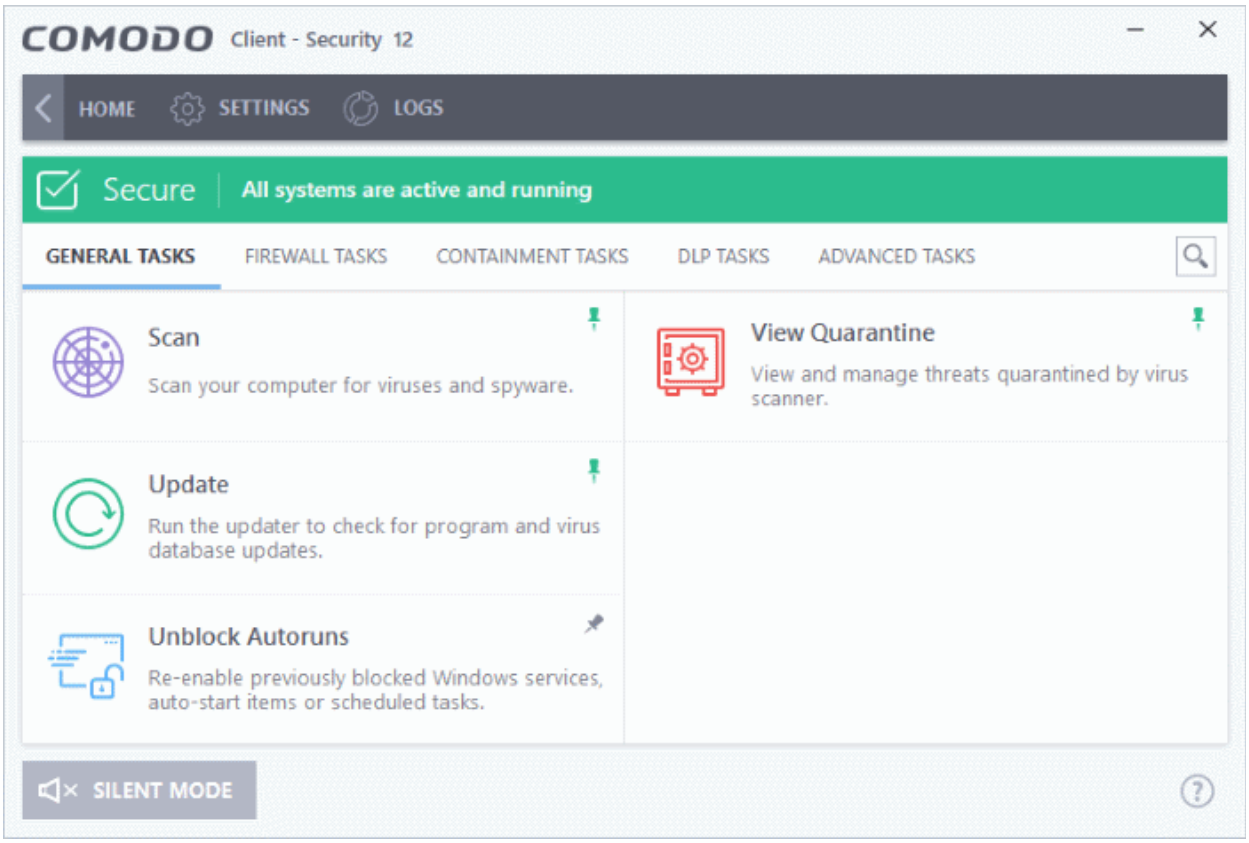
- **Online Help** - Opens Comodo Client Security's online help guide.
- **Diagnostics** - Helps to identify any problems with your installation.
- **About** - Contains version details and legal information:



- **Product Version** - The CCS version number.
- **Database Version** - The version of the virus database you currently have installed. Click 'Import Virus Database' to replace the current version with a locally stored database.
- **File Rating Database Version** - The version of the file rating database used by Endpoint Manager. Click 'Security Sub-Systems' > 'Application Control' in Endpoint Manager to view the file rating interface.
- **Valkyrie** - Indicates whether or not Valkyrie is enabled. Click 'Show' to view your Valkyrie account activation number.
- **Websites Database** - The version number of website filtering database. The database contains list of websites categorized such as malicious, phishing, suspicious and so on and used by CCS to apply web filter rules. Click 'Settings' > 'Website Filtering' to configure **web filter rules**.
- Click VirusScope Details to view the VirusScope recognizers that are active on your system. See '**VirusScope Settings**' for more details.

1.5.2. The Tasks Interface

- Click 'Tasks' on the top-left of the home screen
- The tasks area lets you configure every aspect of Comodo Client Security.

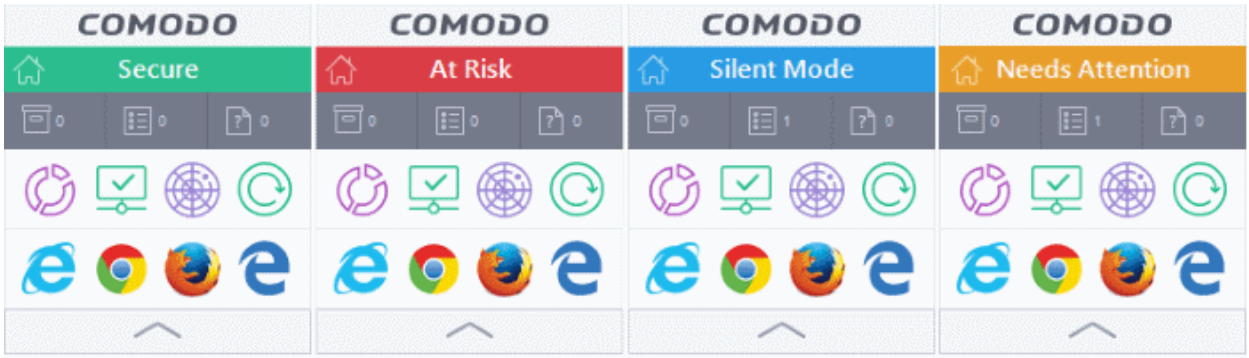


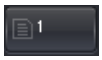
Tasks are broken down into four main sections. Click the following links for more details on each:

- **General Tasks** - Run antivirus scans, update the virus database, run data loss prevention scans and more. See '**General Tasks**' for more details.
- **Firewall Tasks** - Allow or block internet access for specific applications, manage networks, view active connections, and more. See '**Firewall Tasks**' for more details.
- **Containment Tasks** - Run applications in a secure virtual environment, start the virtual desktop, view active processes, and more. See '**Containment Tasks**' for more details.
- **DLP Tasks** - Run data loss prevention scans and manage quarantined files. See **DLP Tasks**
- **Advanced Tasks** - Create a boot disk to clean highly infected systems, submit files to Comodo for analysis, install other Comodo security software, and more. See '**Advanced Tasks**' for more details.

1.5.3. The Widget

- The CCS widget is a handy control that lets you launch key tasks, view your security status, and more.
- The widget is disabled by default but can be enabled from the '**System Tray Icon**' or the '**User Interface**' settings screen.
- Right-click on the widget to enable or disable CCS components and configure various settings. The menu is similar to the one available if you right-click on the system tray icon. See '**The System Tray Icon**' for more details.

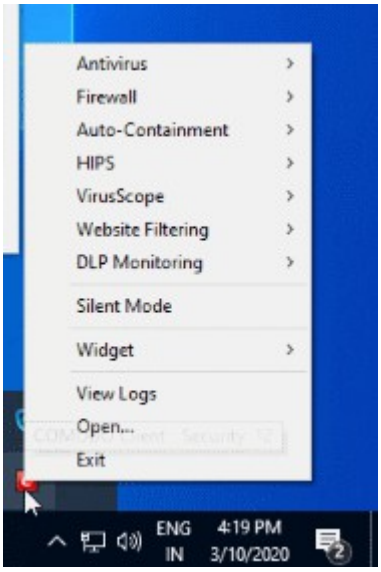


- The color-coded bar at the top of the widget shows your current security status.
  - Double-click on 'At Risk' or 'Needs Attention' statuses to view the recommended fixes.
- The second row tells you about various CCS processes:
  - The first button shows the number of programs/processes that are currently running in the container.
    - Click the button to view a list of all processes running in the container.
    - See **View Active Process List** and **Identify and Kill Unsafe Processes** for more details.
  - The second button shows the number of CCS tasks that are currently running. Click the button to open the '**Task Manager**' interface.
  - The third button  shows how many unrecognized files have been added to the **file list** and are pending submission to Comodo. Click the button to view a list of these files.

  The status pane is disabled by default. Right-click on the tray icon then select 'Widget' > 'Show Status Pane' to enable it.
- The third row contains shortcuts for the common tasks you see on the CCS home screen.
  - Click a shortcut on the widget to run the task.
  - The common tasks row is disabled by default. Right-click on the tray icon then select 'Widget' > 'Common Tasks' to enable it.
- The fourth row shows browsers installed on your computer.
  - Click a browser icon to run the browser in the container. You can tell the browser is running in the container because it has a green border around it. See '**Run an application inside the container**' if you want to read more on this.
  - The browsers row is disabled by default. Right-click on the tray icon then select 'Widget' > 'Show Browsers Pane' to enable it.
- You can expand or collapse the widget by clicking the arrow at the bottom.

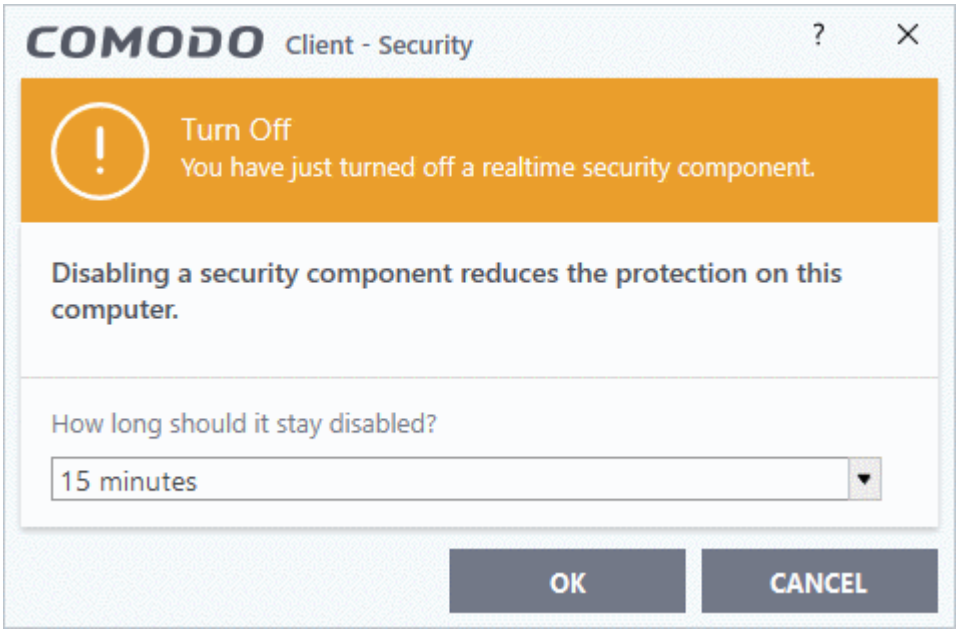
1.5.4. The System Tray Icon

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



- **Antivirus** - Enable or disable the real-time virus monitor.
- **Firewall** - Enable or disable the firewall.
- **Auto-Containment** - Enable or disable auto-containment. See '**Auto-Containment Rules**' for more details.
- **HIPS** - Enable or disable the host intrusion protection system.
- **VirusScope** - Enable or disable VirusScope.
- **Website Filtering** - Enable or disable website filtering

The security panel and the widget will turn red if you disable any of the security components listed above. You will also see a pop-up which lets you specify how long to keep the feature disabled:



- Select the period and click 'OK'.

Unless you select 'Permanently', the security component will be re-enabled after the set time period. You can manually re-enable the component at any time by right-clicking the tray icon and selecting 'Enable'.

- **Silent Mode** - Disables CCS alerts and activities that could potentially interrupt your work.

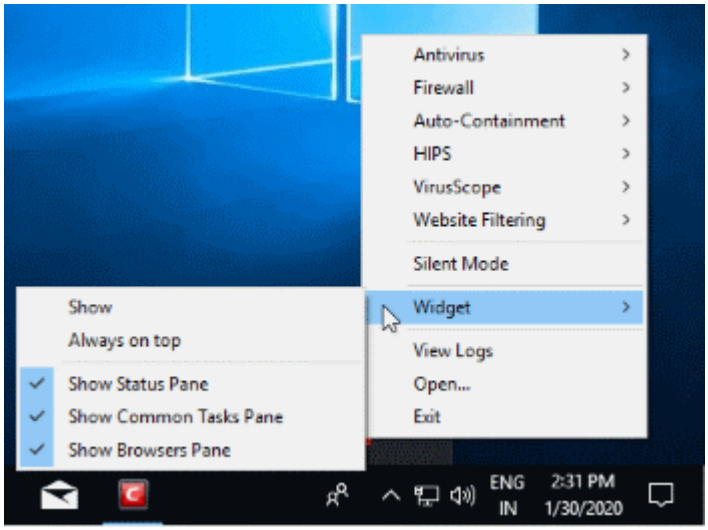
  In silent mode:

  - All security and protection technologies remain fully active

- HIPS/Firewall alerts are suppressed
- AV updates and scheduled scans are postponed

Deactivate silent mode to resume alerts and scheduled scans.

- **Widget** - Select whether or not the **Widget** is shown, and configure widget elements:



  - **Show**: Toggle widget visibility. (***Default = Disabled***)
  - **Always on top**: Shows the widget on top of all windows currently running on your computer. (***Default = Disabled***)
  - **Show Status Pane**: Show overall security status in the widget (***Default = Disabled***)
  - **Show Common Tasks Pane**: Show shortcuts to common CCS tasks in the widget. (***Default = Enabled***)
  - **Show Browsers Pane**: Show shortcuts to browsers in the widget. (***Default = Enabled***)
- **View Logs** - Opens the CCS log viewer module. The log viewer contains a history of events from various CCS security modules. See **View CCS Logs** for more details.
- **Open** - Opens the CCS interface.
- **Exit** - Closes the CCS application.

1.6. Understand Security Alerts

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

Alerts Overview

- CCS alerts warn you about security related activities at the moment they occur.
- Each alert contains information about a particular issue so you can make an informed decision about whether to allow or block it.
- Alerts also let you specify how CCS should behave in future when it encounters activities of the same type.
- The following screenshot shows the basic layout of a CCS alert:

Alert Types

The type of alert you see depends on the security module which generated the alert. Click the links below to find out more about each alert type.

- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts are shown if the **antivirus is enabled** and '**Do not show antivirus alerts**' is disabled in **Real-time Scanner Settings**.
- **Auto-Scan Alerts** - Shown when you connect an external storage device to your computer. Auto-scan alerts are shown if **antivirus is enabled** and '**Do not show auto-scan alerts**' is disabled in **Real-time Scanner Settings**.
- **Firewall Alerts** - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only if **firewall is enabled** and the option '**Do not show popup alerts**' is disabled in **Firewall Settings**.

- **HIPS Alerts** - Shown when a process attempts an unauthorized action or tries to access protected areas. HIPS alerts are shown if **HIPS is enabled** and **Do NOT show popup** alerts is disabled.
- **Containment Alerts** (including **Elevated Privilege Alerts**) - Shown when CCS automatically contains an file. This usually happens if the file has an 'unknown' trust-rating. If privilege elevation alerts are enabled in **Containment Settings**, you will also see this type of alert if a program requires admin privileges to run.
- **VirusScope Alerts** - Shown when a running process tries to perform a suspicious action. VirusScope alerts let you quarantine the process & reverse its changes, or let the process go ahead. Be especially wary if a VirusScope alert appears 'out-of-the-blue' when you have not made any recent changes to your computer. VirusScope alerts are generated if **VirusScope is enabled** in advanced settings.
- **Device Control Notifications** - Shown when an external device that is blocked by the admin is connected to your system. These alerts are shown if 'Device Control' and 'Show notifications when devices...' are both enabled in **Device Control Settings**.

Alerts 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 in he alert.

Note: This section is concerned with alerts generated by CCS security modules (antivirus, firewall, HIPS etc). See **Message Center notifications**, **Notification Messages** and **Information Messages** for other types of alert.

Severity Level

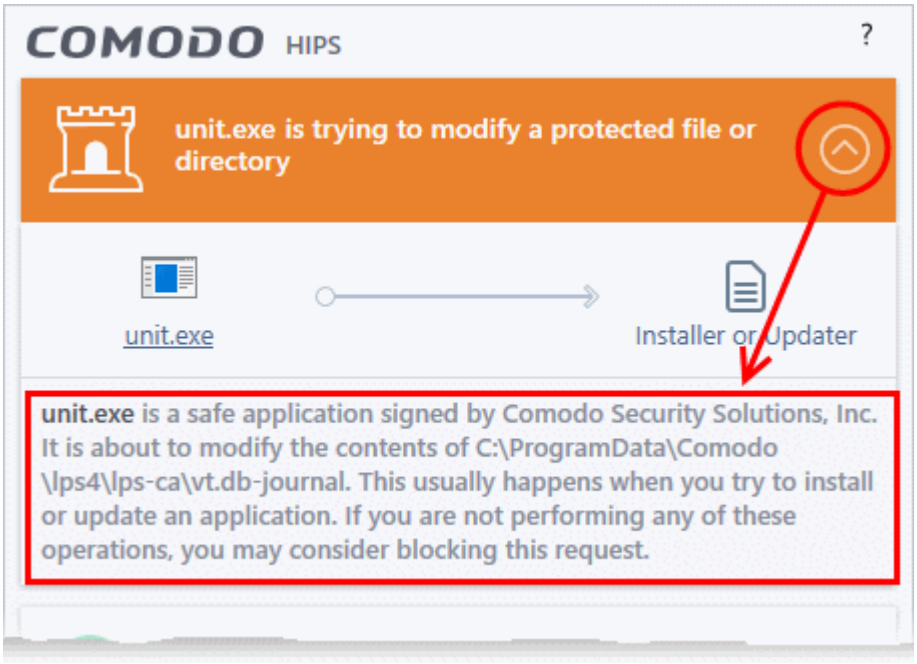
The color of the alert shows the risk level of the reported activity.

- **Yellow** - Low Severity - In most cases, you can safely approve these requests. The 'Remember my answer' option is automatically pre-selected for safe requests
- **Orange** - Medium Severity - Read the information in the alert description area before making a decision. These alerts could be the result of harmless activity by program you trust, but could also indicate malicious activity. If you know the application to be safe, then it is usually okay to allow the request. If you do not recognize the application or connection request then you should block it.
- **Red** - High Severity - Known malware discovered, or highly suspicious behavior by an application/process. Carefully read the information provided when deciding whether to allow it to proceed.

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

Alert Description

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



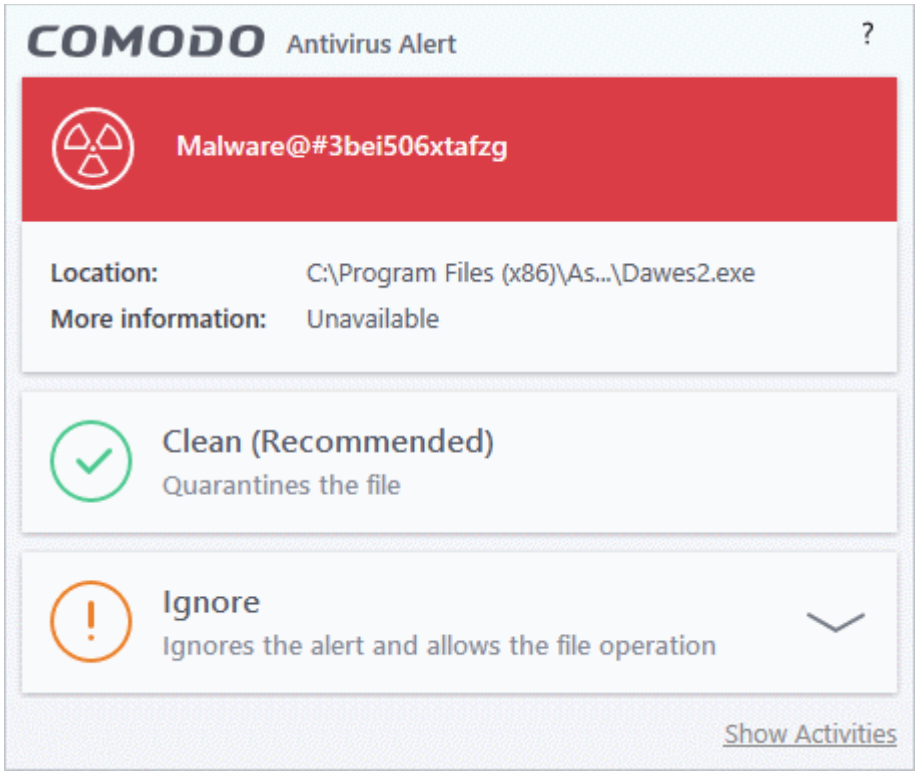
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answer an Antivirus Alert

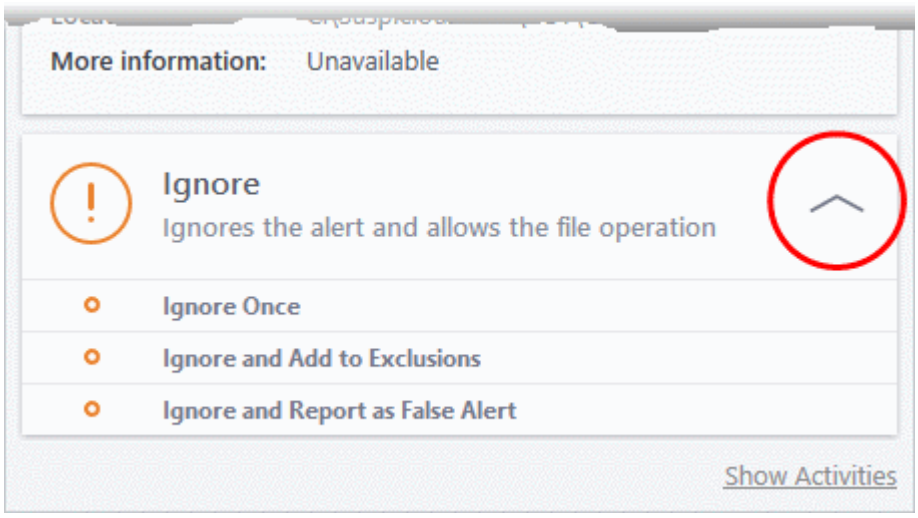
Comodo Client Security generates an antivirus alert whenever a virus or virus-like activity is detected on your computer. The alert contains the name of the virus detected and the location of the file or application infected by it. Within the alert, you are also presented with response-options such as '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, only **antivirus notifications** are shown. This option is found under 'Settings > Antivirus > Realtime Scan'. See **Real-time Scan Settings** for more details.



The following response-options are available:

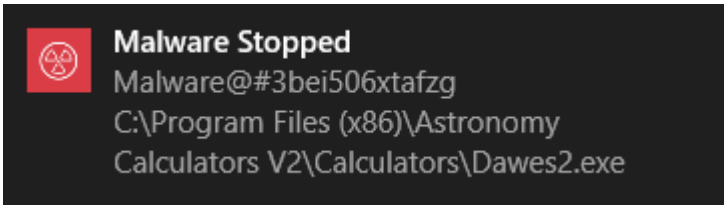
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to quarantine, an isolated storage in which the item is encrypted and stored. Files in the quarantine cannot be executed. If desired, you can submit the file/application to Comodo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



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

Antivirus Notification

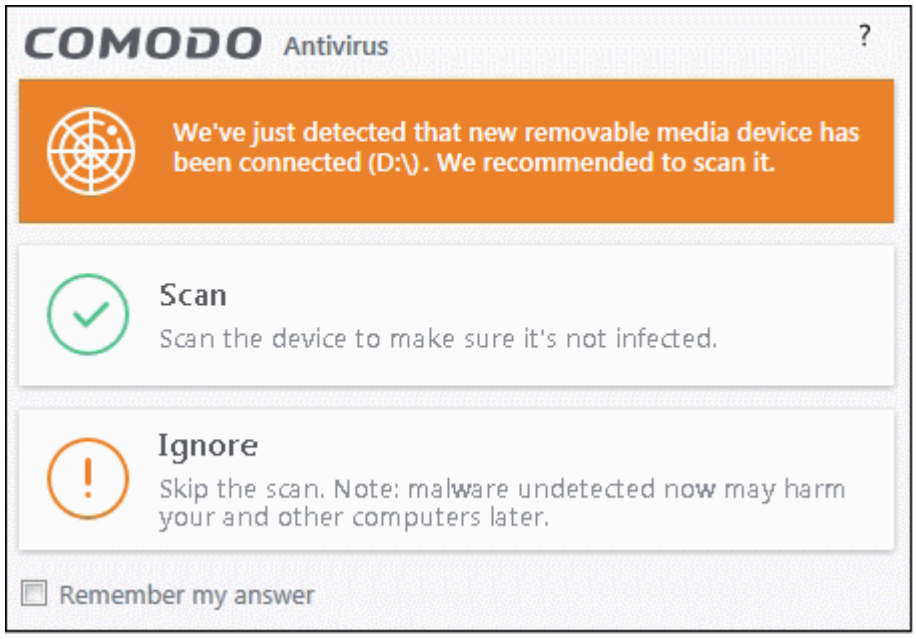
If you have chosen to not to show Antivirus Alerts through **Settings > Realtime Scanner Settings** by leaving the option 'Do not show antivirus alerts' enabled (***default=enabled***) and If CCS identifies a virus or other malware in real time, it will immediately block malware and provide you with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



Answer Auto-Scan Alert

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

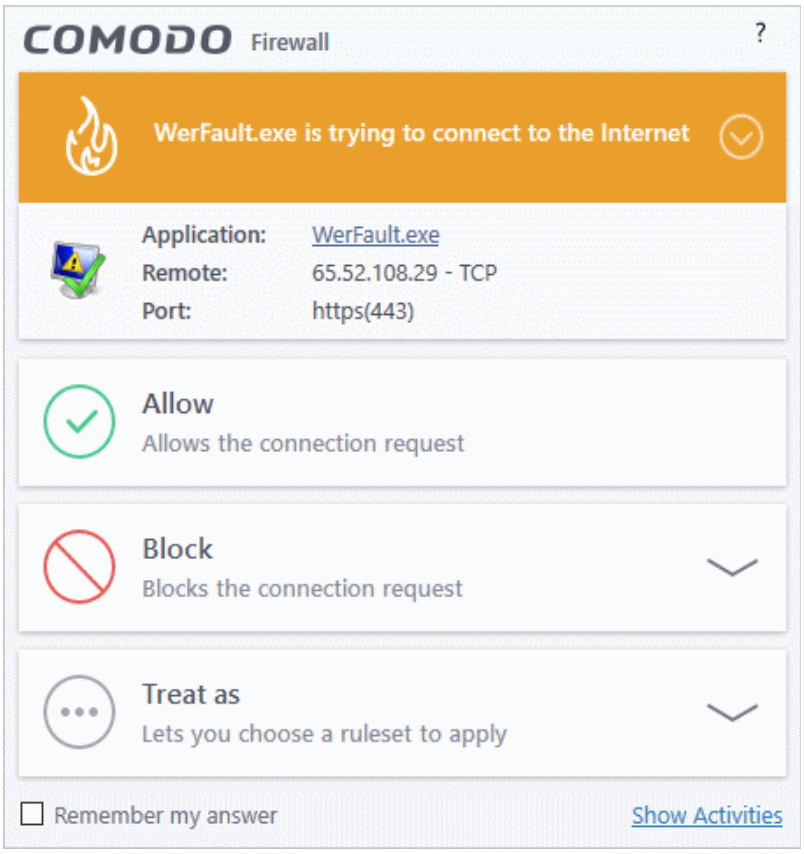
These alerts are only shown if 'Do not show auto-scan alerts' is disabled in 'Settings > Antivirus > Realtime Scan'. See **Real-time Scan Settings** if you want to read more.



- **Scan** - CCS checks the device for viruses using the settings in the 'Manual Scan' profile. If this is not available then the scan uses the settings in the 'Full Scan' profile.
- **Ignore** - The device is not scanned
  - **Remember my answer** - CCS will automatically carry out your choice of scan or ignore when the device is connected in future. This only applies to the specific device. You will still see an alert if you connect a different device.

Answer Firewall Alerts

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

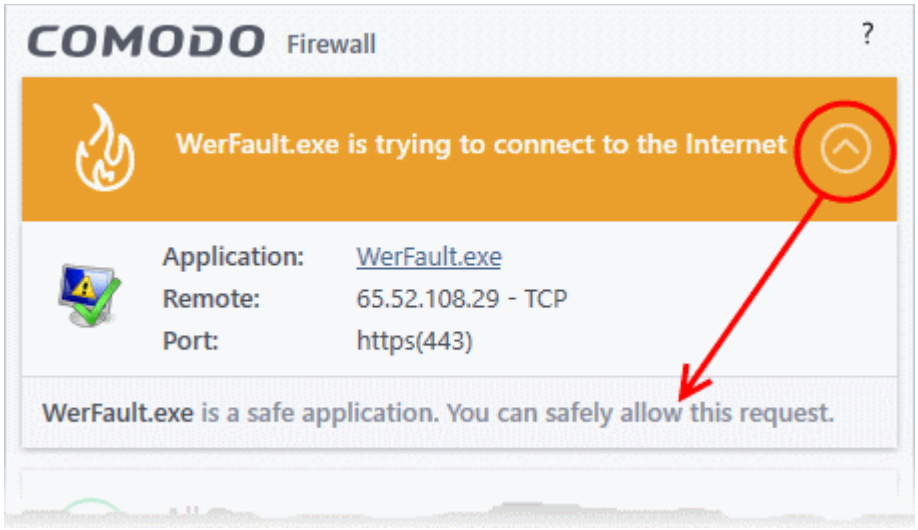


Tip: Click 'Show Activities' to view actions performed by the process in question.

This link is only shown if VirusScope is enabled in **Settings** > **VirusScope**.

The 'Show Activities' link is grayed-out if the process had not started before the alert was generated.

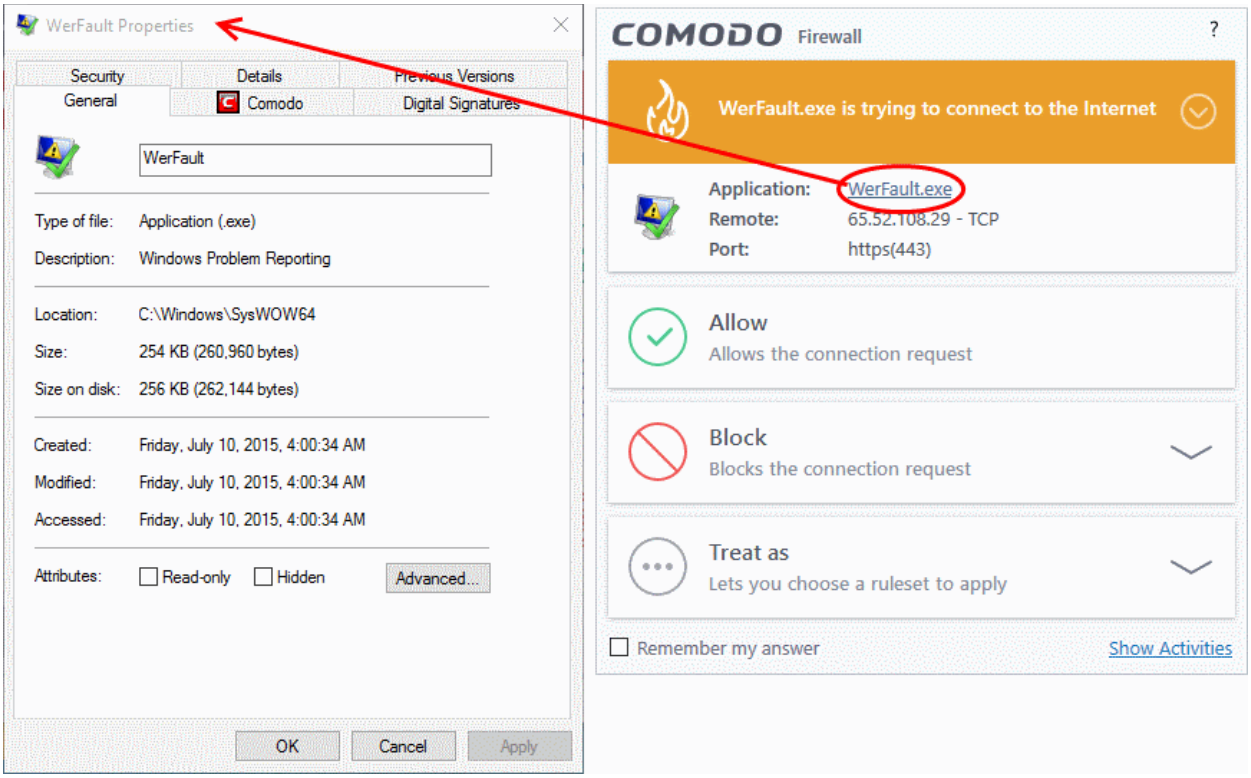
1. Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security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



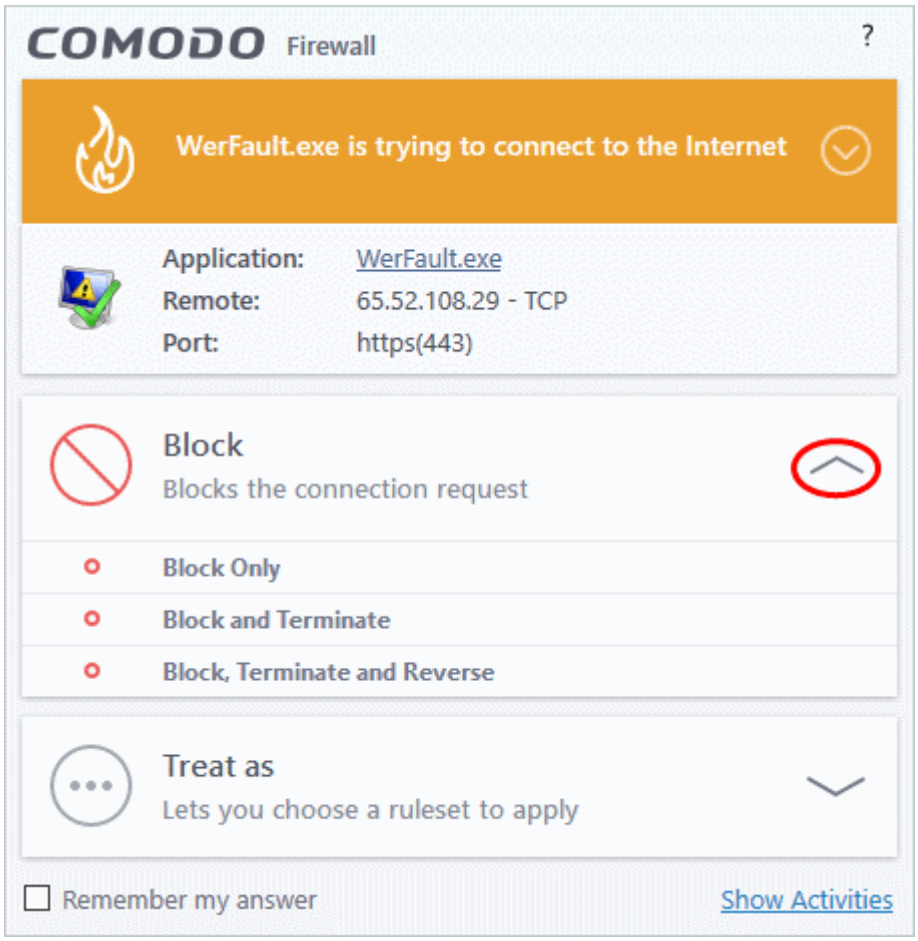
   If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.

In all cases, clicking on the name of the application opens a properties window that can help you determine whether

or not to proceed:



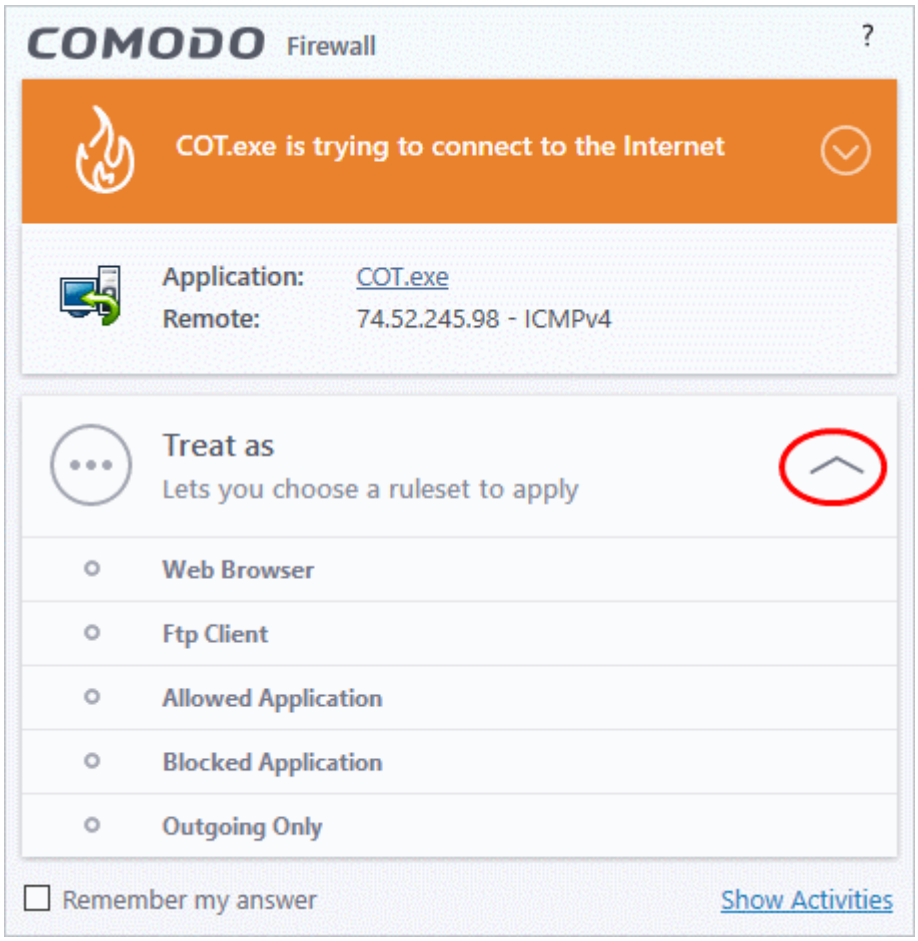
If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand the alert, you can choose to 'Block' the connection (connection is not allowed to proceed), 'Block and Terminate' (connection is not allowed to proceed and the process/application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



Note: 'Block, Terminate and Reverse':

- This option is only available if VirusScope is enabled in **Settings > VirusScope**.
- The option is only shown if the process in question has actually started by the time the alert was generated.

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

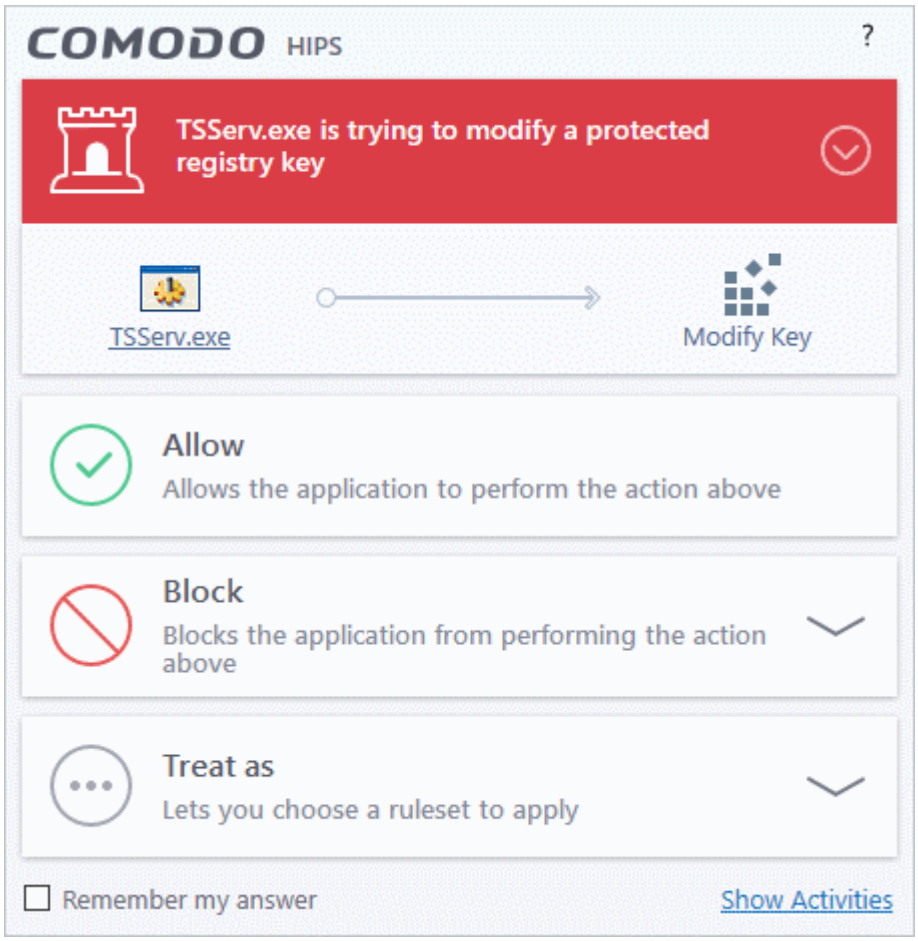


Remember to check the box '**Remember My Answer**' for the ruleset to be applied in future.

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.

Answer HIPS Alerts

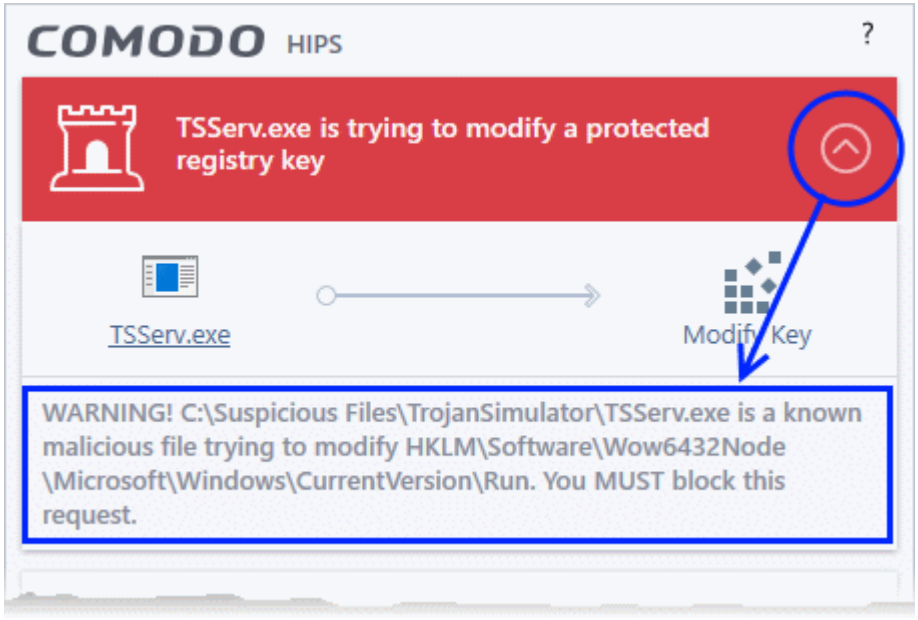
Comodo Client Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:



Tip: Click 'Show Activities' to view actions performed by the process in question.
This link is only shown if VirusScope is enabled in **Settings** > **VirusScope**.

The 'Show Activities' link is grayed-out if the process had not started before the alert was generated.

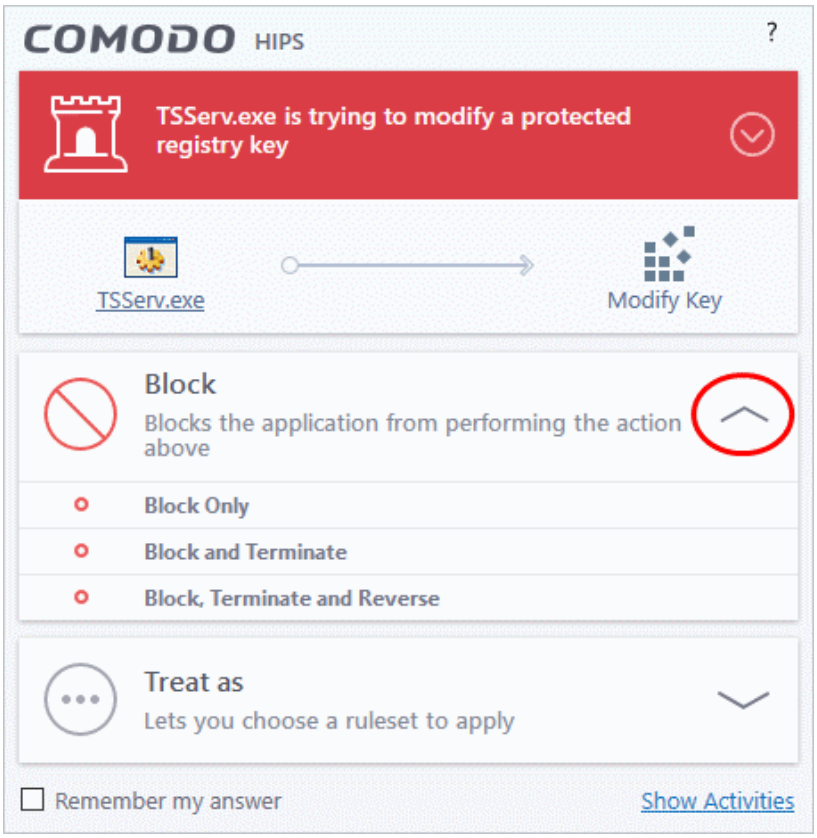
1. Carefully read the information displayed after clicking the handle under the alert description. Comodo Client Security can recognize thousands of safe applications. If the application is known to be safe - it is written directly in the security considerations section along with advice that it is safe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



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

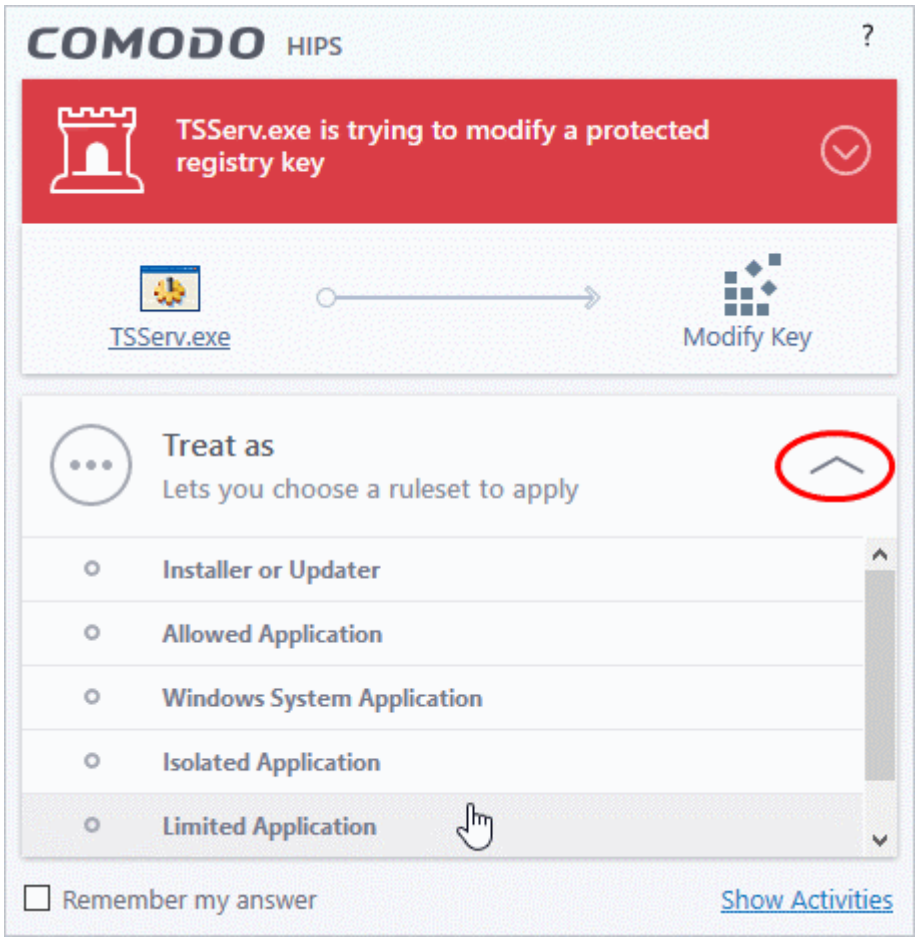
If you don't recognize the application then we recommend you select **Block** the application. By clicking the handle to expand the alert, you can choose to

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



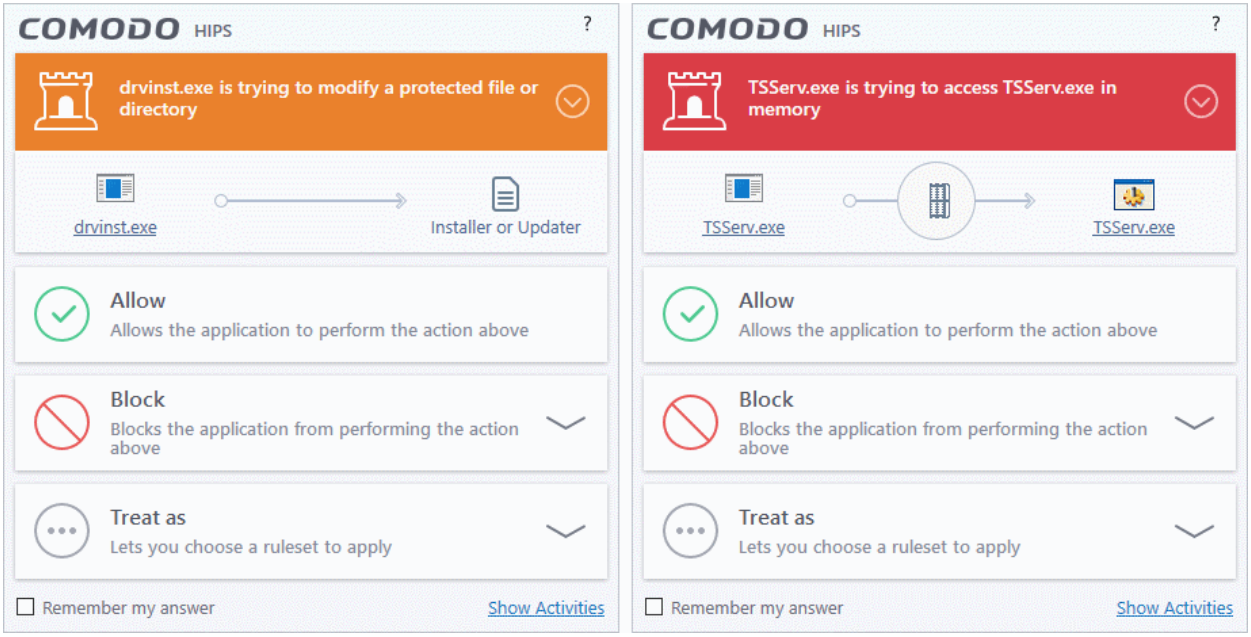
Note: 'Block, Terminate and Reverse' is only shown if VirusScope is enabled in **Settings > VirusScope**.

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

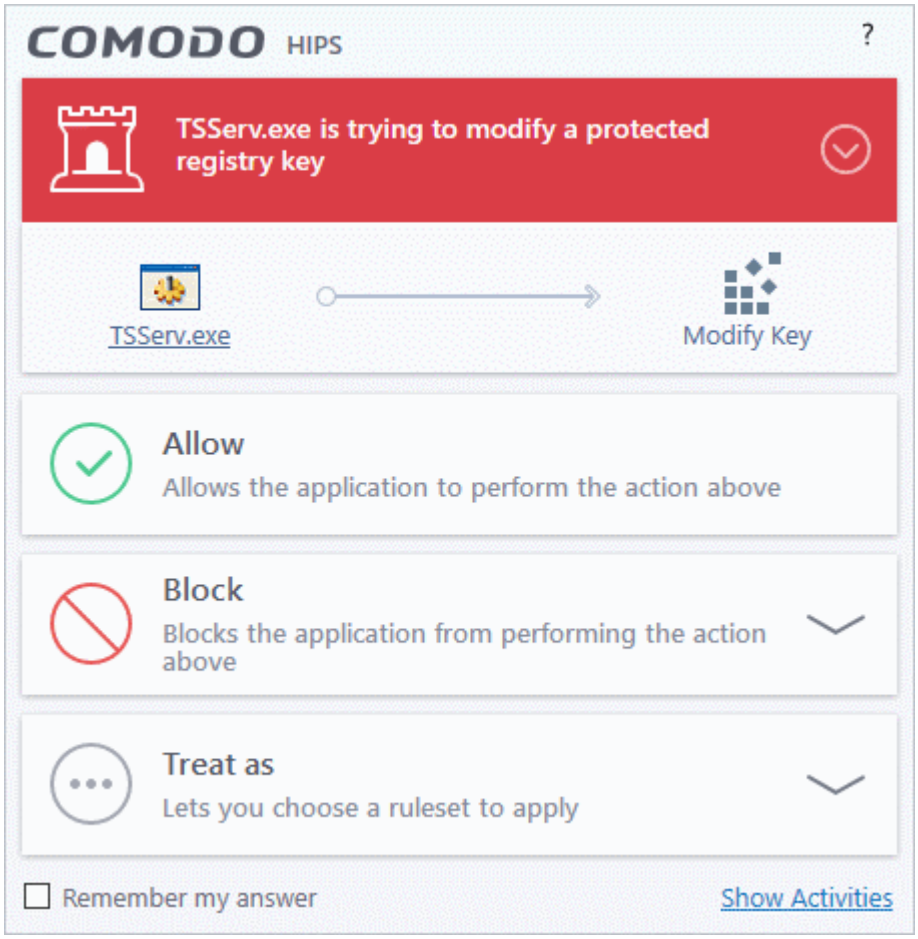


Avoid using the **Installer or Updater** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select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

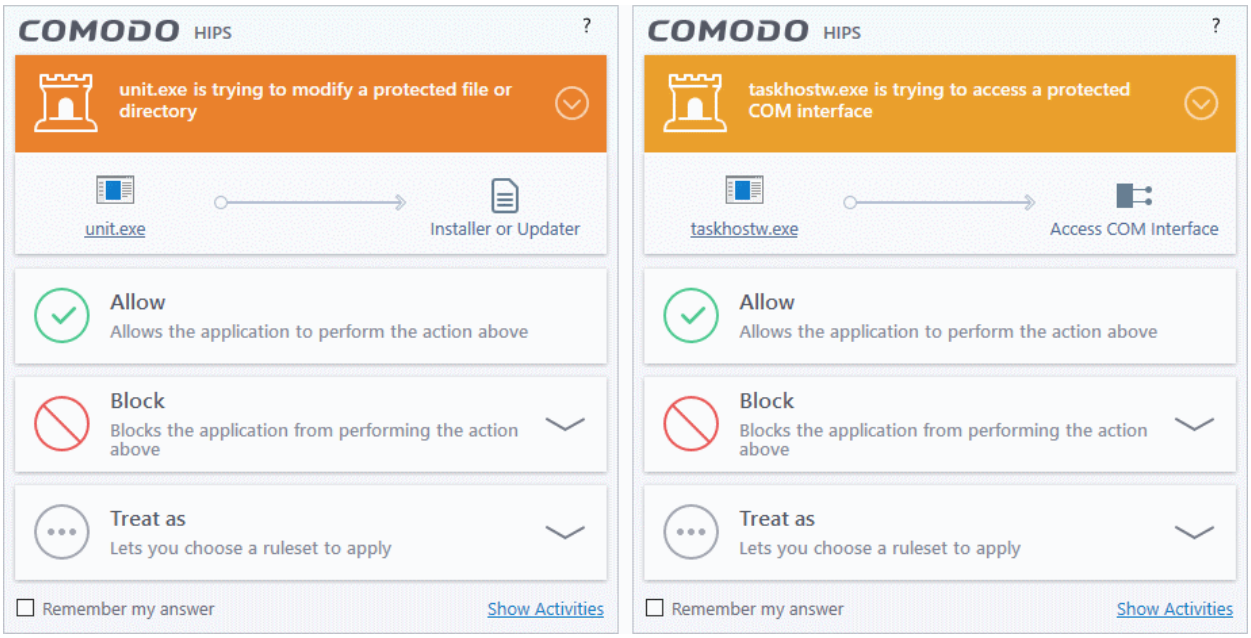
3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity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



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



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



Were you installing new software or trying to download an application from the Internet? If you are

downloading a file from the 'net, select **Allow,** without selecting **Remember my answe**r option to cut down on the creation of unnecessary rules within the firewall.

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

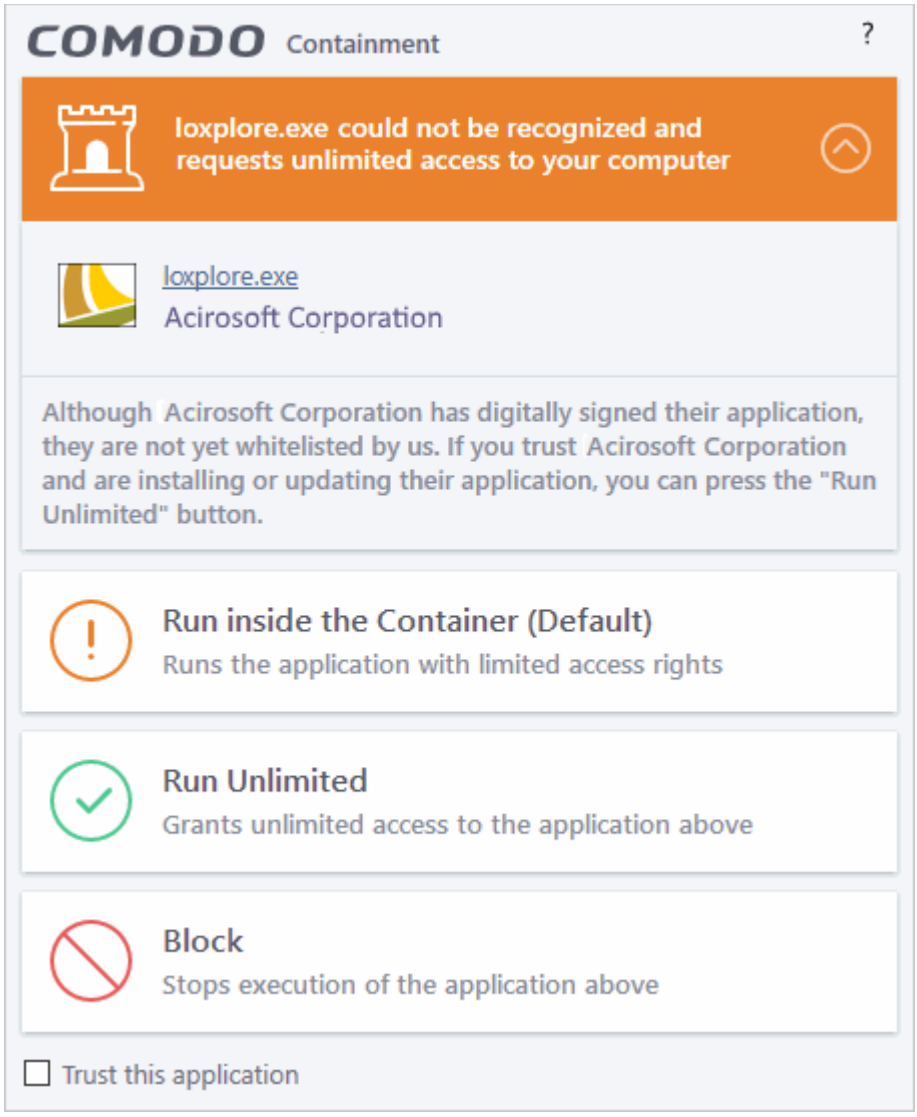
If an application is trying to create a new file with a random file name e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by clicking **Treat As** and choosing **'Isolated Application'** from the options.

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

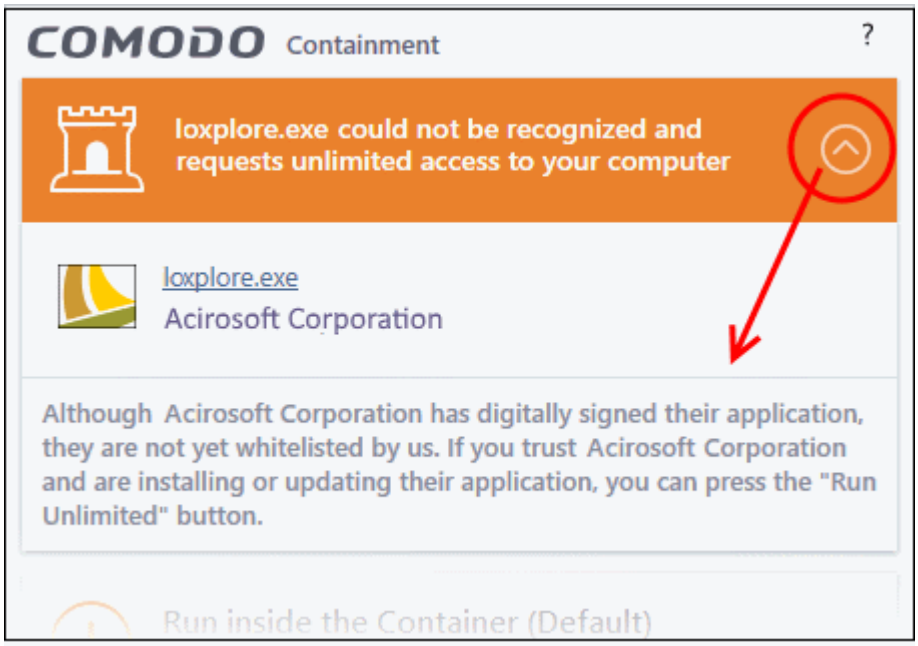
Answer a Containment Alert

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

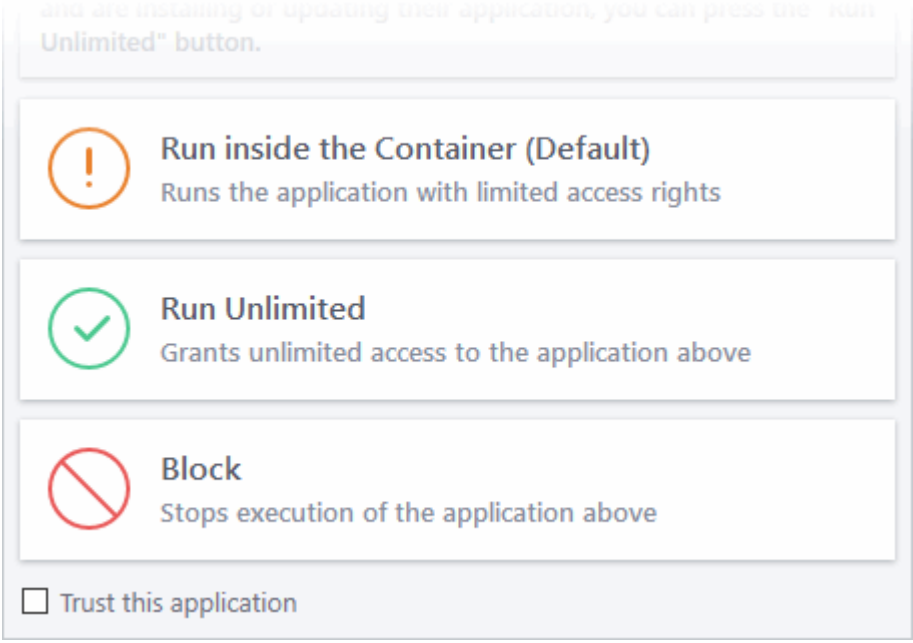
Please read the following advice before answering a Containment alert:



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



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



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

Run with Elevated Privileges Alert

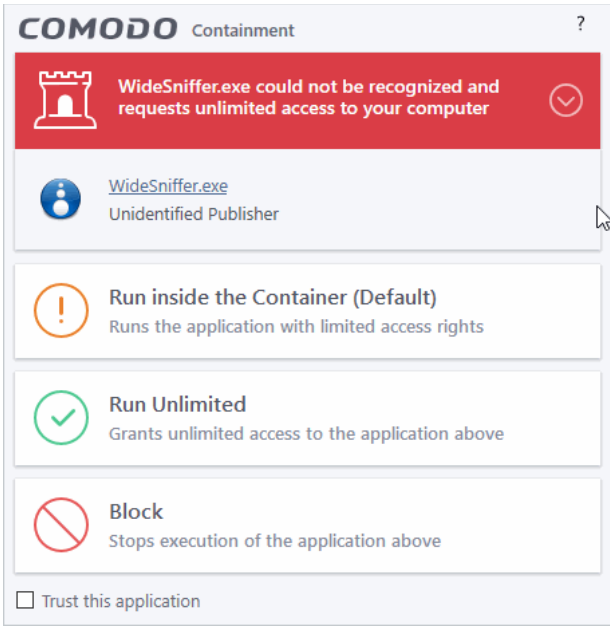
The container will display this kind of alert when the installer of an unknown application requires administrator, or elevated, privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry.

- If you have good reason to trust the publisher of the software then you can click the '**Run Unlimited**' button. This will grant the elevated privilege request and allow the installer to run.

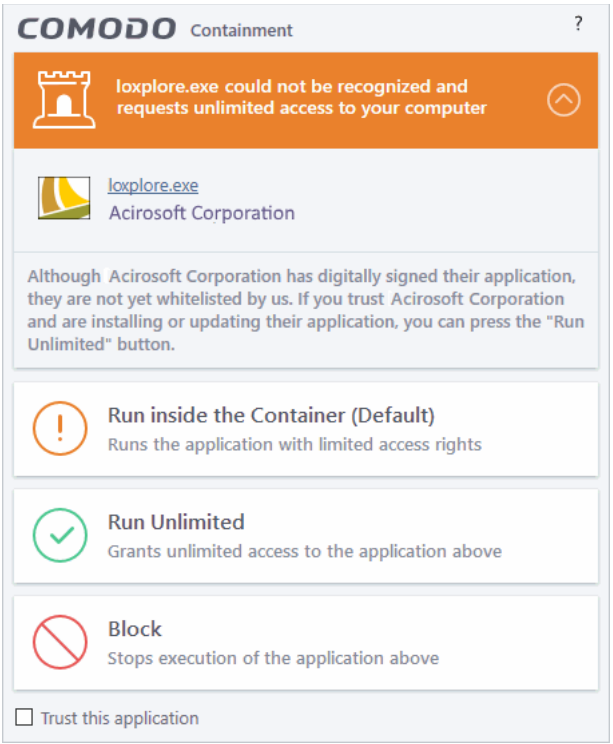
- If you are unsure of the safety of the software, then We recommend that you run it with restricted access to your system resources by clicking the 'Run Isolated' button.
- If this alert is unexpected then you should abort the installation by clicking the 'Block' button (for example, you have not proactively started to install an application and the executable does not belong to an updater program that you recognize)
- If you select 'Trust this application' then CCS will include this to Trusted Files list and no future alerts will be generated when you run the same application.

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

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



Unknown and not digitally signed



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

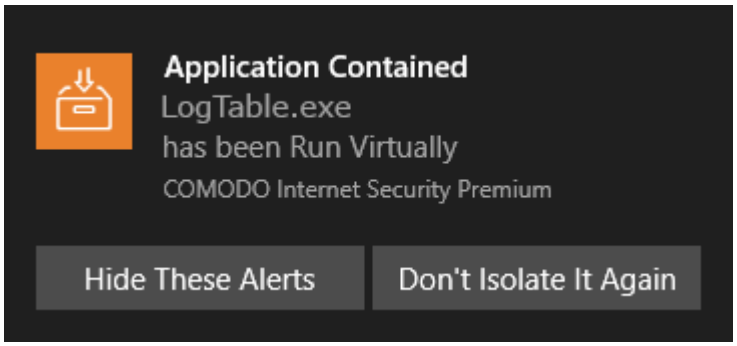
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

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

Containment Notification

CCS shows a notification when it run an application inside the container. This usually happens if the application has an 'unknown' trust-rating.



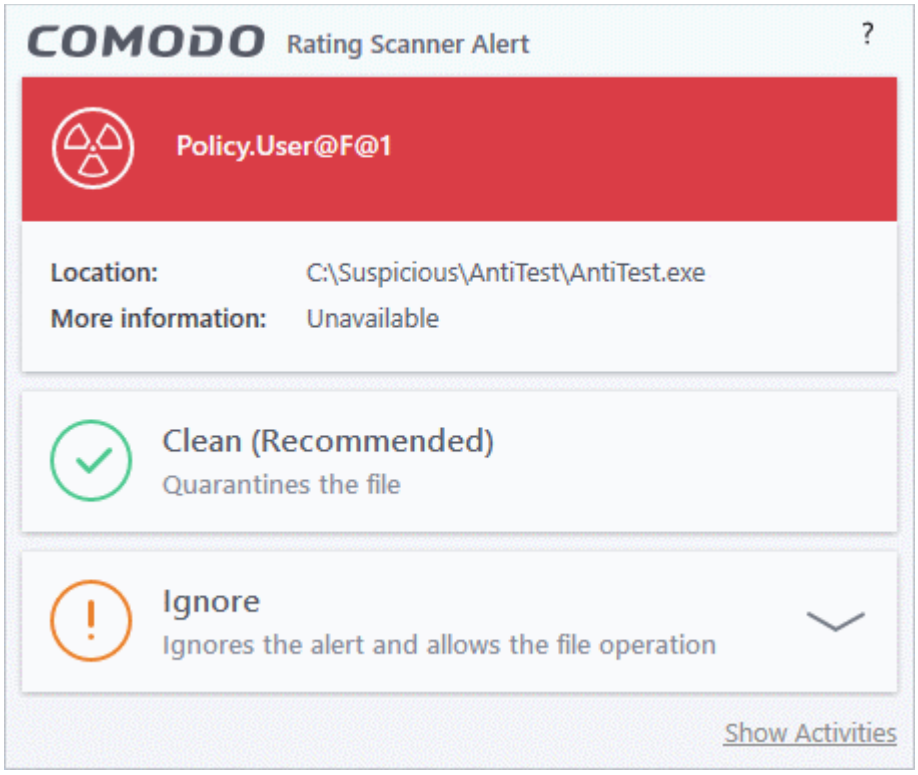
- **Hide These Alerts** - CCS will not show an alert if the same app is auto-contained in future.
- **Don't Isolate It Again** - The application will not be auto-contained in future. An 'Ignore' rule is created for the application in auto-containment rules. See **Auto-Containment Rules** for more on this.

Answer File Rating Alerts

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

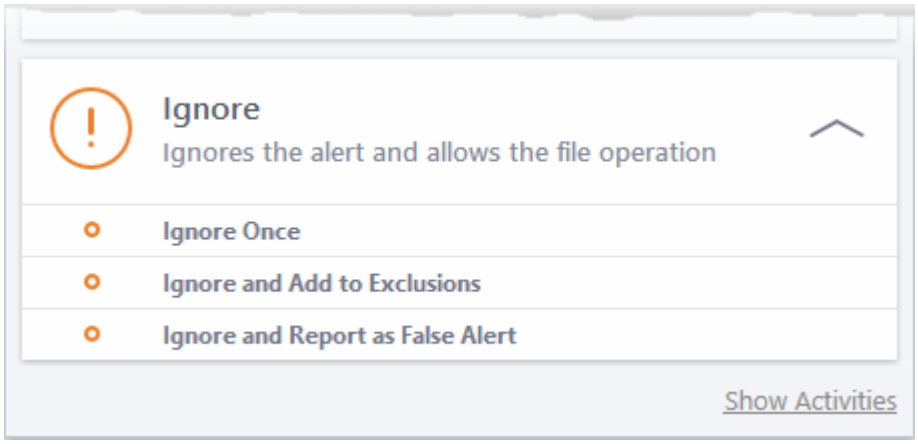
You will see these alerts if you have ***disabled*** 'Do not show popup alerts' in 'Settings' > 'File Rating' > 'File Rating Settings'.

An example alert is shown below:



You can choose from these actions:

- **Clean** - The program is blocked and quarantined
- **Ignore** - Allows the file to run. Does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:



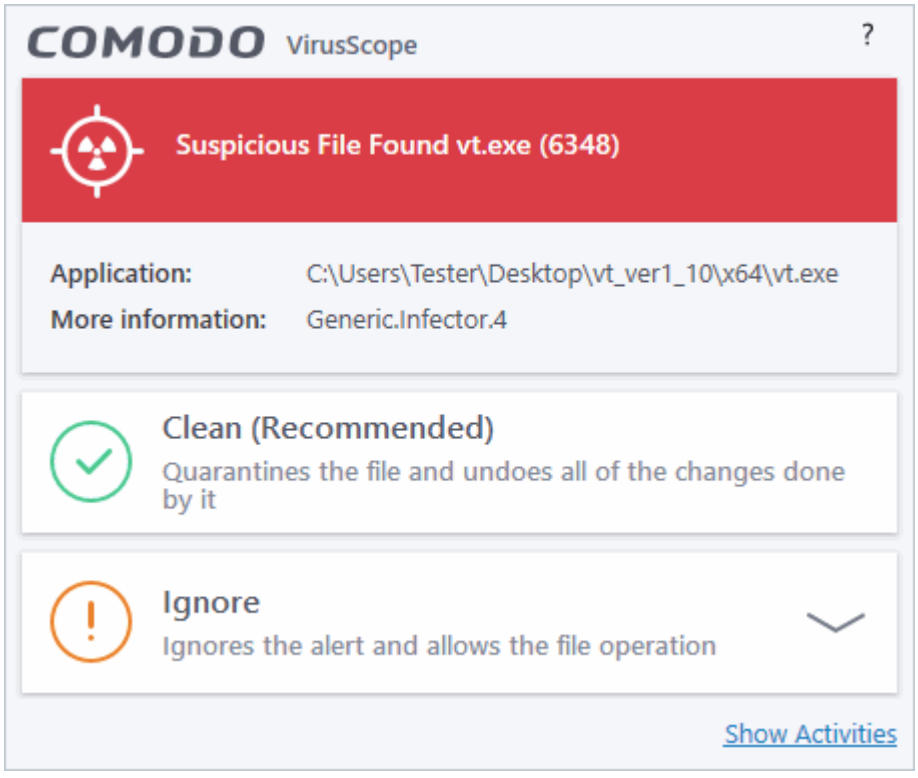
- **Ignore Once** - The file is allowed to run this time, but it will still be flagged as a threat by future scans.
- **Ignore and Add to Exclusions** - The file is allowed to run this time, and will not be flagged as a threat in future scans. The file is placed on the **Exclusions** list, meaning it is ignored permanently by the scanner.
- **Ignore and Report as a False Alert** - The file is allowed to run this time, and submitted to Comodo for analysis. Select this option if you think the file is safe, and that CCS was wrong to flag it as a threat. Comodo will re-examine the file.

Answer a VirusScope Alert

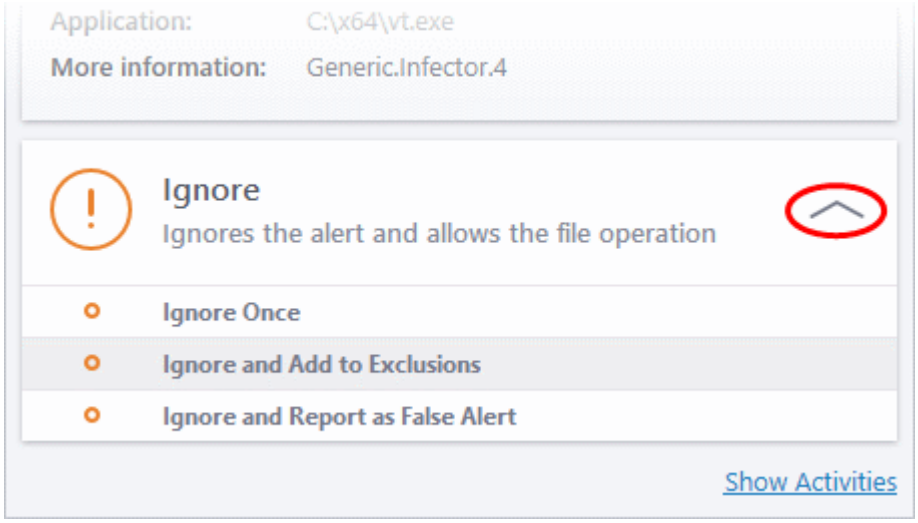
Comodo Client Security generates a VirusScope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that VirusScope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a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

Please read the following advice before answering a VirusScope alert:

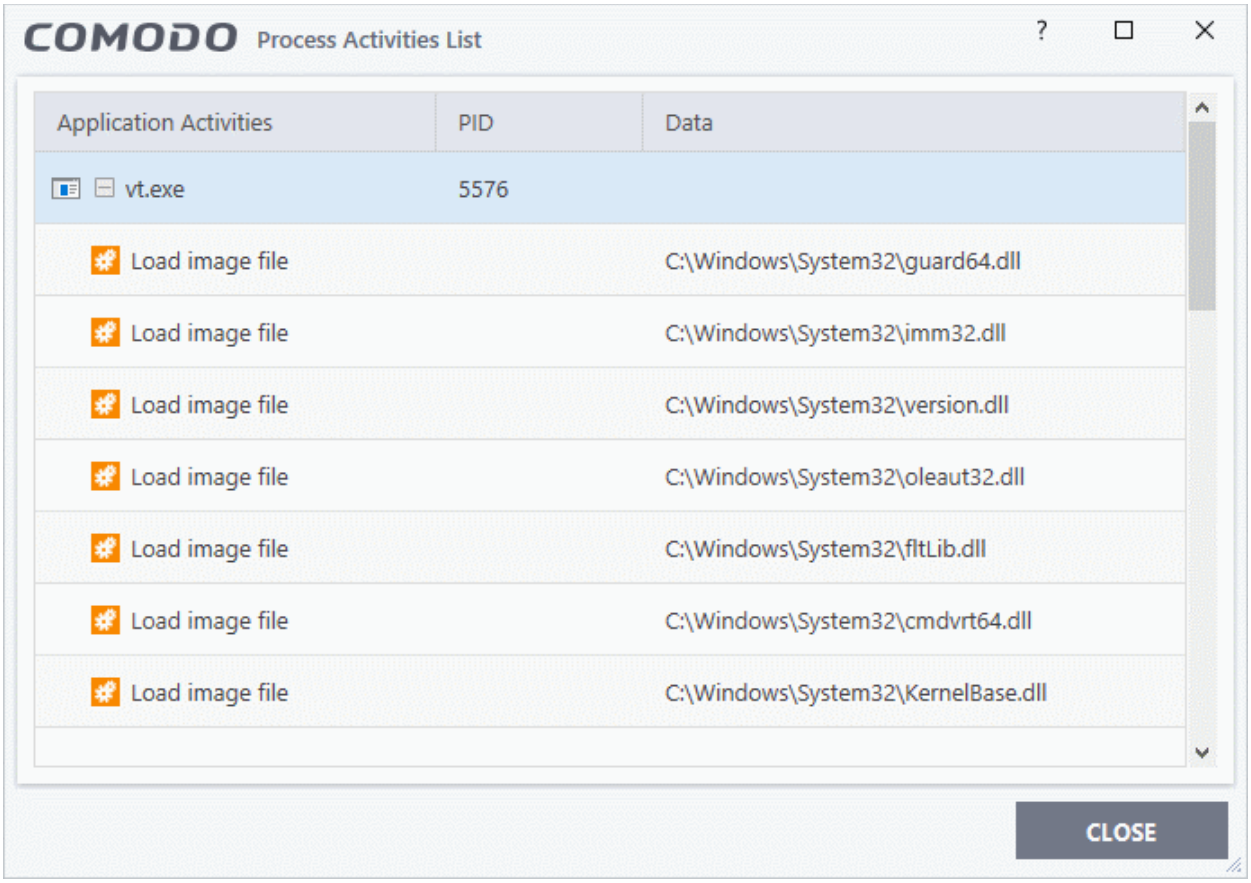
1. Carefully read the information displayed in the alert. The 'More Information' section provides you the nature of the suspicious action.



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



  - **Ignore Once** - The process is allowed to run this time only. Another alert is shown if the process attempts to execute on future occasions.
  - **Ignore and Add to Exclusions** - The file is allowed to run and will not be contained in the future. See **Auto-Containment Rules** for help to configure which types of files should be auto-contained.
  - **Ignore and Report as False Alert** - Select this if you think the file is trustworthy and CCS is wrong to block it. CCS will submit the file to Comodo for analysis. If the false-positive is verified (and the file is trustworthy), it will be added to the safe list.
- Click the 'Show Activities' link to view the actions of the process:

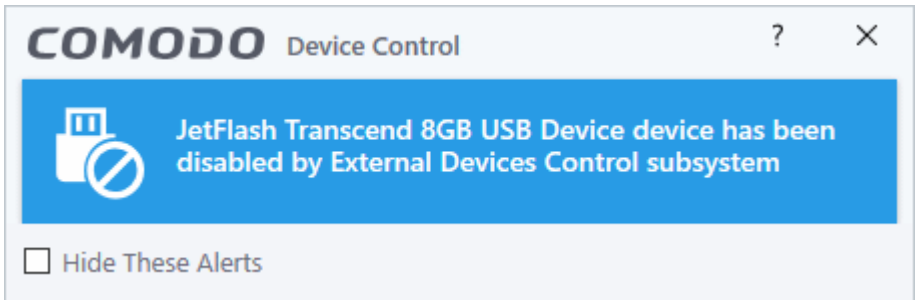


- **Application Activities** - The action executed by each of the processes run by the parent application.
  - - File actions: The process performed a file-system operation (create\modify\rename\delete file) which you might not be aware of.
  - - Registry: The process performed a registry operation (created/modified 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 shown in the list.
- PID - The process identification number.
- Data - The file affected by the action.

Device Control Notifications

These notifications are shown when you connect an external device to your computer (USB stick, external HDD etc). The alert indicates whether the device is allowed or blocked.

- You can add blocked devices in 'Settings' > 'Advanced Protection' > 'Device Control'



- See **Device Control Settings** to find out more.

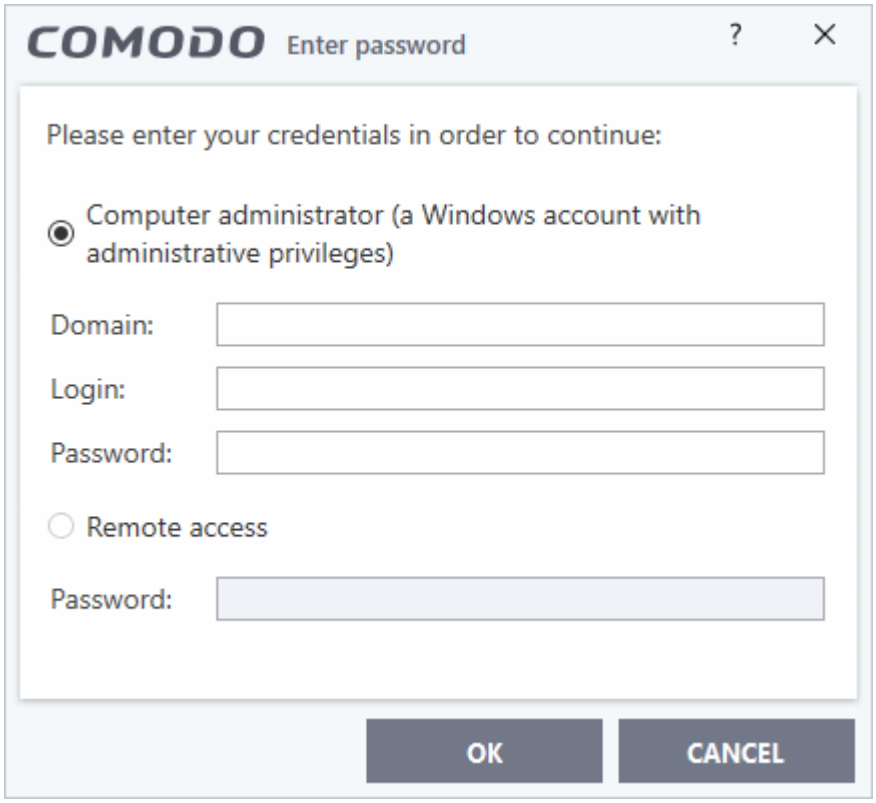
1.7. Password Protection

- In a corporate setup, CCS settings are determined by the Endpoint Manager profile applied to the endpoint.
- One of these settings is the ability to password protect access to the client interfaces. This stops unauthorized users from opening the local clients and making potentially damaging changes.
- Password protection blocks access to the settings area, the various 'Tasks' areas, and the right-click options of the CCS tray icon.
- Local users can, however, still run certain tasks. See Exceptions at the end of this section for more details.

There are two password options you can set in Endpoint Manager:

- **Computer administrator** - CCS requires a local admin password to access the settings area.
  - Admins that are already logged-in can access the settings area without a password.
  - All other users need to enter the admin username/password.
- **Custom password** - An unique key which is set in the Endpoint Manager profile.
- See **https://community.itarian.com/help/topic-459-1-1005-14934-Client-Access-Control.html** for details on the difference between these passwords.

- CCS will request a password if a user tries to access a protected area:



Exceptions

Users can run the following tasks even if password protection is enabled in the Endpoint Manager profile:

On-demand antivirus scans

- Click 'Scan' on the CCS home screen and choose a scan option.
- Click 'Tasks' > 'General Tasks' > 'Scan' > Choose a scan option.
- Right-click on an item and choose 'Scan with COMODO antivirus'.
- See **Scan and Clean Your Computer** and **Instantly Scan Files and Folders** for more details

Virus signature database updates

- Click Tasks > 'General Tasks' > 'Update'.
- See **Manage Virus Database Updates** for more details.

Manually run programs inside the container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'.
- Right-click on an item and choose 'Run in COMODO container'.
- See **Run an Application in the Container** for more details

Run Virtual Desktop

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'.
- See **Start the Virtual Desktop** for more details.

Create Comodo Rescue Disk

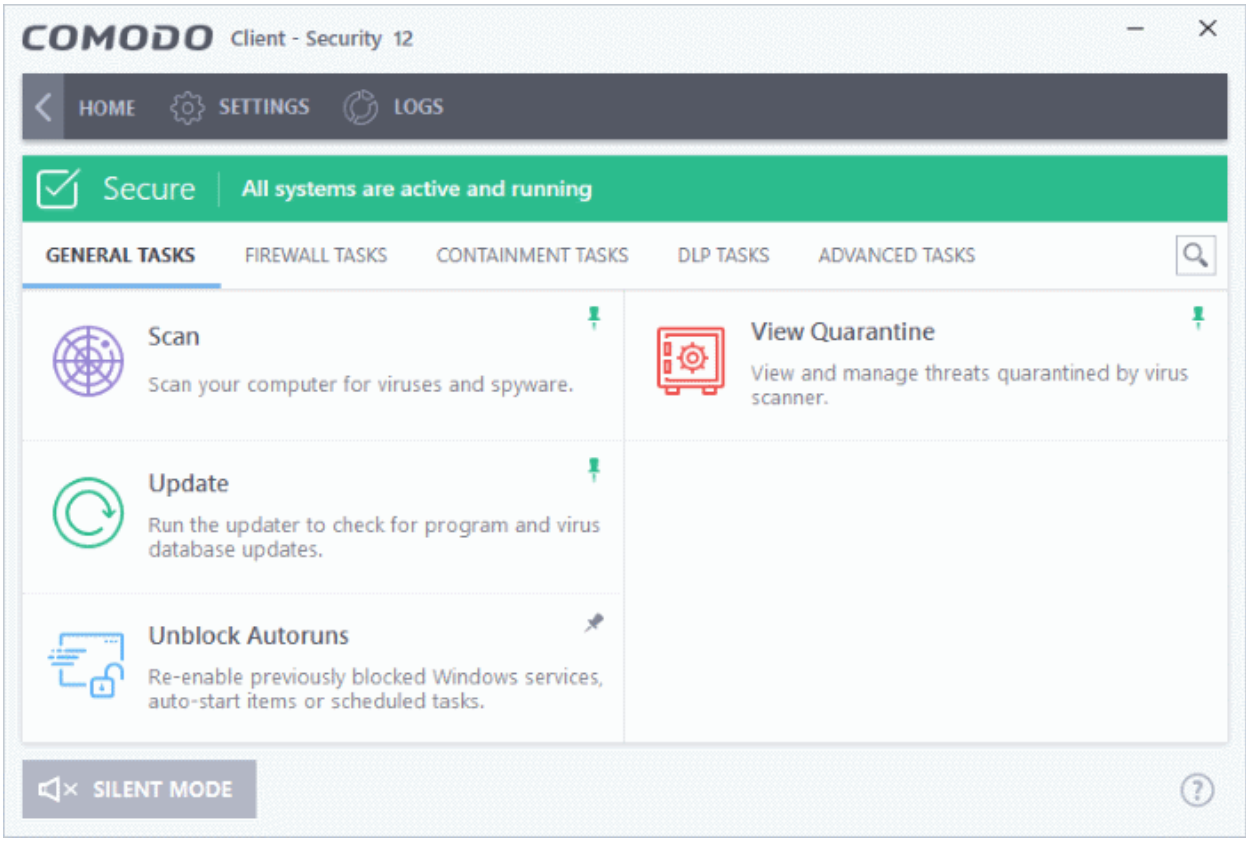
- Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk'.
- See **Create a Rescue Disk** for more details.

2. General Tasks - Introduction

Click 'Tasks' > 'General Tasks'

The general tasks area lets you:

- Quickly run antivirus scans
- Update the virus database
- View and manage items moved to quarantine
- Manage blocked autorun items, Windows services and scheduled tasks.



See the following sections for help with each area:

- **Scan and Clean your Computer**
- **Instantly Scan Files and Folders**
- **Process Infected Files**
- **Manage Virus Database Updates**
- **Manage Blocked Autoruns**
- **Manage Quarantined Items**

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See '**Password Protection**' for more details."

2.1. Scan and Clean Your Computer

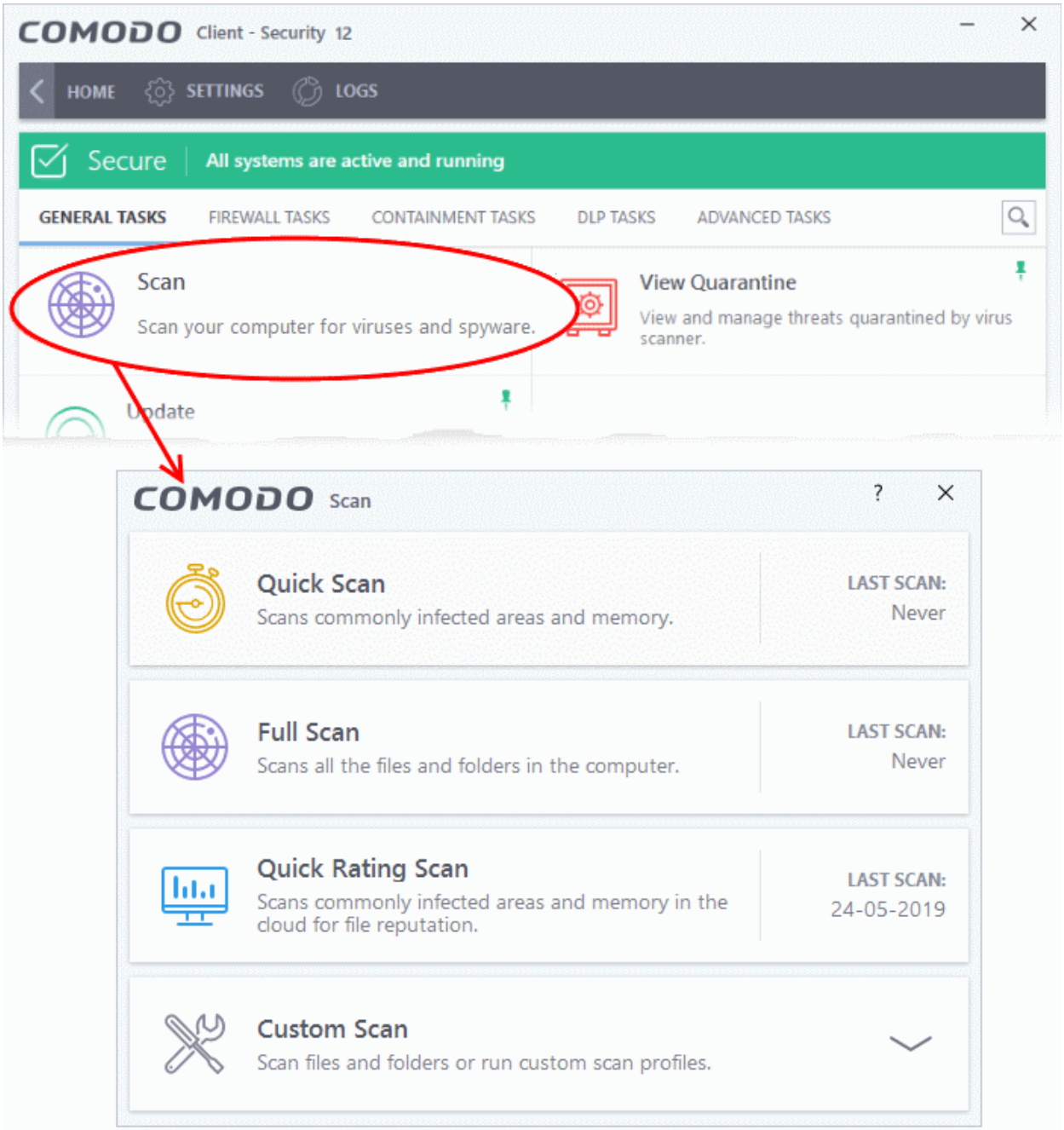
- Click 'Tasks' > 'General Tasks' > 'Scan'
- CCS leverages multiple technologies, including real-time monitoring and on-demand scans, to keep endpoints totally free of malware
- You can schedule a scan to run at a specific time, and also create your own scan profiles to check specific files, folders and drives.

Run an on-demand virus scan

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

  OR

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



- **Quick scan** - Checks important and commonly infected areas
- **Full scan** - Checks your entire computer
- **Rating scan** - Searches for unknown files on your computer. Assigns a trust rating to your files where possible.
- **Custom scan** - You choose specific areas to scan.

The following sections explain more about each scan type:

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

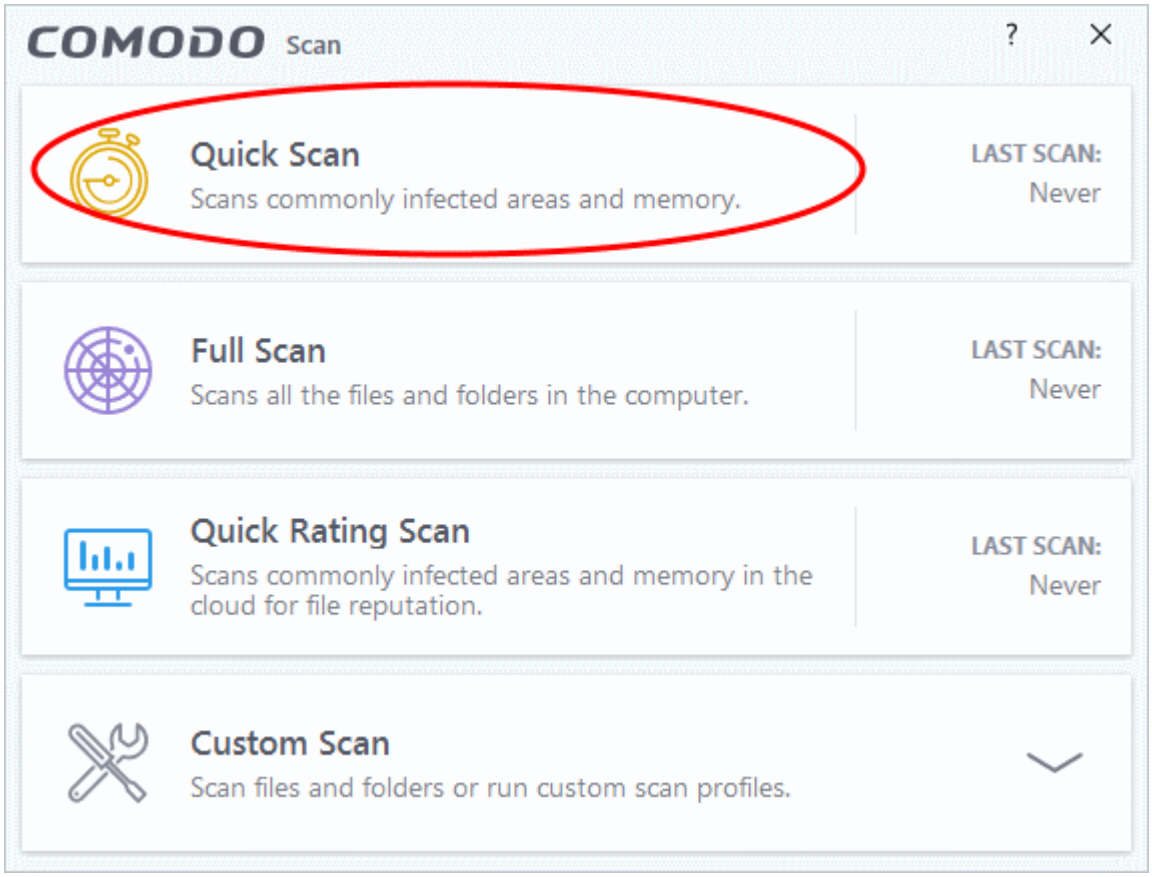
- Scan a File
- Create Schedule and Run a Custom Scan

2.1.1. Run a Quick Scan

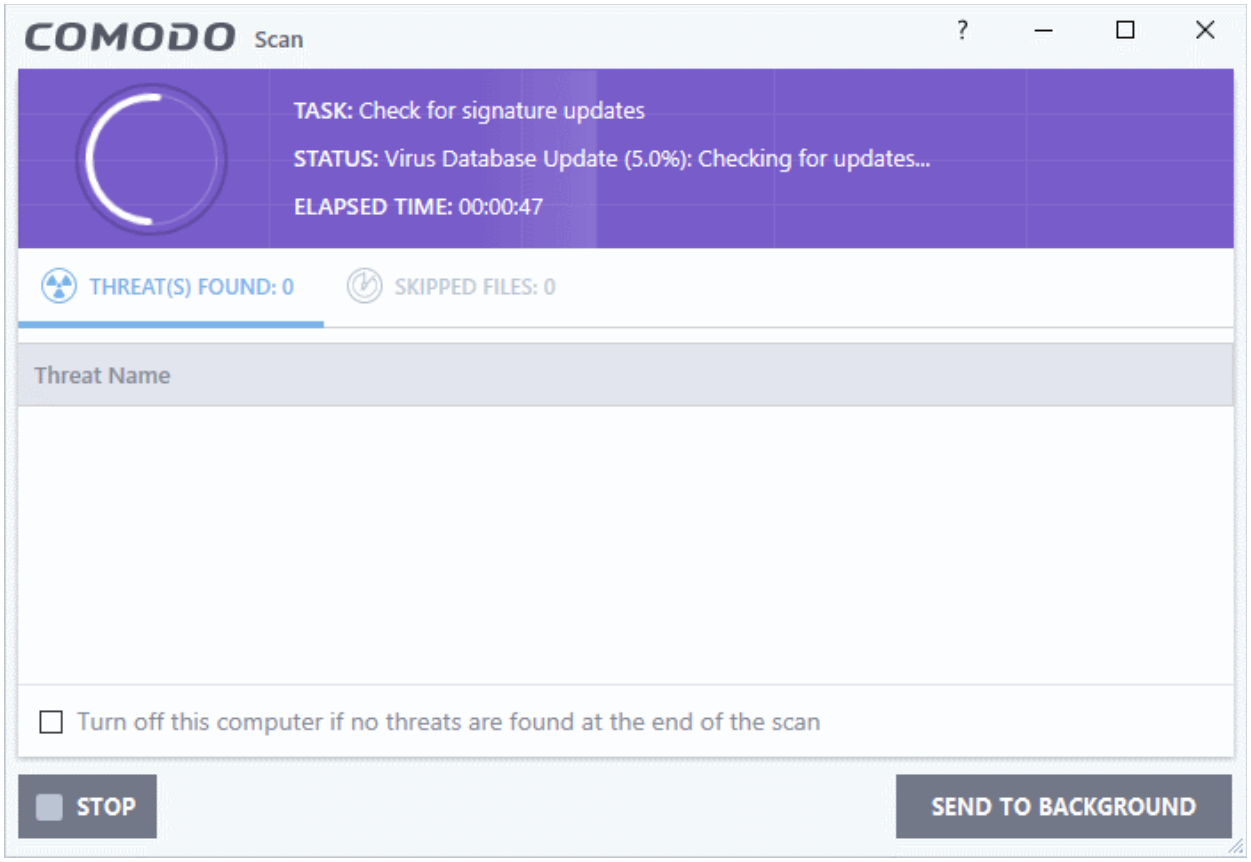
- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Quick Scan'
- The quick scan profile scans important areas of your computer which are most prone to attack.
- This includes system files, auto-run entries, hidden services, boot sectors, and important registry keys.
- These areas are of great importance to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

Run a Quick Scan

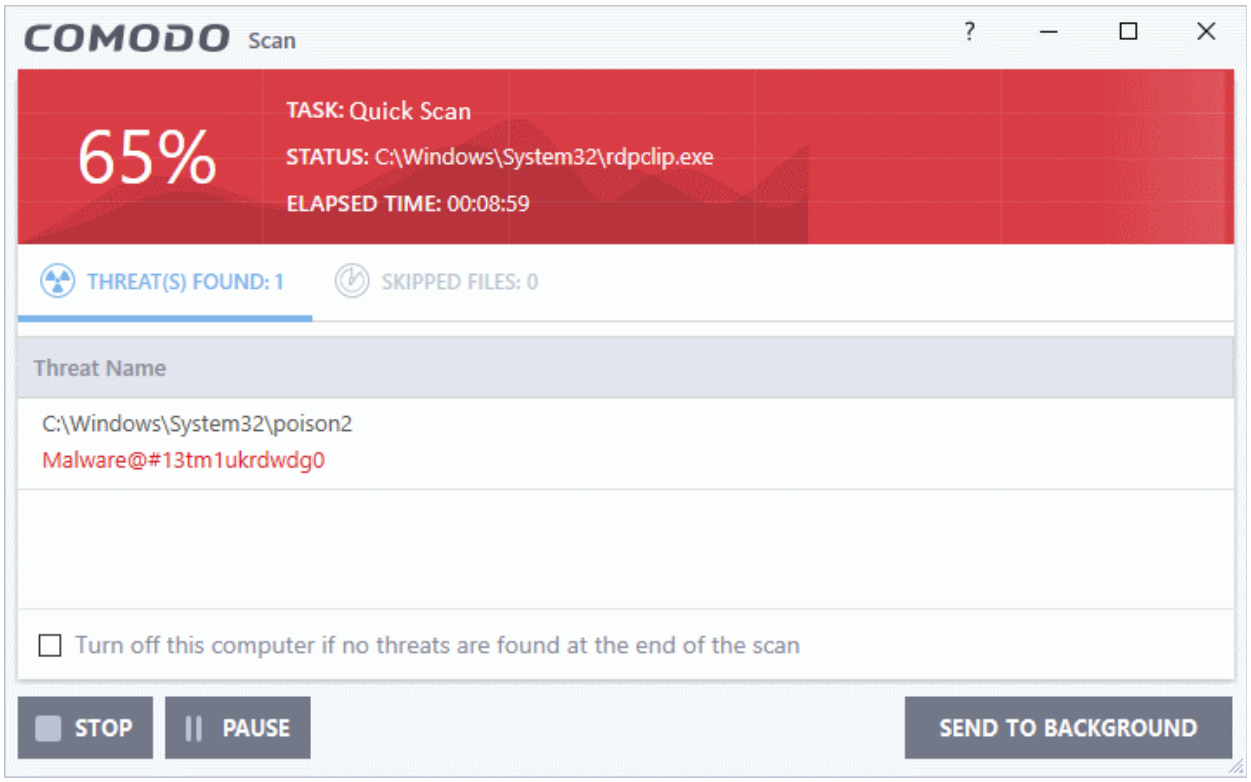
- Click the 'Scan' tile on the CCS home screen
- Select 'Quick Scan' from the 'Scan' interface



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



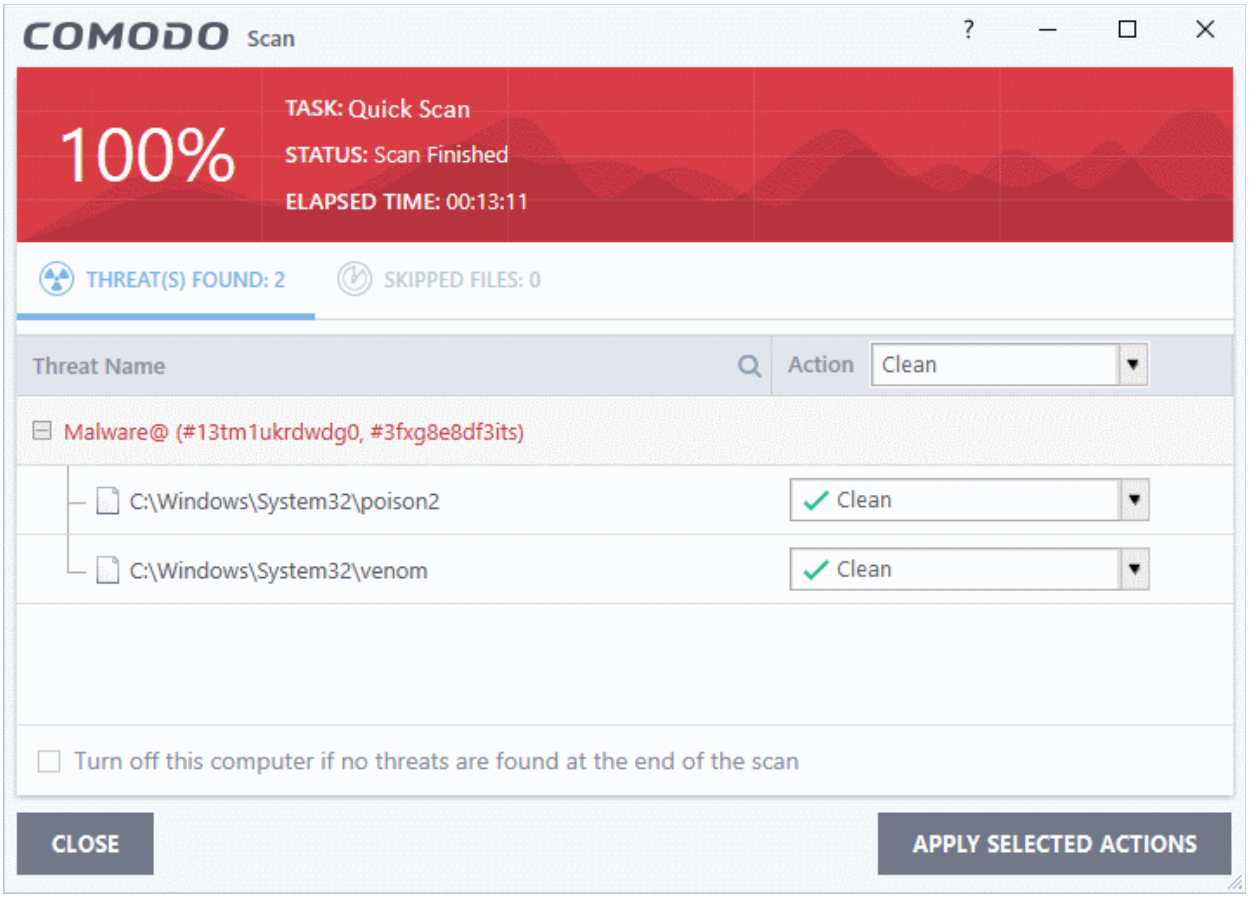
- The scans starts after any updates have been installed:



Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

- You can pause, resume or stop the scan by clicking the appropriate button.
- Send to Background - Runs the scan as a background process which consumes fewer resources. You can still keep track of the scan in the task manager - 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'.

Scan results are shown when the scan finishes:



The results window contains two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

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

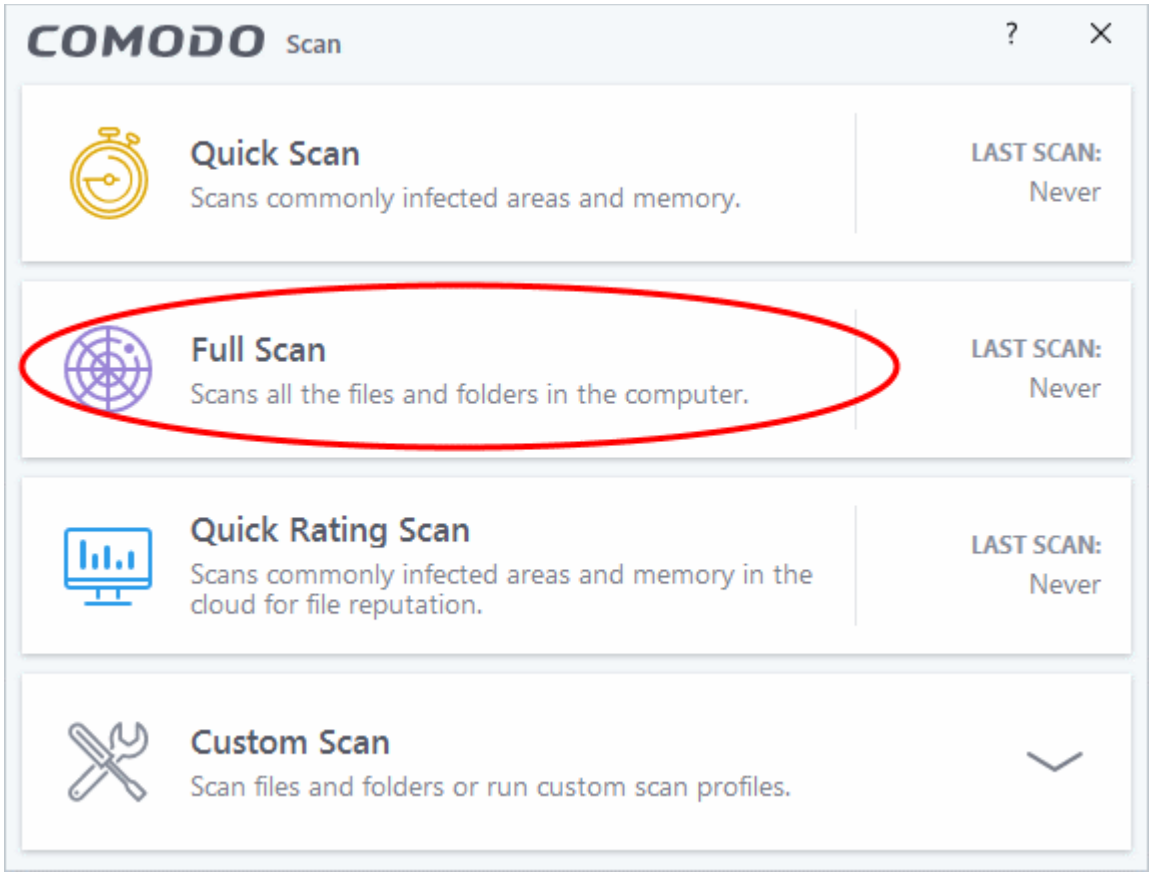
2.1.2. Run a Full Computer Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Full Scan'
- A full scan checks every file, folder and drive on your computer. USB and other external drives are also scanned.
  - Note - You can change the settings of a quick scan in 'Settings' > 'Antivirus' > 'Scans'. See **Antivirus Configuration** > **Scan Profiles** for help with this.

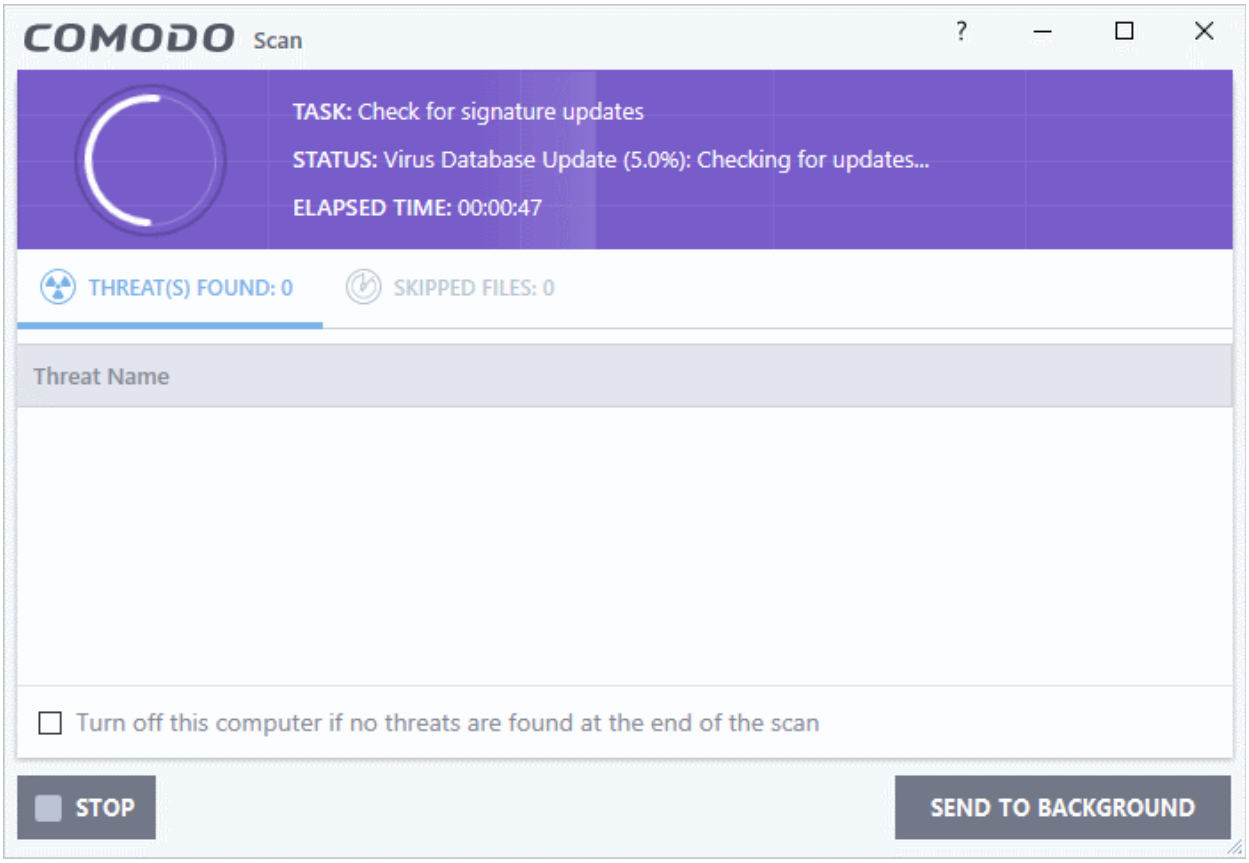
Run a Full Computer Scan

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

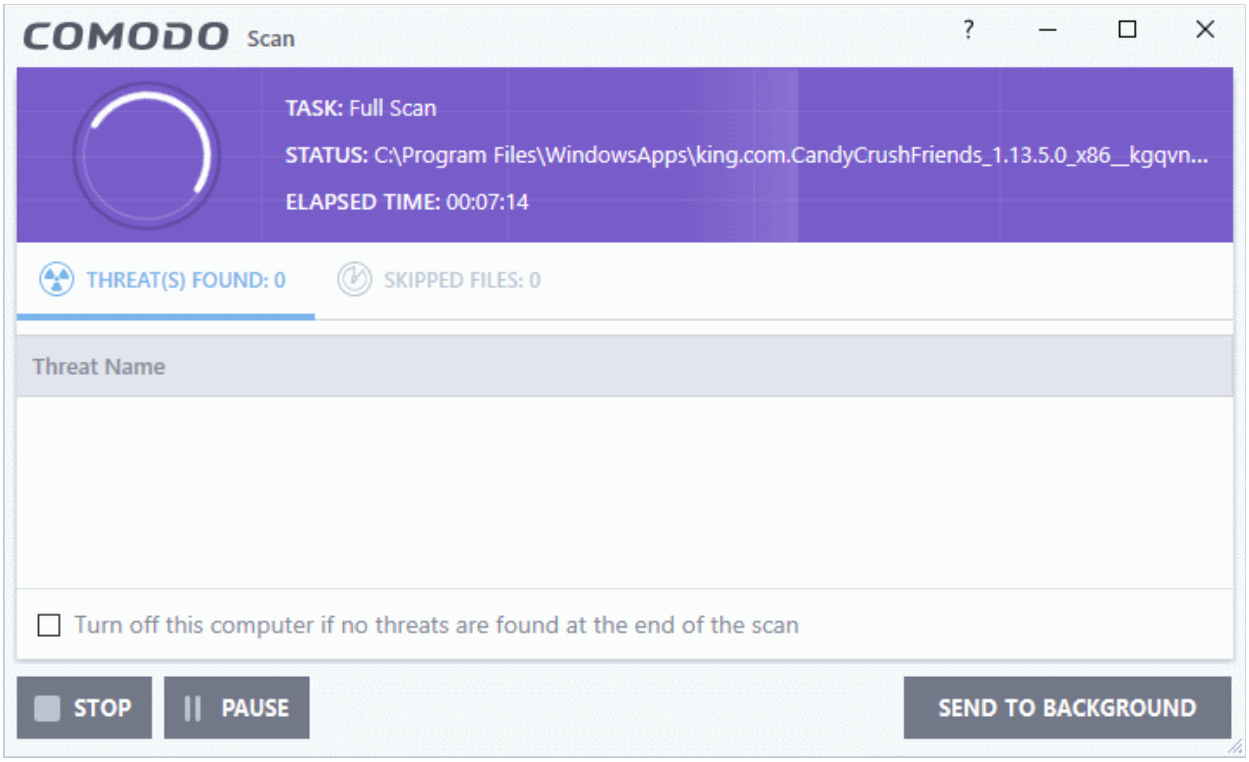
- Select 'Full Scan':



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

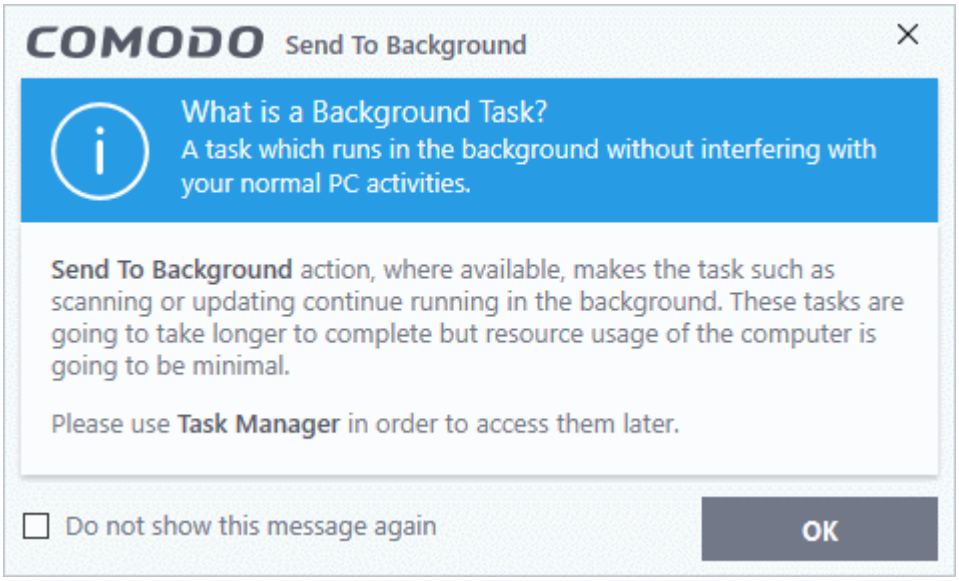


- The scans starts after any updates have been installed:

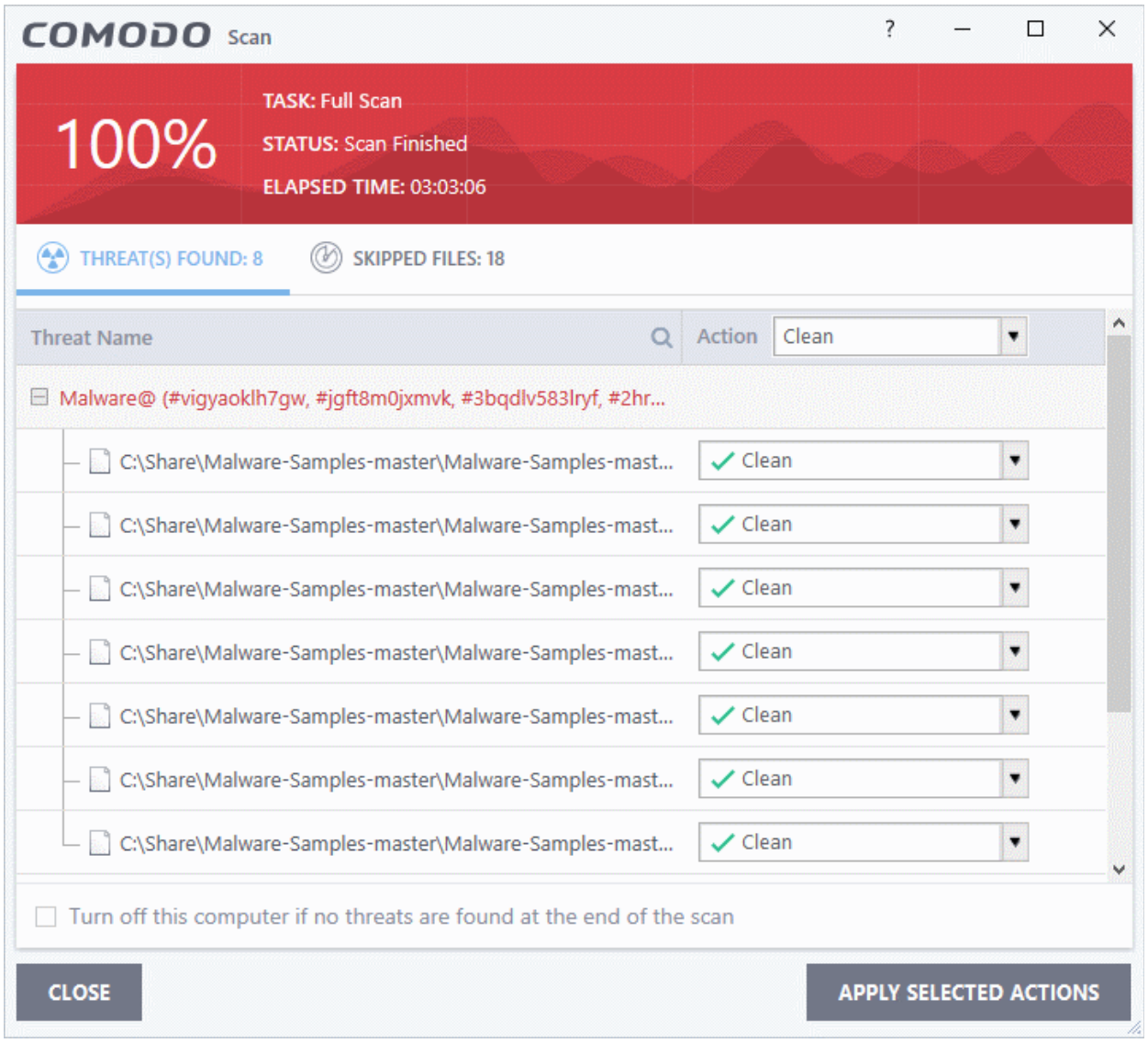


Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

- You can pause, resume or stop the scan by clicking the appropriate button.
- Send to Background - Runs the scan as a background process which consumes fewer resources. You can still keep track of the scan in the task manager - 'Tasks' > 'Advanced Tasks' > 'Open Task Manager'.



  - You can keep still track of scan progress in 'Tasks' > 'Advanced Tasks' > '**Open Task Manager**'.
- Scan results are shown when the scan finishes:

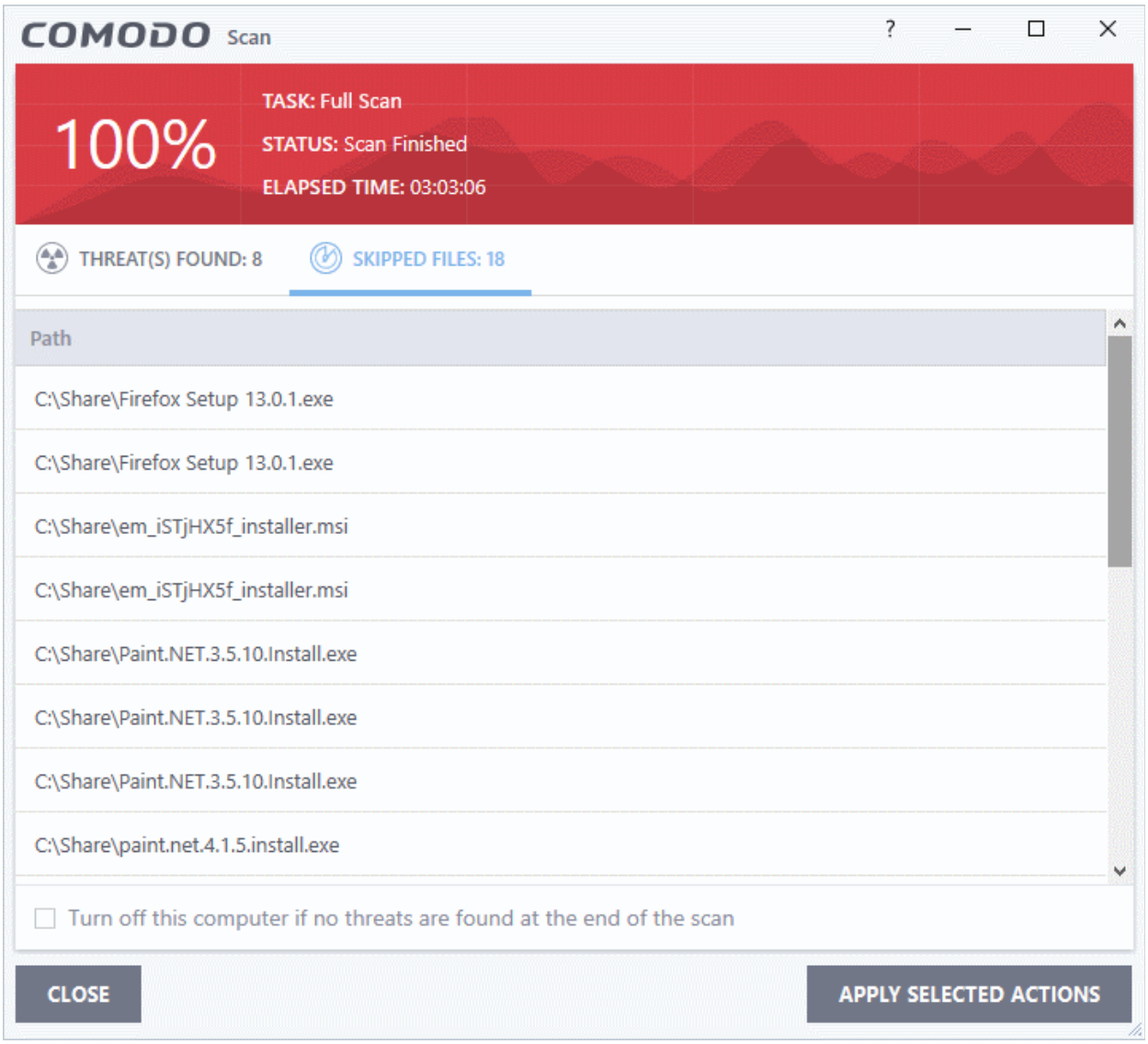


The results window contains two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.

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

- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

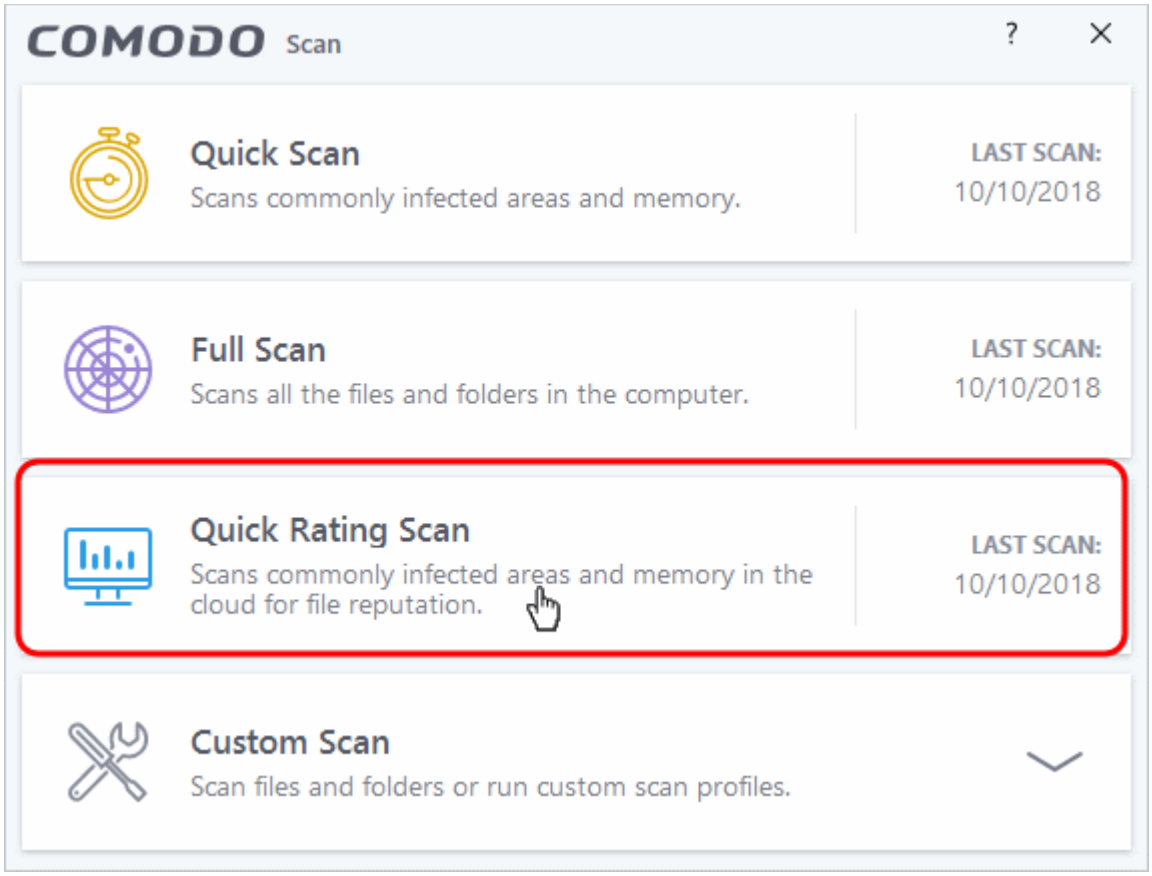


2.1.3. Run a Rating Scan

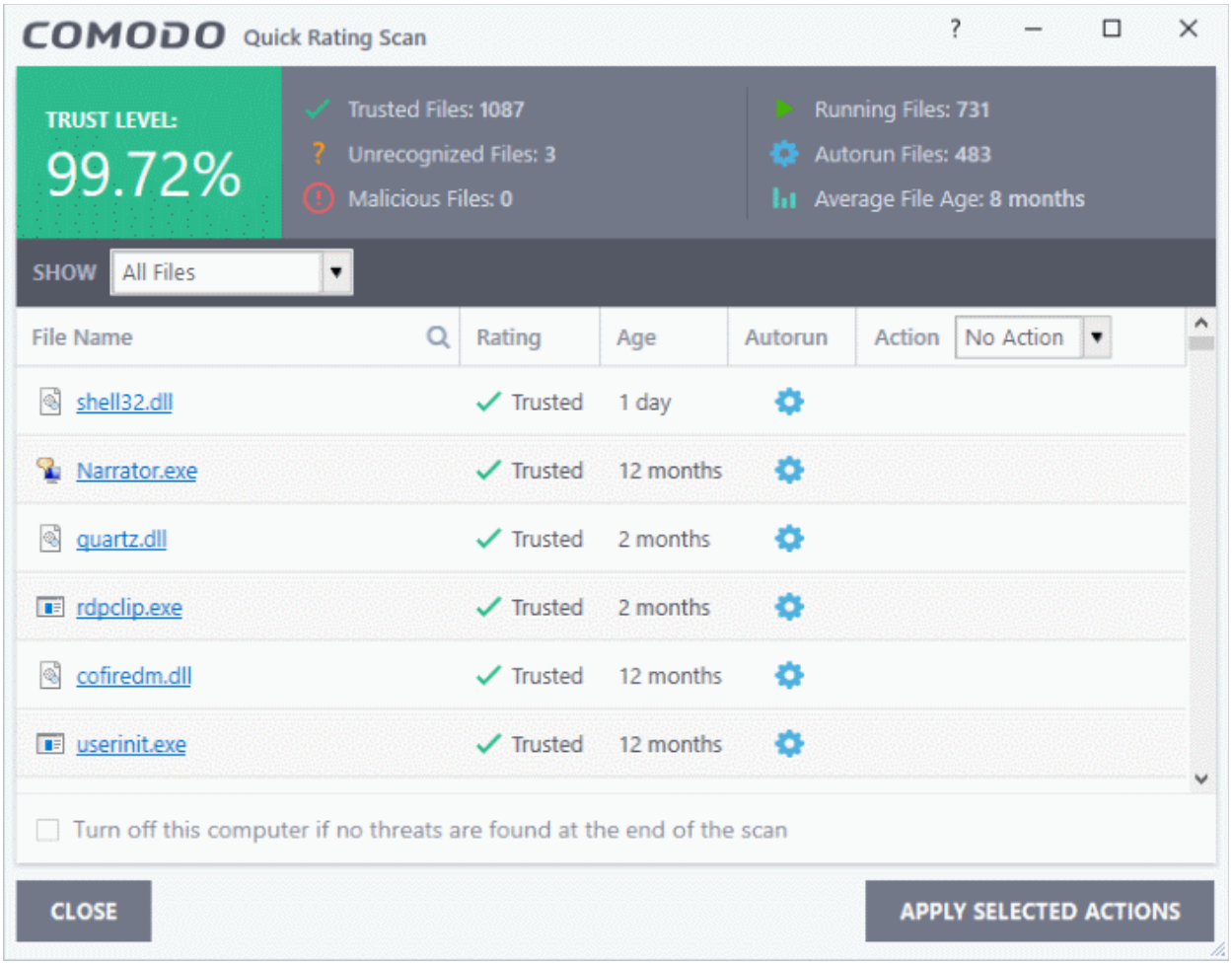
- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Rating Scan'
- A rating scan checks the trust-rating of files on your computer.
- Trust ratings are as follows:
  - **Trusted** - The file is safe to run.
  - **Malicious** - The file is malware. Depending on your settings, CCS will either quarantine the file immediately or present you with disinfection options.
  - **Unrecognized** - Comodo does not currently have a trust rating for the file. Unrecognized files should be run in the container to prevent them potentially attacking your computer. You can simultaneously submit them to Comodo for a trust-rating analysis.

Run a Rating scan

- Click the 'Scan' tile on the CCS home screen (**click here** for alternative ways to open the scan interface)
- Select 'Ratings Scan':

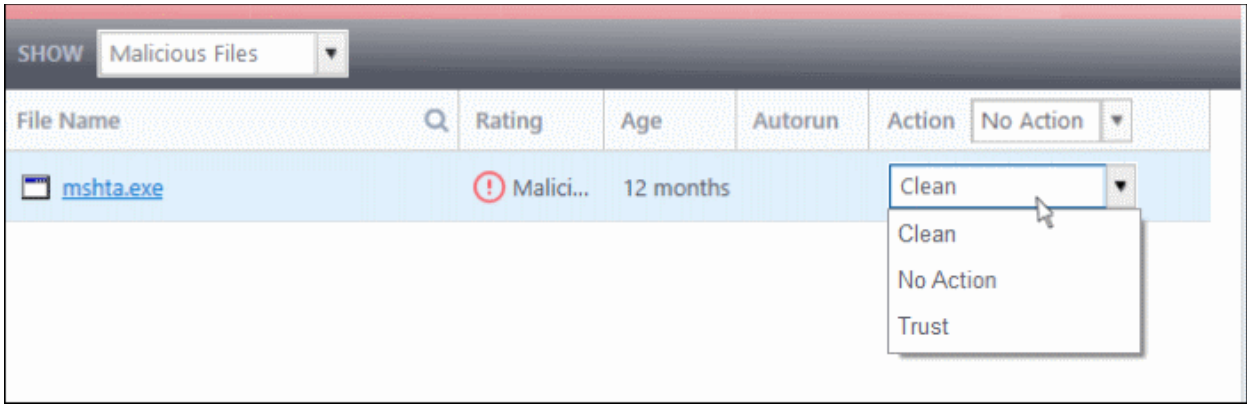


CCS will analyze all files on your computer and assign them a trust rating. File ratings are shown in the results table at the end of the scan:



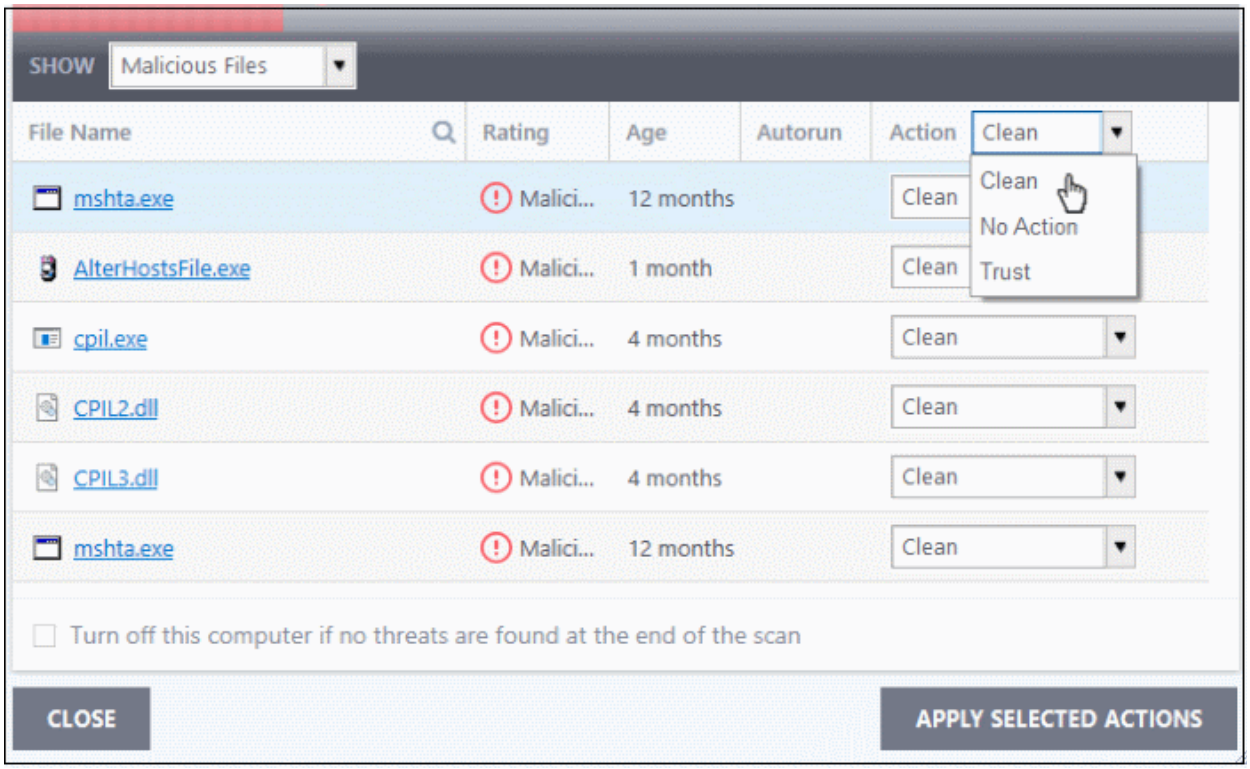
Rating Scan Results Table - Column Descriptions	
Column Header	**Description**
File Name	The label of the scanned item
Rating	The trust level of the file as per the cloud based analysis. The possible values are: • Trusted • Unrecognized • Malicious
Age	The length of time the item has been on your computer
Auto-run	Whether or not the file automatically runs without user intervention.
Action	Select how you want to deal with the listed item. See the explanations given below:

The drop-down menus on the right let you handle unrecognized and malicious items:



- **Clean** - Available only for malicious items. The threat is placed in quarantine for your review. Click 'Tasks' > 'General Tasks' > 'View Quarantine' to open this area. You can restore or permanently delete files from quarantine as required. See **Manage Quarantined Items** for more details.
- **No Action** - Ignores the warning this time only. The file not placed in quarantine. Use this option with caution. The file will be caught again by the next rating scan you run.
- **Trust** - The file is awarded trusted status in the **File List** ('Settings' > 'File Rating' > 'File List'). The file will be excluded from any future rating scans. Only select this option if you are sure the item is trustworthy.

- CCS logs all actions taken in the results screen. You can view the logs at 'Tasks' > 'Advanced Tasks' > 'View Logs'. See **File List Changes Logs** for more details.
- Use the drop-down in the 'Action' column header to apply your choice to all listed files:

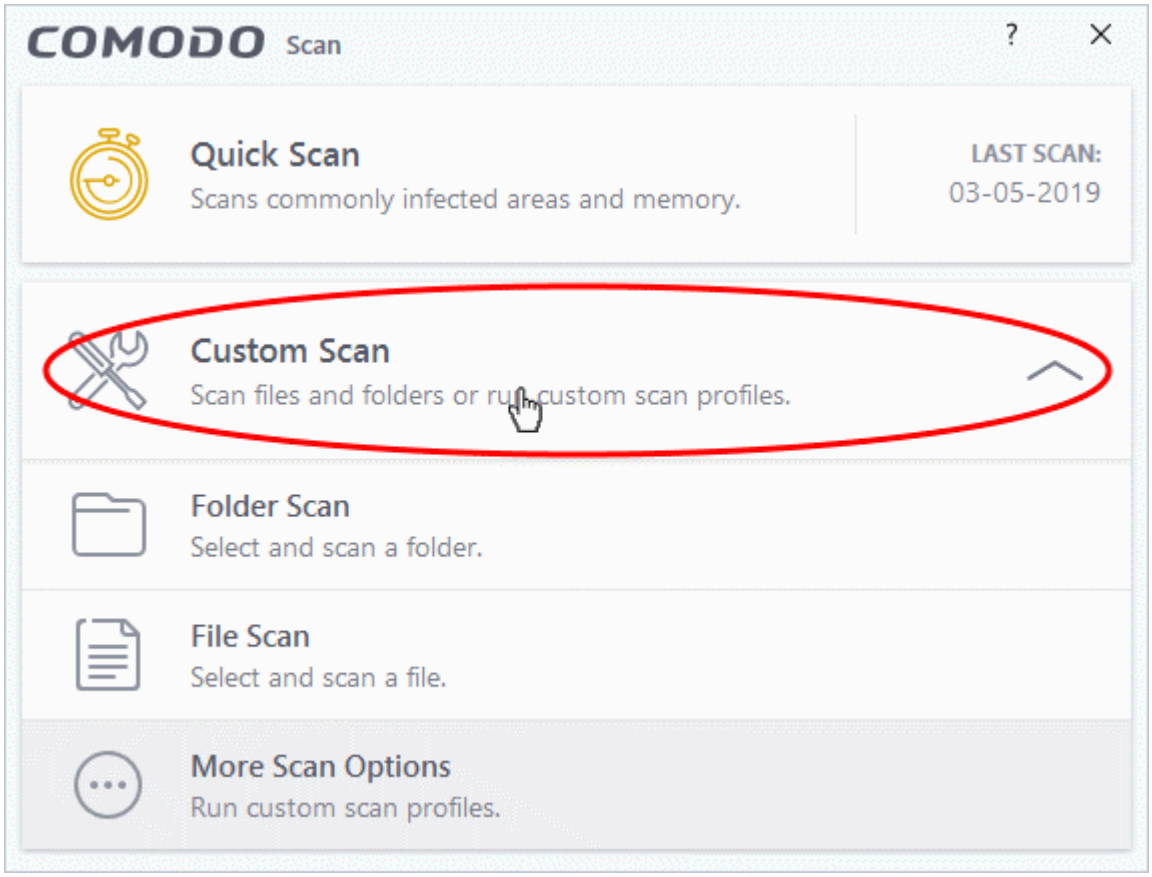


2.1.4. Run a Custom Scan

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan'
- A custom scan lets you check specific files, folders, drives and areas on your computer.

Run a custom scan

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



You now have the following options:

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

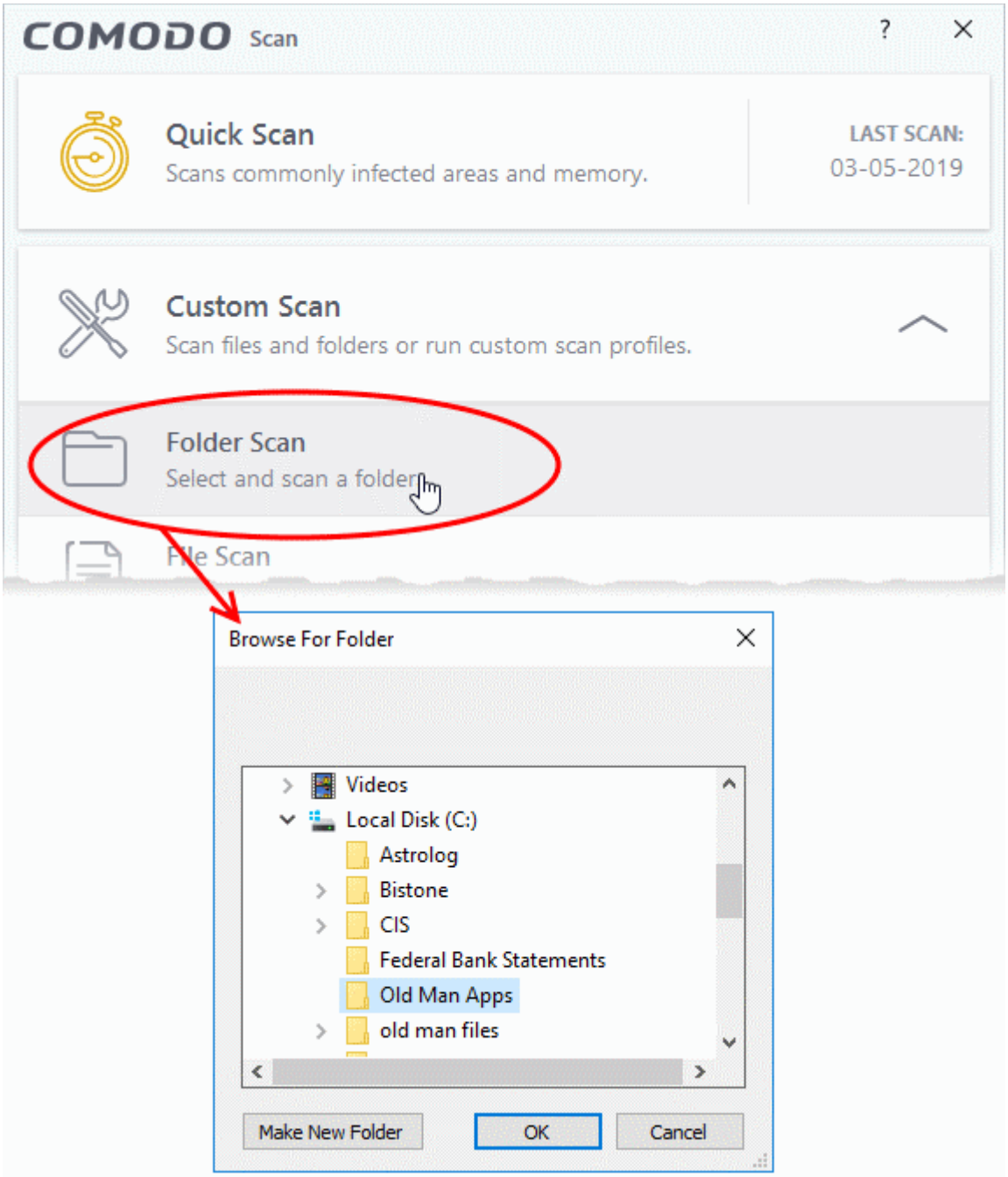
2.1.4.1. Scan a Folder

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'Folder Scan'
- Folder scans let you check specific folders on your hard drive, CD/DVD, or external device.

Tip: Alternatively, simply right-click on a folder then select 'Scan with COMODO Antivirus'.

Scan a specific folder

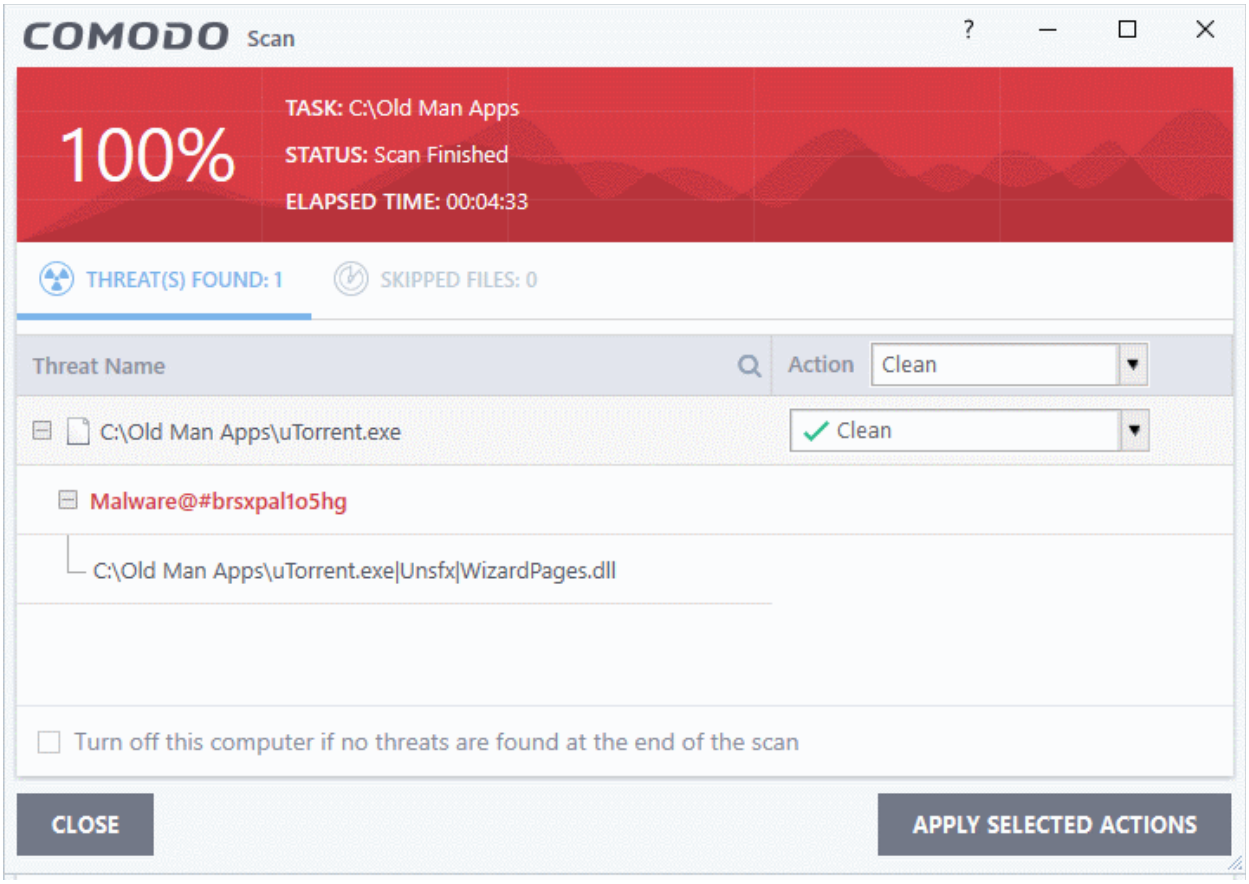
- Click the 'Scan' tile on the CCS home screen
- Select 'Custom Scan' > 'Folder Scan'
- Browse to the folder you want to check then click 'OK':



- The CCS starts scanning the items in the folder.

Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

- Scan results are shown when the scan finishes:



The results window has two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

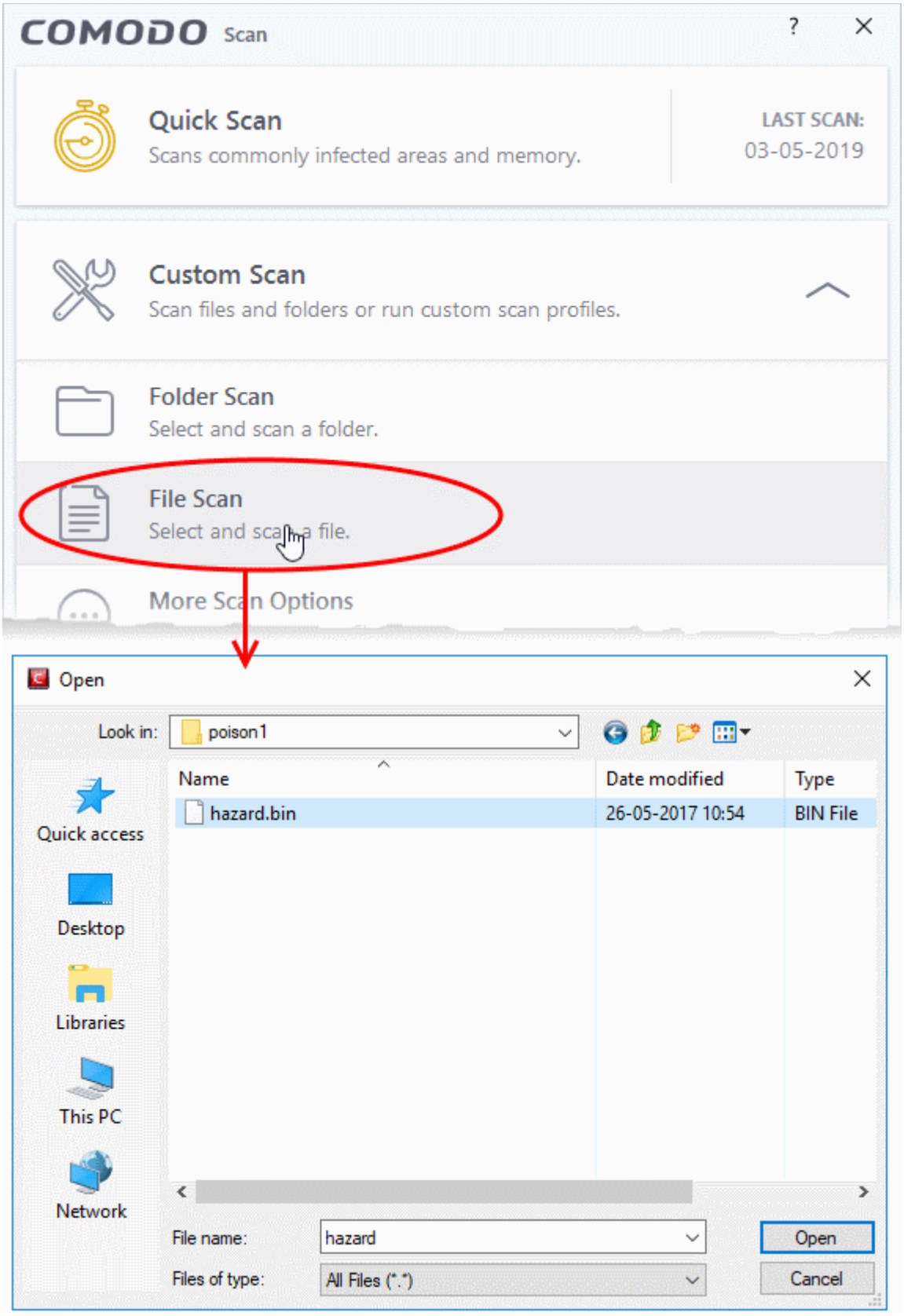
2.1.4.2. Scan a File

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'File Scan'
- File scans let you check specific files on your hard drive, CD/DVD, or external device.
- For example, you might have downloaded a file from the internet which you want to scan before running.

Tip: Alternatively, right-click on file then select 'Scan with COMODO Antivirus'.

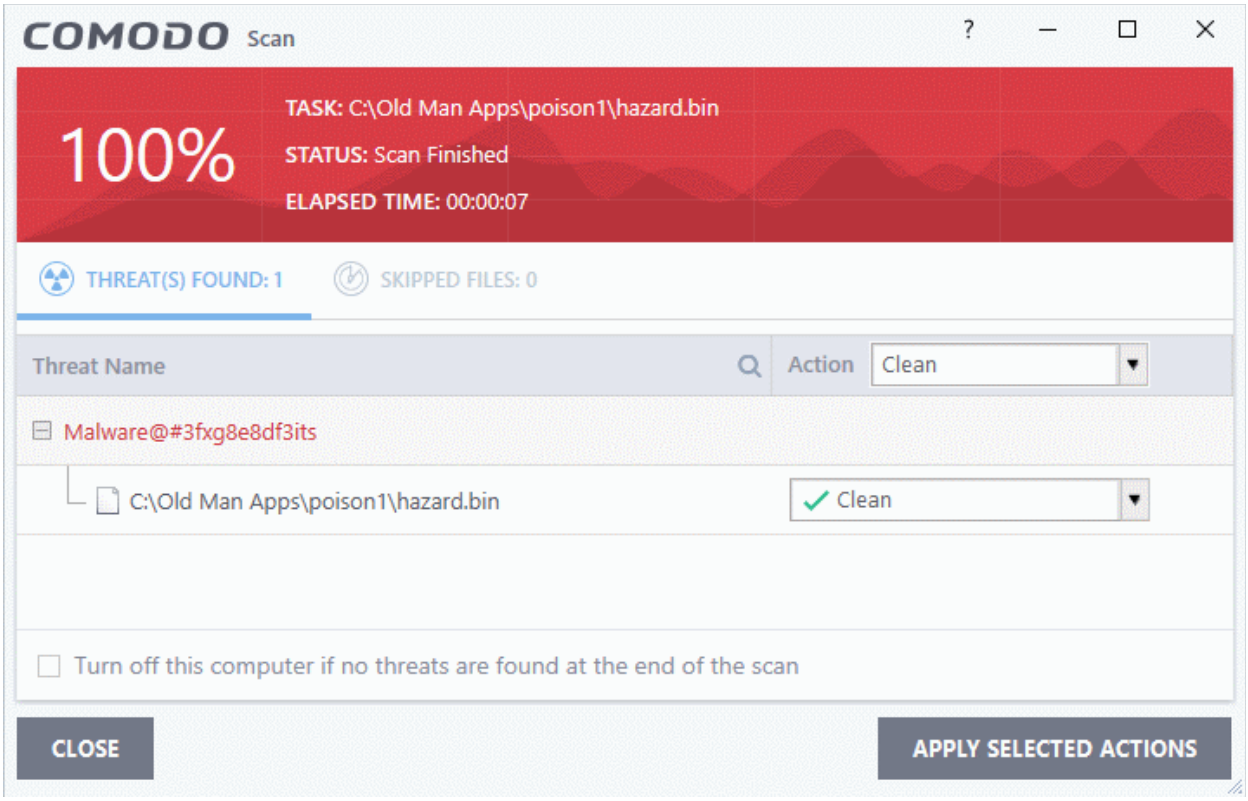
Scan a specific file

- Click the 'Scan' tile on the CCS home screen
- Select 'Custom Scan' > 'File Scan'
- Browse to the file you want to scan and click 'Open'.



Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed in 'Full Scan' profile. Click 'Settings' > 'Antivirus' > 'Scans' to view these thresholds.

- Scan results are shown when the scan finishes:



The results window has two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

2.1.4.3. Create, Schedule and Run a Custom Scan

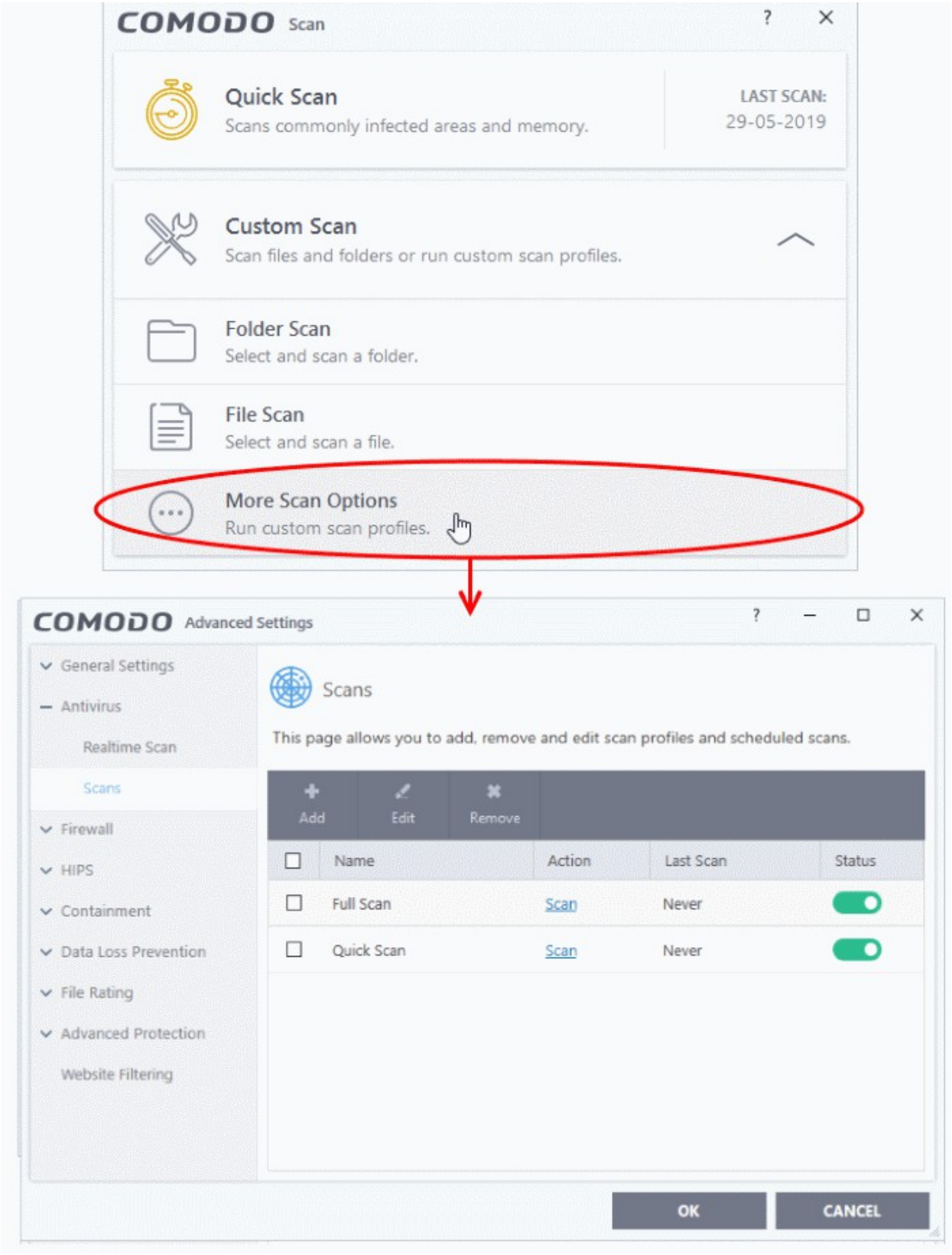
Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'More Scan Options'

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

Create a custom profile

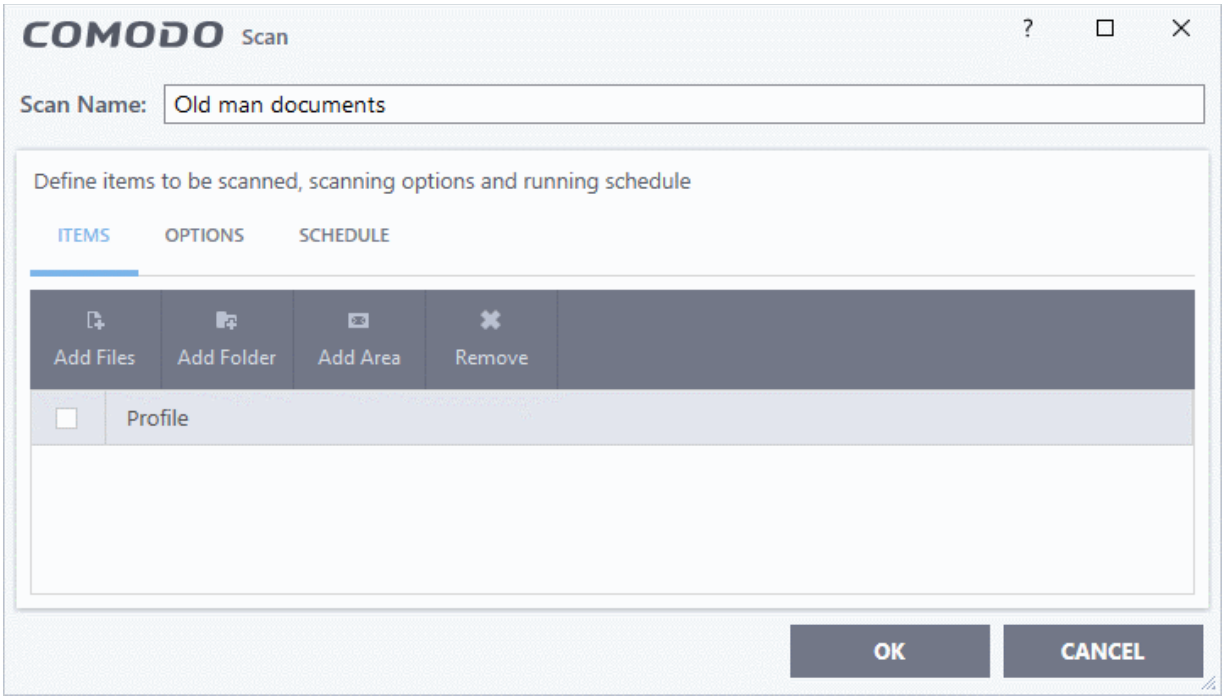
- Click the 'Scan' tile on the CCS home screen
- Select 'Custom Scan' then 'More Scan Options'

The scans page shows pre-defined and user created scan profiles. You can create and manage new profiles in this page:



Tip: You can also get to this screen by clicking 'Settings' > 'Antivirus' > 'Scans'.

- Click 'Add' to create a new custom scan profile.



First, create a name for the profile. The next steps are:

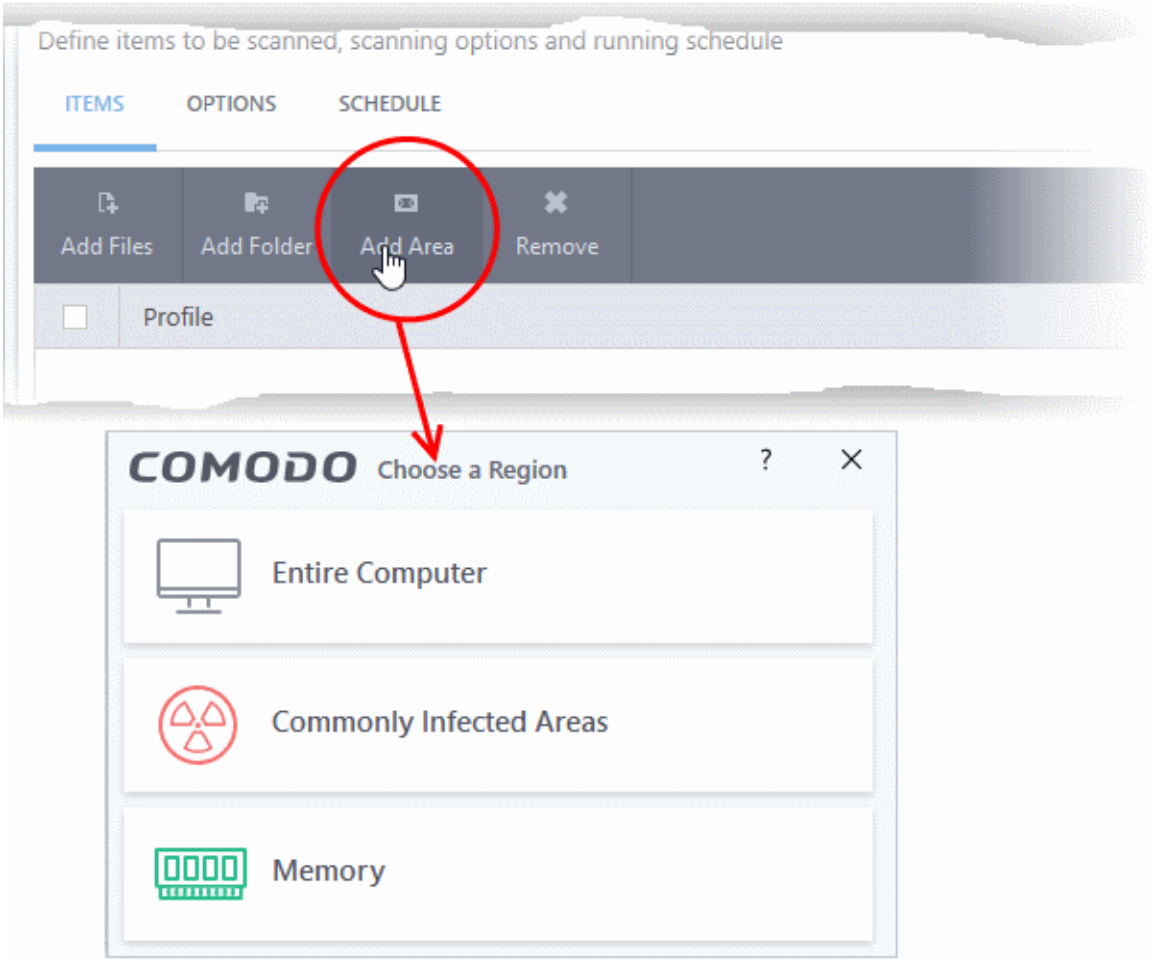
- **Select items to scan**
- **Configure scan options for the profile (optional)**
- **Configure a scan schedule (optional)**

Select items to scan

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

You can add items as follows:

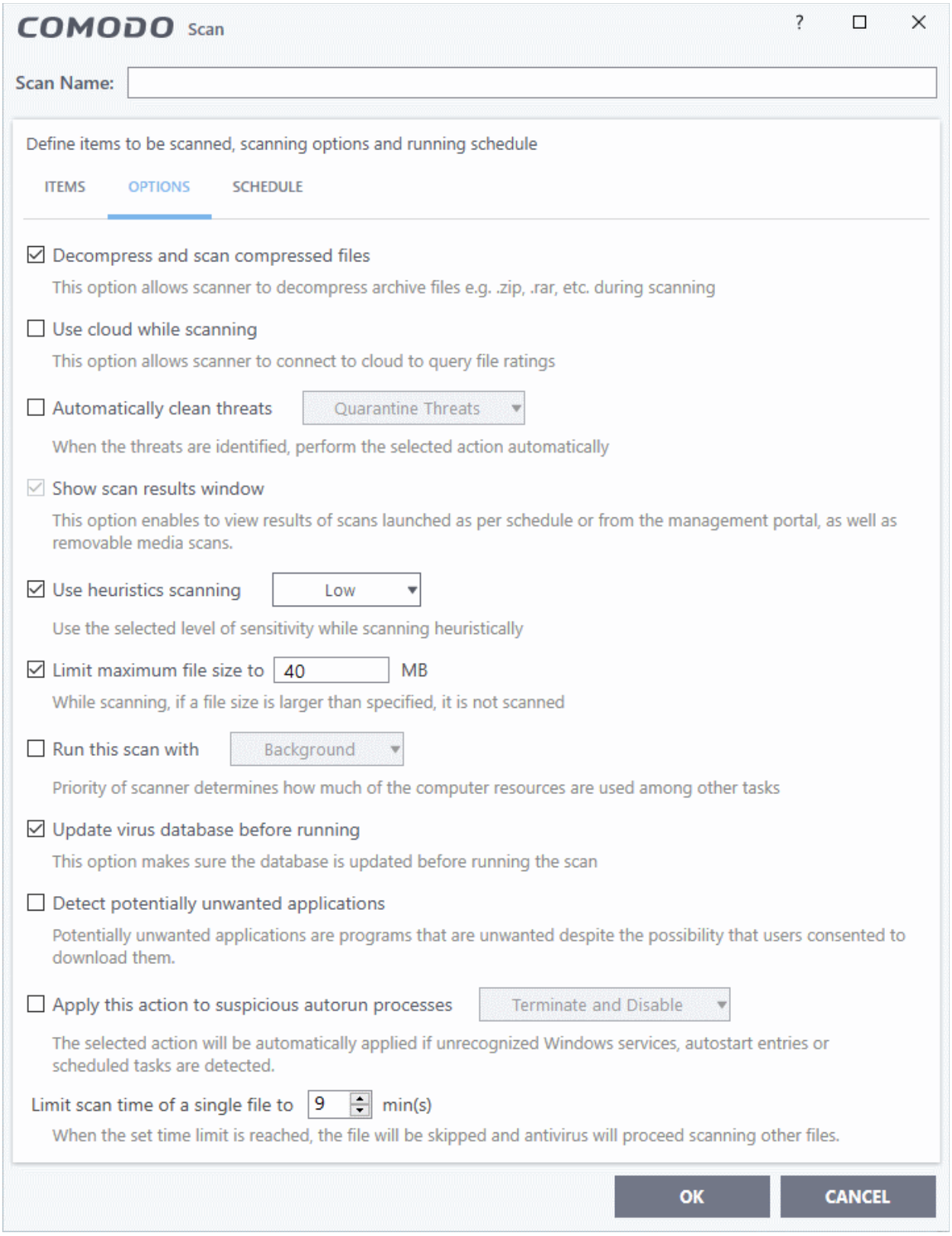
- **Add File** - Pick individual files that you want to scan.
- **Add Folder** - Add entire folders to the profile. All files in the folder are covered by the scan.
- **Add Area** - Scan a computer region. The choices are 'Full Computer', 'Commonly Infected Areas' and 'System Memory'. See screenshot below:



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

Configure Scan Options

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



Decompress and scan compressed files - The scan will include archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (***Default = Enabled***).

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

Automatically clean threats - Select whether or not CCS should automatically remove any malware found by the scan. (***Default = Enabled***).

- **Disabled** = Results are shown at the end of the scan with a list of any identified threats. You can manually deal with each threat in the results screen. See **Process Infected Files** for guidance on manually handling detected threats.
- **Enabled** = Threats are handled automatically. Choose the action that CCS should automatically take:
  - **Quarantine Threats** - Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See '**Manage Quarantined Items**' for more details.
  - **Disinfect Threats** - If a disinfection routine exists, CCS will remove the virus and keep the original file. If not, the file will be quarantined. (***Default***)

Show scan results window - You will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.

Use heuristic scanning - Select whether or not heuristic techniques should be used in scans on this profile. You can also set the heuristic sensitivity level. (***Default = Enabled***).

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

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

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

  Despite the name, this setting combines a very high level of protection with a low rate of false positives. We recommend this setting for most users. (Default)
- **Medium** - Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.

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

Run this scan with - If enabled, you can set the priority of scans on this profile The available options are:

- High
- Normal
- Low
- Background

If you disable this option then the scan runs in the background (***Default***)

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

Detect potentially unwanted applications - The antivirus also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional utility when installing another piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks your activity on the internet. ***(Default = Enabled)***.

Apply this action to suspicious autorun processes - Specify how CCS should handle unrecognized auto-run items, Windows services, and scheduled tasks.

- **Ignore** - The item is allowed to run (***Default***)
- **Terminate** - CCS stops the process / service
- **Terminate and Disable** - Auto-run processes are stopped and the corresponding auto-run entry removed.

In the case of a service, CCS disables the service.

- **Quarantine and Disable** - Auto-run processes are quarantined and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.

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

- See **Miscellaneous Settings** for more details

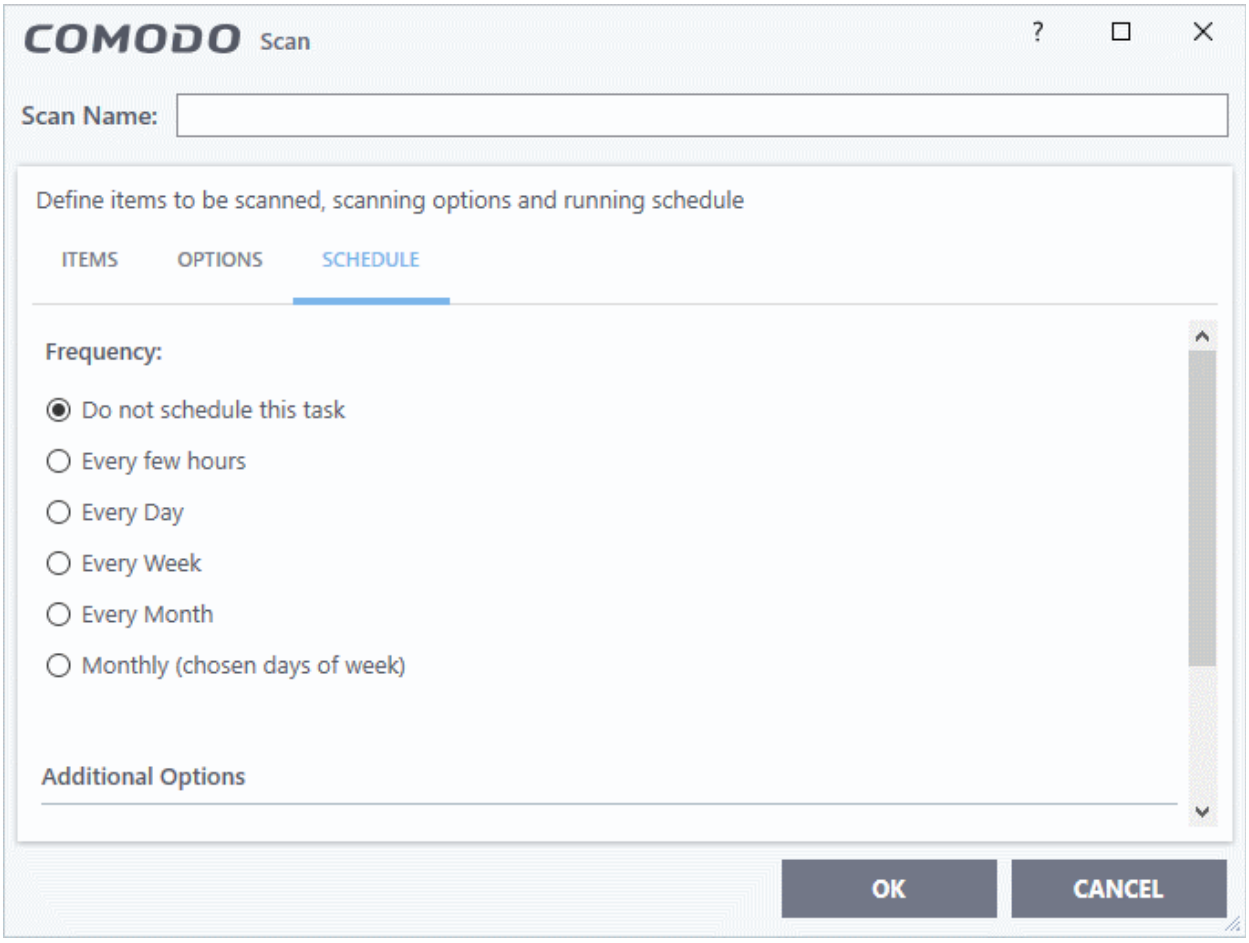
Note 2 - CCS runs script analysis on certain applications to protect their registry records. You can manage these applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

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

Limit scan time of a single file to - Set the maximum time allowed to scan an individual file. CCS will skip files that take longer to scan than the specified time. Omitted files are shown in the 'Skipped Files' tab in the results screen.

Schedule the scan

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



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

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

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

Every Week - Run the scan on the days specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.

Every Month - Run the scan on the dates specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.

Monthly (chosen days of the week) - Run the scan on a specific week, or weeks, in a month. Select the weeks in from the menus.

Additional Options

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

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

- Click 'OK' to save the profile.

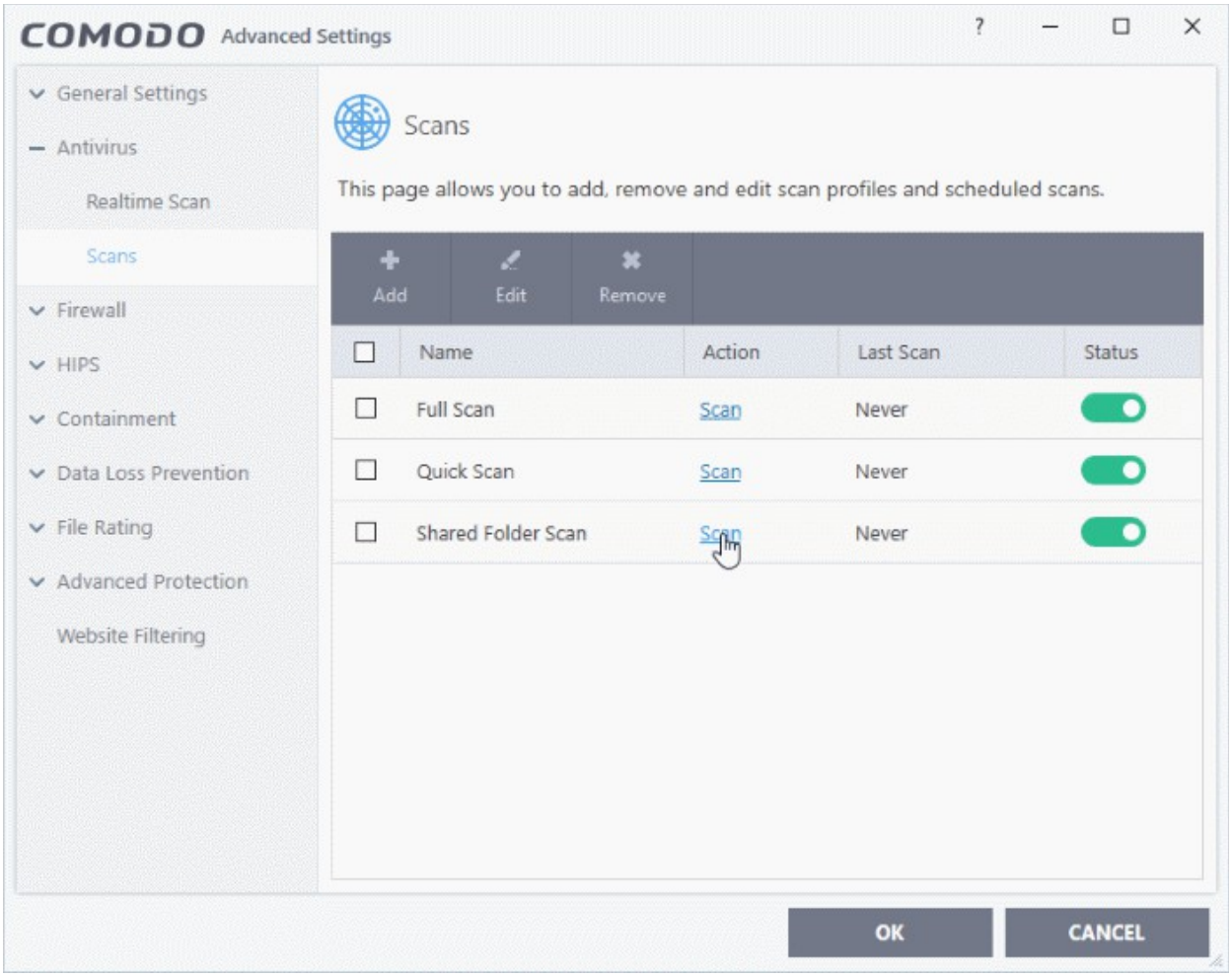
The profile will be available for deployment in future.

Run a custom scan

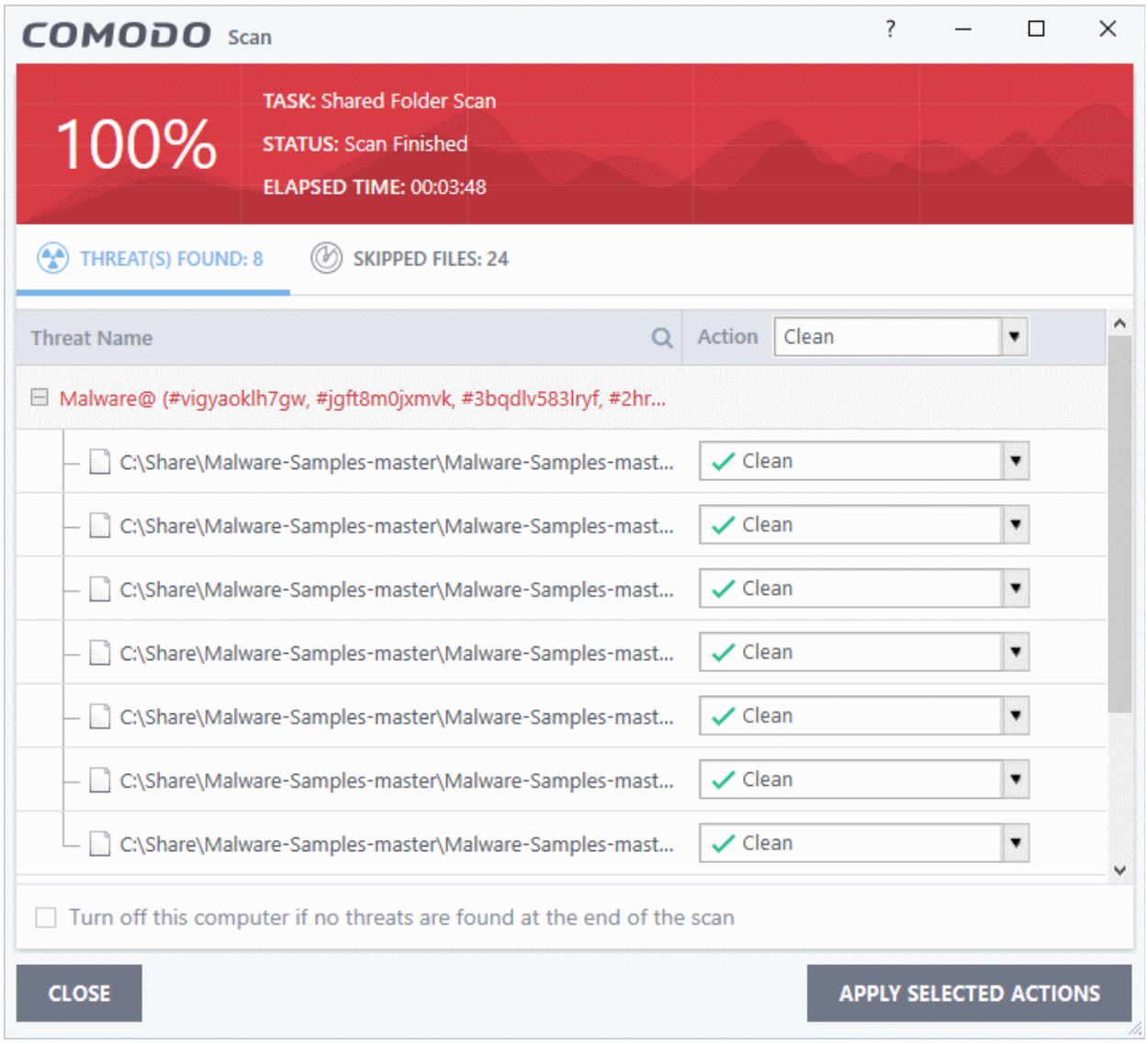
- Click 'Tasks' > 'General Tasks' > 'Scan'
- Click 'Custom Scan' from the 'Scans' interface
- Click 'More Scan Options' from the 'Custom Scan' pane

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

- Click 'Scan' beside the required scan profile.



The scan will start immediately. Results are displayed afterwards:

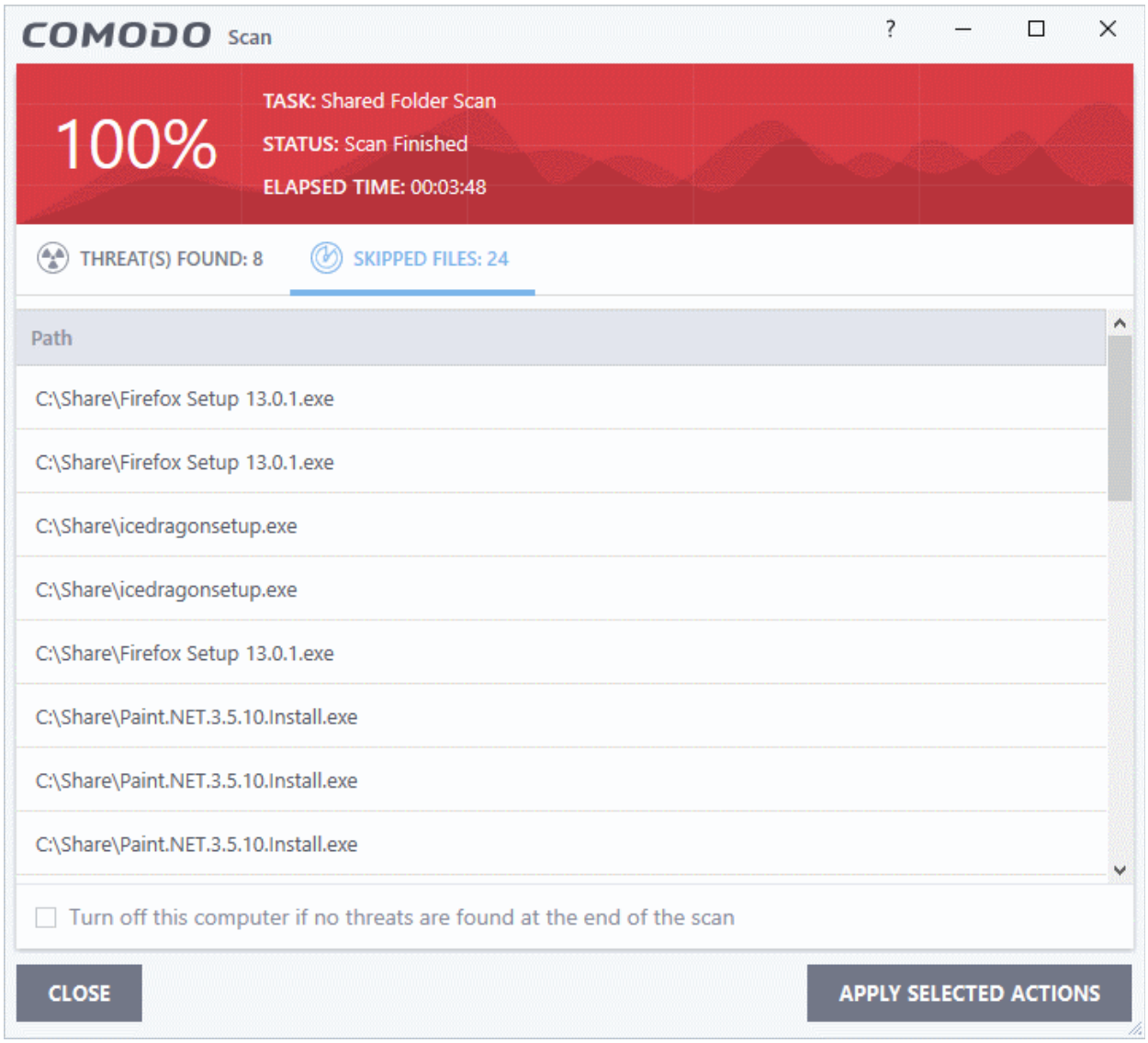


The results window contains two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.

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

- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (***default = 9 mins***).



2.1.5. Automatically Scan Unrecognized and Quarantined Files

- Click 'Settings' > 'File Rating' > 'File Rating Settings'
- CCS can periodically re-scan unknown and quarantined files to check whether a new trust rating is available for them.
- This area lets you specify a schedule and settings for these scans.

File Rating

- CCS checks files whenever they are opened and rates them as 'trusted', 'malicious' or 'unrecognized'.
- The rating is obtained by checking the file's reputation on our master whitelist and blacklist.
- If no rating is available then CCS checks the trust rating of the software vendor
  - CCS will apply the vendor's reputation to the file if one exists. CCS first checks the vendor's local reputation in the 'Vendor List'. If no local rating is available then it checks the file lookup service.

There are two ways a file can get an 'unrecognized' rating:

1. Because there is no rating for the file on Comodo's black or whitelists, and no user has assigned a malicious/trusted rating to the file.

   OR

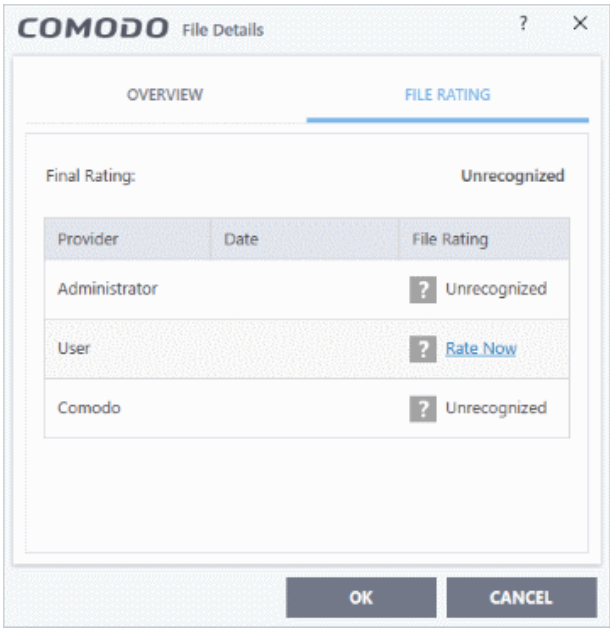
2. Because an admin, user or Comodo specifically assigned an 'unrecognized' rating to the file.

To view the rating:

- Go to 'Settings' > 'File Rating' > 'File List' > select an unrecognized file > Click 'File Details'
- Click the 'File Rating' tab

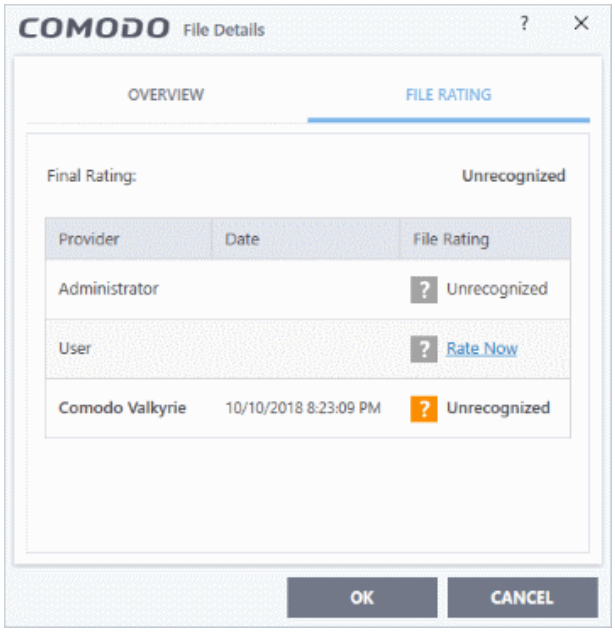
The following examples show files with and without ratings:

- The interface lists 3 ratings, one each from the user (you), the admin and Comodo.
- Unknown files with no rating are shown with a gray ? Icon.



- You can assign a local rating by clicking 'Rate Now'

- A colored icon in the file rating column indicates it has been rated.
  - Yellow - Unrecognized
  - Green - Trusted
  - Red - Malicious



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

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

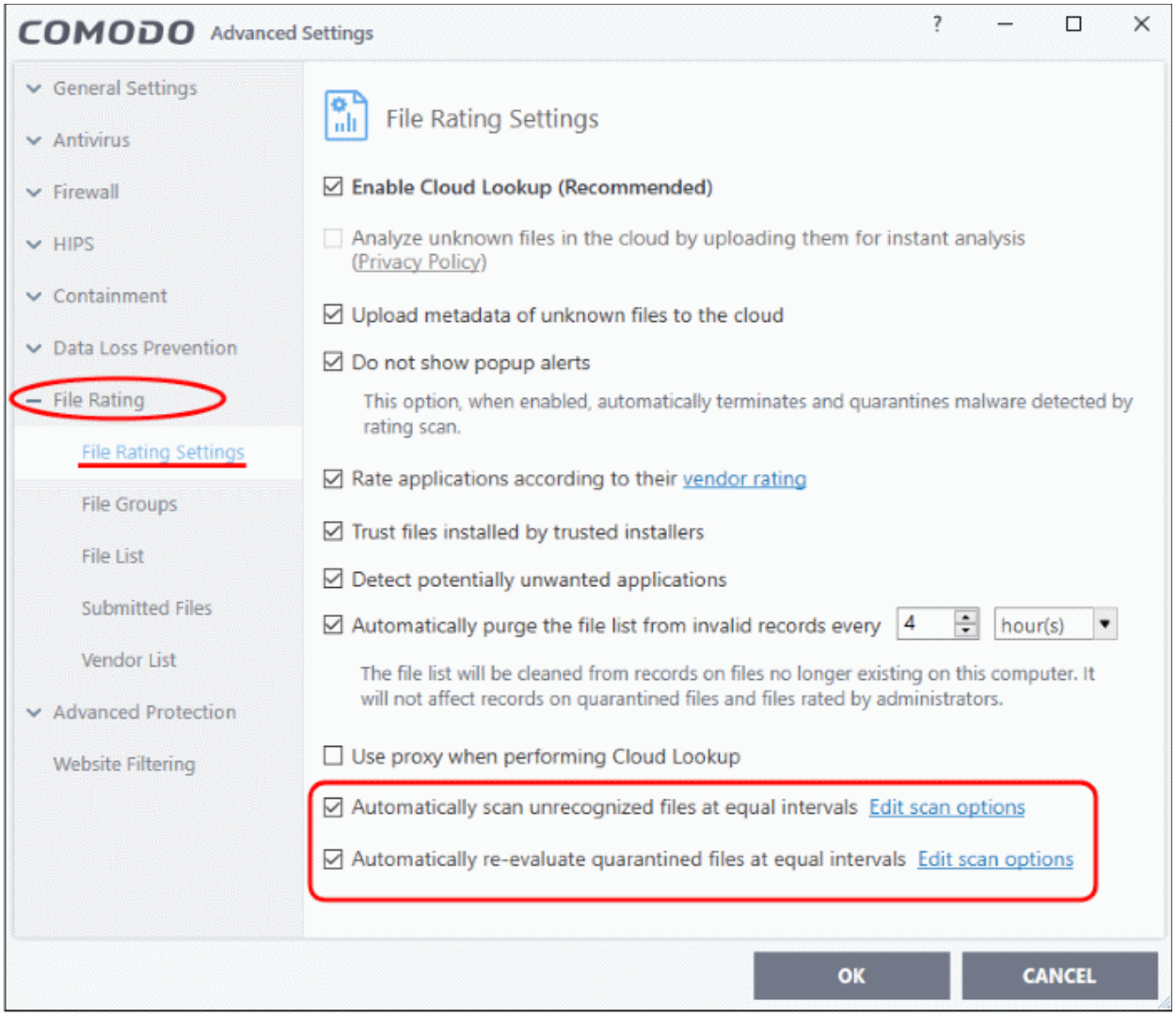
Regardless of the above, all unrecognized files are run in the container by default. If required, you can change auto-containment rules in 'Settings' > 'Containment' > 'Auto-Containment'. See '**Auto-Containment Rules**' for more information.

Quarantined Files

- The antivirus scanner moves threats to quarantine to prevent them from infecting your system.
- All files in quarantine are encrypted, so they cannot run or cause harm.
- You can also manually move suspicious items to quarantine. See **Manage Quarantined Items** for more details.

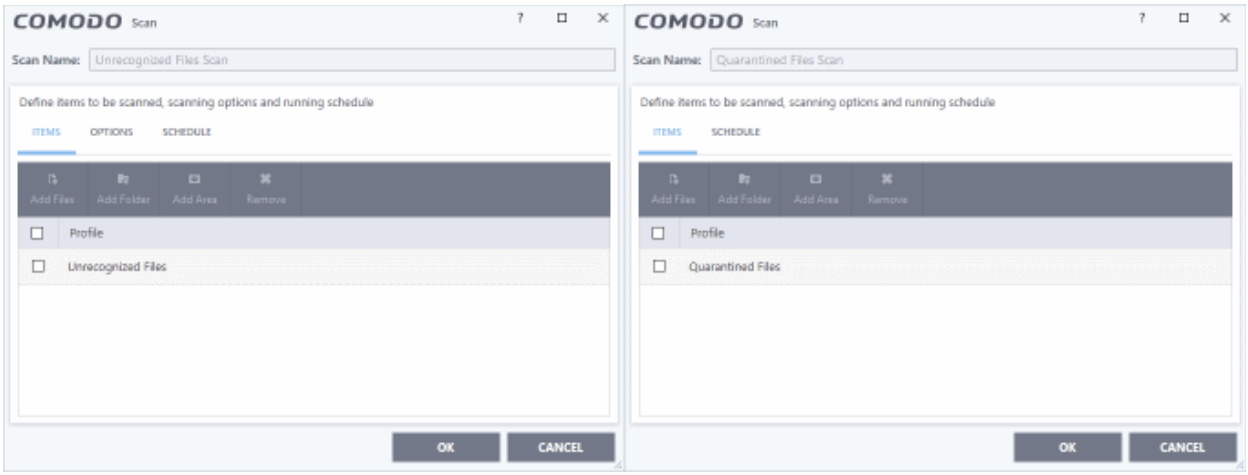
Configure scan settings for unrecognized and quarantined files

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



- **Automatically scan unrecognized files at equal intervals** - CCS will check Comodo's master database to see if a new trust rating is available for unrecognized files. (***Default = Enabled and set for every 4 hours***)
- **Automatically re-evaluate quarantined files at equal intervals** - CCS will check Comodo's master database to see if a new trust rating is available for quarantined files. (***Default = Enabled and set for once everyday***)
- Click 'Edit scan options' to open the unrecognized / quarantined scan profile:

Unrecognized Files Scan | **Quarantined Files Scan**



- **Scan Name** - The label of the scan. This is pre-configured and cannot be edited.
- **Items** - The files that are scanned by the profile. 'Unrecognized' and 'Quarantined' files are the defaults. You cannot edit or add files to this profile.
- **Scan Options** - (unrecognized files scan only) Configure scan technologies, how to handle threats, and more. See **Configure scan options for the profile** in the previous section for help with this.
- **Schedule** - Specify the frequency of the scans. See **Configure a scan schedule** in the previous section if you need help with this. (*Default = Every 4 hours for unrecognized files scan and once in a day for quarantined files scan*).

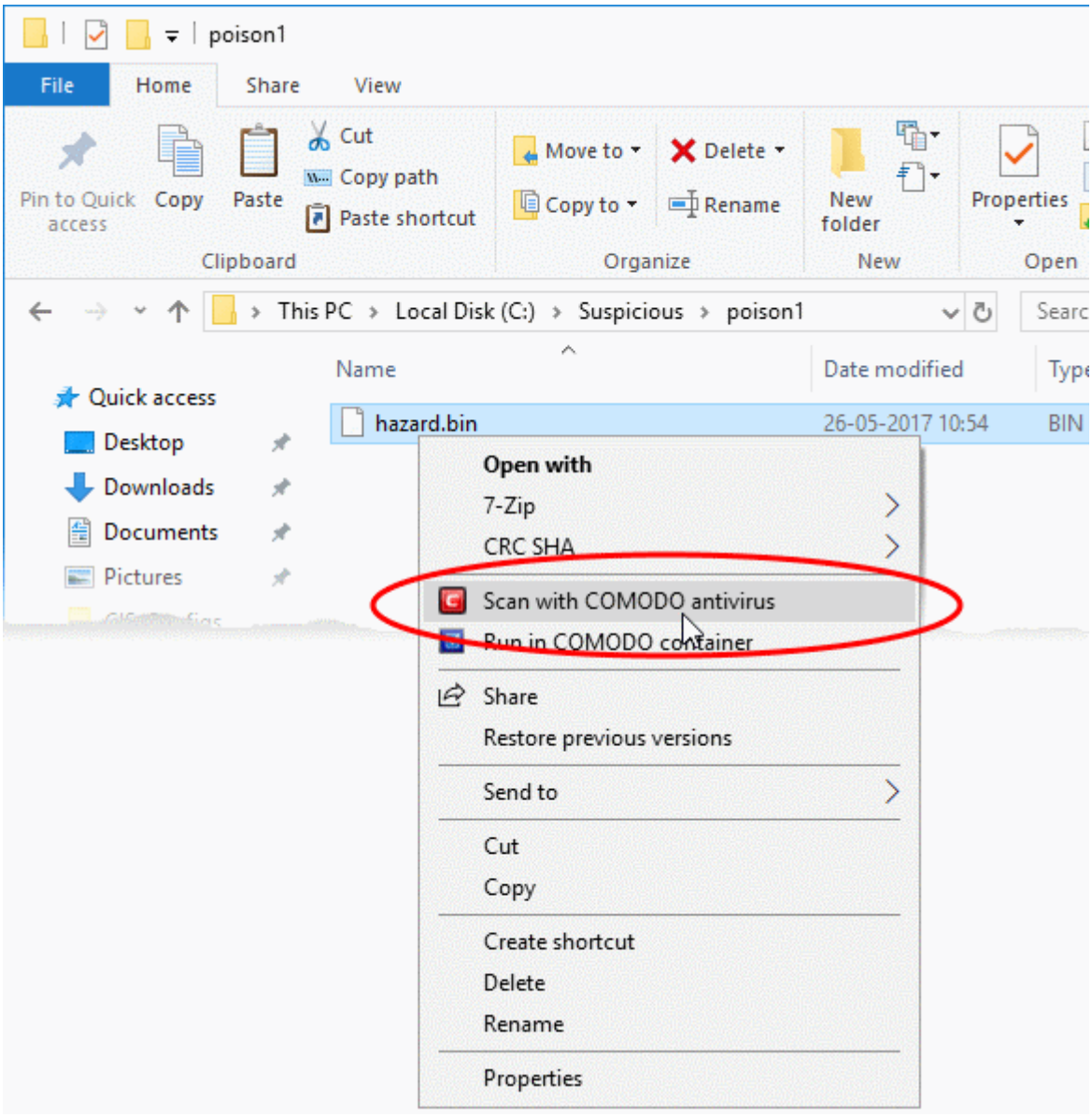
- Click 'OK' to save your changes
- Click 'OK' in the 'Advanced Settings' screen for your settings to take effect.

2.2. Instantly Scan Files and Folders

- You can scan individual files, folders or drives to instantly to check whether they contain threats.
- For example, this is useful if you are wary about an item you have copied from an external source or downloaded from the internet.

Instantly scan an item

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

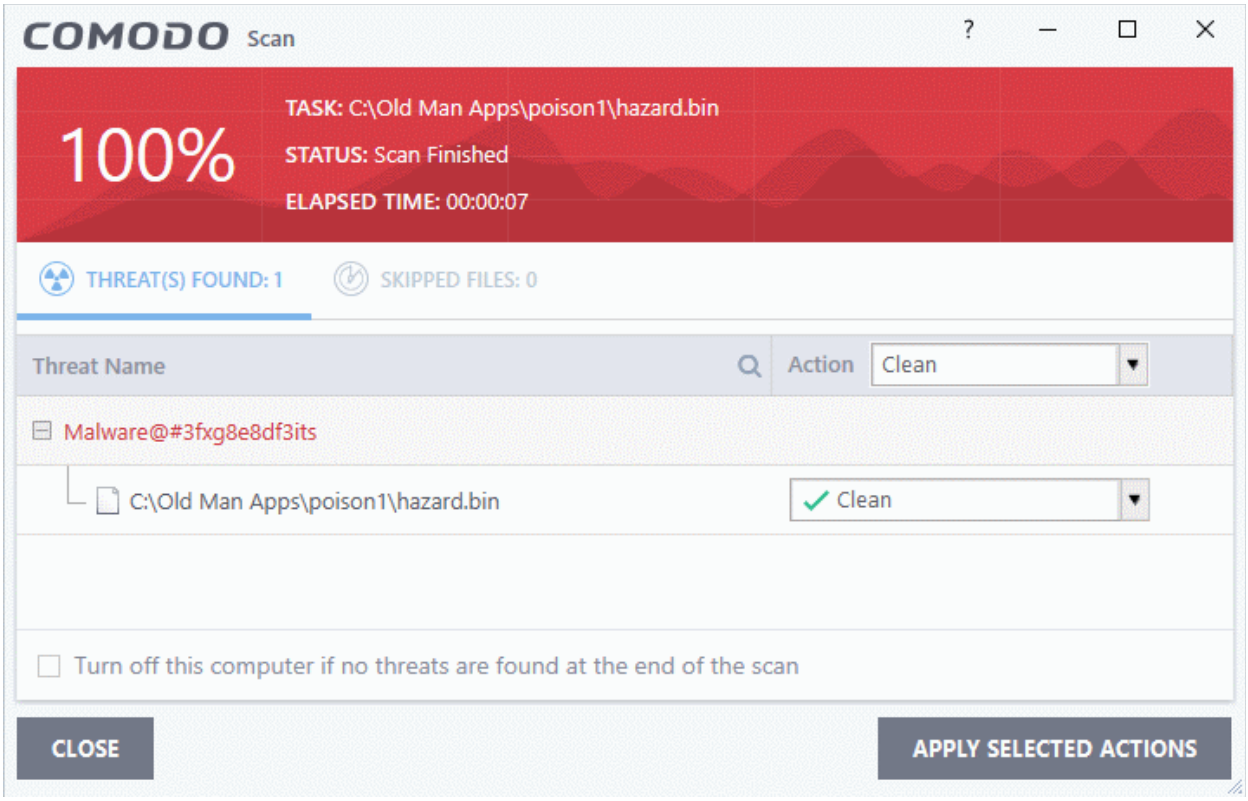


The item will be scanned immediately.

Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed.

Click 'Settings' > 'Antivirus' > 'Scans', then open the 'Full Scan' profile to view these thresholds.

- Scan results are shown when the scan finishes:



The results window has two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.
- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (***default = 9 mins***).

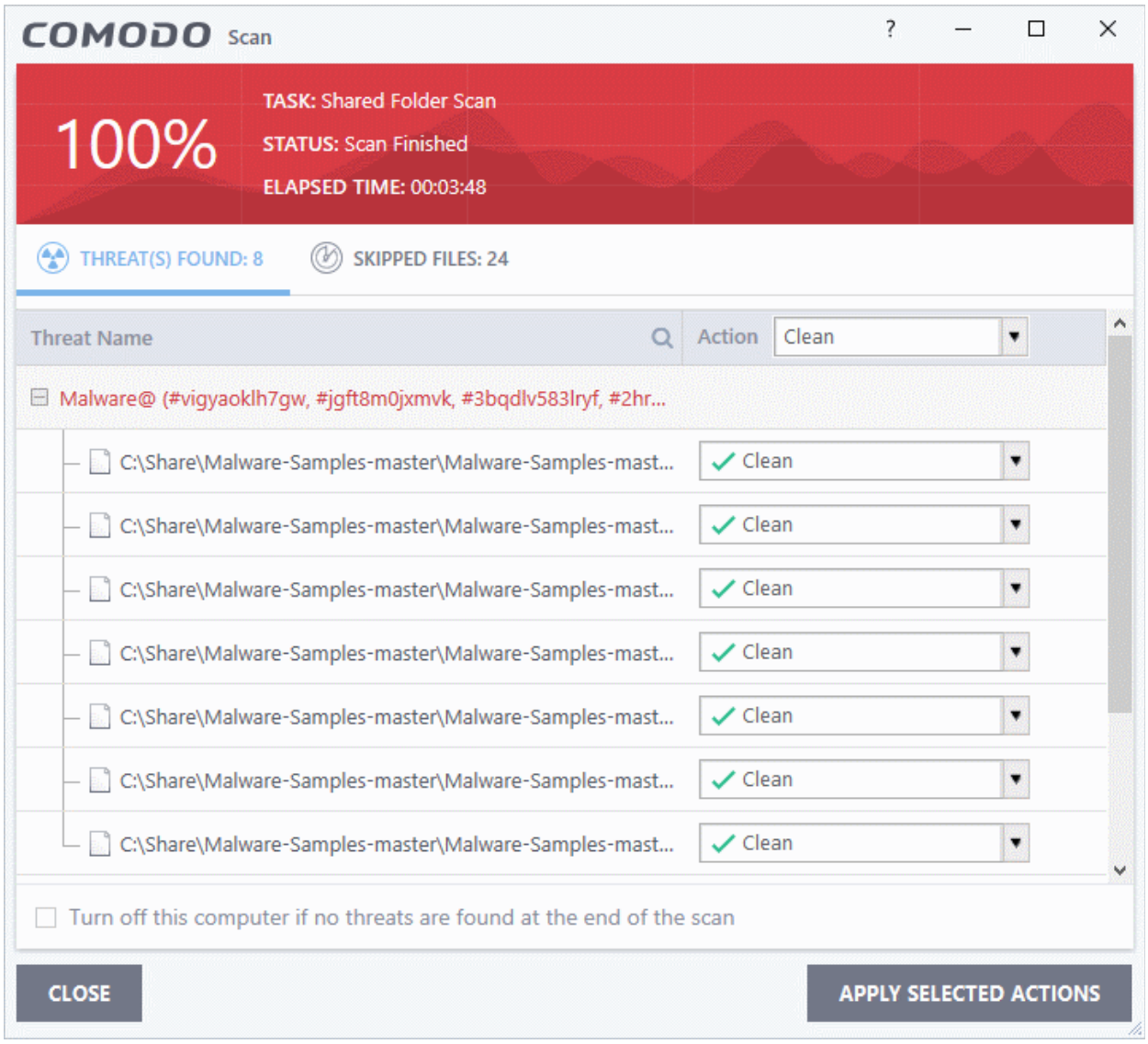
2.3. Process Infected Files

The results screen at the end of a scan lets you clean, quarantine or ignore any detected threats. The screen contains two tabs:

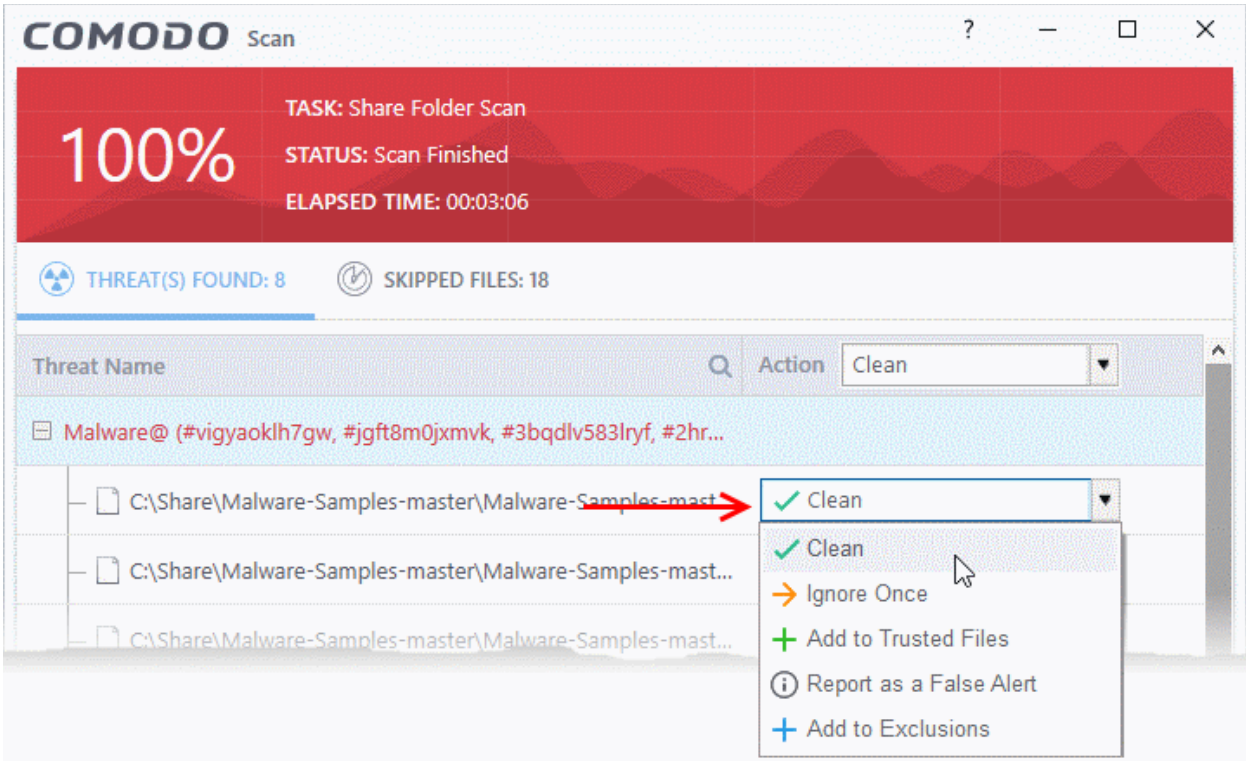
- **Threats Found**: Number of malicious items discovered by the scan. You can clean, quarantine or ignore the threats.
- **Skipped Files**: Files that were omitted because they took longer to scan than the time limit.

View identified threats and take actions

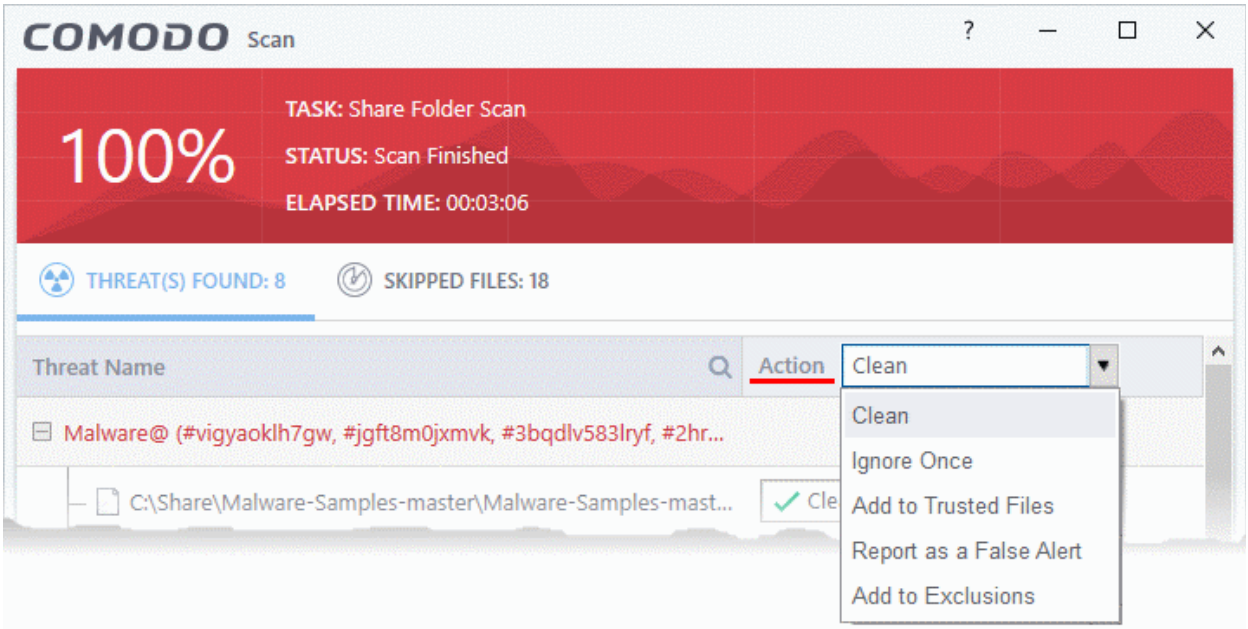
- Click the 'Threats Found' tab (if it is not already open)



- Use the drop-down menus to apply actions to individual files:



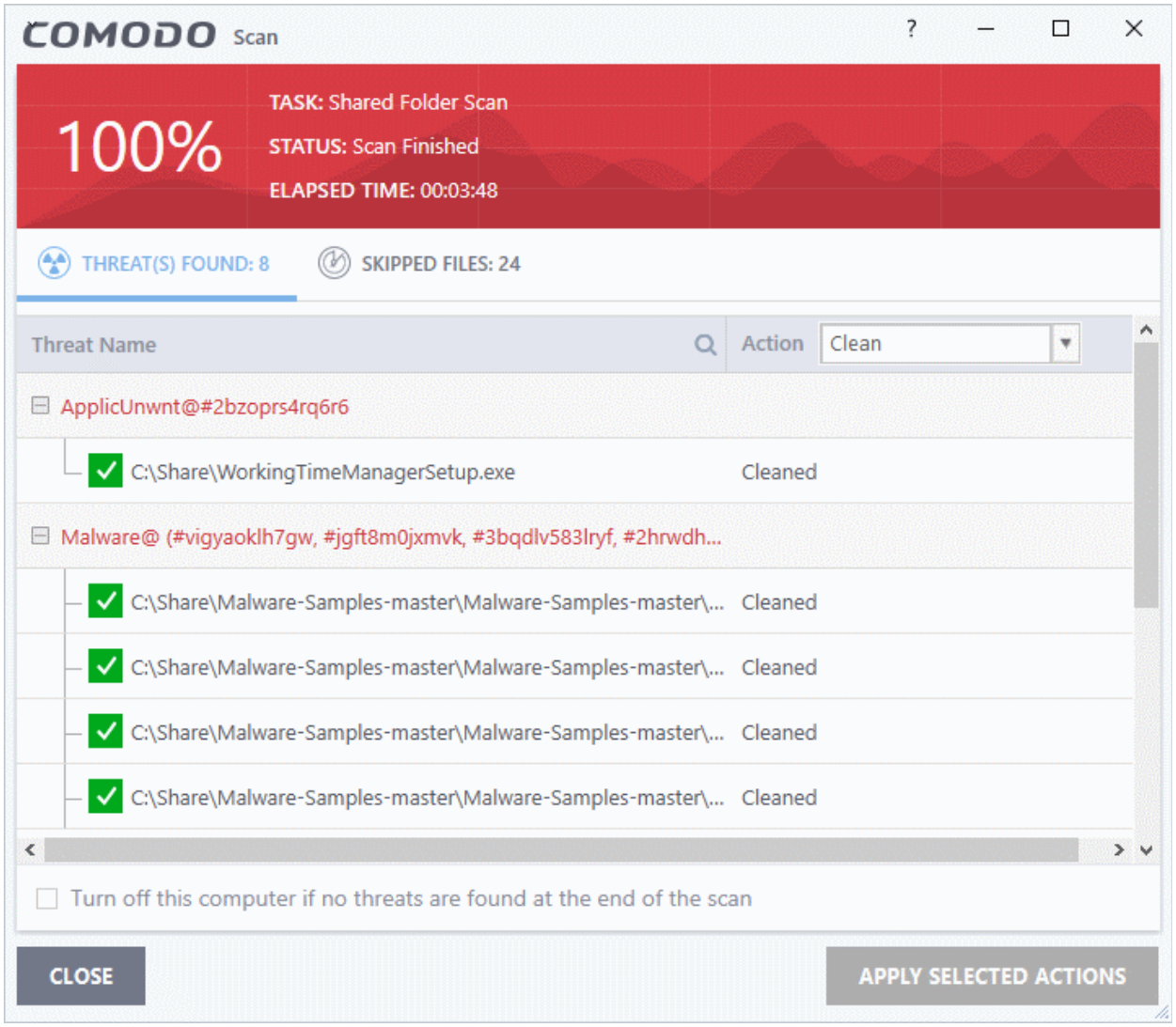
- Or use the 'Action' drop-down at top-right to apply your choice to all threats at once.



Available actions are:

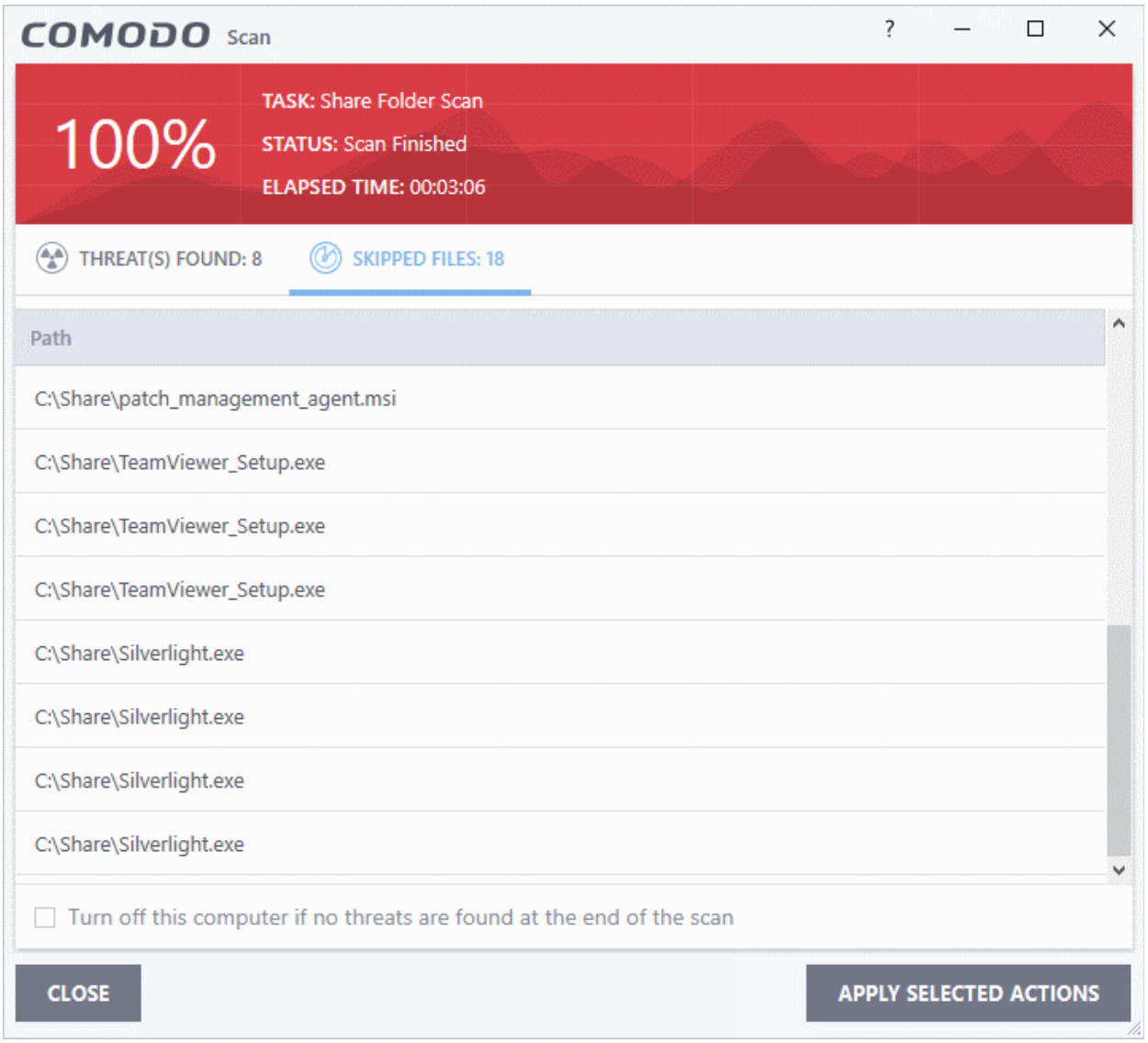
- **Clean** - The virus is removed from the file if a disinfection routine is available. The cleaned file is left in its original location. If no routine exists, the file is quarantined. Click 'Tasks' > 'Advanced Tasks' > 'View Quarantine' to view this area. You can restore or permanently delete files from quarantine as required. See **Manage Quarantined Items** for more details.
- **Ignore Once** - Allows the file to run this time only. The file will still get flagged as a threat by future antivirus scans.
- **Add to Trusted Files** - Creates an exception for the file by giving it a 'Trusted' rating in the **File List** ('Settings' > 'File Rating' > 'File List'). The AV scanner will not detect the file as a threat in future scans. Only select this option if you are sure the file is trustworthy.

- **Report as a False Alert** - Sends the file to Comodo for further analysis. Submitting a false positive will also add the item to trusted files, so it won't get flagged by future scans. The file will be added to the global whitelist if Comodo confirms the false-positive
- **Add to Exclusions** - Creates an exception for the file so it won't get flagged by future virus scans. You can review exclusions at 'Settings > 'Advanced Protection' > '**Scan Exclusions**'. The file's trust rating does not change.
- Click 'Apply Selected Actions'. The result is shown in the 'Actions' column:



View skipped files

- Click the 'Skipped Files' tab



The 'Skipped Files' tab shows files that were omitted from the scan. These files took longer than the max. time allowed to scan a single file. The max. time allowed depends on the profile used for the scan. To view the max. scan time

- Click 'Settings' > 'Antivirus' > 'Scans'
- Open the profile used by the scan
- View/edit the max. scan time as required.

Note - The skipped files tab does not show excluded files, or files that were skipped because they exceeded the maximum file size. It only shows files skipped because they exceeded the max. scan time.

2.4. Manage Virus Database Updates

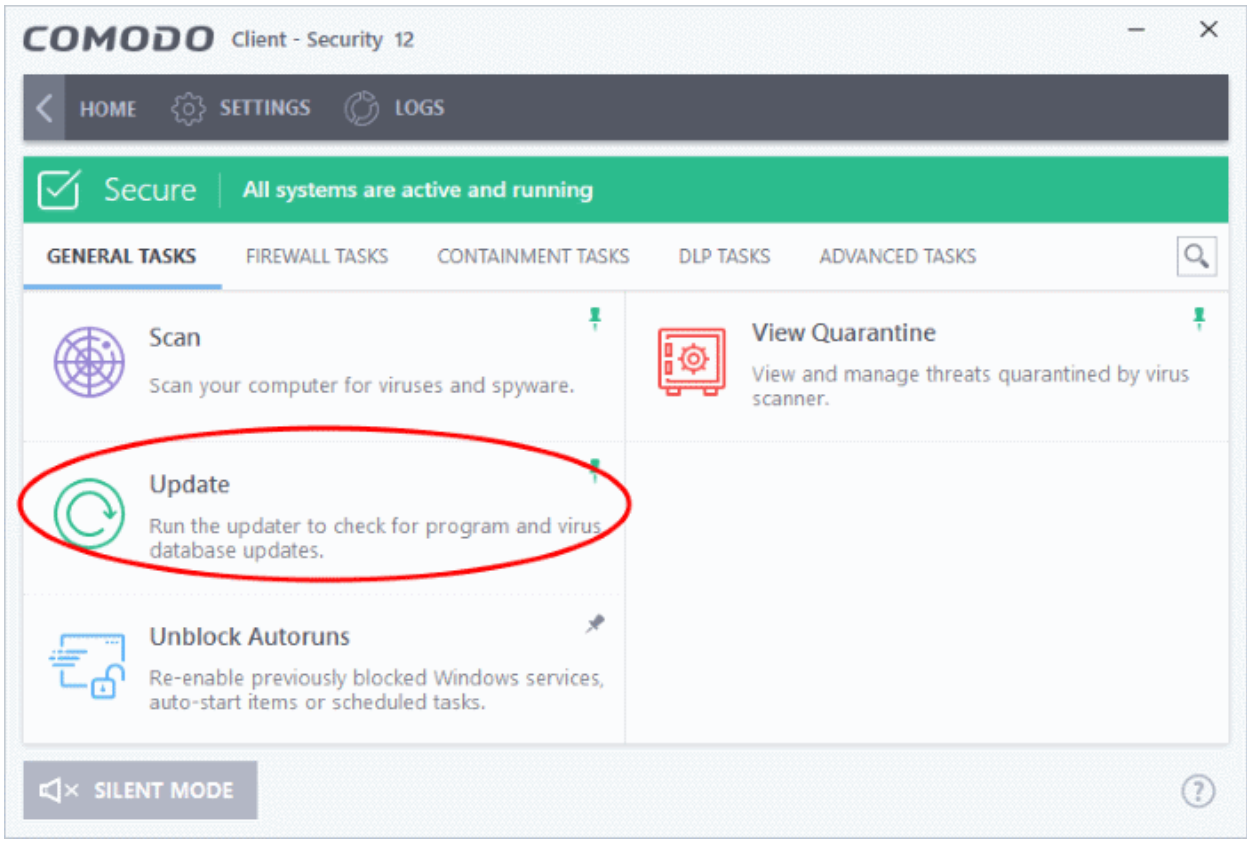
- Click 'Tasks' > 'General Tasks' > 'Update'

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

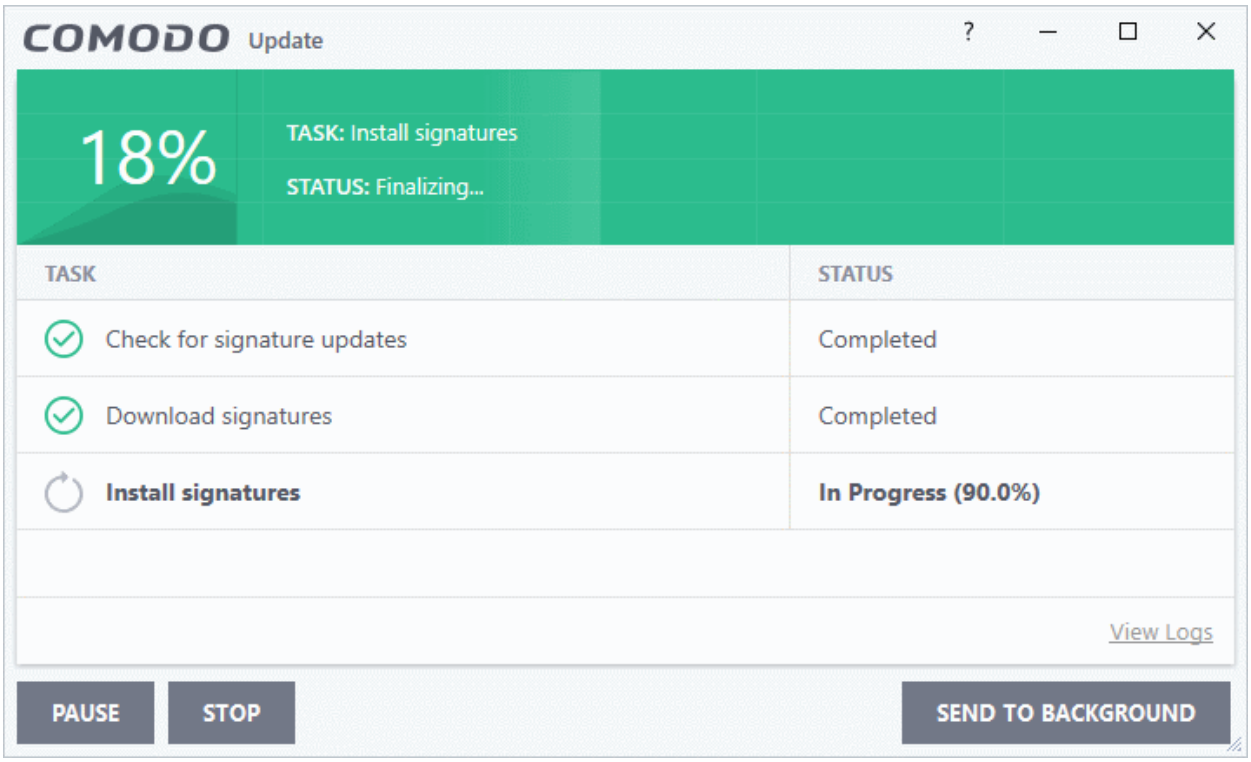
Prerequisite - You must be connected to the internet to download updates.

Manually check for the latest virus and program updates

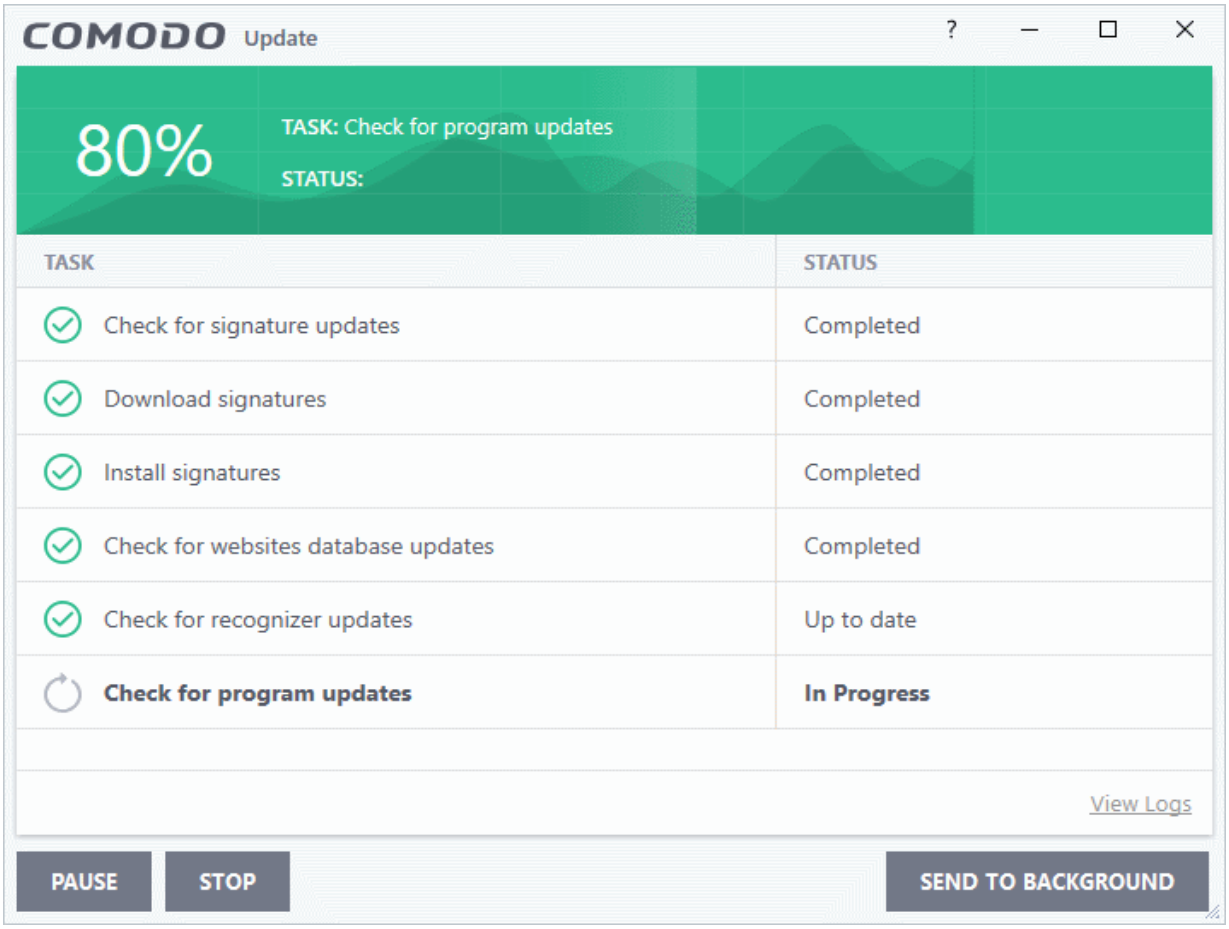
- Click 'Tasks' > 'General Tasks'
- Click the 'Update' tile:



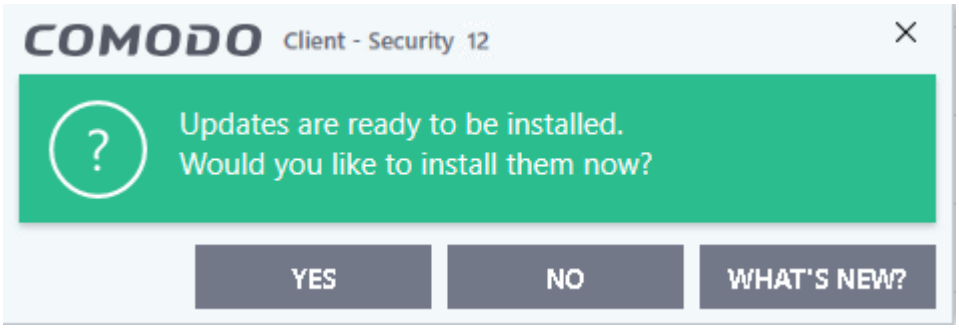
Signature updates are downloaded first if they are available:



The updater then checks for web filter, VirusScope, and program updates:

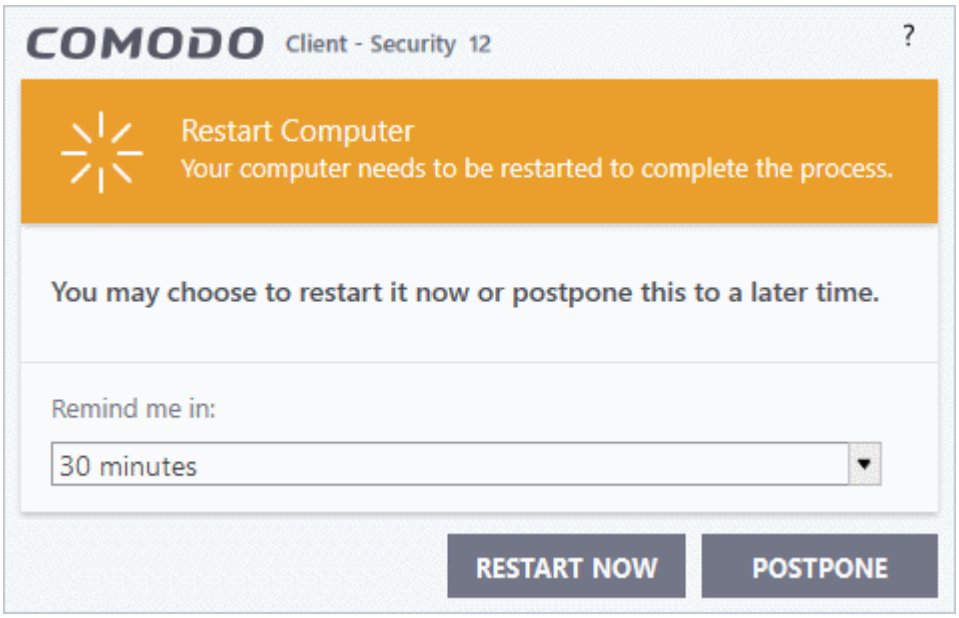


CCS will ask you to confirm the update at the following dialog:



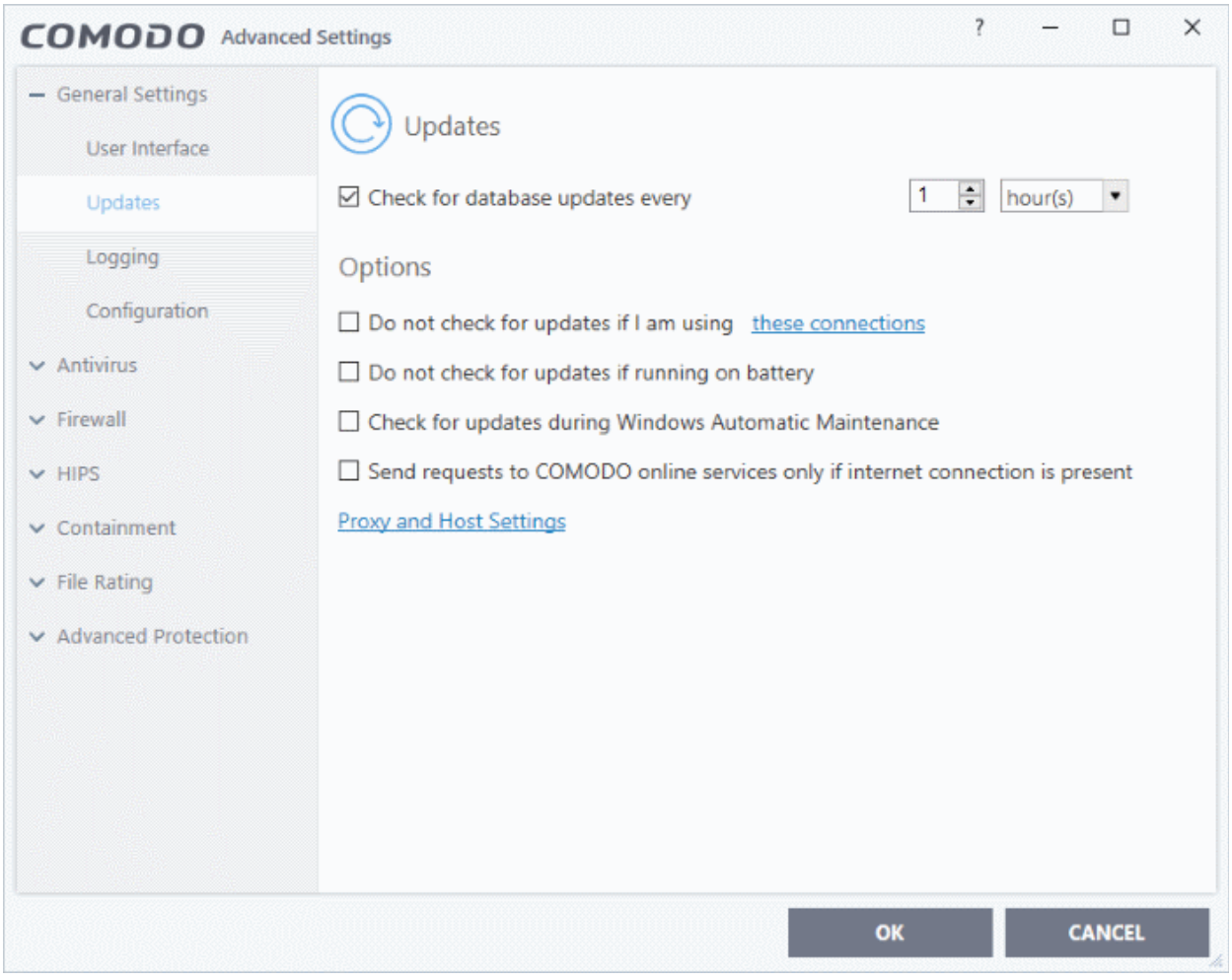
- Click 'Yes' to begin installation:

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



Automatic Updates

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



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

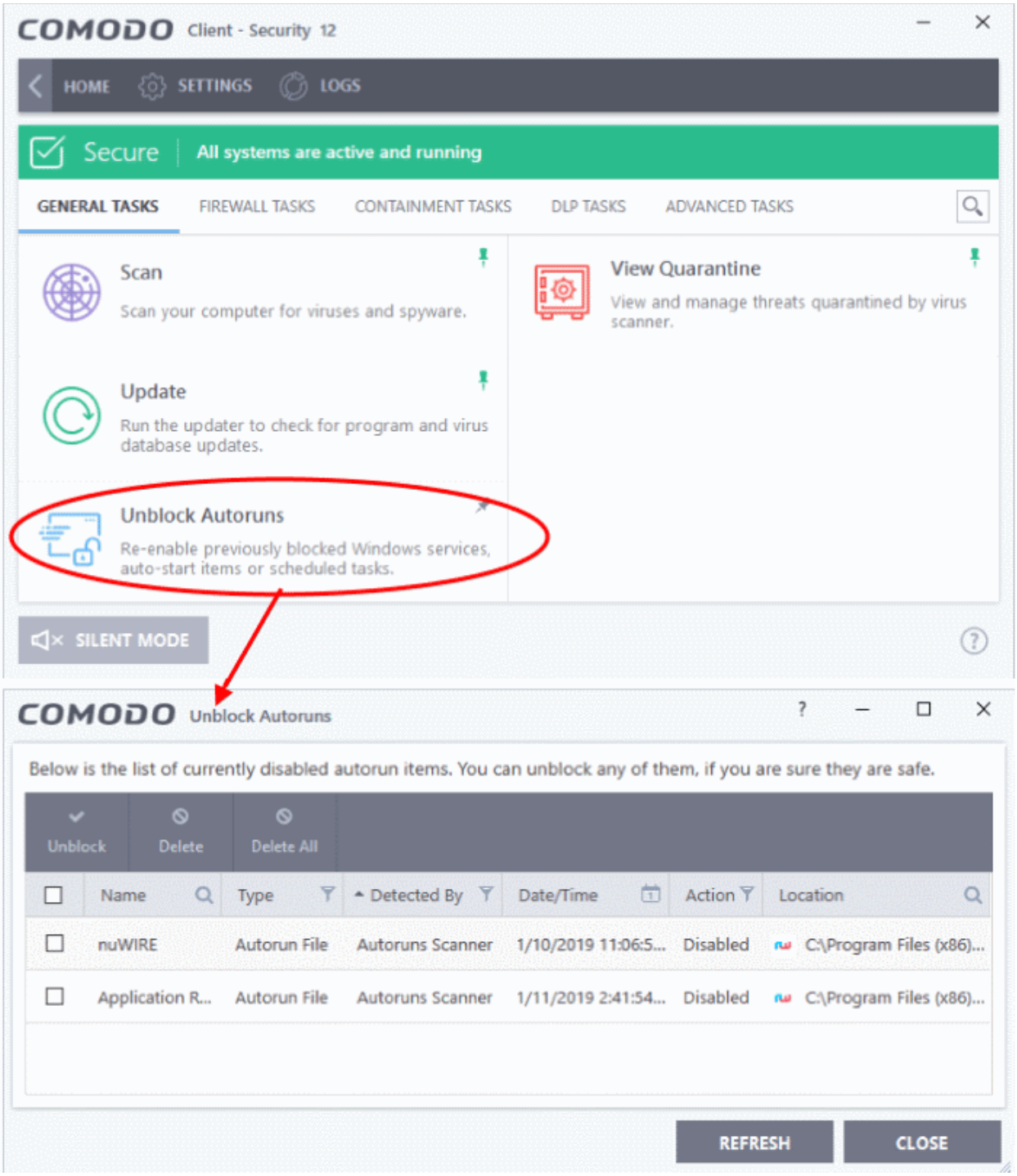
2.5. Manage Blocked Autoruns

Click 'Tasks' > 'General Tasks' > 'Unblock Autoruns'

- The 'Unblock Autoruns' area shows applications that were blocked by the boot protection feature of CCS.
- The feature monitors attempted changes to the registry records of Windows services, auto-start entries and scheduled tasks. The feature can be managed in the following locations:
  - **Realtime Scans** - Click 'Settings' > 'Advanced Protection' > 'Miscellaneous' > ' Apply the selected action to unrecognized autorun entries to new/modified registry items'
  - **On-Demand Scans** - Click 'Settings' > 'Antivirus Settings' > 'Scans' > 'select the scan profile' > 'Options' > 'Apply this action to suspicious auto-run processes'
- CCS will disable apps that attempt to modify protected registry items if 'Terminate and Disable' is chosen for 'Apply this action to suspicious auto-run processes'
- You can also unblock applications that you think are safe.

View and manage blocked autorun items

- Click 'Tasks' > 'General Tasks'
- Click the 'Unblock Autoruns' tile
- The interface shows all auto-run items blocked by CCS:

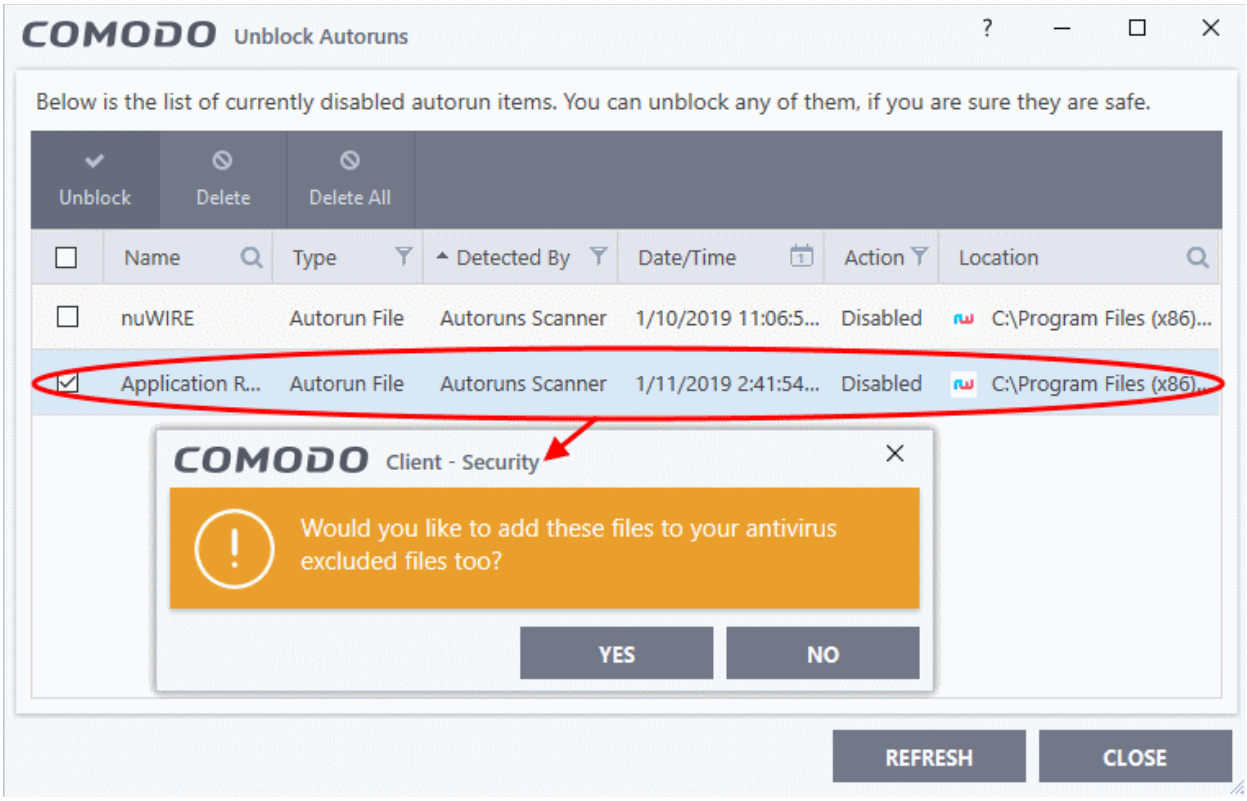


Unblock Autoruns - Column Descriptions	
Column Header	**Description**
Name	The label of the blocked item.
Type	The category of item. For example, 'Autorun File', 'Scheduled Task' or 'Windows Service'.
Detected By	The security module which identified the threat.
Date/Time	When the item was detected.

Action	The response to the threat. The possible actions are: • Ignore • Terminate • Terminate and Disable • Quarantine and Disable
Location	Path of the identified application.

Restore blocked autorun items

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



You will be asked if you want to add the file to the **Scan Exclusions** list.

- Click 'Yes' to add the item to exclusions. It will be restored to its original location and won't be flagged as dangerous by future scans.
- Click 'No' to ignore the item once. It will be restored to its original location, but will still be flagged as a threat by the next scan.

Delete blocked autoruns entries

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

The item will be removed from your computer.

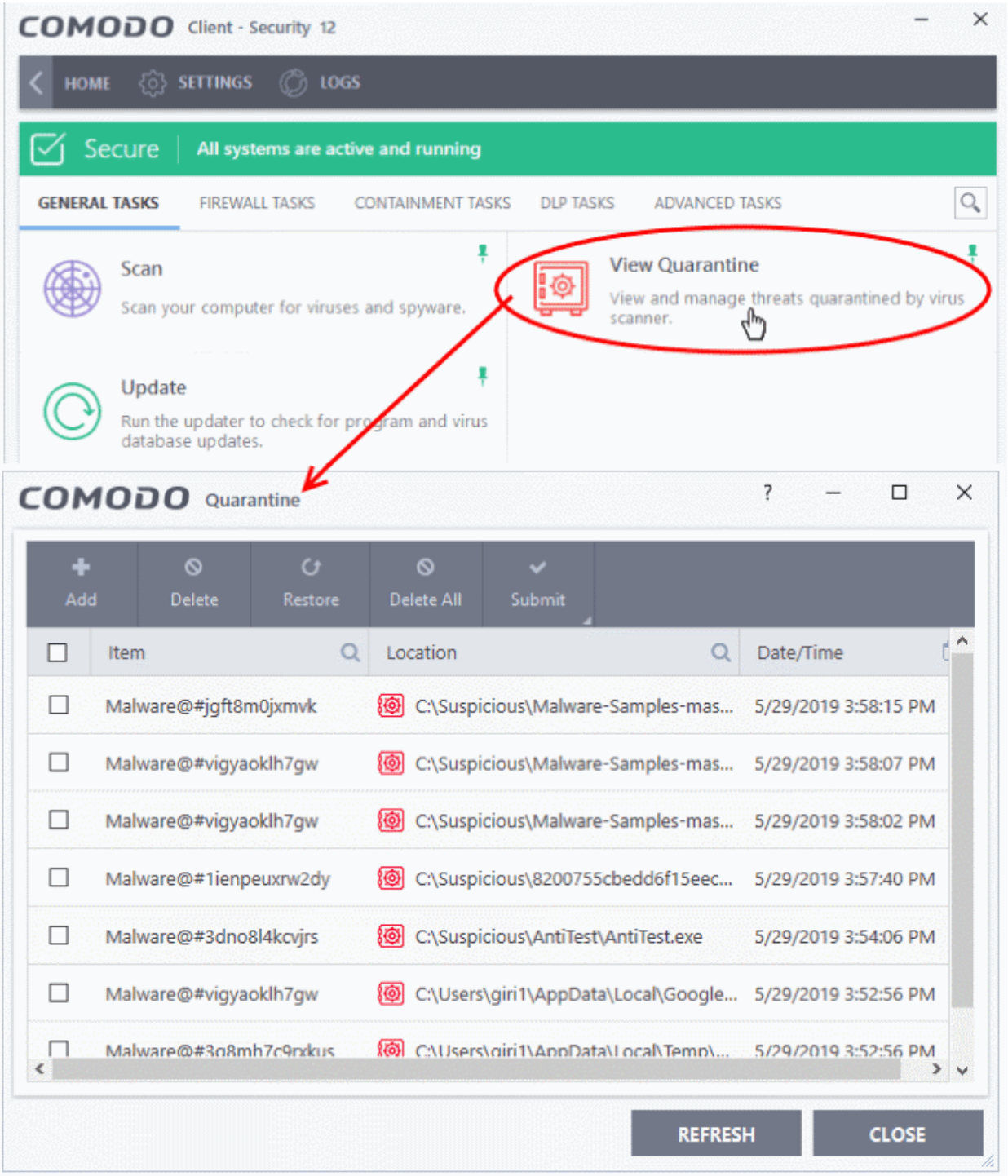
2.6. Manage Quarantined Items

Click 'Tasks' > 'General Tasks' > 'View Quarantine'

- The quarantine area shows malicious files which CCS has isolated to prevent them from infecting your system.
- All files in quarantine are encrypted so they cannot run or cause harm.
- Items are usually quarantined by the antivirus scanner, but it is also possible to manually quarantine items. See '**General Tasks' > 'Scan and Clean Your Computer**' if you want to learn about the AV scanner.

Open the 'Quarantine' interface

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'



- **Item** - The name of the malicious component
- **Location** - The file path of the item
- **Date/Time** - When the item was moved to quarantine.

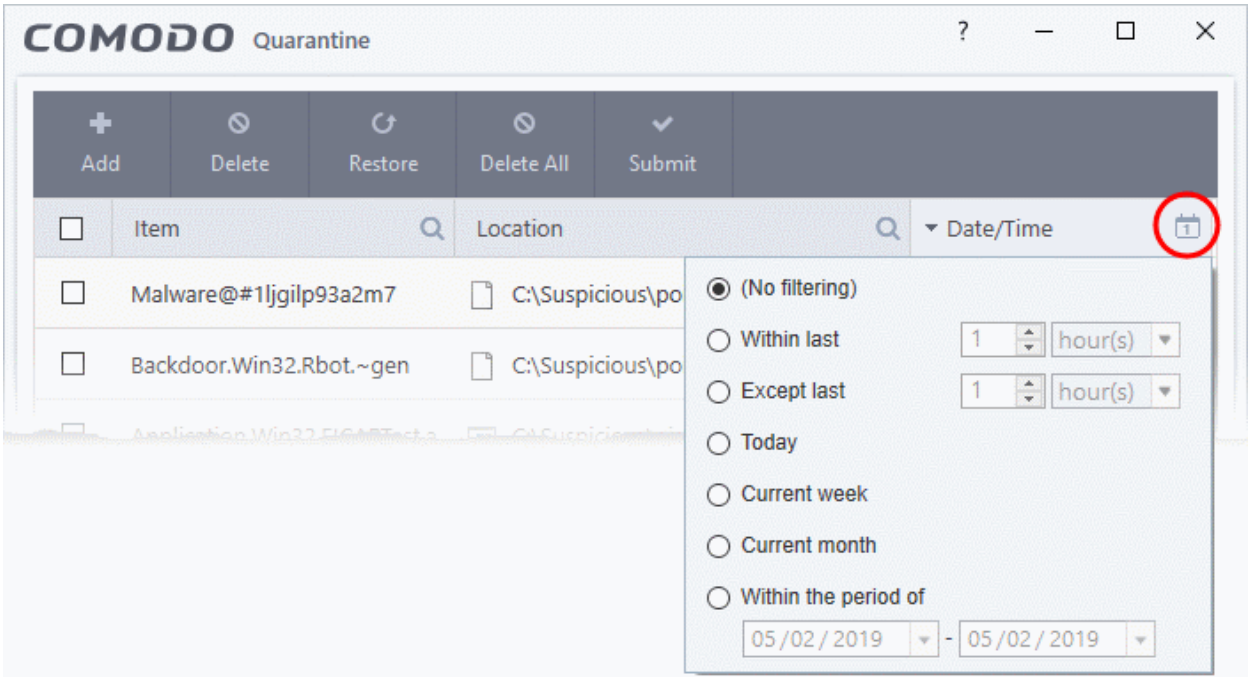
The interface lets you review quarantined files and take the following main actions:

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

Search and filter options:

- Click any column header to sort items in alphabetical order of that column.

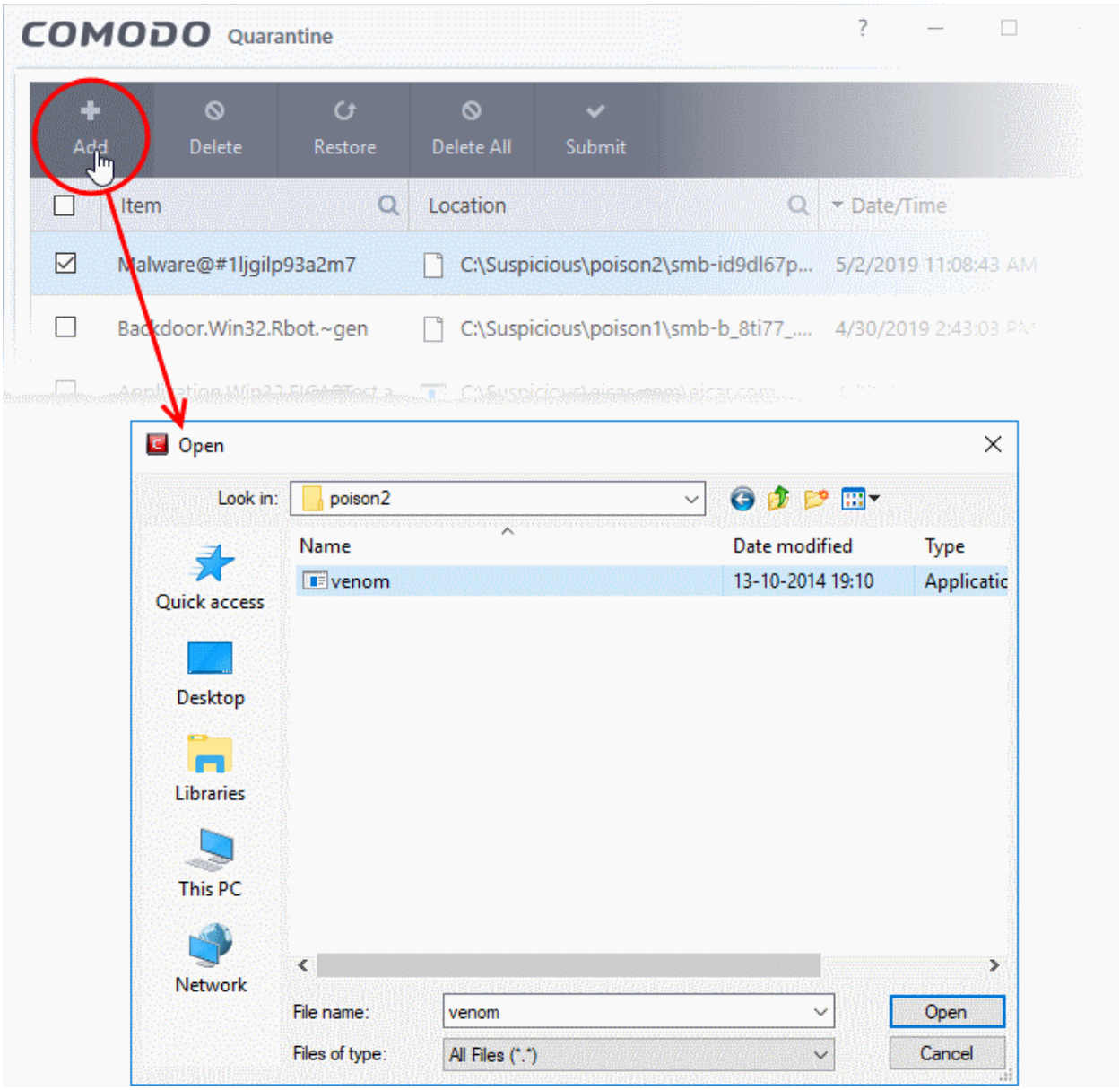
- Click the search icon in the 'Item' column to search for a file by name.
- Click the search icon in the 'Location' column to search by file-path.
- Click the icon in the 'Date/Time' column to filter results by time period.



Manually add files to quarantine

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

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Click the 'Add' button at the top
- Navigate to the file you want to add to the quarantine and click 'Open'.



