COMODO
Creating Trust Online®

Comodo
Internet Security

Software Version 8.2

User Guide

Guide Version 8.2.061115

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

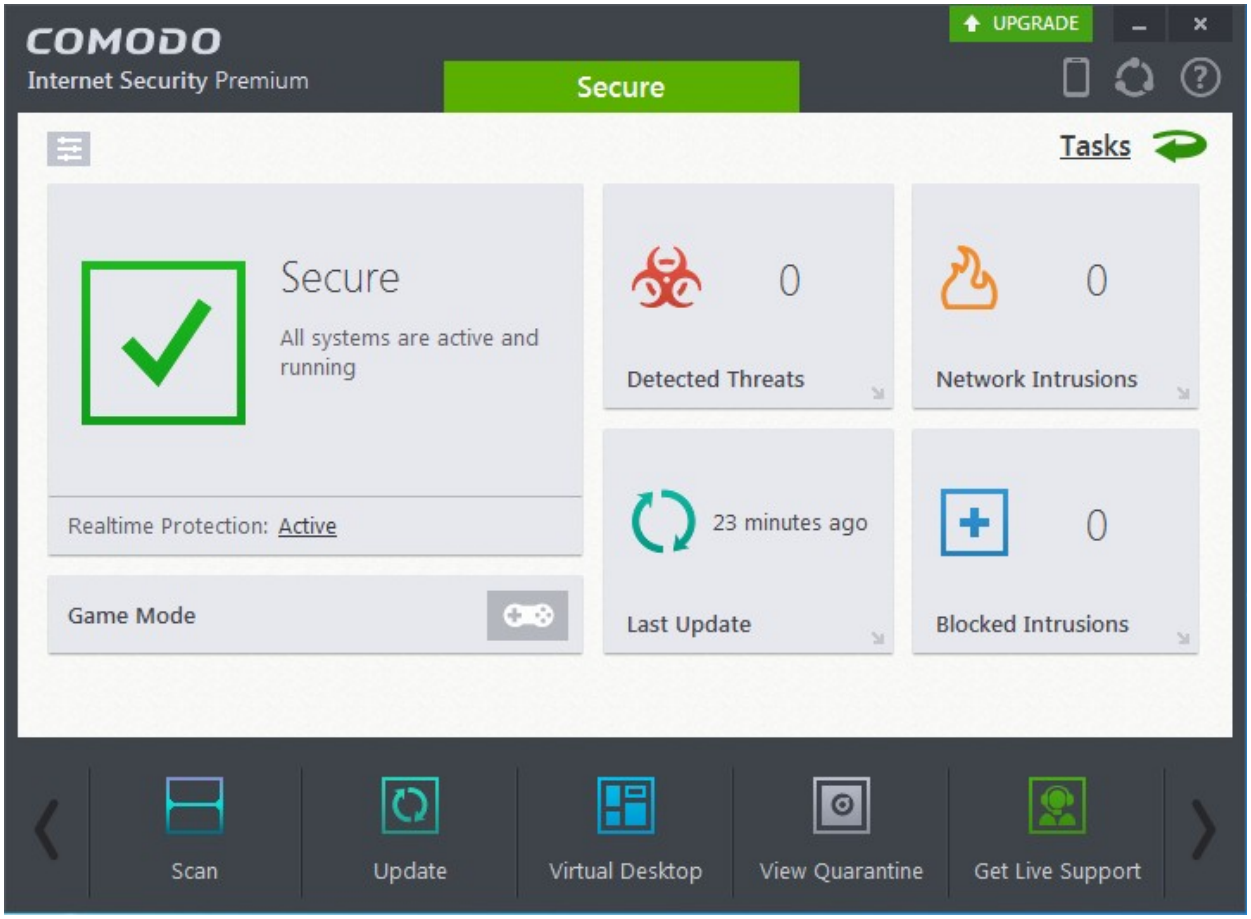
Table of Contents

1.Introduction to Comodo Internet Security

Overview

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

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



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

Comodo Internet Security - Key Features:

- **Antivirus -** Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the powerful on-demand, on-access and scheduled scan capabilities, CIS users can now simply drag-and-drop items onto the home screen to run an instant virus scan.
- **Firewall -** Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.
- **Defense+ -** A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
    - **Sandbox** - Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be auto-sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but

harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

- **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **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.

- **Virtual Desktop** - The Virtual Desktop is a sandboxed operating environment inside of which you can run programs and browse the Internet without fear that those activities will damage your real computer. Featuring a virtual keyboard to thwart key-loggers, home users will find the virtual desktop is ideally suited to sensitive tasks like online banking. Advanced users will appreciate the ability to run beta-software in an environment that will not upset the stability or file structure of their production systems
- **Website Filtering** - Protects you from phishing sites while surfing the 'net and allows you to create rules to prevent specific users from accessing certain websites. CIS ships with several preset lists of malicious websites which form an effective website screening and protection feature for all Internet users. Furthermore, you can easily add or import your own lists of banned URLs and can set up custom access rules for each user on your computer.
- **Rescue Disk -** Built-in wizard that allows you to burn a boot-disk which will run antivirus scans in a pre-Windows / pre-boot environment.
- **Additional Utilities -** The advanced tasks section contains links that allow you to install other, free, Comodo security products - including Comodo Cleaning Essentials and KillSwitch.
- **Chromodo Browser** - Fast and versatile Internet Browser based on Chromium, infused with Comodo's unparalleled level of Security.
- **GeekBuddy** - 24x7 online support service in which Comodo technicians are ready to deal with any computer issues you may have over an instant messenger style interface.
- **Secure Wireless Internet Connectivity** (*Complete version only*) - TrustConnect makes surfing the web safe from any public Wi-Fi location
- **Comodo Guarantee** (*Pro and Complete versions only*) - If your computer becomes damaged as a result of malware and Comodo support services cannot return it to a working condition then well pay the costs of getting it repaired. Please see the **End User License Agreement** for full details.
- **Online BackUp** (*Complete version only*) - Back-up your important data to Comodo's highly secure servers. Data is encrypted and can accessed only by the user from any Internet connected computer in the world (50GB storage space).

Guide Structure

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

- Introduction
  - Special Features
  - System Requirements
  - Installation
    - CIS Premium - Installation
    - CIS Pro - Installation and Activation
    - CIS Complete - Installation and Activation
    - Activating CIS Pro/Complete Services after Installation
  - Starting Comodo Internet Security
  - The Main Interface
  - Understanding Security Alerts

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

- General Tasks - Introduction

1.1. Special Features

Sandbox

- Authenticates the integrity of every program before allowing it to load into your computer's memory
- Performs Cloud Based Behavior Analysis for immediate identification of Malware
- Alerts you every time an unknown or untrusted applications attempts to run or install
- Blocks Viruses, Trojans and Spy-ware before they can ever get onto your system
- Prevents unauthorized modification of critical operating system files and registry entries
- Detects suspicious actions actions taken by processes all allows you to undo them
- Includes auto-sandbox feature to completely isolate untrusted files from the rest of your computer

Viruscope

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

Host Intrusion Prevention System

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

Virtual Desktop

An innovative sandboxed environment to run programs and browse the Internet isolated from your real computer. Applications

and browsers running inside the virtual desktop leave no cookies or history behind on your real system, making it an extremely secure environment for Internet banking and online shopping.

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

Advanced Network Firewall Engine

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

- Stealth Mode to make your PC completely invisible to opportunistic port scans;
- Wizard based auto-detection of trusted zones;
- Predefined Firewall policies allow you to quickly implement security rules;
- Diagnostics to analyze your system for potential conflicts with the firewall and much more;
- Website Filtering enables you to set up user based access restriction to specific websites.

Comprehensive Antivirus Protection

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

Intuitive Graphical User Interface

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

Comodo GeekBuddy (Pro, Complete versions only)

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

The services include:

- Virus & Malware Removal
- Internet and Online Identity Security
- Printer or Email Account Setup
- Software Activation

- General PC Troubleshooting
- Computer Power Setting Optimization
- Comodo Software Installation and Set up
- Comodo Account Questions.

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

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

Comodo TrustConnect

Included with a Complete subscription, Comodo TrustConnect is a fast, secure Internet proxy service that makes surfing the web safe.

- At Coffee shops, Hotels and Airports;
- At any other public Wi-Fi location;
- At your home location;
- For Enterprises with remote workers and road-warriors that need secure access to internal networks.

Comodo Backup

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

- Quickly create backups of your priceless data to a wide range of storage media
- 50 GB of highly secure online storage space that allows you to access your files from anywhere
- Step-by-step wizards allow you to create your first backup within minutes
- Flexible storage options allow you to specify full, incremental or differential backups.
- Granular scheduling options to take automatic backups at a time that suits you.
- Quick recovery of files with a few clicks of the mouse.
- Powerful encryption options to protect your files so that it cannot be accessed by anyone but you.

Chromodo Browser

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

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

Comodo Internet Security - Extended Features

Highly Configurable Security Rules Interface

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

Application Behavior Analysis

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

Cloud Based Behavior Analysis

Comodo Internet Security features cloud based analysis of unrecognized files, in which any file that is not recognized and not in Comodo's white-list will be sent to Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes.

Viruscope

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

Website Filtering

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

Event logging

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

Memory Firewall Integration

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

'Training Mode' and 'Clean PC' Mode

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

Application Recognition Database (Extensive and proprietary application safe list)

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

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

Self Protection against Critical Process Termination

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

Sandboxing as a security feature

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

Submit Suspicious Files to Comodo

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

1.2. System Requirements

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

Windows 10 Support (Both 32-bit and 64-bit versions) Windows 8 (Both 32-bit and 64-bit versions) Windows 7 (Both 32-bit and 64-bit versions) Windows Vista (Both 32-bit and 64-bit versions)	• 384 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • Internet Explorer Version 5.1 or above
Windows XP (Both 32-bit and 64-bit versions)	• 256 MB available RAM • 210 MB hard disk space for both 32-bit and 64-bit versions • Internet Explorer Version 5.1 or above

Important note: The auto-sandbox and Virtual Desktop features are not supported on Windows XP 64 or Windows Server 2003 64 bit.

1.3. Installation

Before you install Comodo Internet Security, read the installation instructions carefully and also review the system requirements. Additional services and features such as activation of your GeekBuddy account and/or Comodo Guarantee are carried out after the base installation has been completed.

Please note - the CIS software itself is identical for all customers regardless of the package type. All versions (including free) include all security features, technologies and updates. The difference between the package types lies in the availability of additional services such as GeekBuddy, rustConnect, Online Storage and the Comodo Guarantee. Activation of additional services is carried out after the base installation has been completed.

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. More specifically, remove any other products of the *same type* as those Comodo products you plan to install. For example, if you plan to install only the firewall then you do not need to remove 3rd party antivirus solutions and vice-versa. If you are installing full CIS (both FW and AV) then you need to remove both types of product if they are present on your system. Failure to remove products of the same type could cause conflicts that mean CIS will not function correctly. Users should consult their vendor's documentation for precise uninstallation guidelines, however the following rough steps will help most Windows users:

- Click the Start button to open the Windows Start menu
- Select Control Panel > Programs and Features (Win 10, Win 8, Win 7, Vista); Control Panel > Add or Remove Programs (XP)
- Select your current antivirus or firewall program(s) from the list
- Click Remove/Uninstall button
- Repeat process until all required programs have been removed

Click the links below for detailed explanations:

- **CIS Premium - Installation**
- **CIS Pro - Installation**
- **CIS Complete - Installation**

1.3.1. CIS Premium - Installation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. **Click here** to read the full note.

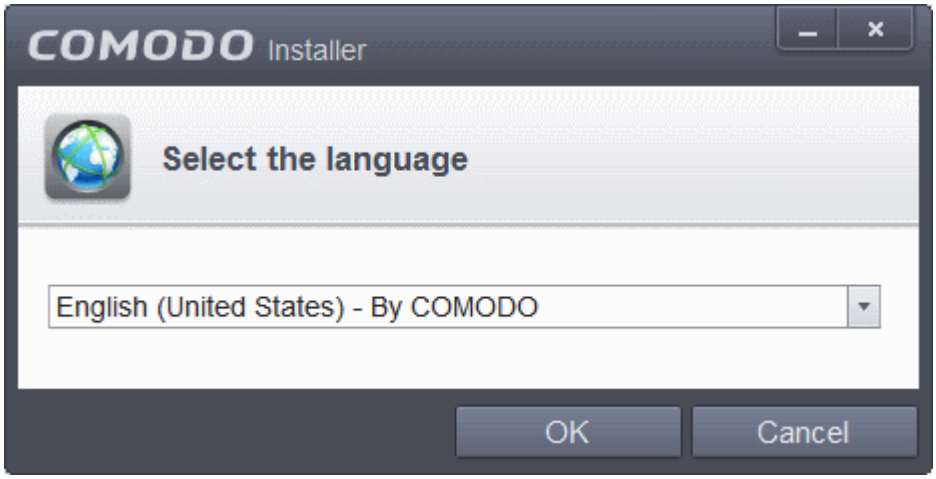
In order to install Comodo Internet Security - Premium, you need to download the setup file from **http://www.comodo.com/home/download/download.php?prod=cis**

- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or 64 bit setup files.

After downloading the required Comodo Internet Security setup file to your local hard drive, double click on it  to start the installation wizard.

Step 1 - Choosing the Interface Language

The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



- Select the language in which you want Comodo Internet Security to be installed from the drop-down menu and click 'OK'.

Step 2 - Installation Configuration

The installation configuration screen will be displayed.

- If you click 'Customize Installation' then you can choose **advanced options**. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

Receive Comodo News and Notifications

Comodo Internet Security Premium is activated free of cost for lifetime usage. If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

Cloud Based Behavior Analysis

Any file that is identified as unrecognized is sent to the 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 contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Send Program Usage Data

Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS instillation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from **Advanced Settings > General Settings > Log Settings** interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.
- Click the 'Next' button.

The next screen allows you to customize the installation of Chromodo, Comodo's secure internet browser:

- **Set Chromodo as the default browser**. If enabled, Chromodo will be automatically used to open web pages whenever you click a website link. De-select to keep your current default browser.
- **Replace existing Google Chrome shortcuts with Chromodo shortcuts at the desktop and Start menu.** If you already have Google Chrome installed, this option will update existing Chrome shortcuts on your desktop or quick launch bar so they use the Chromodo logo and open Chromodo when clicked. This change does not alter shortcuts under the Google folder in the start menu.
- **Import Google Chrome settings** If you already have Chrome installed, this option will import your settings to Chromodo.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.

DNS Settings

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

In this step of installation of Comodo Internet Security, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to **Appendix 2 Comodo Secure DNS Service.**

To enable Comodo Secure DNS, select 'I want to enable added security while in the internet by change my DNS Servers to COMODO SecureDNS Servers'. Click the 'What is this' link to know more about Comodo Secure DNS servers.

Browser Homepage

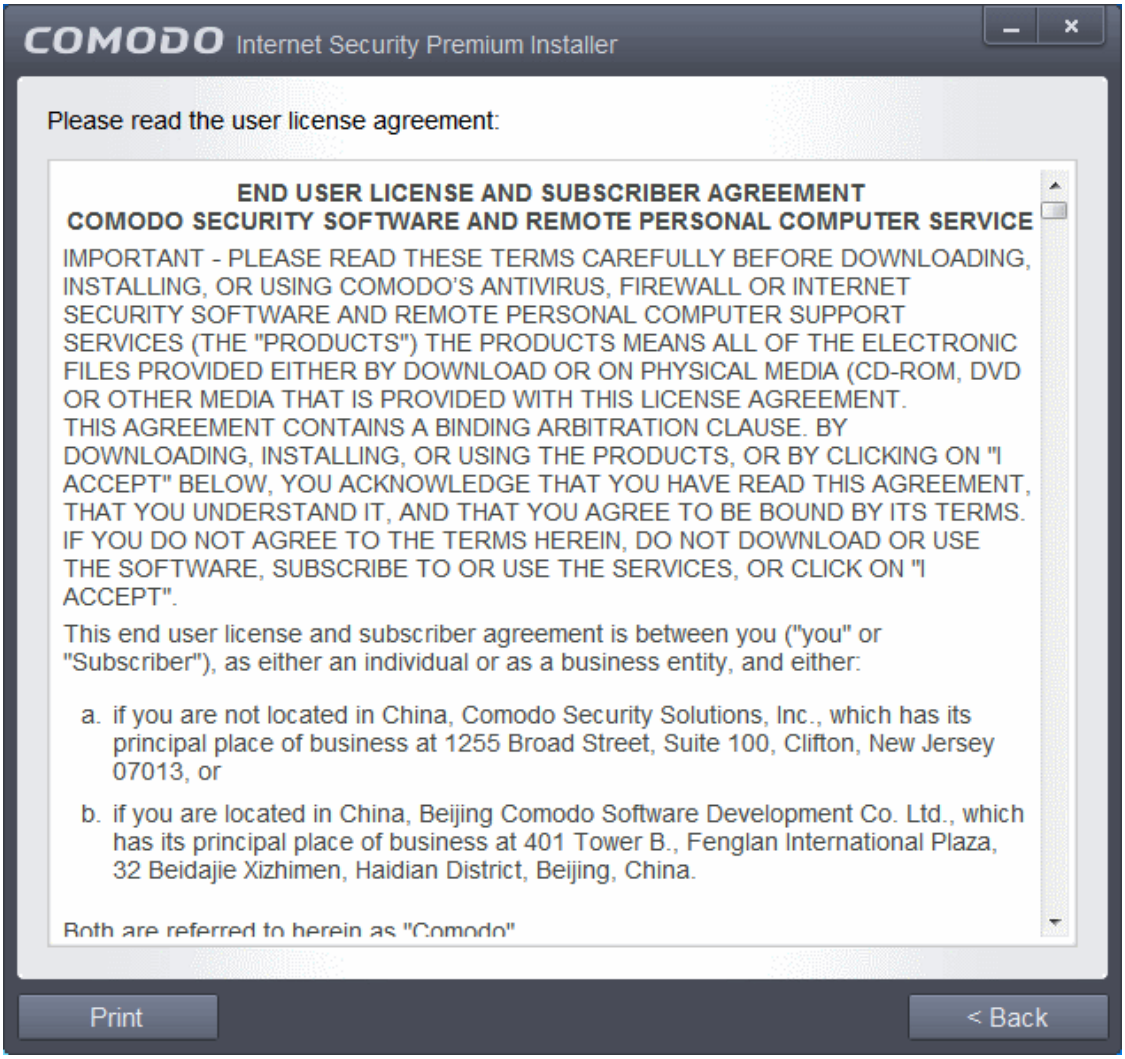
Leaving this setting enabled will:

- Make Yahoo your home page in all supported browsers. Currently supported browsers are Mozilla Firefox, Google Chrome, Internet Explorer, Comodo Dragon, Comodo Ice Dragon, Chromodo and Opera.
- Make Yahoo your default search engine. This means:
  - When you enter a search item into the address bar of a supported browser, the search will be carried out by Yahoo

- A 'Search with Yahoo' menu entry will be added to the right-click menu of supported browsers.
- Yahoo will be set as the default search engine in the 'Search' box of supported browsers
- The instant 'search suggestions' that you see when you start typing a search item will be provided by Yahoo.

End User License Agreement

- Read the complete User License Agreement by clicking the 'License Agreement' link of Comodo Internet Security before proceeding with the installation.



After reading the agreements, click the 'Back' button to return to the installation configuration screen.

Once back at the main installer screen, if you wish to configure advanced options, click '**Customize Installation**'. Otherwise, click 'Agree and Install' to **begin installation**.

Customizing Installation

Clicking the 'Customize Installation' link opens an advanced options interface that enables you to choose which elements you would like to install, configure security popup alerts and choose the installation path. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select all the components to get the full benefit of the product.

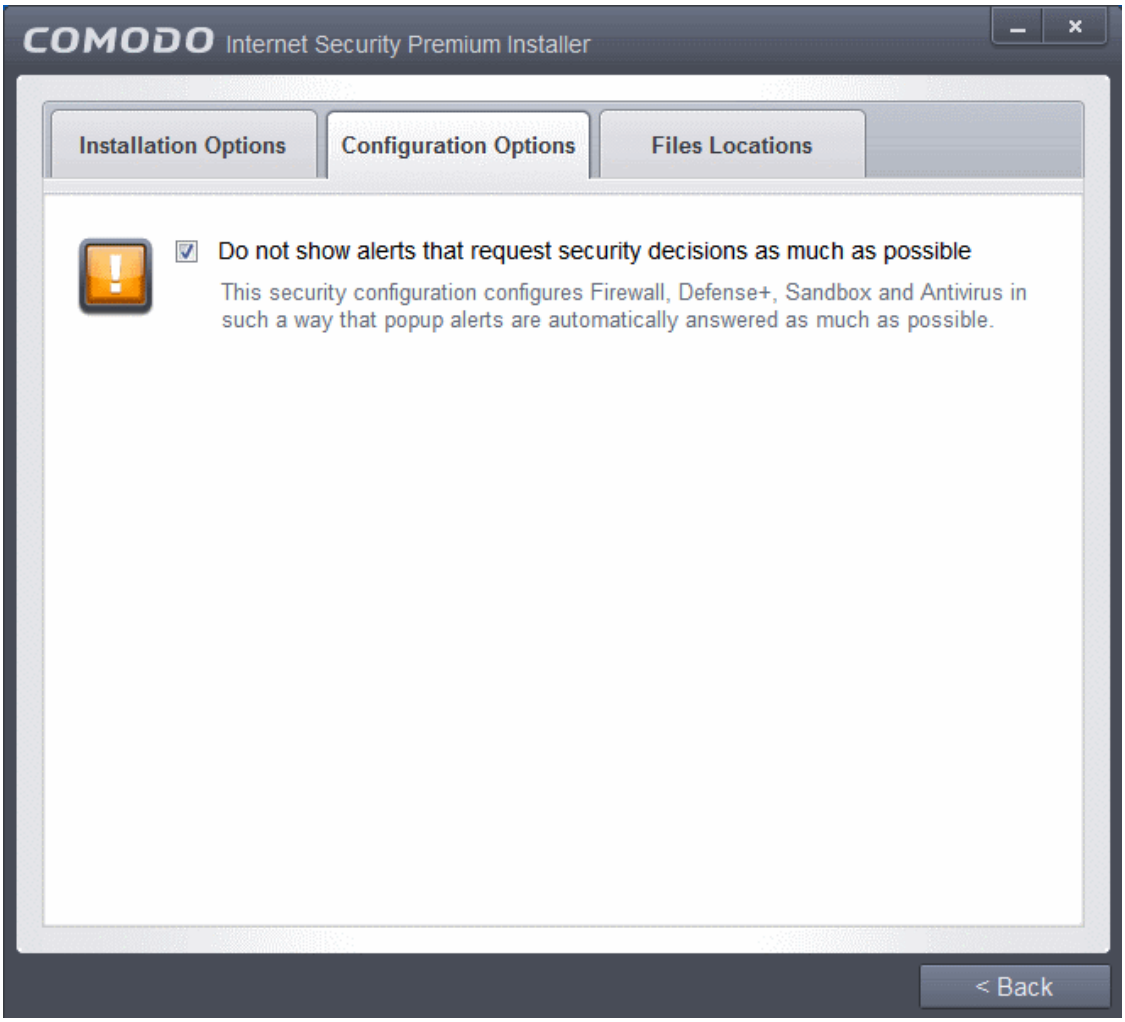
Select Components to Install (Click to go back to Step 2)

Click the 'Installation Options' tab to select the components to be installed.

- **Install COMODO Firewall** - Selecting this option installs Comodo Firewall and Defense+ components. Deselect this option, if you already have third party Firewall protection activated in your computer system. Comodo Firewall installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO Antivirus** - Selecting this option installs Comodo Antivirus and Defense+ components. Deselect this option, if you already have a third party virus protection activated in your computer system. Comodo Antivirus installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24x7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section **Comodo GeekBuddy** for more details.
- **Install Chromodo Browser** - Selecting this option installs Chromodo, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section **Chromodo** for more details.

Configuration Options

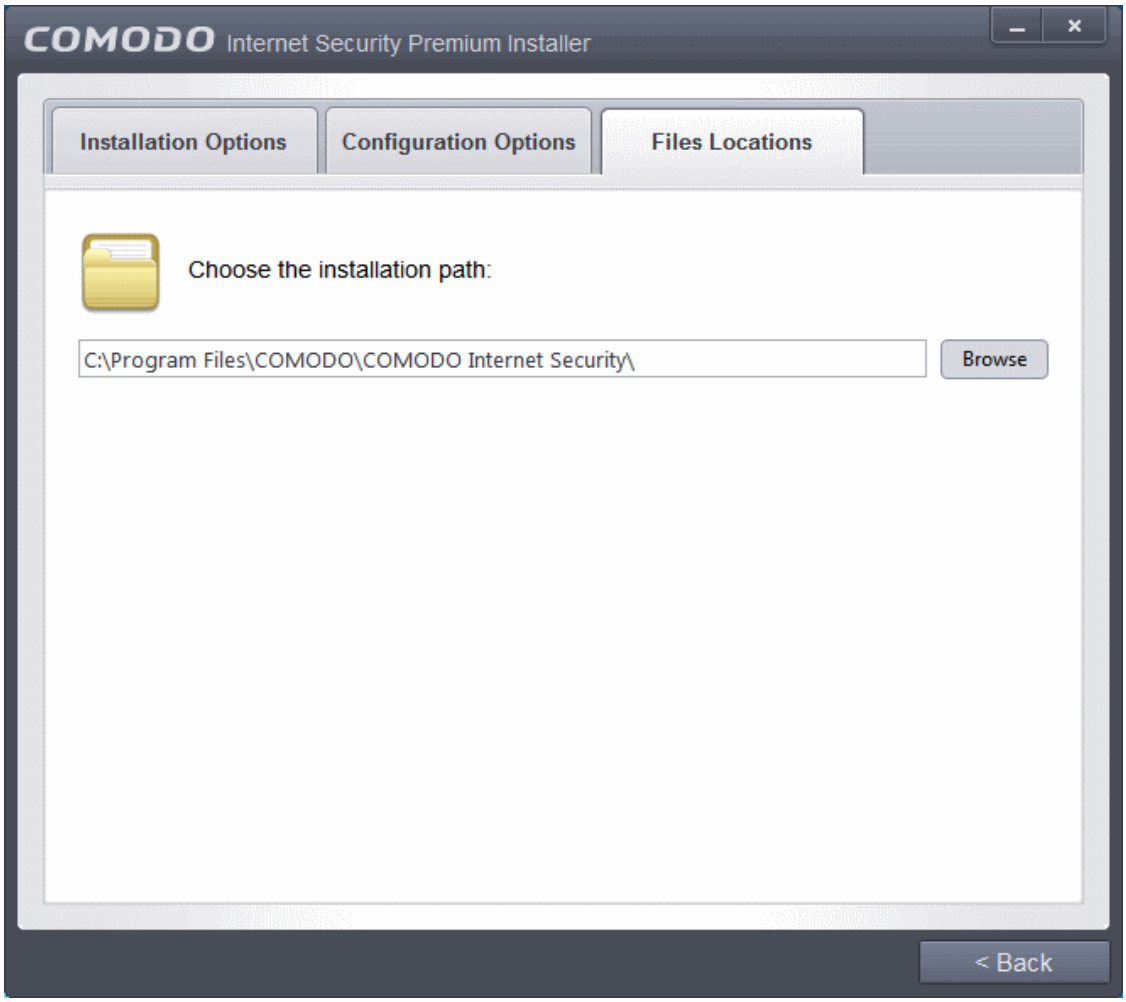
- Click the 'Configuration Options' tab to configure pop-up alert options.



- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

Choosing Installation Location

Click the 'Files Locations' tab to choose the installation path.



This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

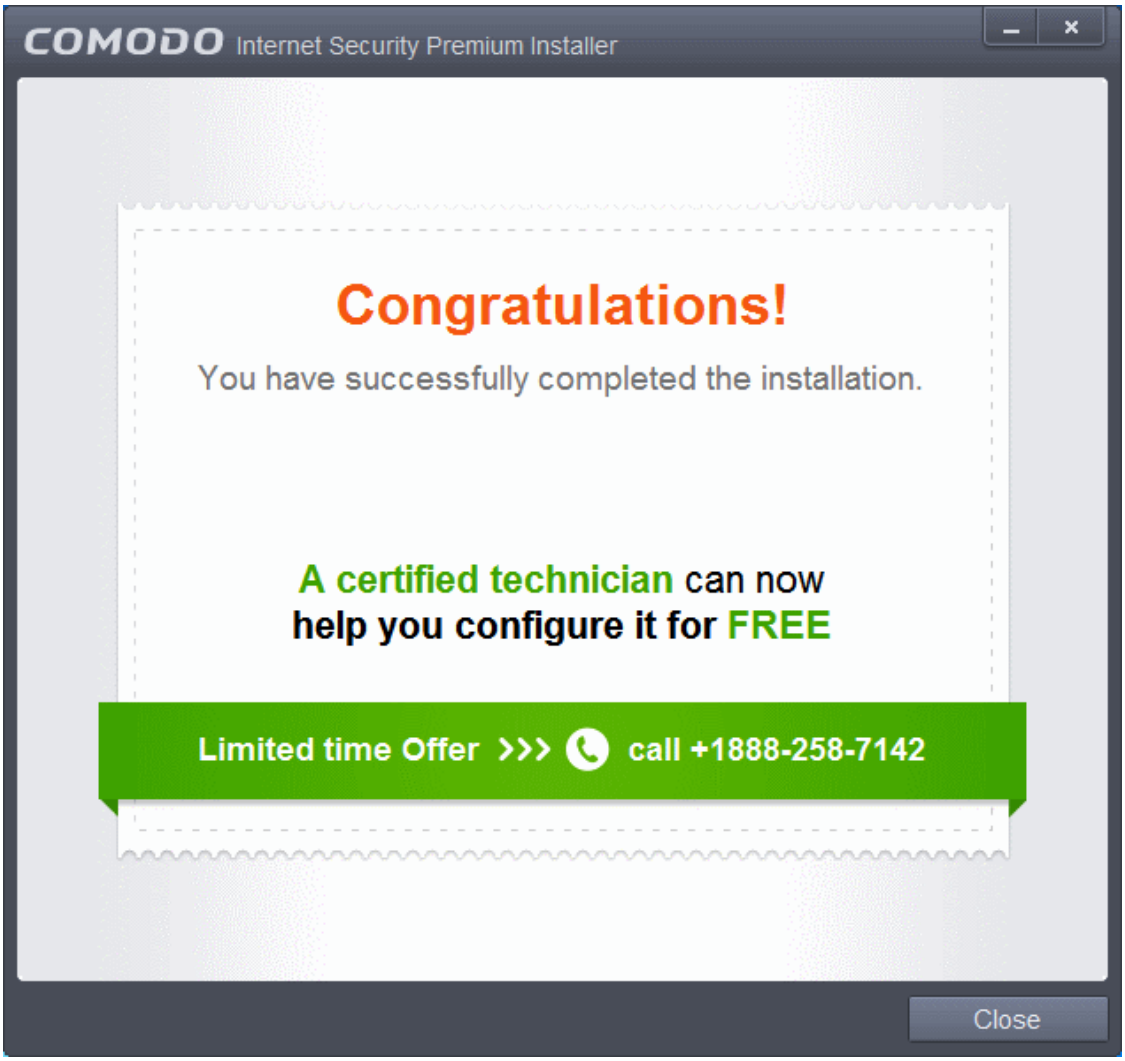
After customizing your installation, click the 'Back' button to return to the installation configuration screen.

- Once you are satisfied with your settings, click 'Agree and Install' to **begin installation** (**Click to go back to Step 2**).

Step 3 - Installation Progress

The installation progress will be displayed...

… and on completion, the successfully completed dialog will be displayed.

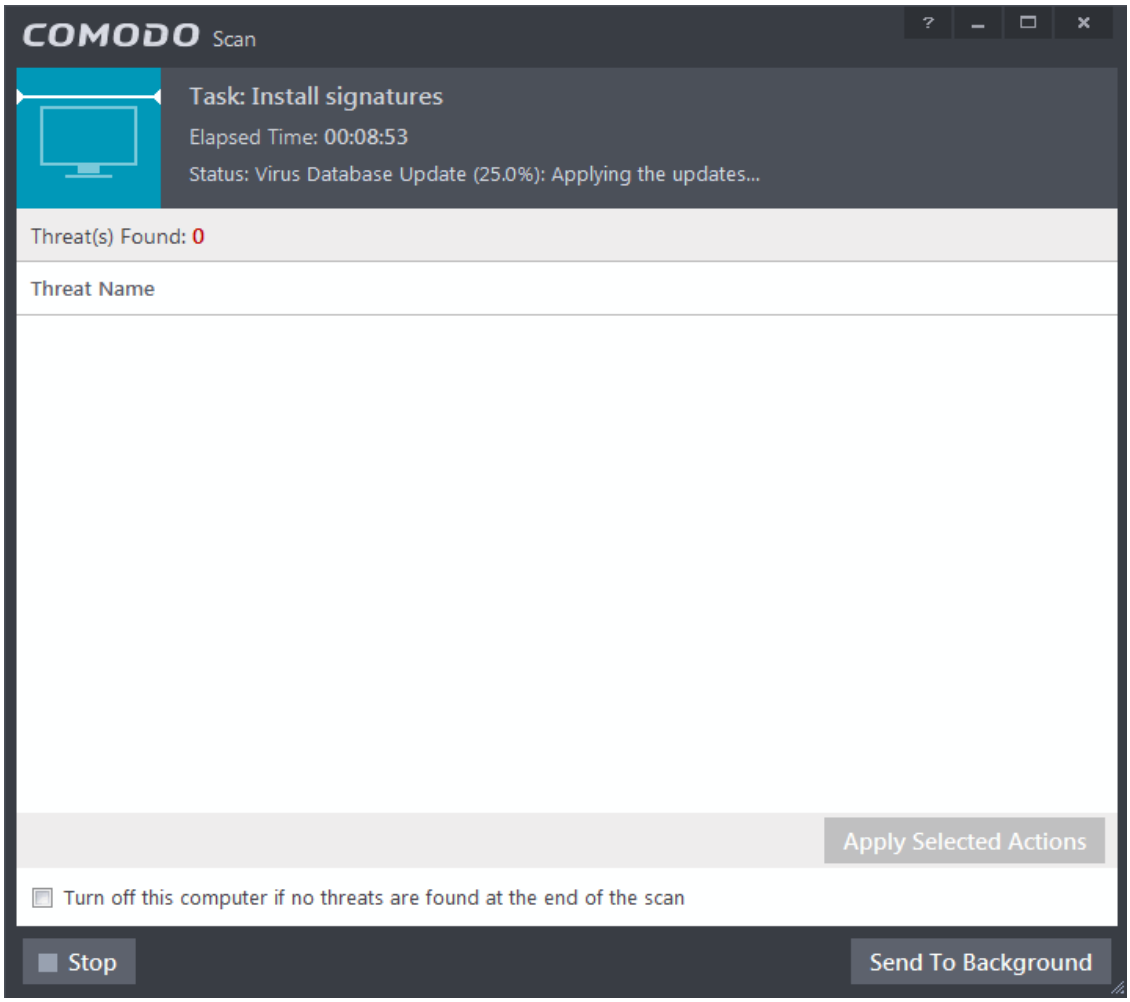


- Click the 'Close' button.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

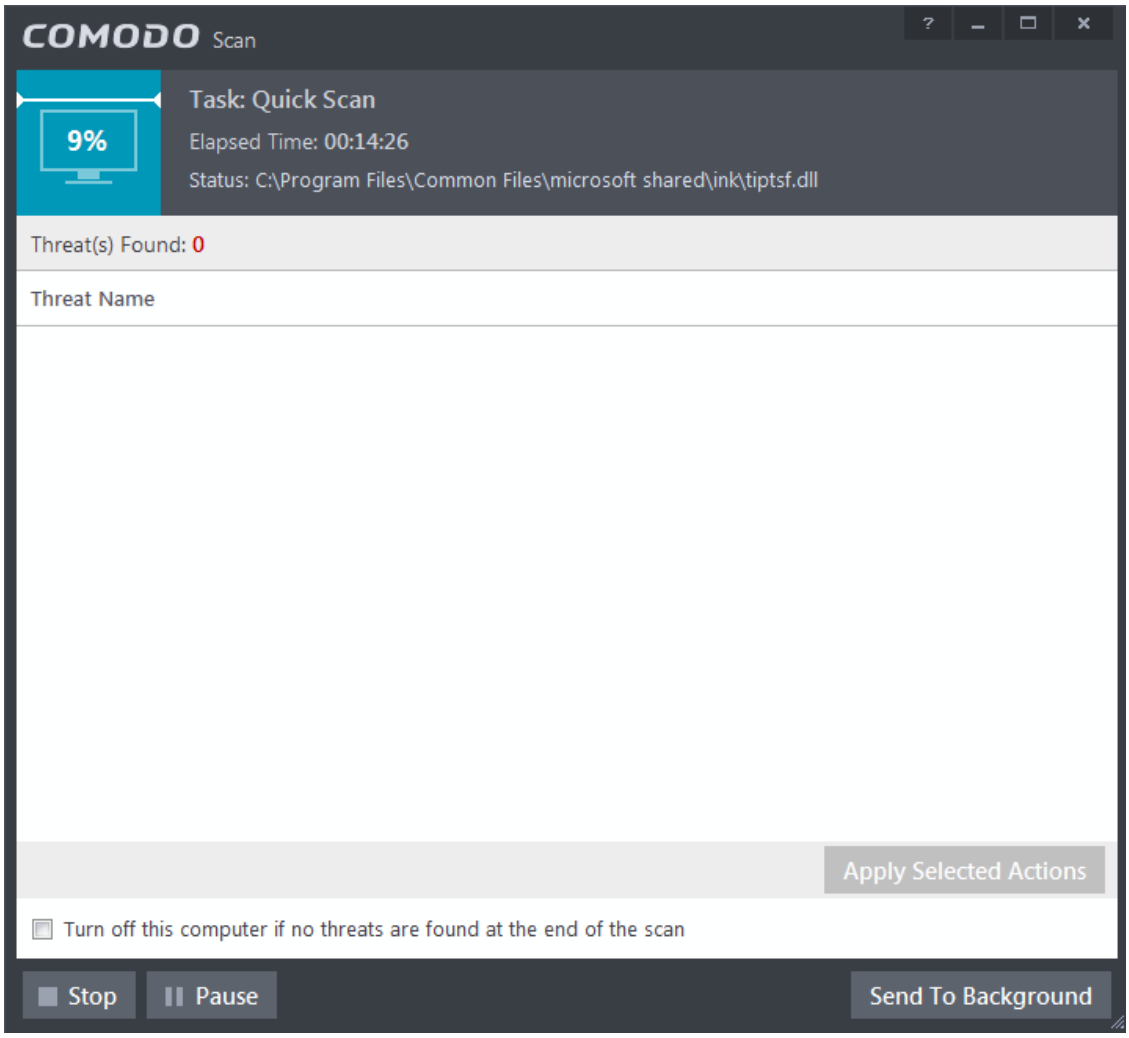
- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '**Network Zones**' and through the '**Stealth Ports Wizard**')

The application initiates the first quick scan on your computer. The virus database will be updated automatically prior to the scan.



You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '**Manage CIS Tasks**' for more details.

CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



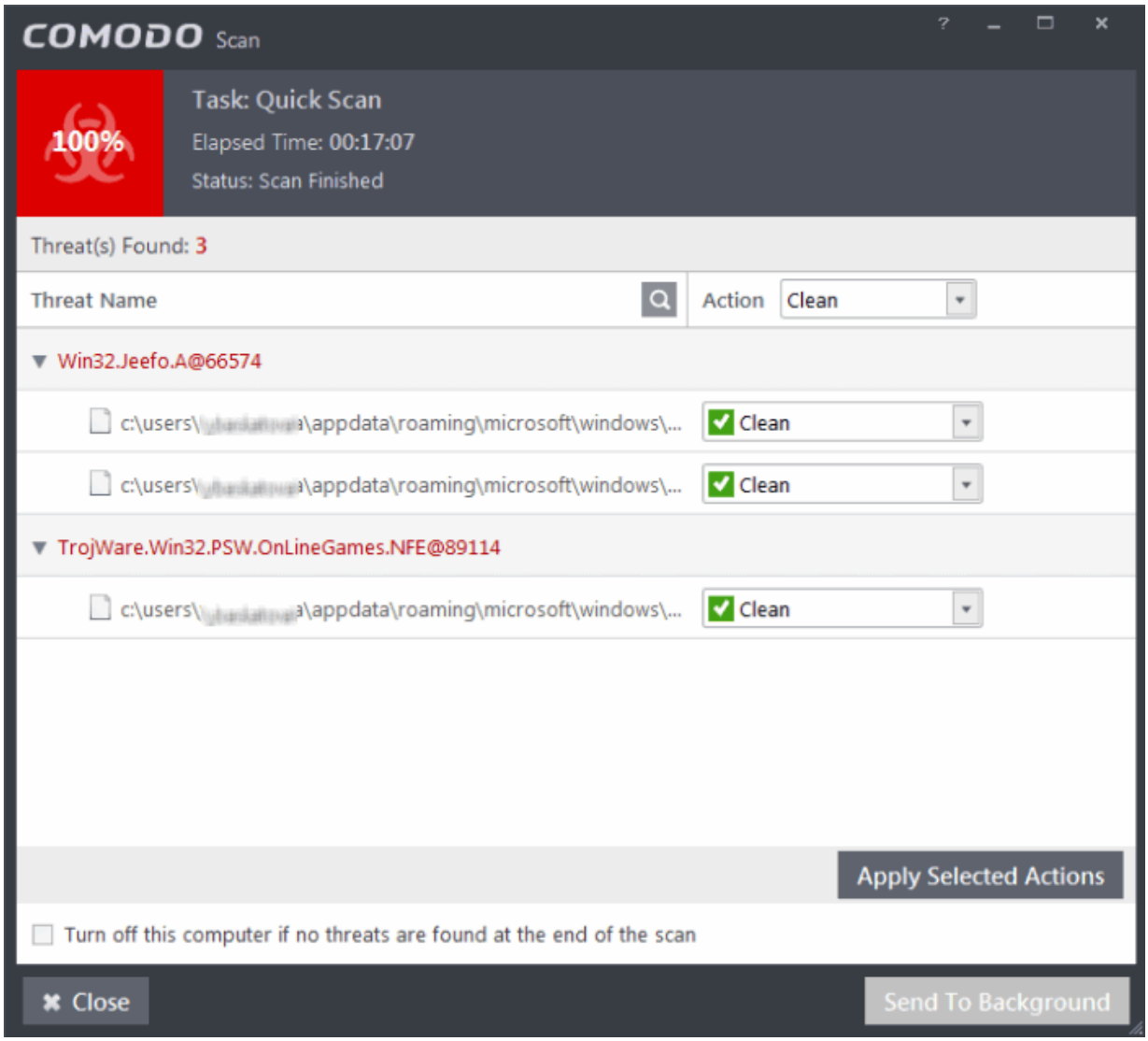
If you do not want the scan to continue at this time, click the 'Stop' button.

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

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

  For more details on GeekBuddy, refer to the section **Comodo GeekBuddy**.

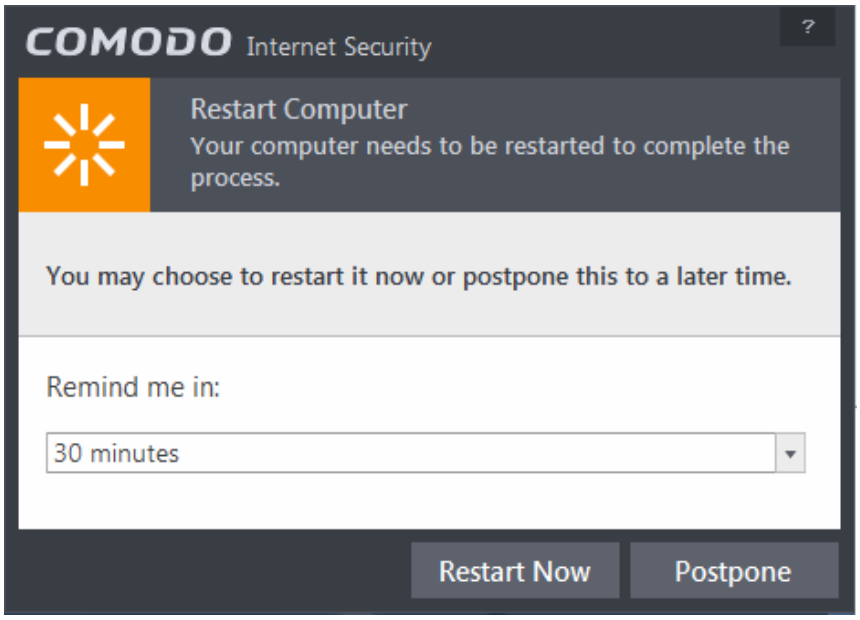
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section '**Processing Infected Files**' for more details.

Step 4 - Restarting Your System

In order for the installation to take effect, your computer needs to be restarted.



- If your want to restart the computer immediately, save all your work and click 'Restart Now'.
- If you want to restart the computer at a later time, select when you need to be reminded from the drop-down and click 'Postpone'.

Step 5 - After Restarting Your System

After restarting, a 'Welcome' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice.

This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in **Network Zones** interface and through the **Stealth your Computer Ports**')

The main interface will be displayed:

1.3.2. CIS Pro - Installation and Activation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. **Click here** to read the full note.

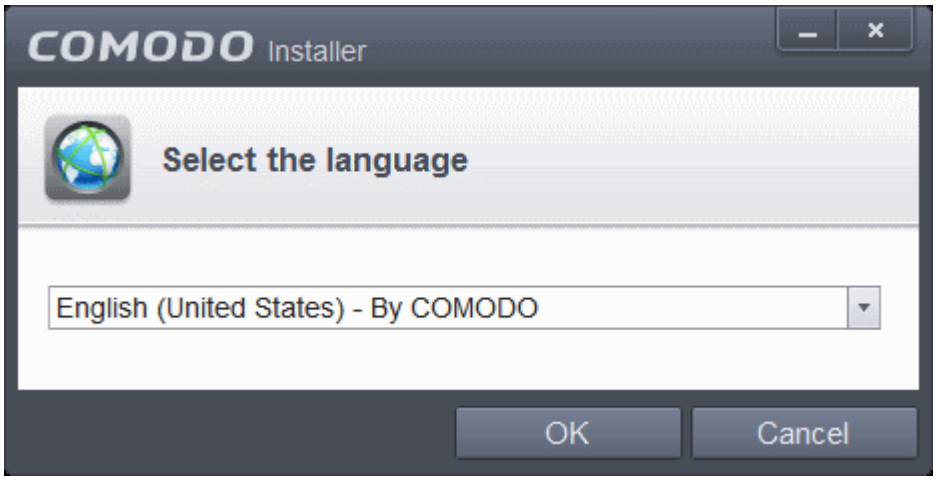
Comodo Internet Security Pro can be downloaded from **http://www.comodo.com/home/download/download.php?prod=cis-pro** after signing up for subscription and includes, **Chromodo Browser**, **GeekBuddy** and the **Comodo Guarantee**.

- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or 64 bit setup files.

After downloading the required Comodo Internet Security setup file to your local hard drive, double click on the setup file to start the installation wizard.

Step 1 - Choosing the Interface Language

The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



- Select the language in which you want Comodo Internet Security to be installed from the drop-down menu and click 'OK'.

Step 2 - Installation Configuration

The installation configuration screen will be displayed.

- If you click 'Customize Installation' then you can choose **advanced options**. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

  Receive Comodo News and Notifications

  If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

  Cloud Based Behavior Analysis

  Any file that is identified as unrecognized is sent to the 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 contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

  Send Program Usage Data

  Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS instillation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from **Advanced Settings > General Settings > Log Settings** interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.

- Click the 'Next' button.

The next screen allows you to customize the installation of Chromodo, Comodo's secure internet browser:

- **Set Chromodo as the default browser**. If enabled, Chromodo will be automatically used to open web pages whenever you click a website link. De-select to keep your current default browser.
- **Replace existing Google Chrome shortcuts with Chromodo shortcuts at the desktop and Start menu.** If you already have Google Chrome installed, this option will update existing Chrome shortcuts on your desktop or quick launch bar so they use the Chromodo logo and open Chromodo when clicked. This change does not alter shortcuts under the Google folder in the start menu.
- **Import Google Chrome settings** If you already have Chrome installed, this option will import your settings to Chromodo.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.

- If you click 'Customize Installation' then you can choose **advanced options**. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

DNS Settings

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

In this step of installation of Comodo Internet Security, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to **Appendix 2 Comodo Secure DNS Service.**

To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

Browser Homepage

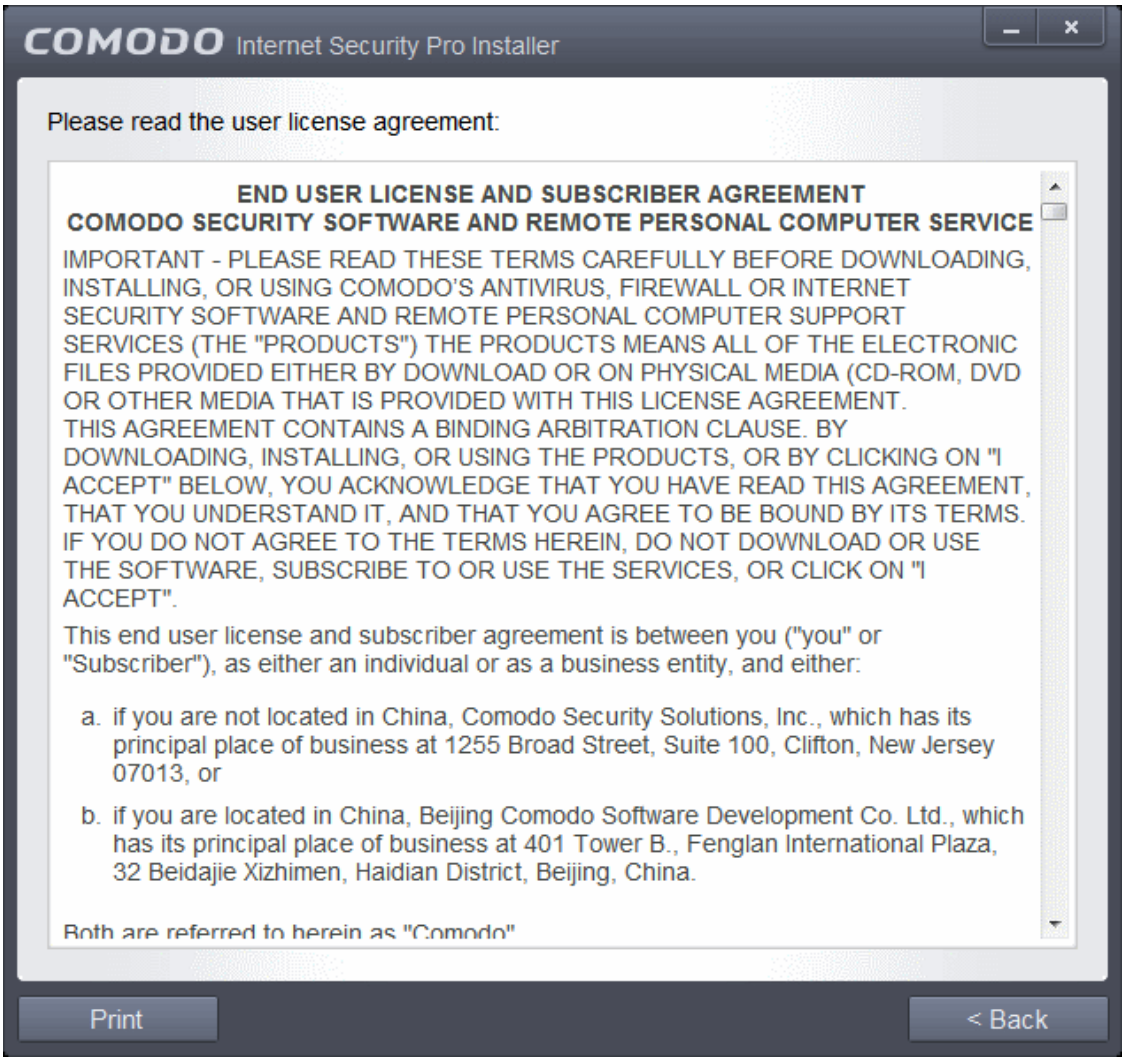
Leaving this setting enabled will:

- Make Yahoo your home page in all supported browsers. Currently supported browsers are Mozilla Firefox, Google Chrome, Internet Explorer, Comodo Dragon, Comodo Ice Dragon, Chromodo and Opera.
- Make Yahoo your default search engine. This means:

- When you enter a search item into the address bar of a supported browser, the search will be carried out by Yahoo
- A 'Search with Yahoo' menu entry will be added to the right-click menu of supported browsers.
- Yahoo will be set as the default search engine in the 'Search' box of supported browsers
- The instant 'search suggestions' that you see when you start typing a search item will be provided by Yahoo

End User License Agreement

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security before proceeding with the installation.



After reading the agreement, click the 'Back' button to return to the installation configuration screen.

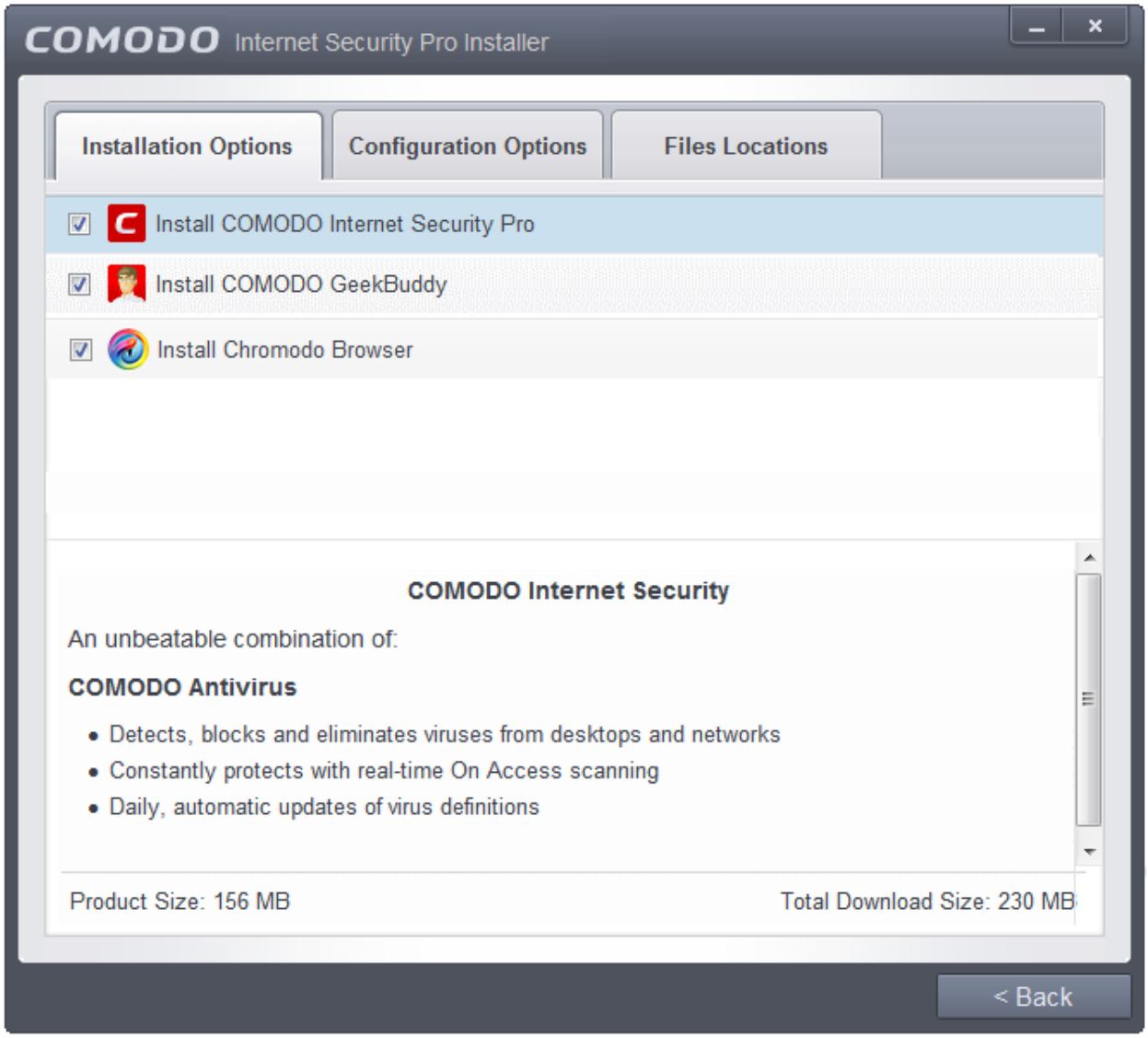
Once back at the main installer screen, if you wish to configure advanced options, click '**Customize Installer**'. Otherwise, click 'Agree and Install' to **begin installation**.

Customizing Installation

Clicking the 'Customize Installer' link opens an advanced options interface that enables you to choose which elements you would like to install, configure security popup alerts and choose the installation path. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select all the components to get the maximum benefit from Comodo Internet Security Pro 2013.

Select the Components to Install (Click to go back to Step 2)

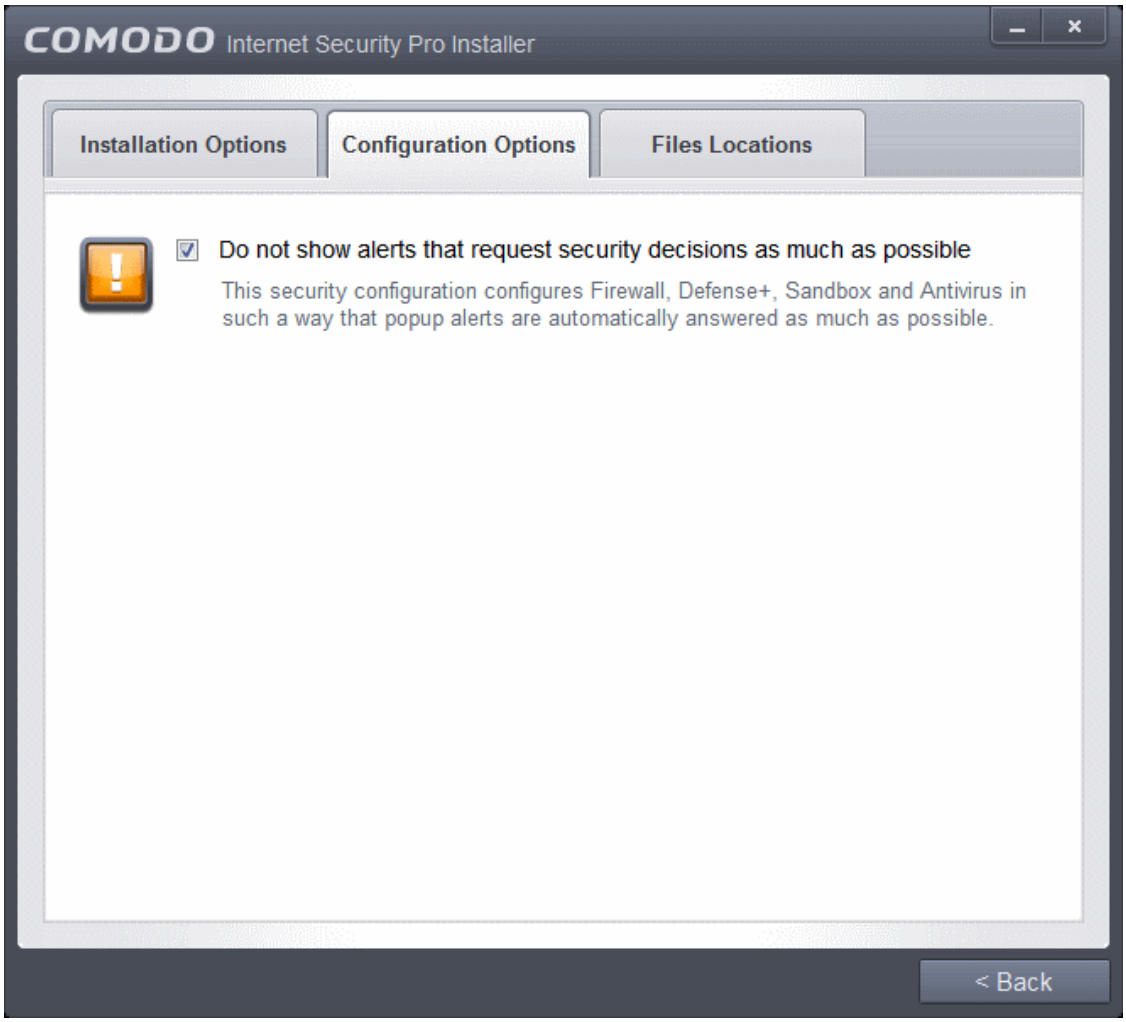
- Click the 'Installation Options' tab to select the components to be installed.



- **Install COMODO Internet Security Pro** - Selecting this option installs Comodo Antivirus, Comodo Firewall, Defense+ components. Installing CIS Pro is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section **Comodo GeekBuddy** for more details.
- **Install Chromodo Browser** - Selecting this option installs Chromodo, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section **Chromodo Browser** for more details.

Configuration Options

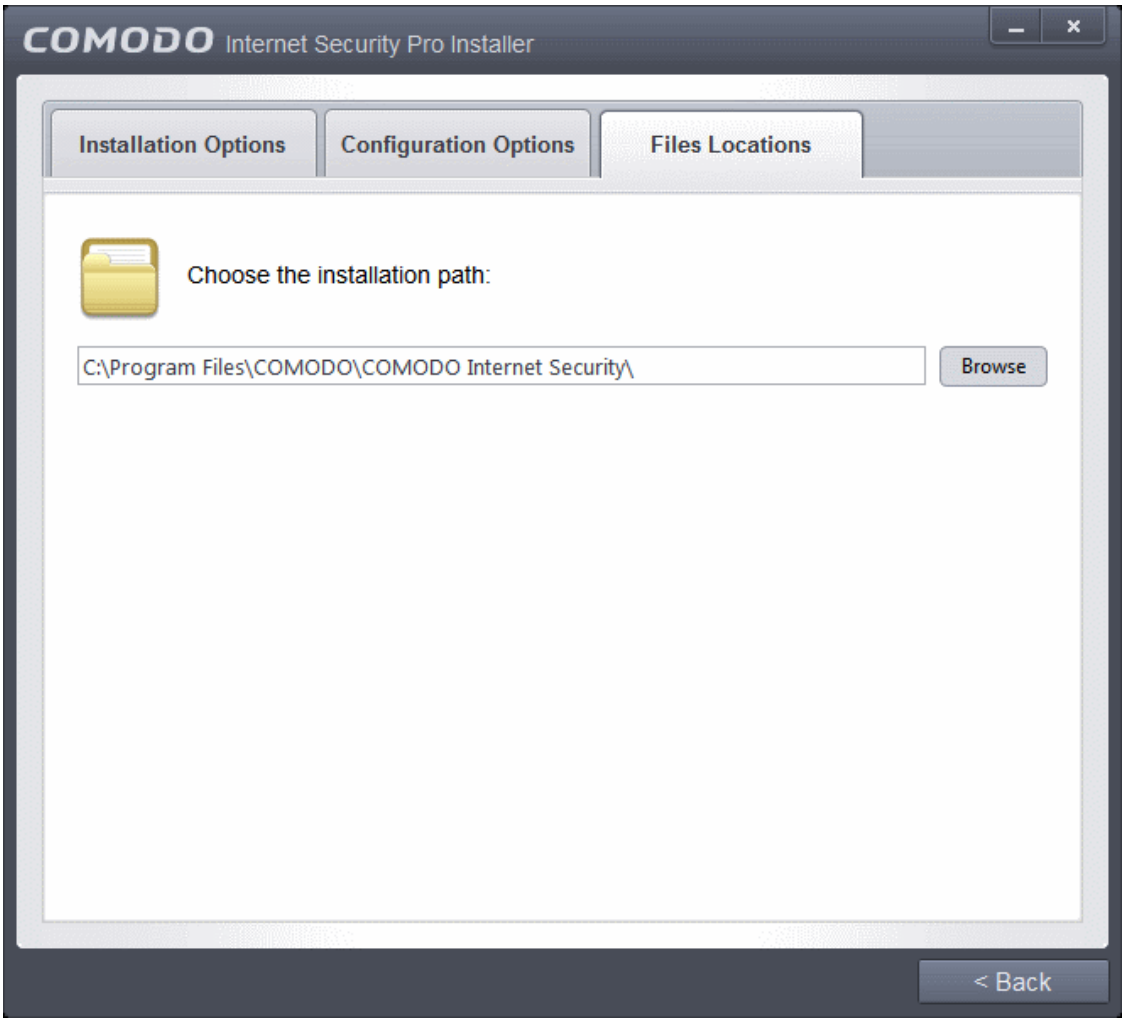
- Click the 'Configuration Options' tab to configure pop-up alert options.



- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

Choose the Installation Location

- Click the 'Files Locations' tab to choose the installation path.



This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

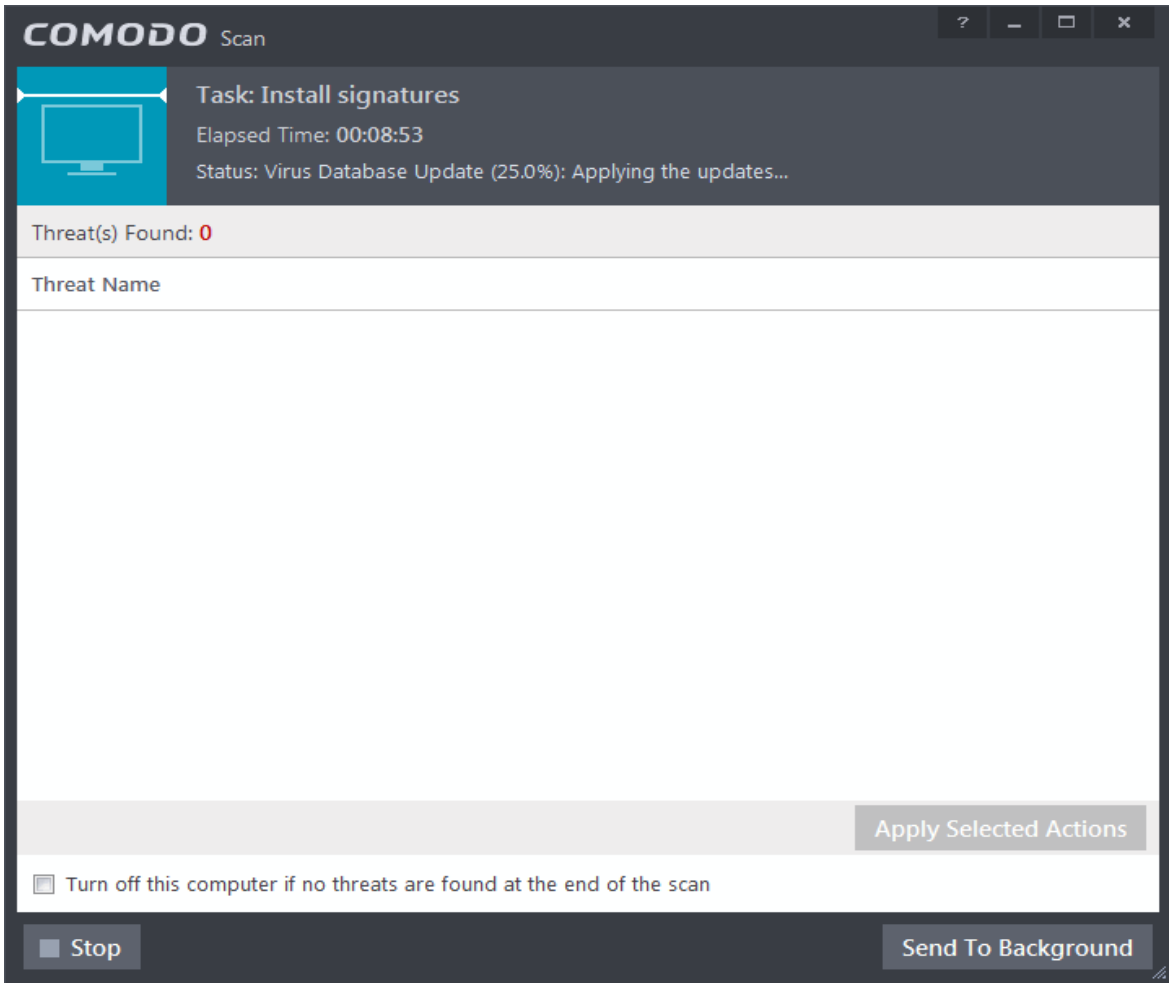
After customizing your installation, click the 'Back' button to return to the installation configuration screen.

Click the 'Agree and Install' button to proceed with the installation.

Step 3 - Installation Progress (**Click to go back to Step 2**)

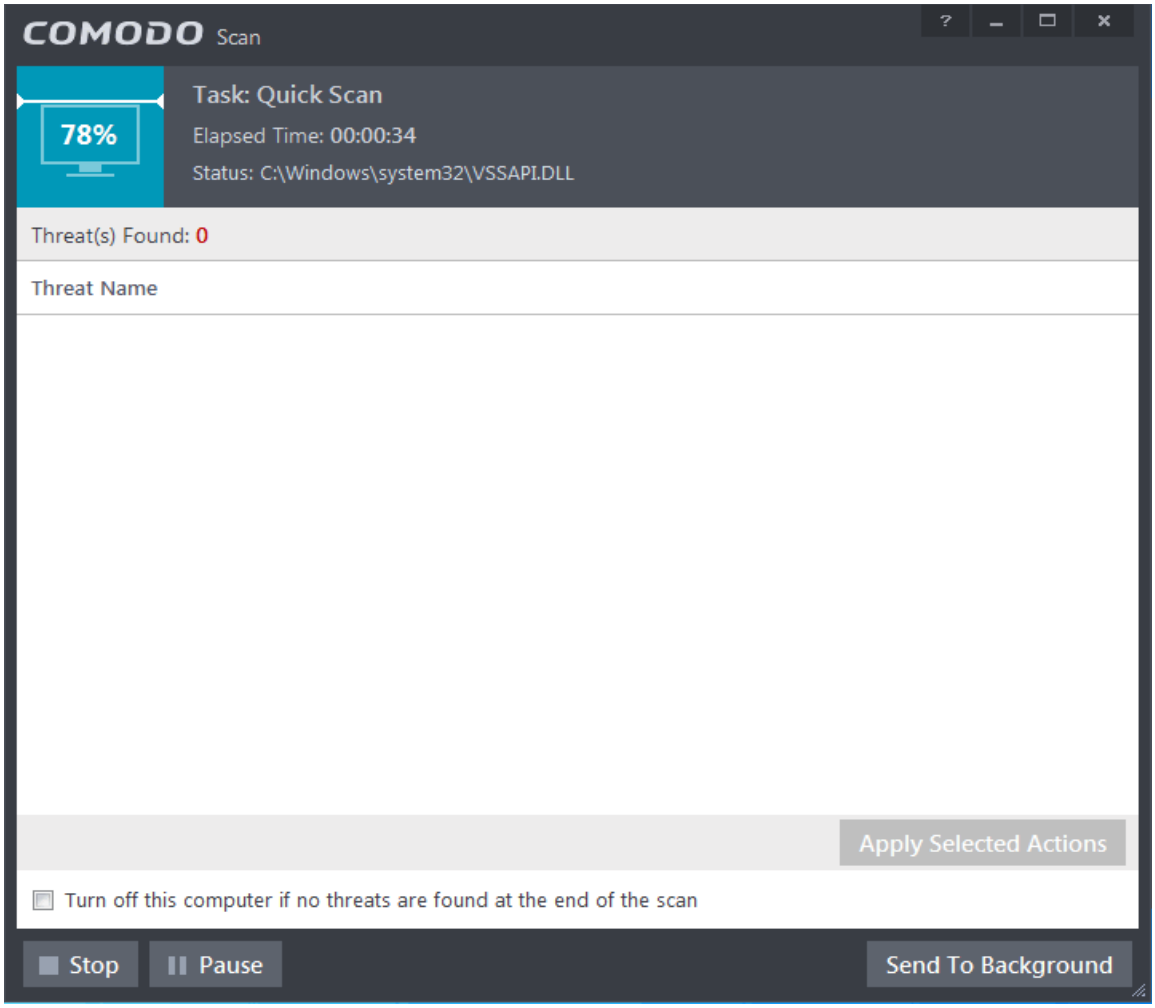
The installation progress will be displayed...

...and on completion, the application initiates the first quick scan on your computer. The virus database will be updated automatically prior to the scan.



You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '**Manage CIS Tasks**' for more details.

CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.

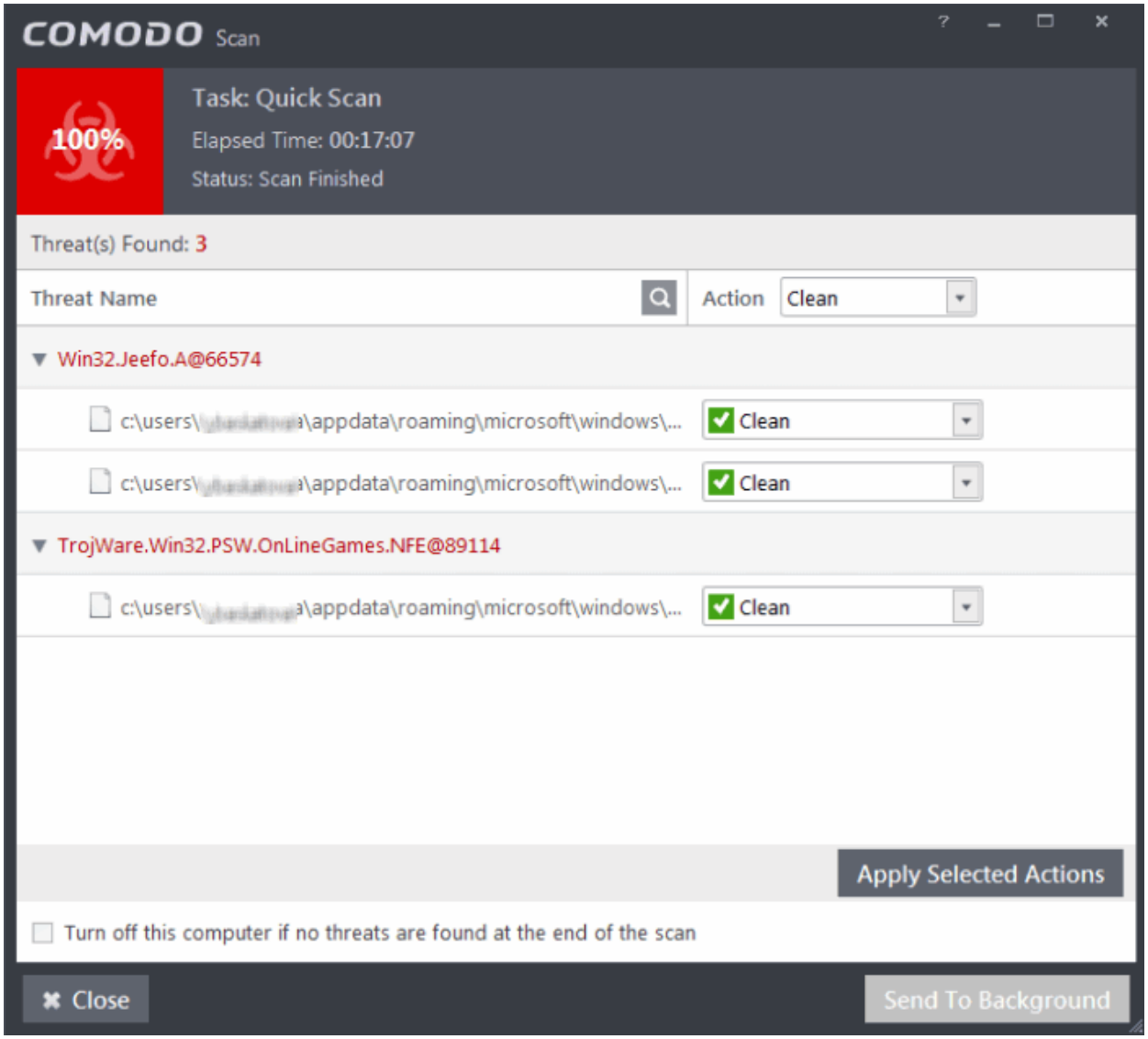


If you do not want the scan to continue at this time, click the 'Stop' button.

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

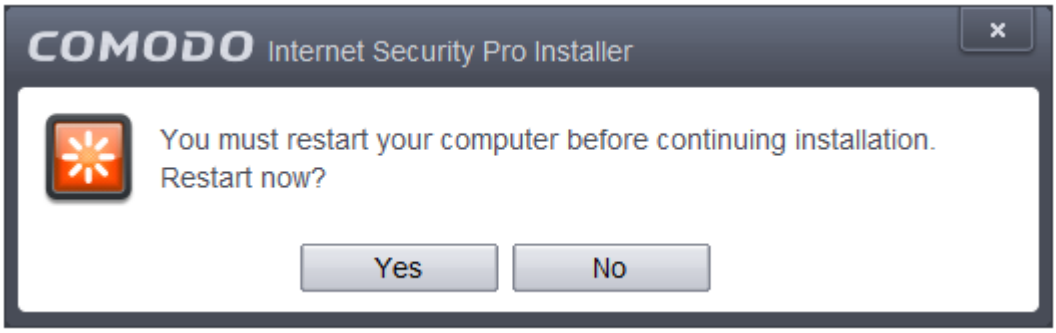
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up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

  For more details on GeekBuddy, refer to the section **Comodo GeekBuddy**.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. Refer to the section Processing Infected Files for more details.
- An example results screen is shown below:



Step 4 - Restarting Your System

In order for the installation to take effect, your computer needs to be restarted.



- To restart the computer click 'Yes'.

Note: The installation will take effect only on the next restart of the computer.

Step 5 - After Restarting Your System

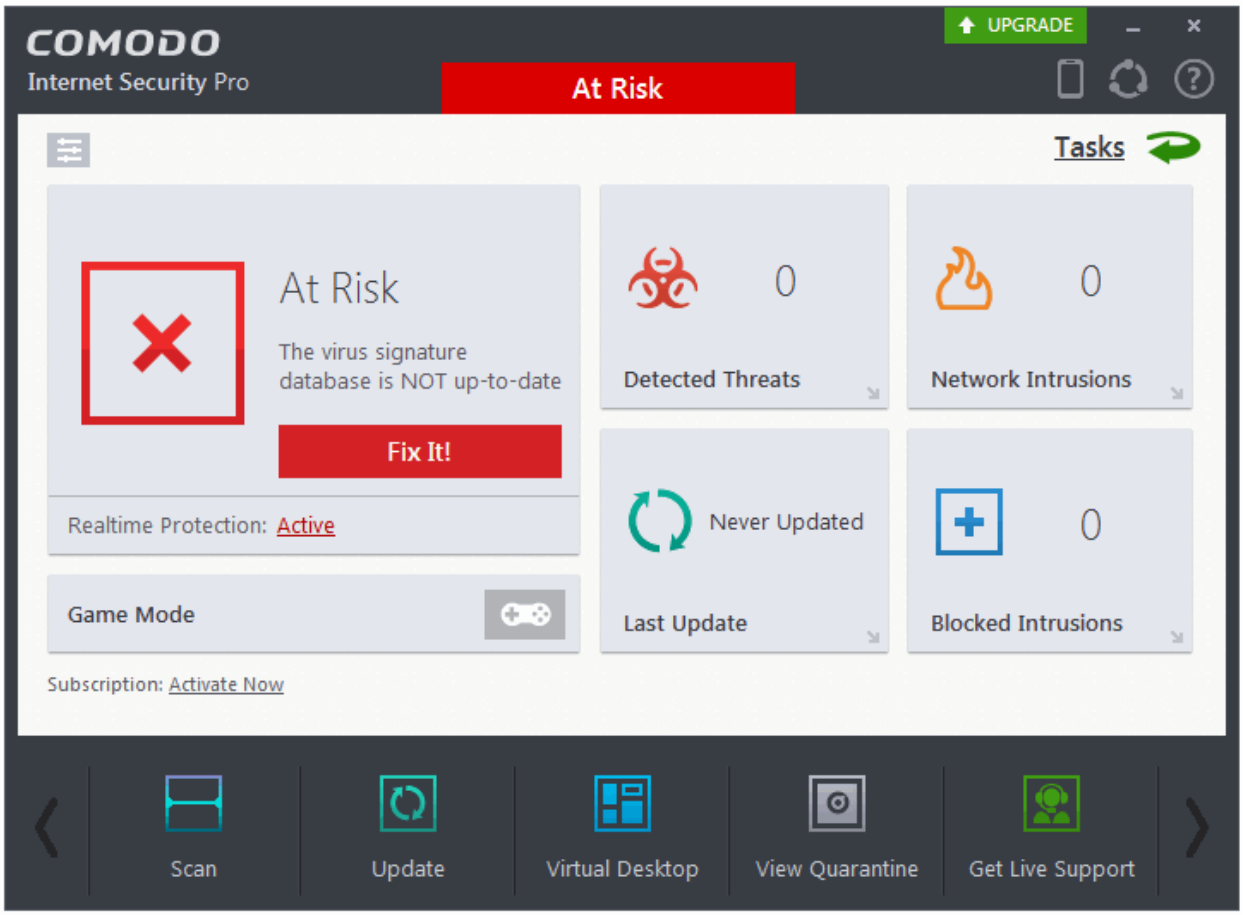
After restarting, a 'Welcome' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice. You can also purchase license key from this screen if you have not done so already.

This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

- Select your location from the three options above
- Select 'Do not automatically detect new networks' 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 main interface will be displayed:



Important Note: After successful installation, you need to activate the license for using the product. In order to get your guarantee coverage, you need to activate the license first.

- For full explanation on activation of license after installation of the product, refer to **Activating Your License.**
- For full explanation on activation of your guarantee, refer to **Activating Your Guarantee Coverage.**

1.3.3. CIS Complete - Installation and Activation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. **Click here** to read the full note.

Comodo Internet Security Complete can be downloaded from **www.comodo.com/home/internet-security/internet-security-complete.php** after signing up for subscription and includes **Chromodo Browser**, **GeekBuddy**, **Comodo Backup**, **TrustConnect** and the **Comodo Guarantee**.

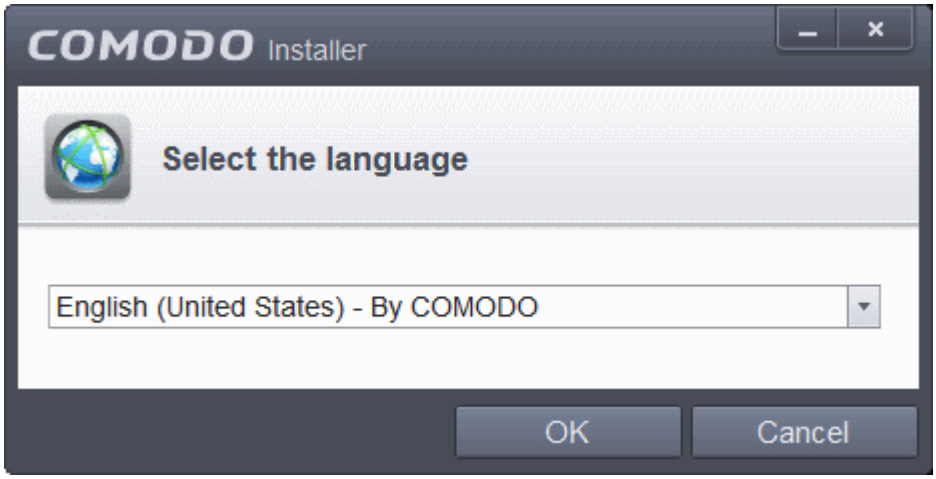
- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or

64 bit setup files.

After downloading the required Comodo Internet Security setup file to your local hard drive, double click on the setup file to start the installation wizard.

Step 1 - Choosing the Interface Language

The language selection dialog will be displayed.



Comodo Internet Security is available in several languages.

- Select the language in which you wish the wizard should continue and Comodo Internet Security Complete is to be installed, from the drop-down menu and click 'OK'.

Step 2 - Installation Configuration

The installation configuration screen will be displayed.

- If you click 'Customize Installation' then you can choose **advanced** options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

  Receive Comodo News and Notifications

  If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

  Cloud Based Behavior Analysis

  Any file that is identified as unrecognized is sent to the 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 contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

  Send Program Usage Data

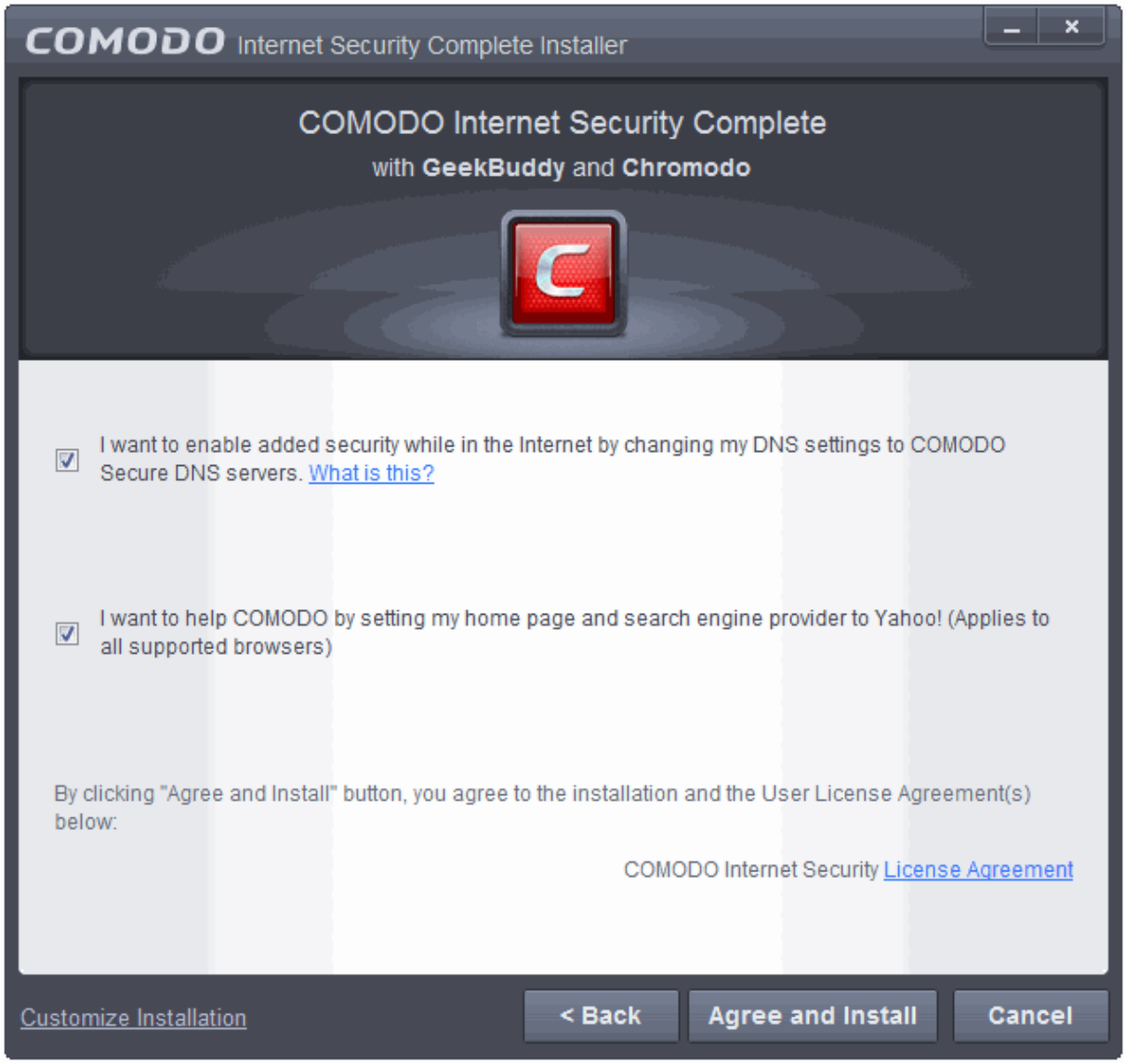
  Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS instillation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from **Advanced Settings > General Settings > Log Settings** interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.
- Click the 'Next' button.

The next screen allows you to customize the installation of Chromodo, Comodo's secure internet browser:

- **Set Chromodo as the default browser**. If enabled, Chromodo will be automatically used to open web pages whenever you click a website link. De-select to keep your current default browser.
- **Replace existing Google Chrome shortcuts with Chromodo shortcuts at the desktop and Start menu.** If you already have Google Chrome installed, this option will update existing Chrome shortcuts on your desktop or quick launch bar so they use the Chromodo logo and open Chromodo when clicked. This change does not alter shortcuts under the Google folder in the start menu.
- **Import Google Chrome settings** If you already have Chrome installed, this option will import your settings to Chromodo.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.



- If you click 'Customize Installation' then you can choose **advanced** options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

  DNS Settings

  Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

  In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

  For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to **Appendix 2 Comodo Secure DNS Service.**

  In this step of installation of CIS Complete, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

  To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

  Browser Homepage

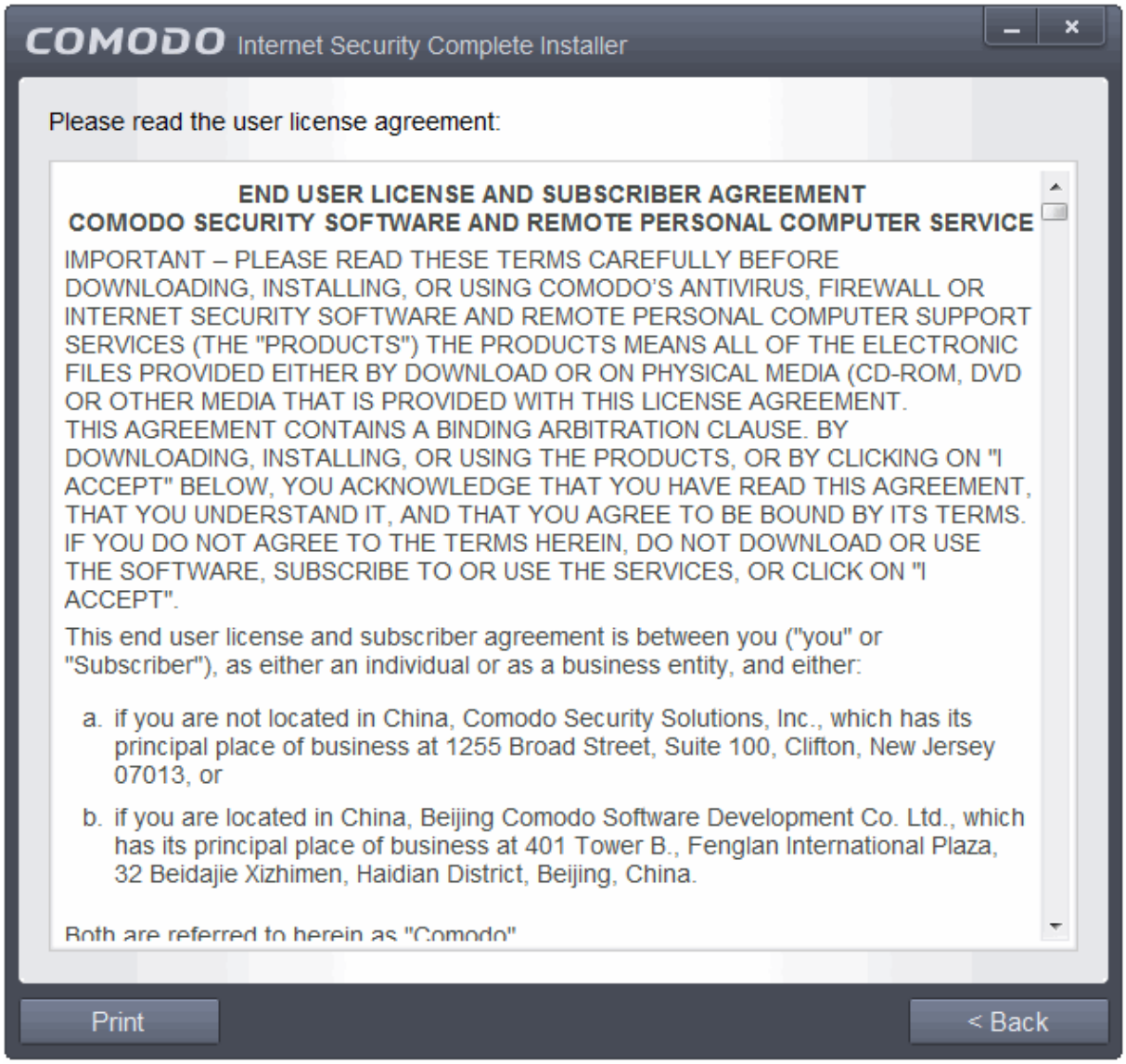
  Leaving this setting enabled will:

- Make Yahoo your home page in all supported browsers. Currently supported browsers are Mozilla Firefox, Google Chrome, Internet Explorer, Comodo Dragon, Comodo Ice Dragon, Chromodo and Opera.
- Make Yahoo your default search engine. This means:

- When you enter a search item into the address bar of a supported browser, the search will be carried out by Yahoo
- A 'Search with Yahoo' menu entry will be added to the right-click menu of supported browsers.
- Yahoo will be set as the default search engine in the 'Search' box of supported browsers
- The instant 'search suggestions' that you see when you start typing a search item will be provided by Yahoo.

End User License Agreements

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security.



After reading the agreement, click the 'Back' button to return to the installation configuration screen.

Once back at the main installer screen, if you wish to configure advanced options, click '**Customize Installation**'. Otherwise, click 'Agree and Install' to **begin installation**.

Customizing Installation

Click the 'Customize Installation' link to select the components to be installed, enable security popup alerts to be minimized and choose installation path.

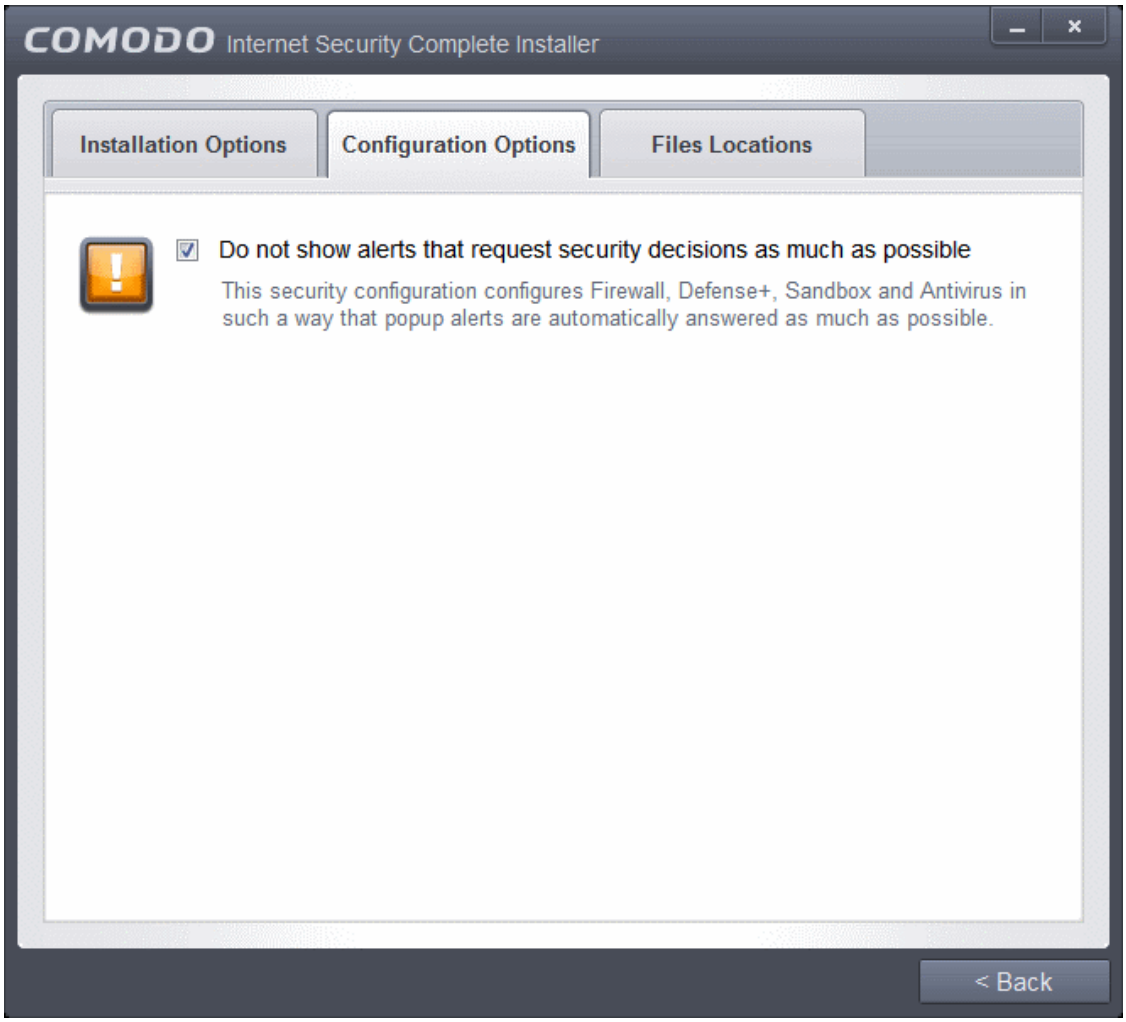
Selecting Components to Install (Click to go back to Step 2)

- Click the 'Installation Options' tab to select the components to be installed.

- **Install COMODO Internet Security Complete** - Selecting this option installs Comodo Antivirus, Comodo Firewall, Defense+ components. Installing CIS Complete is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section **Comodo GeekBuddy** for more details.
- **Install Chromodo Browser** - Selecting this option installs Chromodo, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section **Chromodo Browser** for more details.
- **Install COMODO Backup** - Selecting this option installs Comodo Backup, a powerful and easy-to-use desktop application that helps home and business users protect their valuable data against damage or loss. Refer to the section **Comodo Backup** for more details.

Configuration Options

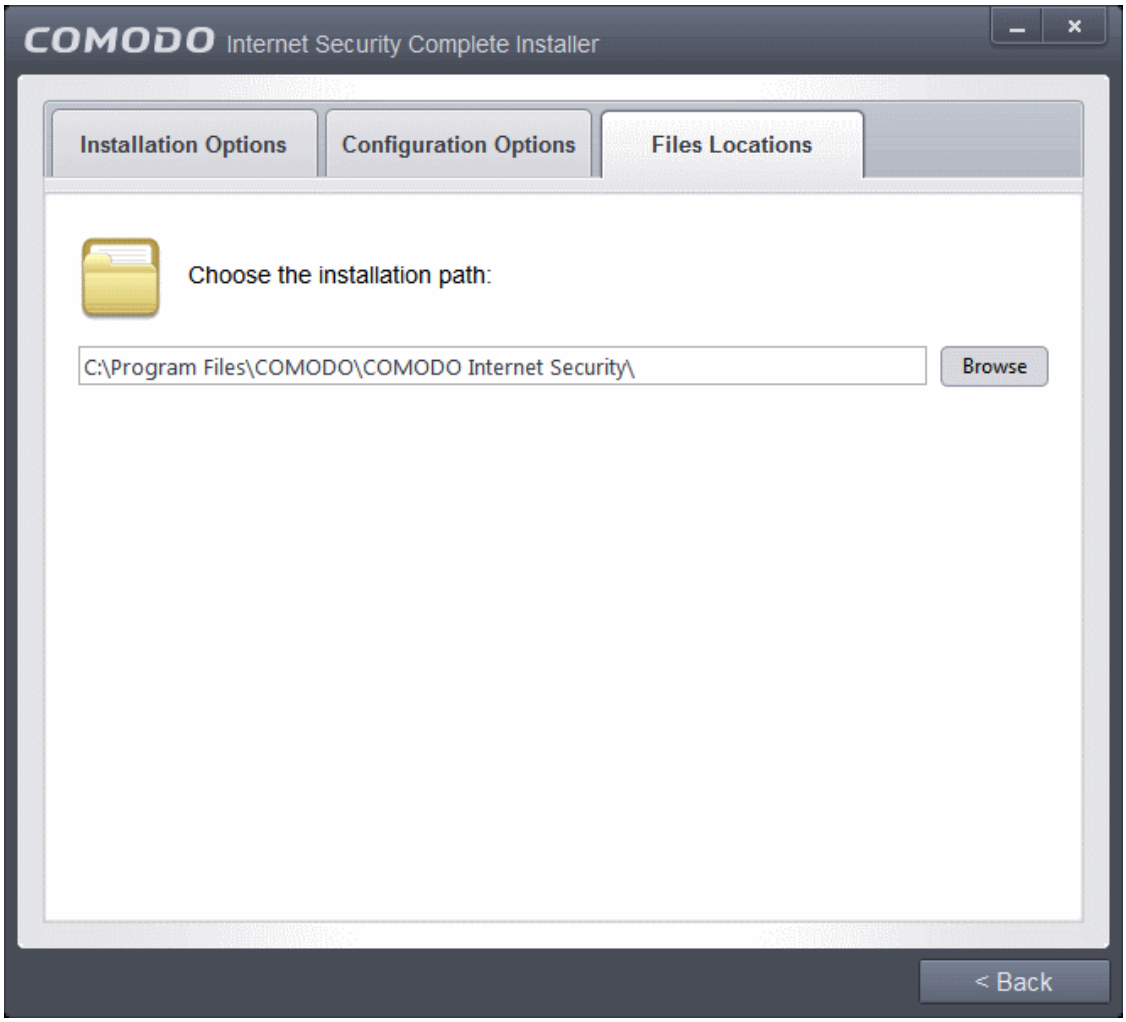
- Click the 'Configuration Options' tab to configure pop-up alert options.



- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

Choosing Installation Location

- Click the 'Files Locations' tab to choose the installation path.



This interface allows you to set the installation folder for Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

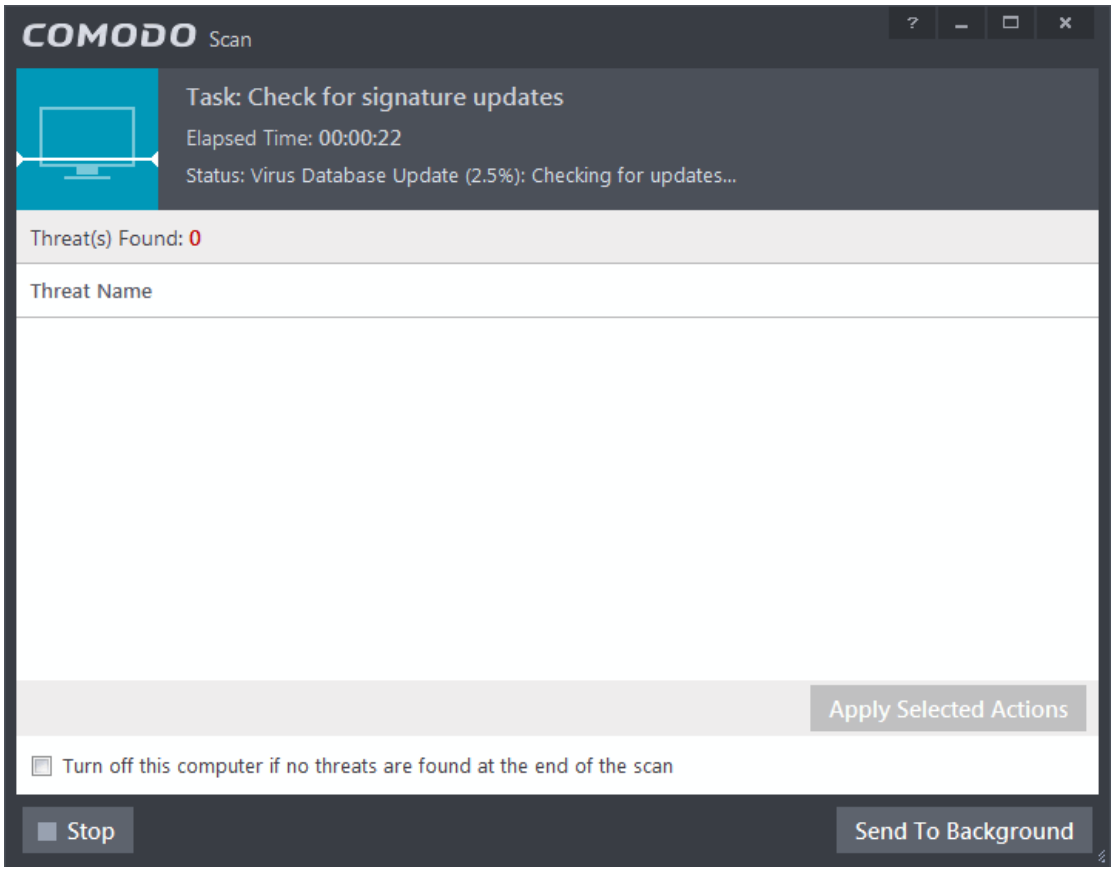
After customizing your installation, click the 'Back' button to return to the installation configuration screen.

- Click the 'Agree and Install' button to proceed with the installation.

Step 3 - Installation progress (**Click to go back to Step 2**)

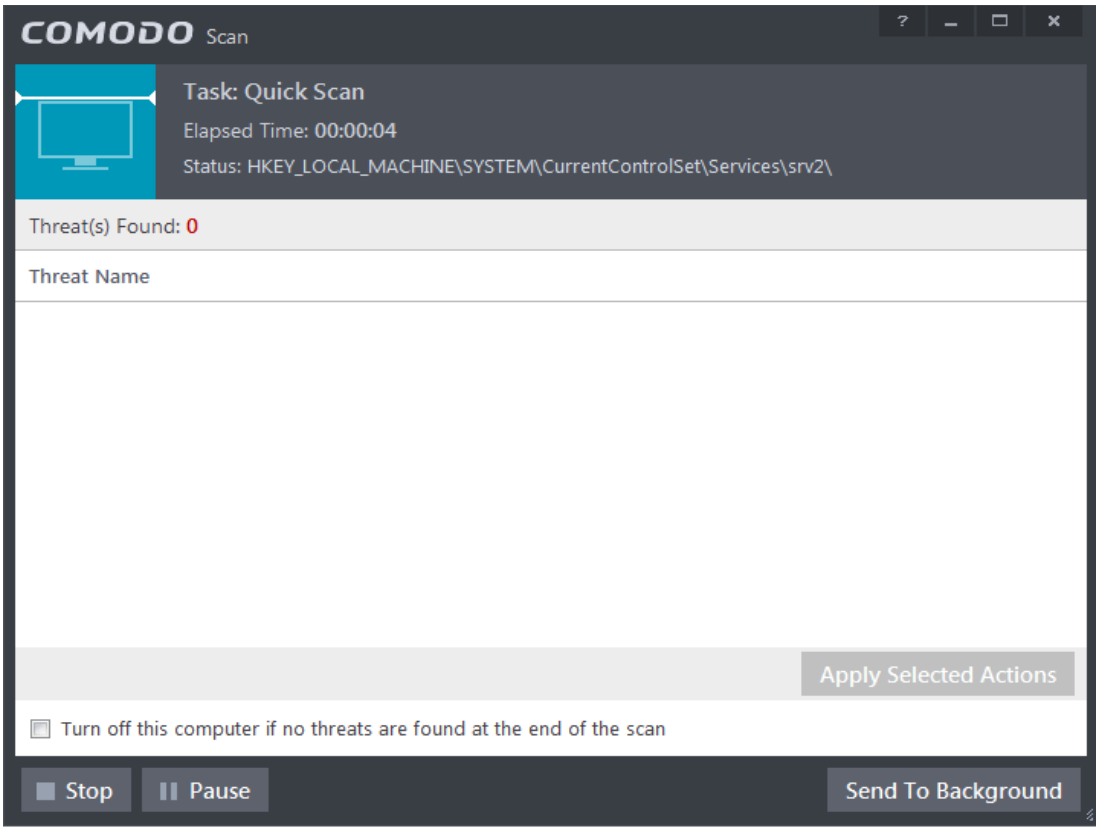
The installation progress will be displayed...

...and on completion, the application initiates the first quick scan on your computer. The virus database will be updated automatically prior to the scan.



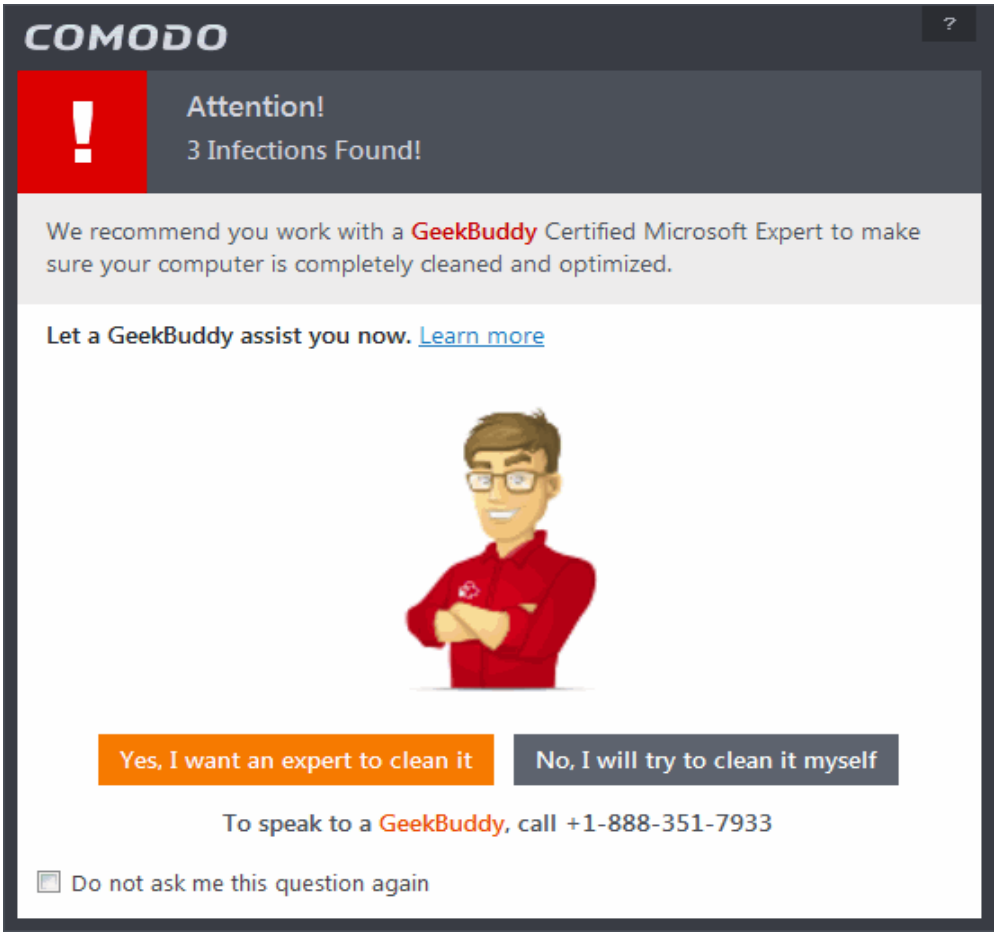
You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '**Manage CIS Tasks**' for more details.

CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



If you do not want the scan to continue at this time, click the 'Stop' button.

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

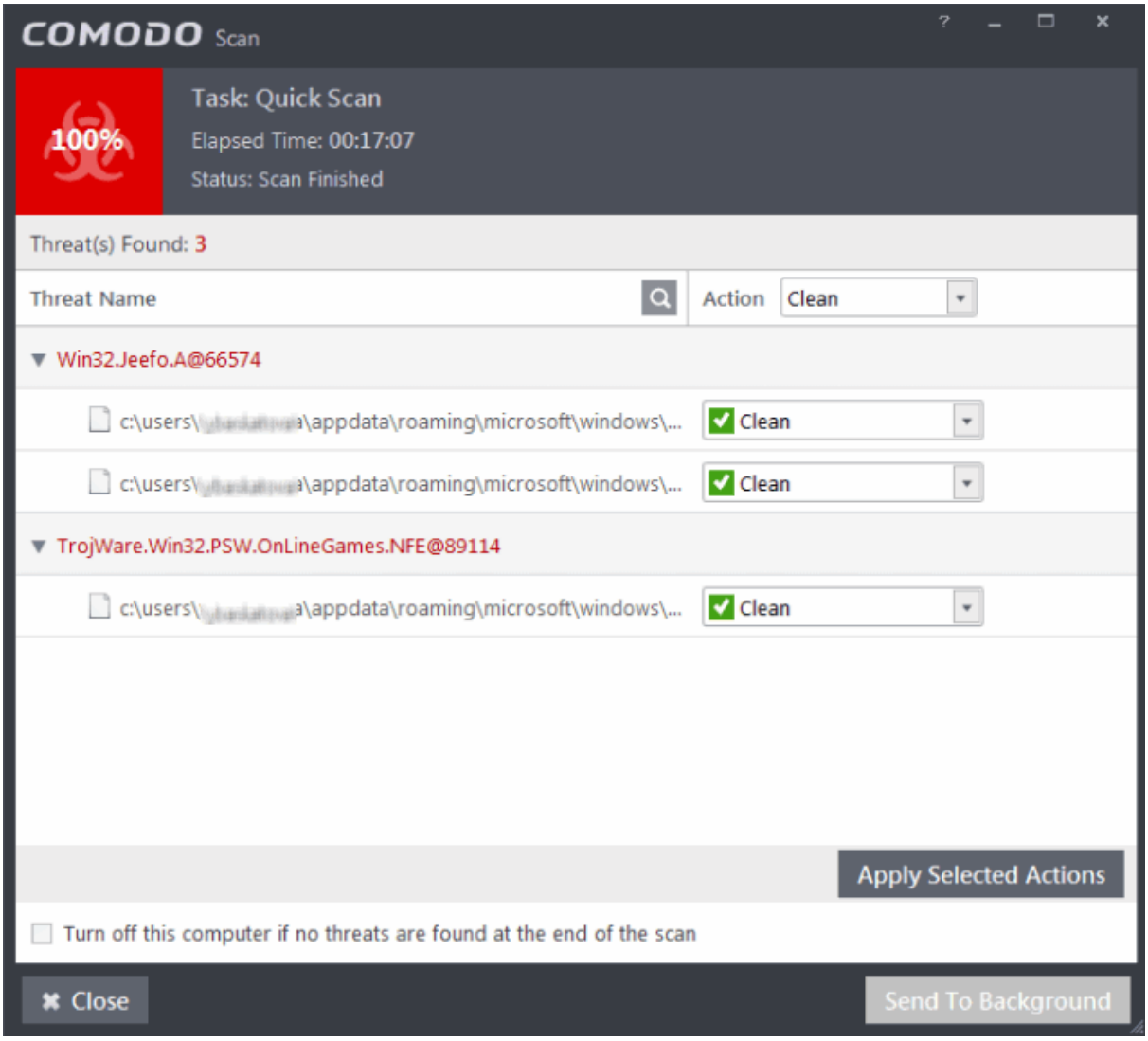


- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up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

  For more details on GeekBuddy, refer to the section **Comodo GeekBuddy**.

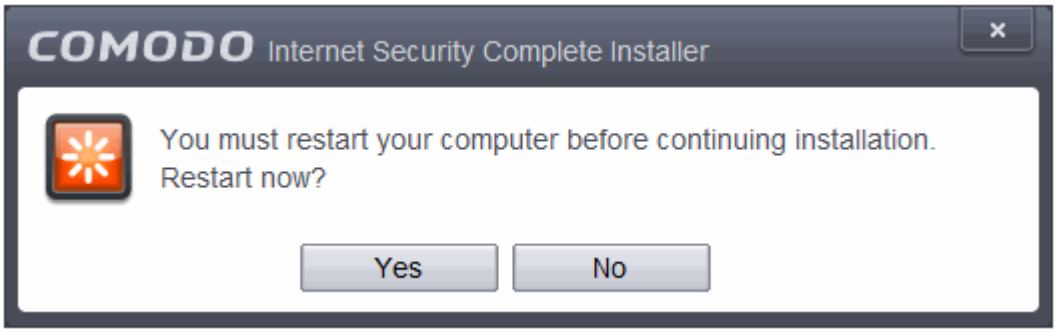
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. Refer to the section '**Processing Infected Files**' for more details.

- An example results screen is shown below:



Step 4 - Restarting Your System

In order for the installation to take effect, your computer needs to be restarted.



- To restart the computer click 'Yes'.

Note: The installation will take effect only on the next restart of the computer.

Step 5 - After Restarting Your System

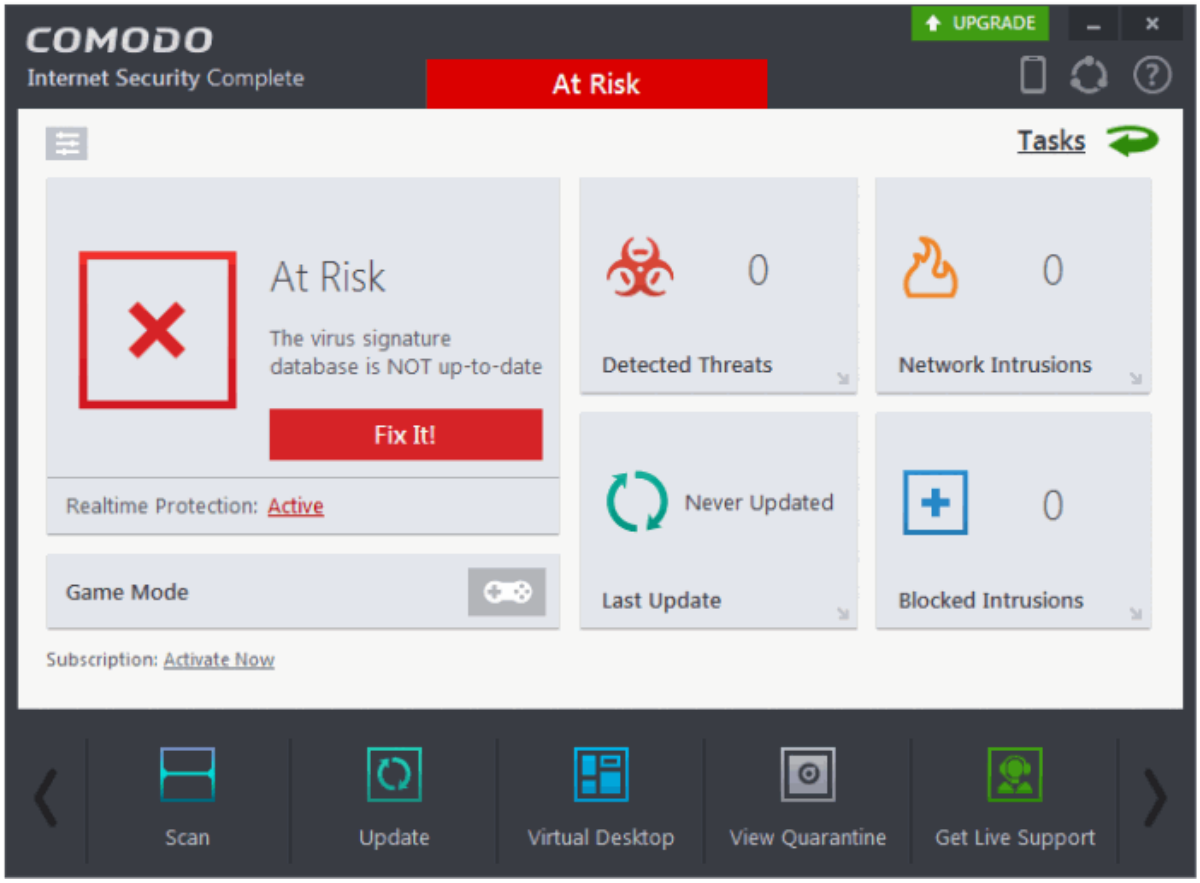
After restarting, a 'Welcome' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice. You can also purchase license key from this screen if you have not done so already.

This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

- Select your location from the three options
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '**Network Zones**' interface and through the **Stealth Ports Wizard**).

The main interface will be displayed:



Important Note: After successful installation, you need to activate the license for using the product. In order to get your guarantee coverage and TrustConnect service enabled, you need to activate the license first.

- For full explanation on activation of license after installation of the product, refer to **Activating Your License.**
- For full explanation on activation of your guarantee, refer to **Activating Your Guarantee Coverage.**

1.3.4. Activating CIS Pro/Complete Services after Installation

CIS Pro and CIS Complete should be activated after installation for contiuned use of the product. You will get alerts to activate the license if it has not been done so. Refer to the following sections for explainations on:

- **Activating Your License**;
- **Activating Your Guarantee Coverage**;
- **Renewal of Your License**.

1.3.4.1. Activating Your License

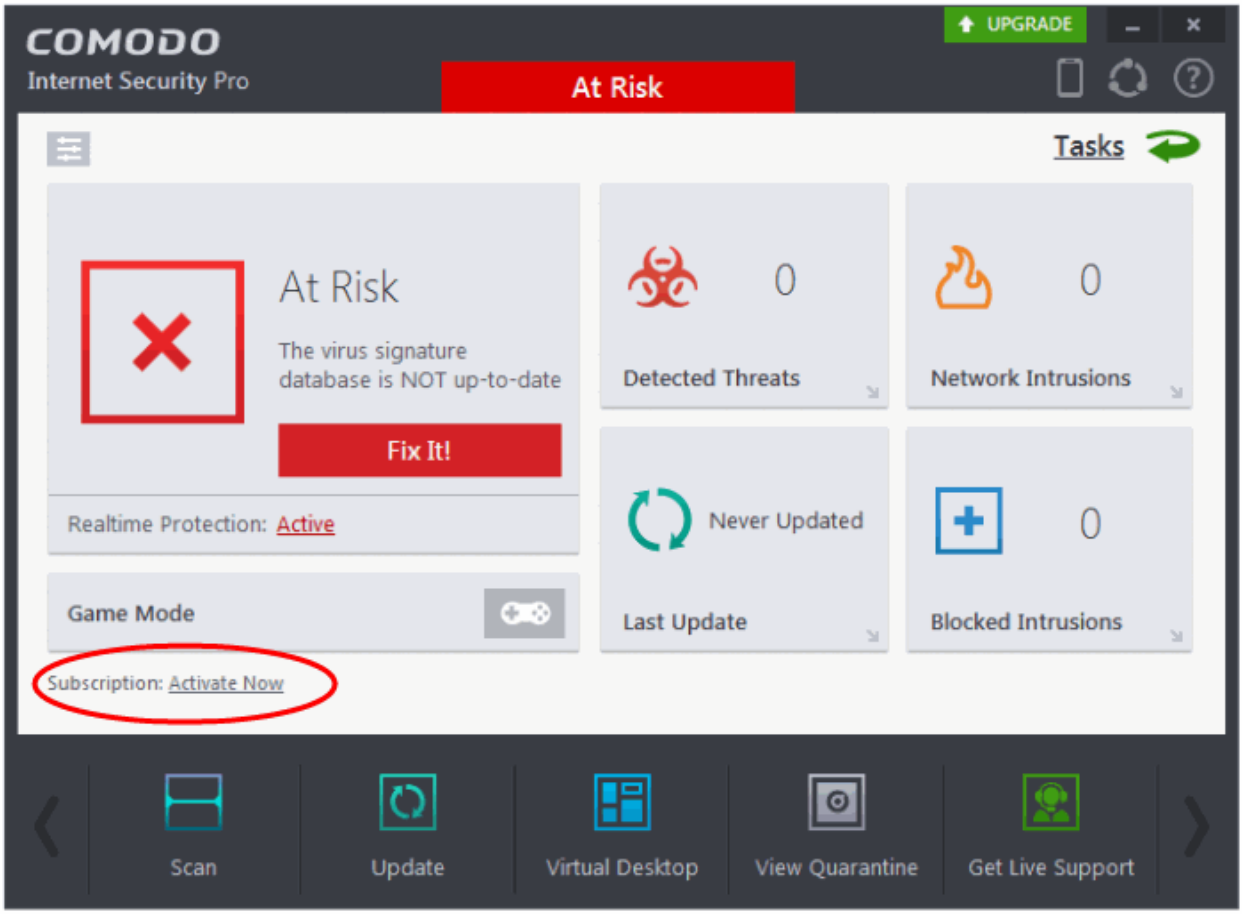
- **Activating your CIS Pro**
- **Activating your CIS Complete**

Activating your CIS Pro

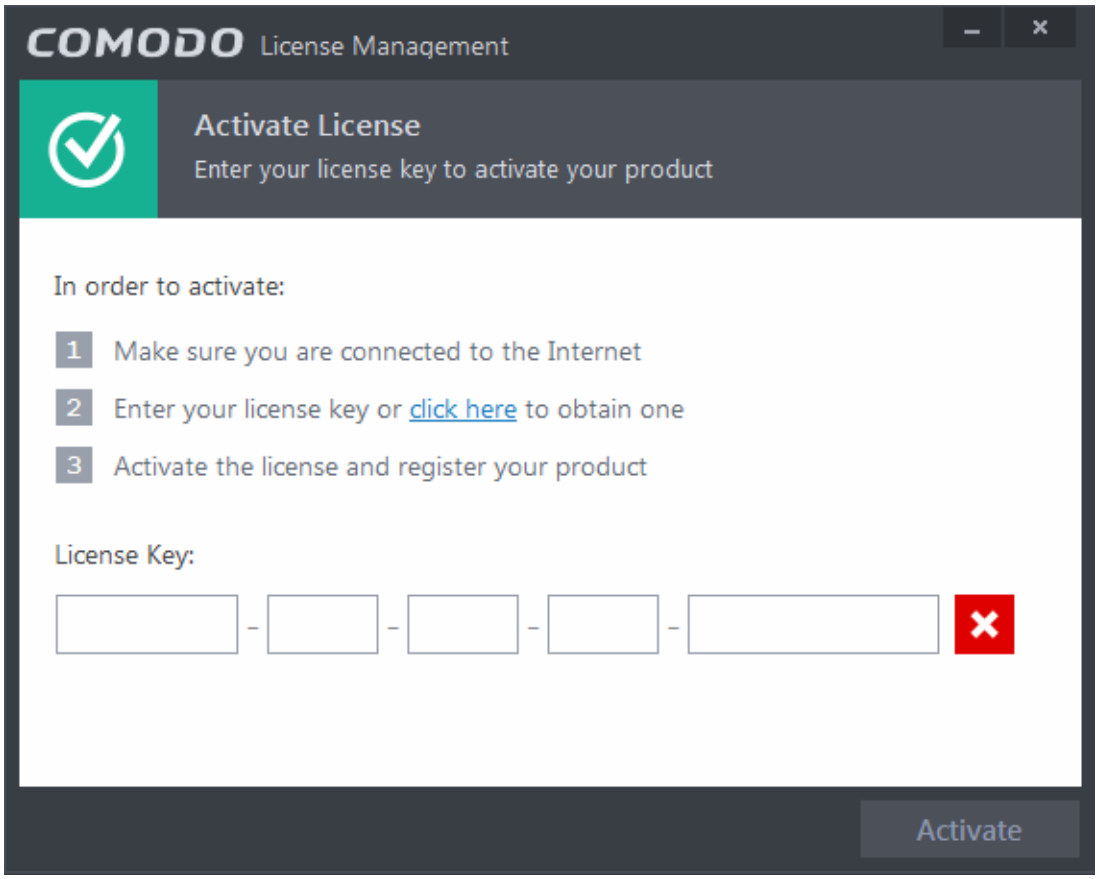
- Start the Comodo Internet Security Pro application as explained in the section **Starting Comodo Internet**

Security.

Step 1: To activate your License, click 'Activate Now' beside 'Subscription' in the home screen.

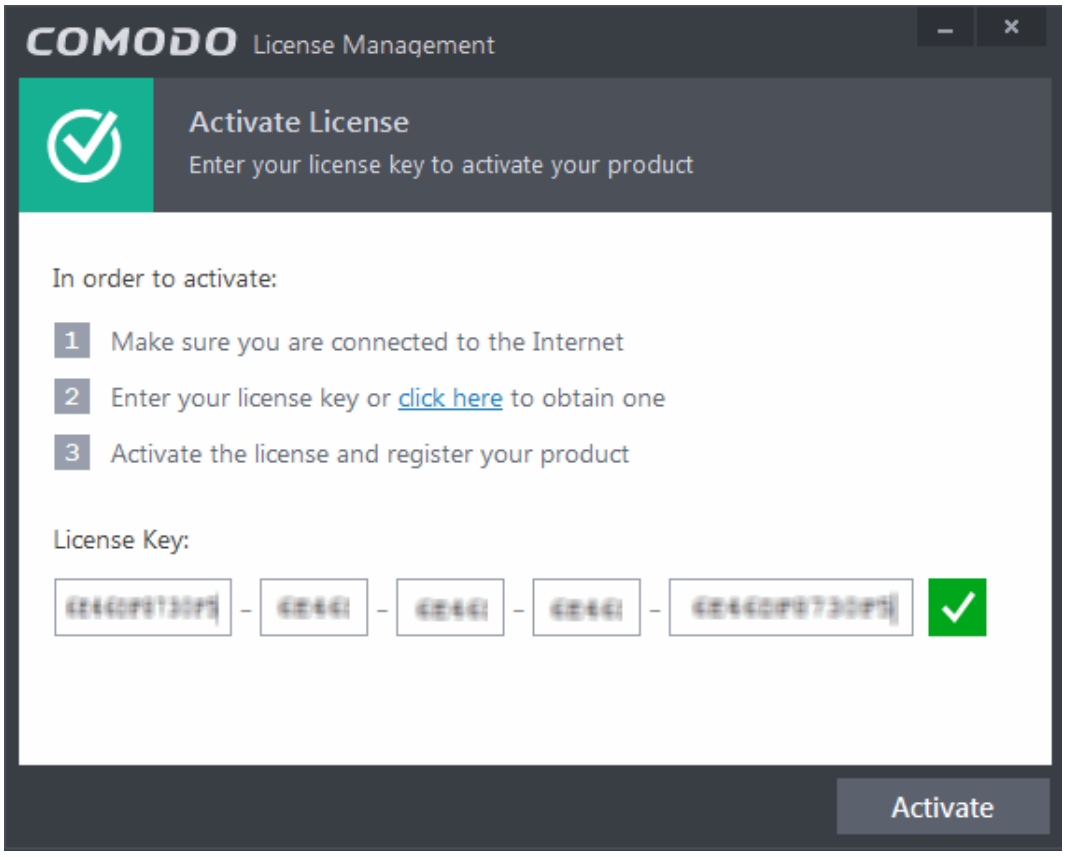


The License Activation Wizard will start.

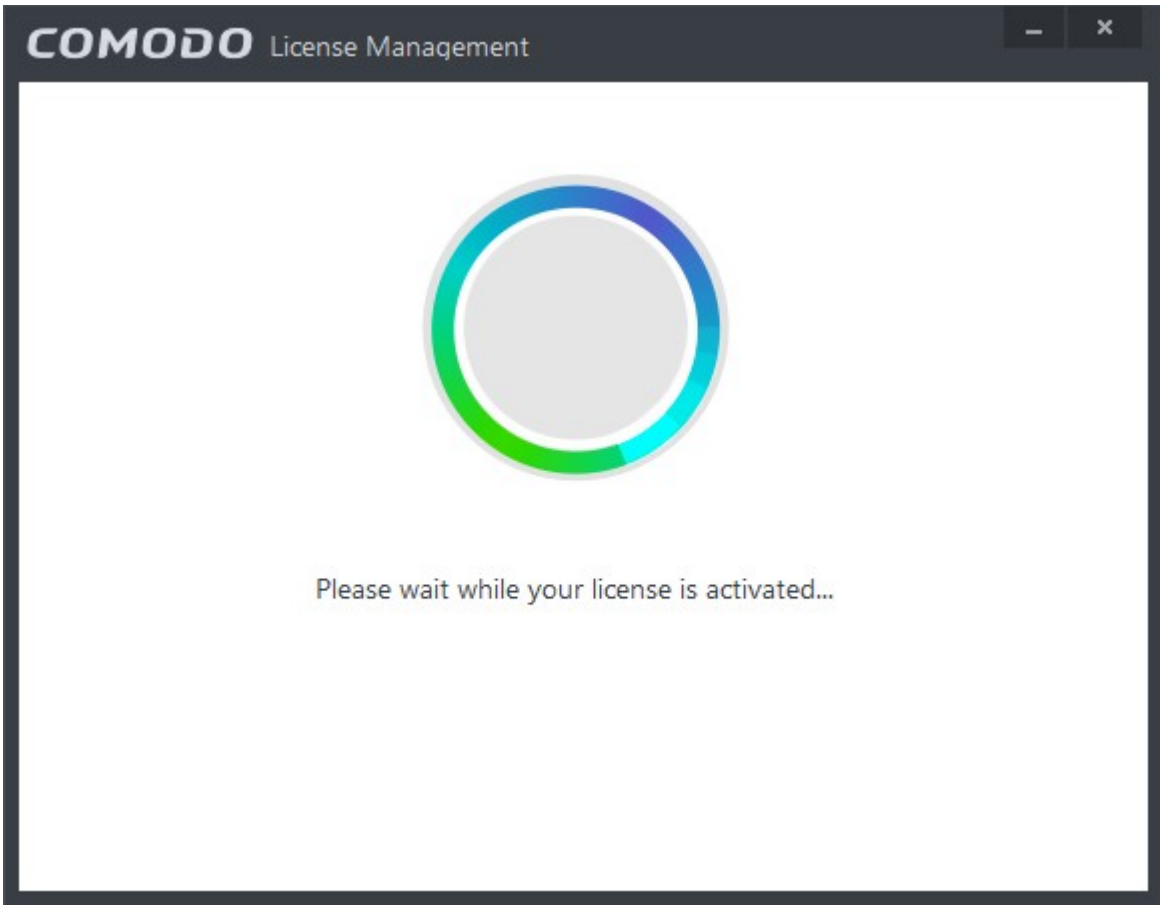


- You should have received your License key through email if you have purchased CIS Pro.

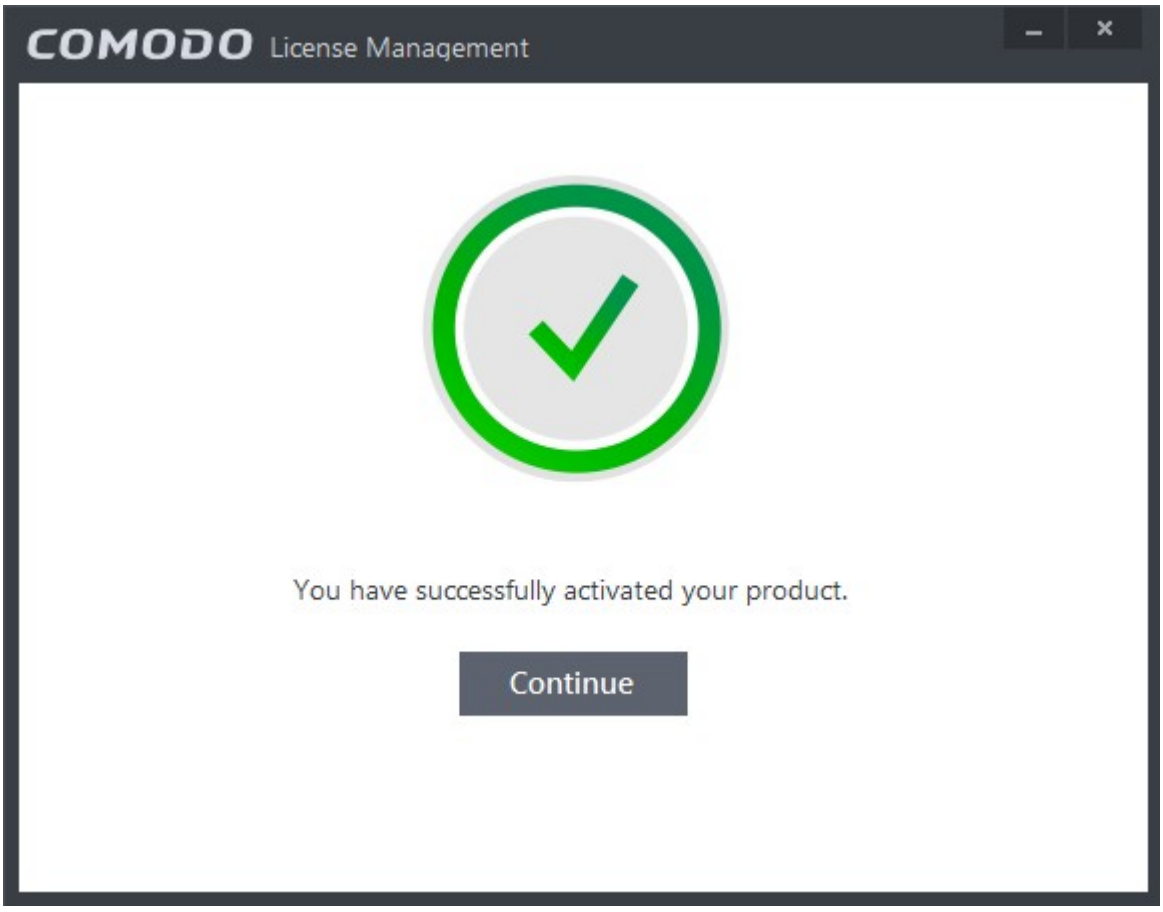
Tip: If you haven't subscribed for Comodo Internet Security - Pro or Complete so far, click the 'click here' link. You will be taken to the Comodo website enabling you to purchase the license.



- The wizard starts validating your key.



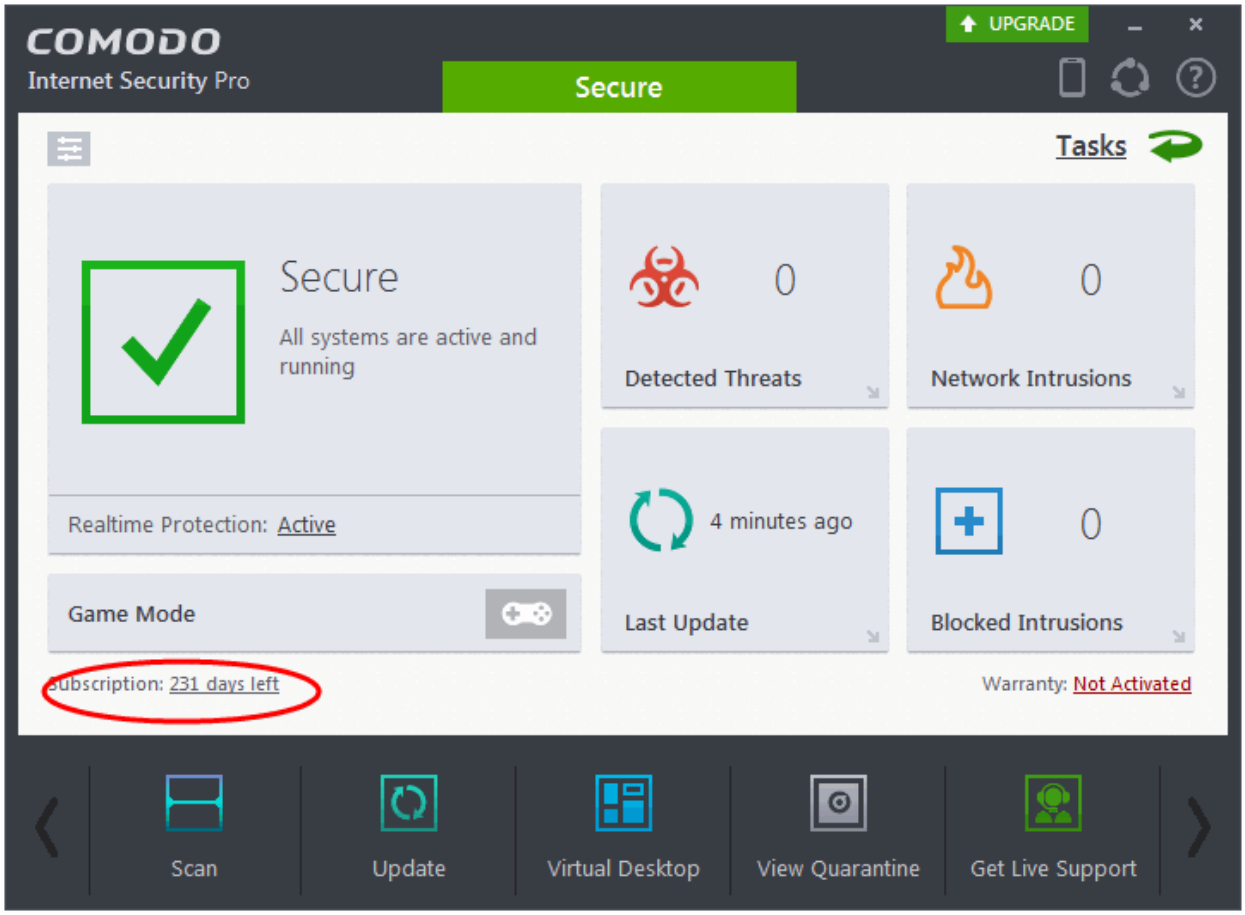
On successful validation, your license will be activated.



- Click 'Continue' to exit the wizard. Your CIS Pro product is now activated.

Tip: You can also enter your activation key by clicking the link 'Enter a license key' in the About dialog, accessible by clicking **Help icon > About** from the title bar.

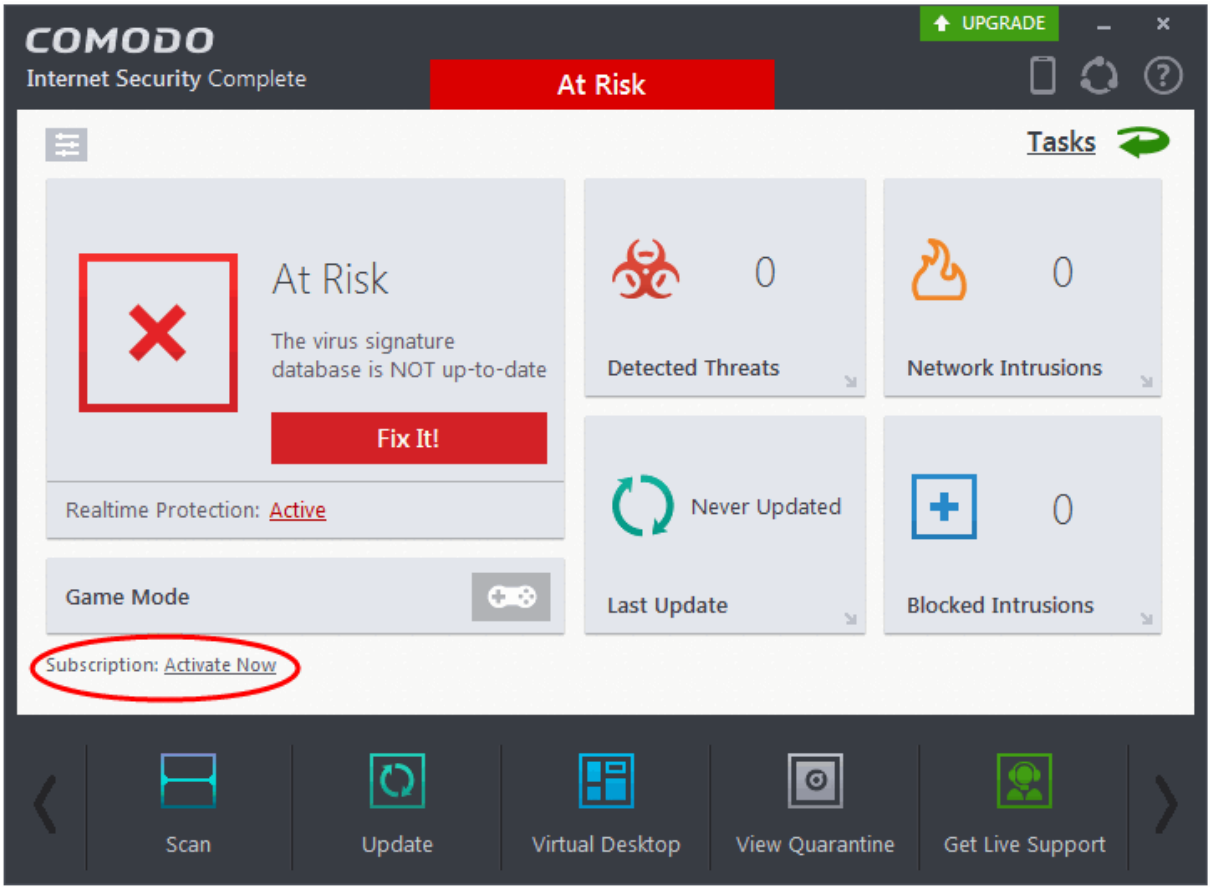
The main interface will display the number of days left for the license before it should be renewed.



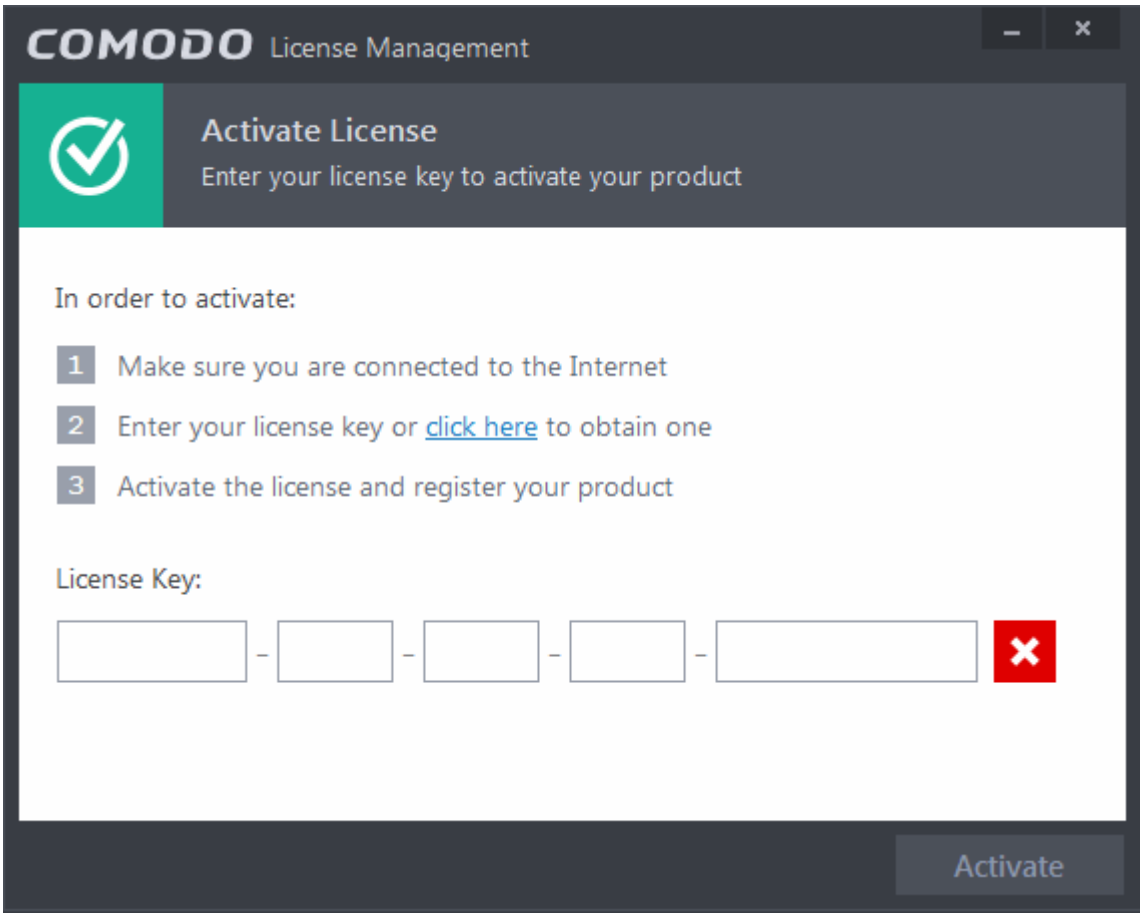
Activating your CIS Complete

- Start the Comodo Internet Security Complete application as explained in the section **Starting Comodo Internet Security**.

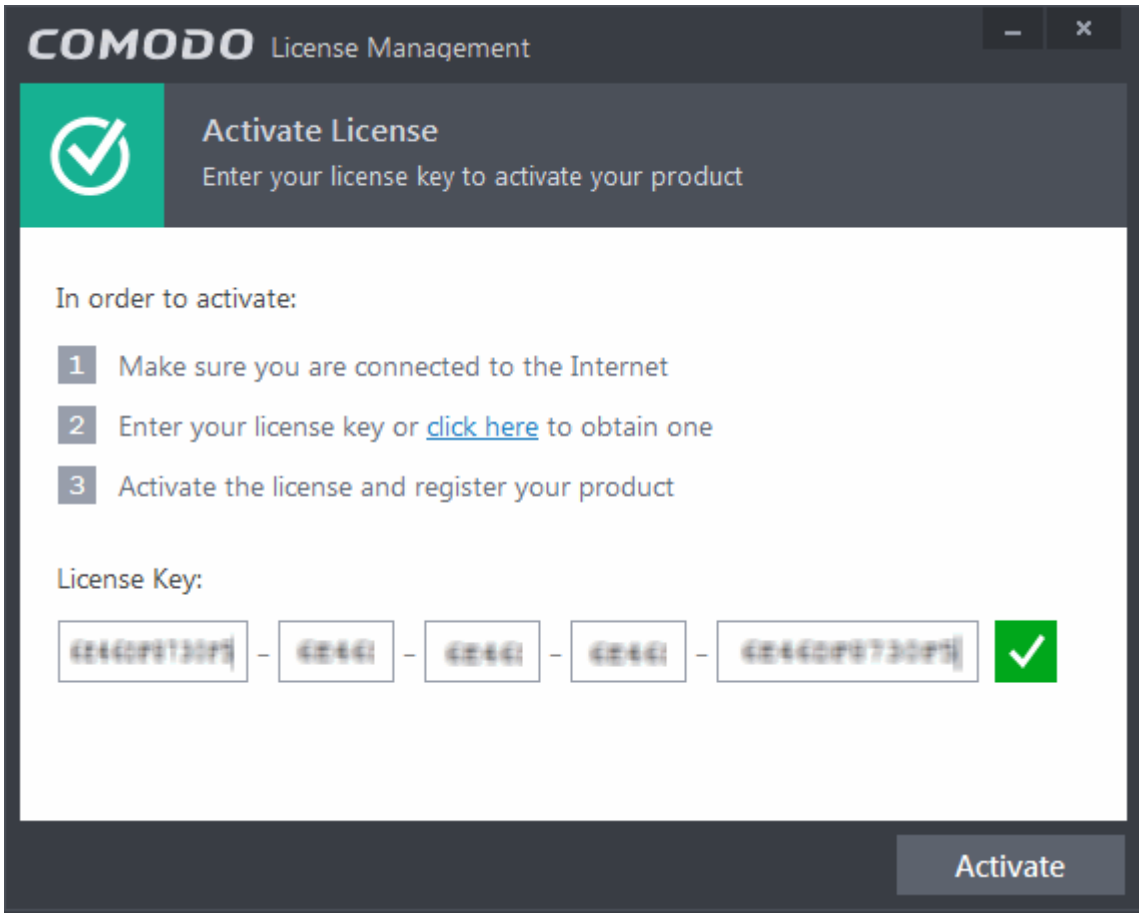
The License Activation Wizard will start.



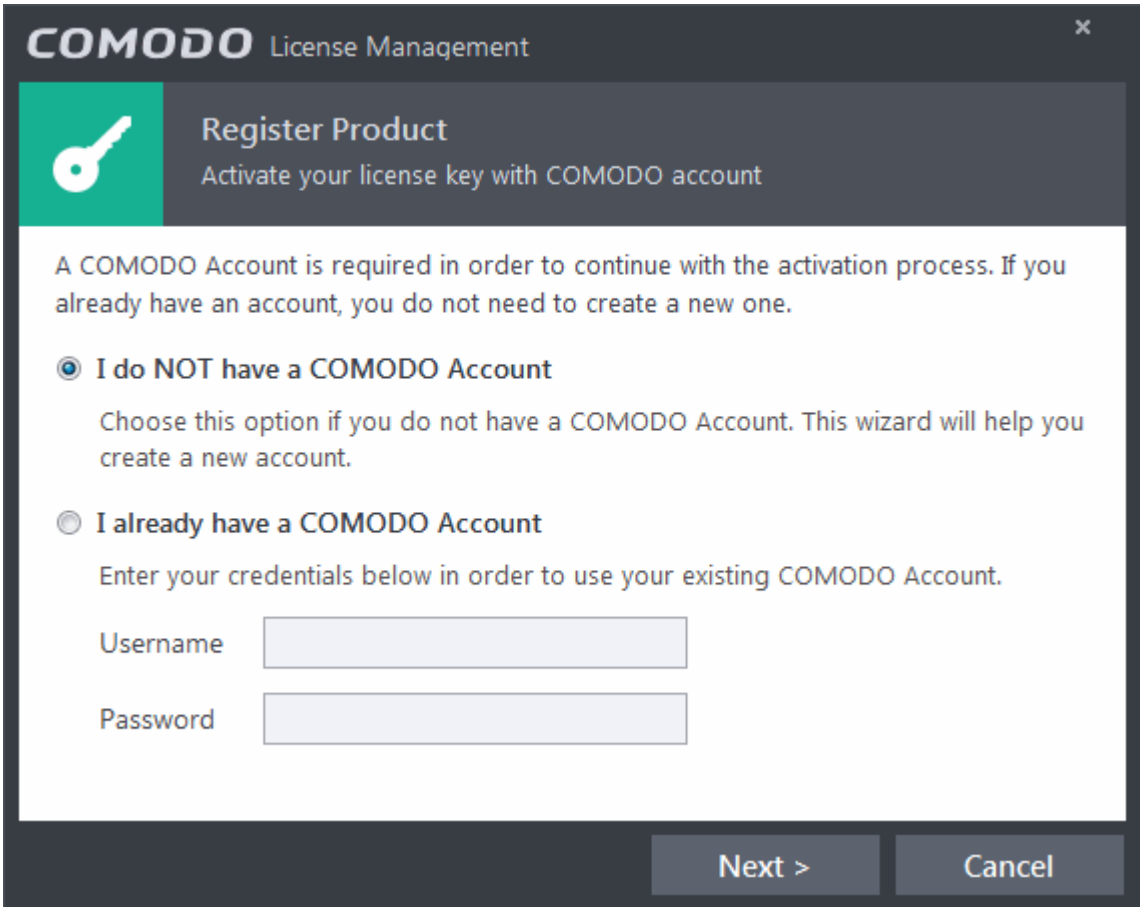
- The CIS Complete license key is available on the DVD itself or printed on an insert included in the box packaging. Enter the license key and click 'Activate'.



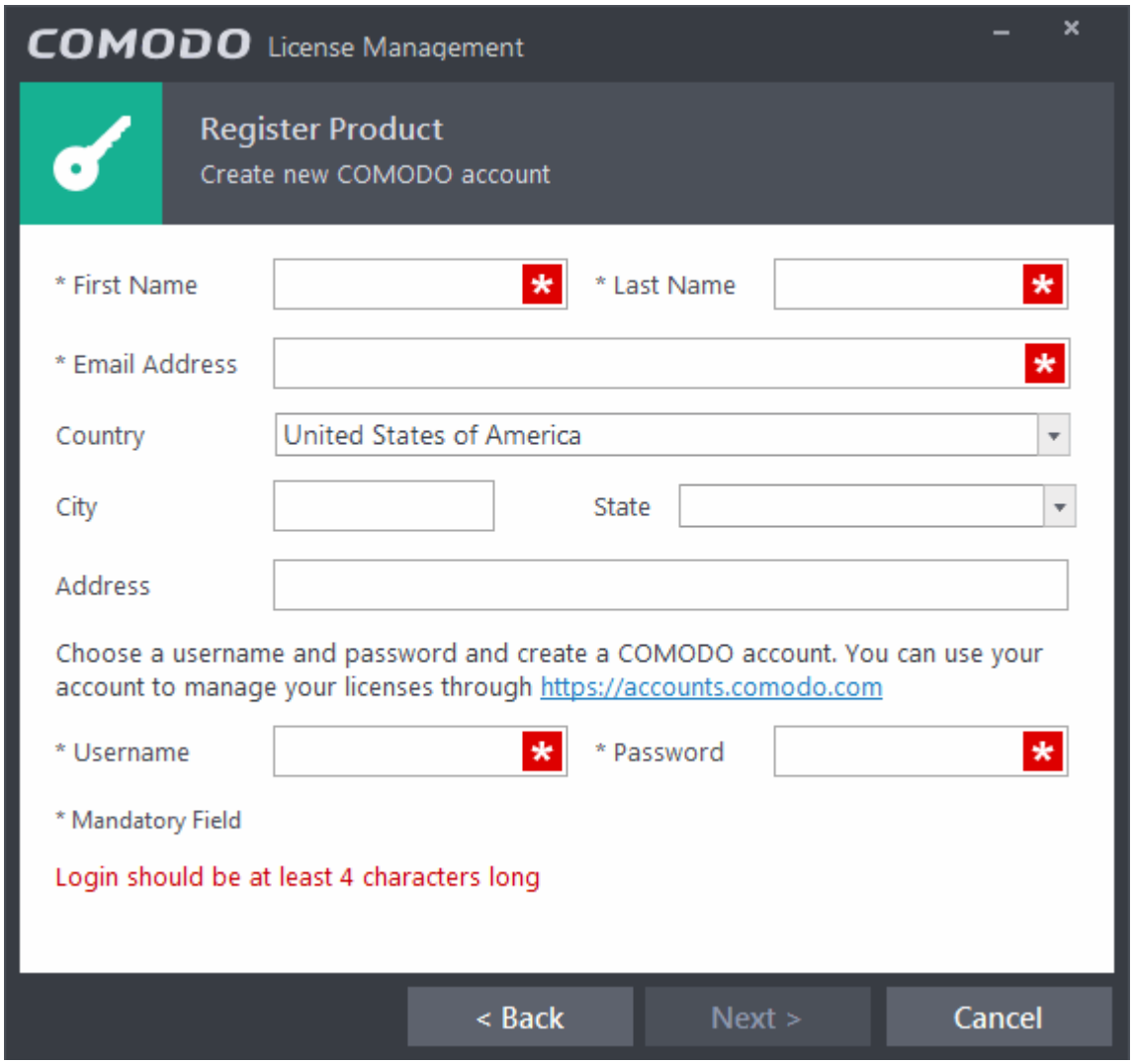
Tip: If you haven't subscribed for Comodo Internet Security - Pro or Complete so far, click the 'click here' link. You will be taken to the Comodo website enabling you to purchase the license.



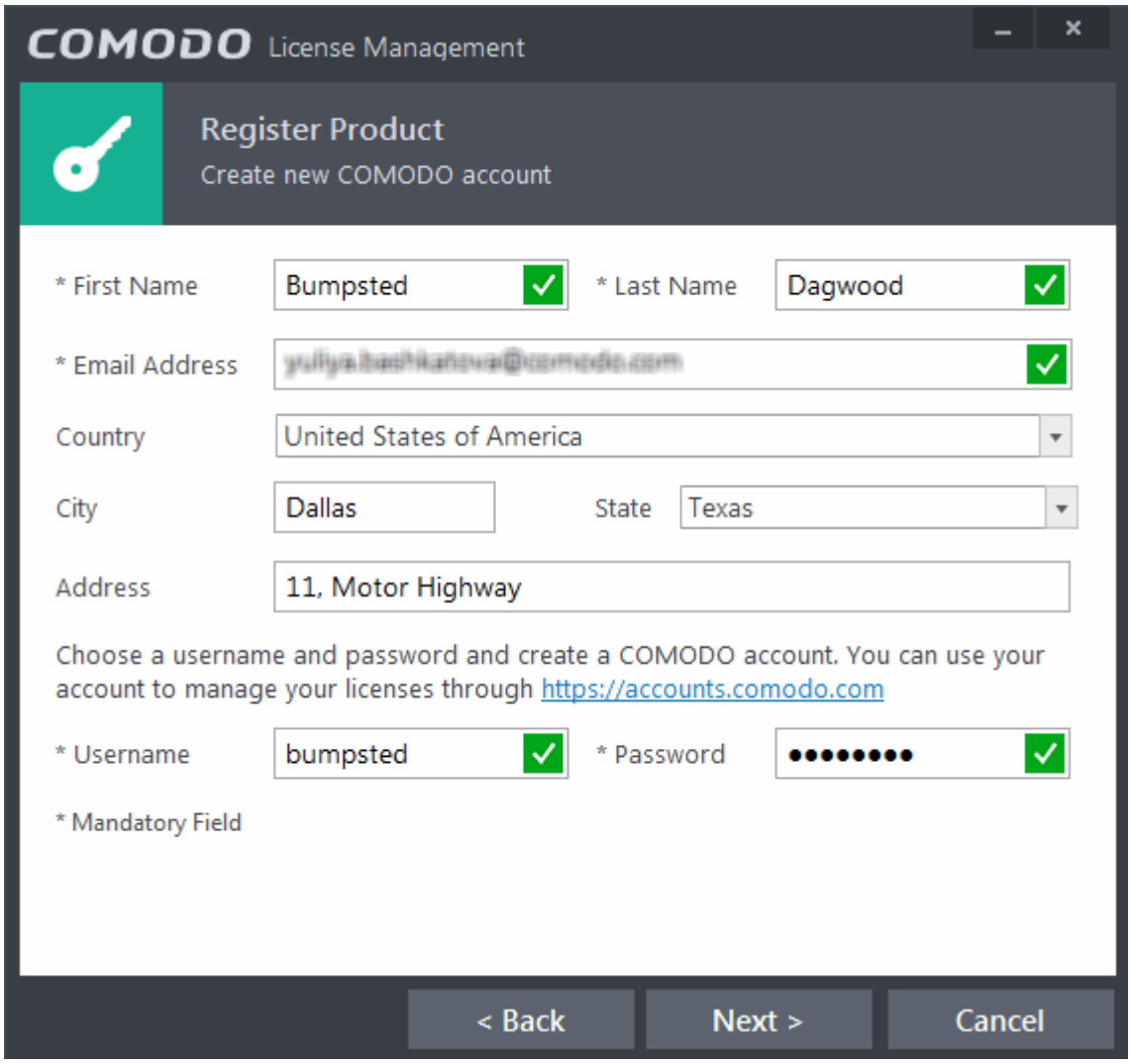
The Product Registration dialog will be displayed.



- If you already have an account with Comodo Accounts Manager (CAM), Select I already have a COMODO Account enter your username and password for the account and click 'Next'. You will be taken to the **validation step**.
- If you do not have a CAM account, select I do not have a COMODO account and click 'Next'. A new account registration from will appear.

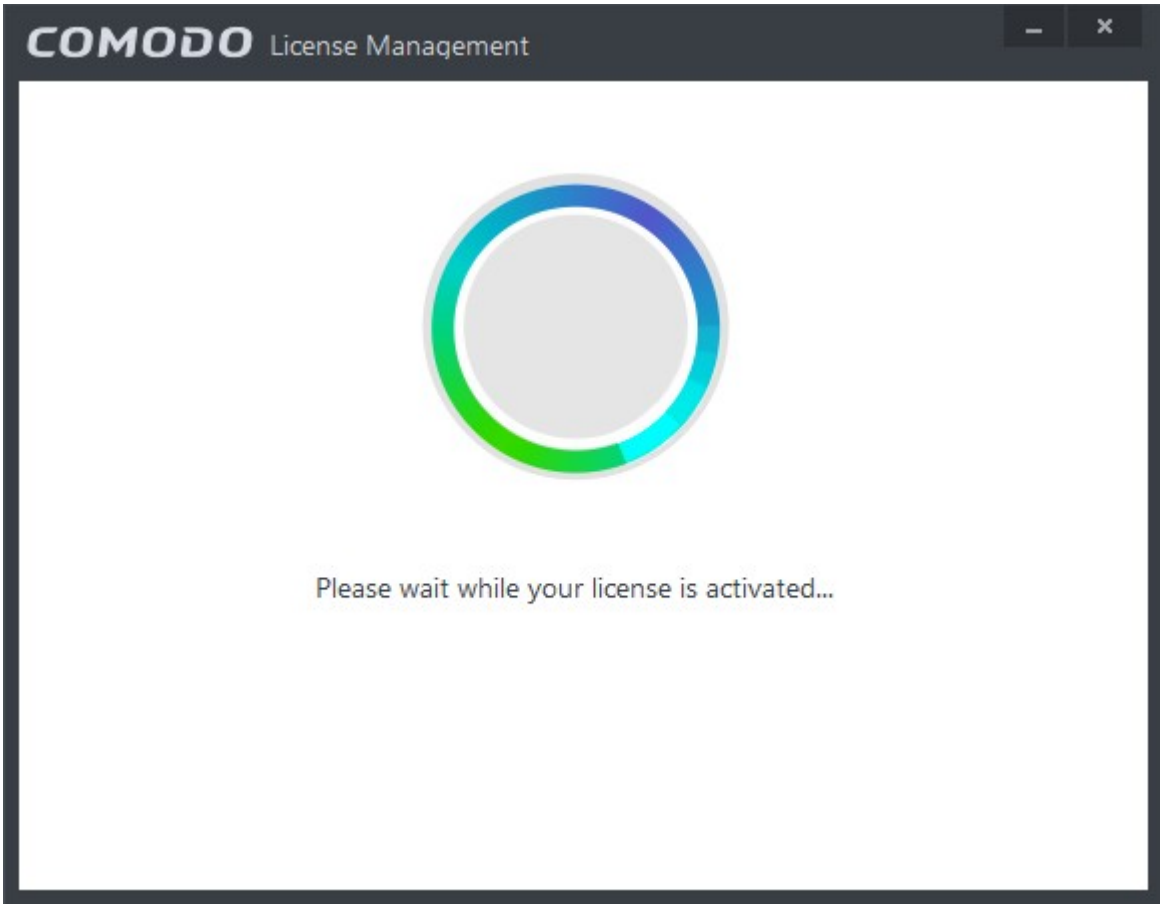


- Fill up the registration form with the login details and password for your Comodo Accounts Manager (CAM) account.

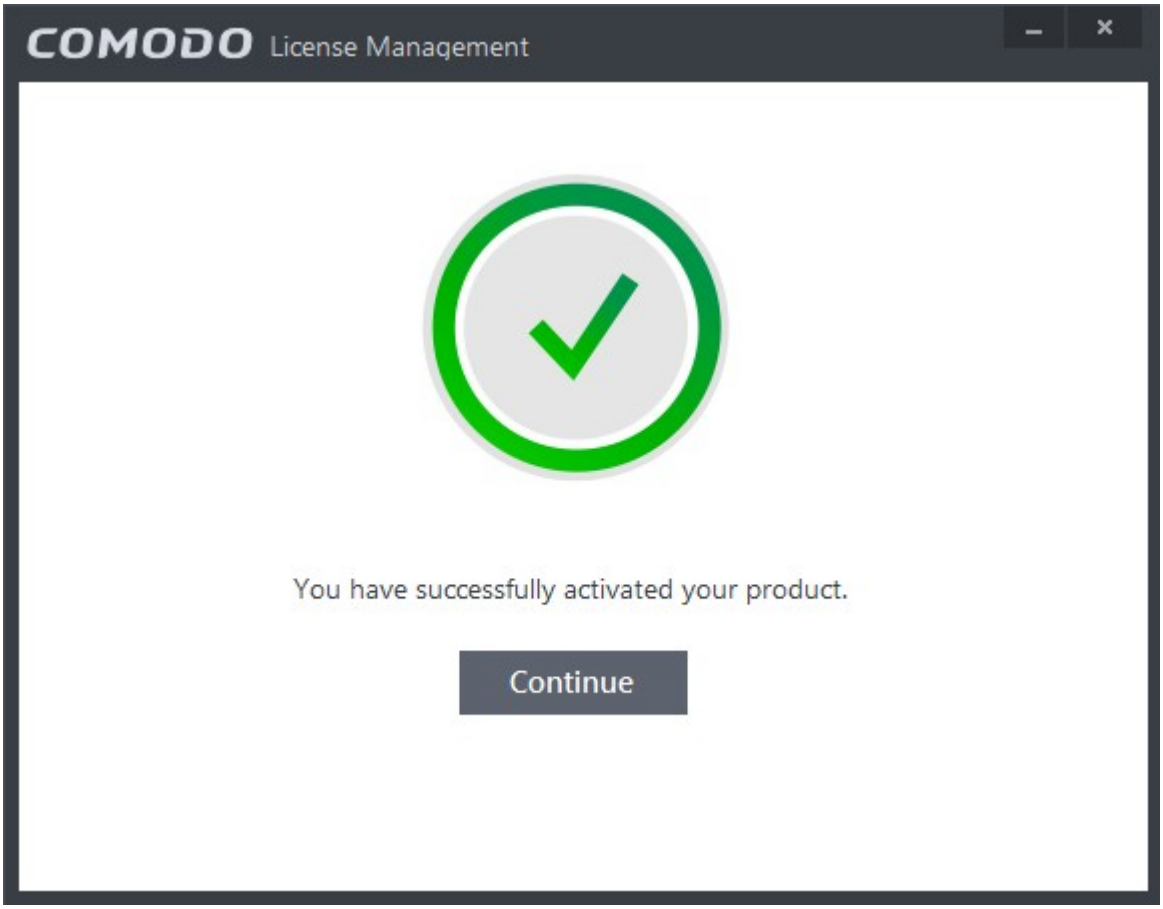


Field	Description
Name	Enter your first name
Last Name	Enter your last name
Email	Enter your email address
Address	Enter your address
City	Enter your city name
Country	Select your country from the drop-down box
State	Select your state from the drop-down box
Address	Enter you full address
Create a new COMODO Account	
• Enter your username and password to create a new Comodo account with Comodo Accounts Manager (CAM)	

- Click 'Next'. Your license will be validated...



... and on successful validation, your subscription will be activated and a confirmation screen will be displayed.



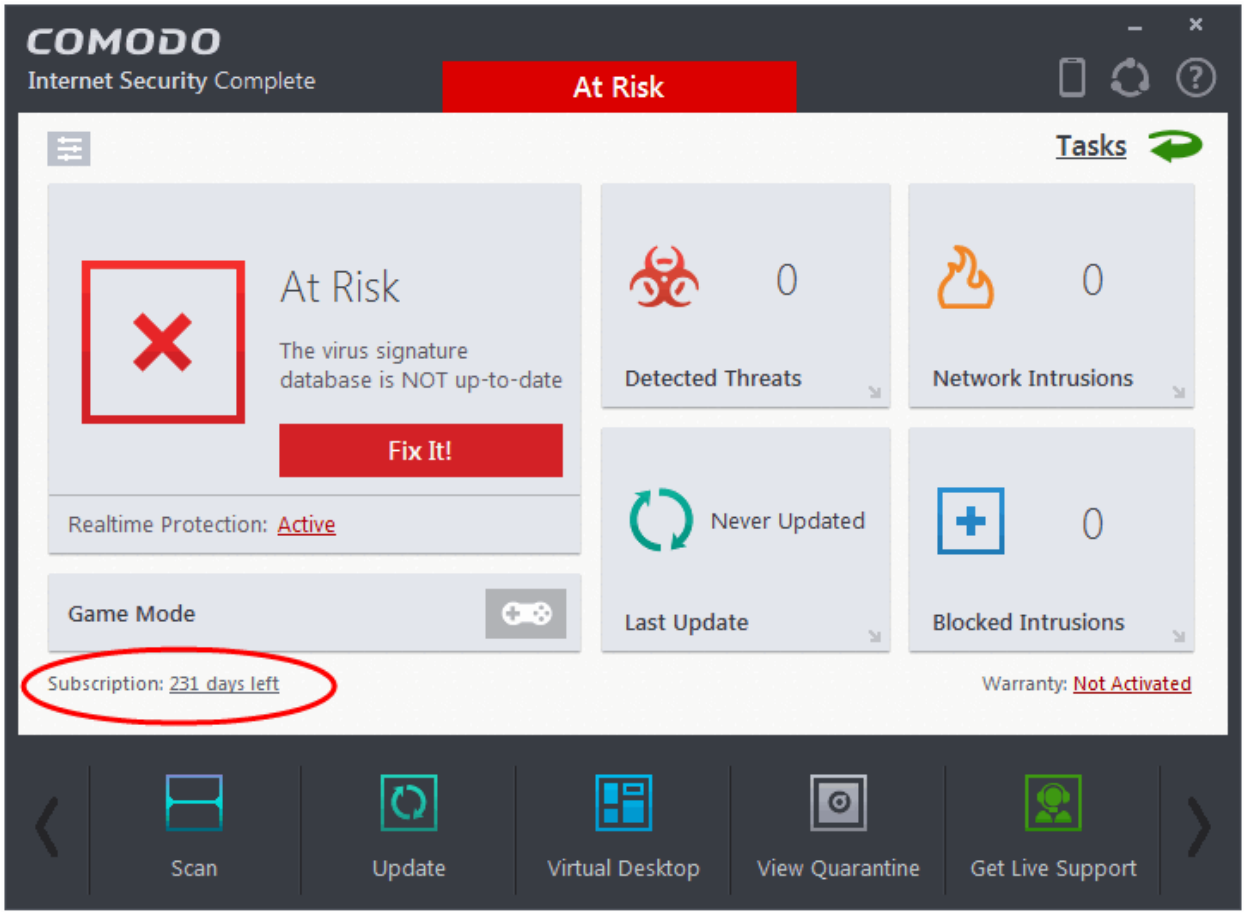
- Click 'Continue' to exit the wizard.

Your CIS Complete product will be activated along with Comodo Backup and TrustConnect

- Accessing Comdo Backup online storage space - Use the login credentials provided during the CIS Complete registration step.
- Using the TrustConnect service - The TrustConnect service will be automatically enabled after successful activation of the license. Please refer to the section **TrustConnect Overview** for more details on how to use the service.

Tip: You can also enter your activation key by clicking the link 'Enter a license key' in the About dialog, accessible by clicking **Help icon > About** from the title bar.

The main interface will display the number of days left for the license before it should be renewed.



1.3.4.2. Activating Your Guarantee Coverage

The Comodo Guarantee is available to customers of CIS Pro and CIS Complete versions. Before enabling guarantee coverage, customers should first have activated their licence. Full details on activating the license can be found in **Activating Your License** section.

- Please note that if you wish to use and activate the Comodo guarantee then you must have installed Comodo Internet Security (both Antivirus and Firewall components) and Comodo GeekBuddy. You must also have run and passed a Comodo Antivirus scan using the latest signature database. Please see the **End User License Agreement** (EULA) for full details.

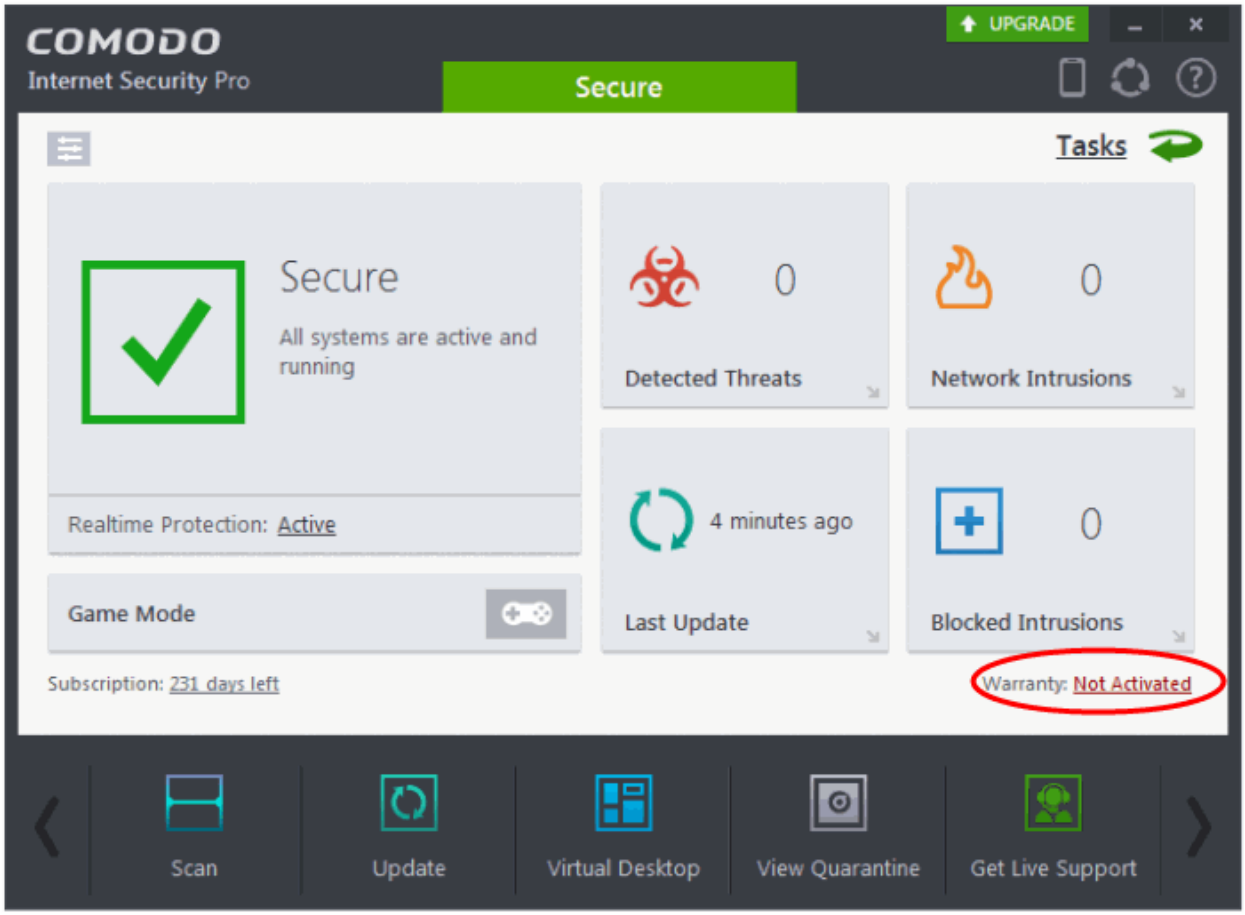
Limits: The guarantee is limited to the lesser of:

- The actual cost of the computer;
- An aggregate total of $500 for all claims paid under a single license key, and
- The actual cost of a Comodo specified and authorized third party provider to repair the computer to an operating condition ('Guarantee Limit').

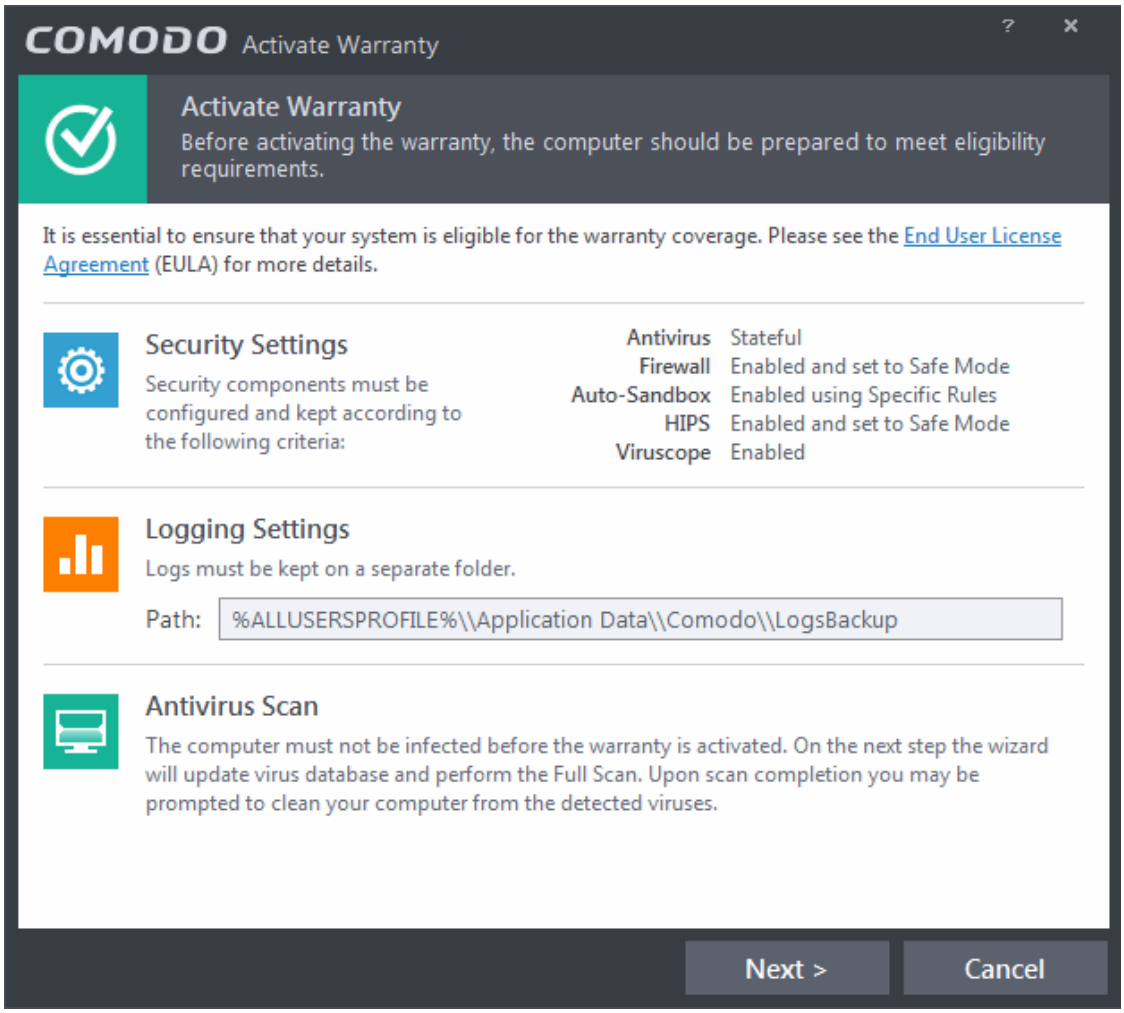
- The guarantee is limited to repairing the computer over the Internet to an operational state and excludes all claims for lost or expected profits, lost or corrupted data, lost or deleted work, or lost or damaged personal files. Comodo does not guarantee against the loss of any file or information. The guarantee is void if you breached this agreement, failed to follow the procedures described in this Section 3 of the EULA or failed to pay any fees applicable to your use of the Software.
- Full Terms and Conditions on the Comodo Guarantee Coverage can be read in Section 3 of CIS EULA (Step 2 of the Installation process for **CIS Pro** and Step 1 for **CIS Complete**).

Important Note: Before activating the guarantee, it is essential to run a full computer AV scan with the latest version of the Comodo Virus database in order to ensure that your system is eligible for the Guarantee coverage. Make sure that the virus database of your CIS installation has been updated to the latest one. The update status is indicated next to 'Last Update' in the 'Virus Defense' box of the CIS main interface and with a green tick mark and the text 'All Systems are active and running' in the lower left corner of the main interface. If your virus database is not up-to-date, click the link next to 'Last Update' in the 'Virus Defense' box to update to the latest version. Then run a full computer scan from the Antivirus Tasks interface of the CIS. For more details on running an Antivirus Scan **Click here**.

Step 1: To activate your guarantee coverage, click 'Not Activated' beside 'Warranty' in the home screen.

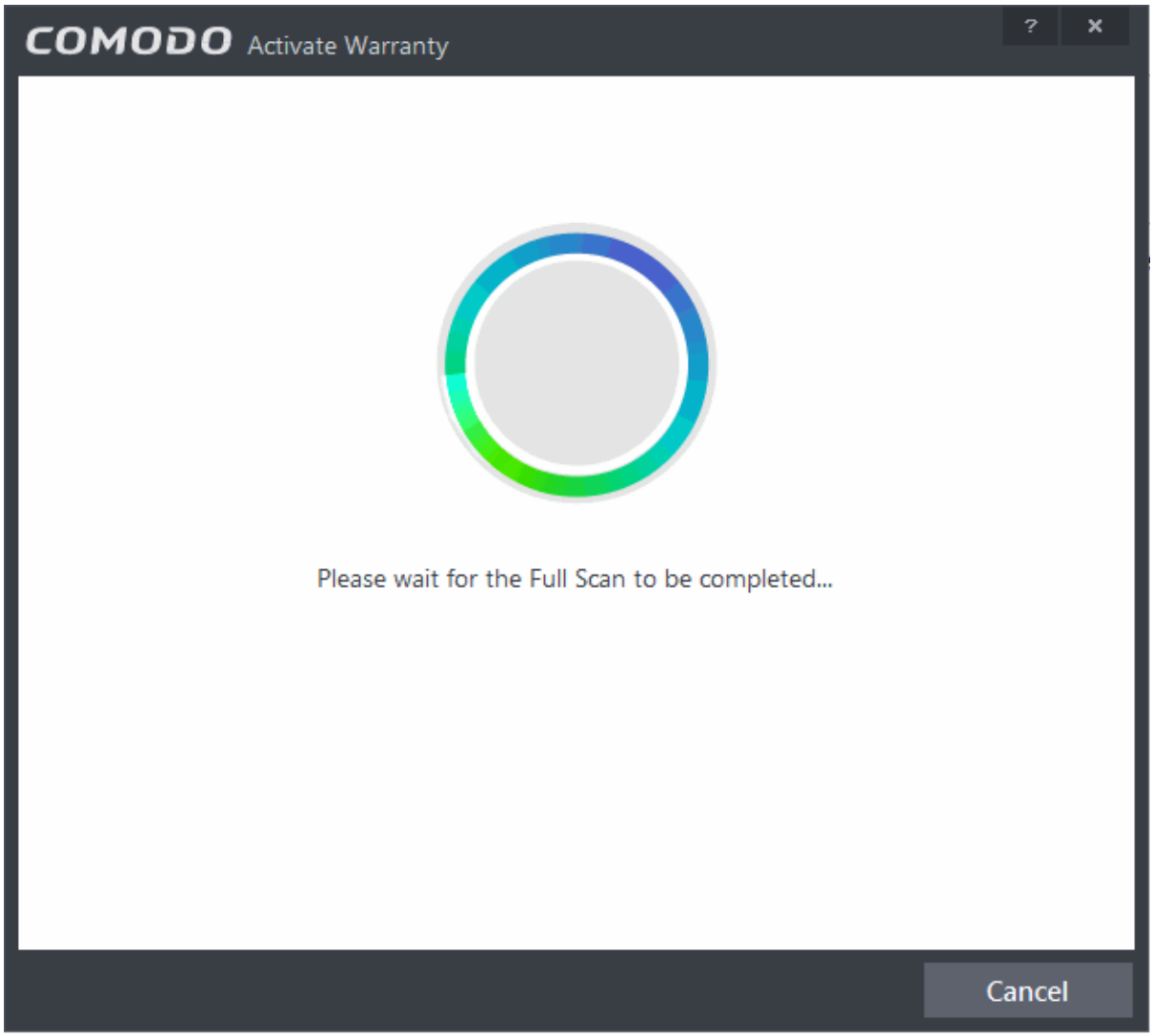


The Warranty Activation Wizard will start.

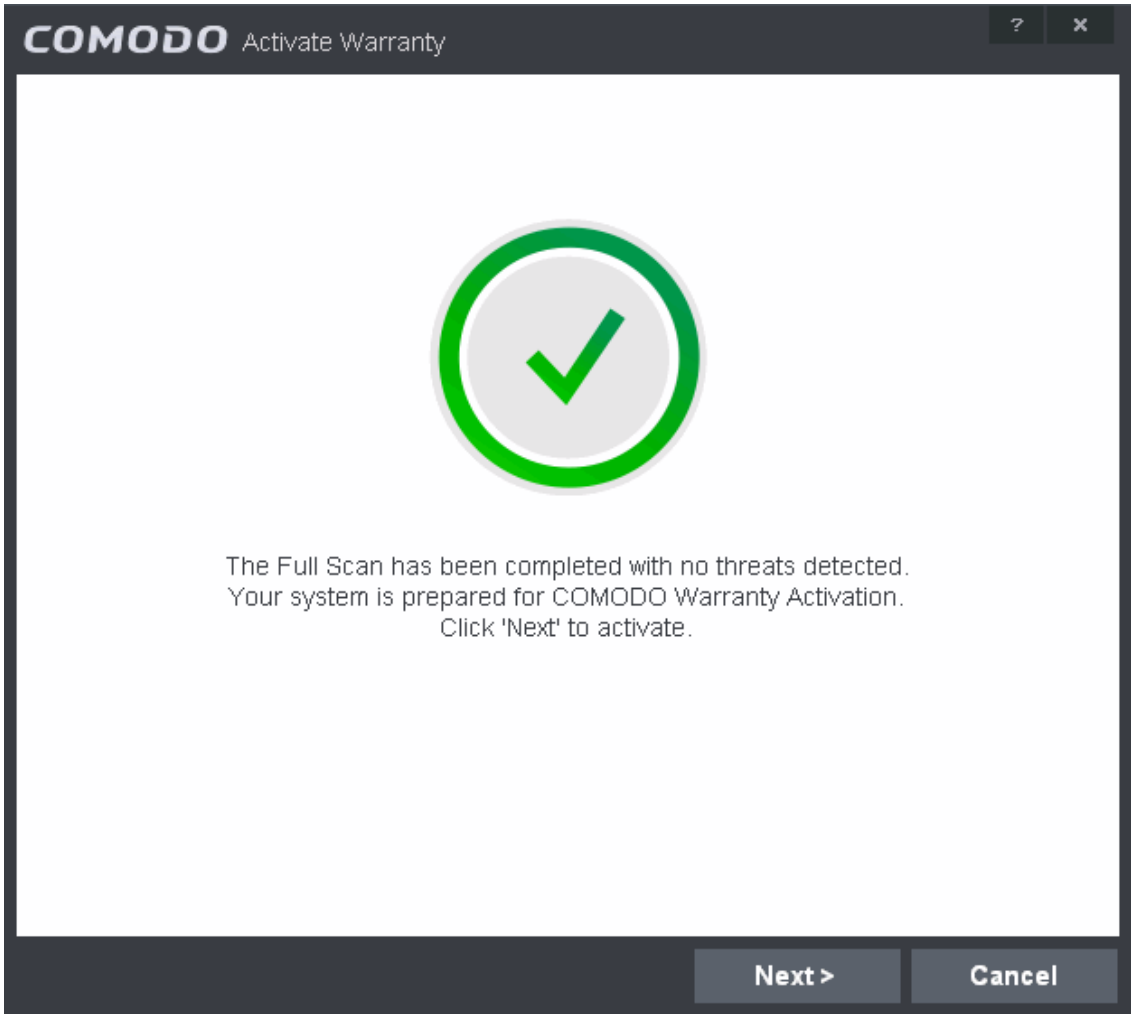


The Warranty Activation screen displays the minimum requirements to be met for the activation of warranty and the default storage location of the product logs.

- **Product Settings** - Displays the settings required for the individual Antivirus, Firewall and Defense+ for the activation of warranty. These will be set by default. If you have changed these settings prior to the activation you will need to set them as stated in this area to proceed with the warranty activation.
- **Product Logs** - Displays the path in which the log files of CIS will be stored
- **Scan** - A full system scan to remove all known viruses is a mandatory requirement if your computer is to be eligible for guarantee coverage.
    - If you have already ran a Full Scan and removed the infection (and your system is clean), then clicking 'Next' proceeds to **step 2**.
    - If you haven't run a Full Scan already, clicking 'Next' will initiate a Full Scan. Refer to the section **Run a Full Computer Scan** for more details on scanning your full computer and cleaning the infected files. All the infections and threats identified during the scan should be cleaned for your computer to be qualify for the warranty. At the end of scanning and cleaning process, the wizard moves to **step 2**.

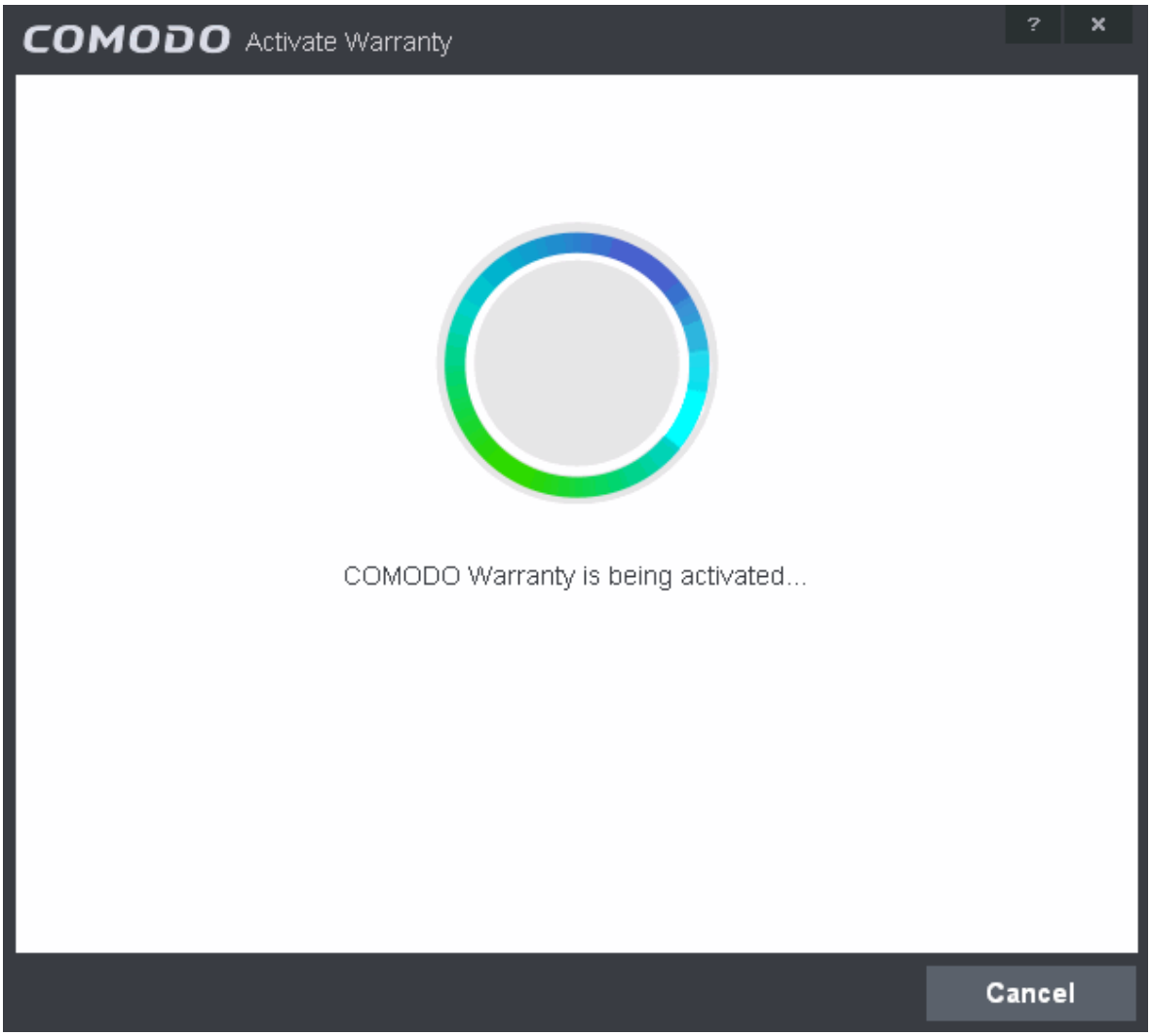


Step 2: The Guarantee Activation Wizard will start again.

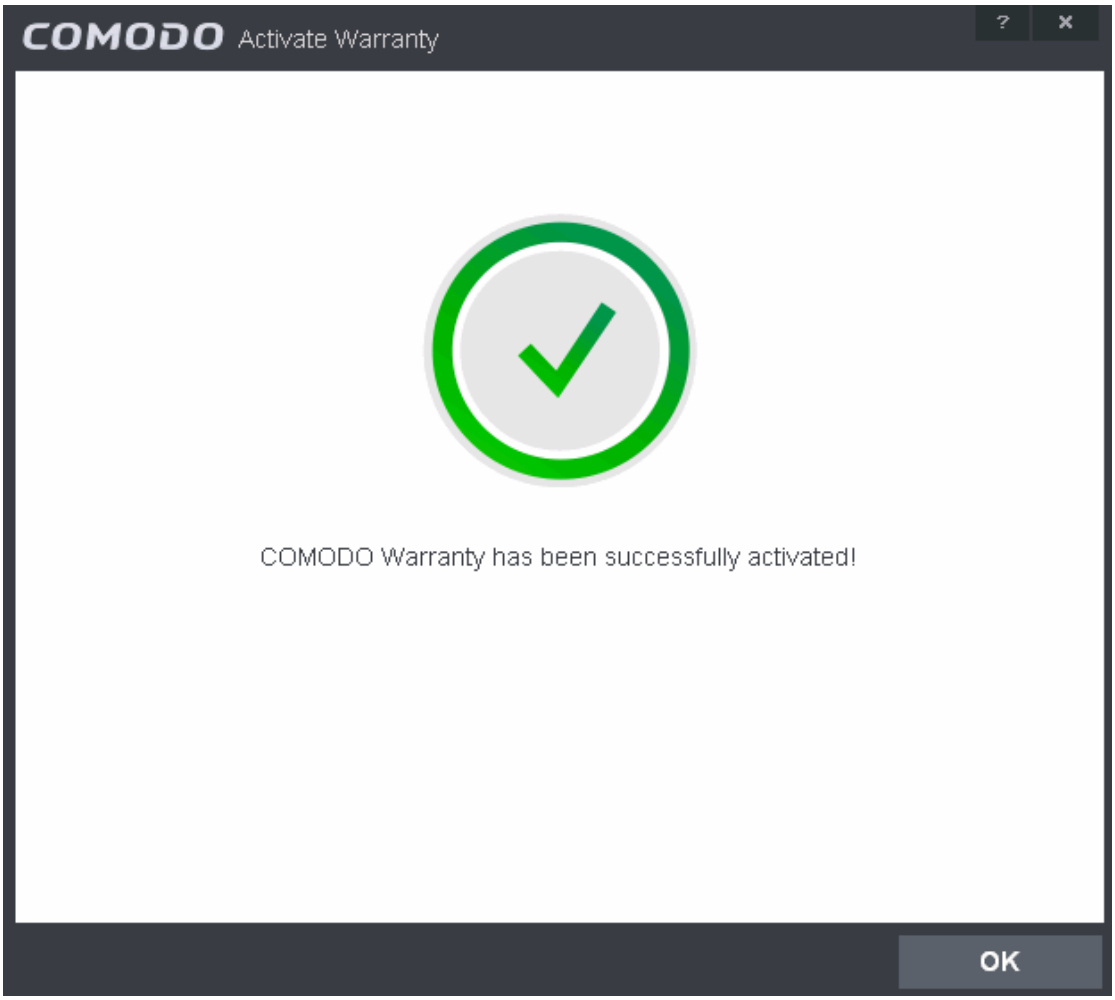


- Click 'Next'. The warranty will be activated...

Note: You must be connected to Internet for activating your warranty.

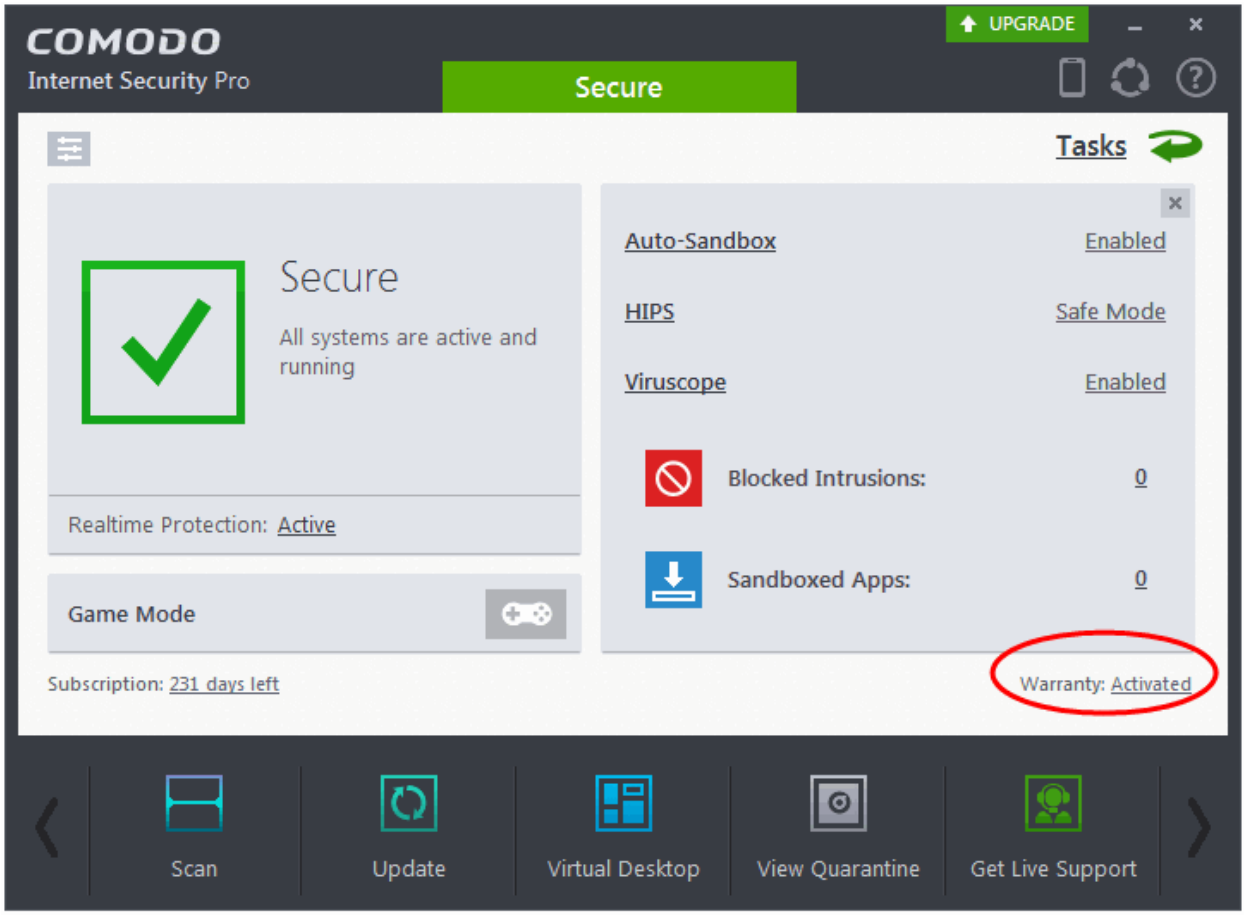


... and on completion, the 'successfully activated' screen will be displayed.

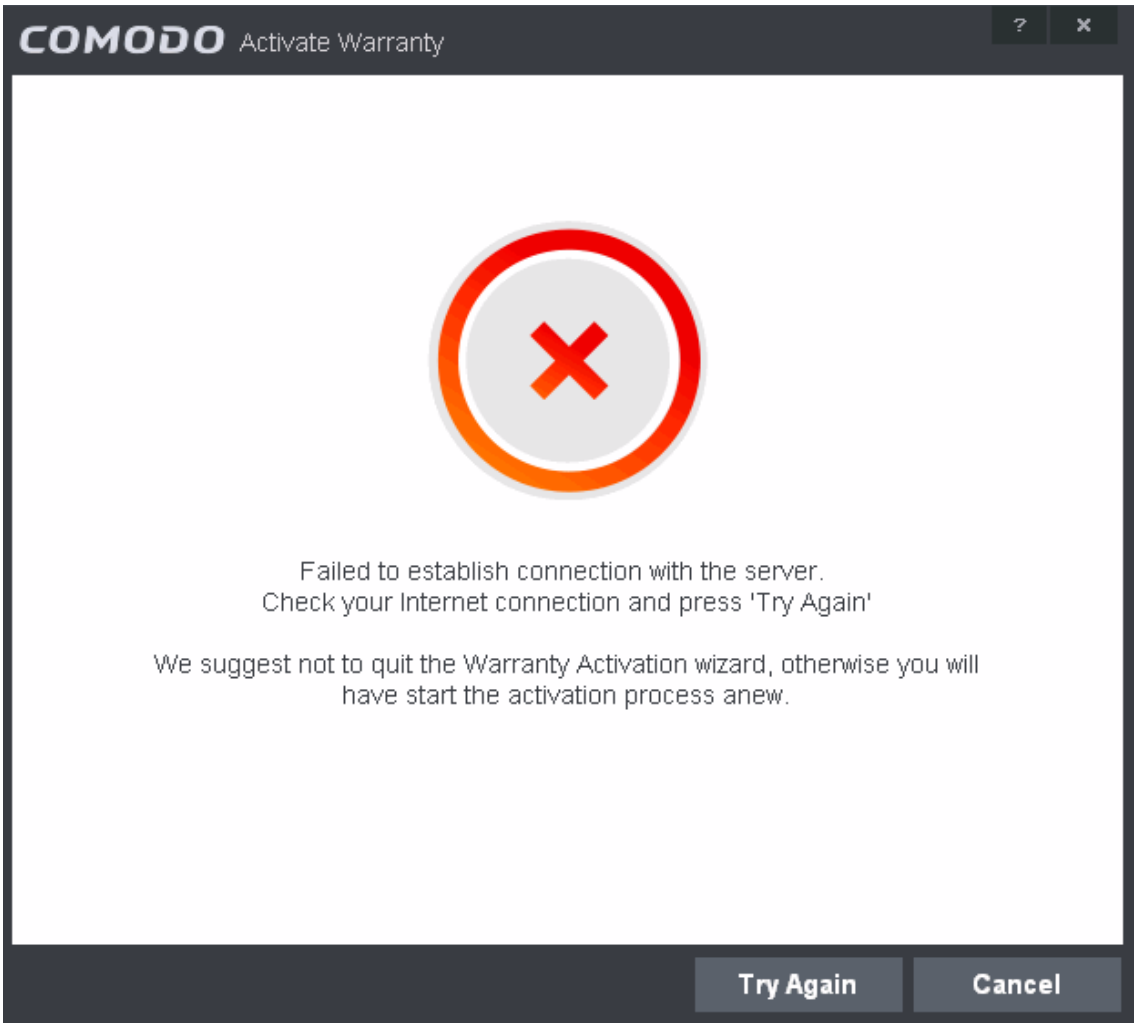


- Click 'Continue' to complete the activation wizard

Successfully activating your Guarantee will change the information displayed beside 'Warranty:' in the Home screen.


COMODO
Internet Security Pro
Secure
UPGRADE
Tasks
Secure
All systems are active and running
Realtime Protection: Active
Game Mode
Auto-Sandbox
Enabled
HIPS
Safe Mode
Viruscope
Enabled
Blocked Intrusions:
0
Sandboxed Apps:
0
Subscription: 231 days left
Warranty: Activated
Scan
Update
Virtual Desktop
View Quarantine
Get Live Support

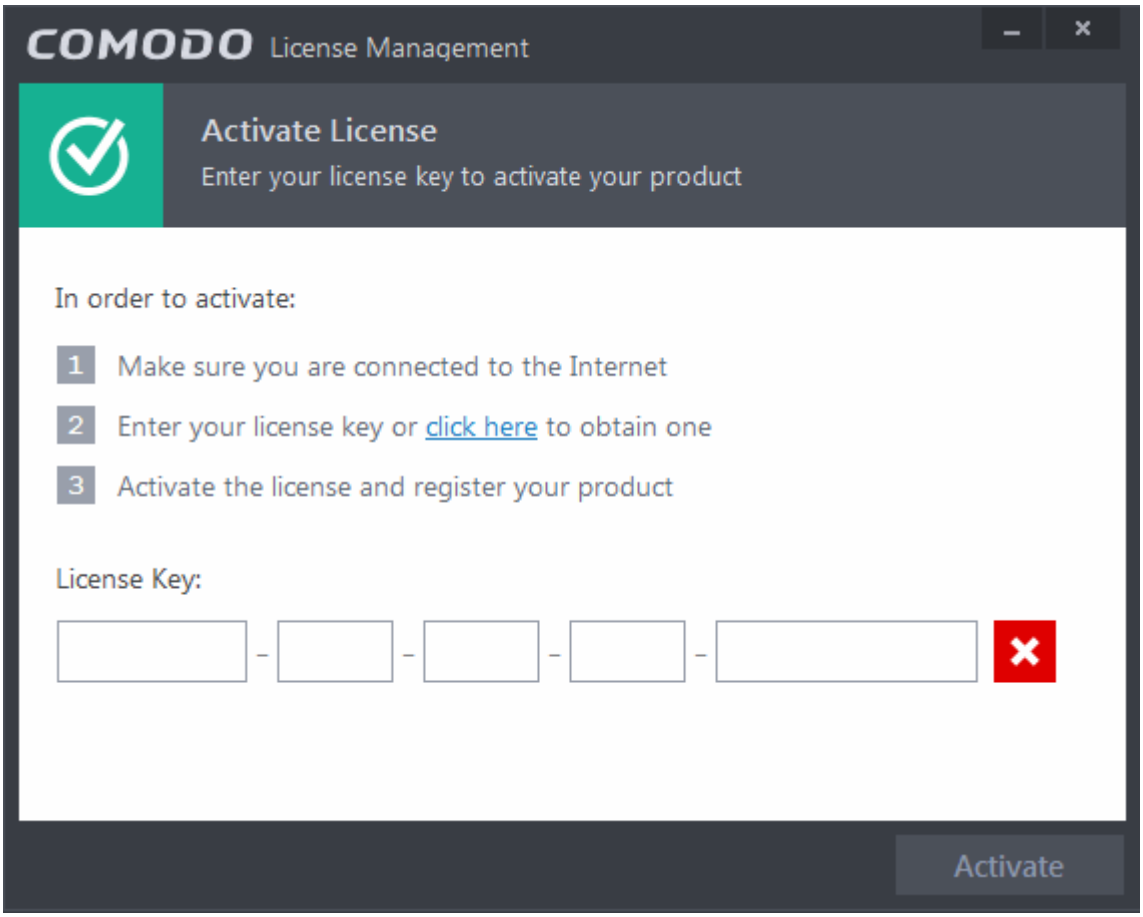
Note: Please ensure that you are connected to Internet during warranty activation. The activation wizard will check Comodo servers to validate your CIS Complete license key in order to activate the warranty. If you are not connected to Internet at the time of warranty activation, the wizard will not continue and a 'Activation Failed' dialog will appear. Check your Internet connection and try again.



1.3.4.3. Renewal of Your License

In order to enjoy continuous services from Comodo after the license period of your CIS Pro/Complete has expired, you need to renew your License.

To renew or upgrade your license, click the 'Activate Now' link beside 'Subscription' on the CIS home screen (alternatively, click 'No. of days left').



The Product Activation Wizard will start.

- Click the 'click here' link. You will be taken to **https://secure.comodo.com/home/purchase.php?afl=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUIzRkY&lid=&** .
- Select your CIS Package.
- Select 'returning user' in the 'Sign-up Information' area, enter your login and password and complete the payment procedures.
- The License key will be sent to you by email. **Activate your License** using the new key to enjoy the continued services.

1.4. Starting Comodo Internet Security

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

There are 4 different ways to open Comodo Internet Security:

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

Start Menu

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

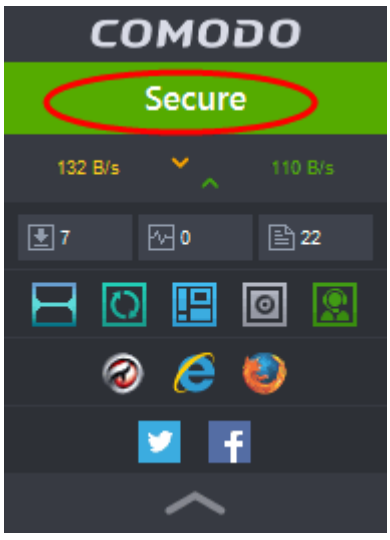
- Click **Start** and select **All Programs** > **Comodo** > **COMODO Internet Security** > **COMODO Internet Security.**

Windows Desktop

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

Widget

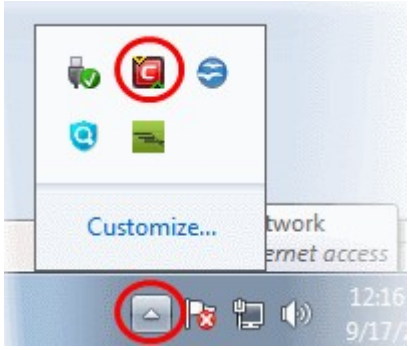
- Just click the information bar in the widget to start CIS.



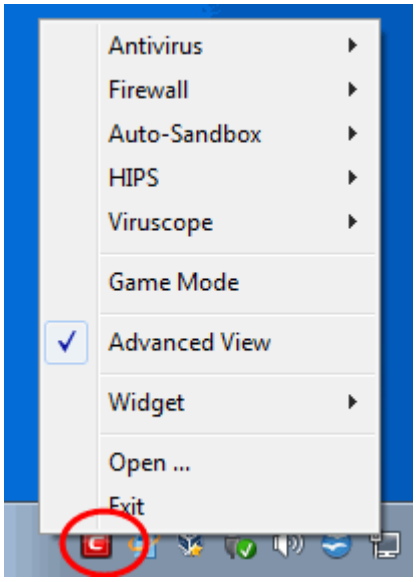
You can also view other details in the widget such as inbound and outbound traffic, number of tasks running, shortcuts to common CIS tasks and browsers and links to social media sites Twitter and Facebook. Refer to the section '**The Widget**' for more details.

CIS Tray Icon

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



Right-clicking the tray icon provides quick access to some important settings. These include settings related to the antivirus, Firewall, Auto-Sandbox, HIPS, Viruscope, Game Mode options and more.



Game Mode - Switches CIS to Game Mode to enable you to play your games without any interruptions from various alerts in your computer. The operations that can interfere with users' gaming experience are either suppressed or postponed.

In game mode:

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

Deactivate Game Mode to resume alerts and scheduled scans.

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

Refer to the section "**The System Tray Icon** for more details.

1.5. The Main Interface

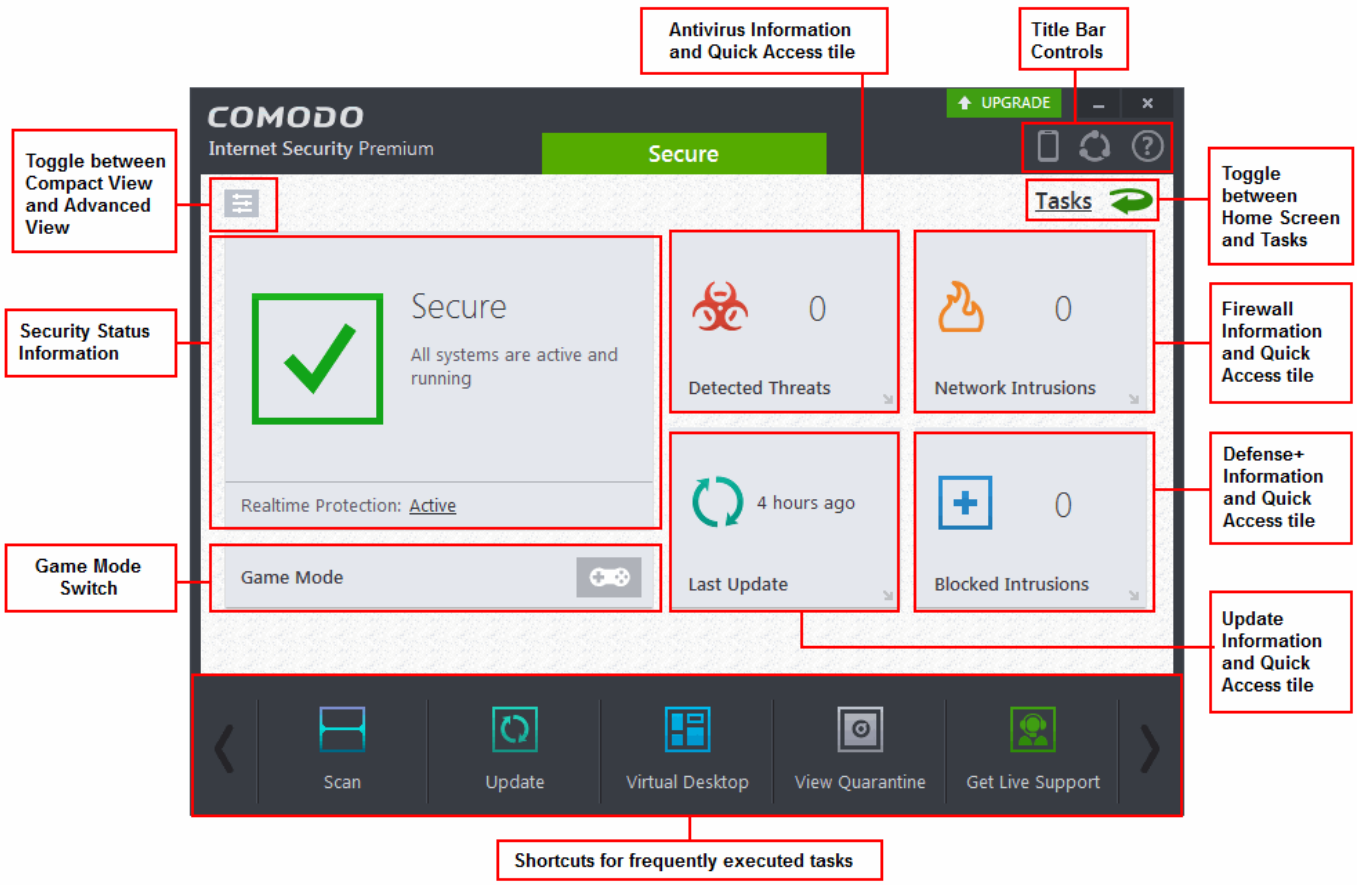
The CIS interface is designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.

The CIS graphical user interfaces depend on the theme selected. There are four different themes that you can choose from and by default CIS is shipped with Flat Tile Theme. Refer to the section **Customize User Interface** for more details.

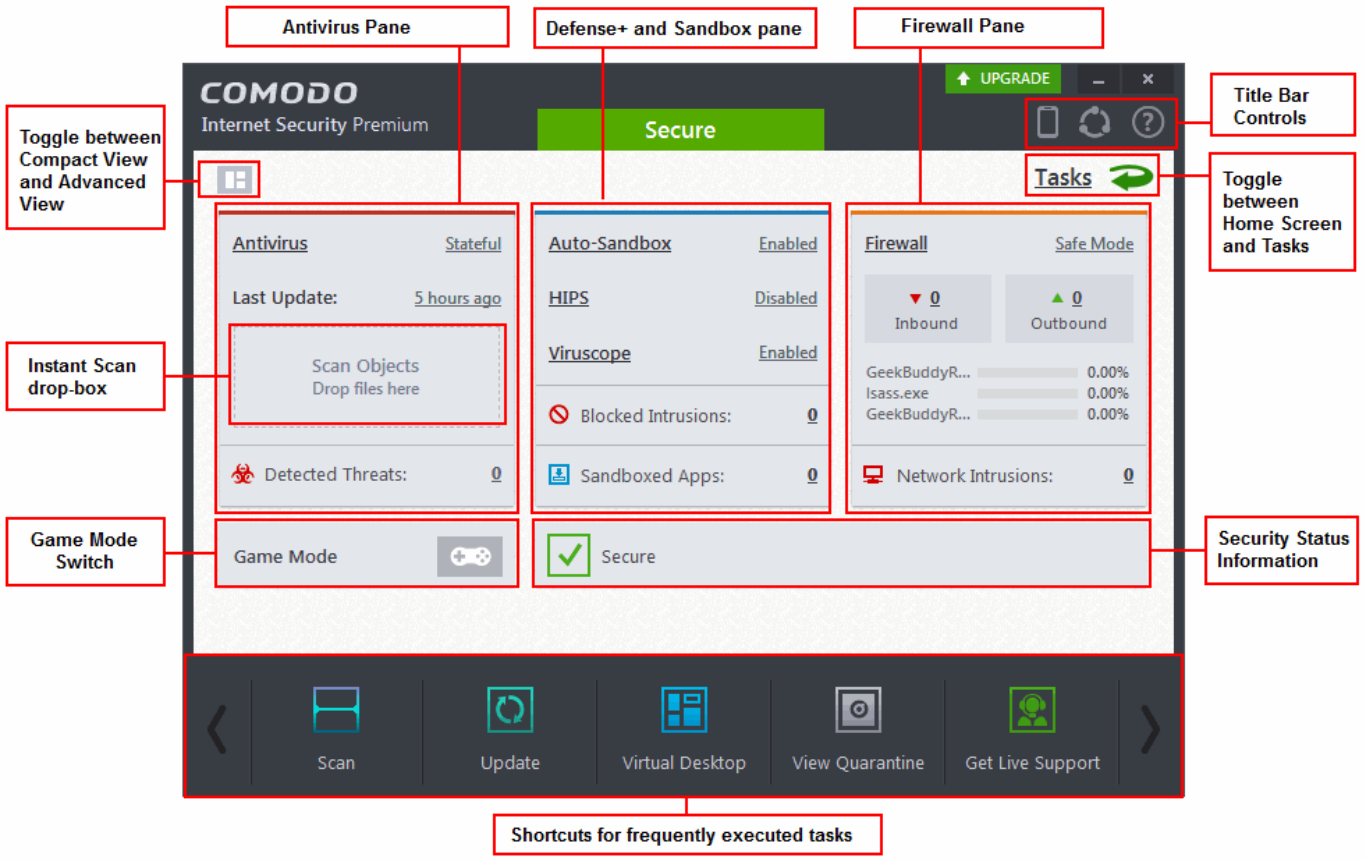
- Click the curved arrow at the upper right to switch between the **home screen** and the **tasks interface**
- Instantly run a virus scan on a file or folder by dragging it into the scan box.
- Switch on 'Game Mode' to make sure nothing interrupts you while you play a full screen game.

- Change the entire look and feel of the home screen from **Advanced Settings**.
- The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the Virtual Desktop, the update checker and the CIS Task Manager.
- The 'Upgrade' button allows Premium users to upgrade to CIS Pro or Complete.
- Flip between 'Compact View' and 'Advanced View' by using the toggle button at the upper left or from the system tray icon

Compact View



Advanced View



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

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

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 the display between the 'Home' screen and the 'Tasks' interface by clicking the green arrow at the upper right of the interface: 

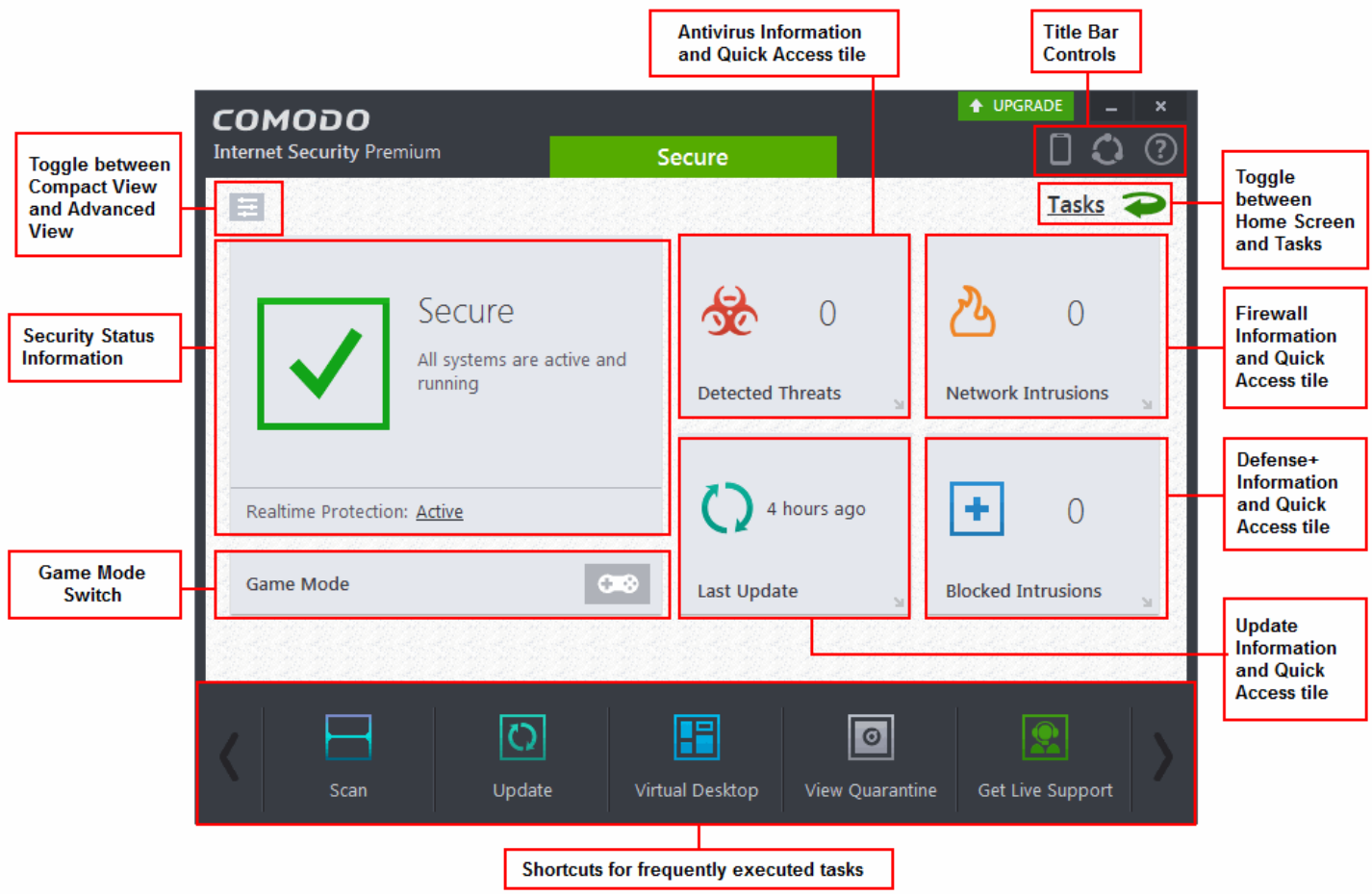
The home screen itself is available in two formats, **'Compact' view** and **'Advanced' view.** Use the button at the top-left to switch between them. 

The following areas are common to both compact and advanced views:

- **Adding tasks to the Task Bar**
- **Title bar controls**
- **Game mode**

Compact View

Compact View presents a simple, easy to understand interface that allows users to quickly launch key tasks and gain an immediate overview of the security of their computer. The large 'security information' tile on the left provides at-a-glance information on overall system security and allows you to run an appropriate CIS task if threats are found. The four tiles on the right provide information from specific CIS security components and act as shortcuts to run an instant antivirus scan, run an update, view network traffic and to configure sandbox/host intrusion settings.



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

You can easily rectify the issue by clicking the 'Fix it!' button. CIS will automatically take necessary actions to resolve the problem.

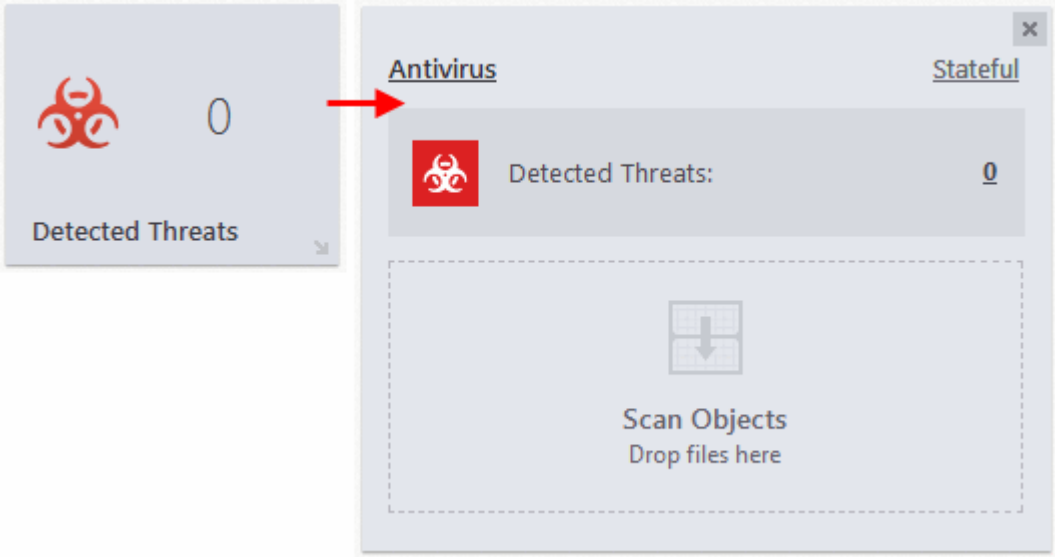
From the Compact View of the home screen you can:

- **Instantly scan objects**

- **Enable or disable security components**

Instantly scan objects

Click the 'Antivirus' tile in the middle of the (compact) home screen to open the drag-and-drop scanner:

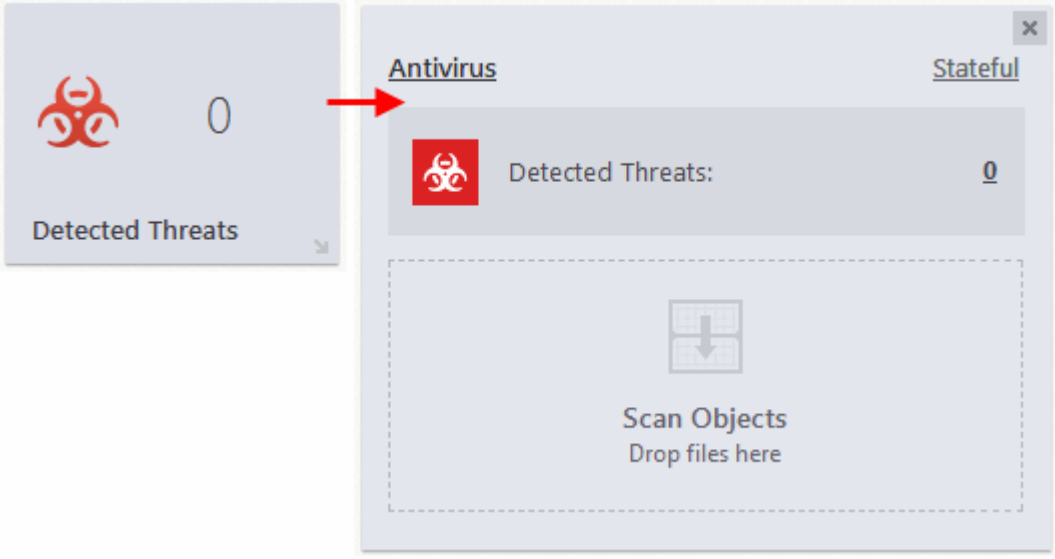


To run an instant scan, navigate to the file/folder that you want to scan and just drag-and-drop the file into the 'Scan Objects' box. The virus scan will commence immediately. Refer to '**Instantly Scan Individual Files and Folders**' for more details.

Enable or disable security components

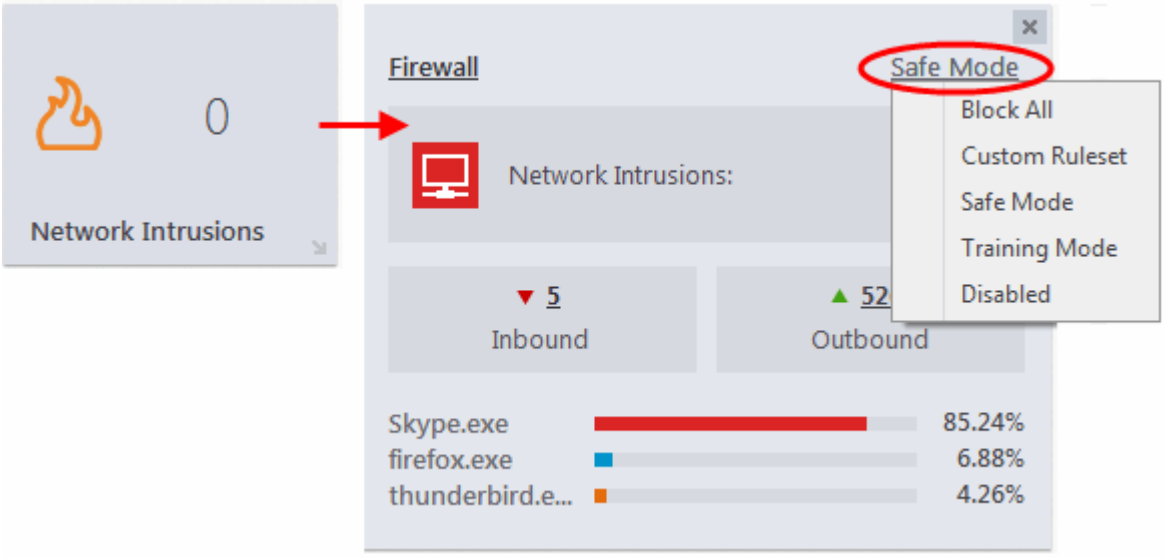
The four tiles on the right can each be flipped to display more detailed information and options

- **Antivirus** - Click the 'Detected Threats' tile to flip open a more detailed tile which displays current antivirus settings, the number of detected threats and the drag-and-drop scanner.
  - Click the link at the top-right to quickly switch AV modes between 'On Access', 'Stateful' and 'Disabled'. Refer to the section '**Real-time Scanner Settings**' for more details.

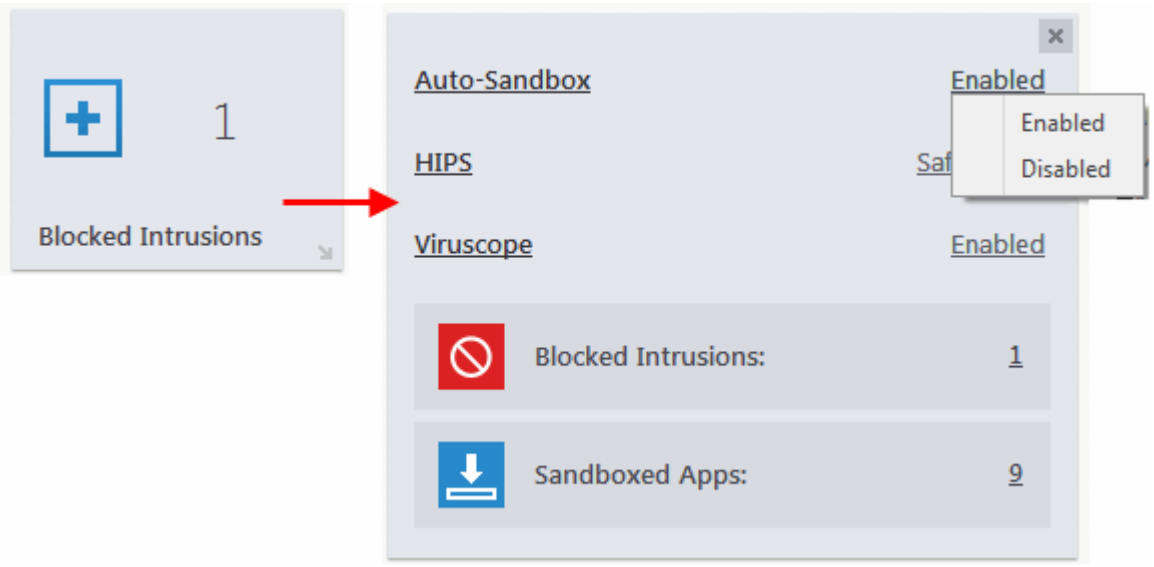


  - Click 'Antivirus' at upper-left to open the 'Realtime Scanner Settings' interface. Refer to the section '**Real-time Scanner Settings**' for more details.
  - Click the number of threats detected to open the **Antivirus Log Viewer Module**.
  - Click the 'X' in the top right corner to return to the 4-tile view.

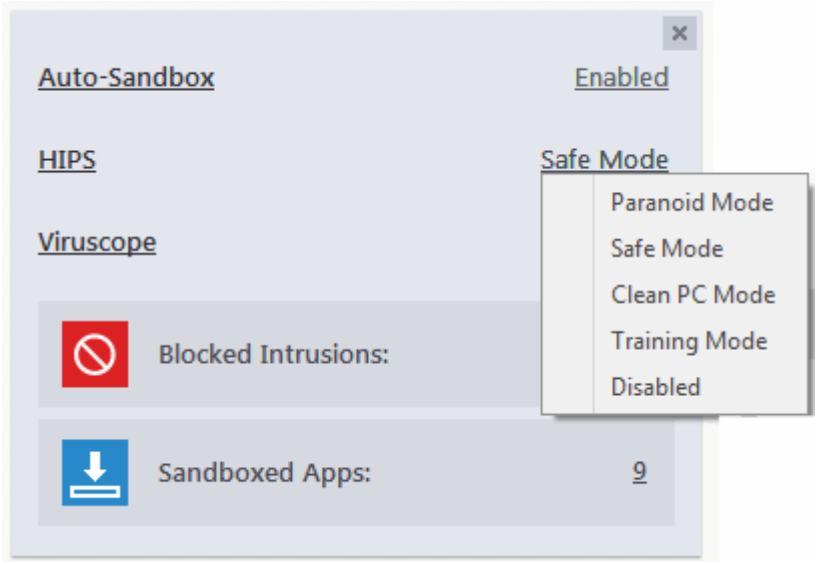
- **Firewall** - Click the 'Network Intrusions' tile to flip open a more detailed pane which displays the current firewall mode, the number of detected network intrusions, the number of current inbound and outbound connections and the share of network bandwidth used by internet-connected applications.
    - Click the link at the top-right to view or modify the current firewall mode. Refer to the section '**Firewall Settings**' for more details.



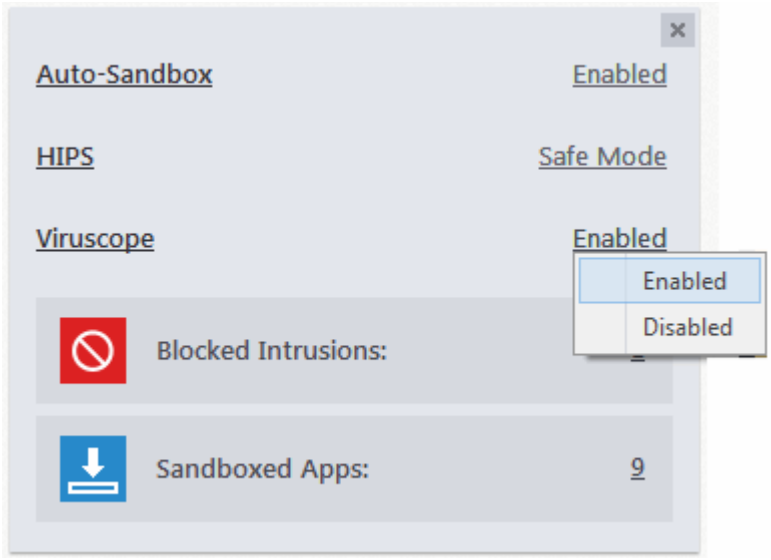
    - Click 'Firewall' to open the detailed 'Firewall Settings' interface. Refer to the section '**Firewall Settings**' for more details.
    - Click the number of detected network intrusions to open the **Firewall Log Viewer Module**.
    - Click the numbers over 'inbound' and 'outbound' to open the **View Connections** dialog. You can also do this by clicking the application names at the bottom of the pane.
    - Click the 'X' in the top right corner to return to the 4-tile view.
- **Defense+** - Click the 'Blocked Intrusions' tile to flip open a more detailed pane which displays the current Auto-Sandbox and HIPS modes and a statistical summary of events handled by Defense+.
    - Click **Auto-Sandbox** to open the Auto-Sandbox Rules Settings interface. Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details.
    - Click the link to the right of this to view and modify auto-sandbox security levels. Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details.



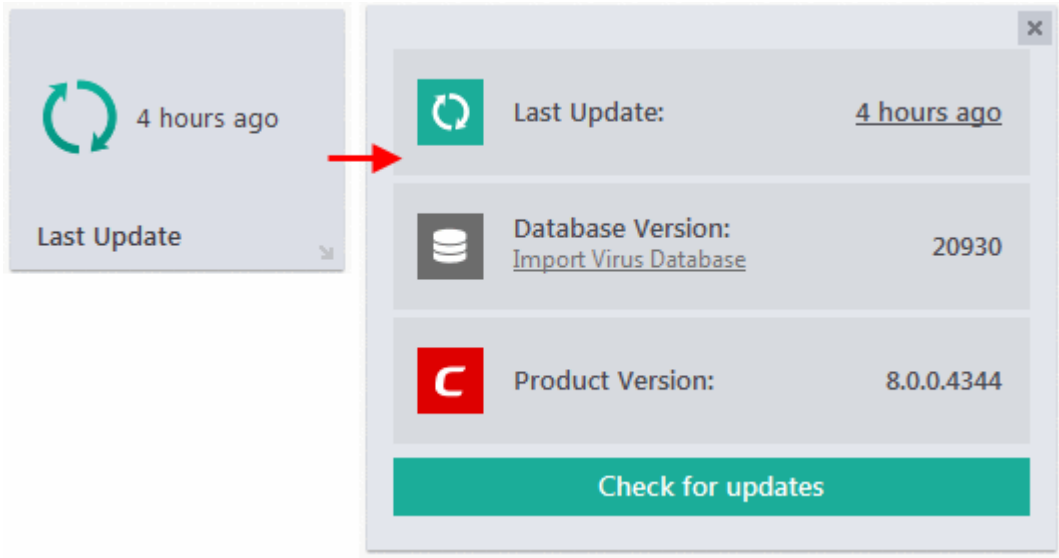
    - Click **HIPS** to open the 'HIPS Settings' interface. Refer to the section '**HIPS Settings**' for more details.
        - Click the link to the right of this to view and modify HIPS security modes. Refer to the section '**HIPS Settings**' for more details.



- Click **Viruscope** to open the 'Viruscope' interface. Refer to the section '**Viruscope**' for more details.
  - Click the link to the right of this to view and modify Viruscope security modes. Refer to the section '**Viruscope**' for more details.



  - Click the number of Blocked Intrusions to open the **Defense+ Log Viewer** module.
  - Click the number of Sandboxed Apps to open the **Active Process List** dialog.
- **Updates** - Click the 'Updates' tile to open a more detailed pane which displays when the virus database was last updated, the database version number and the software version number.

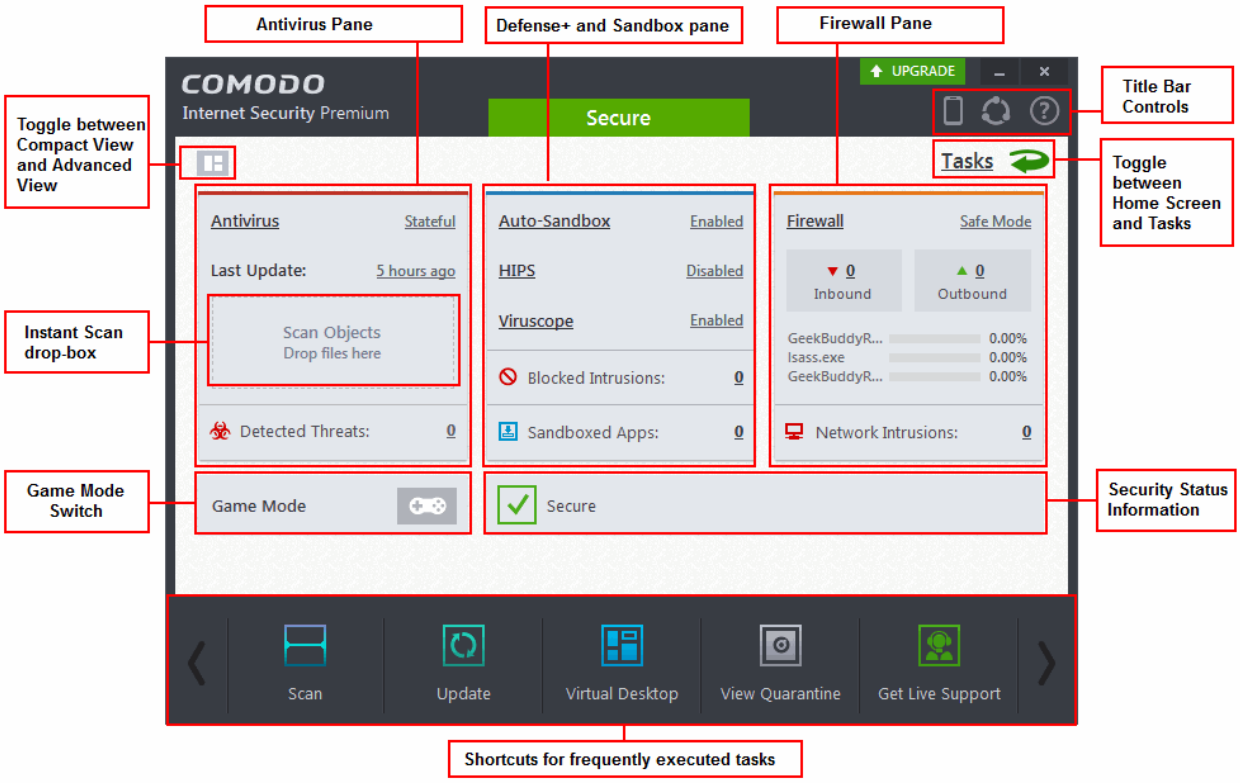


- Click on either the time of the last update or the 'Check for Updates' button to manually check for available updates. Refer to the section **Manage Virus Database and Product Updates** section for more details.
- Click the 'X' in the top right corner to return to the 4-tile view.

Advanced View

The 'Advanced View' provides a more finely-detailed view of the security status of each of the Antivirus, Defense+ and Firewall components.

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



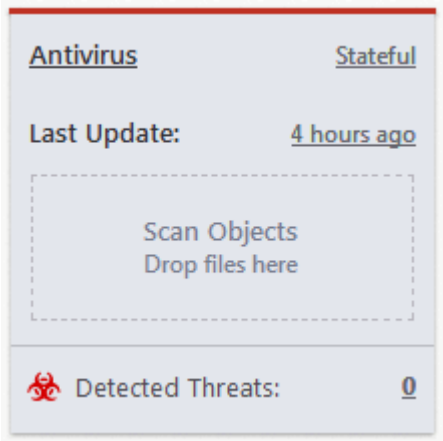
Click the following links to find out more:

- **Antivirus Pane**
- **Defense+ and Sandbox Pane**

- **Firewall Pane**

Antivirus Pane

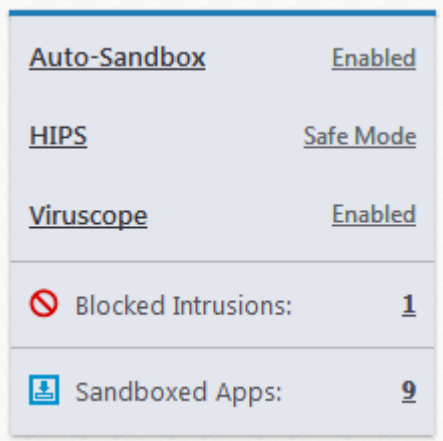
The Antivirus pane allows you to configure antivirus mode, see when the virus database was last updated, view antivirus logs and instantly scan files and folders.



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

Defense+ and Sandbox Pane

The Defense+ and Sandbox Pane allows you to quickly configure Auto-Sandbox and HIPS settings, view Defense+ logs and easily view the number of blocked intrusions, unrecognized files and sandboxed applications.

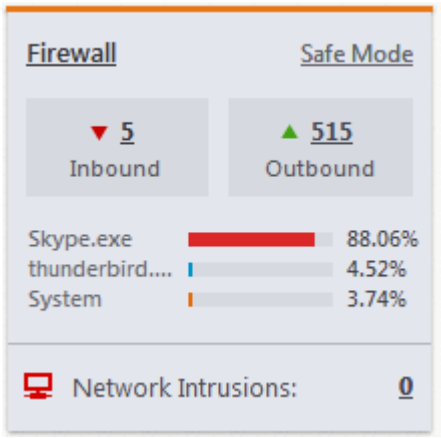


- **Auto-Sandbox** - Displays whether auto-sandbox feature is enabled or not. Click on the security level itself to change it. Click **Auto-Sandbox** to open the 'Auto-Sandbox Settings interface.' Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details.
- **HIPS** - Click the text of the current HIPS mode to view or modify the mode. Click the word HIPS to open the 'HIPS Settings' interface. Refer to the section '**HIPS Settings**' for more details.
- **Viruscope** - Displays whether Viruscope is enabled or not. Click on the security level to change it. Click **Viruscope** to open the 'Viruscope' interface. Refer to the section '**Viruscope**' for more details.

- **Blocked Intrusions** - Displays the number of intrusions blocked by HIPS. Clicking on the numbered link will open the Defense+ logs. Refer to the section **Defense+ Logs** for more details.
- **Sandboxed Apps** - Displays the number of applications that are currently running inside the sandbox. Clicking the numbered link beside it will open the 'Active Processes List (Sandboxed Only)', which provides details of currently sandboxed applications. Refer to the section '**View Active Process List**' for more details.

Firewall Pane

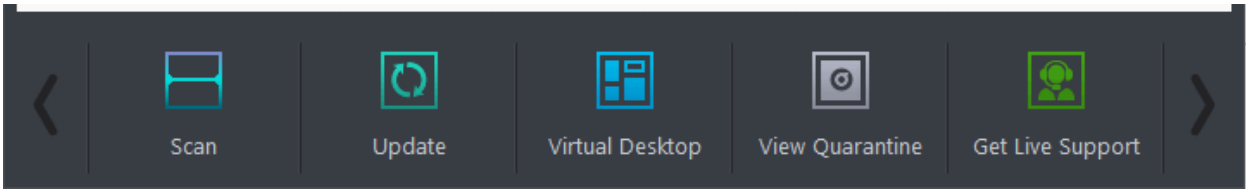
The Firewall Pane allows you to configure Firewall settings, view the number of inbound and outbound connections and the number of network intrusion attempts blocked by Firewall since the start of current session of CIS.



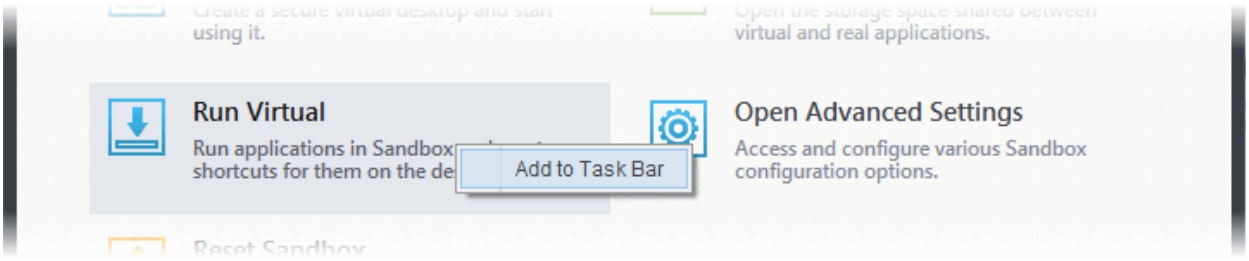
- **Firewall** - Displays the firewall's current security mode. Click on the level itself to quickly view and modify it. Click on '**Firewall**' to open the Firewall Settings interface. Refer to the section '**Firewall Settings**' for more details.
- **Inbound / Outbound Connections** - A numerical summary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

Adding tasks to the Task Bar

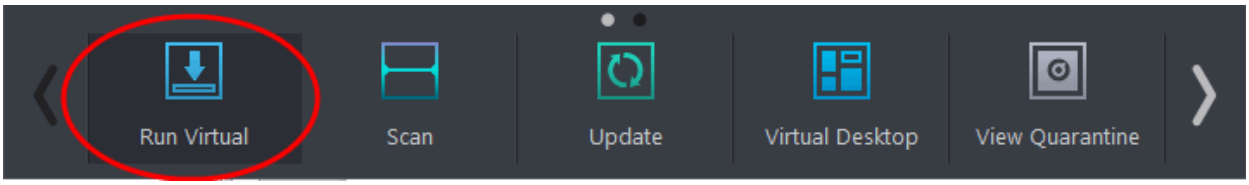
The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles < > on the left and right sides of the task bar to scroll through all tasks.



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

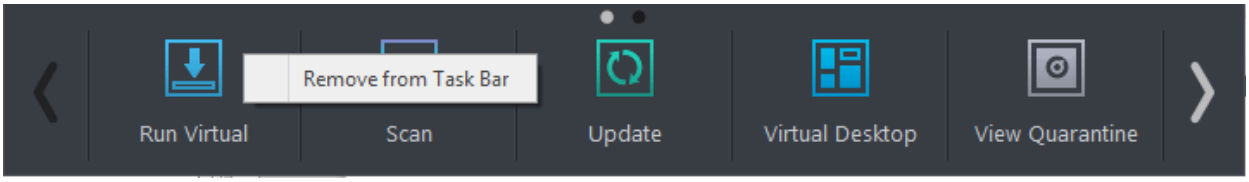


- The selected task will be added to the Task Bar.



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

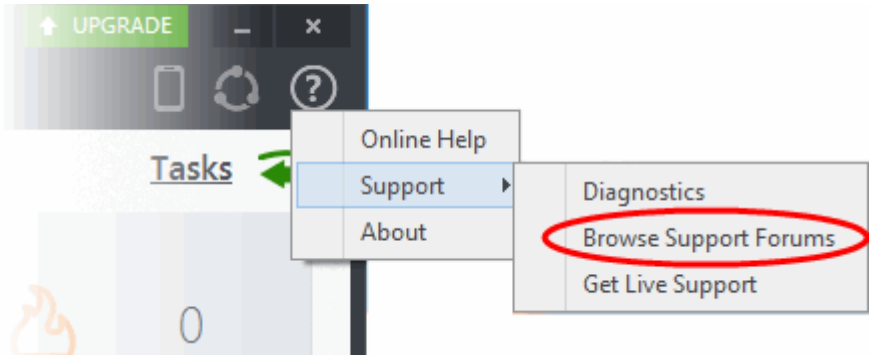
- To remove a task shortcut from the Task Bar, right click on it and choose 'Remove from task bar'.



Title bar controls

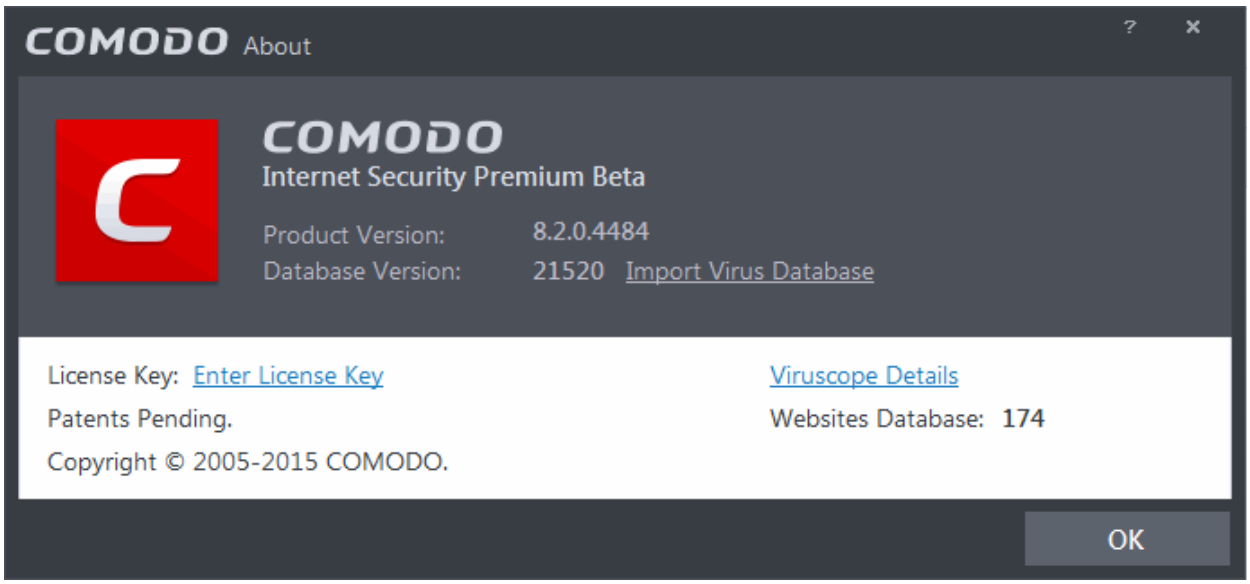
The title bar (top right) contains shortcuts for:

- Comodo Mobile Security app for Android phones and tablets. - Click the mobile icon and scan the QR code with your device to download the latest version of the app. You can also get the app from our website, **https://m.comodo.com/** or from the Google Play app store at **https://play.google.com/store/apps/details?id=com.comodo.pimsecure**
- Refer your Friends - Click the icon to open the 'Comodo Friends' website. Register an account for free, recommend CIS to your friends and get attractive rewards. Visit **http://friends.comodo.com/** for more details.
- Get Help - Click the help icon for the following options:



- Online Help - Opens Comodo Internet Security's online help guide at **http://help.comodo.com/topic-72-1-522-6207-Introduction-to-Comodo-Internet-Security.html**.

- Support - Click this link for the following options:
- Diagnostics - Helps to identify any problems with your installation.
  - Browse Support Forum - Links to **Comodo User Forums**.
  - Get Live Support - Launches the **GeekBuddy** support client.
- **About** - Displays the product version, virus signature database version, website database version (website filtering URLs), details of active Viruscope Recognizers and copyright information. The 'About' dialog also allows you to import a locally stored virus database and to enter a license key for CIS Pro.



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

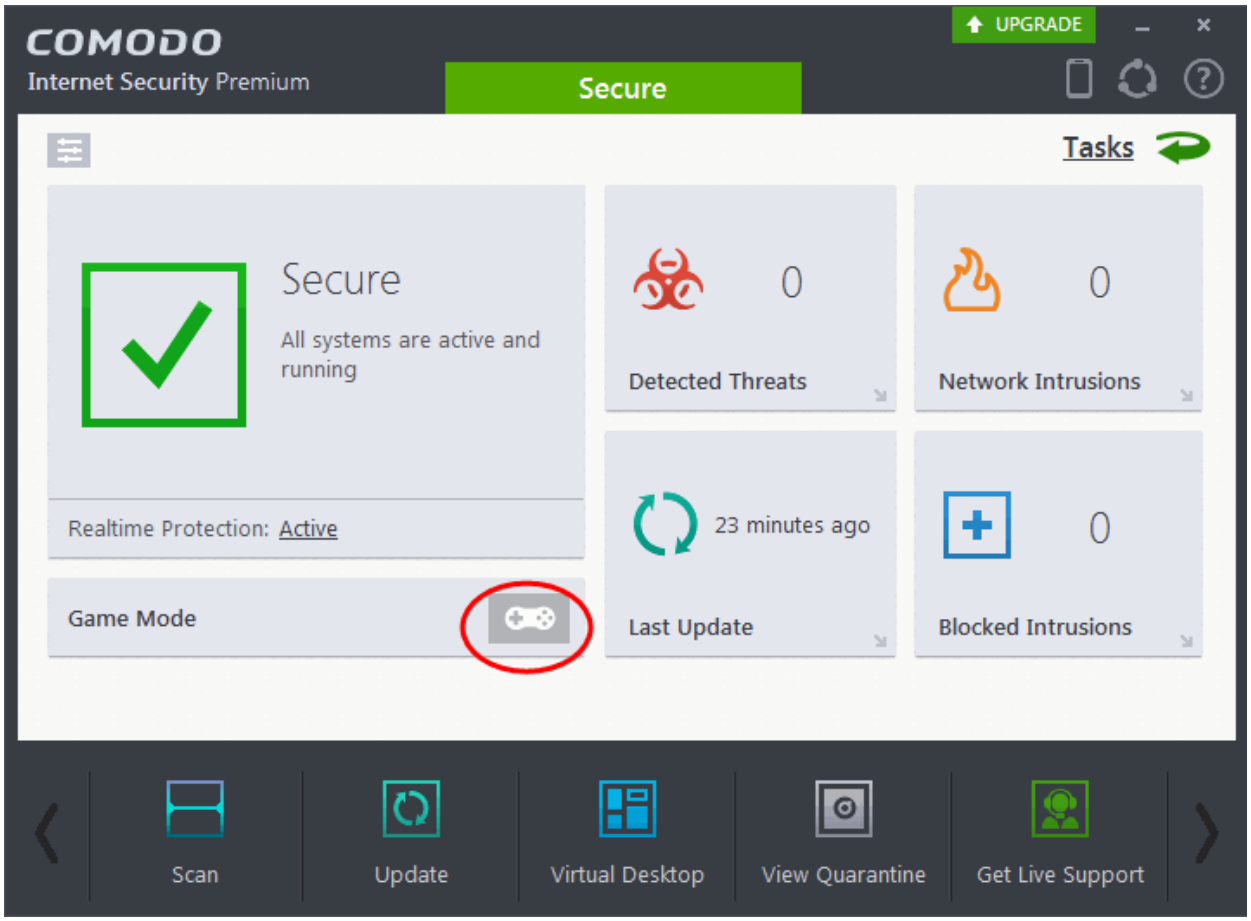
Game mode

Game Mode enables you to play your games without interruptions or alerts. Operations that can interfere with a user's gaming experience are either suppressed or postponed.
In game mode:

- Defense+/Firewall alerts are suppressed.
- AV database updates and scheduled scans are postponed until the gaming is over;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

To switch to Game mode

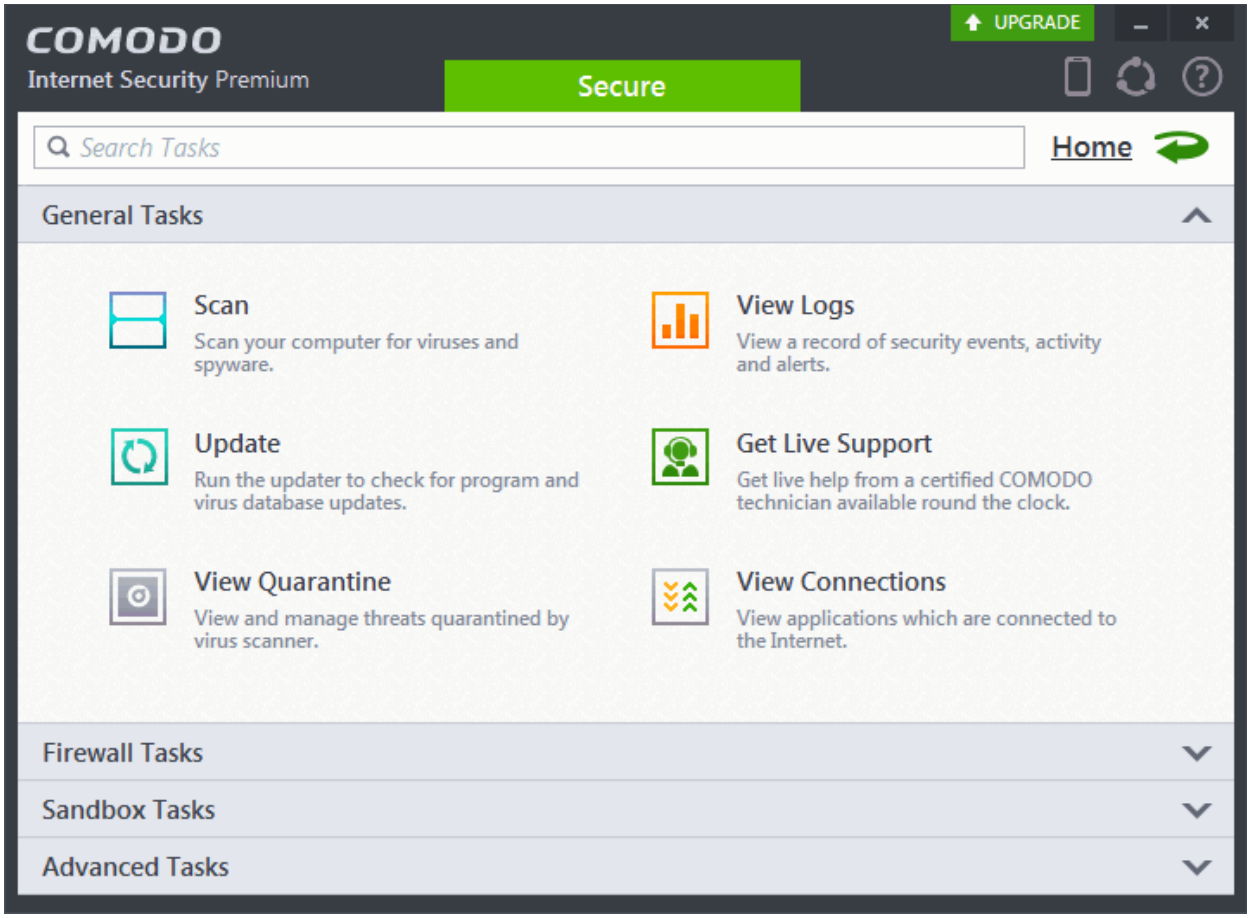
- Click the Game Mode switch at the bottom left of the Home Screen



- Deactivate Game Mode to resume alerts and scheduled scans.

1.5.2. The Tasks Interface

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



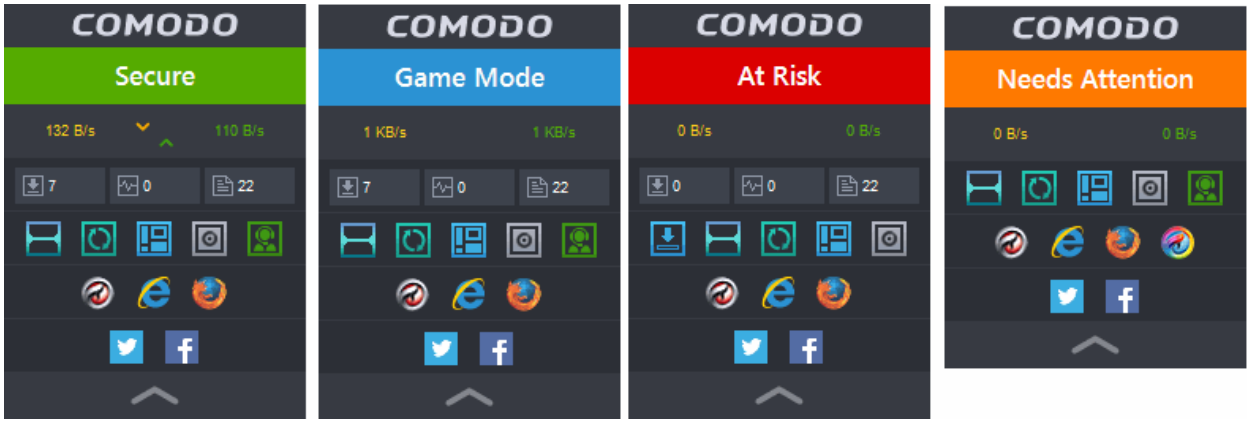
Tasks are broken down into four main sections. Click the following links for more details on each:

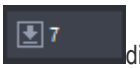
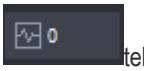
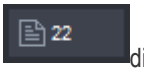
- **General Tasks** - Run antivirus scans, update virus database, view and manage quarantined threats, view logs of security events, activity and alerts and get live support. Refer to the section **General Tasks** for more details.
- **Firewall Tasks** - Allow or block applications, manage ports, manage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

1.5.3. The Widget

The CIS Widget is a handy control that lives on your desktop and provides at-a-glance information about the security status, number of tasks running and shortcuts to common tasks. The Widget starts automatically with CIS unless it is disabled from the **System Tray Icon** or in the '**User Interface**' of **General Settings**.

Right clicking on the Widget opens a context sensitive menu similar to the one displayed when you right click on the CIS system tray icon. The context sensitive menu allows you to enable or disable CIS components and configure various settings. Refer to section **The System Tray Icon** for more details.

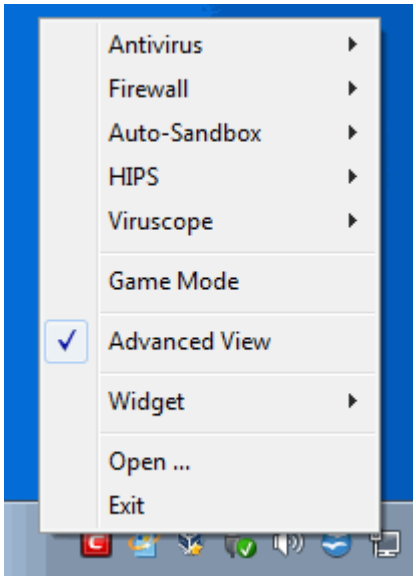


- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' opens the appropriate interface for you to take action immediately.
- The second row displays information about incoming and outgoing network traffic. The network traffic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

  The status row is displayed only if 'Show Status Pane' is enabled. Check this by right clicking the tray icon or the widget itself and look under 'Widget' options. Refer to **The System Tray Icon** for more details. (***Default = Disabled***)
- The forth row contains shortcuts for the five common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task. The 'Common Tasks' row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of the CIS tray icon or the widget right-click menu. Refer to **The System Tray Icon** for more details. (***Default = Enabled***)
- The fifth row displays the browsers installed on your computer. Clicking on a browser icon will open the browser inside the sandbox for a secure browsing session. You can tell the browser is running in the sandbox because it will have a green border around it. Refer to **Running an application inside the sandbox** for more details. The 'Browsers' row is displayed only if 'Show Browsers Pane' is enabled under the 'Widget' section of the CIS tray right-click menu. This can also be viewed by right-clicking the widget itself. Refer to **The System Tray Icon** for more details. (***Default = Enabled***)
- The last row on the widget provides links to social networking sites. This row is displayed only if 'Show Connect Pane' is enabled. To check this setting, right-click on the CIS tray icon and look at the 'Widget' section. Alternatively, right-click the widget itself. Refer to **The System Tray Icon** for more details. (***Default = Enabled***)
- You can expand or collapse the Widget by clicking the arrow at the bottom.

1.5.4. The System Tray Icon

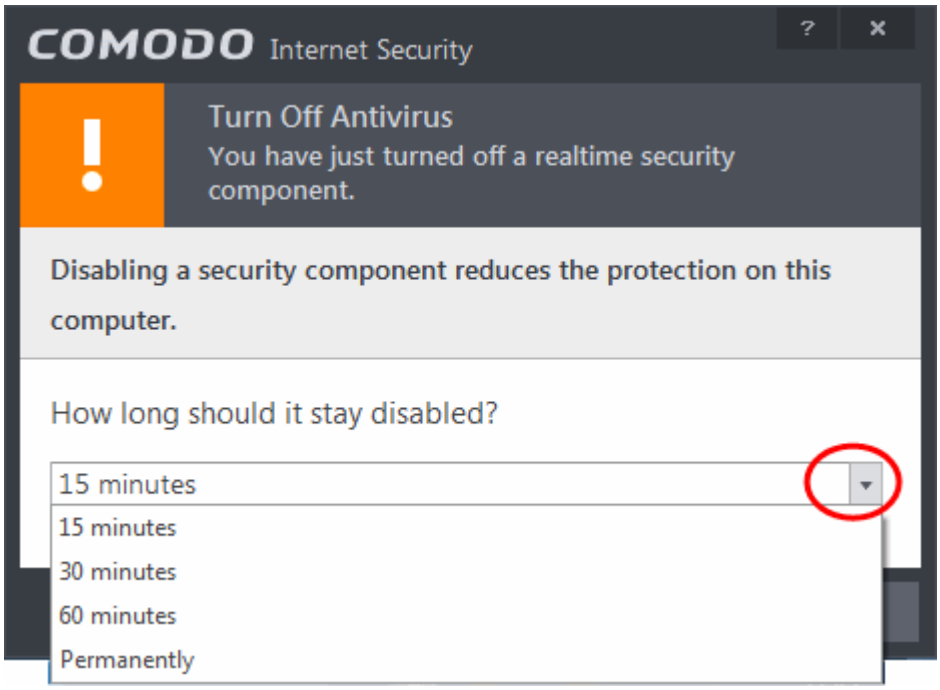
Double-clicking the system tray icon will quickly open the CIS interface. Right-clicking the icon opens a context sensitive menu that allows you to configure various application settings:



The options available for the Antivirus, Firewall and Auto-sandbox menu-items depend on whether you are using **Compact View** or **Advanced View**.

Compact View	Advanced View
Antivirus - You can enable or disable Real-time antivirus scan. **Auto-Sandbox** - You can enable or disable Auto-Sandbox. Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details. **Firewall** - You can enable or disable Firewall.	**Antivirus** - Options available are On Access, Stateful and Disabled. Refer to **Antivirus Pane** for more details. Clicking Settings from the options will open the Realtime Scanner Settings interface. Refer to the section '**Real-time Scanner Settings**' for more details. **Auto-Sandbox** - You can enable or disable Auto-Sandbox settings. Clicking Settings from the options will open the Auto-Sandbox settings interface. Refer to the section **Configuring Rules for Auto-Sandbox** for more details. **HIPS** - Options available are Paranoid Mode, Safe Mode, Clean PC Mode, Training Mode and Disabled. Clicking Settings from the options will open the HIPS Settings interface. Refer to the section **HIPS Settings** for more details. **Viruscope** - Options available are Enabled, Disabled. Clicking Settings from the options will open the Viruscope interface. Refer to the section **Viruscope** for more details. **Firewall** - Options available are Block All, Custom Ruleset, Safe Mode, Training Mode and Disabled. Refer to the section '**Firewall Settings**' for more details. Clicking Settings from the options will open the Firewall Settings interface. Refer to the section **Firewall Settings** for more details.

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



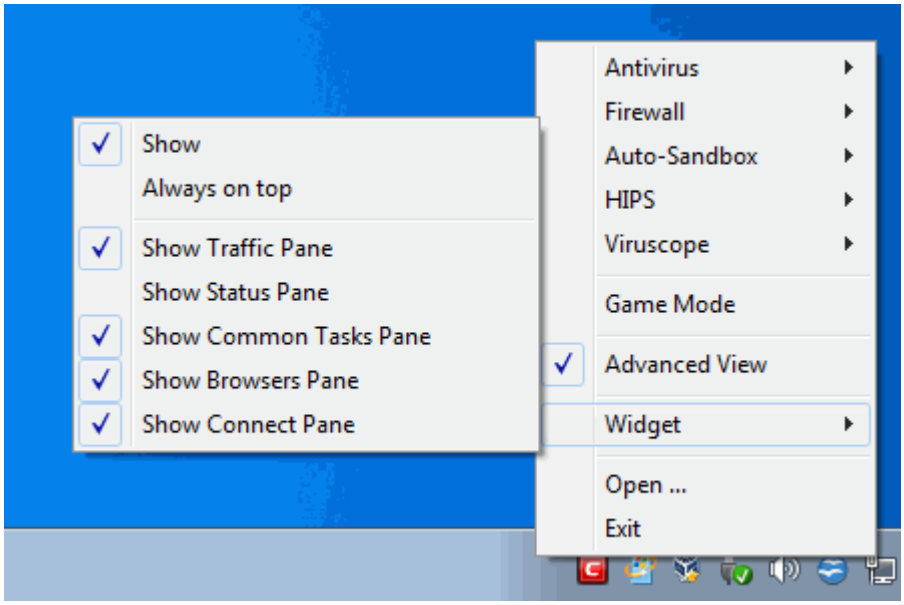
Select the period and click 'OK'. Unless you have selected 'Permanently', the security component will be automatically re-enabled after the stated time period has elapsed. You can, of course, manually re-enable at any time by right-clicking the tray icon and selecting 'Enable' for the component in question.

- **Game Mode** - Switches CIS into Game Mode so you can play your games without any interruptions from various alerts in your computer. Operations that can interfere with the gaming experience are either suppressed or postponed.

  In game mode:
  - Defense+/Firewall alerts are suppressed.
  - AV database updates and scheduled scans are postponed until the gaming is over;
  - Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Game Mode to resume alerts and scheduled scans.

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



- **Show**: Toggles the widget on or off (***Default = Enabled***)

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

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

1.6. Understanding Security Alerts

Alerts Overview

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

Alert Types

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

- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when **Antivirus is enabled** and the option '**Do not show antivirus alerts**' is disabled in **Real-time Scanner Settings**.
- **Firewall Alerts** - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the **Firewall is enabled** and the option '**Do not show popup alerts**' is disabled in **Firewall Settings**.
- **HIPS Alerts** - Shown whenever an application attempts an unauthorized action or tries to access protected areas. HIPS alerts will only be generated if **HIPS is** enabled and **Do NOT show popup** alerts is disabled.
- **Sandbox Alerts** (including **Elevated Privilege Alerts**) - Shown whenever an application tries to modify operating system or related files and when the Defense+ automatically sandboxes an unrecognizable file. Sandbox Alerts will be displayed only if privilege elevation alerts **is enabled** under under **Sandbox Settings**.
- **Viruscope Alerts** - Shown whenever a currently running process attempts to take suspicious actions. Viruscope alerts allow you to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. Viruscope Alerts will be displayed only when **Viruscope is enabled** under Defense+.

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

Note: This section is concerned only with the security alerts generated by the Antivirus, Firewall, HIPS and Auto-Sandbox components of CIS. For other types of alert, see **Comodo Message Center notifications**, **Notification Messages** and **Information Messages**.

Severity Level

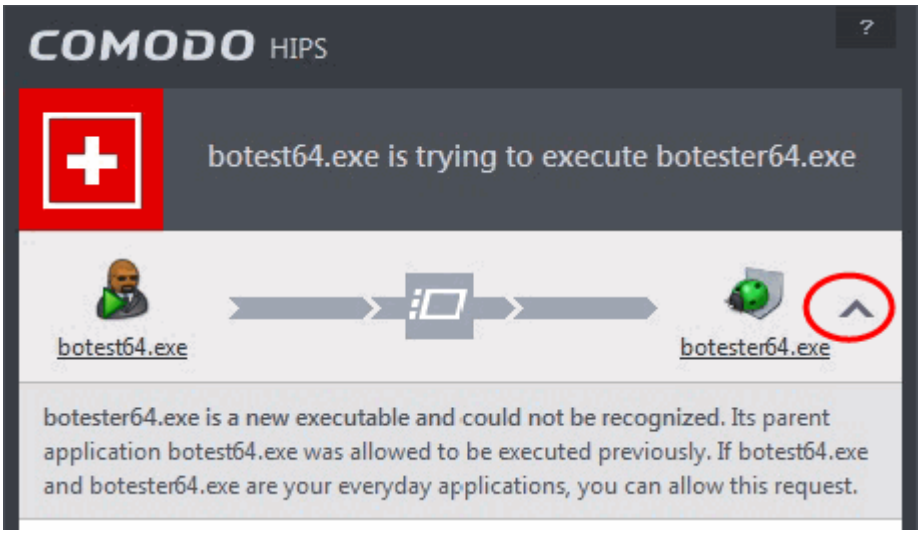
The shield icons at the upper left of each alert are color coded according to the risk level presented by the activity or request. However, it cannot be stressed enough that you should read the entire alert before reaching a decision on whether to allow or block the alert.

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

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

Alert Description

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



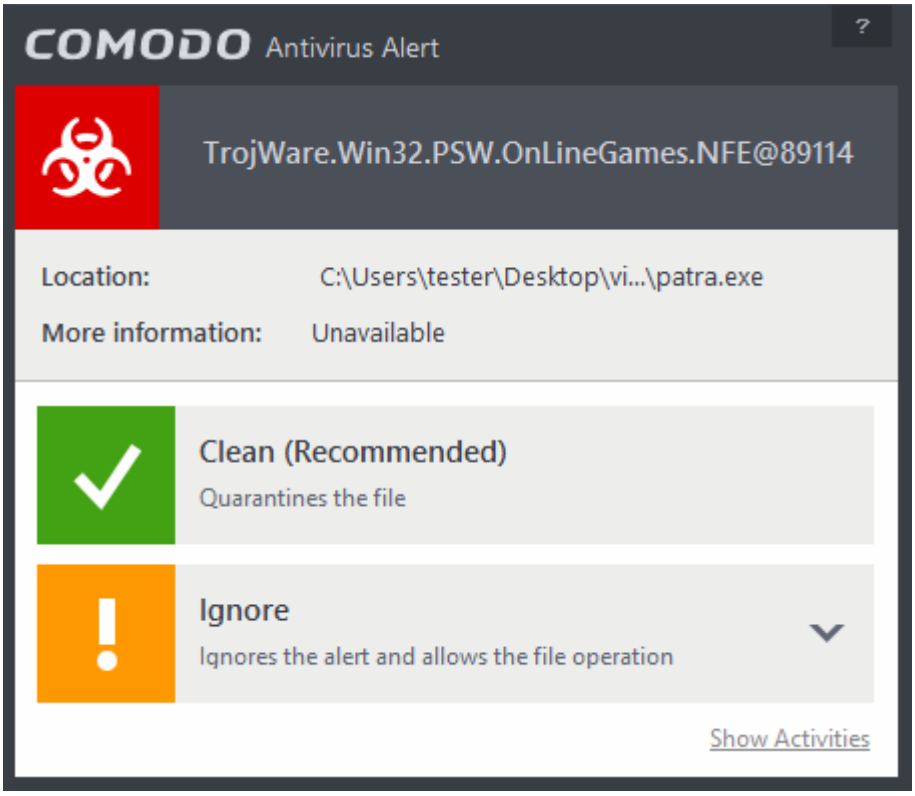
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answering an Antivirus Alert

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

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

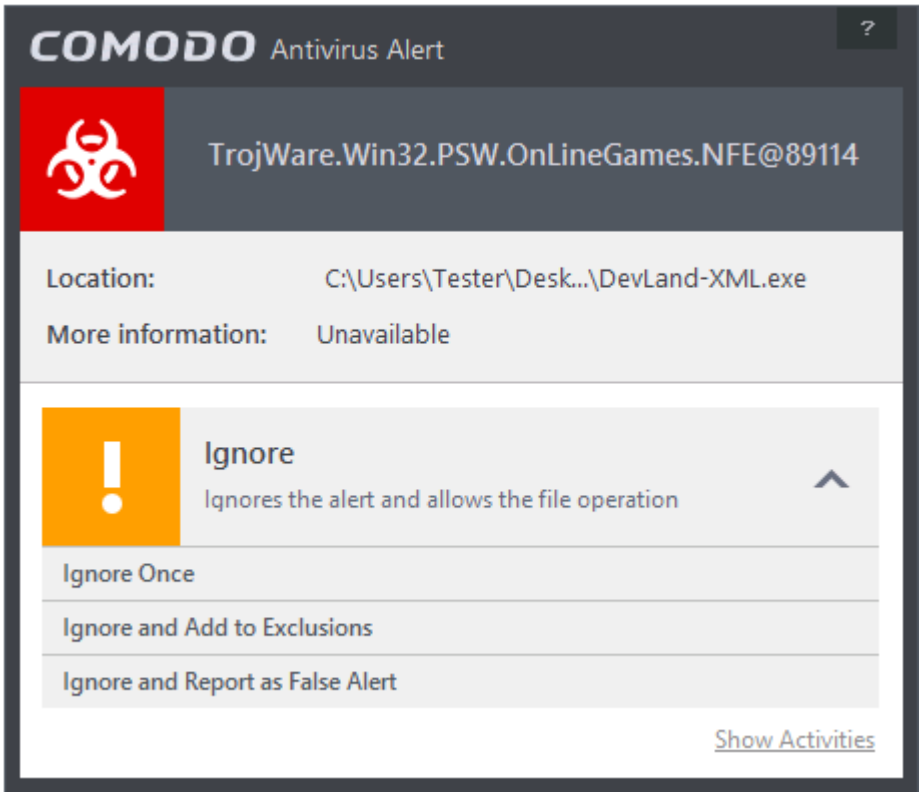


Tip: Clicking the Show Activities link at the bottom right will open the **Process Activities List dialog**. The Process Activities dialog will display the list activities of the processes run by the application.

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

The following response-options are available:

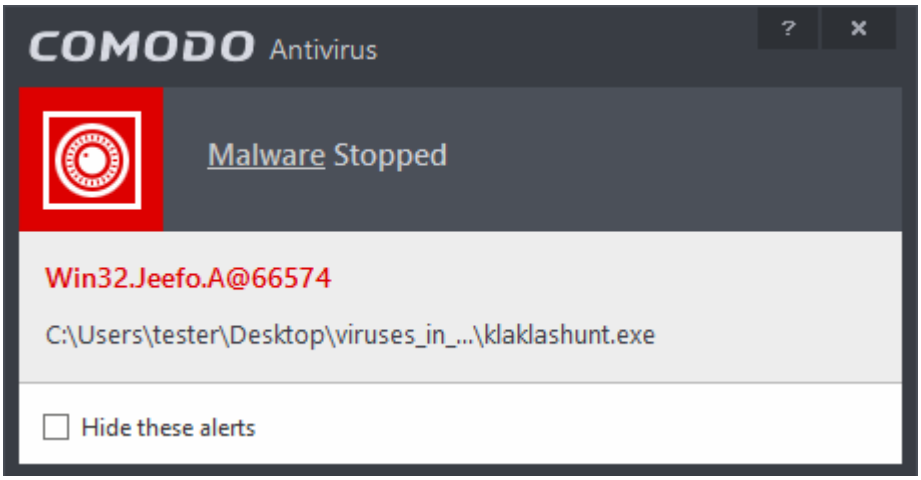
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the **Quarantine** interface. Refer to **Manage Quarantined Items** for more details on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



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

Antivirus Notification

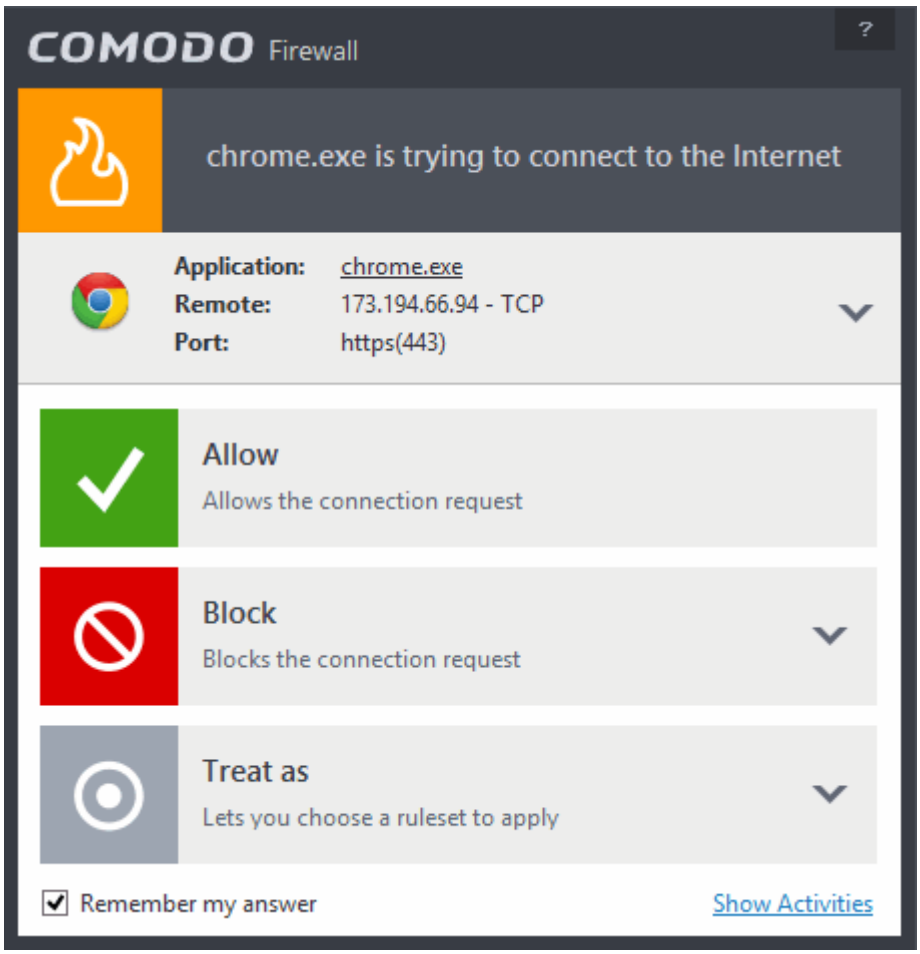
If you have chosen to not to show Antivirus Alerts through **Advanced Settings > Security Settings > Antivirus Settings > Realtime Scanner Settings** by leaving the option 'Do not show antivirus alerts' enabled (***default=enabled***) and If CIS identifies a virus or other malware in real time, it will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



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

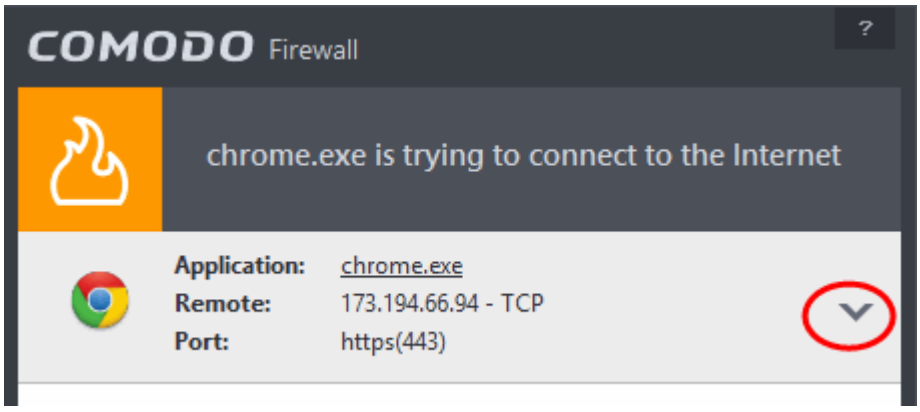
Answering Firewall Alerts

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



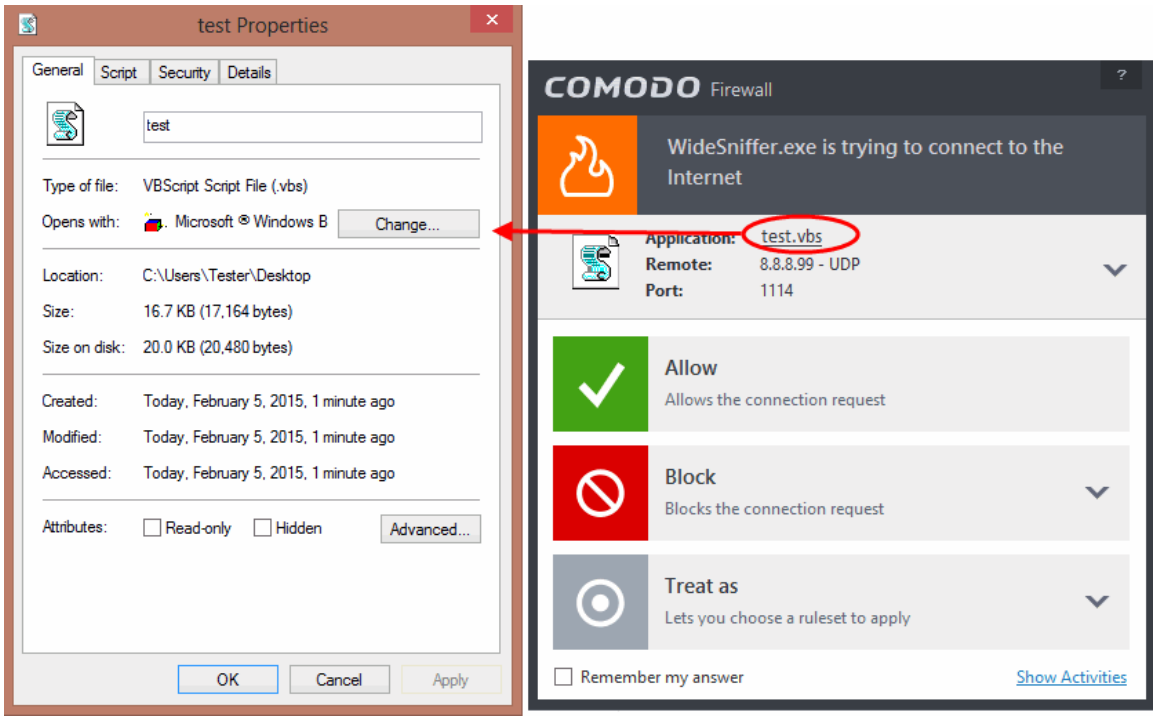
Tip: Clicking the Show Activities link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

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



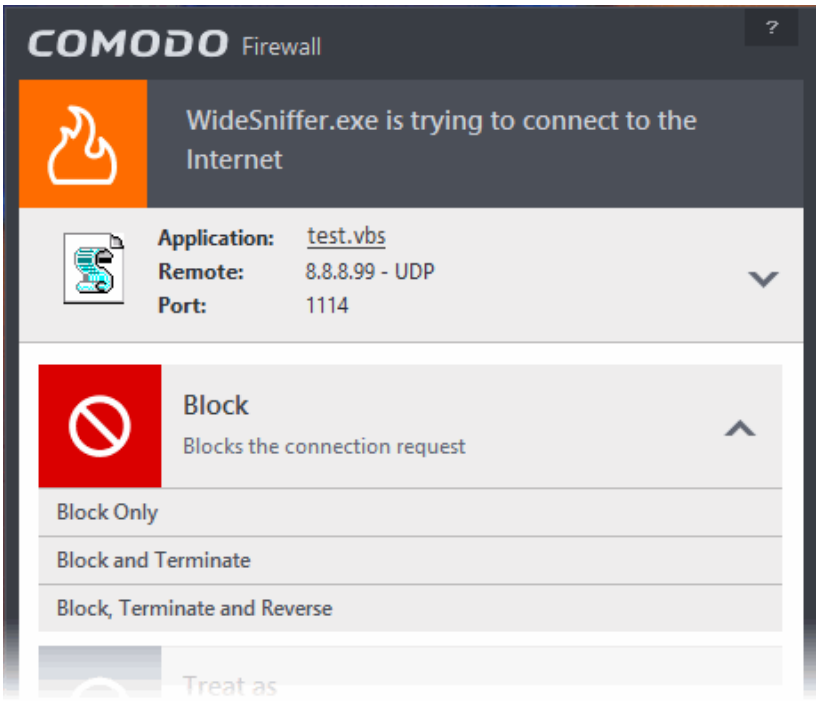
1. Carefully read the information displayed in clicking the down arrow in the alert description area. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security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



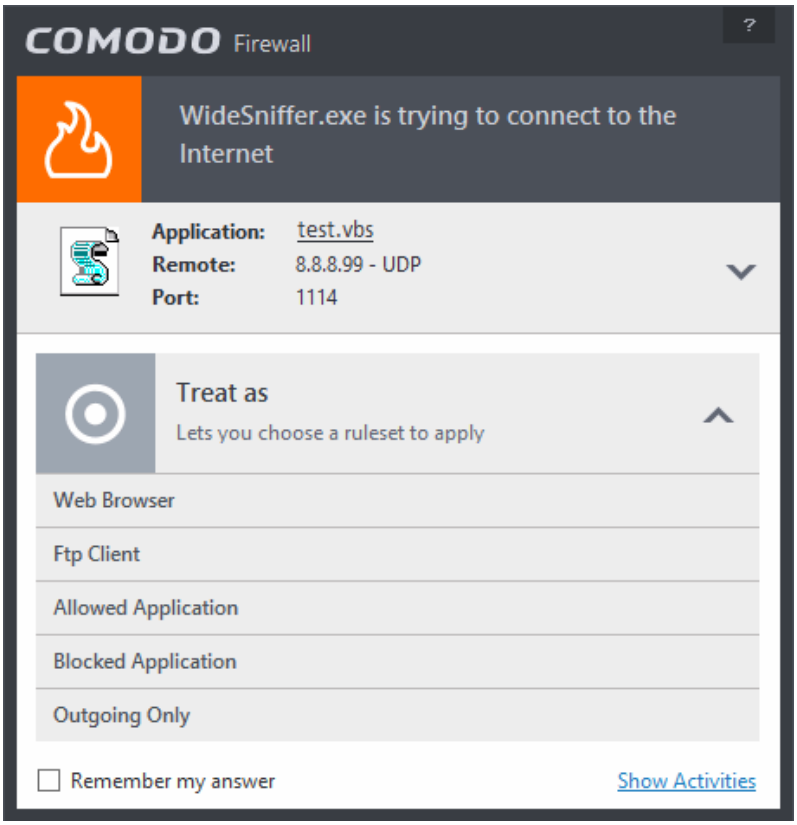
In all cases, clicking on the name of the application opens a properties window that can help you determine whether or not to proceed:

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 & terminate (connection is not allowed to proceed and the process/application that made the request is shut down) or block, terminate and reverse (connection is not allowed to proceed and the process/application that has made any changes will be rolled back)



2. If you are sure that it is one of your everyday application, try to use the '**Treat As**' option as much as possible. This allows you to deploy a **predefined firewall ruleset** on the target application. For example, you may choose to apply the policy **Web Browser** to the known and trusted applications 'Internet Explorer', 'Firefox' and 'Opera'. Each

predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application.

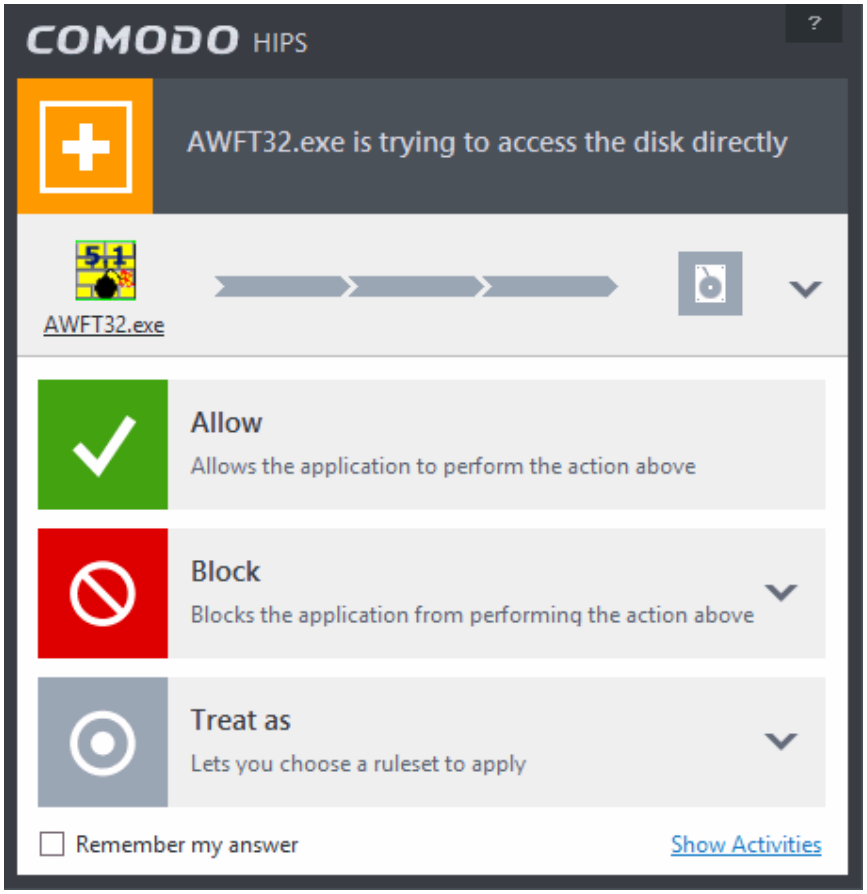


Remember to check the box **Remember My Answer** for the ruleset to be applied in future.

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

Answering HIPS Alerts

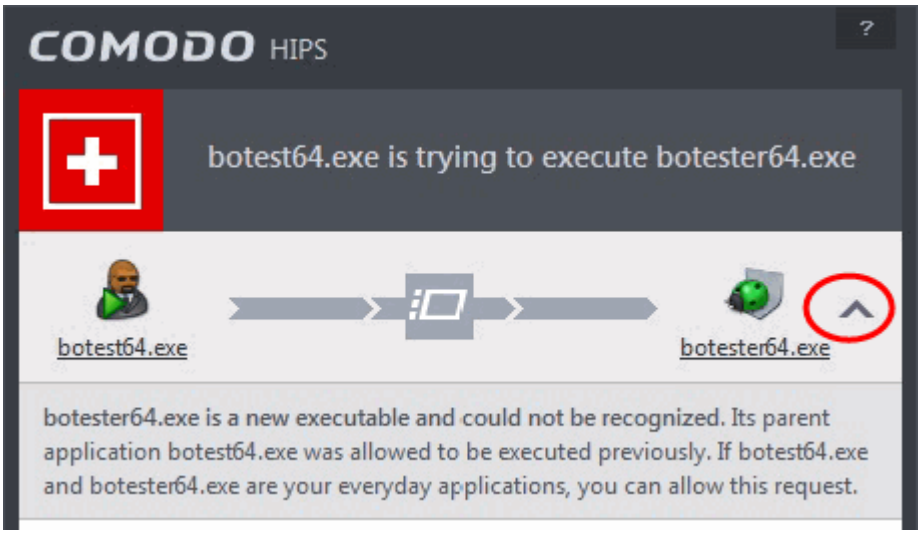
Comodo Internet Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:



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

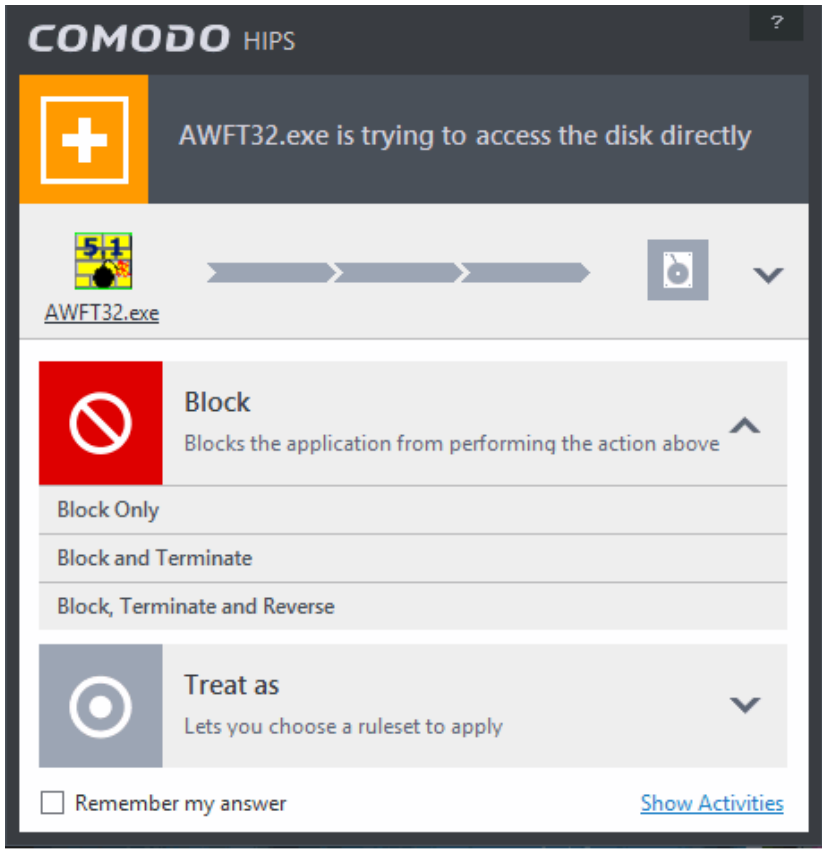
The Show Activities link is available only if Viruscope is enabled under **Advanced Settings > Defense+ >Viruscope** . If none of the processes associated with the application has started before the alert is generated, the Show Activities link is disabled and will not open the Process Activities List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

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

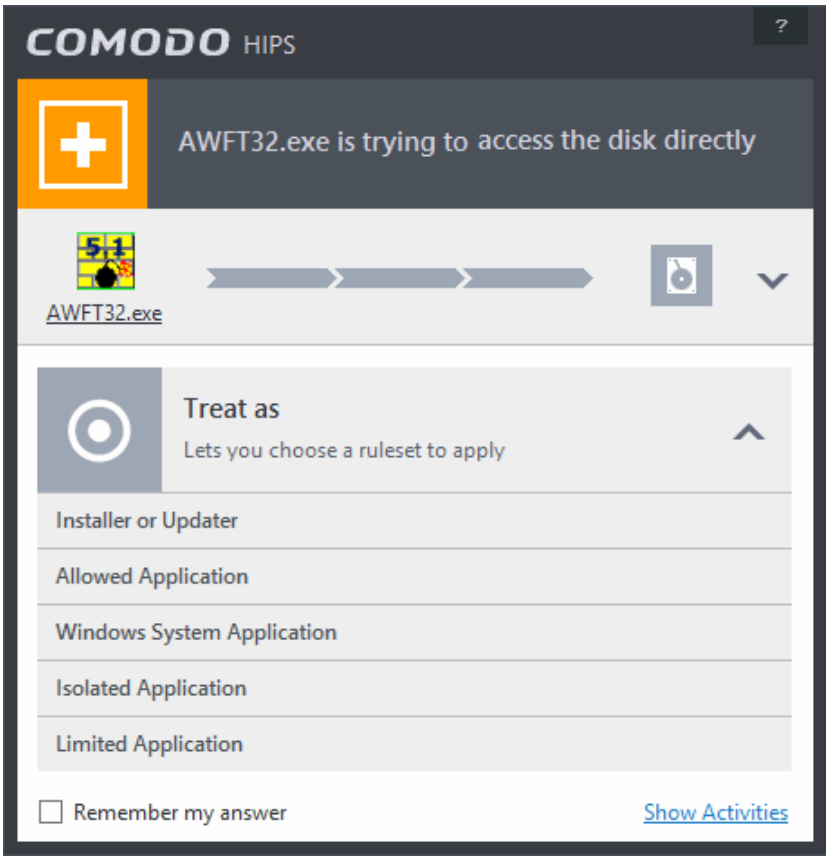


If it is one of your everyday applications and you simply want it to be allowed to continue then you should select **Allow**.

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

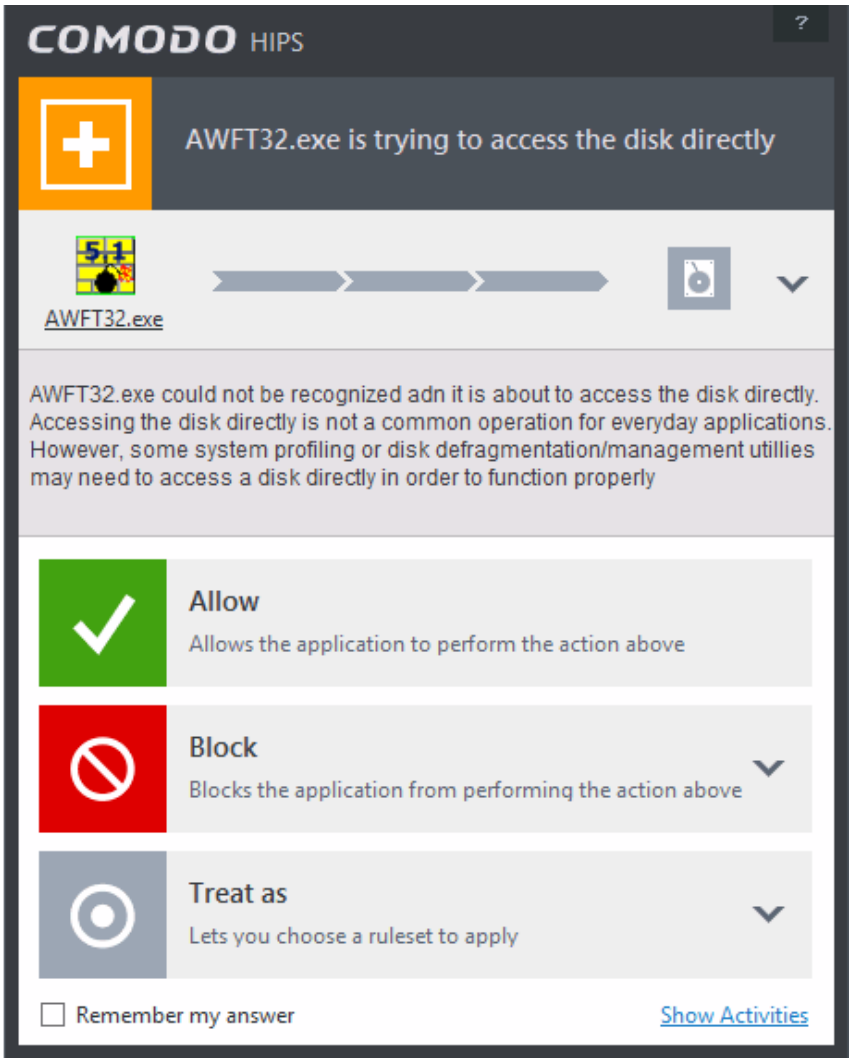


2. If you are sure that it is one of your everyday applications and want to enforce a security policy (ruleset) to it, please use the 'Treat As' option. This applies a **predefined HIPS ruleset** to the target application.

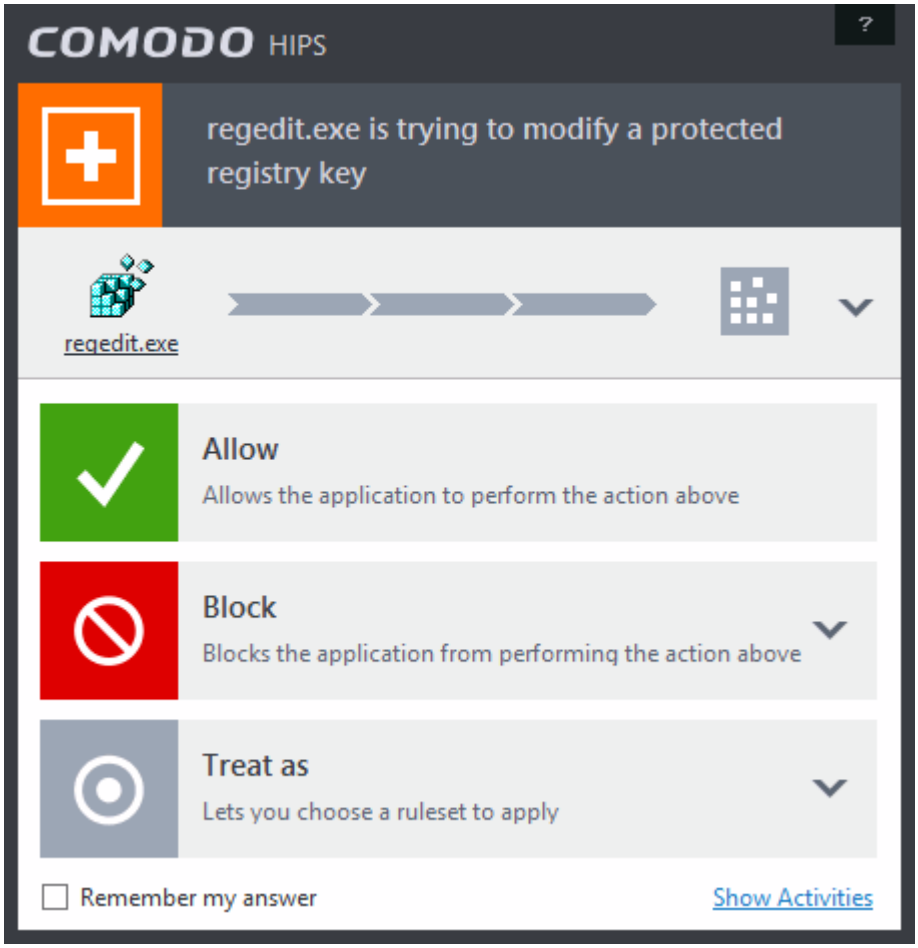


Avoid using the **Installer or Updater** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select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

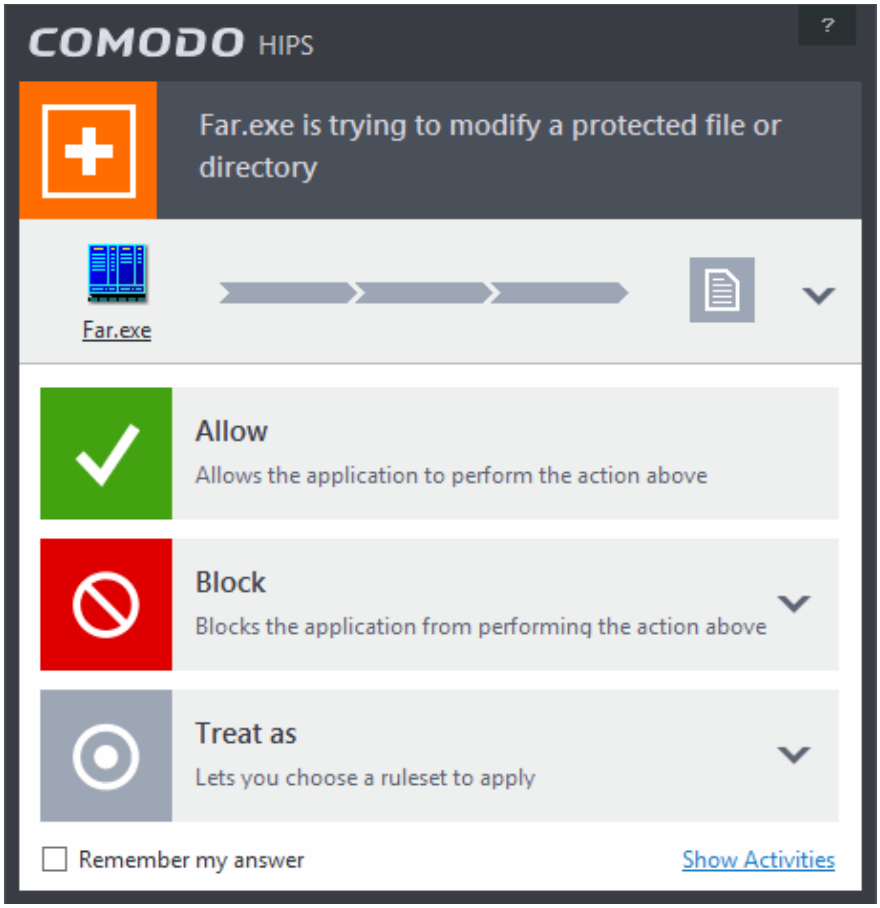
3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity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



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



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



Were you installing new software or trying to download an application from the Internet? If you are downloading a file from the 'net, select **Allow,** without selecting **Remember my 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 subdirectories) then pay special attention. The Windows directory is a favorite target of malware applications. If you are not installing any new applications or updating Windows then make sure you recognize the application in question. If you don't, then click **Block** and choose **Block Only** from the options, without selecting **Remember My answer** option.

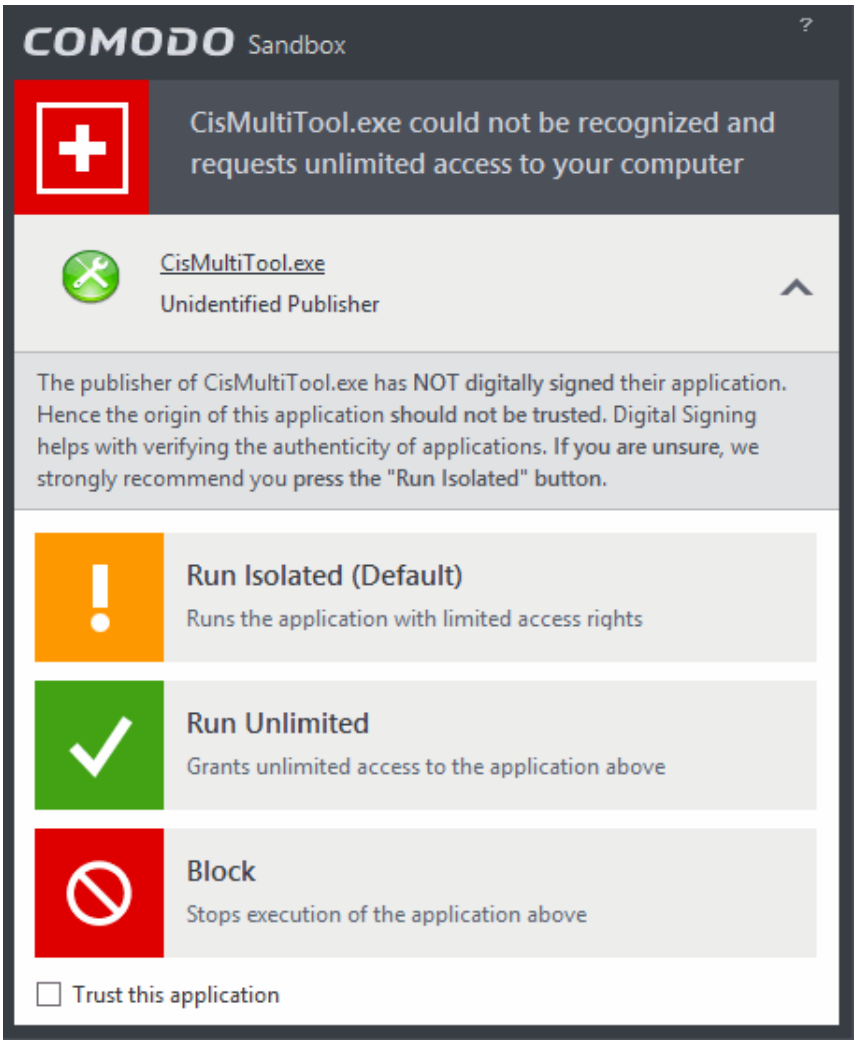
If an application is trying to create a new file with a random file name e.g. "hughbasd.dll" then it is probably a virus and you should block it permanently by clicking **Treat As** and choosing **'Isolated Application'** from the options.

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

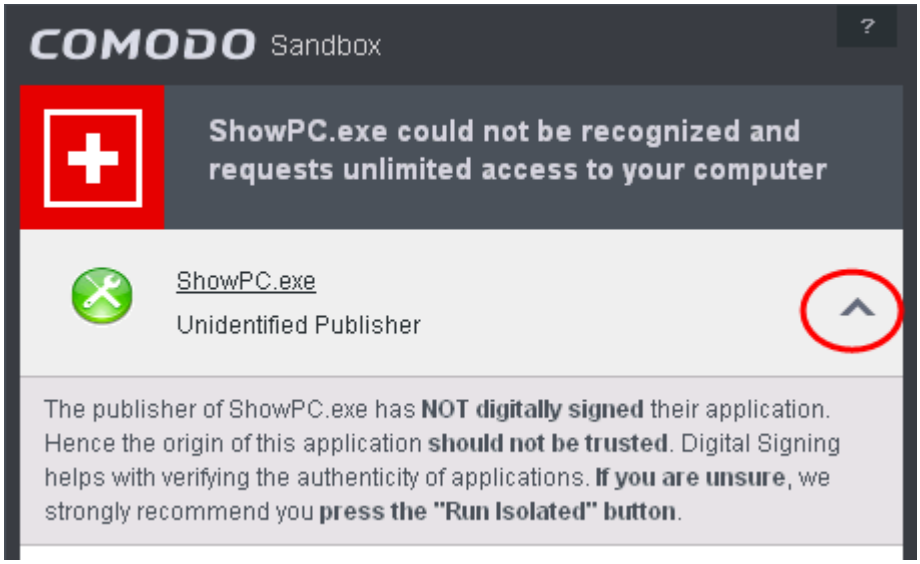
Answering a Sandbox Alert

Comodo Internet Security generates a Behavior Blocker 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 sandboxes an unknown application.

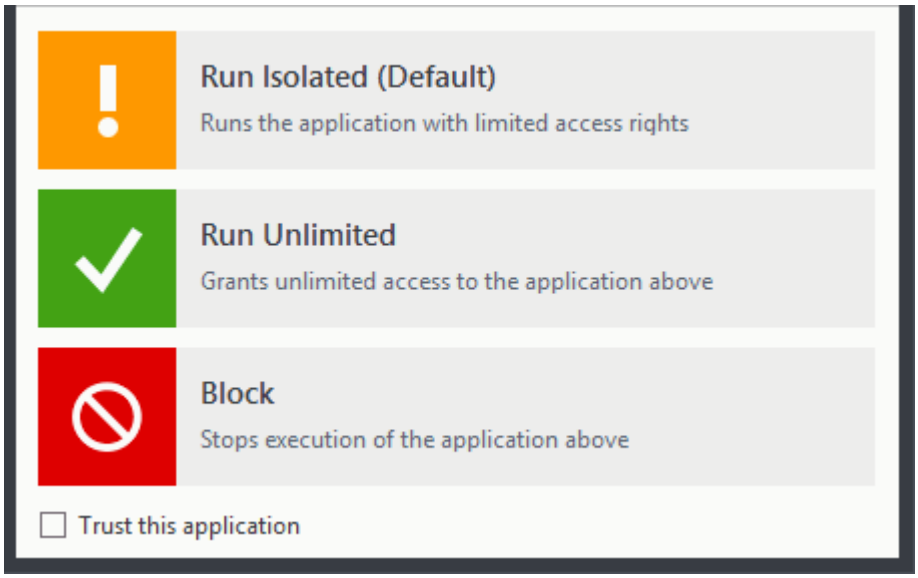
Please read the following advice before answering a Behavior Blocker alert:



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



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



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

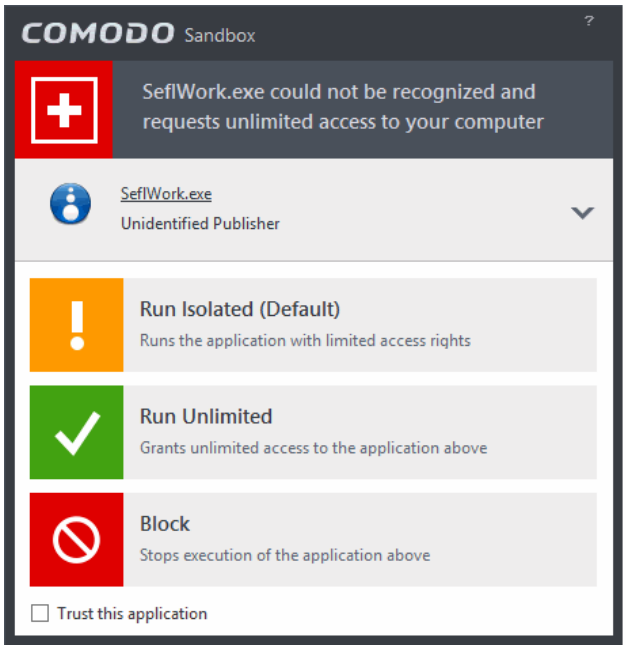
Run with Elevated Privileges Alert

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

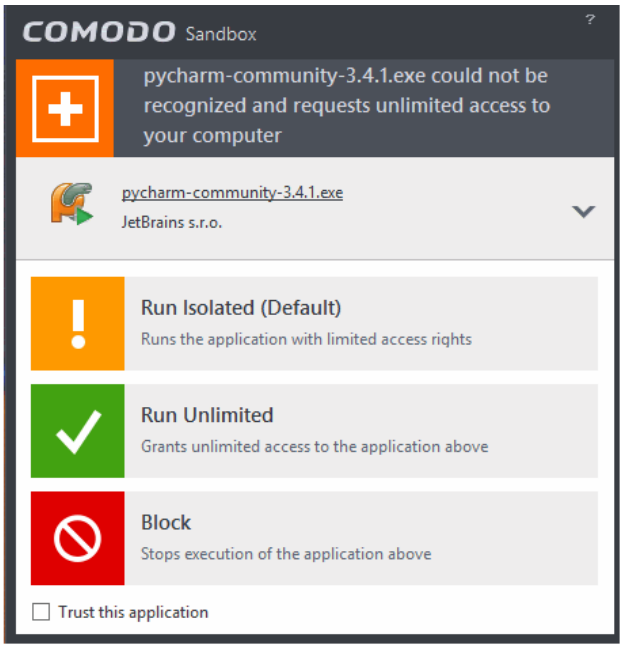
- If you have good reason to trust the publisher of the software then you can click the '**Run Unlimited**' button. This will grant the elevated privilege request and allow the installer to run.
- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted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

Note: You will see this type of alert only if 'Detect installers and show privilege elevation alerts' is enabled. This can be found in 'Advanced Settings > Security Settings > Defense+ > '**Sandbox Settings**'

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



Unknown and not digitally signed



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

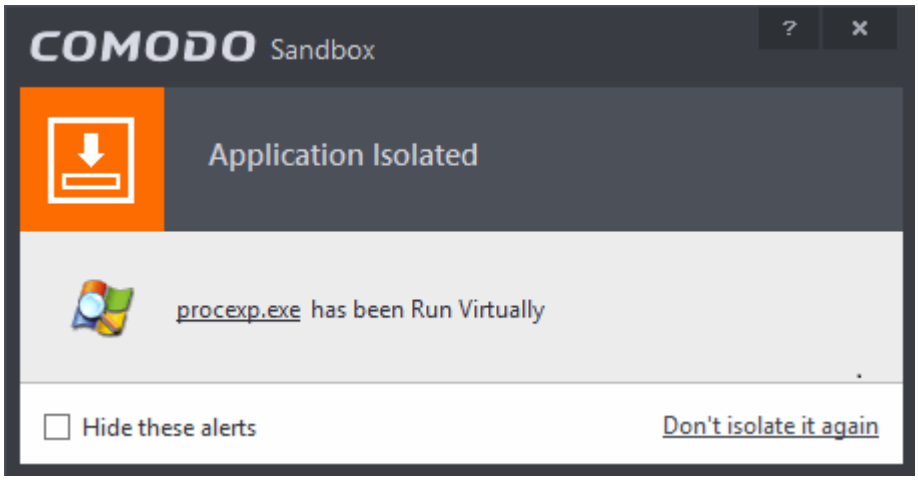
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

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

Sandbox Notification

The Sandbox will display a notification whenever it auto-sandboxes an unknown application:



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

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

Users are also reminded that they should submit such unknown applications to Comodo via the '**File List**' interface. This will

allow Comodo to analyze the executable and, if it is found to be safe, to add it to the global safe list. This will ensure that unknown but ultimately safe applications are quickly white-listed for all users.

Also see:

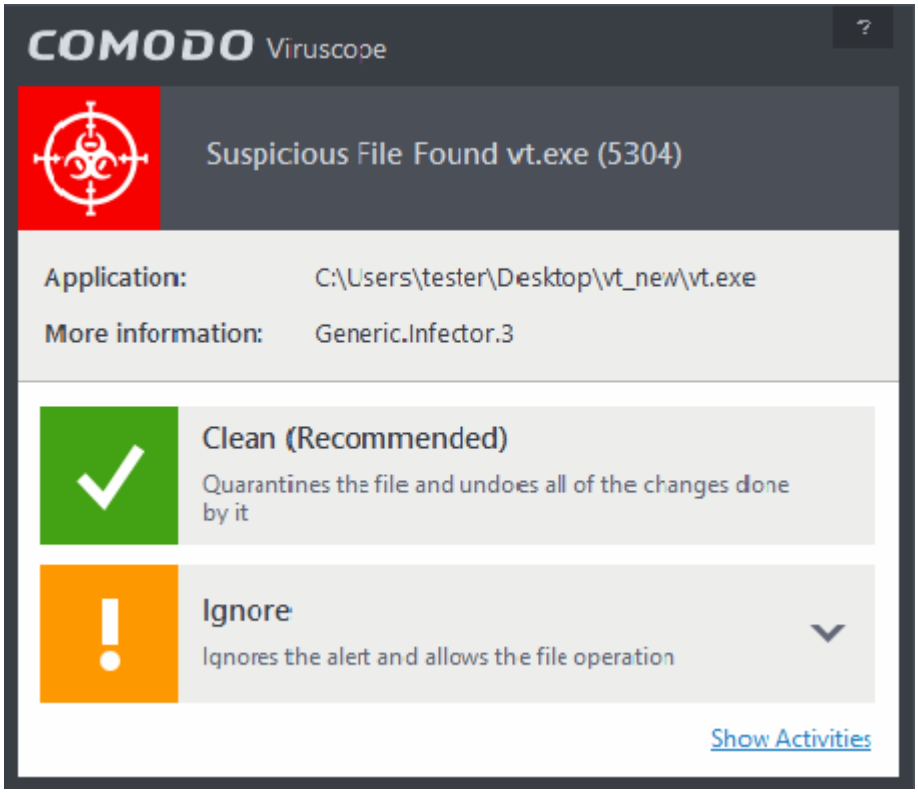
- '**Unknown Files: The Scanning Processes**' - to understand process behind how CIS scans files

Answering a Viruscope Alert

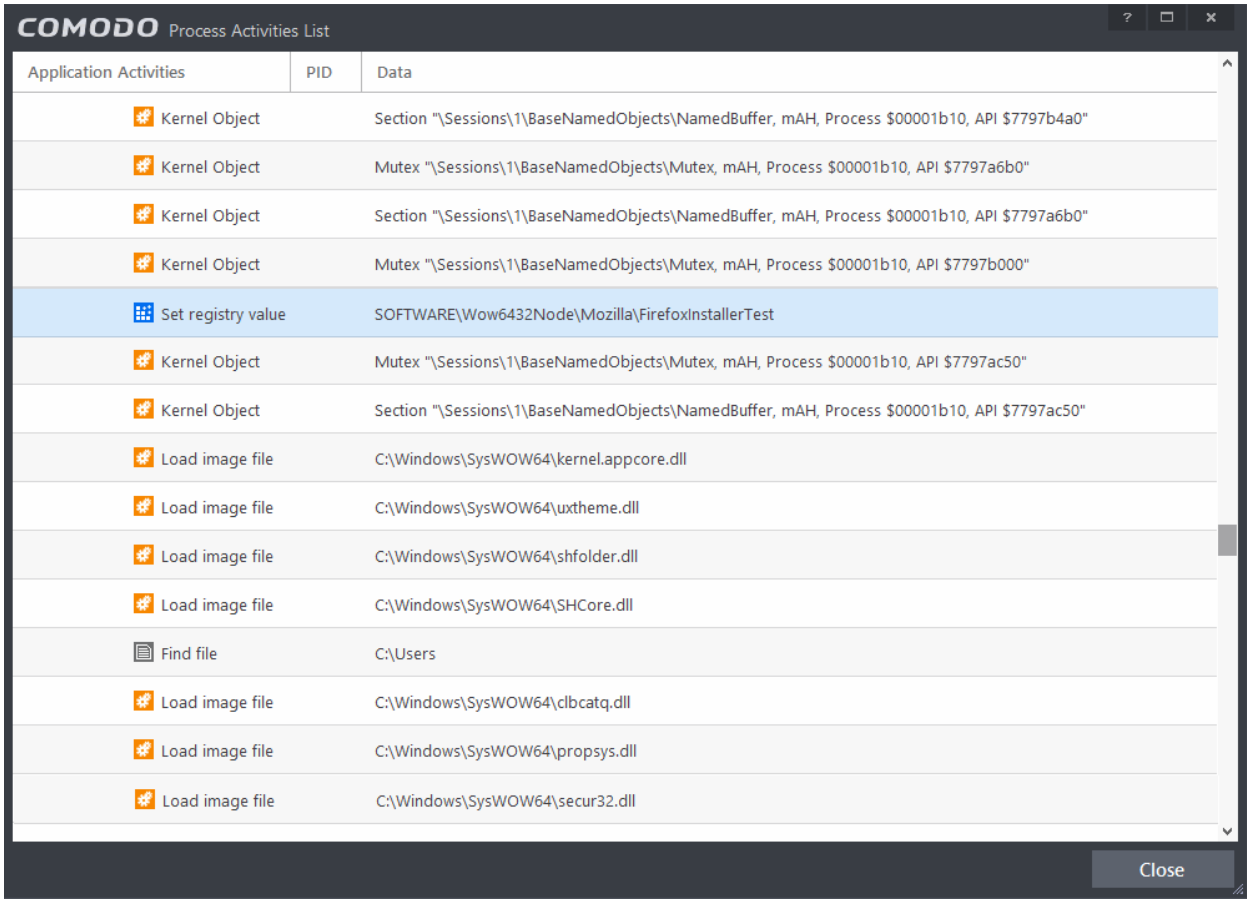
Comodo Internet Security generates a Viruscope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that Viruscope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a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

Please read the following advice before answering a Viruscope alert:

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



- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking Ignore and selecting the option from the drop-down.
  - Ignore Once -The process is allowed to run this time only. If the process attempts to execute on future occasions, another Viruscope alert is displayed.
  - Ignore and Add to Trusted Files - The process is allowed to run and and the parent application is moved to the Trusted Files list - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- To view the activities of the processes, click the Show Activities link at the bottom right. The Process Activities List dialog will open with a list of activities exhibited by the process.

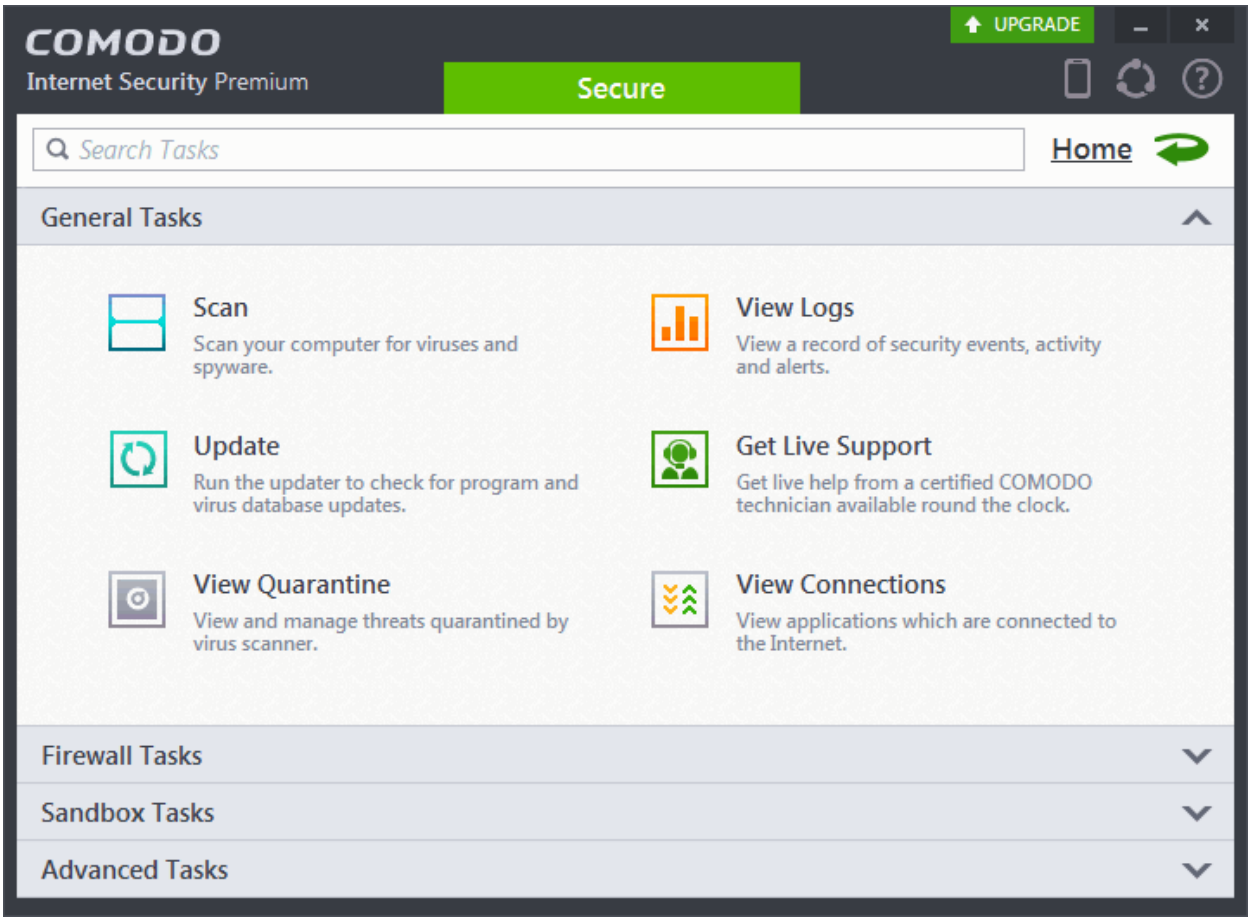


Column Descriptions

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

2.General Tasks - Introduction

The 'General Tasks' interface allows you to quickly perform antivirus scans, update the virus database, manage quarantined files, view CIS event logs, view and manage internet connections and get live help from Comodo technicians.

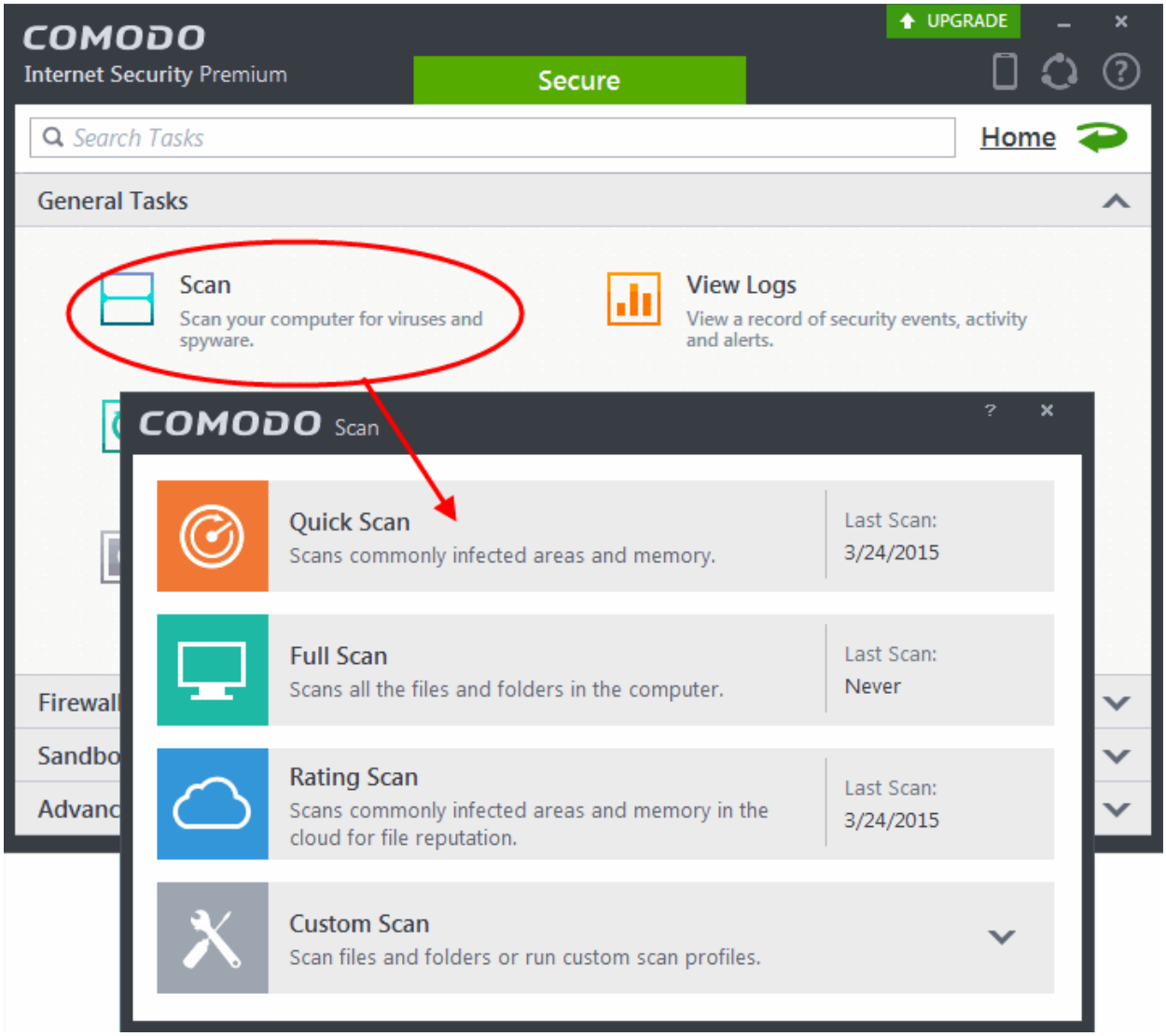


'General Tasks' contains the following areas. Click the links to jump to the help page for that topic.

- **Scan and Clean your Computer**
- **Instantly Scan Files and Folders**
- **Processing Infected Files**
- **Manage Virus Database and Program Updates**
- **Manage Quarantined Items**
- **View CIS Logs**
- **Get Live Support**
- **View Active Internet Connections**

2.1. Scan and Clean Your Computer

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



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

- **Run a Quick Scan**
- **Run a Full Computer Scan**
- **Run a Rating Scan**
- **Run a Custom Scan**
  - **Scan a Folder**
  - **Scan a File**
  - **Create and Schedule a Custom Scan**
- **Scan individual file/folder**
- **Processing Infected Files**

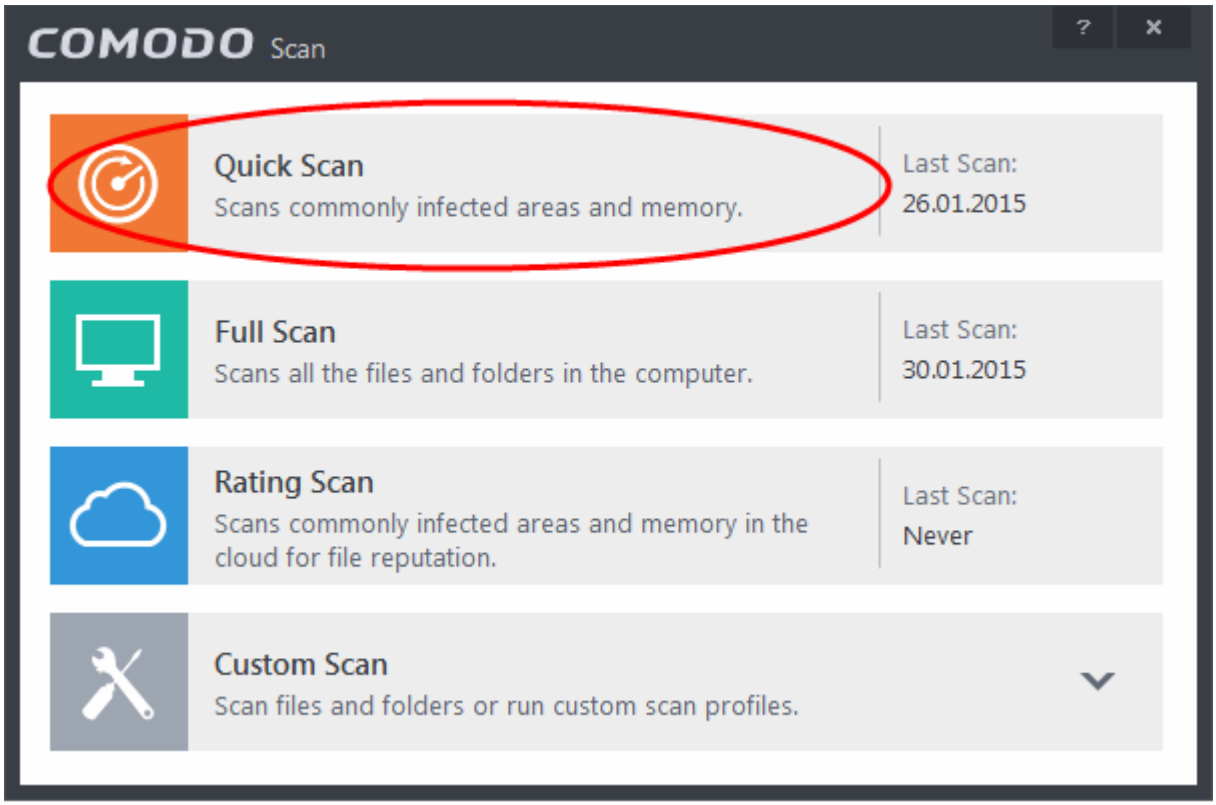
2.1.1. Run a Quick Scan

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

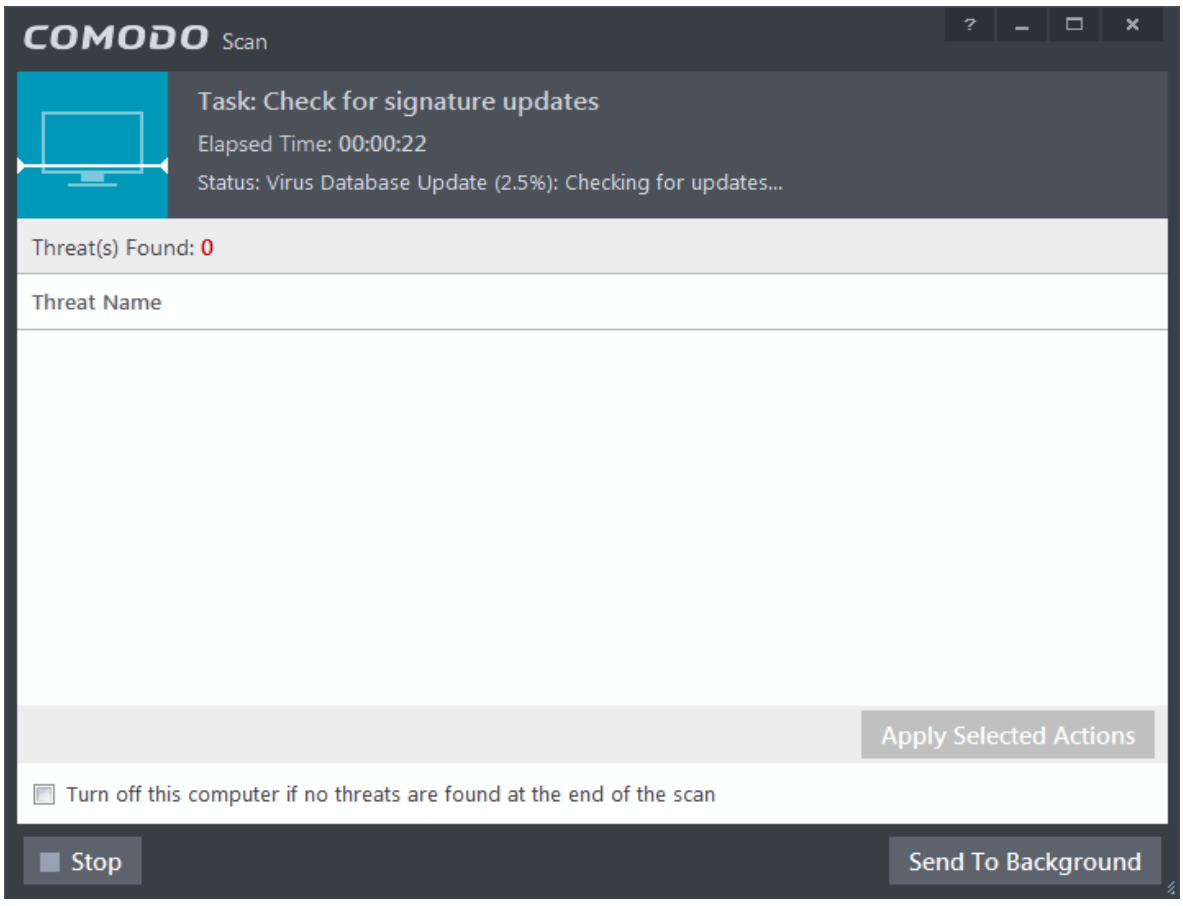
You can customize which items are scanned under a 'Quick Scan' and create a scan schedule from the 'Advanced Tasks' interface. Refer to **Antivirus Settings** > **Scan Profiles** for more details.