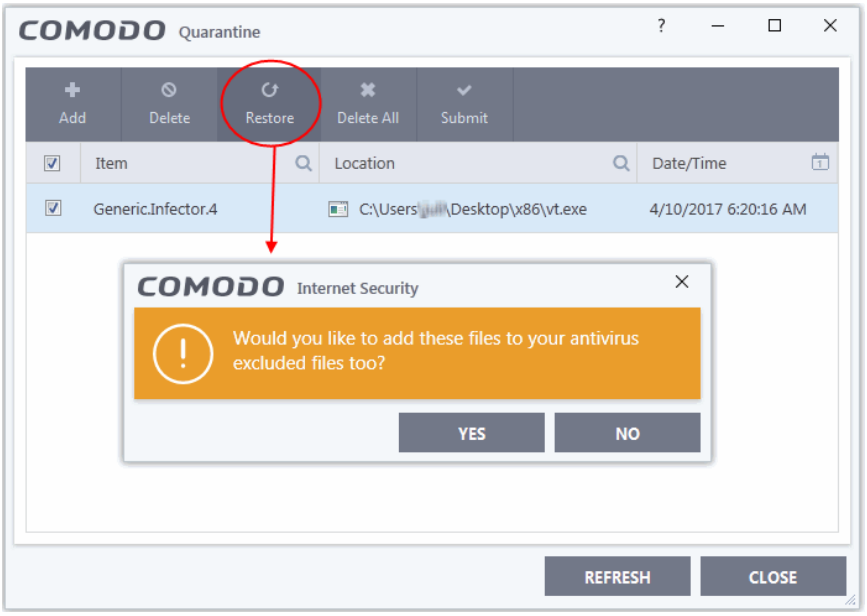
The file will be added to 'Quarantine'. You can even send the file for analysis to Comodo Valkyrie, for inclusion in the white list or black list, by clicking the 'Submit' button.

Remove a quarantined item

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Select the items in the quarantine interface and click the 'Delete' button at the top.
- Click the 'Delete All' button if you want to permanently remove all quarantined items.
- The files will be deleted from your computer

Restore a quarantined item

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Select the items to be moved back to their original locations and click the 'Restore' button at the top.



You will be asked if you want to add the item to the **Scan Exclusions** list:

- '**Yes**' - The file will be restored to its original location. It will not be flagged as dangerous nor quarantined by future antivirus scans.
- '**No**' - The file will be restored to its original location. If the file contains malware it will be re-quarantined by the next antivirus scan.

Submit selected quarantined items to Valkyrie for analysis

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

- Click 'Tasks' on the CCS home screen
- Click 'General Tasks' > 'View Quarantine'
- Select the items you want to submit. You can send several files at once.
- Click 'Submit' > 'Submit to Valkyrie' in the top-menu. The files will be immediately sent to Valkyrie for analysis.

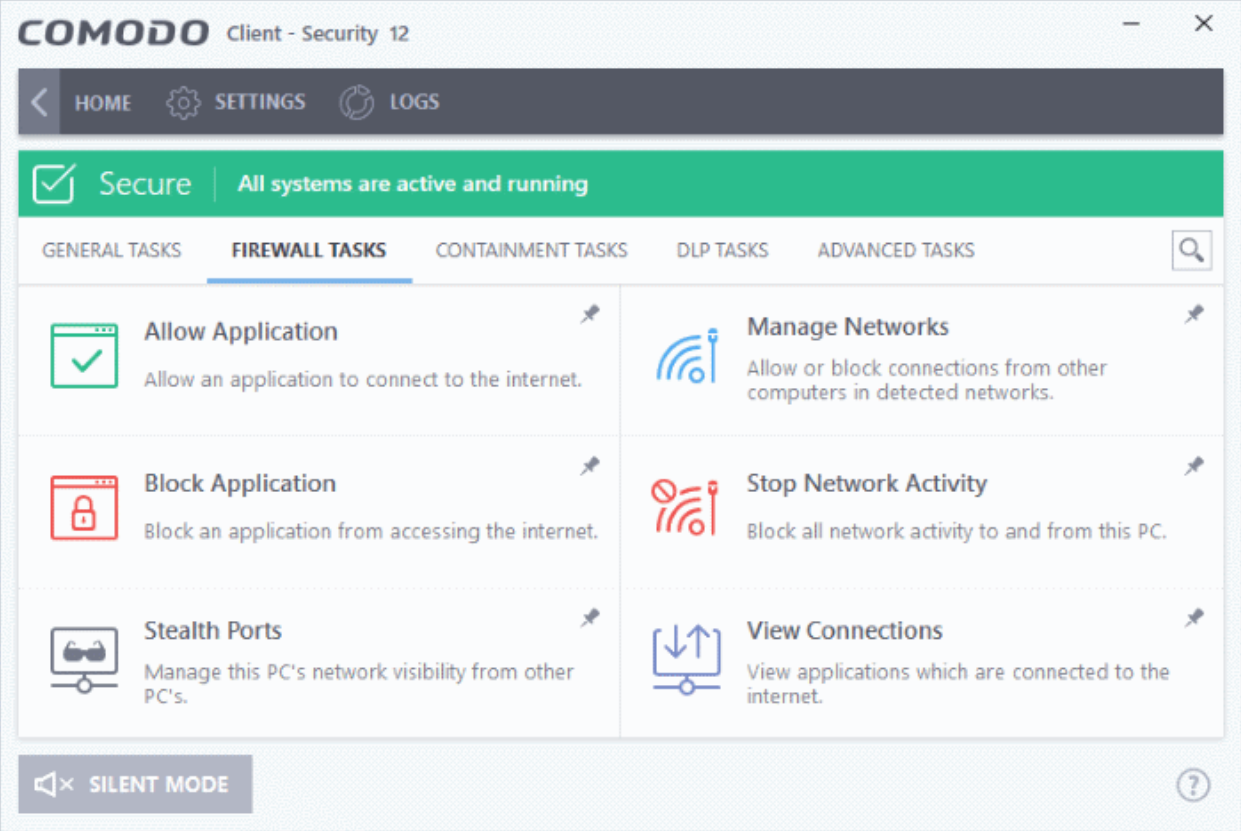
Tip: Alternatively, right click an item then choose 'Submit to Valkyrie' from the menu.

- All submitted files are analyzed at Valkyrie. If they are found to be trustworthy, they will be added to the safe list (white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (blacklisted).

3. Firewall Tasks - Introduction

- Click 'Tasks' > 'Firewall Tasks'
- The firewall offers the following main benefits:
  - Monitors all network traffic to protect your computer against inbound and outbound threats
  - Hides your computer's ports from hackers
  - Blocks malicious software from transmitting your confidential data over the internet.
- The firewall tasks area lets you configure internet access rights per-application, stealth your computer ports, view active connections, and even block all traffic in-and-out of your computer.
  - In addition to this tasks screen, you can also **configure advanced firewall settings** at 'Settings' >

'Firewall'.



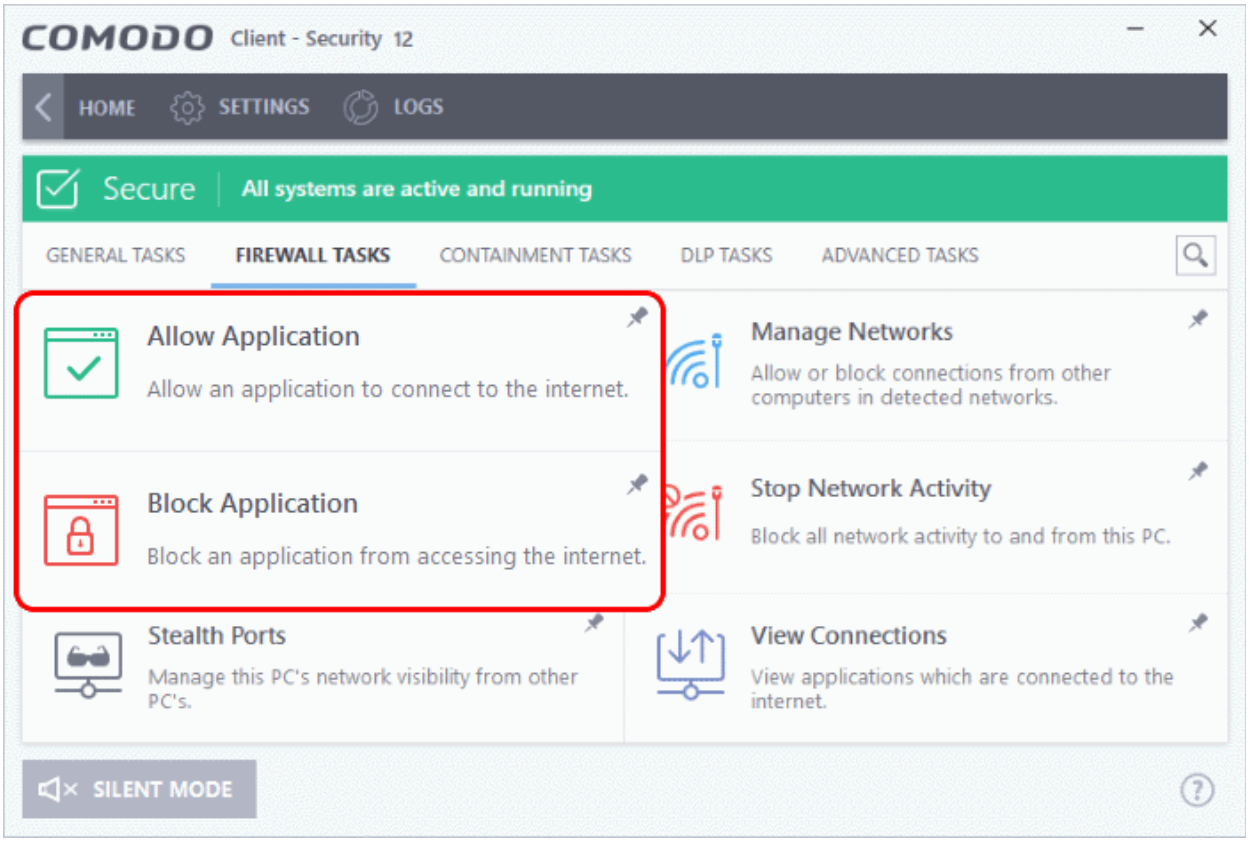
See the following sections for help with each area:

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

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See '**Password Protection**' for more details."

3.1. Configure internet access rights for applications

- Click 'Tasks' > 'Firewall Tasks' > 'Allow Application' or 'Block Application'
- The firewall tasks screen lets you quickly allow or block applications from accessing the internet.



Allow an application to connect to the internet

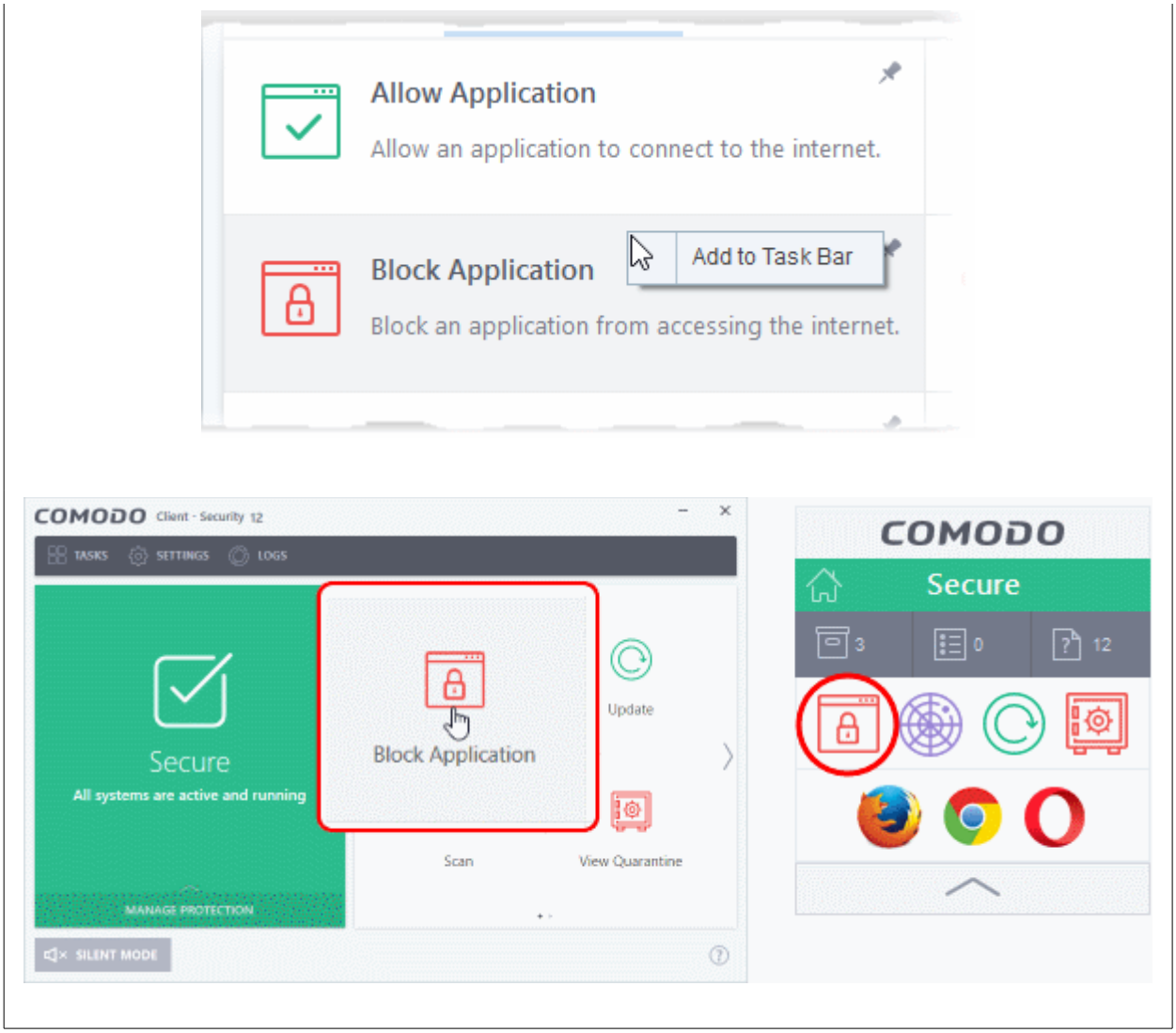
- Click 'Tasks' > 'Firewall Tasks'
- Click 'Allow Application'
- Browse to the main executable file of the application
- Click 'Open'
- This will create an 'Allow Request' rule for the application in 'Settings' > 'Firewall' > 'Application Rules'

Block an application's Internet access rights

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

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

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



3.2. Stealth your Computer Ports

- Click 'Tasks' > 'Firewall Tasks' > 'Stealth Ports'
- Port stealthing is a security feature which hides your ports to the outside world, providing no response to port scanners.

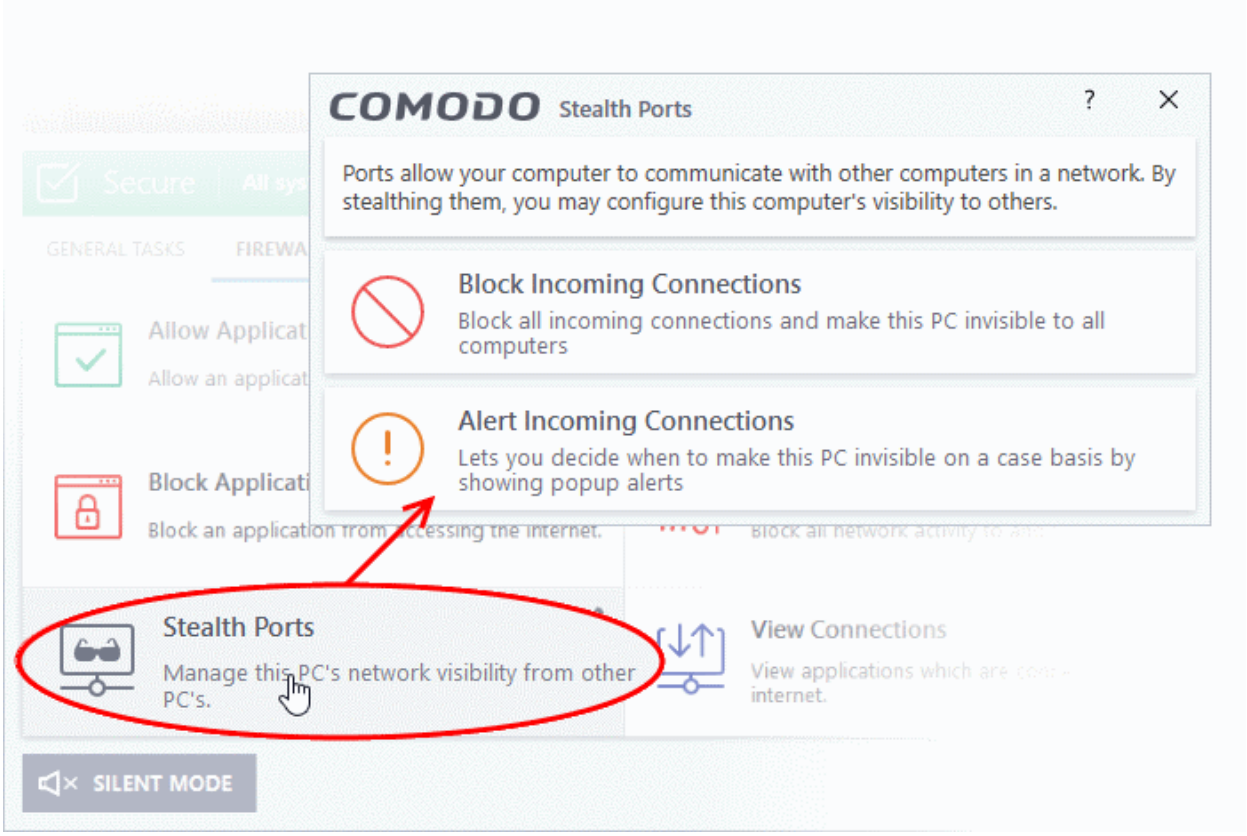
What is a port? Your computer sends and receives data through an interface called a 'port'. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to the internet using ports 80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

- Stealthing a port effectively makes your computer invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt. A closed port responds with a 'closed' reply, which reveals that there is a PC in existence.
- If a hacker or automated scanner cannot 'see' your computer then they will move on to other targets. You can still connect to the internet and transfer information as usual, but remain invisible to outside threats.

Stealth ports on your computer

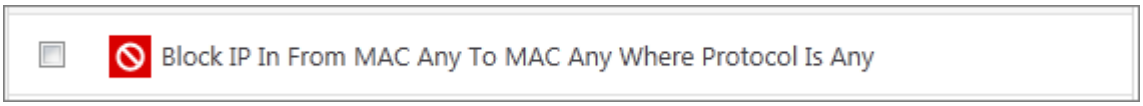
- Click 'Tasks' > 'Firewall Tasks'

- Click 'Stealth Ports'



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

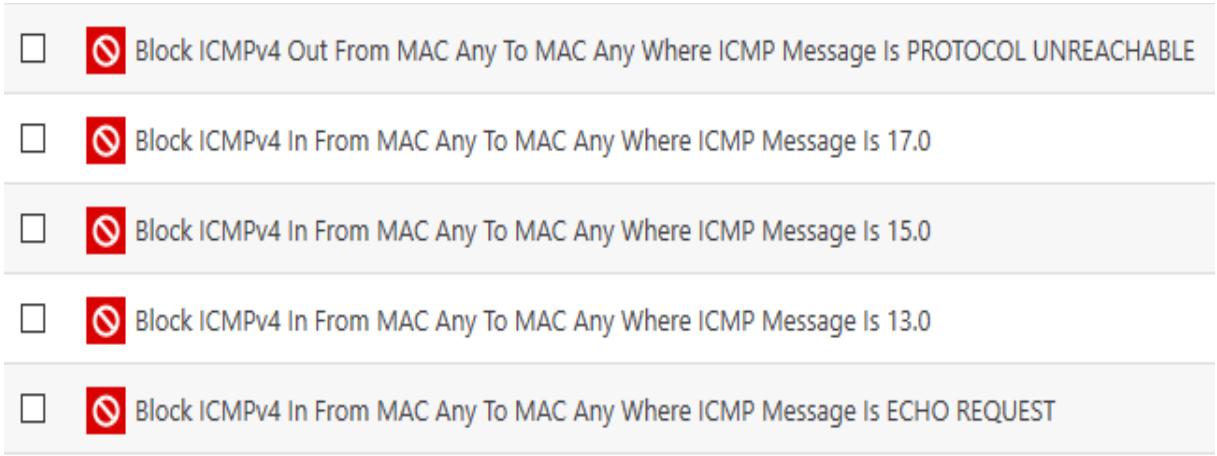
  Block And Log| IP | In| From Any IP Address| To Any IP Address | Where Protocol is Any



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

- **Alert incoming connections** - You will see a **firewall alert** every time there is a request for an incoming connection. The alert asks your permission on whether or not you want the connection to proceed. This can be useful for peer-to-peer and remote desktop applications which need to access your ports in order to connect. Specifically, this option adds the following rules in the '**Global Rules**' interface:

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



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

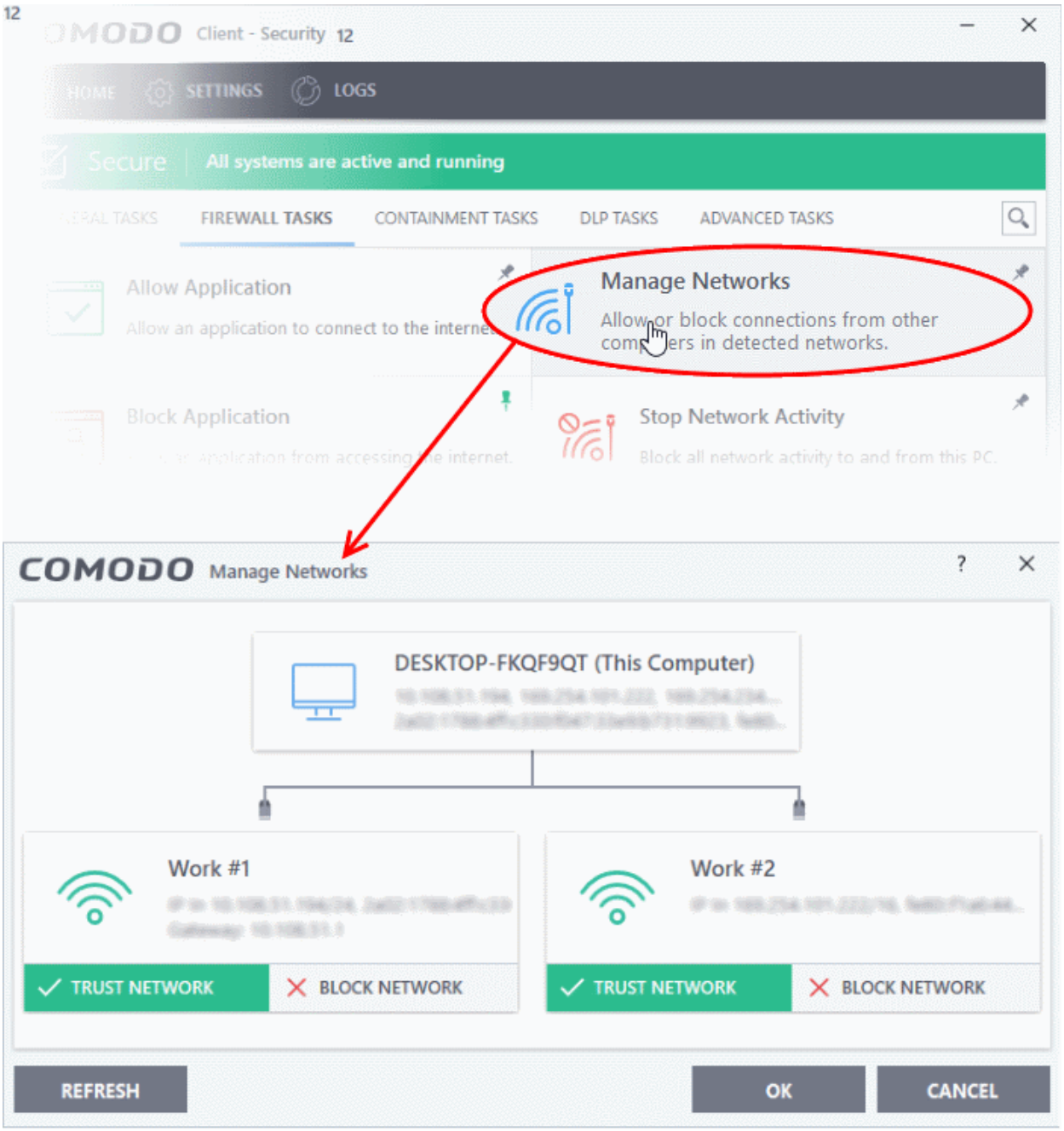
3.3. Manage Network Connections

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

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

View all network connections

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



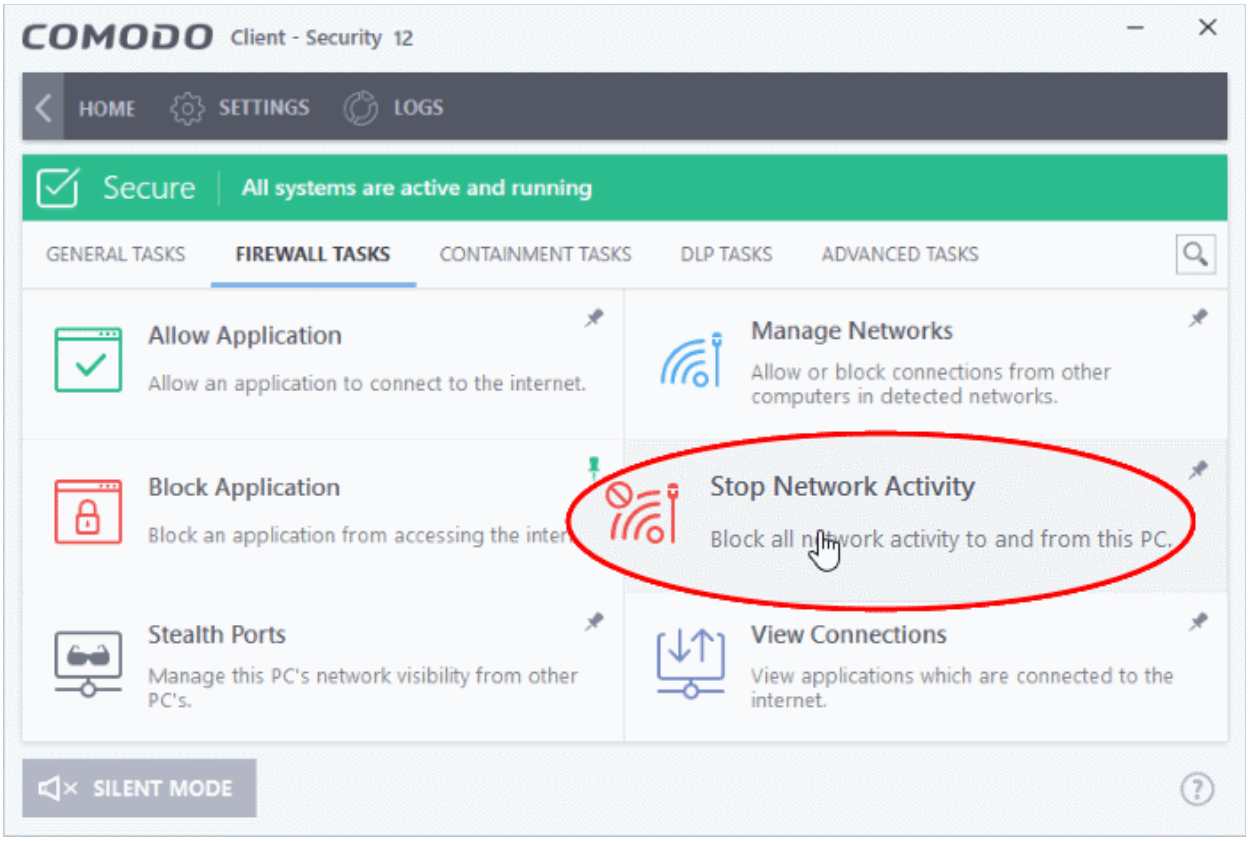
- Use the handles (< >) to scroll through all available networks or computers
- **Trust Network and Block Network** - You can allow or ban a network by clicking the appropriate button under the network in question. You will not receive any inbound or outbound traffic from blocked networks.
- **Refresh** - Reloads the list with the latest network connections. Click this button if you have recently made network changes that are not yet visible in the interface.
- To view, create or block **Network Zones**, click 'Settings' > 'Firewall' > 'Network Zones'

3.4. Stop all Network Activities

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

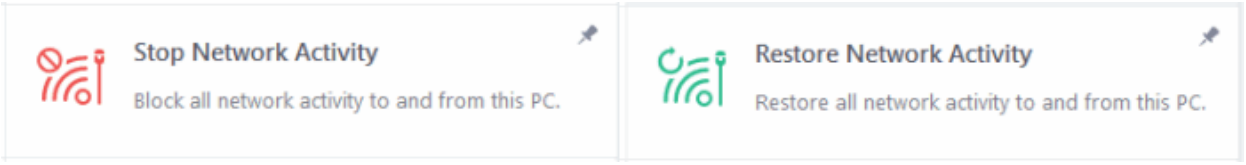
- The 'Stop Network Activity' feature terminates all inbound/outbound communication between your computer and outside networks (including the internet).
- Connections will remain closed until you re-enable them by clicking 'Restore Network Activity'.

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



Manage network activities from your computer:

- Click 'Tasks' > 'Firewall Tasks'
- Click 'Stop Network Activity' to disconnect your computer from all networks
- Click 'Restore Network Activity' to re-enable connectivity



- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have previously blocked in '**Manage Network Connections**' or '**Network Zones**' will remain blocked
- You can assign networks to network zones in the '**Network Zones**' area
- You can configure rules per network zone in the '**Global Rules**' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the '**Manage Network Connections**' area

3.5. View Active Internet Connections

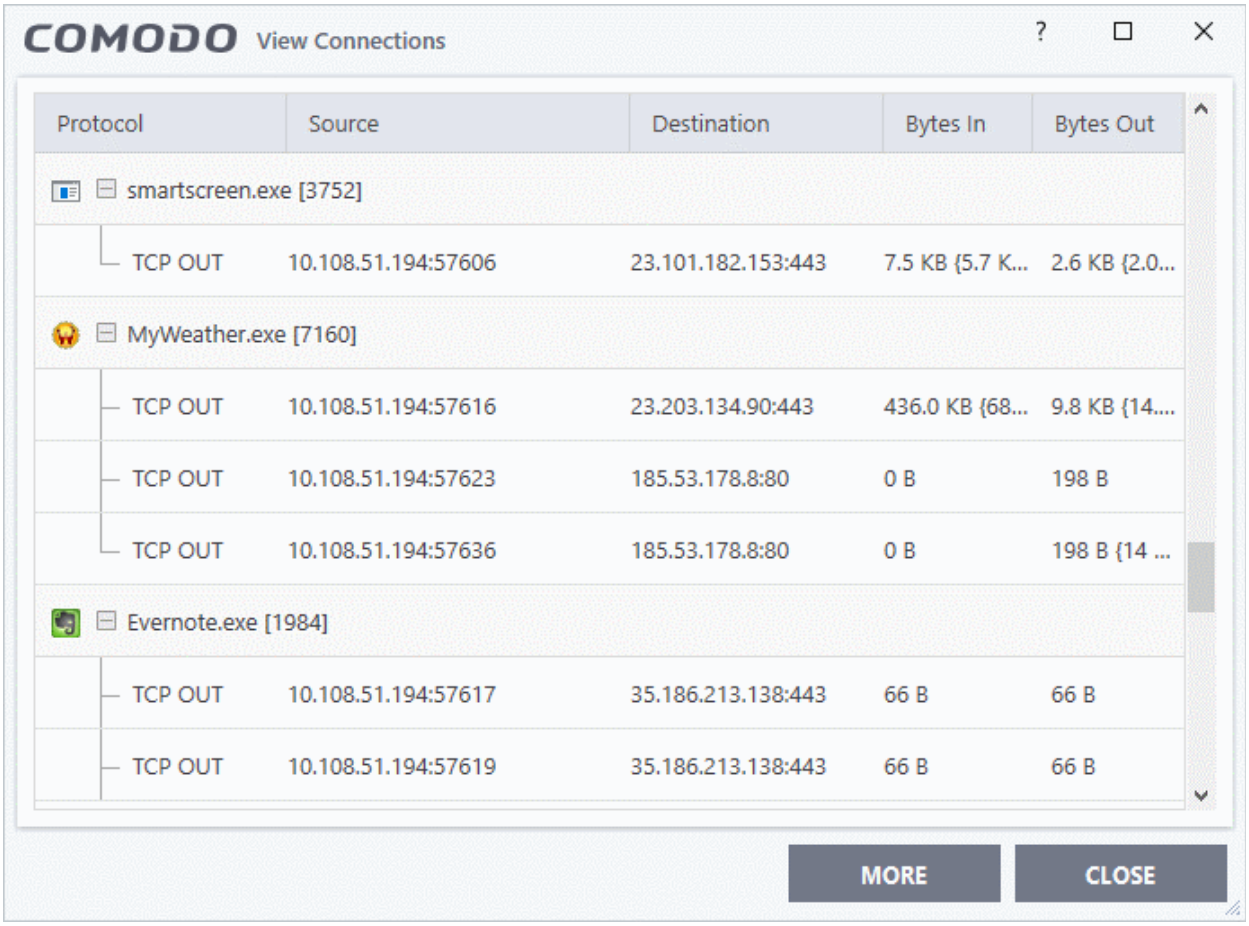
Click 'Tasks' > 'Firewall Tasks' > 'View Connections'

- View connections shows which applications and services currently have an active internet connection.
- You can view the individual connections that each application is responsible for, the direction of the traffic, the source IP/port, and the destination IP/port.
- You can also see the total amount of traffic that has passed in and out of your system over each connection. The list is updated in real time whenever an application opens or drops a connection.
- 'View Connections' is extremely useful when testing firewall configurations or troubleshooting firewall policies and rules. You can also use it to terminate unwanted connections.

View active internet connections on your computer

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

Tip: You can also get to this screen by clicking the number below 'Inbound' or 'Outbound' in the home screen (advanced view).

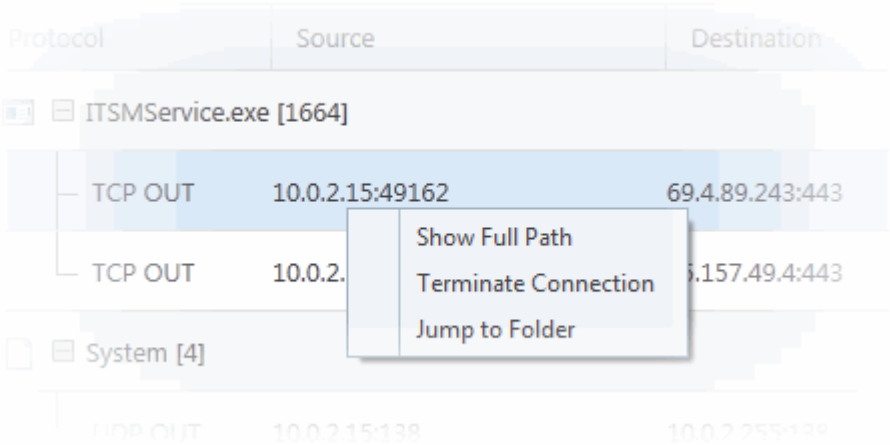


- **Protocol** - The application that is making the connection, the protocol it is using, and the direction of the traffic. Each application may have more than one connection at any time. Click + to expand the list of connections.
- **Source (IP : Port)** - The IP address and port number of the origin of the traffic. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** - The IP address and port number of the target. This is blank if the 'Source' column is 'Listening'.

- **Bytes In** - The total bytes of incoming data since the session started.
- **Bytes Out** - The total bytes of outgoing data since the session started.

Context Sensitive Menu

- Right-click on an item to open the context sensitive menu:



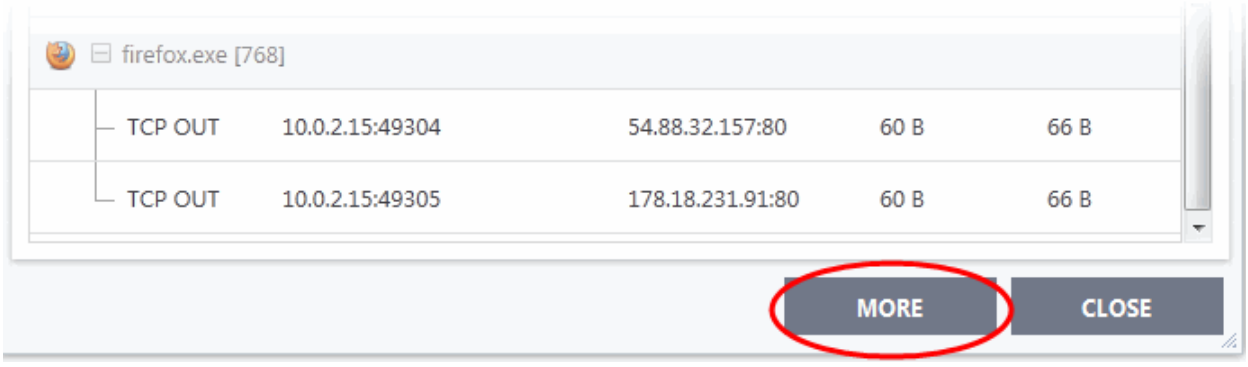
- 'Show Full Path' - view the location of the application
- 'Terminate Connection' - close the application's connection
- 'Jump to Folder' - Open the folder containing the application executable

Identify and kill unsafe network connections

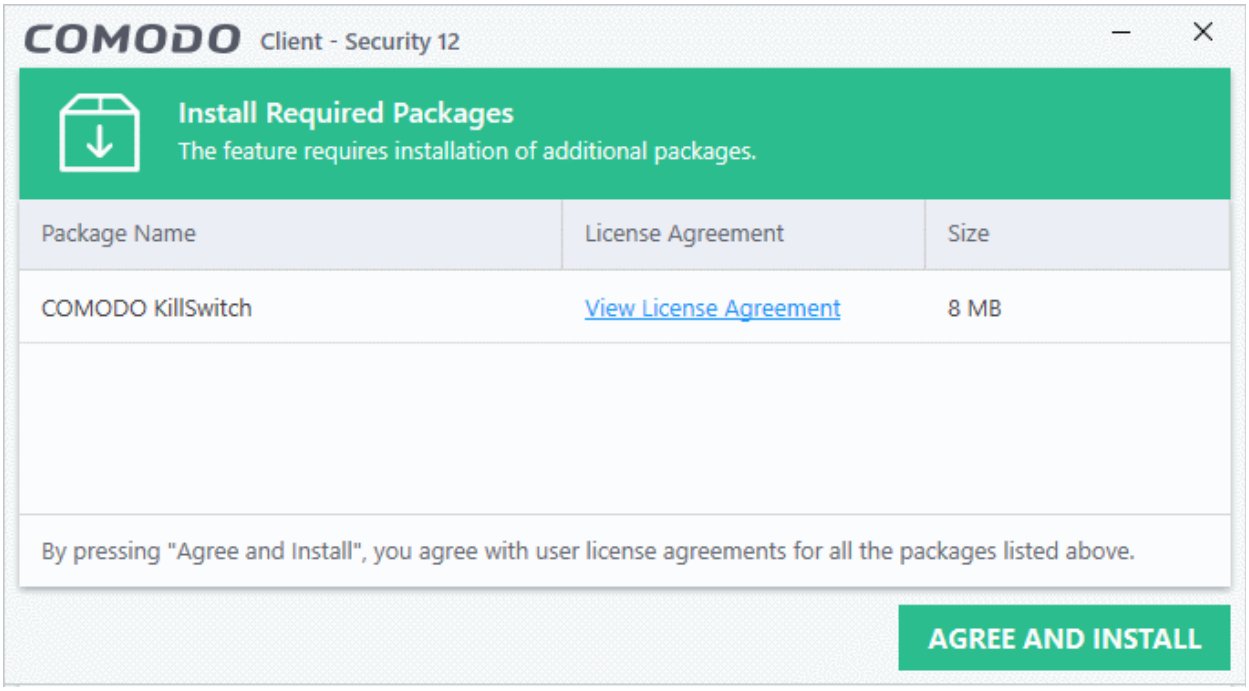
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides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

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

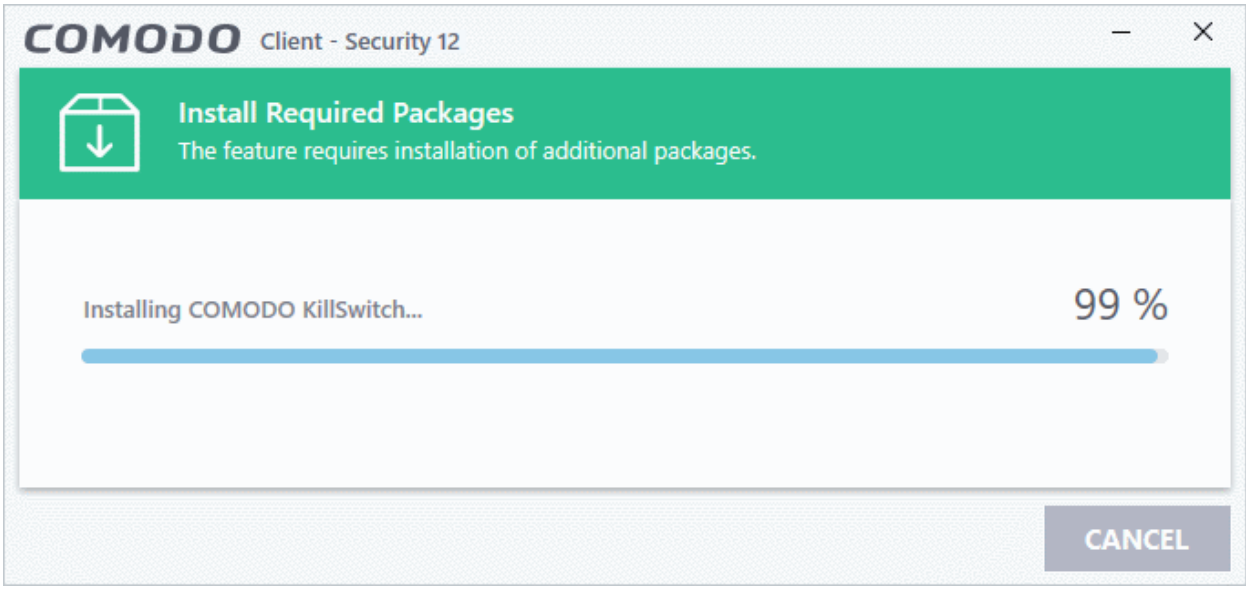
- Click the 'More' button in the 'View Connections' to directly access Comodo KillSwitch



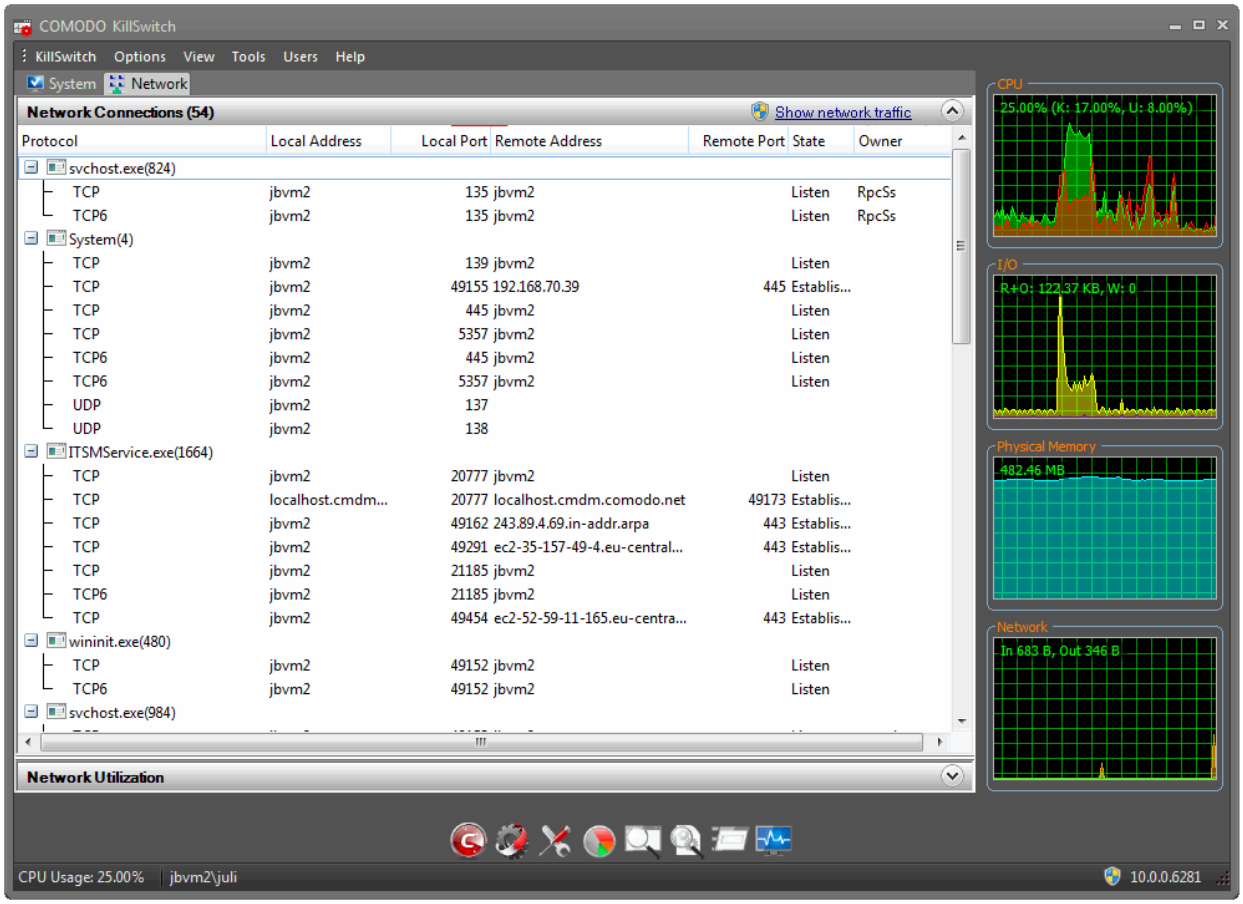
If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CCS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.



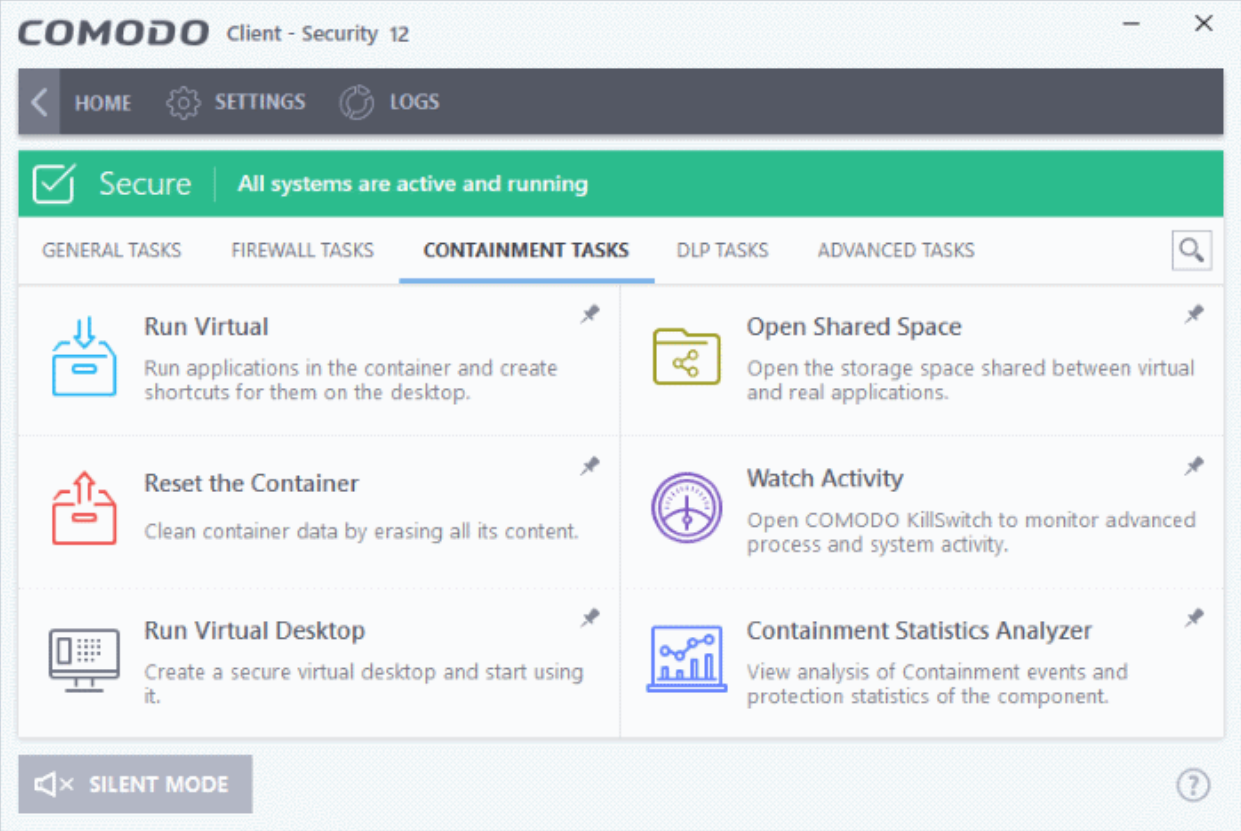
- KillSwitch will open when installation finishes:



4. Containment Tasks - Introduction

Click 'Tasks' > 'Containment Tasks'

- The container is a secure, virtual environment in which you can run unknown, untrusted, and suspicious applications.
- Applications in the container are isolated from the rest of your computer. They are denied access to other processes, write to a virtual file system and registry, and cannot access your personal data.
- This makes it an ideal environment for surfing the internet, because nothing you download can spread to your host system.
- You can run applications in the container on an ad-hoc basis, and you can also create desktop shortcuts to always launch a program in the container.



Note: Containment is not supported on Windows XP or Windows Server 2003

Containment tasks has the following areas:

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

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

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

  The folder is located at 'C:\Documents and Settings\All Users\Application Data\Shared Space'.
- **Reset Containment** - Clears all data written by programs inside the container.
- **Watch Activity** - Open Comodo KillSwitch to identify unsafe processes and manage system activity.
- **Run Virtual Desktop** - Start the virtual desktop environment.
- **Containment Statistics Analyzer** - Detailed information about the processes running on your computer. Processes are split into contained and non-contained processes.

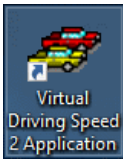
You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See '**Password Protection**' for more details."

4.1. Run an Application in the Container

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

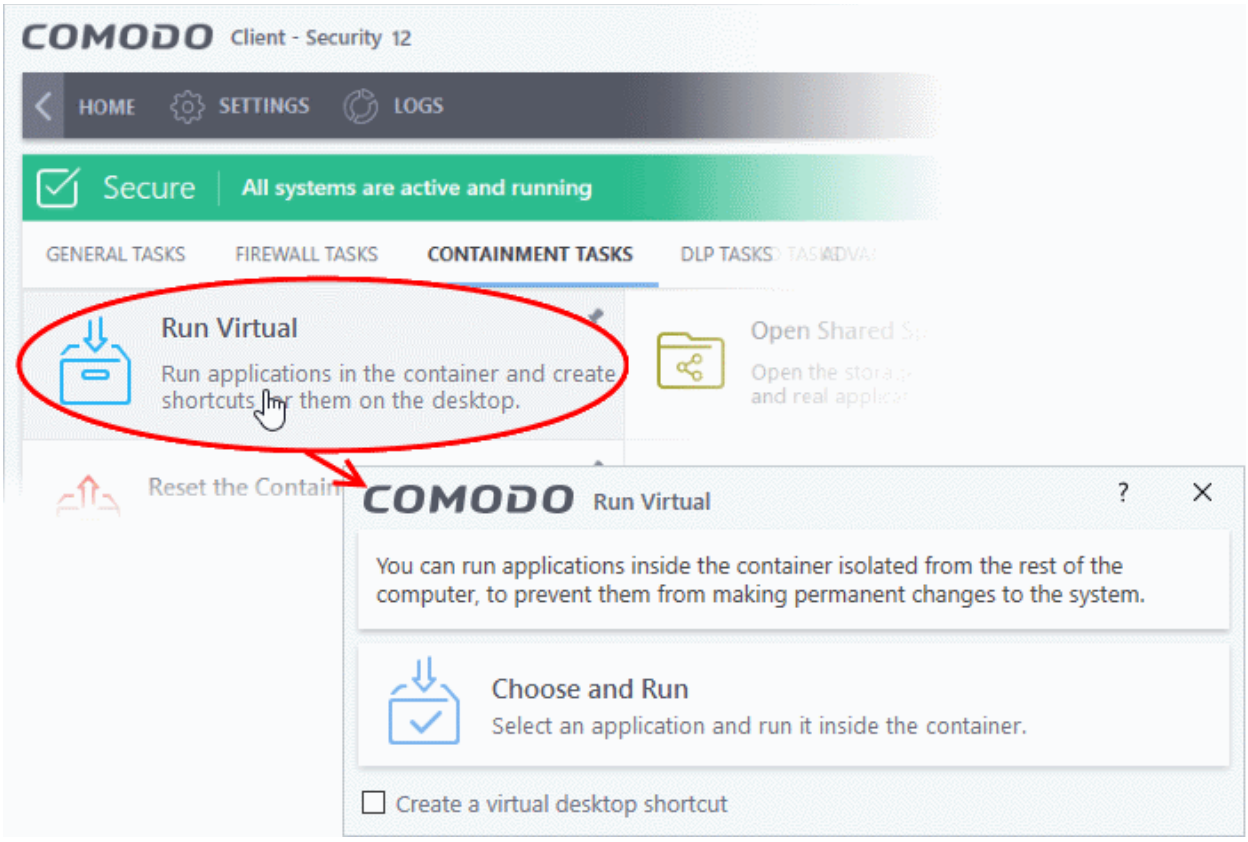
This method above will run the application in the container one-time only. On subsequent executions it will not run in the container. You need to create an **auto-containment rule** if you want it to always run in the container.

You can also create desktop shortcuts to always launch an application in the container:

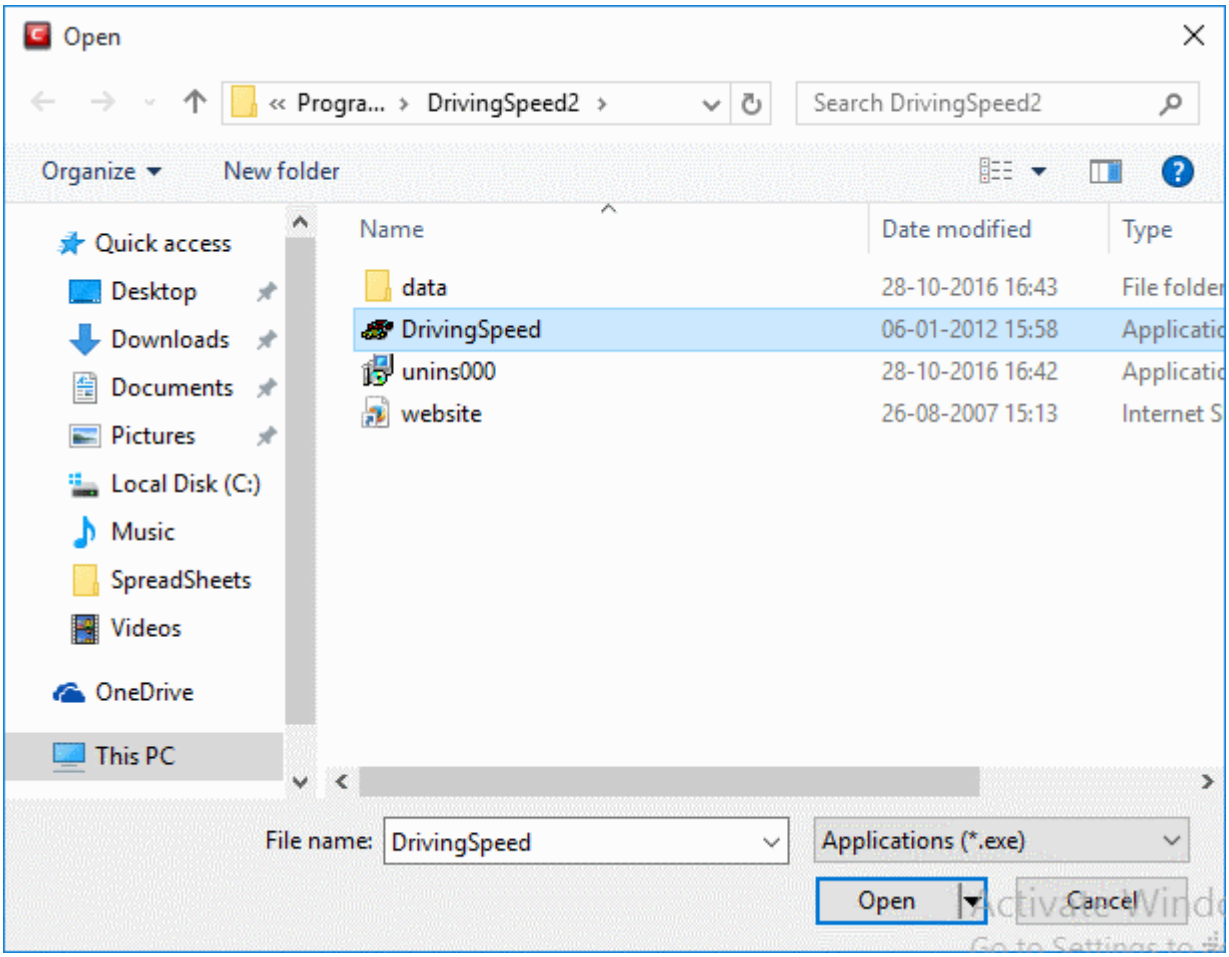


Run an application in the Container

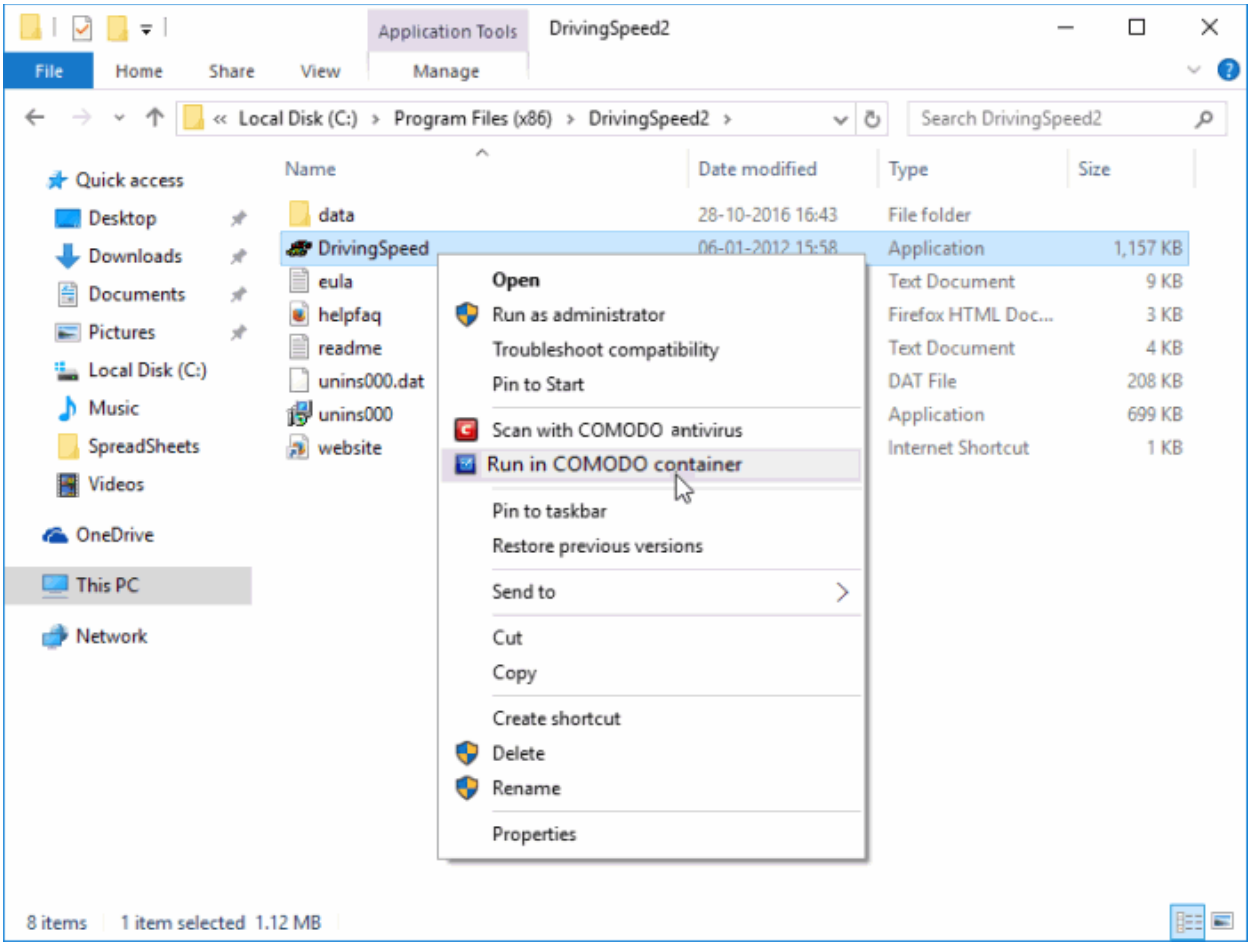
- Click 'Tasks'> 'Containment Tasks'
- Click 'Run Virtual':



- Click 'Choose and Run', browse to your application then click 'Open'.
- The contained application will have a green border around it. Enable 'Create a virtual desktop shortcut' if you plan to run the application in the container in future.



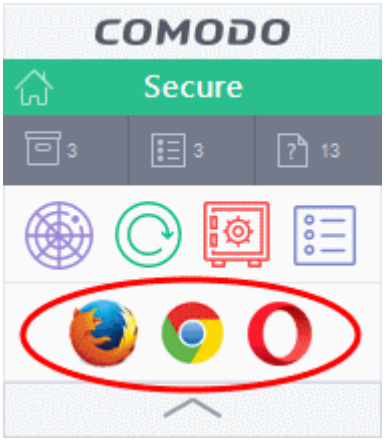
You can also run an applications in the container from the right-click menu:



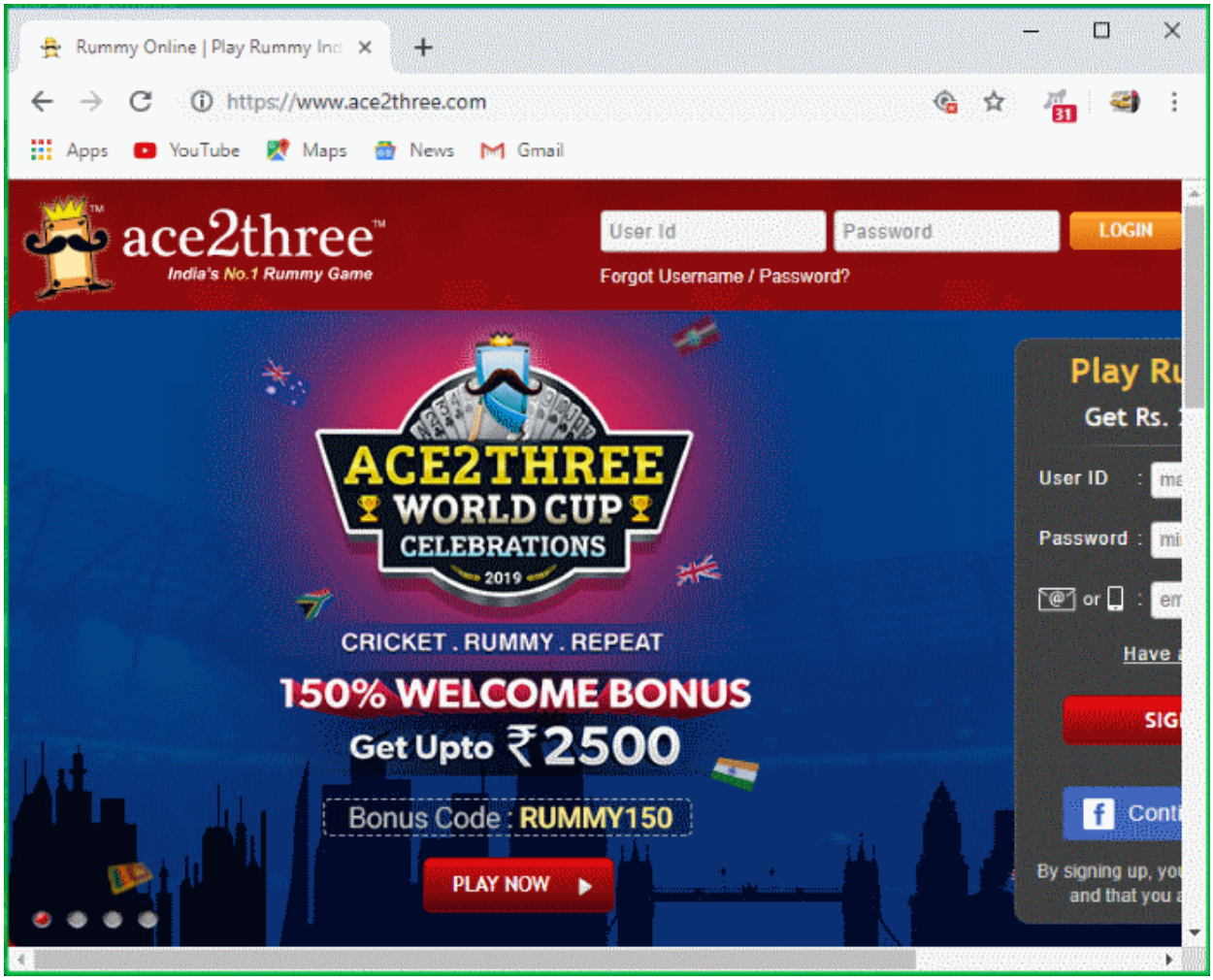
- Choose 'Run in Comodo container' from the context sensitive menu

Run browsers in the container

The CCS widget contains shortcuts to run your browsers in the container:



- The green border indicates that the browser is in the container:



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

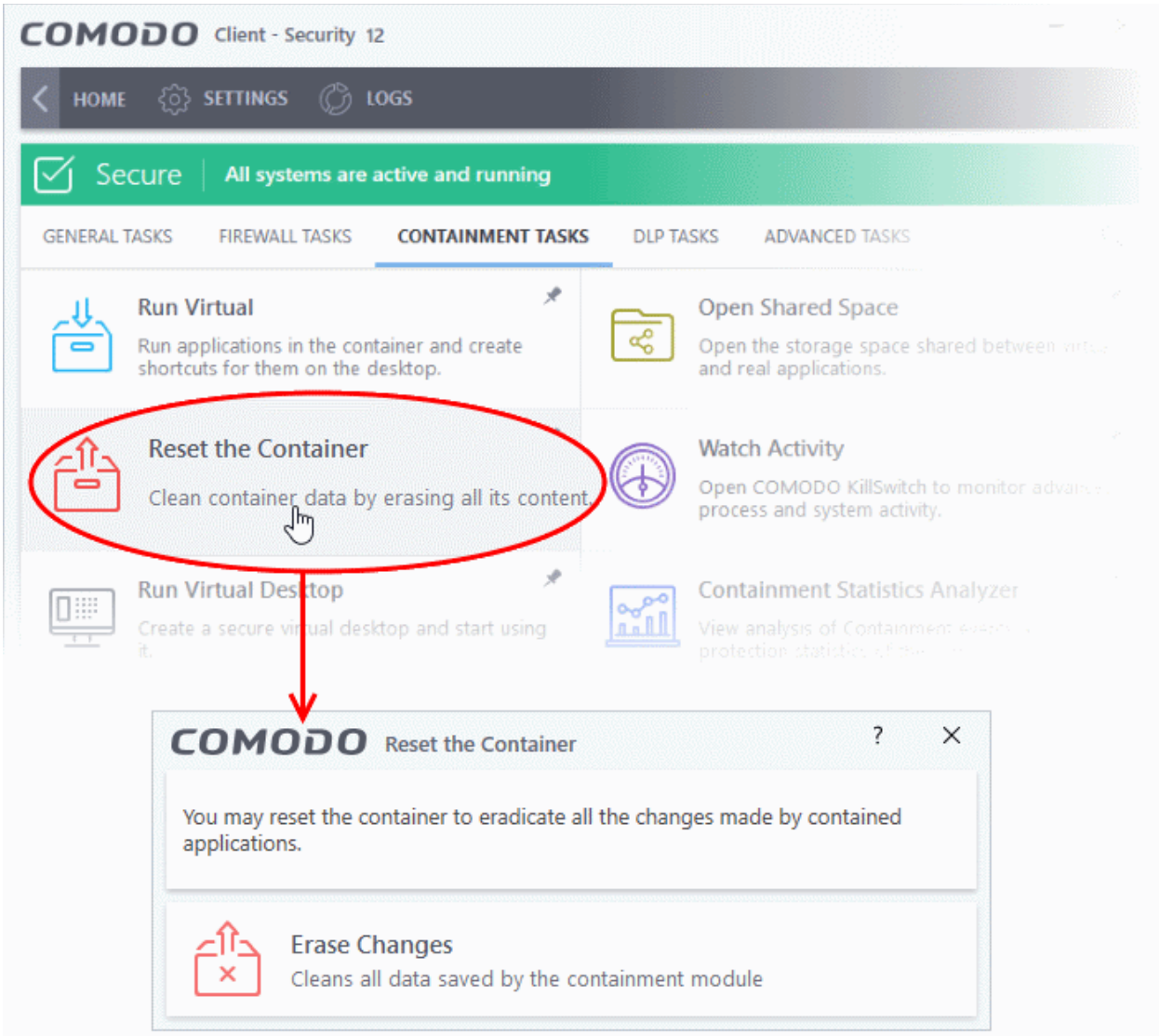
Note. You may see an error if an app on the host tries to update itself at the same time as that app is updating itself in the container. This is a classic Windows sharing violation which is shown when an app attempts to write to a file that is already in use. Please shut down the contained version of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

4.2. Reset the Container

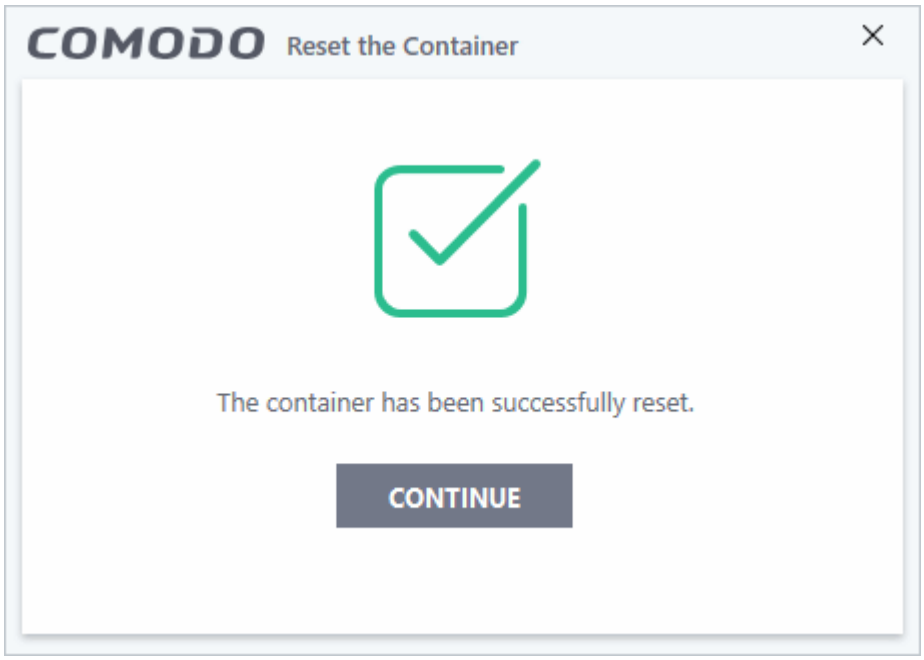
- Click 'Tasks' > 'Containment Tasks' > 'Reset the Container'
- Programs in the container write all data and system changes to a virtual file system. This means the program cannot harm your computer or sensitive data.
- Files saved in the container could contain malware downloaded from websites, or private data in your browsing history.
- Periodically resetting the container will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time, then a reset will also help the container operate more smoothly.
- The 'Reset the Container' option lets you delete all items saved in the container.

Clear the container

- Click 'Tasks' > 'Containment Tasks'
- Click 'Reset the Container'
- Click 'Erase Changes':



The contents in the container will be deleted immediately.



- Click 'Continue' to close the dialog.

4.3. Identify and Kill Unsafe Running Processes

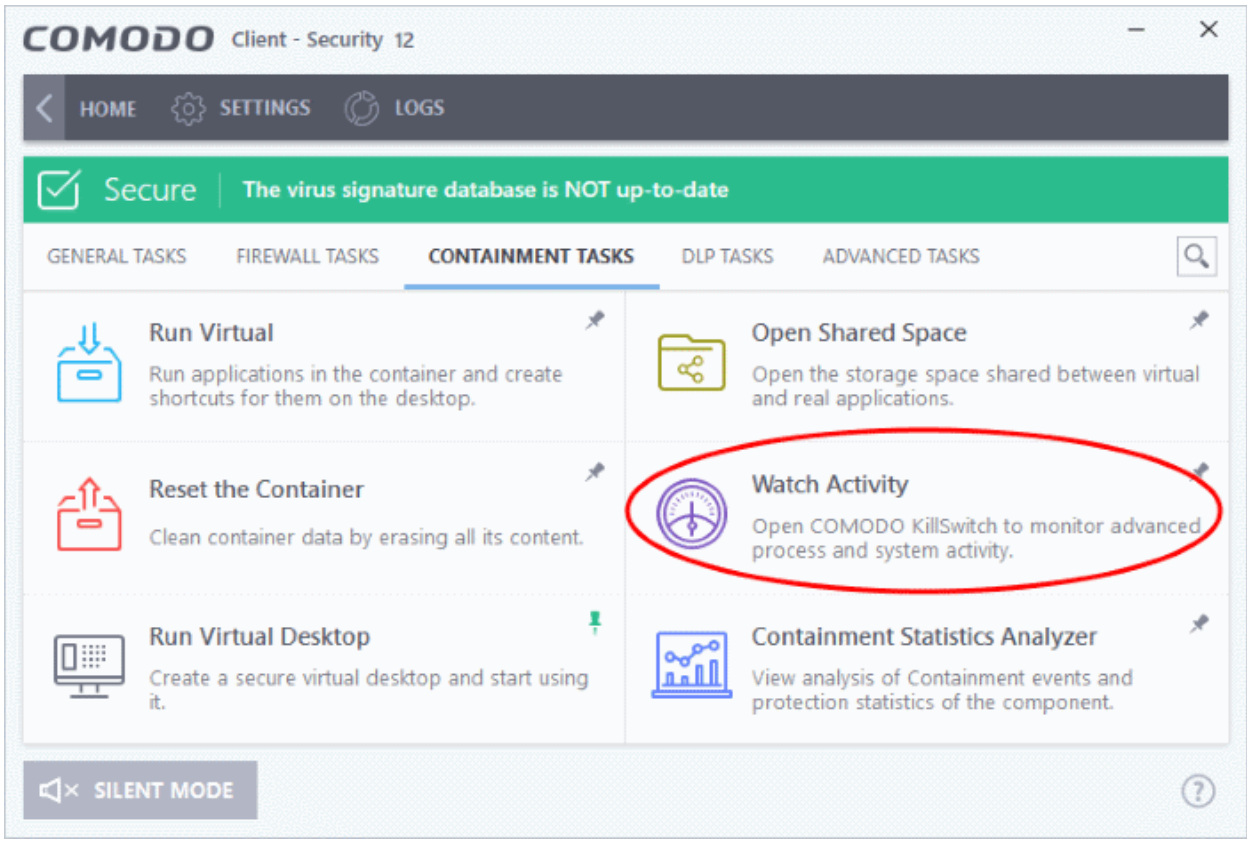
- Click 'Tasks' > 'Containment Tasks' > 'Watch Activity'

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

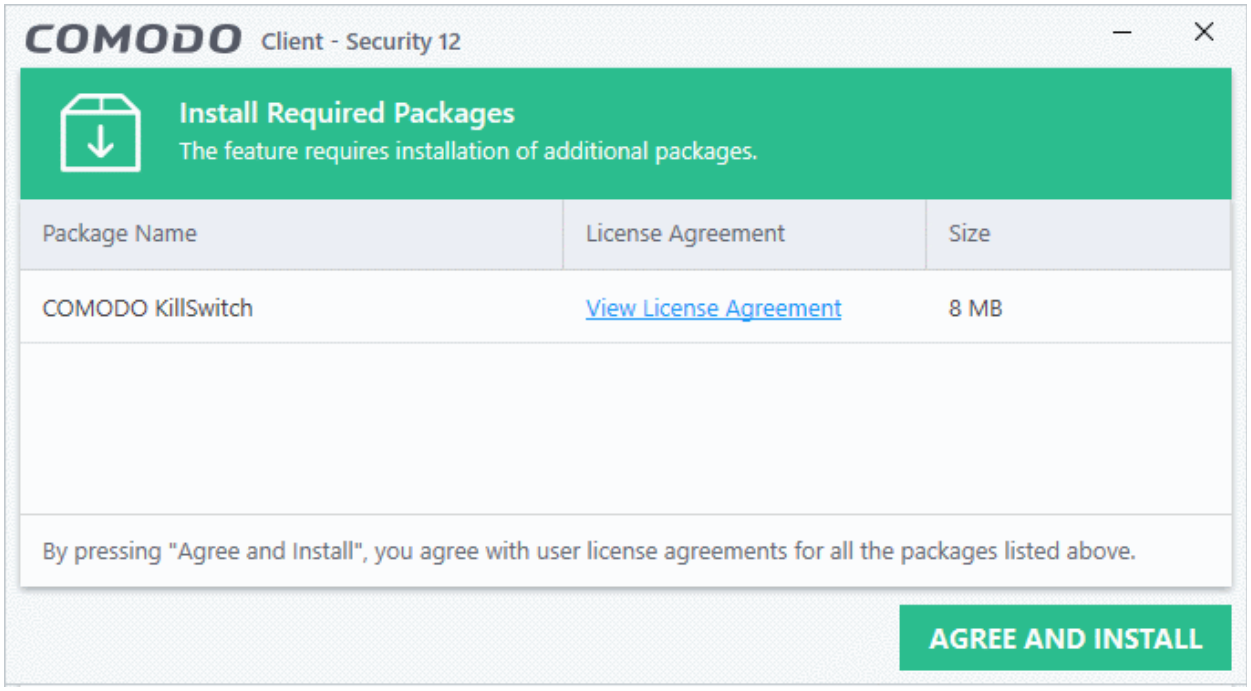
KillSwitch can even show processes that were invisible or very deeply hidden. You can identify all unsafe processes with a single click then quickly shut them down. You can also trace back to the software that generated the process.

Open KillSwitch

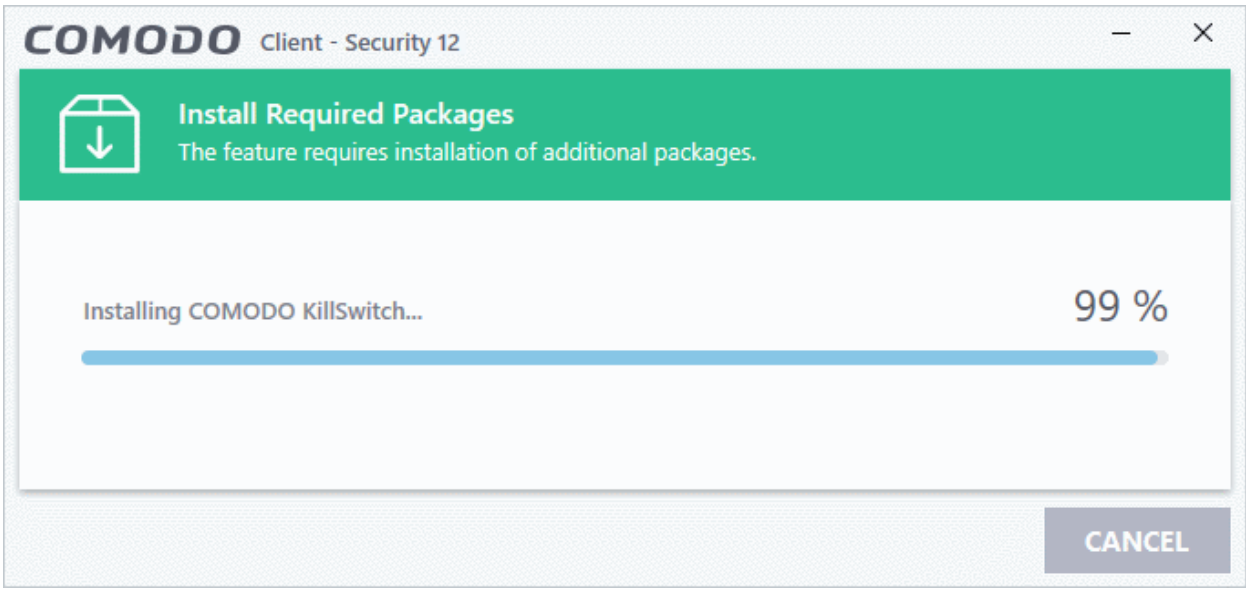
- Click 'Tasks' > 'Containment Tasks'
- Click the 'Watch Activity' tile



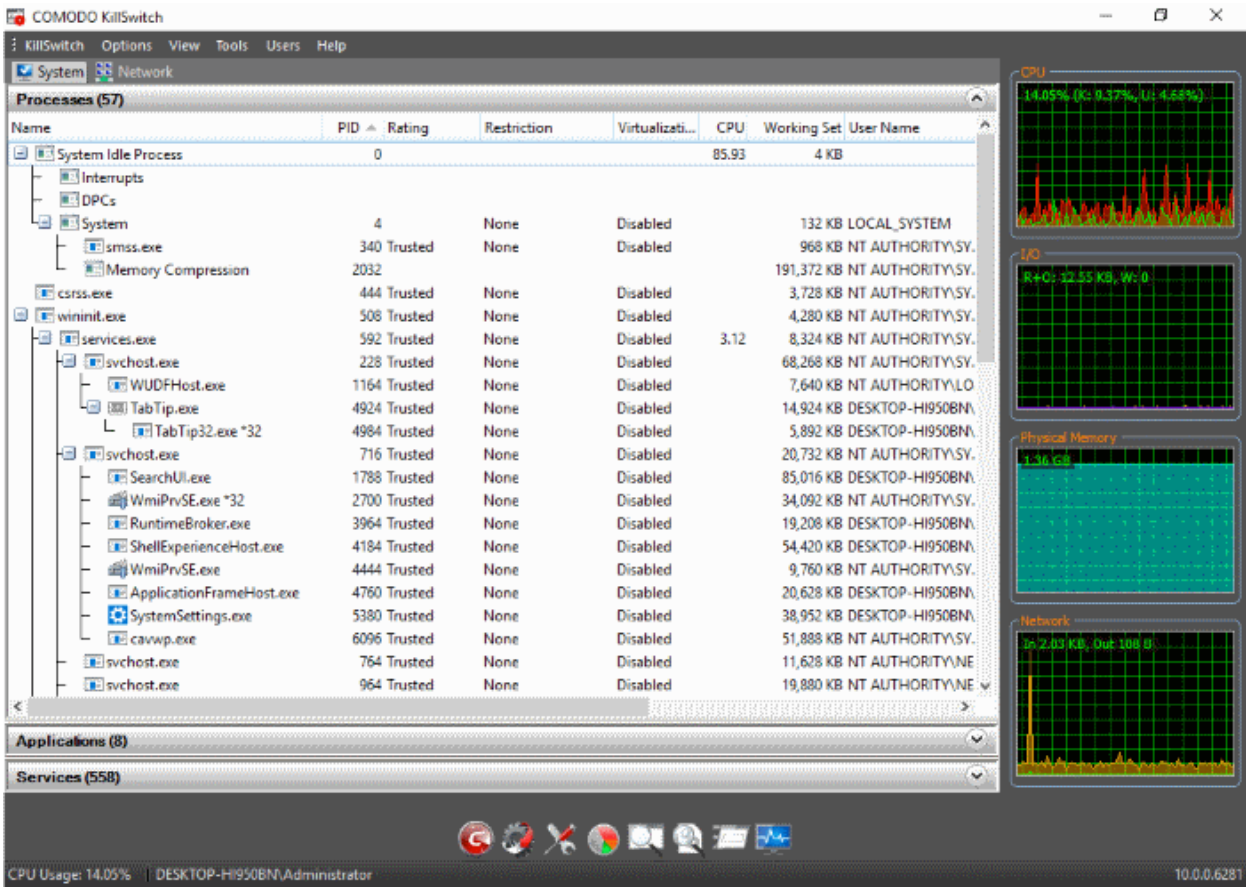
- If Comodo KillSwitch is already installed in your computer, clicking 'Watch Activity' will open the application. If not, CCS will download and install KillSwitch.



- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.



- KillSwitch will open when the installation is over:



- See the KillSwitch guide for help to use the product - **http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html**.

4.4. Open Shared Space

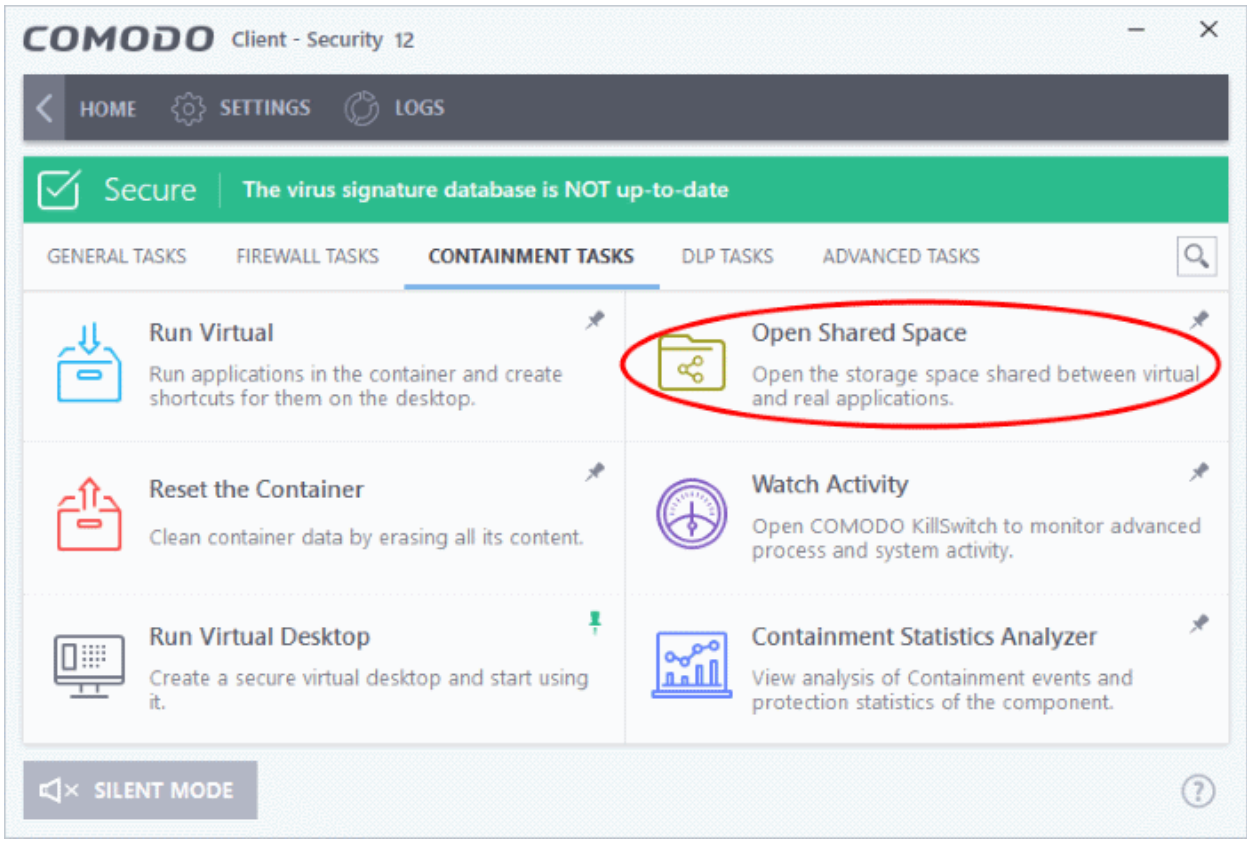
- Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space'
- Applications in the container are not allowed to write to your local drive for security reasons. Instead, they

write all data, and save all files, to a special folder called 'Shared Space'.

- Files in shared space can also be accessed by non-contained applications (those running as normal on your computer).
- If you want to access files in the container from your local system, then you should download them to shared space.
- The default location of shared space is 'C:/Program Data/Shared Space'

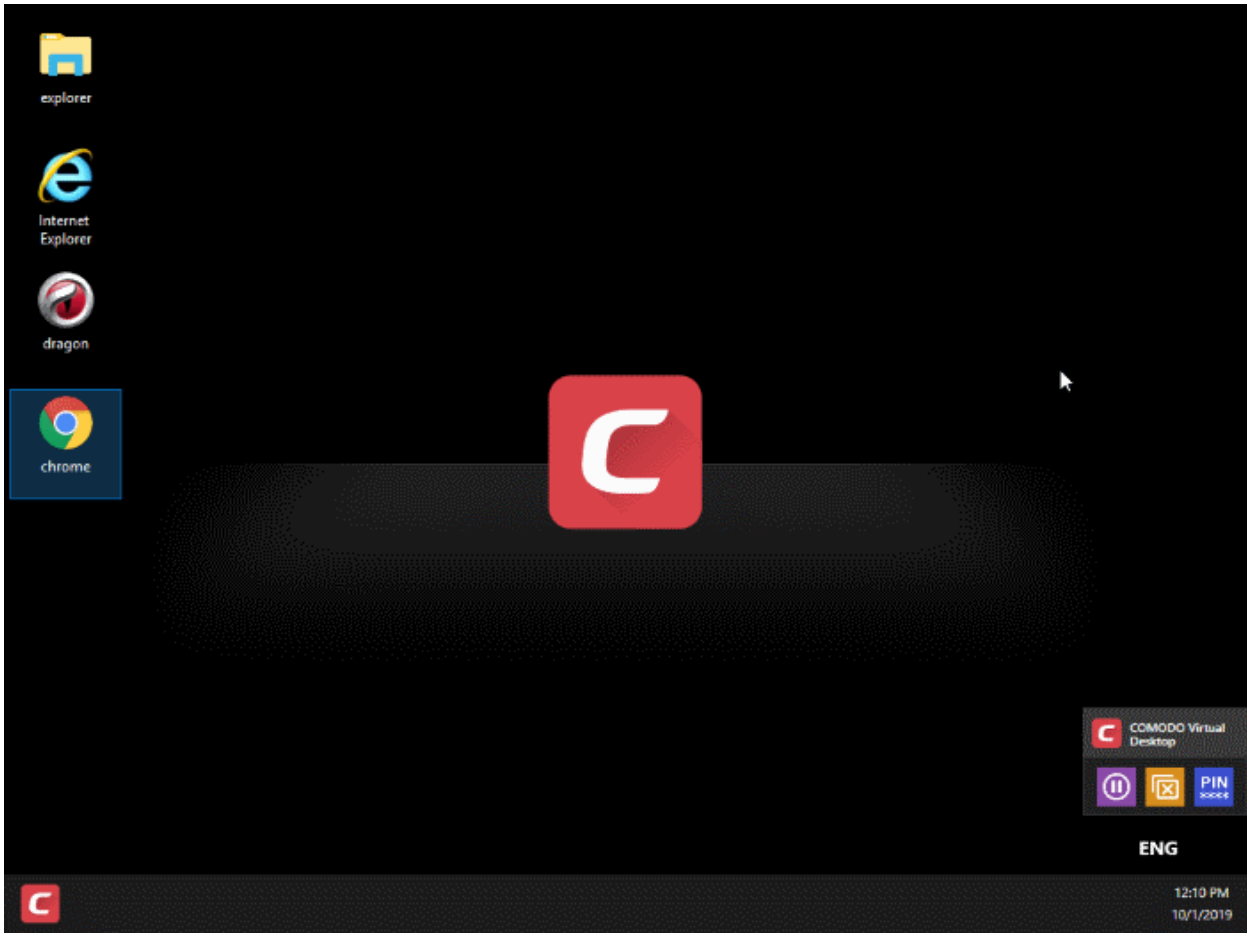
Open shared space

- Click 'Tasks' > 'Containment Tasks' > 'Open Shared Space':



4.5. The Virtual Desktop

- Go to 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- The virtual desktop is a sandbox environment in which you can run programs and browse the internet without fear those activities will damage your computer.
- Applications in the virtual desktop are isolated from the rest of your computer, write to a virtual file system, and cannot access your personal data.
- This makes it ideal for risk-free internet surfing and for testing out beta/unstable software.



Virtual Desktop at a glance:

- The virtual desktop can run any program that you normally run in Windows. It is ideal for running untested, unknown and beta software. You can also use it to visit websites that you are not sure about.
- Any changes made to files and settings in the virtual desktop will not affect the originals on your host system. Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Use the 'Shared Space' folder to save any files you want to access from Windows. This folder is the only place that the virtual desktop can write to on the host file system.
- You can also configure virtual desktop to access removable storage devices like USB sticks and external hard disk drives to store data from it.
- The virtual keyboard lets you securely enter confidential passwords without fear of key-logging software.
- The virtual desktop is also ideal for public computers such as those in a library or classroom. Any actions taken by users cannot damage the host computer. The virtual desktop can be reset and all changes cleared at the end of every session.
- The virtual desktop can be password-protected and configured to start automatically at user logon.
- You can create shortcuts on the host desktop to launch applications in the virtual environment.
- You can white-label the virtual desktop with your own company logos in the Endpoint Manager console.
    - See **https://community.itarian.com/help/topic-459-1-1005-14932-Communication-Client-and-Comodo-Client---Security-Application-UI-Settings.html** for more on this

See the following sections for more help:

- **Start the Virtual Desktop**
- **The Main Interface**

- **Run Browsers inside Virtual Desktop**
- **Open Files and Run Applications inside Virtual Desktop**
- **Pause and Resume the Virtual Desktop**
- **Close the Virtual Desktop**

4.5.1. Start the Virtual Desktop

- Click 'Tasks' on the home screen
- Click 'Containment Tasks' > 'Run Virtual Desktop'

You can start the virtual desktop from the home-screen shortcut, from the widget, or from the 'Containment Tasks' screen. You can also configure the virtual desktop to start automatically after you login to Windows.

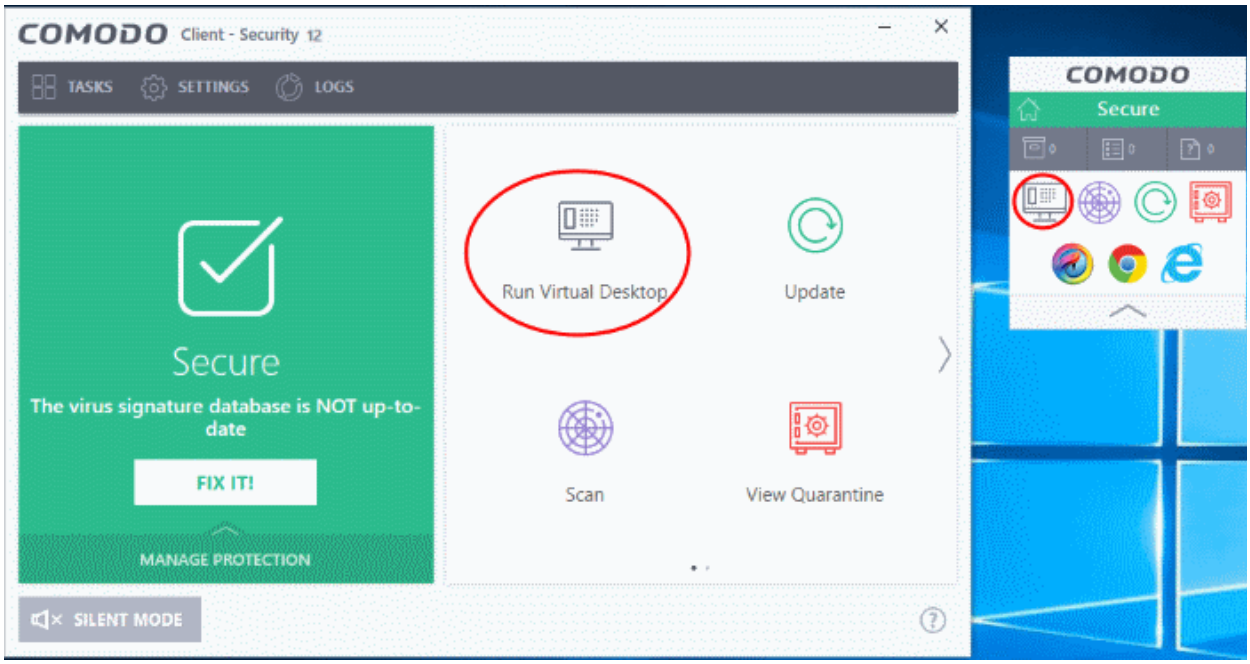
Note. If CCS is in Virtual Desktop mode, you can start the application by simply clicking the desktop shortcut.

See the following sections for more help:

- **Open the virtual desktop from CSS or the widget**
- **Launch the virtual desktop at user logon**
- **Start the virtual desktop from the containment tasks screen**

Start the virtual desktop from CCS or the widget

- Click the virtual desktop icon on the CCS home screen, or on the CCS widget:



Note: The home screen and widget shortcuts are only available if you have added the 'Virtual Desktop' shortcut:

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

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

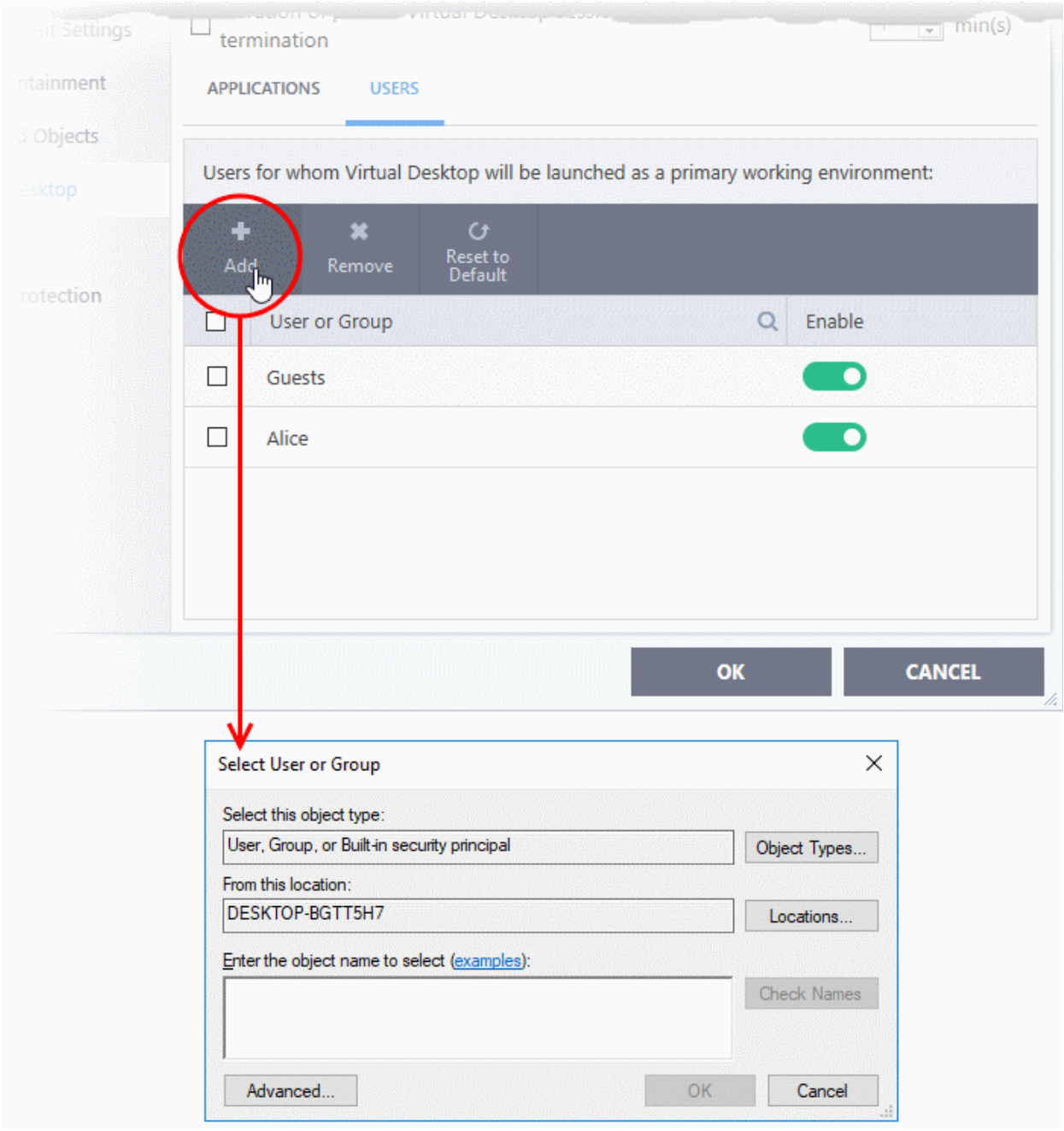
The virtual desktop opens at the **session selection screen**.

Launch the virtual desktop at user logon

- You can configure the virtual desktop to start automatically whenever certain users login to Windows.
- This means the virtual desktop becomes the default operating environment for those users.

Add users

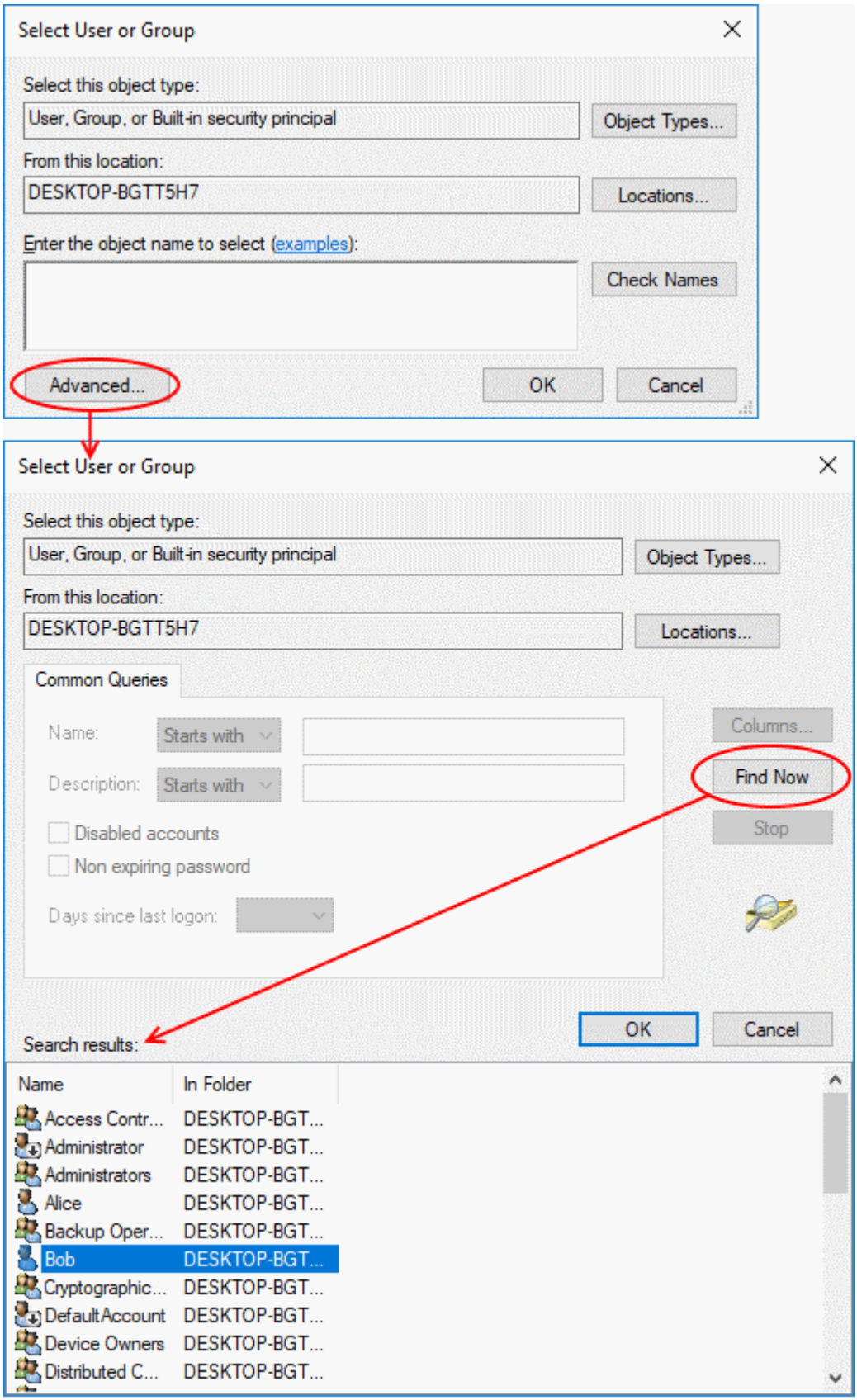
- Click 'Settings' on the home screen
- Click 'Containment ' > 'Virtual Desktop'
- Select the 'Users' tab
- Click 'Add'



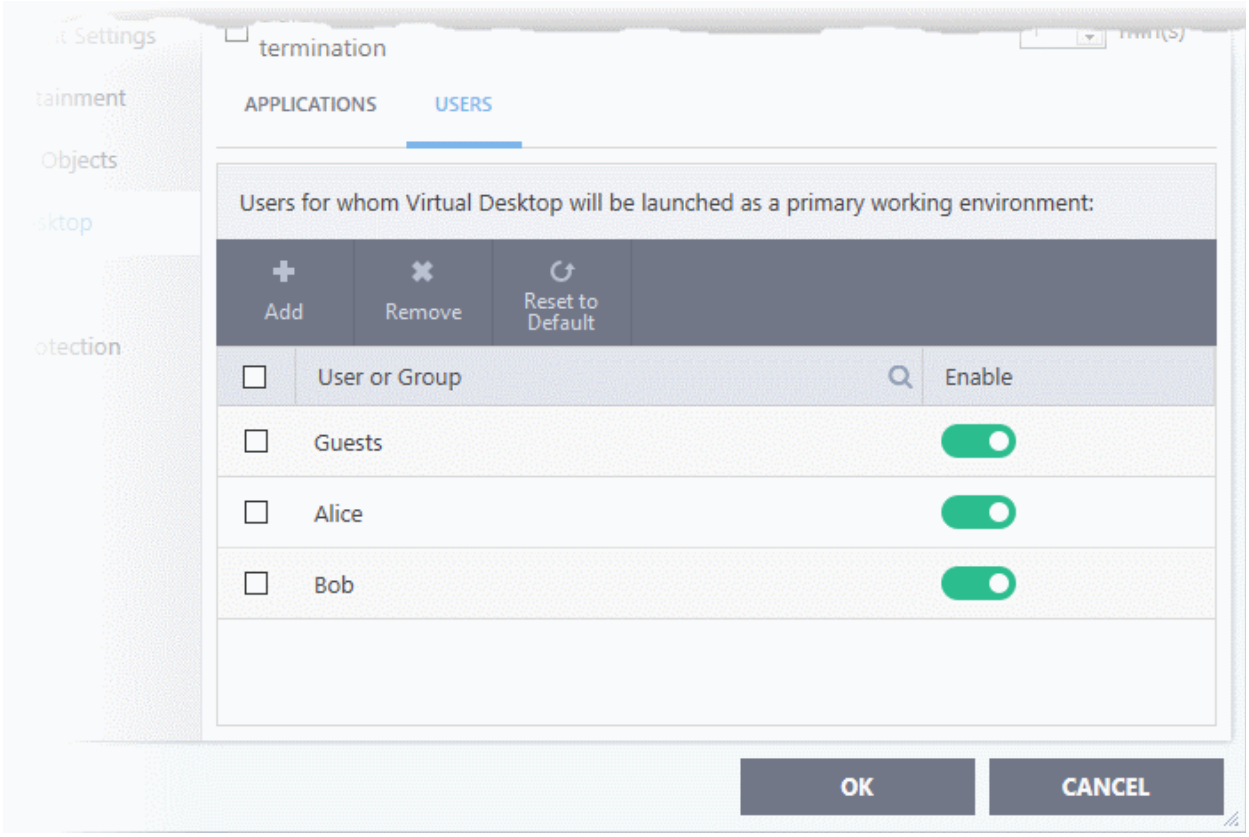
- Select the users or groups to whom you want the rule to apply.
    - Type the names of users or groups in the format <domain name>\<user/group name> or

<user/group name>@<domain name>.

- Alternatively, click 'Advanced' then 'Find Now' to locate specific users/ groups.
- Click 'OK' to confirm.



The user / user group will be added to the list.

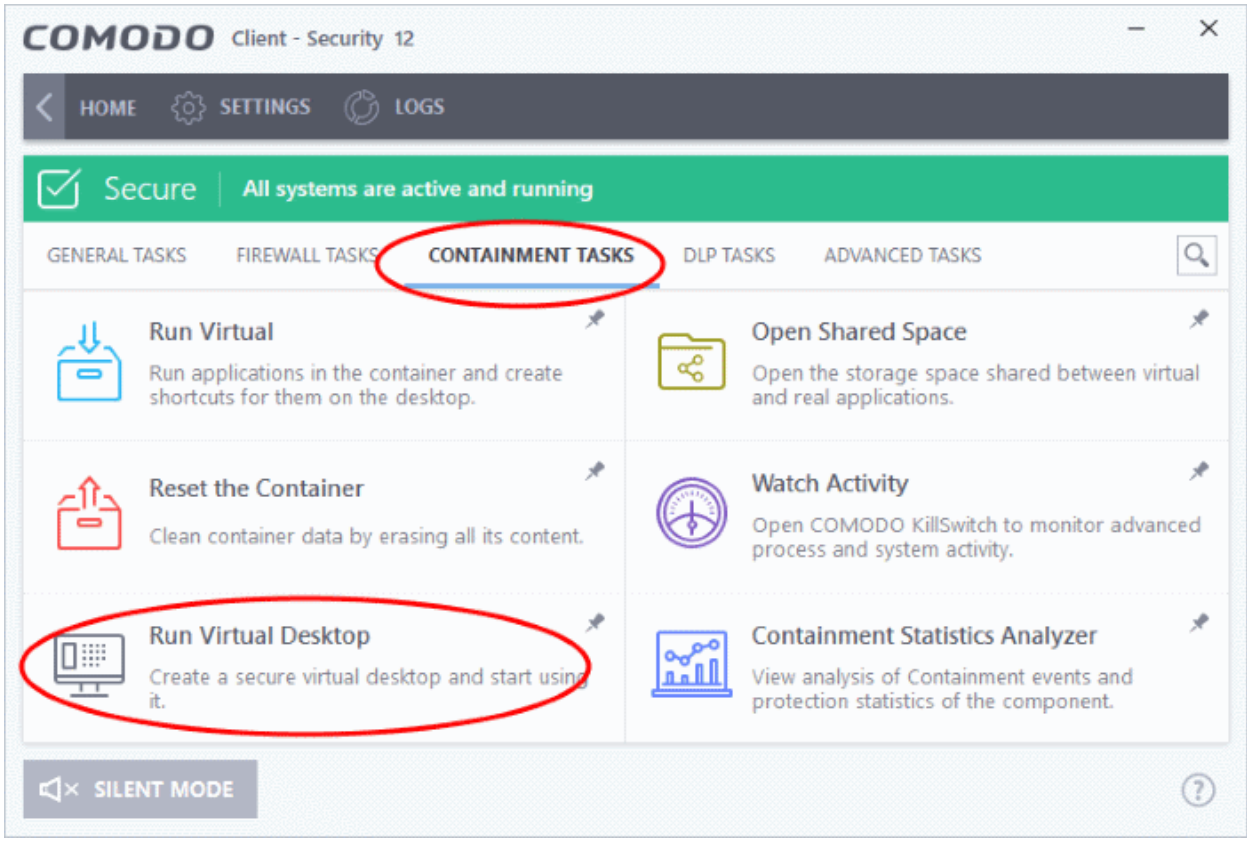


- Repeat the process to add more users.
- Click 'OK' to save your settings
- Click 'OK' in the 'Advanced Settings' dialog for your changes to take effect
  - See '**Virtual Desktop Settings**' if you need more help with this

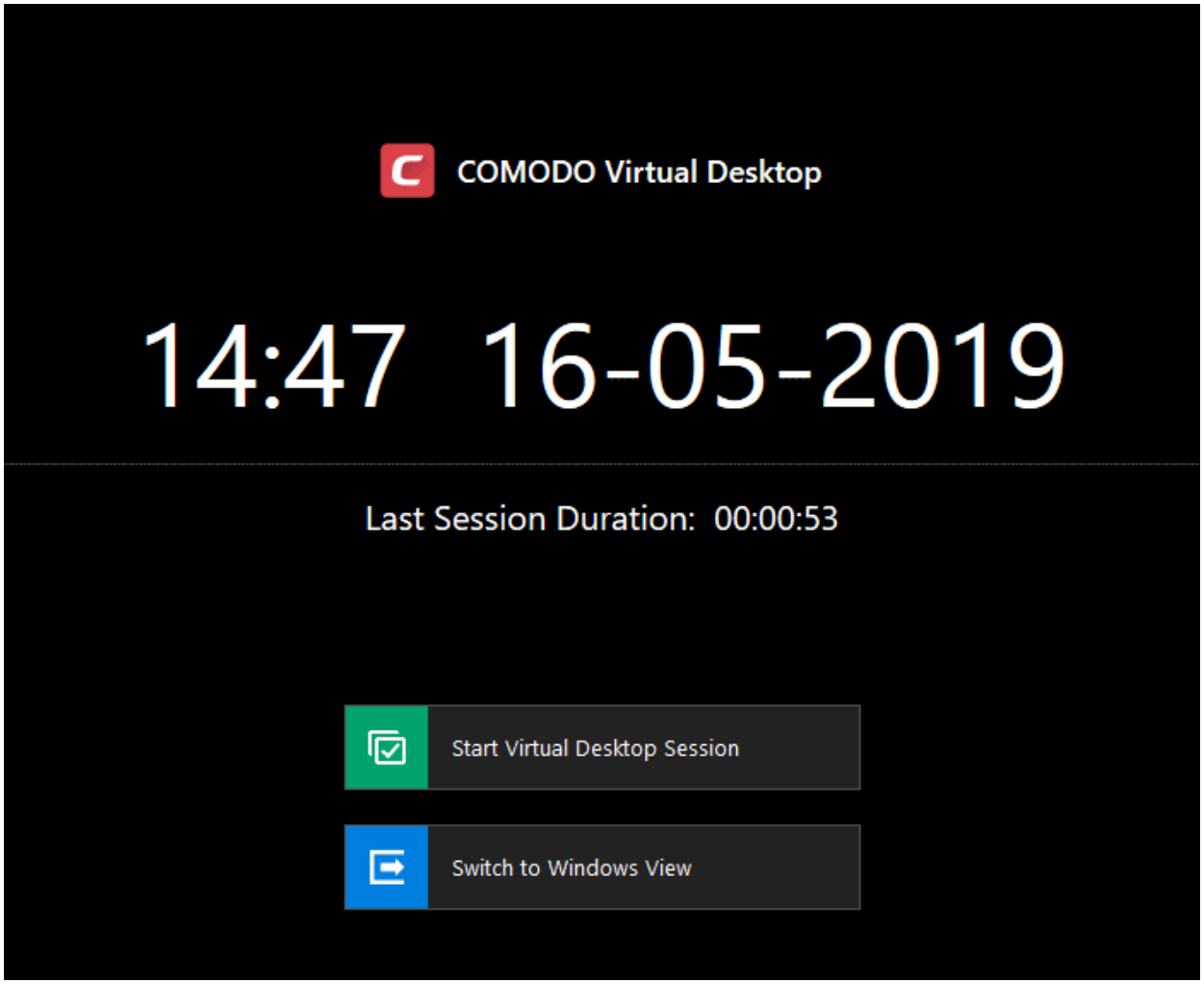
The virtual desktop opens at the **session selection screen** when the selected users log-in.

Start the virtual desktop from the containment tasks screen

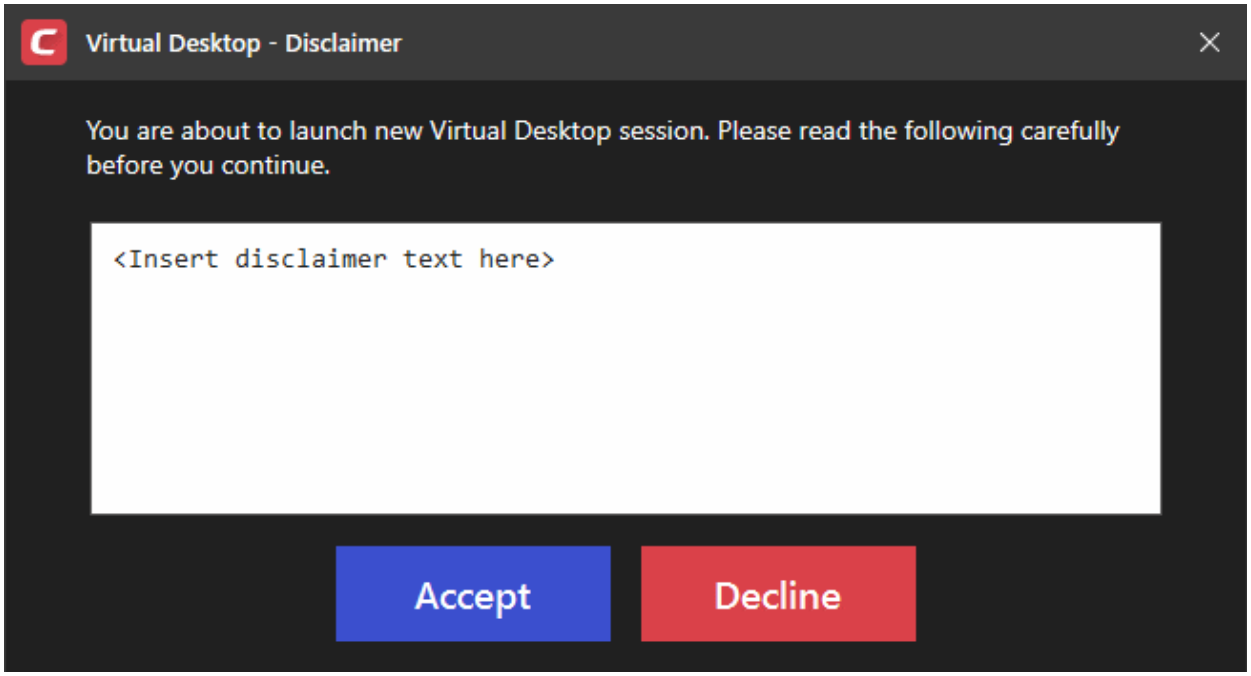
- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'



The virtual desktop opens at the **session selection screen**.



- Click the 'Start Virtual Desktop Session' button
- Click 'Accept' at the disclaimer screen to open the virtual desktop.

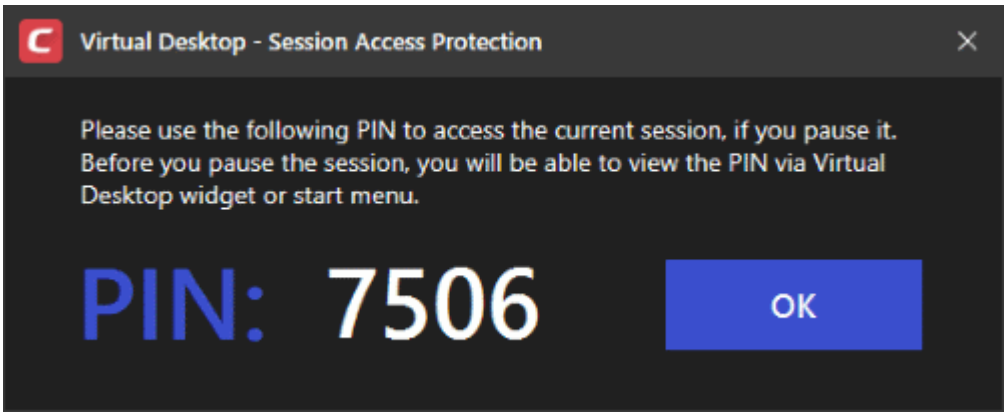


Note: This screen is only relevant for customers who white-label the interface. It can be safely ignored by most customers and end-users.

If you do want to white-label the interface, you can configure the disclaimer message at 'Settings' > 'Containment' > 'Virtual Desktop'. You can also disable the disclaimer entirely from there.

See '**Show disclaimer upon Virtual Desktop startup**' to view help with this. Details on how to white-label CCS are in a wiki article **here**.

- You will see a four digit access code If session protection is enabled:

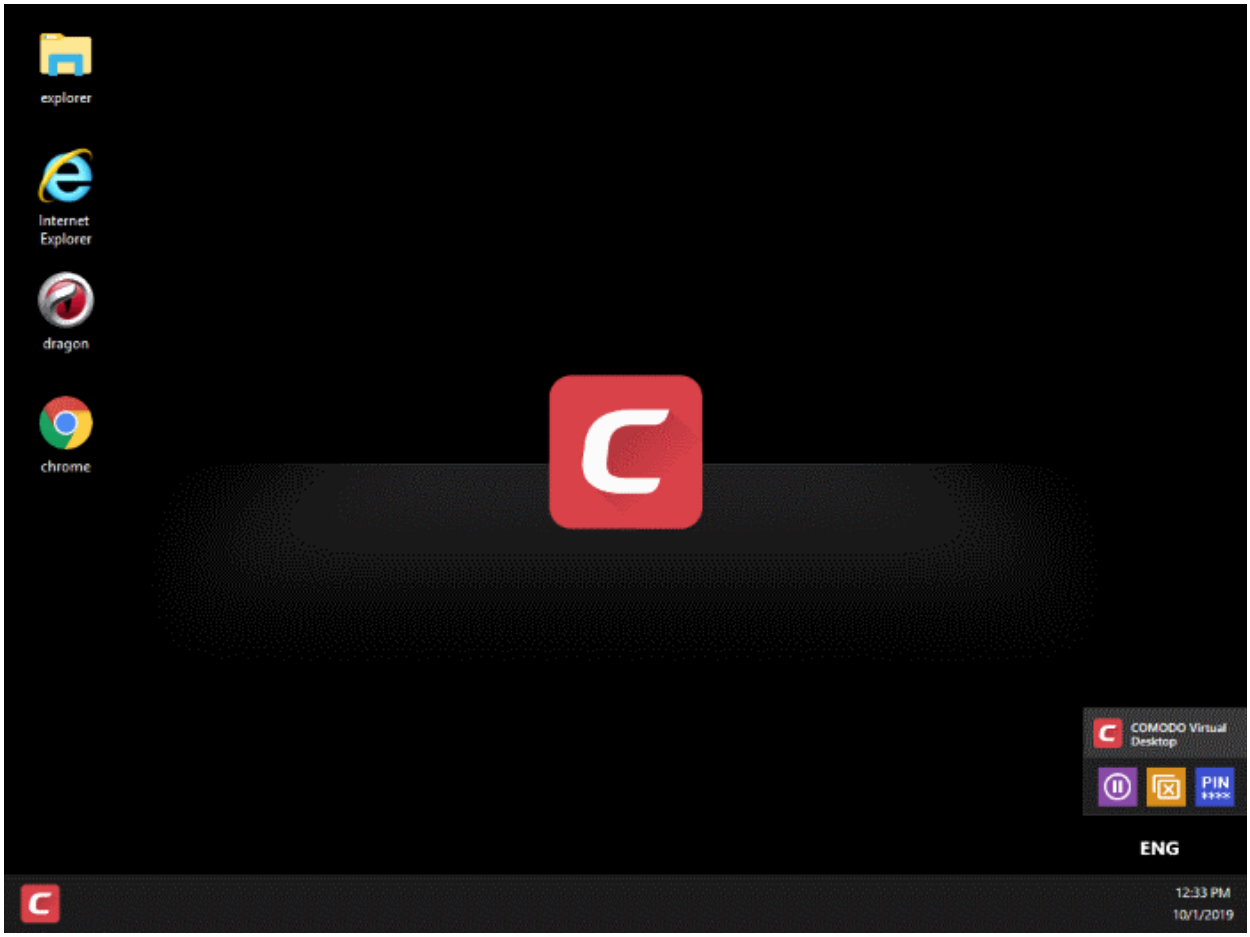


- This feature lets you suspend a virtual desktop session and resume it later without losing any data. The PIN is required to unlock the suspended session.
- Please make a note of the PIN number. See **Pause and Resume the Virtual Desktop** for more details
- Tip: You can view the PIN at any time by clicking the 'Show PIN' icon

in the virtual desktop start menu

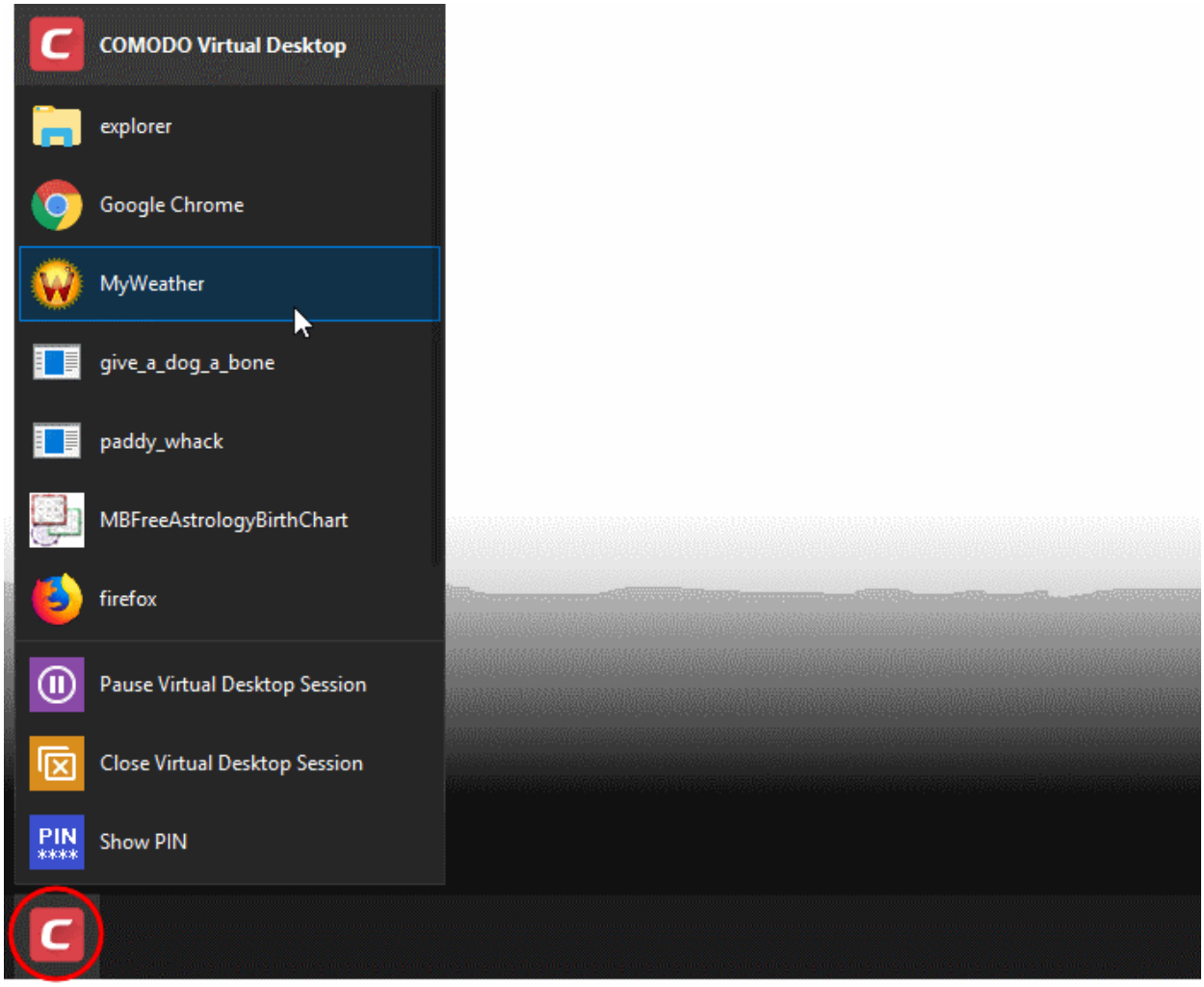
4.5.2. The Main Interface

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- Click the 'Start Virtual Desktop Session' button
- The start menu has application shortcuts, and also lets you pause and close the virtual desktop.
- The start menu has application shortcuts, and also lets you pause and close the virtual desktop.
    - You can add your own application shortcuts and start menu items at 'Settings' > 'Containment' > 'Virtual Desktop'.
- The tool box at bottom-right also has controls to pause and close the virtual desktop.



The 'Start' menu

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

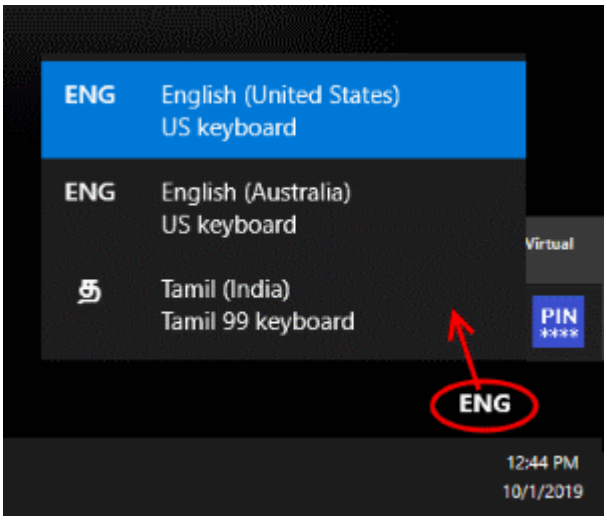


The menu has the following options:

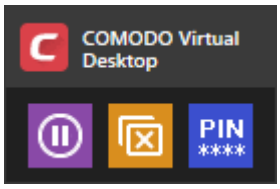
- **Browsers and other applications** - The start menu contains shortcuts for Windows Explorer and the default browser on the endpoint. You can also add shortcuts for other browsers and applications at 'Settings' > 'Containment' > 'Virtual Desktop'. See **Add applications to virtual desktop** in **Virtual Desktop Settings** for more details.
  - Click an item to open it inside the virtual desktop.
- **Pause Virtual Desktop Session** - Temporarily close the virtual desktop. If PIN protection is enabled, you need the PIN to resume a paused session. See **Pause and Resume the Virtual Desktop** for more details.
- **Close the Virtual Desktop Session** - Exit the virtual desktop and return to Windows. If your virtual desktop is password protected, you have to enter the password to exit. See **Close the Virtual Desktop** for more details.
- **Show PIN** - Displayed only if PIN protection is enabled for the virtual desktop. Shows the code generated for the current session. This is required to resume a paused session. See **Pause and Resume the Virtual Desktop** for more details.

Tools and Taskbar

- **Keyboard language** - Click the language button ENG at bottom-right and select the language of your keyboard.



- Note 1 - This list only shows languages that are already enabled in Windows.
- Note 2 - You can use Windows 'On-Screen Keyboard' (OSK) as virtual keyboard in virtual desktop.
  - Enable OSK - Click the Windows 'Start' button > 'Settings' > 'Ease of Access' > 'Keyboard' > enable 'Use On-Screen Keyboard'.
  - The settings above are for Windows 10. The procedure may vary slightly for other Windows versions.
- **Tools Box** - The tools box at the bottom-right contains controls for pausing and closing the virtual desktop.



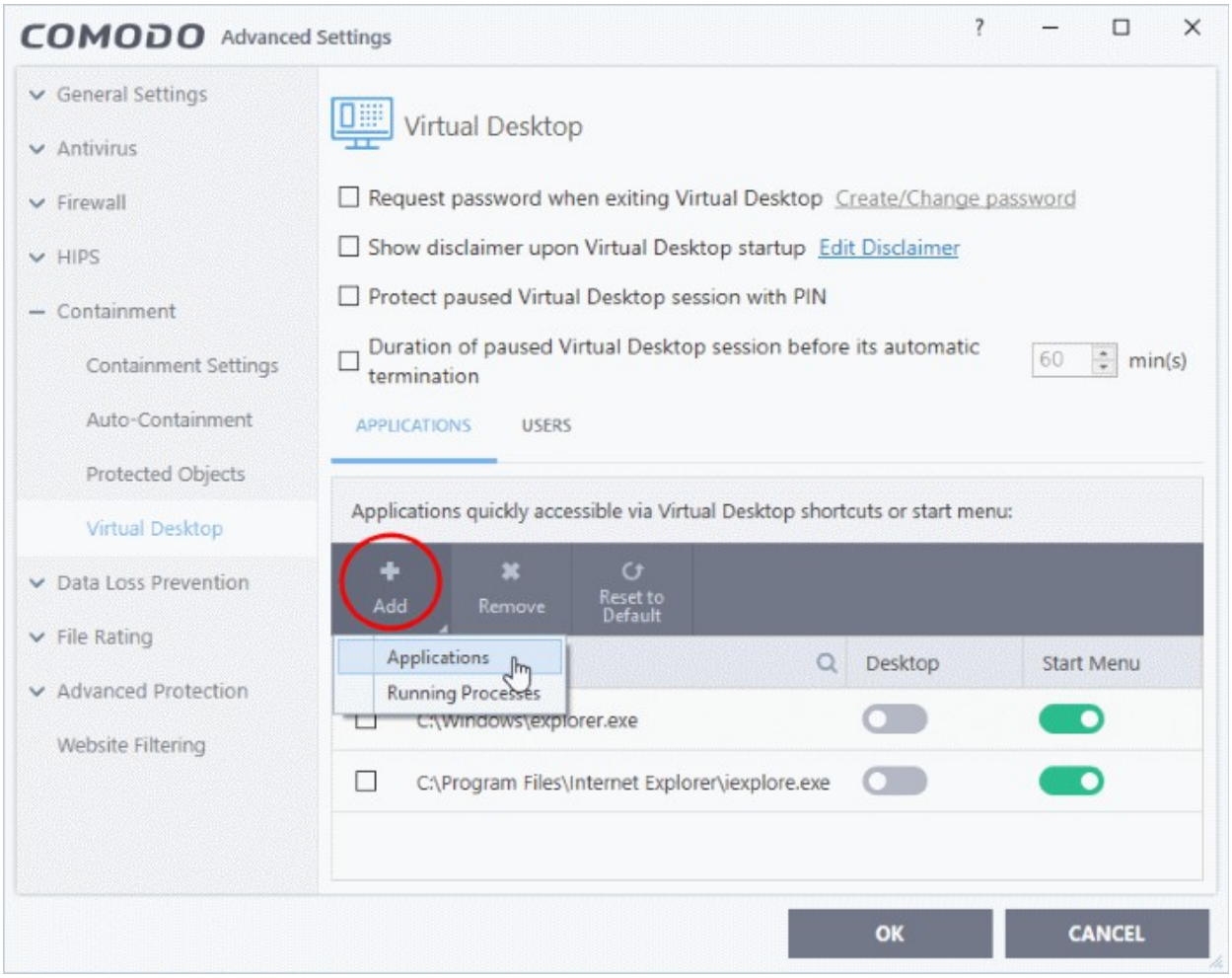
- - Pauses the virtual desktop session. If PIN protection is enabled, you need the PIN to resume a paused session. See **Pause and Resume the Virtual Desktop** for more details.
- - Closes the session.
- - Displayed only if PIN protection is enabled for virtual desktop. Shows the PIN number generated for the current session. This is required for you to resume a paused session. See **Pause and Resume the Virtual Desktop** for more details.

4.5.3. Run Browsers inside the Virtual Desktop

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- Click the 'Start Virtual Desktop Session' button
- The virtual desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer.
- Just by visiting them, malicious websites can install malware, rootkits and spyware on your computer.
- Surfing the internet from inside the virtual desktop removes this threat by preventing websites from installing applications on your real computer.
- Furthermore, the virtual keyboard lets you securely enter your user-names and passwords without fear of key-loggers recording your keystrokes.

Add browser shortcuts inside the virtual desktop

- The virtual desktop start menu contains a shortcut to your default browser.
- You can add shortcuts for other browsers as follows:
    - Click 'Settings' > 'Containment' > 'Virtual Desktop'
    - Click the 'Add' button in the applications section:



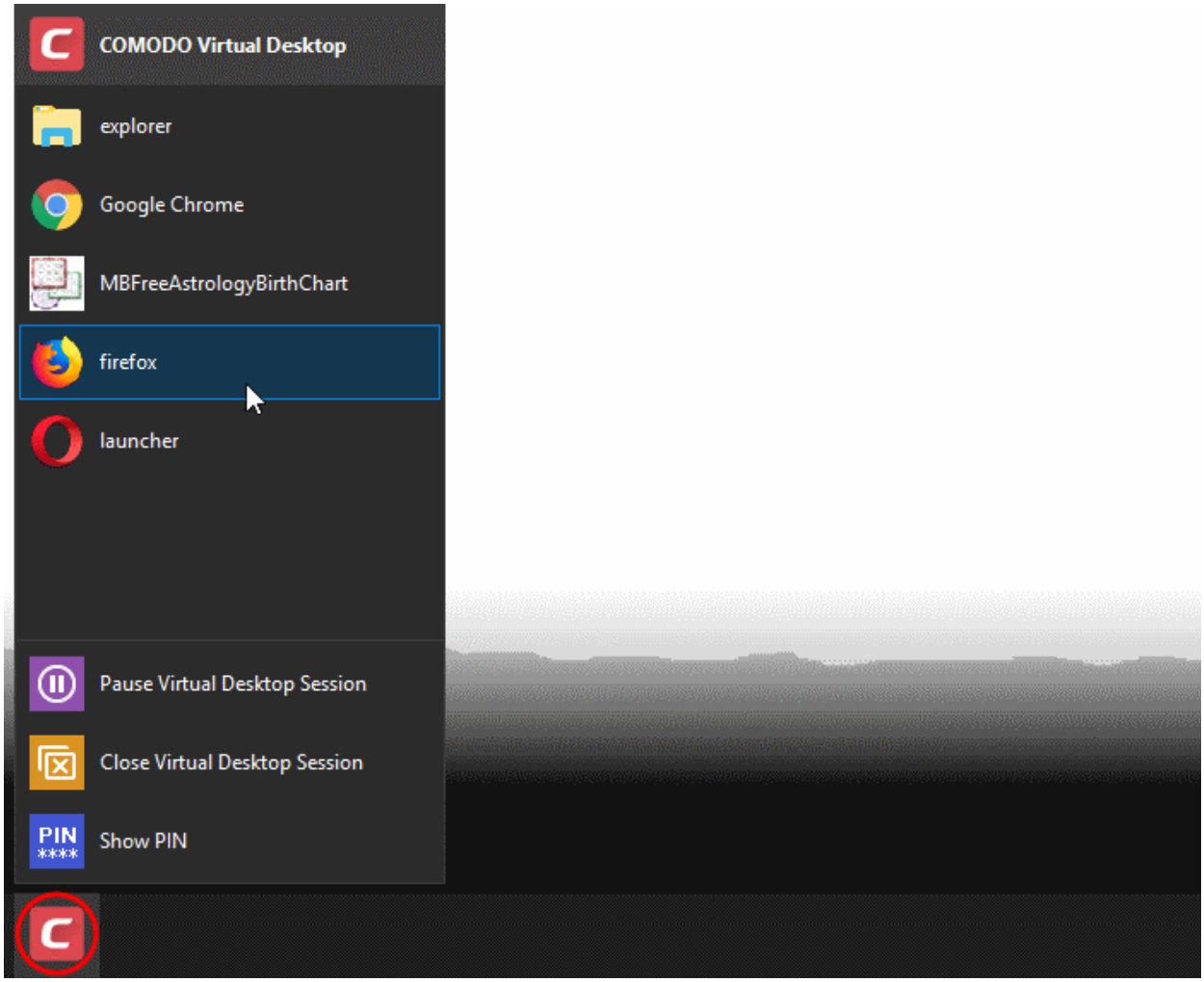
    - Add a browser as follows:
        - Click 'Add' > 'Applications' > locate the executable file of the browser > click 'OK'.

          OR
        - Start the browser on the host computer
        - Click 'Add' > 'Running Processes' > locate the browser process > click 'OK'.
    - Use the 'Desktop' and 'Start Menu' switches to enable/disable each type of shortcut.
    - Click 'OK' to save your settings
    - Click 'OK' in the 'Advanced Settings' dialog for your changes to take effect
    - See **Add applications to virtual desktop** in **Virtual Desktop Settings** if you need more help on this.

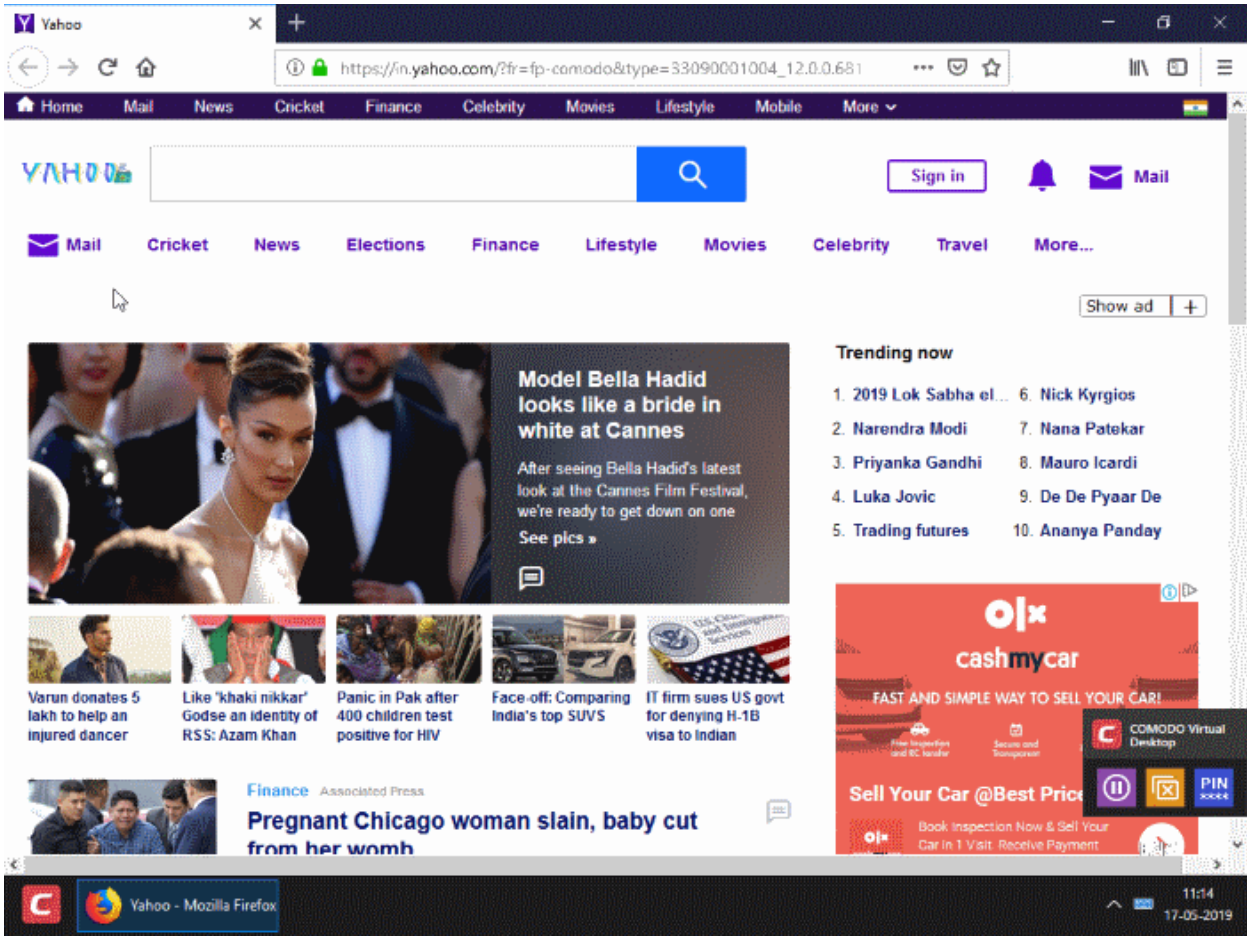
The shortcuts are now available inside the virtual desktop.

Run browsers inside virtual desktop

- Use the desktop shortcuts or start menu items of the browser that you want to run



The selected browser will open at its home page.



- Your browsing history and other internet activity are not stored on your computer when you close the session.

4.5.4. Open Files and Run Applications inside the Virtual Desktop

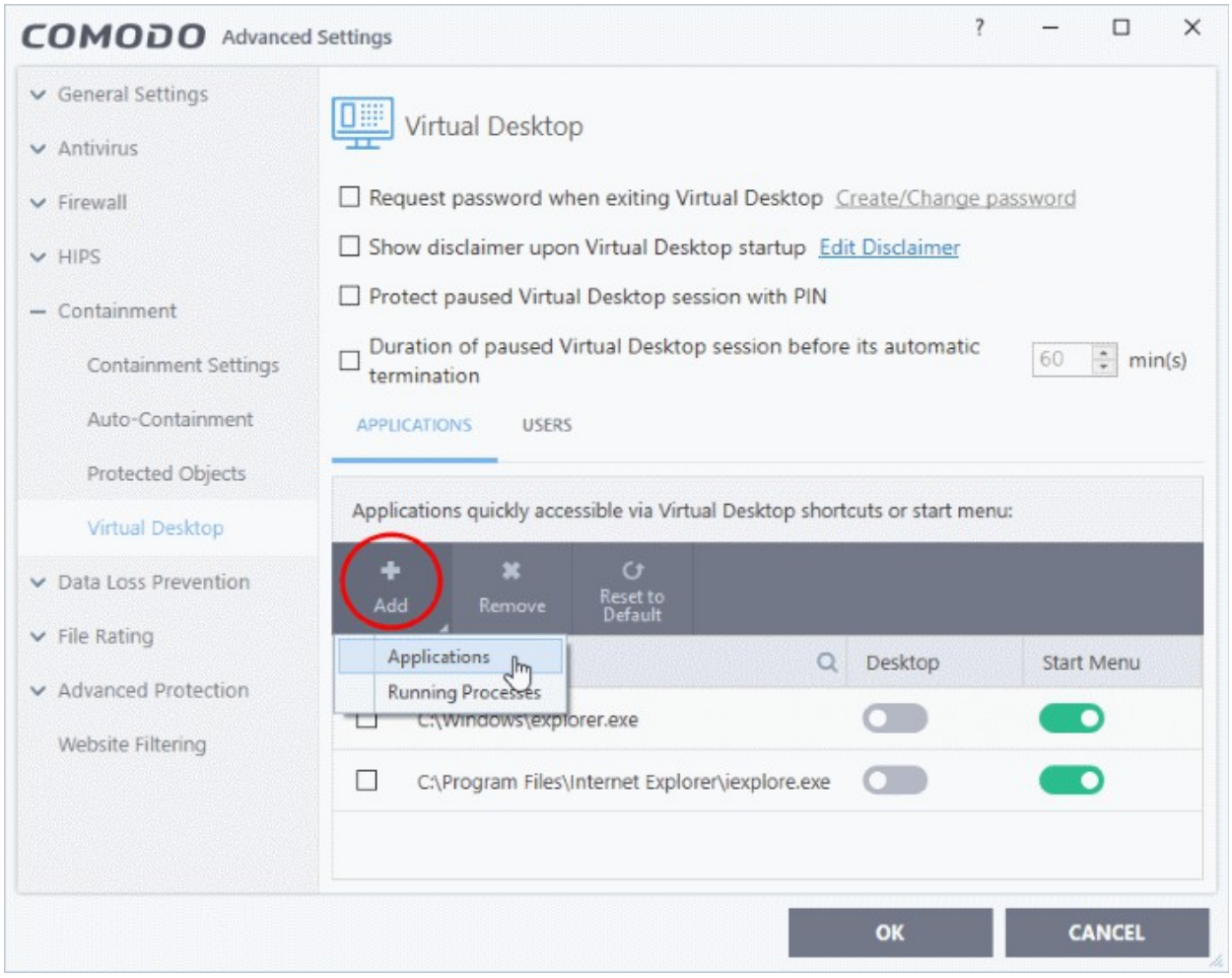
- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual Desktop'
- Click the 'Start Virtual Desktop Session' button

Use any of the following methods to run a local program or file in the virtual desktop:

- **Open applications/files from the desktop shortcuts and start menu items**
- **Navigate to the application/file**

Desktop shortcuts and start menu items

- The virtual desktop start menu contains shortcuts to Windows Explorer and your default web browser.
- You can create other shortcuts in the virtual desktop to open your favorite applications
  - Click 'Settings' > 'Containment' > 'Virtual Desktop'
  - Click the 'Add' button in the applications section:



- Add an application as follows:
  - Click 'Add' > 'Applications' > navigate to the file

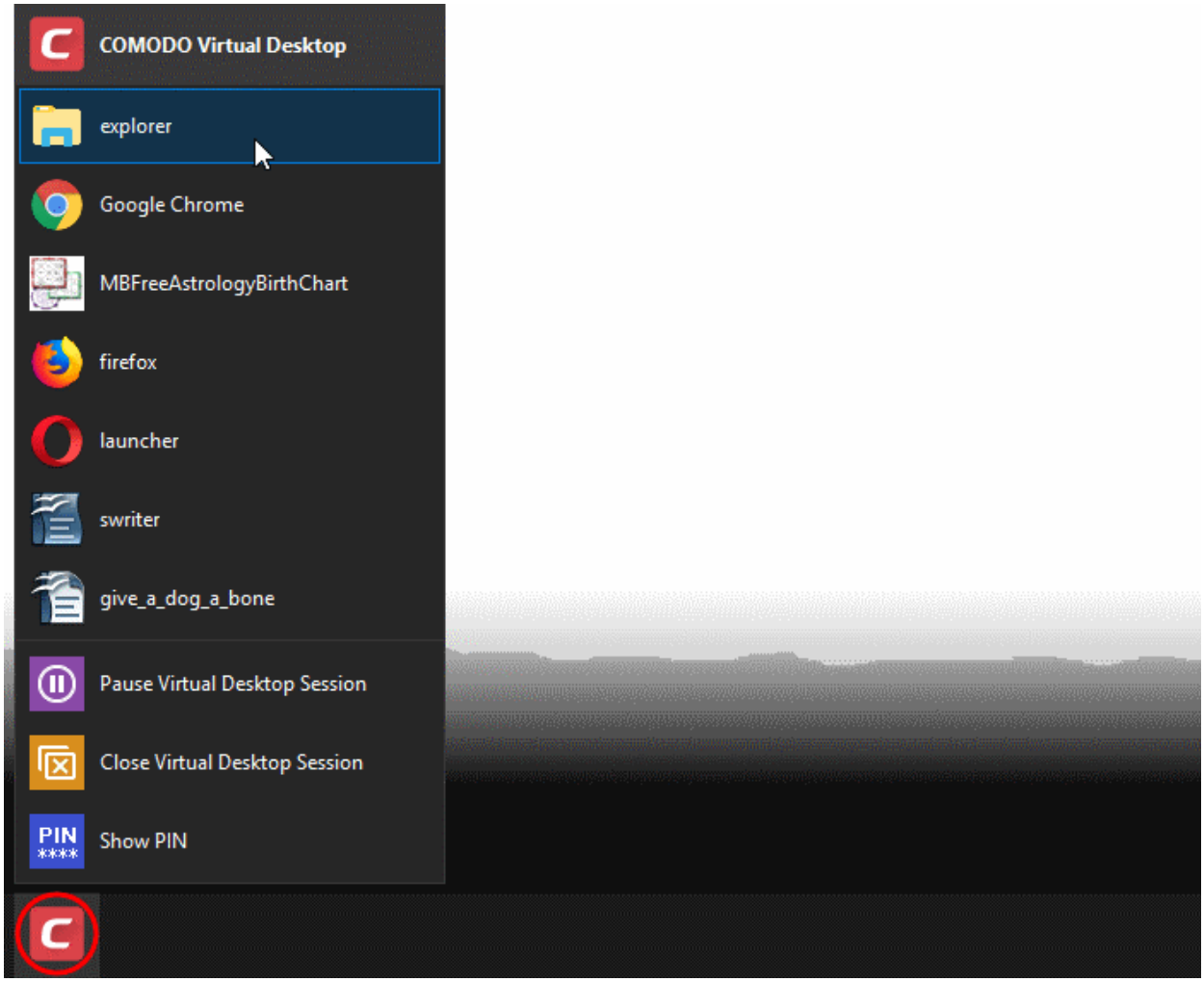
    OR
  - Start the application on the host computer
  - Click 'Add' > 'Running Processes'
  - Select the application's process and click 'OK'
- Use the 'Desktop' and 'Start Menu' switches to enable/disable each type of shortcut.
- Click 'OK' to save your settings
- Click OK in the 'Advanced Settings' dialog for your changes to take effect
- See **Add applications to virtual desktop** in **Virtual Desktop Settings** if you need more help on this.

The shortcuts are now available inside the virtual desktop.

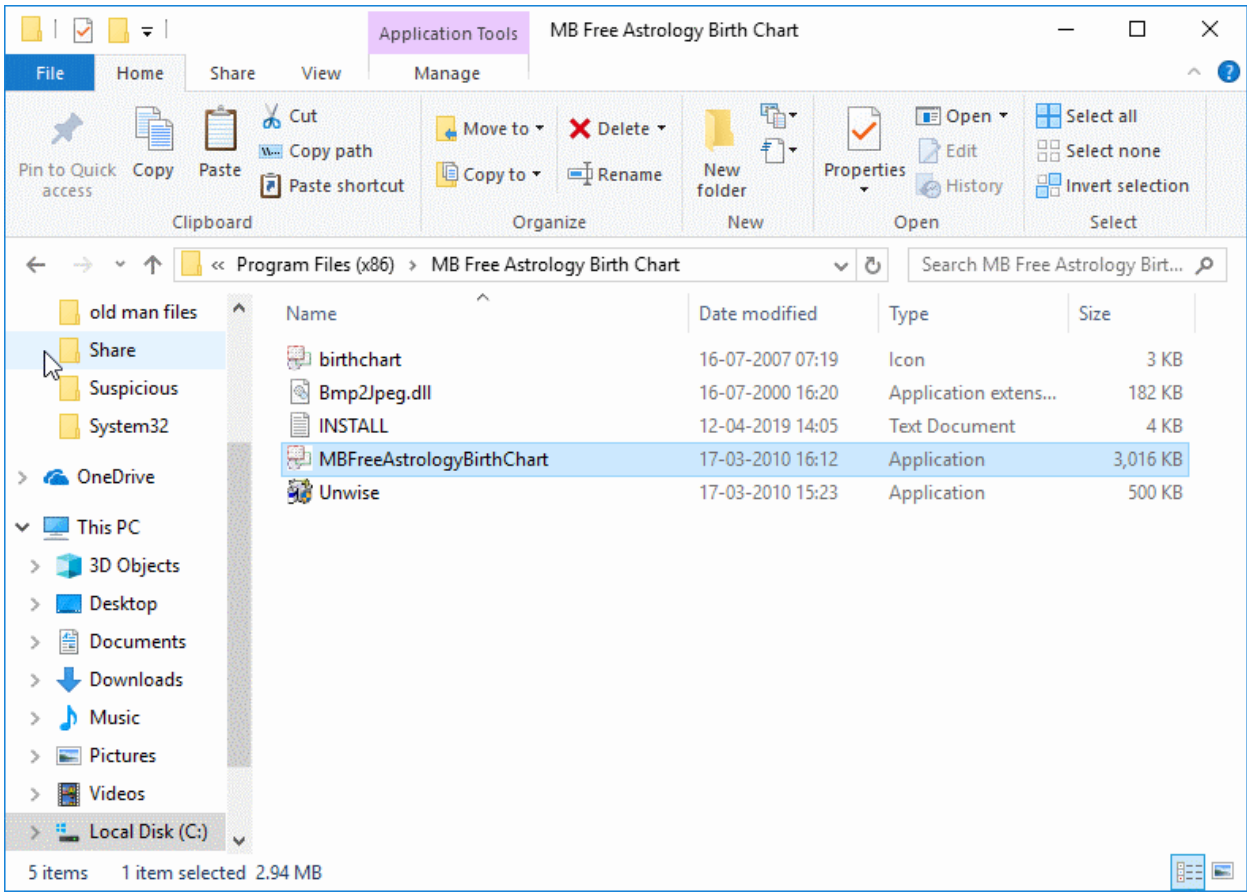
- Use the desktop shortcuts or the start menu items to open the application / file.
- Changes made in the virtual desktop are not be saved to the host system.

Navigate to Application / File

- Click the 'C' button at bottom-left, then 'explorer'



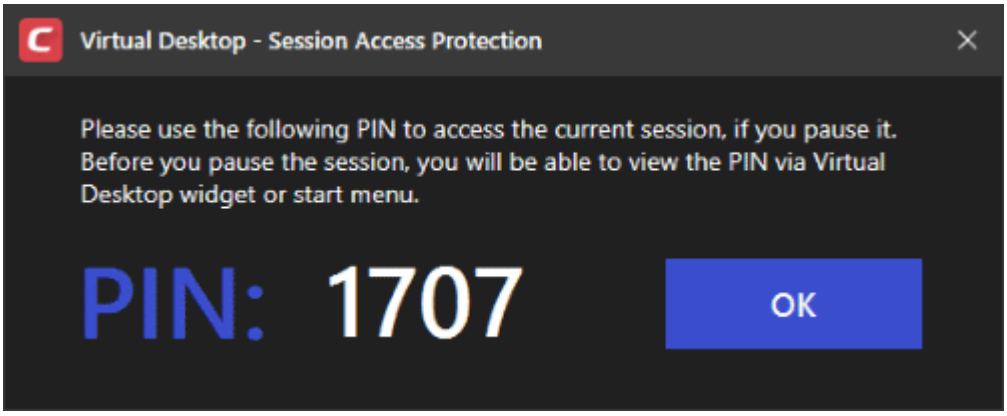
- Navigate to the application / file and open it. The file will open in the virtual desktop.



- The changes made will not be saved to your real Windows system.

4.5.5. Pause and Resume the Virtual Desktop

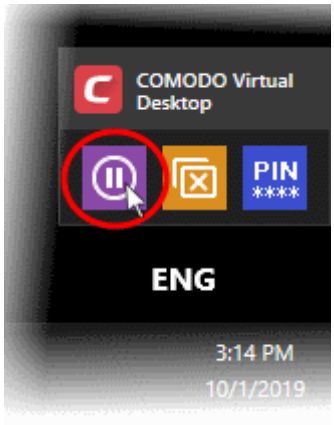
- You can pause a virtual desktop session and resume it at a later time without data loss.
- If pause PIN protection is enabled, you will need to enter a (randomly generated) 4-digit number to resume the virtual desktop.
    - Other users of the computer cannot resume the paused session without knowing the PIN.
    - The PIN is auto-generated for every session and is shown at start up:



- Click 'Show PIN' PIN **** in the start menu / tools box to view the number at any time.
- See **Secure virtual desktop sessions with a PIN** in **Virtual Desktop Settings** for more details on configuring PIN protection for virtual desktop

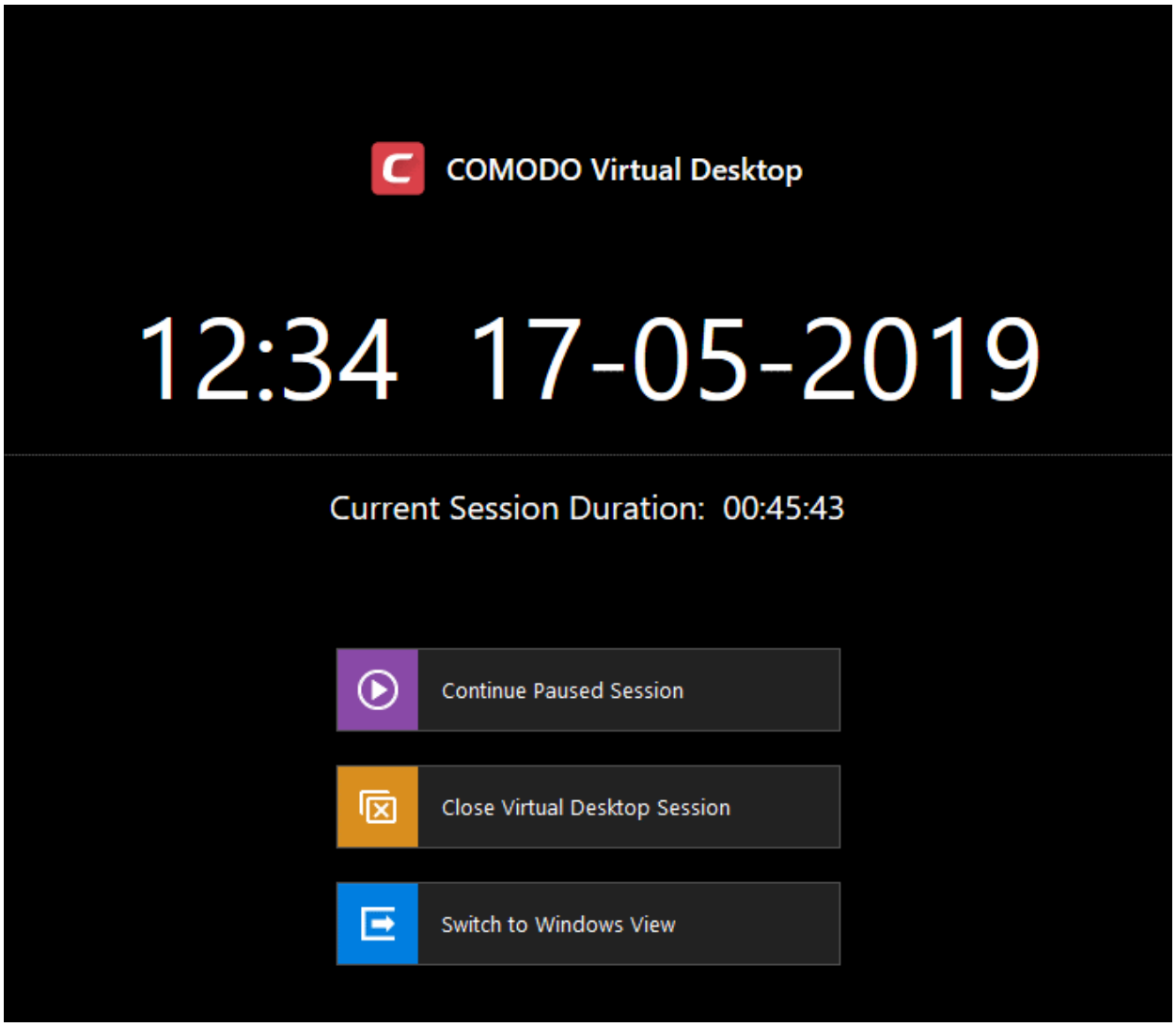
Pause a virtual desktop session

- Click the 'Pause' button in the tools box at the bottom-right

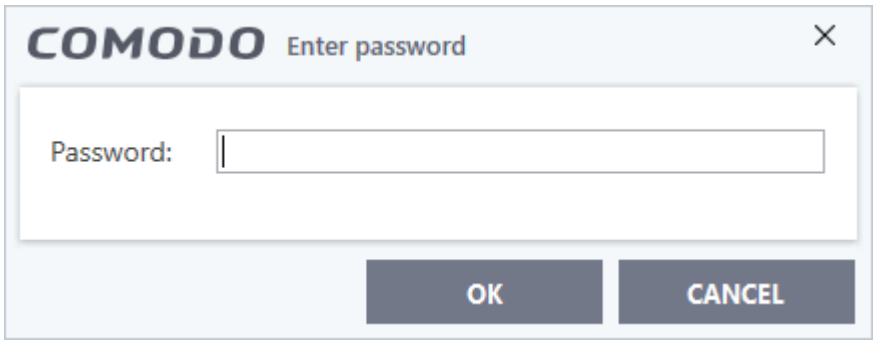


- Alternatively, click the 'C' button at bottom-left, then 'Pause Virtual Desktop Session'

The session temporarily closes:



- Click 'Switch to Windows View' if you want to open your real Windows system.
- If password protection is enabled, you will be asked to enter the exit password for the virtual desktop.



- Enter the password and click 'OK'

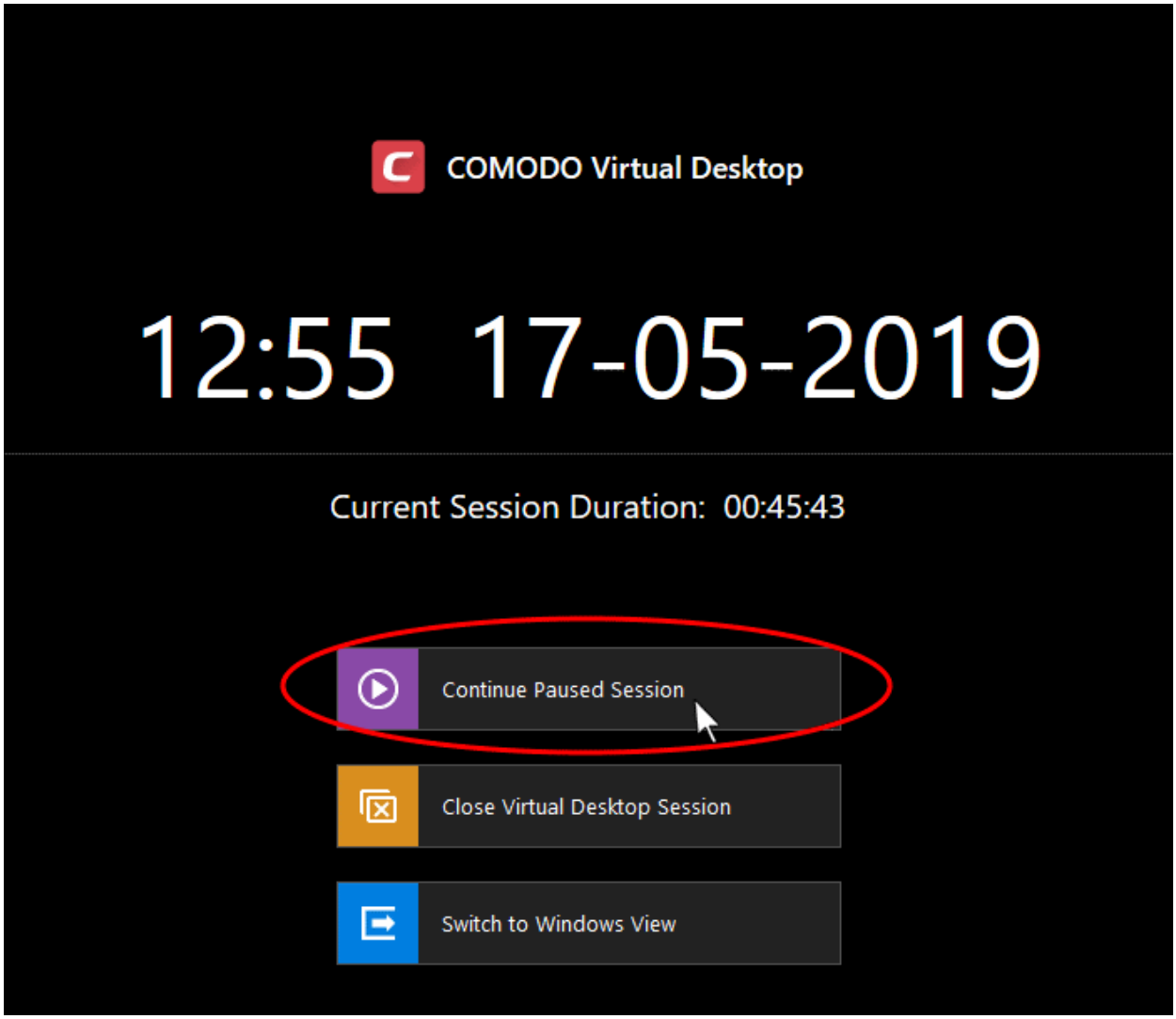
The virtual desktop tool box is shown at the bottom-right corner of the screen:

The box contains the following controls:

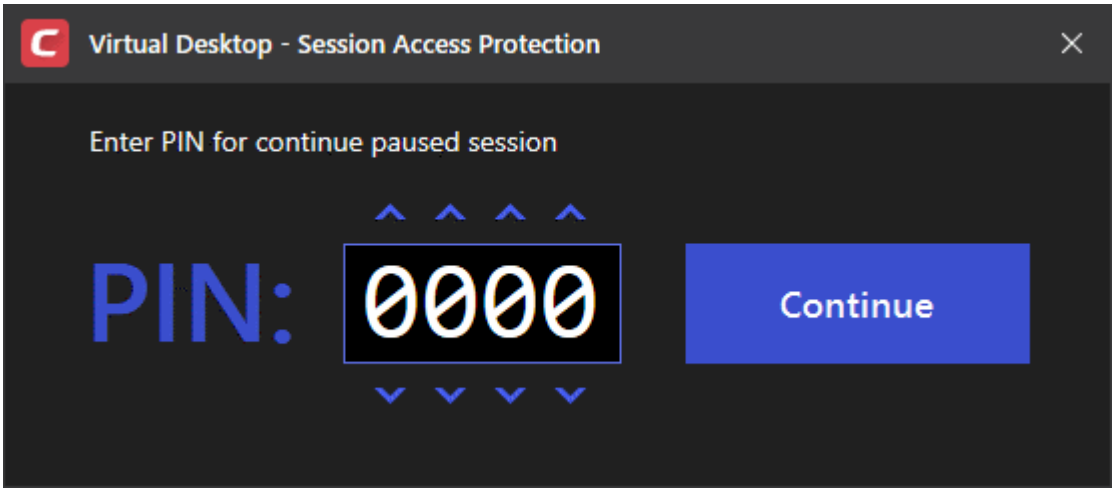
- Returns to the paused virtual desktop session
- Closes the paused desktop session. See **Close the Virtual Desktop** for more details.
- Only shown if PIN protection is enabled. Click to view the PIN for the current session.

Resume a paused virtual desktop session

- Click the return icon the to re-open the virtual desktop:



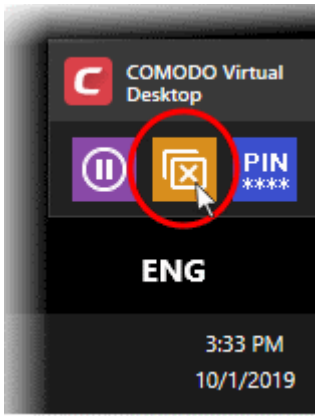
- Click 'Continue Paused Session'
- If PIN protection is enabled, you will be asked to enter the PIN:



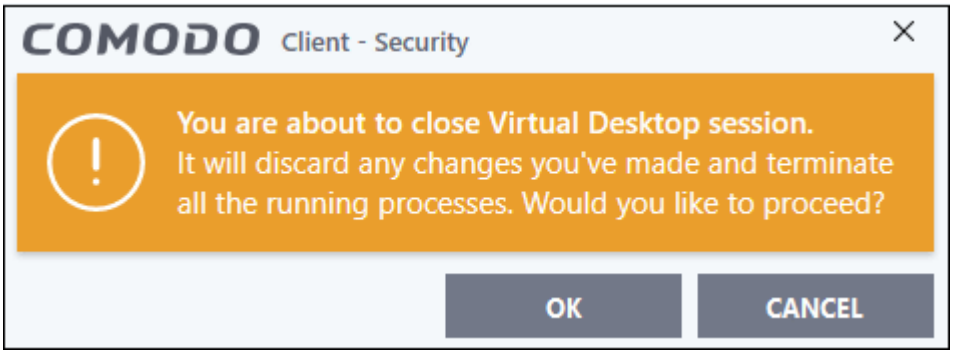
  - Enter the PIN you noted down during the start of the session and click 'Continue'
- If PIN protection is not enabled, you will be directly taken to your virtual desktop.

4.5.6. Close the Virtual Desktop

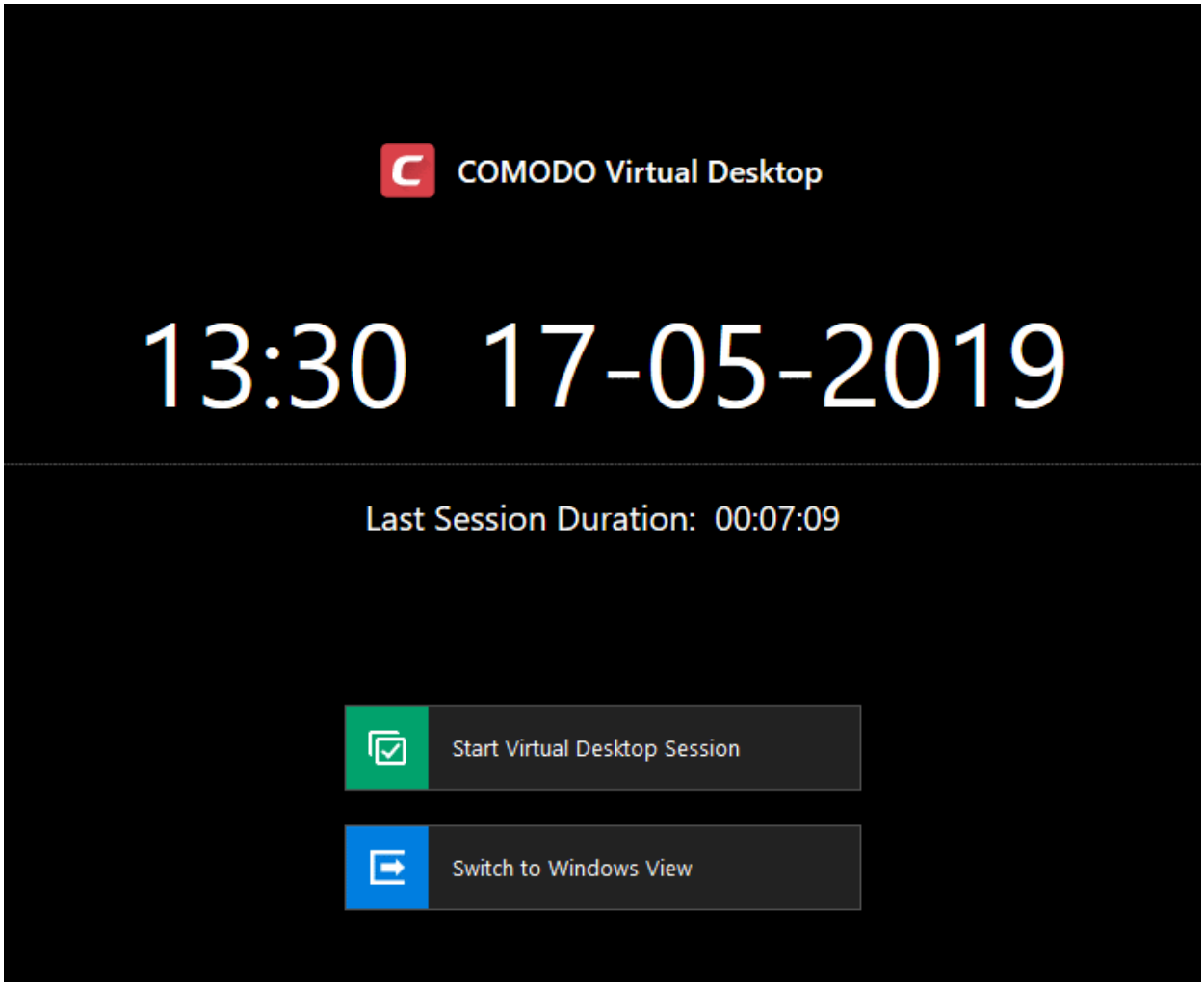
- Click the 'Close' button in the tools box at bottom-right:



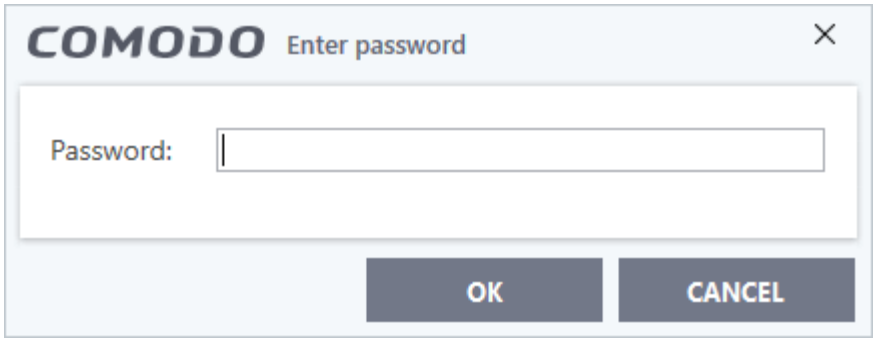
- Alternatively, click the 'C' button at bottom-left then select 'Close Virtual Desktop Session'.



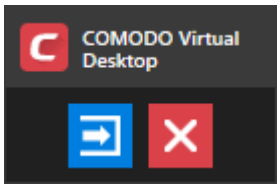
- Click 'OK' to confirm
- You will return to the virtual desktop start screen:



- Click 'Start Virtual Desktop Session' to open a new session
- Click 'Switch to Windows View' to return to the host desktop
- You will need to enter an exit password if password protection has been enabled:



  - Enter the password and click 'OK'
- The virtual desktop tools box is displayed at the bottom-right corner of your Windows screen.



  - Click to return to the virtual desktop and start a new session

- Click to completely close the virtual desktop

Terminate a paused virtual desktop session

When a virtual desktop session is paused, it shows the tools box at the bottom-right of your Windows screen.

- Click to return to the virtual desktop
- Click to completely close the virtual desktop

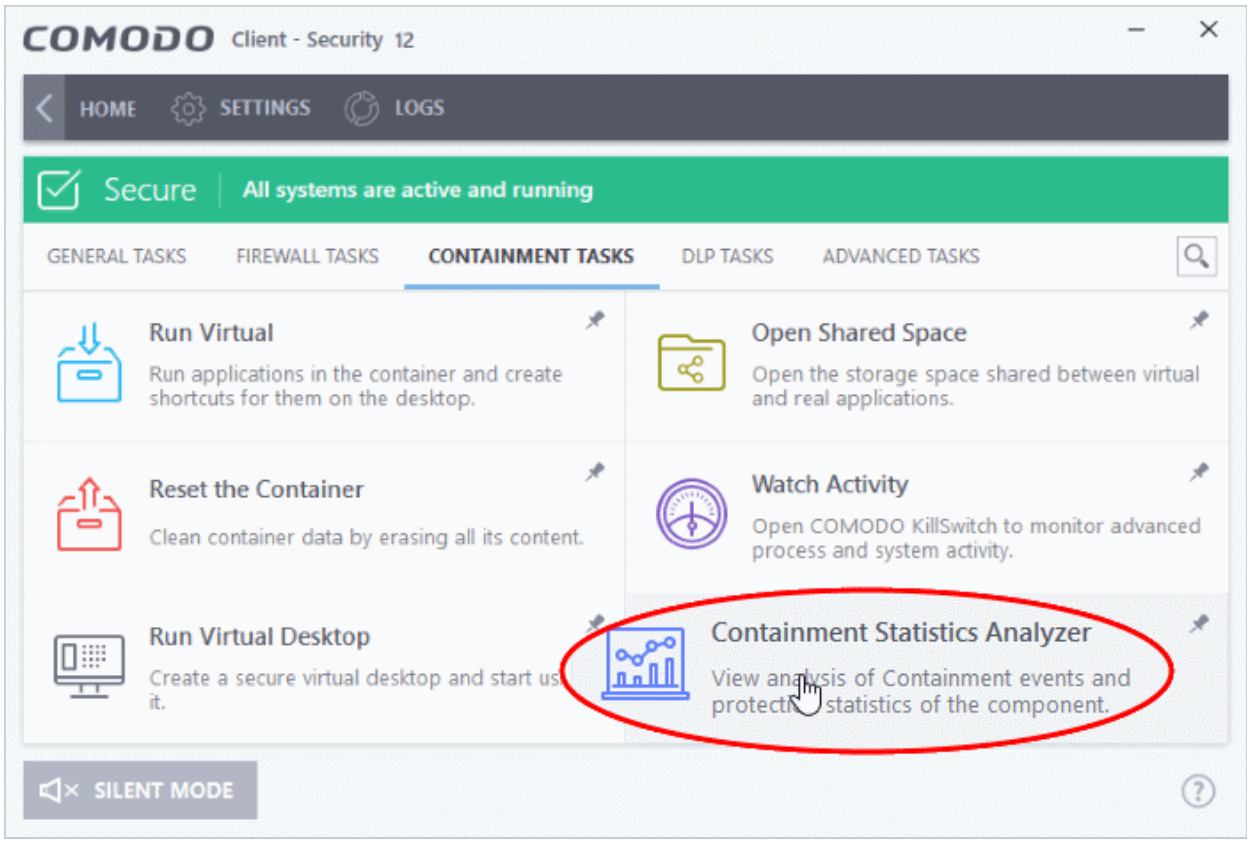
- Enter password if configured in 'Advanced Settings' > 'Containment' > 'Virtual Desktop' > 'Request password when exiting Virtual Desktop'
- Click 'OK'.

4.6. Containment Statistics Analyzer

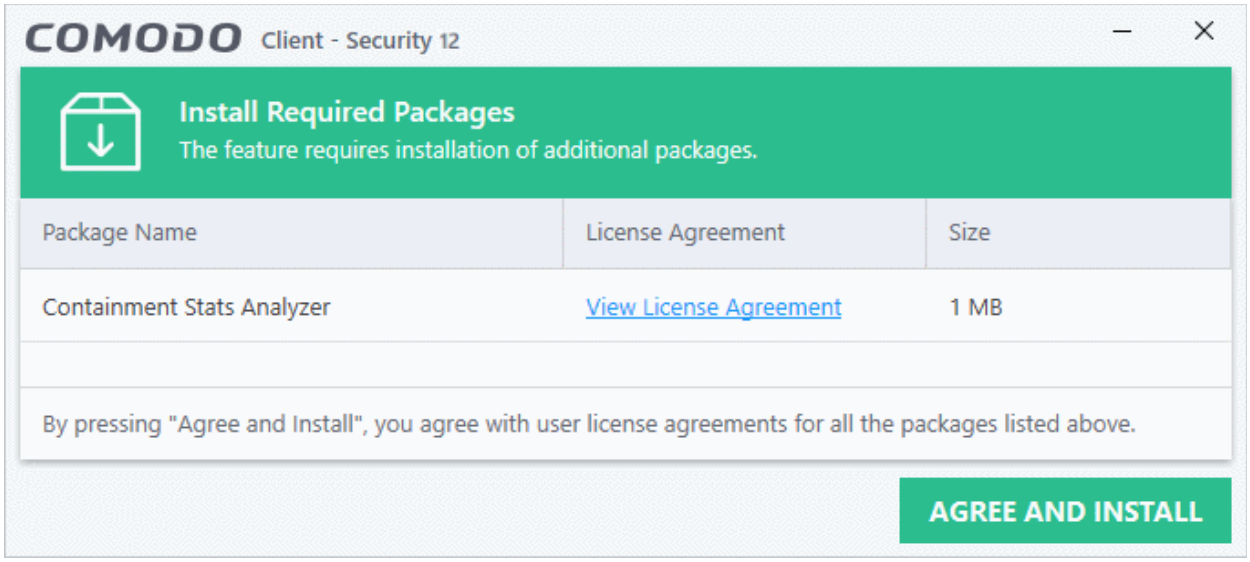
- Click 'Tasks' > 'Containment Tasks' > 'Containment Statistics Analyzer'
- The containment statistics area lets you view the activities of processes on your computer and those in the container.

Open Containment Statistics Analyzer

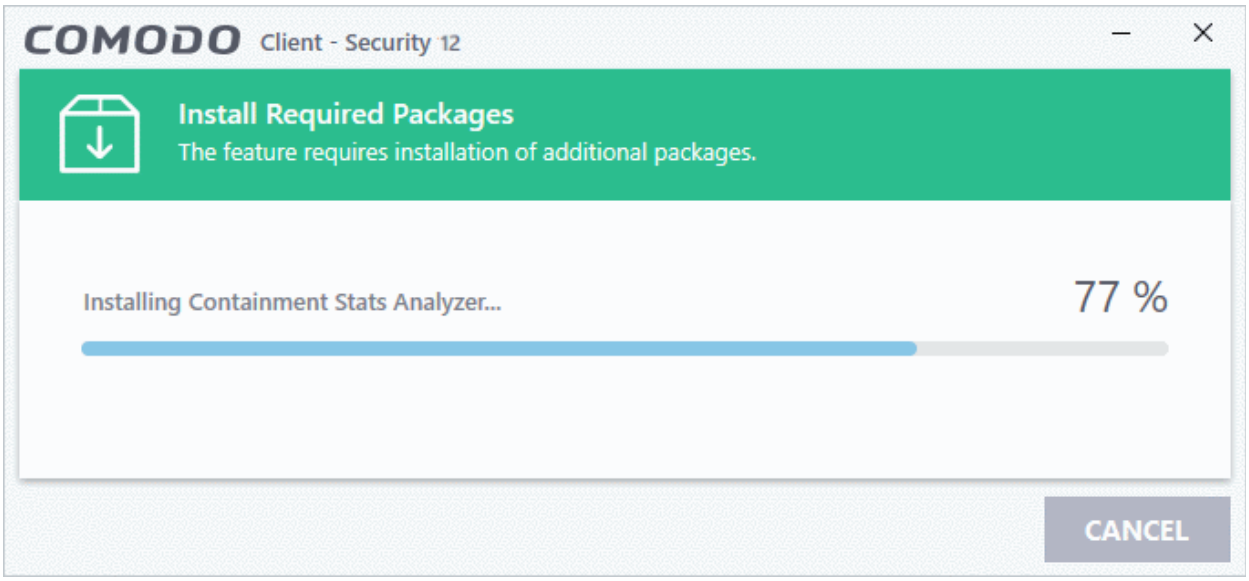
- Click 'Tasks' > 'Containment Tasks'
- Click the 'Containment Statistics Analyzer' tile



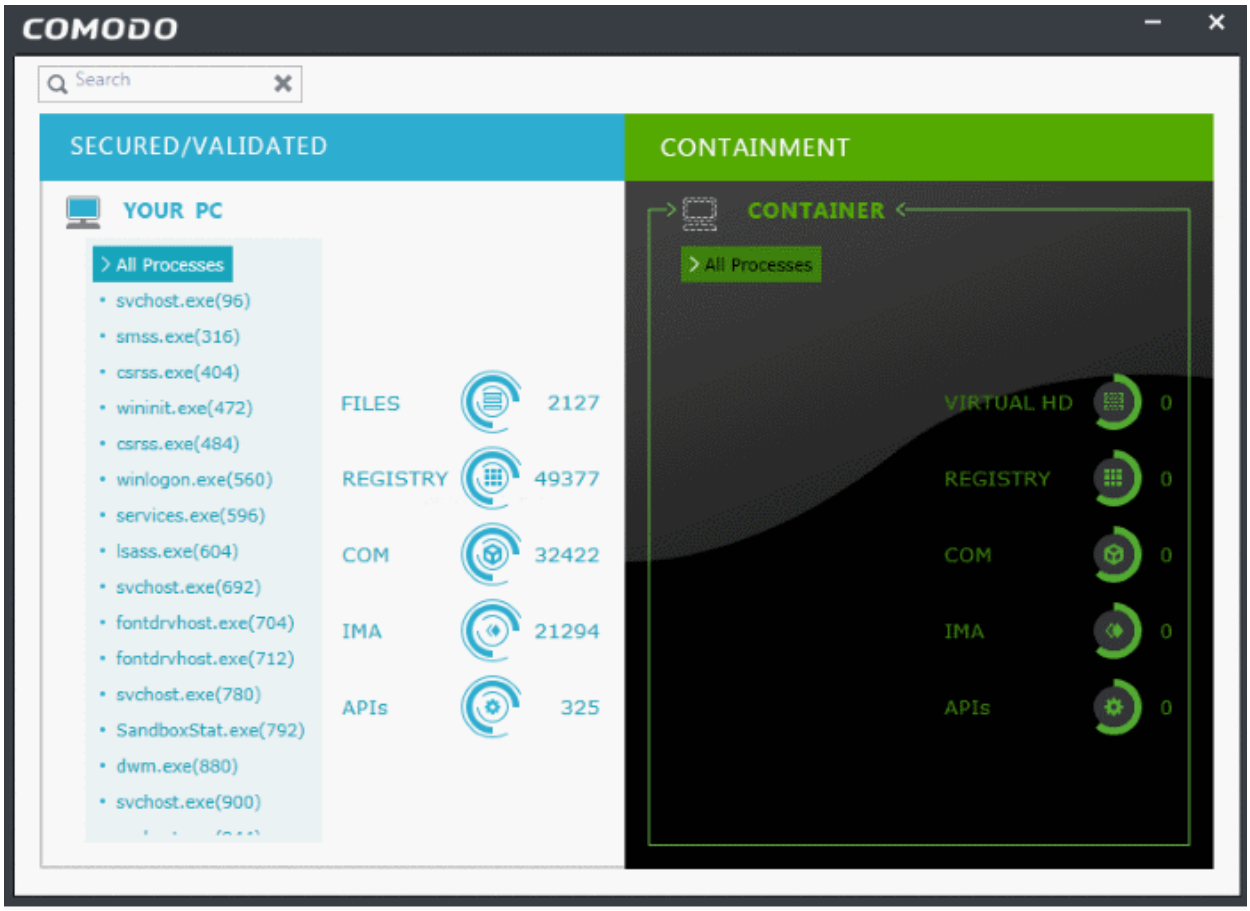
- CCS will install the analyzer if it is not yet on your system:



- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.



- The main interface opens when installation is complete:



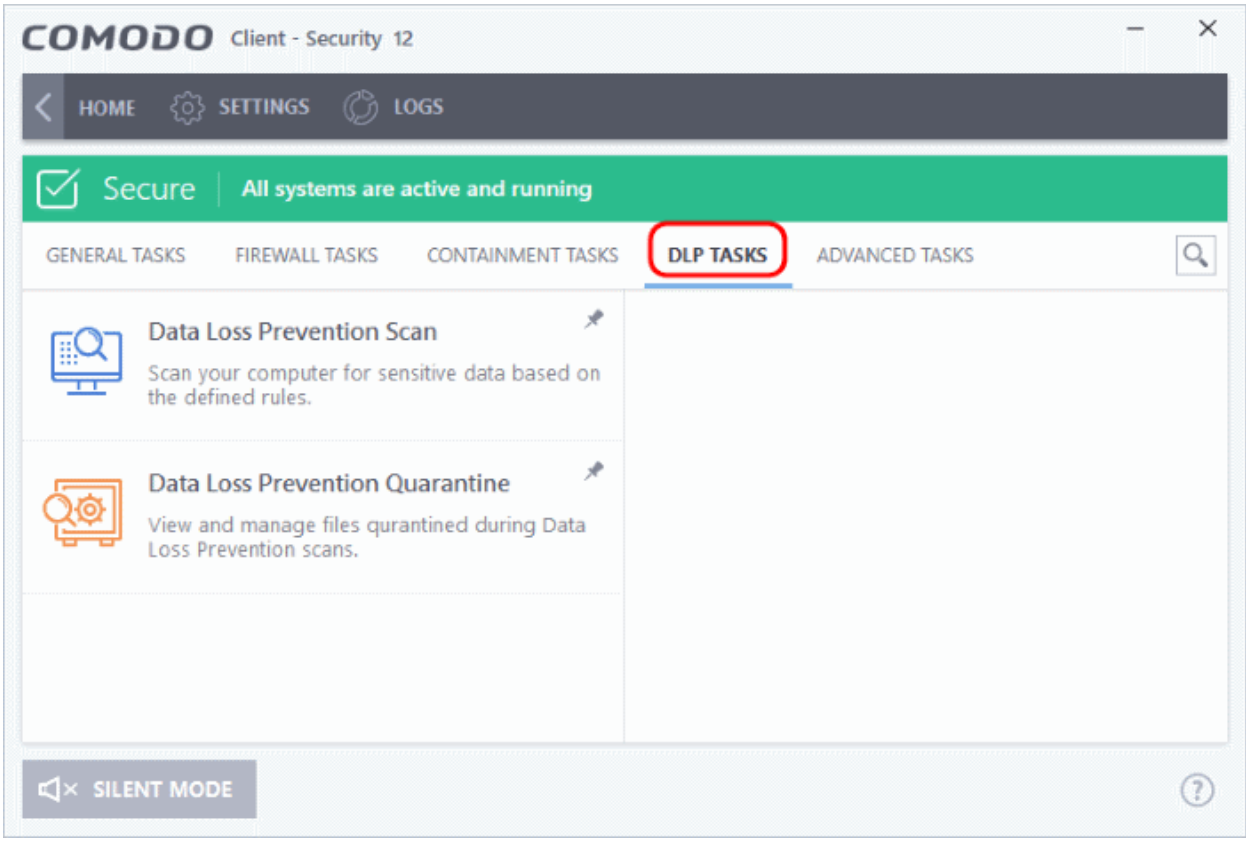
- Processes running on your host computer are shown on the left
- Process running in the container are shown on the right.
- Click a process to view its child processes and resource usage:.
  - **Files** - Number of files accessed by the process
  - **Registry** - Number of registry keys accessed by the process
  - **COM** - The inter-process component object model (COM) interfaces used by the process
  - **IMA** - Other processes, to which the selected process performs write operation

- **APIs** - The protected API's accessed by the process

5. DLP Tasks - Introduction

Click 'Tasks' > 'DLP Tasks'

- Data loss prevention scans let you identify documents which contain confidential information. For example, documents which contain credit card numbers, social security numbers, bank account numbers etc.
- DLP scans are run by selecting the DLP discovery rules active on your device
- Each rule defines the areas to scan, the type of information to search for, and the action to take on discovered files.
- The 'DLP Tasks' area lets you run on-demand DLP discovery scans and view the files quarantined by DLP rules.



See the following sections for help to:

- **Run Data Loss Prevention Scans**
- **Manage DLP Quarantined Files**

5.1. Run Data Loss Prevention Scans

Click 'Tasks' > 'DLP Tasks' > 'Data Loss Prevention Scan'

- Data loss prevention (DLP) scans let you identify documents on your computer which contain sensitive information. Example sensitive data includes credit card numbers, bank account numbers, social security numbers and so on.
- You can select the discovery rules to run a scan
- Each rule defines the areas to scan, the type of information to search for, and the action to take on discovered files. The possible actions are:

- **Ignore** - The file is retained in its original location. But you can view the identified file from the logs
- **Quarantine** - The file is moved from its original location to a secure holding area. Users cannot open quarantined files. You can review quarantined files by clicking 'Data Loss Prevention Quarantine' in the 'DLP Tasks' interface. See **Manage DLP Quarantined Files** for more details.

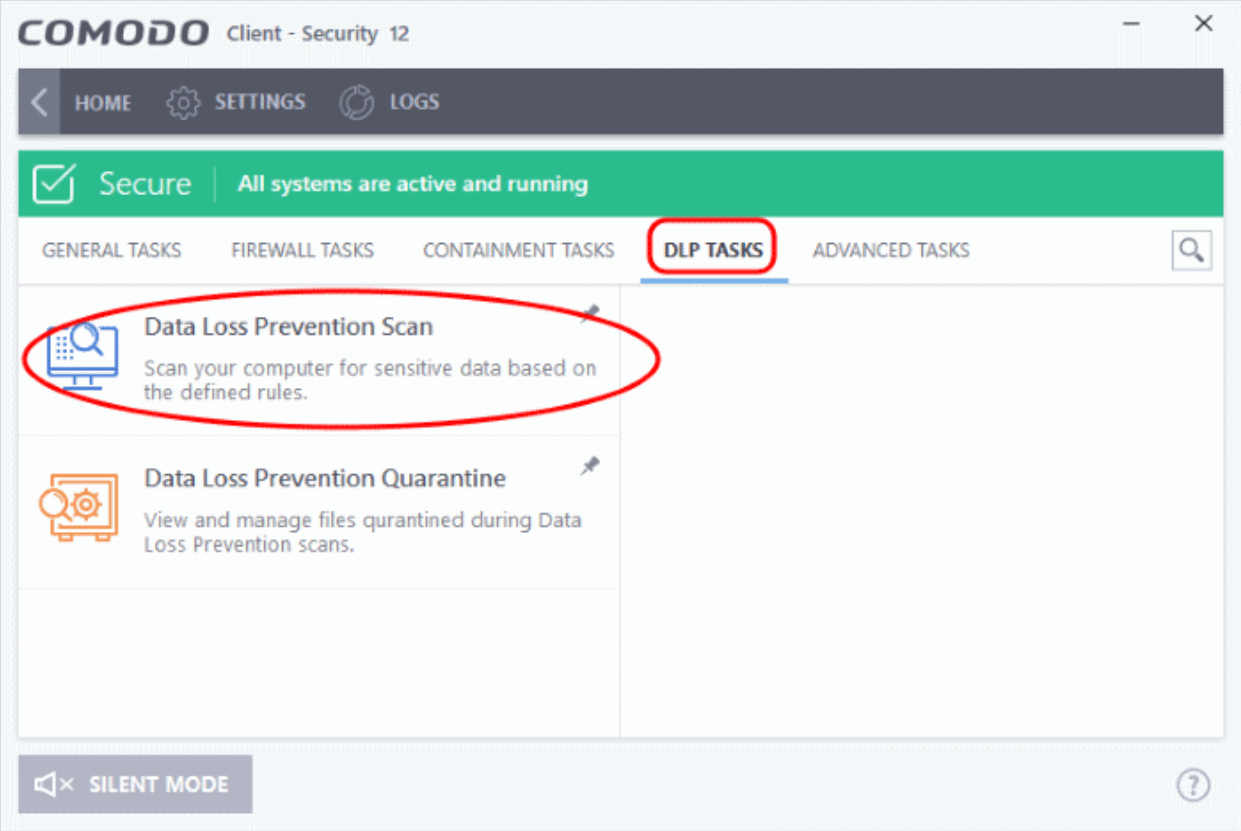
- Your Endpoint Manager admin should have first created a DLP discovery rules in EM portal and added them to the EM profile active on your device. See **DLP Discovery Rules** to view the rules available on your device.

This section explains how to run a DLP scan and view the results:

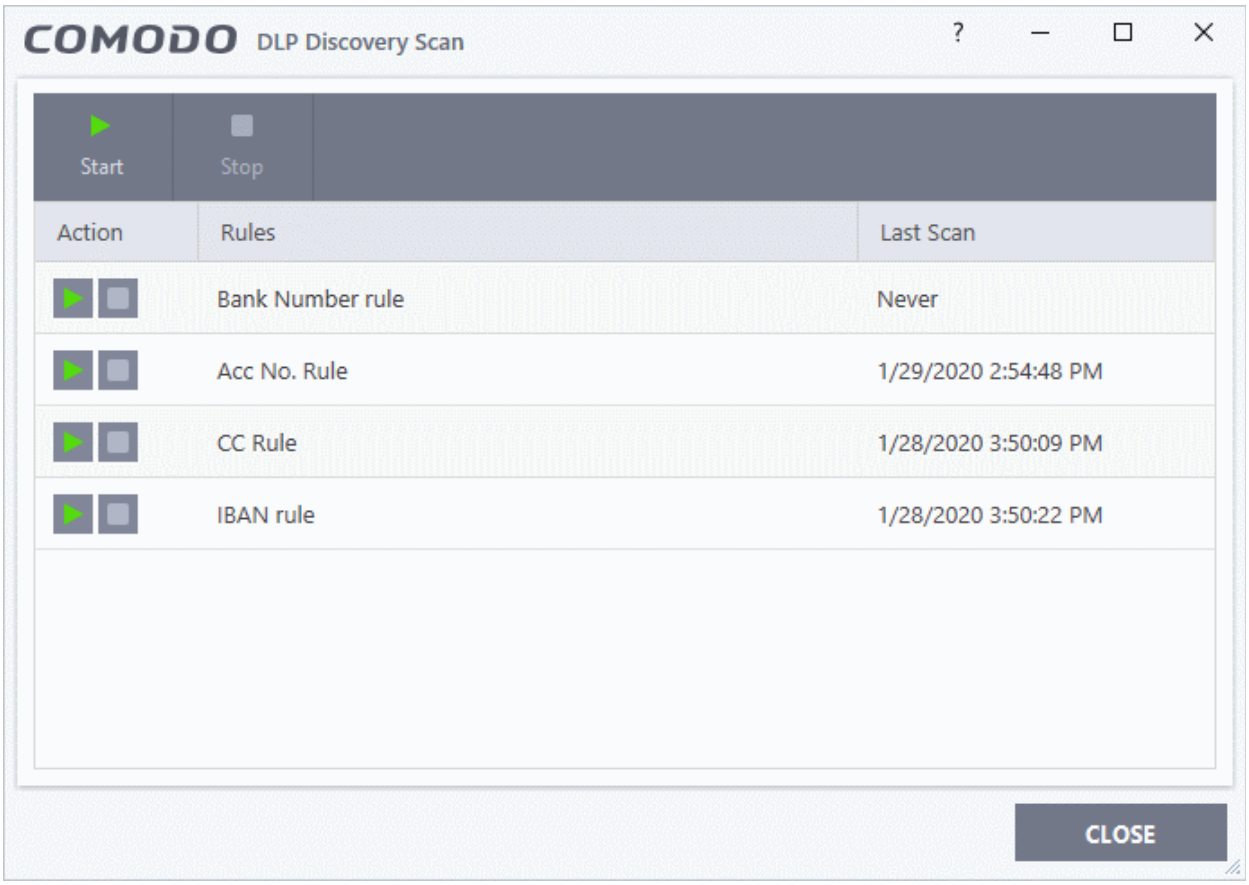
- **Run a DLP scan**
- **View scan results**

Run a Data Loss Prevention Scan

- Click 'Tasks' on the CCS home screen
- Click 'DLP Tasks' > 'Data Loss Prevention Scan'



The scan interface shows all rules added to your device by the EM profile active on your device.

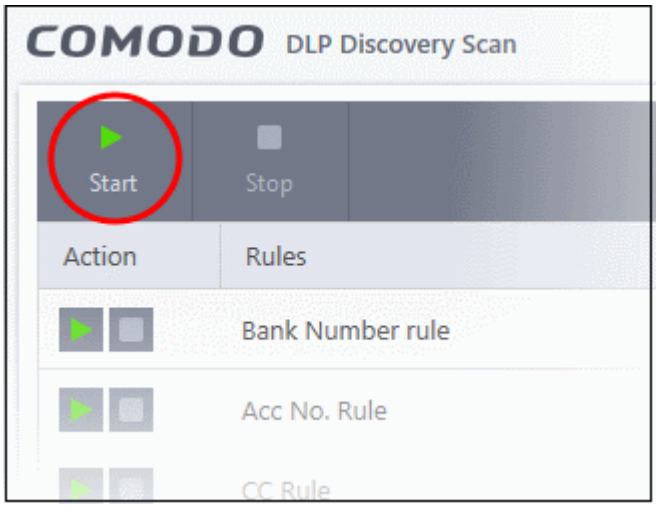


Action - Start and stop scans using a particular rule.

Rules - The label of DLP rule

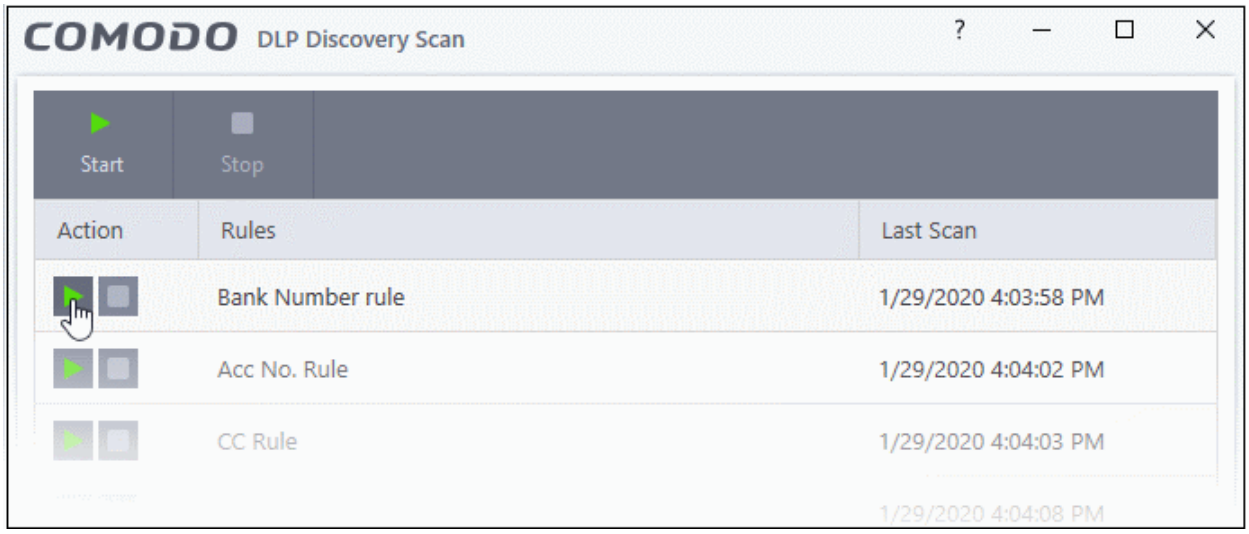
Last Scan - Date and time of the most recent DLP scan

- Click the 'Start' button at the top to run all rules at once



OR

- Use the start buttons on the left to run a scan with a specific rule.



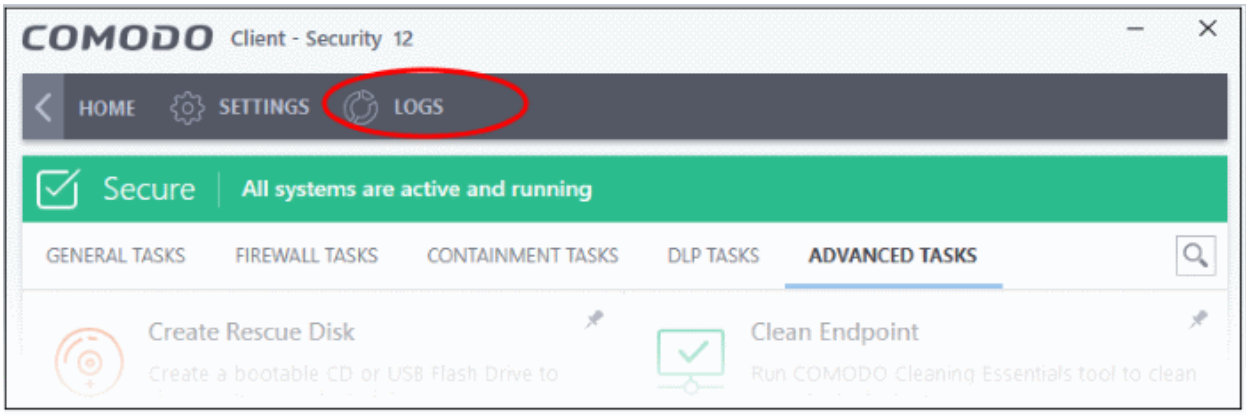
- CCS runs the selected scans
- After the scan is started, you can pause, resume or stop the scan

Next, **view results** of the scan

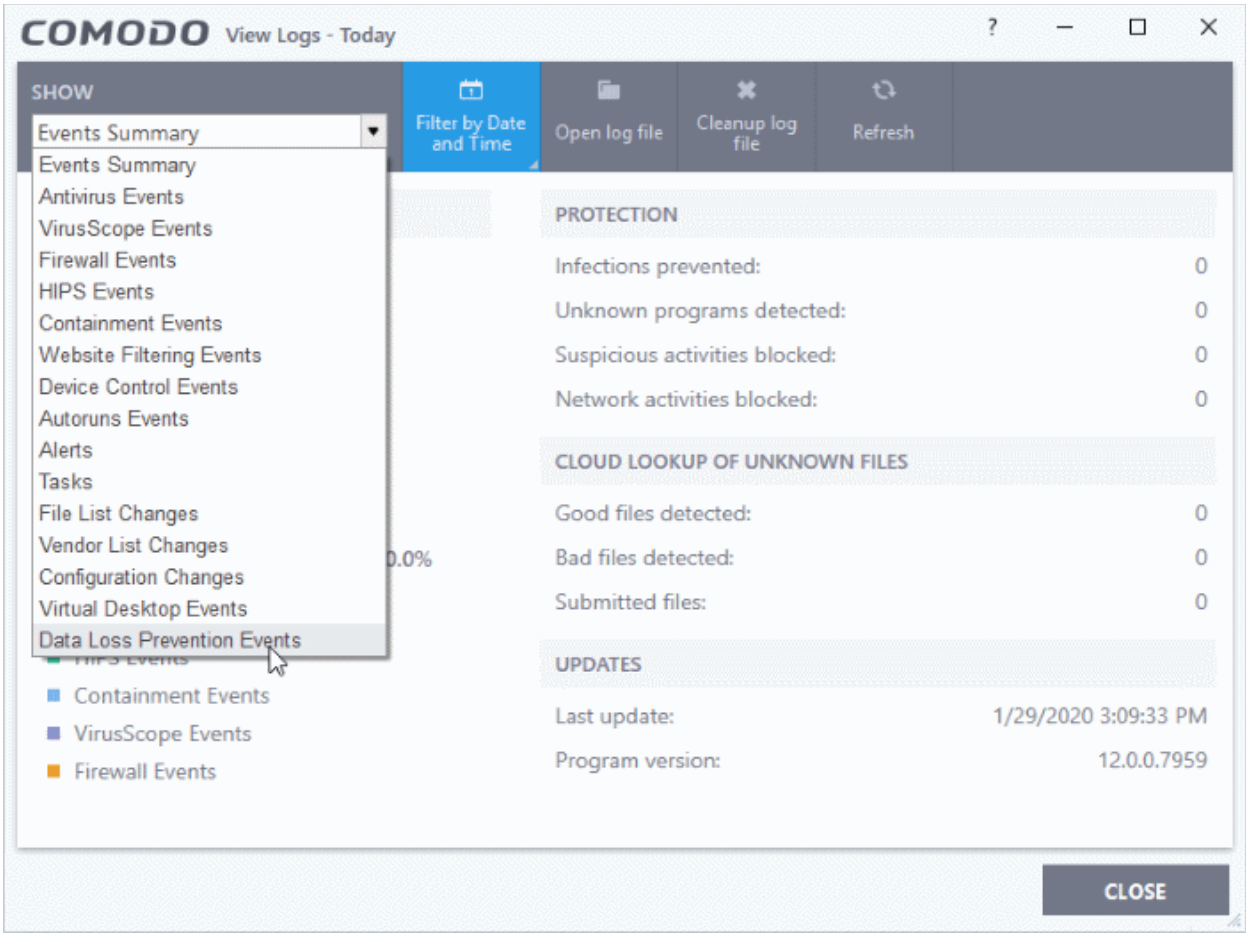
View DLP Scan Results

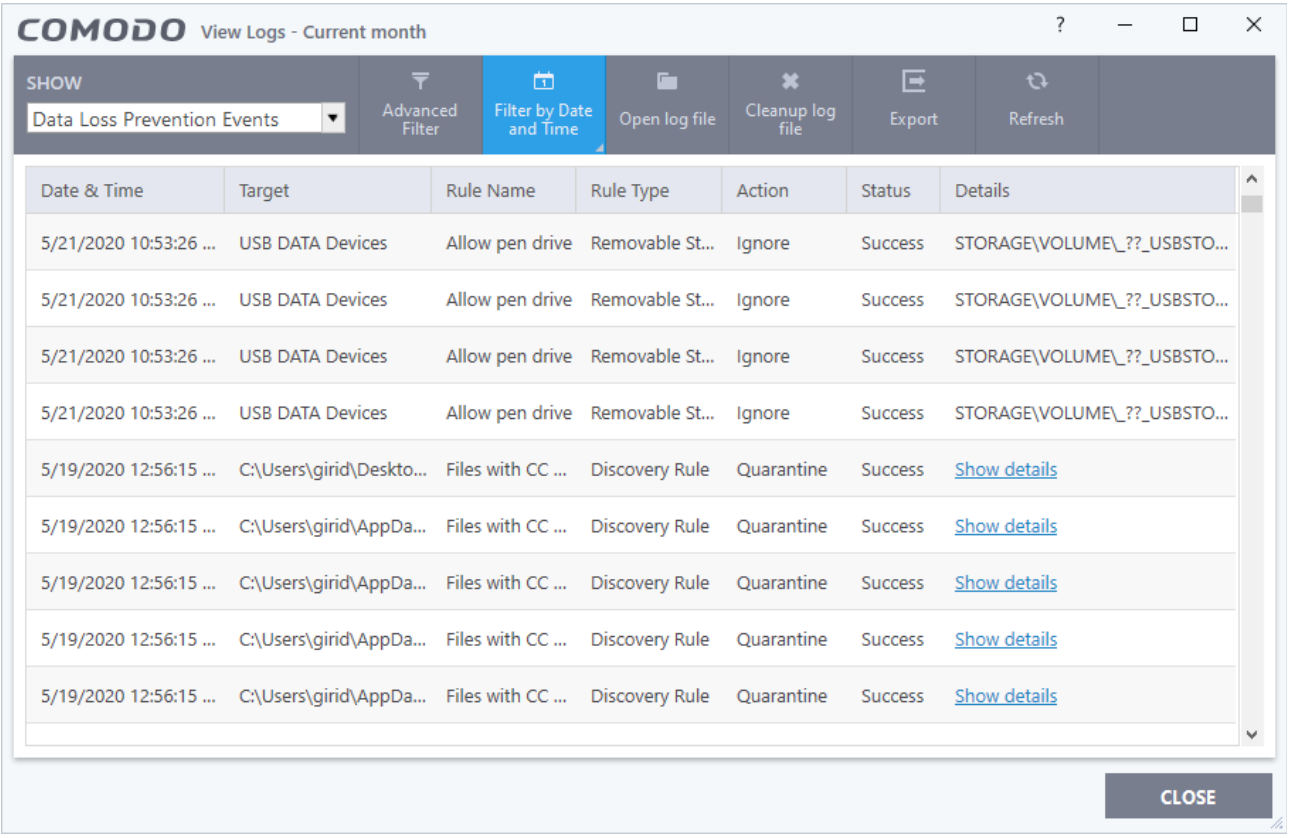
You can view DLP scan results in the logs section.

- Click 'Logs' at the top of the CCS interface:



- Select 'Data Loss Prevention Events' from the first drop-down:





- **Date & Time** - When the event occurred.
- **Target** - The item affected by the rule.

- **DLP Monitoring event** - Shows the type of external storage device to which the data transfer attempt was made
- **DLP Discovery event** - Shows the file path of the identified file

- **Rule Name**- The DLP rule that found the target item. This could be a DLP discovery rule or a monitoring rule.
- **Rule Type** - Whether rule is a DLP discovery rule or a removable storage rule
- **Action** - How the file was handled in the DLP event. The possible values are:
  - Ignore
  - Quarantine
  - Restore from quarantine
  - Delete from quarantine
  - Blocked
- **Status** - Shows whether the rule executed successfully or not
- **Details** - The specifics of the data found.
  - **DLP monitoring rule** - Shows the removable storage device affected by the rule.
  - **DLP Discovery rule** - Has a 'Show details' link which opens the specifics of the event. See **View file details** for more details.

Advanced Filter - Search the logs by file location, rule or action. Use the advanced filter options to filter the logs of discovery events.

Filter by Date and Time - Search for logs generated within a specific time-frame

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

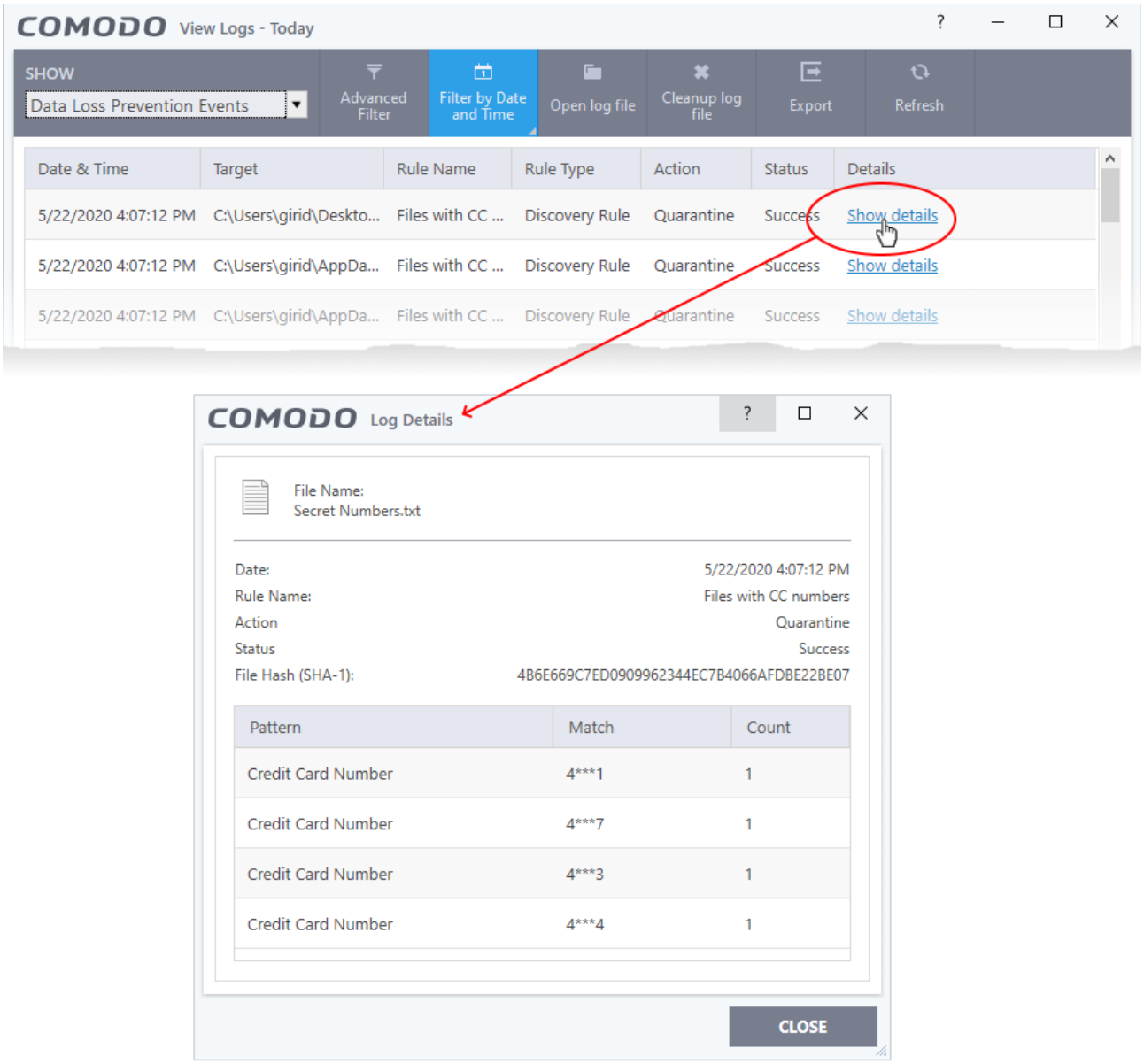
Cleanup log file - Delete the selected event log

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

Refresh - Reload the current list to show the latest logs

View file details

- Click the 'Show details' in the 'Details' column:

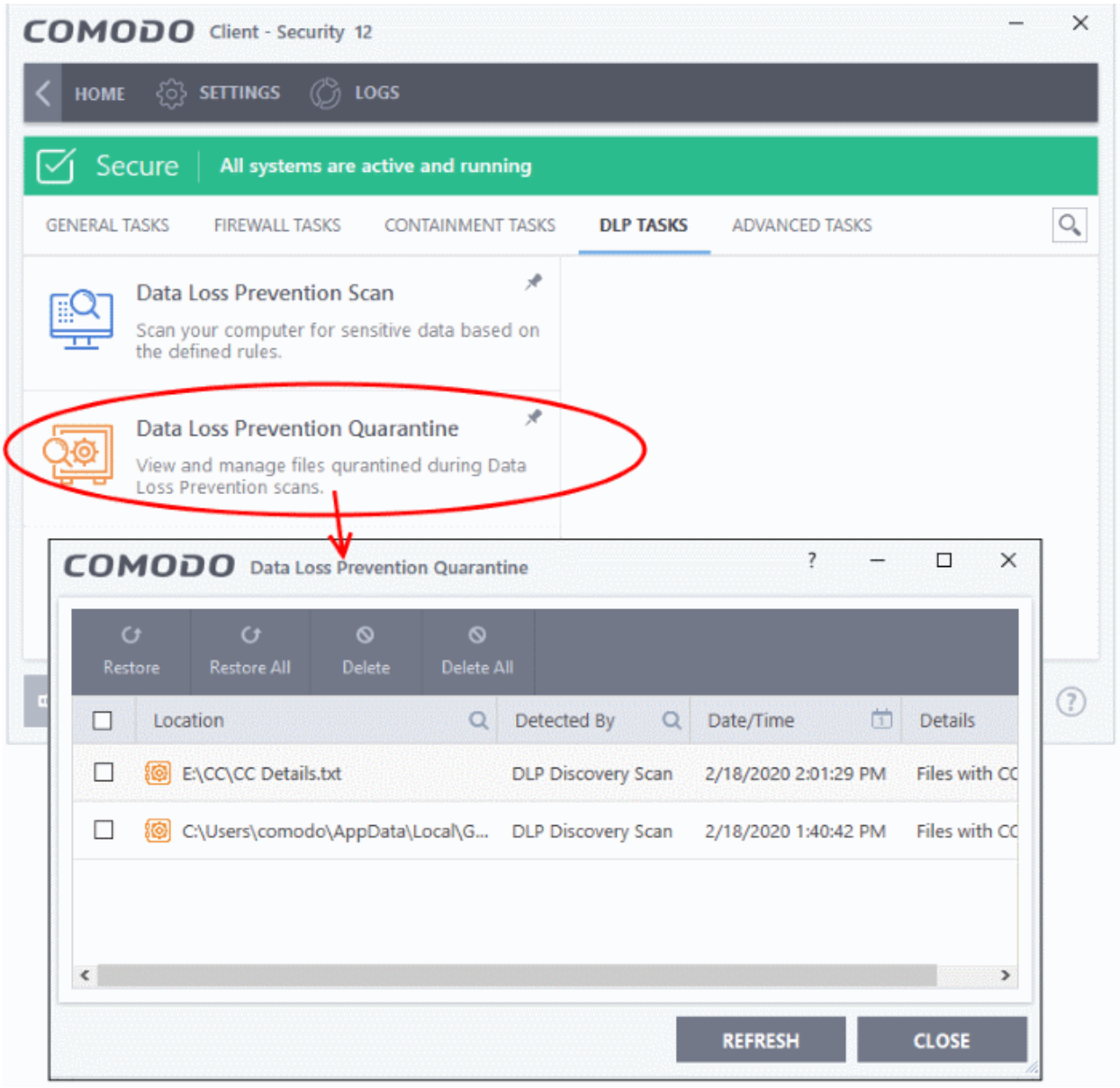


- The screen shows the name of the file, and the rule/pattern which discovered sensitive data in the file.
- The 'match' column shows the first and last characters of the actual discovered data. The option to show this should be enabled in the discovery rule.

5.2. Manage DLP Quarantined Files

Click 'Tasks' > 'DLP Tasks' > 'Data Loss Prevention Quarantine'

- The DLP quarantine area shows files which CCS has isolated because they contain sensitive data. CCS quarantined these files because it was told to do so by a DLP scan rule.



- **Location** - The path of the detected file
- **Detected By** - This version of CCS only supports quarantine by DLP discovery scans. More to come in future versions.
- **Date / Time** - When the item was moved to quarantine.
- **Details** - The name of the discovery rule that quarantined the file

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

- **Delete the quarantined item**

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

  Click 'Delete All' if you want to remove all quarantined items.

- **Restore the quarantined item**

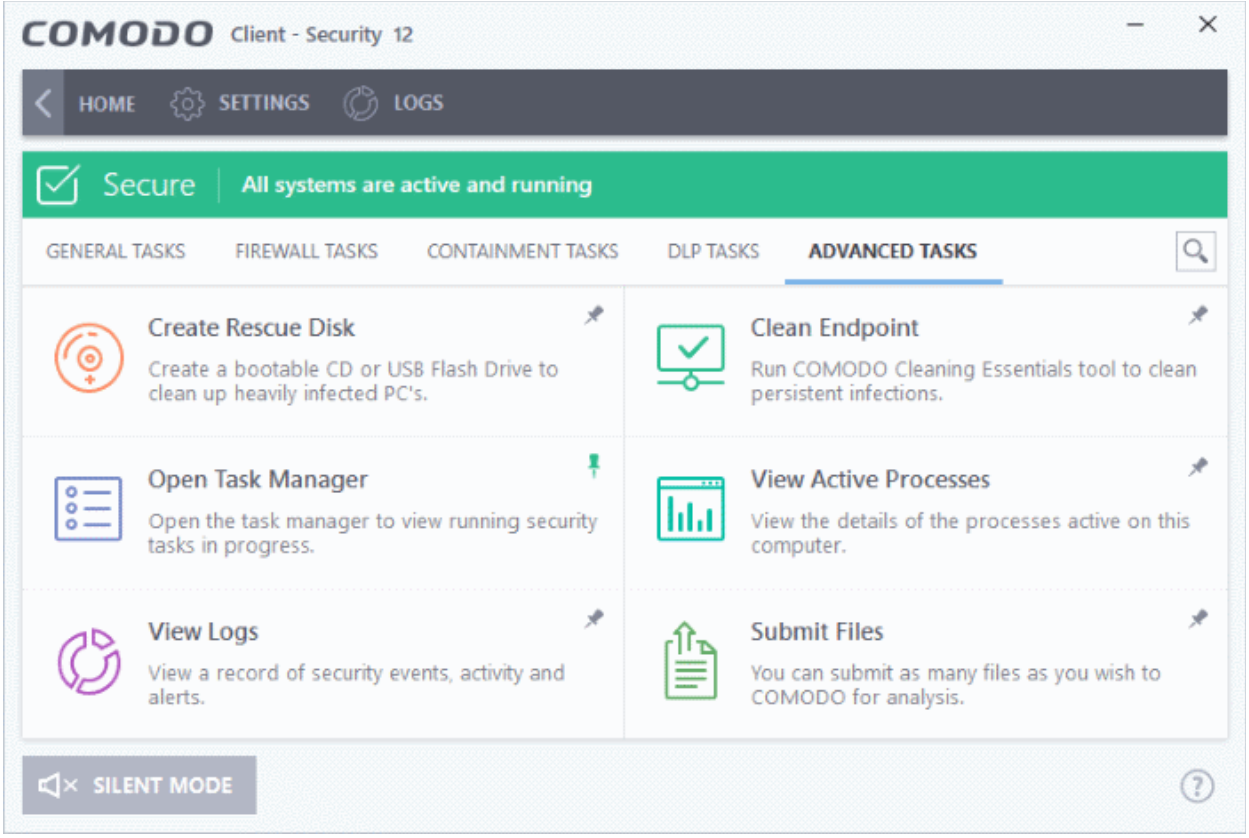
  Moves the items back to their original location. Select the items you want to move then click the 'Restore' button.

  Click 'Restore All' if you want to reinstate all quarantined items.

Click 'Close' to exit the screen.

6.Advanced Tasks - Introduction

- Click 'Tasks' > 'Advanced Tasks'
- Advanced tasks lets you view event logs, manage CCS tasks, and take advantage of several other Comodo utilities.



See the following sections to find out more about each feature:

- **Create Rescue Disk** - Burn a bootable ISO that lets you run virus scans in pre-boot environments
- **Task Manager** - Stop, pause and resume currently running CCS tasks like antivirus scans and updates
- **Clean Endpoint** - Deploy Comodo Cleaning Essentials to remove persistent infections from your PC
- **View Active Process List** - Manage processes which are currently running on your PC. Click the 'More' button to open Comodo **KillSwitch**.
- **CCS Logs** - View the event logs of firewall, antivirus, containment and HIPS modules
- **Submit Files** - Upload unknown/suspicious files to Comodo Valkyrie for analysis

You might need to enter a password to access these tasks if so configured in the Endpoint Manager profile. See '**Password Protection**' for more details."

6.1.Create a Rescue Disk

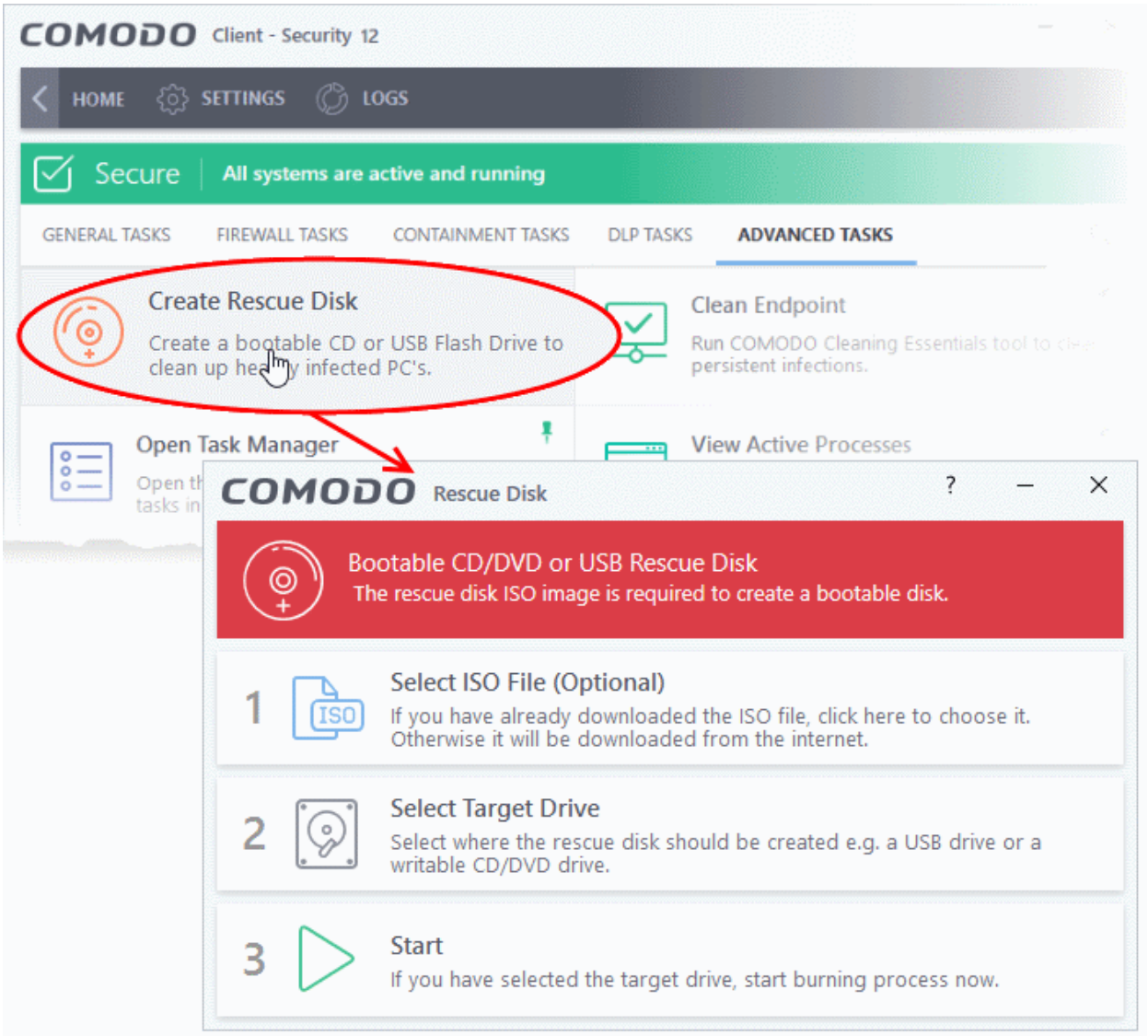
Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk'

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

- CRD can eliminate infections that are preventing Windows from booting in the first place.
- The application is useful for removing malware which has embedded itself so deeply that regular AV

software cannot remove it.

- CRD contains tools to explore files in your hard drive, take screen-shots and browse web pages.
- Click 'Tasks' > 'Advanced Tasks' > 'Create Rescue Disk' to download and burn to ISO, CD/DVD, USB or another drive. See **Download and Burn Comodo Rescue Disk** for a walk-through of this process.

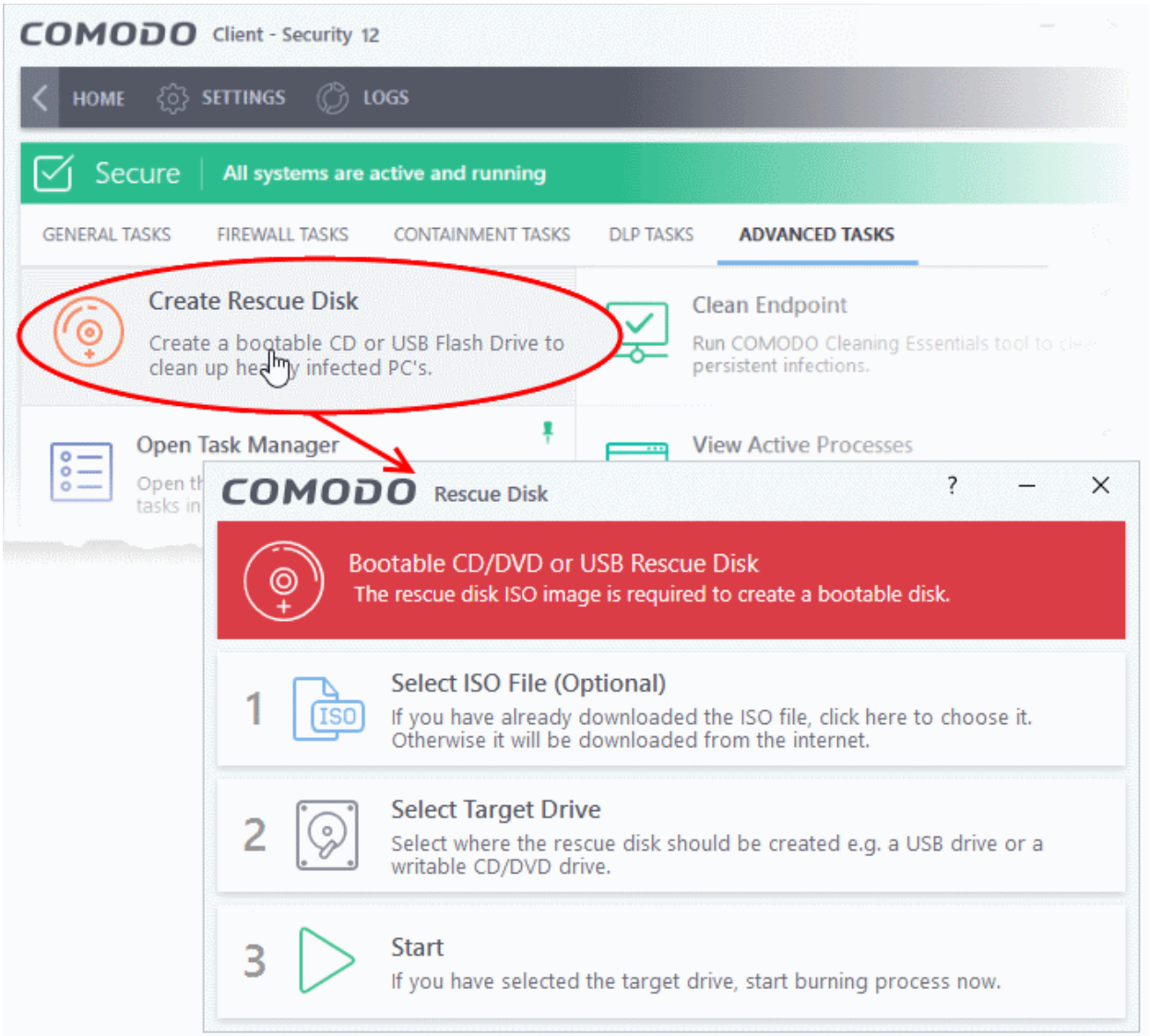


After you have burned the ISO, you need to boot your system to the rescue disk. This will open the scanner in your pre-boot environment.

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

6.1.1. Download and Burn Comodo Rescue Disk

- Click 'Advanced Tasks' on the CCS home screen
- Click 'Create Rescue Disk':



The setup screen shows the steps to create a new rescue disk:

Step 1- Select the ISO file

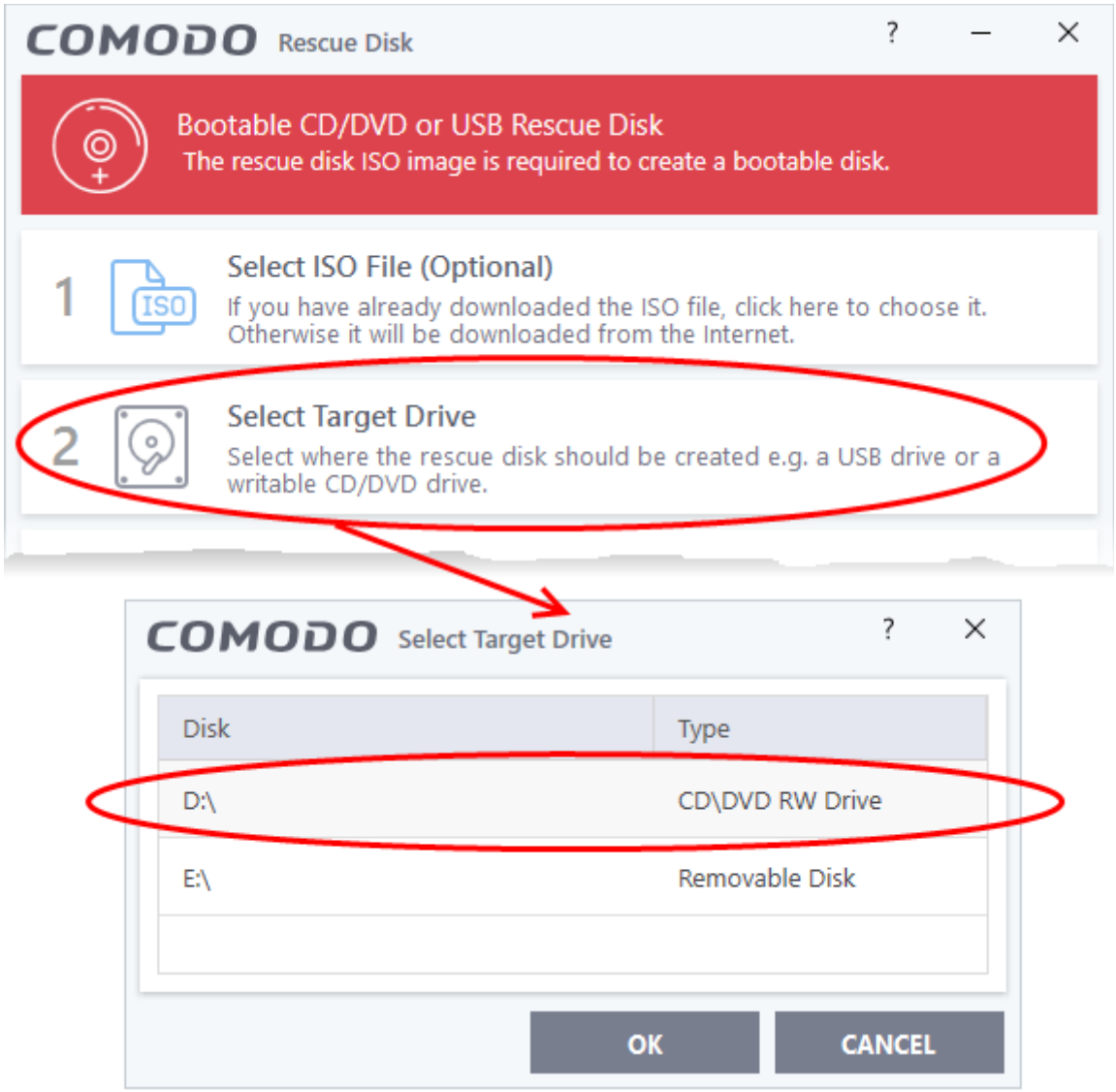
Optional. If you have already downloaded the rescue disk ISO from Comodo then please select it here. If you haven't yet downloaded then please ignore this step - it will be downloaded automatically during Step 3.

Step 2 - Select target drive

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

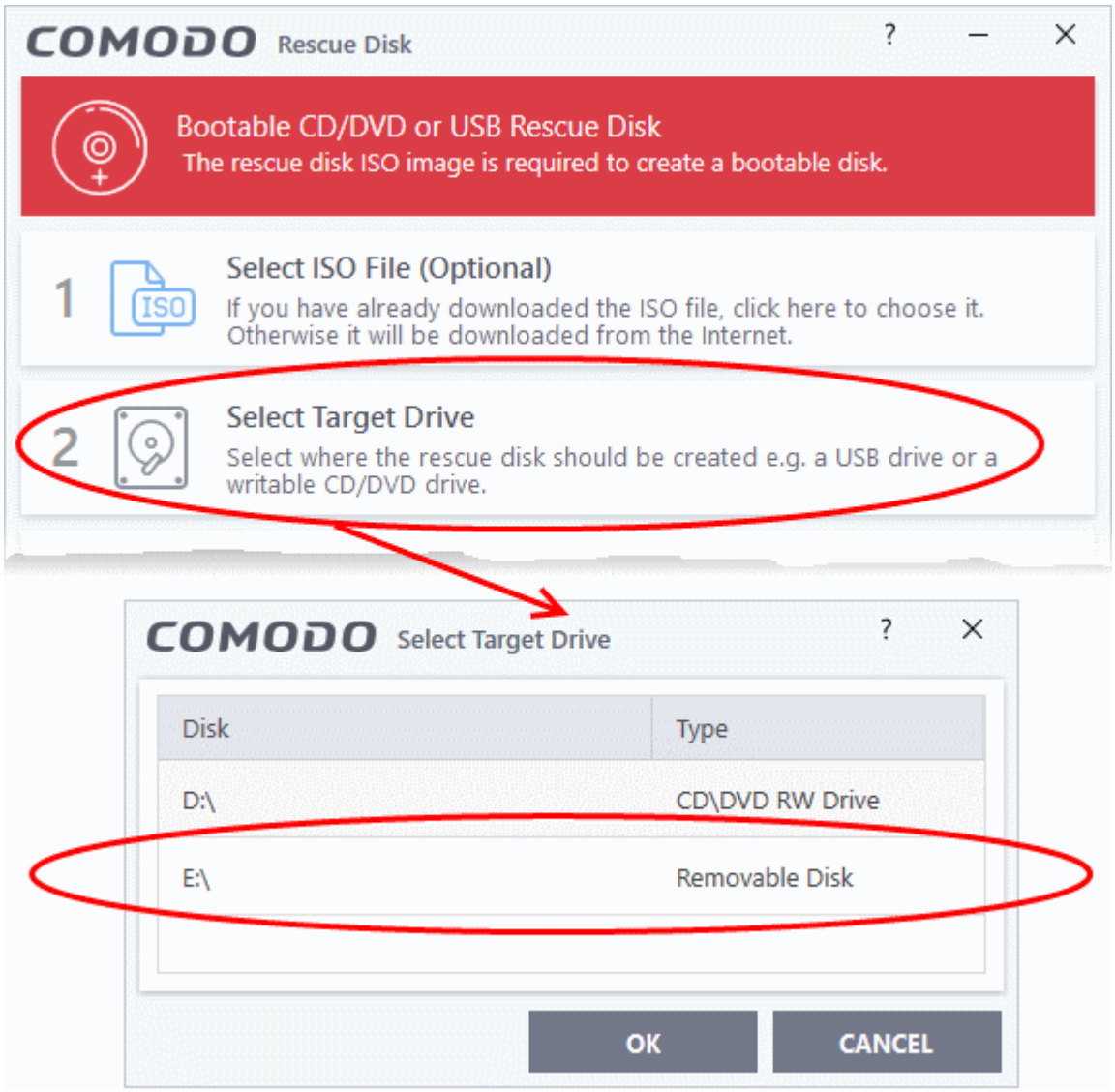
Burn to CD or DVD

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



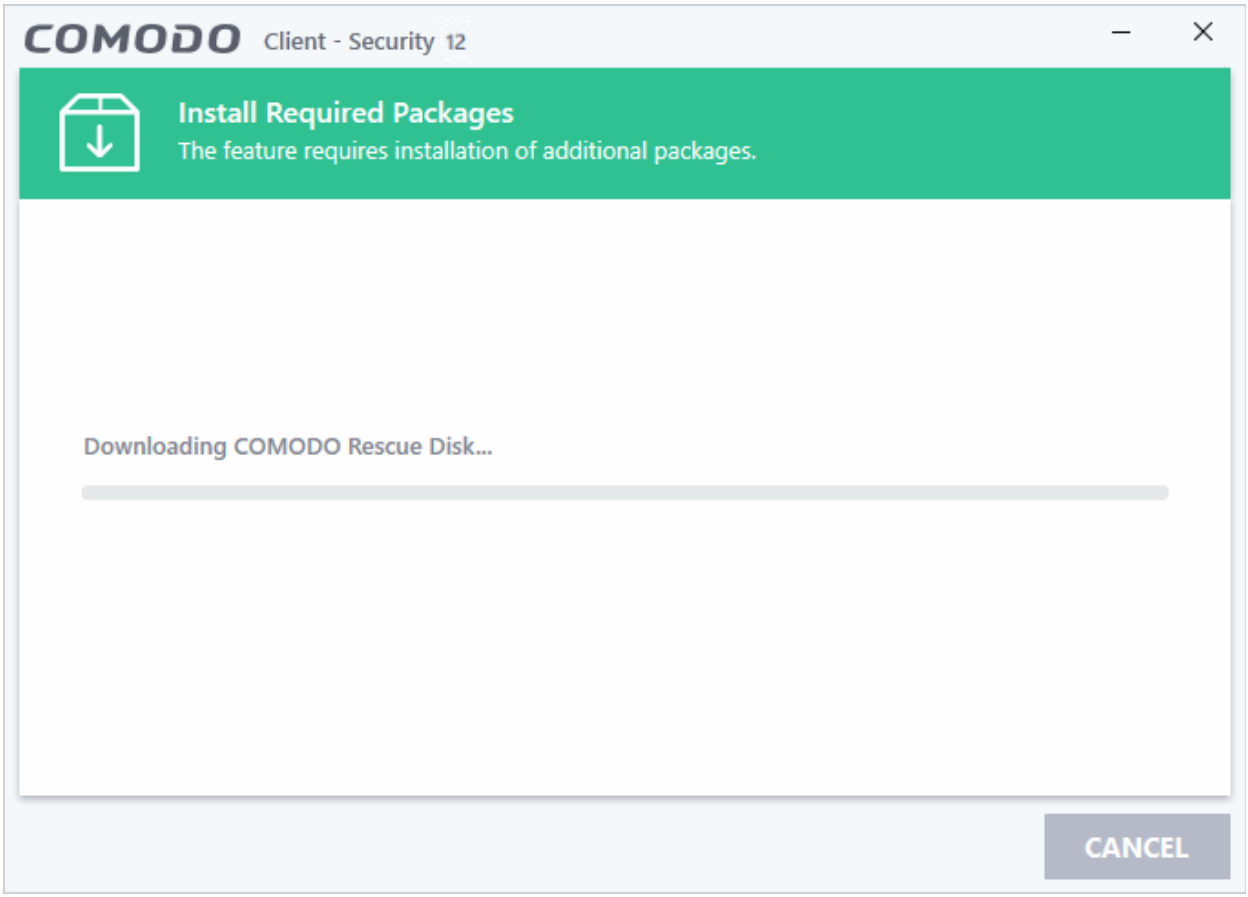
Burn to a USB drive

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

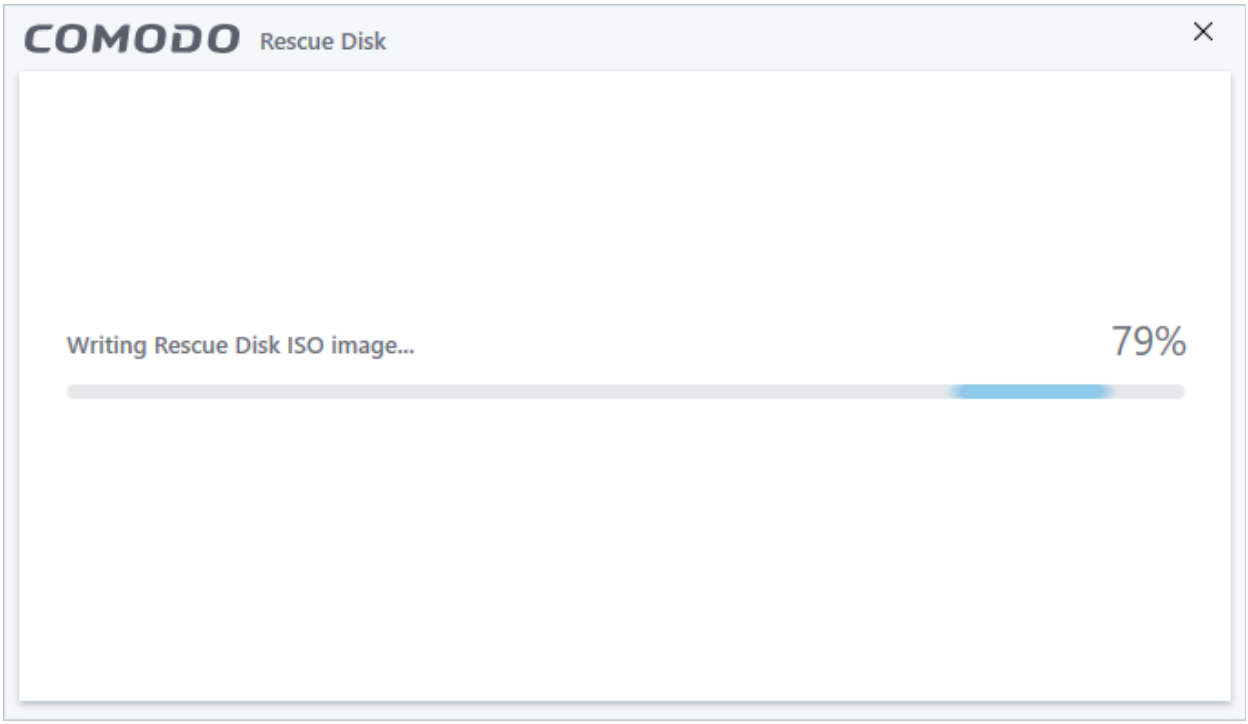


Step 3 - Burn the Rescue Disk

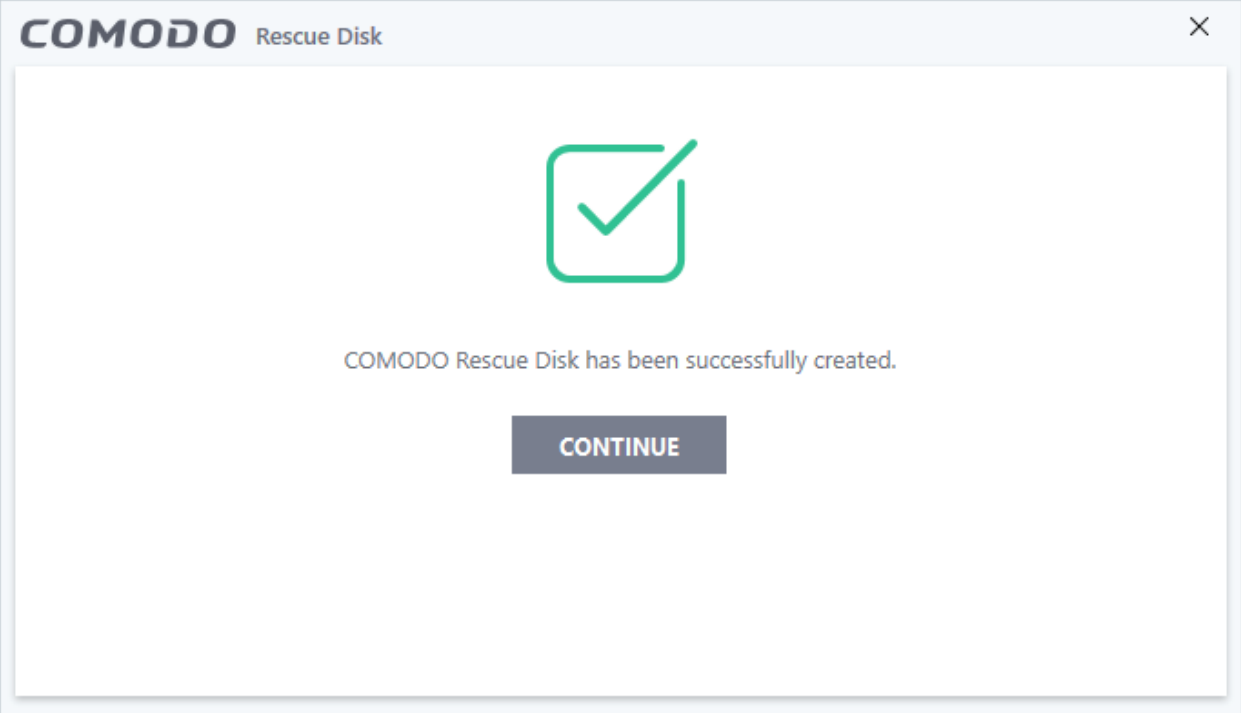
- Click 'Start'
- If you selected a local ISO in step 1 then burning will start immediately. If not, the ISO will be downloaded from Comodo servers:



After downloading, setup will burn the ISO to your target drive:



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



Your bootable Comodo Rescue Disk is ready.

- Click 'Continue' to go back to the CCS interface

6.2. Remove Deeply Hidden Malware

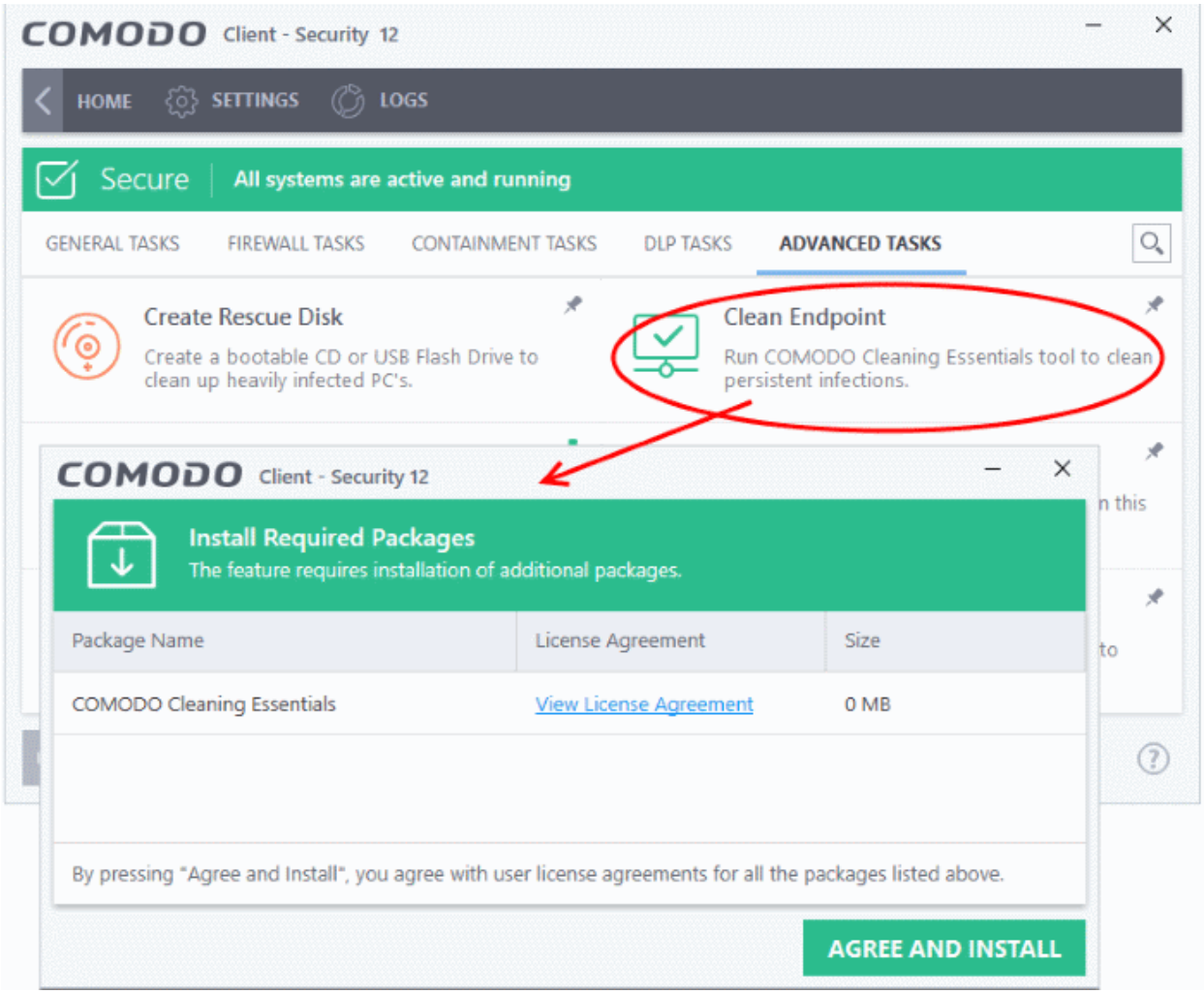
- Click 'Tasks' > 'Advanced Tasks' > 'Clean Endpoint'
- Comodo Cleaning Essentials (CCE) help users identify and remove malware and unsafe processes from infected computers.

Major features include:

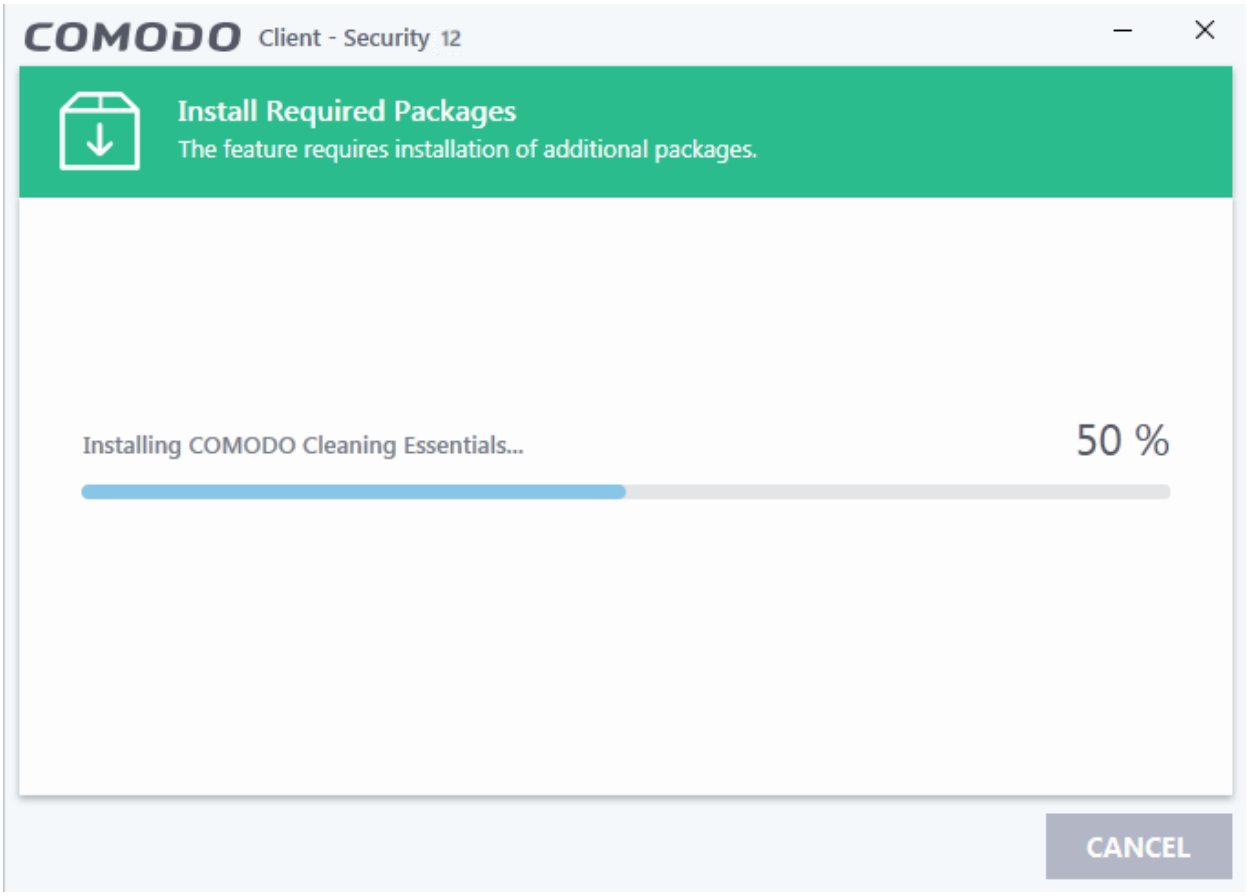
- **KillSwitch** - A system monitoring tool that lets you identify and terminate unsafe processes on your computer.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** -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

Run CCE from CCS interface

- Click 'Tasks' > 'Advanced Tasks' > 'Clean Endpoint'
- If you have already installed Comodo Cleaning Essentials, clicking 'Clean Endpoint' will open the CCE interface directly.
- When you click 'Clean Endpoint' for the first time, CCS will download and install Comodo Cleaning Essentials. After it is installed, clicking this tile in future will open the CCE interface.



- Click 'View License Agreement' to read the license agreement
- Click 'Agree and Install' to download and install the application.



After installation, the Comodo Cleaning Essentials application will open:

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

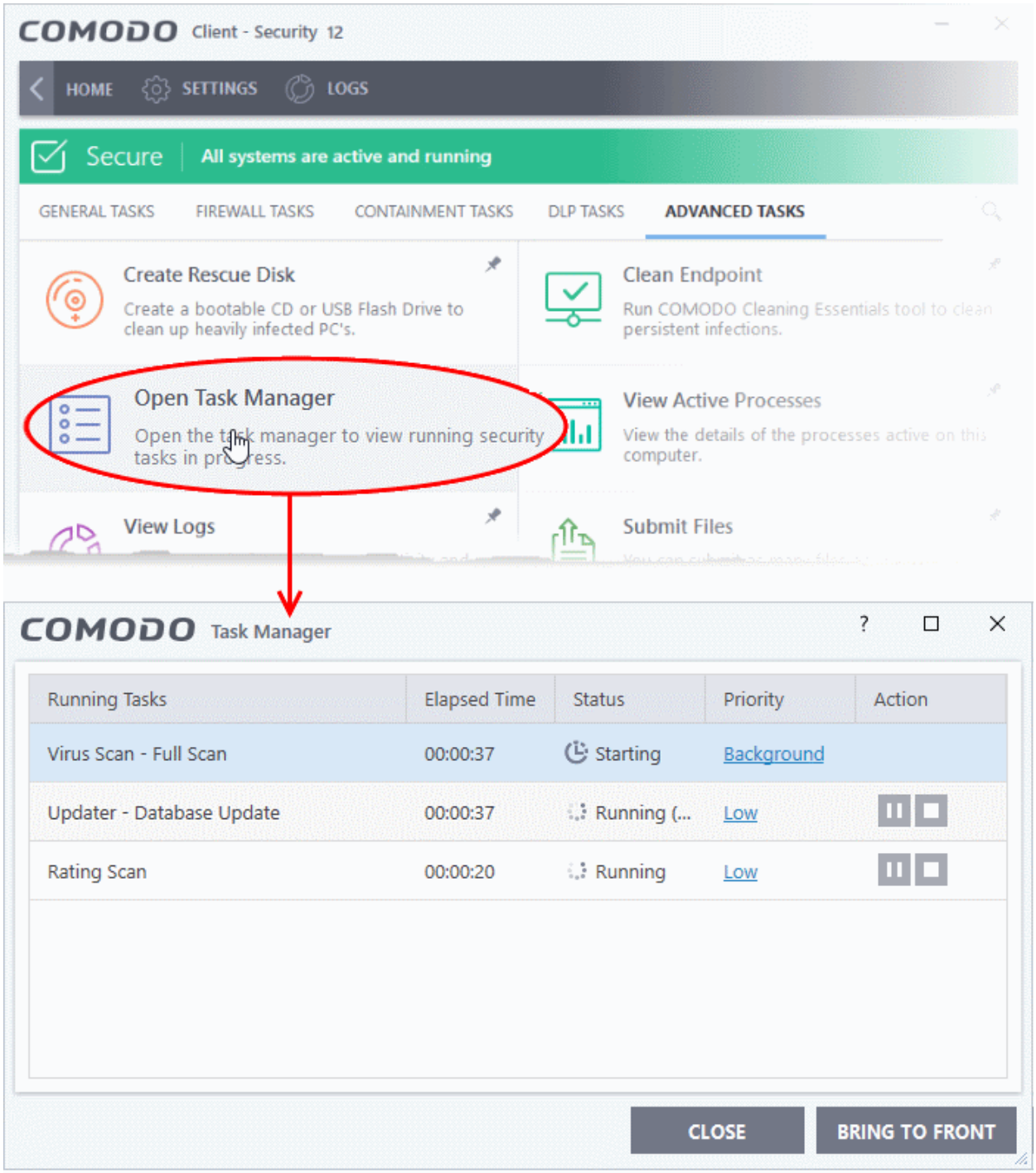
6.3. Manage CCS Tasks

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

- Comodo Client Security may have several tasks running simultaneously.
- For example, virus scans and virus database updates may run concurrently.
- The 'Task Manager' interface lets you view all currently running tasks.