To run a Quick Scan

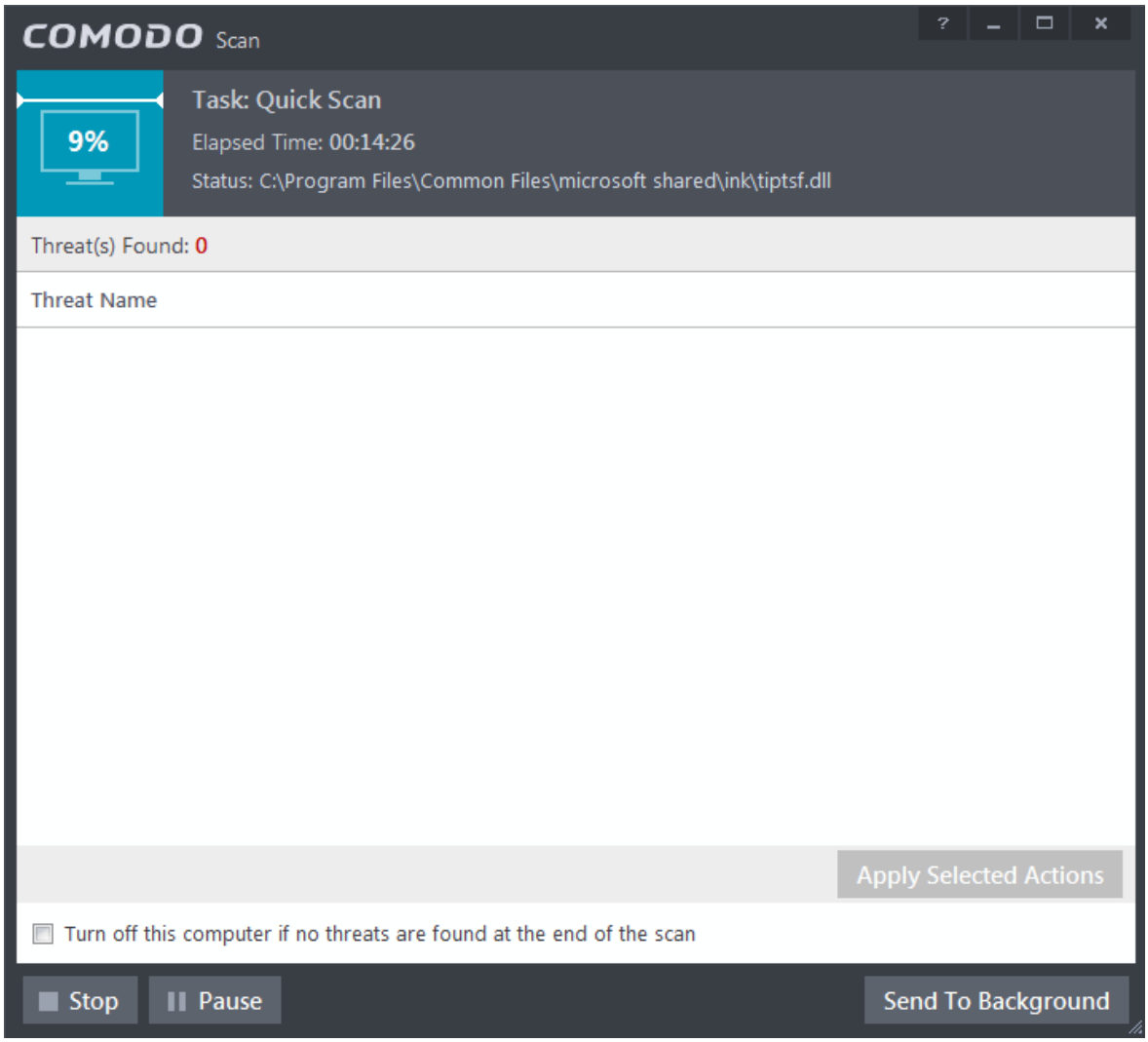
- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



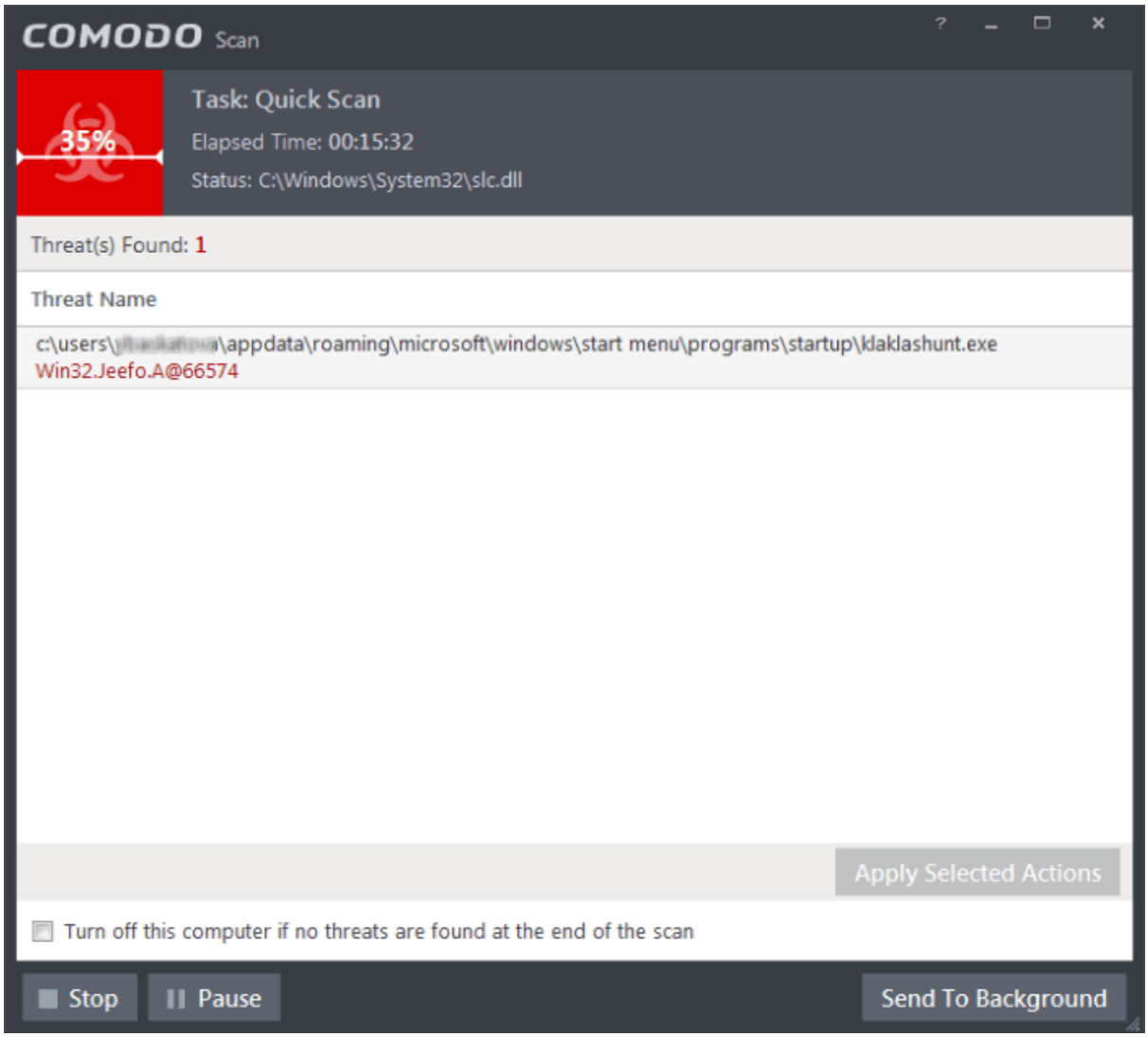
The scanner will start and first check whether your virus signature database is up-to-date:



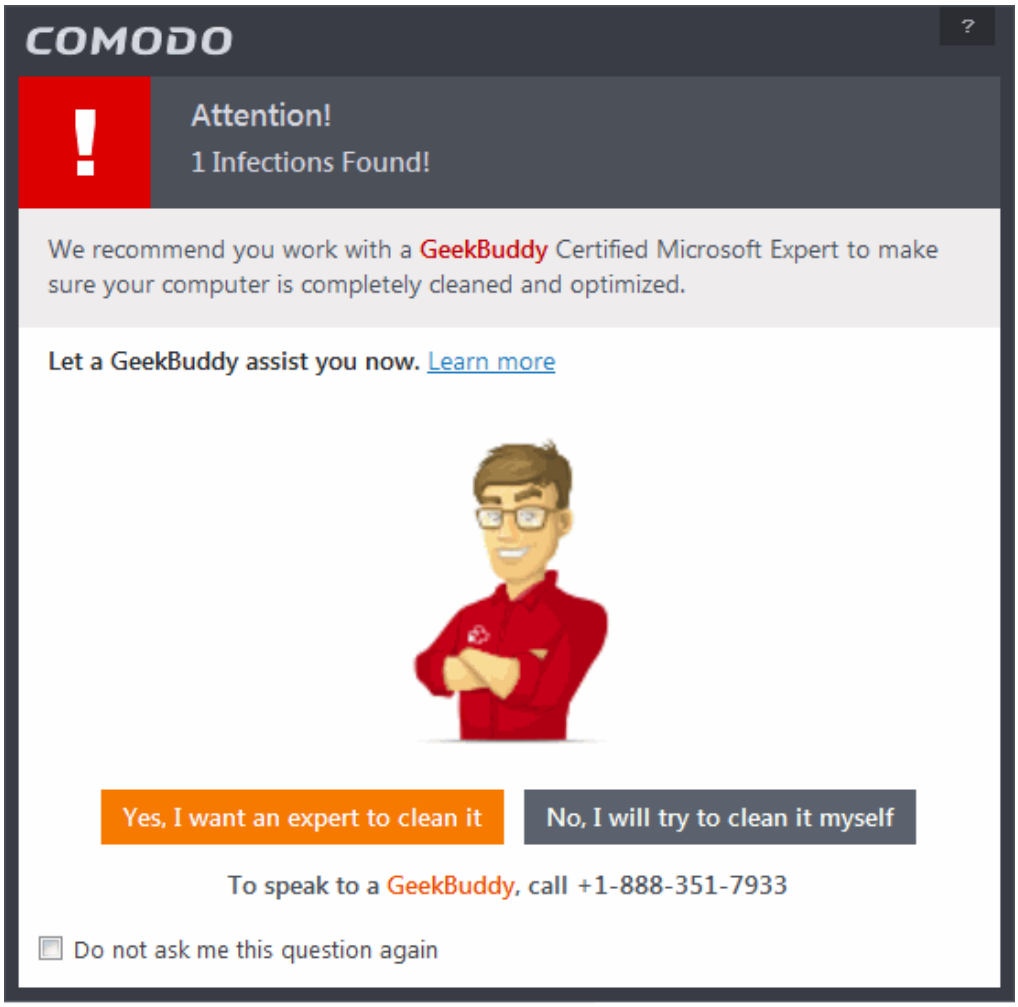
If the database is outdated, the scanner will first download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:



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

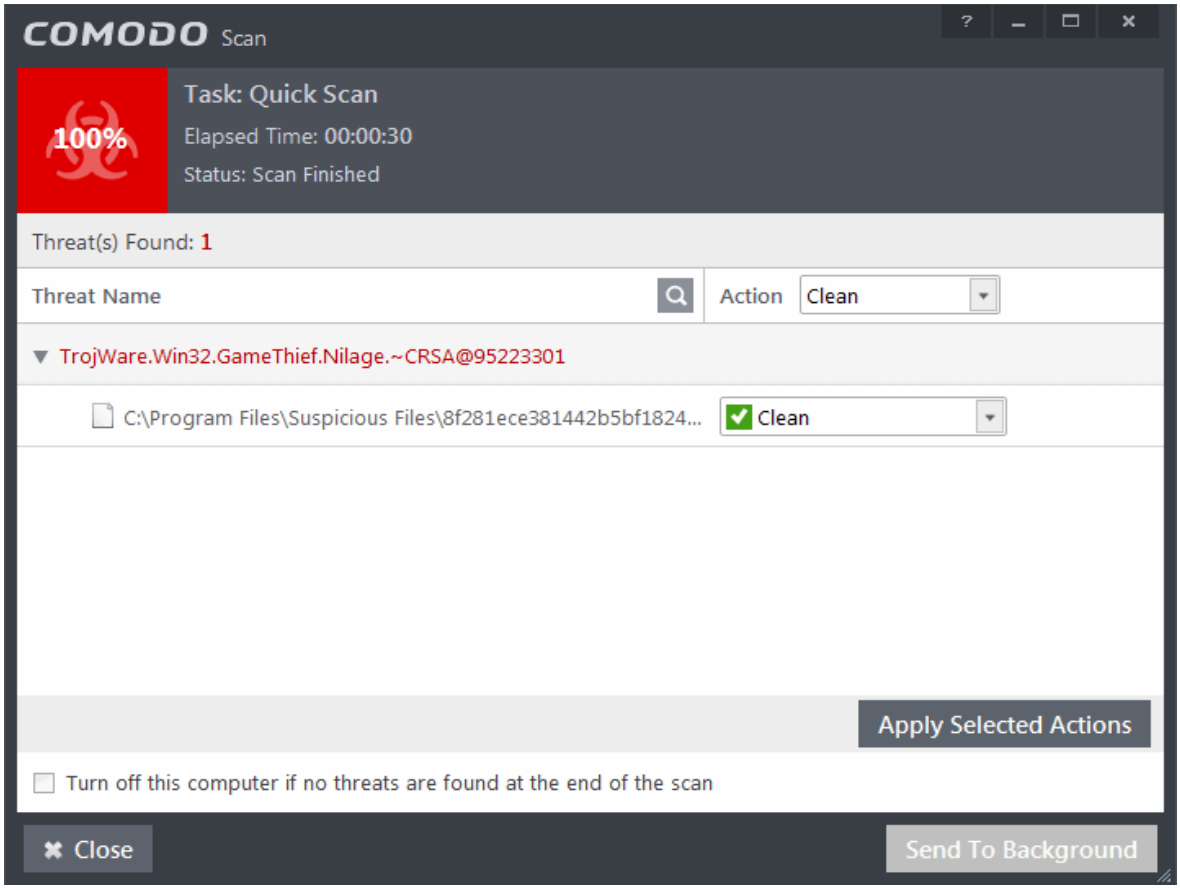


- An alert screen will be displayed at the end of the scan if issues were detected. The alert will display the number of threats/infections discovered and present you with cleaning options:



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

  For more details on GeekBuddy Expert help, refer to the section **Comodo GeekBuddy**.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



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

2.1.2. Run a Full Computer Scan

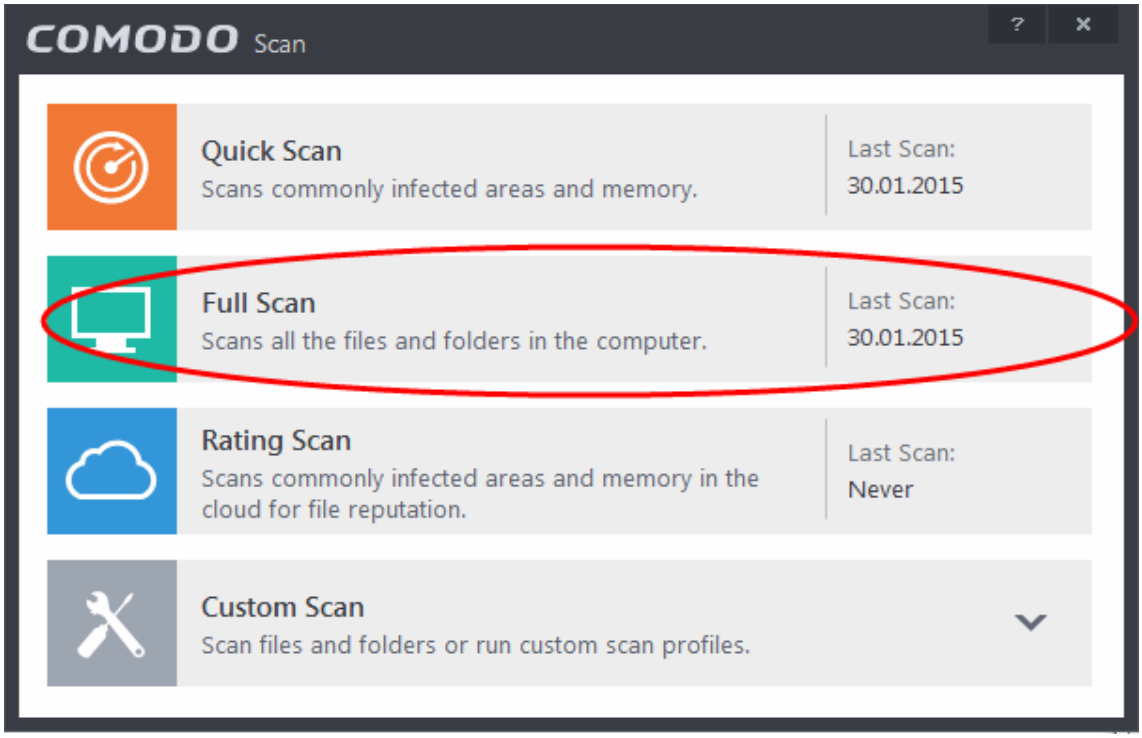
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

You can customize which items are included in a full scan and set-up a scan schedule from the 'Advanced Tasks' interface.

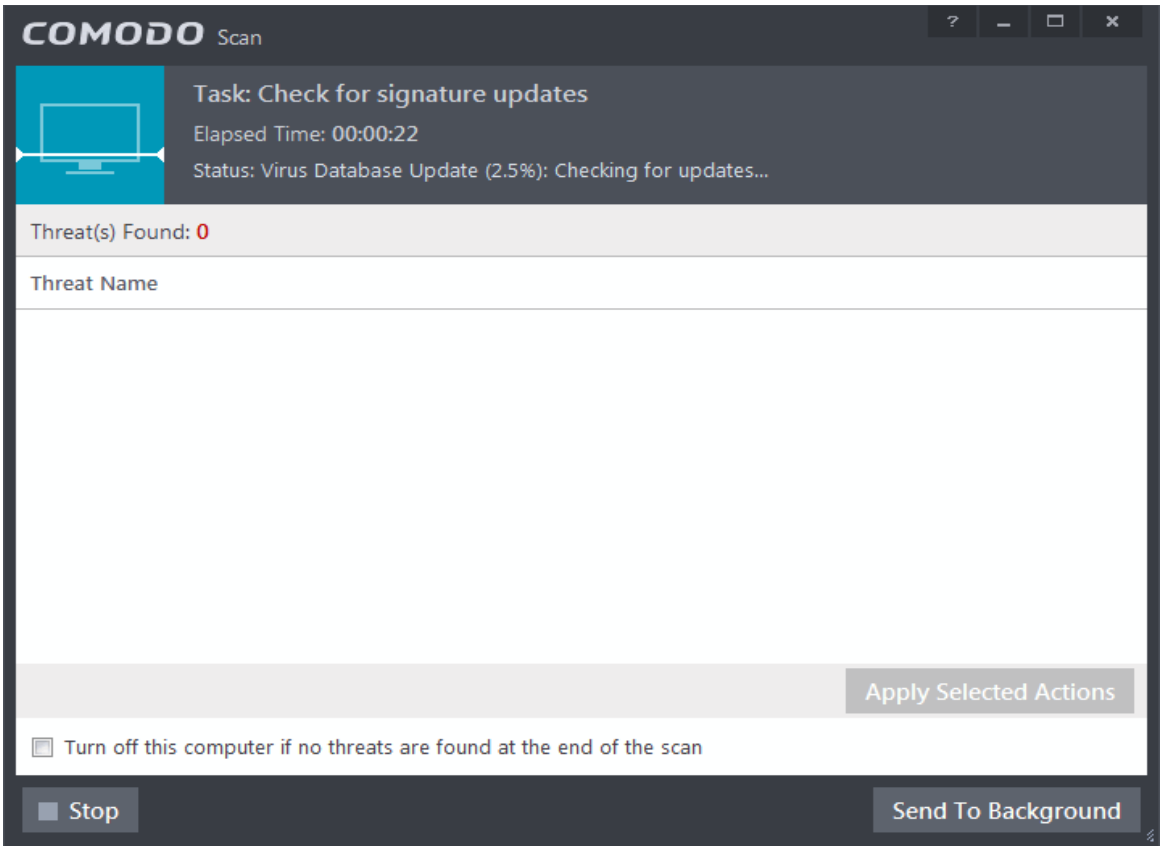
Refer to **Antivirus Settings** > **Scan Profiles** for more details.

To run a Full Computer Scan

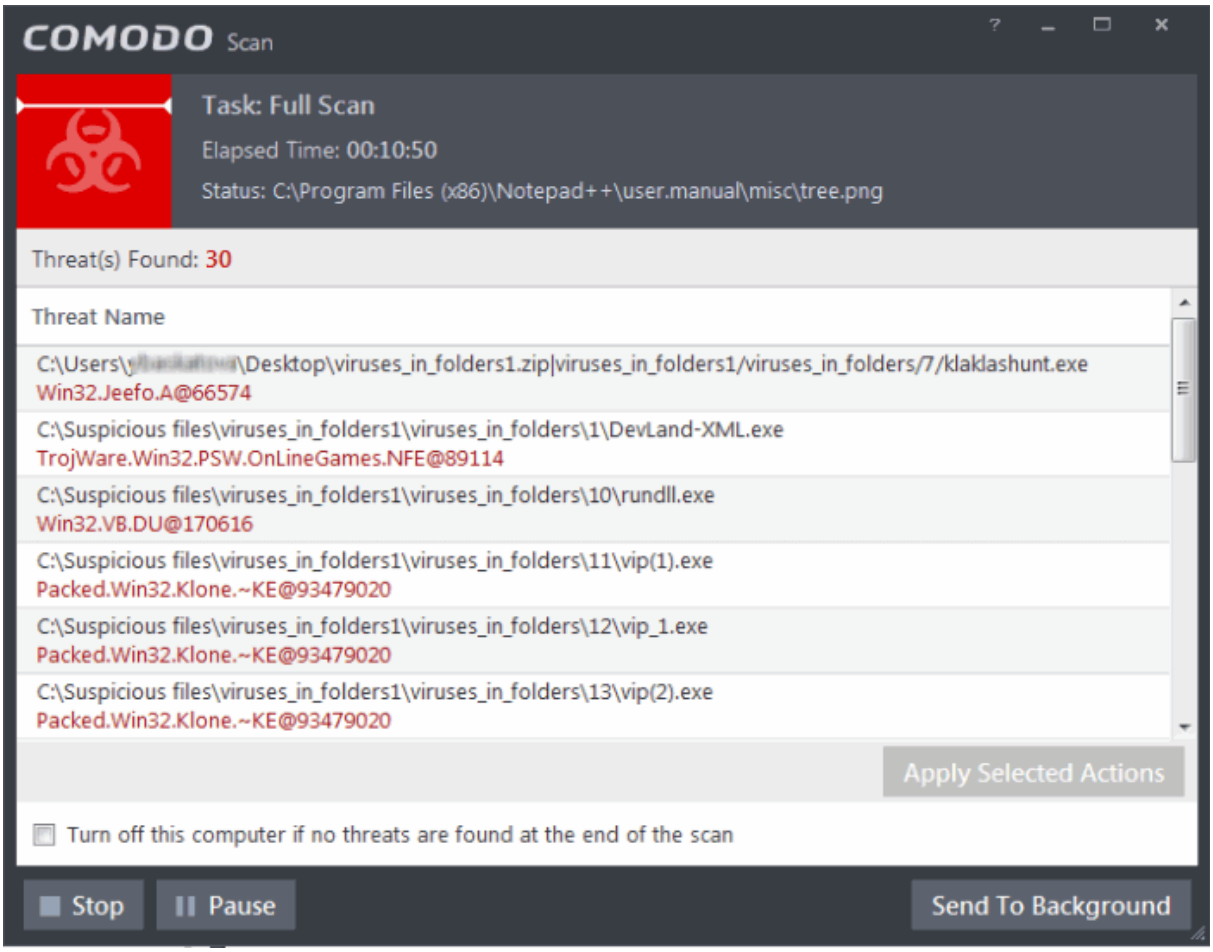
- Click 'Scan' from the General Tasks interface the click 'Full System Scan' from the 'Scan' interface.



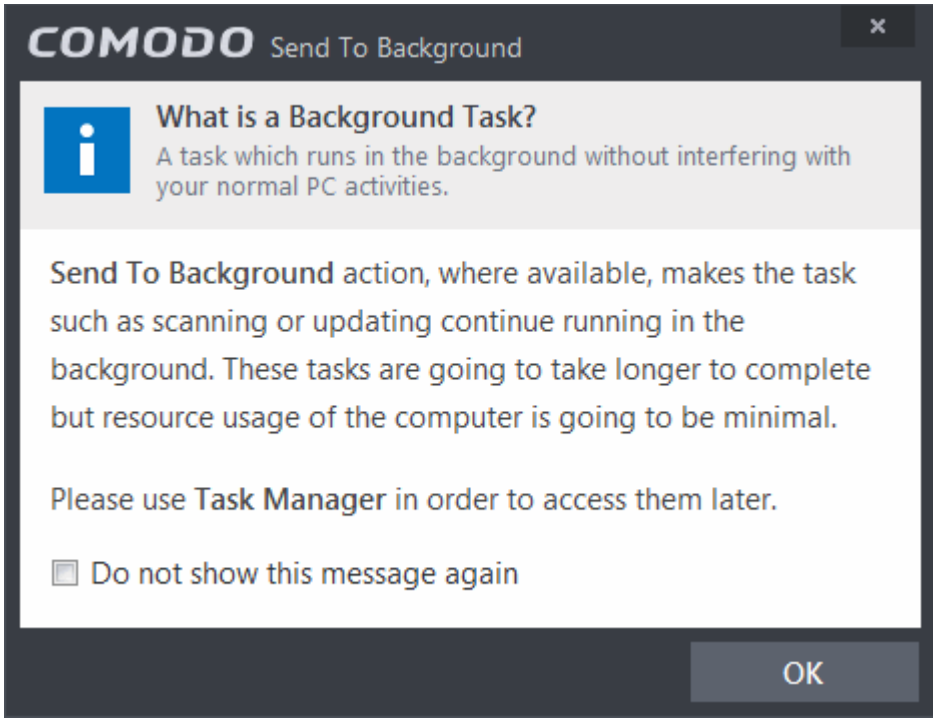
The scanner will start and first check whether your virus signature database is up-to-date.



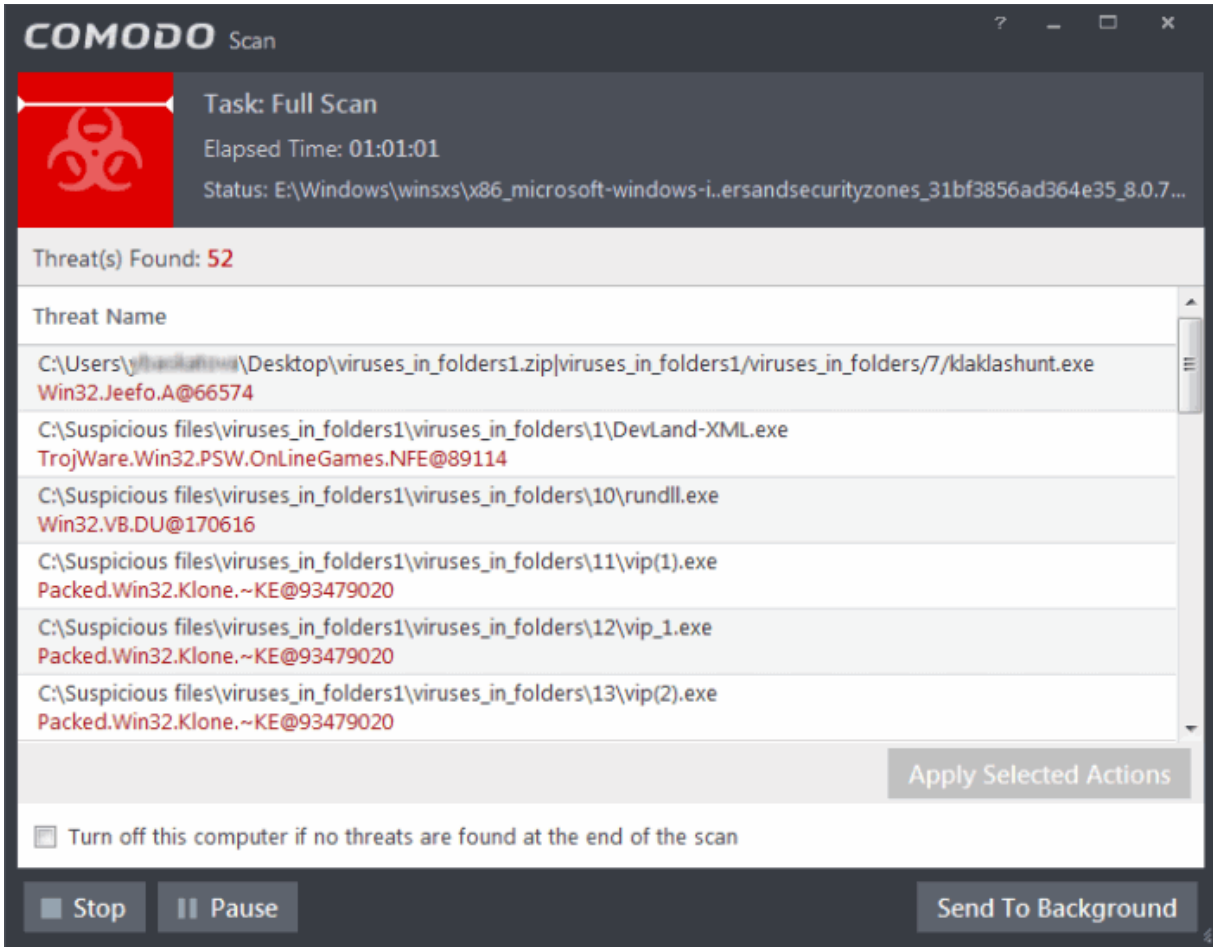
If the database is outdated, CIS will first download and install the latest database before commencing the scan.



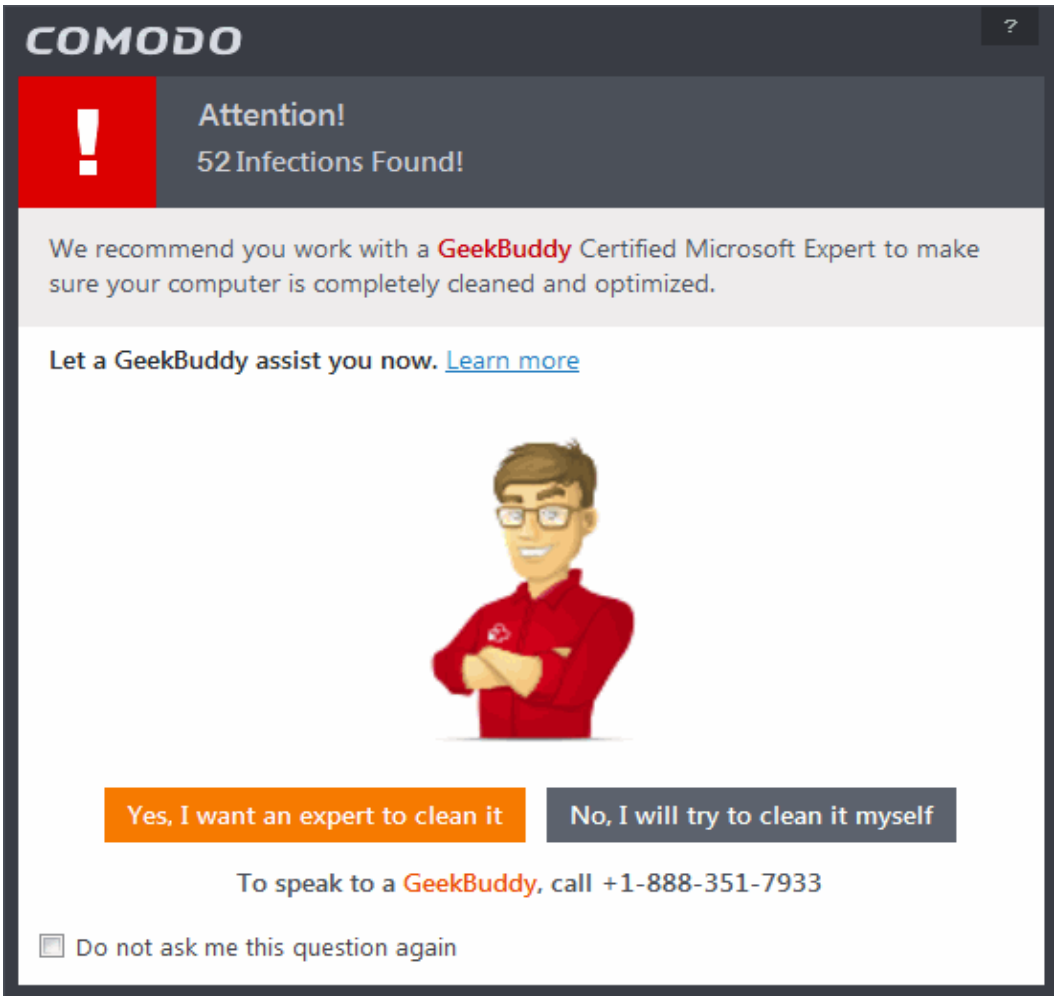
- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



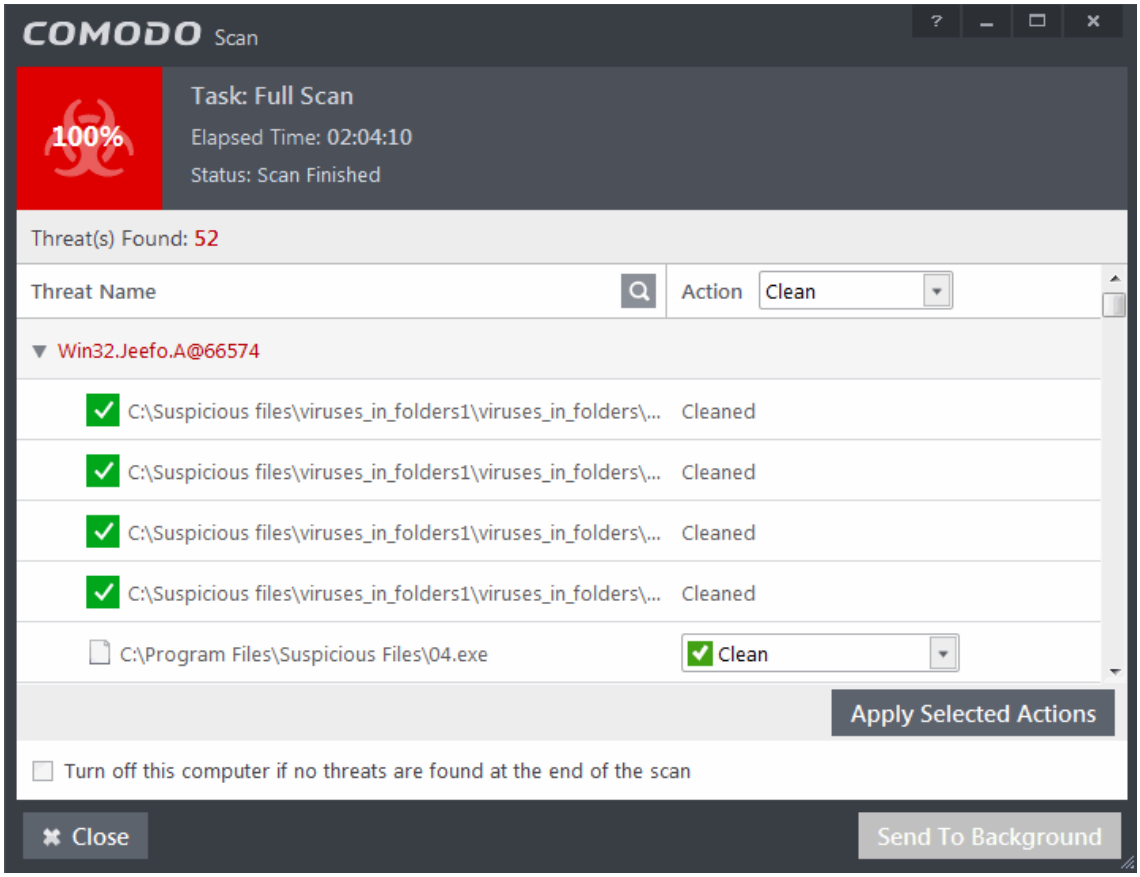
If you send to the background, you can continue to check scan progress by clicking '**Task Manage**r' on the home screen or by clicking '**Open Task Manager**' icon from the 'Advanced Tasks' interface.



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



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



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

2.1.3. Run a Rating Scan

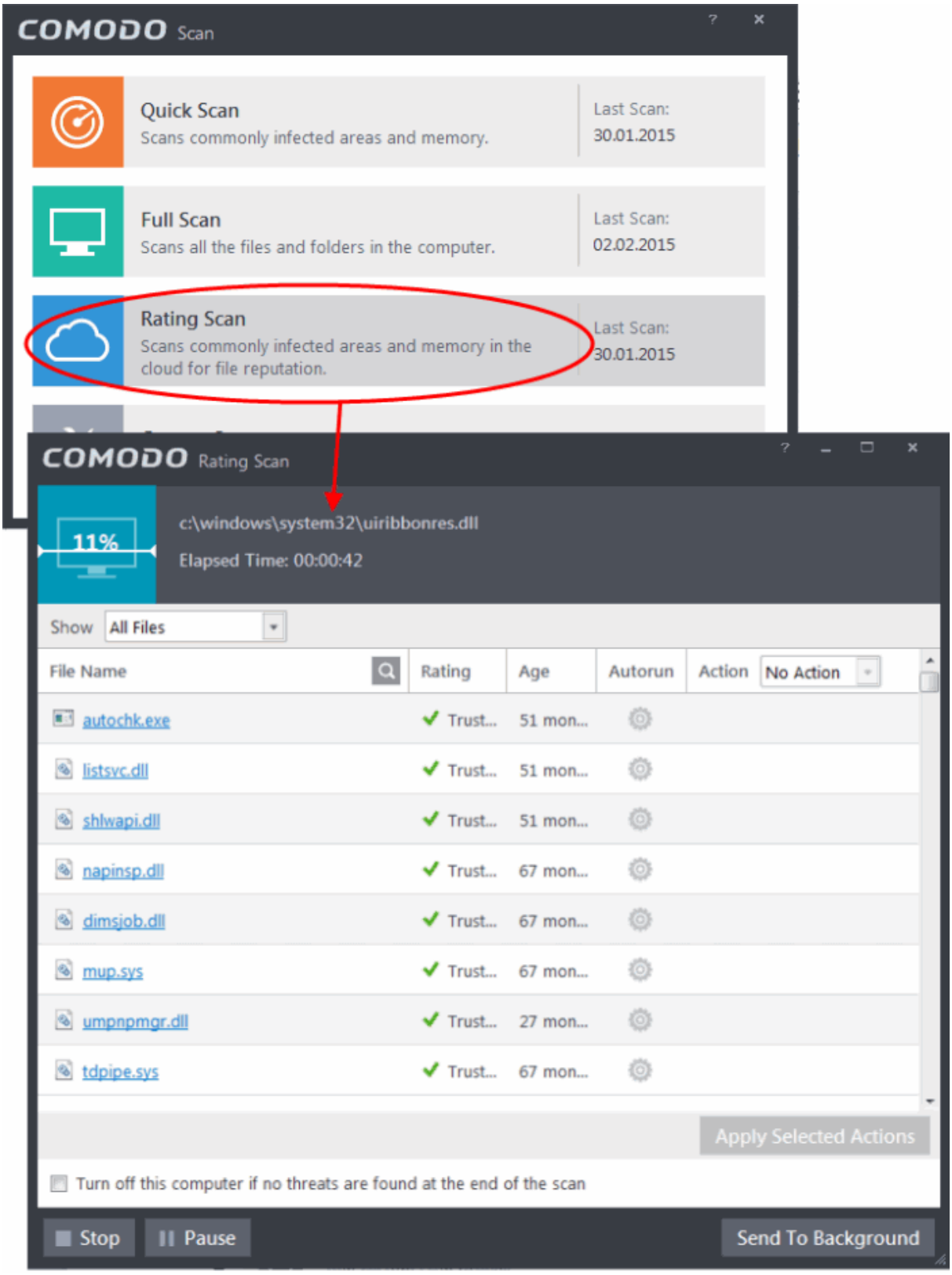
The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

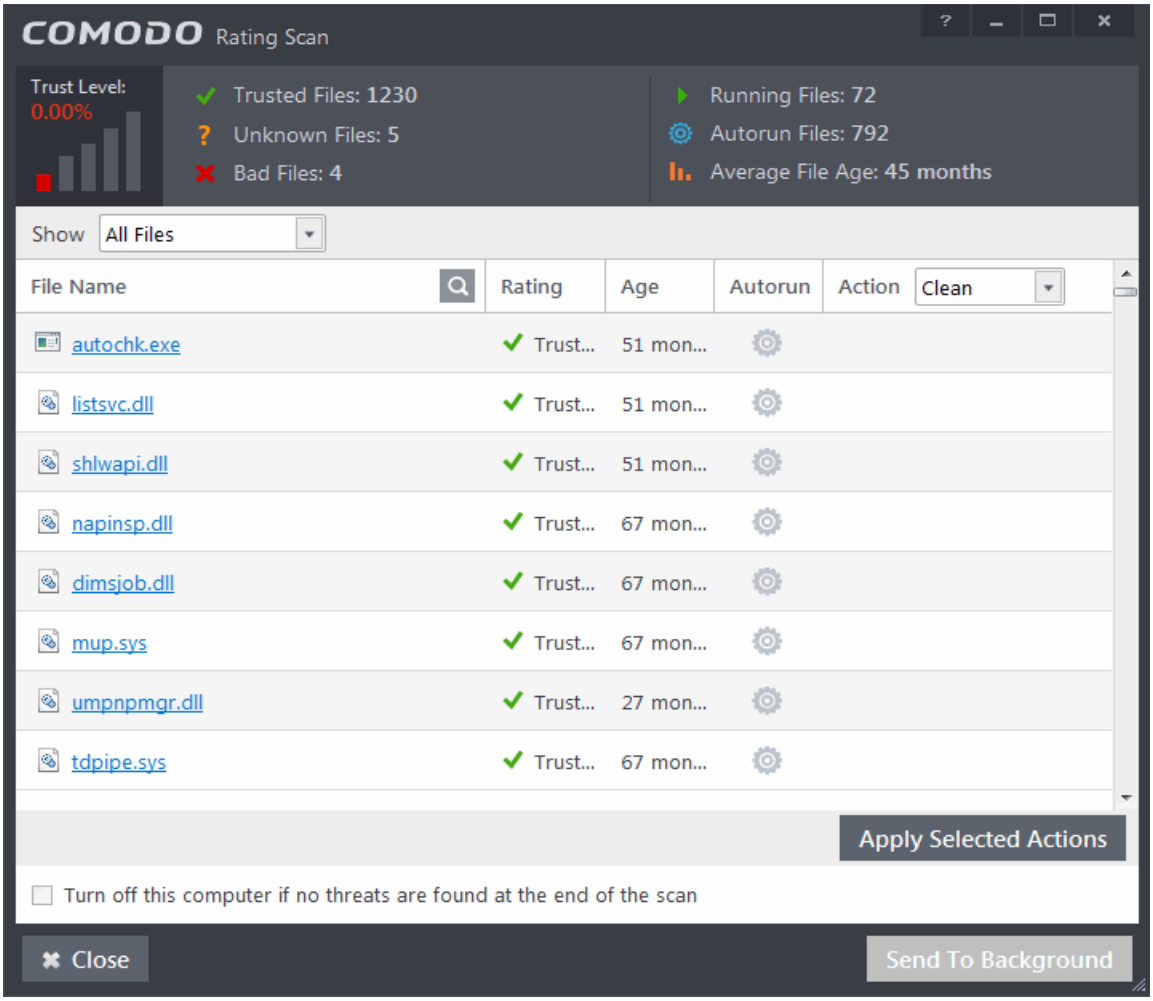
- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Bad - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

To run a Rating scan

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

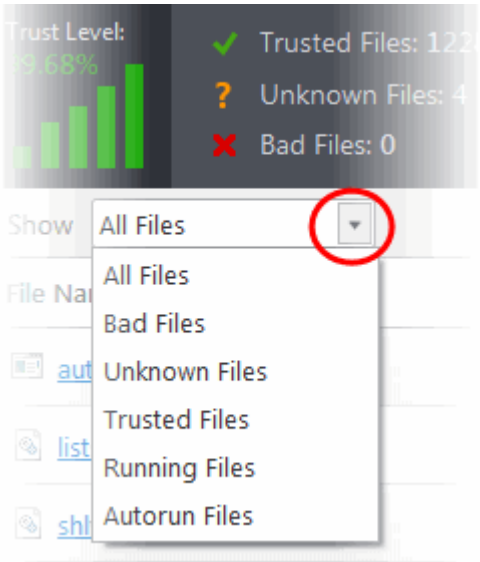


After the cloud scanners have finished their analysis, file ratings will be displayed as follows:

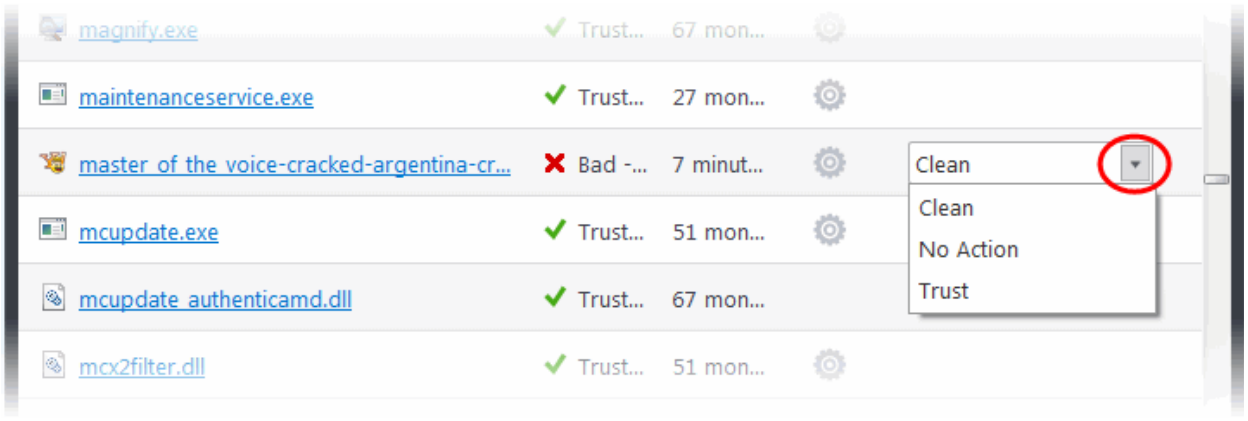


- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your computer
- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous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

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

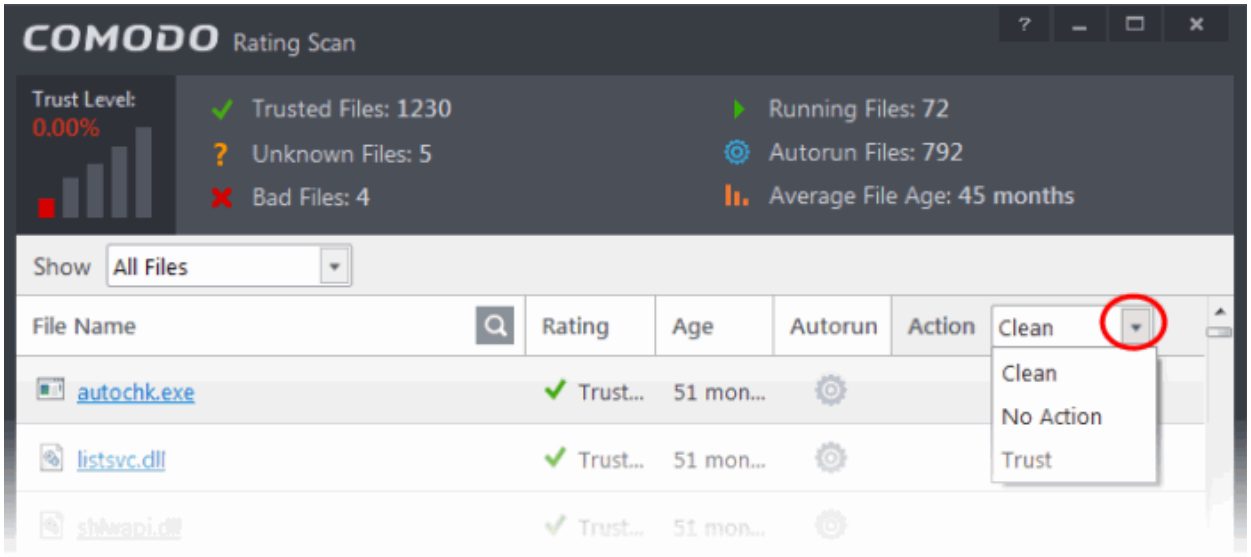


Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'



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

For the same action to be applied to all 'Bad' files, make a selection from the drop-down menu at the top of the 'Action' column.



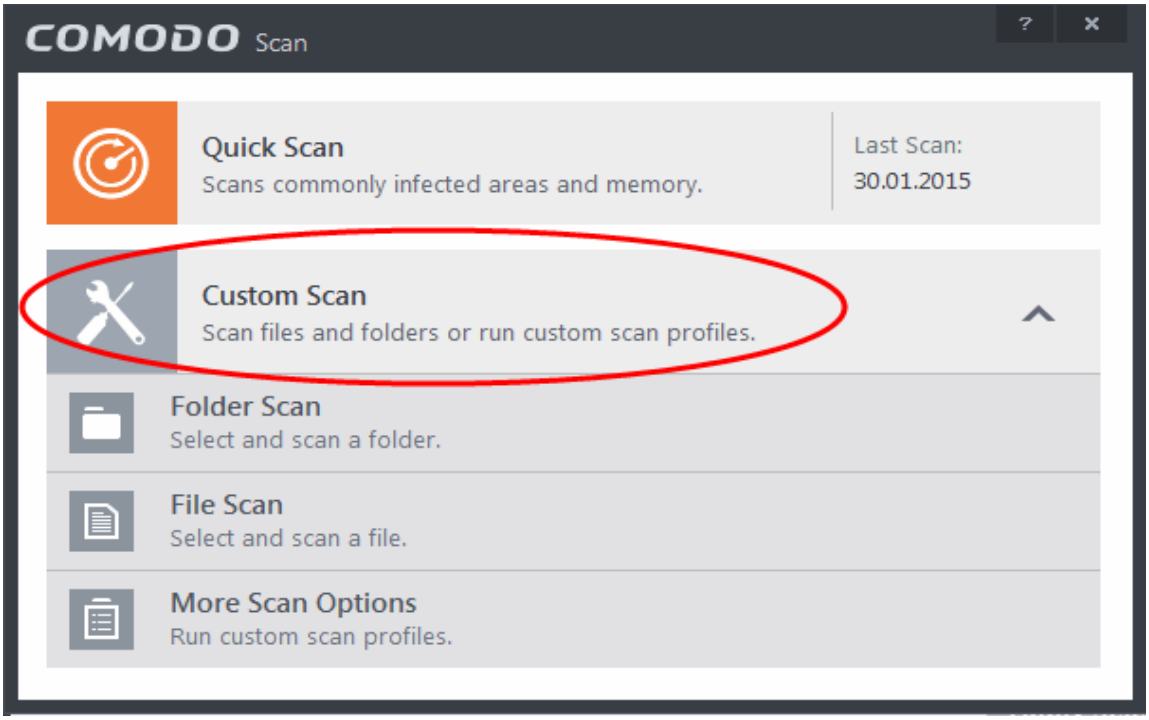
Click 'Apply Selected Actions' to implement your choice. The selected actions will be applied and a progress bar will be displayed underneath the results.

- Click 'Close' to exit.

2.1.4. Run a Custom Scan

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

To run a custom scan, click 'Scan' from the 'General Tasks' interface then click 'Custom Scan'. The Custom Scan panel will open:



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

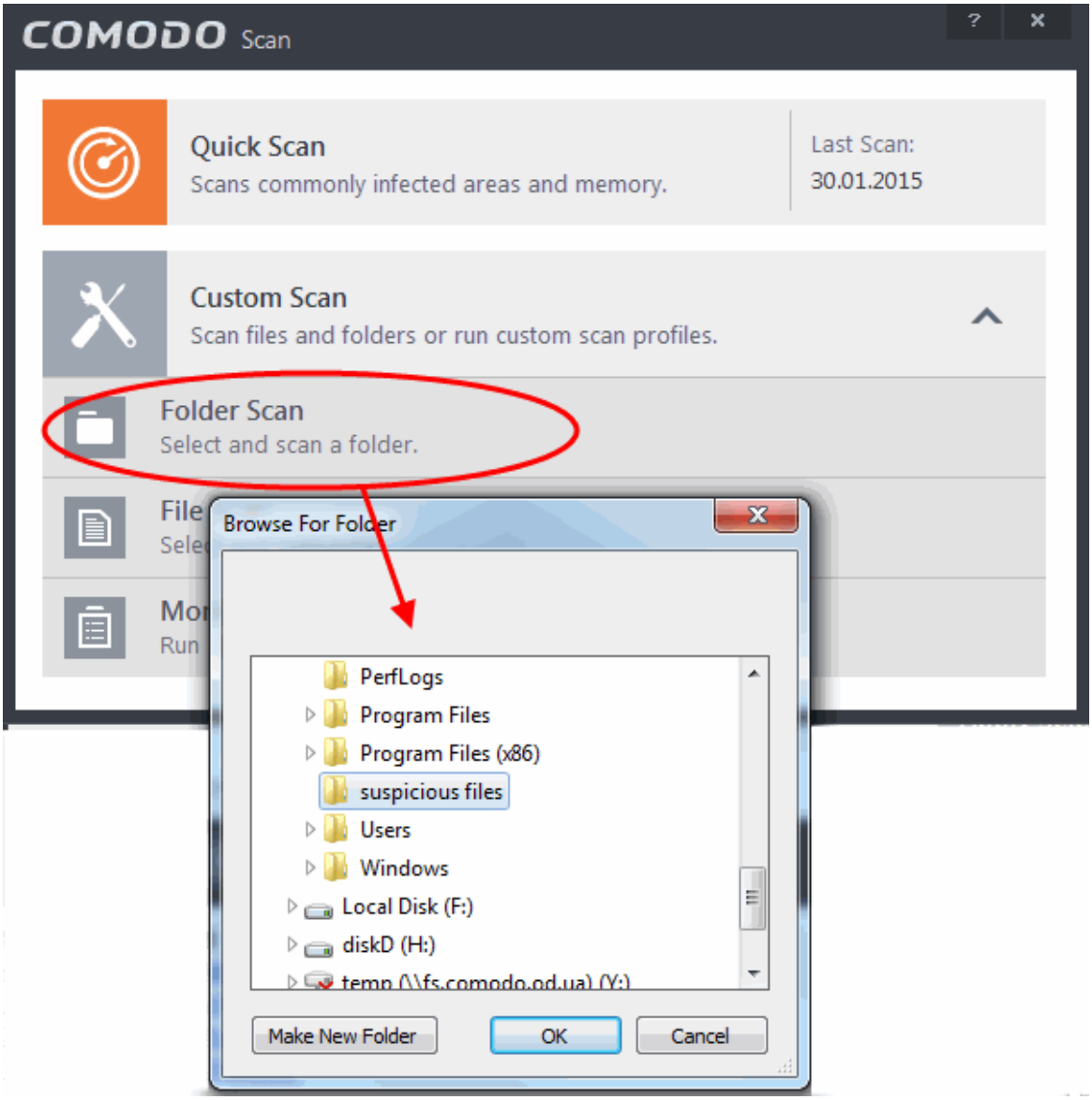
- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file
- **More Scan Options** - create a custom scan profile here

2.1.4.1. Scan a Folder

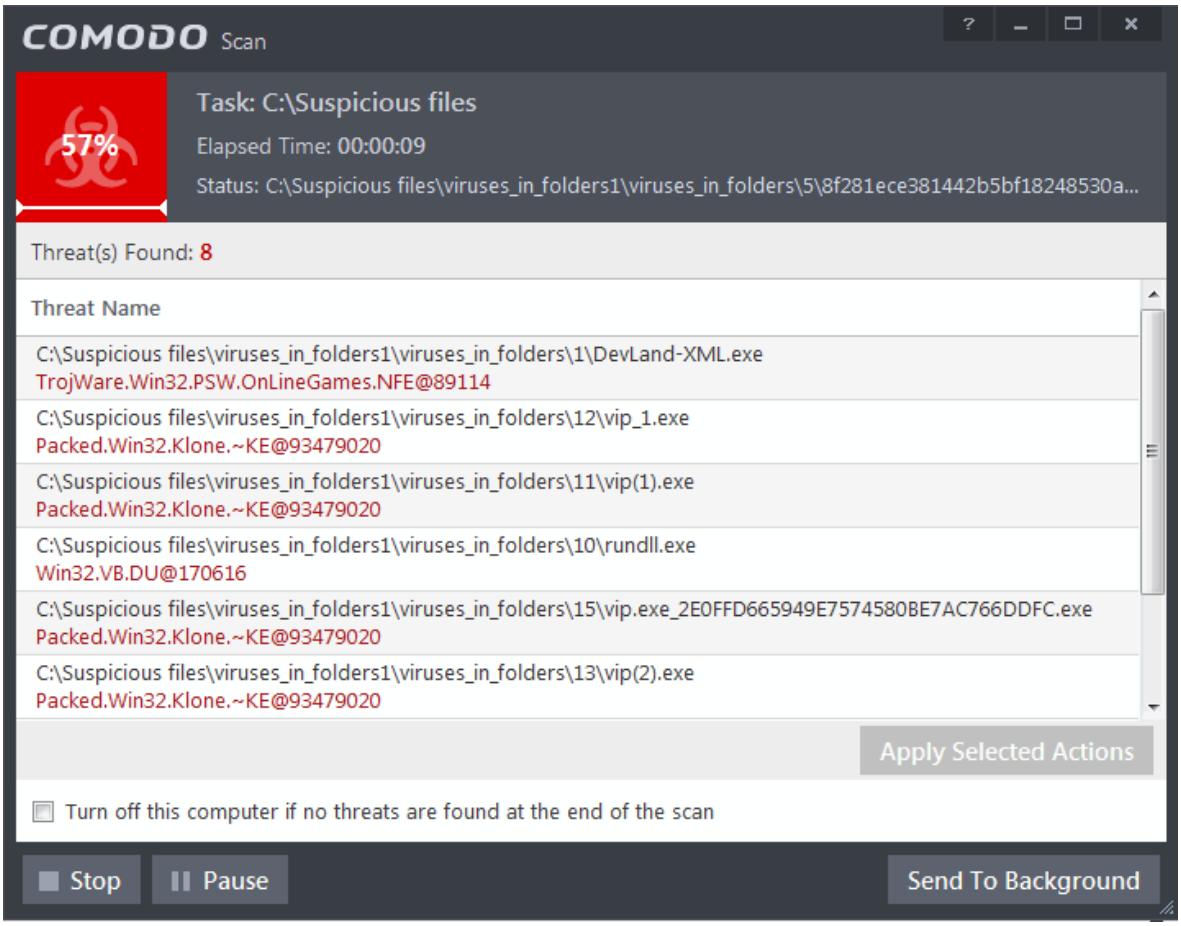
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan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

To scan a specific folder

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

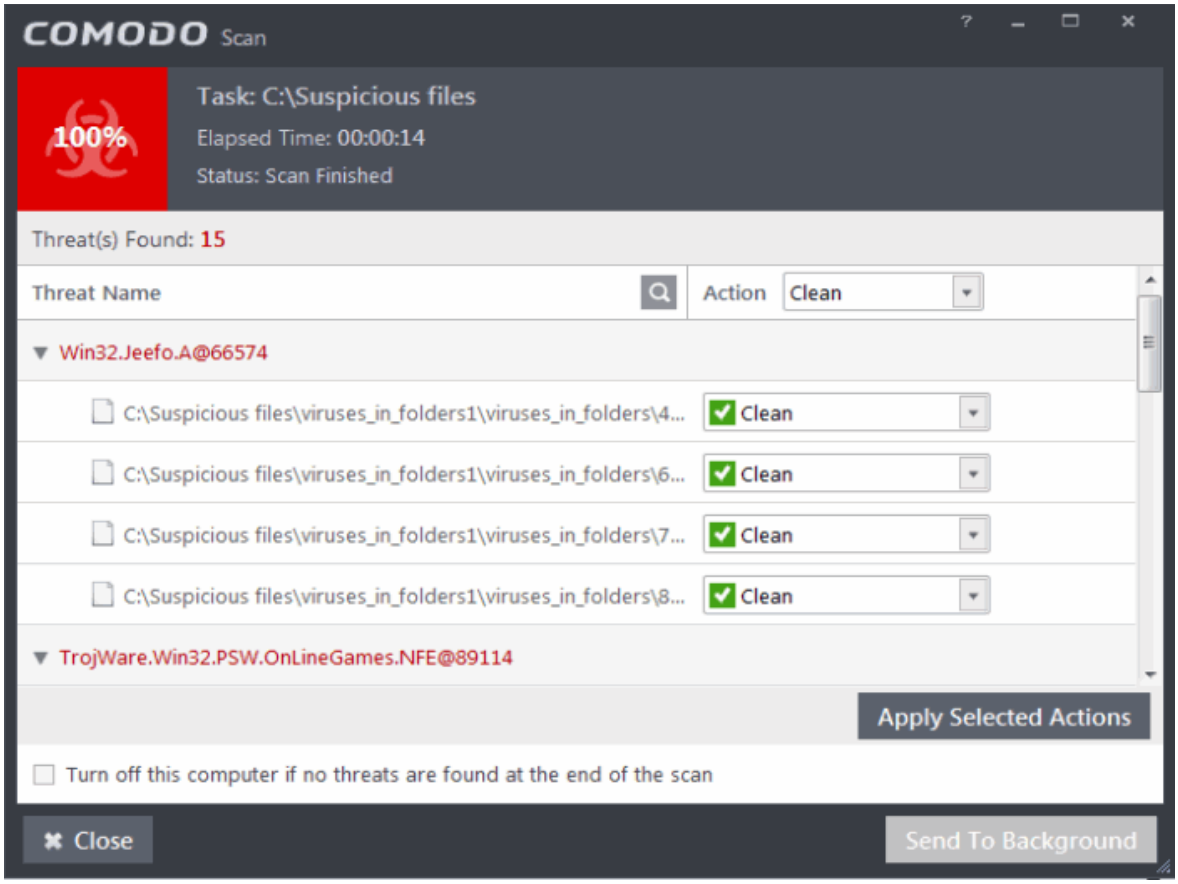


The folder will be scanned instantly and the results will be displayed with a list of any identified infections.



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

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



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

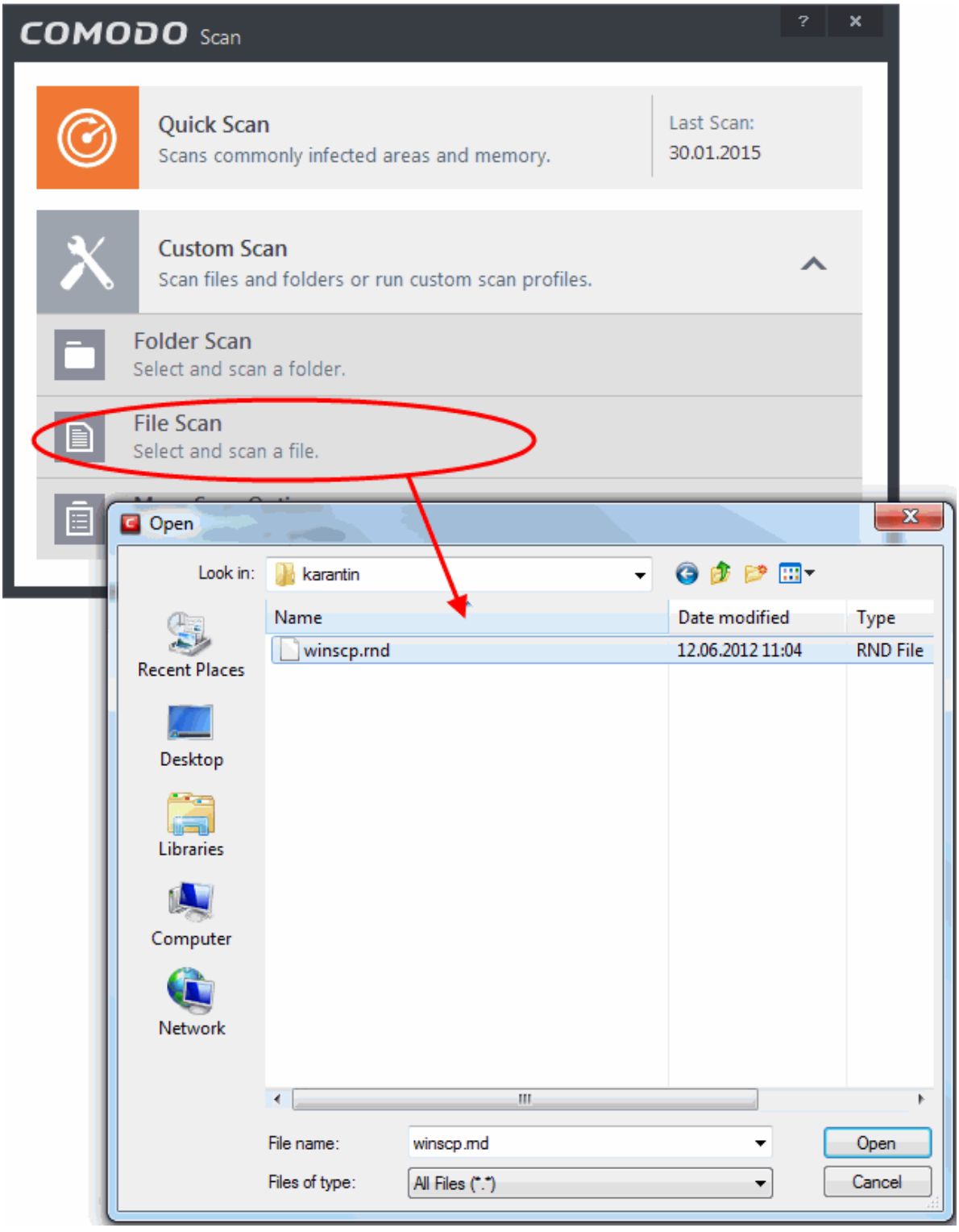
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CIS interface or by right clicking it. Refer to **Scan Individual File/Folder** for more details.

2.1.4.2. Scan a File

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

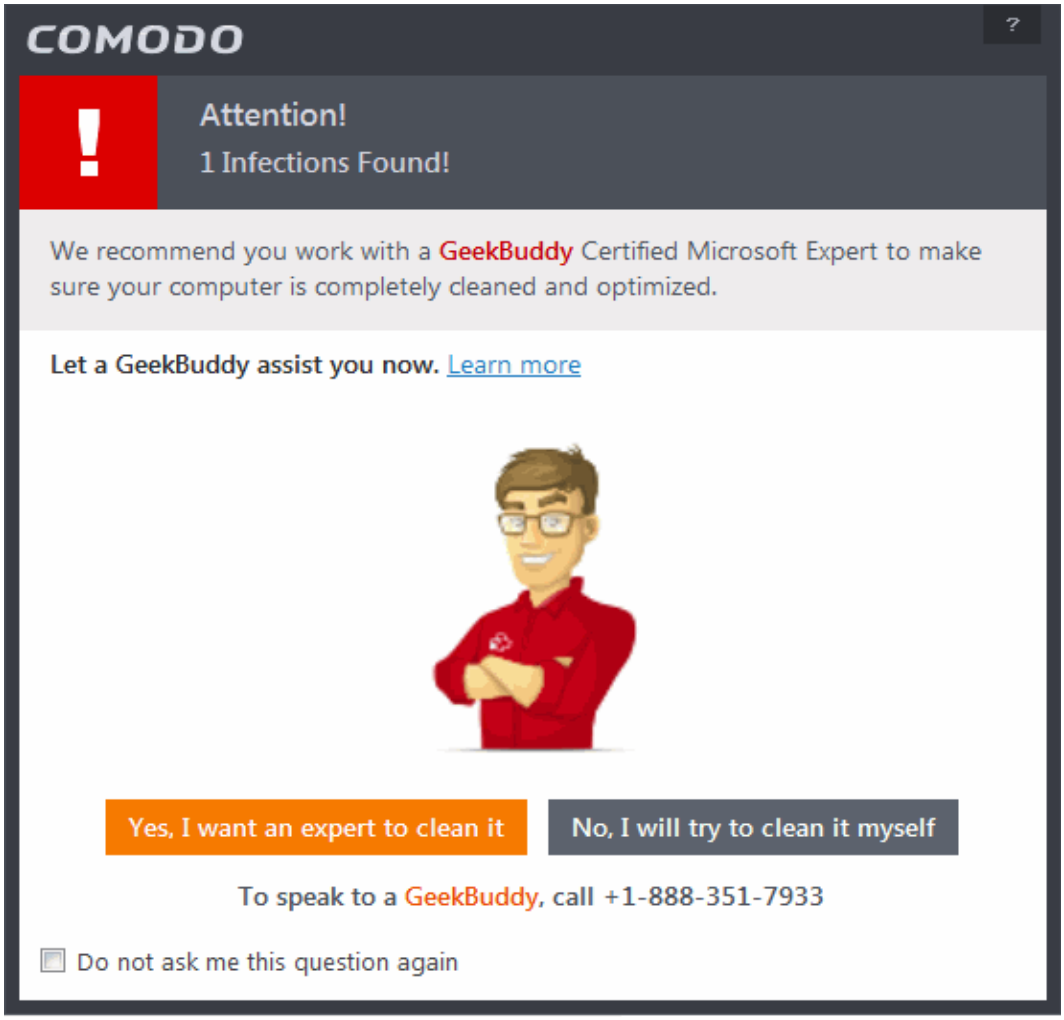
To scan a specific file

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

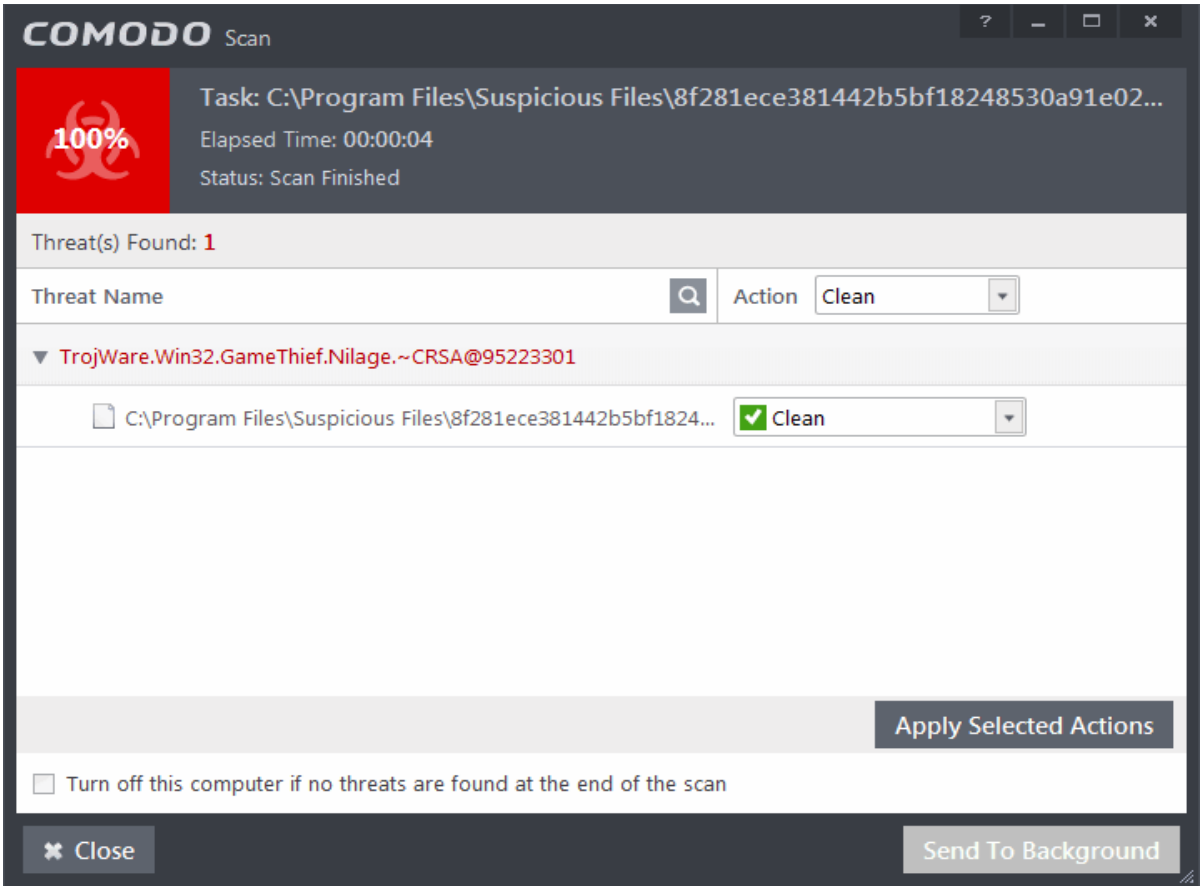


The file will be scanned instantly.

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



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



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

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

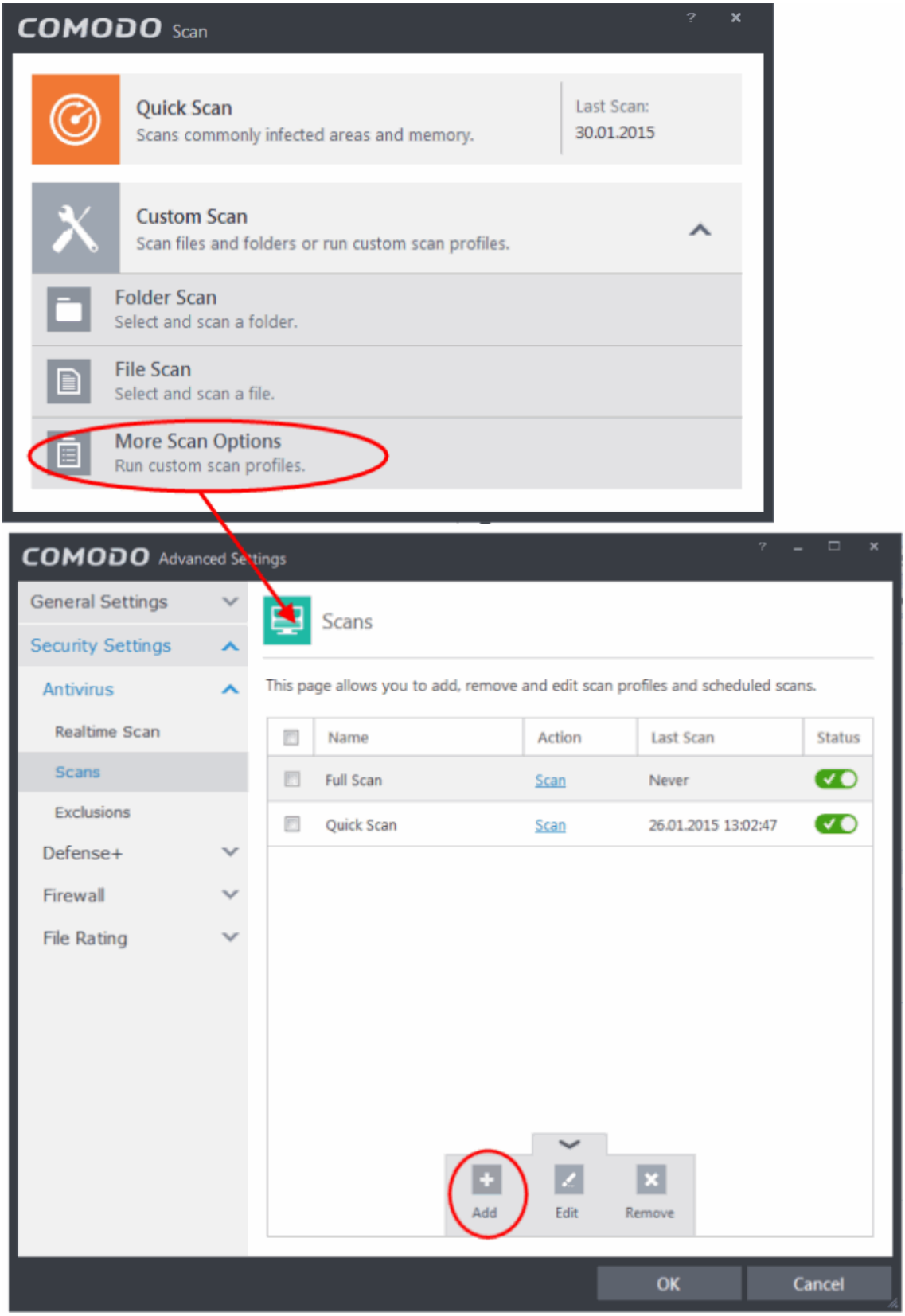
2.1.4.3. Create, Schedule and Run a Custom Scan

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

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

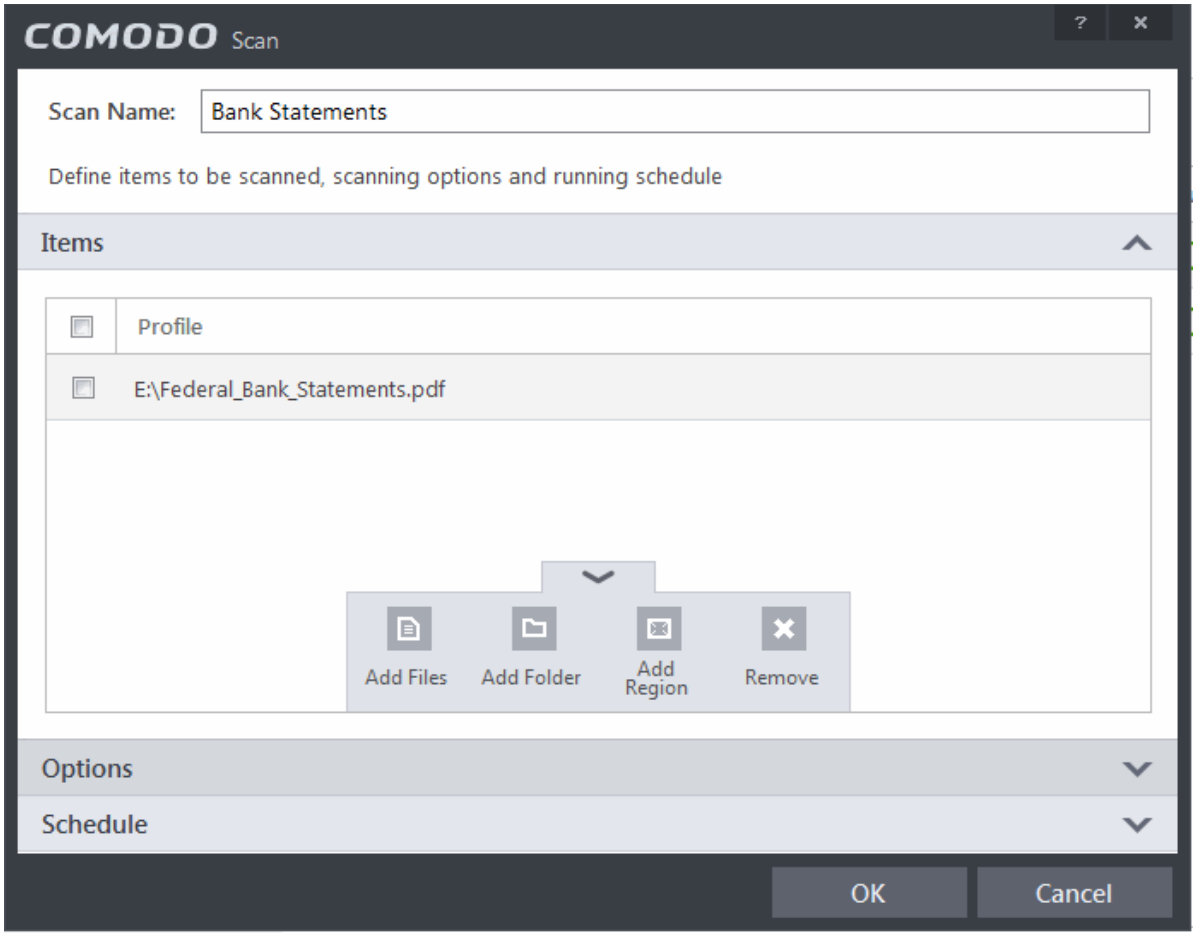
To create a custom profile

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

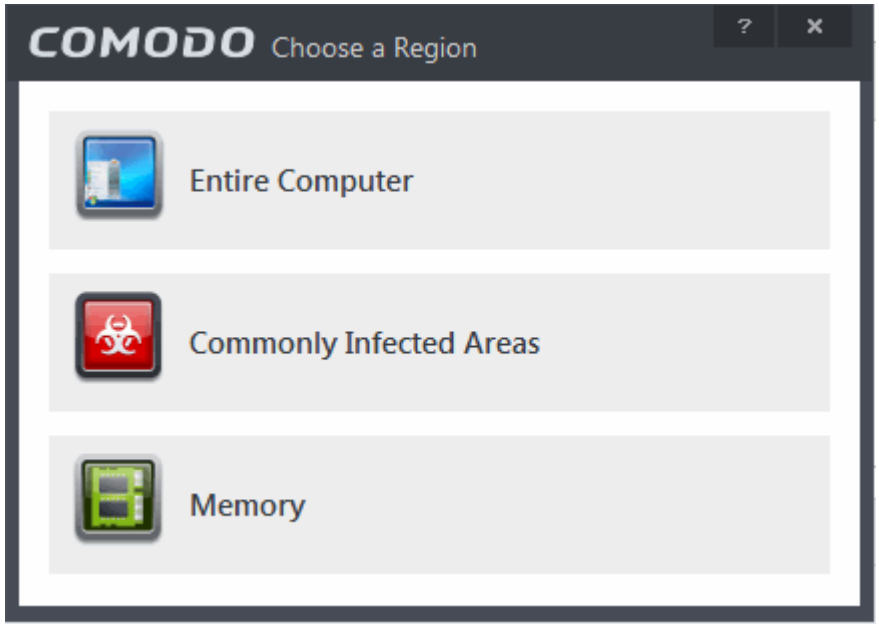


The scan profile interface will be displayed.

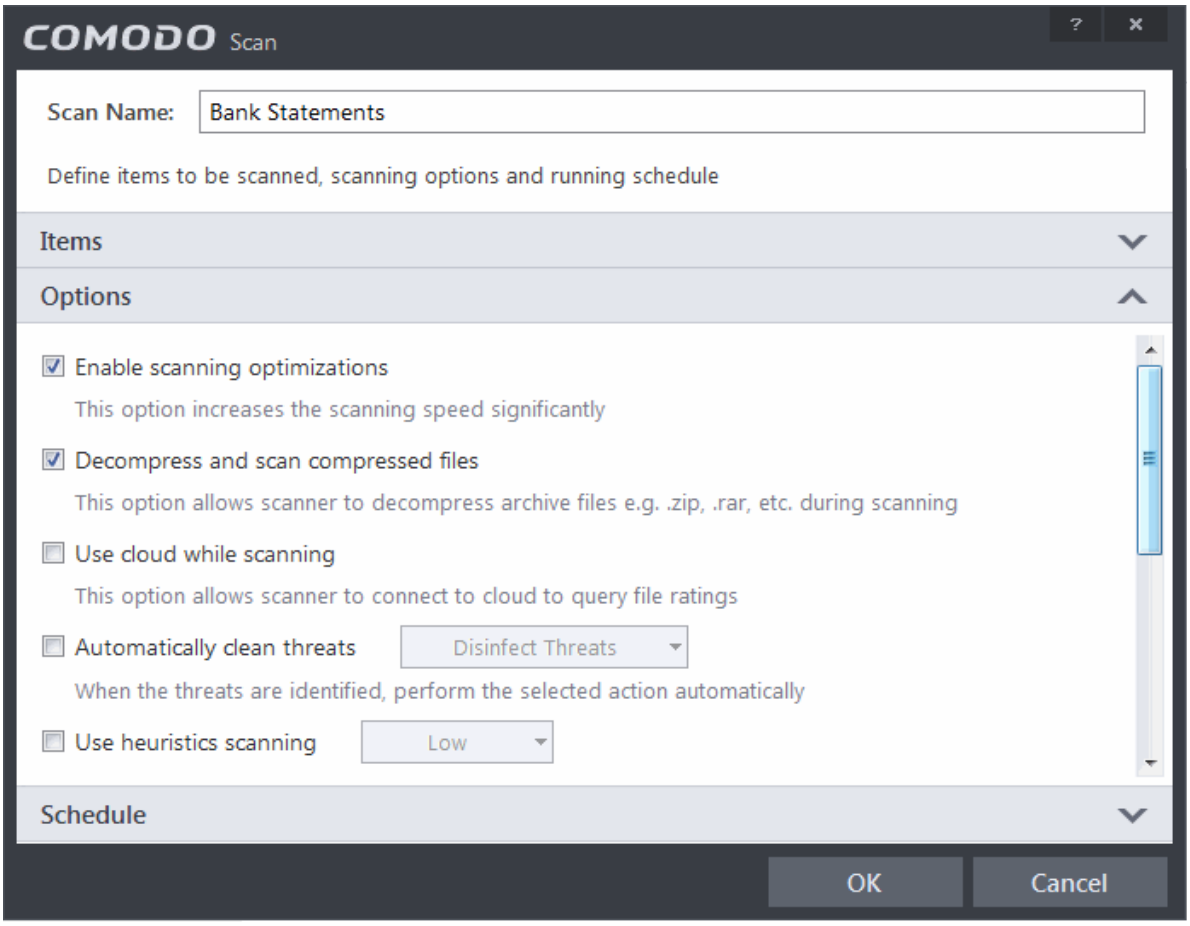
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



- **Add File** - Allows you to add individual files to the profile.
- **Add Folder** - Allows you to select entire folders to be included in the profile
- **Add Region** - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas' and 'System Memory')



- Repeat the process to add more items to the profile. Click 'OK' to confirm your choice.
- Next, click 'Options' to further customize the scan:



- **Options:**
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)*** .
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
  - **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local anitvirus database is out-dated. ***(Default = Disabled)***.
  - **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine.
  - **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Disabled).***

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

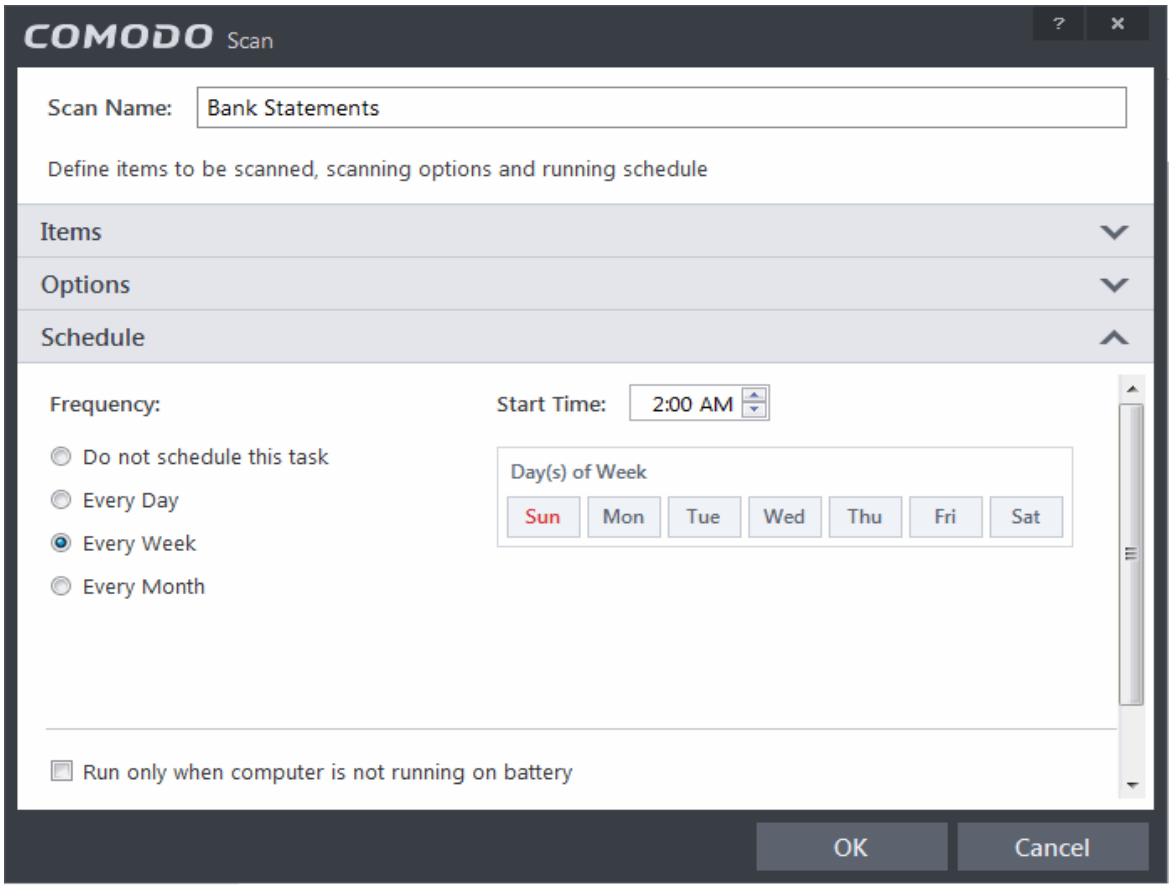
    This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

    - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
    - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.

- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run this scan with** - Enables you to set the priority of the scan profile. You can select the priority from the drop-down.(***Default = Disabled***).
- **Update virus database before running** - Instructs Comodo Internet Security to check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning (***Default = Enabled***) .
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (***Default = Enabled***).

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



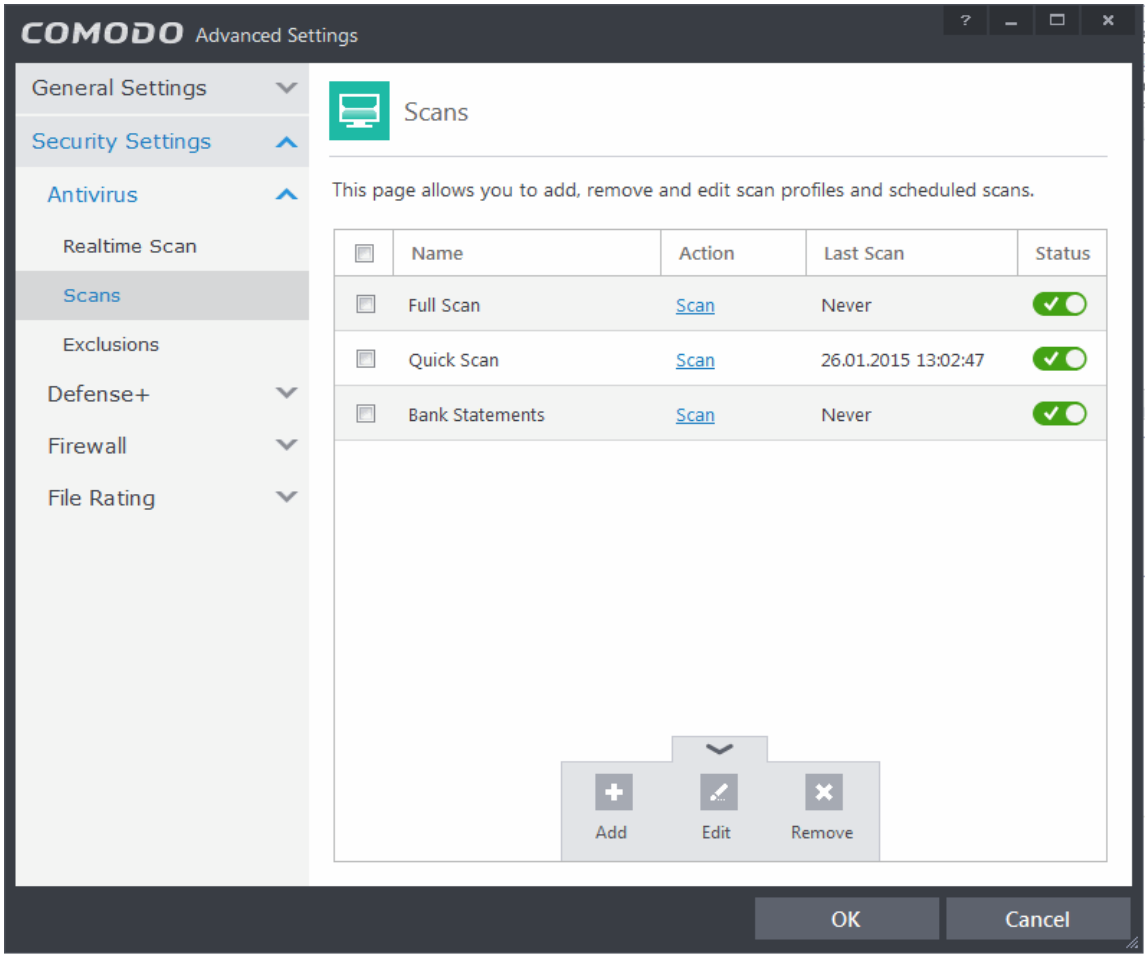
- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - The Antivurus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
- **Every Week** - The Antivurus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - The Antivurus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.

- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
- **Run only when computer is IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.

- Click OK to save the profile.

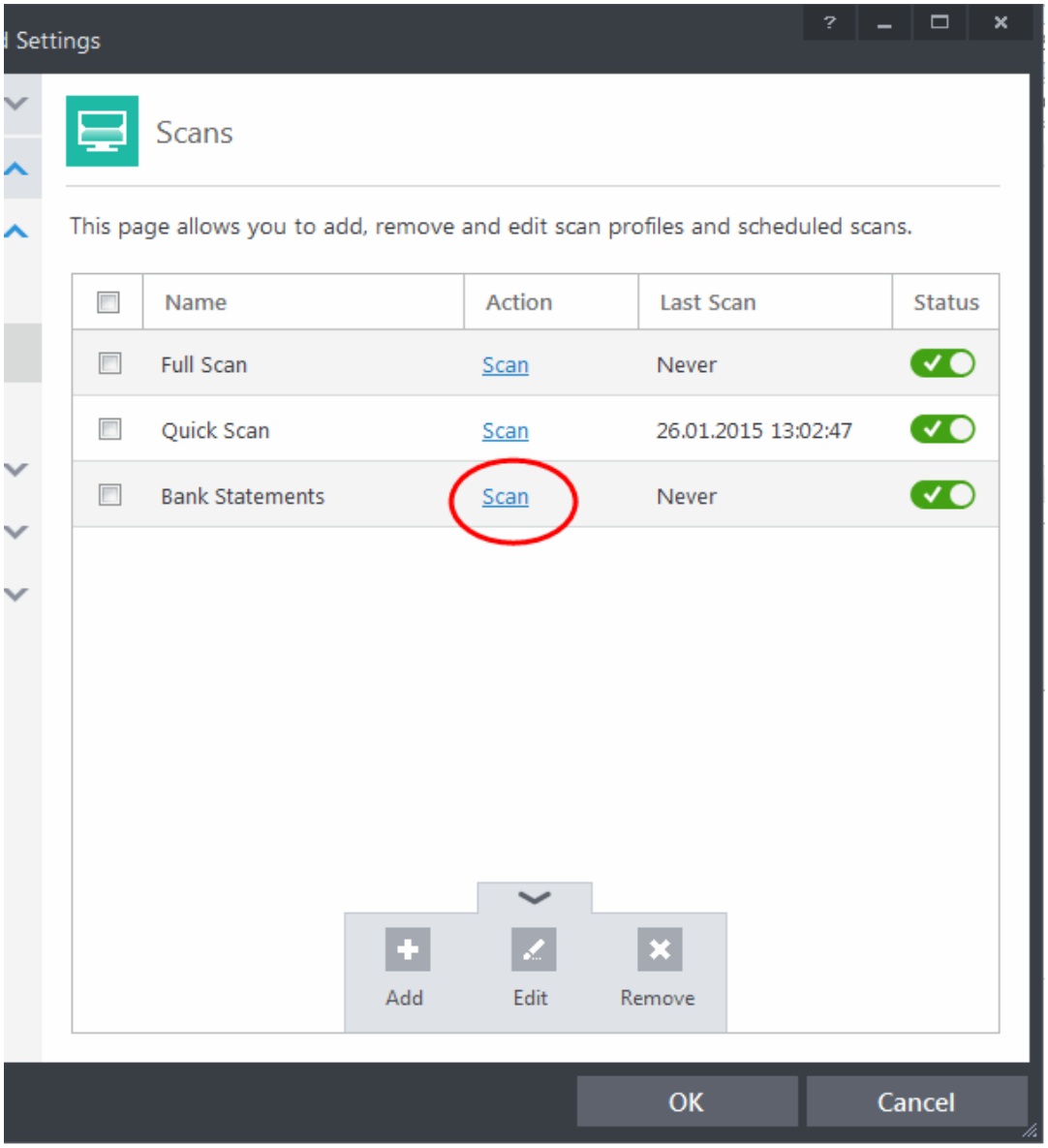
Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.

The profile will be available for deployment in future.

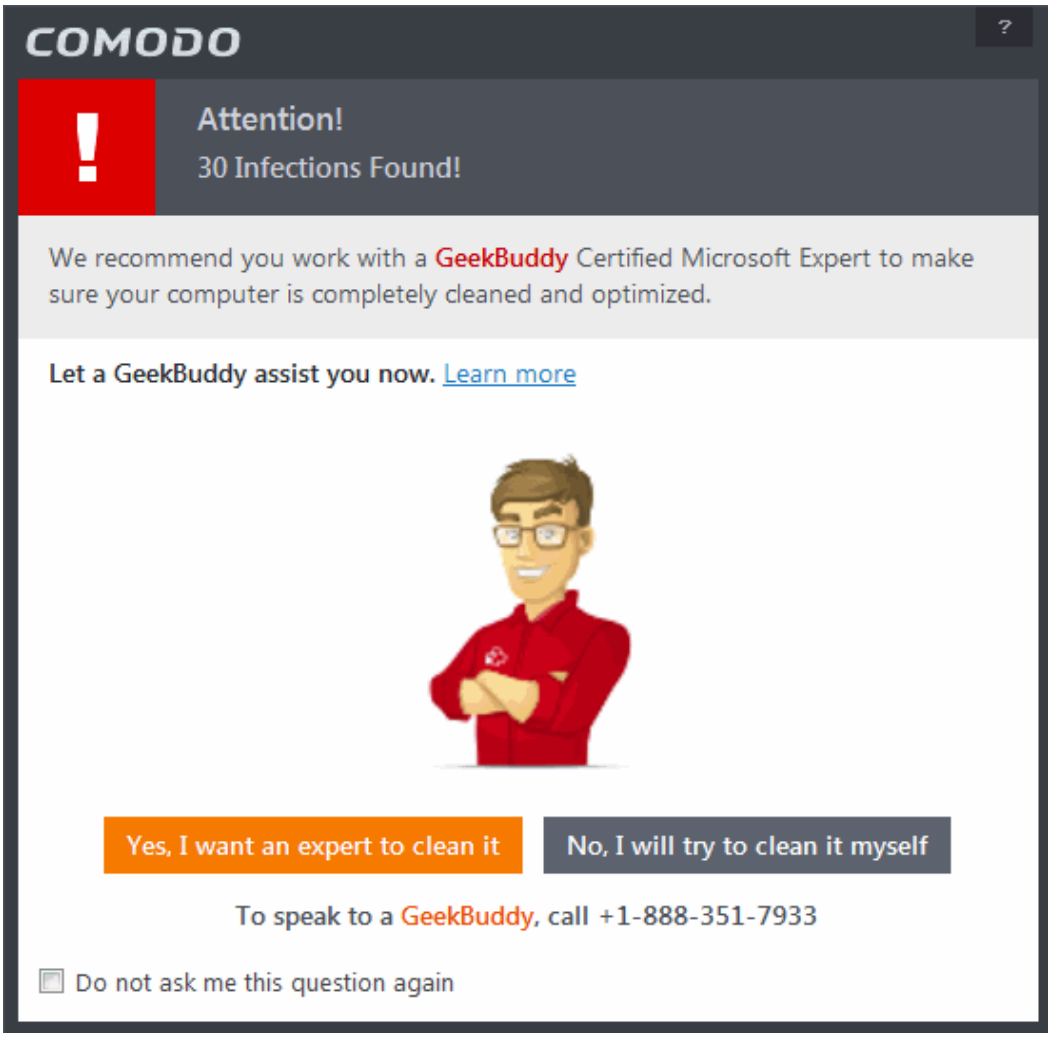


To run a custom scan

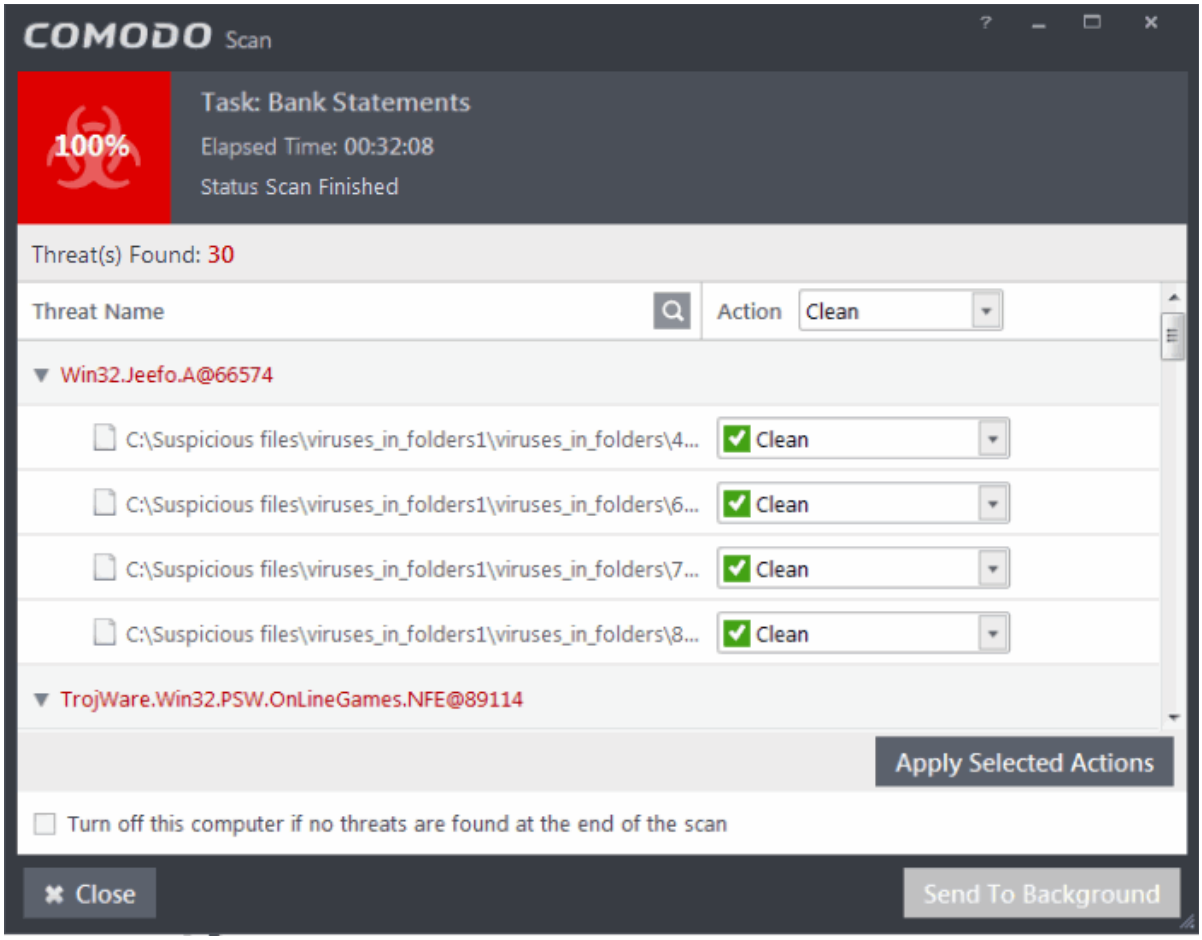
- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click 'Scan' beside the required scan profile.



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



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



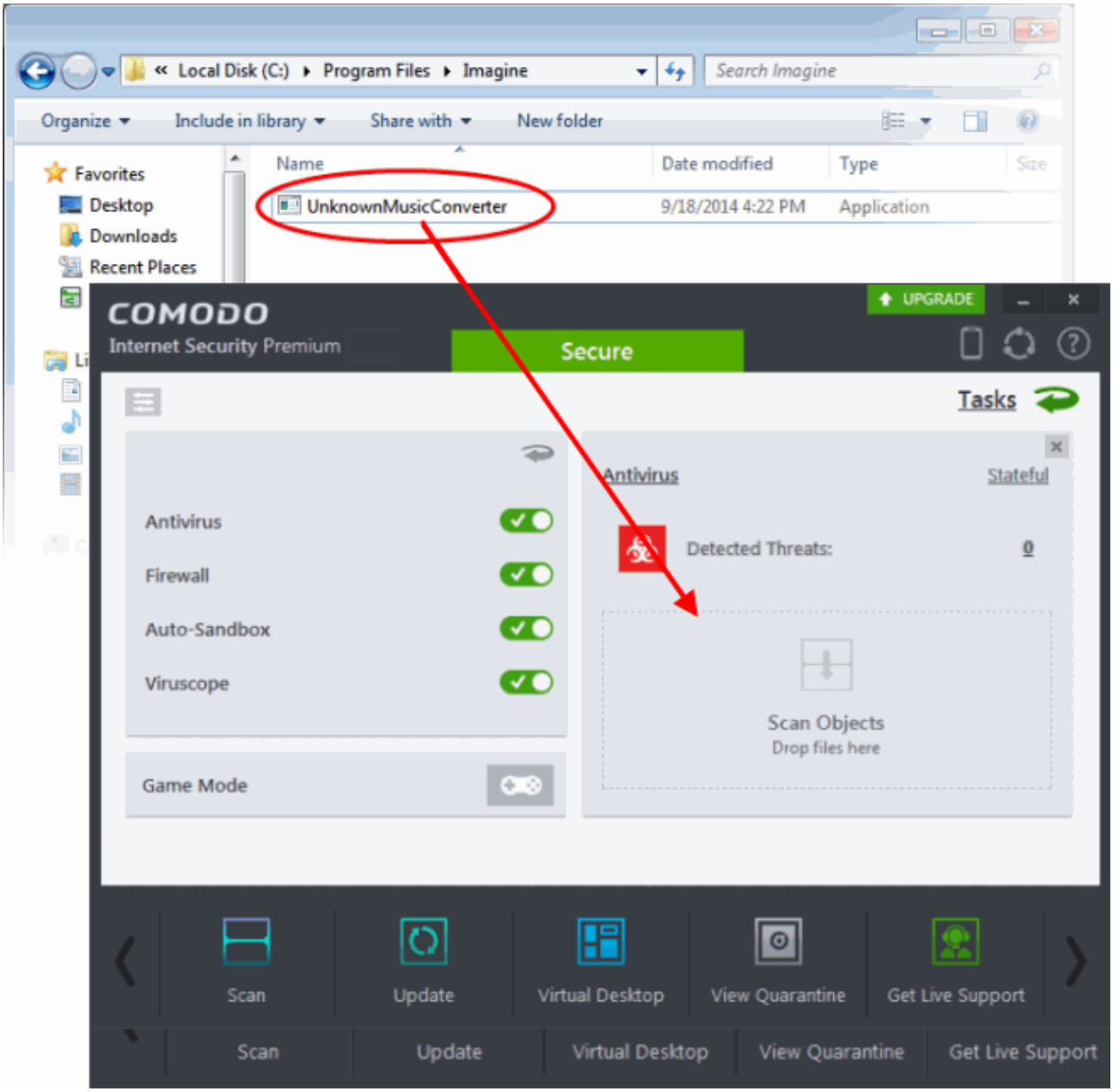
- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to **Processing the infected files** for more details.

2.2. Instantly Scan Files and Folders

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

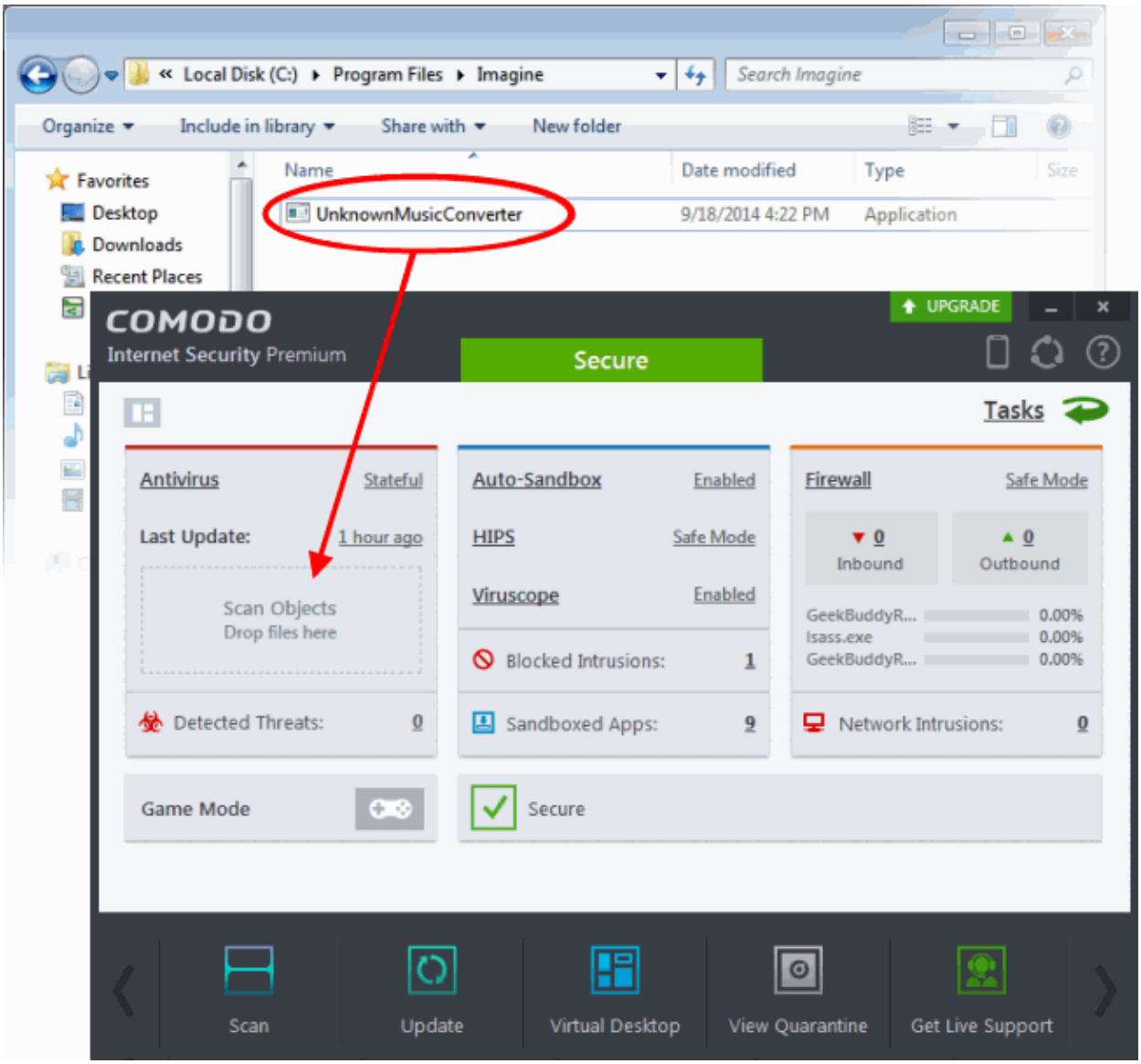
To instantly scan an item

- Click the Antivrus tile at the 'Home' screen in compact view to flip-open the Antivirus pane
- Drag and drop the item over the area marked 'Scan Objects'.



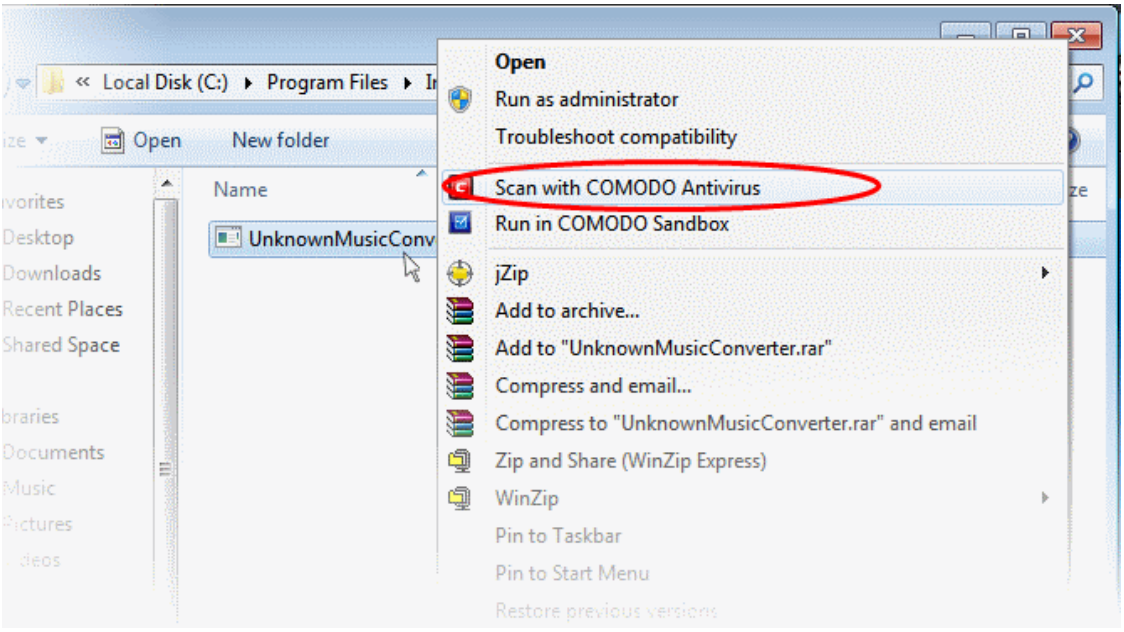
OR

- Switch to 'Advanced' View of the 'Home' screen by clicking the button at the top left of the home screen.
- Drag and drop the item over the area marked 'Scan Objects'.

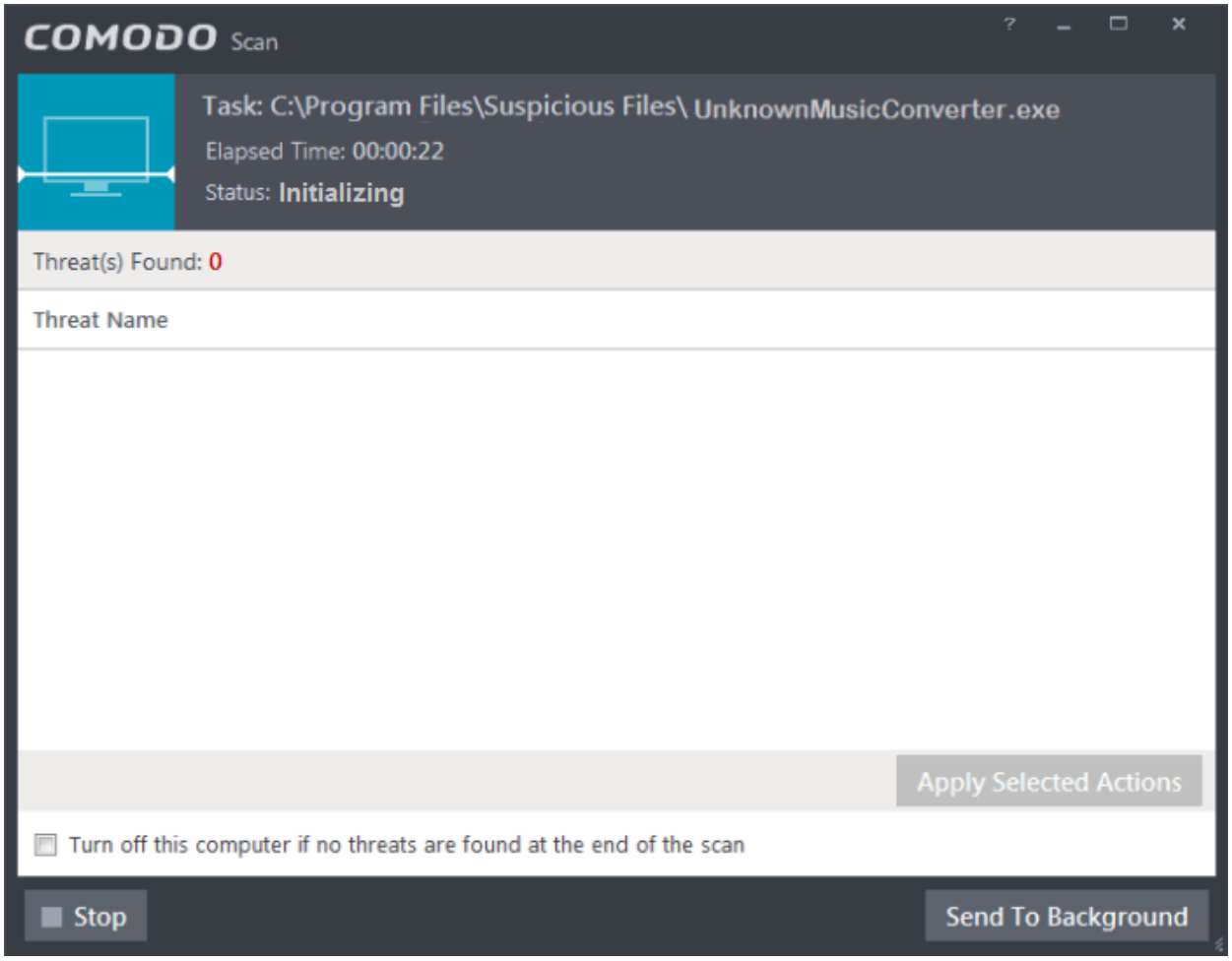


OR

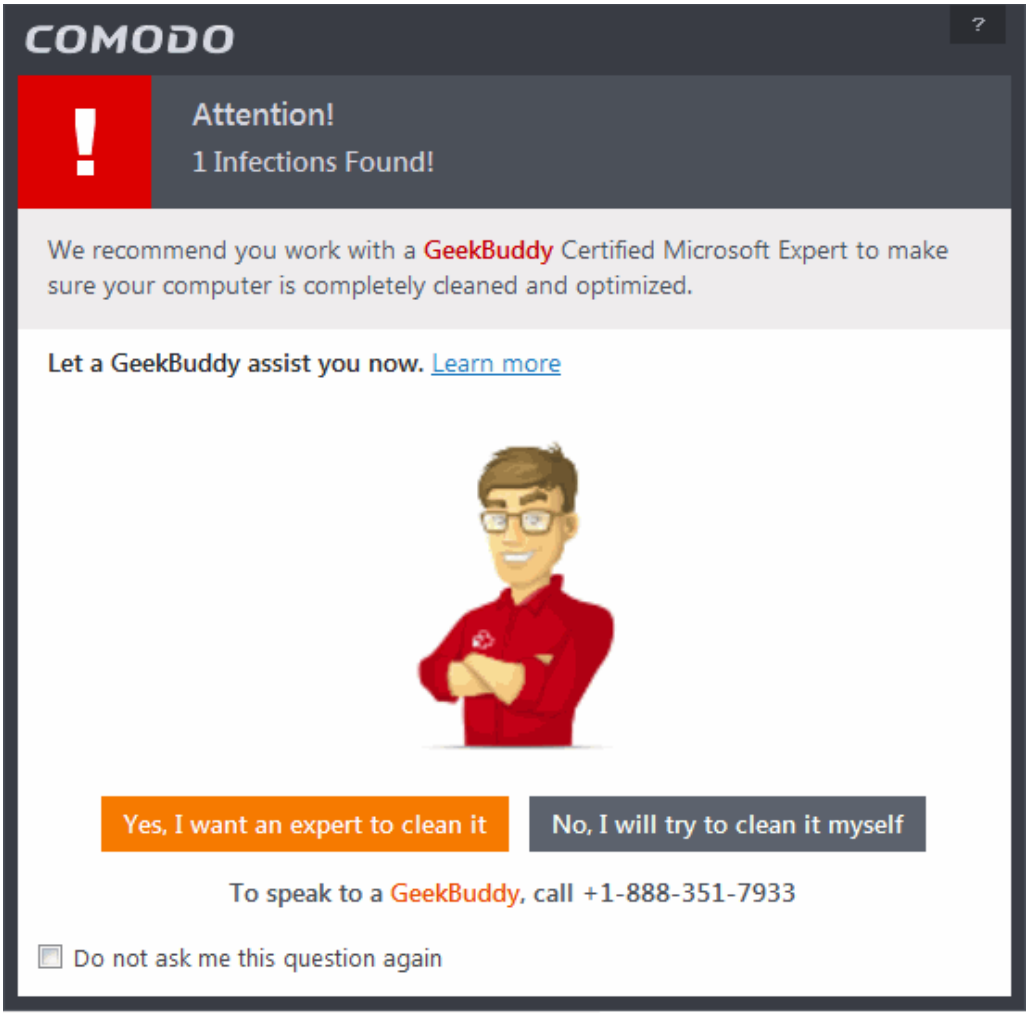
- Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



The item will be scanned immediately.



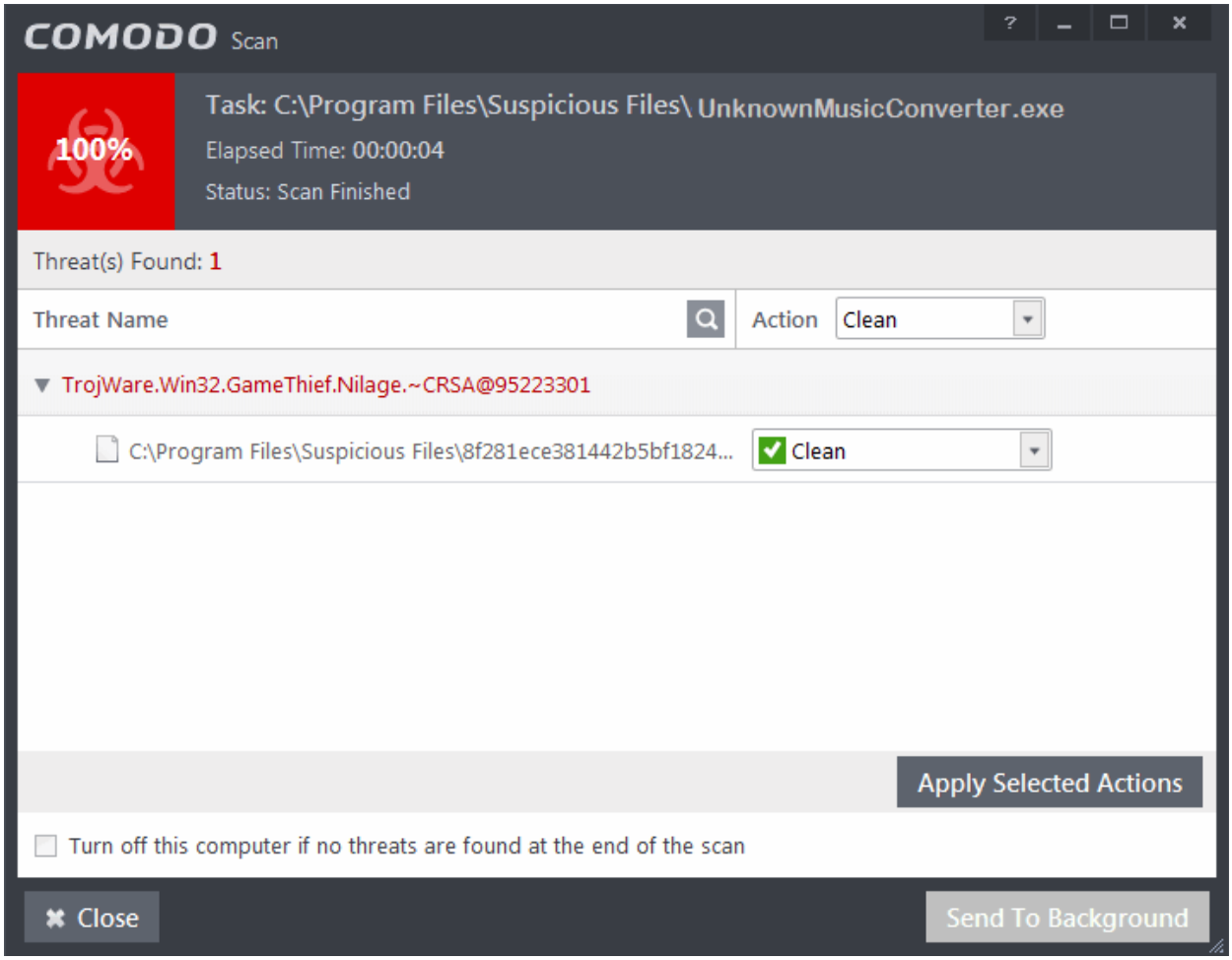
- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



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

  For more details on GeekBuddy Expert help, refer to the section **Comodo GeekBuddy**.

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

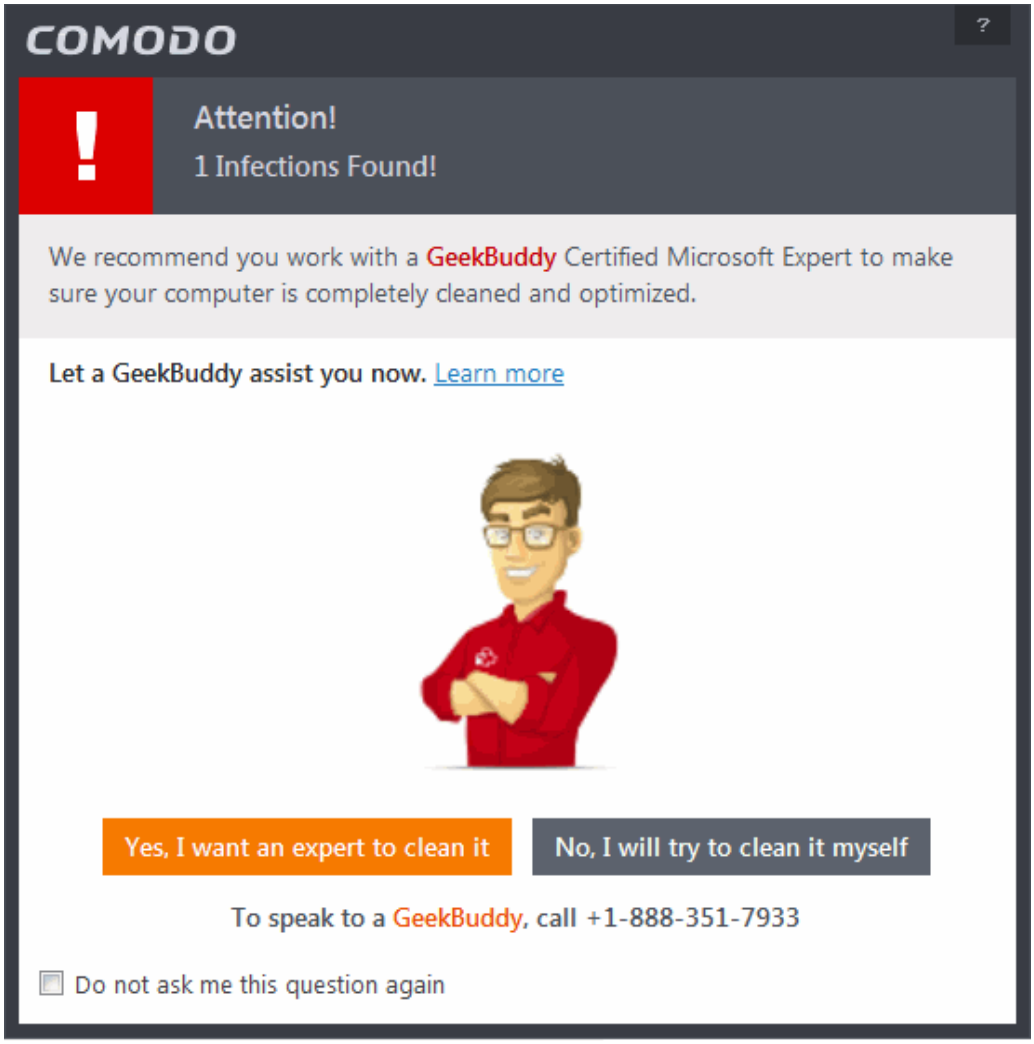


You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to **Processing the infected files** for more details.

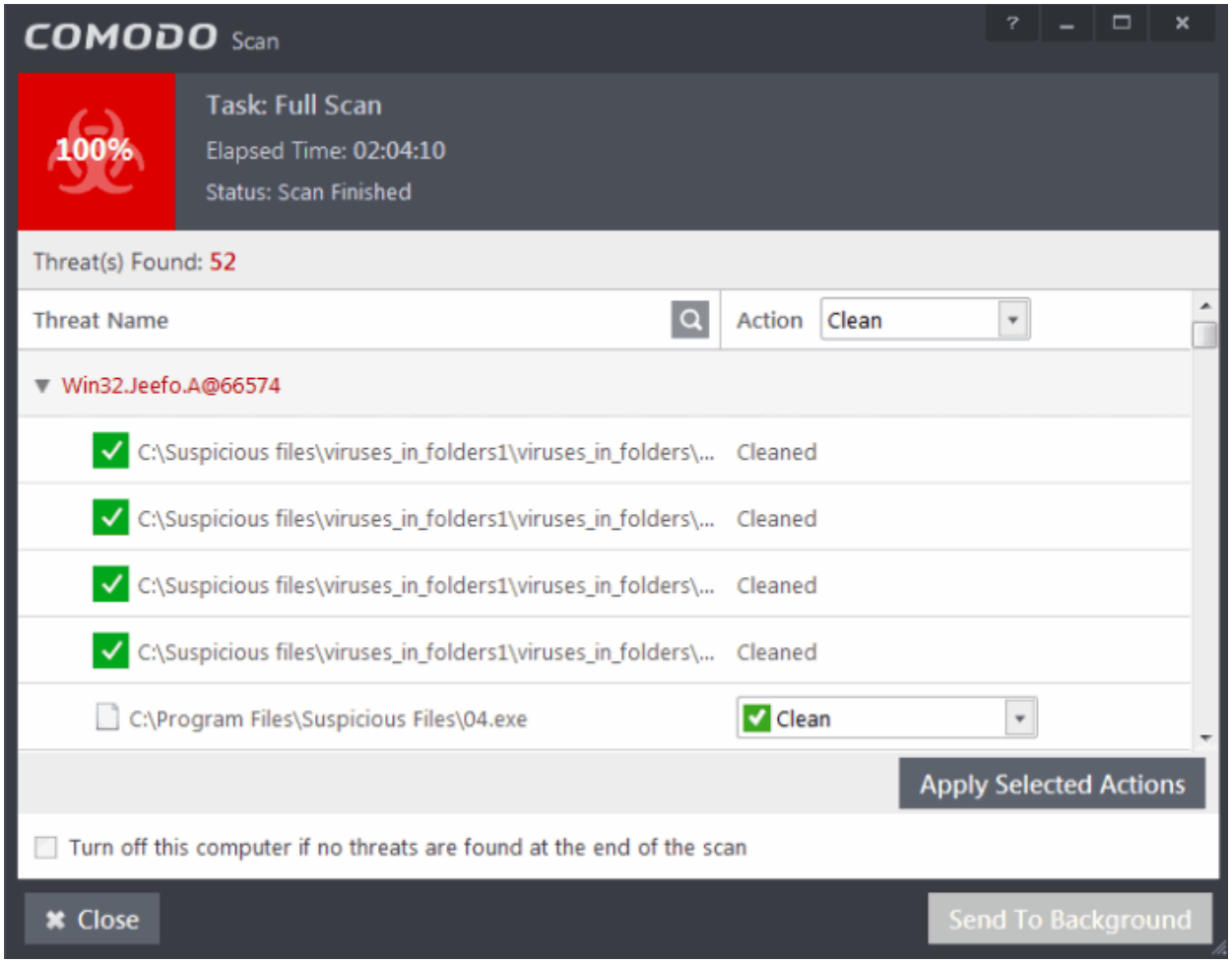
2.3. Processing Infected Files

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

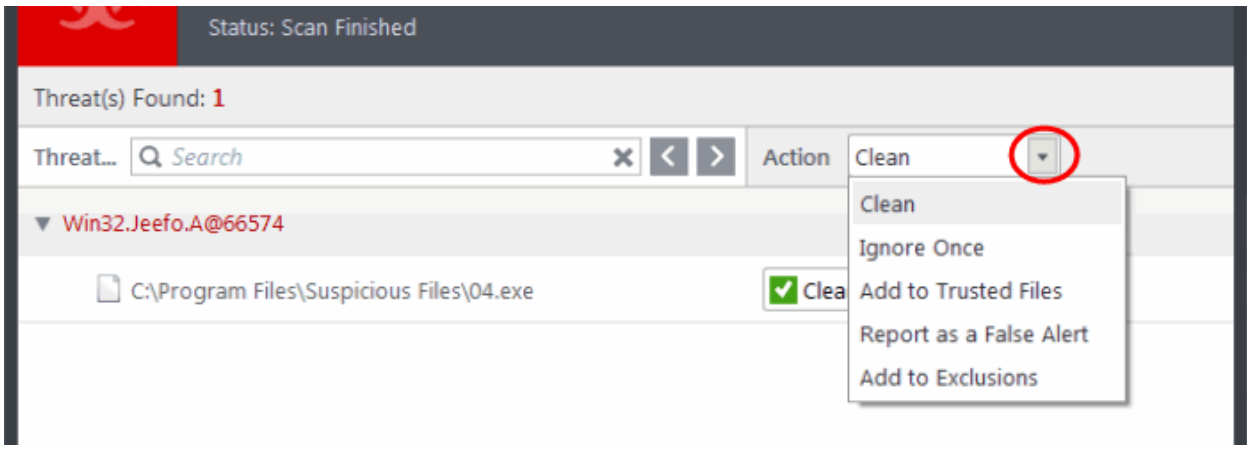
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - For more details on GeekBuddy Expert help, refer to the section **Comodo GeekBuddy**.



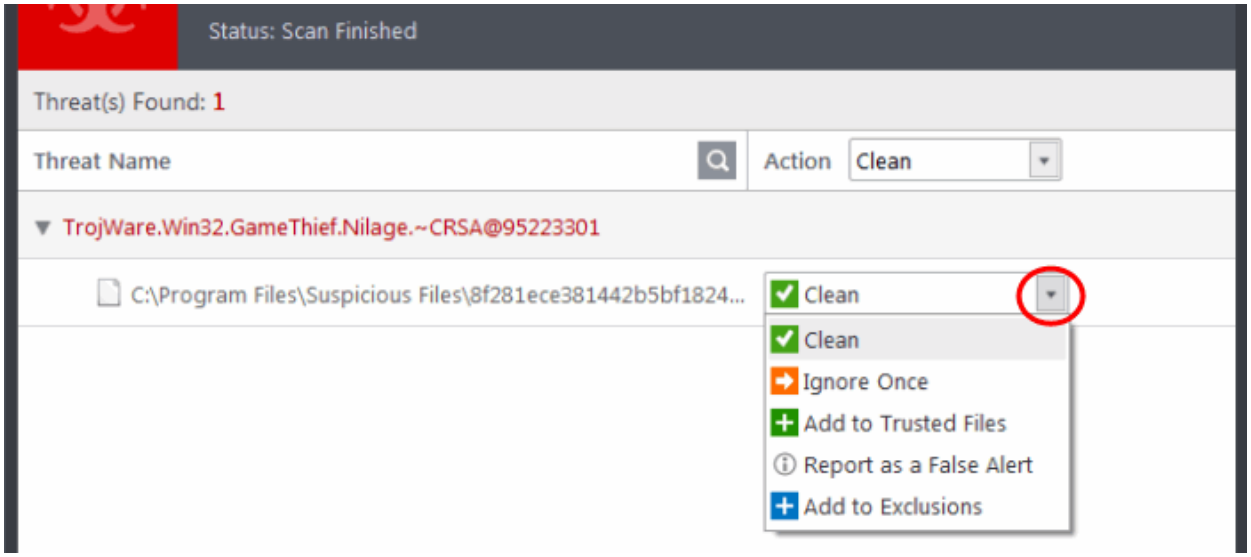
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



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



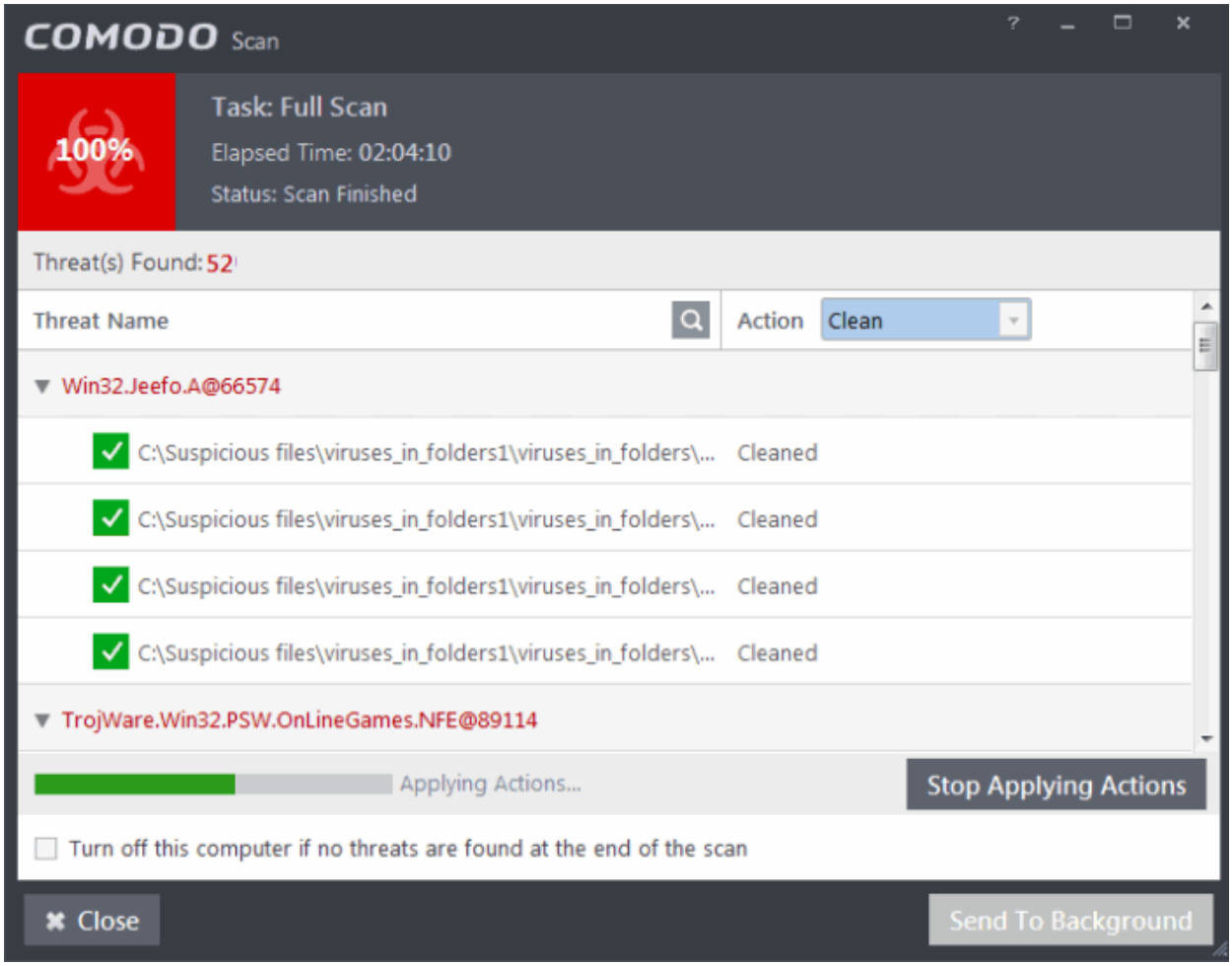
… or the actions to be applied to individual items from the drop-down beside each item.



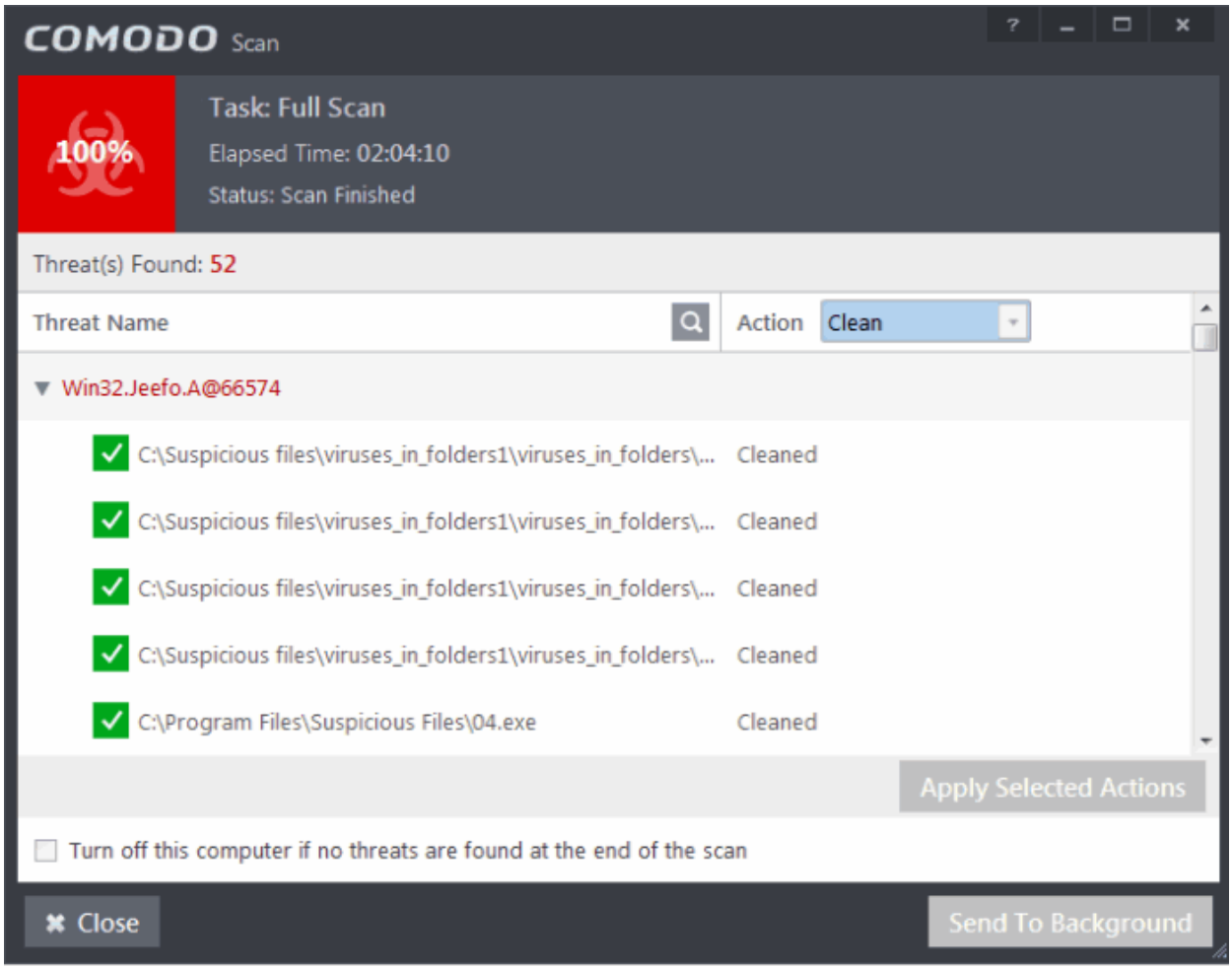
The choices for the actions available are:

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

- After selecting the action(s) to be applied, click 'Apply Selected Actions'. The files will be treated as per the action selected and the progress will be displayed.



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



- Click 'Close' to close the results window.

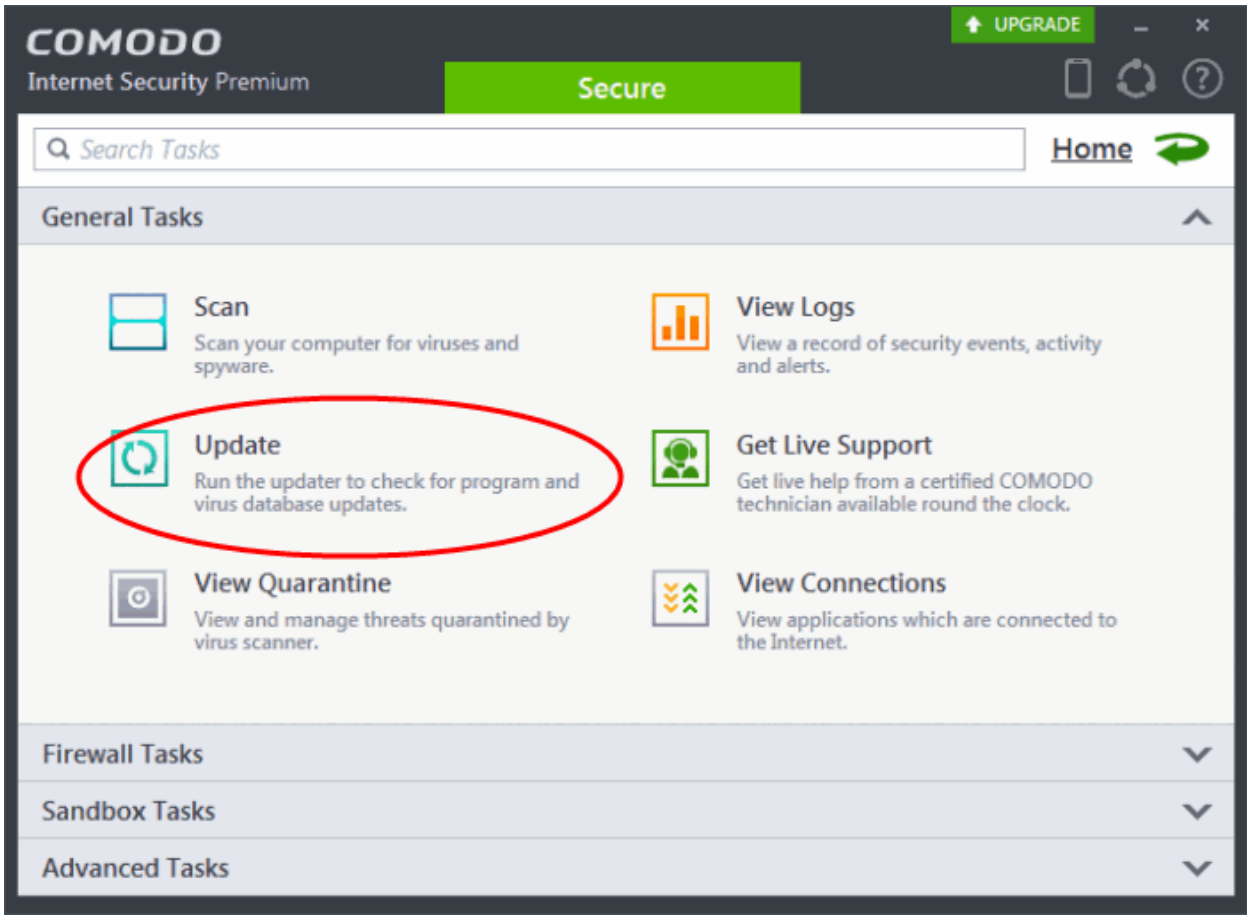
2.4. Manage Virus Database and Program Updates

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

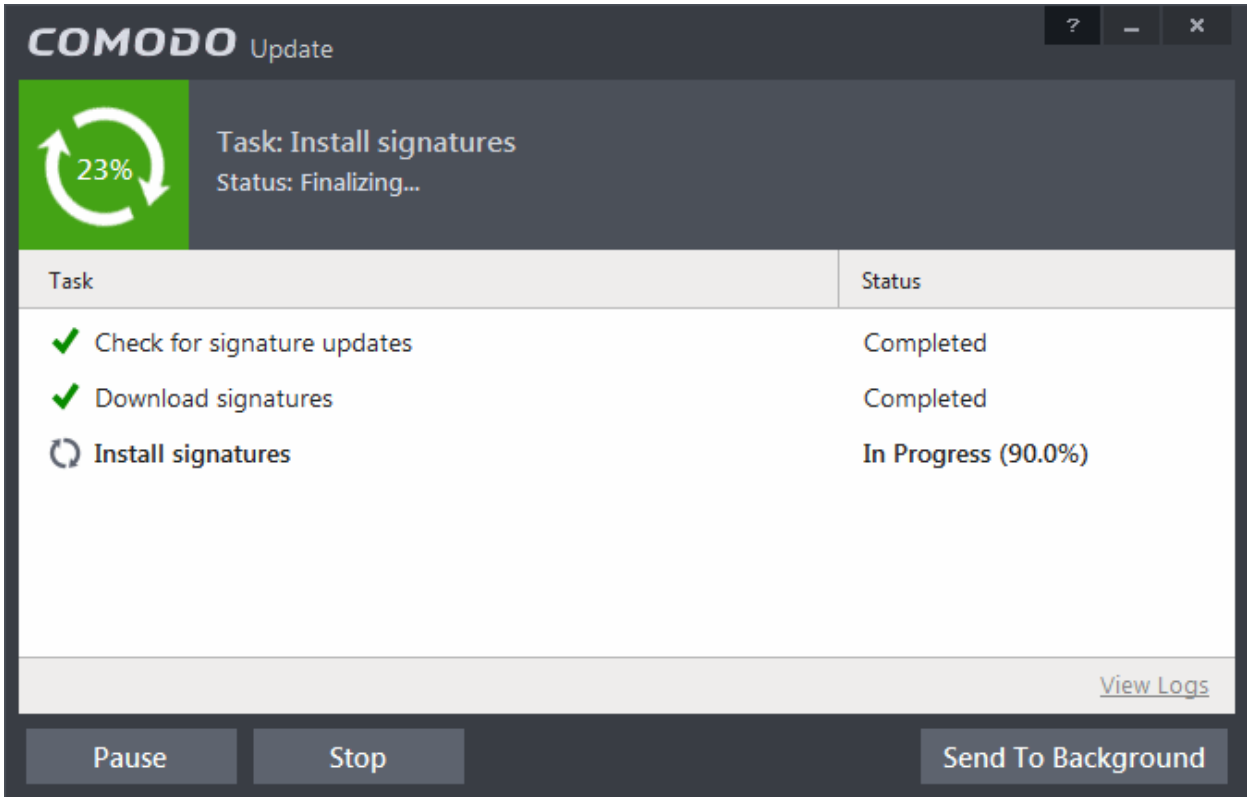
Note: You must be connected to Internet to download updates.

To manually check for the latest virus and program updates

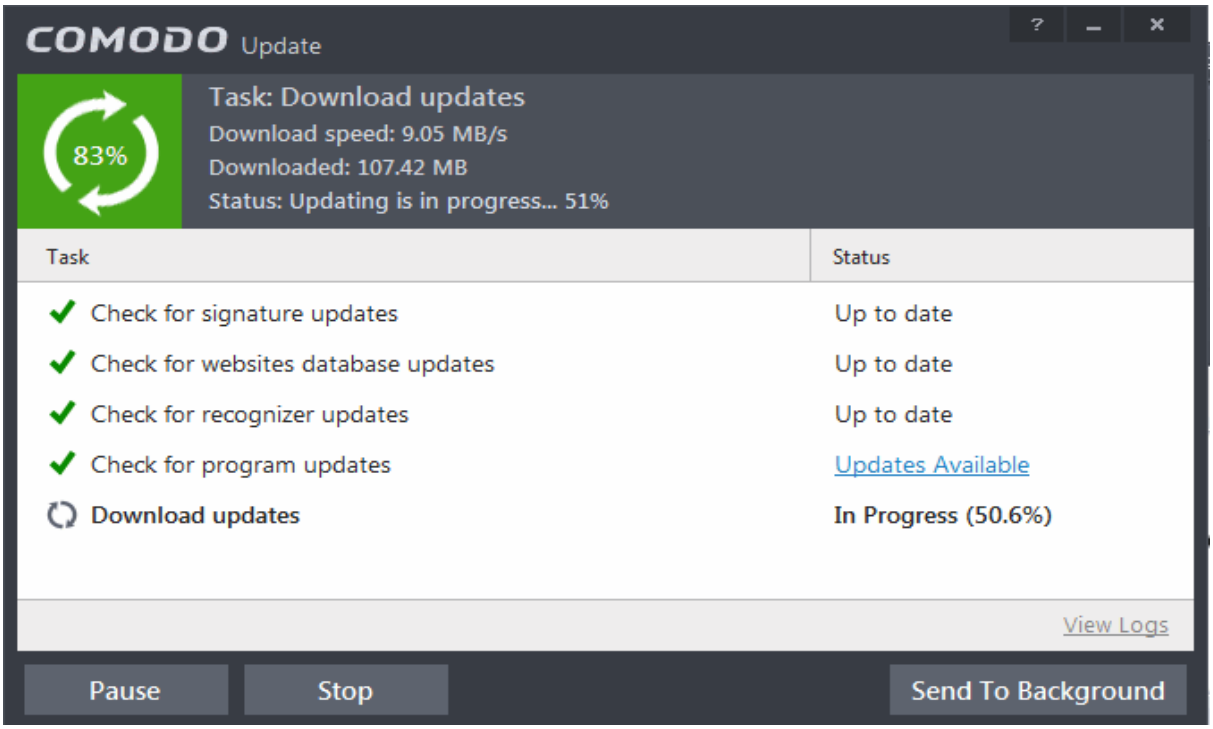
1. Switch to the 'Tasks' screen and click 'General Tasks' to open the 'General Tasks' interface.
2. Click 'Update'. The application will start checking for program and database updates



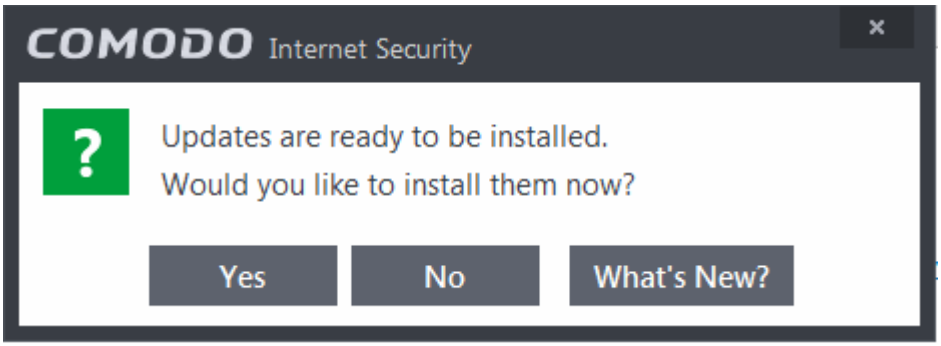
Signature updates will be downloaded and installed first if they are available:



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



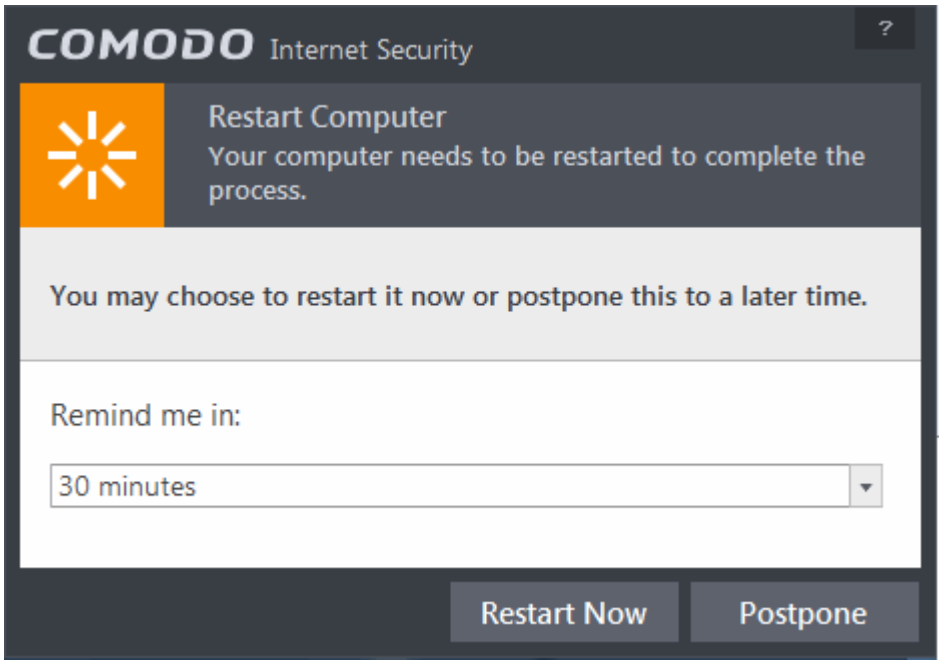
When all updates have been download you will be asked to confirm installation at the following dialog:



- Click 'Yes' to begin installation:

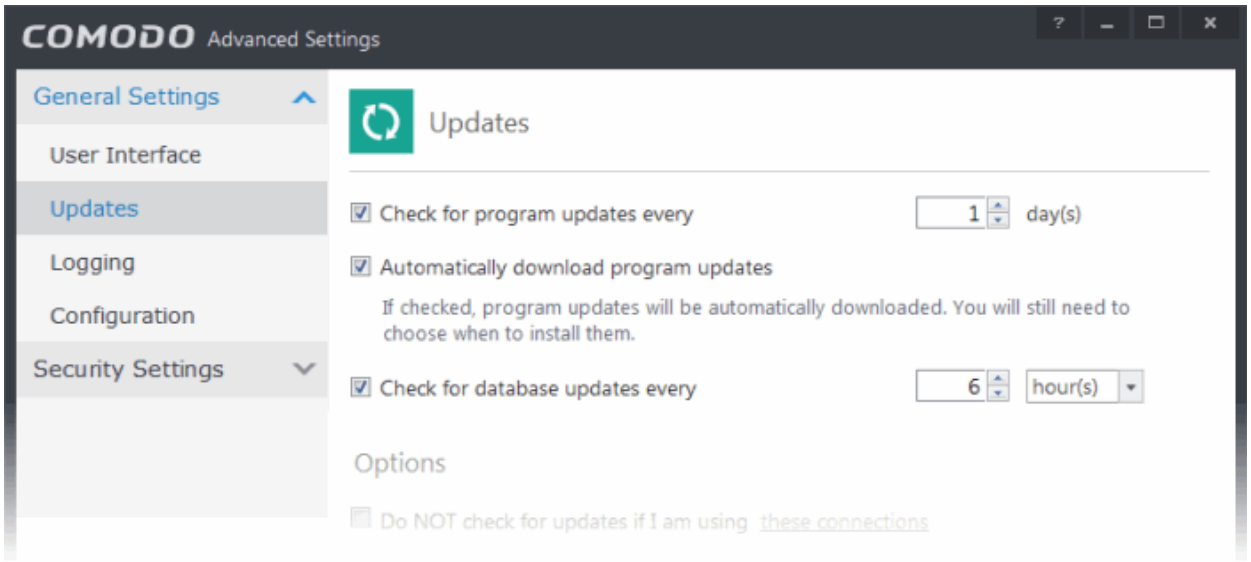
During the update process, new software components or features sometimes become available for installation. As these may alter the behavior of CIS in some manner, please carefully review these types of update before agreeing to their installation.

Your computer will need to be restarted to complete the update process. You can restart immediately or can select a period of after which you want to be reminded and click 'Postpone'.



Automatic Updates

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

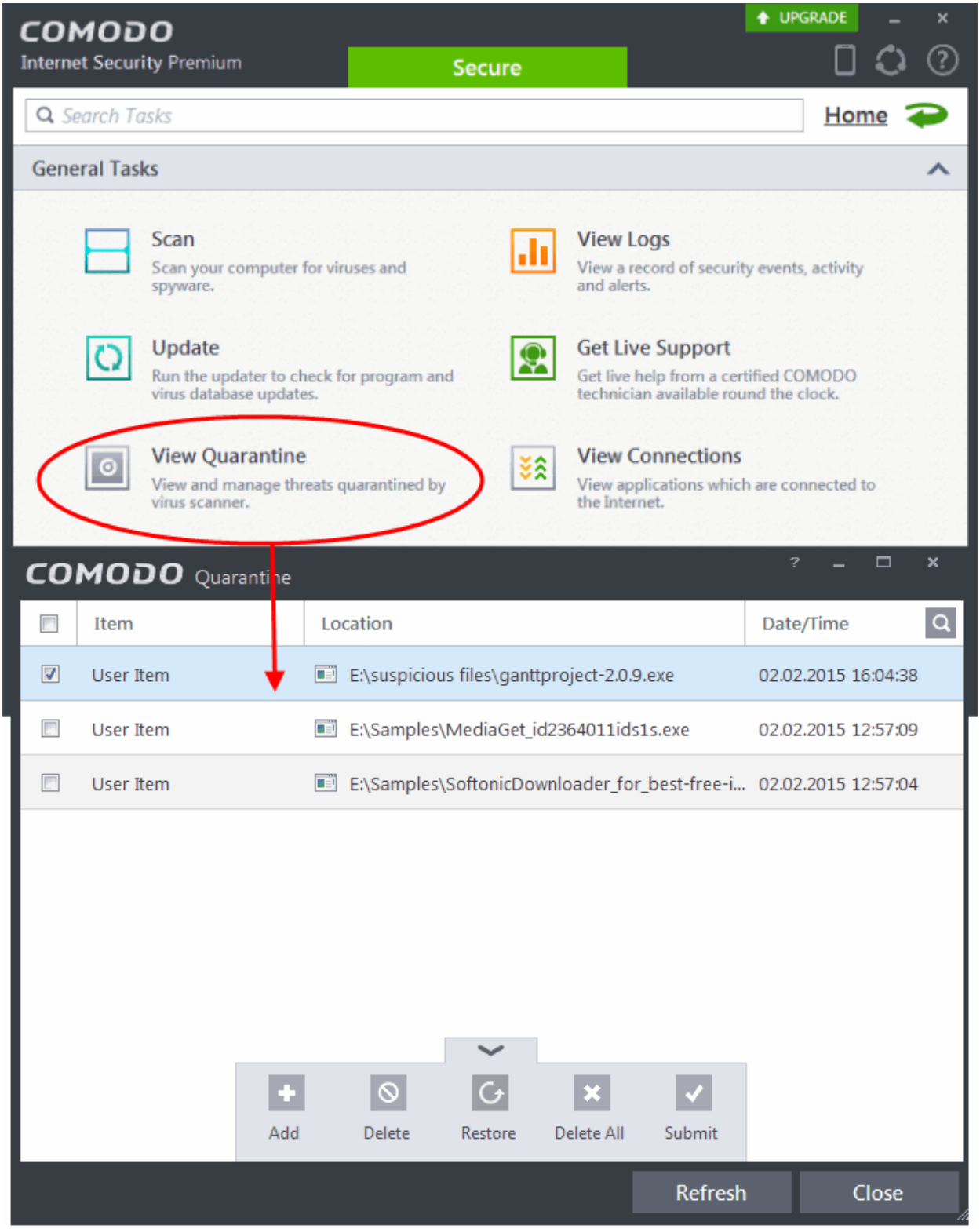


You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. Refer to **Scan Profiles** for more details.

2.5. Manage Quarantined Items

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

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



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

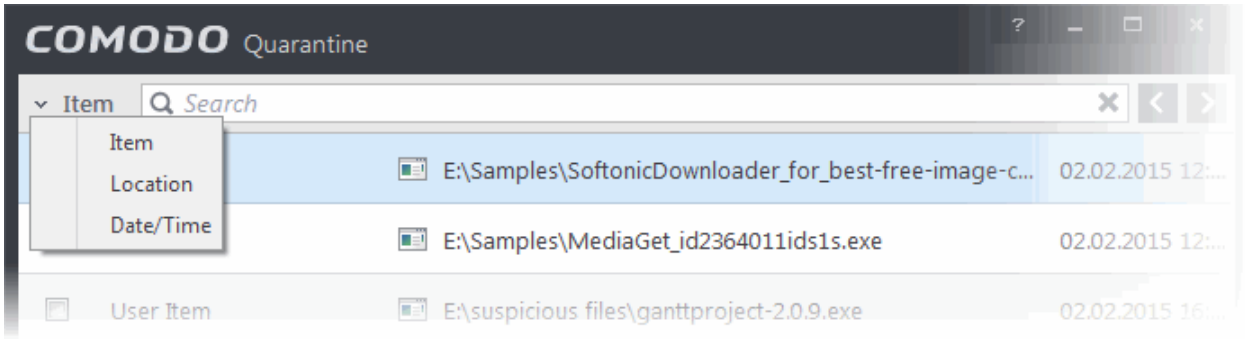
Column Descriptions

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

For details on adding executables identified as infected files during on-demand or real time scans to Quarantine, refer to

General Tasks > Scan and Clean Your Computer.

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



The Quarantined Items interface also allows you to:

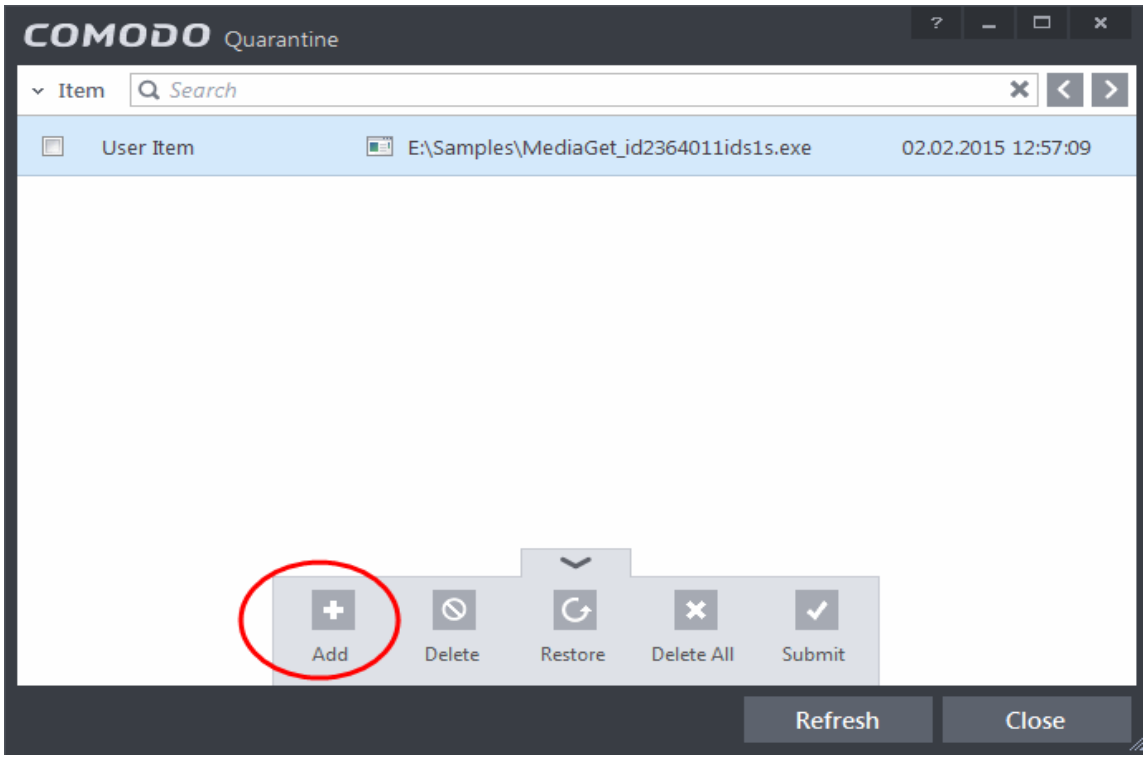
- **Manually add applications, executables or other files, that you do not trust, as a Quarantined item**
- **Delete a selected quarantined item from the system**
- **Restore a quarantined item to oits original location**
- **Delete all quarantined items**
- **Submit selected quarantined items to Comodo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

Manually adding files as Quarantined Items

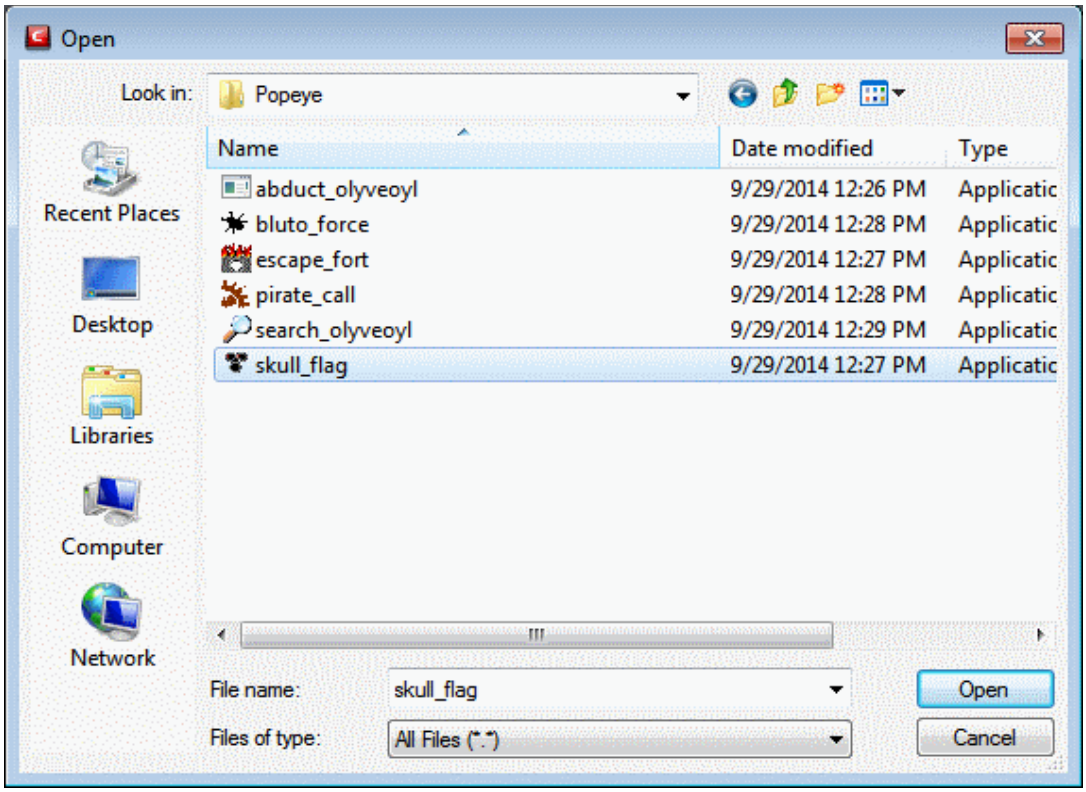
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined Item

1. Click the handle from the bottom of the Quarantine interface and select 'Add' from the options.



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



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

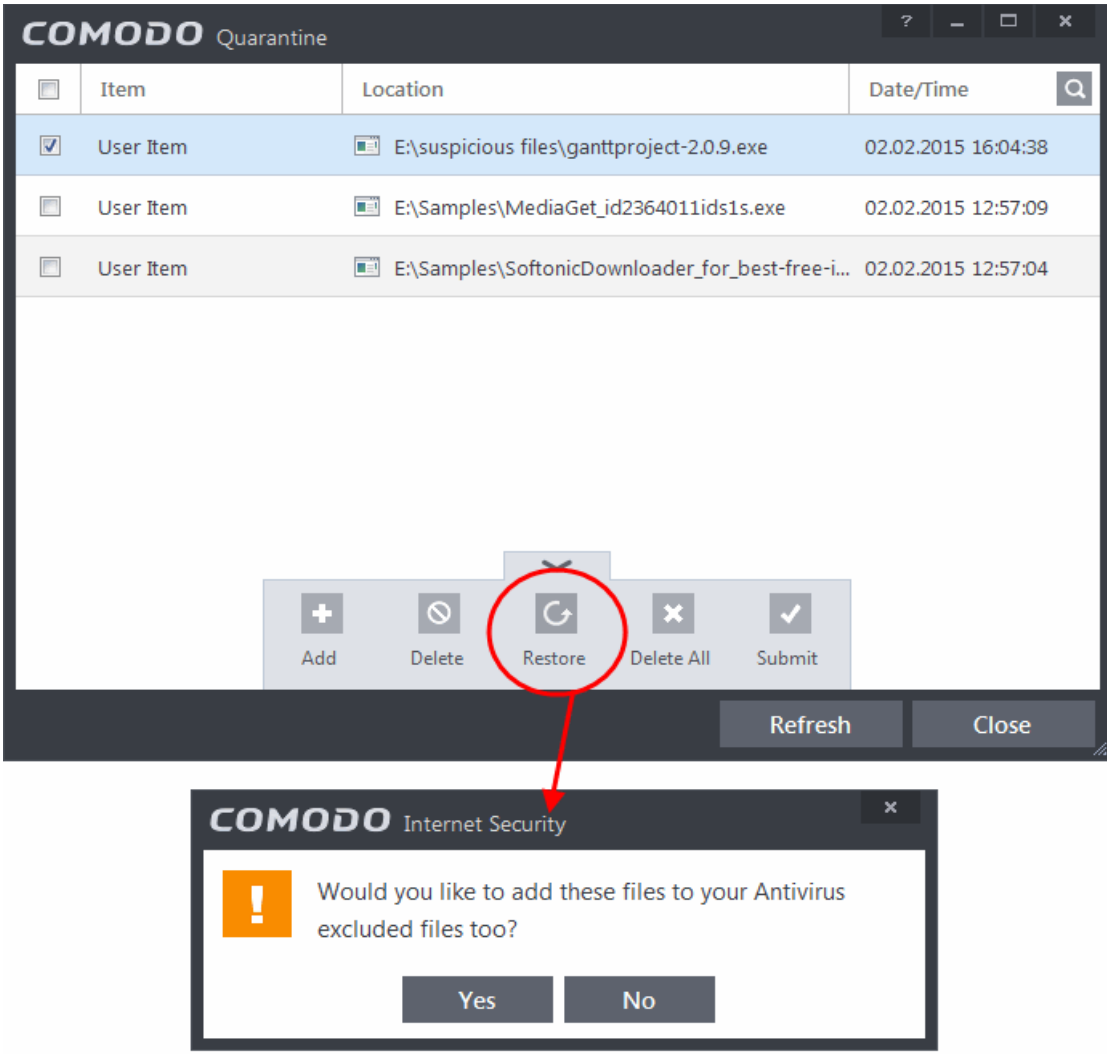
To delete a quarantined item from the system

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

This deletes the file from the system permanently.

To restore a quarantined item to its original location

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



An option will be provided to add the file(s) to **Exclusions** list and if 'Yes' is opted, these files will not be scanned again.

The file will be restored to the original location from where it was moved to Quarantine. If the restored item does not contain a malware, it will operate as usual. But if it contains a malware, it will be detected as a threat immediately, if the Real-Time Scanning is enabled or during the next scan if it is not added to Exclusions list while restoring.

To remove all the quarantined items permanently

- Click the handle from the bottom of the interface and select 'Clear' option.

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

To submit selected quarantined items to Comodo for analysis

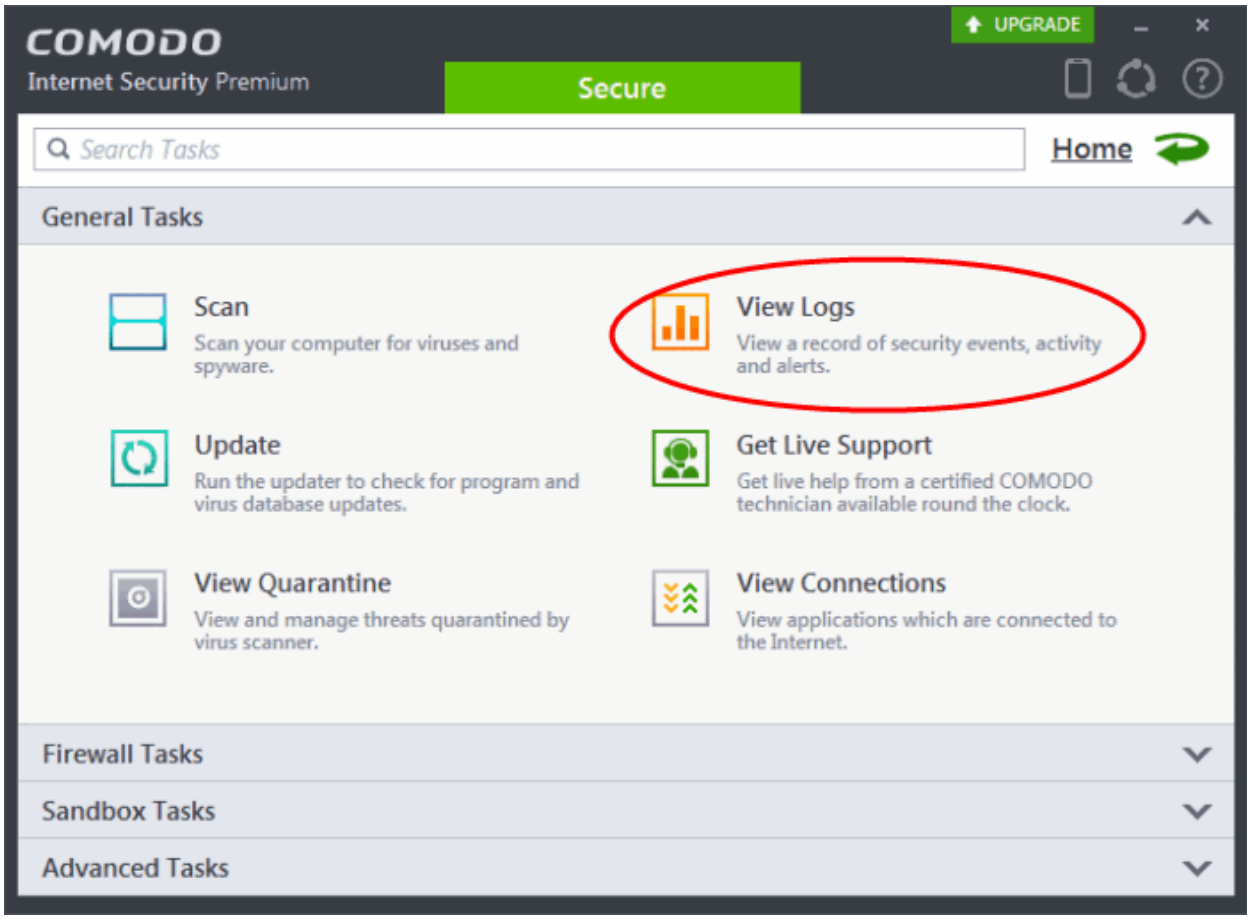
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

You can submit the files which you suspect to be a malware or the files which you consider as safe but identified as malware by Comodo Antivirus (False Positives). Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

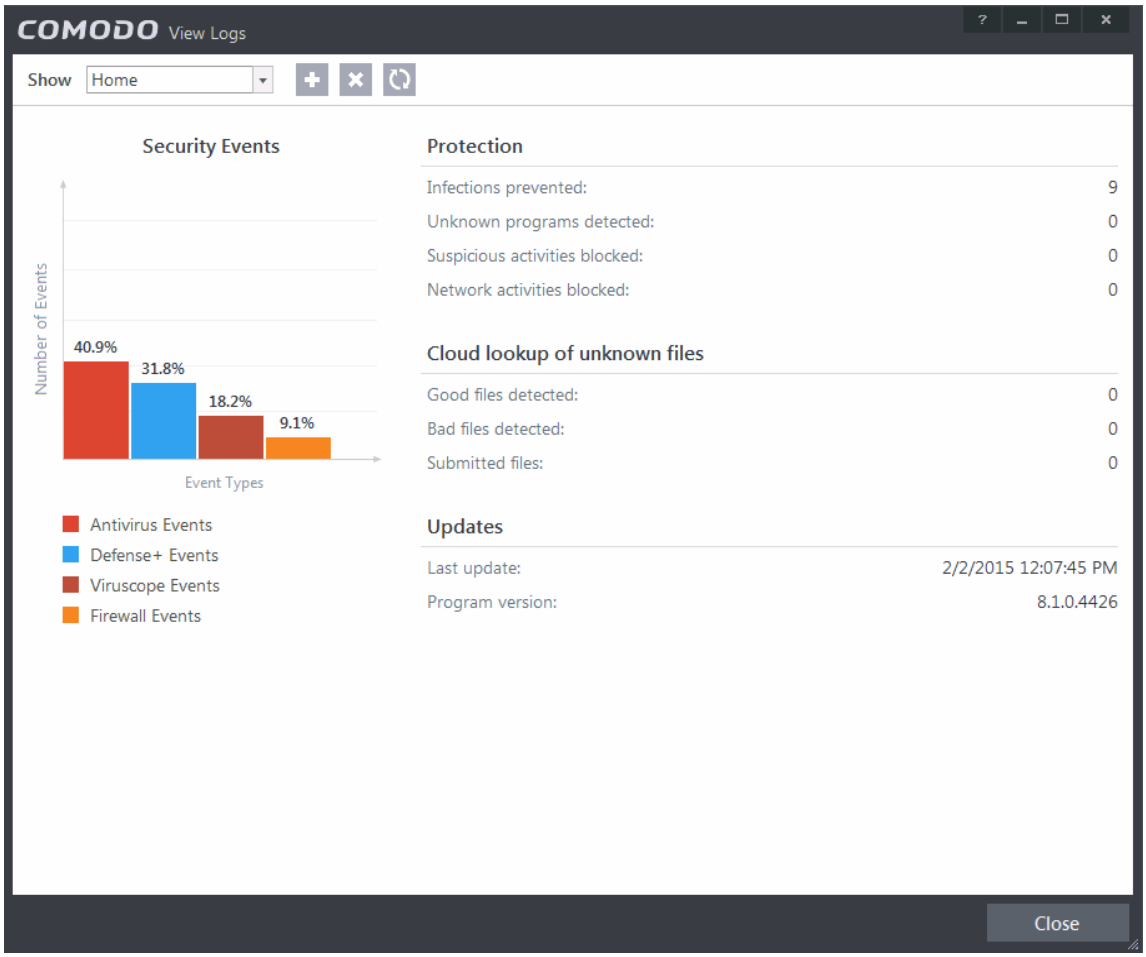
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

2.6. View CIS Logs

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



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



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

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

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

'Logs per Module':

- **Antivirus**
- **Viruscope Logs**
- **Firewall**
- **Defense+**
- **Website Filtering**

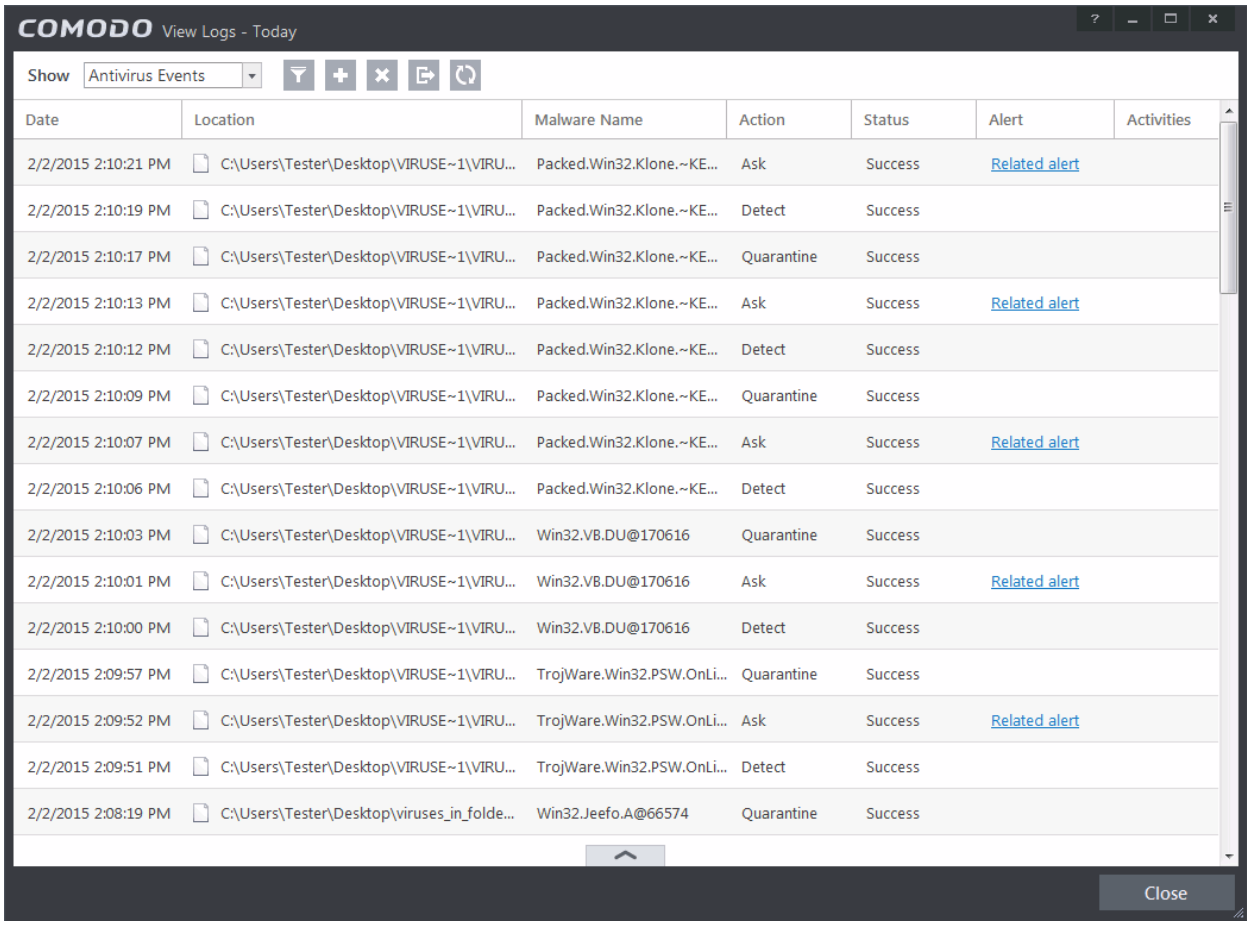
'Other Logs':

- **Alerts Displayed**
- **Tasks Launched**
- **Configuration Changes**

2.6.1. Antivirus Logs

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

The Antivirus logs can be viewed by selecting 'Antivirus Events' from the Show drop-down of the log viewer interface. Alternatively, the Antivirus log screen can be accessed by clicking the number beside 'Detected Threats' in the Advanced View of the Home screen in the Antivirus pane.