Open the task manager

- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' > 'Open Task Manager'



From the 'Task Manager' interface, you can:

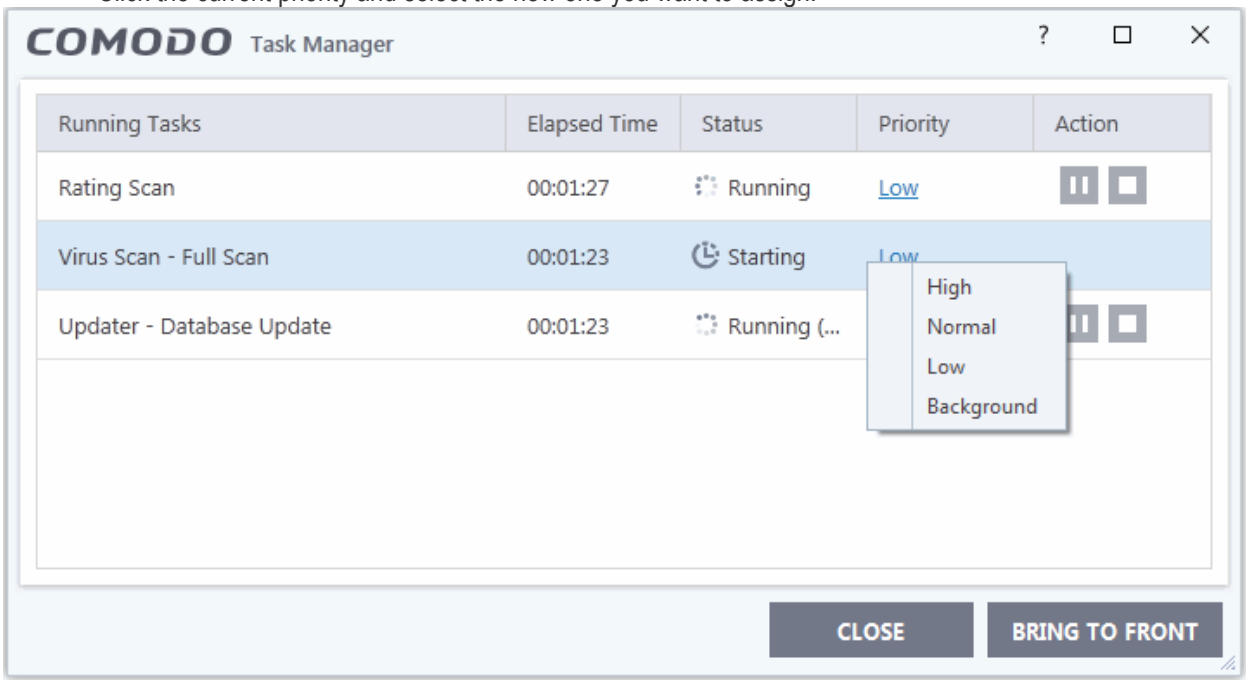
- **Reassign task priorities to the tasks**
- **Pause, resume, or stop a running task**
- **Bring a selected task to foreground**

Reassign task priorities

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

Change the priority of a task

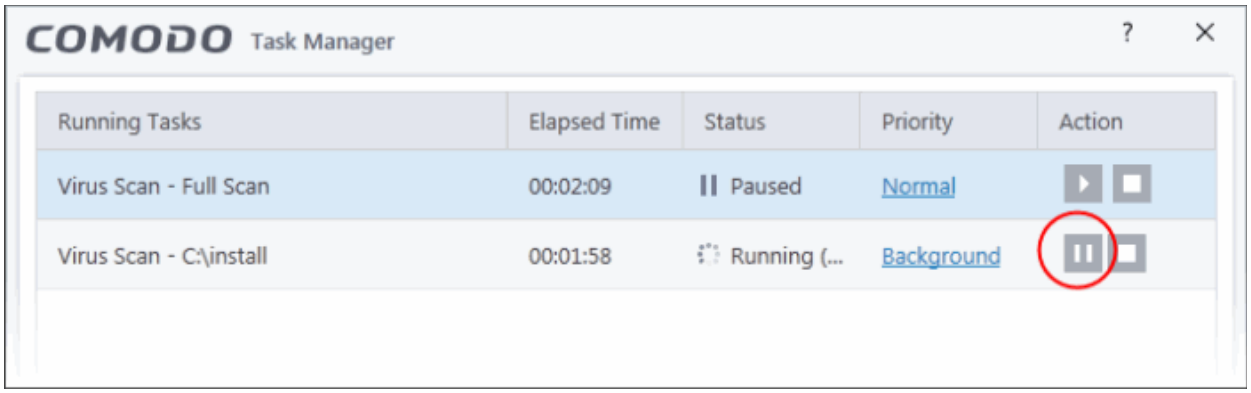
- Click the current priority and select the new one you want to assign:



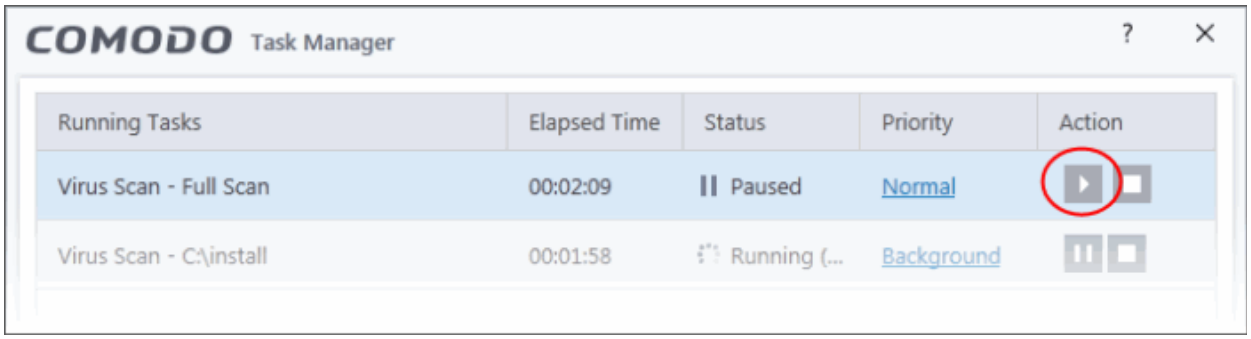
Pause/resume or stop running tasks

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

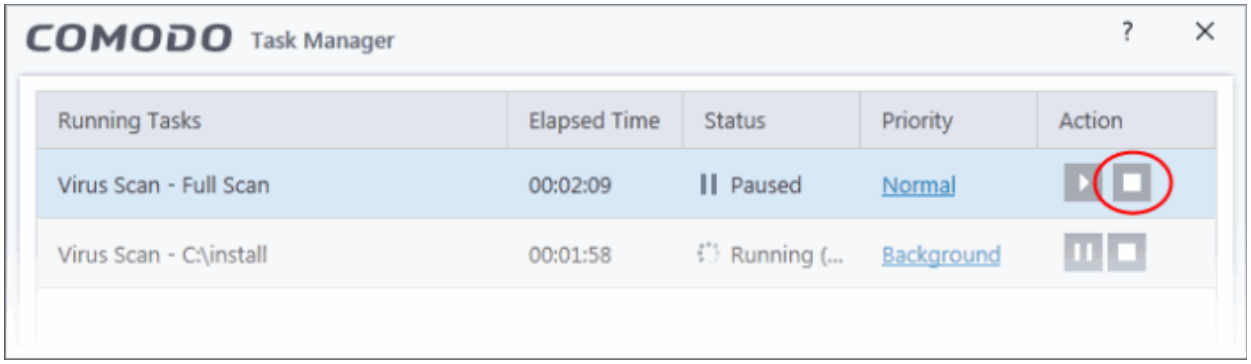
- Click the 'Pause' button to temporarily stop a running task



- Click the 'Resume' button to restart a suspended task

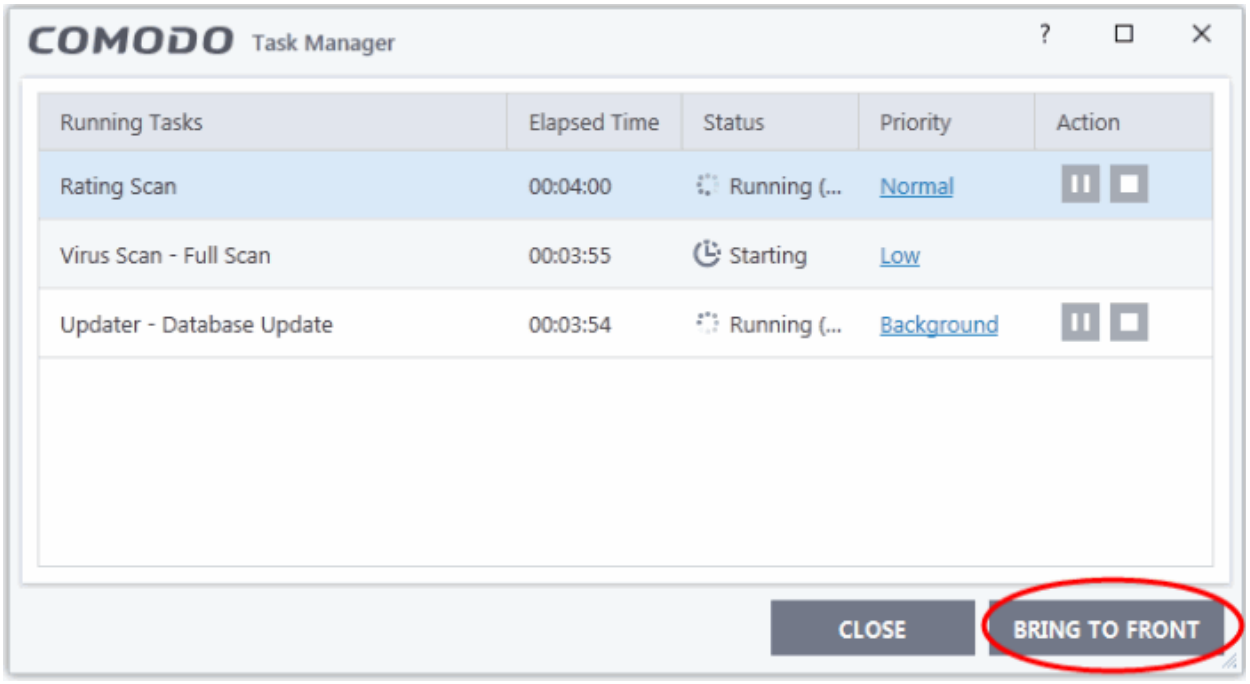


- Click the 'Stop' button to terminate a running task



Bring a running task to the foreground

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

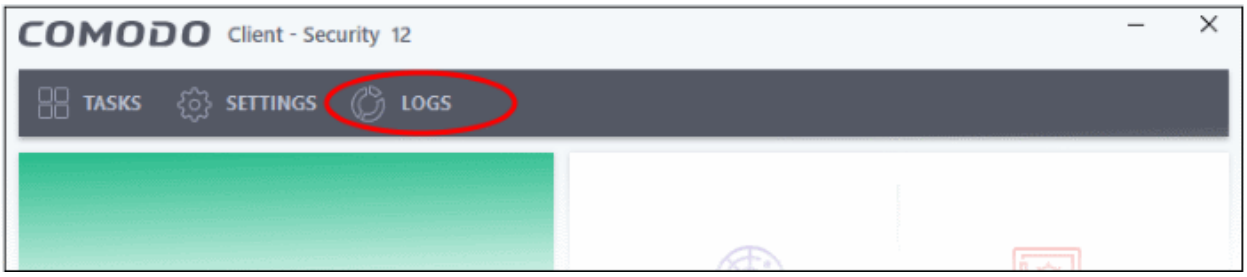


6.4. View CCS Logs

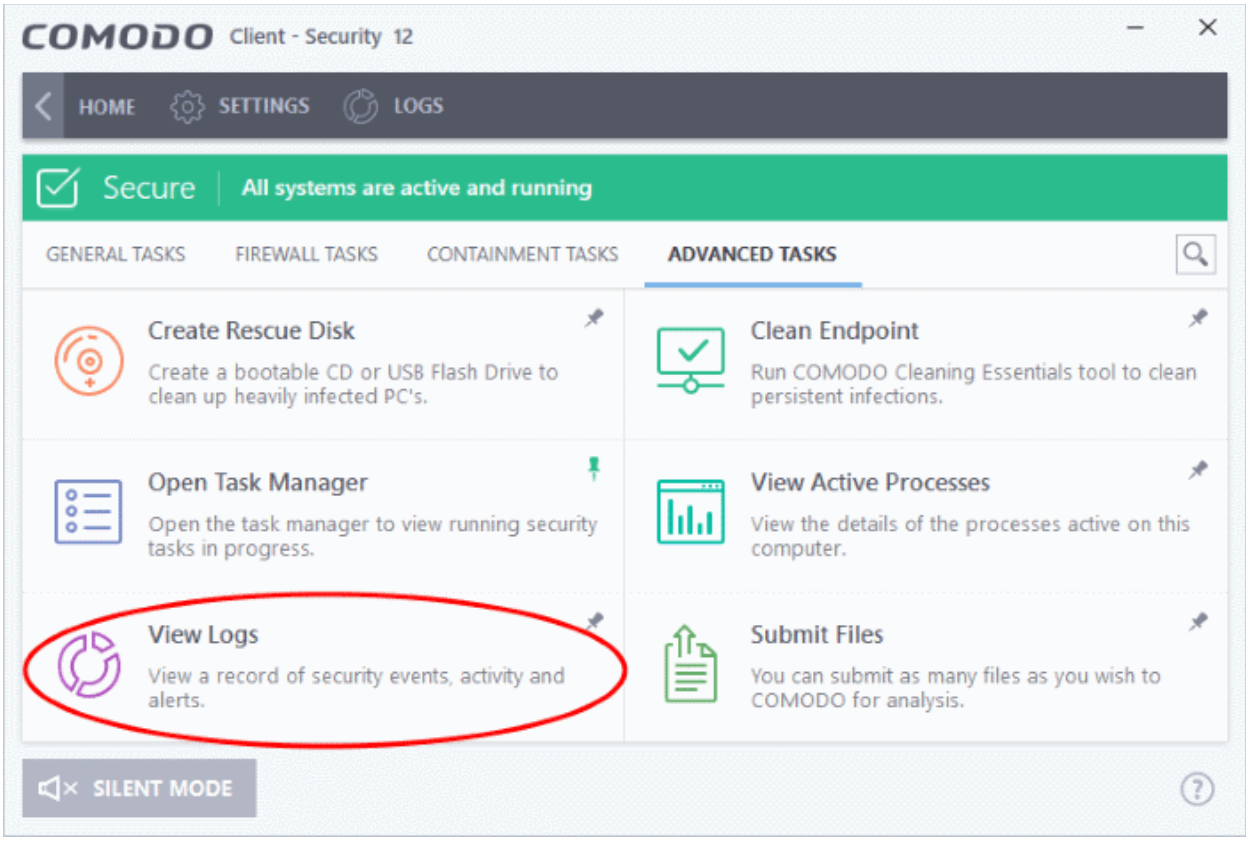
- Click 'Tasks' > 'Advanced Tasks' > 'View Logs'
- CCS logs all events generated by the antivirus, firewall, HIPS, containment and other modules.

There are three ways to open the log viewer:

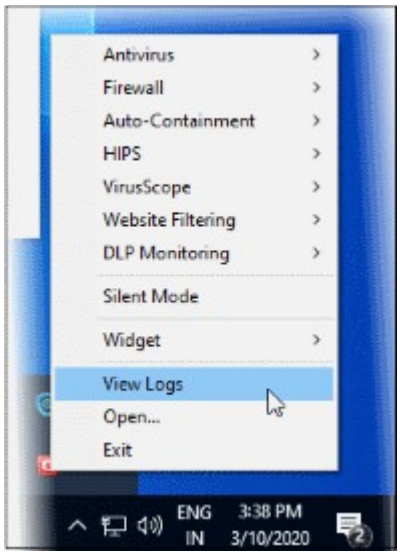
1. Click 'Logs' in the CCS menu bar:



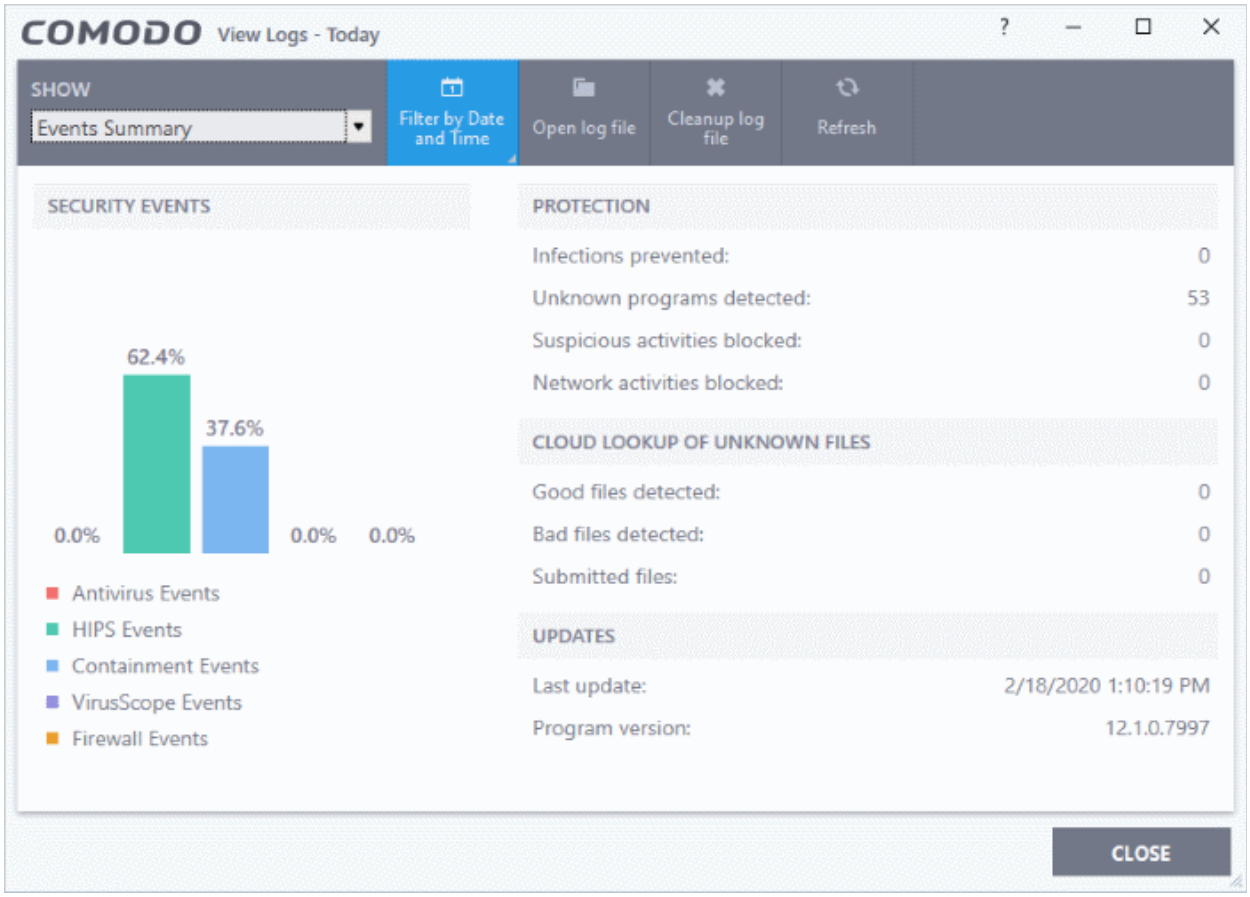
2. Click 'Tasks' on the CCS home screen then 'Advanced Tasks' > 'View Logs':



3. Right-click on the CCS tray icon then select 'View Logs':



The log dashboard shows a summary of events on the endpoint:

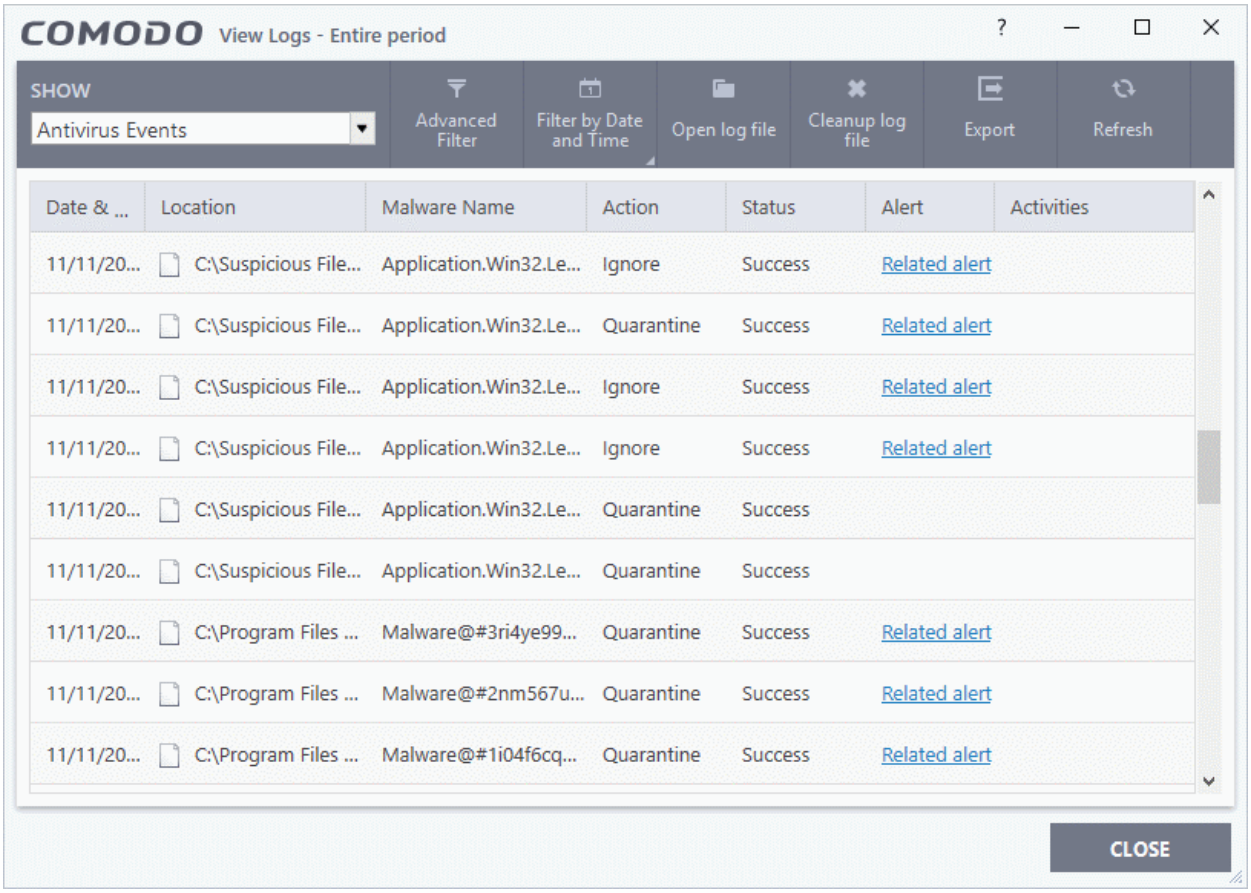


Use the drop-down at top-left to view a specific type of log:

- **Antivirus**
- **VirusScope**
- **Firewall**
- **HIPS**
- **Containment**
- **Website Filtering**
- **Device control**
- **Autorun events**
- **Alerts displayed**
- **Tasks launched**
- **File List settings changes**
- **Vendors List changes**
- **Configuration changes**
- **Virtual Desktop events**
- **Data Loss Prevention events**
- **Search and Filter logs**

6.4.1. Antivirus Logs

- Click 'Logs' in the CCS menu bar
- Select 'Antivirus Events' from the drop-down at upper-left
- Antivirus logs contains stats about scanned objects, the settings used for each task, and a history of actions performed on individual files. Logs are recorded for real-time protection events, antivirus database updates and more.



- **Date & Time** - When the event occurred.
- **Location** - The installation path of the suspicious application
- **Malware Name** - The malicious item that was detected
- **Action** - How the malware was handled by CCS.
- **Status** - Whether the action taken was a success or failure
- **Alert** - Click 'Related Alert' to view the notification generated by the event

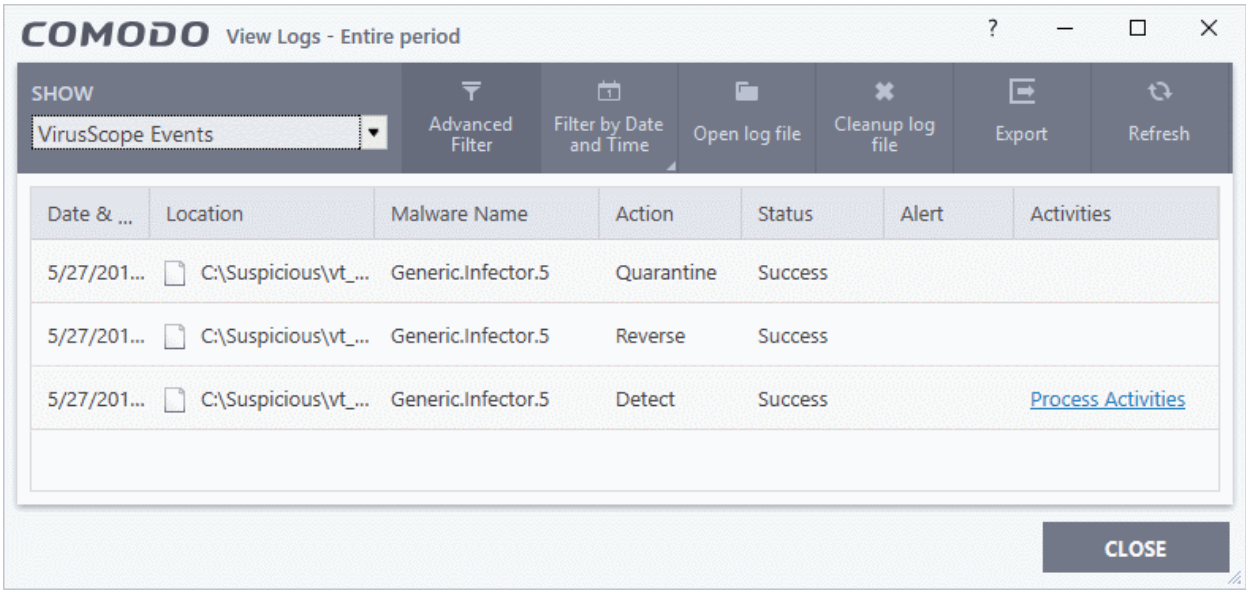
Note: Alerts are only shown if 'Do not Show Antivirus Alerts' is disabled in 'Settings' > 'Antivirus' > 'Real-time Scan'.

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

- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs
- Click any column header to sort the entries in ascending \ descending order.

6.4.2. VirusScope Logs

- Click 'Logs' in the CCS menu bar
- Select 'VirusScope Events' from the drop-down at upper-left

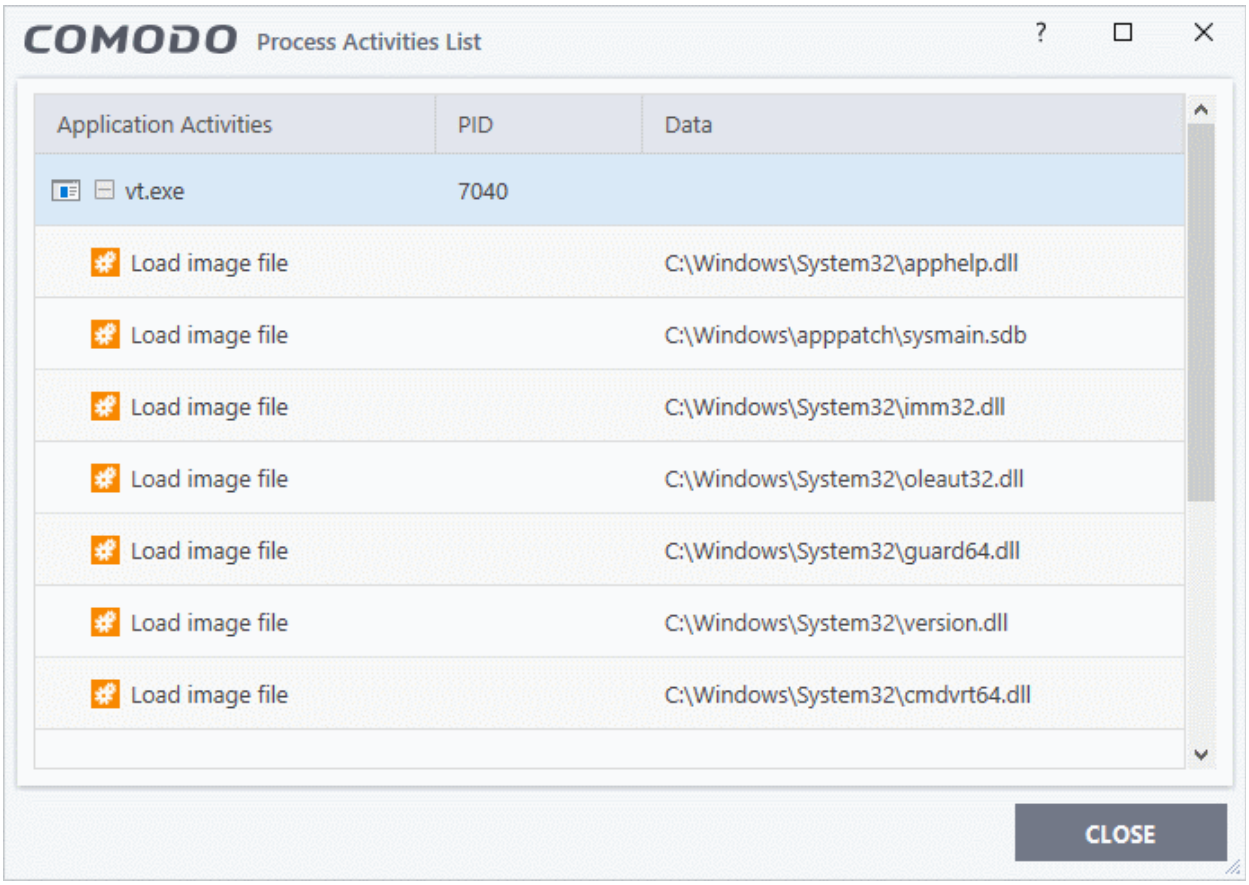


- **Date & Time** - When the event occurred.
- **Location** - The installation path of the suspicious application
- **Malware Name** - The malicious item that was detected
- **Action** - How VirusScope handled the malware.
  - **Reverse** - VirusScope attempted to undo any changes made by the malicious item
  - **Quarantine** - VirusScope placed the suspicious file in quarantine
  - **Detect** - VirusScope observed malicious activity, but did not quarantine the file or reverse its changes
  - **Ask** - VirusScope detected malicious activity and showed an alert. The alert asks whether you want to quarantine the file or reverse its changes
- **Status** - Whether the action taken was a success or failure
- **Alert** - Click 'Related Alert' to view the notification generated by the event

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

See **VirusScope Configuration** for more details.

- **Activities** - Click 'Related Alert' to view the notification generated by the event. An example is shown below:

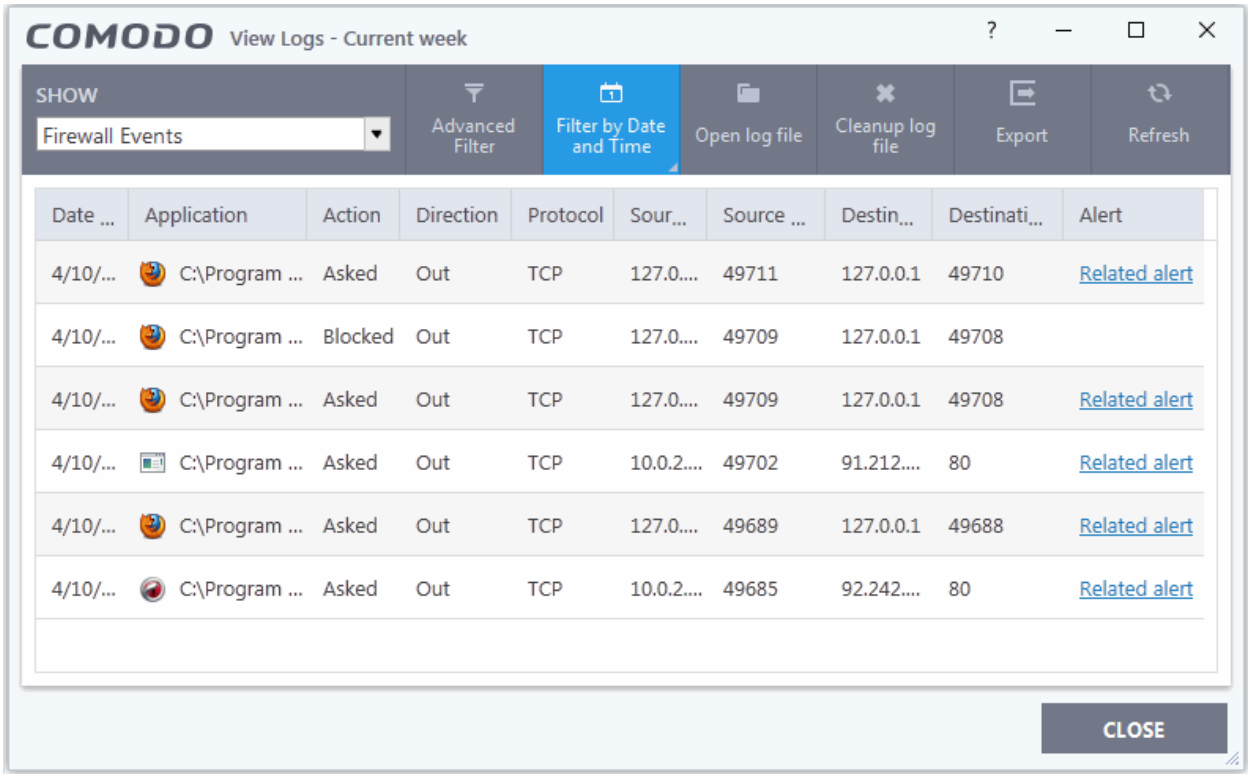


- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs
- Click any column header to sort the entries in ascending \ descending order

6.4.3. Firewall Logs

- Click 'Logs' in the CCS menu bar
- Select 'Firewall Events' from the drop-down at upper-left

Firewall events are created for various reasons. Reasons include when a process attempts a connection that breaks a **firewall rule**, or when there is a change in firewall settings.



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

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

See **General Firewall Settings** for more details.

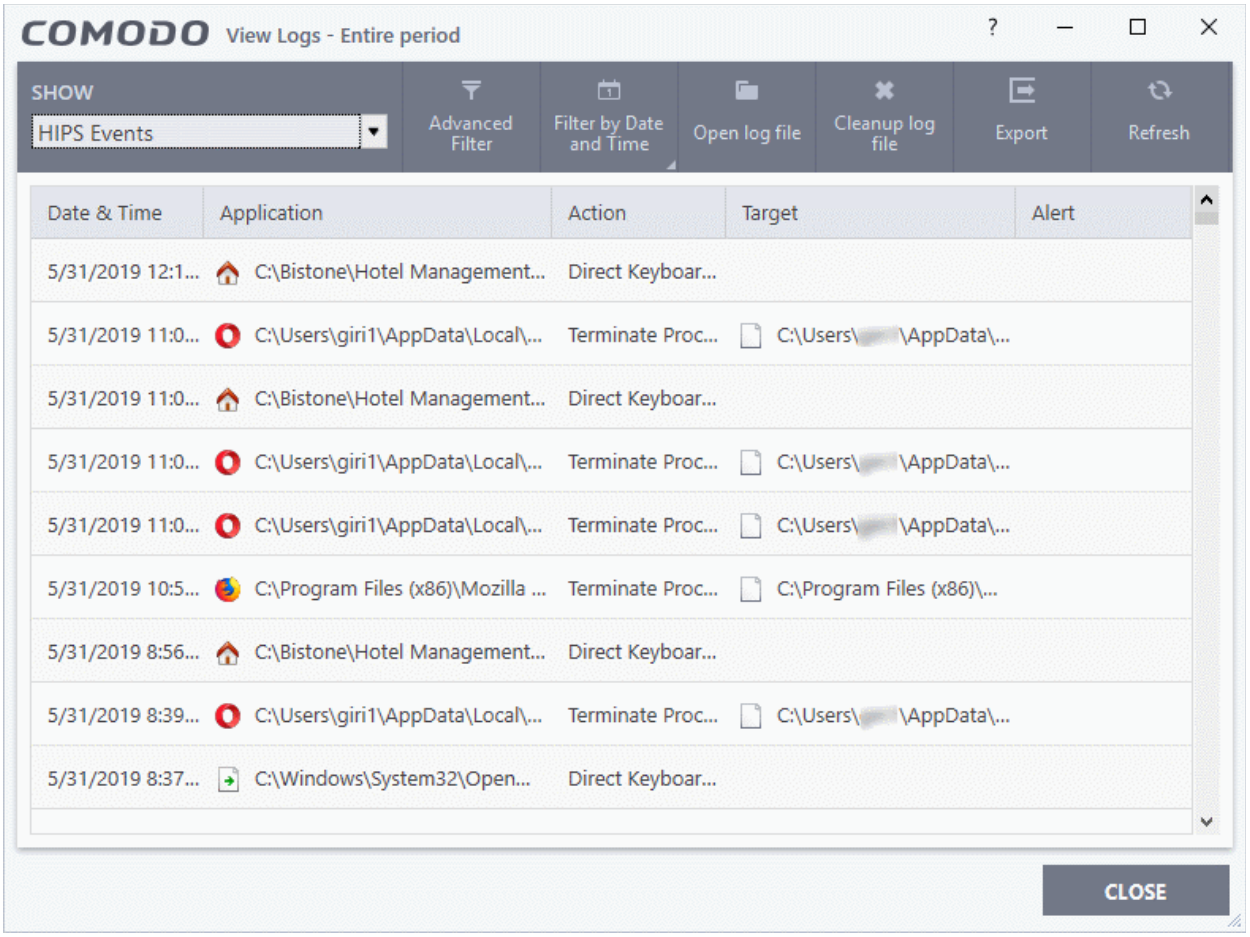
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs

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

6.4.4. HIPS Logs

- Click 'Logs' in the CCS menu bar
- Select 'HIPS Events' from the drop-down at upper-left

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



- **Date & Time** - When the event occurred.
- **Application** - The name of the program or process that caused the event.
- **Action** - The activity of the application and how HIPS handled it
  - If the action was allowed to proceed then this column will show the result of that action.
  - Click the 'Related Alert' link to see the notification that was shown at the time.
  - This column will state 'Block File' if the action was not allowed.
- **Target** - Location of the file, COM interface or registry key accessed by the process.
- **Alert** - Click 'Related Alert' to view the notification generated by the event

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

See **HIPS Settings** for more details.

- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.

- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs

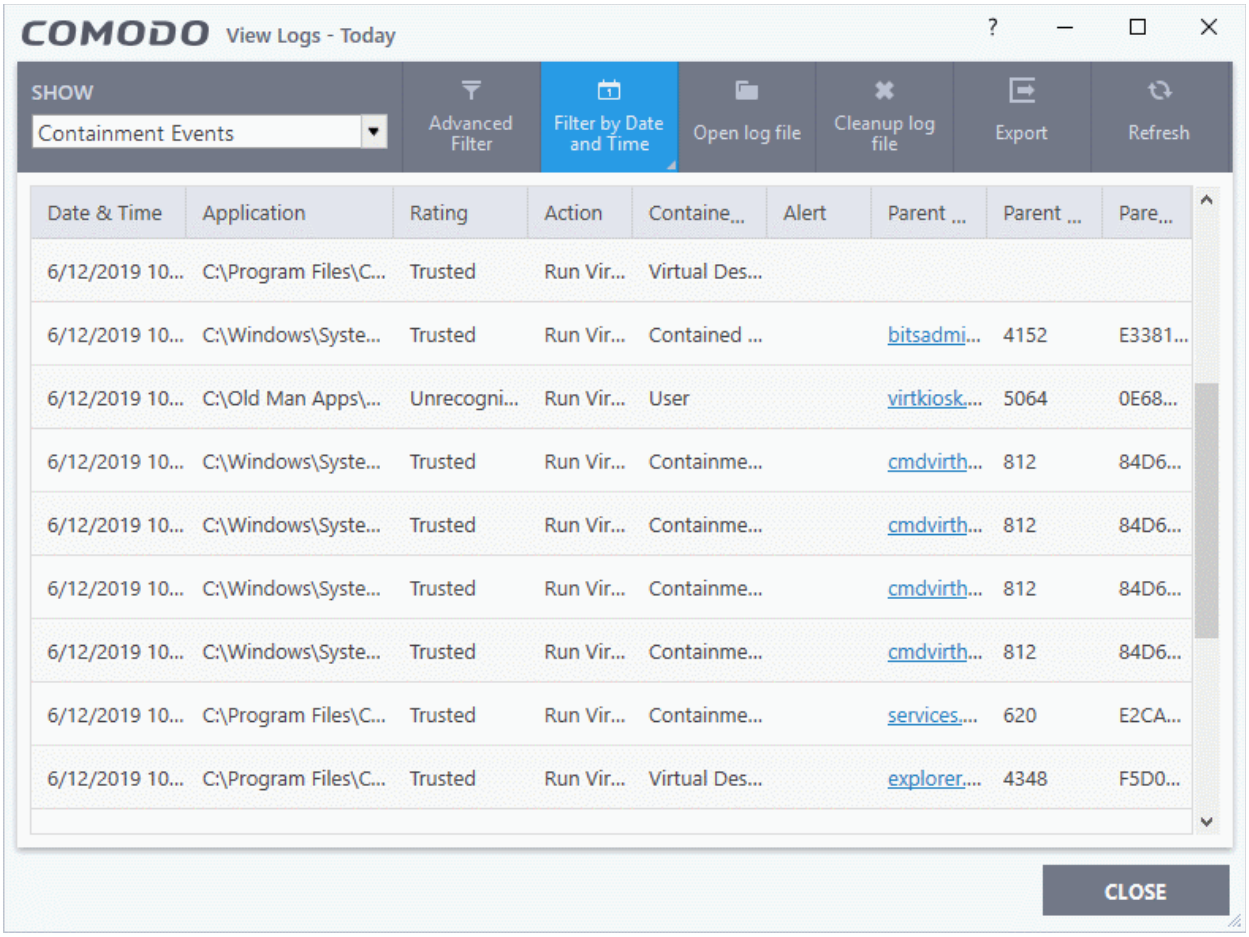
Click any column header to sort the entries in ascending \ descending order

6.4.5. Containment Logs

- Click 'Logs' in the CCS menu bar
- Select 'Containment Events' from the drop-down at upper-left

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

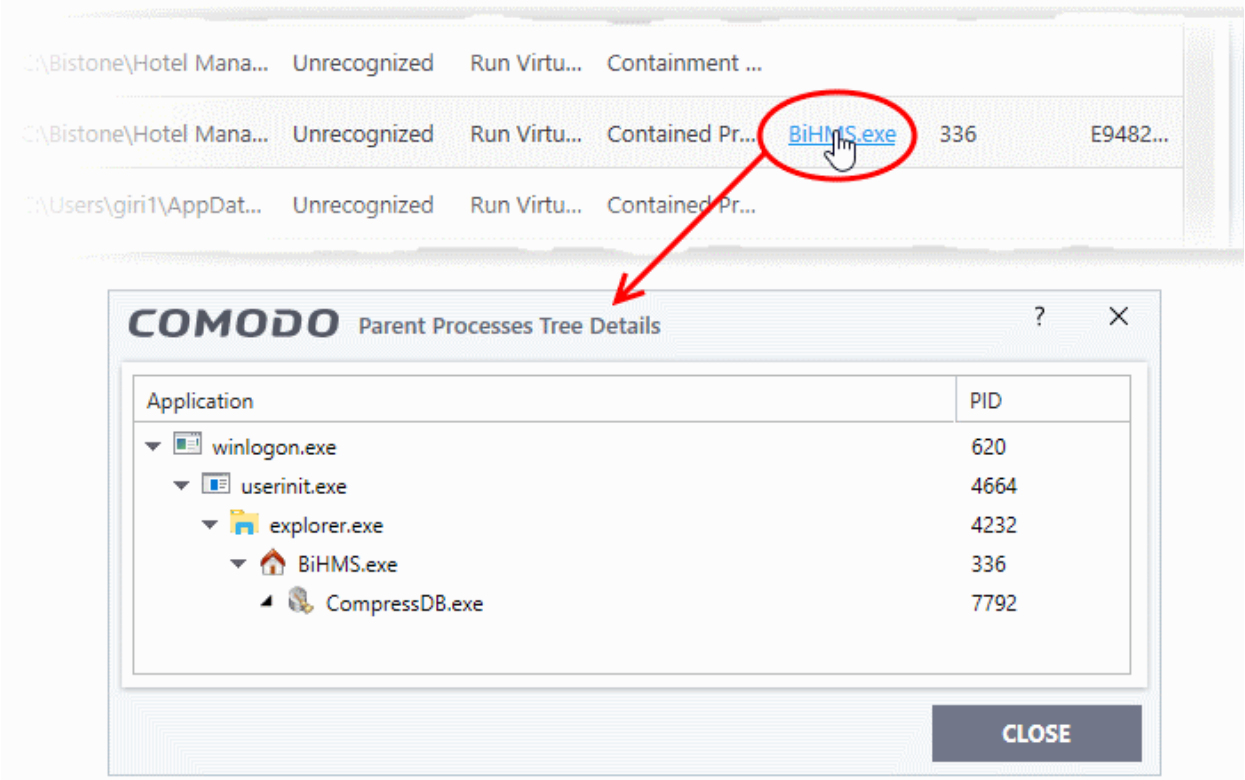
- When you manually run an application in the container
- When an an auto-containment rule runs an application in the container



- **Date & Time** - When the event occurred.
- **Application** - The installation path of the application that was run in the container
- **Rating** - The reputation of the contained application. The trust rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Unrecognized files are run in the container until such time as they can be classified as 'Trusted' or 'Malicious'.
- **Action** - How the malware was handled by CCS. This is also the restriction level imposed on the application by the container.
- **Contained by** - The CCS service, policy or user that placed the application in the container.
- **Alert** - Click 'Related Alert' to view the notification generated by the event

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

- **Parent Process** - The program which spawned the contained process.
  - Click the name of the parent process to view the hierarchical order of processes



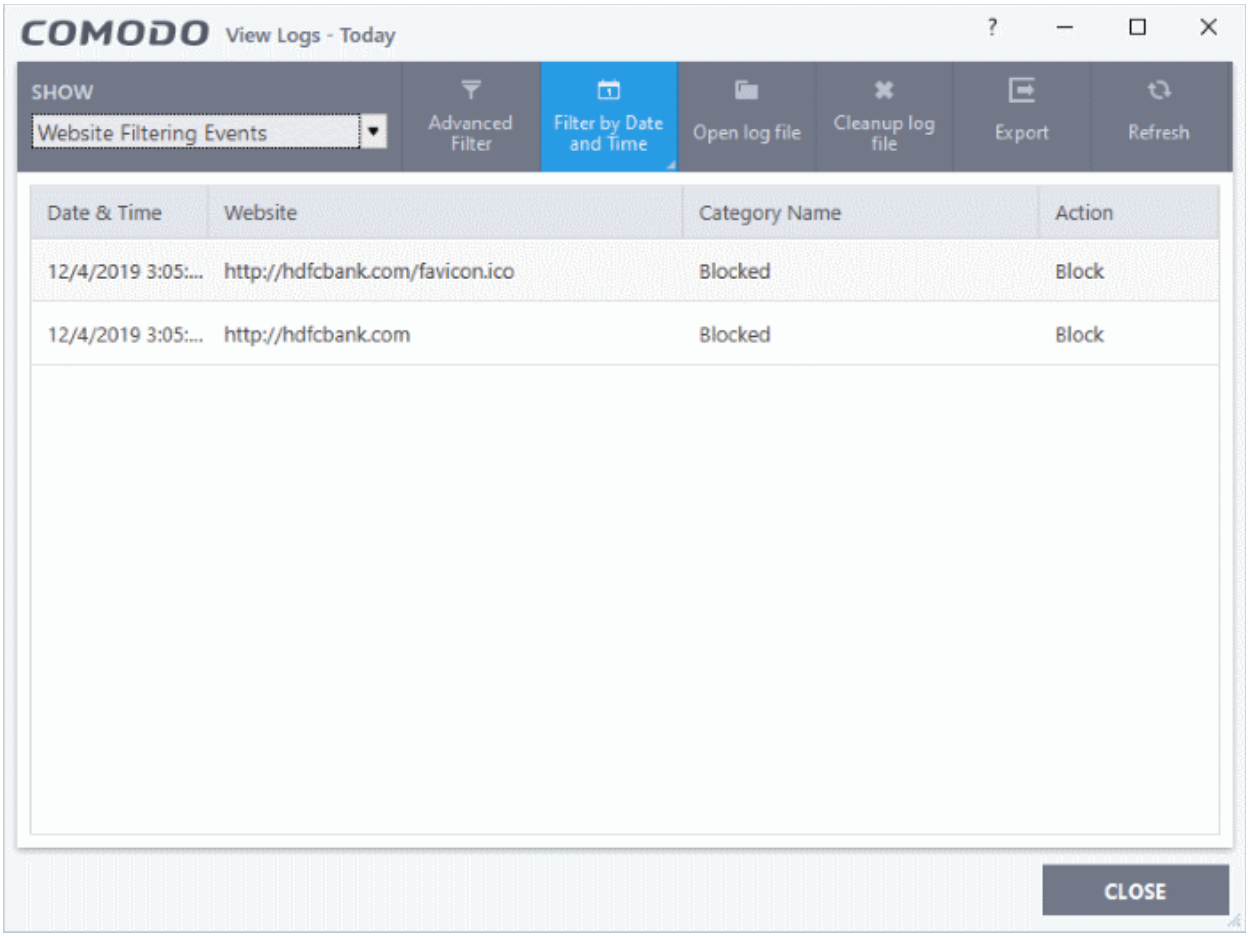
- **Parent Process ID** - The unique identifier that points to the process
- **Parent process hash** - The SHA1 hash value of the program which spawned the contained process.
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs
- Click any column header to sort the entries in ascending \ descending order.

6.4.6. Website Filtering Logs

- Click 'Logs' in the CCS menu bar
- Select 'Website Filtering Events' from the drop-down at upper-left

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

Background Note:
- You can create filtering rules for specific users in 'Advanced Settings' > 'Website Filtering'.
- See '**Website Filtering**' for more details.



- **Date & Time** - When the event occurred.
- **Website** - The URL of the site that was blocked, or allowed.
- **Category** - The genre of the website. Example categories include 'Shopping sites', 'Social Media', 'Boutiques' etc. You can manage categories in 'Advanced Settings' > 'Website Filtering'.
- **Action** - How the filter reacted to the connection attempt. For example, whether the attempt was allowed, blocked or an alert shown to the user.
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log.
- **Refresh** - Reload the current list and show the latest logs.

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

6.4.7. Device Control Logs

- Click 'Logs' in the CCS menu bar
- Select 'Device Control Events' from the 'Show' drop-down

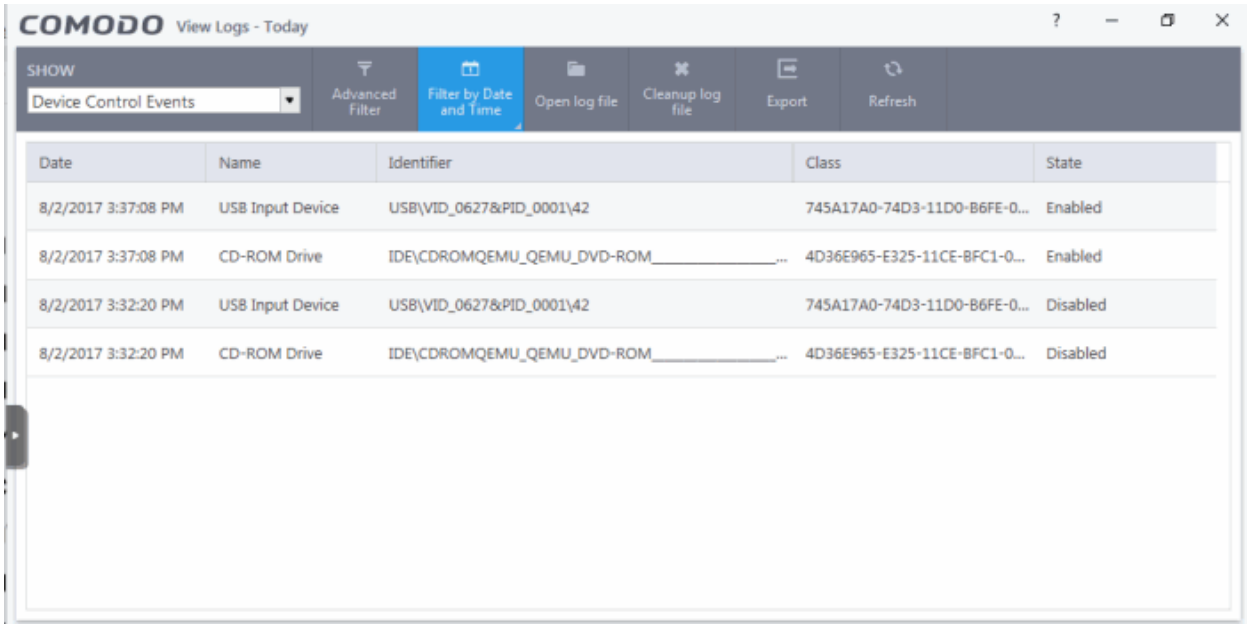
Device control logs record events related to external devices. External devices include USB, optical, and storage drives plugged into your computer.

Events logged include:

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

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

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



- **Date** - When the event occurred.
- **Name** - The type of device associated with the event.
- **Identifier** - The identification string of the device
- **Class** - The GUID (Globally Unique Identifier) string of the category of the device as defined by the Windows operating system.
- **State** - Whether the device was allowed or blocked.
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs
- Click any column header to sort the entries in ascending \ descending order.

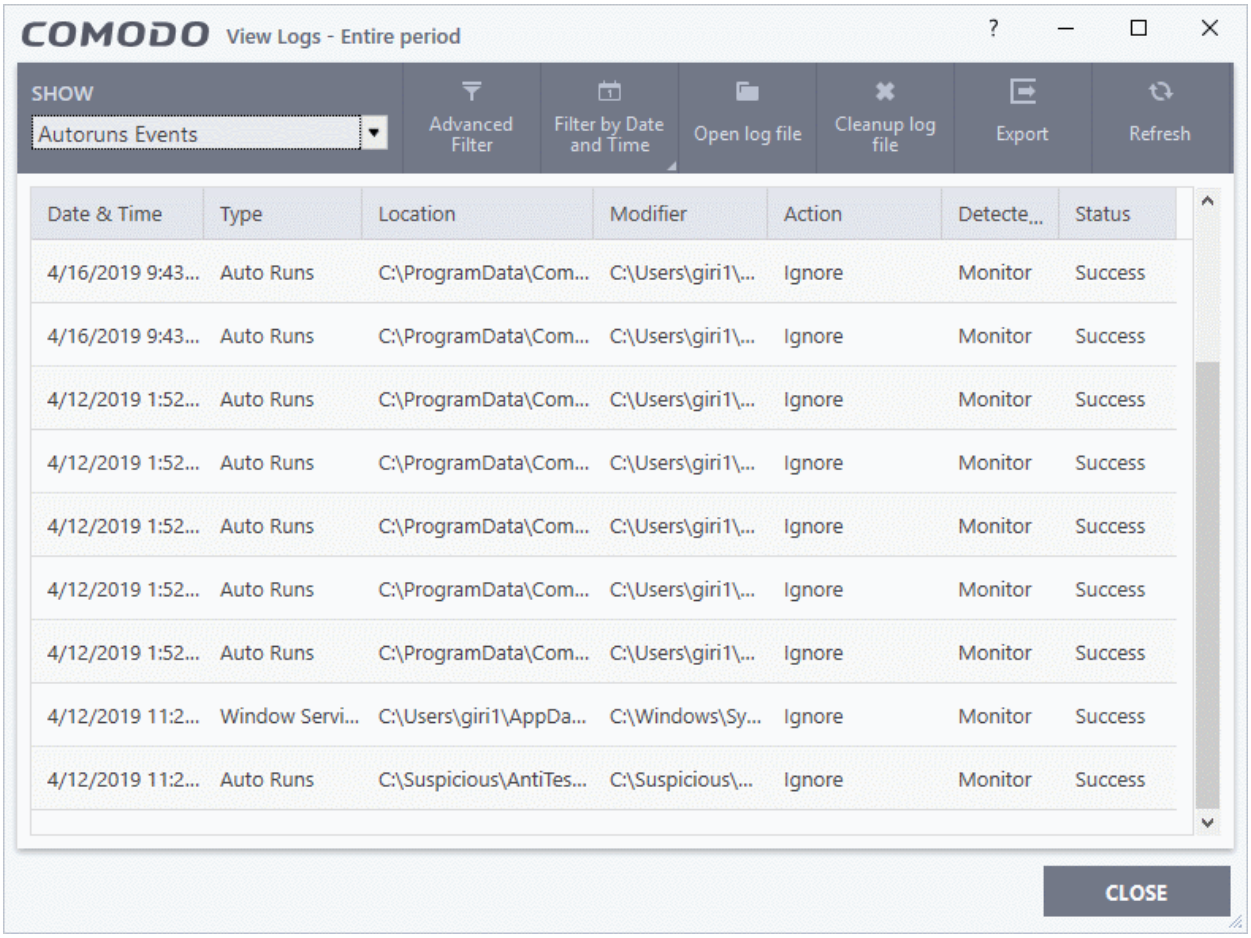
6.4.8. Autorun Event Logs

- Click 'Logs' in the CCS menu bar
- Select 'Autorun Events' from the drop-down at upper-left

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

Background:

- CCS monitors changes to registry items related to Windows Services, Autorun entries and scheduled tasks.
- You can define the response CCS should take against unrecognized autoruns in 'Advanced Settings' > 'Advanced Protection' > 'Miscellaneous'. See **Miscellaneous Settings** for more details.
- You can also define the response to unknown autoruns found by an antivirus scan. See **configure scan options** for more help on this.

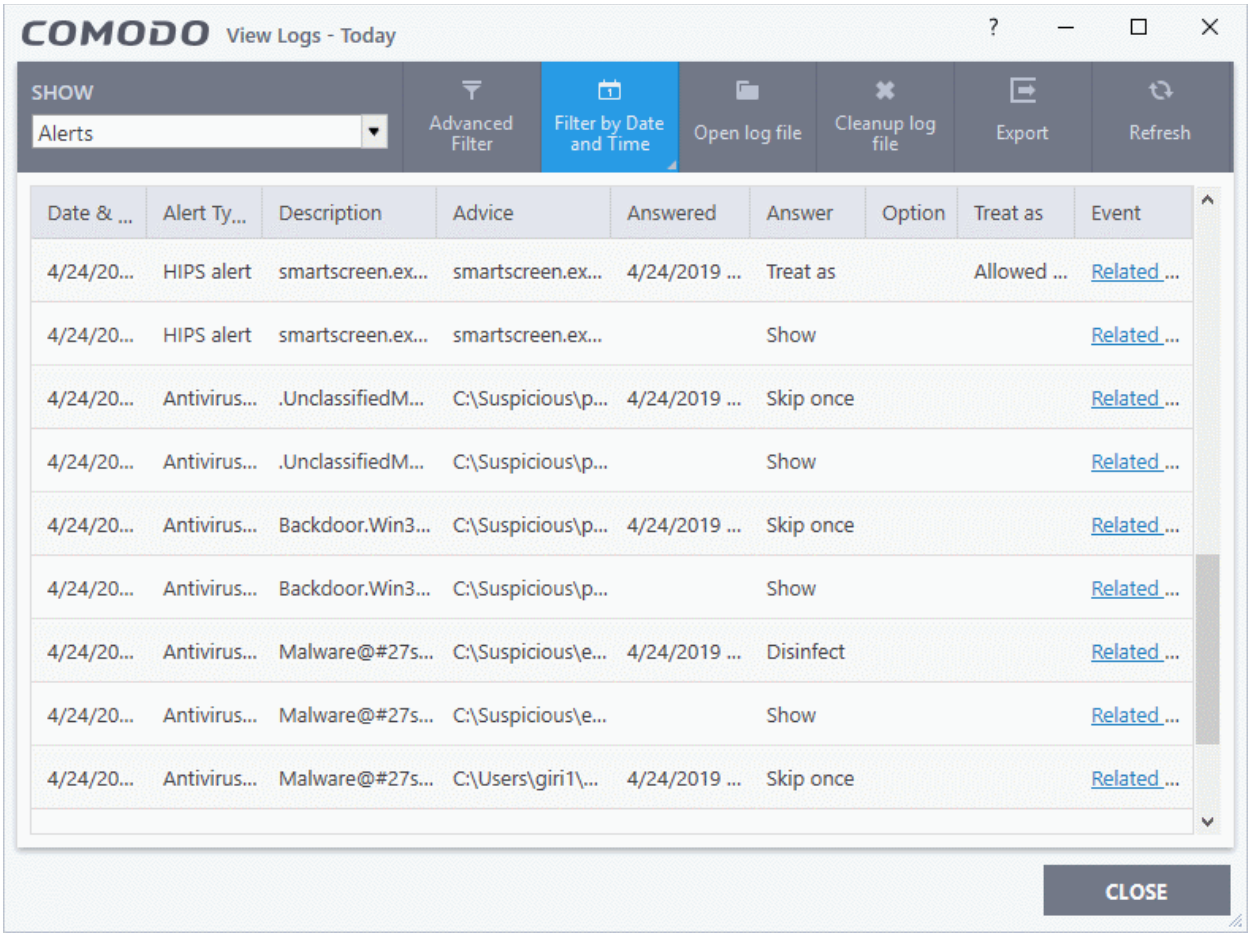


- **Date & Time** - When the event occurred.
- **Type** - Whether the detected item is an autorun entry, Windows service, or scheduled task.
- **Location** - The installation path of the affected item, or the location of the new item
- **Modifier** - The location of the application that made the change.
- **Action** - How CCS responded to the event.
- **Status** - Whether the action taken was a success or failure
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs
- Click any column header to sort the entries in ascending \ descending order

6.4.9. Alert Logs

- Click 'Logs' in the CCS menu bar
- Select 'Alerts' from the drop-down at upper-left

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



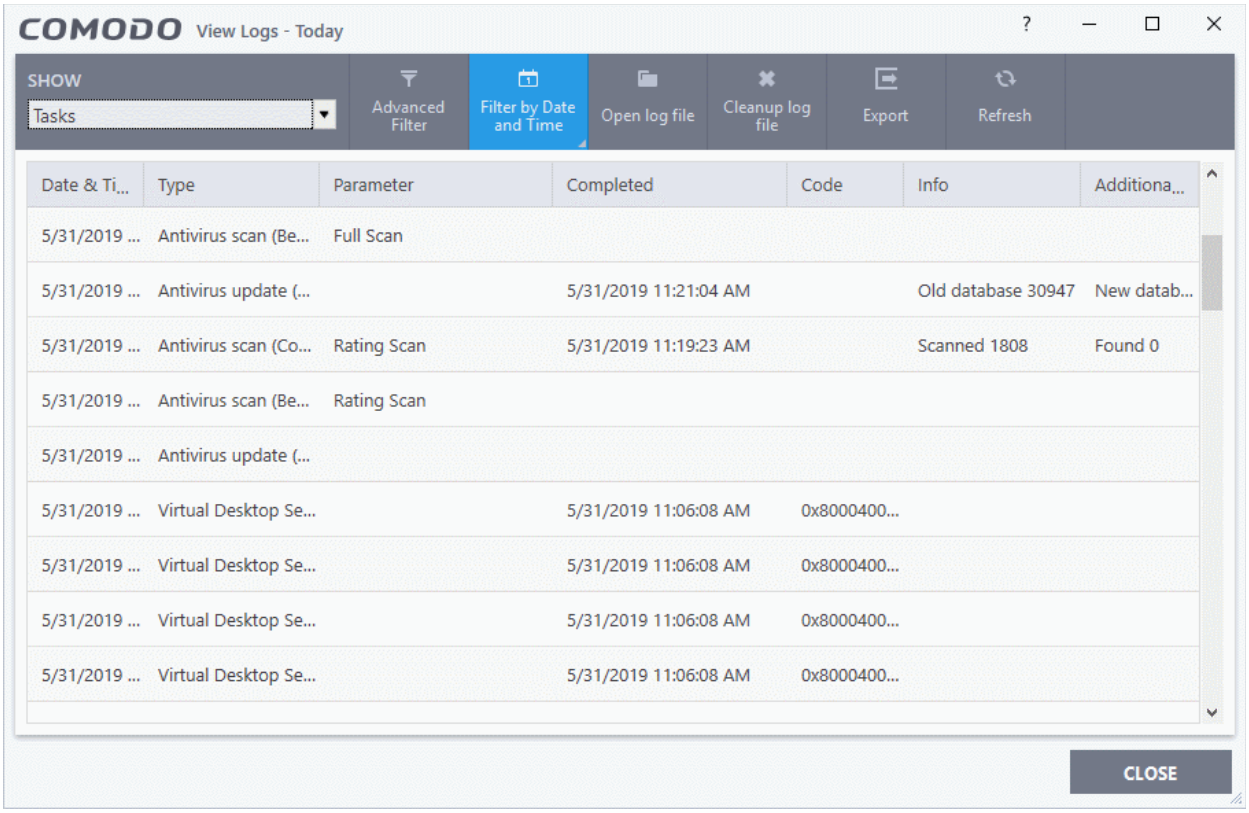
- **Date & Time** - When the event occurred.
- **Alert Type** - The security module that generated the alert. Alert types include antivirus, firewall, HIPS, containment, VirusScope and secure shopping.
- **Description** - Name of the file or event that caused the alert.
- **Advice** -The recommendation, or informational text in the alert. This text is intended to help users decide to respond to the threat.
- **Answered** - Whether or not the alert was answered by the user. You will see the date and time of the response if an answer was provided.
- **Answer** - The user's response to the alert. For example, 'Allow', 'Block', 'Disinfect', 'Skip'.
- **Option** - Additional settings chosen by the user at the alert. For example, 'Remember My Answer'.
- **Treat As** - Whether or not the user applied a specific ruleset to the file at the alert. The ruleset tells CCS the restriction level to apply to the file in future. Example rulesets include 'Treat as a safe application, or 'Treat as an installer'.
- **Event** - Click 'Related Event' to view more details about the incident that triggered the alert.
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Refresh** - Reload the current list and show the latest logs

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

6.4.10. CCS Tasks Logs

- Click 'Logs' in the CCS menu bar
- Select 'Tasks' in the drop-down at upper-left

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



- **Date & Time** - When the event occurred.
- **Type** - The task that was performed. For example, 'Antivirus scan', or 'Database update'.
- **Parameter**:
  - The sub-type of the operation. For example, 'Quick Scan' is a sub-type of 'Antivirus scan'.
    OR
  - The target of the operation. For example, 'C:\Program Files' is the target area scanned.
- **Completed** - The time that the operation finished
- **Code** - Error code generated by Windows for CCS tasks that were not successful. No code is shown if the task finished successfully.
- **Info and additional info** - Shows further details about the task. For update tasks, these fields show the old and new version numbers. For scan tasks, they show the number of items scanned and the number of viruses found.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Refresh** - Reload the current list and show the latest logs

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

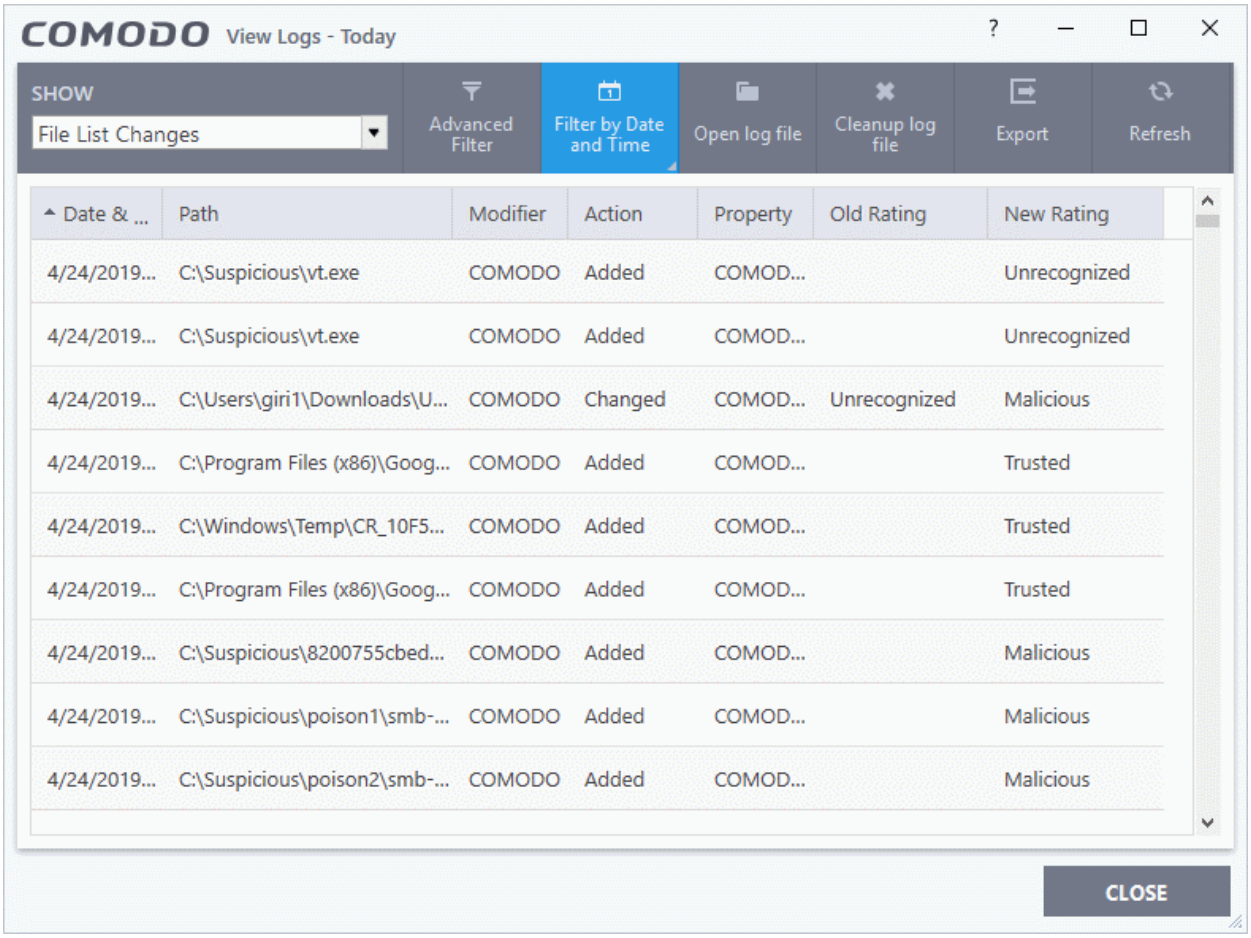
6.4.11. File List Changes Logs

- Click 'Logs' in the CCS menu bar
- Select 'File List Changes' in the drop-down at upper-left

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

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

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



- **Date & Time** - When the event occurred.
- **Path** - The location or the SHA 1 hash value of the file that was changed.
- **Modifier** - The service or user that made the change.
- **Action** - Whether the file was added, removed, or assigned a new rating
- **Property** - Whether the current trust rating was assigned by Comodo, an administrator, or a user.
- **Old Rating** - The trust rating of the file before the change.
    - The rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Under default settings, unrecognized files are run in the container until Comodo classifies them as 'Trusted' or 'Malicious'.
- **New Rating** - The trust rating of the file after the change.
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log.

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

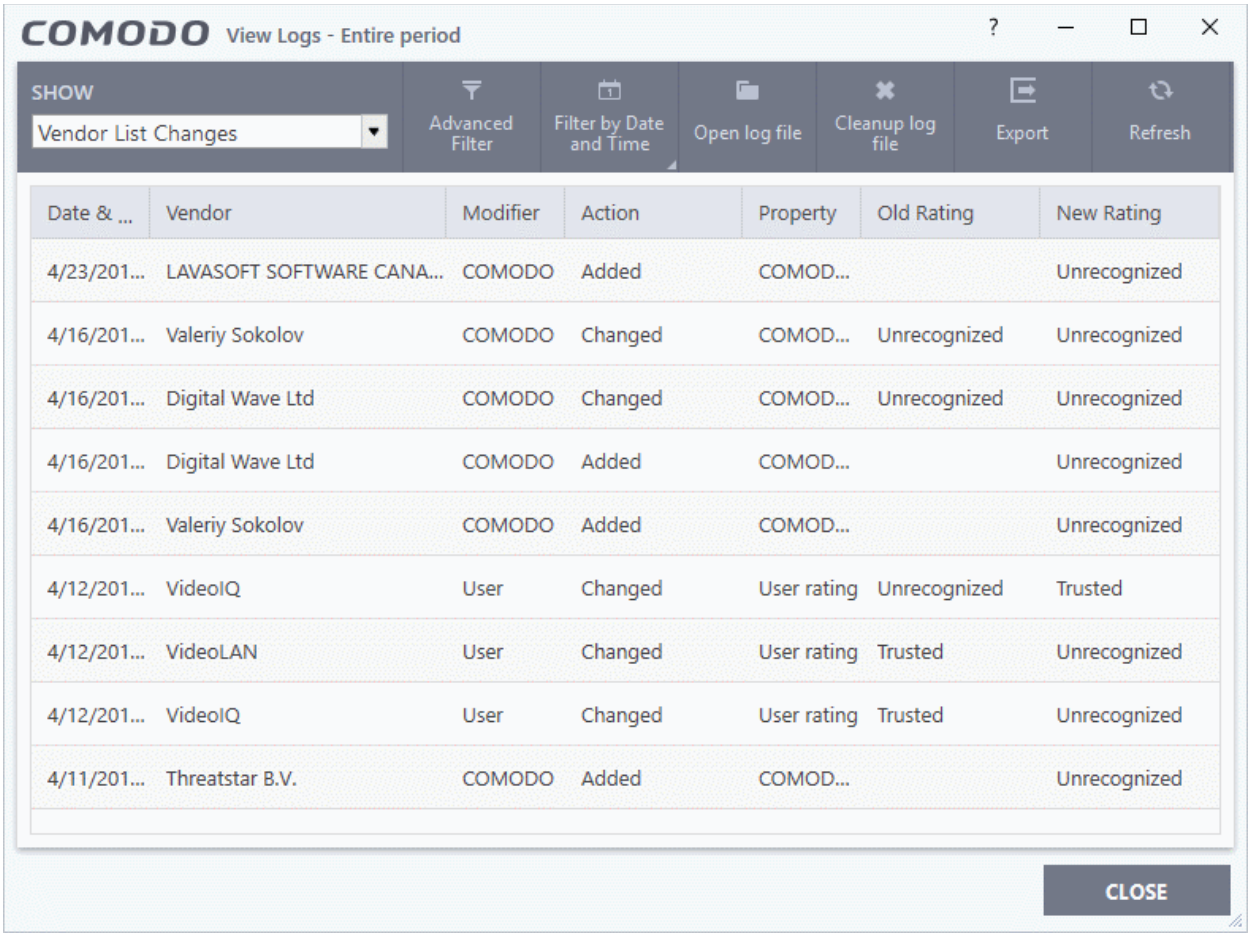
Click any column header to sort the entries in ascending \ descending order.

6.4.12. Vendor List Changes Logs

- Click 'Logs' in the CCS menu bar
- Select 'Vendor List Changes' in the drop-down at upper-left

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

- You can also add new vendors, and change the rating of existing vendors. Admin / User ratings supersede the Comodo rating.
- The files published by these vendors are rated depending on the current rating assigned to the vendor
- Any changes to vendors in the list are logged in 'Vendor List Changes'.



- **Date & Time** - When the change event occurred.
- **Vendor** - The name of the software publisher
- **Modifier** - Who made the change (User or Comodo).
- **Action** - Whether the vendor was added, removed, or assigned a new rating
- **Property** - Whether the current rating was assigned by Comodo, an admin, or a user.
- **Old Rating** - The trust rating of the vendor before the change.
    - The rating can be 'Trusted', 'Unrecognized' or 'Malicious'. Under default settings, unrecognized files are run in the container until Comodo classifies them as 'Trusted' or 'Malicious'.

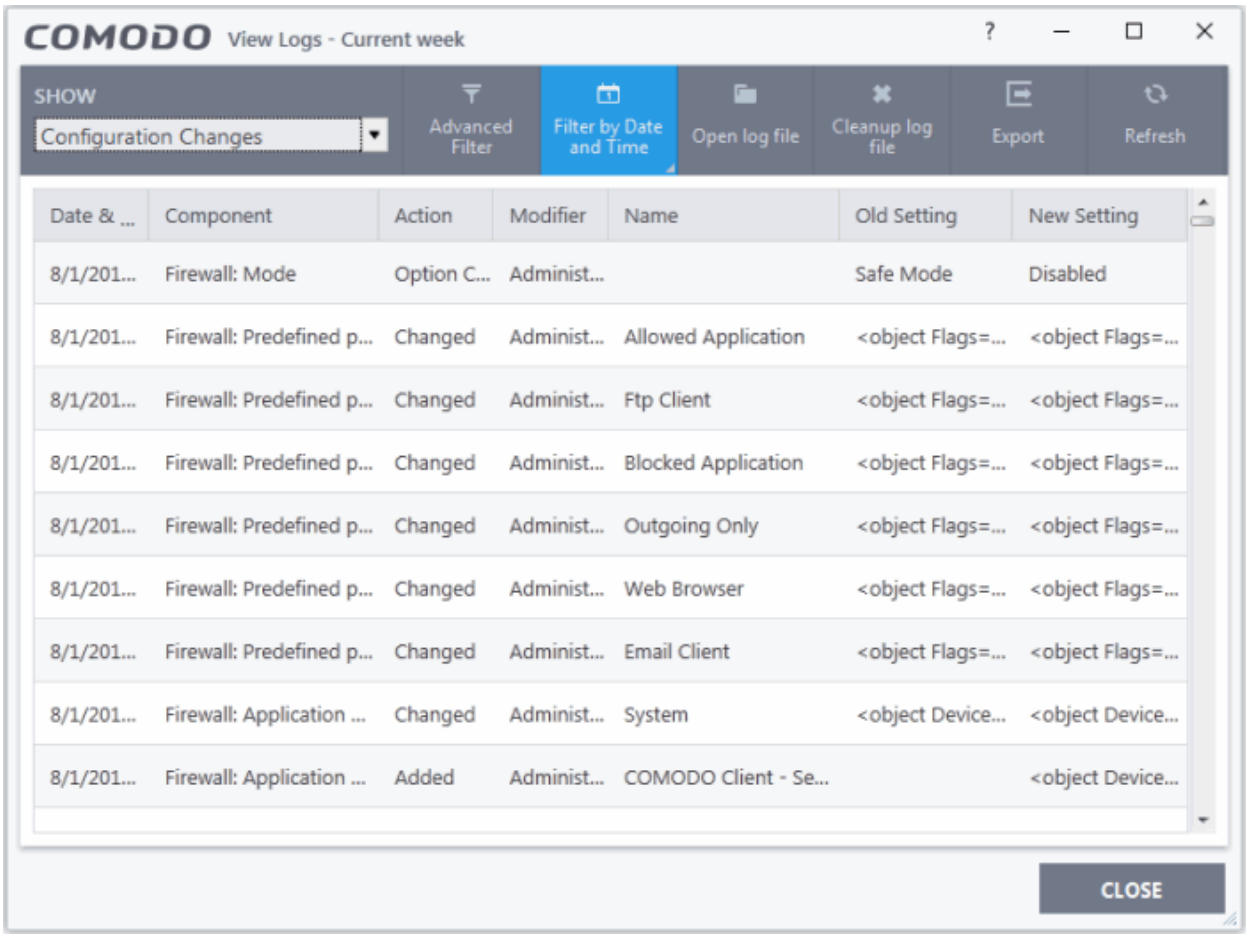
- **New Rating** - The trust rating of the vendor after the change.
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log.
- **Refresh** - Reload the current list and show the latest logs.

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

6.4.13. Configuration Change Logs

- Click 'Logs' in the CCS menu bar
- Select 'Configuration Changes' in the drop-down at upper-left

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



- **Date & Time** - When the configuration change was done.
- **Component** - The CCS interface that was modified.
- **Action** - Short description of the change made to the CCS component. For example, if a setting was changed, or an exclusion was created.
- **Modifier** - The service or user that made the change. Possible modifiers include 'User', 'Antivirus Alert', 'Auto-Learn', 'Firewall Alert', 'HIPS Alert', 'Containment Alert', 'Scheduler' and 'Comodo'.
- **Name** - The item featured in the modification. This will vary depending on the component.
- **Old Setting** - The value before the configuration change.

- **New Setting** - The value after the configuration change.
    - Pace your mouse over an entry in the 'Old Value' or 'New Value' column to view the full setting string
- **Export** - Save the logs as a HTML file. You can also right-click inside the log viewer and choose 'Export'.
- **Open log file** - Browse to and view a saved log file.
- **Cleanup log file** - Delete the selected event log.
- **Refresh** - Reload the current list and show the latest logs.

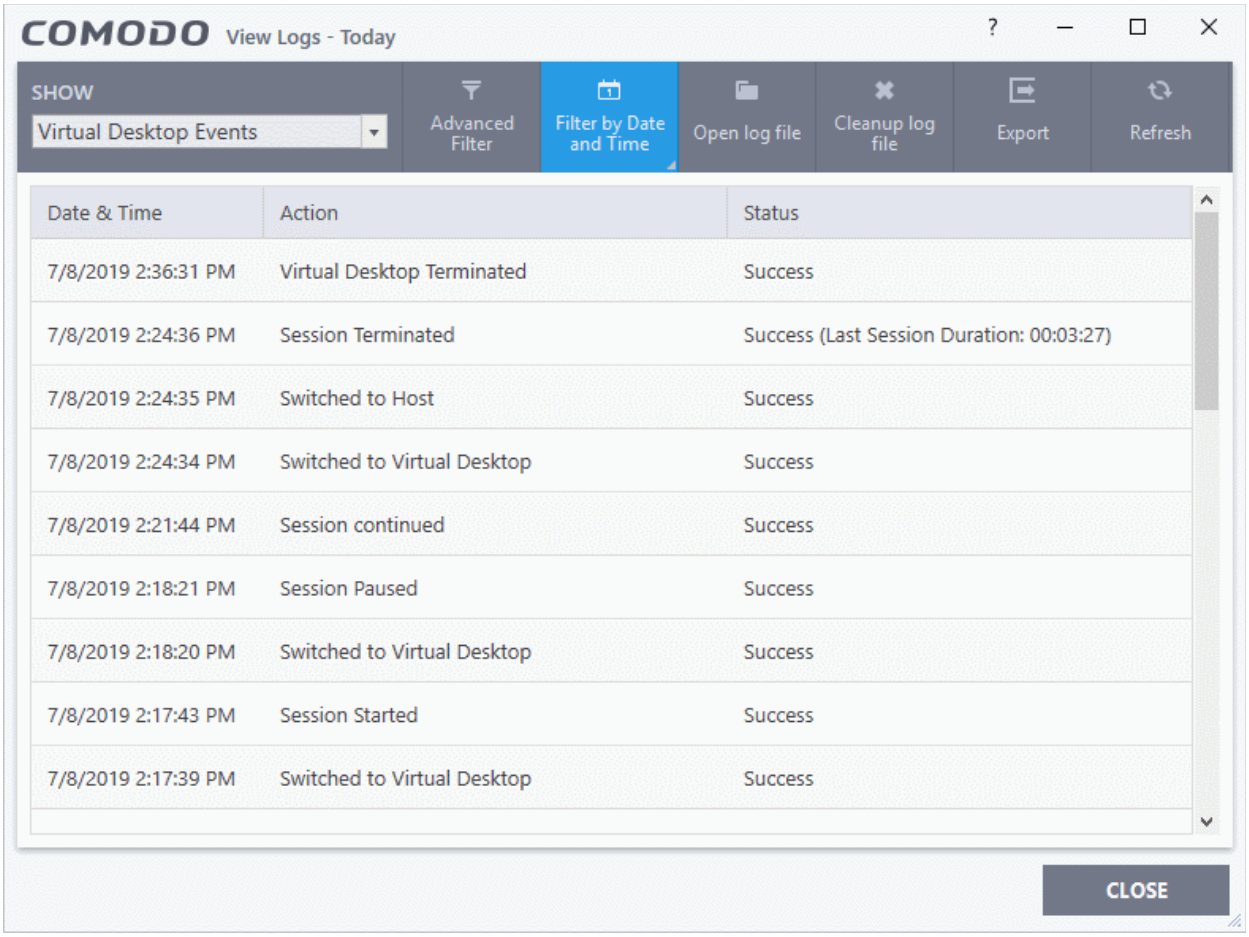
Click any column header to sort the entries in ascending \ descending order.

6.4.14. Virtual Desktop Event Logs

- Click 'Logs' in the CCS menu bar
- Select 'Virtual Desktop Events' in the drop-down at upper-left

CCS records all events from the virtual desktop. Events that are recorded include:

- Launch and close the virtual desktop
- Pause, resume, and terminate a virtual desktop session
- Switch between the virtual desktop and the host desktop

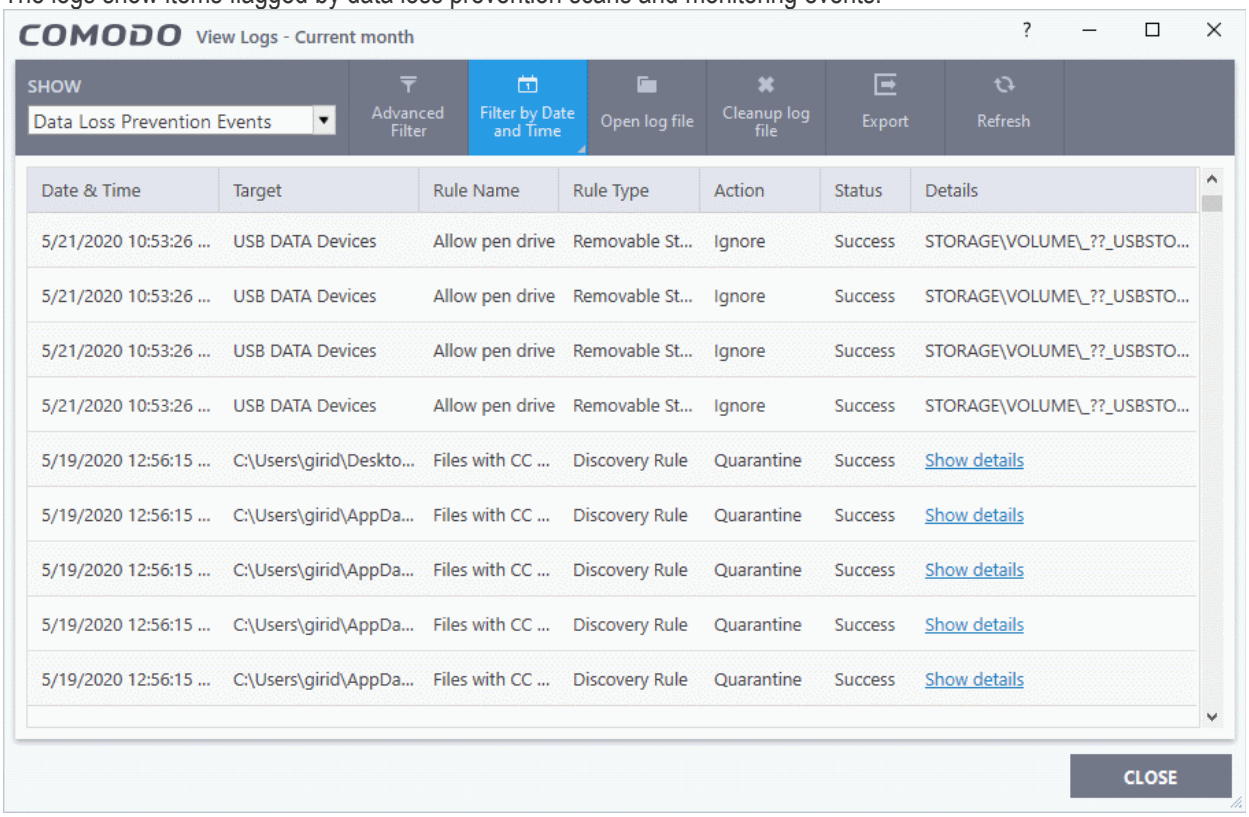


- **Date & Time** - When the event occurred
- **Action** - The operation executed
- **Status** - Whether the action taken was a success or failure
- Click any column header to sort the entries in ascending \ descending order.

6.4.15. Data Loss Prevention Event Logs

- Click 'Logs' in the CCS menu bar
- Select 'Data Loss Prevention Events' in the drop-down at top-left

The logs show items flagged by data loss prevention scans and monitoring events:



- **Date & Time** - When the event occurred.
- **Target** - The item affected by the rule.
  - **DLP Monitoring event** - Shows the type of external storage device to which the data transfer attempt was made
  - **DLP Discovery event** - Shows the file path of the identified file
- **Rule Name**- The DLP rule that found the target item. This could be a DLP discovery rule or a monitoring rule.
- **Rule Type** - Whether rule is a DLP discovery rule or a removable storage rule
- **Action** - How the file was handled in the DLP event. The possible values are:
  - Ignore
  - Quarantine
  - Restore from quarantine
  - Delete from quarantine
  - Blocked
- **Status** - Shows whether the rule executed successfully or not
- **Details** - The specifics of the data found.
  - **DLP monitoring rule** - Shows the removable storage device affected by the rule.
  - **DLP Discovery rule** - Has a 'Show details' link which opens the specifics of the event. See **View file details** for more details.

Advanced Filter - Search the logs by file location, rule or action.

Filter by Date and Time - Search for logs generated within a specific time-frame

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

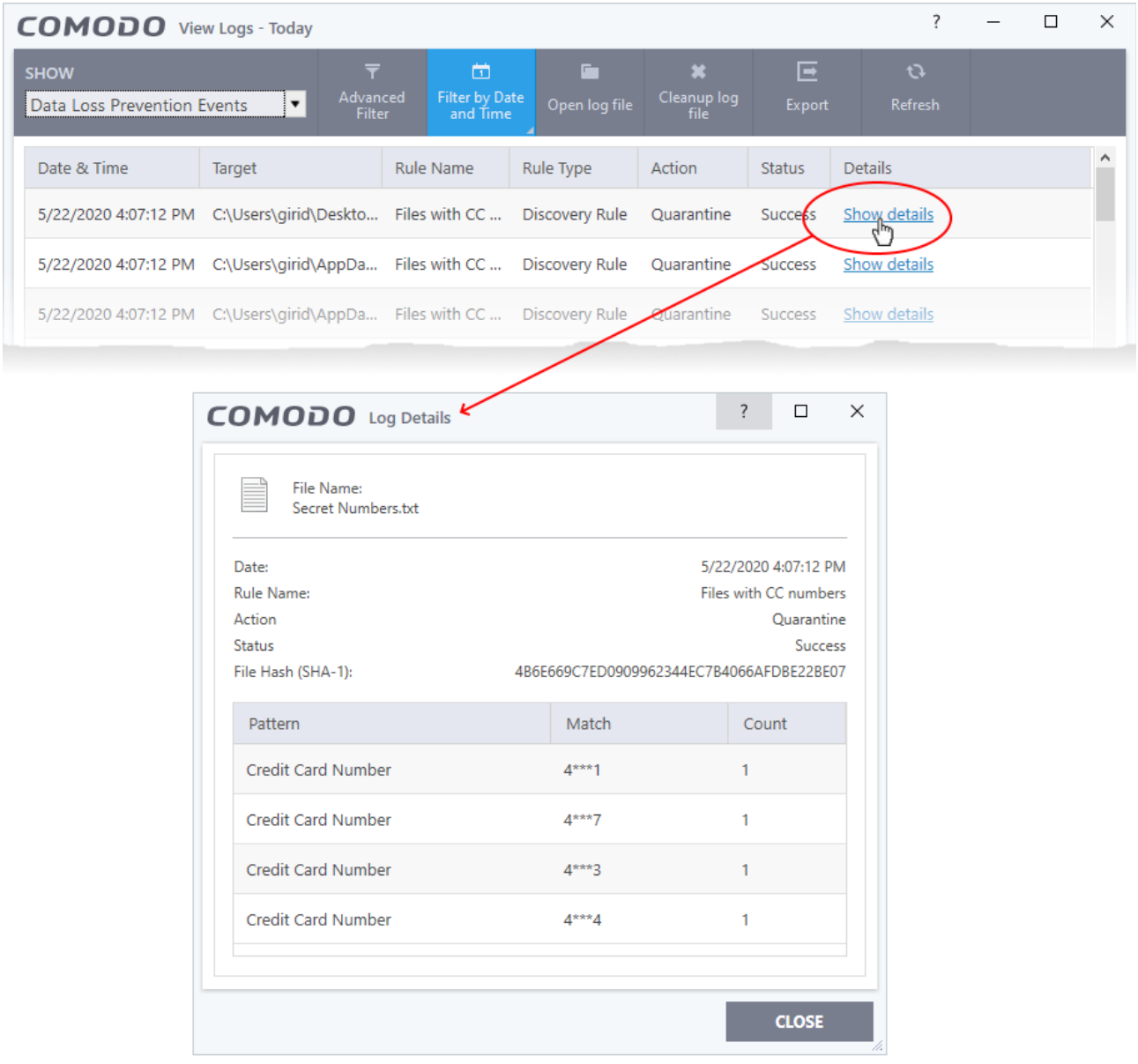
Cleanup log file - Delete the selected event log

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

Refresh - Reload the current list to show the latest logs

View file details

- Click the 'Show details' column shows different information depending on the type of DLP event:



- The screen shows the name of the file, and the rule/pattern which discovered sensitive data in the file.
- The 'match' column shows the first and last characters of the actual discovered data. The option to show this should be enabled in the discovery rule.

6.4.16. Search and Filter Logs

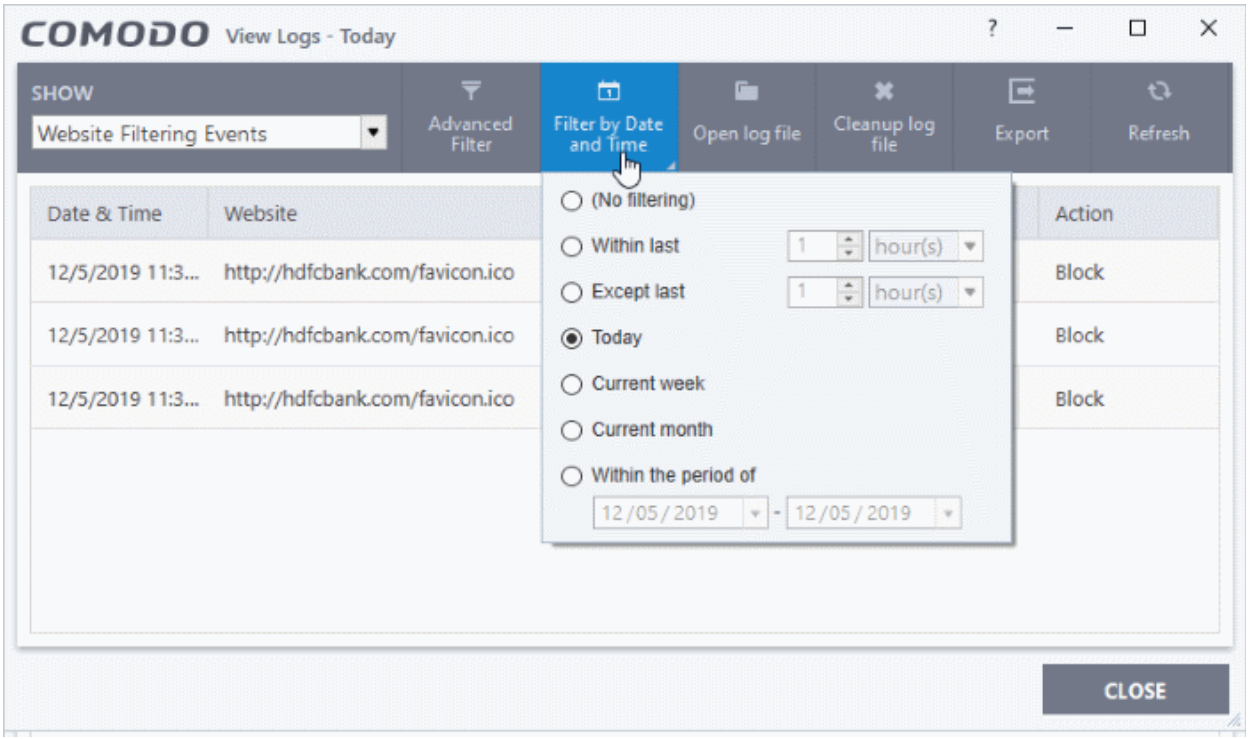
You can run a simple filter of events by date, and use advanced filters to conduct more complex searches.

- **Filter by date/time**

- **Advanced Filters**

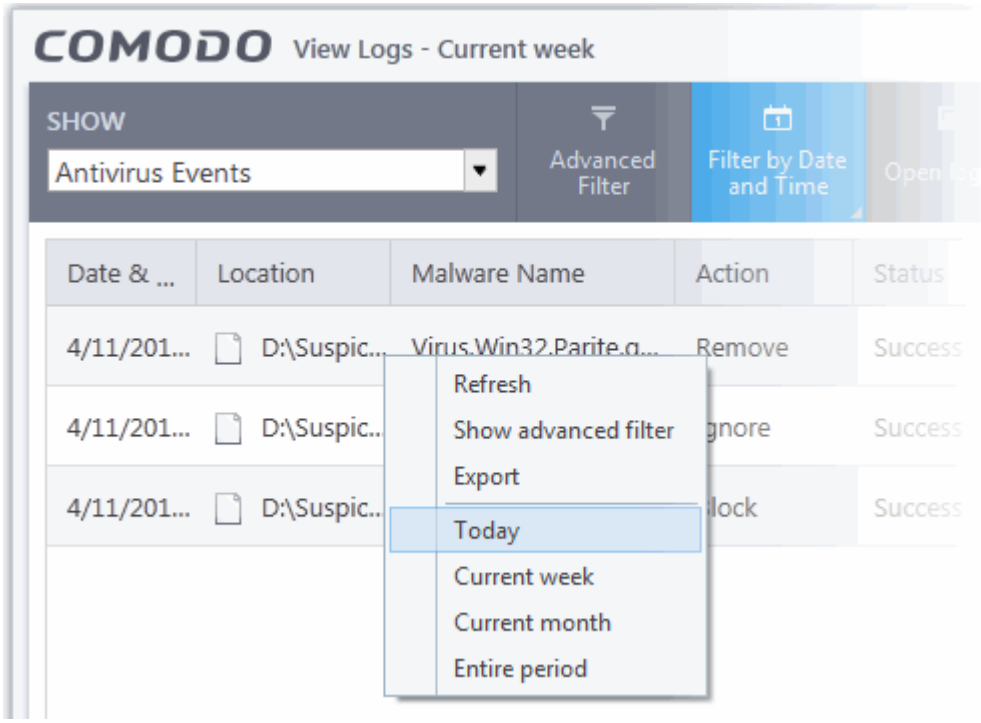
Filter by date/time

- Click 'Logs' in the CCS menu bar
- Select an event category from the drop-down at top-left
- Click 'Filter by Date and Time' to choose a specific period:



- **No filtering** - Show every event logged since CCS was installed. If you have cleared the logs since installation, this option shows all logs created since that clearance.
- **Within last** - Show all logs from a certain point in the past until the present time.
- **Except last** - Exclude all logs from a certain point in the past until the present time.
- **Today** - Show all events logged today, from 12:00 am to the current time. ***(Default)***
- **Current Week** - Show all events logged from the previous Sunday to today.
- **Current Month** - Display all events logged from 1st of the current month to today.
- **Within the period of** - Show logs between a custom date range.

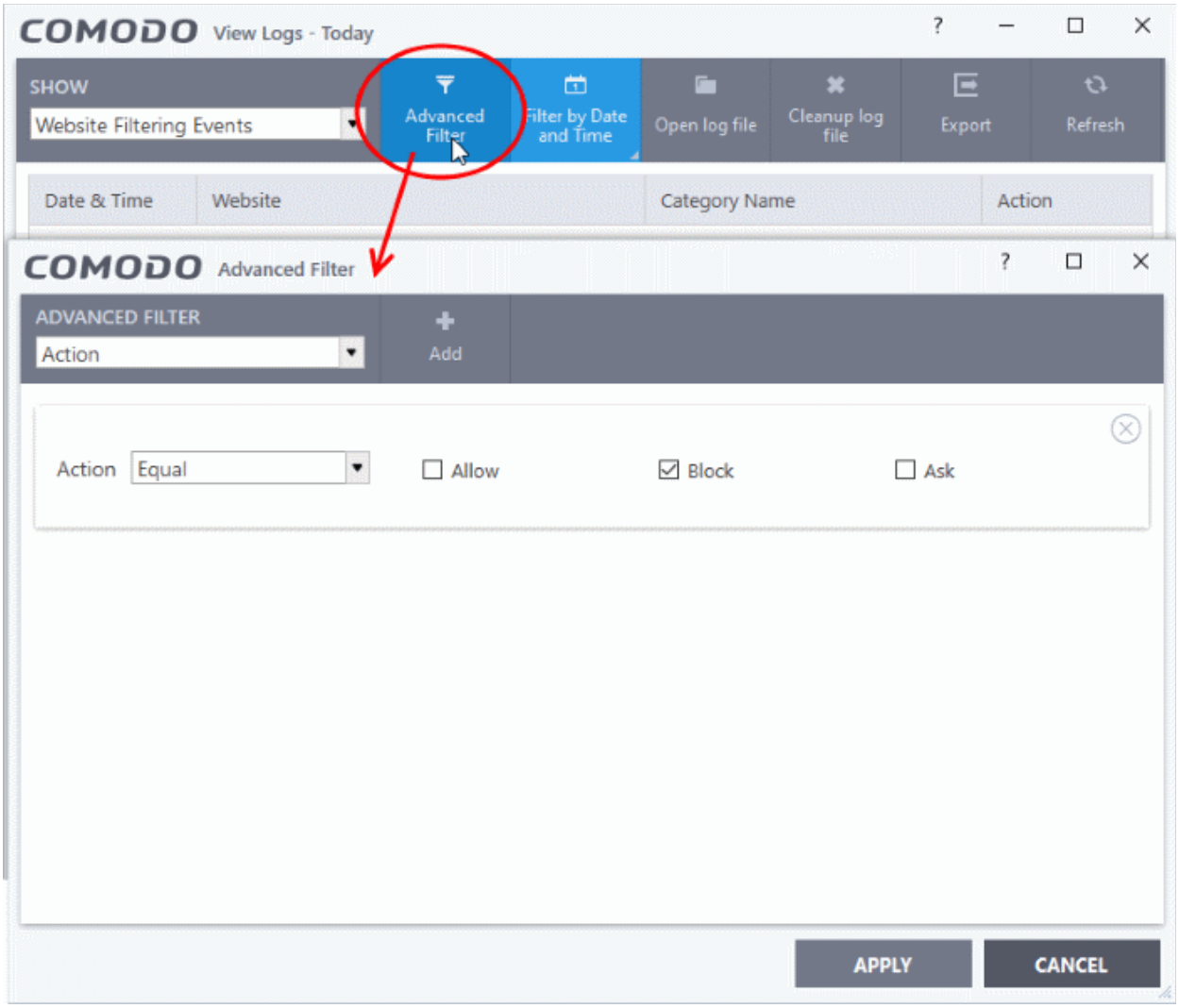
You can also right-click inside the log viewer module and choose the time period.



Advanced Filters

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

- Click 'Logs' in the CCS menu bar
- Select a module in the drop-down on the left
- Click 'Advanced Filter':



- Select a filter category at top-left then click 'Add'
- Search parameters vary according to the filter category. You can include multiple filter categories to refine your search.

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

- **Antivirus Events**
- **VirusScope Events**
- **Firewall Events**
- **HIPS Events**
- **Containment Events**
- **Website Filtering Events**
- **Device Control Events**
- **Autorun Events**
- **Alerts**
- **CCS Tasks**
- **File List Changes**
- **Vendor List Changes**
- **Configuration Changes**

- Virtual Desktop Events
- Data Loss Prevention

Antivirus Events

Filter Category	Description	Parameters
Action	Filter logs based on the action taken by CCS against the detected threat. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • Quarantine: Shows events at which the user chose to quarantine a file • Remove: Shows events at which the user chose to delete the detected threat • Ignore: Shows events at which the user chose to ignore the detected threat • Detect: Shows events involving only the detection of malware • Ask: Displays events where an alert was shown to the user so they could choose an action against a piece of detected malware • Restore: Shows events at which quarantined applications were restored to original location by admin from Endpoint Manager • Block: Shows events where suspicious applications were stopped • Reverse: Shows events where VirusScope overrode potentially malicious actions • False positive: Shows events where files flagged as threats by CCS were submitted to Comodo by the user as a false positive. • Add To exclusions: Shows events in which the user chose to add an item to antivirus exclusions • Add To trusted files: Shows events in which the user changed the file rating to 'Trusted' • Restore from Quarantine: Shows events in which files were returned to original location from quarantine • Delete from Quarantine: Shows events in which files were removed permanently from quarantine
Location	Filter the log entries related to events logged from a specific location.	• Enter the text or word that needs to be filtered For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:/Program Files/' in the text field, then all events containing the entry 'C:/Program Files/' in the 'Location' field are displayed.
Malware Name	Filter the log entries related to specific malware.	• Enter the text in the name of the malware that needs to be filtered. For example, if you choose 'Contains' from the drop-down and type 'siins' in the text field, then all events with 'siins' in the 'Malware Name' field are shown.

Status	Filter the log entries based on the success or failure of the action taken against the threat by CCS. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • Success: Shows events in which the actions against the detected threat were successfully executed (for example, the malware was successfully quarantined) • Failure: Shows events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected)

VirusScope Events

Filter Category	Description	Parameters
Action	Filter logs based on the action taken by CCS against the detected threat.	Select the filter parameter: • Quarantine: Shows events at which the user chose to quarantine a file • Remove: Shows events at which the user chose to delete the detected threat • Ignore: Shows events at which the user chose to ignore the detected threat • Detect: Shows events involving only the detection of malware • Ask: Displays events where an alert was shown to the user so they could choose an action against a piece of detected malware • Restore: Shows events at which quarantined applications were restored to original location by admin from Endpoint Manager • Block: Shows events where suspicious applications were stopped • Reverse: Shows events where VirusScope overrode potentially malicious actions • False positive: Shows events where files flagged as threats by CCS were submitted to Comodo by the user as a false positive. • Add To exclusions: Shows events in which the user chose to add an item to antivirus exclusions • Add To trusted files: Shows events in which the user changed the file rating to 'Trusted' • Restore from Quarantine: Shows events in which files were returned to original location from quarantine • Delete from Quarantine: Shows events in which files were removed permanently from quarantine
Location	Filter the log entries related to events logged from a specific location.	• Enter the text or word that needs to be filtered For example, if you select 'Contains' option from the drop-down and enter the phrase 'C:/Program Files/' in the text field, then all events containing the entry 'C:/Program Files/'

		in the 'Location' field are displayed.
Malware Name	Filter the log entries related to specific malware.	• Enter the text in the name of the malware that needs to be filtered. For example, if you choose 'Contains' from the drop-down and type 'siins' in the text field, then all events with 'siins' in the 'Malware Name' field are shown.
Status	Filter the log entries based on the success or failure of the action taken against the threat by CCS. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • Success: Shows events in which the actions against the detected threat were successfully executed (for example, the malware was successfully quarantined) • Failure: Shows events at which the actions against the detected threat failed to execute (for example, the malware was not disinfected)

Firewall Events

Filter Category	Description	Parameters
Action	Filter logs based on events according to the response (or action taken) by the firewall. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • Blocked: Shows events where CCS prevented the connection • Allowed: Shows events where the connection was allowed to proceed • Asked: Shows events where an alert was shown to the users so they could choose whether or not to allow the connection
Application	Filter logs based on events propagated by a specific application	• Enter the text or word that needs to be filtered. For example, if you choose 'Contains' from and enter the phrase 'cuckoo' in the text field, then all FW events containing the entry 'cuckoo' in the 'Application' column are displayed
Destination IP	Filter logs based on events with a specific target IP address 1. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice. 2. Select 'IPv4' or 'IPv6' from the drop-down box.	• Enter the IP address of the destination server or host, to filter the events that involve the connection attempts from/to that destination server or host. For example, if you choose 'Contains' option from the drop-down, select IPv4 and enter 192.168.111.11 in the text field, then all events containing the entry '192.168.111.11' in the 'Destination IP' column will be displayed.
Destination Port	Filter logs based on events that involved a specific target port number	• Enter the destination port number in the text entry field For example, if you choose 'Equal' option from the drop-

Filter Category	Description	Parameters
	Select any one of the option the drop-down: • Equal • Greater than • Greater than or Equal • Less than • Less than or Equal • Not Equal	down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.
Direction	Filter logs based on events of inbound or outbound nature. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • In: Shows a list of events involving inbound connection attempts • Out: Shows a list of events involving outbound connection attempts For example, if you choose 'Equal' option from the drop-down and select the 'In' checkbox, then all inbound connection attempts will be displayed.
Protocol	Filter logs based on events that involved a specific protocol. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the filter parameter: • TCP • UDP • ICMP • IPV4 • IGMP • GGP • PUP • IDP • IPV6 • ICMPV6 • ND For example, if you choose 'Equal' option from the drop-down and select the 'TCP' checkbox, then all connection attempts involving TCP protocol will be displayed.
Source IP	Filter logs based on events that originated from a specific IP address 1. Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice. 2. Select 'IPv4' or 'IPv6' from the drop-down box.	• Enter the IP address of the source server or host, to filter the events that involve the connection attempts from/to that source server or host system. For example, if you choose 'Contains' then select IPv4 and enter 192.168.111.22 in the text field, then all events containing the entry '192.168.111.11' in the 'Source IP' column will be displayed.

Filter Category	Description	Parameters
Source Port	Filter logs based on events that involved a specific source port number Select any one of the option the drop-down: • Equal • Greater than • Greater than or Equal • Less than • Less than or Equal • Not Equal	• Enter the destination port number in the text entry field For example, if you choose 'Equal' and enter 8080 in the text field, then all events containing the entry '8080' in the 'Source Port' column will be displayed.

HIPS Events

Filter Category	Description	Parameters
Application	Filter logs based on events propagated by a specific application	• Enter the search criteria for filtering the logs in the text field. For example, if you choose 'Contains' from the drop-down and enter the phrase 'cuckoo' in the text field, then all events containing the entry 'cuckoo' in the 'Application' column are displayed.
Action	Filter logs based on events according to the response (or action taken) by HIPS Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • Scanned online and found malicious • Access memory • Create process • Terminate process • Modify key • Modify file • Direct memory access • Direct disk access • Direct keyboard access • Direct monitor access • Load driver • Send message • Install Hook • Access COM interface • Execute image • DNS/RPC client access • Change HIPS Mode • Shellcode injection • Block file • Suspicious

Filter Category	Description	Parameters
		• Hook • Alert Suppressed • Scanned and found safe For example, if you choose 'Equal' and select 'Create process', only events involving the creation of a process by applications are displayed.
Target	Filter logs based on events that involved a specified target application.	• Enter the search criteria for filtering the logs in the text field. For example, if you choose 'Contains' and enter the phrase 'svchost.exe' in the text field, then all events containing the entry 'svchost.exe' in the 'Target' column will be displayed.

Containment Events

Filter Category	Description	Parameters
Application	Show events propagated by a specific application.	• Enter the search criteria for filtering the logs in the text field. For example, if you choose 'Contains' and enter the phrase 'pcflank' in the text field, then all events containing the entry 'pcflank' in the 'Application' column are displayed.
Rating	Show events which concern files that have a specific trust-rating. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice.	Select the filter parameter: • None • Unrecognized • Trusted • Malicious For example, if you choose 'Equal' and select the 'Unrecognized' file rating, only the containment events involving applications that are categorized as 'Unrecognized' are displayed.
Action	Show events where a specific action was applied to the file by CCS Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the restriction level(s) applied by the container to the applications, either automatically of or chosen by the user from the alert. • Run Restricted • Run Virtually • Blocked • Ignored For example, if you choose 'Equal' from the drop-down and select 'Run Virtually', only the events of applications that are run inside the container are displayed.
Contained by	Show events where the file was isolated by a specific module or user	Select the source(s) by which the applications were contained.

Filter Category	Description	Parameters
	Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' will invert your selected choice.	• Containment Policy • User • Contained Process • Containment Service For example, if you choose 'Contains' and select the 'User' checkbox, then only events involving applications that were manually run inside the container are displayed.
Parent Process	Show files contained based on its source process	• Enter the name of the application associated with the process, that launched contained item as the search criteria for filtering the logs in the text field. For example, if you choose 'Contains' and enter the phrase 'RuntimeBroker.exe' in the text field, then all events containing the entry 'RuntimeBroker.exe' in the 'Parent Process' column are displayed.
Parent Process ID	Show events created by a source process ID Select 'Contains' or 'Does Not Contain' from the drop-down menu.	• Enter the process ID of the application associated, that launched contained item as the search criteria for filtering the logs in the text field. For example, if you choose 'Contains' and enter the ID '2612' in the text field, then all events containing the entry '2612' in the 'Parent Process ID' column will be displayed.
Parent Process Hash	Show events where items was contained based on its source process(es) specified by hash value(s) of executable file(s) associated with the source process(es) Select 'Contains' or 'Does Not Contain' from the drop-down menu.	• Enter the SHA1 hash value of the executable file associated with the process, that launched contained item as the search criteria.

Website Filtering Events

Filter Category	Description	Parameters
Website	Show only events that involved a specific website Select 'Contains' or 'Does Not Contain' from the drop-down menu.	• Enter the website address in part or full, to filter the logs involving the website. For example, if you choose 'Contains' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that involve the website 'facebook.com' in the 'Website' column are displayed.
Category Name	Show events that involved websites which are covered by a website filtering category.	• Enter the website filter category name, to filter the logs involving the category For example, if you choose 'Contains' and enter the phrase 'Malware Sites' in the text field, then all events involving websites in the 'Malware Sites' category are displayed.

Filter Category	Description	Parameters
Action	Show only events that involved a specific response by CCS Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Select the action(s) to filter the logs involving those action(s). • Allow • Block • Ask For example, if you choose 'Equal' and 'Block', then only events where websites blocked are displayed.

Device Control Events

Filter Category	Description	Parameters
Name	Filter the entries based on the type of the device.	• Enter the type of the device in full or part as your filter criteria in the text field. For example, if you choose 'Contains' and type 'USB Input Device' in the text field, you will see logs related to USB input devices like keyboards, mice and finger print scanners.
Identifier	Filter entries based on the device ID of the external device.	• Enter the device ID of the device in full or part as your filter criteria in the text field. For example if you have chosen 'Contains' and entered 'USB\VID_0627&PID_0001', in the text field only those log entries related to external devices whose device ID contains the string are displayed.
Class	Filter the entries based on the GUID of the device	• Enter a Device Class ID (GUID) in part or full as your search criteria For example, if you select 'Contains' option from the drop-down field and enter '4D36E967', then all events containing the entry '4D36E967' in the 'Class' field are displayed..
State	Filter events based on whether the device connection attempt was allowed or blocked.	Select the parameter to refine your search. • Enabled • Disabled

Autorun Events

Filter Category	Description	Parameters
Type	Filter entries based on the class of autorun Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' will invert your choice	Choose from: • Windows Service • Autostart entry • Scheduled task
Location	Filter entries based on application path Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not	• Enter the location or a part of it as your filter criteria in the text field. For example if you have chosen 'Contains' and entered 'C:/Program Files (x86)/Cuckoo Files/Cuckoo.exe in the text field, then only log entries with the same value in the 'Path'

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

Alerts

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

Filter Category	Description	Parameters
	what action the user selected at the alert. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Unknown • Allow • Deny • Treat as • Disinfect • Quarantine • Quarantine and reserve • Skip once • Add to exclusions • Add to trusted files • False positive • Skip • Terminate • Keep inside the Container • Run outside the Container • Deny and Terminate • Deny, Terminate and Reverse • Containment • Visit with Secure Browser • Run Unlimited • Run inside the Container • Blocked For example, if you choose 'Equal' from the drop-down and select the 'Add to exclusions' checkbox, only the alerts where you answered 'Ignore' > 'Ignore and Add to exclusions' are displayed.
Answered	Filter logs based on the date the user answered the alerts. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Enter or select the required date from the date picker For example, if you select 'Equal' and select '07/31/2017', only alerts answered on 07/31/2017 are displayed.
Description	Filter the entries based on the description of the attempt displayed in the alert. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the text or word as your filter criteria. For example, if you select 'Contains' from the drop-down and enter 'connect to the internet', only the log entries of firewall alerts that contain the phrase 'connect to the internet' in the description are displayed.
Option	Filter the log entries where the	Select the specific filter parameters to refine your search.

Filter Category	Description	Parameters
	user selected an additional options like 'Remember my answer', 'Submit as False Positive' from the alert. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Remember • Restore point • Submit • Trusted publisher For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected are displayed.
Treat as	Filter events where the user chose specific actions on the alert. For example, 'treat as a safe application', 'treat as an installer' and so on. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the text or word as your filter criteria For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the log entries containing the phrase 'Installer' in the 'Treat As' column are displayed.
Alert Type	Filter the log entries based on the CCS component that triggered the alert Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the specific filter parameters to refine your search. • Antivirus Alert • Firewall Alert • HIPS alert • Containment alert • VirusScope Alert • Network alert For example, if you select 'Equal' from the drop-down and select 'Antivirus Alert' checkbox, only the log of antivirus alerts are displayed.

CCS Tasks

Filter Category	Description	Parameters
Code	Filter the entries based on specified error code Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Enter the code or a part of it as your filter criteria in the text field. For example, if you have select 'Equal' and entered '0x80004004' in the text field, then only entries containing the value '0x80004004' in the 'Code' column are displayed.
Completed	Filter events based on tasks successfully finished on the specified date Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Enter or select the required date from the date picker For example, if you choose 'Equal' and select '08/01/2019', only the logs of tasks completed on 08/01/2019' are displayed.

Filter Category	Description	Parameters
Parameter	Filter the entries based on the specified parameter. A 'parameter' is a sub-type of the main task type. For example, 'Quick Scan' and 'Rating Scan' are both parameters of the main task type 'Antivirus Scan'. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the text or word as your filter criteria. For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Quick Scan' in the text field, then only the entries of 'Antivirus Scan Tasks' with the scan parameter 'Quick Scan' are displayed.
Type	Filter the entries based on the CCS tasks category. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the specific filter parameters to refine your search. • Antivirus update • Antivirus scan • Log Clearing • Product upgrade • Binary update • File Rating DB Upgrade • Purge file list • Virtual Desktop Session • Reset the Container • DLP Discovery Scan

File List Changes

Filter Category	Description	Parameters
Location	Filter the entries based on the file path whose trust rating was changed Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the location or a part of it as your filter criteria in the text field. For example if you have chosen 'Contains' and entered 'C:/Program Files (x86)/Cuckoo Files/Cuckoo.exe in the text field, then only log entries with the same value in the 'Path' column are displayed.
Modifier	Filter events based on who changed the file rating Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the filter parameter to refine your search • Administrator • User • Comodo For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only logs of changes done by the users are displayed.
Action	Filter the entries based on the	Select the filter parameter to refine your search

Filter Category	Description	Parameters
	file activity Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	• Added • Changed • Removed For example, if you select 'Equal' from the drop-down and select 'Removed' checkbox, only the logs of files that were removed from the file list are displayed.
Rating Source	Filter the entries by who provided the file rating Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Ratings can be provided by: • Administrator • Administrator (by Vendor) • User • User (by Vendor) • AV database • Trusted installer • FLS • FLS (by Vendor) • Valkyrie • SmartScreen • Signed by Comodo • Signed by Microsoft For example, if you select 'Equal' from the drop-down and select 'User' checkbox, only the logs of files that were rated by the users are displayed.
Old Rating	Filter the entries based on trust rating of files before the change Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Select the filter parameter to refine your search • Unrecognized • Trusted • Malicious For example, if you select 'Contains' from the drop-down and select 'Unrecognized' checkbox, only the logs of files that are rated as 'Unrecognized' in the 'Old Rating' column are displayed.
New Rating	Filter logs by the trust rating of files after the change Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	Select the filter parameter to refine your search • Unrecognized • Trusted • Malicious For example, if you select 'Contains' from the drop-down and select 'Malicious' checkbox, only the logs of files that are rated as 'Malicious' in the 'New Rating' column are displayed.
File Hash	Filter logs by hash value	• Enter the SHA1 hash value of the file in the text field to refine your search

Filter Category	Description	Parameters
	Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	

Vendor List Changes

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

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

Configuration Changes

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

Filter Category	Description	Parameters
Component	Filter logs by the object modified by the action. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Select the affected object. It is not possible to list all possible objects in this table. Please consult the list in the search interface.

Virtual Desktop Events

Filter Category	Description	Parameters
Action	Filter logs by the type of virtual desktop activity. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Possible activities: • Virtual Desktop Launched • Virtual Desktop Terminated • Session Started • Session Paused • Session Continued • Session Terminated • Switched to Windows View • Switched to Virtual Desktop For example, if you select 'Equal' from the drop-down and select 'Session Started' checkbox, only the session initiated events are displayed in the 'Action' column.
Status	Filter logs by whether the event was was successful or not. Examples include paused sessions successfully resumed, wrong PIN entered and user could not resume a paused session. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Possible outcomes are: • Success • Failure • Expired

Data Loss Prevention Events

Filter Category	Description	Parameters
Target	Filter entries by document location and / or storage device. Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the location, or a part of it, as your filter criteria.
Rule	Filter entries by rule name Select 'Contains' or 'Does Not Contain' option from the drop down menu. 'Does Not Contain' inverts your choice.	• Enter the DLP rule name, or a part of it, as your filter criteria.
Action	Filter entries by the action taken on the target. The action may be: 1) An action CCS took on target a file. 2) An action that a user took on the target file. 3) An action CCS took on an external device.e detected document.	• **Ignore** - CCS did not take any action on the file. You are, of course, free to review and assess the file. • **Quarantine** - CCS moved the files to quarantine • **Restore from Quarantine** - The file was moved back to its original location by the user • **Delete from Quarantine** - The file was removed from the system by the user • **Blocked** - CCS implemented 'Read-only' mode on an external device, preventing users from copying potentially sensitive files to it.
Status	Filter logs by whether the event was was successful or not. Select 'Equal' or 'Not Equal' from the drop down. 'Not Equal' inverts your choice.	Possible outcomes are: • Success • Failure

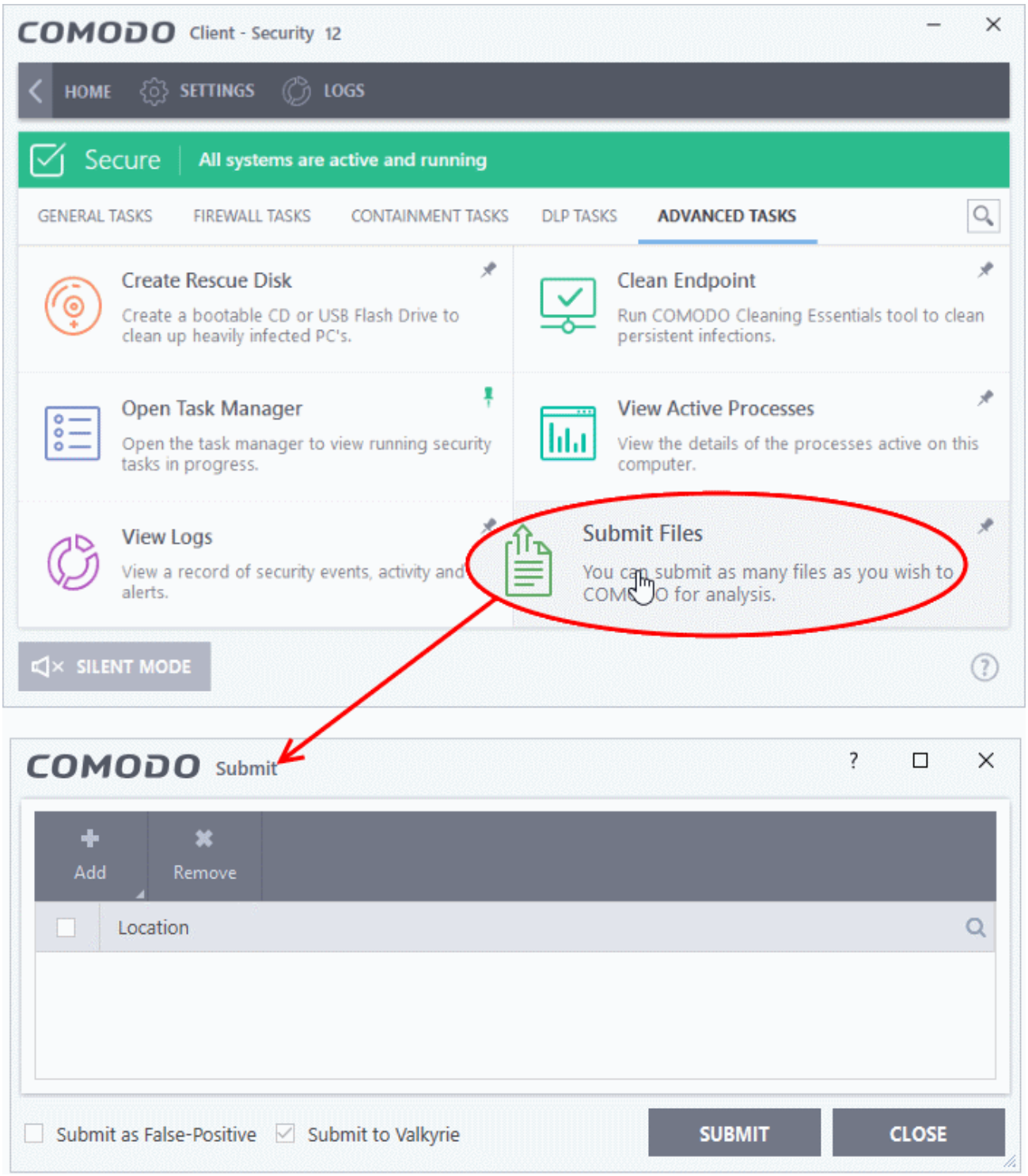
6.5. Submit Files for Analysis to Comodo

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

Tip - You can also submit files to Valkyrie from the **Quarantine** and **File List** interfaces.

Upload files for analysis

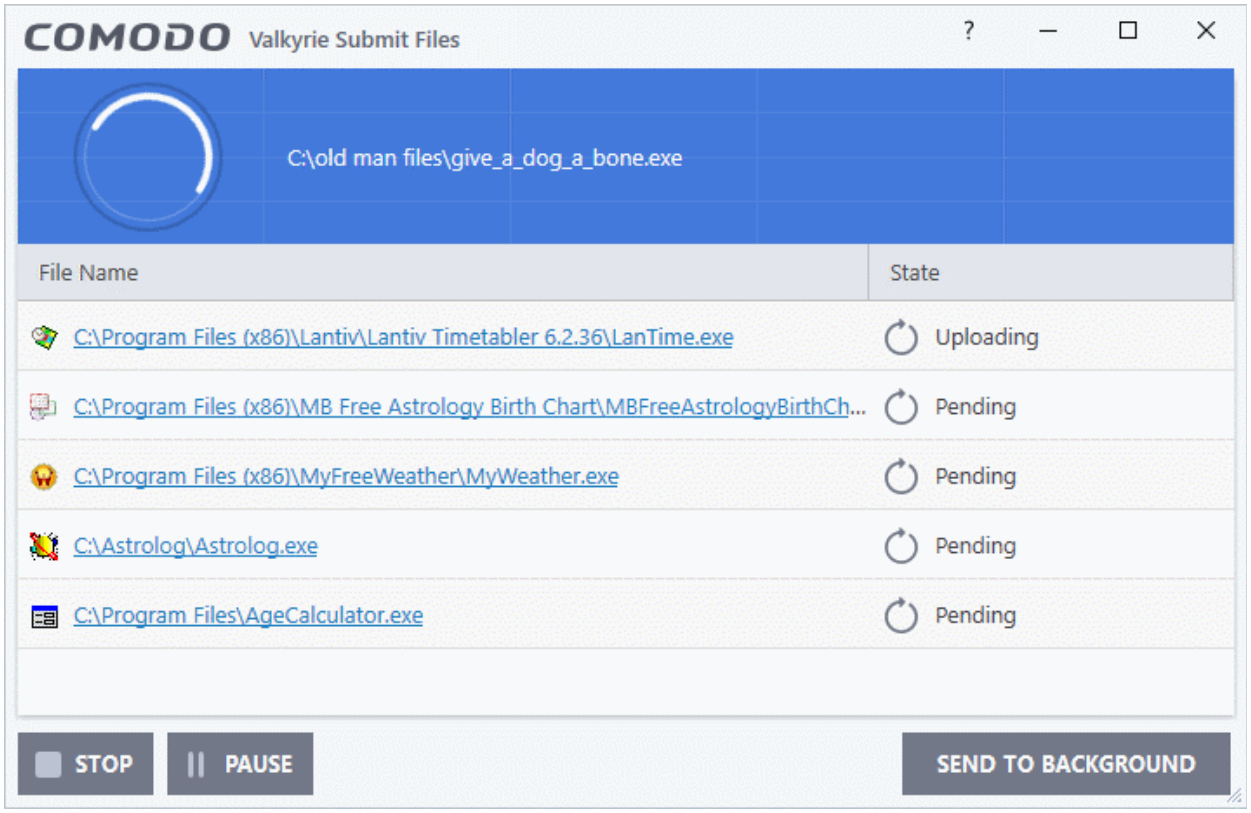
- Click 'Tasks' on the CCS home screen
- Click 'Advanced Tasks' then 'Submit Files'



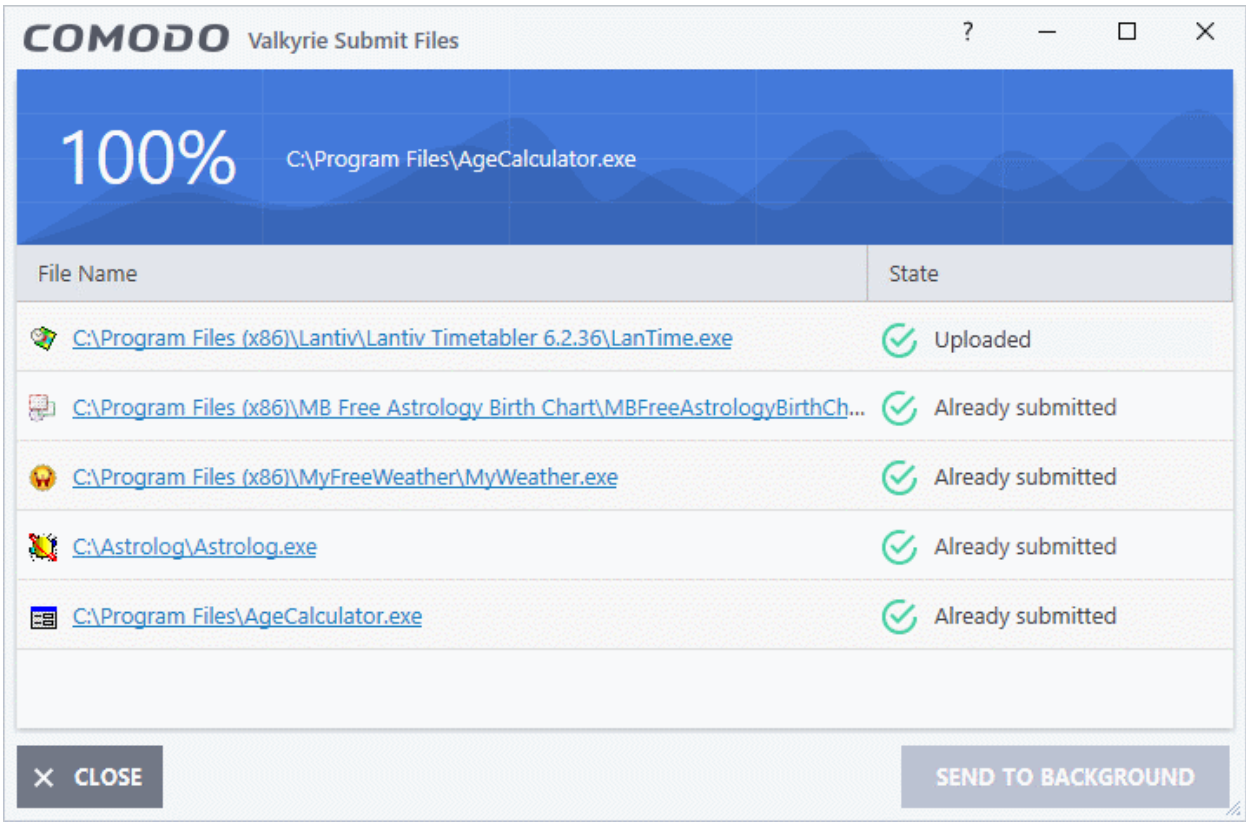
- Click 'Add' at top right.

- There are three ways to select a file:
  - **Files** - Browse to the file or executable you want to add to the 'Submit Files' list.
  - **Folders** - Browse to the folder you want to add. All files in the folder will be added to the 'Submit Files' list.
  - **Running Processes** - Select a currently active process. The parent application of the process will be added to the 'Submit Files' list.
- Repeat the process to add more files
- Please note that 'Submit to Valkyrie' is pre-selected by default. You cannot change this setting.
- Click the 'Submit' button

The uploading process will commence. You can stop, pause/resume or send the submission process to background by clicking respective buttons.



When a file is first submitted, the file look-up service checks whether the file is already queued for analysis by our technicians. Results are shown below:



- **Uploaded** - The file was accepted for review by our research labs. The file's signature was not among the list of files waiting to be tested.
- **Already submitted** - The file has already been uploaded by another CCS user and is queued for testing. This means the file was not uploaded from your machine.

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

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

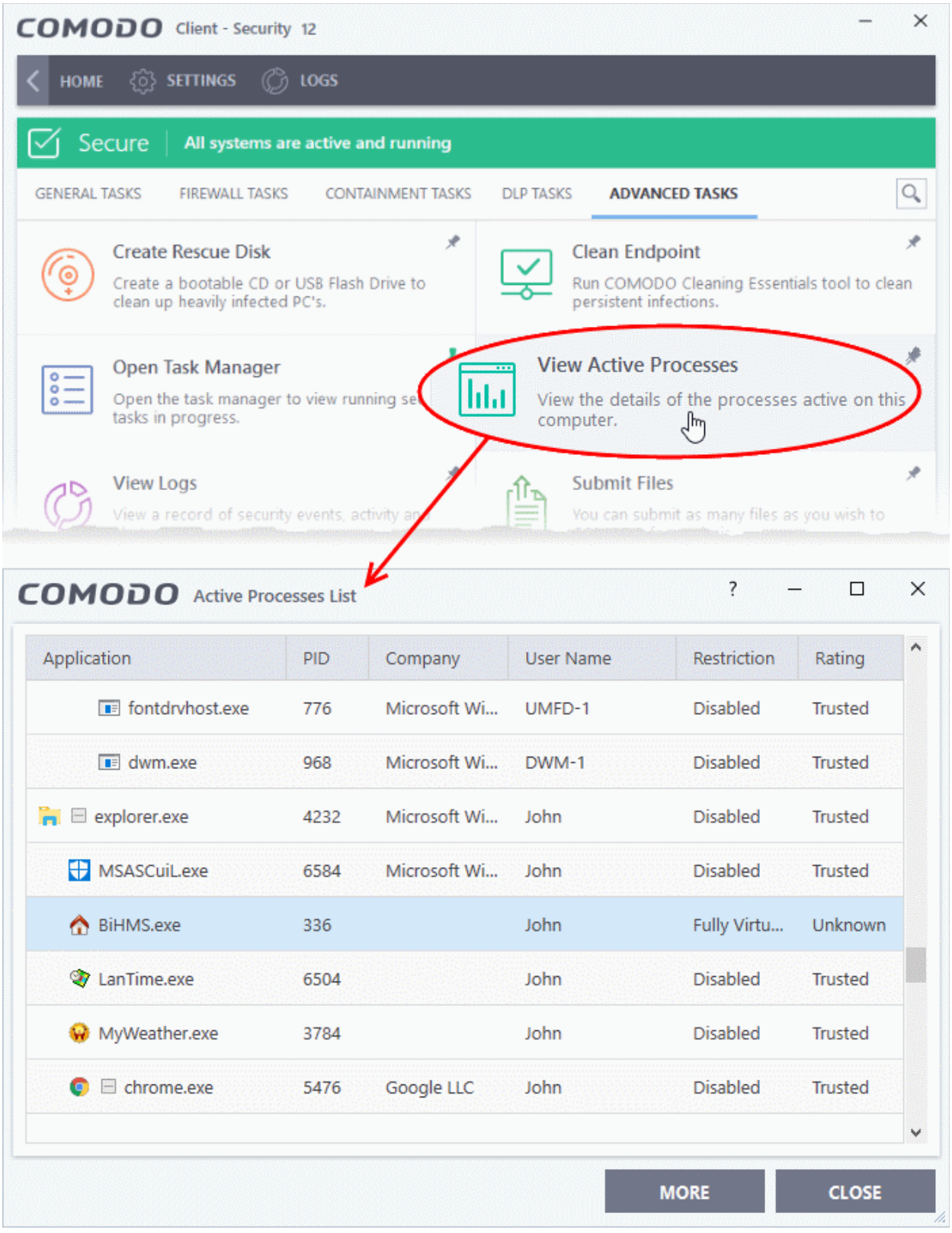
6.6. View Active Process List

Click 'Tasks' > 'Advanced Tasks' > 'View Active Processes'

- The active process list shows all processes started by applications currently running on your system.
- CCS can identify the parent application of a process to detect when a non-trusted application is trying to spawn a trusted application. CCS can then deny access rights to the trusted application.
- This deep level of inspection protects you against malware that tries to use trusted software to launch an attack.
- The interface also lets you run an online lookup on the parent application. Here, you can check its trust rating on the latest cloud databases. You can also submit an application to Comodo for analysis.

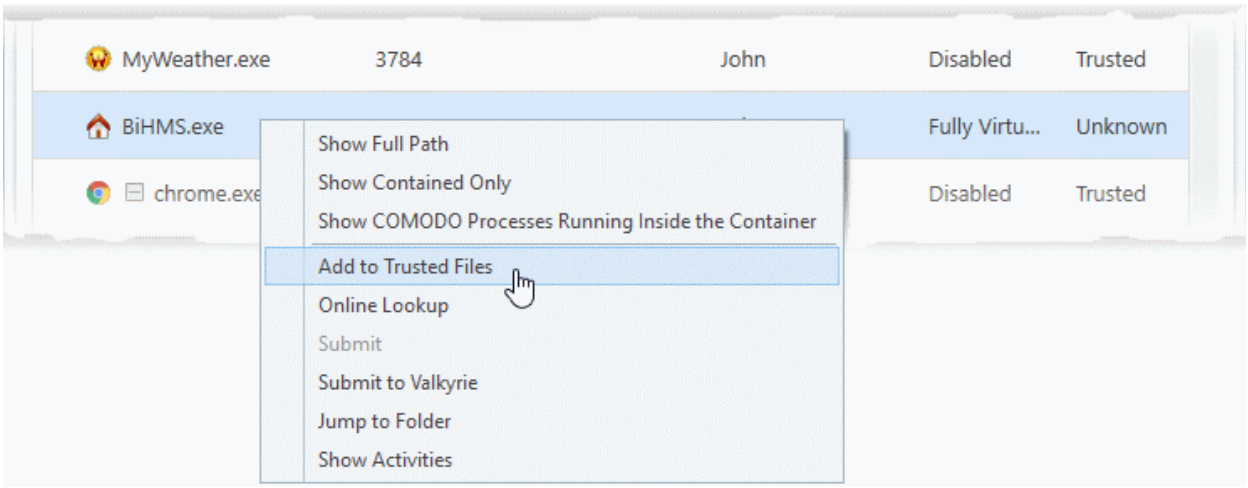
View the active process list

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

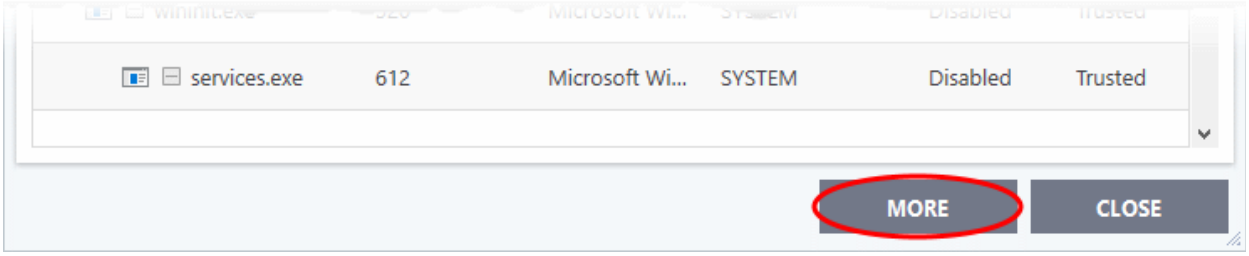


- **Application** - The name of the parent executable of the process.
- **PID** - The unique process identifier.
- **Company** - The vendor who created the software
- **User Name** - The user account under which the program is run
- **Restriction** - The security limitations placed on the program by the CCS containment module.
- **Rating** - The trust level of the program as per the local **file list** ('Settings' > 'File Rating' > File List')

- Right-click on any process to open the context sensitive menu:



- **Show Full Path** - View the install location of the parent program
- **Show Contained Only** - Hides all processes except those running in the container.
- **Show COMODO Processes Running Inside the Container** - Hide all processes except Comodo processes running in the container.
- **Add to Trusted Files** - Assign 'Trusted' status to the executable that started the process. This allows the file to run as normal in future. You can view trusted files in the CCS '**File List**' ('Settings' > 'File Rating' > 'File List').
- **Online Lookup** - Search for the executable in Comodo's global blacklist and whitelist. The results will tell you if the file is clean, malicious or unknown.
- **Submit to Valkyrie** - Uploads the parent executable to Comodo Valkyrie for analysis. Valkyrie is Comodo's file testing and verdicting system that analyzes the submitted files with a range of static and dynamic tests to determine the file's trust rating. The files are added to the safe list (white-listed) or to the database of virus signatures (blacklisted) depending on the results.
- **Jump to Folder** - Opens the folder containing the executable.
- **Show Activities** - Shows all actions by processes of the application. This option is available only for contained applications and if **VirusScope is enabled** ('Settings' > 'Advanced Protection > 'VirusScope').
- Click the 'More' button to open Comodo KillSwitch - an advanced system monitor that lets you quickly identify and terminate any unsafe processes on your system.



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

View 'Active Processes' list of contained applications

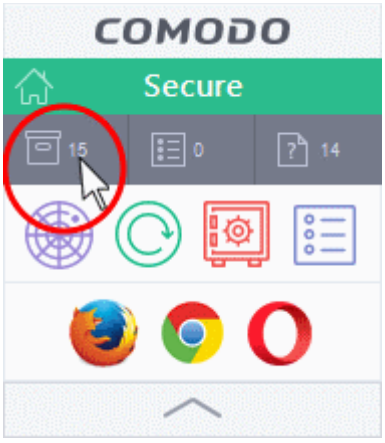
Click the shortcut on the widget to view processes by applications inside the container. These applications include:

- **Auto-Containment** - Applications that are made to run in the container by a containment rule. See '**Auto-Containment Rules**' for more details on defining auto-containment rules.
- **Run Virtual** - Applications that were manually run in containment. See '**Run an Application in Containment**' for more details.

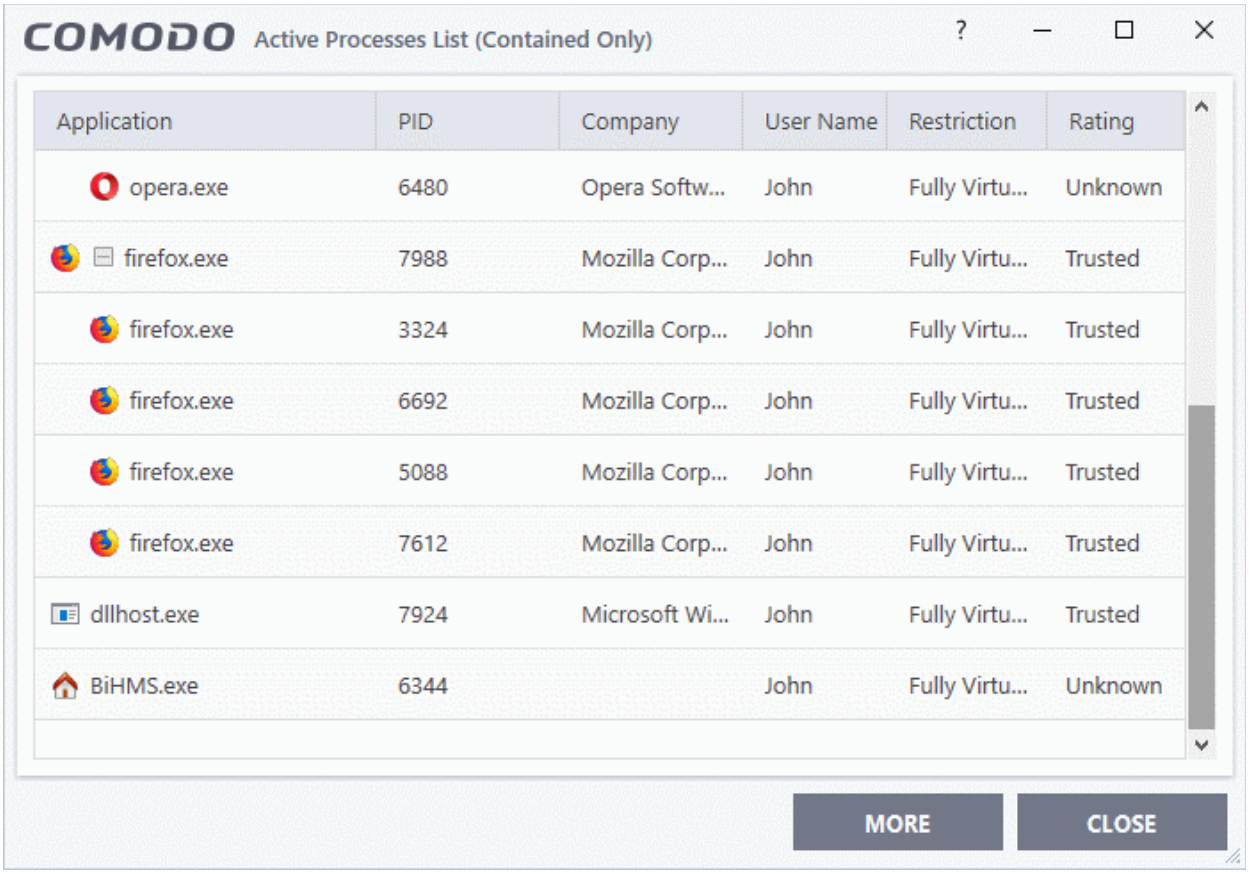
- Applications that are run inside the containment using the context sensitive menu - **Click here** for more details.
- Running browsers inside the containment from the widget - **Click here** for more details.
- Programs that are added manually - See '**Auto-Containment Rules**' for more details.

View active processes from contained applications

- Click the first box in the second row in the CCS Widget.



The Active Processes List (Contained Only) screen appears:

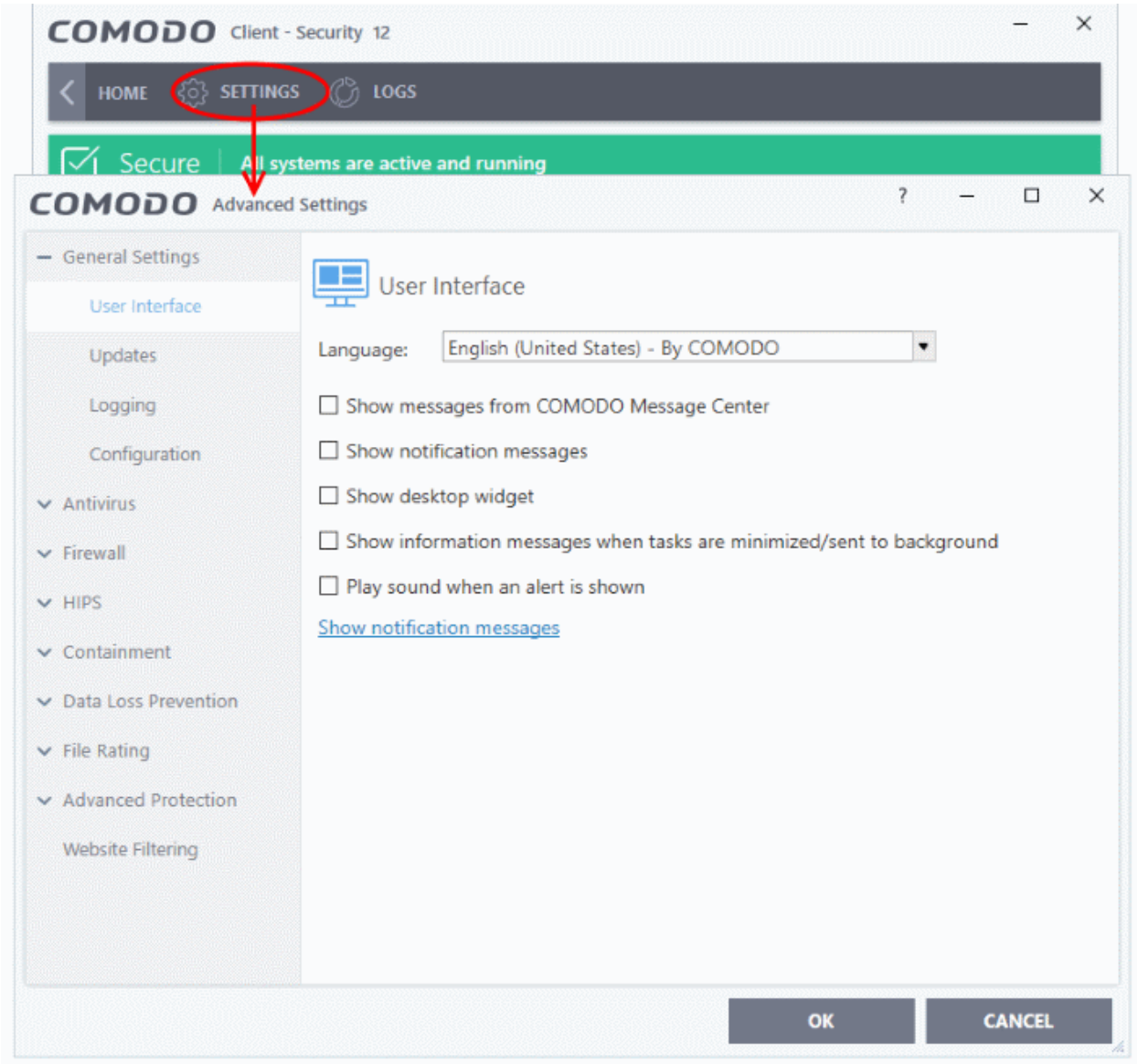


7. CCS Advanced Settings

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

The settings area lets you configure every aspect of the operation, behavior and appearance of Comodo Client Security. There are two main areas:

- **General settings** - Specify top-level preferences regarding the interface, updates and event logs.
- **Security settings** - Configure each CCS security module. Modules include antivirus, firewall, file-rating, containment and data loss prevention.



You might need to enter a password to access the settings if so configured in the Endpoint Manager profile. See '**Password Protection**' for more details.

Click the following links for help with specific settings:

- **General Settings** - Configure the appearance and behavior of the application
  - **Customize User Interface**
  - **Configure Virus database Updates**
  - **Log Settings**
  - **Manage CCS Configurations**
- **Antivirus Settings**
  - **Real-time Scanner Settings**
  - **Scan Profiles**

- Firewall Settings
  - General Firewall Settings
  - Application Rules
  - Global Rules
  - Firewall Rule Sets
  - Network Zones
  - Port Sets
- HIPS Settings
  - General HIPS Settings
  - Active HIPS Rules
  - HIPS Rule Sets
  - Protected Objects - HIPS
  - HIPS Groups
- Data Loss Prevention
  - DLP Monitoring Rules
  - DLP Discovery Rules
  - DLP Keyword Groups
- Containment Settings
  - Containment Settings
  - Auto-Containment Rules
  - Protected Objects - Containment
  - Virtual Desktop Settings
  - Containment - An Overview
  - Unknown Files: The Scanning Process
- File Ratings
  - File Rating Settings
  - File Groups
  - File List
  - Submitted Files
  - Vendor List
- Advanced Protection
  - VirusScope Settings
  - Scan Exclusions
  - Device Control Settings
  - Script Analysis Settings
  - Miscellaneous
- Web Filter Settings
  - Web Filter Rules
  - Website Categories

7.1. General Settings

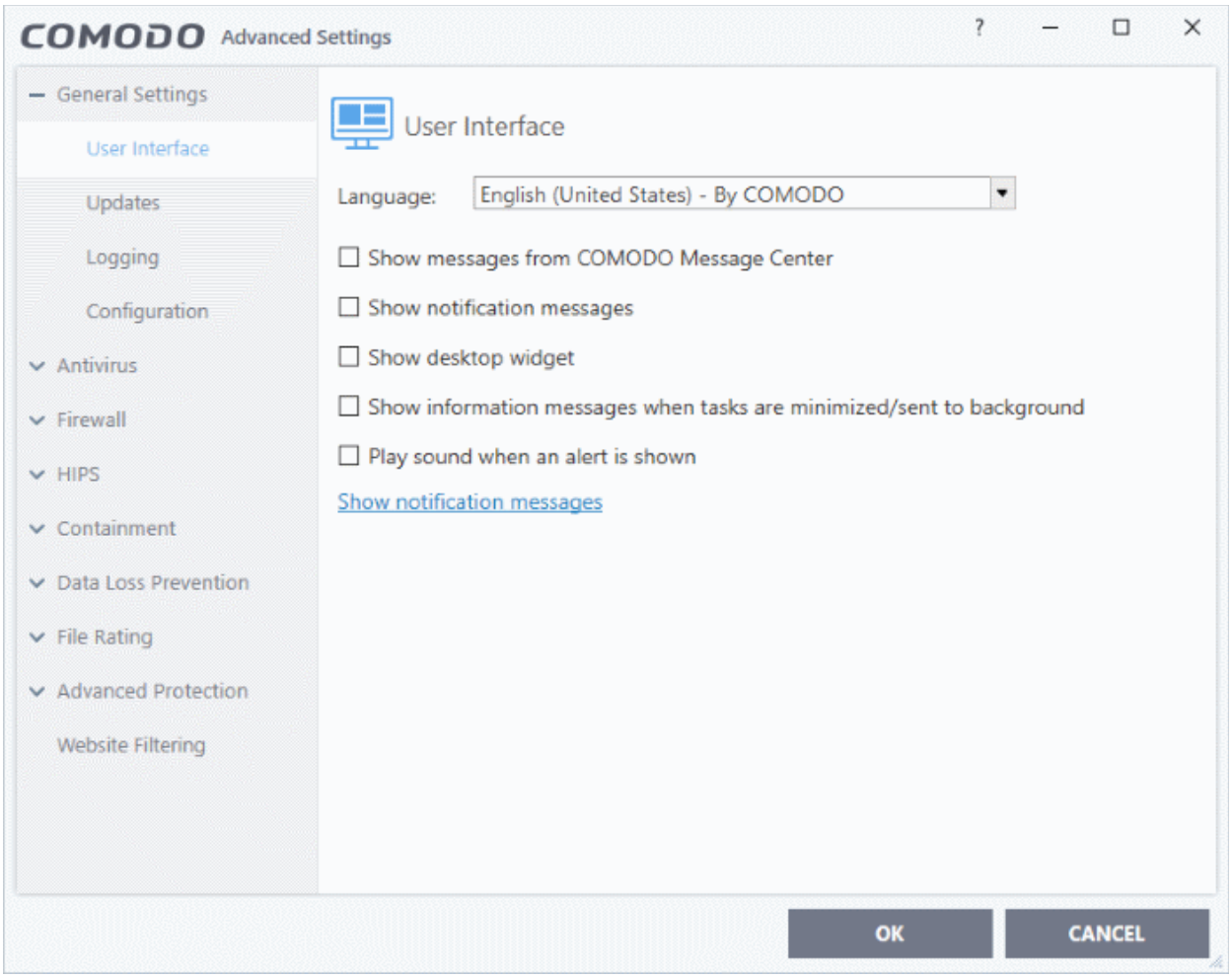
- Click 'Settings' > 'General Settings'
- The general settings area lets you customize the appearance and overall behavior of Comodo Client

Security.

- You can configure the interface language, notifications, automatic updates, logging, and more.

Configure General CCS Settings

- Click 'Settings' on the CCS home screen
- Click 'General Settings' on the left:

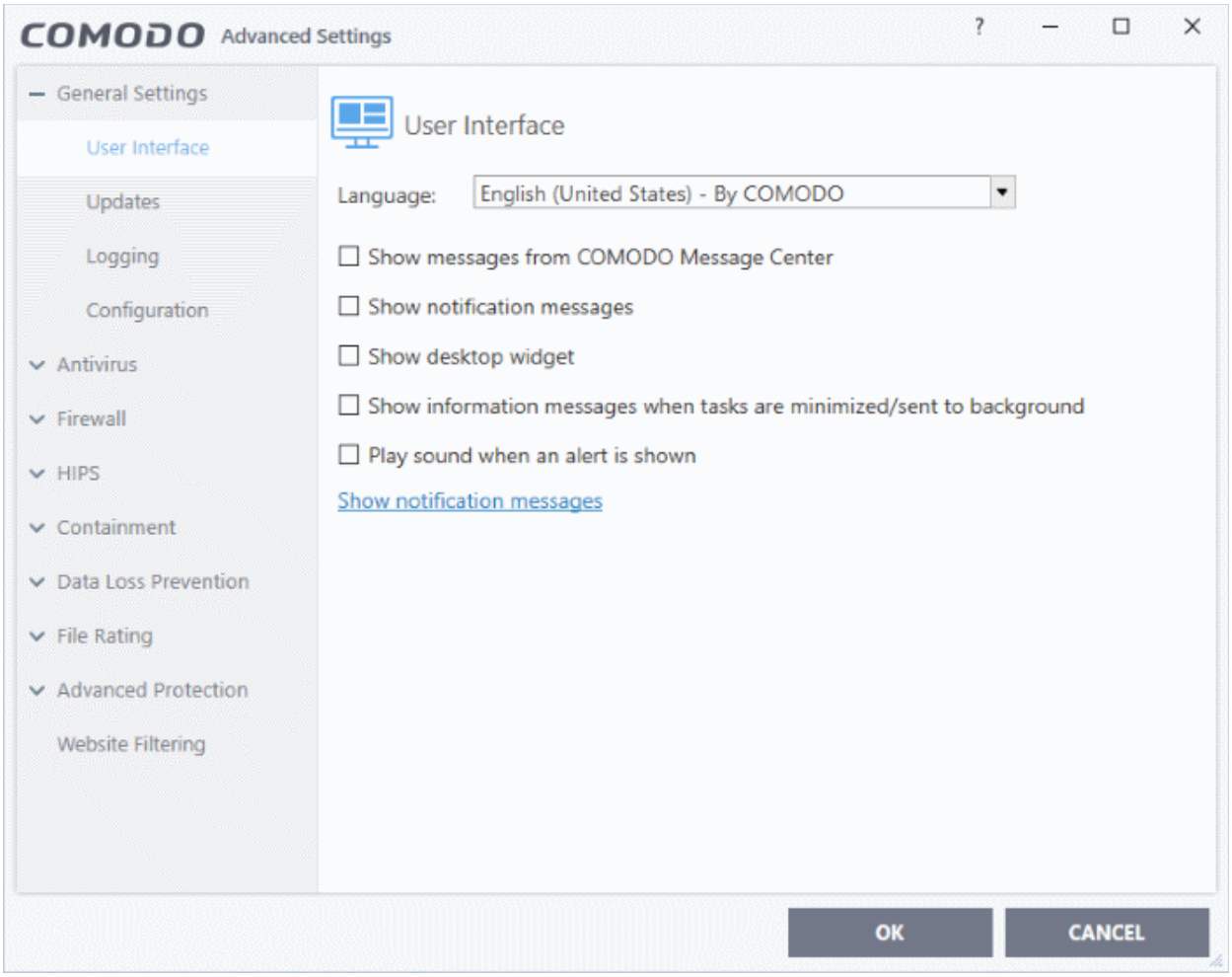


General settings is broken down into the following areas:

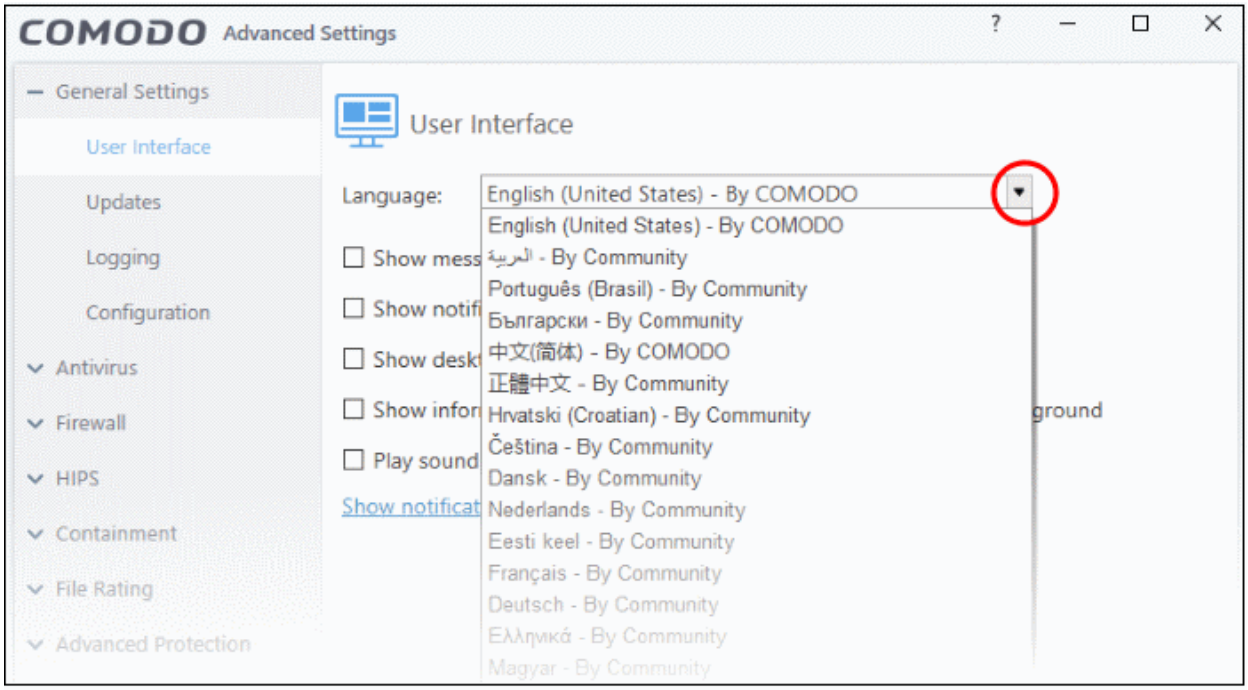
- **User Interface**
- **Updates**
- **Logging**
- **Configuration**

7.1.1. Customize User Interface

- Click 'Settings' > 'General Settings' > 'User Interface'
- The user interface tab lets you choose your preferred language, and customize the look and feel of the application.



- **Language Settings** - Comodo Client Security is available in many different languages. Switch languages by clicking the 'Language' drop-down menu: (***Default = English (United States)***).

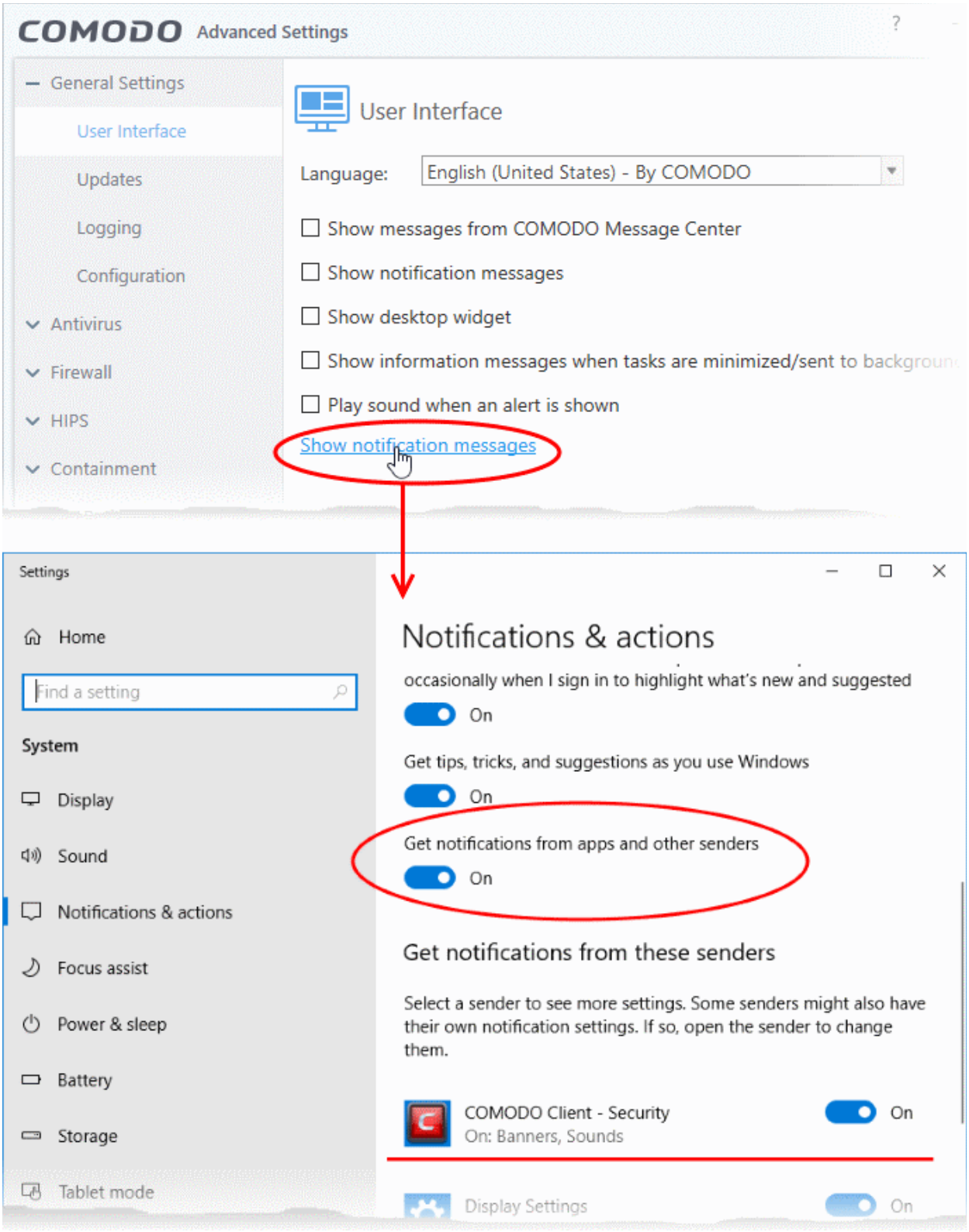


- **Show messages from COMODO Message Center** - Message center messages keep you abreast of Comodo news and special offers. If enabled, the messages will periodically appear as small pop-ups. (***Default = Disabled***)

- **Show notification messages** - CCS system notices appear in the bottom right-hand corner of your screen (just above the tray icons). They inform you about any actions that CCS is taking, and any CCS status updates. (***Default = Disabled***)

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

  - Click the 'Show notification messages' link
  - This opens the Windows 'Notifications and Actions' page
  - Enable 'Get notifications from apps and other senders'
  - Enable 'Comodo Client - Security' in the senders list

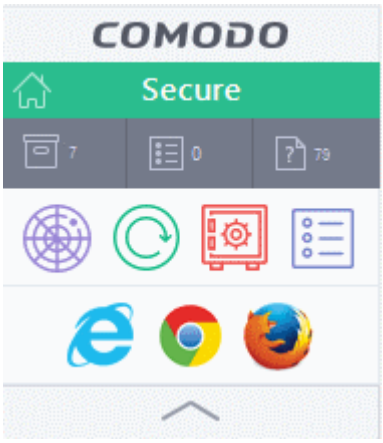


- **Show desktop widget** - The desktop widget shows your overall security status, outgoing and incoming traffic, and any background tasks.

  The widget also contains shortcuts to open CCS, to open the task manager, to open your browsers, and to visit social network sites.

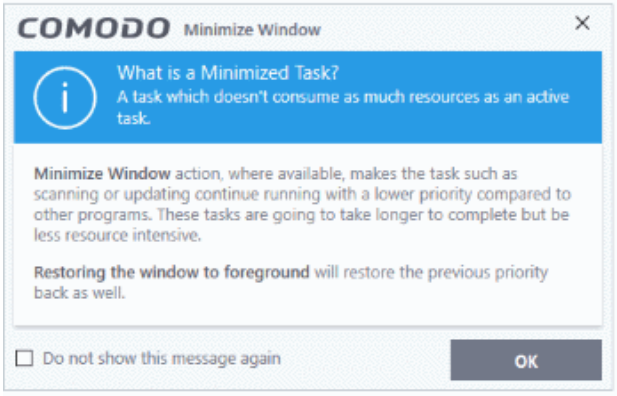
  Select this checkbox if you want the widget on your desktop. (***Default = Disabled***)

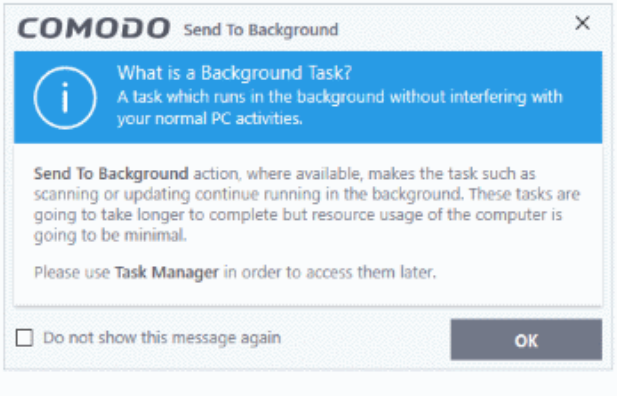
Tip: You can also enable or disable the widget by right-clicking on the CCS system icon.



See **The Widget** for more details.

- **Show information messages when tasks are minimized/sent to background** - CCS can show messages which explain what happens when you minimize or move a task:





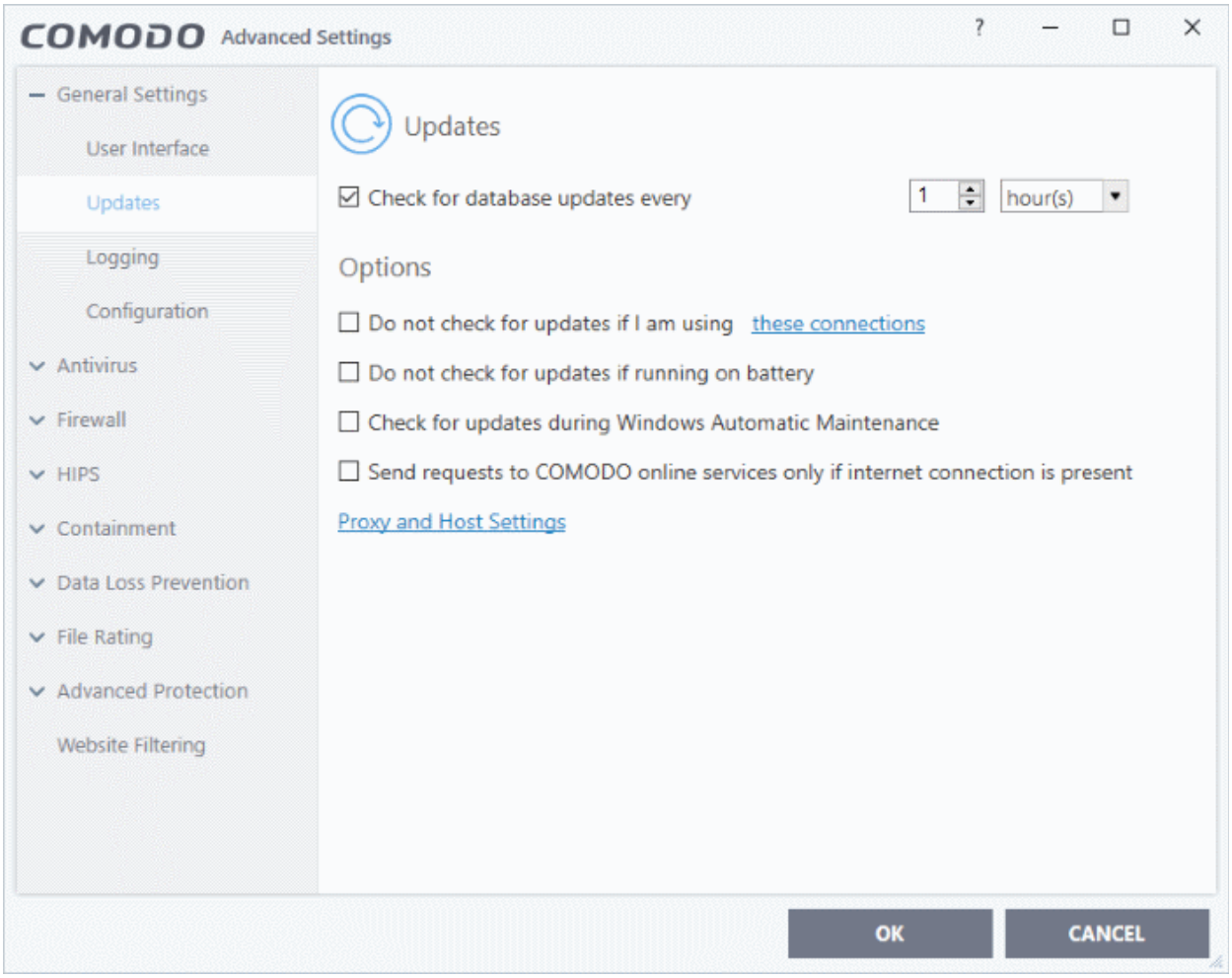
Disable this setting if you don't want to view these messages (***Default = Disabled***).

- **Play sound when an alert is shown** - CCS plays a chime when it shows a security alert. (***Default = Disabled***).
- Click 'OK' for your settings to take effect

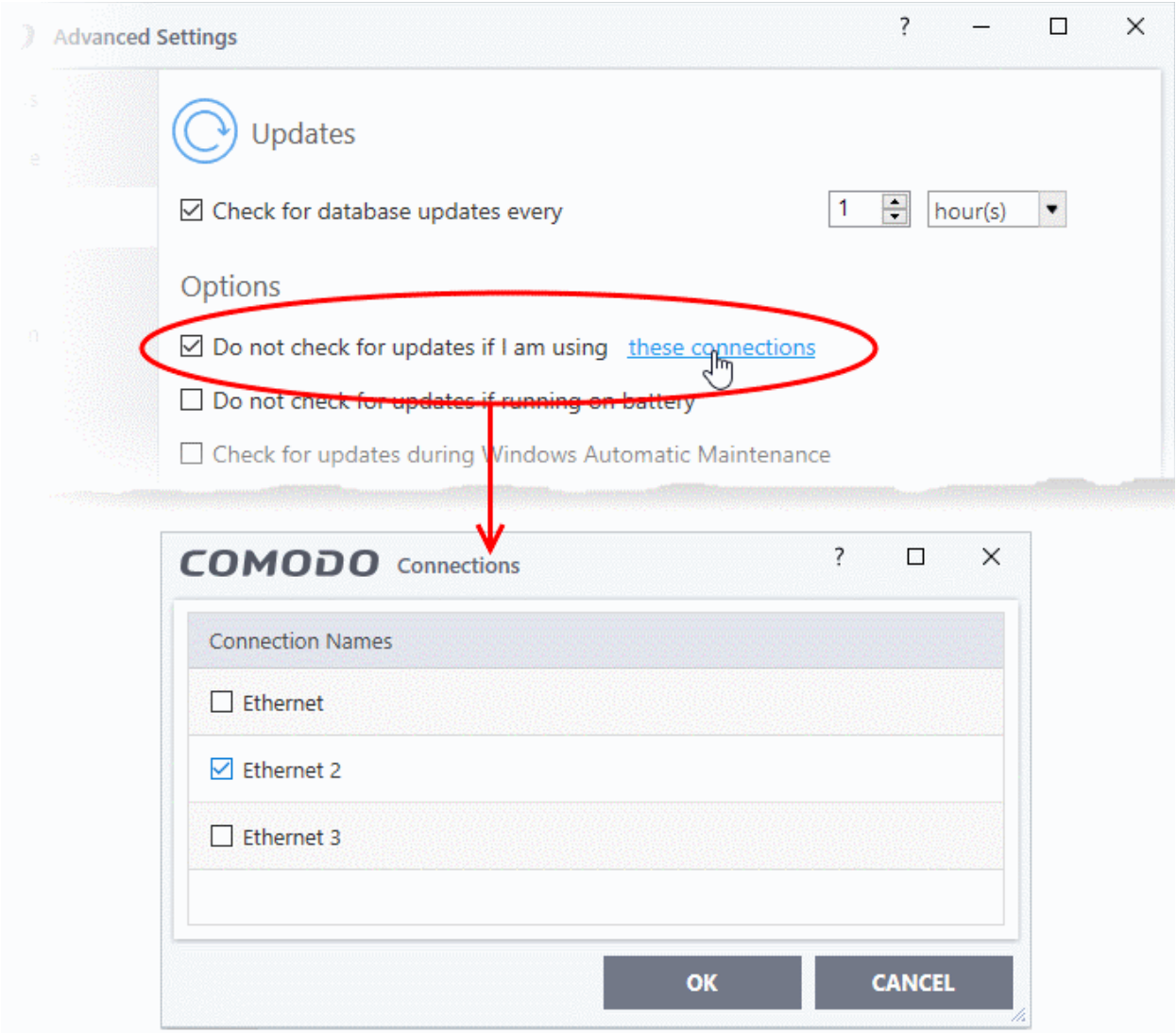
Note: In a managed network, CCS settings are governed by Endpoint Manager.

7.1.2. Configure Virus Database Updates

- Click 'Settings' > 'General Settings' > 'Updates'
- This area lets you configure CCS program and database updates:



- **Check for database updates every...** - Set how frequently CCS should check for application updates. Updates are downloaded from Comodo servers by default, but you have the option to **set a local server** to handle them instead. Select the interval in hours / days. (***Default and recommended = every 1 hour***)
- **Do not check updates if am using these connections** - CCS will not check for updates if you are using specific internet connections. For example, you may not wish to check for updates when using a wireless connection you know is slow or insecure. (***Default = Disabled***)
    - Enable 'Do not check updates if am using these connections'.
    - Click the 'these connections' link.
    - Select the connection over which you do not want to check for updates.
    - Click 'OK'.



- **Do not check for updates if running on battery** - CCS will not download updates if it detects your computer is on battery power. This is intended to extend battery lifetime on laptops. (***Default = Disabled***).
- **Check for updates during Windows Automatic Maintenance** - Allow CCS to receive updates when Windows is updating itself (***Default = Disabled***).
- **Send requests to COMODO online services only if internet connection is present** - By default, CCS automatically connects to Comodo servers for updates and essential services such as FLS, Endpoint Manager, and Valkyrie. This setting lets you disable these connection requests if you are not connected to the internet.

  This is how CCS will proceed if you enable or disable this setting:

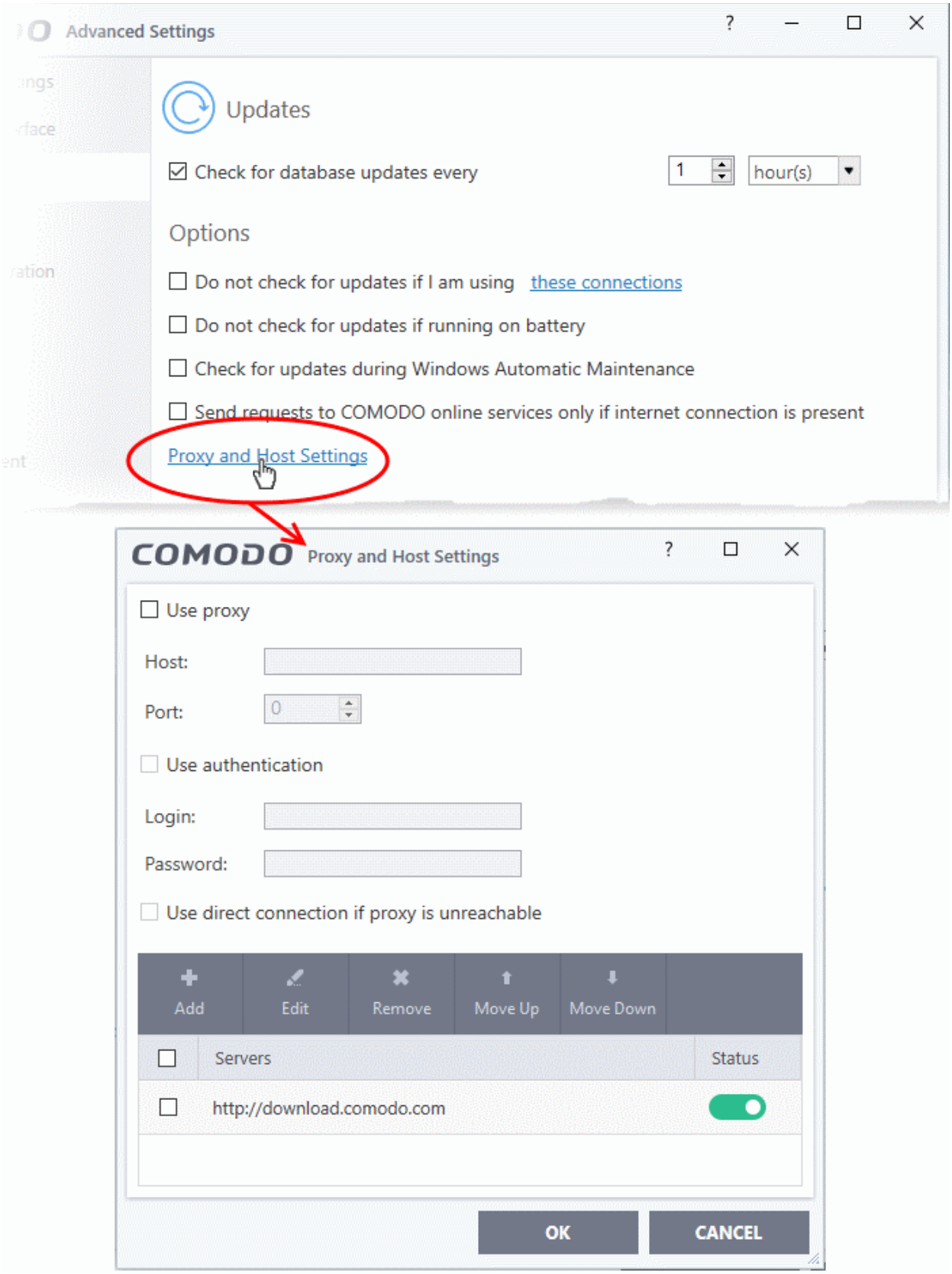
  - **Enabled + No internet connection** - CCS will not make requests to Comodo online services. A failure message is shown if you attempt a manual lookup, submit or update.
  - **Enabled + Connected to internet** - CCS makes requests to Comodo online services.
  - **Disabled + Connected to internet** - CCS makes requests to Comodo online services.
  - **Disabled + No internet connection** - CCS will make requests to Comodo online services, but will not be able to connect. An error message is shown.

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

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

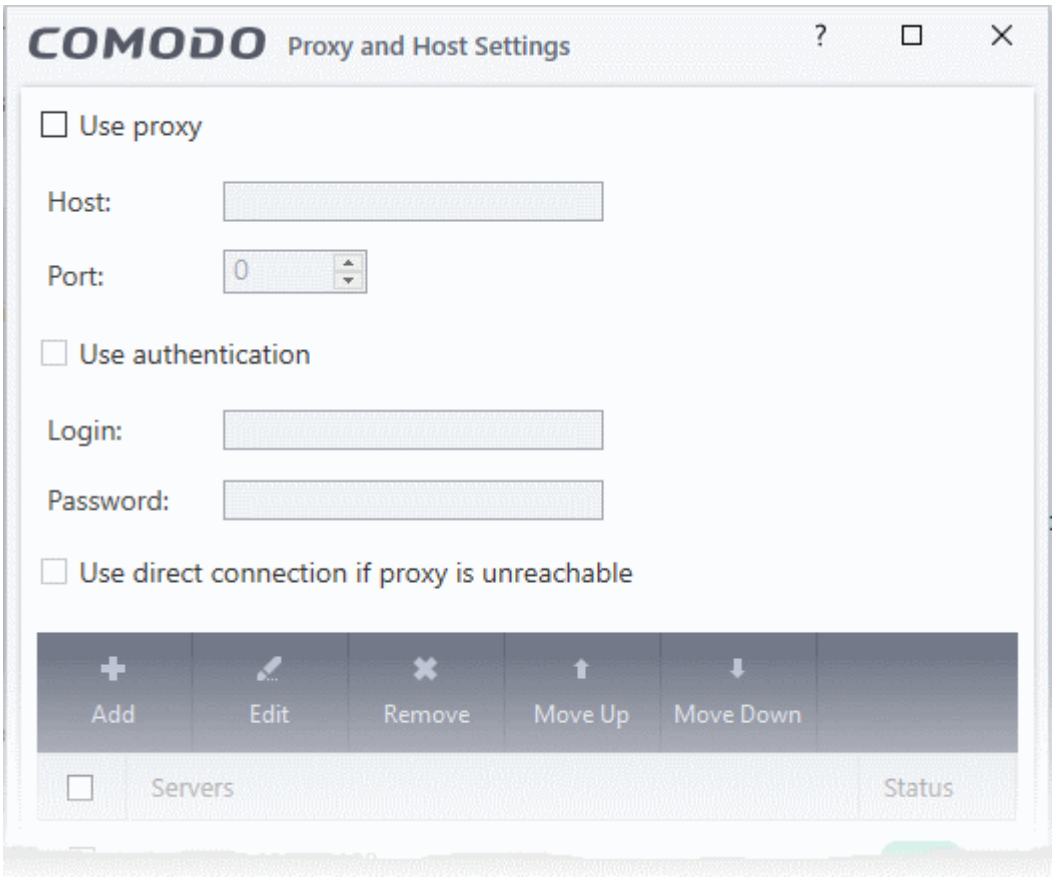
Configure proxy and host settings

- Click 'Proxy and Host Settings' at the bottom of the updates interface:



- **Configure a proxy server**
- **Add local servers for CCS to download updates from**

Configure a proxy server



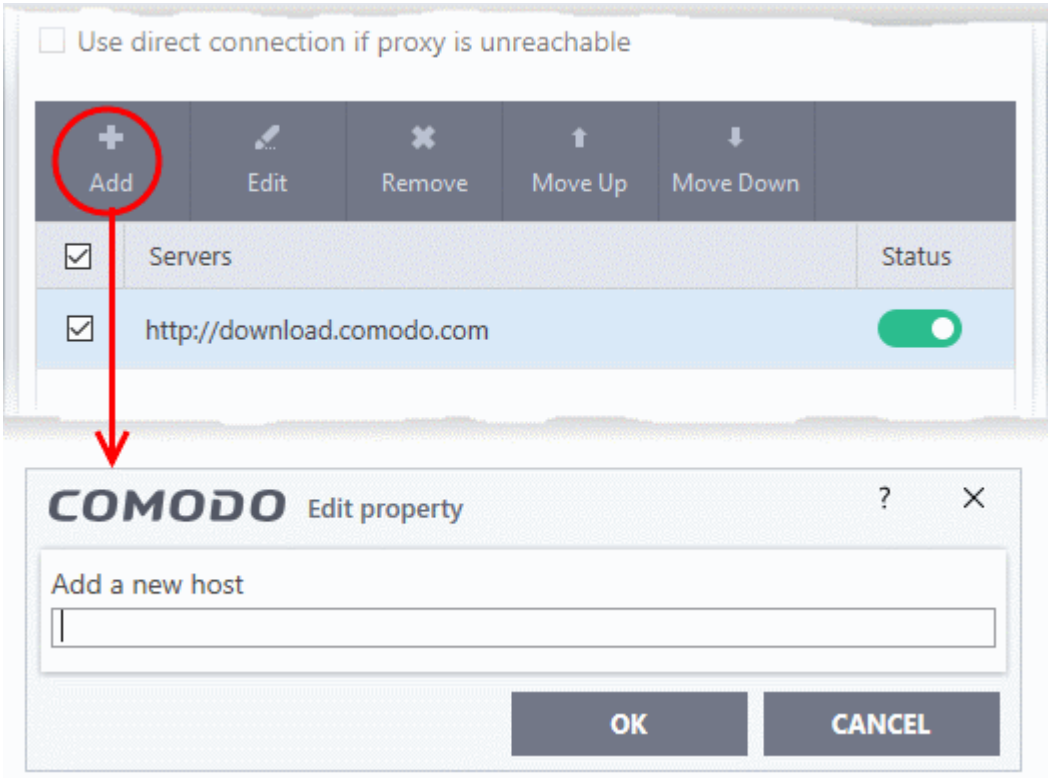
- **Use Proxy** - CCS will to connect to the update server through a proxy server.
  - Enter the host name or IP address of the proxy and the connection port
- **Use Authentication** - Provide the username and password of the proxy if required.
- **Use direct connection if proxy is unreachable** - Allow CCS to fallback to a direct internet connection if the proxy fails.
  - If you specify a proxy BUT disable direct connections, then CCS will not be able to connect to the download servers if the proxy fails.

Configure updates via local update server

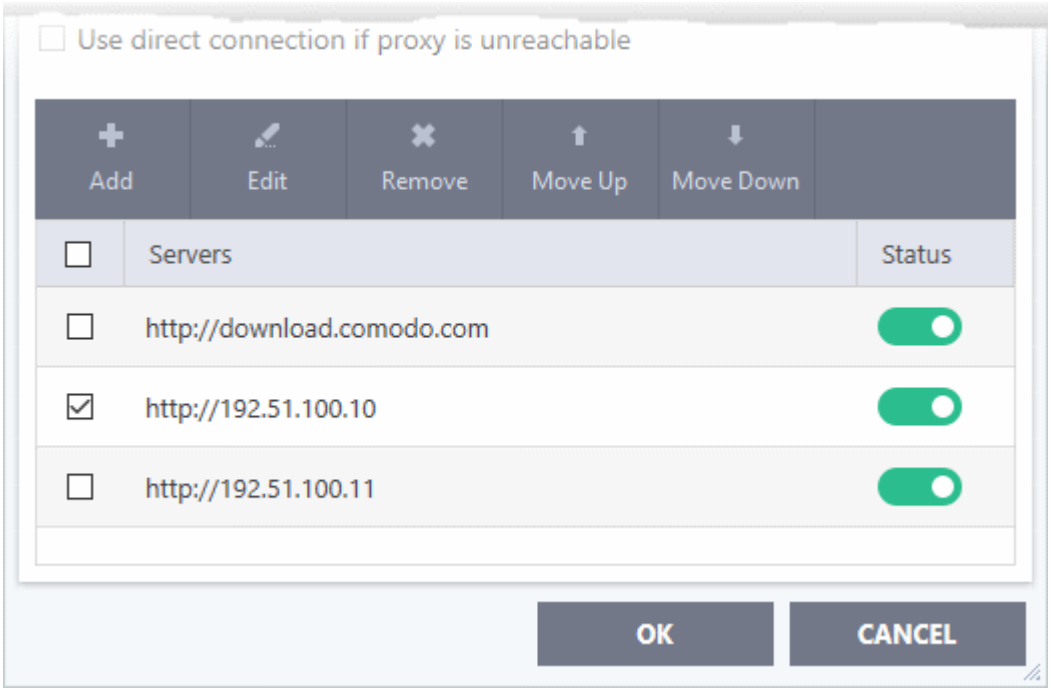
Note: You need to install the 'ESM Update Mirror' utility to download updates to the local server.

- Download the setup file from **https://drive.google.com/file/d/0B4qKr5xfENWBS0FOUHM2VDFQMnc/view**.
- Run the setup file on a Windows server and follow the wizard to install the application
- Ensure that the service has started:
  - 'Run' > Enter 'services.msc' > locate 'Apache2.2'
  - Click the 'Start' link on the left if the service is not running

  - Click the 'Add' button in the lower pane



- Enter the IP address or hostname of the server (with 'http://' prefix) and click 'OK'
- Repeat the process to add more local update servers



- Use the 'Move Up' and 'Move Down' buttons to choose the order in which servers should be consulted. CCS will download from the first server that contains new updates.
- Use the status switches to activate or deactivate individual servers

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

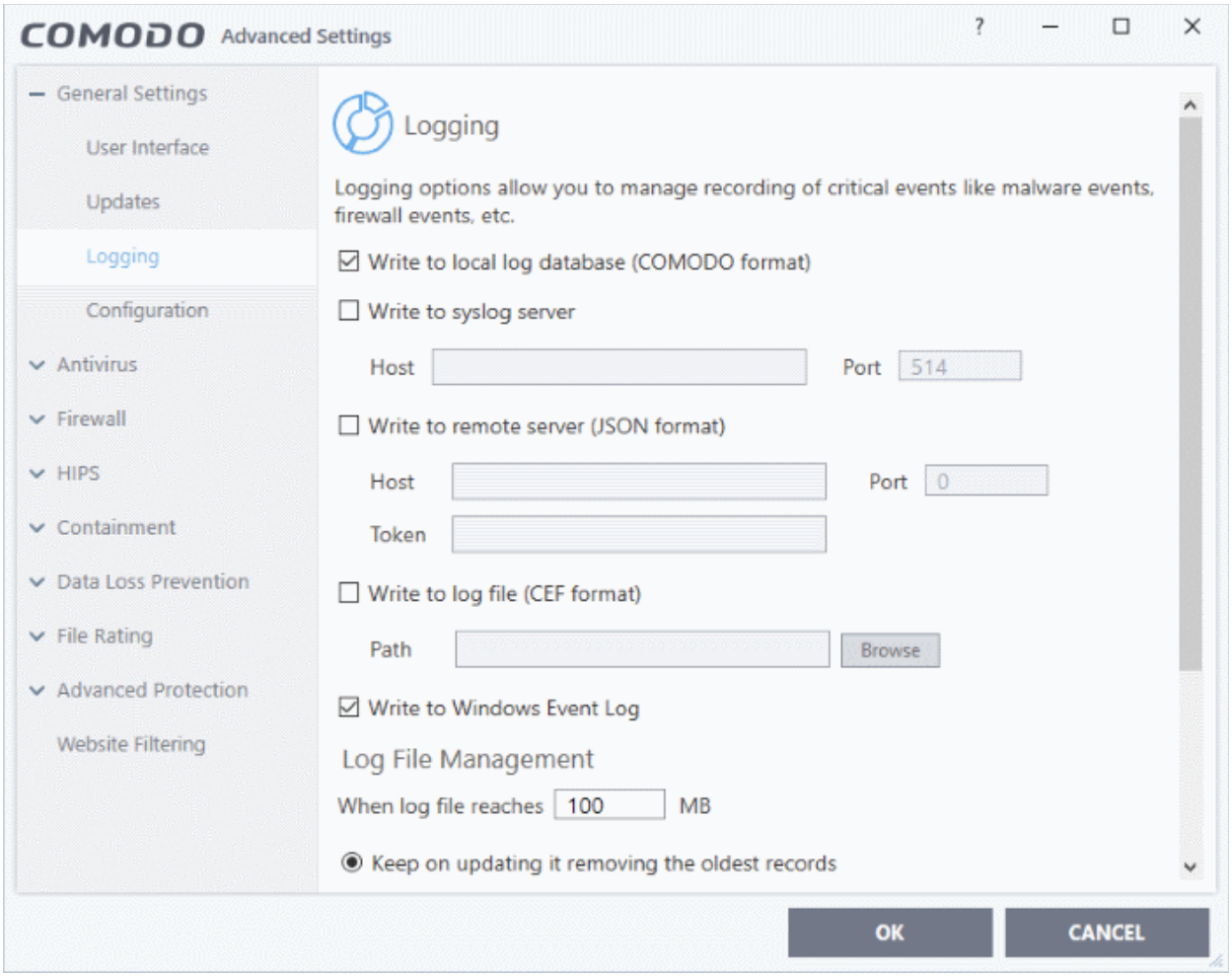
7.1.3. Log Settings

- Click 'Settings' > 'General Settings' > 'Logging'
- Comodo Client Security keeps detailed records of all antivirus, firewall, HIPS, containment, device control, VirusScope and autorun events.
- Logs are also created for 'Alerts Displayed', 'Tasks Launched', 'File List' changes, 'Vendor list changes' and 'CCS Configuration Changes'.
- Log settings let you specify the storage location, the maximum size of log files, and how CCS should react if the maximum file size is exceeded.

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

Configure log settings

- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Logging':



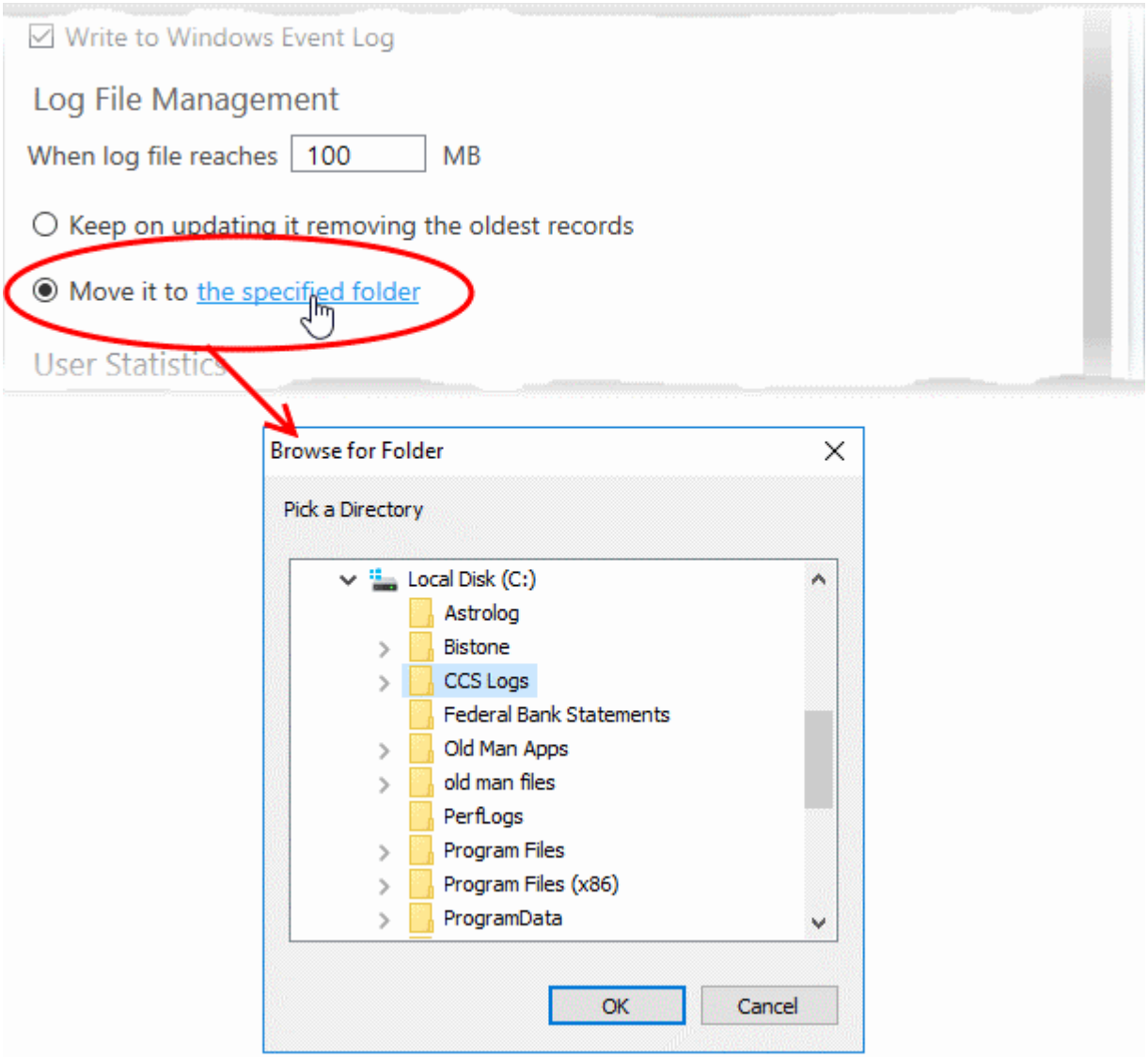
Logging

- **Write to local log database (COMODO format)** - Enable or disable logs in Comodo format (***Default = Enabled***)
- **Write to Syslog Server (CEF Format)** - CCS forwards the logs to an external Syslog server integrated with Endpoint Manager (EM). Enter the IP/hostname and port of the Syslog server in fields provided. (Default = Disabled).

- **Write to remote server (JSON format)** - CCS forwards the logs over https to a server integrated with Endpoint Manager. (***Default = Disabled***).
    - **Host** - Enter the IP address or the host name of the server
    - **Port** - The port through which the server listens to the CCS logs
    - **Token** - Enter the client authentication token so CCS can connect and forward logs to the server. The token is generated when you configure the HTTP Event Collector (HEC) on the server.
    - See **https://docs.splunk.com/Documentation/Splunk/7.2.6/Data/UsetheHTTPEventCollector** if you need help to setup the event collector and generate a token.
    - Enter the IP/hostname and port of the server in fields provided. Enter the security token to access the remote server in the field provided.
- **Write to Log file (CEF) Format** - CCS stores the logs at a specific local or network location. Click 'Browse' to select the storage location (Default = Disabled).
- **Write to Windows Event Logs** - CCS logs are appended to 'Windows Event' logs . (Default = Enabled)
    - Type 'Event Viewer' in Windows search to view Windows logs

Log File Management

- Specify what should happen when the log file reaches a certain size. You can choose keep the older logs or discard them.
    - **When log file reaches** - Enter the maximum size of a log file in MB. (Default = 100MB)
    - **Keep on updating it removing the oldest records** - When a log file reaches the max. size, CCS will delete the earliest log entries to make room for the new entries. (Default = Enabled)
    - **Move it to the specified folder** - When a log file reaches the max. size, CCS starts a new log file and moves the old one to a folder of your choice. (Default = Disabled)
        - Select the option and click 'the specified folder' to choose the storage folder:



The selected folder path will appear beside 'Move it to'.

User Statistics

- **Send anonymous program usage statistics to Comodo** - Comodo collects usage details so we can analyze how our users interact with CCS. This real-world data allows us to create product improvements which reflect the needs of our users. If you enable this option, CCS will periodically send usage data to Comodo servers through a secure, encrypted channel. Your privacy is not affected because the data is anonymized. Disable this option if you don't want to send usage details to Comodo. ***(Default = Enabled)***

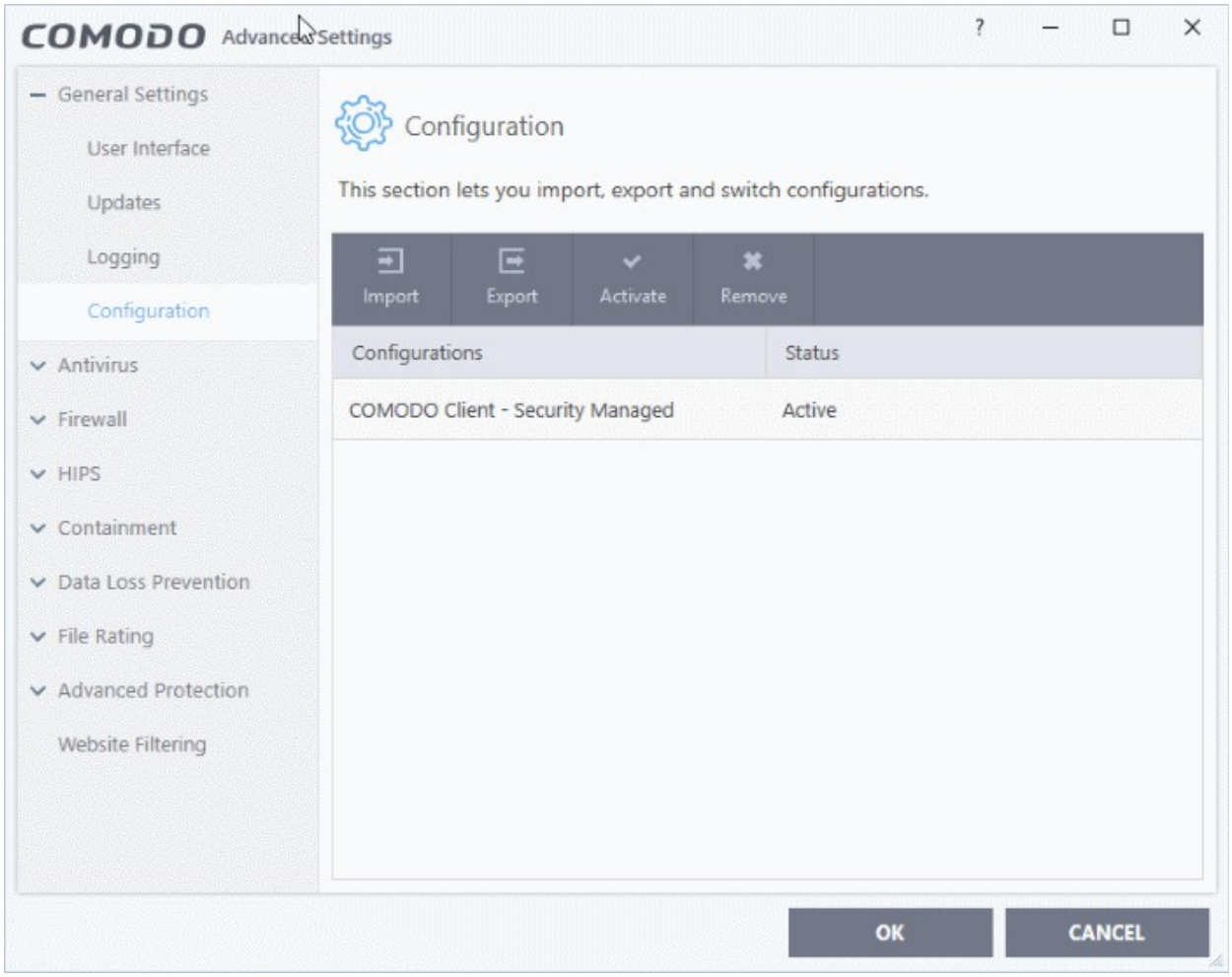
- Click 'OK' for your changes to take effect

7.1.4. Manage CCS Configurations

- Click 'Settings' > 'General Settings' > 'Configuration'
- CCS lets you export your current security settings as a profile. You can then import the profile on another computer with CCS installed, and avoid having to configure everything again.
- Exporting your settings is a great time-saver if:
  - You are a network admin who wants to implement a standard configuration on multiple computers.
  - You need to uninstall and re-install CCS or Windows, and want to quickly implement your old settings.

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

- The configurations area lets you switch your currently active profile and import/export profiles.
- Access the configuration settings interface
- Click 'Settings' at the top of the CCS home screen
- Click 'General Settings' > 'Configuration'



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

- **Comodo Preset Configurations**
- **Importing/Exporting and Managing Personal Configurations**

7.1.4.1. Comodo Preset Configurations

- Comodo preset configurations implement strong security settings on your endpoints.
- CCS ships with two preset configurations - 'Comodo Client Security' and 'Comodo Client Security Managed'.
  - 'Comodo Client Security Managed' is applied to managed endpoints by default.
  - 'Comodo Client Security' is applied to unmanaged endpoints
- Reminder - the 'Active' profile is, in effect, your current CCS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time.

Comodo Client Security Managed - The default configuration for computers managed by Endpoint Manager.
Important configuration information:

- HIPS is disabled.
- Auto-Containment is enabled.
- VirusScope 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.
- VirusScope alerts are disabled

Comodo Client Security - The default configuration on standalone (unmanaged) computers.
Important configuration information:

- HIPS is disabled.
- Auto-Containment is enabled.
- VirusScope is disabled.
- Realtime scan is enabled.
- Traffic filtering (Firewall) is enabled in Safe mode.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Advanced Protection is tuned to prevent infection of the system.
- Alert message notification is enabled.
- VirusScope alerts are disabled

If you wish to switch to Comodo Client - Security option, you can **select** the option from the 'Configuration' panel.

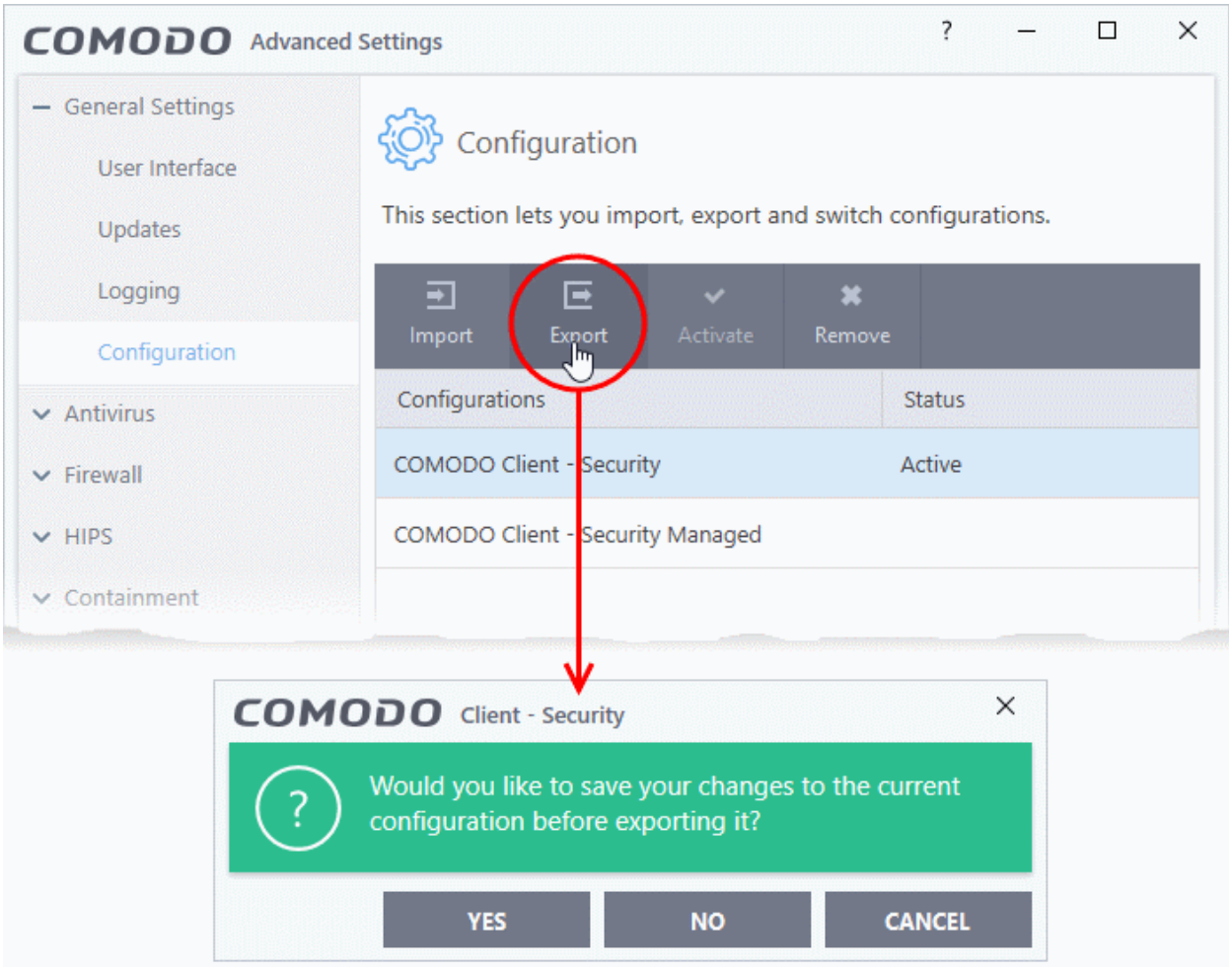
7.1.4.2. Personal Configurations

- Click 'Settings' > 'General Settings' > 'Configuration'
- You can import, export, activate and manage your custom CCS configurations
- Exported Configuration profiles have the file extension .cfgx.
- See the following sections for more information:
  - **Export a stored configuration to a file**
  - **Import a saved configuration from a file**

- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

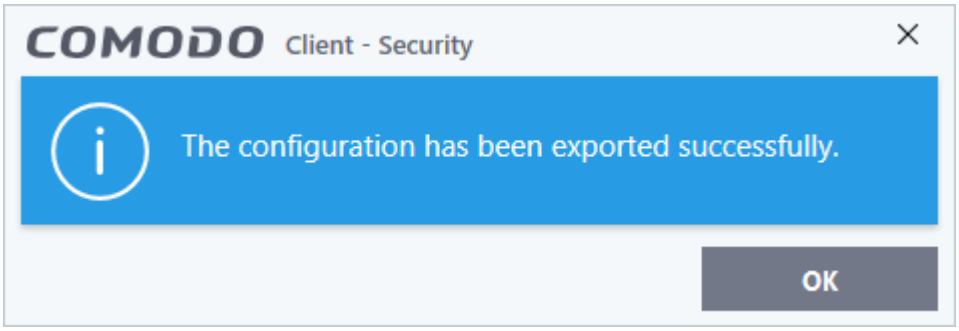
Export a stored configuration to a file

- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Configuration'
- Select a configuration profile then click 'Export'
- You will be given the chance to save any unsaved config. changes before exporting:



- Next, browse to the location where you want to save the configuration file.
- Create a name for the profile. For example, 'My CCS Settings', or 'CCS Highest Security Settings'
- Click 'Save':

A confirmation dialog will appear if the export is successful:

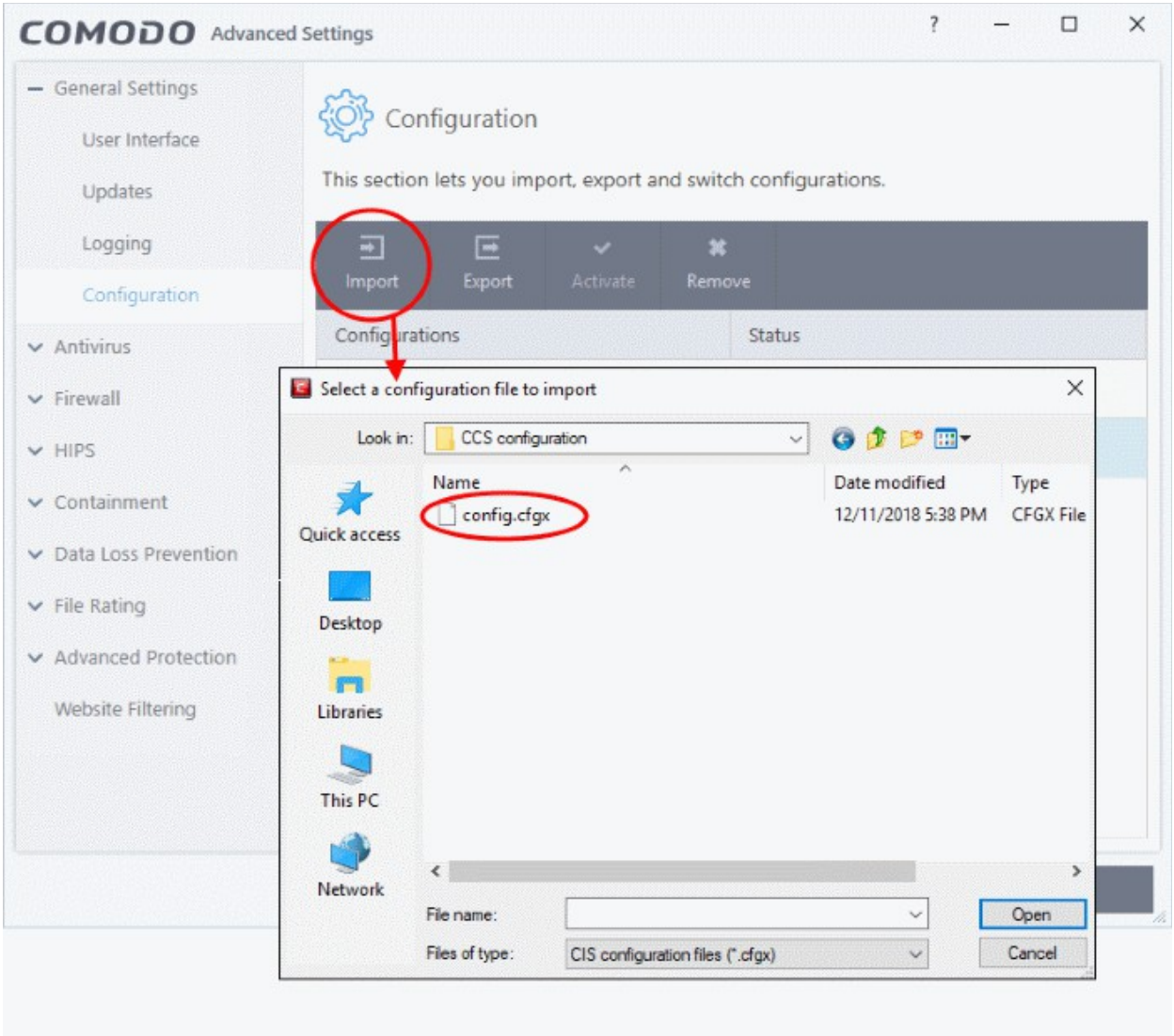


Import a saved configuration from a file

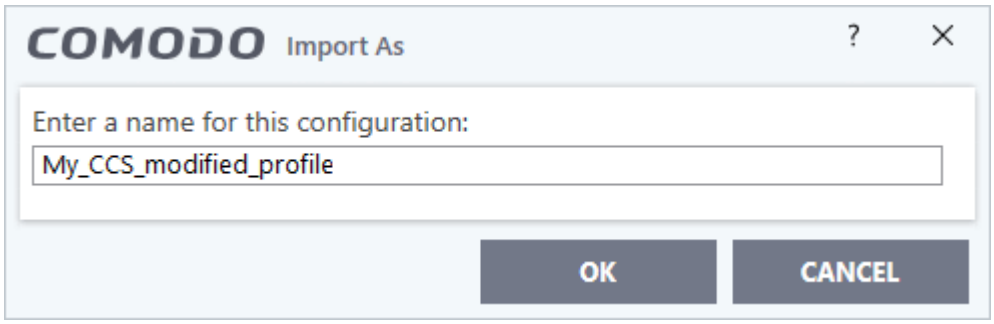
- You can import a CCS configuration from a previously saved file
- Note - After importing, you must **activate the profile** for it to take effect

Import a profile

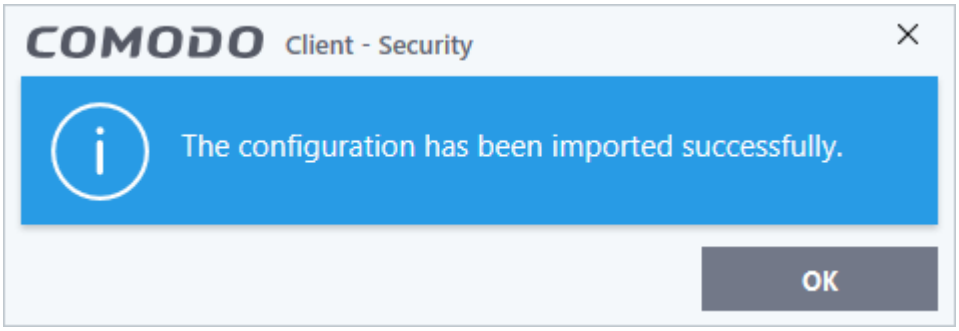
- Click 'Settings' at the top of the CCS home screen
- Click 'General Settings' > 'Configuration'
- Click the 'Import' button:



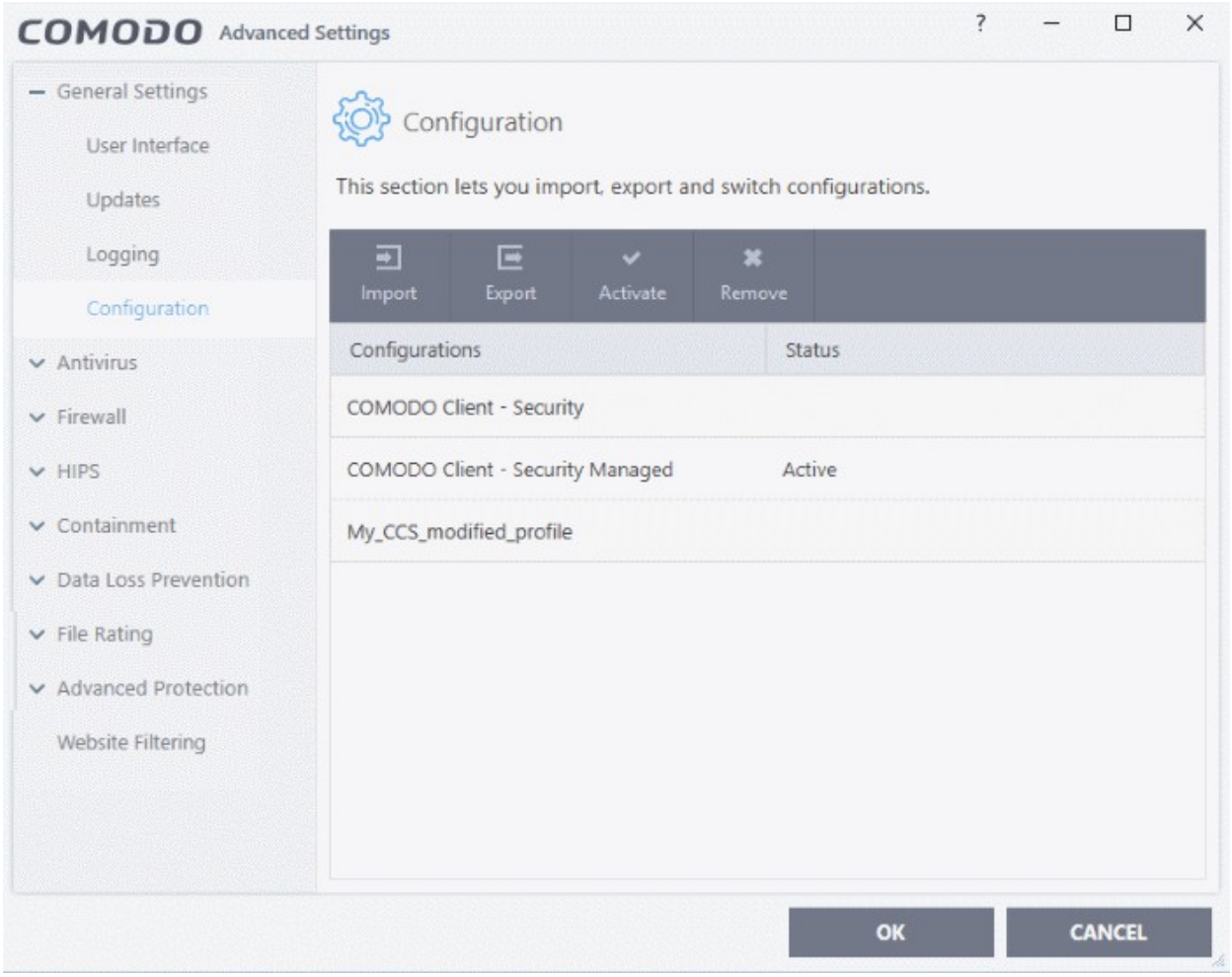
- Navigate to the location of the saved profile and click 'Open'. Configuration files have a .cfgx extension.
- Enter a name for the profile you wish to import and click 'OK'.



The following message is shown after a successful import:



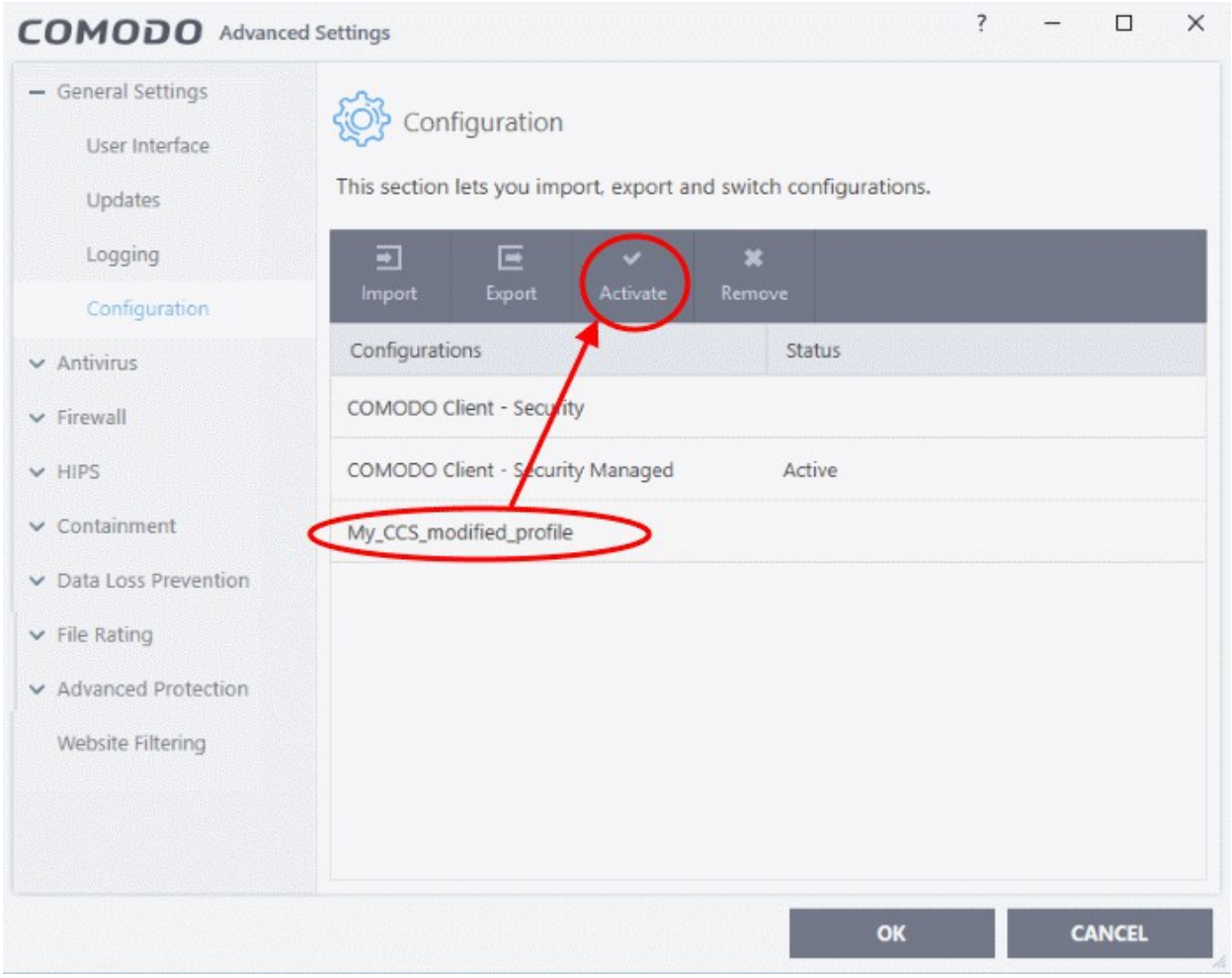
Activate the profile - Select the profile you just imported and click the 'Activate' button:



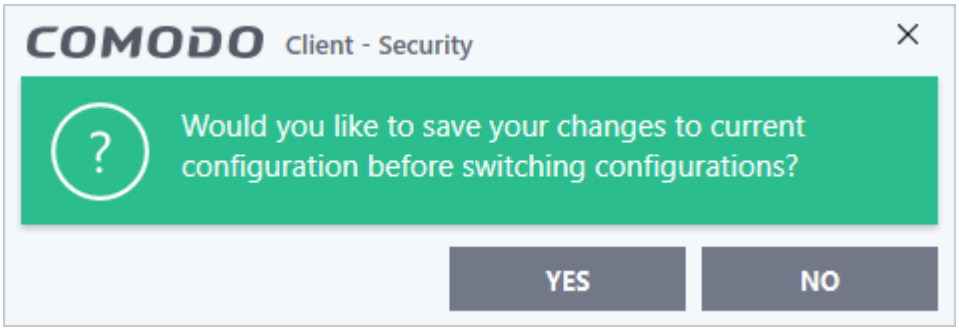
Select and implement a different configuration profile

You can change the active configuration profile at any time.

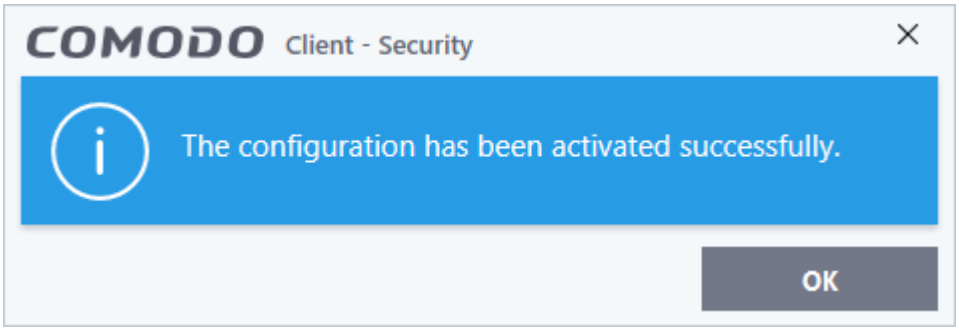
- Click 'Settings' at the top of the CCS home screen
- Click 'General Settings' > 'Configuration'
- Choose the profile you want to enable and click the 'Activate' button:



You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.



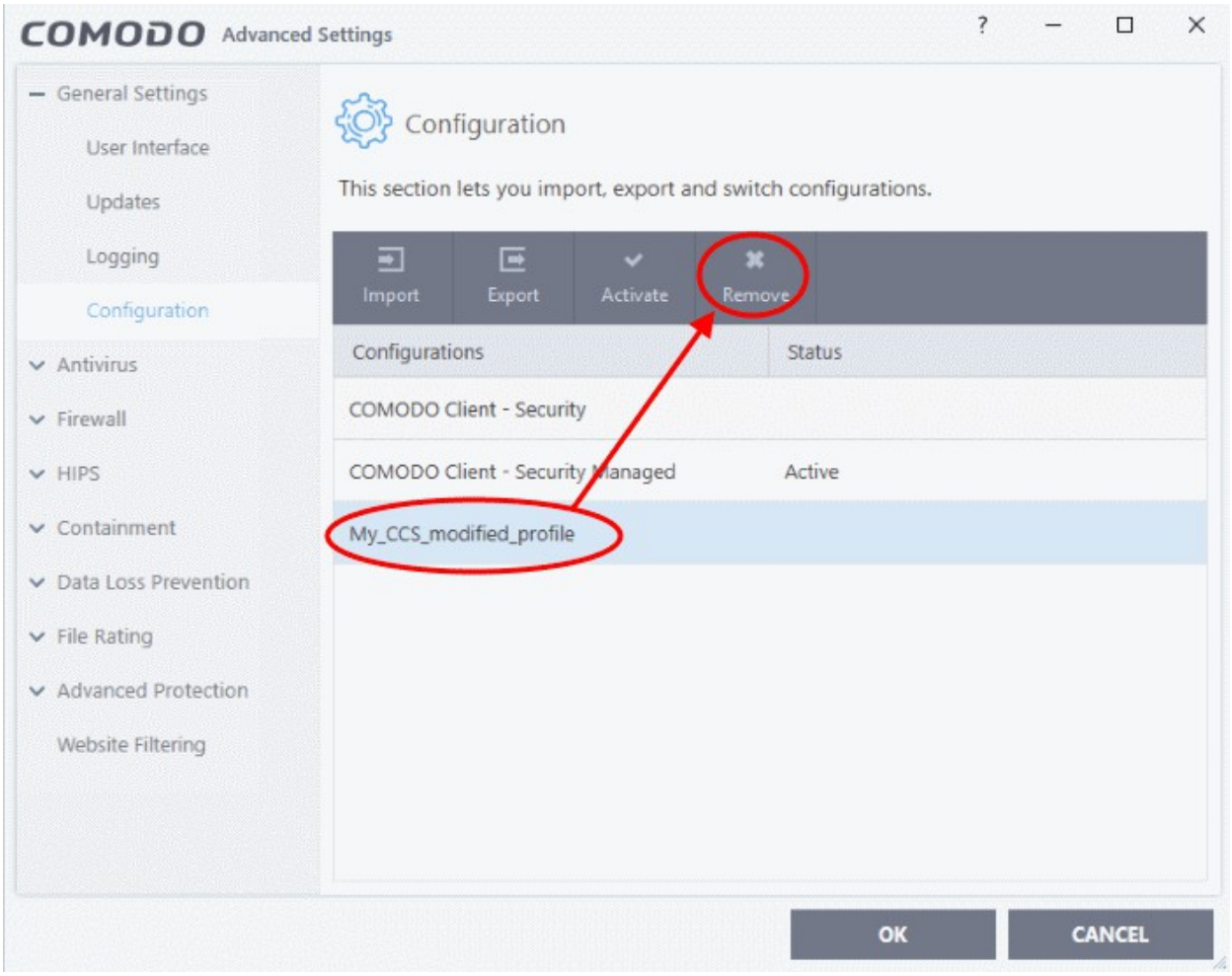
4. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.



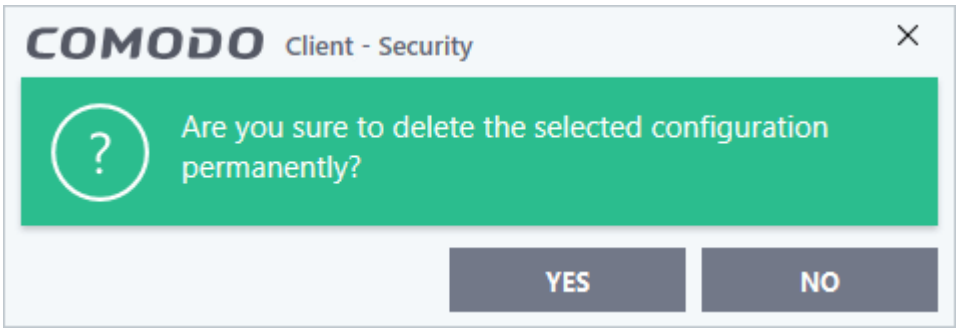
Delete an inactive configuration profile

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

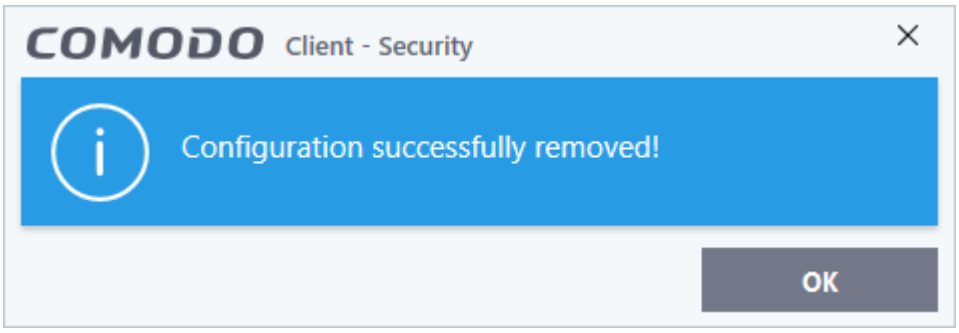
- Click 'Settings' on the CCS home screen
- Click 'General Settings' > 'Configuration'
- Choose the configuration profile you want to delete then click the 'Remove' button



A confirmation dialog will be displayed.



5. Click 'Yes'. The configuration profile will be deleted from your computer.

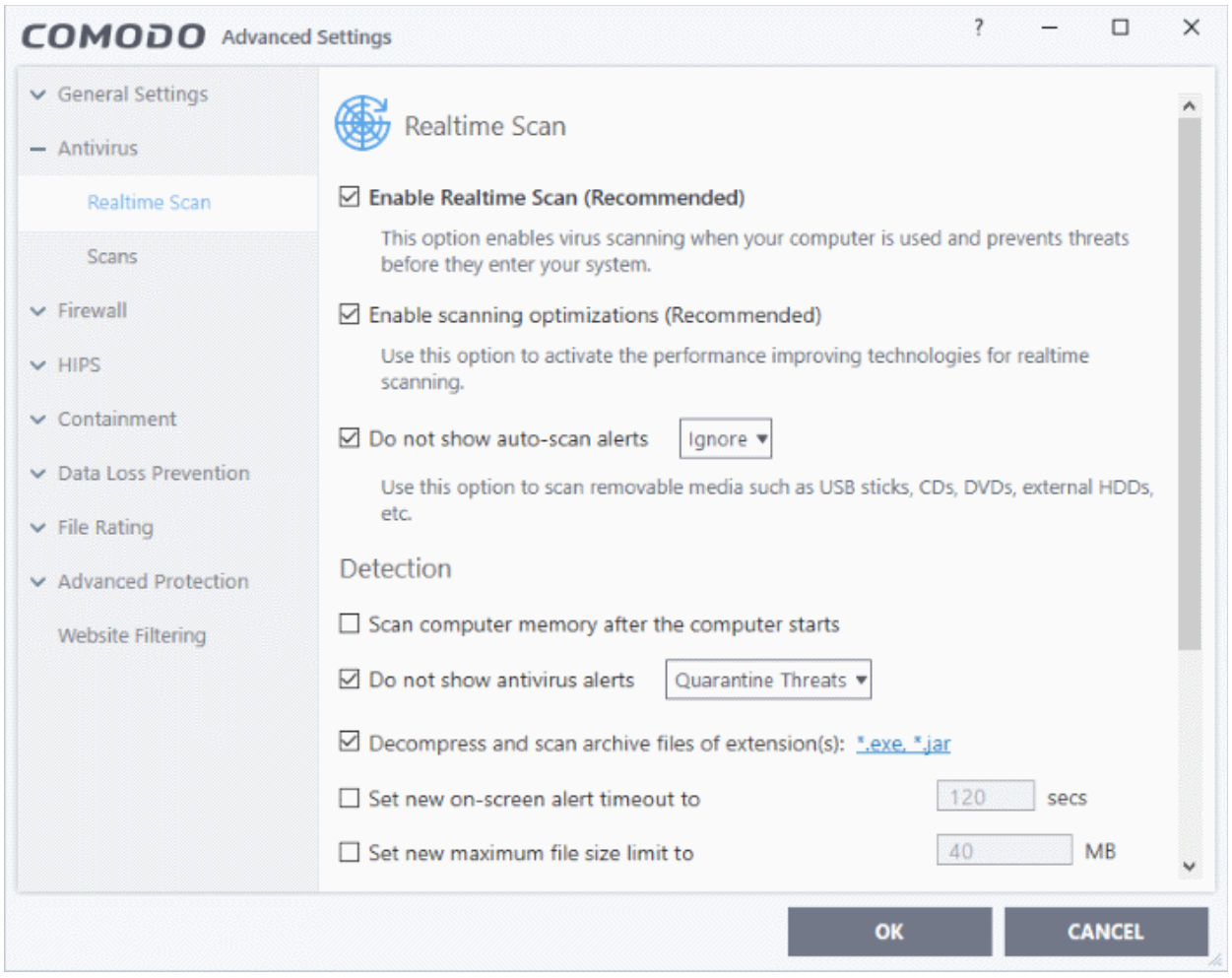


7.2. Antivirus Configuration

- Click 'Settings' > 'Antivirus'

The 'Antivirus' settings area lets you configure:

- The behavior of the real-time antivirus monitor
- Scan profiles for on-demand and scheduled scans



The following sections explain about:

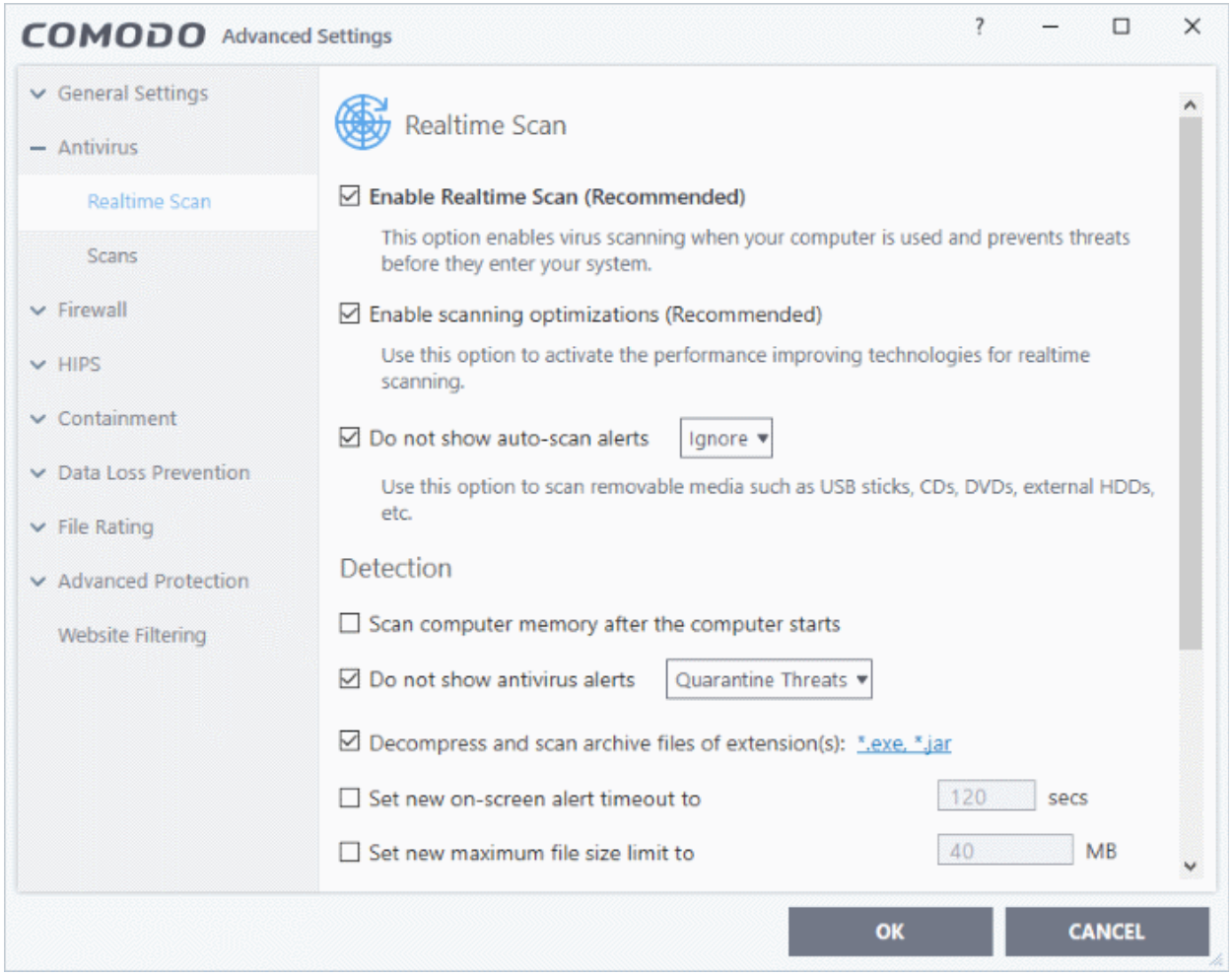
- **Real-time Scan Settings**
- **Custom Scan Profiles**

7.2.1. Real-time Scanner Settings

- Click 'Settings' > 'Antivirus' > 'Realtime Scan'
- The real-time scanner automatically checks for viruses whenever you open or move a file. It also monitors background activity for malicious processes.
- The real-time scanner also scans:
  - System memory on system startup
  - Any plugged-in removable storage devices
- You can specify that CCS does not show you alerts when it finds a threat, but automatically deals with the threat. You can choose to automatically quarantine or delete threats if you disable alerts.
- We strongly recommend you leave the real-time scanner enabled at all times.

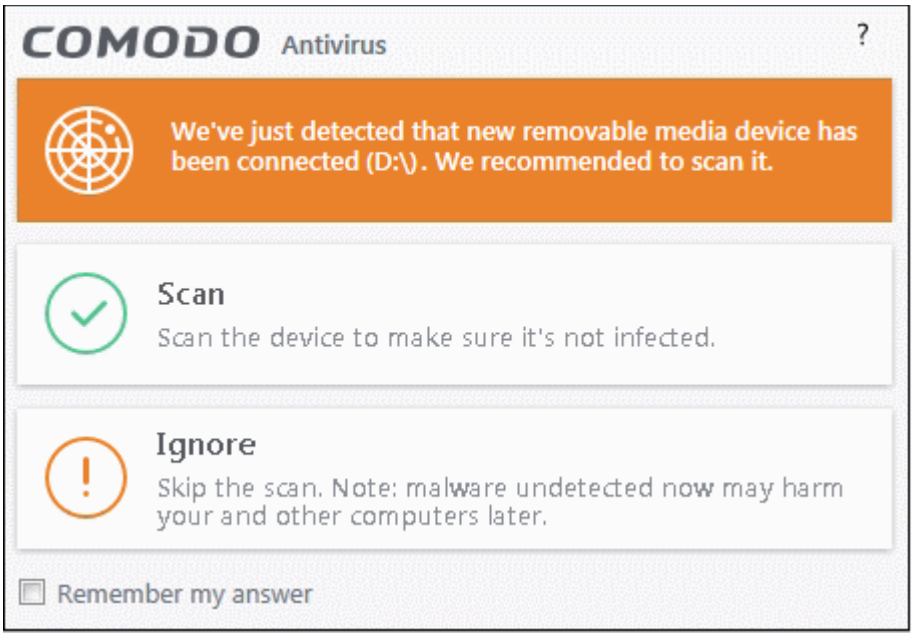
Configure real-time scans

- Click 'Settings' at the top of the CCS home screen
- Click 'Antivirus' > 'Realtime Scan' on the left



- **Enable Realtime Scan** - Activate or deactivate real-time scanning. The real-time scanner continually monitors your computer for malicious activity and protects you from threats as soon as they occur. Comodo strongly recommends you keep this option enabled. (***Default=Enabled***)
- **Enable scanning optimizations** - Will enable various techniques during a virus scan to reduce resource usage and speed-up the scan process. For example, antivirus scans will run in the background. ***(Default = Enabled)***

- **Do not show auto-scan alerts** - Select whether CCS alerts you when you plug a removable device into your computer (USB stick, portable HDD etc). The alert asks you whether you want to scan the device for viruses.
    - **Enabled** = Alerts are not shown. CCS will automatically take the action shown in the drop-down box next to the setting.
    - **Disabled** = Alerts are shown when you plug a removable device into your computer. You can choose to scan the device, or skip the scan. An example is shown below:



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

Detection Settings

- **Scan computer memory after the computer starts** - The antivirus scans system memory immediately after your computer starts up. Disable to remove the scan from the list of Windows startup processes. ***(Default = Disabled)***
- **Do not show antivirus alerts** - Configure whether or not alerts are shown to end-user when CCS finds malware.

  'Do not show antivirus alerts' will minimize disturbance but at some loss of user awareness. If you disable alerts alerts then please choose the default responses that CCS should take:

    - **Quarantine Threats** - Prevents the threat from running and moves it to quarantine (***Default***). You can review quarantined files at 'Tasks' > 'Advanced Tasks' > 'View Quarantine'.
    - **Block Threats** - Prevents the threat from running then deletes it from your computer.

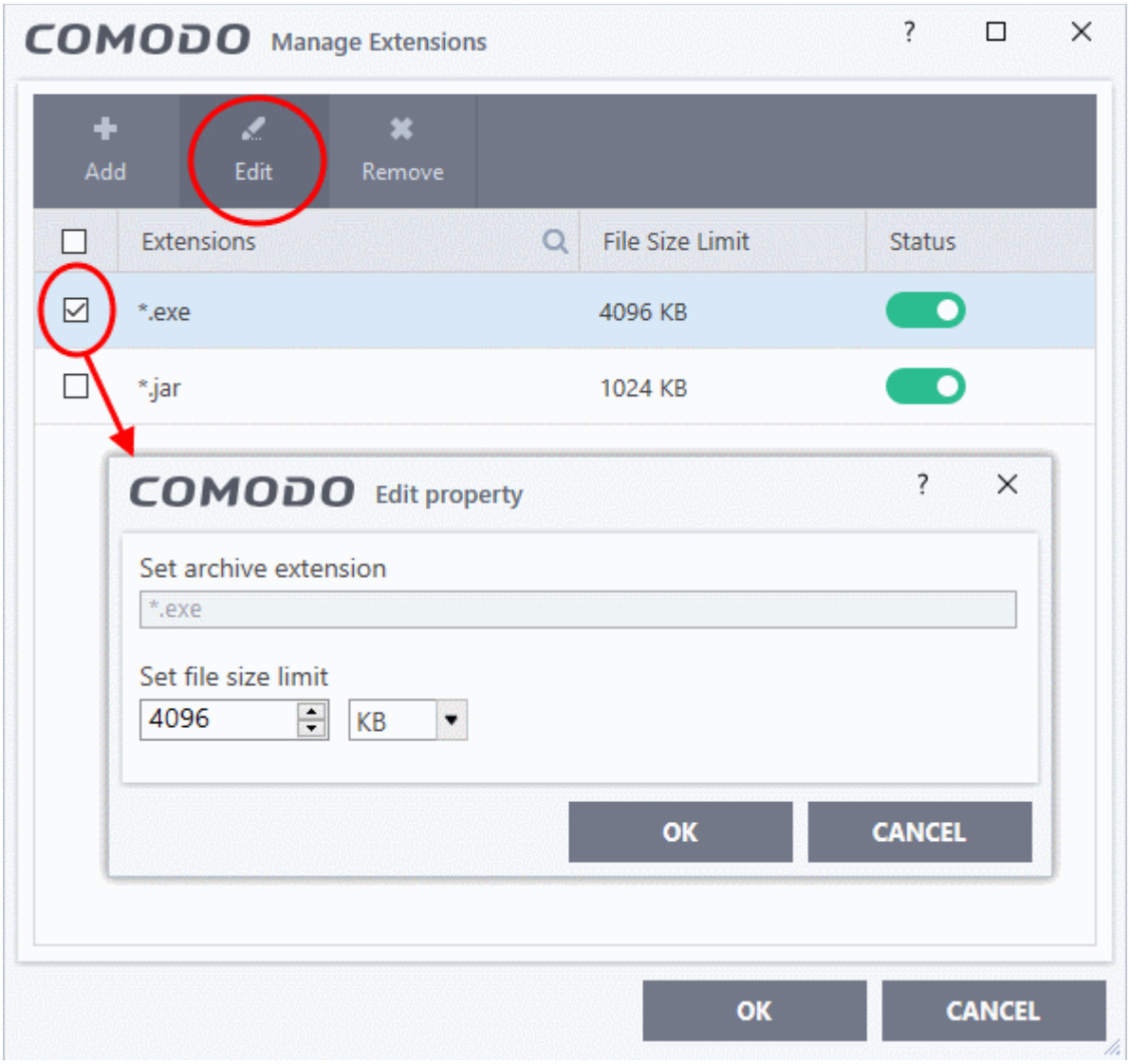
Note: If you disable this option then alerts are shown to users when malware is detected. The alert offers users the choice to quarantine or block the threat.

- **Decompress and scan archive files of extension(s)** - Comodo Antivirus will scan all types of archive files. Archive file types include .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB files. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default = Enabled)***

  You can manage the types of archives decompressed and scanned by Comodo Antivirus as follows:

    - Click file type link next to the setting (*.exe, *.jar)

- Click 'Add' to add another file type to the list.



- Enter the extension type you wish to scan and click 'OK'.
  - Example archive extensions include .zip , .rar, .msi, .7z , .jar and .cab.
- Set the max. size of this file type that CCS should scan. Files larger than this will not be scanned.
- Repeat the process to add more extensions
- Click 'OK' in the 'Manage Extensions' dialog

- **Set new on-screen alert timeout to** - Specify the length of time that virus alerts should stay on the screen. (***Default = 120 seconds***)
- **Set new maximum file size limit to** - Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here. (***Default = 40 MB***)
- **Set new maximum script size to** - Specify the largest script size that the antivirus should scan. CCS will not scan scripts bigger than the size specified here. (***Default = 4 MB***)
- **Use heuristics scanning** - Enable or disable heuristic scans, and define the sensitivity of the scanner. (***Default = Disabled***)

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

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

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

  Despite the name, this setting combines a very high level of protection with a low rate of false positives. We recommend this setting for most users.
- **Medium** - Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.

- **Enable realtime scanning of files on network** - Activate or deactivate automatic scans of files on network drives ***(Default = Disabled)***
  - If enabled, the scanner will check all files you interact with on a network drive, even if you do not copy them to your local machine.
  - If disabled, network files are not checked unless you copy them to your local machine.
- **Use Windows Anti-malware Scan Interface (AMSI) technology** - Microsoft AMSI technology allows 3rd party applications to request scans from antivirus products installed on the machine. CCS is on the AMSI provider's list. This feature provides enhanced malware protection for users, their data and applications. ***(Default = Enabled)***
  - Enabled - CCS will accept scan requests from AMSI enabled applications.
  - Disabled - CCS removes itself from the local AMSI providers list, and will not respond to scan requests.
- **Use cloud services while scanning via AMSI** - Available if 'Use Windows Anti-malware Scan Interface (AMSI) technology' is enabled. (***Default = Disabled***)
  - Enabled - CCS check a file's trust rating on our cloud severs as part of the AMSI scan process.
    - Note - Cloud Lookup must also be enabled in '**File Rating Settings**'.

7.2.2. Scan Profiles

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

An antivirus scan profile is a collection of scanner settings that tell CCS:

- What to scan (which files, folders or drives)
- When to scan (you can create a scan schedule)
- How to scan (you can configure the behavior of the scan engine)

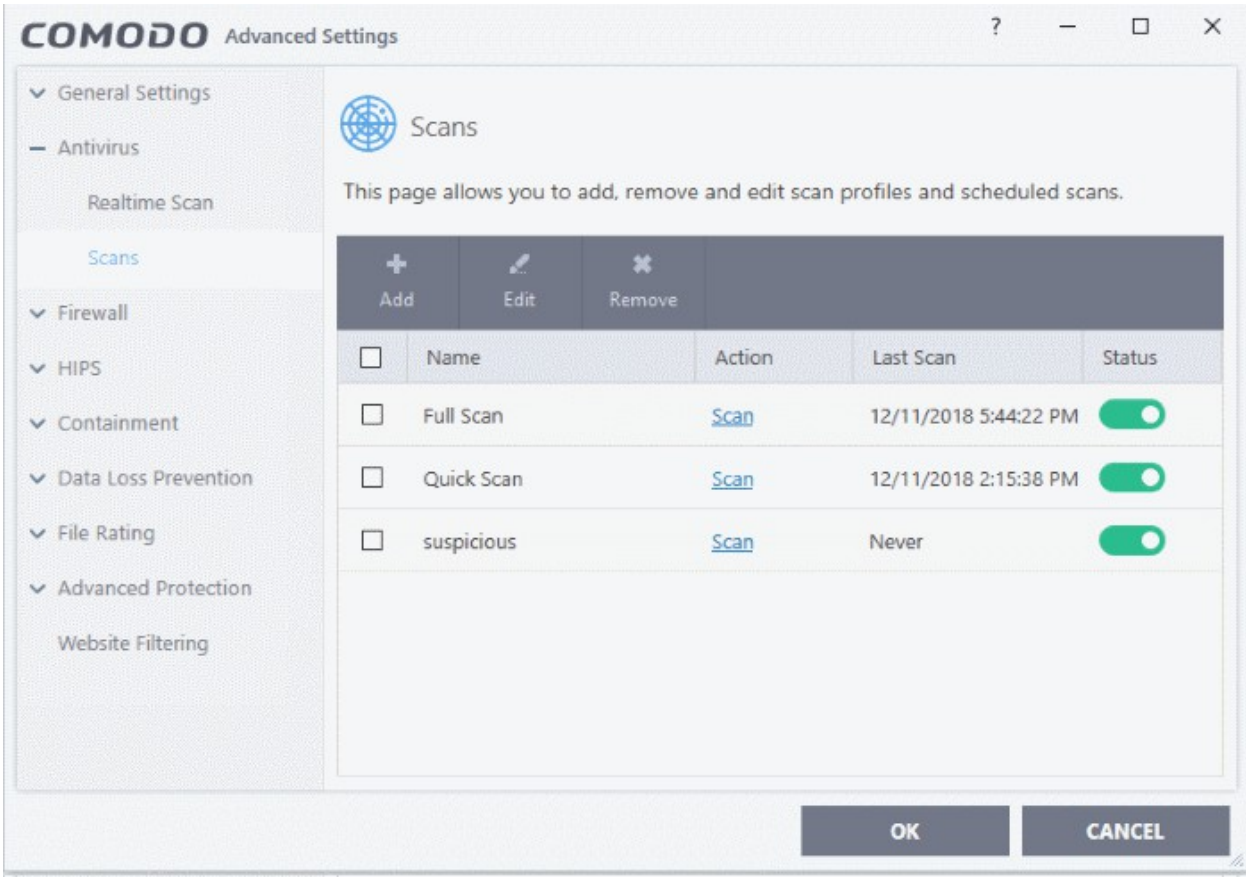
CCS ships with two pre-defined scan profiles and allows you to create custom scan profiles.

- **Full Scan** - Scans every file, folder and drive on your system. External devices such as USB sticks and storage drives are also scanned if connected.
- **Quick Scan** - Scans critical areas of your computer which are highly prone to infection and attack. Areas scanned include system memory, auto-run entries, hidden services, boot sectors, important registry keys, and system files. These areas are of great importance to the health of your computer, so it is essential to keep them clean.

You cannot modify the areas scanned in a pre-defined profile, but you can edit the scan parameters. You can also create custom profiles and scan schedules.

Open the 'Scans' panel

- Click 'Settings' on the CCS home screen
- Click 'Antivirus' > 'Scans'



Scan Profiles - Column Descriptions	
Column Header	**Description**
Name	Name of the scan profile.
Action	The activity that the profile is set to perform. Click this link to manually run a scan according to the profile's parameters.
Last Scan	Date and time of the most recent virus scan using this profile.
Status	Enable or disable the profile. 'On' - Any scheduled scans configured in the profile will continue to run. In addition, you can manually run the scan at any time by clicking the 'Scan' link. 'Off' - Any scheduled scans configured in the profile will not run. You can still manually run the scan by clicking the 'Scan' link.

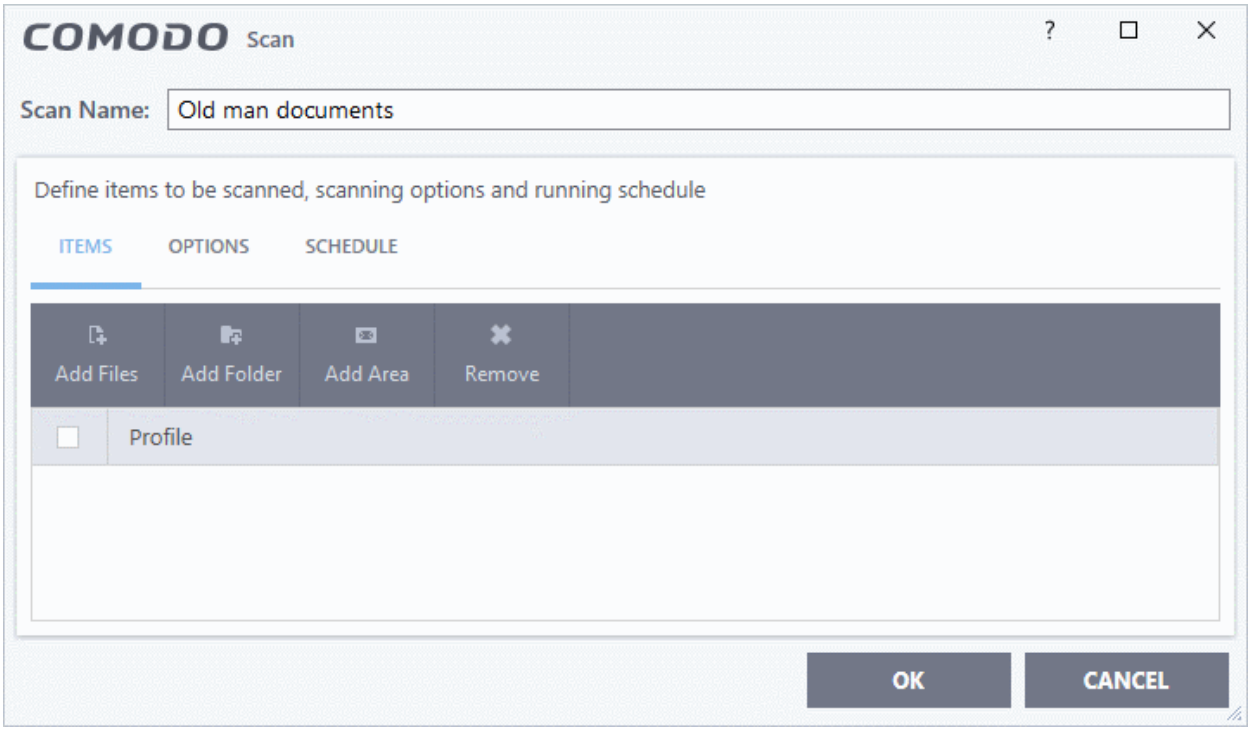
Click the following links for more details about:

- **Create a scan profile**
- **Run a custom scan**

Create a custom profile

- Click 'Settings' on the top of the CCS home screen
- Click 'Antivirus' > 'Scans'
- Click 'Add' from the options at the top.

The profile configuration screen opens:



- Type a name for the profile.

The next steps are to:

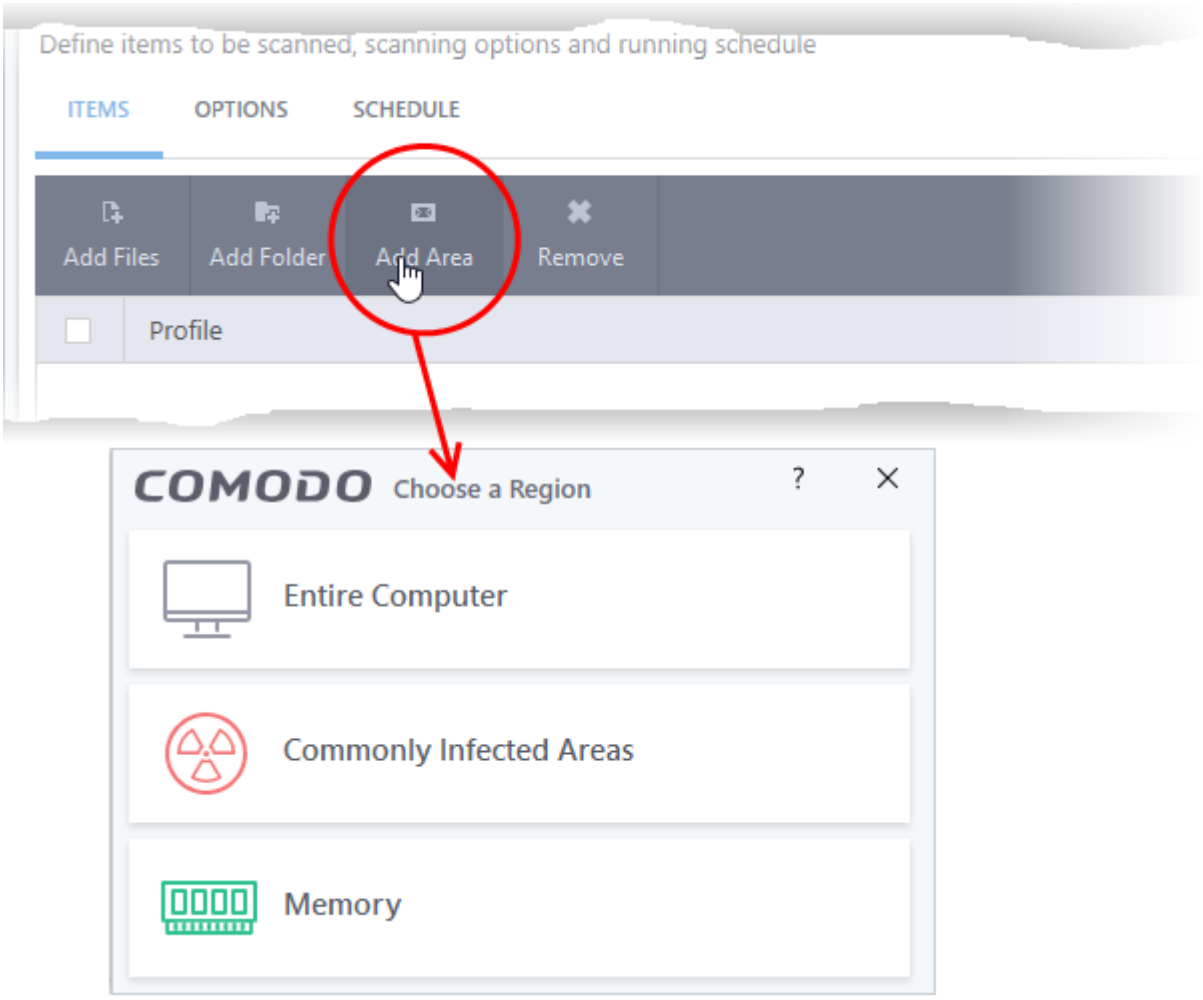
- **Select the items to scan**
- **Configure scan options for the profile**
- **Configure a schedule for the scan**

Select the items to scan

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

The buttons along the top let you add three types of item to the scan. You can add any combination of items.