Column Descriptions

1. **Date** - Indicates the date of the event.
2. **Location** - Indicates the location where the application detected with a threat is stored.
3. **Malware Name** - Name of the malware event that has been detected.
4. **Action** - Indicates action taken against the malware through Antivirus.
5. **Status** - Gives the status of the action taken. It can be either 'Success' or 'Fail'.
6. **Alert** - Gives the details of the alert displayed for the event
7. **Activities** - Gives the details of activities executed by the processes that are run by the infected application.

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

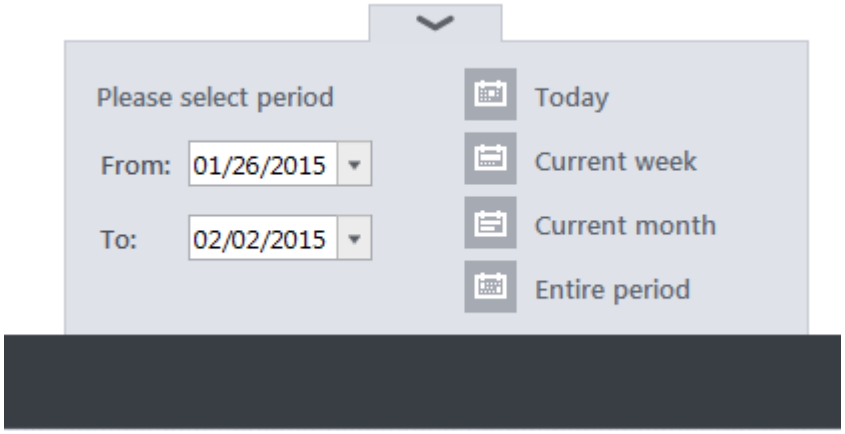
2.6.1.1. Filtering Antivirus Logs

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

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

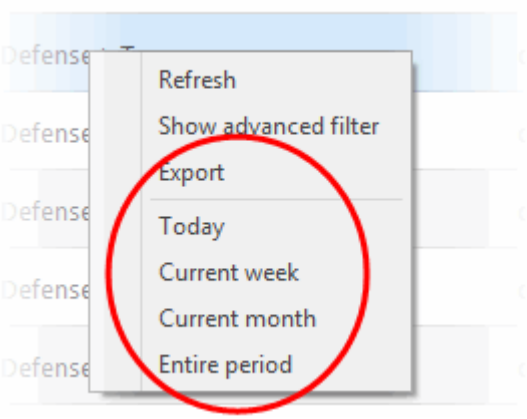
Preset Time Filters:

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



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

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



Advanced Filters:

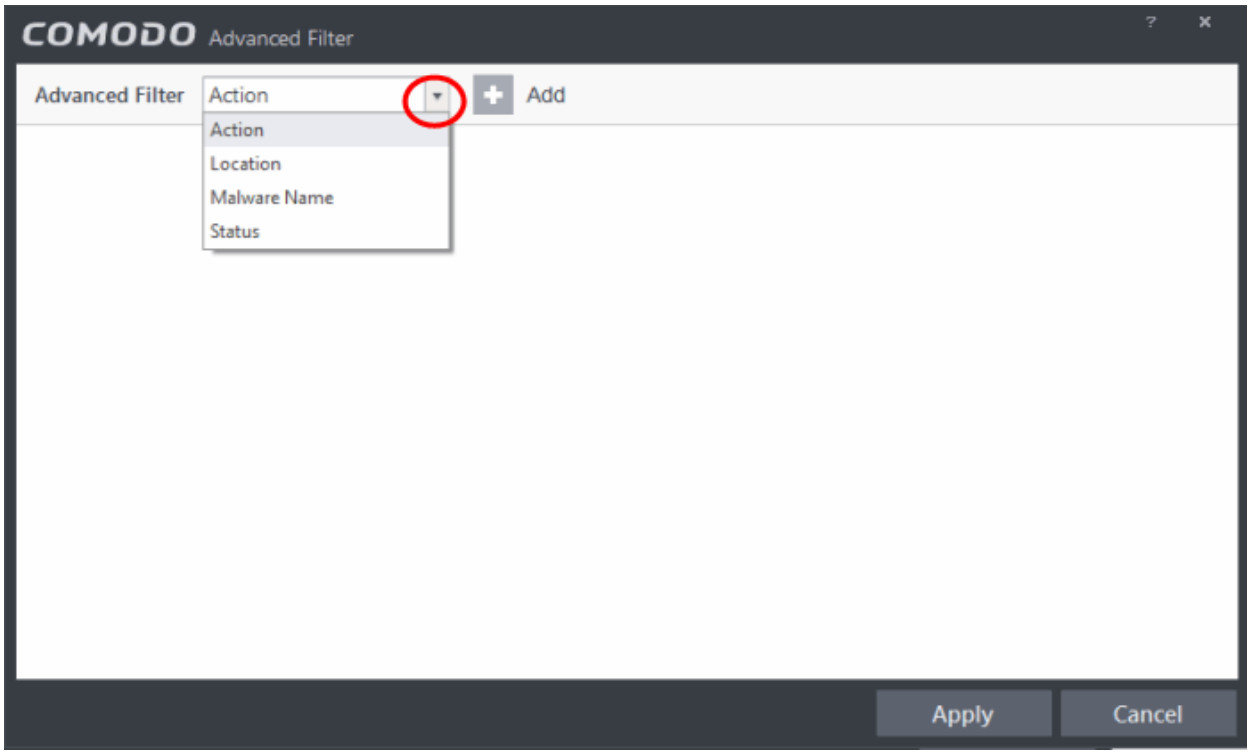
Having chosen a **preset time filter**, you can further refine the displayed events according to specific filters. Following are available filters for Antivirus logs and their meanings:

- **Action** - Displays events according to the response (or action taken) by the Antivirus

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

To configure Advanced Filters for Antivirus events

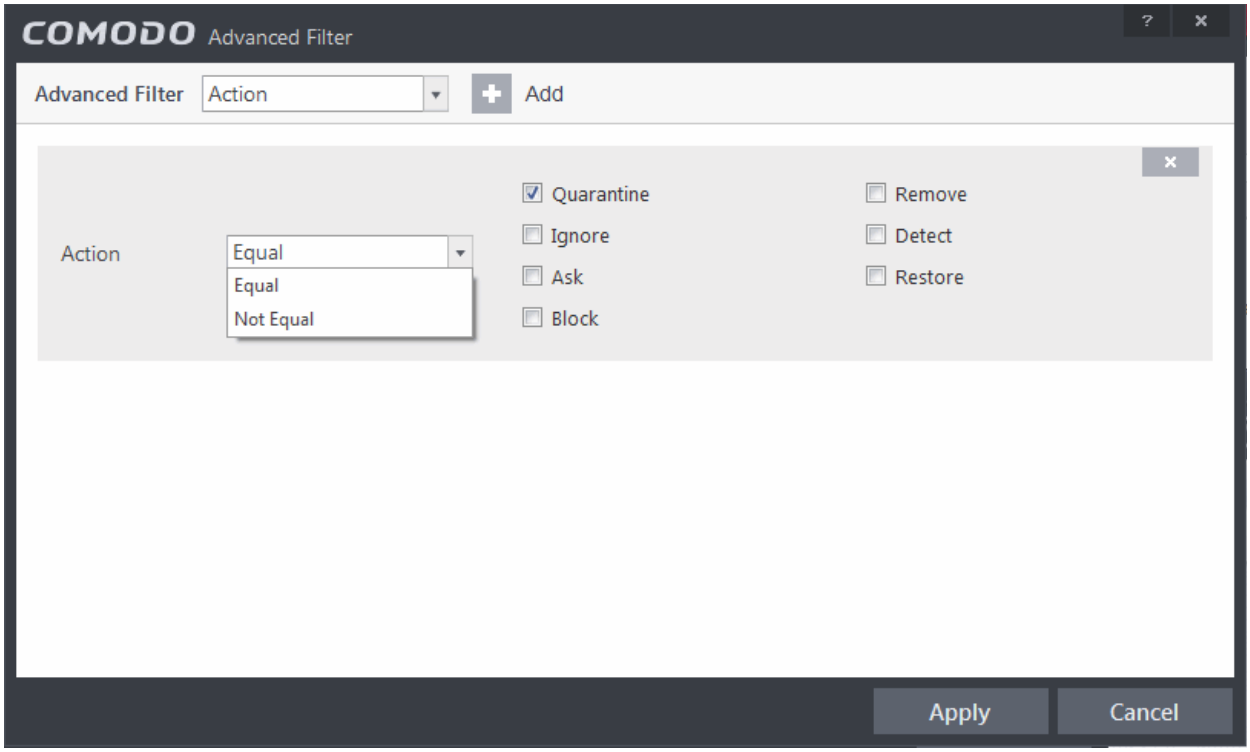
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for AV events will open
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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



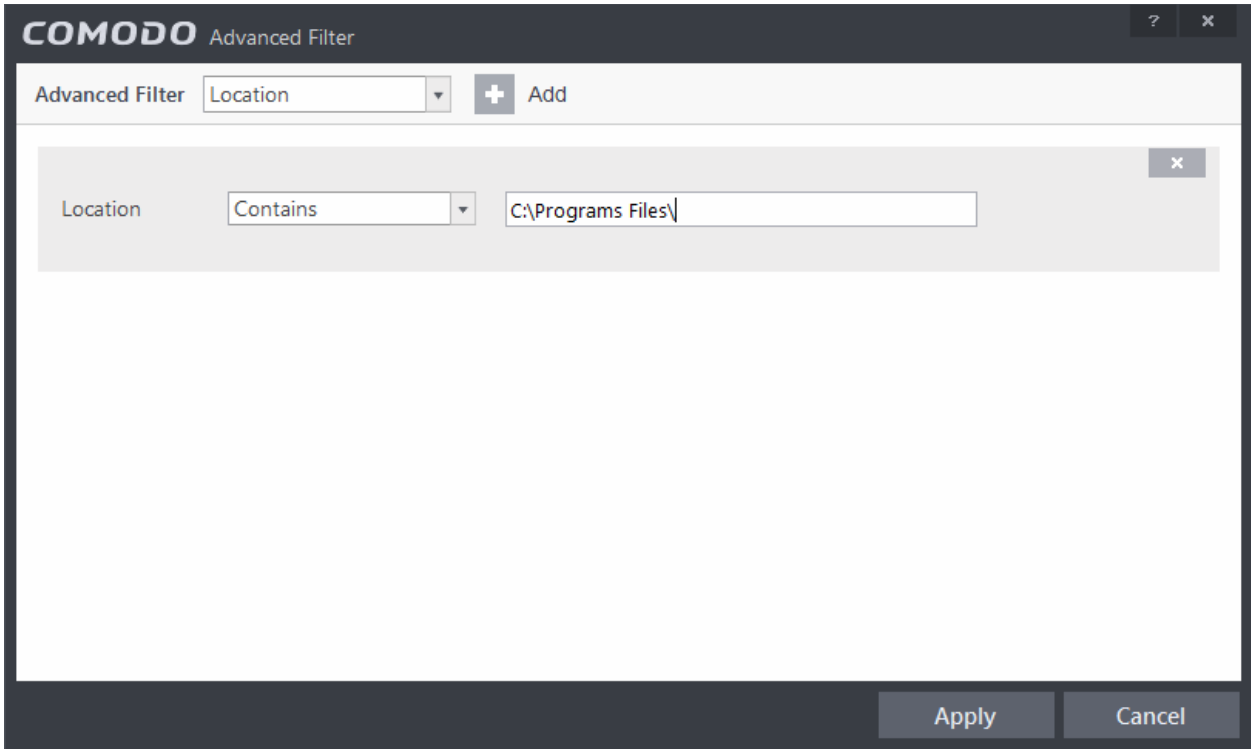
a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

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

- Quarantine: Displays events where the user chose to quarantine a file
- Remove: Displays events where the user chose to delete an item
- Ignore: Displays events where the user chose to ignore an item
- Detect: Displays events for detection of a malware
- Ask: Displays events when user was asked by alert concerning some Defense+, Firewall or Antivirus event
- Restore: Displays events of the applications that were quarantined and restored
- Block: Displays events of the applications that were blocked

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

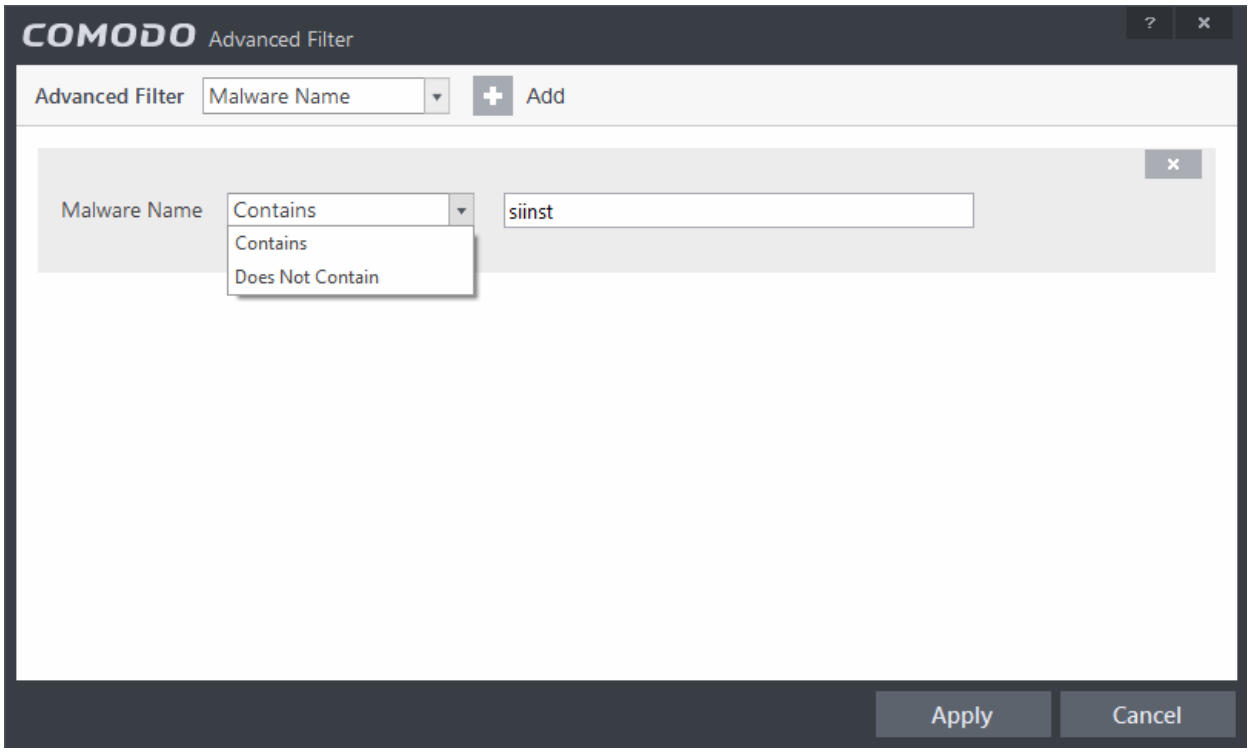
ii. **Location**: The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



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

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

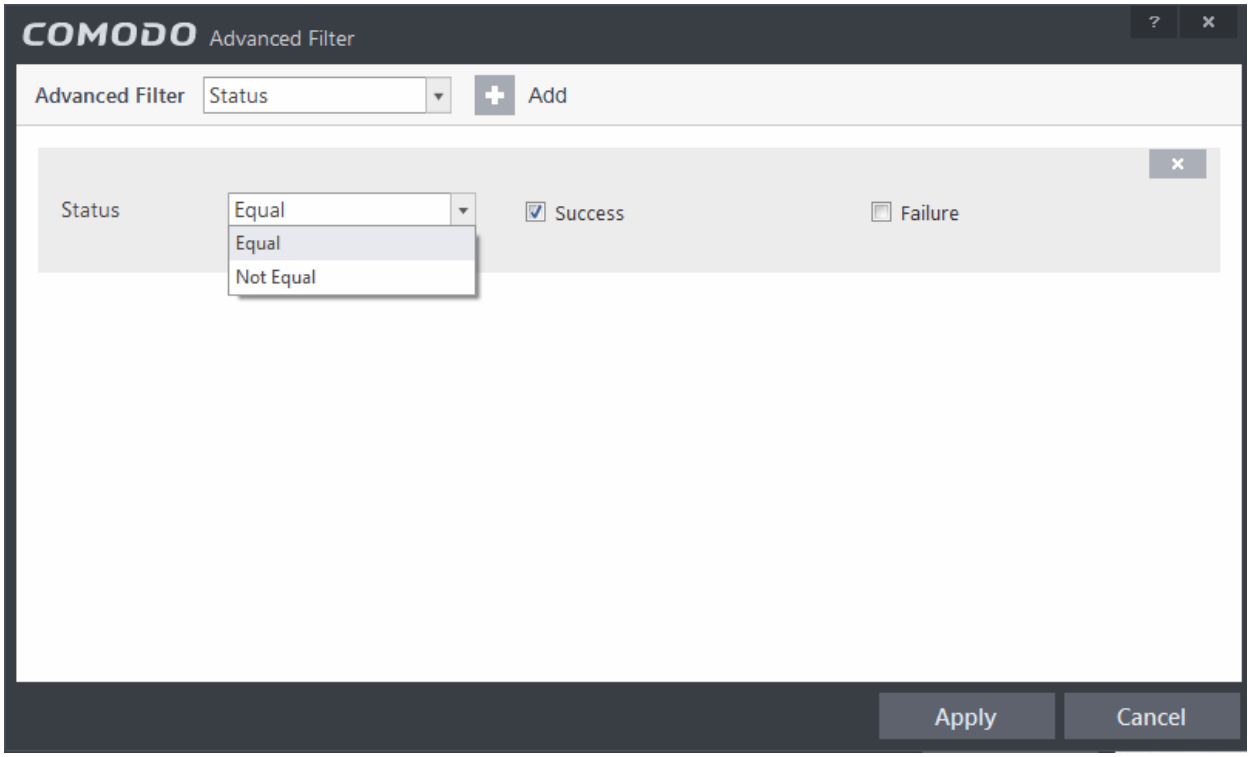
iii. **Malware Name**: The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



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

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

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



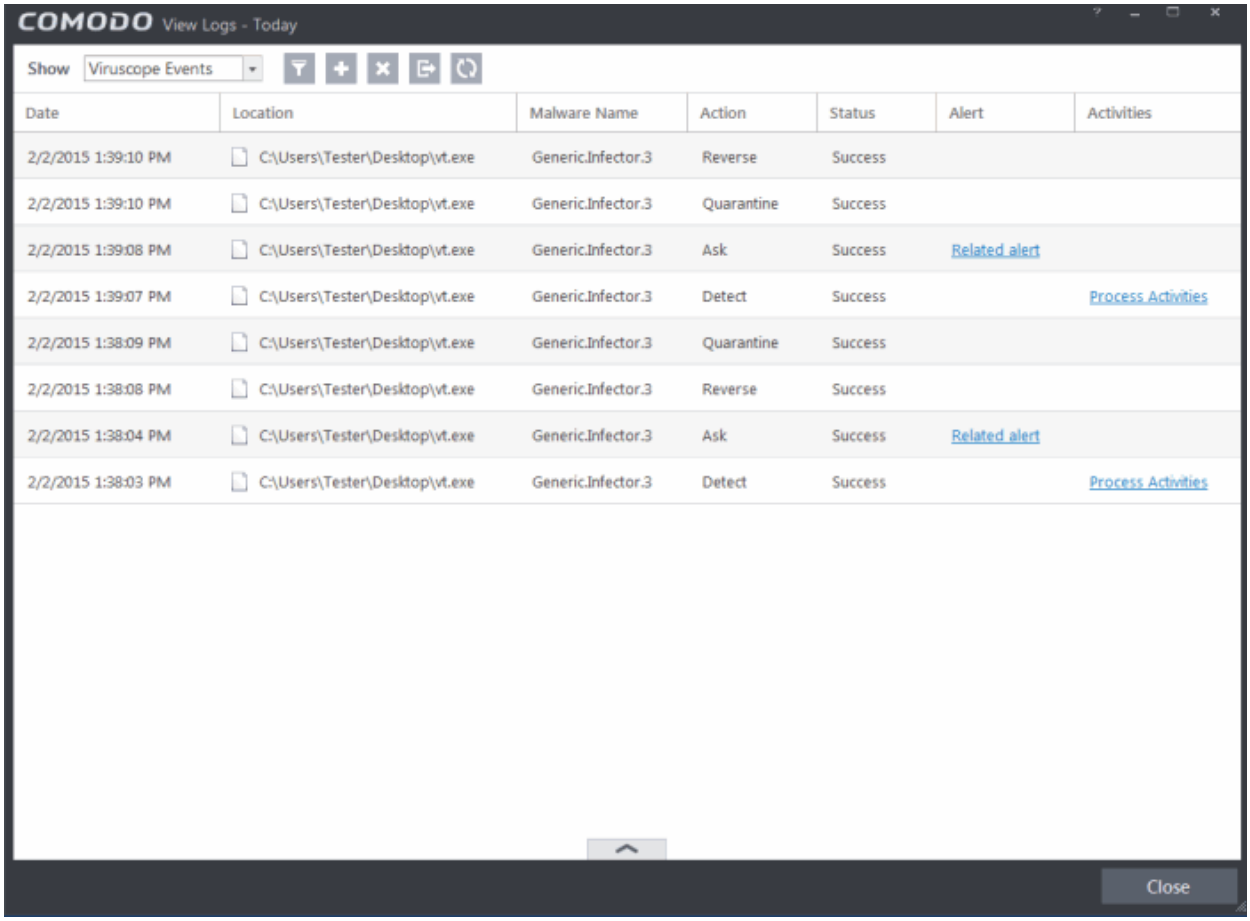
a) Select 'Equal' or 'Not Equal' option from the drop-down field. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
   - Success: Displays Events that successfully executed (for example, the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

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

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

2.6.2. Viruscope Logs

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



Column Descriptions

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

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

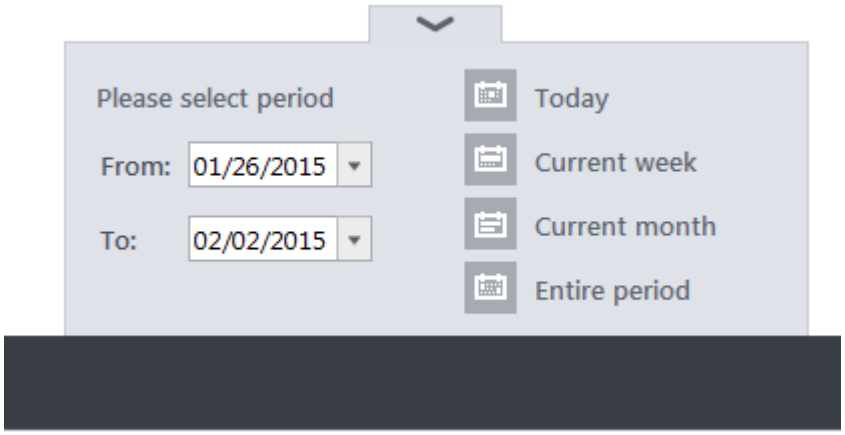
2.6.2.1. Filtering Viruscope Logs

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

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

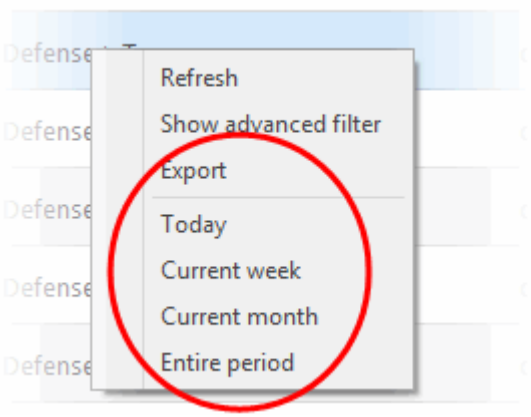
Preset Time Filters:

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



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

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

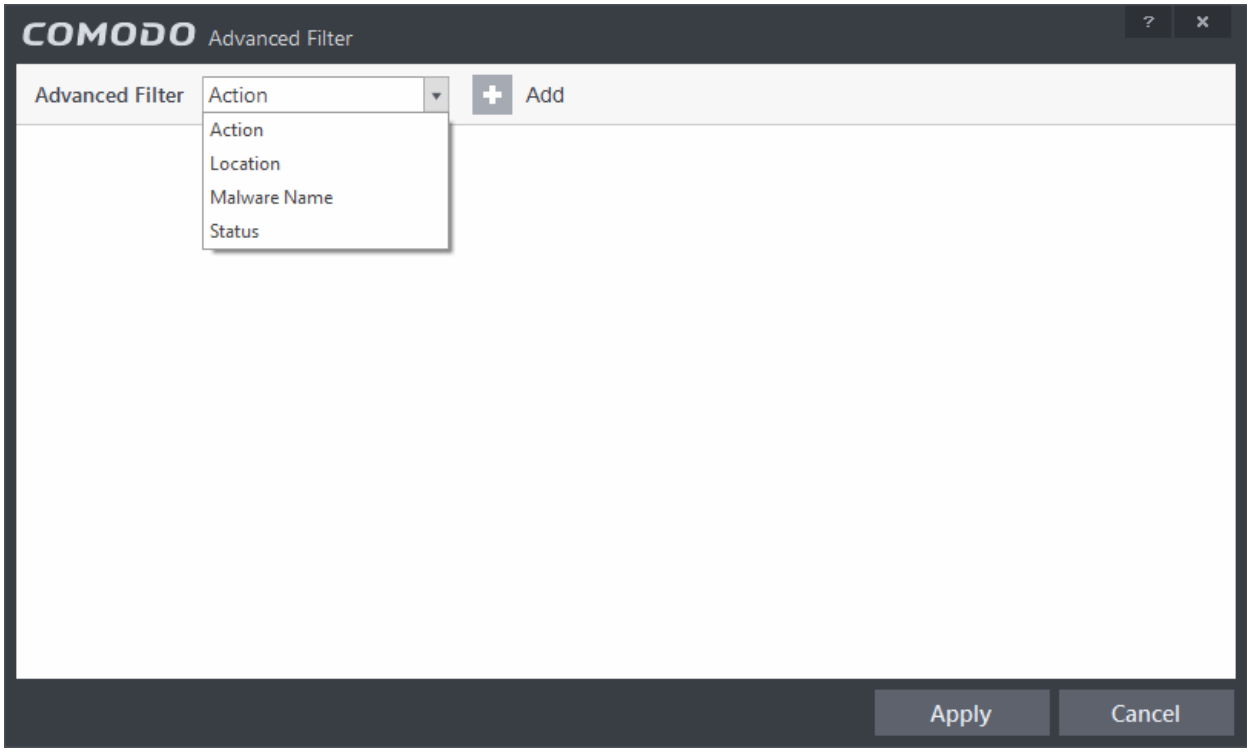


To configure Advanced Filters for Viruscope events

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

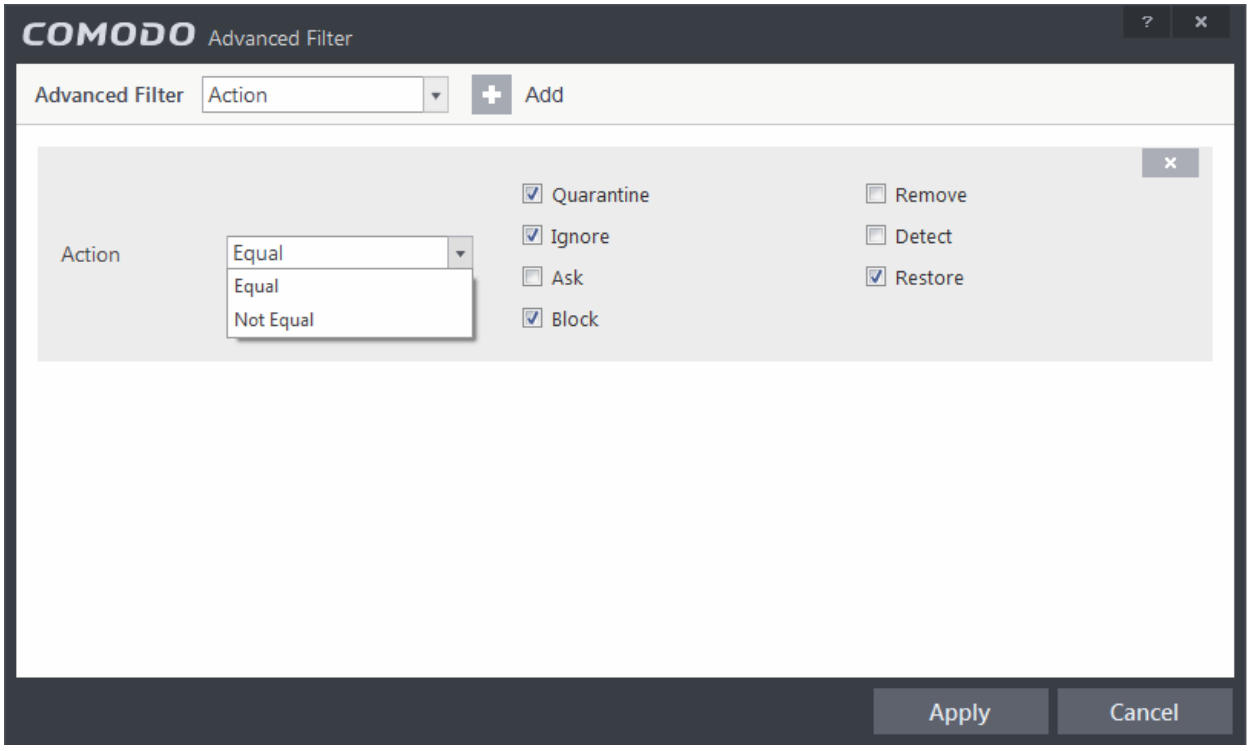
- **Action** - Displays events according to the response (or action taken) by the Viruscope
- **Location** - Displays only the events logged from a specific location
- **Malware Name** - Displays only the events logged corresponding to a specific malware

- **Status** - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'



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

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



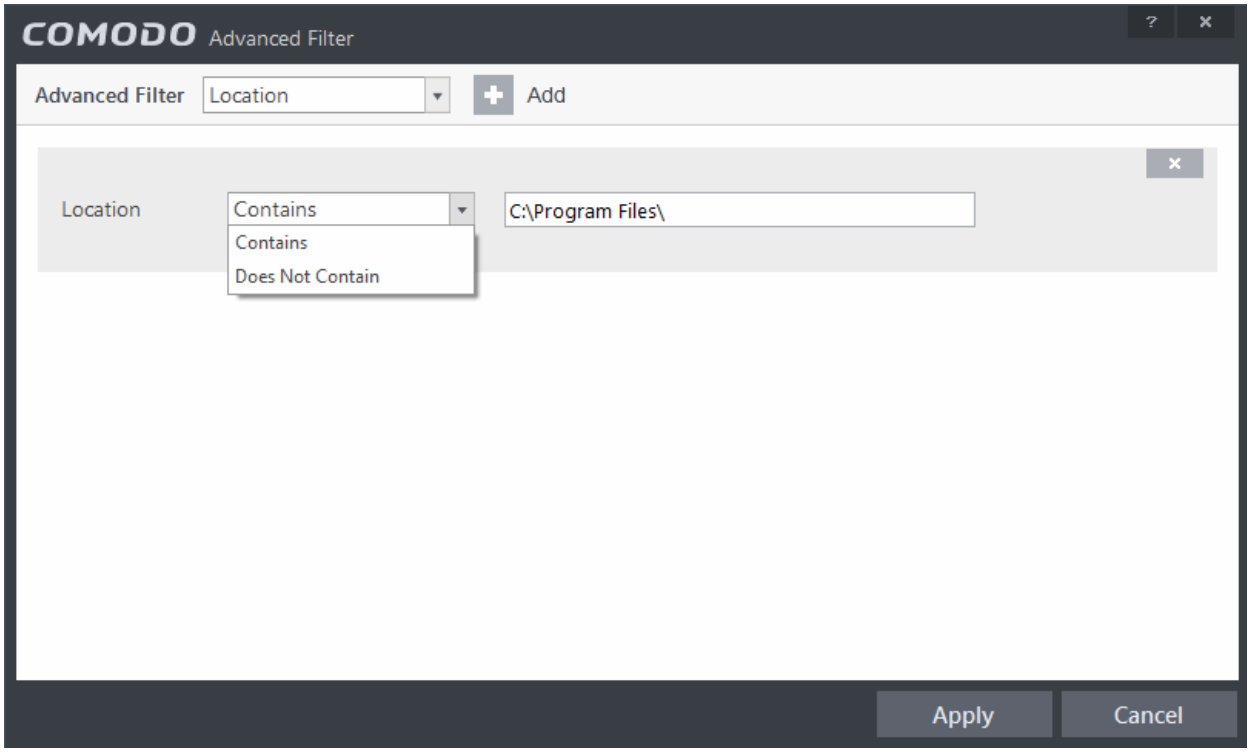
a. Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

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

- Quarantine: Displays events where the user chose to quarantine a file
- Remove: Displays events where the user chose to delete an item
- Ignore: Displays events where the user chose to ignore an item
- Detect: Displays events for detection of a malware
- Ask: Displays events when user was asked by alert concerning some Defense+, Firewall or Antivirus event
- Restore: Displays events of the applications that were quarantined and restored
- Block: Displays events of the applications that were blocked

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

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

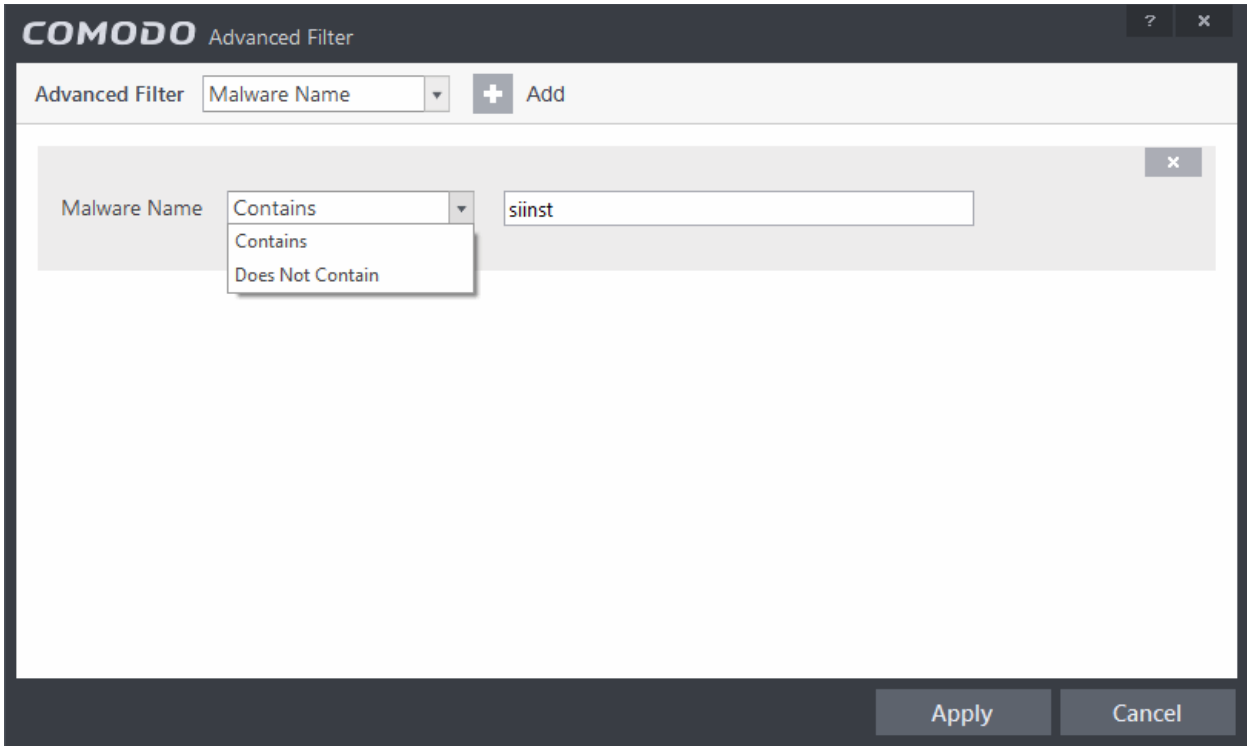


a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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

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

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

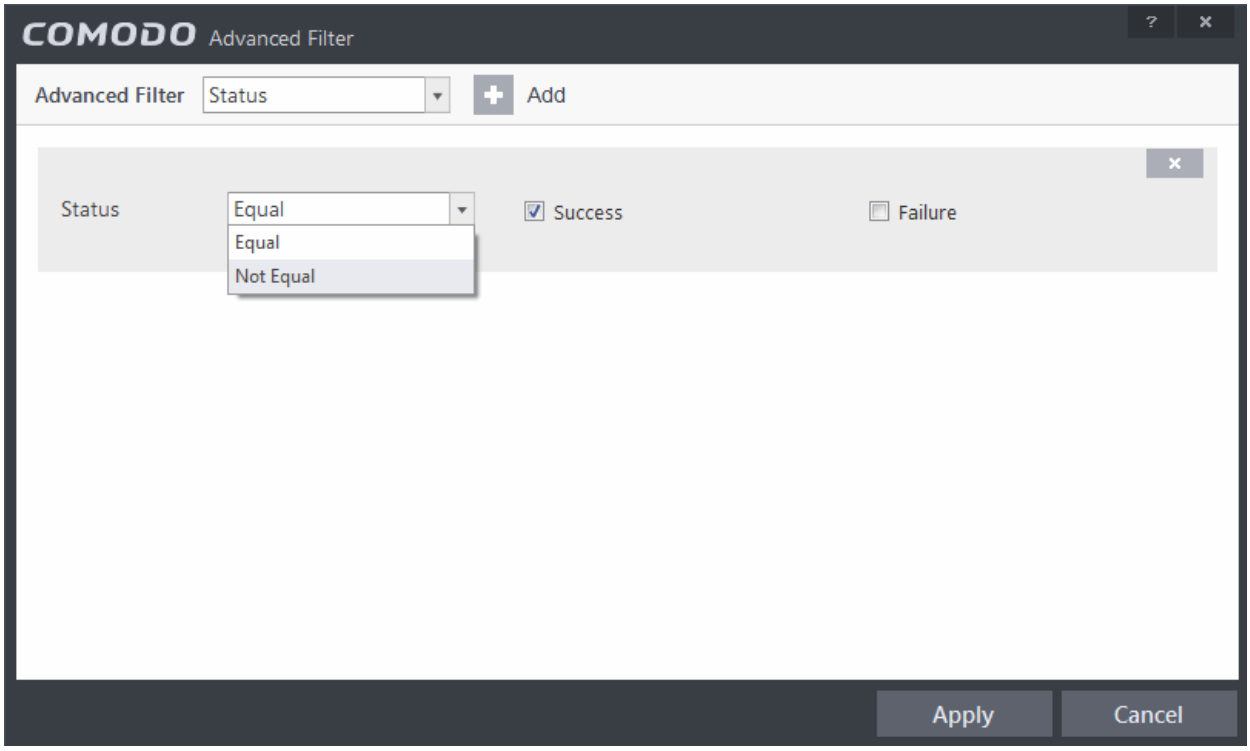


a. Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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

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

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



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

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

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

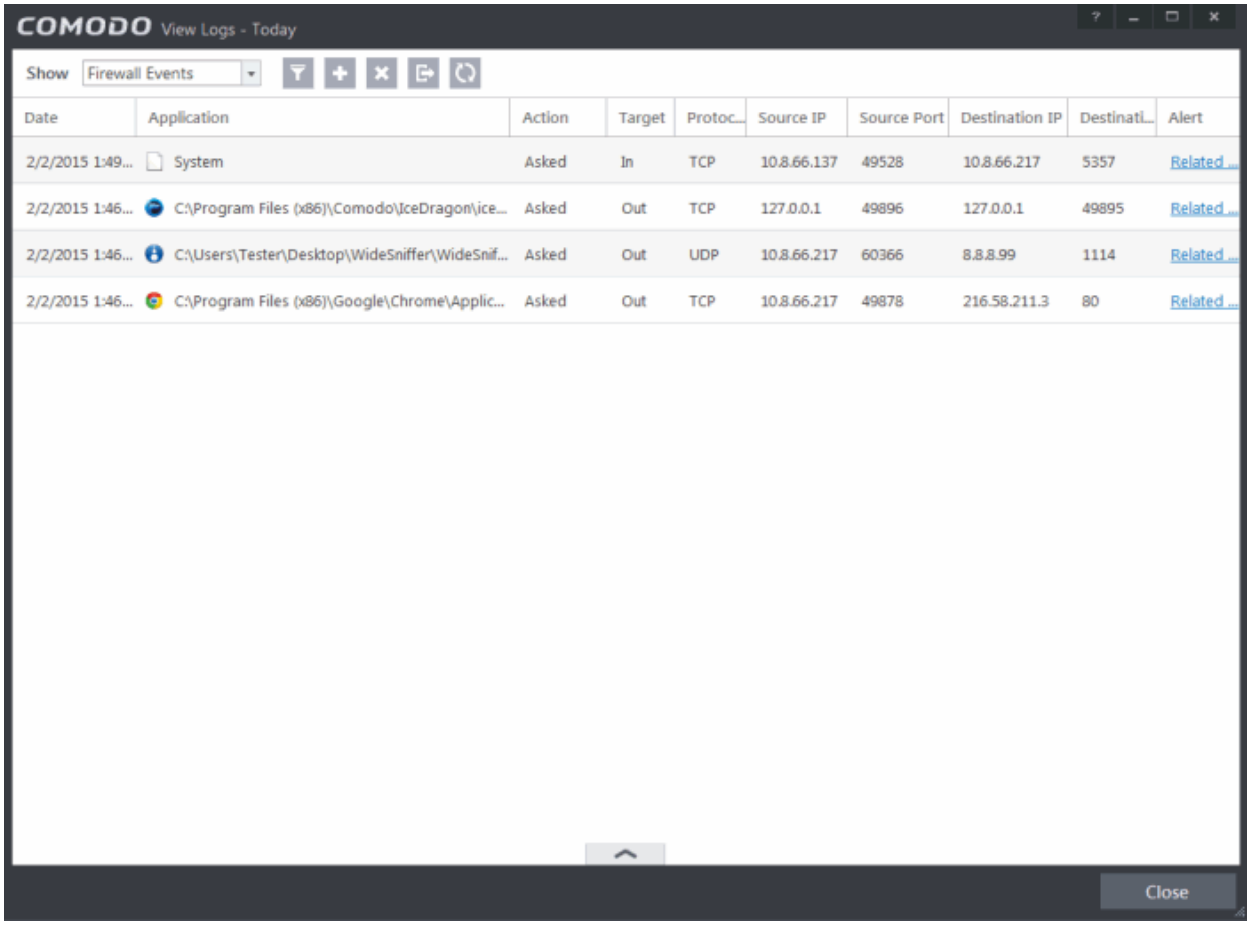
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.3. Firewall Logs

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

The Firewall logs can be viewed by selecting 'Firewall Events' from the 'Show' drop-down of the log viewer interface. Alternatively, the Firewall log screen can be accessed by clicking the number beside 'Network Intrusions' in the Advanced View of the Home screen in the Firewall pane.



Column Descriptions

1. **Date** - Contains precise details of the date and time of the connection attempt.
2. **Application** - Indicates which application or process propagated the event. If the application has no icon, the default

system icon for executable files are used

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

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

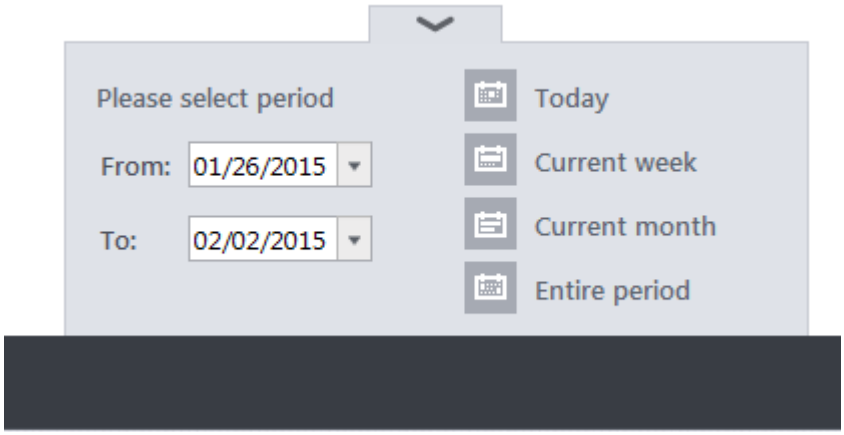
2.6.3.1. Filtering Firewall Logs

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

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

Preset Time Filters:

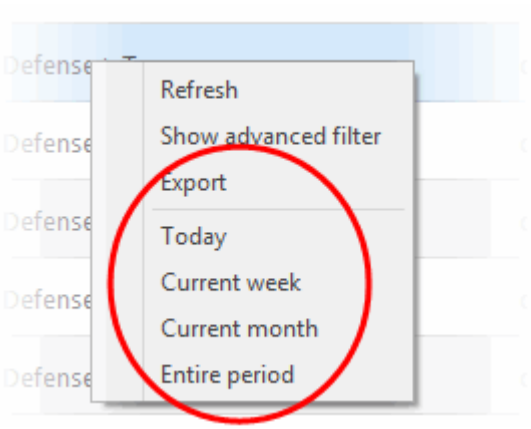
Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).

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

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



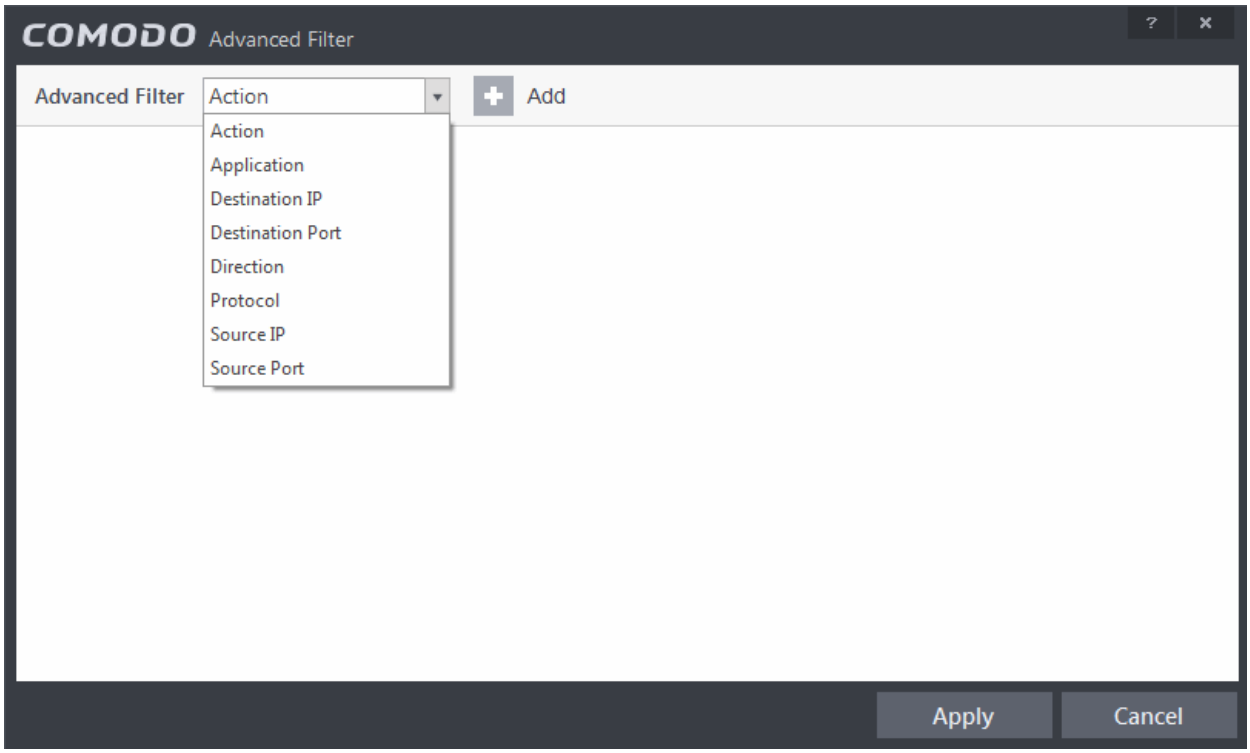
Advanced Filters

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

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

To configure Advanced Filters for Firewall events

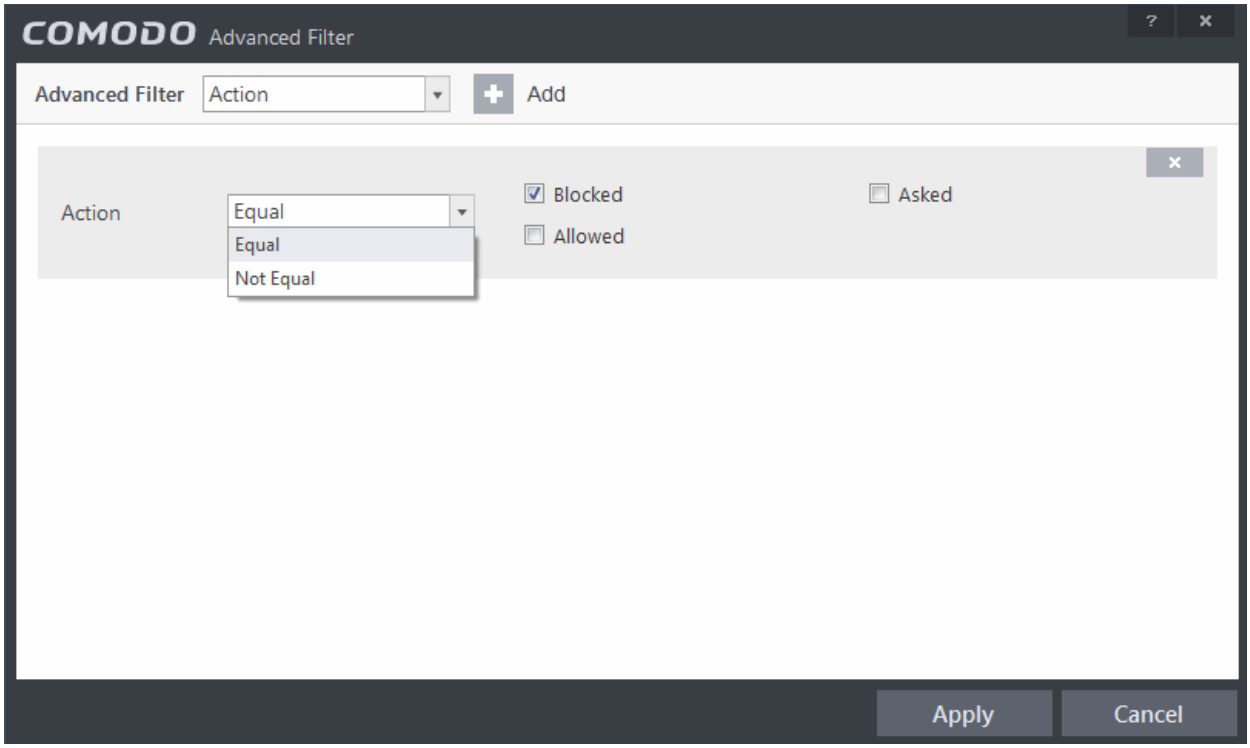
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply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



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

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

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



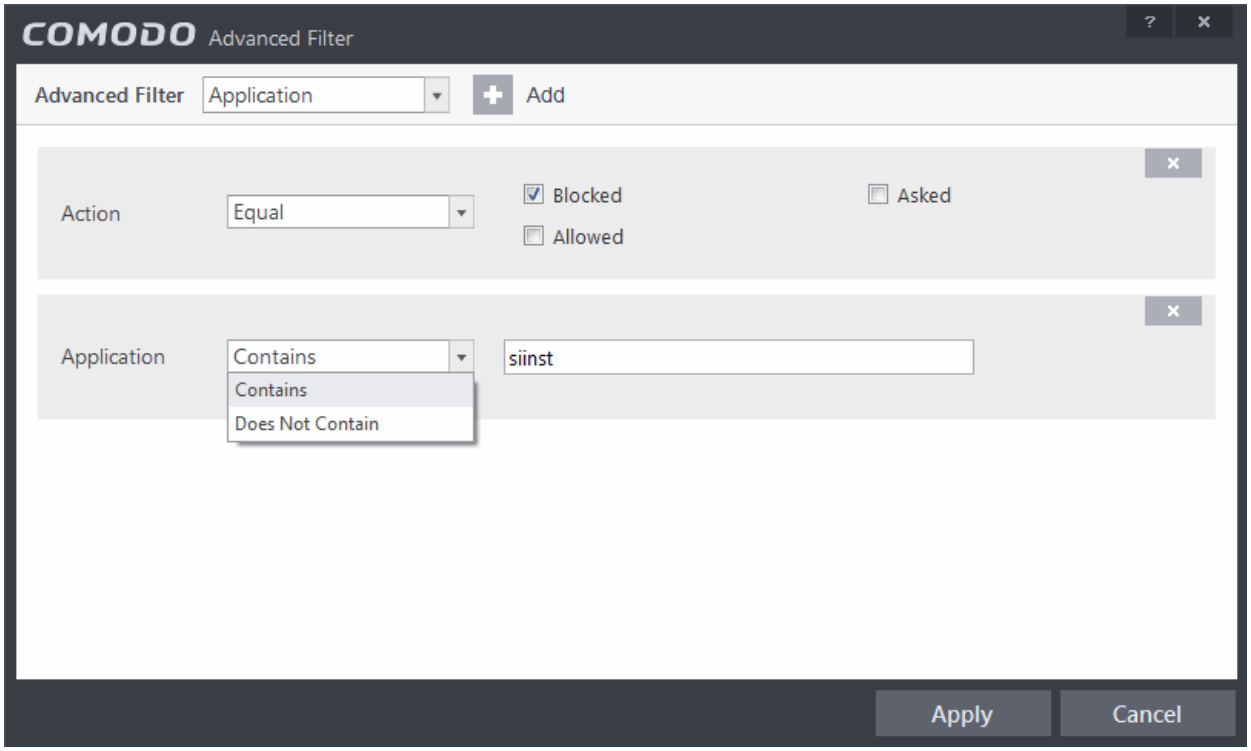
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

- Blocked: Displays list of events that were blocked

- Allowed: Displays list of events that were allowed
- Asked: Displays list of events that were asked to the user
- Suppressed: Displays list of events that were suppressed by the user

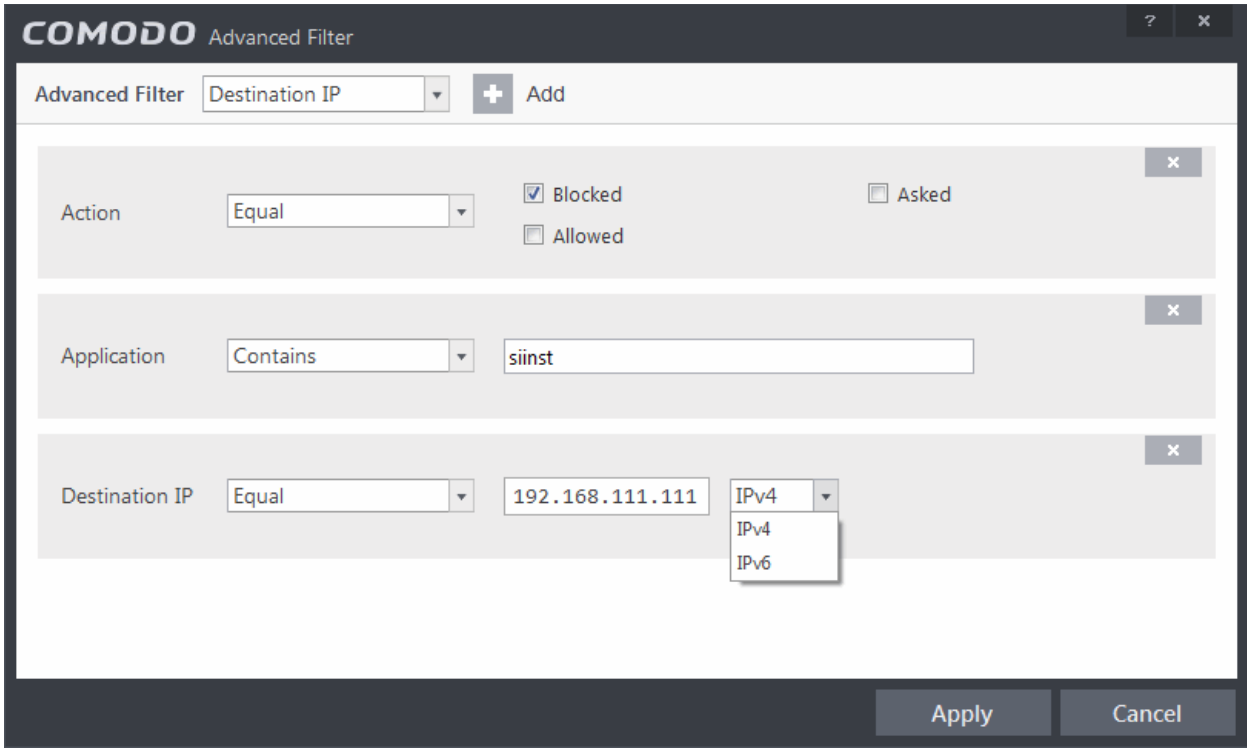
ii. **Application**: Selecting the 'Application' option displays a drop-down box and text entry field.



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

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

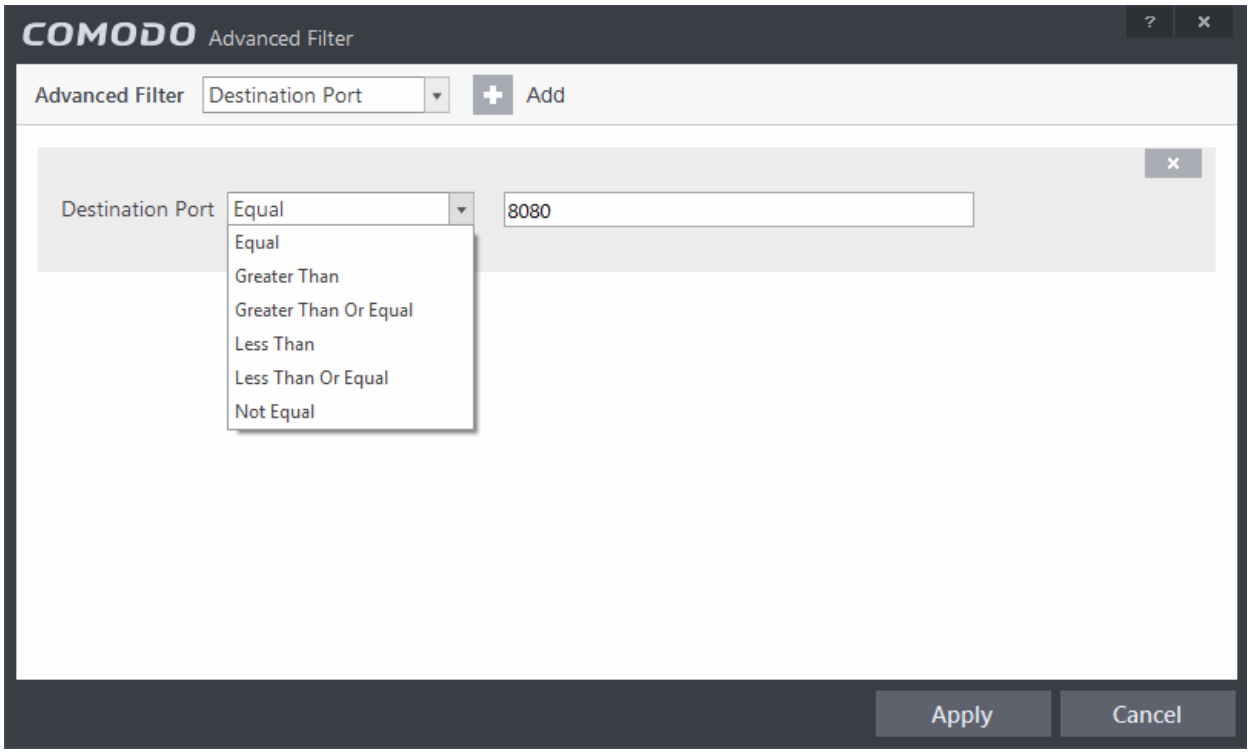
iii. **Destination IP:** Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.



a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Select 'IPv4' or 'IPv6' from the drop-down box.
c) Enter the destination system's IP address that needs to be filtered.

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

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



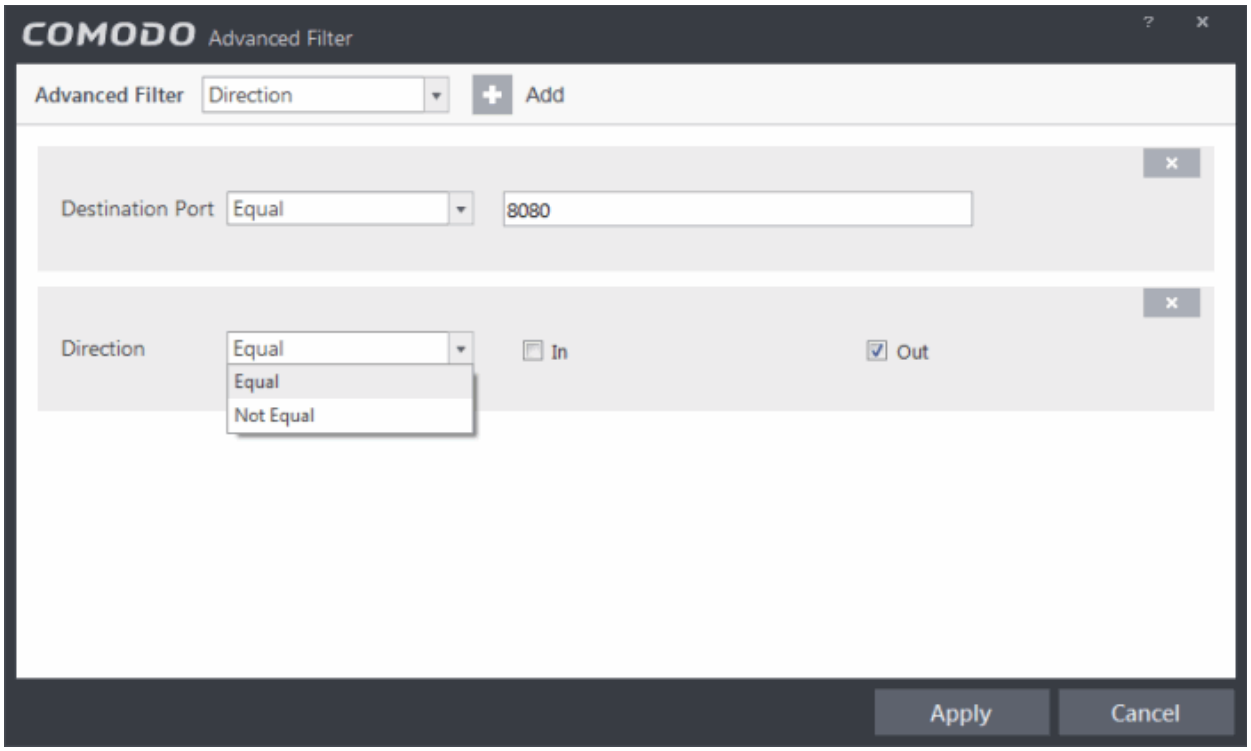
a) Select any one of the following option the drop-down box.
   - Equal
   - Greater than

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

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

For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

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

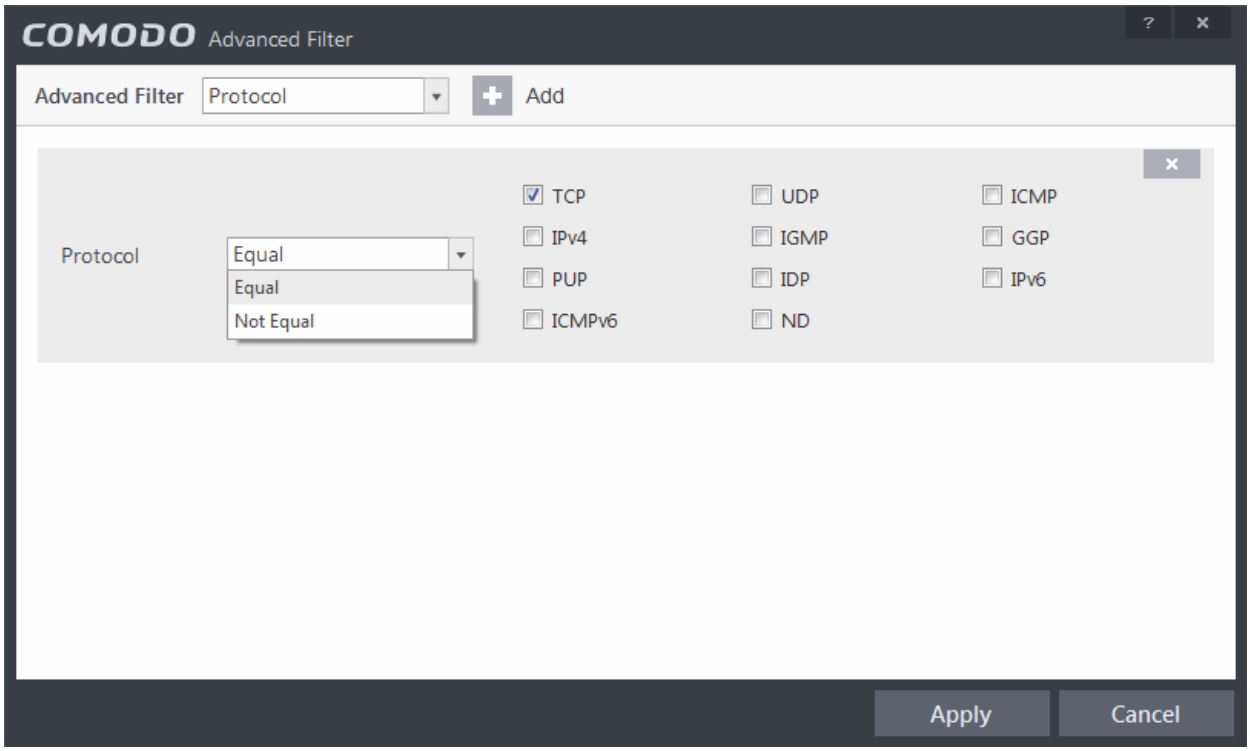


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

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

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

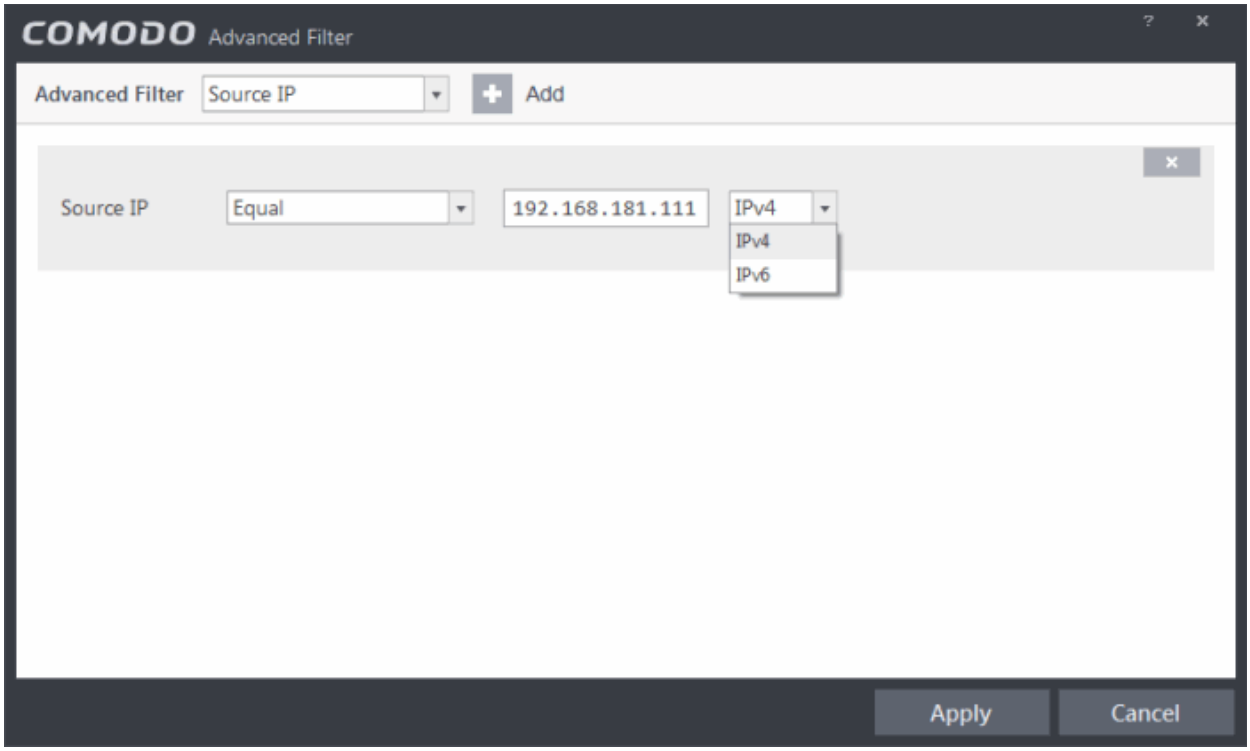


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

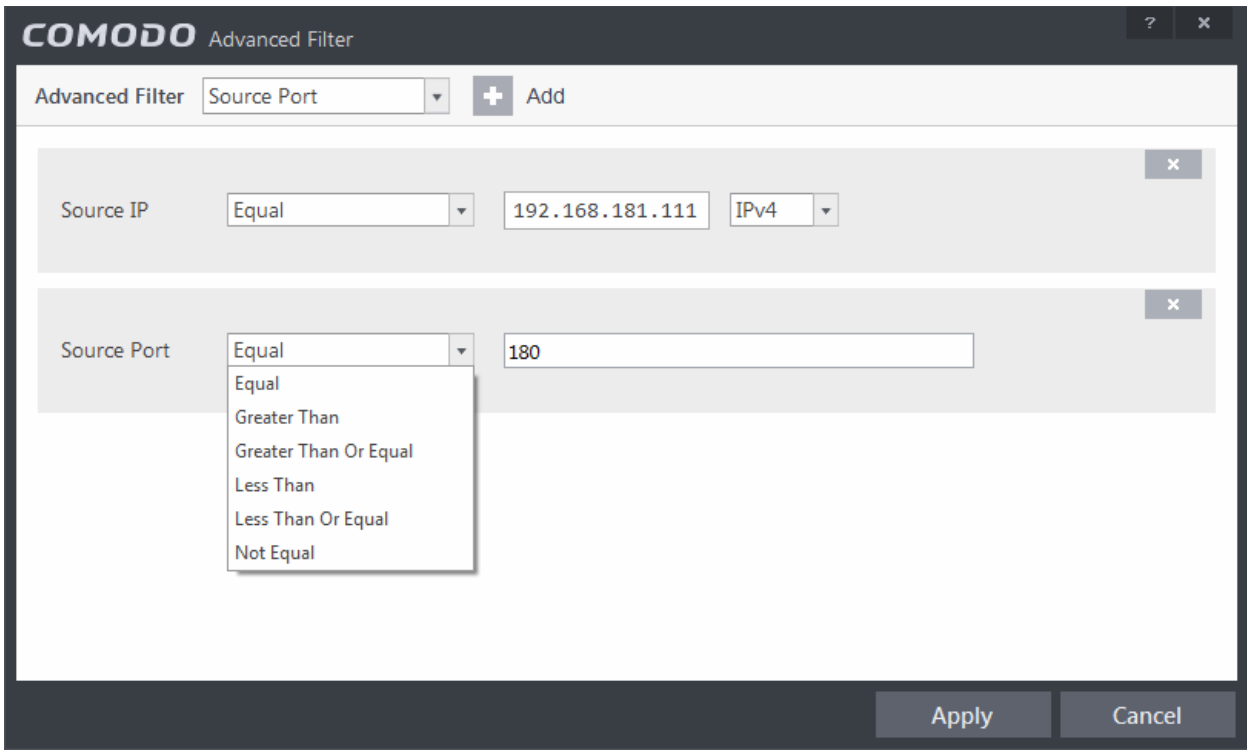
- TCP
- UDP
- ICMP
- IPV4
- IGMP
- GGP
- PUP
- IDP
- IPV6
- ICMPV6
- ND

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



a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Select 'IPv4' or 'IPv6' from the drop-down box.
c) Enter the source system's IP address that needs to be filtered.

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



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

- Less than
- Less than or Equal
- Not Equal

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

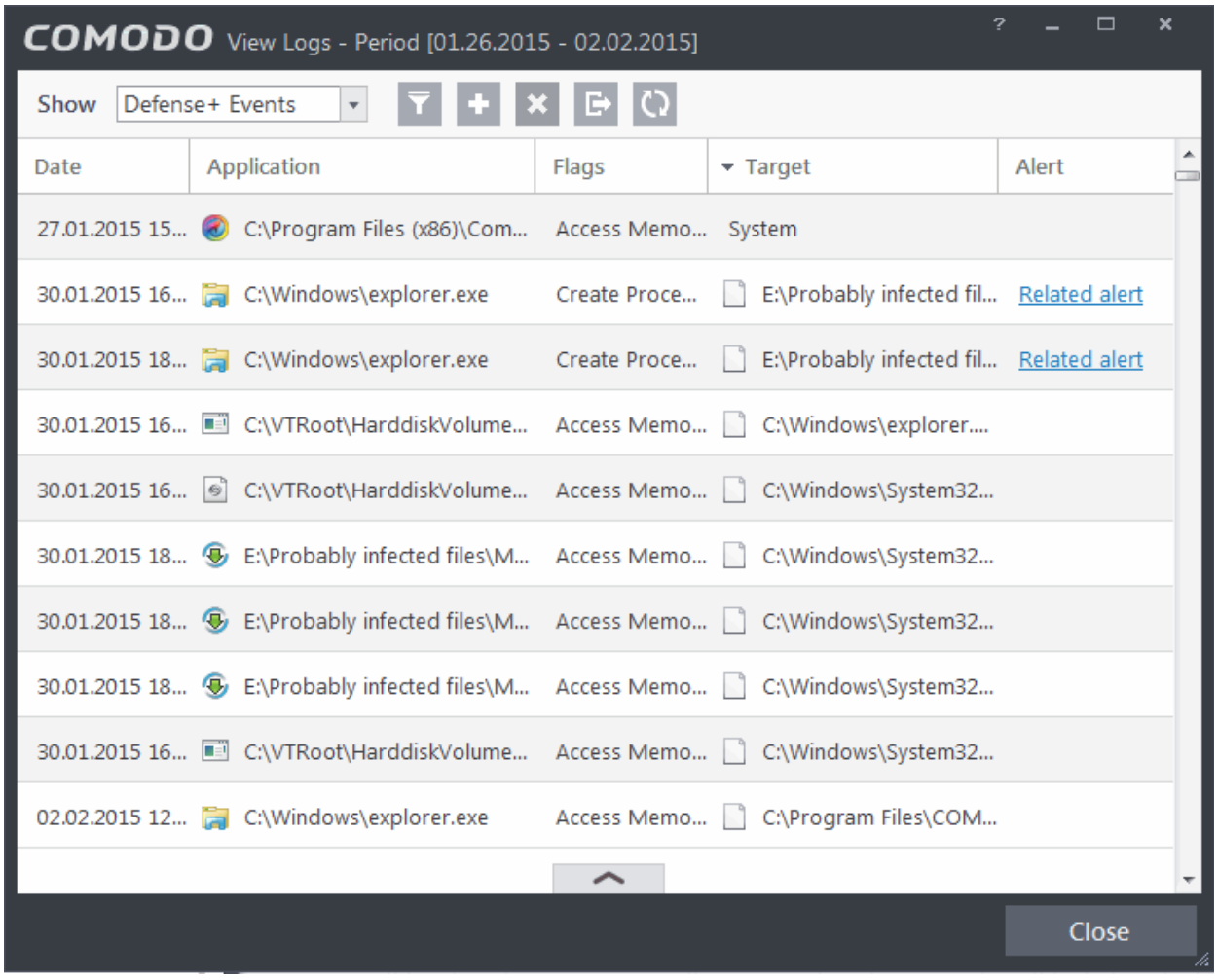
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.4. Defense+ Logs

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

The Defense+ logs can be viewed by selecting ' Defense+ Events' tab from the 'Show' drop-down of the log viewer interface. Alternatively, the Defense+ log screen can be accessed by clicking the number beside 'Blocked Intrusions' in the Advanced View of the Home screen in the Auto-Sandbox pane.



Column Descriptions

1. **Date** - Contains precise details of the date and time of the access attempt.
2. **Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used.
3. **Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
4. **Target** - Represents the location of the target file.
5. **Alert** - Gives the details of the alert displayed for the event

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

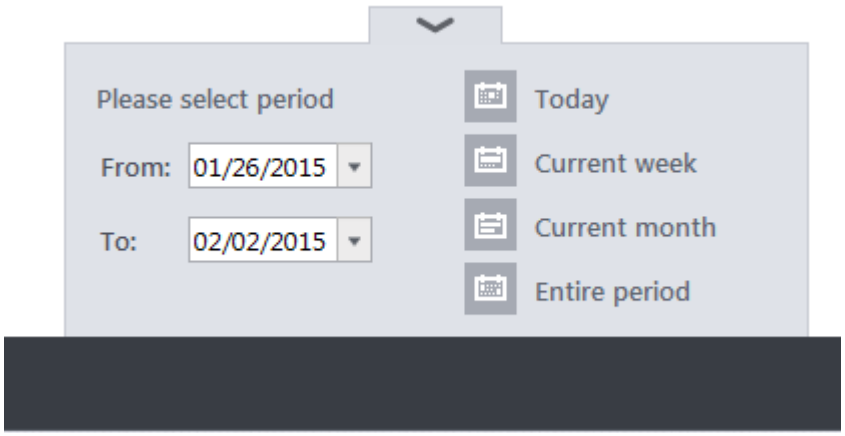
2.6.4.1. Filtering Defense+ Logs

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

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

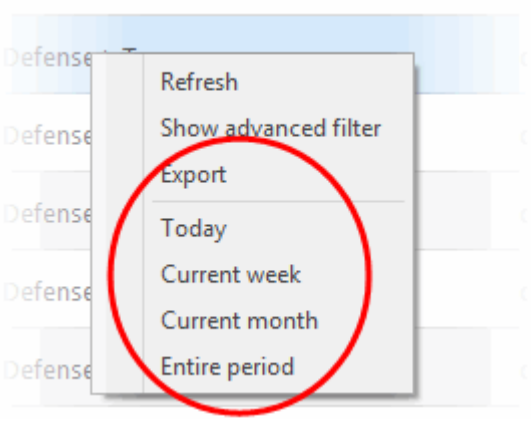
Preset Time Filters

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



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

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



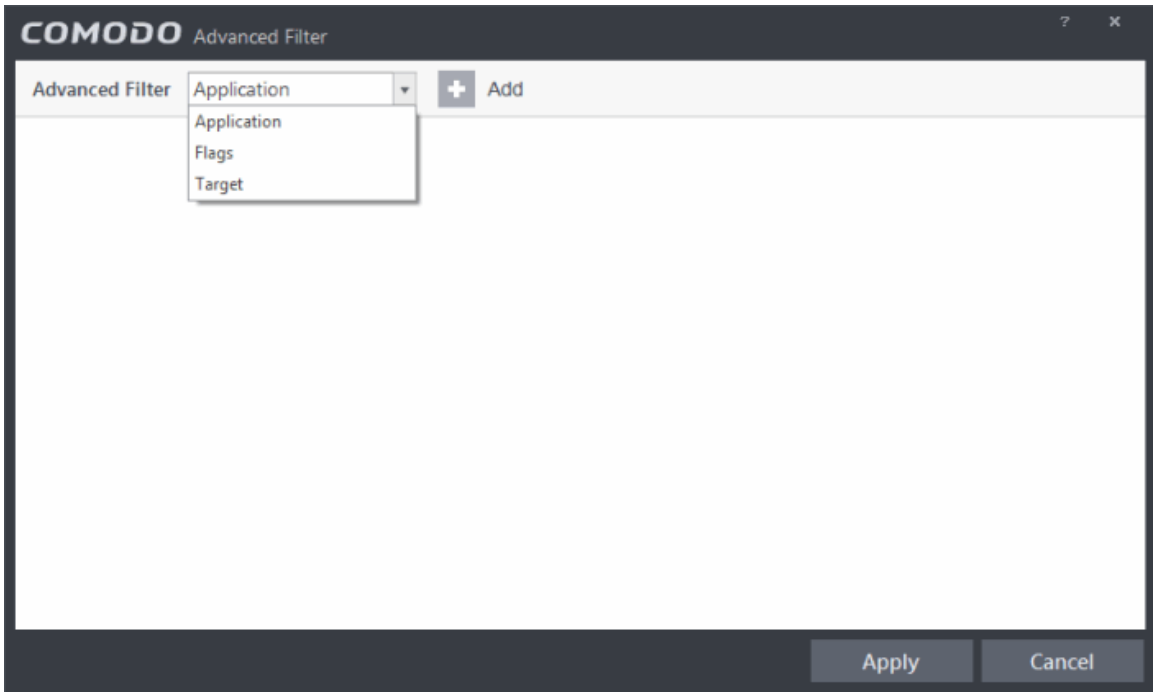
Advanced Filters

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

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

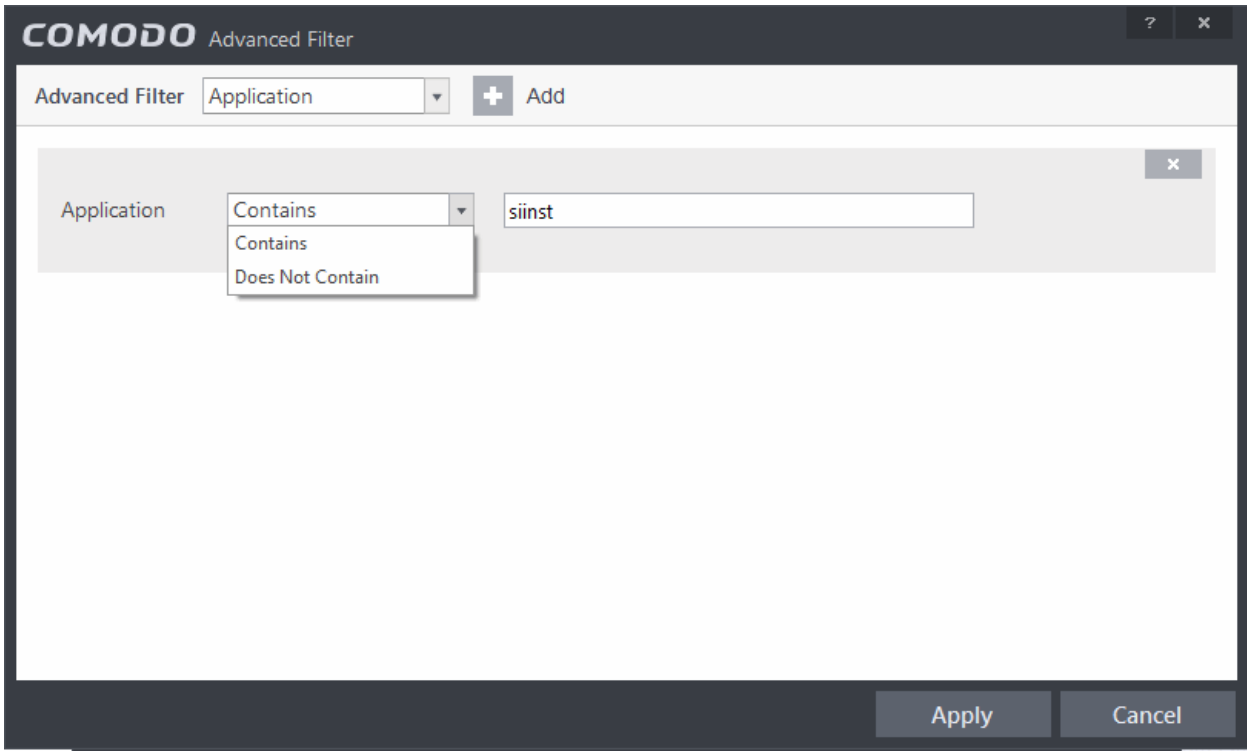
To configure Advanced Filters for Defense+ events

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



You have 3 categories of filter that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. Following are the options available in the 'Advanced Filter' drop-down:

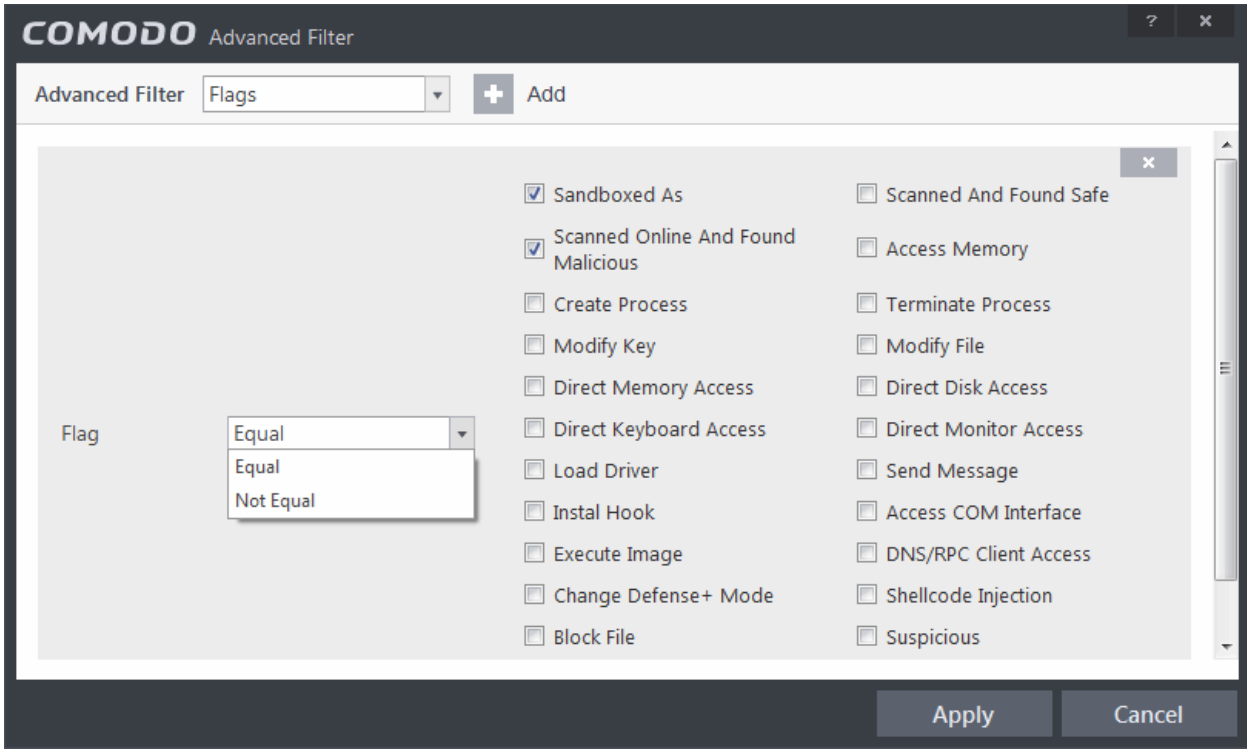
i. **Application**: Adding the 'Application' option displays a drop-down field and text entry field.



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

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

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



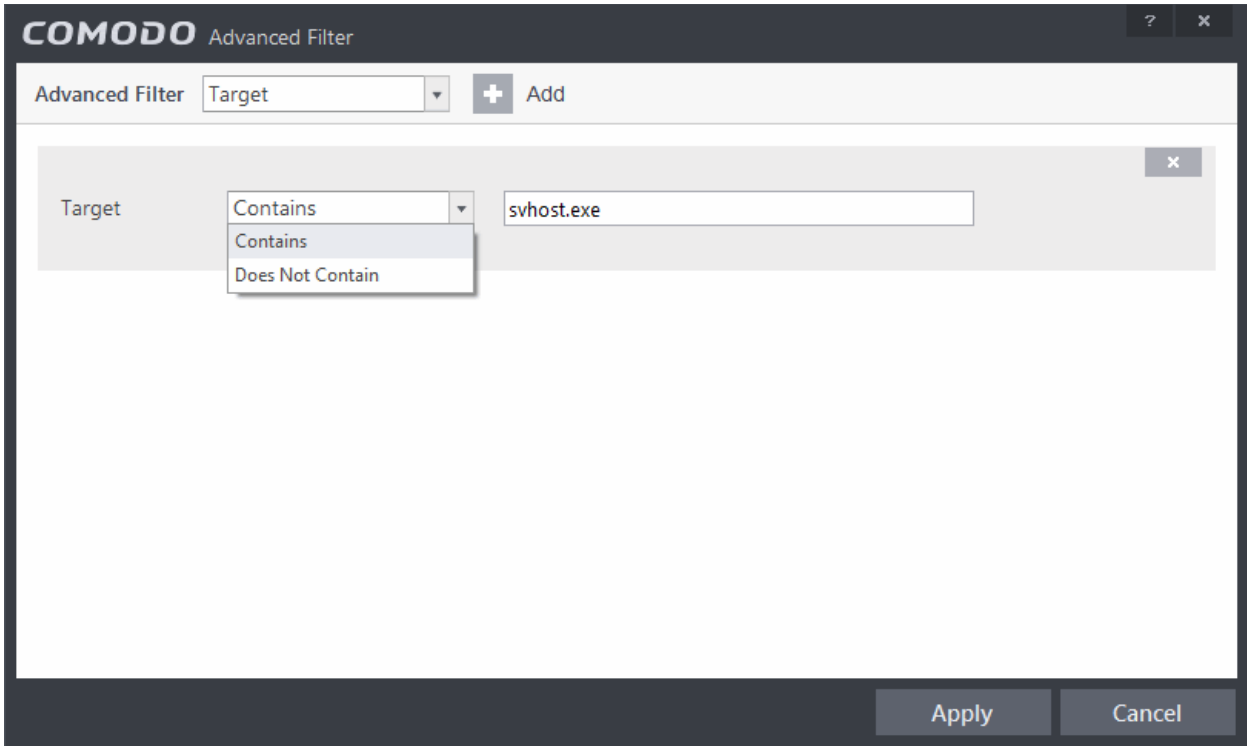
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- Sandboxed As
- Scanned Online and Found Safe
- Scanned Online and Found Malicious
- Access Memory
- Create Process
- Terminate Process
- Modify Key
- Modify File
- Direct Memory Access
- Direct Disk Access
- Direct Keyboard Access
- Direct Monitor Access
- Load Driver
- Send Message
- Install Hook
- Access COM Interface
- Execute Image
- DNS/RPC Client Access
- Change Defense+ Mode
- Shellcode Injection
- Block File
- Suspicious
- Hook
- Alert Suppressed

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

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



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

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

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

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

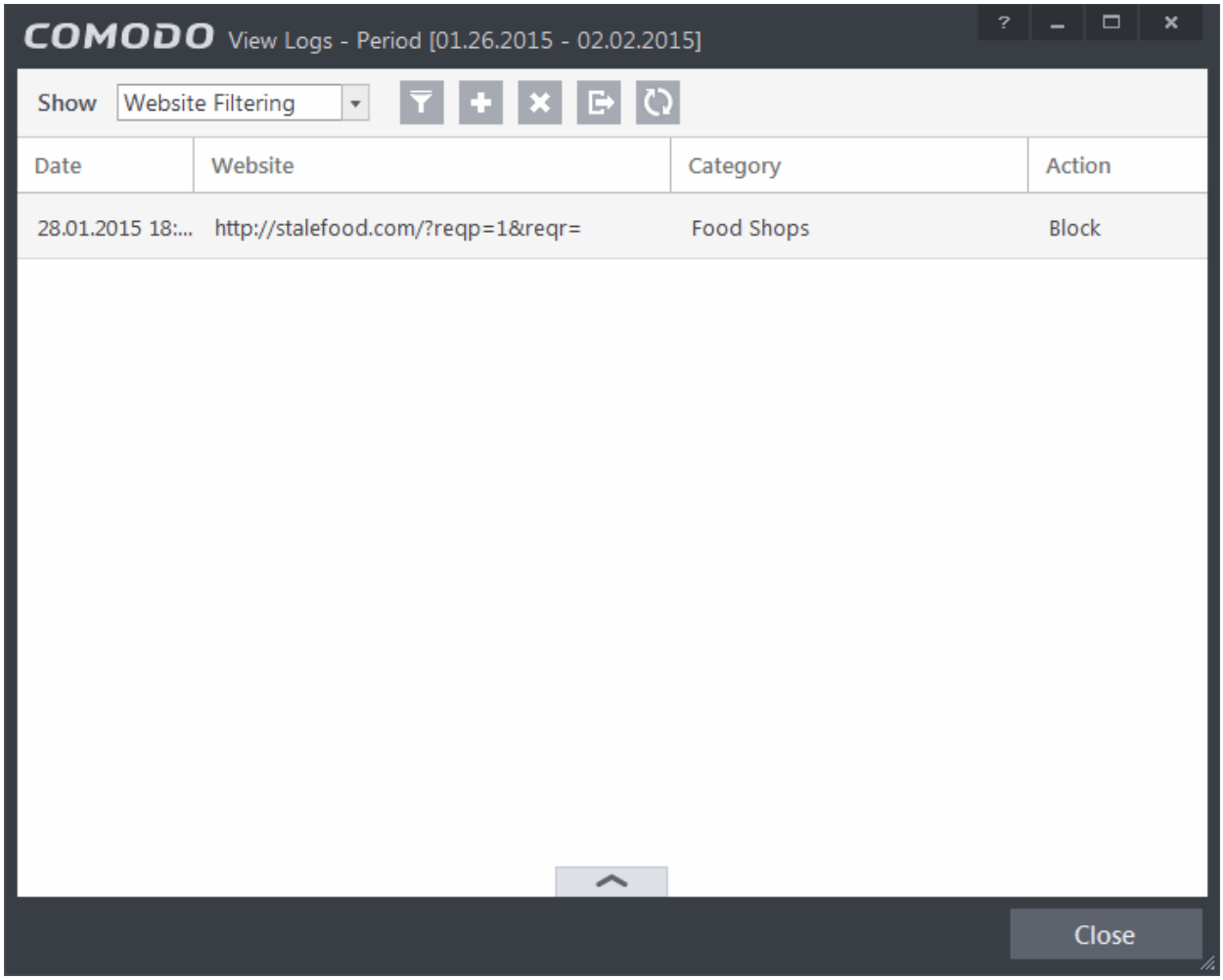
- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those Defense+ entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button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

2.6.5. 'Website Filtering' Logs

Comodo Internet Security maintains a log of Websites allowed or blocked to specific users by the 'Website Filter'.

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

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



Column Descriptions

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

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

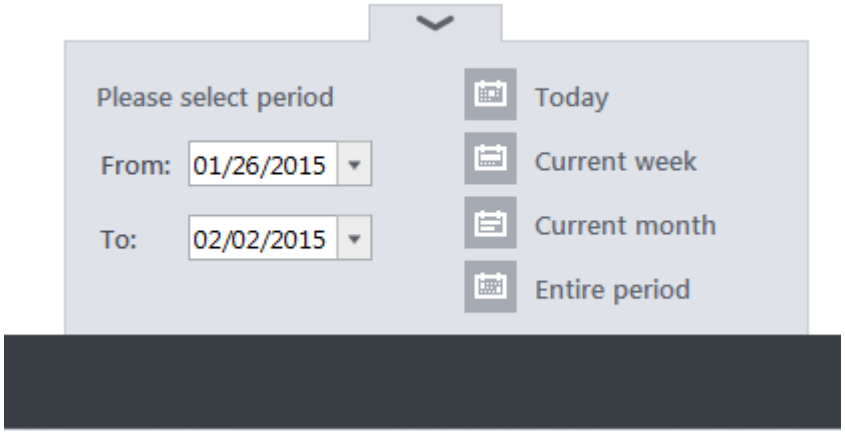
2.6.5.1. Filtering 'Website Filtering' Logs

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

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

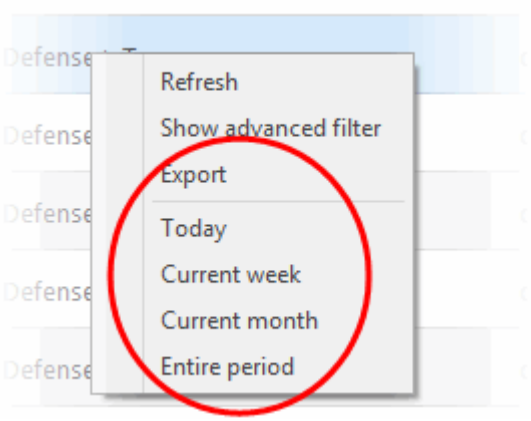
Preset Time Filters

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



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

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



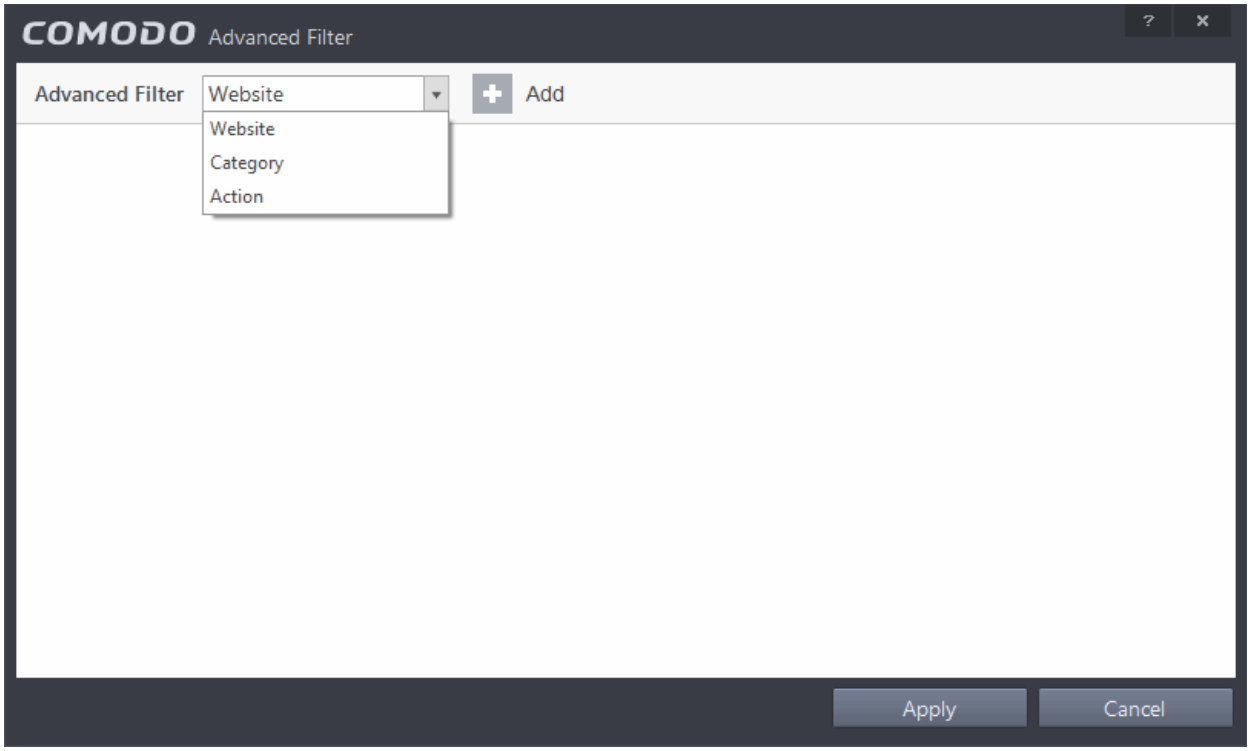
Advanced Filters

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

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

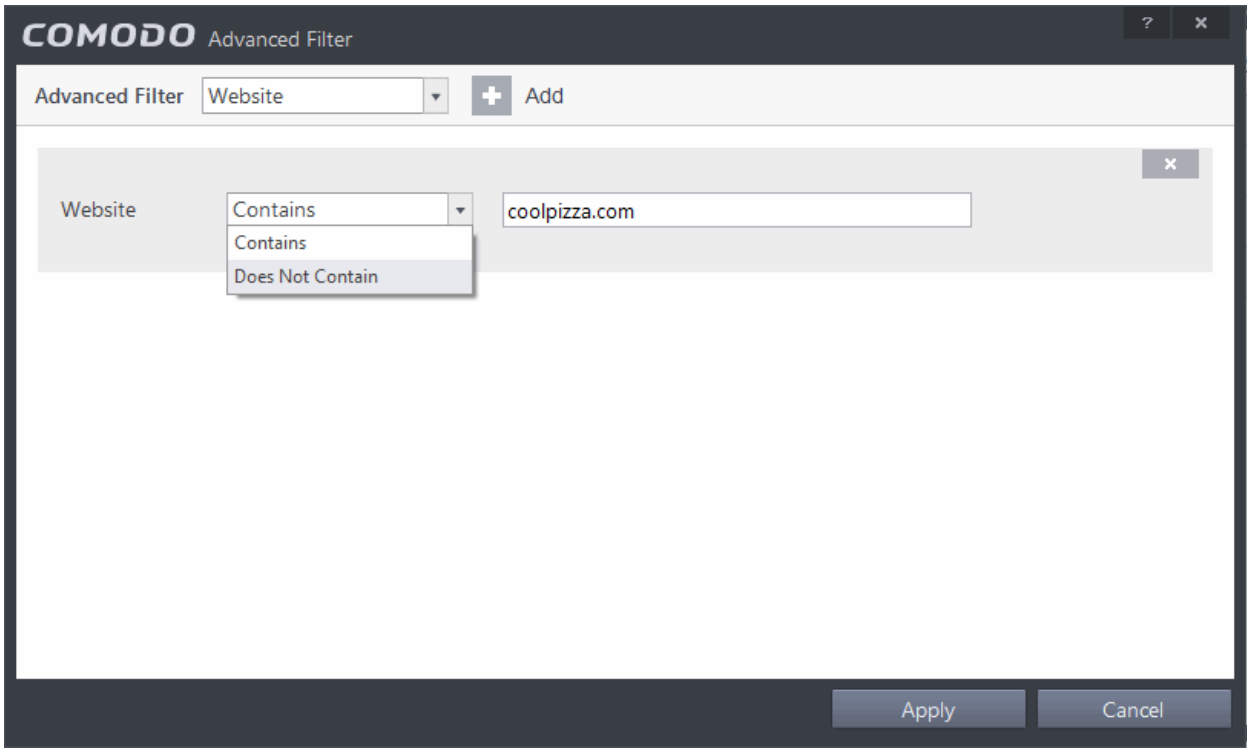
To configure Advanced Filters for Defense+ events

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



You have 3 categories of filter that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. Following are the options available in the 'Advanced Filter' drop-down:

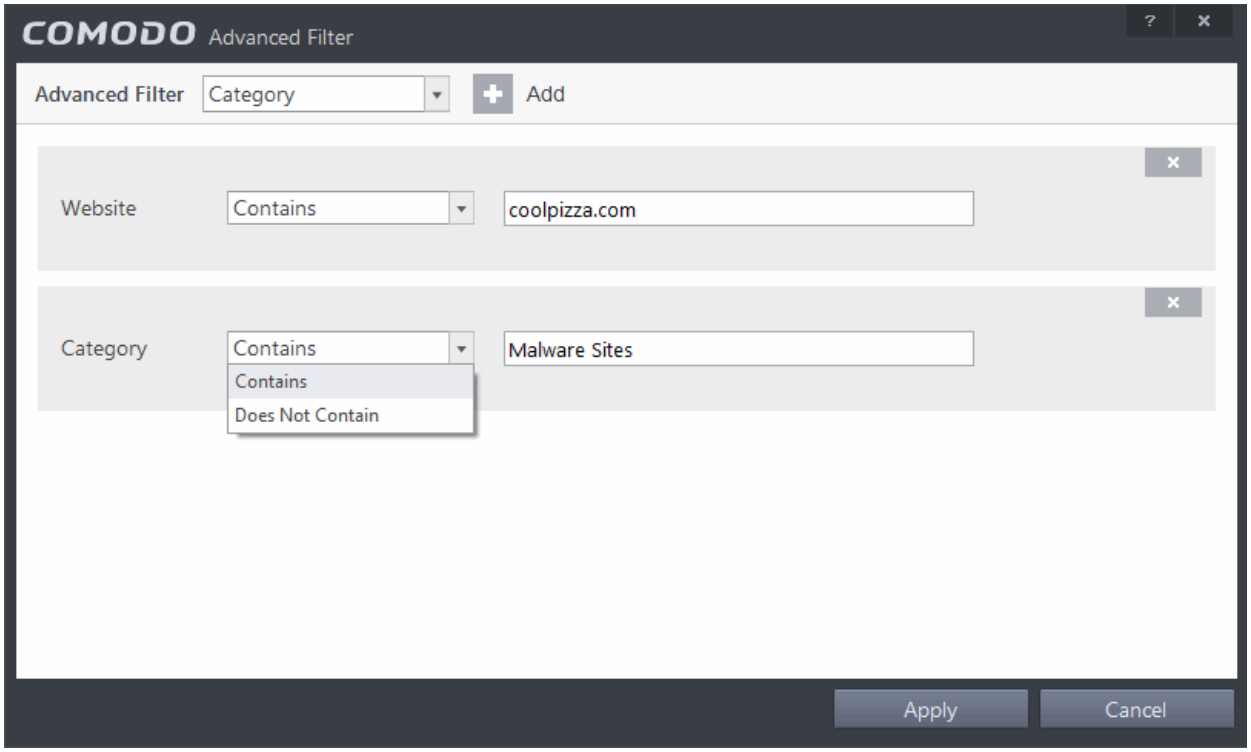
i. **Website**: Adding the 'Website' option displays a drop-down menu and text entry field.



a) Select 'Equal' or 'Not Equal' option from the drop-down menu.
b) Enter the url of the website that needs to be filtered.

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

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

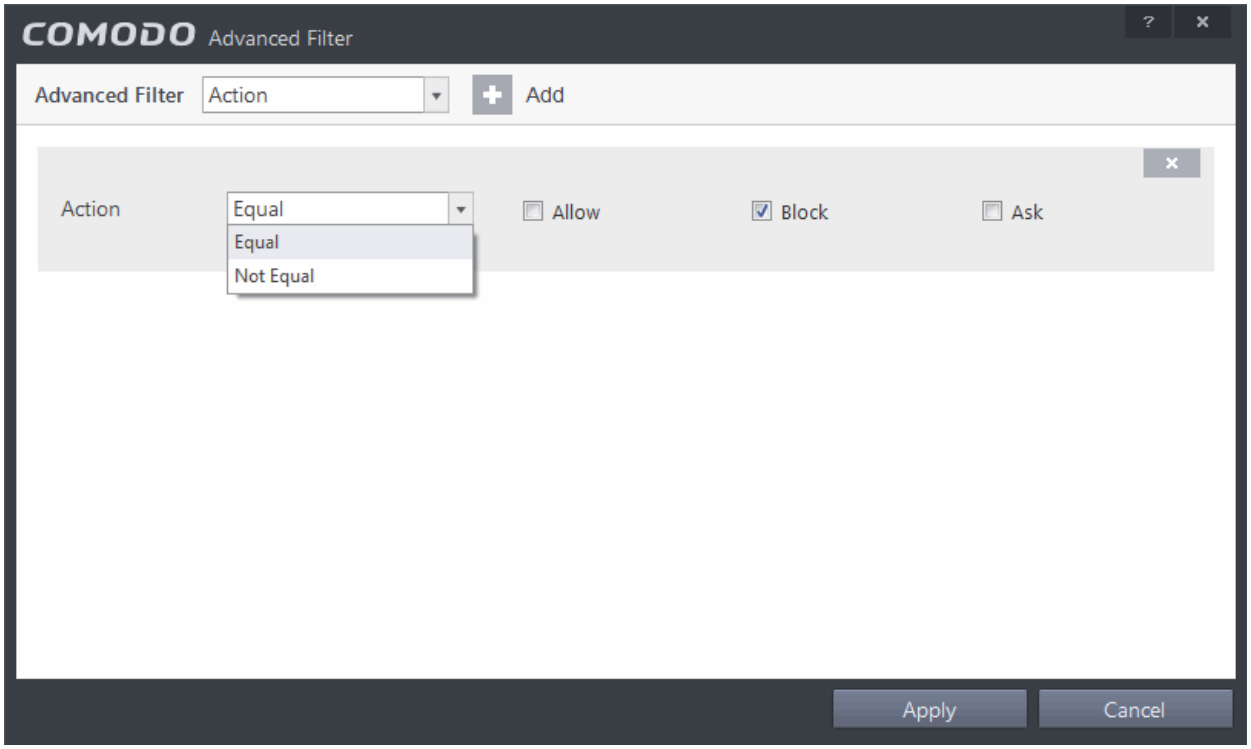


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

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



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

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

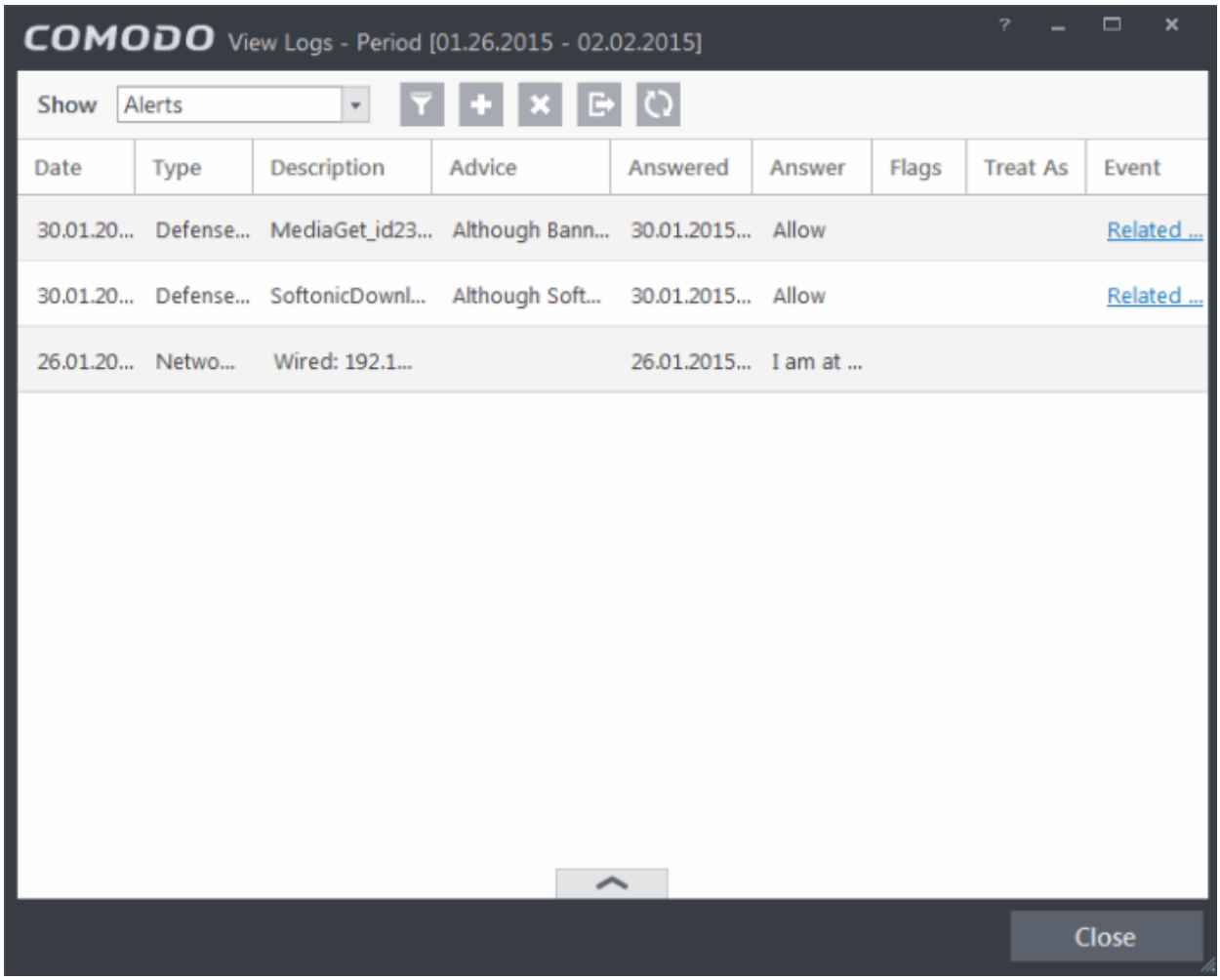
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.6. 'Alerts' Logs

CIS maintains a history of pop-up security alerts generated by its Antivirus, Firewall and Defense+ components and the actions taken against the threats discovered, depending on the response to the alerts by the user.

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



Column Descriptions

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

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

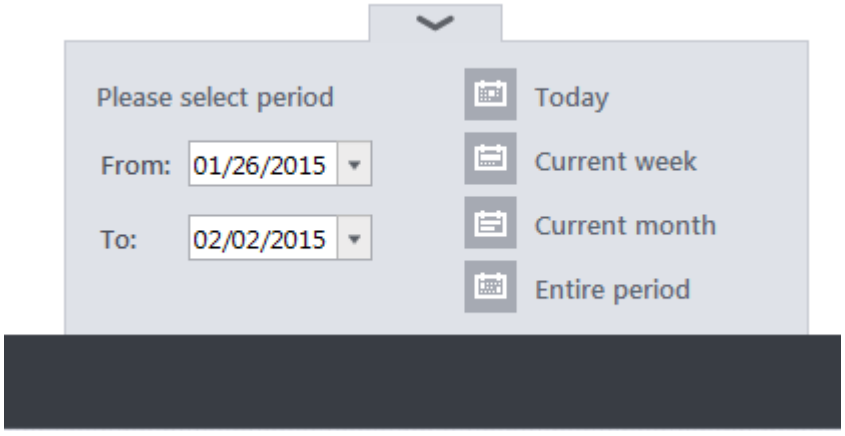
2.6.6.1. Filtering 'Alerts Displayed' Logs

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

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

Preset Time Filters

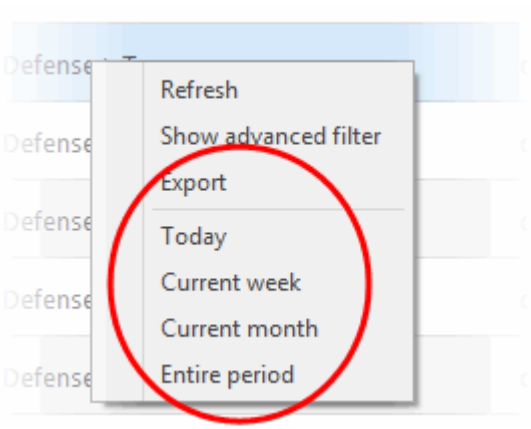
Clicking on the handle at the bottom enables you to filter the logs for a selected time period:



- **Today** - Displays all logged events for today.
- **Current Week** - Displays all logged events during the current week. (The current week is calculated from the Sunday to Saturday that holds the current date.)
- **Current Month** - Displays all logged events during the month that holds the current date.
- **Entire Period** - Displays every event logged since Comodo Internet Security was installed. (If you have cleared the log history since installation, this option shows all logs created since that clearance).

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

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



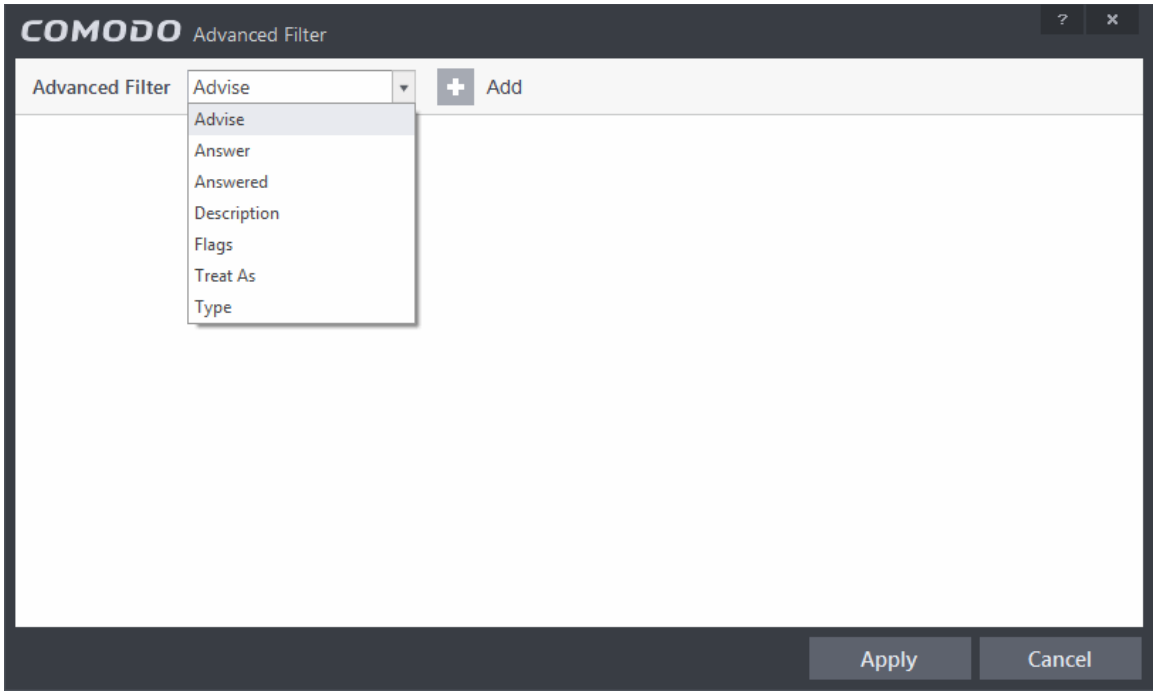
Advanced Filters

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

- **Advice:** Displays only the log of alerts that matches the advice entered
- **Answer:** Displays only the log of alerts that were answered by you with the selected response
- **Answered** Displays only the log of alerts that were answered on a selected date and time
- **Description:** Displays only the log of alerts that matches the description entered
- **Flags:** Displays only the log of alerts based on the selected flags set for the corresponding events
- **Treat As:** Displays only the log of alerts based on their 'Treat As' response you entered in the pop-up alert
- **Type:** Displays only the log of alerts of selected type. They can be Antivirus, Firewall or Defense+ (HIPS, Behavior Blocker or Auto-Sandbox) alerts.

To configure Advanced Filters for Alerts Displayed

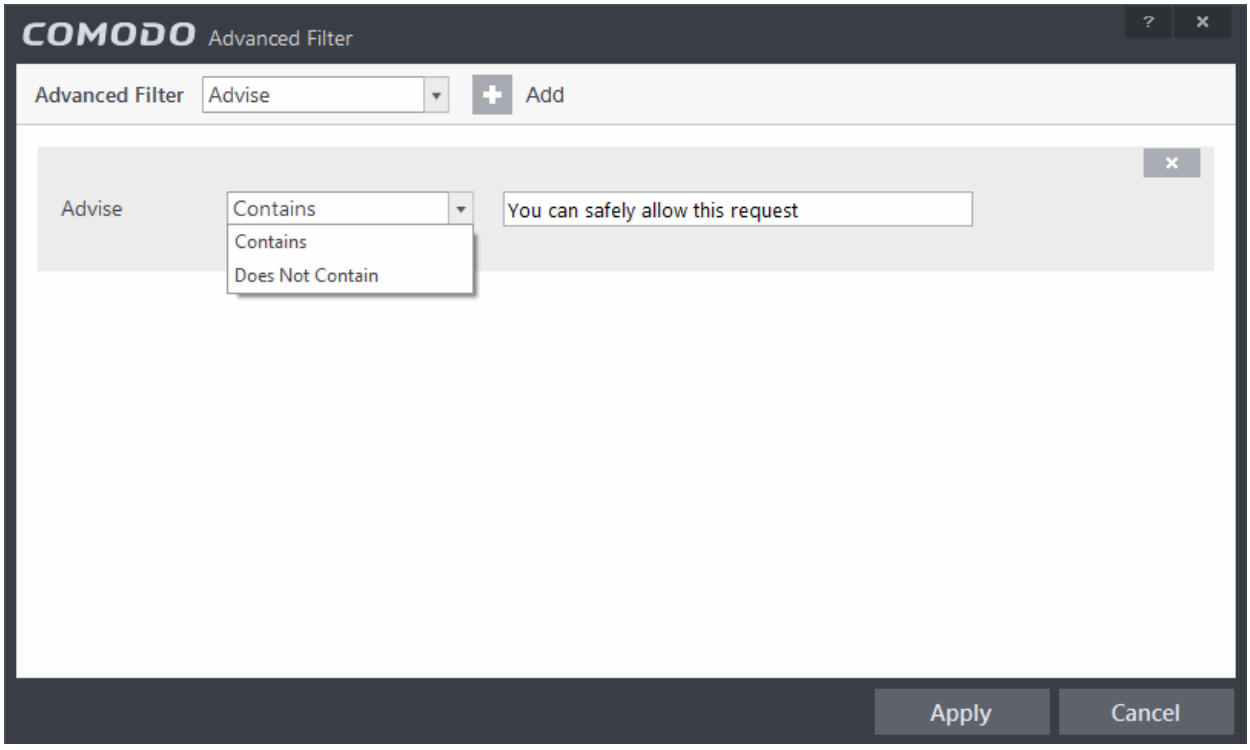
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Alerts' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the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



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

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

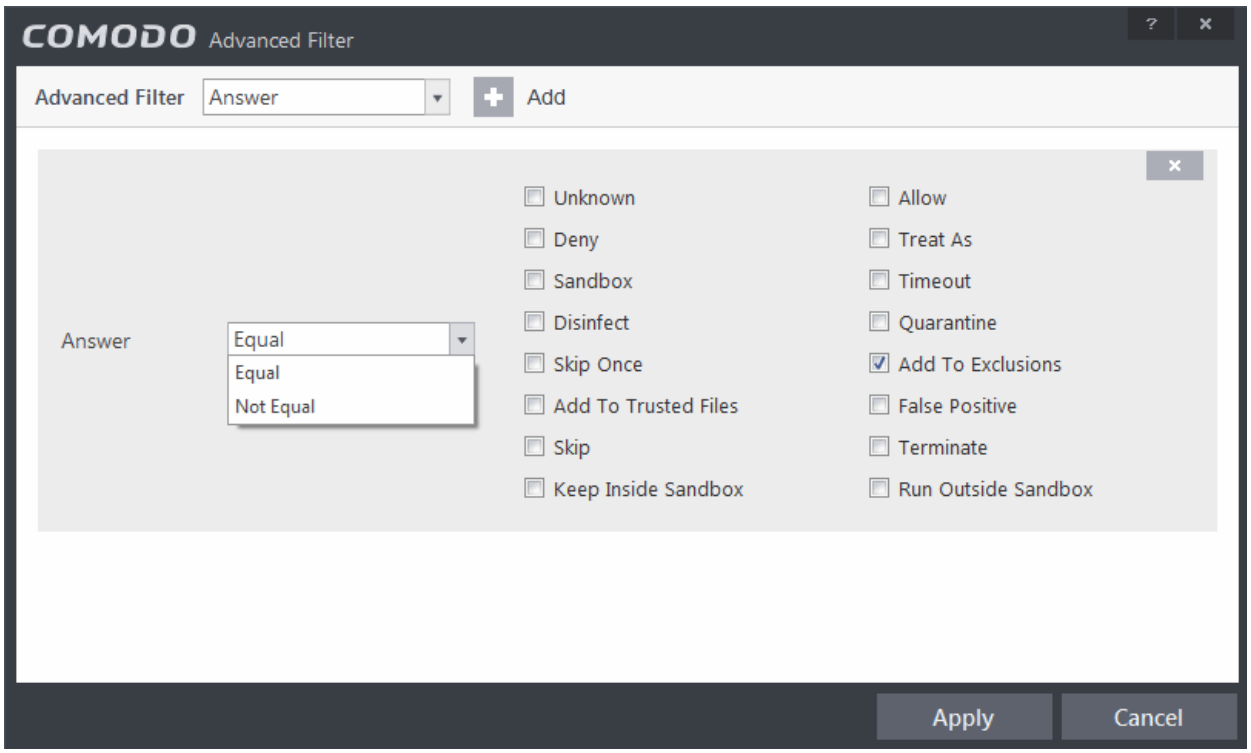
i. **Advice**: The 'Advise' option enables you to filter the alerts based on advices given by CIS in the alert. Selecting the 'Advice' option displays a drop-down field and text entry field.



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

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

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



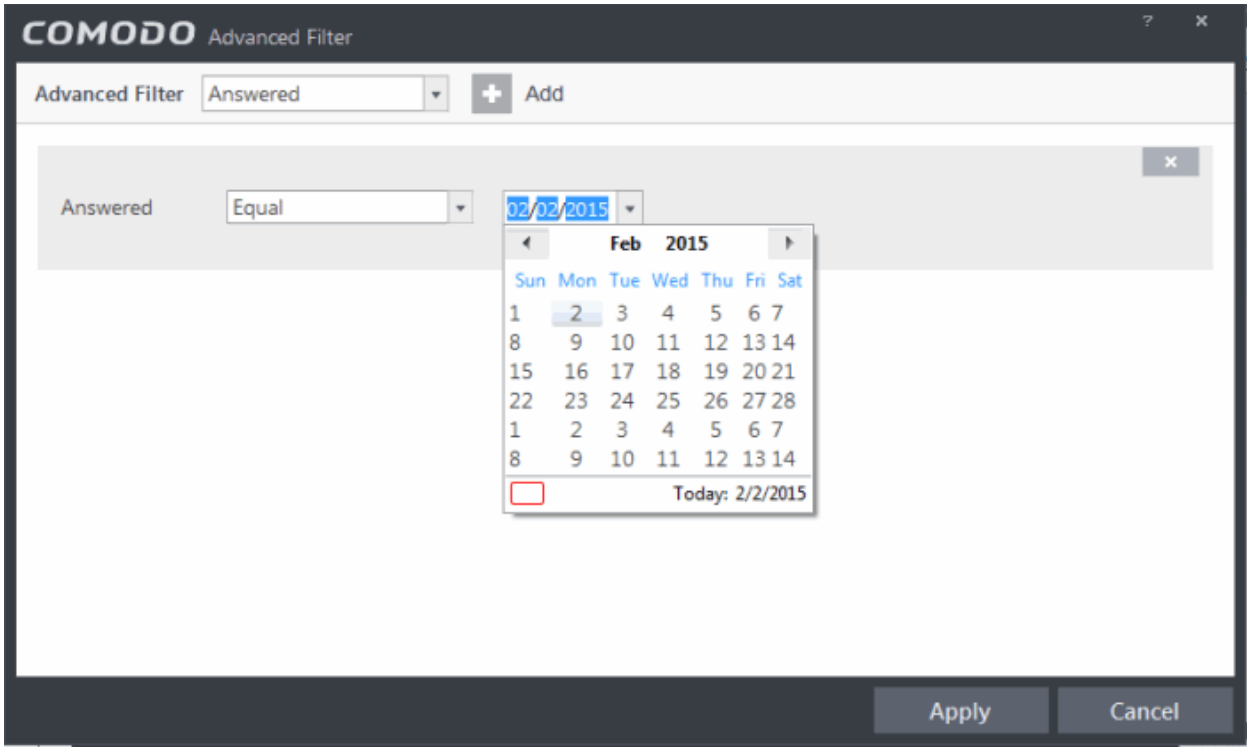
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- Unknown
- Allow
- Deny
- Treat As
- Sandbox
- Time-out
- Disinfect
- Quarantine
- Skip Once
- Add to Exclusions
- Add to Trusted Files
- False Positive
- Skip
- Terminate
- Keep inside Sandbox
- Run outside Sandbox

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

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

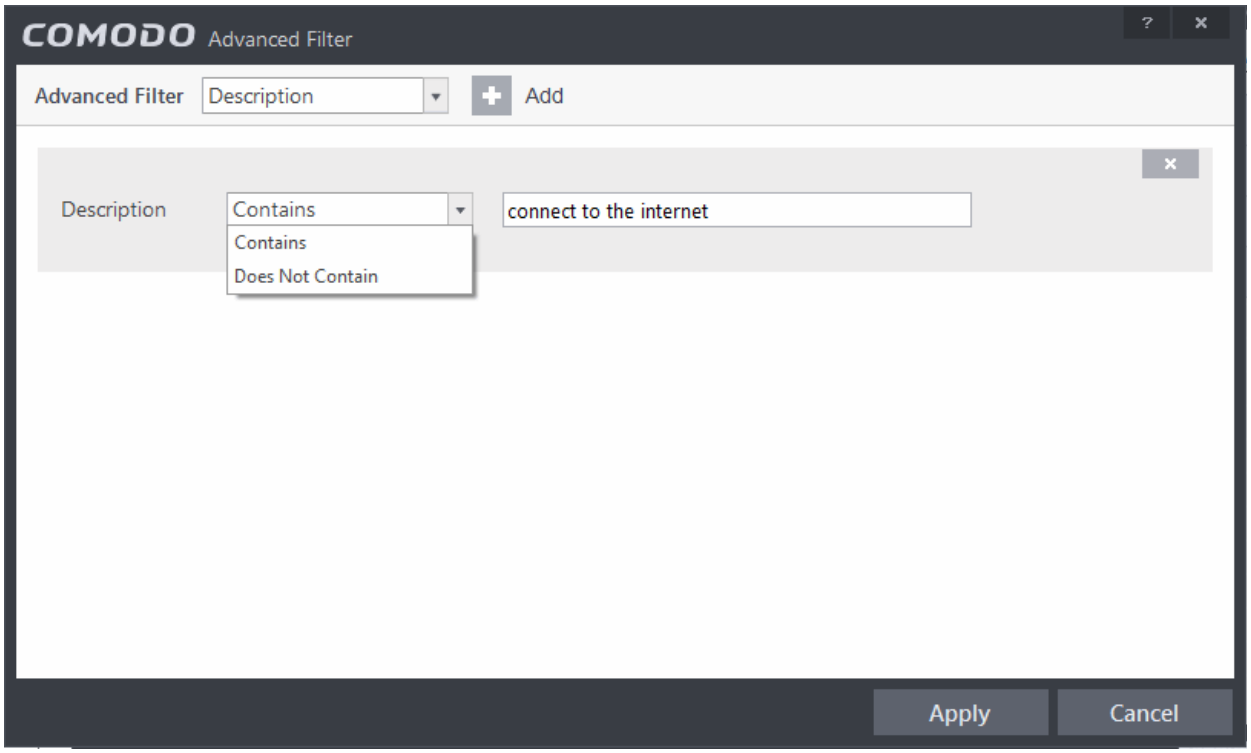


a) Select any one of the following option the drop-down box.
   - Equal
   - Not Equal

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

For example, if you select 'Equal' from the drop-down and select '01/22/2014', only the log of alerts answered on 01/22/2014 will be displayed.

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

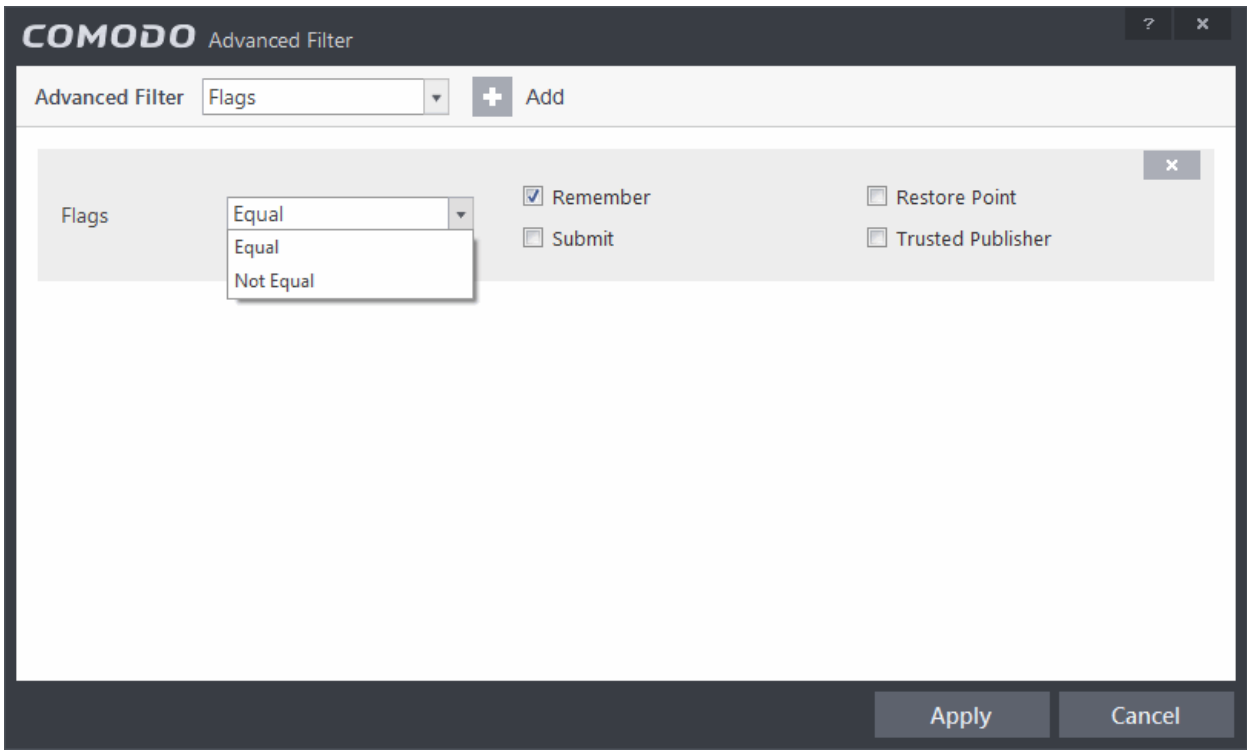


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

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



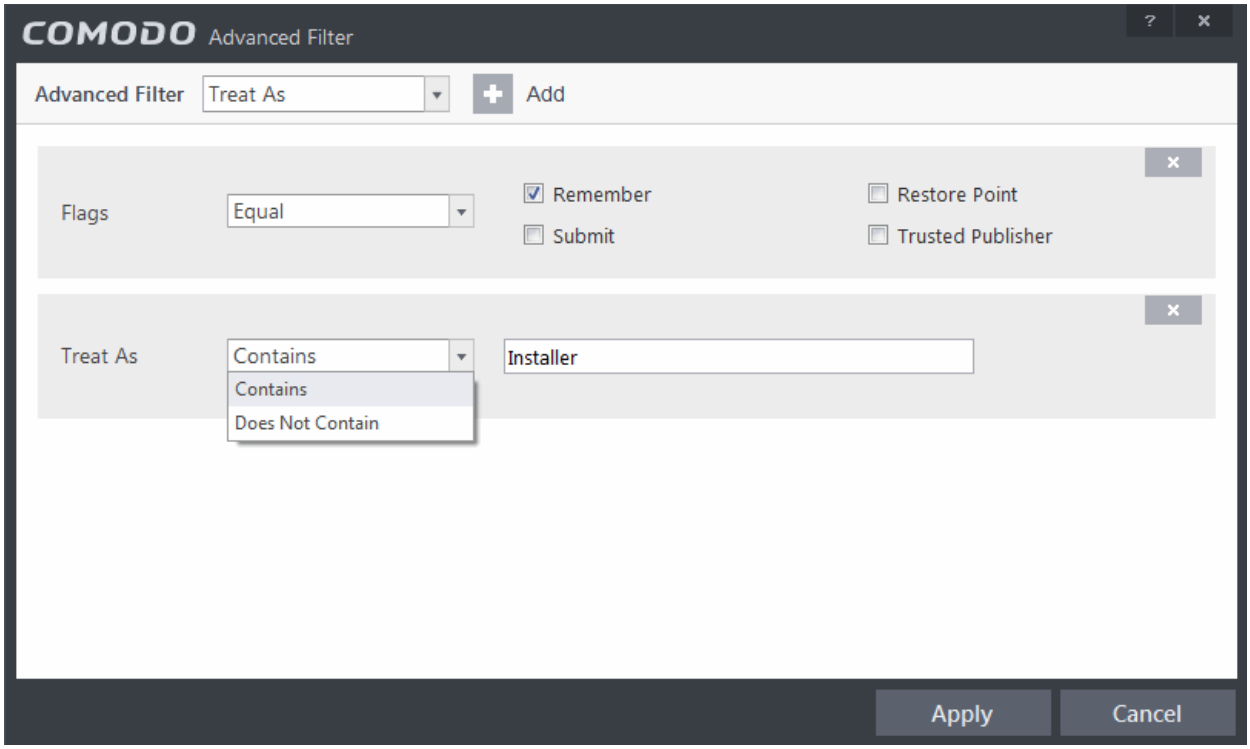
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- Remember
- Restore Point
- Submit
- Trusted Publisher

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

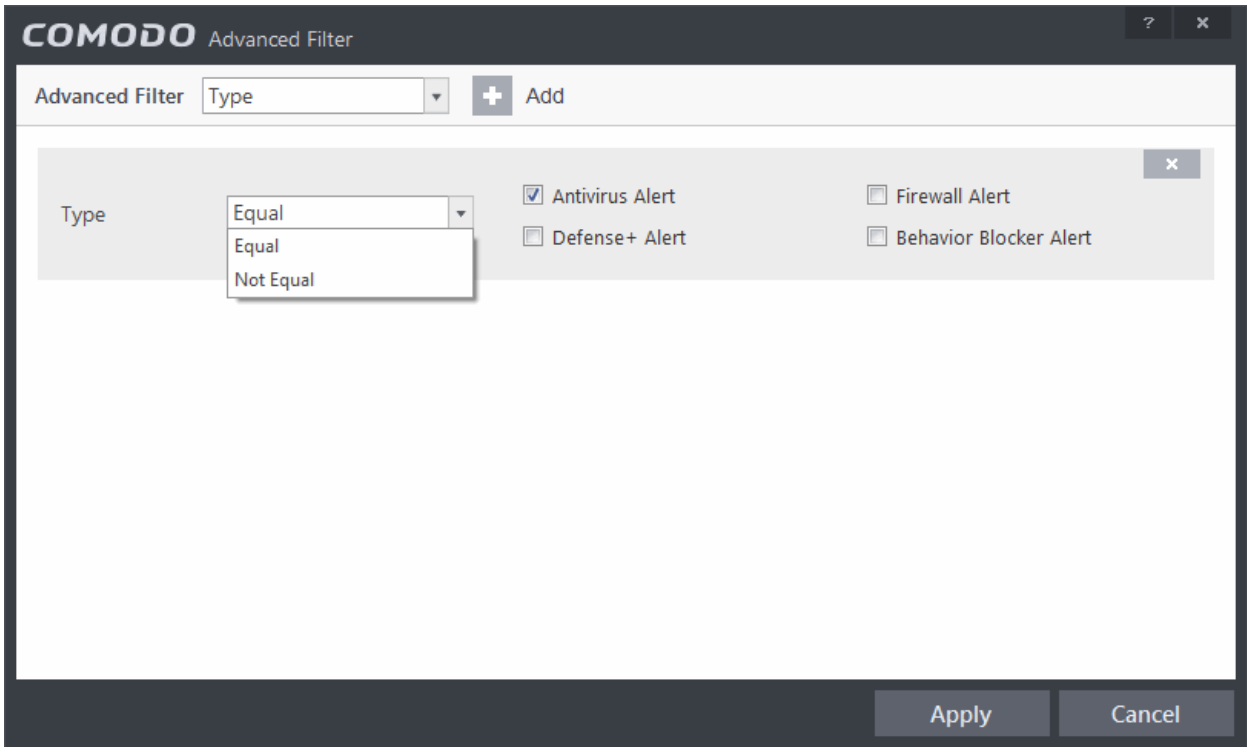
vi. **Treat As**: The 'Treat As' enables you to filter the log entries based on their 'Treat As' response you entered in the pop-up alert. Selecting the 'Treat As' option displays a drop-down menu and text entry field.



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

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

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



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

are:

- Antivirus Alert
- Firewall Alert
- Defense+ Alert
- Behavior Blocker Alert

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

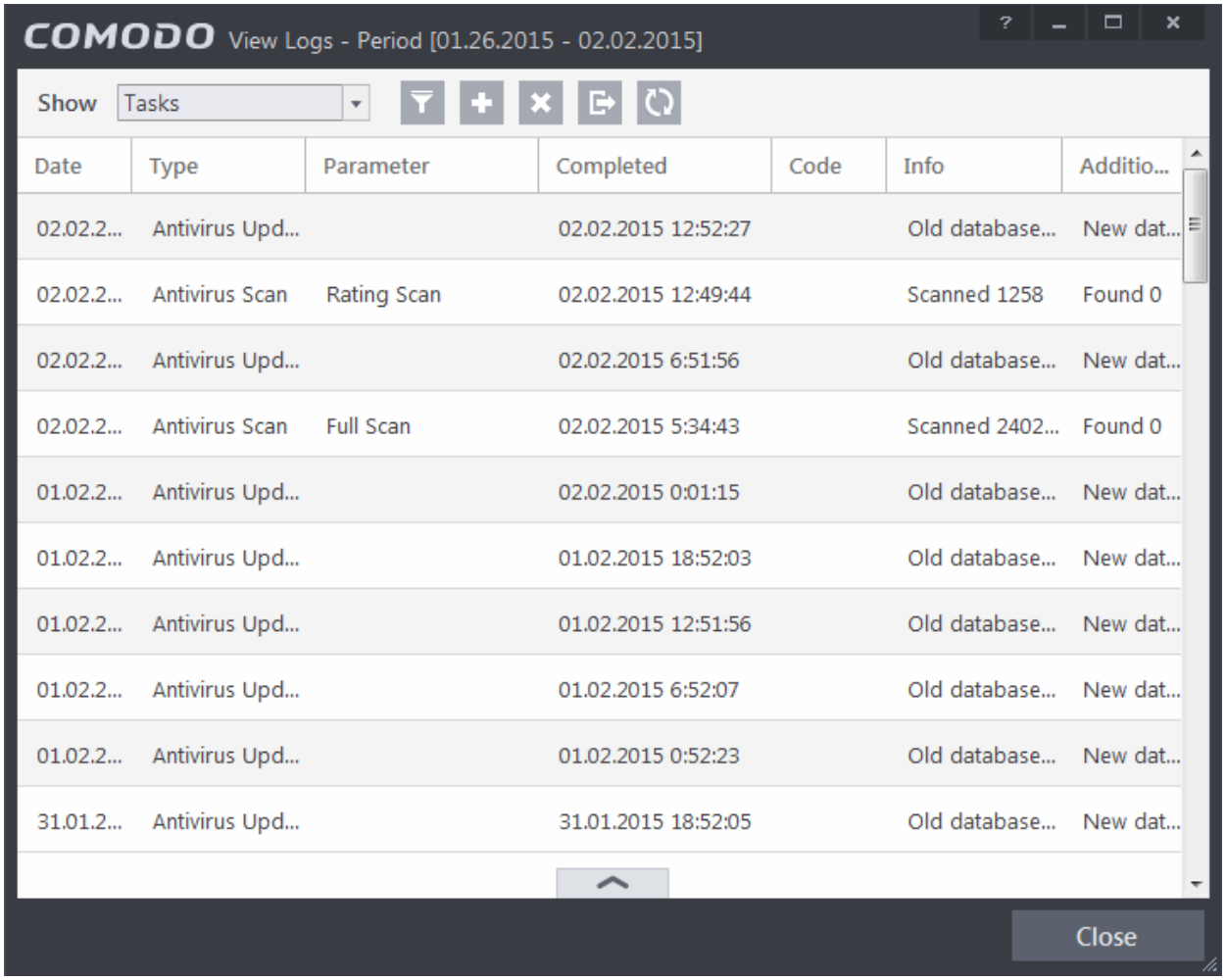
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.7. Tasks

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

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



Column Descriptions

1. **Date** - Contains precise details of the date and time when the task is launched.

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

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

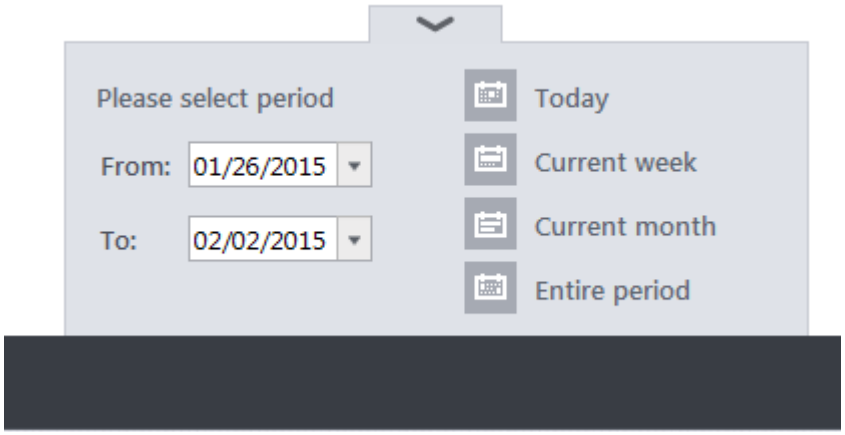
2.6.7.1. Filtering 'Tasks Launched' Logs

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

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

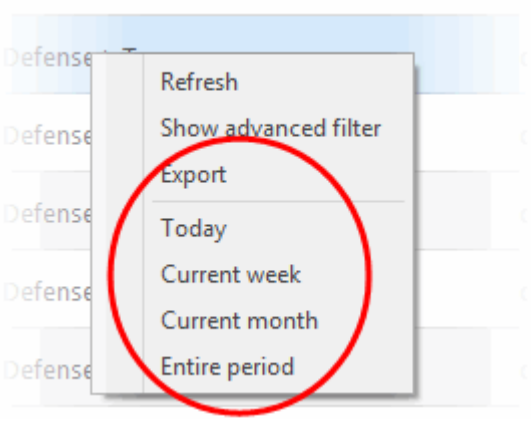
Preset Time Filters

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



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

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



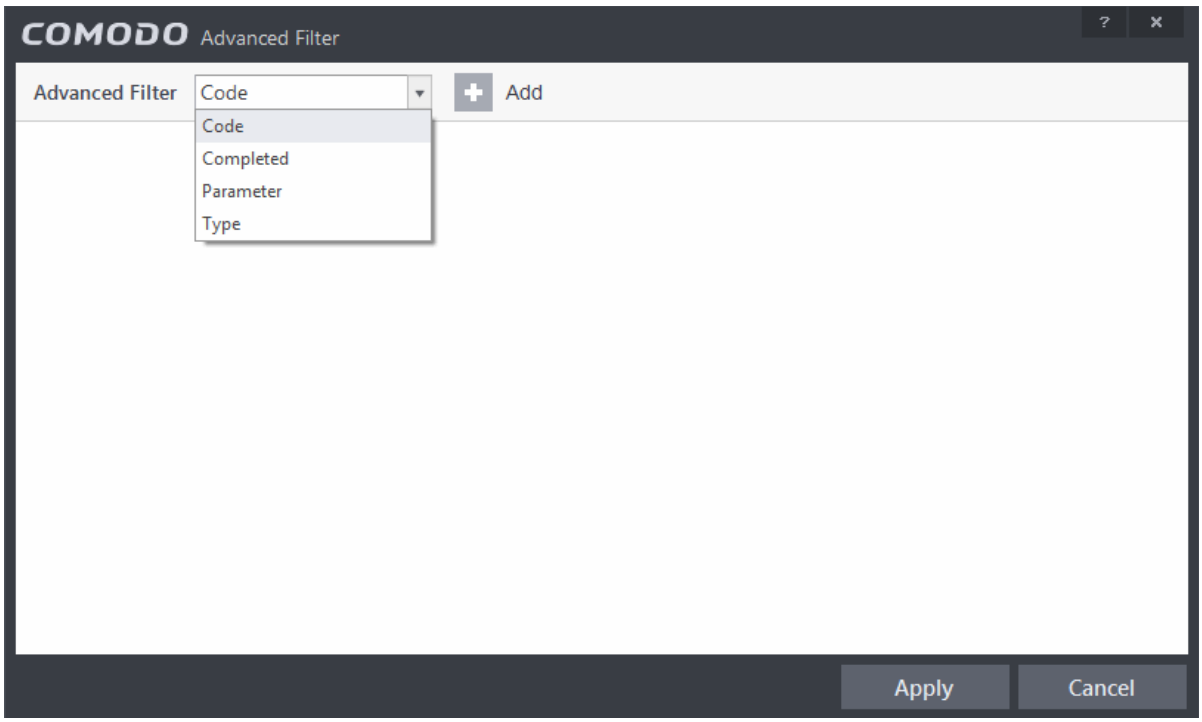
Advanced Filters

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

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

To configure Advanced Filters for 'Tasks' logs

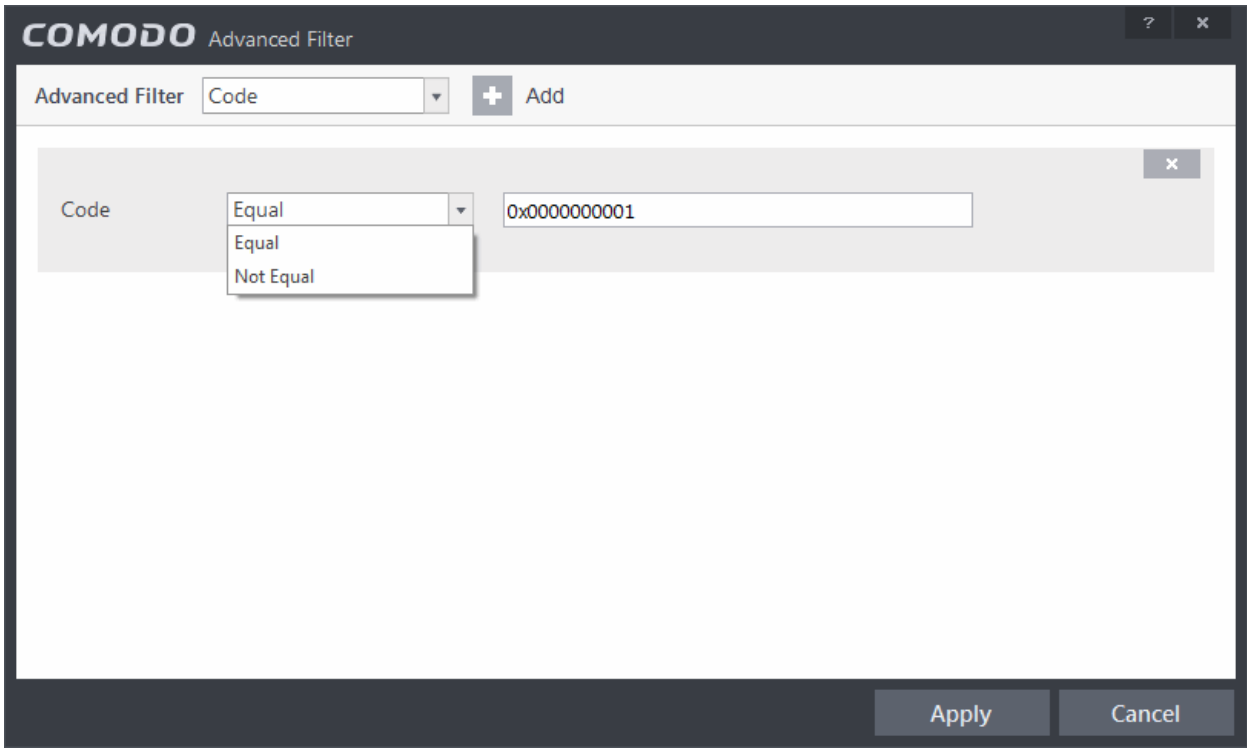
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Tasks log viewer will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply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



You can chose the category of filter from a drop down box. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.

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

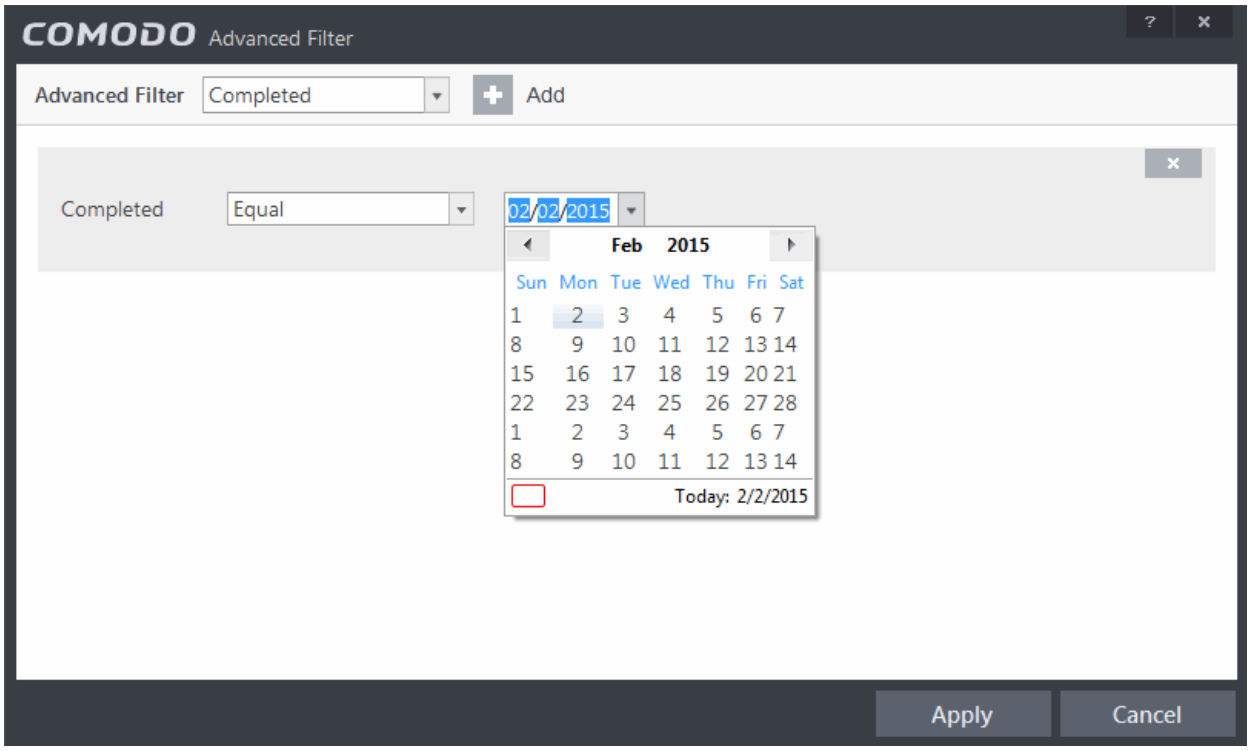
i. **Code**: The Code option enables you to filter the tasks based on their code value. Selecting the 'Code' option displays a drop-down field and text entry field.



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

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

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

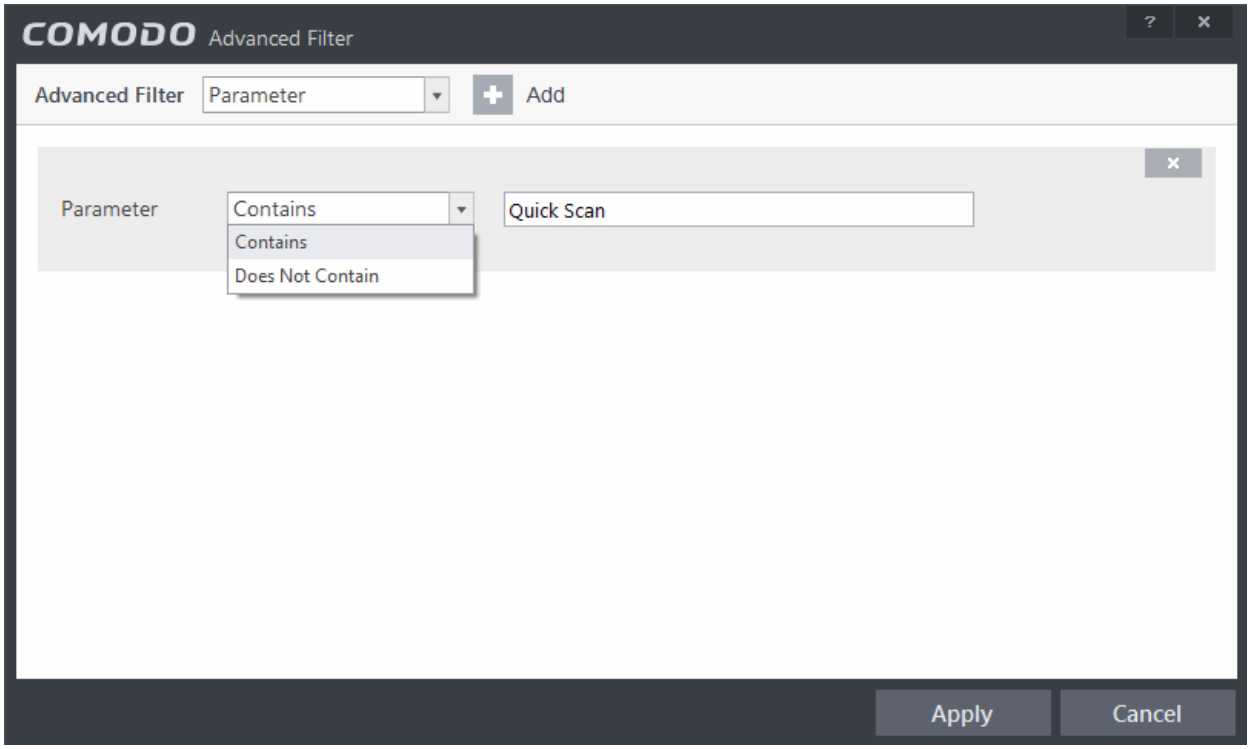


a) Select any one of the following option the drop-down box.
   - Equal
   - Not Equal

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

For example, if you select 'Equal' from the drop-down and select '01/22/2014' , only the log of Tasks completed on 01/22/2014 will be displayed.

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

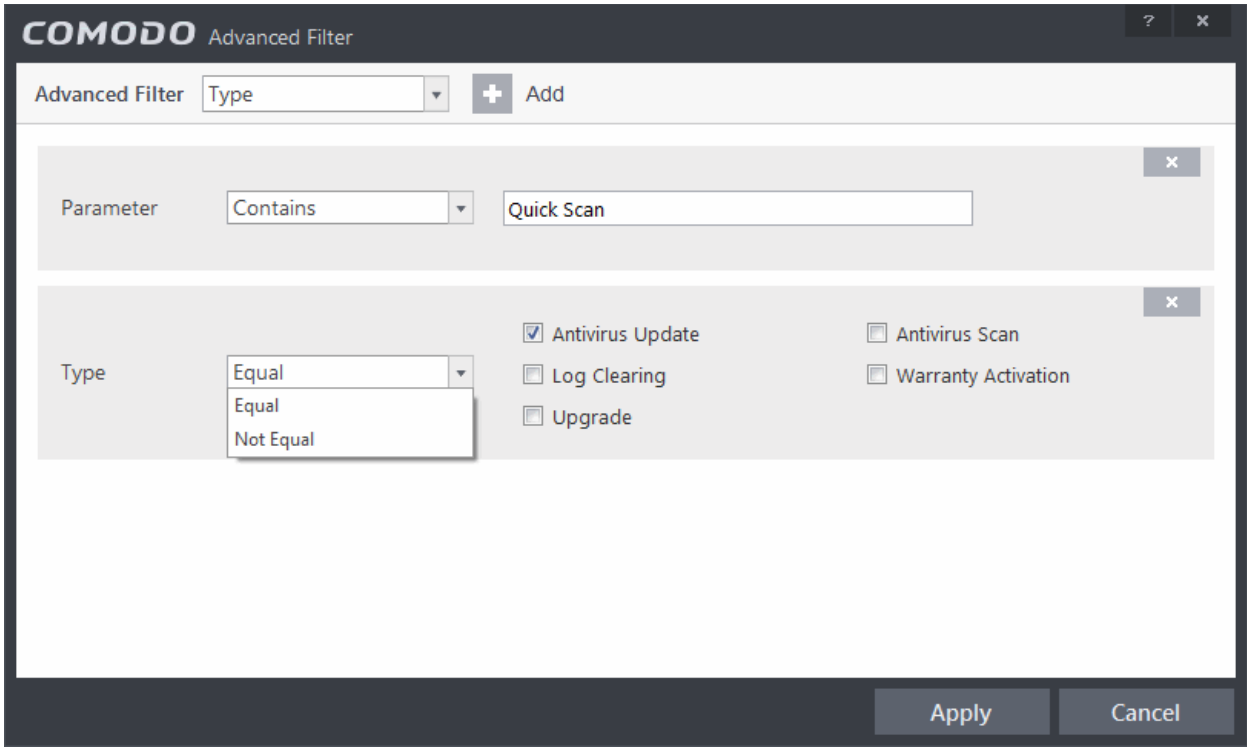


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Quick Scan' in the text field, then only the entries of Antivirus Scan Tasks with the scan parameter 'Quick Scan' will be displayed.

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



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

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

- Antivirus update
- Log Clearing
- Upgrade
- Antivirus Scan
- Warranty Activation

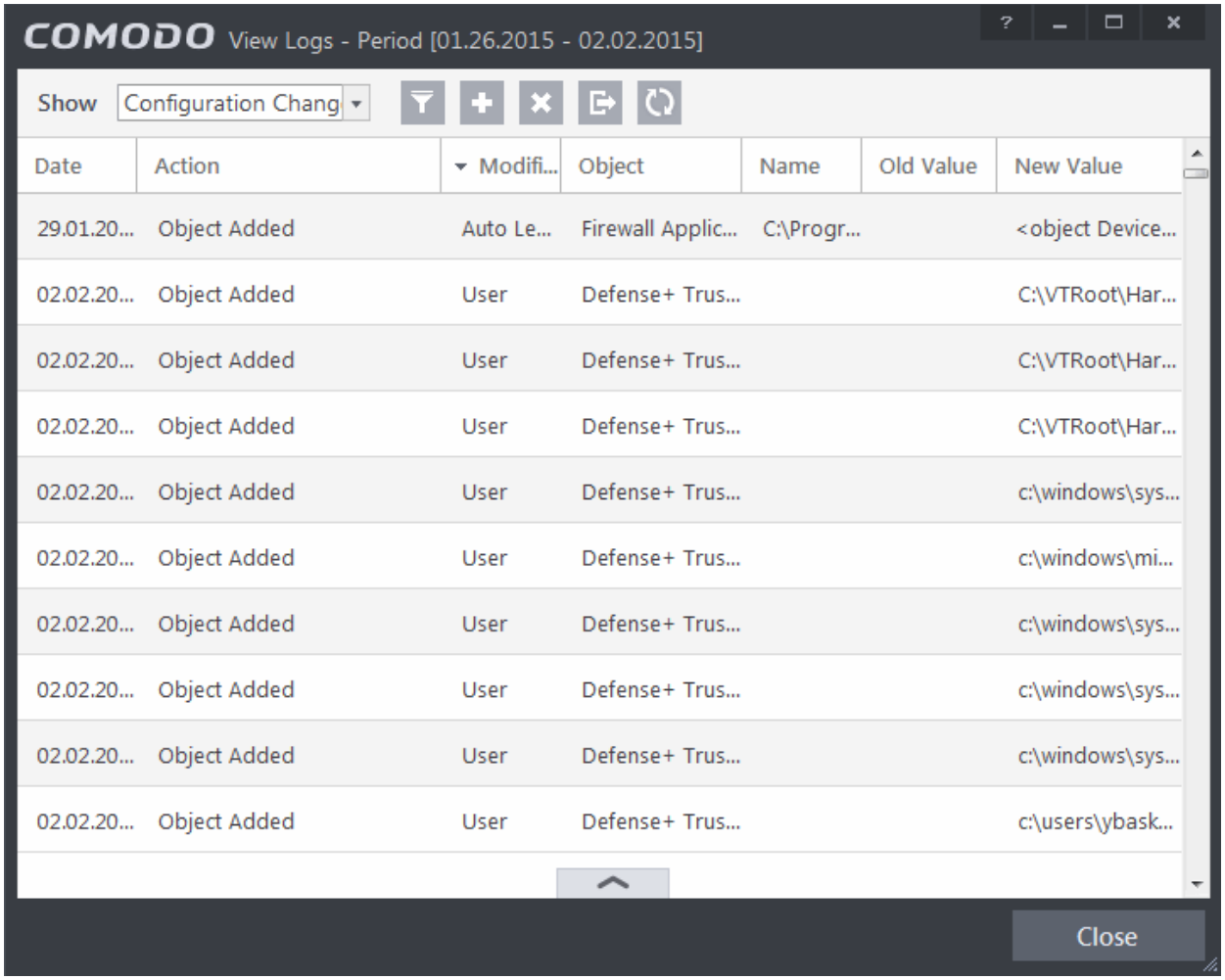
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.8. Configuration Changes

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

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



Column Descriptions

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

- To view the full details of a configuration change, place the mouse cursor on the entry in the Old Value or New Value column of the respective row.

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

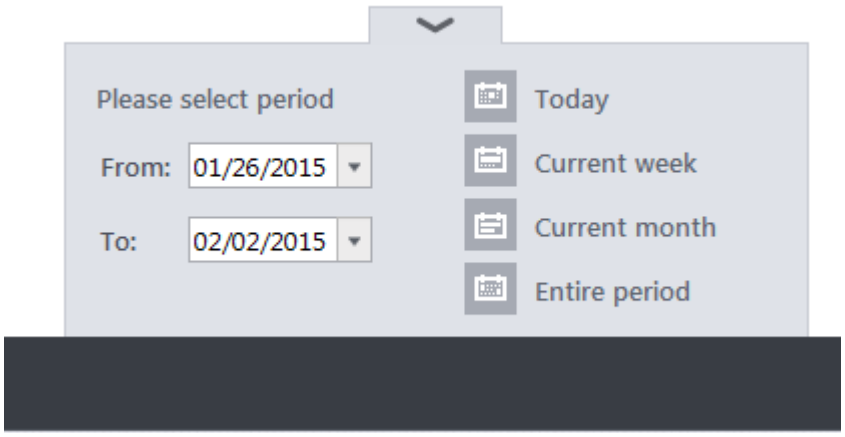
2.6.8.1. Filtering 'Configuration Changes' Logs

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

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

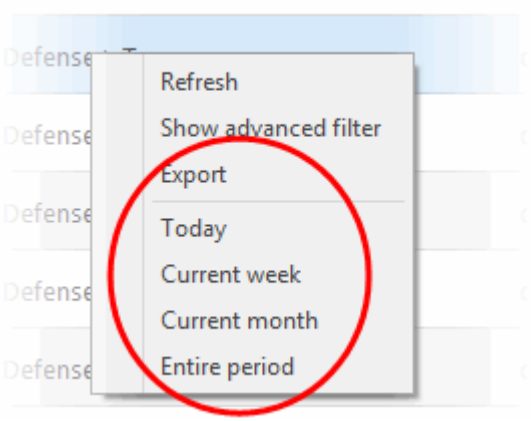
Preset Time Filters

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



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

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



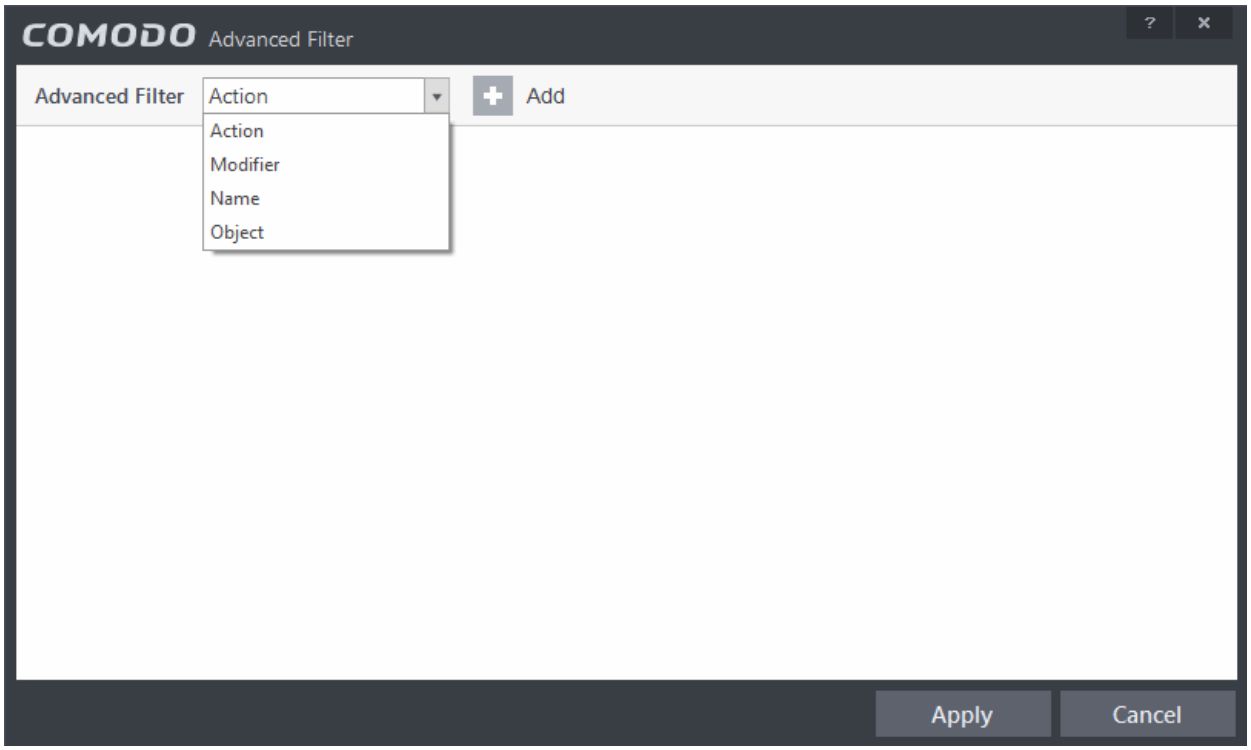
Advanced Filters

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

- **Action:** Displays only the selected type of configuration change(s) like change in options, addition of objects, strings and so on.
- **Modifier:** Displays only the configuration changes effected by the selected entity like the user, response to Antivirus, Firewall or Defense+ Alerts and so on.
- **Name:** Displays only the configuration change with the name entered as search criteria.
- **Object:** Displays only the configuration changes on addition or removal of selected objects

To configure Advanced Filters for Configuration Changes Logs

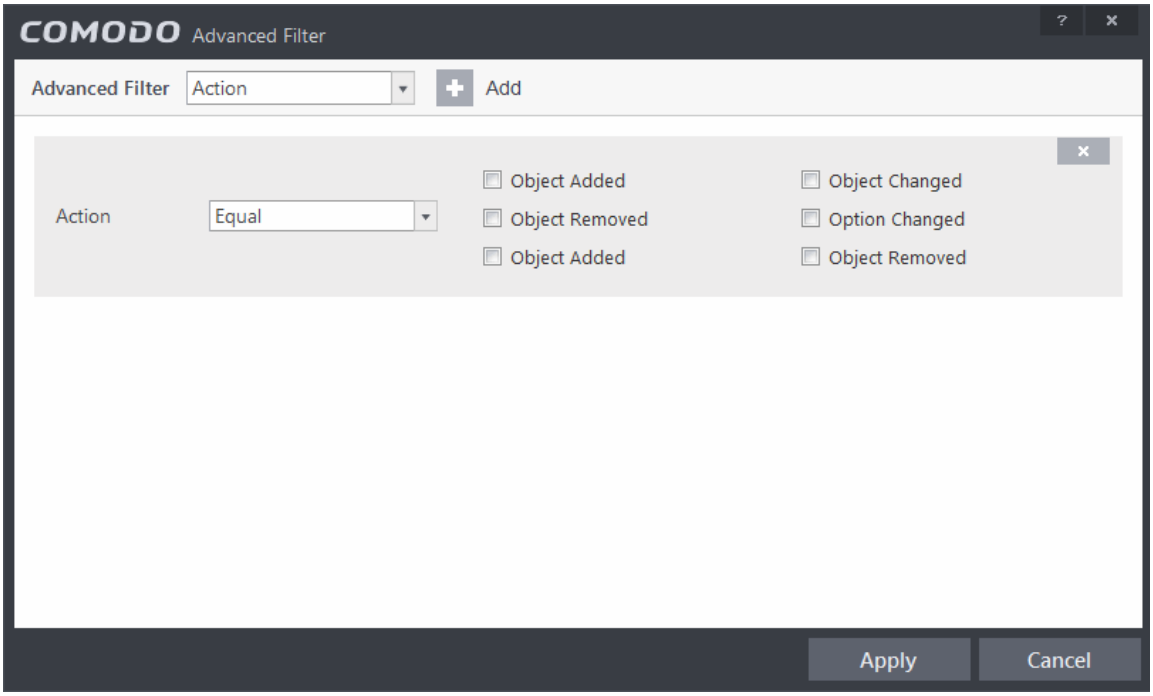
1. Click the funnel button from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Configuration Changes' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add'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



You can chose the category of filter from the 'Advanced Filter' drop-down. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. Following are the

options available in the 'Add' drop down menu:

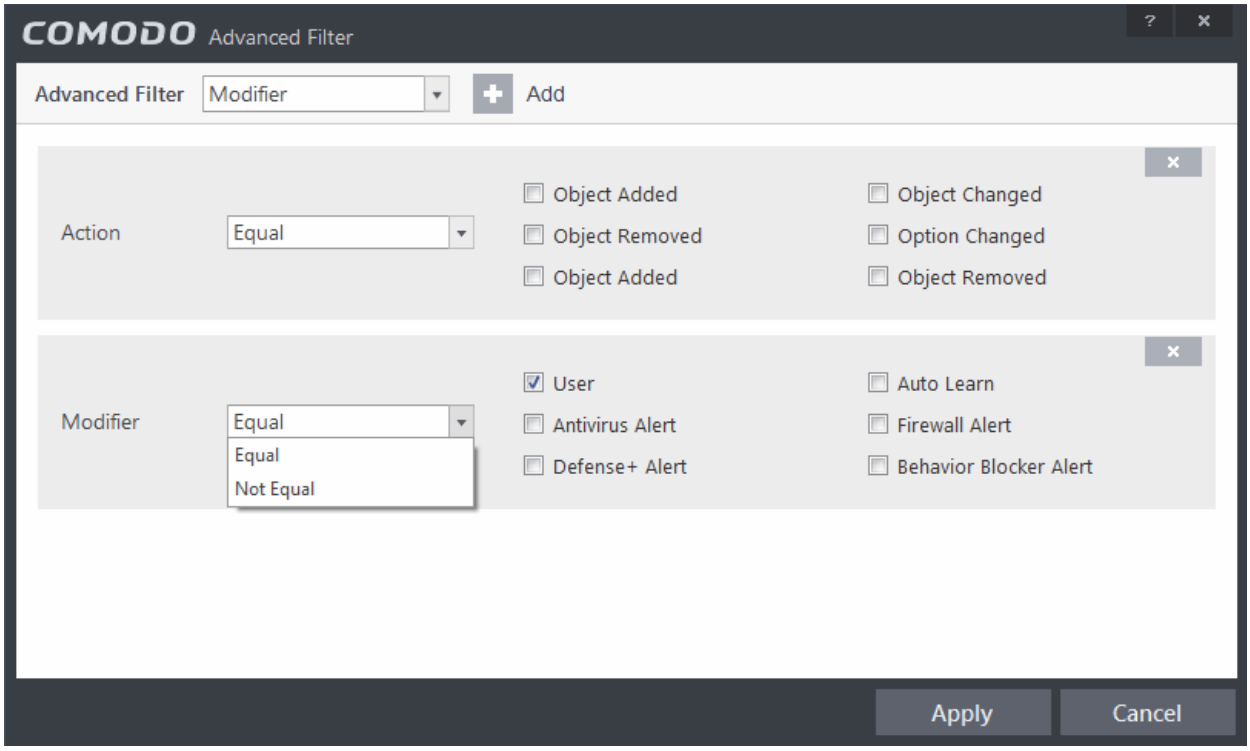
i. **Action**: The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



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

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

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



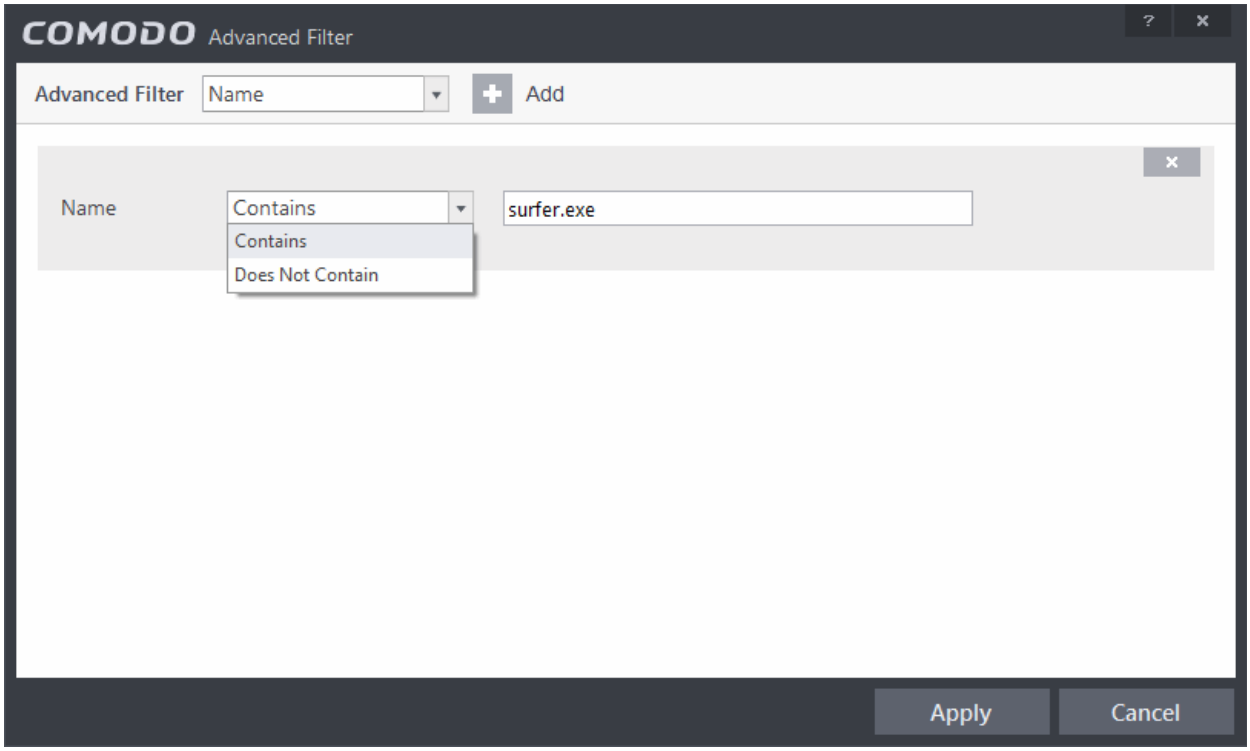
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

- User
- Auto Learn
- Antivirus Alert
- Firewall Alert
- Defense+ Alert
- Behavior Blocker Alert

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

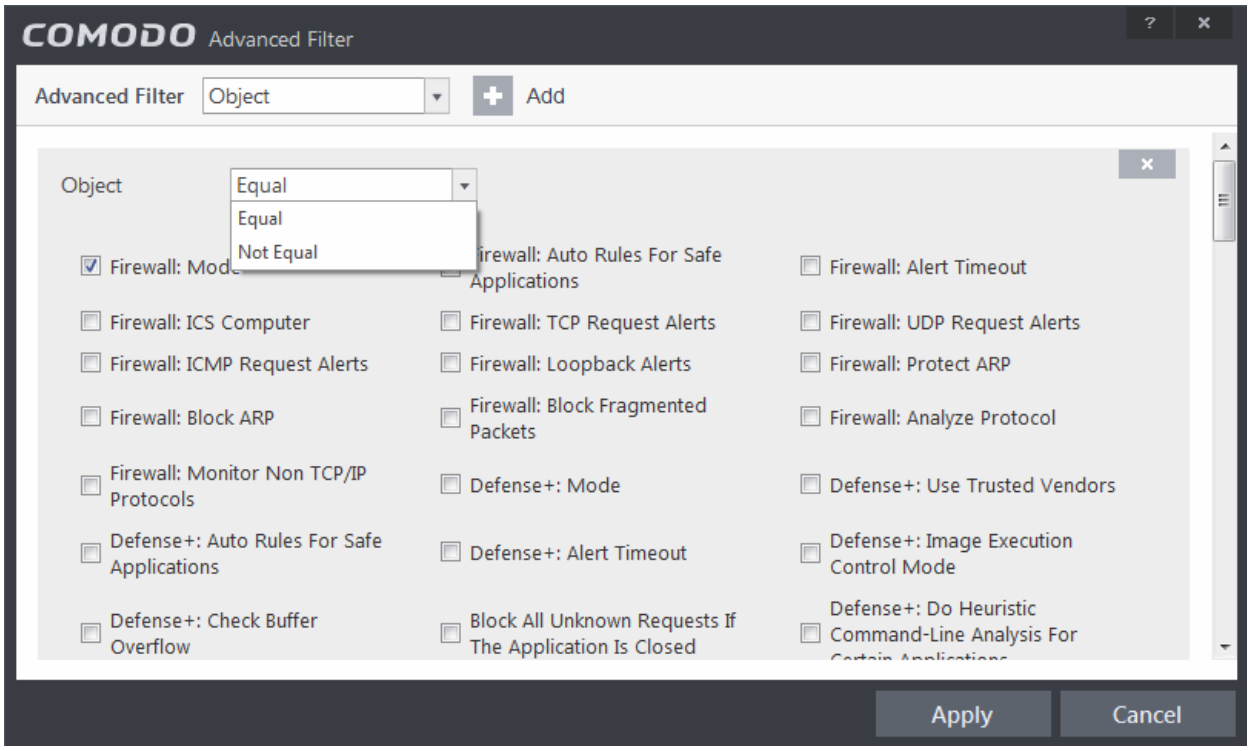
iii. **Name**: The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
b) Enter the name of the change, partly or fully as filter criteria in the text box.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'surfer.exe' in the text field, then only the log entries containing the surfer.exe in the name column will be displayed.

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



a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
b) Now select the check-boxes of the specific objects as filter parameters to refine your search. Scroll down the

window to see all the parameters options.

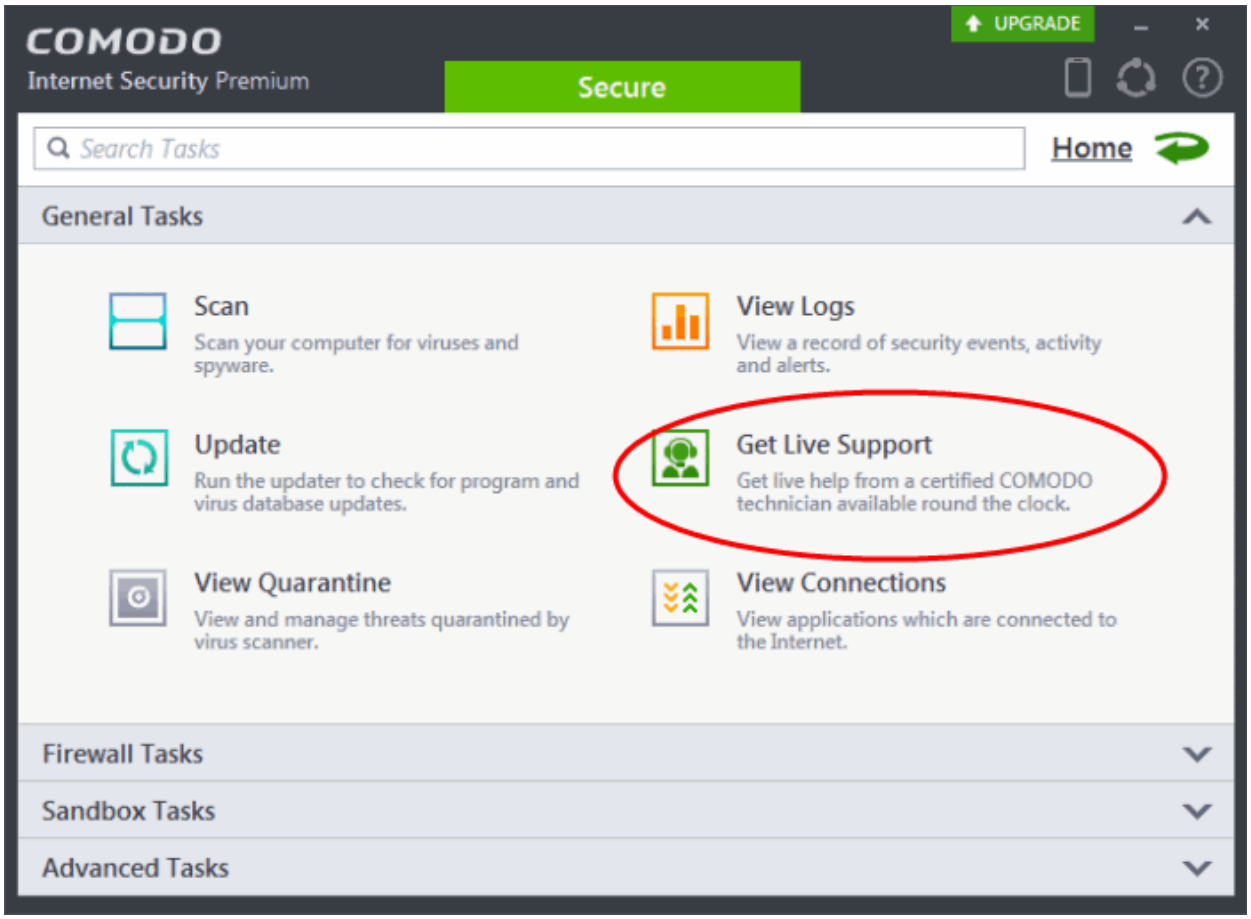
For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode ' checkbox, only the log entries related to the change of Firewall mode will be displayed.

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

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

2.7. Get Live Support

Opens the GeekBuddy instant-chat client and connects you to a Comodo support technician.



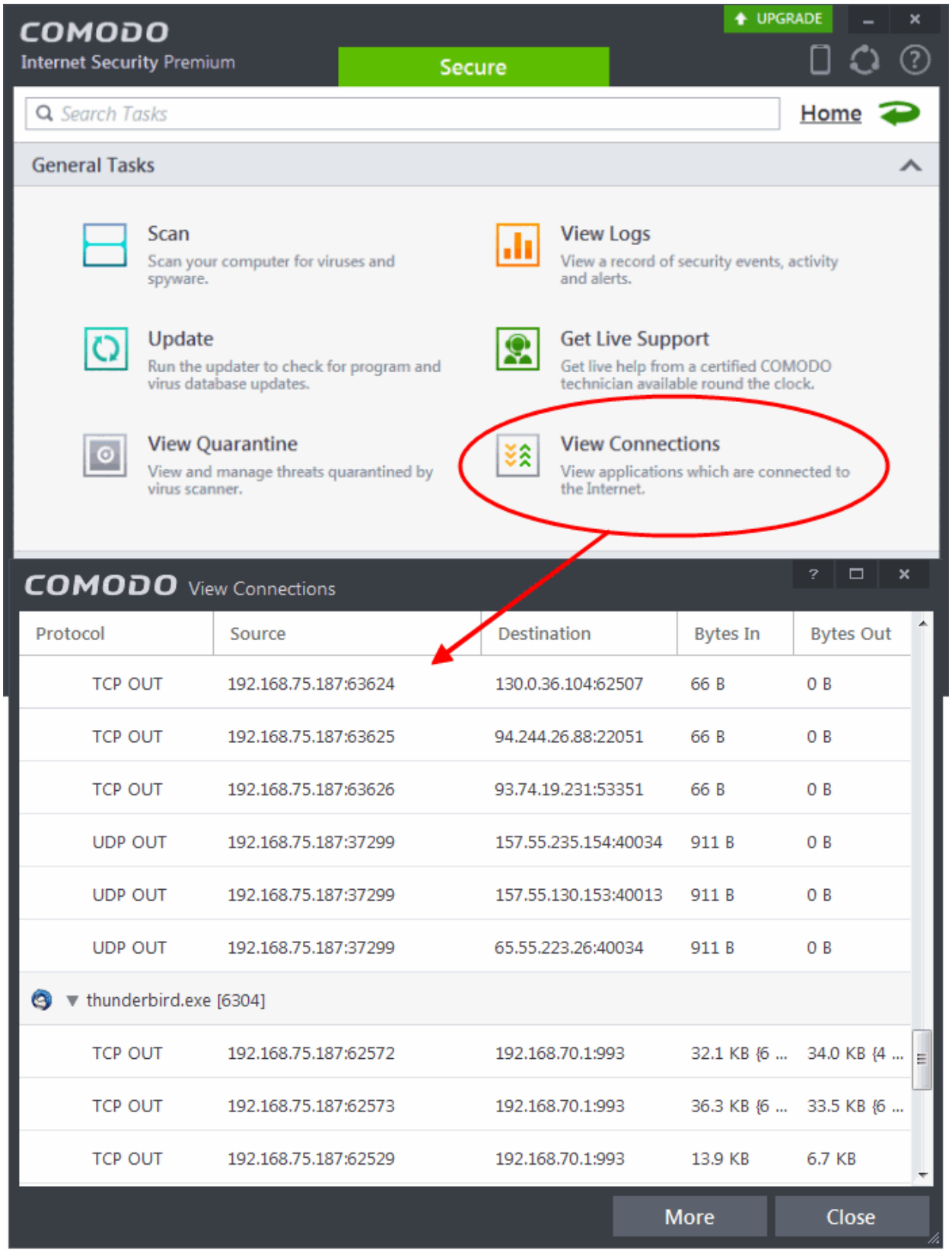
GeekBuddy technicians can help solve most computer issues that you are experiencing. Do you need help to get rid of a particularly nasty virus? Has your computer slowed down to a crawl for no apparent reason? Are you having trouble setting up that wireless router you just bought? GeekBuddy techs can offer you expert guidance and, with your permission, can even remote-desktop into your computer and fix your problems while you sit back and watch. For more details about this service, please refer to **Comodo GeekBuddy**.

2.8. View Active Internet Connections

The 'View Connections' interface displays an at-a-glance summary of all currently active Internet connections on a per-application basis. You can view all the applications that are connected; all the individual connections that each application is responsible for; the direction of the traffic; the source IP and port and the destination IP and port. You can also see the total amount of traffic that has passed in and out of your system over each connection.

This list is updated in real time whenever an application creates a new connection or drops an existing connection. The 'View Connections' is an extremely useful aid when testing firewall configuration; troubleshooting new firewall policies and rules; monitoring the connection activity of individual applications and your system as a whole and for terminating any unwanted connections.

The 'View active Connections' interface can be accessed by clicking 'View Connections' from the 'General Tasks' interface. Alternatively, this screen can be accessed by clicking the number above Inbound or Outbound in the Advanced View of the Home screen in the Firewall pane.



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

Column Descriptions

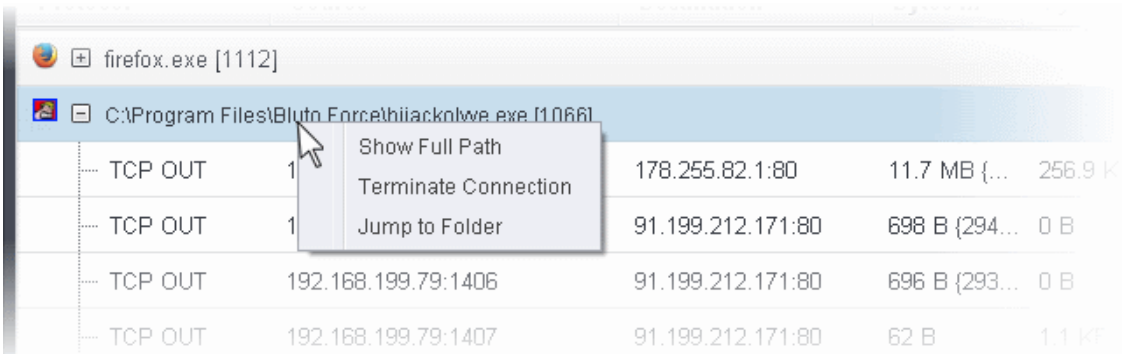
- **Protocol** - Shows the application that is making the connection, the protocol it is using and the direction of the traffic. Each application may have more than one connection at any time. Clicking + at the left of the application name expands the list of connections made by it.
- **Source (IP : Port)** - The source IP Address and source port that the application is connecting through. If the

application is waiting for communication and the port is open, it is described as 'Listening'.

- **Destination (IP : Port)** - The destination IP Address and destination port address that the application is connecting to. This is blank if the 'Source' column is 'Listening'.
- **Bytes In** - Represents the total bytes of incoming data since this connection was first allowed.
- **Bytes Out** - Represents the total bytes of outgoing data since this connection was first allowed.

Context Sensitive Menu

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



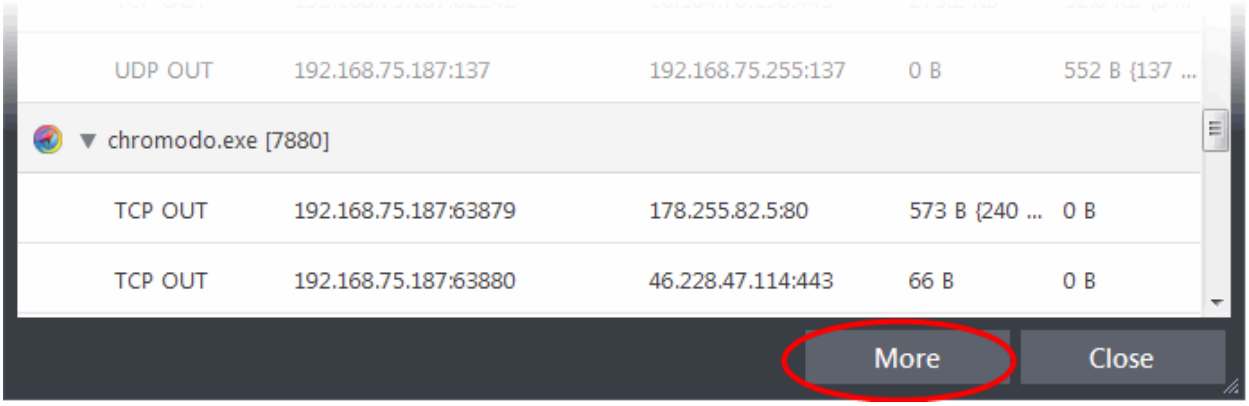
- If you wish to view the full path of the application, right click on the application name and select 'Show Full Path'.
- If you wish to terminate a connection belonging to an application, right click on the specific connection and click 'Terminate Connection'.
- If you wish to open the folder containing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

Identify and Kill Unsafe Network Connections

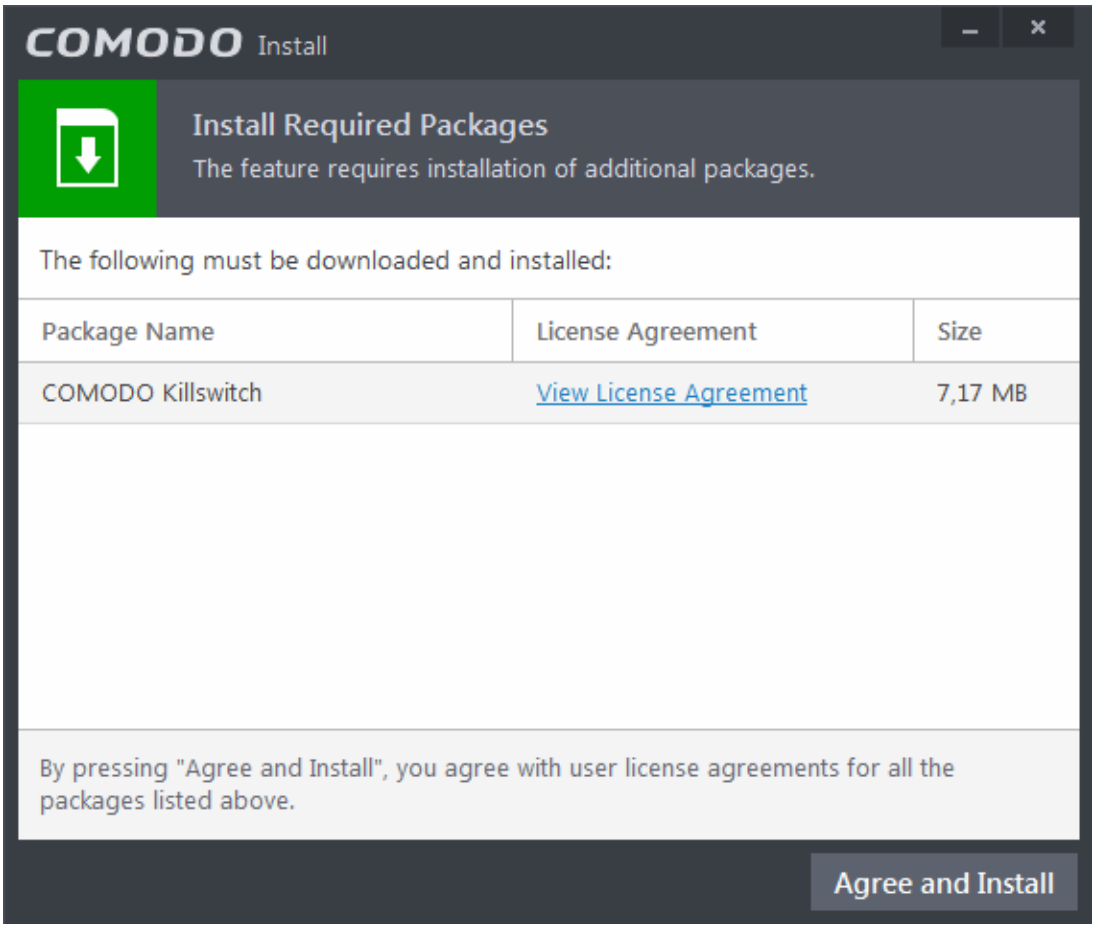
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides 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.

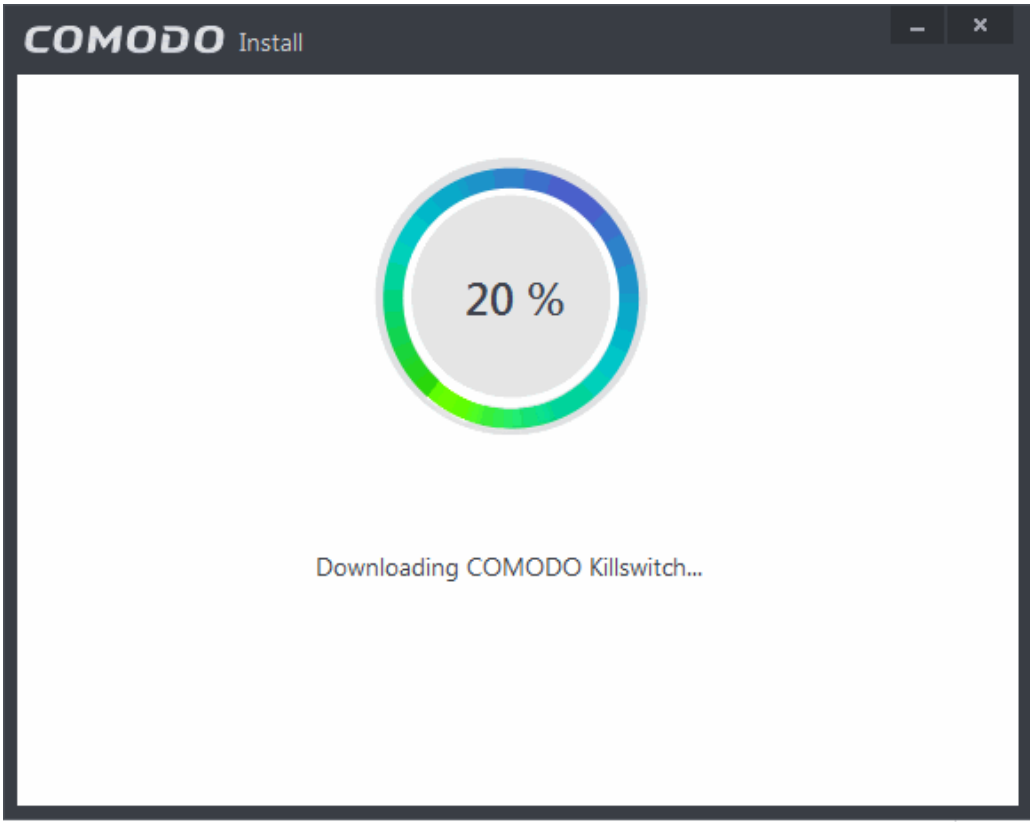
Comodo KillSwitch can be directly accessed from the 'View Connections' by clicking the 'More' button.



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

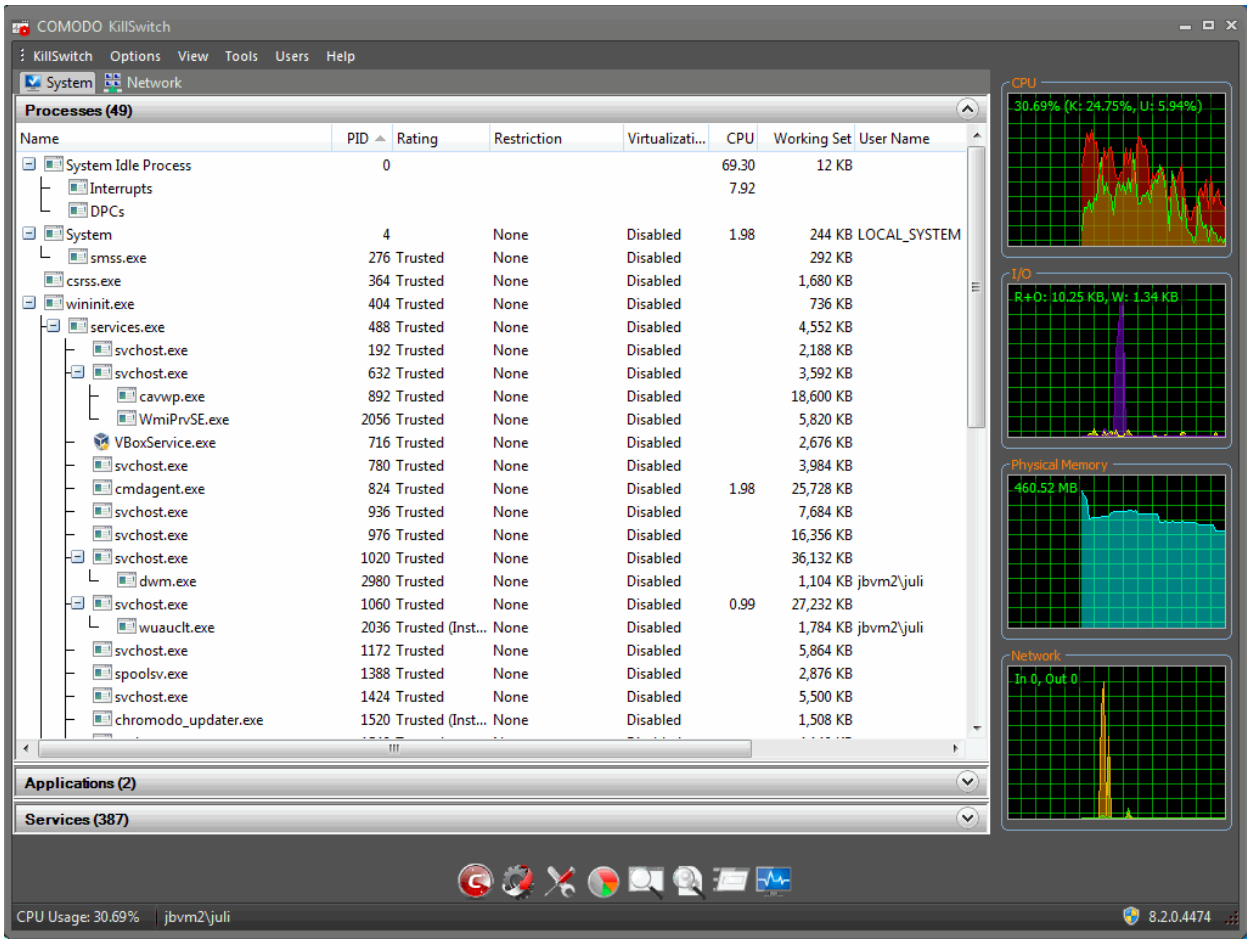


- Read the license agreement by clicking 'View License Agreement' and click 'Agree and Install'. CIS will download and install the application.



On completion of installation, the Comodo KillSwitch main interface will be opened. Clicking the Network tab will display the

Network Connections and Network Utilization panes.



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

2.9. View Active Process List

The Active Process List interface displays all currently active processes initiated by applications that are currently running in the sandbox environment . By tracing an application's parent process, CIS can detect whether a non-trusted application is attempting to spawn an already trusted application and thus deny access rights for that trusted application. This system provides the very highest protection against Trojans, malware and rootkits that try to use trusted software to launch an attack. By default, the list displays the processes of sandboxed applications only, but can be made to display all the processes from the right-click options.

The processes of sandboxed applications include:

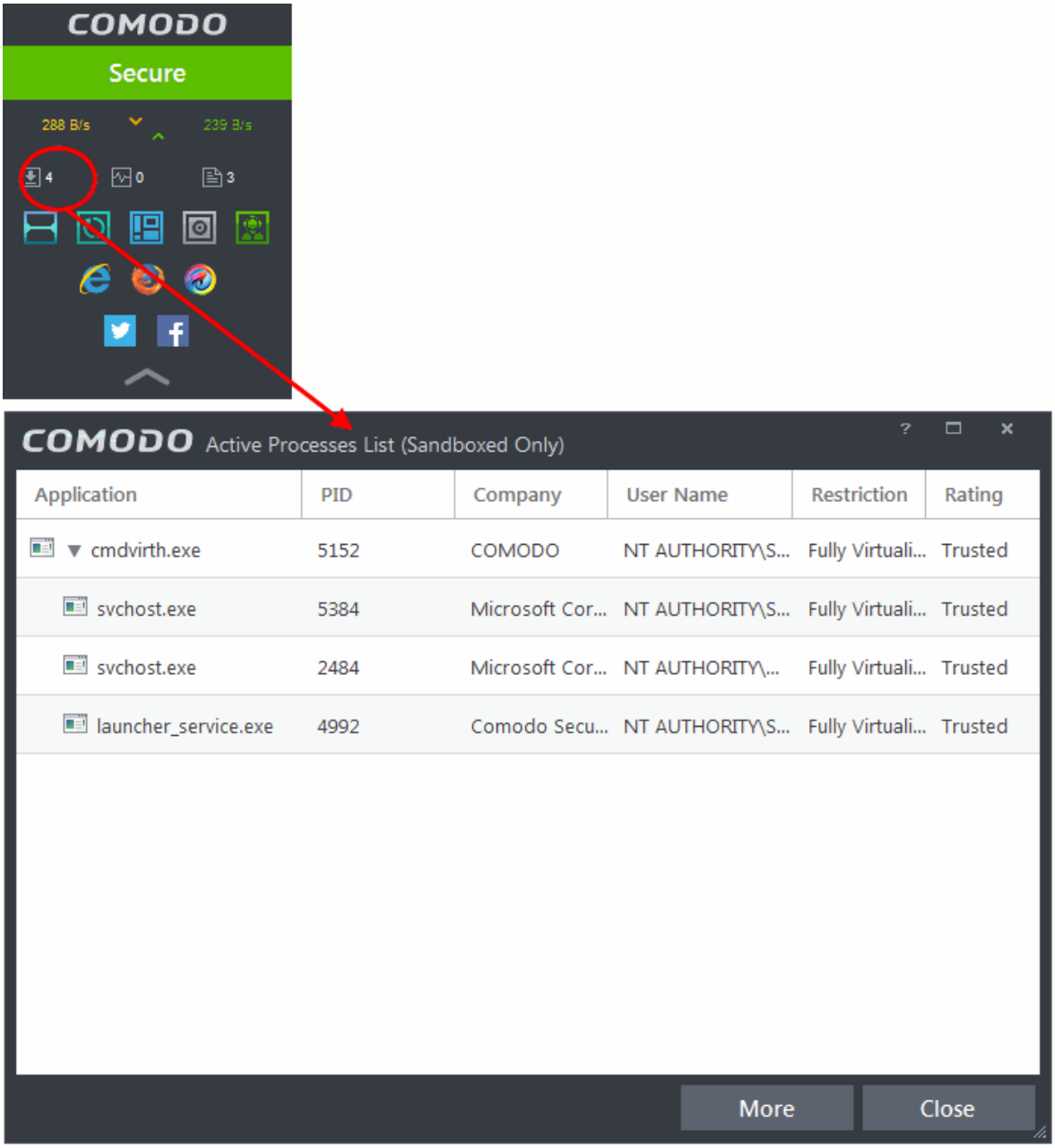
- Auto-Sandbox - Applications that are run inside the sandbox as per the rules defined for them or by default sandbox rules. Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details on defining auto-sandbox rules.
- Run Virtual - Applications that are selected and run in Sandbox. Refer to '**Run an Application in the Sandbox**' for more details.
- Applications that are run inside the sandbox using the context sensitive menu - **Click here** for more details.
- Running browsers inside the sandbox from the Widget - **Click here** for more details.
- Drag-and-drop applications on to CIS Home Screen - **Click here** for more details.

- Programs that are added manually - Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details.

To view Active Process list

- Click the first box in the status pane (third row) in the CIS Widget.

Note: The Status Pane is not displayed by default in the widget. To enable the Status Pane, right click on the CIS tray icon and select 'Show Status Pane' from the options.



- Alternatively, the screen can be accessed by clicking the number beside 'Sandboxed Apps' in the Advanced View of the Home screen in the Defense+ and Sandbox pane.

The Active Processes List (Sandboxed Only) screen will be displayed by default.

Column Descriptions

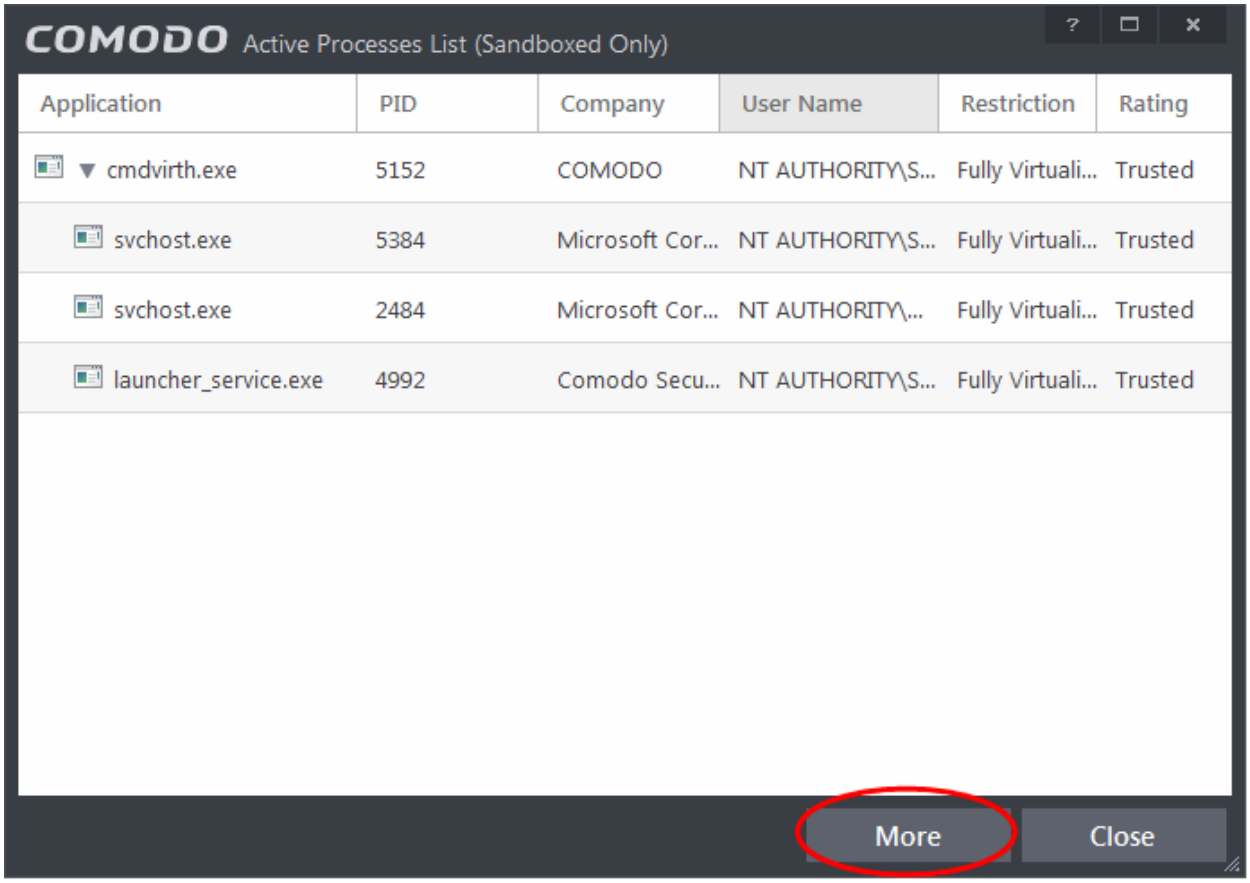
- Application - Displays the names of applications that are currently running.
- PID - Process Identification Number.

- Company - Displays the name of the software developer.
- User Name - The name of the user that started the process.
- Restriction - Displays the level of sandbox setting selected for the program.
- Rating - Displays the rating of the application whether trusted or unknown.

Right-click on any process to:

- Show full path: Displays the location of the the executable in addition to it's name.
- Show Sandboxed Only: Displays the details of the sandboxed programs only. Disable this option to view all the current active process list.
- Add to Trusted Files: The selected unknown program is added to **Trusted Files list**.
- Online Lookup: The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: The folder containing the executable file of the application will open.
- Show Activities: Opens the **Process Activities List dialog**. The Process Activities dialog will display the list activities of the processes run by the application. The 'Show Activities' option is available only if **Viruscope** is enabled under **Advanced Settings > Defense+ > Viruscope**.

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



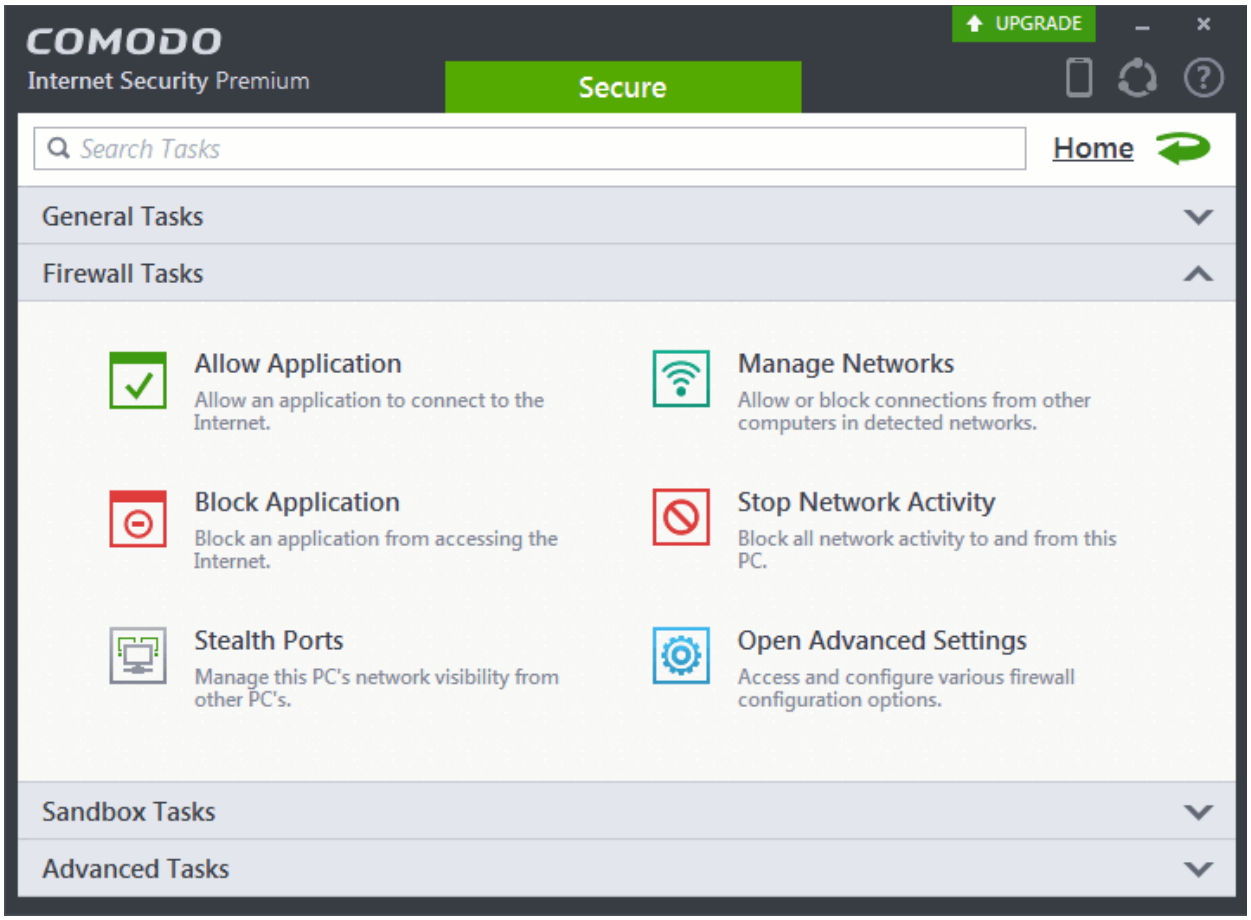
If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the section **Identify and Kill Unsafe Processes** for more details.

3. Firewall Tasks - Introduction

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

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

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



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

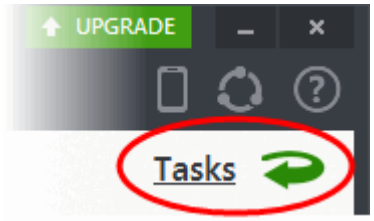
- **Allow or block Internet access to applications selectively**
- **Stealth your computer ports**
- **Manage network connections**
- **Stop all network activity**
- **Advanced firewall settings**

3.1. Allow or Block Internet Access to Applications Selectively

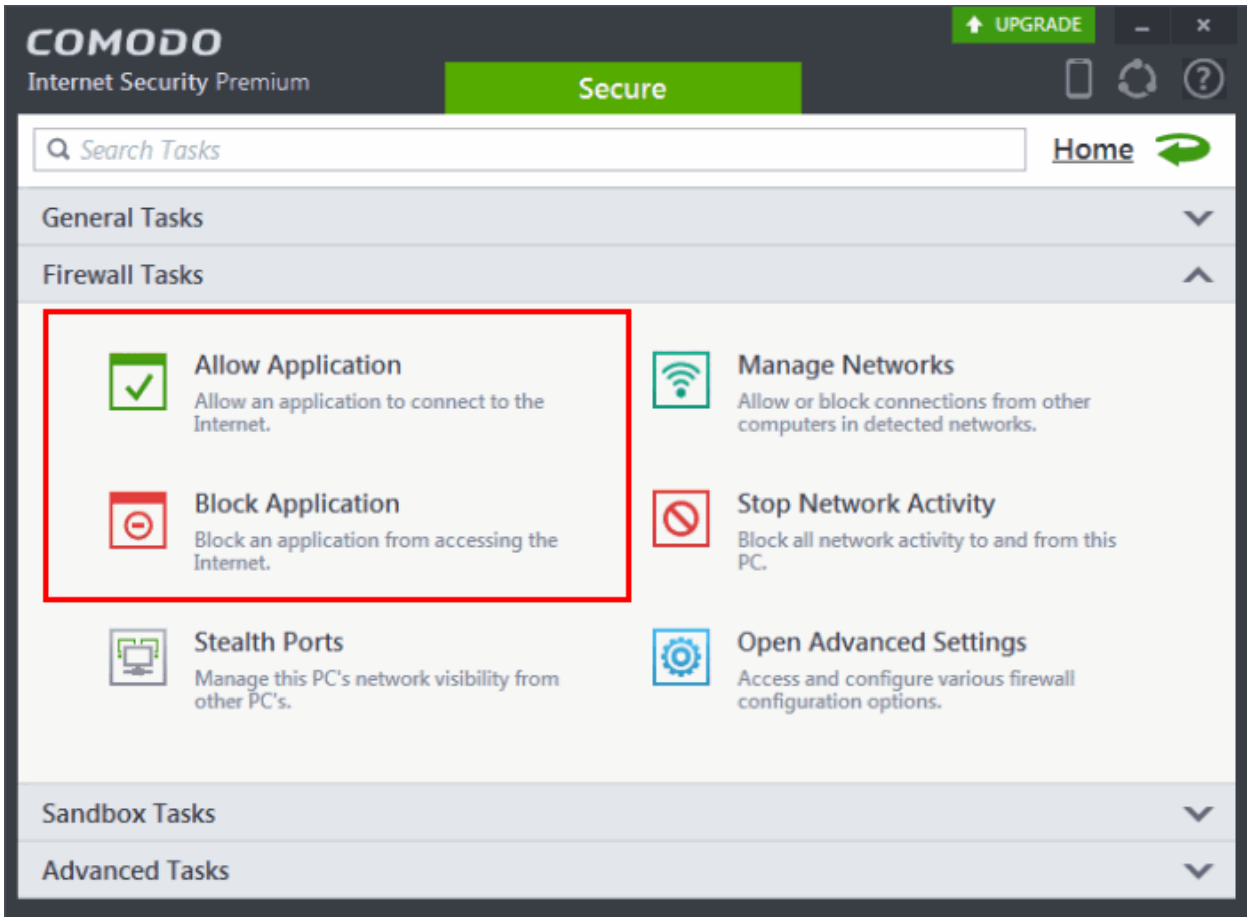
The Firewall Tasks interface allows you to selectively allow or block certain applications from accessing the Internet. These shortcuts represent a convenient way to create an automatic 'Allow Requests' rule or 'Block Requests' rule for individual applications - meaning that inbound and outbound connections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

To open the 'Firewall Tasks' interface:

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



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



To allow an application to access to the Internet:

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

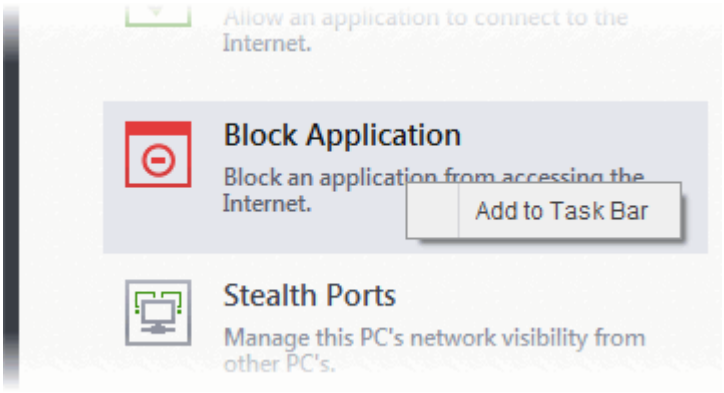
To block an application's Internet access rights

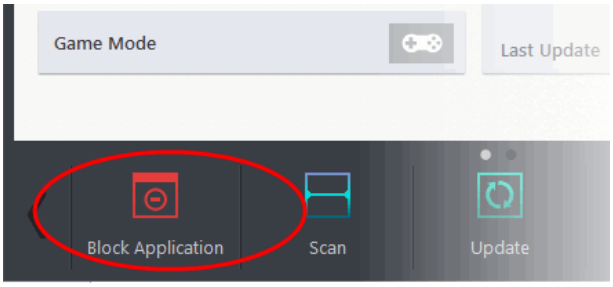
- Click the 'Block Application' button from the 'Firewall Tasks' interface.
- Browse to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to prohibit Internet access to the selected application.

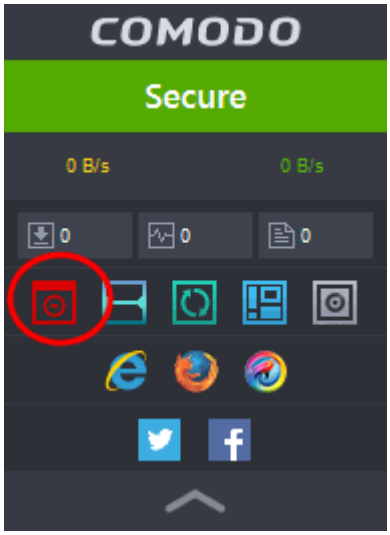
The advanced application rules interface can be accessed by clicking 'Tasks' from the CIS home screen > Firewall Tasks > Open Advanced Settings > Application rules. The application you just allowed or blocked should be listed here. For further information on application rules governing Internet access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

Tip: if you plan to regularly allow/block applications, you can right click on the appropriate button and select 'Add to Taskbar'. It

will then be quickly accessible from both the CIS home screen and the widget:







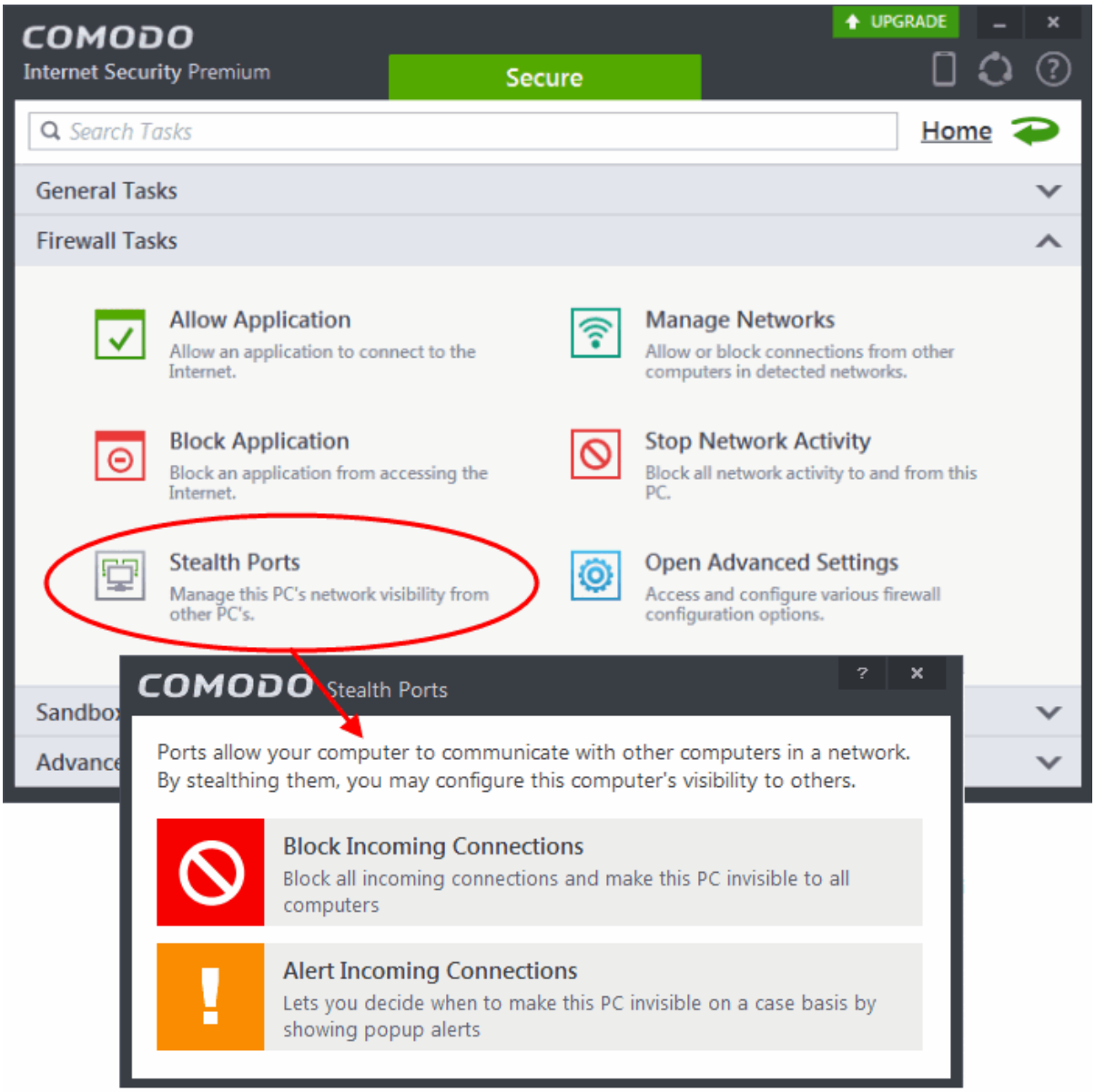
3.2. Stealth your Computer Ports

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

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

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

- Click on 'Stealth Ports' link in Firewall Tasks

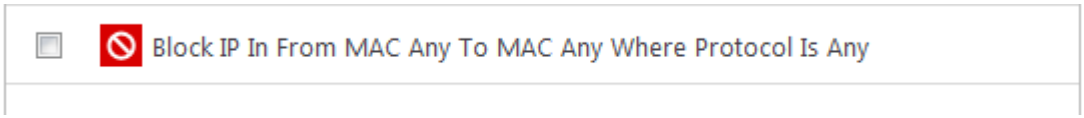


You have two options to choose from:

Block incoming connections

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

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



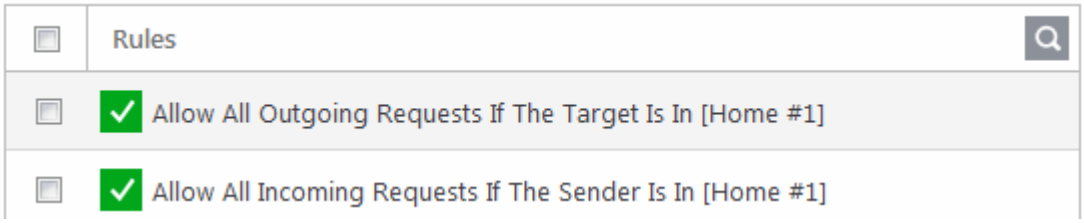
If you would like more information on the meaning and construction of rules, please **click here.**

Alert incoming connections

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

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

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

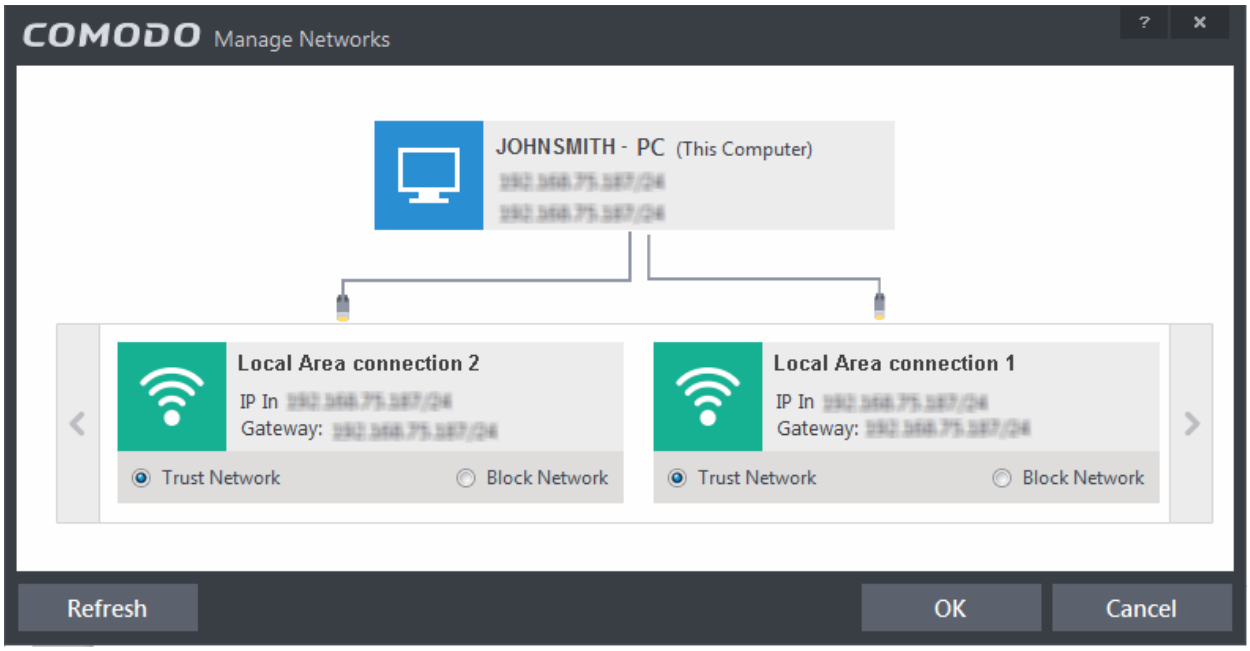


If you would like more information on the meaning and construction of rules, please **click here**.

3.3. Manage Network Connections

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

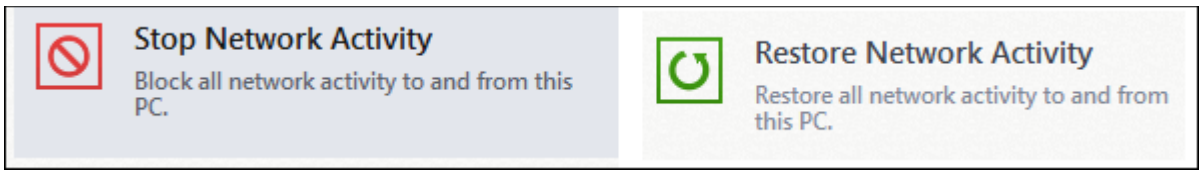
- You can choose to trust or block a network by selecting the appropriate radio button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks.
- Use the handles (< >) to scroll through all available networks or computers
- Use the refresh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



- The 'Manage 'Networks' interface can be opened by clicking 'Tasks > Firewall Tasks > Manage Networks'.
- To view, create or block **Network Zones**, click 'Tasks > Firewall Tasks > Open Advanced Settings > Network Zones'.

3.4. Stop all Network Activities

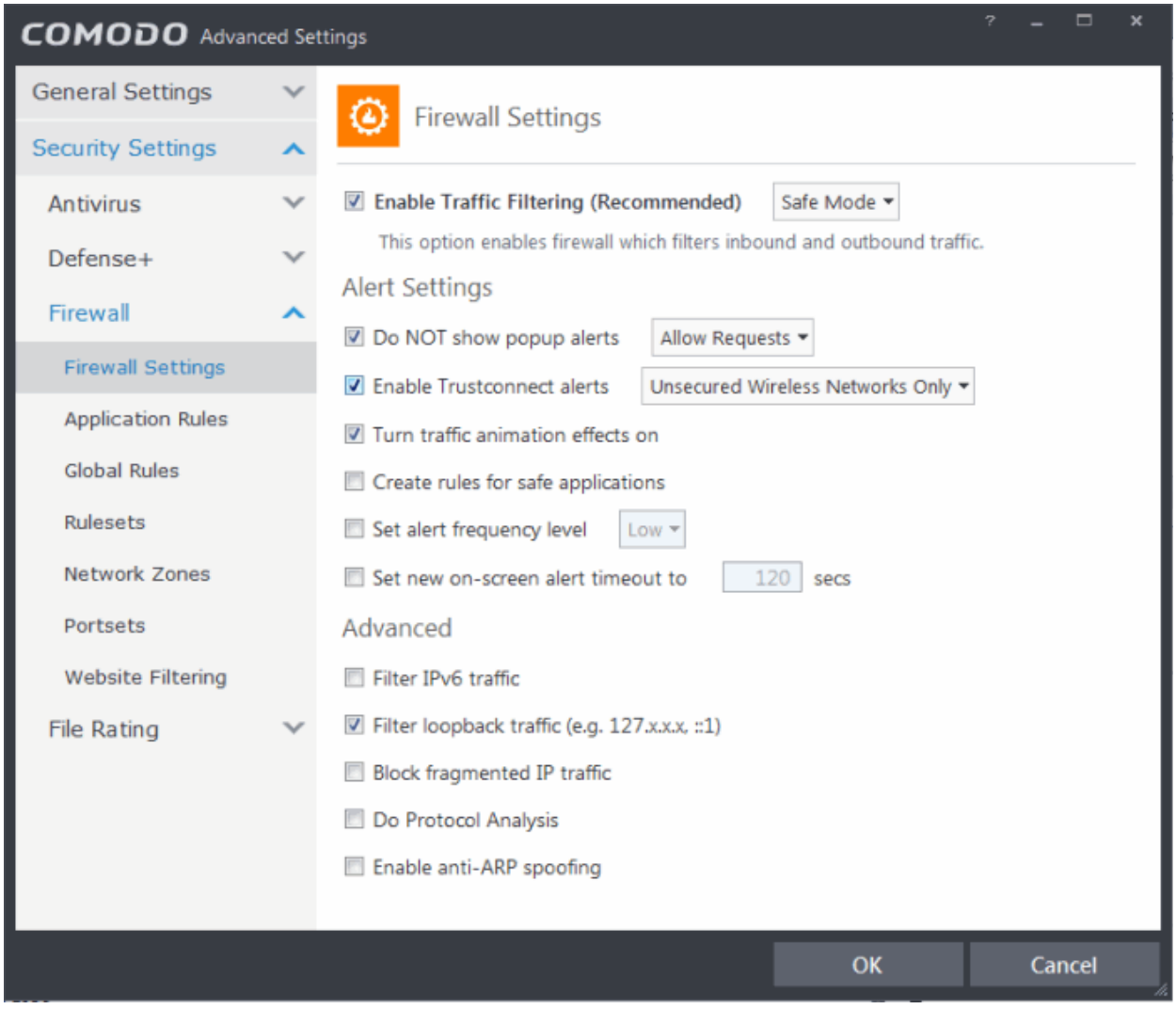
As the name suggests, the 'Stop Network Activity' button instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and all available networks (including the Internet). Connections will remained closed until you re-enable them by clicking the button a second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



- Access the network activity 'on/off' button by clicking Tasks > Firewall Tasks
- Disconnect your computer from all networks by clicking 'Stop Network Activity' (button will be red)
- Re-enable connectivity by clicking 'Restore Network Activity' (button will be green)
- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have previously blocked in '**Manage Network Connections**' or '**Network Zones**' will remain blocked.
- You can assign networks into network zones in the '**Network Zones**' area
- You can configure rules per network zone in the '**Global Rules**' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the '**Manage Network Connections**' area

3.5. Advanced Firewall Settings

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



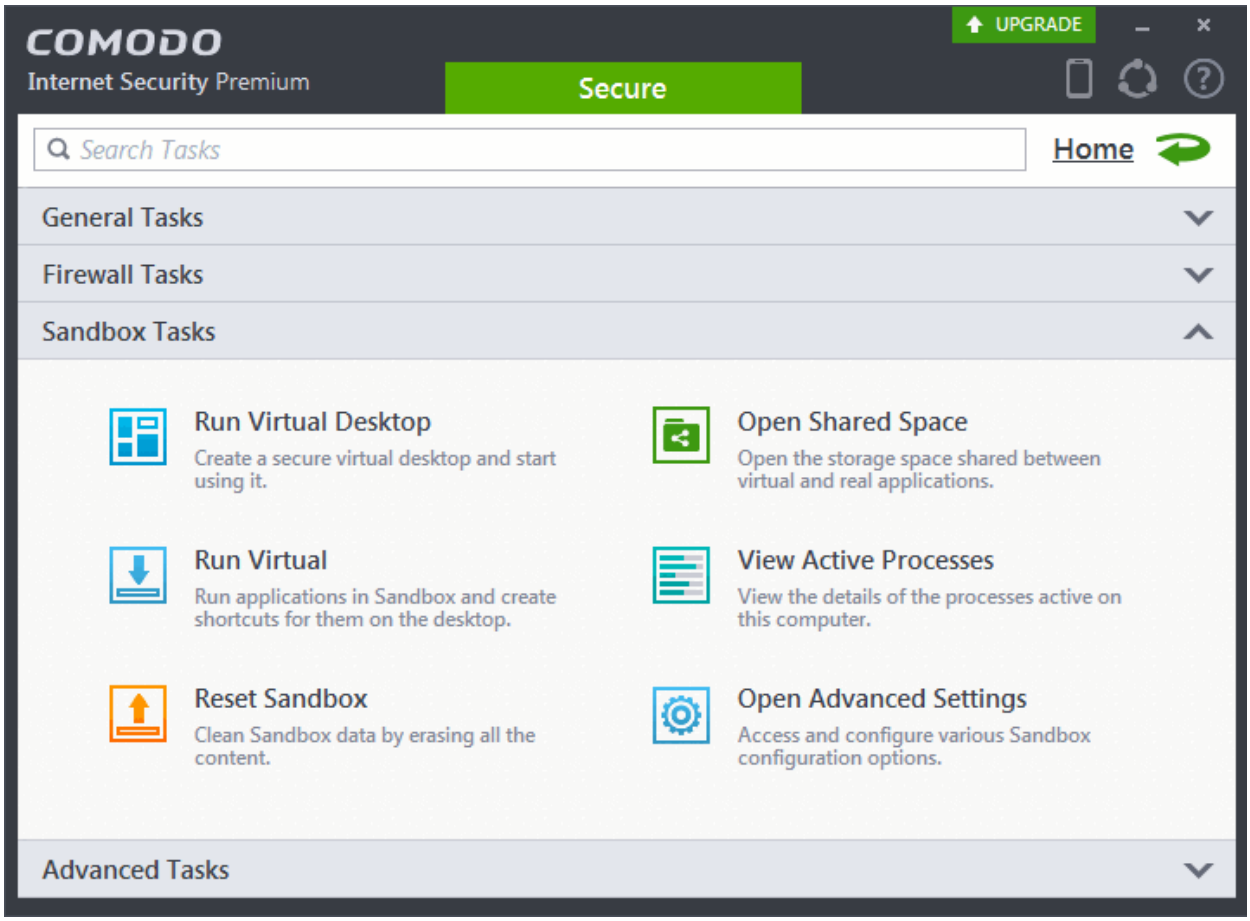
The interface is divided into seven main sections - **Firewall Settings**, **Application Rules**, **Global Rules**, **Rulesets**, **Network**

Zones, **Portsets** and **Website Filtering**. Click the links below to jump to more details on each section:

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

4.Sandbox Tasks - Introduction

Comodo Internet Security features a fully functional sandbox called the '**Virtual Desktop**'- an isolated operating environment for running unknown, untrusted and suspicious applications. Applications executed inside the sandbox/virtual Desktop will not affect other processes, programs or data on your real computer. In addition to running suspicious applications inside the sandbox on an ad-hoc basis, you can create a specific list of programs that should always run in the sandbox.



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

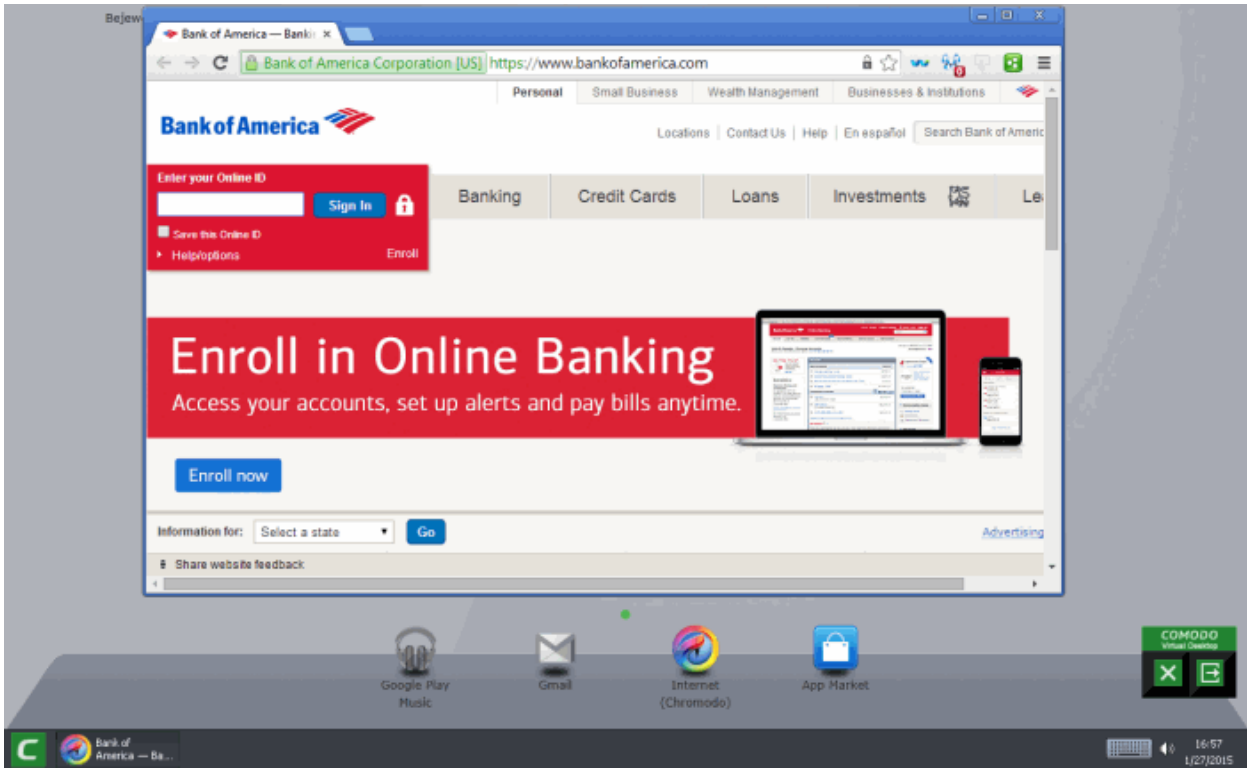
- Windows XP 64 bit
- Windows Server 2003 64 bit

The Sandbox Tasks interface has shortcuts for the following tasks:

- **Run Virtual Desktop** - Starts the Virtual Desktop
- **Open Shared Space** - Opens the folder 'Shared Space' which is shared by your host operating system and the Virtual Desktop. The folder is created by the Virtual Desktop at the location 'C:\Documents and Settings\All Users\Application Data\Shared Space'. The folder can be opened in both your host operating system and inside the Virtual Desktop, and enables to share files and applications between the OS and the Virtual Desktop.
- **Run Virtual** - Allows you to run individual applications in the sandbox
- **Reset Sandbox** - Allows you to clear all data written by programs run inside the sandbox
- **View Active Process List** - Allows you to view processes which are currently running on your PC. Clicking the 'More' button will open Comodo **KillSwitch**, or present you with the opportunity to install KillSwitch if you do not have it installed.
- **Open Advanced Settings** - Add programs that should always run inside the sandbox and access advanced sandbox settings. This is covered in the '**Configuring Rules for Auto-Sandbox**' section of 'Advanced Settings'

4.1. The Virtual Desktop

The Virtual Desktop is a sandboxed operating environment inside of which you can run programs and browse the Internet without fear that those activities will damage your real computer. Applications running in the Virtual Desktop also leave no cookies or history behind on your real system, making it a secure environment for Internet banking and online shopping. It is also ideal for visiting any risky websites/links and for testing out beta/unstable software.



Virtual Desktop at a glance:

- The Virtual Desktop can run any program that you can run in regular Windows and is particularly useful for browsing the Internet in a secure manner.
- Any changes made to files and settings in the Virtual Desktop will not affect the original versions on your host system. Changes will only be visible in the Virtual System itself.
- Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Any files you wish to keep and access from your host operating system can be saved to 'Shared Space'.
- The Virtual Desktop can be password-protected for added privacy.
- The virtual keyboard allows you to securely enter confidential passwords without fear of key-logging software.
- The Virtual Desktop UI can be used in both 'Classic' (Windows style) and 'Tablet' modes by selecting the mode from **Settings**.
- You can reset the Virtual Desktop and clear shared space at any time. We recommend that you do this regularly to maximize your privacy and security. Please note that all settings, stored data and any applications installed sandboxed will be deleted.

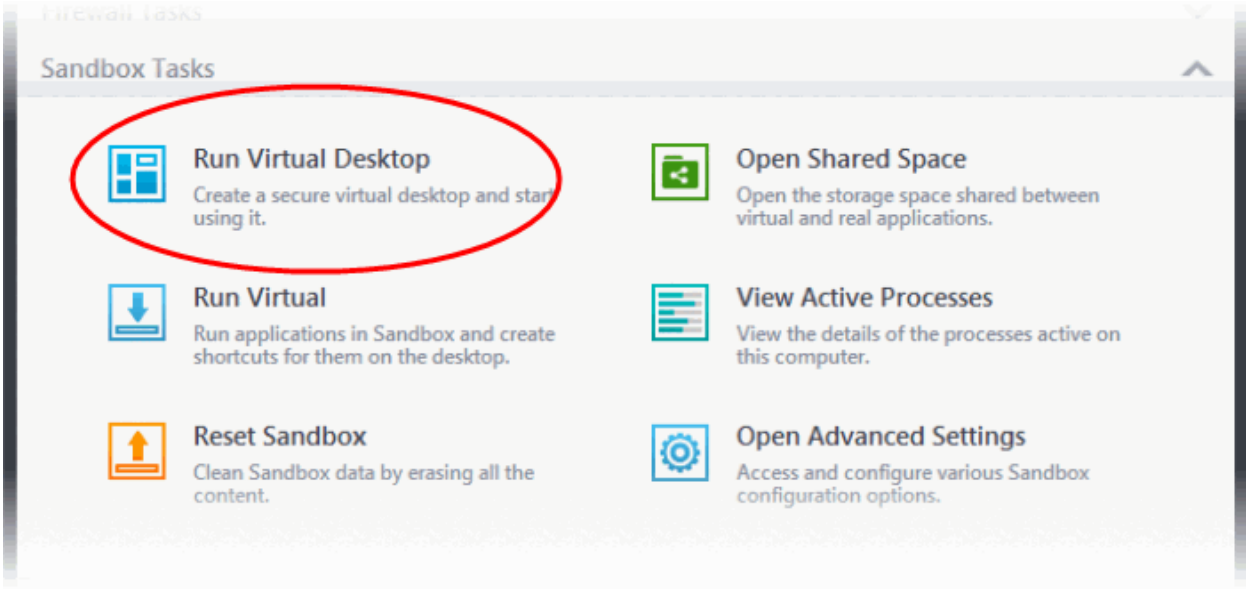
Click the following links to find out more details on:

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

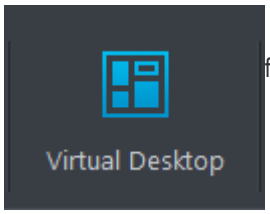
4.1.1. Starting the Virtual Desktop

The Virtual Desktop can be started by:

- Clicking Tasks > Sandbox Tasks > Run Virtual Desktop



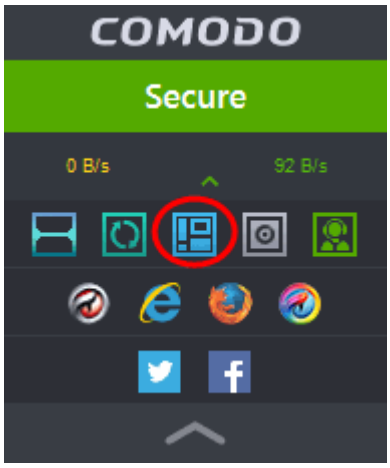
OR

- by clicking the Virtual Desktop shortcut button 

from the task bar at the bottom of Home Interface

OR

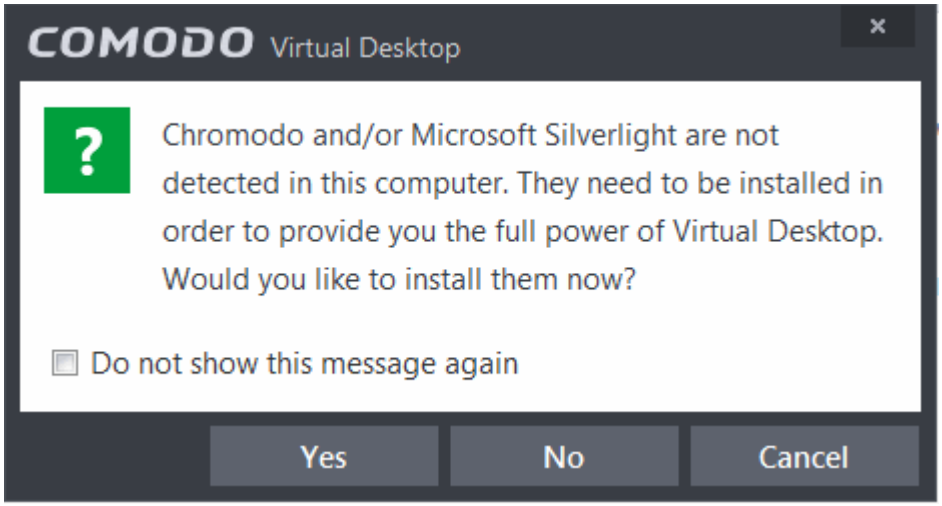
- By clicking the Virtual Desktop shortcut button from the CIS widget



The following software is needed to utilize the Virtual Desktop to its full potential:

- Chromodo Browser
- Microsoft Silverlight

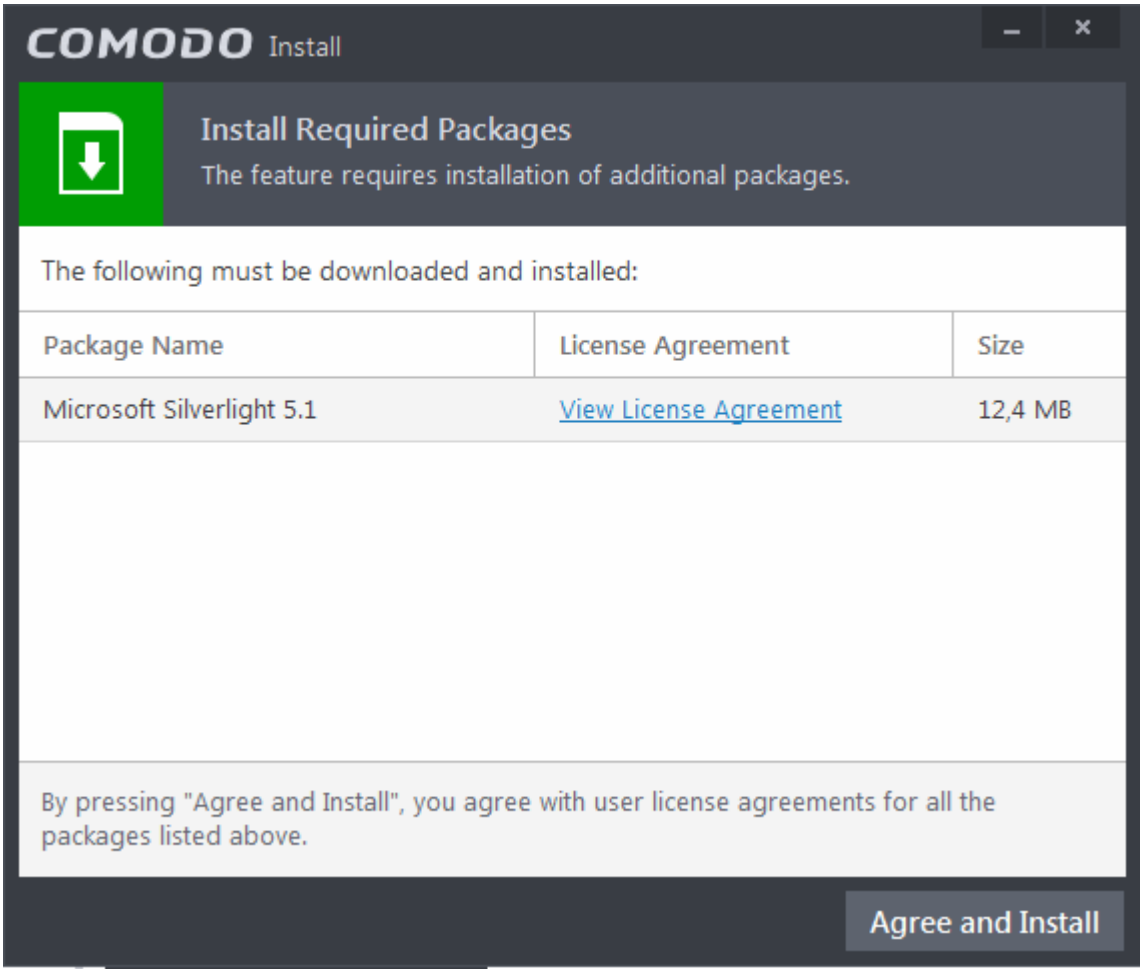
Whenever you run the Virtual Desktop, Comodo Internet Security checks whether these components are installed. If they aren't, you will be prompted to install them.



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

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

The 'Install Required Packages' dialog will be displayed.



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

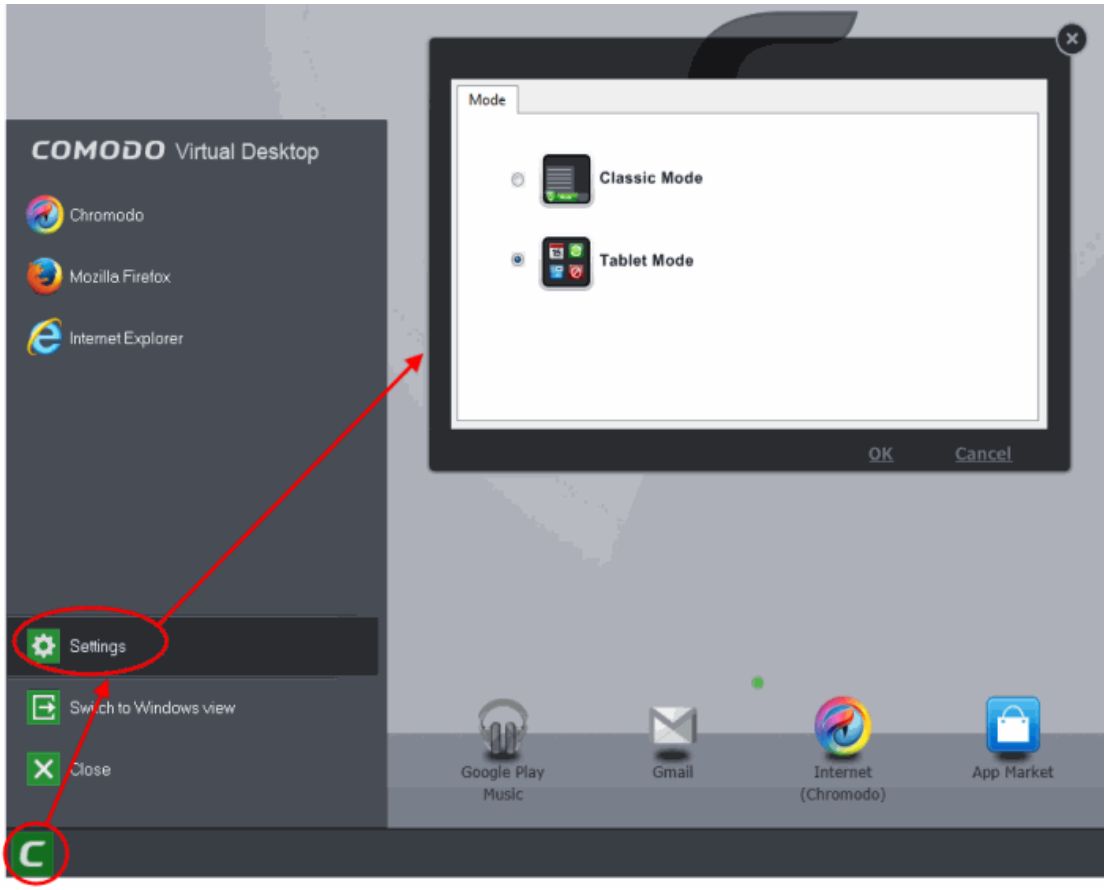
The software package(s) will be downloaded and installed automatically.

4.1.2. The Main Interface

The Virtual Desktop is presented with two switchable interfaces:

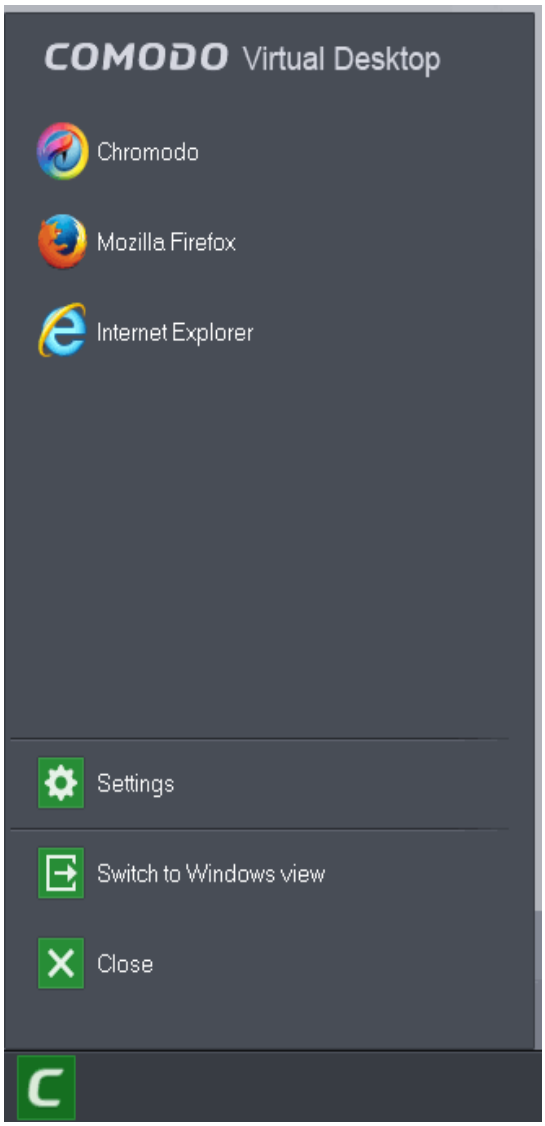
- **Classic Windows style Desktop mode**
- **Tablet mode**

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



In 'Classic' mode,

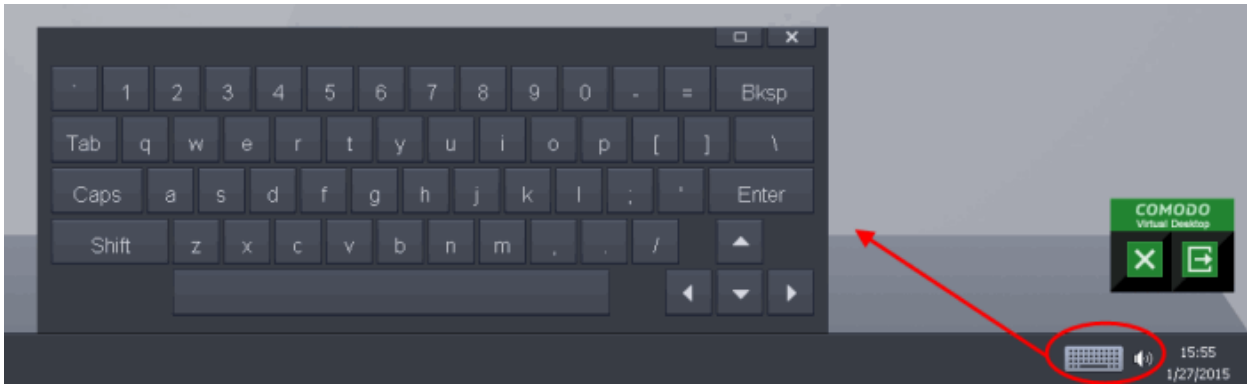
- All items on your real desktop are displayed. Clicking the shortcuts on the Virtual Desktop will run the program or file inside the virtual computer system.
- Clicking the green 'C' button at bottom-left will open a Windows-style 'Start Menu'.



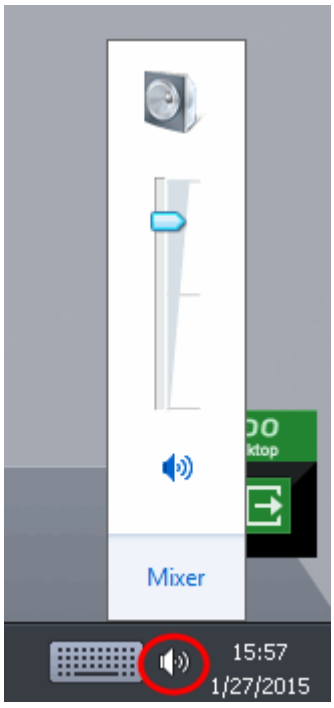
The start menu allows you to:

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

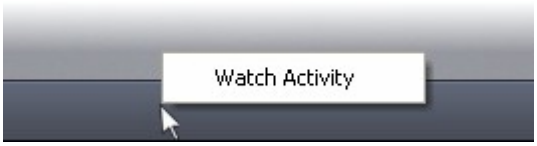
- Clicking the keyboard icon on the system tray opens a virtual keyboard that can be used to input confidential data like website user-names, passwords and credit card numbers.



- Clicking the 'Volume Control' icon at the system tray enables you to control the system volume.



- Right-clicking on the task bar and selecting 'Watch Activity' opens the 'Windows Task Manager' to view your computer's performance, close unresponsive programs and to troubleshoot problems with Windows.



Tablet Mode

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

There are two variations of this mode:

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

You can swap between the two modes by clicking the green arrow at the top right corner: 

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

Tablet Mode A - Pure Tablet

Tablet Mode B - Tablet + Windows

The following table gives a comparison of the classic and tablet modes of the main interface:

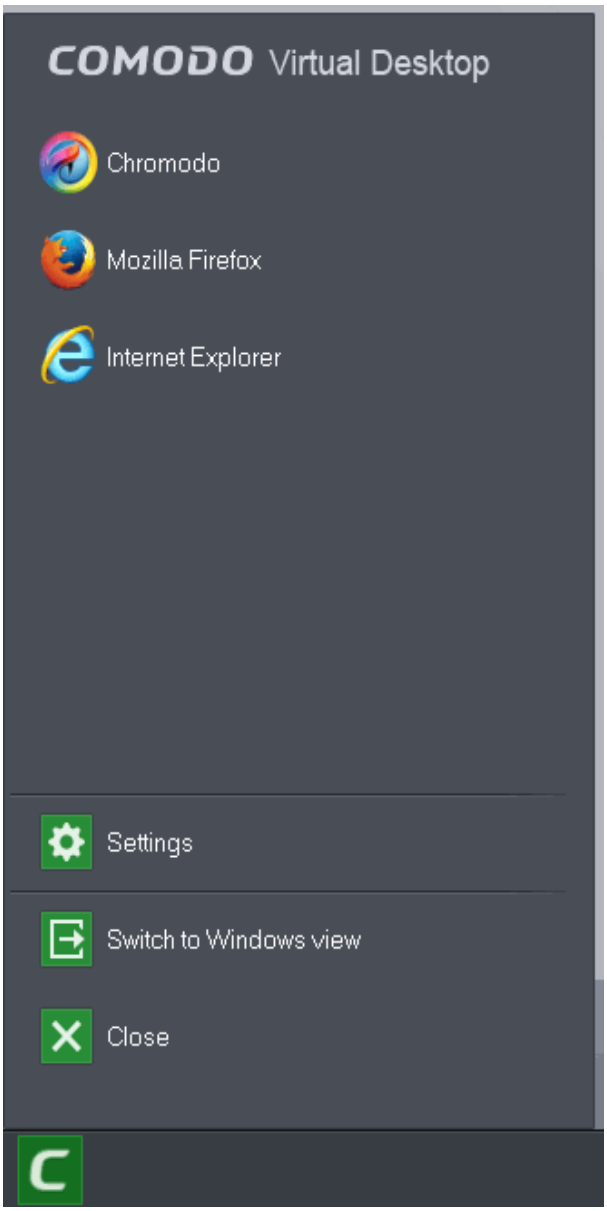
Classic Mode	Mode A - Pure Tablet	Mode B - Tablet + Windows
Windows desktop style interface.	Tablet style interface.	Tablet style interface.
Your real desktop shortcuts and files are displayed	Shortcut icons of the apps installed on the tablet are displayed	Your real desktop shortcuts and files are displayed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

4.1.3. Running Browsers Inside the Virtual Desktop

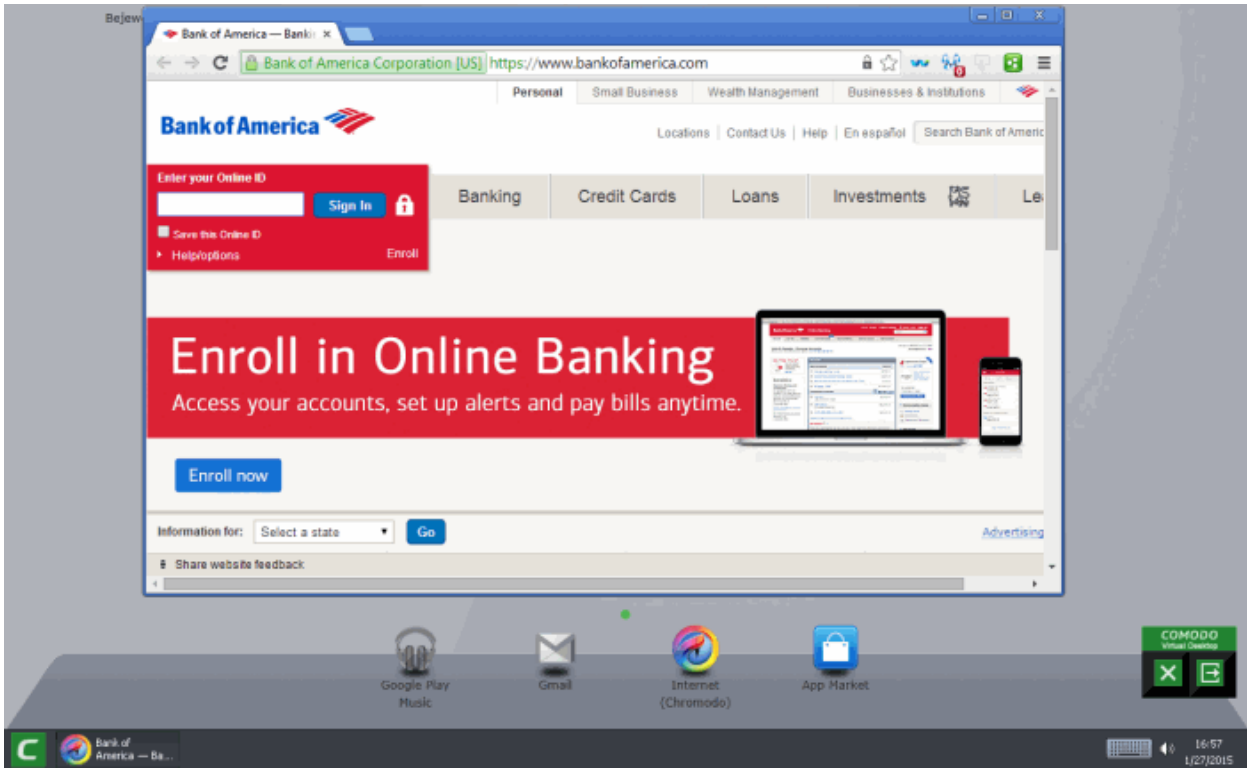
The Virtual Desktop provides an extremely secure environment for Internet related activities because it isolates your browser from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net from inside the virtual computer system removes this threat by preventing websites from installing applications on your real computer. Furthermore, the Virtual Keyboard allows you to securely enter user-names, credit card numbers and passwords without fear of key-logging software recording your physical keystrokes.

To run a browser inside the Virtual Desktop

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



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



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

4.1.4. Opening Files and Running Applications inside the Virtual Desktop

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

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

Desktop Shortcuts

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

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

Shared Space

The Virtual Desktop creates a folder Shared Space in the location "C:\Documents and Settings\All Users\Application Data\Shared Space". The 'Shared Space' folder can be shared by your host operating system and the Virtual Desktop.

The Shared Space can be accessed in the following ways:

- Click 'Open Shared Space' under 'Sandbox' Tasks in the Tasks Interface
- Click the 'Shared Space' shortcut icon from the home screen of CIS
- Click the 'Shared Space' shortcut icon from the CIS widget
- Click the 'Shared Space' desktop shortcut icon

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

1. Open the 'Shared Space' as mentioned above
2. Copy/Move the application or the file to be opened into the Shared Space
3. Start 'Virtual Desktop'

4. Open Shared Space inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.

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

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

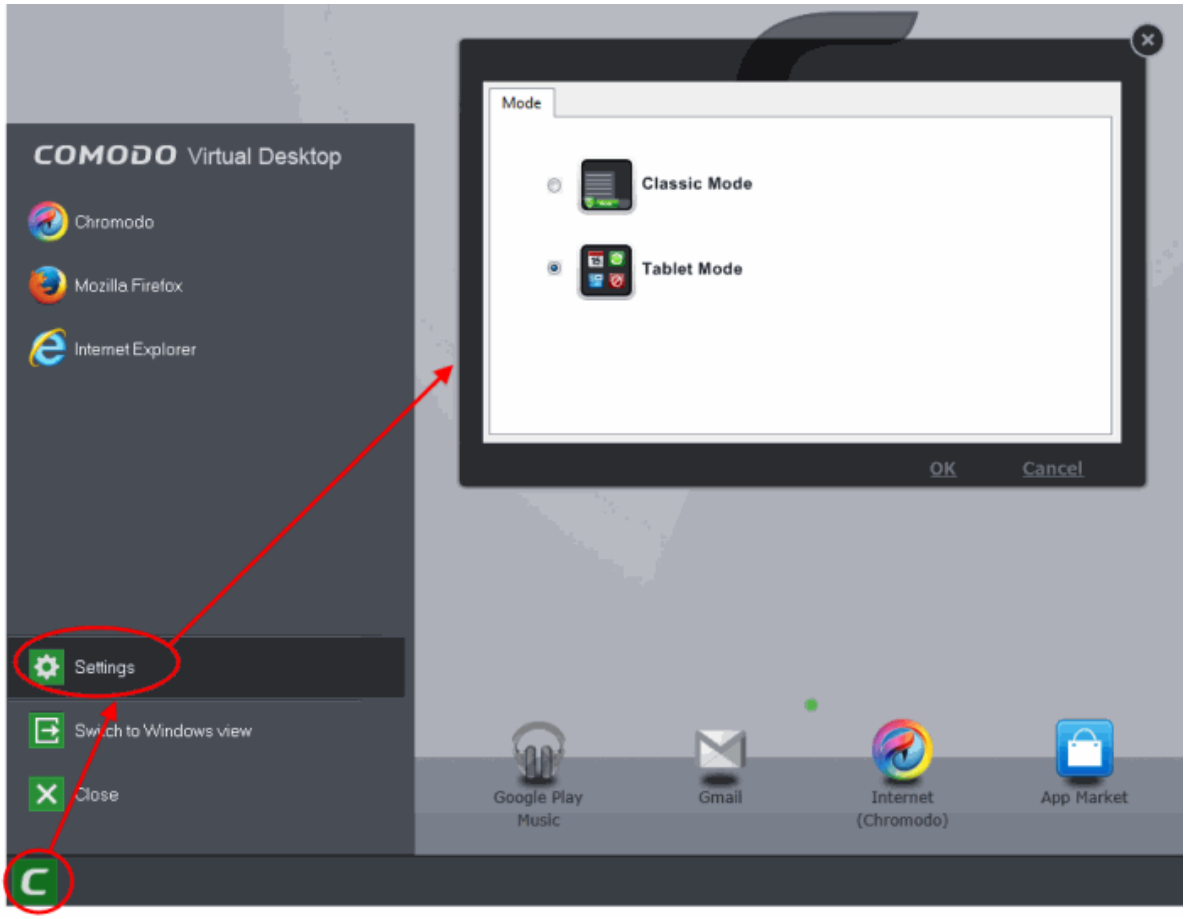
The changes you make to the file will be stored to the file only inside the Virtual Desktop and not in the real computer system.

4.1.5. Configuring the Virtual Desktop

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

To open the settings panel:

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



The Settings panel has two tabs:

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

3. Click OK for your settings to take effect

4.1.6. Closing the Virtual Desktop

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

To temporarily switch to your real Windows system

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

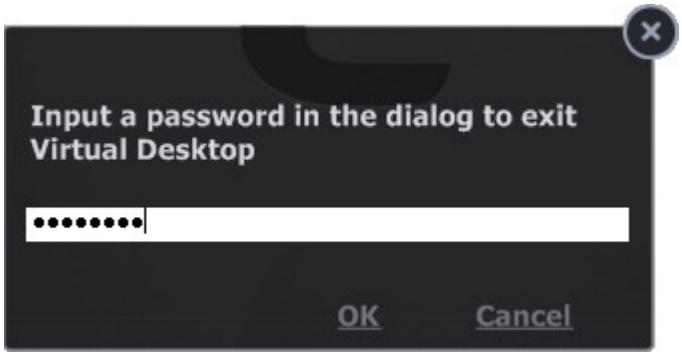
The Virtual Desktop will be temporarily closed. You can quickly return to it by clicking the right switch from the Virtual Desktop shortcut buttons displayed at the bottom right of your Windows Desktop 

or by clicking 'Run Virtual Desktop' from the 'Sandbox Tasks' interface.

To close the Virtual Desktop

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

In either case, if password protection is enabled under **Advanced Settings > Security Settings > Defense+ > Sandbox Settings**, you will be prompted to enter the password. Else the Virtual Desktop will be closed.



- Enter the password and click OK.

Note: Remember to save the changes before you exit the Virtual Desktop. Your changes will be lost if you exit the Virtual Desktop.

4.2. Run an Application in the Sandbox

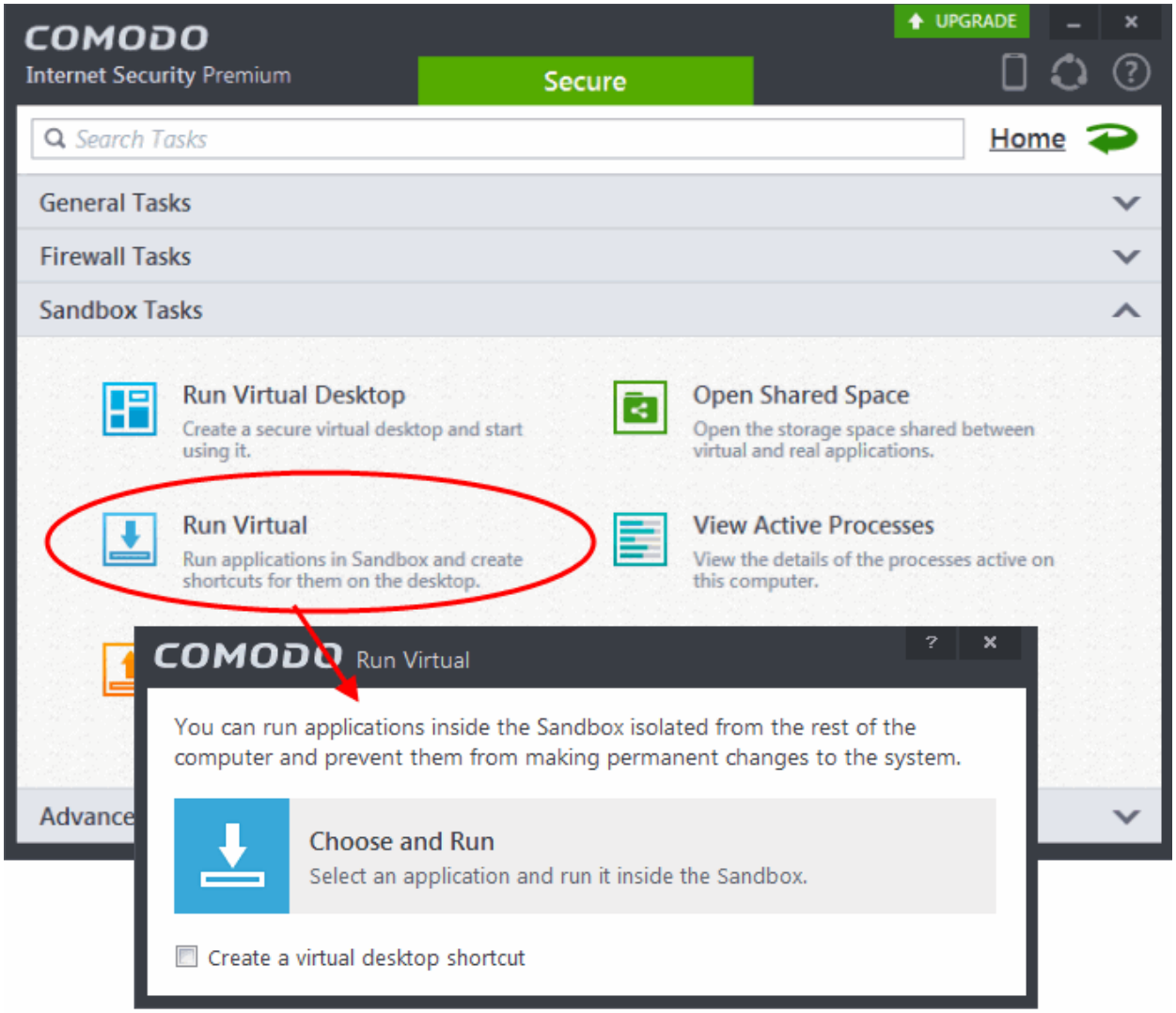
Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. Adding a program in this way means that it will run in the Sandbox this time only. On subsequent executions it will not run in the sandbox (presuming it passes **the sandboxing process**).

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

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

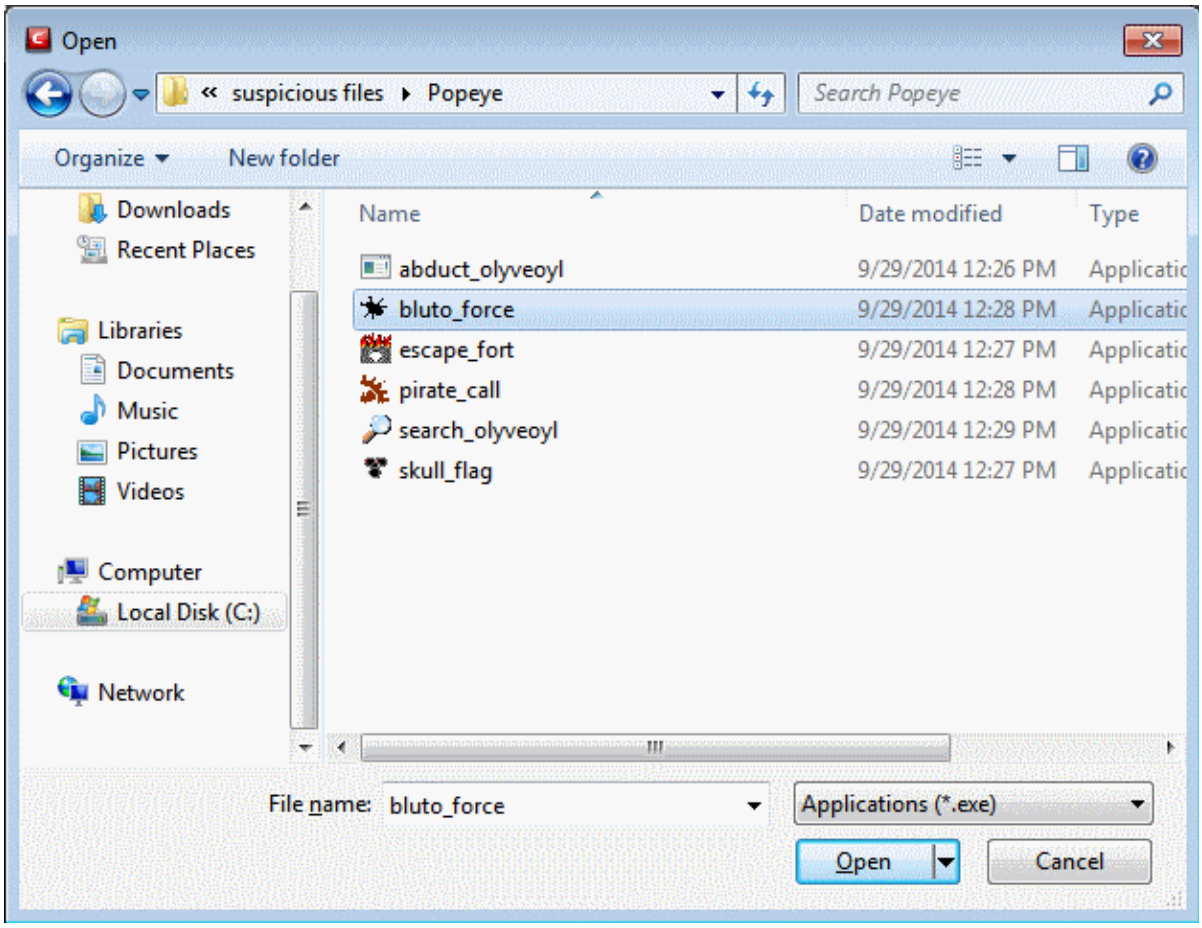
To run an application in the Sandbox

1. Open the Sandbox Tasks interface and Click 'Run Virtual'.



The 'Run Virtual' dialog will be displayed.

2. To run an application inside the sandbox, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is sandboxed. If you wish to run the application in the sandbox in future, then select 'Create a virtual desktop shortcut'.



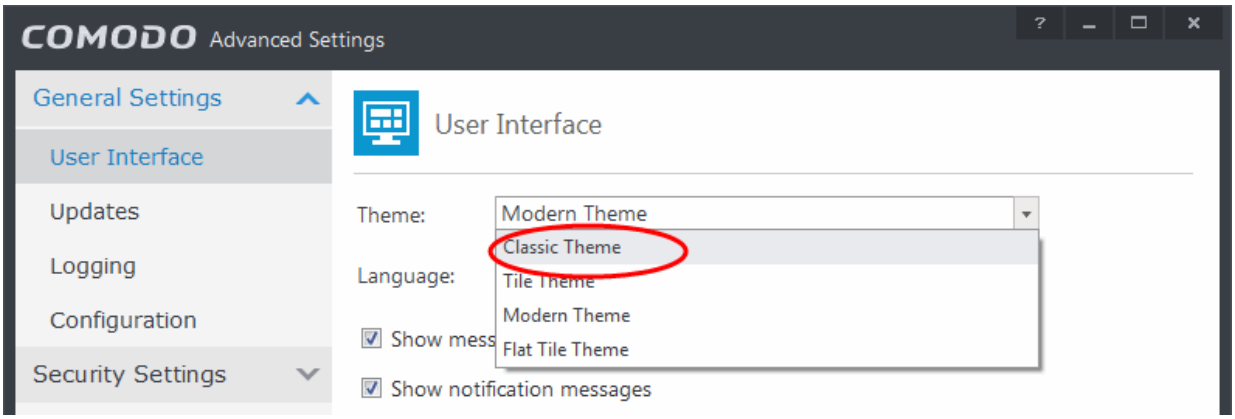
3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

Alternatively, you can run an application inside the sandbox by the following shortcut methods:

- **By dragging-and-dropping the application on to CIS Home screen**
- **From the context sensitive menu**
- **Running browsers inside sandbox**

Drag-and-drop the application on to CIS Home Screen

Note: This feature is available only if you use 'Classic theme' for the user interface. You can switch to this by selecting 'Classic Theme' from the 'Theme' drop-down in Advanced Settings > General Settings > User Interface. Please restart the application to implement the change. For more details, refer to the section **Customize User Interface**.

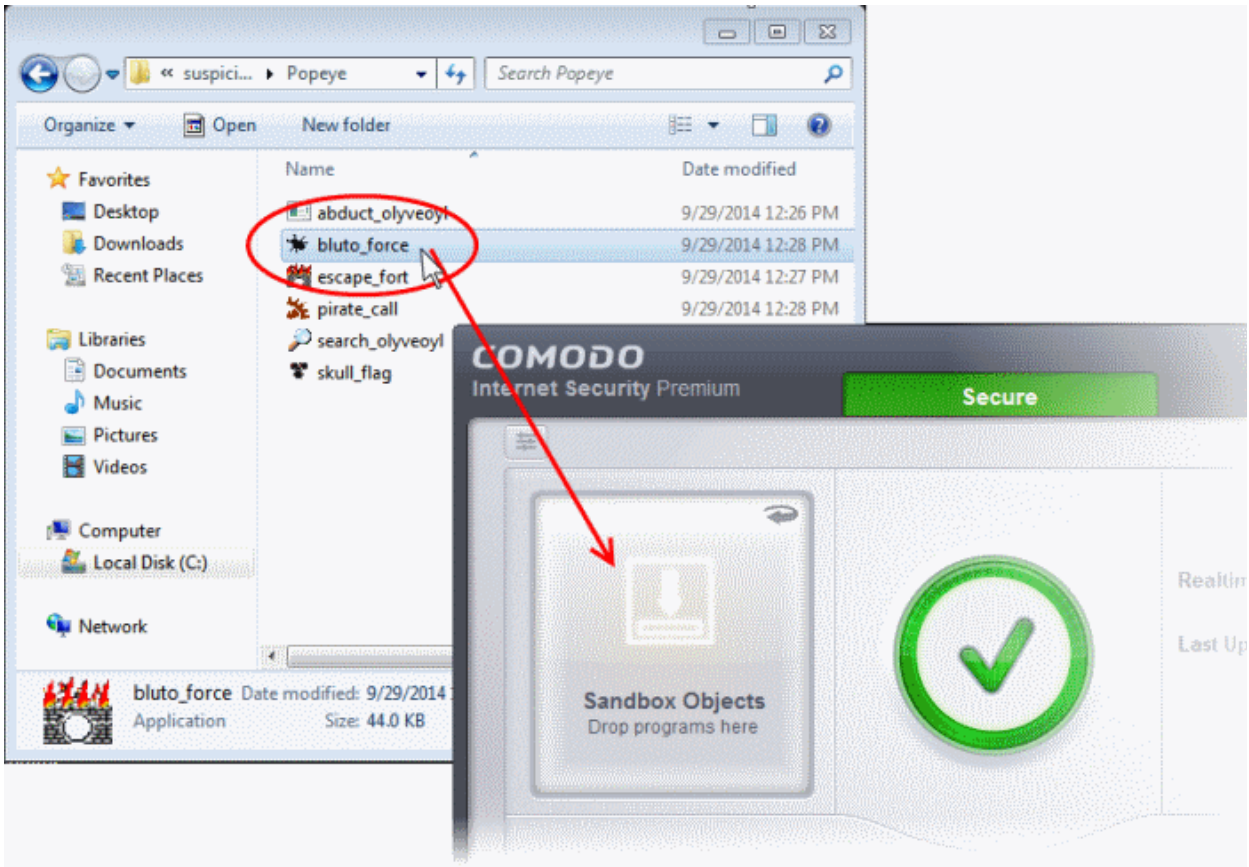


In Classic Theme, the Home screen has a flippable pane on the left which allows you to run instant AV scans on an object or to

run a program in sandbox. Click the curved arrow at the top left of the box to switch between the two.

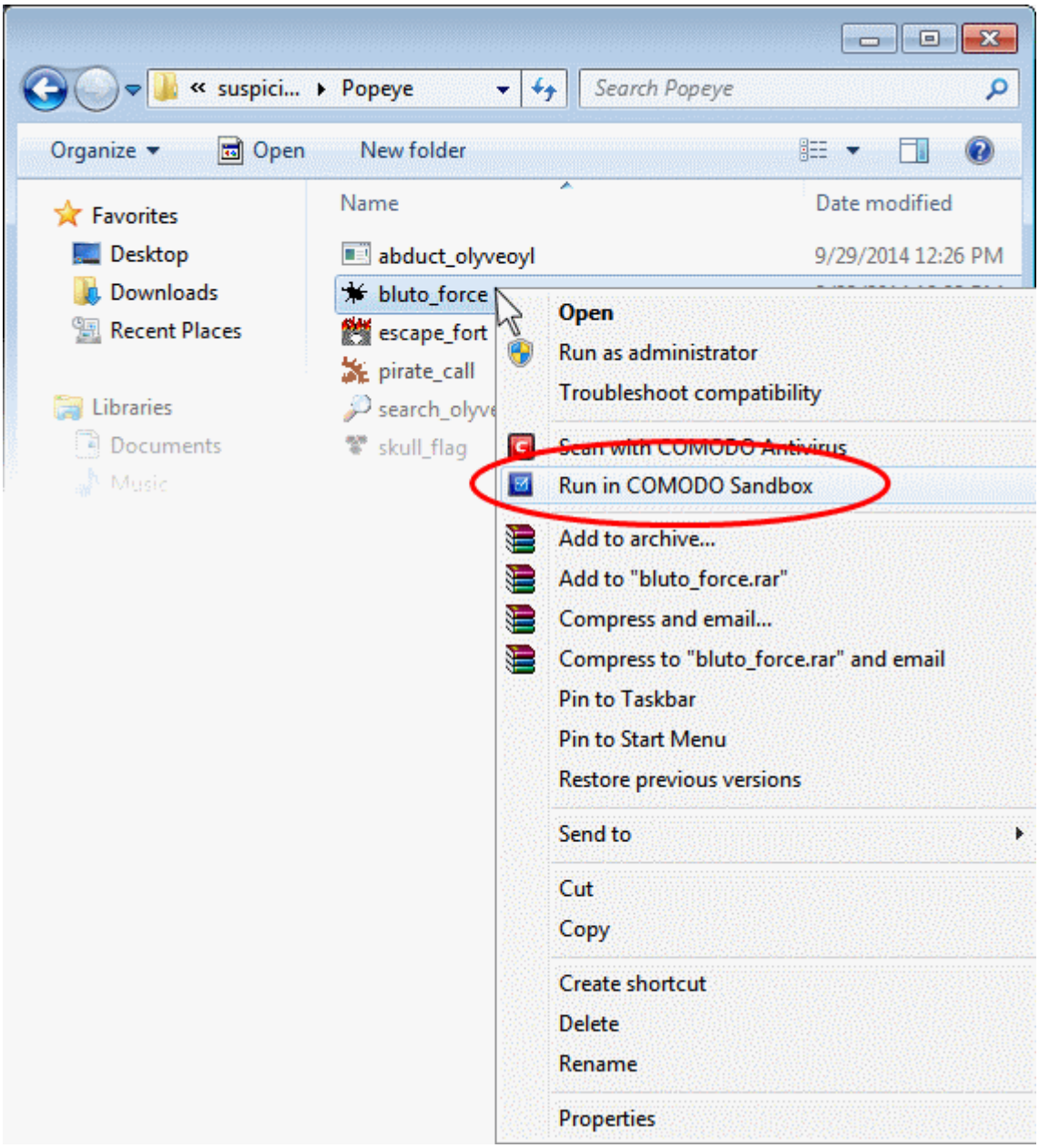
- To run a program in a sandbox, flip the pane so it displays 'Sandbox Objects'.

- Navigate to the program that you want to run in the sandbox and drag and drop it into the box.



Running a program from the context sensitive menu

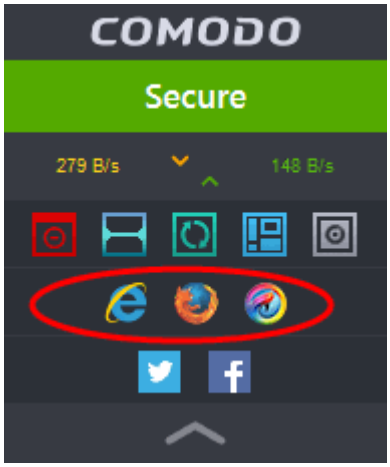
- Navigate to the program in your system that you want to run in sandboxed environment and right click on it



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

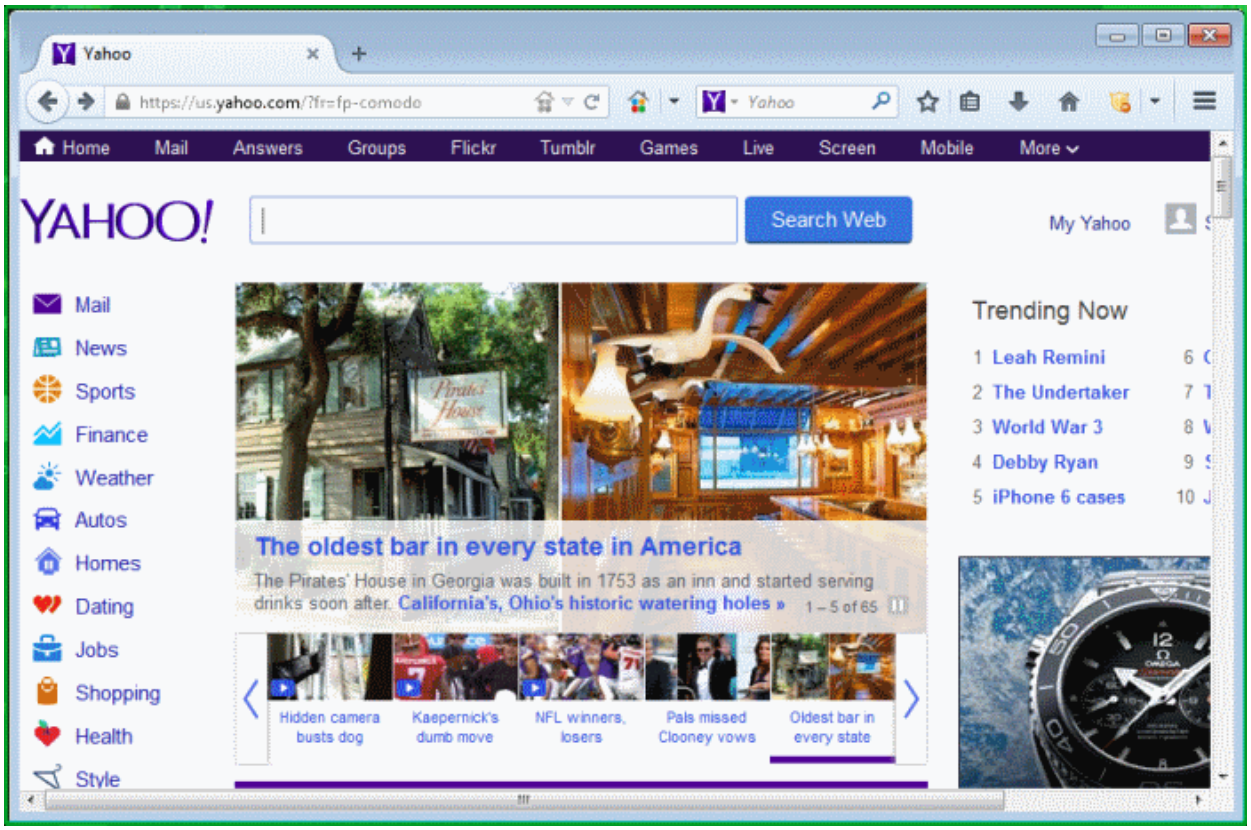
Running Browsers inside the Sandbox

The CIS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- Clicking on a browser icon will start the browser inside the sandbox.

The browser will be started and executed inside the sandbox at 'Fully Virtualized' level. CIS displays a green border around the windows of programs to indicate that they are running inside the sandbox, if the setting '**Show highlight frame for virtualized programs**' is enabled in **Sandbox Settings**.



The application will run in the Sandbox on this occasion only.

- If you often want the browser to run sandboxed then create a 'virtual shortcut' for the application. Run the browser from the Sandbox tasks interface as explained under '**To run an application in the Sandbox**' and select the check-box 'Create a virtual desktop shortcut' in step 2.
- If you wish to run an application in the sandbox on a long-term/permanent basis then **add the file to the Sandbox**.

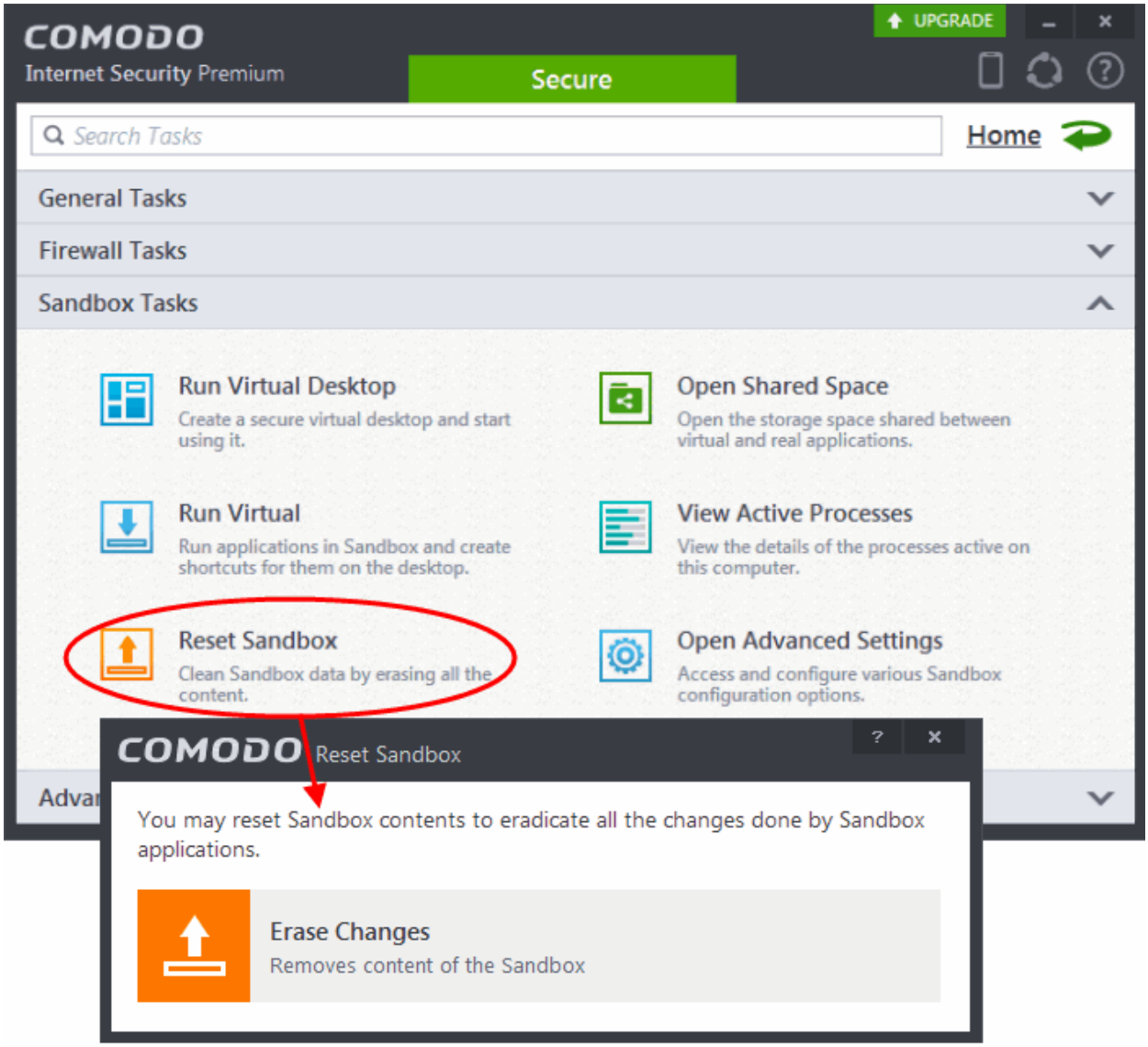
4.3. Reset the Sandbox

Programs running inside the Virtual Desktop store the changes to the files accessed by them inside the sandbox so that the changes do not affect the real computer system. Items stored in the sandbox/ Virtual Desktop could, depending on your usage patterns, contain malware downloaded from websites or private data in your browsing history. Periodically resetting the sandbox will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time, then resetting the sandbox will also help the Virtual Desktop operate more smoothly.

The Reset Sandbox option under the Sandbox Tasks allows you to delete all the items stored in the sandbox.

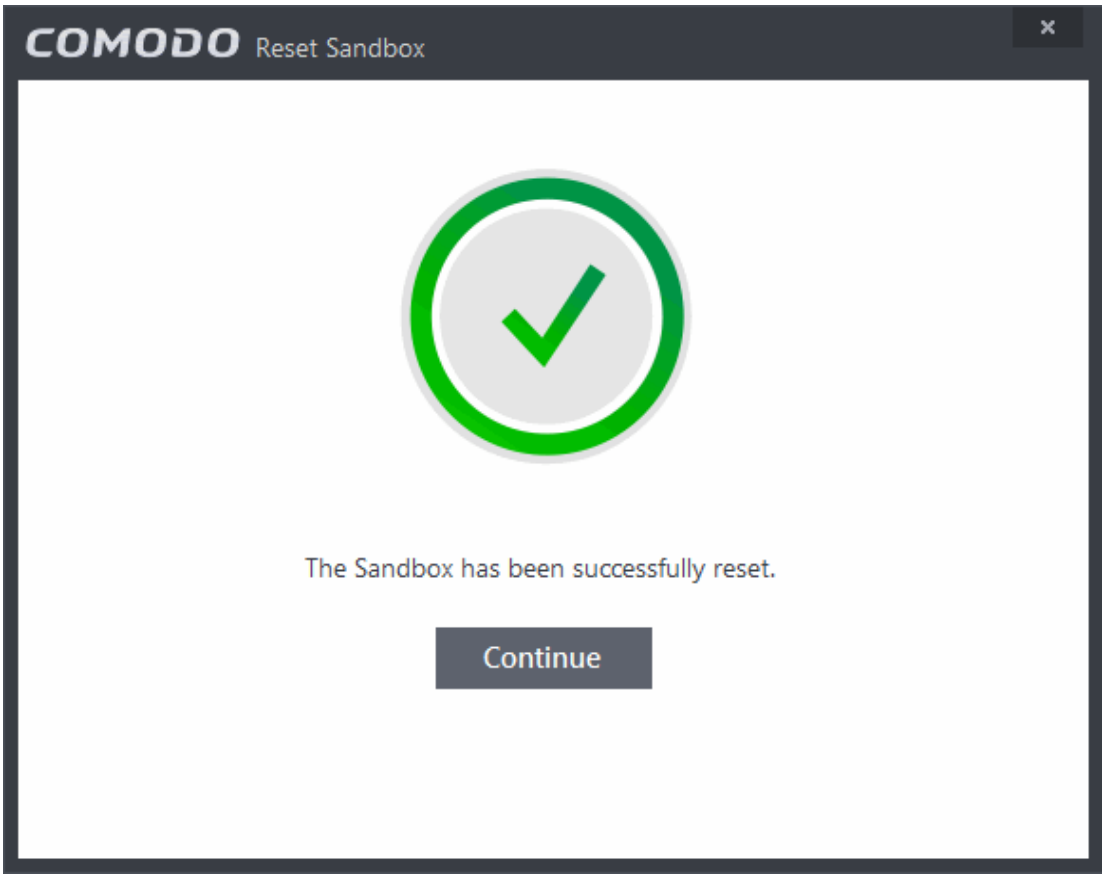
To clear the sandbox

- Click on the 'Sandbox Tasks' bar from the Tasks interface and then click 'Reset Sandbox'



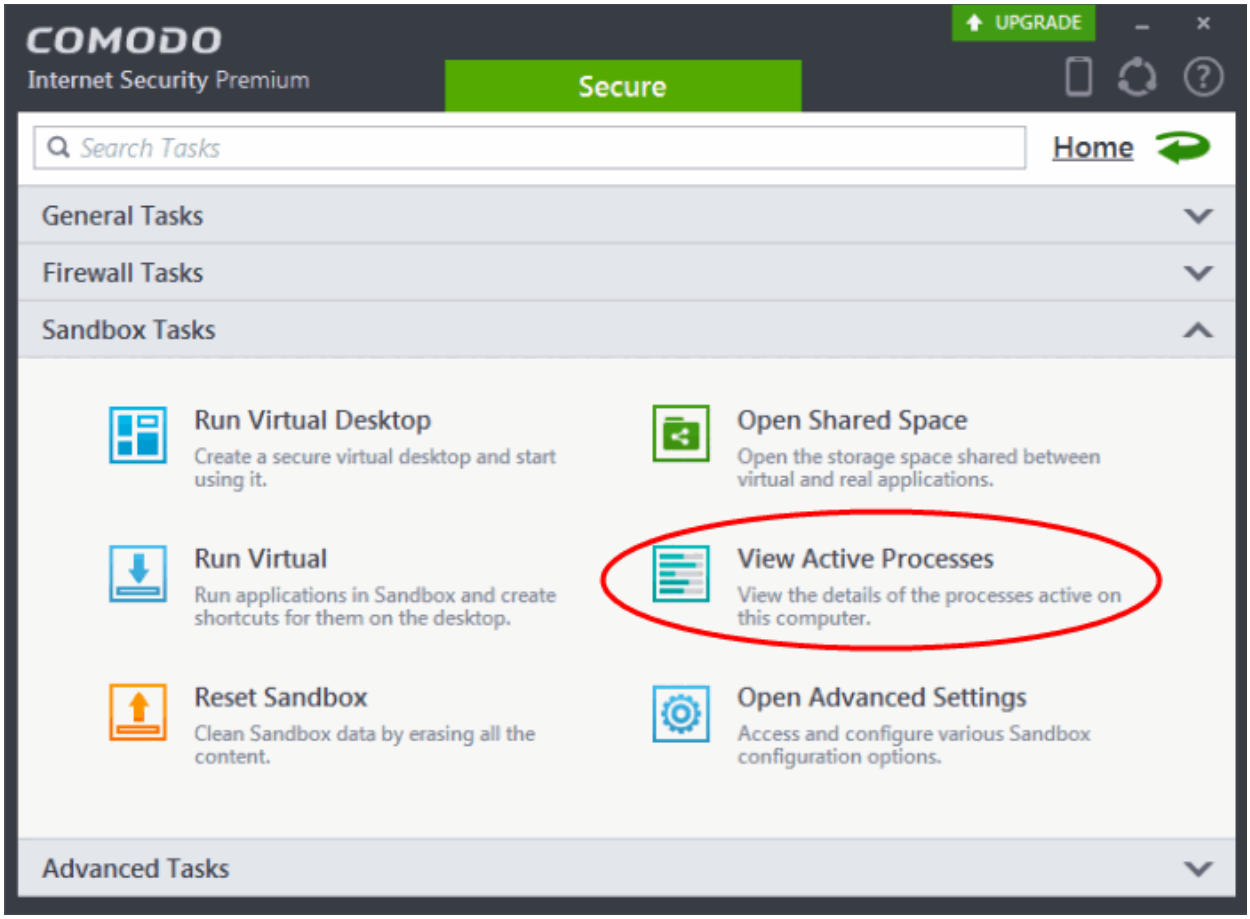
The 'Reset Sandbox' dialog will appear.

- Click 'Erase Changes'. The contents in the sandbox will be deleted immediately.

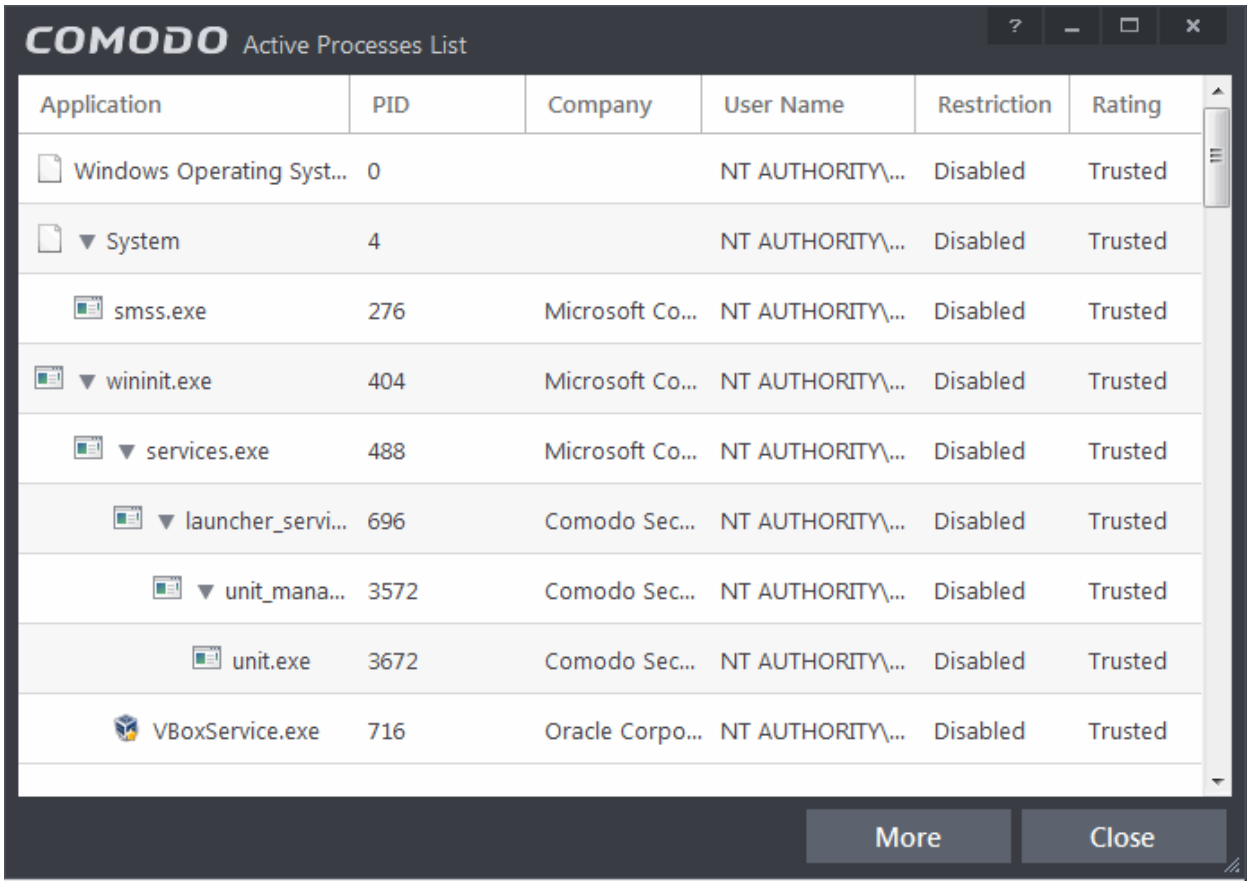


4.4. View Active Process List

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



- The 'View Active Processes' panel can be accessed by clicking 'Tasks > Sandbox Tasks > View Active Processes



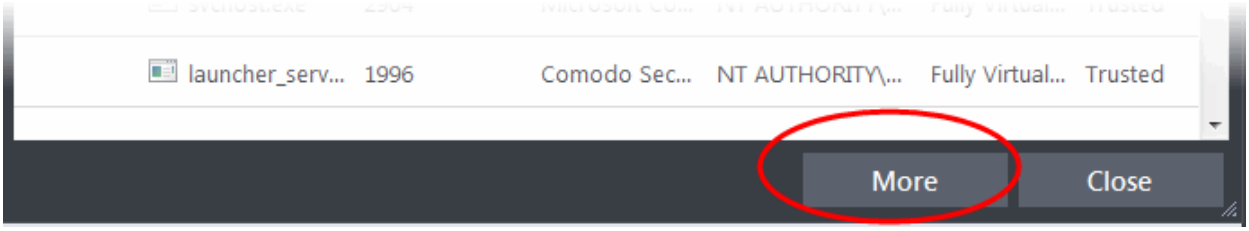
Column Descriptions

- **Application** - Displays the names of the applications which are currently running on your PC.
- **PID** - Process Identification Number.
- **Company** - Displays the name of the software developer.
- **User Name** - The name of the user that started the process.
- **Restriction** – Displays the level of sandbox setting selected for the program.
- **Rating** – Displays the rating of the application whether trusted or unknown.

Right-click on any process to:

- Show full path: Displays the location of the executable in addition to it's name.
- Show Sandboxed Only: Displays the details of the sandboxed programs only. Disable this option to view all the current active process list.
- Add to Trusted Files: The selected unknown program is added to CIS **File List** with Trusted Status. Refer to the section **File List** for more details.
- Online Lookup: The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: The folder containing the executable file of the application will open.
- Show Activities: Opens the **Process Activities List dialog**. The Process Activities dialog will display the list activities of the processes run by the application. The 'Show Activities' option is available only if **Viruscope is enabled** under **Viruscope**.

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



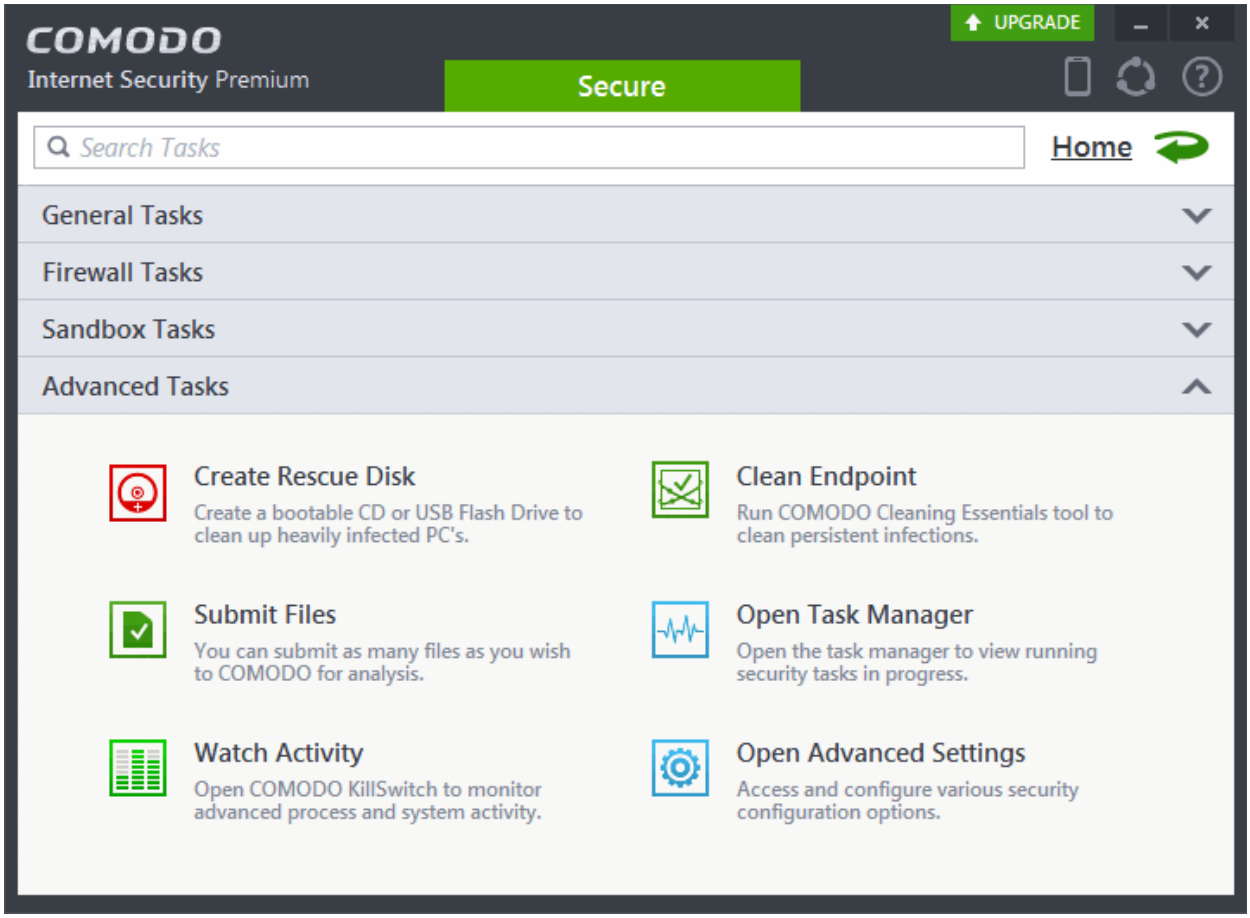
If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the section **Identify and Kill Unsafe Running Processes** for more details.

5.Advanced Tasks - Introduction

The 'Advanced Tasks' area allows you modify the overall configuration of CIS, manage CIS tasks like AV scans and updates currently running in the backgound or in minimized window and to take advantage of several other Comodo utilities. Click the following links to find out more about each item:

- **Create Rescue Disk - Burn a bootable ISO that lets you run virus scans in pre-boot environments**
- **Submit Files - Directly Submit unknown/suspicious files to Comodo for analysis**
- **Watch Activity - Use Comodo Killswitch to identify unsafe processes and manage system activity**
- **Clean Endpoint - Deploy Comodo Cleaning Essentials to eradicate persistent infections from your PC**
- **Task Manager - Manage priorities of, stop, pause and resume currently running CIS tasks like Antivirus scans and updates**
- **Open Advanced Settings - Configure overall behavior, define custom rulesets and much more**

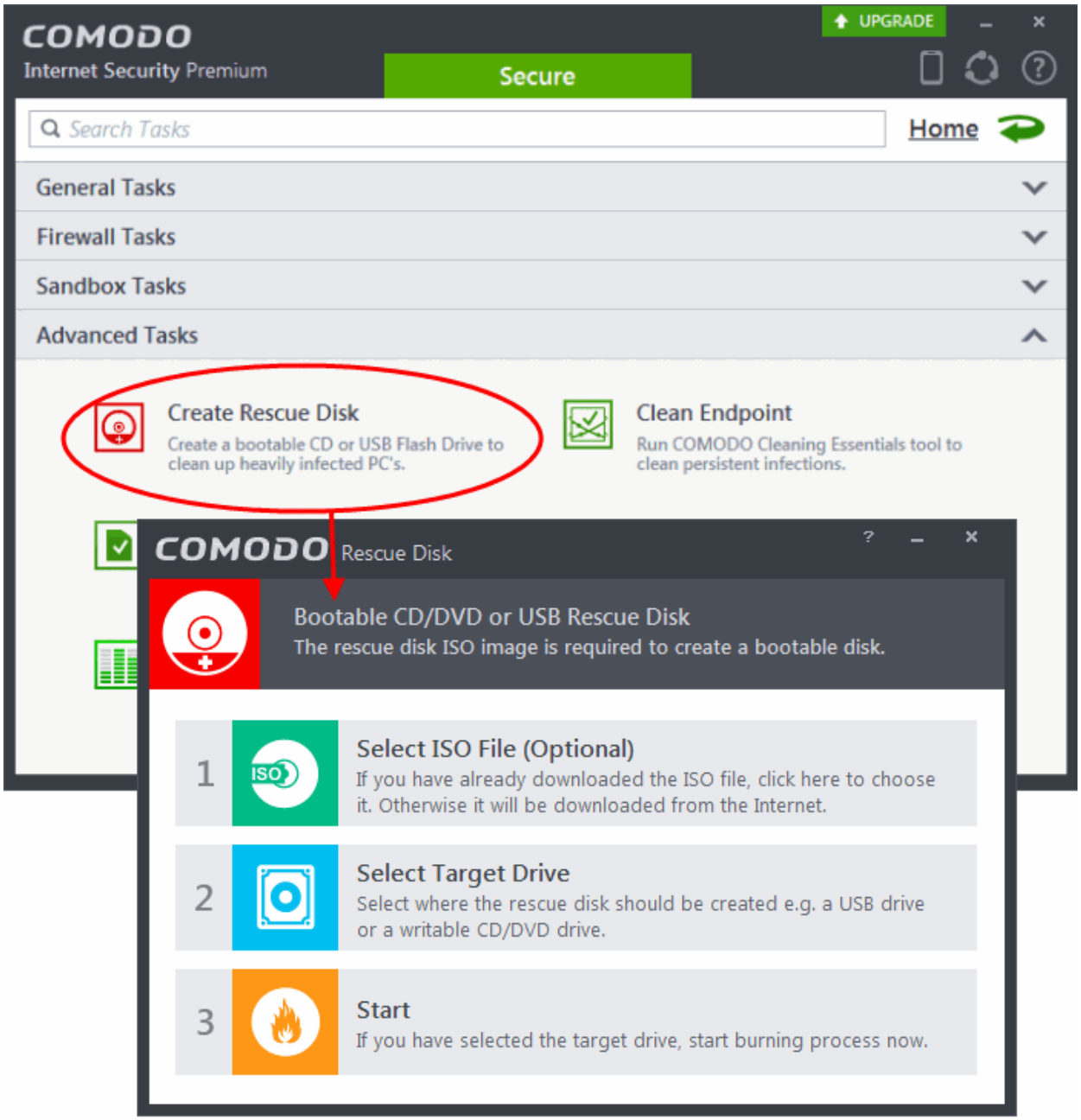
Some of these utilities require the download and installation of additional setup files. After installation, the utility will start directly next time you click the button.



5.1. Create a Rescue Disk

Comodo Rescue Disk (CRD) is a bootable disk image that allows users to run virus scans in a pre-boot environment (before Windows loads). CRD runs Comodo Cleaning Essentials on a lightweight distribution of the Linux operating system. It is a powerful virus, spyware, rootkit scanner and cleaner which works in both GUI and text mode. The tool can provide a more comprehensive and thorough scan than regular malware cleaning applications because it cleans your system before Windows is loaded. CRD is intended to be used when malware embeds itself so deeply into your system that regular AV software cannot remove it. The rescue disk is also very effective at removing infections that are preventing Windows from booting in the first place. Apart from the virus scanner, CRD also provides tools to explore files in your hard drive, take screen-shots and browse web pages.

- Clicking the 'Create Rescue Disk' button in CIS 'Advanced Settings' opens a utility that allows you to download and burn the CRD iso to a CD/DVD, USB or other drive. **Click here** to jump to a walk-through of this process

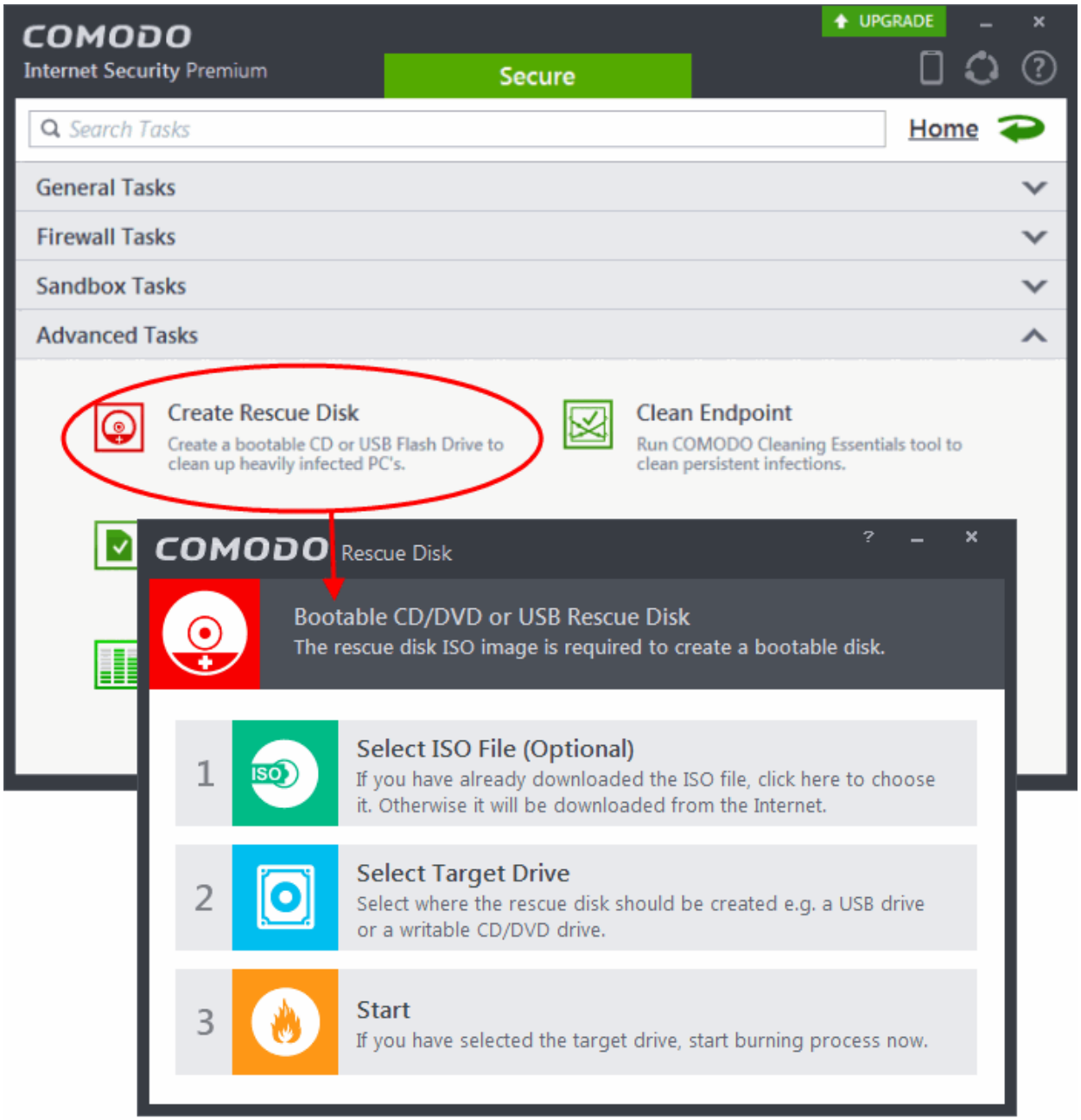


After you have burned the ISO, you need to boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

- Details of how to change boot order on your computer can be found in the Rescue Disk user guide at **http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html**
- Details of how to initiate CRD after booting can be found at **http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html**
- Details of how to start running scans on your pre-boot environment are available at **http://help.comodo.com/topic-170-1-493-5216-Starting-Comodo-Cleaning-Essentials.html** and **http://help.comodo.com/topic-170-1-493-5217-CCE-Interface.html**

5.1.1. Downloading and Burning Comodo Rescue Disk

To create a Comodo Rescue Disk, Click 'Create Rescue Disk' button from the Advanced Tasks interface.



The Comodo Rescue Disk interface will open. The interface displays the steps involved in creation of a new Rescue Disk on a CD/DVD or in a USB drive.

Step 1- Select the ISO file

This step allows you to select the Comodo Rescue Disk image file in .iso format stored in your hard drive, if you have already downloaded the same from Comodo servers or copied from another computer. Pre-storing the .iso file and burning the rescue disk from it conserves your Internet connection bandwidth usage. This step is optional. If you haven't downloaded the iso file, it will be automatically downloaded from Comodo Servers prior to execution of Step 3 - Burning the Rescue Disk.

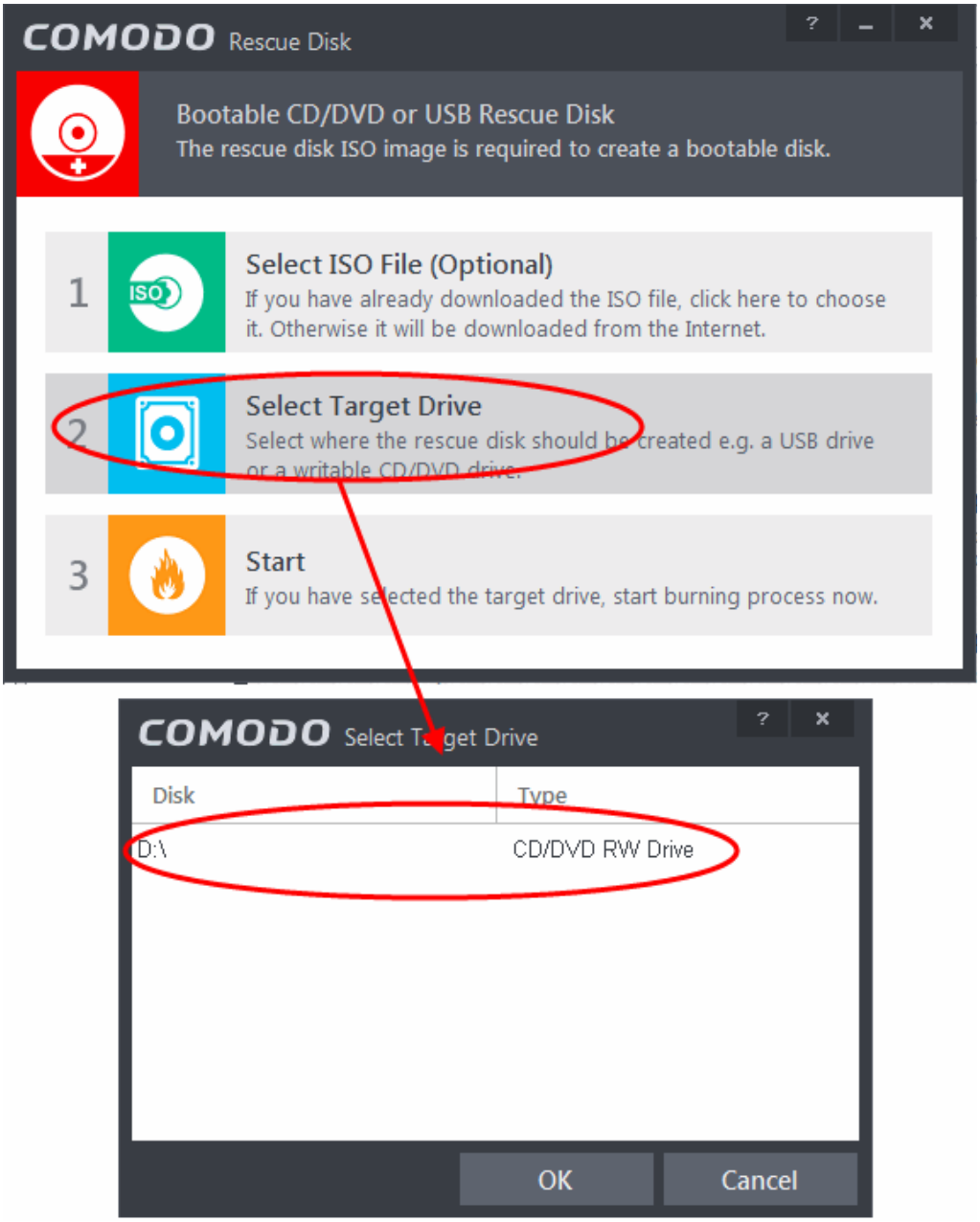
- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

This step allows you to select the CD/DVD drive or the USB drive to burn the Rescue Disk.

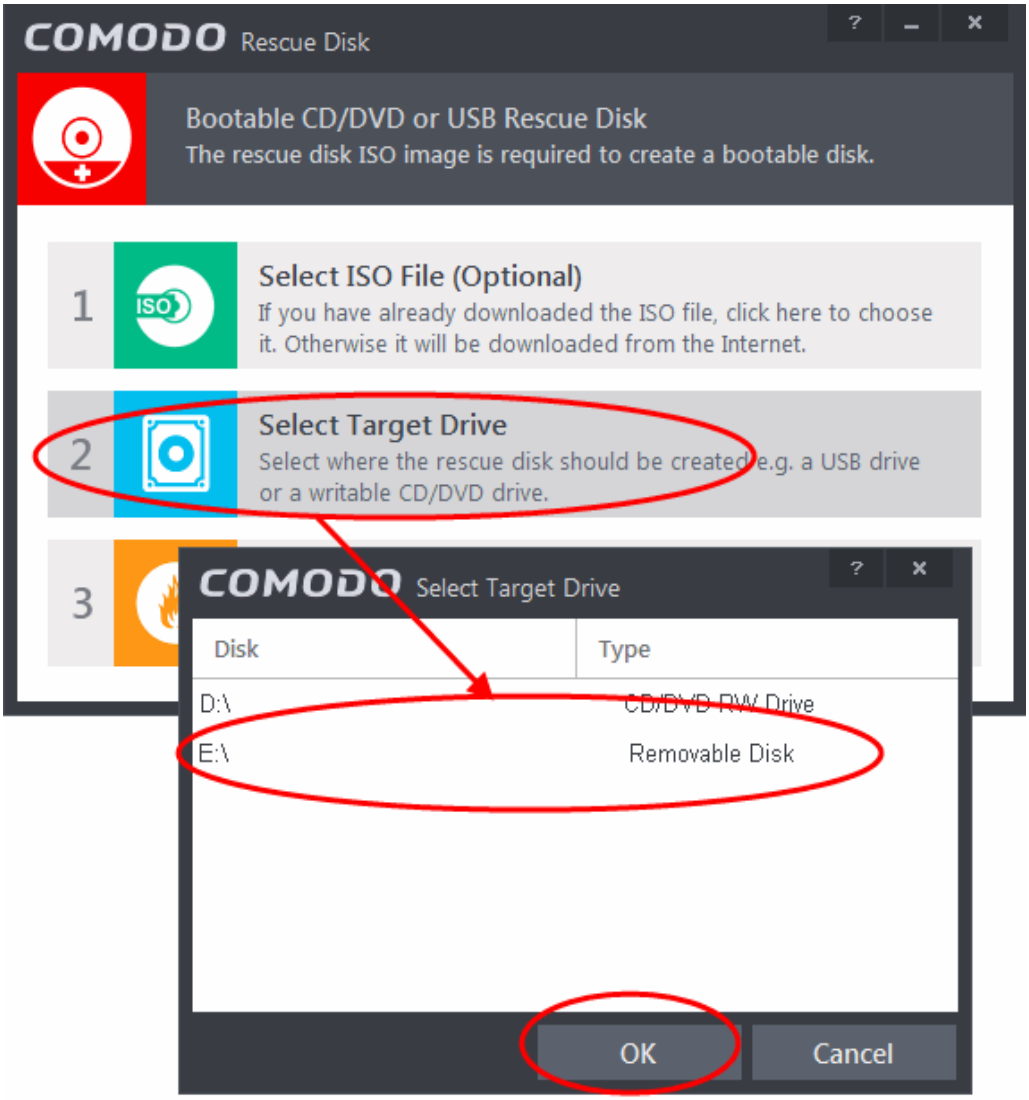
To burn the Rescue disk on a CD or a DVD

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



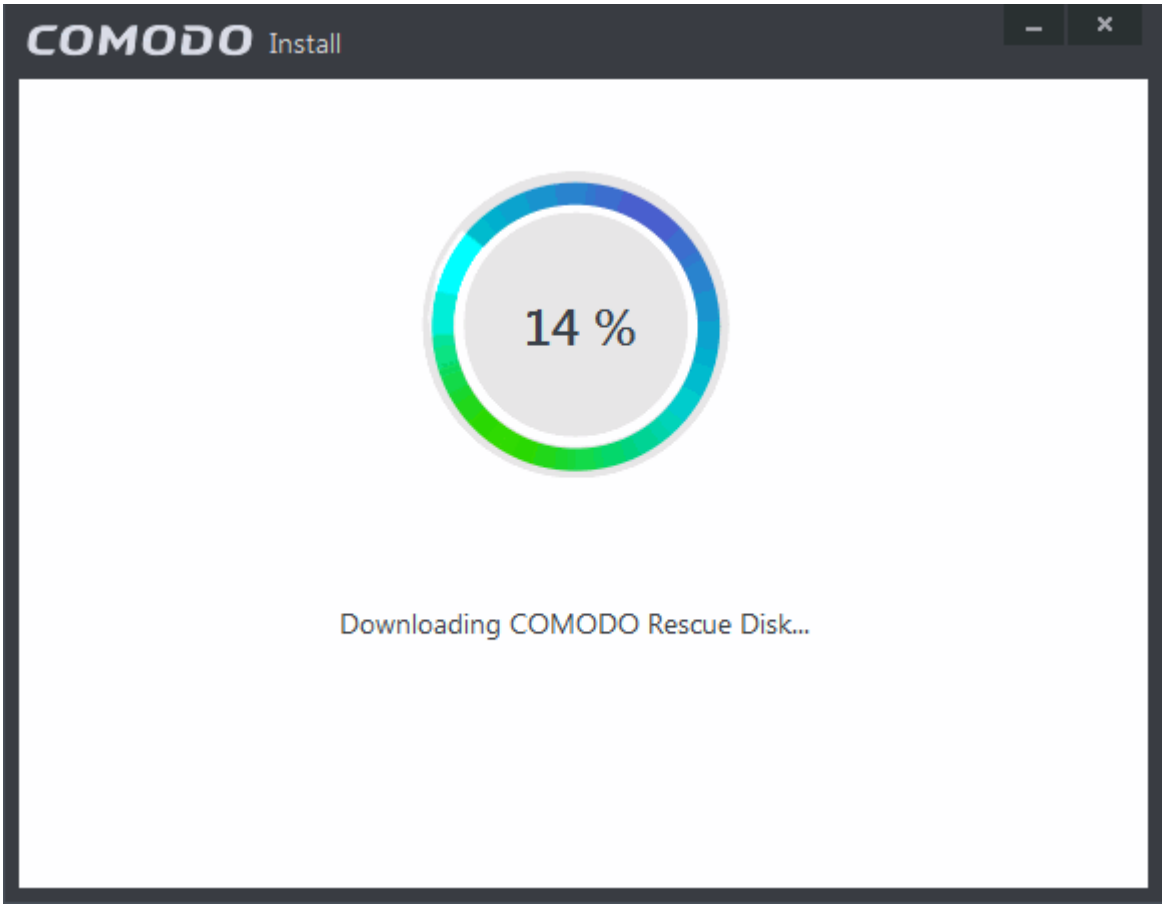
To burn the Rescue disk on a USB Drive

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

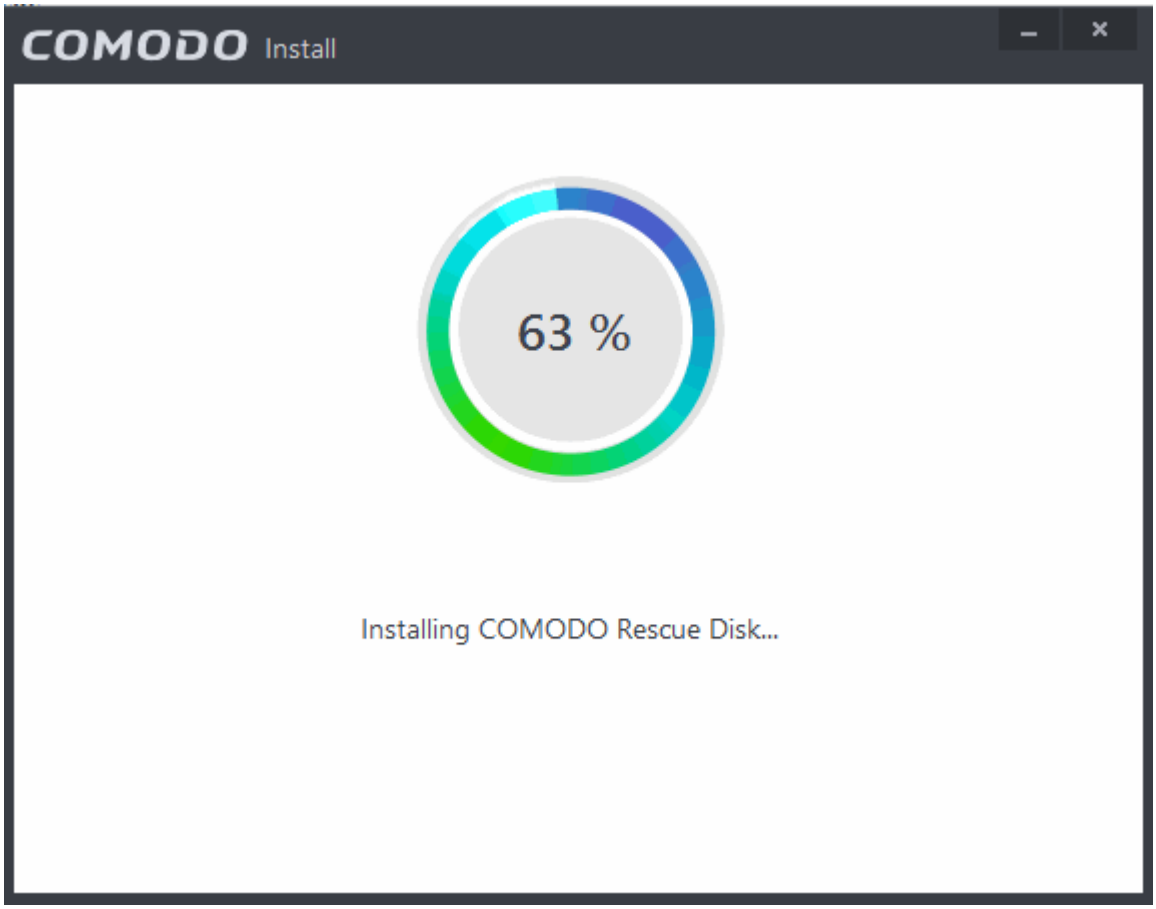


Step 3 - Burn the Rescue Disk

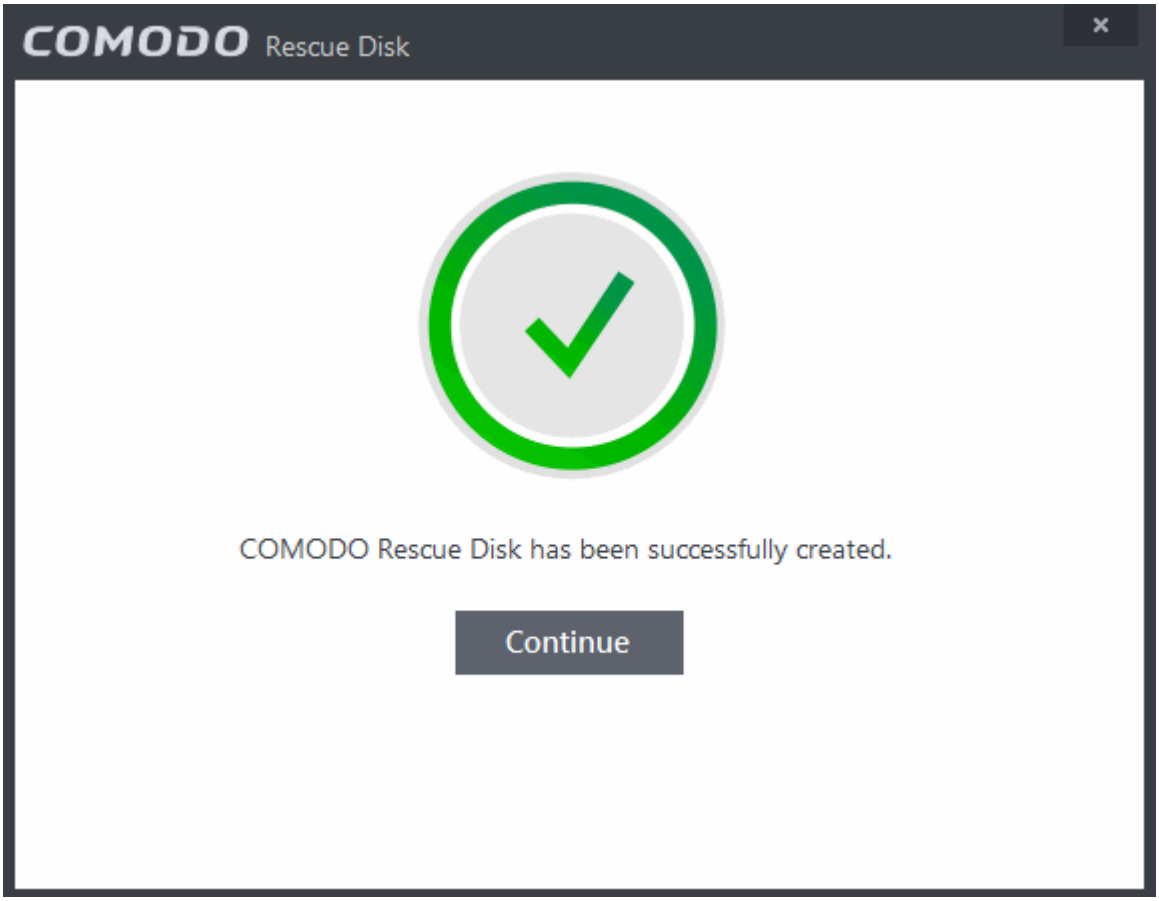
- After you selected the target drive, click 'Start'. If you have selected an .iso file from your hard disk, the burning of the disk will start immediately. Else, the .iso file will be downloaded from Comodo Servers.



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



- Wait till the completion of the process. Do not eject the CD/DVD or the USB drive. On completion of the process, the CD/DVD will be ejected automatically.



Your Bootable Comodo Rescue Disk is created. Click 'Continue' to go back to CIS interface.

5.2. Remove Deeply Hidden Malware

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

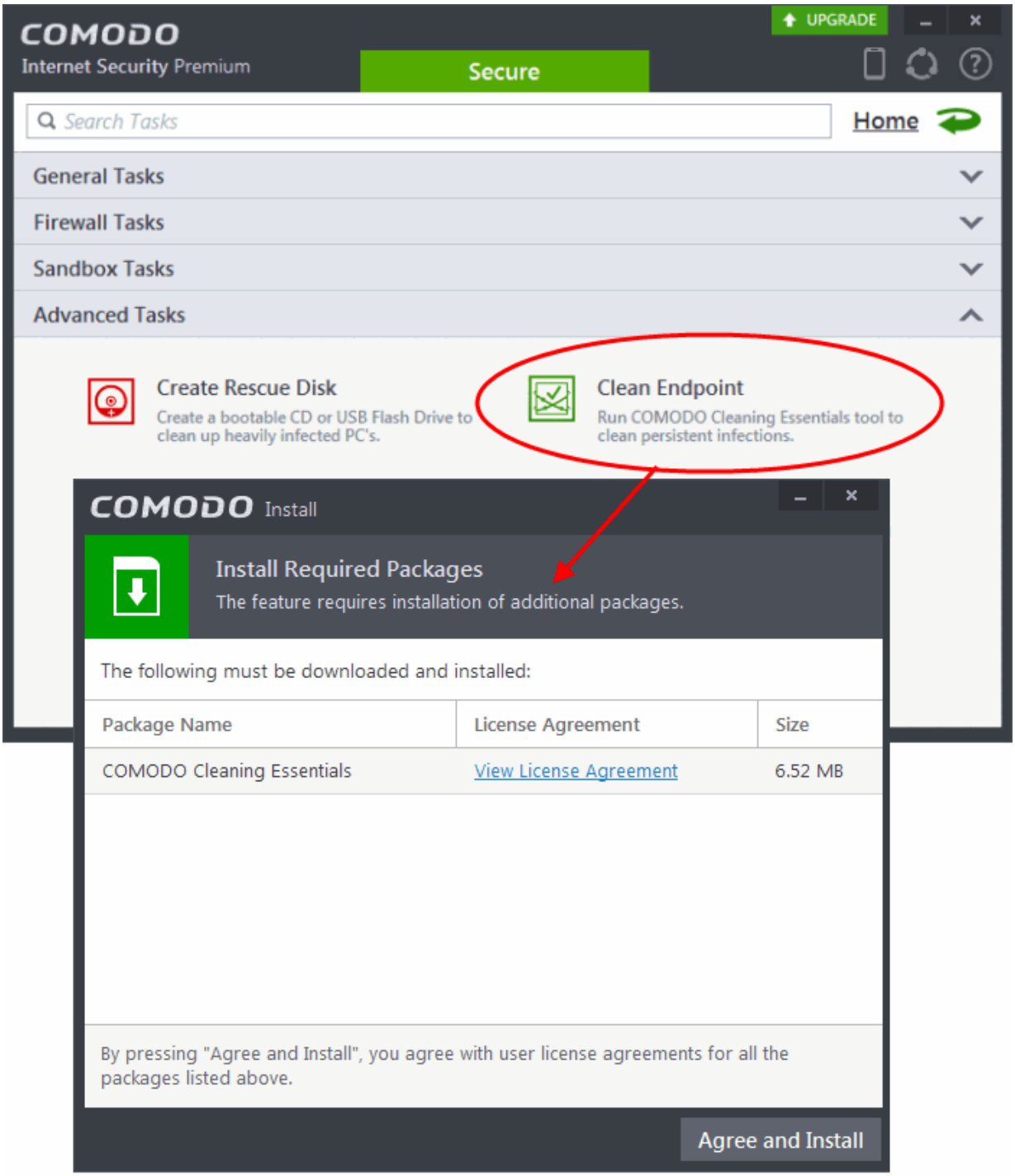
Major features include:

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

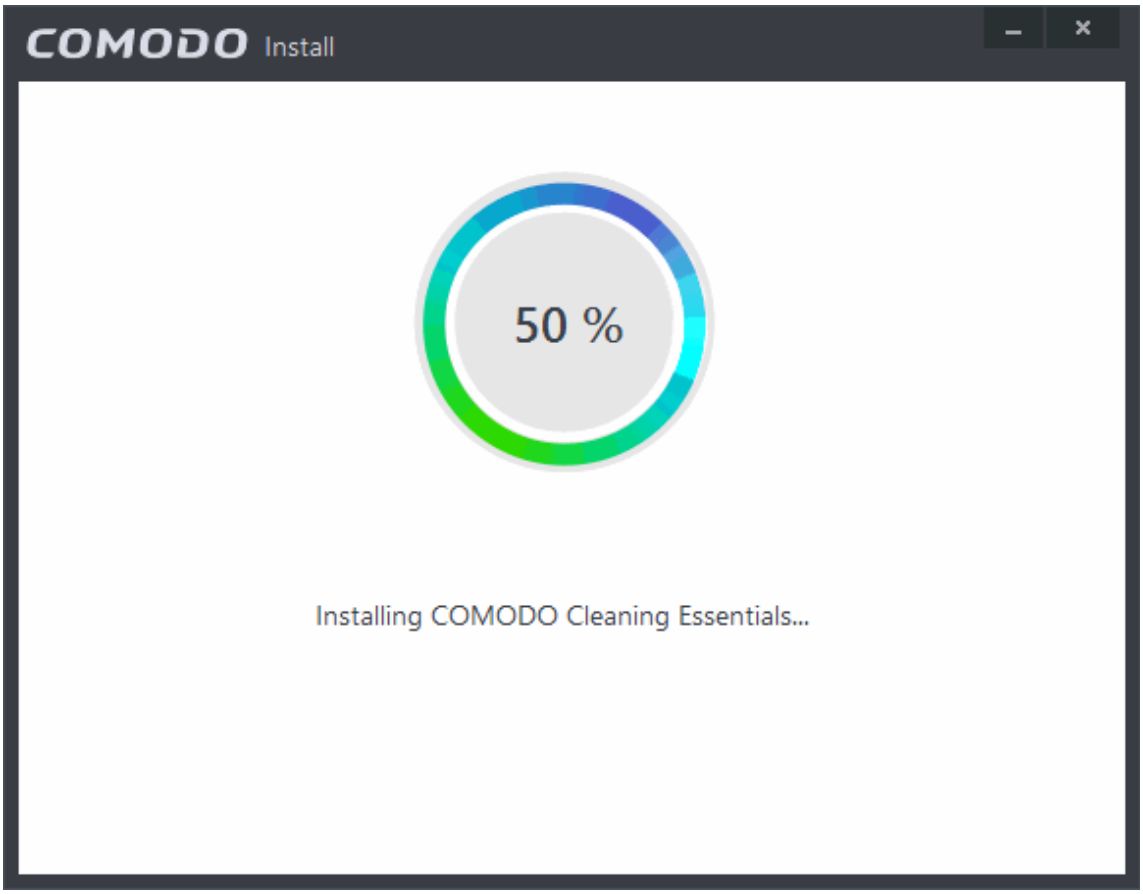
CCE enables home users to quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.