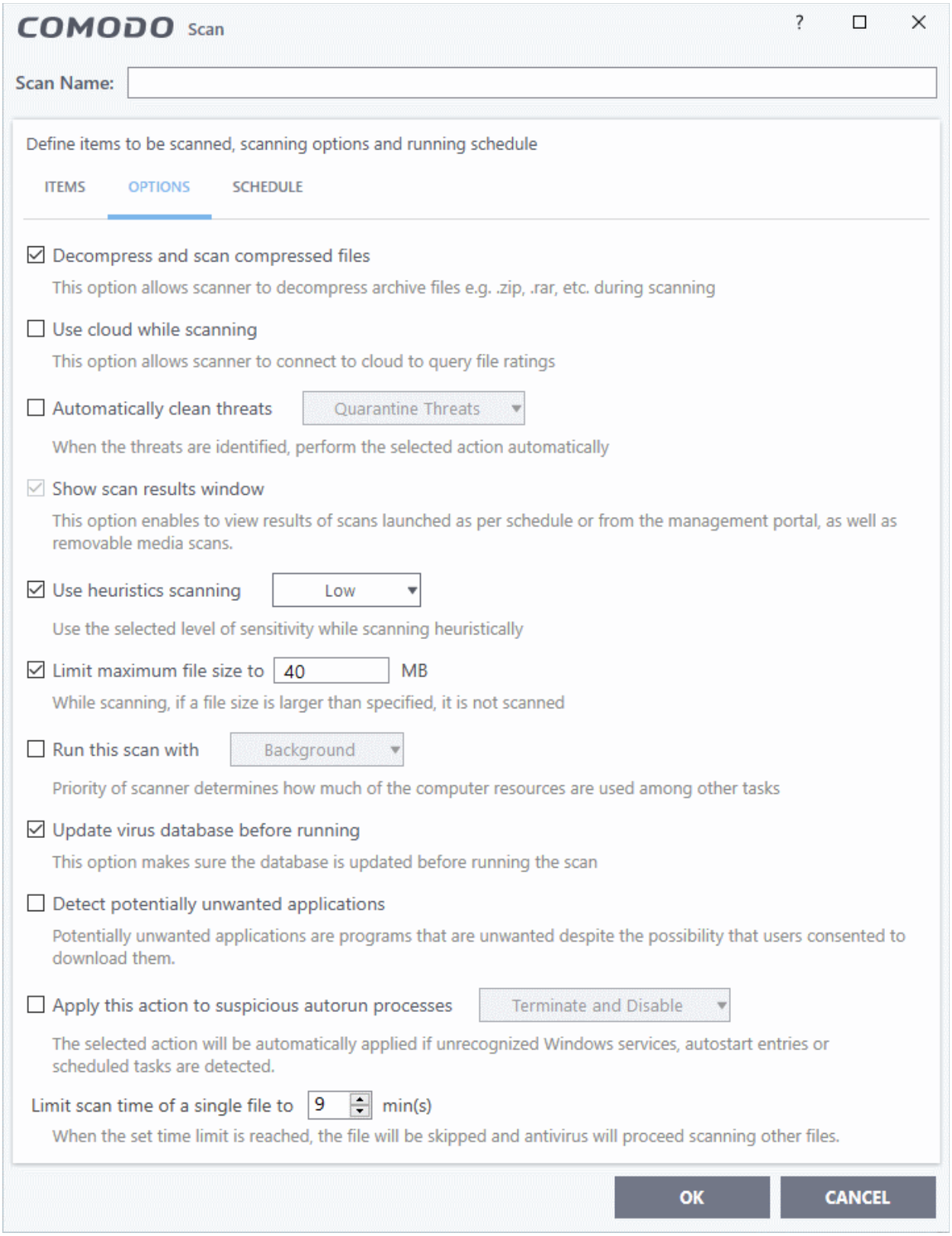
- **Add Files** - Scan individual files. Click the 'Add Files' button and navigate to the file you want to scan. Repeat to add more files.
- **Add Folder** - Scan entire folders. The scan covers all files inside the target folders. Click the 'Add Folder' button and choose the folder you want to scan.
- **Add Area** - Scan pre-defined regions. Regions include 'Full Computer', 'Commonly Infected Areas' and 'Memory'.



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

Configure Scan Options

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



- **Decompress and scan compressed files** - The scan will include archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
- **Use cloud while scanning** - Improves scan accuracy by augmenting the local scan with an online look-up of Comodo's latest signature database. Cloud Scanning means CCS can detect the latest malware even if your virus database is out-dated. ***(Default = Disabled)***.
- **Automatically clean threats** - Whether or not CCS should automatically remove any malware found by the scan.

- **Disabled** = Results are shown at the end of the scan with a list of any identified threats. You can select the action to be taken on them individually, or on all items at-once. See **Process Infected Files** for guidance on manually handling detected threats.
- **Enabled** = You can choose the automatic action taken against detected threats. The options are:
  - **Quarantine Threats** - Infected items will be moved to Quarantine. You can review quarantined items later and remove them or restore them (in case of false positives). See **Manage Quarantined Items** for more details on managing quarantined items.
  - **Disinfect Threats** - If a disinfection routine is available, the antivirus will remove the infection and keep the original, safe, file. If not, the item is moved to 'Quarantine'. (***Default***)

- **Show scan result window** - If selected, you will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.
- **Use heuristics scanning** - Enable or disable heuristic scans, and define the sensitivity of the scanner. (Default = Enabled)

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

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

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

    Despite the name, this setting combines a very high level of protection with a low rate of false positives. We recommend this setting for most users. (Default)
  - **Medium** - Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
  - **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.
- **Limit maximum file size to** - Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here. (***Default = 40 MB***)
- **Run this scan with** - Whether you want to set a priority for the scans with this profile
  - **Enabled** = You can set the priority. The available options are:
    - High
    - Normal
    - Low
    - Background.
  - **Disabled** = The scan will be run at the background (***Default***)
- **Update virus database before running** - CCS checks for and downloads the latest virus signatures before starting every scan with this profile (***Default = Enabled***) .
- **Detect potentially unwanted applications** - The antivirus also scans for applications that (i) a user may or may not be aware is installed on their computer, or (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional utility when installing another piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar that tells you the weather forecast might also track your online activity. ***(Default = Enabled).***
- **Apply this action to suspicious autorun processes** - Specify how CCS should handle unrecognized auto-run items, Windows services and scheduled tasks.
  - **Ignore** - The item is allowed to run (Default)

- **Terminate** - CCS stops the process / service
- **Terminate and Disable** - Auto-run processes will be stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- **Quarantine and Disable** - Auto-run processes will be quarantined and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.

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

- See **Miscellaneous Settings** for more details

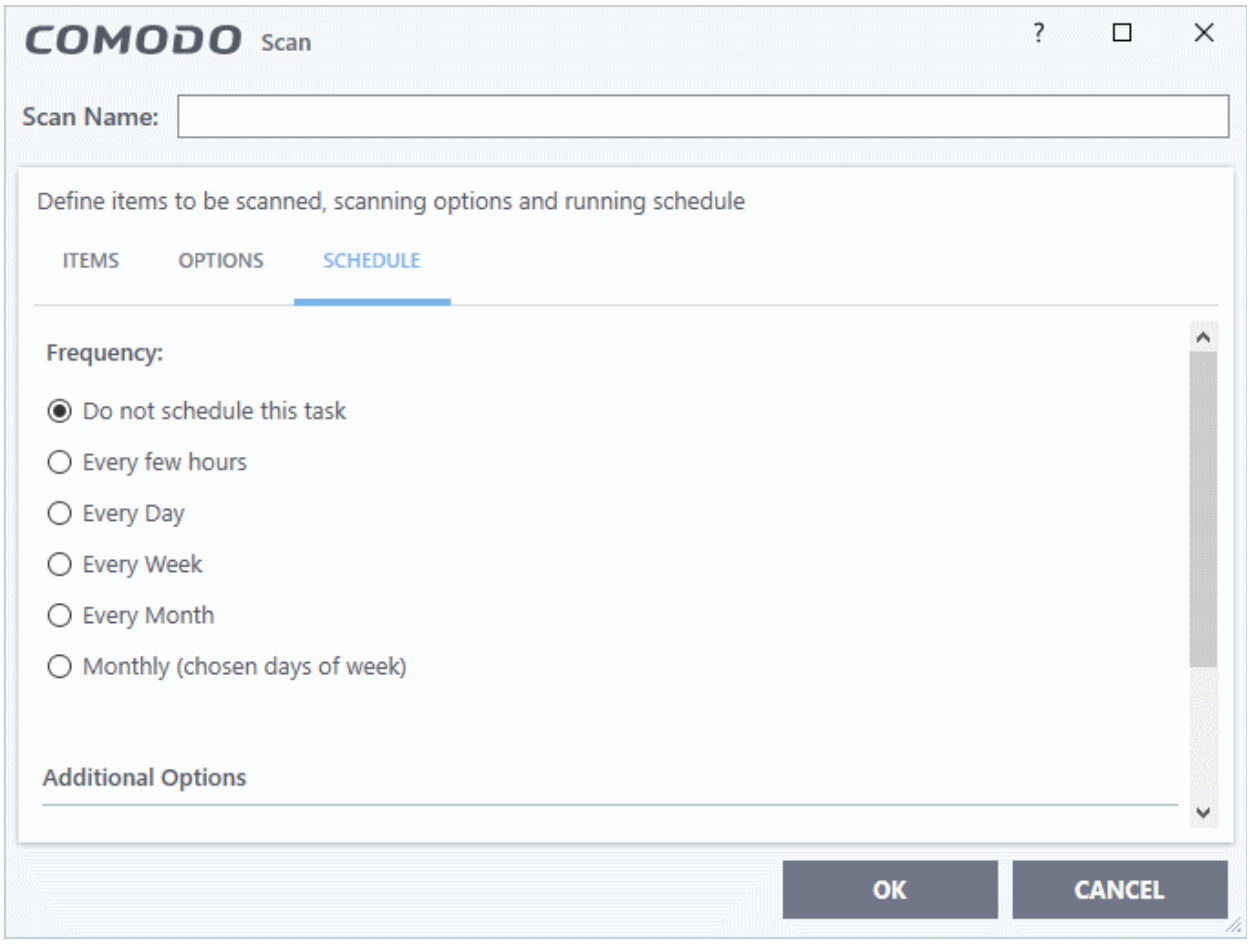
Note 2 - CCS ships with a list of applications for which script analysis will be performed to protect the registry records. You can manage the list of applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

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

- **Limit scan time of a single file to** - Set the maximum time allowed to scan an individual file. CCS will skip files that take longer to scan than the specified time. Omitted files are shown in the 'Skipped Files' tab in the results screen.

Schedule the scan

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



You have the following options:

- **Do not schedule this task** - The scan profile will be created but will not run automatically. The profile will be available for on-demand scans.
- **Every few hours** - Run the scan at the intervals of the hours specified in 'Repeat scan every NN hour(s)'

- **Every Day** - Run the scan every day at the time specified in the 'Start Time' field.
- **Every Week** - Run the scan on the day(s) specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.
- **Every Month** - Run the scan on the date(s) specified in 'Days of the month', at the time specified in the 'Start Time' field. You can select the dates of the month by clicking on them.
- **Monthly (chosen days of the week)** - Run the scan on specific weeks in a month. Select the target weeks in the menus provided.

Additional Options

- **Run only when computer is not running on battery** - The scan only runs when the computer is plugged into the power supply. This option is useful when you are using a laptop or other mobile device.
- **Run only when computer is IDLE** - The scan will run only if the computer is in idle state at the scheduled time. Select this option if you do not want the scan to disturb you while you are using your computer.
- **Turn off computer if no threats are found at the end of the scan** - Will turn off your computer if no threats are found during the scan. This is useful when you are scheduling scans to run at nights.
- **Run during Windows Automatic Maintenance** - Only available for Windows 8 and later. Select this option if you want the scan to run when Windows enters into automatic maintenance mode. The scan will run at maintenance time *in addition* to the configured schedule.

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

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

- Click 'OK' to save the profile.

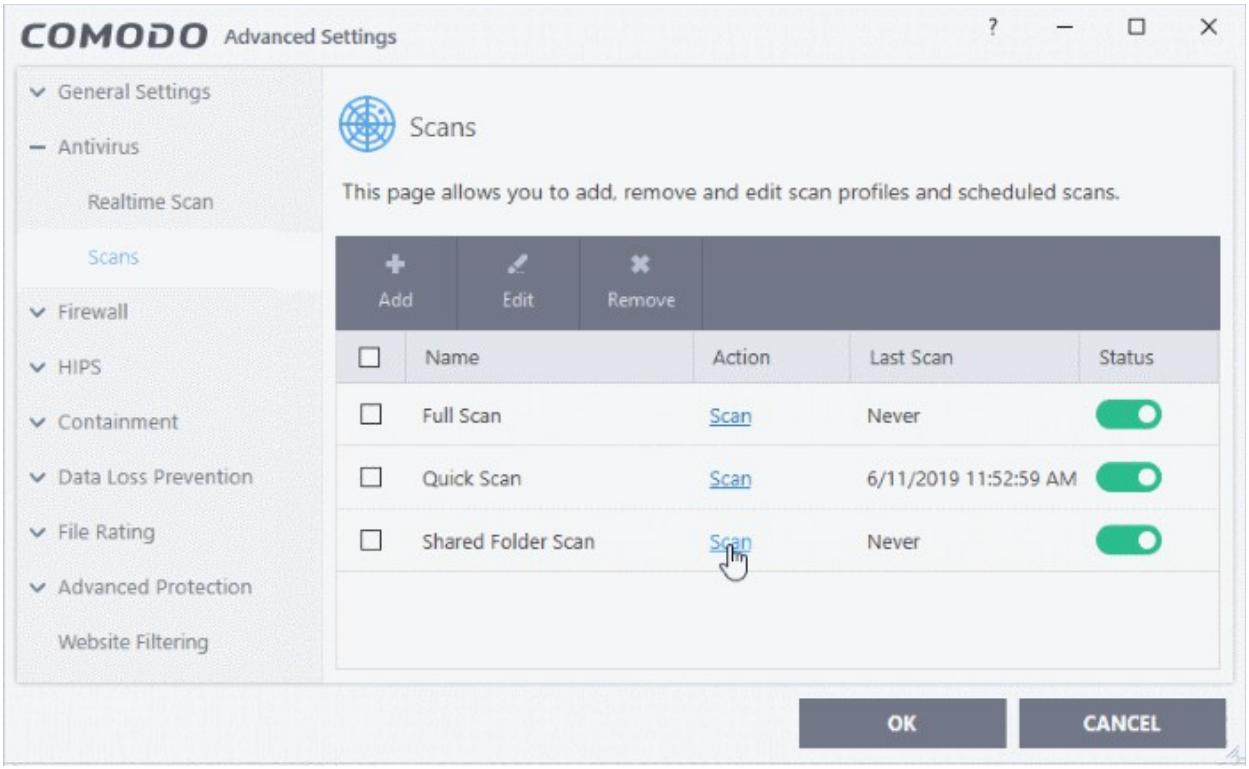
The profile will be available for deployment in future.

Run a custom scan as per a scan profile

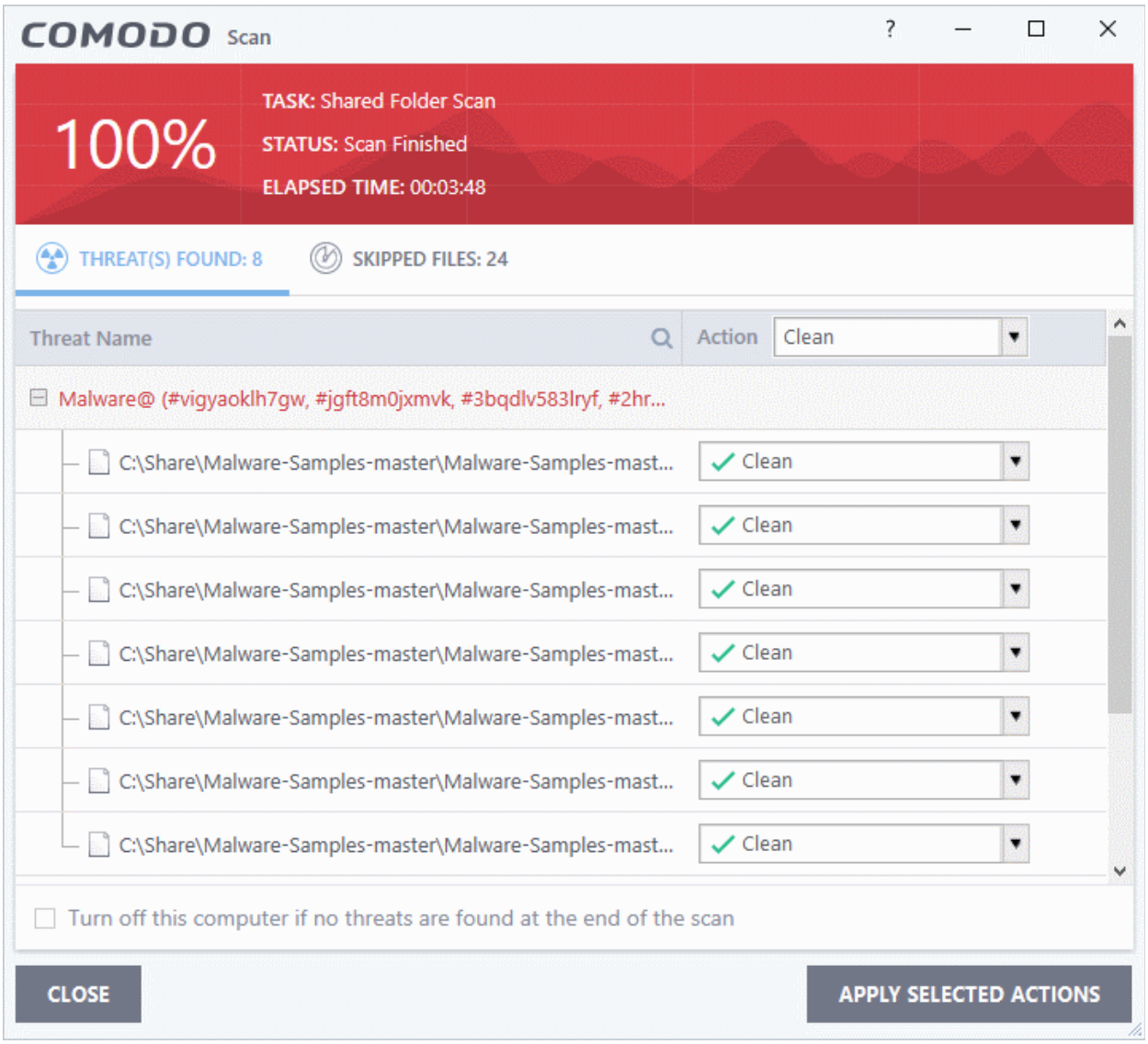
- Click 'General Tasks' on the CCS home screen
- Click 'Scan' > 'Custom Scan'
- Click 'More Scan Options'

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

- Click 'Scan' beside the required scan profile.



The scan will start immediately. Results are displayed afterwards:

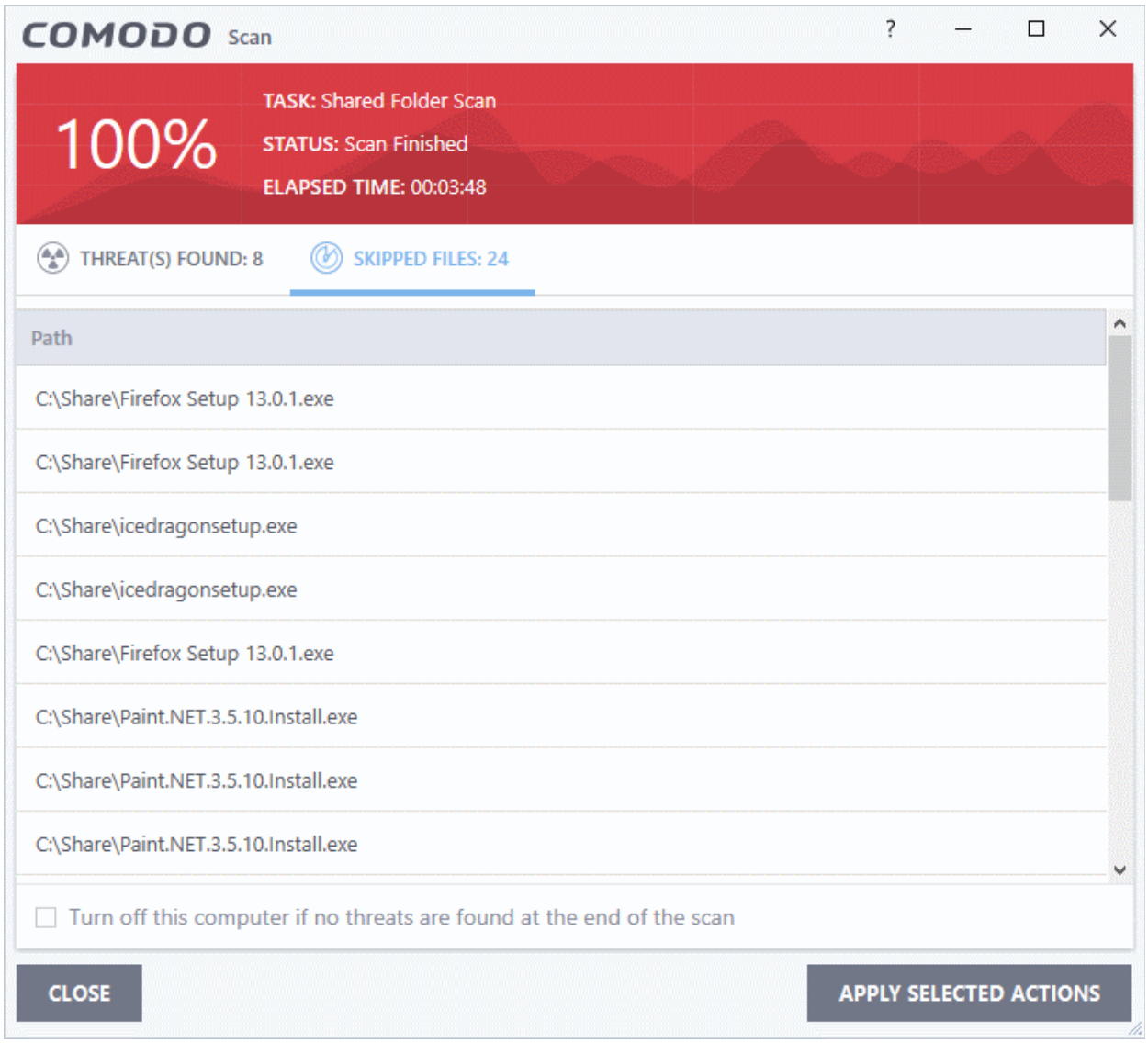


The results window has two tabs:

- **Threats Found**: The number of files scanned and the number of viruses found.
  - Use the drop-down to choose whether to clean, quarantine or ignore the threat.
  - See '**Process infected files**' if you need help with these options.

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

- **Skipped Files**: Files that were not checked for viruses. The scanner skipped these files as they took longer than the scan time limit (default = 9 mins).

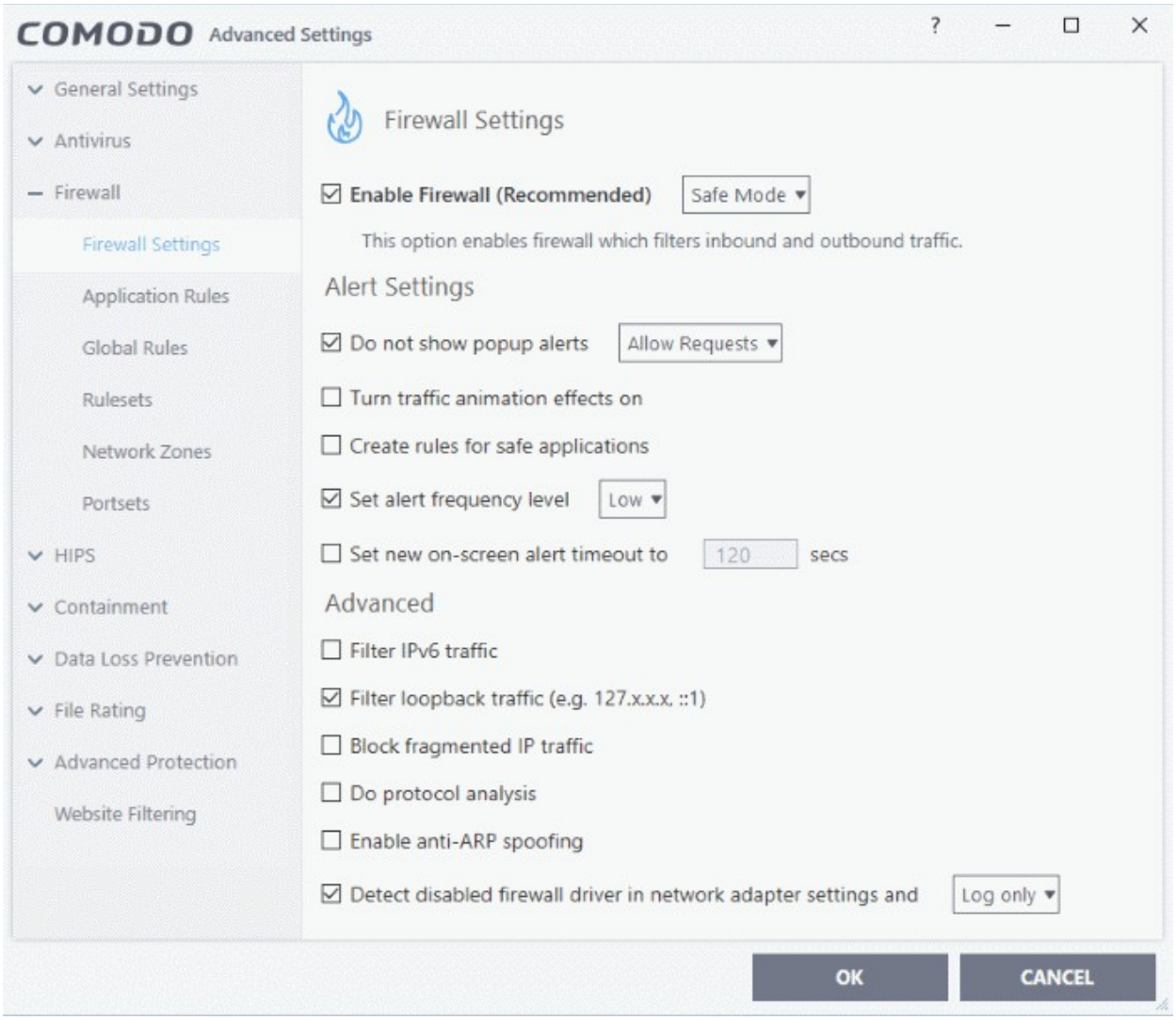


7.3. Firewall Configuration

- Click 'Settings' > 'Firewall'
- The firewall protects your computer against inbound and outbound threats.
- It checks that all network traffic in and out of your computer is legitimate, hides your computer ports against hackers, and blocks software from transmitting your personal data over the internet.
- The simple rules interface lets you specify exactly which applications can access the internet.
- You can choose to receive alerts if the firewall detects suspicious activity, or have the firewall auto-implement a specific action.

Configure the 'Firewall' module

- Click 'Settings' on the CCS home screen
- Click 'Firewall' on the left:



Firewall settings has the following sections:

- **General Firewall Settings** - Settings that govern the overall behavior of the firewall.
- **Application Rules** - Rules which control the network access rights of specific applications, or types of application.
- **Global Rules** - Rules which apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Collections of rules that can be applied to internet capable applications like browsers and email/FTP clients.
- **Network Zones** - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Predefined groups of regularly used ports that can be used and reused when creating traffic filtering rules.

Background note on rules:

Both application rules and global rules are consulted when the firewall decides whether to allow or block a connection:

Outgoing connections - Application rules are consulted first then global rules.

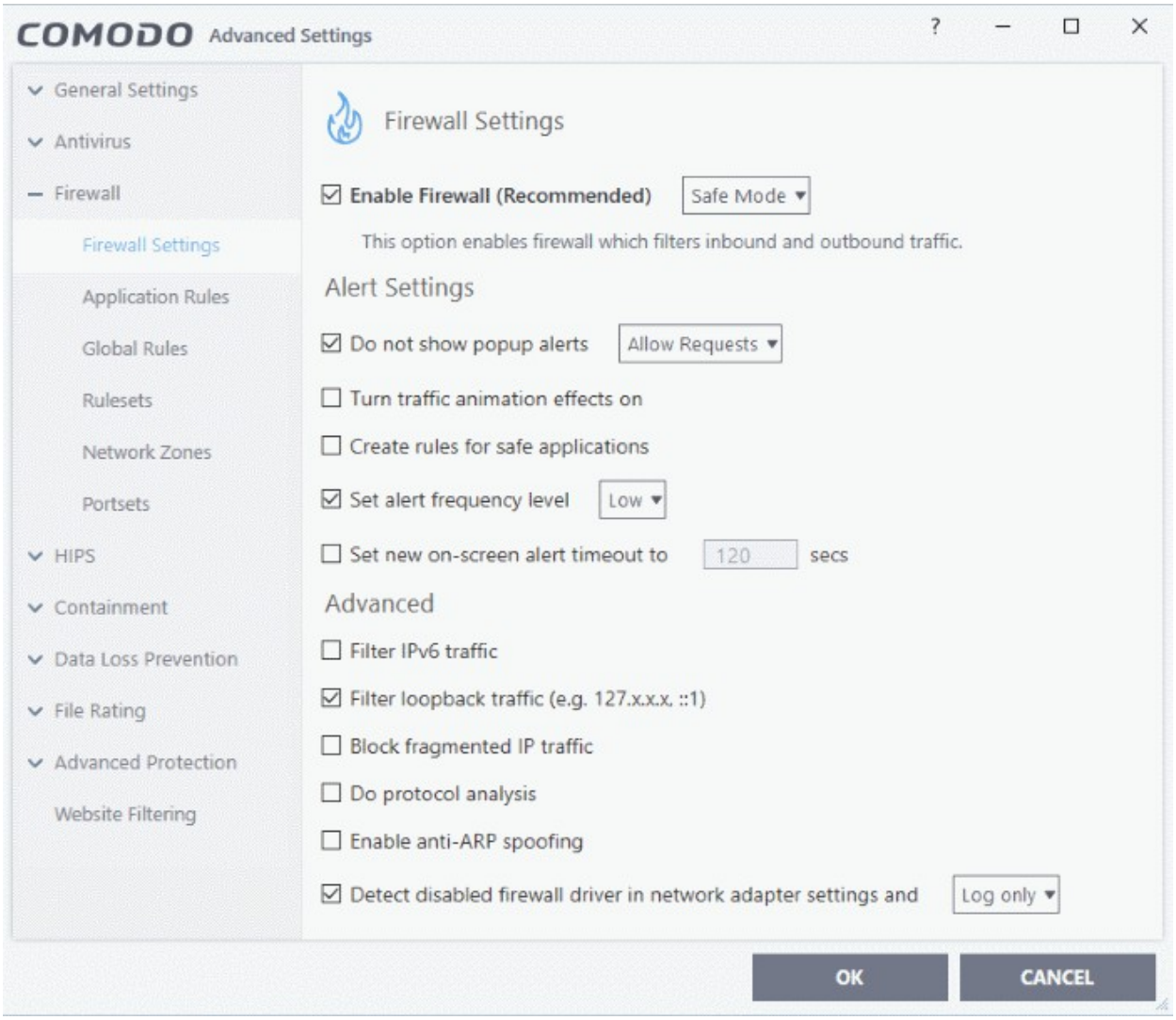
Incoming connections - Global rules are consulted first then application rules.

7.3.1. General Firewall Settings

- Click 'Settings' > 'Firewall' > 'Firewall Settings'
- Firewall settings let you quickly configure the overall behavior of the firewall. Settings are divided into three main areas:
  - **General Settings**
  - **Alert Settings**
  - **Advanced Settings**

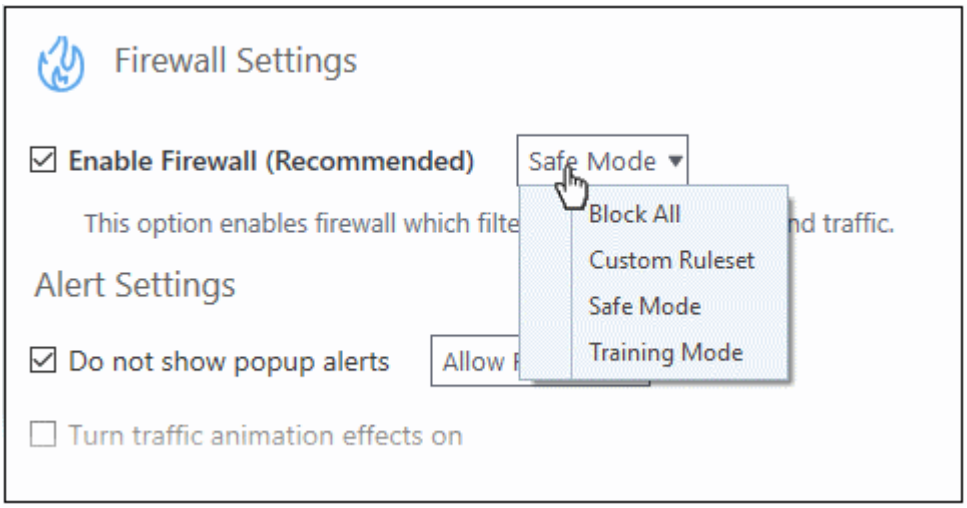
Configure the firewall settings

- Click 'Settings' at the top of the CCS home screen
- Click 'Firewall' > 'Firewall Settings'



General Settings

- **Enable Firewall** - Activate or deactivate firewall protection. (***Default and recommended = Enabled***)
  - If enabled, you can also choose the security level from the drop-down menu:



The choices available are:

- **Block All**: The firewall stops all traffic in and out of your computer, regardless of any other settings or rules. The firewall does not attempt to learn the behavior of any application, and does not create traffic rules for any applications. This option prevents your computer from accessing any networks, including the internet.
- **Custom Ruleset Mode**: The firewall applies ONLY **network traffic rules** that you have created. 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 Safe list (unless, of course, you have specified rules and policies that instruct the firewall to trust the application's connection attempt).

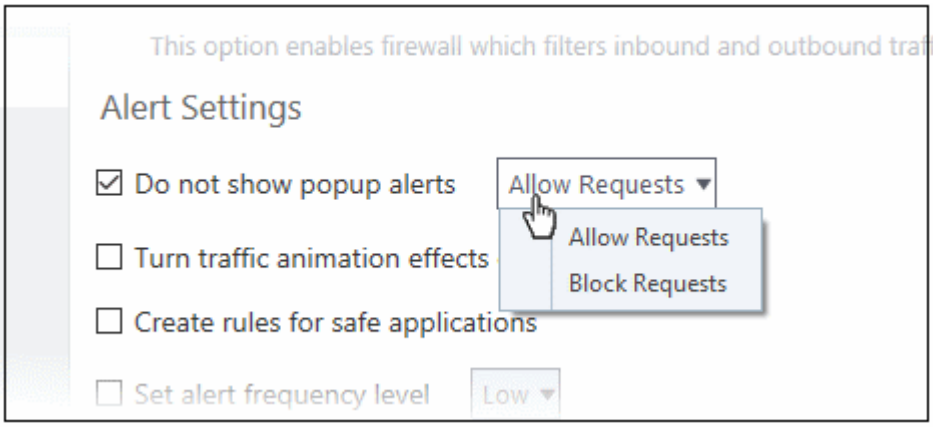
  If any application tries to make a outbound connection, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.
- **Safe Mode *(Default)***: If **Create rules for safe applications** is enabled then the firewall automatically creates rules to allow traffic by applications certified as 'Safe' by Comodo. For new, unknown applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application internet access by choosing 'Treat this application as a Trusted Application' at the alert. This deploys the **predefined firewall ruleset** 'Trusted Application' onto the application.

  'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.
- **Training Mode**: The firewall monitors network traffic and creates automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the **correct network access rights**.

Alert Settings

- **Do not show popup alerts** - Whether or not you want to be notified when the firewall encounters a request for network access. Choosing 'Do not show pop-up alerts' will minimize disturbances but at some loss of user awareness. (***Default = Enabled***)

  If you choose this option then you have a choice of default responses that CCS should take - either 'Block Requests' or 'Allow Requests'.



- **Turn traffic animation effects on** - By default, the Comodo Client Security's 'Shield' tray icon displays a small animation whenever traffic moves to or from your computer.

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

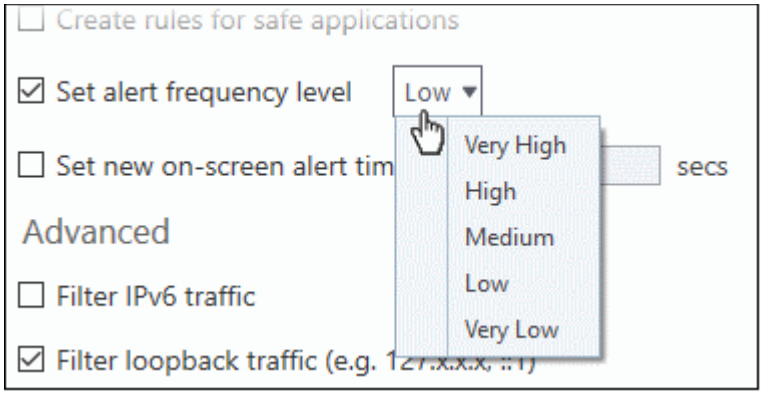
  - Clear this check box If you would rather not see this animation. ***(Default = Disabled)***

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

  By default, CCS does not automatically create 'allow' rules for safe applications. This helps to lower resource usage and simplifies the rules interface. It also reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

  Enabling this checkbox instructs CCS to begin learning the behavior of safe applications so that it can automatically generate 'Allow' rules. These rules are listed in the **Application Rules** interface. The Advanced users can edit/modify the rules as they wish. ***(Default = Disabled)***

- **Set alert frequency level** - Configure the amount of alerts that the firewall generates. Please note that this does not affect your security level, which is determined by the actual rules you have in place (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of suspicious behavior while not getting overwhelmed with alerts. (***Default =Disabled***)



The options available are:

- **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.
- **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.
- **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.
- **Low:** The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.
- **Very Low**: The firewall shows only one alert for an application.

The alert frequency settings refer only to connection attempts by applications or from IP addresses that you do not trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.

- **Set new on-screen alert time out to**: How long a firewall alert remains on-screen if it is not answered. The default timeout is 120 seconds. You may adjust this setting to your own preference.

Advanced Settings

Advanced detection settings help protect your computer against common types of denial of service (DoS) attack. When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server.

- **Filter IP v6 traffic** - If enabled, the firewall will filter IPv6 network traffic in addition to IPv4 traffic.(***Default = Disabled***)

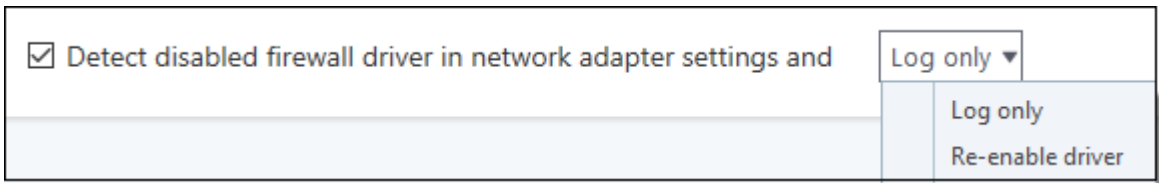
Background Note: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost 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 by its domain name of '**http://localhost**'. This is the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this option enabled means the firewall will filter traffic sent through this channel. (***Default = Enabled***)
- **Block fragmented traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using. When a datagram is larger than the MTU of the network

over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, fragmentation can double the amount of time it takes to send a single packet and slow down your download time. (***Default = Disabled***)

- **Do Protocol Analysis** - Protocol Analysis is key to the detection of fake packets used in denial of service attacks. Enabling this option means Comodo Firewall checks that every packet conforms to that protocols standards. If not, then the packets are blocked. (***Default = Disabled***)
- **Enable anti-ARP spoofing** - A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update your machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in a machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update your ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in your home network. Enabling this setting helps to block such requests - protecting the ARP cache from potentially malicious updates. (***Default = Disabled***)
- **Detect disabled firewall driver in network adapter settings** - The firewall will take action if it discovers its driver is not enabled.

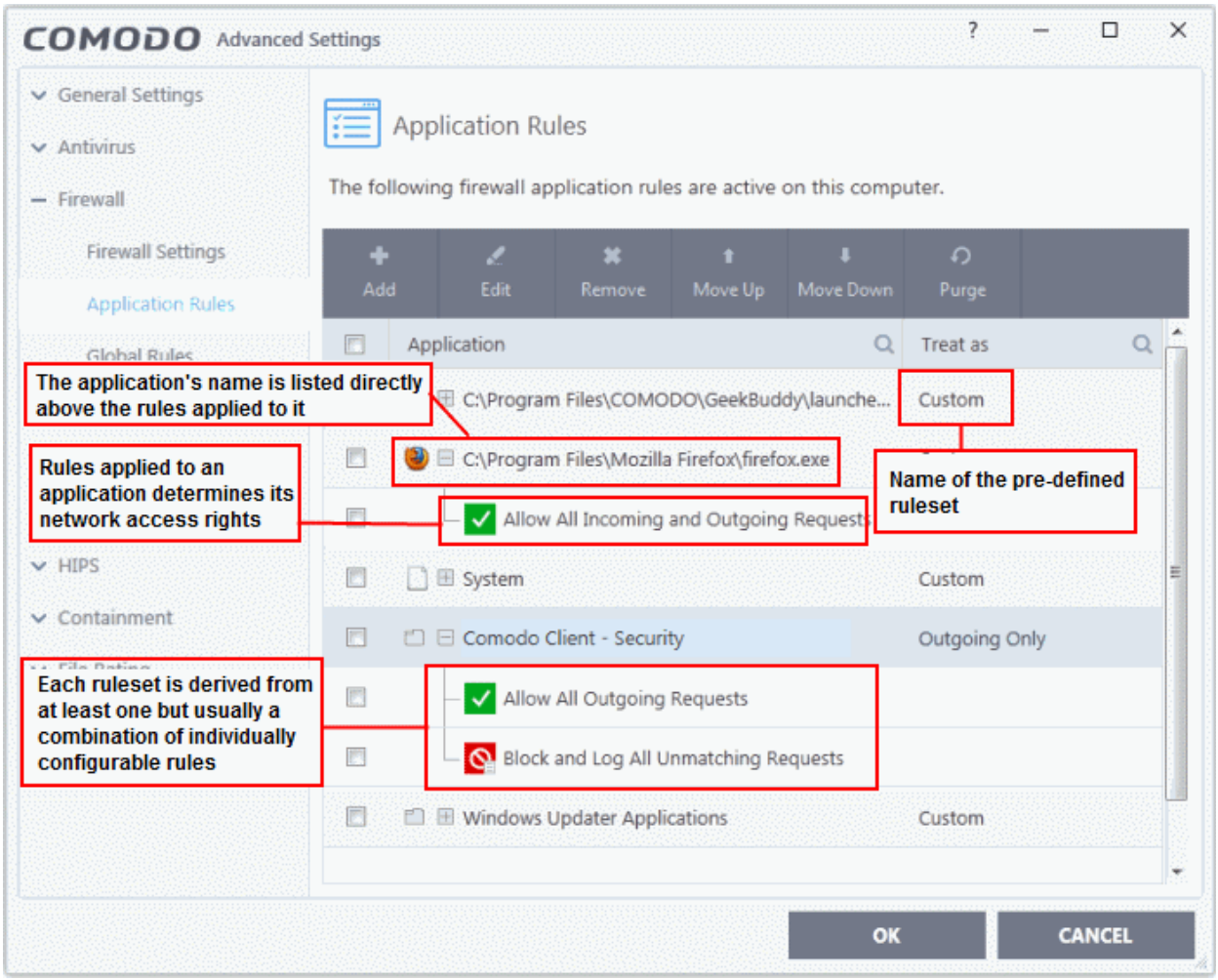


You can choose the following actions if this condition is met:

- **Log only** - Creates an event log but does not notify the administrator.
- **Re-enable Driver** - Attempts to turns the driver back on automatically.

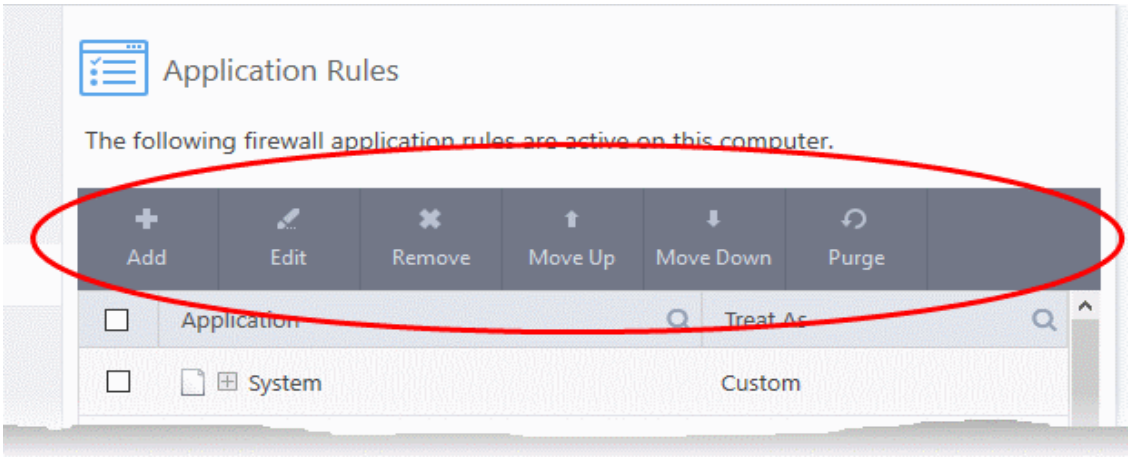
7.3.2. Application Rules

- Click 'Settings' > 'Firewall' > 'Application Rules'
- Application rules let you manage network access rights for specific applications.
- Whenever an application makes a request for network access, CCS allows or denies the request based on the ruleset applied to the application.
- Firewall rulesets are made up of one or more application rules. Each rule outlines an application's permissions regarding a specific type of traffic.



- **Application** - Programs or file groups for which a firewall ruleset has been created. In the case of file groups, all member applications will use the ruleset of the group.
    - Click '+' next to the name to view the rules which apply to the application/group.
- **Treat as** - Name of the ruleset assigned to the application or group.

The controls above the table let you manage the rule sets:



- **Add** - Add a new application/application group then create a ruleset for it.
- **Edit** - Modify an application rule/ruleset.
- **Remove** - Delete a selected rule.

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

Predefined rulesets

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

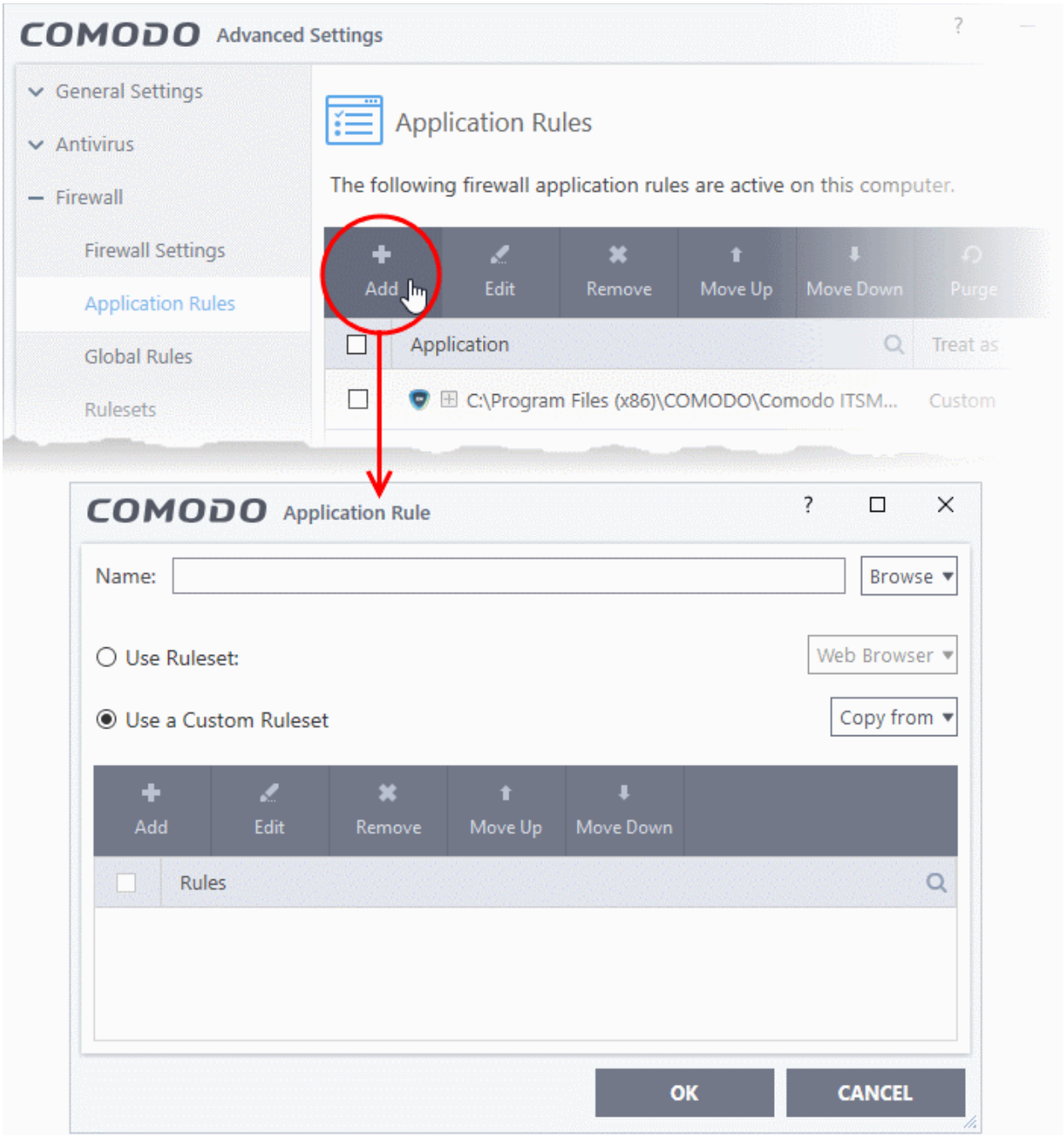
Create a firewall ruleset

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

Step 1 - Select the target application or group

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

The 'Application Rule' interface appears:



- Click the 'Browse' button beside the 'Name' field:

There are three types of target you can add:

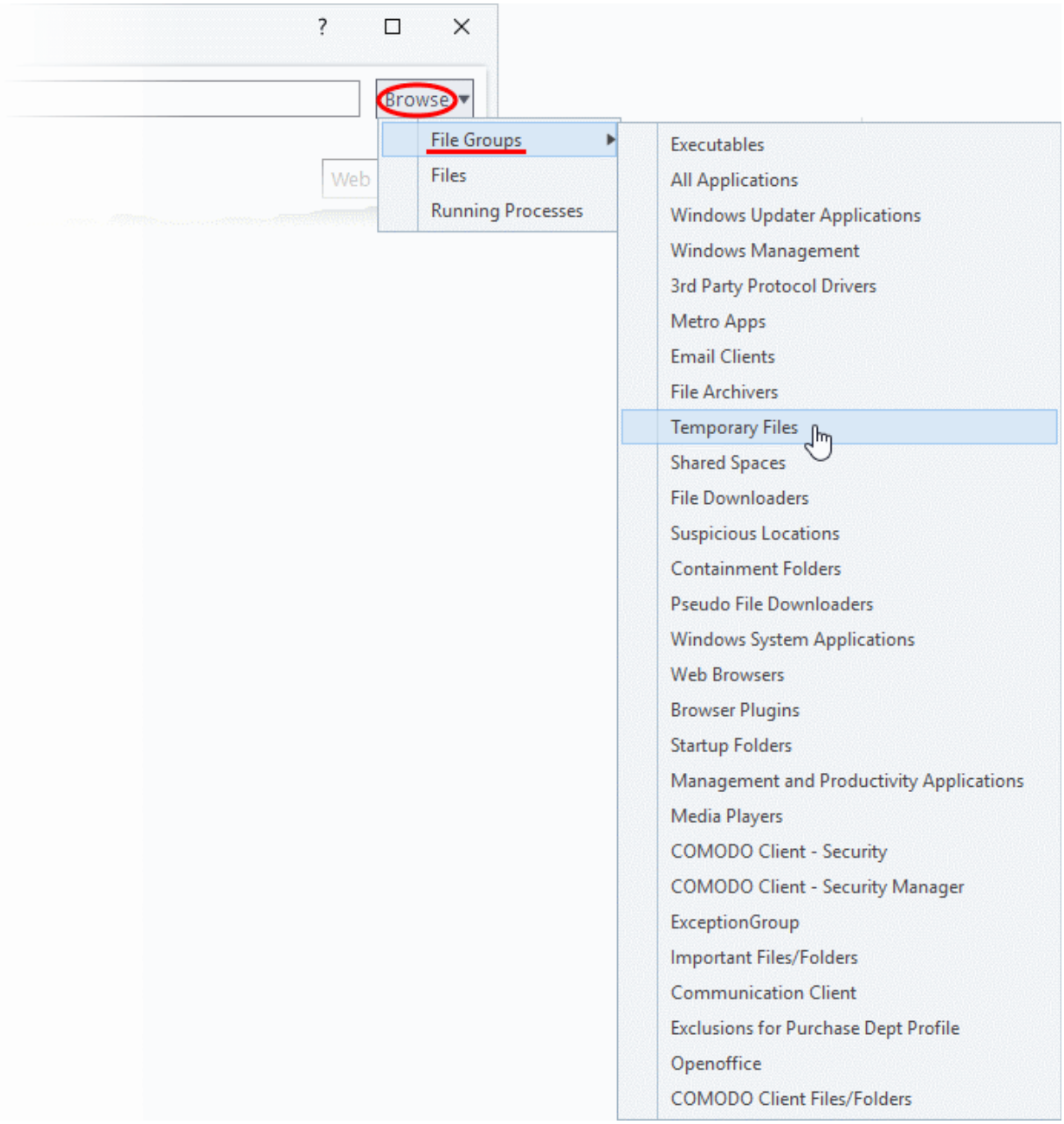
- **File Groups** - Apply the ruleset to a predefined file group. All members of the group are covered by the rule. See **File Groups** if you need help with file groups.
- **Files** - Apply the ruleset to a specific application.

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

Add a File Group

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

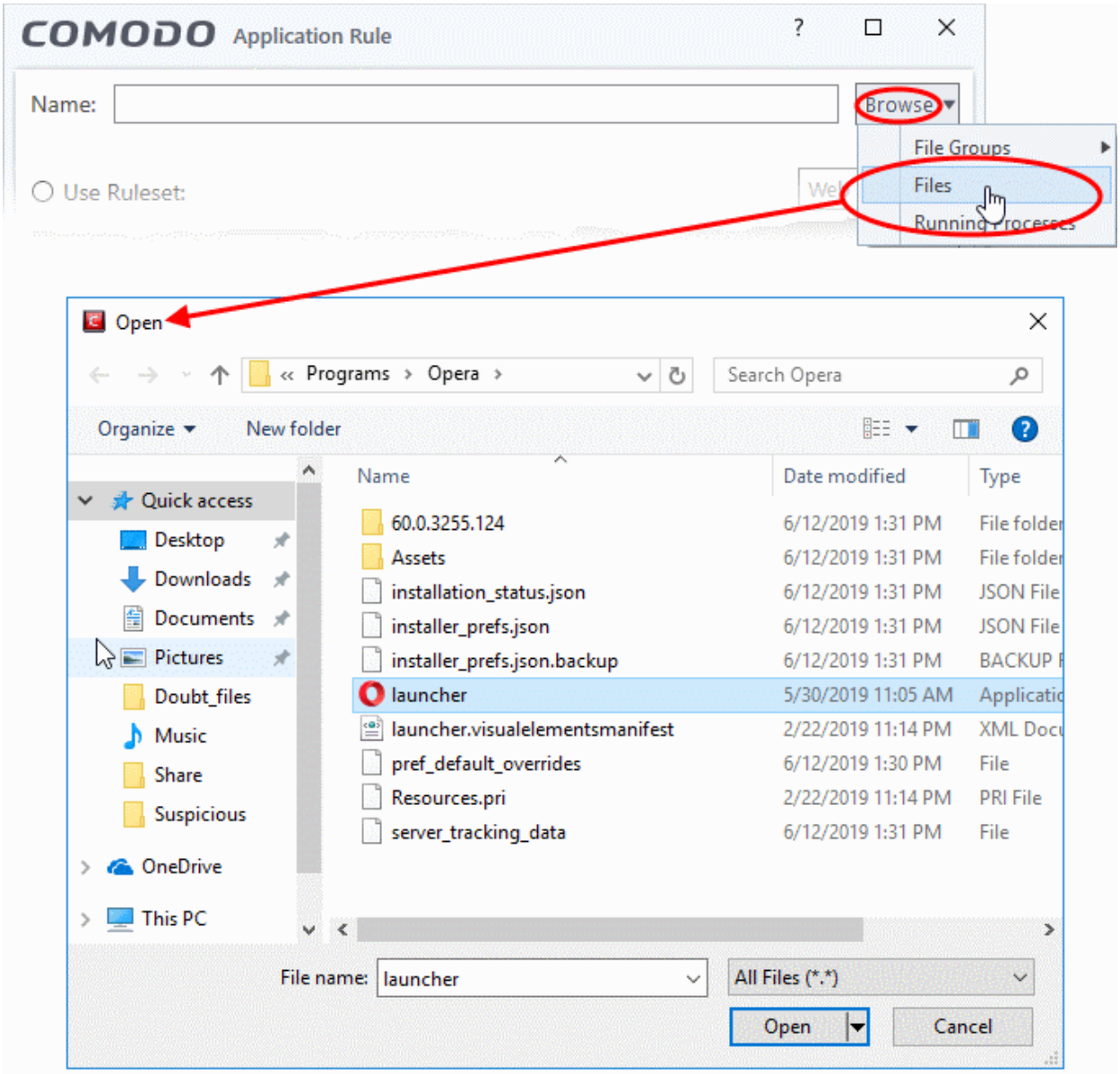
- Choose 'File Groups' from the 'Browse' drop-down.



- Select a file group from the drop-down. The ruleset will apply to all executable files in the group.
  - The next stage is **Step 2 - Configure the rules** for the selected file group.

Add an individual File

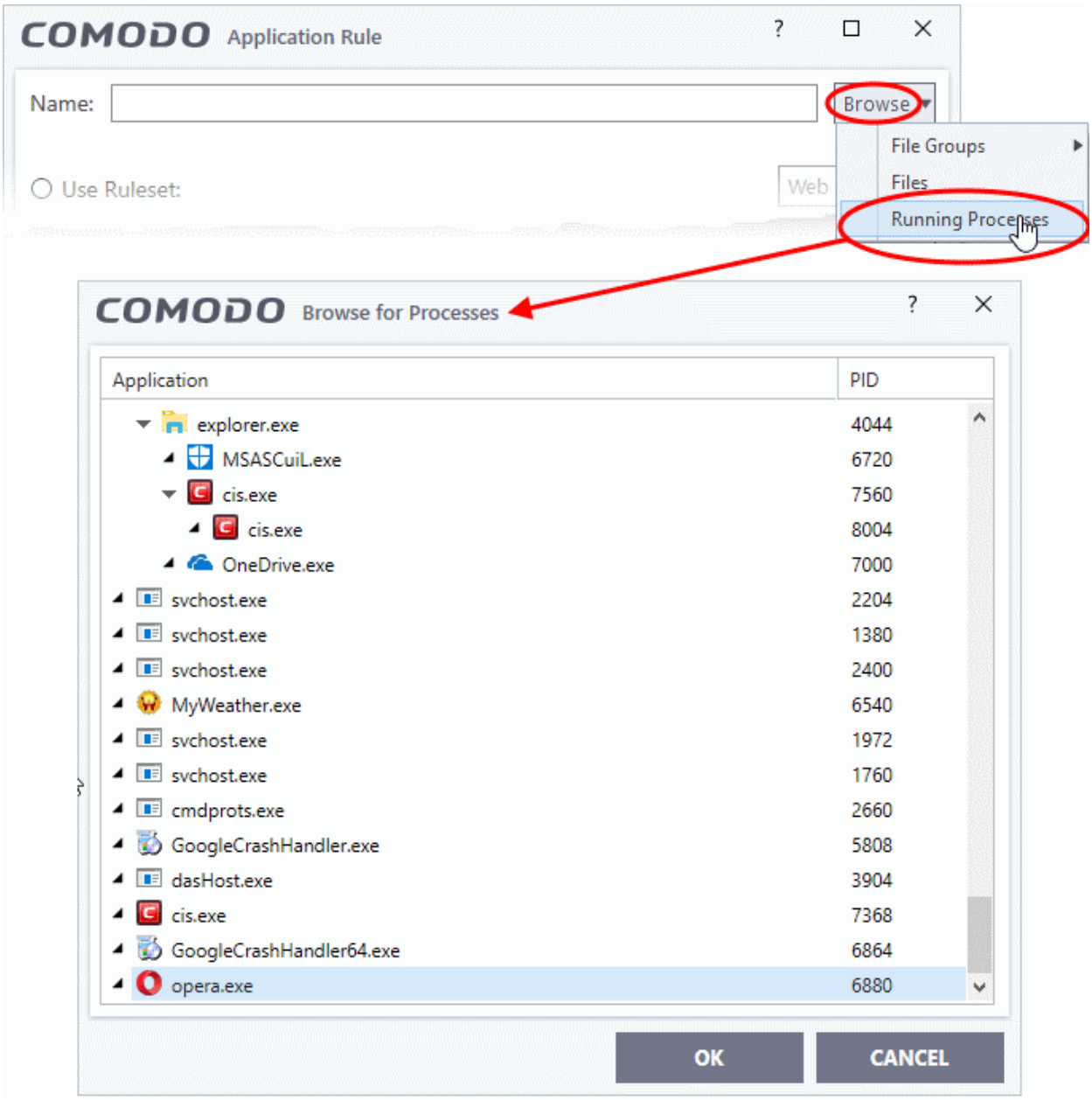
- Choose 'Files' from the 'Browse' drop-down:



- Navigate to the file you want to add as target and click 'Open'. The rule will apply only to the specific application.
    - The next stage is **Step 2 - Configure the rules** for the selected application.

Add a currently running application by choosing its process

- Choose 'Running Processes' from the 'Browse' drop-down.



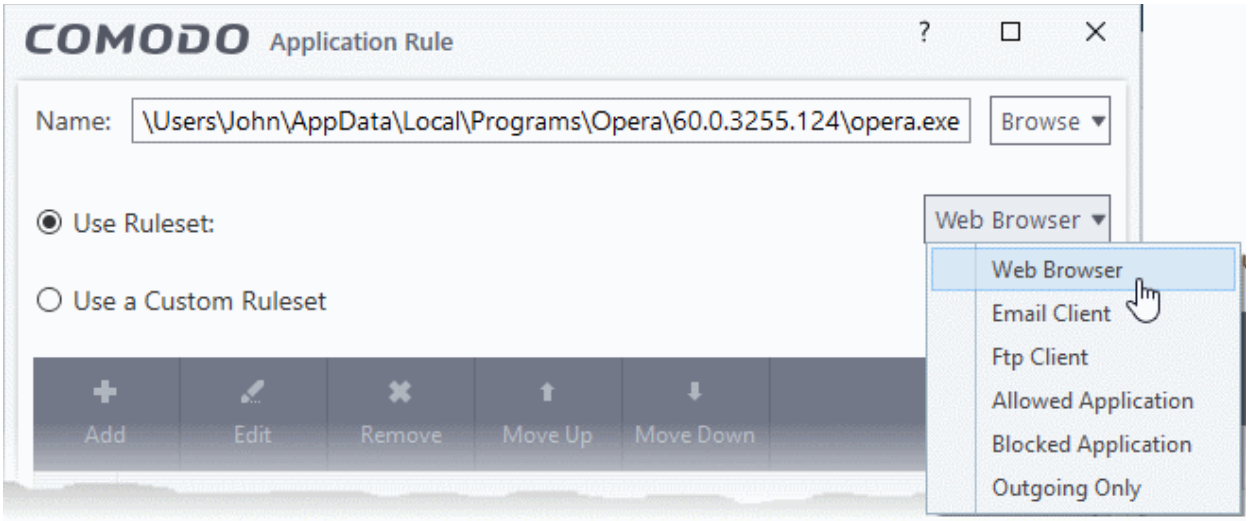
- Select the target process and click 'OK'. The parent application of the process will be added as the target.
    - The next stage is to configure the rules for the selected application.

Step 2 - Configure the rules in ruleset

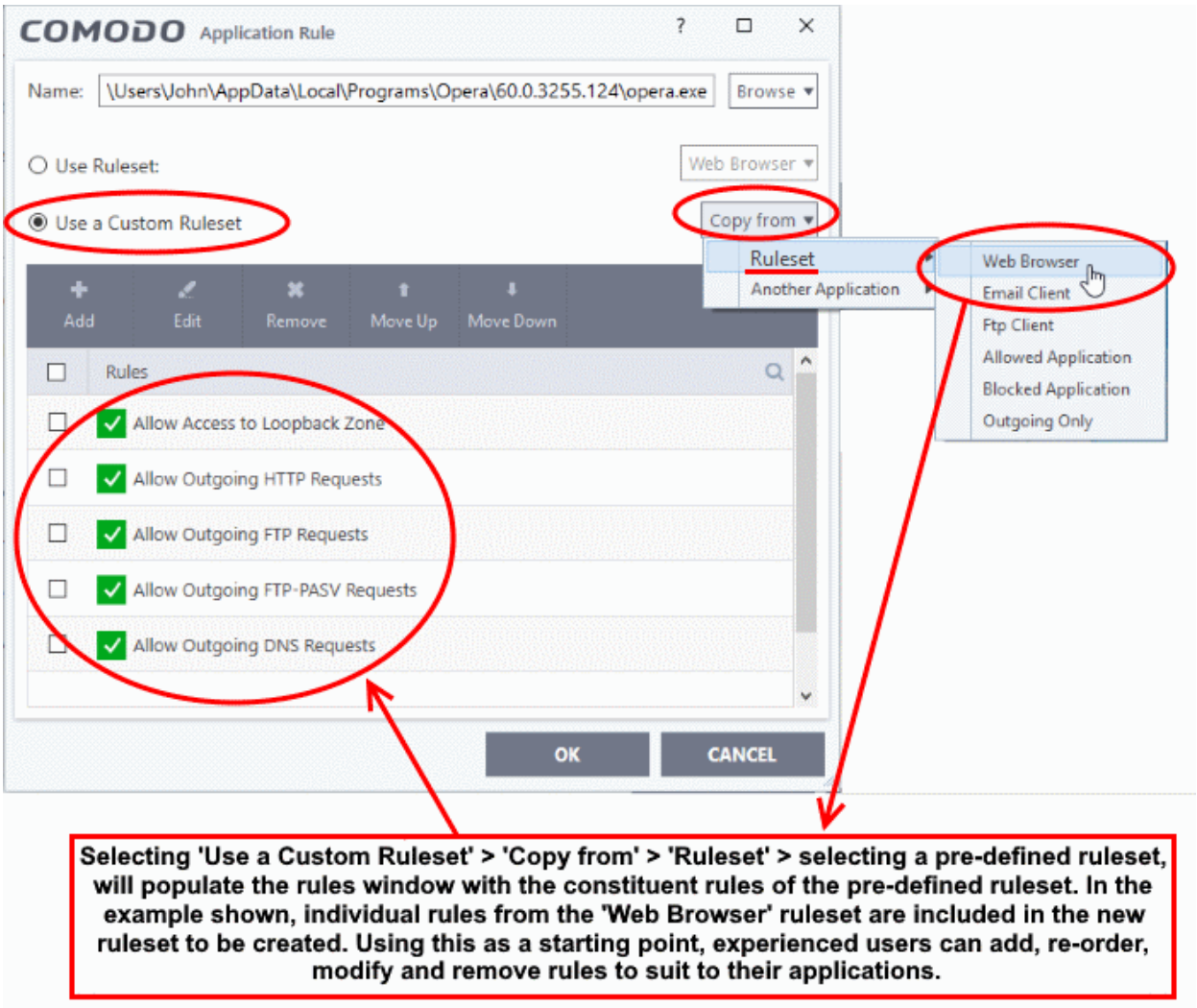
There are two broad options for creating a ruleset - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

Use Ruleset

- A ruleset is a collection of rules designed to implement optimum security on a specific type of application. You can manage and create rulesets in 'Settings' > 'Firewall Configuration' > 'Firewall Rule Sets'.
- Comodo provides a range of curated rulesets for popular types of application. These include 'Web browser', 'FTP client' and 'Email client'.
- The example below shows us applying the 'Web Browser' ruleset to the Opera browser:



- **Use a Custom Ruleset** - Designed for more experienced users, 'Custom Ruleset' lets you fully configure all rules in the ruleset. You can create an entirely new ruleset, or use a predefined set as a starting point.



Selecting 'Use a Custom Ruleset' > 'Copy from' > 'Ruleset' > selecting a pre-defined ruleset, will populate the rules window with the constituent rules of the pre-defined ruleset. In the example shown, individual rules from the 'Web Browser' ruleset are included in the new ruleset to be created. Using this as a starting point, experienced users can add, re-order, modify and remove rules to suit to their applications.

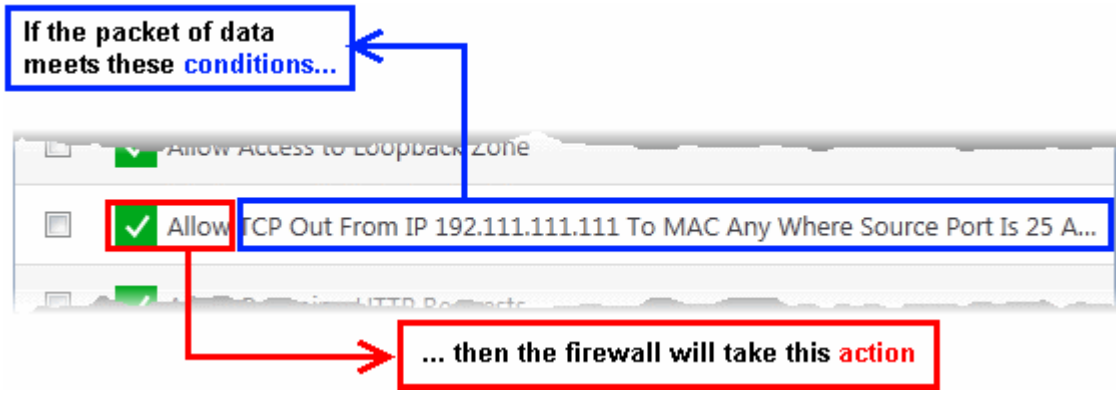
- Select the 'Use custom ruleset' radio button
- **Add** - Create individual rules for the set. See '**Add and Edit a Firewall Rule**' for an overview of the process.
- Copy From - Populate the list with the rules of a **Predefined Firewall Rule**. Edit/add/remove rules to

create your custom ruleset.

Understand Firewall Rules

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

As a packet filtering firewall, Comodo firewall analyzes the attributes of every packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding firewall rule, then the connection is automatically blocked until a rule is created.



The actual **conditions** (attributes)* you see on a particular firewall rule are determined by the protocol chosen while **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 **Add and Edit 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 **Add and Edit a Firewall Rule** to see the list of available IP protocols that can be displayed here.

Once a rule is applied, the firewall monitors all traffic relating to the application and takes 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'.

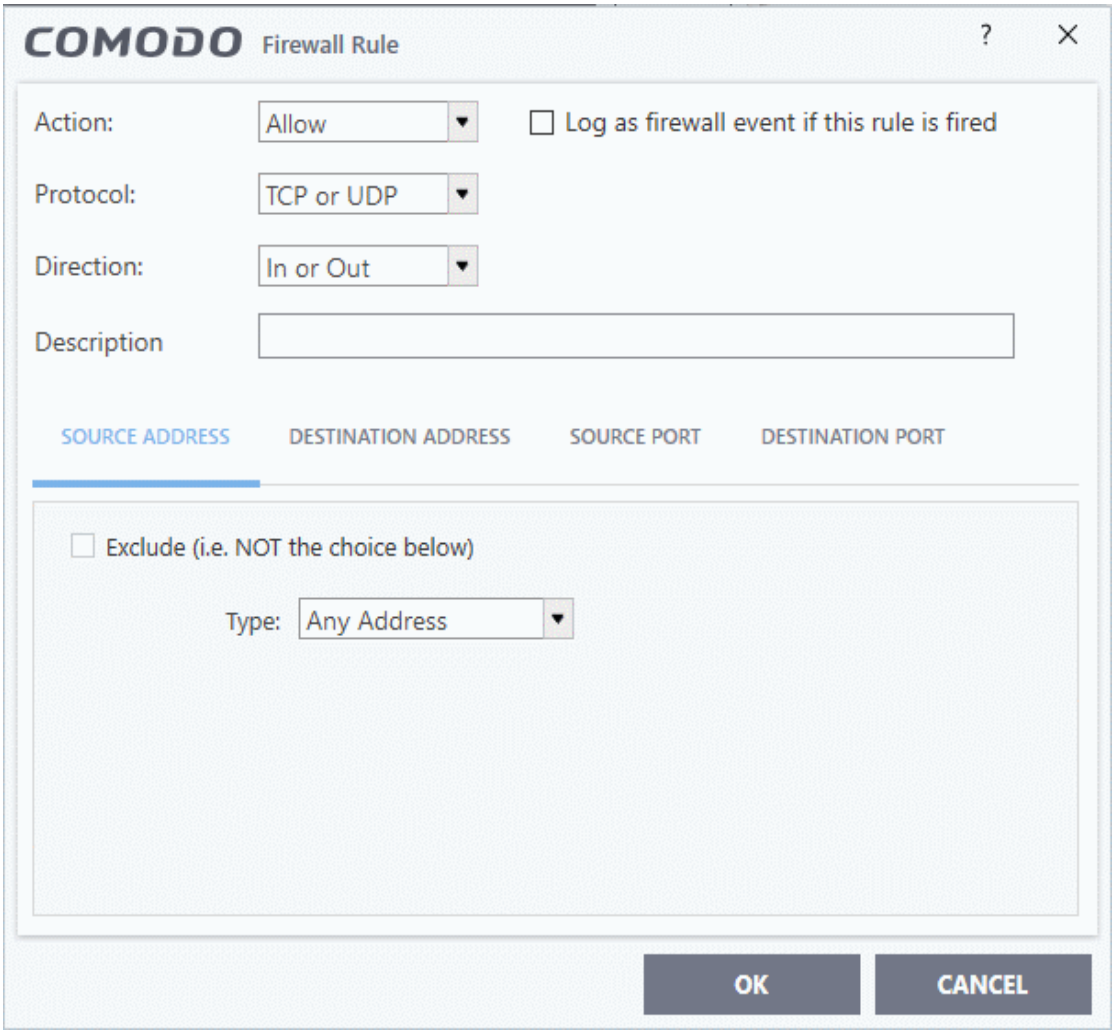
* *If you chose to add a descriptive name when creating the rule then this name is displayed here rather than it's full parameters. See the next section, '**Add and Edit a Firewall Rule**', for more details.*

** *If you selected 'Log as a firewall event if this rule is fired' then the action is postfixed with 'Log'. (e.g. Block & Log)*

Add and Edit a Firewall Rule

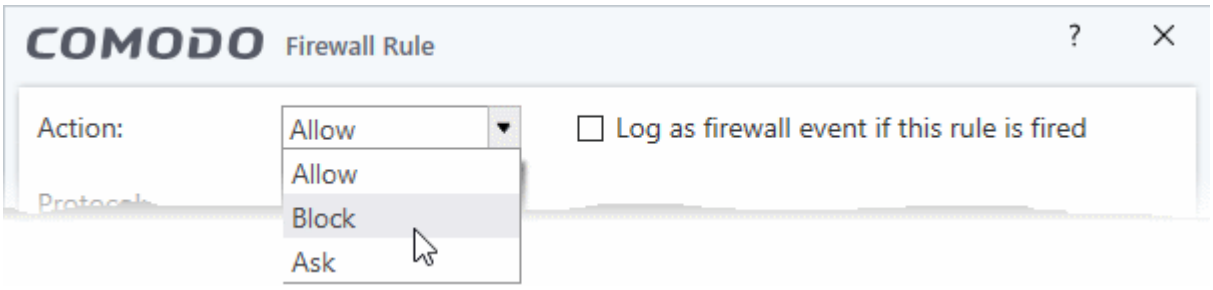
The firewall rule interface is used to configure the actions and conditions of an individual rules. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading '**Understanding Firewall Rules**', '**Overview of Rules and Policies**' and '**Create and Modify Firewall Rulesets**'.

- Click 'Add' in the 'Application Rule' interface to create a new rule
- Double click on an existing rule or select a rule and click 'Edit' to edit an existing rule



General Settings

- **Action**: Specify how firewall should handle the connection request when the conditions of the rule are met. Options available are '**Allow**' ***(Default)***, '**Block**' or '**Ask**'.



- **Protocol**: Specify which protocol the data packet should be using. Options available are **'TCP'**, **'UDP'**, **'TCP or UDP'** ***(Default)***, **'ICMP'** or **'IP'** .

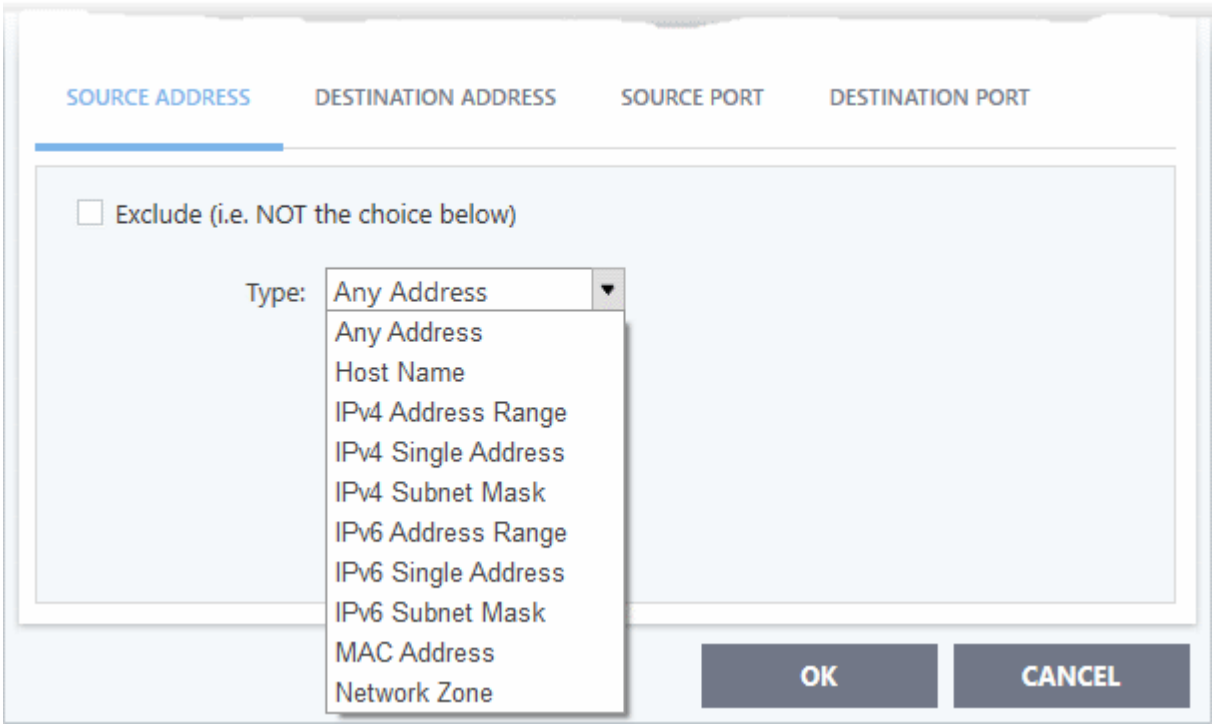
Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- **Direction**: Define whether the rule should intercept inbound or outbound traffic. Options available are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired**: Creates an entry in the **firewall event log viewer** whenever this rule is triggered. (i.e. when ALL conditions have been met) ***(Default = Disabled).***
- **Description**: Enter a friendly name for the rule. For example, 'Allow Outgoing HTTP requests'. The friendly name is shown in the **Application Rules interface**.

Protocol

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

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

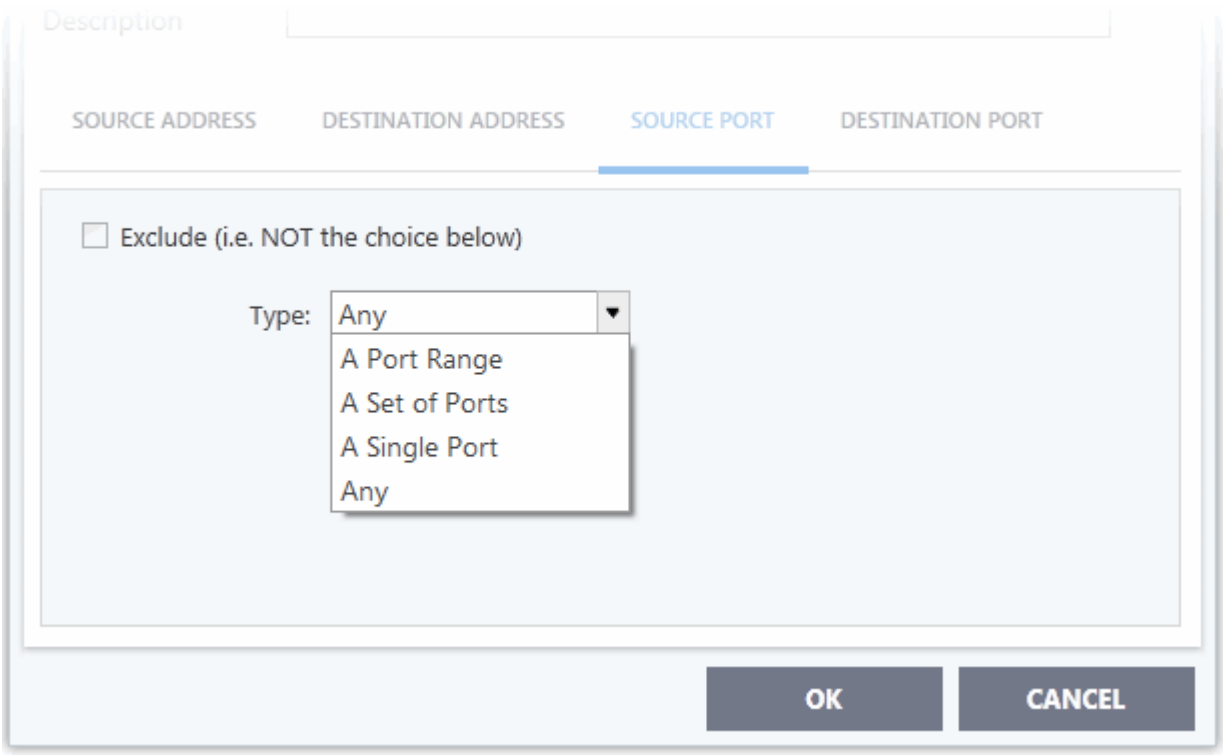


Source Address and Destination Address:

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

- **IPv4 Address Range** - Choose all IP addresses covered by a range - for example a range in your private network.
  - Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.
- **IPv4 Single Address** - Choose a single IPv4 address
  - Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.
- **IPv4 Subnet mask** - Choose an IPv4 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and Mask of the network.
- **IPv6 Address Range** - Choose all IPv6 addresses covered by a range - for example a segment in your private network
  - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.
- **Single IPv6 Address** - Choose an IPv6 address
  - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- **IPv6 Subnet Mask** - Choose a IPv6 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and 'Mask' of the network in the respective fields
- **MAC Address** - Choose a single source/destination by specifying its physical address
  - Enter the physical address in the 'MAC Address' text box.
- **Network Zone** - Choose an entire network. This menu defaults to Local Area Network. But you can also define your own zone by first creating a 'Network Zone' through the 'Network Zones' area.
  - **Exclude (i.e. NOT the choice below)** - Applies the action to all items except the one you specify. For example, you create a block rule, specify an IP address, then select 'Exclude'. The rule will block traffic for every address except the one you specified.

Source Port and Destination Port:



- **Any** - Apply the rule to any port number - set by default, 0- 65535.
- **A Single Port** - Specify a one port number

- Enter the single port number in the 'Port' drop-down combo-box .
- **A Port Range** - Specify a set of ports covered by a range.
  - Enter the first port number and last port number in the respective fields
- **A Set of Ports** - Choose a predefined **Port Set**. If you wish to create a custom port set then please see the section '**Port Sets**'.

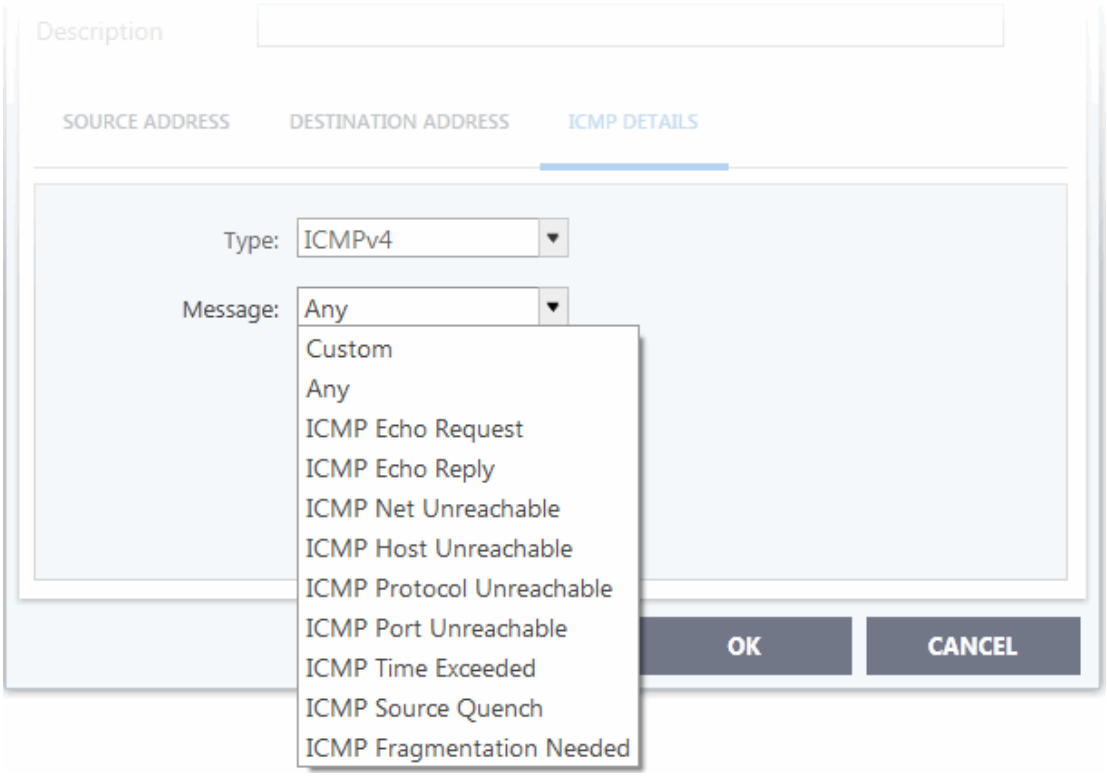
ii. **ICMP**

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

- **ICMP Details**

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

- **'Source' and 'Destination' addresses** - Enter the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.



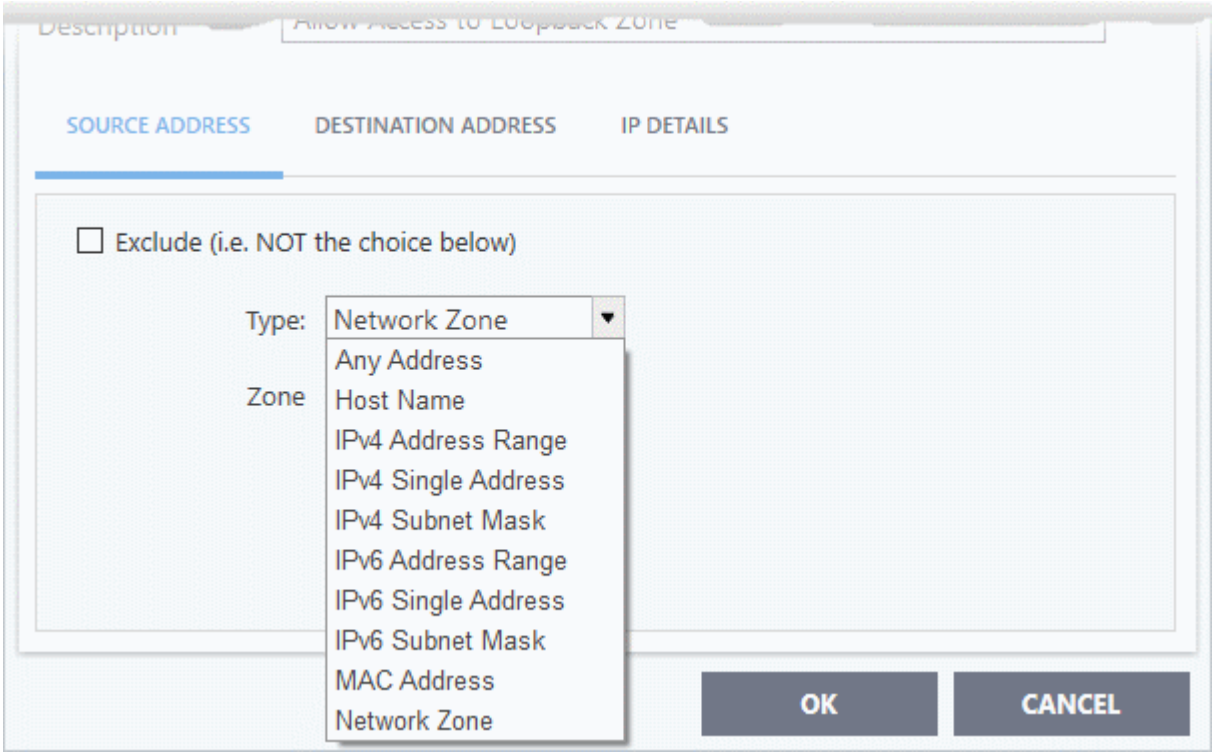
- **Type** - Choose the ICMP version.
- **Message** - Specify the type of the ICMP Message.

When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

iii. **IP**

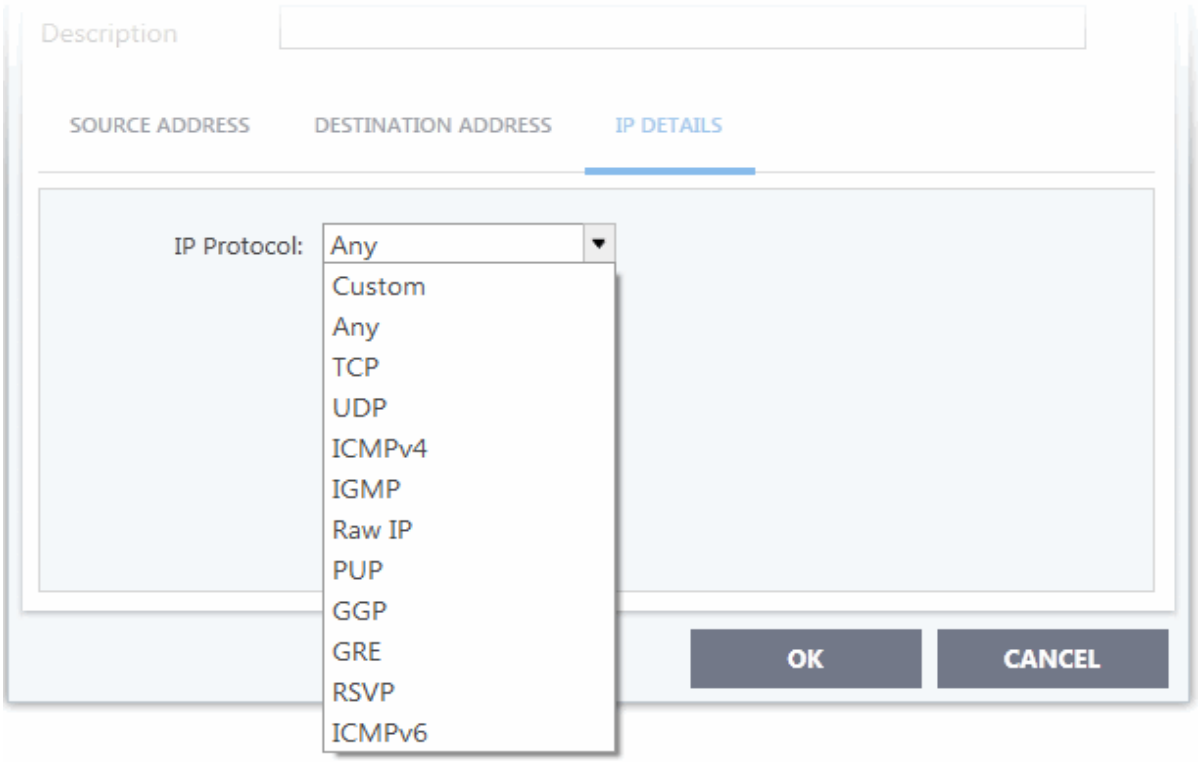
When you select IP as the protocol in **General Settings**, you are shown a list of IP message type in the 'IP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are

configured identically to the **explanation above**. You cannot see the source and destination port tabs.



- **IP Details**

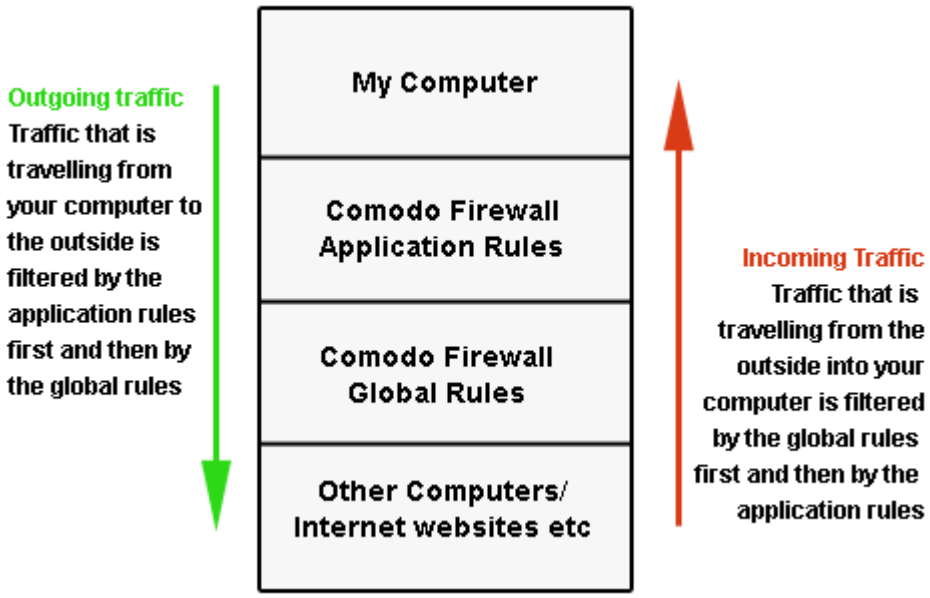
Select the types of IP protocol that you wish to be intercepted by the rule, from the ones that are listed.



- Click 'OK' to save the firewall rule.

7.3.3. Global Rules

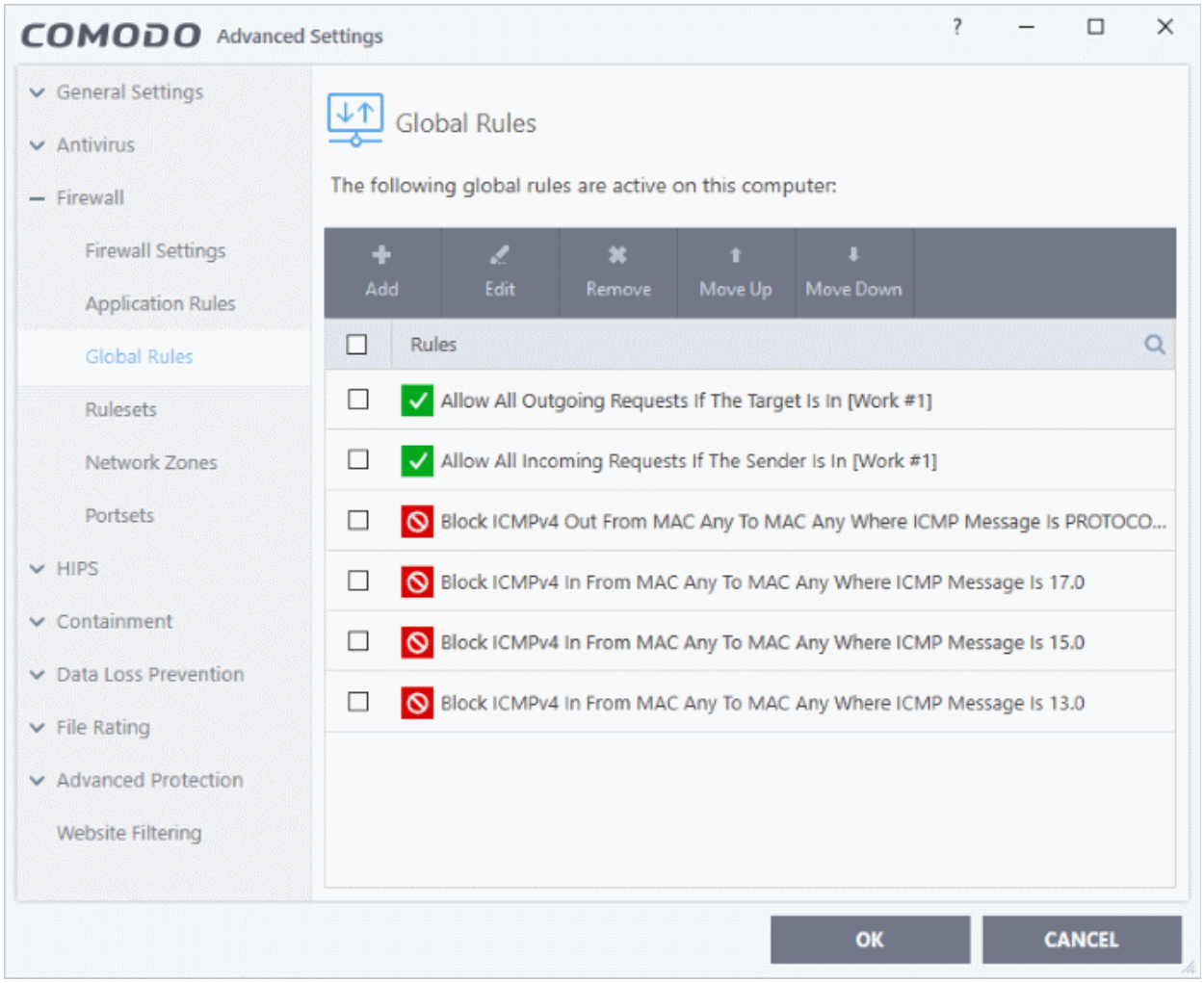
- Click 'Settings' > 'Firewall' > 'Global Rules'
- 'Global Rules' apply to all traffic in and out of your computer. This makes them different to application rules, which apply to the traffic of a specific application.
- Comodo firewall analyzes every packet of data in and out of your PC using combination of application rules and global rules.
  - Outgoing connection attempts - Application rules are consulted first and the global rules second.
  - Incoming connection attempts - Global rules are consulted first and the application rules second.



  - So outgoing traffic has to pass the application rule first then any global rules before it is allowed out. Similarly, incoming traffic has to pass the global rules first then the application rules.
  - Global rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

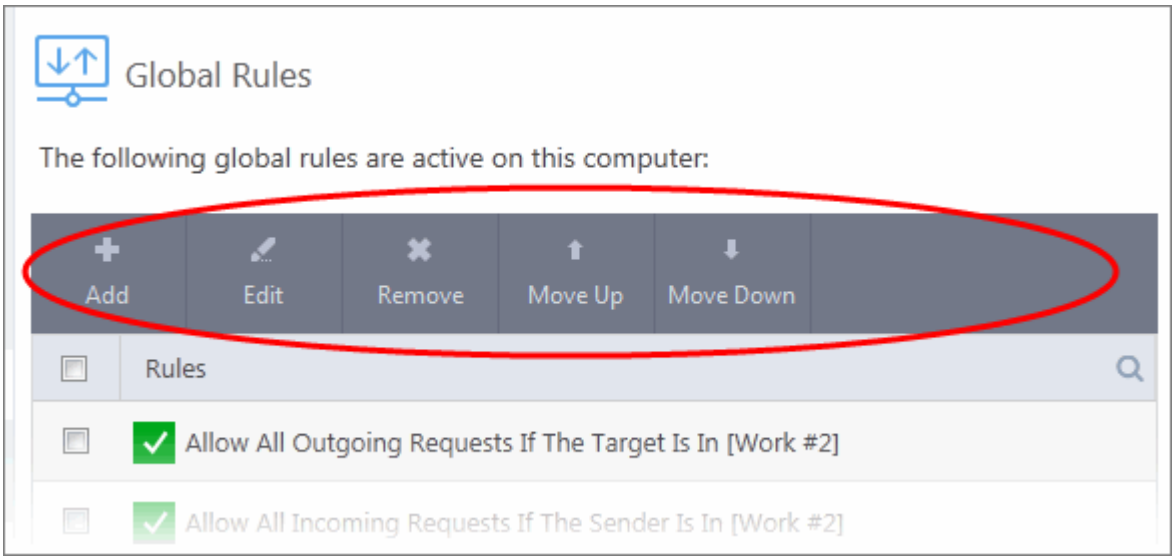
Manage Global Rules

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Global Rules'



General Navigation:

The controls above the table let you create and manage global rules:



- **Add** - Create a new global rule. See '**Add and Edit a Firewall Rule**' in the previous section 'Application Rules' for guidance on creating a new rule.
- **Edit** - Modify an existing global rule. See '**Add and Edit a Firewall Rule**' in the previous section

'Application Rules' for guidance on editing a new rule.

- **Remove** - Deletes the selected rule.
- **Purge** - Runs a system check to verify that all the applications for which rules are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down** - Rules at the top of the list have a higher priority. In the event of a conflict in settings for a piece of traffic, CCS will apply the setting in the rule nearer the top of the list. The 'Move Up' and 'Move Down' buttons let you change the priority of a rule.

- The configuration of global rules is identical to that of application rules. See **Application Rules** for an introduction to the rule setting interface.
- See **Understand Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Add and Edit a Firewall Rule** for an explanation of individual rule configuration.

7.3.4. Firewall Rule Sets

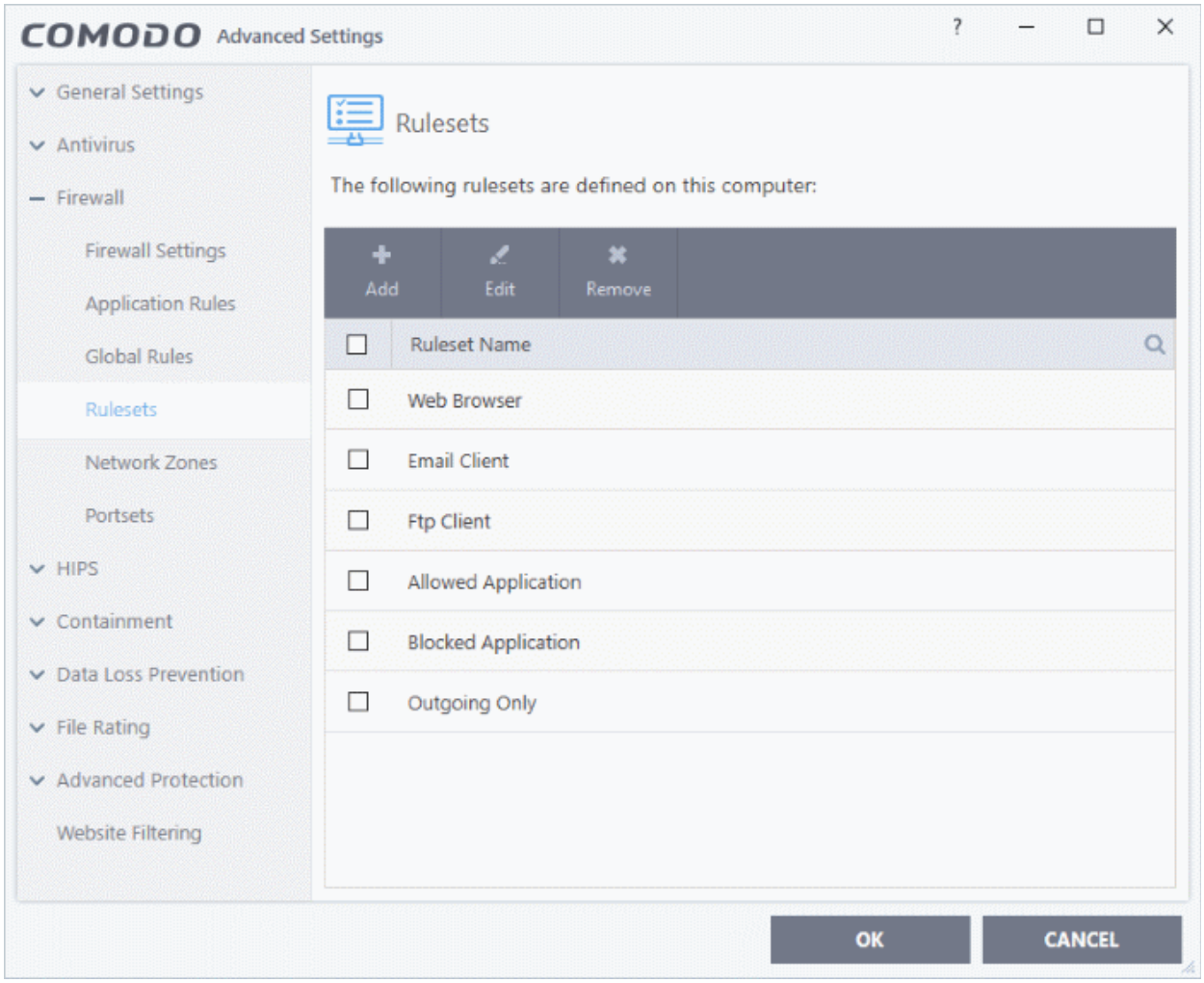
- Click 'Settings' > 'Firewall' > 'Rulesets'
- A firewall ruleset is a collection of one or more firewall rules which can be deployed to applications on your computer.
- CCS ships with six predefined rulesets that provide a very high level of protection. You can also create your own, custom rulesets.

This section contains advice on the following:

- **Predefined Rulesets**
- **Custom Rulesets**
- **Create a new ruleset**

Open the 'Rulesets' panel

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Rulesets'



- The interface shows all existing rulesets. These may be Comodo predefined rules, or custom rulesets.
- Use the search feature to look for a specific ruleset

Predefined Rulesets

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring separate rules, this practice would prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Chrome'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can modify pre-defined policies to suit their environment and requirements. For example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of its rules.

CCS ships with six predefined firewall rulesets for different categories of applications:

- Web Browser
- Email Client
- FTP Client
- Allowed Application
- Blocked Application
- Outgoing Only

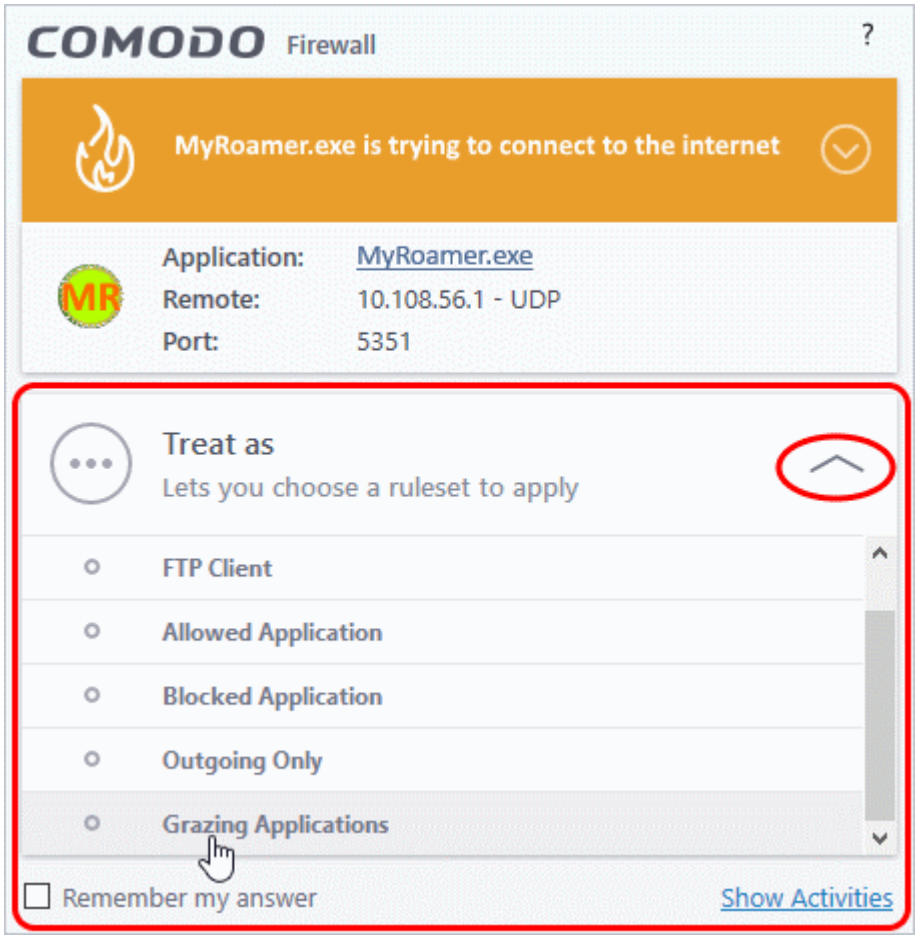
These rulesets can be edited for adding new rules or re-configuring the existing rules. For more details, see **Add and Edit Firewall Rules** in '**Application Rules**'.

Custom Rulesets

You can create new rulesets with custom network access control rules as per your requirements. These can then be applied to specific applications when **creating an application rule**.

The Firewall Alert

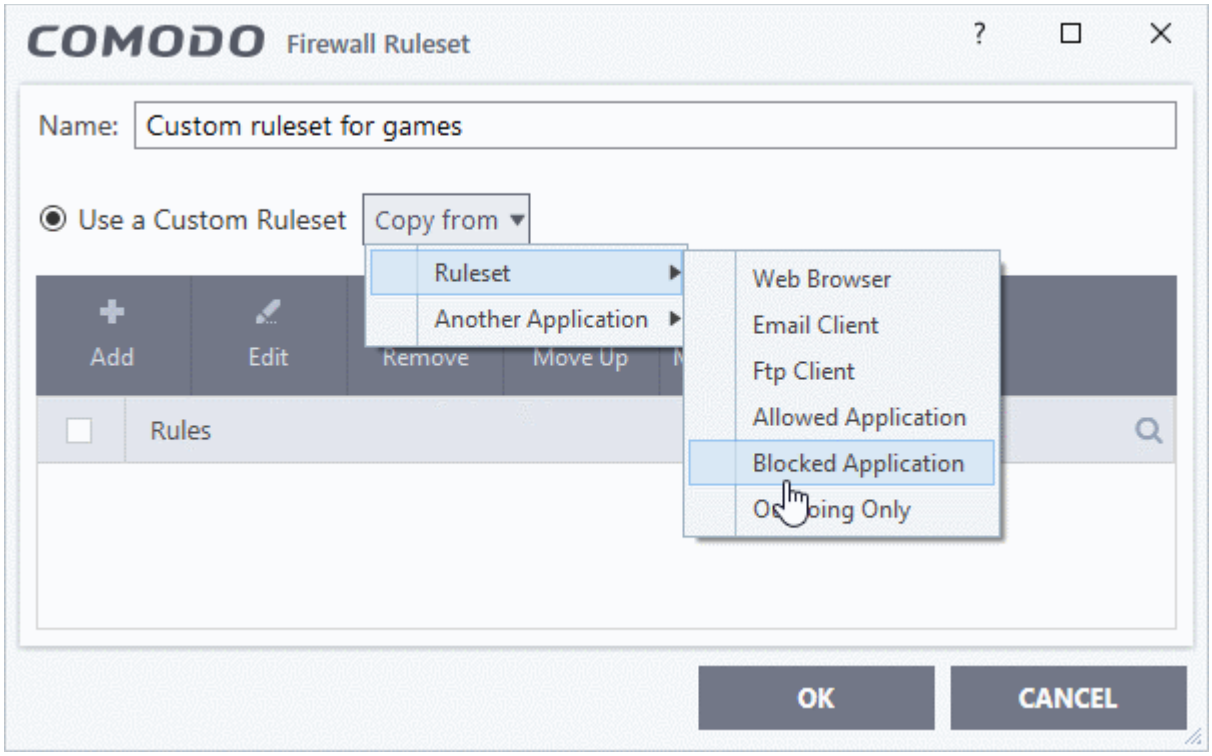
You can apply a firewall ruleset to an application at a firewall alert. Both predefined and custom rulesets are made available. An example alert is shown below:



- See **answering firewall alerts** if you want more help with alerts.

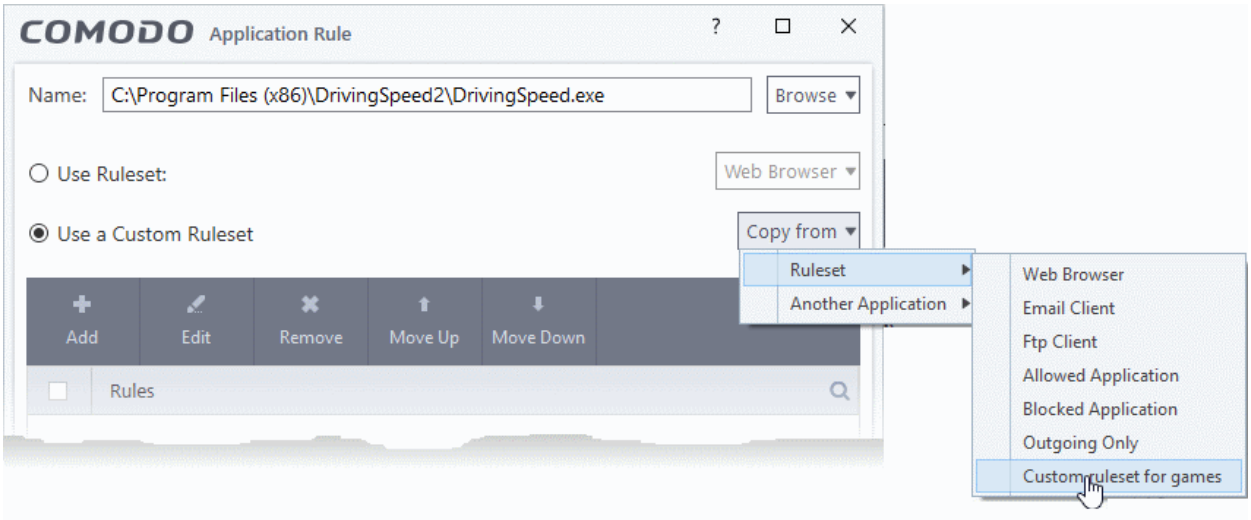
Add a new ruleset

- Click the 'Add' button at the top of the list of rulesets in the 'Rulesets' panel



- Enter a name for this new ruleset. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for.
- Next you should add and configure the individual rules for this ruleset. You can choose to use an existing ruleset as a starting point and add/edit rules as required. See '**Add and Edit a Firewall Rule**' for more advice on this.

Once created, this ruleset can be quickly called when **creating or modifying a firewall ruleset** for an application:



View or edit an existing predefined Ruleset

- Double click on the ruleset Name in the list

Or

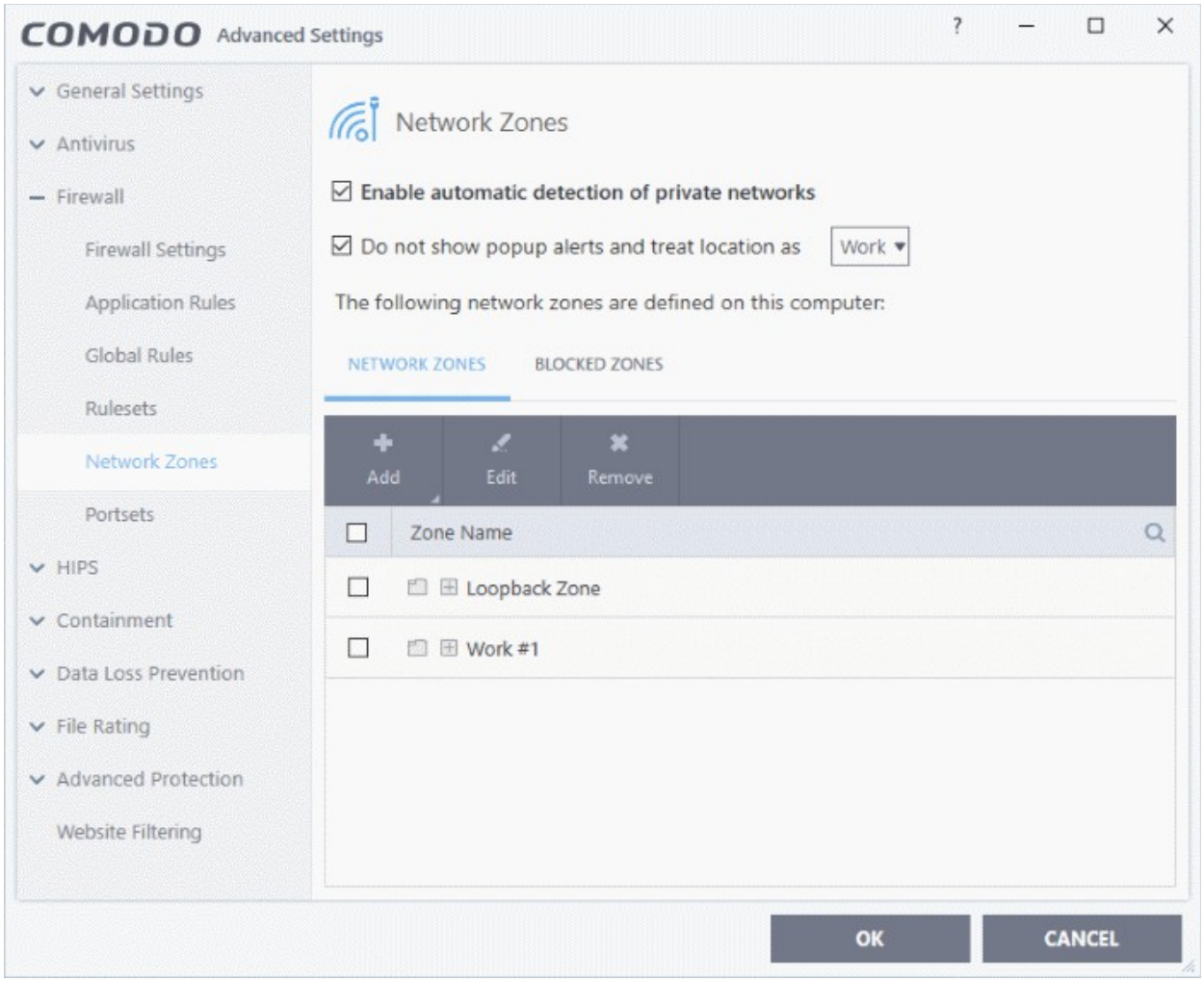
- Select the ruleset name then click the 'Edit' button
- Details of the process from this point on can be found **here**.

7.3.5. Network Zones

- Click 'Settings' > 'Firewall' > 'Network Zones'
- A 'Network Zone' can consist of an individual machine (like a home computer connected to the internet), or a network of thousands of machines. Access to any network zone can be easily granted or denied in the network zones panel.
- The 'Network Zones' panel lets you configure:
  - Automatic detection of networks to which your computer can connect
  - Alerts for network connections
  - Trusted network zones which you want to allow
  - Untrusted network zones which you want to block

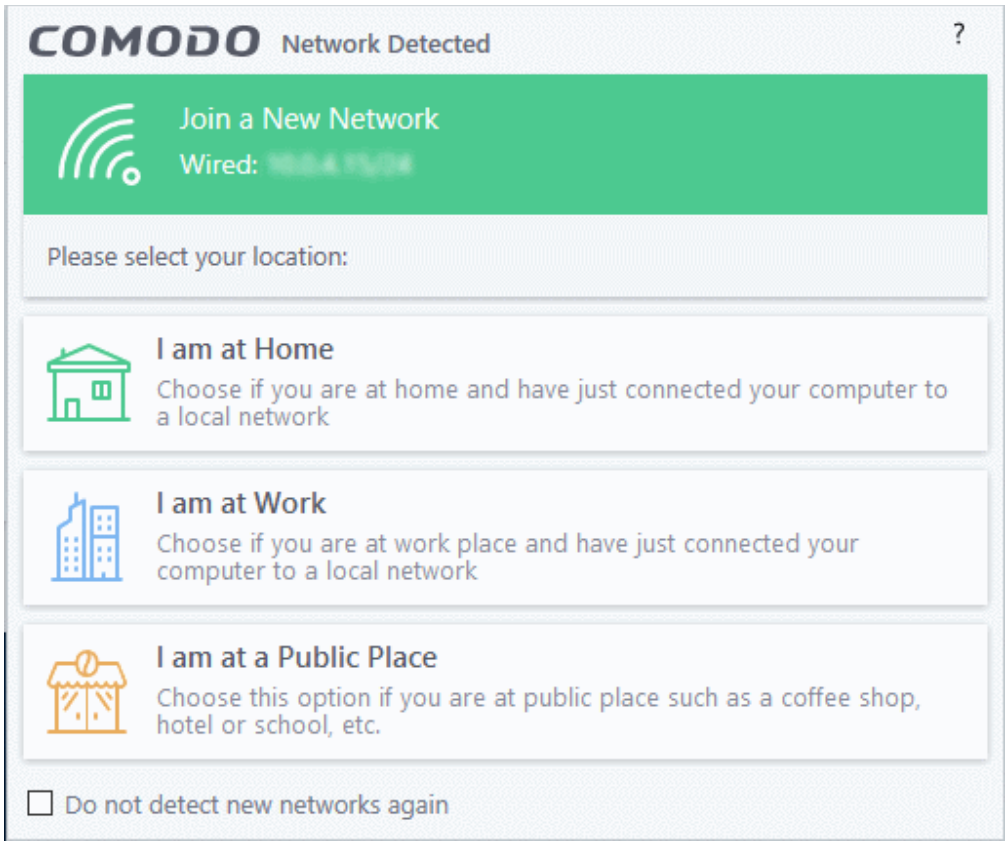
Open the 'Network Zones' panel

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'



- **Enable automatic detection of private networks** - The firewall monitors attempted connections to any new wired or wireless network (***Default = Enabled***). Deselect this option if you are an experienced user and wish to manually set-up your own trusted networks (this can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**').
- **Do not show popup alerts and treat location as** - CCS can show an alert when your computer attempts to connect to a new network.

- **Disabled** - The alert is shown. Select the appropriate network type for your connection. CCS will optimize the firewall for security and usability based on your choice. (***Default***)
- **Enabled** - The alert is not shown. You now need to pick a default network type from 'Home', 'Work', or 'Public'. CCS will automatically apply your choice of network type to all new connections.



- Select 'Do not detect new networks again' If you are an experienced user that wishes to manually set-up their own trusted networks. This can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**'.

The panel has two tabs:

- **Network Zones** - Define network zones with specific access rights. Application access privileges are specified in the **Application Rule** interface. See '**Create or Modify Firewall Rules**' for more details.
- **Blocked Zones** - Define networks that are not trusted. CCS will deny all connections to blocked zones.

7.3.5.1. Network Zones

- Click 'Settings' > 'Firewall' > 'Network Zones' > 'Network Zones'
- A 'Network Zone' can consist of an individual machine (like a home computer connected to the internet) or a network of thousands of machines. You can grant or deny access to a network zone as required.

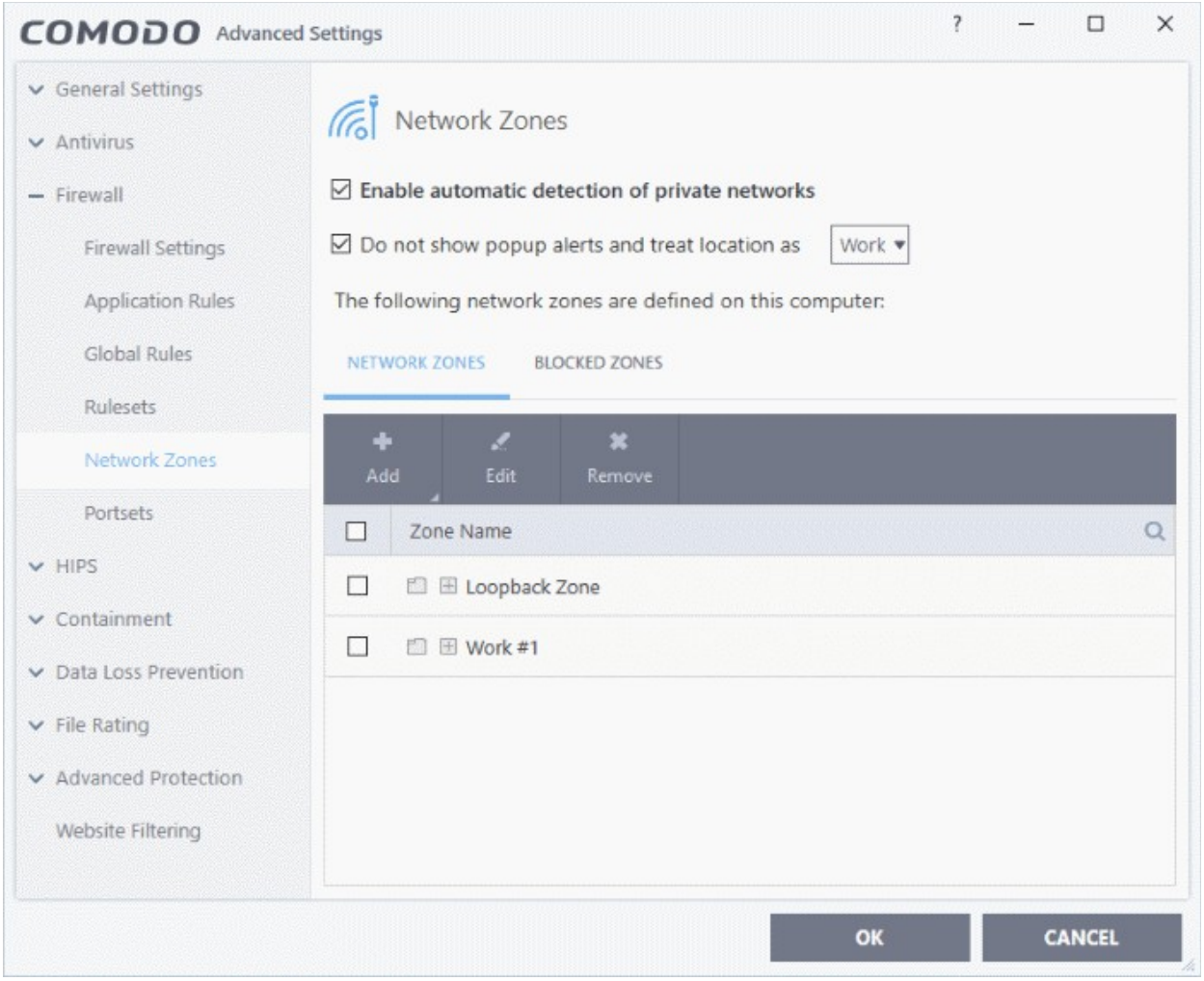
Background Note:

- A computer network is a connection between computers through a cabled or wireless connection.
- A network allows users to share information and resources with other computers/users on the network.
- There are some networks which you trust and want to grant access to, including your home or work network.
- Conversely, there may be other networks with which you want to restrict communication, or even block entirely.

- The network zones panel lets you configure trusted and untrusted networks.

Add and manage network zones

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab



The network zones tab shows zones that have already been added to CCS. You can add new zones and manage existing zones.

Note 1: Adding a zone to this area does not, by itself, define any permissions or access rights to the zone. This area lets you define the zones so you can assign such permissions **in other areas of the firewall**.

Note 2: A network zone can be designated as 'Trusted' and allowed access from the '**Manage Network Connections**' interface. An example would be your home computer or network.

Note 3: A network zone can be designated as 'Blocked' and denied access by using the '**Blocked Zones**' interface.

Note 4: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rule** assigned to a zone will inspect all traffic to/from a zone.

Note 5: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc) once you connect

to them. This can be disabled by deselecting the option 'Enable automatic detection of private networks' in the **Firewall Settings** panel.

You can use search for a specific zone by clicking the search icon and entering the name of the zone in part or full.

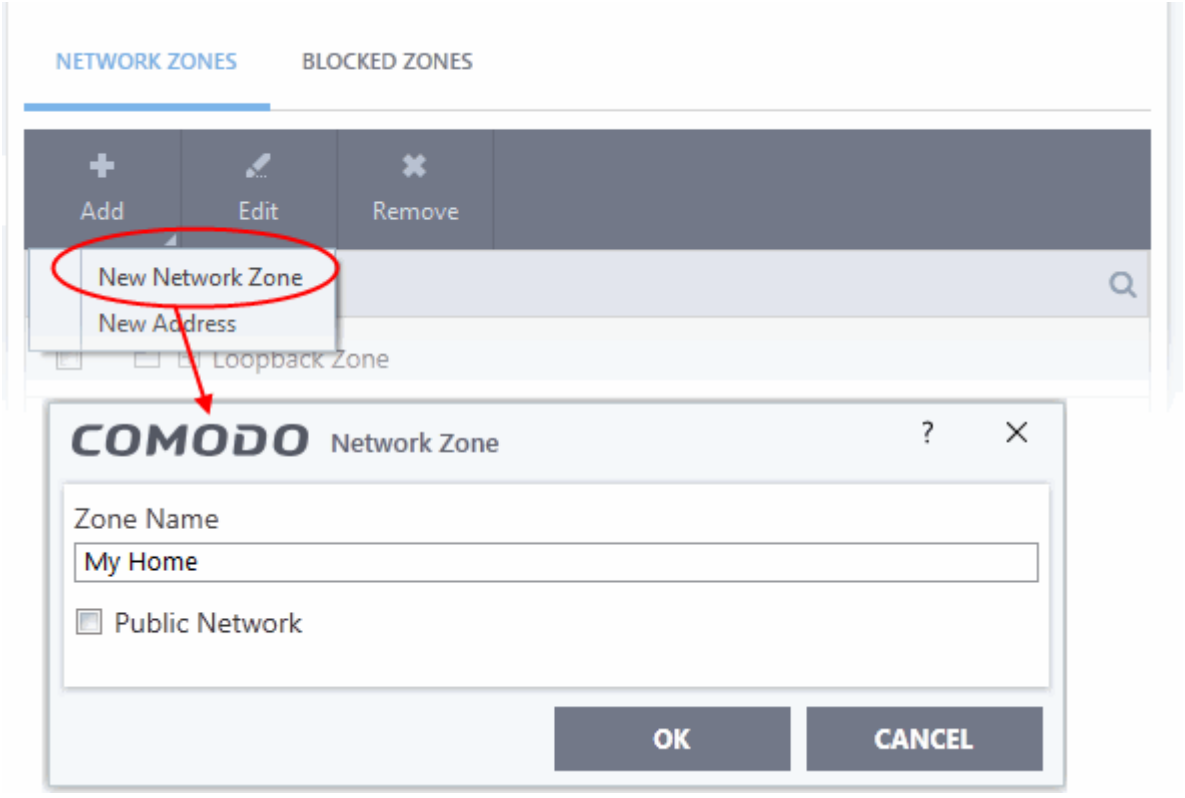
Defining a new Network Zone

To add a new network zone:

- Step 1 - **Define a name for the zone**.
- Step 2 - **Select the addresses to be included in the zone.**

Step 1 - Define a name for the zone

- Click 'Settings' on CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab
- Click the 'Add' button at the top of the list and choose 'New Network Zone' from the options.



- Choose a name that accurately describes the network zone you are creating.
- Select 'Public Network' if you are defining a network zone for a network in a public place. For example, when you are connecting to a Wi-Fi network at an airport, restaurant etc. The firewall will optimize the connection accordingly.
- Click 'OK' to confirm your zone name.

This adds your new zone to the 'Network Zones' list.

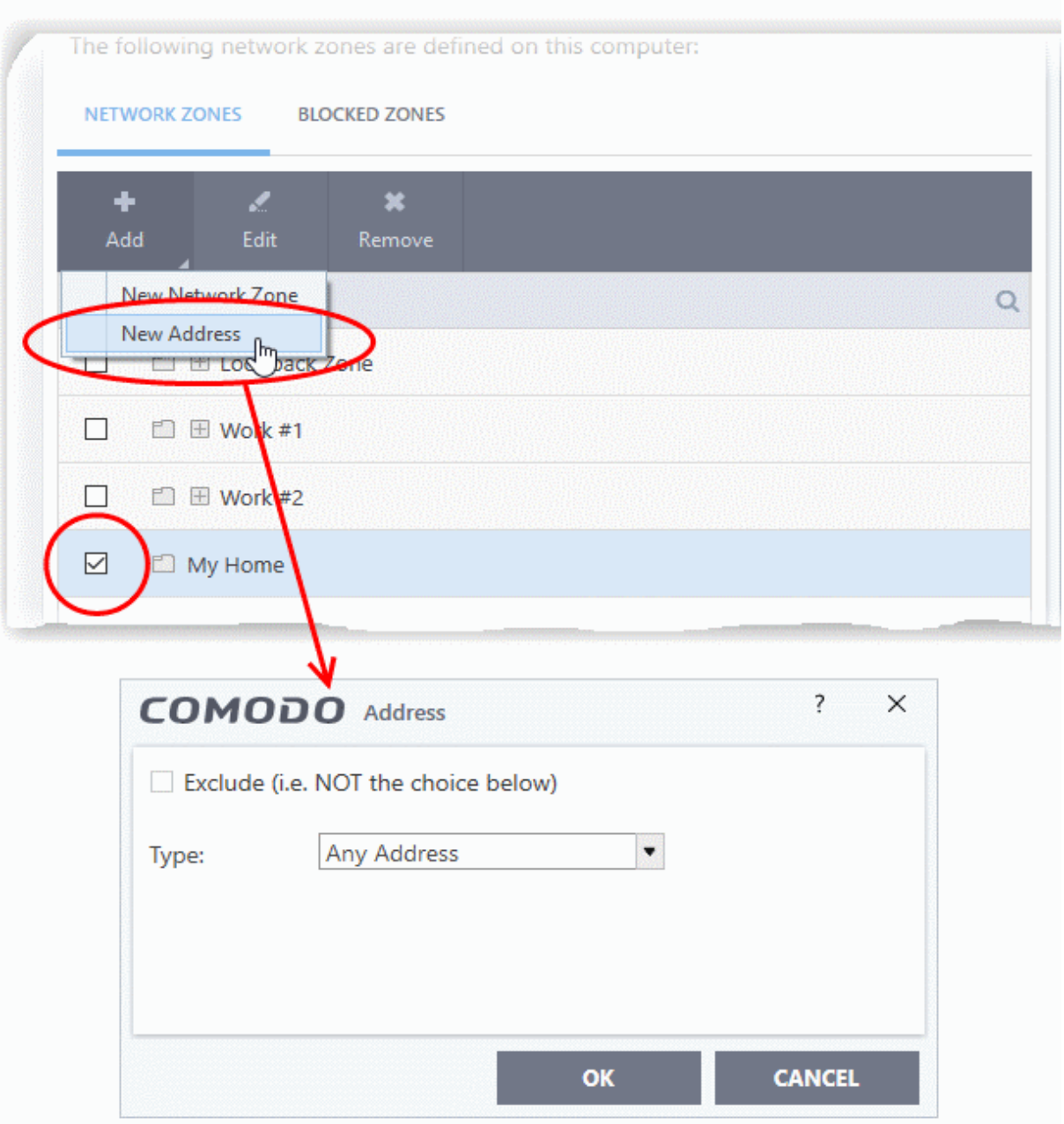
Step 2 - Select the addresses to be included in this zone

- Select the network zone name then click the 'Add' button at the top
- Choose 'New Address' from the options

- Alternatively, right click on the network zone and choose 'Add' > 'New Address' from the context sensitive menu

The 'Address' dialog allows you to select an address from the 'Type' drop-down box shown below ***(Default = Any Address)***.

The 'Exclude' check box will become active if you select anything other than 'Any Address'



Address Types:

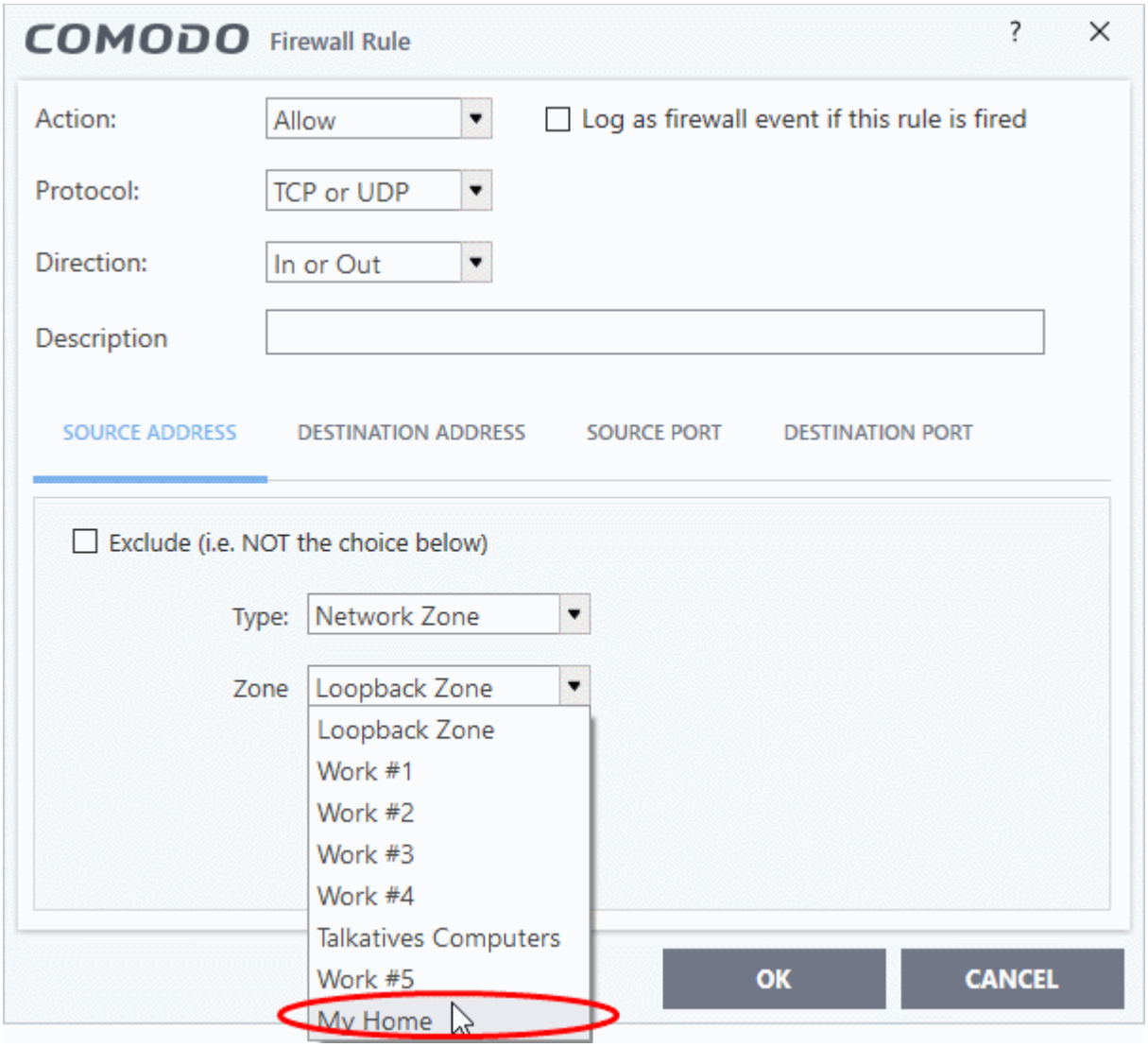
- **Any** - Defaults to an IP range of 0.0.0.0- 255.255.255.255 to block connection from all IP addresses.
- **Host Name** - Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field
- **IPv4 Address Range** - Choose all IP addresses covered by a range - for example a range in your private network.
  - Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.
- **IPv4 Single Address** - Choose a single IPv4 address

        - Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.
    - **IPv4 Subnet mask** - Choose an IPv4 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
        - Enter the IP address and Mask of the network.
    - **IPv6 Address Range** - Choose all IPv6 addresses covered by a range - for example a segment in your private network
        - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.
    - **Single IPv6 Address** - Choose an IPv6 address
        - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
    - **IPv6 Subnet Mask** - Choose a IPv6 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
        - Enter the IP address and 'Mask' of the network in the respective fields
    - **MAC Address** - Choose a single source/destination by specifying its physical address
        - Enter the physical address in the 'MAC Address' text box.
    - **Exclude (i.e. NOT the choice below)** - The opposite of what you specify is applicable.
- Click 'OK' to confirm your choice.
- Click 'OK' in the 'Network Zones' interface.

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

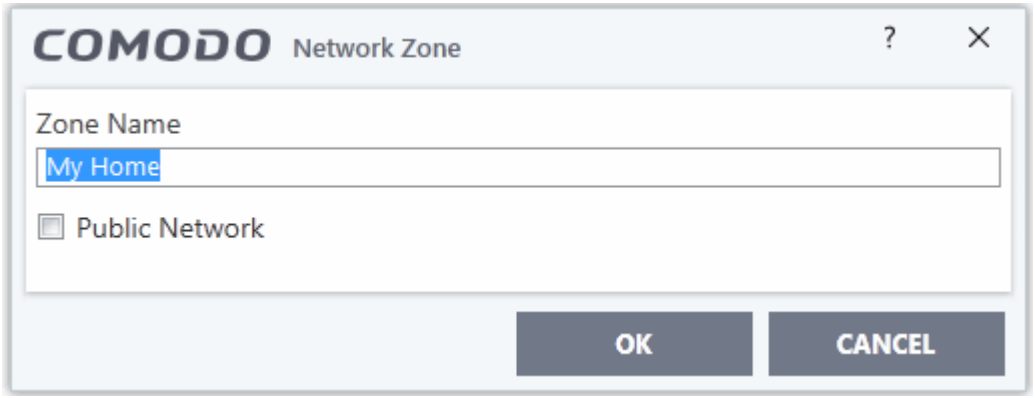
- Quickly called as 'Zone' when **creating or modifying a firewall ruleset**



- Quickly called and designated as a blocked zone from the '**Blocked Zones**' interface

Edit the name of an existing Network Zone

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Network Zones' tab
- Select the zone from the list (e.g., My Home) and click the 'Edit' button from the top or double click on the network zone name.



- Change the name of the zone and click 'OK'.

To add more addresses to an existing Network Zone

- Select the network name, click the 'Add' > 'New Address' from the top.
- Add new address from the **'Address' interface**.

To modify or change the existing address in a zone

- Click the + button beside the network zone name to expand the addresses
- Double click on the address to be edited or select the address, click 'Edit' at the top
- Edit the address from the **'Address' interface**.

To remove an existing address in a zone

- Click the '+' button beside the network zone name to expand the addresses
- Select the address and click 'Remove' from the top

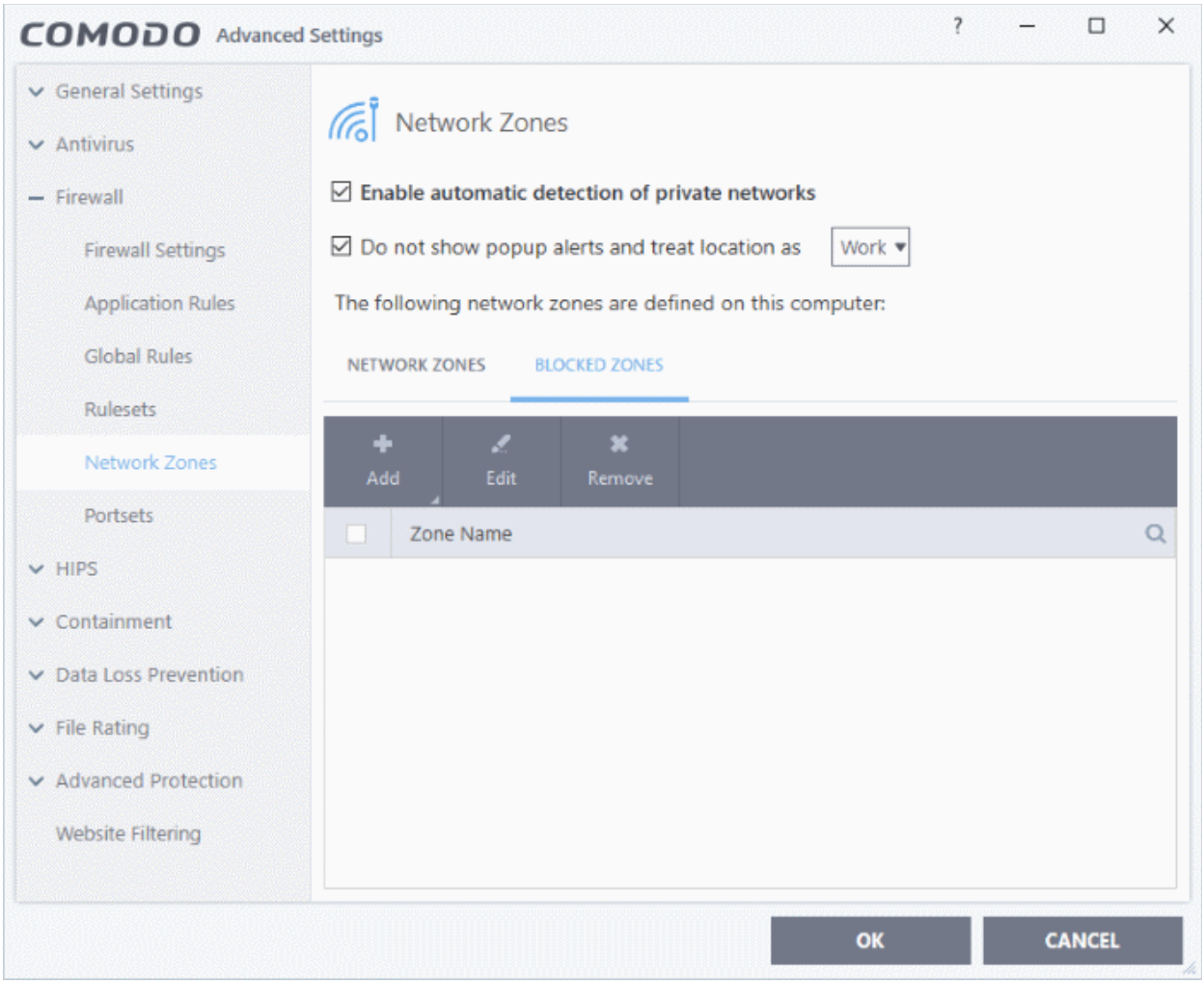
7.3.5.2. Blocked Zones

- Click 'Settings' > 'Firewall' > 'Network Zones' > 'Blocked Zones'
- A computer network lets you share information and resources with other users and computers.
- There are some networks which you trust and want to grant access to, including your home or work network.
- Conversely, there may be other networks with which you want to restrict communication, or even block entirely.
- The 'Blocked Zones' section allows you to configure restrictions on network zones that you do not trust.

Note: We advise new or inexperienced users to first read '**Network Zones**', '**Stealth Ports Wizard**' and '**Application Rules**' before blocking zones in this interface.

Add and manage blocked zones

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab:



The 'Blocked Network Zones' tab allows you to:

- **Deny access to an existing network zone**
- **Deny access to a network by manually defining a new blocked zone**

Note 1: You must create a zone before you can block it. There are two ways to do this;

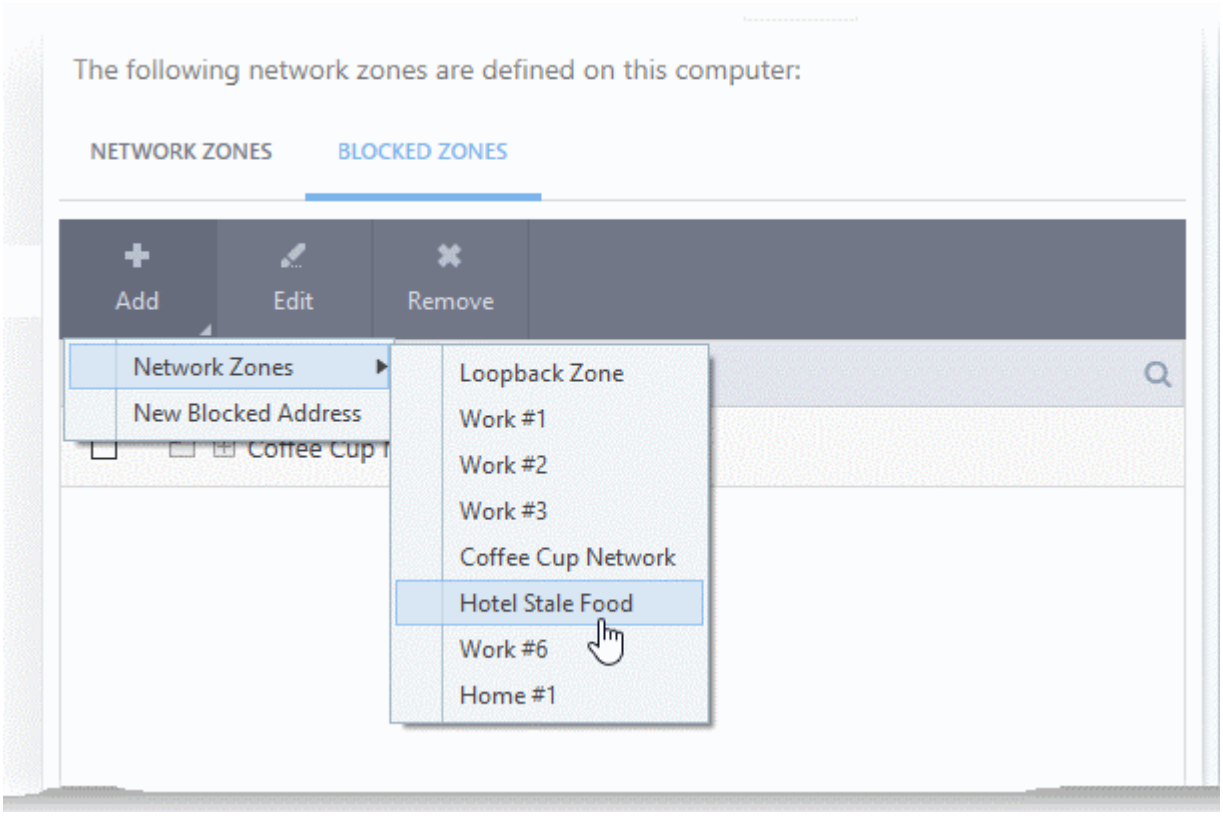
1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

Note 2: You cannot reconfigure *existing* zones from this interface (e.g., to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

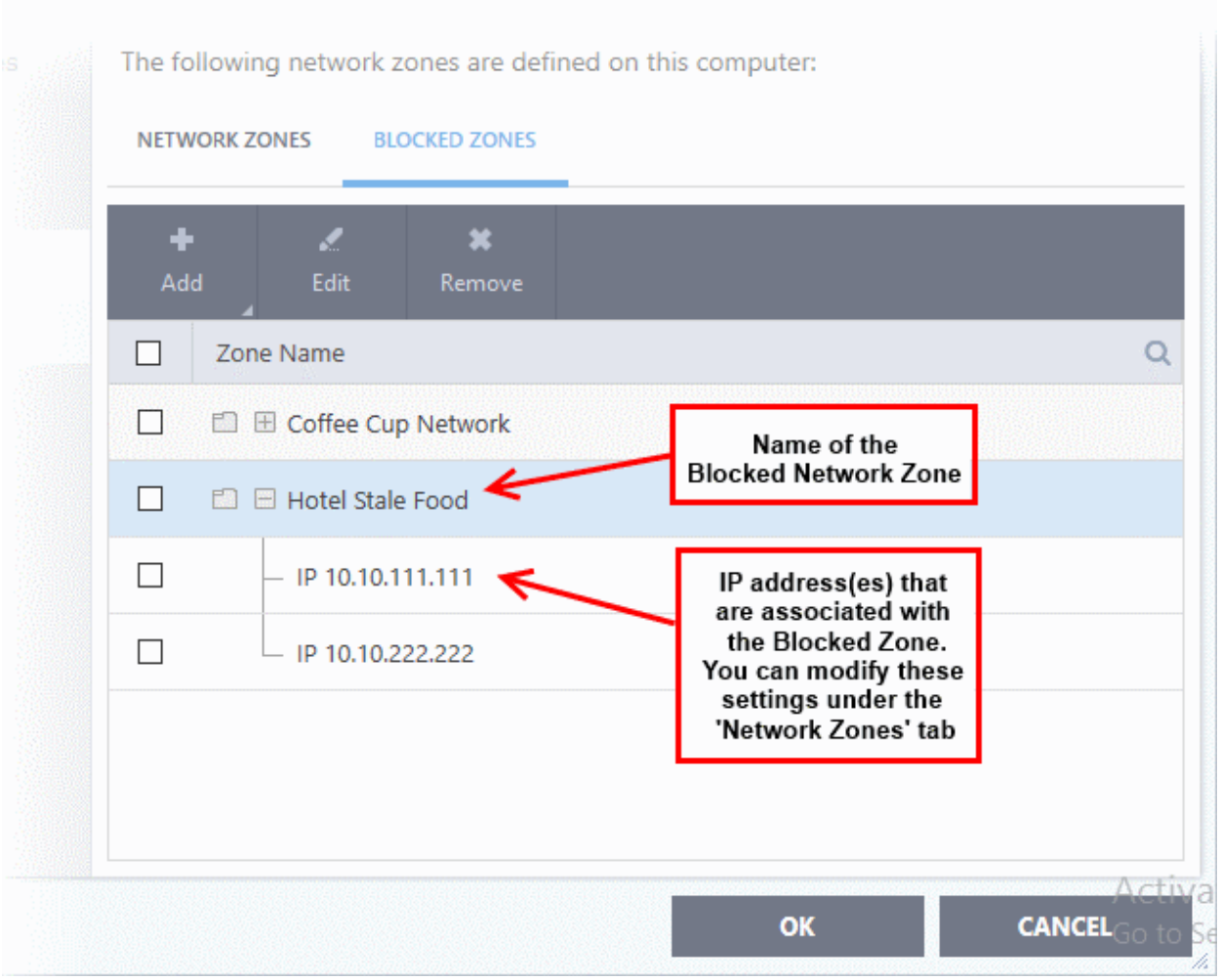
You can search for specific blocked zone by clicking the magnifying glass icon and entering the name of the zone in part or full.

Deny access to an existing network zone

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab
- Click 'Add' button at the top and choose 'Network Zones' from the options
- Select the particular zone you wish to block.



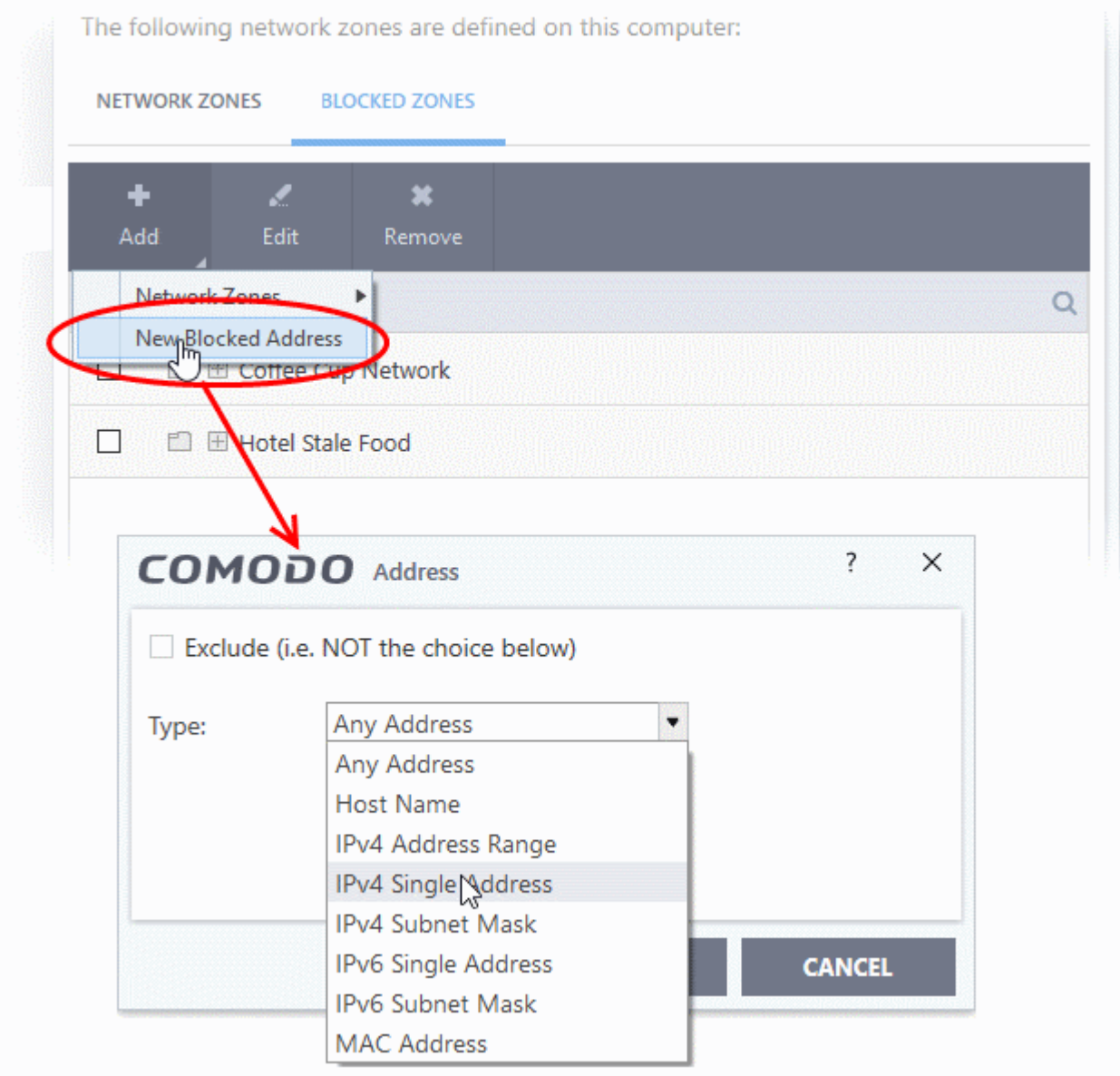
The selected zone will appear in the 'Blocked Zones' interface.



- Click 'OK' to confirm your choice.
- All traffic to and from devices in this zone is now blocked.

Deny access to a network by manually defining a new blocked zone

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Network Zones'
- Click the 'Blocked Zones' tab
- Click the 'Add' button and choose 'New Blocked Address':



Select the address type you wish to block from the 'Type' drop-down. Select 'Exclude' if you want to block all IP addresses except for the ones you specify using the drop-down.

Address Types:

- **Any** - Defaults to an IP range of 0.0.0.0- 255.255.255.255 to block connection from all IP addresses.
- **Host Name** - Choose a named host which denotes your IP address. Enter the name in the 'Host Name' text field
- **IPv4 Address Range** - Choose all IP addresses covered by a range - for example a range in your

private network.

- Enter the first and last IP addresses in the 'Start IP' and 'End IP' text boxes.

- **IPv4 Single Address** - Choose a single IPv4 address
  - Enter the IP address in the 'IP' text box, e.g., 192.168.200.113.
- **IPv4 Subnet mask** - Choose an IPv4 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and Mask of the network.
- **IPv6 Address Range** - Choose all IPv6 addresses covered by a range - for example a segment in your private network
  - Enter the first and last IPv6 addresses in the 'Start IP' and 'End IP' text boxes.
- **Single IPv6 Address** - Choose an IPv6 address
  - Enter the IP address in the 'IP' text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
- **IPv6 Subnet Mask** - Choose a IPv6 network. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network.
  - Enter the IP address and 'Mask' of the network in the respective fields
- **MAC Address** - Choose a single source/destination by specifying its physical address
  - Enter the physical address in the 'MAC Address' text box.
- **Exclude (i.e. NOT the choice below)** - The opposite of what you specify is applicable.

- Select the address to be blocked and click 'OK'

  The address(es) you block will appear in the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

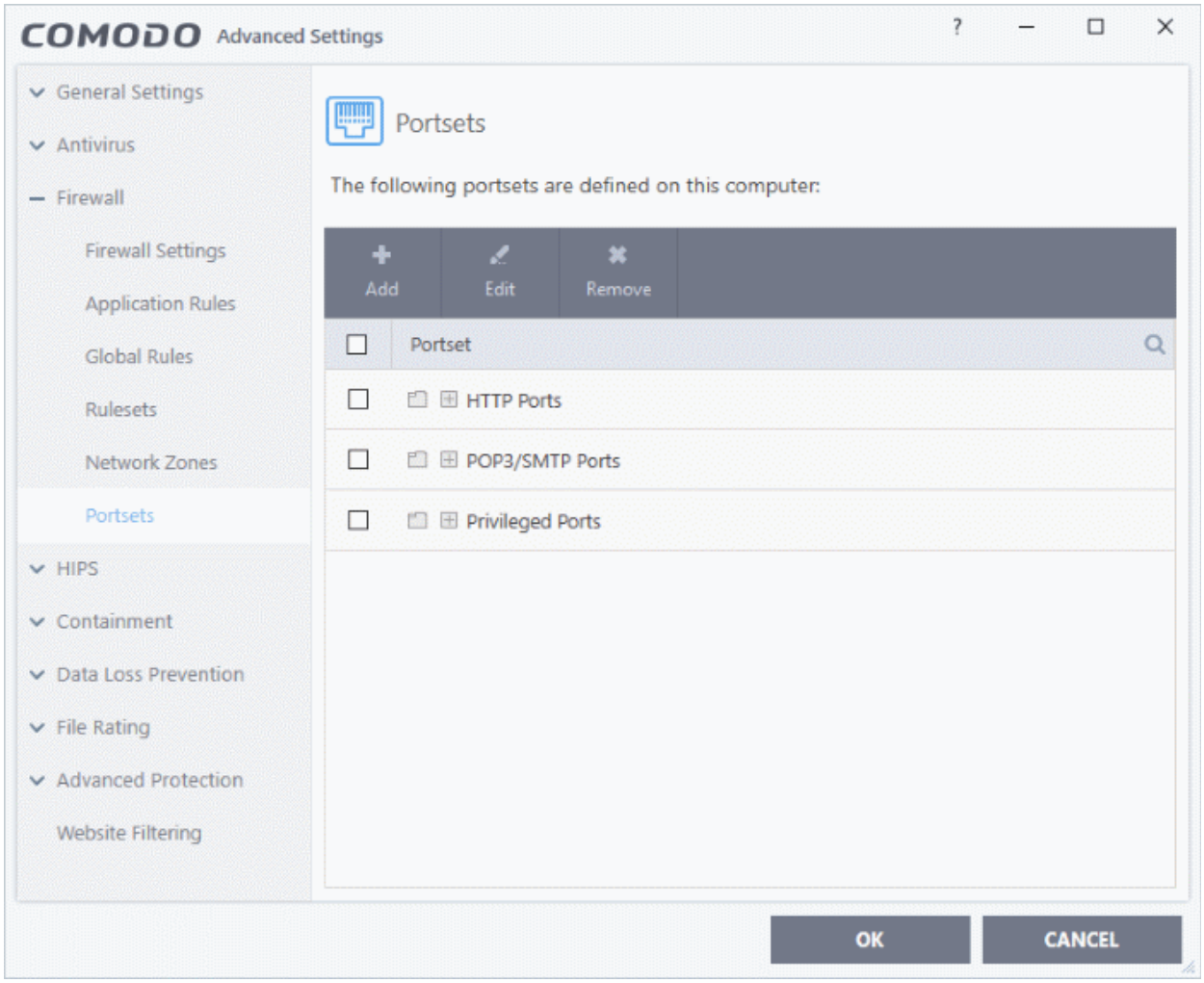
- Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from devices in this zone is now blocked.

7.3.6. Port Sets

- Click 'Settings' > 'Firewall' > 'Portsets'
- Port sets are predefined groups of one or more ports. These sets can be named as the target of **Application Rules** and **Global Rules**. For example, you might want to block all inbound traffic to certain set of ports.
- The port sets panel lets you add, view and manage port sets

Open the Portsets panel

- Click 'Settings' at the top of the CCS home screen
- Click 'Firewall' > 'Portsets'



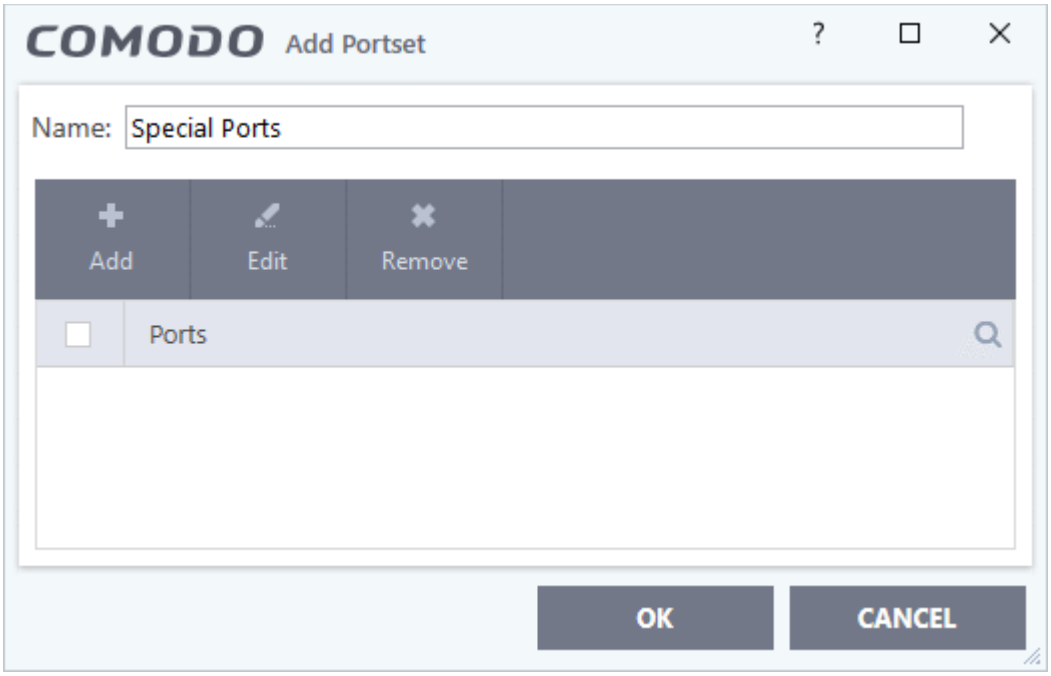
- The interface lists all existing port sets. Click the + button to view all ports in a set.
- CCS ships with three default portsets:
  - **HTTP Ports**: 80, 443 and 8080. These are the default ports for http traffic. Your internet browser uses these ports to connect to the internet and other networks.
  - **POP3/SMTP Ports**: 110, 25, 143, 995, 465 and 587. These ports are typically used for email communication by mail clients like Outlook and Thunderbird.
  - **Privileged Ports:** 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports. This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range.

Define a new port set

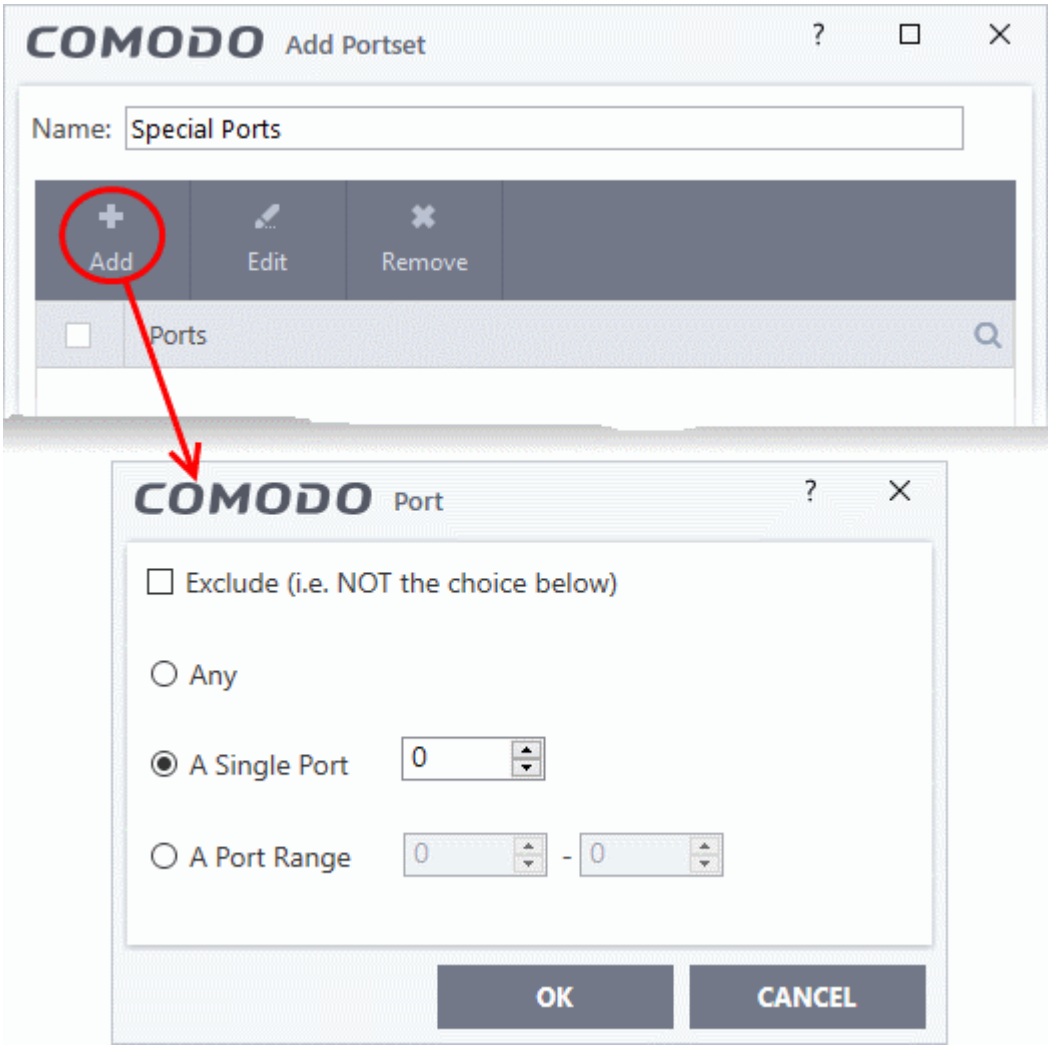
After defining a new port set, you can apply it to applications through the **Application Rule** interface. See '**Creating or Modifying Firewall Rules**' for more details.

Add a new portset

- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Portsets'
- Click the 'Add' button at the top.

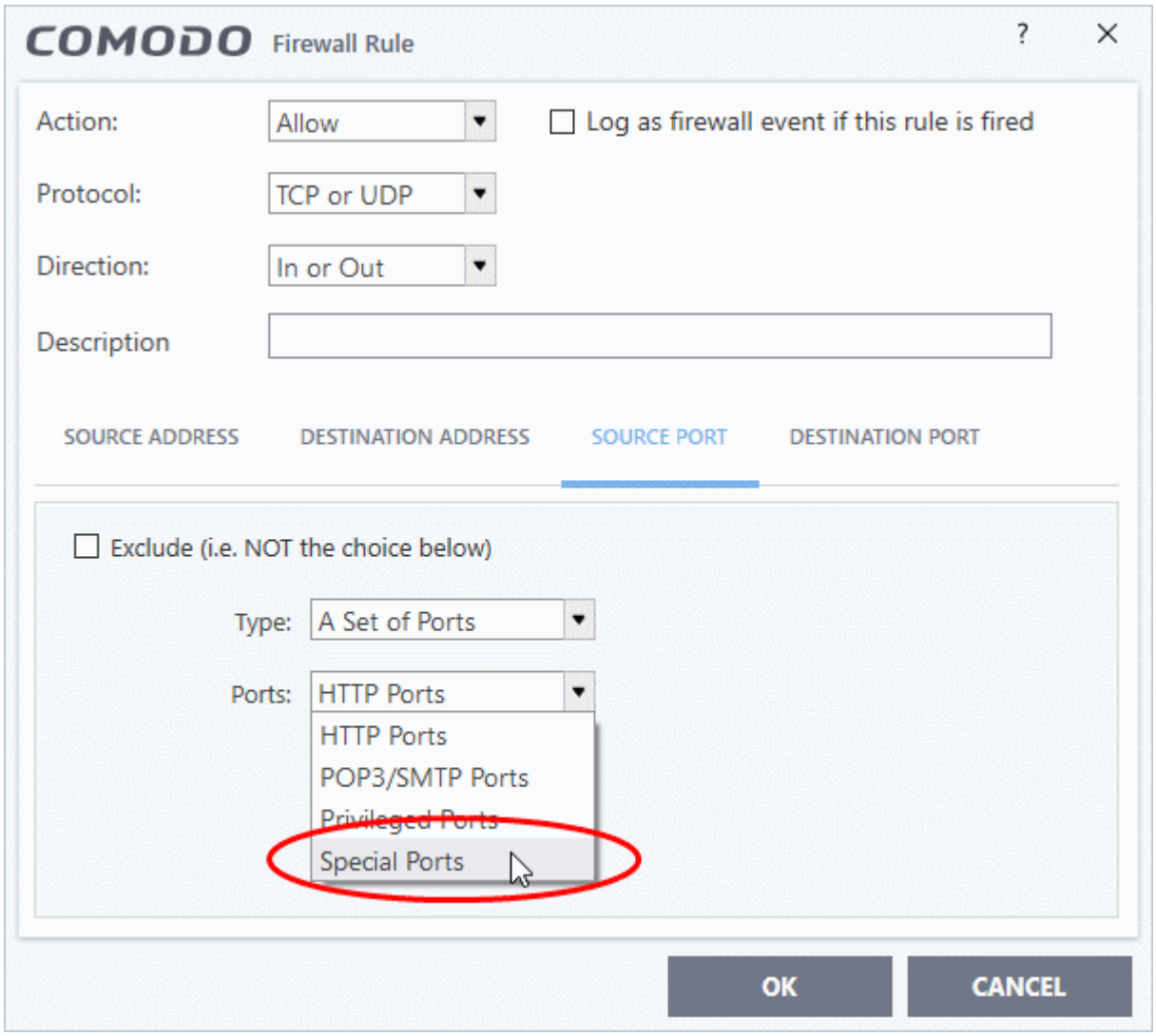


- Create a name for the port set
- Click 'Add' to specify ports and port ranges for the set:



- Specify the ports to be included in the new portset:
  - **Any -** to choose all ports
  - **A single port -** Specify the port number
  - **A port range** - Enter the start and end port numbers in the respective combo boxes.
  - Exclude (i.e. NOT the choice below): Means all ports will be included in the portset except the ones you specify here
- Click 'OK' in the 'Port' dialog then click 'OK' in the 'Add Portset' interface

  You can now select 'A Set of Ports', then choose this rule-set, when **creating or modifying a Firewall Ruleset**



Edit an existing port set

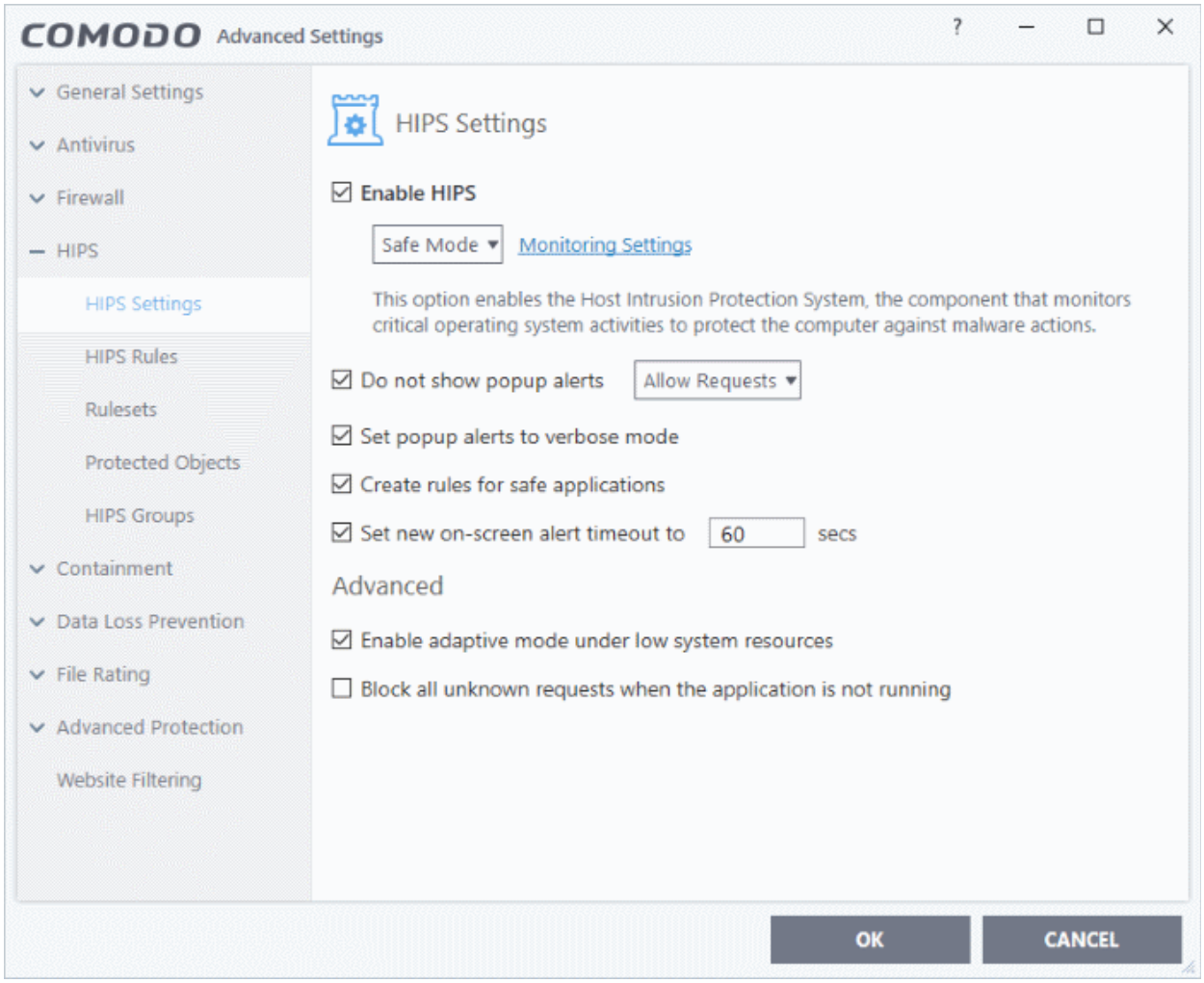
- Click 'Settings' on the CCS home screen
- Click 'Firewall' > 'Portsets'
- Select the port set from the list
- Click the 'Edit' button
- The editing procedure is similar to **adding the portset** explained above.

7.4. HIPS Configuration

- Click 'Settings' > 'HIPS'
- The host intrusion protection system (HIPS) constantly monitors system activity and stops processes from modifying important files and interfaces.
- Comodo Client Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection.
  - For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs.
- Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

Configure HIPS settings

- Click 'Settings' on the CCS home screen
- Click 'HIPS' on the left:



- **HIPS Settings** - General settings that govern the overall behavior of the HIPS component.
- **HIPS Rules** - These rules determine what actions an application is allowed to perform, and what level of protection it enjoys from other processes.
- **Rulesets** - View predefined rulesets and create new rulesets that can be applied to your applications in your system.
- **Protected Objects** - Define objects to be protected by HIPS such as specific folders, system critical

registry keys and so on.

- **HIPS Groups** - View and edit predefined 'Registry Groups' and 'COM Groups', create new groups so as to add them to Protected Objects.

Note for beginners:

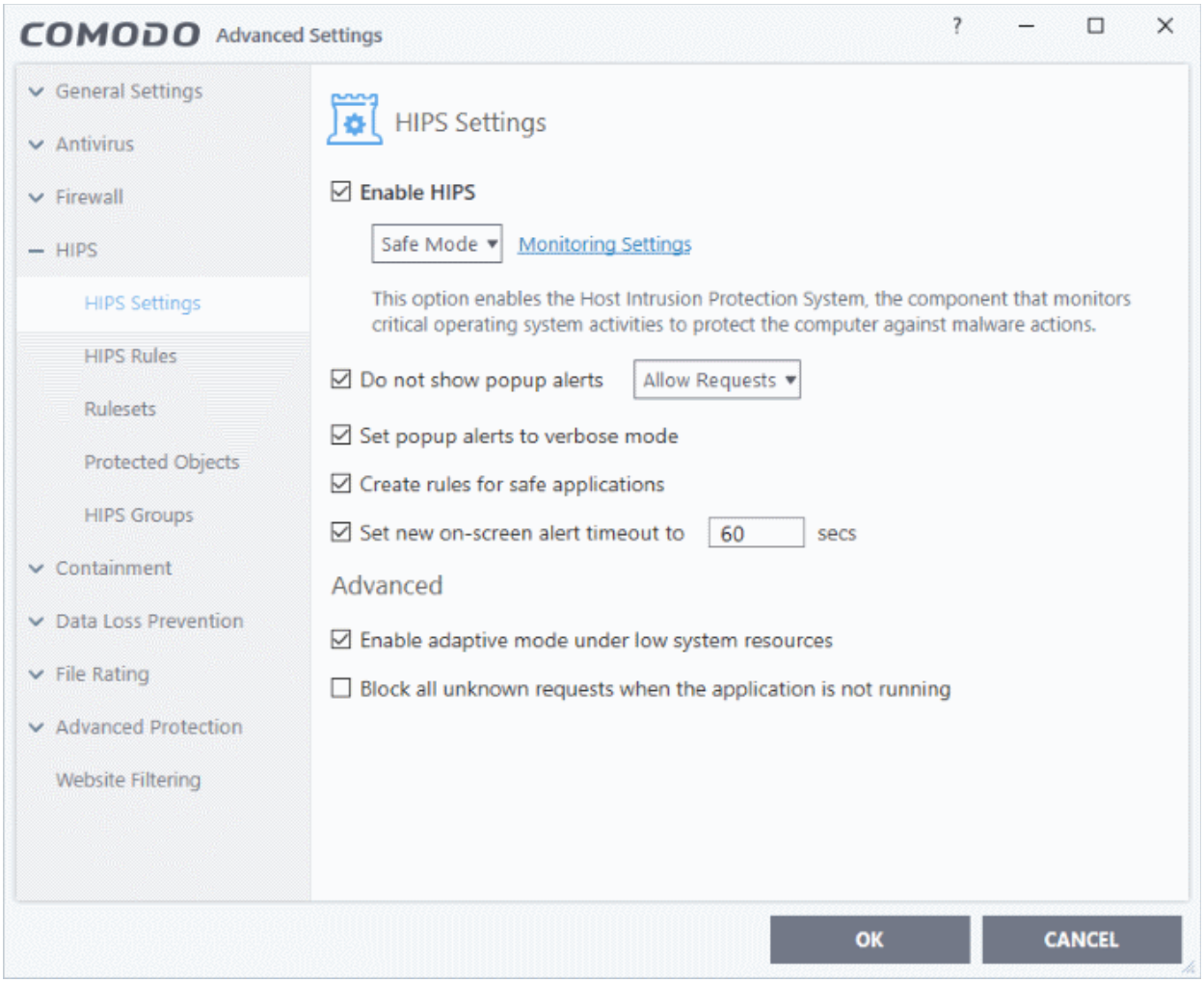
- This section often refers to 'executables' (or 'executable files'). An executable is a file that can instruct your computer to perform a task or function.
- Every program, application and device you run on your computer requires an executable file of some kind to start it.
- The most recognizable type of executable file is the '.exe' file. For example, 'winword.exe' is the name of the executable that instructs your computer to start and run Microsoft Word. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.
- Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data, steal your identity, corrupt system files, hand control of your PC to a hacker and more. You may also have heard these referred to as Trojans, scripts and worms.

7.4.1. HIPS Settings

- Click 'Settings' > 'HIPS' > 'HIPS Settings'
- HIPS settings let you enable/disable HIPS, set HIPS security level, and configure the general behavior of the HIPS module.

Open the 'HIPS Settings' panel

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'HIPS Settings'

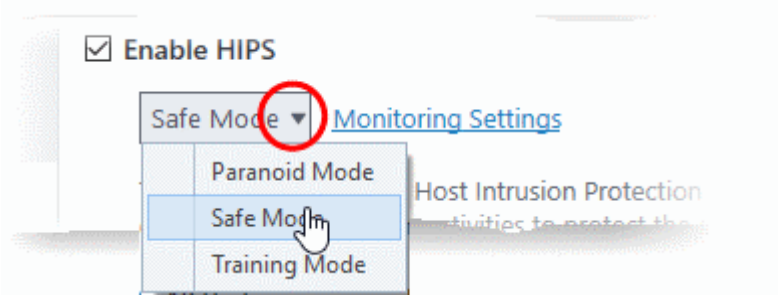


- **Enable HIPS** - Activate or deactivate the HIPS protection. (***Default=Disabled***)

If enabled, you can configure the HIPS security level and monitoring settings:

Configure HIPS Security Level

- Choose the security level from the drop-down under the 'Enable HIPS' check-box:



The choices available are:

- **Paranoid Mode**: This is the highest security level setting and means that HIPS monitors and controls all executable files apart from those that you have deemed safe. Comodo Client Security does not attempt to learn the behavior of any applications - even those applications on the safe list and only uses *your* configuration settings to filter critical system activity. Similarly, CCS does not automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their system.
- **Safe Mode**: While monitoring critical system activity, HIPS automatically learns the activity of executables

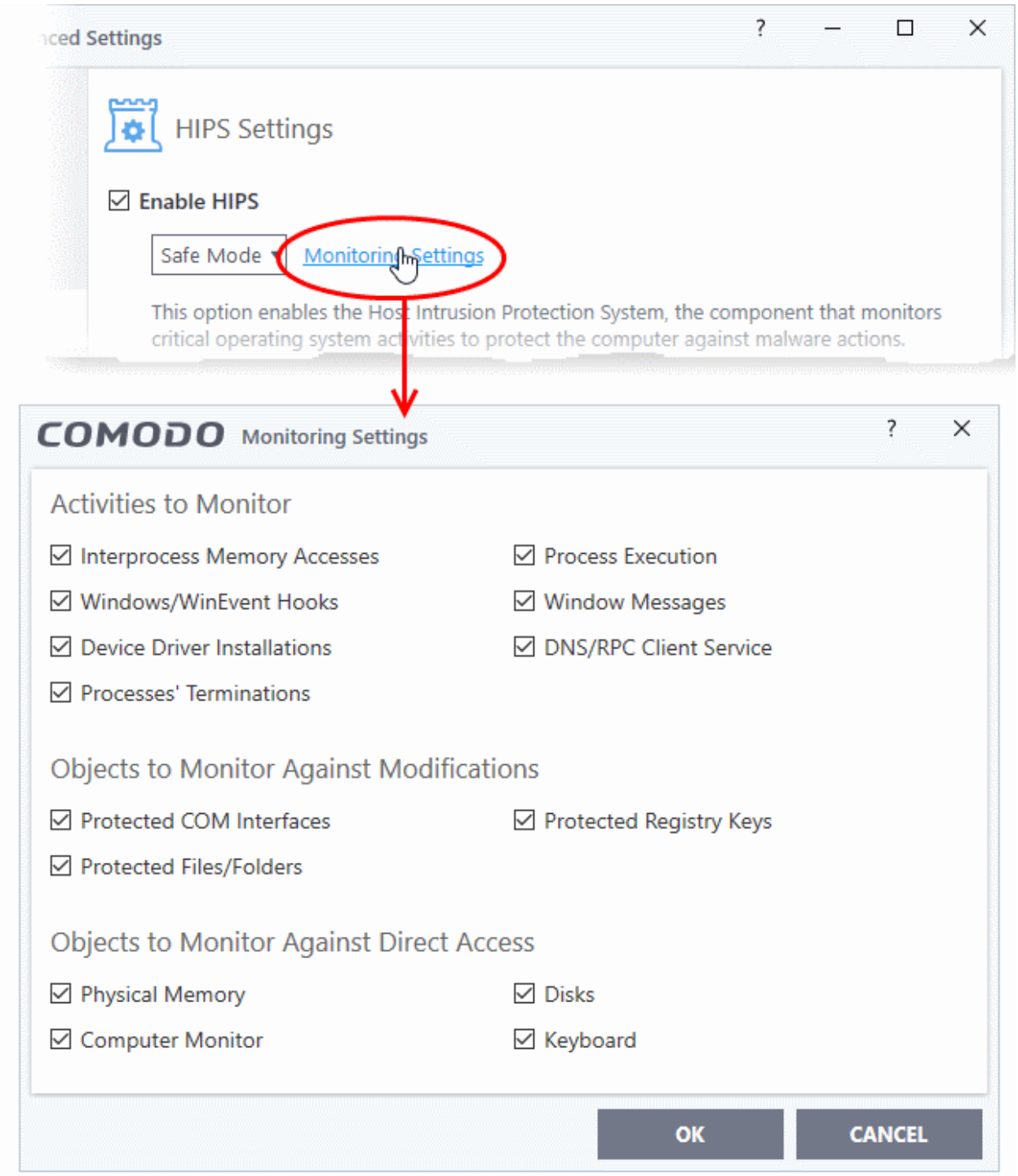
and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules for these activities, if the checkbox '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the HIPS rules list by choosing 'Treat as' and selecting 'Allowed Application' at the alert with 'Remember my answer' checked. This instructs the HIPS not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.

- **Training Mode**: HIPS monitors and learns the activity of any and all executables and creates automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

Configure Monitoring Settings

- Click the Monitoring Settings link to select the activities and objects that should be monitored by HIPS

Note: The settings you choose here are universally applied. If you disable monitoring of an activity or object here, it completely switches off monitoring of that activity on a ***global*** basis - effectively creating a universal '*Allow*' rule for the activity. This 'Allow' setting ***over-rules*** any specific 'Block' or 'Ask' setting for the activity that you may have created in the '**Access Rights**' and '**Protection Settings**' interfaces.



Activities To Monitor:

- **Interprocess Memory Access -** Malware programs use memory space modification to inject malicious code for numerous types of attacks. These include recording your keyboard strokes; modifying the behavior of applications and stealing data by sending confidential information from one process to another. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of a compromised process to 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application ***(Default = Enabled)***.
- **Windows/WinEvent Hooks -** In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events *before* they reach an application. Example intercepted events include messages, mouse actions and keystrokes. Hooks can react to these events and, in some cases, modify or

discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer and take remote control of your computer. Leaving this box checked means that you are warned every time a hook is executed by an untrusted application ***(Default = Enabled)***.

- **Device Driver Installations -** Device drivers are small programs that allow applications and/or operating systems to interact with hardware devices on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable damage to your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application ***(Default = Enabled)***.
- **Processes' Terminations -** A process is a running instance of a program. (for example, the Open VPN GUI process is called 'openvpn.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your system). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, HIPS monitors and alerts you to all attempts by an untrusted application to close down another application ***(Default = Enabled)***.
- **Process Execution** - Malware such as rootkits and key-loggers often execute as background processes. With this setting enabled, HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. ***(Default = Enabled)***.
- **Windows Messages -** This setting means Comodo Client Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) ***(Default = Enabled)***.
- **DNS/RPC Client Service -** This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service (DDoS) attack whereby a malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed so that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' PCs which are sending out these requests without their owners' knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack ***(Default = Enabled)***.

Background Note: DNS stands for Domain Name System. It is the part of the internet infrastructure that matches a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the internet routes messages to their destinations using these IP addresses, not the domain name you type into your browser. Whenever you enter a domain name, your internet browser contacts a DNS server and makes a 'DNS Query'. In simple terms, this query is 'What is the IP address of example.com?'. The DNS server replies to your browser, telling it to connect to the IP in question.

Objects To Monitor Against Modifications:

- **Protected COM Interfaces** - HIPS monitors the COM interfaces you specified from the **COM Protection** pane. ***(Default = Enabled)***
- **Protected Registry Keys -** HIPS monitors the Registry keys you specified from the **Registry Protection** pane. ***(Default = Enabled)***.
- **Protected Files/Folders** - HIPS monitors the files and folders you specified from the **File Protection** pane. ***(Default = Enabled)***.

Objects To Monitor Against Direct Access:

- Whether or not Comodo Client Security should monitor access to system critical objects on your computer. Using direct access methods, malicious applications can obtain data from storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these

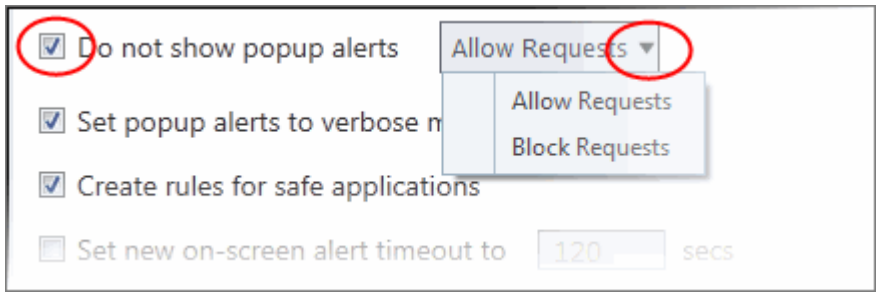
settings enabled:

- **Physical Memory:** Monitors your computer's memory for direct access by applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code ***(Default = Enabled)***.
- **Computer Monitor:** Comodo Client Security raises an alert every time a process tries to directly access your computer monitor. Although legitimate applications sometimes require this access, spyware can also use such access to take screen shots of your current desktop, record your browsing activities and more. ***(Default = Enabled).***
- **Disks:** Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data ***(Default = Enabled)***.
- **Keyboard:** Monitors your keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Client Security alerts you every time an application attempts to establish direct access to your keyboard ***(Default = Enabled)***.

Checkbox Options

- **Do not show popup alerts** - Whether or not you want to be notified when the HIPS encounters malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness ***(Default = Disabled).***

  If you choose not to show alerts then you have a choice of default responses that CCS should automatically take - either 'Block Requests' or 'Allow Requests'.



- **Set popup alerts to verbose mode** - HIPS alerts provide more information and options for the user to allow or block the requests ***(Default = Disabled).***
- **Create rules for safe applications** - HIPS trusts applications if:
  - The application is on the safe list, a global white-list of trusted software.
  - The application has a 'Trusted' rating in the local file list. See **File List** if you need more details.
  - The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file. See **Vendor List** if you need more details.

  By default, CCS does not automatically create 'allow' rules for safe applications. This helps to reduce resource usage, to simplify the rules interface by reducing the number of 'Allow' rules, and can reduce the number of pop-up alerts. Enabling this option instructs CCS to begin learning the behavior of safe applications so that it can automatically generate 'Allow' rules. These rules are listed in the **HIPS Rules** interface. Advanced users can edit / modify the rules as they wish.
- **Set new on-screen alert time out to**: How long a HIPS alert remains on-screen if it is not answered. The default timeout is 120 seconds. You may adjust this setting to your own preference.

Advanced HIPS Settings

Note: These settings are recommended for advanced users only.

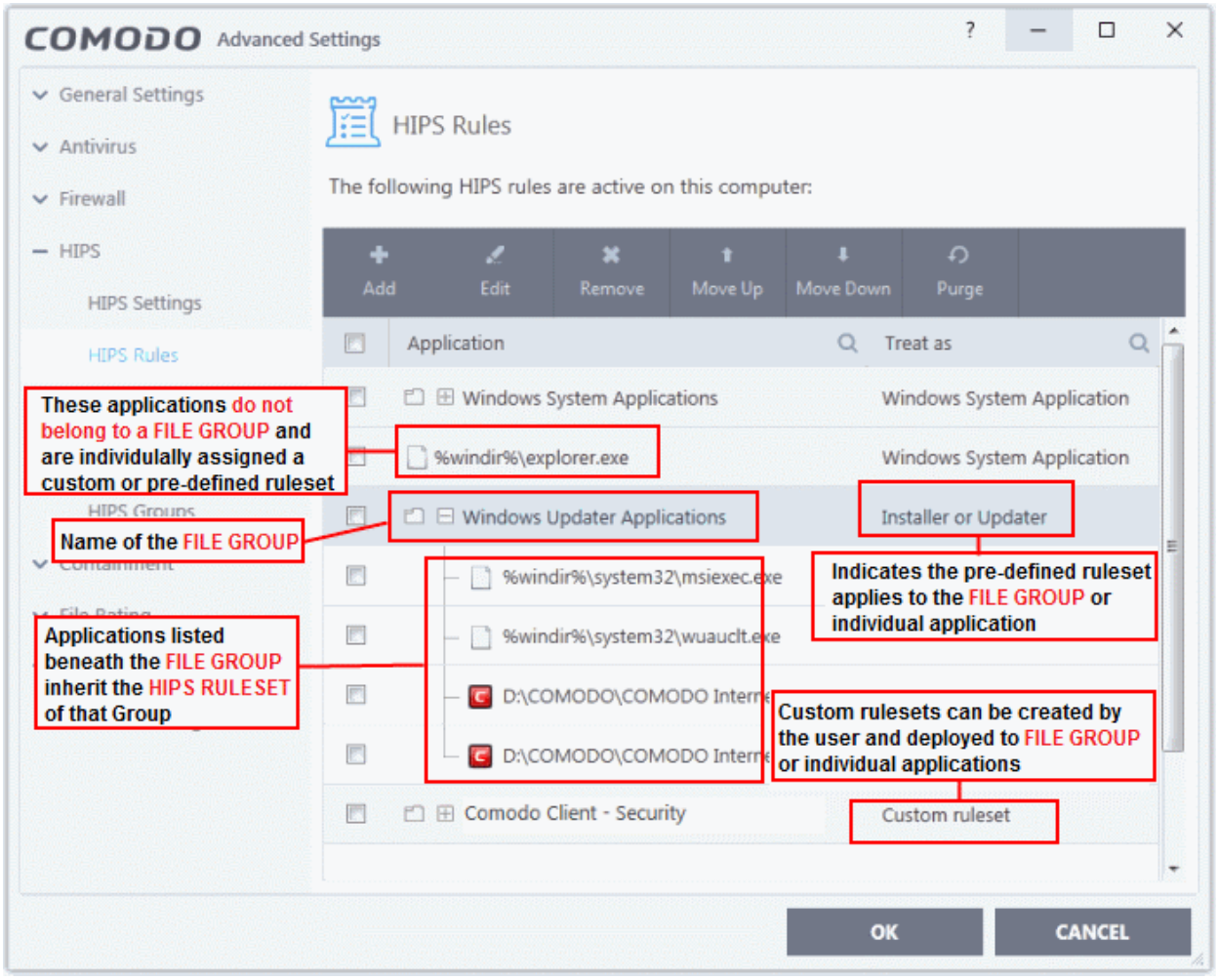
- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CCS functions to fail. With this option enabled, CCS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, enabling this option may reduce performance in even lightly loaded systems ***(Default = Disabled)***.
- **Block all unknown requests if the application is not running** - Prohibits execution of unknown applications if CCS 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)***

7.4.2. Active HIPS Rules

- Click 'Settings' > 'HIPS' > 'HIPS Rules'
- The rules screen shows your installed applications classified into file groups, and the HIPS ruleset that applies to them.
- You can change the ruleset of a specific application or file group, and create your own custom rulesets.

Open the 'HIPS Rules' panel

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'HIPS Rules'

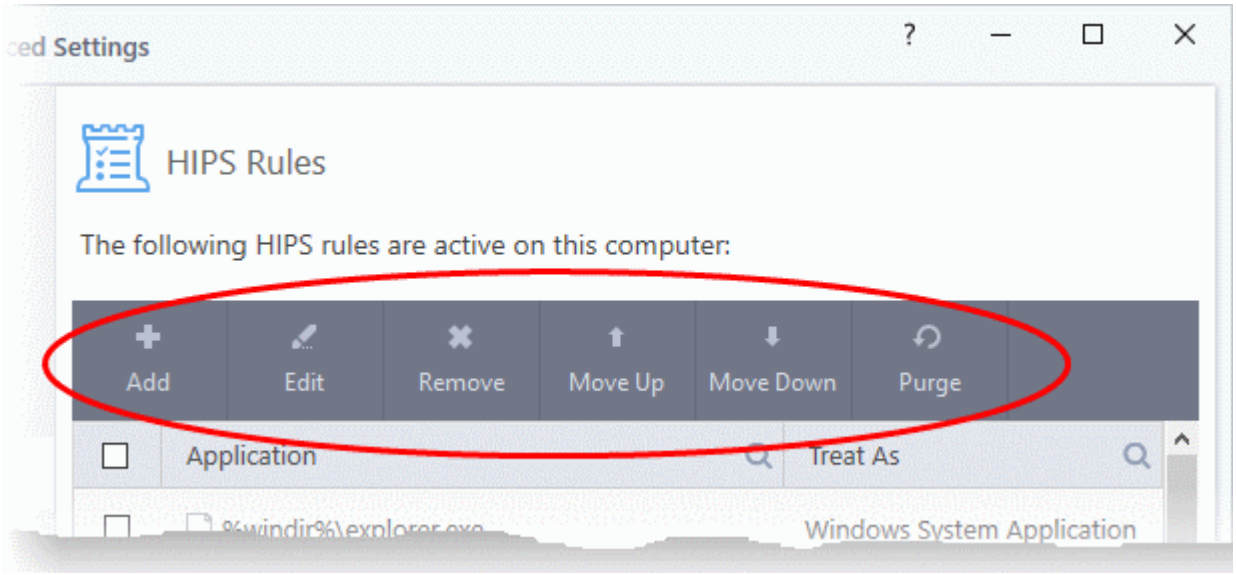


The first column, **Application**, displays a list of the applications on your system for which a HIPS ruleset has been defined. If the application belongs to a file group, then all member applications assume the ruleset of the group. The second column, **Treat As**, displays the name of the HIPS ruleset assigned to the application or group of applications.

You can use the search option to find a specific file in the list by clicking the search icon at the far right of the column header and entering the name in full or part.

General Navigation:

The control buttons at the top of the list enable you to create and manage application rule sets.



- **Add** - Allows the user to add a new application to the list and then create its ruleset. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **Remove** - Deletes the selected ruleset.

Note: You cannot add or remove individual applications from a file group using this interface - you must use the '**File Groups**' interface to do this.

- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move UP/Move Down** - Users can re-order the priority of rules by simply selecting an application name or file group and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the '**File Groups**' interface.

Creating or Modifying a HIPS Ruleset

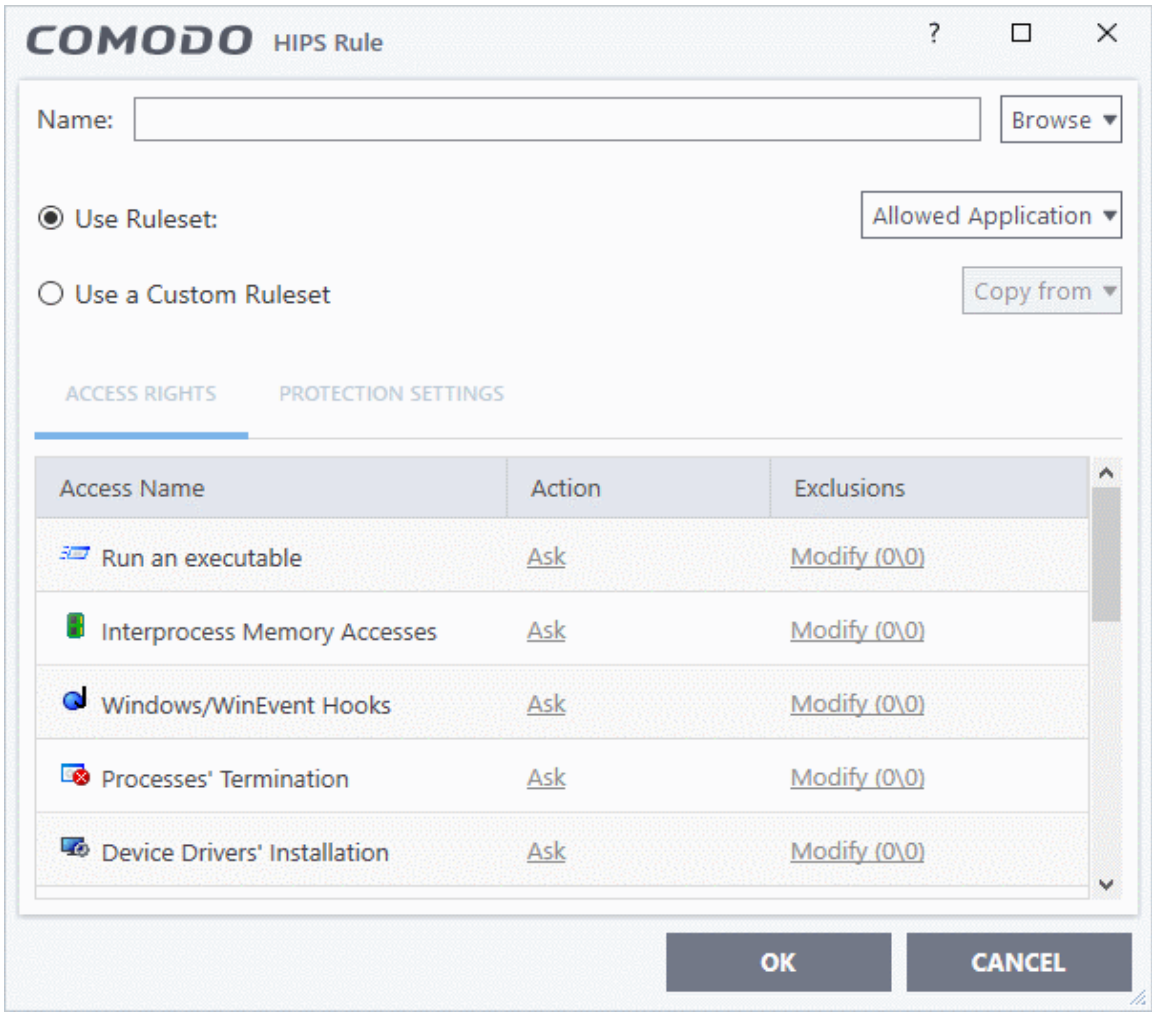
Defining a HIPS Ruleset for an application or File group involves two steps:

1. **Select the application or file group that you wish the ruleset to apply to.**
2. **Configure the ruleset for this application.**

Step 1 - Select the application or file group that you wish the ruleset to apply to

- To define a rule for a new application (i.e. one that is not already listed), click the 'Add' button at the top of the **HIPS Rules pane**.

This brings up the 'HIPS Rule' interface as shown below.

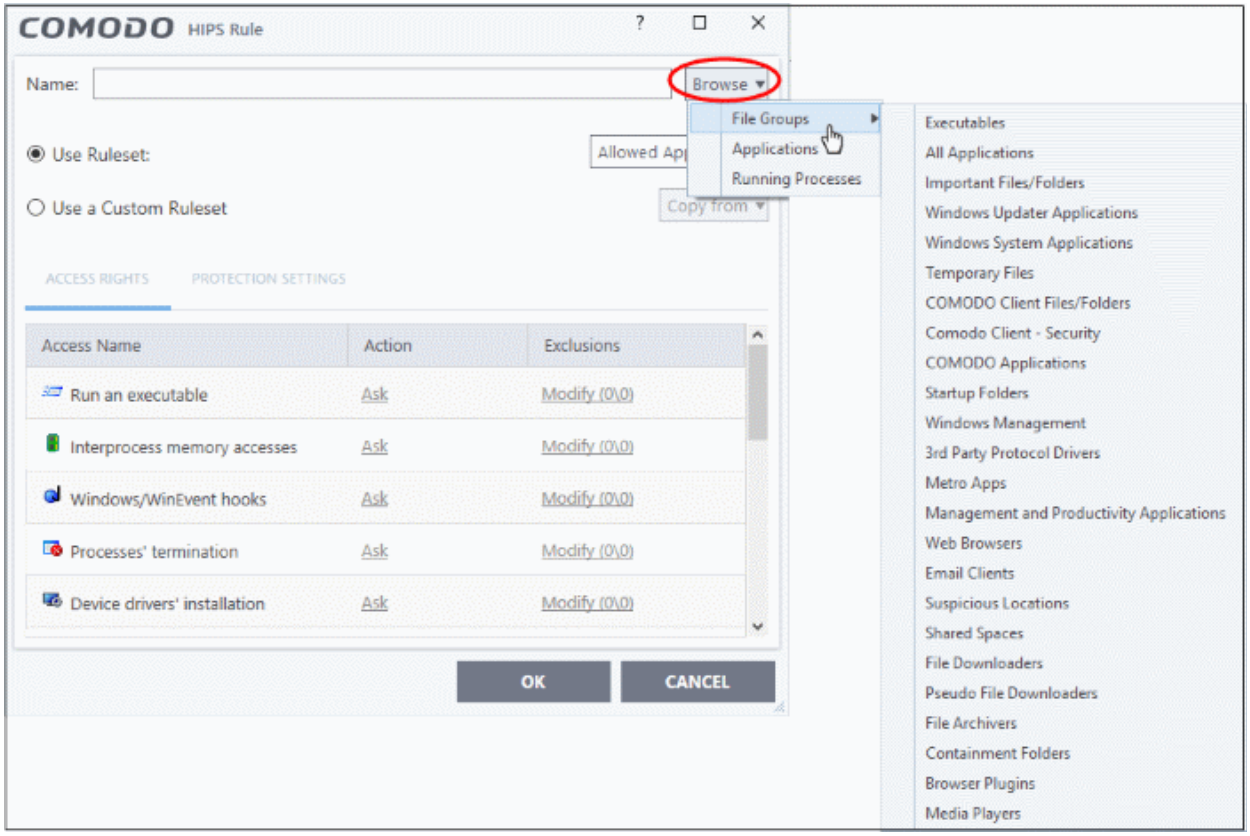


The 'Name' box is blank because you are defining a HIPS rule settings for a new application. If you were editing an existing rule, this field would show the application name and its installation path, or the application group name.

- Click 'Browse' to begin.

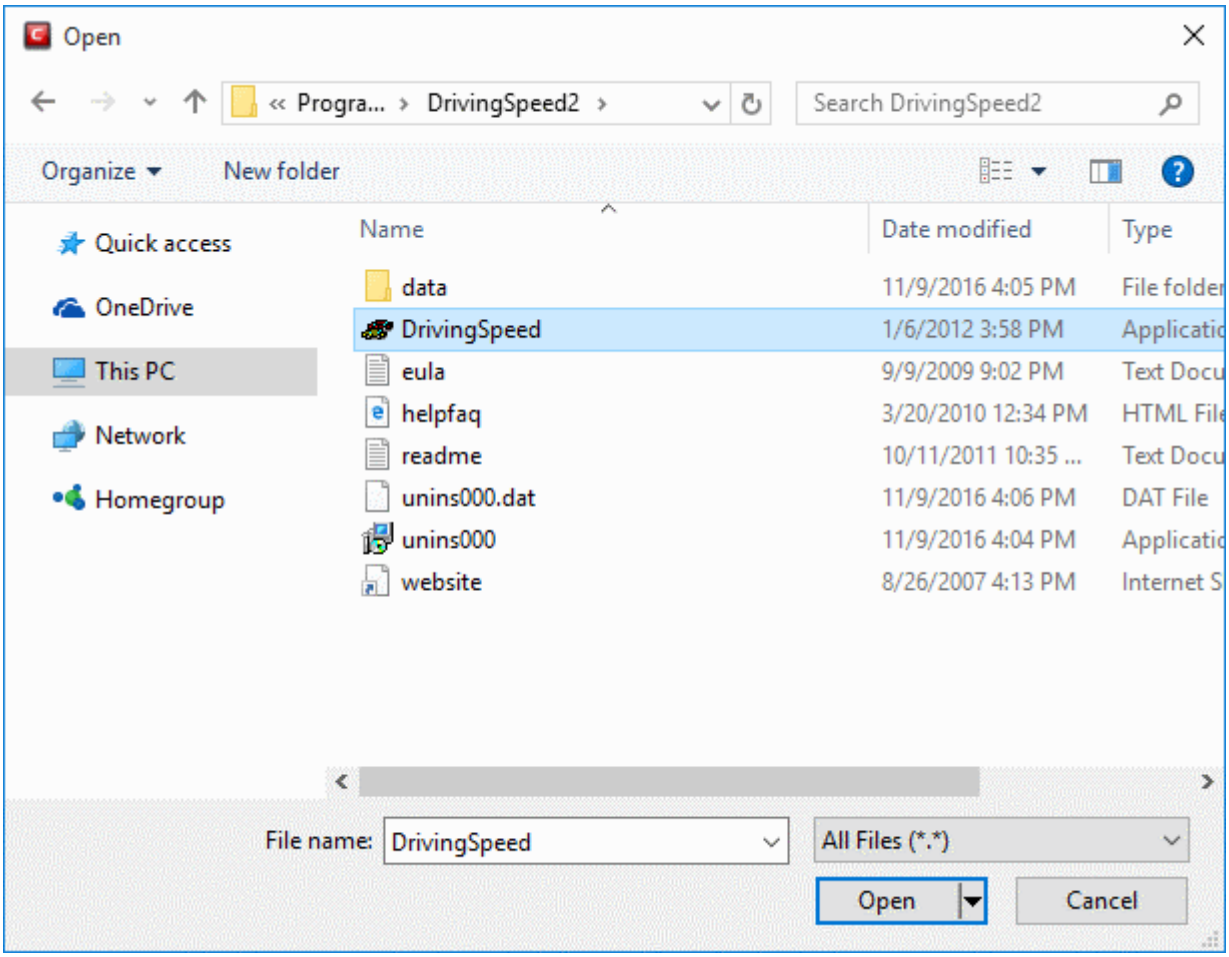
You now have 3 methods available to choose the application for which you wish to create a Ruleset - **File Groups**; **Applications** and **Running Processes**.

1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl *\cmd.exe, *.bat, *.cmd. Other such categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

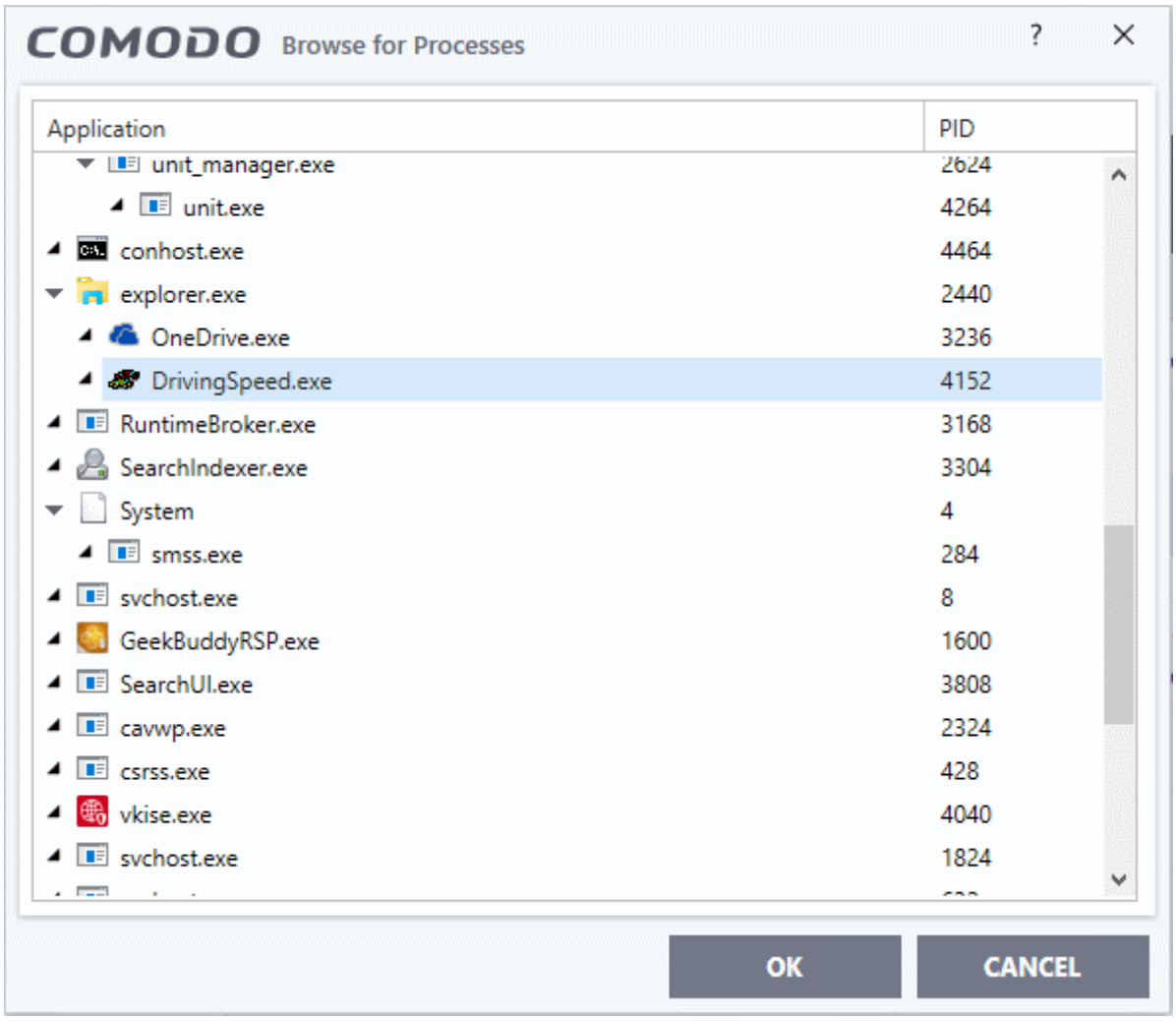


To view the file types and folders that are affected by choosing one of these options, you need to visit the '**File Groups**' interface.

2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.



3. **Running Processes** - as the name suggests, this option allows you choose any process that is currently running on your PC in order to create and deploy a ruleset for its parent application.

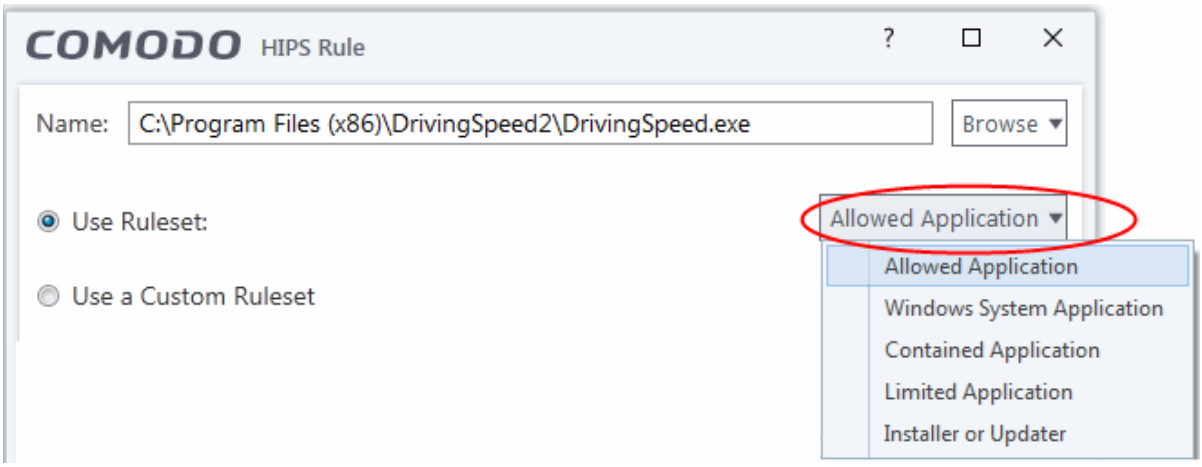


Having selected the individual application, running process or file group, the next stage is to configure the rules for this ruleset.

Step 2 - Configure the HIPS Ruleset for this application

There are two broad options available for selecting a ruleset that applies to an application - **Use Ruleset** or **Use a Custom Ruleset**.

1. **Use Ruleset** - Selecting this option allows you to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the **HIPS Rules** interface ***(Default = Enabled).***



Note on 'Installer or Updater' Rule: Applying this rule to an application defines it as a trusted installer. All files created by this application will also be trusted. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo advises you to use this 'Predefined Ruleset' - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.

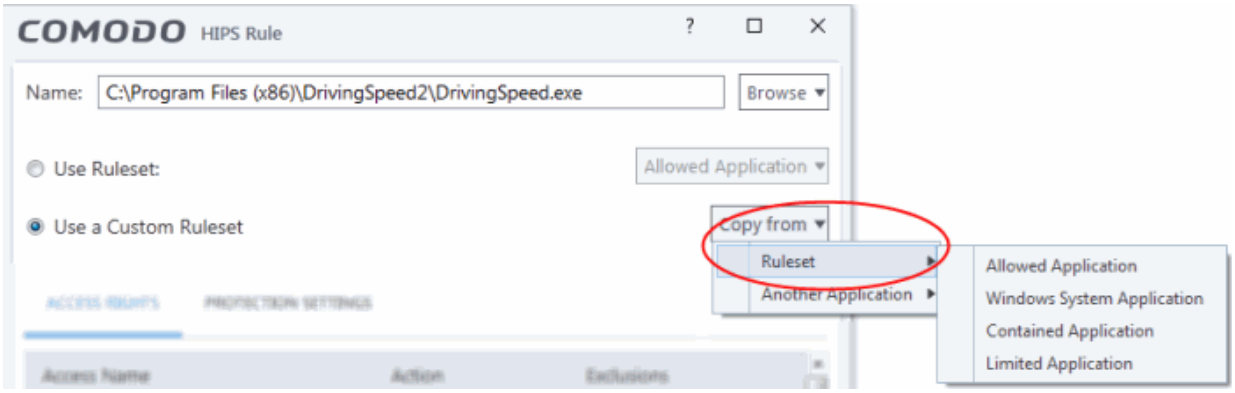
General Note: Predefined Rulesets cannot be modified directly from this interface - they can only be modified and defined using the '**Rulesets**' interface. If you require the ability to add or modify settings for a specific application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use a Custom Ruleset** option instead.

2. **Use a Custom Ruleset** - Designed for more experienced users, the 'Custom Ruleset' option grants full control over the configuration of each rule within that ruleset.

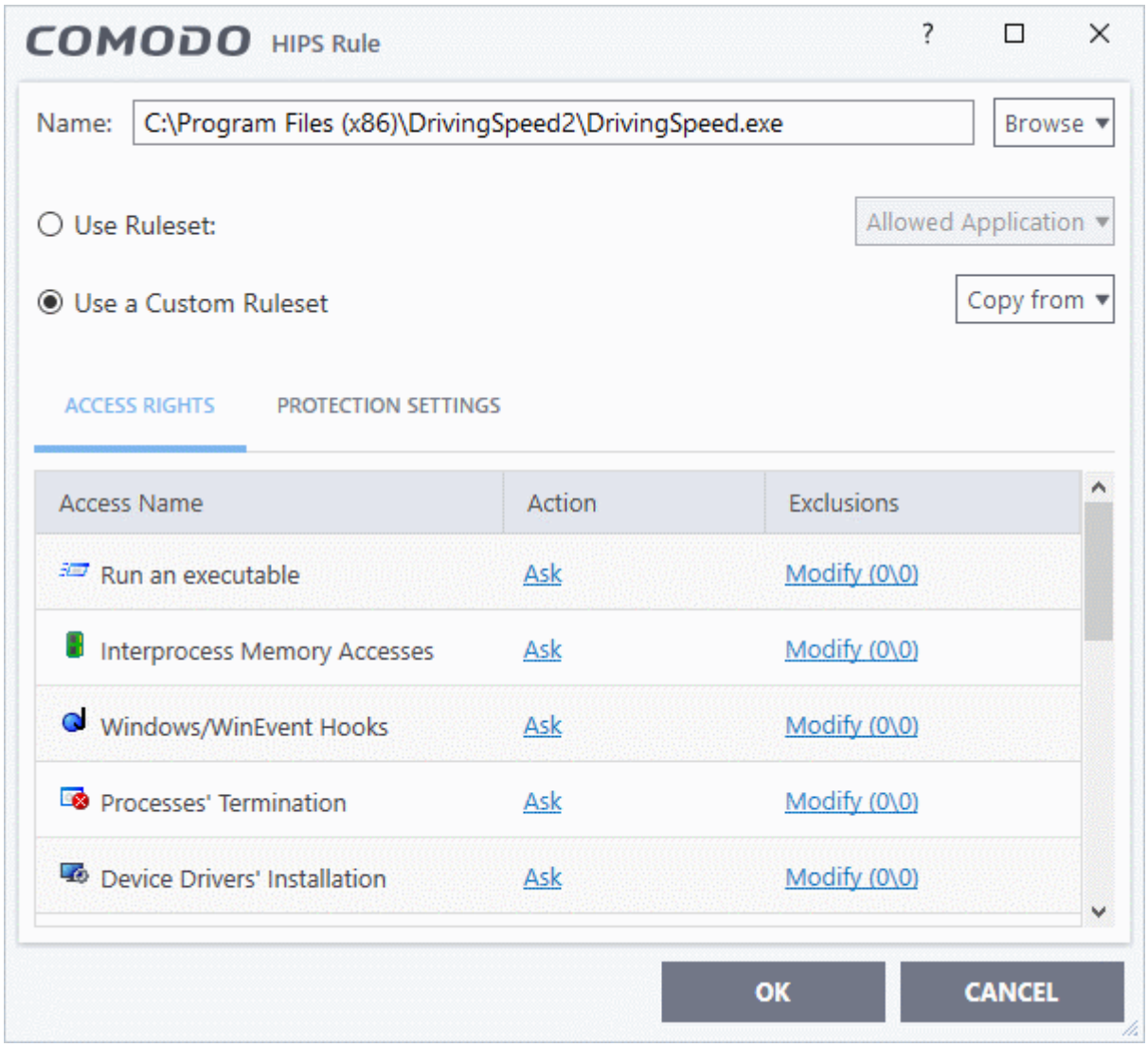
   The custom ruleset has two main configuration areas - **Access Rights** and **Protection Settings**.

   In simplistic terms 'Access Rights' determine what the application *can do to other processes* and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

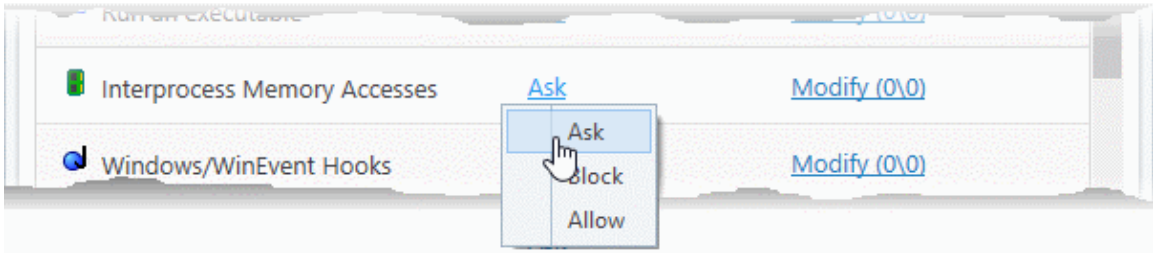
Tip: You can use the 'Copy from' drop-down to choose an existing rule set for an application or file group. Using that as a starting point, you can customize the 'Access Rights' and 'Protection Settings' for the rules as required.



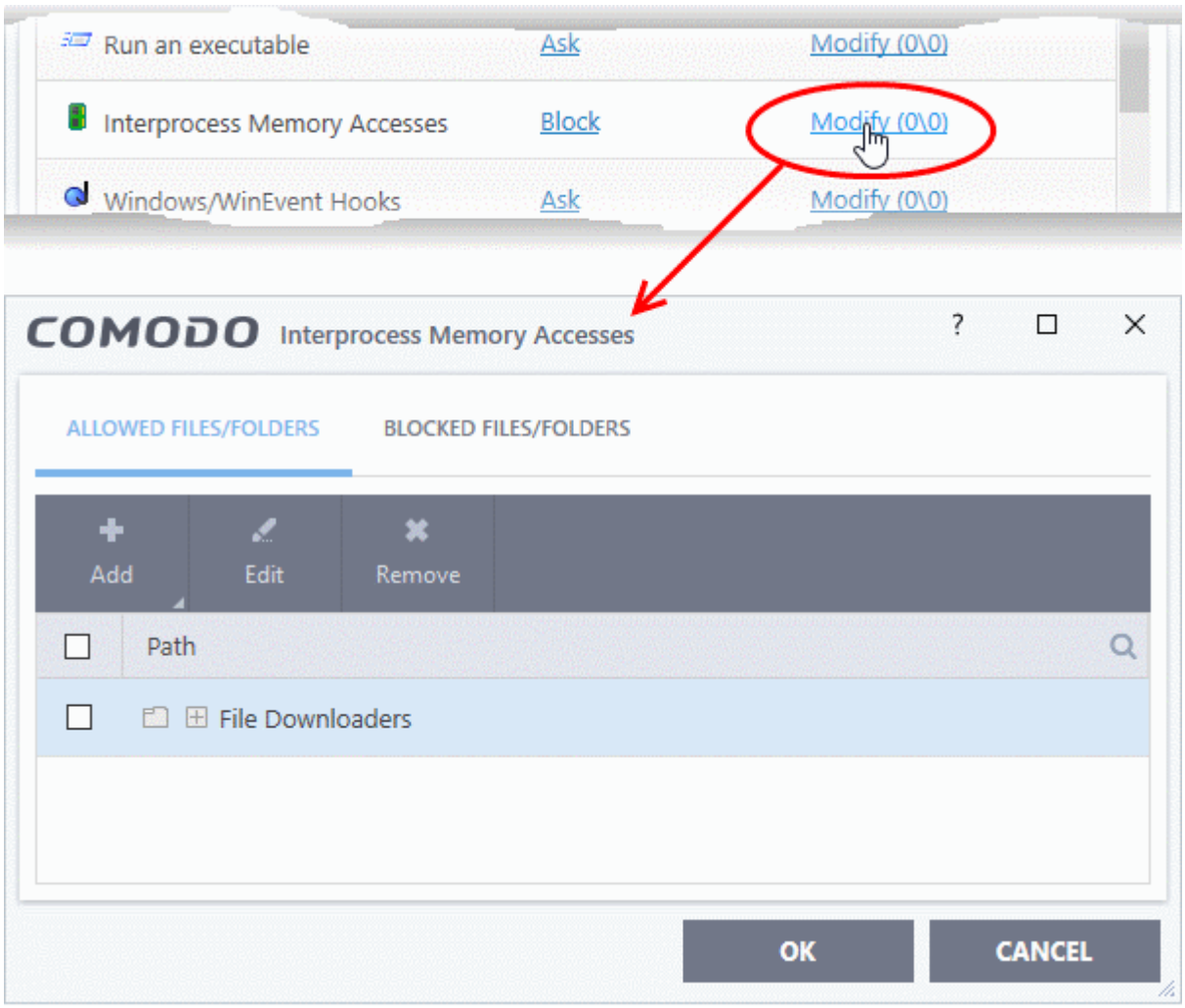
   i. **Access Rights** - The 'Process Access Rights' area allows you to determine what activities can be performed by the applications in your custom ruleset. These activities are called 'Access Names'.



See **HIPS Settings > Activities to Monitor** to see definitions of the 'Action Names' listed above, and the implications of choosing 'Ask', 'Allow' or 'Block':



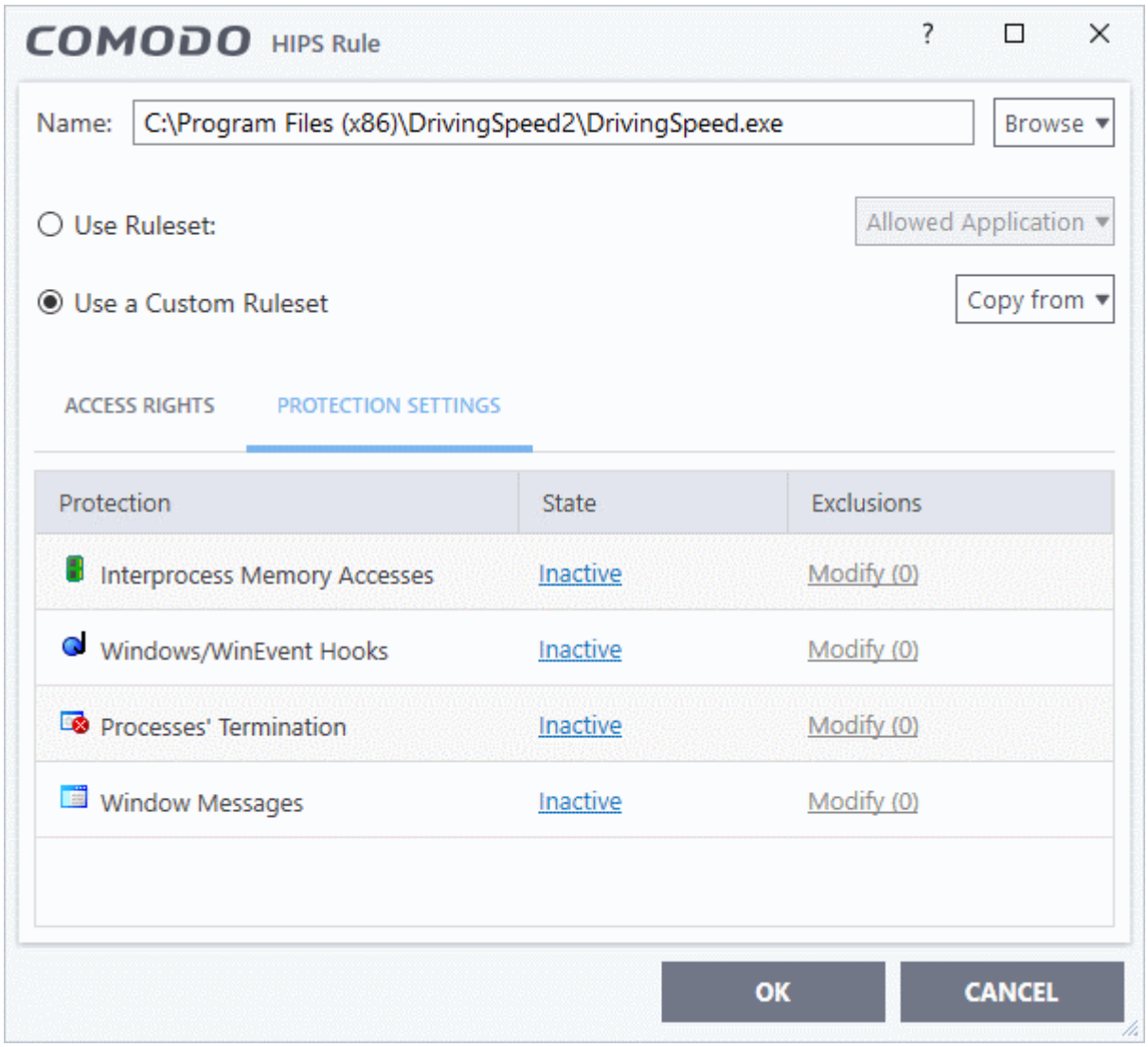
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Files/Folders' or 'Blocked Files/Folders' tab depending on the type of exception you wish to create.



Clicking the 'Add' button at the top allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

In **the example above**, the default action for 'Interprocess Memory Access' is 'Block'. This means HIPS will block the action if 'DrivingSpeed.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'File Downloaders' File Group to the 'Allowed Files\Folders' area creates an exception to this rule. 'DrivingSpeed.exe' can now modify the memory space of files belonging to the 'File Downloaders' File Group.

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



- Set the 'State' as 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

7.4.3. HIPS Rule Sets

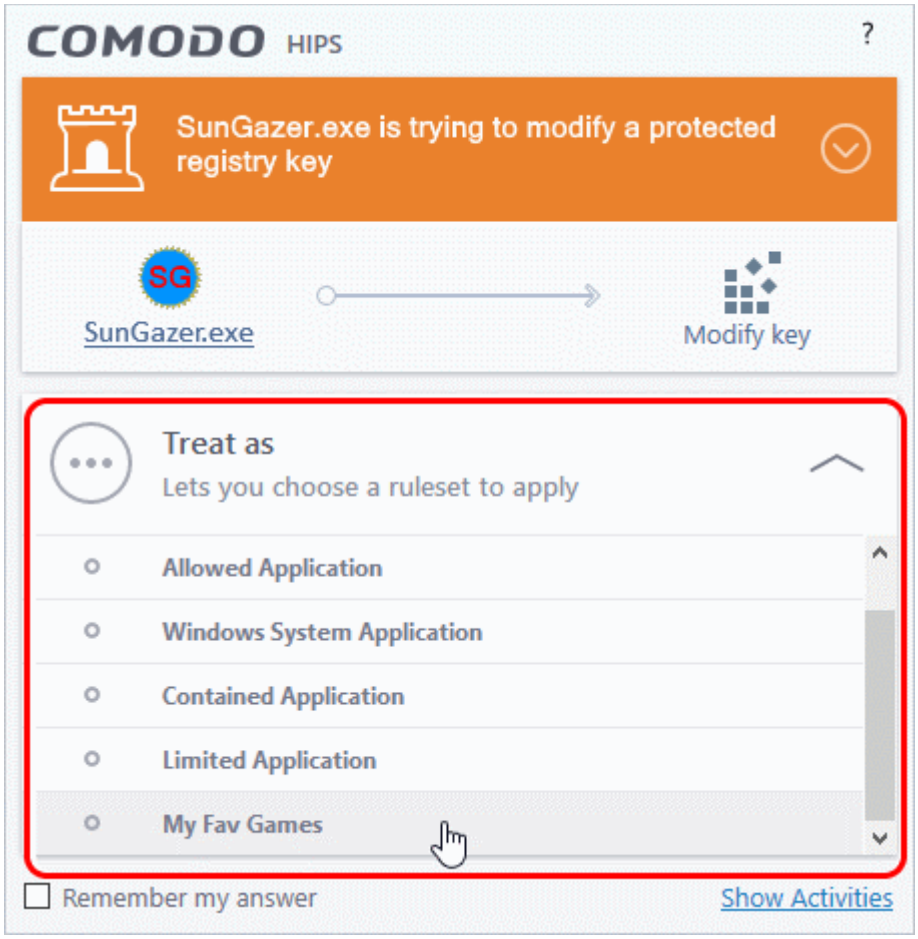
- Click 'Settings' > 'HIPS' > 'Rulesets'
- A ruleset is a collection of **access rights and protection settings** that can be applied to applications on your computer.
- Each ruleset consists of a number of rules, and each of these rules is defined by a set of conditions and parameters. Rulesets govern an application's rights to access memory, other programs, the registry etc.
- CCS ships with six predefined rulesets that provide a very high level of protection. You can also create your own.

Note: This section is for advanced users. If you are new CCS user, we advise you first read the **Active HIPS Rules**

section in this help guide.

Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo provide a set of pre-defined rulesets which optimize security on a range of application types.

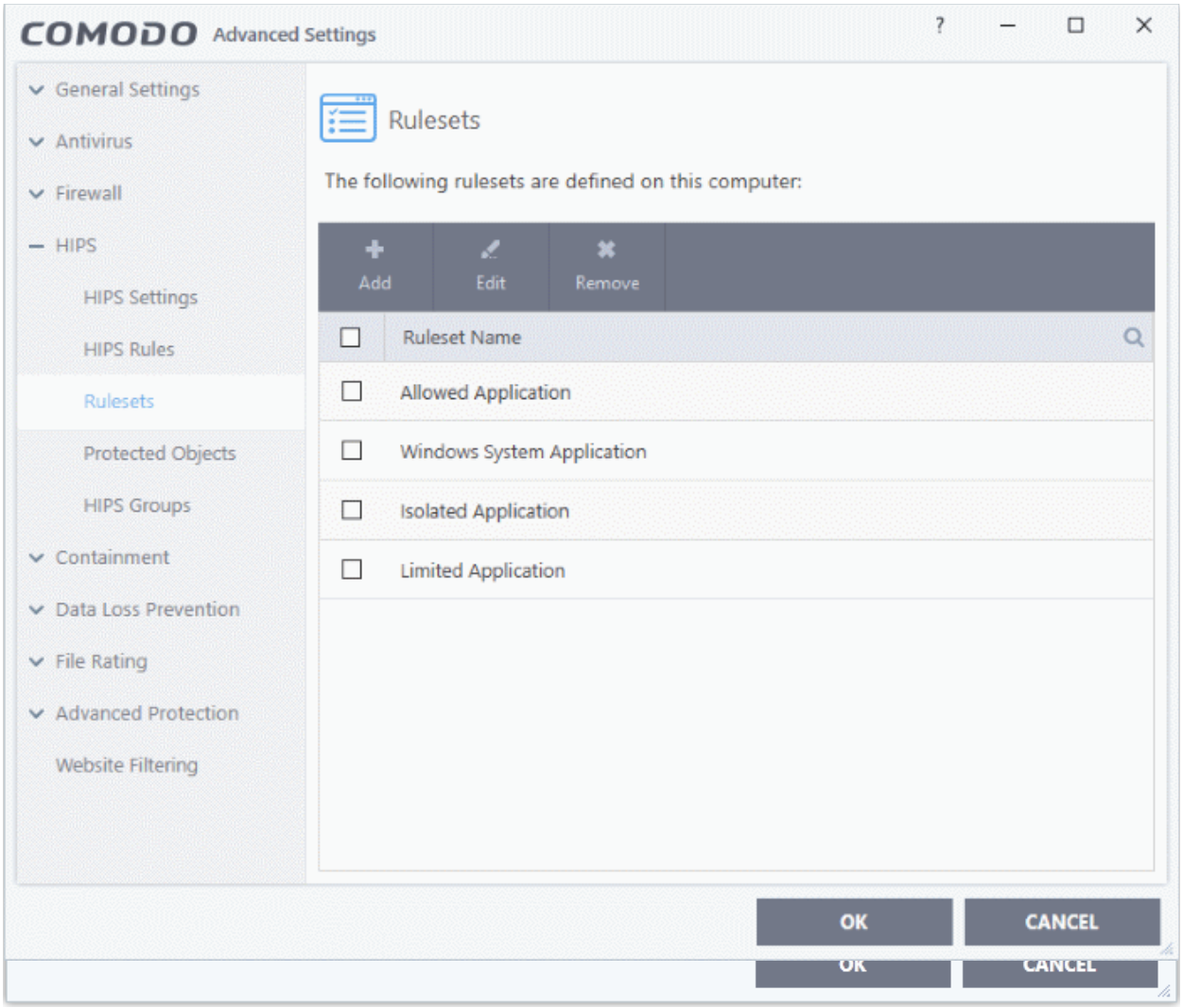
- You can modify these predefined rulesets to suit your requirements.
- You can also create new custom rule sets with your own constituent rules
- You can also apply a HIPS ruleset to an application at a HIPS alert. Both predefined and custom rulesets are made available. An example alert is shown below:



- See **answering HIPS alerts** if you want more help with alerts.

View the list of HIPS Rulesets

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Rulesets'



- Click the search icon and enter the name of a ruleset name in full or part to search for a specific ruleset.

View or edit a ruleset

- Double click on the 'Ruleset' in the list

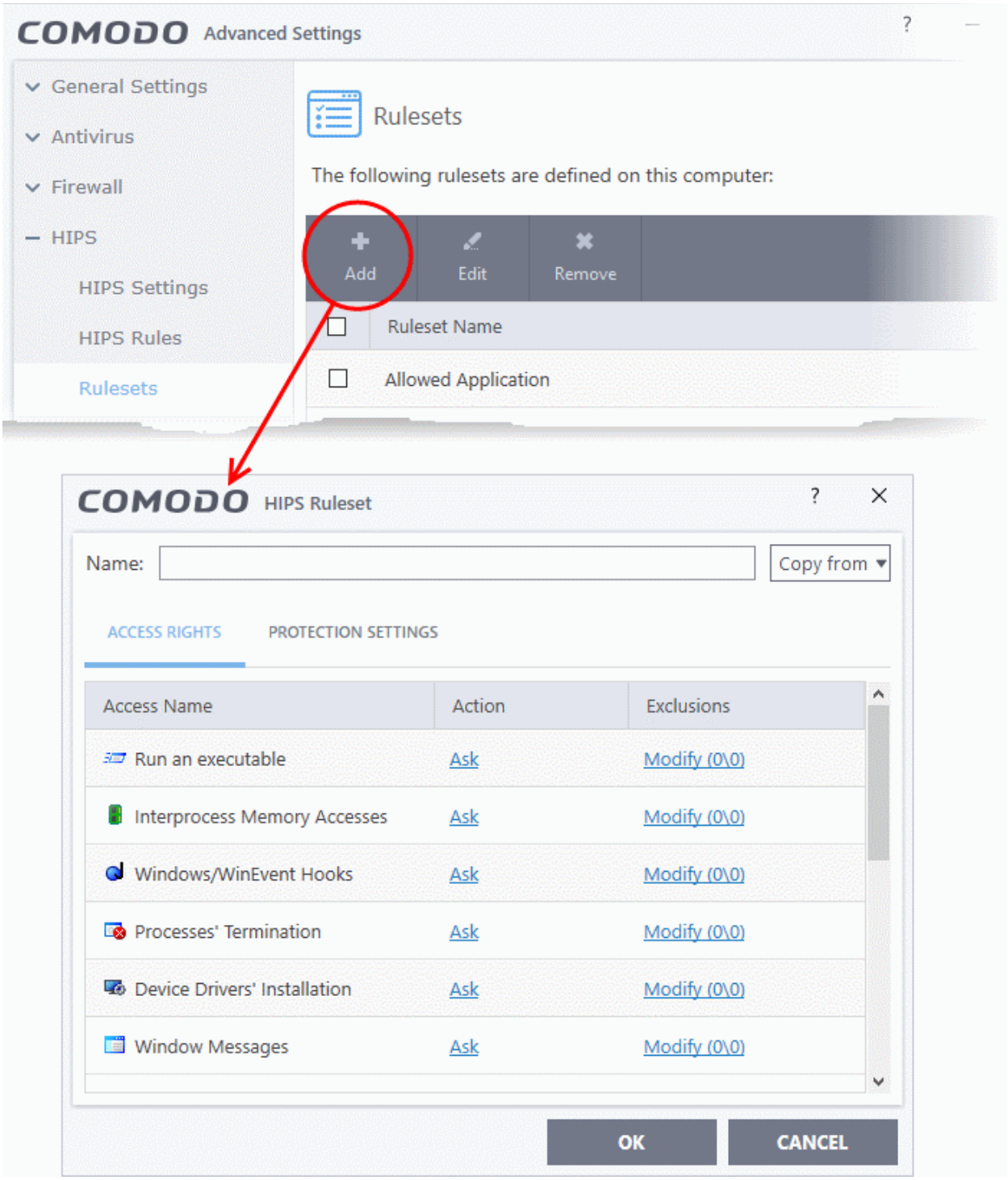
  or

- Select the 'Ruleset' and click the 'Edit' button at the top of the interface

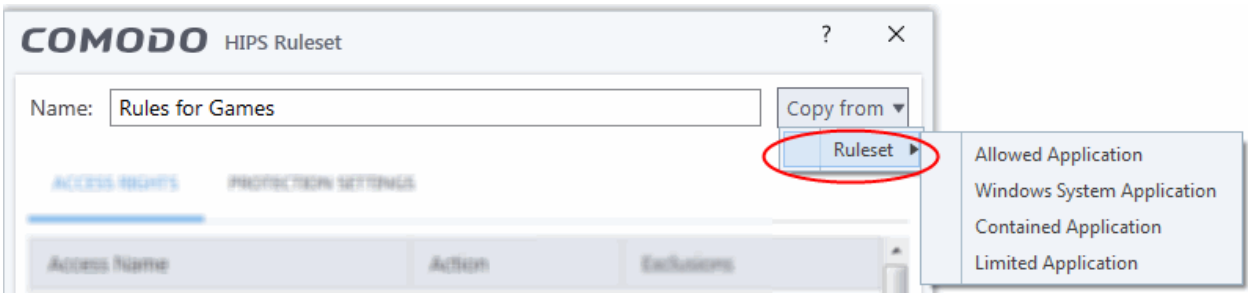
From here, you can make changes to its **'Access Rights' and 'Protection Settings'**. Any changes you make here are automatically rolled out to all applications that are covered by the ruleset.

Create a new ruleset

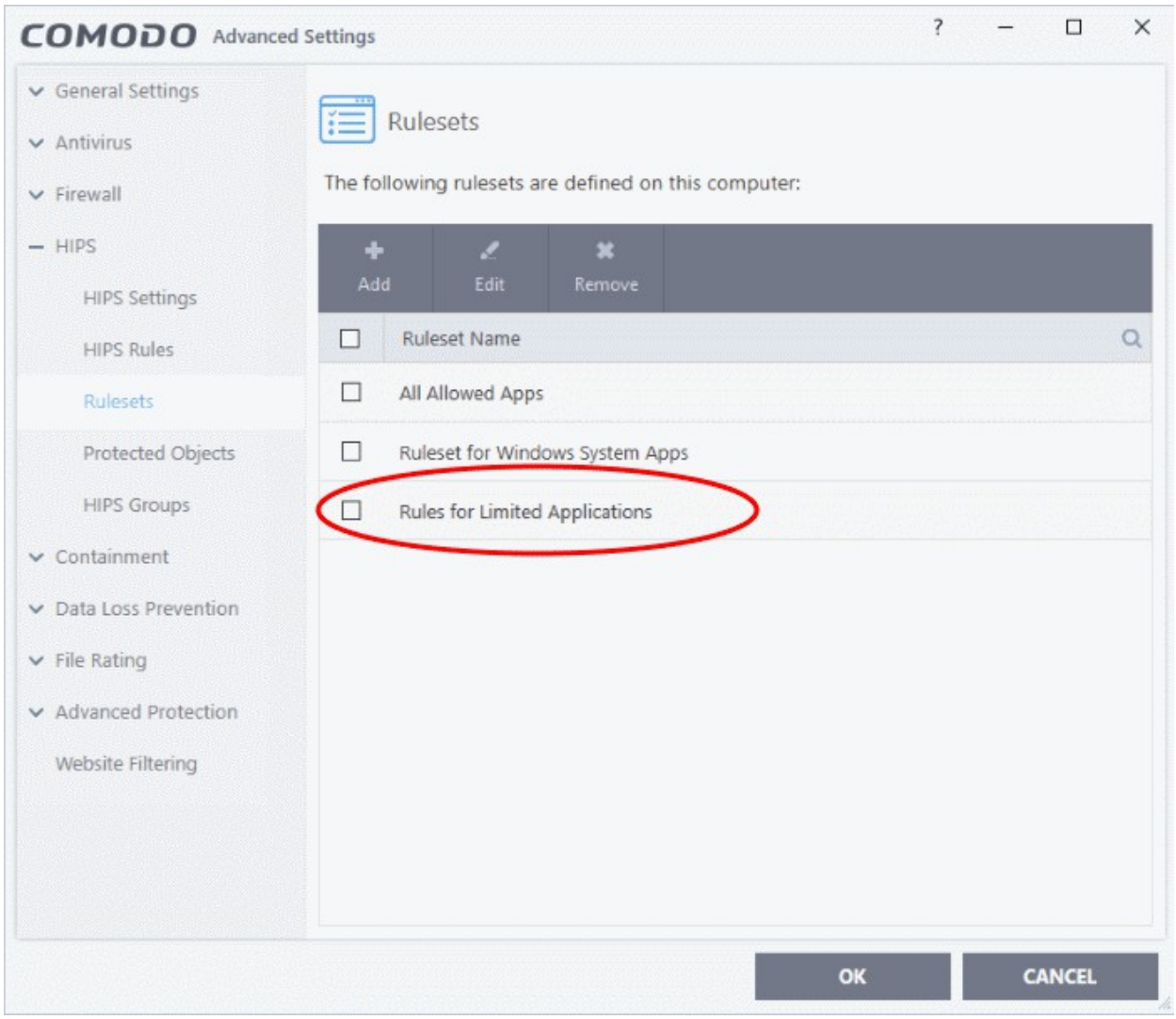
- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Rulesets'
- Click the 'Add' button at the top of the interface



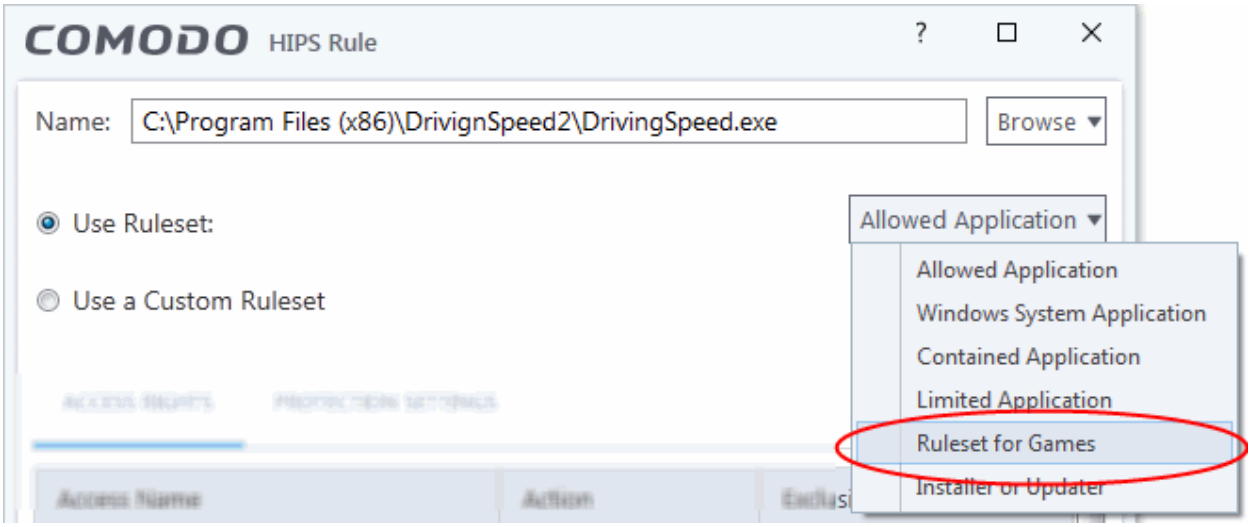
- Enter a name for the new ruleset.
- To copy the **Access Rights** and **Protection Settings** from an existing ruleset, click 'Copy From' and choose the ruleset from the drop-down.



- To customize the **Access Rights** and **Protection Settings** of this new rule set, follow the procedure explained under **Use a Custom Ruleset** in the section **Active HIPS Rules**.
- Click 'OK' to save the new ruleset.



Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.

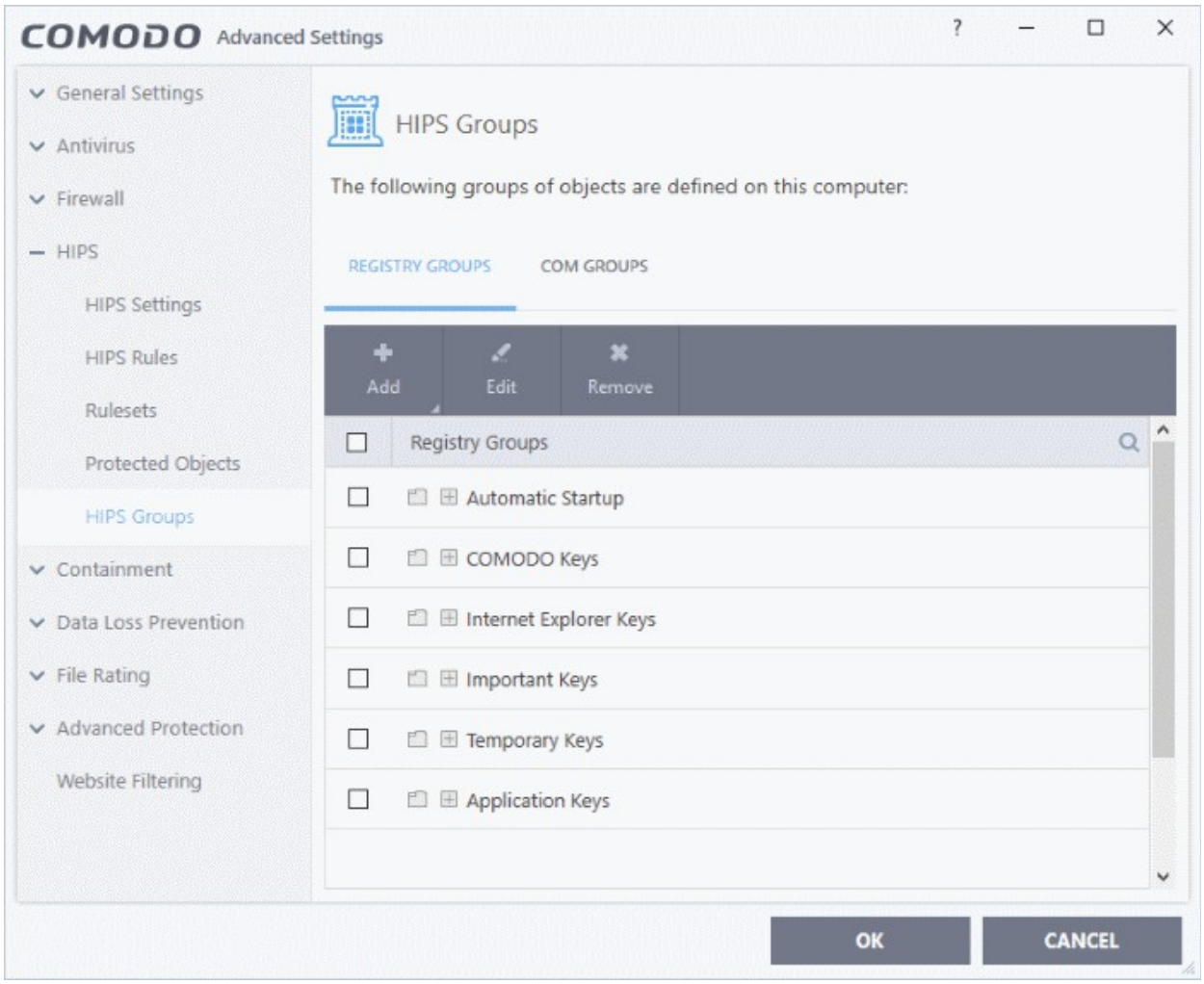


7.4.4. HIPS Groups

- Click 'Settings' > 'HIPS' > 'HIPS Groups'
- HIPS groups are collections of one or more COM interfaces or registry keys.
- After defining a HIPS group, it will be available for selection and protection in the **Registry Keys** and **COM Interfaces**.
- CCS ships with predefined 'Registry' and 'COM' groups, and allows you to add new groups.
- You can view manage all groups in the 'HIPS Groups' interface.

Open the 'HIPS Groups' interface

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left:



- Please note, this area is just where you can view and define the groups. You need to select the group in the **Protected Objects** interface to actually apply the protections.

The panel has two sections:

- **Registry Groups** - View, edit and create groups of registry keys which you want to protect from changes.
- **COM Groups** - View, edit and create groups of COM interfaces which you want to protect from changes.

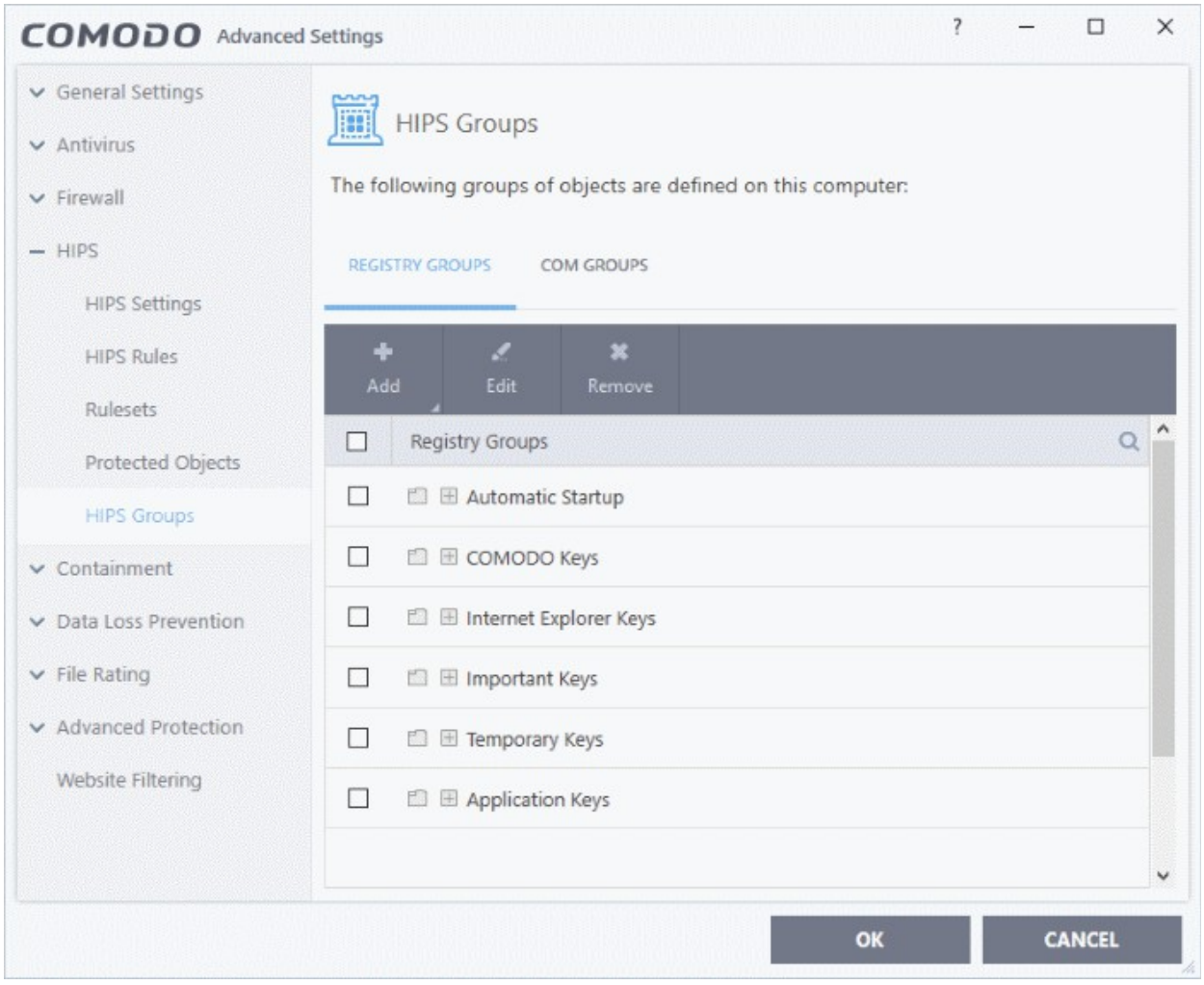
7.4.4.1. Registry Groups

- Click 'Settings' > 'HIPS' > 'HIPS Groups' > 'Registry Groups'

- Registry groups are predefined batches of one or more registry keys.
- Comodo Client Security ships with a set of important registry groups: 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.
- Creating a registry group allows you to quickly add it to the list of protected keys. See '**Protected Registry Keys**' for help with this.

To open the 'Registry Groups' section

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left.
- Click the 'Registry Groups' tab:

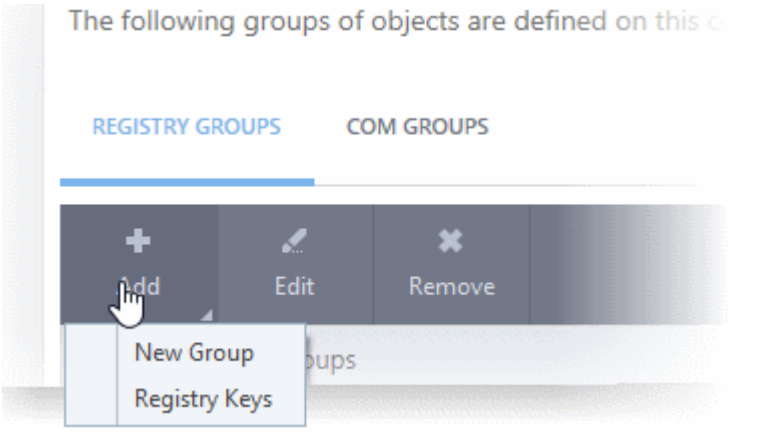


- Click the search icon on the right to find a specific item. You can enter a full or partial name.

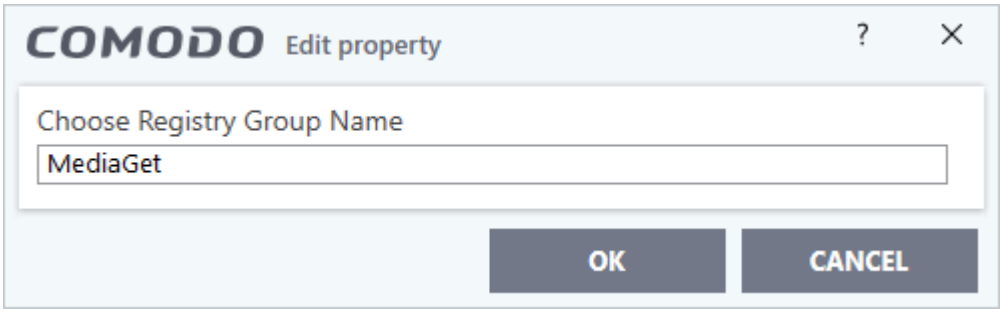
This interface allows you to:

- **Create a new Registry Group**
- **Add Registry key(s) to an existing group**
- **Edit the names of an Existing Registry Group**
- **Remove existing group(s) or individual key(s) from existing group**

- To add a new group or add key(s) to an existing group, click the 'Add' button

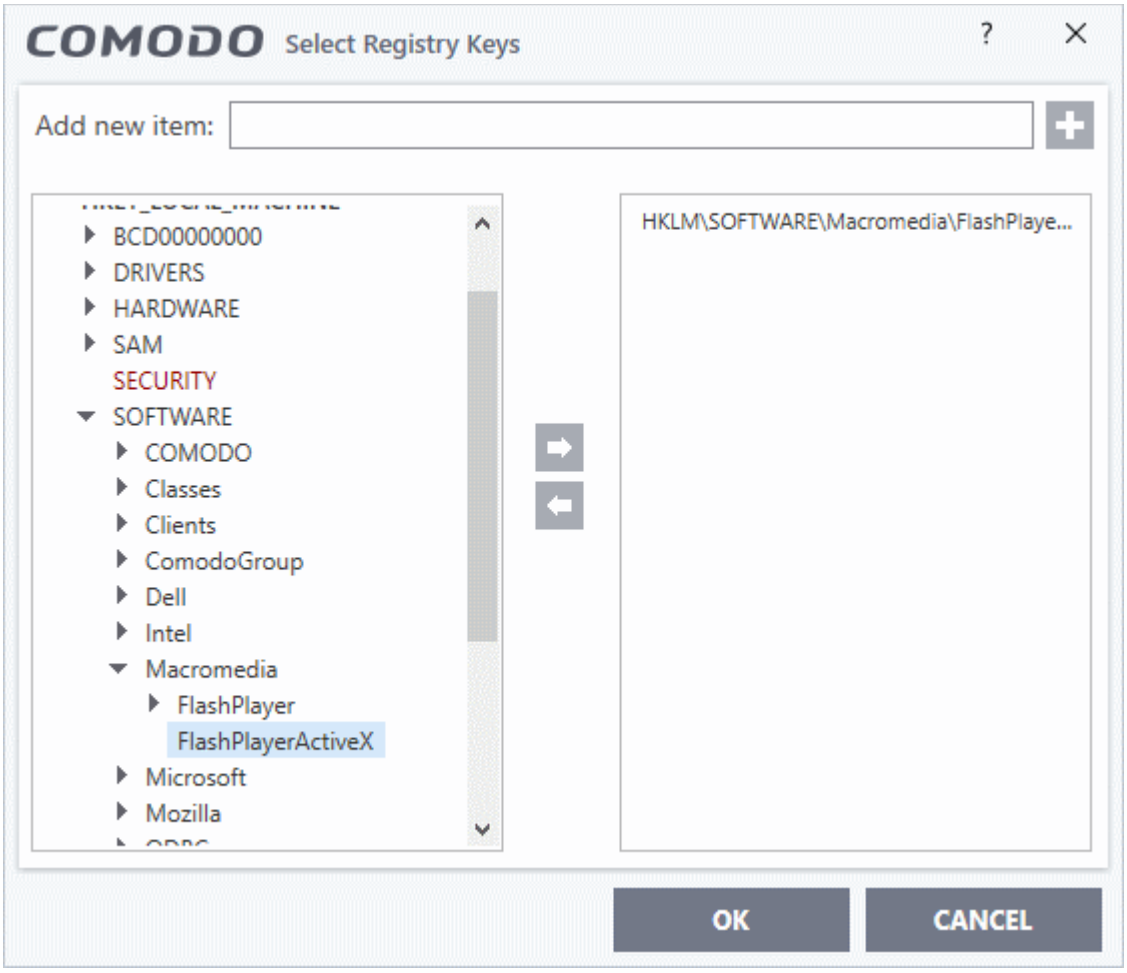


- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.

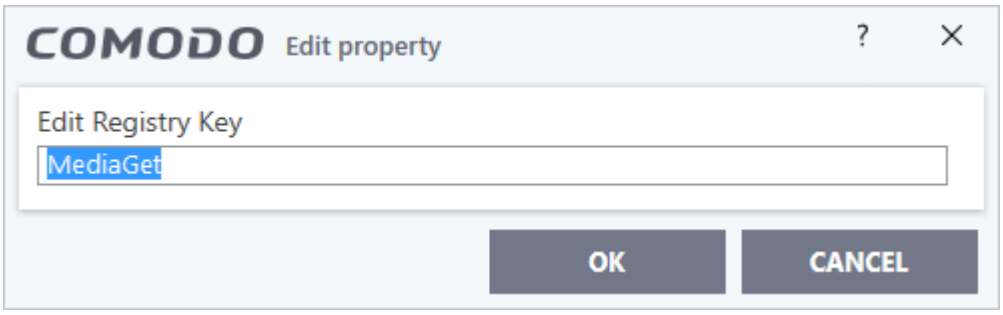


The group will be added to the list.

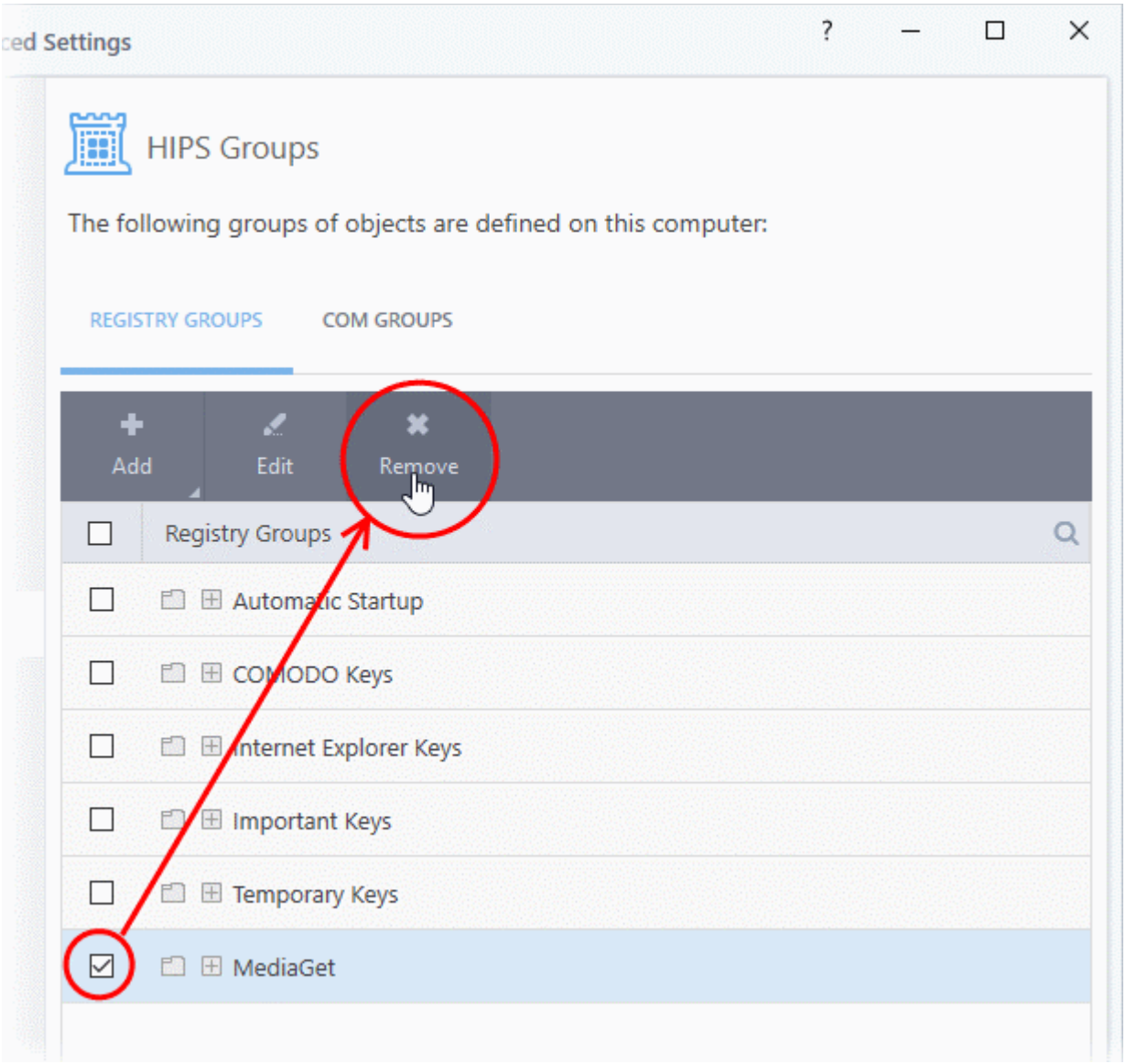
- **Add keys to a group** - Select the group from the list, click 'the Add' button and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



- Select a key on the left then click the right arrow to add a new key to the group. You can add a key manually by typing its name in the 'Add new item' field then clicking the '+' button.
- To edit an existing group, select the group from the list and click the 'Edit' button.



- Modify the name of the group as required and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.



- To remove a key from a group, first expand the group by clicking its '+' symbol, select the key to be removed and click the 'Remove' button.

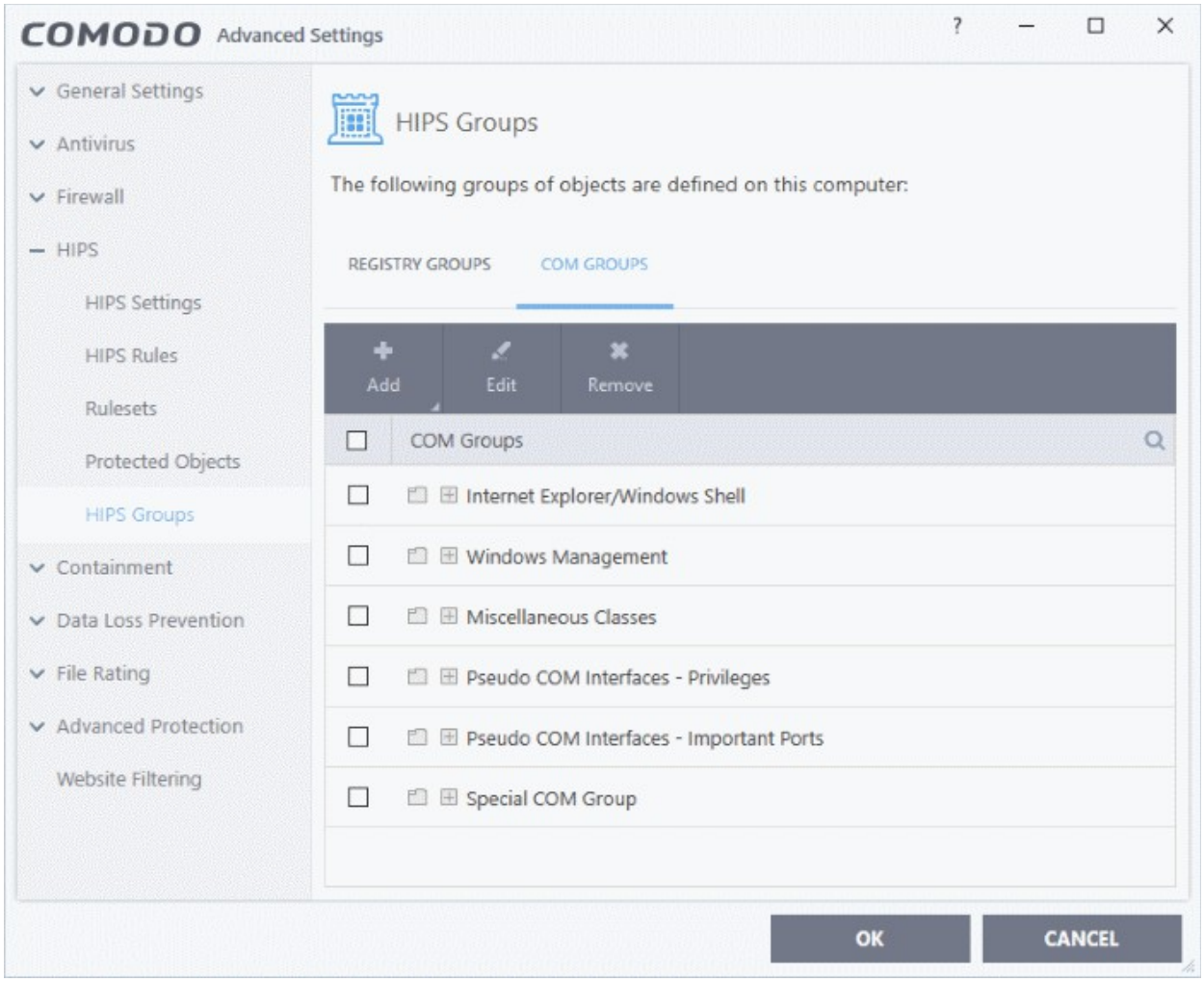
7.4.4.2. COM Groups

- Click 'Settings' > 'HIPS' > 'HIPS Groups' > 'COM Groups'
- COM groups are predefined collections of COM interfaces. COM interfaces are used by Windows to define how objects interact within a single application or between applications.
- COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks. It is therefore essential that COM interfaces are protected.
- Comodo Client Security ships with the following, important COM groups: 'Internet Explorer/Windows Shell', 'Windows Management', 'Miscellaneous Classes', 'Pseudo COM Interfaces - Privileges' and 'Pseudo COM Interfaces - Important Ports'.
- Creating a COM group allows you to quickly add it to the 'COM' protection list. See '**Protected COM Interfaces**' for more details.

To open the 'COM Groups' section

- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'HIPS Groups' on the left.

- Click the 'COM Groups' tab:

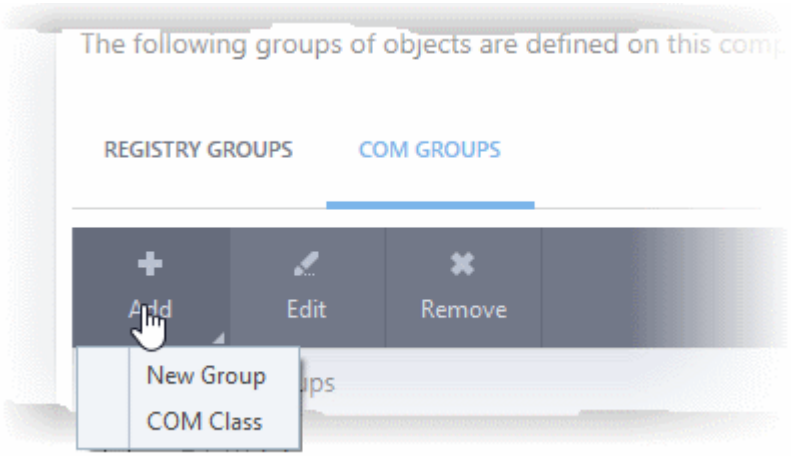


- Click the search icon on the right to find a specific item. You can enter full or partial names.

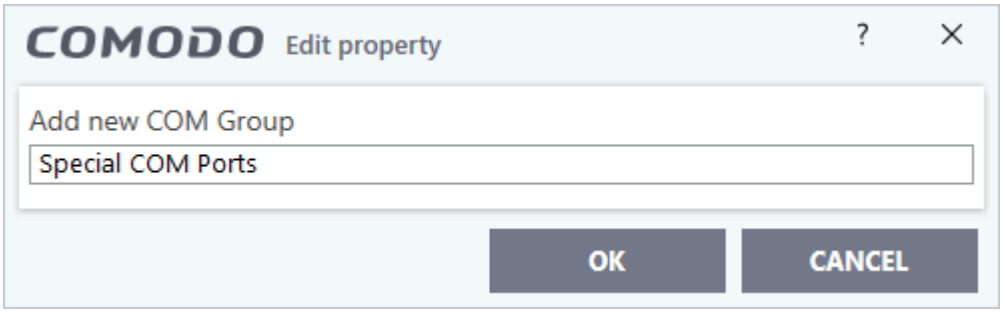
This interface allows you to:

- **Create a new COM Group**
- **Add COM Component(s) to an existing group**
- **Edit the names of an Existing COM Group**
- **Remove existing group(s) or individual COM Component(s) from existing group**

- To add a new group or add new COM Component(s) to an existing group, click the 'Add' button

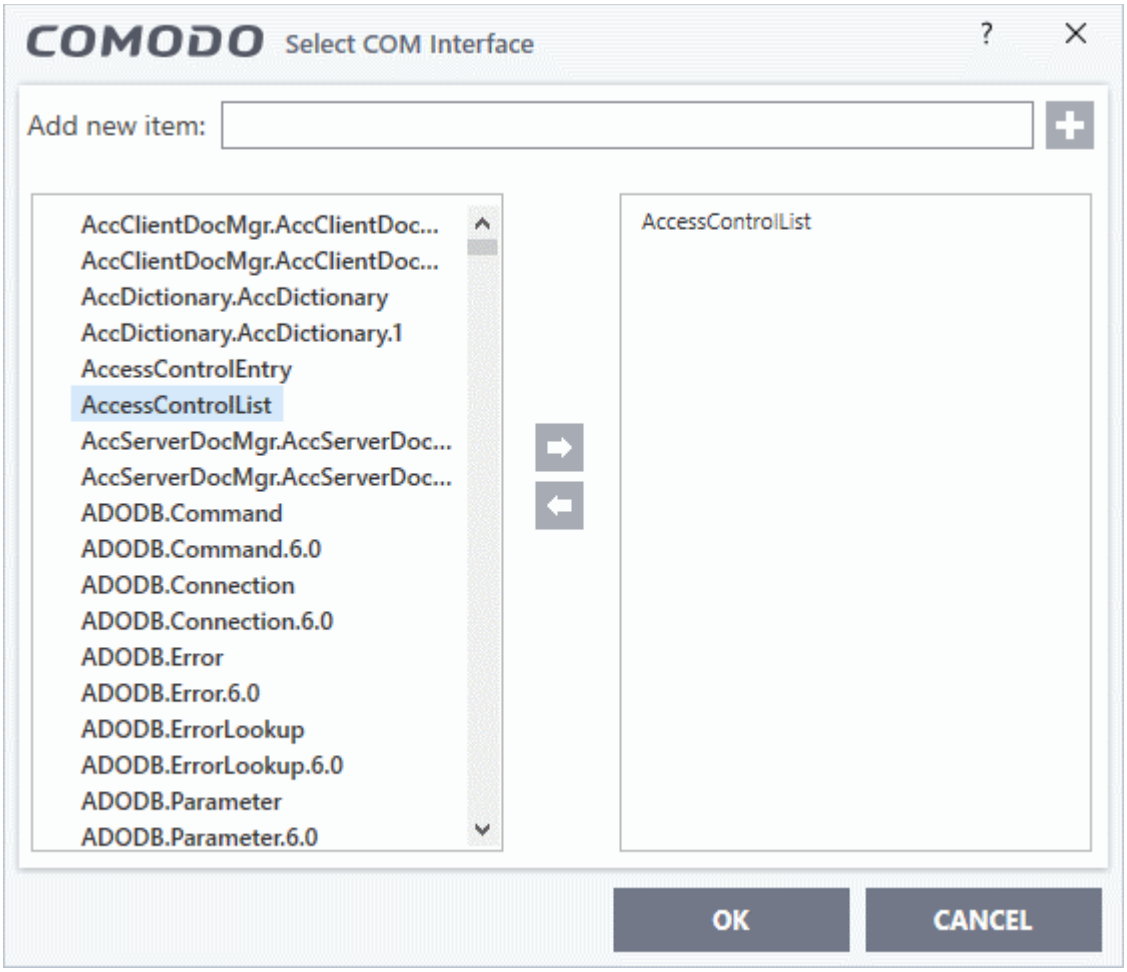


- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'.



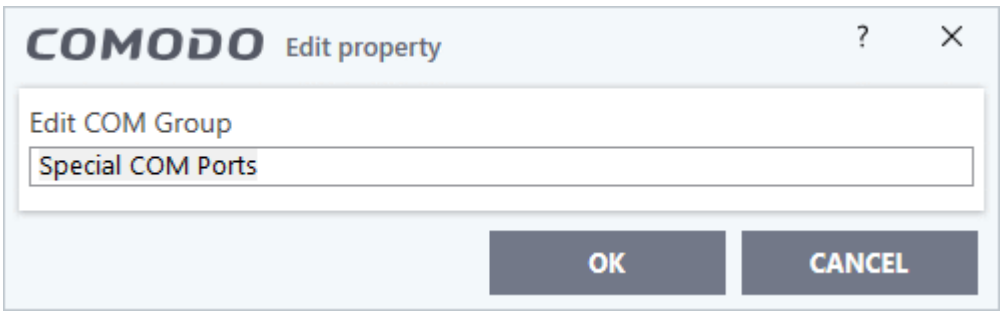
The group will be added to the list.

- **Add COM Components to a group** - Select the group, click the 'Add' button and choose 'COM Class'. The 'Select COM Interface' dialog will be opened.

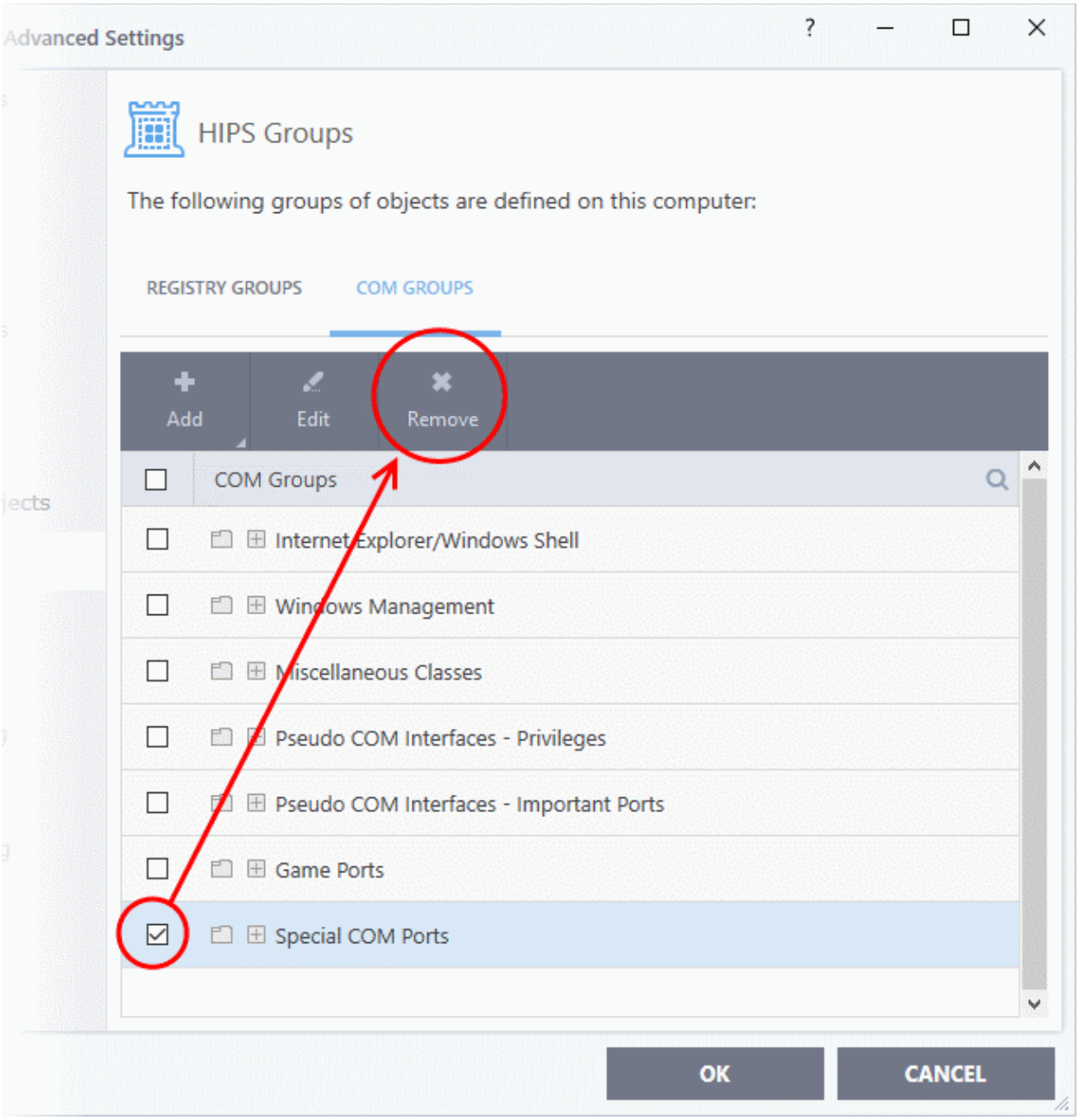


You can add new items by selecting them on the left and clicking the right arrow button. To add items manually, type their name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group from the list and click the 'Edit' button.



- Edit the name of the group in the 'Edit Property' dialog and click 'OK'.
- To remove a group, select the group from the list and click the 'Remove' button.



- To remove an individual COM component from a group, click + at the left of the group to expand the group, select the item to be removed and click the 'Remove' button.

7.5. Protected Objects

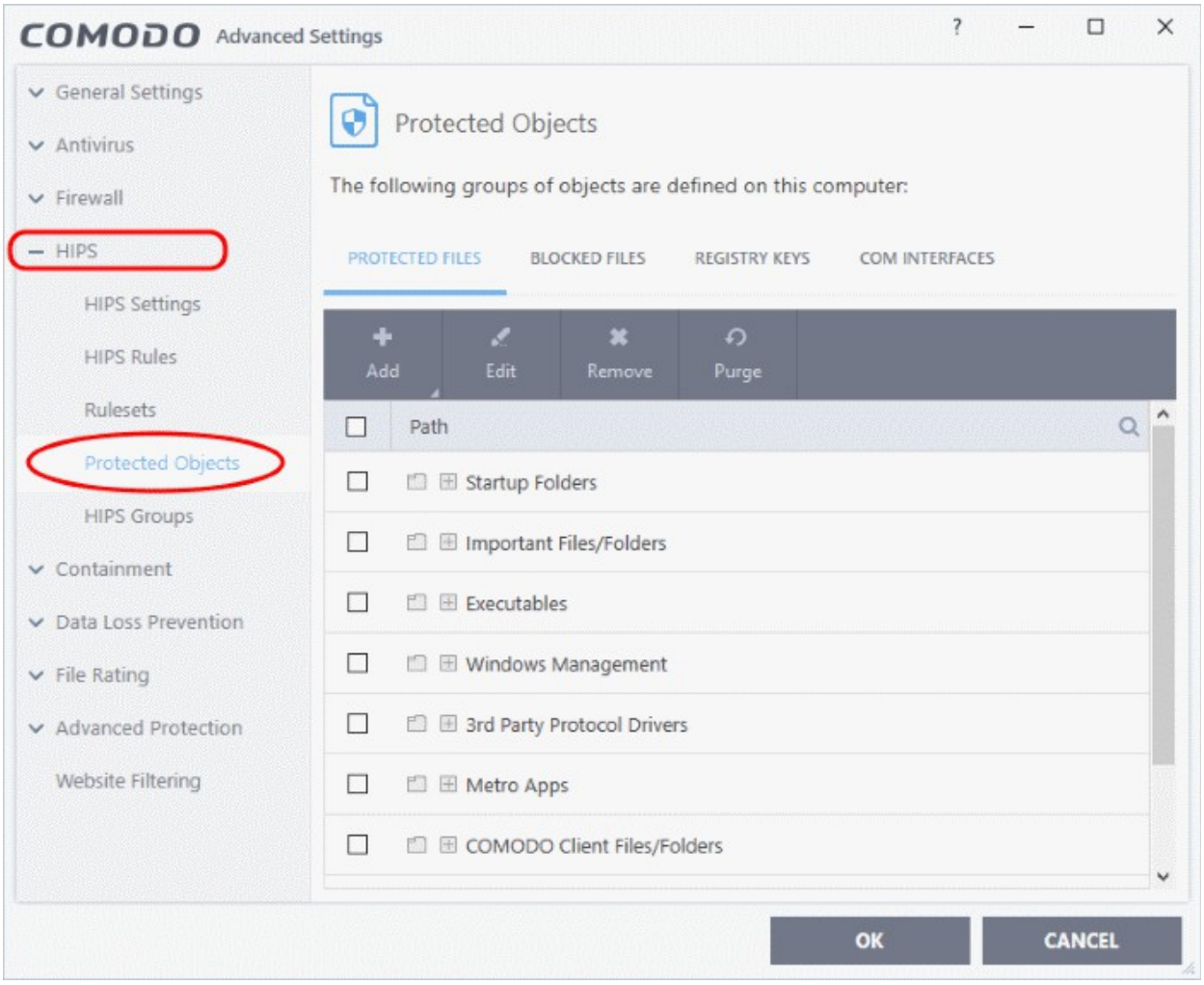
- The protected objects area lets you protect files, folders, registry keys and COM interfaces against access or modification by unauthorized processes.

There are two basic options you can choose:

- **Read access only** - Processes can access but not modify the protected item
  - Click 'Advanced Settings' > 'HIPS' > 'Protected Objects'.
  - See '**Protected Objects - HIPS**' for more help
- **Deny all** - Applications in the container cannot read or modify the protected item
  - Click 'Advanced Settings' > 'Containment' > 'Protected Objects'
  - See '**Protected Objects - Containment**' for more help

7.5.1. Protected Objects - HIPS

- This area lets you protect specific files, folders, registry keys and COM interfaces against modification by unauthorized processes.
- Click 'Settings' on the CCS home screen to open the 'Advanced Settings' interface.
- Click 'HIPS' > 'Protected Objects' on the left:



The interface has the following sub-sections:

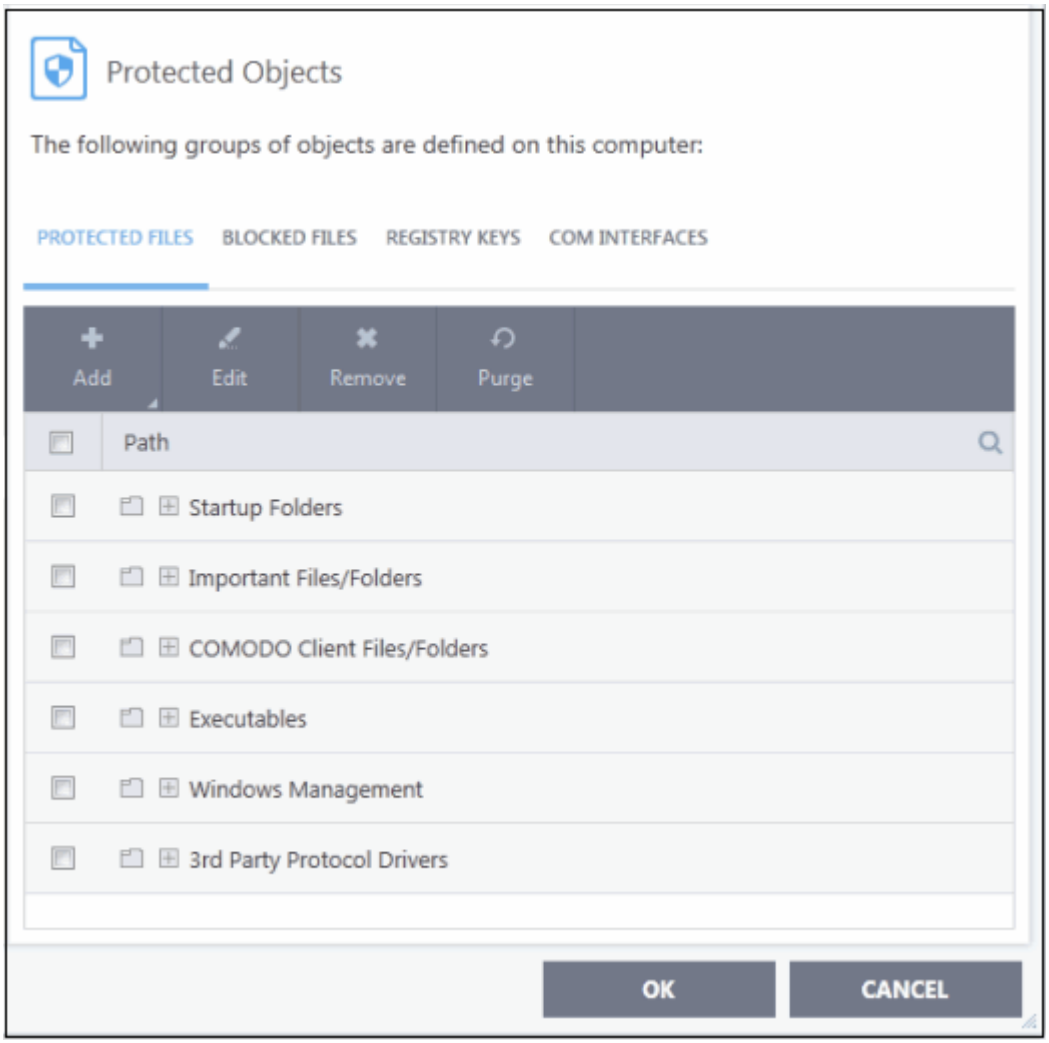
- **Protected Files** - Applications and files which are protected from modification by other processes
- **Blocked Files** - Applications and files that are prevented from running
- **Registry Keys** - Registry keys that are protected from modification by other processes
- **COM Interfaces** - COM interfaces that are protected from modification

7.5.1.1. Protected Files

- The protected files screen shows file groups that are protected from access by other programs.
- Files in this area are 'read only'. They can be accessed and read by other programs, but not modified.
- This prevents malicious programs from hijacking important files. It is also useful for safeguarding valuable files (spreadsheets, databases, documents) against accidental or deliberate sabotage.
- A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Adding your host file to this area will allow web browsers to use the file as normal, but will block any attempt to modify it.
- You can create exceptions if you want to allow a trusted application to access a protected file. See **Exceptions** for more details about how to allow access to files placed in 'Protected Files'.

Open the 'Protected Files' area

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Protected Files' tab:



The buttons at the top provide the following options:

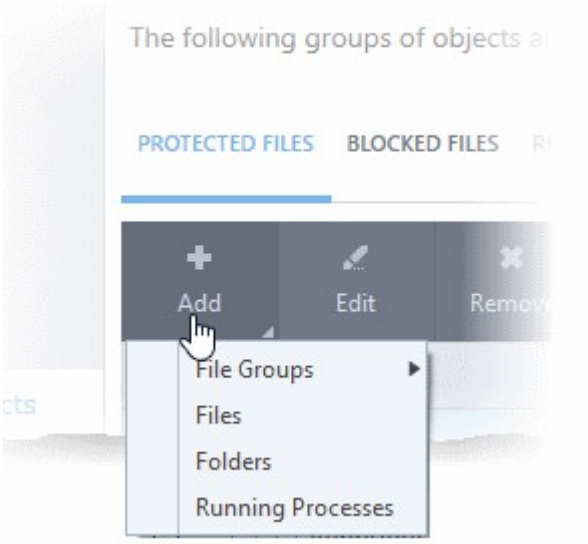
- **Add** - Select files/folders that you want to protect
- **Edit** - Modify the path of the file or group
- **Remove** - Delete the currently highlighted item
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the item is removed (purged) from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

Manually add protected items

You can protect individual files, folders, file groups or processes:

- Click the 'Add' button above the list:

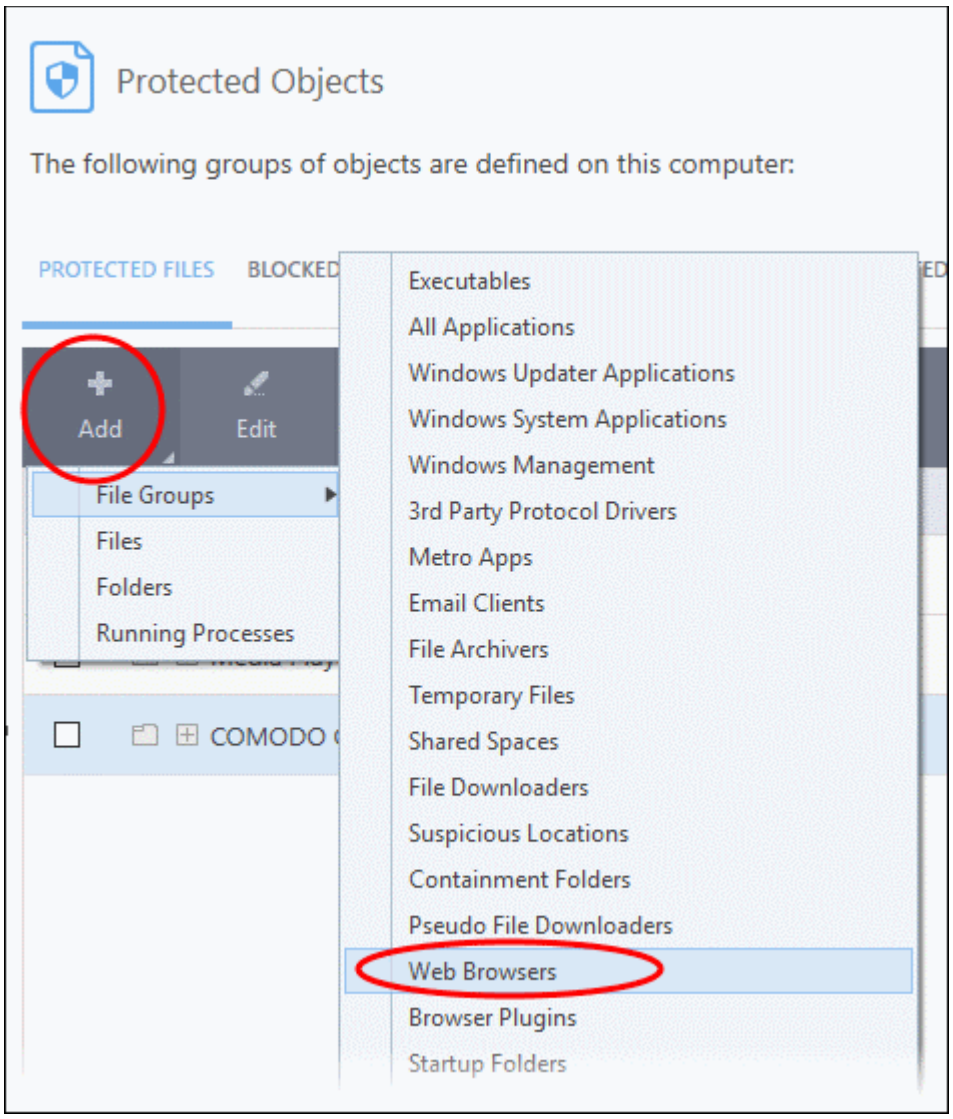


You can add items using any of the following methods:

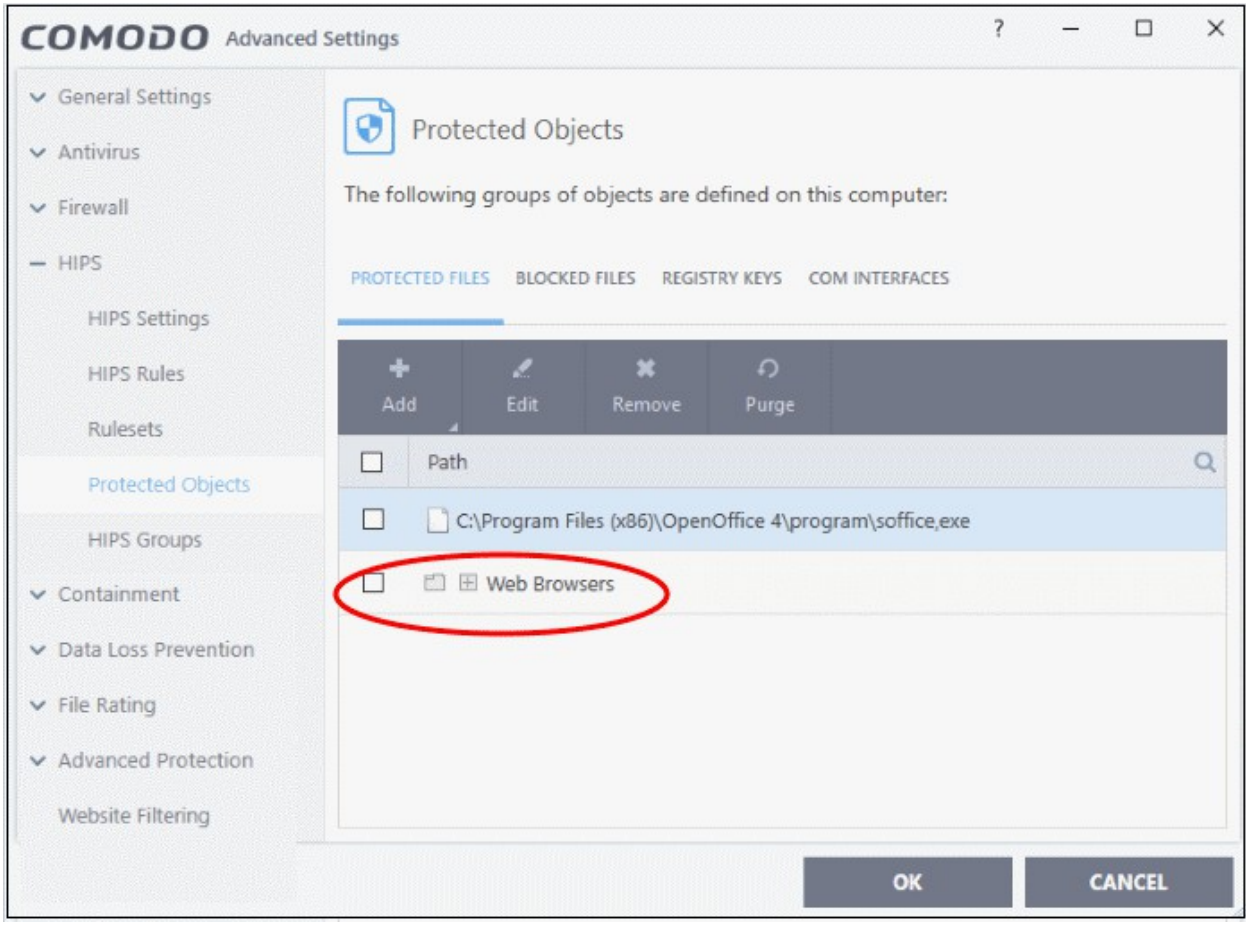
- **Select from File Groups**
- **Browse to a File**
- **Browse to a Folder**
- **Select from currently running processes**

Add a File Group

- Choosing 'File Groups' allows you to protect a category of pre-set files or folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.
  - Background - CCS ships with a set of predefined 'File Groups' which can be viewed in 'Settings' > 'File Rating' > '**File Groups**'. You can also add your own file groups if required.
- Click 'Add' > 'File Groups' and select the type of 'File Group' from the list:

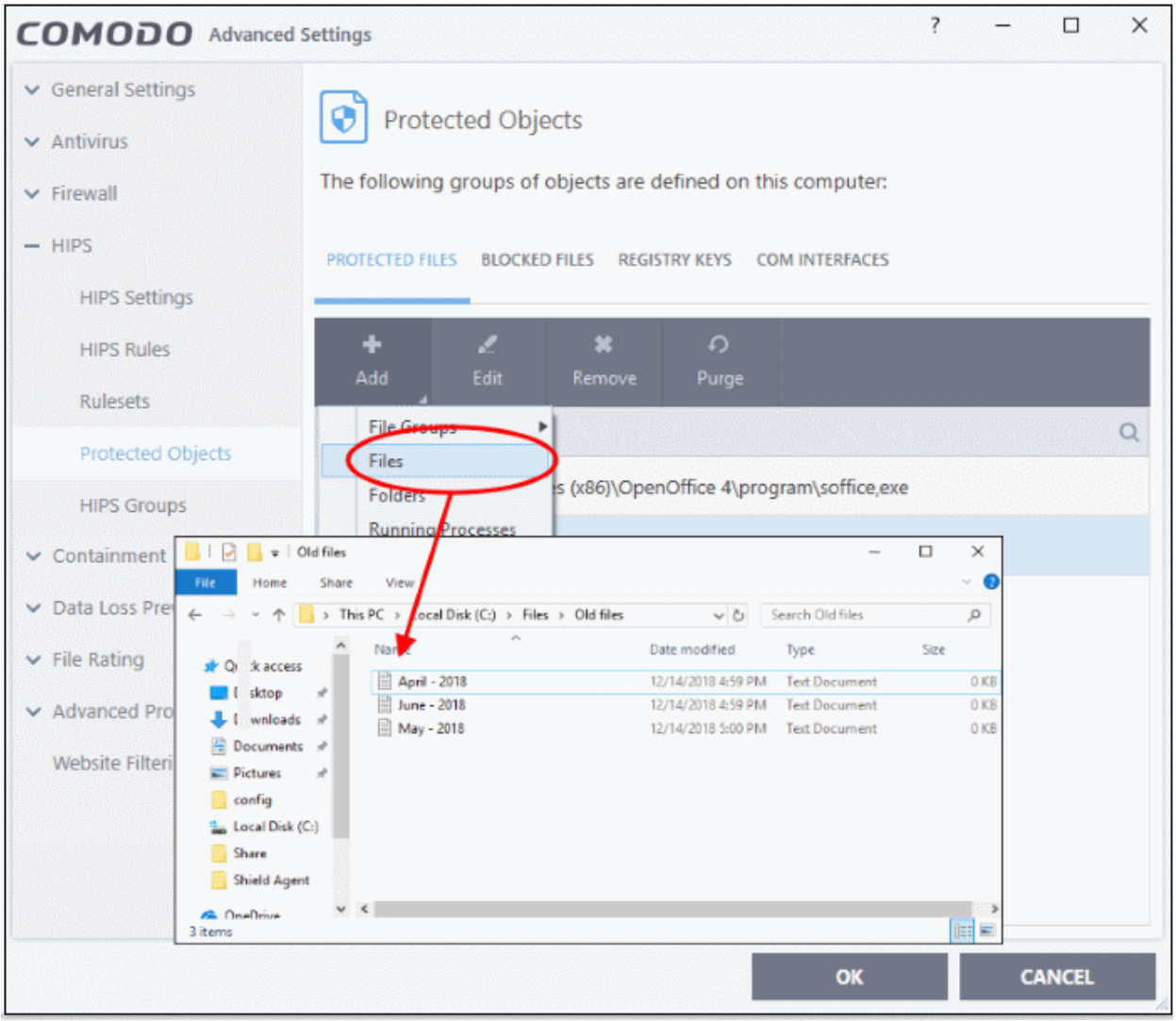


The selected group will be added to the 'Protected Files' list:



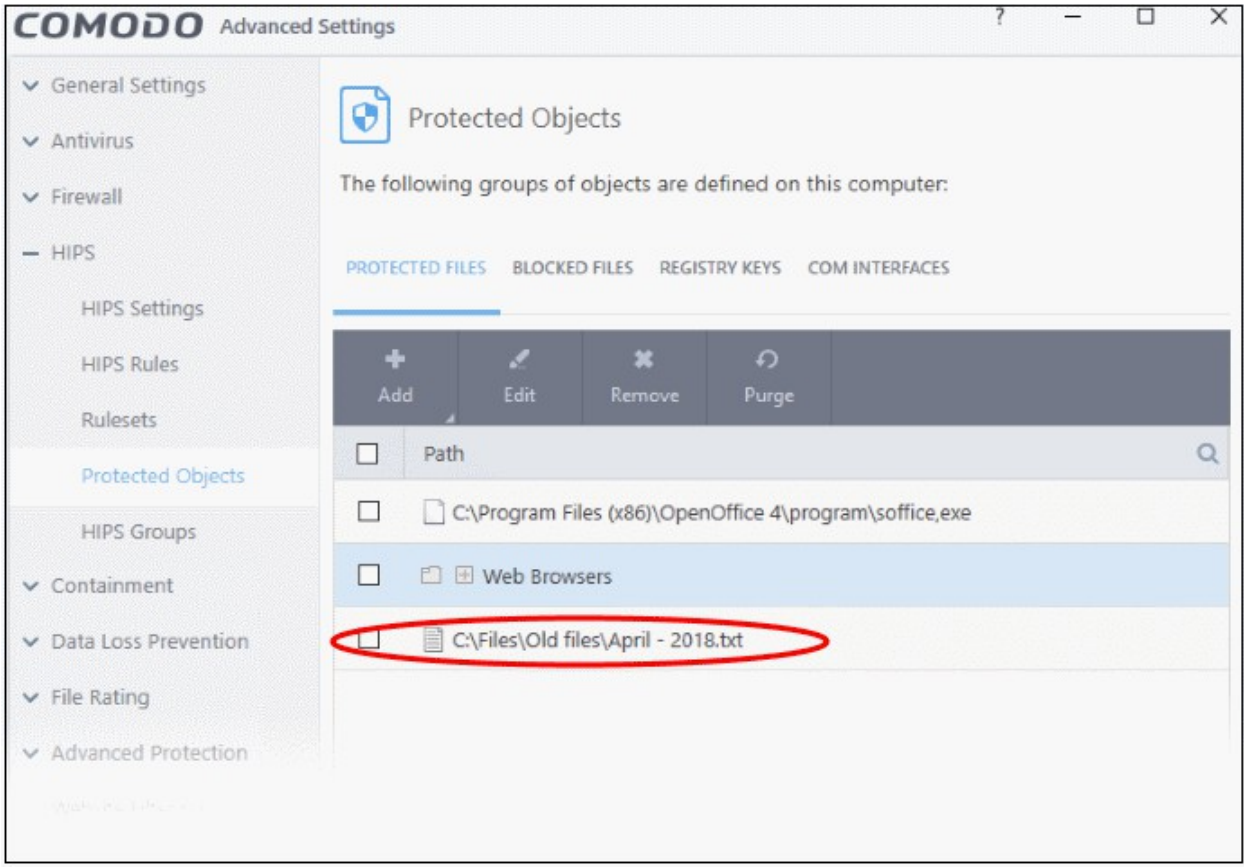
Add an individual file

- Click 'Add' and choose 'Files' from the options:



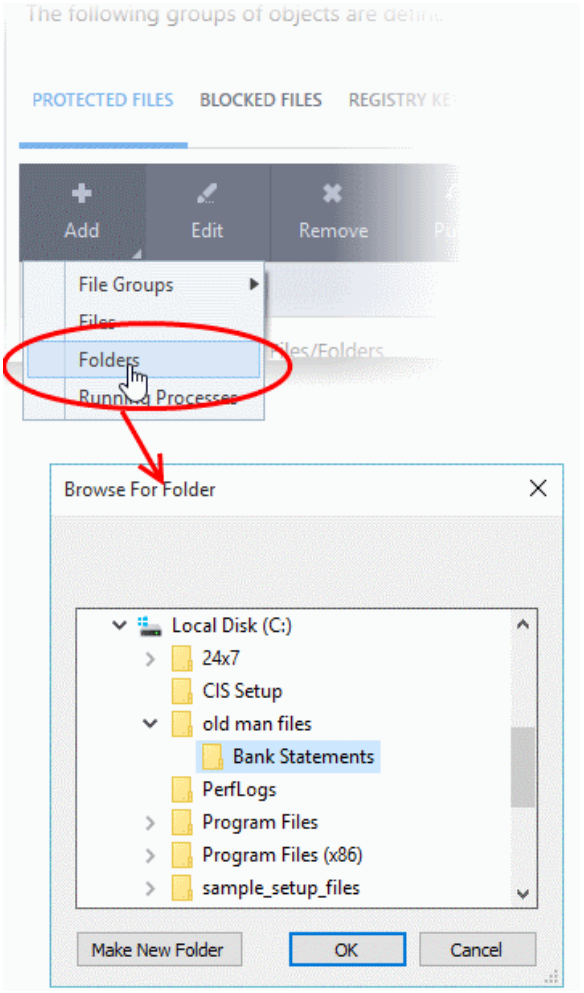
- Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open'

The file will be added to 'Protected Files'.



Add a Drive Partition/Folder

- Click 'Folders' from the 'Add' drop-down.

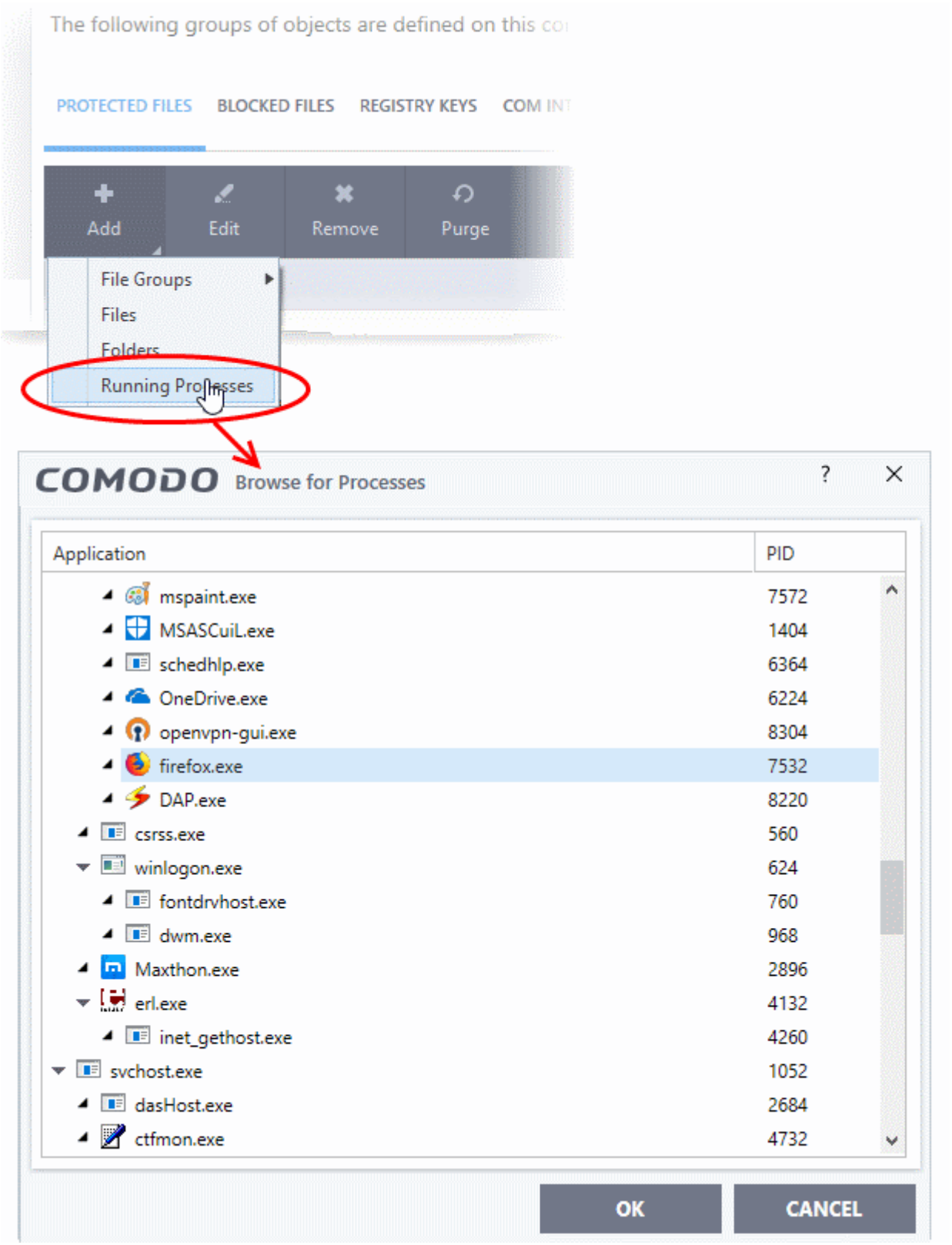


The 'Browse for Folder' dialog will appear.

- Select the folder/drive and click 'OK'. Repeat the process to add more items.

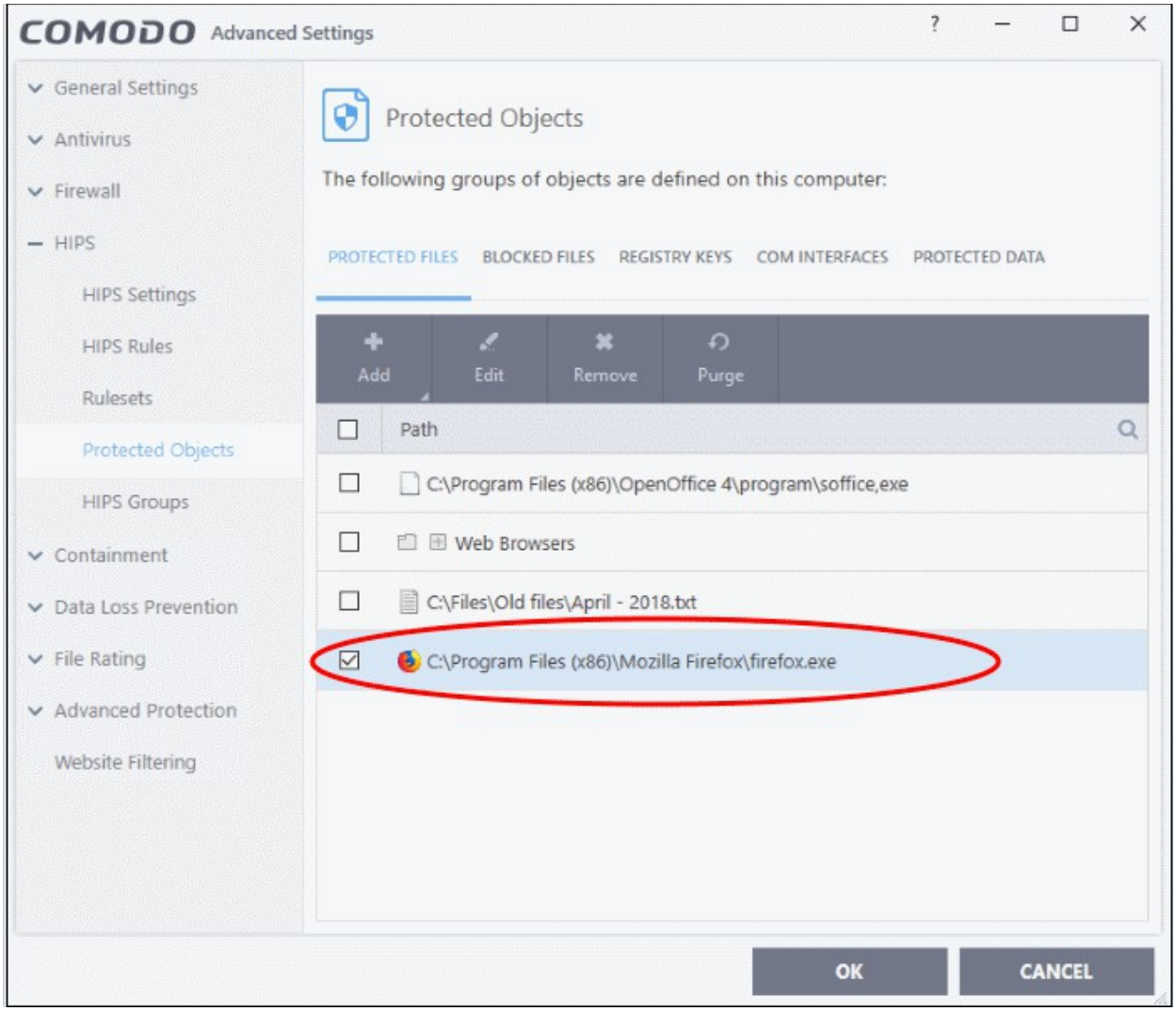
Add an application from a running process

- Choose 'Running Processes' from the 'Add' drop-down
- This will open a list of processes that are currently running on your computer:



- Select the process you want to protect
- Click 'OK'

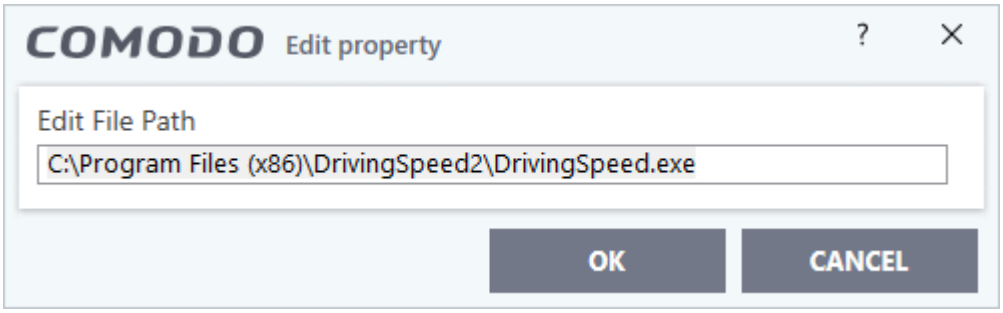
The parent application will be added to the 'Protected Files' list:



- Repeat the process to add more files. The items added to the 'Protected Files' will be protected from access by other programs.

To edit an item in the Protected Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click 'OK'

To delete an item from Protected Files list

- Select the item from the list and click the 'Remove' button

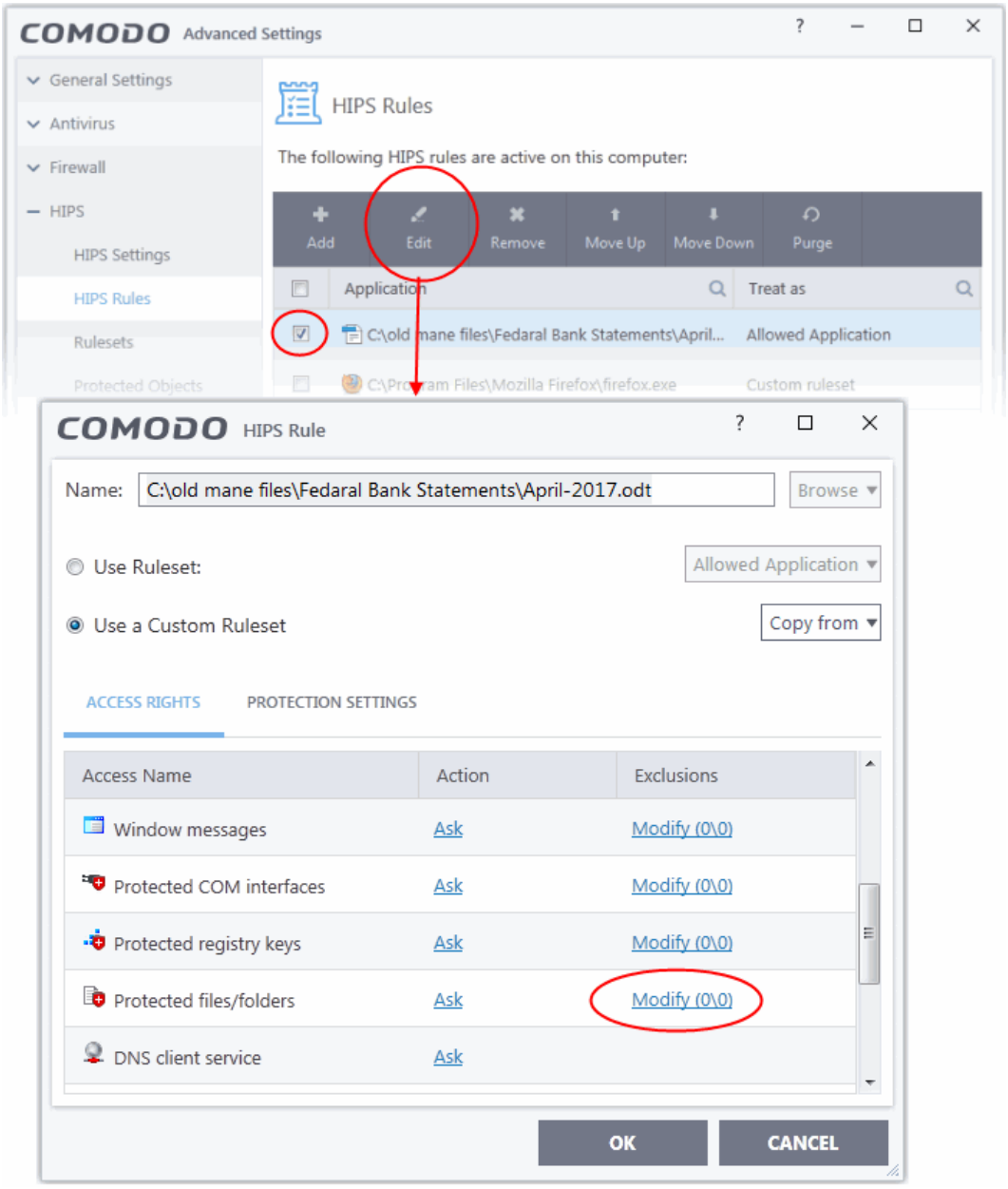
The selected item will be deleted from the protected files list. CCS will not generate alerts, if the file or program is subjected to unauthorized access.

Exceptions

Users can selectively allow another application (or file group) to modify a protected file by affording the appropriate 'Access Right' in '**Active HIPS Rules**' interface.

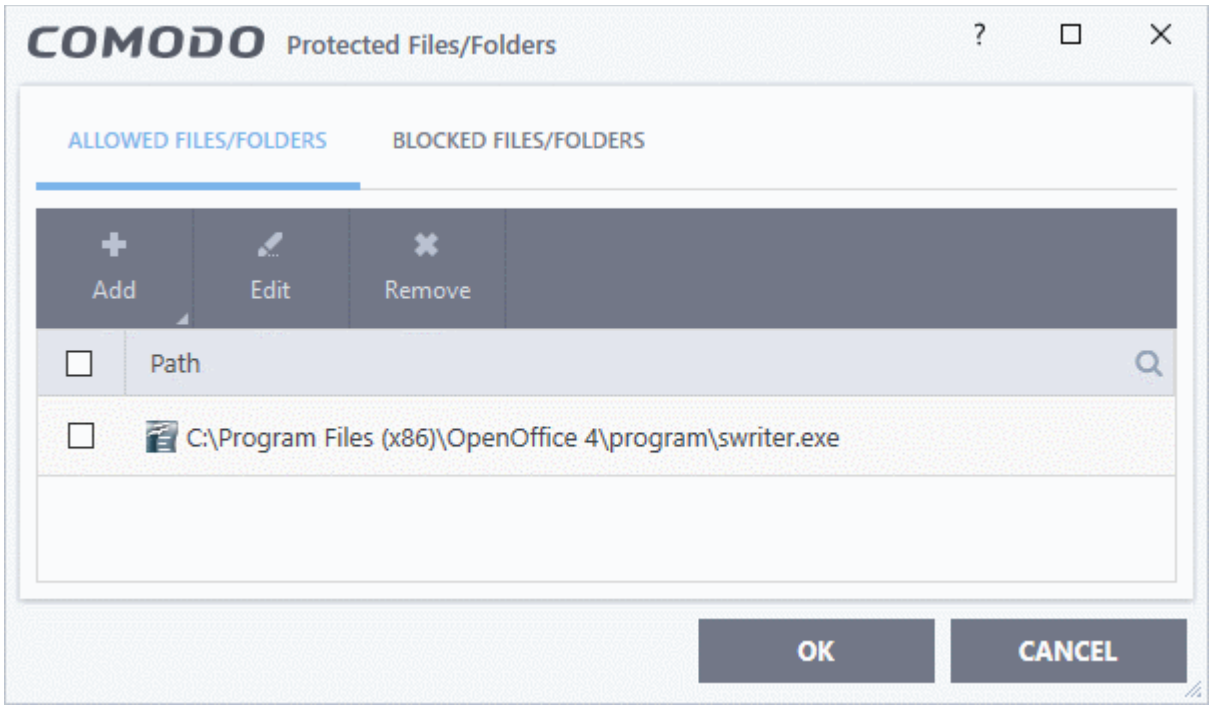
A simple example would be the imaginary file 'April - 2018.odt'. You would want the 'Open Office Writer' program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potentially malicious program. You would first **add** the document to the 'Protected Files' area. Once added to 'Protected Files', you would go into '**Active HIPS Rules**' and create an exception for 'swriter.exe' so that it alone could modify 'June - 2016.odt'.

- First add 'April - 2017.odt' to 'Protected Files'
- Then go to the 'HIPS Rules' interface and add it to the list of applications.
- Click the 'Edit' button after selecting it.
- In the 'HIPS Rule' interface, select 'Use a Custom Ruleset'.



- Under the 'Access Rights' section, click the link 'Modify' beside the entry 'Protected Files/Folders'. The 'Protected Files/Folders' interface will appear.

- Under the 'Allowed Files/Folders' section, click 'Add' > 'Files' and add swriter.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



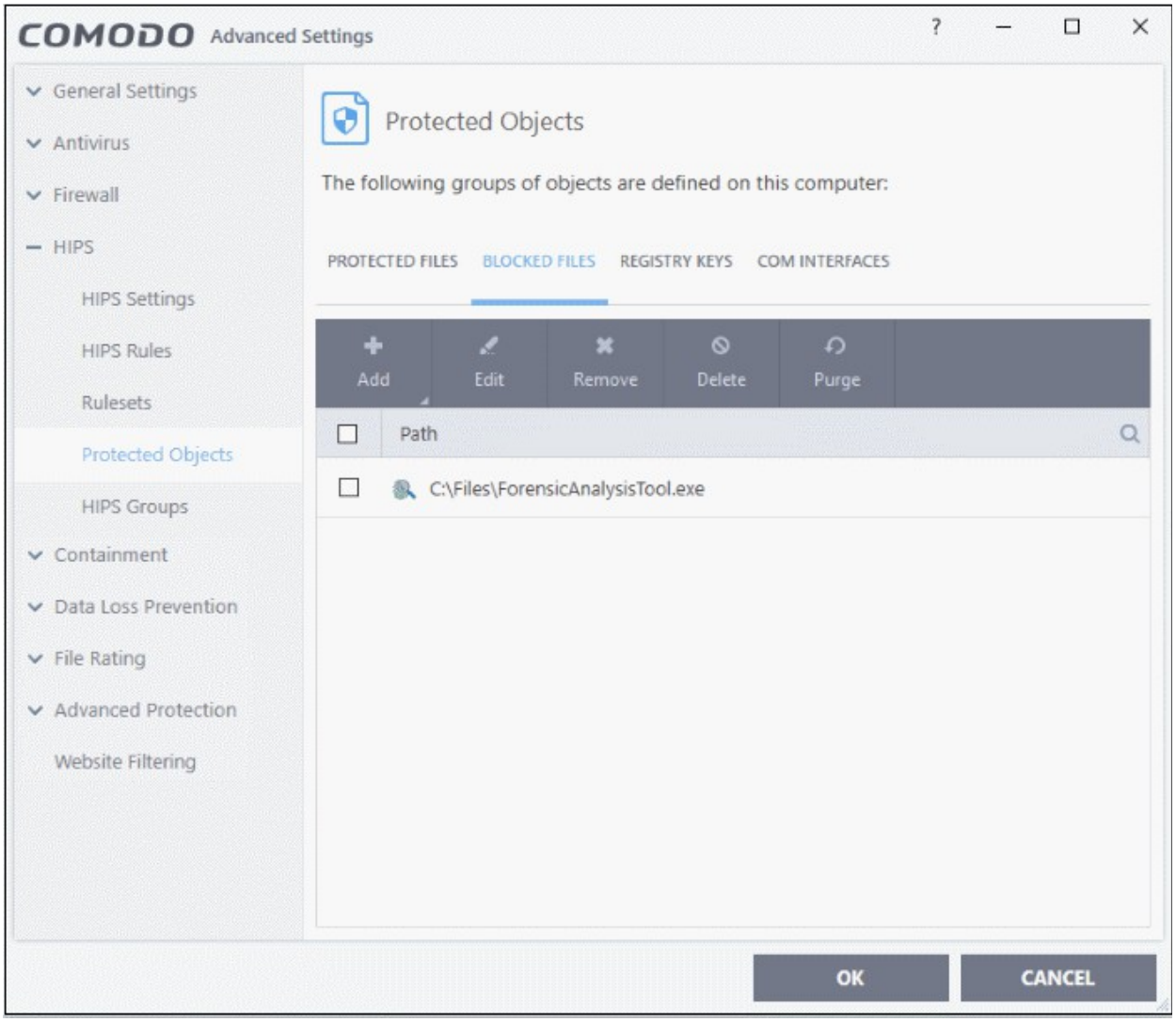
Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

7.5.1.2. Blocked Files

- CCS allows you to lock-down files and folders by denying all access rights to them from other processes or users - effectively cutting them off from the rest of your system.
- If the file you block is an executable, then neither you nor anything else is able to run that program.
- Unlike files in 'Protected Files', users cannot selectively allow access to a blocked file.

Open the blocked files section

- Click 'Settings' on the CCS home screen.
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Blocked Files' tab:



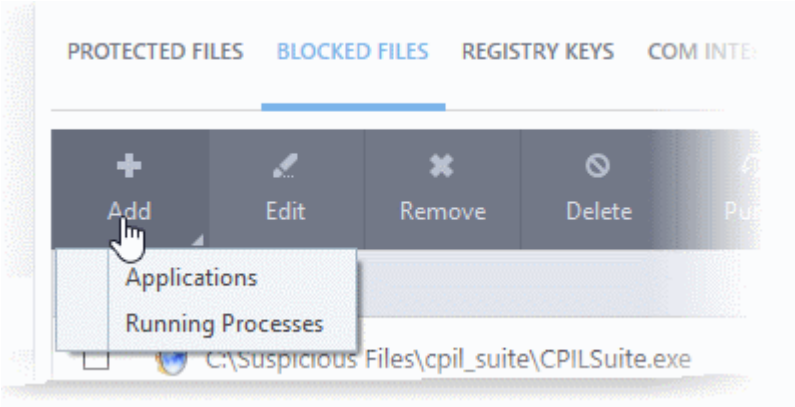
The buttons at the top provide the following options:

- **Add** - Select files/folders that you want to block
- **Edit** - Modify the path of the file or group
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the item is removed (purged) from the list.

Click the search icon on the right to find a specific item. You can enter full or partial names.

Manually add an item to the block list

- Click the 'Add' button:

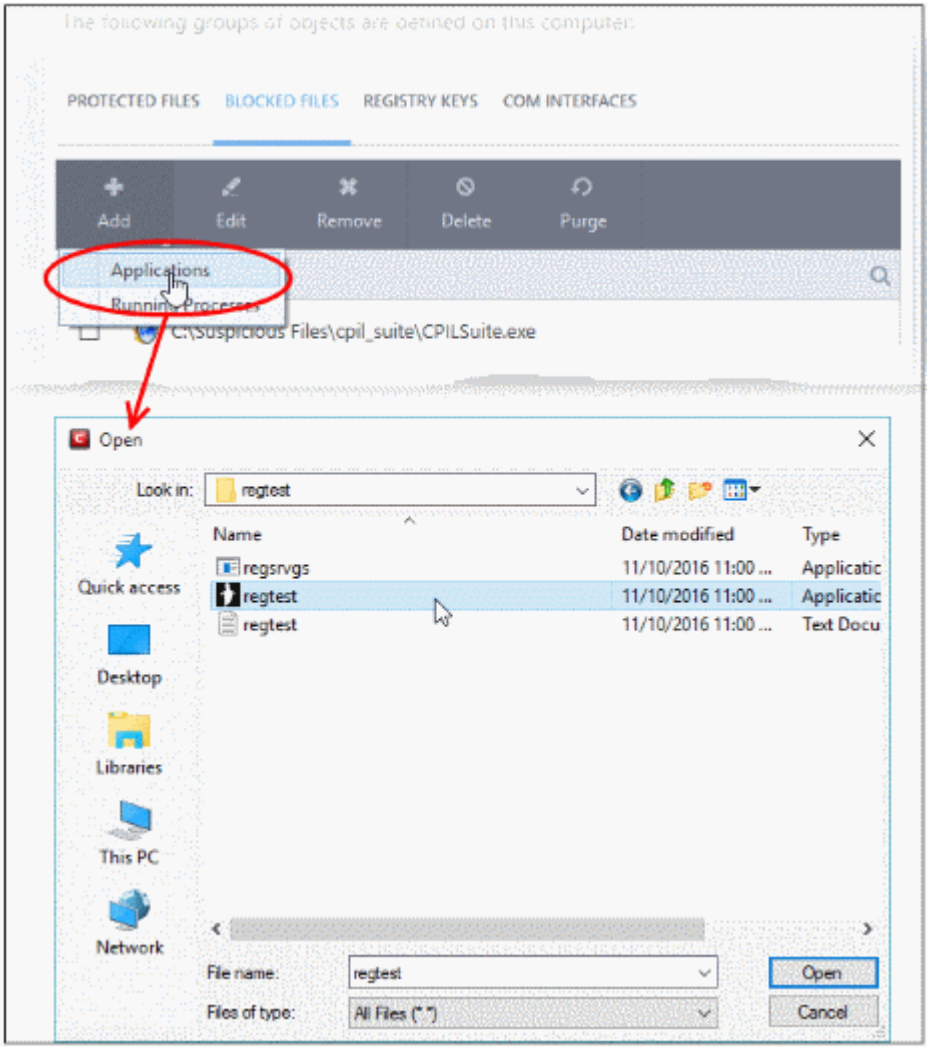


You can add the files by following methods:

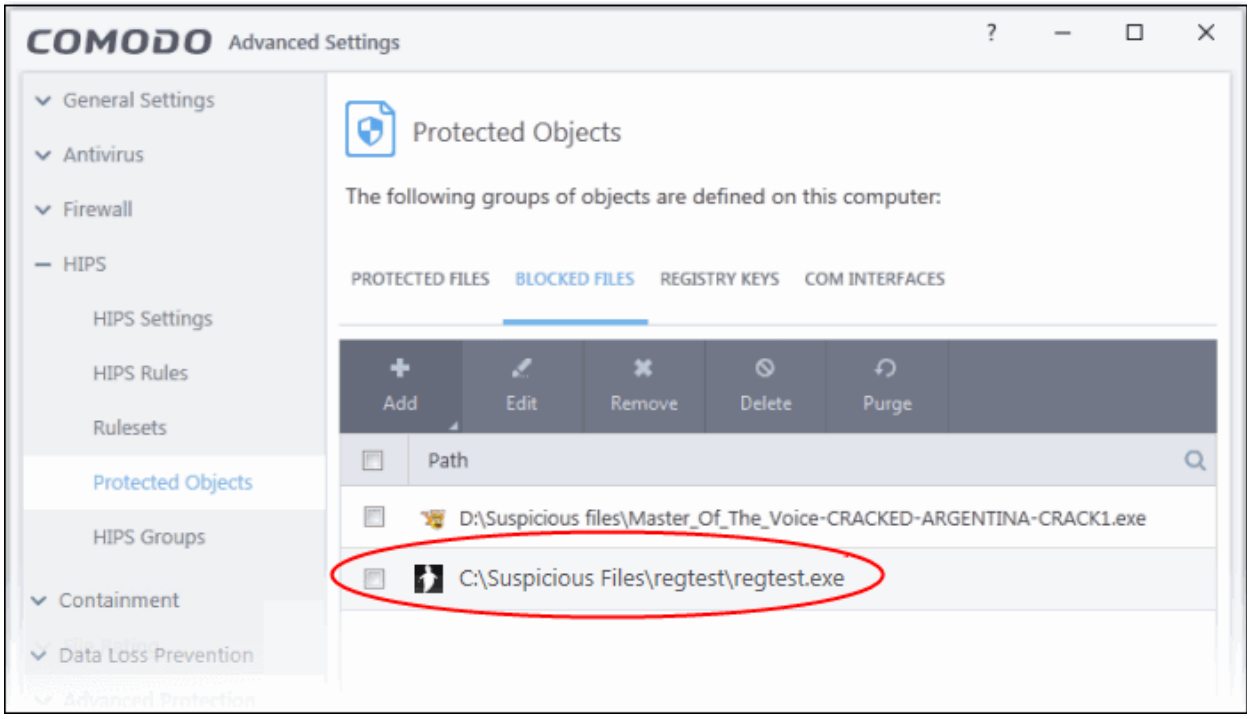
- **Select a file**
- **Select a currently running process**

Add a File

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



The file will be added to 'Blocked Files' list.



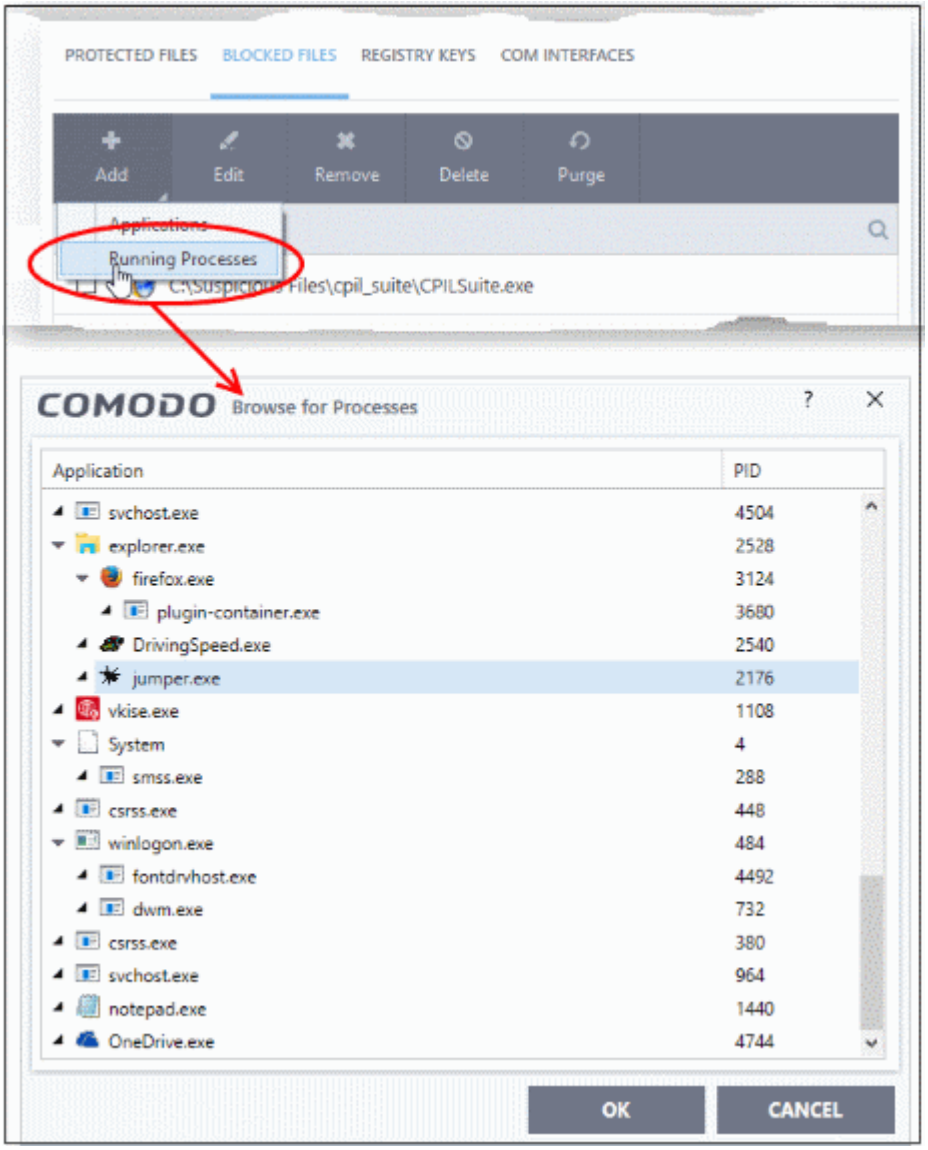
- Repeat the process to add more files.

Add a running process

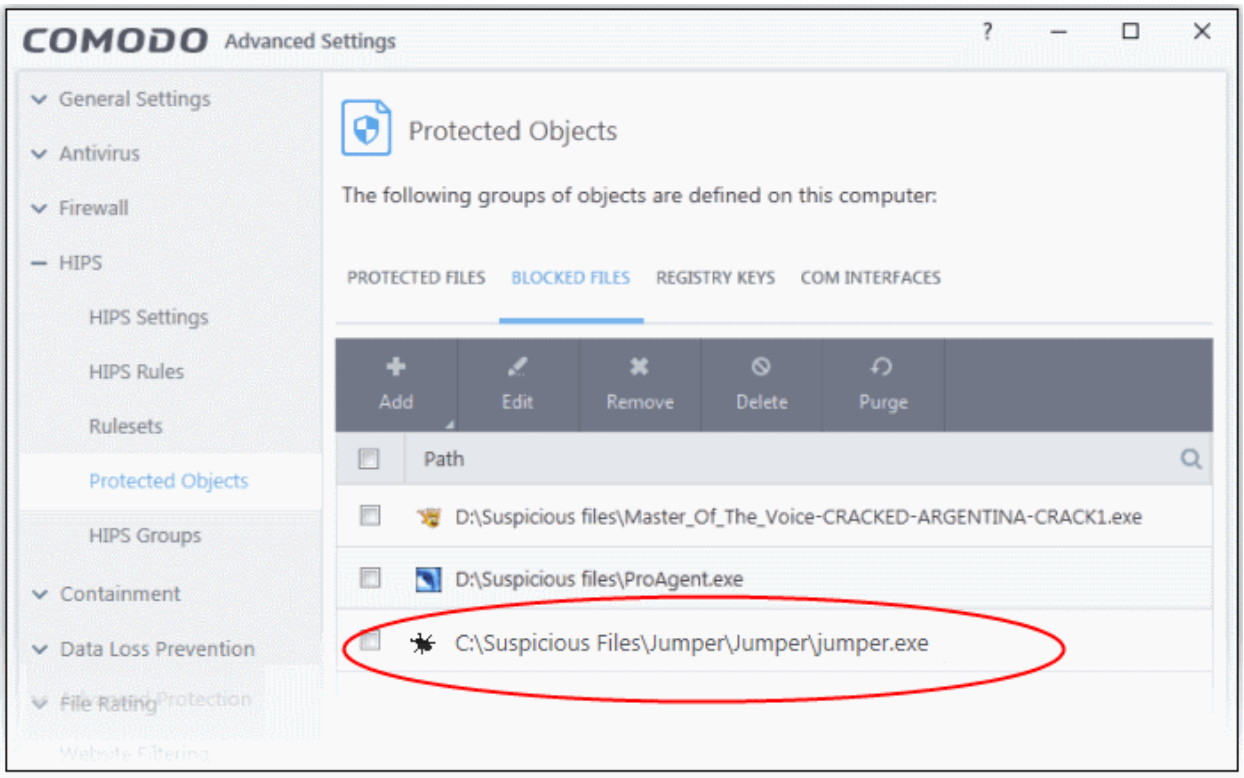
- Choose 'Running Processes' from the 'Add' drop-down

This will open a list of processes that are currently running on your computer:

- Select the process you want to protect
- Click 'OK'



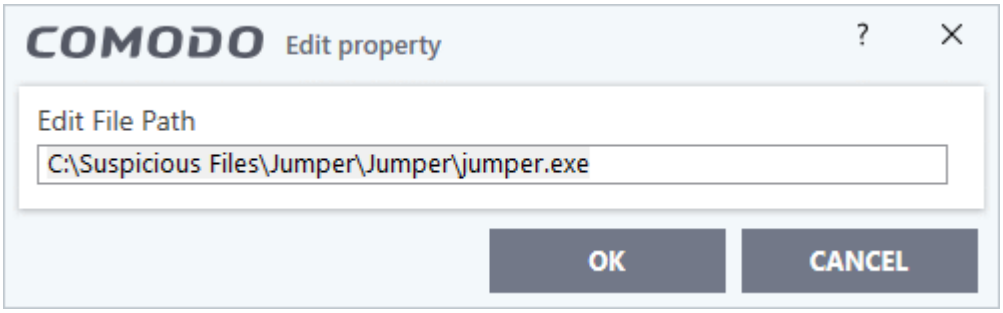
The parent application will be added to the 'Protected Files' list:



- Repeat the process to add more files.

To edit an item in the Blocked Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click 'OK'

To release an item from Blocked Files list

- Select the item from the list and click the 'Remove' button

The selected item will be removed from the 'Blocked Files' list. CCS will not block the application or file from execution or opening then onwards.

To permanently delete a blocked file from your system

- Select the item from the list and click the 'Delete' button

The selected item will be deleted from your computer immediately.

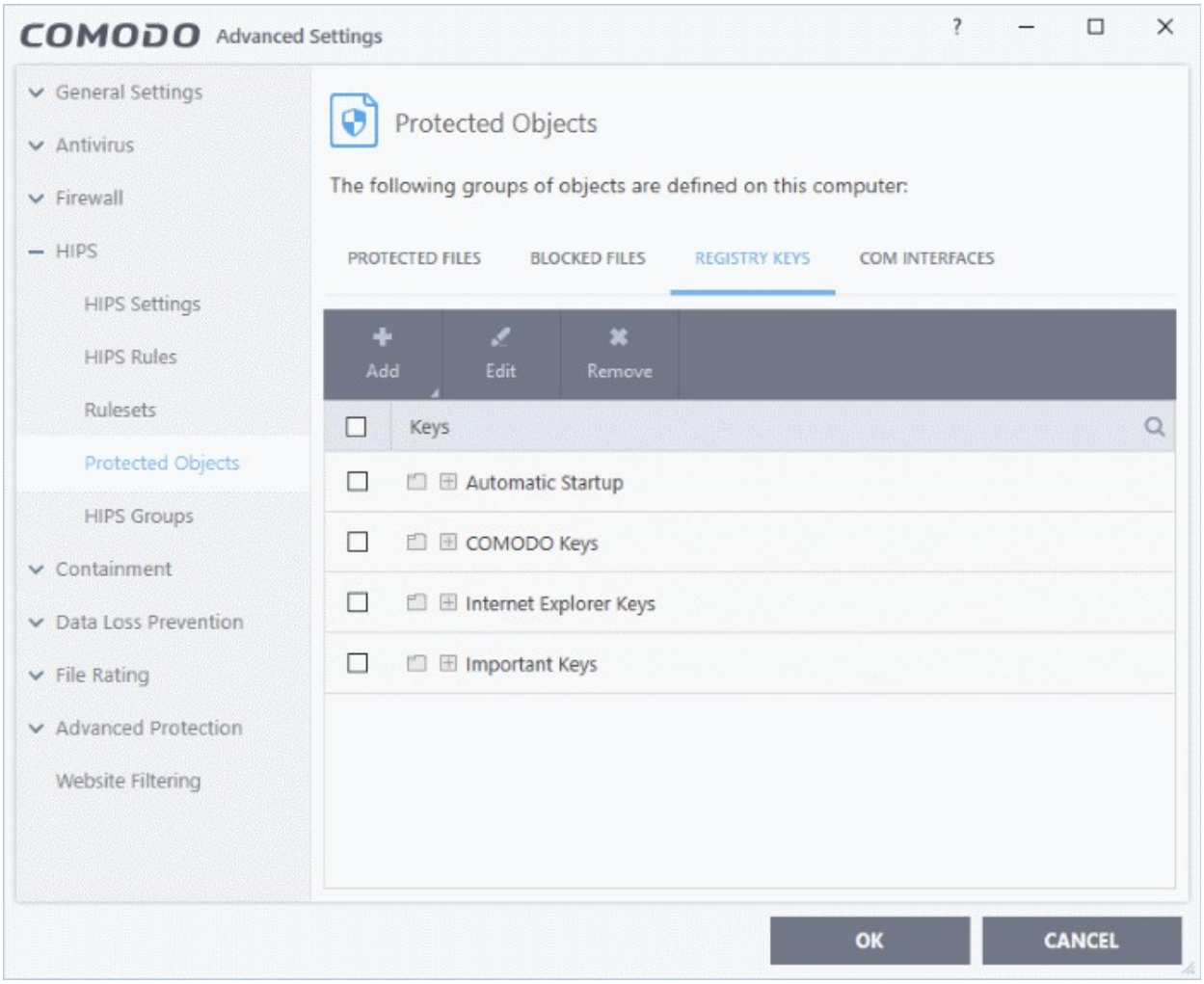
Warning: Deleting a file from from the 'Blocked Files' interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

7.5.1.3. Protected Registry Keys

The 'Registry Keys' area lets you define system critical registry keys which should protected against modification. Irreversible damage can be caused to your system if important registry keys are corrupted or modified.

Open the 'Registry Keys' section

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'Registry Keys' tab:



The buttons at the top provide the following options:

- **Add** - Select registry groups or individual keys that you want to protect
- **Edit** - Modify the path of the key or key group
- **Remove** - Delete the currently highlighted item
- Click the magnifying glass on the right to search for a specific item.

Manually add individual keys or registry groups

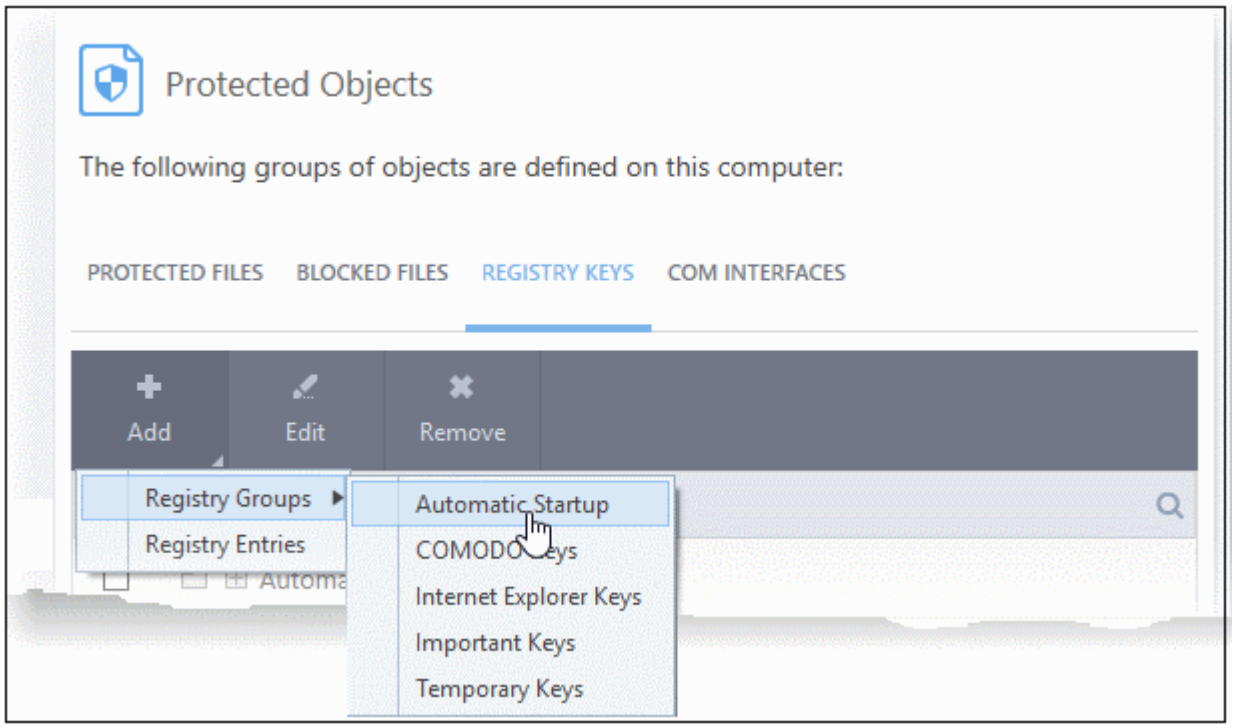
- Click the 'Add' button

You can add keys individually or by registry group:

- **Add Registry Groups** - Adding a registry group allows you to batch select and import groups of important registry keys. Comodo Client Security provides the following, pre-defined groups - 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys', 'Important Keys' and 'Temporary Keys'.

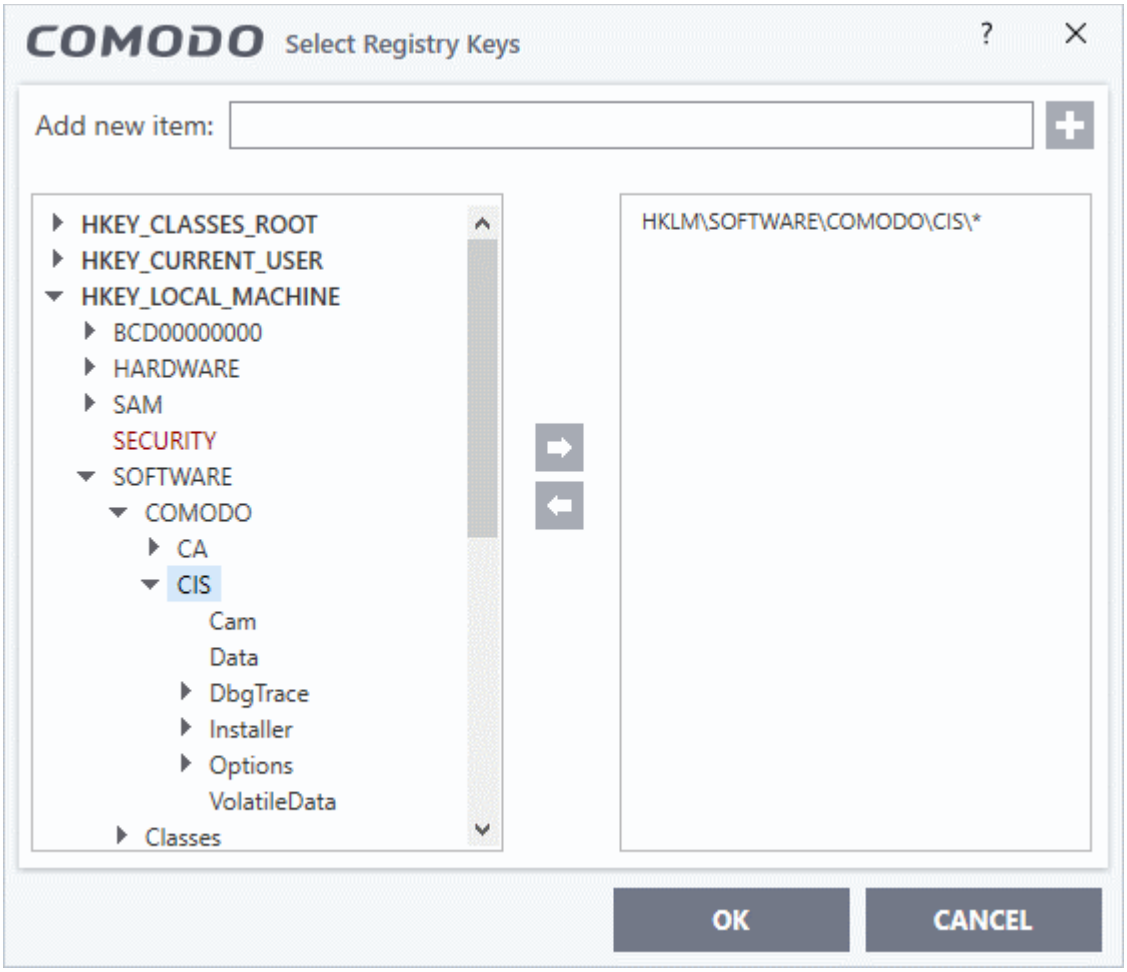
You can also create custom registry groups containing keys you wish to protect.

- To add a new group, click the 'Add' button > 'Registry Groups' and select the predefined group from the list and click 'OK'



See **Registry Groups** in the **HIPS Groups** section if you want to read more on this interface.

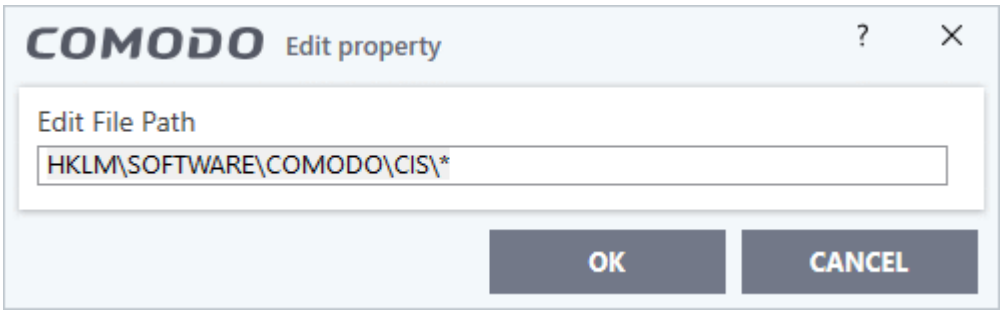
- **Add individual Registry Keys** -
  - Click the 'Add' button and then select 'Registry Entries'
  - Choose a key on the left then click the right arrow to add it to the protected list:



- Alternatively, you can type the key name in the field at the top then click '+'.

Edit an item in the Registry Protection list

- Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the key path, if you have relocated the key and click 'OK'.

Note: The 'Registry Groups' cannot be edited from this interface. You can edit only from **Registry Groups** in **HIPS Groups** section.

To delete an item from Registry Protection list

- Select the item from the list and click the 'Remove' button.

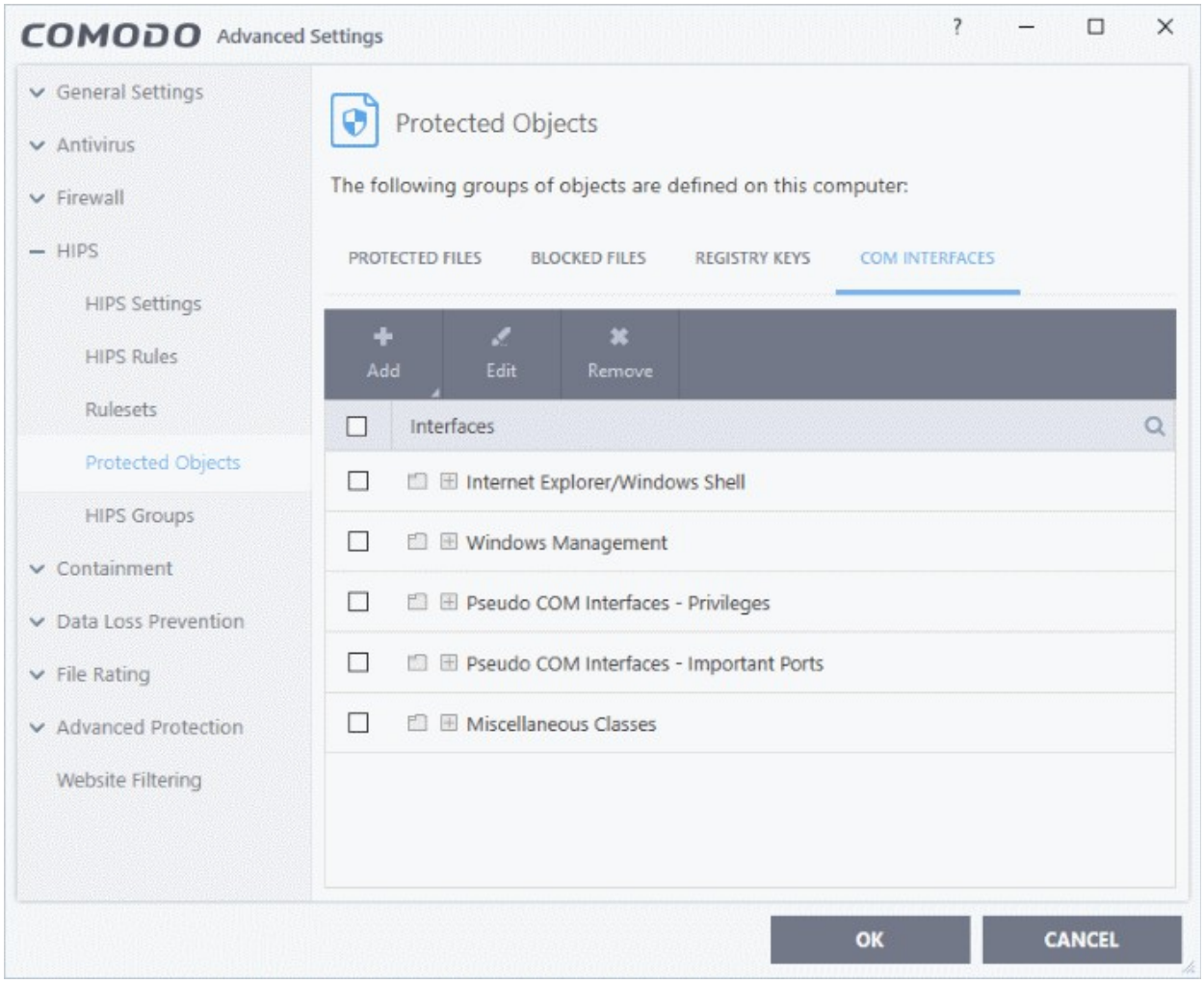
The selected item will be deleted from the 'Registry Keys' protection list. CCS will not generate alerts, if the key or the group is modified by other programs.

7.5.1.4. Protected COM interfaces

- The Component Object Model (COM) is Microsoft's object-oriented programming model. It defines how objects interact within a single application, or between applications.
- COM is used as the basis for Active X and OLE - two favorite targets of hackers and malware for launching attacks on your computer.
- Comodo Client Security automatically protects COM interfaces against modification and manipulation by malicious processes.
- 'Protected Objects' > 'COM Interfaces' lets you view, add and edit these protected interfaces.
  - Background - CCS ships with a set of COM groups - category based collections of COM interface components.
  - Click 'Settings' > 'HIPS Groups' > 'COM Groups' if you want to view these groups. You can create custom groups if required. See **COM Groups** for the help page on this area.

Open the protected COM interfaces area

- Click 'Settings' on the CCS home screen
- Click 'HIPS' > 'Protected Objects' on the left.
- Click the 'COM Interfaces' tab:



The buttons at the top provide the following options:

- **Add** - Select COM groups or individual components that you want to protect

- **Edit** - Edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or COM component.

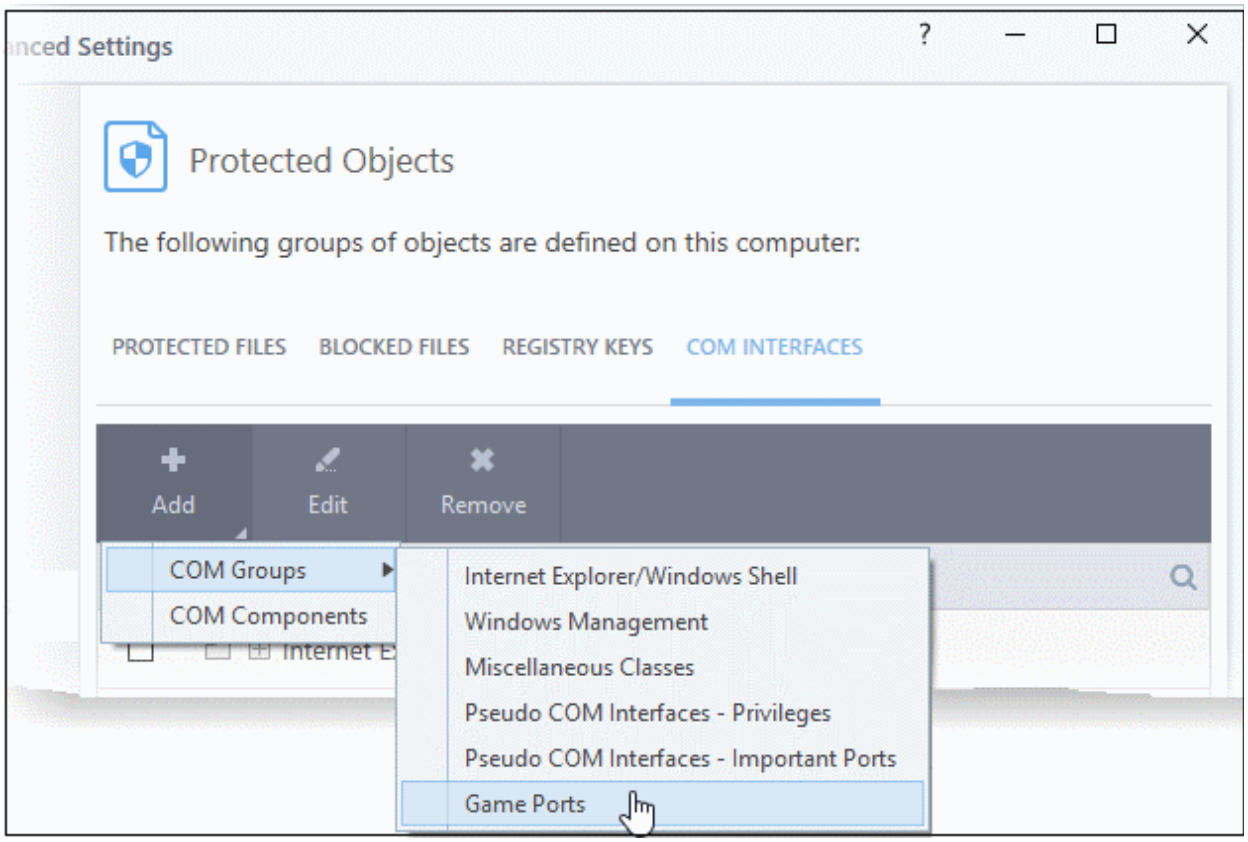
You can search for a specific interface by clicking the magnifying glass icon at the far right of the column header.

Manually add a COM group or individual component

- Click the 'Add' button

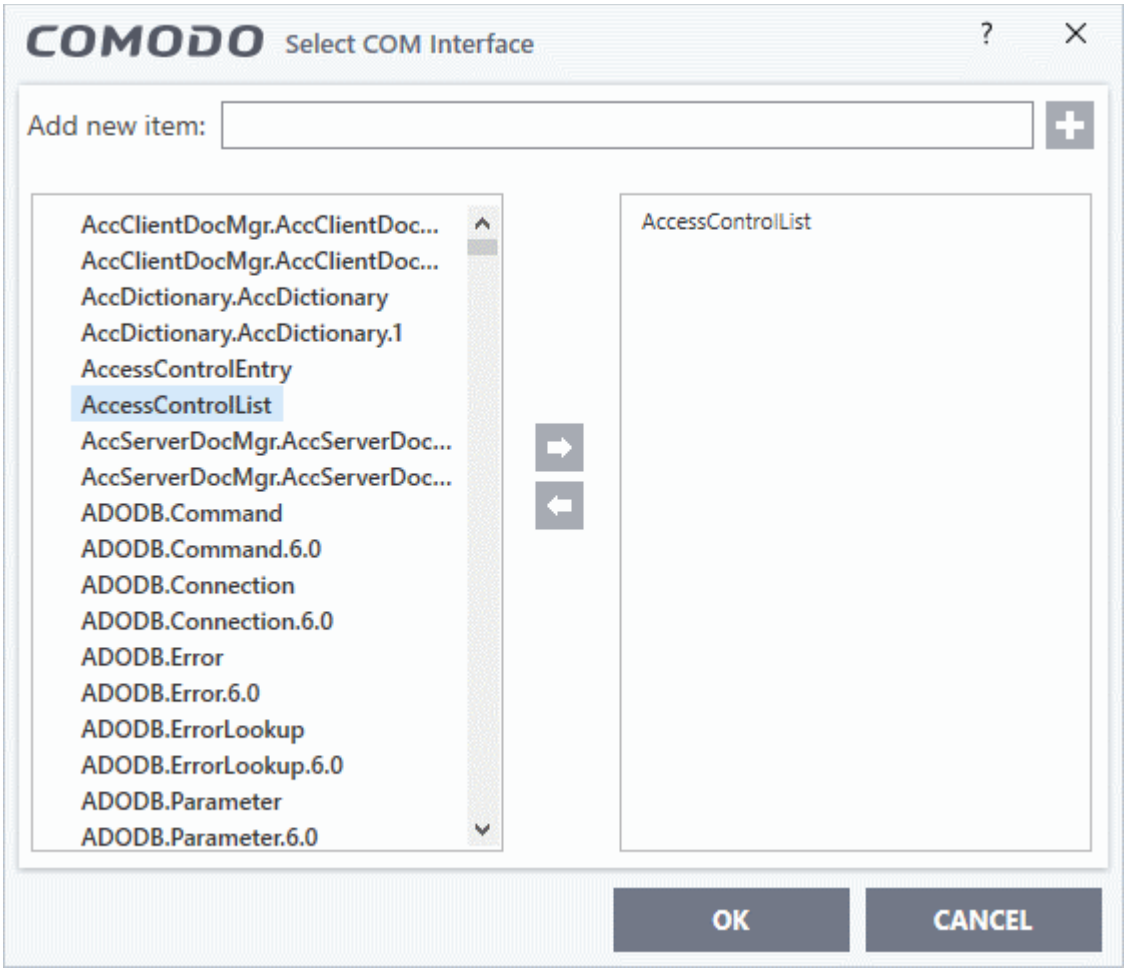
You can add items as follows:

- **Add COM Groups** - Batch select and import predefined groups of important COM components.
  - Click 'Add' > 'COM Groups'
  - Select the group you want to add
  - Click 'OK'



For explanations on editing existing 'COM Groups' and creating new groups, see **COM Groups**.

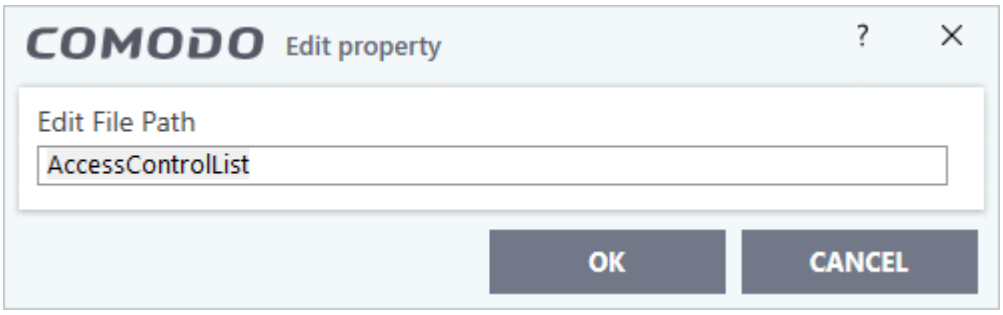
- **Add individual components**
  - Click the 'Add' button then 'COM Components'.
  - Select a component on the left
  - Click the right arrow to add it to the protected list:



- Click 'OK' to add the items to the list

Edit an item in the COM Interfaces protection list

- Select the COM component from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Edit the COM Class file path and click 'OK'

Note: The COM Groups cannot be edited from this interface. You can edit only from **COM Groups** in **HIPS Groups** section.

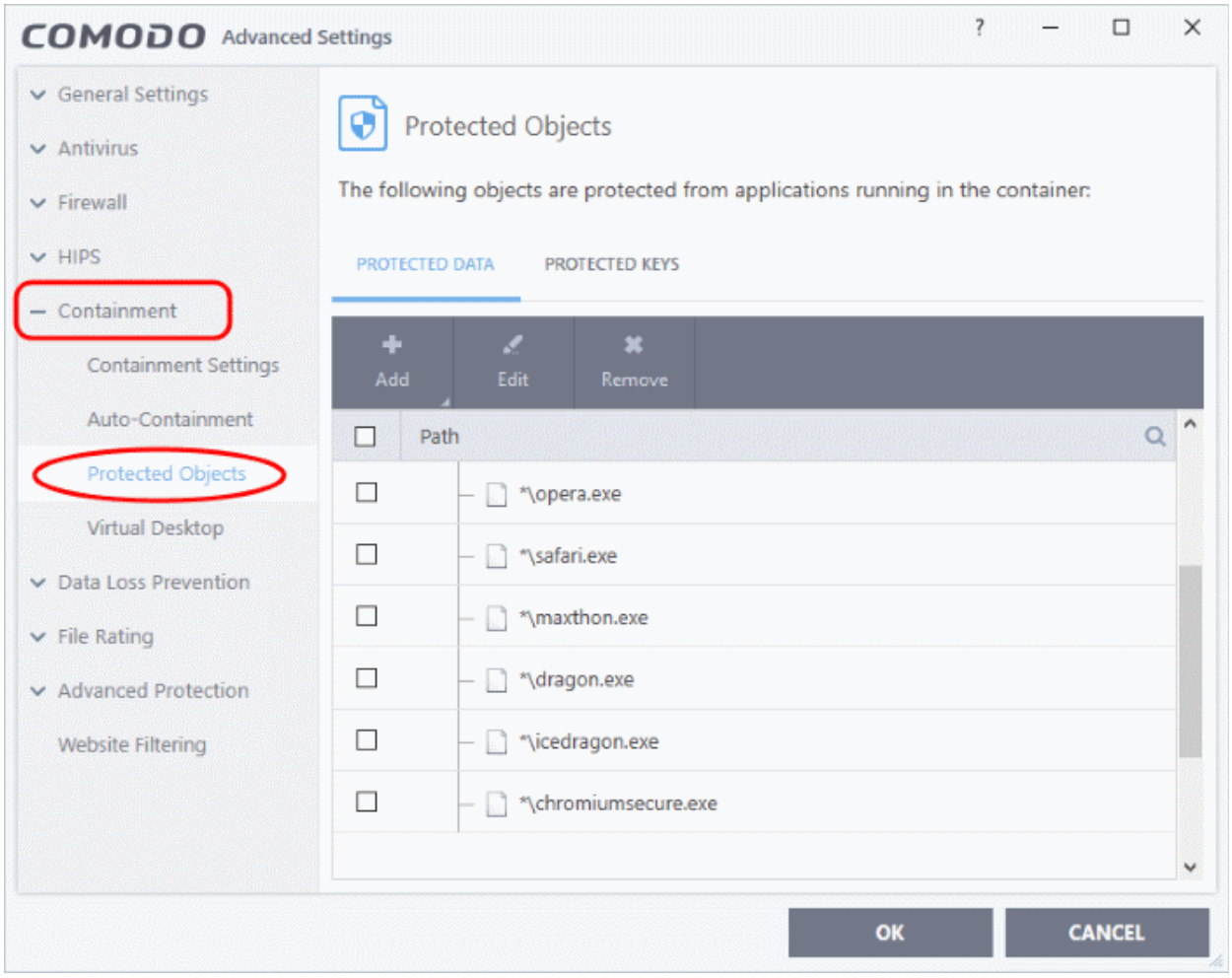
To delete an item from COM Interfaces protection list

- Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the 'COM Interfaces' protection list. CCS will not generate alerts, if the COM component or the group is modified by other programs or processes.

7.5.2. Protected Objects - Containment

- Click 'Settings' > 'Containment' > 'Protected Objects'
- Items that you add to this area cannot be read or modified by applications running in the container.
- Examples items you can add are files, folders and registry keys.
- This prevents unknown/untrusted applications from causing damage to, or stealing data from, important items



Click the following links for more details:

- **Protected Files and Folders**
- **Protected Keys**

7.5.2.1. Protected Files and Folders

- Click 'Settings' > 'Containment' > 'Protected Objects' > 'Protected Data'
- Items in 'Protected Data' cannot be seen, accessed or modified by applications running in the container.
- This fortifies files containing sensitive data from unrecognized and potentially malicious programs.

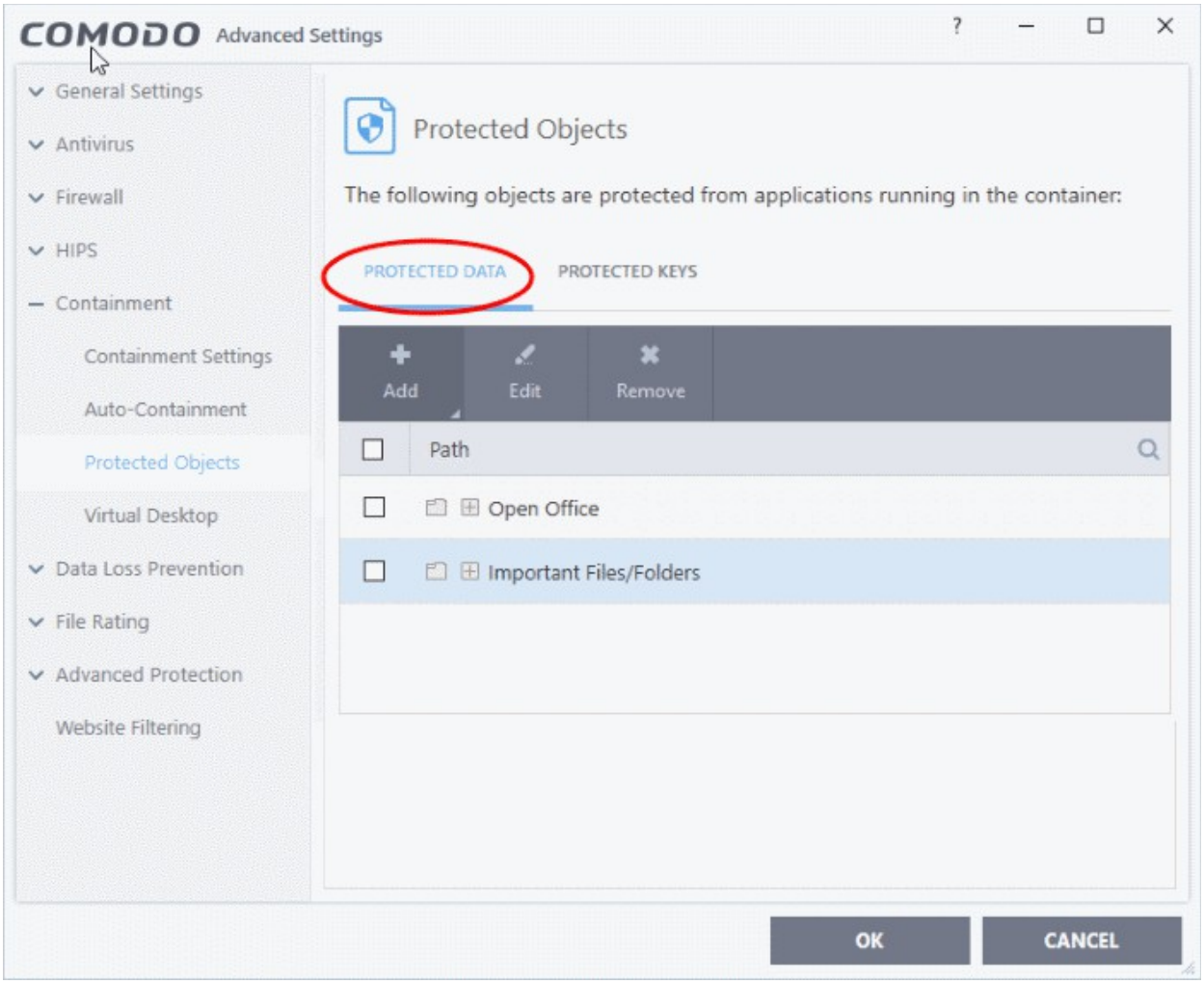
Protected Files versus Protected Data

- Items in '**Protected Files**' ('Settings' > 'HIPS' > 'Protected Objects' > 'Protected Files') can be read by any program, but not modified by them. This contrasts to items in 'Protected Data', which are totally hidden to contained programs.

- If you want a file/folder to be read by other programs, but protected from modification, then add it to 'Protected Files' list.
- If you want to totally conceal an item from contained programs, but allow read/write access to trusted programs, then add it to 'Protected Data'.
- You can add the same item to both areas. This means trusted programs have read-only access to the file, and contained programs have no access rights.

Add and manage protected data

- Click 'Settings' on the CCS home screen.
- Click 'Containment' > 'Protected Objects'
- Select the 'Protected Data' tab

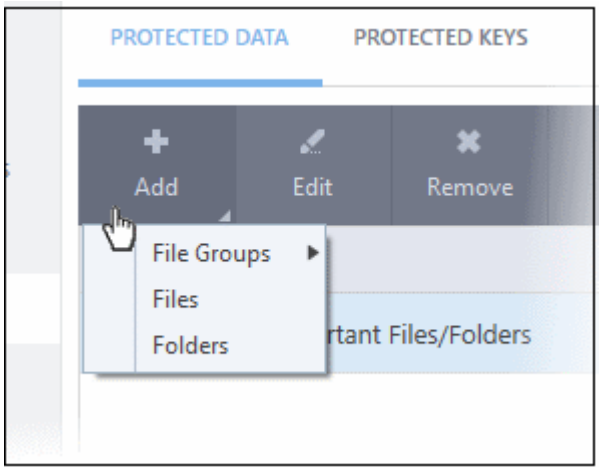


The buttons at the top provide the following options:

- **Add** - Select files/folders that you want to protect
- **Edit** - Modify the path of the file or group.
- **Remove** - Delete the currently highlighted item
- Click the search icon at the far right to search for a specific item

Manually add a file, folder or file group

- Click the 'Add' button

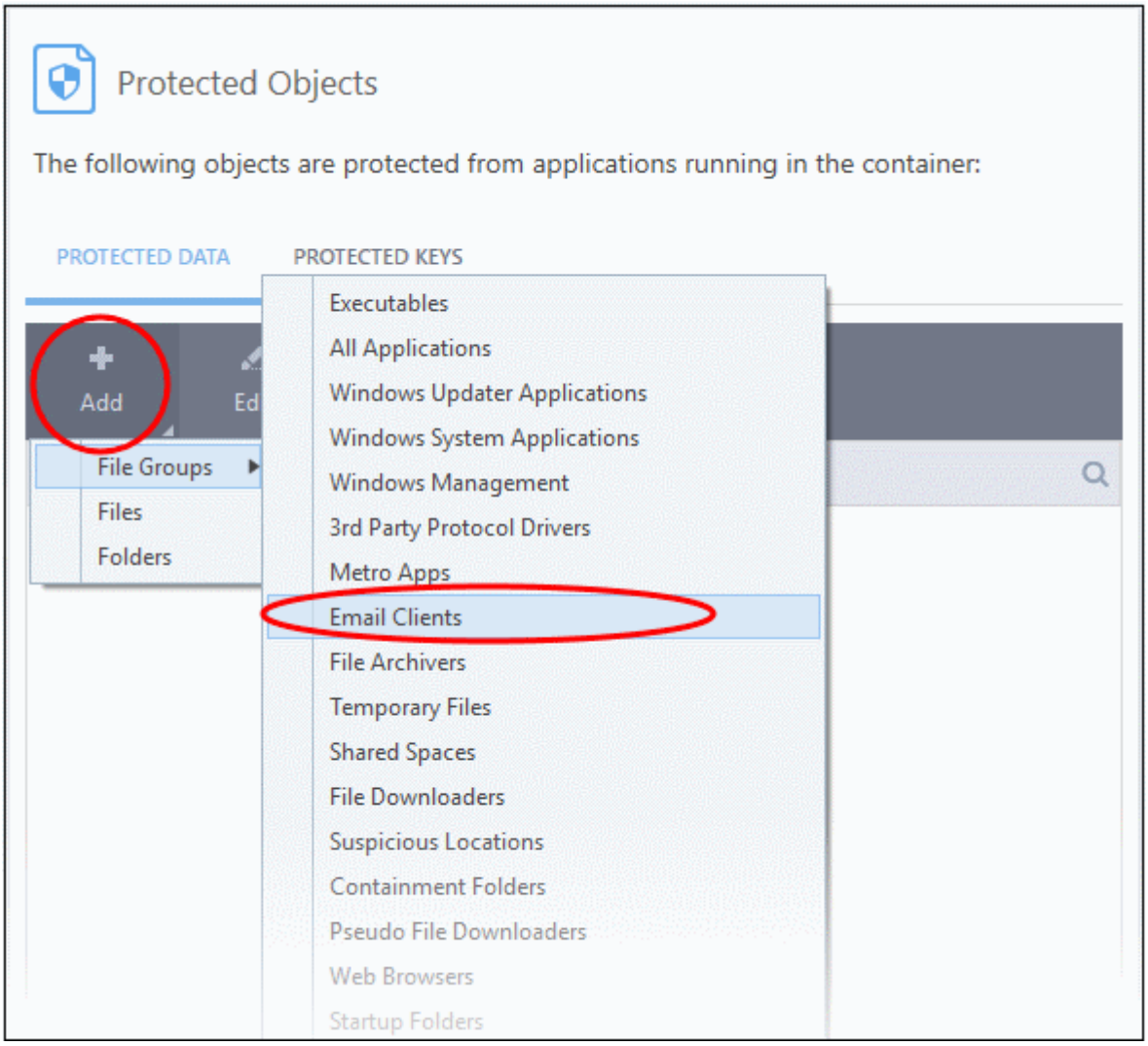


You can add items using any of the following methods:

- **Select from File Groups**
- **Browse to a File**
- **Browse to a Folder**

Add a File Group

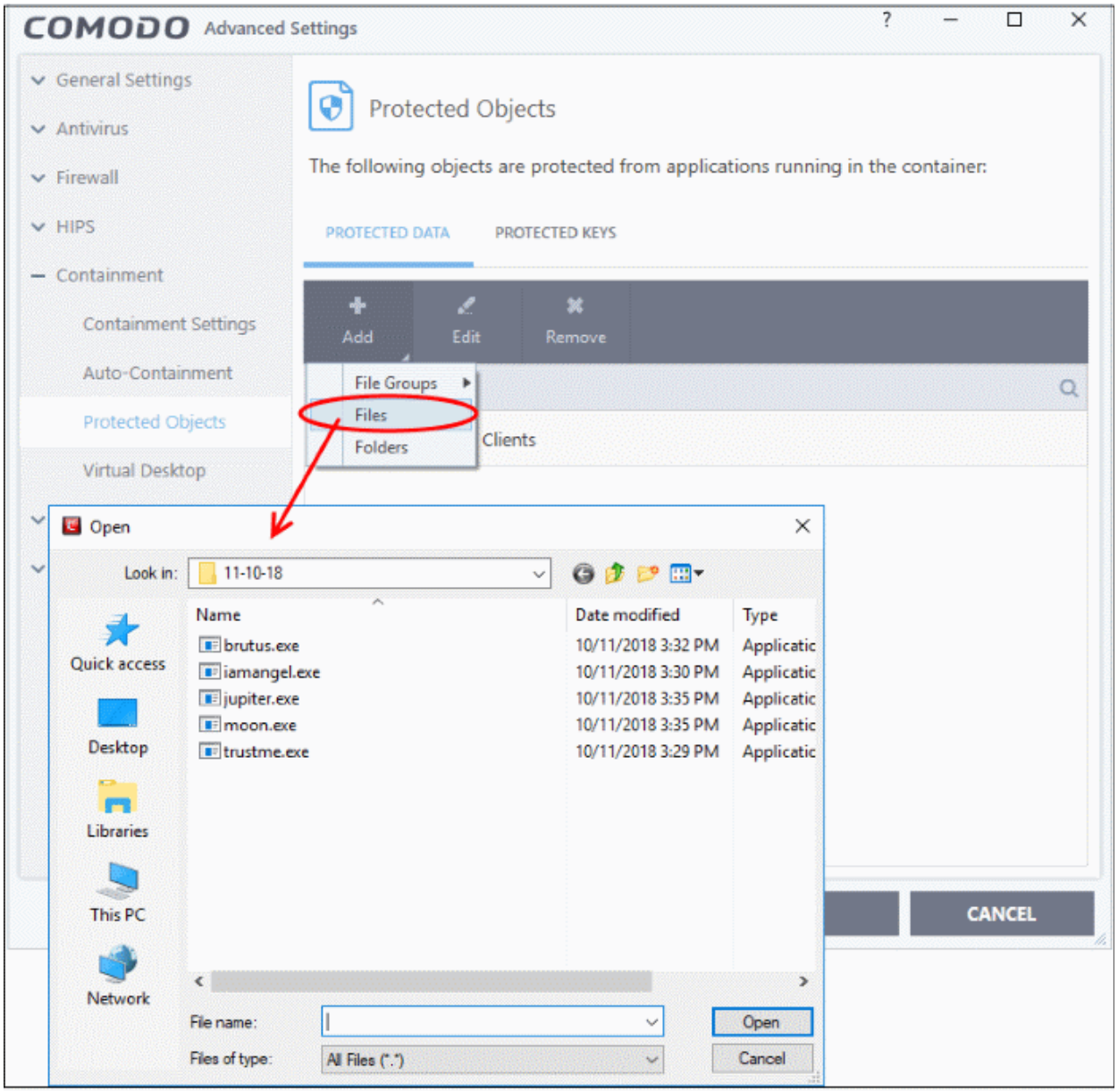
- Choose 'File Groups' from the 'Add' drop-down and select a file group
- CCS ships with a set of predefined 'File Groups' which can be viewed in 'Settings' > 'File Rating' > '**File Groups**'. You can also add your own file groups if required.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' and so on. Each of these provide a fast and convenient way to apply a generic ruleset to important files and folders.



The selected group will be added to the 'Protected Files' list:

Add an Individual File

- Click 'Add' and choose 'Files' from the options:

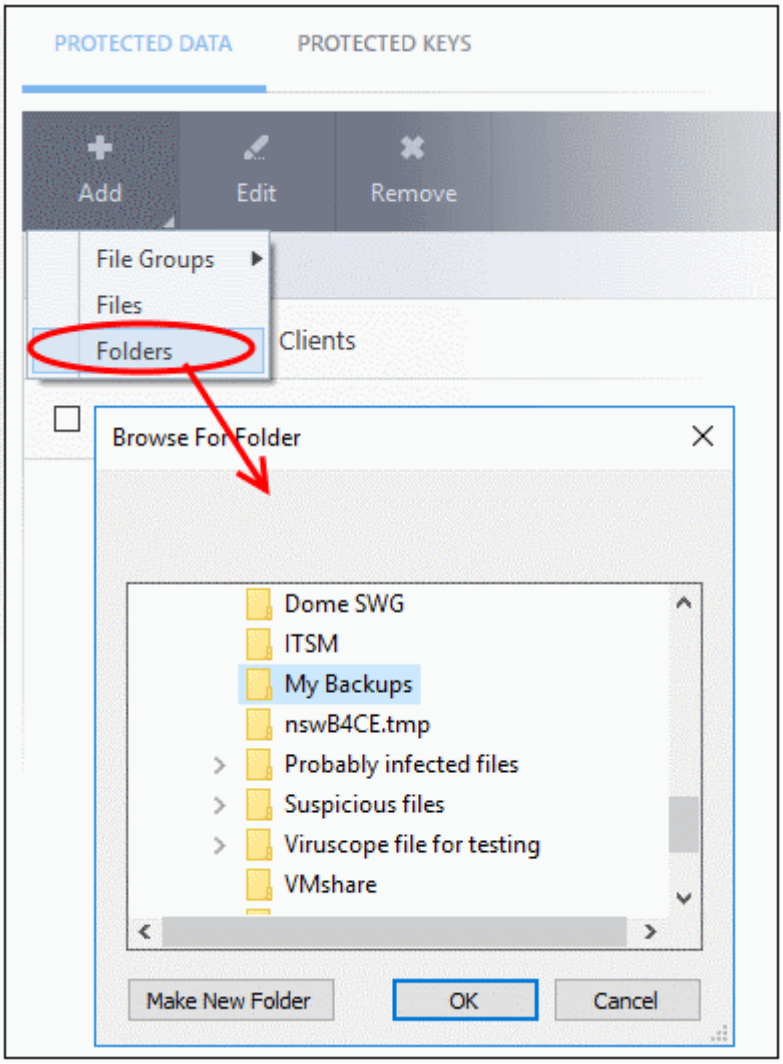


- Navigate to the file you want to add to 'Protected Files' in the 'Open' dialog and click 'Open'

The file will be added to 'Protected Files'.

Add a Drive Partition / Folder

- Click 'Folders' from the 'Add' drop-down.

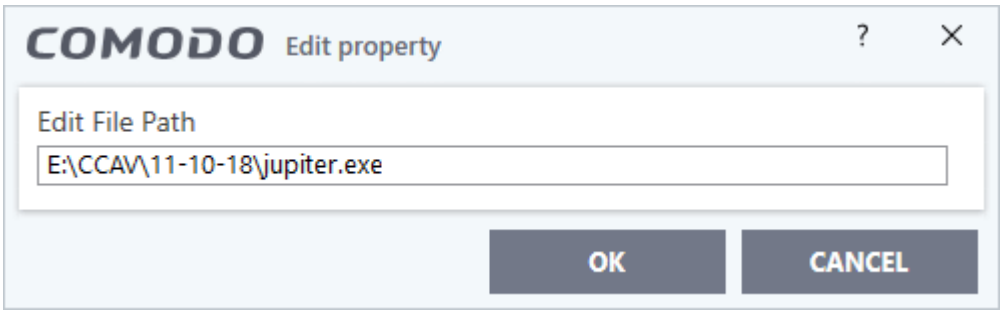


The 'Browse for Folder' dialog will appear.

- Select the folder/drive and click 'OK'. Repeat the process to add more items. The items added to the 'Protected Files' will be protected from programs that are contained.

Edit an item in the Protected Files list

- Select the item from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Update as required and click 'OK'

Delete an item from Protected Files list

- Select the item from the list and click the 'Remove' button

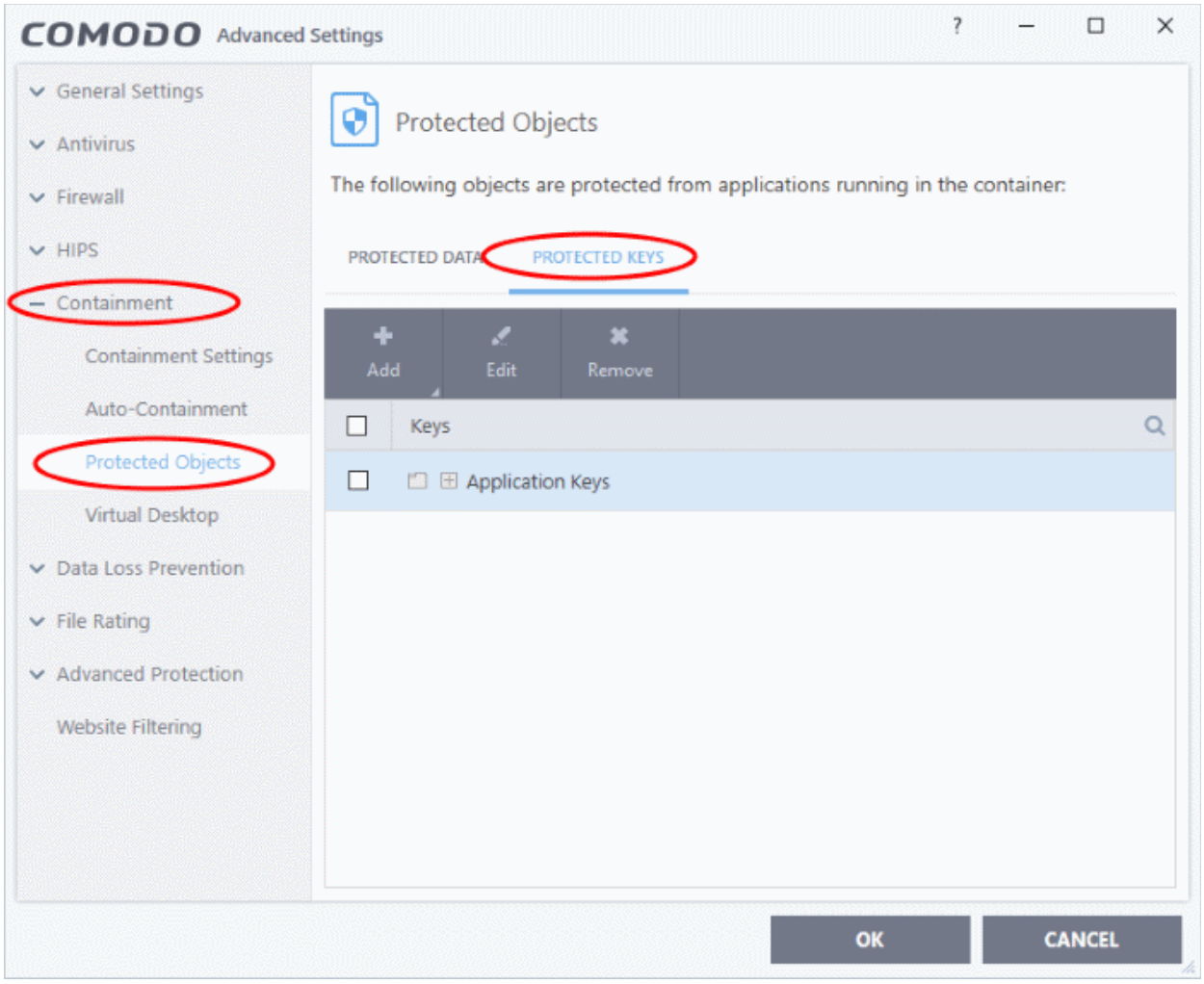
The selected item will be deleted from the protected files list.

7.5.2.2. Protected Keys

- Click 'Settings' > 'Containment' > 'Protected Objects' > 'Protected Keys'
- Registry items in 'Protected Keys' cannot be seen, accessed or modified by applications running in the container.
- Adding important registry keys to this area will protect them from unknown and potentially malicious programs.

Open the 'Protected Keys' section

- Click 'Settings' on the CCS home screen.
- Click 'Containment' > 'Protected Objects'
- Select the 'Protected Keys' tab

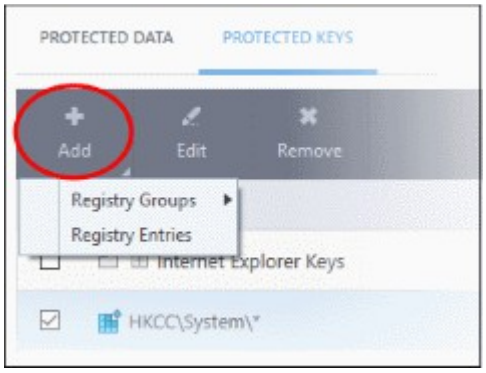


The buttons at the top provide the following options:

- **Add** - Select registry groups or individual keys that you want to protect
- **Edit** - Modify the path of a key or key group
- **Remove** - Delete the currently highlighted item
- Click the search icon at the far-right to search for a specific item

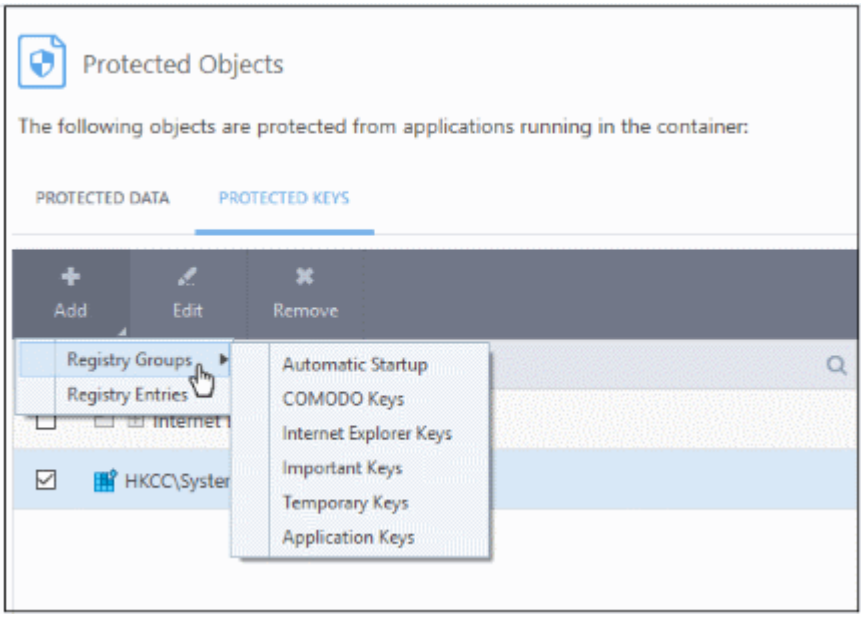
Manually add individual keys or registry groups

- Click the 'Add' button

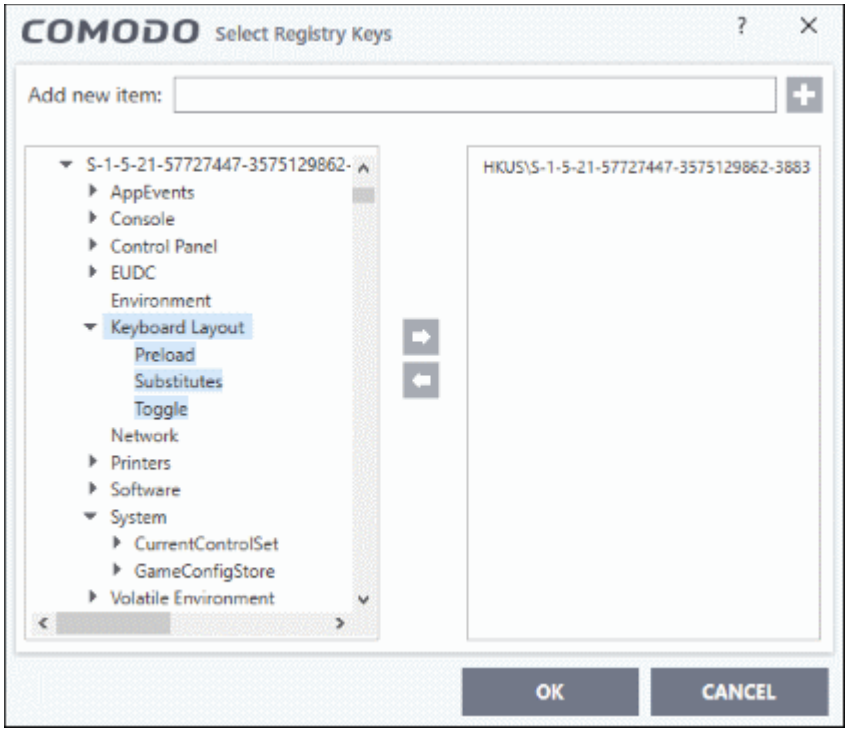


- **Registry Groups** - Select a pre-defined group of important registry keys. CCS ships with the following, pre-defined groups:
  - Automatic Startup keys
  - Comodo Keys
  - Internet Explorer Keys
  - Important Keys
  - Temporary Keys

  You can also create custom groups of the keys you want to protect. See **Registry Groups** in **HIPS Groups** if you want help on this.
  - Click the 'Add' button > 'Registry Groups' > Select a key group from the list > Click 'OK'



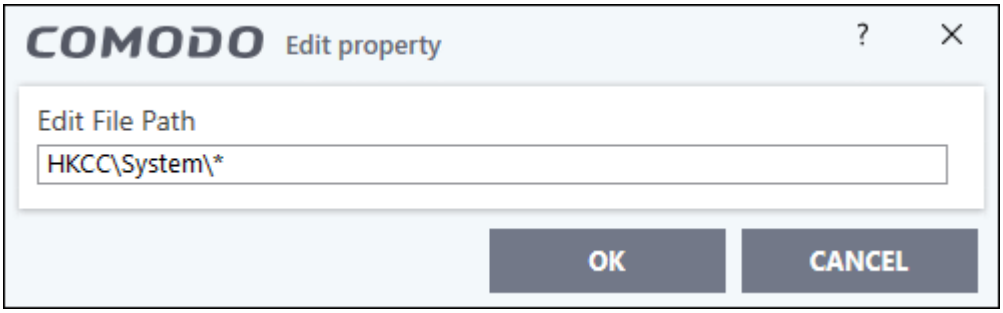
- **Registry Entries** - Add individual keys to the protected list
  - Click 'Add' > 'Registry Entries'
  - Select the keys you want to protect in the left-pane
  - Click the right-arrow to move them to the protected list:



- Alternatively, you can type the key name in the field at the top then click the '+' button
- Click OK. All items in the right pane will be added to the protected keys list

Edit an item in the list

- Select the key from the list and click the 'Edit' button. The 'Edit Property' dialog will appear.



- Update as required and click 'OK'

Note: Click 'Settings' > 'HIPS' > 'HIPS groups' > 'Registry Groups' to edit registry groups.
See **Registry Groups** if you need more help.

Delete an item from Registry Protection list

- Select the item from the list and click the 'Remove' button.

The selected item will be deleted from the protected register list.

7.6. Data Loss Prevention

Click 'Settings' > 'Data loss prevention'

- The data loss prevention (DLP) section lets you identify and control the movement of sensitive data from your device.

There are three components:

DLP Monitoring Rules

- Rules which allow or block files copied to USB and other storage devices.
- Monitoring rules are created by your Endpoint Manager administrator and added to the EM profile applied to your device. You can view the monitoring rules active on your device from the CCS interface.

DLP Discovery Rules

- Rules which scan your computer for files which contain sensitive information. For example, The rules can search for credit card numbers, social security numbers, bank routing numbers etc.
- Discovery rules are created by your Endpoint Manager administrator and added to the EM profile applied to your device. You can view the rules active on your device from the CCS interface.
  - Click 'Tasks' > 'DLP Tasks' > 'Data Loss Prevention Scan' to run DLP scans to identify the files containing sensitive information defined in the rules
  - See **Run Data Loss Prevention Scans** for help to run scans and view results

DLP Keyword Groups

- A keyword group is a list of search-terms. For example, the 'Names' group is a list of common first names and surnames.
- Keyword groups are used in the construction of DLP discovery rules.
- The 'Names' group must be populated in order for many of the patterns in a discovery rule to work.
- Keyword groups are created by your Endpoint Manager administrator at the portal. You can view the keywords added to the groups from the CCS interface.

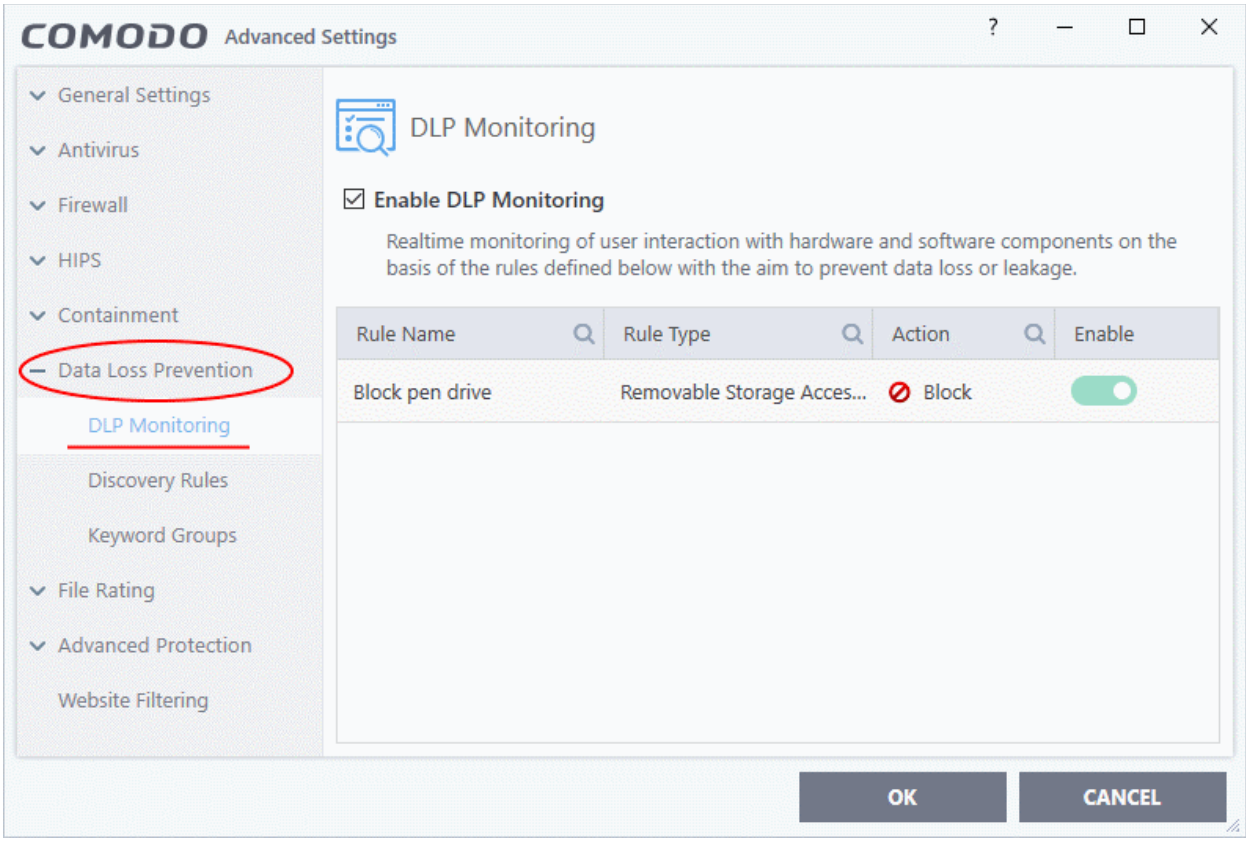
7.6.1. DLP Monitoring Rules

Click 'Settings' > 'Data Loss Prevention' > 'DLP Monitoring'

- DLP monitoring rules allow or block copying files to external storage devices.
- Monitoring rules are configured by your Endpoint Manager admin. Rules are applied to your device by adding them to the EM profile active on your device.
- CCS continuously monitors attempted data transfers to devices like USB drives and allows/blocks the transfer as per the rules in real time. The the following storage devices are covered:
  - USB Data Devices like pen drives
  - External HDDs /SSDs
  - USB connected external optical disk drives (CD/DVD)
  - SD, Micro SD Cards, SDXC-SDHC cards
  - eSata removable drives
  - FireWire connected devices
  - Devices using MTP protocol
- You can view the log details in CCS Logs.
  - Click 'Logs' on the top and select 'Data Loss Prevention Events' in the 'Show' drop-down'
  - See **Data Loss Prevention Event Logs** to read more about DLP logs
- The 'DLP Monitoring' interface shows you the monitoring rules active on your device.

View DLP monitoring rules

- Click 'Settings' on the CCS home screen.
- Click 'Data Loss Prevention' > 'DLP Monitoring'



- See the online help page at **https://help.comodo.com/topic-399-1-786-10262-Create-DLP-Monitoring-Rules-and-Add-Them-to-Profiles.html** to read more about configuring monitoring rules in Endpoint Manager portal.

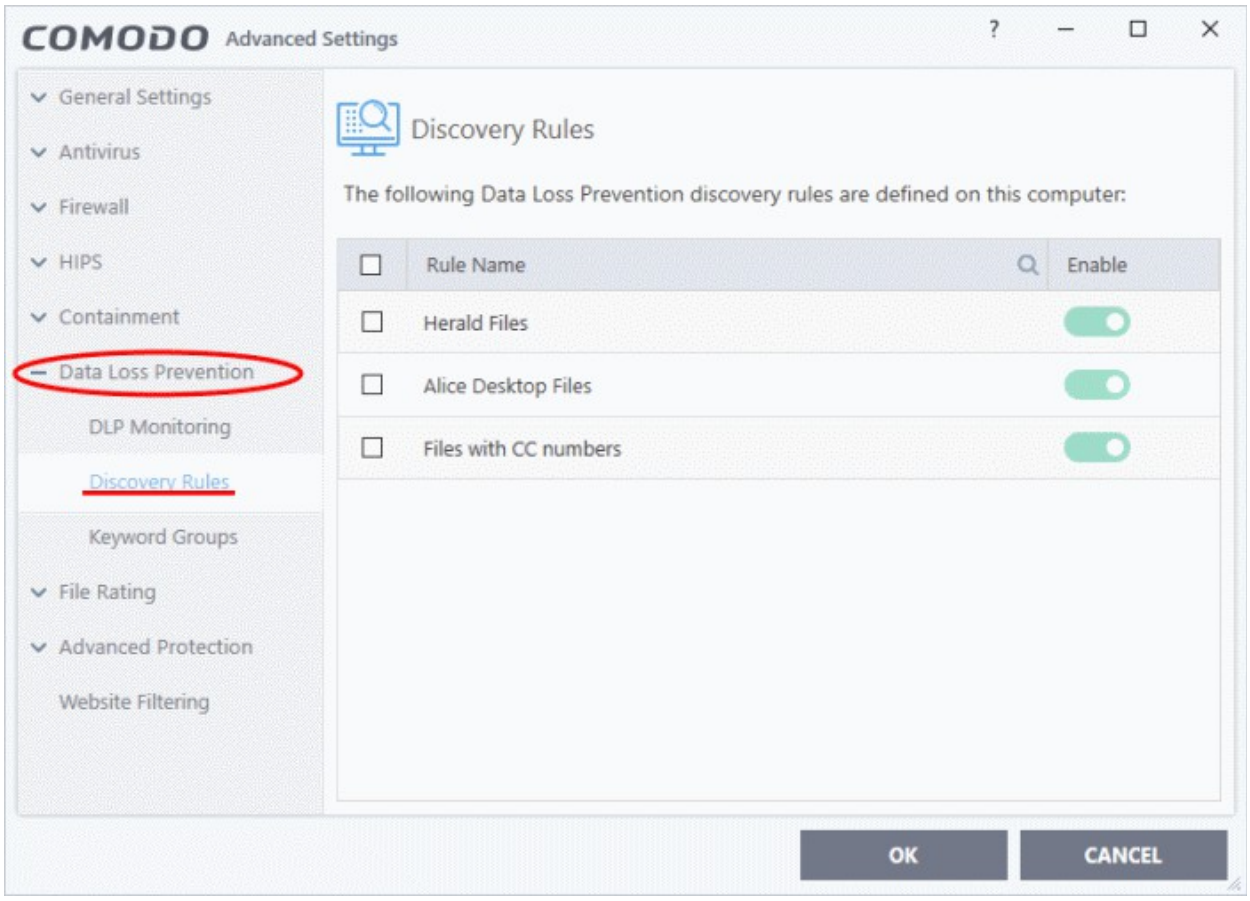
7.6.2. DLP Discovery Rules

Click 'Settings' > 'Data Loss Prevention' > 'Discovery Rules':

- Discovery rules are used to identify files containing sensitive information like credit card numbers, social security numbers, bank account numbers and so on.
- Each rule defines the areas to scan, the type of information to search for, and the action to take on discovered files.
- You can run DLP scans to discover the files containing sensitive information as defined in the rules
  - Click 'Tasks' > 'DLP Tasks' > 'Data Loss Prevention Scan' to run a scan
  - See **Run Data Loss Prevention Scans** for help to run DLP discovery scans and view the files identified by the scans.
- Discovery rules are configured by your Endpoint Manager admin. Rules are applied to your device by adding them to the EM profile active on your device.
- The 'Discovery Rules' interface shows the discovery rules active on your device.

View discovery rules

- Click 'Settings' on the CCS home screen.
- Click 'Data Loss Prevention' > 'Discovery Rules'



- See the online help page at **https://help.comodo.com/topic-399-1-786-15419-Create-DLP-Discovery-Rules-and-Add-them-to-Profiles.html** to read more about configuring discovery rules in Endpoint Manager portal.

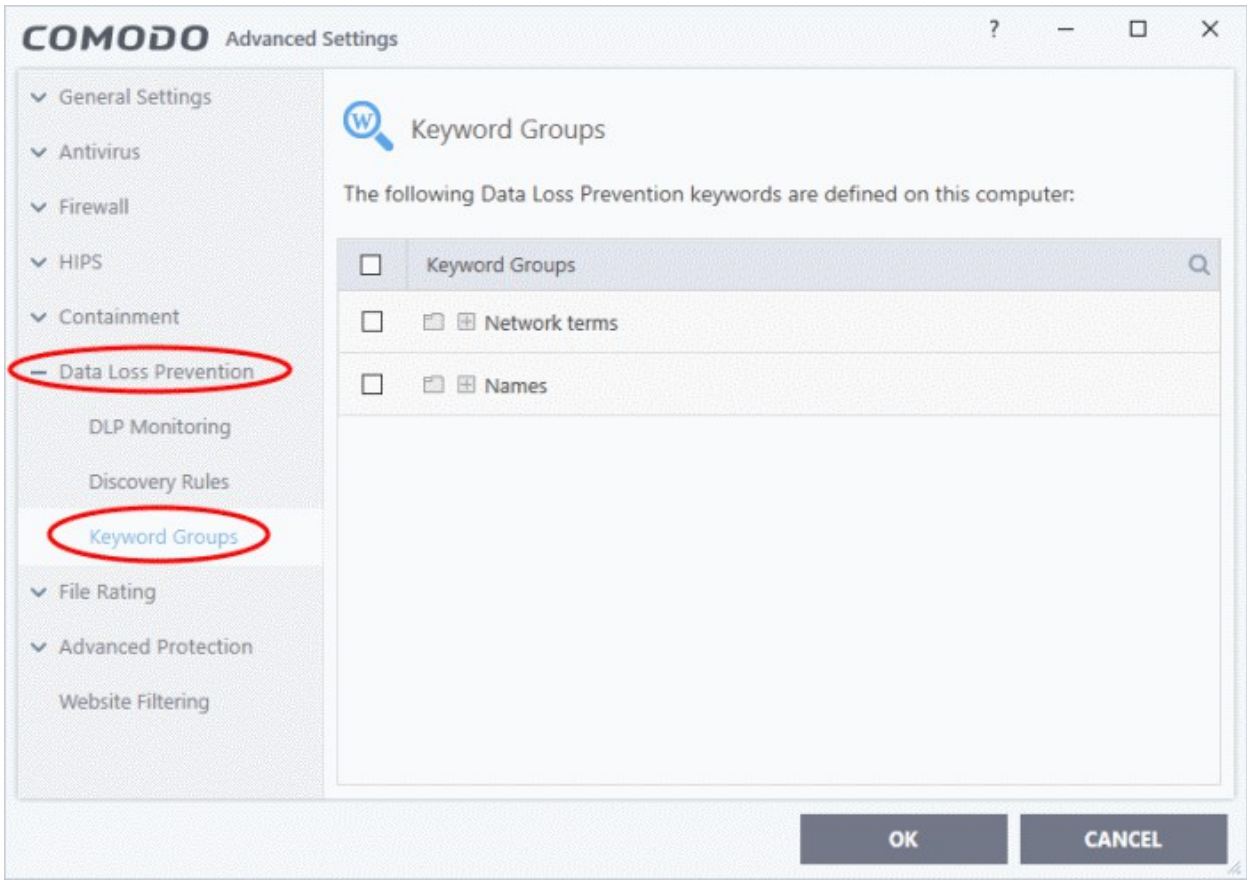
7.6.3. DLP Keyword Groups

Click 'Settings' > 'Data Loss Prevention' > 'Keyword Groups'

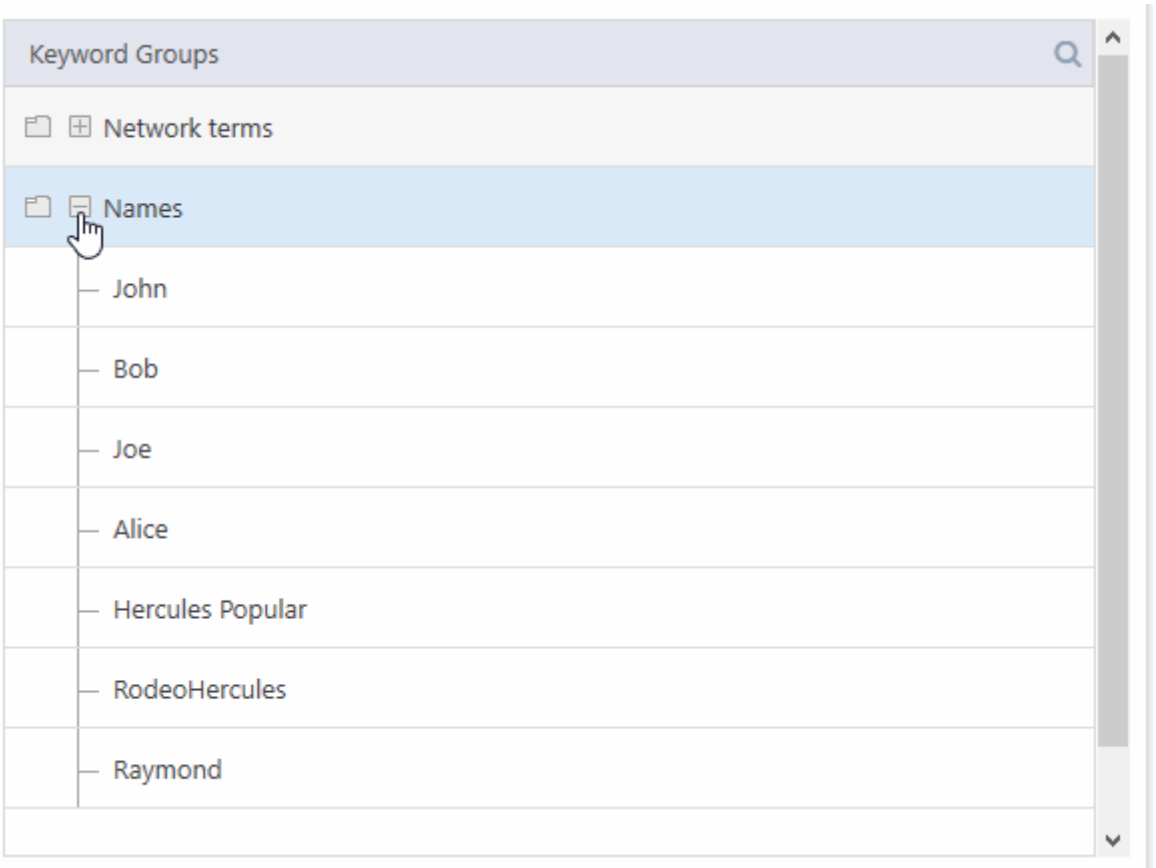
- Keyword groups are used by DLP rules to identify sensitive data. They are a list of specific items which the scan searches for. For example, the 'Names' group is a list of common first names and surnames.
- Keyword groups are used in combination with an 'information format' to form a 'pattern'. An information format is the notation used by the type of data you want to find. For example, the information format of an SSN is a nine digit number in a 3-2-4 formation, like '123-45-6789'.
- The information formats are used in discovery rules to specify the type of sensitive information to be identified by a rule.
- Keyword groups are configured by your Endpoint Manager admin.
- The 'Keyword Groups' shows the available keyword groups and entries in each group.

View keyword groups

- Click 'Settings' on the CCS home screen.
- Click 'Data Loss Prevention' > 'Keyword Groups'



- Click the '+' icon to expand a group and view its entries:

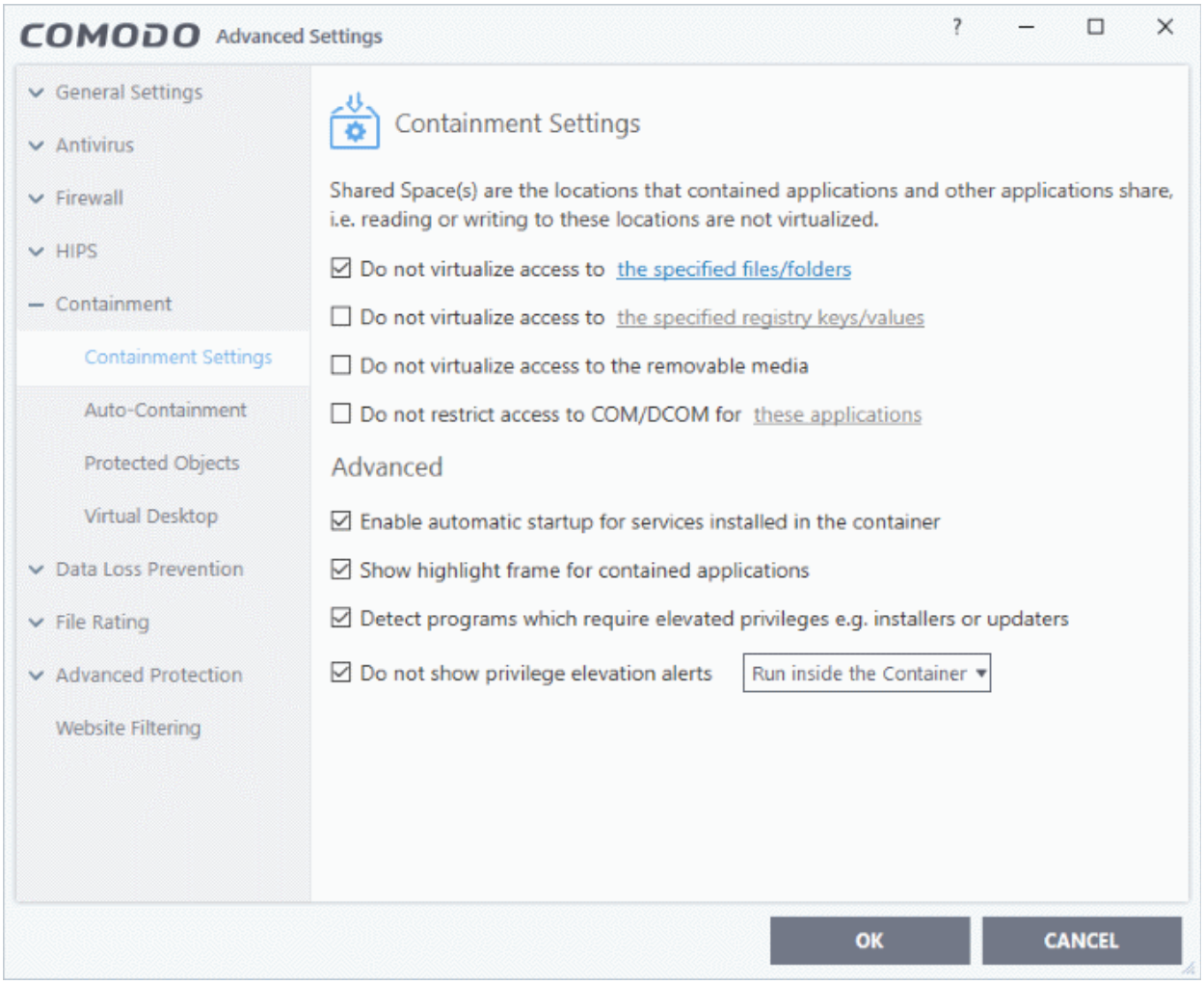


- See the online help page at **https://help.comodo.com/topic-399-1-786-15423-View-and-Manage-**

Keyword-Groups.html to read more about configuring keyword groups in Endpoint Manager portal.

7.7. Containment Settings

- Click 'Settings' > 'Containment' to open this interface.
- If CCS encounters a file that has a trust status of 'Unknown' then you have the option to automatically run that file in the container.
- The container is a secure, virtual environment where unknown files can run, but cannot affect the rest of your computer.
  - Files in the container are isolated from other processes, write to a virtual file system and registry, and cannot access your user data.
- Shared Space - Because applications in the container cannot save files to your local file system, CCS creates a special folder at 'C:\ProgramData\Shared Space' for you to save files from the container. You can access files in this folder from your local desktop.
- If required, you can also allow contained applications save files to external storage devices. For example, to USB sticks and external storage drives.
- The containment settings area lets you configure all aspects of the container:



See the following sections for more help:

- **Containment Settings** - Configure exceptions to virtualization and other general settings
- **Auto-Containment Rules** - Create and manage rules which tell CCS how to handle unknown files.

- **Protected Objects - Containment** - Define files, folders and registry keys which cannot be accessed by applications running in the container.
- **Virtual Desktop Settings** - Configure options related to the Virtual Desktop application.
- **Containment - An Overview** - Background information about the containment process
- **Unknown Files: The Scanning Processes** - Background information on how CCS determines the reputation of a file.

Note: The containment feature is not supported on the following platforms:

- Windows XP 64 bit
- Windows Server 2003 64 bit

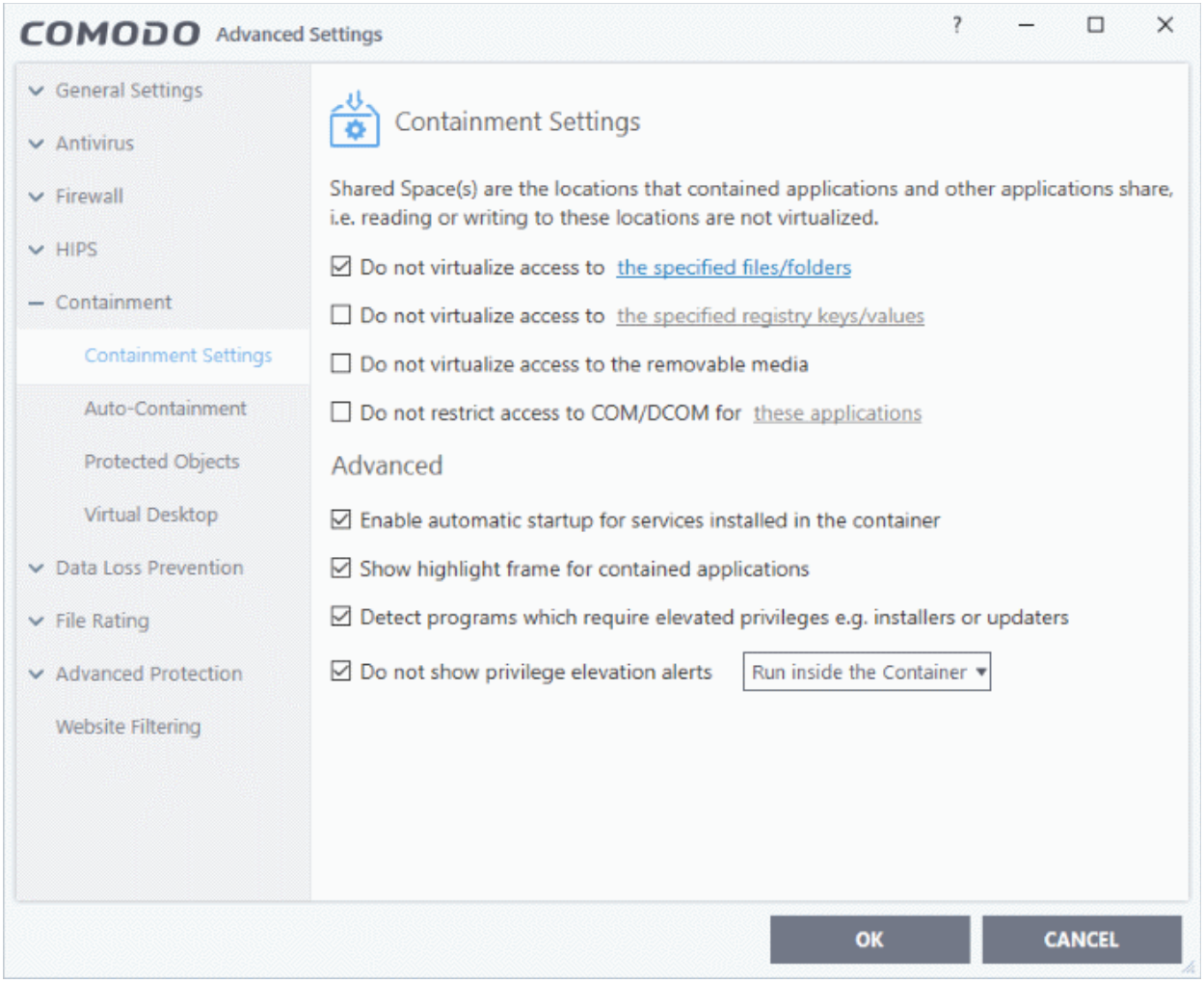
7.7.1. Containment Settings

- Click 'Settings' > 'Containment' > 'Containment Settings'.

The settings area lets you configure how proactive the auto-containment feature should be, and which types of files it should check.

Configure containment settings

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Containment Settings'

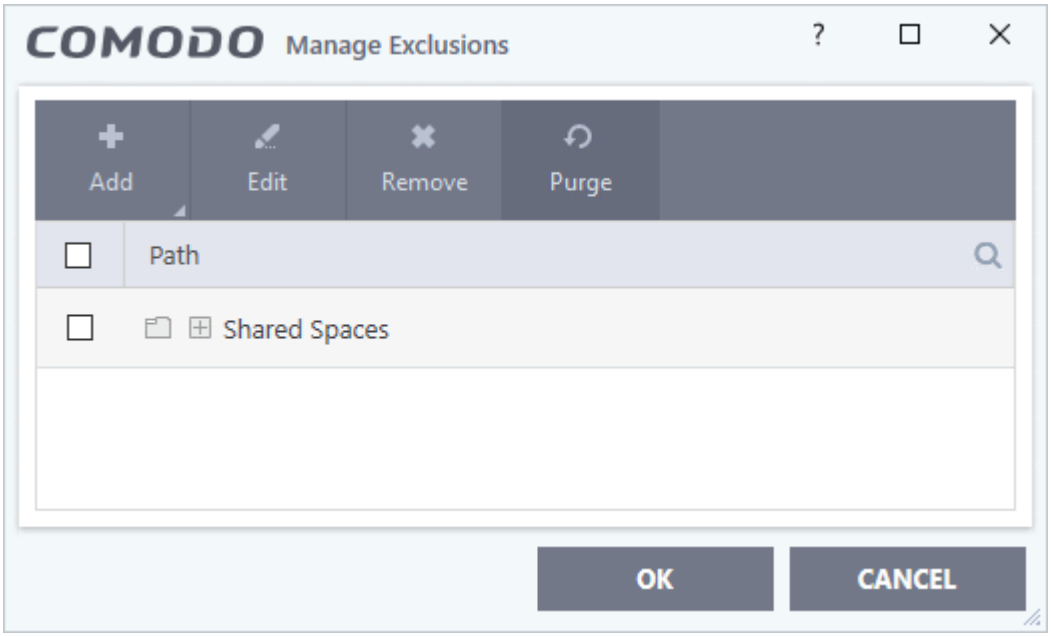


- By default, contained applications can access folders, files and registry keys on your local system, but cannot make changes to them.

- Contained apps are also prevented from accessing Component Object Model (COM) and Distributed Component Object Model (DCOM) components on your computer
- The settings screen lets you create exceptions to these policies if required.
- You can also allow contained applications to access removable storage like USB sticks and external hard disk drives.

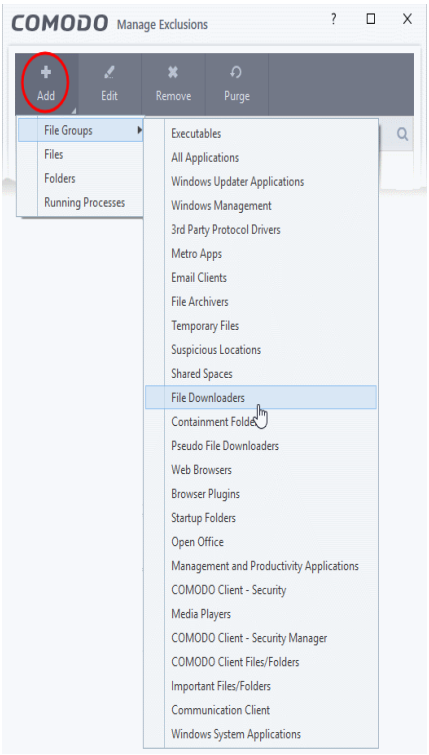
Do not virtualize access to the specified files/folders - Specify files/folders on the host computer that contained applications are allowed to write to. By default, contained applications write to a virtual file system, and cannot access files/folders on the host system.

- Select the option then click 'the specified files/folders' link.
- The 'Manage Exclusions' dialog shows files and folders that can be modified by contained applications. By default, 'Shared Space' is the only folder they can write to:



Define an exception:

- Click the 'Add' button in the 'Manage Exclusions' dialog:

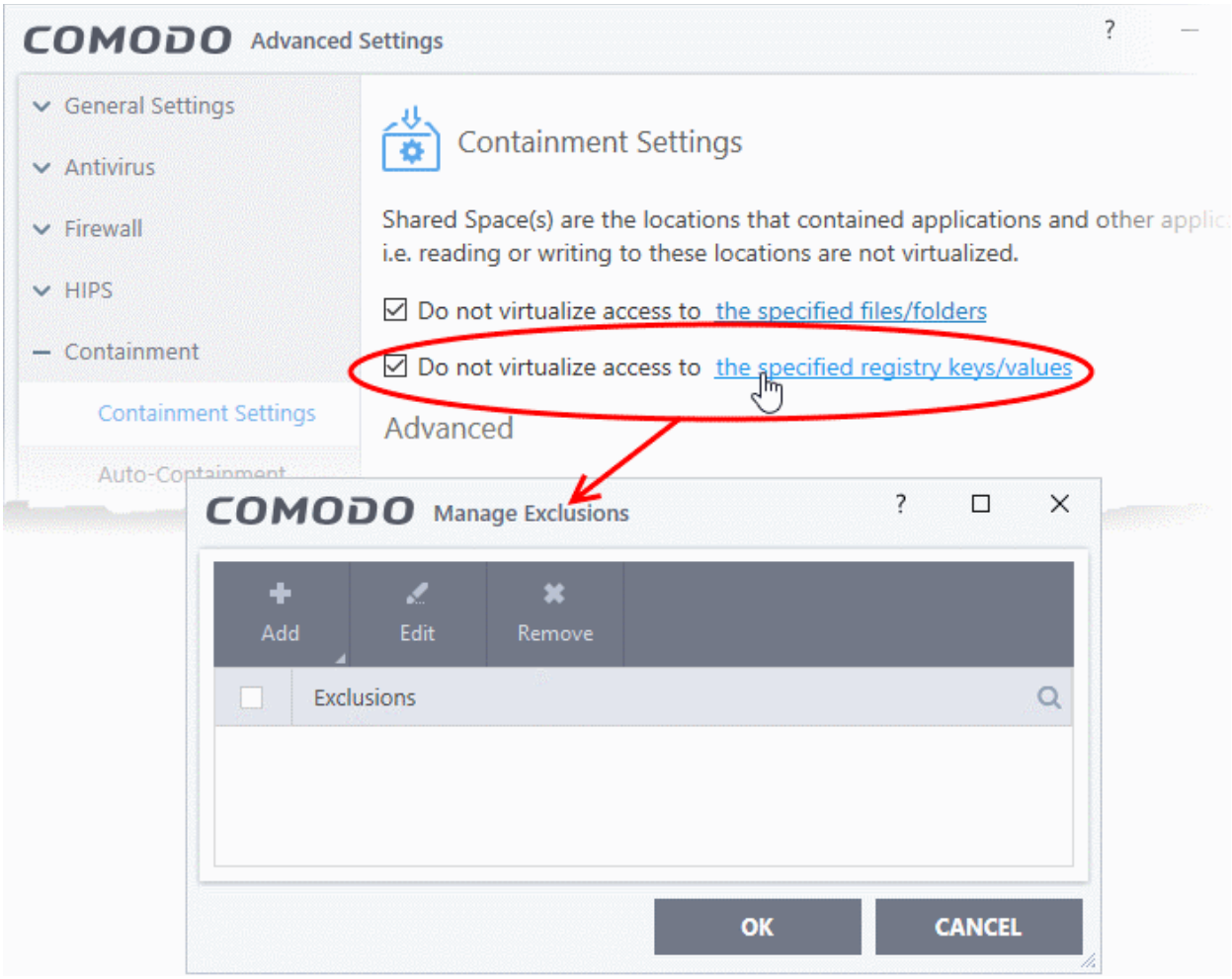


- **File Groups** - Choose a category of files or folders to which access should be granted. For example, select 'Executables' to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd. See '**File Groups**', for more details on file groups.
- **Files** - Pick specific files or applications that contained applications can access
- **Folders** - Specify folders that can be accessed by contained applications. Access is granted to all files in the folder.
- **Running Processes** - Choose a process currently running on your computer. The parent application of the process is added to the exclusions.

- **Edit** - Select an item and click 'Edit' to change the target file or folder
- **Remove** - Select an item and click 'Remove' to delete an exception
- **Purge** - Checks that all files and folders covered in exceptions are still present on your computer. Purge automatically removes any items it can no longer locate.
- Click 'OK' to implement your settings

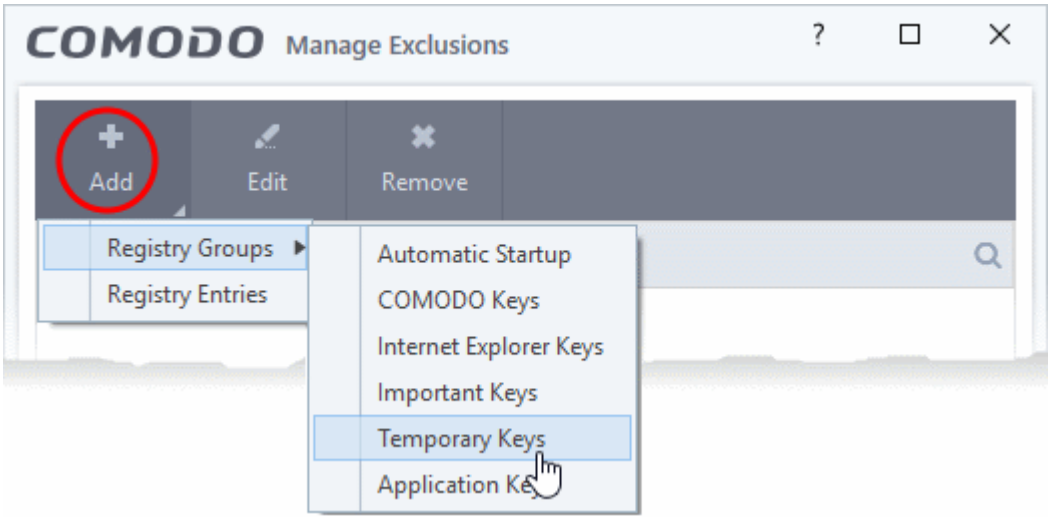
Do not virtualize access to the specified registry keys/values - Specify registry keys on the host computer that contained applications are allowed to write to. By default, contained applications write to a virtual registry, and cannot access the real registry on the host system.

- Select the option then click 'the specified registry keys/values' link.
- The 'Manage Exclusions' dialog shows keys which you have allowed contained applications to access:

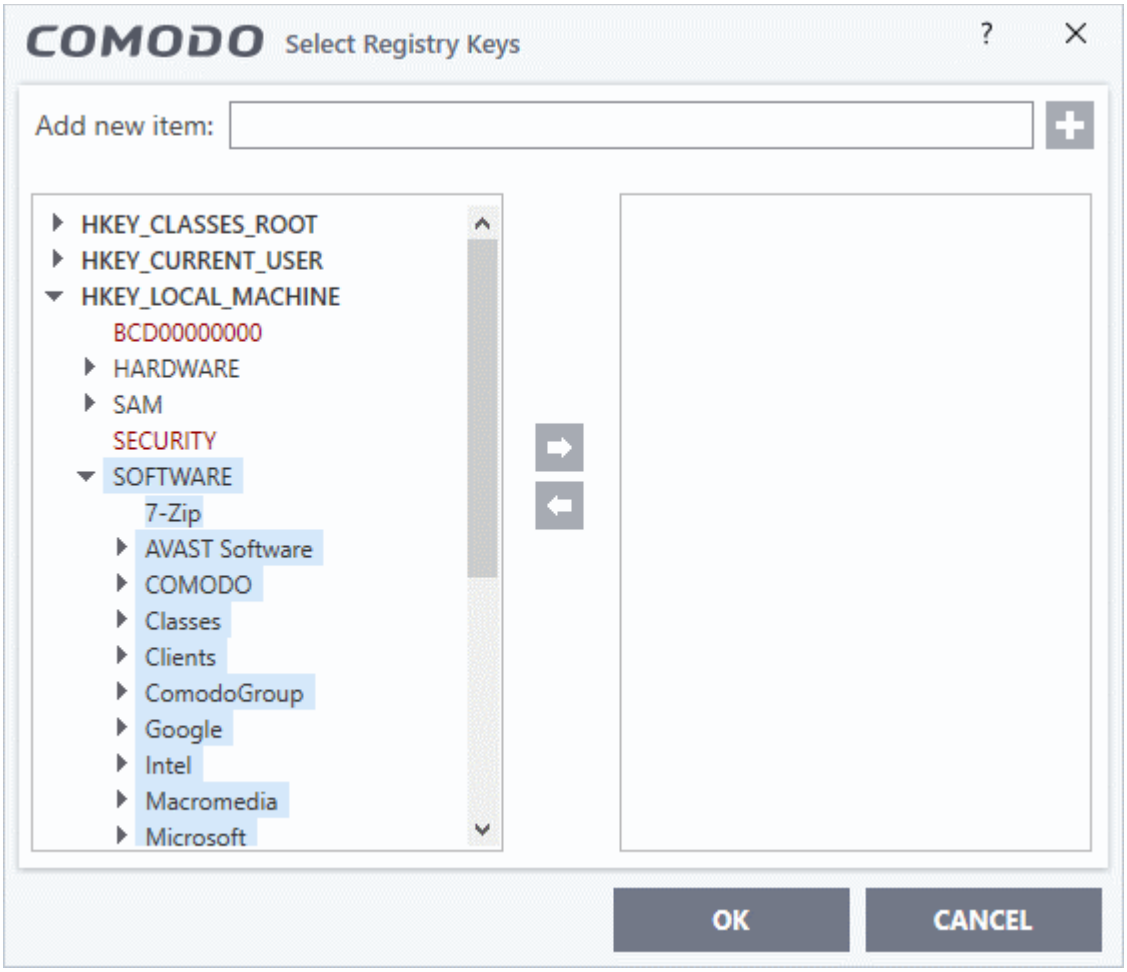


Add a registry key exception:

- Click the 'Add' button in the 'Manage Exclusions' dialog.



- **Registry Groups** - Batch select a predefined group of important registry keys as exclusions. See '**Registry Groups**' for an explanation of registry groups defined in CCS.
- **Registry Entries** - Browse to individual Windows registry keys and add them as exclusions:

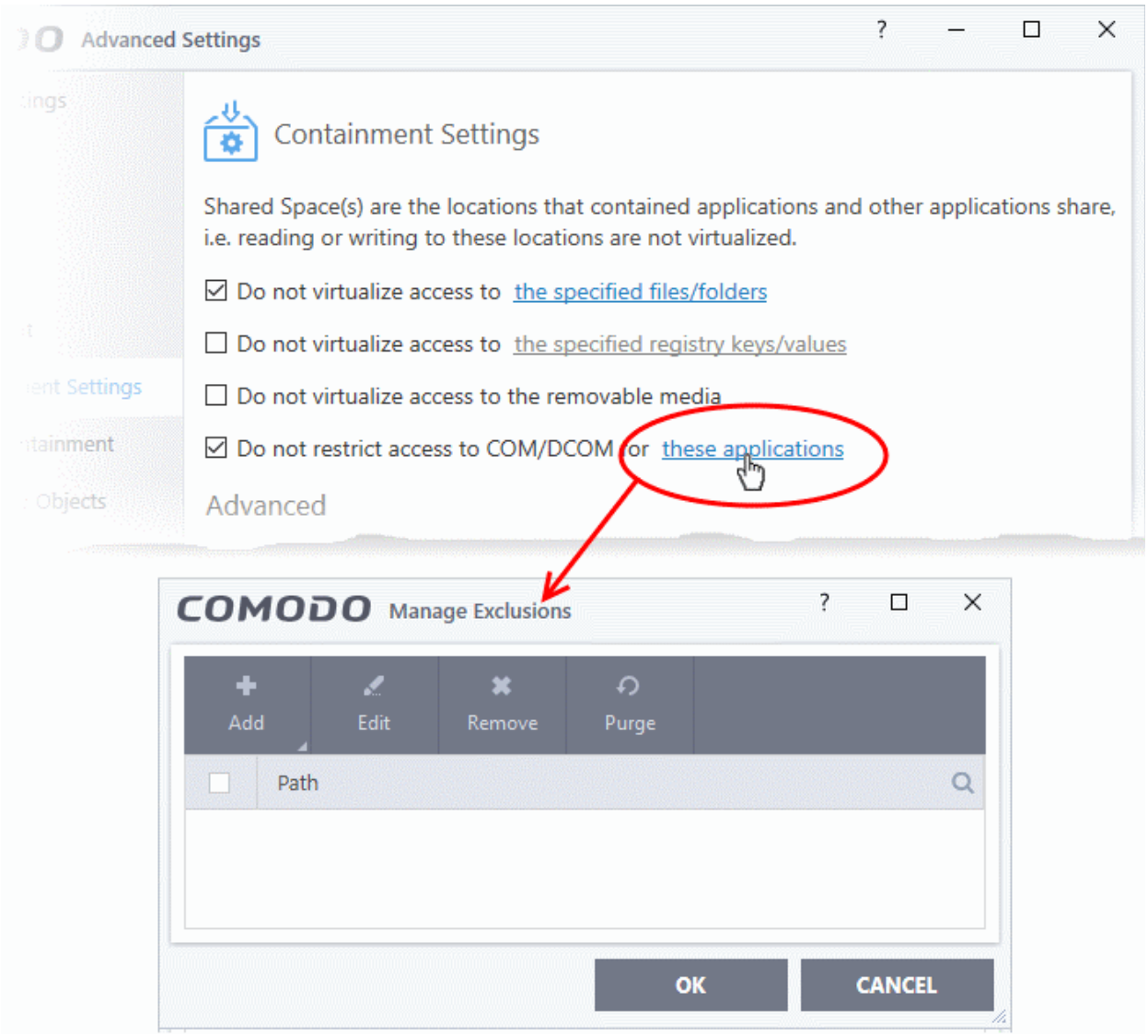


- **Edit** - Select an item and click 'Edit' to change the target path
- **Remove** - Select a key or group and click 'Remove' to delete the exception
- Click 'OK' to implement your settings

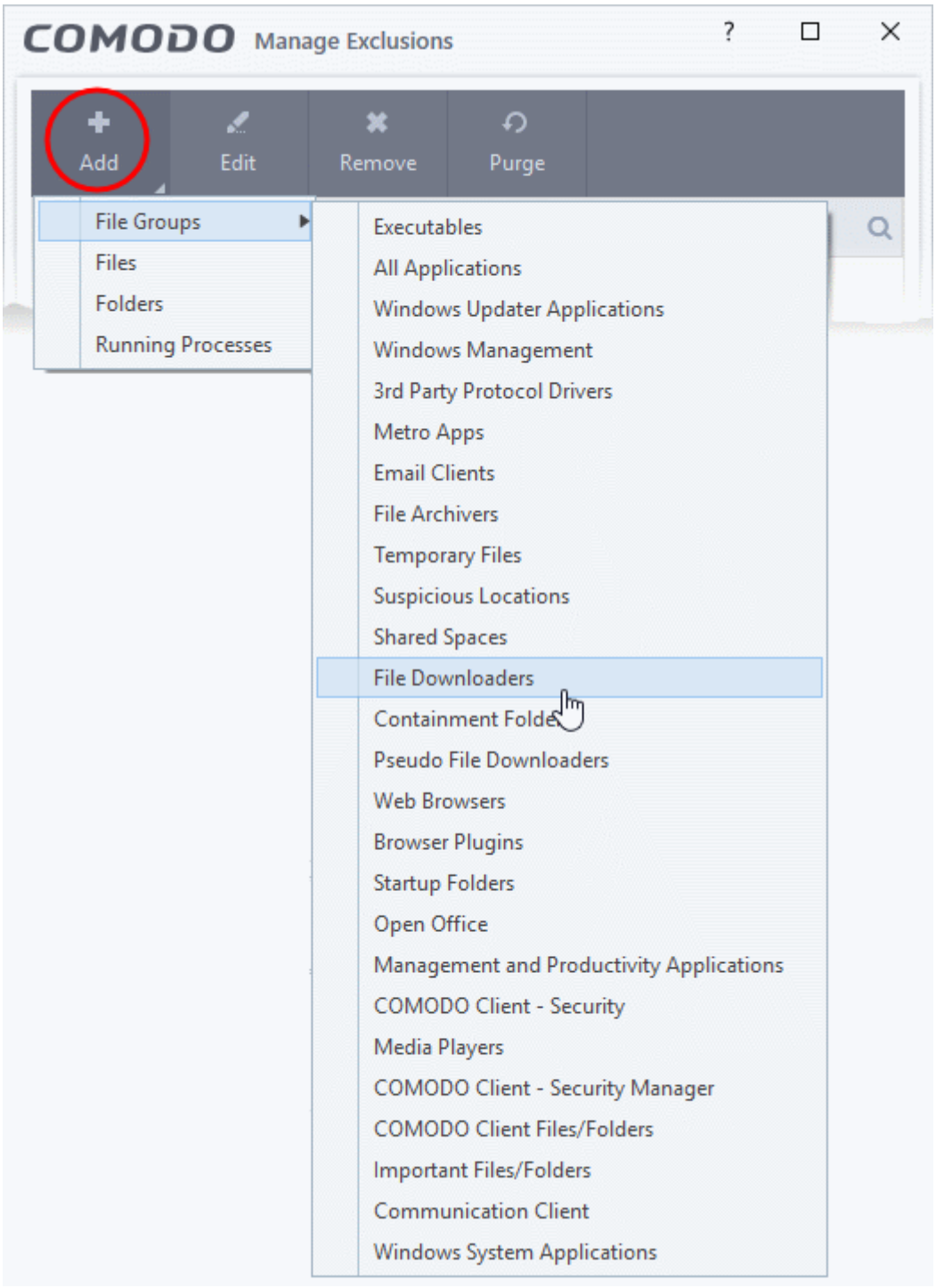
Do not virtualize access to the removable storage media - Allow contained applications and virtual desktop applications to write to external storage devices. Example devices include USB sticks and external hard drives. (***Default = Disabled***)

Do not restrict access to COM/DCOM for these applications - By default, contained applications cannot access the COM and DCOM components running on your computer. This setting lets you specify applications that can access COM / DCOM components, even if the app is in the container.

- Select the option then click the 'these applications' link.



- Click the 'Add' button in the 'Manage Exclusions' dialog.



- **File Groups** - Choose a category of files or folders to which access should be granted. For example, select 'Executables' to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *\cmd.exe *.bat, *.cmd. See '**File Groups**', for more details on file groups.
- **Files** - Pick specific files or applications that can access COM / DCOM when run inside the containment.
- **Folders** - Specify folders as exclusions. Access to COM and DCOM is granted to all files in the folder even if they are run inside the containment.
- **Running Processes** - Choose a process currently running on your computer. The parent application of the process is added to the exclusions.

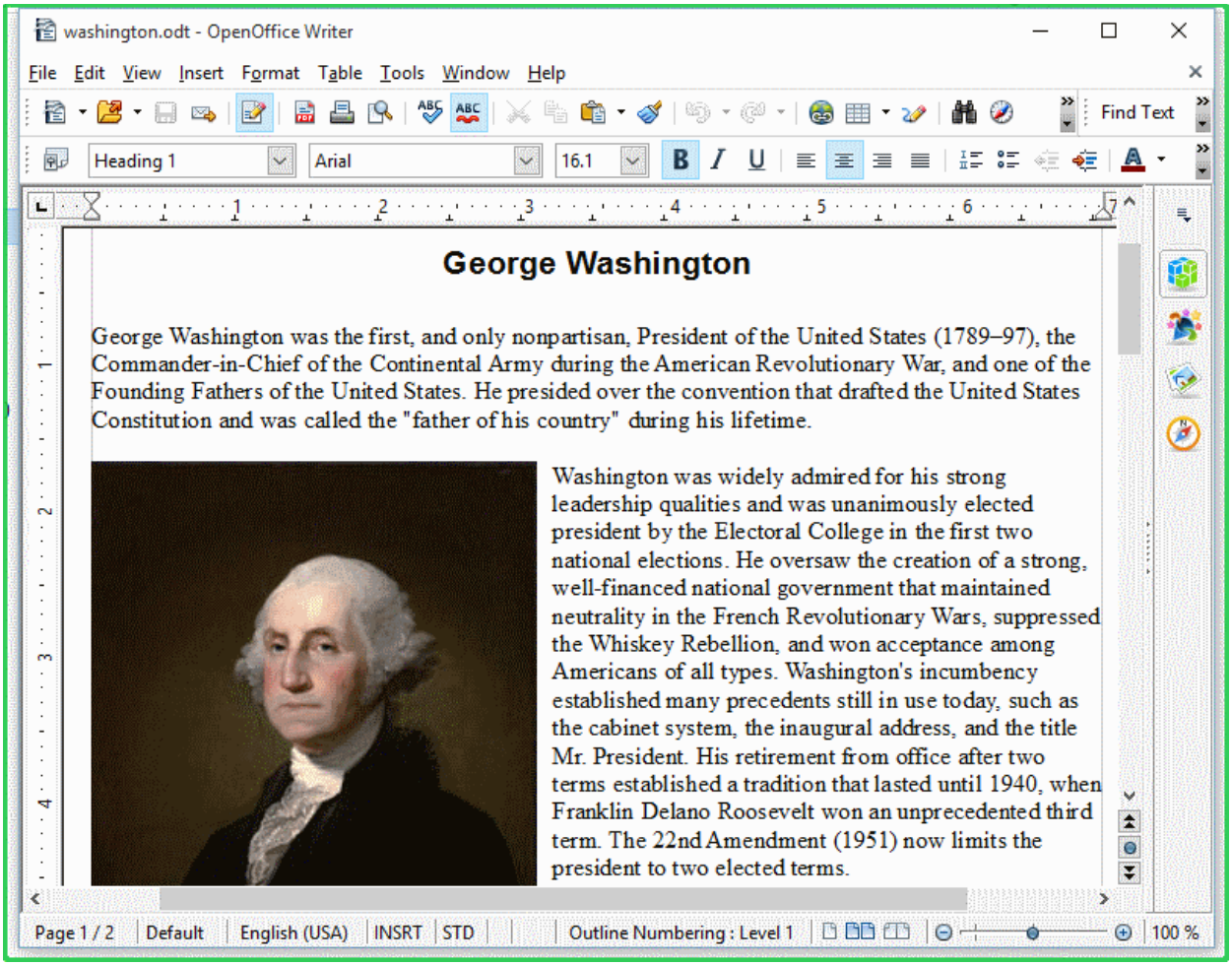
- **Edit** - Select an item and click 'Edit' to change the target file or folder

- **Remove** - Select an item and click 'Remove' to delete an exception
- **Purge** - Checks that all files and folders covered in exceptions are still present on your computer. Purge automatically removes any items it can no longer locate.
- Click 'OK' to implement your settings

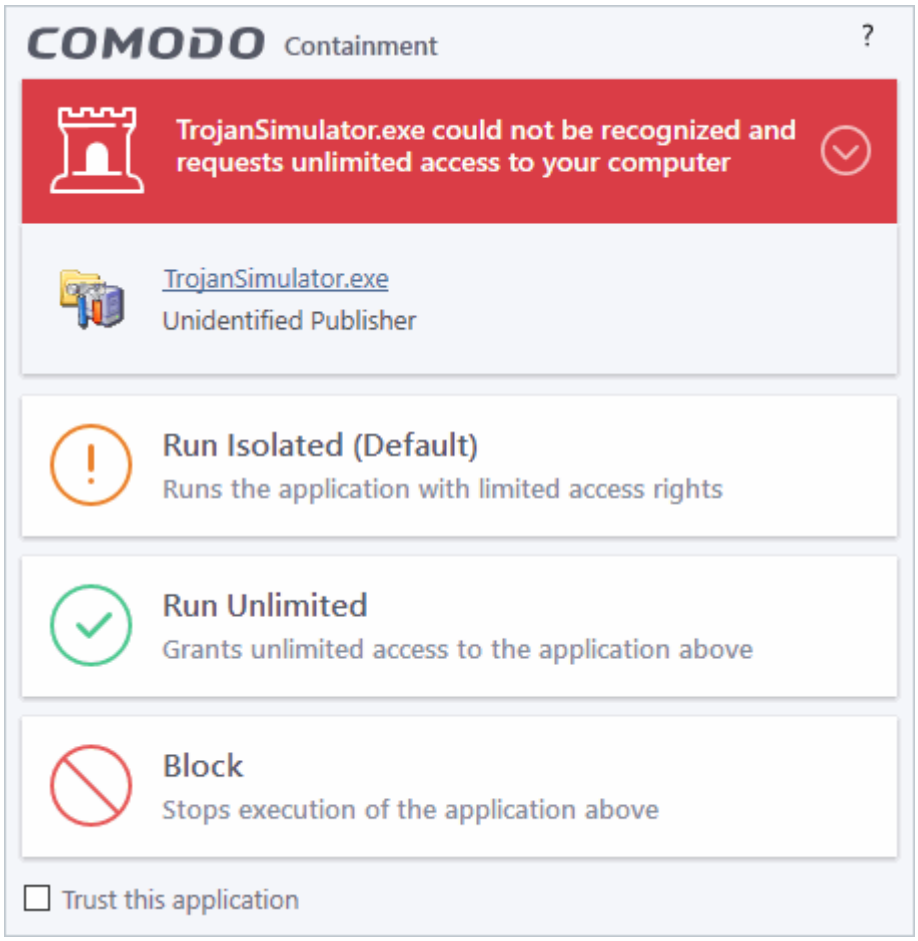
Advanced Settings:

- **Enable automatic startup for services installed in the container** - CCS launches contained services at Windows startup if this option is enabled. (***Default = Enabled***)
- **Show highlight frame for contained applications** - CCS displays a green border around the windows of programs that are running in the container. (***Default = Enabled***)

The following screenshot shows an Open Office document running in the container:



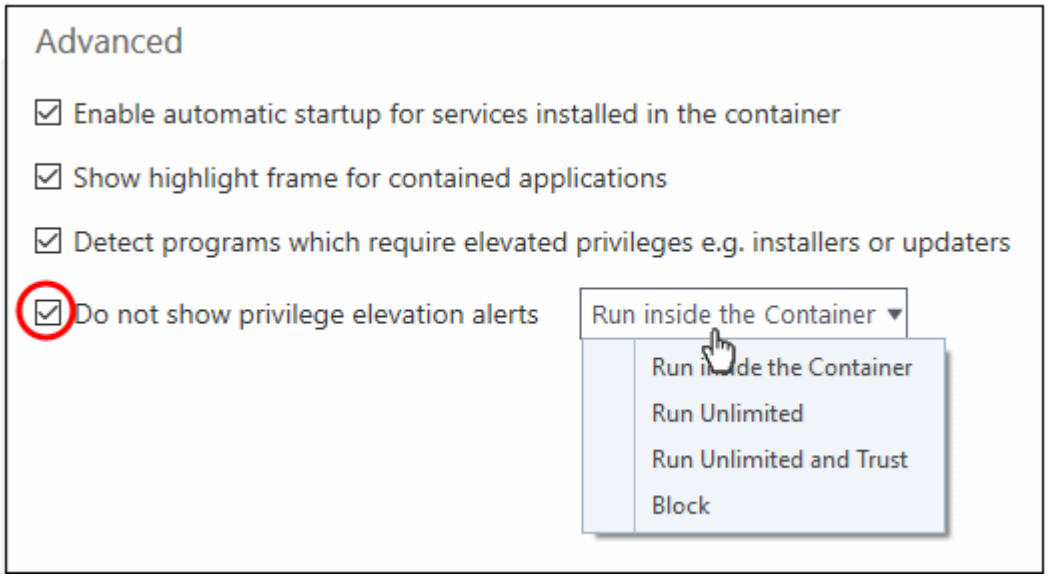
- **Detect programs which require elevated privileges, e.g., installer or updaters**: CCS generates an alert when it detects an installer/updater that requires admin/elevated privileges to run. An installer that is allowed to run with elevated privileges can make changes to important areas of your computer such as the registry. (***Default = Enabled***)
- Example alert:



- **Run Isolated** - Runs the installer/updater in the container
- **Run Unlimited** - Runs the installer/updater on your local computer, outside the container.
- **Block** - Terminates the installer/updater.
- See '**Understand Security Alerts**' for more details.

- Disable this option if you want CCS not to monitor applications that request elevated privileges on your computer

- **Do not show privilege elevation alerts**: CCS will not show alerts (as shown above) when a new or unrecognized application requires admin or elevated privileges to run.
  - If you disable alerts, you need to choose a default action that CCS should implement when it detects such an application:



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

7.7.2. Auto-Containment Rules

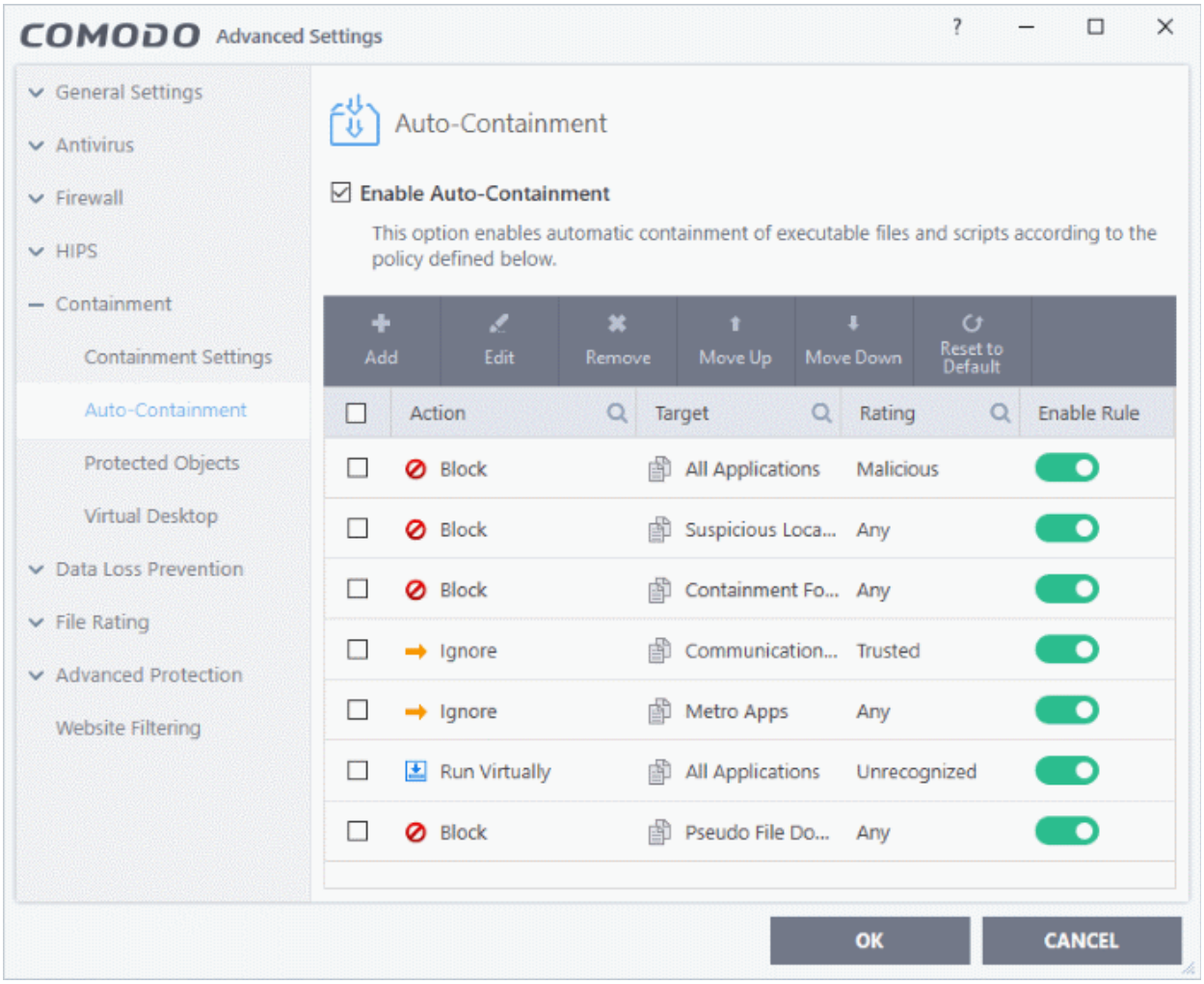
- Click 'Settings' > 'Containment' > 'Auto-Containment'
- Auto-containment rules determine whether a program is allowed to run as normal, run with restrictions, or run in the virtual environment.
- A contained application has much less opportunity to damage your computer because it is isolated from your operating system, important system files and personal data.
- CCS consults these rules whenever you open an application. Rules at the top of the list have a higher priority. You can re-prioritize rules using the 'Move Up' and 'Move Down' buttons.
- Programs running in the container have a green border around them.
- CCS ships with a set of pre-configured rules which provide maximum protection against unknown, potentially malicious applications. You can also create your own custom rules.

Click the following links for help on specific areas:

- **The rules interface**
- **Containment rules explained**
- **Predefined rules**
- **Create a containment rule**
  - **Choose the rule action**
  - **Choose the rule target**
  - **Choose additional rule options**

The rules interface

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Auto-Containment'



- The higher a rule is in the list, the higher priority it has. Use the move up/down buttons to change a rule's priority. In the event of a conflict in settings, CCS will obey the rule that is higher in the list.
- You can also add new rules and manage existing rules from this panel.

General Settings

- **Enable Auto-Containment** - Enable or disable the containment system. If enabled, applications are run in the container as per the rules in this interface. (***Default = Enabled***)

Containment rules explained

A rule performs a specific action on targets which have a certain reputation.

Containment Rules - Column Descriptions	
Column Header	**Description**
Action	The operation that the containment system should perform on the target if the rule is triggered.
Target	The file, file group, or location on which the rule should run.
Rating	The trust status of the target item - 'Malware', 'Trusted', 'Unrecognized' or 'Any'. The rule will apply to target items which have the reputation you choose here.
Enable Rule	Activate / deactivate the rule

- CCS ships with a set of pre-defined auto-containment rules which provide maximum protection for your system.
- There are five 'Block' rules, seven 'Run Virtually' rules, and one 'Ignore' rule.
- The rule numbers indicate their default priority in CCS. If there is a conflict, CCS implements the rule with the highest priority. You can, of course, rearrange priorities as required.
- Click the following links to view the details of each rule:
  - **Block rules**
  - **Run virtually rules**
  - **Ignore rule**

'Block' Rules

1 - Block and quarantine any malicious application

2 - Block any file in the 'Suspicious locations' file group (i.e. anything in CCS quarantine and recycle bin)

3 - Block any file in the folders Comodo uses for the container (i.e. anything in the \vtroot\ folder)

9 - Block pseudo file downloaders which are downloaded by browsers. Example downloaders are wscript.exe, powershell.exe, perl.exe etc.

13 - Block any file in the 'File Transfer Protocols' file group (i.e. any file in a URL starting with 'http:// or https://'. This blocks installation of MSI packages via URL in a command line)

Rule Number			1	2	3	9	13
Action			Block	Block	Block	Block	Block
Target			File Group - All Applications	File Group - Suspicious Locations	File Group - Containment Folders	File Group - Pseudo File Downloaders	File Group - File Transfer Protocols
File Reputation			Malicious	Any	Any	Any	Any
File origin	Source of file creation	Application	Any	Any	Any	Any	Any
		Process(es)	Any	Any	Any	Web Browsers Rating = Any	Any
		user(s)	Any	Any	Any	Any	Any
	Downloaded from		Any	Any	Any	Any	Any
Vendor			Any	Any	Any	Any	Any
Age of file			Any	Any	Any	Any	Any
Log Action			On	On	On	On	On
Restriction Level			N/A	N/A	N/A	N/A	N/A
Limit Maximum Memory			N/A	N/A	N/A	N/A	N/A
Limit Program Execution Time			N/A	N/A	N/A	N/A	N/A

Quarantine	On	Off	Off	Off	On
Exclude child processes from the action	N/A	N/A	N/A	N/A	N/A

'Run Virtually' Rules

5 - Virtualize unrecognized files which are less than three days old

6 - Virtualize unrecognized files downloaded from the intranet, internet or removable storage devices.

7 - Virtualize unrecognized files created by applications that belong to any of these file groups:

- Web Browsers
- Email Clients
- File Downloaders
- Pseudo File Downloaders
- File Archivers
- Management and Productivity Applications
- Browser Plug-ins
- Media Players

8 - Virtualize any unrecognized file in the 'Shared Spaces' file group

10 - Virtualize 'msiexec.exe' if it was started by any process in the 'Management and Productivity Applications' group. The rule will search back ten parent levels of the process tree. 'msiexec.exe' is the MSI installer application.

11 - Virtualize 'cmd.exe' if it was started by 'eqnedt32.exe'

12 - Virtualize 'powershell.exe' if it was started by 'eqnedt32.exe'

'cmd.exe' is the name of the command shell executable, and 'powershell.exe' runs the task automation framework in Windows. 'eqnedt32.exe' is Microsoft's Equation Editor program. Rules 11 and 12 block malware which is impersonating or using the editor to launch attacks.

Rule Number			5	6	7	8	10	11	12
Action			Run Virtually	Run Virtually	Run Virtually	Run Virtually	Run Virtually	Run Virtually	Run Virtually
Target			File Group - All Applications	File Group - All Applications	File Group - All Applications	File Group - Shared Spaces	File Location - *.msiexec.exe	File Location - *\cmd.exe	File Location - *\powershell.exe
File Reputation			Unrecognized	Unrecognized	Unrecognized	Unrecognized	Any	Any	Any
File origin	Source of file creation	Application	Any	Any	Web Browsers Email Clients File Downloaders Pseudo File Downloaders File Archivers Management and Productivity Applications Browser Plug-ins Media Players	Any	Any	*\EQNEDT32.EXE	*\EQNEDT32.EXE
		Process(es)	Any	Any	Any	Any	File Group - Management and Productivity Applications	Any	Any

							Number of parent process levels to be analyzed = 10		
		user(s)	Any	Any	Any	Any	Any	Any	Any
	Downloaded from		Any	Intranet Removable media Internet	Any	Any	Any	Any	Any
Vendor			Any	Any	Any	Any	Any	Any	Any
Age of file			Less than 3 days	Any	Any	Any	Any	Any	Any
Log Action			On	On	On	On	On	On	On
Restriction Level			Off	Off	Off	Off	Off	Off	Off
Limit Maximum Memory			Off	Off	Off	Off	Off	Off	Off
Limit Program Execution Time			Off	Off	Off	Off	Off	Off	Off
Quarantine			N/A	N/A	N/A	N/A	N/A	N/A	N/A
Exclude child processes from the action			N/A	N/A	N/A	N/A	N/A	N/A	N/A

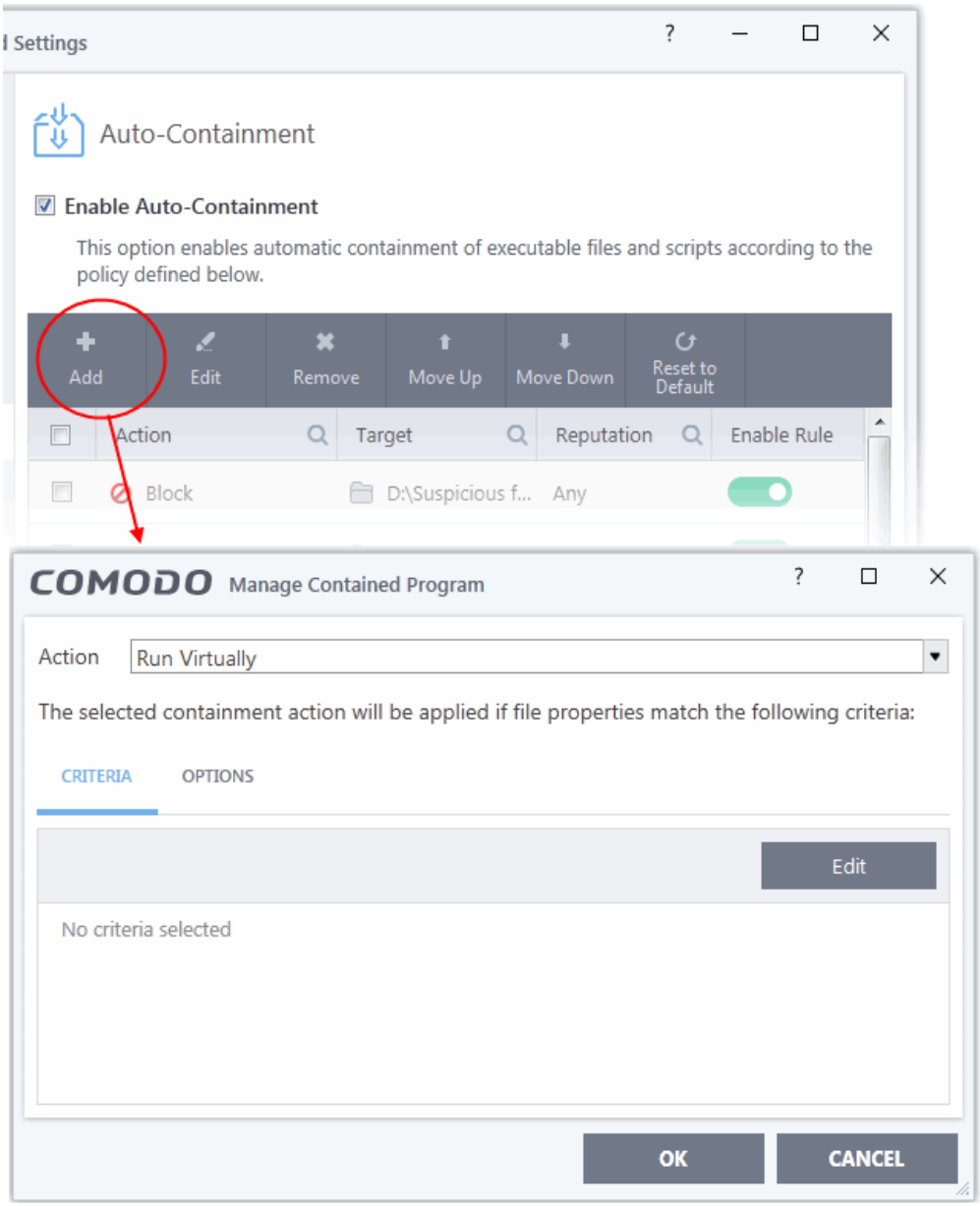
Ignore Rule

4 - Do not auto-contain metro apps

Rule Number			**4**
Action			Ignore
Target			File Group - Metro Apps
File Reputation			Any
File origin	**Source of file creation**	**Application**	Any
		Process(es)	Any
		user(s)	Any
	Downloaded from		Any
Vendor			Any
Age of file			Any
Log Action			On
Restriction Level			N/A
Limit Maximum Memory			N/A
Limit Program Execution Time			N/A
Quarantine			N/A
Exclude child processes from the action			Off

Add an Auto-Containment Rule

- Auto-containment rules can be created for a single application, for all applications in a folder/file group, for running processes, or for a file/process hash value.
- You can create precision rules by specifying 'file creation source', 'file rating of the source', 'file origin', 'file rating' or 'file age'.
- You can also create simple rules to run an application in the container just by specifying the action and the target application.
- Click the 'Add' button at the top of the list in the Auto-Containment panel:



The 'Manage Contained Program' dialog will appear. The 'Manage Contained Program' displays the action at the top and contains two tabs:

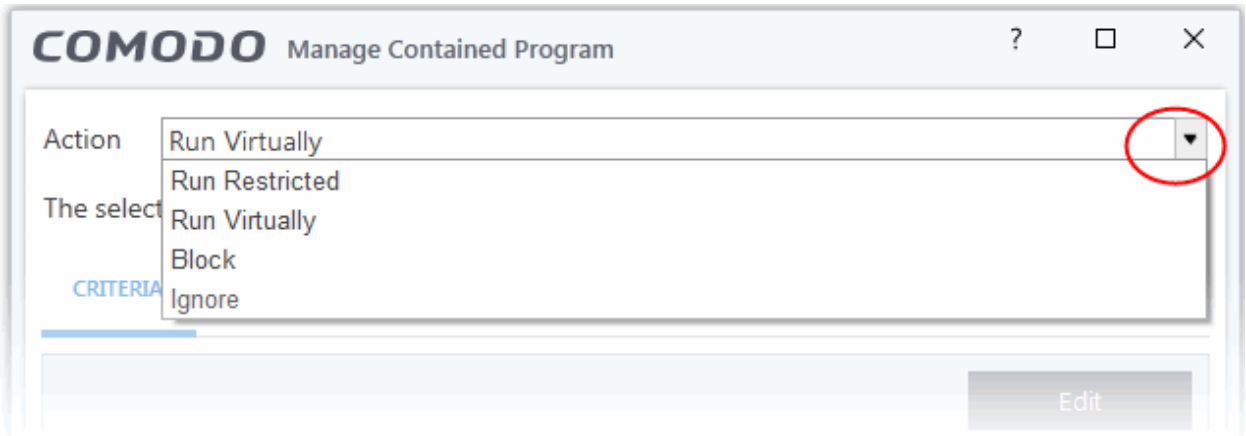
- **Criteria** - Allows you to define conditions upon which the rule should be applied.
- **Options** - Allows you to configure additional actions like logging, setting memory usage and execution time restrictions.

Creating a new containment rule involves the following steps:

- **Step 1 - Choose the action**
- **Step 2 - Select the target file/group and set the filter criteria for the target files**
- **Step 3 - Select the options**

Step 1 - Choose the action

The settings in the 'Action' drop-down combined with the restriction level in the 'Options' tab determine the privileges of an auto-contained application. This determines what right it has to access other processes and hardware resources on your computer.



The options available under the 'Action' drop-down are:

- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Run Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be contained and allowed to run with all privileges.

- Choose the action from the options.

Step 2 - Select the target file/group and set the filter criteria

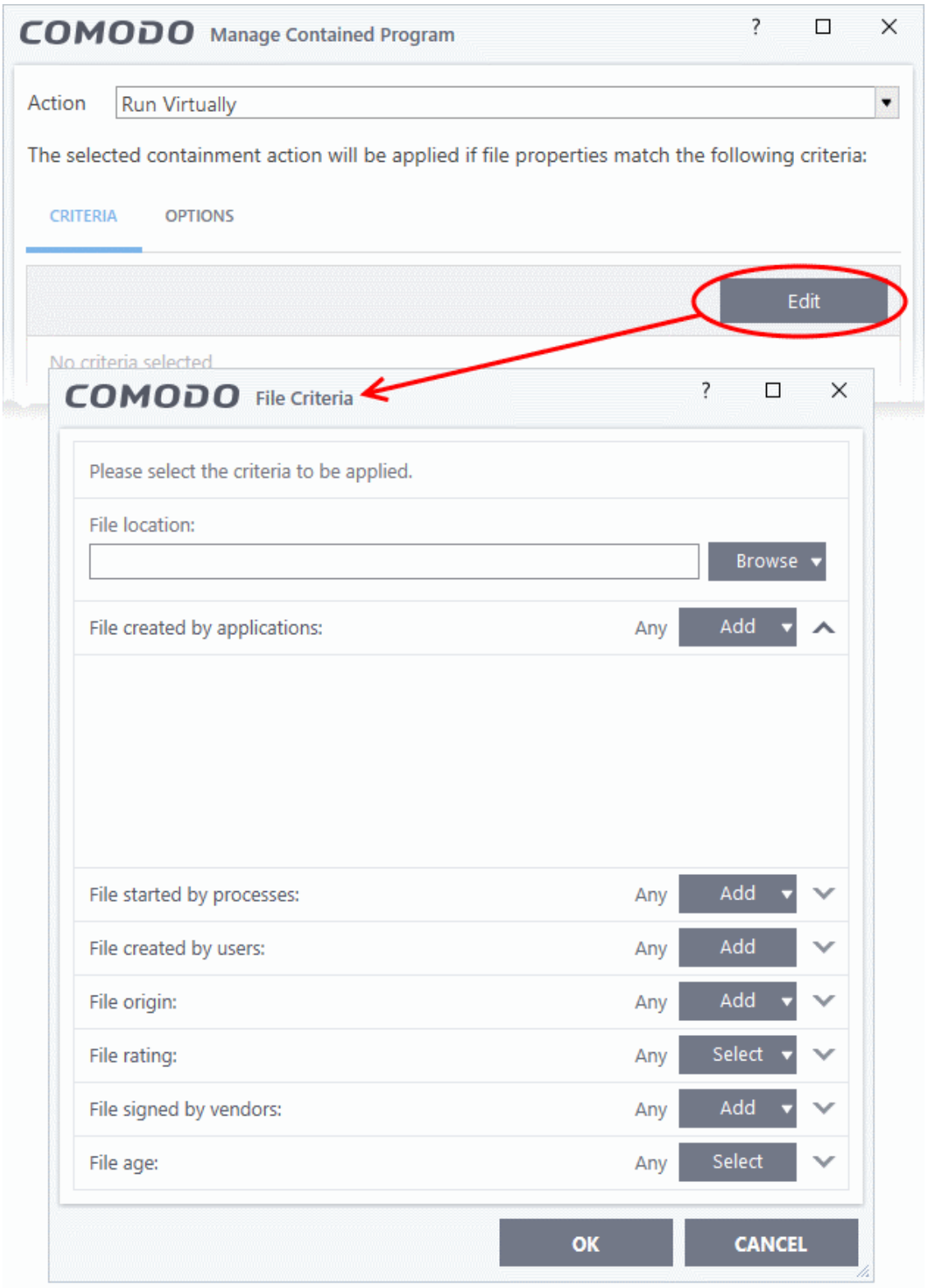
- The next step is to select the target files and configure filters.
- You can filter a rule so it applies to specific types of file.
  - For example, you can specify 'All executables' as the target, then add a filter so it only affects executables from the internet.
  - Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target, then add 'Files created by a specific user' as the filter.

Select the target and set the filters

- Click the 'Criteria' tab.

The target and the filter criteria, if any, configured for the rule will be displayed.

- To add new target and filter criteria, click the 'Edit' button at the far right

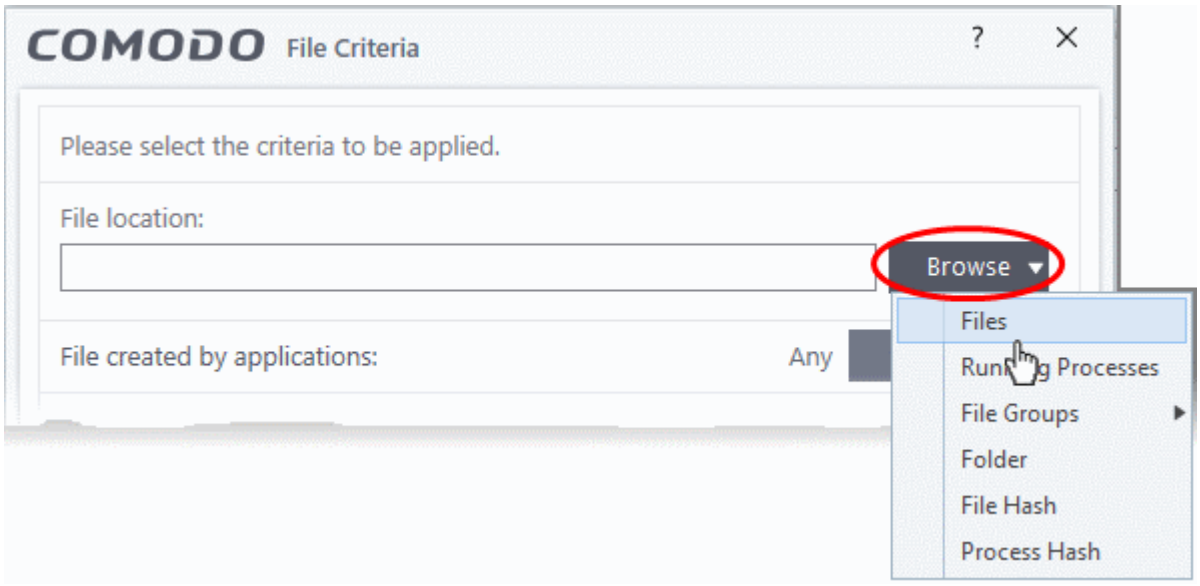


The 'File Criteria' dialog will open. The file criteria dialog allows you:

- **Select the target**
- **Configure the filter criteria**

Select the target

- To select the target, click the 'Browse' button beside the 'File Location' field

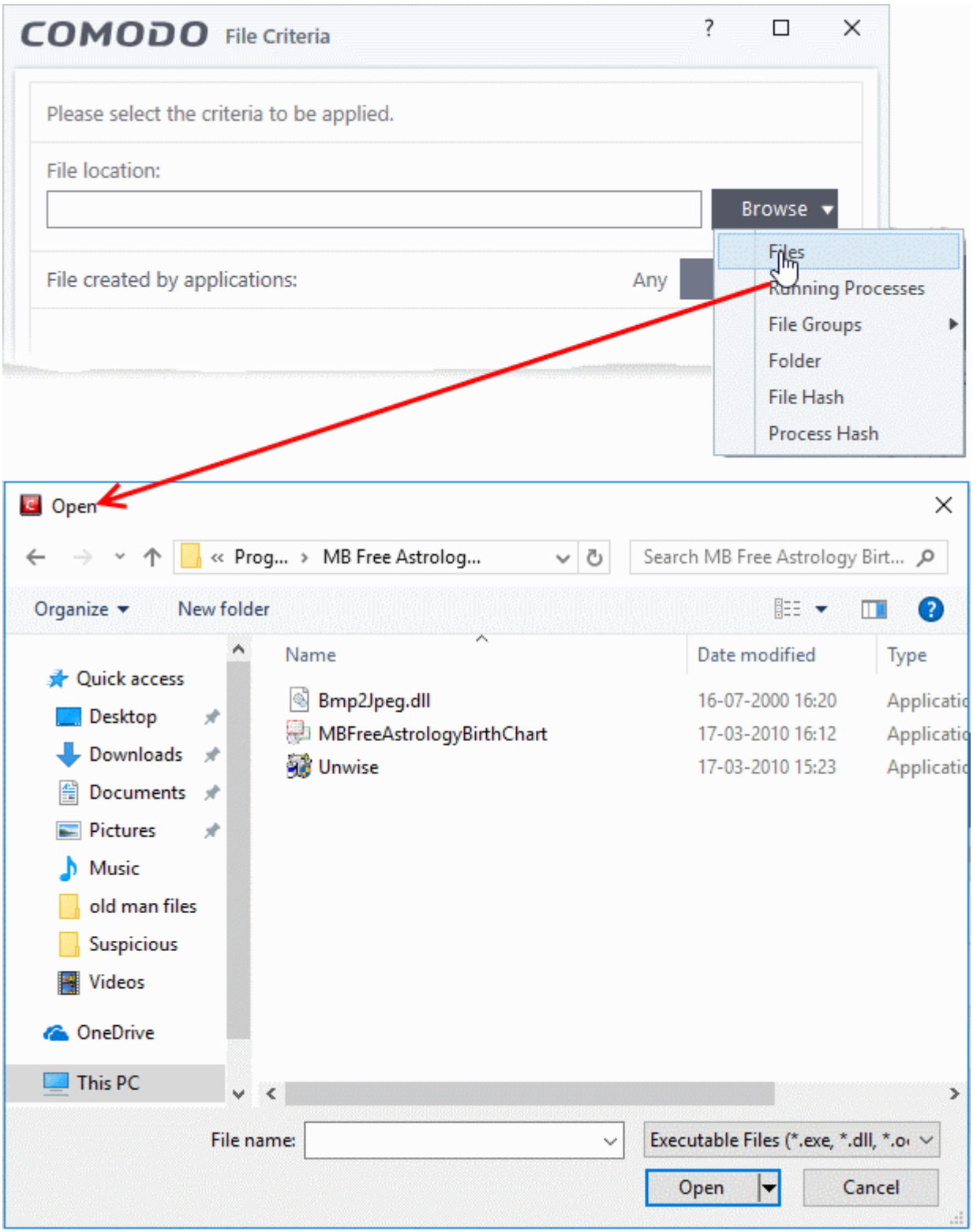


There are six types of target you can add:

- **Files** - Apply the rule to specific files.
- **Running Processes** - Apply the rule to a process that is currently running on your computer.
- **File Groups** - Apply the rule to predefined file groups. See **File Groups** for help to add or modify a file group.
- **Folder** - Apply the rule to a folder or drive.
- **File Hash** - Create a hash value from a file and use it as the rule target. A hash value is a large number which is generated by passing the file through a hashing algorithm. The number uniquely identifies and represents the file, and it is extremely unlikely that two files will ever generate the same hash value. The benefit of using a file hash is that the rule will still work even if the file name changes.
- **Process Hash** - Create a hash value of a process and use it as the rule target. Please see description above if required.

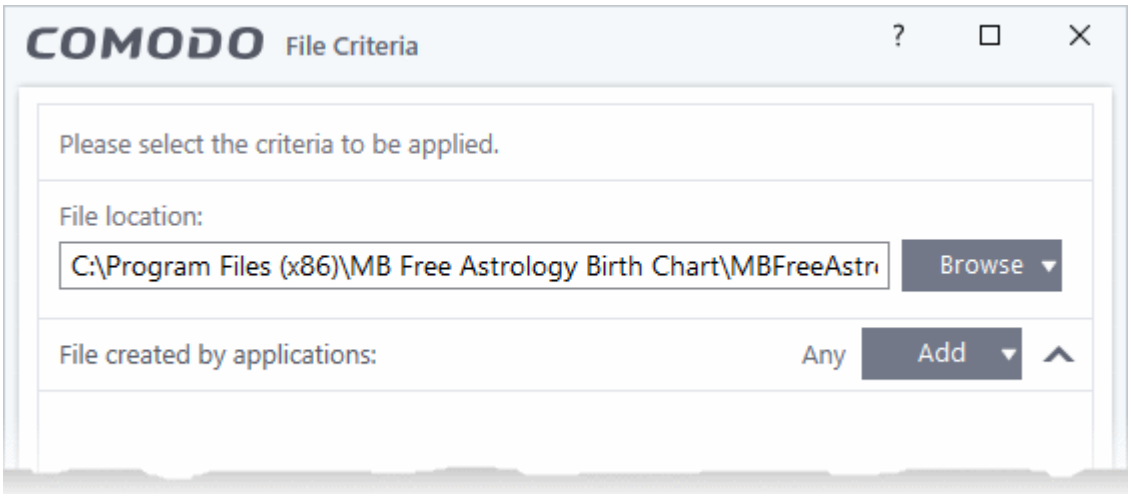
Add an individual File

- Choose 'Files' from the 'Browse' drop-down.



- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'

The file will be added as target and will be run as per the action chosen in **Step 1**.



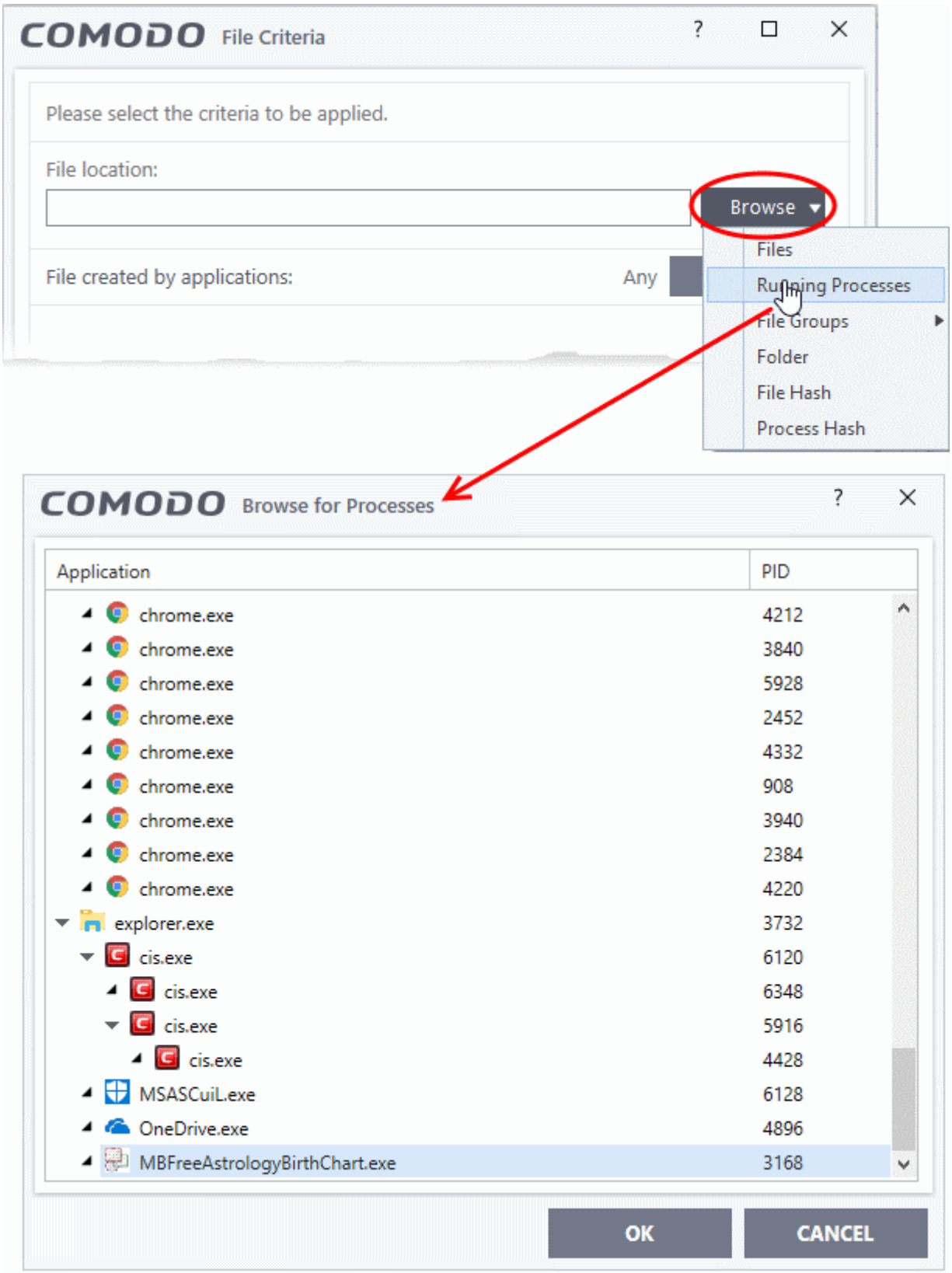
- Click 'OK', if you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria** and file rating and **options** for the rule.

Add a currently running application by choosing its process

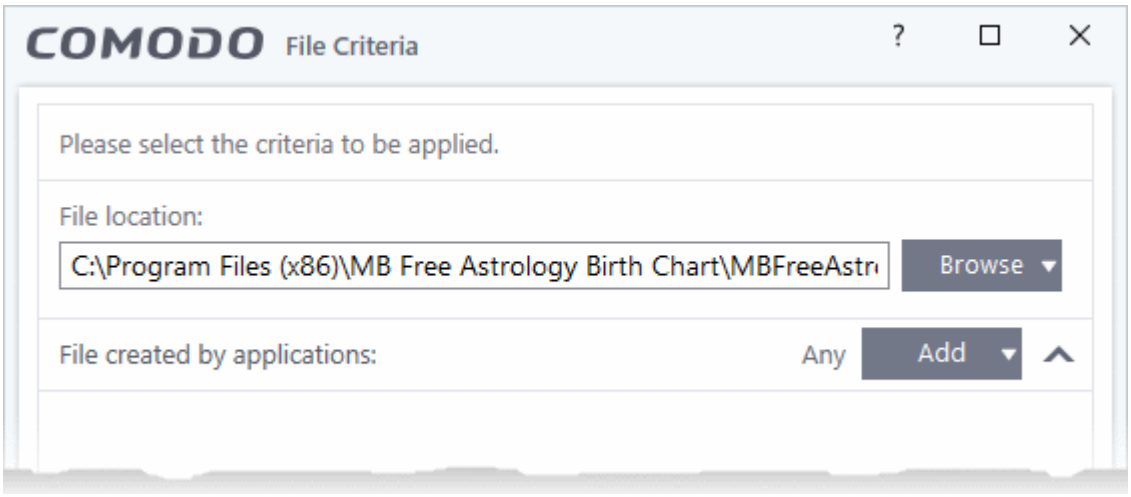
- Choose 'Running Processes' from the 'Browse' drop-down.



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

- Select the process, whose target application is to be added to target and click 'OK' from the 'Browse for Process' dialog.

The parent application of the process is added as the target and run as per the action in Step 1.



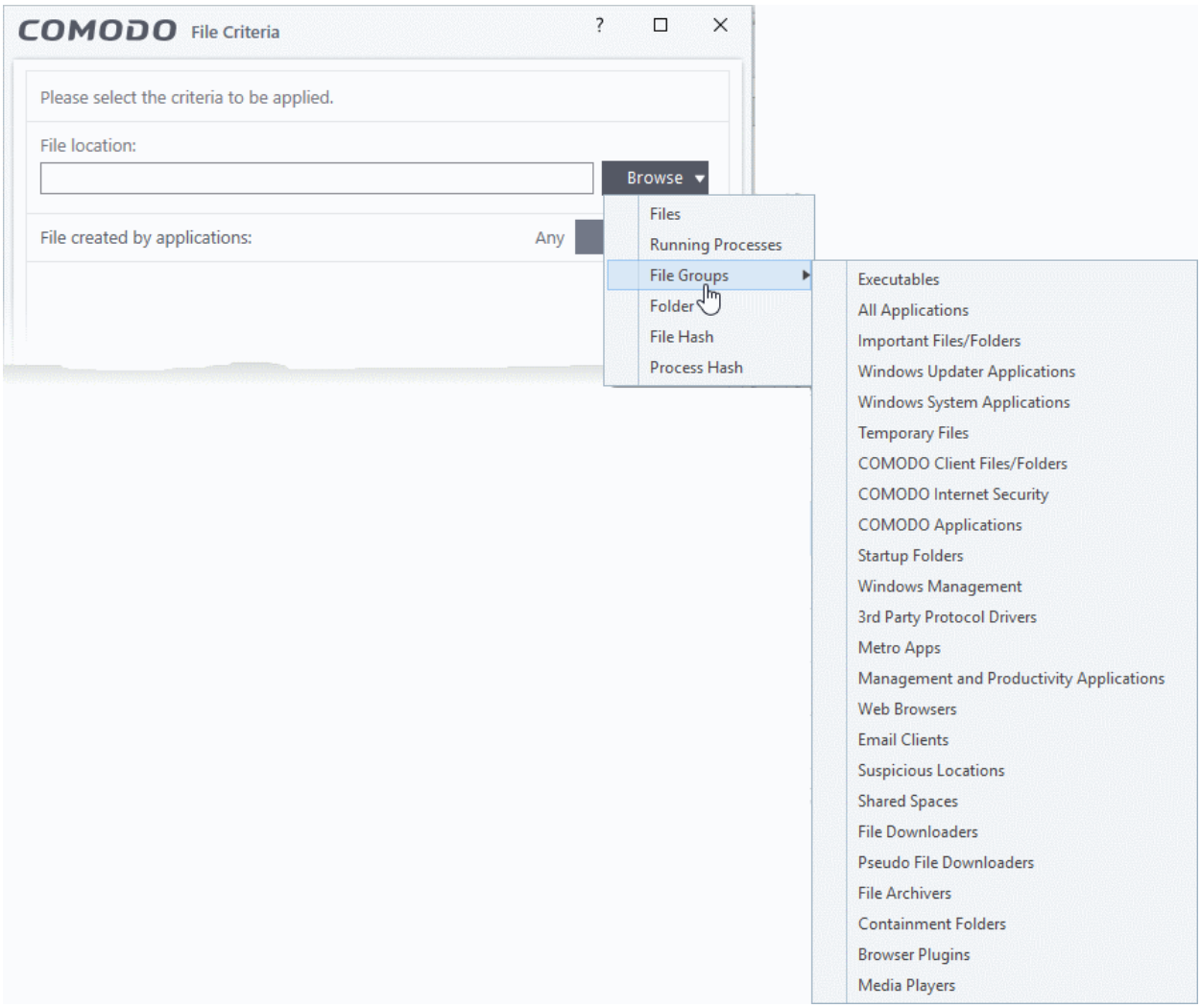
- Click 'OK', if you want to just add the application for a particular action as selected in **Step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria** and file rating and **options** for the rule.

Add a File Group

- Choose 'File Groups' from the 'Browse' drop-down. Choosing File Groups allows you to include a category of files or folders configured as a 'File Group'. See **File Groups**, for more details on viewing and managing pre-defined and user-defined file groups.



- Select the file group from the drop-down.

The file group will be added as target and will be run as per the action chosen in **Step 1**.

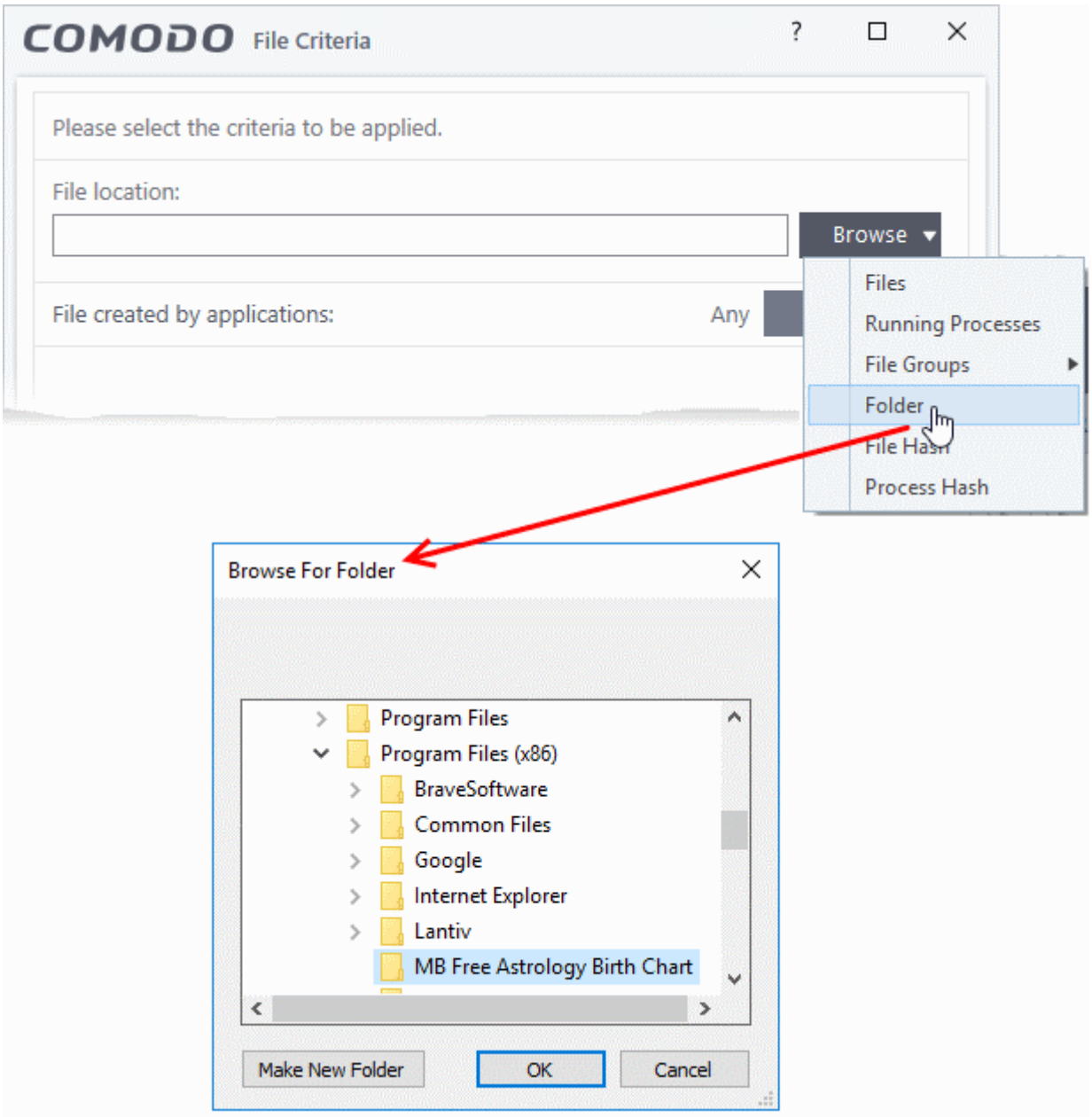
- Click 'OK', if you want to just add the file group for a particular action as selected in Step 1 without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria and file rating** and **options** for the rule.

Add a folder/drive partition

- Choose 'Folder' from the 'Browse' drop-down.



The 'Browse for Folder' dialog will appear.

- Navigate to the drive partition or folder you want to add as target and click 'OK'

The drive partition/folder will be added as the target. All executable files in the folder will be run as per the action chosen in **step 1**.

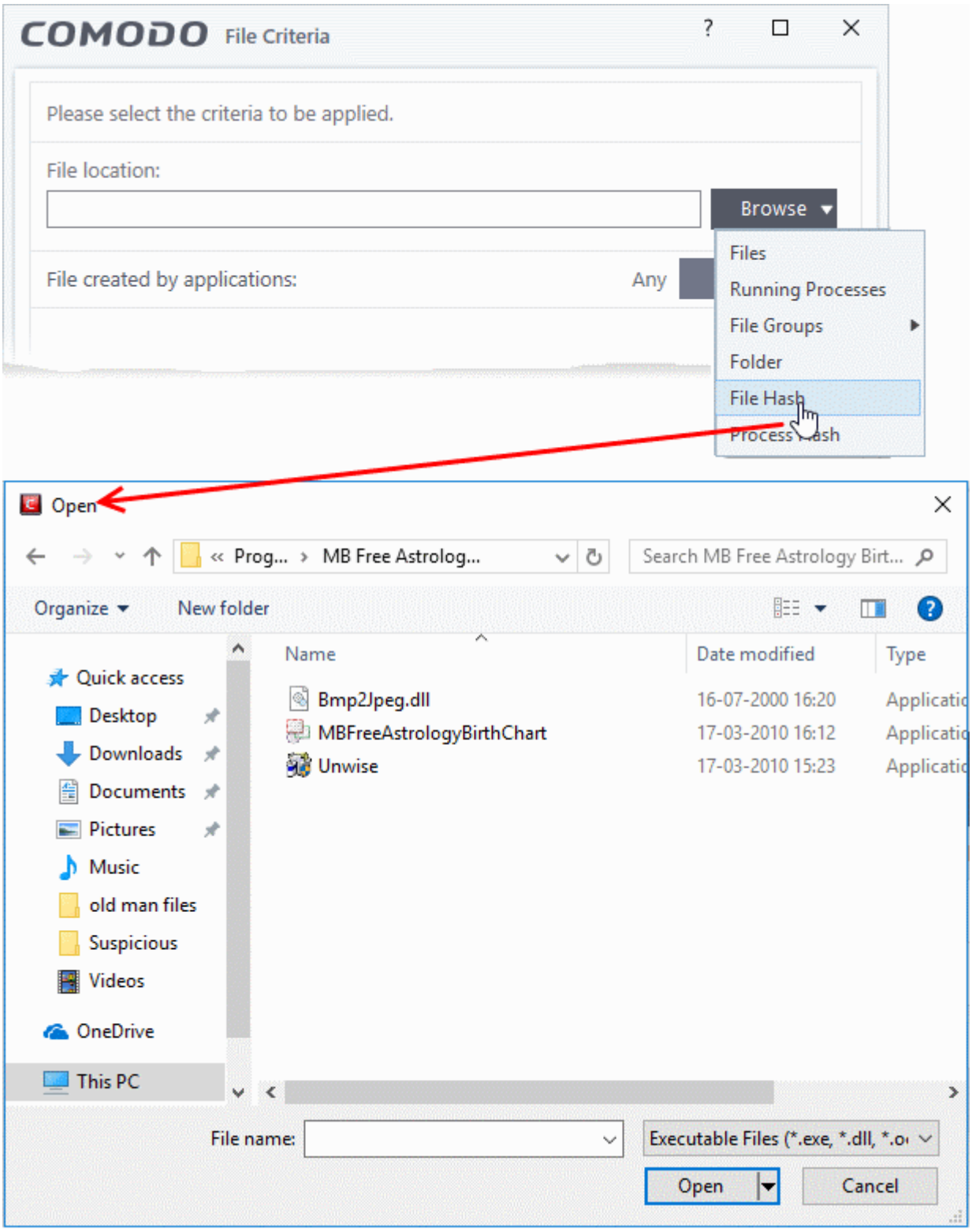
- Click 'OK', if you want to just add the applications for a particular action as selected in **step 1** without specifying any filters or options.

The default values for filter criteria and file rating will be 'Any' and for 'Options' it will be 'Log when this action is performed'.

- If required you can **configure filter criteria** and file rating and **options** for the rule.

Add a file based on its hash value

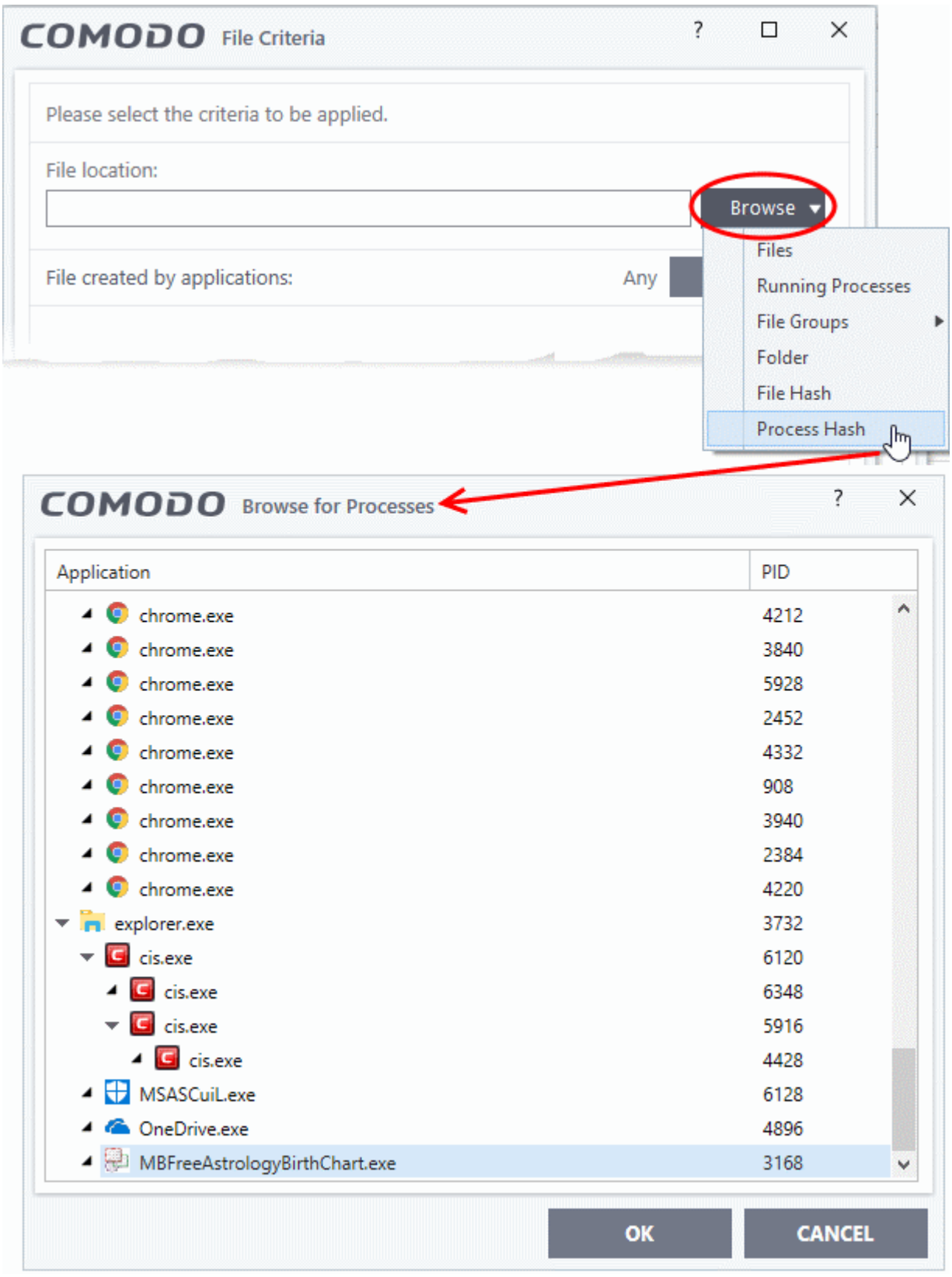
- Choose 'File Hash' from the 'Browse' drop-down



- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'
- Click 'OK', if you want to just add the file for a particular action as selected in **step 1** without specifying any filters or options.
- If required you can **configure filter criteria** and file rating and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.
- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

Add an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



A list of currently running processes in your computer is shown.

- Select the process, to add the hash value of its parent application as the target and click 'OK'
- Click 'OK', if you want to just add the application for a particular action as selected in **step 1** without

specifying any filters or options.

- If required you can **configure filter criteria** and file rating and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.
- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the process name changes.

Configure the Filter Criteria and File Rating

You can apply an action to a file if the file meets certain criteria.

The available criteria are:

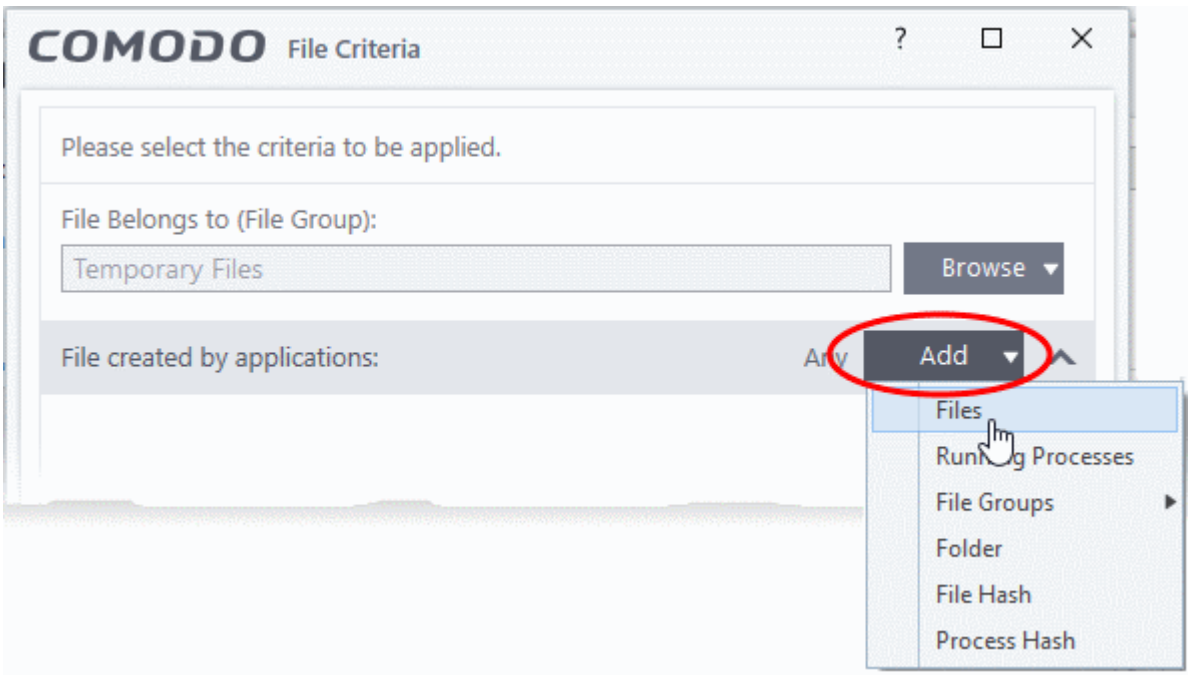
- **By application that created the file**
- **By process that created the file**
- **By user that created the file**
- **By file origin**
- **By file rating**
- **By vendor who signed the file**
- **By file age**

Auto-contain a file if it was created by a specific application

- You can create a filter to apply an action to a file based on its source application.
- You can also specify the file rating of the source application. The rule will then only contain a file if its parent app has a certain trust rating.

Specify source application(s):

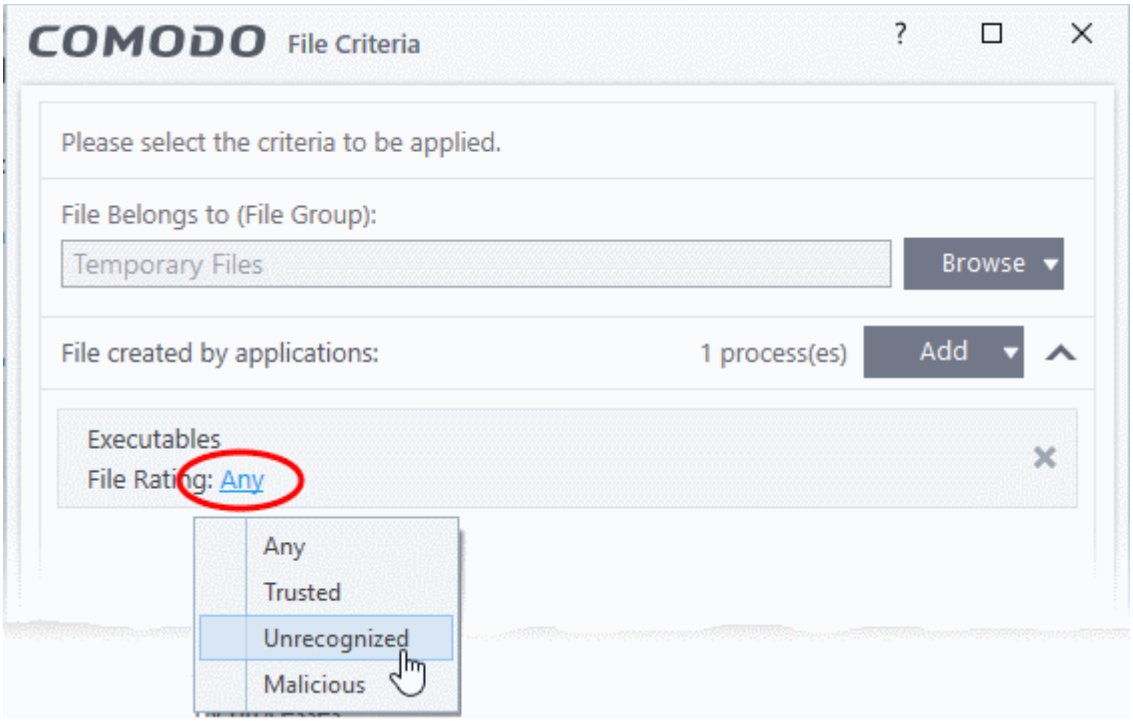
- Click the 'Add' button in the 'File Created by applications' stripe.



- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.

The selected source application, file group or the folder will be added.

- Click the 'Any' link beside 'File Rating' and select the file rating of the source



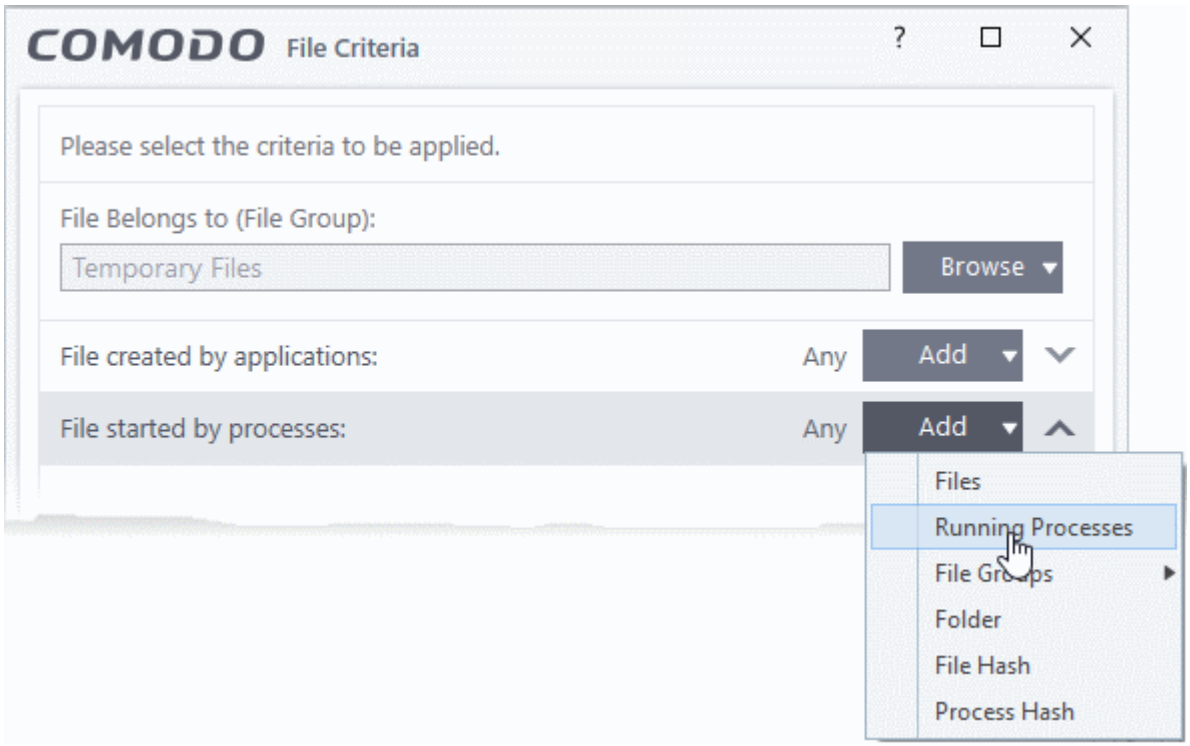
- Repeat the process to add more applications or groups/folders.