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

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



- Clicking the 'Clean Endpoint' for the first time, CIS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.



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

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

- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at

http://help.comodo.com/topic-119-1-328-3525-The-Main-Interface.html

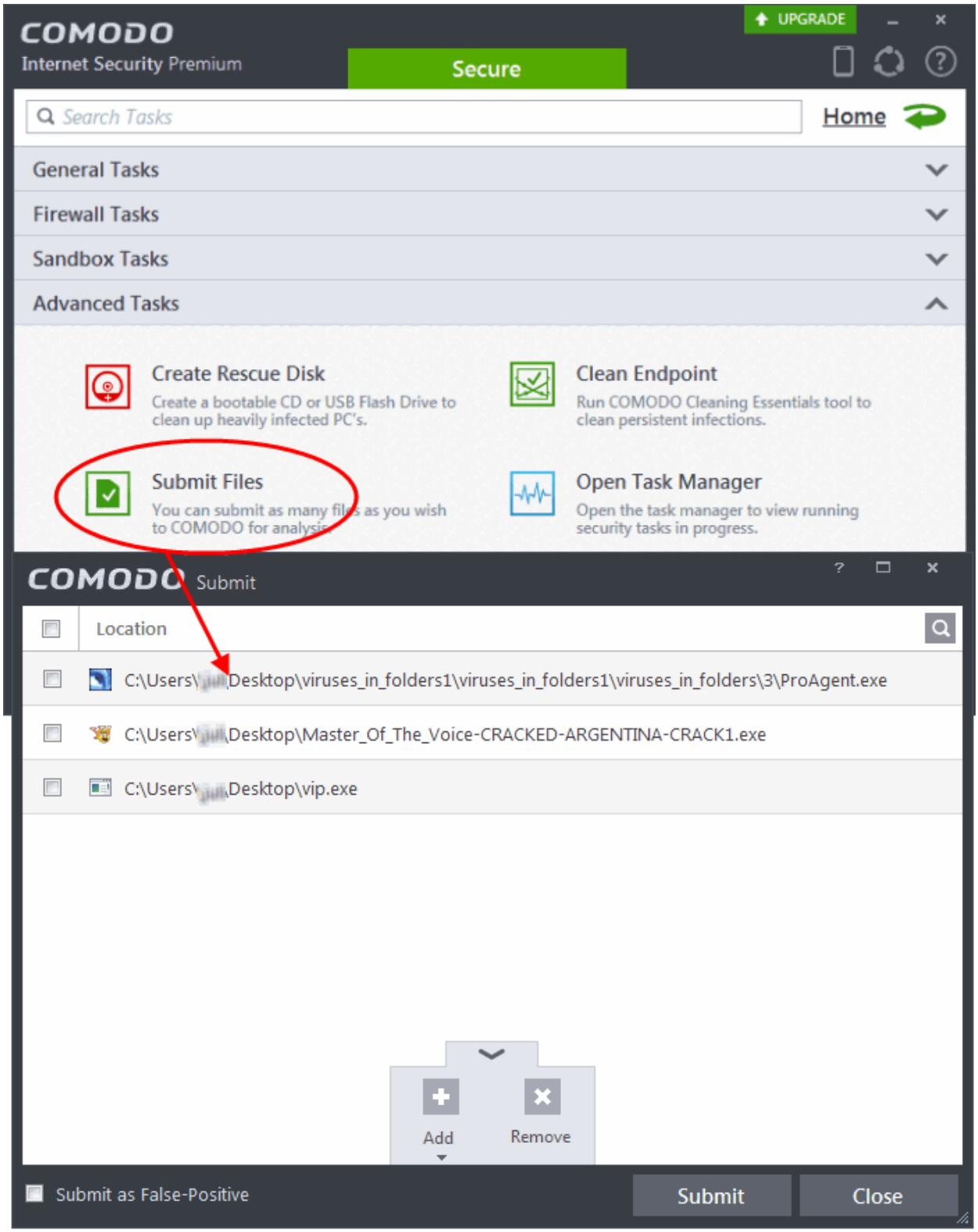
- On clicking the 'Clean Endpoint' button from next time onwards, Comodo Cleaning Essentials will be opened.

5.3. Submit Files

As the name suggests, the 'Submit Files' interface allows you to send as many files as you wish to Comodo for analysis. Files which CIS classifies as 'Unknown' or 'Unrecognized' are not in the Comodo safe list but have also not been identified as known malware. By sending these files to Comodo, you allow our team to analyze them and classify them as either 'Safe' or 'Malicious'. You can also submit files you suspect of being 'false positives' (those files that you feel CIS has incorrectly identified as malware). Subsequent to classification, they will be added to the white or black list accordingly.

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

To open the 'Submit Files' interface, click 'Tasks' on the home screen followed by 'Advanced Tasks' > 'Submit Files'

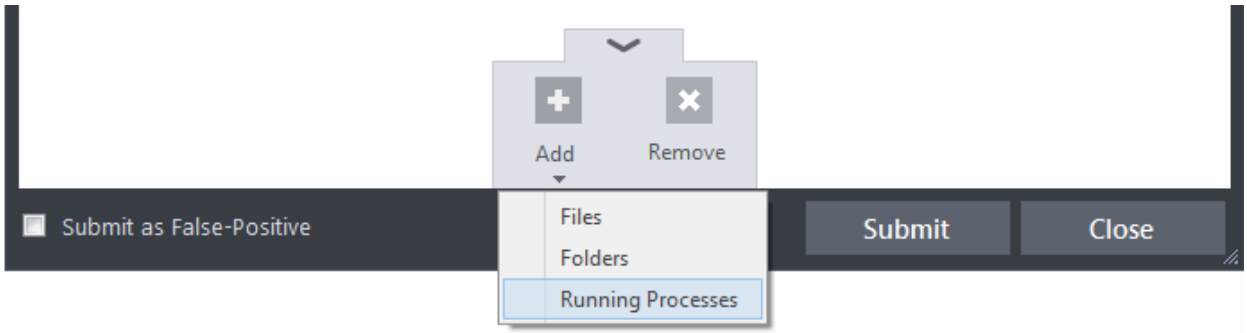


Clicking the handle at the bottom center of the panel opens the following options:

- **Add** - Allows you to add files to the 'Submit Files' list
- **Remove** - Allows you to remove files from the 'Submit Files' list

To add new file(s) to 'Submit Files' list

- Click the handle from the bottom center and choose 'Add'



You can add files to the Submit Files list by three ways:

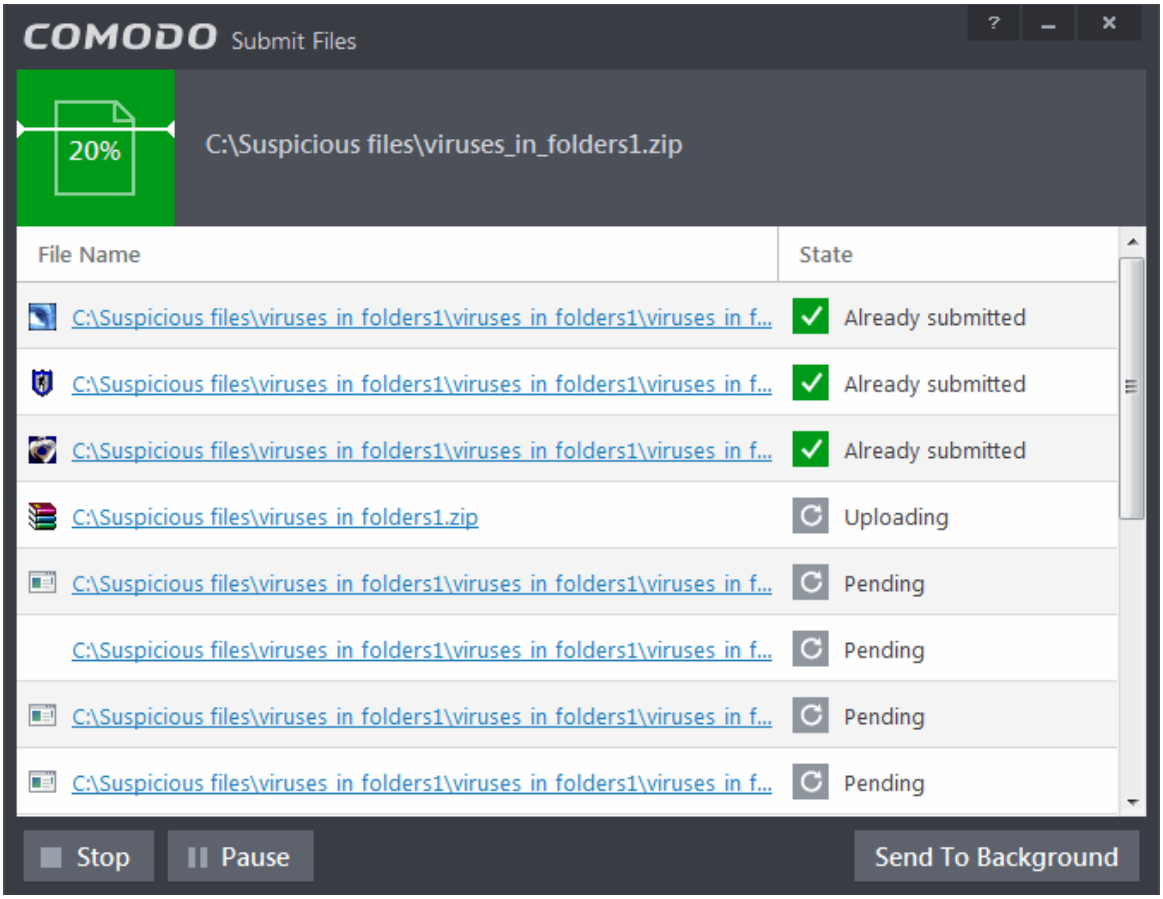
- **Files** - Allows you to navigate to the file or executable of the program you wish to add.
- **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'Trusted Files' list.
- **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'Trusted Files' list.
- Repeat the process to add more files and to submit them at-once.

To remove the files from 'Submit Files' list

- Select the file from the list
- Click the handle from the bottom center and select Remove

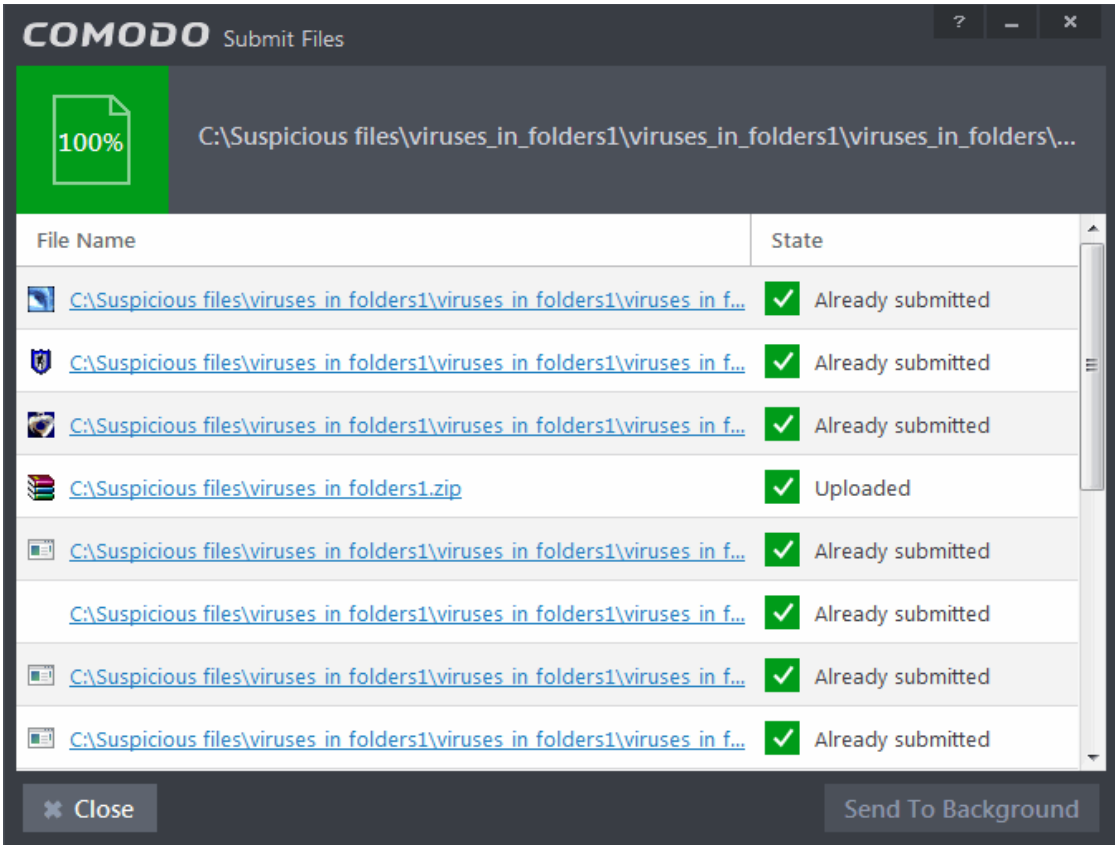
After adding the files you want to submit, click 'Submit' button. If you want to submit the files as False Positives to Comodo, select the 'Submit as False-Positive check' box.

The files will be submitted and the progress will be displayed



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

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen displays these results on completion.



- 'Uploaded' - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- 'Already submitted' - The file has *already* been submitted to our labs by another CIS user and was not uploaded from your machine at this time.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

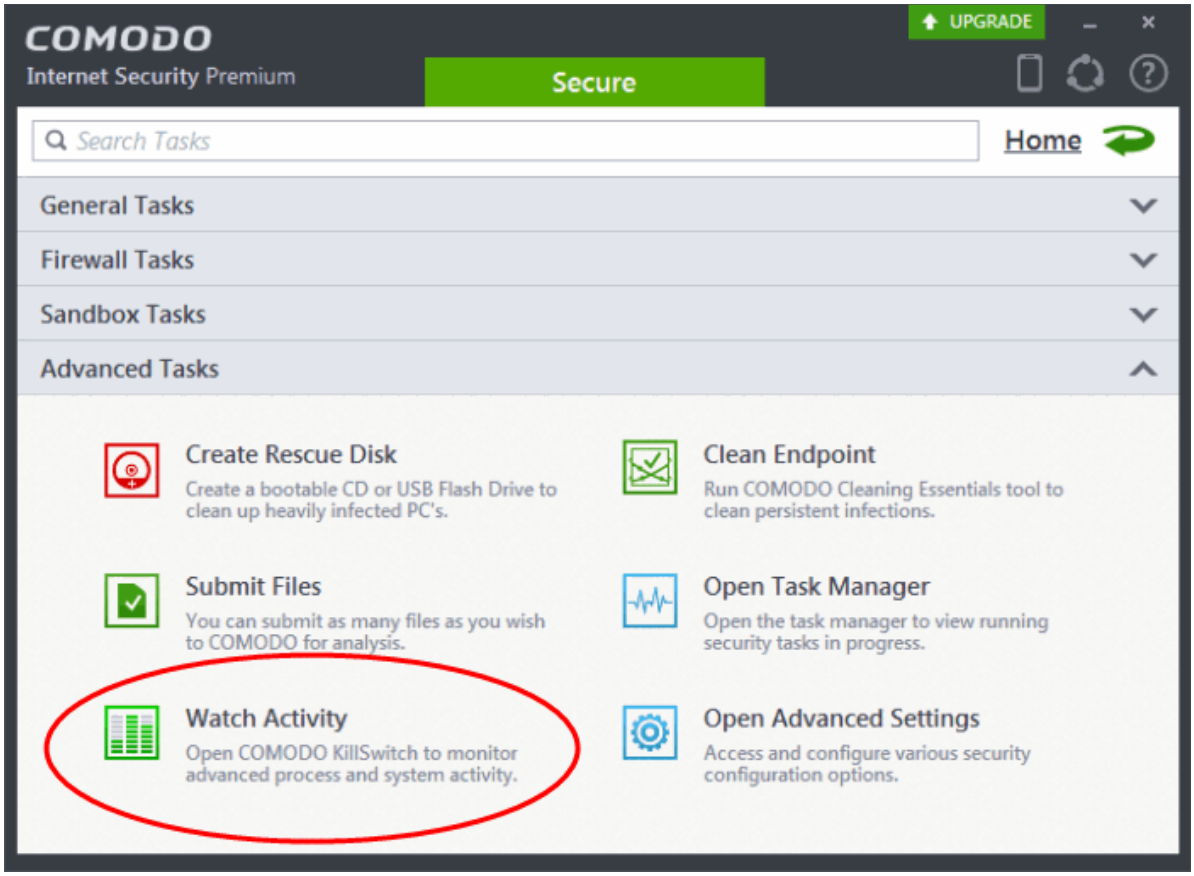
The list of files submitted from your computer can be viewed from the **Submitted Files** interface.

5.4. Identify and Kill Unsafe Running Processes

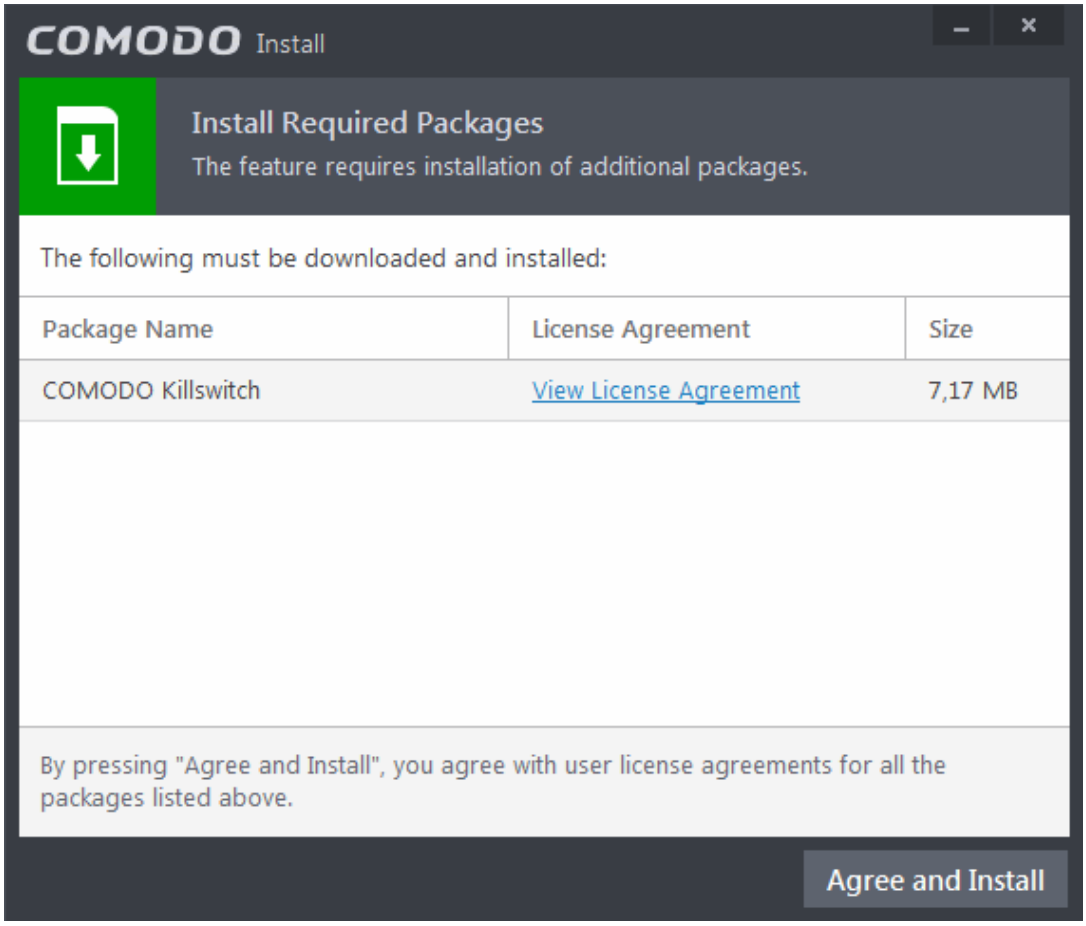
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer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

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

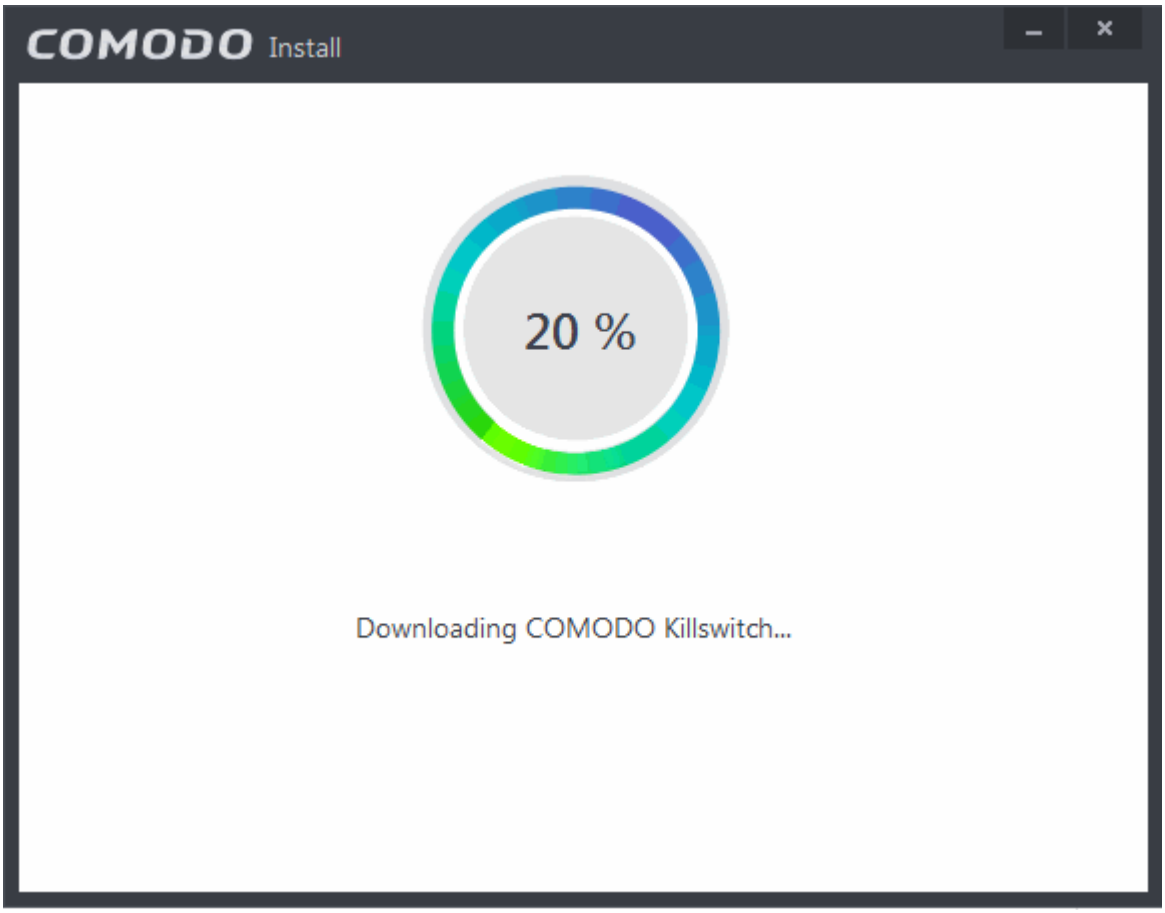
Comodo KillSwitch can be directly accessed from the CIS interface by clicking the 'Watch Activity' button in the 'Advanced Tasks' interface.



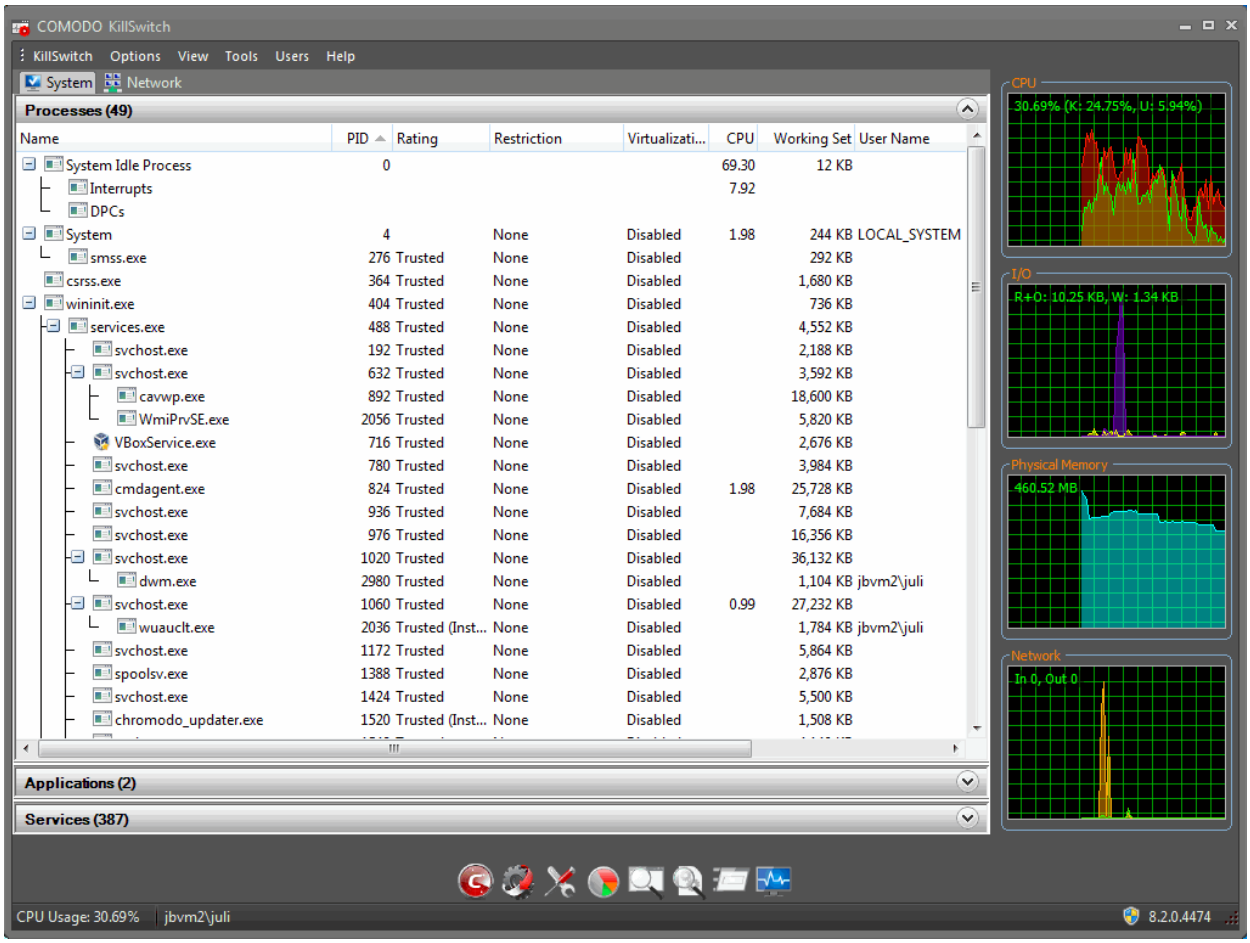
- Killswitch is a component of Comodo Cleaning Essentials. If you have already installed Comodo Cleaning Essentials by clicking 'Clean Endpoint' from the 'Advanced Tasks' interface, clicking the 'Watch Activity' will open the **KillSwitch interface** directly. Refer to the section **Remove Deeply Hidden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



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



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

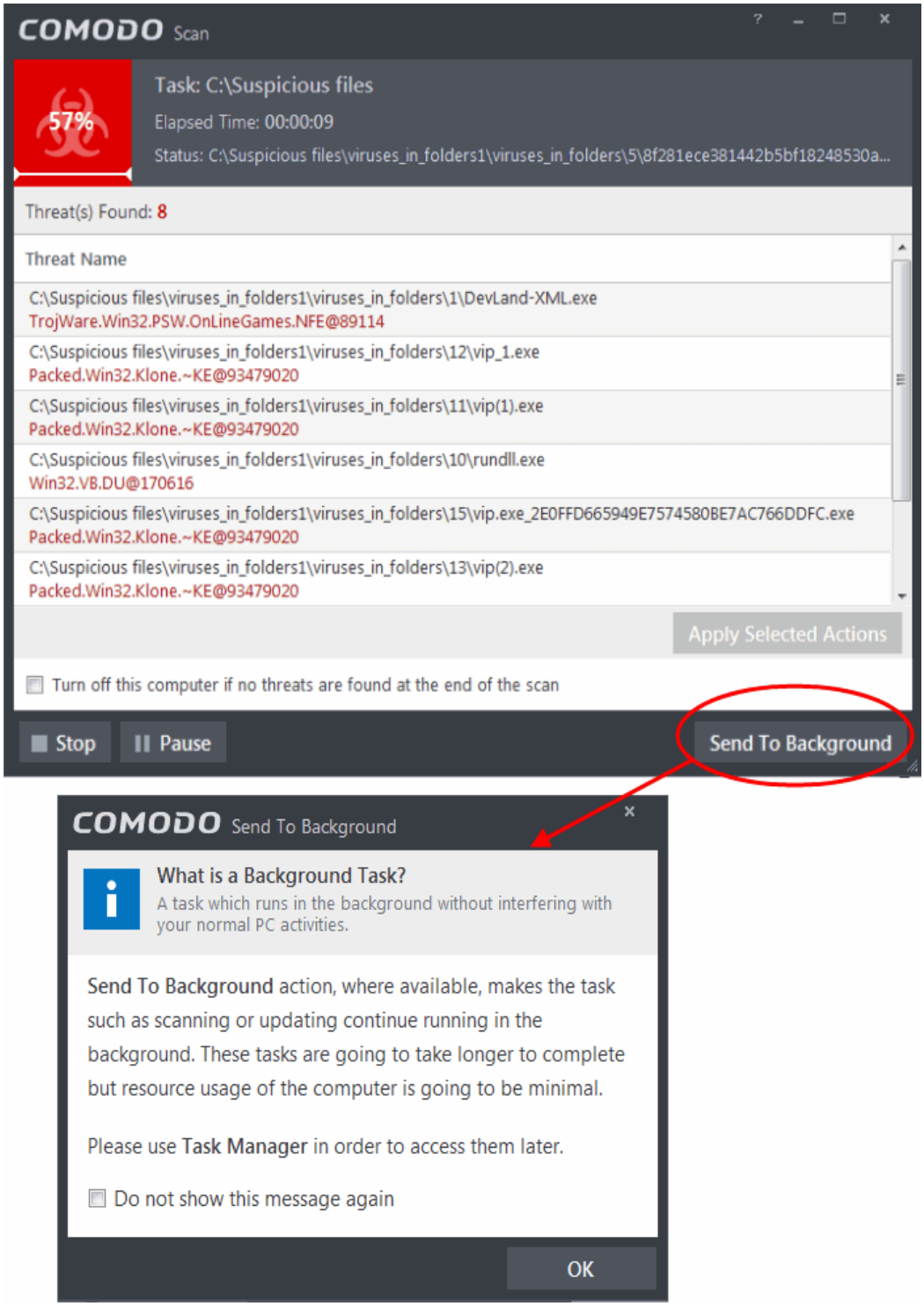


On clicking the 'Watch Activity' button from next time onwards, Comodo Killswitch will be opened.

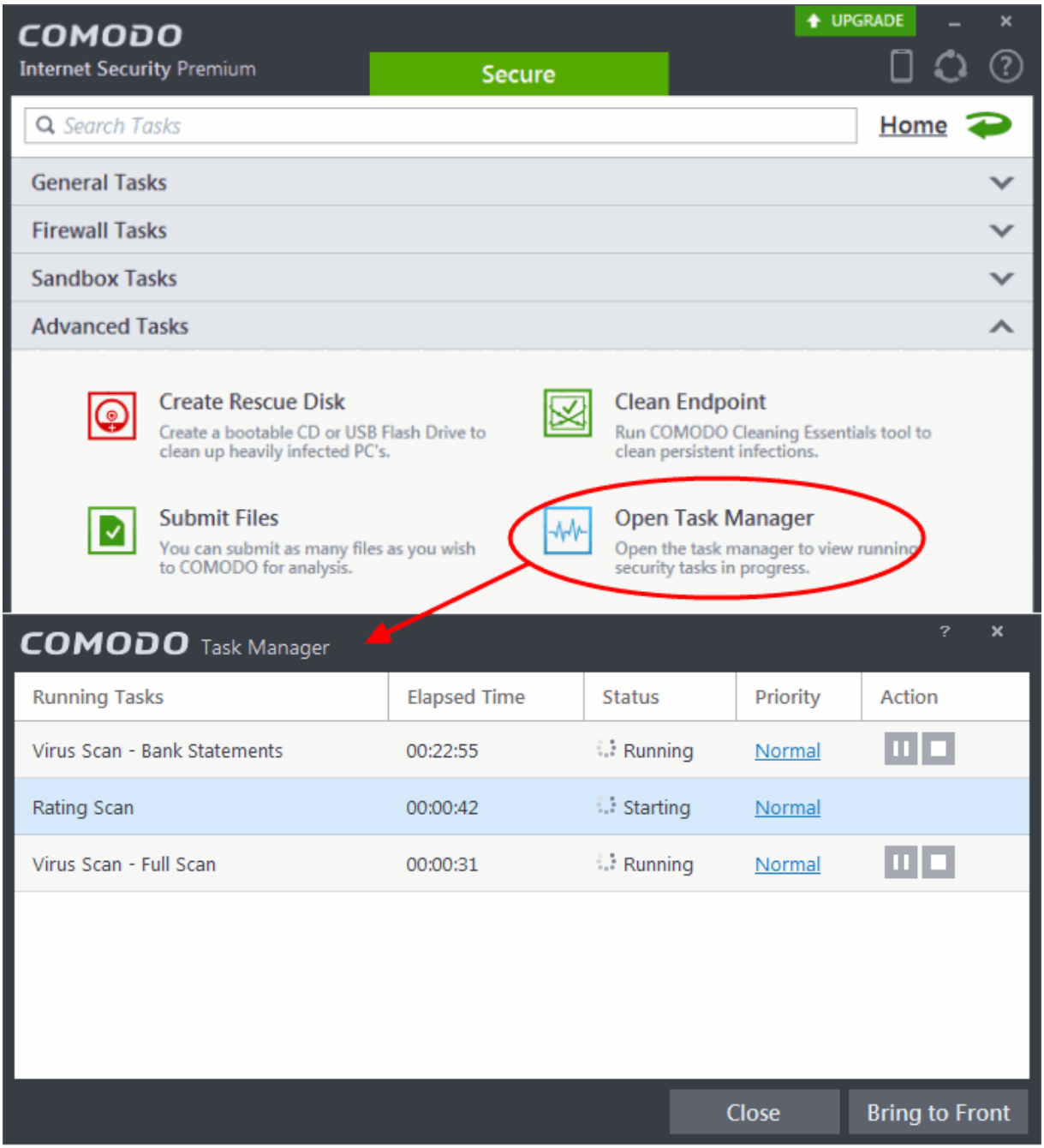
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at **http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html**

5.5. Manage CIS Tasks

Comodo Internet Security has the ability to concurrently run several tasks like on-demand or scheduled scans, virus signature database updates and so on. The tasks that are currently run, can be sent to background from the progress interface, by clicking Send to Background as shown in the example below.



These tasks can be managed, through the Task manager interface that can be accessed at anytime by clicking Open Task Manager from the 'Advanced Tasks' interface.



Tip: The Task Manager can also be opened by clicking on the center tab in the Status row of the **widget** , that displays the number of tasks that are currently running.

The Task Manager window displays a list of background tasks that are currently running with the details of time elapsed on each task, status and priority.

From the Task Manager interface, you can:

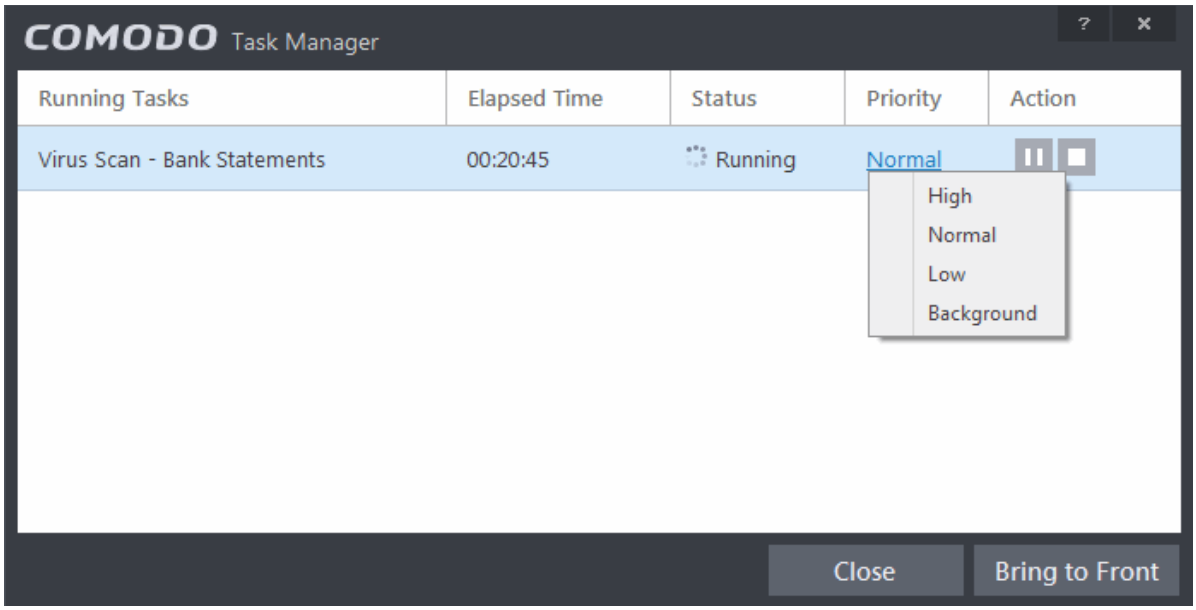
- **Reassign priorities to the tasks**
- **Pause/Resume or Stop a running task**
- **Bring a selected task to foreground**

Reassigning Priorities for a task:

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

To change the priority for a task

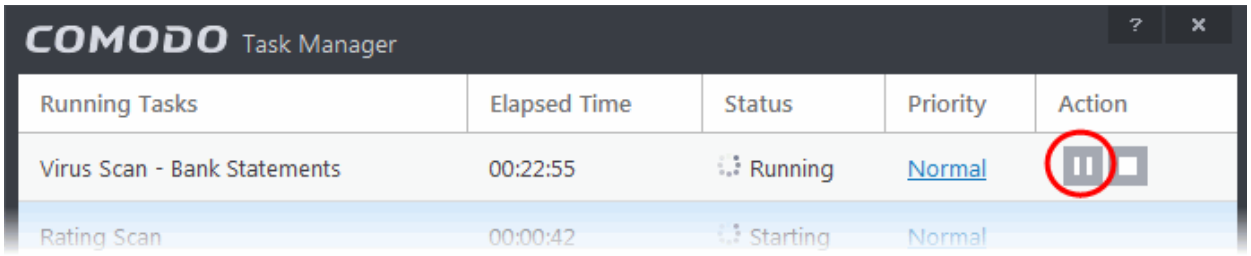
- Click on the current priority and select the priority you want to assign from the options.



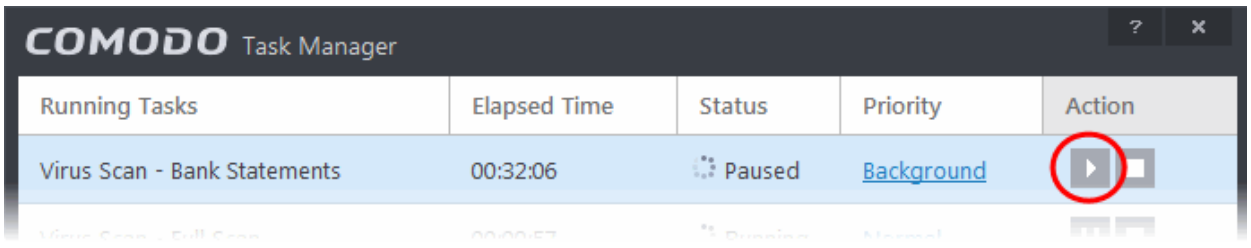
Pausing/Resuming or Stopping running tasks

The Action column displays the Pause/Resume and Stop buttons

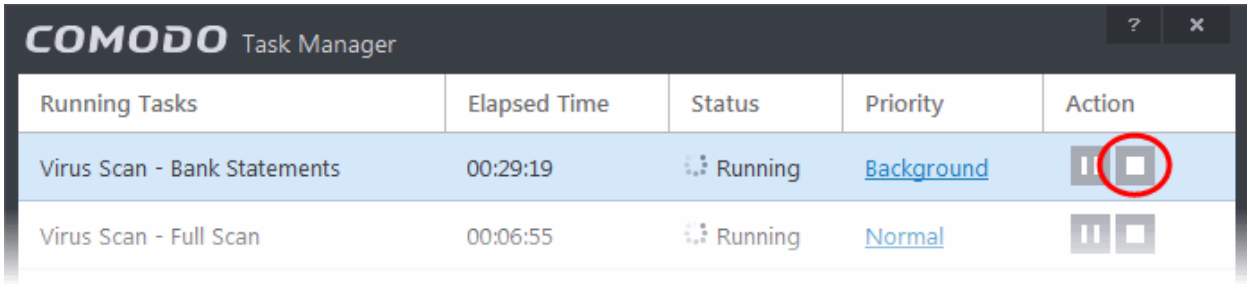
- To pause a running task, click the Pause button



- To resume a paused task, click the Resume button

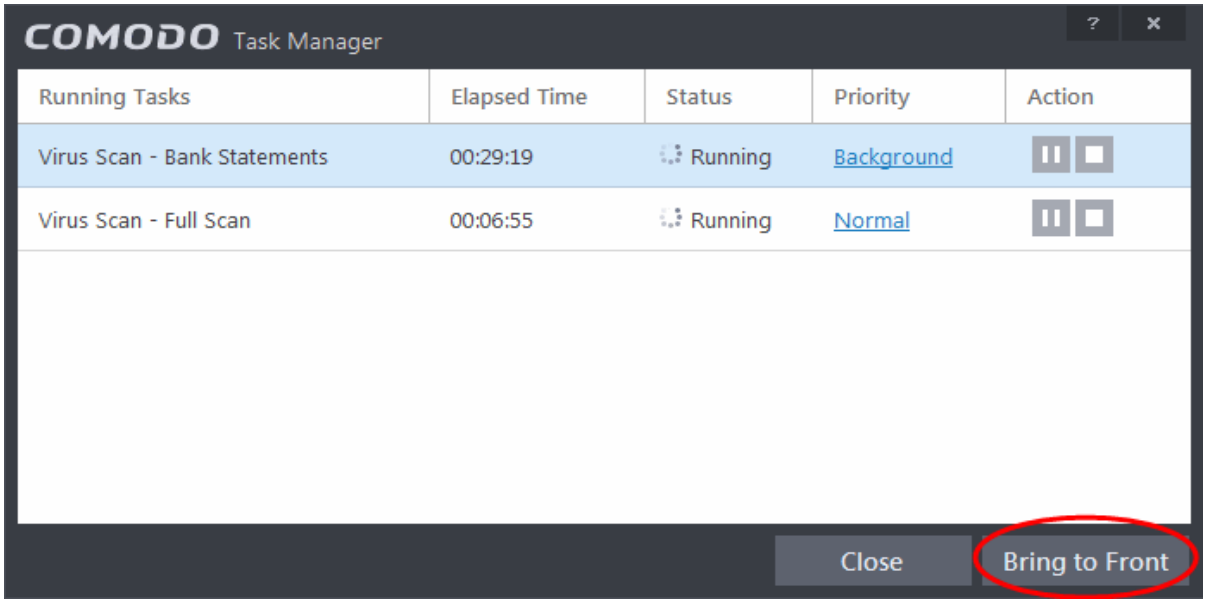


- To stop a running task, click the stop button

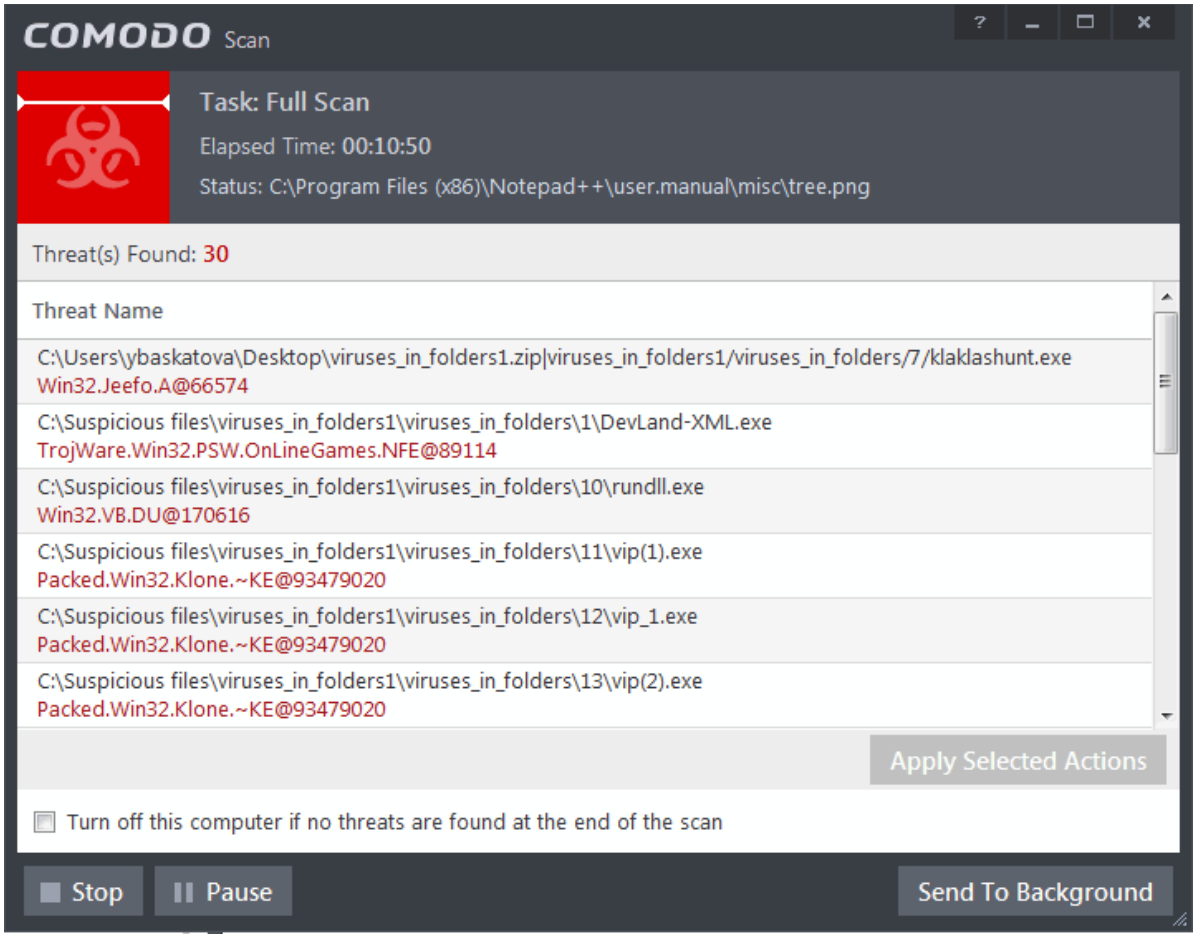


Bringing a running task to foreground

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



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

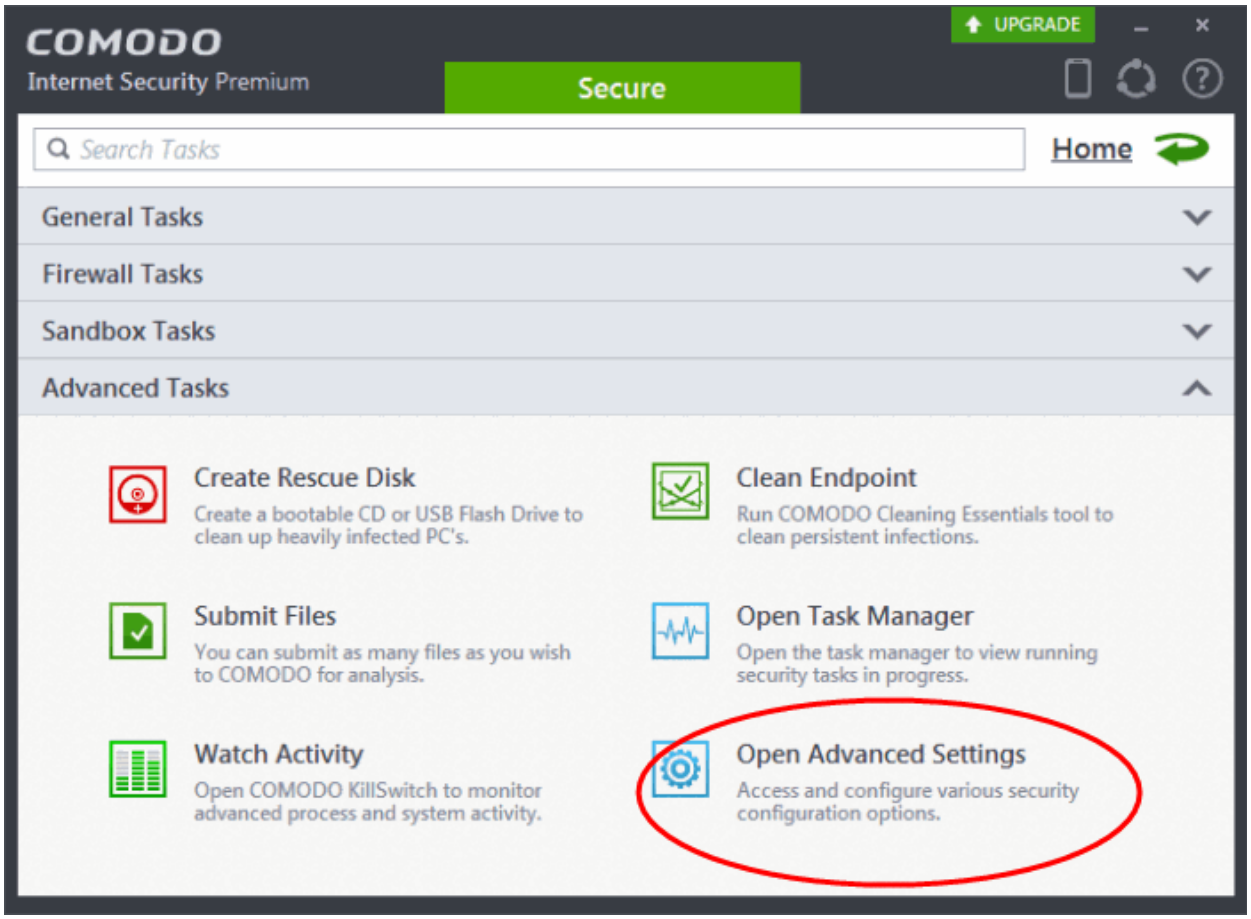


6.Advanced Settings

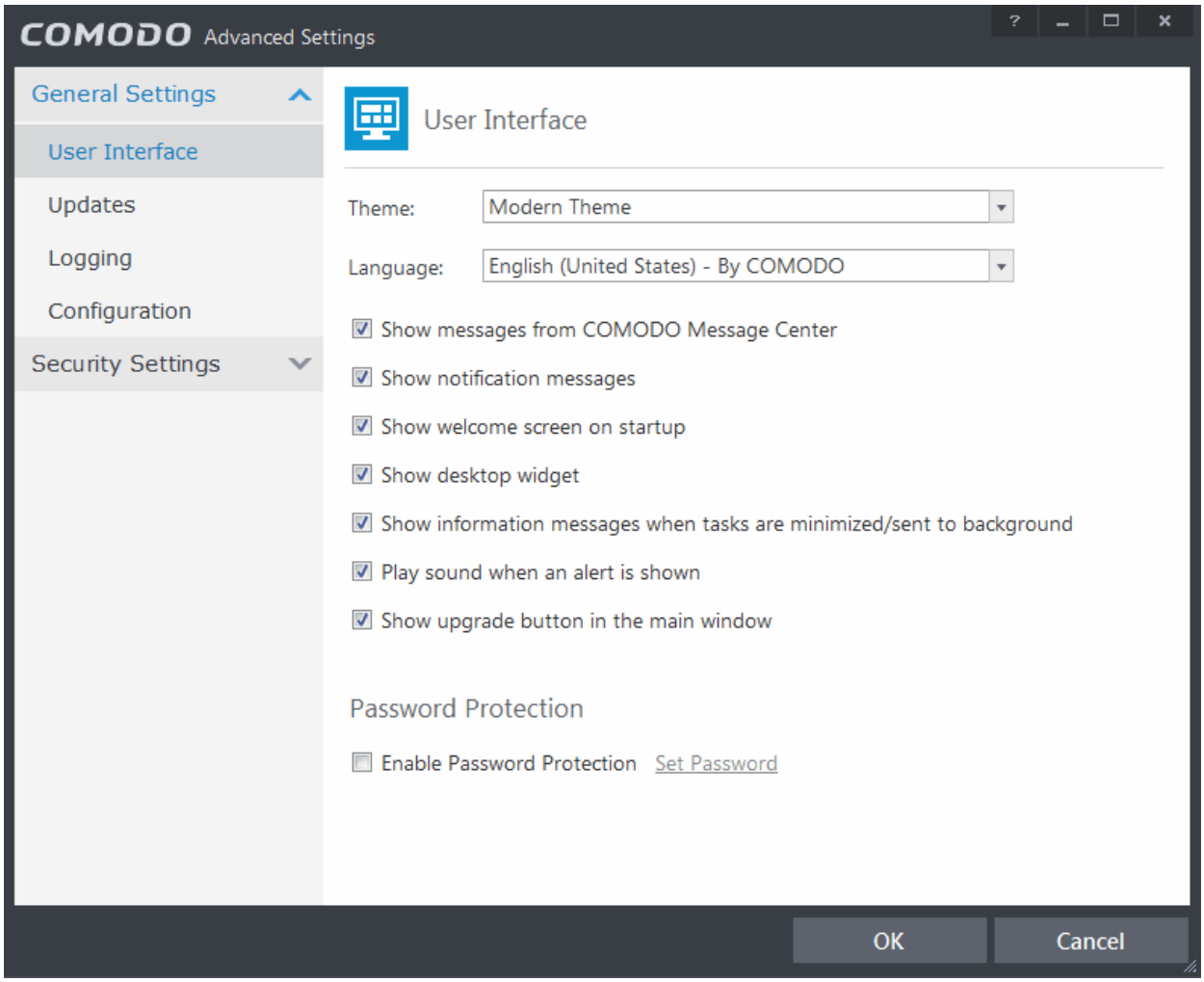
The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Internet Security. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced users delve into granular configuration of the Antivirus, Firewall, Defense+ and File Ratings modules. For example, the 'Security Settings' area allows you to create custom virus scan schedules, create virus exclusions, create Firewall and HIPS rules, modify sandbox behavior, define network zones and specify how the file rating system deals with trusted and untrusted files.

To open 'Advanced Settings':

- Click the 'Tasks' arrow if you are on the CIS home screen
- Click 'Advanced Tasks' then 'Open Advanced settings'



The 'Advanced Settings' panel will open:

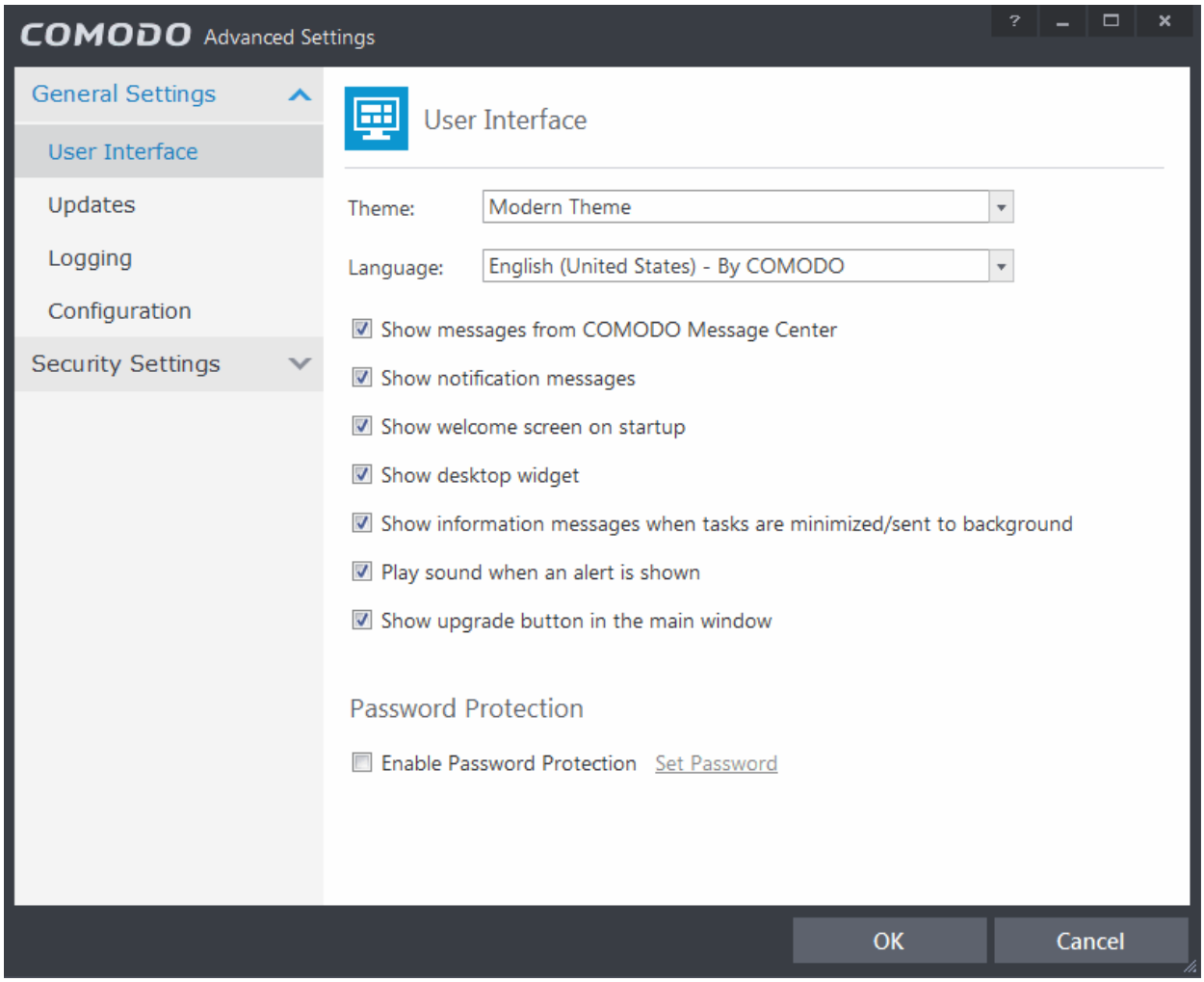


Please click the links below to find out more about each section:

- **General Settings** - Allows you to configure the appearance and behavior of the application
  - **Customize User Interface**
  - **Configure Program and database Updates**
  - **Log Settings**
  - **Manage CIS Configurations**
- **Security Settings** - Advanced configuration of Antivirus, Firewall, Defense+ and File Ratings modules
  - **Antivirus Settings**
  - **Defense+ Settings**
  - **Firewall Settings**
  - **File Ratings**

6.1. General Settings

The 'General Settings' area enables you to customize the appearance and overall behavior of Comodo Internet Security. You can configure general properties like the interface language, notification messages, automatic updates, logging and more.

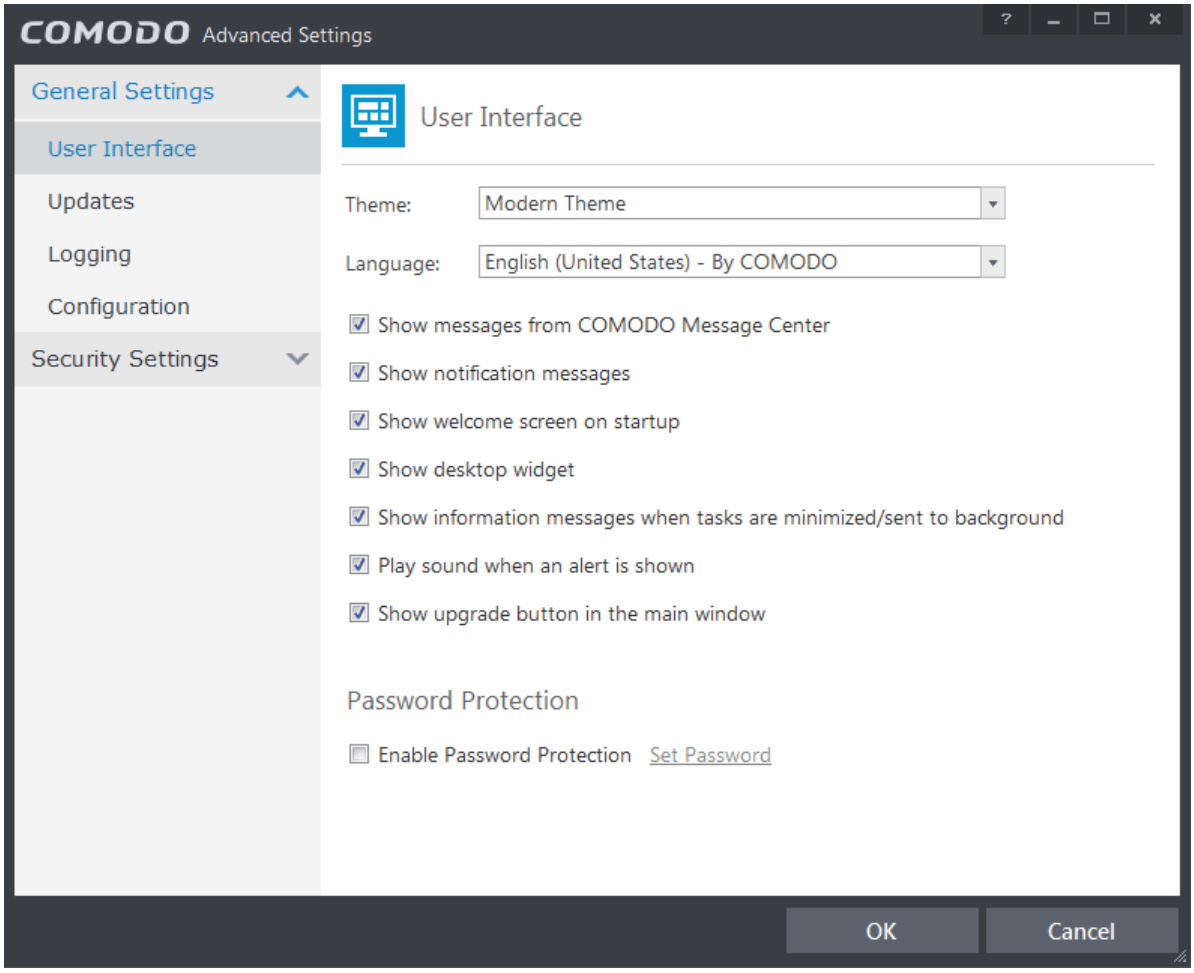


The category has the following settings:

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

6.1.1. Customize User Interface

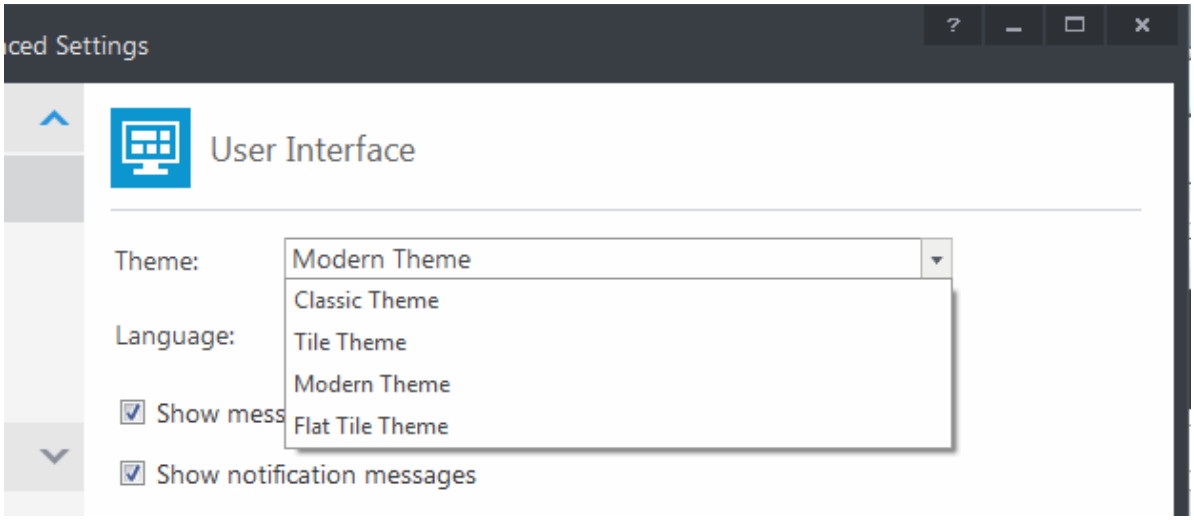
The 'User Interface' tab lets you choose the display theme, interface language and customize the look and feel of Comodo Internet Security according to your preferences. You can also configure how messages are displayed and enable password protection for your settings.



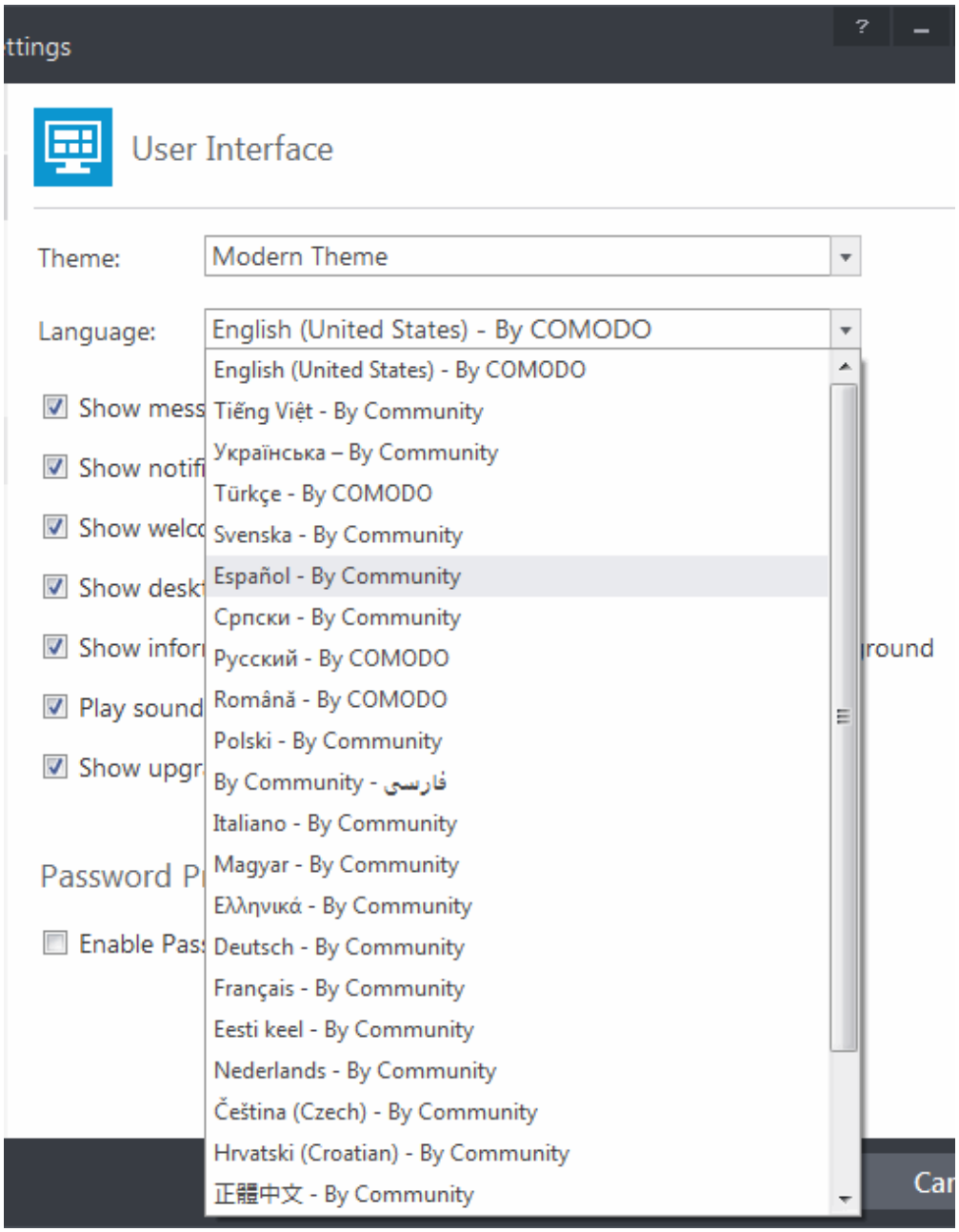
The User Interface Settings allows you configure the following:

- **Themes**
- **Language**
- **Show messages from COMODO Message Center**
- **Show notification messages**
- **Show Welcome screen on start up**
- **Show desktop widget**
- **Show information messages when tasks are minimized/sent to background**
- **Play sound when an alert is shown**
- **Show upgrade button in the main window**
- **Enable Password Protection**

- **Theme -** The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (***Default = Tile Theme***).



- **Language Settings** - Comodo Internet Security is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (***Default = English (United States)***).



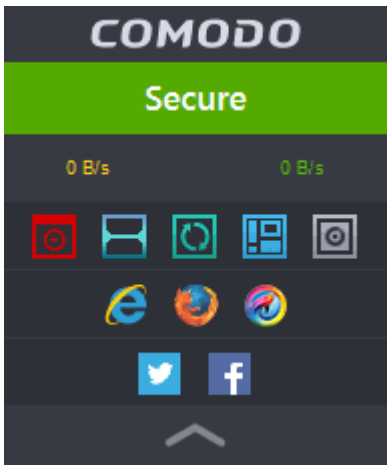
- **Show messages from COMODO Message Center** - If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world.

They contain news about product updates, occasional requests for feedback, info about other Comodo products you may be interested to try and other general news. (***Default = Enabled***).

- **Show notification messages** - These are the CIS system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CIS is taking and any CIS status updates. For example ' Comodo Firewall is learning ' or 'Defense+ is learning ' are generated when these modules are learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in **Antivirus > Real-time Scan settings** screen. Clear this check box if you do not want to see these system messages (***Default = Enabled***).
- **Show Welcome Screen on start up** - If enabled, CIS will display a welcome screen when the application first starts . (***Default = Enabled***):

Tip: You can disable the Welcome Screen by selecting the checkbox 'Do not show this window again' in the window itself.

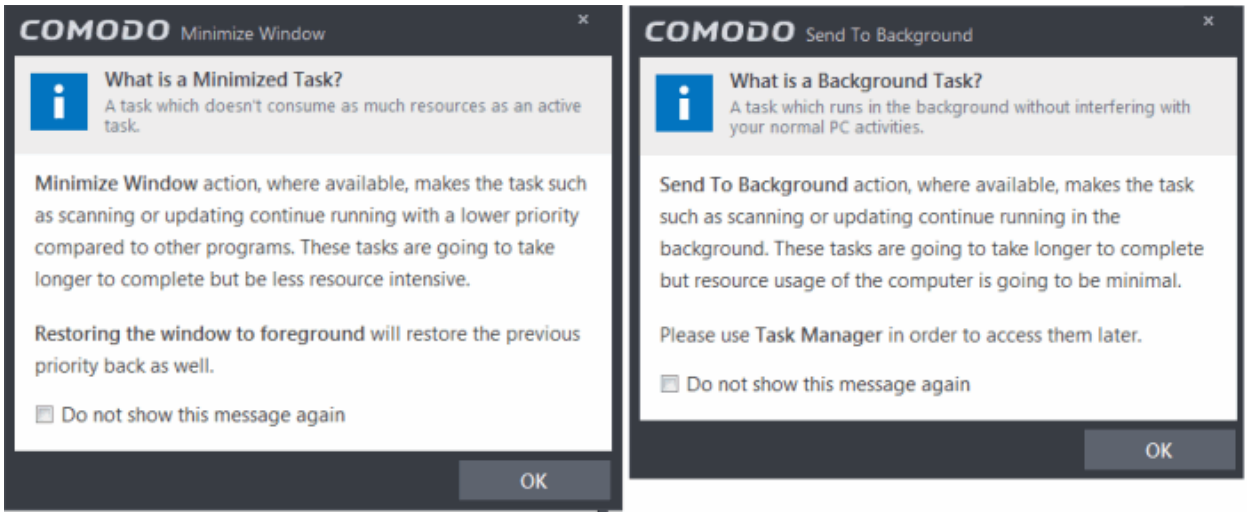
- **Show desktop widget** - The CIS desktop widget displays at-a-glance information about CIS security status, speed of outgoing and incoming traffic, number of background tasks and links to social networking sites.



The widget also acts as a shortcut to open the CIS main interface, the Task Manager, your browsers and so on. If you do not want the widget to be displayed on your desktop, clear this checkbox. (***Default = Enabled***).

Tip: You can disable the widget from the CIS system tray icon. Right click on the CIS system tray icon and deselect the 'Show' option that appears on hovering the mouse cursor on 'Widget'.

- **Show information messages when tasks are minimized/sent to background** - CIS displays messages explaining the effects of minimizing or moving a running task like an AV scan to the background:



If you do not want these messages to be displayed, clear this check-box (***Default = Enabled***).

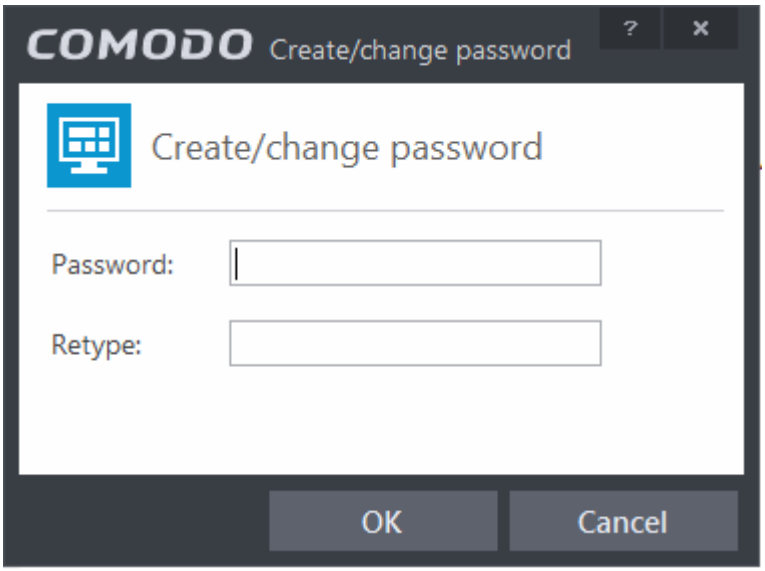
Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **Play sound when an alert is shown** - CIS generates a chime whenever it raises a security alert to grab your attention. If you do not want the sound to be generated, clear this check box (***Default = Enabled***).
- **Show upgrade button in the main window** - If enabled, CIS will display the green upgrade button at the top right of the interface (***Default = Enabled***).
- **Enable Password Protection** - Enforces password protection for all important configuration sections and wizards within the interface. If you enable this feature, you must first specify and confirm a password by clicking the 'Set Password' link. You will then be asked for this password whenever you try to access important configuration areas (for example, all sections in the **General Tasks**, **Firewall Tasks**, **Sandbox Tasks** and **Advanced Tasks** will request the password).

This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and exposing the machine to threats (***Default = Disabled***).

To enable password protection

- Select the 'Enable Password Protection' check-box then click 'Set Password'. The Change password dialog will appear.

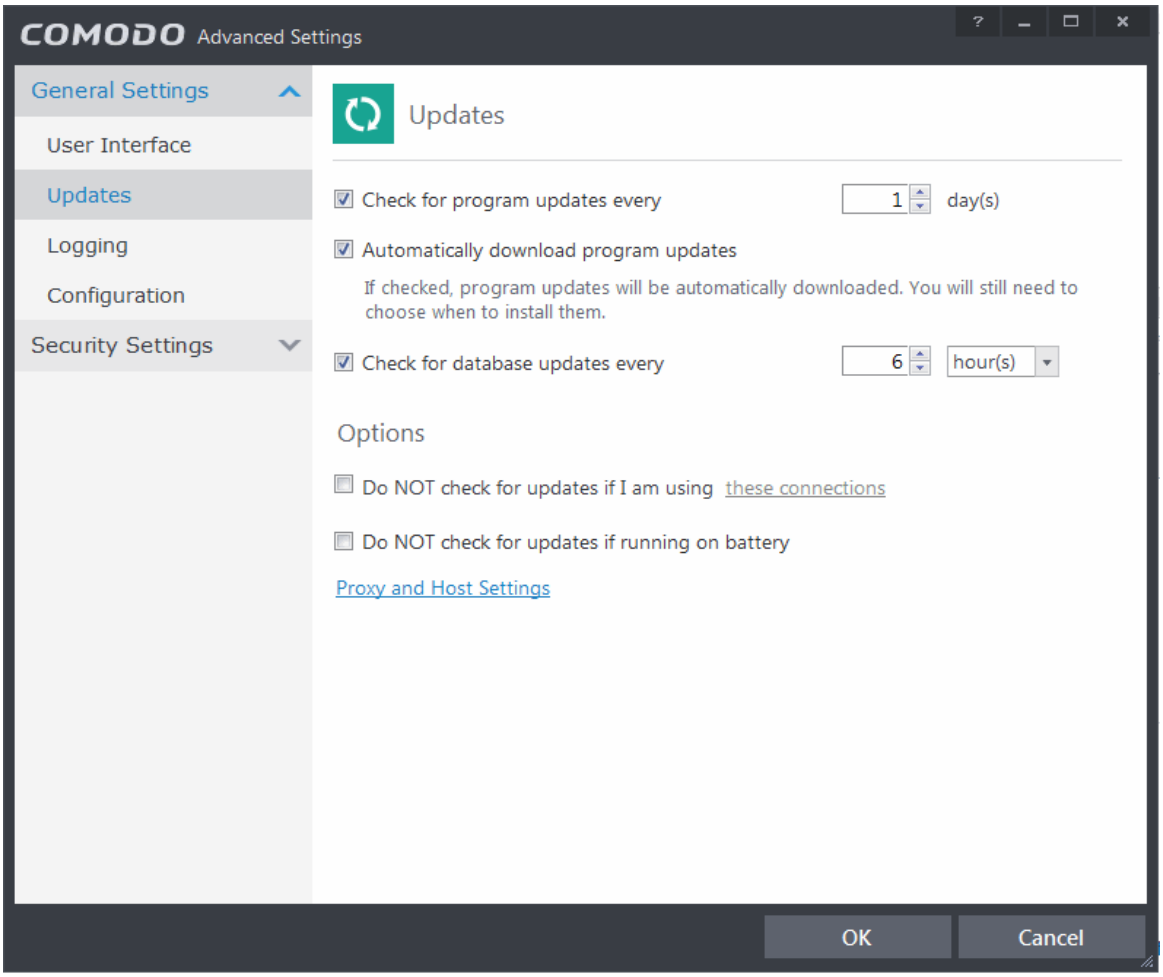


- Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

6.1.2. Configure Program and Virus Database Updates

The 'Updates' area allows you to configure settings that govern CIS program and virus database updates.

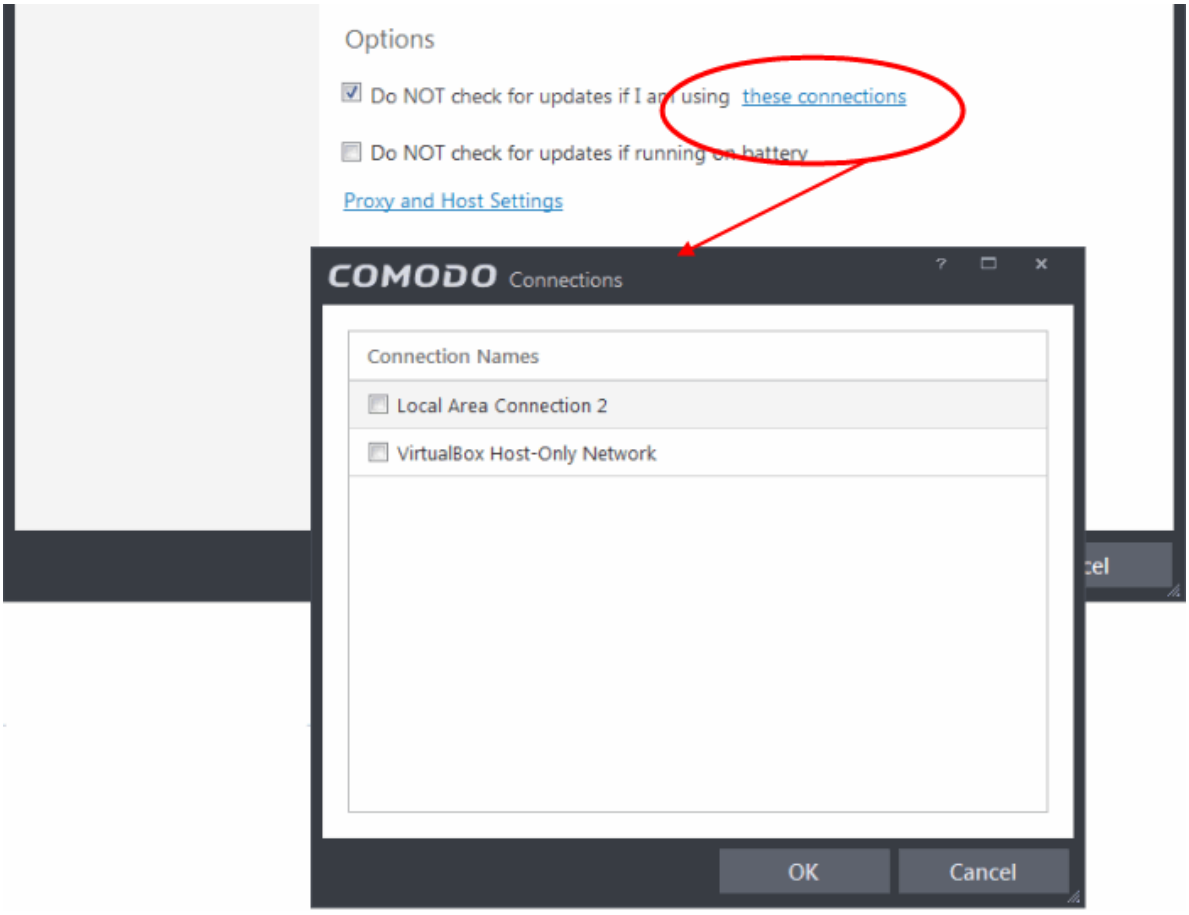
This screen can be accessed by clicking 'Updates' under the 'General Settings' section of 'Advanced Settings':



- **Check program updates every NN day(s)** - Enables you to set the interval at which CIS will check for program updates. Select the interval in days from the drop-down combo box. ***(Default = 1 day)***
- **Automatically download program updates** - Instructs CIS to automatically download program updates as soon as they are available. ***(Default=Enabled)***
- **Check for database updates every NN hour(s)/day(s)** - Enables you to set the interval at which CIS will check for virus signature database updates. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 6 hours)***
- **Do NOT check updates if am using these connections** - Enables you to restrict CIS from checking for updates if you use certain types of Internet connection. For example, you may not wish to check updates if using a wireless connection you know to be slow or not secure ***(Default = Disabled)***

  To do this:

  - Select the 'Do NOT check updates if am using these connections' check-box
  - Then click the 'these connections'. The connections dialog will appear with the list of connections you use.



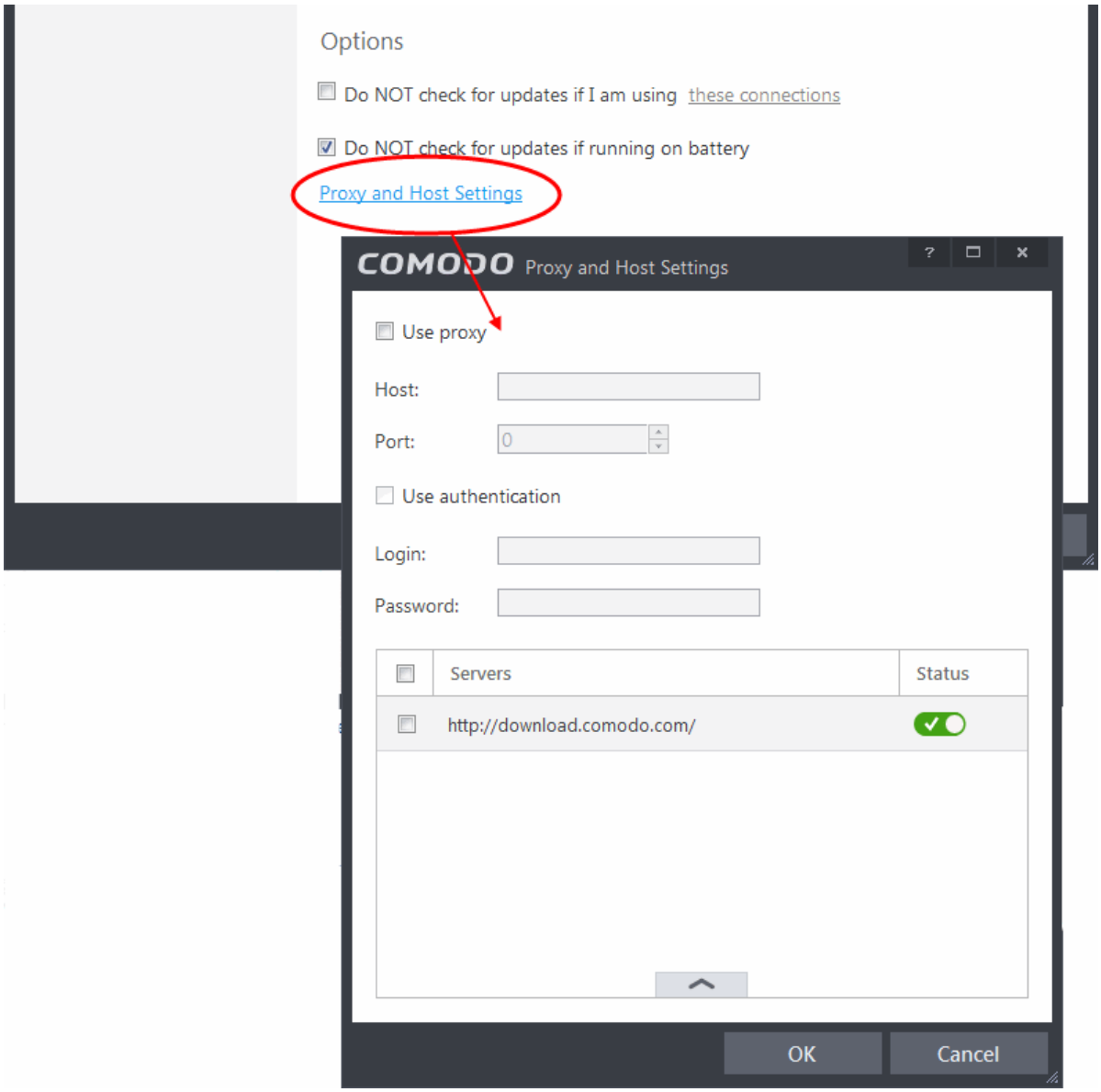
- Select the connection through which you do not want CIS to check for updates and click OK.

- **Do NOT check for updates if running on battery** - If enabled, CIS will not download updates if it detects your computer is running from battery power. This is intended to extend battery lifetime on laptops. ***(Default = Enabled)***
- **Proxy and Host Settings** - Allows you to select the host from which updates are downloaded. By default, CIS will directly download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CIS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CIS at this proxy/staging server. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

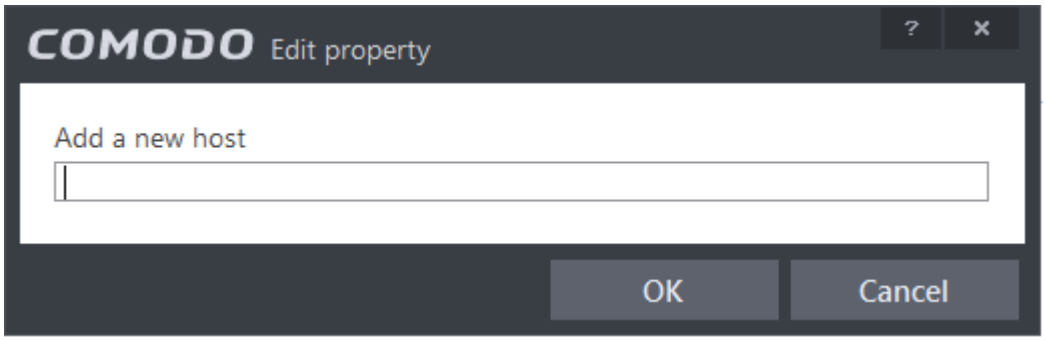
Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from **http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php**

To configure updates via proxy server

- Click 'Proxy and Host Settings' at the bottom of the 'Updates' interface. The 'Proxy and Host Settings' interface will open.



- Select the 'Use Proxy' check-box.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- You can add multiple servers from which updates are available. To do this, click the handle at the bottom center of the 'Servers' panel, click the 'Add' button then enter the host name in the 'Edit Property' dialog.



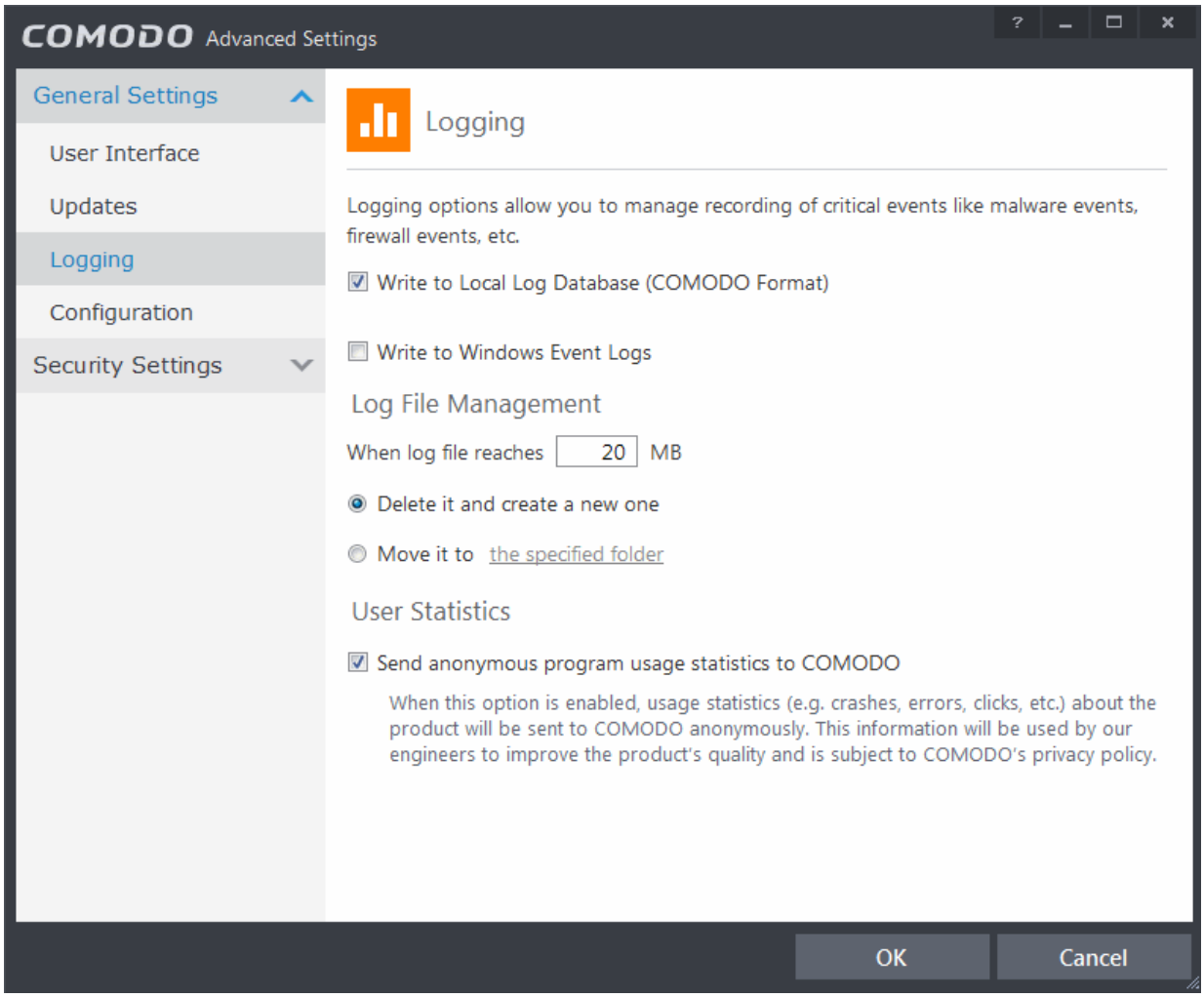
- If you specify multiple servers:
  - Activate or deactivate each update server using the 'Active' toggle switch alongside it
  - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CIS will commence downloading from the first server that contains new updates.

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

6.1.3. Log Settings

By default, Comodo Internet Security maintains detailed logs of all Antivirus, Firewall and Defense+ events. Logs are also created for 'Alerts Displayed', 'Tasks Launched' and 'Configuration Changes'.

- This 'Logging' interface allows you to specify whether you want to enable logging; the maximum size of the log file and how CIS should react if the maximum file size is exceeded.
- Note: If you wish to actually view, manage and export logs, then you need to open the '**View Logs**' interface under 'General Settings' (Tasks > General Settings > View Logs)



Logging Options

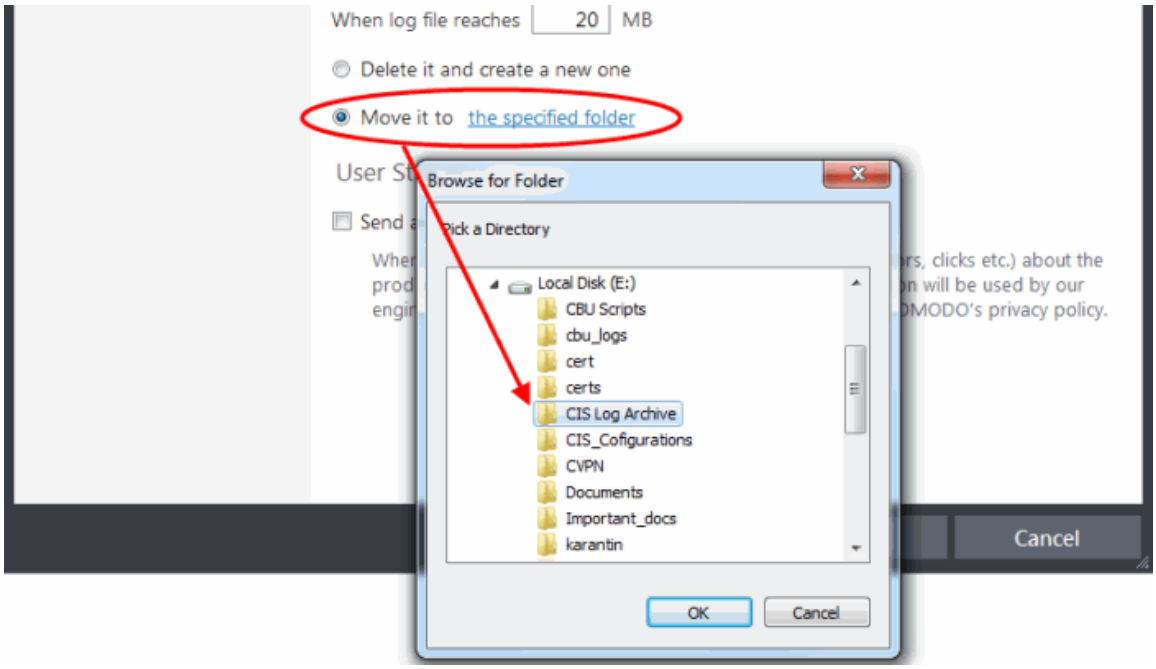
- **Write to Local Log Database (COMODO Format)** - CIS logs events in Comodo format and the log storage depends on settings done in Log File Management section below. ***(Default = Enabled***)
- **Write to Windows Event Logs** - CIS log events are written to Windows Event Logs. ***(Default = Disabled)***

Log File Management

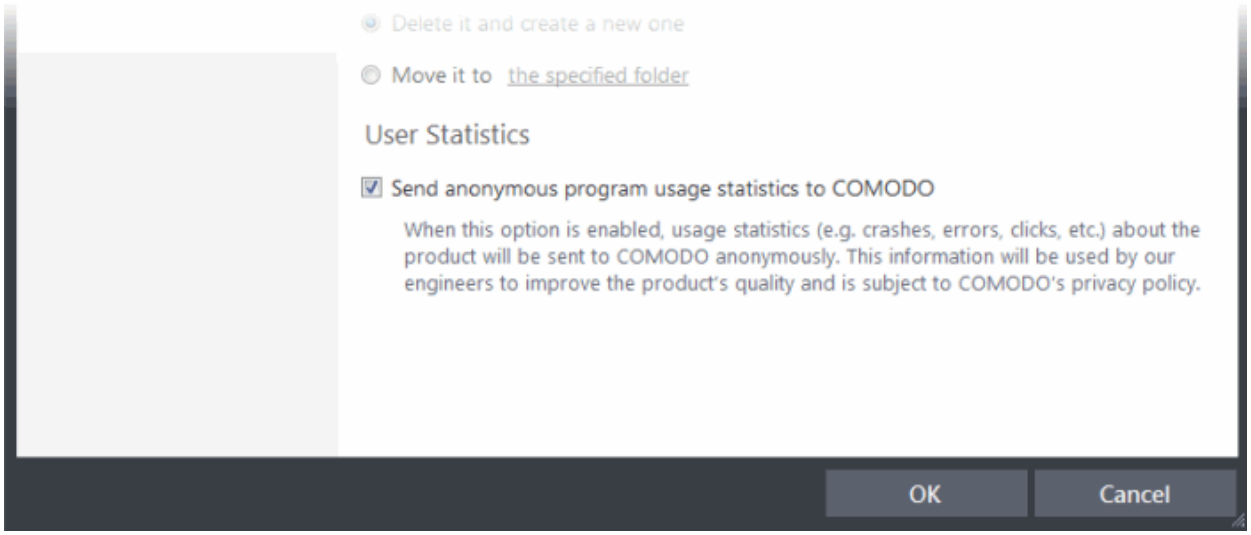
- **When log file reaches (Mb(s))** - Enables you to specify behavior when the log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.
    - Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' ***(Default = 20MB).***

  If you want to discard the log file if it reaches the maximum size, select **'Delete it and create a new one'.** Once the log file reaches the specified maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant ***(Default = Enabled).***

If you want to save the log file even if it reaches the maximum size, select **'Move it to'** and select a destination folder for the log file ***(Default = Disabled).***



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



Once the log file reaches the maximum size, it will be automatically moved to the selected folder and a new log file will be created with the log of events occurring from that instant.

User Statistics

- **Send anonymous program usage statistics to COMODO** - Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS instillation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. ***(Default = Enabled).***

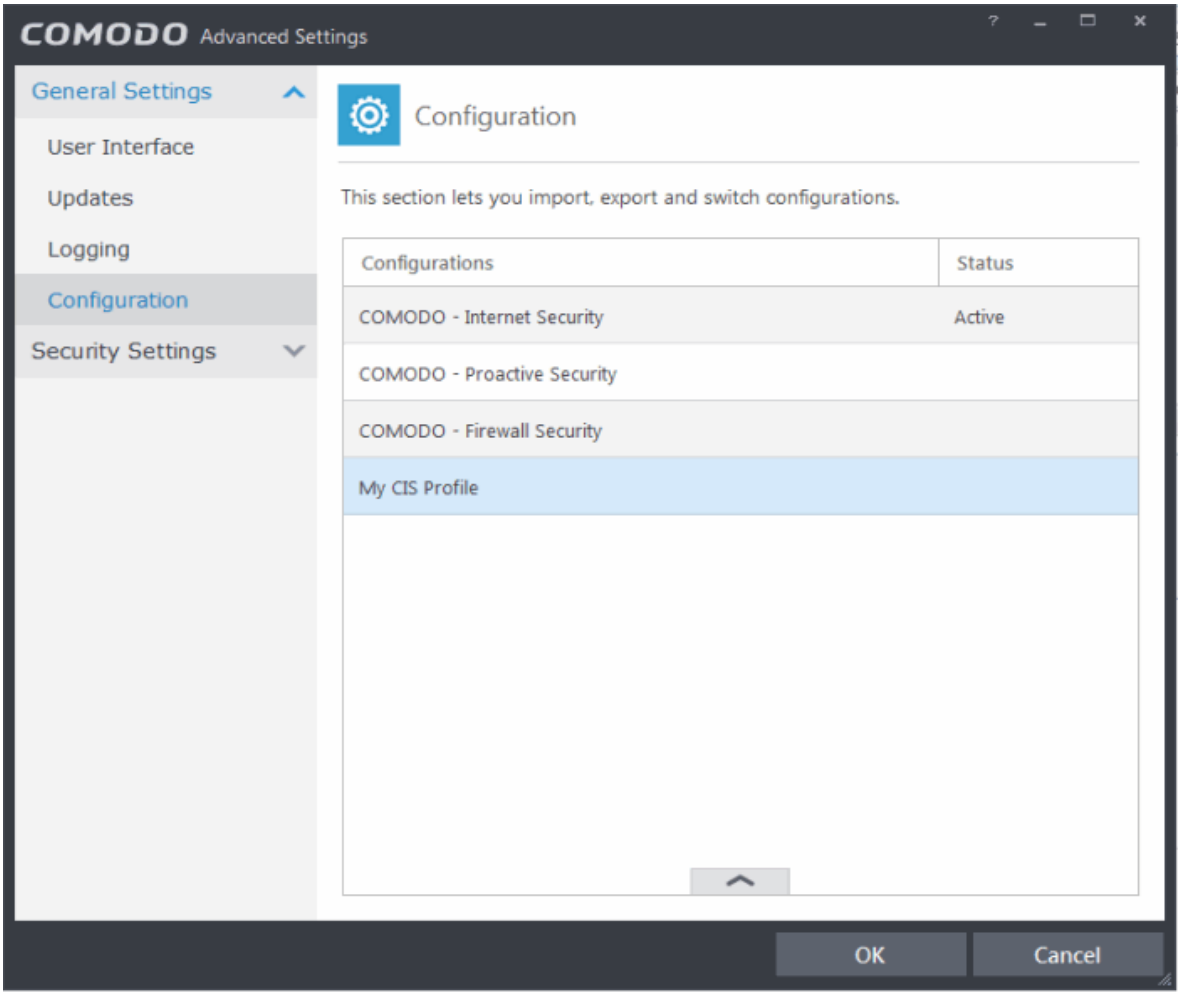
6.1.4. Manage CIS Configurations

Comodo Internet Security allows you to maintain, save and export multiple configurations of your security settings as configuration profiles. This is especially useful if you are a network administrator looking to roll out a standard security

configuration across multiple computers. If you are upgrading your system and there is a need to uninstall and re-install Comodo Internet Security then it can be great time-saver to export your configuration settings beforehand. After re-installation, you can import your previous settings and avoid having to configure everything over again.

Note: Any changes you make over time will be automatically stored in the currently active profile. If you want to export your current settings then export the 'Active' profile.

This panel can be accessed by clicking 'Configuration' under the 'General Settings' section of 'Advanced Settings':



The currently active configuration is indicated under the 'Active' column. Click the following links for more details:

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

6.1.4.1. Comodo Preset Configurations

By default, CIS is installed with 'COMODO - Internet Security' as the active configuration. Reminder - the active profile is, in effect, your current CIS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time from the 'Configuration' panel.

Click the links below to find out more details on each configuration:

- **COMODO - Internet Security**
- **COMODO - Proactive Security**
- **COMODO - Firewall Security**

COMODO - Internet Security - This configuration is activated by default, when both Antivirus and Firewall components are installed (i.e. the complete installation). The firewall is always set to 'Safe mode' but, according to the results of the malware scan performed during the setup process, the HIPS setting may vary. If no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is 'Safe Mode'.

- Behavior Blocker is Enabled.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Defense+ is tuned to prevent infection of the system.

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

COMODO - Proactive Security - This configuration turns CIS into the ultimate protection machine. All possible protections are activated and all critical COM interfaces and files are protected. During the setup, if only Comodo Firewall installation option is selected, the next screen allows users to select this configuration as default CIS configuration. If selected, Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

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

COMODO - Firewall Security - This configuration is activated when the user chooses to install Firewall only and selects optimum protection settings for HIPS. Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

- Behavior Blocker is disabled.
- Computer Monitor and Keyboard are NOT monitored.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- HIPS is tuned to prevent infection of the system and detect Internet access request leaks even if it is infected.

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

6.1.4.2. Importing/Exporting and Managing Personal Configurations

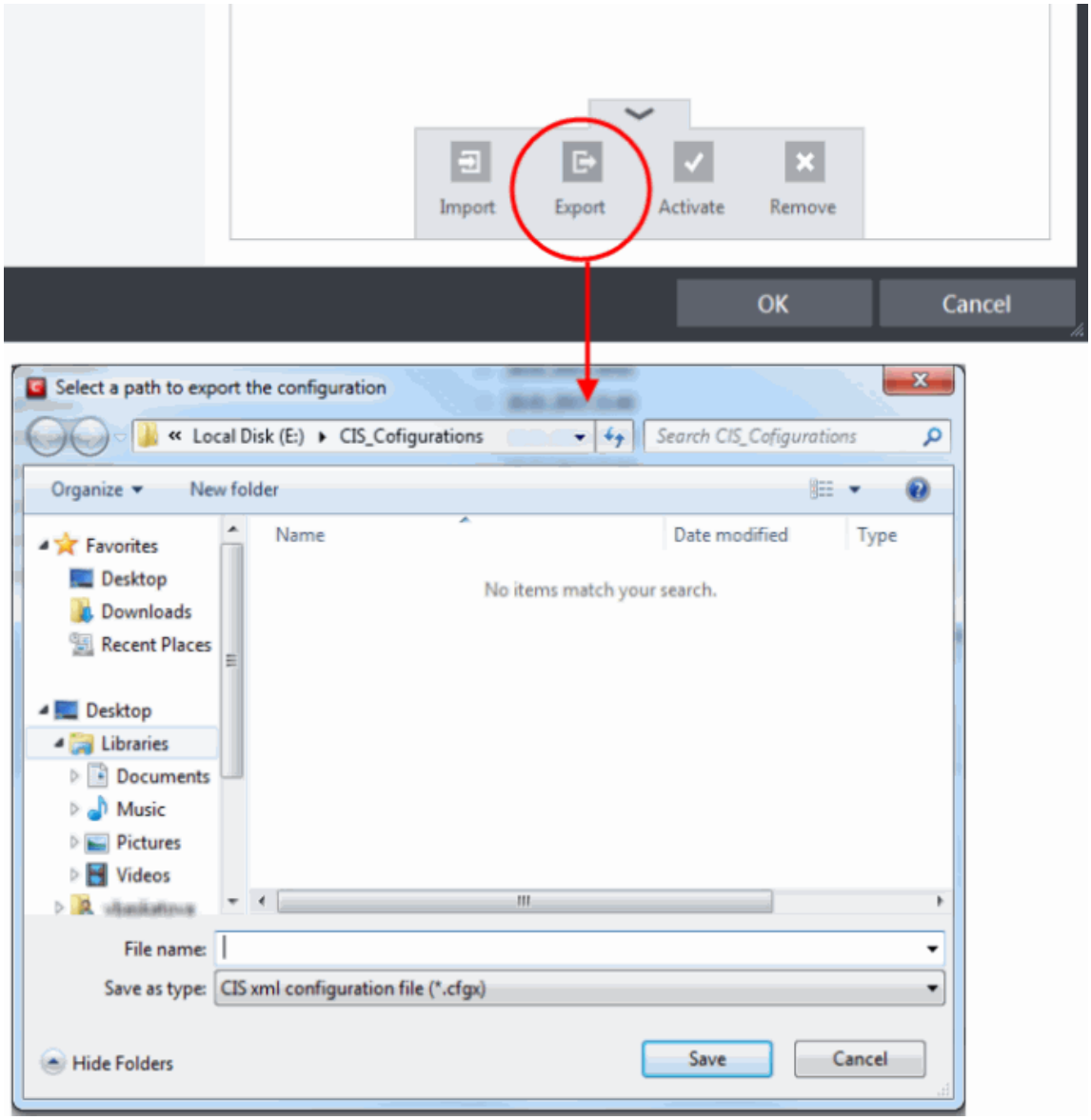
The CIS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Configuration' tab under 'General Settings' in 'Advanced Settings' interface.

Click the area on which you would like more information:

- **Export a stored configuration to a file**
- **Import a saved configuration from a file**
- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

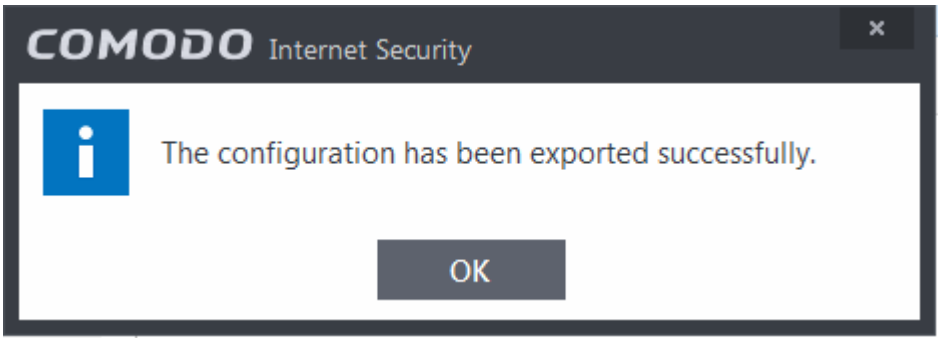
Exporting a stored configuration to a file

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration, click the handle at the foot of the interface and choose 'Export'. The 'Select a path to export the configuration' dialog will open.



3. Navigate to the location where you want to save the configuration file, type a name (e.g., 'My CIS Profile') for the file to be saved in .cfgx format and click 'Save'.

A confirmation dialog will appear on successful export of the configuration.

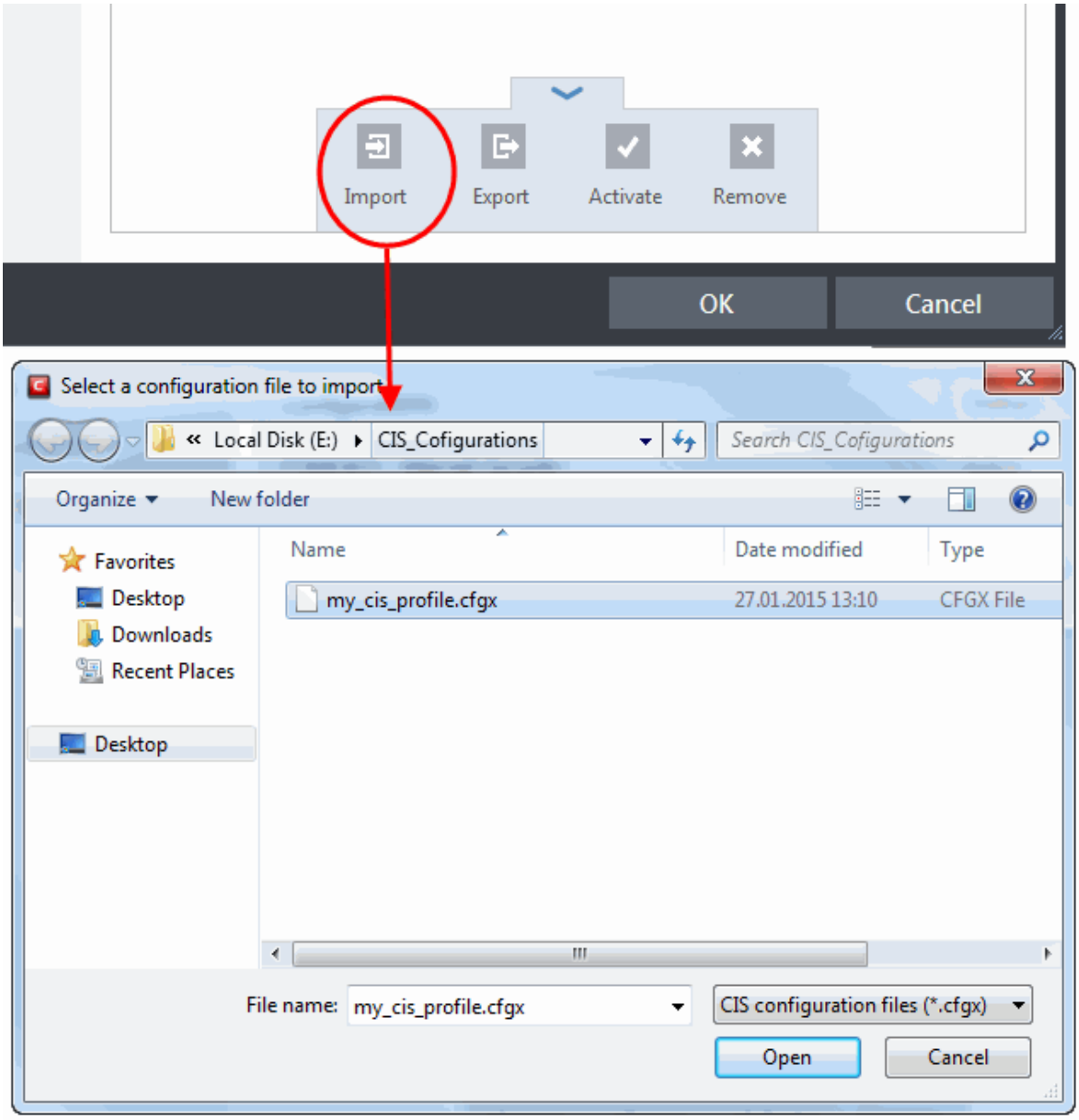


Importing a saved configuration from a file

Importing a configuration profile allows you to store any profile within Comodo Internet Security. Any profiles you import do not become active until you **select them for use**.

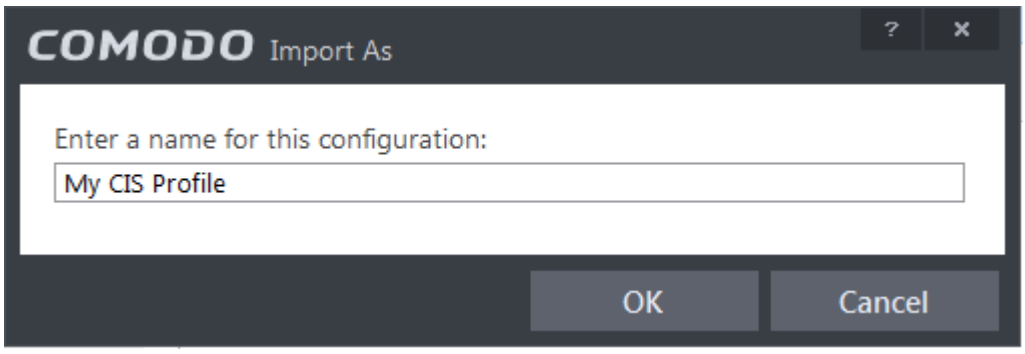
To import a profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface, click the handle at the foot of the interface and choose Import from the options.

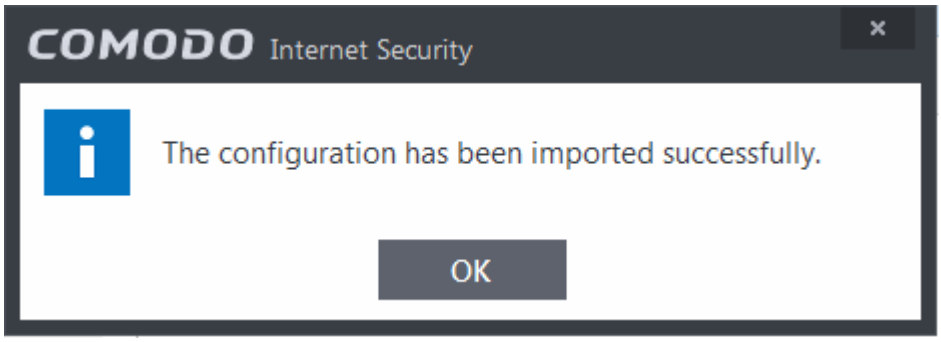


The 'Select a configuration file to import' dialog will open.

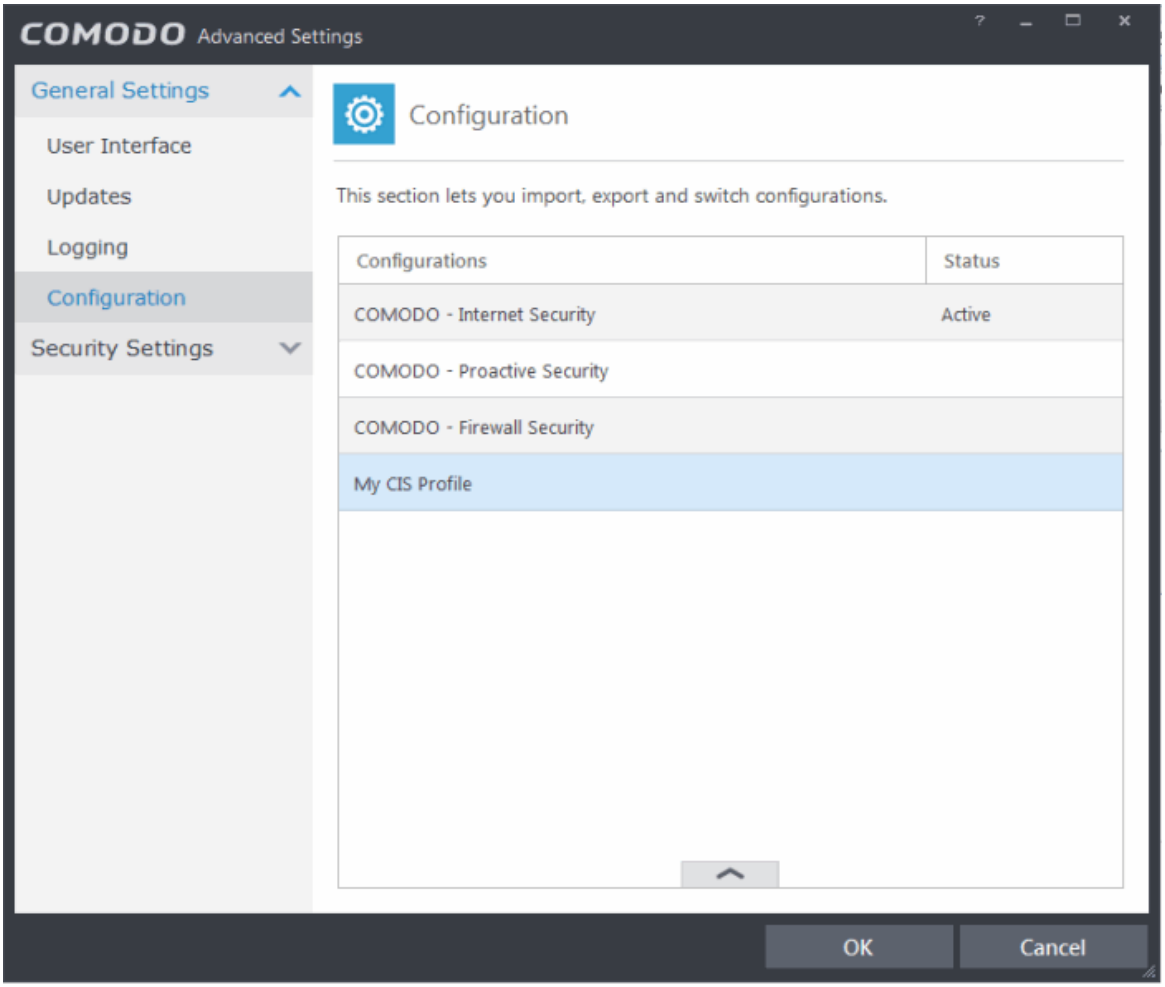
2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



A confirmation dialog will appear indicating the successful import of the profile.



Once imported, the configuration profile is available for deployment by **selecting it**.

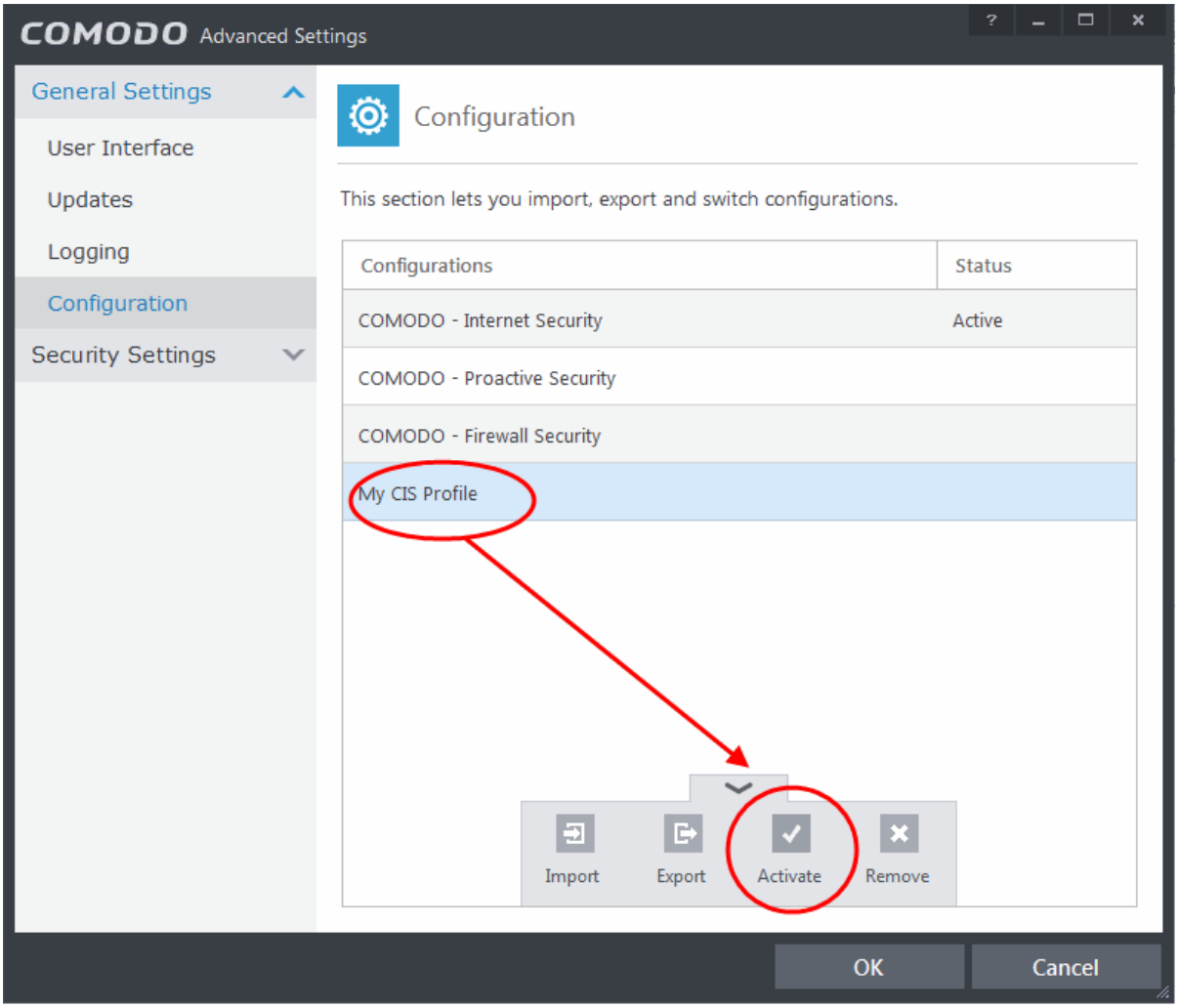


Selecting and Implementing a different configuration profile

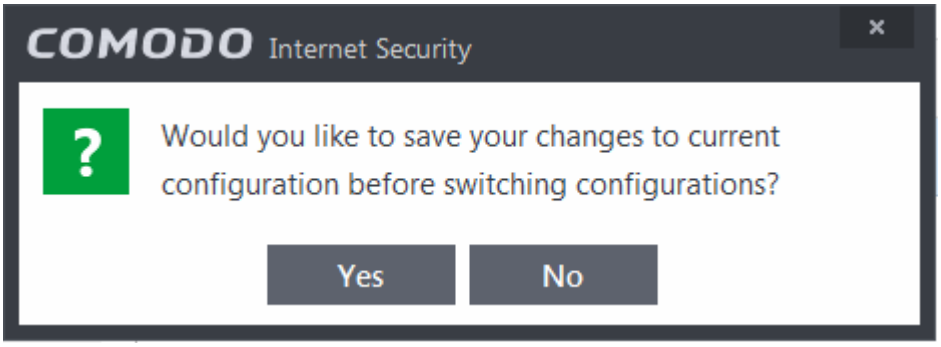
You can change the configuration profile active in CIS at any time from the 'Configurations' panel

To change the active configuration profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to activate, click the handle at the foot of the interface and choose Activate from the options.

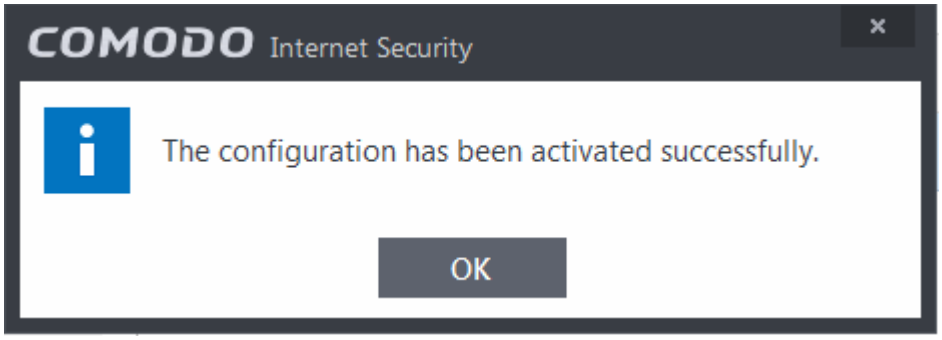


You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.

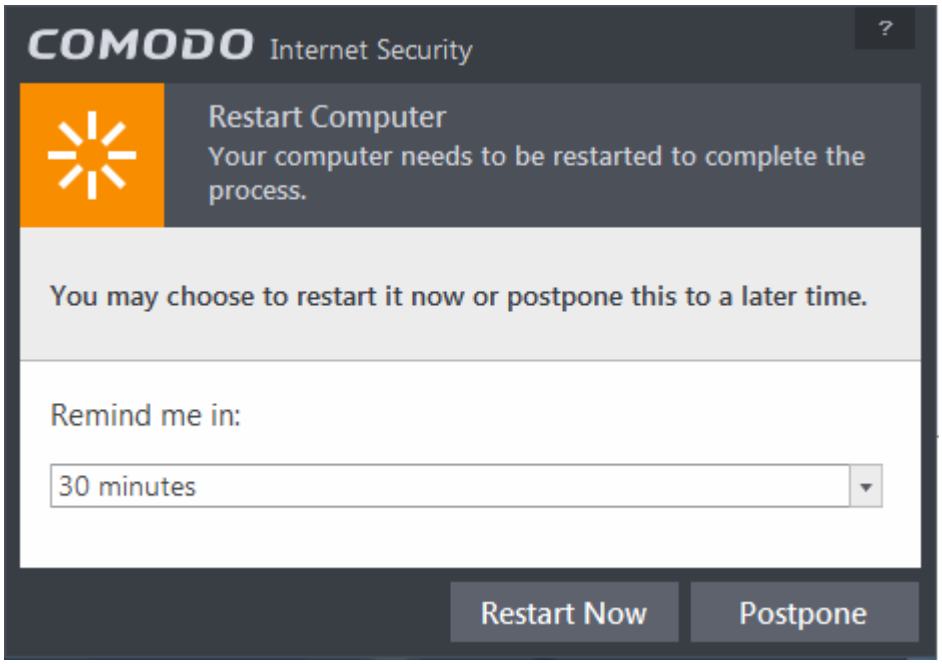


3. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

An activation confirmation dialog will be displayed. But the new profile will be implemented only on the next restart of the computer.



A 'Restart Computer' alert will appear at the bottom right of the screen.



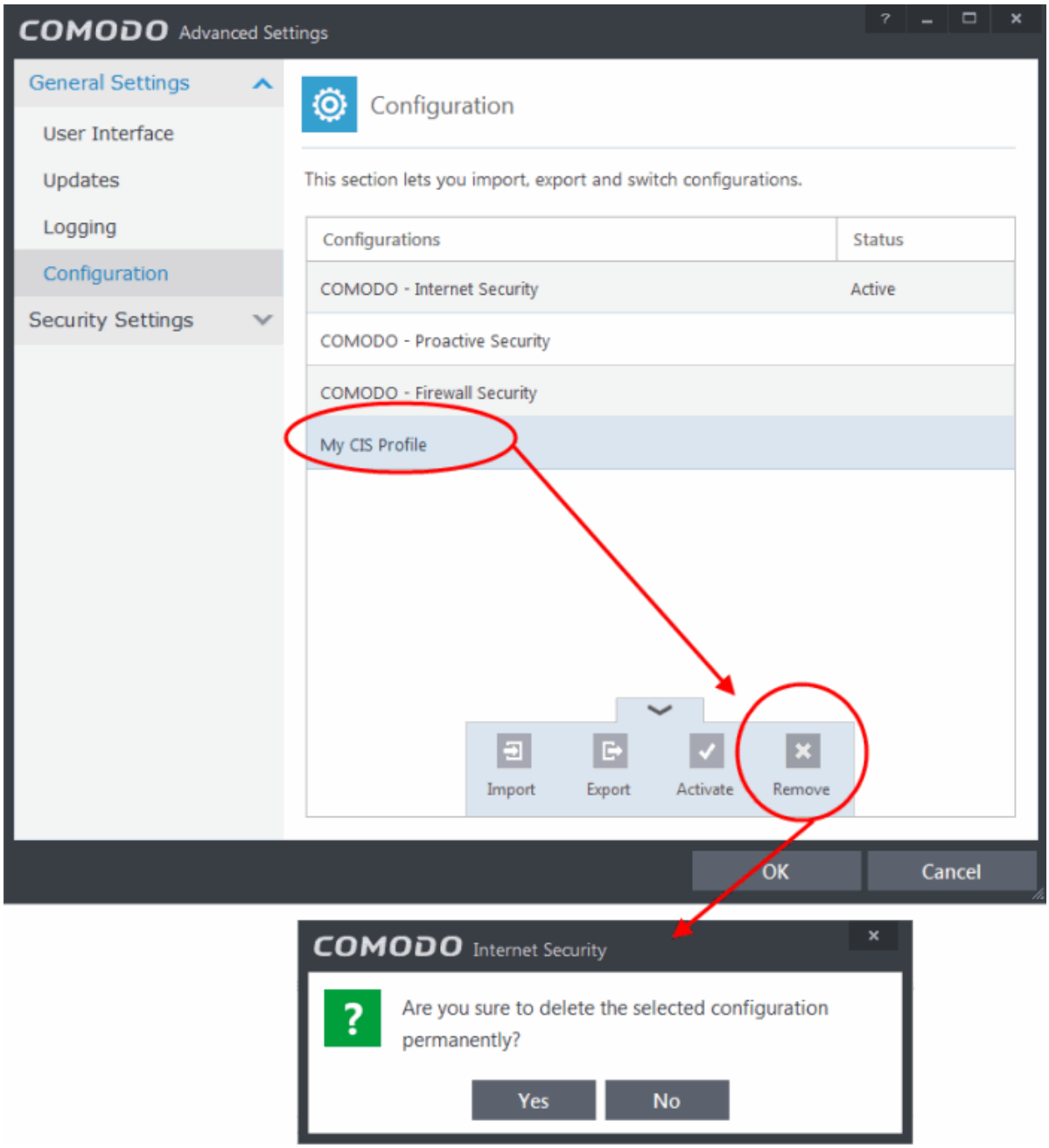
- If your want to restart the computer immediately, save all your work and click 'Restart Now'.
- If you want to restart the computer at a later time, select when you need to be reminded from the drop-down and click 'Postpone'.

Deleting an inactive configuration profile

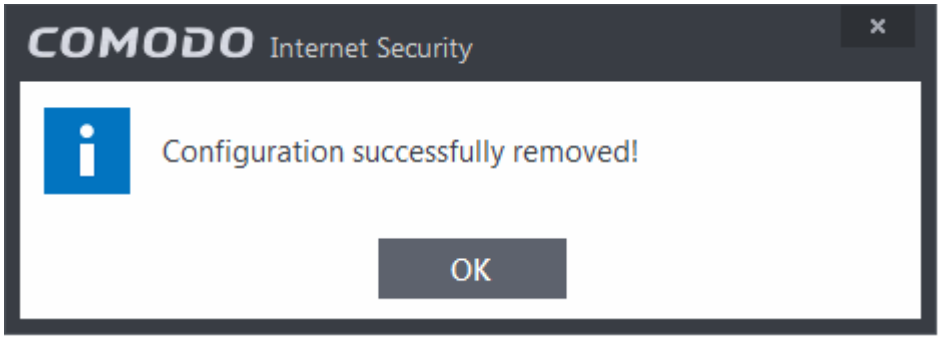
You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that Comodo Internet Security is currently using - only the inactive ones. For example if the COMODO - Internet Security is the active profile, you can only delete the inactive profiles, 'COMODO - Proactive Security, 'My_CIS_Configuration and so on.

To remove an unwanted profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to delete, click the up arrow from the bottom center and choose 'Remove' from the options. A confirmation dialog will be displayed.

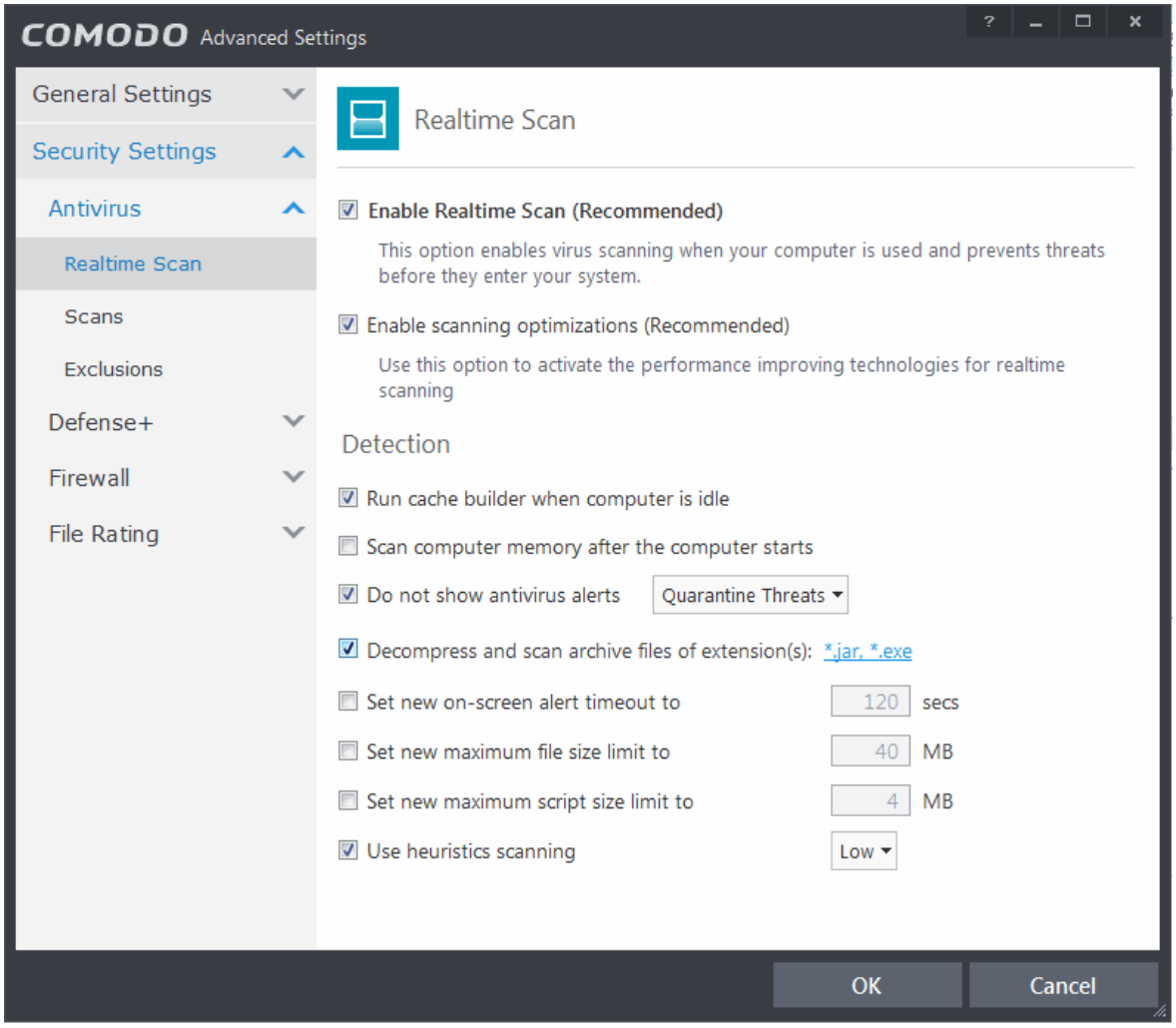


3. Click 'Yes'. The configuration profile will be deleted from your computer.



6.2. Security Settings

The Security Settings area enables you to perform granular configuration of the Antivirus, Firewall, Defense+ and File ratings components of Comodo Internet Security. Although these settings play a large part in governing the level of security offered by the application, Comodo Internet Security 6.2 does ship with secure defaults for all major settings so provides 'out-of-the-box' protection for all users.



Click the following links to go straight to the topic that explains the respective settings screen:

- **Antivirus Settings**
  - **Real-time Scanner Settings**
  - **Custom Scan Settings**
  - **Exclusions**
- **Defense+ Settings**
  - **HIPS Settings**
  - **Active HIPS Rules**
  - **Predefined HIPS Rule Sets**
  - **Protected Objects**
  - **HIPS Groups**
  - **Sandbox**
  - **Sandbox Settings**
  - **Auto-Sandbox Settings**
  - **Viruscope**
- **Firewall Settings**

- **Firewall Settings**
- **Application Rules**
- **Global Rules**
- **Predefined Rule Sets**
- **Network Zones**
- **Port Sets**
- **Website Filtering**

- **Manage File Rating**
  - **File Rating Settings**
  - **File Groups**
  - **File List**
  - **Submitted Files**
  - **Trusted Vendors List**

6.2.1. Antivirus Settings

The Antivirus Settings category has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe).

Click the following links to jump to each section:

- **Real Time Scan** - To set the parameters for on-access scanning;
- **Custom Scan** - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans;
- **Exclusions** - To see the list of ignored threats and to set the parameters for Exclusions.

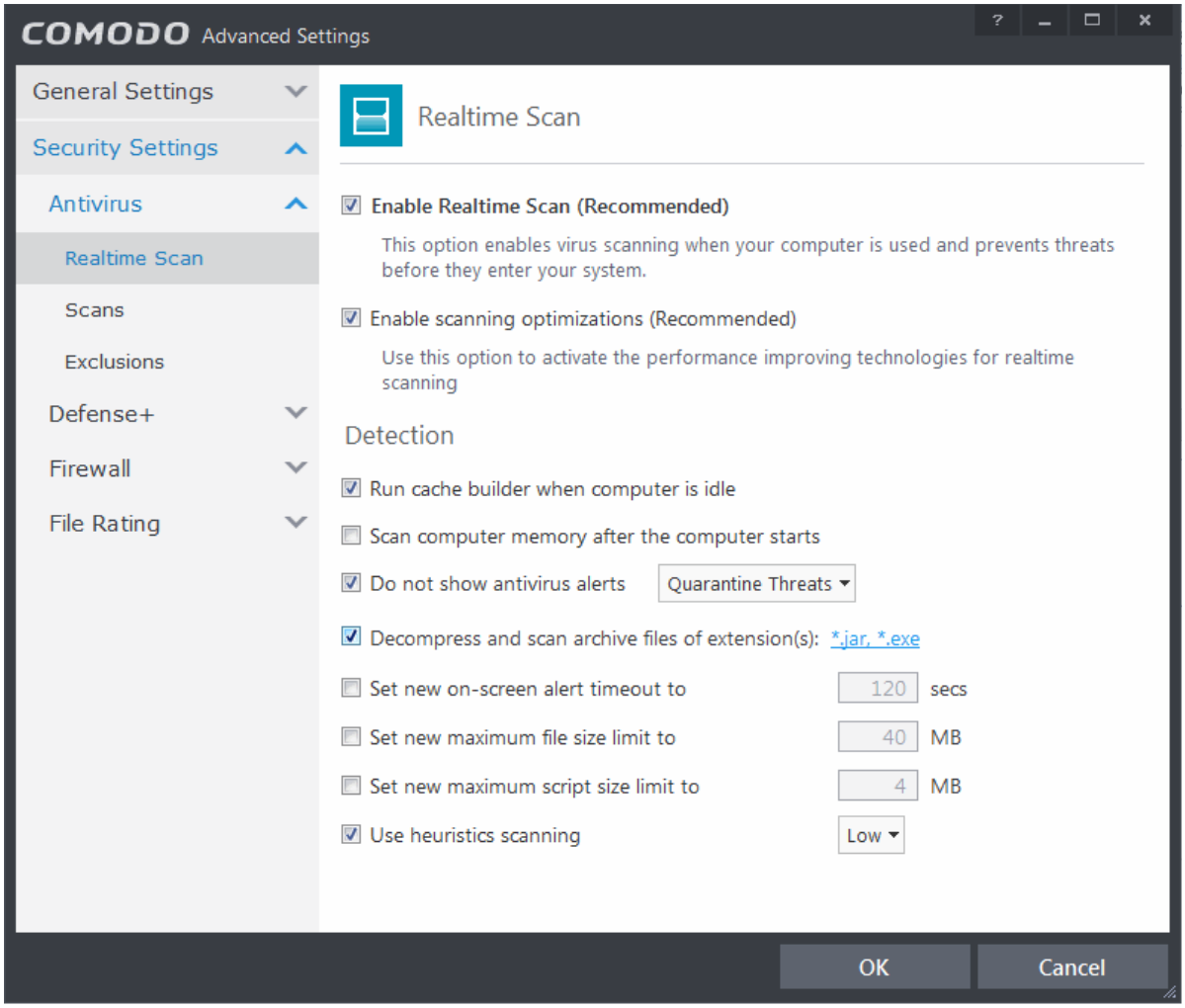
6.2.1.1. Real-time Scanner Settings

The real-time scanner (aka 'On-Access Scan') is always ON and checks files in real time when they are created, opened or copied (as soon as you interact with a file, Comodo Antivirus checks it). This instant detection of viruses assures you, the user, that your system is perpetually monitored for malware and enjoys the highest level of protection.

The real-time scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, however, you can specify that CIS does not show you alerts if viruses are found but automatically deals with them (choice of auto-quarantine or auto-block/delete). It is highly recommended that leave the Real Time Scanner enabled to ensure your system remains continually free of infection.

To open the Real Time Scan settings panel

- Click 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Antivirus > Realtime Scan':



- **Enable Realtime Scan** - Allows you to enable or disable real-time scanning. Comodo recommends to leave this option selected.(***Default=Enabled***)
- **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to reduce consumption of system resources and speed-up the scanning process ***(Default = Enabled)***

Note: The above two settings can be modified from the 'Advanced View' of the Home screen by clicking the status link beside Antivirus. If you choose Disabled option, both 'Enable Realtime Scan' and 'Enable scanning optimizations' will be disabled. If you choose 'Stateful', both the settings will be enabled and on choosing 'On Access', only 'Enable Realtime Scan' will be enabled.

Detection Settings

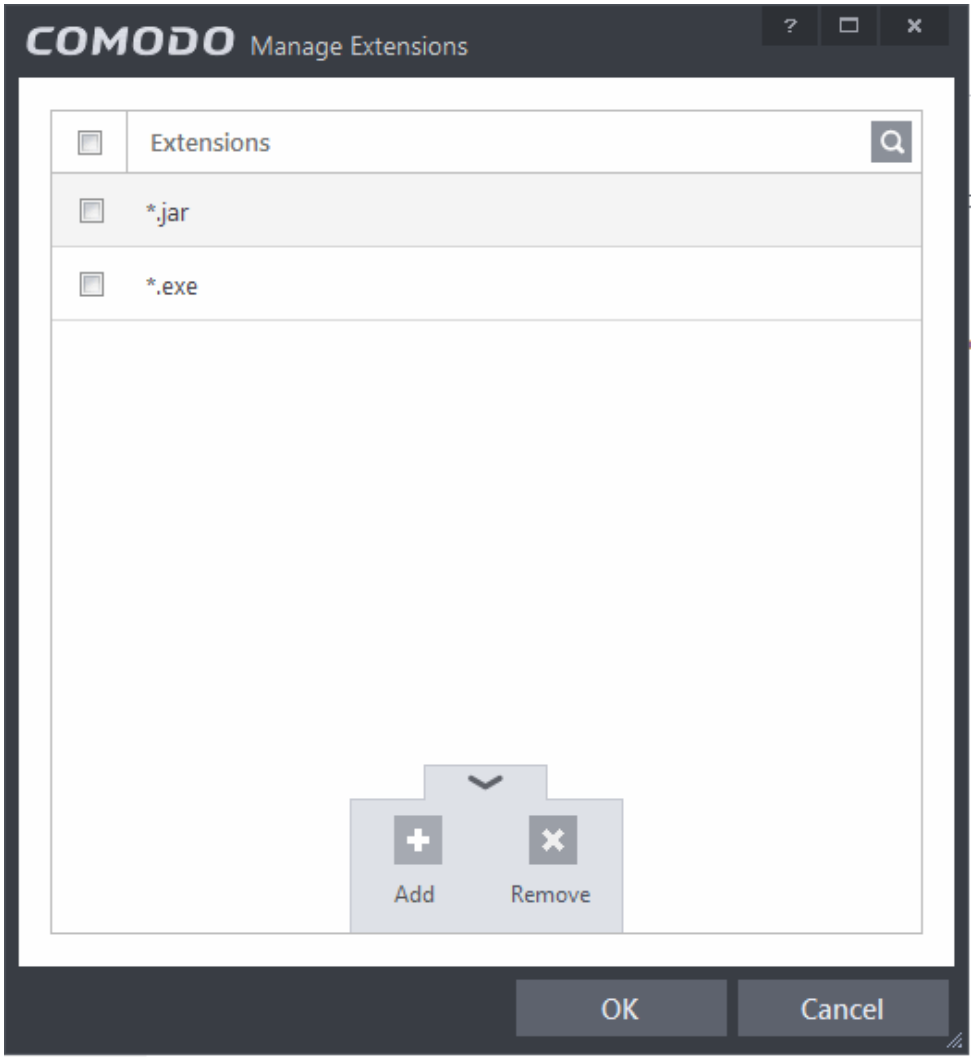
- **Run cache builder when computer is idle** - CIS runs the Antivirus Cache Builder whenever the computer is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (***Default = Enabled***).
- **Scan computer memory after the computer starts** - When this check box is selected, the Antivirus scans the system memory during system start-up ***(Default = Disabled)***
- **Do not show antivirus alerts** - Allows you to configure whether or not to show antivirus alerts when malware is encountered. Choosing 'Do not show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Threats' or 'Quarantine Threats'. (***Default = Enabled***)
  - **Quarantine Threats** - Moves the detected threat(s) to quarantine for your later assessment and action. (***Default***)
  - **Block Threats** - Stops the application or file from execution, if a threat is detected in it.

Note: If you deselect this option and thus enable alerts then your choice of quarantine/block is presented within the alert itself.

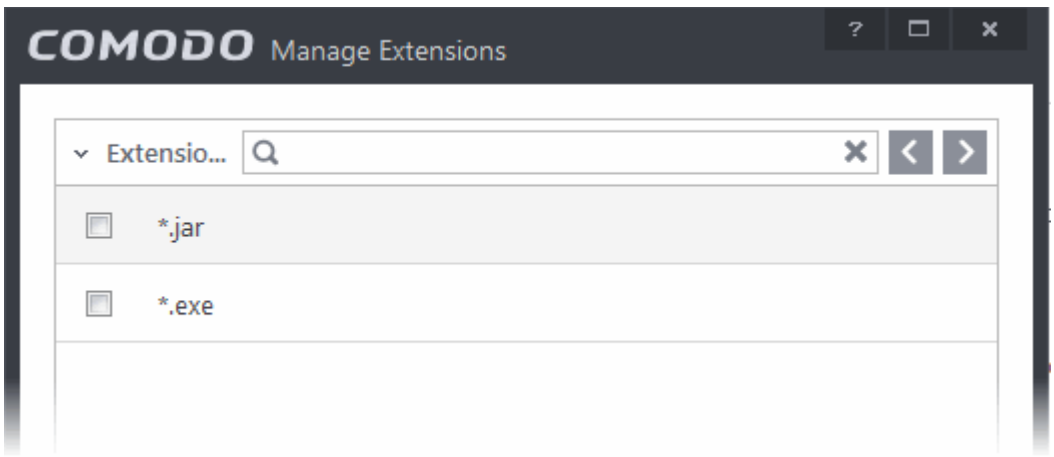
- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default = Enabled)***

  You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

  - Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.



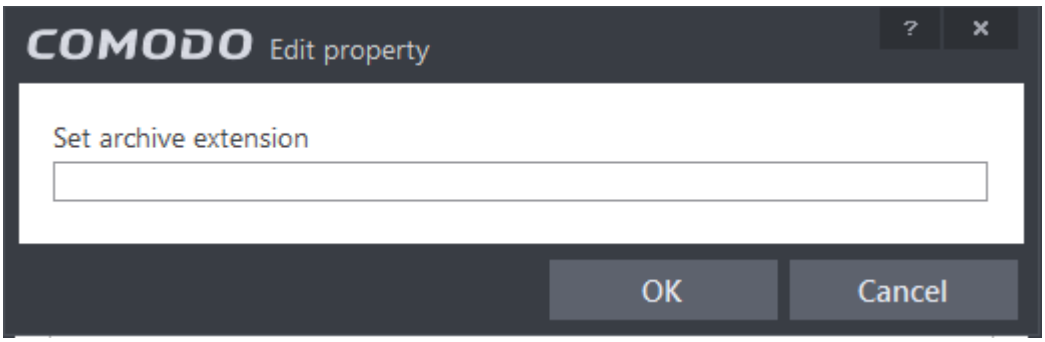
You can use the search option to find a specific file extension in the list by clicking the search icon at the far right in the column header.



- Enter the file extension to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Adding a New File Type

- To add a file type, click the up arrow at the bottom center and click 'Add'.



- Enter the extension (e.x.: rar, msi, zip, 7z, cab and so on) to be included in the Edit property dialog and click OK.
- Repeat the process to add more extensions
- Click OK in the 'Manage Extensions' dialog

- **Set new on-screen alert timeout to** - This box allows you to set the time period (in seconds) for which the alert message should stay on the screen. (***Default = 120 seconds***)
- **Set new maximum file size limit to** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned. (***Default = 40 MB***)
- **Set new maximum script size limit to** - This box allows you to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (***Default = 4 MB***)
- **Use heuristics scanning** - Allows you to enable or disable Heuristics scanning and define scanning level. (***Default = Enabled***)

  Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  Leave this option selected to keep Heuristics scanning enabled. Else, deselect this checkbox. If enabled, you can select the level of Heuristic scanning from the drop-down:

  - **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users. (***Default***)
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

6.2.1.2. Scan Profiles

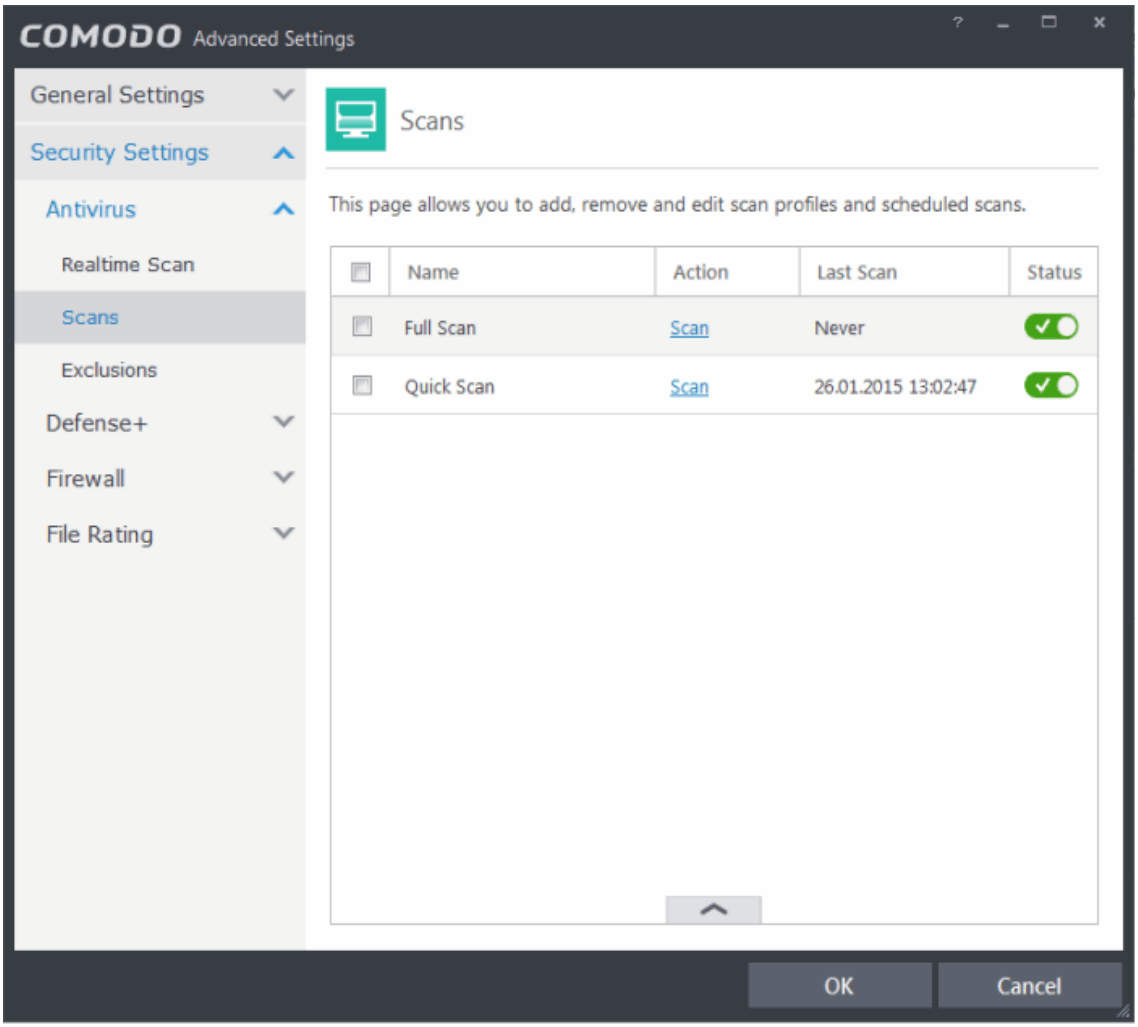
The Scan Profiles area allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CIS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)

- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To open the panel

- Click Security Settings > Antivirus > 'Scans' tab in the 'Advanced Settings' panel.



CIS ships with two predefined scan profiles:

- **Full Scan** - Covers every local drive, folder and file on your system.
- **Quick Scan** - Covers critical areas in your system which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of your computer and keeping them clean is essential.

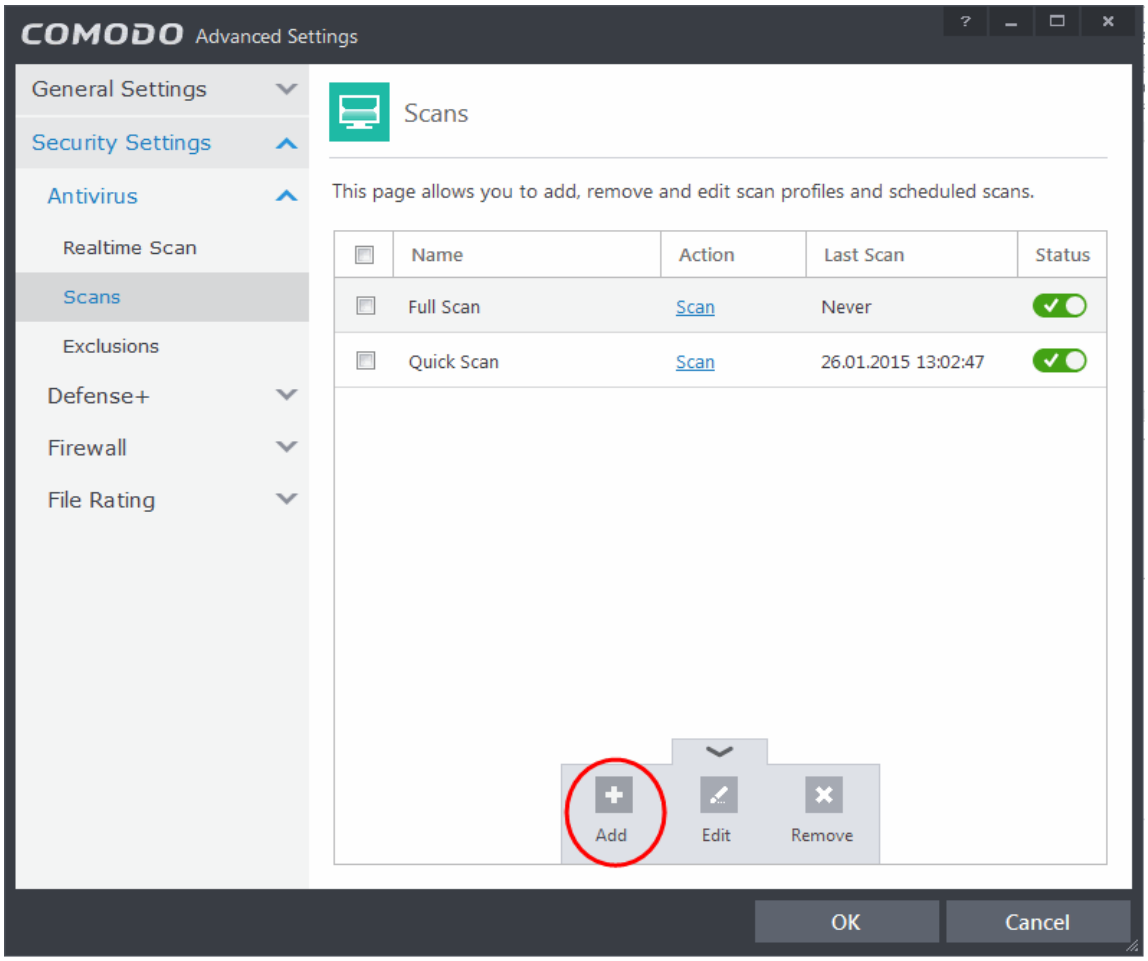
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

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

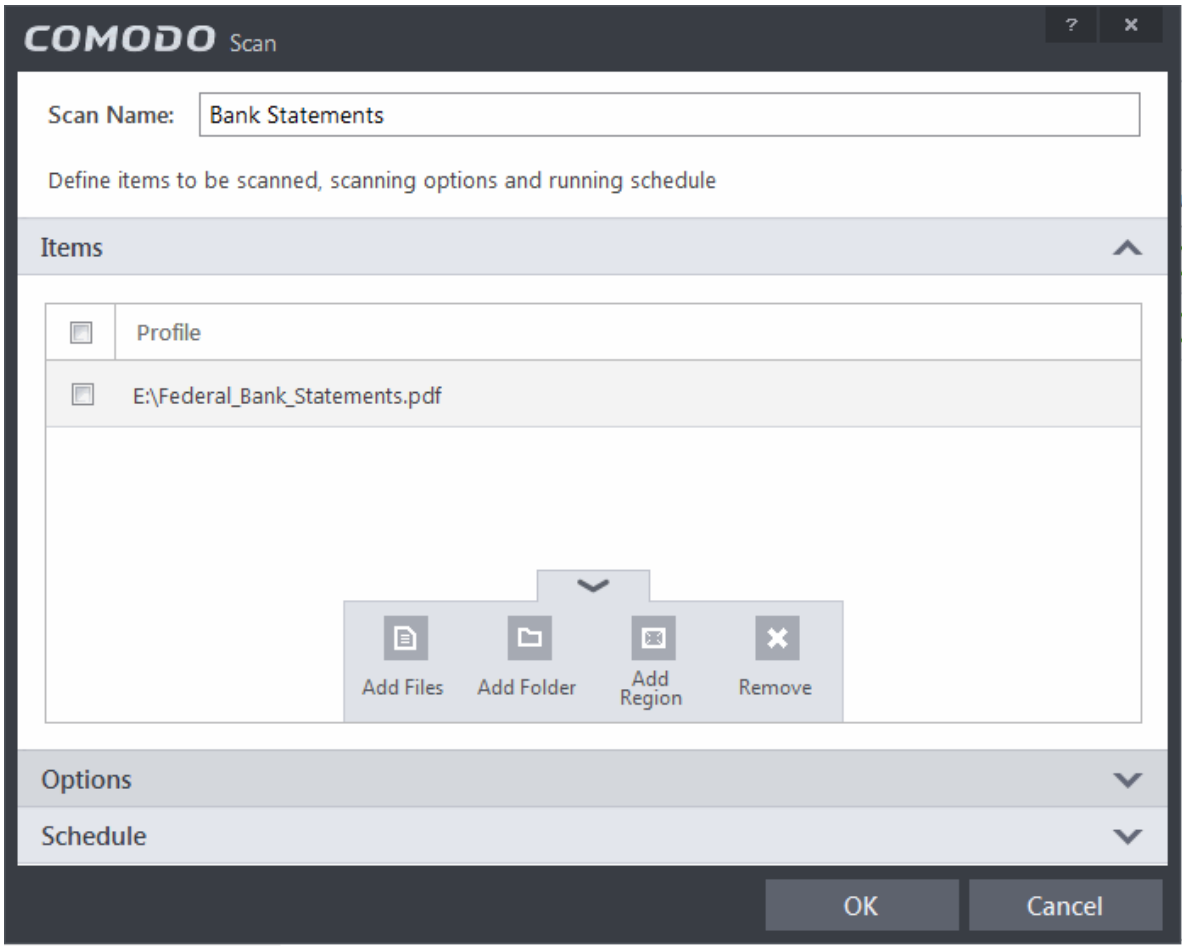
To create a custom profile

- Click the handle at the bottom of the interface then click the 'Add' button:

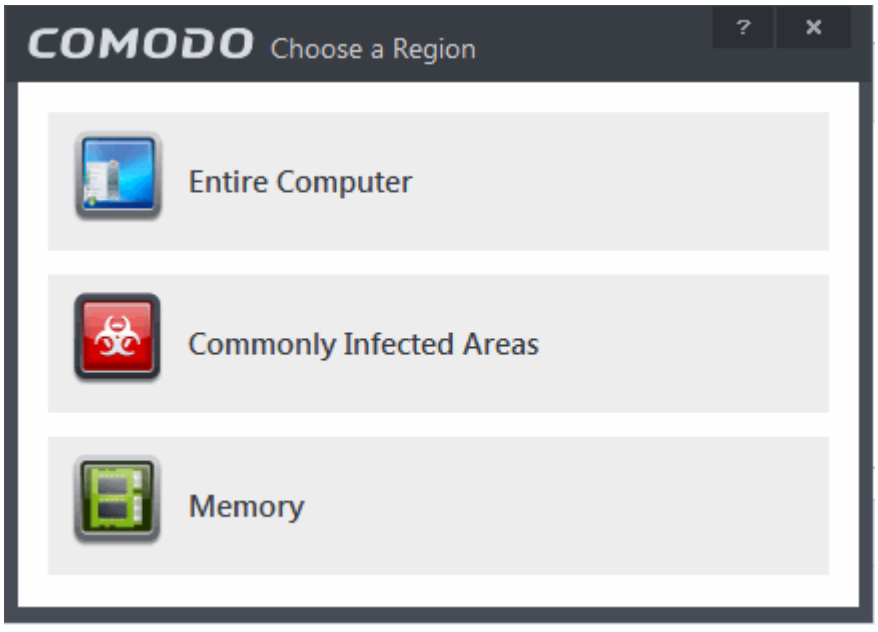


The scan profile interface will be displayed.

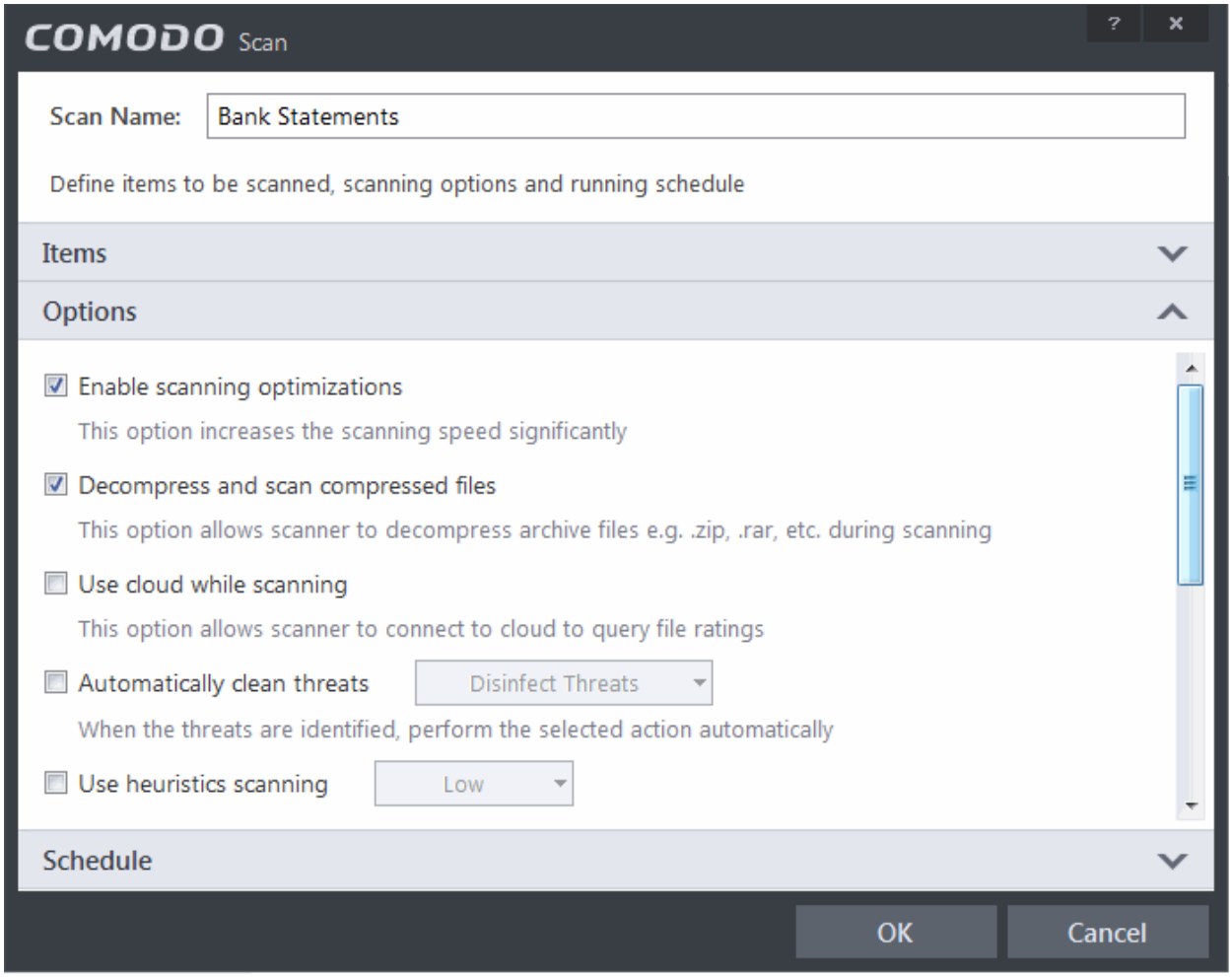
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items that should be included in the profile



- **Add Files** - Allows you to navigate to specific files that you wish to add to the profile
- **Add Folder** - Opens the 'Browse For Folder' window and allows you to select entire folders
- **Add Region** - Allows you to add predefined regions to the profile. For example, 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.



- Repeat the process to add more items into the profile
- Click 'Options' to further customize the scan



- **Options**:
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)*** .
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
  - **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. ***(Default = Disabled)***.
  - **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine. ***(Default = Disabled).***
  - **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Disabled).***

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

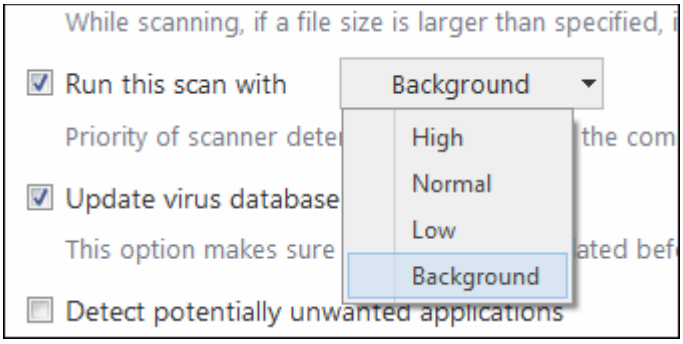
    This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

    - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false

positives. Comodo recommends this setting for most users.

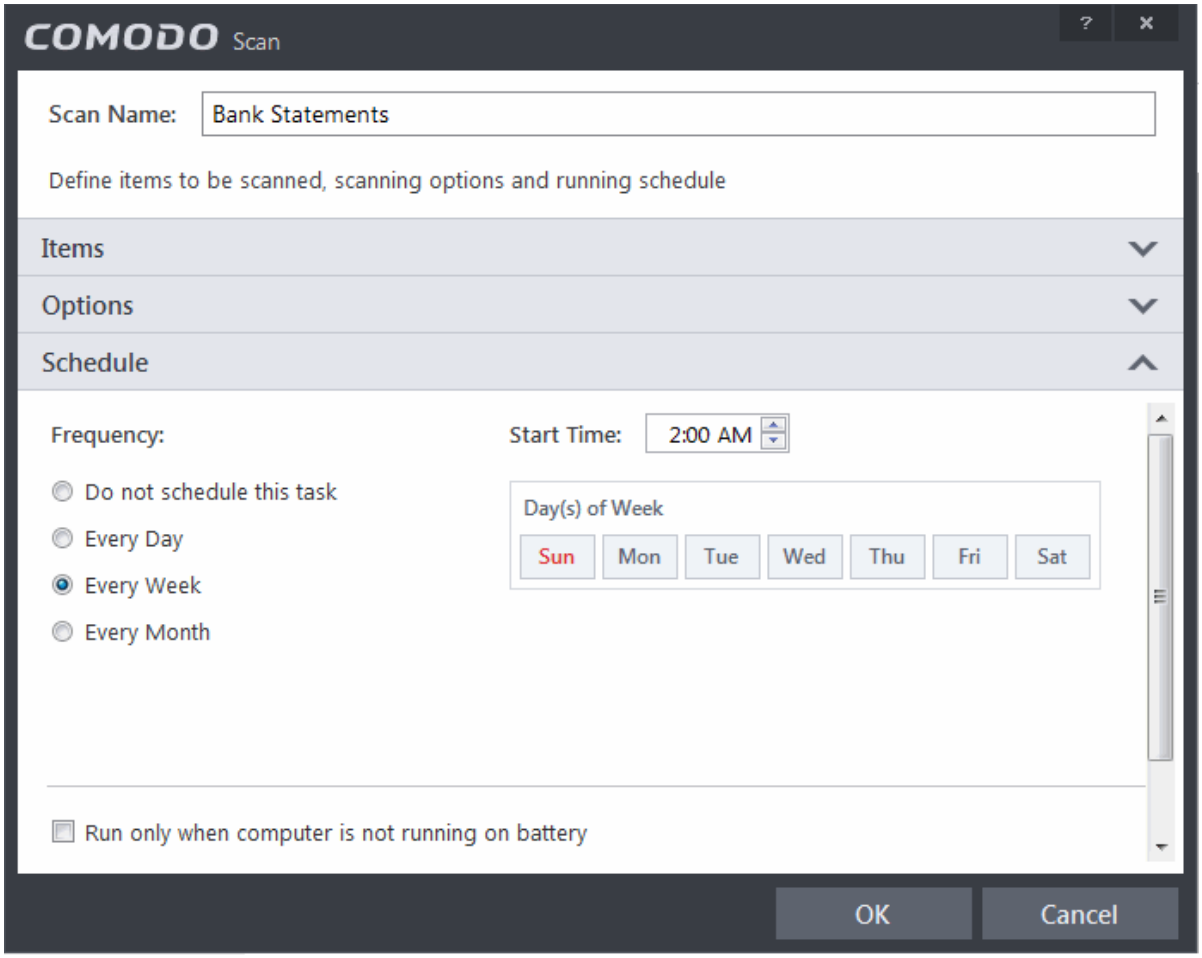
- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run Scan with** - Enables you to set the priority of the scanning from High to Low or to run at background. ***(Default = Disabled)***.



- **Update virus database before running** - Selecting this option makes CIS to check for virus database updates and if available, update the database before commencing the scan. ***(Default = Enabled)***.
- **Detect potentially unwanted applications** - When this check box is selected, virus scans will also check for potentially unwanted applications (PUA's). This is software that (i) a user may or may not be aware is installed on their computer and (ii) may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the internet. ***(Default = Enabled)***.