Auto-contain a file if it was created by a specific process

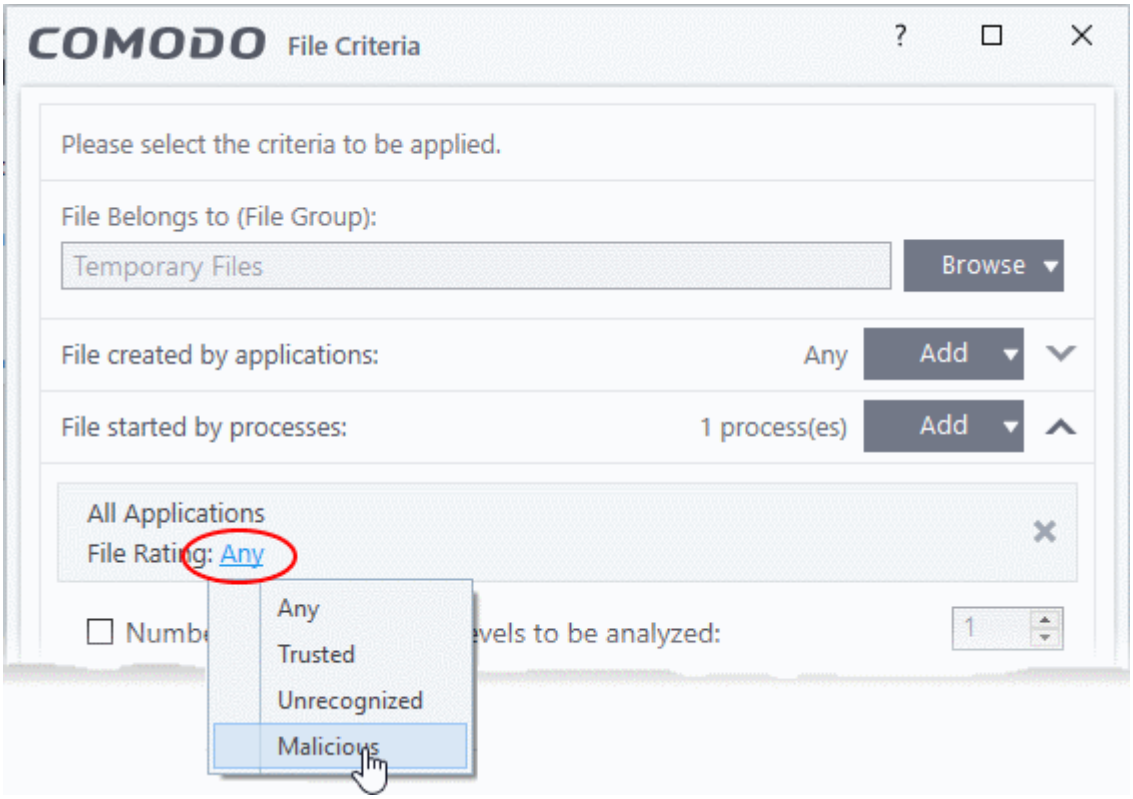
- You can create a filter to apply an action to a file based on its parent process.
- Optionally, you can also specify:
  - The file rating of the source. The rule will then only contain a file if its parent process has a certain trust rating.
  - The number of levels in the process chain that should be inspected.

To specify source process(es)

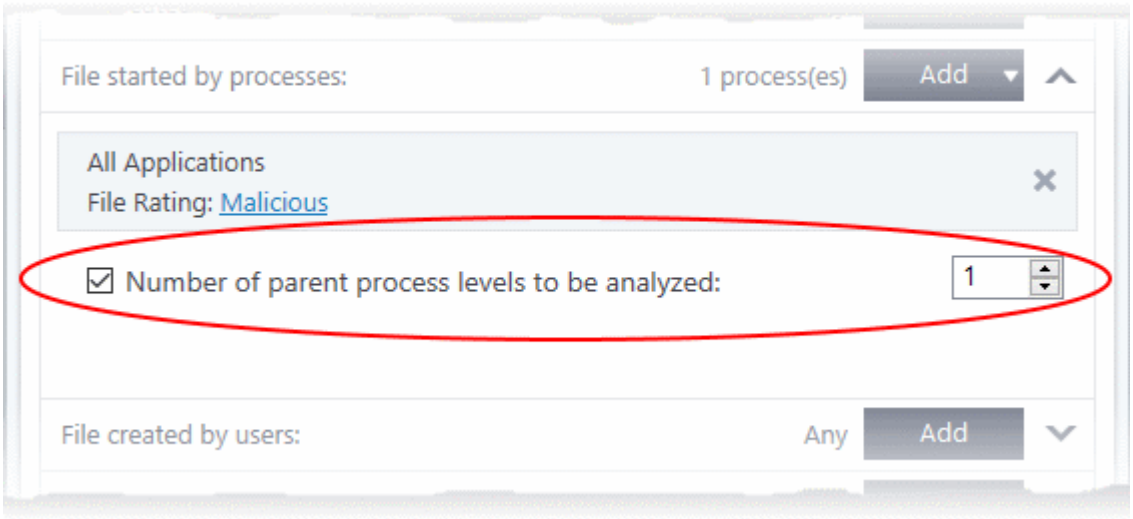
- Click the 'Add' button in the 'File Created by Process(es)' stripe.



- The options available are same as those available under the 'Browse' button beside 'Target', as explained **above**.
- The selected source application, file group or the folder will be added. The file created / invoked by the process, started by the selected source will be added as the target for the rule.
- Click the 'Any' link beside 'File Rating' and select the file rating of the source



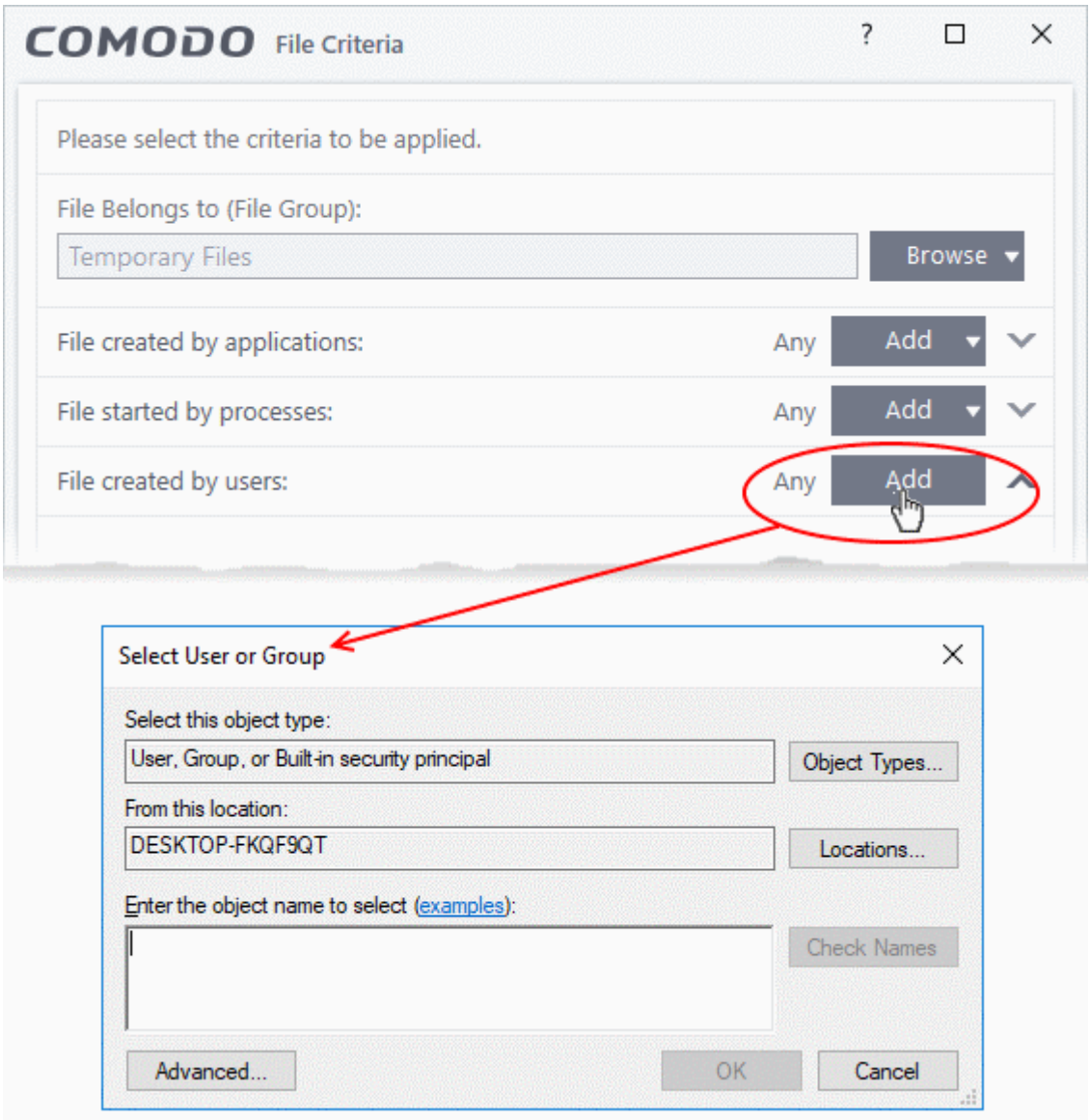
- '**Number of parent process levels to be analyzed**' - Specify how far up the process tree CCS should check when inspecting the file's sources. 1 = will only check the file's parent process. 2 = will check the parent process and the grand-parent process, etc., etc.



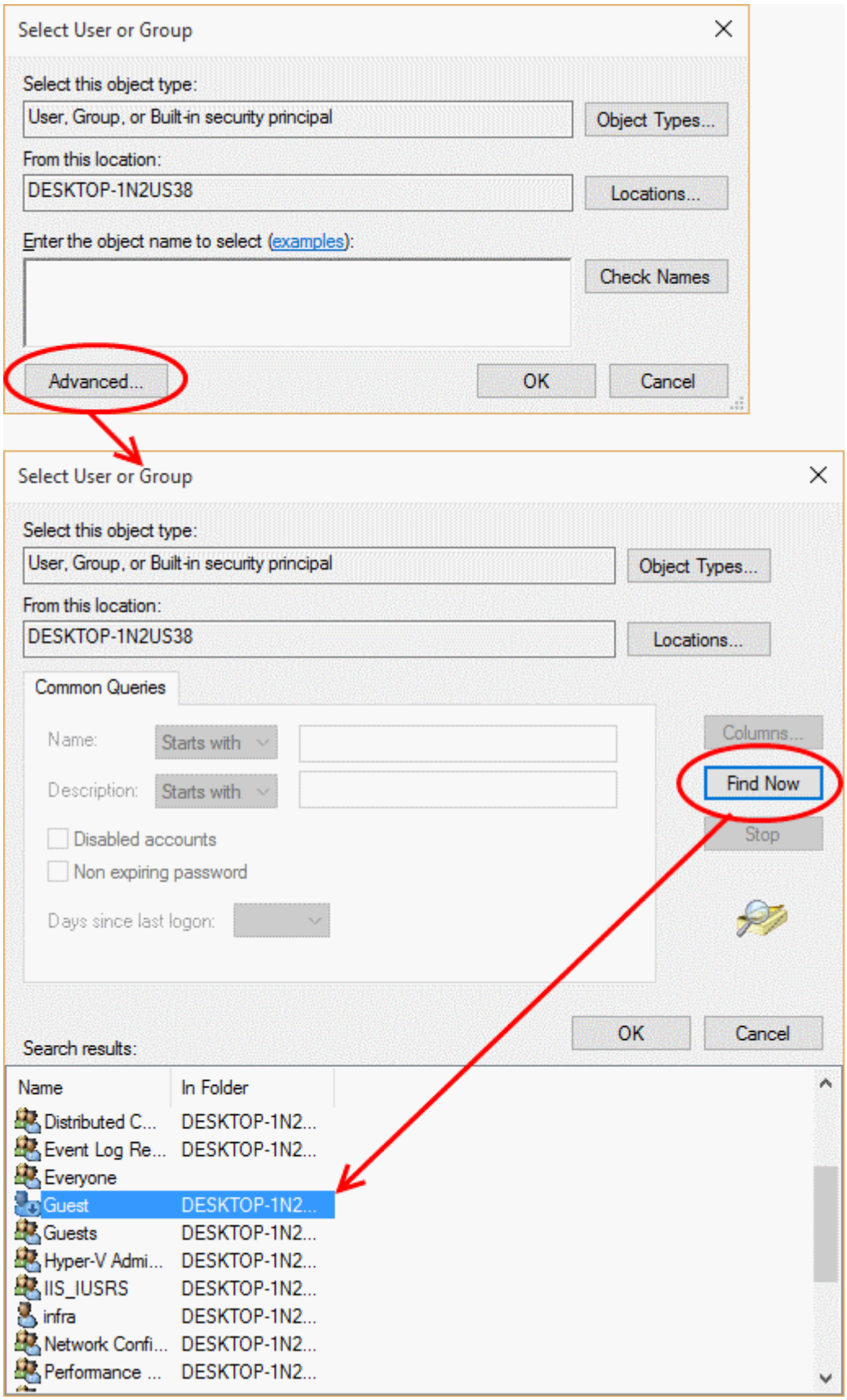
- Repeat the process to add more process(es)

Auto-contain a file created by specific user(s)

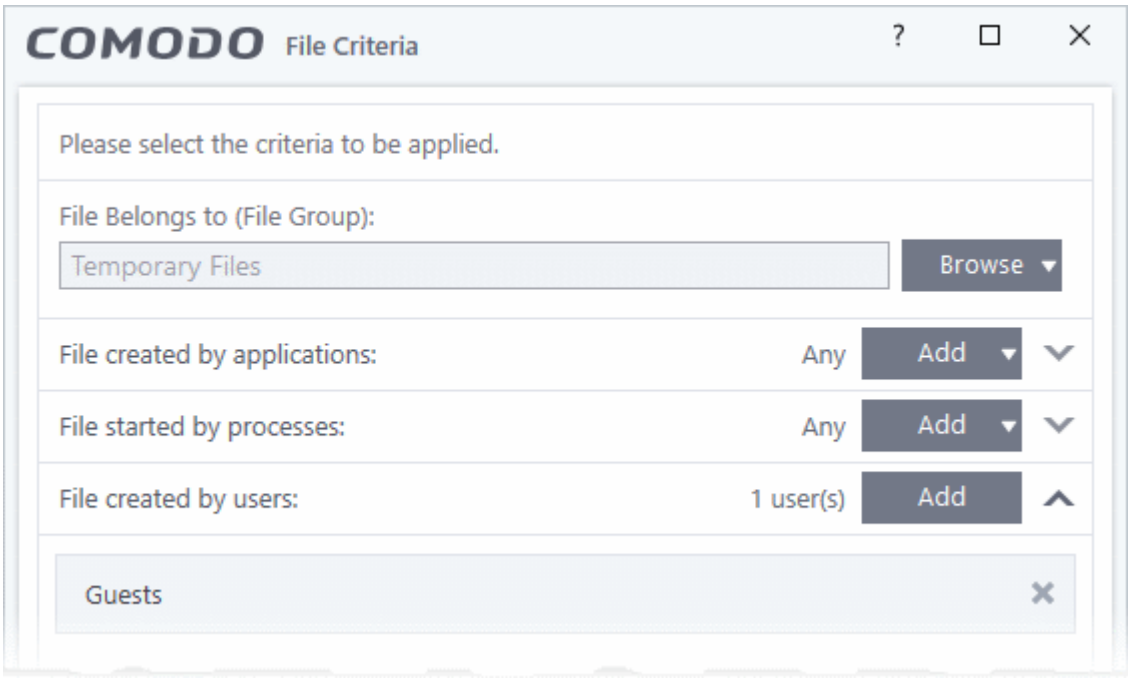
- Click the 'Add' button in the 'File Created by User(s)' stripe.



- The 'Select User or Group' dialog will appear.
  - Type the names of the users to be added to the rule. Use the format <domain name>\<user/group name> or <user/group name>@<domain name>.
  - Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



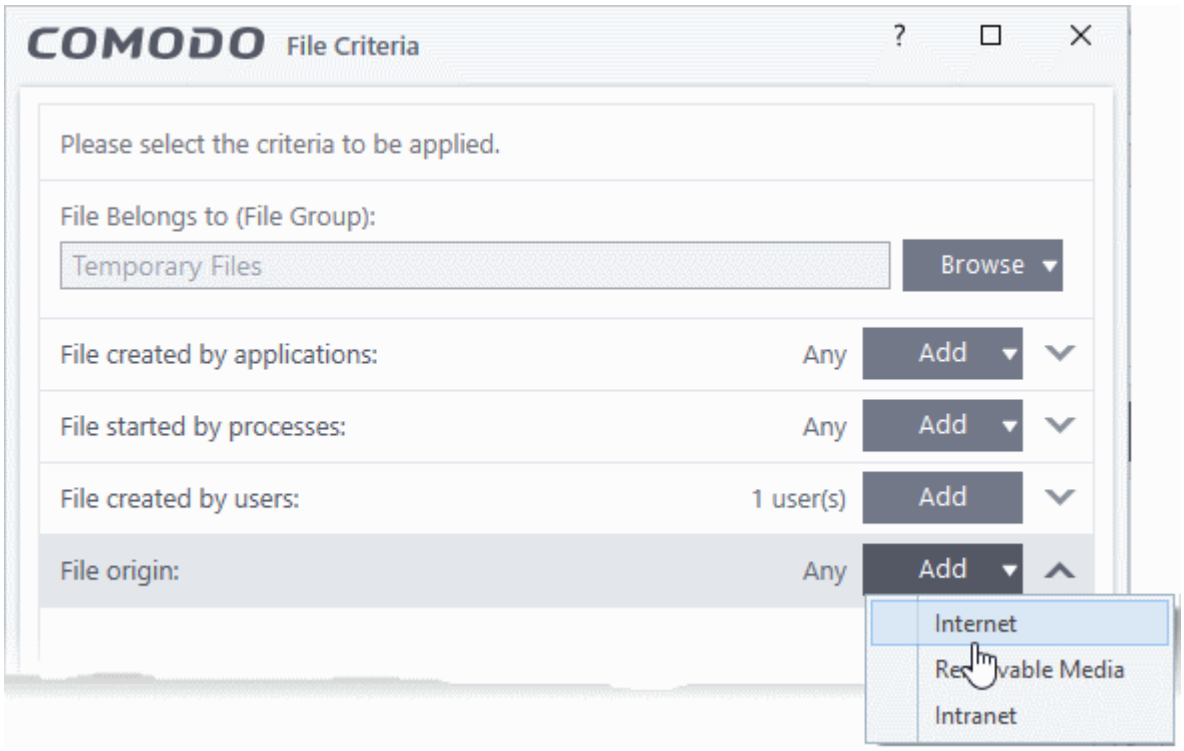
The user will be added to the list.



- Repeat the process to add more users.
- To remove the user added by mistake or no longer needed in the list, click the 'X' icon at the right end of the user name.

Auto-contain a file downloaded/copied from a specific source

- Click the 'Add' button in the 'File Origin(s)' stripe.
- Choose the source from the options:



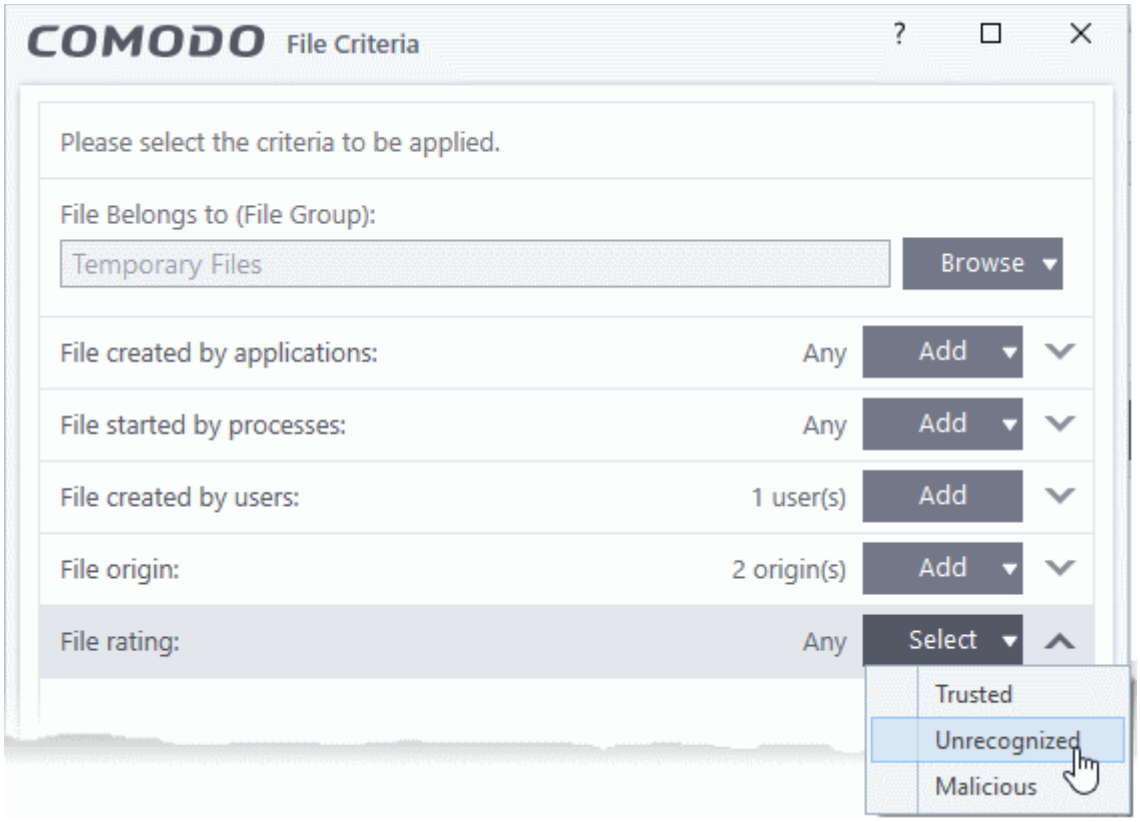
- **Internet** - The rule will only apply to files that were downloaded from the internet.
- **Removable Media** - The rule will only apply to items copied to the computer from removable devices like a USB drive, CD/DVD or external storage.

- **Intranet** - The rule will only apply to files that were downloaded from the local intranet.

- Repeat the process to add more sources

Select the file rating as filter criteria

- Click the 'Select' button in the 'File Rating' stripe:



- This will apply the rule to files which match the trust rating you set. You can choose from the following trust ratings:
  - **Trusted** - Applications are categorized as 'Trusted' if:
    - The file is on the global whitelist of safe files
    - The file is signed by a trusted company in the **Vendor List**
    - The file was installed by a trusted installer
    - The file was given a trusted rating in the **File List** by a user
  - See **File Rating Settings** for more information.
  - **Unrecognized** - Files that do not have a current trust rating. The file is on neither the blacklist nor the safelist, so is given an 'unknown' trust rating. See **File List** for more information.
  - **Malware** - Malicious files - those that are on the blacklist of known harmful files..

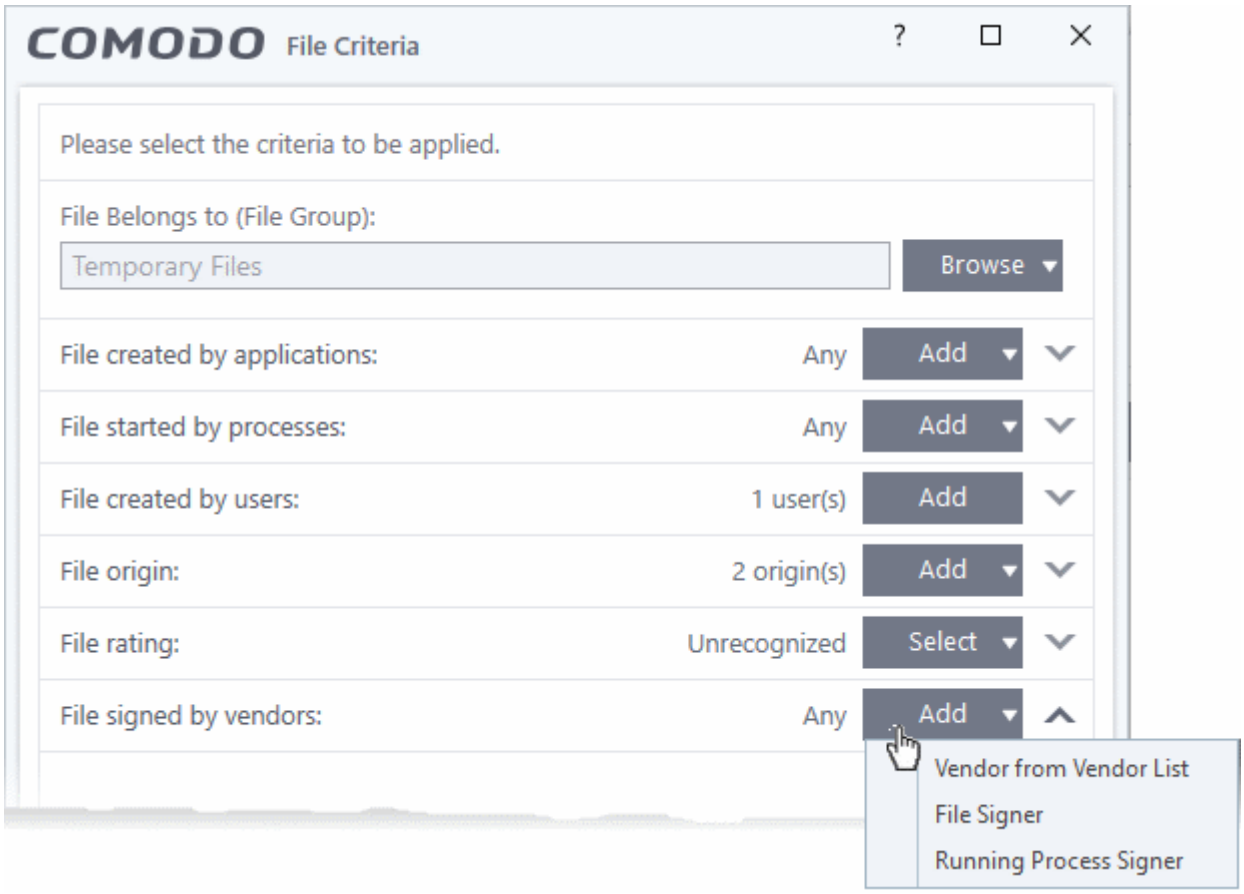
Auto-contain a file based on the software vendor

- You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.
- You can also specify the file rating of the vendor. The rule will only contain a file if its vendor has the stated trust rating.

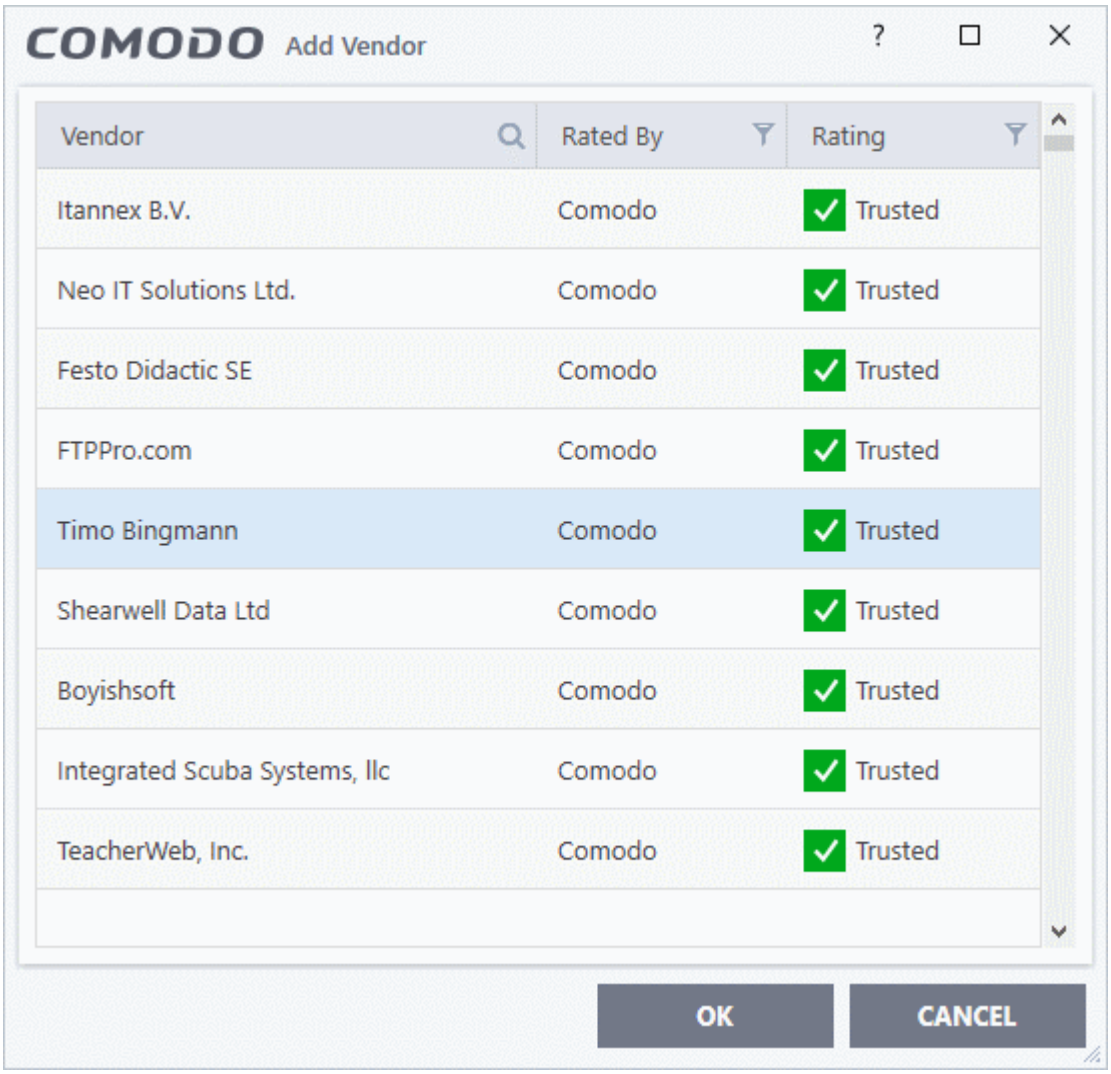
Specify vendors

- Click the 'Add' button in the 'File signed by vendors' stripe.
- There are three ways you can add a vendor:

  1. Directly select a vendor



- Choose 'Vendor from a Vendor List' from the drop-down
- The 'Add Vendor' dialog opens with a list of vendors in the **Vendor List**



- Use the sort and filter options in the column headers to search for the vendor to be specified
- Choose the vendor and click 'OK'. The vendor will be added as a criterion.

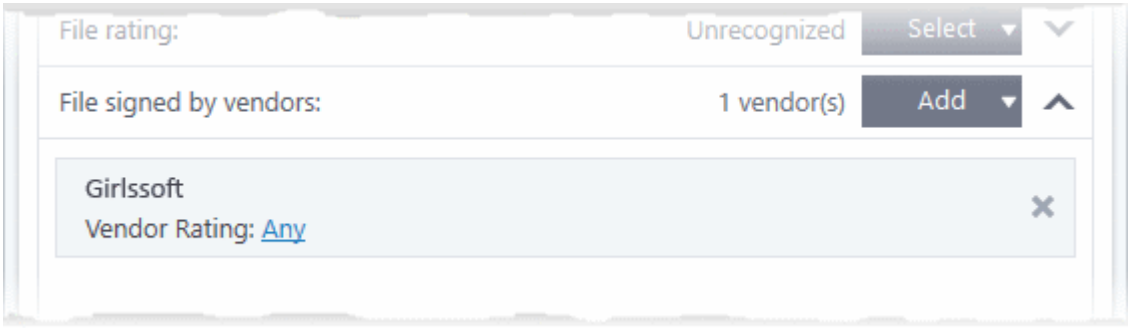
2. Specify an executable file on your local drive

- Choose 'File Signer' from the drop-down
- Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
- CCS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

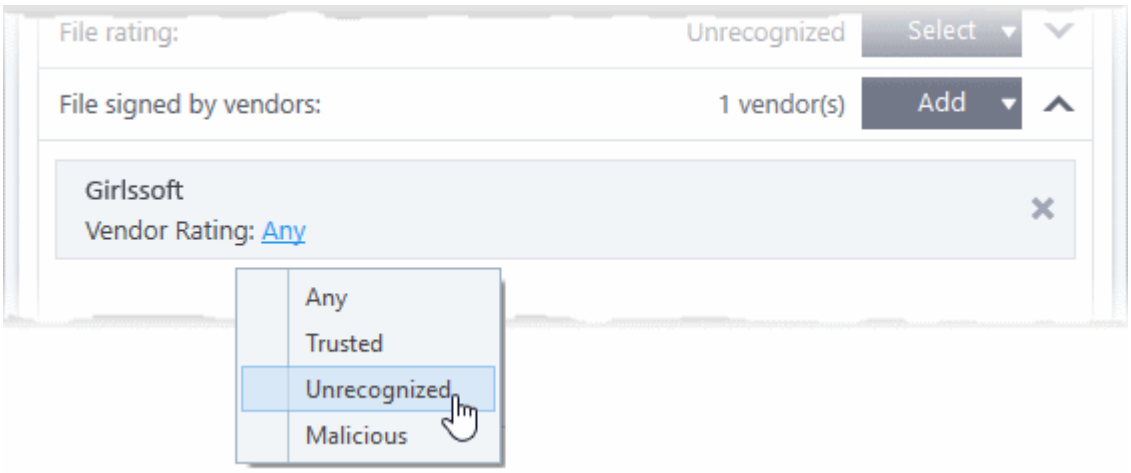
3. Select a currently running process

- Choose 'Running Process Signer' from the drop-down
- A list of all processes running at present on your computer is shown
- Select the process to specify the publisher of the application that started the process and click 'OK'
- CCS checks that the .exe file that started the process is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

The selected vendor is added:



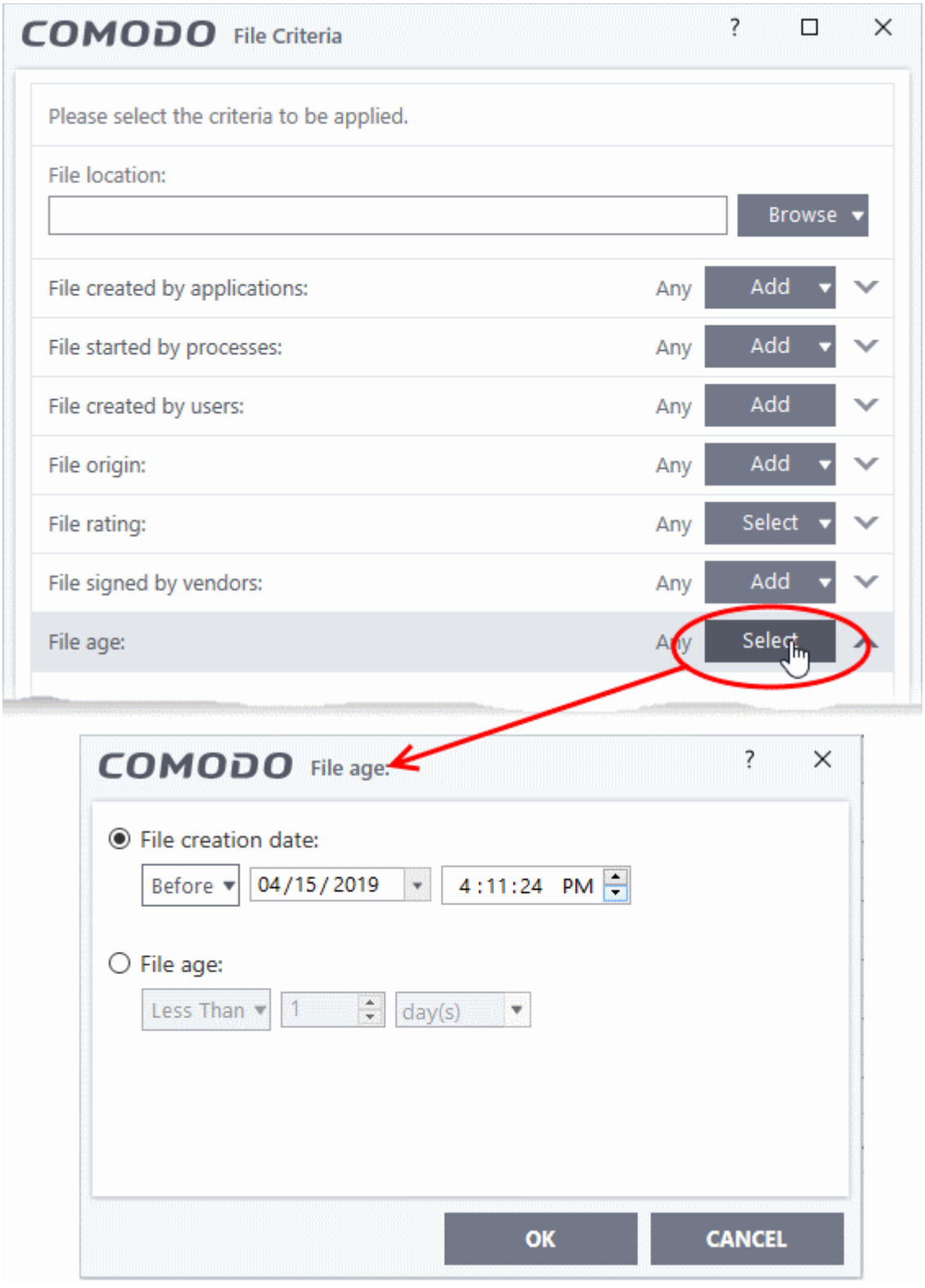
- **Vendor Rating** - The rule will only apply to the vendor's files IF the vendor has this rating at the time the file is checked. Note, the rating you set here can be different to the actual vendor rating in 'Settings' > 'File Rating' > 'File List' > 'Vendor Rating'.
  - Example. If you select 'Trusted' here, then CCS will apply the rule if the vendor is trusted at the time the file is checked. If the vendor's rating changes to 'Malicious' or 'Unrecognized', then the rule isn't applied.



- Repeat the process to add more vendors

Set the file age as filter criteria

- Click the 'Select' button in the 'File age' stripe.

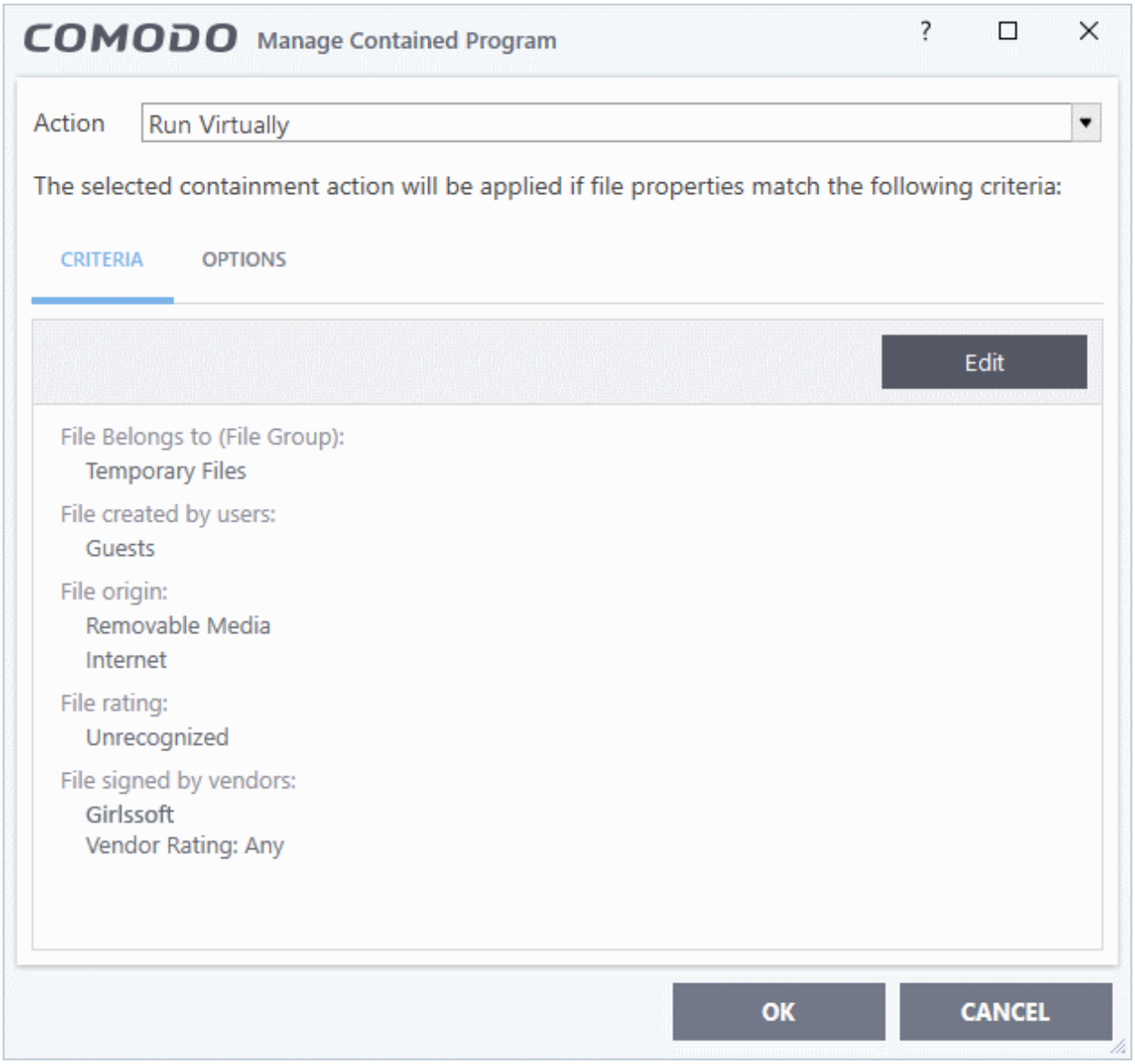


The 'File Age' dialog will appear. You can set the file age in two ways:

- **File Creation Date** - To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- **File age** - To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - **Less Than** - CCS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)

- **More Than** - CCS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)

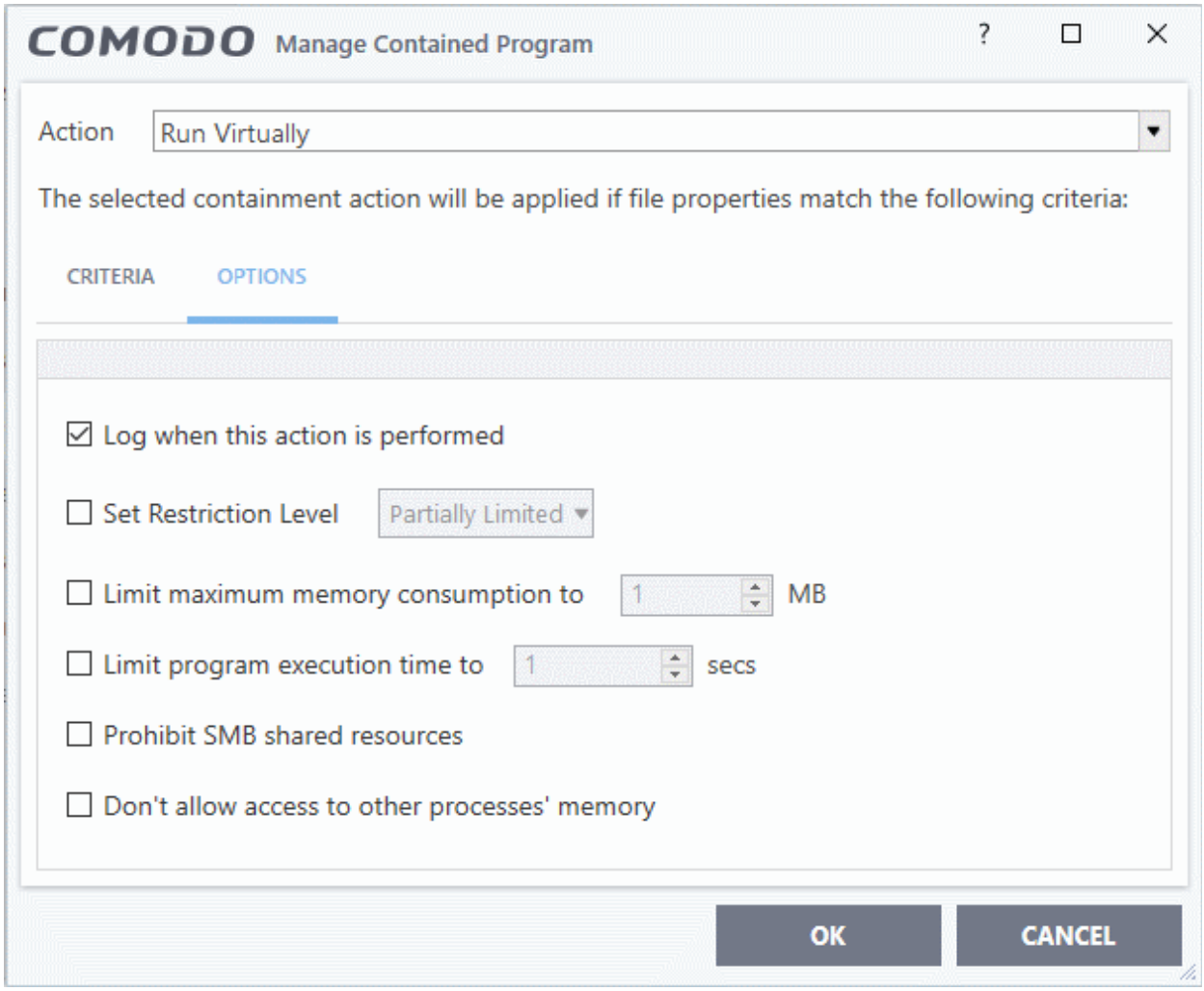
- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.



Step 3 - Select Options

The next step is to choose additional options and restrictions on items contained by the rule.

- Click the 'Options' tab.



The options available depend on the 'Action' chosen in **Step 1**.

The '**Ignore**' action has the following options:

- **Log when this action is performed** - CCS will create a containment log when the rule is triggered.
- **Don't apply the selected action to child processes** - Child processes are those started by the target application.
  - This option is disabled by default, so the ignore rule also applies to child processes.
  - If enabled, the ignore rule does not apply to child processes. Each child process will be inspected individually and all relevant rules applied.

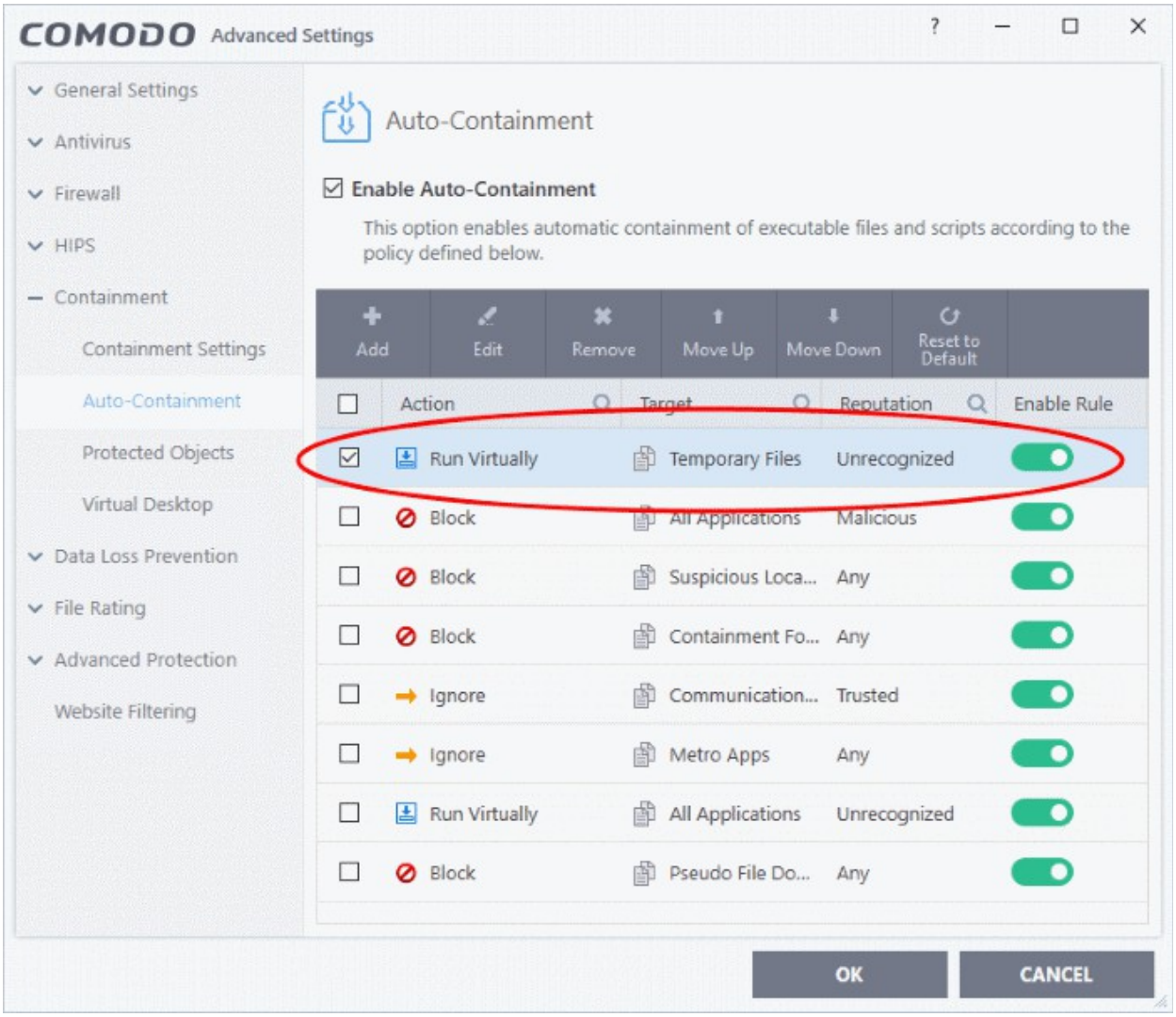
The '**Run Restricted**' and '**Run Virtually**' actions have the following options:

- **Log when this action is performed** - CCS will create a containment log when the rule is triggered.
- **Set Restriction Level** - If you choose 'Run restricted' or 'Run virtual' as the action, then you can also choose a restriction level. Here are the possible levels:
  - **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.
- **Prohibit SMB shared resources** - Programs contained by the rule cannot access network resources over the server message block (SMB) protocol. This includes, for example, shared disks, printers, folders, data or storage devices.
- **Don't allow access to other processes' memory** - Available only if you chose 'Run restricted' or 'Run virtual' as the action in step 1.
    - By default, contained applications are allowed to read the memory of other applications.
    - Enable this option if you want block this read capability.
    - This is useful, for example, to prevent unknown applications in the container from reading sensitive data loaded into memory by other programs. However, it may cause some contained programs to run incorrectly.

The '**Block**' action has the following options:

- **Log when this action is performed** - CCS will create a containment log when the rule is triggered.
- **Quarantine program** - If checked, the programs will be automatically quarantined. See **Manage Quarantined Items** for more information.
- Choose the options and click 'OK' to save them for the rule. The rule will be added and displayed in the list.



You can move the rule up or down the list to change its priority.

Edit an Auto-Containment Rule

- Select a rule from the list in the Auto-Containment panel and click 'Edit' from the top.
- The edit procedure is similar to **adding an auto-containment rule**.
- Click 'OK' to save the rule changes.

Important Note: Please make sure auto-containment rules do not conflict. In the event of a conflict, the setting in the rule that is higher in the list prevails. The 'Reset to Default' button lets you restore the original rules.

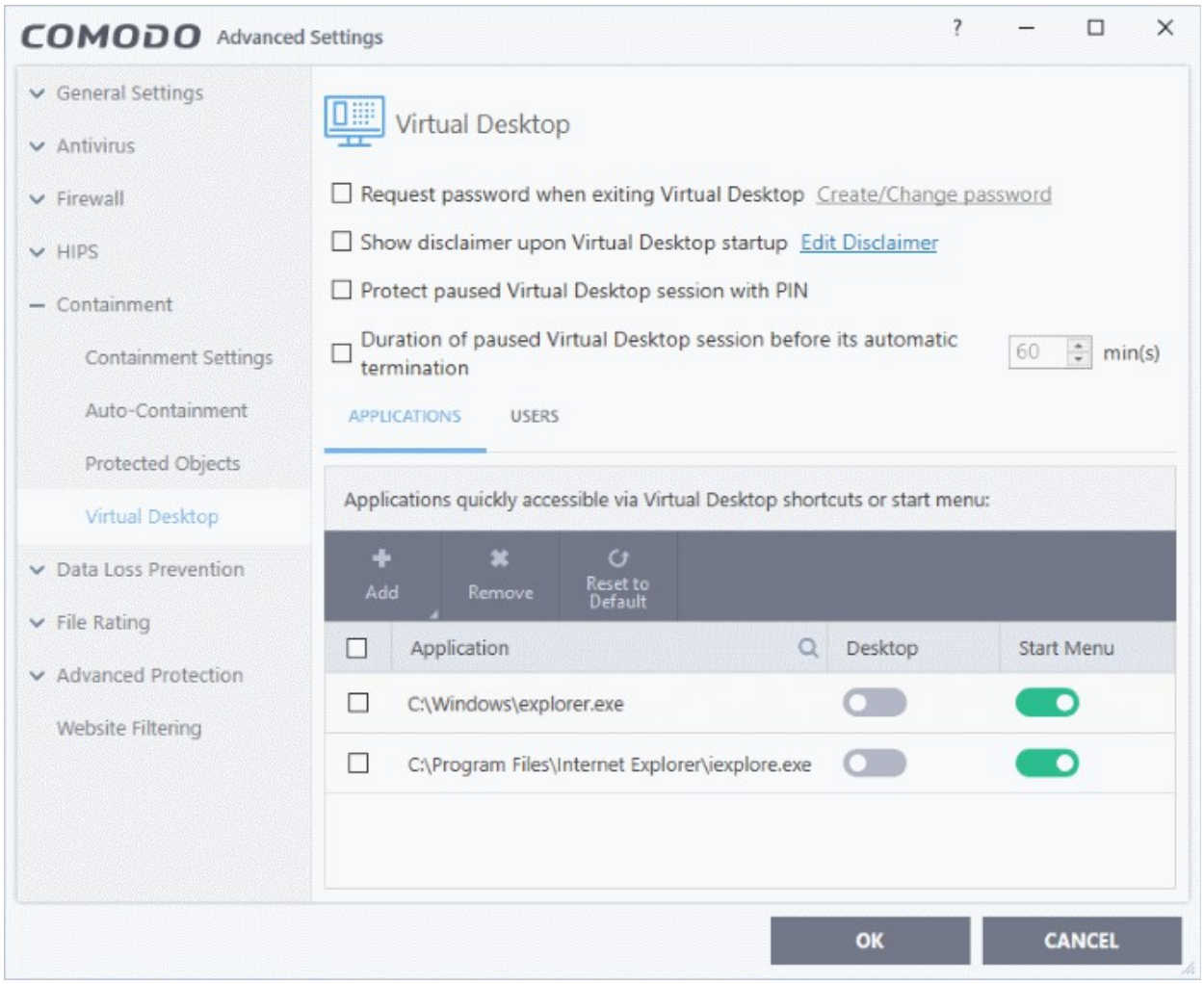
7.7.3. Virtual Desktop Settings

- Click 'Settings' > 'Containment' > 'Virtual Desktop'
- Virtual desktop settings let you set password protection, automatic login for specific users, and more.
- You can also configure desktop and start-menu shortcuts which will launch applications in the virtual desktop

Configure virtual desktop settings

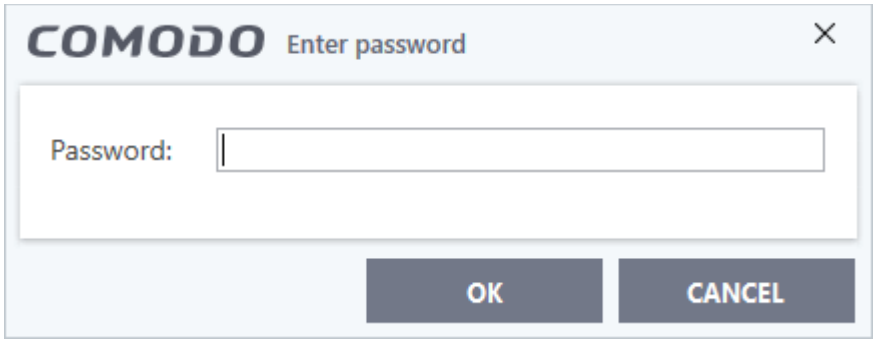
- Click 'Settings' on the CCS home screen

- Click 'Containment' > 'Virtual Desktop'



The interface allows you to:

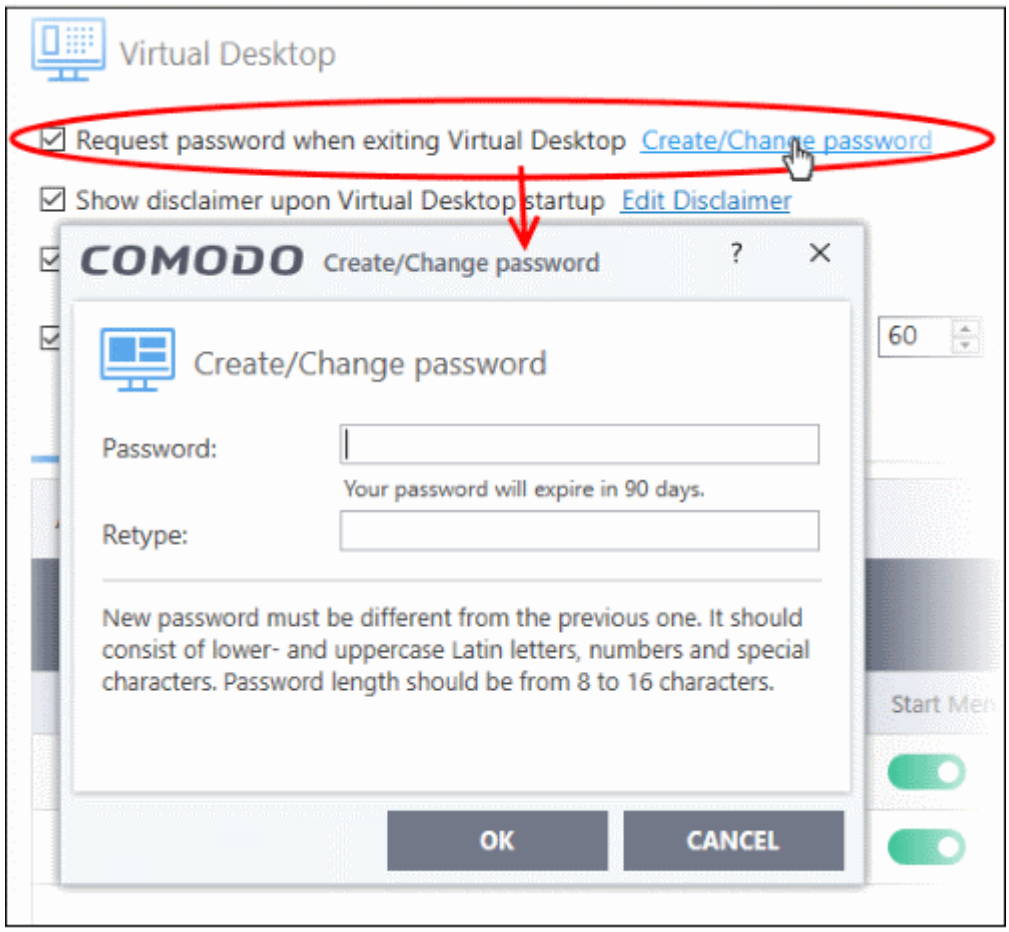
- **Set an exit password for virtual desktop**
- **Configure 'Disclaimer' shown during startup of virtual desktop**
- **Secure virtual desktop sessions with a PIN**
- **Set time-out period for paused virtual desktop sessions**
- **Add applications to virtual desktop**
- **Set virtual desktop to start automatically when selected users / users in selected user group log-in**
- **Request password when exiting Virtual Desktop** - Create an 'exit' password for the virtual desktop. Users need to enter the password in order to close the virtual desktop.



This prevent users from closing the virtual desktop and accessing the host, potentially exposing the

computer to danger. (***Default = Disabled***)

- Click 'Settings' > 'Containment' > 'Virtual Desktop'
- Enable 'Request password when exiting Virtual Desktop'
- Click the 'Create/Change password' link:

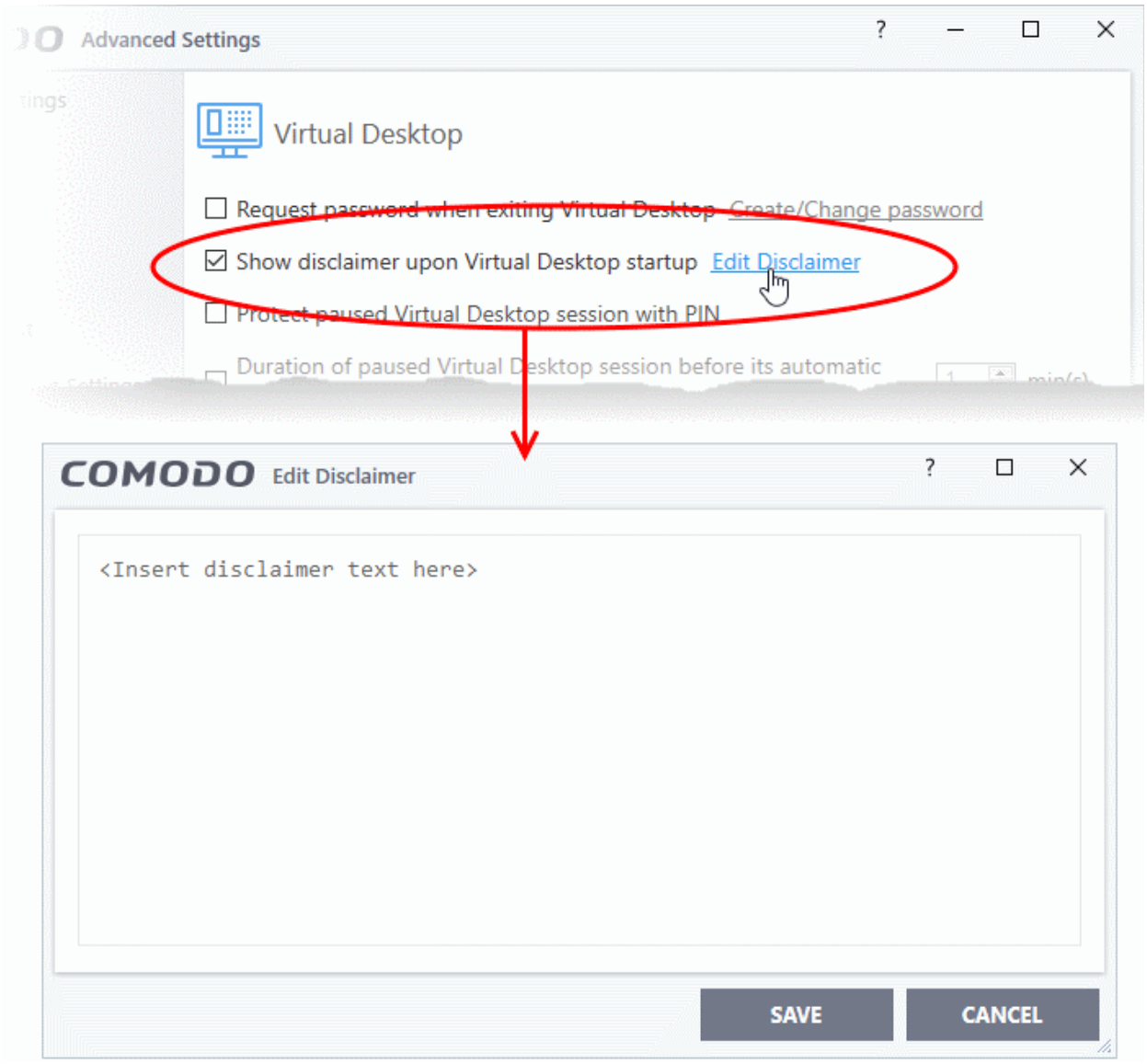


- Type a password that cannot easily be guessed.
- It should be 8-16 characters long and contain a mix of upper case letters, lower case letters, numbers, and special characters.
- Confirm the password then click 'OK'.
- The validity of the password is 90 days. You need to reset the password when it expires.

- **Show disclaimer upon Virtual Desktop startup** - Create a disclaimer which is shown when the virtual desktop starts. Users must accept the disclaimer before they can access the virtual desktop. Default = Enabled.

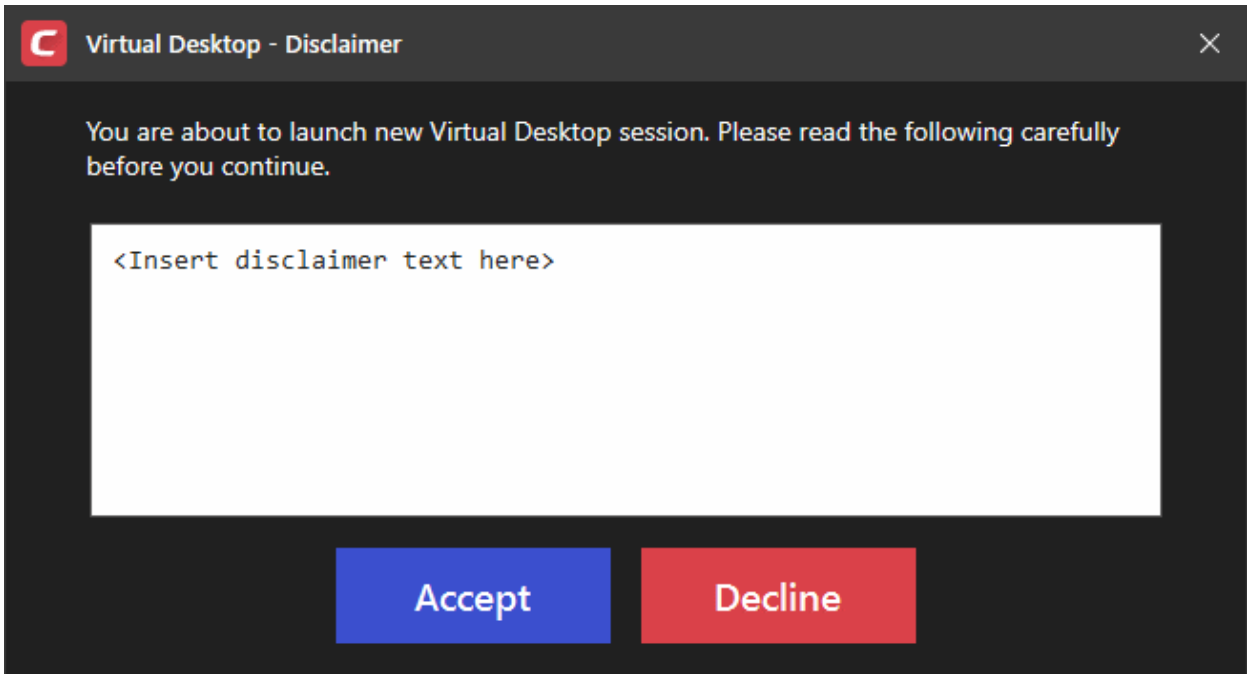
Create Virtual Desktop disclaimer

- Click 'Settings' > 'Containment' > 'Virtual Desktop'
- Enable 'Show disclaimer upon Virtual Desktop startup'
- Click the 'Edit Disclaimer' link:

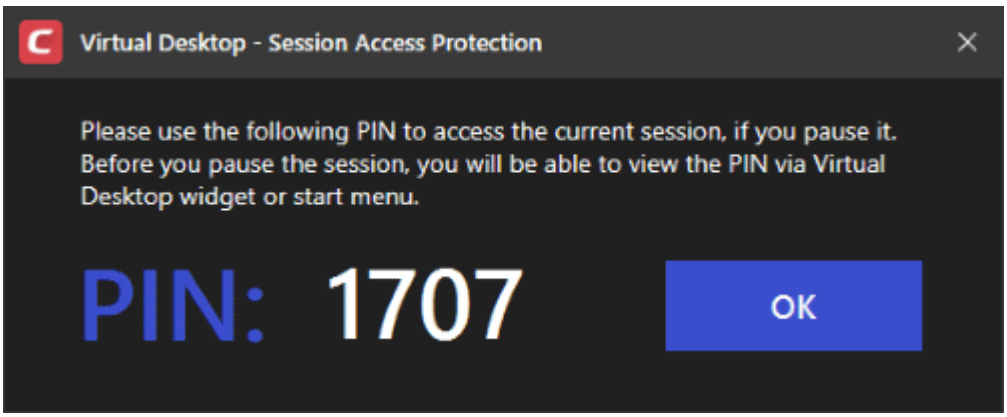


- Enter the disclaimer message and click 'Save'.

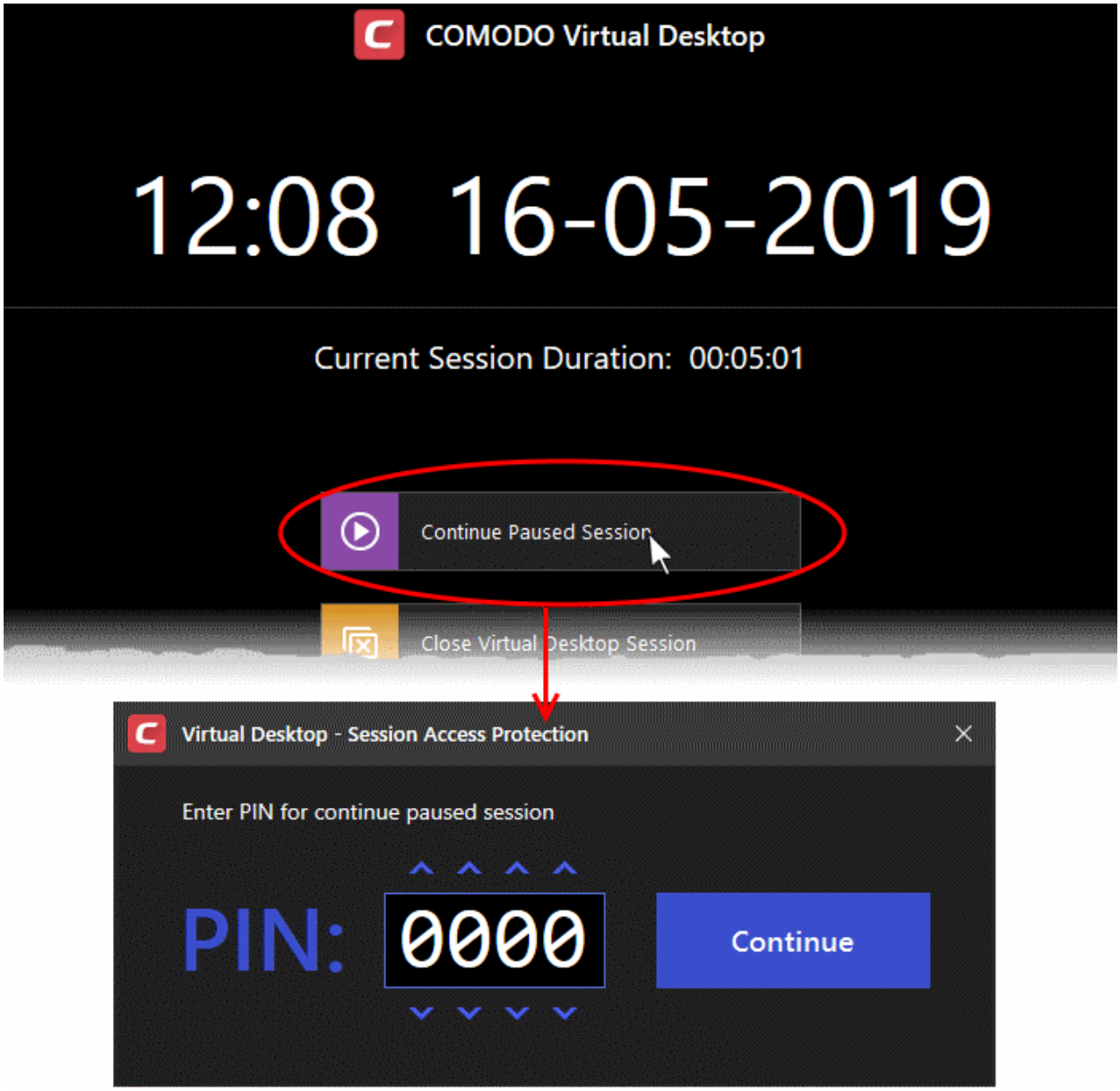
- The message is shown when the virtual desktop starts.
- Users should read the disclaimer and click 'Accept':



- **Protect paused Virtual Desktop session with a PIN** - Generates a session specific PIN number during virtual desktop startup. The PIN is required to resume the session from a paused state. This creates a second layer of authentication on top of the regular Windows username/password for any sensitive data in the virtual desktop. The feature is also useful on shared computers as it prevents other users from accessing the session. (***Default = Disabled***).
    - Select this option if you want to secure virtual desktop sessions with a PIN



    - Click 'Show PIN' in the start menu to view the number at any time.
    - The user needs to make a note of the PIN. If they pause the virtual desktop session they will need to enter the PIN to resume.



- See **Pause and Resume the Virtual Desktop** for more details on pausing and resuming a virtual desktop session

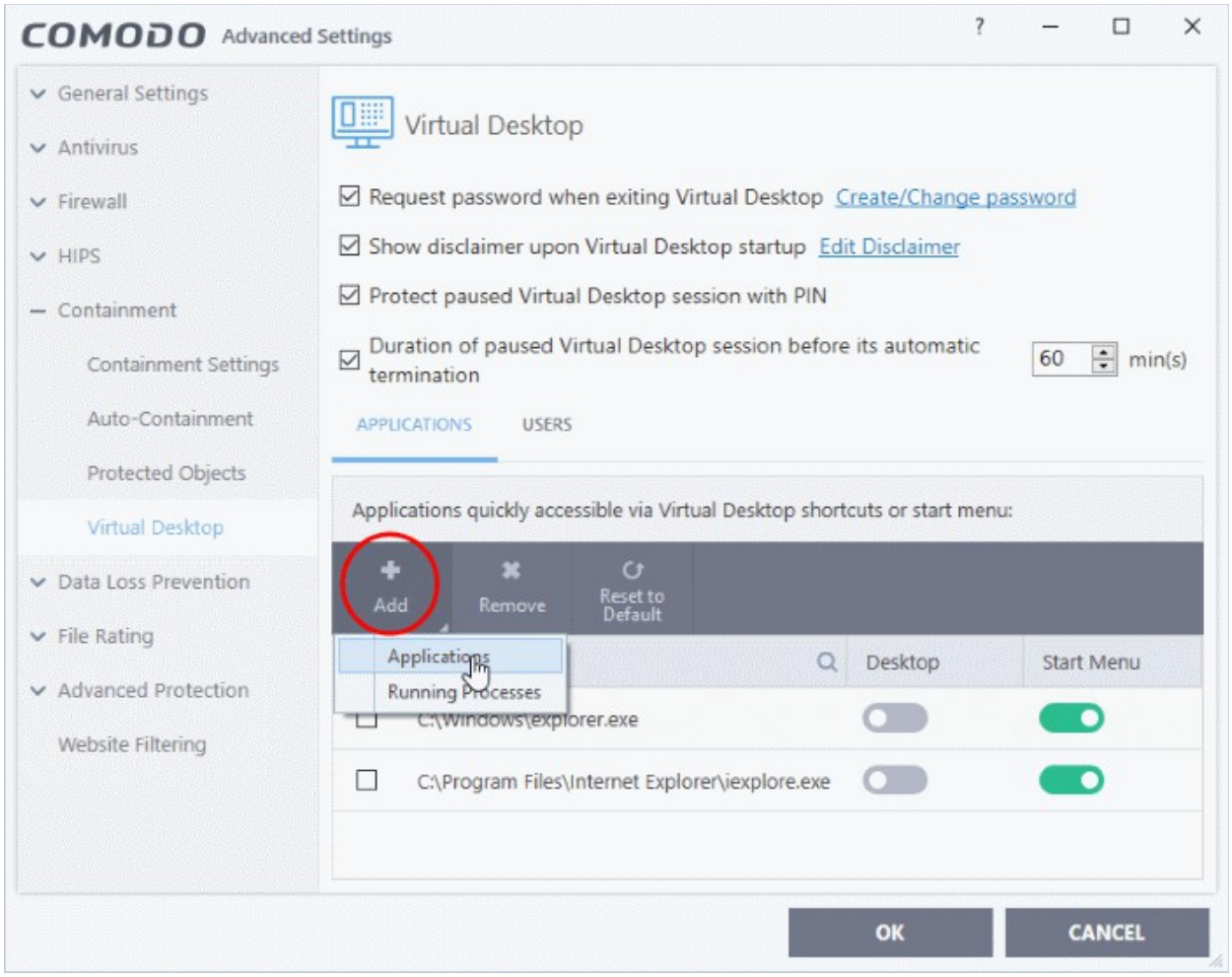
- **Duration of paused Virtual Desktop session before its automatic termination** - Set the maximum length of time a virtual desktop session can be left in paused state. The session gets automatically terminated when this period elapses. (***Default = Disabled***)

Add applications to virtual desktop

- The virtual desktop start menu has shortcuts for Windows explorer and your installed browsers.
- You can also add shortcuts in the virtual desktop for any other application.
- Alternatively, you can open any application inside the virtual desktop by navigating to the executable file.
- This section explains how to add and shortcuts for applications that you want to run inside the virtual desktop

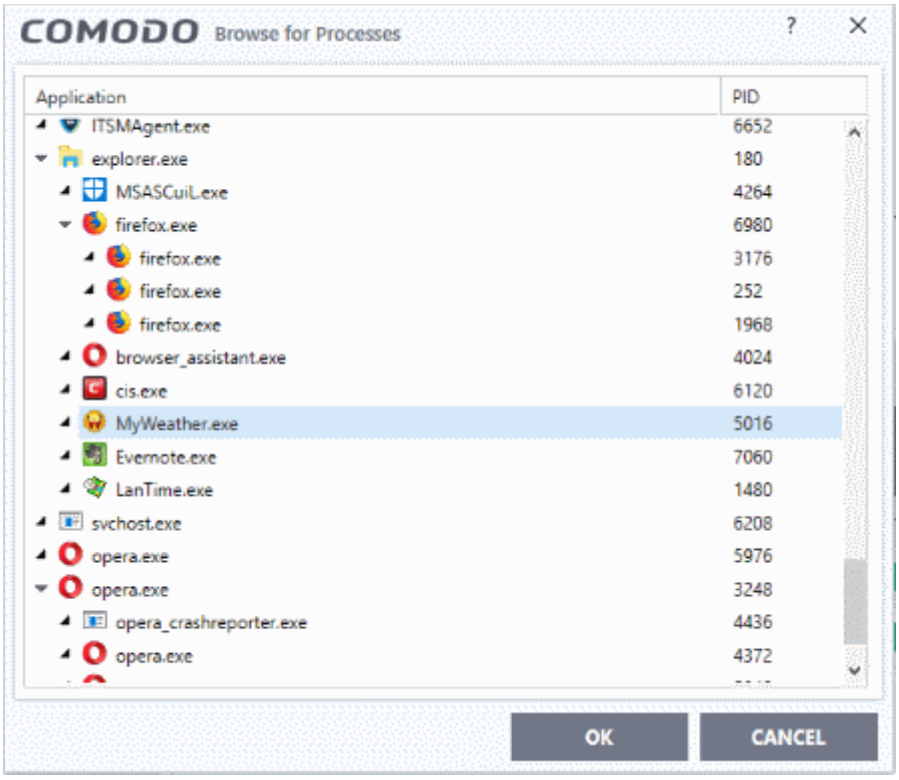
Add application shortcuts and start menu items to virtual desktop

- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Virtual Desktop'
- Click 'Add' under 'Applications' in the 'Virtual Desktop' settings interface

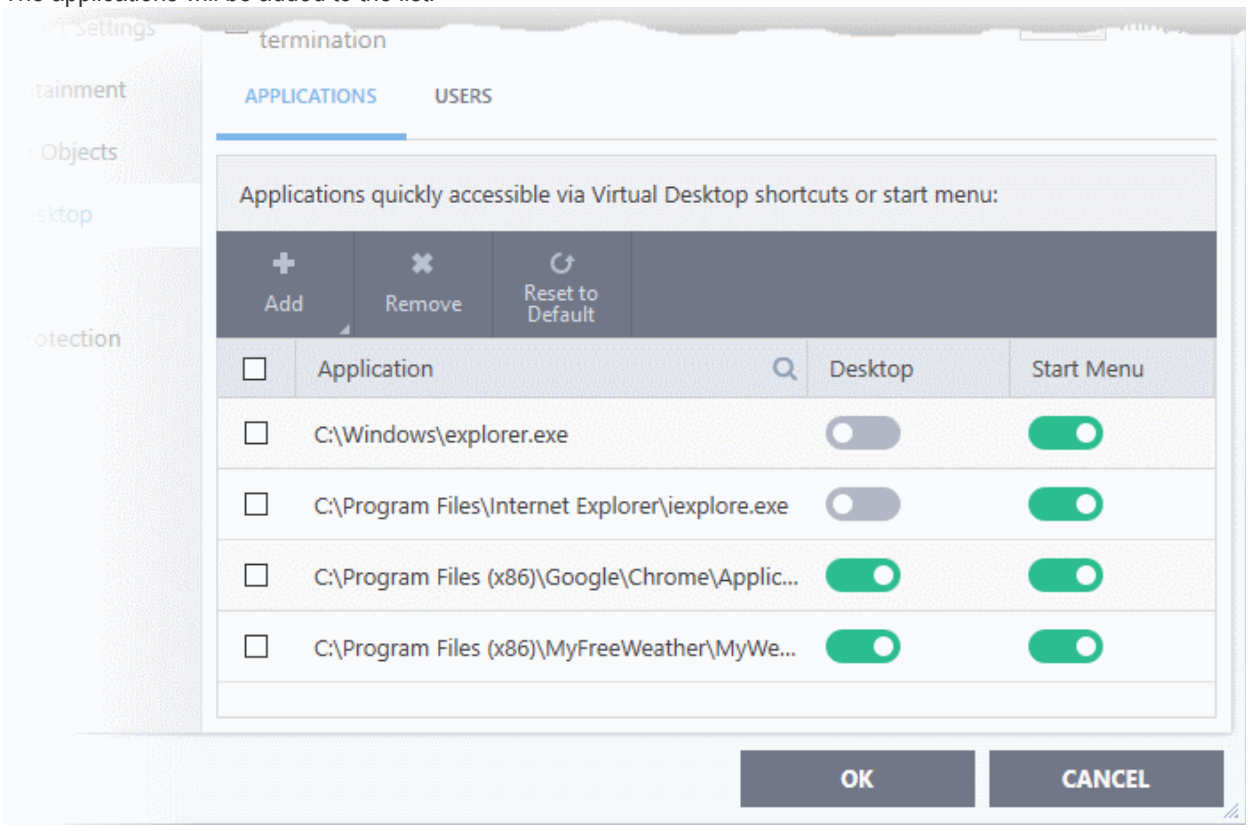


You can add applications in two ways:

- **Application** - Navigate to the location of the executable file for the application and select 'Open'
- **Running Processes** - Select the process from the list of currently running processes, whose parent application is to be added click 'OK'.



The applications will be added to the list:

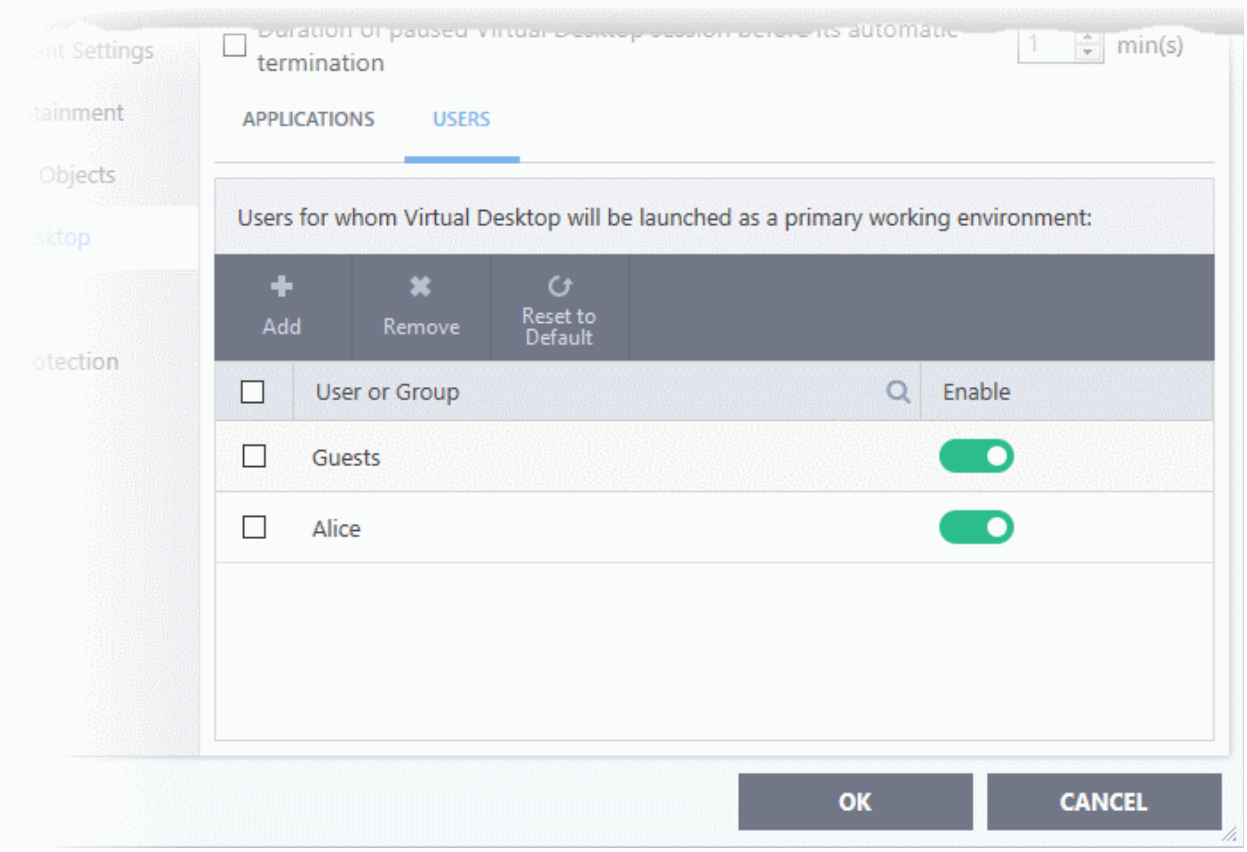


- Use the 'Desktop' and 'Start Menu' switches to enable/disable each type of shortcut per application.
- Click 'OK' to save your settings
- Click OK in the 'Advanced Settings' dialog for your changes to take effect

Add users who should log straight into the virtual desktop

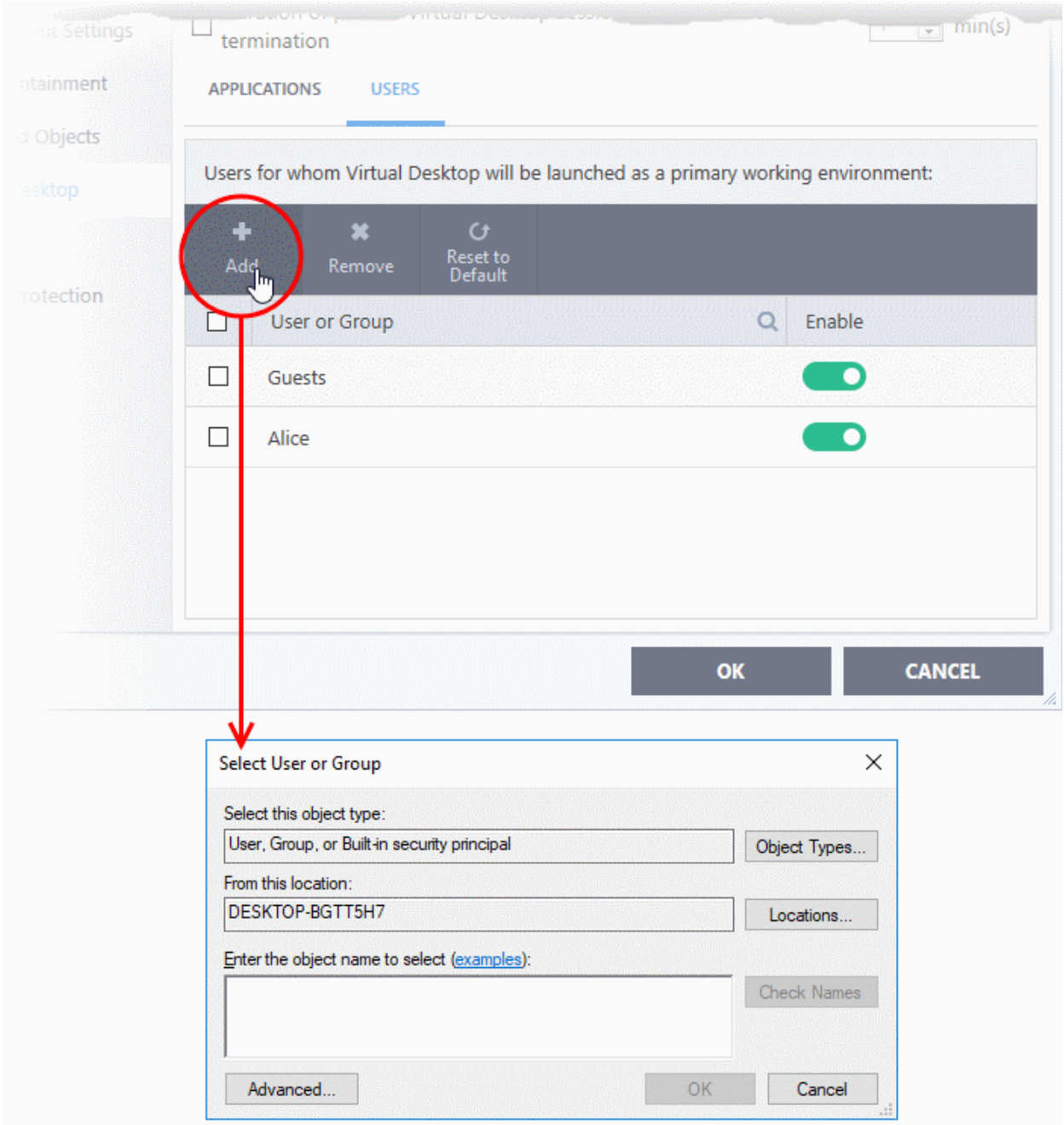
- You can configure the virtual desktop to start automatically whenever certain users login to the system.

- This means the virtual desktop becomes the default operating environment for those users.

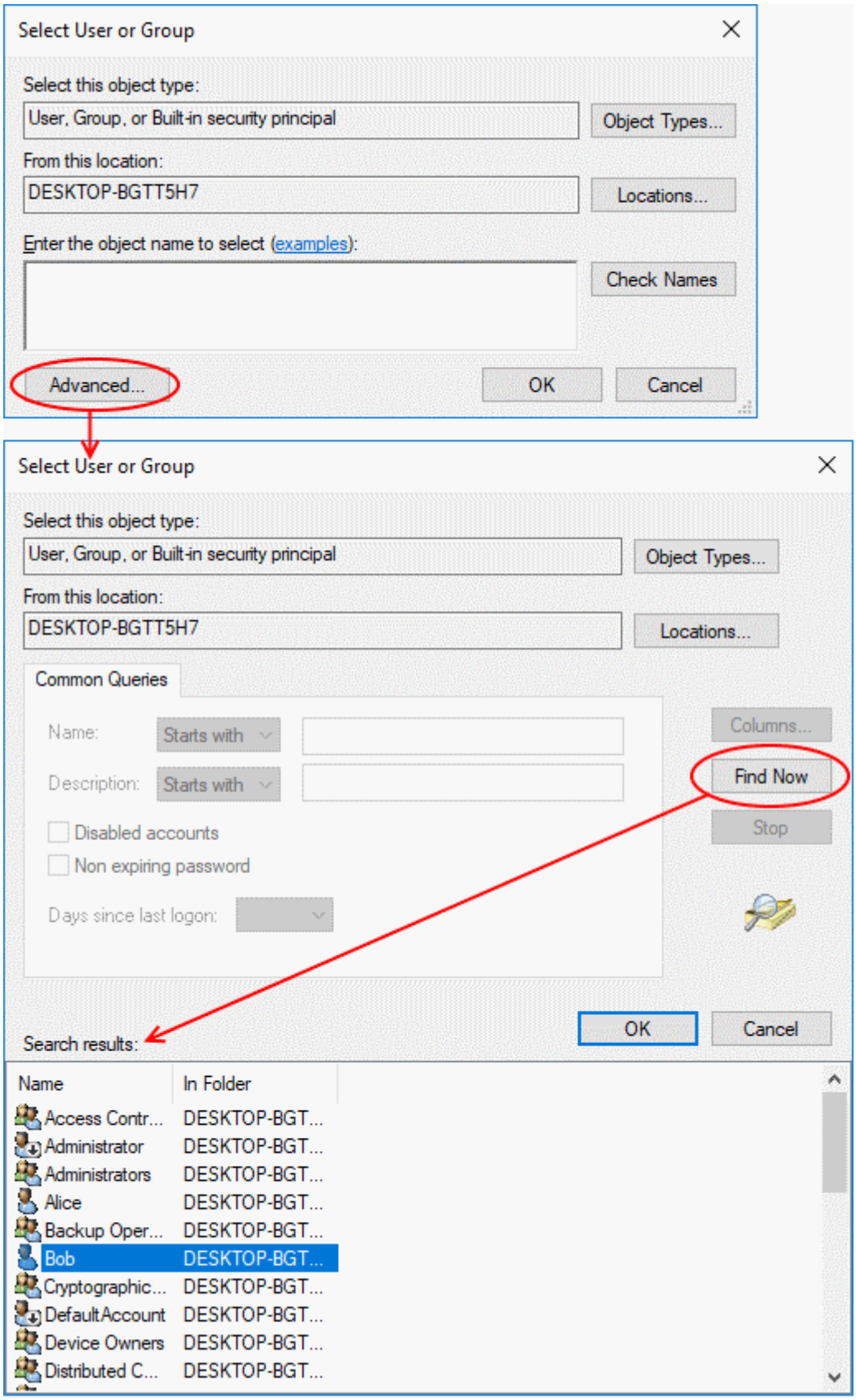


Add users

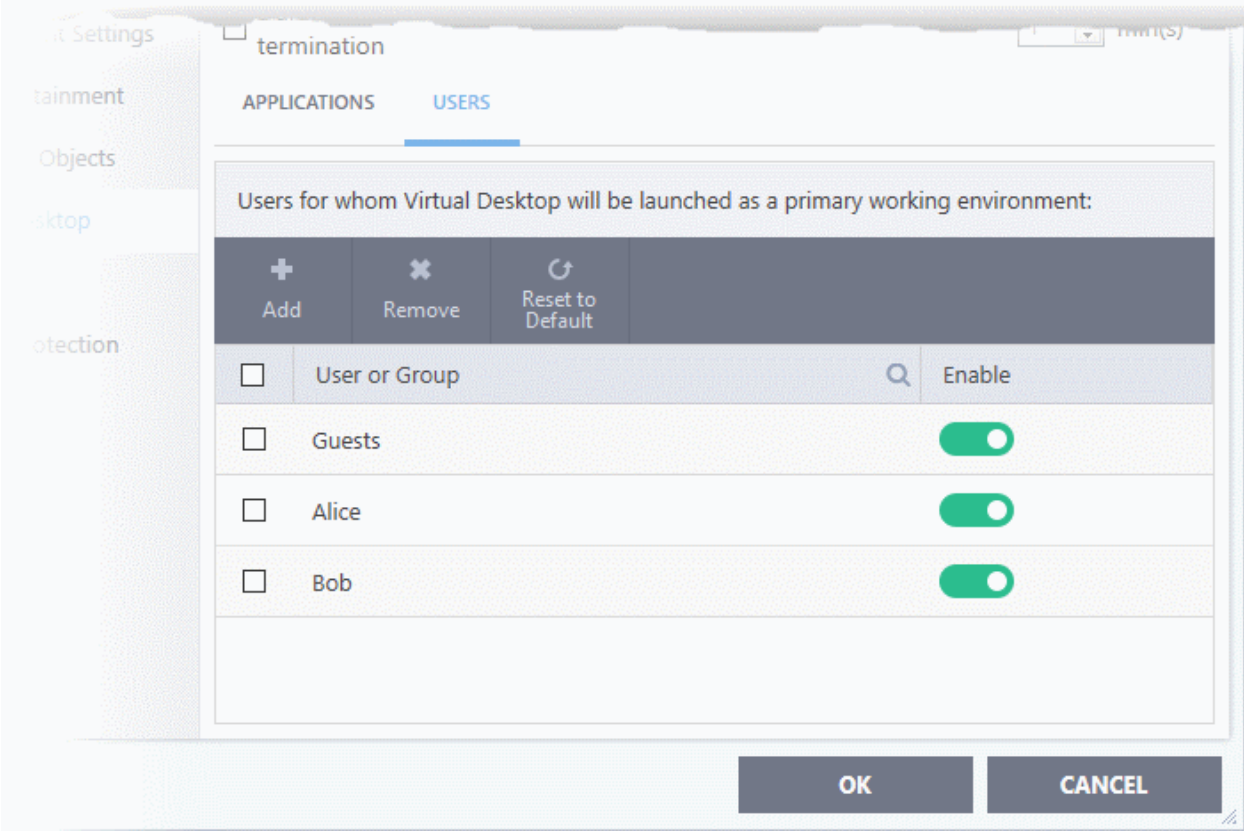
- Click 'Settings' on the CCS home screen
- Click 'Containment' > 'Virtual Desktop'
- Select the 'Users' tab
- Click 'Add'



- Select the users or user groups to whom you want this rule to apply.
  - Type the names of users or groups in the format <domain name>\<user/group name> or <user/group name>@<domain name>.
  - Alternatively, click 'Advanced' then 'Find Now' to locate specific users/user groups.
  - Click 'OK' to confirm.

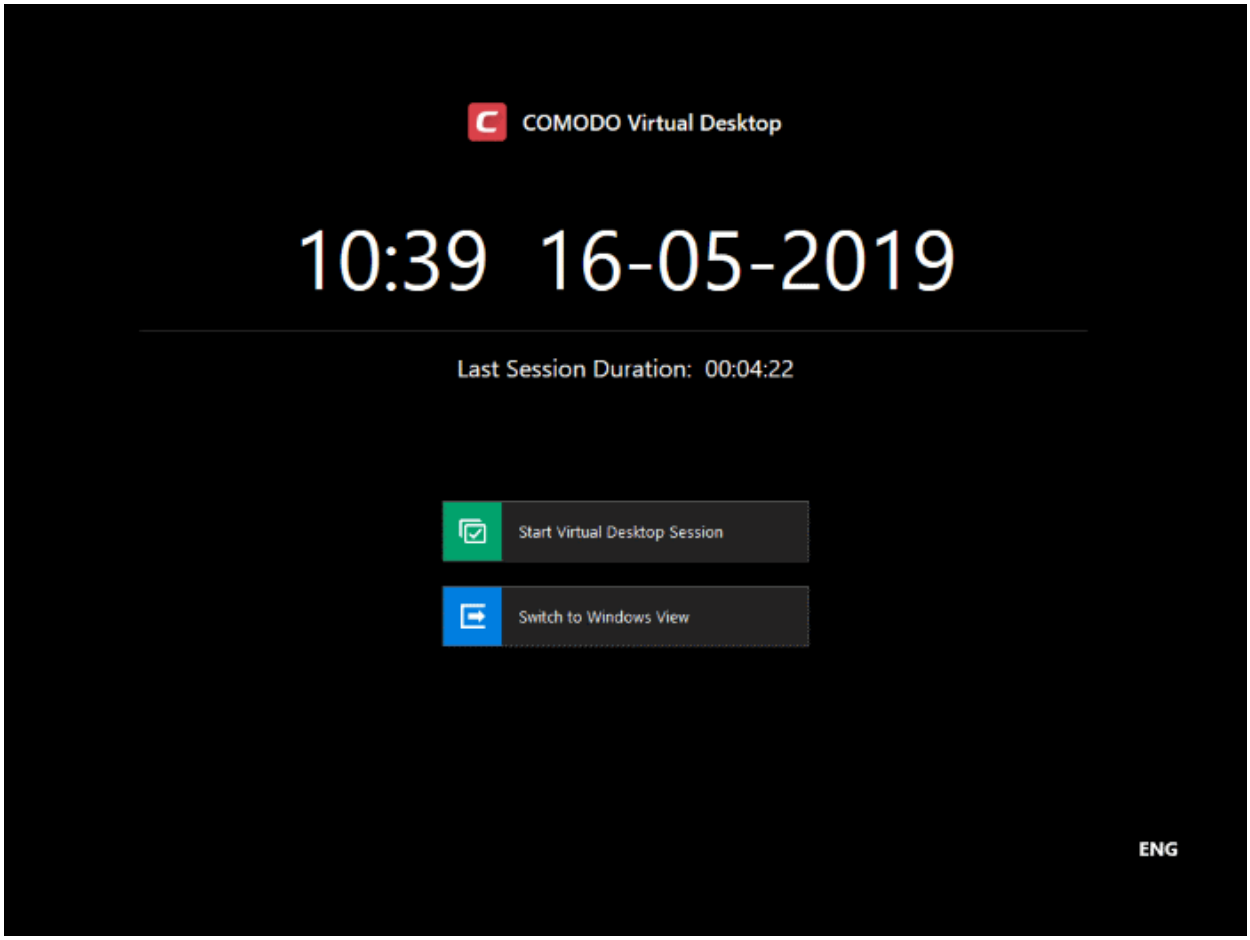


The user / user group will be added to the list.



- Repeat the process to add more users.
- Click 'OK' to save your settings
- Click OK in the 'Advanced Settings' dialog for your changes to take effect

The virtual desktop starts automatically when the user signs-in to the computer.



- The user can decide whether to continue with the virtual desktop or switch to the host OS.
- If so configured, users will need to provide a password to close the virtual desktop.

7.7.4. Containment - An Overview

- The container is an isolated operating environment for unknown and untrusted applications.
- Running an application in the container means that it cannot make changes to other processes, programs or data on your local computer. Applications in the container are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of you real system.
- This delivers a smooth user experience by letting unknown applications run as normal while denying them the potential to cause damage.
- After an unknown application has been placed in the container, CCS also submits it to Valkyrie for behavior analysis. Valkyrie tests include:
  - Static analysis
  - Dynamic analysis
  - Valkyrie plugins and embedded detectors
  - Signature-based detection
  - Trusted vendor and certificate validation
  - Reputation system
  - Human expert analysis
  - If Valkyrie discovers that a file is malicious then it is added to the antivirus black list. The file is quarantined on the local machine and the user is alerted.
- Users can print documents from within the container. This is useful, for example, if a suspicious PDF has valid information that should be printed.

By uniquely deploying 'containment as security', CCS offers improved security, fewer pop-ups and greater ease of use than ever before.

7.7.5. Unknown Files: The Scanning Processes

- When an executable is first run it passes through the following CCS security inspections:
  - Antivirus scan
  - HIPS Heuristic check
  - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CCS (and therefore not scanned in the cloud) in the following ways:
  - Because it is on the local Comodo White List of known safe applications
  - Because the user has rated the file as 'Trusted' in the **File List**
  - Because the software publisher is rated as 'Trusted' in the **Vendor List**.
  - By the user granting the installer elevated privileges (CCS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CCS regards the installer and all files generated by the installer as safe)
- Additionally, a file is not sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS Ruleset (See **Active HIPS Rules** for more details)
- **Cloud Scanning**

  Step 1 - Comodo File Look-up Server (FLS)
- In order to try to establish whether a file is safe or not, CCS will first consult Comodo's File Look-Up Server (FLS) to check the latest signature databases:
  - A digital hash of the unrecognized process or file is created.
  - These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all known malware and a white list of the signatures of the 'safe' files.
    - First, our servers check these hashes against the latest available black-list
    - If the hash is discovered on this blacklist then it is malware
    - The result is sent back to the local installation of CCS
  - If the hash is not on the latest black-list, it's signature is checked against the latest white-list
    - If the hash is discovered on this white-list then it is trusted
    - The result is sent back to local installation of CCS
    - The local white-list is updated
  - The FLS checks detailed above are near instantaneous.
  - If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'.

    Step 2 - Vendor Rating
  - If a file is still 'unrecognized' after FLS check up, CCS checks the rating of the software publisher.
    - **'Trusted' vendor rating** - CCS will award trusted status to the file.
    - **'Malicious' vendor rating** - CCS will award malicious status to the software file and place it in quarantine.
    - **'Unrecognized' vendor rating** - The file will keep its unknown status and is run in the container. The file is also sent to Valkyrie for analysis.

    Step 3 - Valkyrie Analysis
  - Applications that have neither file rating nor vendor rating are first contained then submitted to Valkyrie for analysis.

- Unrecognized files uploaded to Valkyrie undergo a battery of static and dynamic analysis. At the end of the automated tests, files are analyzed by human experts for confirmation.
- Valkyrie returns its verdicts to CCS which will quarantine, allow or contain the file as appropriate.
- **Click here** to view Valkyrie online help guide

Important Note: In order for the software to submit unknown files to our file rating and malware analysis servers, please make sure the following IP addresses and ports are allowed on your network firewall:

- To allow communication with our FLSs:
  - IPs that need to be allowed:
    - 91.209.196.27
    - 91.209.196.28
    - 199.66.201.20
    - 199.66.201.21
    - 199.66.201.22
    - 199.66.201.25
    - 199.66.201.26
  - Ports that need to be allowed: 53 UDP and 80 TCP
  - Direction: Outgoing (Endpoints to FLSs)

7.8. File Rating Configuration

Click 'Settings' > 'File Rating' to open this interface.

- The file rating area lets you view and manage all trusted, malicious and unrecognized files.
- File ratings in CCS are obtained from our online file look-up service (FLS). This is a huge database of trust ratings of known files.
- When a file is first opened, CCS will consult the FLS to check the file's reputation on our global whitelist and blacklists.
- CCS will award 'Trusted' status to the file if:
  - The application is on our global whitelist of safe files.
  - The application has a 'Trusted' status in the CCS **File List**
  - The application is from a vendor rated as 'Trusted' in the **Vendor List**
- Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource use.
- Conversely, files which are on the blacklist of harmful files are given a status of 'Malicious'. These files are quarantined or deleted automatically.
- Files which are on neither the blacklist nor the whitelist are awarded 'Unrecognized' status.
- You can review unrecognized files in the **File List** interface ('Settings' > 'File Rating' > 'File List').
- You can also submit unknown files to Comodo for further analysis, or to run an on-demand file-lookup.

Important Note: In order to submit unknown files to our file rating and malware analysis servers, please make sure the following IP addresses and ports are allowed on your network firewall:

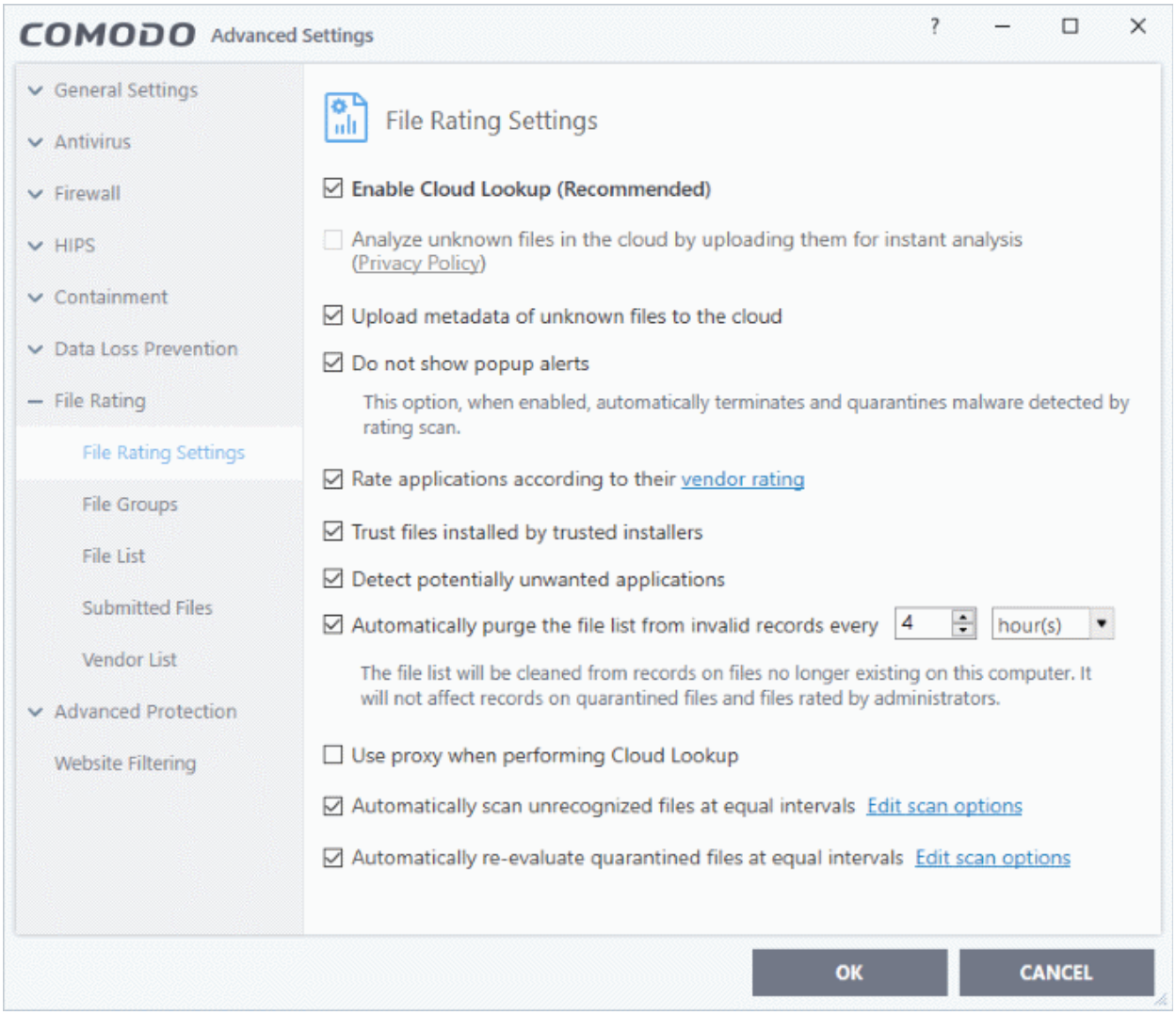
- FLS communication - please allows the software to access the following IP addresses:
  - 91.209.196.27
  - 91.209.196.28

- 199.66.201.20
- 199.66.201.21
- 199.66.201.22
- 199.66.201.25
- 199.66.201.26
- Allow ports 53 UDP and 80 TCP
- Direction: Outgoing (Endpoints to FLS)

The file ratings area lets you:

- Manually add files to the file list and assign them a rating.
- Submit unrecognized files for a file look-up, and view all files you have submitted previously.
- View and manage the vendor list, and assign trust ratings to vendors.

- Click 'Settings' on the CCS home-screen
- Click 'File Rating':



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

- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **File Groups** - Create predefined groups of one or more file types.

- **File List** - View, manage and investigate executable files on your computer and their current trust rating.
- **Submitted Files** - View any files already submitted to Comodo for analysis.
- **Vendor List** - View and manage the list of software publishers. Manually add vendors and assign trust ratings to them.

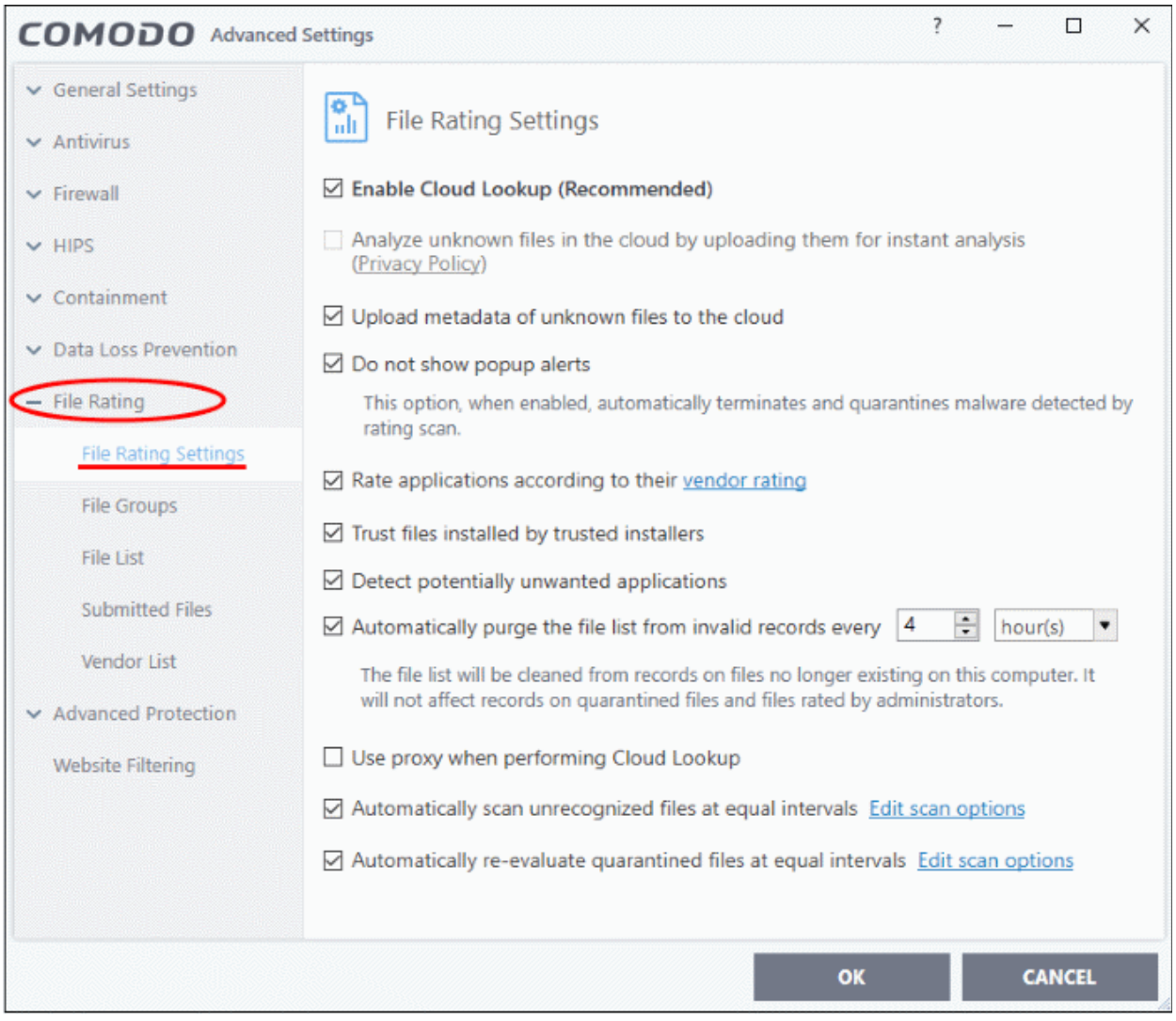
7.8.1. File Rating Settings

Click 'Settings' > 'File Rating' > 'File Rating Settings'

- A file rating determines how CCS interacts with a file:
  - 'Trusted' files are safe to run.
  - 'Untrusted' files are malware so they get quarantined or deleted.
  - 'Unknown' files are run in the container until they get rated as trusted or untrusted.
- The rating of a file can change over time, especially in the case of 'unknown' files. For example, an unknown file might be re-classified as 'trusted' or 'untrusted' after it has been tested.
- You can also configure whether CCS should auto-upload unknown files to Comodo for analysis.

Open the 'File Rating Settings' interface

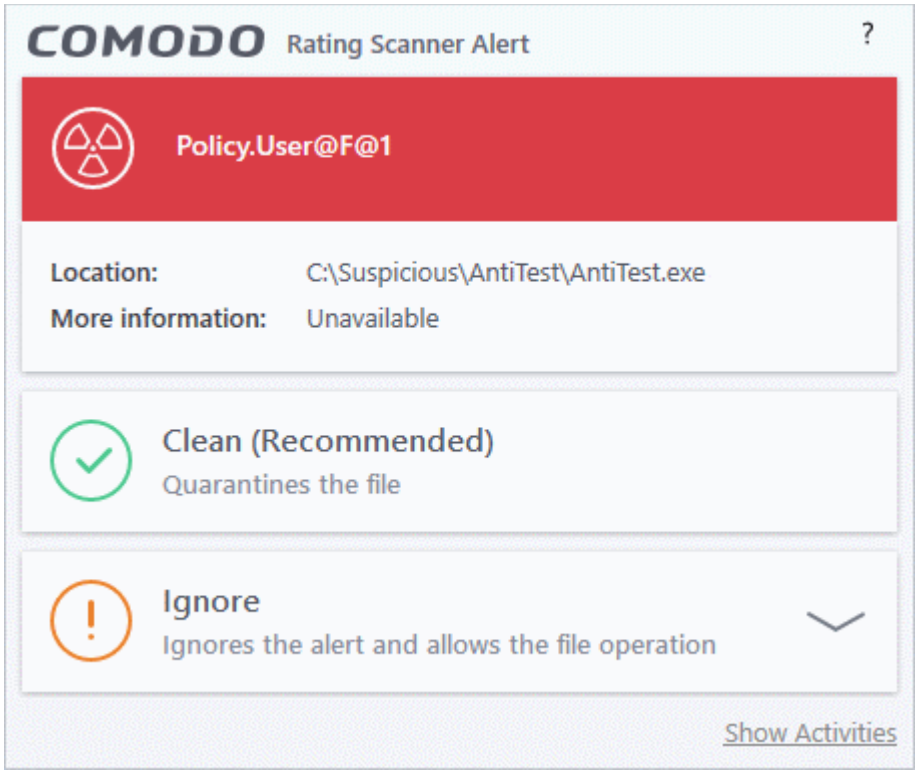
- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'File Rating Settings'



- **Enable Cloud Lookup** - CCS checks a file's trust rating on our cloud severs as part of the real-time scan

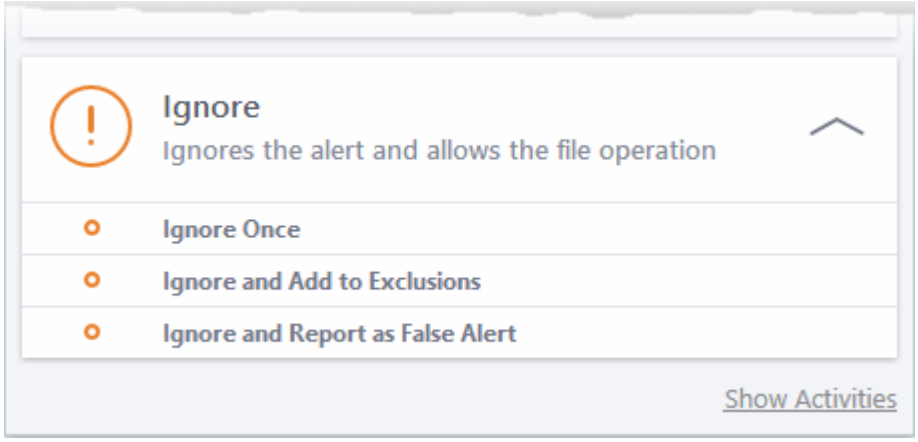
process.(***Default and recommended =Enabled***)

- **Analyze unknown files in the cloud by uploading them for instant analysis** - CCS uploads files with an 'unknown' trust rating to Comodo for further analysis. Our experts will analyze the file, award it a trust rating, and add it to the global whitelist or blacklist as appropriate. (***Default = Disabled***)
- **Upload metadata of unknown files to the cloud** - Metadata is basic file information such as file source, author, date of creation and so on. If enabled, CCS will also send the file metadata when uploading unknown files to Comodo. ***(Default =Enabled)***
- **Do not show popup alerts** - Whether or not CCS should show an alert when malware is detected by the cloud scanner (FLS). (**Default = Enabled**)
    - **Enabled** - No alerts are shown. This minimizes disturbances but at some loss of user awareness. CCS will automatically block and quarantine the threat.
    - **Disabled** - A rating scanner alert is shown for malicious files.



You can choose from these actions:

- **Clean** - The program is blocked and quarantined
- **Ignore** - Allows the file to run. Does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:



- **Ignore Once** - The file is allowed to run this time, but it will still be flagged as a threat by future scans.
- **Ignore and Add to Exclusions** - The file is allowed to run this time, and will not be flagged as a threat in future scans. The file is placed on the **Exclusions** list, meaning it is ignored permanently by the scanner.
- **Ignore and Report as a False Alert** - The file is allowed to run this time, and submitted to Comodo for analysis. Select this option if you think the file is safe, and that CCS was wrong to flag it as a threat. Comodo will re-examine the file.

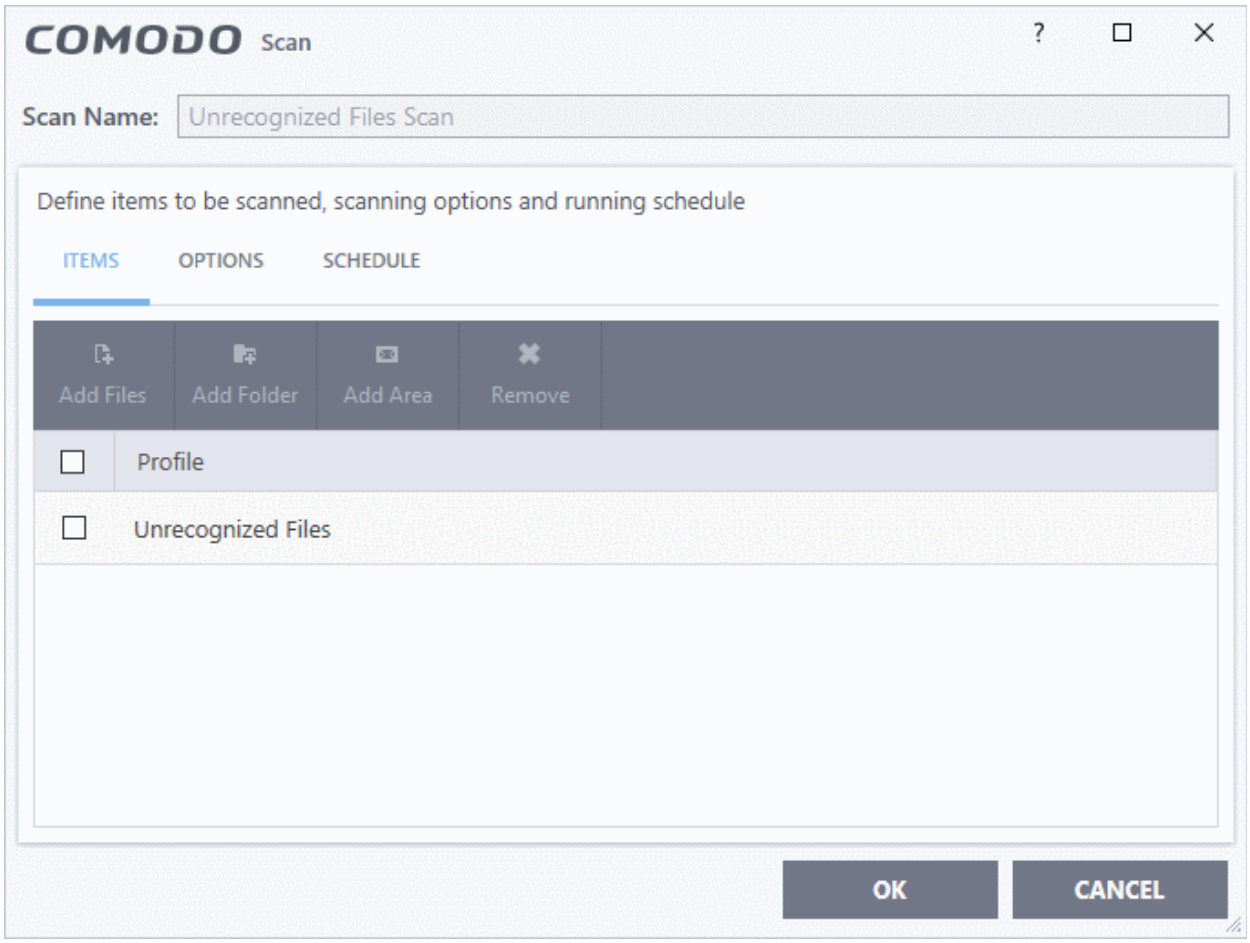
- **Rate applications according to their vendor rating** - CCS will give files the same rating as the trust rating of the publisher (software creator). For example - if the vendor is trusted, then all files created by the vendor will be trusted. (***Default =Enabled***)
  - The vendor is the software company who created and digitally signed the file.
  - You can view vendor trust ratings in 'Advanced Settings' > 'File Rating' > 'Vendor List'.
  - CCS ships with a list of vendors with 'Trusted' status. You can add new vendors to the list and set your own vendor ratings as required.
  - The vendor rating priority is shown below:
    - Admin
    - User
    - Comodo
  - Click the 'Vendor Rating' link to open the 'Vendor List' screen. See **Vendor List** for more details.
- **Trust files installed by trusted installers** - CCS awards trusted status to files whose parent applications are listed in the 'Installer or Updater' rule in **HIPS Rules**. (***Default = Enabled***)
- **Detect potentially unwanted applications (PUA)** - CCS scans will flag applications that:

  (i) a user may or may not be aware is installed on their computer

  (ii) may contain functionality and objectives that are not clear to the user.

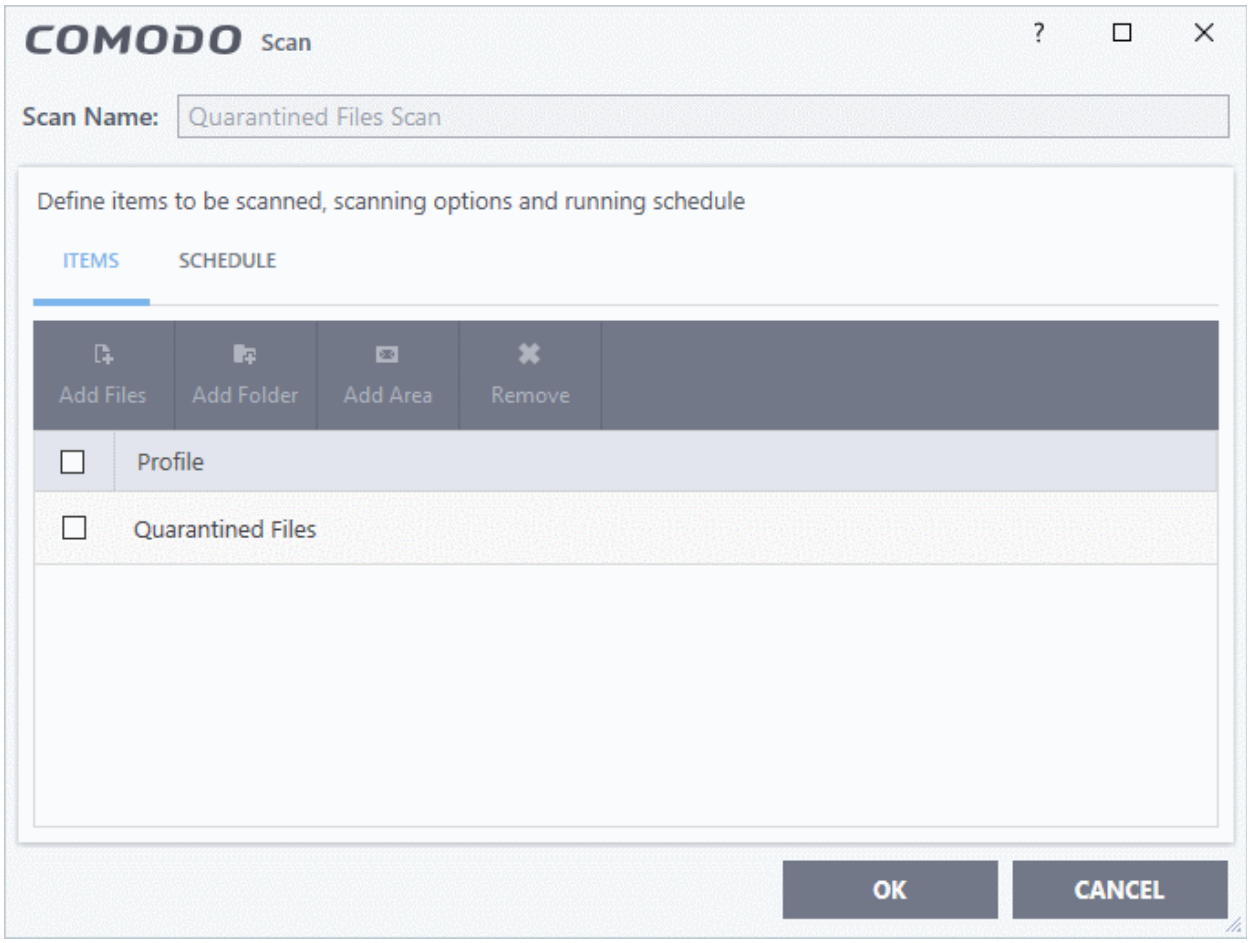
  Example PUA's include adware and browser toolbars.

  PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar that tells you the weather may also contain code that tracks your online activity (***Default = Enabled***).
- **Automatically purge unrecognized files every NN hour(s)** - CCS periodically checks that all unrecognized files in the list are still installed at the path specified. If not, the file is removed from the list. Select the interval in hours from the drop-down box. **(*Default = Enabled, 4 Hours*)**
- **Use proxy when performing Cloud Lookup** - CCS submits files to FLS for analysis through a proxy. The proxy server is same one that is defined for program and database updates.
  - See '**Configure Program and Virus Database Updates**' for more details. (***Default = Disabled***)
- **Automatically scan unrecognized files at equal intervals** - CCS can periodically re-scan unknown files to check whether a new trust rating is available for them. (***Default = Enabled and set for every 4 hours***)
  - Click 'Edit Scan Options' to configure the scan settings and schedule.



- **Scan Name** - The label of the scan. This is pre-configured and cannot be edited.
- **Items** - The files that are scanned by the profile. 'Unrecognized Files' is the default. You cannot edit or add files to this profile.
- **Scan Options** - Configure scan technologies, how to handle threats, and more. See **Configure scan options for the profile** in **Scan Profiles** for help with this.
- **Schedule** - Specify the frequency of the automated scans. See **Configure a scan schedule** in **Scan Profiles** for help with this. (***Default = Every 4 hours***).

- **Automatically re-evaluate quarantined files at equal intervals** - CCS checks our master online database for the latest trust rating on currently quarantined files. (***Default = Enabled and set for once every day***)
  - Click 'Edit Scan Options' to configure the scan schedule.



- **Scan Name** - The label of the scan. This cannot be edited.
- **Items** - The files that are scanned by the profile. 'Quarantined Files' is the default. You cannot edit or add files to this profile.
- **Schedule** - Specify the frequency of the automated scans. See **Configure a scan schedule** in **Scan Profiles** for help with this. (***Default = Once every day***).

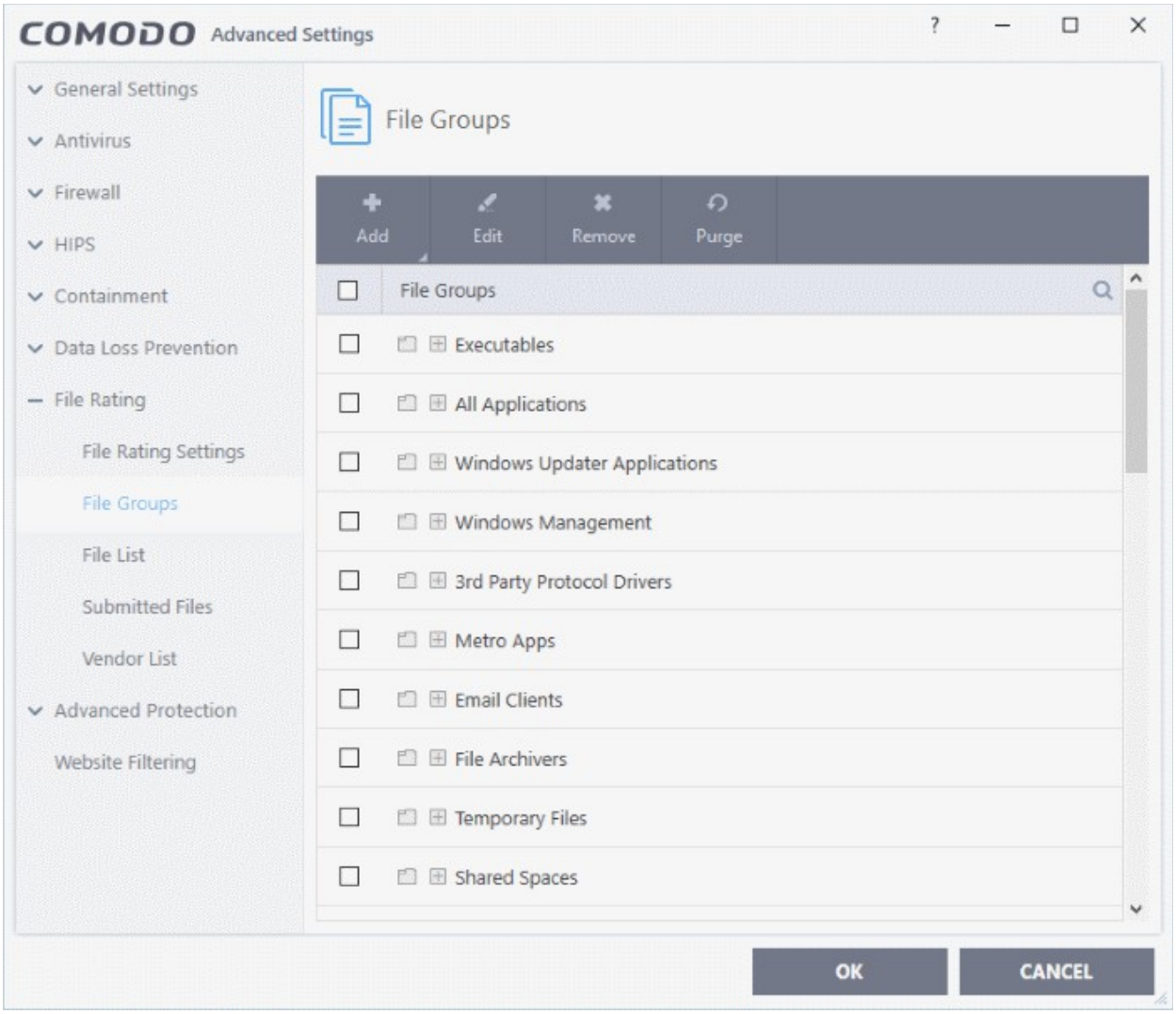
- Click 'OK' to save your changes
- Click 'OK' in the 'Advanced Settings' screen for your settings to take effect.

7.8.2. File Groups

- Click 'Settings' > 'File Rating' > 'File Groups'
- As the name suggests, a file group is a collection of one or more file types. For example, the 'Executables' group is a list of file types that can run code on your computer.
- Once created, file groups can be named as the target of a rule in other areas of CCS. This makes it easy to add an entire class of files to exclusions, HIPS rules, firewall rules, containment rules and more.
- CCS ships with a set of predefined file groups. You can also create your own groups and edit existing groups as required.

Open the 'File Groups' interface

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



Search Option:

- Click the search icon at upper-right and enter the name of a file group in full or part.

Controls:

The buttons at the top provide the following options:

- **Add** - Create a new file group. Add files, folders or running processes to an existing group.
- **Edit** - Rename a group. Change the file path of items in a file group.
- **Remove** - Delete a file group, or specific items in a group.
- **Purge** - Runs a check to verify that all files in a group are actually installed at the path specified. If not, the file or file group is removed from the list.

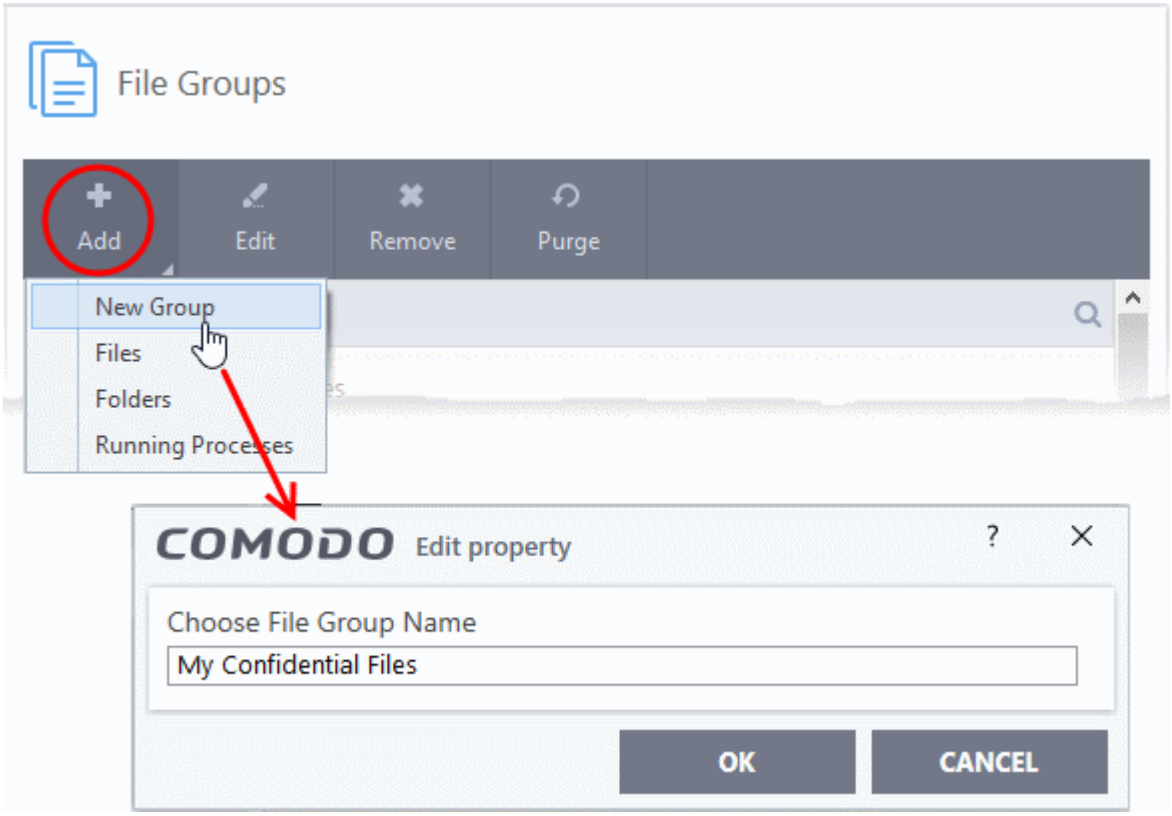
See the following links if you need more help:

- **Create a new File Group**
- **Edit the 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**

Create a File Group

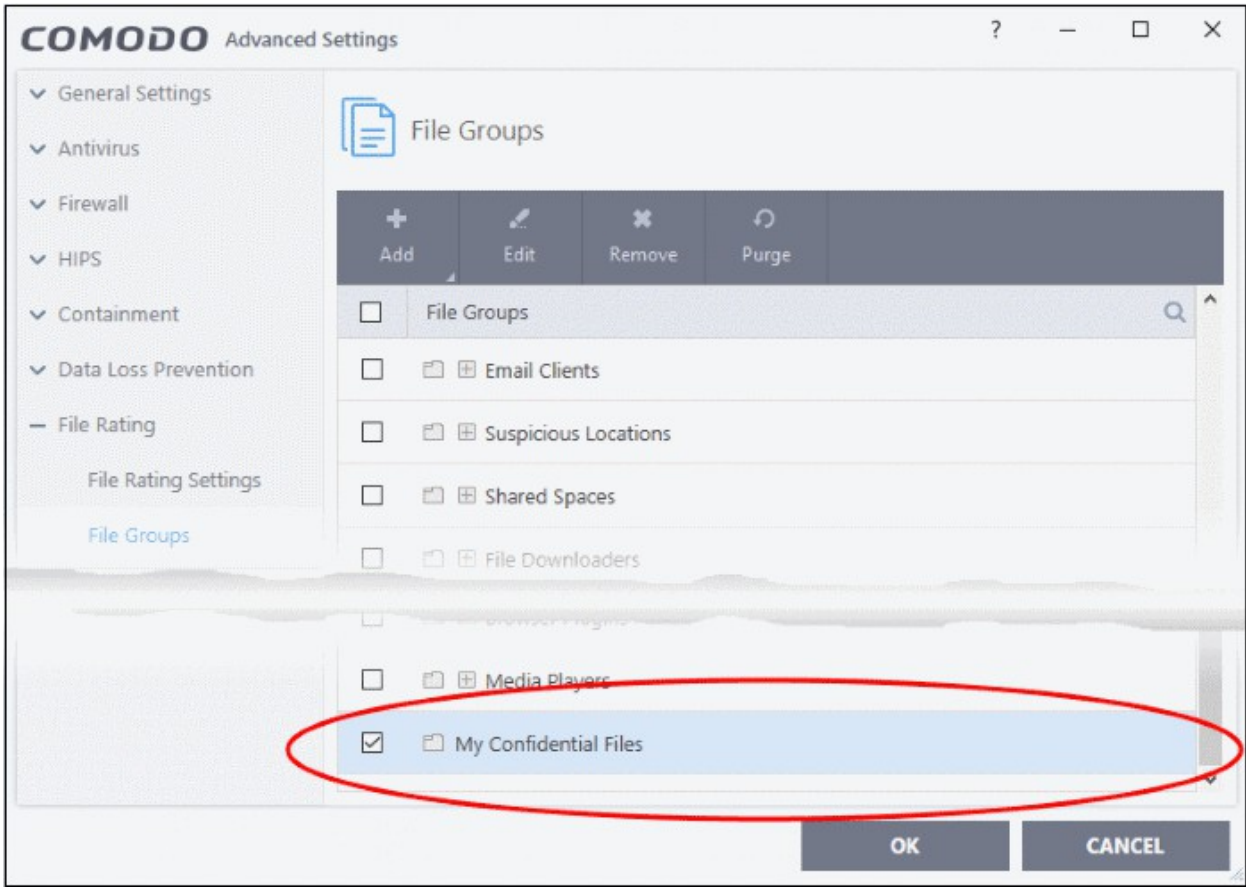
- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File Groups'

- Click the 'Add' button and select 'New Group':



- Create a label for the file group and click 'OK'.

The new group will be added and shown in the list:

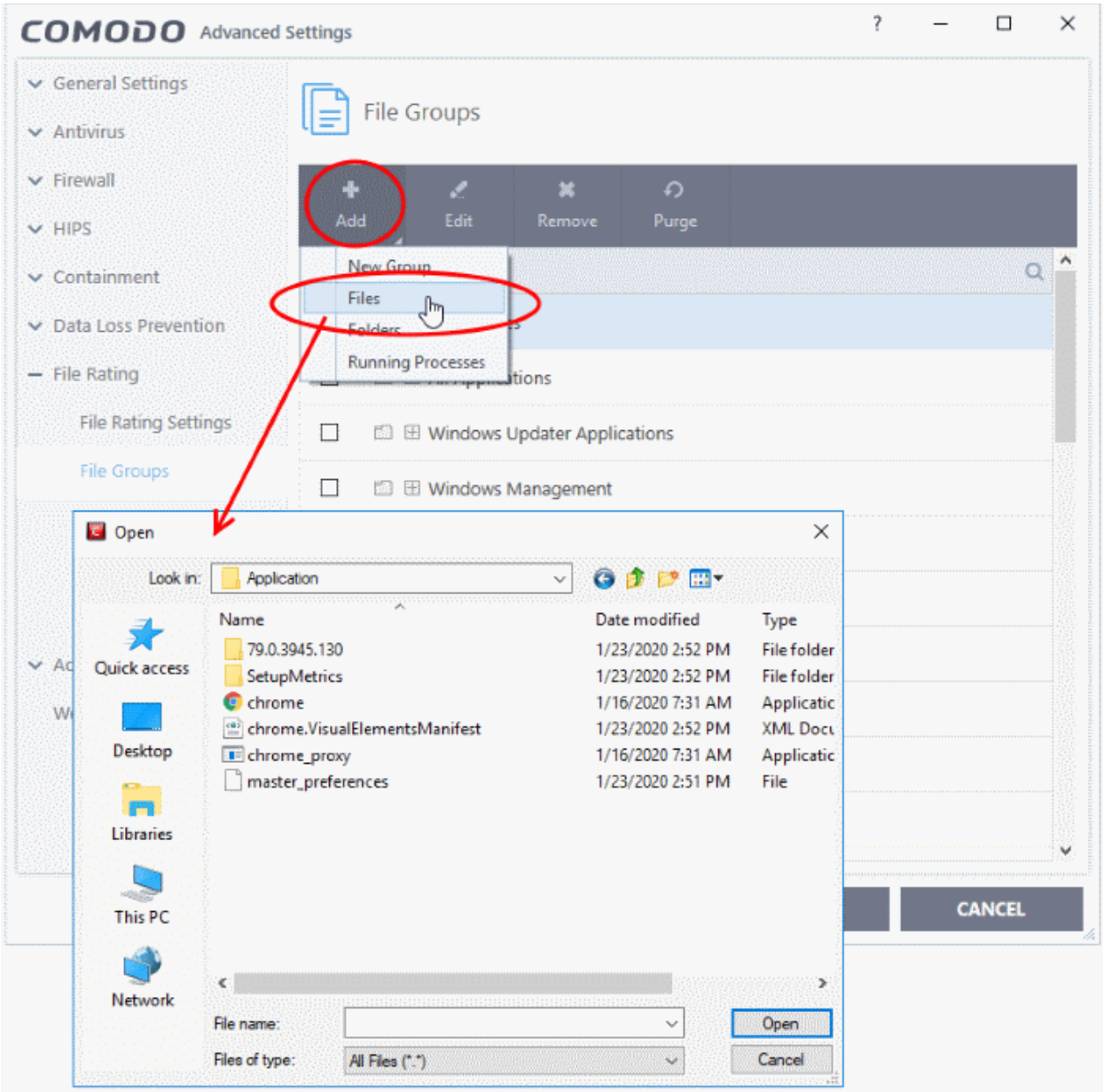


Add files or folder to a group

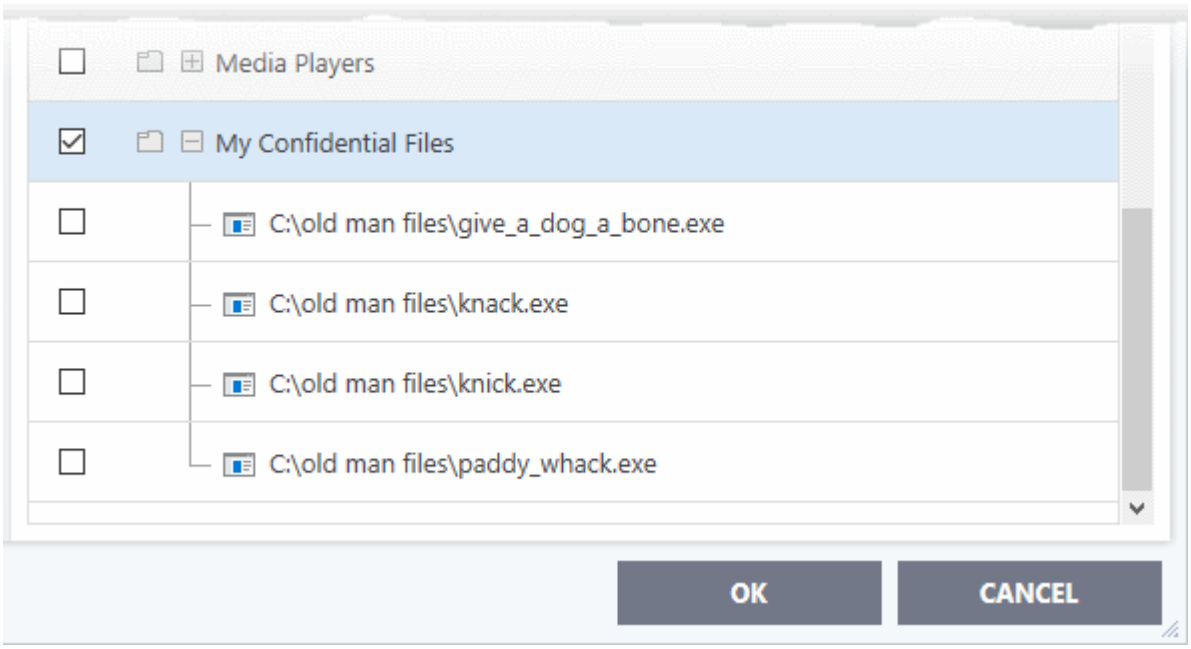
- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File Groups'
- Select the group from the list
- Click the 'Add' button > Choose from 'Files', 'Folders' or 'Running Processes'

  Add individual files or folders

  - Choose 'Files' or 'Folders' from the 'Add' drop-down menu.



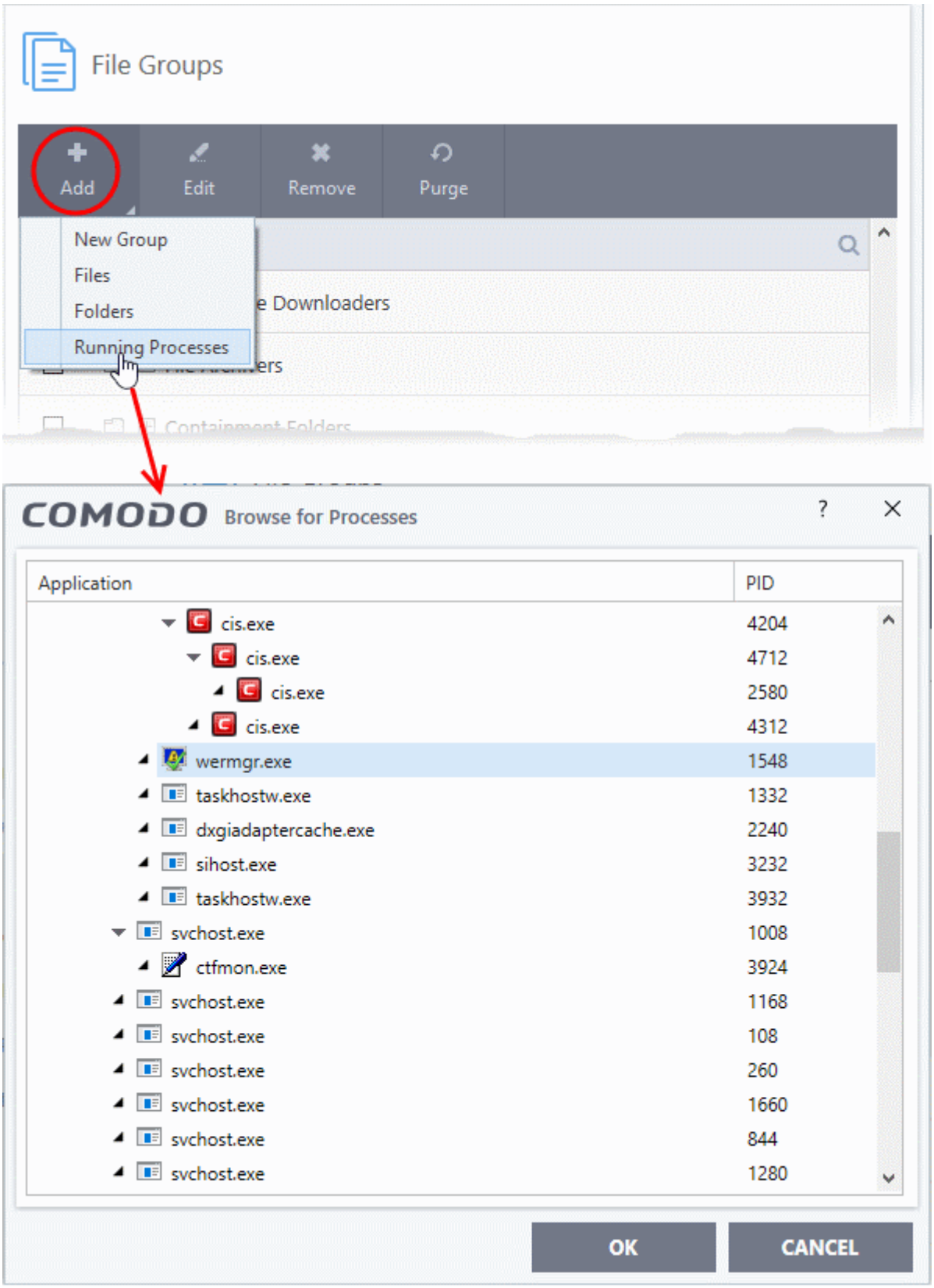
- Navigate to the file or folder you want to add to the group. Click 'OK'



- Repeat the process to add more files or folders.

Add an application from a running process

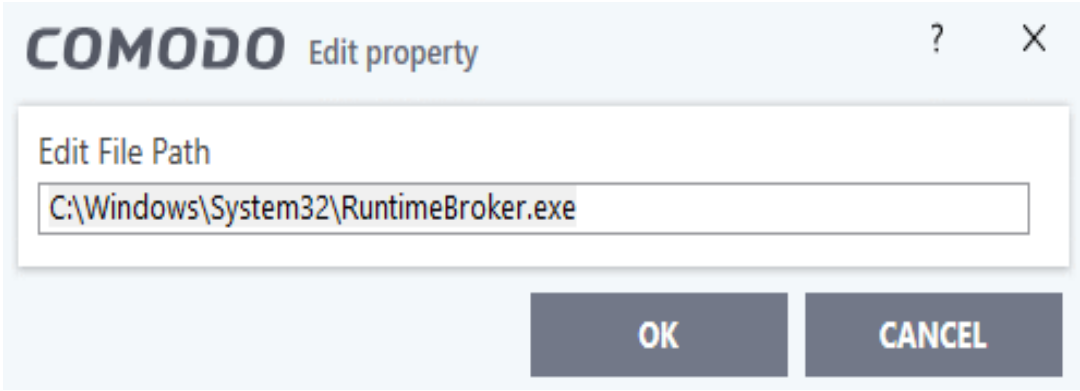
- Click the 'Add' button then 'Running Processes'
- This opens a list of processes currently running on your computer:



- Select the desired process. The parent application of the process will be added to the group.
- Click 'OK'.

Edit an item in the 'Files Groups' list

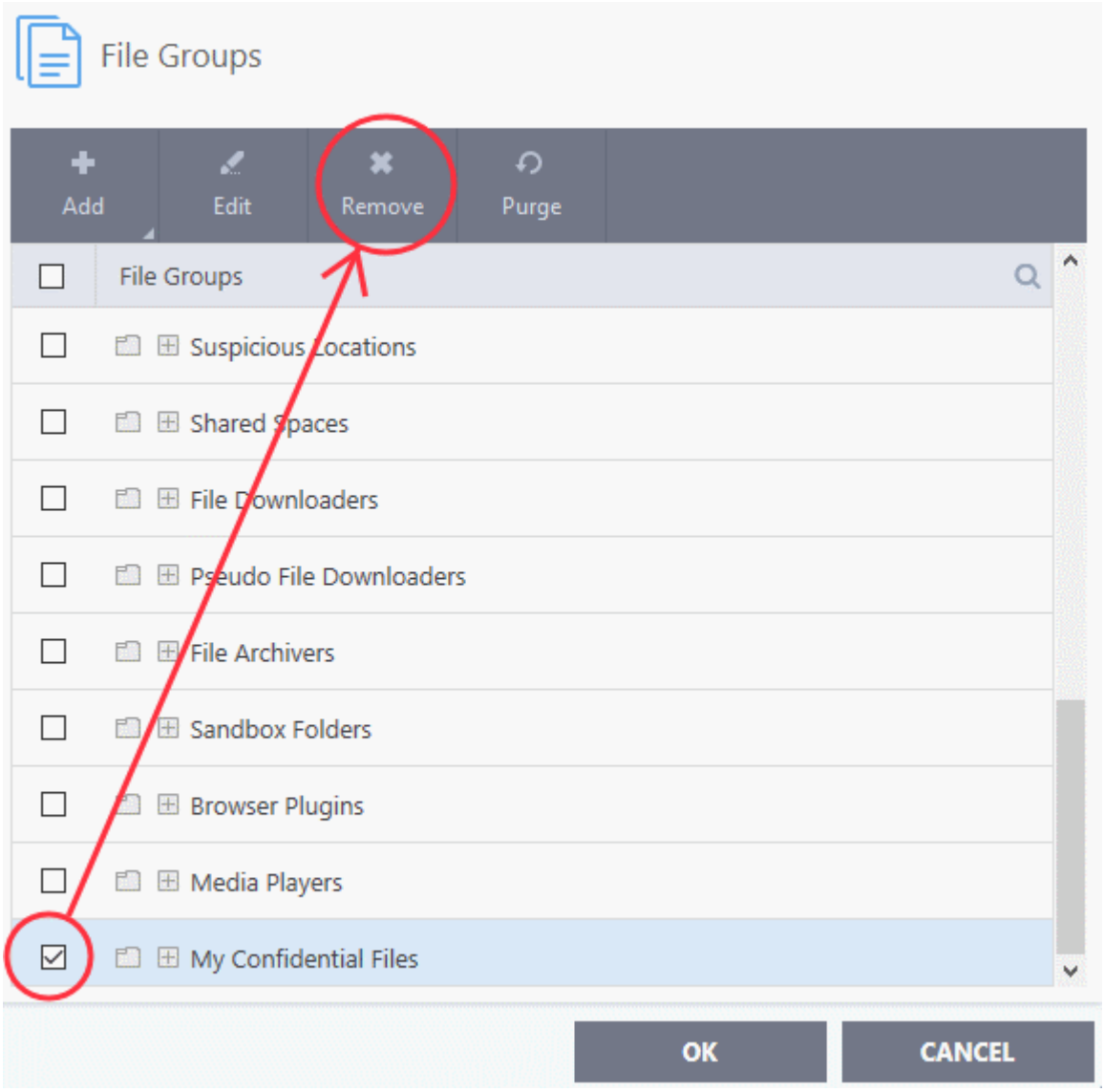
- Select the item from the list and click the 'Edit' button. The 'Edit property' dialog is shown:



- Edit the file path if required and click 'OK'.

Delete a file group, or an individual file from a group

- To remove a file group, select it from the list and click the 'Remove' button.



- To remove an individual file from a group - expand the group by clicking '+' at the left of the group, select the file to be removed and click the 'Remove' button.
- Alternatively, right-click on a file and choose remove from drop-down menu.

7.8.3. File List

- Click 'Settings' > 'File Rating' > 'File List'

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

CCS rates files as:

- **Trusted** - the file is safe to run outside the container.
- **Unrecognized** - no trust-rating was found for the file, so it will be run in the container.
- **Malicious** - the file is known malware and will be quarantined or deleted.

Trusted Files

Files can be awarded a 'Trusted' status in the following ways:

- **Cloud-based file lookup service (FLS)** - When a file is first opened, CCS will check the file's reputation on our global whitelist and blacklists. It will award trusted status if the file is on the global whitelist of safe files.
- **Vendor rating** - The application is from a software publisher who has a 'Trusted' status in the **Vendor List**.
- **Administrator rating** - Admins can elect to trust files on a local endpoints and networks. Only applies if your CCS installation is remotely managed by an administrator.
- **User Rating** - You can manually assign a trusted rating to a file as follows:
  - Click 'Settings' > 'File Rating' > 'File List'
  - Select the target file then click the 'File Details' button
  - Click the 'File Rating' tab
  - Click the 'Rate Now' link
  - Set the rating as 'Trusted'
  - Click 'OK'
  - See **change the file rating** in **File Details** if you want more help on this.

Unrecognized Files

- Once installed, HIPS monitors and verifies all file activity on your computer.
- Every new executable file is first scanned against the virus blacklist (known 'bad' files) and the file whitelist (known 'good' files).
- If the file is on neither list it is given an 'Unrecognized' file rating.
- Any executable that is modified is also given 'Unrecognized' status. This protects you against malware changing the behavior of a previously trusted application.

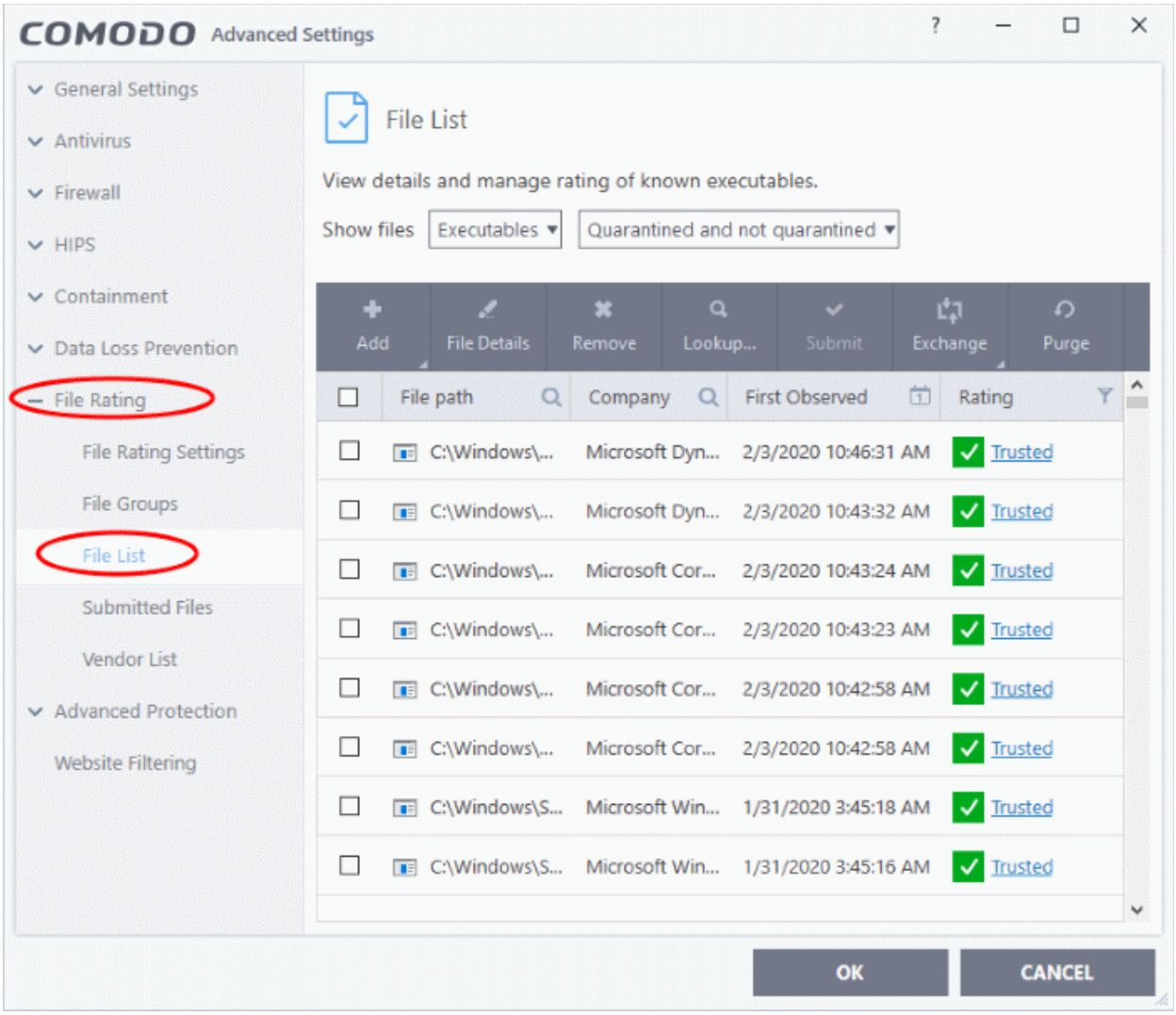
You can review pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be given a 'Trusted' rating. See '**Change the file rating**' for more details. You can also submit files to Comodo for analysis. Experts at Comodo will test the files and add them to global white-list or black-list accordingly.

Malicious Files

Files identified as malware are given a 'Malicious' rating, and are blocked and quarantined.

Open the 'File List' interface

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



The file list shows applications and executable files discovered on your computer.

- **File Path** - The location of the file on your computer
- **Company** - The software vendor that published/created the file
- **First Observed** - Date and time at which the file was first discovered by CCS.
- **File Rating** - Current trust rating of the file. The possible values are:
  - **Trusted**
  - **Unrecognized**
  - **Malicious**

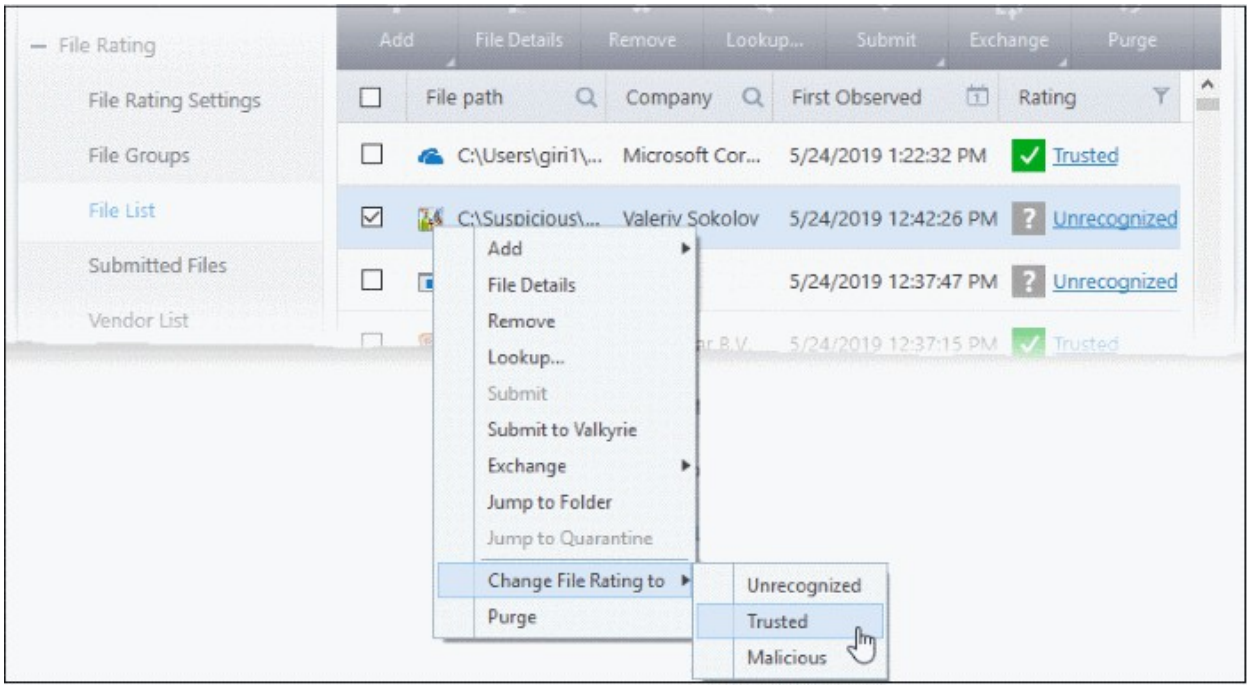
CCS obeys ratings in the following order of priority:

1. Administrator rating - Rating set by the Endpoint Manager admin who remotely manages your CCS installation.
2. User rating - A rating that you, or another user, gave to the file in the local CCS installation.
3. FLS rating - The rating of the file on Comodo's master database. CCS automatically fetches this rating from the file-lookup server (FLS) when it scans a file.

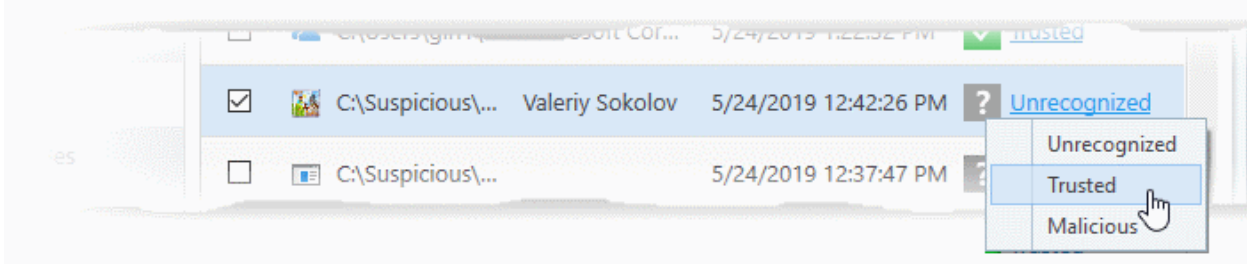
There are three ways you can set user rating for a file:

1. Right-click on a file in the file list
- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'

- Right-click on a file > Select 'Change File Rating to' > Choose a new rating:



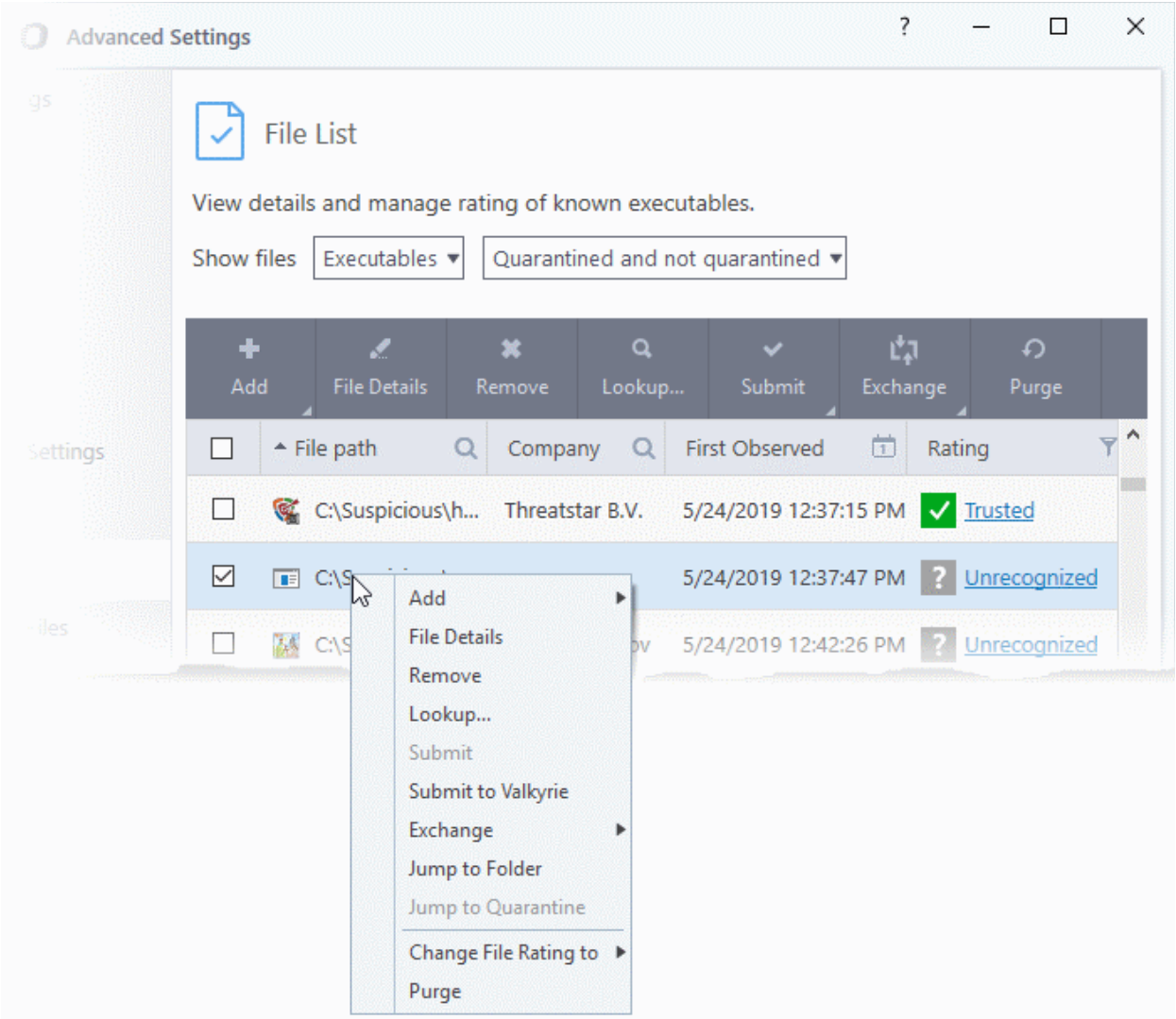
2. In the file rating column
- Click on the rating of a file in the 'Rating' column
- Choose a new rating from the options:



3. From the 'File Details' dialog
- Select a file in the file list
- Click the 'File Details' button at the top
- Click the 'File Rating' tab
- Click the 'Rate Now' link
- Set the rating as required
- Click 'OK'

Context Sensitive Menu

- Right-click on a file to open a context sensitive menu that allows you to view the 'File Details' dialog, remove the file from the list, submit the file to Comodo for analysis and more.



- **Add** - Manually add a file to the list and specify its trust rating
- **File Details** - View information about the selected item. You can also set the file rating from here.
- **Remove** - Delete files from the list.
- **Lookup** - Check the file-lookup server for more details about the file, including the latest trust rating.
- **Submit to Valkyrie** - Upload an item to Valkyrie, Comodo's file analysis system.
- **Exchange - Consists of two options (Import and Export).**
  - **Import** - Add files to the list from an XML file
  - **Export** - Save the current list as an XML file
- **Jump to Folder** - Opens the folder containing the file in Windows Explorer.
- **Jump to Quarantine** - Opens the 'Quarantine' interface of CCS to view or restore the file. Available only for items moved to quarantine. See **Manage Quarantined Items** for more details.
- **Change File Rating to** - Set user defined trust rating to the file.
- **Purge** - Check that all files in the list are still installed at the path specified. If not, the file is removed from the list.

Sort, search and filter options

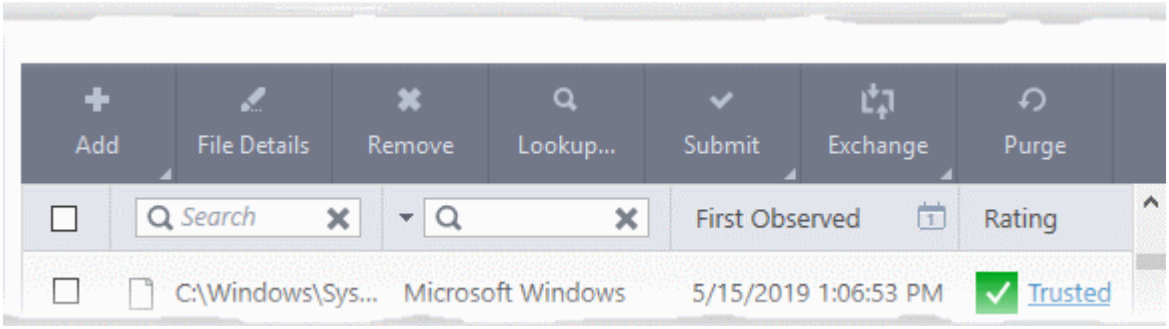
Sort option

- Click any column header to sort the items in alphabetical / ascending / descending order of entries in that column

Search options

You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and 'File rating'.

- Click the search icon at the far right in the 'File path' and/or 'Company' column header.



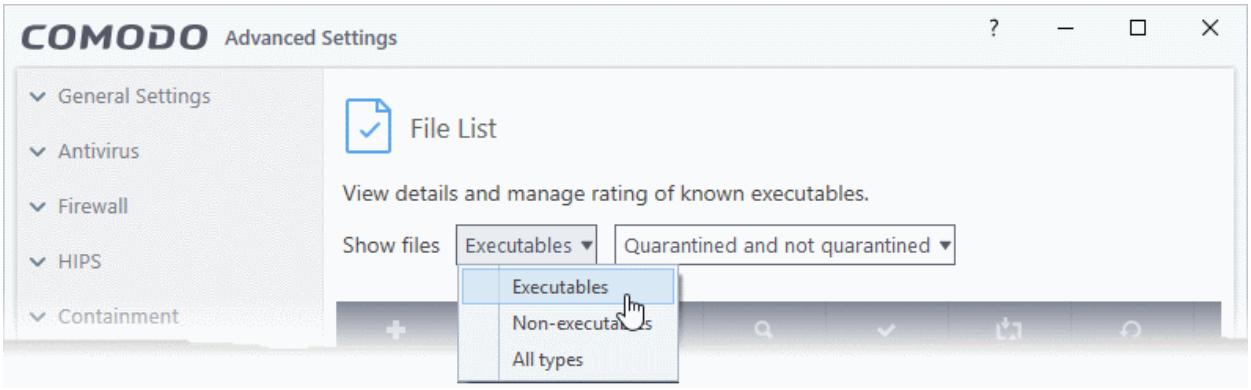
- Enter the file path and/or the name of company in part or full as per the selected criteria in the search field

The result for the entered criteria will be listed automatically. Click the 'X' icon to clear the search criteria and display all the items again in the list.

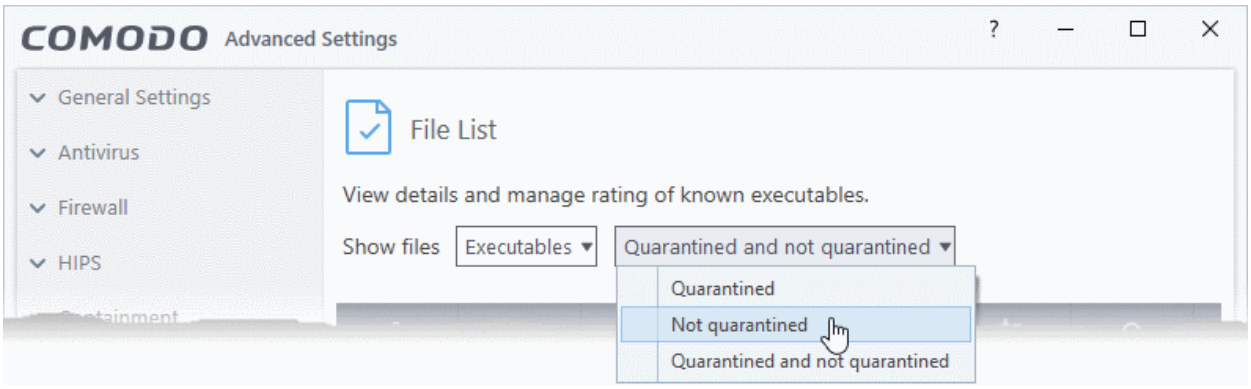
Filter options

The 'Show files' filter lets you view the following file types:

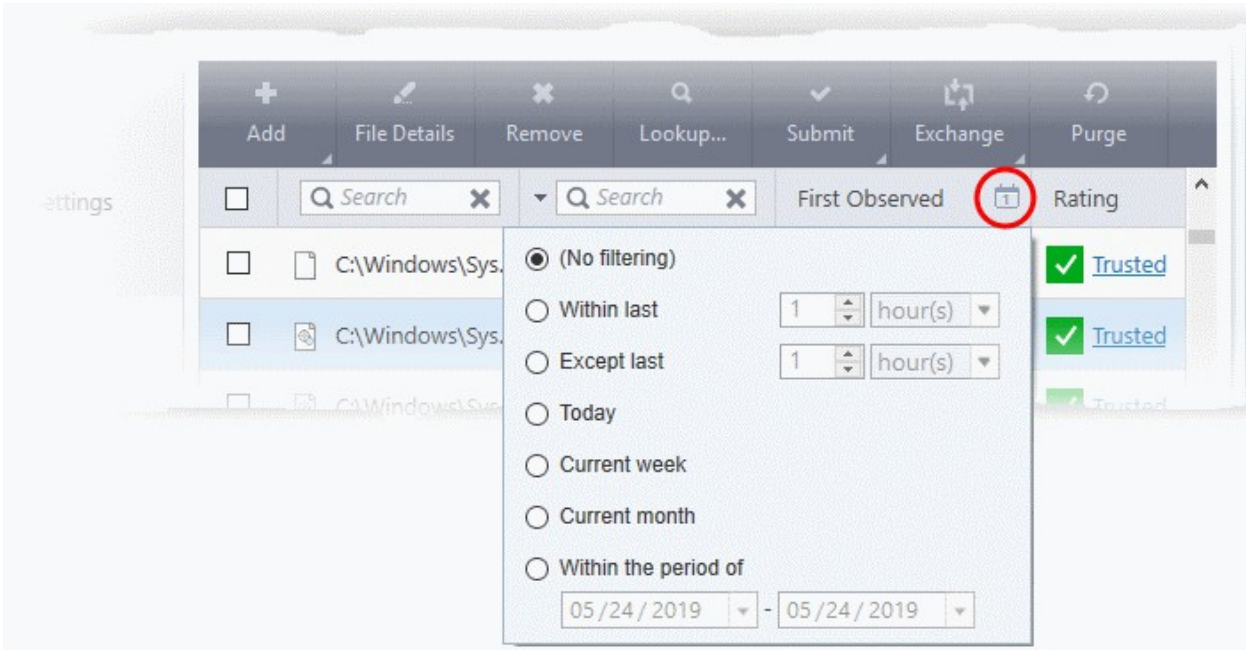
- **Executables** - Files capable of running code. Example extensions include .exe, .msi, .com, .bin, .vbs, etc. These files are usually applications, scripts or installers.
- **Non-executables** - Files that were created by executables, but which are not capable of running code themselves. Note - User-created files, like Word documents, saved emails and spreadsheets etc, are not shown with this option.
- **All types** - Show both executable and non-executable files.



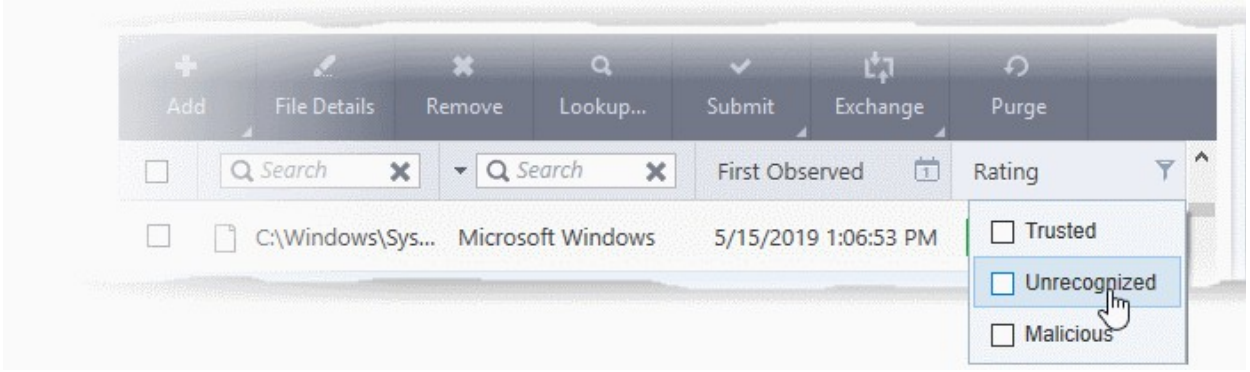
- Select the file type from the drop-down on the left
- Select whether you want to view quarantined items, non-quarantined items, or both:



- Click the calendar icon at the right of the 'First Observed' column
- Choose the time period you require
- This will show only those files discovered in the time-frame you set:

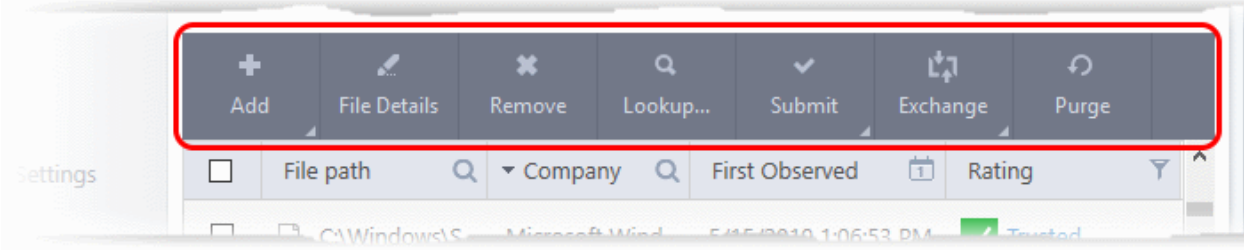


- Click the funnel icon at the right of the 'File Rating' column to filter files by rating:



Control Buttons

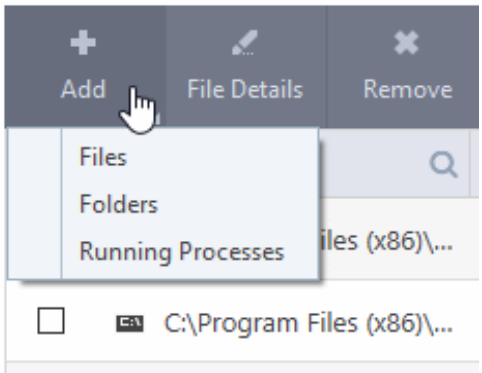
The buttons at the top provide the following options:



- **Add** - Manually add files to the 'File List' with user defined rating
- **File Details** - View the information about the selected item. You can also set user defined rating to the selected file
- **Remove** - Delete files from 'File List'.
- **Lookup...** - Check the details of the selected file from the master Comodo safelist
- **Submit to Valkyrie** - Uploads selected files to Valkyrie for behavior analysis. Valkyrie is Comodo's file testing and verdicting system.
- **Exchange** - Consists of two options (**Import** and **Export**).
  - **Import** - Fetch the files from a file list saved as an XML file
  - **Export** - Save the current file list with existing ratings as an XML file
- **Purge** - Runs a system check to verify that all the files for which the ratings are listed are actually installed on the host machine at the path specified. If not, the fie is removed from the list.

Manually add files to 'File list'

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Add' button at the top



Tip: Alternatively, right click inside the File List page and choose 'Add' from the context sensitive menu.

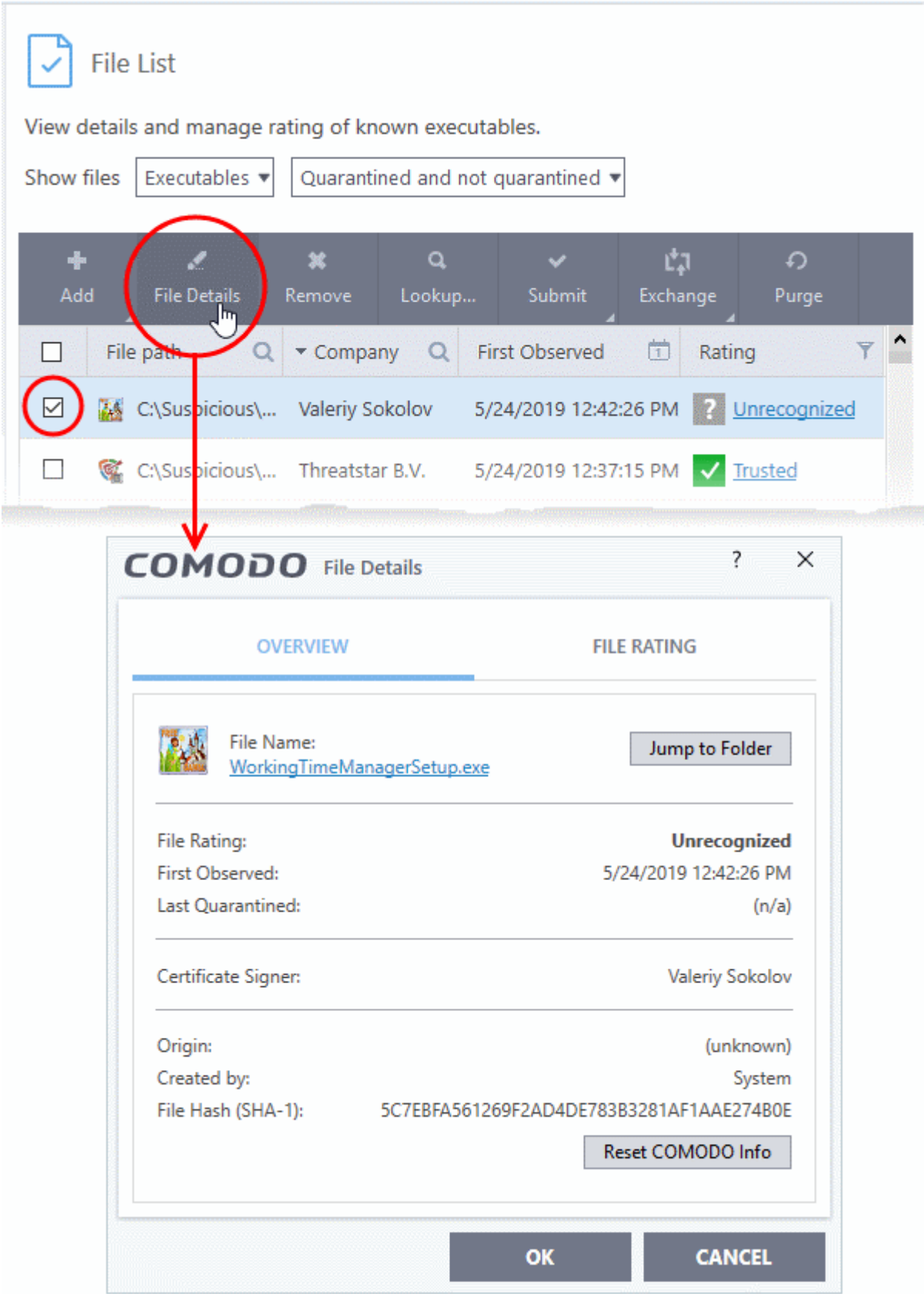
You can add three types of items:

- **Files** - Browse to the file you want to add and assign a rating.
- **Folders** - Browse to the folder you want to add an assign a rating. All files in the folder will inherit the rating you gave to the folder.
- **Running Processes** - Select a currently active process and assign a rating. The parent application of the process will be added to the file list with the rating you assign.

View the 'File Details' and change the rating

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

- Select a file and click the 'File Details' button.



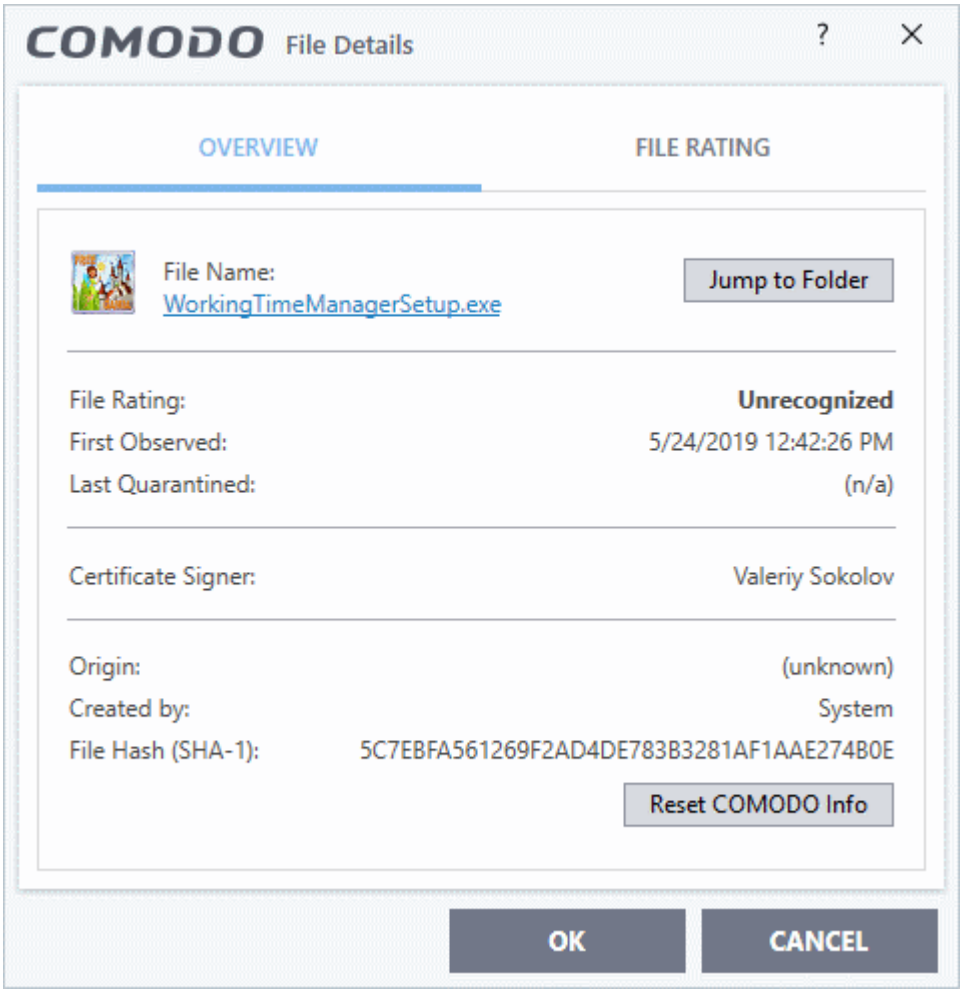
Tip: Alternatively, right click on the selected file and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog has two tabs:

- Overview
- File Rating

Overview

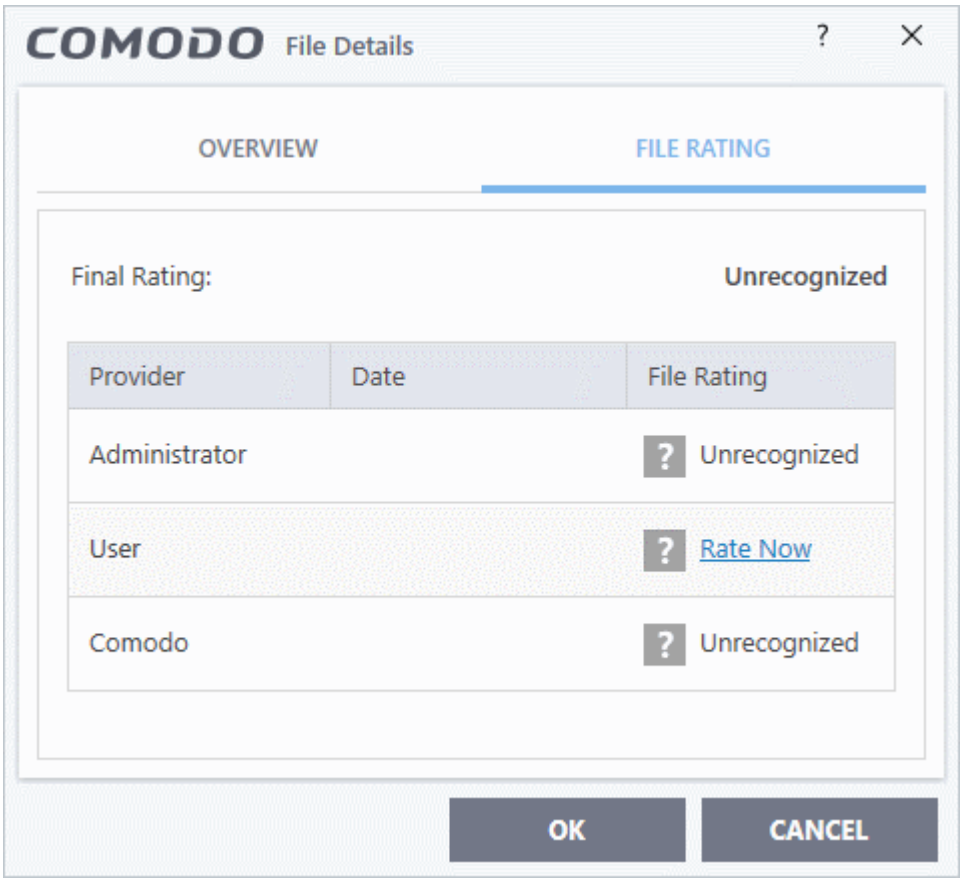
The 'Overview' tab shows general details such as the file rating, discovery date, hash value and publisher (signer):



- Click the file name to open the Windows 'File Properties' dialog.
- Click 'Jump to folder' to open the folder containing the file in Windows Explorer, with the respective file selected.
- Click 'Reset COMODO Info' to refresh the information from Comodo FLS database

File Rating

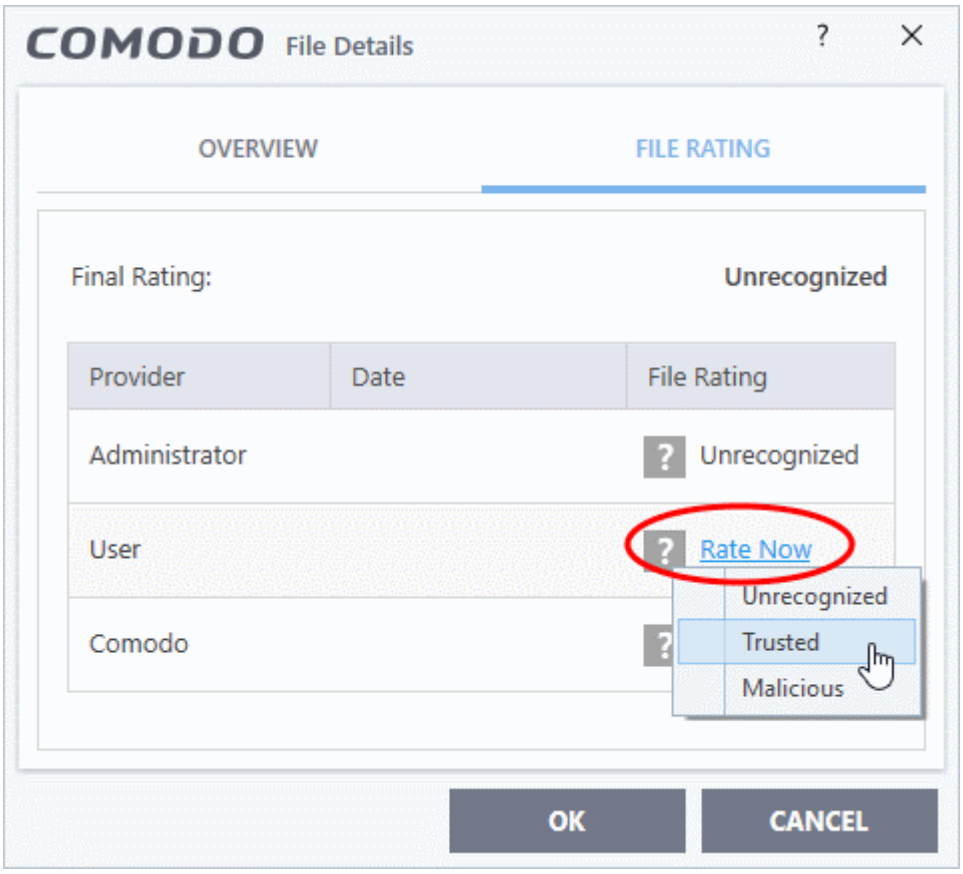
- Shows the file's current trust rating from Comodo and lets you set your own rating:



Note: If your CCS installation is remotely managed by Endpoint Manager, your administrator's file rating for individual file will override your user file rating.

Change the user rating of the file

- Select the file from the 'File List' pane and click the 'File Details' button
- Click the 'File Rating' tab
- Click the 'Rate Now' link and choose the rating from the drop-down:



The options available are:

- **Trusted** - The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- **Unrecognized** - The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- **Malicious** - The file will be deleted or placed in quarantine and will not be allowed to run.

- Click 'OK' in the 'Files Details' dialog

Tip: Alternatively, right click on a file then choose 'Change File Rating to'

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

Remove files from the file list

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be removed
- Click the 'Remove' button at the top. The file(s) is / are only removed from the list and not deleted from your system.

Tip: Alternatively, right click on a file then choose 'Remove' from context sensitive menu.

- Click 'OK' for your changes to take effect.

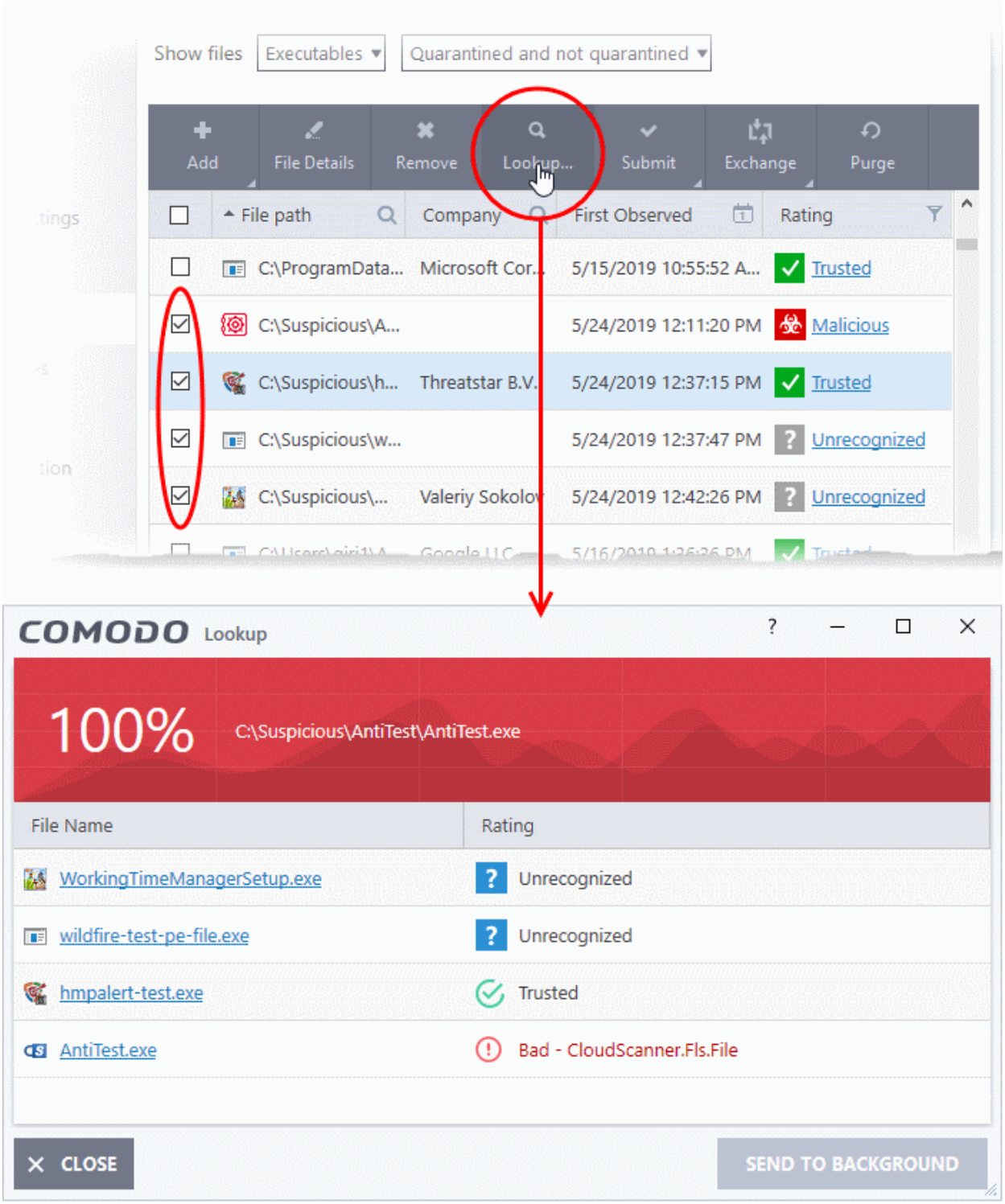
Perform an online lookup for files

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be checked from the 'File list' pane.

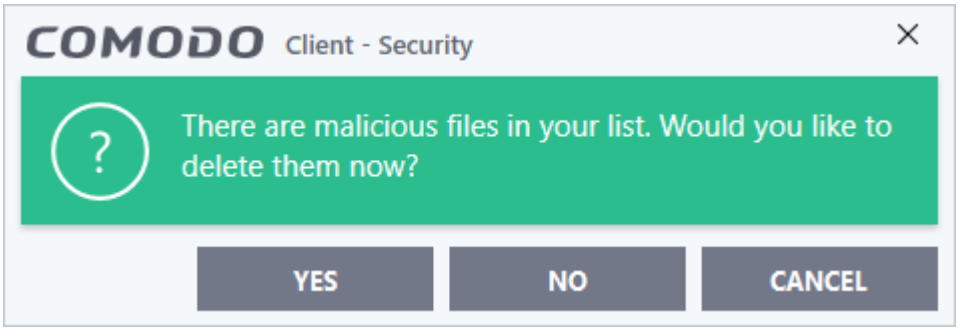
- Click the 'Lookup...' button at the top from the 'File list' pane.

Tip: Alternatively, right click on a file then choose 'Lookup' from the context sensitive menu.

Comodo servers will be contacted immediately to conduct a search of Comodo's master safe list database to check if any information is available about the files in question and the results will be displayed.



If any malicious or unwanted file(s) is/are found, you will be given an option to delete the file from your computer on closing the dialog.



- Click 'Yes' to permanently delete the malicious file(s) from your computer.

- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. See the description of **changing the file rating** under the section **File Details** for more details.
- If no information is available, it will be indicated as 'Needs to be submitted' with a yellow icon. You can submit the file to Comodo for analysis from the dialog that appears on closing the 'Lookup' dialog. See **explanation below** for more details.

Manually submit files to Valkyrie

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

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Select the file(s) to be submitted from the 'File List' pane.
- Click 'Submit' > 'Submit to Valkyrie' in the top-menu. The files will be immediately sent to Valkyrie for analysis.

Tip: Alternatively, right click on a file then choose 'Submit to Valkyrie' from the menu.

You can view the list of files you submitted so far, from the **Submitted Files** panel.

Export and Import the File List

You can save the list of files with their currently assigned ratings to an XML file and store it in a safe place. This is useful to restore your list if you have to uninstall/reinstall CCS, or if you want to implement the same list on another machine that has CCS installed.

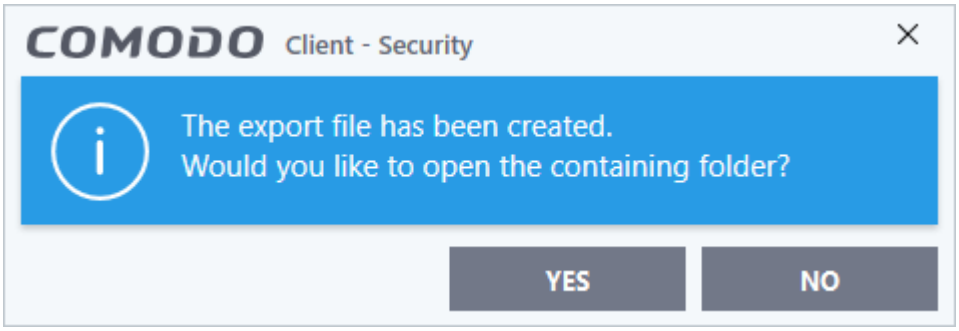
Export the File List

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Exchange' button at the top of the 'File List' pane then select 'Export' from the menu

Tip: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Export'

- Navigate to where you want to store the exported list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.



Import a saved file list

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'File List'
- Click the 'Exchange' button then select 'Import' from the menu

Tip: Alternatively, right click inside the 'File List' page then select 'Exchange' > 'Import'

- Navigate to the location of the XML file containing the file list and click 'Open'.

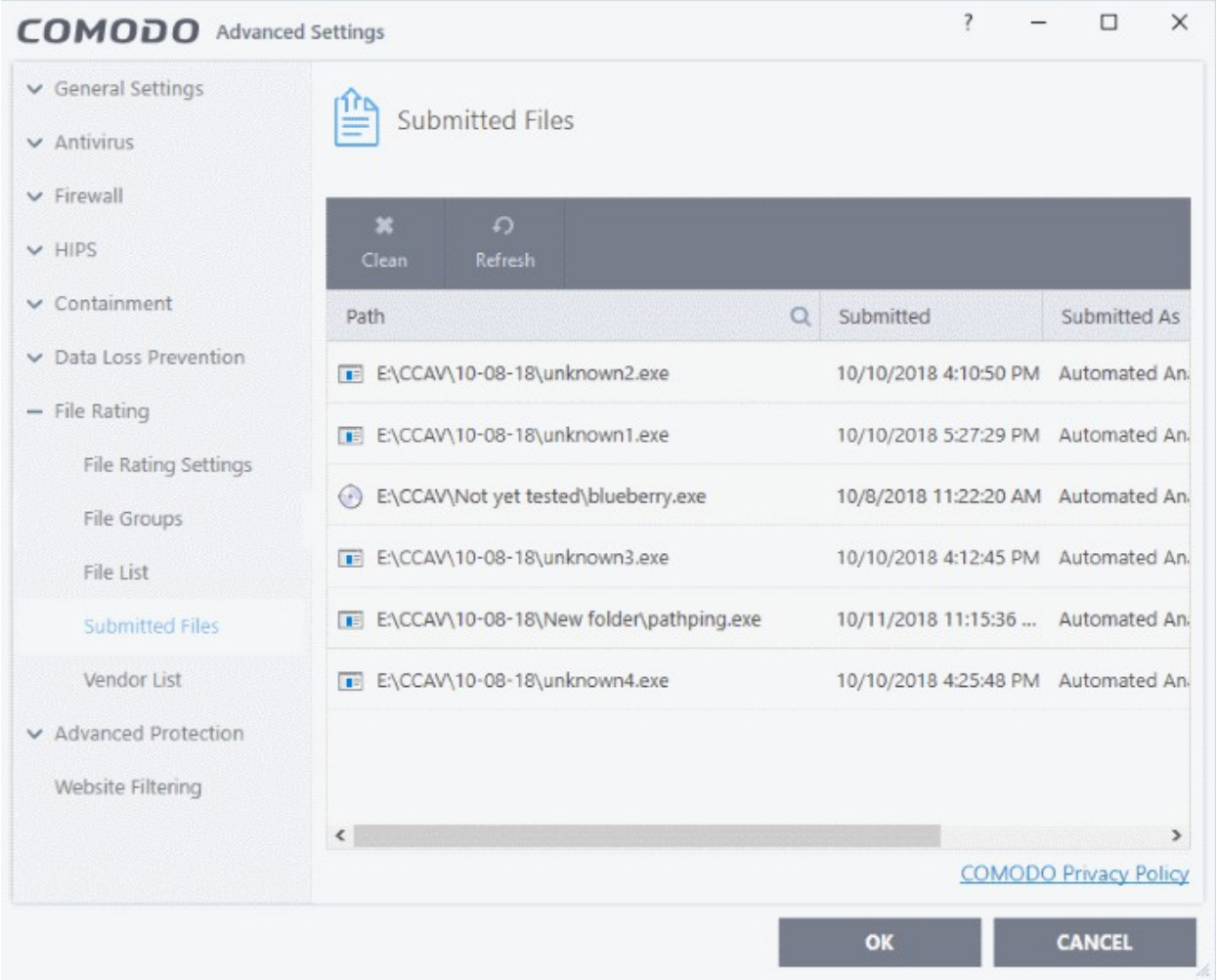
The 'File List' will be populated as per the imported 'File List'.

7.8.4. Submitted Files

- Click 'Settings' > 'File Rating' > 'Submitted Files'
- The 'Submitted Applications' area lets you review and manage the files that you have uploaded to Comodo Valkyrie for analysis.
- Valkyrie is Comodo's file testing and verdicting system.
- You can submit suspicious files, files with an 'unknown' trust rating, or false-positive files (those files you feel CCS has incorrectly identified as malware).
- After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.
- After manual classification by Valkyrie, they will be added to global white or black list accordingly.

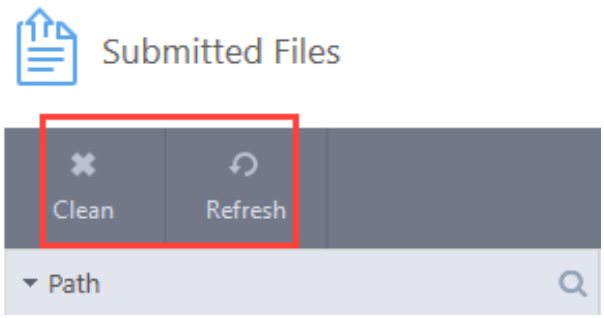
Open the 'Submitted Files' interface

- Click 'Settings' on the CCS home screen
- Click 'File Rating' > 'Submitted Files' on the left:



- **Path** - The location of the file on your computer
- **Submitted** - Date and time the file was uploaded for analysis.
- **Submitted As** - The status under which the file was uploaded. Examples include 'automated' and 'contained'.
- **Cloud Service** - The name of the Comodo cloud service to which the files were submitted. This is usually the Valkyrie analytic system operated by Comodo.

The buttons at the top provide the following options:



- **Clean** - Clears the list
- **Refresh** - Reloads the list to add items that are submitted recently

7.8.5. Vendor List

- Click 'Settings' > 'File Rating' > 'Vendor List'

There are three ways that a file can be treated as safe in CCS:

- The file is on the safe list (a global white-list of trusted software)
- The user has assigned 'Trusted' rating to the file in the CCS file list (**'Settings' > 'File Rating' > 'File List'**)
- The file is published and signed by a trusted vendor. The 'vendor' is the software company that created the file.

With regards to vendor settings, CCS handles ***unknown*** files as follows:

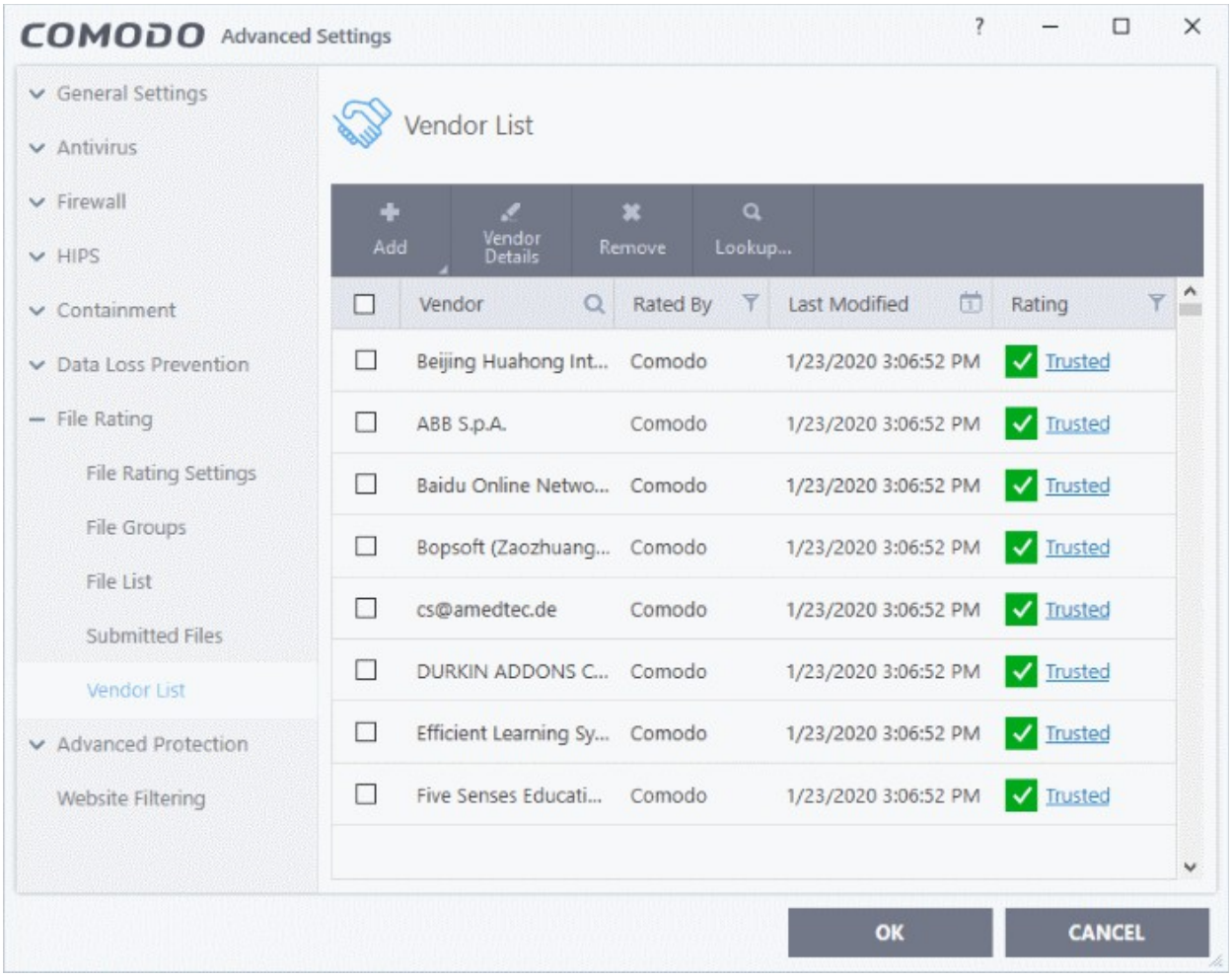
- The file is allowed to run normally if:
  - The vendor rating is 'Trusted' AND you have enabled 'Rate applications according to their vendor rating' in **File Rating Settings**
- The file is run in the container if:
  - The vendor rating is 'Unrecognized' AND you have enabled 'Rate applications according to their vendor rating' in **File Rating Settings**
  - The vendor is not in the vendor list (regardless of whether you have enabled 'Rate applications according to their vendor rating')
- The file is blocked and quarantined if:
  - The vendor rating is 'Malicious' AND you have enabled 'Rate applications according to their vendor rating' in **File Rating Settings**

Vendor List

- CCS ships with a list of trusted vendors who have a reputation of creating legitimate, safe software. CCS allows unknown files which are digitally signed by one of these vendors to run.
- Click 'Settings' > 'File Rating' > 'Vendor List' to view this list of trusted vendors.
- You can also add new vendors, and change the rating of existing vendors.
  The vendor rating priority is as follows:
  - Admin
  - User
  - Comodo
- Software publishers can get themselves added to trusted vendors by contacting Comodo with their software details. **Click here** to read more about this.
  - **Click here** if you want to read background information on digitally signing software

Open the 'Vendor List' interface

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List':



The interface allows you to:

- **Add a new vendor to the list**
- **View details of vendors and assign user rating**
- **Perform an online lookup for vendors**
- **Remove vendors from the list**

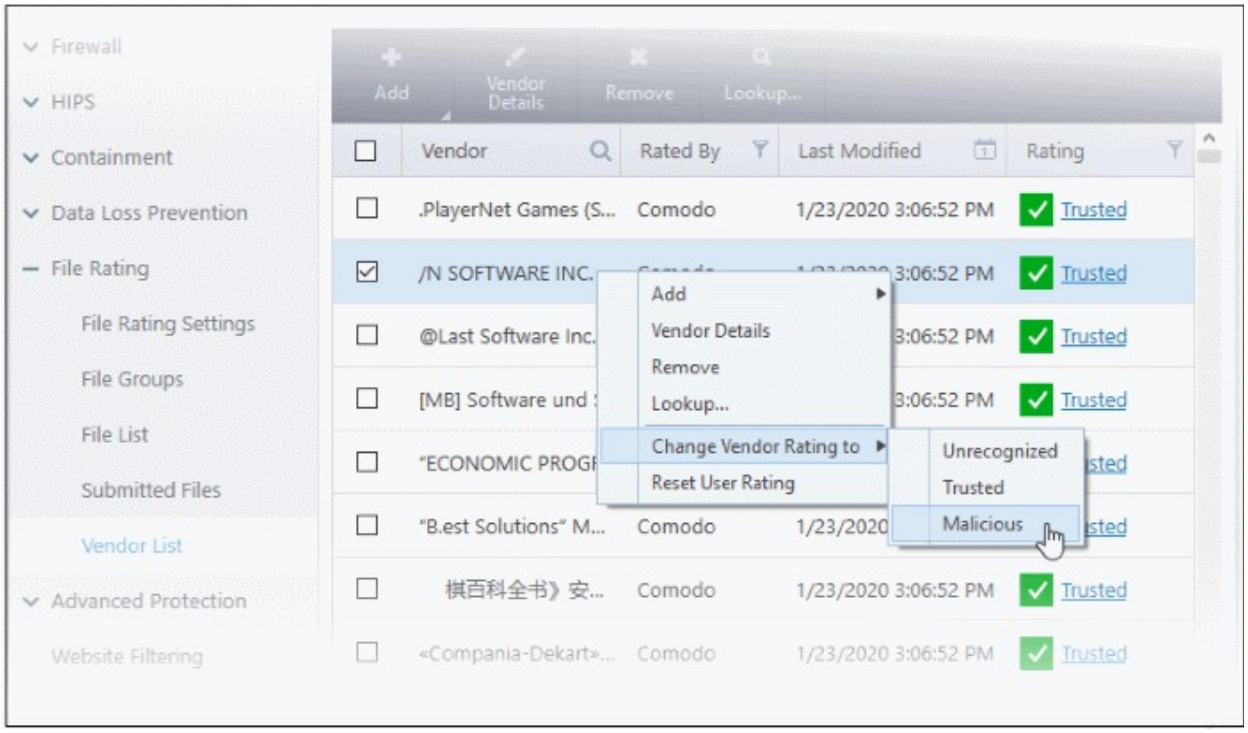
Column Descriptions:

- **Vendor** - The name of the software publisher
- **Rated By** - The entity that assigned the rating you see in the 'Rating' column. This can be 'Administrator', 'User' or 'Comodo' rating.
- **Last Modified** - Date and time the rating was most recently updated.
- **Rating** - Current trust rating of the vendor. The possible values are:
    - Trusted
    - Unrecognized
    - Malicious
    - Click on the rating to assign a new rating
    - CCS obeys vendor ratings with the following priority:
        - Admin rating
        - User rating
        - **Comodo rating**

There are three ways you can set a vendor rating:

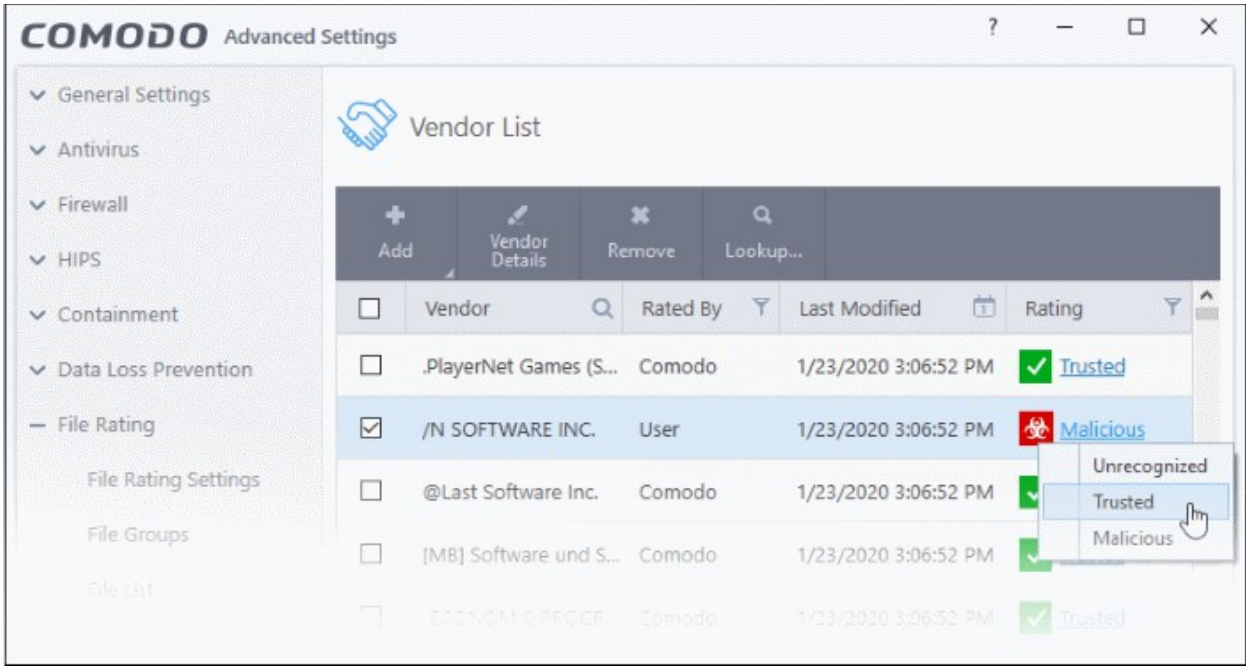
1. Right-click on a vendor in the 'Vendor List'

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Right-click on a vendor > Select 'Change File Rating to' > Choose a new rating:



2. In the file rating column

- Click on the rating of a vendor in the 'Rating' column
- Choose a new rating from the options:



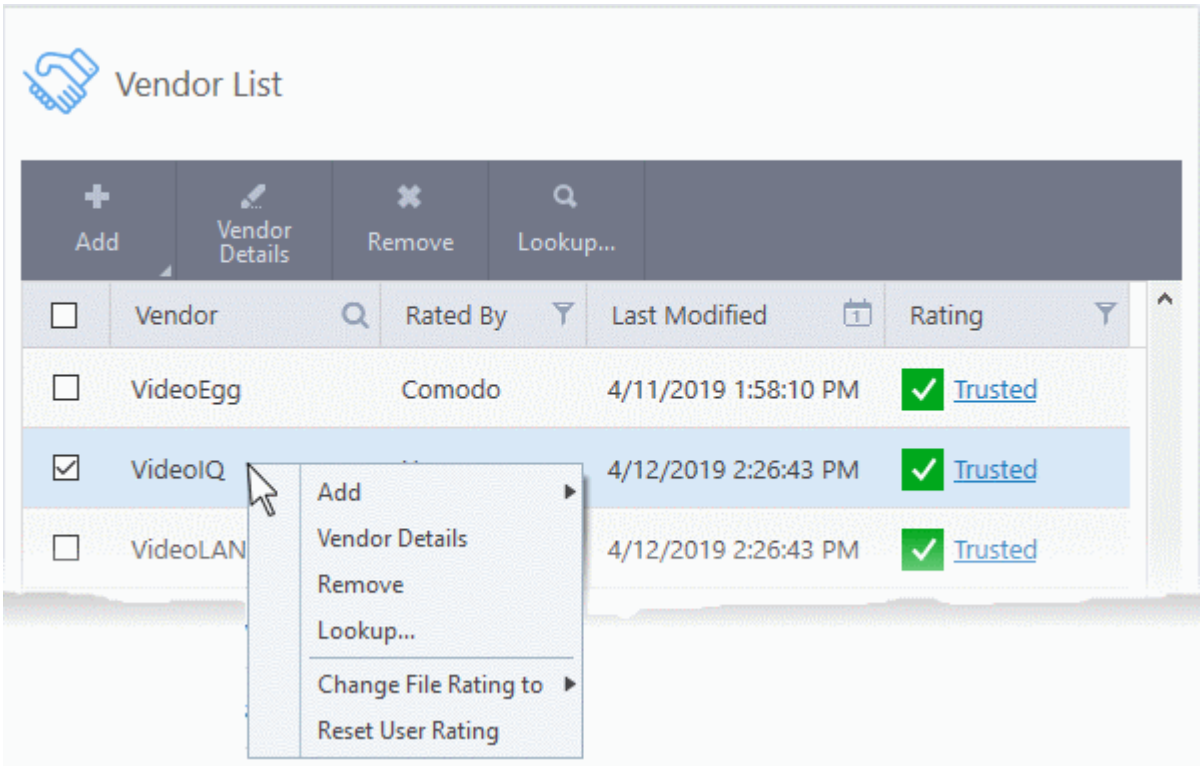
3. From the 'File Details' dialog

- Select a vendor in the file list

- Click the 'Vendor Details' button at the top
- Click the 'Vendor Rating' tab
- Click the 'Rate Now' link beside 'User'
- Set the rating as required
- Click 'OK'

Context Sensitive Menu

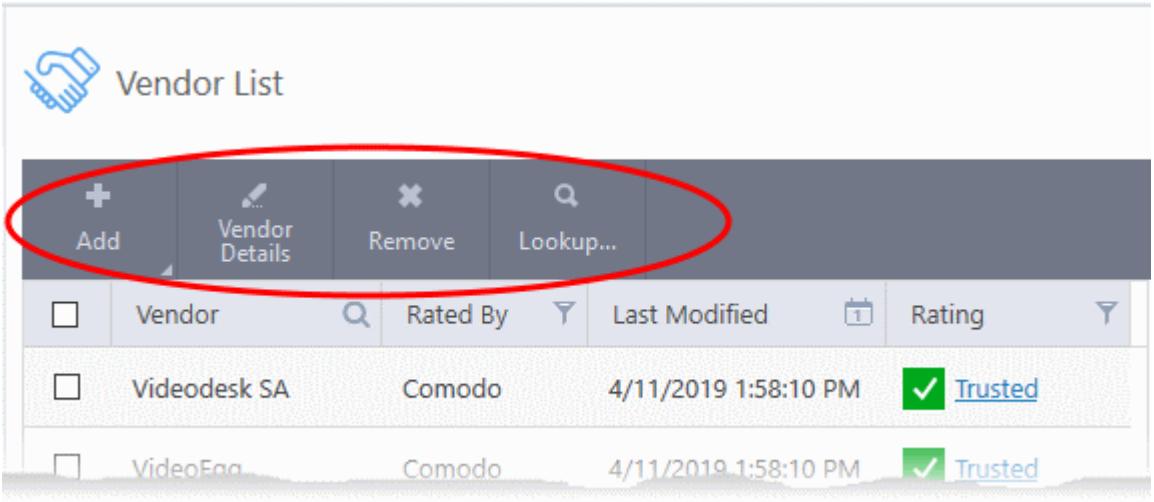
- Right-click on a vendor to open a context sensitive menu that allows you to view the 'Vendor Details' dialog, assign a rating to a vendor, add / remove vendors, and more.



- **Add** - Manually add a new vendor to the vendor list. You can select an executable file or a currently running process to add the publisher who signed that file to the list.
- **Vendor Details** - View the information about the vendor. You can also assign user defined trust rating to the vendor
- **Remove** - Delete the vendor from the list
- **Lookup...** - Check details of the vendor from the master Comodo trusted vendor list
- **Change File Rating to** - Set user defined trust rating to the vendor
- **Reset User Rating** - Clear user rating and reinstate Comodo rating

Controls

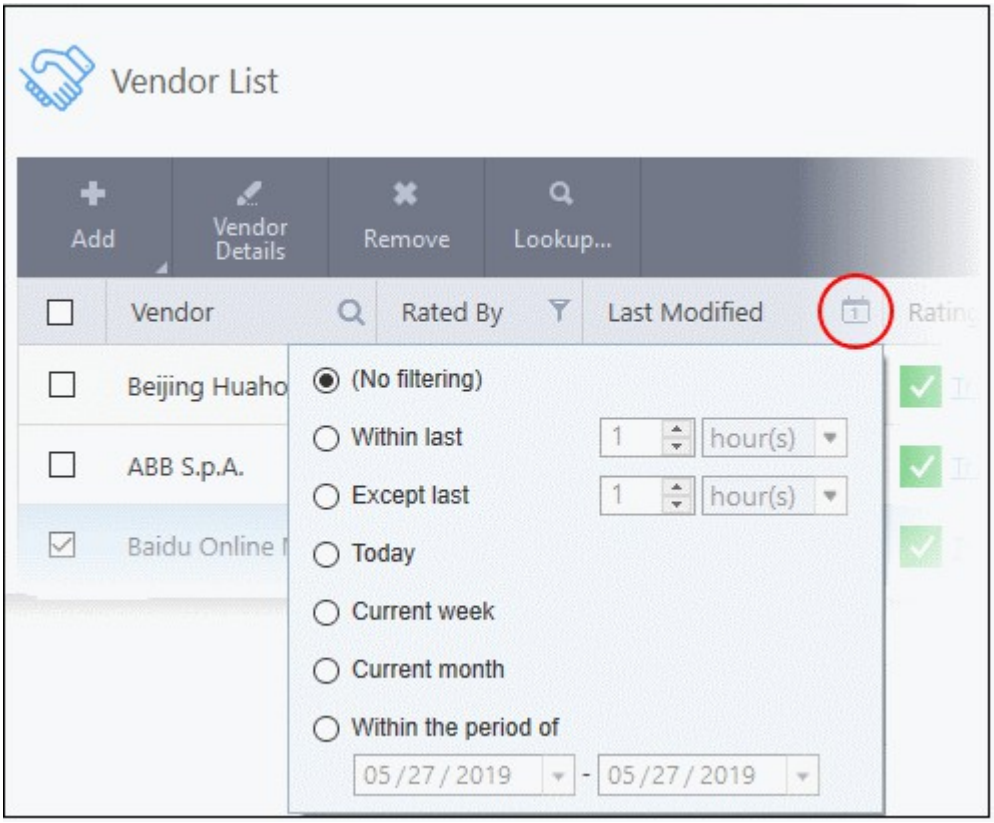
The buttons at the top provide the following options:



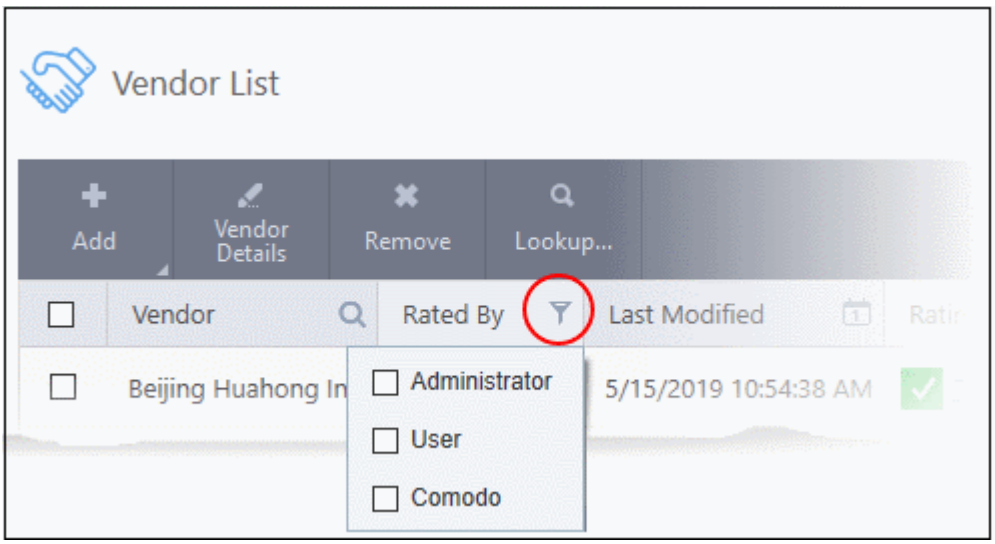
- **Add** - Manually add a new vendor to the list. You can add a vendor by simply selecting a file or a running process. CCS will extract the publisher who signed the file/process.
- **Vendor Details** - View information about the selected vendor. You can also set your own trust rating for the vendor from here.
- **Remove** - Delete selected vendors from the list. You can only remove user-added vendors.
- **Lookup...** - Check details of a vendor on Comodo's online trusted vendor list

Sort, Search and Filter options

- Click any column header to sort the list in order of the entries in that column
- Click the search icon in the 'Vendor' column header to look for specific vendors
- Click the calendar icon in the 'Last Modified' column header to filter vendors by date modified:



- Click the funnel icon in the 'Rated By' / 'Rating' columns to filter vendors by trust rating, and by who assigned the rating:



Add a new vendor to the list

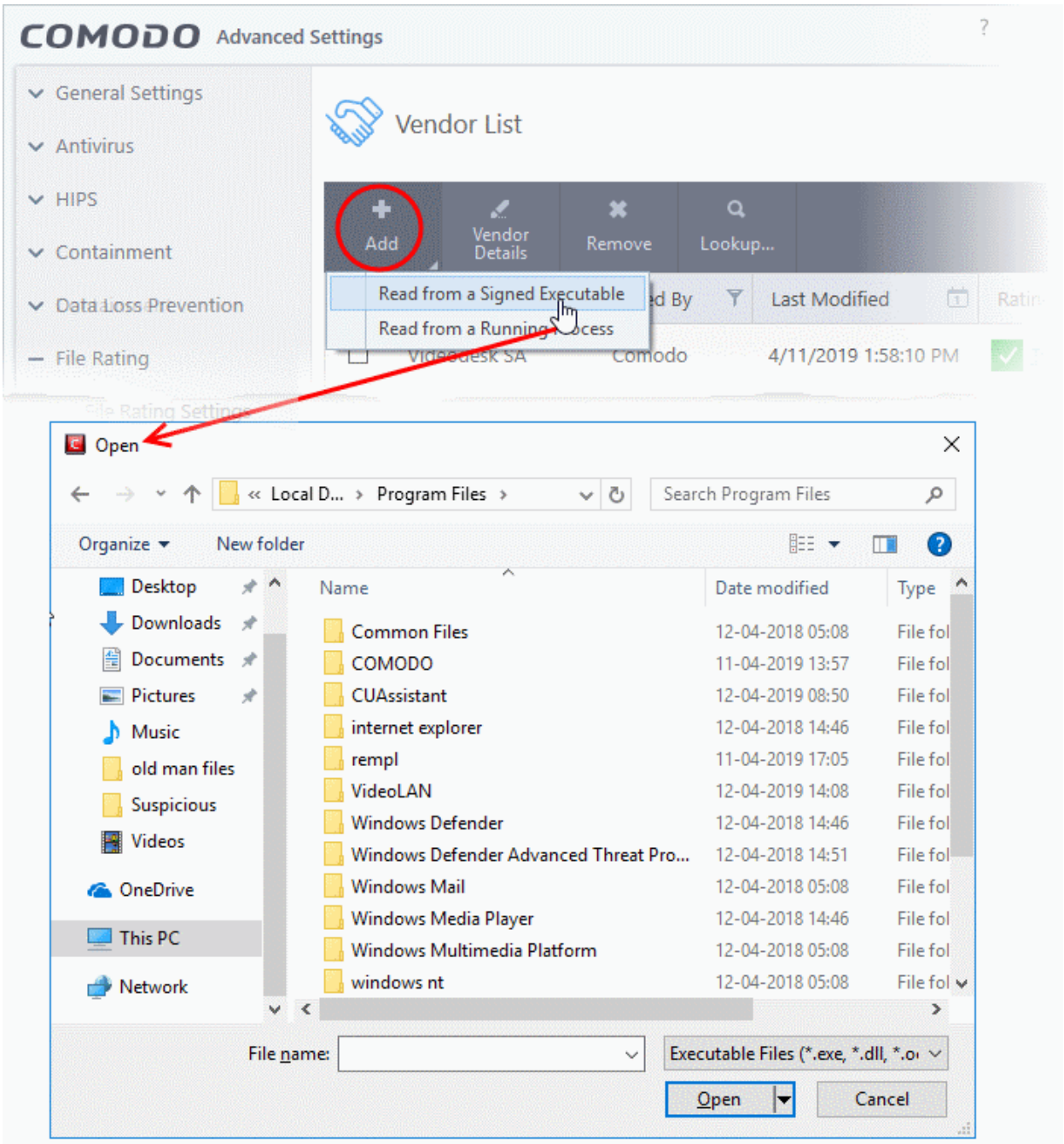
- You can add vendors simply by browsing to a file they have digitally signed
- CCS will read the vendor's signature from the file and add them to the list
- You can then assign your own rating to the vendor

There are two ways to add vendors:

- **Specify an executable file on your local drive**
- **Select a currently running process**

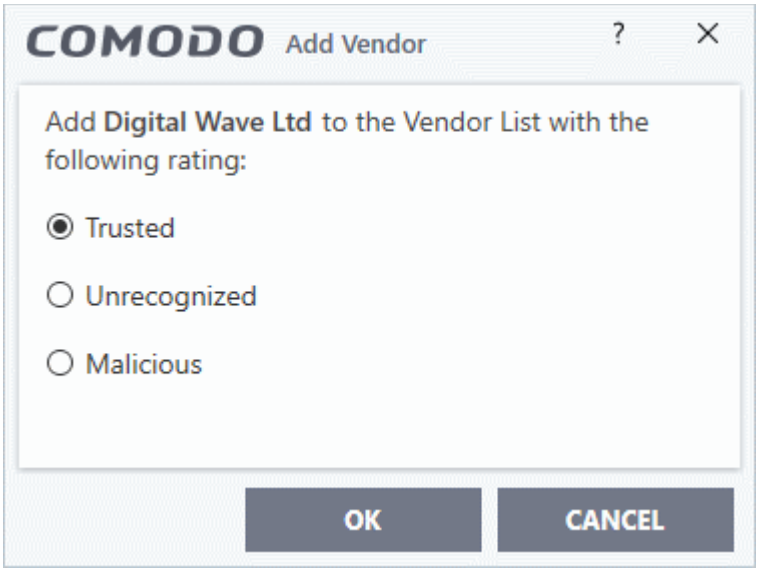
Add a vendor by reading the vendor's signature from an executable

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Click the 'Add' button at the top and select 'Read from a signed executable'
- Alternatively, right-click inside the vendor list and select 'Add' > 'Read from a signed executable'



- Navigate to the executable file whose publisher you want to add to the vendor list and click 'Open'.

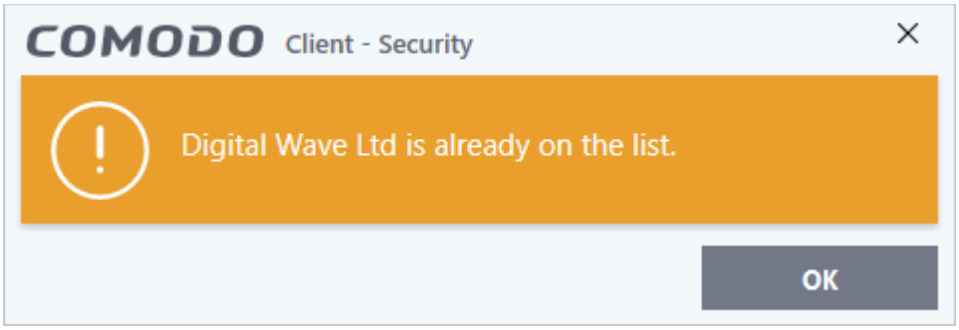
CCS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, you can add the vendor to the list by assigning your trust rating'.



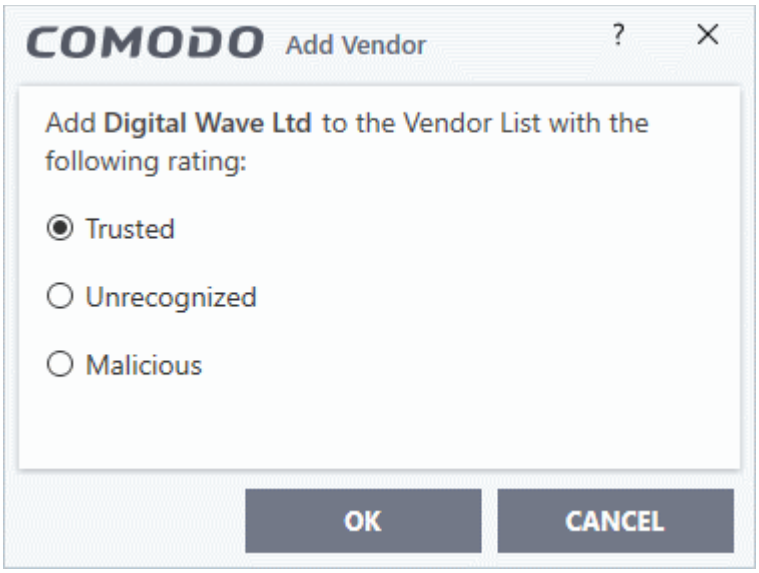
- Choose your rating and click 'OK'

- The vendor will be added to the list with your rating.

  If the vendor is already on the list you will be notified:



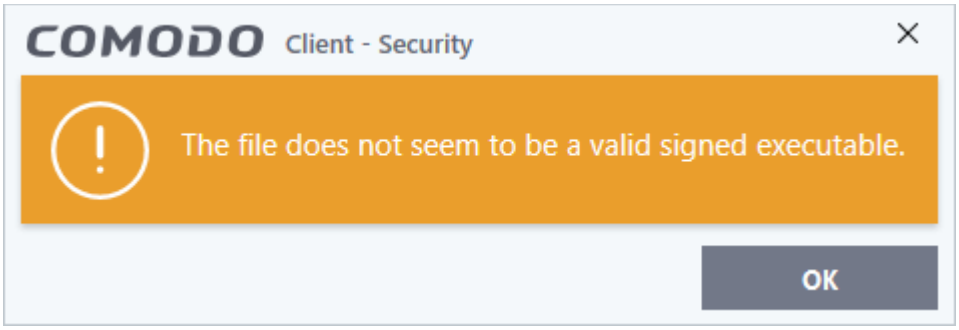
You can assign your own rating to the existing vendor:



- Choose your rating and click 'OK'

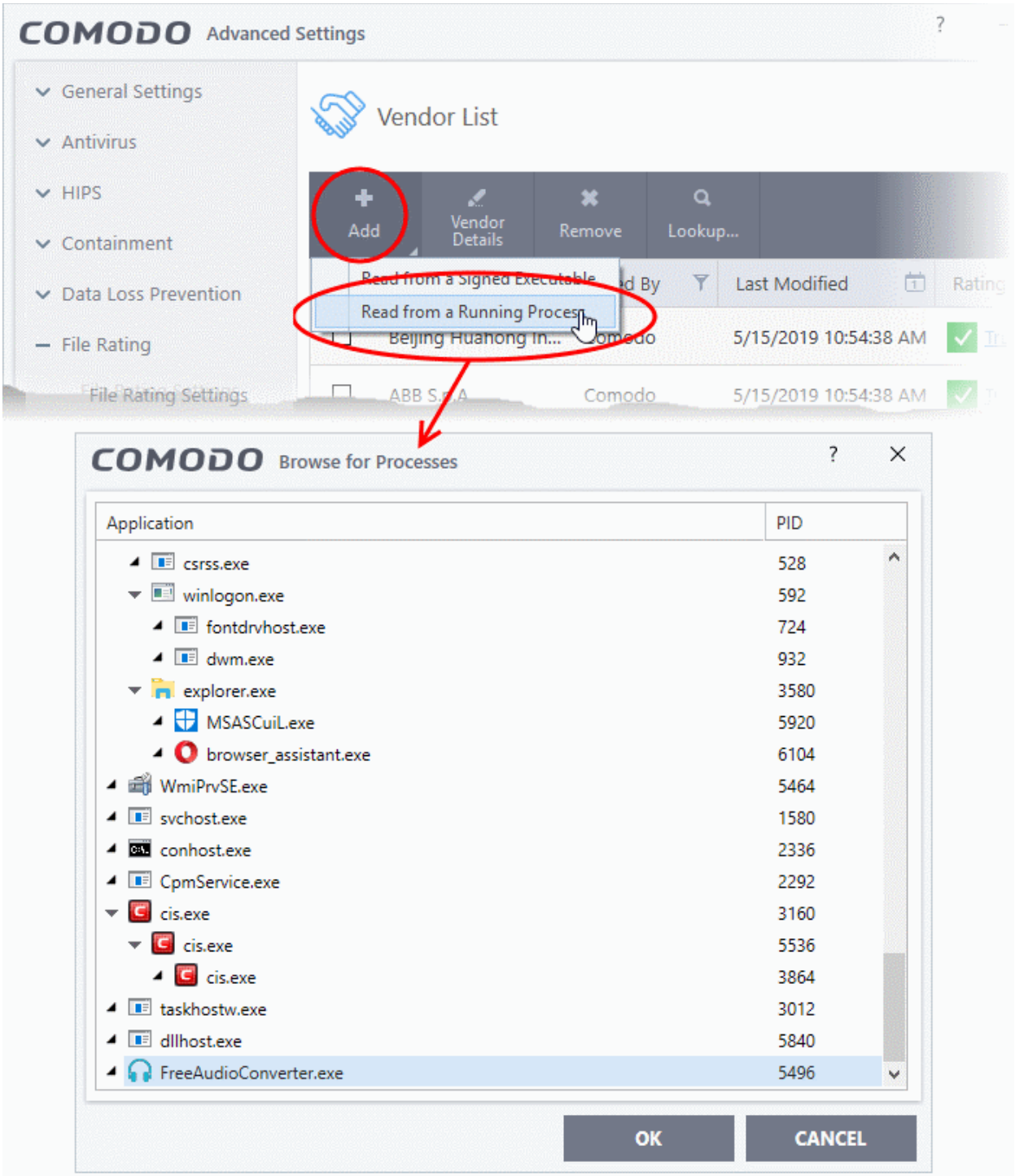
- The user rating for the vendor will be assigned as you set.
- If CCS cannot verify that the software certificate is signed by a Trusted CA then it does not add the software

vendor to the vendor list. In this case, you can see the following error message.



Add a trusted vendor from a currently running process

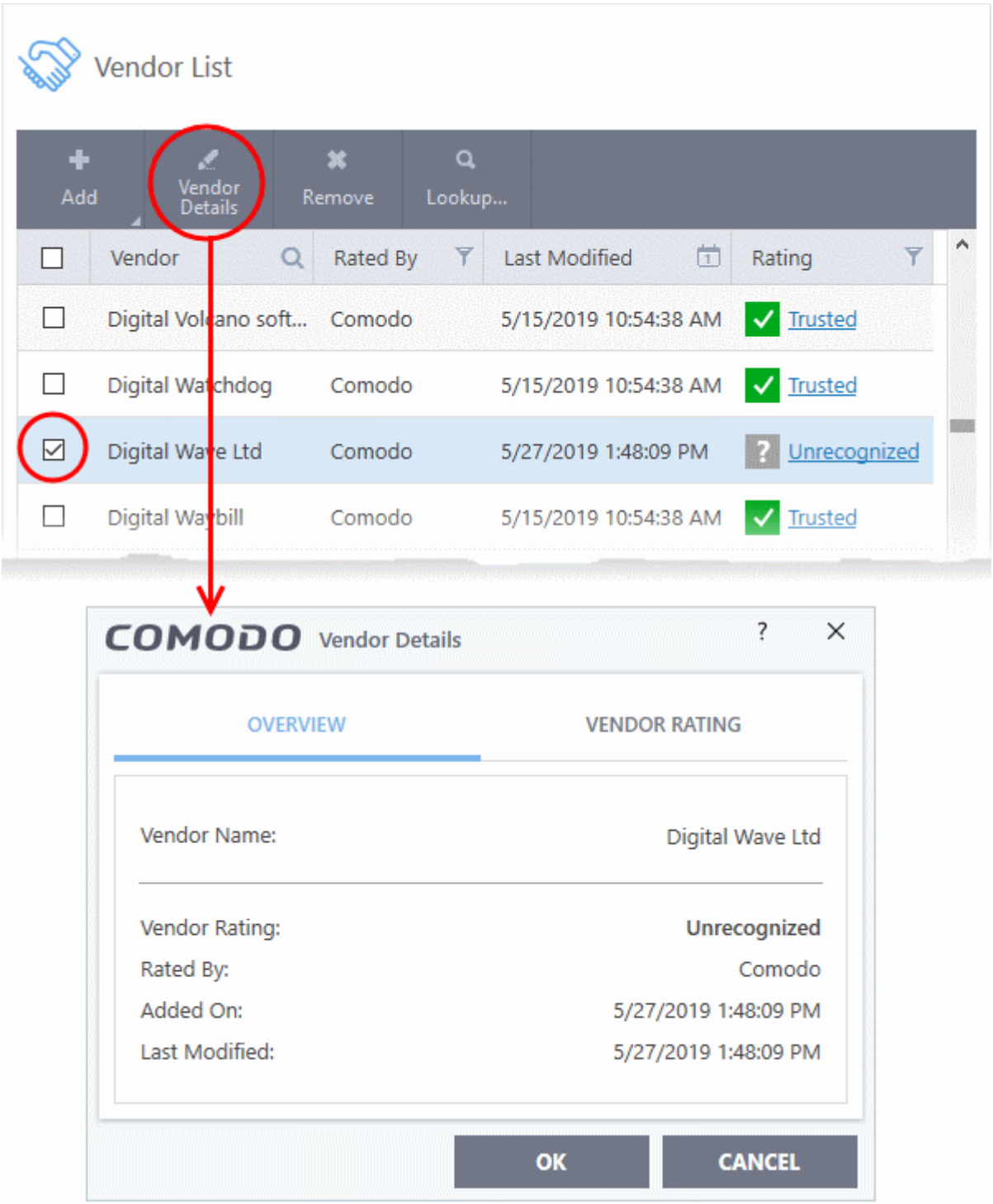
- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Click the 'Add' button at the top and select 'Read from a Running Process'
- Alternatively, right-click inside the vendor list and select 'Add' > 'Read from a Running Process'



- Select the signed executable that you want to trust and click the 'OK' button.
- Comodo Client Security performs the same certificate check as described above. If the parent application of the selected process is signed, you will be able to assign a rating and add the vendor as described **above**.

View details of vendors and assign user rating

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Select a vendor and click the 'Vendor Details' button
- Alternatively right-click on a vendor and select 'Vendor Details'

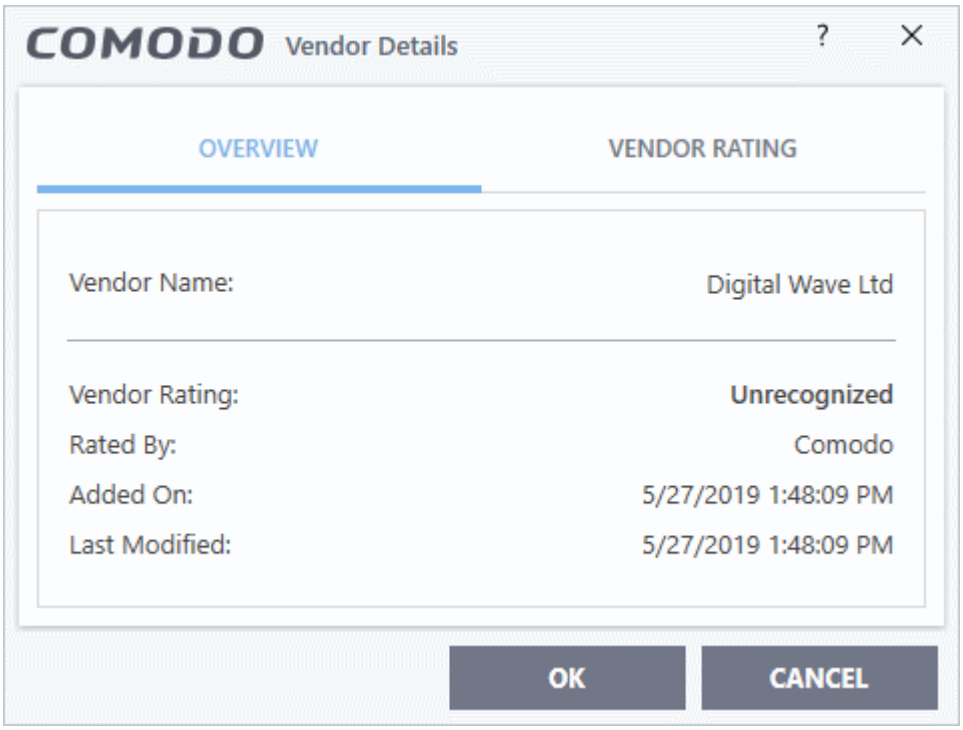


The 'Vendor Details' dialog will open. The dialog has two tabs:

- **Overview**
- **Vendor Rating**

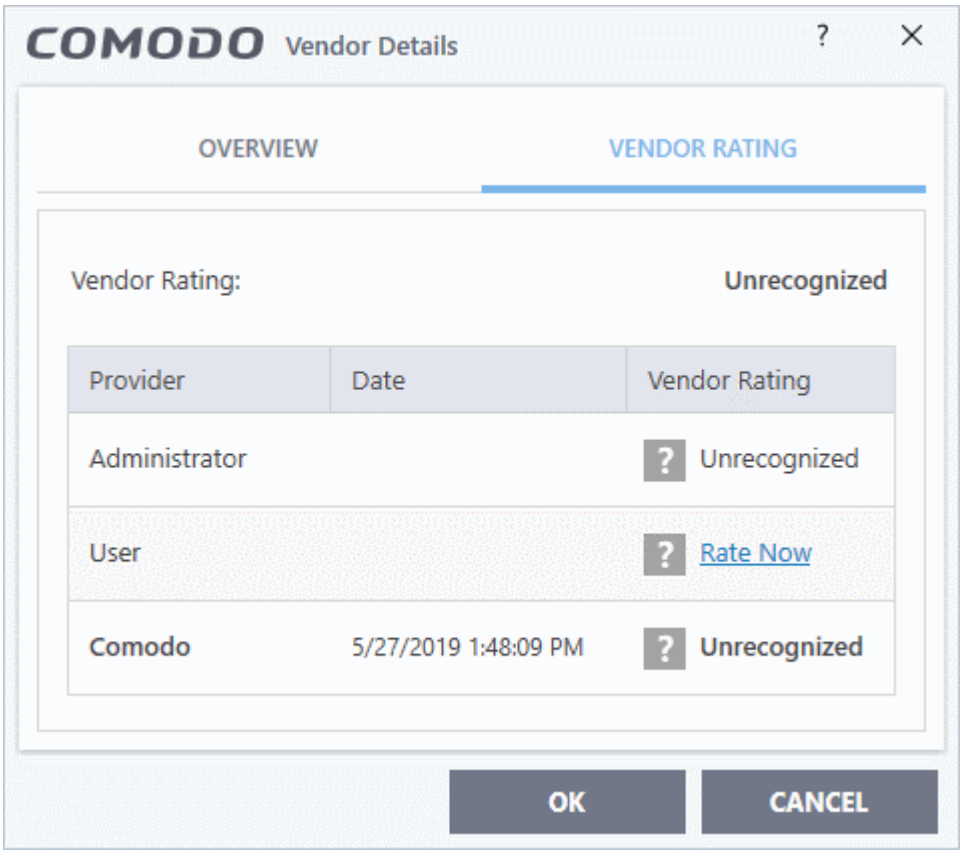
Overview

The 'Overview' tab shows general details such as the vendor name, Comodo assigned rating, when the vendor was added and more:



Vendor Rating

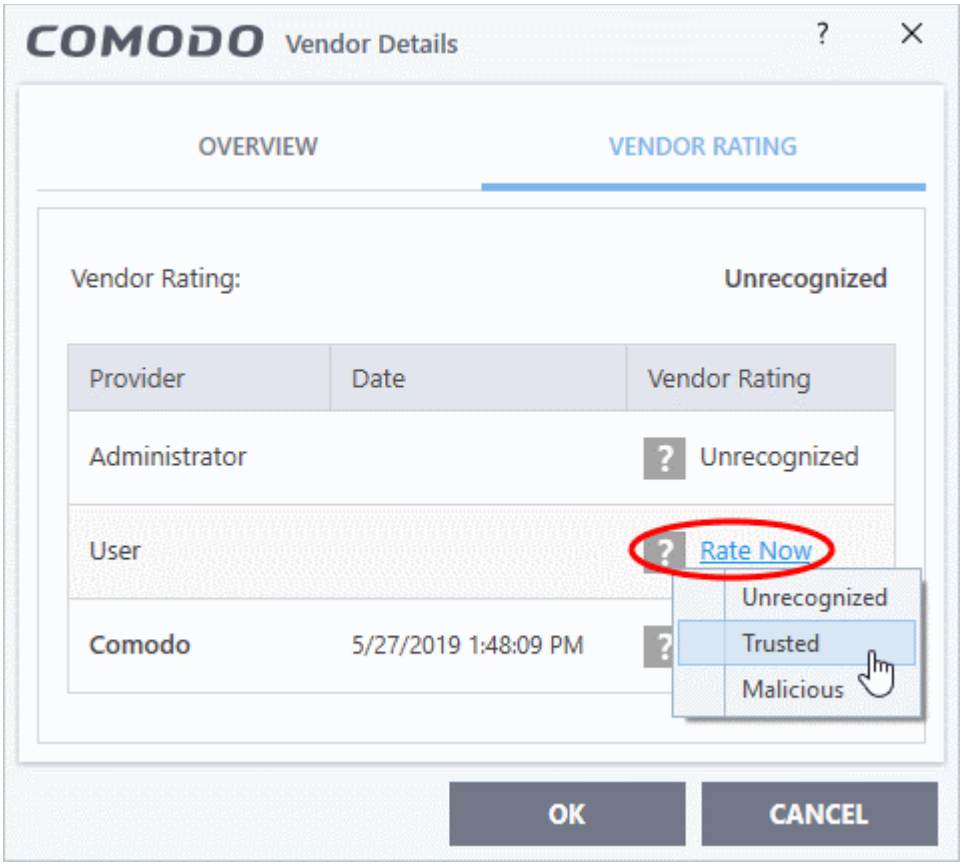
The 'Vendor Rating' tab shows the vendor's current trust rating from Comodo and your admin and lets you set your own rating:



Change the user rating of the file

- Select the vendor from the 'Vendor List' pane and click the 'Vendor Details' button
- Click the 'Vendor Rating' tab from the 'Vendor Details' pane

- Click the 'Rate Now' link beside 'User' and choose the rating from the drop-down



- Click 'OK'
- The trust rating of the vendor will be updated with the user rating in the 'Vendor List' interface.
- You can change the rating for the vendor at anytime by following the same process

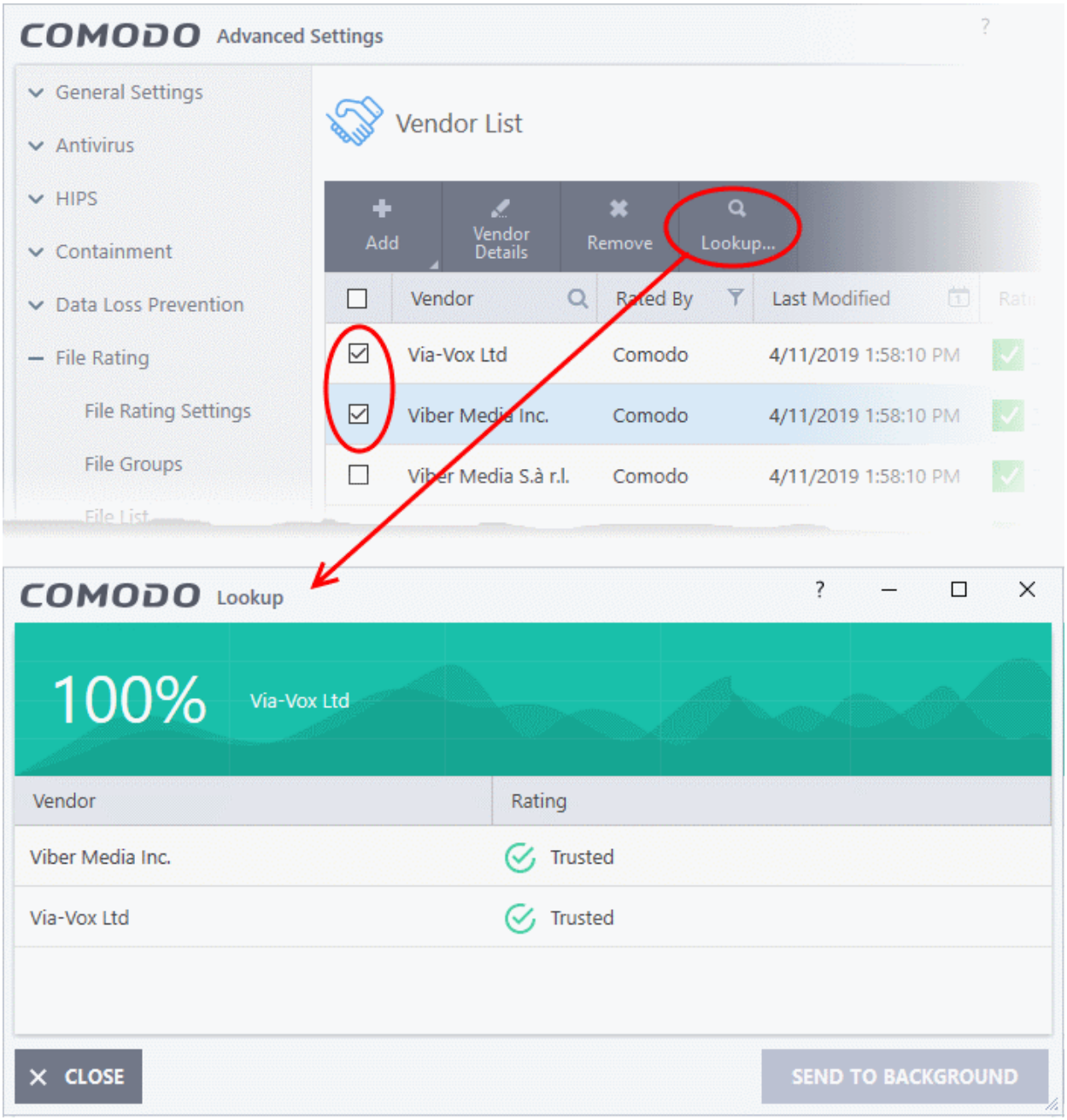
Tip: Alternatively, right click on a selected vendor, then choose 'Change File Rating to' from context sensitive menu and select the rating.

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

Perform an online lookup for vendors

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Select vendor(s) and click the 'Look Up...' button
- Alternatively right-click on a vendor and select 'Look up...'

Comodo servers will be contacted immediately to conduct a search of Comodo's trusted vendor list database to check if any information is available about the vendor in question and the results will be displayed.



Remove vendors from the list

- Click 'Settings' on the CCS home-screen
- Click 'File Rating' > 'Vendor List'
- Select vendor(s) and click the 'Remove' button
- Alternatively right-click on a vendor and select 'Remove'

Background

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

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

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

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

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the vendor list.

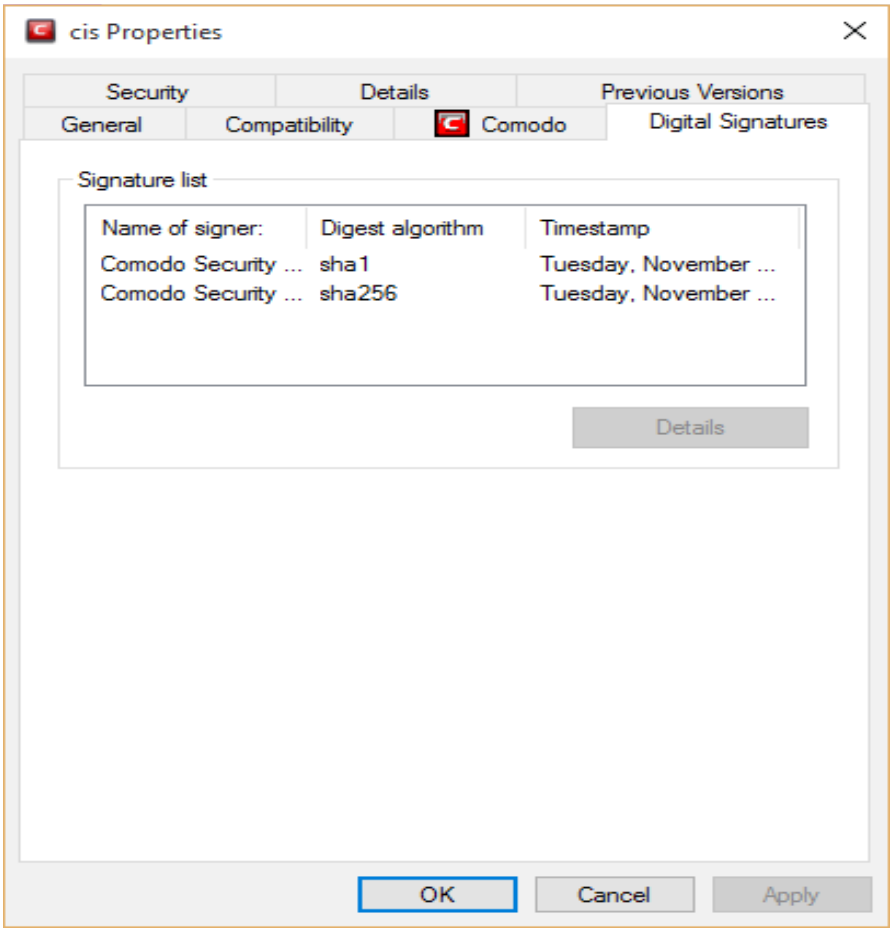
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Sectigo', 'Identrust' and 'Digicert' are examples of trusted CA's authorized to counter-sign 3rd party software. The counter-signature is critical to the trust process, so a CA only counter-signs a certificate after conducting strict background checks on the vendor.