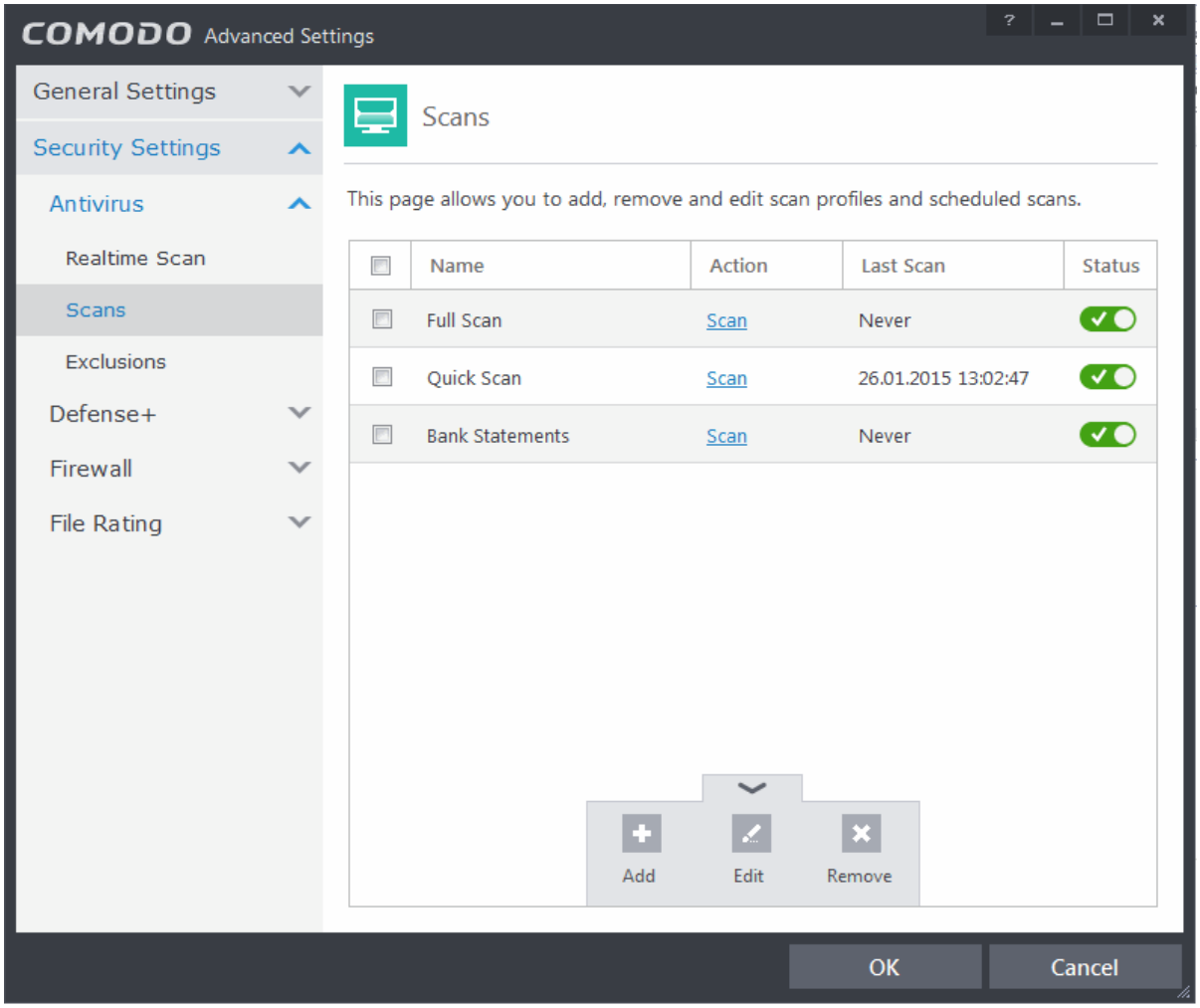
- If you want the scan to be performed periodically, set a Schedule for the custom scan by clicking 'Schedule'



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

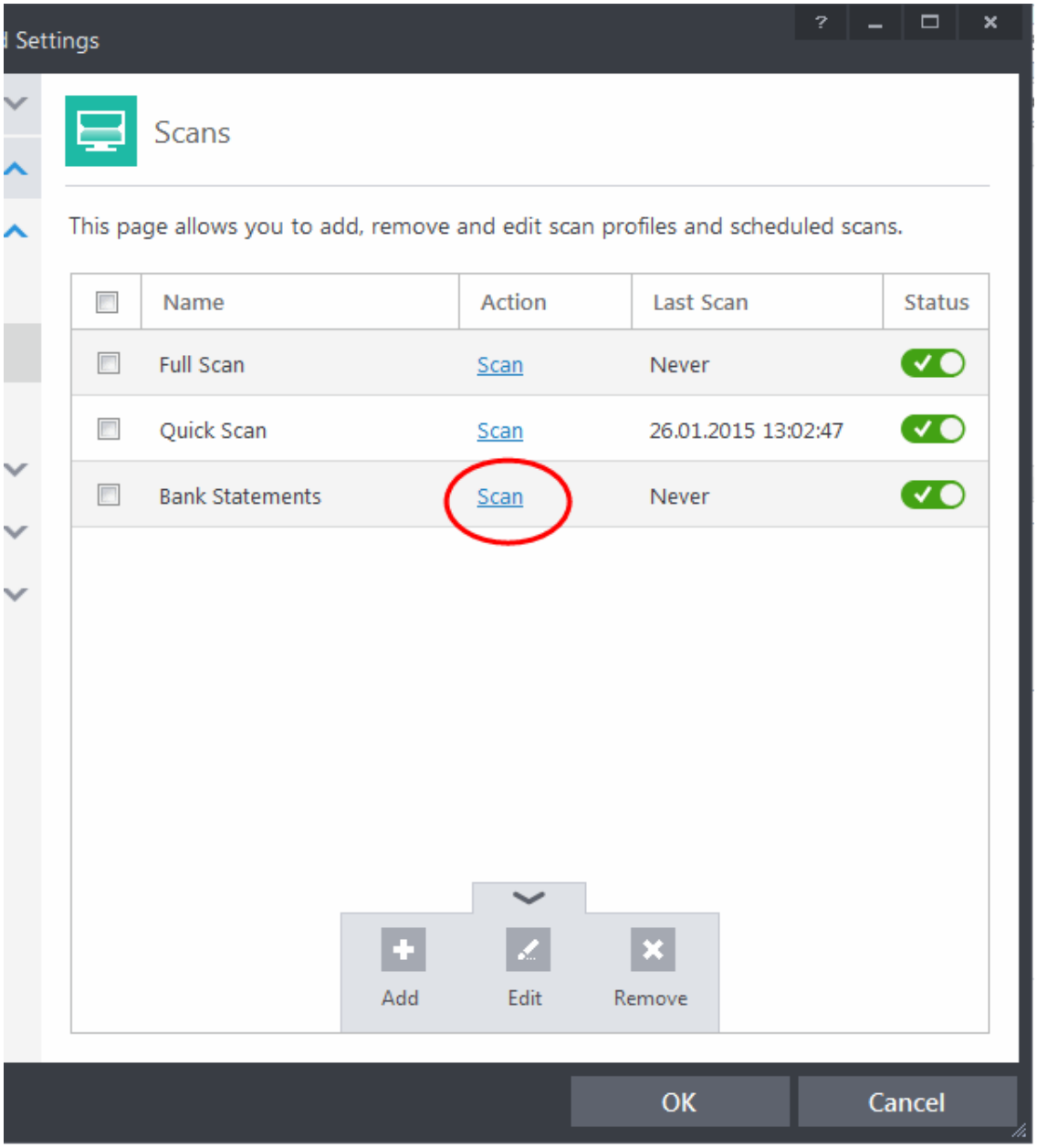
- Click OK to save the profile.

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

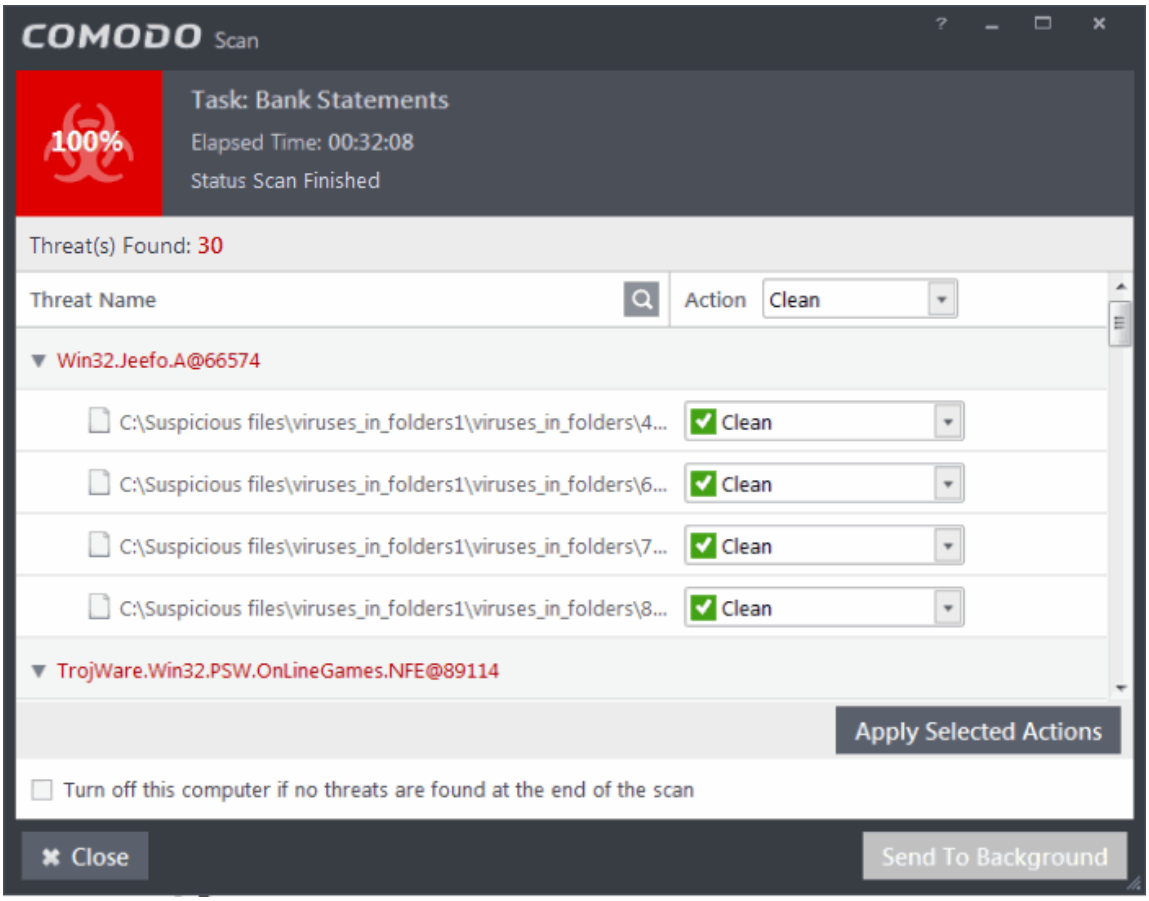


To run a custom scan as per scan profile

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



- The scan will be started and on completion the results will be displayed.



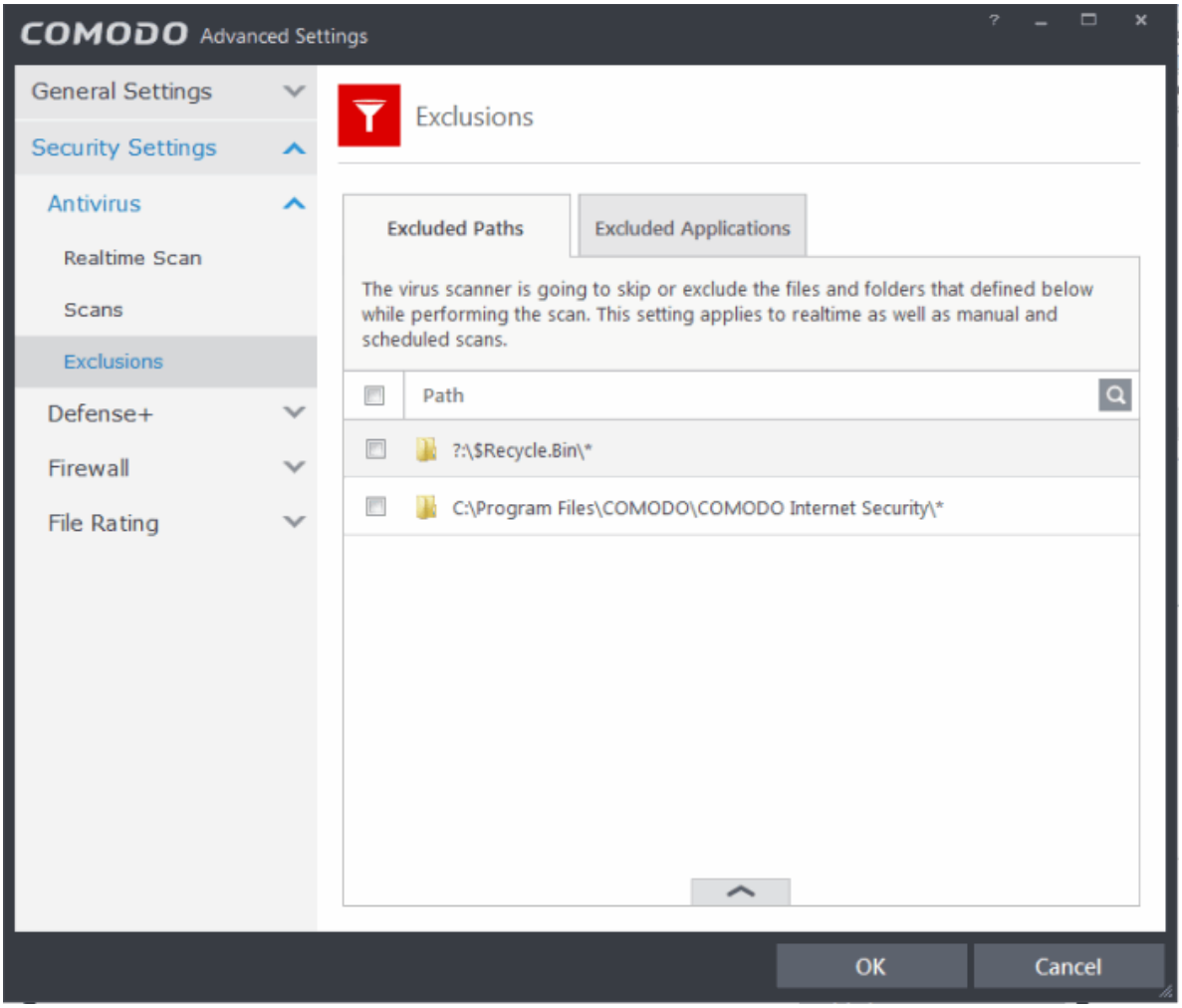
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to **Processing the infected files** for more details.

6.2.1.3. Exclusions

The 'Exclusions' panel under the Antivirus Settings Settings displays a list of paths and applications/files for which you have selected **Ignore** from the **Scan Results** window of various scans or added to the Exclusions from an antivirus alert.

To open the Exclusions panel

- Click Security Settings > Antivirus > 'Exclusions' tab in the 'Advanced Settings' panel.

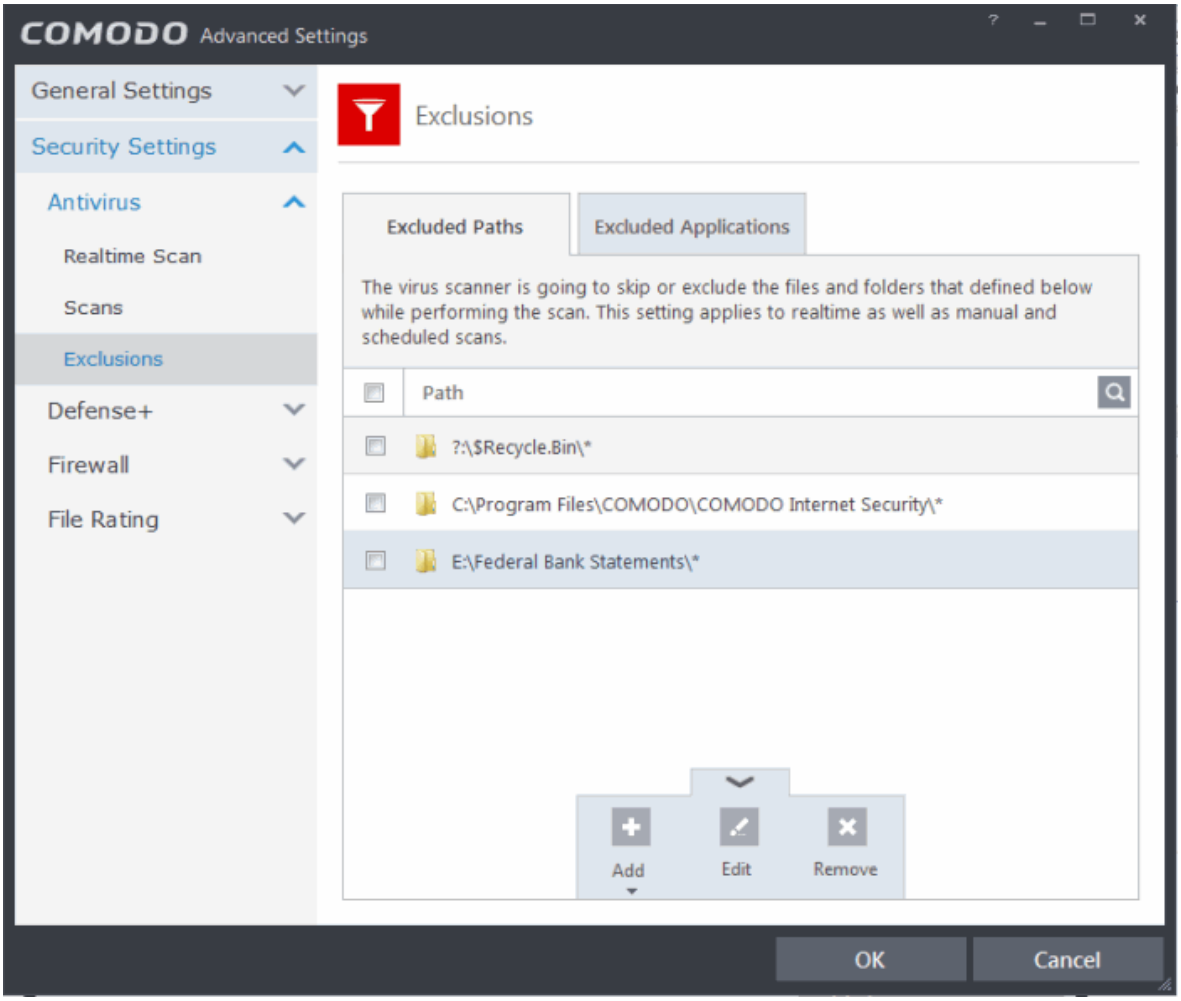


The 'Exclusions' panel has two tabs:

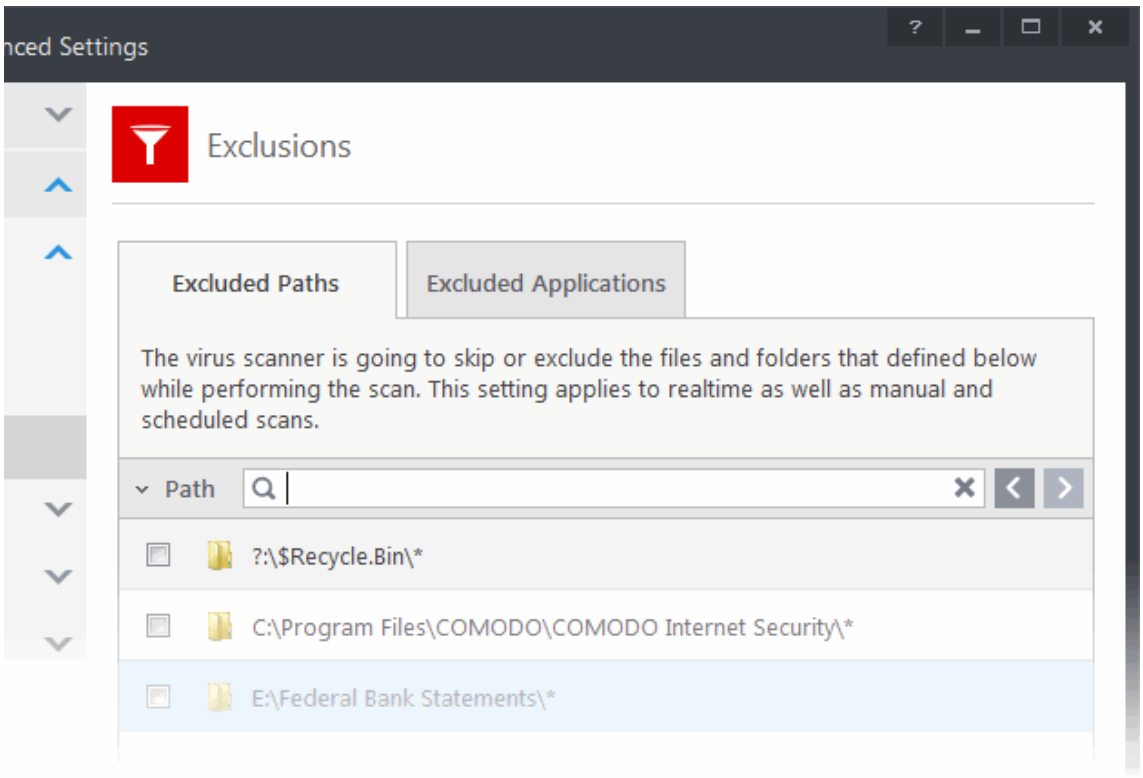
- **Excluded Paths** - Displays a list of paths/folders/files in your computer, which are excluded from both real-time and on-demand antivirus scans. Refer to the section **Excluding Drives/Folders/Files from all types of scans** for more details on adding and removing exclusion items in this interface.
- **Excluded Applications** - Displays a list of programs/applications in your computer, which are excluded from real-time antivirus scans. The items are included on clicking 'Ignore' from the **Scan Results** window of various scans and **Antivirus Alerts** or manually. Please note that these items are excluded only on real-time sans but will be scanned on running on-demand scans Refer to the section **Excluding Programs/Applications from real-time scans** more details on manually adding and removing exclusion items in this interface.

Excluding Drives/Folders/Files from all types of scans

You can exclude a drive partition, a folder, a sub-folder or a file from both the real-time and on-demand/custom scheduled antivirus scans at any time, by adding them to Excluded Paths.



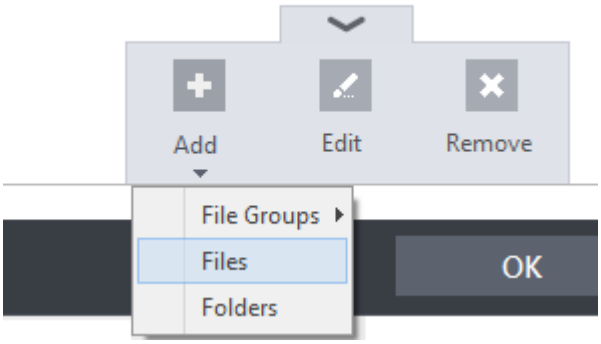
You can use the search option to find a specific excluded path, folder or file from the list by clicking the search icon at the far right in the column header.



- Enter the path, folder name or file name to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

To add item(s) to excluded paths

- Click the handle from the bottom center and click on 'Add' from the options



You can choose to add a:

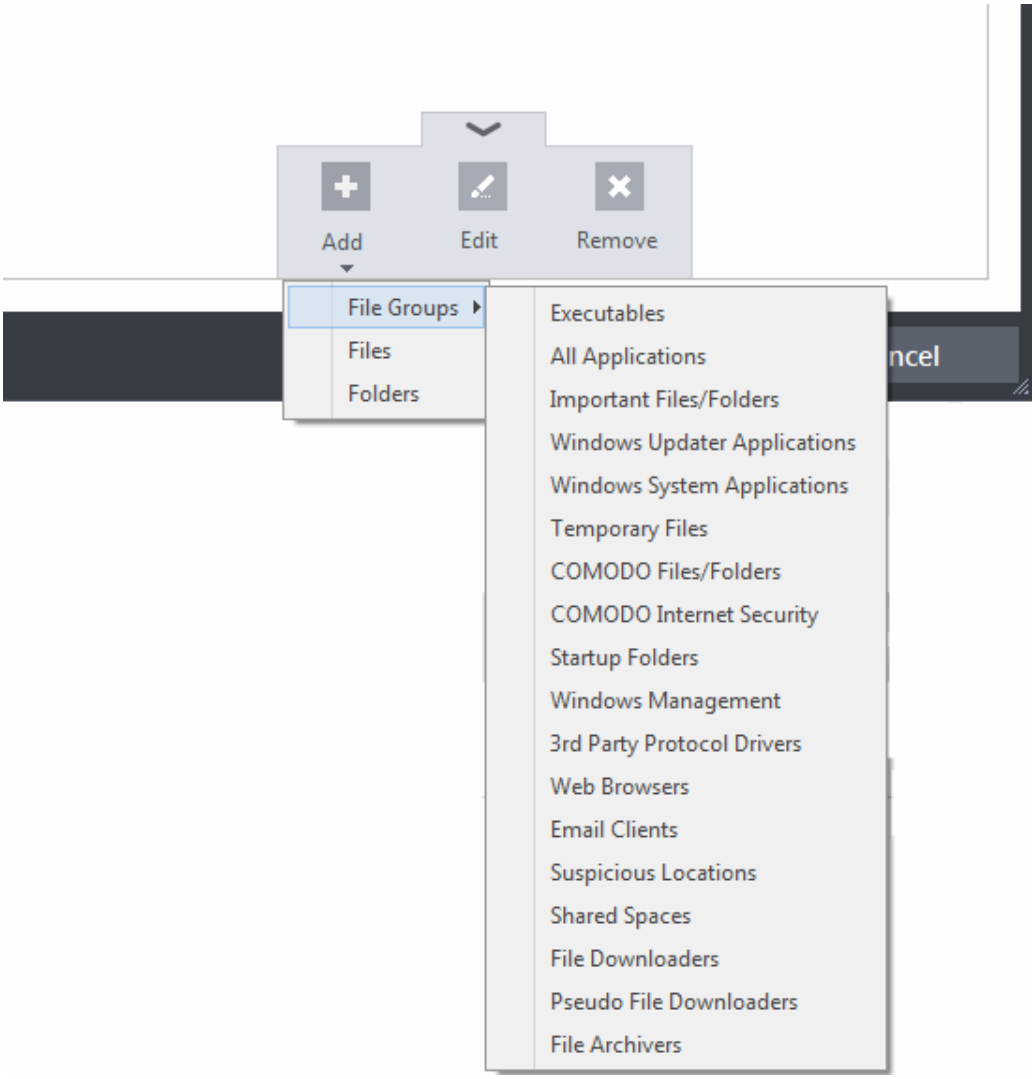
- **File Group**
- **Drive partition/Folder**

  or

- **an individual file**

Adding a File Group

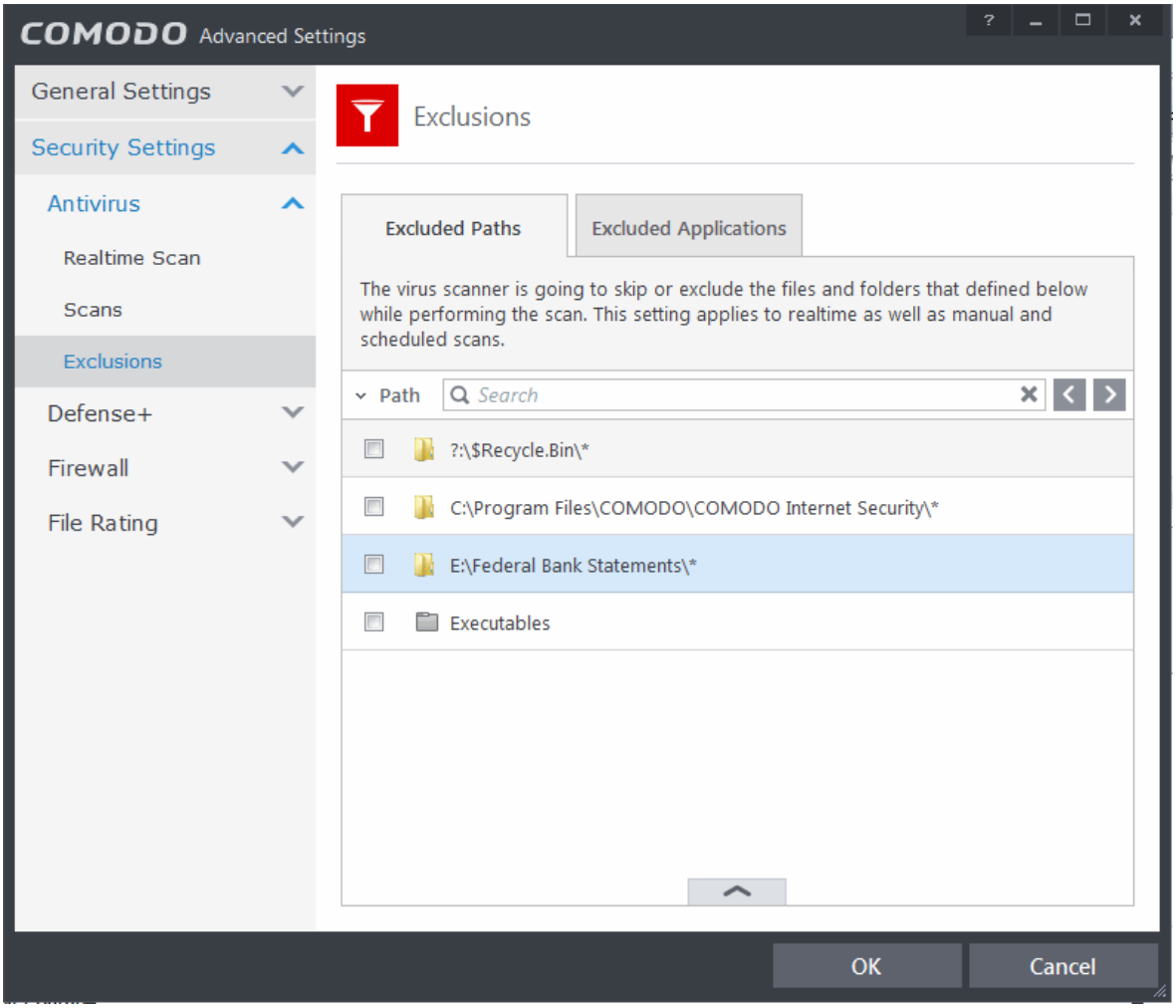
- Choosing File Groups allows you to exclude a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.



CIS ships with a set of predefined File Groups and can be viewed in Advanced Settings > File Rating > **File Groups**. You can also add new file groups here which will be displayed in the predefined list.

To add a file group to Excluded Paths, click Add > File Groups and select the type of File Group from the list.

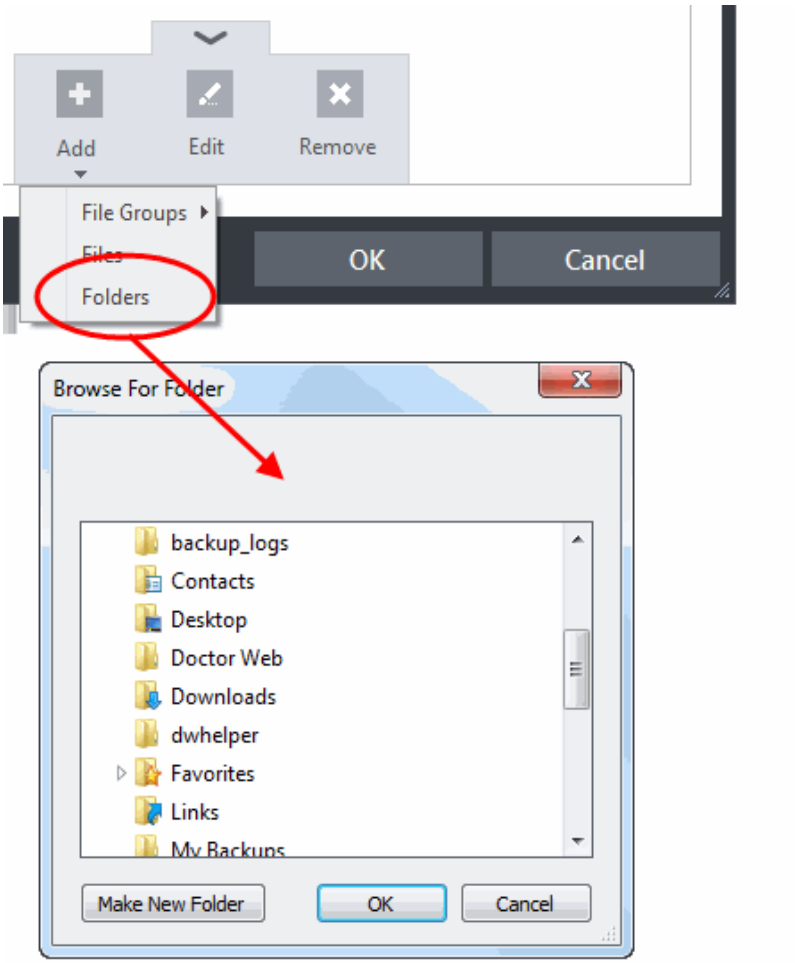
The file groups will be added to Excluded Paths.



- Repeat process to add more file groups. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding a Drive Partition/Folder

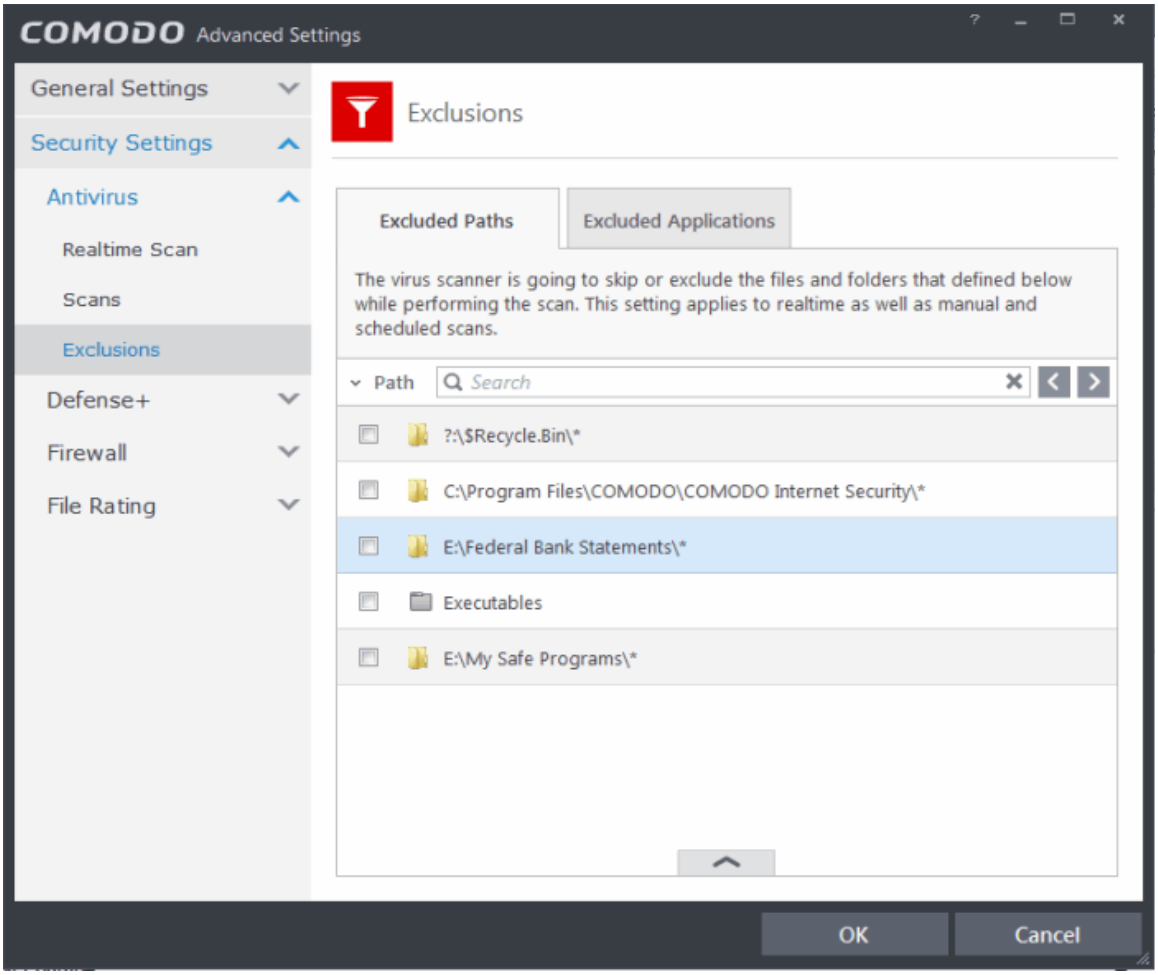
- To add a folder, choose 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will appear.

- Navigate to the drive partition or folder you want to add to excluded paths and click OK

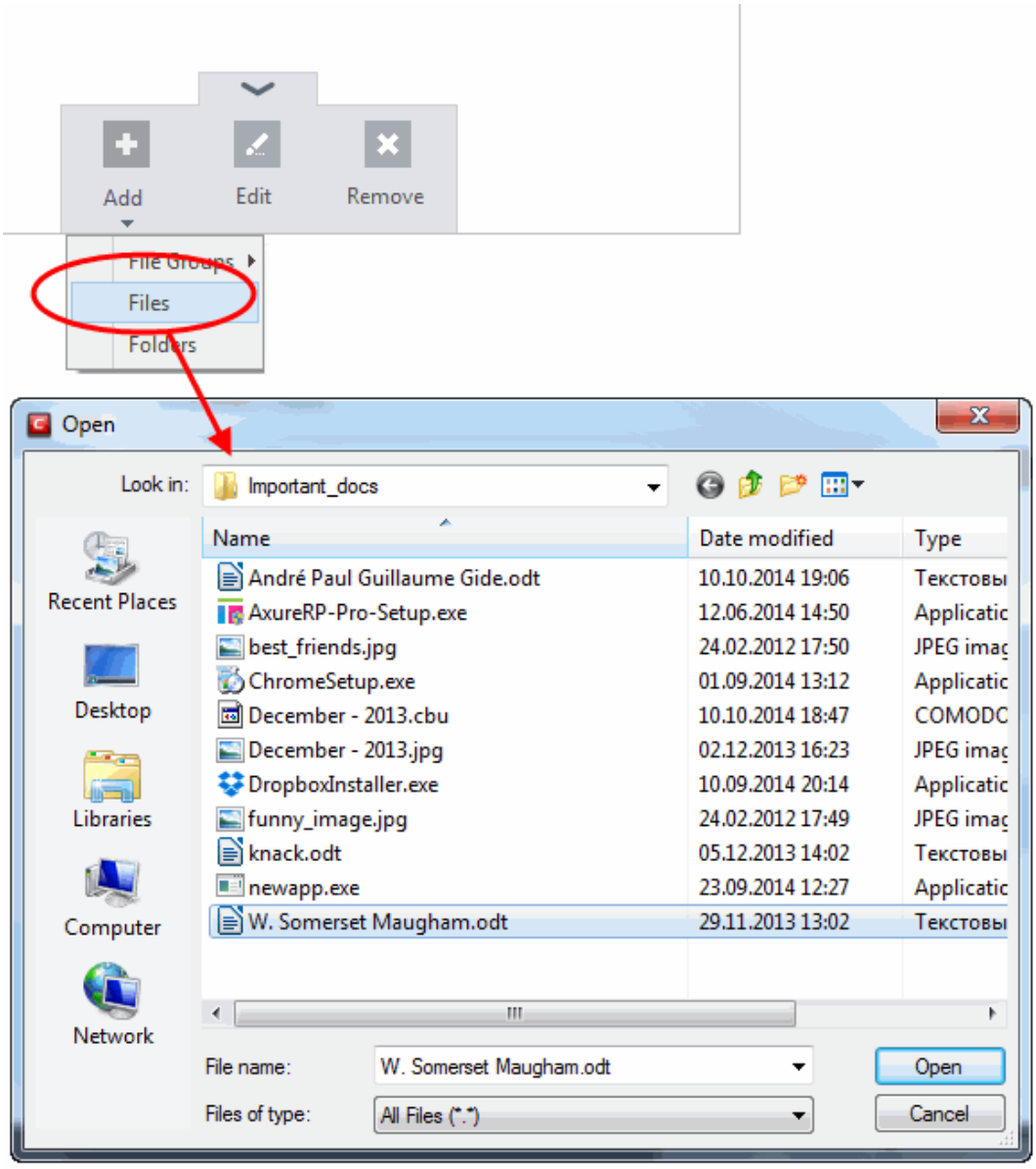
The drive partition/folder will be added to Excluded Paths.



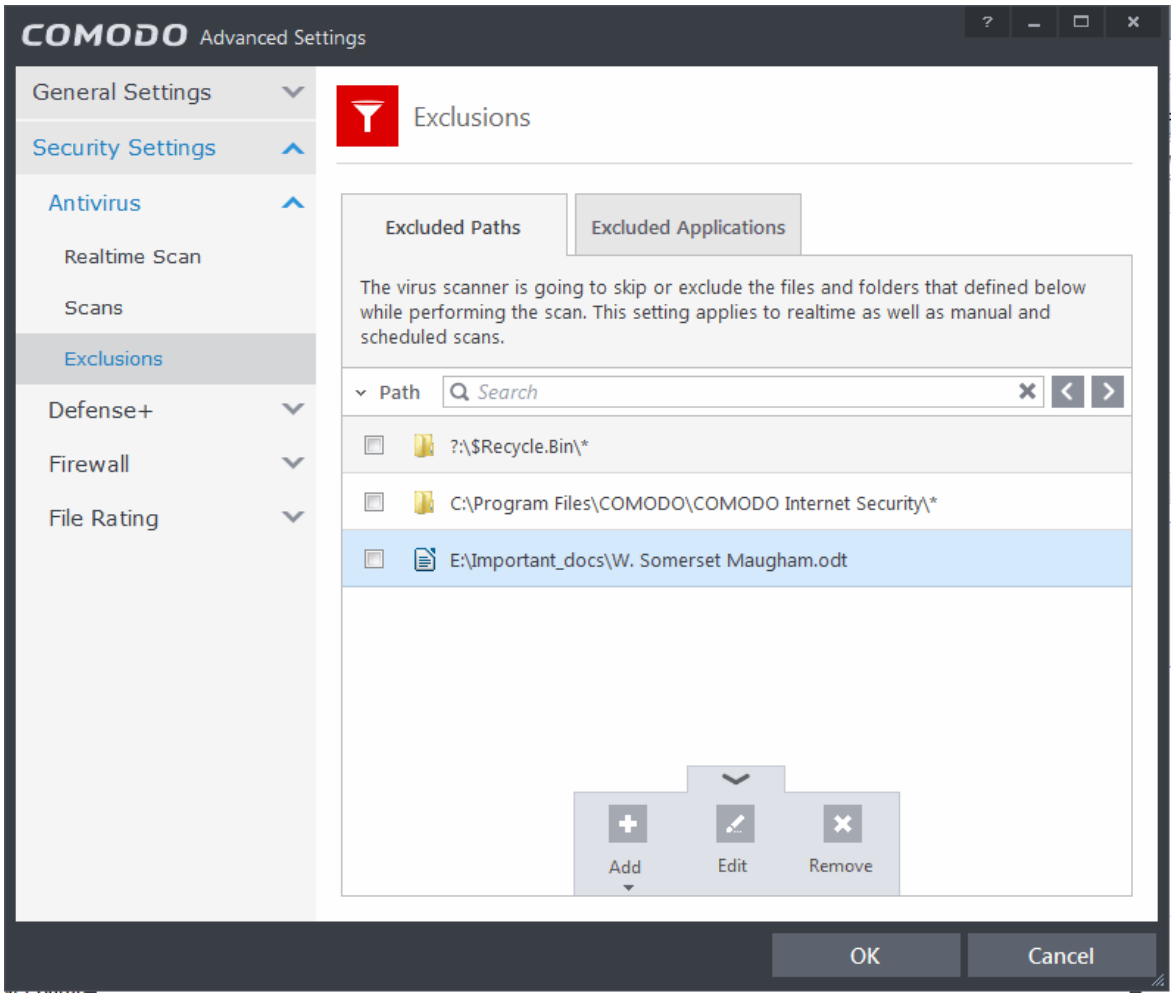
- Repeat process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding an individual File

- Choose 'Files' from the 'Add' drop-down.



- Navigate to the file you want to add to Excluded Paths in the 'Open' dialog and click 'Open'

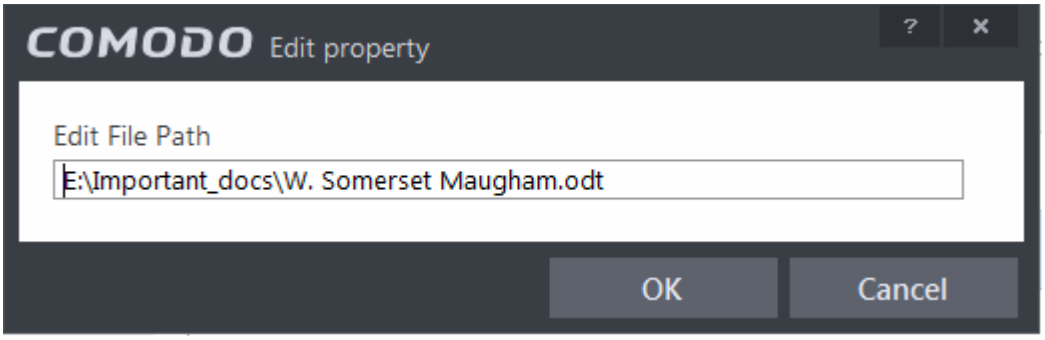


The file will be added to Excluded Paths.

- Repeat process to add more paths. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

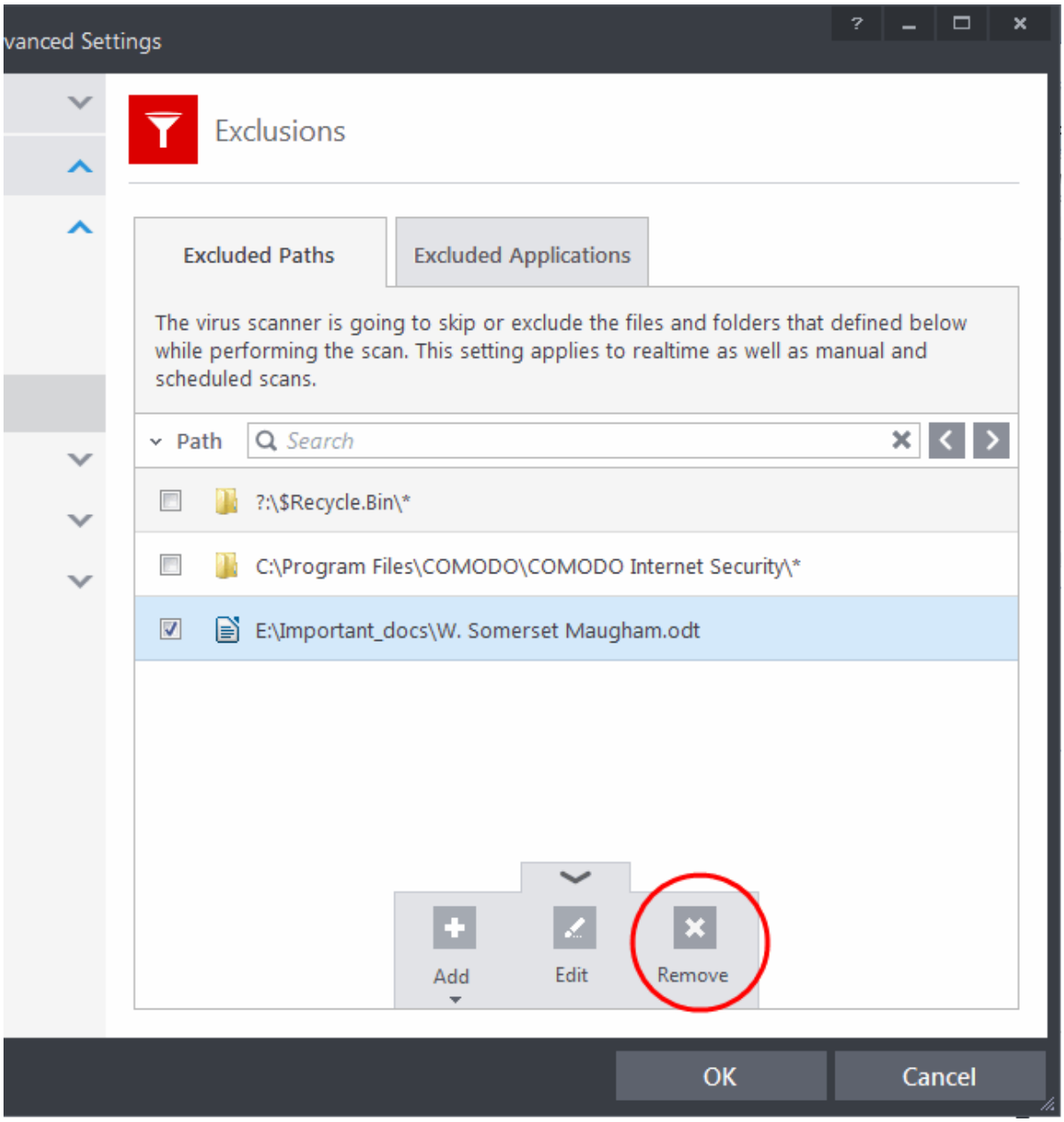
To edit the path of an added item

- Select the item, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



To remove an item from the Excluded Paths

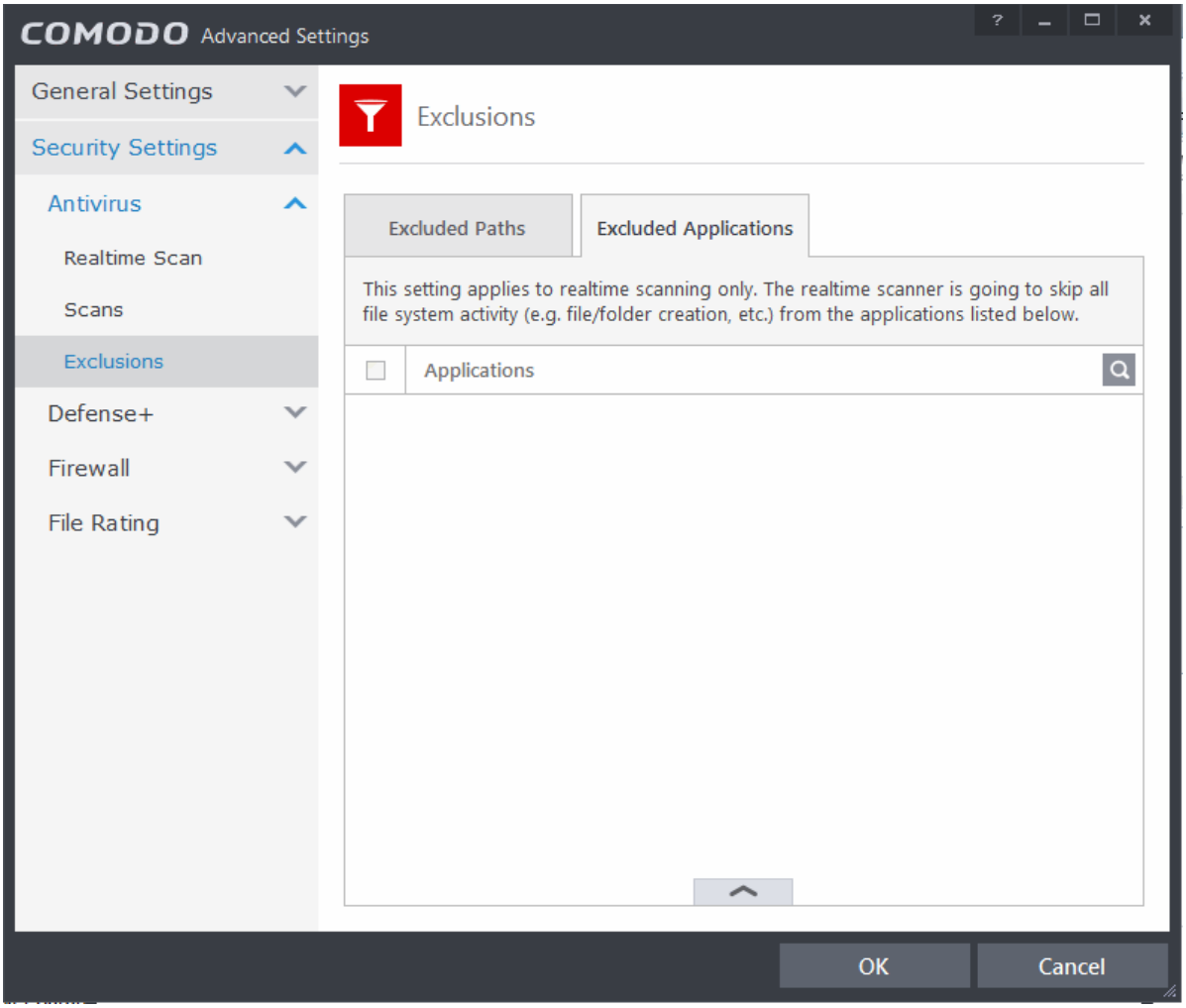
- Select the item, click the handle from the bottom center and select 'Remove'.



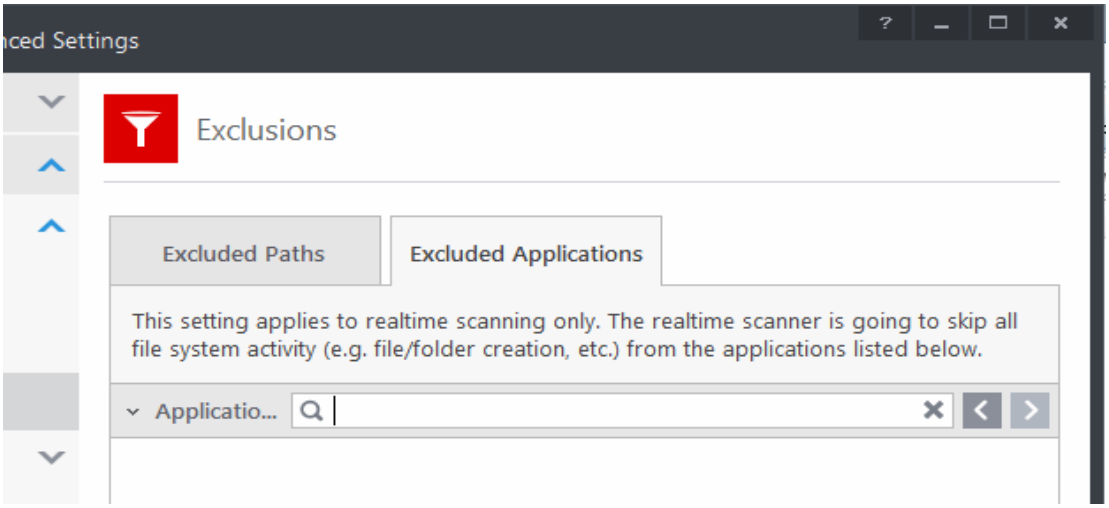
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

The 'Excluded Applications' tab allows you to manually add programs, applications of files to Excluded Applications list for excluding them from real-time scans. Also you can remove the items from Excluded Applications that were added by mistake.



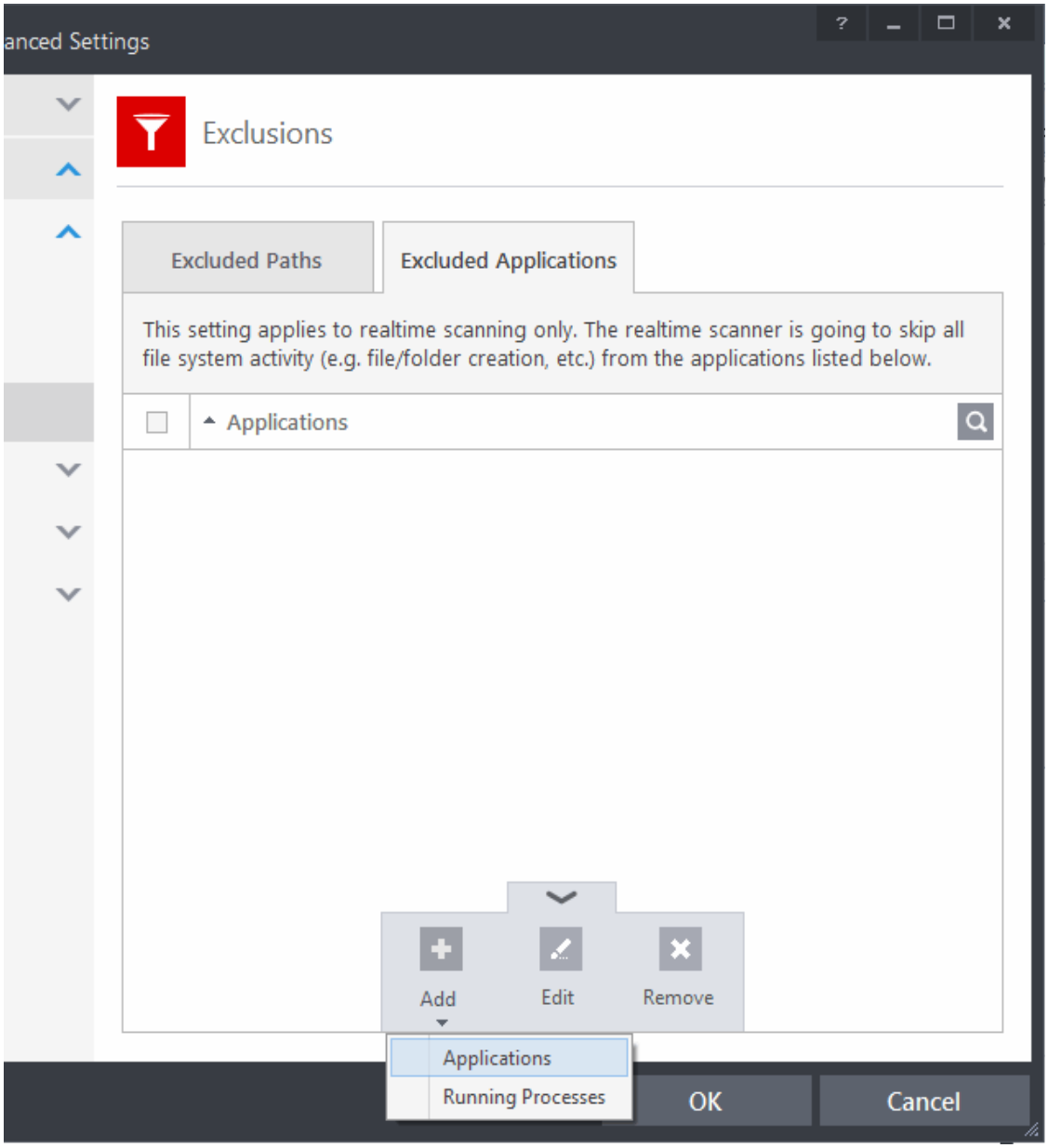
You can use the search option to find a specific excluded application from the list by clicking the search icon at the far right in the column header.



- Enter the name of the application to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

To add an item to Excluded Applications

- Click the handle from the bottom center and click on 'Add' from the options

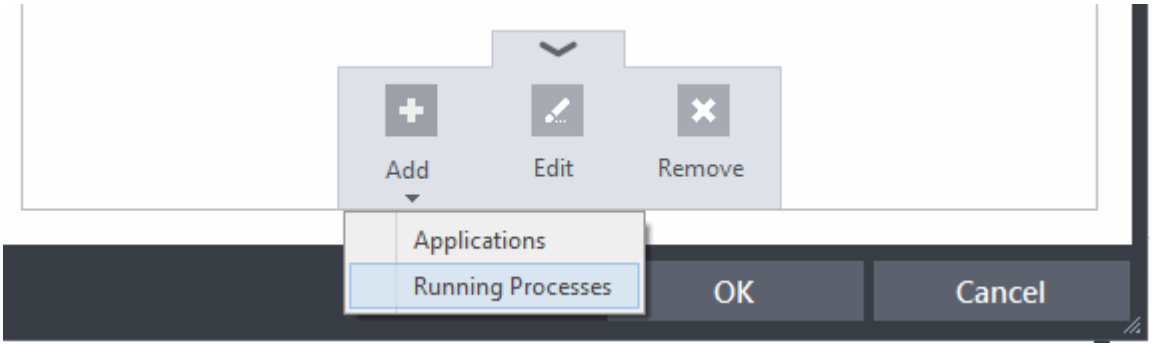


You can choose to add an application by:

- **Selecting it from the running processes** - This option allows you to choose the target application from the list of processes that are currently running on your PC.
- **Browsing your computer for the application** - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.

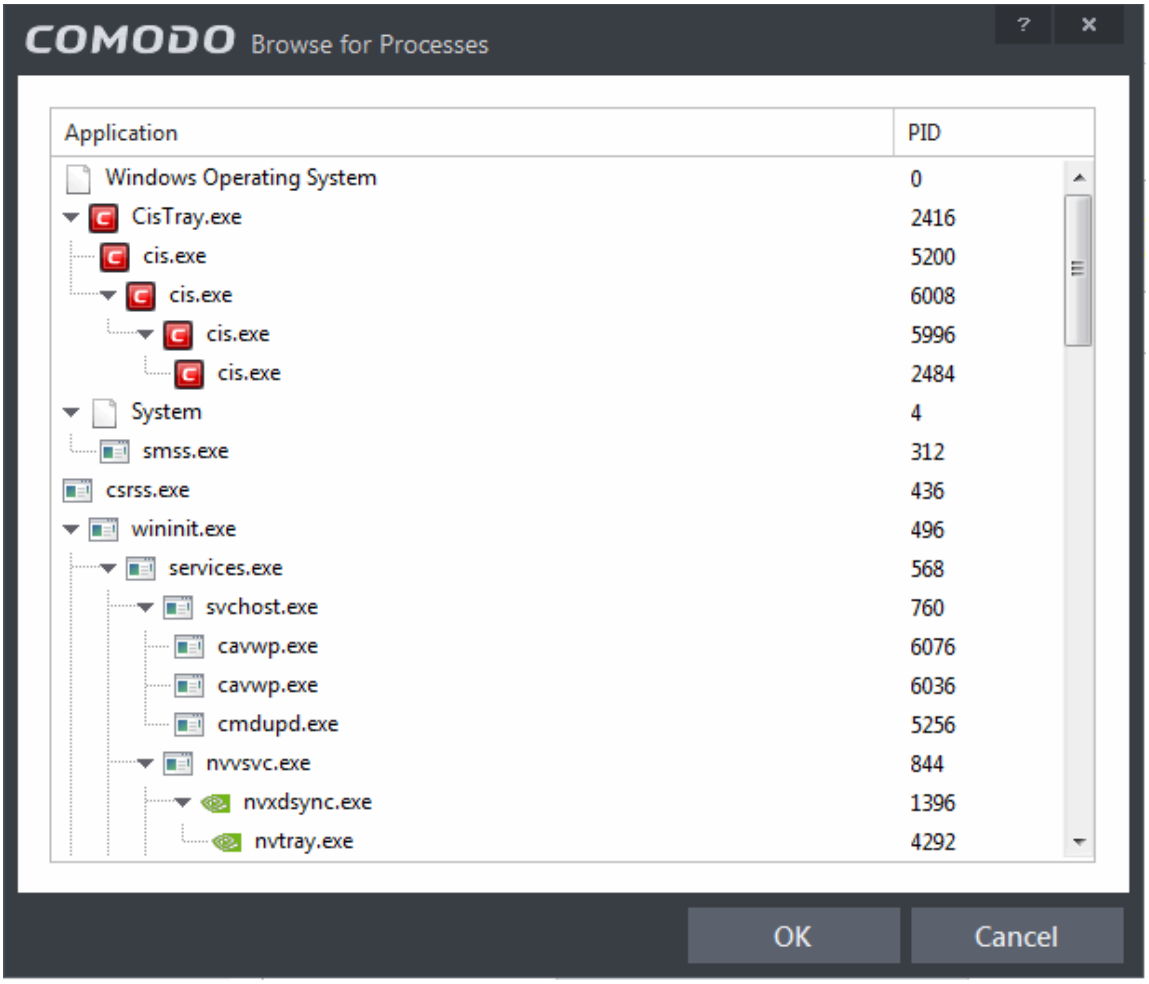
Adding an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down

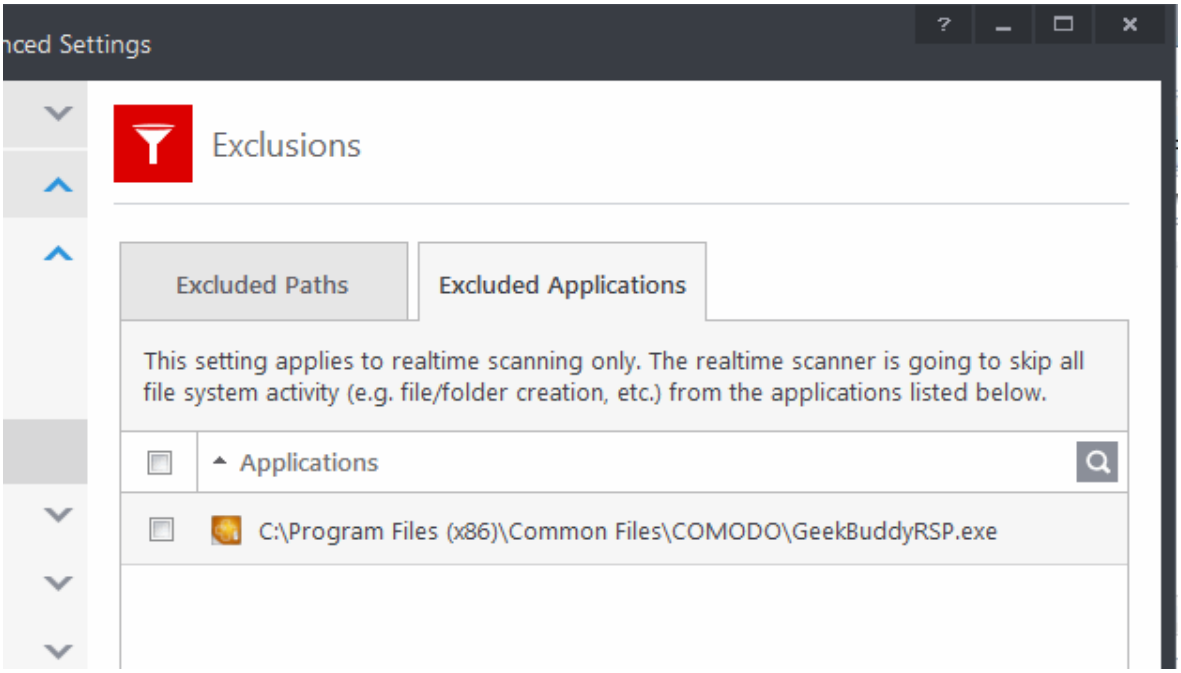


A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to excluded applications and click OK from the Browse for Process dialog.

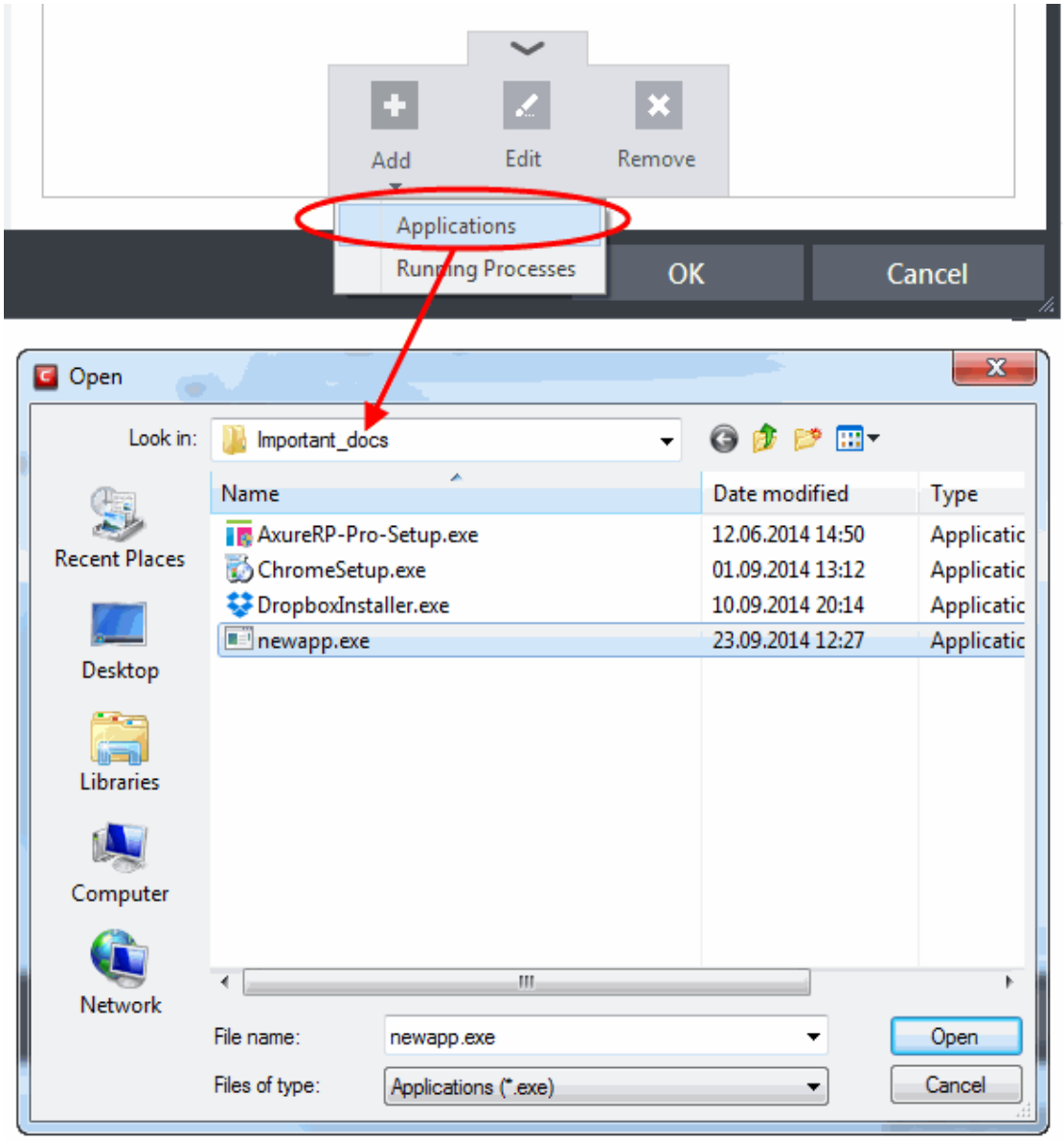


The application will be added to Excluded Applications.



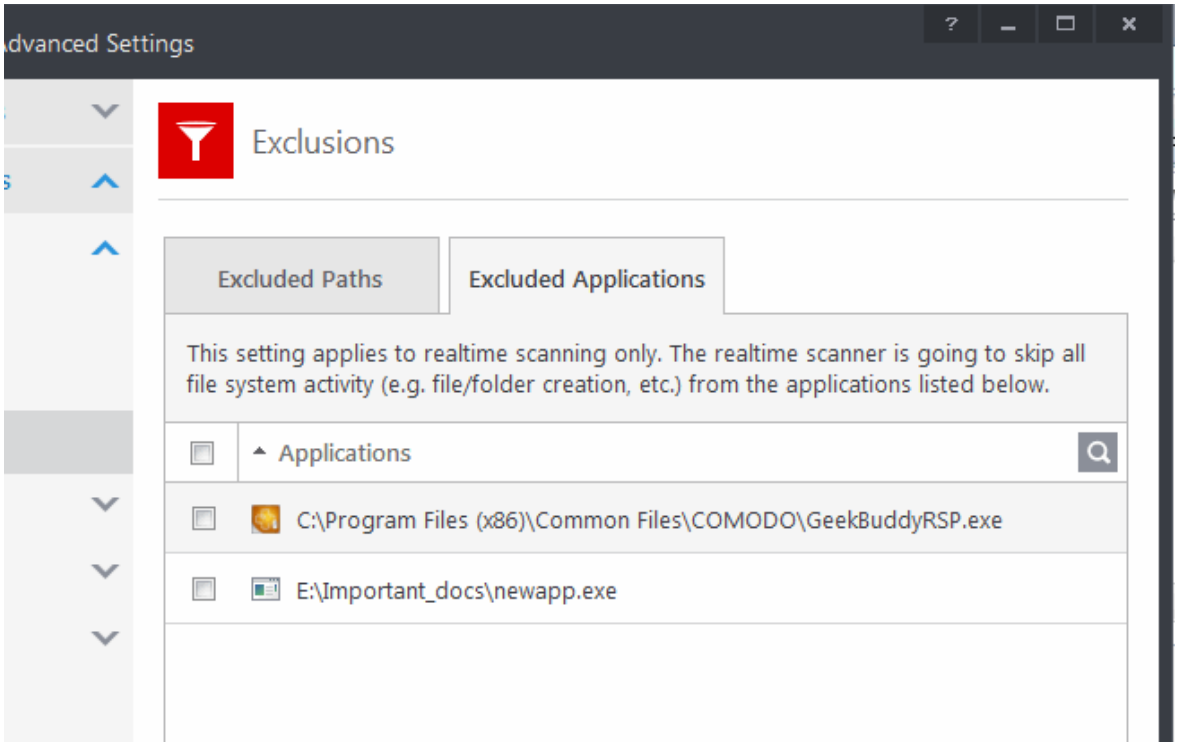
Browsing to the Application

- Choose 'Applications' from the 'Add' drop-down



- Navigate to the file you want to add to Excluded Applications in the 'Open' dialog and click 'Open'.

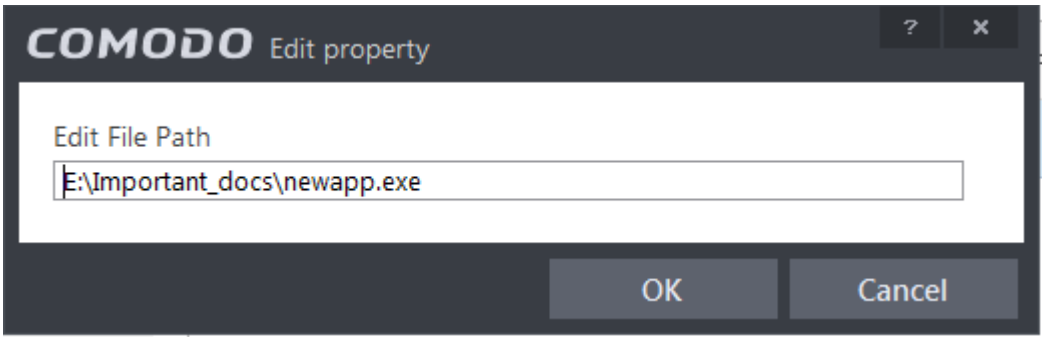
The file will be added to 'Excluded Applications'.



- Repeat process to add more items. The items will be skipped from future real-time scans.

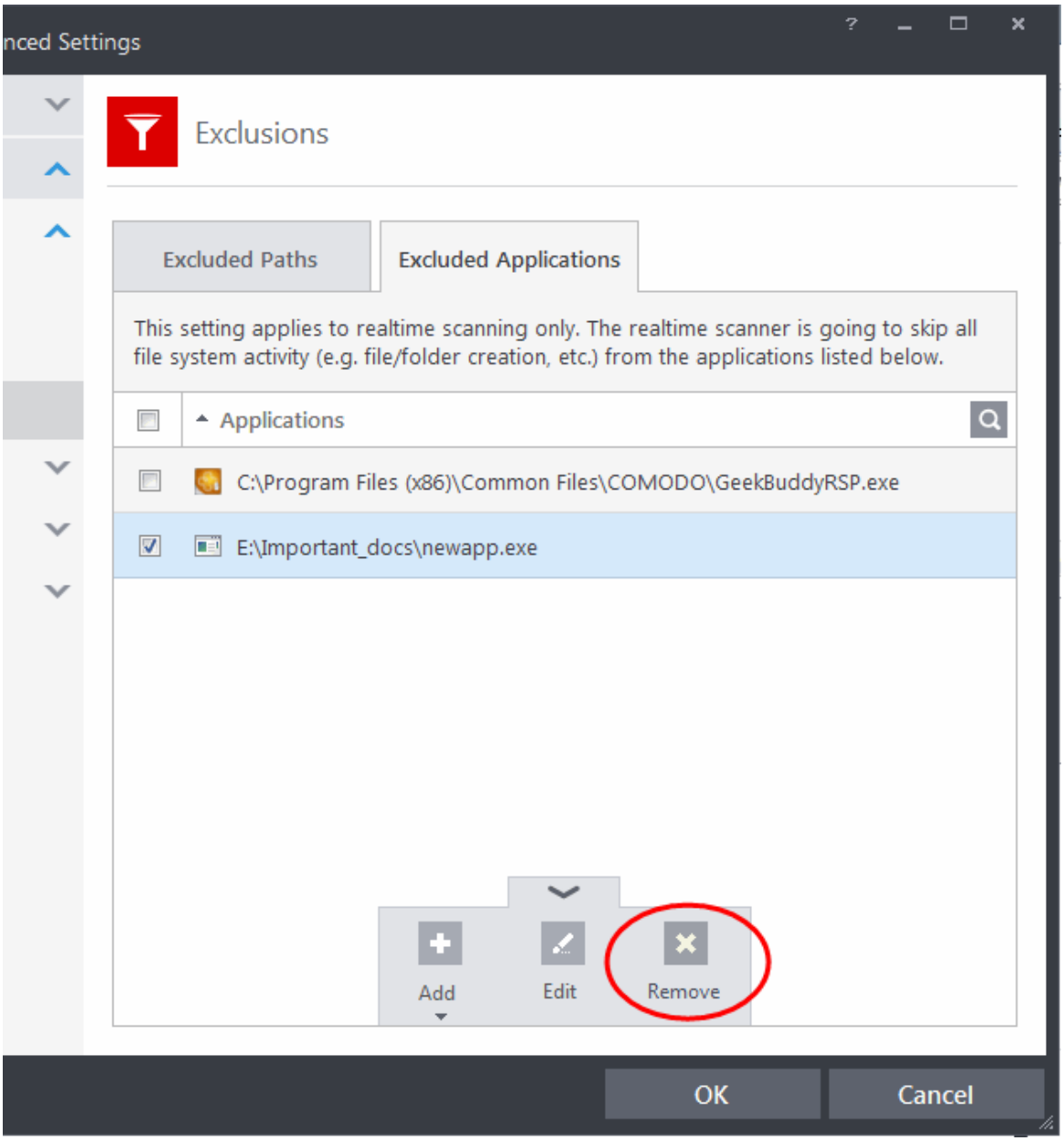
To edit the path of the application added to Excluded Application

- Select the application, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



To remove an item from the Excluded Applications

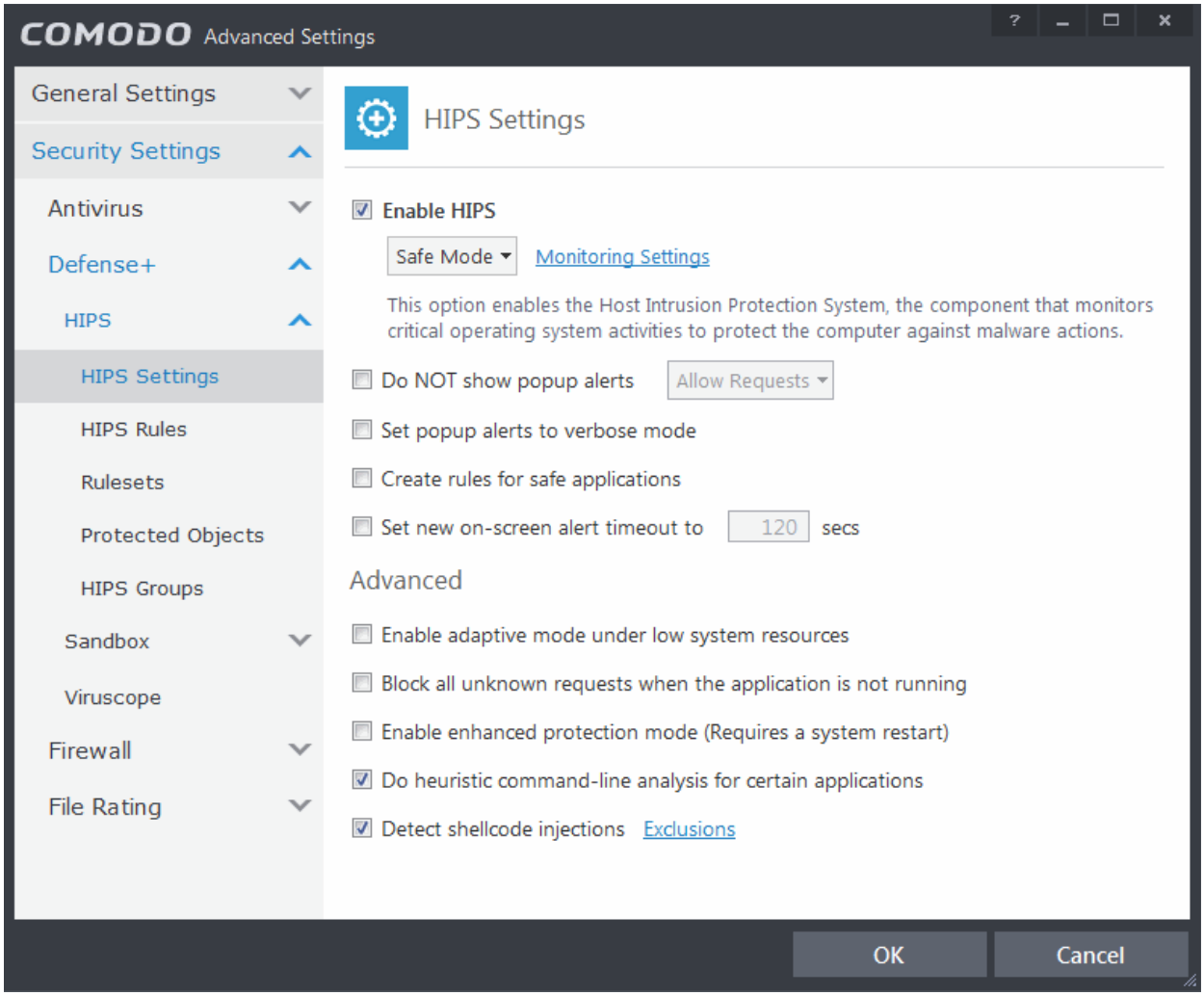
- Select the item, click the handle from the bottom center and select 'Remove'.



- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

6.2.2. Defense+ Settings

Defense+ is a collective term that covers the Host Intrusion Prevention (HIPS), Sandboxing and Viruscope components of Comodo Internet Security. Together, these technologies ensure all applications, processes and services on your PC behave in a secure manner - and are prevented from taking actions that could damage your computer or your data.



The Defense+ settings area allows you to configure the following:

- HIPS
  - **HIPS Settings**
  - **Active HIPS Rules**
  - **Predefined HIPS Rule Sets**
  - **Protected Objects**
  - **HIPS Groups**
- **Sandbox**
  - **Sandbox Settings**
  - **Rules for Auto-Sandbox**
- **Viruscope**

6.2.2.1. HIPS Settings

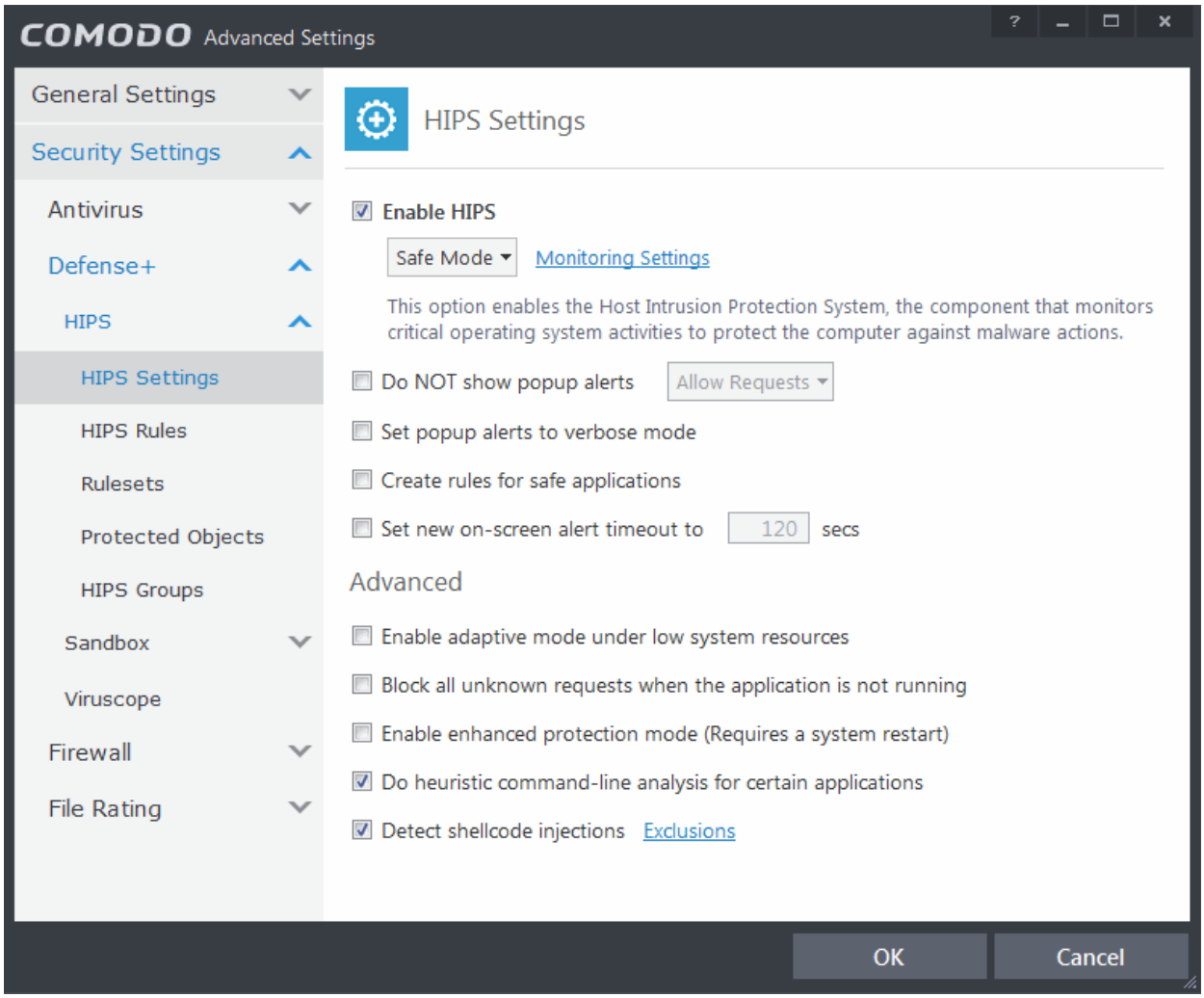
HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo Internet Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs. Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

Note for beginners: This page often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your

computer to perform a task or function. Every program, application and device you run on your computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. (e.g., when you start Microsoft Word, the executable file 'winword.exe' instructs your computer to start and run the Word application). Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data; steal your identity; corrupt system files; give control of your PC to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms.

- The HIPS Settings panel allows you to enable/disable HIPS, set its security level and configure its general behavior.
- The HIPS Settings panel can be accessed by clicking Security Settings > Defense+ > HIPS > 'HIPS Settings' tab from 'Advanced Settings' interface



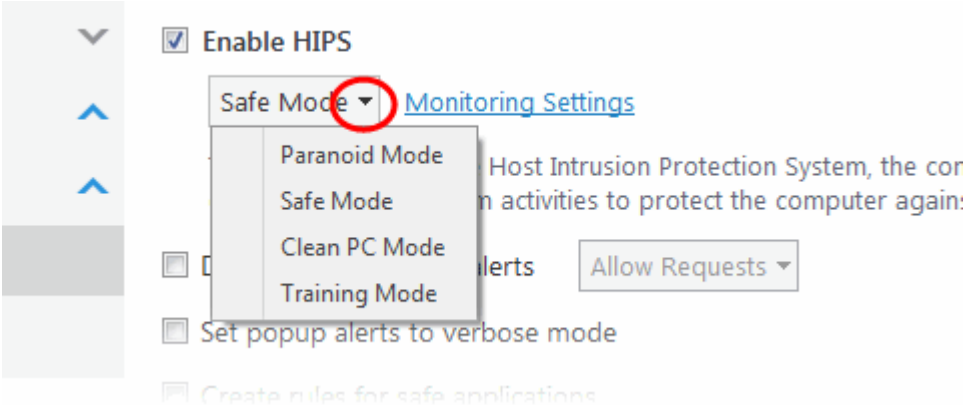
- **Enable HIPS** - Allows you to enable/disable the HIPS protection. ***(Default=Enabled)***

Note: The HIPS settings can also be configured in the 'Advanced View' of the 'Home' screen by clicking the status link beside HIPS in the 'Defense+ and Sandbox' pane.

If enabled, you can choose the security level and configure the monitoring settings for the HIPS component.

Configuring Security Level of HIPS

The security level can be chosen from the drop-down that becomes active only on enabling HIPS:



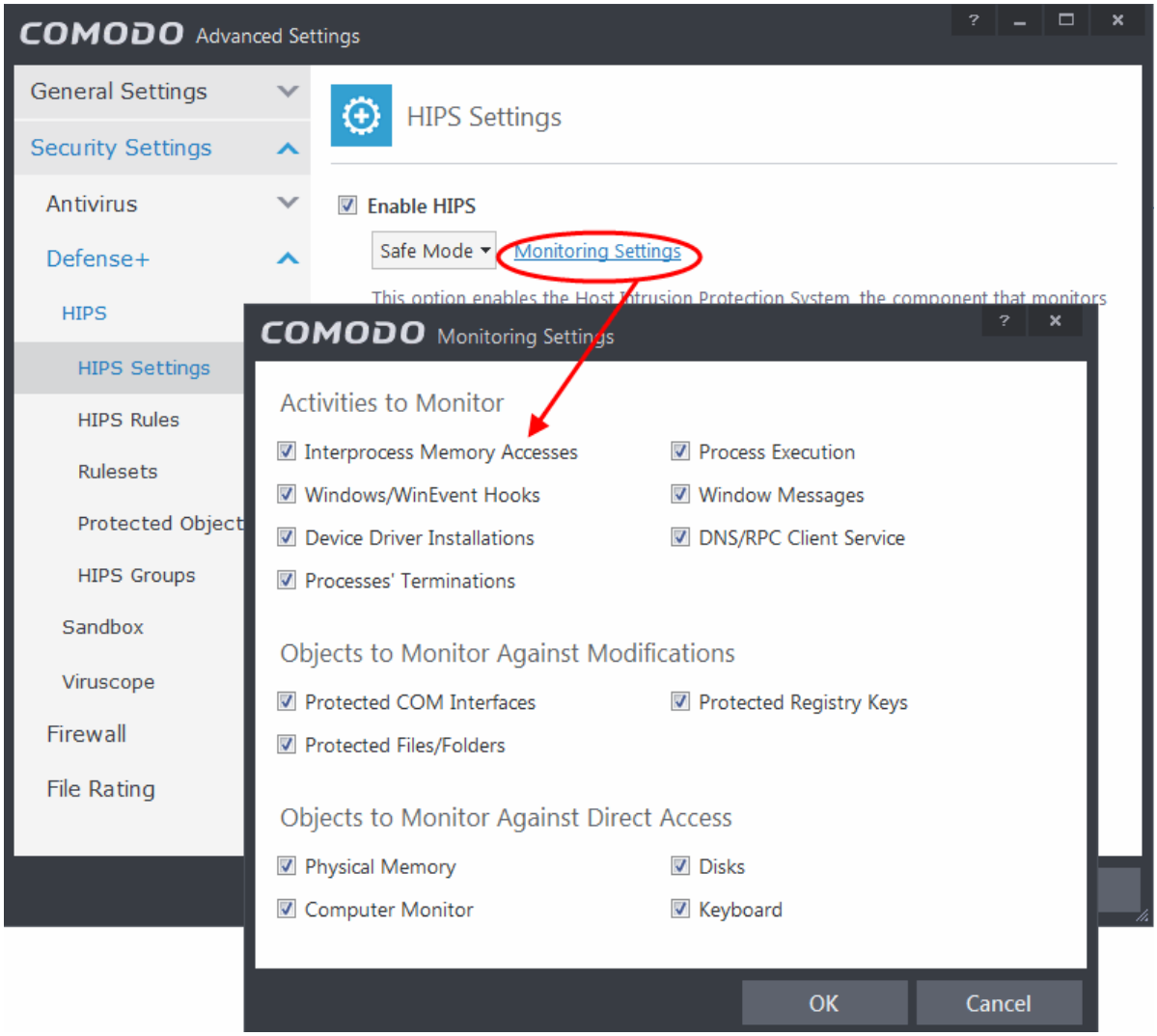
The choices available are:

- **Paranoid Mode**: This is the highest security level setting and means that Defense+ monitors and controls all executable files apart from those that you have deemed safe. Comodo Internet Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses *your* configuration settings to filter critical system activity. Similarly, the Comodo Internet Security does 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, Defense+ automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules these activities, if the checkbox '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs the Defense+ not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Clean PC Mode:** From the time you set the slider to 'Clean PC Mode', Defense+ learns the activities of the applications currently installed on the server while all new executables introduced to the server are monitored and controlled. This patent-pending mode of operation is the recommended option on a new server or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files with 'Unrecognized' rating in the **'File List** ' are excluded from being considered as clean and are monitored and controlled.
- **Training Mode**: Defense+ monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

Configuring the Monitoring Settings

The activities, entities and objects that should monitored by HIPS can be configured by clicking the Monitoring Settings link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a ***global*** basis - effectively creating a universal '**Allow**' rule for that activity . This 'Allow' setting ***over-rules*** any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the '**Access Rights**' and '**Protection Settings**' interface.



Activities To Monitor:

- **Interprocess Memory Access -** Malware programs use memory space modification to inject malicious code for numerous types of attacks, including recording your keyboard strokes; modifying the behavior of the invaded application; stealing confidential data by sending confidential information from one process to another process etc. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of the invaded process, or 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application ***(Default = Enabled)***.
- **Windows/WinEvent Hooks -** In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) *before* they reach an application. The function can act on events and, in some cases, modify or discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer; take over control of your mouse and keyboard to remotely administer your computer. Leaving this box checked means that you are warned every time a hook is executed by an untrusted application ***(Default = Enabled)***.
- **Device Driver Installations -** Device drivers are small programs that allow applications and/or operating systems to interact with a hardware device on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable damage to your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application ***(Default = Enabled)***.
- **Processes' Terminations -** A process is a running instance of a program. (for example, the Comodo Internet Security process is called 'cis.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your

system). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, Defense+ monitors and alerts you to all attempts by an untrusted application to close down another application ***(Default = Enabled)***.

- **Process Execution** - Typical malware like rootkits, keylogger etc. would often invoke by itself and runs its process mostly at the background. These processes, invisible at the foreground will act as agents for infecting your computer and to steal your confidential and sensitive information like your credit card details and passwords and pass to hackers. With this setting enabled, the HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. ***(Default = Enabled)***.
- **Windows Messages -** This setting means Comodo Internet Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) ***(Default = Enabled)***.
- **DNS/RPC Client Service -** This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby a malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' pc's which are sending out these requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack ***(Default = Enabled)***.

Background Note: DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever you type a domain name, your Internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to your computer, telling it to connect to the IP in question.

Objects To Monitor Against Modifications:

- **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the **COM Protection** pane. ***(Default = Enabled)***
- **Protected Registry Keys** enables monitoring of Registry keys you specified from the **Registry Protection** pane. ***(Default = Enabled)***.
- **Protected Files/Folders** enables monitoring of files and folders you specified from the **File Protection** pane. ***(Default = Enabled)***.

Objects To Monitor Against Direct Access:

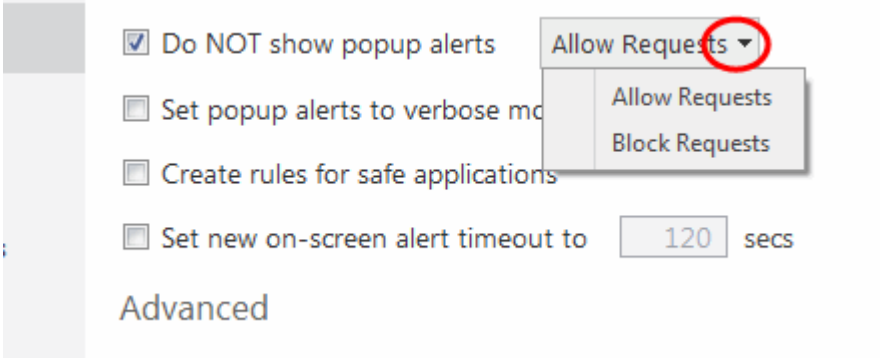
Determines whether or not Comodo Internet Security should monitor access to system critical objects on your computer. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:

- **Physical Memory:** Monitors your computer's memory for direct access by an applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code ***(Default = Enabled)***.
- **Computer Monitor:** Comodo Internet Security raises an alert every time a process tries to directly access your computer monitor. Although legitimate applications sometimes require this access, there is also an emerging category of spyware programs that use such access to monitor users' activities. (for example, to take screen shots of your current desktop; to record your browsing activities etc) ***(Default = Enabled).***
- **Disks:** Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data ***(Default = Enabled)***.
- **Keyboard:** Monitors your keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Internet Security alerts you every time an application attempts to establish direct access to your keyboard ***(Default = Enabled)***.

Checkbox Options

- **Do NOT show popup alerts** - Configure whether or not you want to be notified when the HIPS encounters a malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness ***(Default = Disabled).***

  If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Requests' or 'Allow Requests'.



- **Set popup alerts to verbose mode** - Enabling this option instructs CIS to display HIPS Alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests ***(Default = Disabled).***
- **Create rules for safe applications -** Automatically creates rules for safe applications in HIPS Ruleset ***(Default = Disabled).***

Note: HIPS trusts the applications if:

- The application/file is rated as 'Trusted' in the **File List**
- The application is from a vendor included in the **Trusted Software Vendors** list
- The application is included in the extensive and constantly updated Comodo safelist.

By default, CIS does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

Enabling this checkbox instructs CIS to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the **HIPS Rules** interface. The Advanced users can edit / modify the rules as they wish.

Background Note: Prior to version 4.x , CIS would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CIS version 3.x).

- **Set new on-screen alert time out to**: Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced HIPS Settings

- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. With this option enabled, CIS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, the cost of enabling this option may be reduced performance in even lightly loaded systems ***(Default = Disabled)***.
- **Block all unknown requests if the application is closed -** Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked. ***(Default = Disabled)***
- **Enable enhanced protection mode** - On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to countermeasure extremely sophisticated malware that tries to bypass regular

countermeasures. Because of limitations in Windows 7/8 x64 systems, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. CIS requires a system restart for enabling enhanced protection mode. (***Default = Disabled***)

- **Do heuristic command-line analysis for certain applications** - Selecting this option instructs Comodo Internet Security to perform heuristic analysis of programs that are capable of executing code such as visual basic scripts and java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscipt.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CIS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the Internet, for example, the alert will state 'test.vbs' is attempting to connect to the Internet (***Default = Enabled***).
- If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the Internet'.

Background note: 'Heuristics' describes the method of analyzing a file to ascertain whether it contains codes typical of a virus. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. This helps to identify previously unknown (new) viruses.

- **Detect shellcode injections (i.e. Buffer overflow protection)** - Enabling this setting turns-on the Buffer over flow protection.

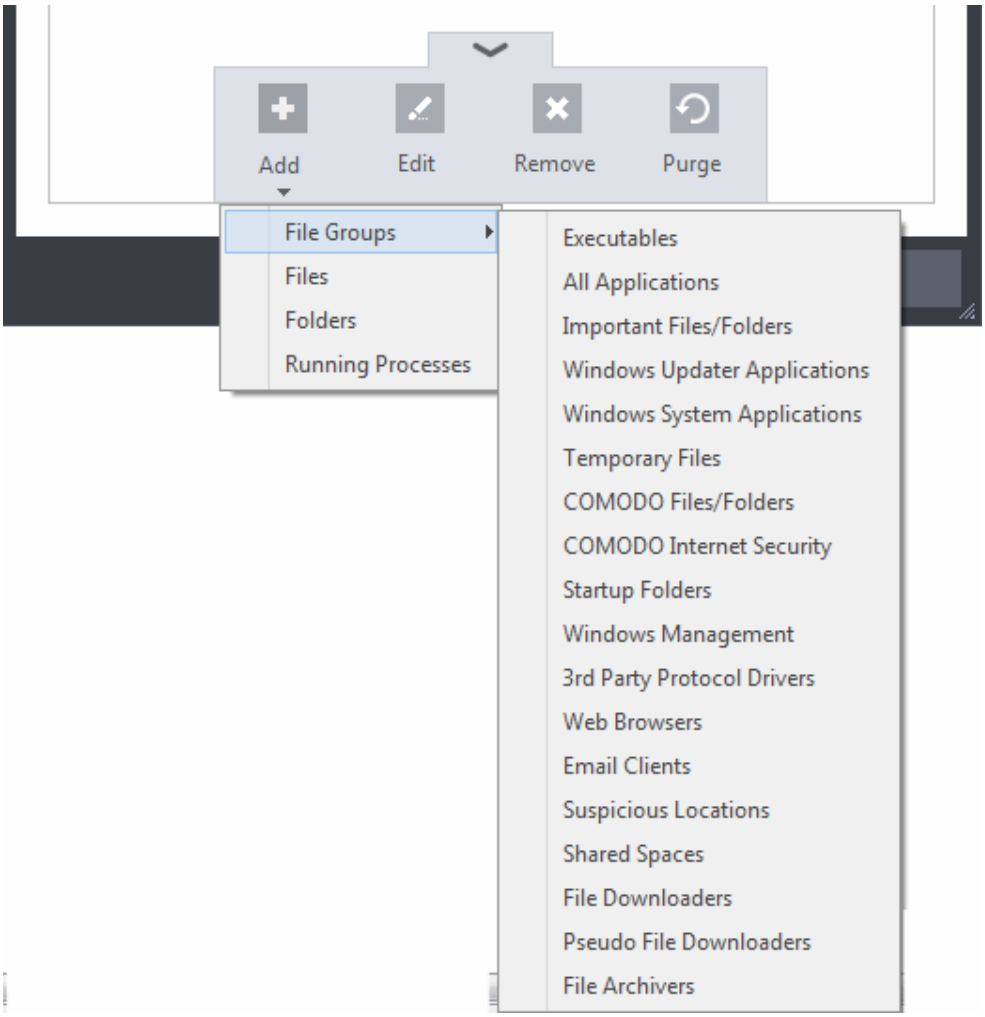
Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

Turning-on buffer overflow protection instructs the Comodo Internet Security to raise pop-up alerts in every event of a possible buffer overflow attack. You can allow or deny the requested activity raised by the process under execution depending on the reliability of the software and its vendor.

Comodo recommends that this setting to be maintained selected always (Default = Enabled).

To exclude some of the file types from being monitored under Detect Shellcode injections.

- Select the 'Detect shellcode injections' checkbox and click the Exclusions link. The 'Manage Exclusions' dialog will appear.



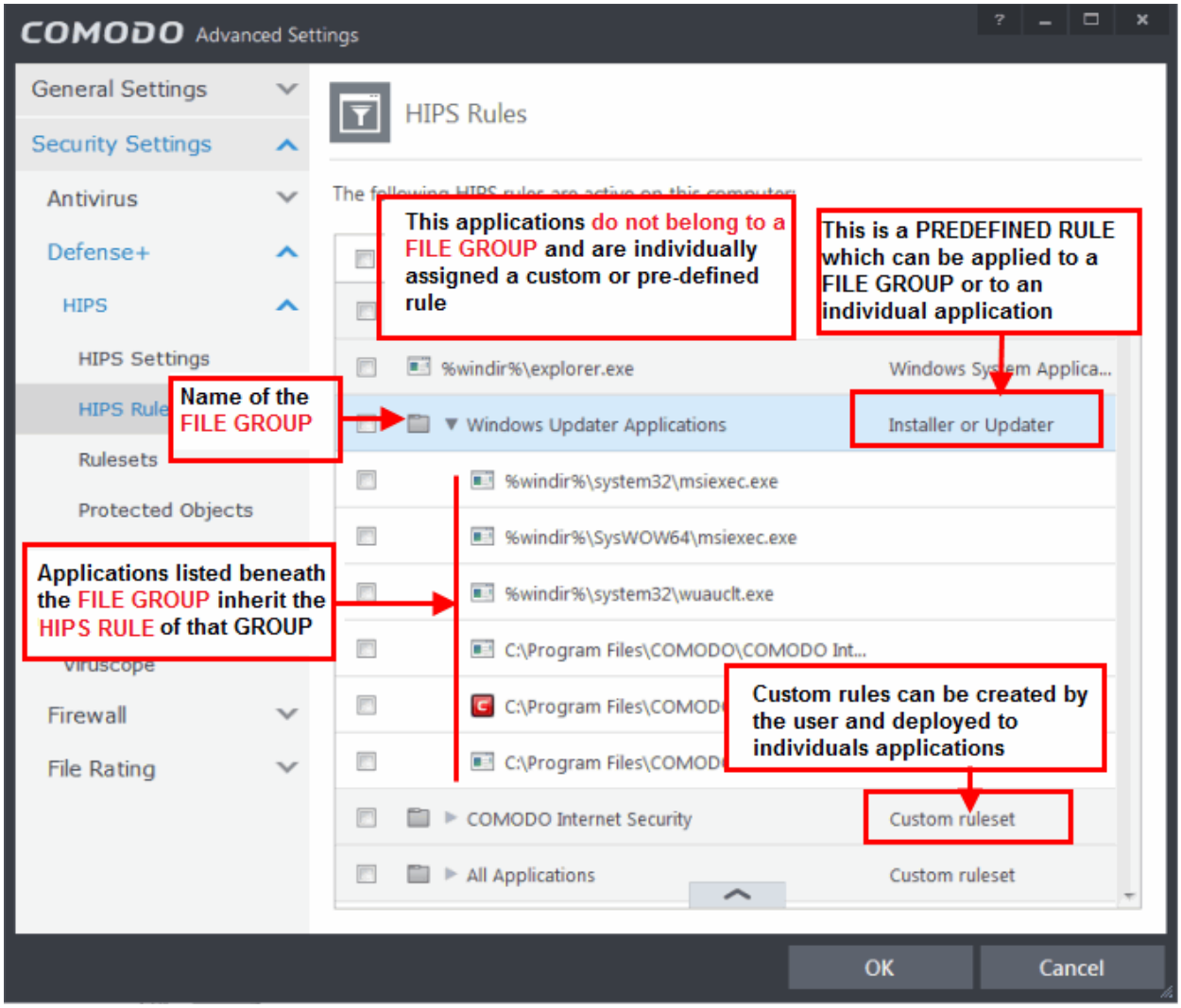
- Click the handle from the bottom of the interface and choose 'Add'
- You can add items by selecting the required option from the drop-down:
  - **File Groups** - Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl. Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. For more details on file groups, refer to the section **File Groups**.
  - **Running Processes** - As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.
  - **Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
  - **Files** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.

Note: These settings are recommended for advanced users only.

- Click 'OK' to implement your settings.

6.2.2.2. Active HIPS Rules

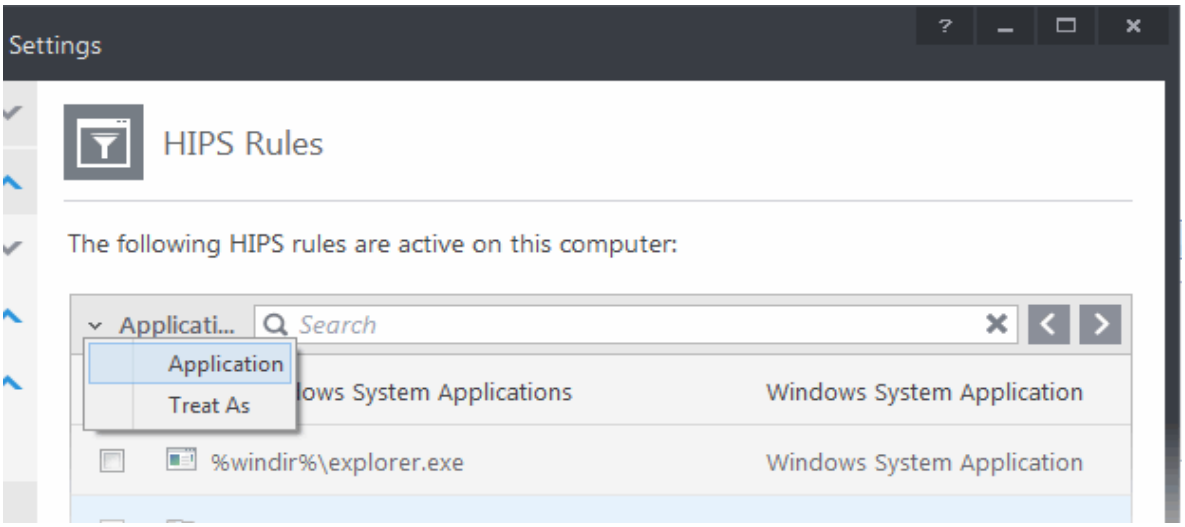
The HIPS rules tab lists the different groups of applications installed in your system and the Rulesets applied to them. You can change the ruleset applied to selected applications and also create custom rulesets to be applied to selected applications.



The first column, **Application Name**, displays a list of the applications on your system for which a HIPS ruleset has been deployed. If the application belongs to a file group, then all member applications assume the ruleset of the file group. The second column, **Treat as**, column displays the name of the HIPS ruleset assigned to the application or group of applications in column one.

You can use the search option to find a specific file or a company in the list.

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



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.

- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

General Navigation:

Clicking the Up arrow at the bottom center of the interface opens an option panel with the following options:

- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **Remove** - Deletes the selected ruleset.

Note: You cannot remove individual applications from a file group using this interface - you must use the '**File Groups**' interface to do this.

- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

Users can re-order the priority of rules by simply selecting the application name or file group name in question, clicking the handle at the bottom center and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the '**File Groups**' interface.

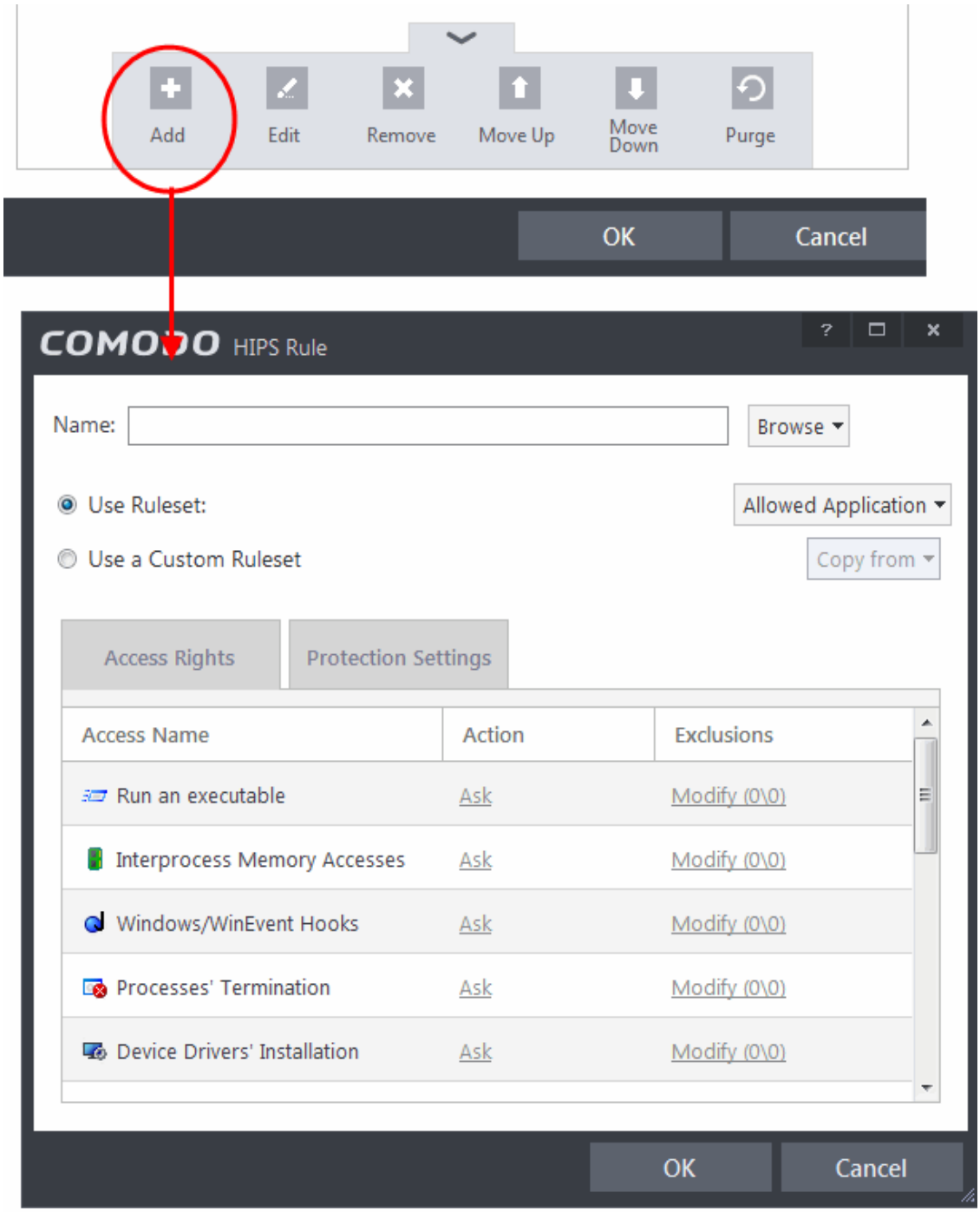
Creating or Modifying a HIPS Ruleset

To begin defining an application's HIPS Ruleset

1. **Select the application or file group that you wish the ruleset to apply to.**
2. **Configure the ruleset for this application.**

Step 1 - Select the application or file group that you wish the ruleset to apply to

If you wish to define a rule for a new application (i.e. one that is not already listed), click the handle from the **HIPS Rules pane** and select 'ADD'. This brings up the 'HIPS Rule' interface as shown below.

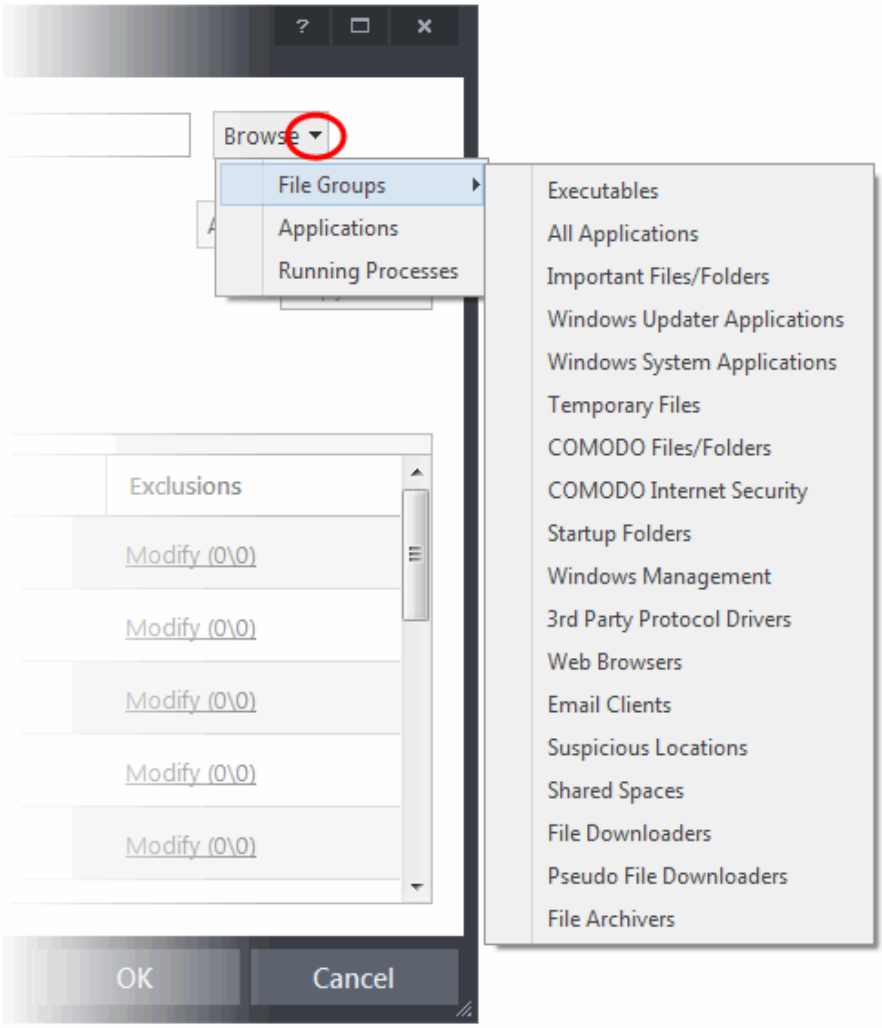


Because you are defining the HIPS rule settings for a new application, you can notice that the 'Name' box is blank. (If you were editing an existing rule instead, then this interface would show that application's name with installation path or application group's name.)

- Click 'Browse' to begin.

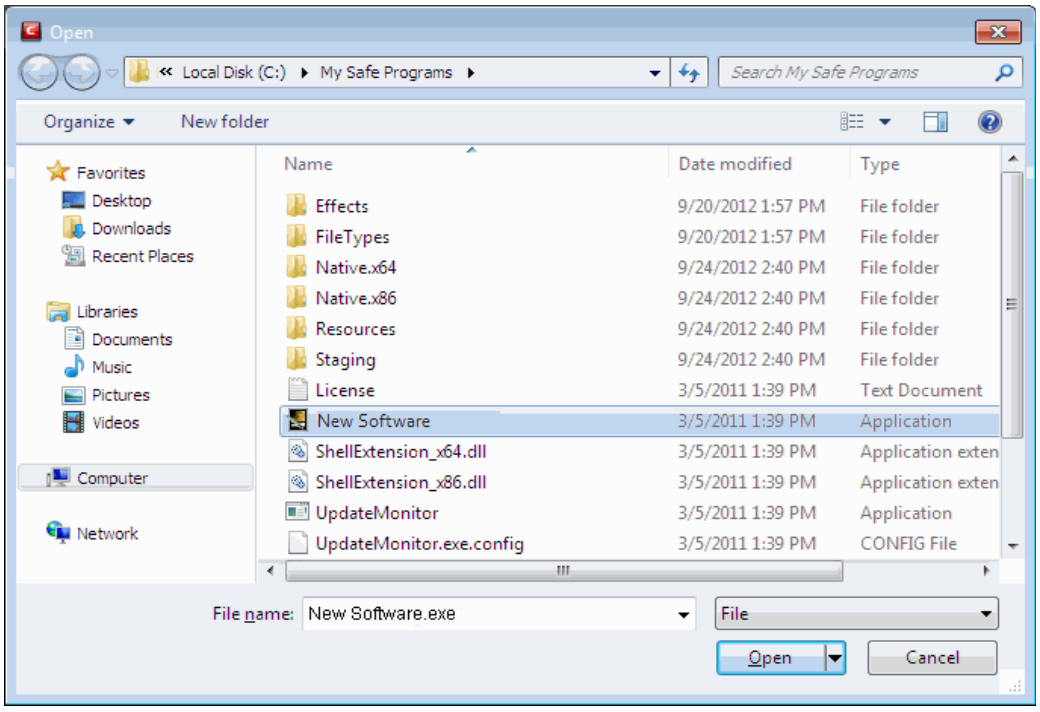
You now have 3 methods available to choose the application for which you wish to create a Ruleset - **File Groups**; **Applications** and **Running Processes**.

1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

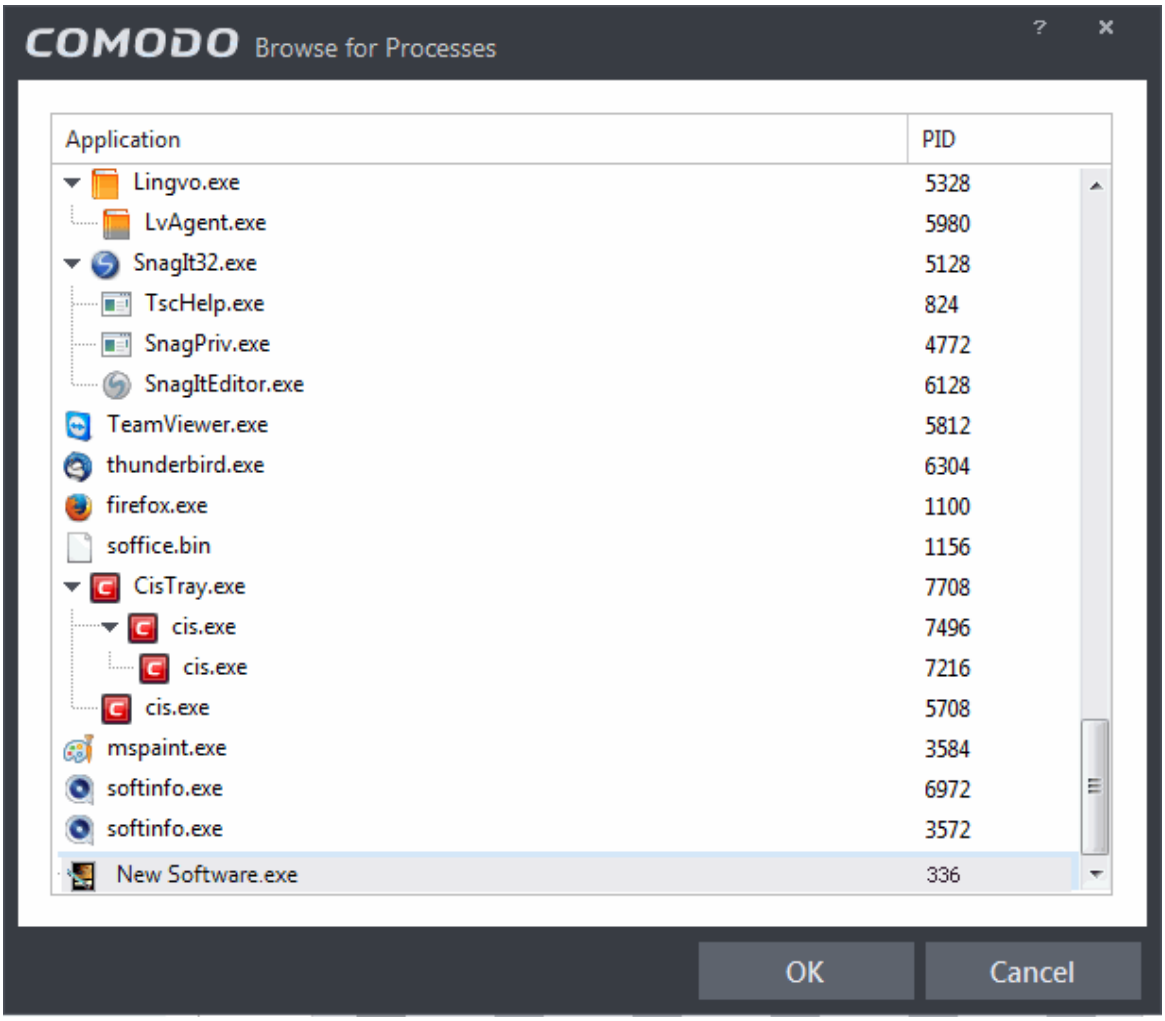


To view the file types and folders that are affected by choosing one of these options, you need to visit the '**File Groups**' interface.

2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.



3. **Running Processes** - as the name suggests, this option allows you to create and deploy a ruleset for any process that is currently running on your PC.

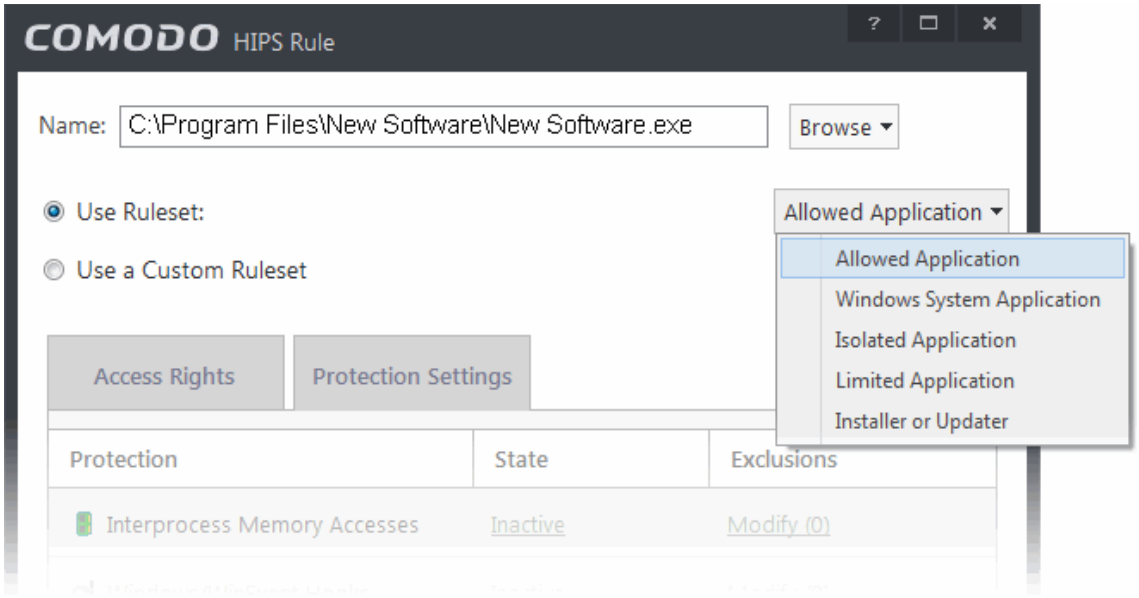


Having selected the individual application, running process or file group, the next stage is to Configure the rules for this ruleset.

Step 2 - Configure the HIPS Ruleset for this application

There are two broad options available for selecting a ruleset that applies to an application - **Use Ruleset** or **Use a Custom Ruleset**.

1. **Use Ruleset** - Selecting this option allows the user to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the **HIPS Rules** interface ***(Default = enabled).***



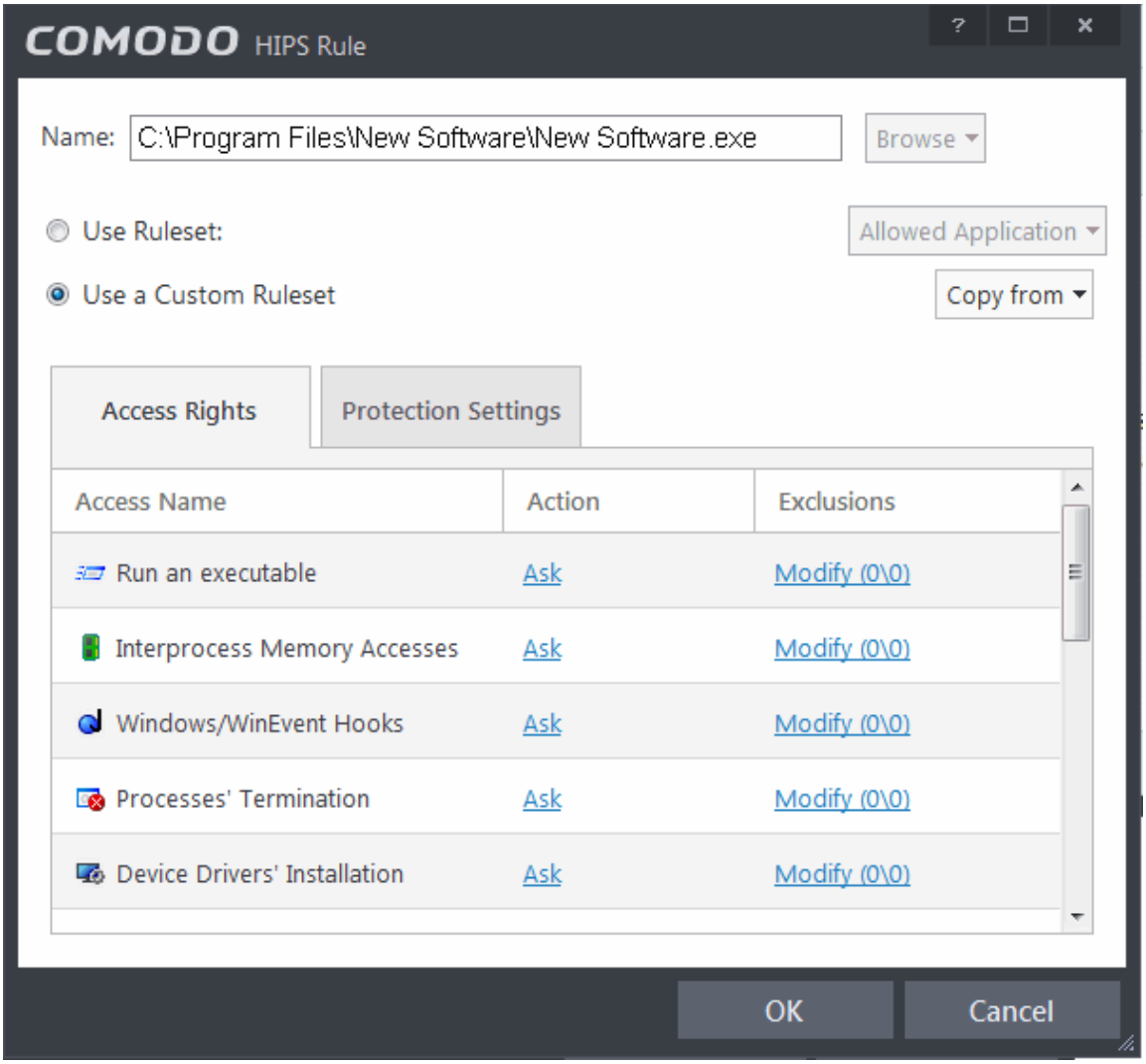
Note on 'Installer or Updater' Rule : Applying the Predefined Ruleset 'Installer or Updater' for an application defines it as a trusted installer and all files created by the application will also be considered as trusted files. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo advises you to use this Predefined Ruleset - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.

General Note: Predefined Rulesets, once chosen, cannot be modified directly from this interface - they can only be modified and defined using the '**Rulesets**' interface. If you require the ability to add or modify settings for an specific application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use a Custom Ruleset** option instead.

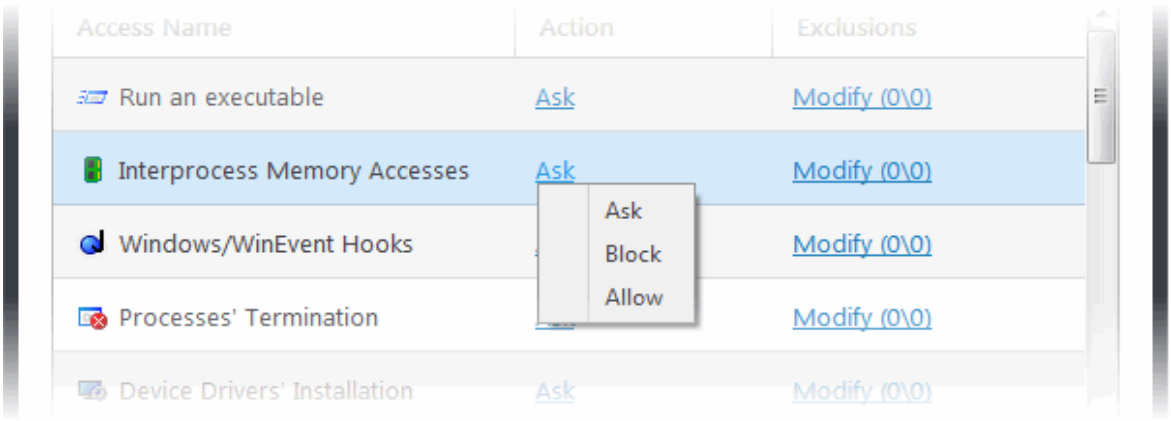
2. **Use a Custom Ruleset** - designed for more experienced users, the 'Custom Ruleset' option enables full control over the configuration specific security ruleset and the parameters of each rule within that ruleset. The Custom ruleset has two main configuration areas - **Access Rights** and **Protection Settings** ***(Default = Disabled).***

   In simplistic terms 'Access Rights' determine what the application *can do* to other processes and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

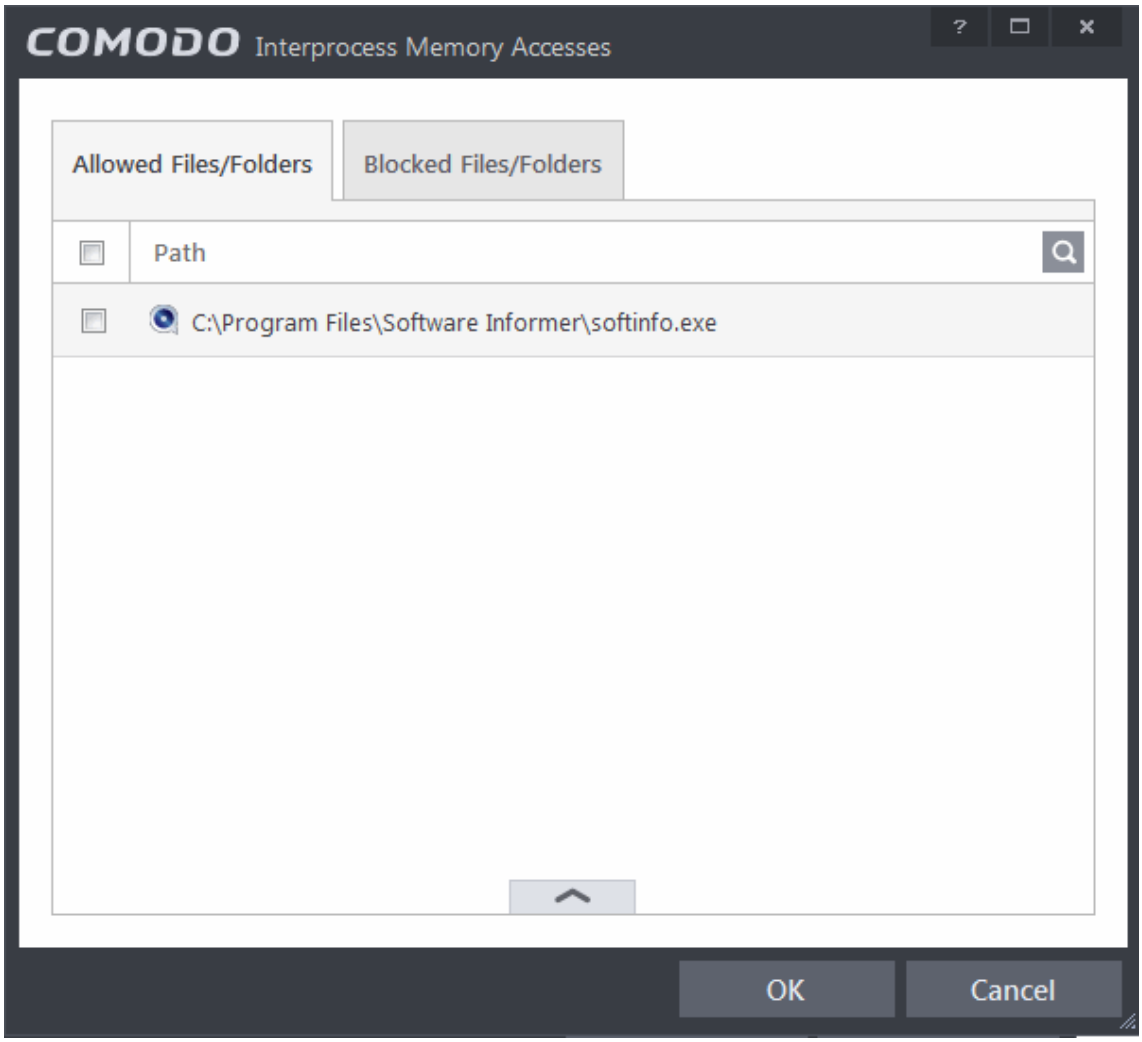
   i. **Access Rights** - The Process Access Rights tab allows you to determine what activities the applications in your custom ruleset are allowed to execute. These activities are called 'Access Names'.



Refer to the section **HIPS Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:



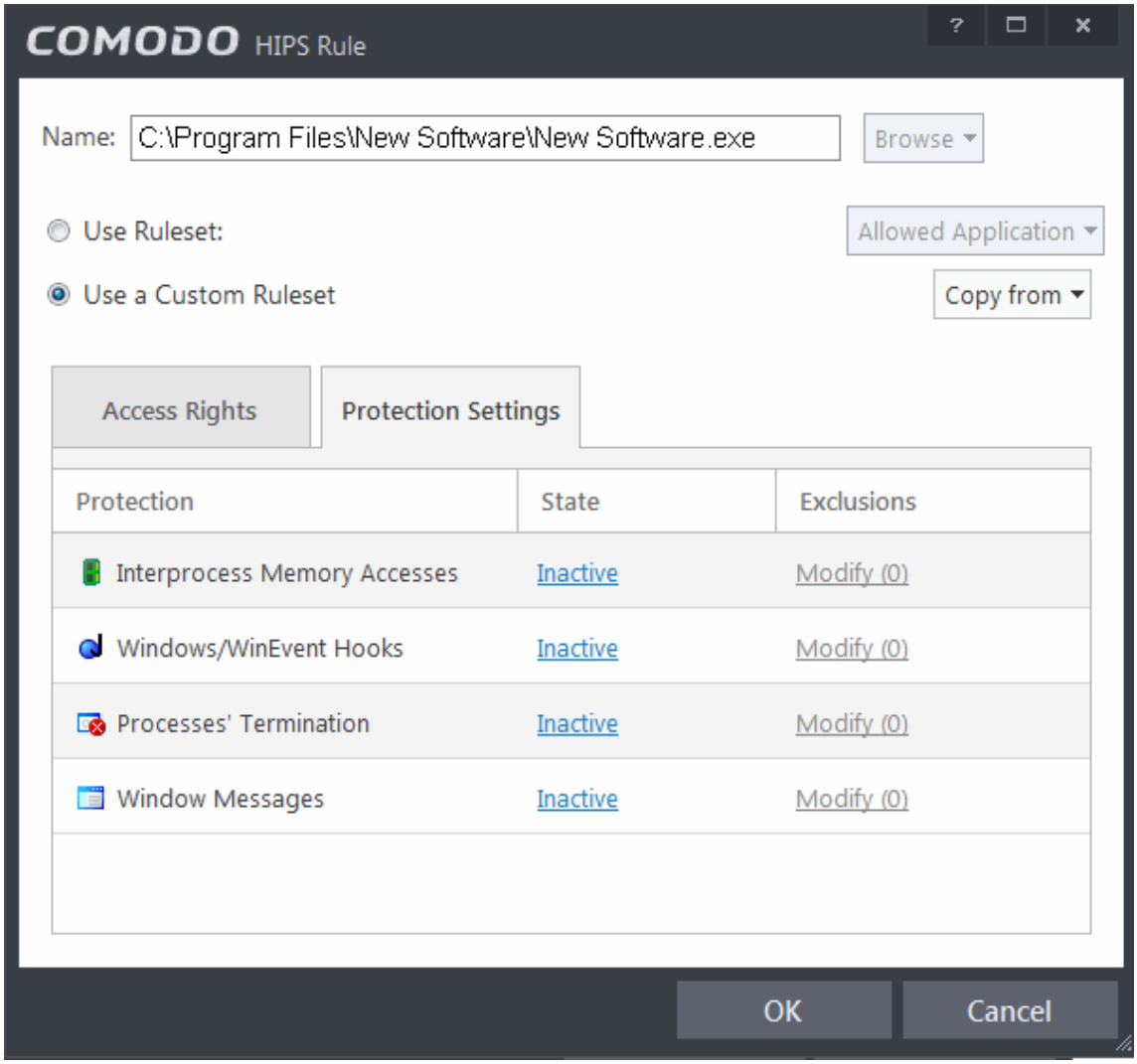
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.



Clicking the handle and selecting 'Add' allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

In **the example above**, the default action for '*Interprocess Memory Access*' is '*Ask*'. This means HIPS will generate an alert asking your permission if 'New Software.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'opera.exe' to the 'Allowed Applications' tab creates an exception to this rule. New Software.exe can now modify the memory space of opera.exe.

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection Type' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

6.2.2.3. HIPS Rule Sets

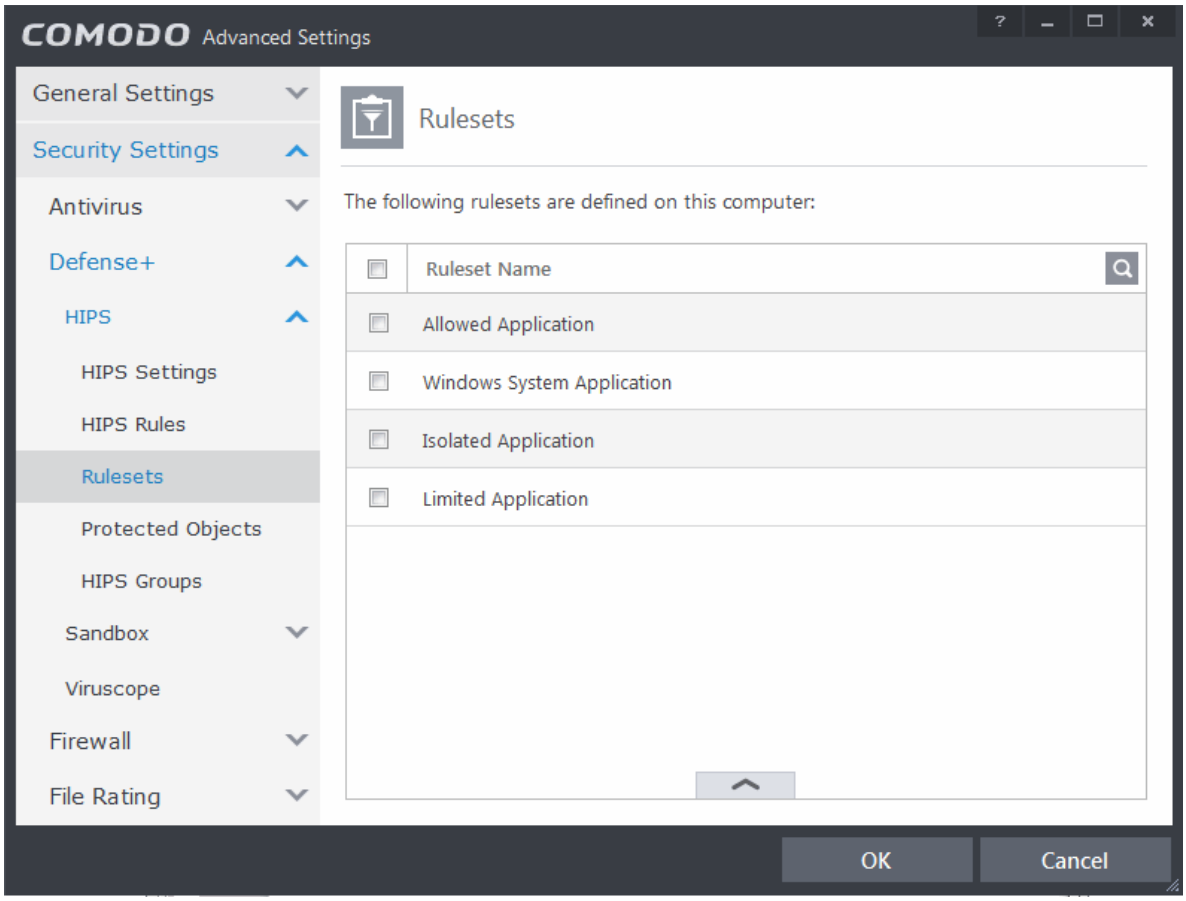
A Pre-defined ruleset is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined rulesets' is a set of rulesets that concern an application's access rights to memory, other programs, the registry etc.

Note: This section is for advanced and experienced users. If you are a novice user to Comodo Internet Security, we advise you first read the **Active HIPS Rules** section in this help guide if you have not already done so.

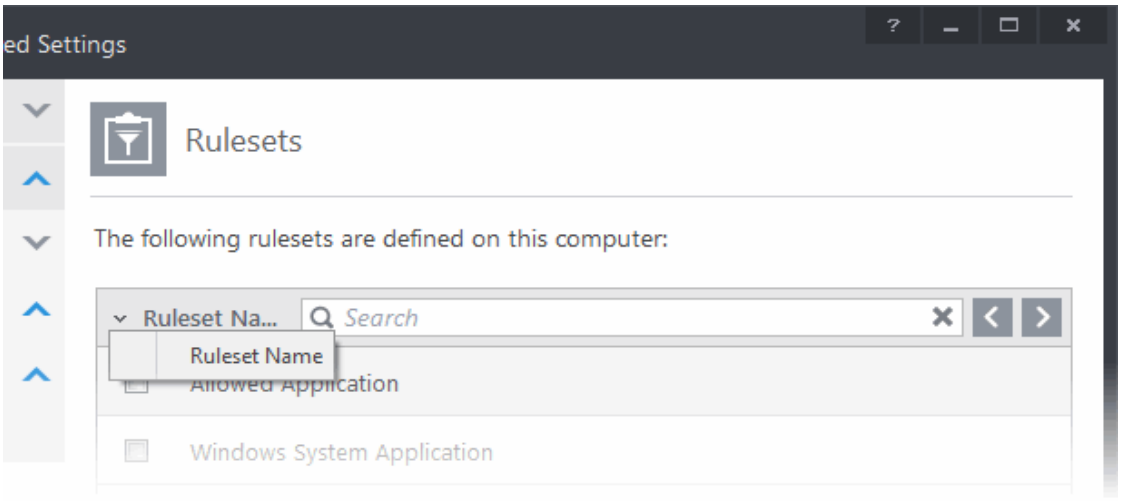
Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Internet Security contains a selection of rulesets according to broad application categories. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements.

To configure this category

- Navigate to: Advanced Tasks > Security Settings >Defense+ > HIPS > Rulesets. There are four default Rulesets listed under the 'Rules' column.



You can use the search option to find a ruleset in the list by clicking the search icon at the far right in the column header.



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

To view or edit an existing predefined ruleset

- Double click on the Ruleset in the list

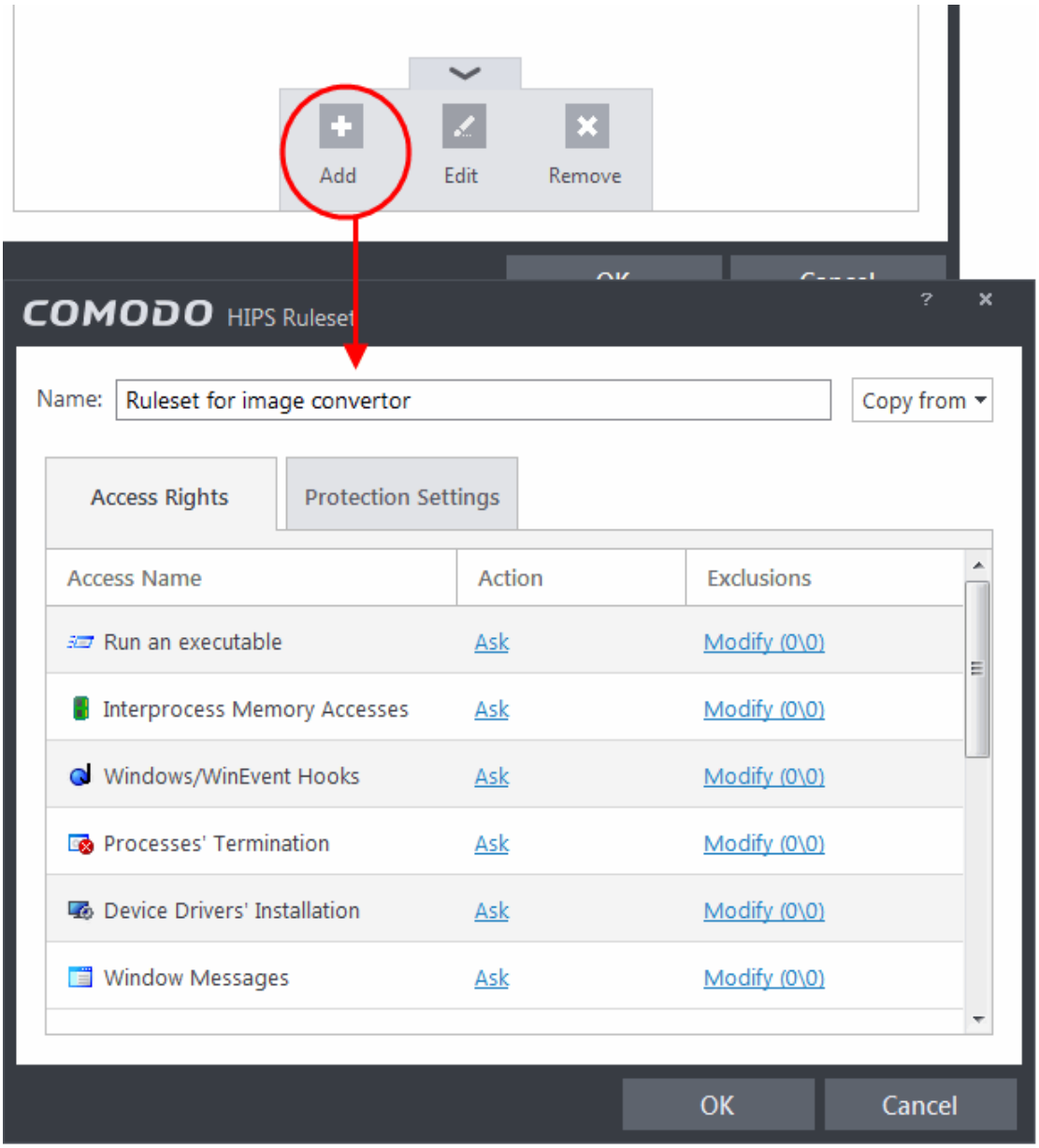
or

- Select the Ruleset, click the handle at the bottom of the interface and choose 'Edit' from the options.

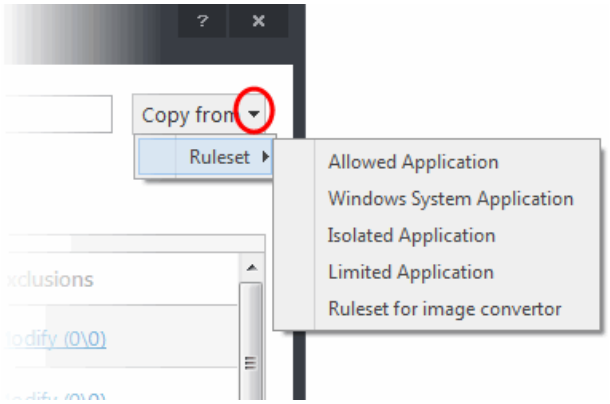
From here, you can modify a ruleset and, if desired, make changes to its **'Access Rights' and 'Protection Settings'**. Any changes you make here are automatically rolled out to all applications that are currently applied with the ruleset.

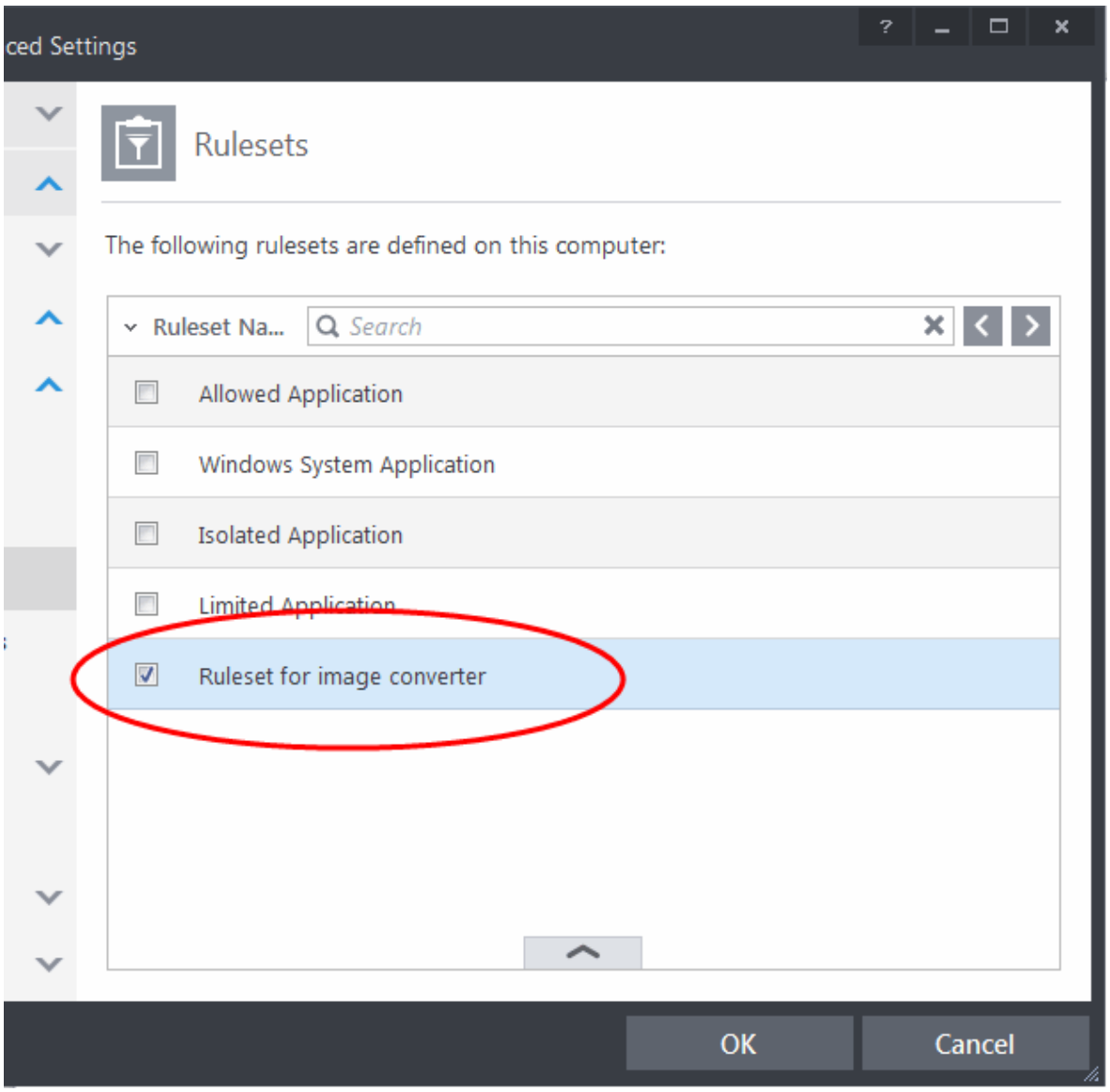
To create a new predefined ruleset

- Click the handle at the bottom of the interface and choose 'Add' from the options.



- Enter a name for the new ruleset.
- To copy the **Access Rights** and **Protection Settings** from another pre-existing ruleset, click 'Copy From' and select the ruleset from the drop-down
- To customize the **Access Rights** and **Protection Settings** as per the requirements of this new rule set, follow the procedure explained in the section **Use a Custom Ruleset**.
- Click OK to save the new ruleset.



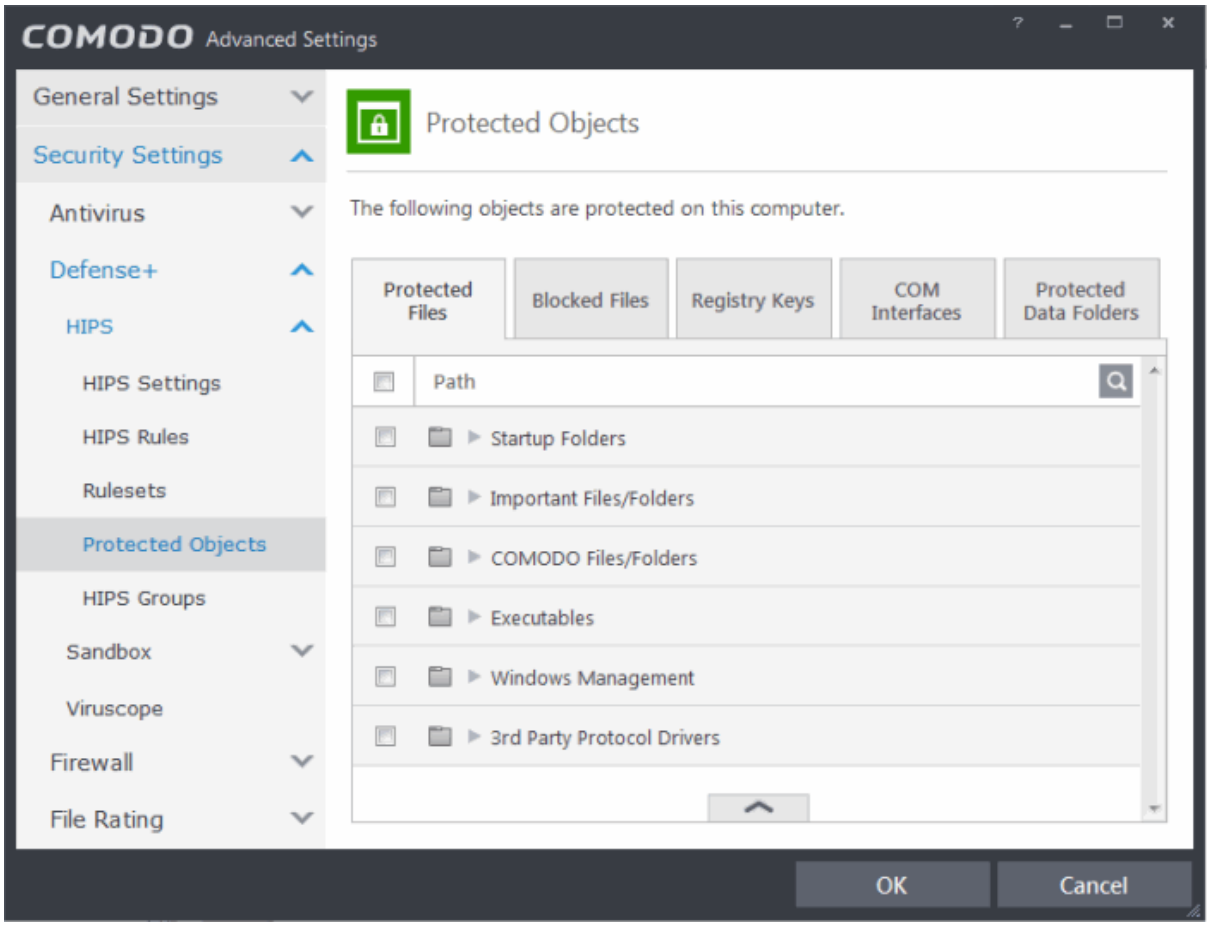


Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.

6.2.2.4. Protected Objects

The Protected Objects panel allows you to protect specific files and folders, system critical registry keys and COM interfaces against access or modification by unauthorized processes and services. You can also add files in Protected Data Folders, so that Sandboxed programs will be blocked from accessing them.

The Protected Objects panel can be accessed by clicking Security Settings > Defense+ > HIPS > Protected Objects from the Advanced Settings interface.



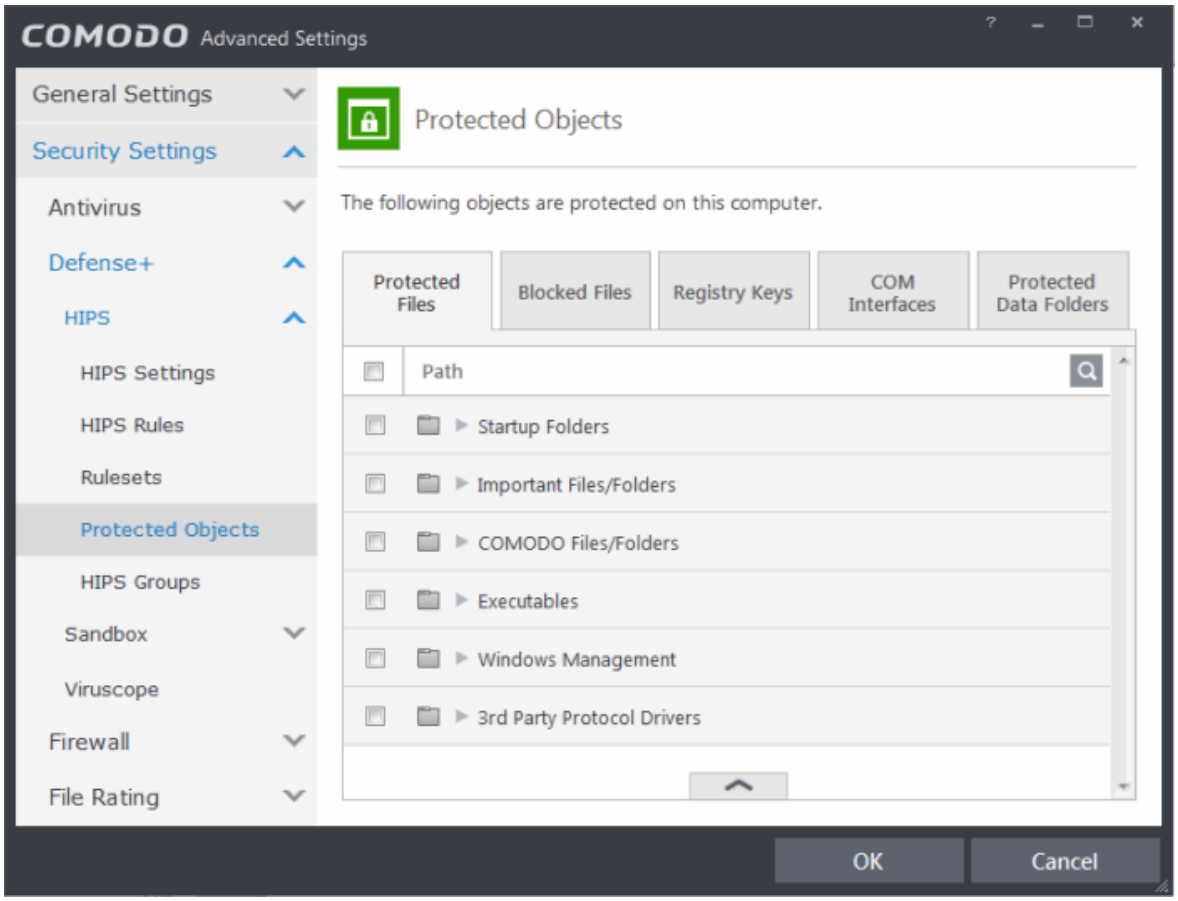
The panel has five tabs:

- **Protected Files** - Allows you to specify programs, applications and files that are to be protected from changes
- **Blocked Files** - Allows you to specify programs, applications and files that are to be blocked from execution and opening
- **Registry Keys** - Allows you to specify registry keys that are to be protected from changes
- **COM Interfaces** - Allows you to specify COM interfaces that are to be protected from changes
- **Protected Data Folders** - Allows you to specify folders containing data files that are to be protected from changes by Sandboxed programs

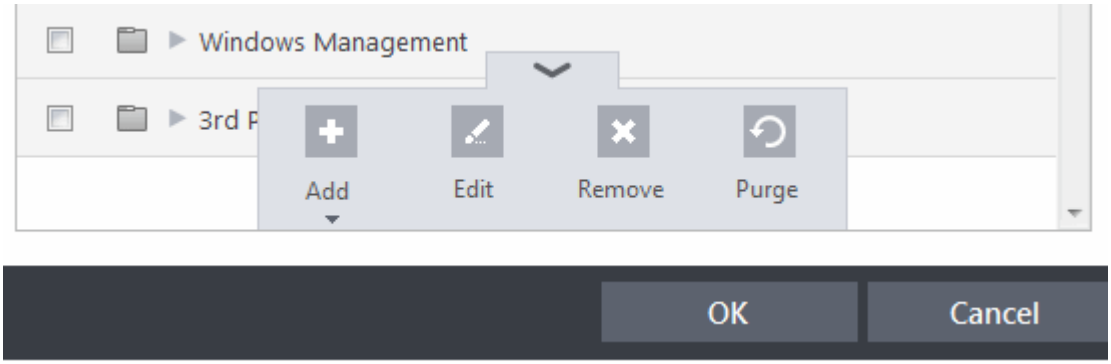
6.2.2.4.1. Protected Files

The Protected Files tab displays a list of files and file groups that are protected from access by other programs, especially malicious programs such as virus, Trojans and spyware. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying anyone and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files and Folders' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Internet Security blocks this attempt and produce a 'Protected File Access' pop-up alert.

If you add a file to Protected Files, but want to allow trusted application to access it, then rules can be defined in HIPS Rulesets. Refer to the section **Exceptions** for more details about how to allow access to files placed in Protected Files.

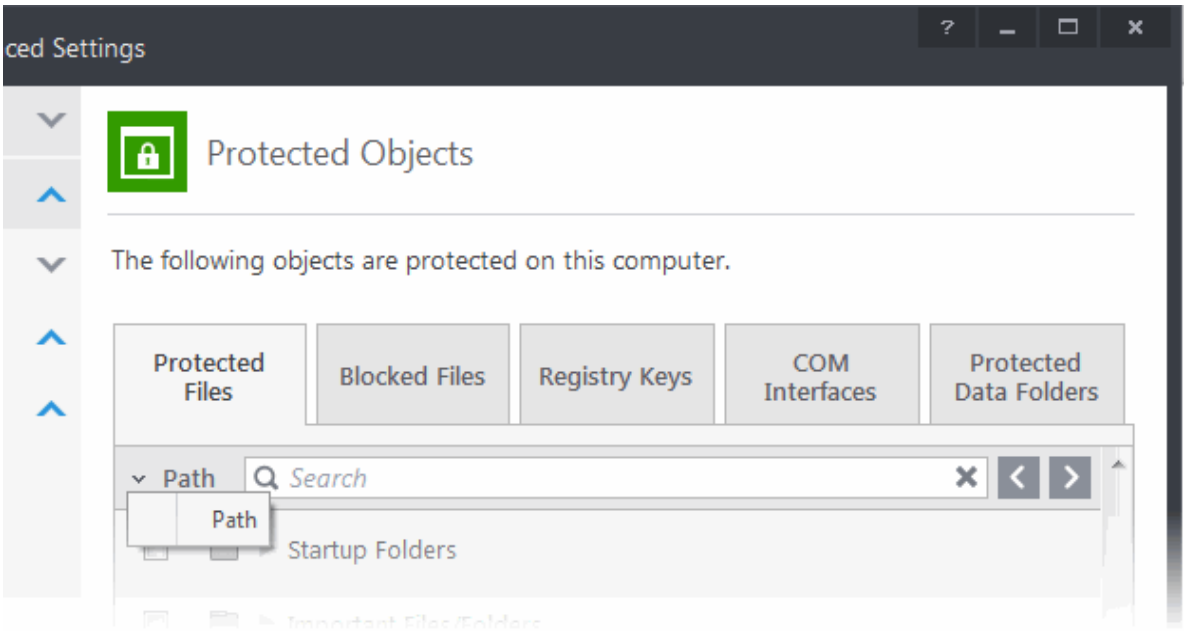


Clicking the handle at the bottom of the interface opens an options panel with the following options:



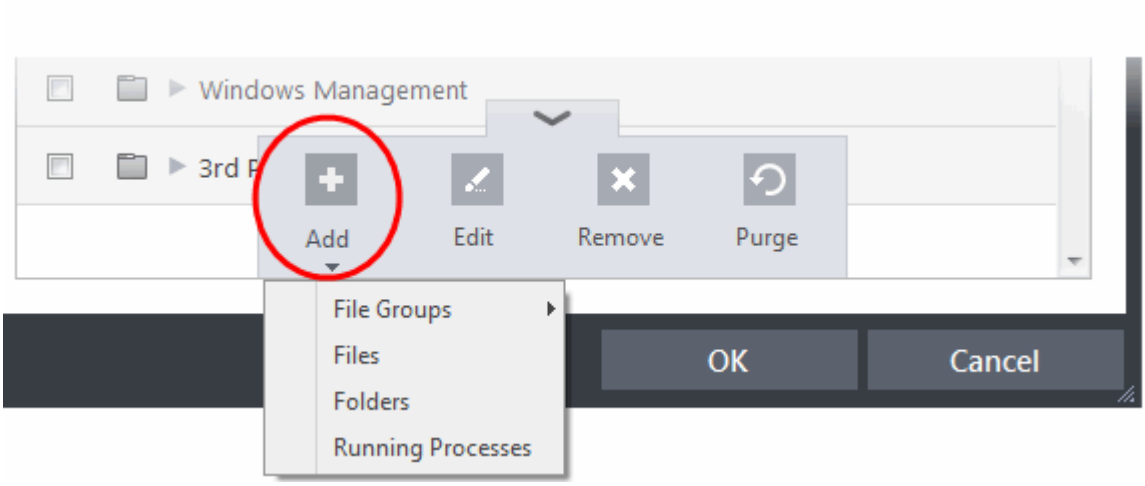
- **Add** - Allows you to add individual files, programs, applications to Protected Files.
- **Edit** - Allows you to edit the path of the file or group of a selected item in the Protected Files interface.
- **Remove** - Deletes the currently highlighted file or file group.
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

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



To manually add an individual file, folder, file group or process

- Click the handle from the bottom and select 'Add'.

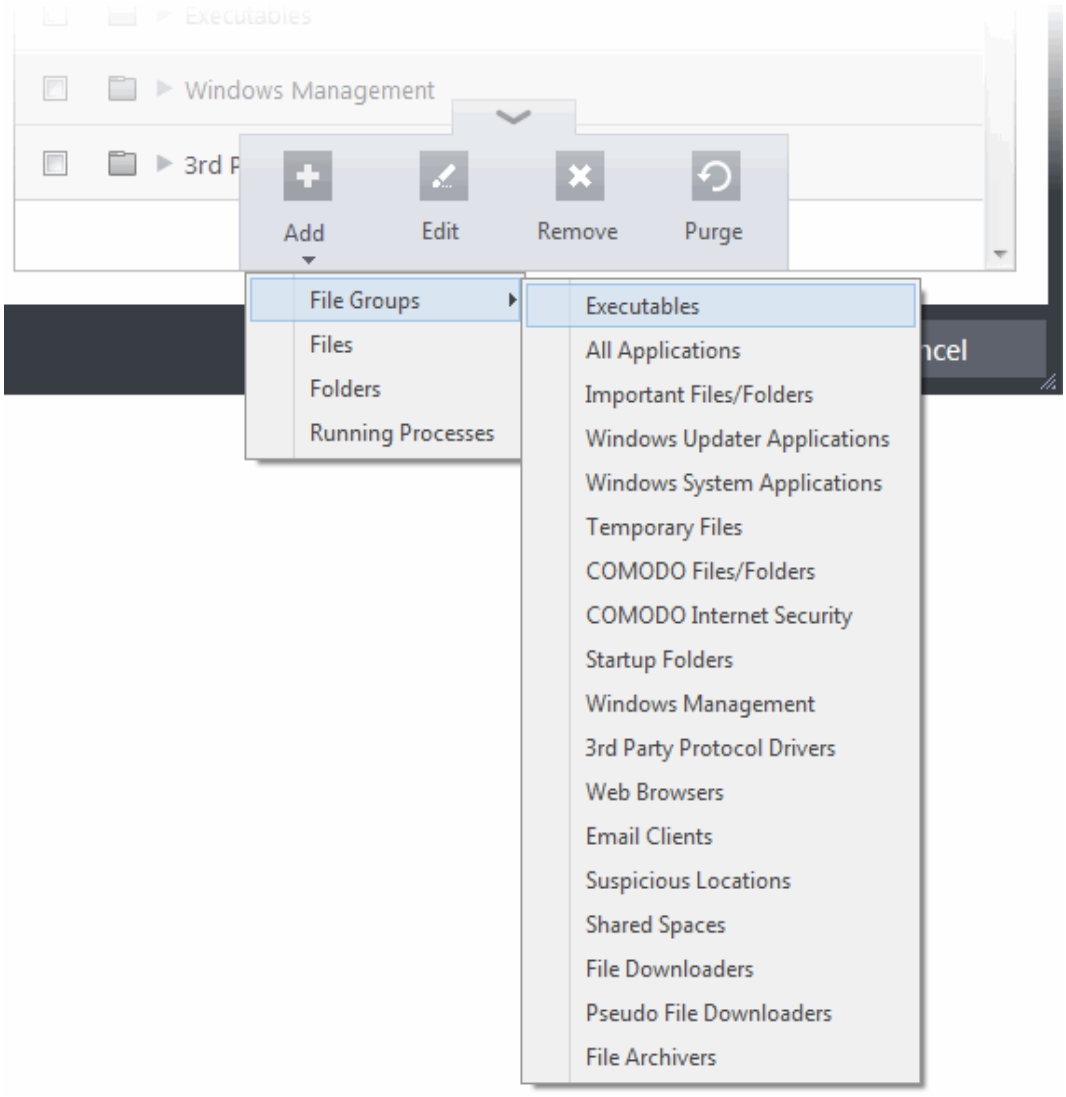


You can add the files by following methods:

- **Selecting from File Groups**
- **Browsing to a File**
- **Browsing to a Folder**
- **Selecting from currently running Processes**

Adding a File Group

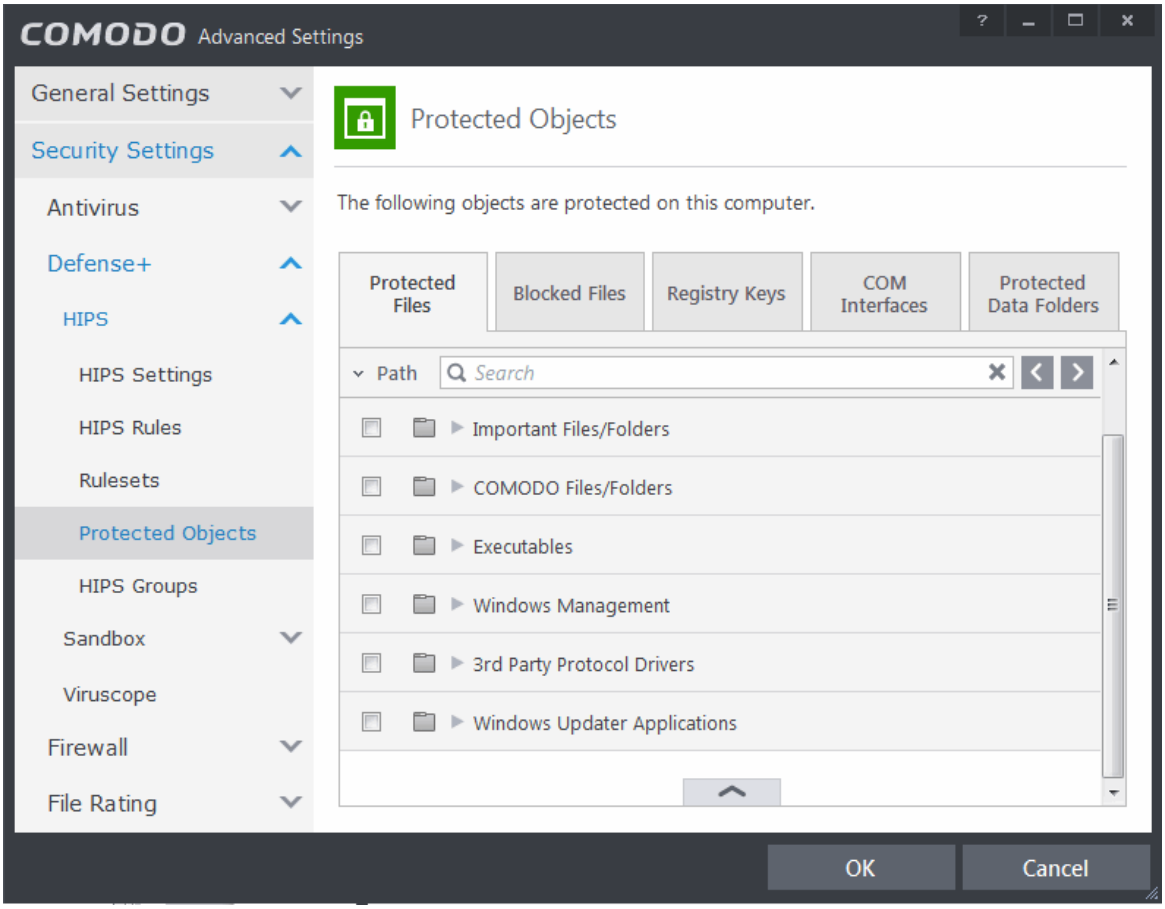
Choosing File Groups allows you to add a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' and so on - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.



CIS ships with a set of predefined File Groups and can be viewed in Advanced Settings > File Rating > **File Groups**. You can also add new file groups here which will be displayed in the predefined list.

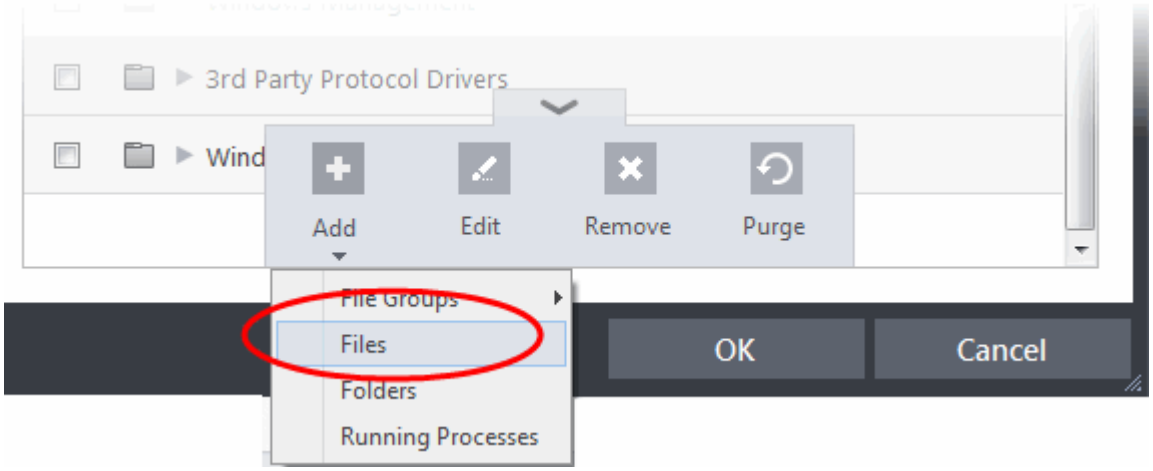
- To add a file group to Protected Files, click Add > File Groups and select the type of File Group from the list.

The file group will be added to Protected Files.