If a file is signed by a vendor with 'Trusted' rating in the vendor list and the user has 'Rate applications according to their vendor rating' in the 'File rating Settings' then it will be automatically trusted by Comodo Client Security.

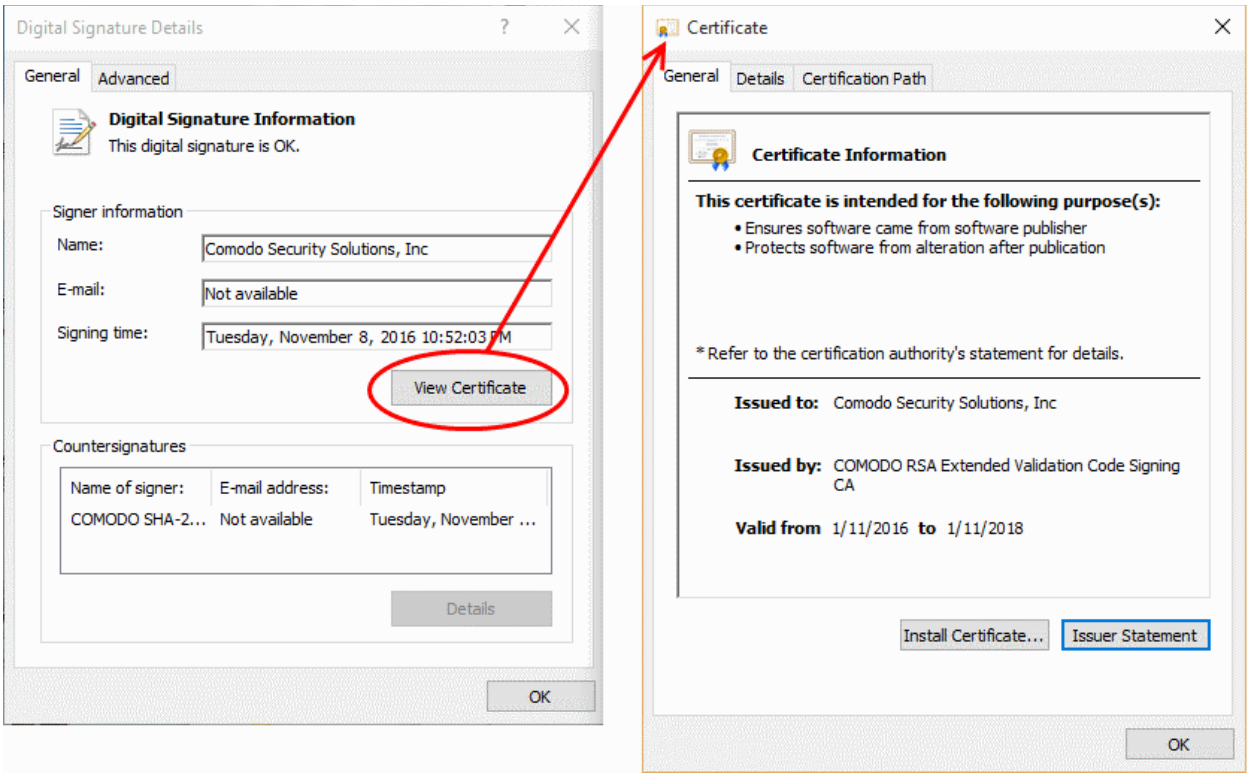
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main executable for Comodo Client Security is called 'cis.exe', which has been counter-signed by Sectigo certificate authority.

- In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with. They know they are downloading and installing the genuine software.
- The 'Vendors' that digitally sign their software are the software publishers. These are the company names you see listed in the vendor list
- However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Certificate Authority' (CA).
- 'Sectigo CA Limited' and 'Verisign' are two example CAs who are authorized to counter-sign 3rd party software.
- The counter-signature is critical to the trust process. A CA only counter-signs a certificate after it has conducted detailed background checks on the publisher.
- One of the methods of identifying whether an executable file has been digitally signed is by checking the properties of the .exe file in question.
- For example, the main program executable for Comodo Client Security is called 'cis.exe' and has been digitally signed.
    - Browse to the (default) installation directory of Comodo Client Security.
    - Right click on the file cis.exe.
    - Select 'Properties' from the menu.
    - Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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



Click the 'Details' button to view certificate details. Click the 'View Certificate' button to inspect the actual code signing certificate. (see below).



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

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default 'Vendor List' with 'Trusted' status that is shipped with Comodo 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 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 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 vendor list of the next release of CCS.

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

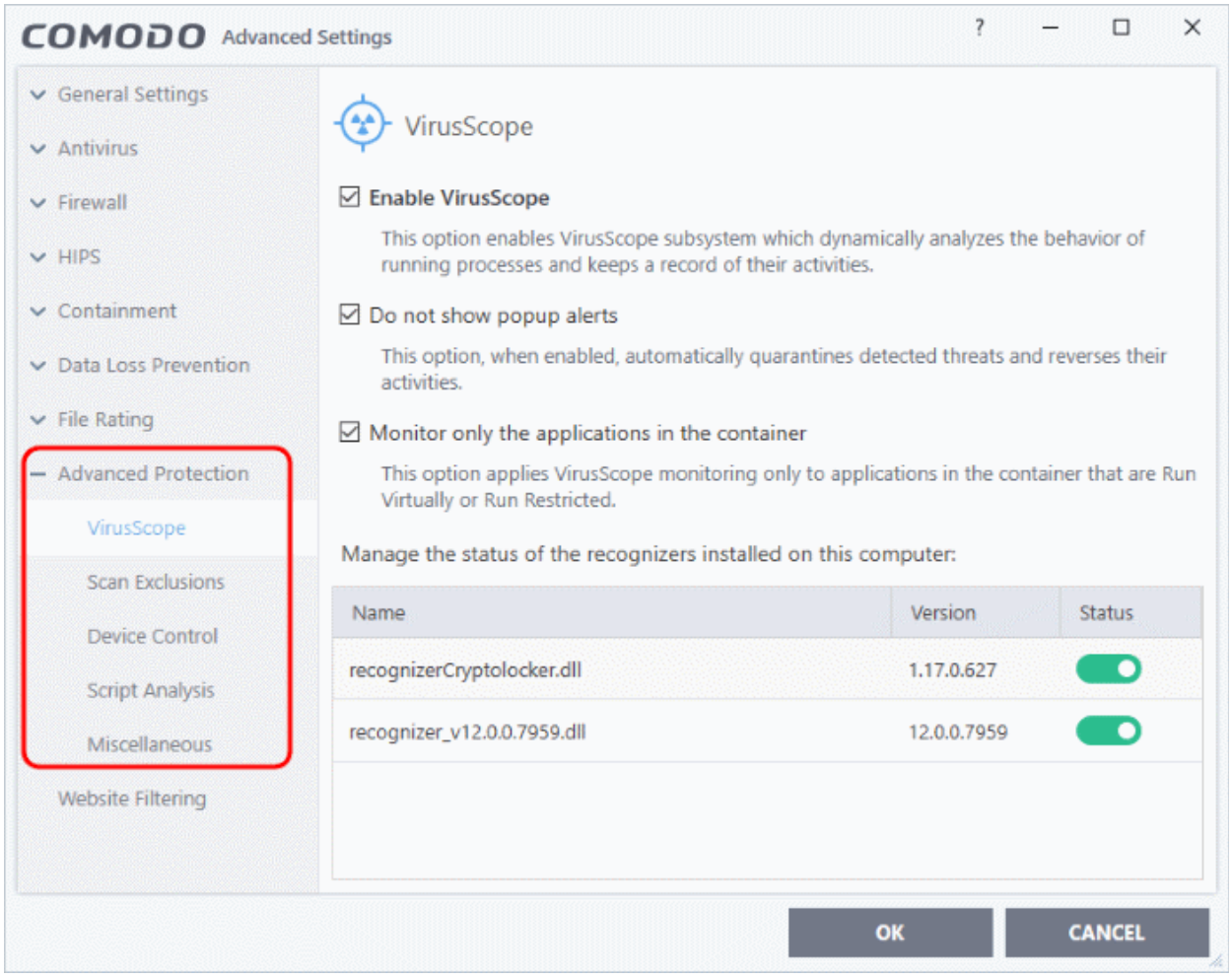
7.9. Advanced Protection

The 'Advanced Protection' section allows you to:

- Configure the VirusScope component
- Specify items you want to exclude from detection during a virus scan
- Specify types of external devices are to allowed / blocked
- Configure heuristic command line analysis and embedded code detection on files that can execute code
- Configure miscellaneous settings.

Open the 'Advanced Protection' area

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' on the left:

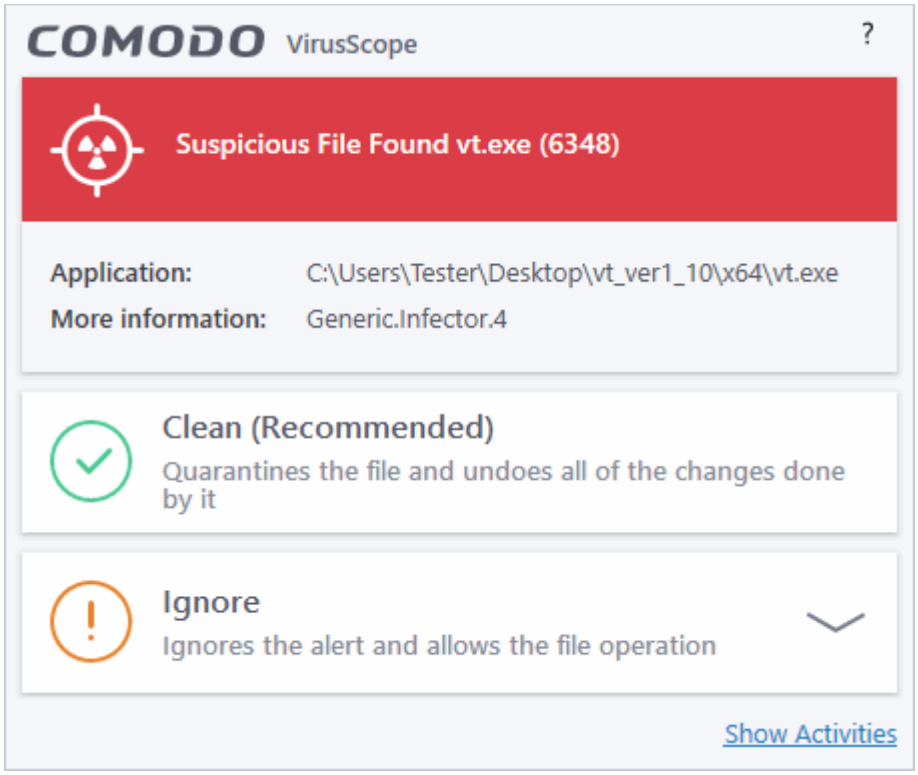


Click the following links to jump to the section you need help with:

- **VirusScope Settings** - Configure VirusScope behavior
- **Scan Exclusions** - Add and manage items that should be ignored during a scan
- **Device Control Settings** - Manage types of external devices like USB drives, and printers that can connect to and are to be blocked
- **Script Analysis** - Manage heuristic command line analysis and embedded code detection
- **Miscellaneous Settings** - Exclude files from buffer overflow monitoring, configure browser alerts, and more

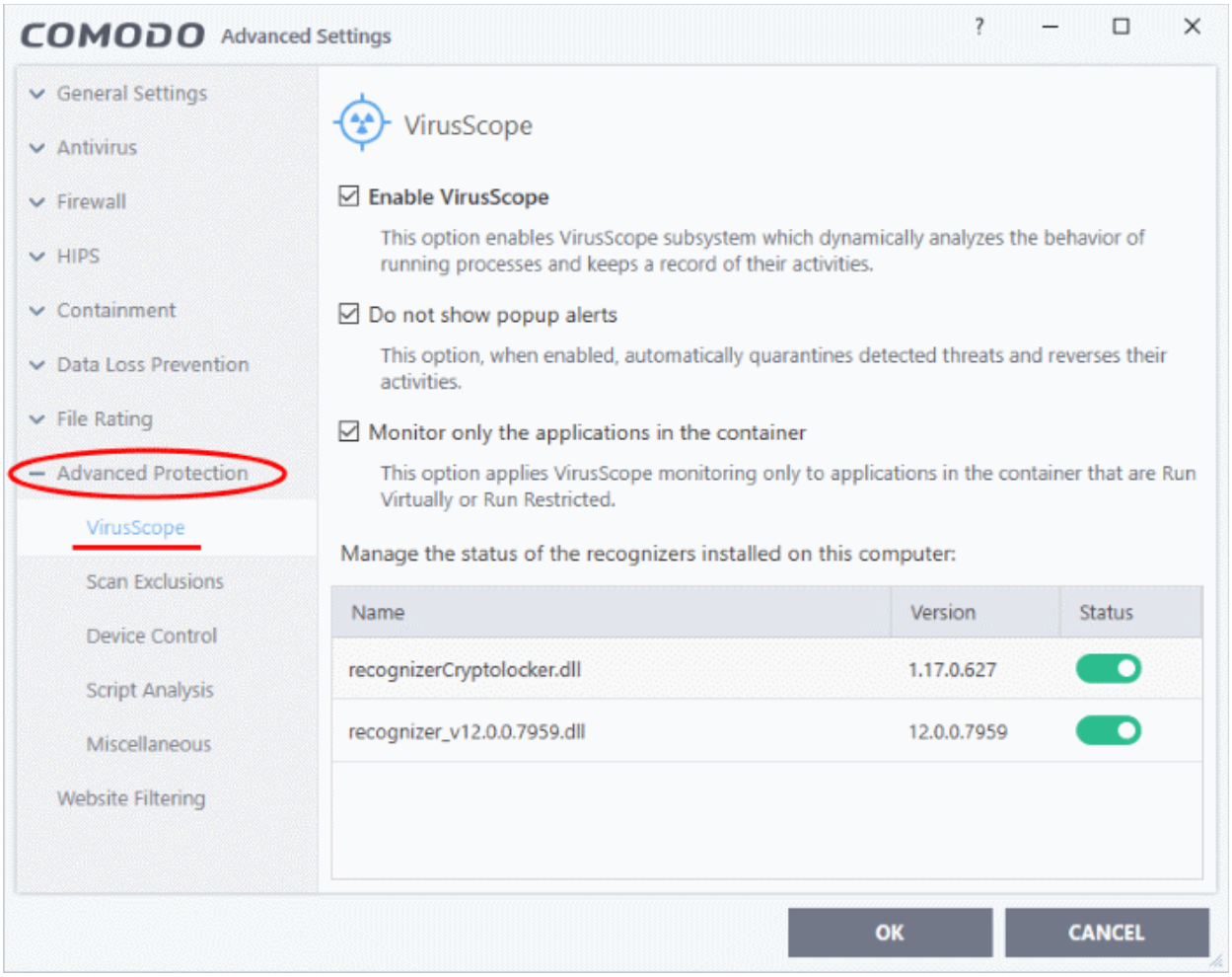
7.9.1. VirusScope Settings

- Click 'Settings' > 'Advanced Protection' > 'VirusScope'
- VirusScope monitors the activities of processes running on your computer and alerts you if they take actions that could threaten your privacy or security.
- VirusScope also allows you to reverse the actions of software without blocking the software itself. This provides more flexibility over legitimate software which requires certain actions to be implemented in order to run correctly.
- VirusScope alerts give you the opportunity to quarantine the process & reverse its changes, or to let the process go ahead.
- Be especially wary if a VirusScope alert appears 'out-of-the-blue' when you have not made any recent changes to your computer.



Open the 'VirusScope' settings section:

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'VirusScope':



VirusScope Settings

VirusScope monitors running processes and alerts you to suspicious activity. You then have the option to quarantine the suspicious file and undo its activities.

- **Enable VirusScope** - Activate VirusScope. If enabled, VirusScope monitors the activities of running processes and generates alerts if suspicious activity is detected. (***Default = Enabled***)
- **Do not show pop-up alerts** - Whether CCS should show an alert if VirusScope detects suspicious activity. (***Default = Disabled***)
  - If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed.
- **Monitor only applications in the container** - VirusScope only tracks the activities of processes that a running in the container. It will not track processes directly running on the host (***Default = Enabled***)
- Applications can be made to run in the container in two ways:
  - Run a program in the container on a 'one-off' basis. See **Run an Application in the Container** for more details.
  - Create a rule to auto-contain programs that match certain criteria. See **Auto-Containment Rules** for more details.

Manage the status of recognizers

- VirusScope detects zero-day malware by analyzing the behavior and actions of an application.
- If the detected behavior corresponds to that of known malware, then VirusScope will generate an alert which allows you to quarantine the application and reverse any changes that it made.
- A 'recognizer' file contains the sets of behaviors that VirusScope needs to look out for.

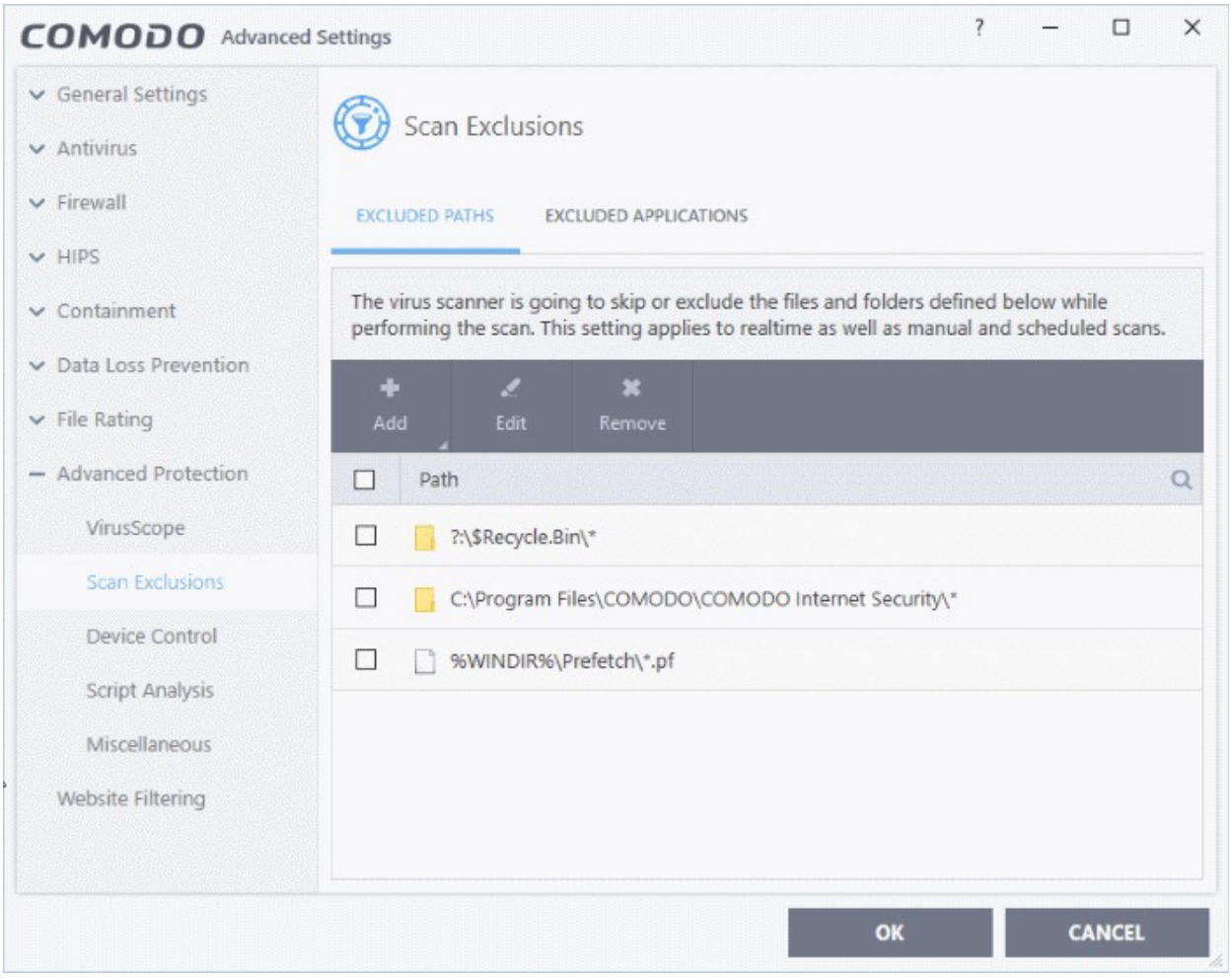
- If you disable a recognizer, VirusScope will no longer show an alert if an application exhibits behavior described by the recognizer.
- We recommend most users to leave the 'Status' of recognizers at their default settings.
- Advanced users, however, may want to try disabling recognizers if they are experiencing a large number of VirusScope false positives.

7.9.2. Scan Exclusions

- Click 'Settings' > 'Advanced Protection' > 'Scan Exclusions'
- The 'Scan Exclusions' panel shows files and paths which you have chosen to skip during a virus scan.
- CCS will not generate an alert for an excluded item, even if the item is rated as malicious in the global blacklist.
- Items may have been added to this list because you selected 'Ignore' at the scan results window, or because you added them to exclusions at an alert.

Open the 'Scan Exclusions' panel

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'



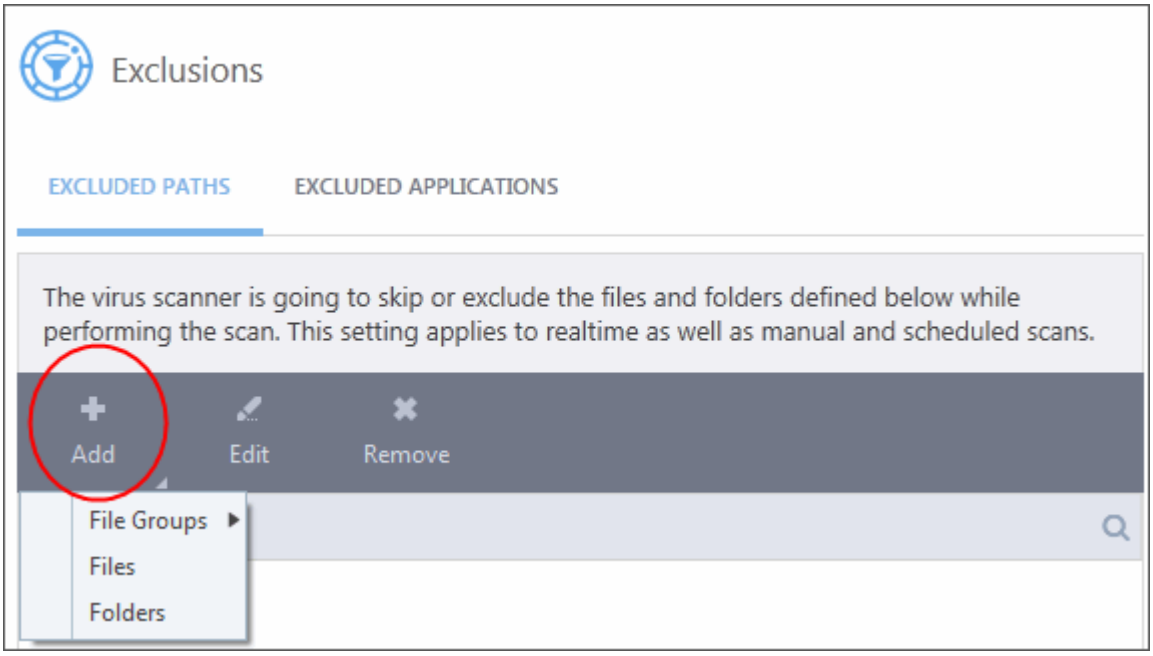
The 'Scan Exclusions' panel has two tabs:

- **Excluded Paths** - A list of paths/folders/files on your computer which are excluded from real-time, on-demand and scheduled antivirus scans. See '**Exclude Drives/Folders/Files from all types of scans**' for more details.

- **Excluded Applications** - A list of applications which are excluded from real-time antivirus scans. Items can be excluded by clicking 'Ignore' in the virus '**Scan Results**', or by clicking 'Ignore' at an **Antivirus Alert**, or by excluding it manually. Note - excluded items are skipped by the real-time scanner but will be scanned during on-demand scans. See '**Exclude Programs/Applications from real-time scans**' for more details.

Exclude Drives/Folders/Files from all types of scans

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click the 'Add' button:



You can add a:

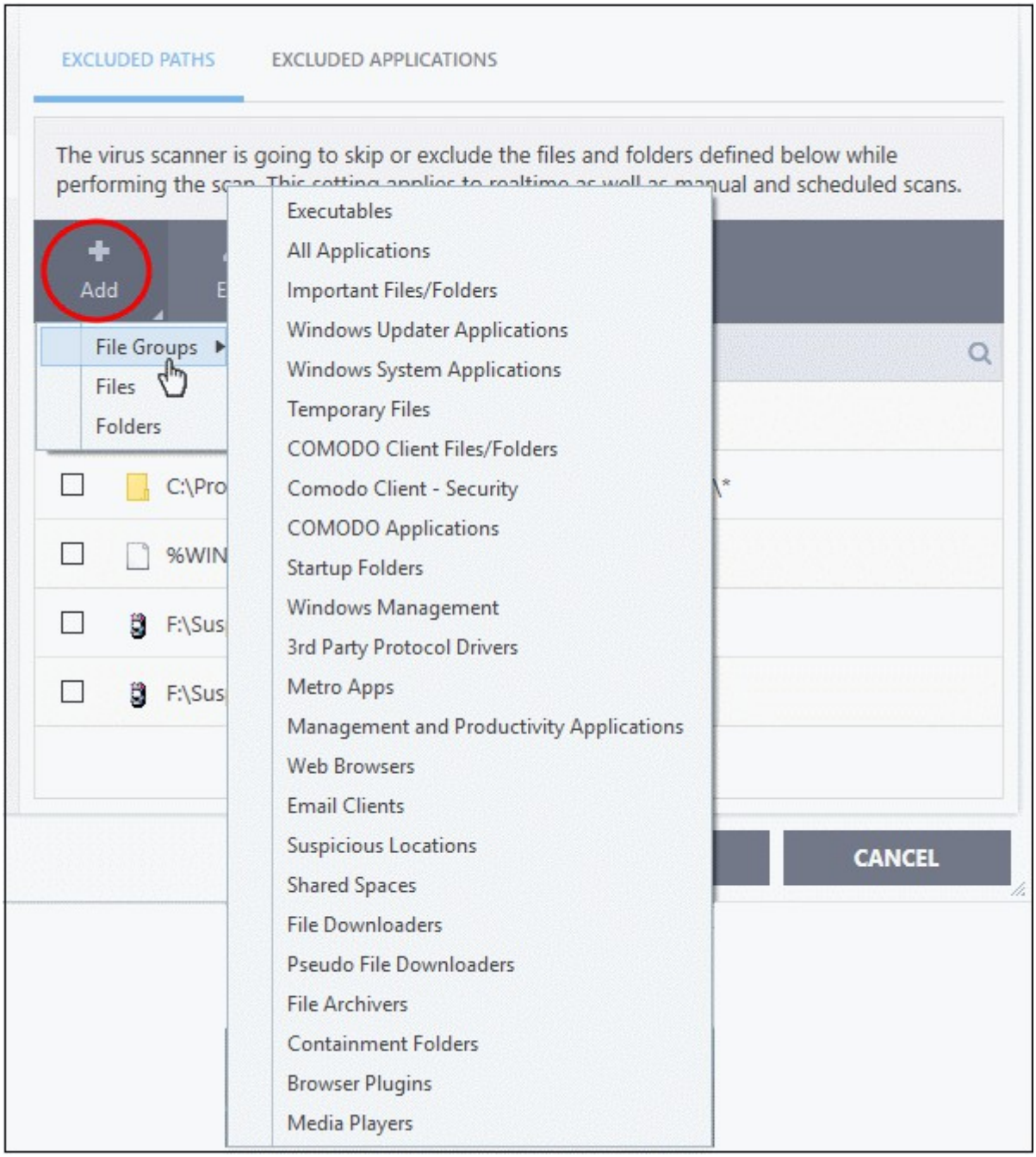
- **File Group**
- **Drive partition/Folder**

  or

- **Individual file**

Add a File Group

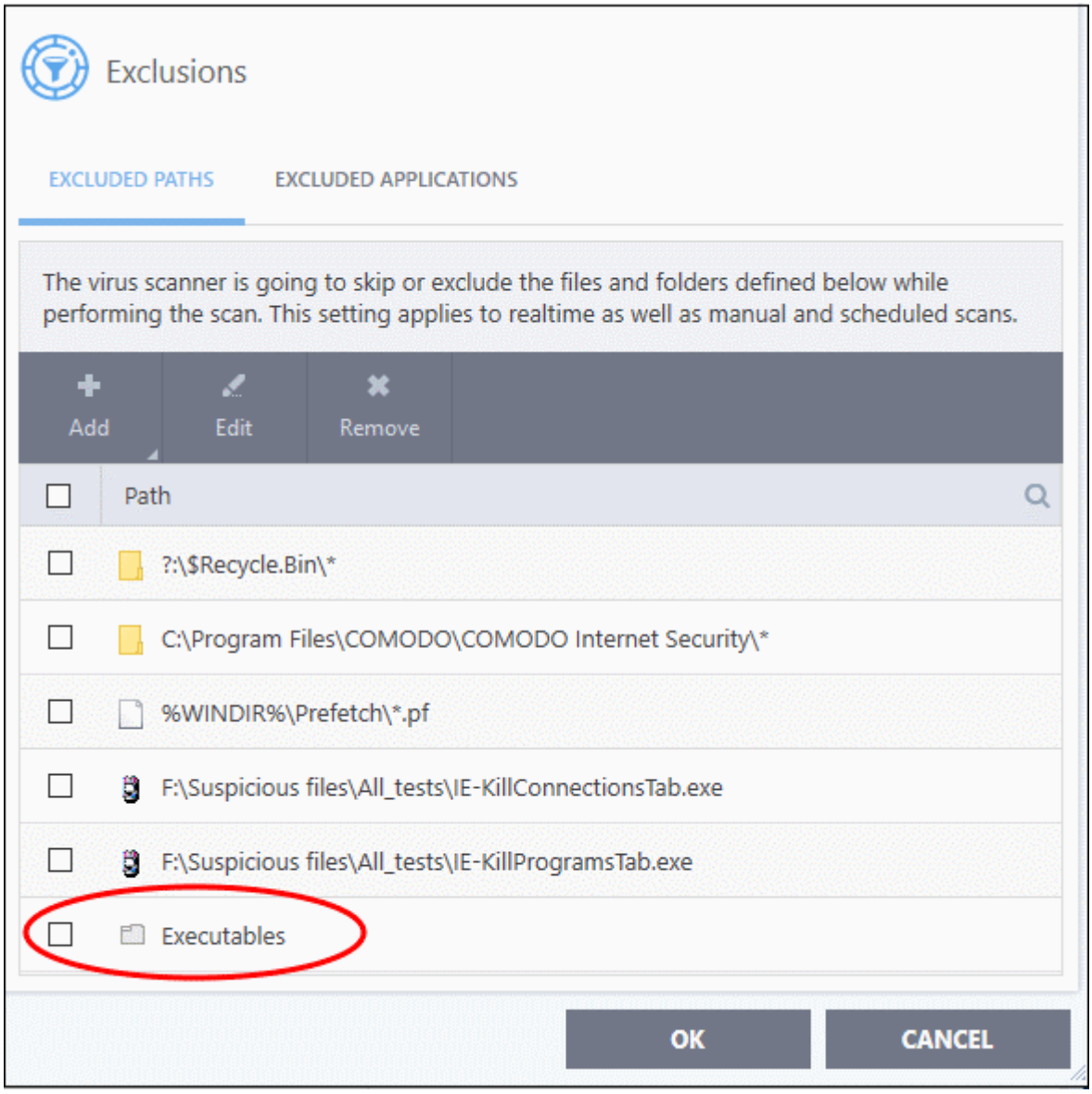
- Choose 'File Groups' to exclude a pre-set category of files or folders. This provides a convenient way to apply a generic ruleset to important files and folders.
- For example, selecting 'Executables' allows you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl *\cmd.exe, *.bat, *.cmd.
- Other categories include 'Windows System Applications', 'Windows Updater Applications' and 'Start Up Folders'.



- CCS ships with a set of predefined file groups which can be viewed in 'Advanced Settings' > 'File Rating' > 'File Groups'.
- You can also add new file groups as required. See **File Groups** for more details.

Add new file groups to exclusions

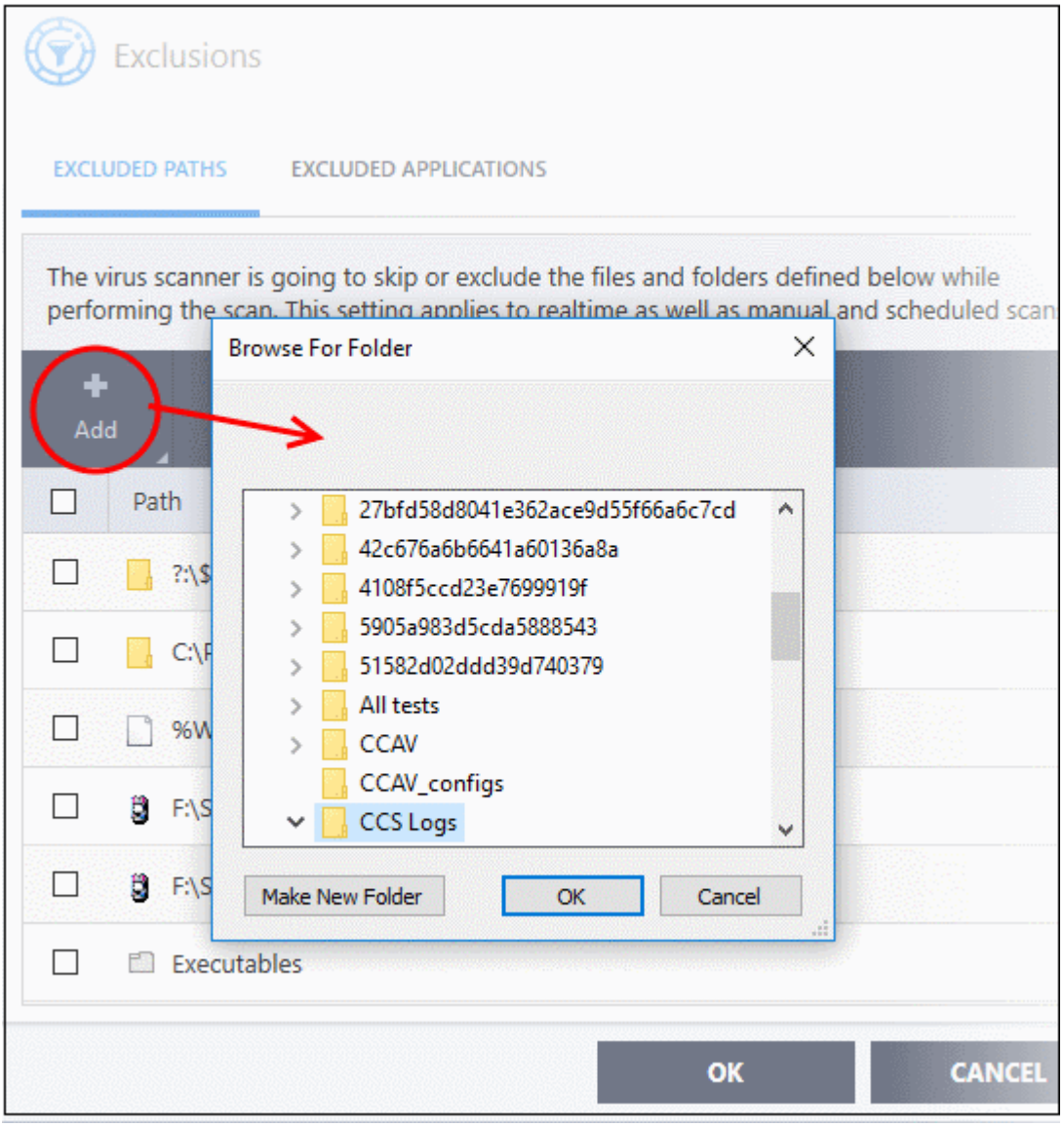
- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Click 'Add' > 'File Groups'
- Select the target file group from the list:



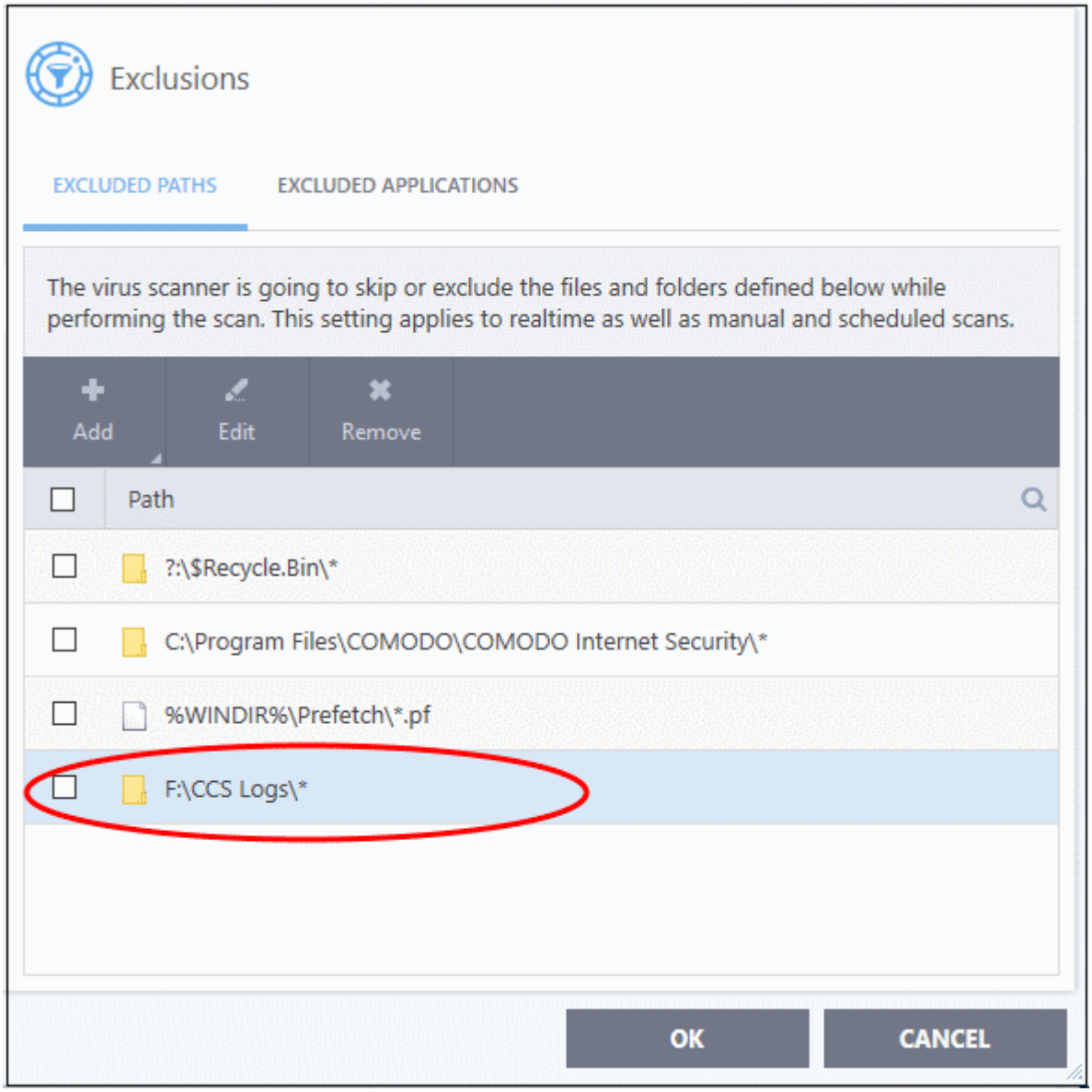
- Repeat the process to add more file groups.
- Items added to the 'Excluded Paths' will be omitted from all types of future Antivirus scans.

Add a Drive Partition/Folder

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click 'Add' > 'Folders'
- Navigate to the drive partition or folder you want to add to excluded paths and click 'OK'.



The folder/partition will be added to the list of excluded items:

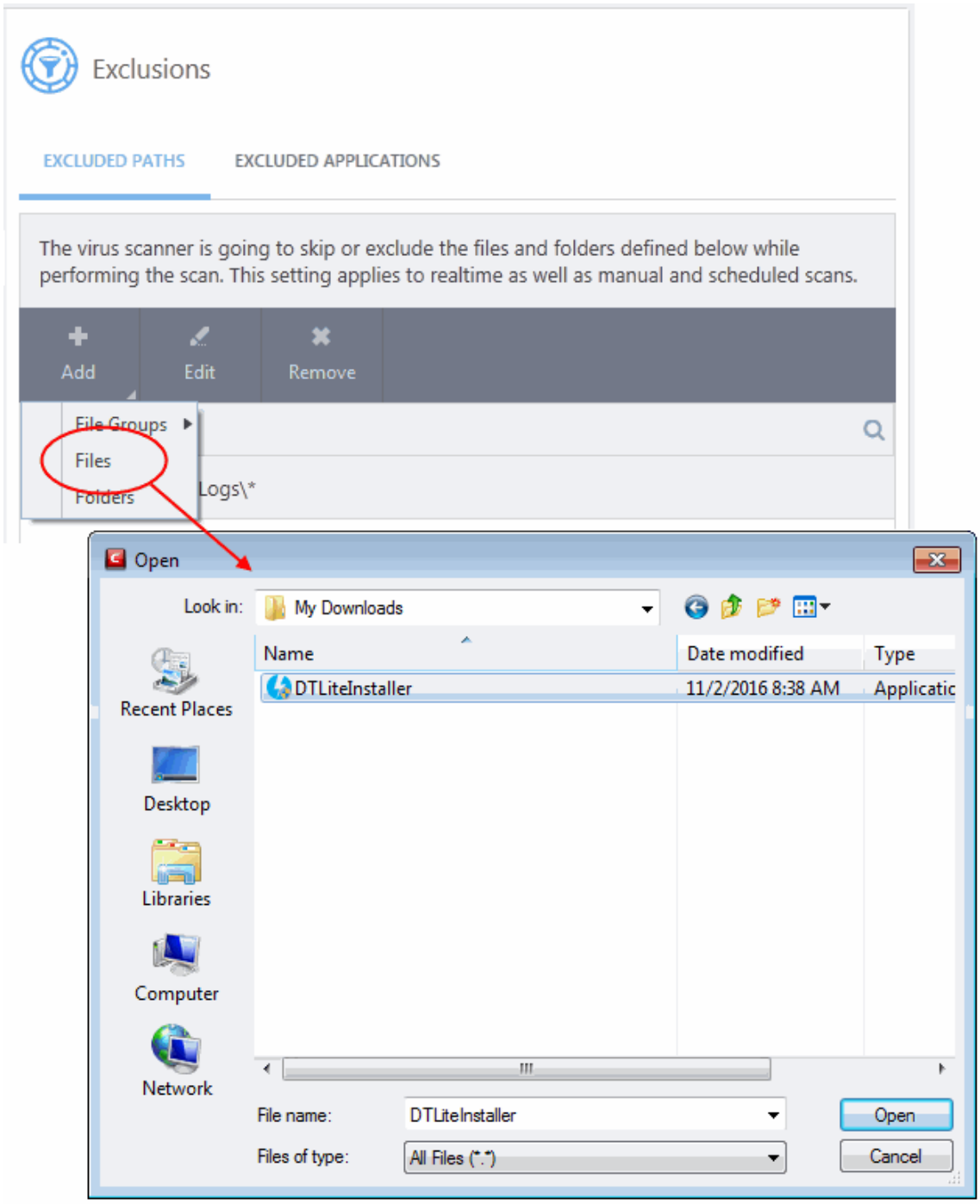


- Repeat the process to add more folders. Items added to 'Excluded Paths' will be omitted from all types of antivirus scans in future.

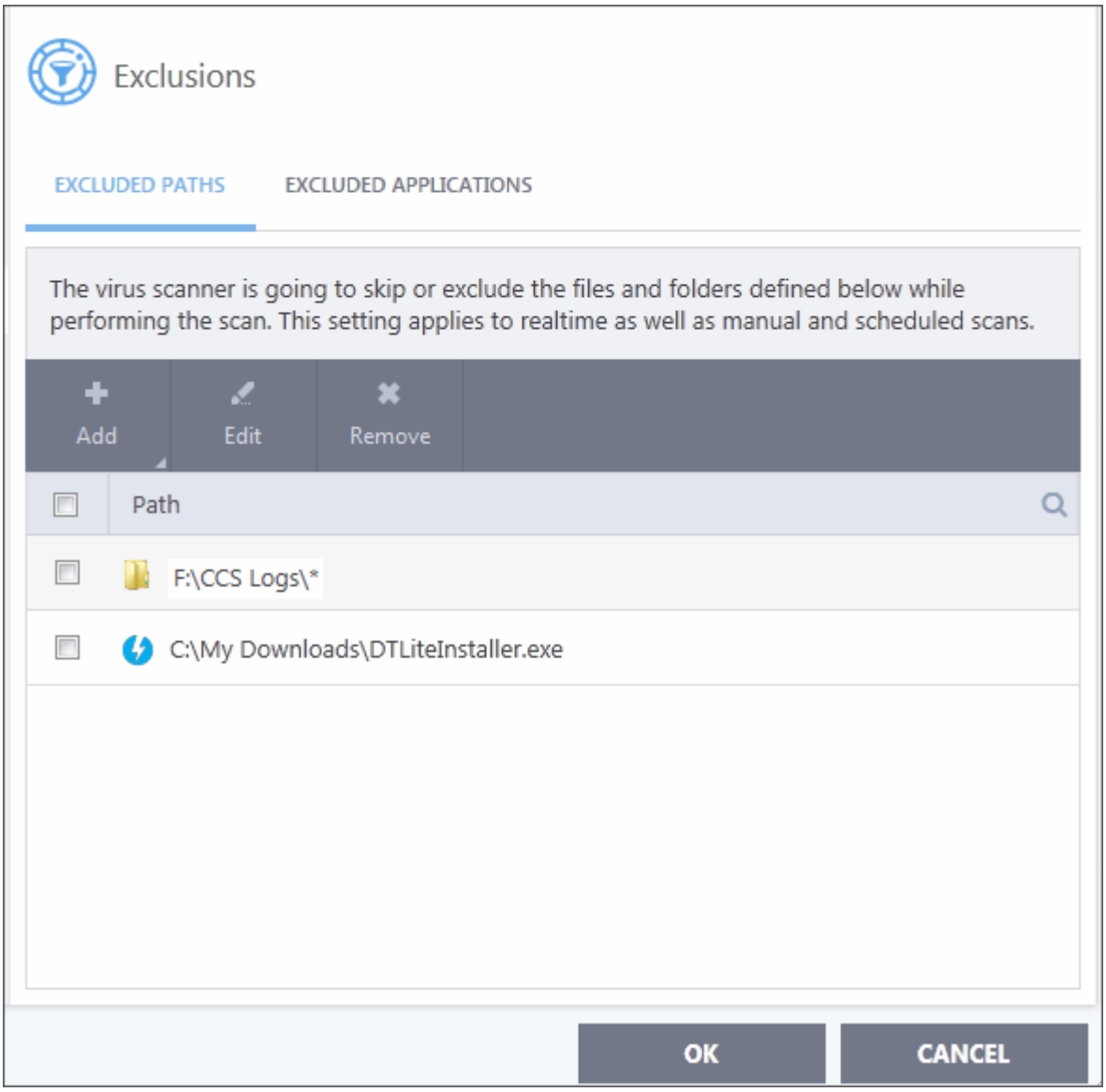
Add an individual file

You can specify individual files as excluded path.

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Click 'Add' > 'Files'
- Navigate to the file you want to add to excluded paths and click 'OK'.



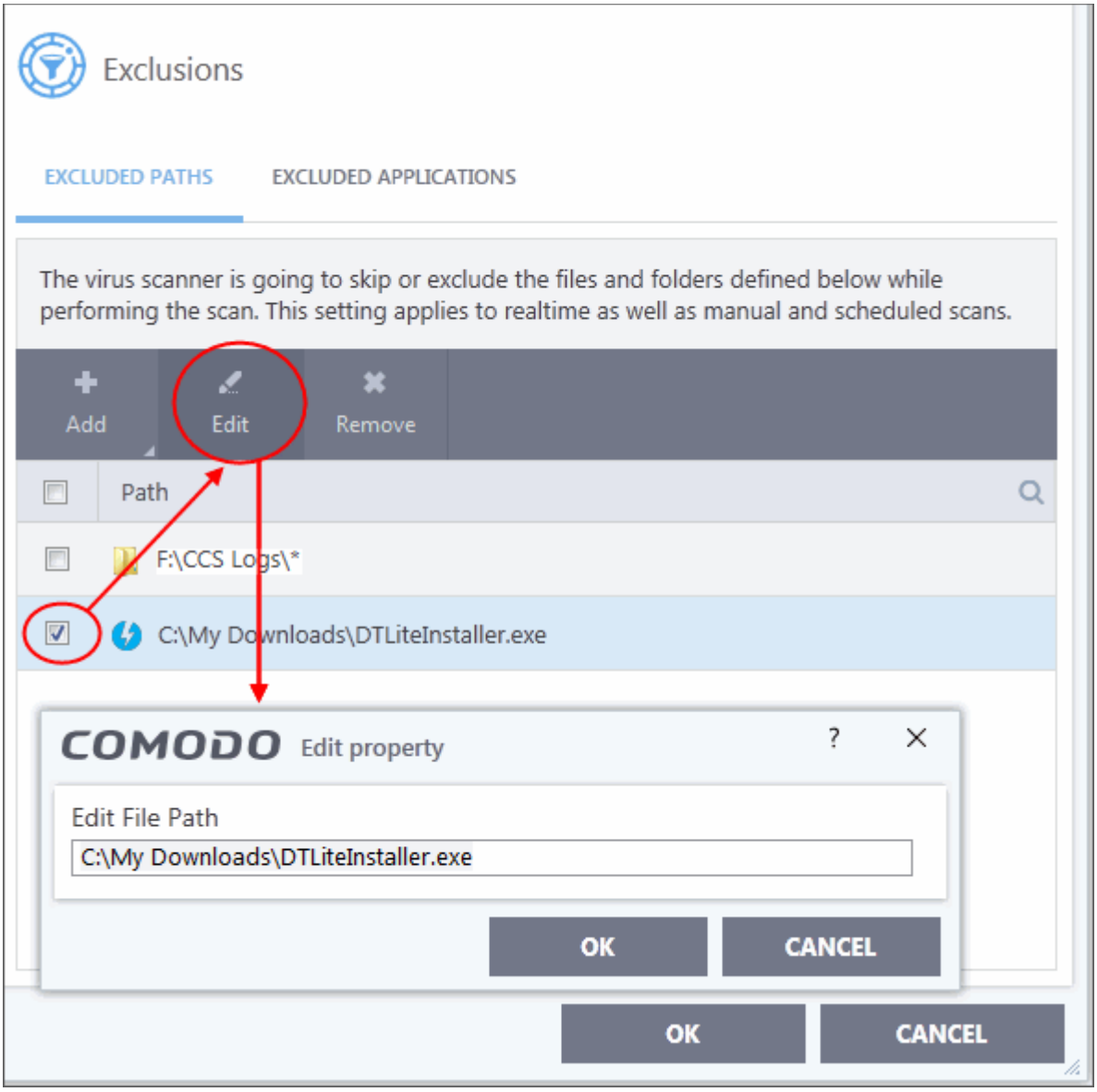
- The file will be added to excluded paths:



- Repeat the process to add more paths.
- Items added to 'Excluded Paths' will be omitted from all types of virus scan in the future.

Edit the path of an added item

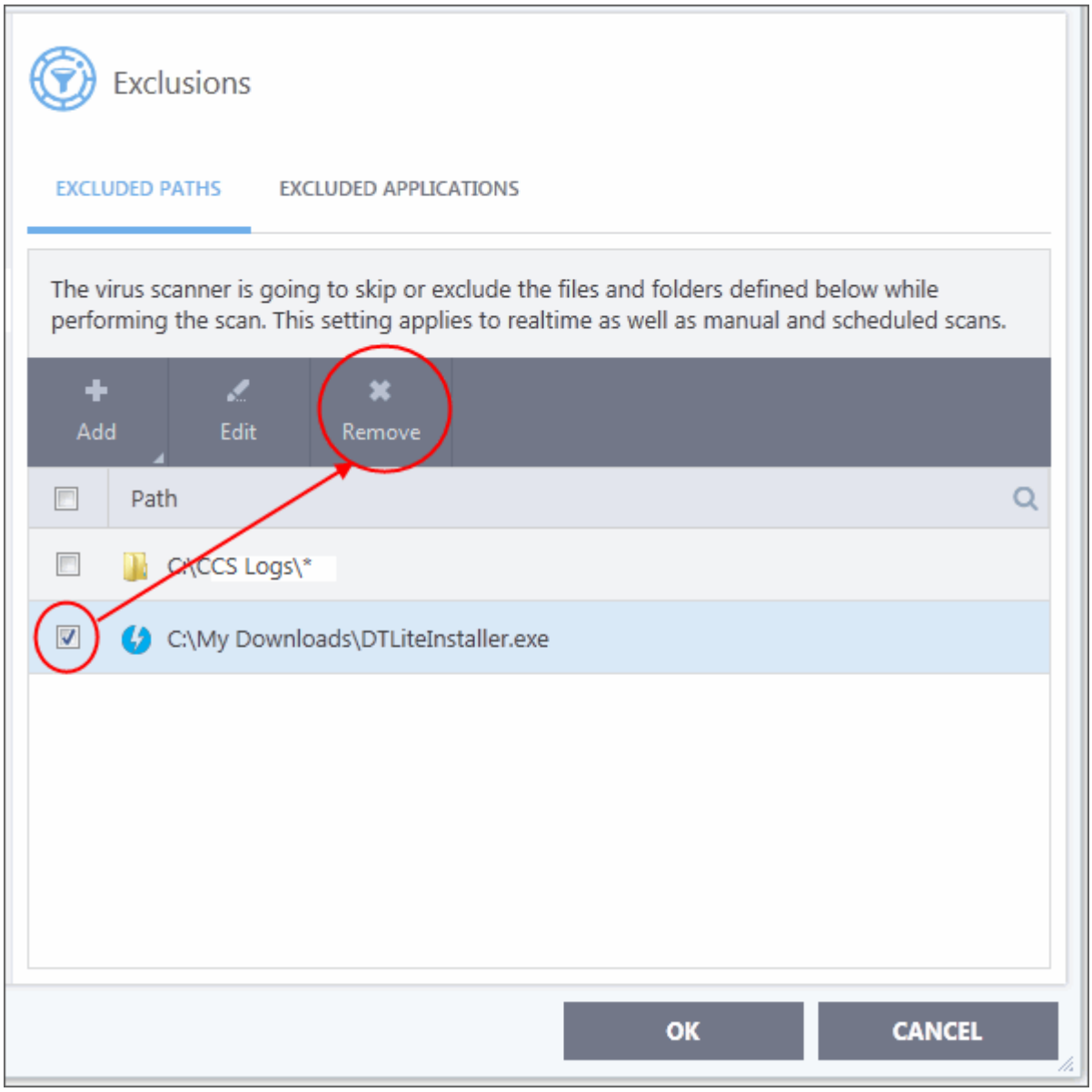
- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Select the target item and click 'Edit':



- Modify the file-path as required and click 'OK'.

Remove an item from 'Excluded Paths'

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Paths' tab
- Select the target item and click 'Remove':



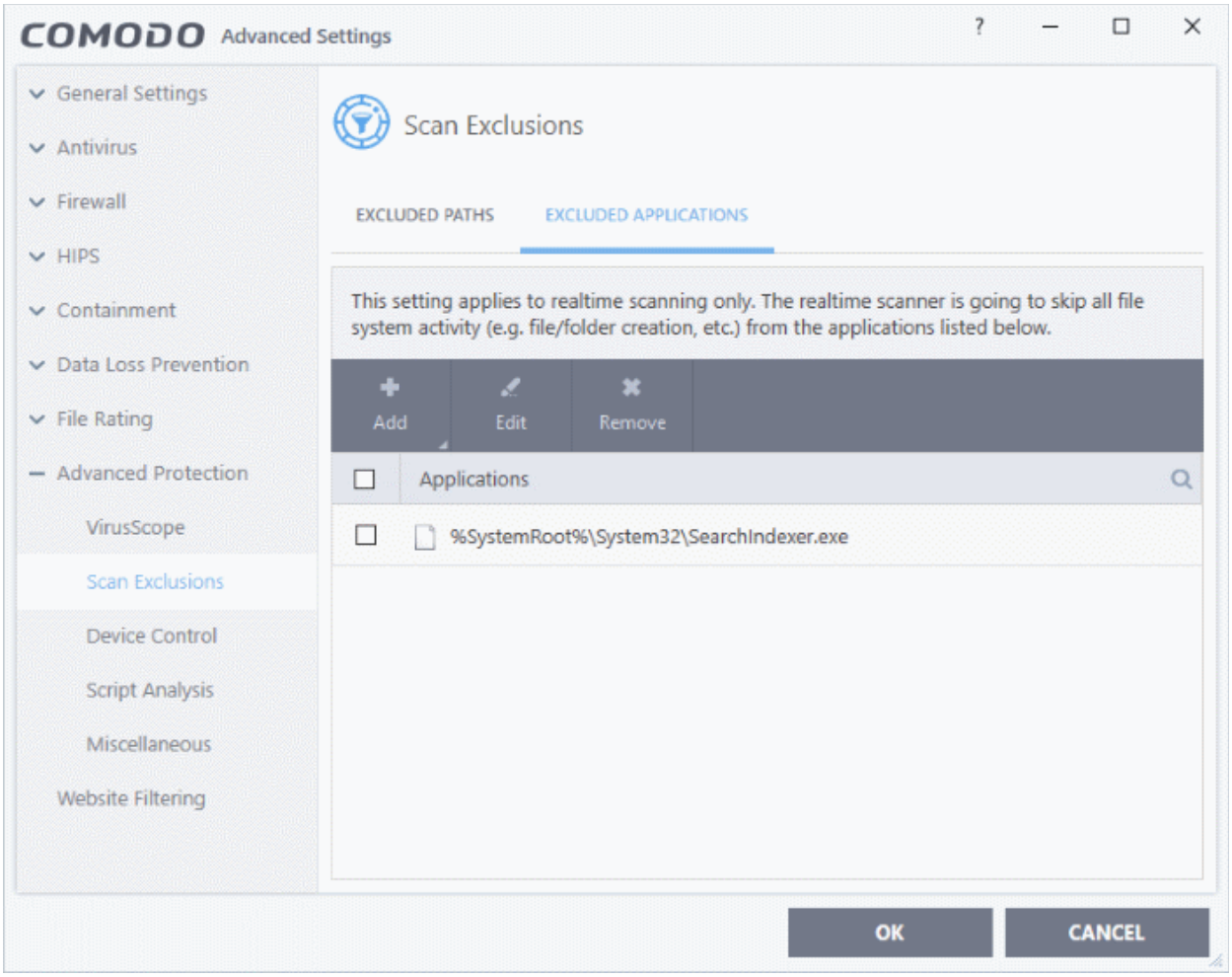
- Click 'OK' for your settings to take effect.

Exclude Programs/Applications from Real-time Scans

- The 'Excluded Applications' screen lets you specify programs which should be skipped by real-time virus scans.
- Applications which you chose to '**Ignore**' in an antivirus alert or in the **Scan Results** window are automatically added to this list.
- You can manually add and remove programs to/from the list as required

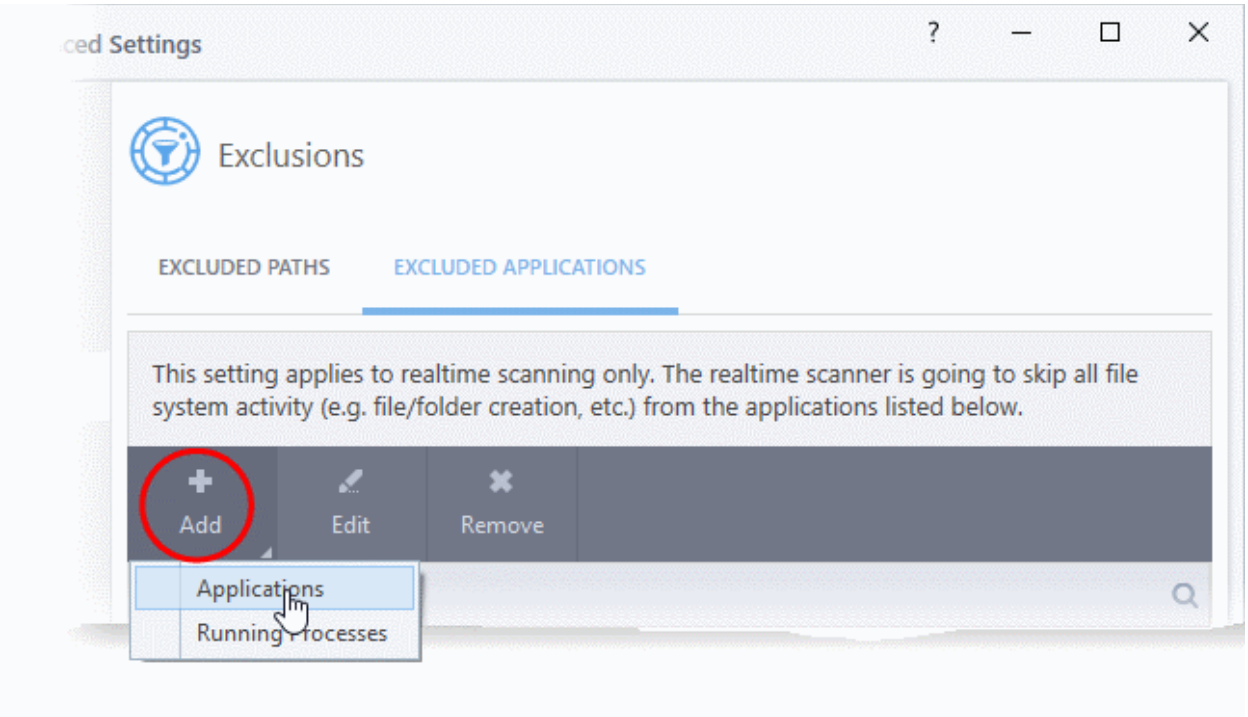
Open 'Excluded Applications' pane

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab:



Add an item to excluded applications

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab
- Click 'Add' at the top of the 'Excluded Applications' pane.

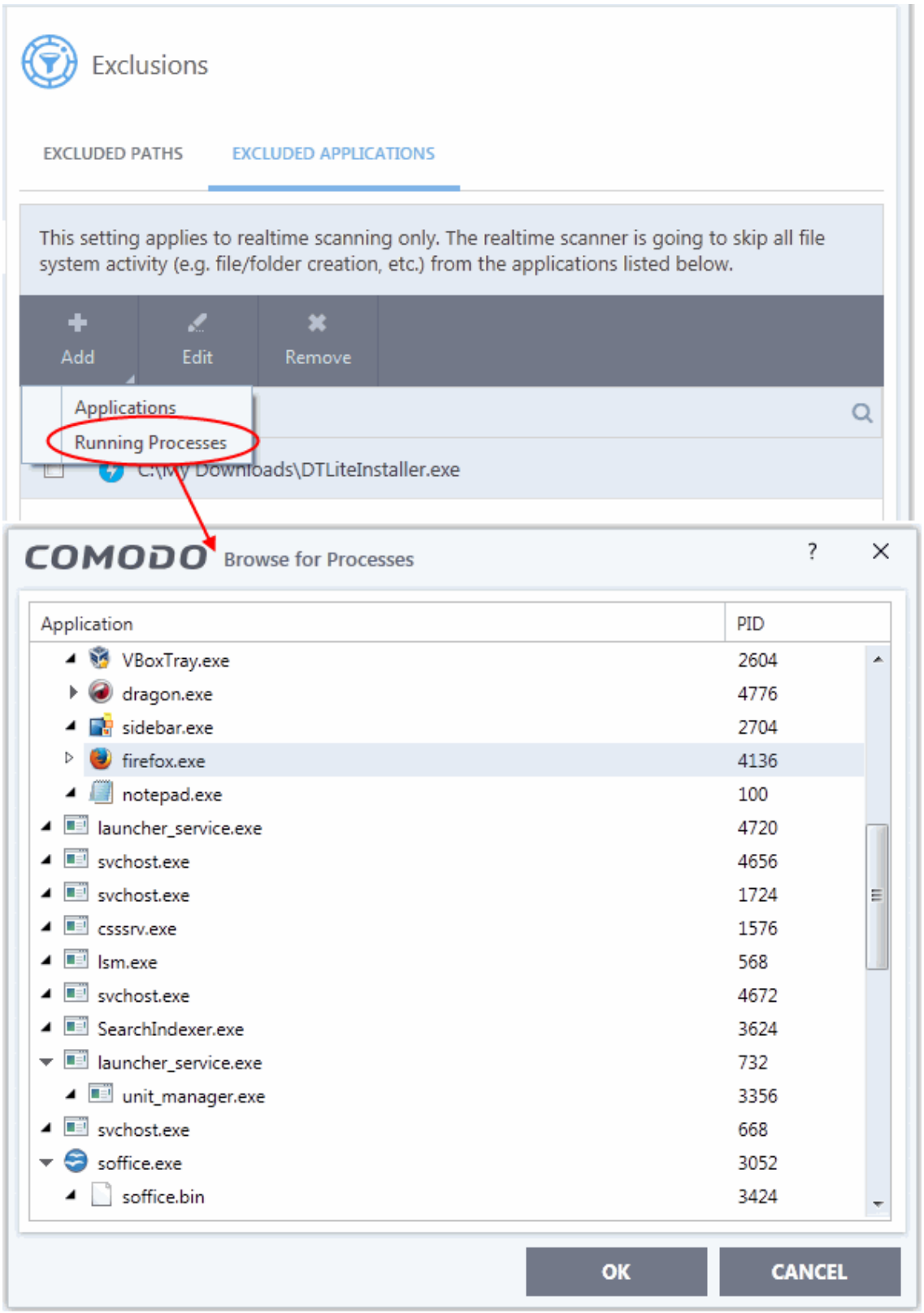


You can choose to add an applications by:

- **Selecting it from the running processes** - This option allows you to choose the target application from the list of processes that are currently running on your PC.
- **Browsing your computer for the application** - This option is the easiest for most users and simply allows you to browse to the files which you want to exclude.

Add an application from a running processes

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



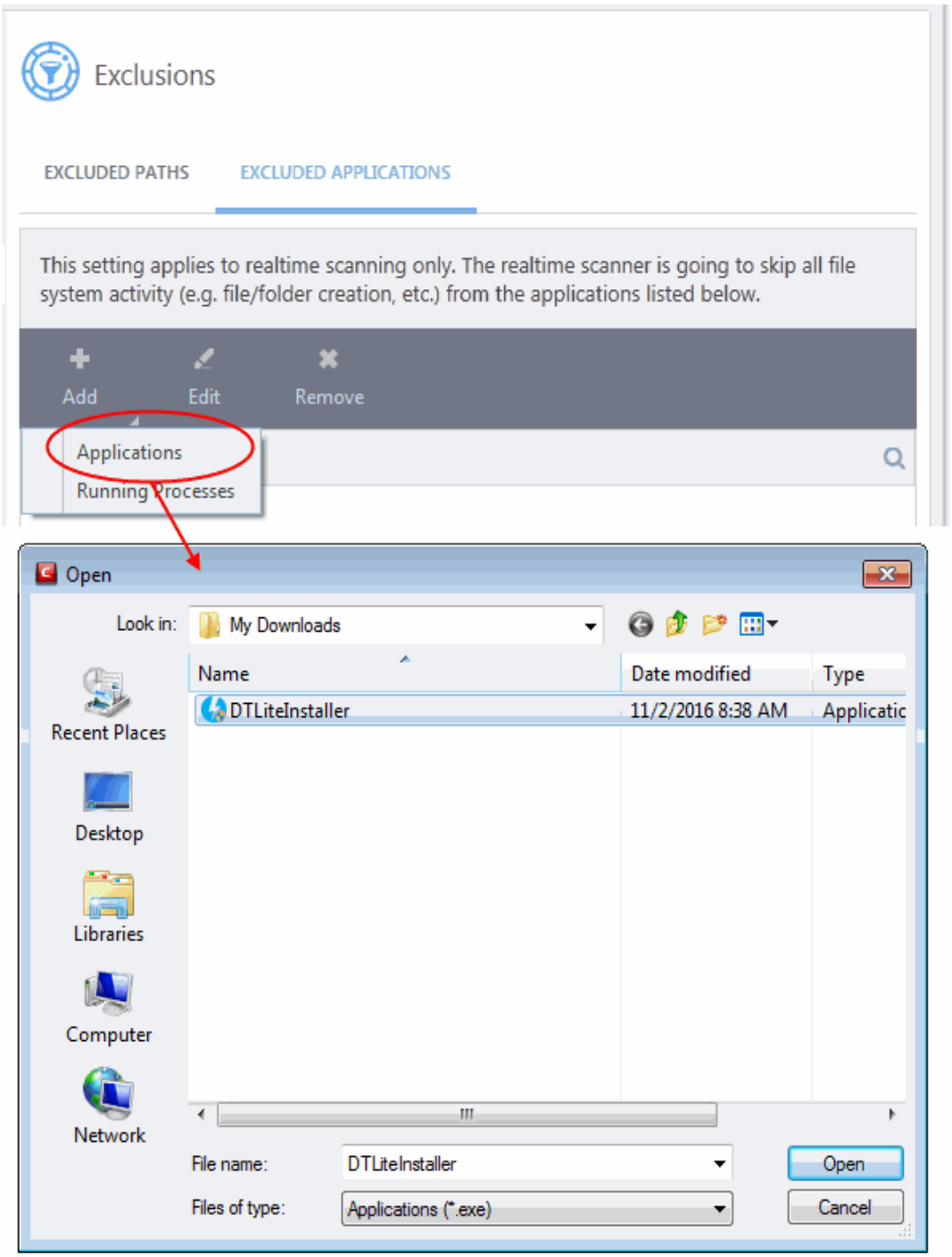
A list of currently running processes in your computer will be displayed:

- Select the process whose target application you wish to exclude and click 'OK':

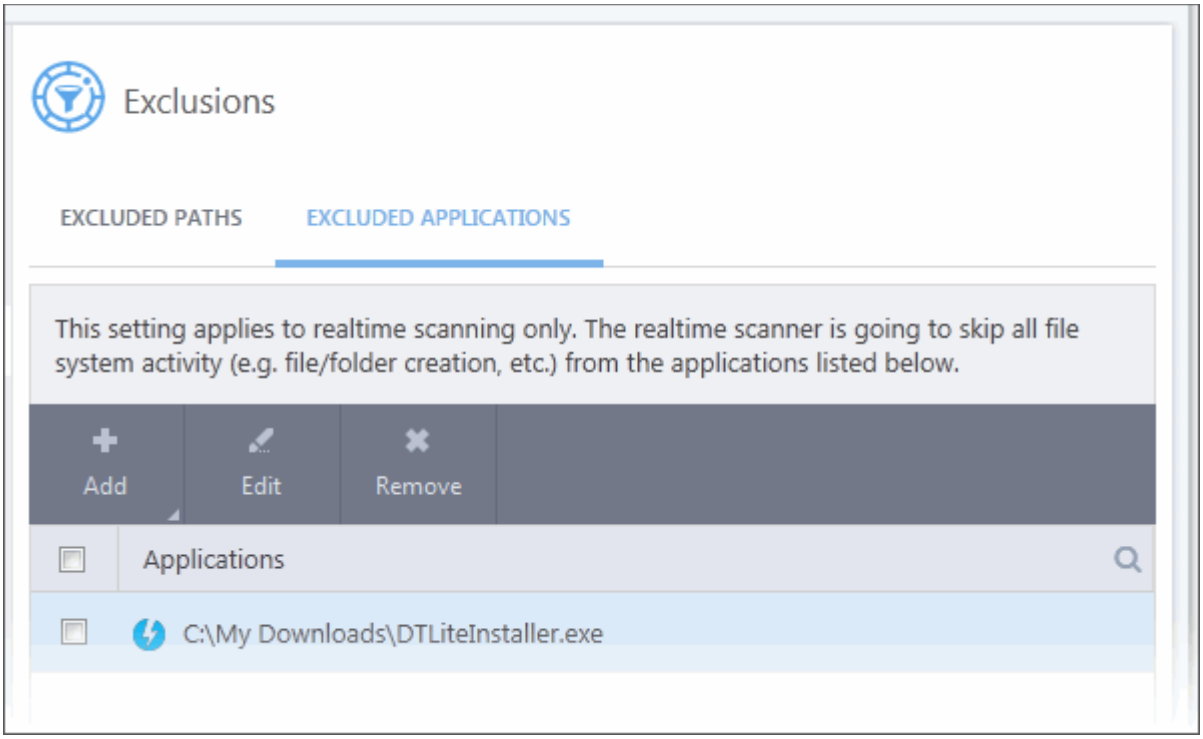
The application will be added to 'Excluded Applications'.

Browse to the Application

- Choose 'Applications' from the 'Add' drop-down



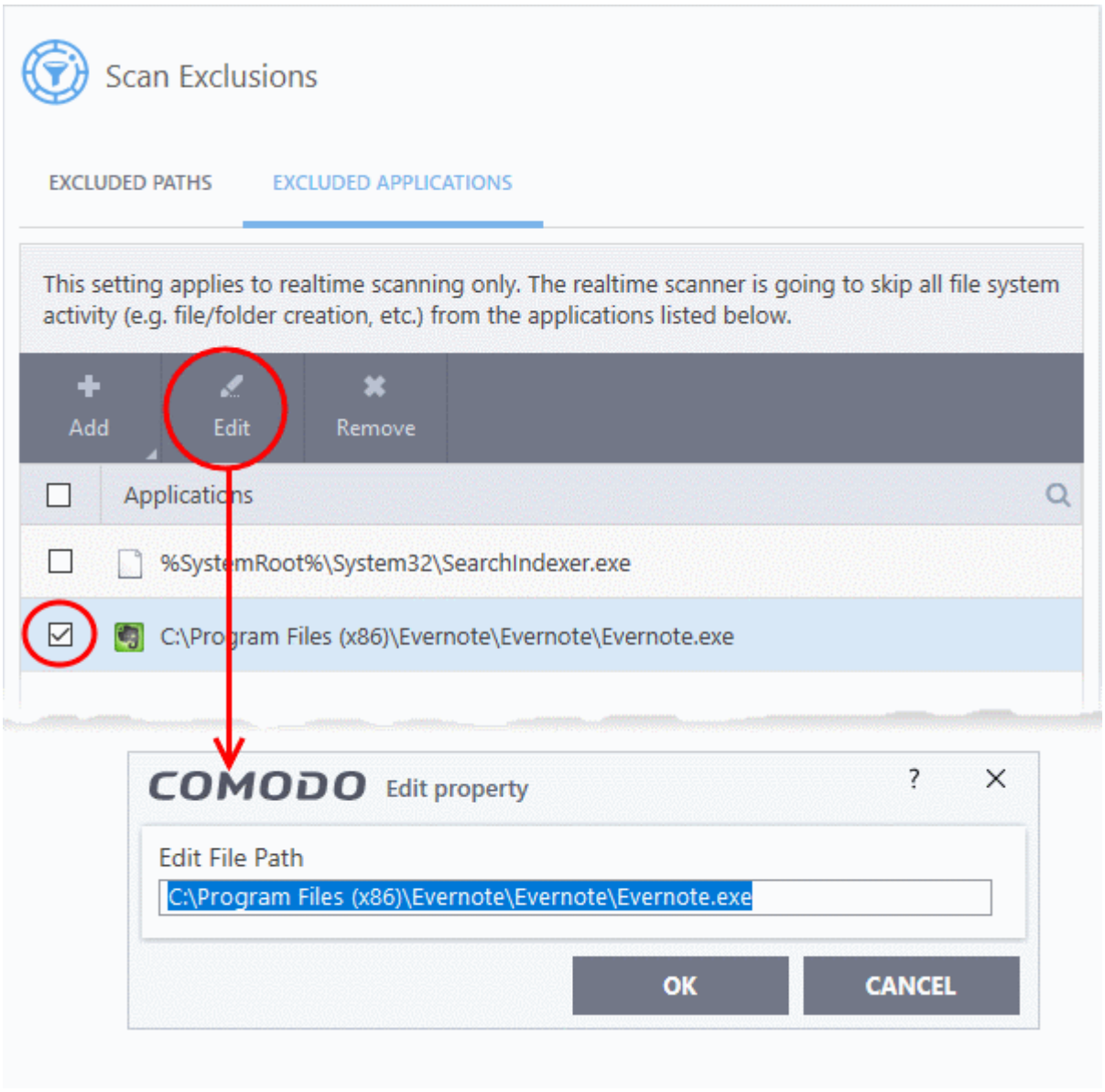
- Navigate to the file you want to exclude and click 'Open'.



- Repeat the process to add more items. Excluded items will be skipped from future real-time scans.

Edit the path of the application added to 'Excluded Applications'

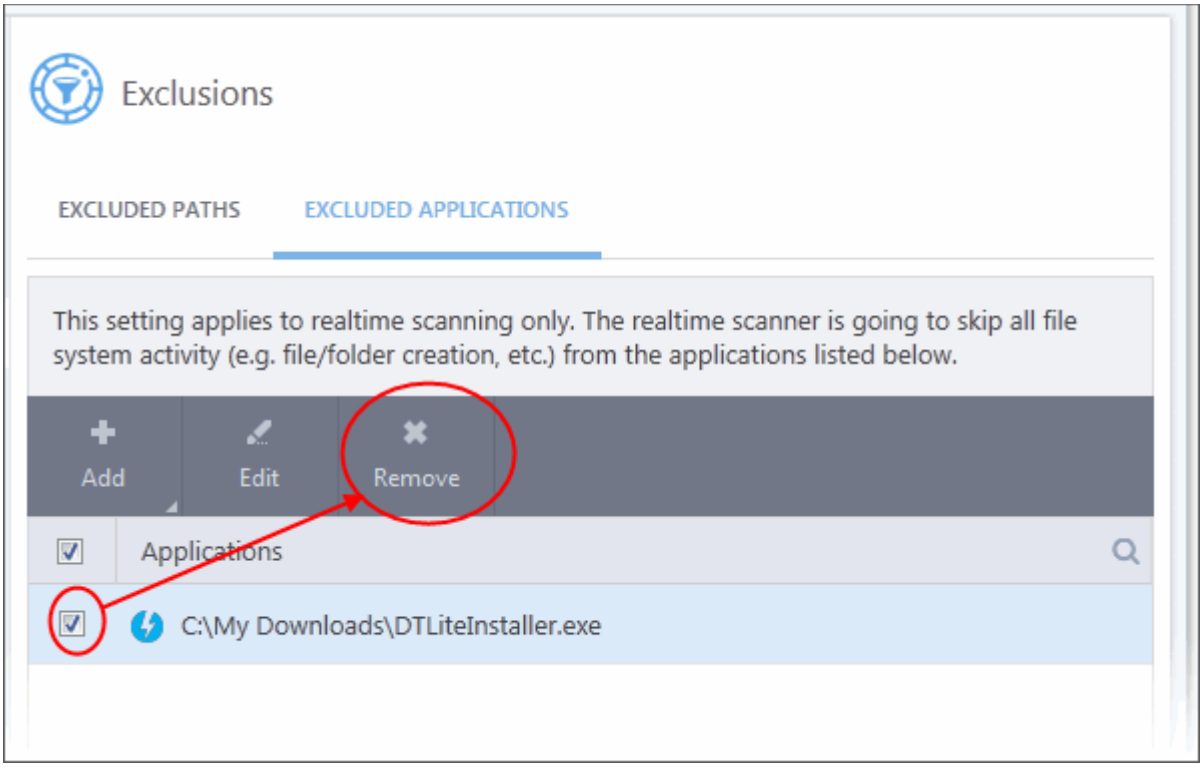
- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab
- Select the application and click 'Edit' at the top.
- Make required changes to the file path in the 'Edit Property' dialog.



- Click 'OK' to save your changes

Remove an item from the Excluded Applications

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Scan Exclusions'
- Open the 'Excluded Applications' tab
- Select the item and click 'Remove' at the top:



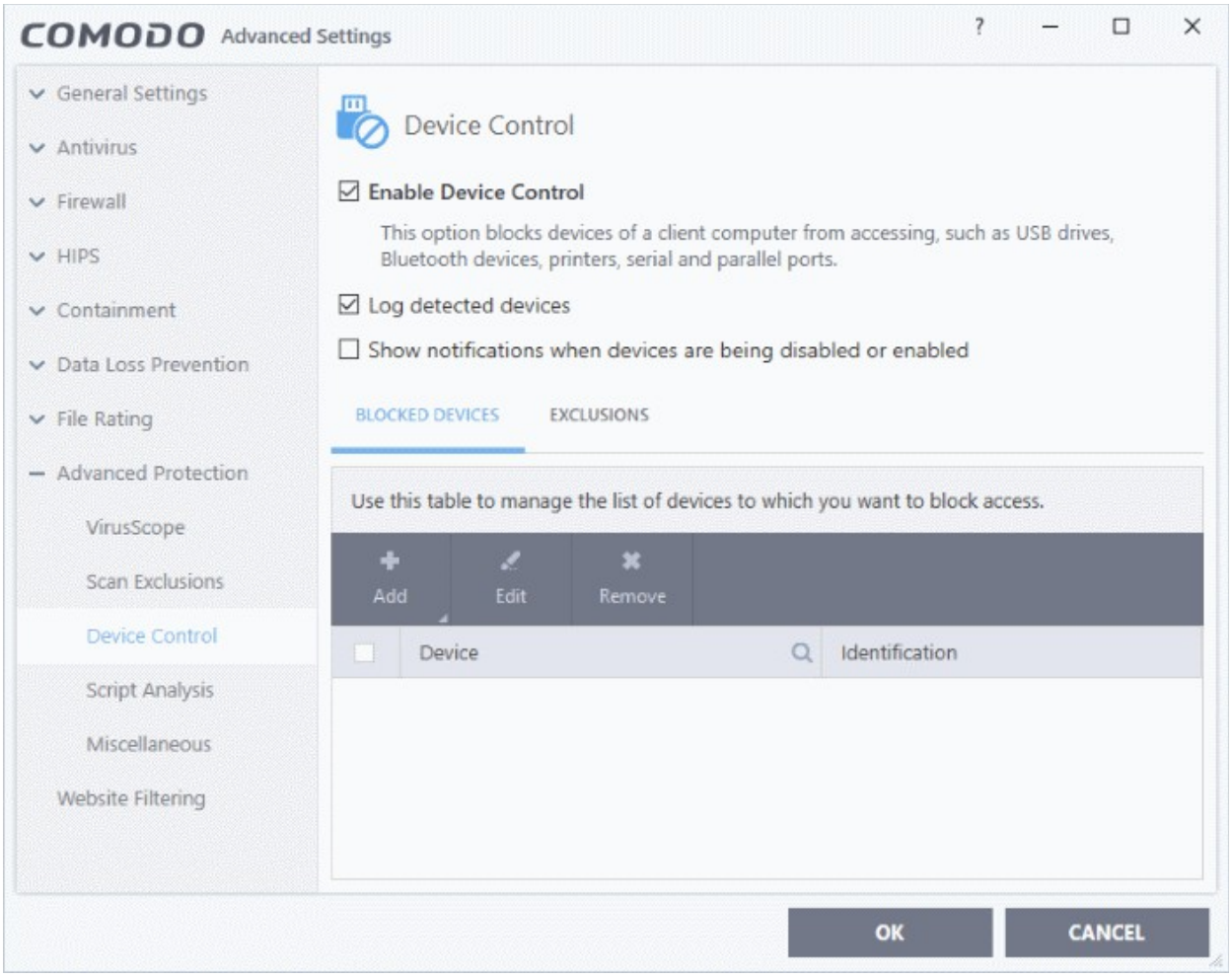
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

7.9.3. Device Control Settings

- Click 'Settings' > 'Advanced Protection' > 'Device Control'
- The 'Device Control' panel lets you specify types of external devices that are to be blocked and define exclusions to it

Open the Device Control panel

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'



- **Enable Device Control** - Activate the device control functionality to selectively prohibit access to external devices. You should specify devices to be banned in the 'Blocked Devices' pane. ***(Default = Enabled)***
- **Log Detected Devices** - CCS logs events like connection attempts of external devices ***(Default = Enabled)***
- **Show Notifications when devices are being disabled or enabled** - CCS displays an alert whenever an external device is connected or disconnected.***(Default = Disabled)***
- **Blocked Devices** - List of external device classes which are not allowed to connect to the endpoint. Example classes include 'USB Storage Devices', 'CD/DVD Drives', 'BlueTooth Devices' and 'Firewire Devices'.
- **Exclusions** - Add exceptions to a blocked class. For example, if you wish block the class 'USB Devices' but wish to allow access for your company's authentication tokens, then you should add those USB tokens as exceptions.

Click the following links for more information on blocked devices and exclusions:

- **Block devices**
- **Specify exclusions**

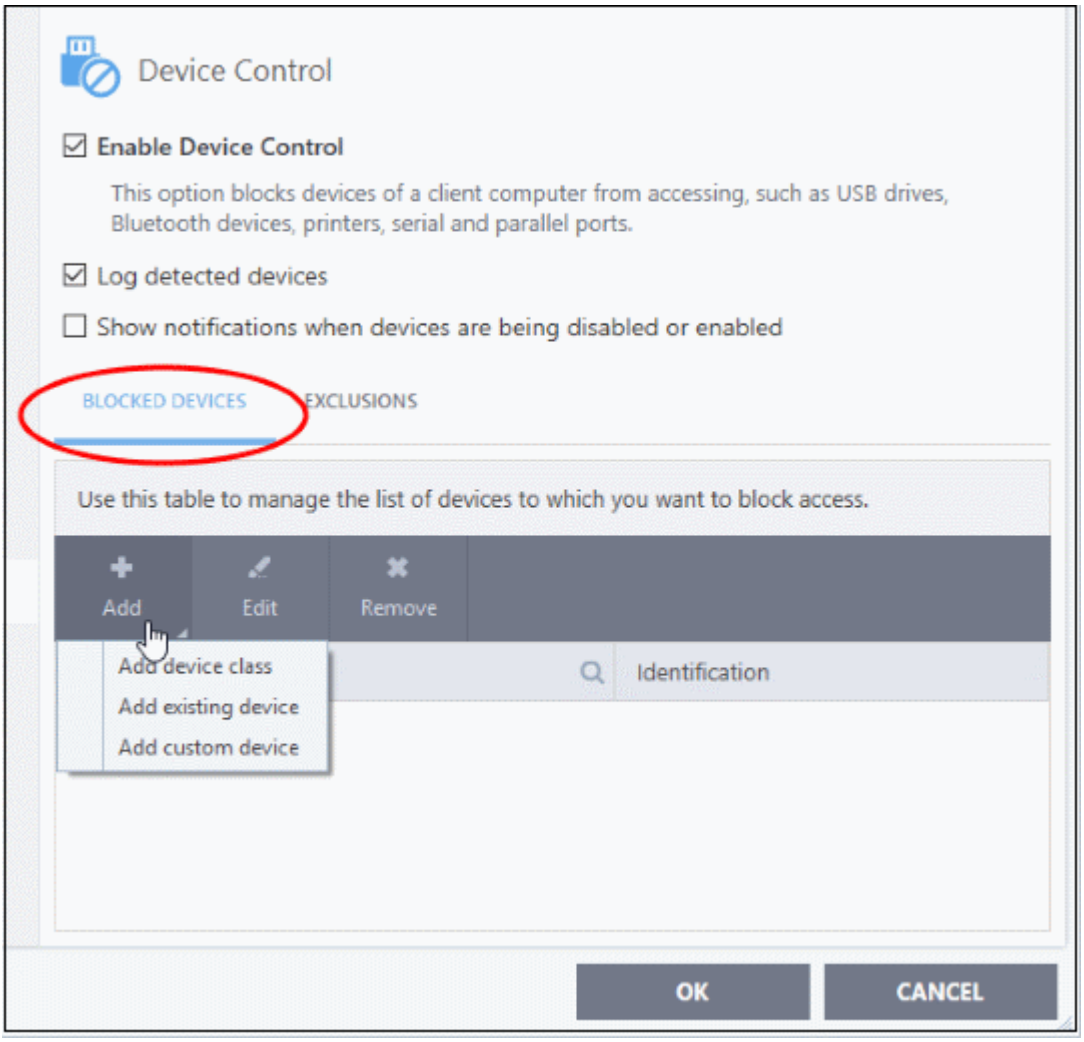
Block Devices

You can specify devices to be blocked in three ways:

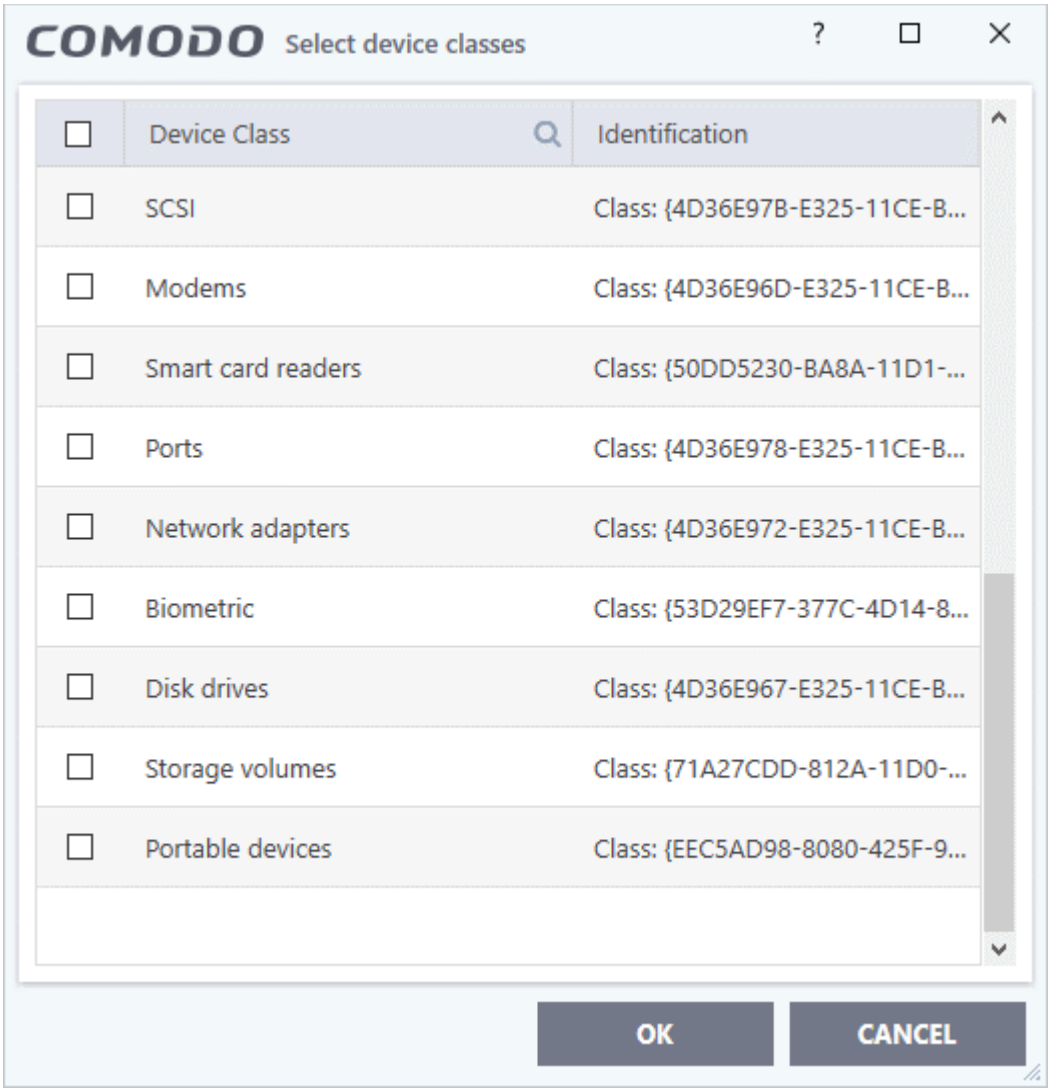
- **Select device classes**
- **Select from currently connected devices**
- **Specify custom devices**

Block a device class

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button
- Click 'Add device class' from the options:



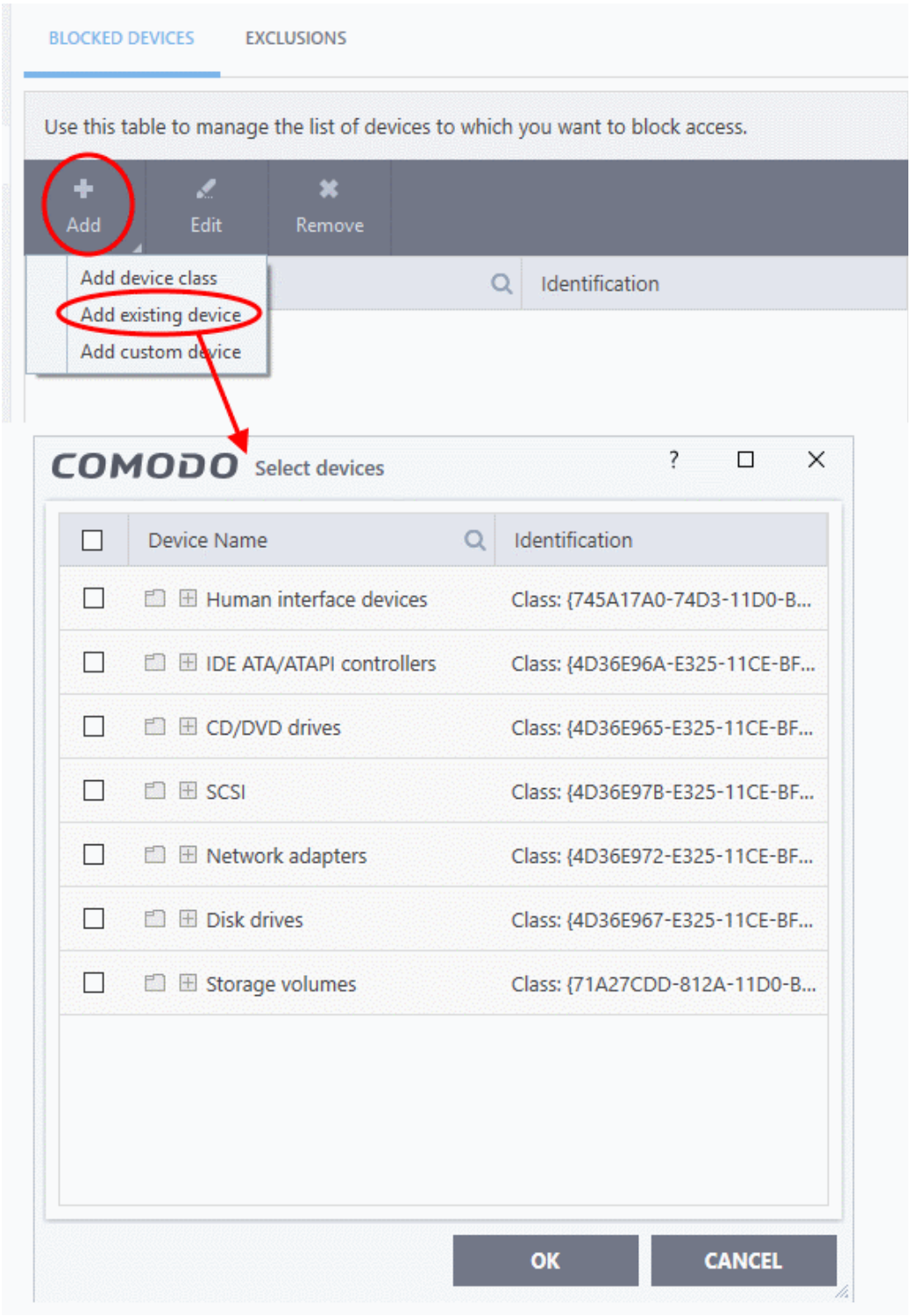
- Choose the device class you wish to block.
  - For example, to block all USB devices that are plugged to your computer, select "Portable devices" from the list
  - If you want to exclude any specific device from this class, enter the device name in the exclusion list.



- Select the device(s) you wish to block
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

Select devices from currently connected devices

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button
- Click 'Add existing device' from the options

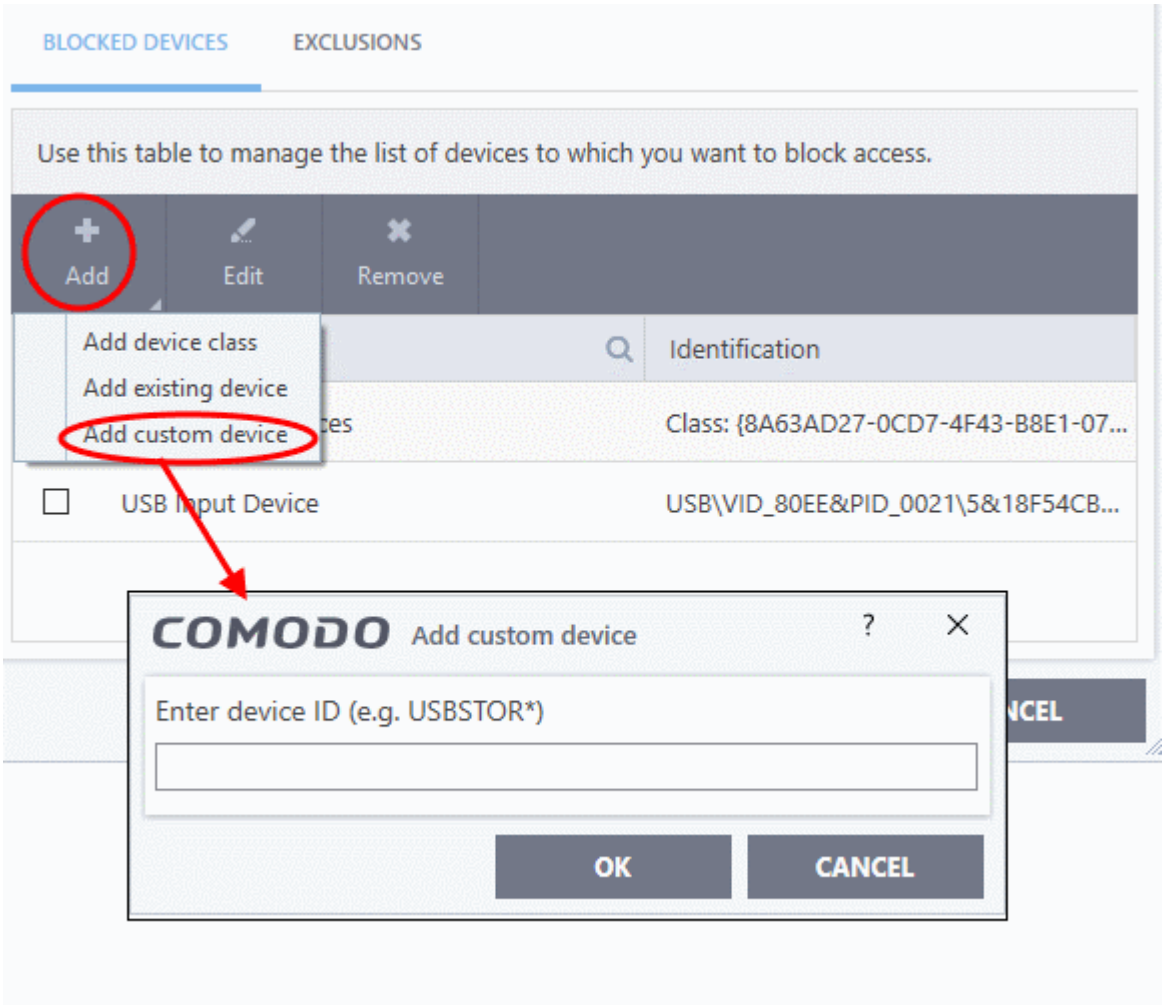


- Choose the device class you wish to block. For example, Network adaptor devices, CD/DVD drives, Storage devices or Disk drives.
- Click the '+' sign of the class to which your device belongs
- Select the device(s) you wish to block
- Click 'OK' and again click 'OK' in the 'Device Control' panel to save your settings.

Specify a custom devices to be blocked

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Blocked Devices' tab then click the 'Add' button

- Click 'Add custom device' from the options



- Enter the device ID and click 'OK'

Specify exclusions

The 'Exclusions' tab lets you allow access to specific devices that fall within a blocked device class.

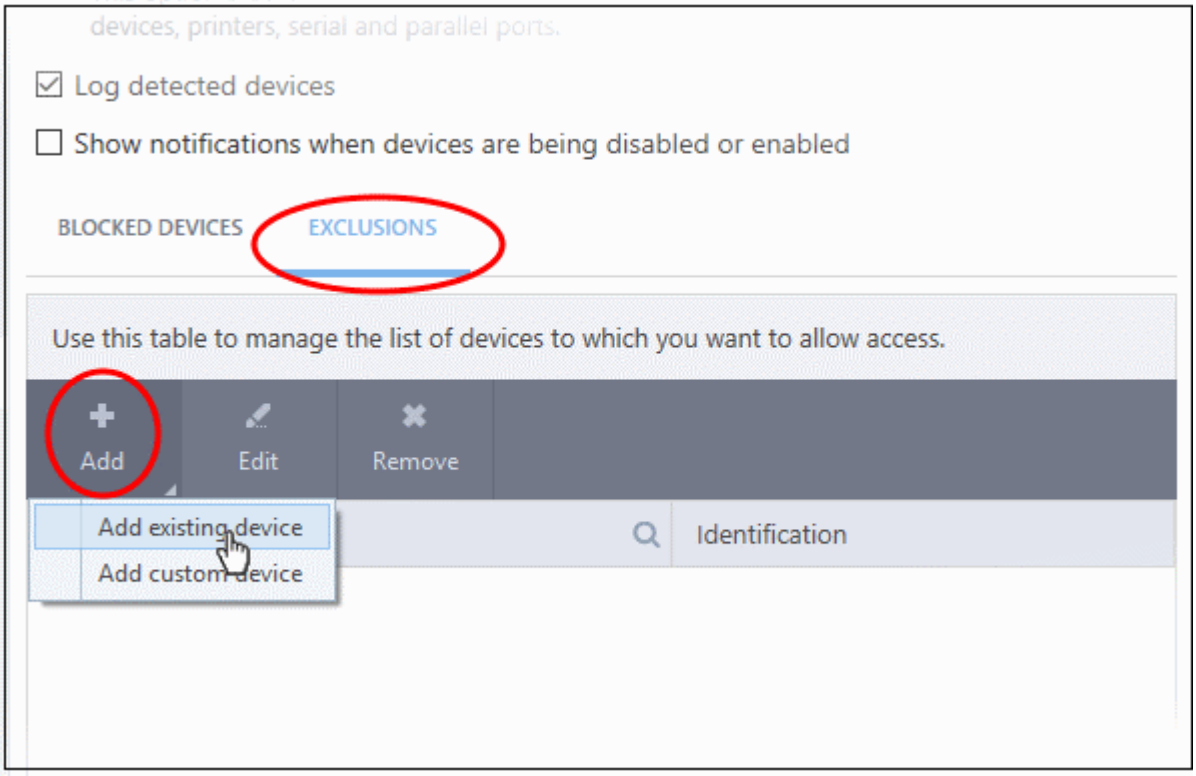
You can specify the exceptions in two ways:

- **Select from currently connected devices**
- **Specify a custom device**

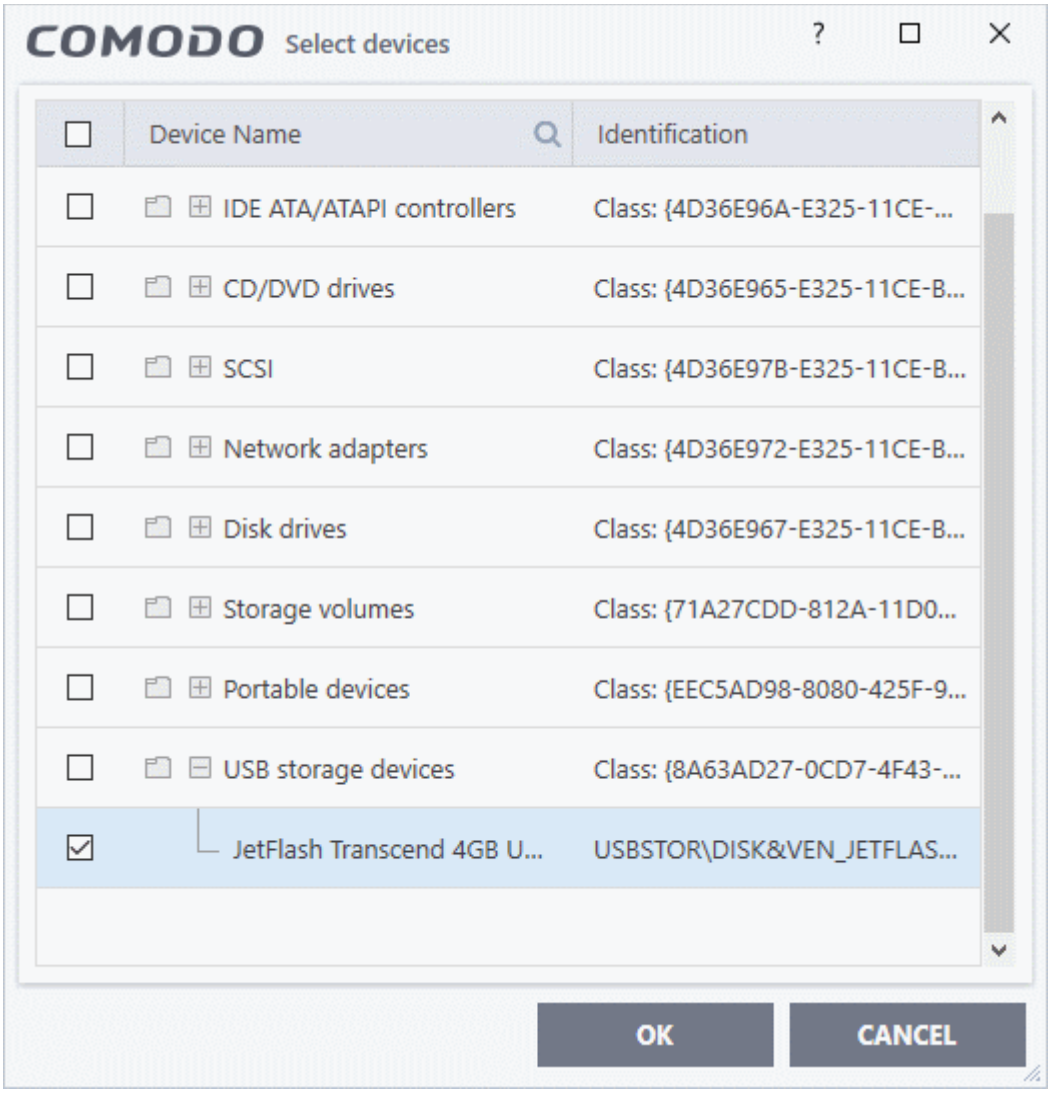
Add exclusions from currently connected devices

You need to add the device to the exclusion list before blocking the device class.

- Make sure the external device is connected to the computer
- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Exclusions' tab then click the 'Add' button



- Select 'Add existing device' from the options



- Click the '+' sign of the class to which your device belongs
- Select the device(s) you wish to exclude

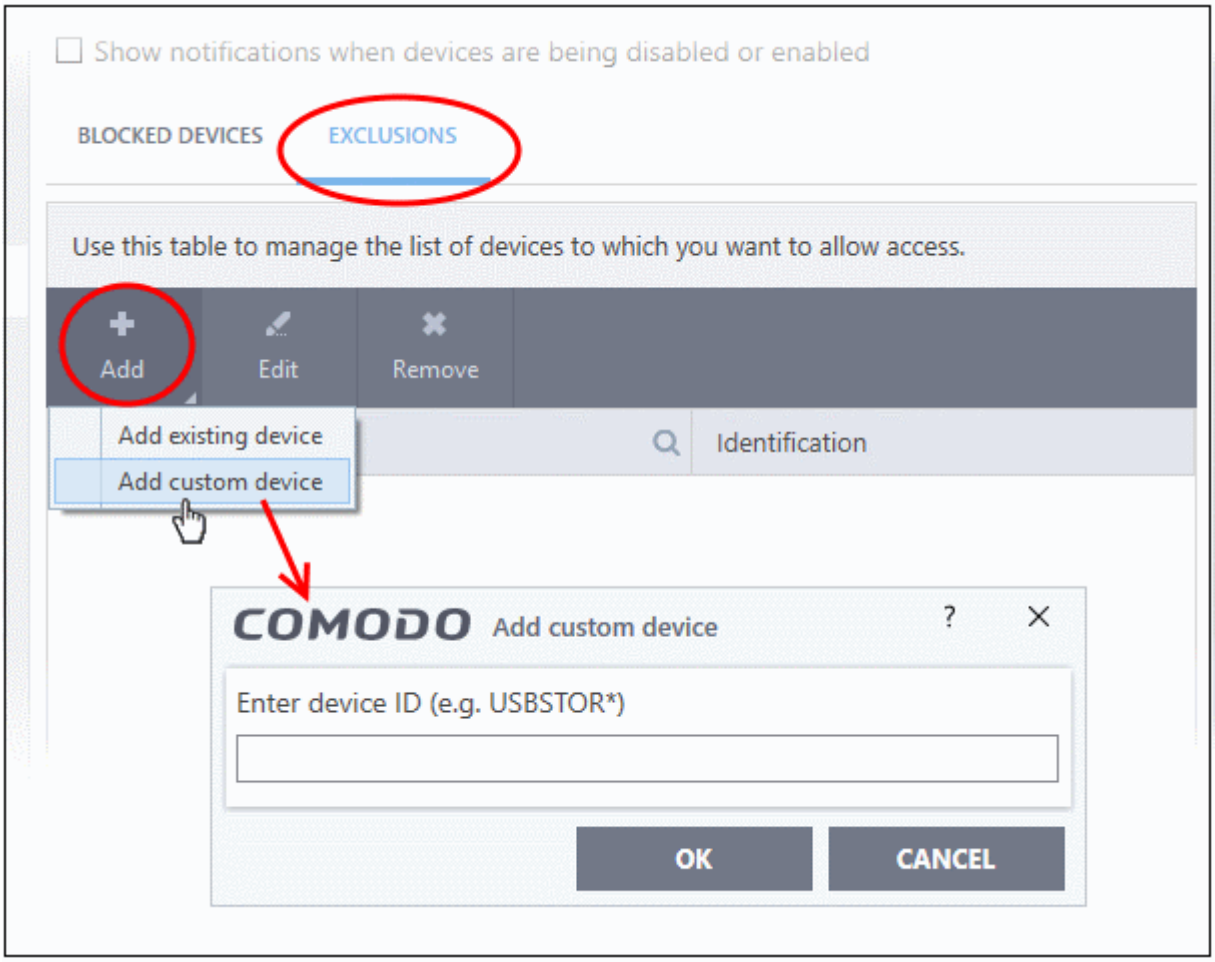
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

Add custom device to be excluded

- You can also add exclusions by specifying the device Ids.
- For example, you want to block all USB storage devices apart from the type of SANDISK devices used by your company, you could specify a device exclusion ID of 'USBSTOR\DISK&VEN_SANDISK\4C5310*'.
- You can also use the wildcard character - ' * ' to cover a range of devices

Specify custom devices to be excluded

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Device Control'
- Open the 'Exclusions' tab then click the 'Add' button
- Select 'Add custom device' from the options



- Enter the unique device identifier in the 'Device ID' field, for example to exclude all USB storage devices whose device IDs start with "4C5310", you could enter: USBSTOR\DISK&VEN_SANDISK\4C5310*
- Click 'OK' in the screen and again 'OK' in the 'Advanced Settings' interface.

7.9.4. Script Analysis Settings

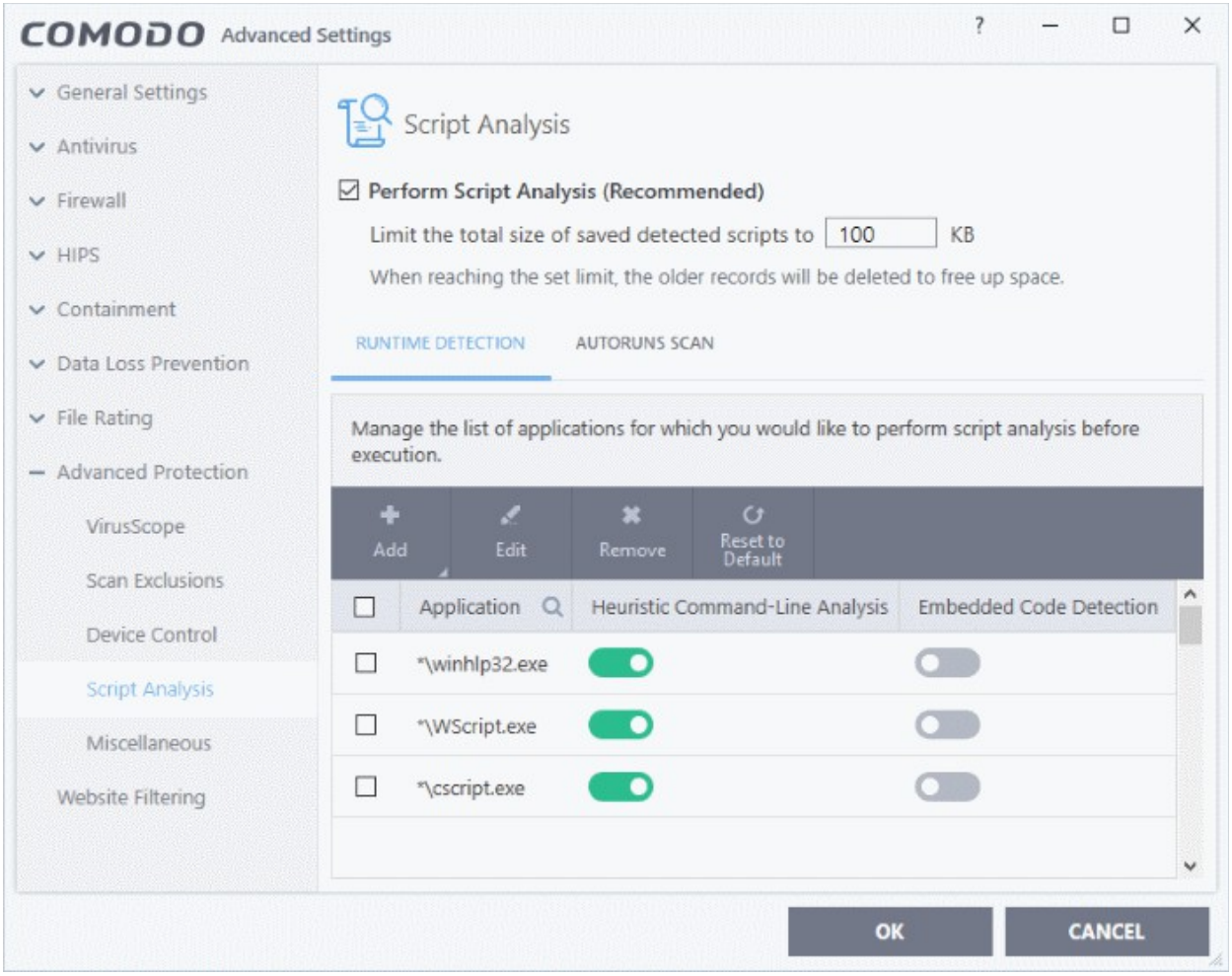
- Click 'Settings' > 'Advanced Protection' > 'Script Analysis'
- The script analysis settings panel lets you:

- Configure heuristic command line analysis for applications in real-time
- Configure heuristic command line analysis for auto-run entries. Auto-run entries include Windows services, auto-start items and scheduled tasks.

Background note: 'Heuristics' is a technology which analyzes a file to see if it contains code typical of a virus. Heuristics is about detecting 'virus-like' traits in a file. This helps to identify previously unknown (new) viruses.

Open the 'Script Analysis' settings panel

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Script Analysis'



- **Perform Script Analysis (Recommended)** - Enable / disable script analysis of managed applications ***(Default = Enabled)***
  - **Limit the total size of saved detected scripts to 'N' KB** - CCS stores the list of executing scripts that are run by the managed applications for analysis. This options allows you to specify the total size of the stored scripts. When the set limit is reached, the older scripts are deleted automatically.

The interface has two tabs:

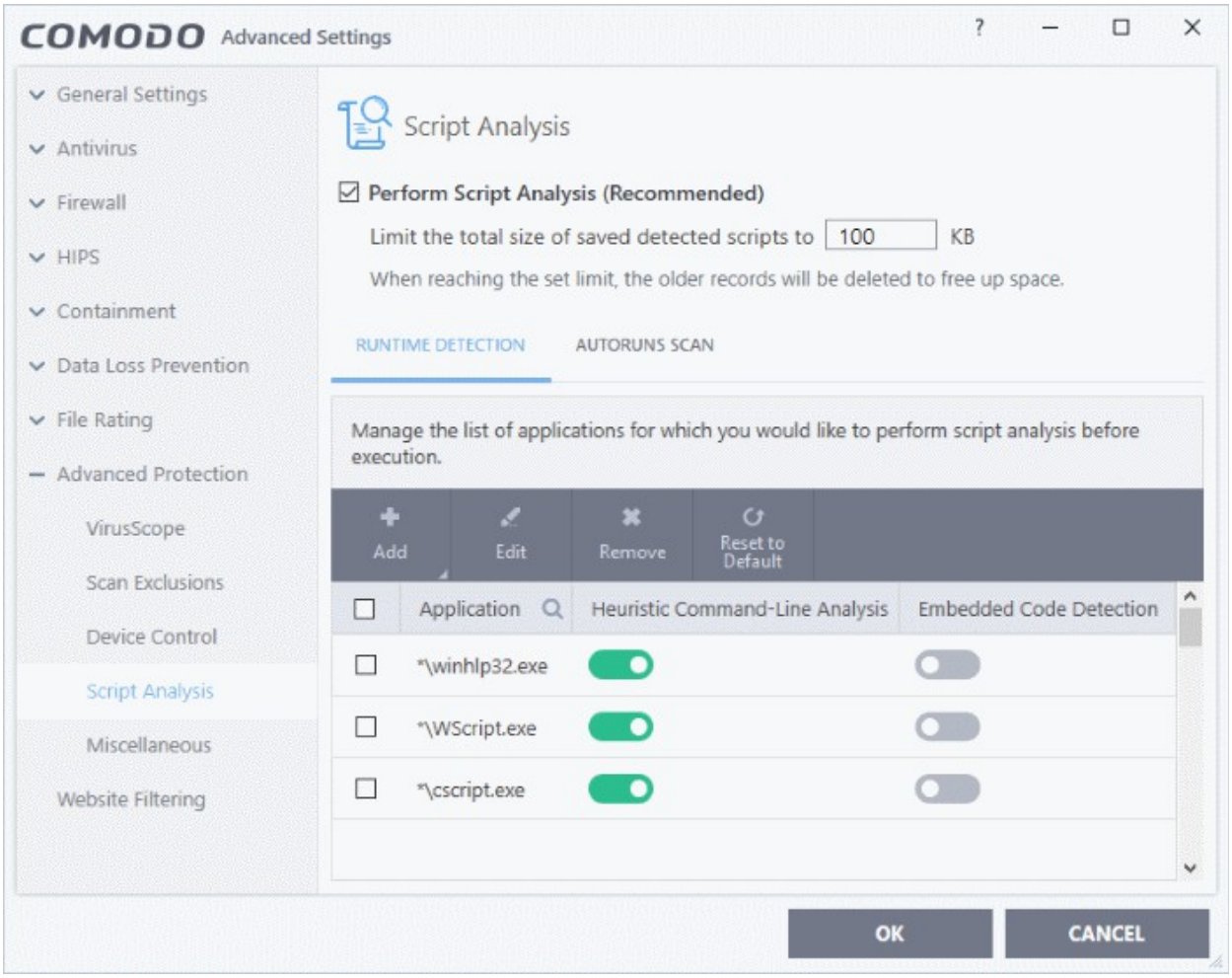
- **Runtime Detection**
- **Autoruns Scans**

Runtime Detection

CCS performs heuristic analysis on certain programs because they are capable of executing code. Example programs are wscript.exe, cmd.exe, java.exe and javaw.exe. Example code includes Visual Basic scripts and Java

applications.

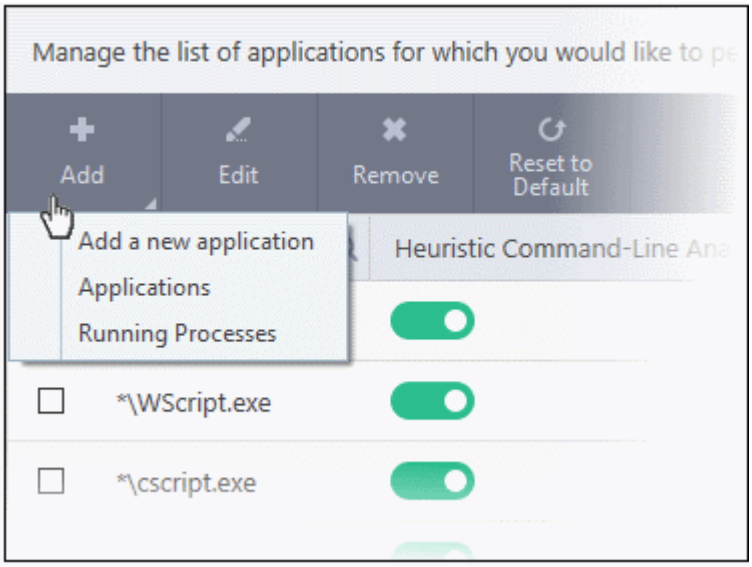
- For example, the program wscript.exe can be made to execute Visual Basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'.
- If this option is selected, CCS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the internet, for example, the alert will state 'test.vbs' is attempting to connect to the internet
- If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the internet'.
- Relevant settings are applied to the scripts. For example, if a script is detected by the containment module, then auto-containment rules are applied. Each module (AV, FW, VirusScope and so on) that detects a script will apply its appropriate settings.



Runtime Detection - Column Descriptions	
Column Header	**Description**
Application	Names of existing applications covered by this rule
Heuristic Command-Line Analysis	Enable or disable command line tracking
Embedded Code Detection	Enable or disable embedded code tracking

Manually add a new application to the list for analysis

- Click 'Add' at the top

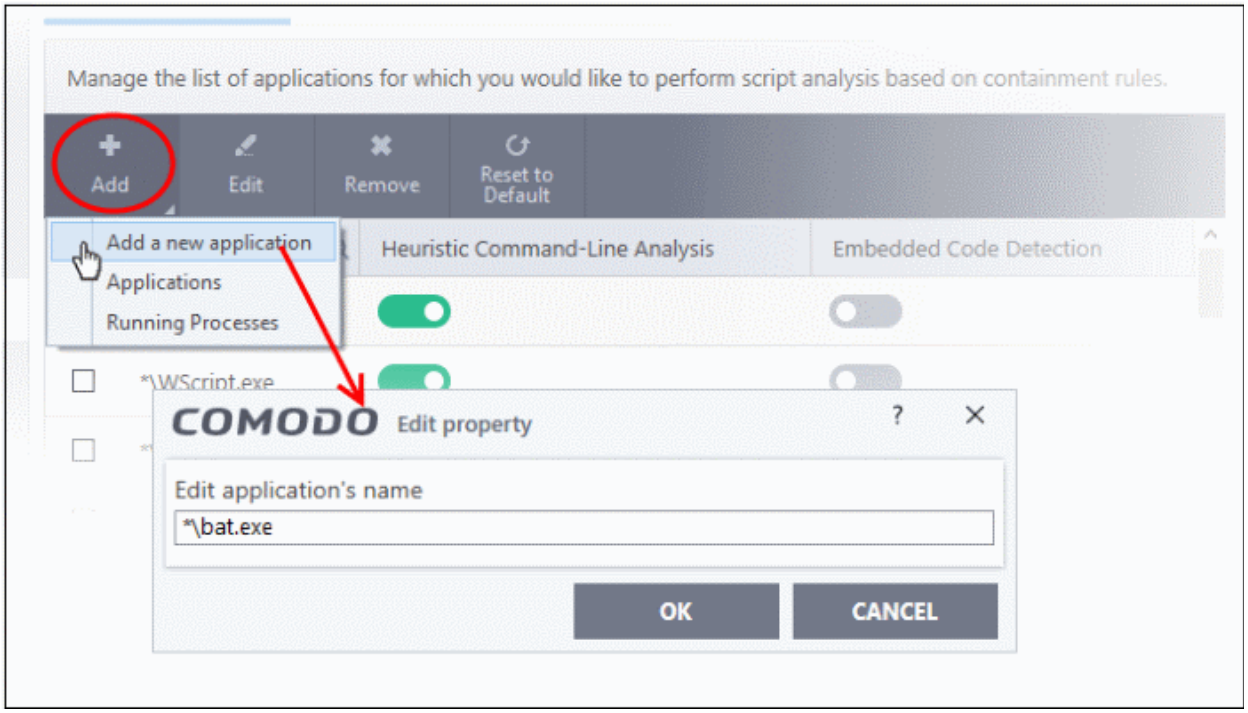


You can add an application by following methods:

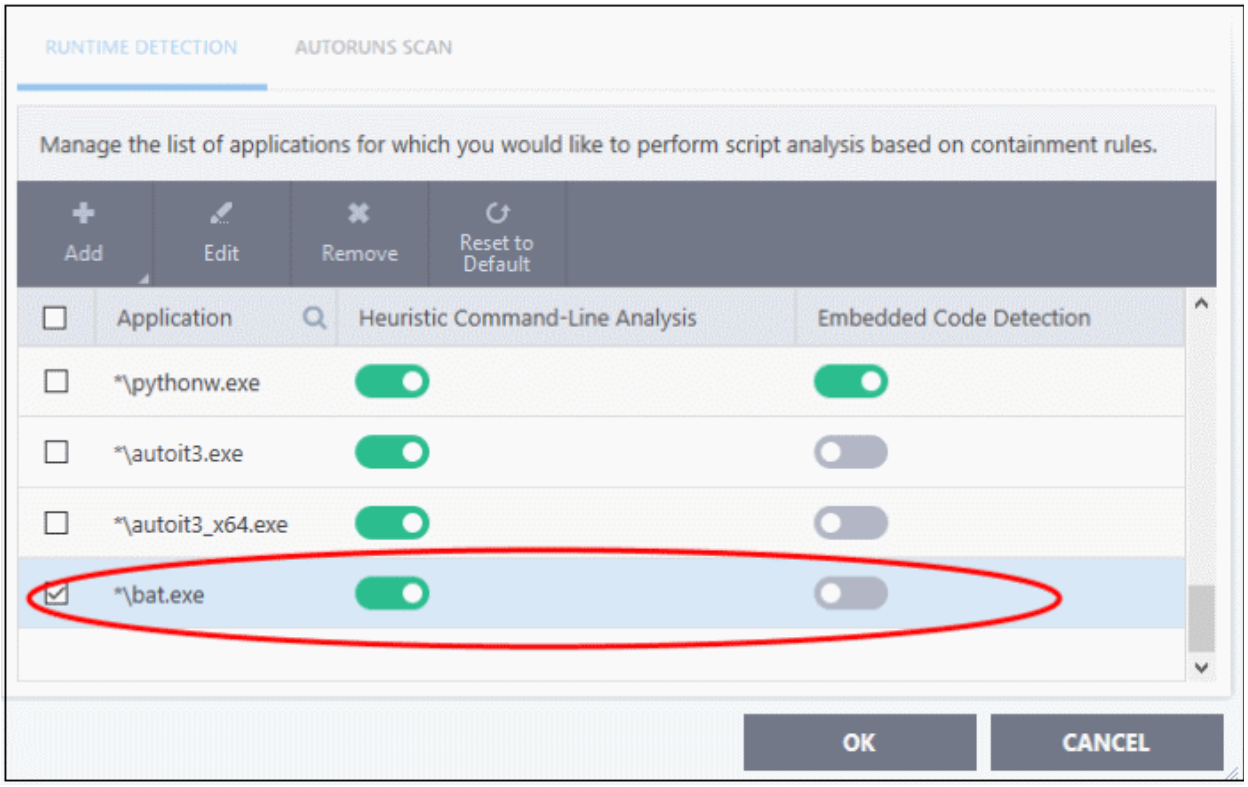
- **Add a new application**
- **Add a current application**
- **Add application from the currently running processes**

Add a new application

- Click 'Add new application' from the 'Add' drop-down
- Enter the file path in the 'Edit Property' dialog and click 'OK'



The application will be added and displayed in the list.



- Click "OK" to apply your settings

Add a current application

- Click 'Add' then 'Applications' from the drop-down
- Navigate to the file you want to add in the 'Open' dialog and click 'Open'
- The file will be added to the list
- Click "OK" to apply your settings

Add a currently running processes

- Choose 'Running Process' from the 'Add' drop-down
- A list of currently running processes in your computer will be displayed
- Select the process whose parent application you wish to add for analysis
- Click 'OK' from the 'Browse for Process' dialog
- The application will be added to the list
  - Use the slider beside the applications to enable/disable them for analysis.
  - Click the 'Edit' button to update the details of an application.
  - To remove an application, select it from the list and choose 'Remove' at the top.
  - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

Autoruns Scans

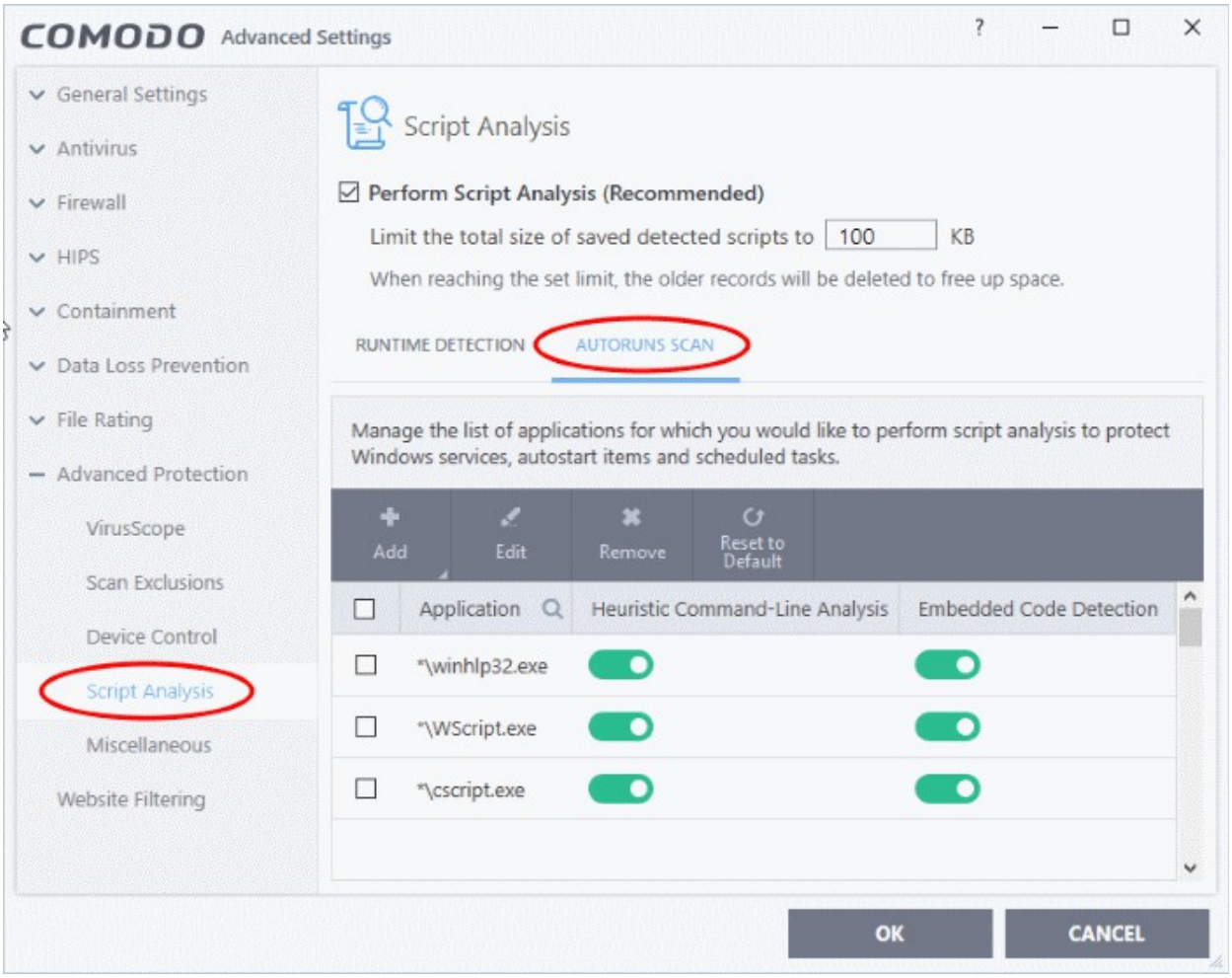
- Add and manage applications for which you want to perform heuristic command-line analysis and embedded code detection in order to protect Windows services, autostart items and scheduled tasks.
- CCS ships with a list of predefined applications for which it performs heuristic analysis on programs that are capable of executing code.
- The applications added here are applicable for the settings in:
  - '**Scan Options**' > '**Apply this action to suspicious autorun processes**' (monitors only during on-

demand scans)

- 'Advanced Settings' > '**Miscellaneous**' > '**Apply the selected action to unrecognized autorun entries related to new/modified registry items**' (monitors constantly)

Open the 'Autoruns Scans' interface

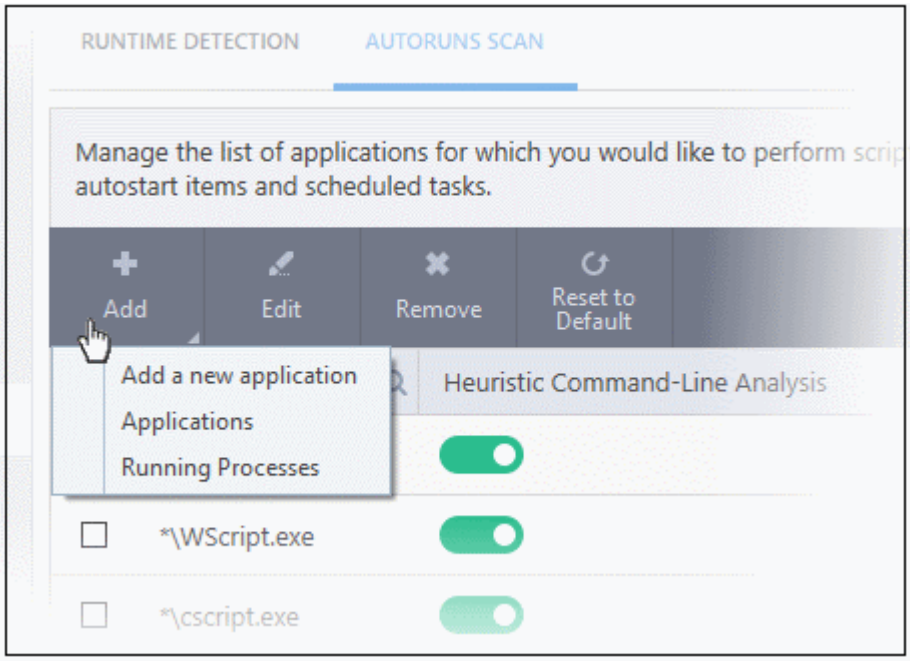
- Click 'Settings' on the CCS home screen.
- Click 'Advanced Protection' > 'Script Analysis'



Autroruns Scans - Column Descriptions	
Column Header	**Description**
Application	Names of existing applications covered by this rule
Heuristic Command-Line Analysis	Enable or disable command line tracking
Embedded Code Detection	Enable or disable embedded code tracking

To manually add a new application to the list for analysis

- Click 'Add' at the top

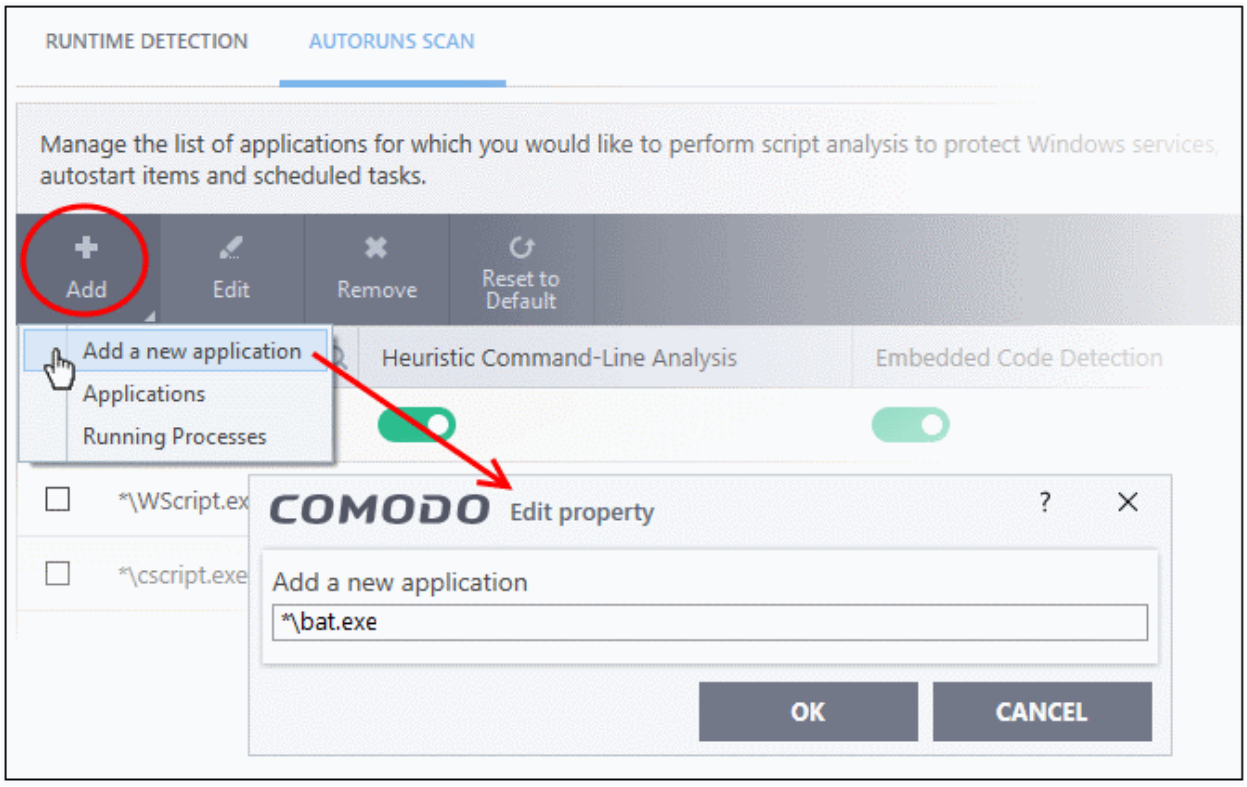


You can add an application by following methods:

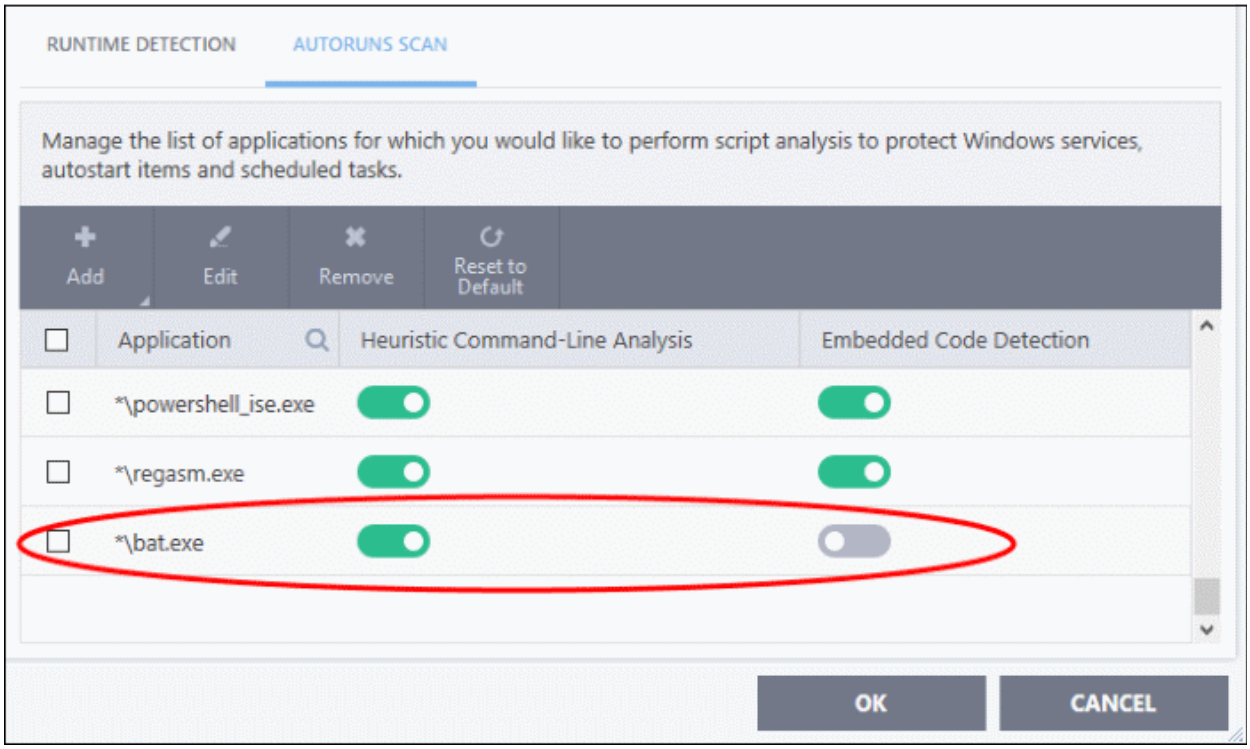
- **Add a new application**
- **Add a current application**
- **Add application from the currently running processes**

Add a new application

- Click 'Add new application' from the 'Add' drop-down
- Enter the file path in the 'Edit Property' dialog and click 'OK'



The application will be added and displayed in the list.



- Click "OK" to apply your settings

Add an application

- Click 'Add' then 'Applications' from the drop-down
- Navigate to the executable 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 a currently running process

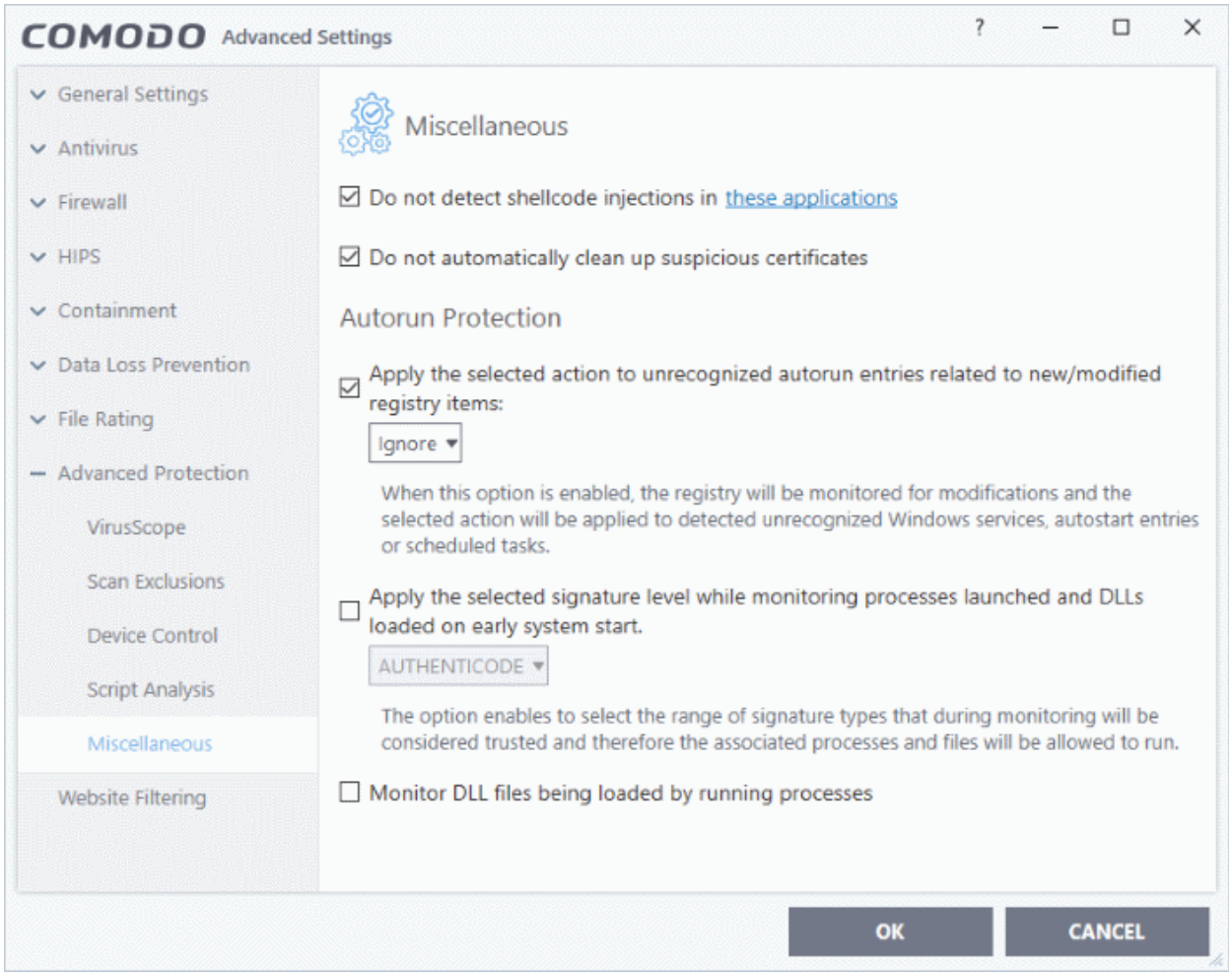
- Choose 'Running Process' from the 'Add' drop-down
- A list of currently running processes in your computer will be displayed
- Select the process whose parent application you wish to add for analysis
- Click 'OK' from the 'Browse for Process' dialog
- The application will be added to the list
  - Use the slider beside the applications to enable/disable them for analysis.
  - Click the 'Edit' button to update the details of an application.
  - To remove an application, select it from the list and choose 'Remove' at the top.
  - To reset to default applications for analysis, click 'Reset to Default' at the top.
- Click 'OK' at the bottom to apply your changes.

7.9.5. Miscellaneous Settings

- Click 'Settings' > 'Advanced Protection' > 'Miscellaneous'
- The miscellaneous settings panel lets you:
  - Configure protection against shellcode injections (buffer overflow attacks)
  - Skip automatic cleanup of suspicious certificates.
  - Configure protection settings for auto-start entries and scheduled tasks

Open 'Miscellaneous' settings:

- Click 'Settings' on the CCS home screen
- Click 'Advanced Protection' > 'Miscellaneous'



This interface allows you to:

- **Disable shellcode injection detection for certain applications**
- **Skip automatically clean-up of suspicious certificates**
- **Define actions to be taken on unrecognized auto-start entries/scheduled tasks**
- **Specify the signature level for monitoring processes launched and DLL's loaded during system start-up**
- **Enable or disable monitoring DLL files loaded to memory by currently running processes**

Disable shellcode injection detection

By default, protection against shellcode injection is enabled for all applications on your computer. Use this setting to define applications which you ***do not*** want to monitor for shellcode injections.

Background:

- Shellcode injection is a malicious technique which allows an attacker to cause a buffer overflow on your system.
- A buffer is an area of memory designed to hold a specific amount of data. A buffer overflow occurs when a process stores data beyond the boundaries of this fixed-length buffer.
- The result is that the extra data overwrites adjacent memory locations. The overwritten data may include

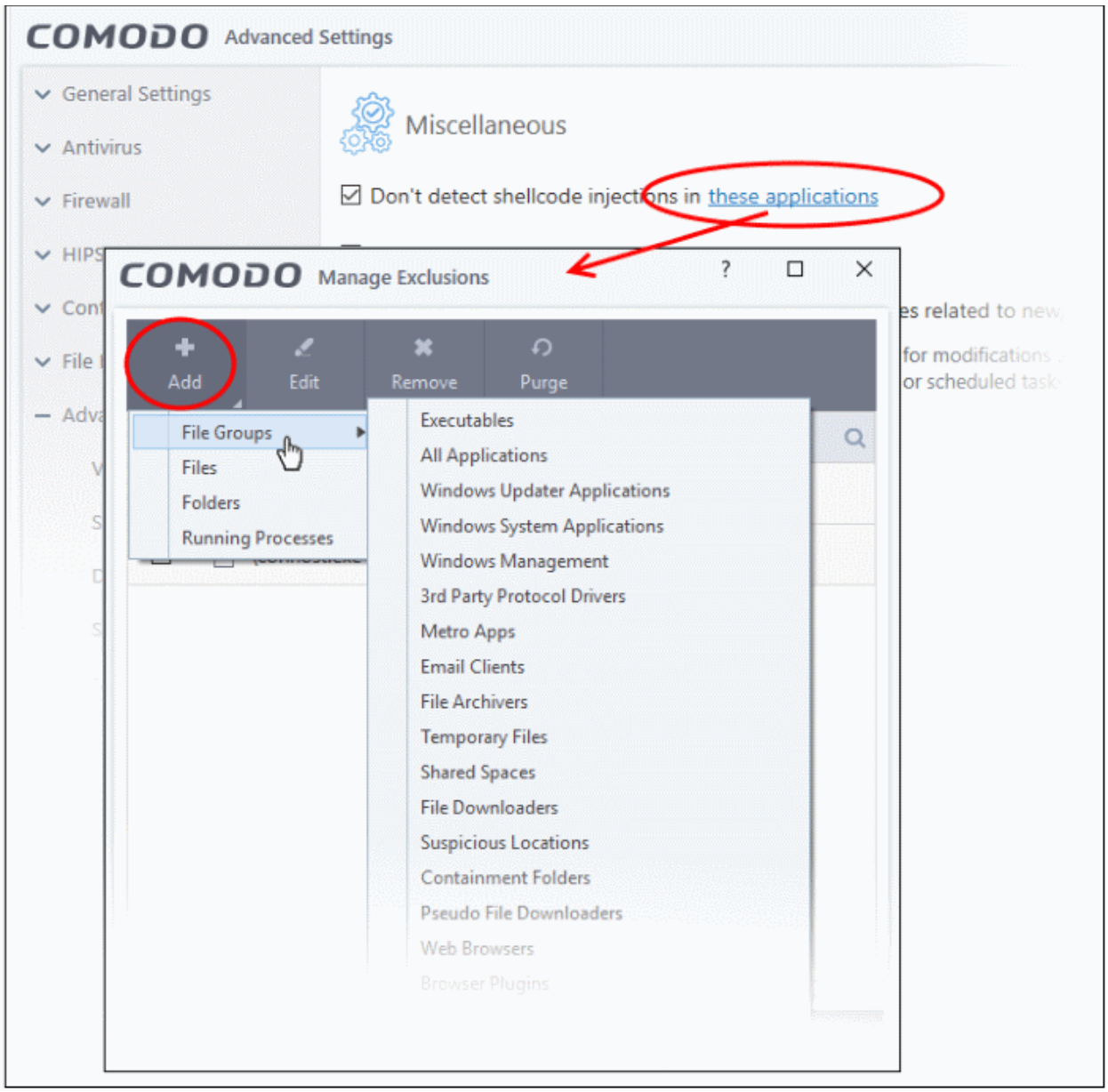
other buffers, variables and program flow data.

- Malware can deliberately cause buffer overflows in order to run malicious code or make the program operate incorrectly.

Exclude certain applications from shellcode injection protection

- Make sure 'Don't detect shellcode injections in these applications' is enabled then click the 'these applications' link. The 'Manage Exclusions' dialog appears.
- Click the 'Add' button at the top

You can add items by selecting the required option from the drop-down:



- **File Groups** - Select a category of pre-set files or folders. For example, 'Executables' lets you create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl, *cmd.exe *.bat, *.cmd. Other categories available include 'Windows System Applications', 'Windows Updater Applications', 'Start Up Folders' etc. See **File Groups**, for more details on file groups.
- **Running Processes** - Select an application or executable from the processes that are currently running on your PC.

- **Folders** - Specify a folder on your computer to include all files in the folder to the exclusions .
- **Files** - Select a specific executable file you wish to add to the exclusions.

Click 'OK' to implement your settings.

Do not automatically cleanup suspicious certificates

- Choose whether or not to delete any root certificates that were not signed by a trusted certificate authority.
- By default, CCS warns you if any fake root certificates are found in your browsers but does not delete them.
- Disable this option if you want CCS to delete those fake certificates whenever they are found

Background:

- SSL certificates are used by websites to encrypt the connection between your browser and their web-server.
- This ensures nobody can intercept the traffic sent between you and the site. All information sent from your browser to the site is private. This is especially important for sensitive transactions like online payments, where you send your credit card information over the internet.
- You can tell a site is using an SSL certificate by the padlock icon in the browser address bar.
- SSL certificates are issued to website owners by an organization known as a 'Certificate Authority' (CA). The CA checks that the applicant owns the website in question, and is a legitimate business.
- Once these checks have been passed, the CA will sign the applicant's certificate with what is known as a 'root certificate'. You should only trust websites whose certificates have been signed by the root certificate of a trusted CA.
- These trusted root certificates are embedded in your browser (Firefox, Chrome, Edge etc). Your browser checks that the SSL certificate on a site is signed by a trusted root each and every time you visit the site.
- A fake root certificate would, therefore, bypass this check of legitimacy. It could tell you to trust a website run by a hacker.
- CCS can detect and remove fake root certificates from the endpoint during on-demand and scheduled scans. Disable 'Do not automatically cleanup suspicious certificates' to activate this feature.

Define actions to be taken on unrecognized auto-start entries/scheduled tasks

- **Apply the selected action to unrecognized autorun entries related to new / modified registry items** - Specify what CCS should do if applications added to **Script Analysis** > **Autoruns Scans** try to create or modify one of the following registry items:
  - Windows services
  - Auto-start entries
  - Scheduled tasks

The available options are:

- **Ignore** - CCS does not take any action (***Default***)
- **Terminate** - CCS stops the process / service
- **Terminate and Disable** - Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- **Quarantine and Disable** - The application is quarantined and the corresponding auto-start entry is removed. In the case of a service, CCS disables the service.

Background:

- CCS can perform heuristic command-line analysis and embedded code detection in order to protect Windows services, autostart items and scheduled tasks.
- CCS ships with a list of predefined applications for which it performs heuristic analysis on programs that

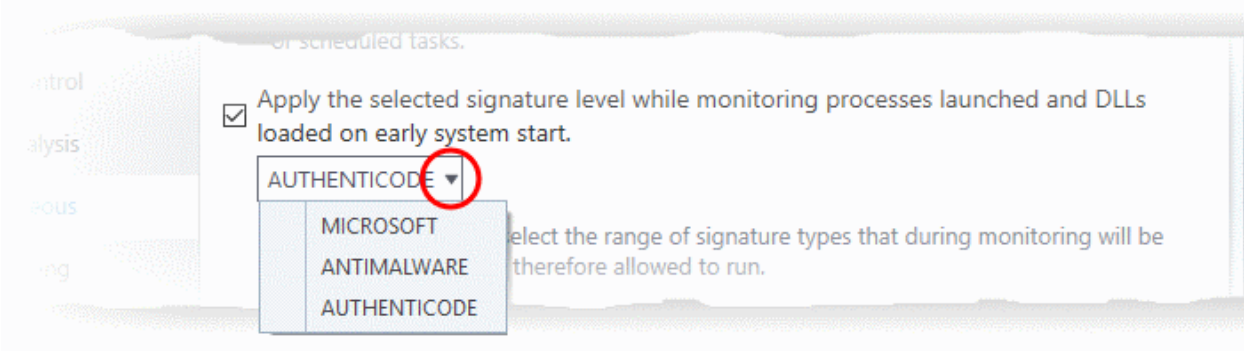
are capable of executing code.

- You can also add programs for which you want CCS to perform heuristics analysis in 'Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autoruns Scan'. See **Autoruns Scans** in **Script Analysis Settings** for more details on this.

Monitor processes and DLLs loaded at start up:

- You can instruct CCS to identify untrusted DLLs, apps, portable executables (PE) and autoruns launched before CCS starts on the endpoint. These may expose the endpoint to a danger if those items turn to be malicious.
- By default, CCS does not monitor these items.
- CCS checks whether startup items are signed by a trusted authority and marks them as trusted or untrusted. The flag is used at next restart to allow or block the item.

Apply the selected signature level...loaded on early system start - Choose how strict the certificate check should be:



- **Microsoft** - Only items signed by Microsoft certificates are marked as trusted
- **Antimalware** - Trusts files signed by either Microsoft or Antimalware certificates
- **Authenticode** - Flags all signed files as trusted

Monitor DLL files loaded by currently running processes

- By default, CCS does not monitor the DLL files loaded to system memory, by processes that are currently running on the endpoint.

Monitor DLL files being loaded by running processes - If enabled, CCS runs a file rating scan on each DLL loaded to identify its trust rating.

- The trust rating is reported to Endpoint Manager and added to local logs. Files with an Unrecognized' rating are submitted to Valkyrie for analysis.
- You can view these details at 'Security Sub-Systems' > 'Application Control'.
- See **https://help.comodo.com/topic-399-1-786-10102-Manage-File-Trust-Ratings-on-Windows-Devices.html** for more details.

Click 'OK' to save your settings.

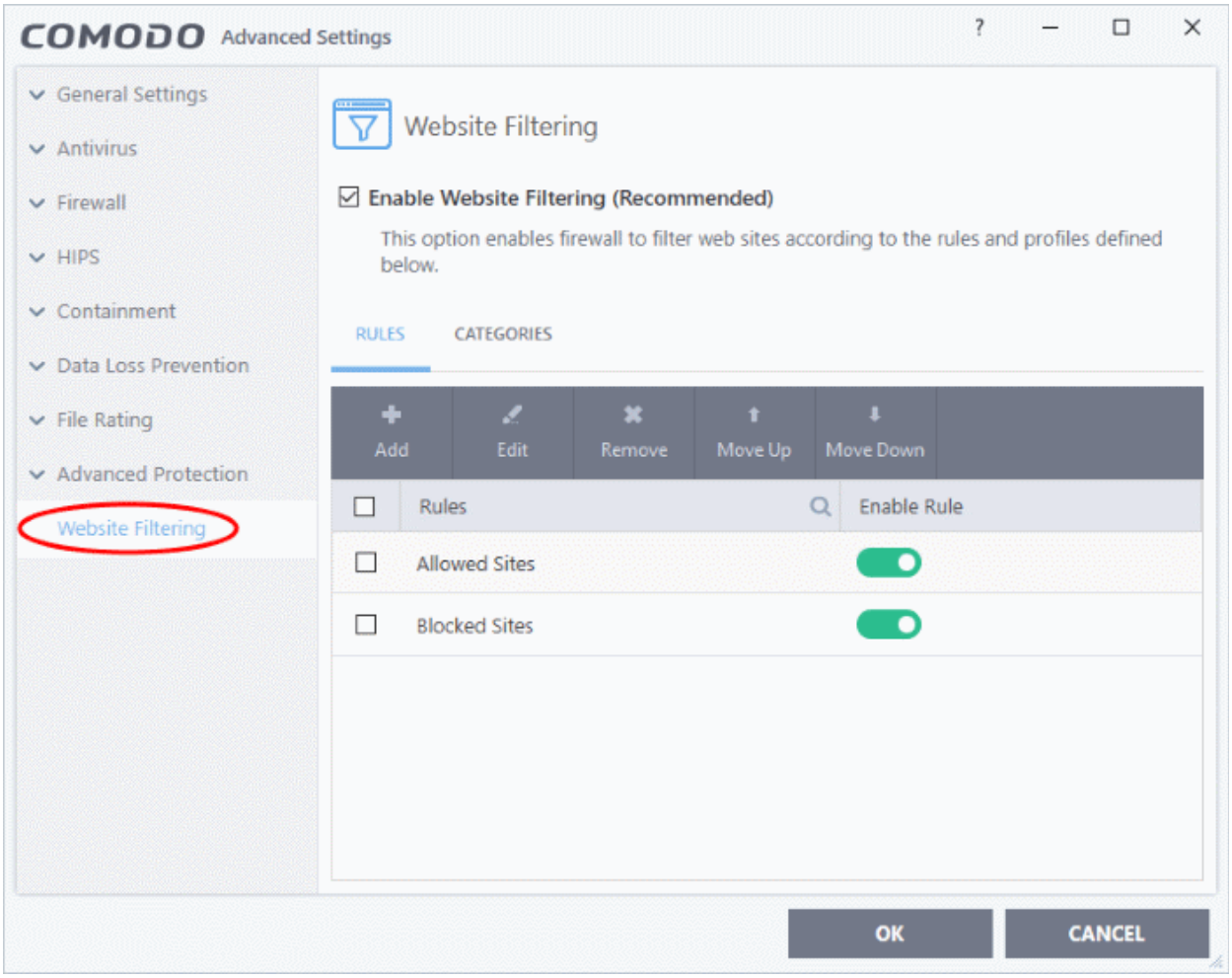
7.10. Web Filter Settings

- The web filter section lets you 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, and companies can prevent employees from visiting leisure sites during working hours.

- You can also log when a user tries to visit a site blocked by a rule.

Open the website filtering section

- Click 'Settings' at the top-left of the CCS home screen to open the advanced settings interface
- Click 'Website Filtering' on the left and choose the 'Rules' tab



Overview:

- You add websites to a category, then add the category to a rule.
  - A rule targets one or more website categories.
  - A category is a collection of one or more websites.
  - A 'website' can be a full URL, a text string, or a text string with a wildcard character (*)
- You must set a rule to be 'Allow' or 'Block', and must specify the users to which it applies.

Categories

- CCS ships with six preset categories of websites which can be added to rules that you create. The categories are: Safe, Suspicious, Phishing, Malware, Malicious and PUA (sites that host potentially unwanted applications).
- The other two categories, 'Exclusions' and 'Blocked', are empty by default and let you specify sites that should be allowed or blocked. You can add sites to 'Exclusions' if you want to access a site blocked by

another category.

Rules

- CCS also ships with two predefined rules, 'Allowed Sites' and 'Blocked sites', both of which are modifiable.
- The 'Blocked Sites' rule will prevent access to sites in the 'Comodo defined Malware sites' and 'Comodo defined Phishing Sites' categories. If you wish, you can add other categories to this rule to expand its coverage.
- The 'Allowed Sites' rule will permit access to websites in the Comodo 'Safe Sites' and 'Exclusions' categories.

Set up a new rule

- Click the 'Rules' tab
- Click 'Add' then name your rule
- Add categories to the rule
- Specify users to whom the rule should apply
- Specify whether the rule should be 'Allow' or 'Block'

The 'Website Filtering' panel has two sections:

- **Rules** - Define rules for website filtering and assign to required users. See '**Website Filtering Rules**' for more details.
- **Categories** - Define categories of websites to be allowed or blocked in website filtering rules. See '**Website Categories**' for more details.

General Advice:

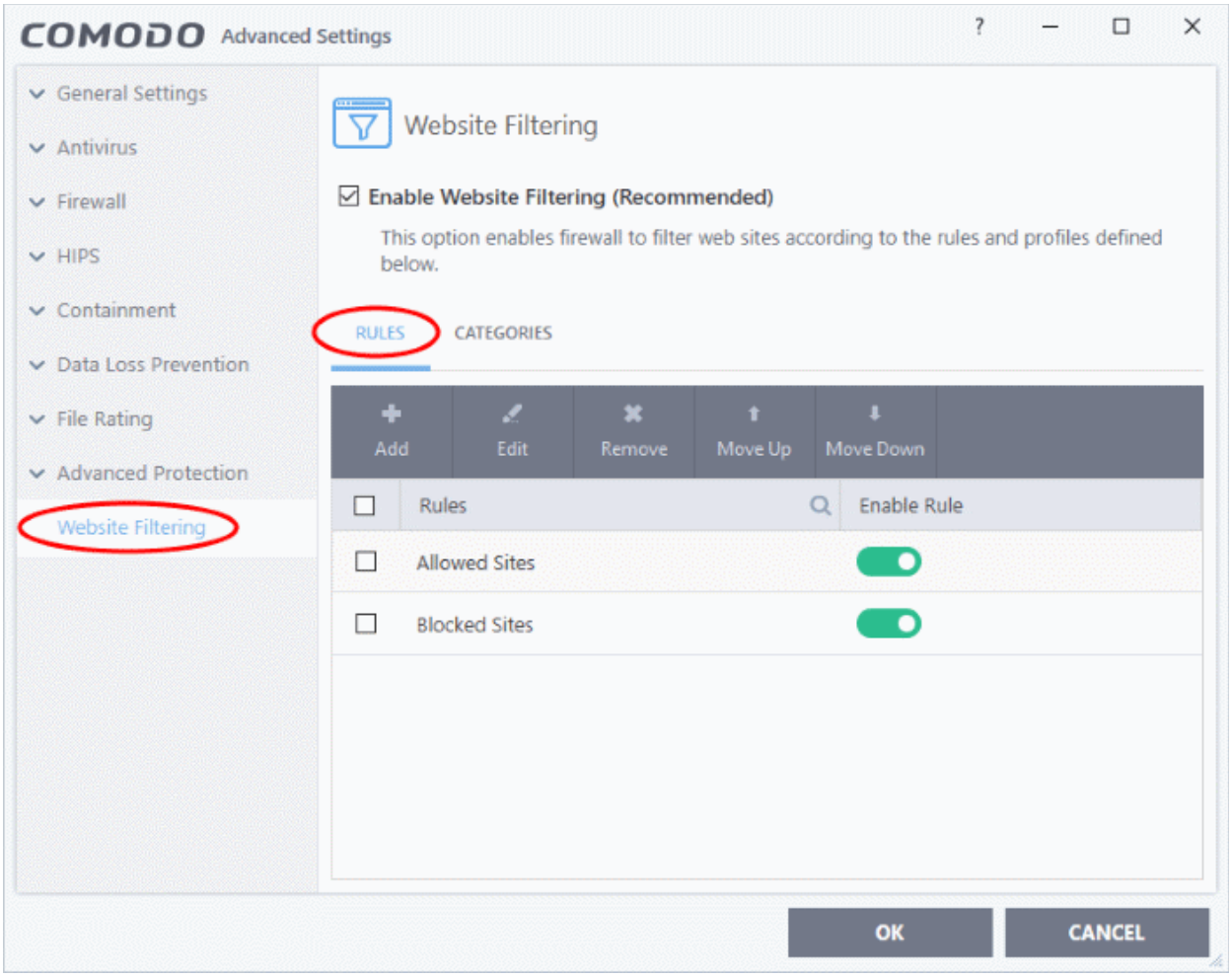
- It is the 'Categories' section where you specify the sites you want to block or allow, not the 'Rules' section. Rules are for specifying target users, and specifying whether a site-category should be allowed or blocked.
- If you want to filter specific websites, you need to create your own category.
- See '**Website Categories**' for more help on this.

7.10.1. Website Filtering Rules

- The powerful rule-configuration interface lets you create rules which are as sweeping or as granular as you require. Rules can be created on a per-user basis, allowing you to control exactly which websites certain people can or cannot visit. You can also disable or enable a rule as required at any time.
- Comodo Firewall implements rules in the order they are in this list. Should a conflict exist between individual rules, then the rules at the top takes priority. Click the 'Move Up' or 'Move Down' buttons at the top to change a rule's priority.

Open the website filtering rules section

- Click 'Settings' at the top left of the CCS home screen to open the advanced settings interface
- Click 'Website Filtering' on the left and choose the 'Rules' tab



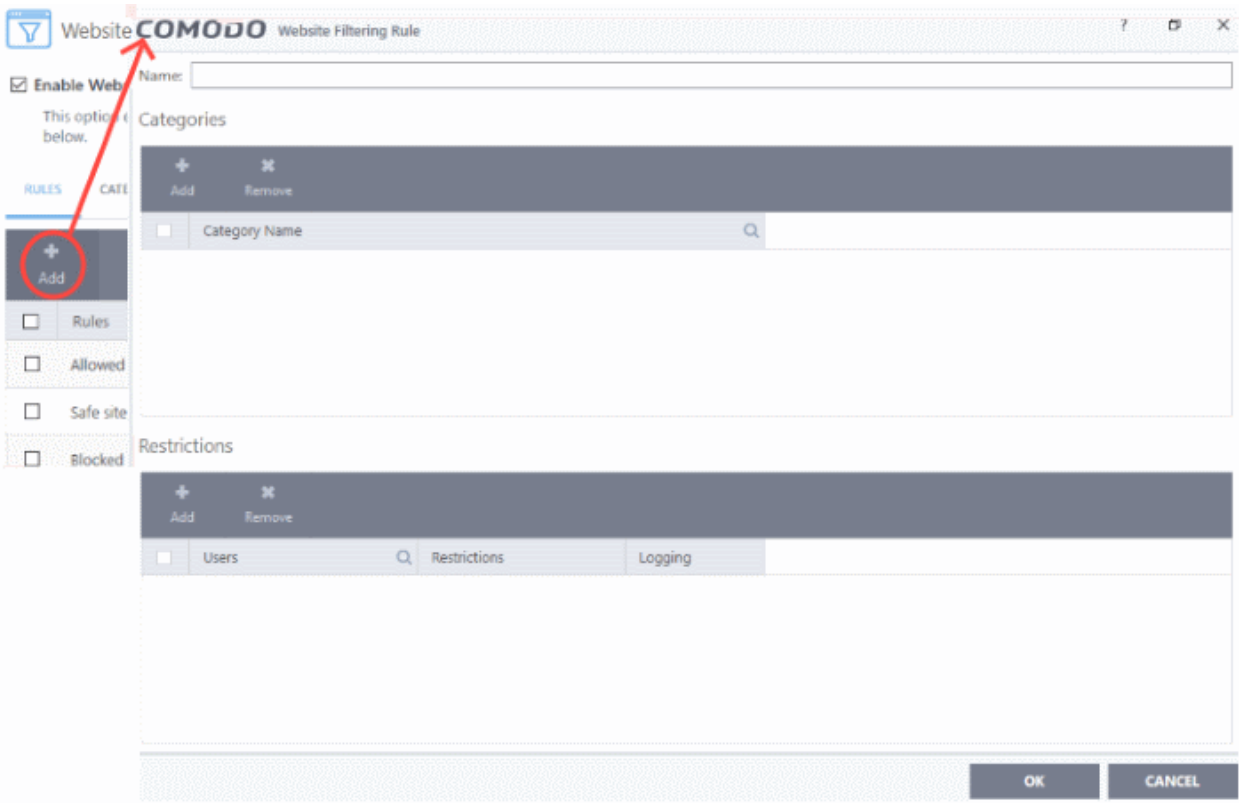
- The enable rule switch allows you to turn a rule on or off.
- The check-boxes next to a rule name let you select it for editing, deleting or re-prioritizing.
- Click the magnifying glass icon to search for a specific rule in the list.

The rules interface allows you to:

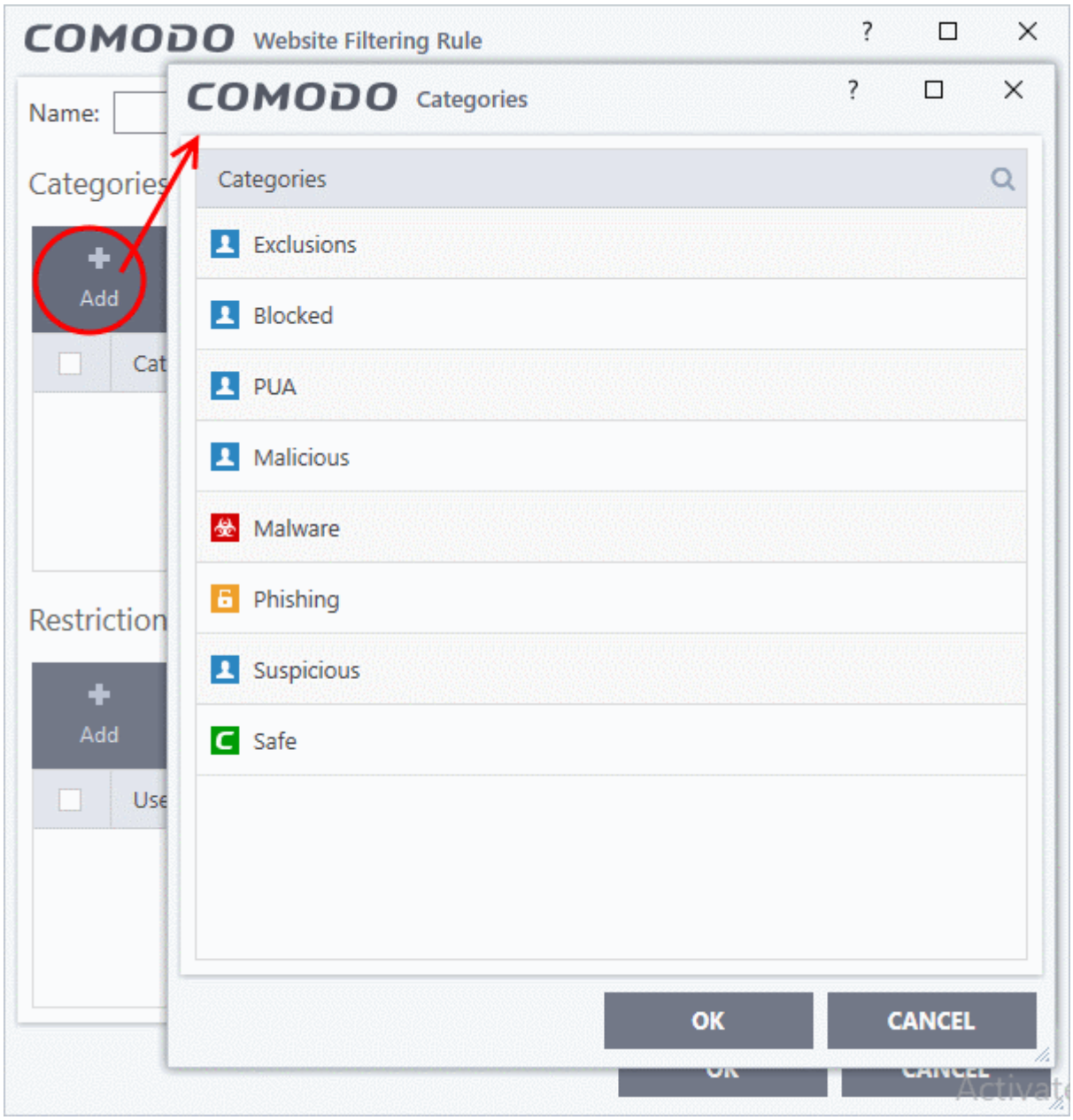
- **Create new website filtering rules**
- **Edit existing rules**
- **Remove unwanted rules**
- **Change priority of the rules**

Create a new Website Filtering rule

1. Open the website filtering panel by clicking 'Settings' from the CCS home screen and then select 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the 'Add' button at the top.



3. Enter a name for your new filter.
4. Select the categories that should be added to the filter:
    - Click the 'Add' button from the 'Category' pane



- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

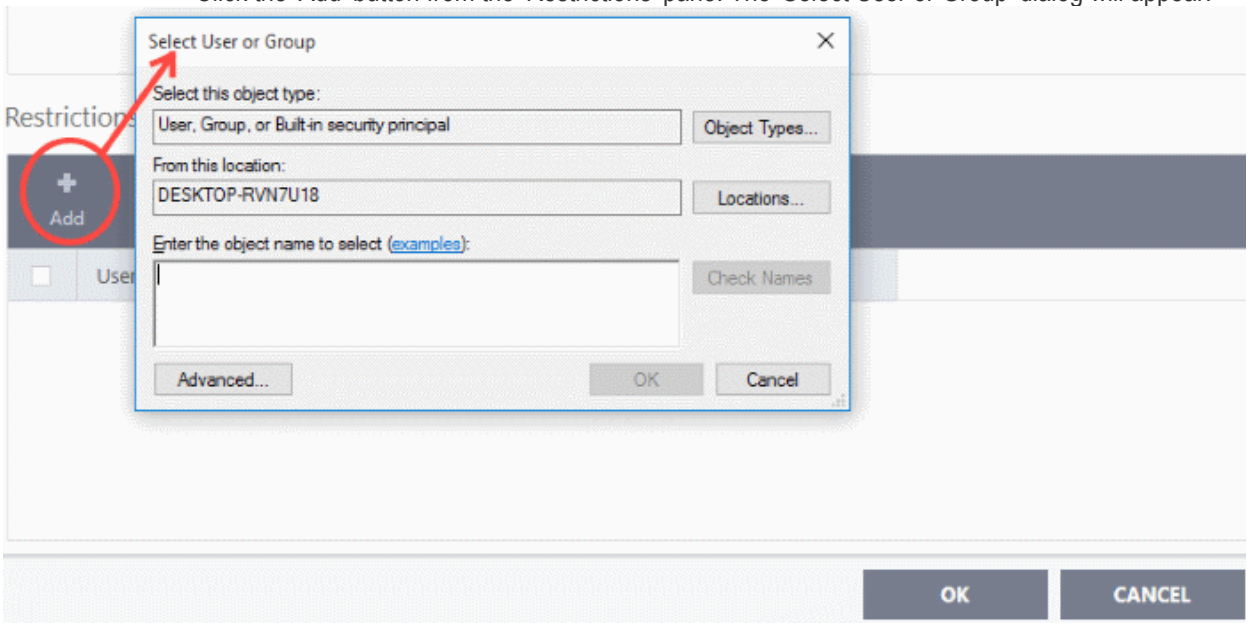
The 'Categories' window contains a list of pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Exclusions -** Websites you have decided to trust and allow connections to for the current session and future sessions.
- **Blocked** - Websites you have decided not to trust and deny connections.
- **PUA Sites -** Sites that host 'Potentially Unwanted Applications' (PUA). While not strictly speaking malware, a PUA is a piece of software that has functionality that may not have been made clear to a user. An example is a browser toolbar which tells you the weather forecast, but which also tracks your online activity.
- **Malicious Sites** - Sites that are known to host or contain links to malware, malicious scripts or deceptive content. These are intended to cause damage to your computer or steal personal data.
- **Malware Sites** - The URL leads to a direct malware download. Malware is designed to damage your computer, steal sensitive information or gain unauthorized access to your system.

- **Phishing Sites** - Fake copies of popular banking, shopping and social media websites that intend to steal customer data.
- **Suspicious Sites** - Sites which have shown strong evidence of suspicious behavior but have not yet hosted content which would warrant placing them in the 'Malware' or 'Malicious' categories. Users are advised to be on high alert should they visit these sites.
- **Safe Sites** - Websites that are considered safe according to the global whitelist.

See **Website Categories**, for more details on creating and modifying user specified categories.

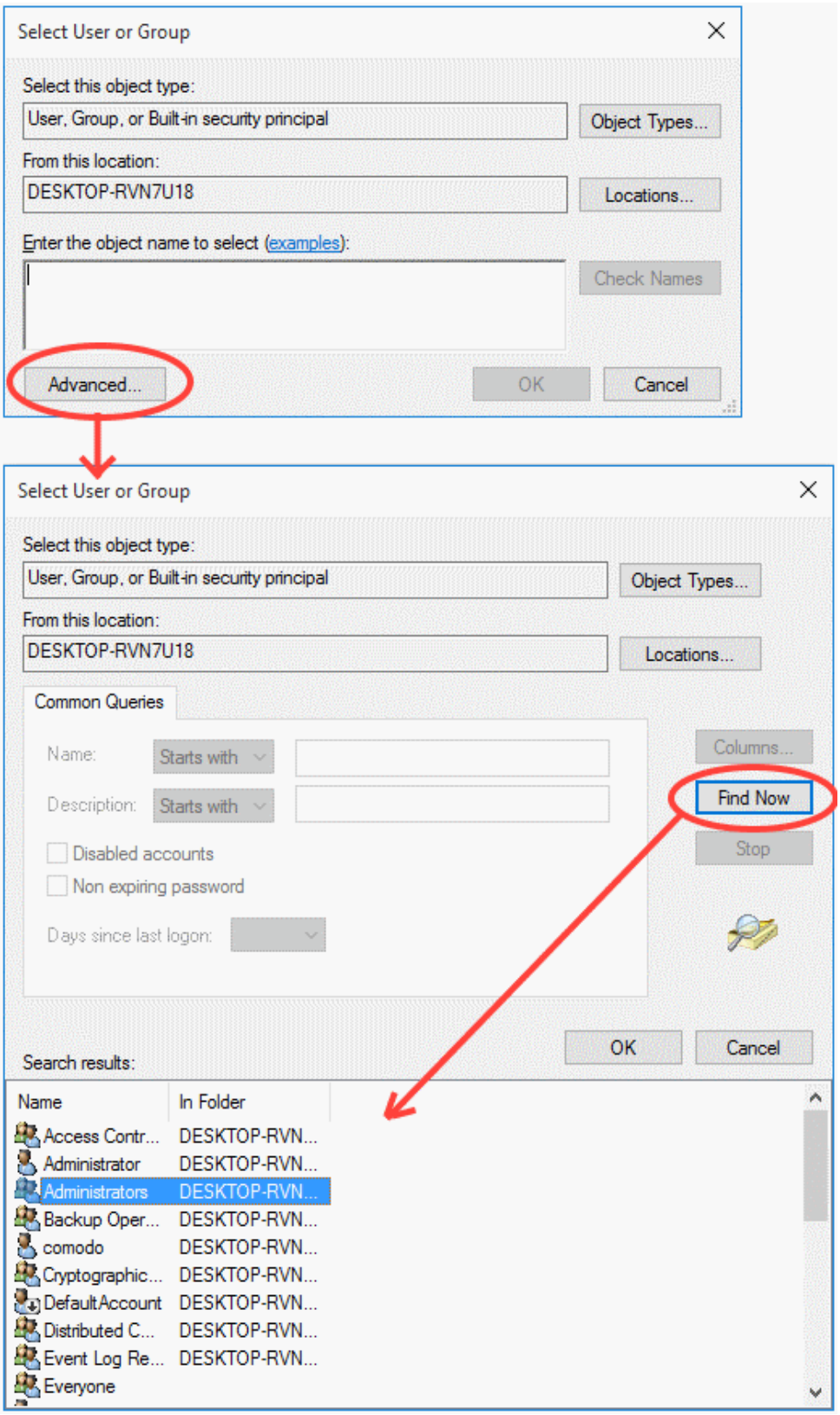
5. Add 'Users' or 'User Groups' to whom the rule should be applied:
   - Click the 'Add' button from the 'Restrictions' pane. The 'Select User or Group' dialog will appear:



   - **Enter the object name to select** - add users to whom the filter should be applied. Names should be in the format:

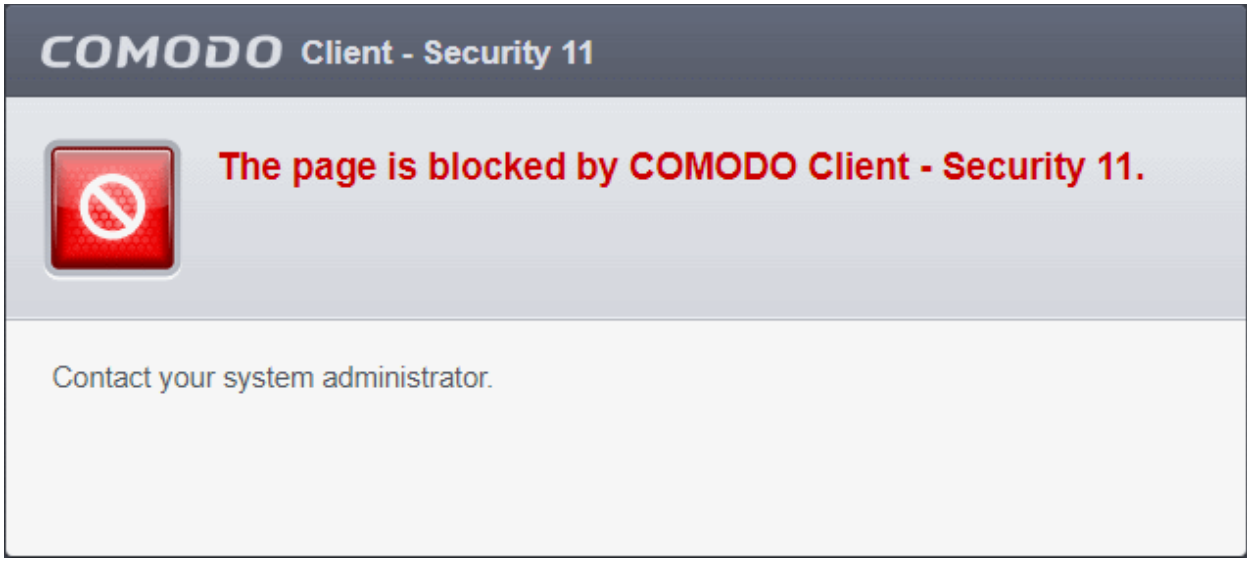
     <domain name>\<user/group name> OR <user/group name>@<domain name>.

     Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



You next need to specify whether those users should be allowed or blocked from viewing the websites, or whether they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:

- **Allow** - The websites in the categories can be accessed by the user.
- **Block** - The websites in the categories cannot be accessed by the user.



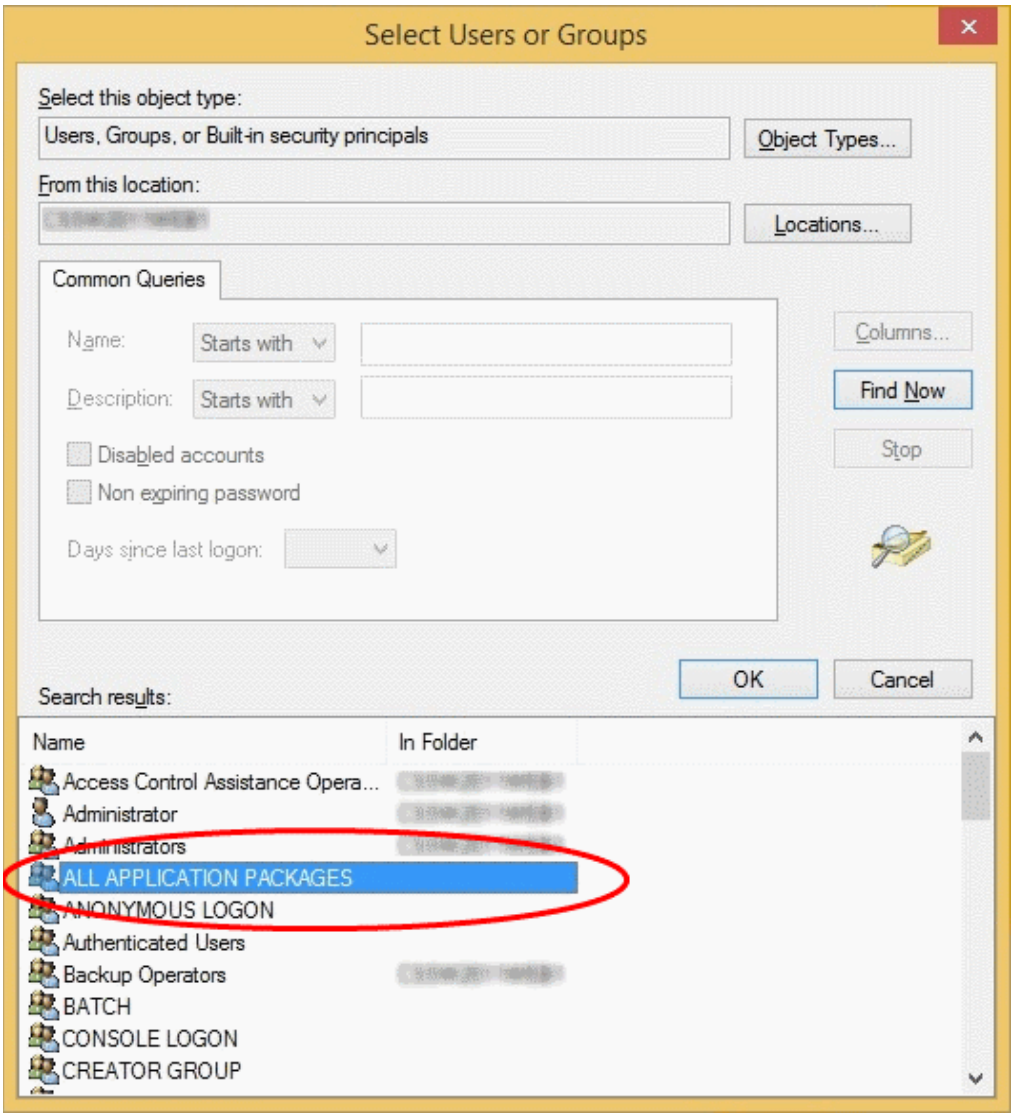
6. Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.
7. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
8. Make sure that the rule is enabled using the toggle switch under the 'Enable Rule' column for the rule to take effect.
    - You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Important Note to Windows 8 and Windows 8.1 users: If you are using Internet Explorer 11 version 11.0.9600.16384, it is mandatory to add the user group 'ALL APPLICATION PACKAGES' to the Restrictions list in addition to the intended users for each rule you create.

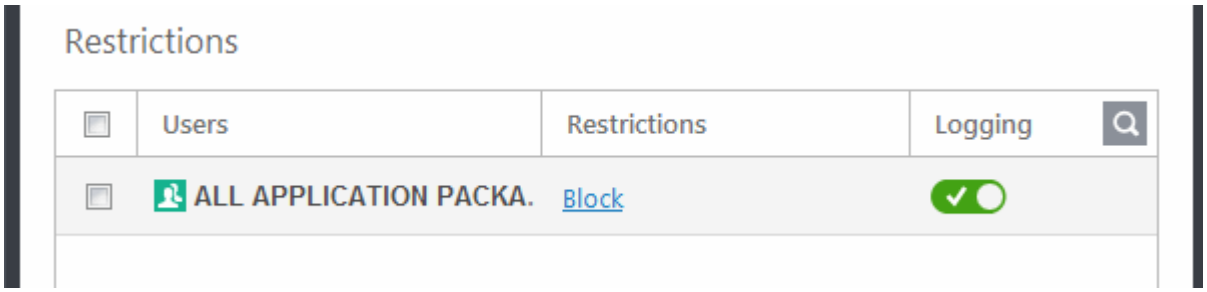
If you or other users access websites using Internet Explorer 11 on Windows 8/8.1, then you must add this user group or your rules will have no effect. For example, users will still be able to access blocked websites.

To add 'ALL APPLICATION PACKAGES' to the restrictions list

- Click 'Advanced' in the 'Select User or Group' dialog



- Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom
- Click 'OK'



Edit existing rules

1. Open the 'Website Filtering' Panel by clicking 'Settings' from the CCS home screen and then 'Website Filtering' from the 'Advanced Settings' interface.
2. Choose the website filtering rule to be edited under the 'Rules' tab by selecting the checkbox beside the rule.
3. Click the 'Edit' button at the top.

The ' Website Filtering Rule' interface for the selected rule will open. You can add/remove categories, add/remove users or change the restriction for selected users from this interface. See **Create a new website filtering rule** for more details on this interface.

Remove a website filtering rule

1. Open the 'Website Filtering' panel by clicking 'Settings' then 'Website Filtering' in the 'Advanced Settings' interface.
2. Open the 'Rules' tab. Choose the rule(s) you want to move by selecting the checkbox(es) beside the rule.
3. Click the 'Remove' button at the top.
4. Click 'OK'.

Change the priority of website filtering rules

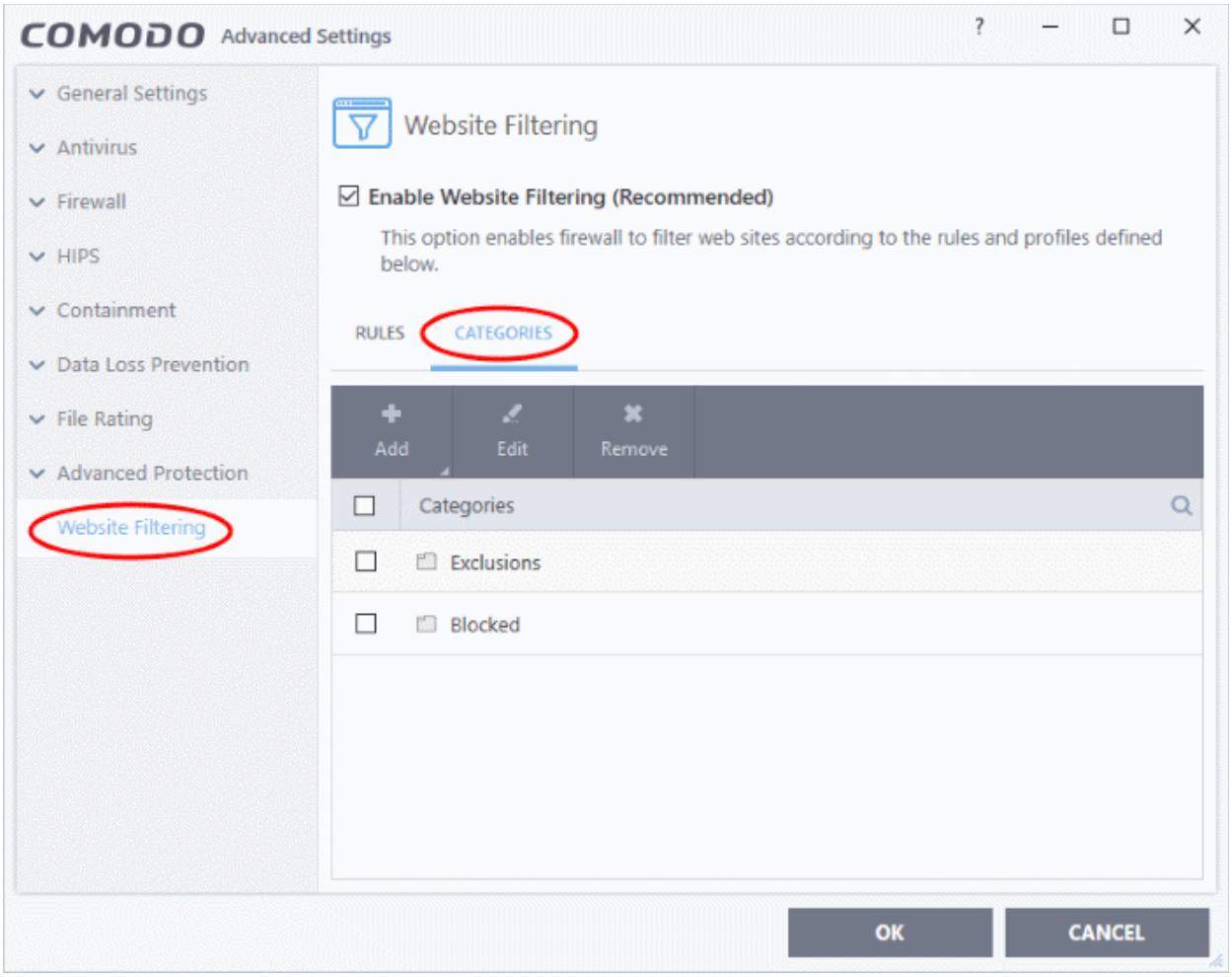
1. Open the 'Website Filtering' panel by clicking 'Settings' then 'Website Filtering' in the 'Advanced Settings' interface.
2. Open the 'Rules' tab. Choose the rule you want to move by selecting the checkbox beside the rule.
3. Click the 'Move Up' or 'Move Down' buttons to change the order of the rules.
4. Click 'OK'.

7.10.2. Website Categories

- The categories tab shows all built-in and user-defined web categories.
- Categories contain a list of 'Websites' which can be allowed or blocked in a rule.
- A 'Website' can be a URL or a simple phrase / term. You can use wildcard characters (*) with both URLs and terms.

Open the website filtering categories section

- Click 'Settings' at the top left of the CCS home screen to open the advanced settings interface
- Click 'Website Filtering' on the left and choose the 'Categories' tab



- Click the search icon to find a specific rule header. You can type rule names in full or in part.

The categories pane lets you:

- **Add a new category of websites**
- **Rename a category**
- **Remove unwanted websites from a category**
- **Remove a category**

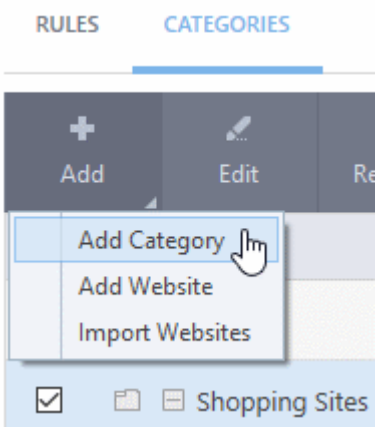
Add a new category of websites

Adding a new category involves two steps:

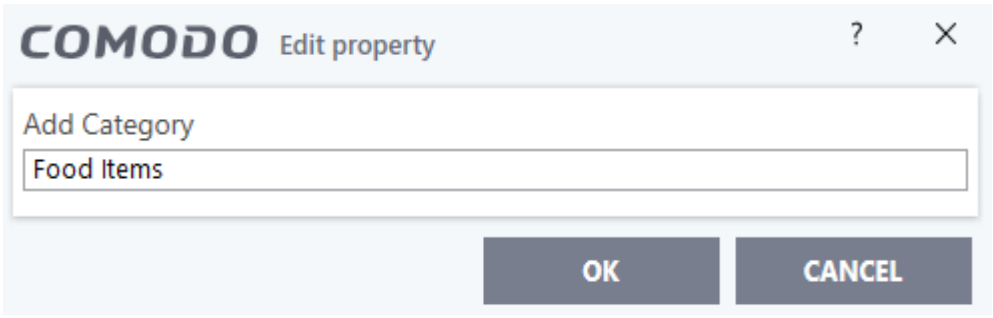
- **Step 1 - Define a name for the category**
- **Step 2 - Add Websites to be included to the category**

Step 1 - Define a name for the category

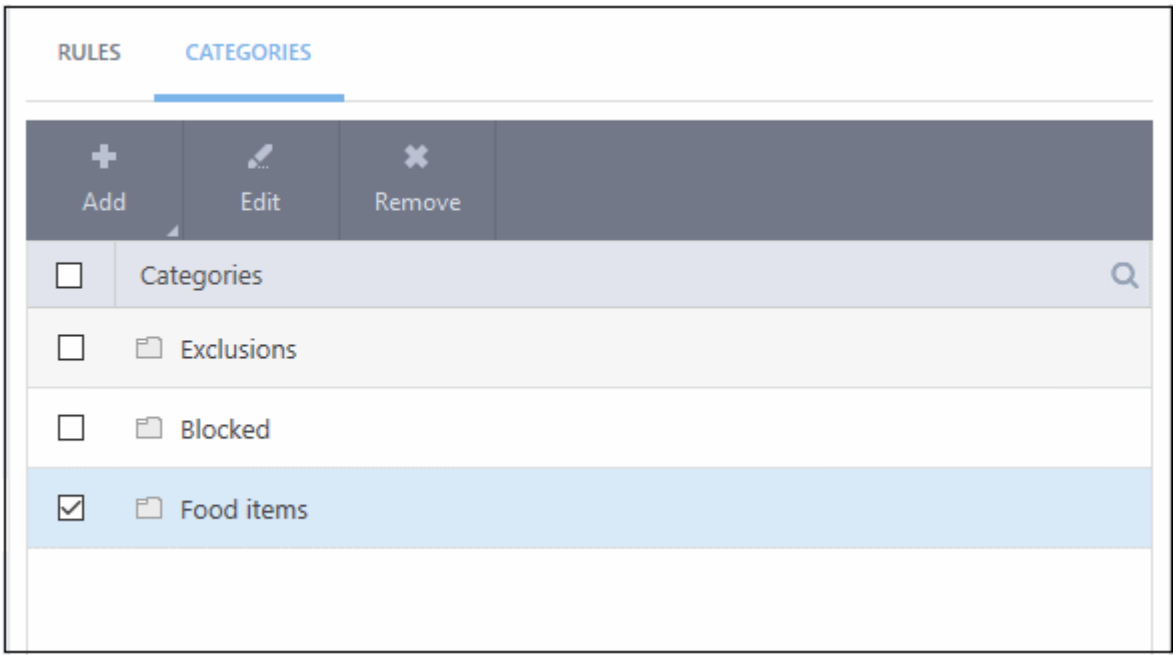
1. Click 'Settings' on the CCS home screen
2. Click 'Website Filtering' on the left
3. Click the 'Categories' tab
4. Click the 'Add' button at the top and select 'Add Category' from the drop-down menu.



Type a name for the category in the 'Add Category' box:



The new category will be listed in the categories tab:



Next, add websites to be included in the category:

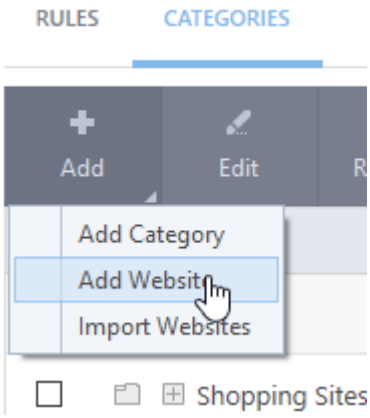
Step 2 - Add URLs to be included to the category

You can add websites to a category in two ways:

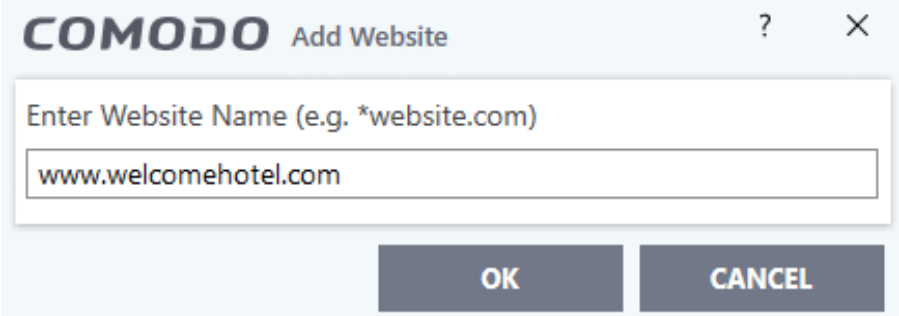
- **Manually Specify Websites**
- **Upload Website URLs from a text file**

Manually specify websites

1. Select the 'Category' from the list.
2. Click the 'Add' button.
3. Select 'Add Website' from the drop-down menu.



Type the address of the website you wish to add to the category in the 'Add Website' box:

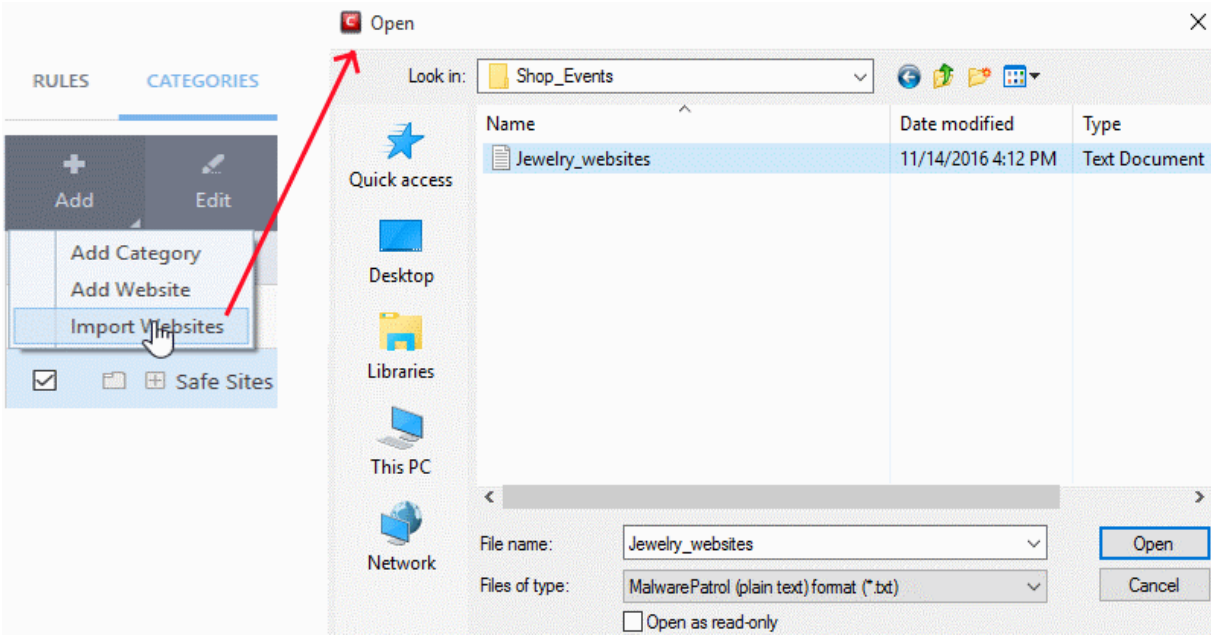


- To add a specific webpage, enter the full path to the page.
- To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
- To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, *pizza** will cover 'pizzahut.com', 'pizzacorner.net', and so on.
- To include all the websites with URLs that contain a specific string, add the wildcard character before and after the string. For example, **pizza** will cover hotpizza.com, spicypizza.net and so on.
- Click 'OK'.
- The website will be added to the category.

4. Repeat the process to add more websites.

Upload a list of websites from a text file

1. Select the target category from the list.
2. Click the 'Add' button and select 'Import Websites' from the drop-down menu.
3. Navigate to the file containing your list of URLs.



Note: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.

4. Click 'Open'.

CCS will automatically add the websites specified in the text file into the selected category.

Rename a category

1. Click 'Settings' on the CCS home screen
2. Click 'Website Filtering' on the left
3. Click the 'Categories' tab
4. Select the category to be renamed.
5. Right-click and select 'Edit' from the drop-down menu.
6. Enter the new name of the category in the 'Edit Property' dialog box and click 'OK'.

The category will be renamed immediately both under the 'Categories' section and in the 'Website Filtering Rules' to which it is applied.

Remove a website from a category

1. Click 'Settings' on the CCS home screen
2. Click 'Website Filtering' on the left
3. Click the 'Categories' tab
4. Click the '+' button beside the category to be edited to expand the website list.
5. Select the Website(s) to be removed.
6. Right-click then select 'Remove' from the drop-down menu.

Remove a Category

1. Click 'Settings' on the CCS home screen
2. Click 'Website Filtering' on the left

3. Click the 'Categories' tab
4. Select the category to be removed.
5. Right-click then select 'Remove' from the drop-down menu.

Note: You cannot remove a category if it is currently being used in a website filtering rule. Make sure to first remove the category from any rules in which it is applied.

Appendix 1 - CCS How to... Tutorials

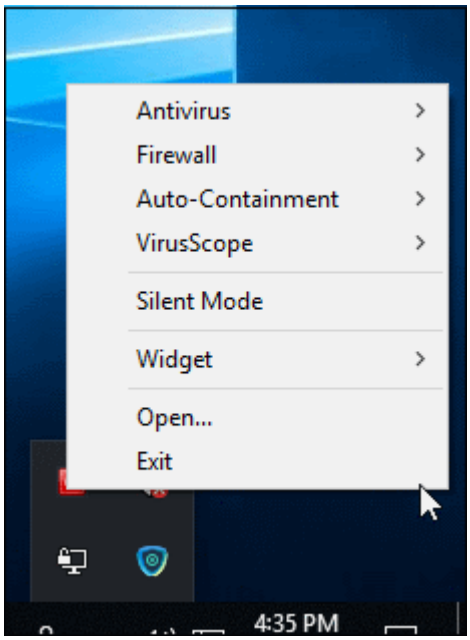
The 'How To...' section of the guide contains guidance on key tasks in Comodo Client Security. Use the links below to go to each tutorial's page.

How to...:

- **Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily** - How to quickly enable or disable various CCS modules.
- **Setup the Firewall for maximum security and usability** - How to set up a secure connection to the internet
- **Block Internet Access while allowing local network (LAN) Access** - Configure the firewall to only allow intranet/LAN connections while blocking the internet
- **Set up HIPS for Maximum Security and Usability** - How to set up the host intrusion protection system for the optimum balance between security and usability
- **Create Rules to Auto-Contain Applications** - How to set auto-containment rules for maximum security against untrusted applications
- **Run an instant Antivirus scan on selected items** - Run a manual scan on selected folders/files to check for viruses and other malware
- **Create an Antivirus scan schedule** - Set up antivirus scans to automatically run at specific times.
- **Run an untrusted program inside the container** - Launch programs that you do not trust inside the container to eliminate the possibility of them causing damage to your computer.
- **Run Browsers inside the Container** - Run your browser inside the container when you plan to visit untrusted websites
- **Restore incorrectly quarantined item(s)** - Restore files and executables that had been moved to quarantine by mistake
- **Submit quarantined items to Comodo for analysis** - Send suspicious files/executables to Comodo for analysis
- **Enable file sharing applications like BitTorrent and Emule** - Configure firewall for file sharing through popular software
- **Block any downloads of a specific file type** - Configure HIPS to block downloads of files of a specific type
- **Disable Auto-Containment on a Per-application Basis** - Exclude specific files or file types from the auto-containment process
- **Switch Off Automatic Antivirus Updates** - Stop automatic virus updates
- **Suppress alerts when playing games** - Switch off CCS pop-up alerts to avoid interruptions while playing games
- **Control External Device Accessibility** - Restrict access to external devices such as USB pen drive on the endpoints.

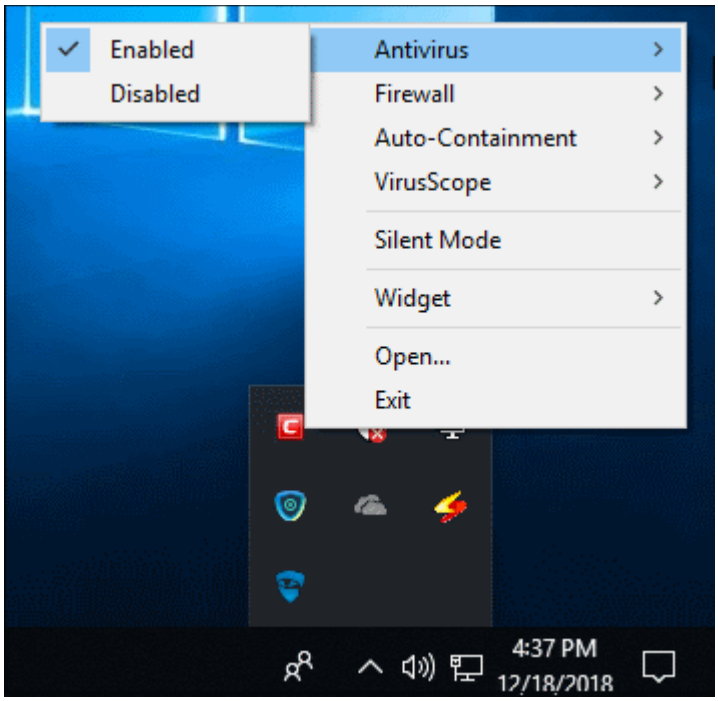
Enable / Disable AV, Firewall, Auto-Containment and VirusScope Easily

- Right-click on the CCS tray icon to quickly switch **Antivirus**, **Firewall**, **Auto-Containment** or **VirusScope** on or off:



Antivirus

1. Right-click on the system tray icon
2. Move your mouse over 'Antivirus'

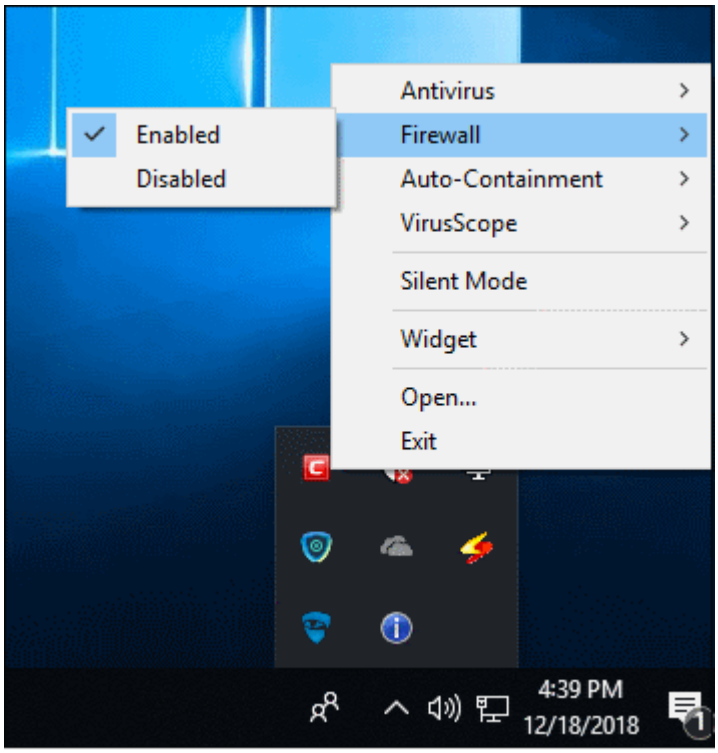


3. Choose 'Enabled' or 'Disabled' as required

You can also set security level in **the Home Screen**.

Firewall

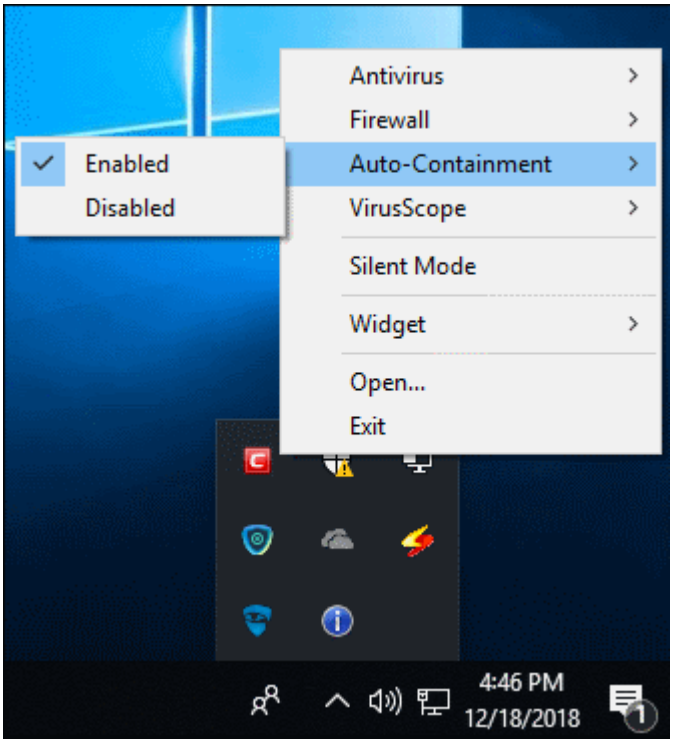
1. Right-click on the system tray icon
2. Move your mouse over 'Firewall'
3. Choose 'Enabled' or 'Disabled' as required



You can also set security level in **the Home Screen**.

Auto-Containment

1. Right-click on the system tray icon
2. Move your mouse over 'Auto-Containment'

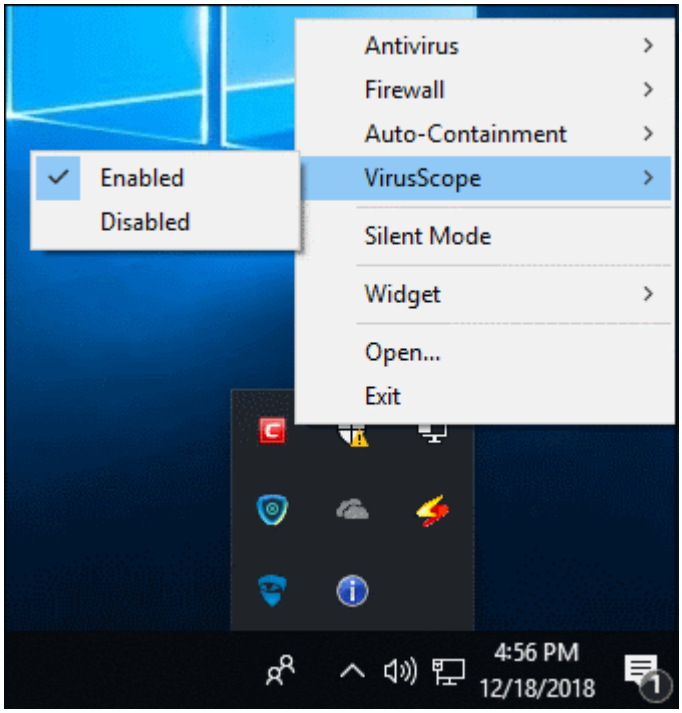


3. Choose 'Enabled' or 'Disabled' as required

You can also set security level in **the Home Screen**.

VirusScope

1. Right-click on the system tray icon
2. Move your mouse over 'VirusScope'



3. Choose 'Enabled' or 'Disabled' as required

You can also set security level from **the Home Screen**.

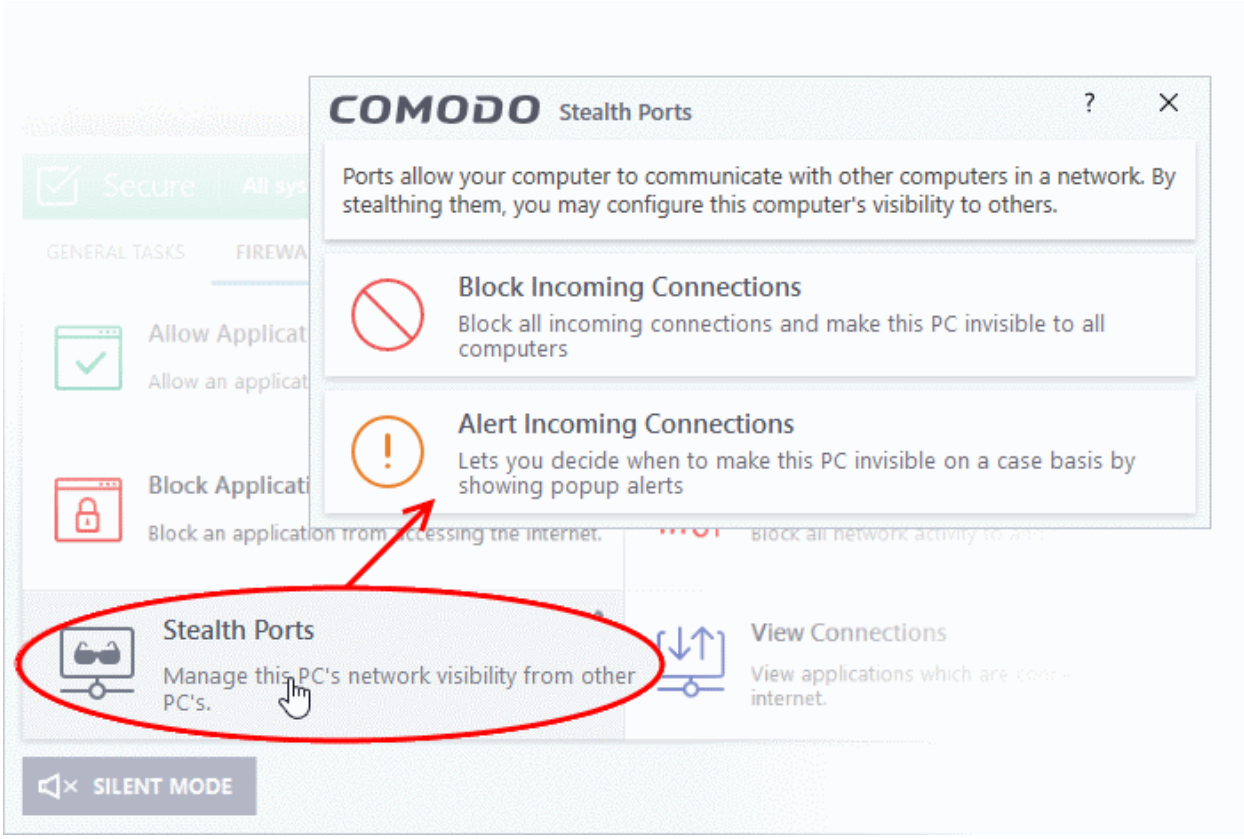
Set up the Firewall For Maximum Security and Usability

This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the internet.

Stealth Ports Settings

Port stealthing is a security feature whereby ports on an internet connected PC are hidden from sight, sending no response to opportunistic port scans.

1. Click 'Tasks' > 'Firewall Tasks'
2. Click 'Stealth Ports'



3. Select 'Block Incoming Connections' to make your computer's ports are invisible to all networks

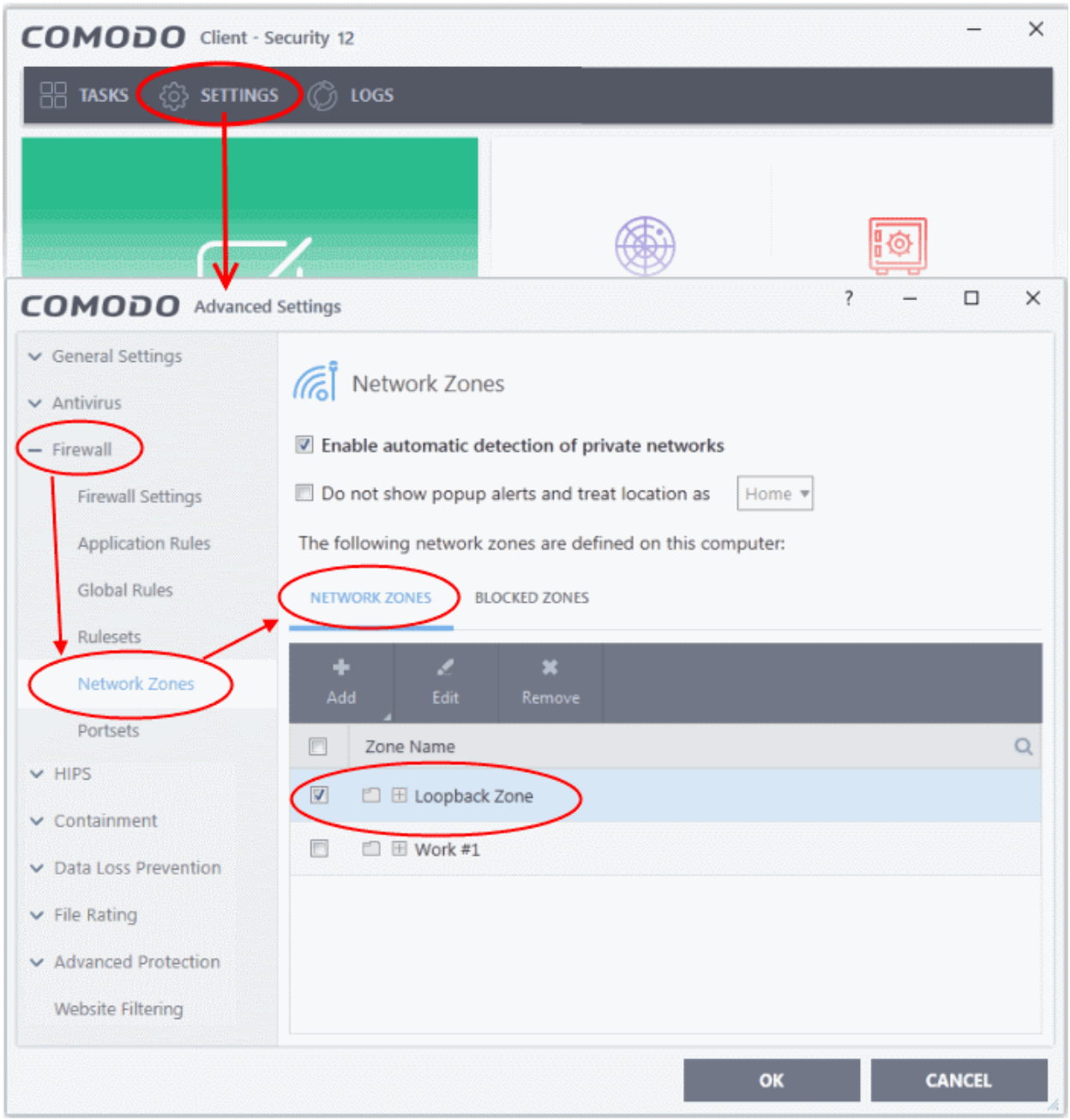
Click here for more information about port stealthing

Network Zone Settings

'Network Zones' settings allow you to configure the protection level for connections to a router/home network (this is usually done **automatically** for you).

View the configurations

1. Click 'Settings' at the top of the CCS home screen
2. Select 'Firewall' > 'Network Zones'
3. Click 'Network Zones' tab in the 'Network Zones' interface



4. Inspect the 'Loopback zone' and 'Local Area Network #1' (exact name may vary) by clicking the '+' button beside the zone name
    - **In most cases**, the loopback zone IP address should be 127.0.01/255.0.0.0
    - **In most cases**, the IP address of the auto-detected Network zone should be 10.nnn.nnn.nnn/255.255.255.0
5. Click 'OK'.

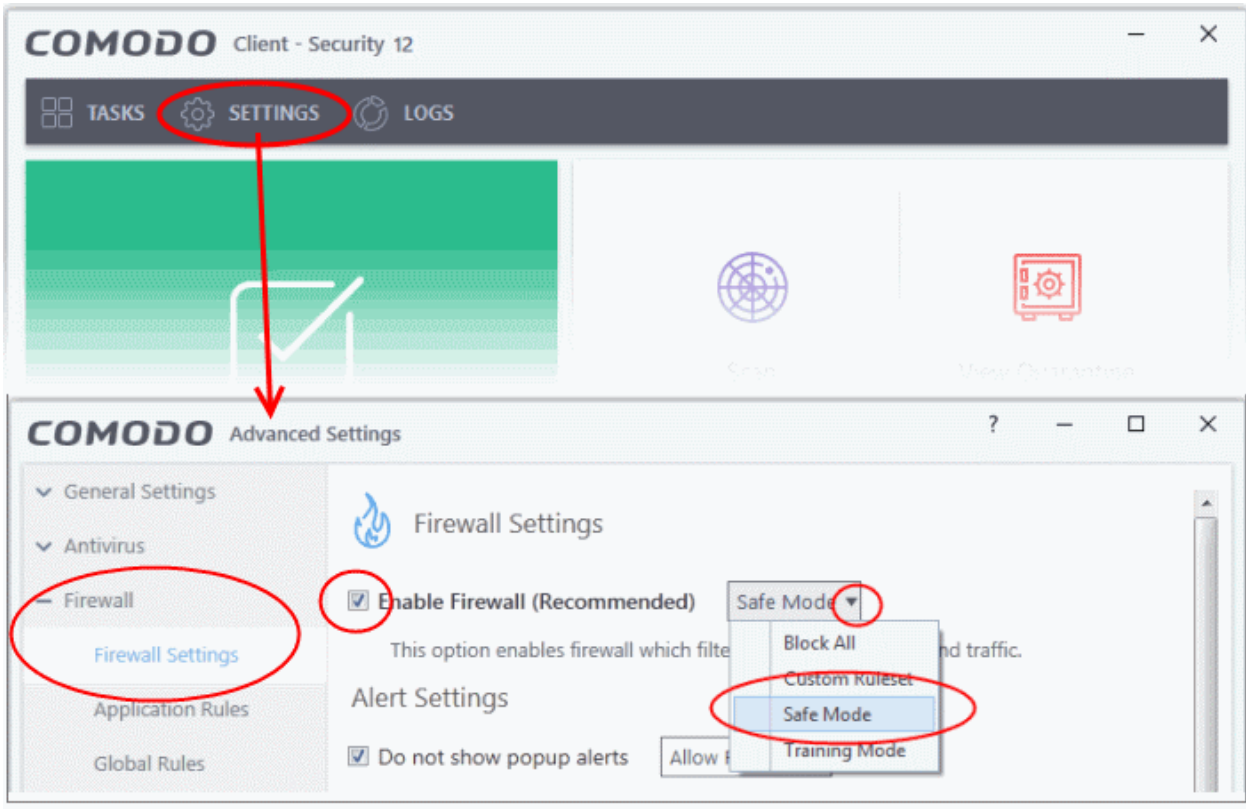
Click here for more details on network zones settings

Firewall Settings

The firewall settings option lets you configure the protection level for your internet connection, and the frequency of alerts generated.

1. Click 'Settings' at the top of the CCS home screen
2. Click 'Firewall' > 'Firewall Settings'

3. Select 'Enable Firewall' and choose 'Safe Mode' from the drop-down

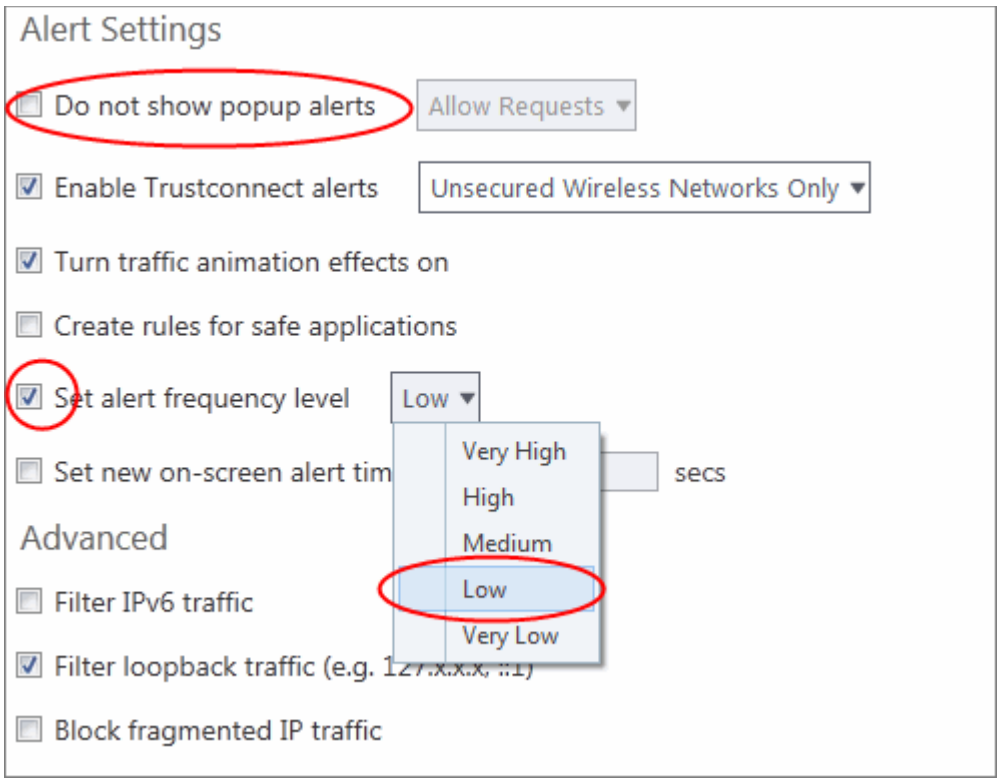


Safe Mode: While filtering network traffic, the firewall will automatically create rules which allow traffic for application components certified as 'Safe' by Comodo. For non-certified, new, applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

Under 'Alert Settings' in the same interface:

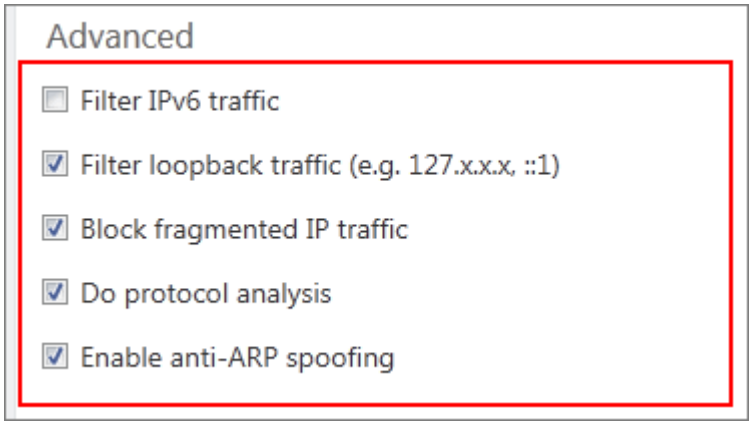
- Deselect 'Do not show pop-up alerts'
- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.



Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- Select **'Filter loopback traffic'**
- Ensure that the '**Block fragmented IP traffic'** is selected
  - **Block fragmented IP traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time.
- Select **'Do Protocol Analysis'** checkbox to detect fake packets used in denial of service attacks
- Select **'Enable anti-ARP spoofing'**



4. Click 'OK' for your settings to take effect.

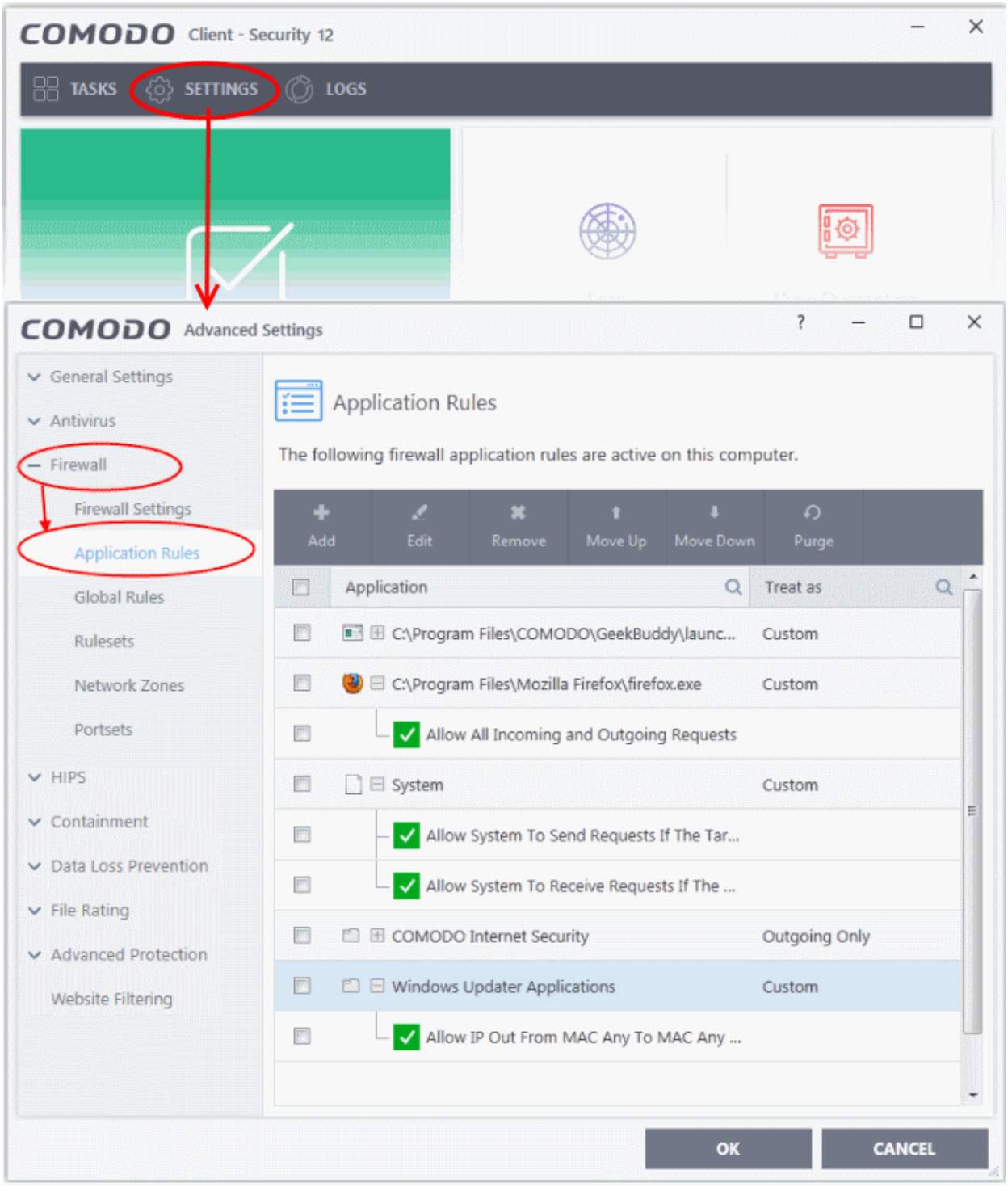
Click here for more details on the firewall settings

Set-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules and policies on an application-specific and global basis.

View the 'Application Rules'

1. Click 'Settings' on the CCS home screen
2. Click 'Firewall > 'Application Rules'

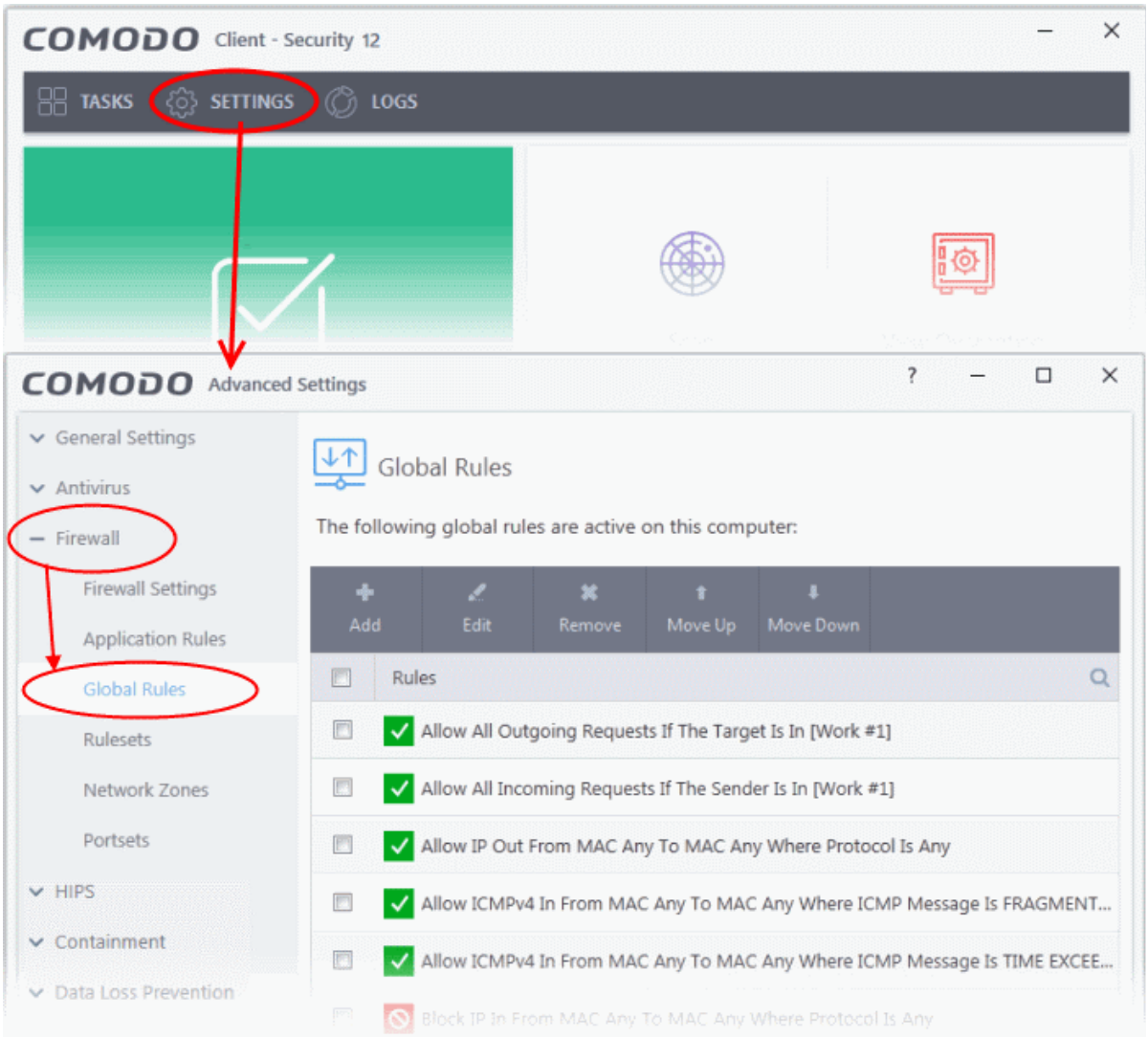


3. Click 'Add' to create a new application rule
4. Select a rule and click 'Edit' to edit the rules for a specific application manually or click 'Remove' to remove them
5. Click 'OK' for your settings to take effect

Click here for more details on application rules

View the Global Rules

1. Click 'Settings' on the CCS home screen
2. Click 'Firewall' > 'Global Rules'



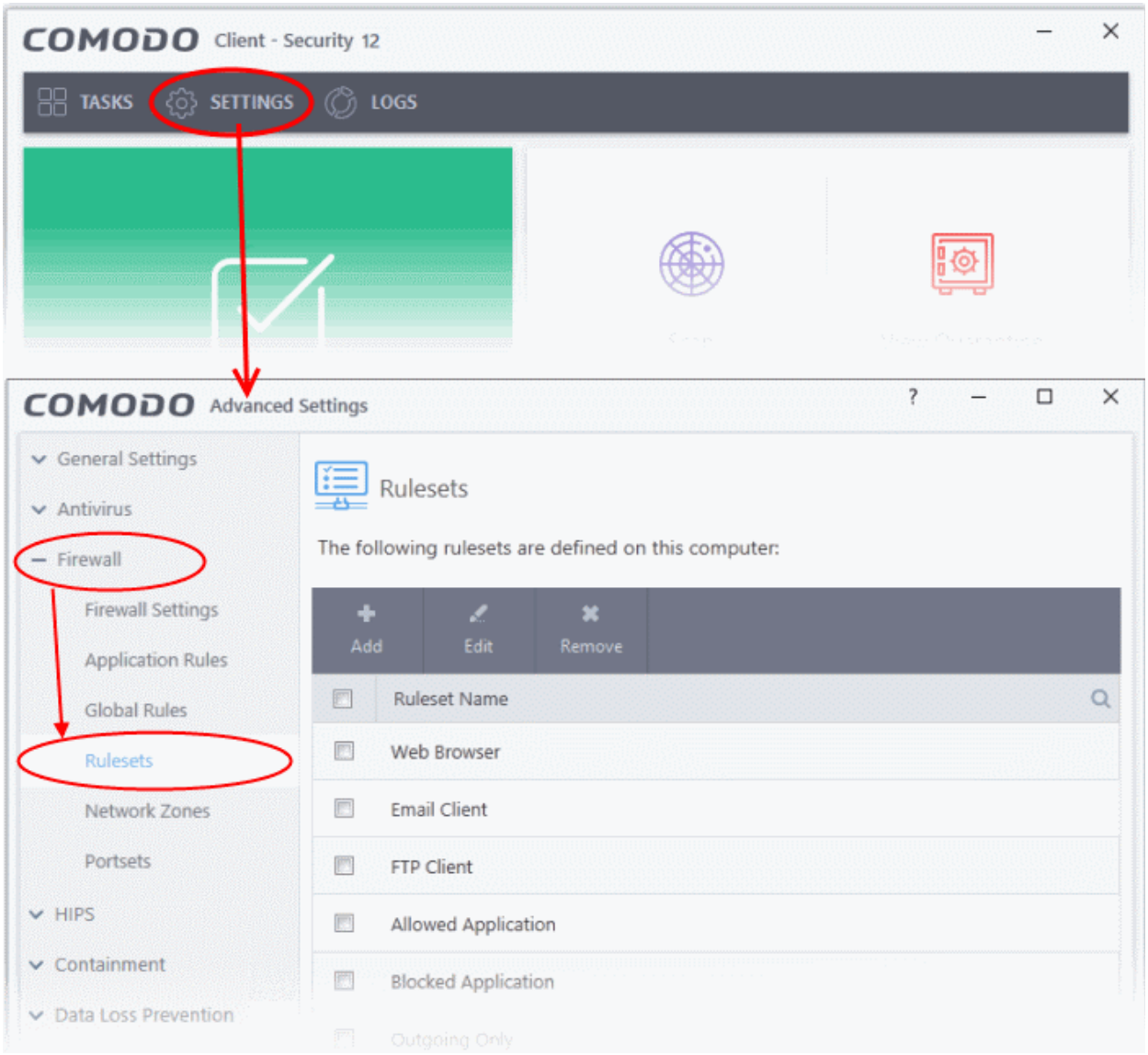
3. Click 'Add' to create a new global rule
4. Select a rule and click 'Edit' to edit the a rule manually or click 'Remove' to remove them
5. Click 'OK' for your settings to take effect

Click here for more details on global rules

View Predefined Firewall rulesets

1. Click 'Settings' on the CCS home screen

2. Click 'Firewall' > 'Rulesets'



3. Click 'Add' to create a new ruleset
4. Select a ruleset and click 'Edit' to edit the rules manually or click 'Remove' to remove them
5. Click 'OK' for your settings to take effect

Note: You need not make your own rulesets, the defaults are usually enough.

Click here for more details on pre-defined firewall rulesets

Block Internet Access while Allowing Local Area Network (LAN) Access

You can configure the firewall to block internet access while allowing connections to an internal network (intranet or LAN).

Example scenarios:

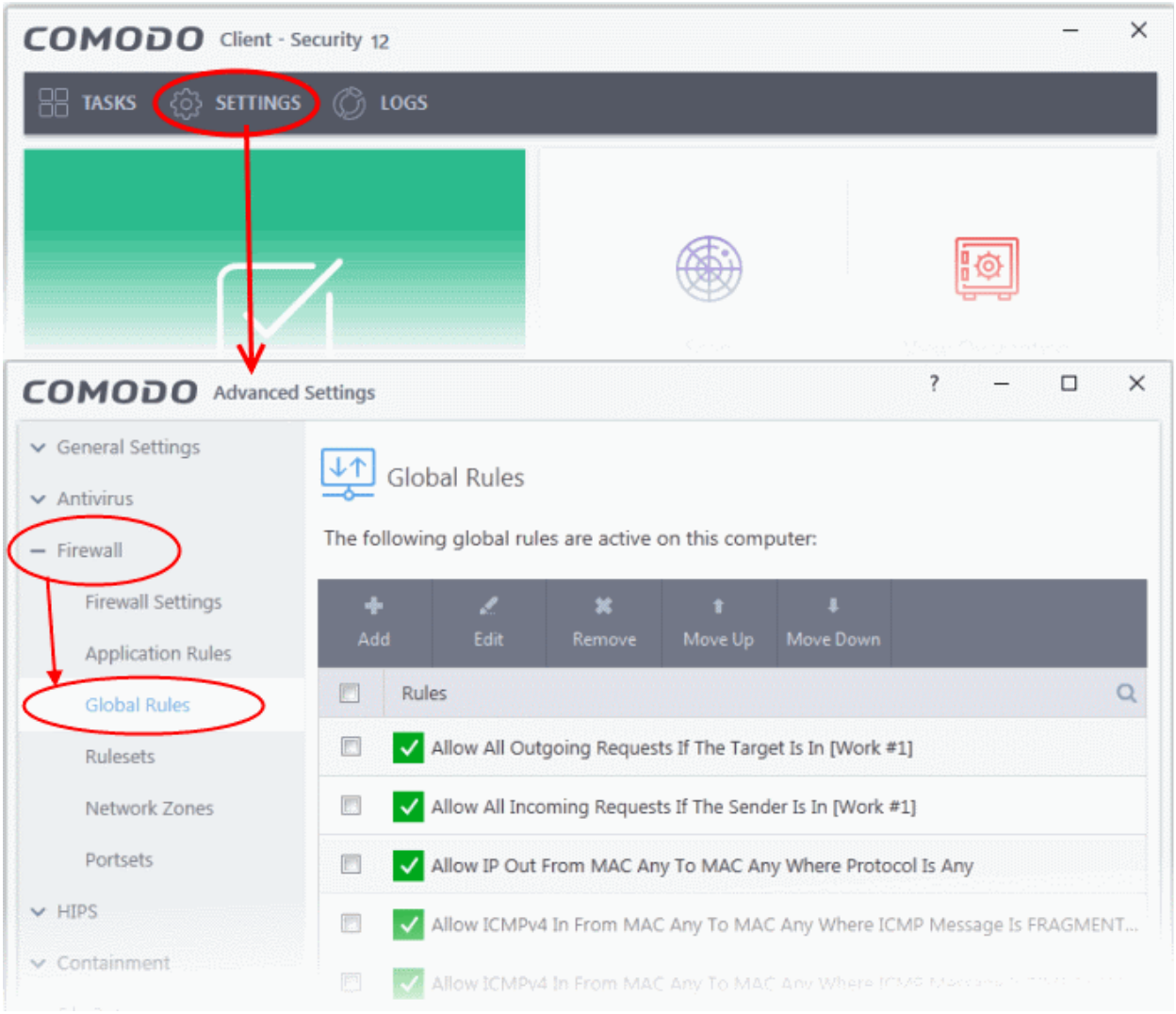
- In your network at home, you want your child's computer to connect to other computers at home but disable their internet access for safety reasons

- In a company network, you want employee computers to connect to your network but disable internet access for bandwidth reasons

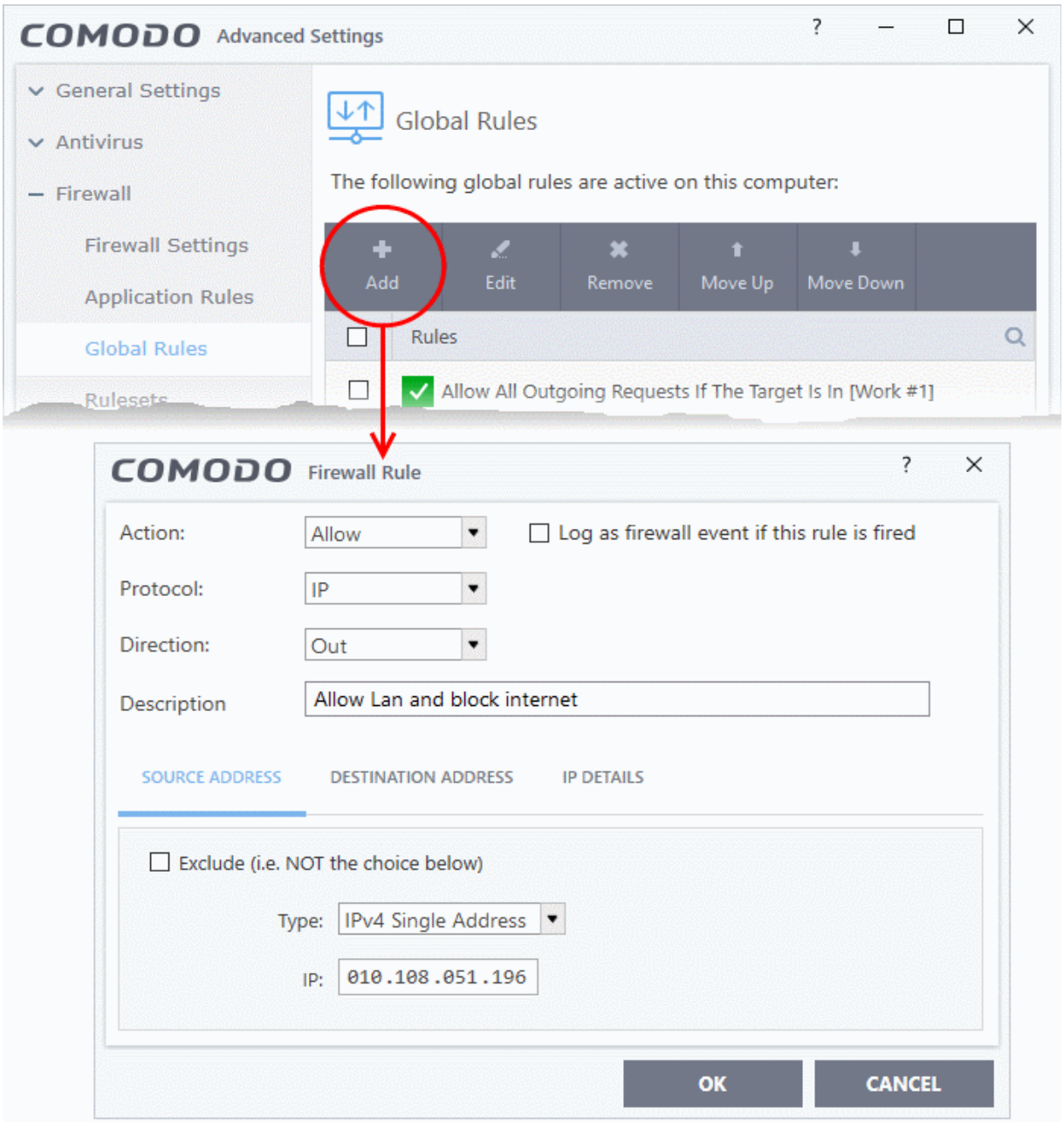
You need to create a global firewall rule to block internet access while allowing internal connections.

Create the global rule

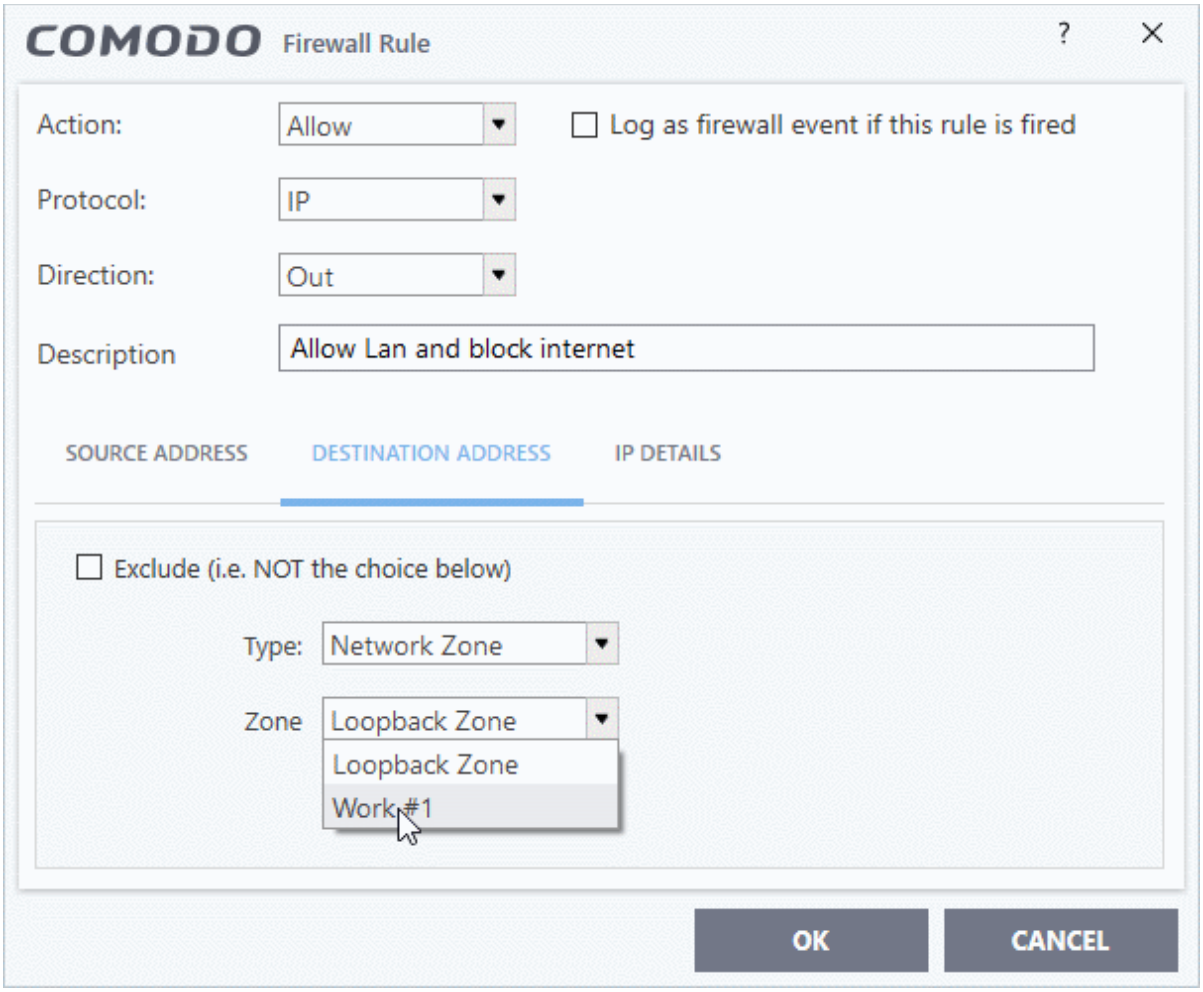
1. Click 'Settings' on the CCS home screen
2. Click 'Firewall' > 'Global Rules'



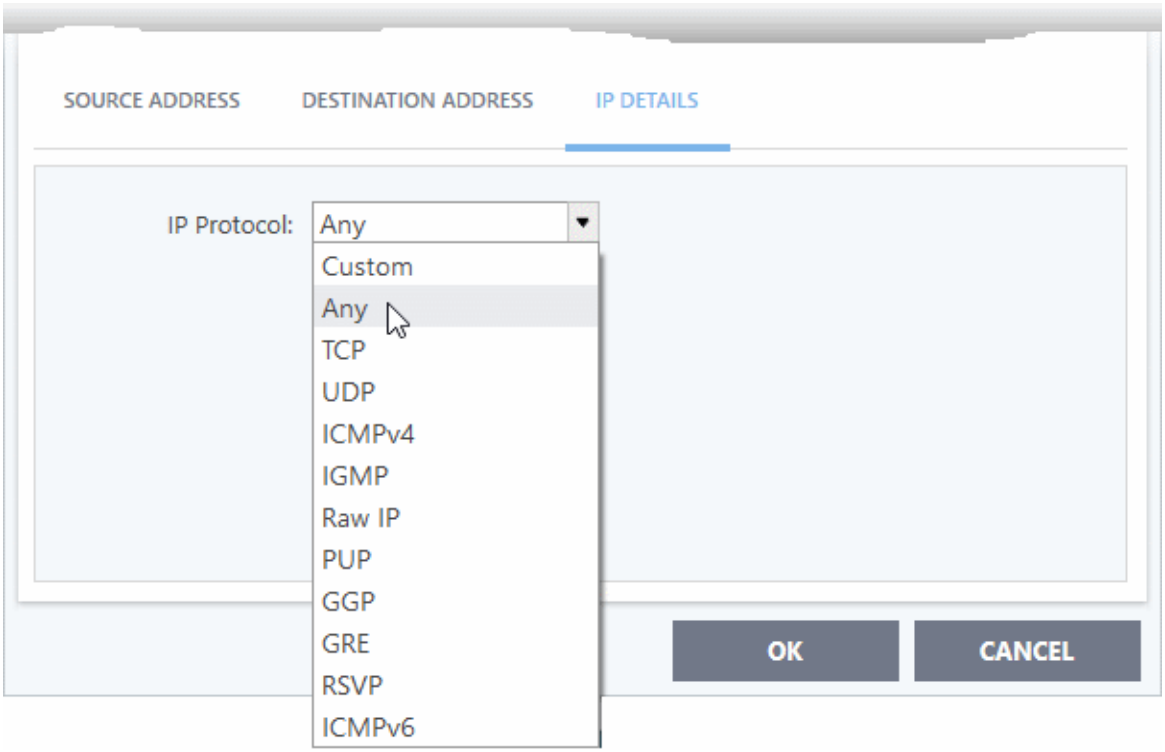
3. Choose 'Add' from the options at the top.



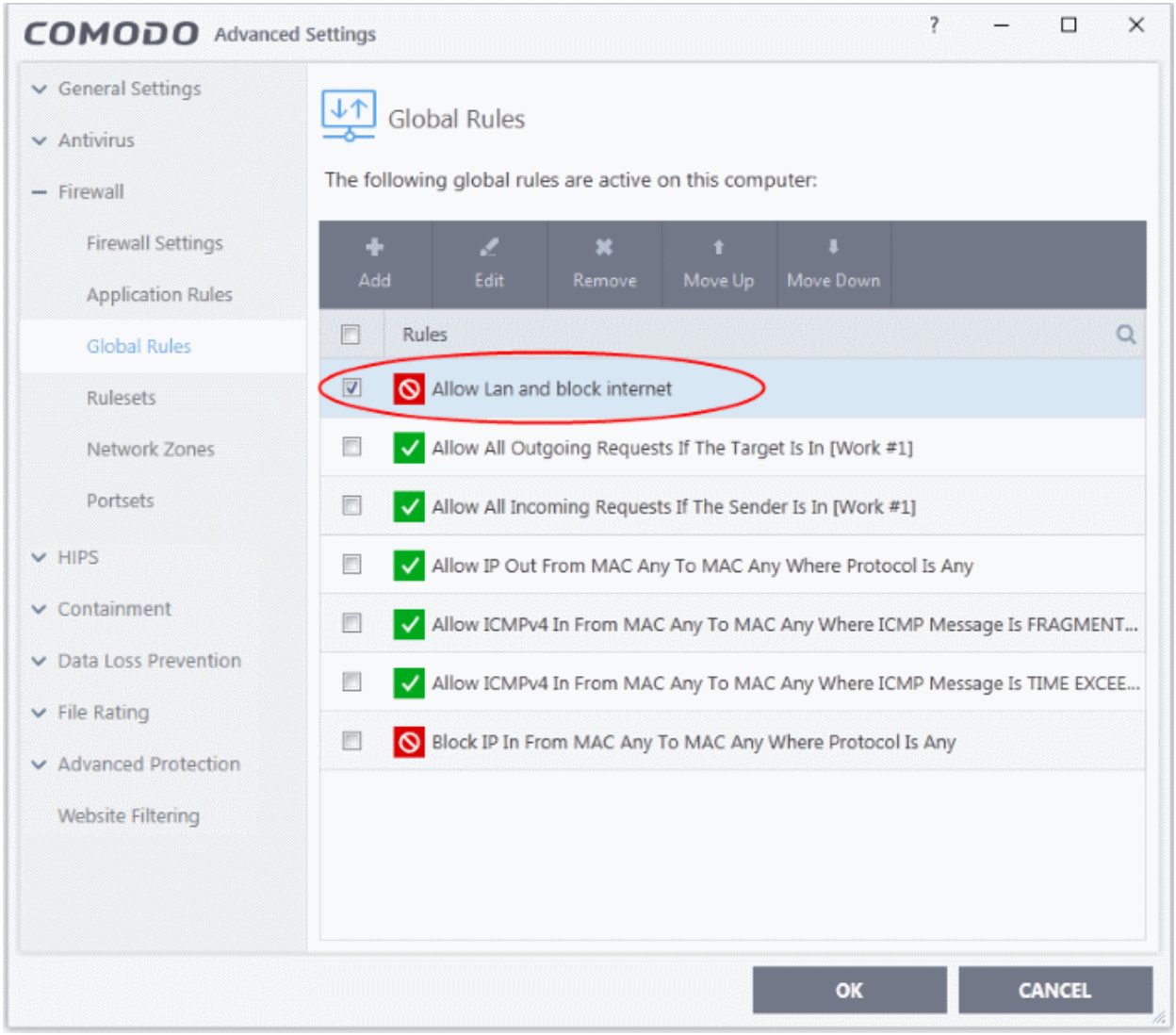
4. Choose the following options from the respective drop-downs:
   - Action = 'Block';
   - Protocol = 'IP';
   - Direction = 'Out'.
5. Enter a description for the new rule in the 'Description' text box.
6. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network and enter the IP address of the computer in the IP text box.
7. Click the 'Destination Address' tab, choose 'Network Zone' from the 'Type' drop-down and choose your local area network from the 'Zone' drop-down.



8. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.



9. Click 'OK'. The created policy will be added to the list of 'Global Rules'.
10. Select the rule and click the 'Move Up' button until the rule is in first position:



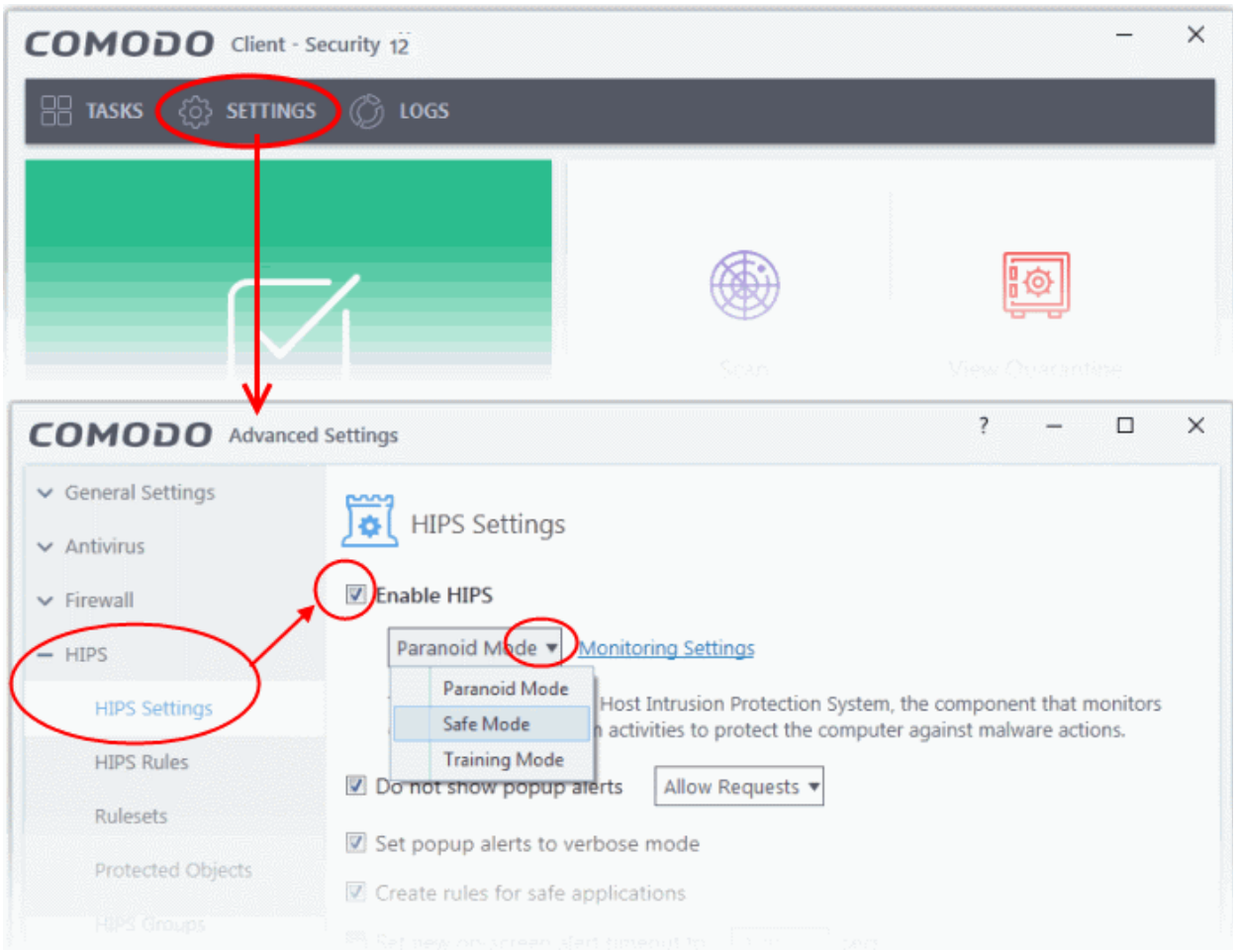
11. Click 'OK' for your configuration to take effect.

Your firewall is now configured to allow access to the internal network but to block internet access.

Set up HIPS for Maximum Security and Usability

This page explains how to configure the host intrusion prevention system (HIPS) to provide maximum security against malware and hackers.

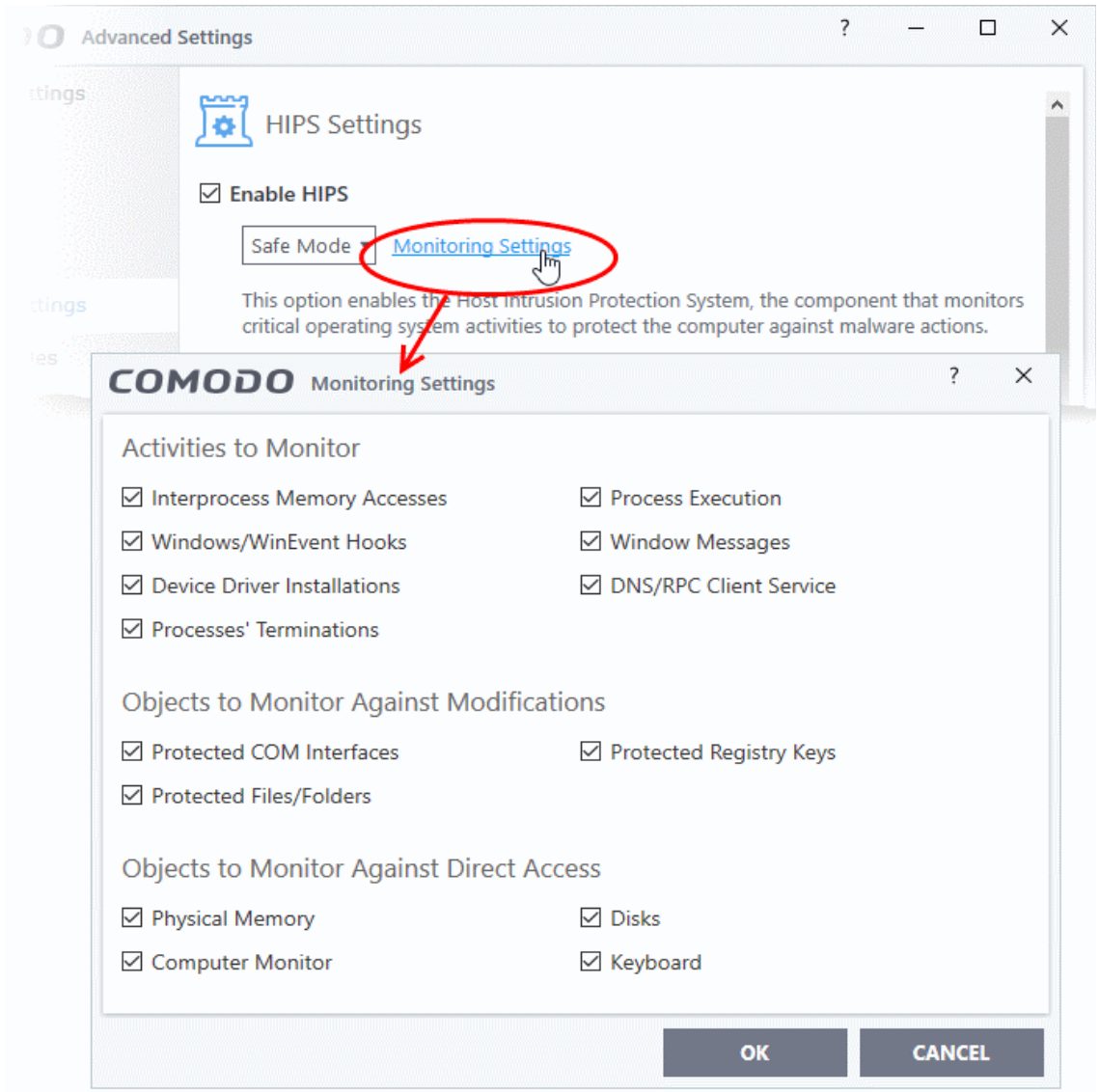
1. Click 'Settings' on the CCS home screen
2. Click 'HIPS' > 'HIPS Settings'
3. Select 'Enable HIPS'



4. Choose 'Safe Mode' from the drop-down.

Monitoring Settings

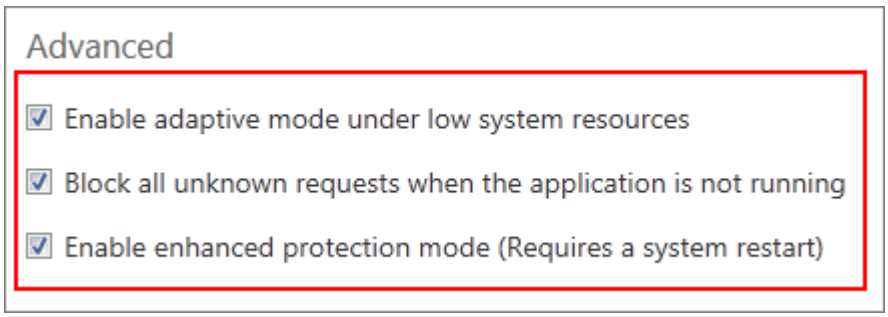
1. Click the 'Monitoring Settings' link in the 'HIPS Settings' interface



2. Make sure that all the check boxes are selected then click 'OK'

Advanced Settings

1. Enable the following settings in the 'Advanced' area of the HIPS Settings interface:



- Enable 'Block all unknown requests if the application is not running' (Optional) - Selecting this option blocks all unknown execution requests if Comodo Client Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CCS security settings, then it is 'OK' to leave this box unchecked.

- Select 'Enable enhanced protection mode (Requires a system restart)' - If you are using a 64-bit system, in order to maximize the security, it is important to enable this mode to activate additional host intrusion prevention techniques in HIPS to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures.
- Because of limitations in Windows 7 x64, some HIPS functions in previous versions of CCS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS functionality.

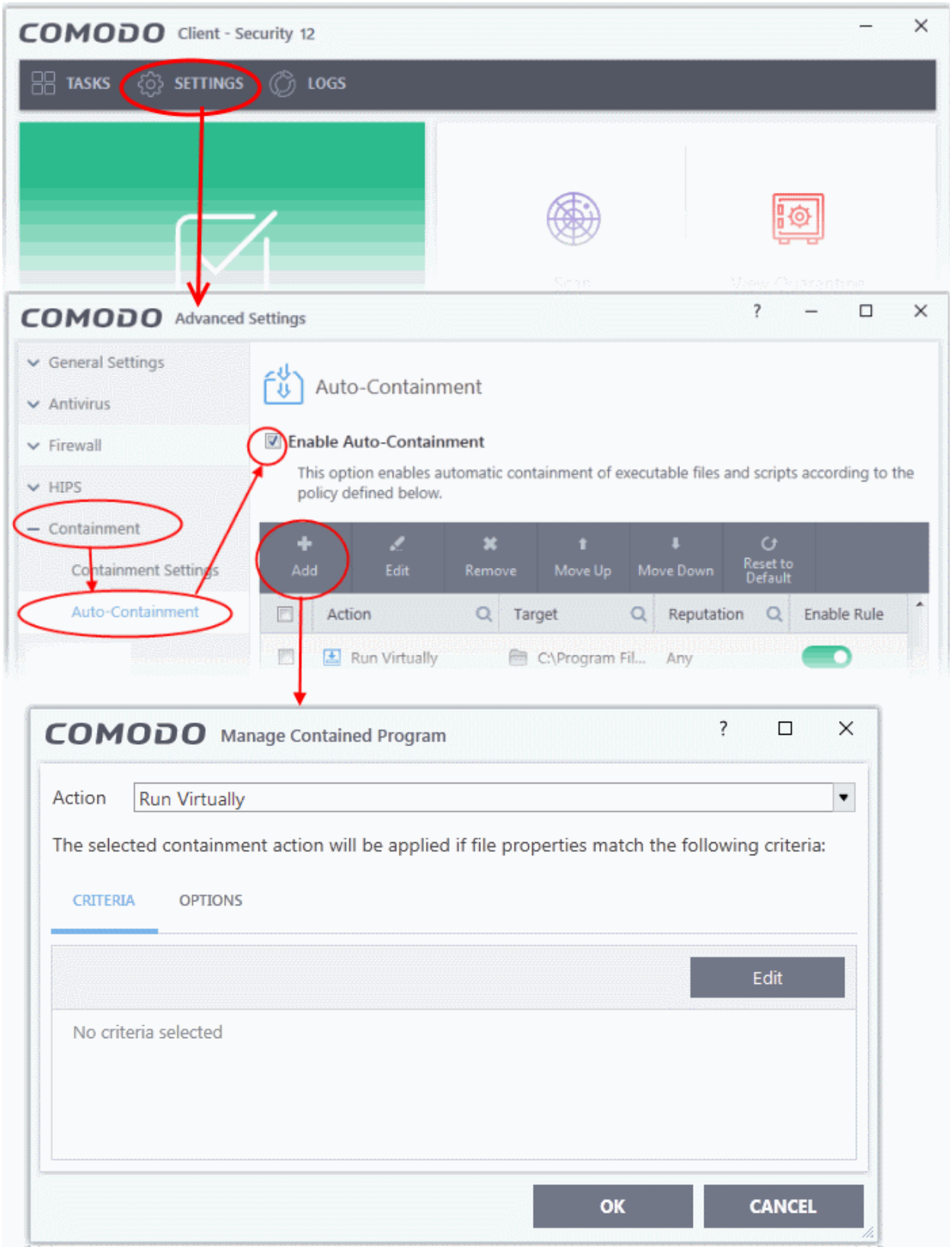
Click here for more details on HIPS Settings

Create Rules to Auto-Contain Applications

- Click 'Settings' > 'Containment' > 'Auto-Containment'
- Auto-containment rules let you define which types of files should automatically run in the container.
- You can contain files based on various criteria, including location and file source.
- A contained application has much less opportunity to damage your computer because it runs isolated from your operating system and your files.
- CCS ships with some pre-defined rules configured to provide maximum protection for your system. **Click here** to check whether these rules meet your needs before creating a custom rule.
- The rest of this tutorial explains how to create a custom auto-containment rule.

Create auto-containment rules

1. Click 'Settings' on the CCS home screen
2. Click 'Containment' > 'Auto-Containment'
3. Make sure 'Enable Auto-Containment' is selected
4. Click 'Add'



The add rule screen contains two tabs:

- **Criteria** - Define the conditions of the rule.
- **Options** - Configure additional actions like logging, memory usage and time restrictions.

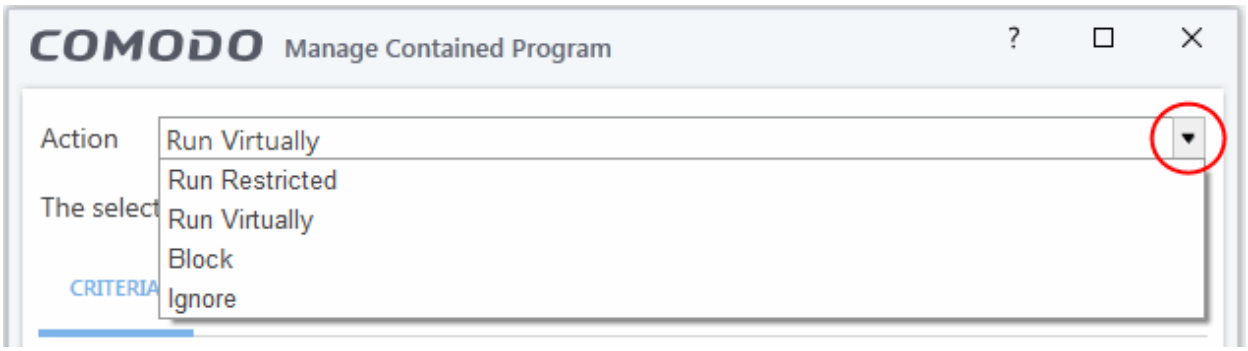
There are three steps:

- **Step 1 - Choose the action**

- Step 2 - Select the rule targets
- Step 3 - Choose additional options

Step 1 - Choose the action

The setting in the action drop-down combined with the restriction level in the options tab determine the privileges of an auto-contained application. These items specify what right the application has to access other processes and hardware resources.



Choose one of the following actions:

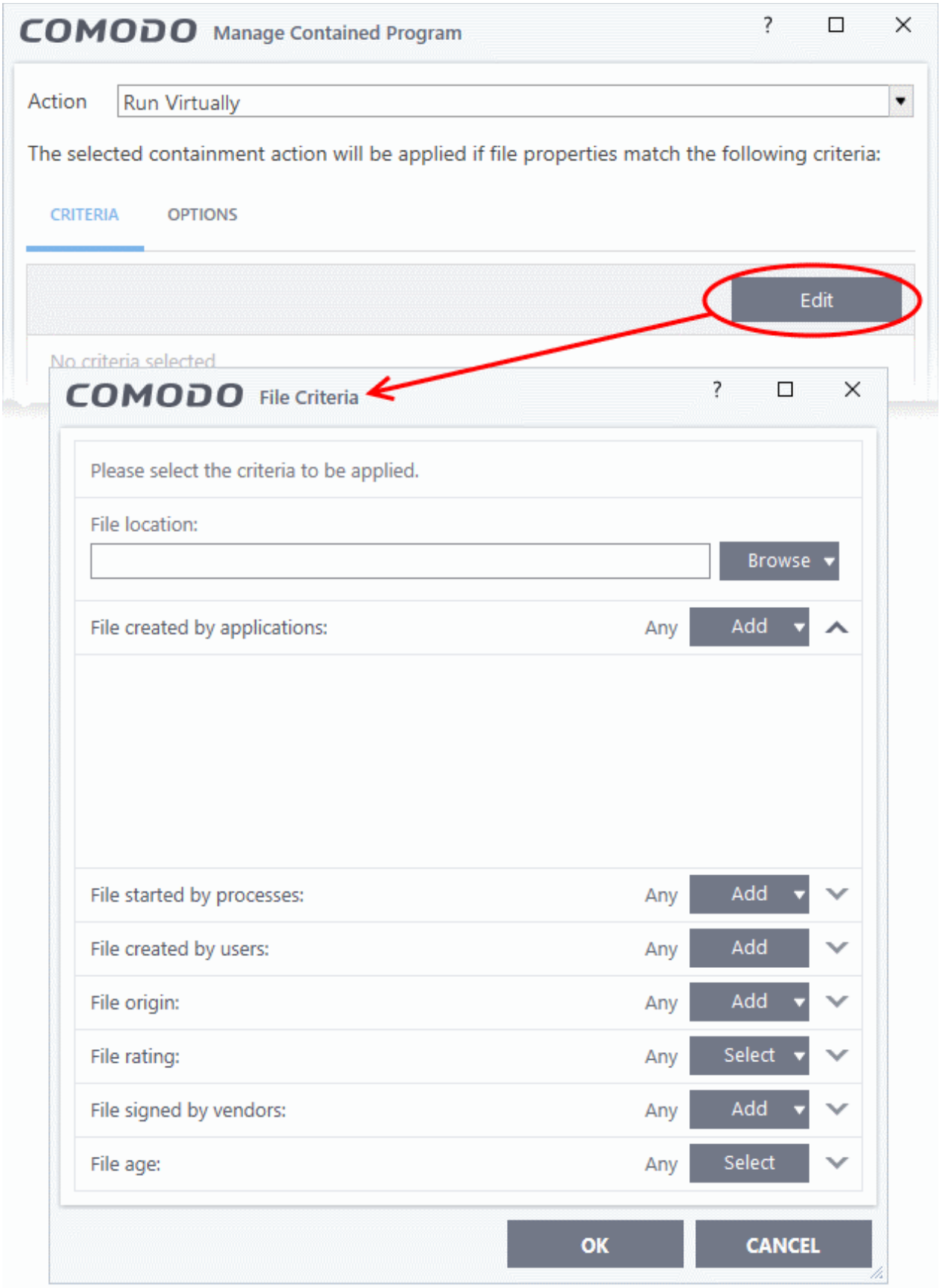
- **Run Virtually** - The application will run in a virtual environment, completely isolated from your operating system and the rest of your files.
- **Run Restricted** - The application is allowed limited access to operating system resources. The application is not allowed to execute more than 10 processes at a time. Some applications, like games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application is not contained. It is allowed to run as normal on your computer.

Step 2 - Select the rule targets

- Next, select the types of files which will be covered by your rule.
- You can add rule filters so the rule only applies to specific types of file.
  - For example, you can specify 'All executables' as the target and add a filter so it only affects executables downloaded from the internet.
  - Another example is if you want to allow unrecognized files created by a specific user to run outside the container. You would create an 'Ignore' rule with 'All Applications' as the target and 'File created by specific user' as the filter criteria.

Select targets and filters

- Click the 'Criteria' tab.
- Click the 'Edit' button at the far right:

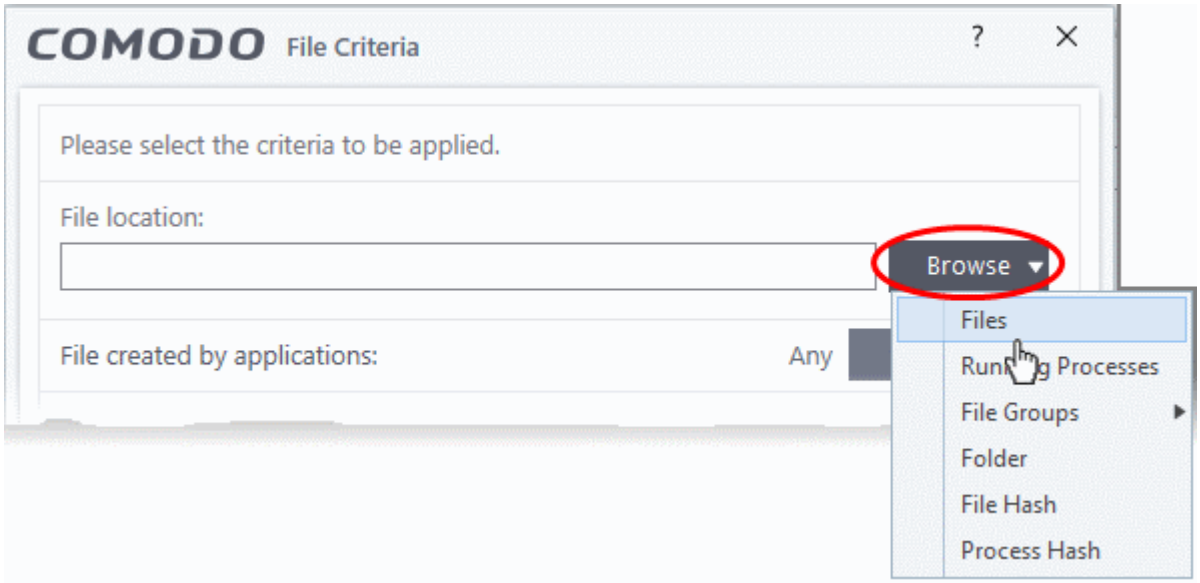


Next:

- **Select the target**
- **Configure the filters**

Select the target

- Click the browse button next to the file location field:

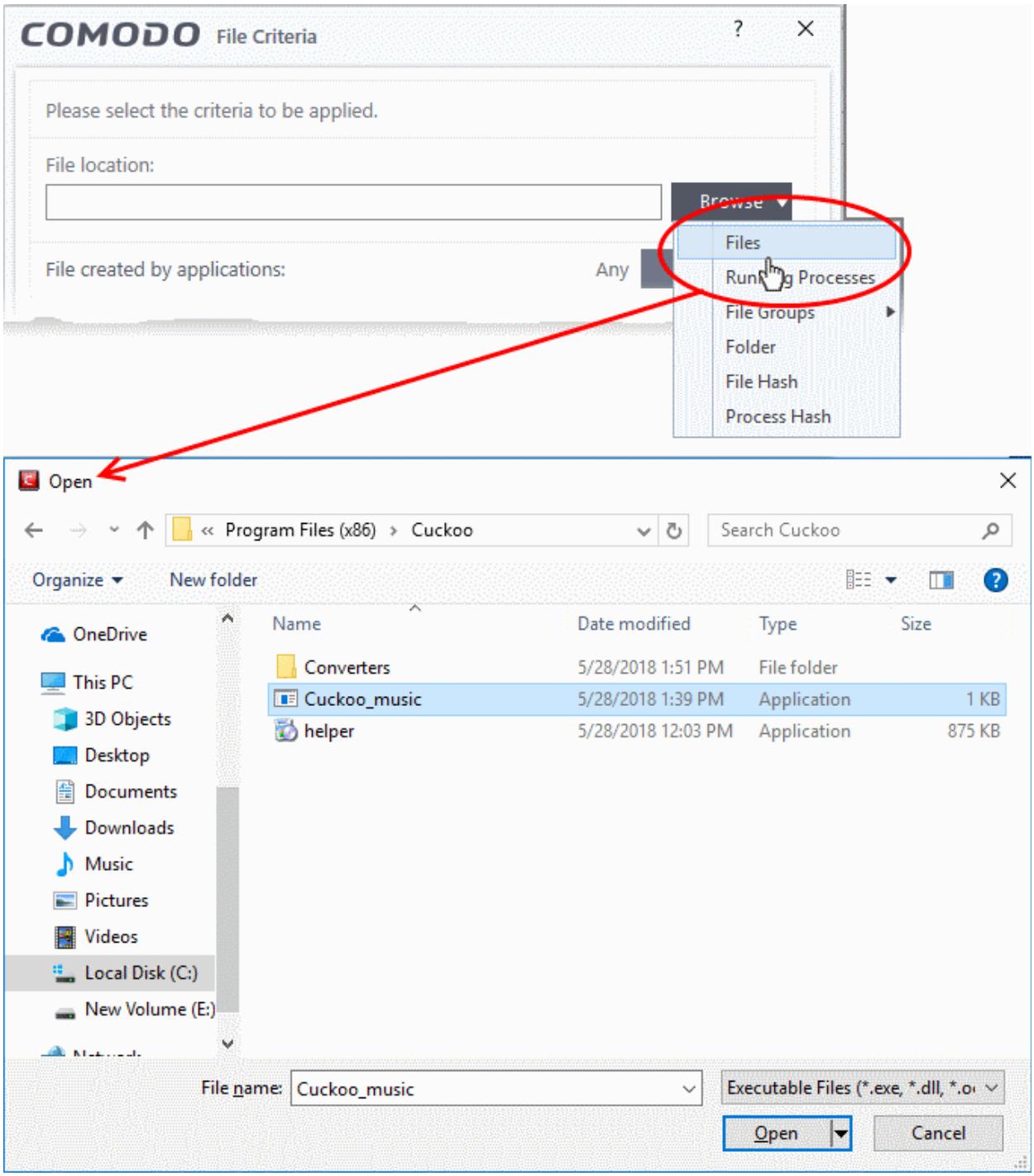


Select one of the following target types:

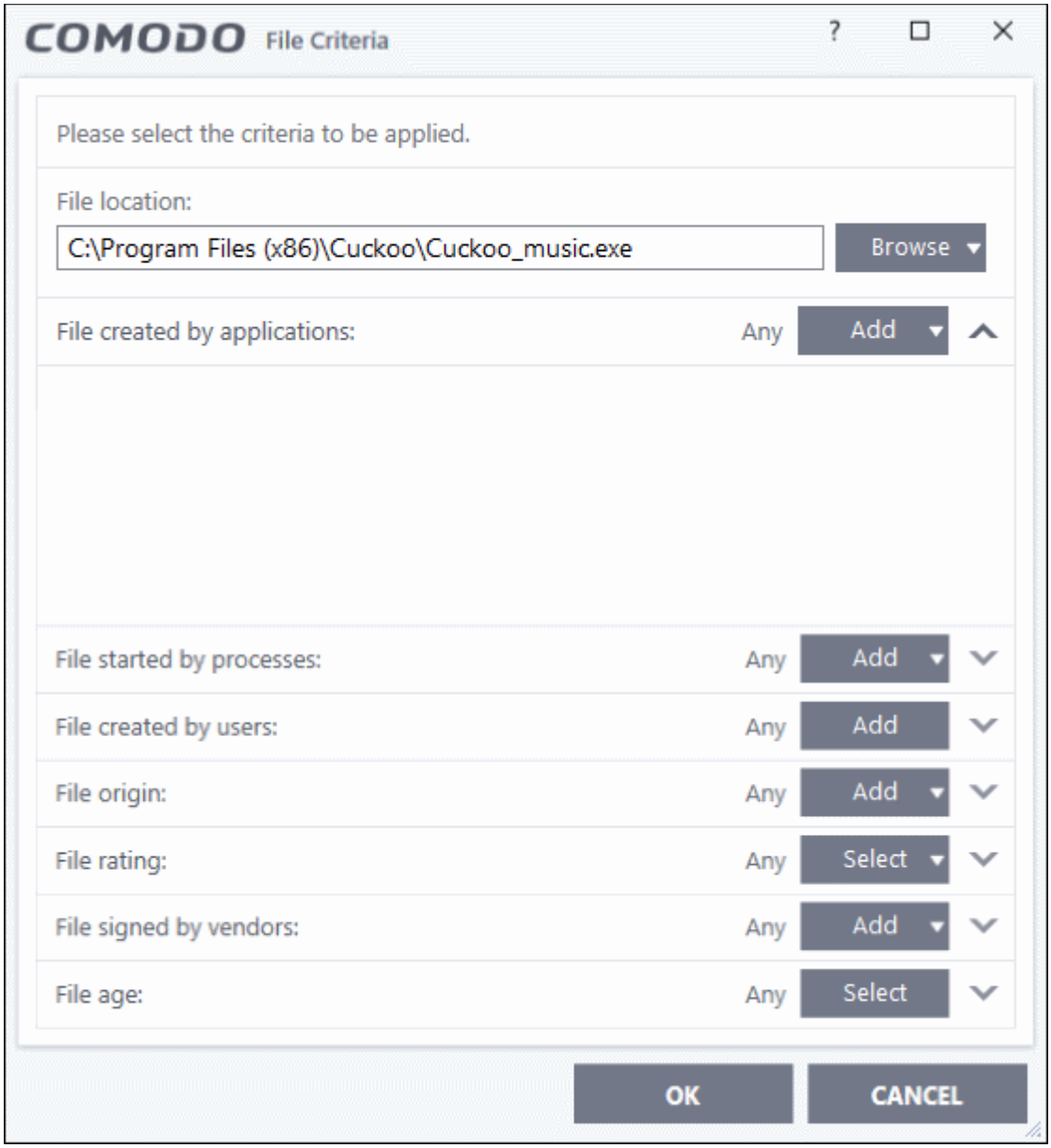
- **Files** - Add individual files as the target.
- **Running Processes** - Add any process that is currently running on your computer. This targets the parent application of the process.
- **File Groups** - Add a predefined file group as the target. For example, the 'Executables' group contains a list of file types that can run code on your computer. Click 'Settings' > 'File Rating' > 'File Groups' to add or modify a file group.
- **Folder** - Add a directory or drive as the target. All files in the target folder are covered by the rule.
- **File Hash** - Add a file's hash value as the target of the rule. A hash value is a number derived from the file itself, which uniquely identifies and represents the file. It is extremely unlikely that two files can ever generate the same hash value. The rule will apply to the target file, even if the file name changes.
- **Process Hash** - Add a processes hash value as the target of the rule. Please see description above if required.

Add an individual File

- Choose 'Files' from the 'Browse' drop-down.



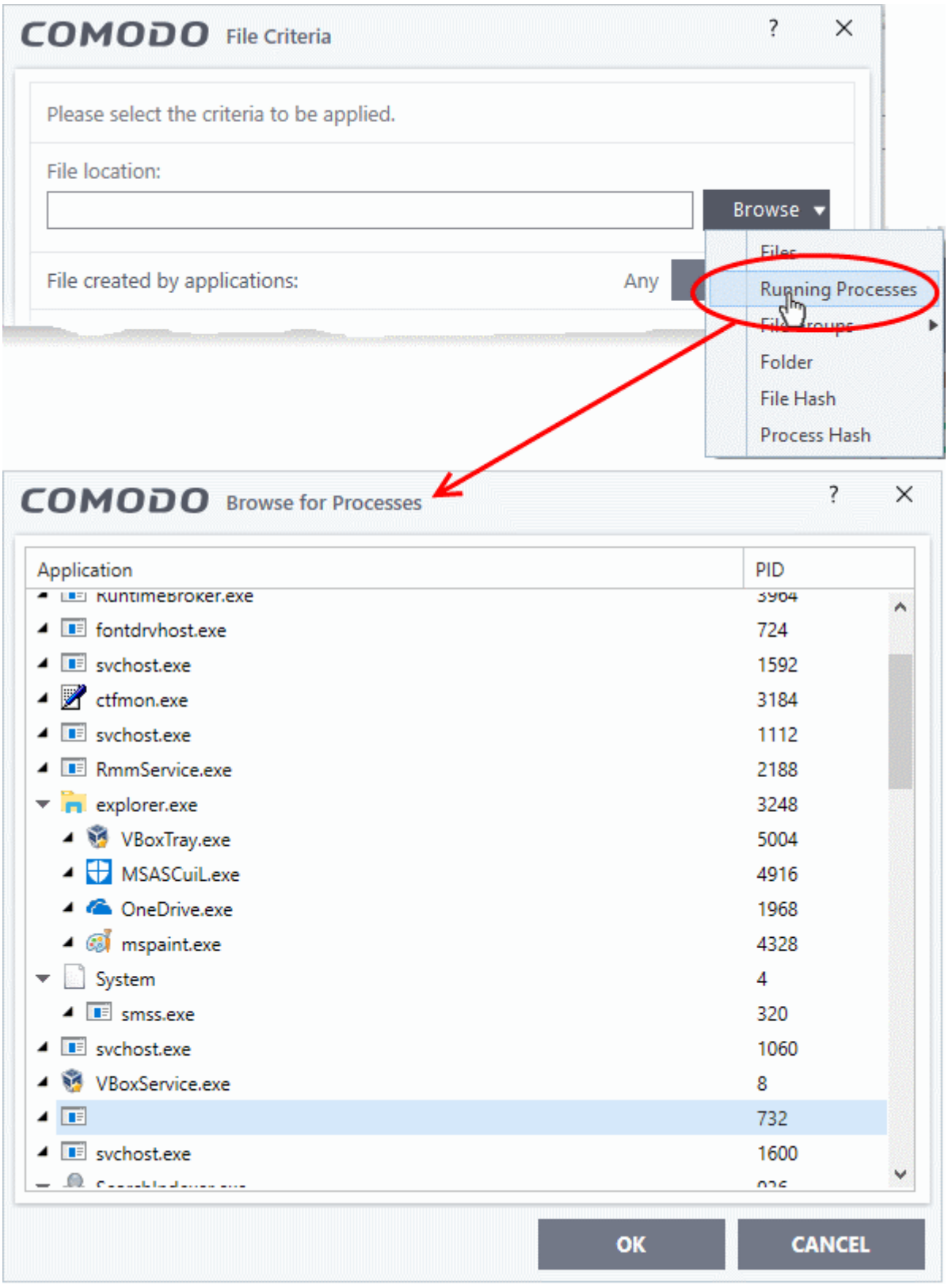
- Navigate to the target file and click open
- The file will be added as the target and run as per the action chosen in **Step 1.**



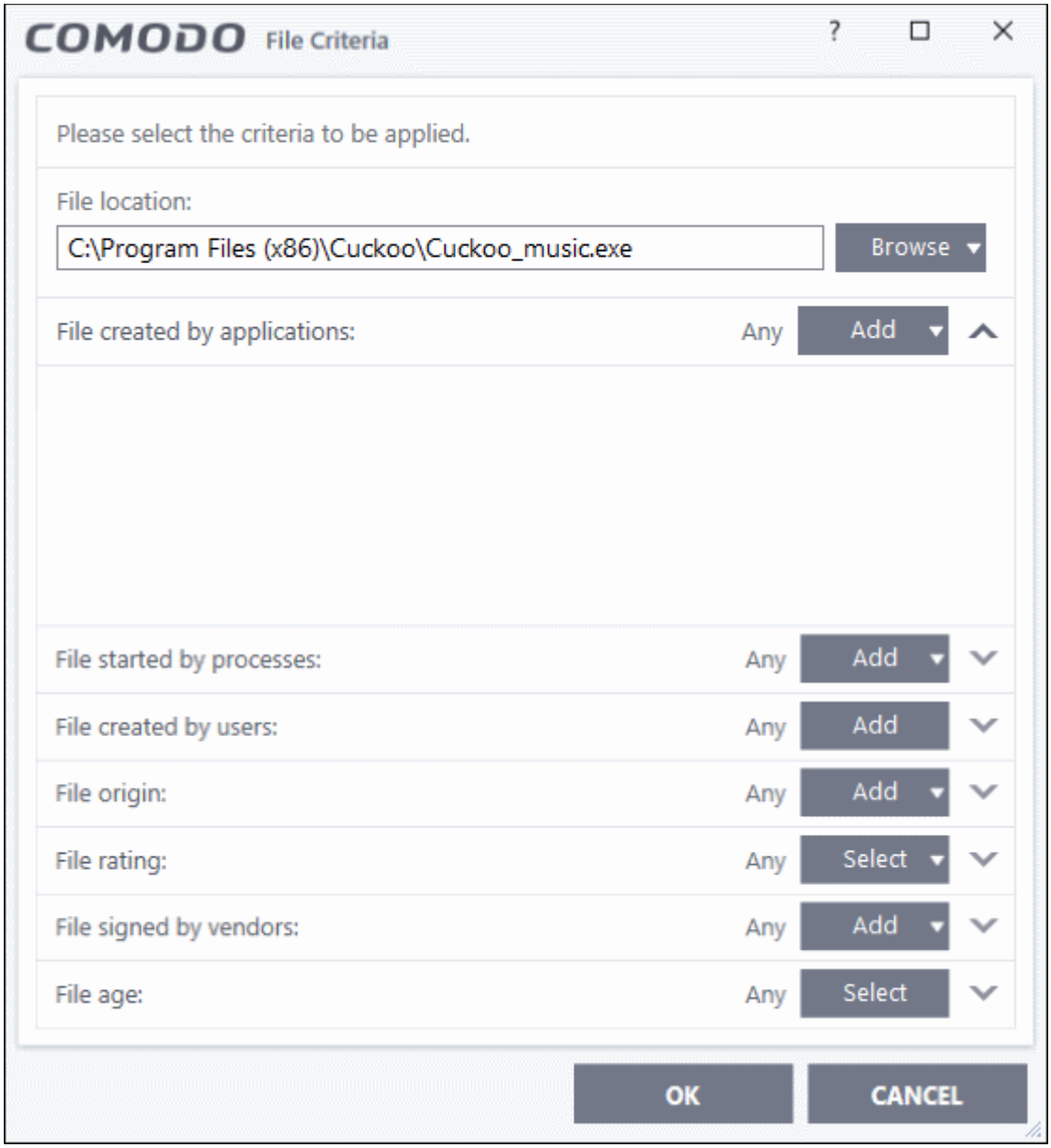
- Click 'OK' if you don't want to specify any filters or options.
- If required ,you can **configure filter criteria and file rating** and **options** for the rule.

Add a currently running process

- Choose 'Running Processes' from the drop-down:



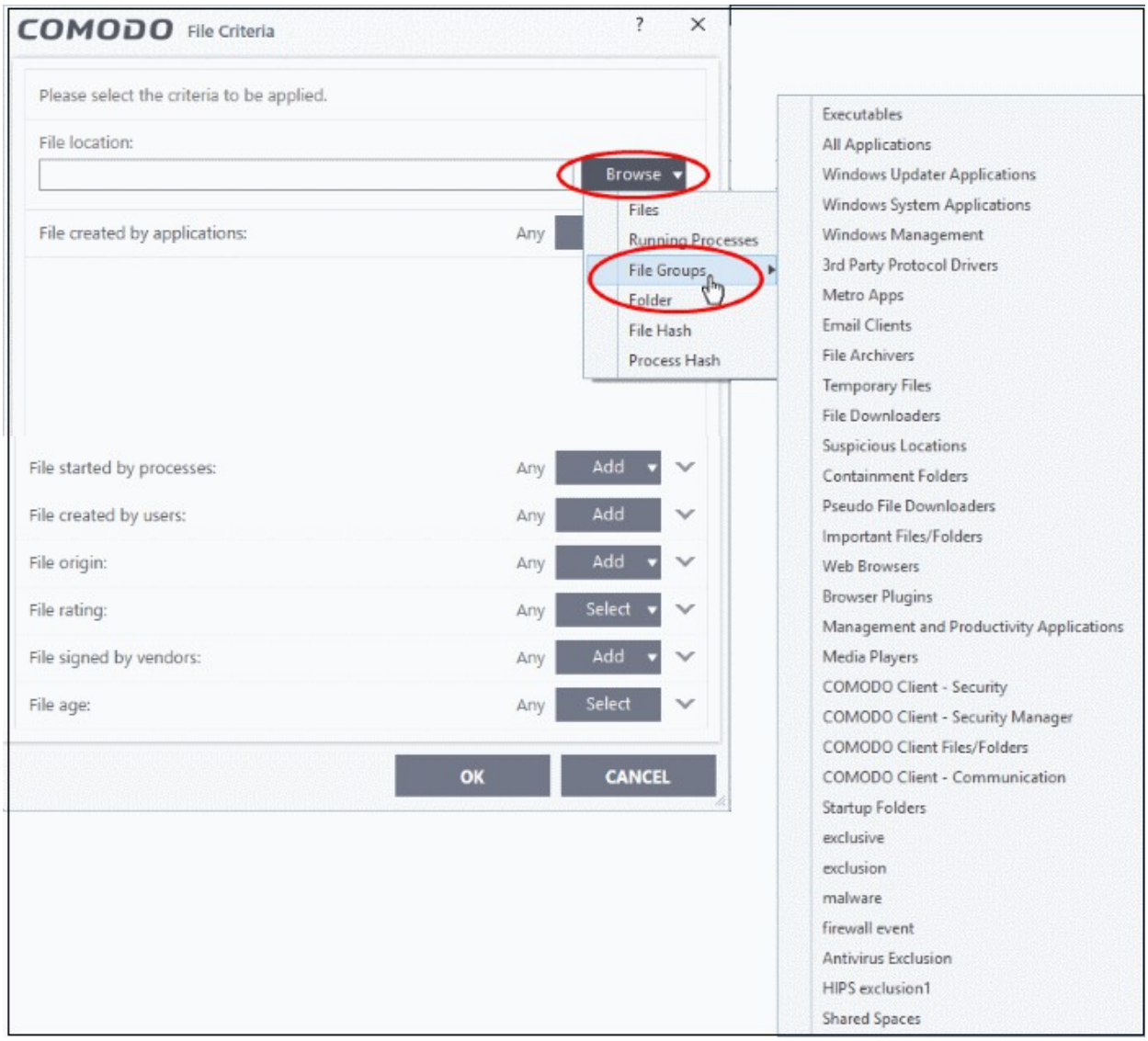
- Select the process belonging to the parent application you want to add and click 'OK'.
- The parent application of the process will be added as the target.



- Click 'OK' if you don't want to specify any filters or options.
- If required ,you can **configure filter criteria and file rating** and **options** for the rule.

Add a file group

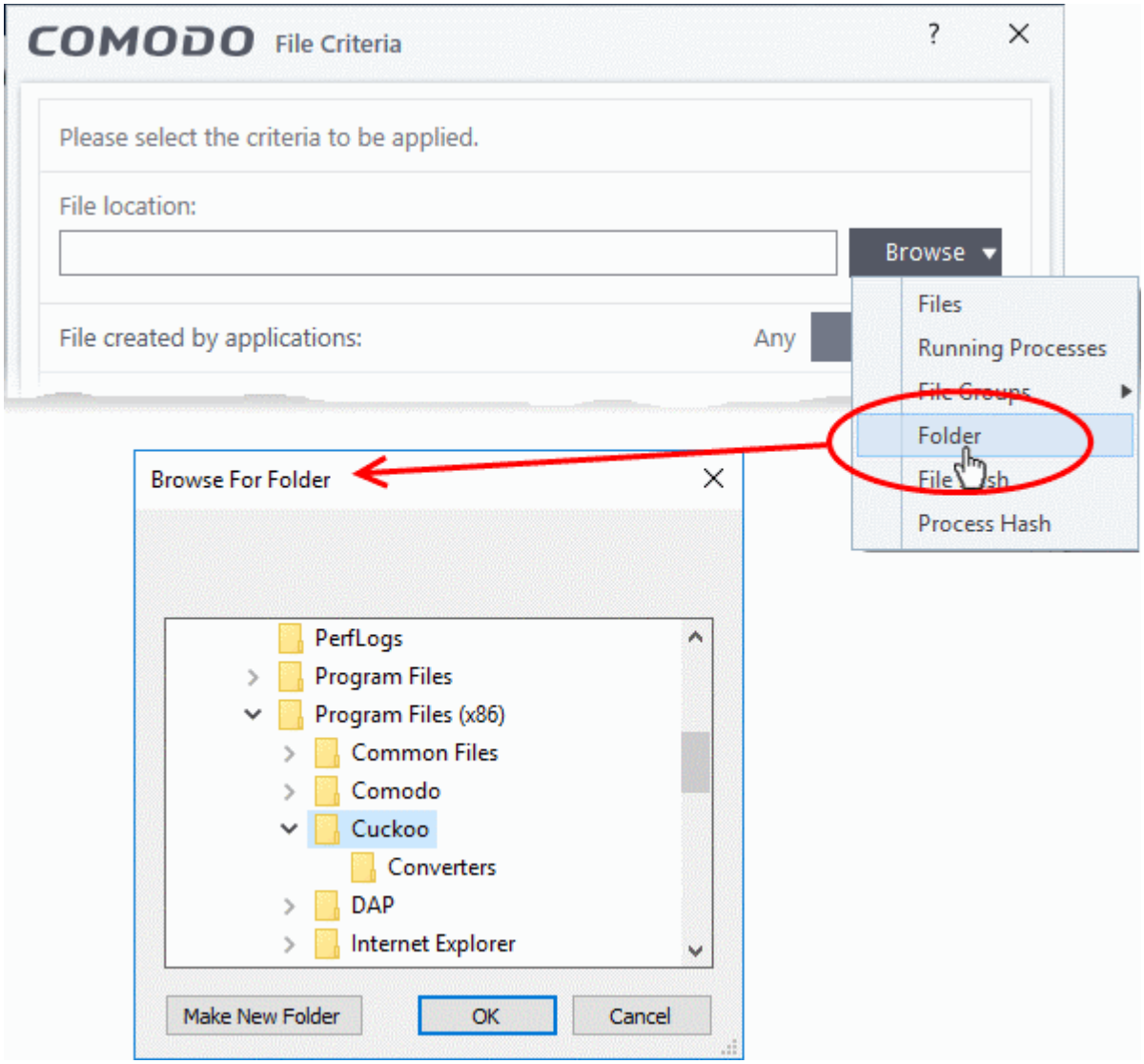
- Choose 'File Groups' from the drop-down.
  - For example, the 'Executables' group contains a list of file types that can run code on your computer. Click 'Settings' > 'File Rating' > 'File Groups' to add or modify a file group.
- Select the file group you want to target with the rule:



- Click 'OK' if you don't want to specify any filters or options.
- If required, you can **configure filter criteria and file rating** and **options** for the rule.

Add a folder/drive partition

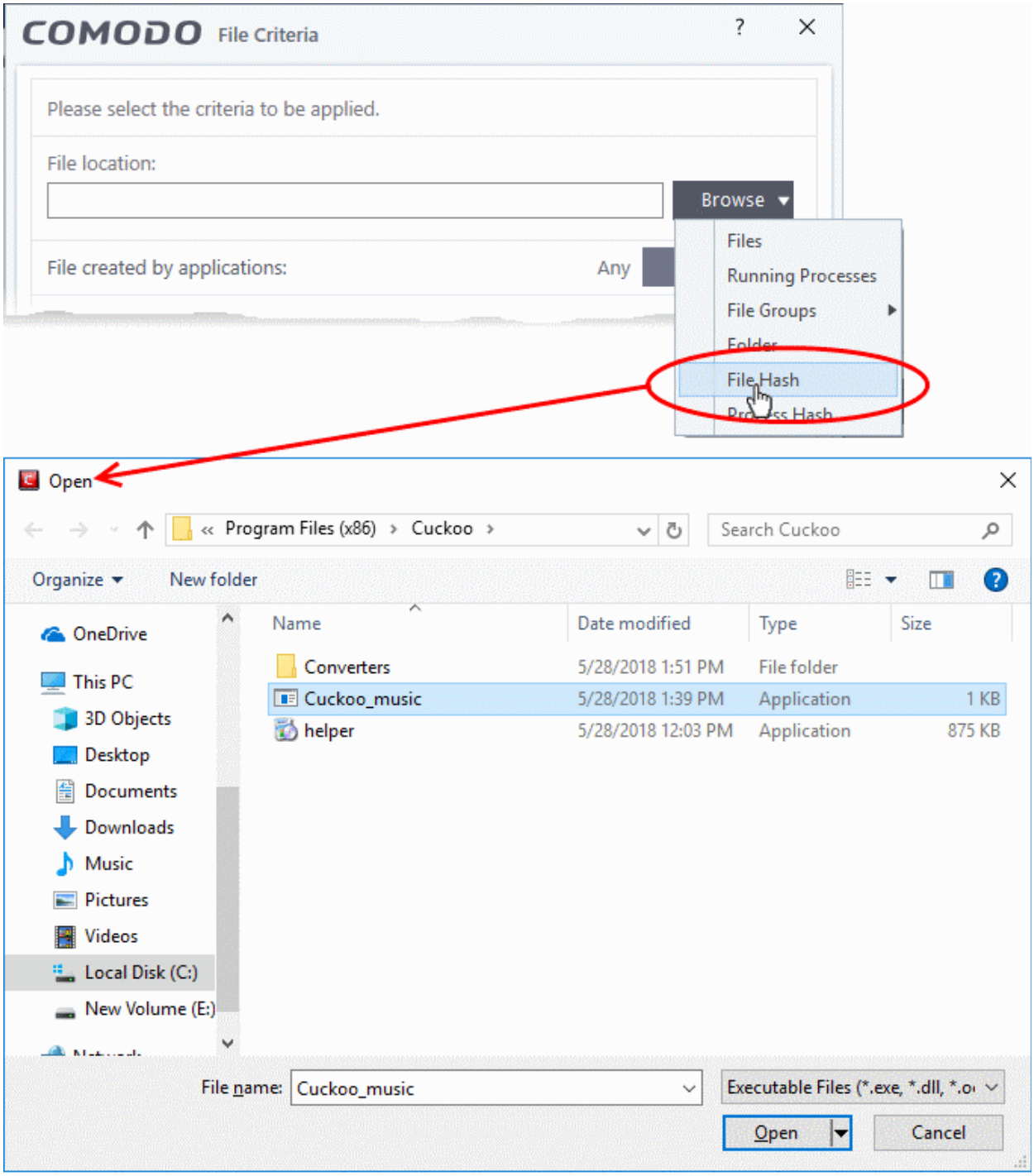
- Choose 'Folder' from the 'Browse' drop-down.



- Navigate to the drive partition or folder you want to add as target and click 'OK'
- Click 'OK', if you don't want to specify any filters or options.
- If required you can **configure filter criteria and file rating** and **Options** for the rule.

Add a file using its hash value

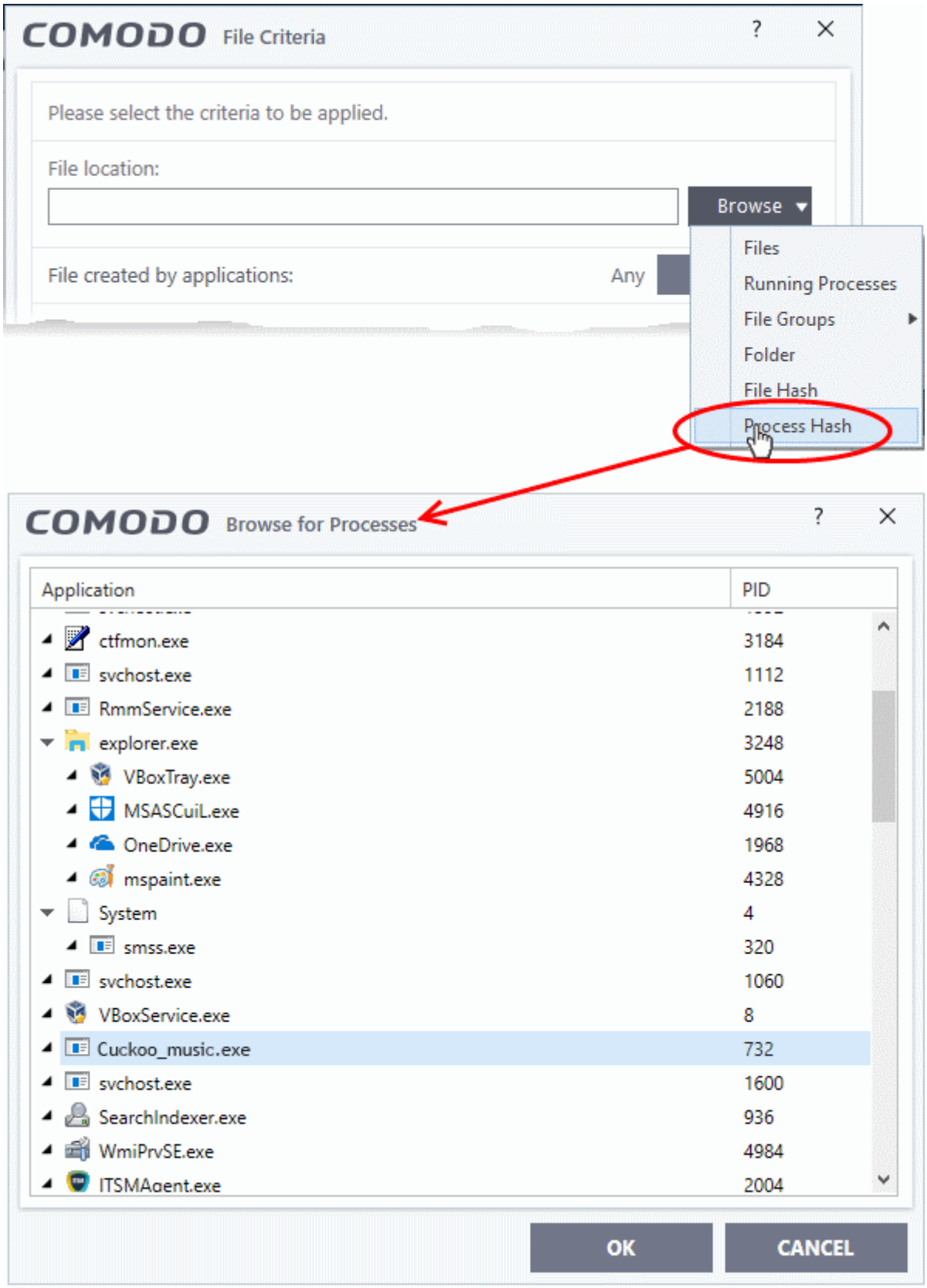
- Choose 'File Hash' from the drop-down.



- Navigate to the file whose hash value you want to add as target and click 'Open'
- Click 'OK', if you don't want to specify any filters or options.
- If required you can **configure filter criteria and file rating** and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.
- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

Add an application from a running process based on its hash value

- Choose 'Process Hash' from the drop-down.



- Select the process, to add the hash value of its parent application to target and click 'OK' from the 'Browse for Process' dialog.
- Click 'OK', if you don't want to specify any filters or options.
- If required you can **configure filter criteria and file rating** and **options** for the rule.
- CCS generates the hash value of the parent file and stores that as the target.

- CCS uses this hash value to identify the file and apply the rule, so that the rule intercepts the target even if the file name changes.

Configure Filter Criteria and File Rating

You can apply an action to a file if it meets certain criteria.

The available filter criteria are:

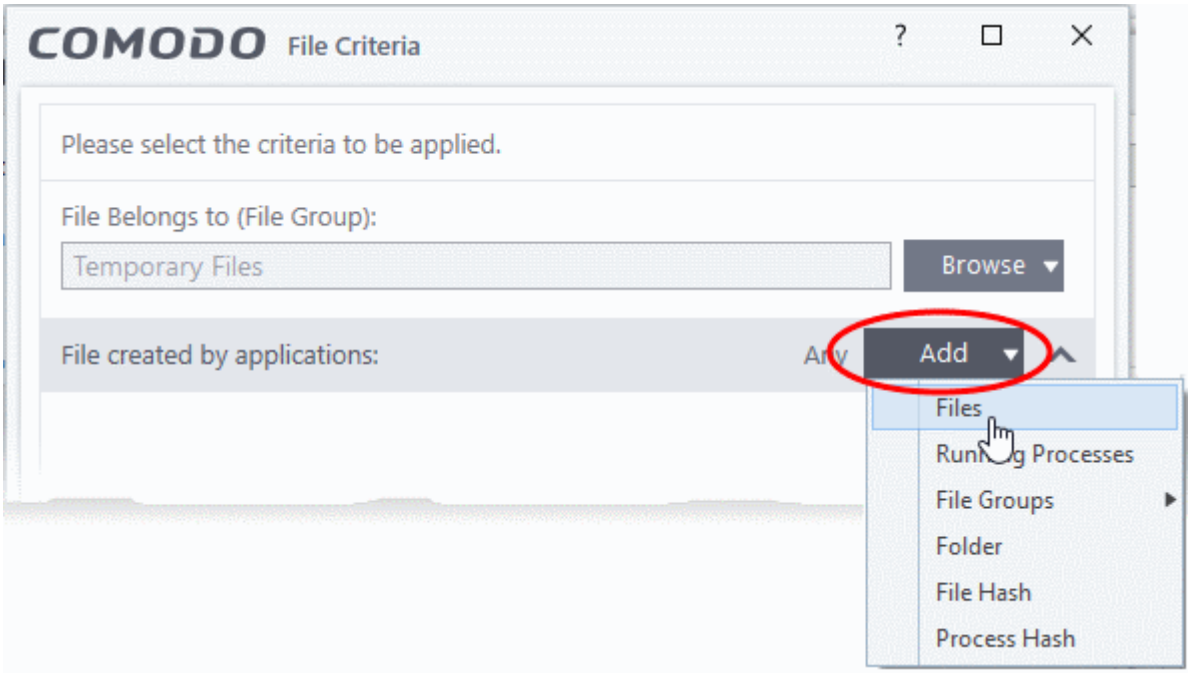
- **By application that created the file**
- **By process that created the file**
- **By user that created the file**
- **By file origin**
- **By file rating**
- **By vendor who signed the file**
- **By file age**

Auto-contain a file if it was created by a specific application

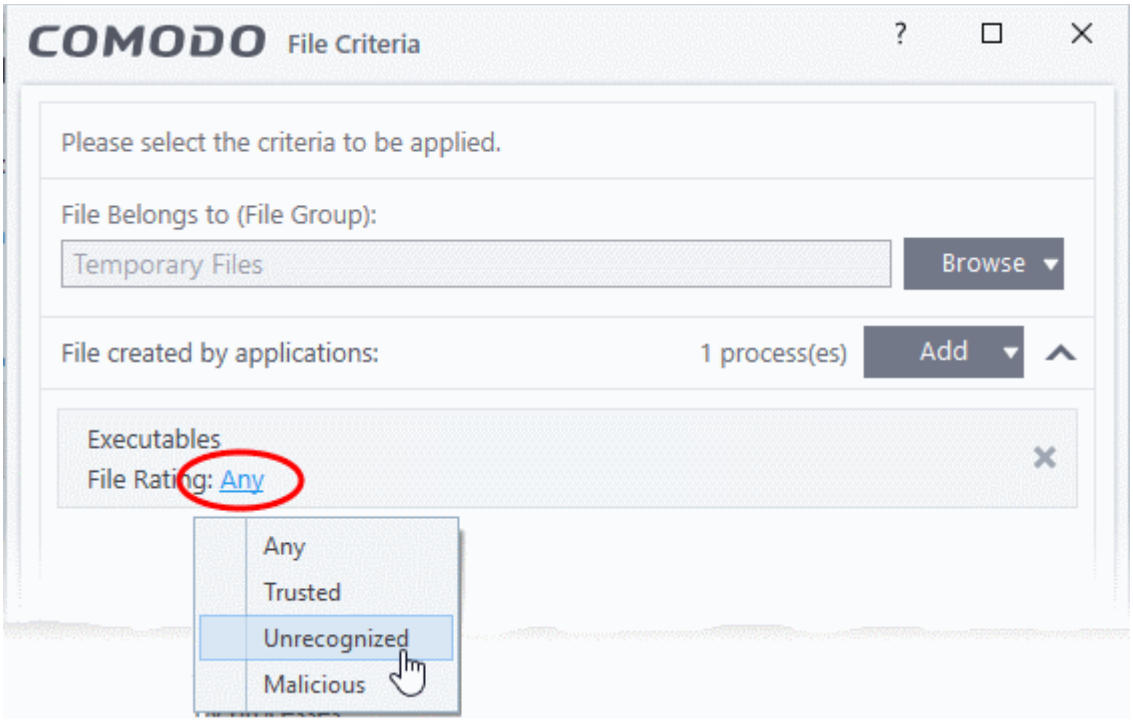
- This will apply the rule to a file based on its parent application.
- You can also specify the file rating of the parent application. The rule will then only contain a file if the parent app has a certain trust rating.

Specify parent applications:

- Click the add button in the 'File created by applications' stripe:



- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.
- Click the 'Any' link beside 'File Rating' and select the file rating of the source



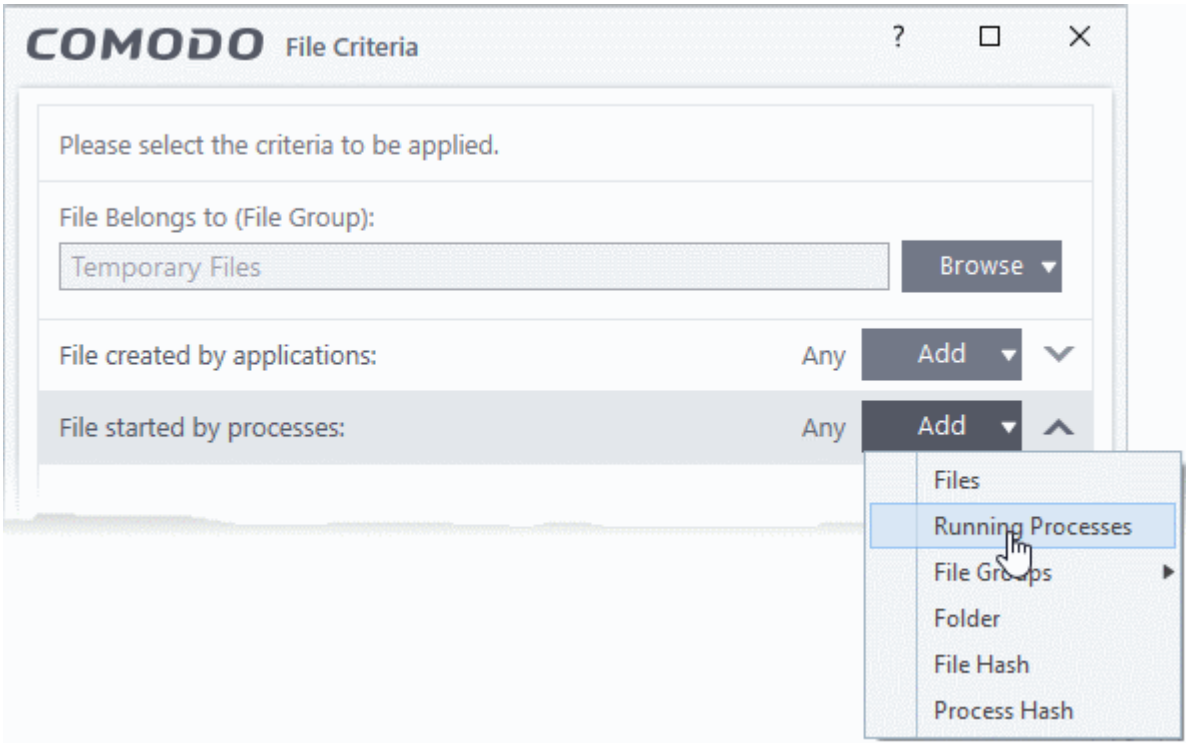
- Repeat the process to add more applications or groups/folders.

Auto-contain a file if it was launched by a specific process

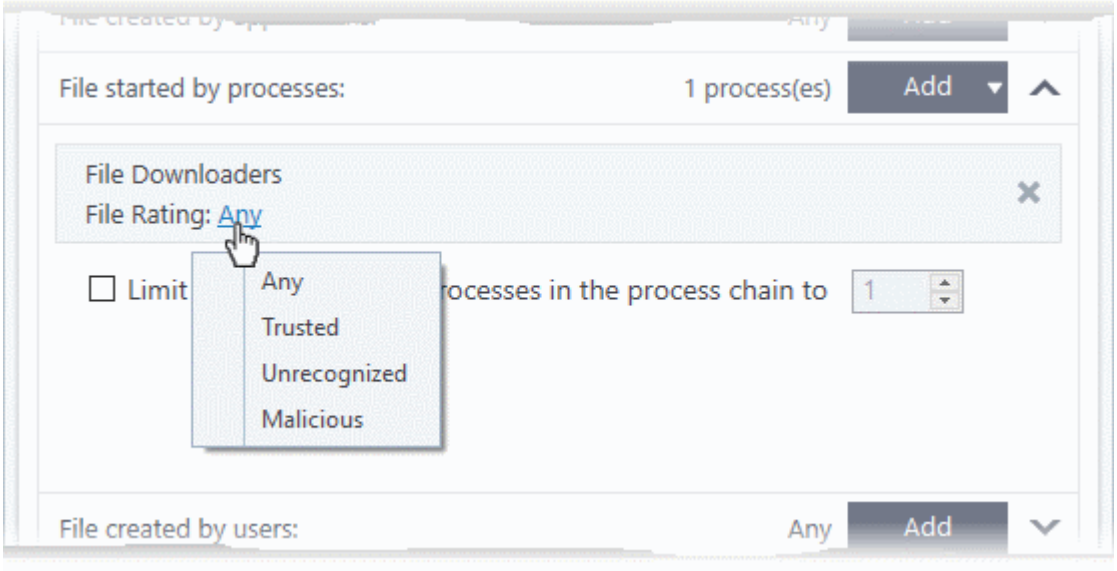
- This will apply the rule to a file based on its based on its parent process.
- You can also specify:
  - The trust rating of the parent process. The rule will then only contain a file if the parent process has a certain trust rating.
  - The number of levels in the process chain that should be inspected.

Specify source process:

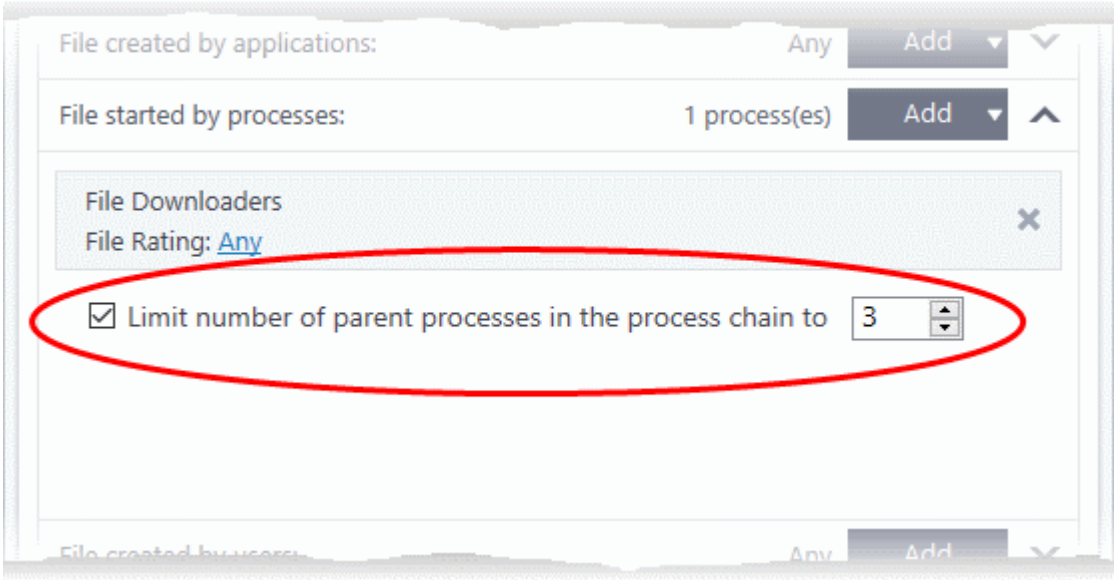
- Click the 'Add' button in the 'File started processes' stripe:



- The options available are same as those available under the 'Browse' button beside 'File location', as explained **above**. See the previous section for each of options for more details.
- Click the 'Any' link beside 'File Rating' and select the file rating of the source



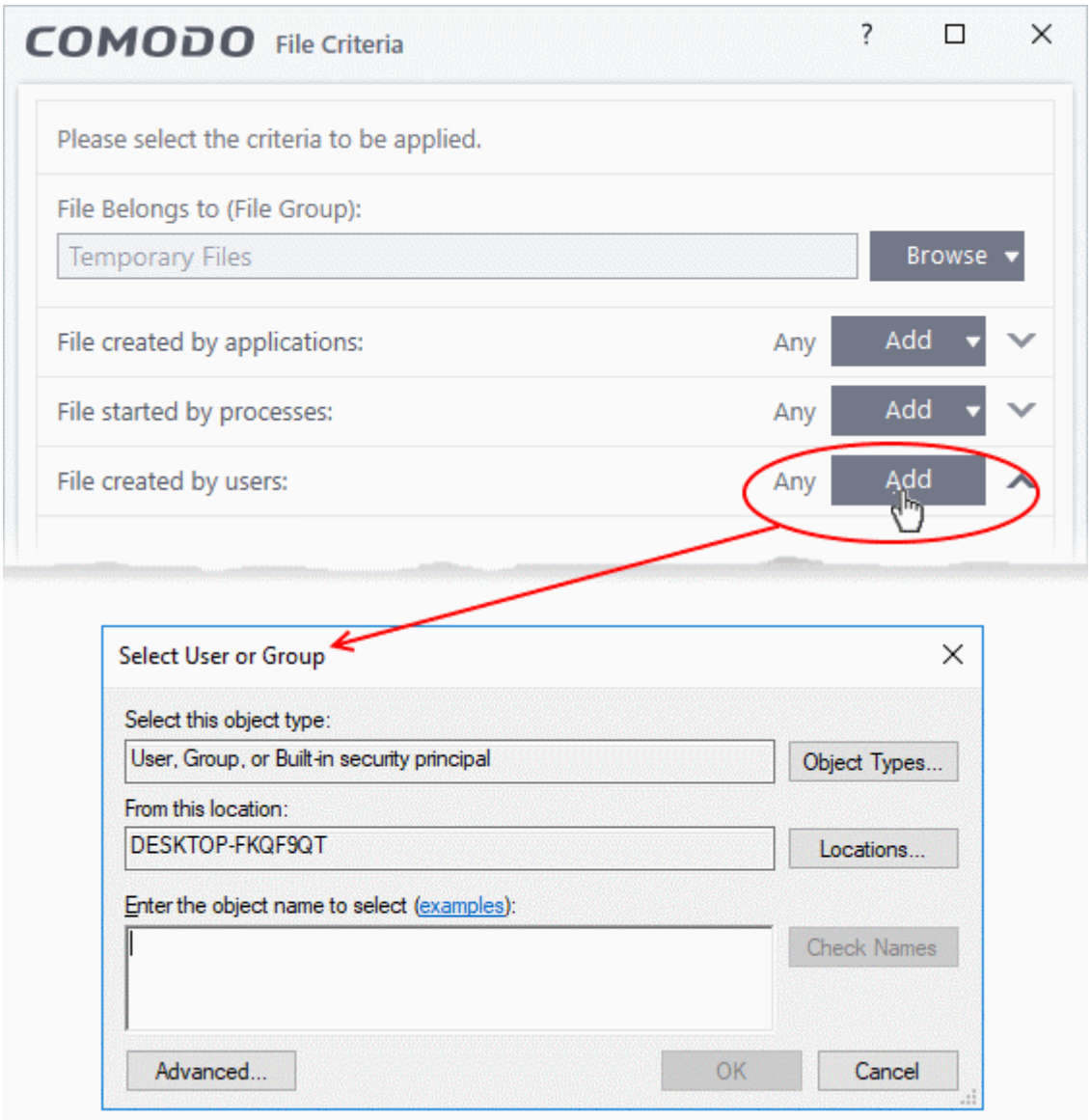
- '**Limit number of parent processes in the process chain to**' - Specify how far up the process tree CCS should check. 1 = will only check the trust rating of the file's parent process. 2 = will check the trust rating of the parent process and the grand-parent process. Etc.



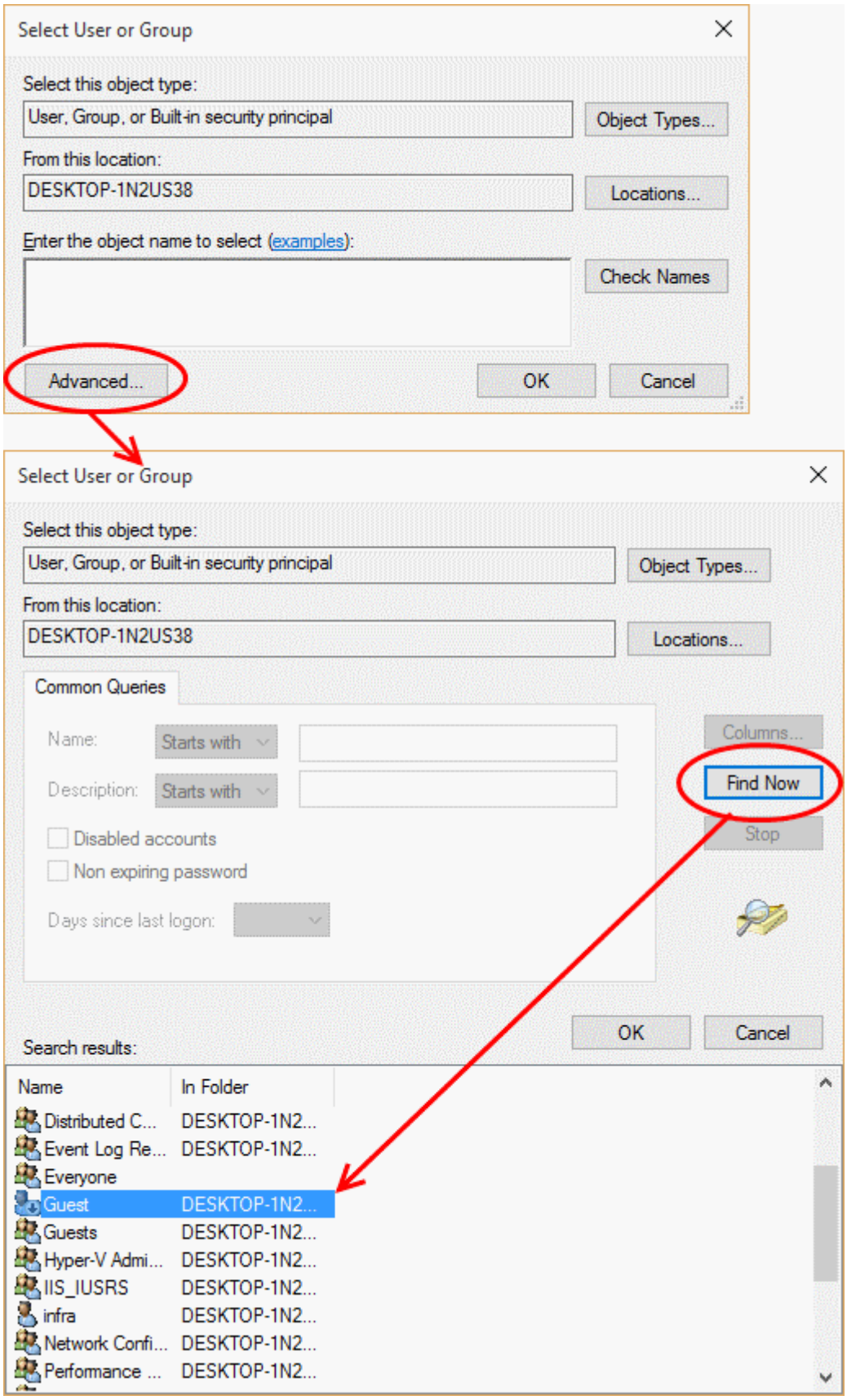
- Repeat the process to add more processes

Auto-contain a file created by specific users

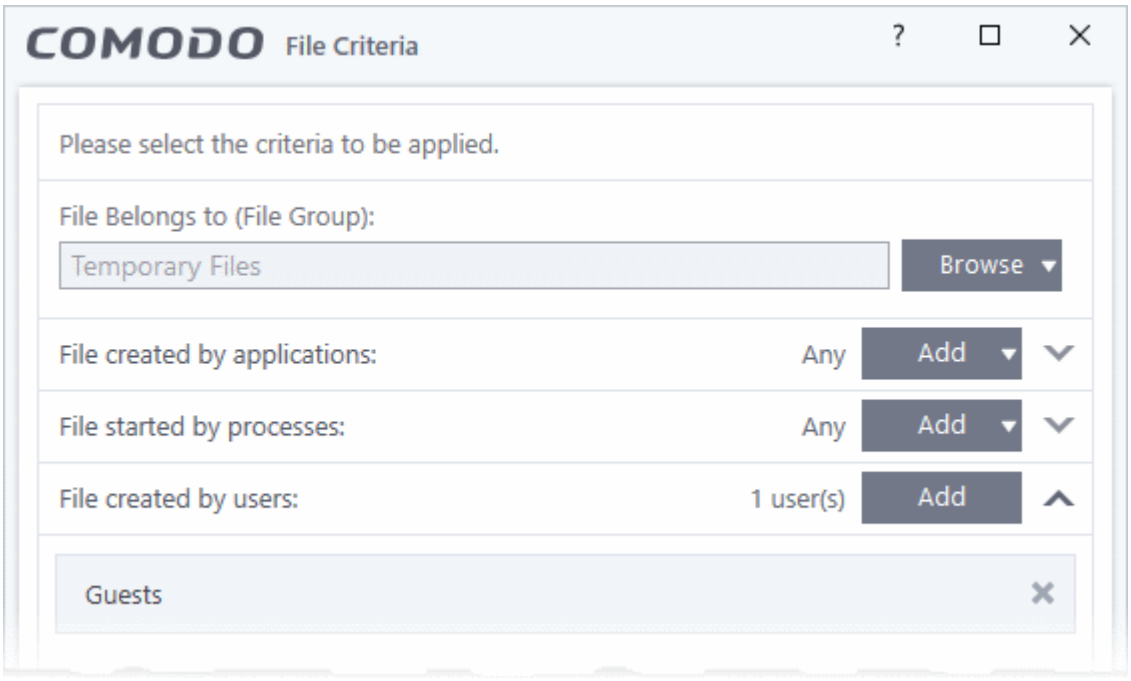
- Click the 'Add' button in the 'File created by users' stripe.



- Enter the names of the users you want to add in the large text box.
- Name format = <domain name>\<user/group name>, or <user/group name>@<domain name>.
- Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm your choice.



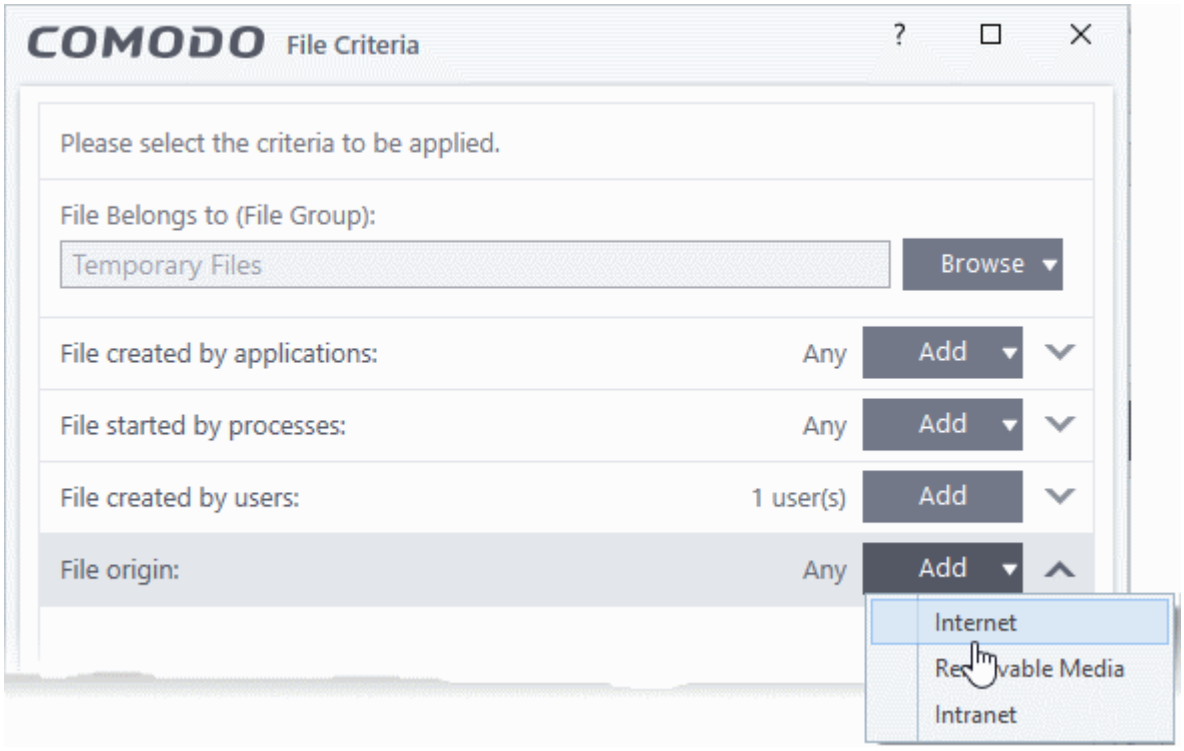
The user will be added to the list.



- Repeat the process to add more users.

Auto-contain a file if it was downloaded/copied from a specific source

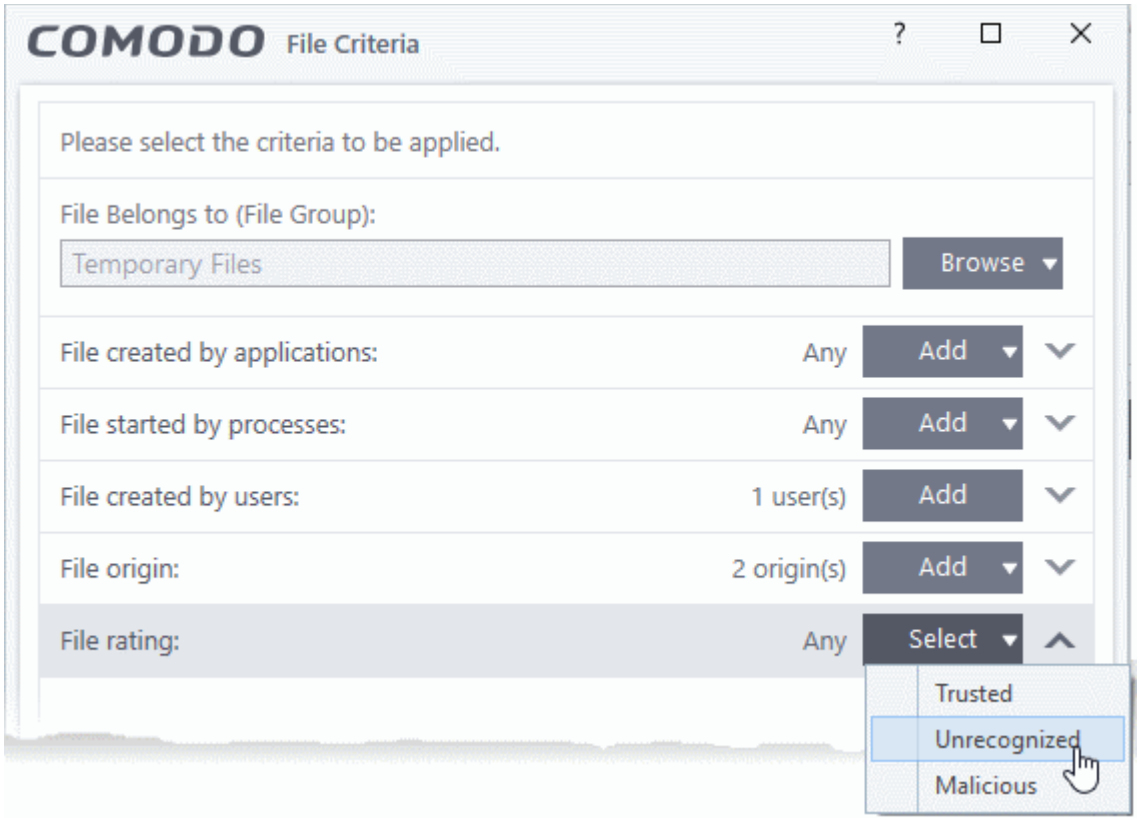
- Click the 'Add' button in the 'File origin' stripe.



- Choose the source from the options:
  - **Internet** - Apply the rule to files that were downloaded from the internet.
  - **Removable Media** - Apply the rule to items copied to your computer from removable storage devices.
  - **Intranet** - Apply the rule to files downloaded from the local intranet.
- Repeat the process to add more sources

Select file rating as filter criteria

- Click the 'Select' button in the 'File Rating' stripe



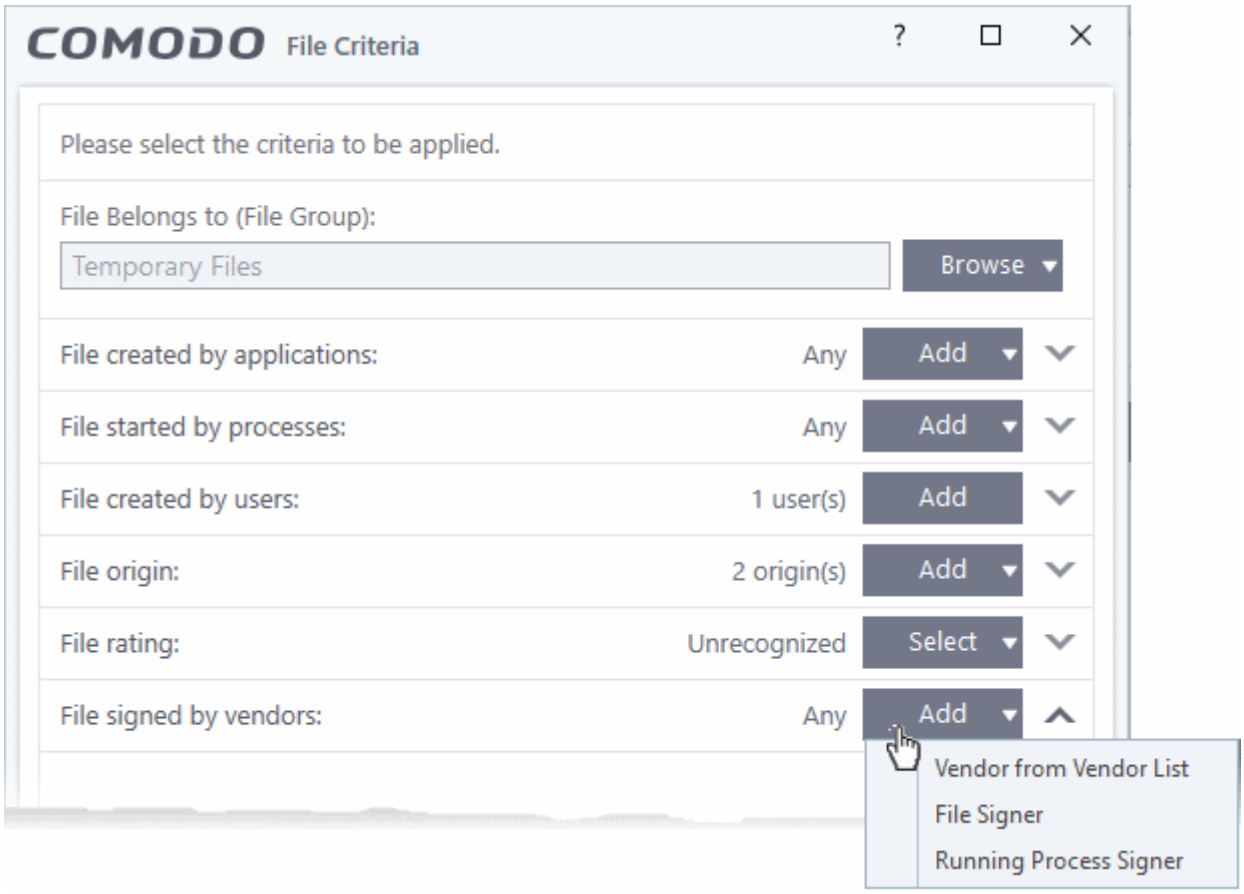
- **Trusted** - A file will have a trusted rating if:
  - The file is on the Comodo whitelist of safe files
  - The file is signed by a vendor who has a trusted rating in 'Settings' > 'File Rating' > 'Vendor List'
  - The file was installed by trusted installer
  - The user has given the file a trusted rating in 'Settings' > 'File Rating' > 'File List'
  - See **File Rating Settings** for more information.
- **Malware** - The file has a trust rating of 'Malicious'.
- **Unrecognized** - Any file that does not have a 'Trusted' or 'Malicious' rating is classed as 'Unrecognized'. Although these files may not turn out to be malicious, Comodo auto-contains these files until we have established their true trust rating.

Auto-contain a file based on software vendor

- You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.
- You can also specify the trust rating of the vendor. The rule will only contain a file if its vendor has the stated trust rating.

Choose vendors:

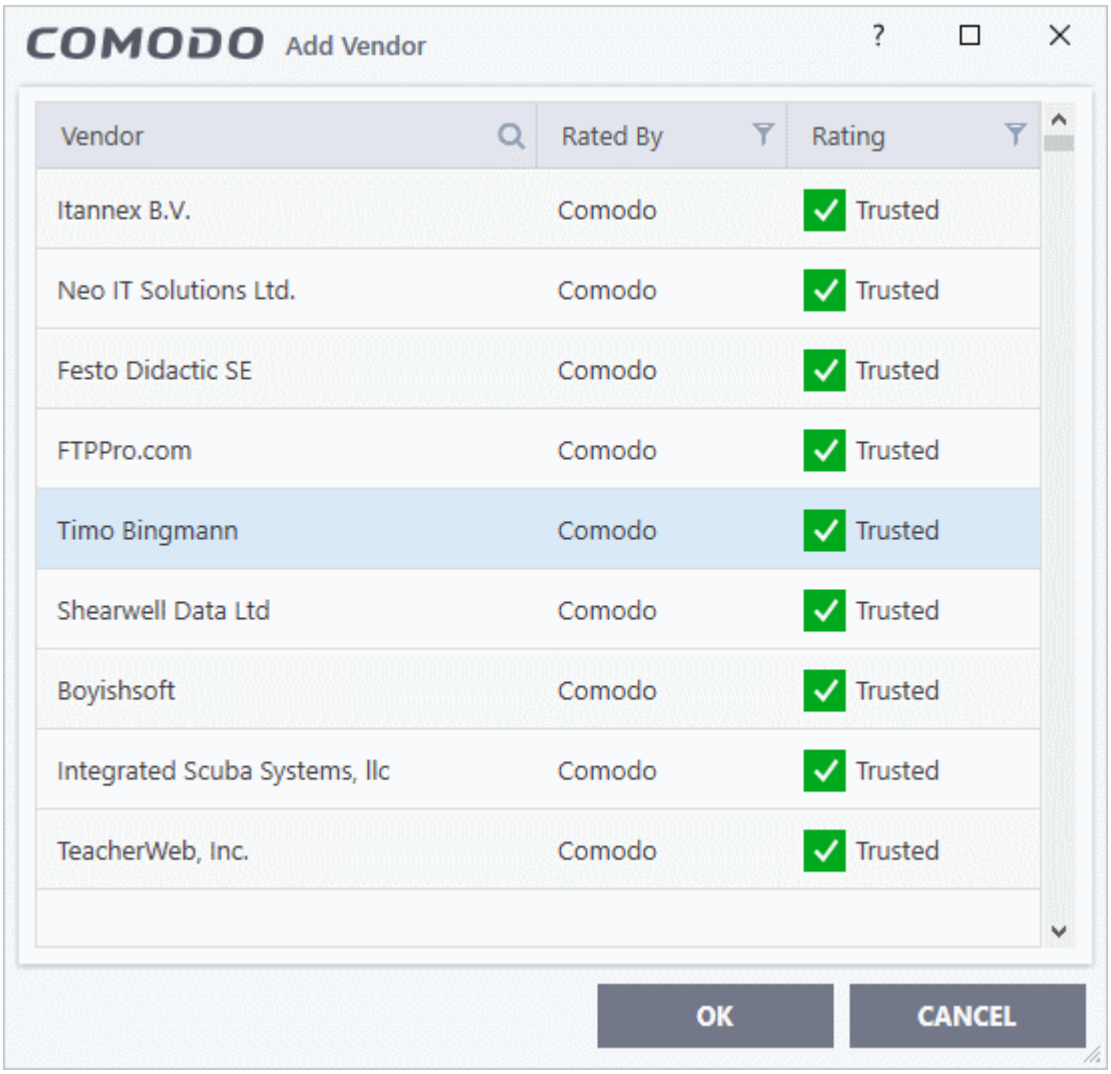
- Click the 'Add' button in the 'File signed by vendors' stripe.



- There are three ways you can add a vendor:

  1. Directly select a vendor

  - Choose 'Vendor from a Vendor List' from the drop-down
  - The 'Add Vendor' dialog opens with a list of vendors in the **Vendor List**



- Use the sort and filter options in the column headers to search for the vendor to be specified
- Choose the vendor and click 'OK'. The vendor will be added as a criterion.

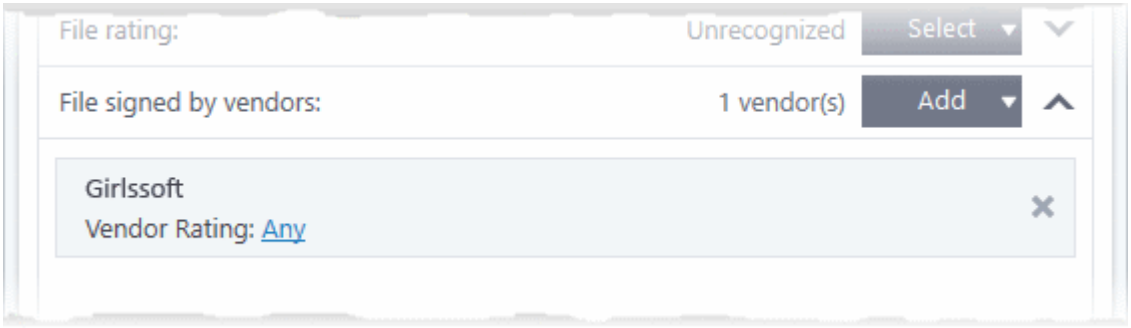
2. Specify an executable file on your local drive

- Choose 'File Signer' from the drop-down
- Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
- CCS identifies the vendor of the file and adds the to the rule.
- The rule will apply to files digitally signed by the vendor.

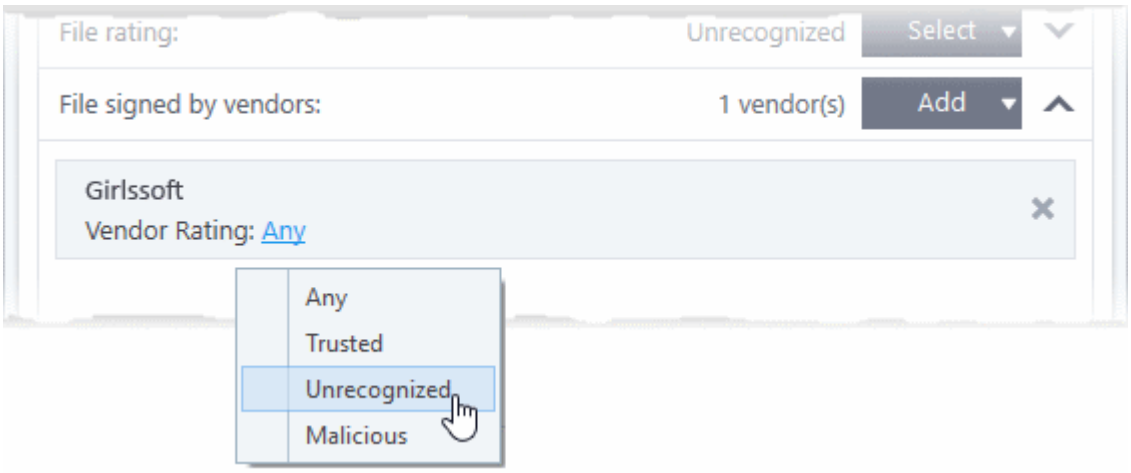
3. Select a currently running process

- Choose 'Running Process Signer' from the drop-down
- A list of all processes running at present on your computer is shown
- Select the process to specify the publisher of the application that started the process and click 'OK'
- CCS identifies the vendor of the process and adds the to the rule.
- The rule will apply to files digitally signed by the vendor.

The selected vendor is added:



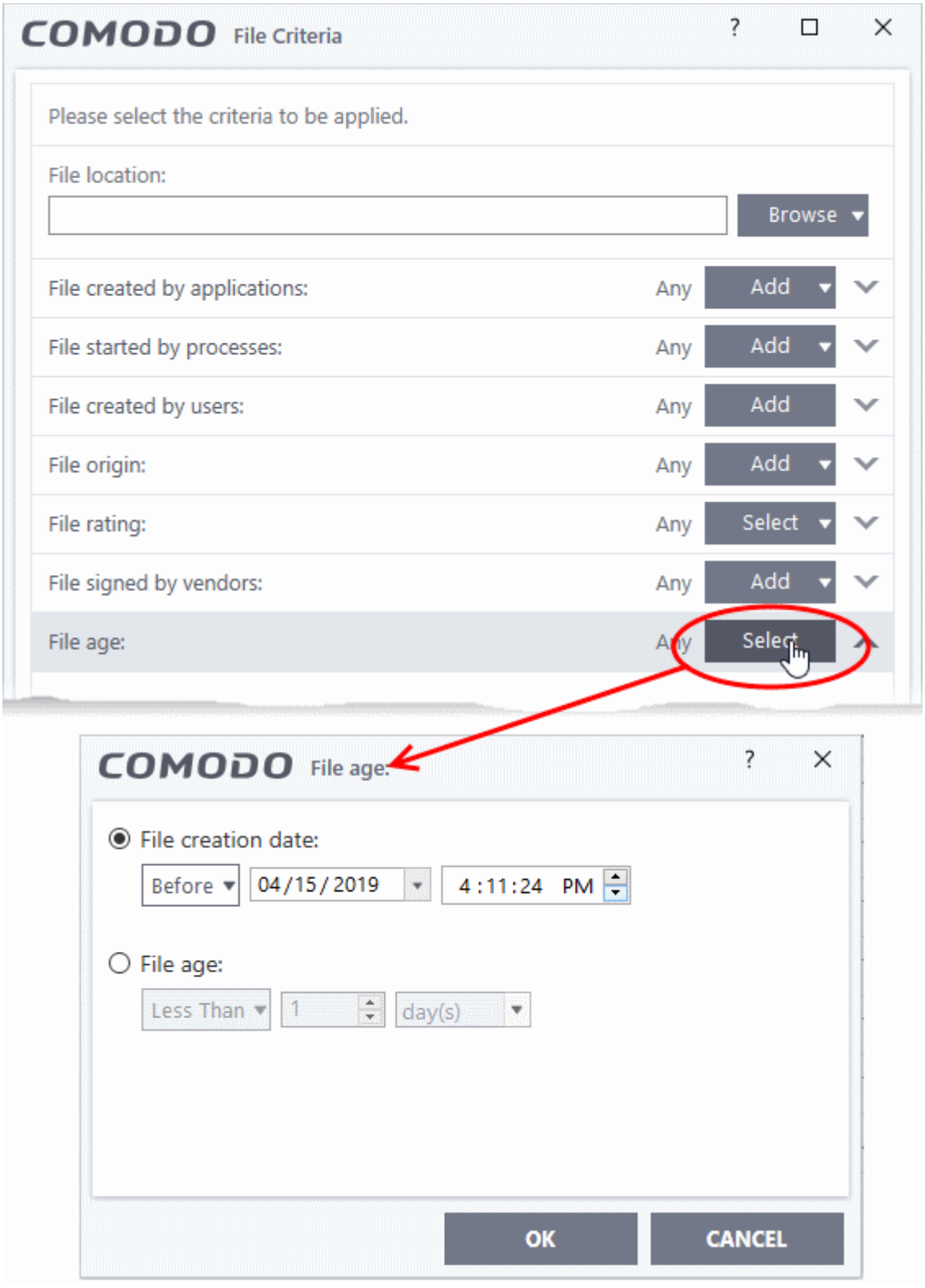
- **Vendor Rating** - The rule will only apply to the vendor's files IF the vendor has this rating at the time the file is checked. Note, the rating you set here can be different to the actual vendor rating in 'Settings' > 'File Rating' > 'File List' > 'Vendor Rating'.
  - Example. If you select 'Trusted' here, then CCS will apply the rule if the vendor is trusted at the time the file is checked. If the vendor's rating changes to 'Malicious' or 'Unrecognized', then the rule isn't applied.



- Repeat the process to add more vendors

Set the file age as filter criteria

- Click the 'Select' button in the 'File age' stripe.

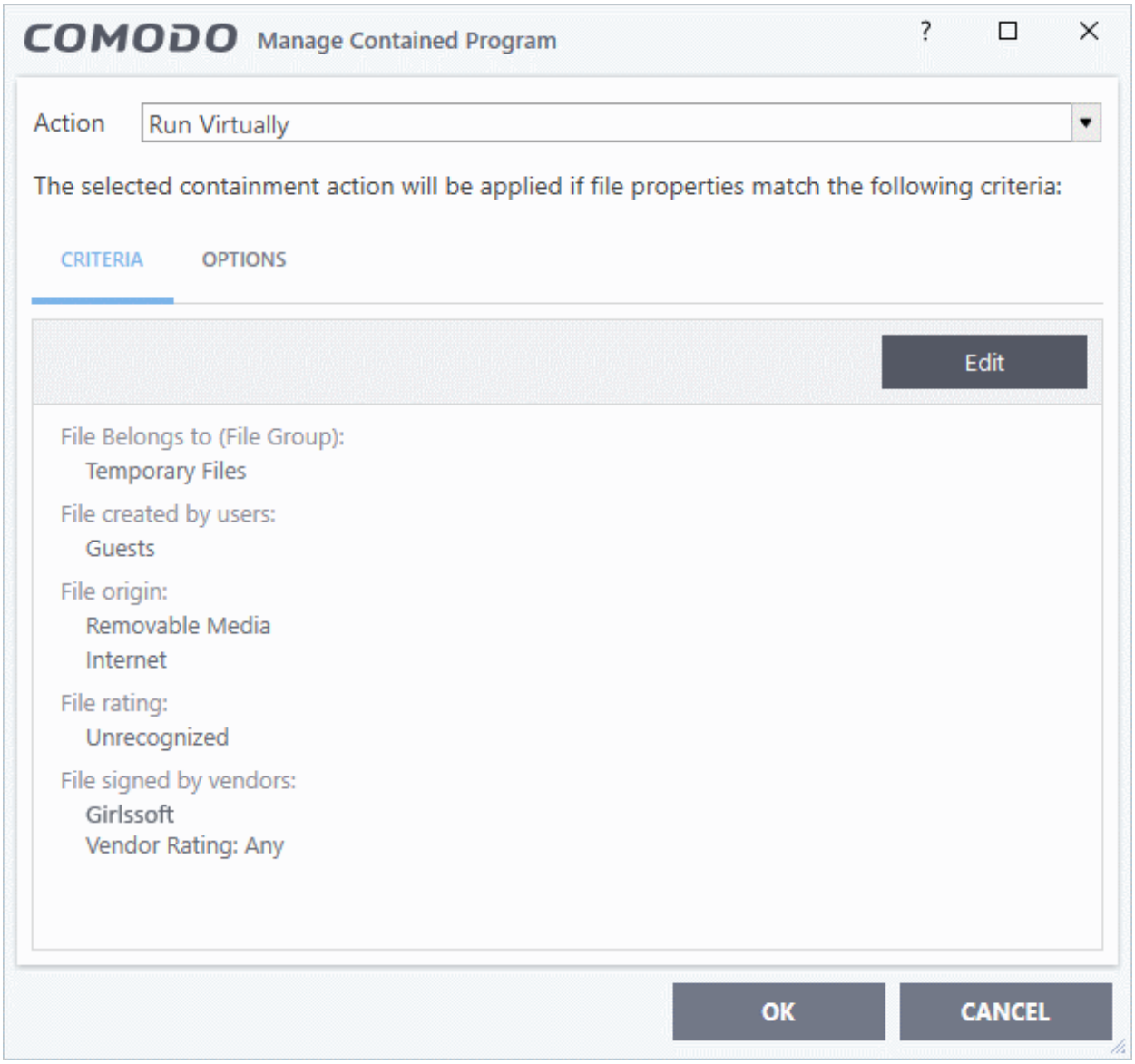


You can set the file age in two ways:

- **File Creation Date** - To set a threshold date to include the files created before or after that date, choose this option, choose 'Before'/'After' from the first drop-down and set the threshold date and time in the respective combo-boxes.
- **File age** - To select the files whose age is less than or more than a certain period, choose this option and specify the period.
  - **Less Than** - CCS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)

- **More Than** - CCS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (Default and recommended = 1 hours)

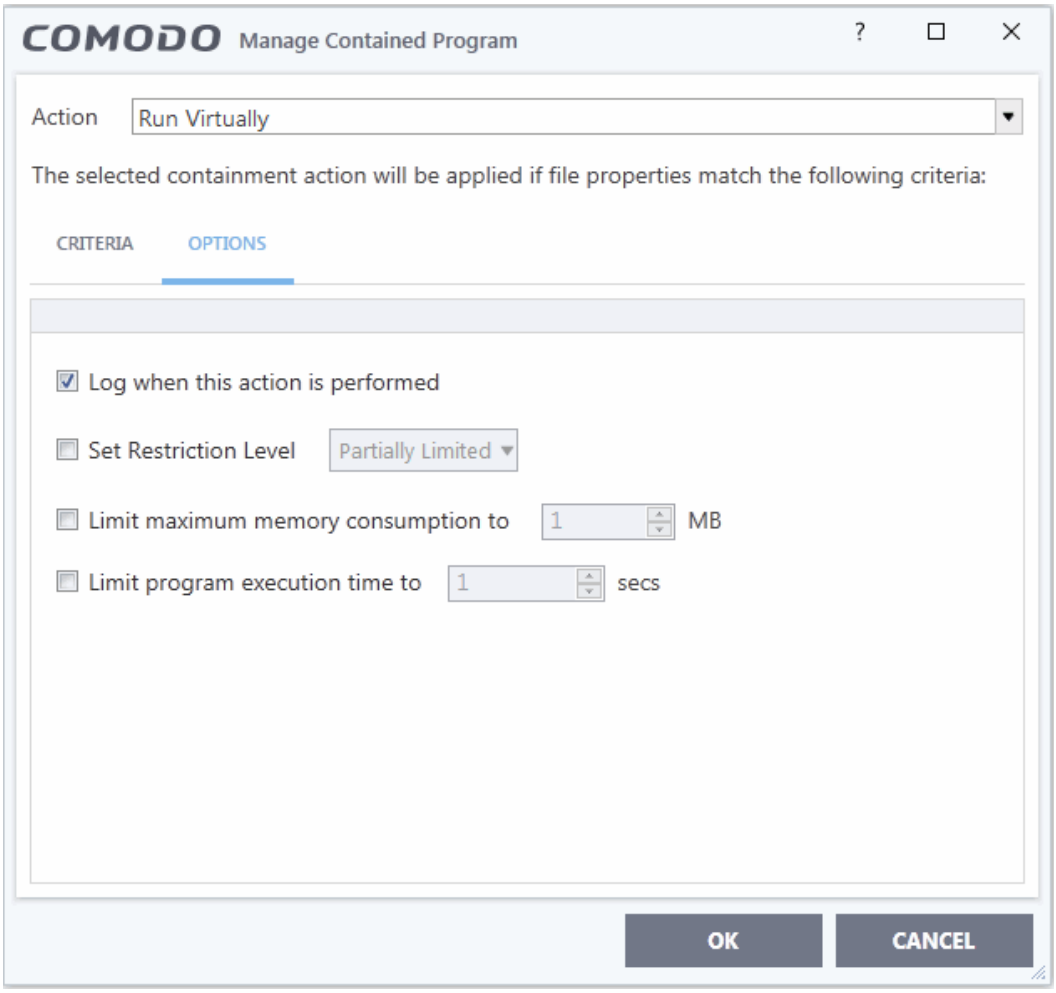
- Click 'OK' in the File Criteria dialog after selecting the filters to save your settings to the rule. The list of criteria will be displayed under the Criteria tab in the 'Manage Contained Program' dialog.



Step 3 - Select the Options

The next step is to choose optional actions and restrictions to be imposed on items contained by the rule.

- Click the 'Options' tab.



The options will be displayed, depending on the 'Action' chosen in **Step 1**.

The options available for '**Ignore**' action are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be added to CCS containment logs.
- **Don't apply the selected action to child processes** - Child processes are the processes launched by the application. CCS treats all child processes as individual processes and forces them to run as per the file rating and the containment rules.
  - By default, this option is not enabled and the 'Ignore' rule will also apply to child process of the target application(s).
  - If this option is enabled then the 'Ignore' rule will be applied only to the target application. Any child processes will be checked and containment rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the 'Ignore' action only.

The options available for '**Run Restricted**' and '**Run Virtually**' actions are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be added to CCS containment logs.
- **Set Restriction Level** - When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
  - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. ***(Default)***
  - **Limited -** Only selected operating system resources can be accessed by the application. The

application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.

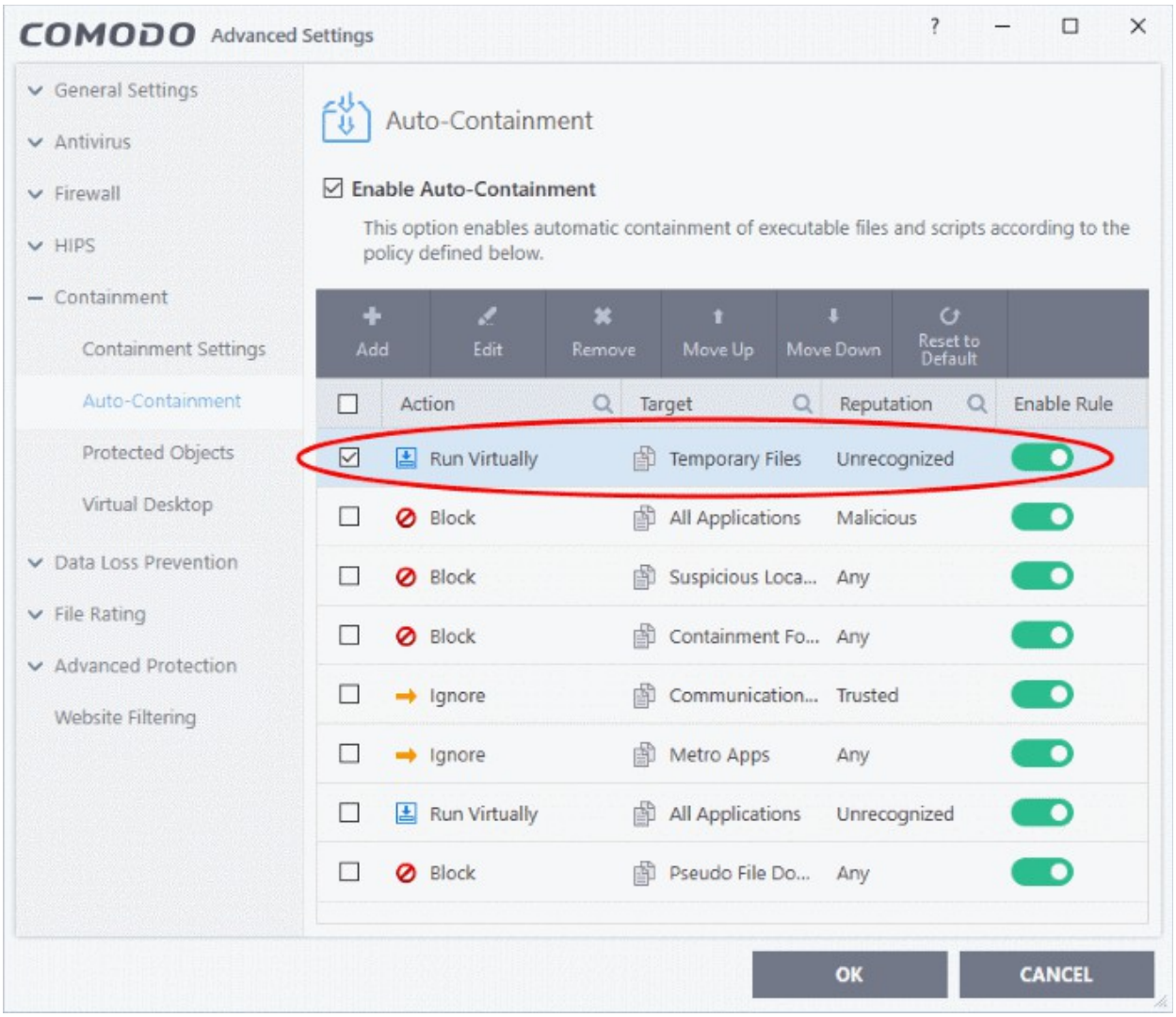
- **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Untrusted -** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.

- **Limit maximum memory consumption to** - Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** - Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

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 added to CCS containment logs.
- **Quarantine program** - If checked, the programs will be automatically quarantined. See **Manage Quarantined Items** for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



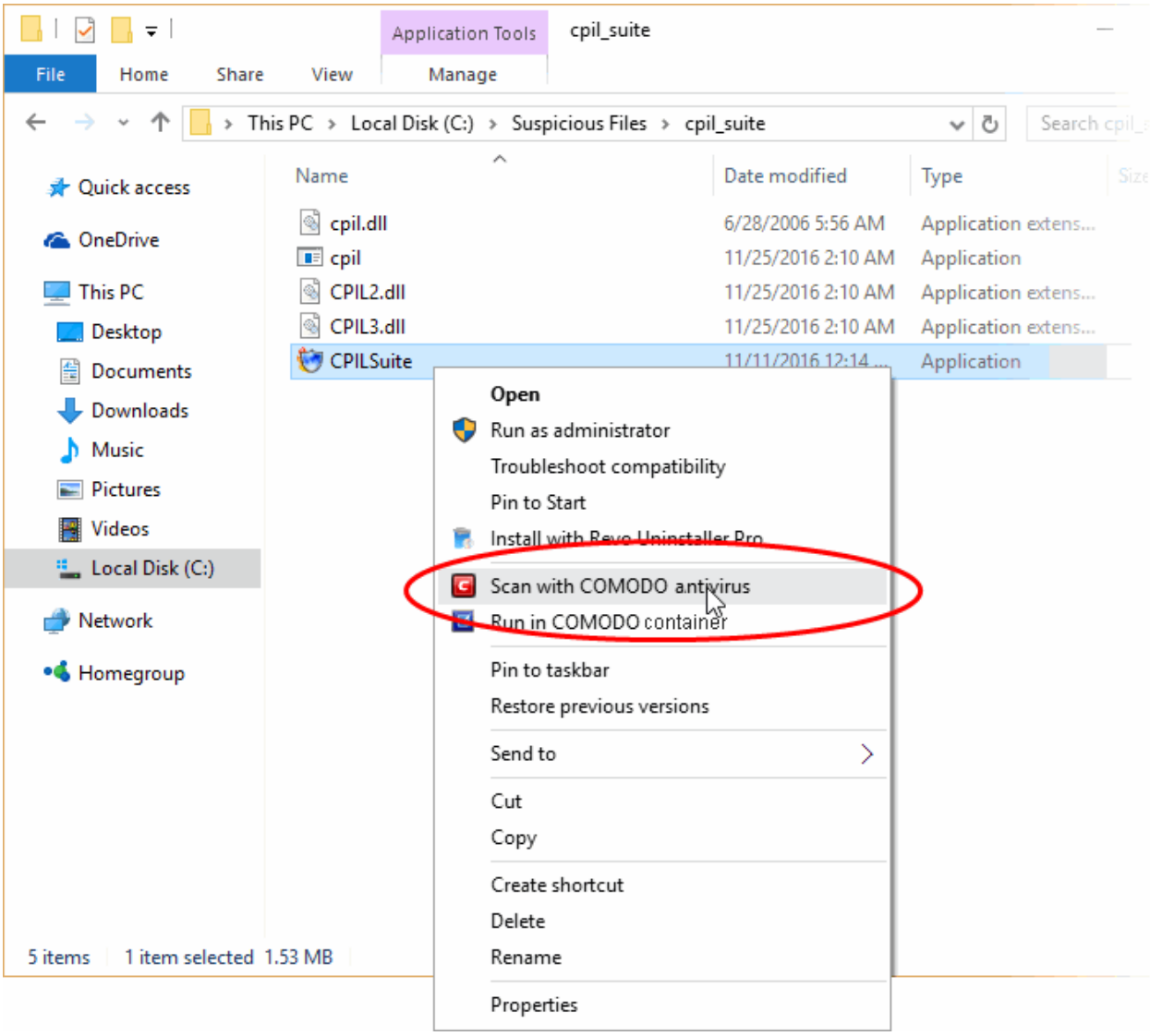
Important Note: Please make sure the auto-containment rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail. You can restore the rules to default rules at any time by clicking the 'Reset to Default' button at the top.

Run an Instant Antivirus Scan on Selected Items

- You can scan individual files or folders instantly to check whether they contain any threats.
- This is useful if you are wary about an item you have copied from an external source or downloaded from the internet.

Instantly scan an item

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

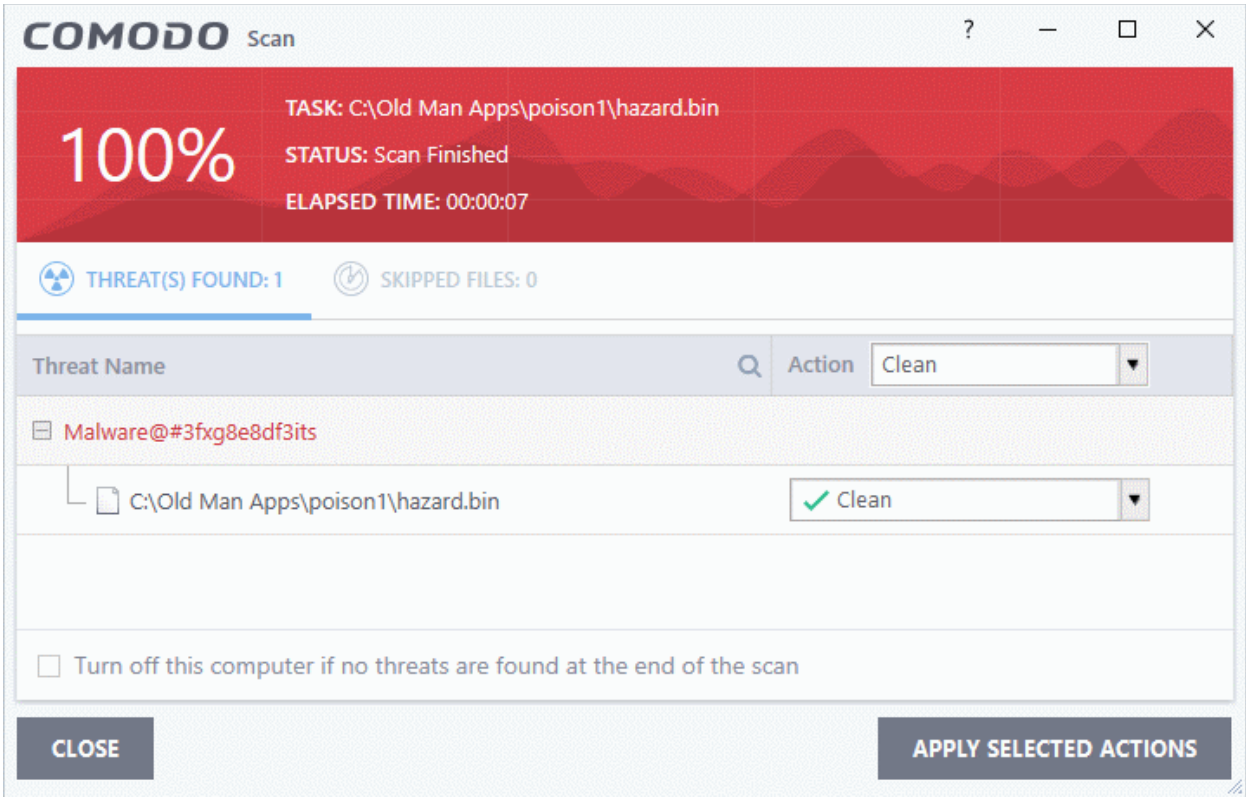


The item will be scanned immediately.

Note - CCS skips files which are larger than the max. size, and those that take longer to scan than the max time allowed.

Click 'Settings' > 'Antivirus' > 'Scans', then open the 'Full Scan' profile to view these thresholds.

- Scan results are shown when the scan finishes:



Click here for more details to take action on the infected item(s).

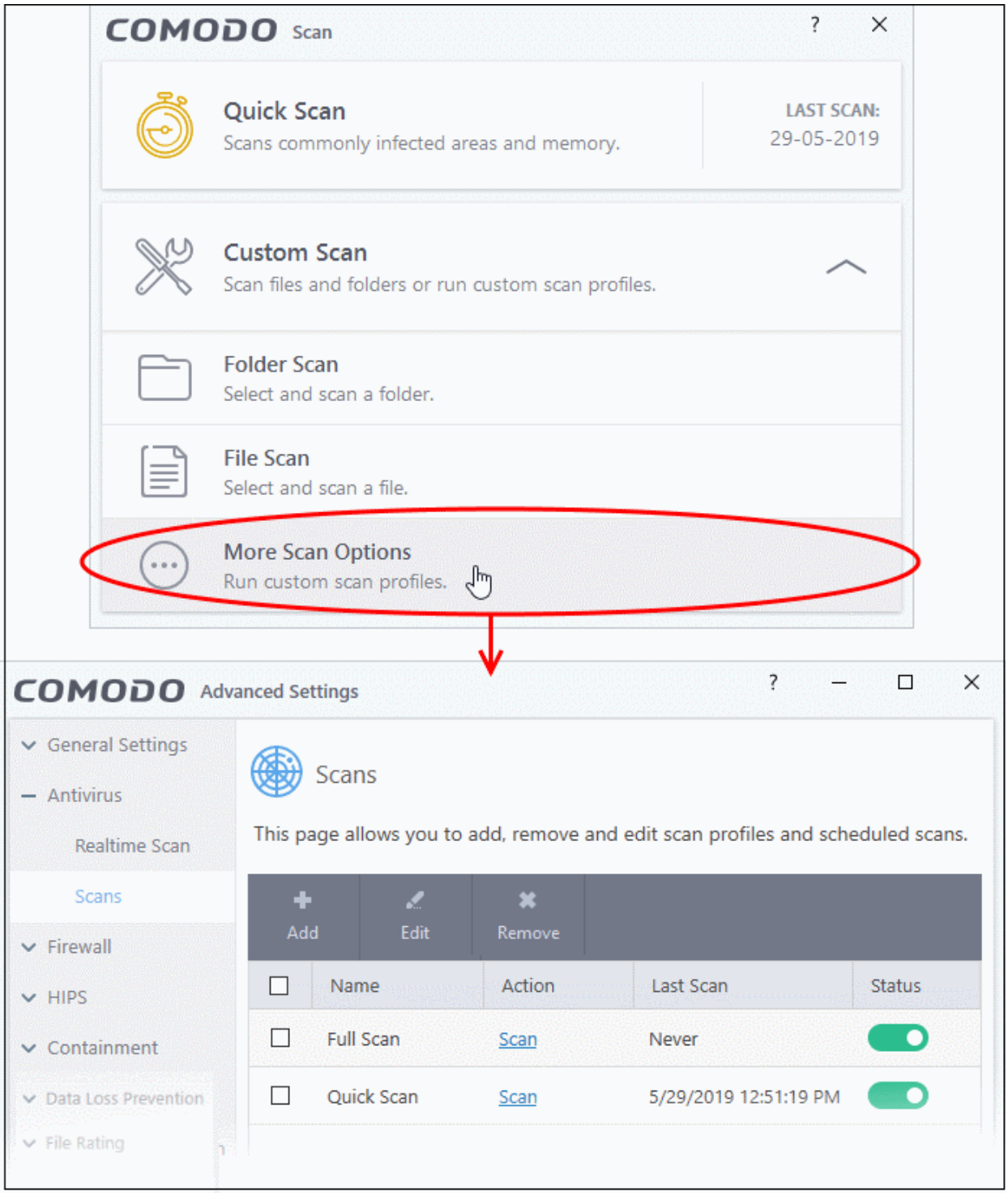
Create an Antivirus Scan Schedule

- Click 'Tasks' > 'General Tasks' > 'Scan' > 'Custom Scan' > 'More Scan Options'
- A custom scan profile lets you configure your own scan with your own scan settings.
- You can define exactly which files and folders to scan, what time they should be scanned, and configure scan settings.

Create a scan schedule

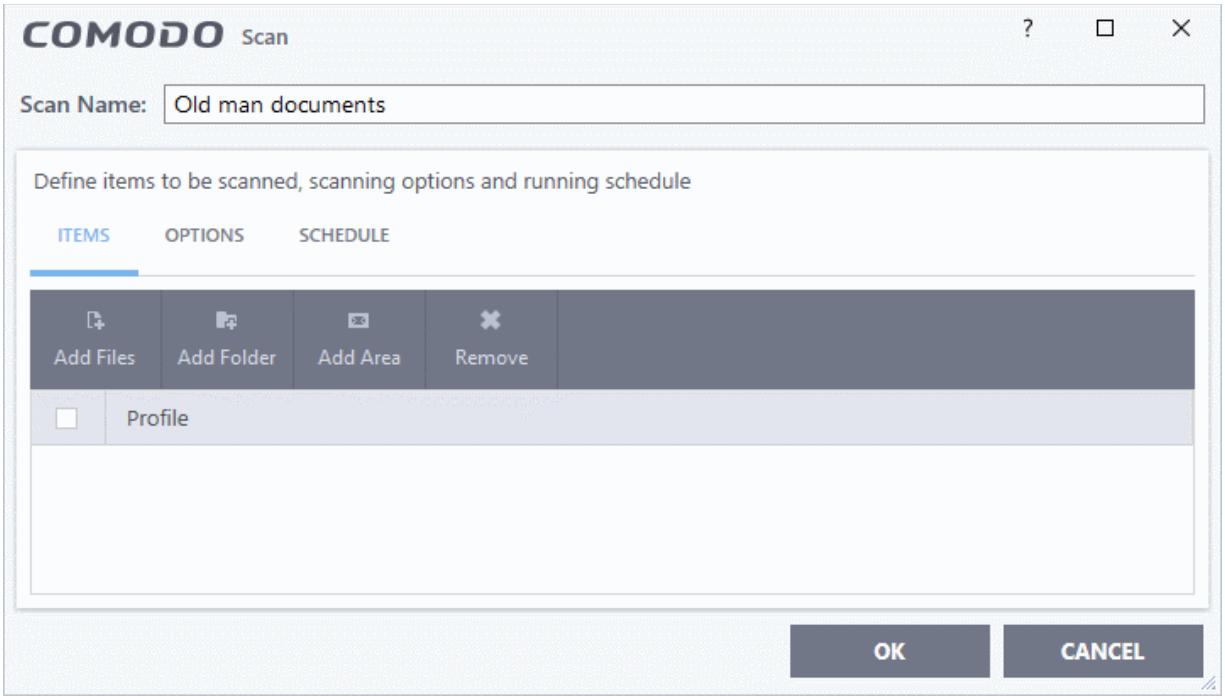
- Click 'Tasks' > 'General Tasks' > 'Scan'
- Select 'Custom Scan' then 'More Scan Options'

The 'Scans' page shows pre-defined and user created scan profiles. You can create and manage new profiles in this page:



Tip: You can also get to this screen by clicking 'Settings' > 'Antivirus' > 'Scans'.

- Click 'Add' to create a new custom scan profile.



First, create a name for the profile. The next steps are:

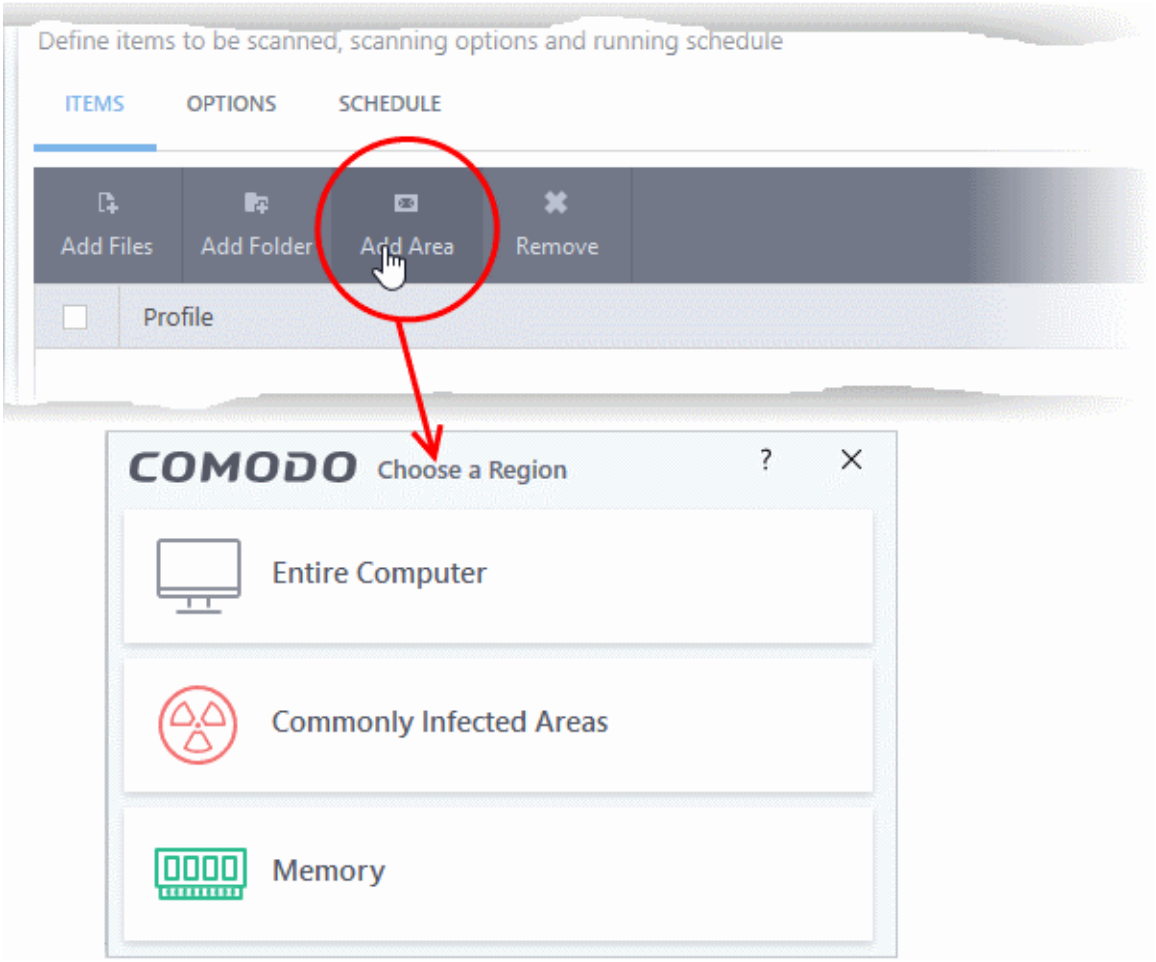
- **Select the items to be scan**
- **Configure scan options for the profile (optional)**
- **Configure a scan schedule (optional)**

Select items to scan

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

You can add items as follows:

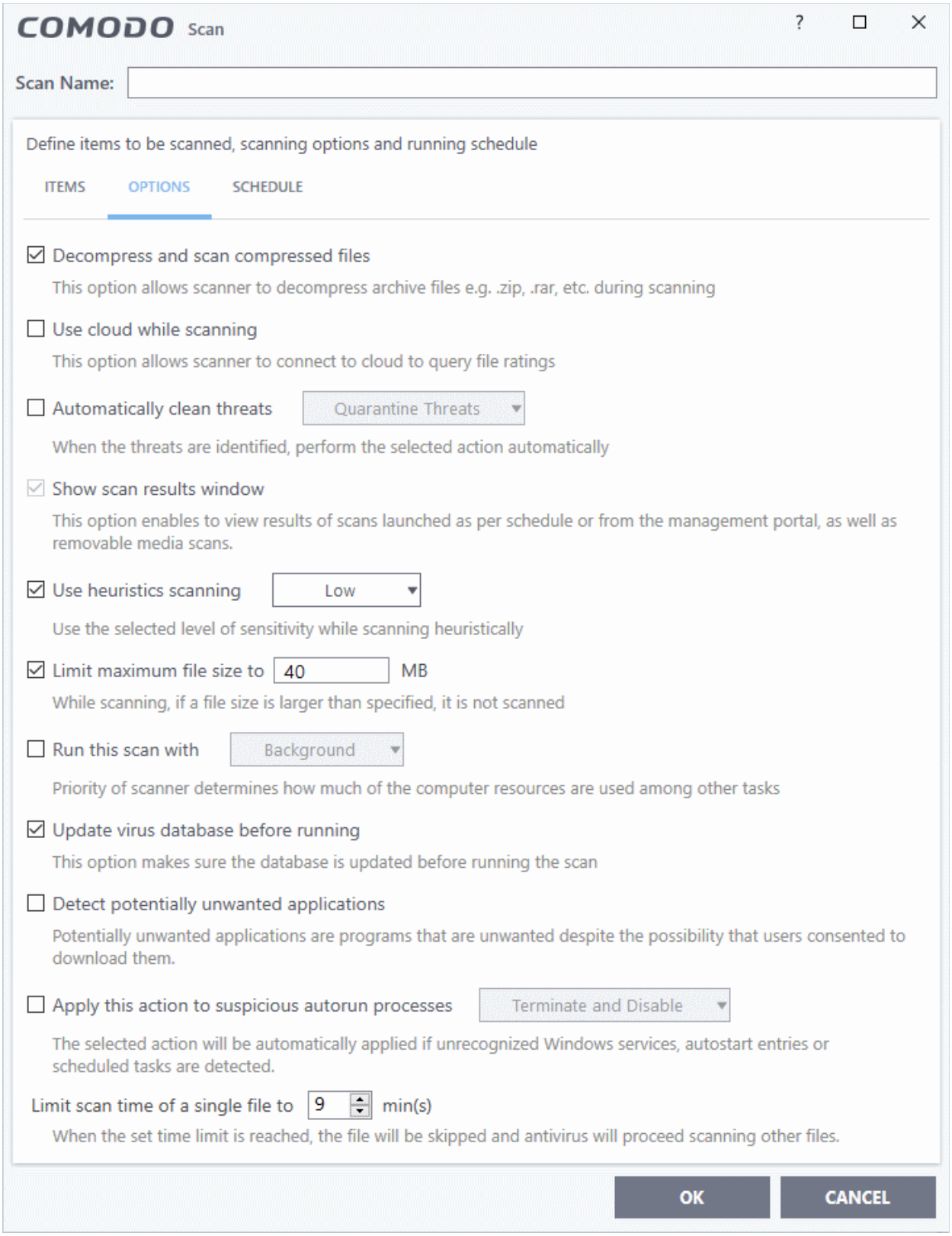
- **Add File** - Add individual files to the profile. Click the 'Add Files' button and browse to the file you want to include.
- **Add Folder** - Add entire folders to the profile. Click the 'Add Folder' button and choose the folder you want to include. All files in the folder are covered by the scan.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



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

Configure scan options

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



Decompress and scan compressed files - The scan will include archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (***Default = Enabled***).

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

Automatically clean threats - Select whether or not CCS should automatically remove any malware found by the

scan. (***Default = Enabled***).

- **Disabled** = Results are shown at the end of the scan with a list of any identified threats. You can manually deal with each threat in the results screen. See **Process Infected Files** for guidance on manually handling detected threats.
- **Enabled** = Threats are handled automatically. Choose the action that CCS should automatically take:
  - **Quarantine Threats** - Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See '**Manage Quarantined Items**' for more details.
  - **Disinfect Threats** - If a disinfection routine exists, CCS will remove the virus and keep the original file. If not, the file will be quarantined. (***Default***)

Show scan results window - You will see a summary of results at the end of the scan. This includes the number of objects scanned and the number of threats found.

Use heuristic scanning - Select whether or not heuristic techniques should be used in scans on this profile. You can also set the heuristic sensitivity level. (***Default = Enabled***).

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

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

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

  Despite the name, this setting combines a very high level of protection with a low rate of false positives. We recommend this setting for most users. (Default)
- **Medium** - Detects unknown threats with greater sensitivity than the low setting, but with a corresponding rise in possible false positives.
- **High** - Highest sensitivity to detecting unknown threats. This also raises the possibility of more alerts and false positives.

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

Run this scan with - If enabled, you can set the priority of scans on this profile The available options are:

- High
- Normal
- Low
- Background

If you disable this option then the scan runs in the background (***Default***)

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

Detect potentially unwanted applications - The antivirus also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may contain functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often bundled as an additional utility when installing another piece of software. Unlike malware, many PUA's are legitimate pieces of software with their own EULA agreements. However, the true functionality of the utility might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks your activity on the internet. ***(Default = Enabled)***.

Apply this action to suspicious autorun processes - Specify how CCS should handle unrecognized auto-run items, Windows services, and scheduled tasks.

- **Ignore** - The item is allowed to run (***Default***)
- **Terminate** - CCS stops the process / service

- **Terminate and Disable** - Auto-run processes are stopped and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.
- **Quarantine and Disable** - Auto-run processes are quarantined and the corresponding auto-run entry removed. In the case of a service, CCS disables the service.

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

- See **Miscellaneous Settings** for more details

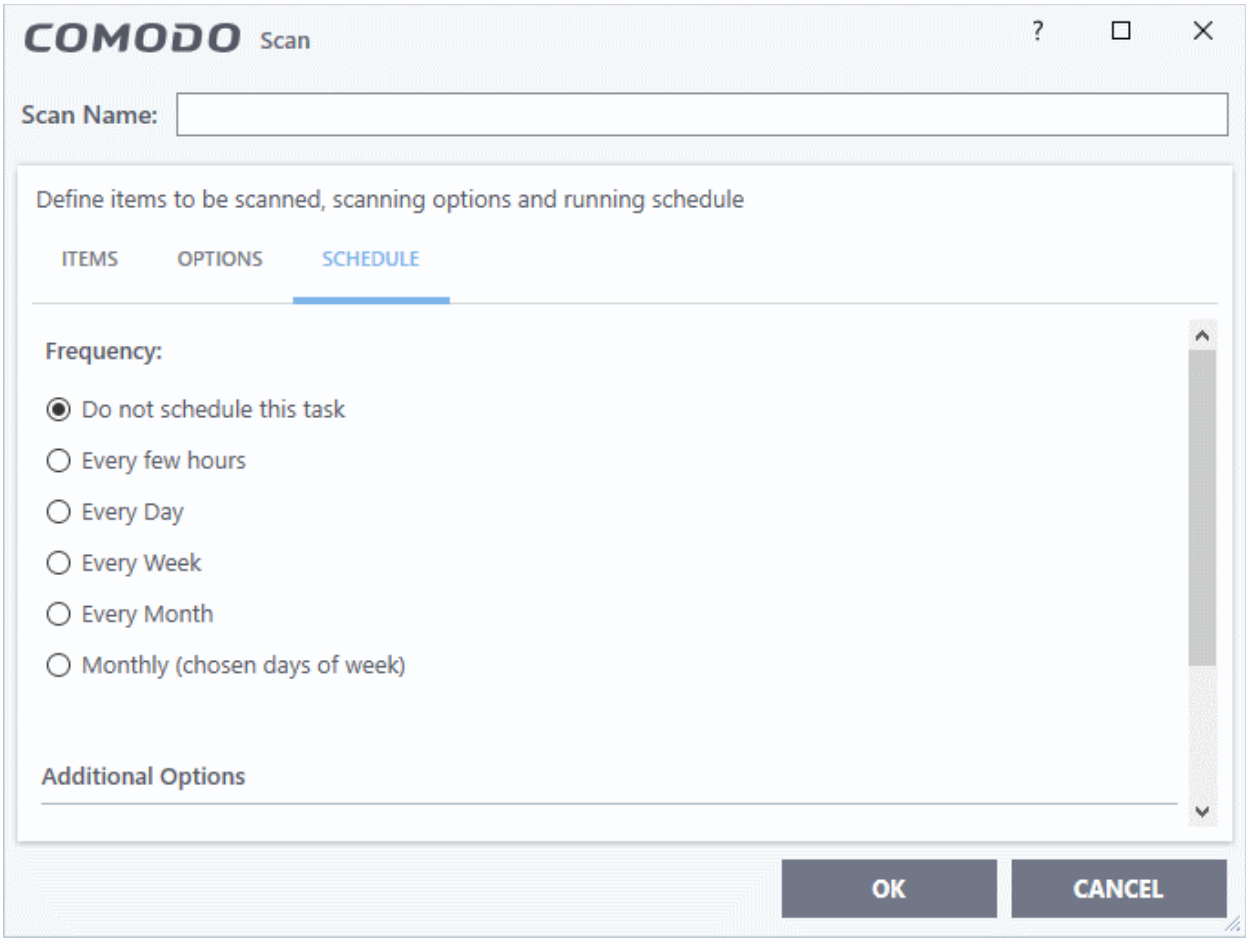
Note 2 - CCS runs script analysis on certain applications to protect their registry records. You can manage these applications in 'Advanced Settings' > 'Advanced Protection' > 'Script Analysis' > 'Autorun Scans'.

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

Limit scan time of a single file to - Set the maximum time allowed to scan an individual file. CCS will skip files that take longer to scan than the specified time. Omitted files are shown in the 'Skipped Files' tab in the results screen.

Schedule the scan

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



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

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

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

Every Week - Run the scan on the days specified in 'Days of the Week', at the time specified in the 'Start Time' field. You can select the days of the week by clicking on them.

Every Month - Run the scan on the dates specified in 'Days of the month', at the time specified in the 'Start Time'

field. You can select the dates of the month by clicking on them.

Monthly (chosen days of the week) - Run the scan on a specific week, or weeks, in a month. Select the weeks in from the menus.

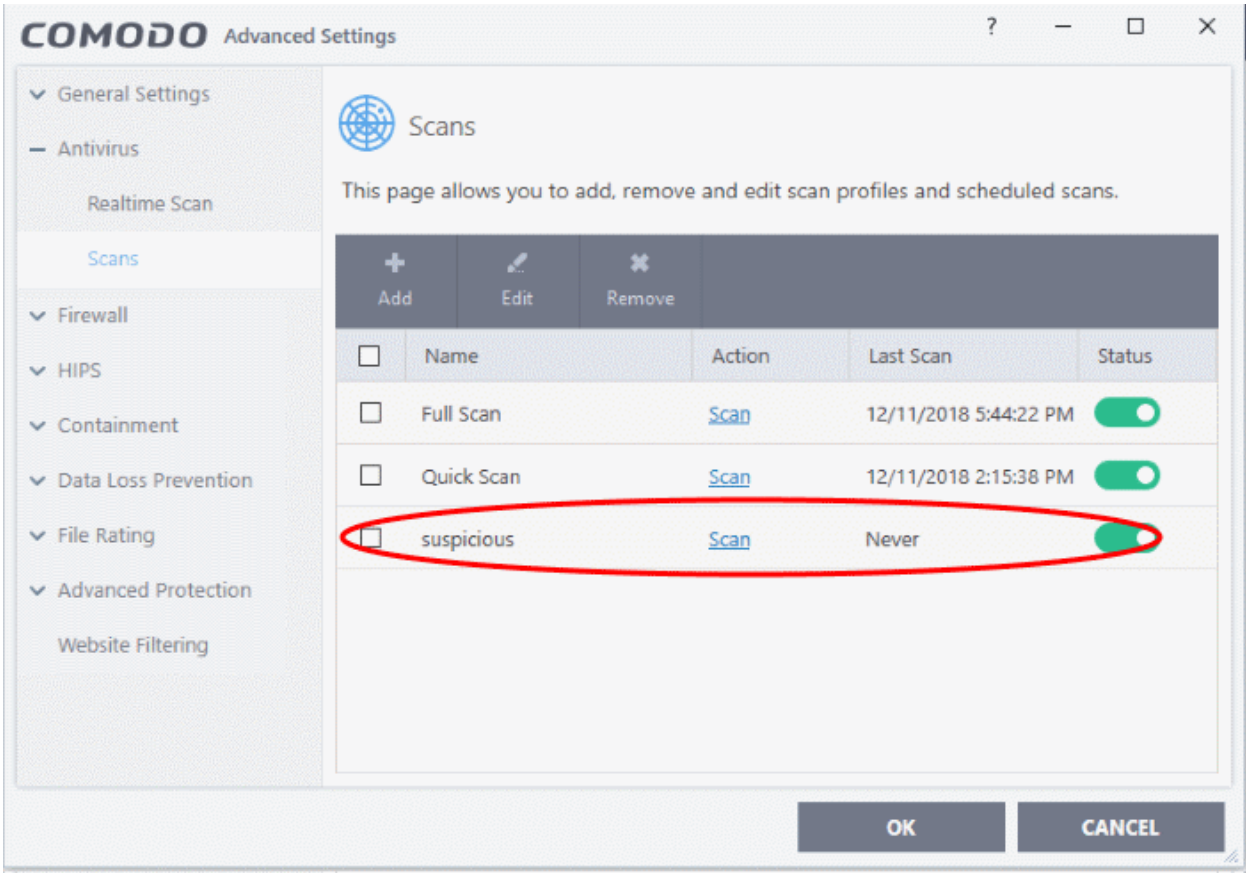
Additional Options

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

Note: Scheduled scans will only run if the profile is enabled. Use the switch in the 'Status' column to turn the profile on or off.

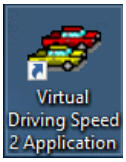
- Click 'OK' to save the profile.

The profile will be available for deployment in future.



Run Untrusted Programs inside the Container

- Click 'Tasks' > 'Containment Tasks' > 'Run Virtual'
  - Choose the program you want to run
  - Click 'Open'
- CCS lets you run programs inside the container on a 'one-off' basis.
- This is helpful to test new/beta programs you have downloaded but are not yet sure you trust.
- You can also create a desktop shortcut to run the application inside the container on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:

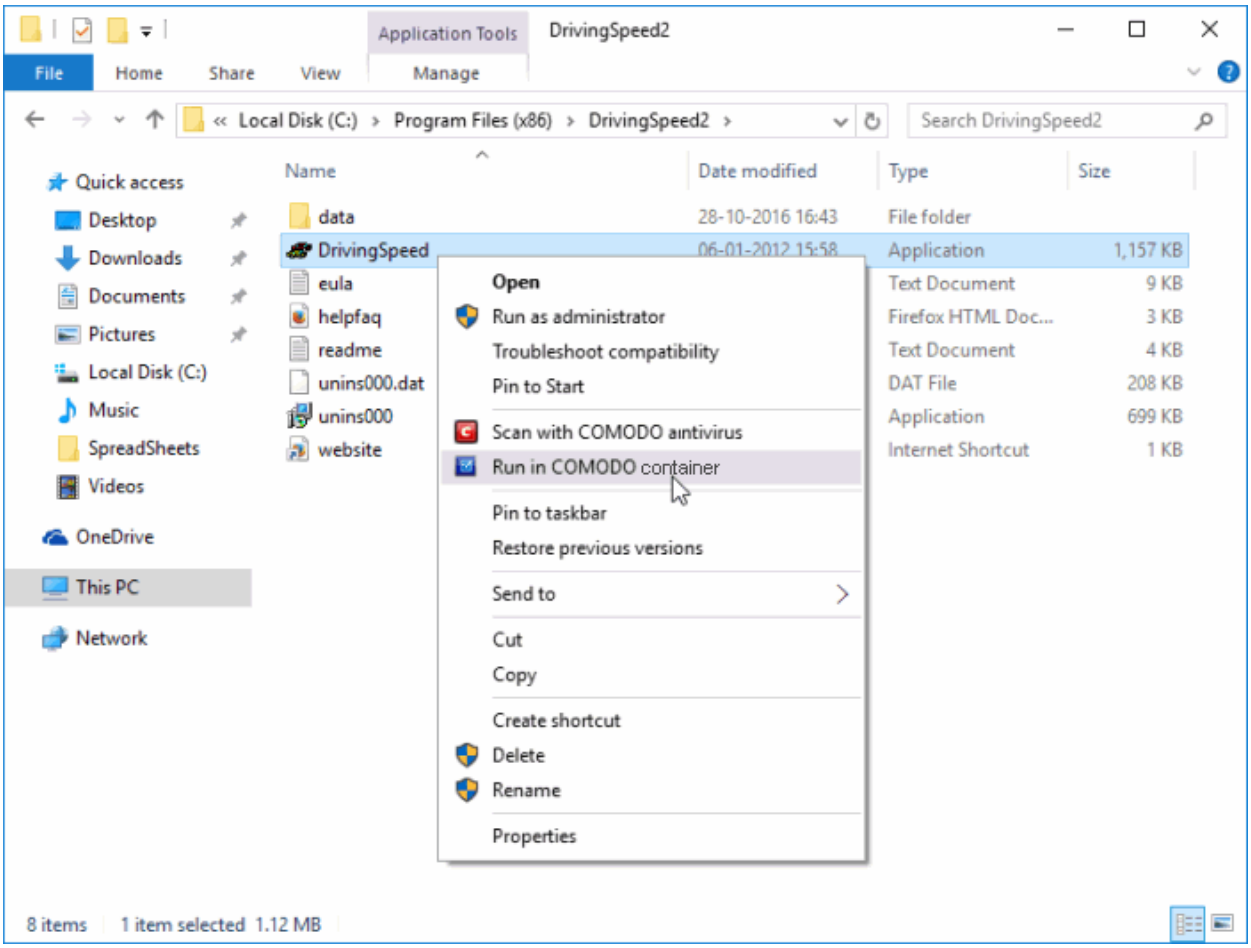


Use any of the following methods to run a program in the container:

- **Right click menu**
- **From the 'Containment Tasks' area**
- **From the widget (browsers only)**

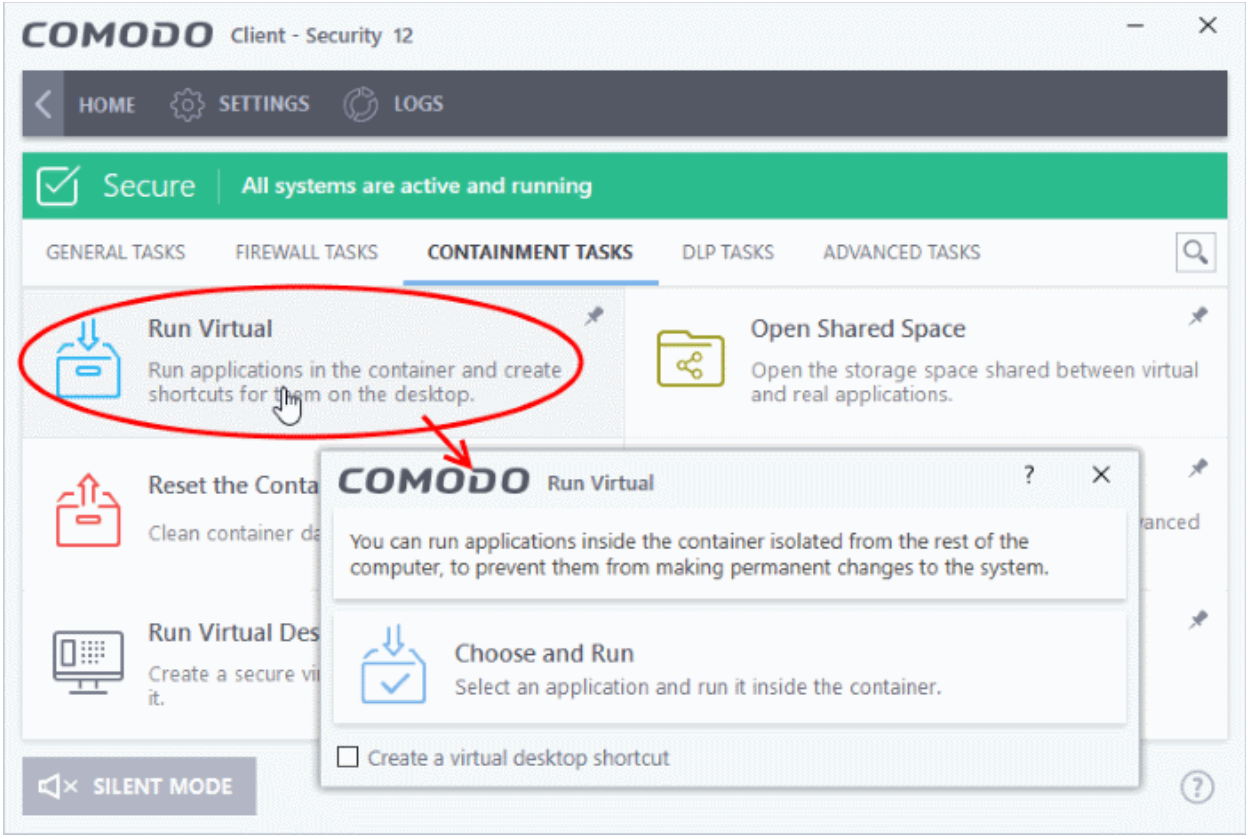
Right-click menu

1. Navigate to the program you want to run in the container
2. Right-click on the program
3. Choose 'Run in COMODO container' from the context sensitive menu:



The 'Containment Tasks' interface

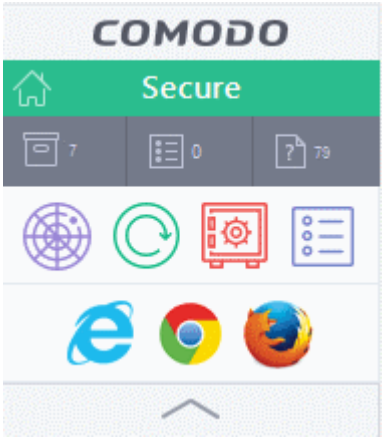
1. Click 'Tasks' > 'Containment Tasks'
2. Click the 'Run Virtual' tile



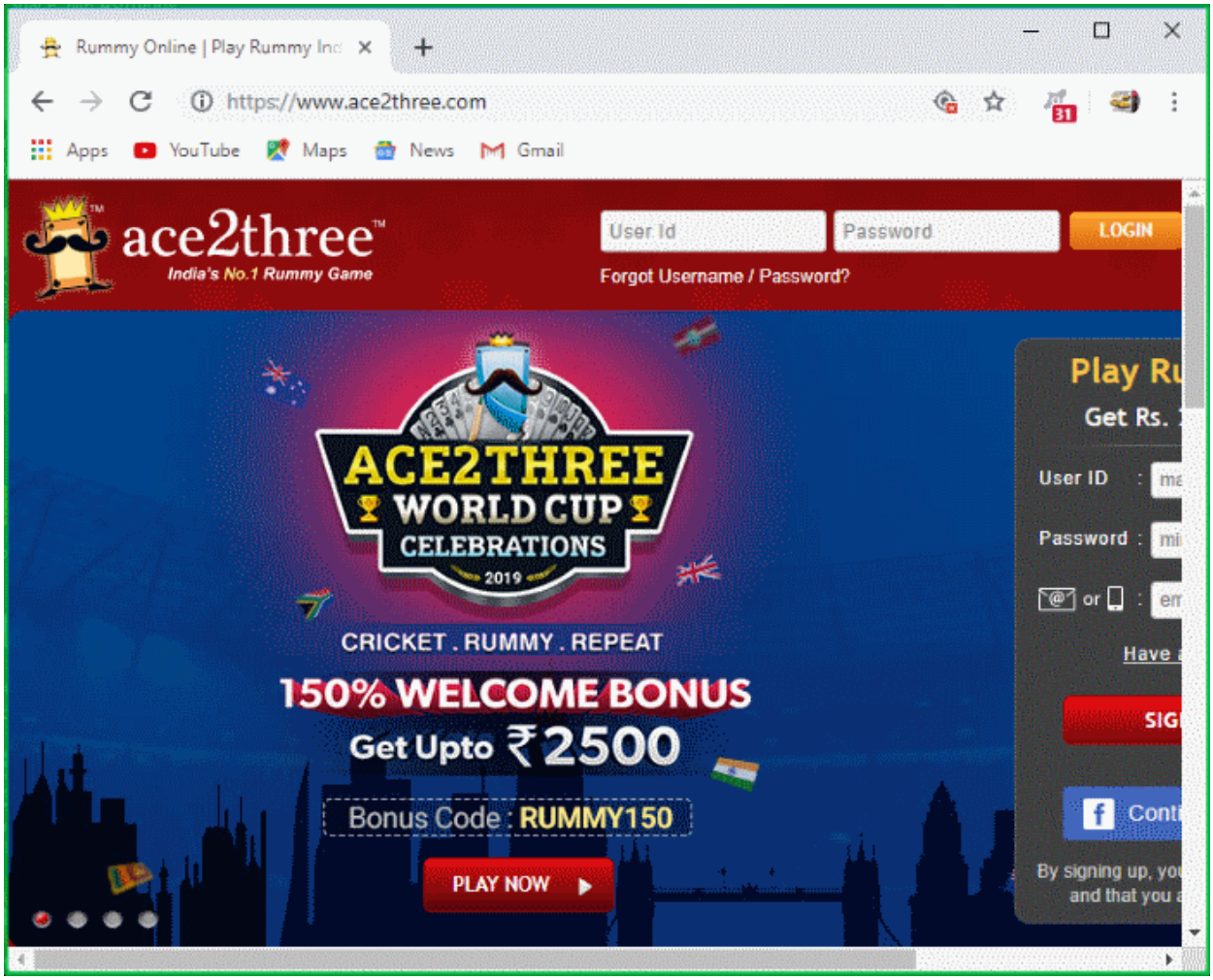
- Click 'Choose and Run', browse to your application then click 'Open'.
- The contained application will have a green border around it. Enable 'Create a virtual desktop shortcut' if you plan to run the application in the container in future.

Run browsers in container

The CCS widget contains shortcuts to run your browsers in the container:



- Click a browser icon to start the browser inside the container
- The green border indicates that the browser is in the container:



Run Browsers Inside the Container

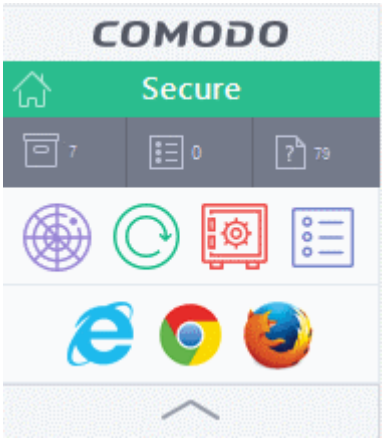
- This topic explains how to run your internet browser inside the container.
- Surfing the internet from within the container is the same as normal, with the benefit that any malicious files you inadvertently download cannot damage your real computer.
- You can also create a desktop shortcut to run the browser inside the container on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:

There are two ways to run a browser in the container:

- **From the desktop widget**
- **From the 'Containment Tasks' area**

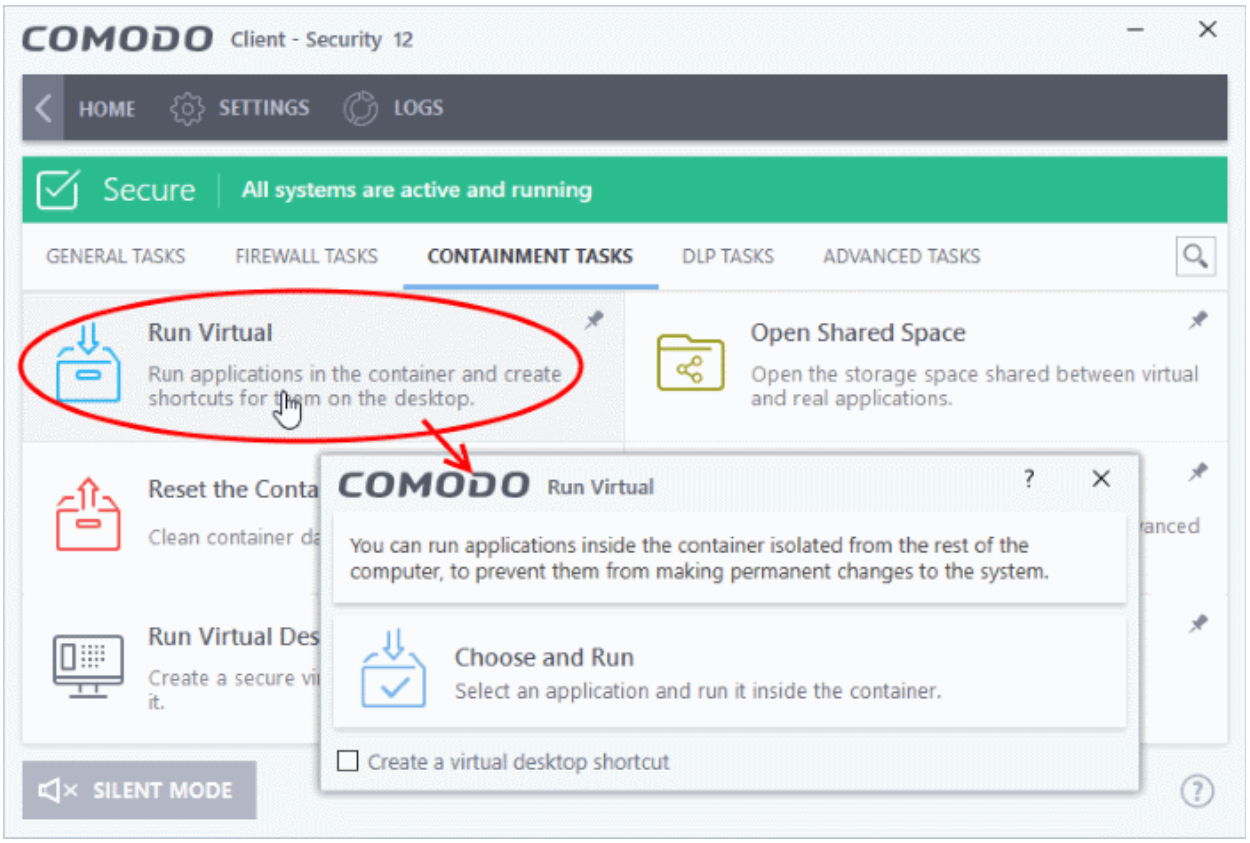
Start a browser from the desktop widget

- The CCS widget contains shortcuts to run your browsers in the container:



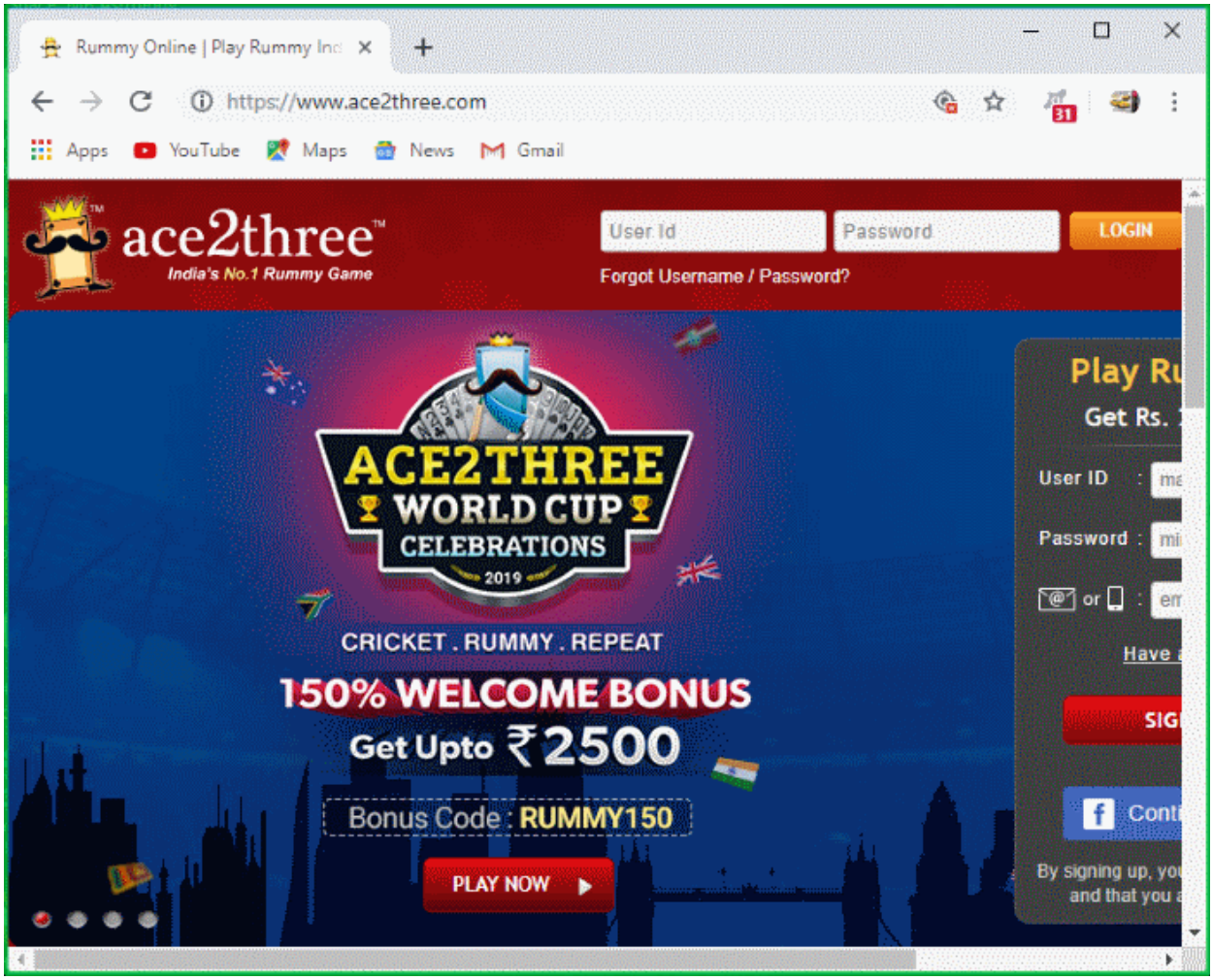
Start a browser from the 'Containment Tasks' interface

1. Click 'Tasks' > 'Containment Tasks'
2. Click 'Run Virtual'



3. Click 'Choose and Run' then navigate to the install location of the browser. Select the .exe file of the browser.
4. Select 'Create a virtual desktop shortcut' to quickly run the application in the container in future.

The browser will run with a green border around it, indicating that it is contained:



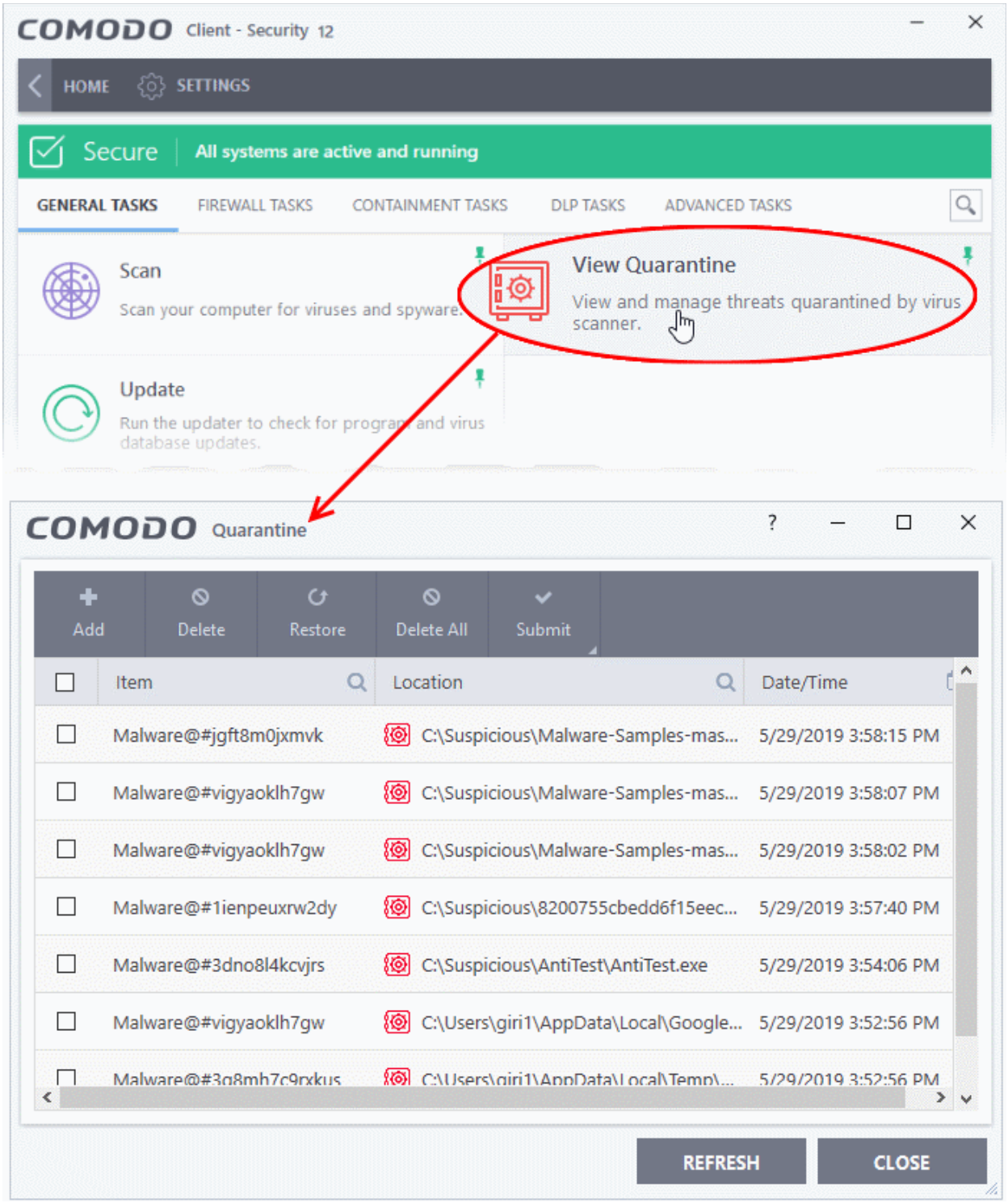
Restore Incorrectly Quarantined Items

This page explains how to restore an item from quarantine. You may want to do this if

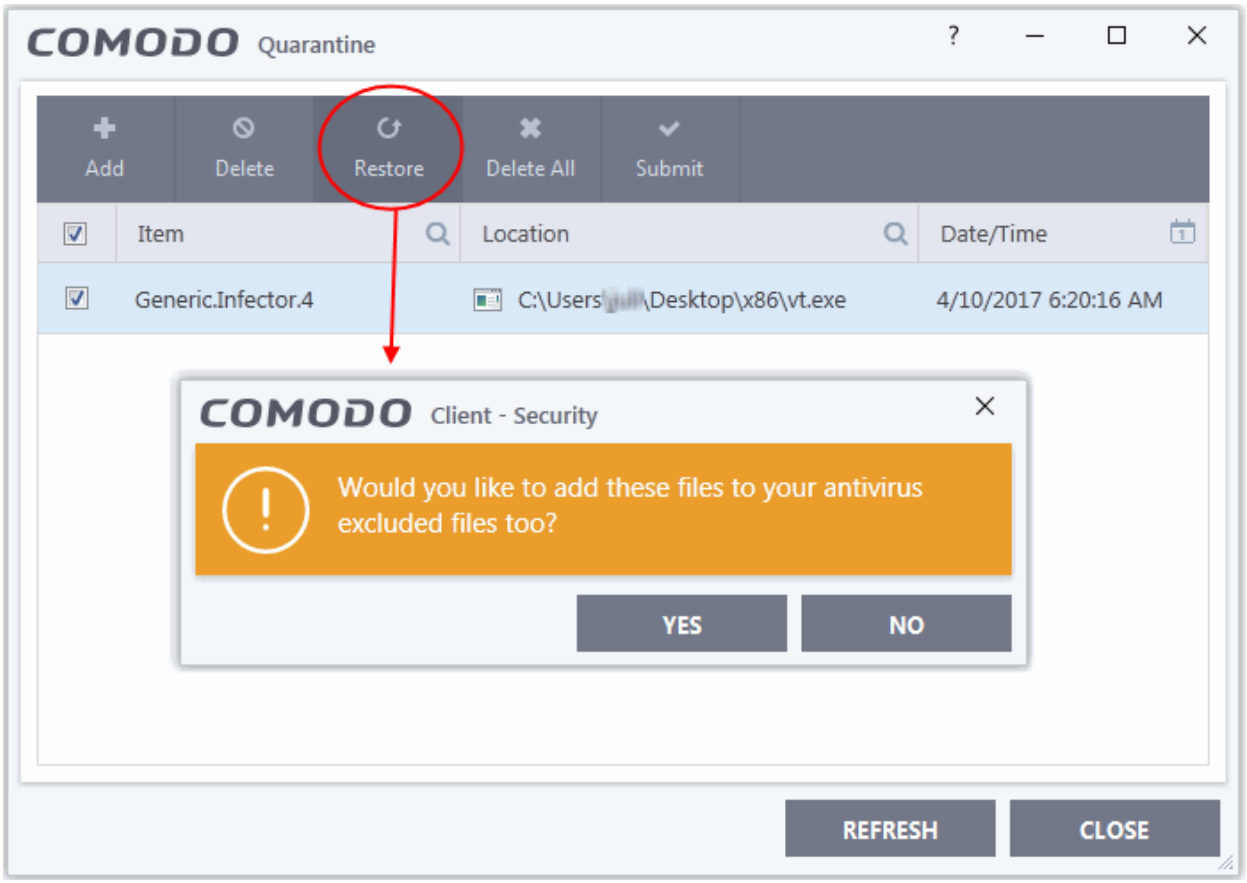
- You think CCS has incorrectly classed it as malicious (a false positive)
- It was manually moved to quarantine by mistake

Restore an item from quarantine

- Click 'Tasks' > 'General Tasks'
- Click 'View Quarantine'



- Select the item(s) you wish to move out of quarantine and click the 'Restore' button.
- You will then be asked if you wish to create an exclusion for the file so that it will not be flagged by future antivirus scans:



- 'Yes' - The items will be restored to their original locations and added to the antivirus exclusion list. The restored files will be skipped in future AV scans.
- 'No' - The items will be restored to their original locations but may still be flagged by future AC scans.
- Click 'Close' to exit.

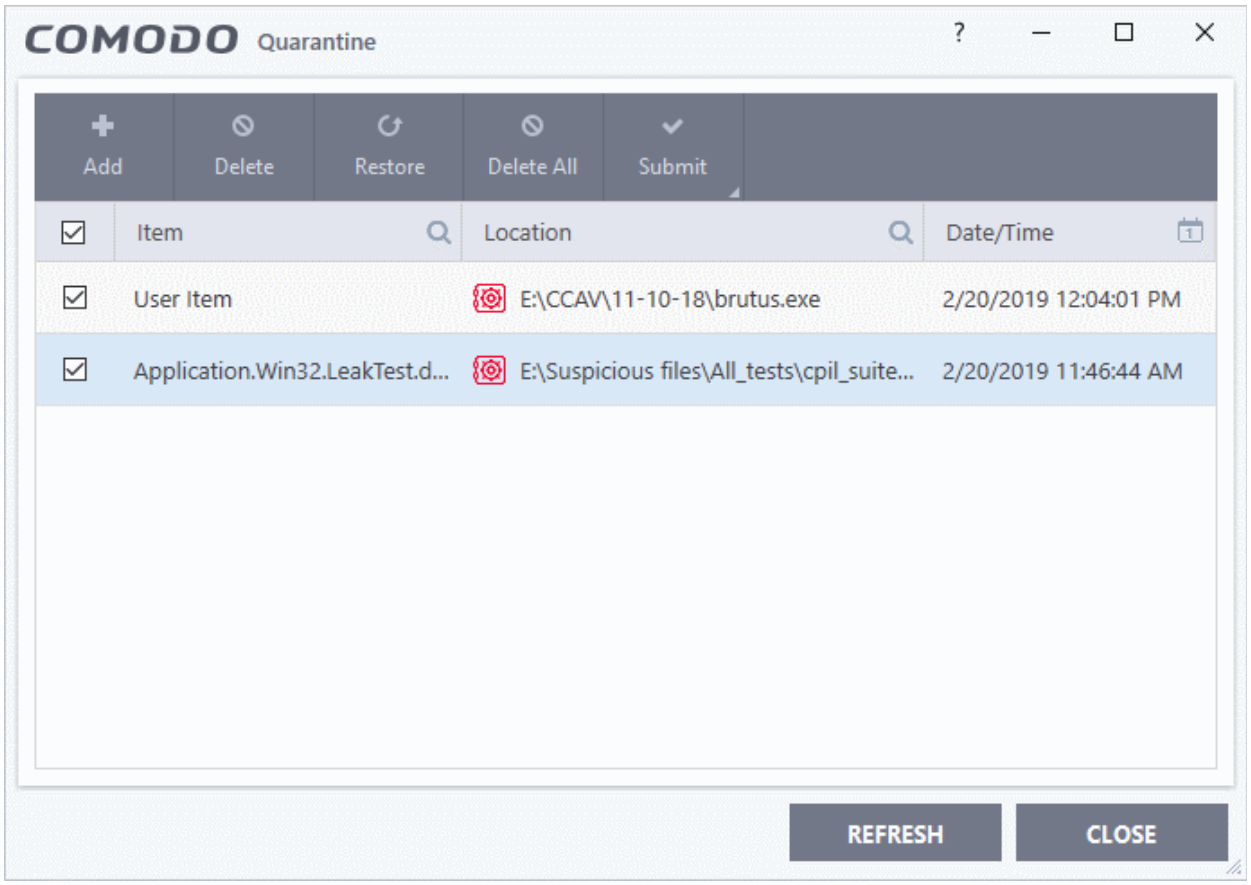
See **Manage Quarantined Items** and **Submit Quarantined Items to Comodo for Analysis** for more information on this topic.

Submit Quarantined Items to Comodo Valkyrie for Analysis

- You can send quarantined items to Valkyrie for analysis. You may want to do this if you think the item is a false positive - it was incorrectly flagged as malicious by CCS.
- Valkyrie is Comodo's file testing and verdicting system. After submitting your files, Valkyrie will analyze them with a range of static and dynamic tests to determine the file's trust rating.
- If the submitted item is found to be a false positive, it will be added to the Comodo white-list.
- If it is found to be malware, it will be added to the virus black-list.
- Submitting files helps Comodo enhance its virus signature database and benefits millions of CCS users. See **Quarantined Items** for more detailed information on the quarantine system.

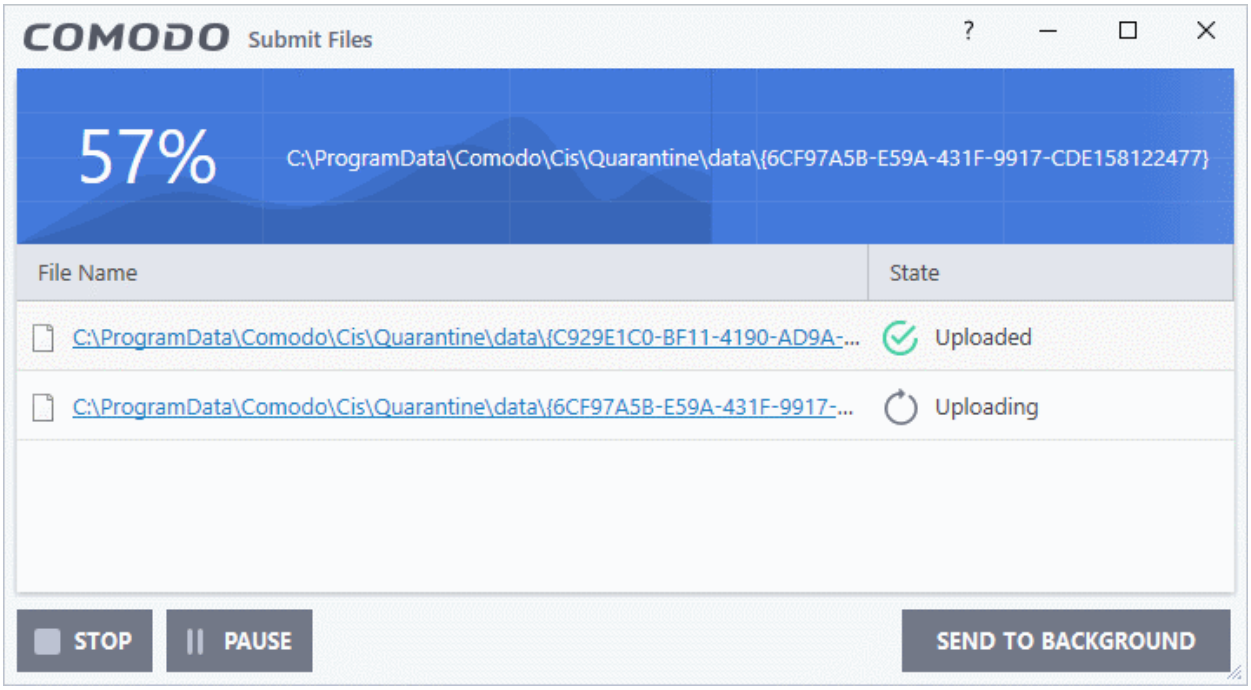
Submit quarantined items

- Click 'Tasks' > 'General Tasks'
- Click 'View Quarantine'



- Select the item(s) you wish to send for analysis
- Click 'Submit' > 'Submit to Valkyrie'

The submission progress will start:



The results state whether the file was successfully submitted, or whether it has already been submitted by other users and is pending analysis.

Enable File Sharing Applications like BitTorrent and Emule

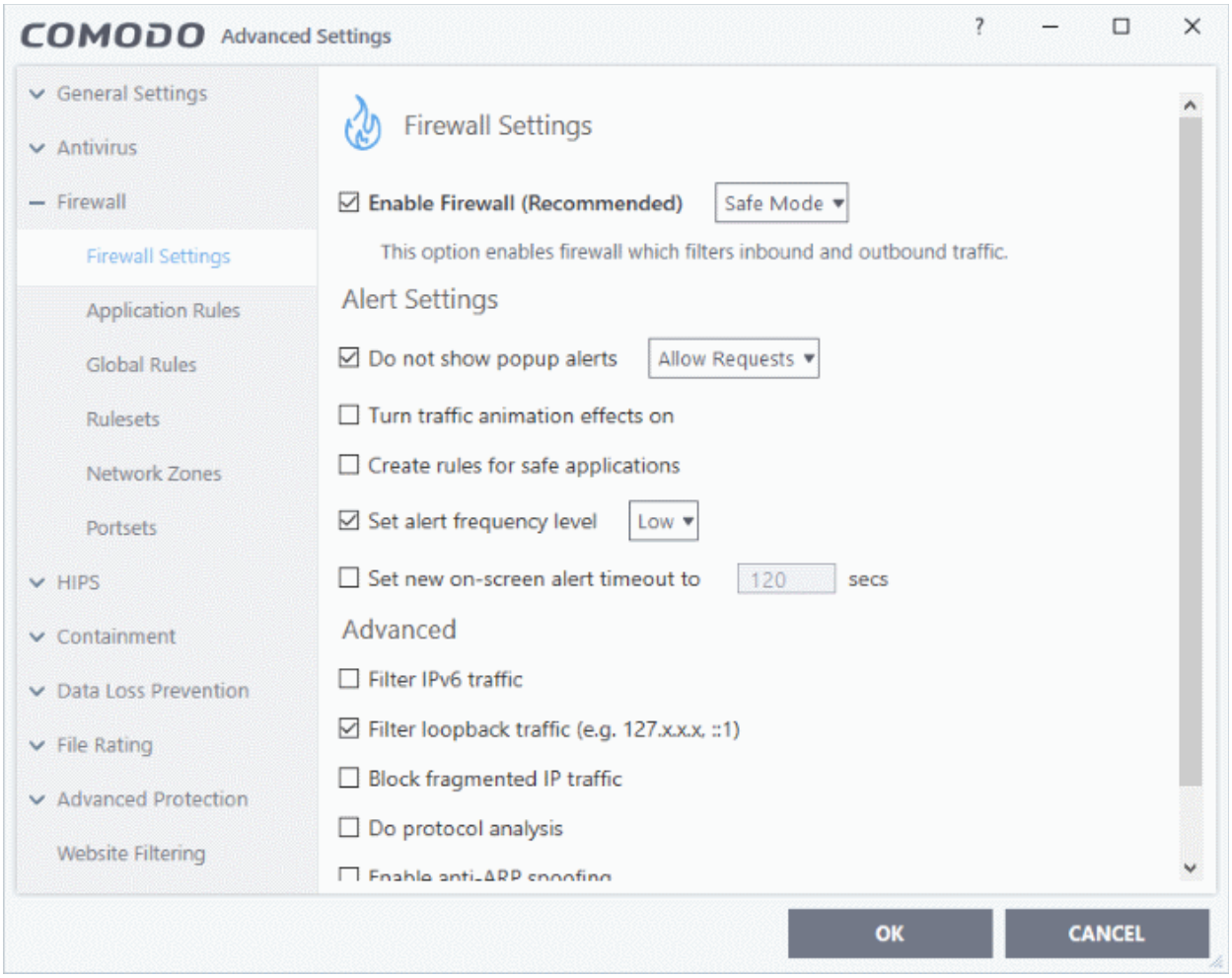
This topic explains how to configure Comodo Firewall to work with file sharing applications like Shareaza/Emule and BitTorrent/UTorrent.

To allow file sharing applications:

- **Disable 'Do Protocol analysis' (disabled, by default)**
- **Create a 'Predefined Firewall Ruleset' for Shareaza/Emule**
- **Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent**

Disable 'Do Protocol analysis'

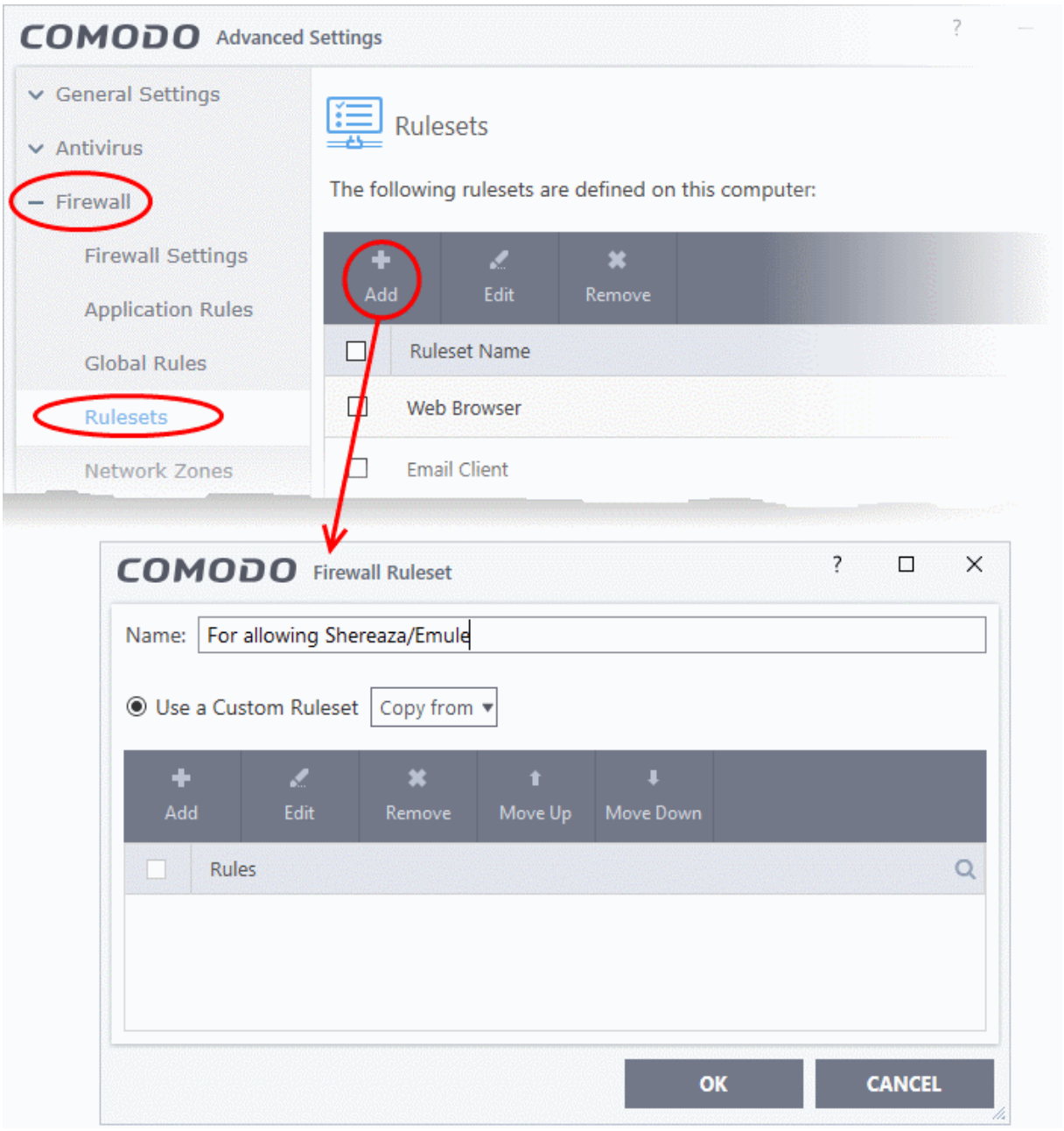
1. Click 'Settings' on the CCS home screen
2. Click 'Firewall' > 'Firewall Settings'



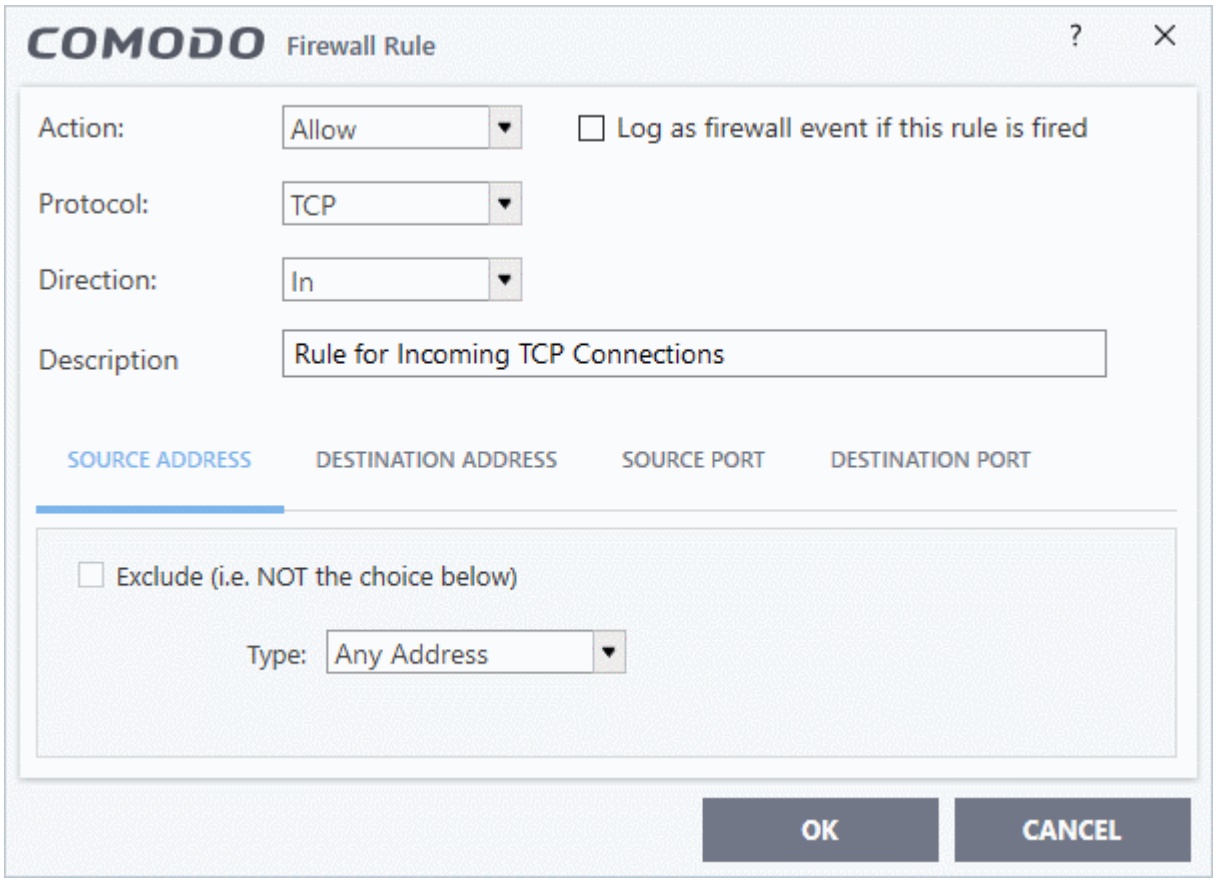
3. Disable 'Do not Show popup alerts' so CCS will generate alerts when you open Shareaza or Emule.
4. Disable 'Do Protocol Analysis'
5. Click 'OK' to save your settings.

Create a 'Predefined Firewall Ruleset' for Shareaza/Emule

1. Click 'Settings' > 'Firewall' > 'Rulesets'
2. Click 'Add' from the options at the top.



3. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing Shareaza/Emule'.
4. Now you need to create six rules for the newly created ruleset.
   - Click 'Add' to open the 'Firewall Rule' interface
   - Choose options for each setting as described in 'Rule 1' below
   - After the rule is created, click 'OK' to add the rule
   - Repeat until all 6 rules have been added



Rule 1

- Action : Allow
- Protocol : TCP
- Direction : In
- Description : Rule for incoming TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1024 / End Port = 65535)
- Destination port : A Single Port : (Port : Your TCP port of Shareaza/Emule)

Rule 2

- Action : Allow
- Protocol : UDP
- Direction : In
- Description : Rule for incoming UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1024 / End Port = 65535)
- Destination port : A Single Port : (Port : Your UDP port of Shareaza/Emule)

Rule 3

- Action : Allow
- Protocol : TCP or UDP
- Direction : Out

- Description : Rule for outgoing TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1024 / end port = 65535)
- Destination port : A port range : (start port = 1024 / end port = 65535)

Rule 4

- Action : Allow
- Protocol : ICMP
- Direction : Out
- Description : Ping the server (edk network)
- Source Address : Any Address
- Destination Address : Any Address
- ICMP Details : Message : ICMP Echo Request

Rule 5

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1024 / end port = 65535)
- Destination port : Type : Single Port; (Port : 80)

Rule 6

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.

7. Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start Shareaza or Emule. When CCS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'For allowing Shareaza/Emule')
- Select 'Remember my answer'.

Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Settings' > 'Firewall' > 'Rulesets'
2. Click 'Add' from the options at the top.
3. Enter a name for the new ruleset in the 'Description' text box. For example: 'For allowing For allowing BitTorrent/Utorrent'.
4. Now you need to create six rules for the newly created ruleset.

To do so,

- Click 'Add' to open the 'Firewall Rule' interface
- Choose options for each setting as described in 'Rule 1' below
- After the rule is created, click 'OK' to add the rule
- Repeat until all 6 rules have been added

Rule 1

- Action : Allow
- Protocol : TCP or UDP
- Direction : In
- Description : Rule for incoming TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port : A Single Port (Port: The port of BitTorrent/Utorrent)

Rule 2

- Action : Allow
- Protocol : TCP
- Direction : Out
- Description : Rule for outgoing TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port : A Port Range : (Start port = 1024 / End port = 65535)

Rule 3

- Action : Allow
- Protocol : UDP
- Direction : Out
- Description : Rule for outgoing UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Single Port: Port: the port of utorrent
- Destination port : A Port Range : (Start port = 1024 / End port = 65535)

Rule 4

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1024 / End port = 65535)
- Destination port ; A Single Port (Port = 80)

Rule 5

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP

- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

- Click 'OK' in the 'Firewall Ruleset' interface.
- Click 'OK' in the 'Advanced Settings' interface to save your ruleset.

The new ruleset will be created and added. Start BitTorrent or Utorrent. When CCS raises an alert:

- Choose 'Treat this application as...'
- Select the the ruleset you just created from the options (e.g. 'BitTorrent/Utorrent')
- Select 'Remember my answer'.

Block any Downloads of a Specific File Type

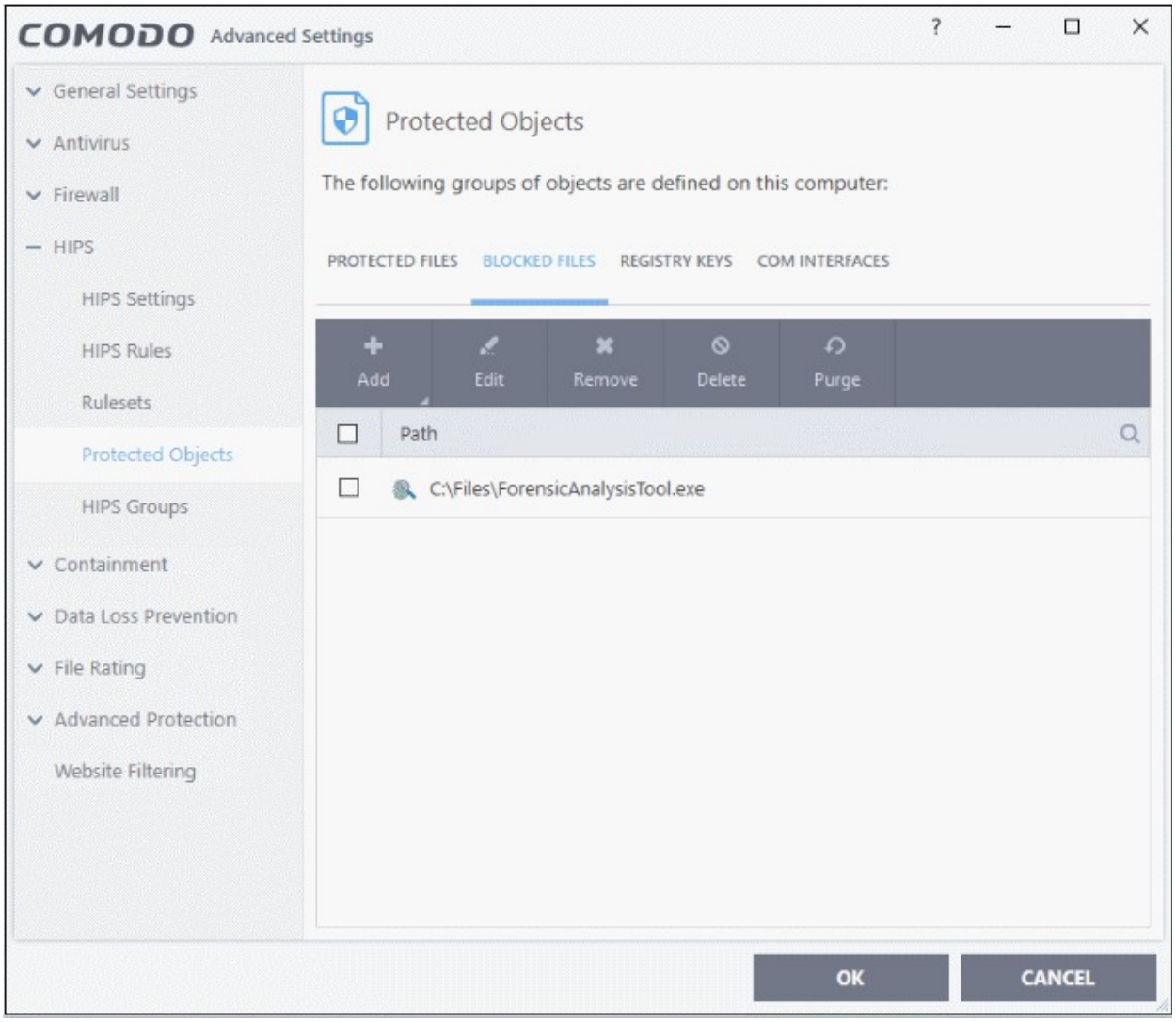
This page explains how to configure CCS to prohibit downloads of specific types of file.

Example scenarios:

- Some malicious websites try to push malware in .exe file format. These files, known as executables, can run commands on your computer. If the .exe is malicious then these commands could install a virus, initiate a buffer overflow attack or could contain code to turn your PC into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You may also want to block the download of audio files (.wma, .mp3, .wav, .midi), video files (.wmv, .avi, .mpeg, .swf) or image files (.bmp. .jpg, .png) for various reasons.

You can block downloads of a specific file type by configuring 'Blocked Files' in the HIPS module:

1. Click 'Settings' on the CCS home screen
2. Click 'HIPS' > 'Protected Objects'
3. Click the 'Blocked Files' tab:



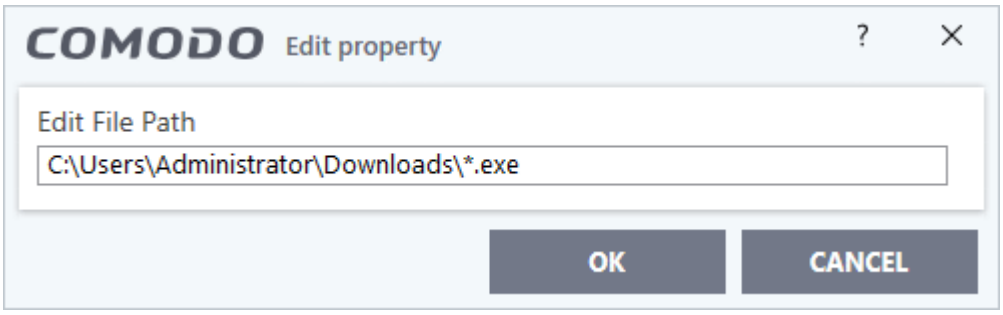
4. Click 'Add' > 'Applications'.
5. Browse to the default download folder for your browser from the 'Open' dialog:

The default download location for most browsers is C:\Users\[username]\Download.

6. Select any file from the folder and click 'Open'.

The file will be added to the 'Blocked Files' list.

7. Select the entry from the Blocked Files interface, and click 'Edit' at the top
8. Replace the name of the file with simply '*.file_extension', where 'file_extension' is the file type you wish to block. For example:
    - Change 'C:\Users\[username]\Downloads\file-name.pdf' to C:\Users\[username]\Downloads*.exe to block all files with *.exe extension.
    - Change 'C:\Users\[username]\Downloads\file-name.xls' to C:\Users\[username]\Downloads*.jpg to block all files with *.jpg extension.



9. Click 'OK' in the 'Edit Property' dialog.
10. Click 'OK' to save your settings.

This will block browser downloads of the specific file type to your 'Downloads' folder. Repeat the process if other browsers on your system have a different download folder.

Note: Blocking files in this way will only block downloads of specific file types to specific folders. If you change the folder for browser downloads then the download will be allowed.

Tip:

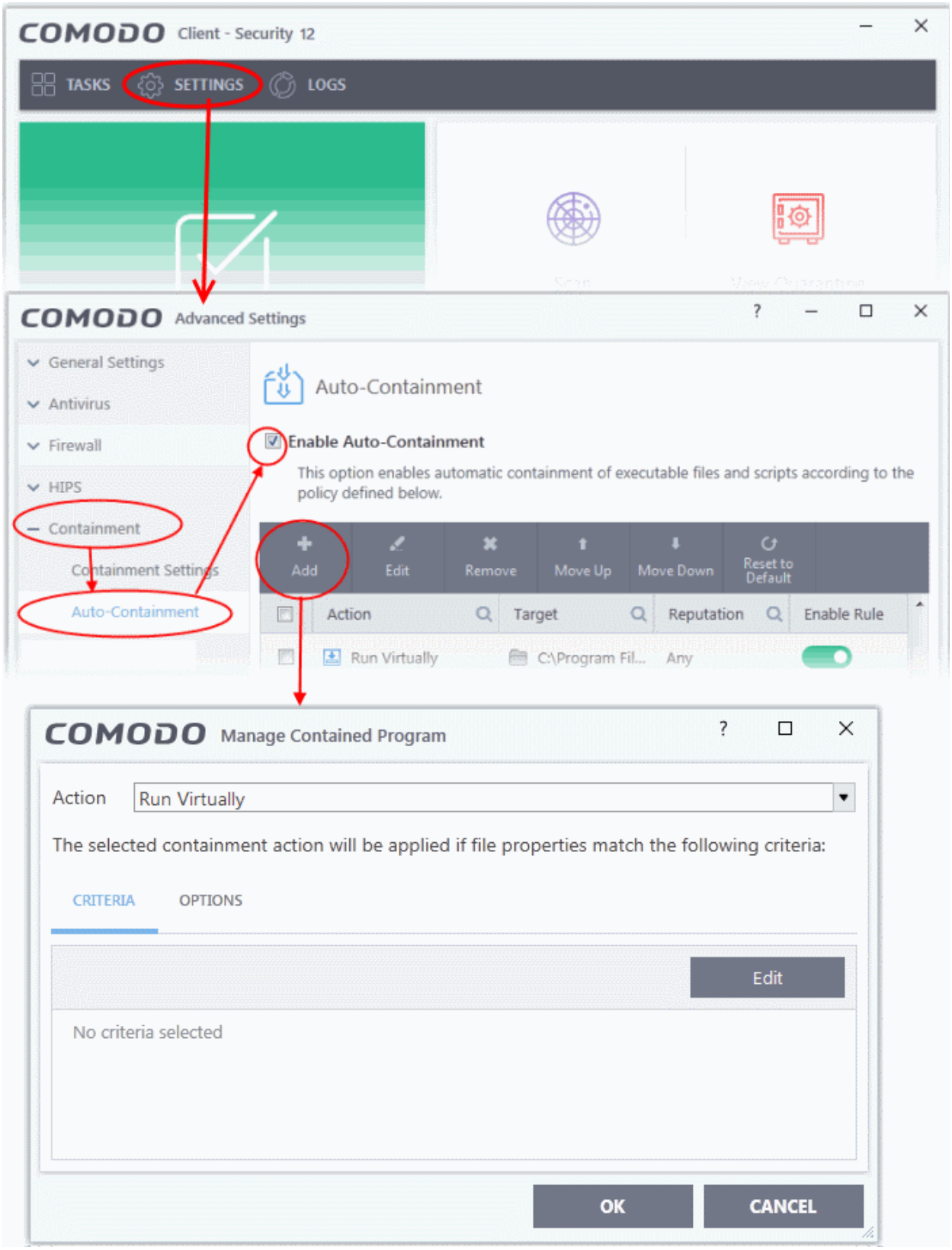
- To unblock future downloads, go to 'HIPS' > 'Protected Objects' > 'Blocked Files', select the file path, and choose 'Remove'.
- To unblock individual files, go to 'General Tasks' > 'Unblock Applications' and choose 'Unblock'.

Disable Auto-Containment on a Per-application Basis

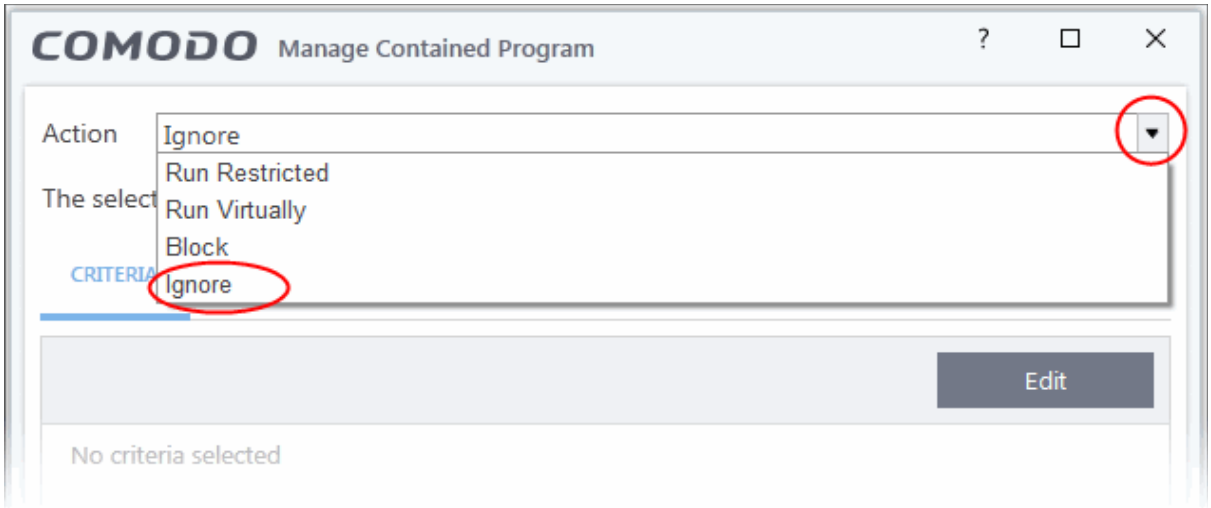
- The default auto-containment rules will run all unknown executables in the container and queue them for submission to Comodo for behavior analysis.
- We recommend most users leave this setting intact to ensure the highest protection levels.
- Should you wish, you can create an 'Ignore' rule to exclude certain files or file types from containment.
- This is could be useful for developers testing new applications which, by their nature, are unknown to the safe list.

Create an auto-containment exception

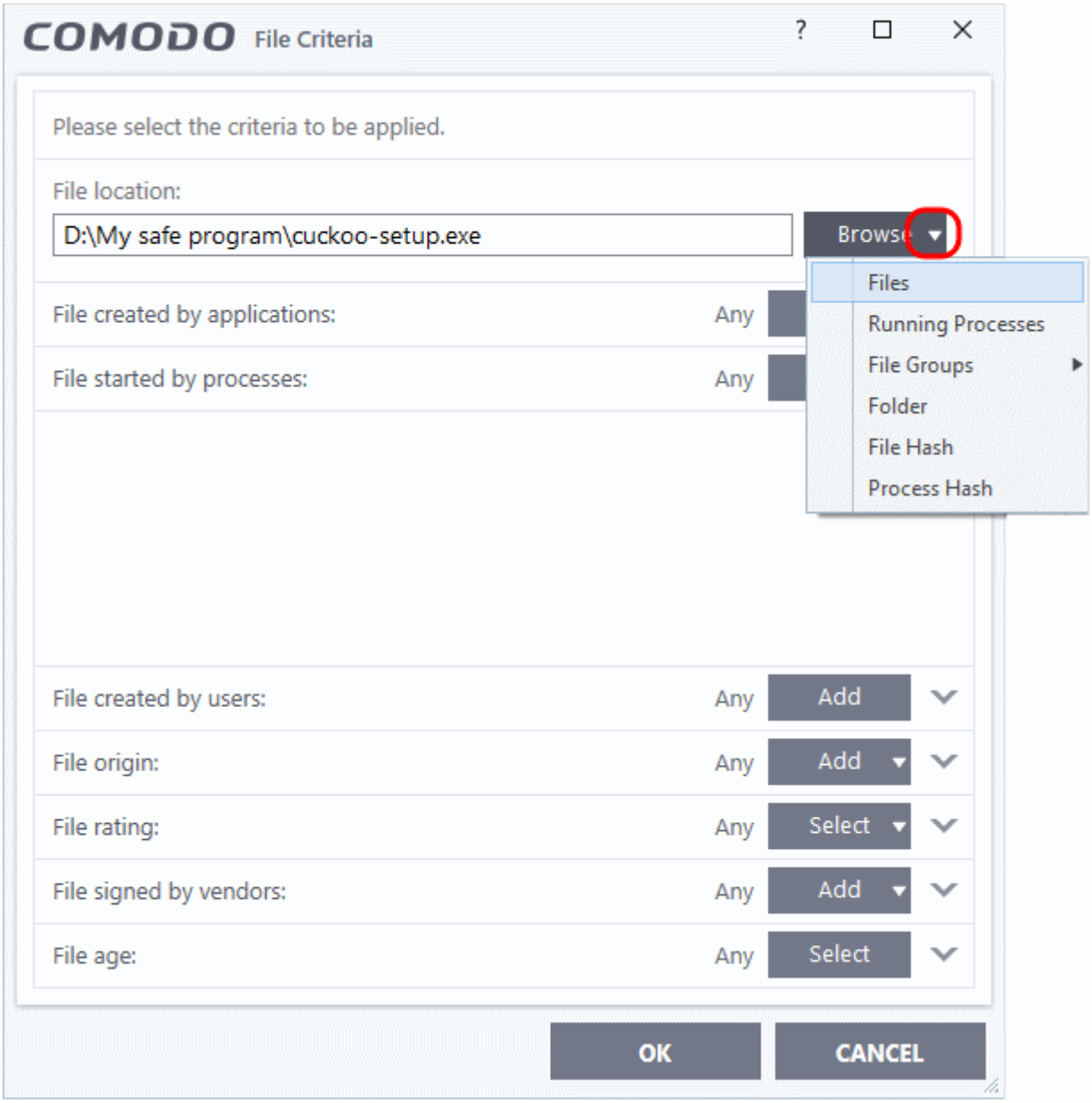
1. Click 'Settings' on the CCS home screen
2. Click 'Containment' > 'Auto-Containment' on the left
3. Ensure that 'Enable Auto-Containment' is selected
4. Click 'Add' to create a new rule:



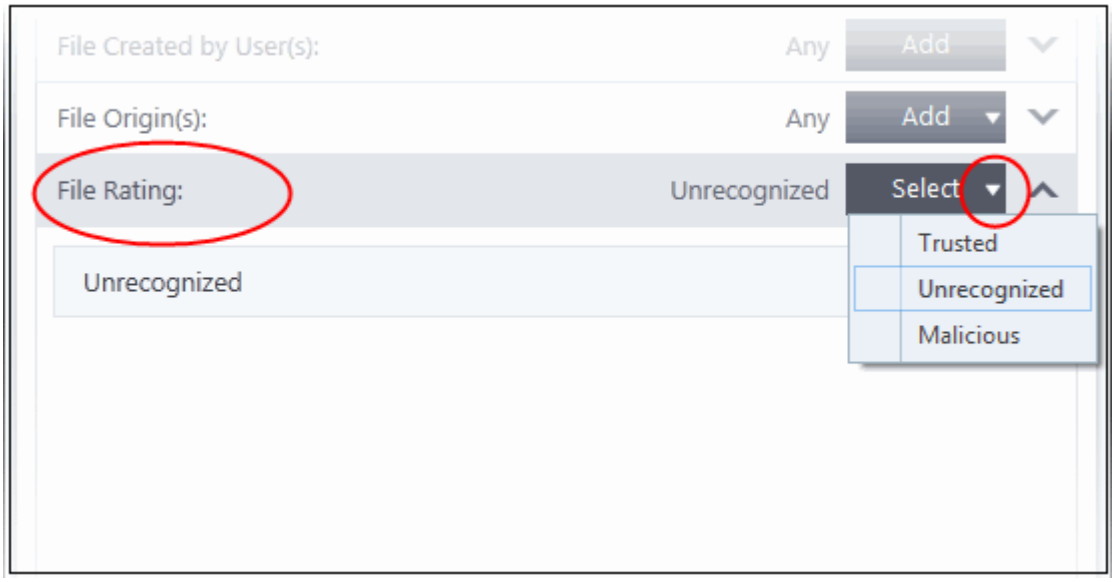
5. Select 'Ignore' from the 'Action' drop-down:



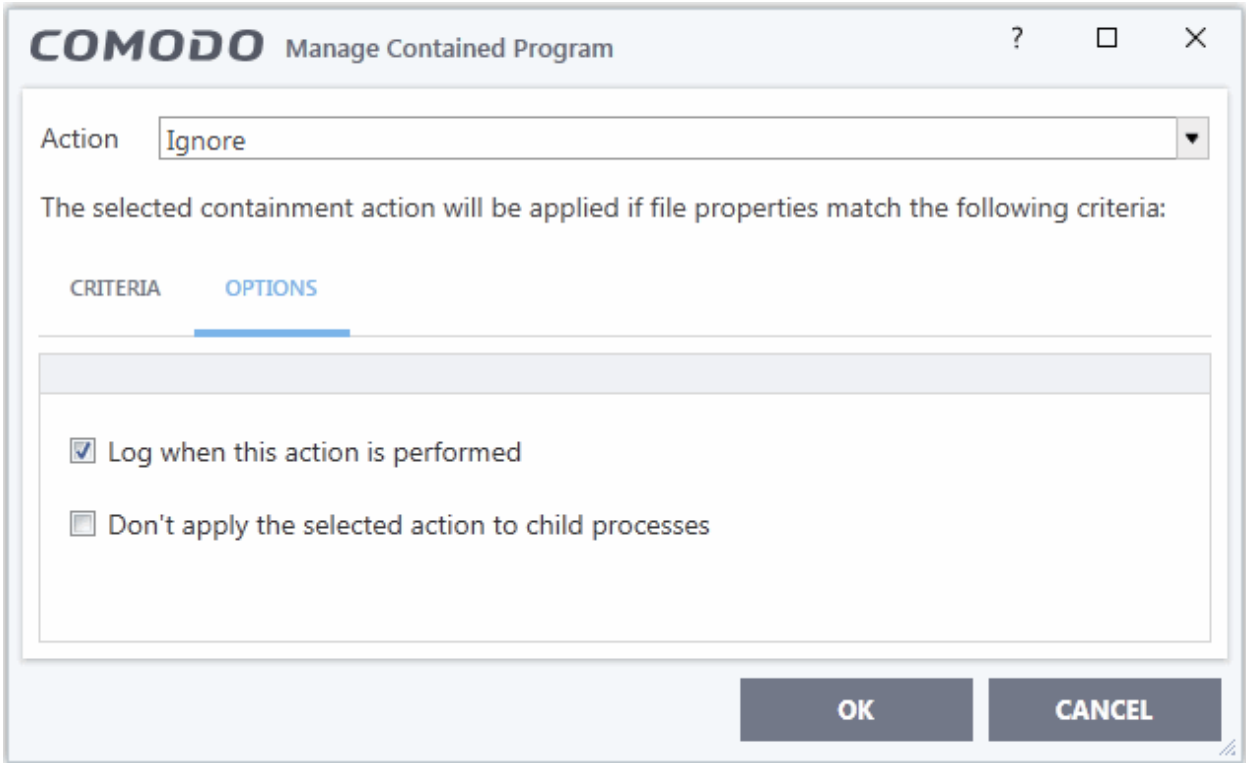
6. Click the 'Edit' button under the 'Criteria' tab
7. Click 'Browse' to specify the type of item you wish to exclude:



8. You can select individual files, folders, processes, file groups or hashes. Click 'Open' when you have made your selection.
9. Click 'Select' at the end of the 'File Rating' row and select 'Unrecognized' from the drop-down:



10. Next, click the 'Options' tab.

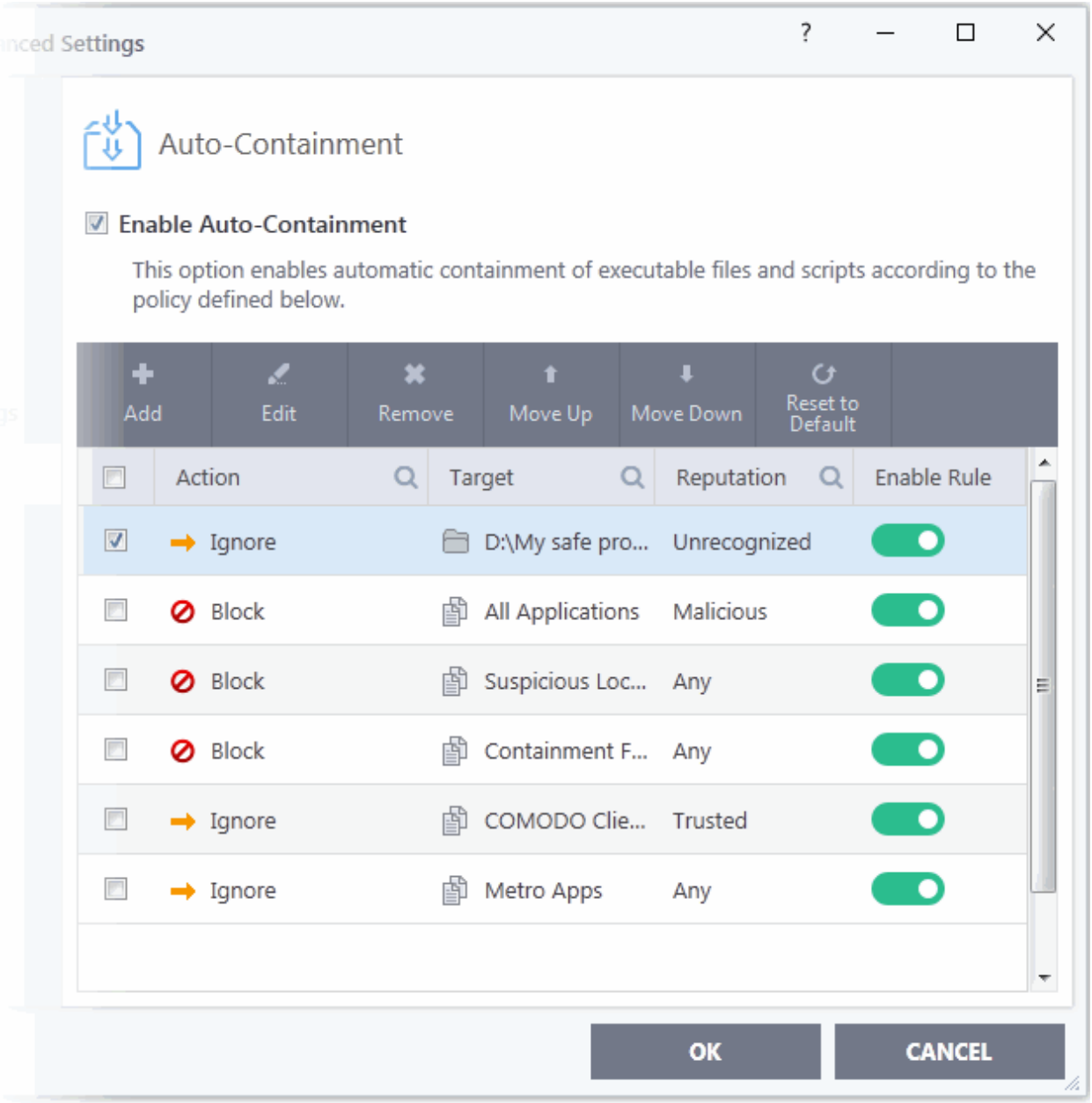


- **Log when this action is performed** - Optional. Whenever this rule is applied for a file, it will be added to CCS containment logs.
- **Don't apply the selected action to child processes** - Child processes are processes spawned by a parent application. By default, CCS treats all child processes individually.
  - Disabled - The ignore rule will apply to the target application and all child processes that it spawns. All

will be allowed to run outside the container.

- Enabled - The ignore rule will apply only to the target application. All child processes will be inspected and possibly contained as per their file rating.

11. Select options as required and click 'OK'.



The new rule will be listed in the 'Auto-Containment' screen. Make sure to keep this rule above all other rules for unrecognized files.

Alternatively...

1. Assign a 'Trusted' rating to the file in the **File List** interface
2. Digitally sign your files with a code signing certificate from a trusted CA then manually add your organization to the **Vendors List** as trusted.
3. Disable auto-containment by de-selecting the 'Enable Auto-Containment' check box in the 'Auto-containment' settings panel. *Not recommended*

See **Unknown Files: The Scanning Processes**, for more details on auto-containment process.

Switch Off Automatic Antivirus Updates

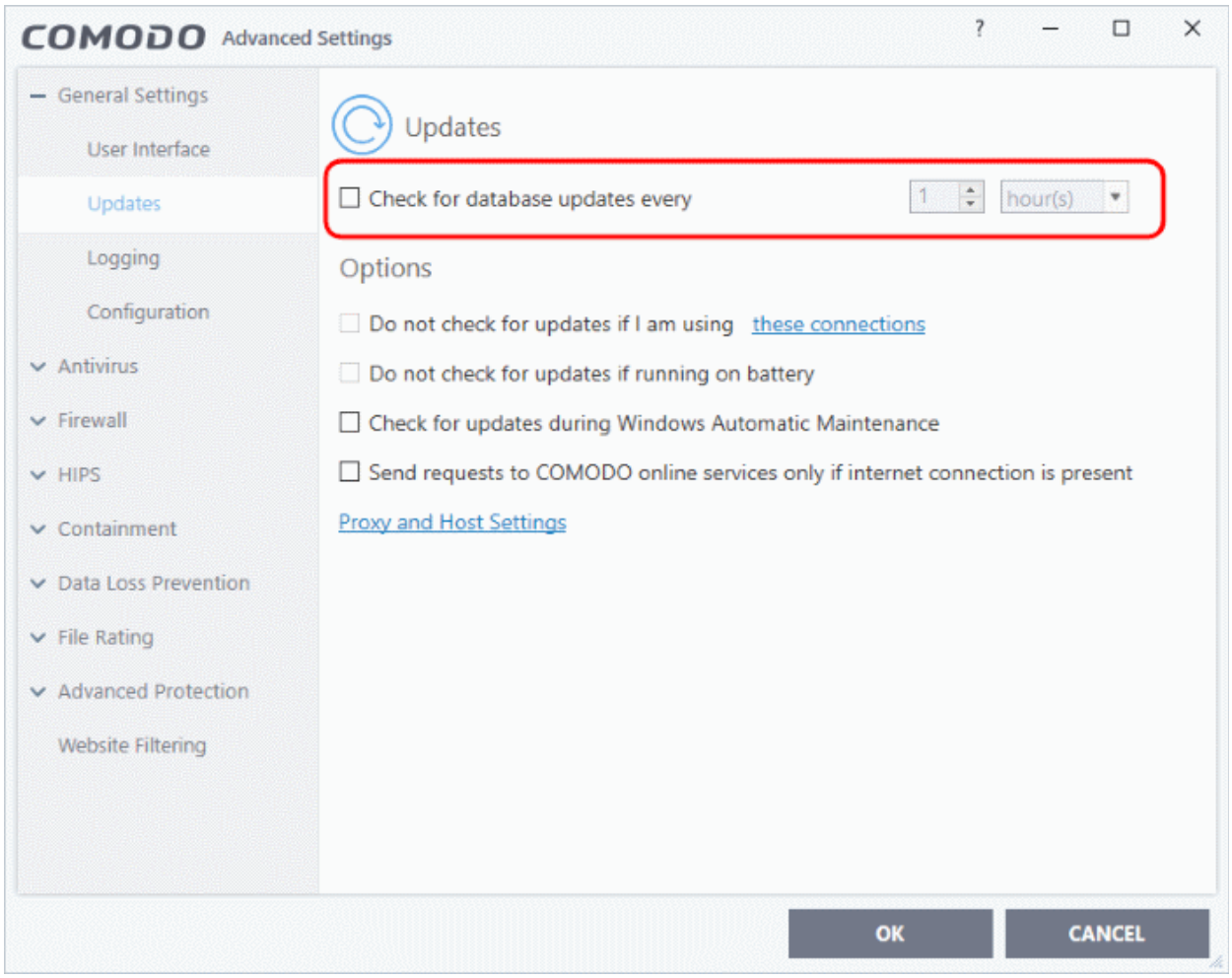
- By default, Comodo Client Security automatically downloads software and antivirus database updates.
- However, some users like to control when updates are downloaded. For example, network admins may not want automatic updates because they take up too much bandwidth during the day.

CCS provides full control over virus and software updates. Click the appropriate link below to find out more:

- **Switch off automatic updates entirely**
- **Switch off automatic virus updates selectively**
- **Switch off automatic virus signature database updates prior to Antivirus Scans**

Switch off automatic updates entirely

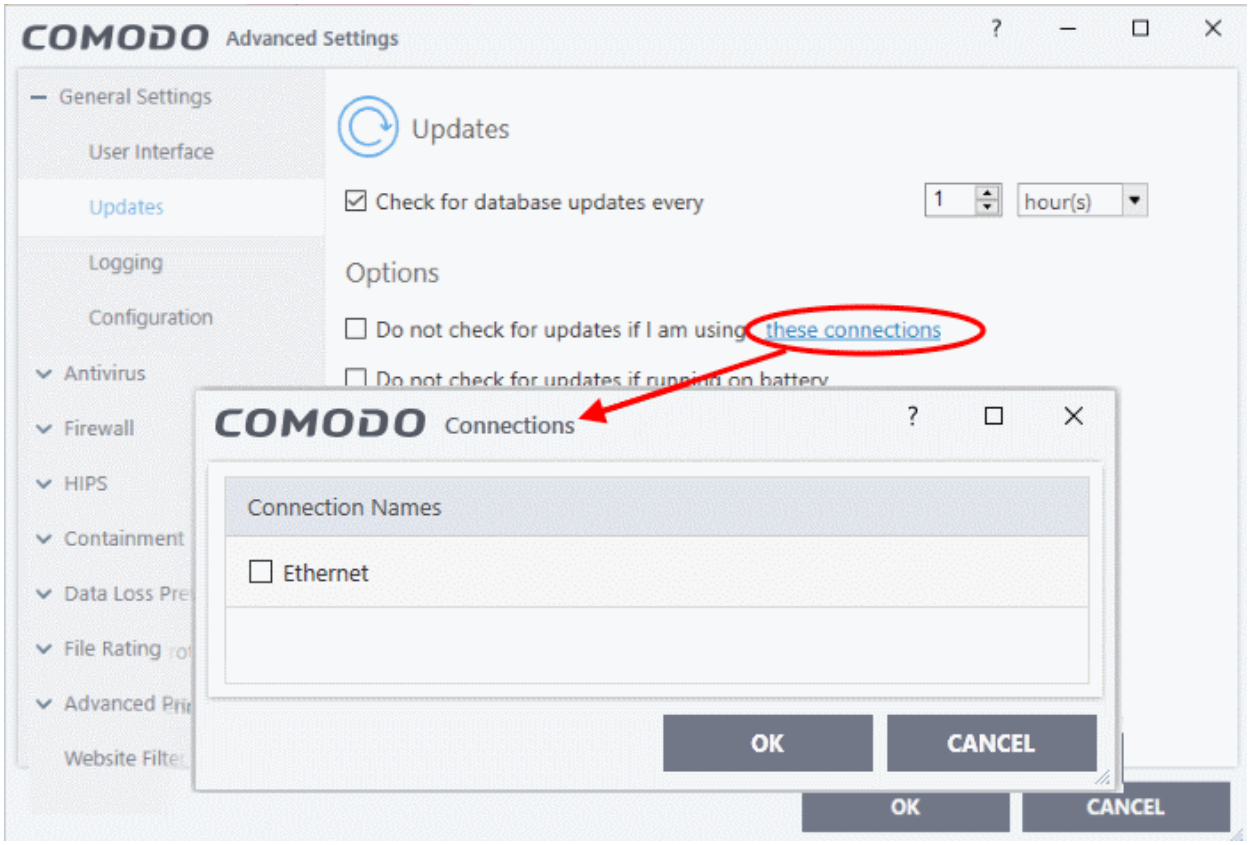
1. Click 'Settings' on the CCS home screen
2. Click 'General Settings' > 'Updates'
3. Disable 'Check for database updates every'



4. Click 'OK' for your settings to take effect

Switch off automatic updates selectively

1. Click 'Settings' on the CCS home screen
2. Click 'General Settings' > 'Updates'

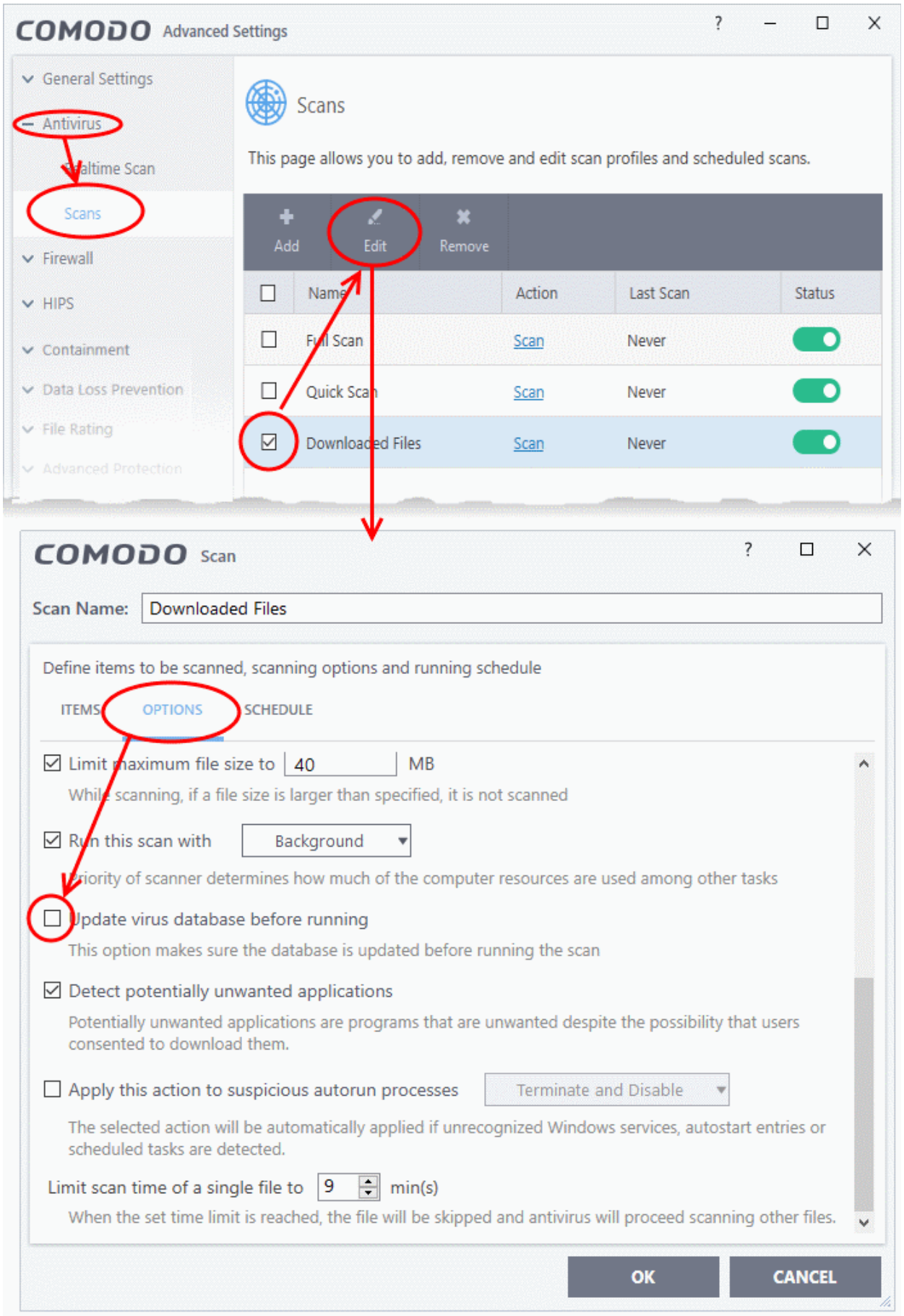


- Suppress automatic updates when using certain networks:
  - Select the 'Do not check updates if am using these connections' check-box
  - Then click 'these connections' to view a list of connections you use.
  - Select the connection over which you do not want CCS to check for updates and click 'OK.'
- **Do not check for updates if running on battery** - Will only download updates when the computer is plugged in to the mains.

5. Click 'OK' for your settings to take effect

Switch off automatic virus signature database updates prior to AV Scans

1. Click 'Settings' on the CCS home screen
2. Click ' Antivirus' > 'Scans'
3. Select a target scan profile
4. Click 'Edit' from the options at the top
5. Click 'Options', scroll down, and clear the 'Update virus database before running' checkbox.


COMODO Advanced Settings
General Settings
Antivirus
Realtime Scan
Scans
Firewall
HIPS
Containment
Data Loss Prevention
File Rating
Advanced Protection
Scans
This page allows you to add, remove and edit scan profiles and scheduled scans.
Add
Edit
Remove
Name
Action
Last Scan
Status
Full Scan
Scan
Never
Quick Scan
Scan
Never
Downloaded Files
Scan
Never
COMODO Scan
Scan Name:
Downloaded Files
Define items to be scanned, scanning options and running schedule
ITEMS
OPTIONS
SCHEDULE
Limit maximum file size to
40
MB
While scanning, if a file size is larger than specified, it is not scanned
Run this scan with
Background
Priority of scanner determines how much of the computer resources are used among other tasks
Update virus database before running
This option makes sure the database is updated before running the scan
Detect potentially unwanted applications
Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download them.
Apply this action to suspicious autorun processes
Terminate and Disable
The selected action will be automatically applied if unrecognized Windows services, autostart entries or scheduled tasks are detected.
Limit scan time of a single file to
9
min(s)
When the set time limit is reached, the file will be skipped and antivirus will proceed scanning other files.
OK
CANCEL

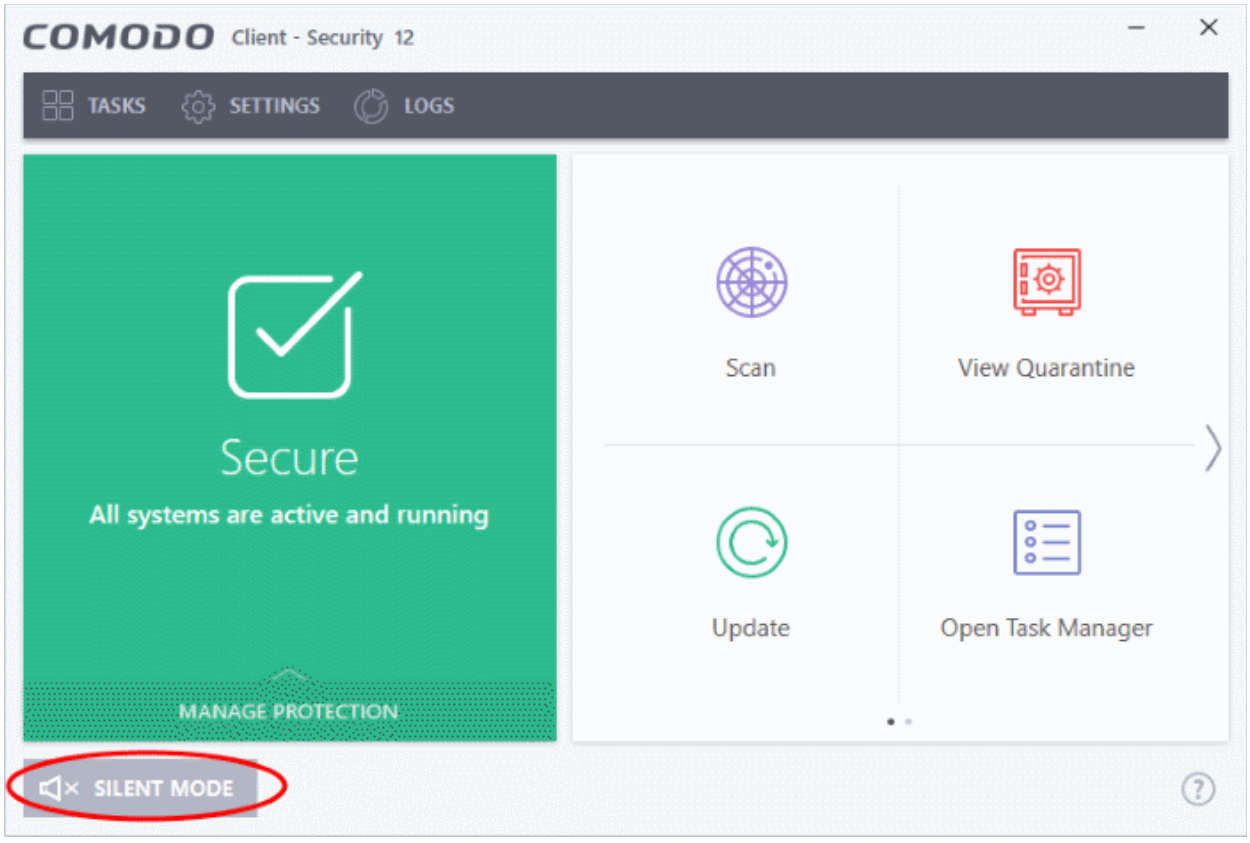
6. Click 'OK' on the 'Scan' interface.
7. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

Suppress CCS Alerts Temporarily

- CCS shows you an alert if it finds a security threat, and also shows alerts for general system messages.
- 'Silent mode' lets you temporarily disable these alerts so they don't interrupt games or a presentation etc.
- During this time, operations that can interfere with user experience are either suppressed or postponed. This includes alerts and scheduled scans.
- All protection components are still 100% active in silent mode.

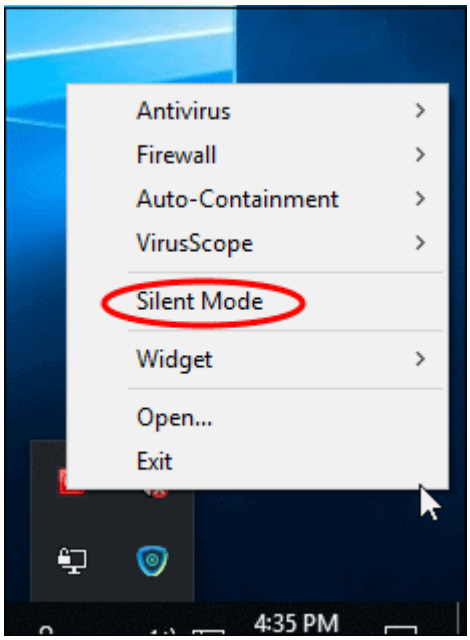
Temporarily stop pop-up alerts

- Click 'Silent Mode' button on the CCS home screen:



OR

- Right-click on the CCS tray icon and select 'Silent Mode'



The alerts are now suppressed.

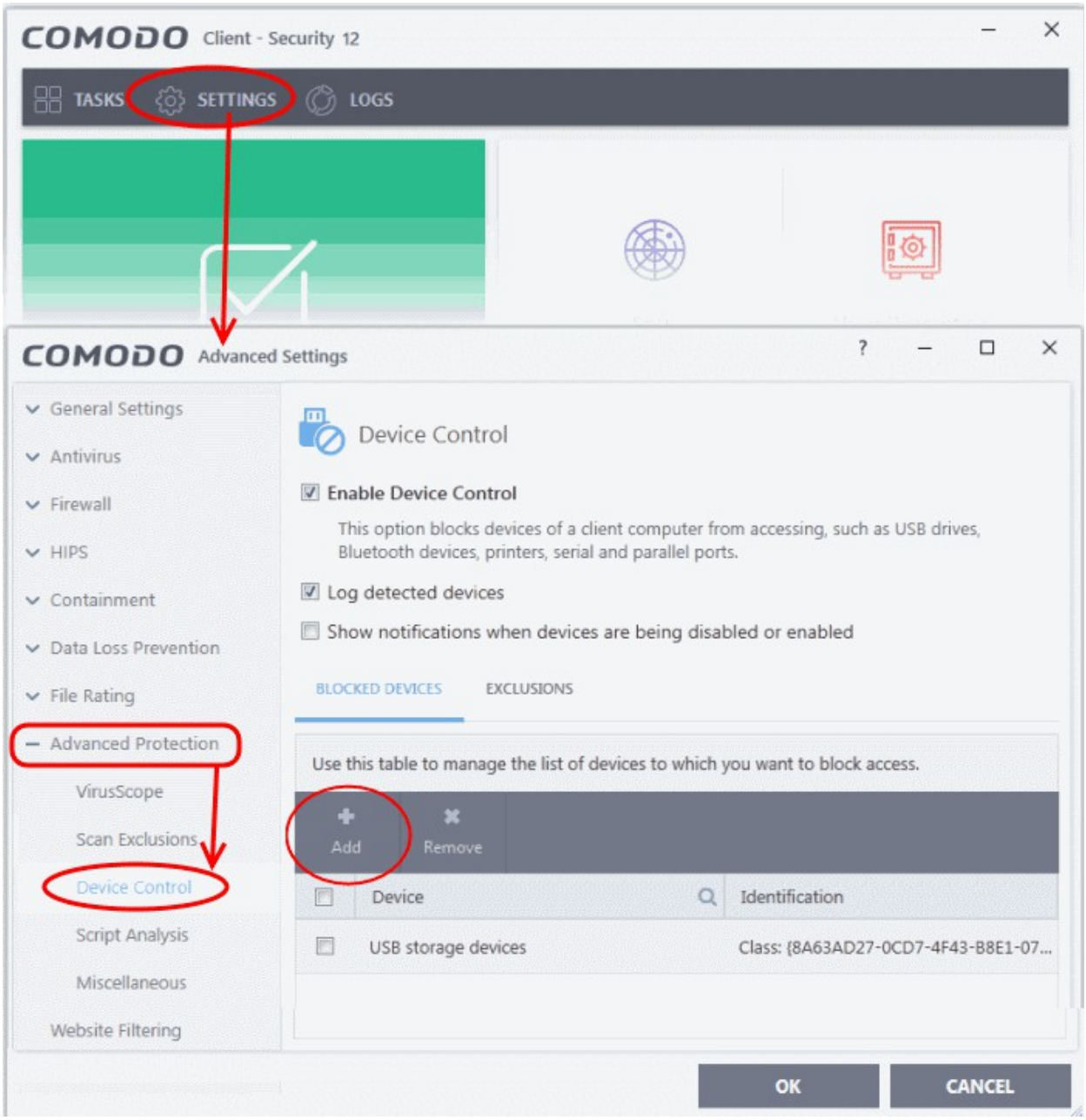
- To resume alerts and scheduled scans, just deactivate 'Silent Mode' from the home screen or tray icon.

Control External Device Accessibility

- Click 'Settings' > 'Advanced Protection' > 'Device Control'
- CCS helps you block access to selected external devices attempting to connect to your computer.
- The 'Device Control' panel lets you specify types of external devices that are to be blocked and define exclusions to it

Block an external device

1. Click 'Settings' on the CCS home screen
2. Click 'Advanced Protection' > 'Device Control'



- **Enable Device Control** - Activate the device control functionality to selectively prohibit access to external devices. You should specify devices to be banned in the 'Blocked Devices' pane. ***(Default = Enabled)***
- **Blocked Devices** - List of external device classes which are not allowed to connect to the endpoint. Example classes include 'USB Storage Devices', 'CD/DVD Drives', 'BlueTooth Devices' and 'Firewire Devices'.
- **Exclusions** - Add exceptions to a blocked class. For example, if you wish block the class 'USB Devices' but wish to allow access for your company's authentication tokens, then you should add those USB tokens as exceptions.

Click 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 address) or a 128-bit number (IPv6 address). While this is perfectly satisfactory for computers, humans are far more comfortable remembering names rather than a string of numbers. The 'Domain Name System' (DNS) provides the translation between those names and numbers. Virtually every piece of software, device, and service on the internet utilizes DNS to communicate with one another. DNS also makes this information available across the entire span of the internet, allowing users to find information remotely.

Comodo Secure DNS is a broadly distributed Recursive DNS service that gives you full control to determine how your clients interact with 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. 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**

Router - Enable or Disable Comodo Secure DNS

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. We recommend 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

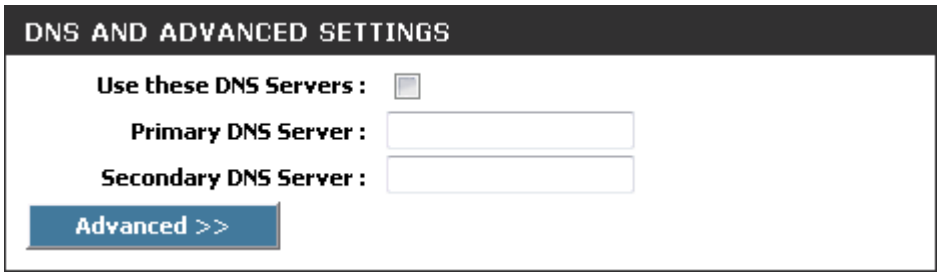
Modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

   http://192.168.0.1
   http://192.168.1.1
   http://192.168.10.1

   If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).

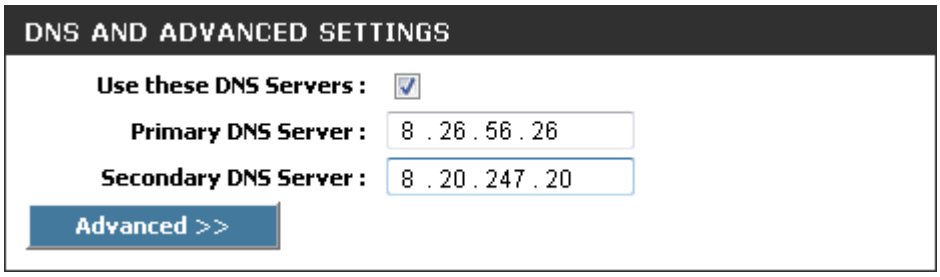


3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

   Primary DNS server address for Comodo Secure DNS is: 8.26.56.26

   Secondary DNS server address for Comodo Secure DNS is: 8.20.247.20

   When you are done, the above example would look like this.



Disable Comodo DNS

You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

OR

- Entering different preferred and alternate DNS server IP addresses.

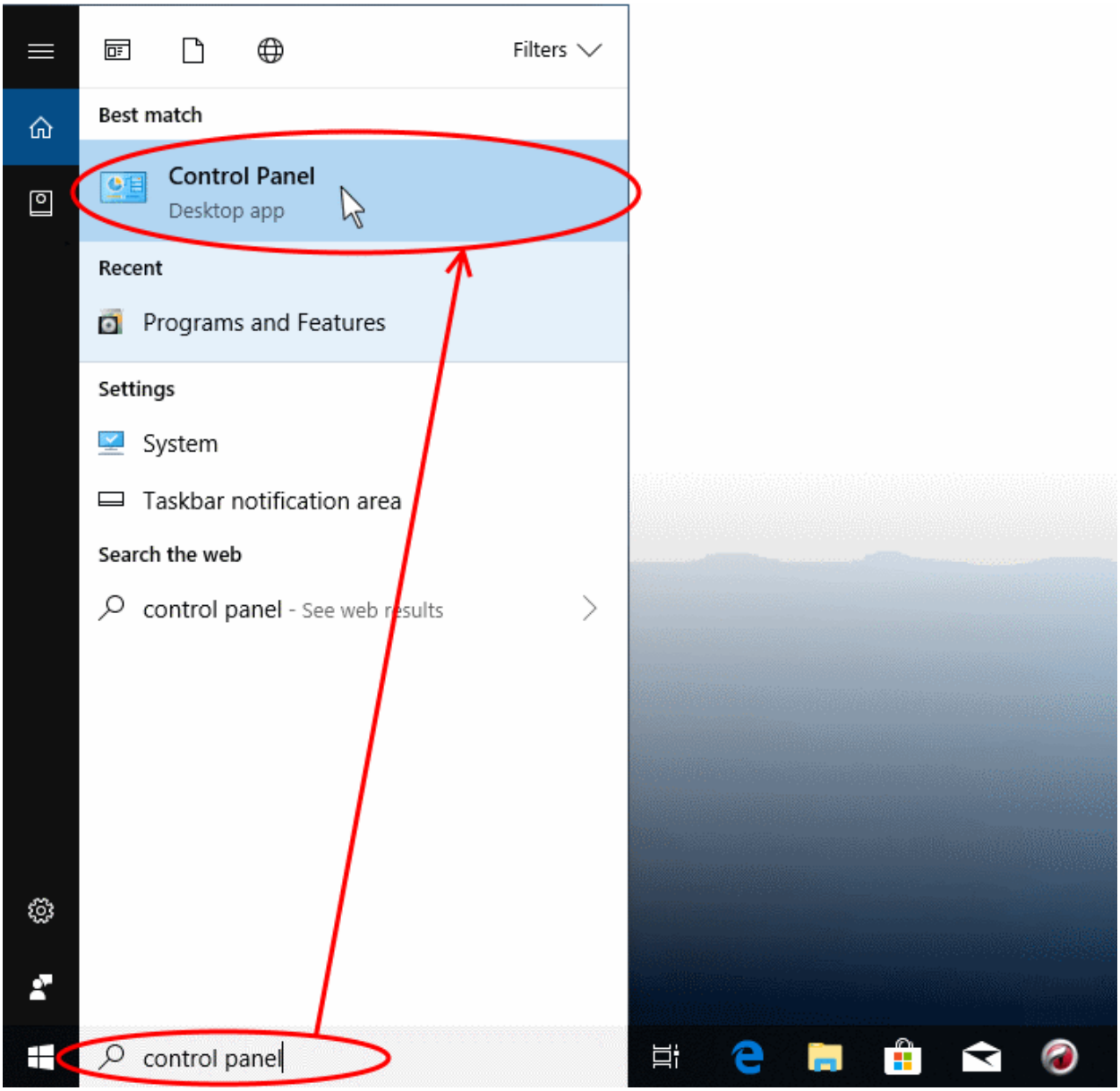
Windows - Enable Comodo Secure DNS

You can manually enable Comodo Secure DNS by changing your DNS server addresses to:

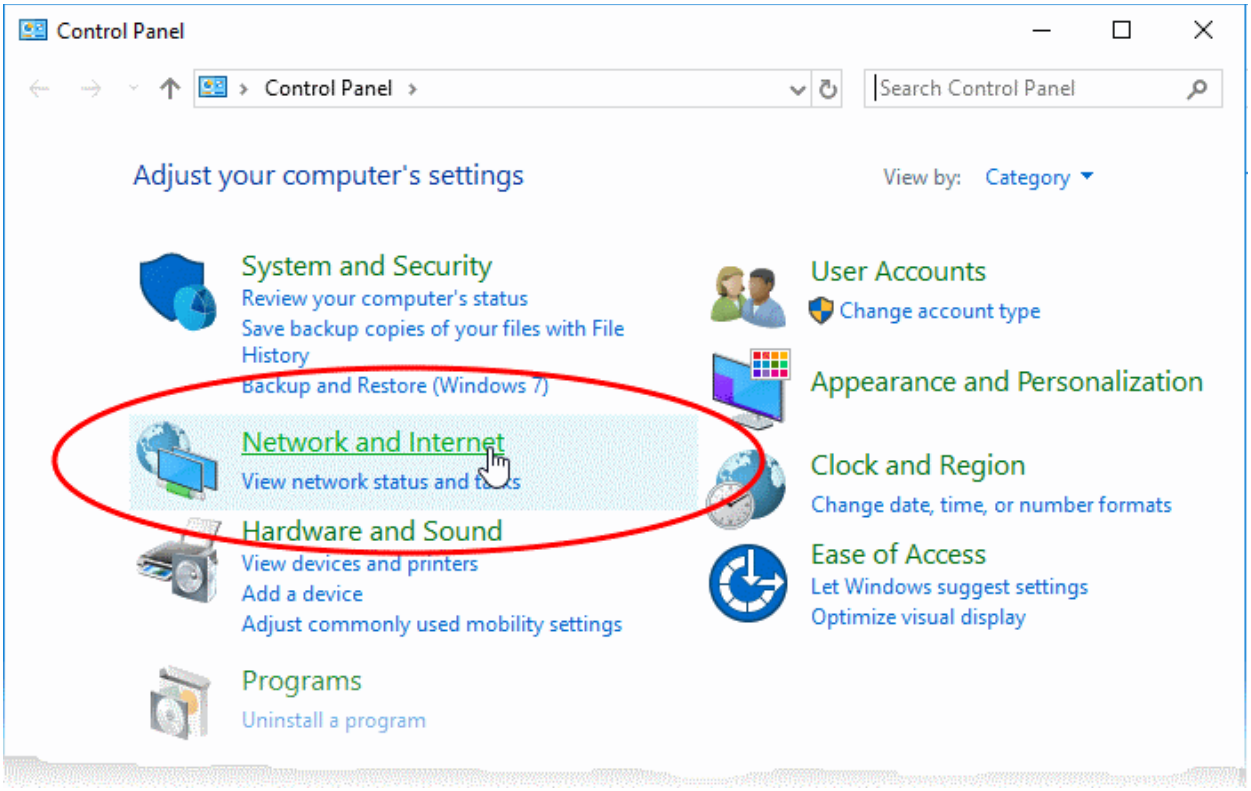
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

Enable Comodo Secure DNS

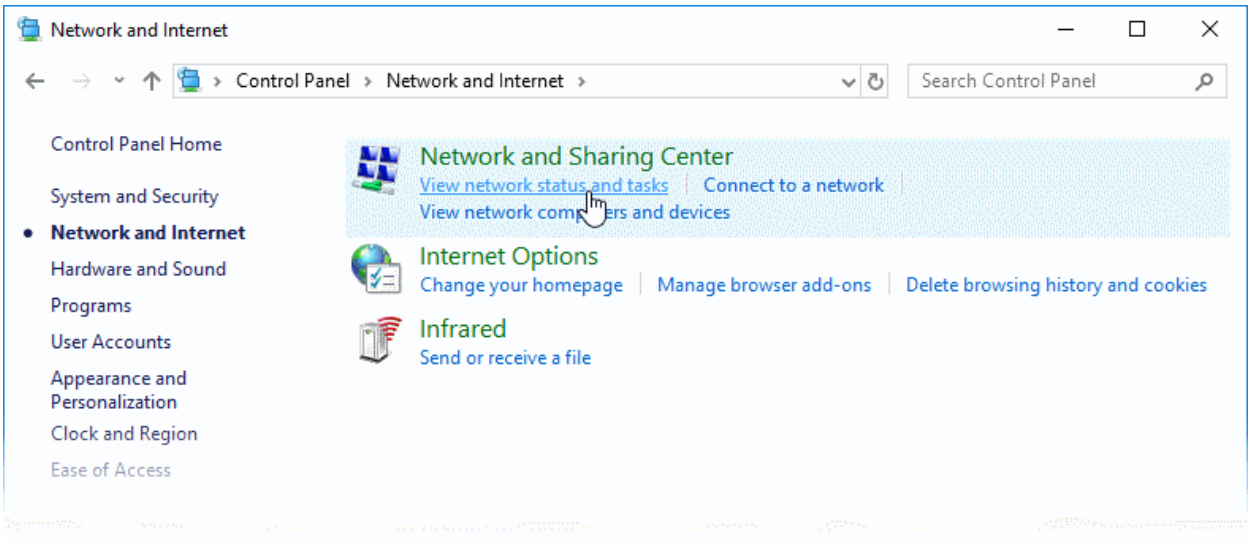
1. Click the Windows 'Start' menu
2. Type 'control panel' into the search box then click the program name:



3. Select 'Network and Internet' from the control panel menu:

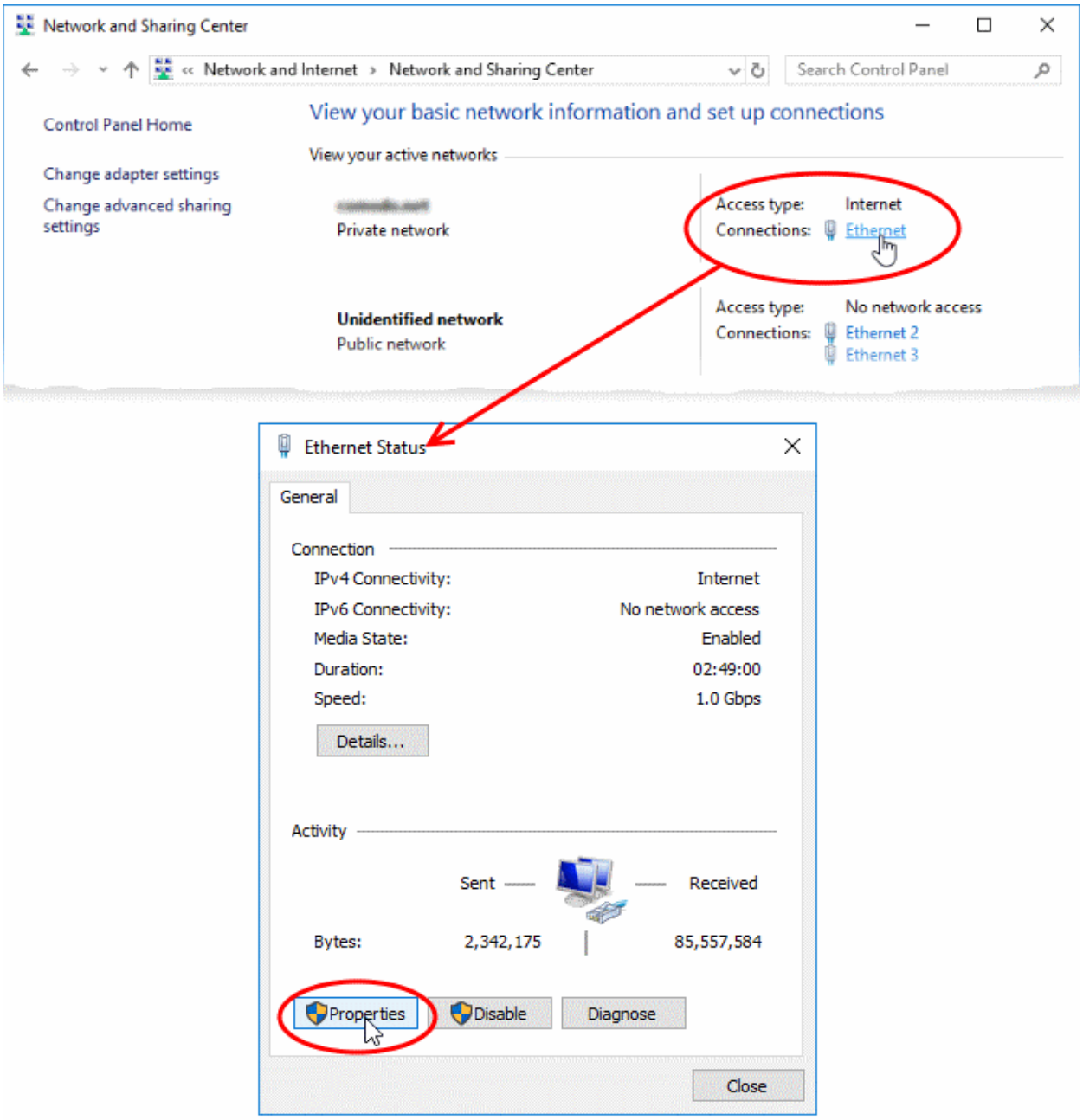


4. Select 'View network status and tasks' under Network and Sharing Center' as shown below:



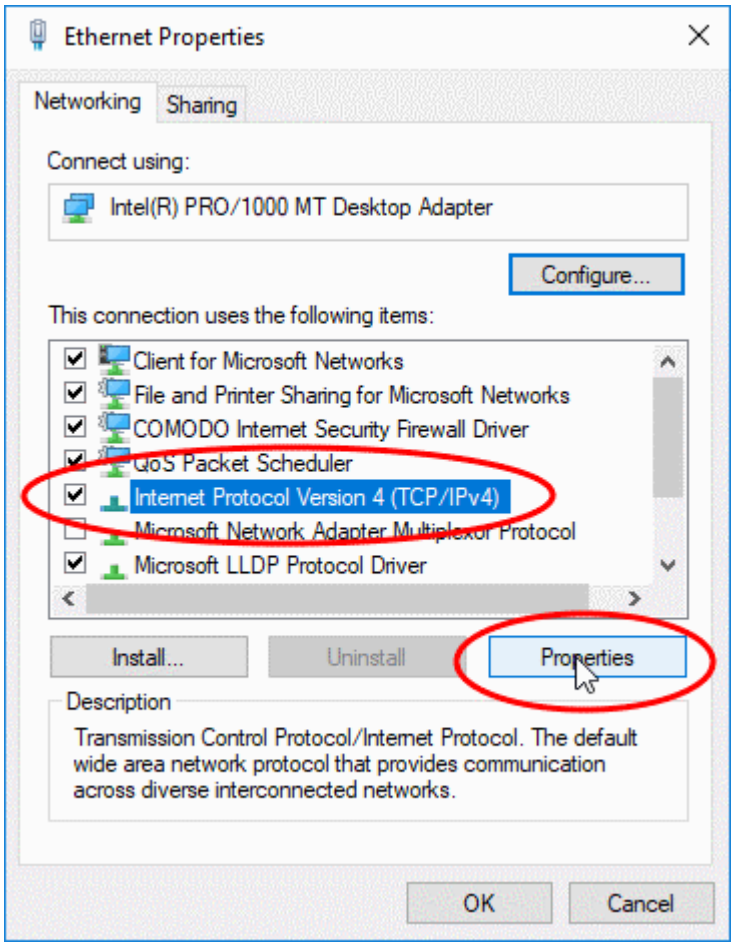
The list of networks to which you are currently connected is shown.

5. Click the network type link in the network through which you are connected to internet:



This opens the 'Status' dialog for the selected connection.

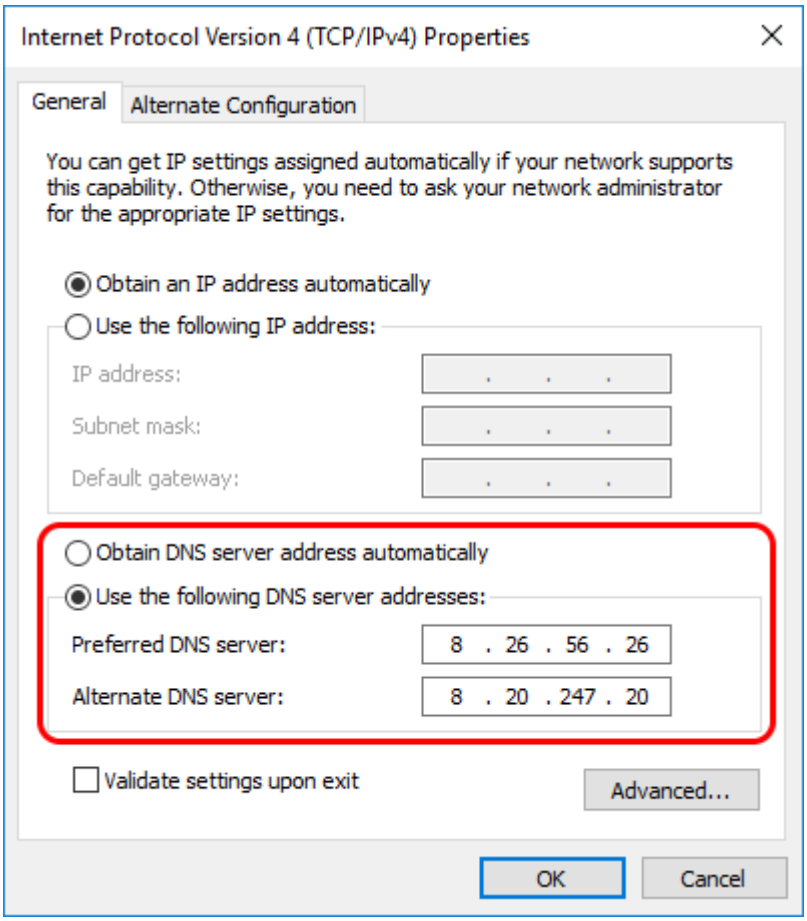
6. Click 'Properties' in the status dialog
    - At this point, Windows might ask for your permission to continue or request that you enter an administrator password.
    - Once you have granted permission/entered an admin password, the 'Connection Properties' dialog appears:



7. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button as shown above.
8. Enable 'Use the following DNS server addresses'.
9. Enter the addresses listed below:

   Preferred DNS : 8.26.56.26

   Alternate DNS : 8.20.247.20



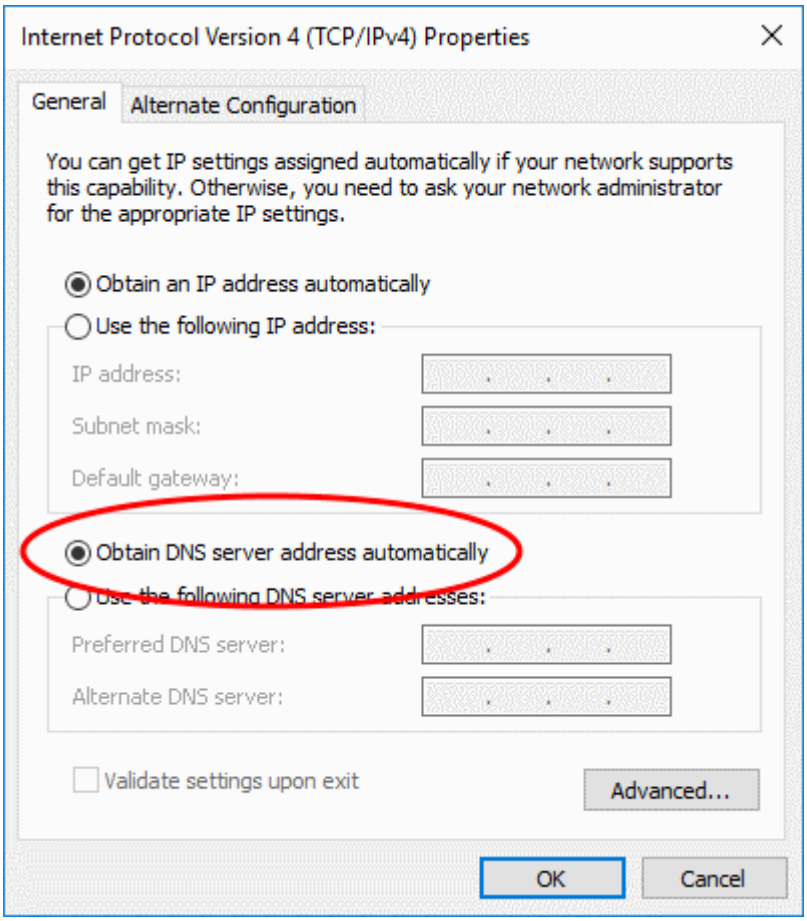
10. Click 'OK' to save your settings
11. Click 'OK' in the connection properties dialog to activate your settings

- Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the internet.

Disable Comodo DNS

You can revert to the DNS servers provided by your ISP at anytime by instructing Windows to automatically obtain the address of a DNS servers.

- Follow steps 1 to 7 of the '**Enable Comodo DNS**' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'