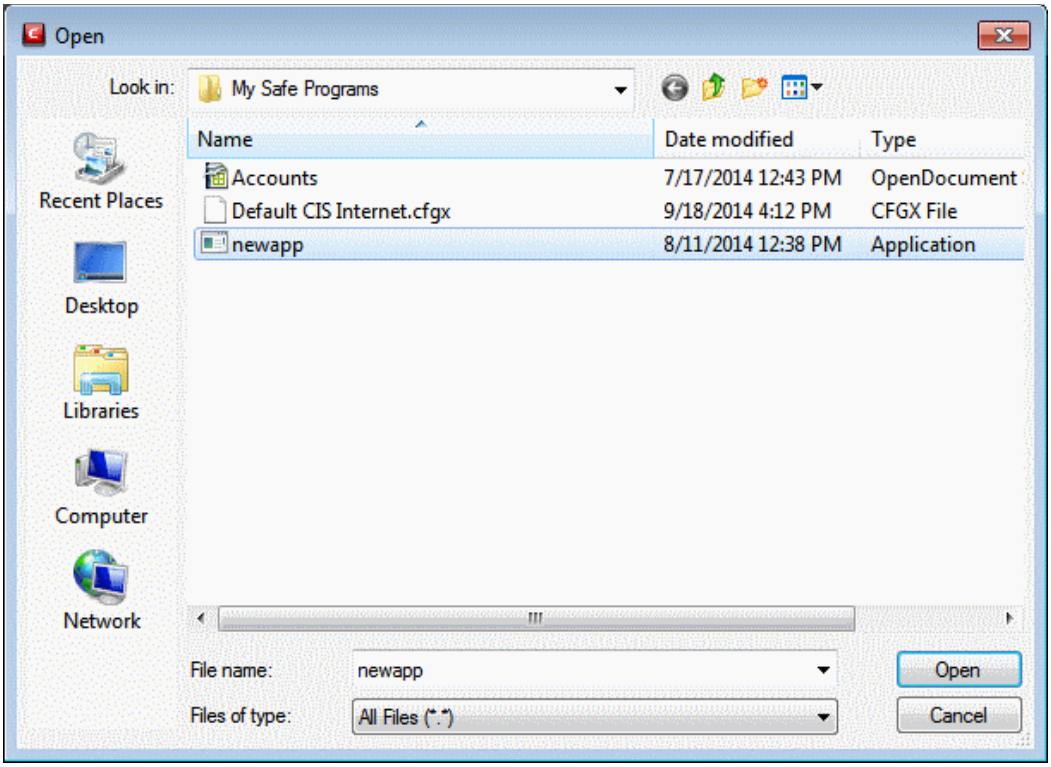


Adding an individual File

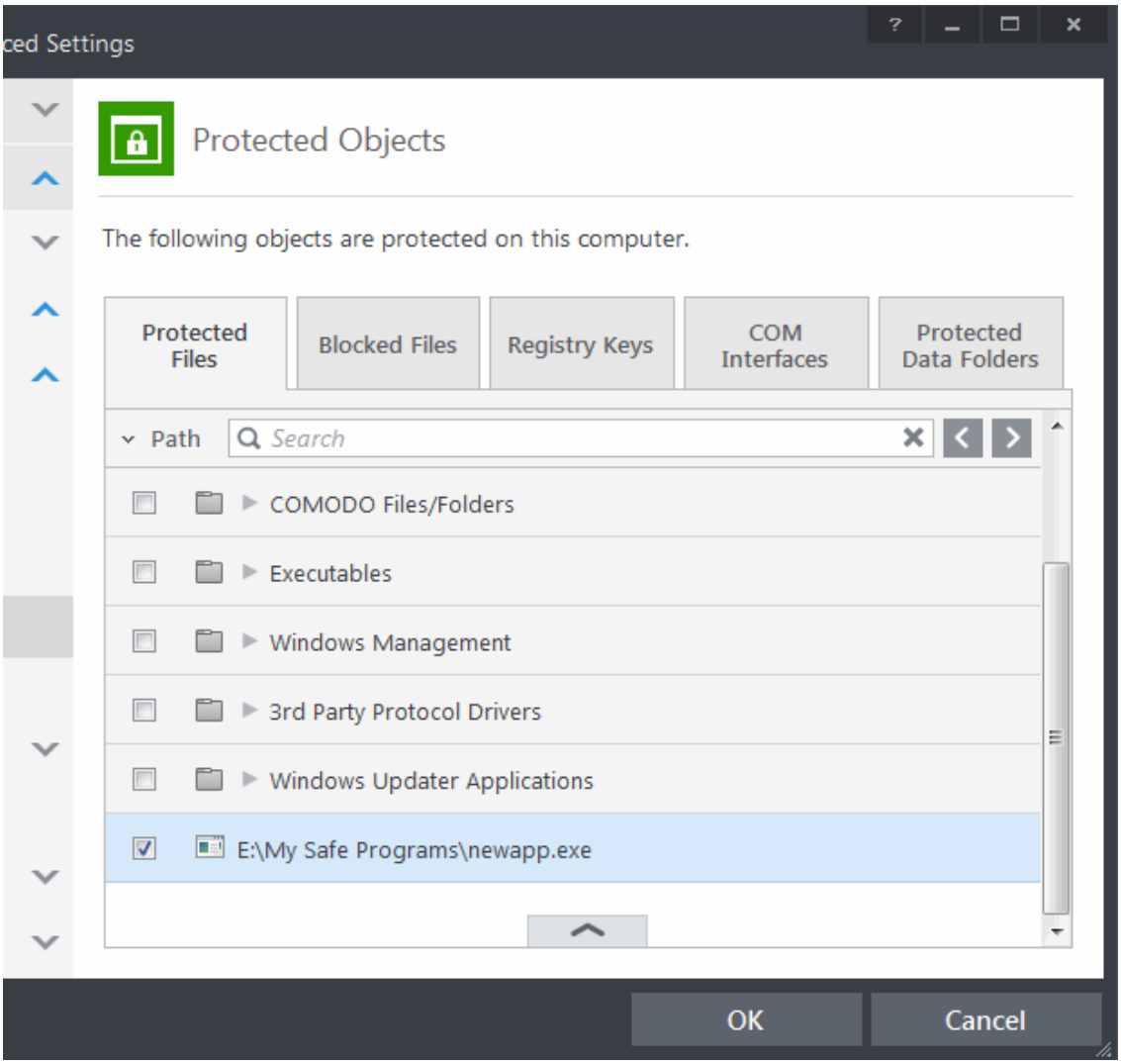
- Choose 'Files' from the 'Add' drop-down.



- Navigate to the file you want to add to Protected Files in the 'Open' dialog and click 'Open'

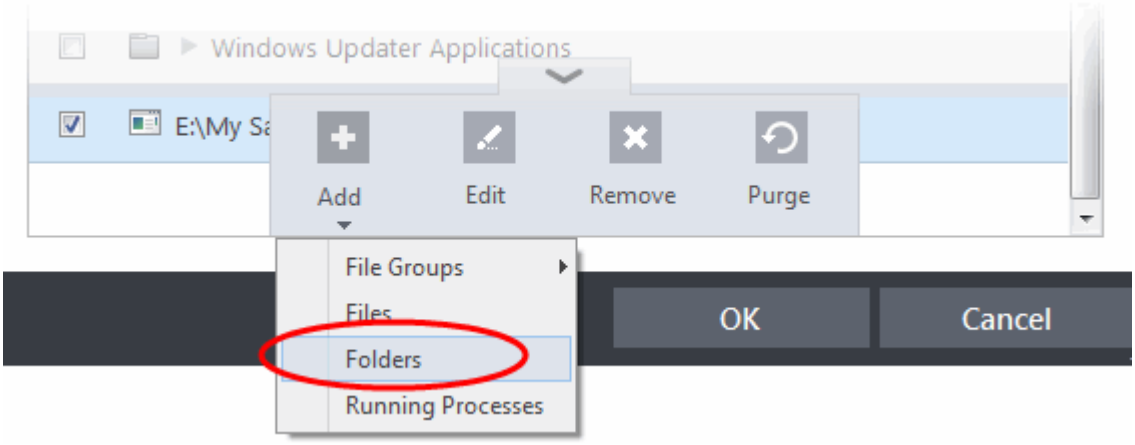


The file will be added to Protected Files.

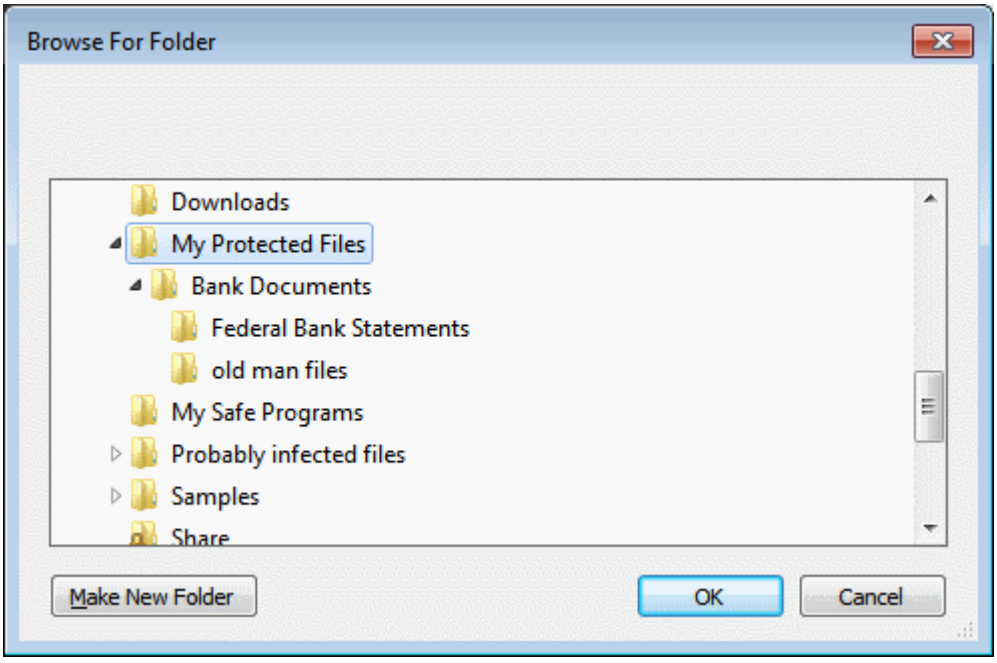


Adding a Drive Partition/Folder

- To add a folder, choose 'Folders' from the 'Add' drop-down.



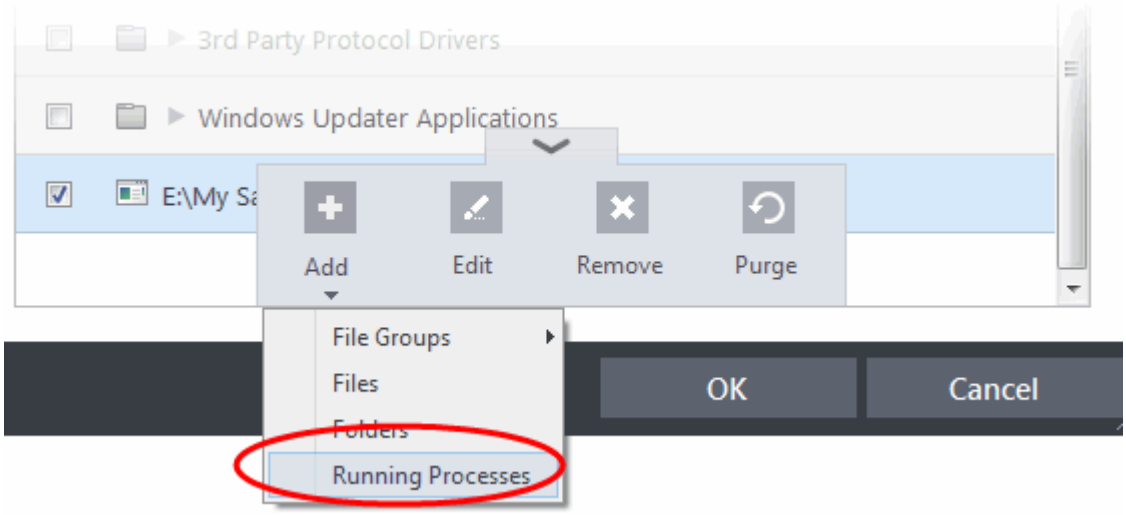
The 'Browse for Folder' dialog will appear.



- Repeat the process to add more folders. The items added to the Protected Files will be protected from access by other programs.

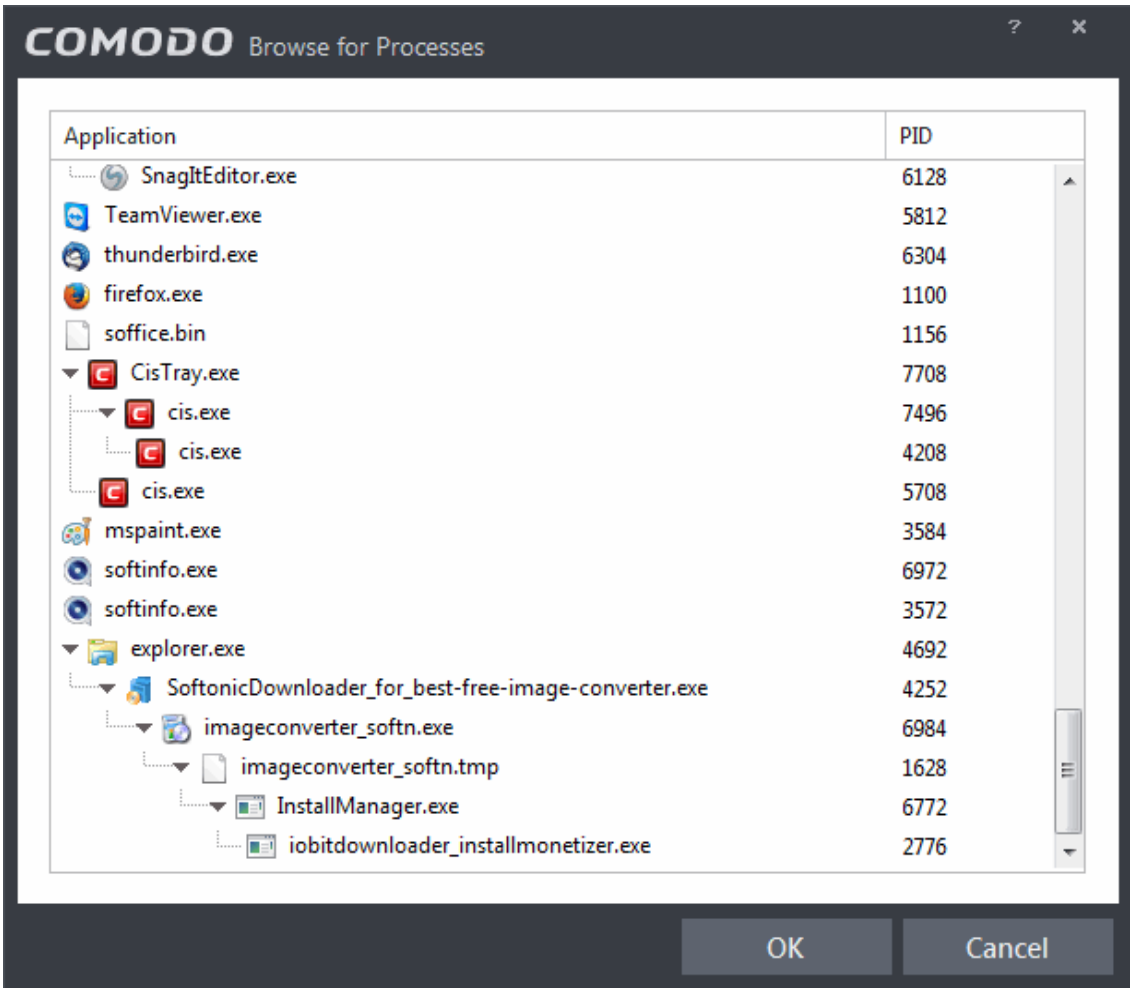
Adding an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down

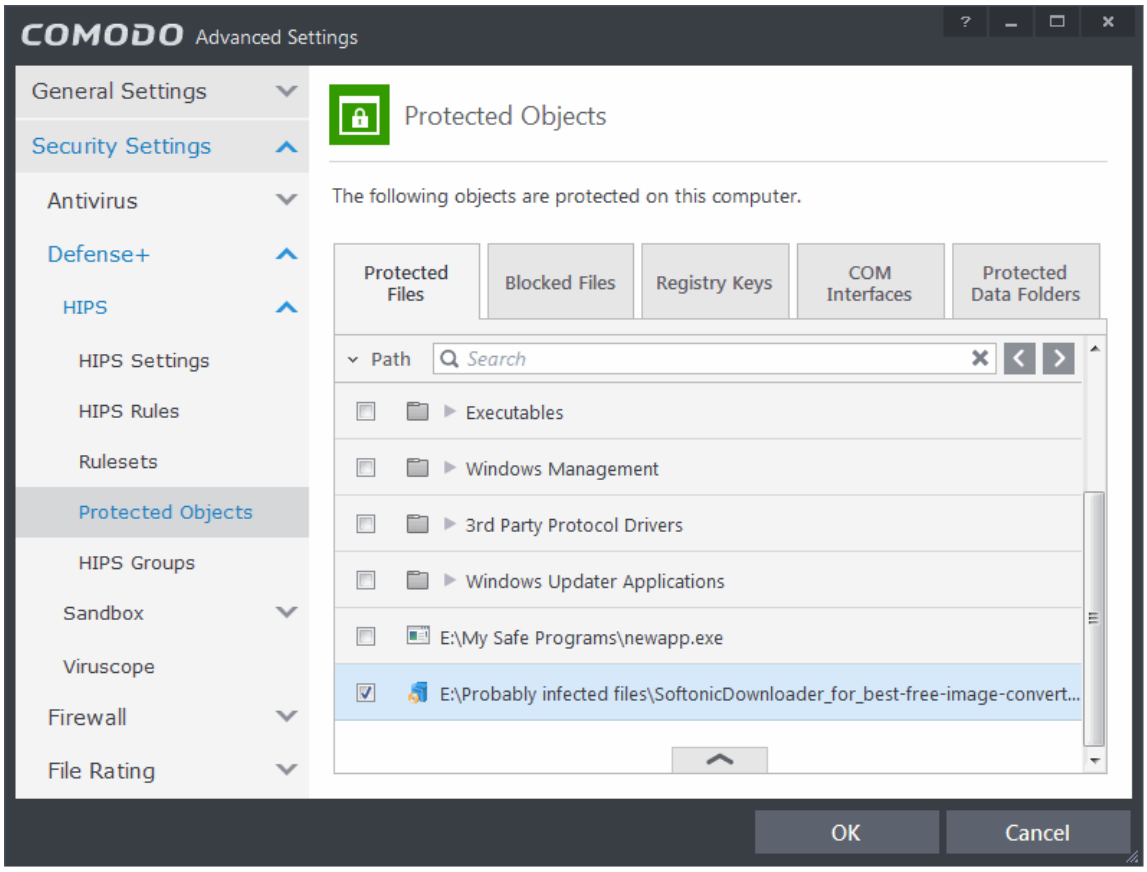


A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to Protected Files and click OK from the Browse for Process dialog.



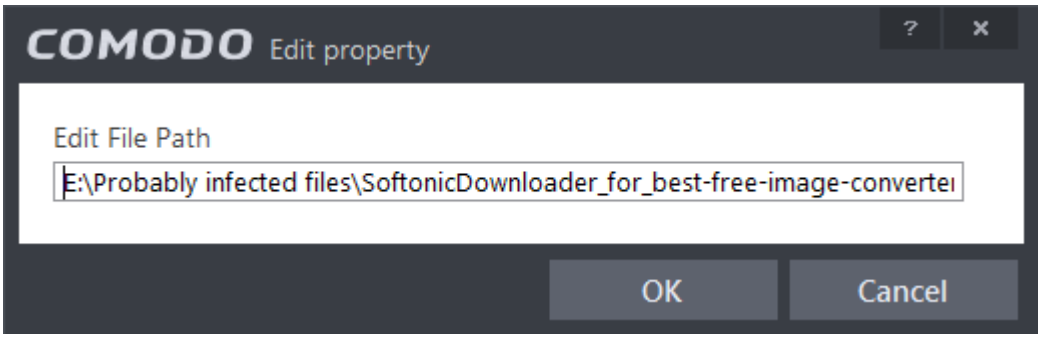
The application will be added to Protected Files.



- Repeat the process to add more files. The items added to the Protected Files will be protected from access by other programs.

To edit an item in the Protected Files list

- Select the item from the list, click the handle from the bottom and select Edit. 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

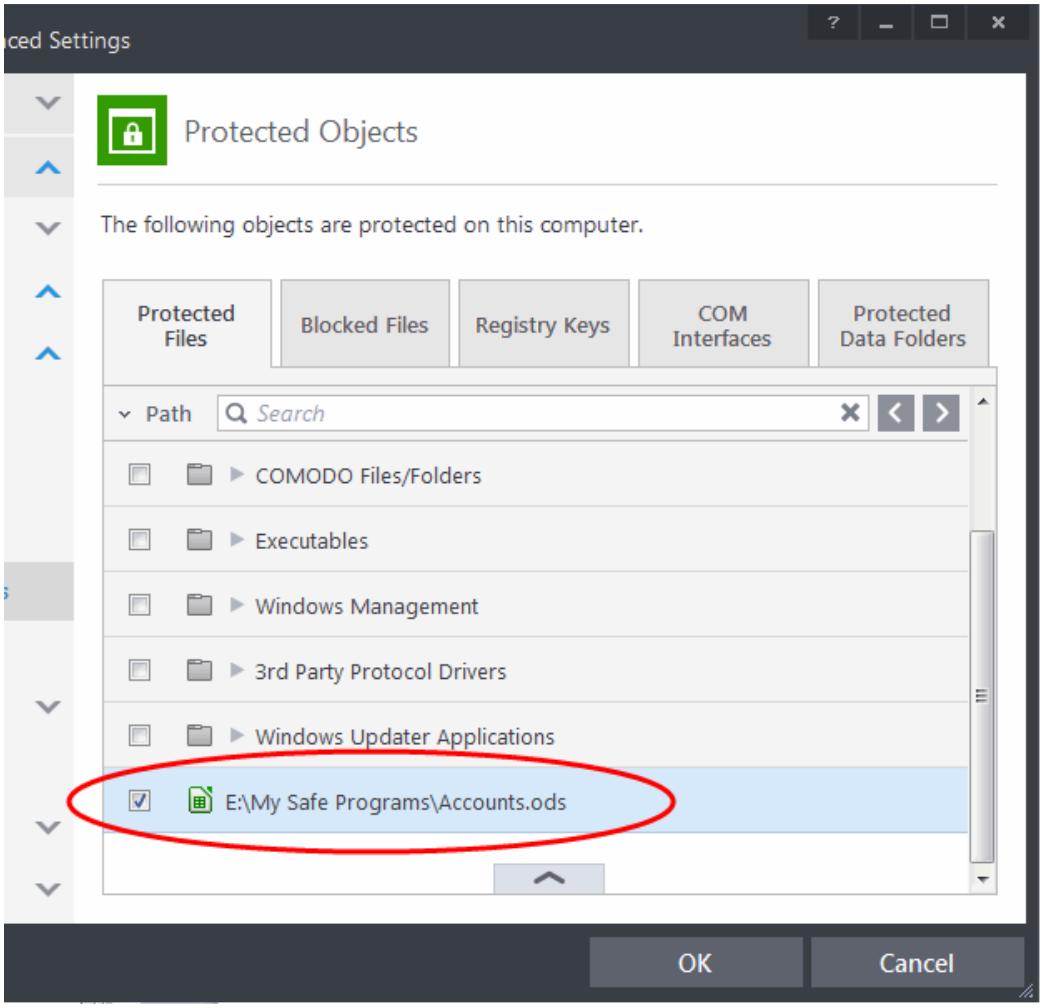
- Select the item from the list, click the handle from the bottom and select 'Remove'.

The selected item will be deleted from the protected files list. CIS will not generate alerts, if the file or program is subjected to unauthorized access.

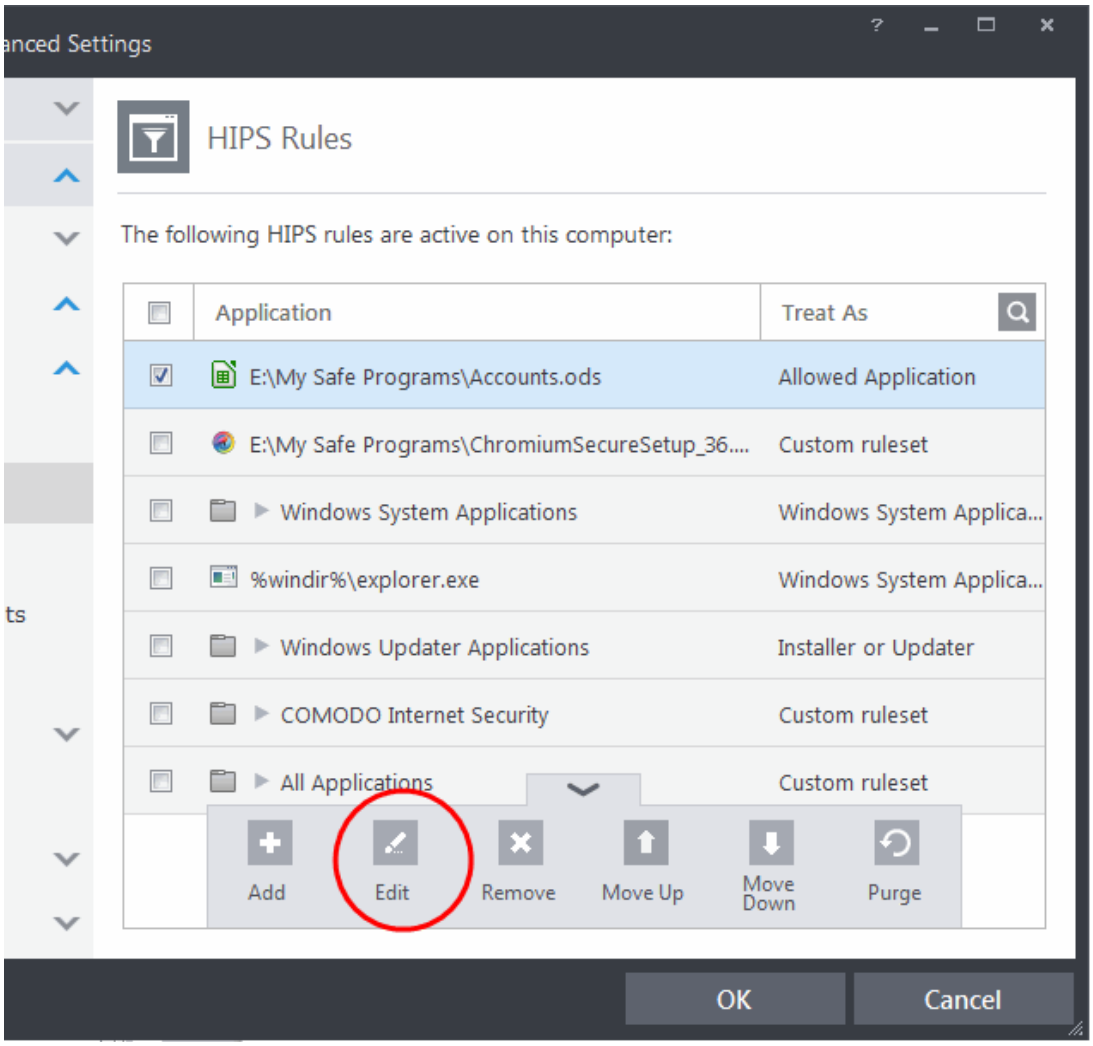
Exceptions

Users can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate Access Right in '**Active HIPS Rules**' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the Open Office Calc program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potential malicious program. You would first **add** the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into '**Active HIPS Rules**' and create an exception for 'scalc' so that it alone could modify 'Accounts.ods'.

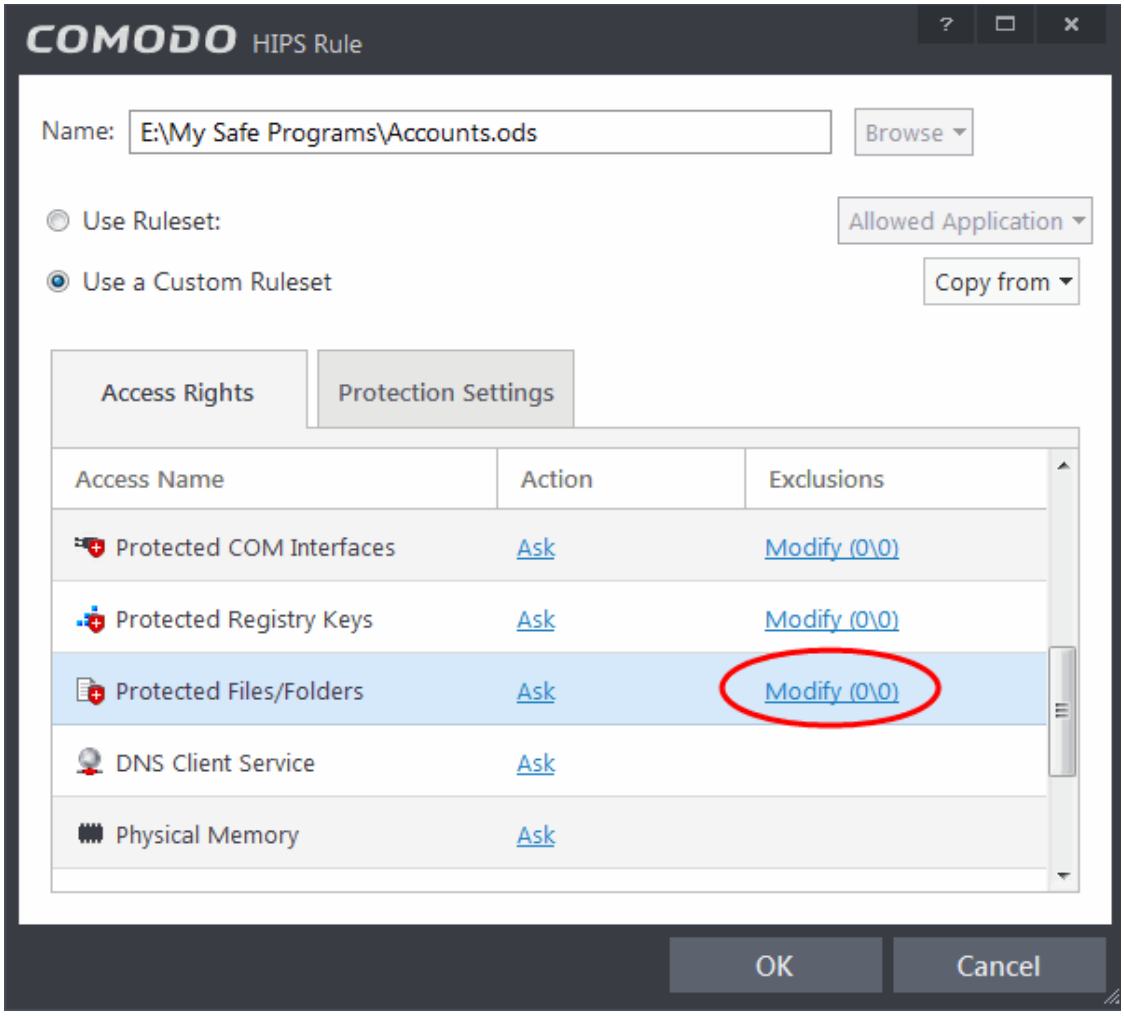
- First add Accounts.odt to Protected Files area.



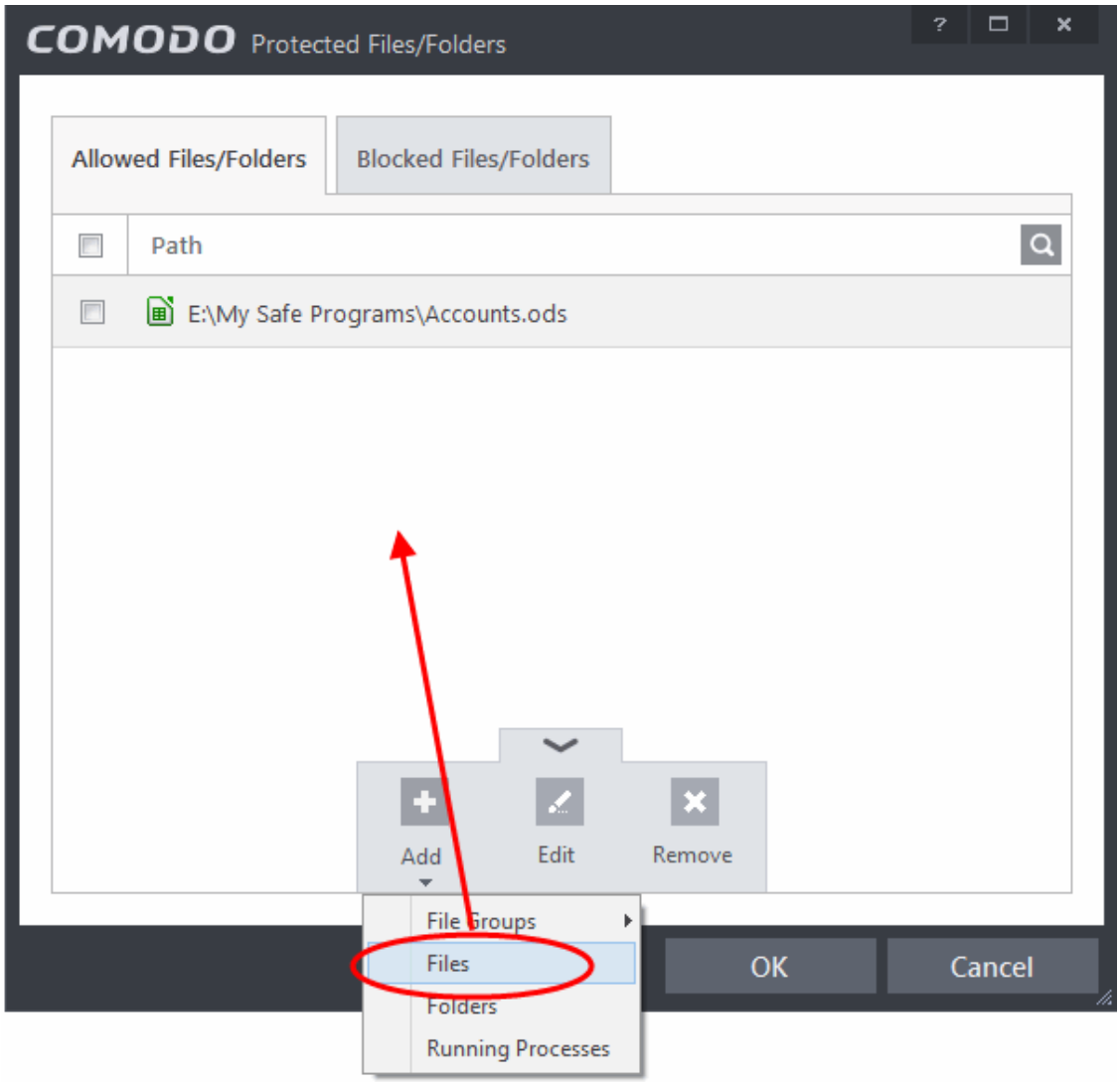
- Then go to HIPS Rules interface and add it to the list of applications. Click the handle at the bottom and choose 'Edit' after selecting the checkbox beside it.



- In the HIPS Rule interface, select 'Use a custom rule set'.



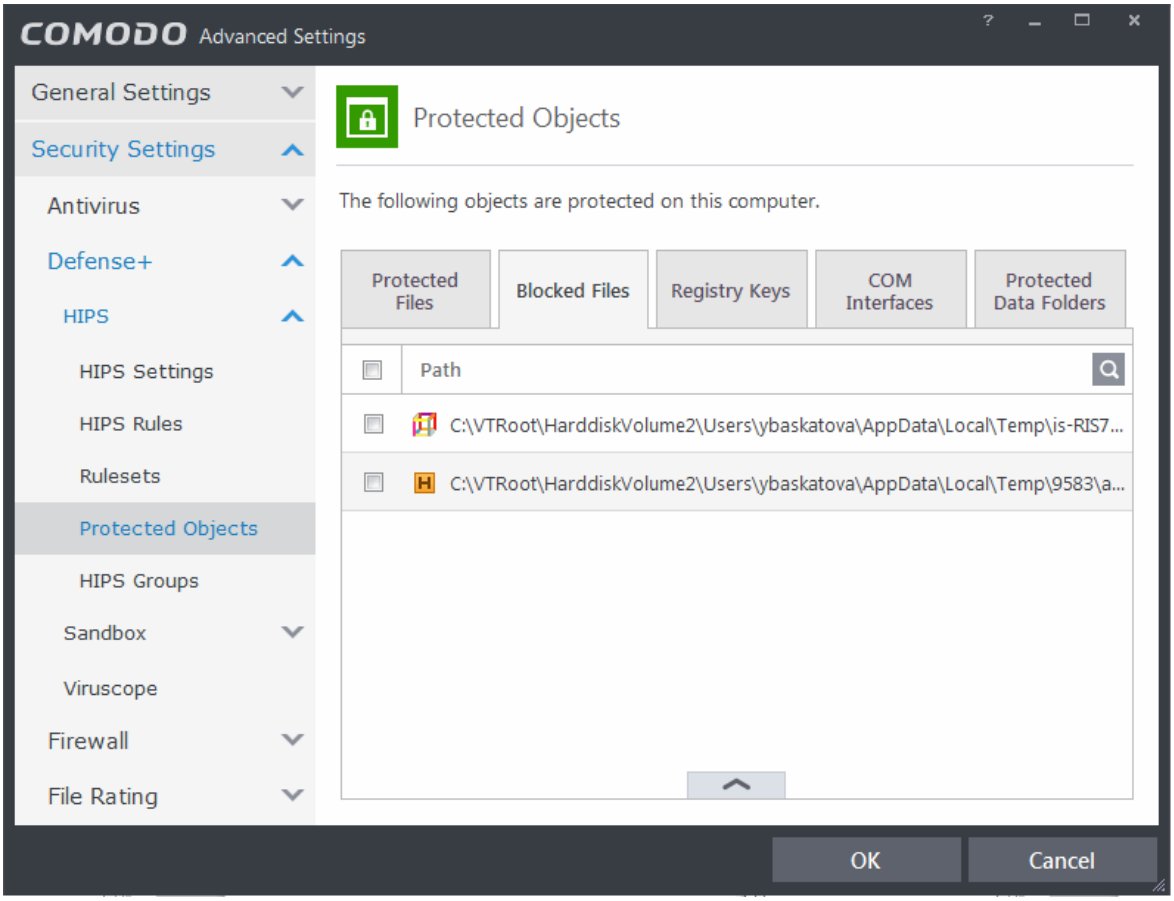
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



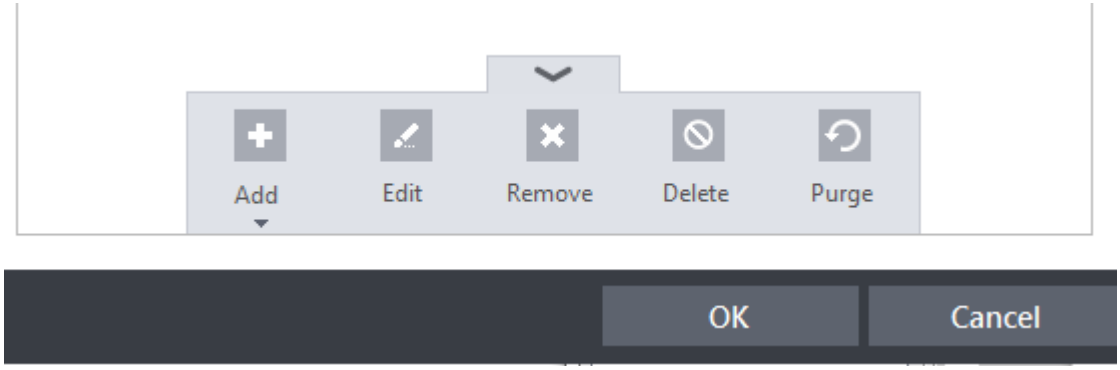
Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

6.2.2.4.2. Blocked Files

Defense+ allows you to lock-down files and folders by completely denying all access rights to them from other processes or users - effectively cutting it off from the rest of your system. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files that are placed in 'Protected Files', users cannot selectively allow any process access to a blocked file.

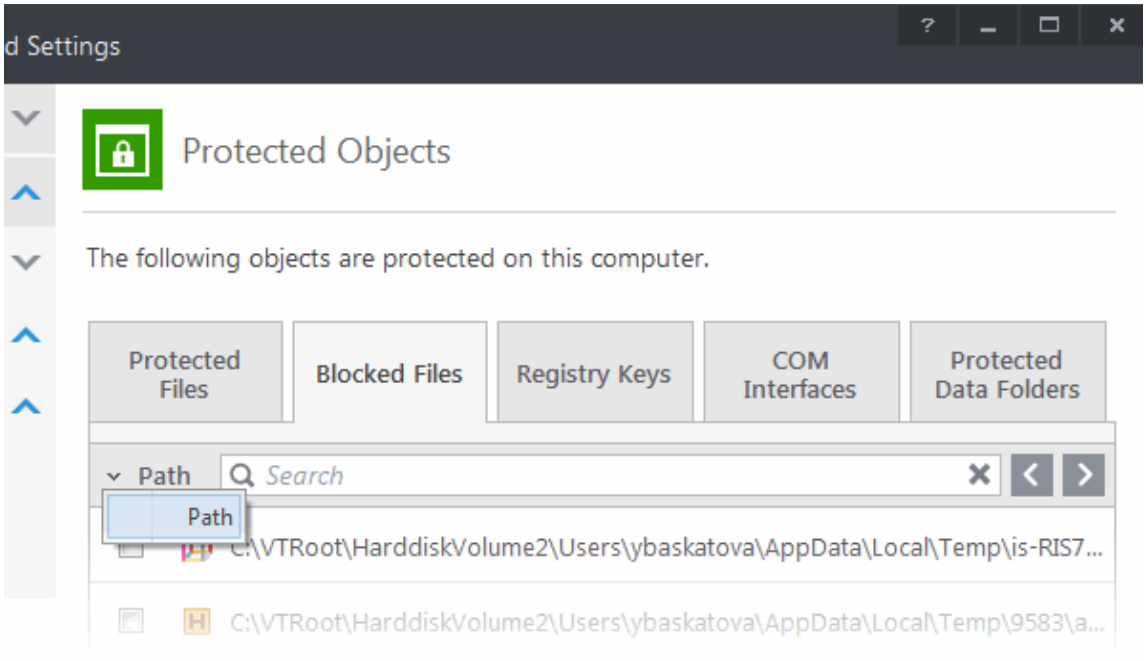


Clicking the handle at the bottom of the interface opens an options panel with the following options:



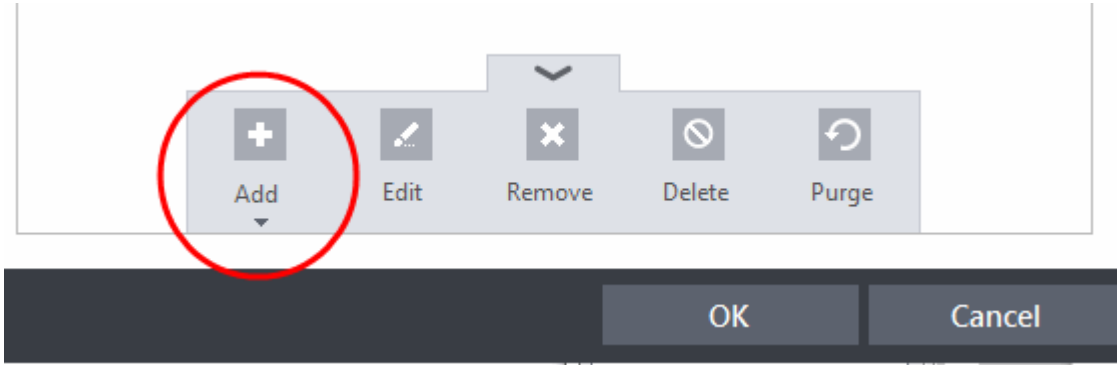
- **Add** - Allows you to add individual files, programs, applications to Blocked Files.
- **Edit** - Allows you to edit the path of the file.
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

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



To manually add an individual file or application

- Click the handle from the bottom center and select 'Add'.

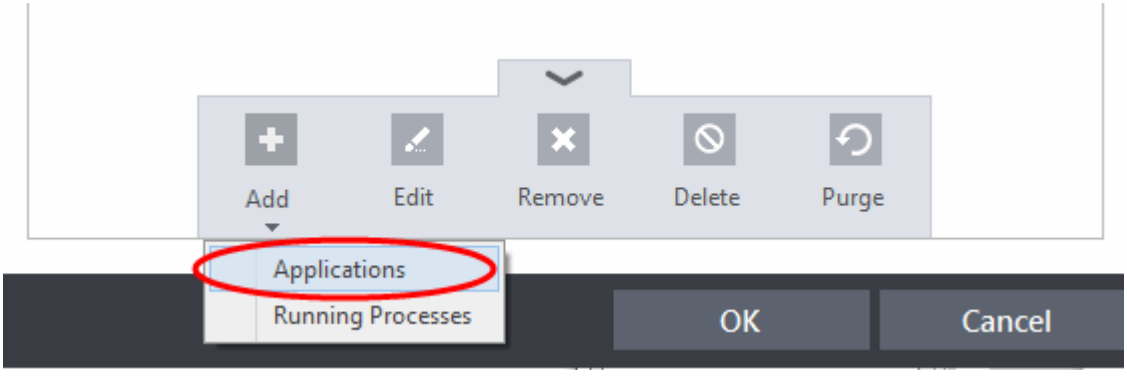


You can add the files by following methods:

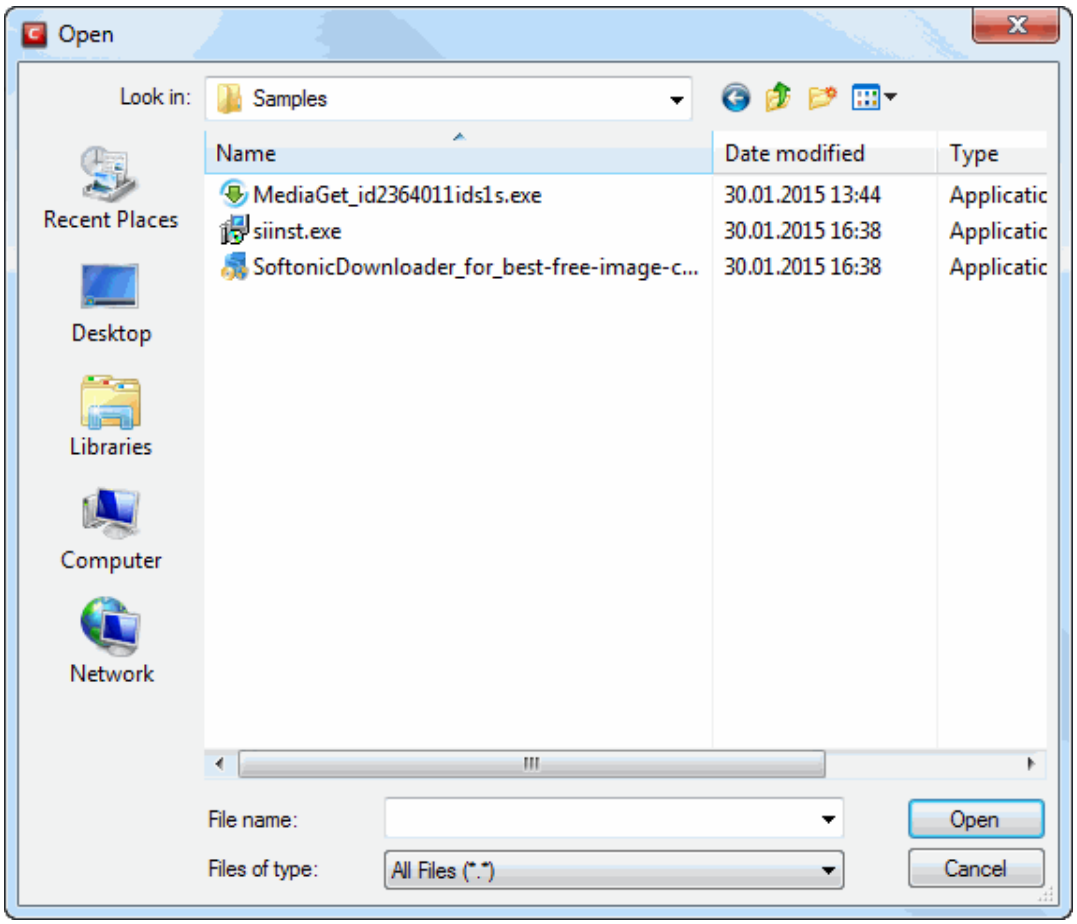
- **Selecting a File**
- **Selecting from currently running Processes**

Adding a File

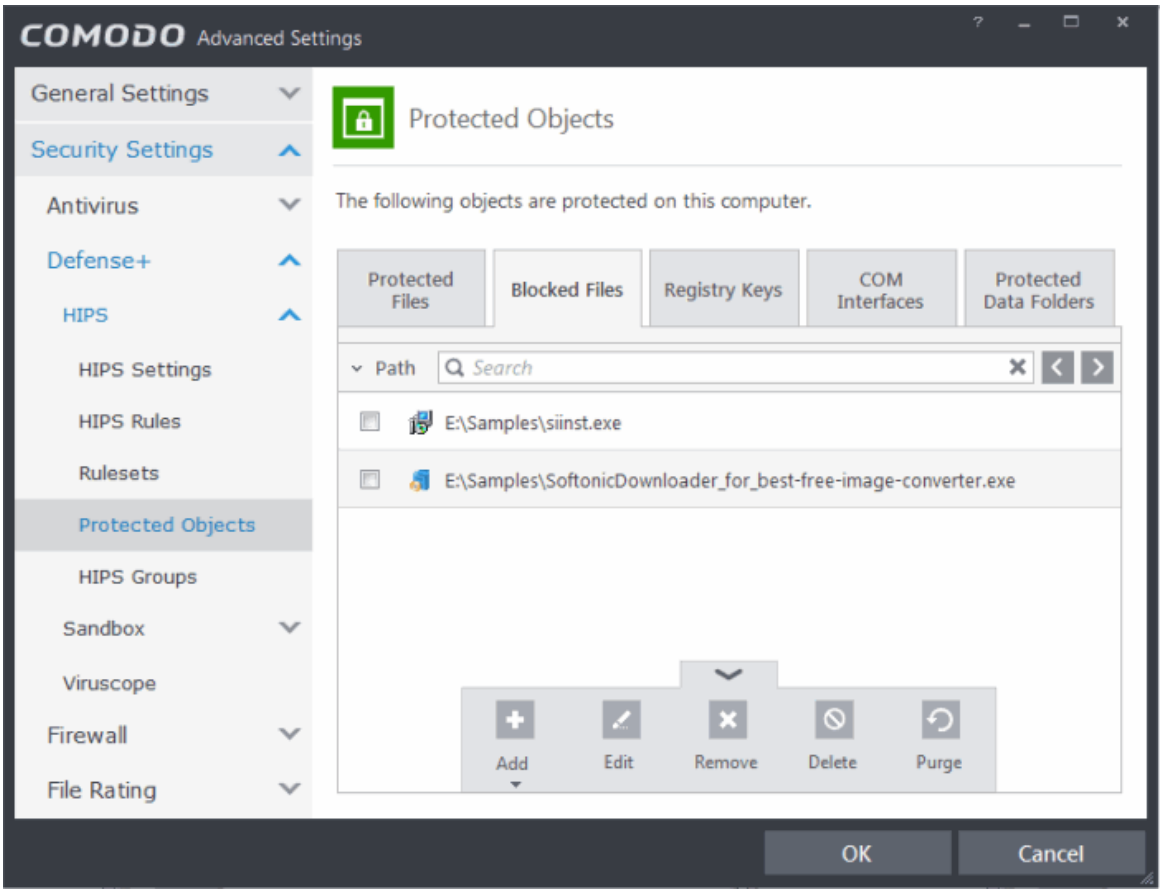
- Choose 'Applications' from the 'Add' drop-down.



- Navigate to the file you want to add to Blocked Files in the 'Open' dialog and click 'Open'



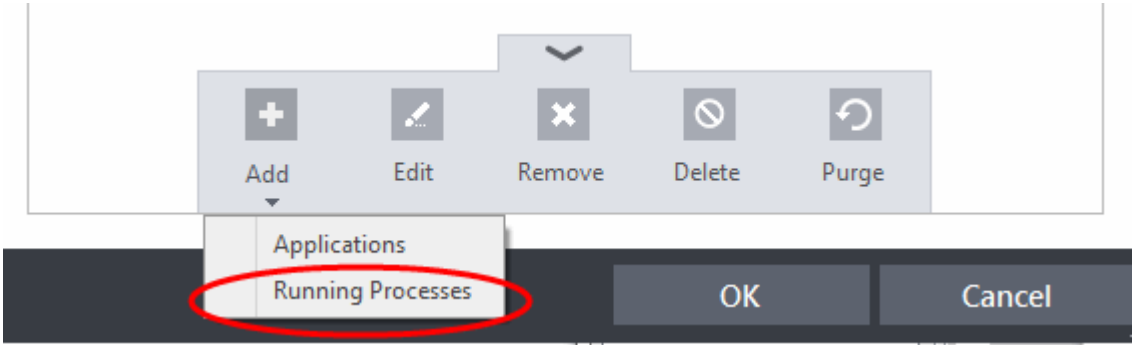
The file will be added to Blocked Files.



- Repeat the process to add more files.

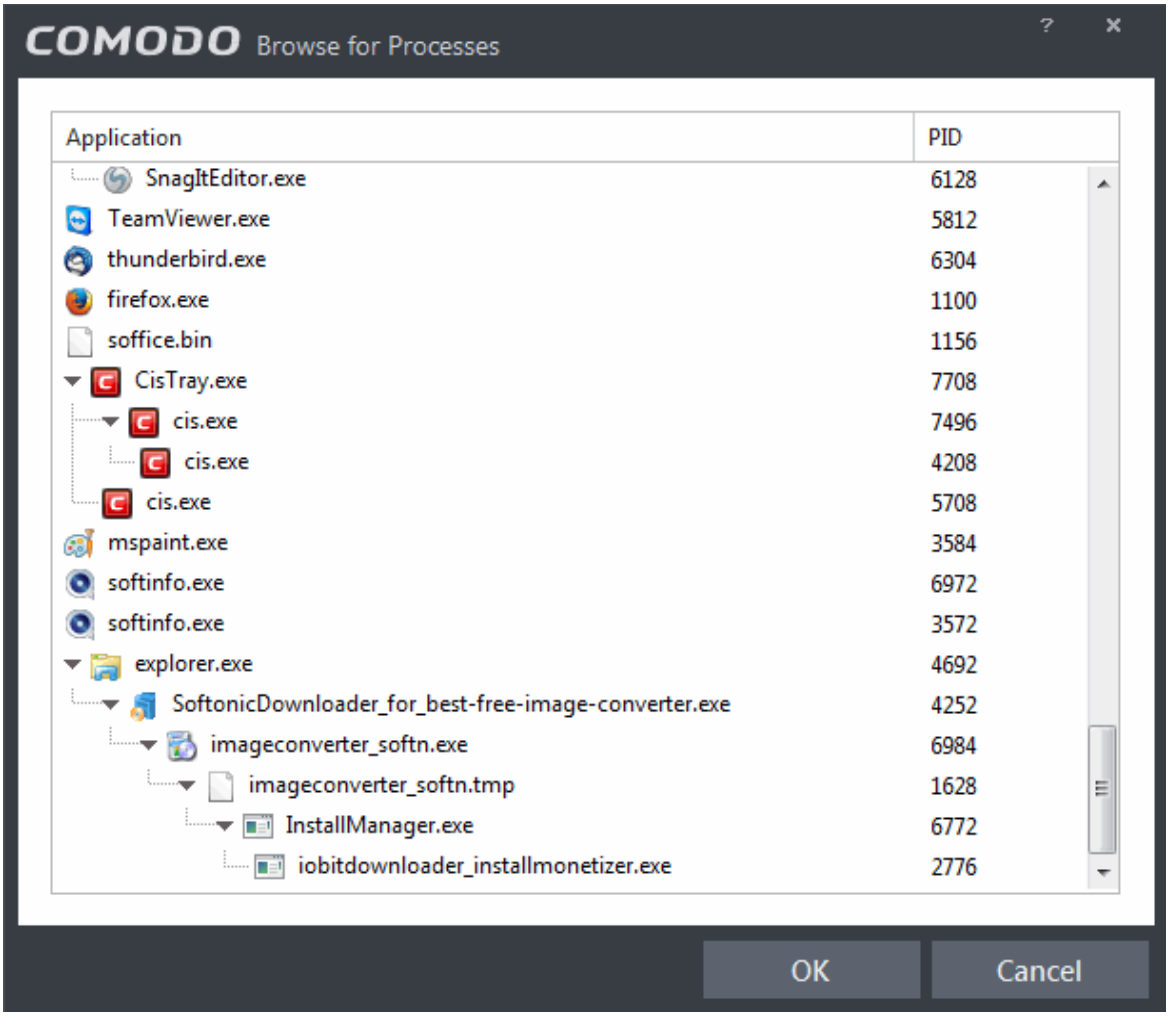
Adding an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down

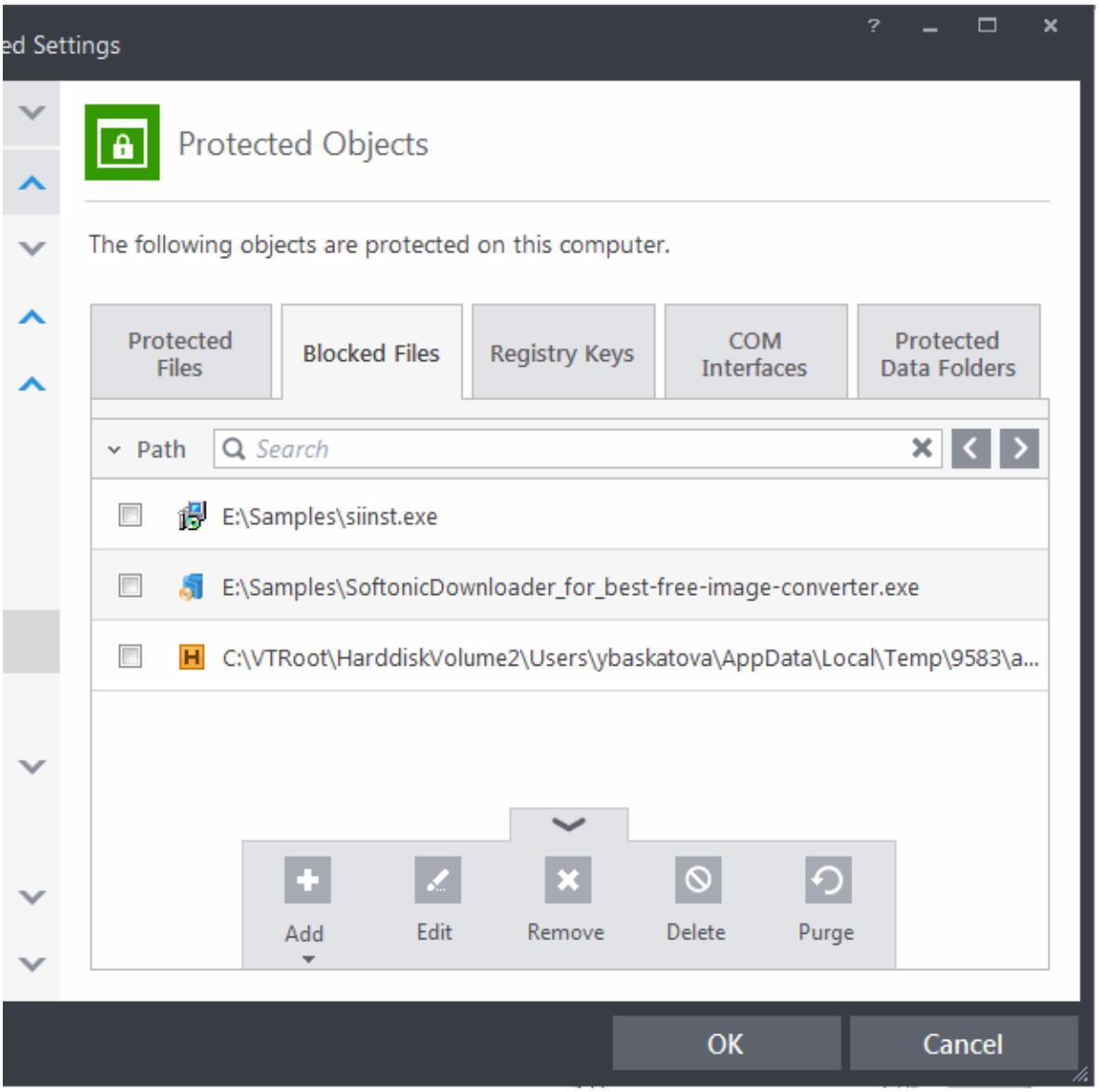


A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to Blocked Files and click OK from the Browse for Process dialog.



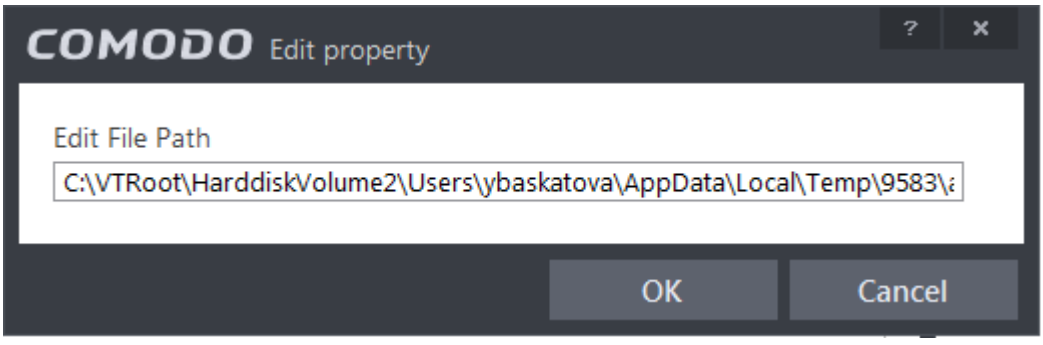
The application will be added to Blocked Files.



- Repeat the process to add more files.

To edit an item in the Blocked Files list

- Select the item from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click OK

To release an item from Blocked Files list

- Select the item from the list, click the handle from the bottom and select 'Remove'.

The selected item will be removed from the Blocked Files list. CIS will not block the application or file from execution or opening

then onwards.

To permanently delete a blocked file from your system

- Select the item from the list, click the up arrow from the bottom and select 'Delete'.

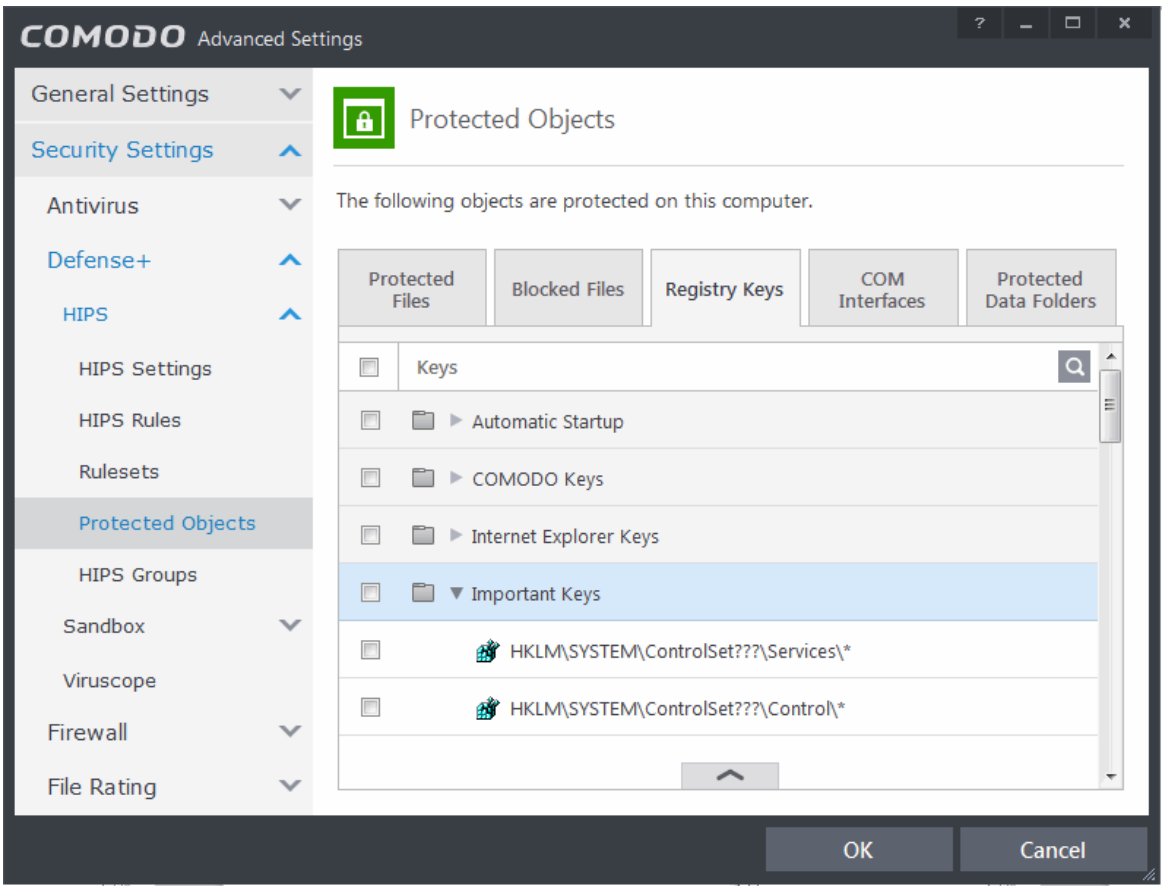
The selected item will be deleted from your computer immediately.

Warning: Deleting a file from from the Blocked Files interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

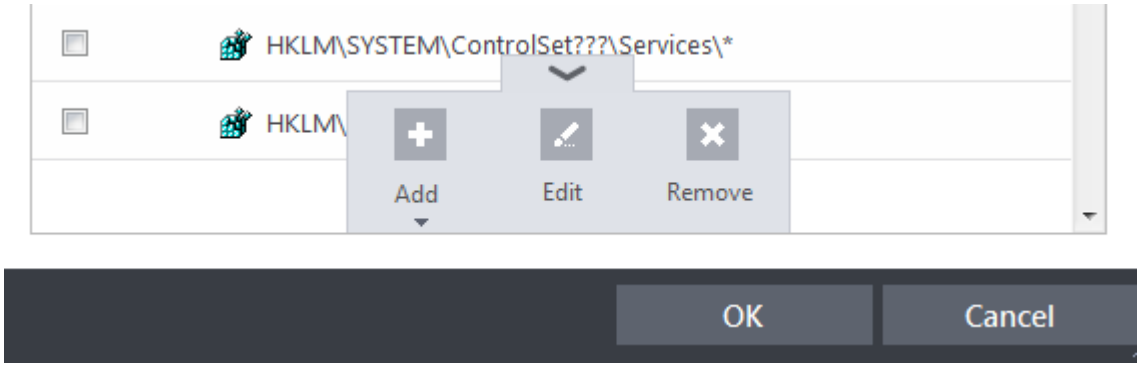
6.2.2.4.3. Protected Registry Keys

The 'Registry Keys' panel allows you to protect system critical registry keys against modification. Irreversible damage can be caused to your system if important registry keys are corrupted or modified in any way. It is essential that your registry keys are protected against any type of attack.

Click the 'Registry Keys' tab in the Protected Objects interface.

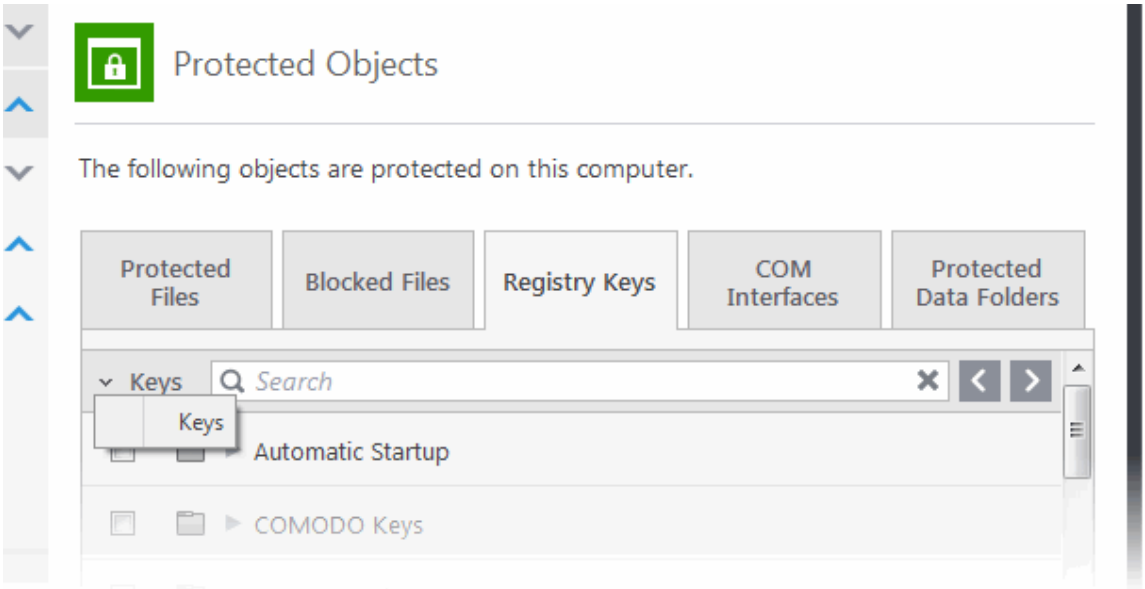


Clicking the handle at the bottom of the interface opens an options panel with the following options:



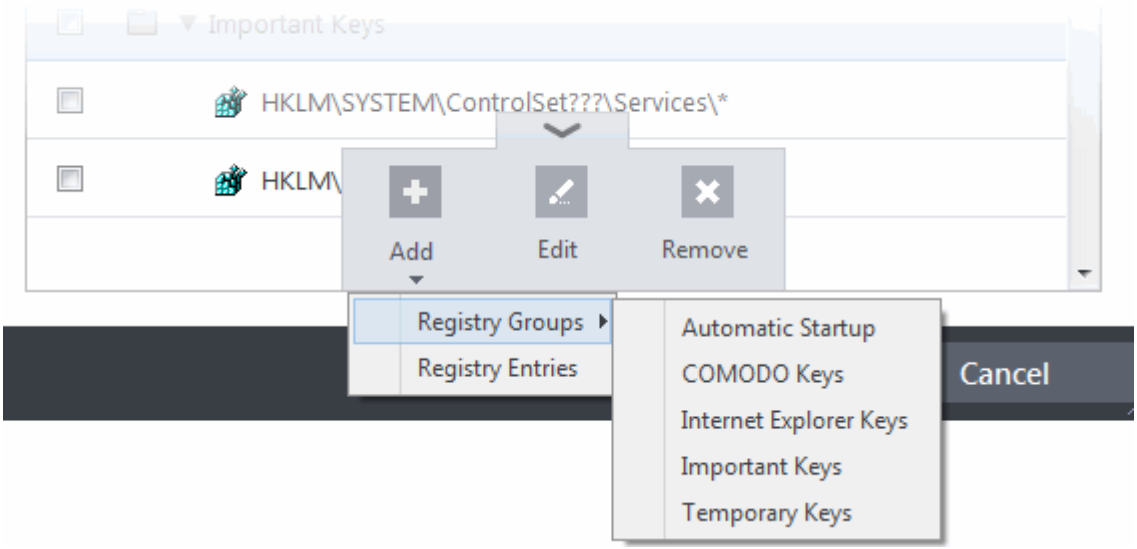
- **Add** - Allows you to add Registry groups or individual registry keys/entries to Registry Protection list.
- **Edit** - Allows you to edit the path of the Registry group or individual registry keys/entries of the selected item in the Registry Protection interface.
- **Remove** - Deletes the currently highlighted Registry group or individual registry key from the Registry Protection list.

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



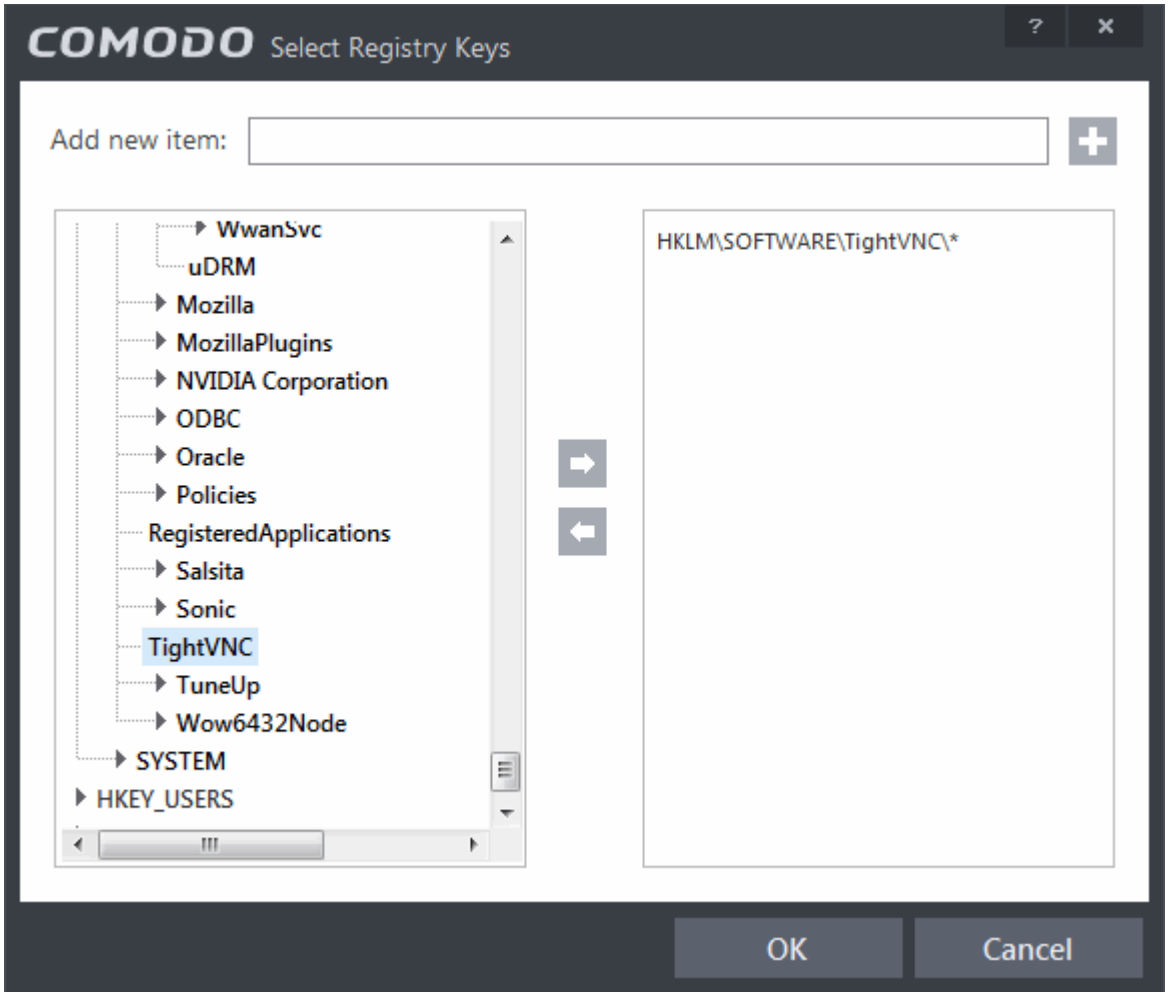
To manually add an individual Registry key or Registry Group

- Click the handle from the bottom and select 'Add'.



You can add the items by following methods:

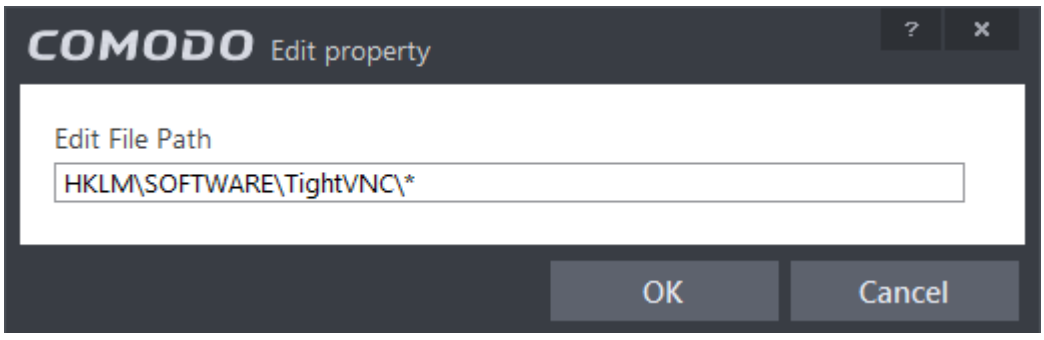
- **Adding Registry Groups** - Selecting Registry Groups allows you to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'. For explanations on editing existing registry groups and creating new groups refer to **Registry Groups** in **HIPS Groups** section.
- **Adding individual Registry Keys** - Selecting 'Registry Entries' opens the 'Select Registry Keys' screen.



You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the Registry Protection list

- Select the key from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the key path, if you have relocated the file and click OK.

Note: The Registry Groups cannot be edited from this interface. You can edit Registry Groups from the Manage Registry Groups interface. Refer to **Registry Groups** in **HIPS Groups** section.

To delete an item from Registry Protection list

- Select the item from the list, click the up arrow from the bottom and select 'Remove'.

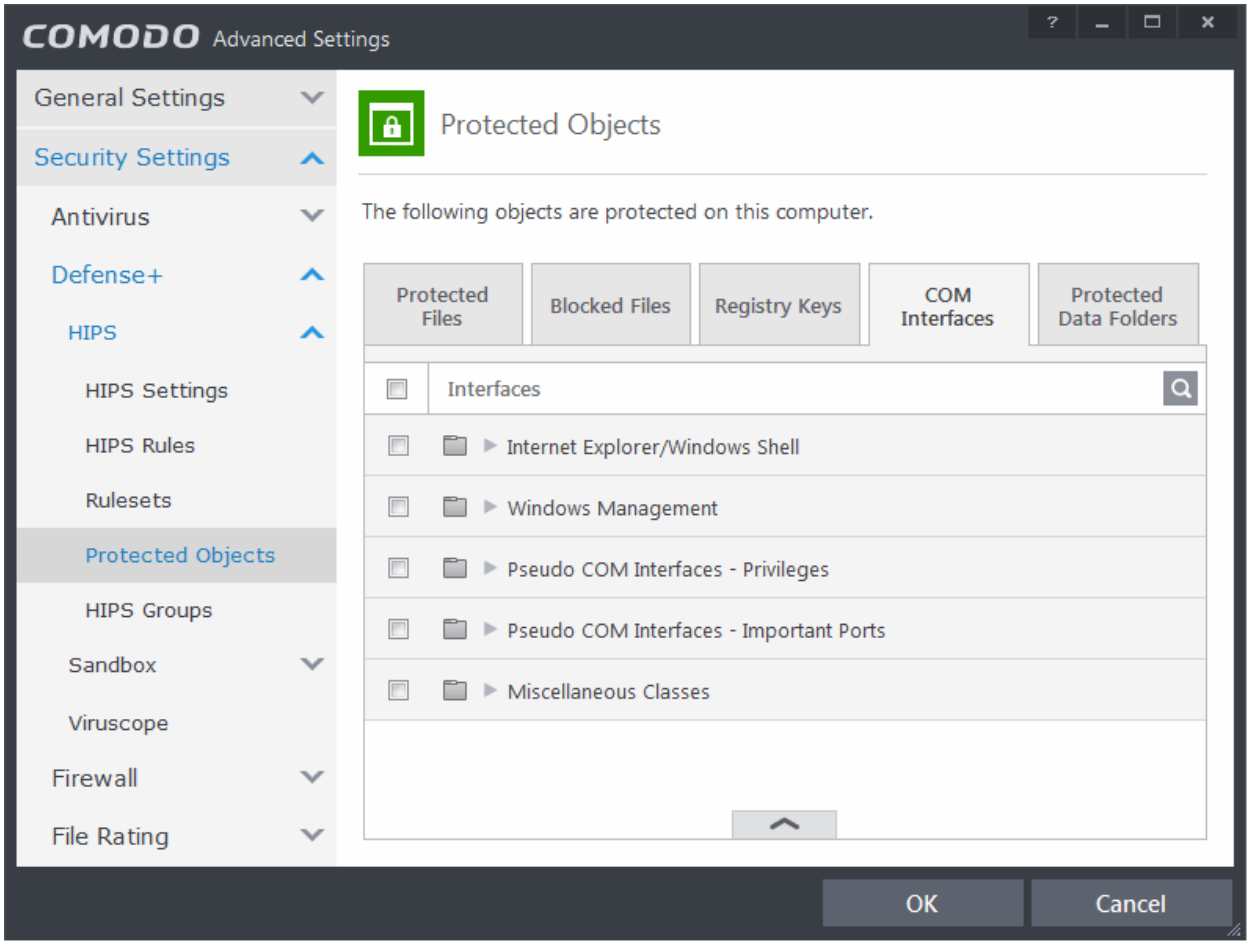
The selected item will be deleted from the Registry Protection list. CIS will not generate alerts, if the key or the group is modified by other programs.

6.2.2.4.4. Protected COM Interfaces

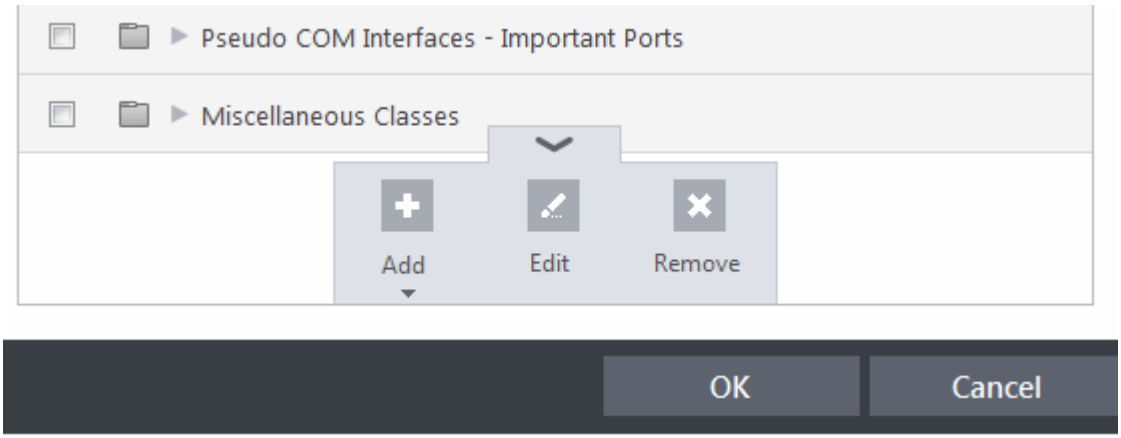
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on your computer. It is a critical part of any security system to restrict processes from accessing the Component Object Model - in other words, to protect the COM interfaces.

Comodo Internet Security automatically protects COM interfaces against against modification, corruption and manipulation by malicious processes. The predefined **COM Interface groups** can be accessed by clicking the 'Groups...' button.

The 'COM Interface' allows you to view the list of predefined **COM Interface groups** protected by CIS, edit them and to add new COM interface components to the list. This interface can be accessed by clicking the 'COM Interfaces' tab in the Protected Objects interface.

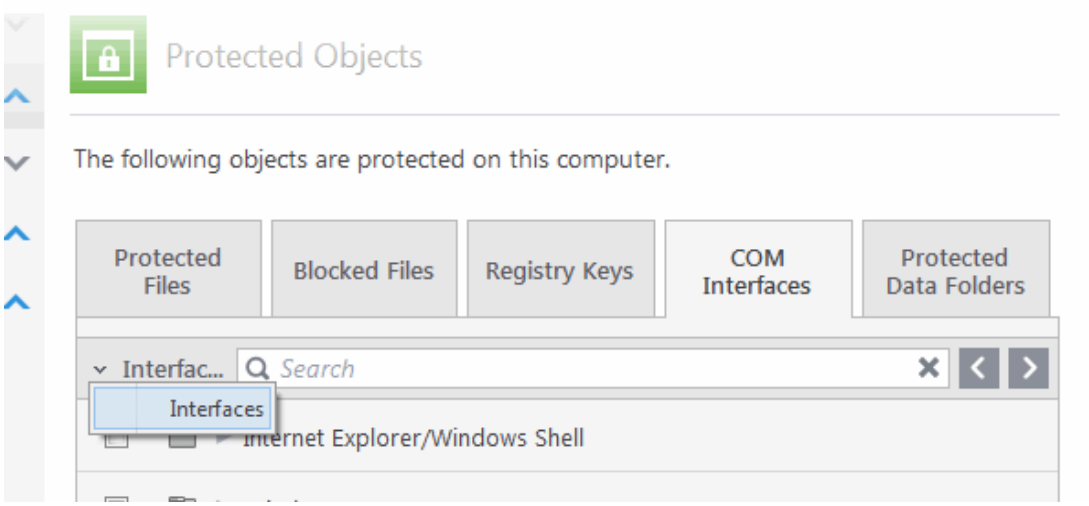


Clicking the handle at the bottom of the interface opens an options panel:



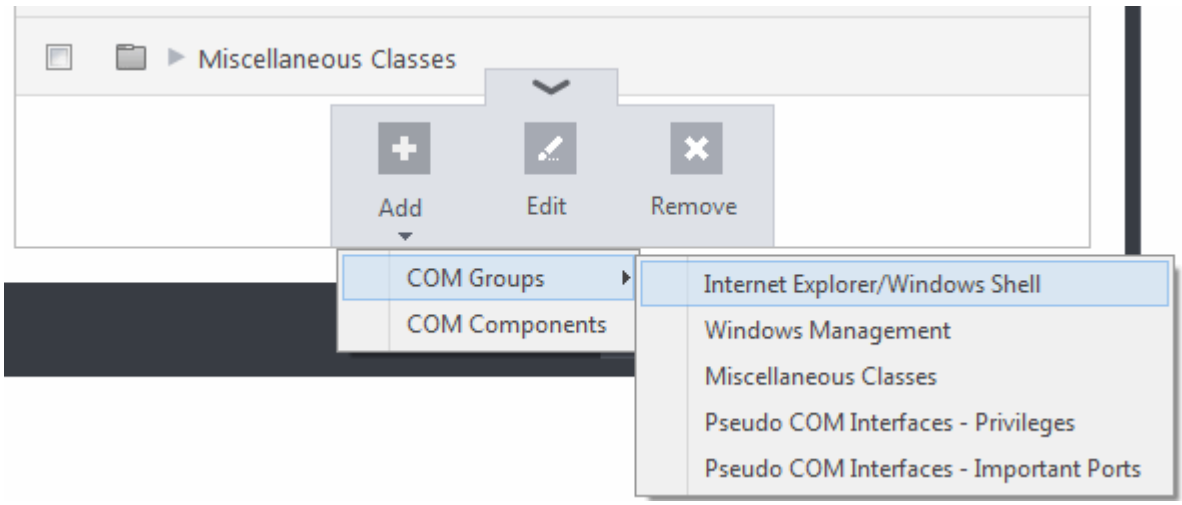
- **Add** - Allows you to add COM groups or individual COM components to COM Protection list.
- **Edit** - Allows you to edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.

You can search for a specific COM interface from the list by clicking the search icon at the far right in the column header and entering the name of the COM interface in full or part. You can navigate through the successive results by clicking the left and right arrows.



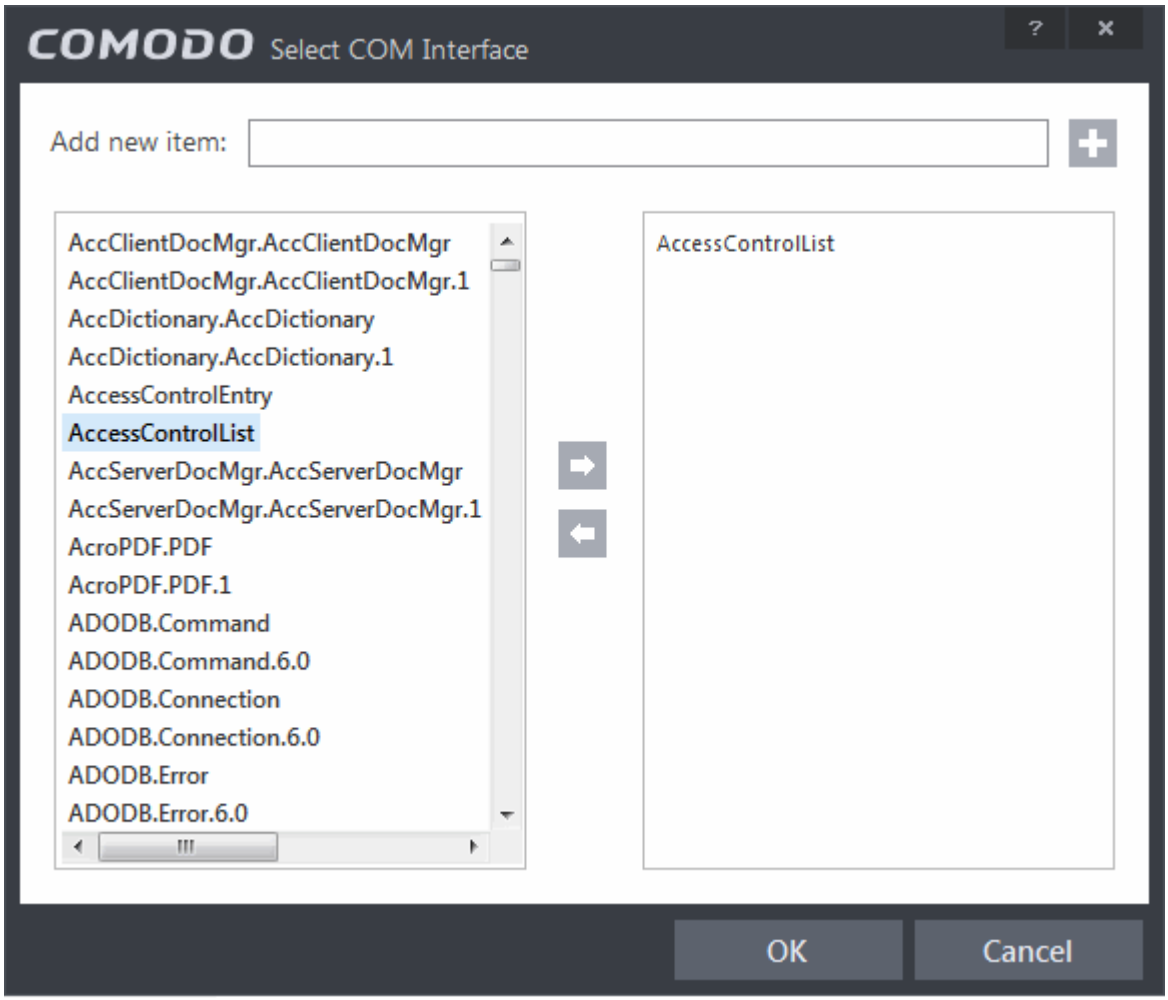
To manually add a COM Group or individual COM component

- Click the handle from the bottom and select 'Add'.



You can add the items by following methods:

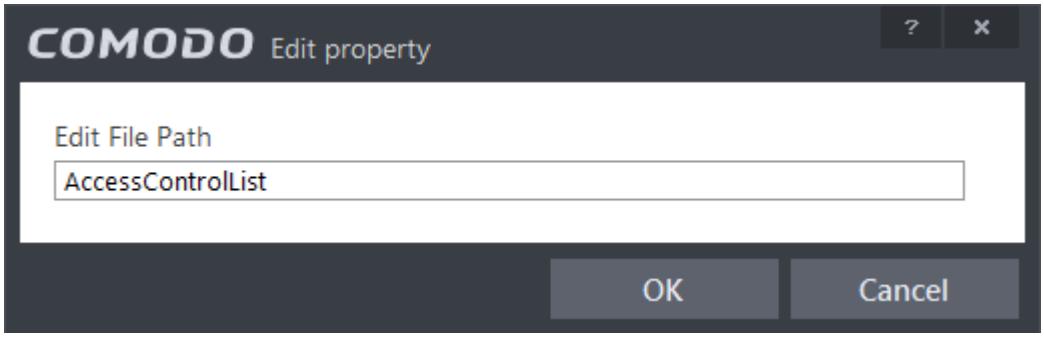
- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section **COM Groups**.
- **Adding COM Components** - Selecting 'COM components' opens the 'Select COM Interfaces' dialog.



You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the COM Protection

- Select the COM component from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the COM Class and click OK

Note: The COM Groups cannot be edited from this interface. You can edit COM Groups from the Manage COM Groups interface. Refer to the section **COM Groups** for more details.

To delete an item from COM Protection list

- Select the item from the list, click the handle from the bottom and select 'Remove'.

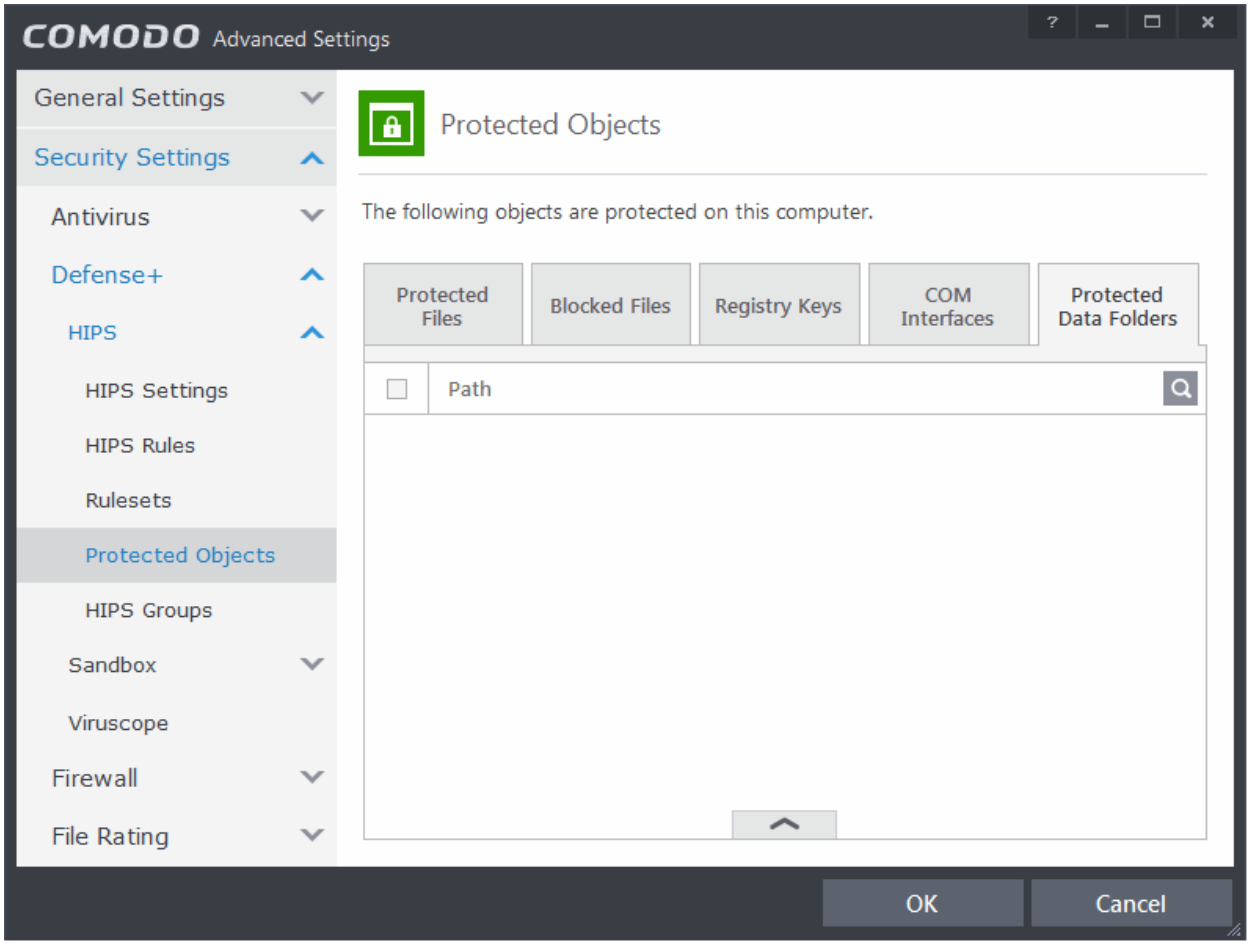
The selected item will be deleted from the COM Protection list. CIS will not generate alerts, if the COM component or the group is modified by other programs or processes.

6.2.2.4.5. Protected Data Folders

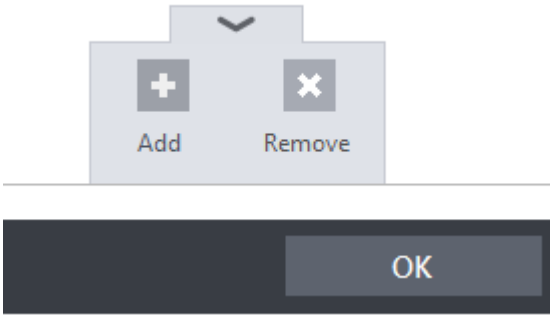
The data files in the folders listed under the Protected Data Folders area cannot be seen, accessed or modified by any known or unknown application that is running inside the sandbox.

Tip: Files and folders that are added to '**Protected Files**' interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to sandboxed programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all the sandboxed programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

To open the Protected Data Folders interface, Click the 'Protected Data Folders' tab in the Protected Objects interface:

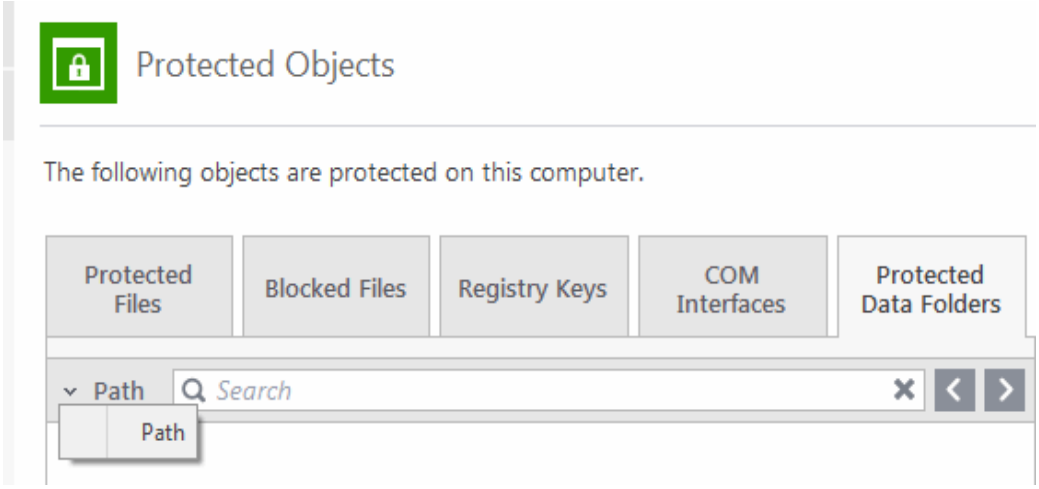


Clicking the handle at the bottom of the interface opens an options panel with the following options:



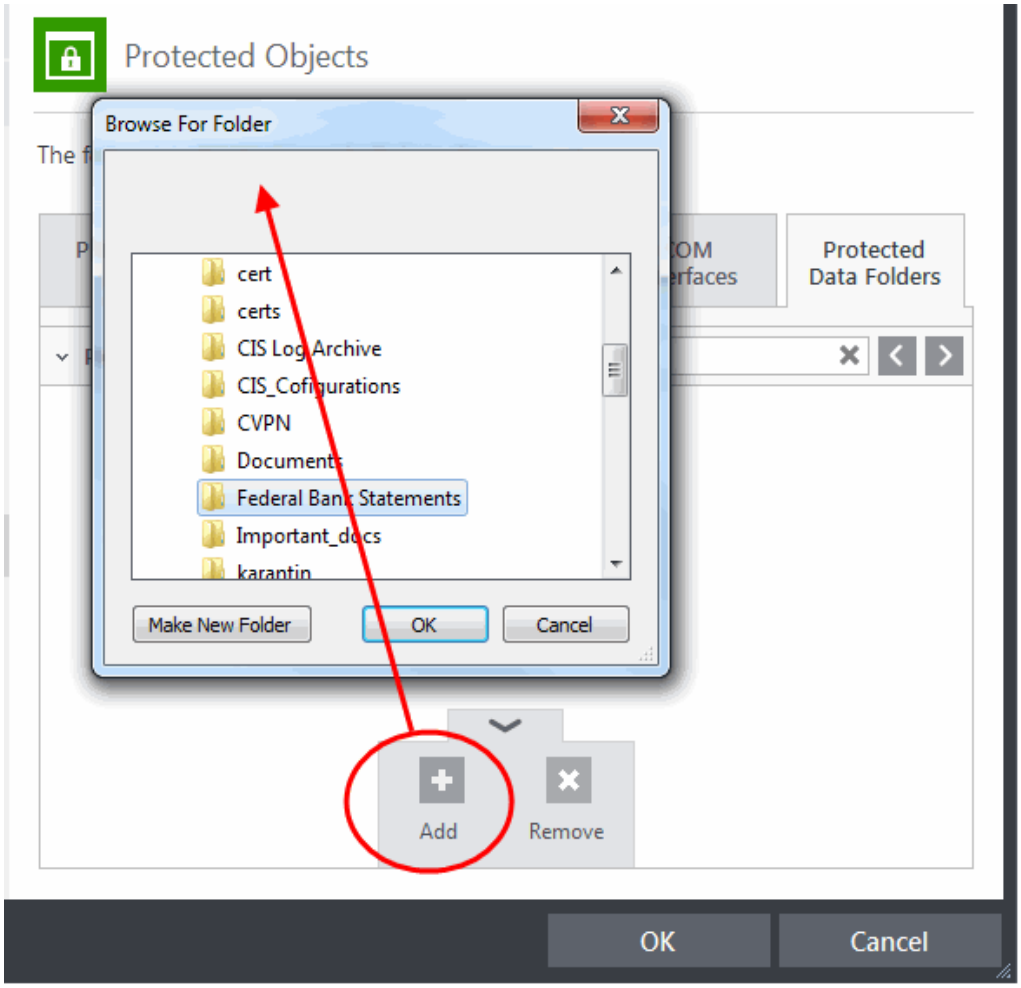
- **Add** - Allows you to add folders to Protected Data Folders list.
- **Remove** - Deletes the currently selected folder.

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

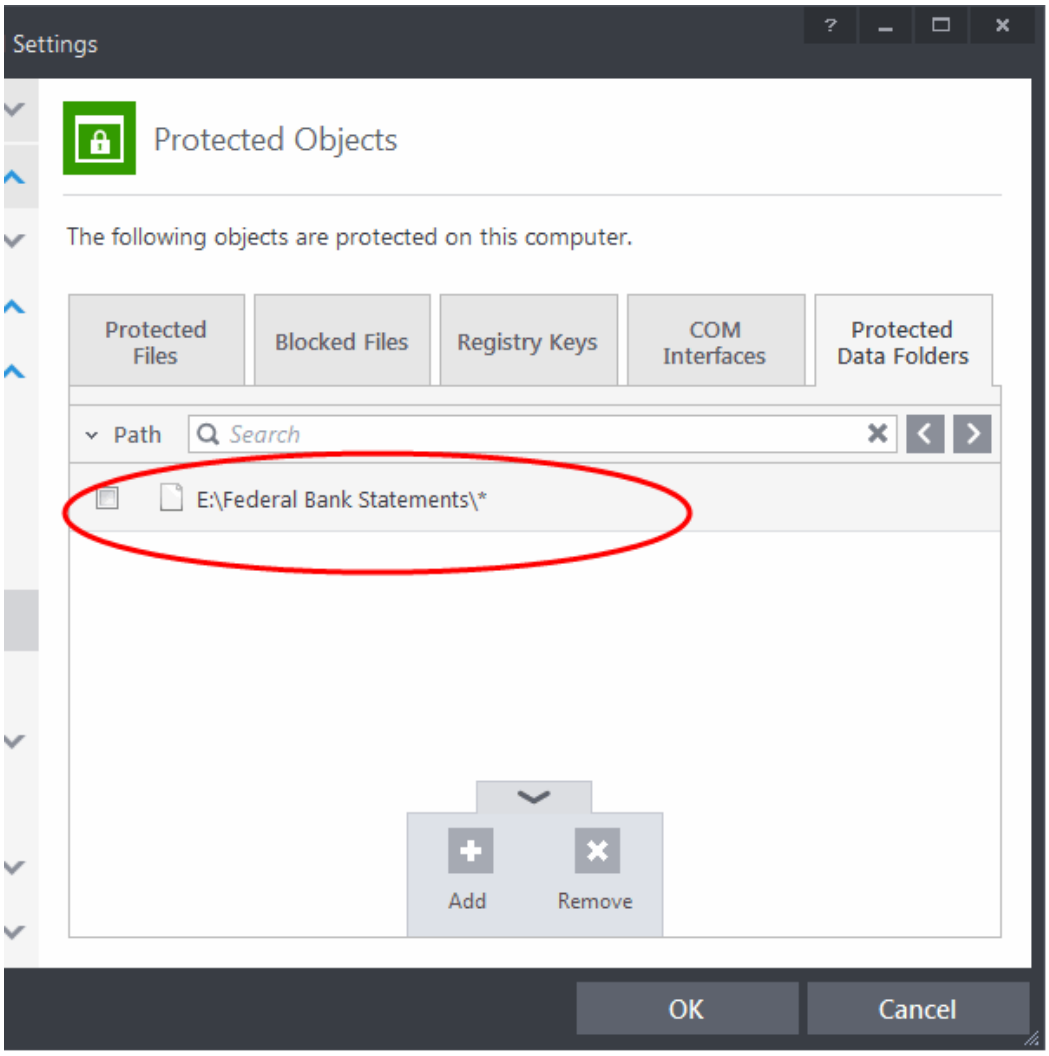


To add a folder to be protected

- Click the handle from the bottom and select 'Add'.



- Navigate to the folder to be added and click OK.



- Click OK to confirm your choice.

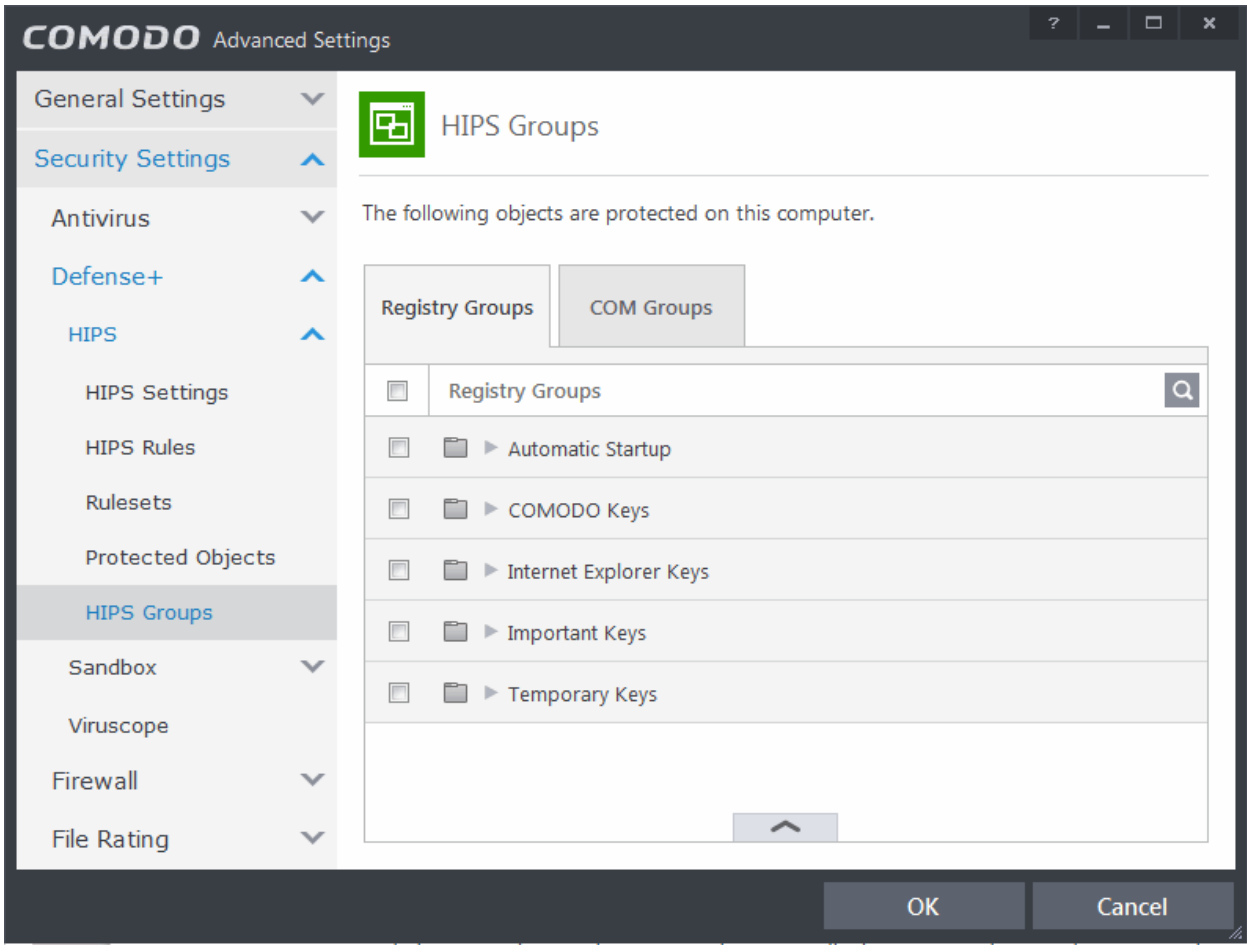
To remove an item from Protected Data Folders list

- Select the folder from the list, click the handle from the bottom and choose 'Remove'.
- The selected folder will be removed from the protected folders list. CIS will not generate alerts, if the folder is subjected to unauthorized access.

6.2.2.5. HIPS Groups

The HIPS Groups panel allows you to add, edit or remove predefined Registry and COM Groups. CIS ships with some important predefined Registry and COM Groups and this interface allows you to add new groups. Once added, these newly added groups are also available for including in the **Registry Keys** and **COM Interfaces** for protection.

The HIPS Groups panel can be accessed by clicking Security Settings > Defense+ > HIPS > HIPS Groups from the Advanced Settings interface.



The panel has two tabs:

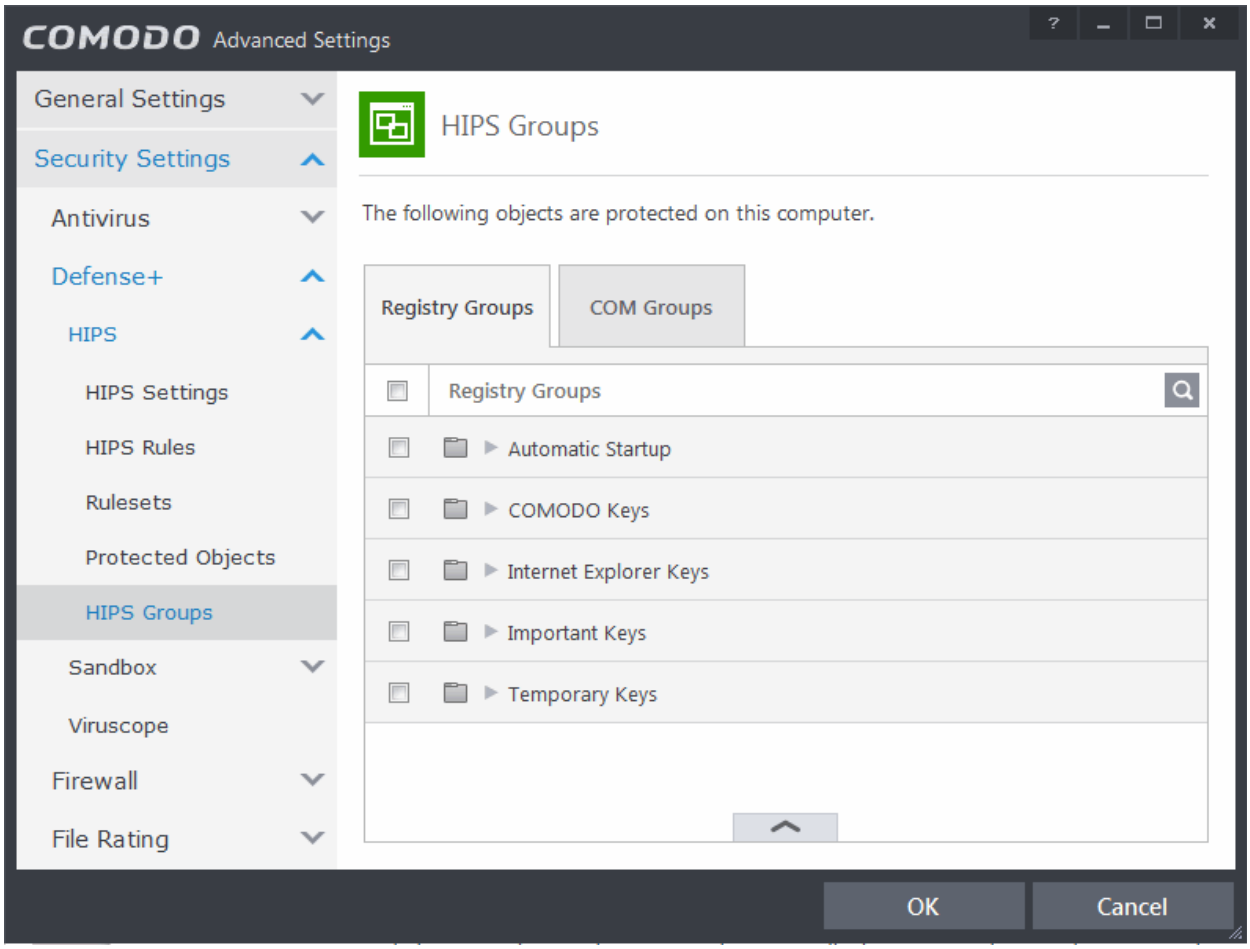
- **Registry Groups** - Allows you to create new groups and add registry keys to groups that are to be protected from changes
- **COM Groups** - Allows you to create new COM groups and add COM classes to groups that are to be protected from changes

6.2.2.5.1. Registry Groups

Registry groups are predefined batches of one or more registry keys. Creating a registry group allows you to quickly add it to Registry Protection list.

To open the Registry Groups interface

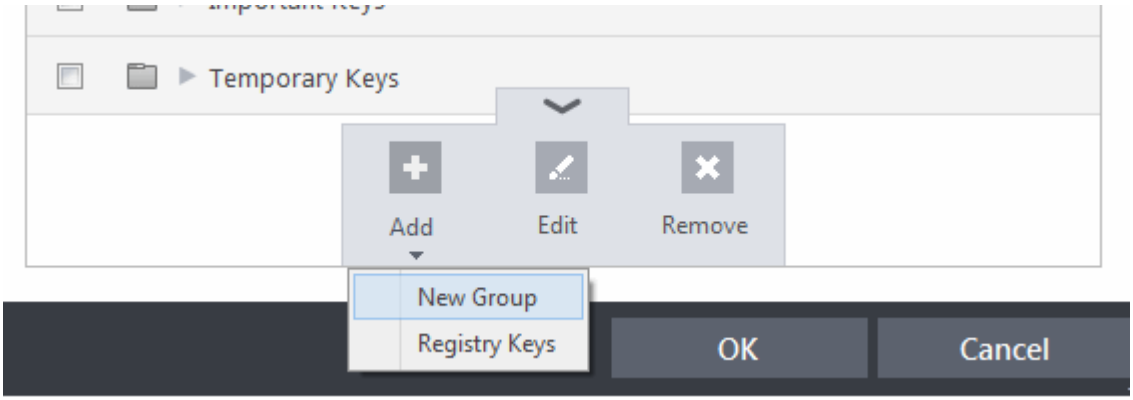
- In the Advanced Settings screen, click Security Settings > Defense+ > HIPS > HIPS Groups and select the Registry Groups tab.



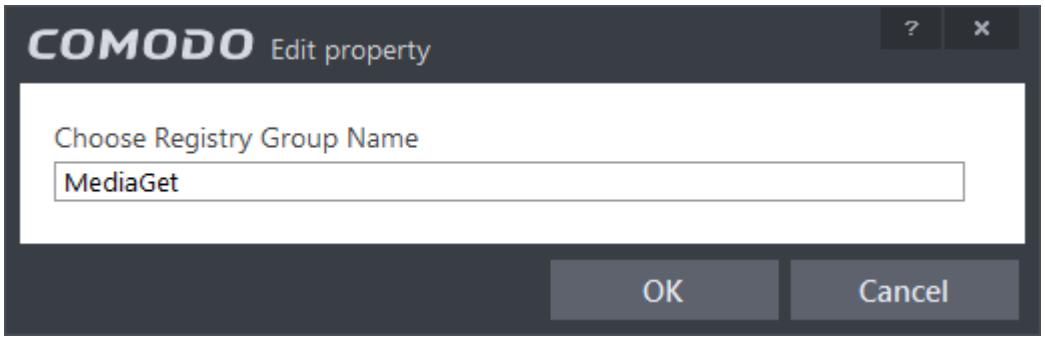
This interface allows you to

- **Create a new Registry Group**
- **Add Registry key(s) to an existing group**
- **Edit the names of an Existing Registry Group**
- **Remove existing group(s) or individual key(s) from existing group**

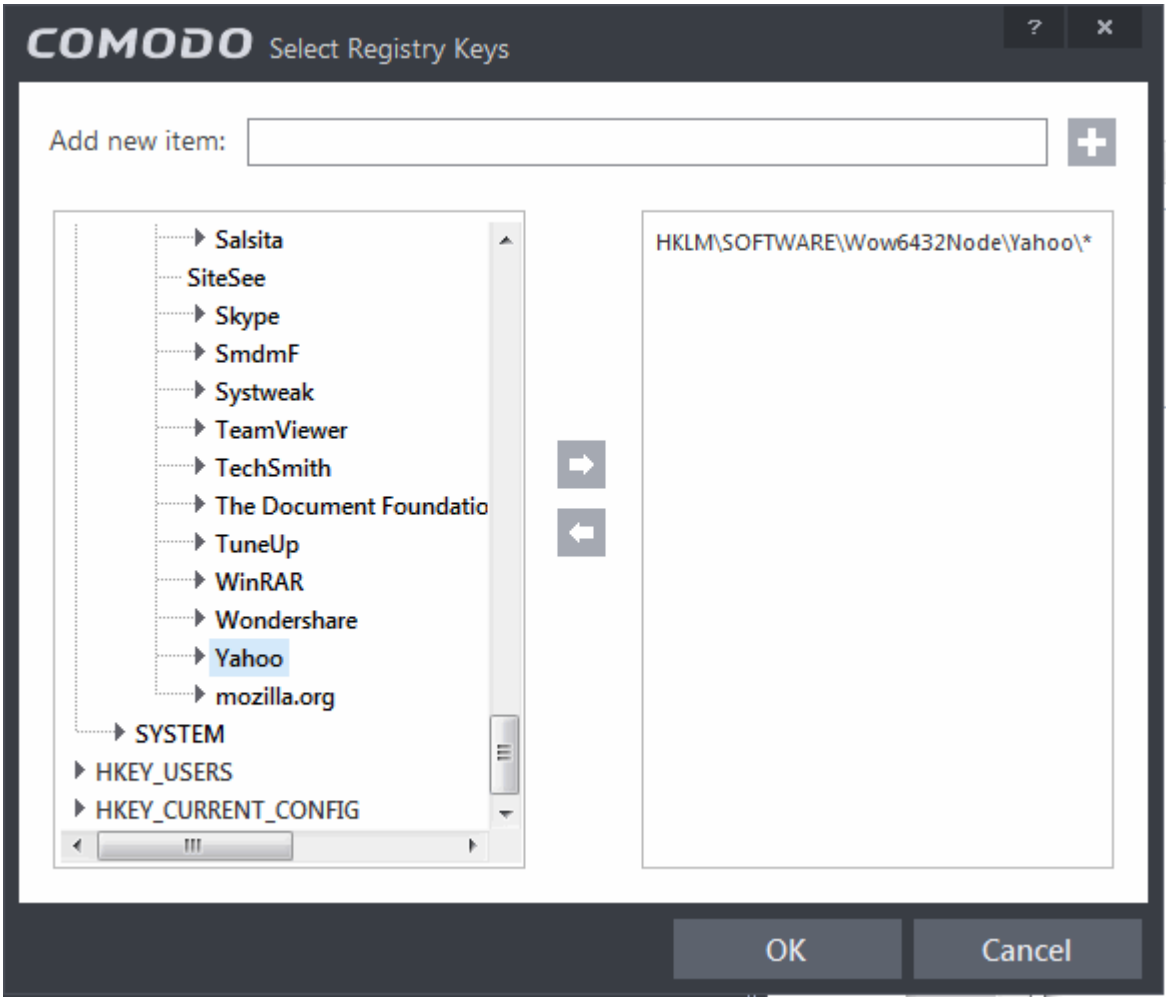
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK

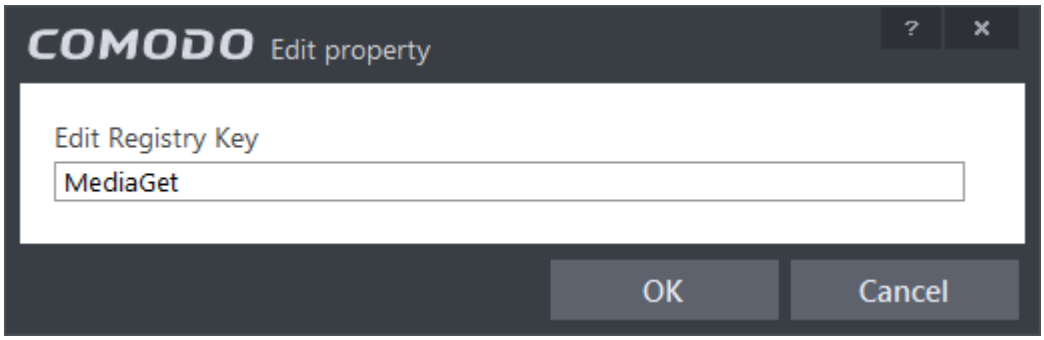


- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



- To remove a group, select the group, click the handle and choose Remove.

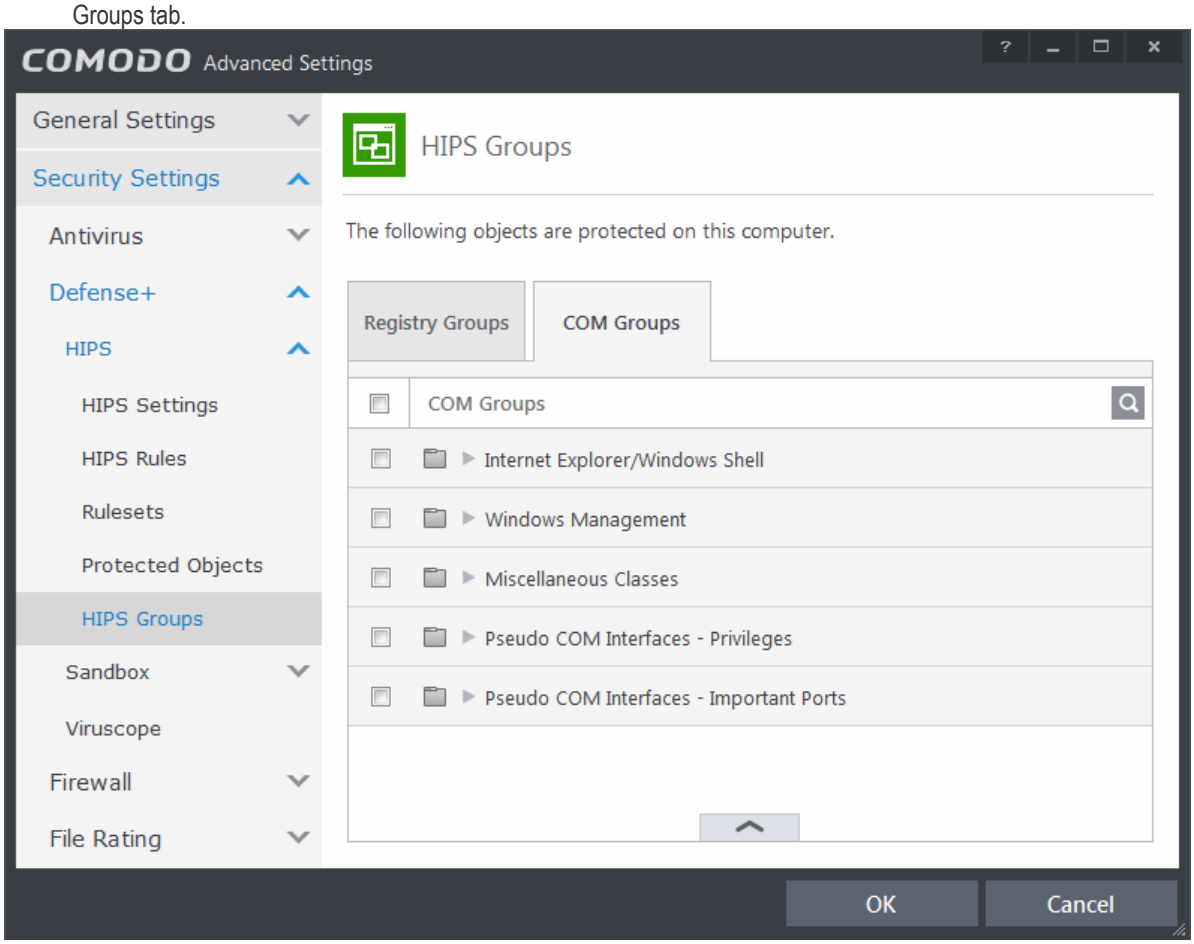
To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.5.2. COM Groups

COM groups are handy, predefined groupings of COM interfaces. Creating a COM group allows you to quickly add it to COM Protection list.

To open the Manage COM Groups interface

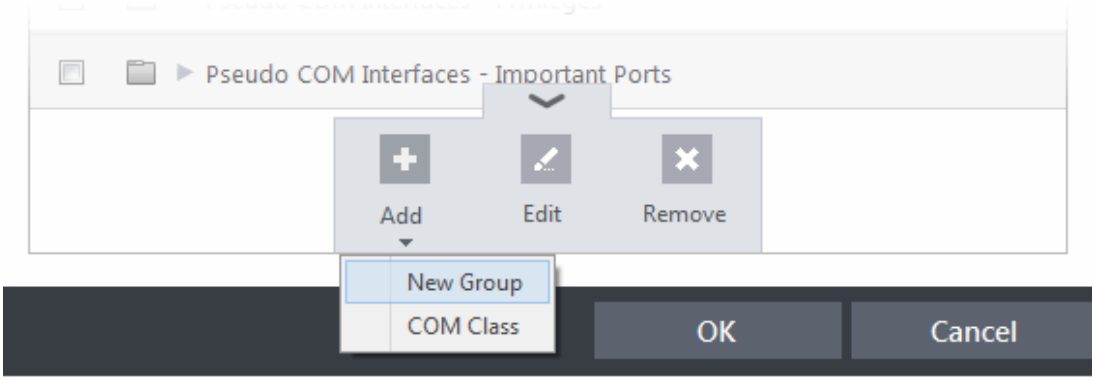
- In the Advanced Settings screen, click Security Settings > Defense+ > HIPS > HIPS Groups and select the COM Groups tab.



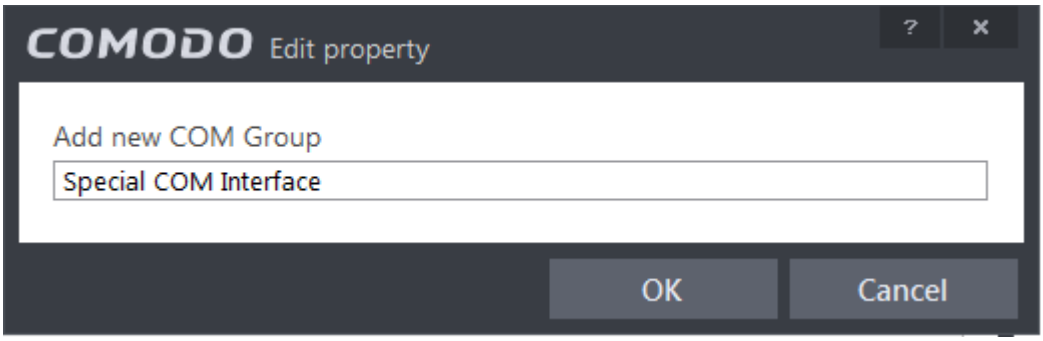
This interface allows you to:

- **Create a new COM Group**
- **Add COM Component(s) to an existing group**
- **Edit the names of an Existing COM Group**
- **Remove existing group(s) or individual COM Component(s) from existing group**

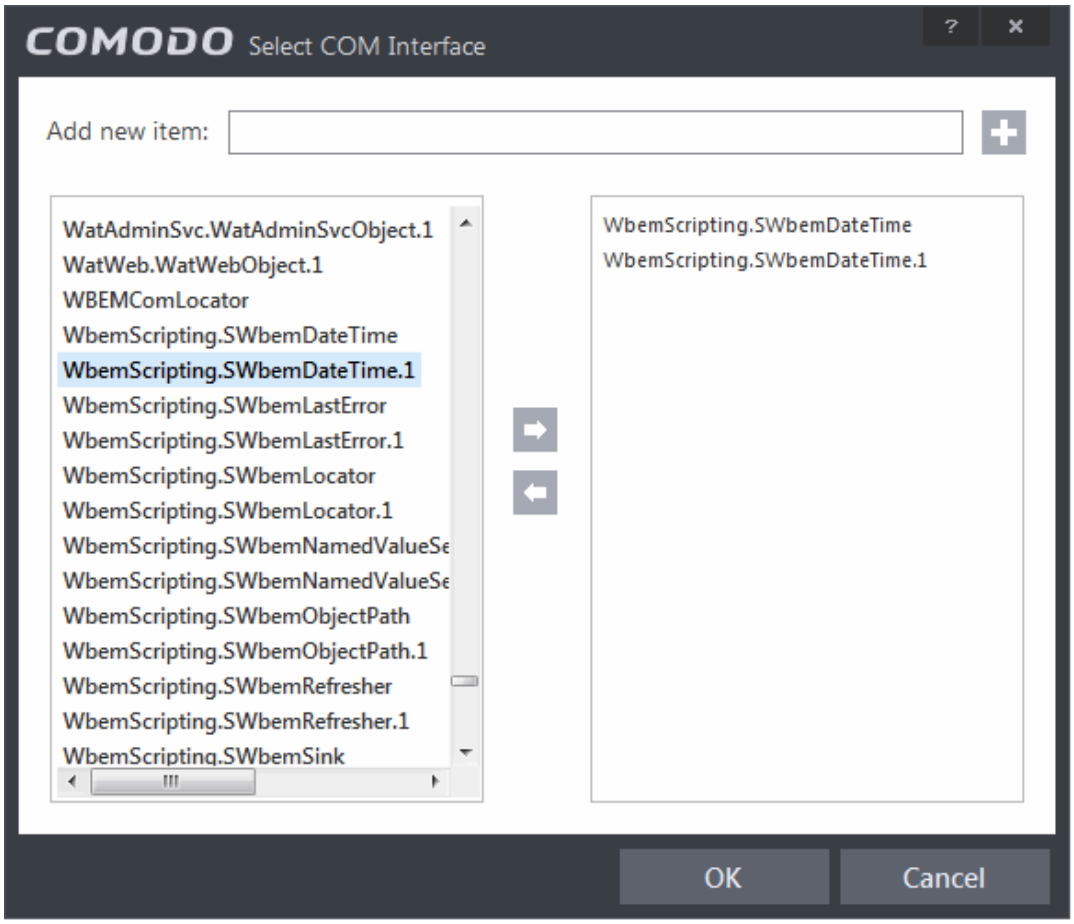
- To add a new group or add new COM Component(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK.

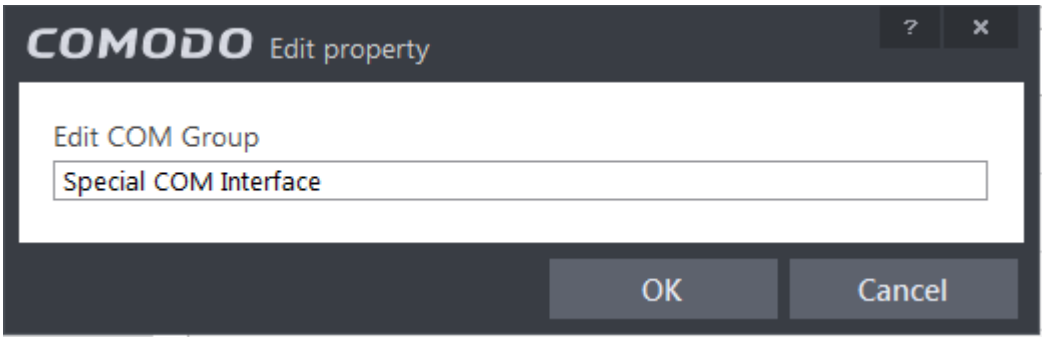


- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class. The 'Select COM Interface' dialog will be opened.



You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual COM Component from a group, click + at the left of the group to expand the group, select the item to be removed, click the handle and choose 'Remove'.

6.2.2.6. Sandbox

The Sandbox is an integral part of the Defense+ engine and is used to run potentially unsafe applications in an isolated environment to prevent damage to your system. The Defense+ engine through various analysis determines whether an application is trusted, unrecognized or malware. You can define rules how these identified applications can be run in the Sandbox, that is,

- run with restricted access to operating system resources
- run completely isolated from your operating system and files on the rest of your computer
- completely block from running
- or allow it to run outside the sandbox environment without any restriction.

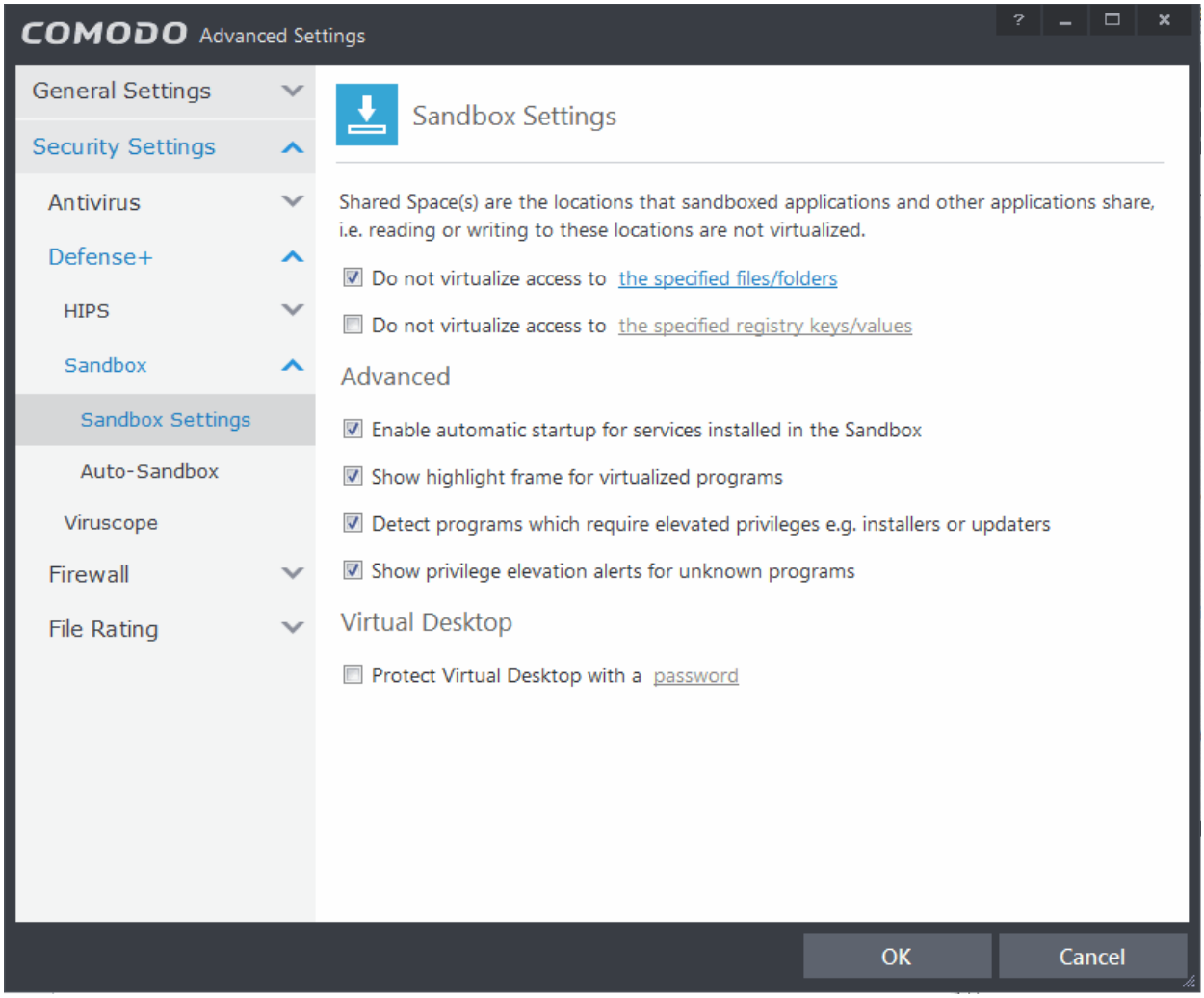
For more information about defining rules, refer to the section **Configuring Rules for Auto-Sandbox**.

The Sandbox creates a new folder called Shared Space in your system by default at 'C:/Program Data/Shared Space' for sharing files between it and the real computer system. The applications running inside the sandbox will be allowed to store their data in the shared space for future sessions. This data will can also be accessed by non-sandboxed applications. The settings for accessing Shared Space, generating sandbox alerts, enabling startup services for applications installed in sandbox can be configured in Sandbox Settings screen. Refer to the section **Configuring the Sandbox** for more details.

- For more information about the Sandbox environment refer to the section **The Sandbox - An Overview**.
- For more information about how the Defense+ engine determines the reputation of a file, refer to the section **Unknown Files: The Scanning Processes**.

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

- Windows XP 64 bit
- Windows Server 2003 64 bit



The 'Sandbox' configuration panel can be accessed by clicking 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Defense + > Sandbox'. The options 'Sandbox Settings' and 'Auto-Sandbox' under Sandbox allow you to quickly configure Sandbox settings and create rules and conditions for auto-sandboxing selected programs.

Refer to the following sections for more details:

- **The Sandbox - An Overview**
- **Unknown Files: The Scanning Processes**
- **Configuring the Sandbox Settings**
- **Configuring Rules for Auto-Sandbox**

6.2.2.6.1. The Sandbox - An Overview

Comodo Internet Security's new sandbox is an isolated operating environment for unknown and untrusted applications. Running an application in the sandbox means that it cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have integrated sand-boxing technology directly into the security architecture of Comodo Internet Security to complement and strengthen the Firewall, Defense+ and Antivirus modules.

Applications in the sandbox are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of the real system. This delivers the smoothest user experience possible by allowing unknown applications to run and operate as they normally would while denying them the potential to cause lasting damage.

After an unknown application has been placed in the sandbox, CIS also automatically queues it for submission to Comodo Cloud Scanners for automatic behavior analysis. Firstly, the files undergo another antivirus scan on our servers. If the scan discovers the file to be malicious, then it is designated as malware, the result is sent back to the local installation of CIS and the local black-list is updated. If the scan does not detect that the file is malicious then its behavior will be monitored by running it in a virtual environment within Comodo's Instant Malware Analysis (CIMA) servers and all its activities are recorded. If these behaviors are found to be malicious then the signature of the executable is automatically added to the antivirus black list. If no

malicious behavior is recorded then the file is placed into the '**File List**' with a rating of 'Unrecognized' and will continue to be executed in the sandbox. It will also be forwarded to our technicians for further checks. The cloud scanning processes take around 15 minutes to complete and report their results back to CIS.

By uniquely deploying 'sandboxing as security', CIS offers improved security, fewer pop-ups and greater ease of use than ever before.

6.2.2.6.2. Unknown Files: The Scanning Processes

- When an executable is first run it passes through the following CIS security inspections:
  - Antivirus scan
  - HIPS Heuristic check
  - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CIS (and therefore not auto-sandboxed or scanned in the cloud) in the following ways:
  - Because it is on the local Comodo White List of known safe applications
  - Because the user has rated the file as 'Trusted' in the **File List**
  - By the user granting the installer elevated privileges (CIS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CIS regards the installer and all files generated by the installer as safe)
  - Additionally, a file is not auto-sandboxed or sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS Ruleset (See **Active HIPS Rules** for more details)
- **Cloud Scanning**

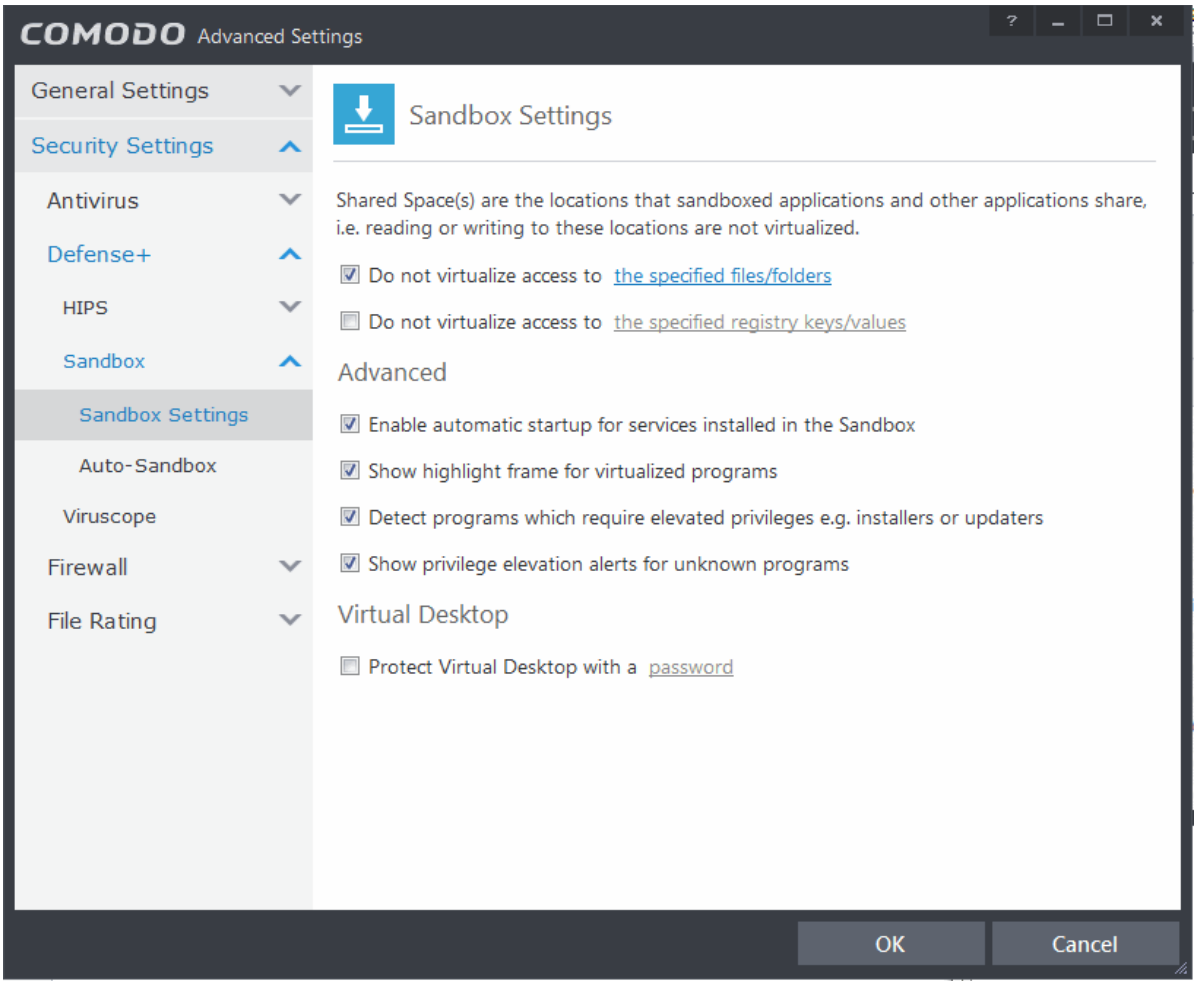
  Files and processes that pass the security inspections above but are not yet recognized as 'safe' (white-listed) are 'Unrecognized' files. In order to try to establish whether a file is safe or not, CIS will first consult Comodo's File Look-Up Server (FLS) to check the very latest signature databases:
  - A digital hash of the unrecognized process or file is created.
  - These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all known malware and a white list of the signatures of the 'safe' files.
    - First, our servers check these hashes against the latest available black-list
    - If the hash is discovered on this blacklist then it is malware
    - The result is sent back to the local installation of CIS
  - If the hash is not on the latest black-list, it's signature is checked against the latest white-list
    - If the hash is discovered on this white-list then it is trusted
    - The result is sent back to local installation of CIS
    - The local white-list is updated
  - The FLS checks detailed above are near instantaneous.
  - If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'.
- Unrecognized files are simultaneously uploaded to Comodo's Instant Malware Analysis servers for further checks:
  - Firstly, the files undergo another antivirus scan on our servers.
  - If the scan discovers the file to be malicious (for example, heuristics discover it is a brand new variant) then it is designated as malware. This result is sent back to the local installation of CIS and the local and global black-list is updated.
  - If the scan does not detect that the file is malicious then it passes onto the next stage of inspection - behavior monitoring.
  - The behavior analysis system is a cloud based service that is used to help determine whether a file exhibits malicious behavior. Once submitted to the system, the unknown executable will be automatically run in a virtual environment and all actions that it takes will be monitored. For example, processes spawned, files and registry key modifications, host state changes and network activity will be recorded.

- If these behaviors are found to be malicious then the signature of the executable is automatically added to the antivirus black list.
- If no malicious behavior is recorded then the file is placed into 'Unrecognized Files' and will be submitted to our technicians for further checks. Note: Behavior Analysis can identify malicious files and add to the global black list, but it cannot declare that a file is 'safe'. The status of 'safe' can only be given to a file after more in-depth checks by our technicians.
- In either case, the result is reported back to your CIS installation in approximately 15 minutes. If the executable was not found to be malicious then it will be run in the auto-sandbox. It will simultaneously be added to the 'Unrecognized Files' list and uploaded to our technicians for analysis. If it is discovered to be a threat then CIS will show an AV alert to the user. From this alert the user can opt to quarantine, clean (delete) or disinfect the malicious file. This new threat will be automatically added to the global black list database and therefore benefit all CIS users.

6.2.2.7. Configuring the Sandbox

The 'Sandbox Settings' section of 'Advanced Settings' allows you to configure the Sandbox settings that determine how proactive the Sandbox should be and which types of files it should check.

- The 'Sandbox Settings' panel can be accessed by clicking 'Tasks > Sandbox Tasks > Open Advanced Settings > Security Settings > Defense+ > Sandbox > Sandbox Settings

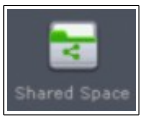


Click the following links to find out more about each section:

- **Shared Space Settings** - Files downloaded or generated by sandboxed applications that you wish to be able to access from your real system should be downloaded to the shared space
- **Advanced Settings** - Allows you to configure Sandbox alert settings as well as to enable automatic startup services for programs installed in the Sandbox.
- **Virtual Desktop** - Create an 'exit' password for the Virtual Desktop. If set, the Virtual Desktop cannot be closed or

minimized until the correct password is entered. This prevents guests or younger users from exiting this sandbox environment.

Shared Space Settings:



'Shared Space' is a dedicated area on your local drive that sandboxed applications are permitted to write to and which can also be accessed by non-sandboxed applications (hence the term 'Shared Space'). For example, any files or programs you download via a sandboxed browser that you wish to be able to access from your real system should be downloaded to the shared space. This folder is also used by the Virtual Desktop and is located by default at 'C:/Program Data/Shared Space'.

You can access the shared space folder in the following ways:

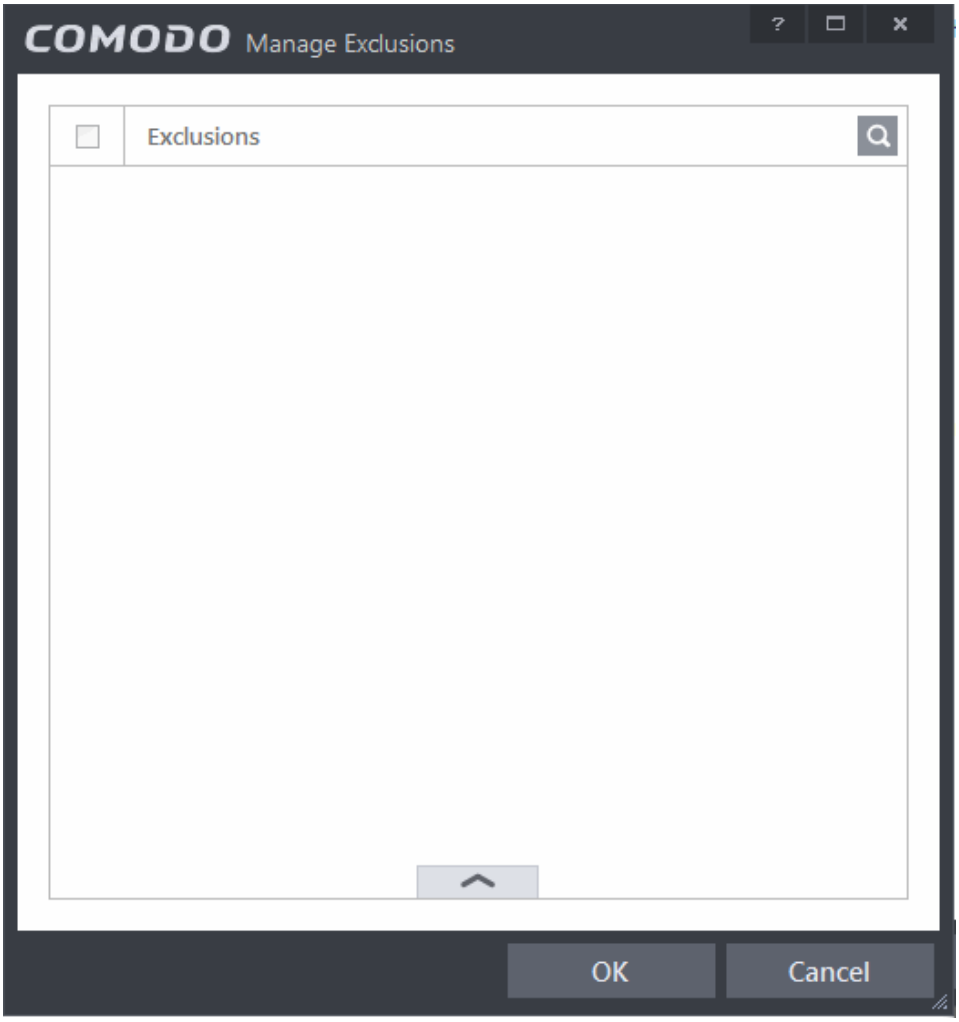
- Clicking the 'Shared Space' shortcut on your computer desktop
- Clicking 'Shared Space' button on the CIS interface
- Opening 'Sandbox Tasks' from the Tasks interface then clicking 'Open Shared Space'
- By default, sandboxed applications can access folders and files on your 'real' system but cannot save any changes to them. However, you can define exclusions to this rule by using the 'Do not virtualize access to...' links.

To define exclusions for files and folders

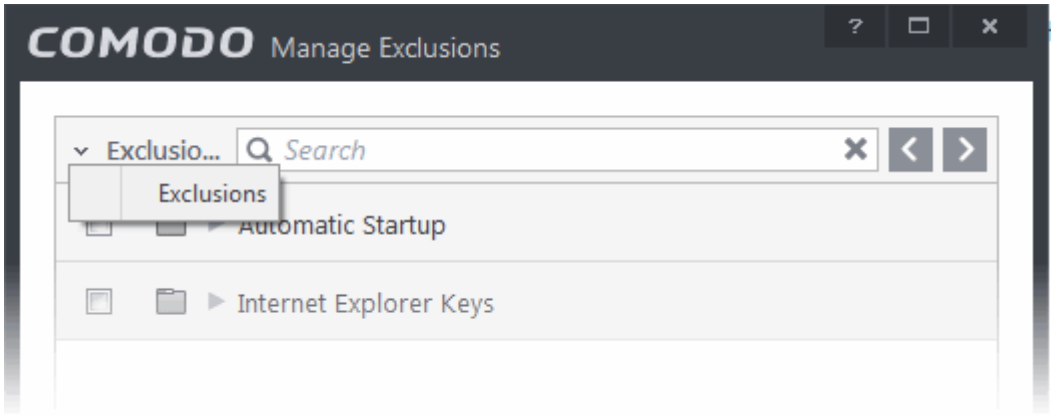
- Enable the 'Do not virtualize access to the specified files/folders' check-box then click on the words the specified files/folders. The 'Manage Exclusions' dialog will appear.
  - Click the handle at the bottom to open the tools menu then click 'Add.
  1. **Files** - Allows you to specify files or applications that sandboxed applications are able to access
  2. **Folders** - Specify a folder that can be accessed by sandboxed applications
  3. **File Groups** - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl. For more details on file groups, refer to the section **File Groups**.
  4. **Running Processes** - Allows you to add a program that sandboxed applications are able to access
- To edit an exception, select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Change file or folder location path and click 'OK'
- Click 'OK' to implement your settings

To define exclusions for specific Registry keys and values

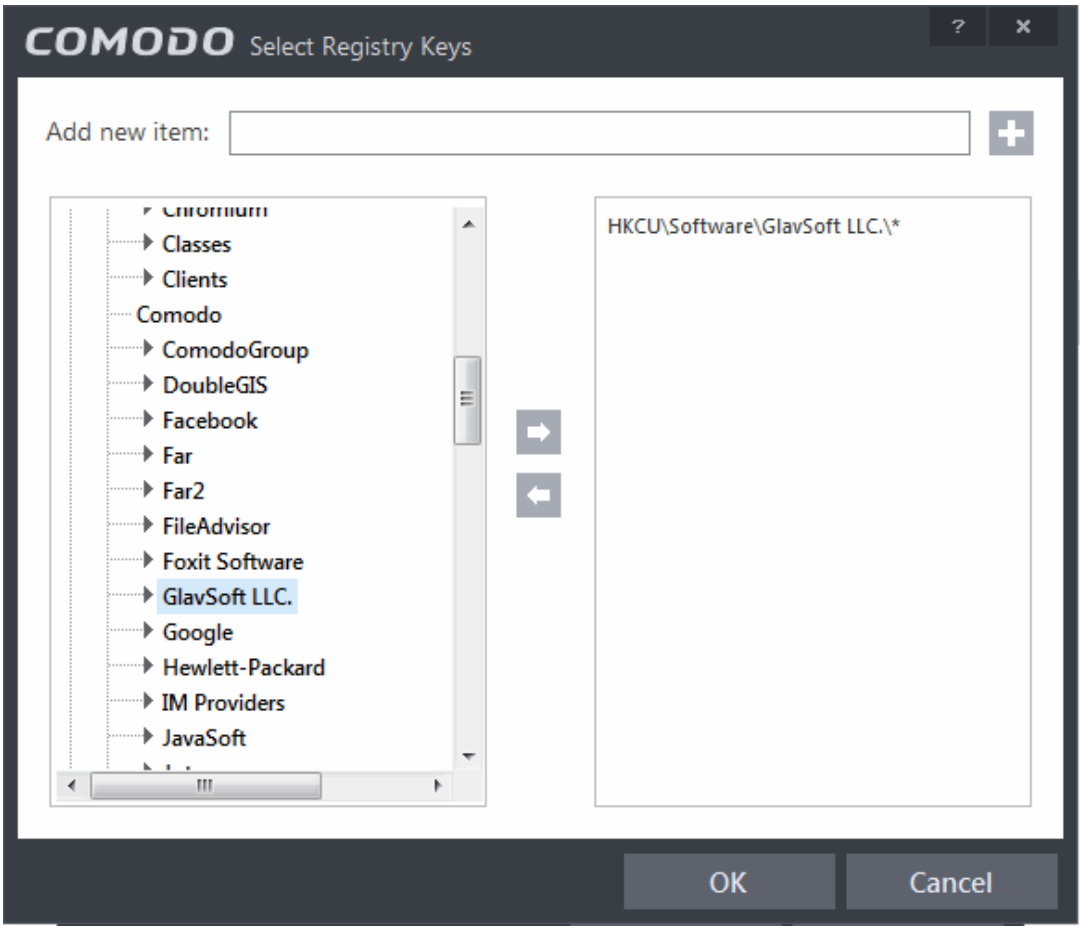
- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the words 'the specified registry keys/values'. The 'Manage Exclusions' dialog will appear.



You can search for specific excluded Registry Keys or Values from the list by clicking the search icon at the far right in the column header and entering the name of the key/value in full or part. You can navigate through the successive results by clicking the left and right arrows.

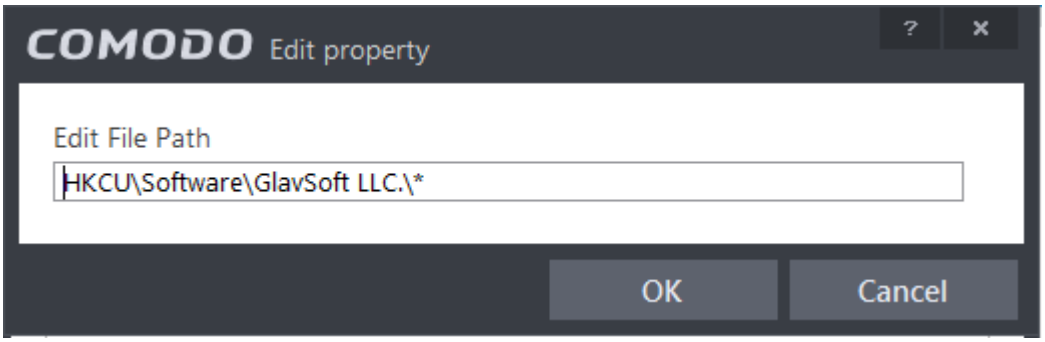


- Click the handle at the bottom to open the tools menu then click 'Add'.
  - **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exclusions. For an explanation of CIS registry groups, refer to the section **Registry Groups**.
  - **Registry Entries** - Opens an interface that allows you to quickly browse Windows registry keys and add them as exclusions:



- Click 'OK' to implement your settings.

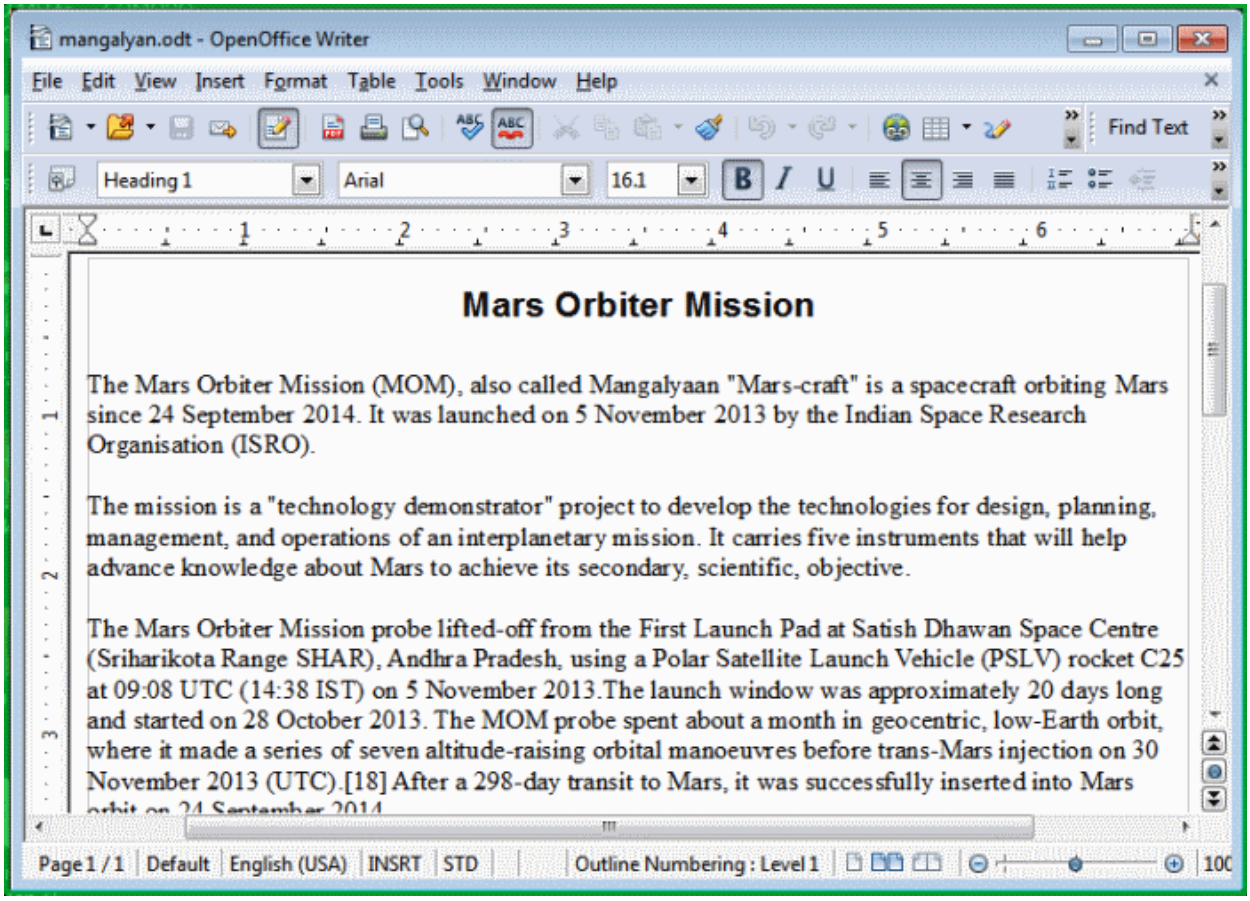
- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Edit the key path and click OK.



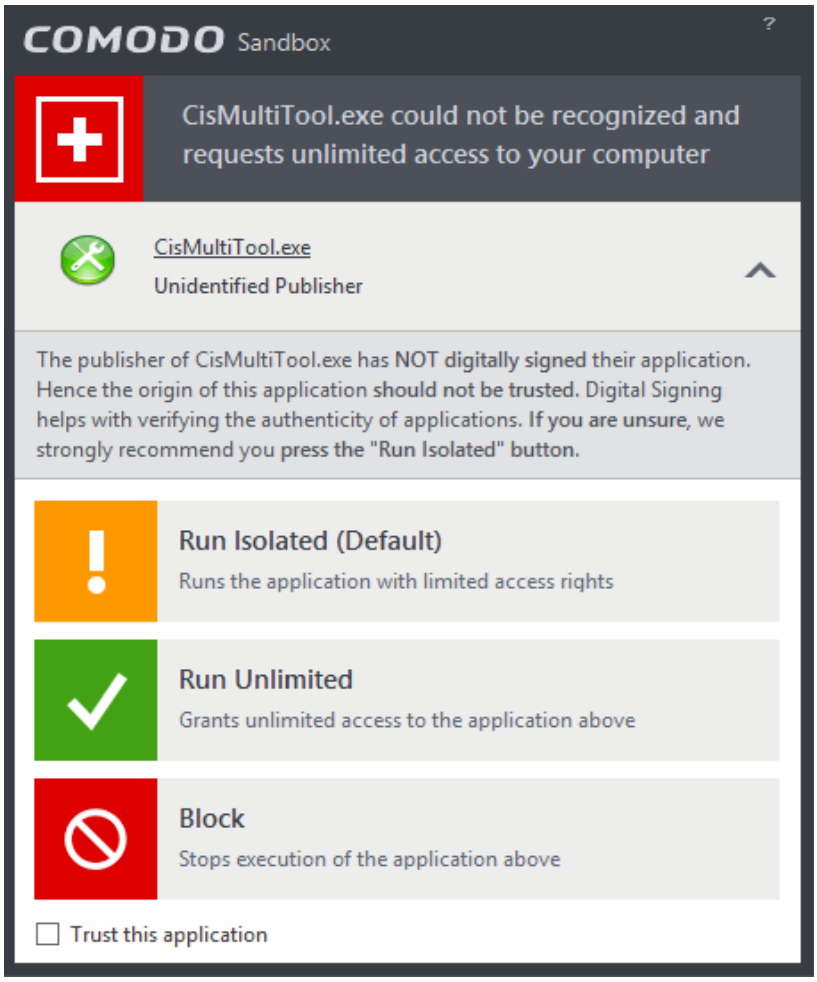
Advanced Settings:

- **Enable automatic startup for services installed in the sandbox** - By default, CIS does not permit sandboxed services to run at Windows startup. Select this check-box to allow them to do so. (***Default = Enabled***)
- **Show highlight frame for virtualized programs** - If enabled, CIS displays a green border around the windows of programs that are running inside the sandbox. (***Default = Enabled***)

The following example shows an .odt document opened with a sandboxed version OpenOffice Writer:



- **Detect programs which require elevated privileges:** Allows you to instruct the Sandbox to display alerts when an installer or updater requires administrator or elevated privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry. Refer to the section **Understanding Security Alerts** for more details.

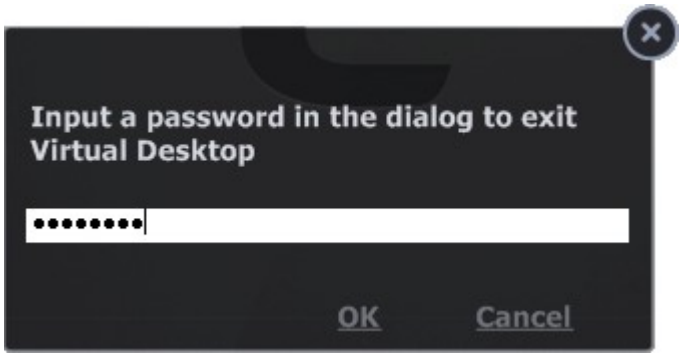


You can decide on whether or not to allow the installer or update based on your assessment, from the alert itself. (***Default=Enabled***)

- **Show privilege elevation alerts for unknown programs** : Allows you to instruct the Sandbox to display alerts when a new or unrecognized program, application or executable requires administrator or elevated privileges to run. You can decide on whether or not to allow the unknown application based on your assessment, from the alert itself. (***Default=Enabled***)

Virtual Desktop Settings

The Virtual Desktop Settings area allows you to password protect your Virtual Desktop. Once set, the password has to be entered every time when the Virtual Desktop is closed.

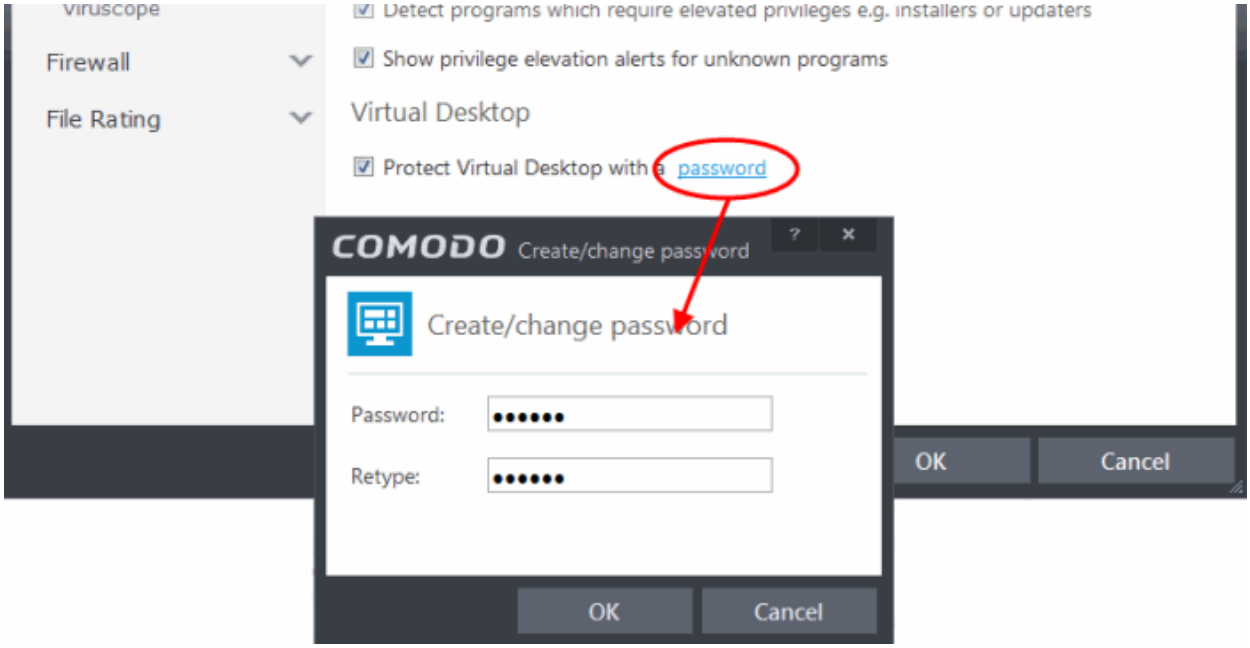


The exit password for the Virtual Desktop acts as a security measure to prevent guest users or younger users from exiting out of the isolated environment you have prepared for them and potentially exposing the real system to danger.

To set an exit password for Virtual Desktop:

- Select the 'Protect Virtual Desktop with a password' check-box then click the words password. The 'Change password'

dialog will appear.



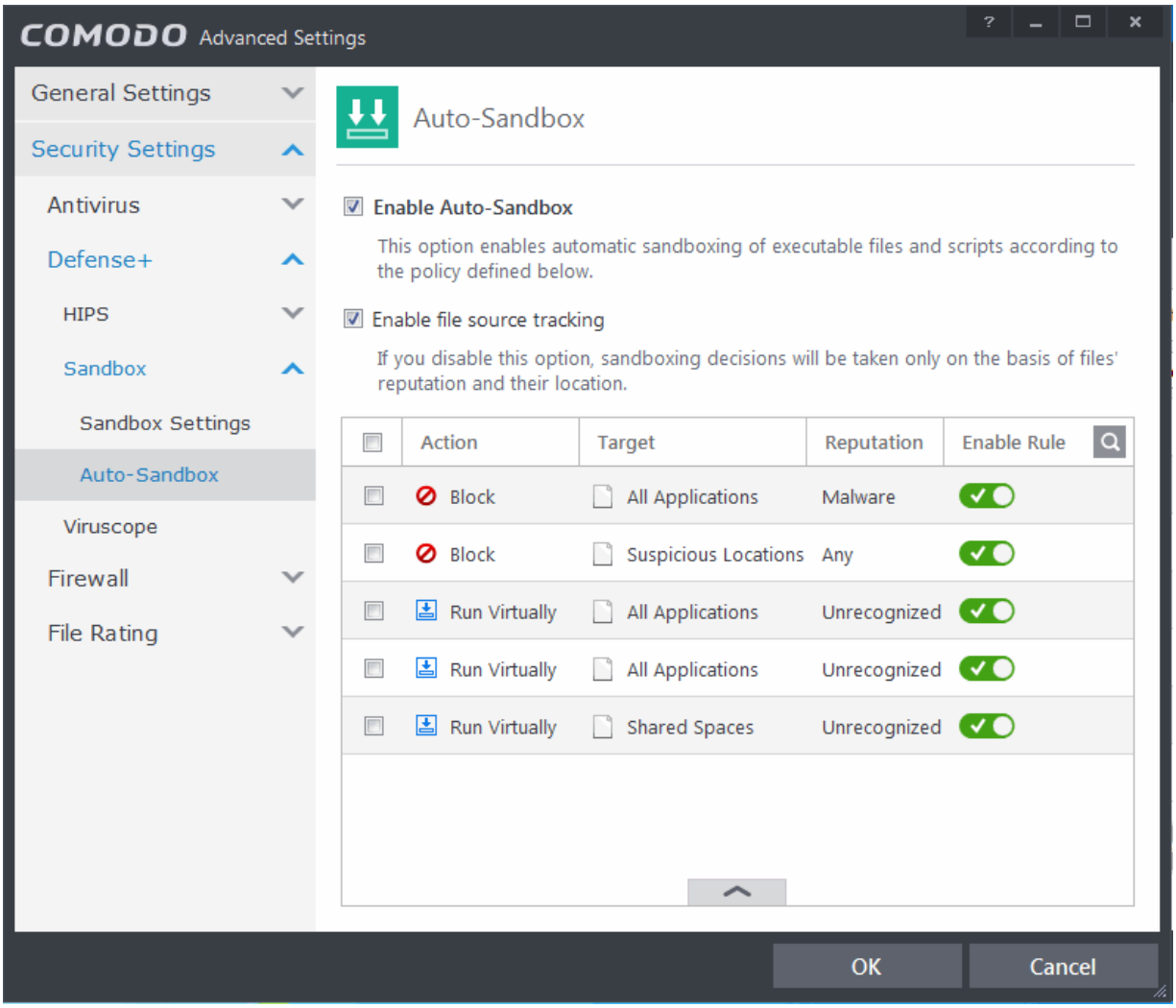
- Type a password which contains a combination of alphabetic and numeric characters and symbols which cannot be easily guessed by others. We recommend a password of at least 8 character in length.
- Re-enter the password in the 'Retype' field then click 'OK'.

You will now be asked for a password every time you exit the Virtual Desktop.

6.2.2.8. Configuring Rules for Auto-Sandbox

The 'Auto-Sandbox' interface allows you to add and define rules for programs that should be run in the sandboxed environment. A sandboxed application has much less opportunity to damage your computer because it is run isolated from your operating system and your files. This allows you to safely run applications that you are not 100% sure about. Auto-sandbox rules allows you to determine whether programs should be allowed to run with full privileges, ignored, run restricted or run in fully virtualized environment. For easy identification, Comodo Internet Security will show a green border around programs that are running in the sandbox.

- The 'Auto-Sandbox' panel can be accessed by clicking 'Tasks > Sandbox Tasks > Open Advanced Settings > Security Settings > Defense+ > Sandbox > Auto-Sandbox



- **Enable Auto-Sandbox** - Allows you to enable or disable the Sandbox. If enabled, the applications are run inside the sandbox as per the rules defined. (***Default = Enabled***)
- **Enable file source tracking** – If enabled, CIS will decide whether to sandbox a file based on file source, reputation and location. If disabled, sandbox decisions are based only on file reputation and location. ***(Default = Enabled)***

The interface displays the configured rules:

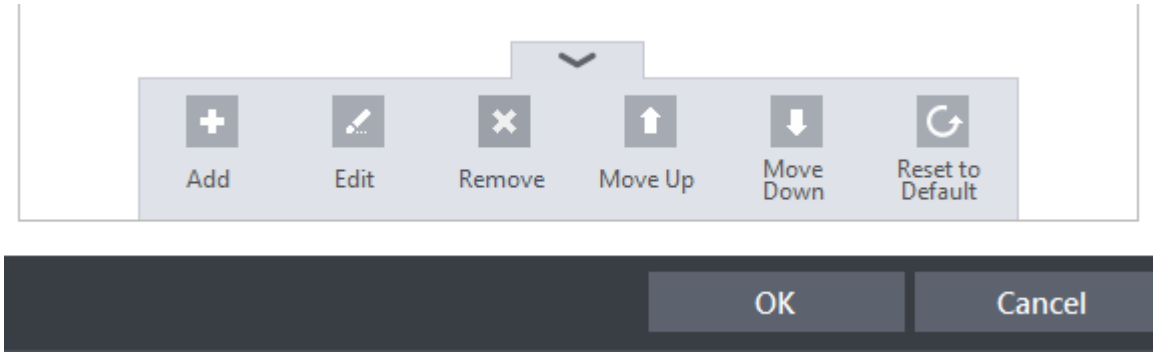
- **Action** - Displays the operation that the sandbox should perform on the target files if the rule is triggered.
- **Target** - The files, file groups or specified locations on which the rule will be executed.
- **Reputation** - The trust status of the files to which the rule should apply. Can be 'Malware', 'Trusted' or 'Unrecognized'.
- **Enable Rule** - Allows you to enable/disable the rule.

CIS ships with a set of pre-defined auto-sandbox rules that are configured to provide maximum protection for your system. The table provides the configuration settings for these pre-defined rules:

Rule	Action	Target	Restriction Level	Rating	Source			Log Action	Limit Maximum memory	Limit Program Execution Time	Quarantine
					Created by	Located on	Downloaded from				
1	Block	File Group - All Applications	N/A	Malware	Any	Any	Any	On	N/A	N/A	On

Rule	Action	Target	Restriction Level	Rating	Source			Log Action	Limit Maximum memory	Limit Program Execution Time	Quarantine
					Created by	Located on	Downloaded from				
2	Block	File Group - Suspicious Locations	N/A	Any	Any	Any	Any	On	N/A	N/A	Off
3	Run Virtual	File Group - All Applications	Off	Unrecognized	Any	Any	Internet	On	Off	Off	N/A
					Any	Network Drive	Any				
					Any	Removable Drive	Any				
4	Run Virtual	File Group - All Applications	Off	Unrecognized	File Group - Web Browsers	Any	Any	On	Off	Off	N/A
					File Group - Email Clients	Any	Any				
					File Group -File Downloaders	Any	Any				
					File Group -Pseudo-File Downloaders						
5	Run Virtual	File Group - Shared Spaces	Off	Unrecognized	Any	Any	Any	On	Off	Off	N/A

Clicking the handle at the bottom of the interface opens a rule configuration panel:



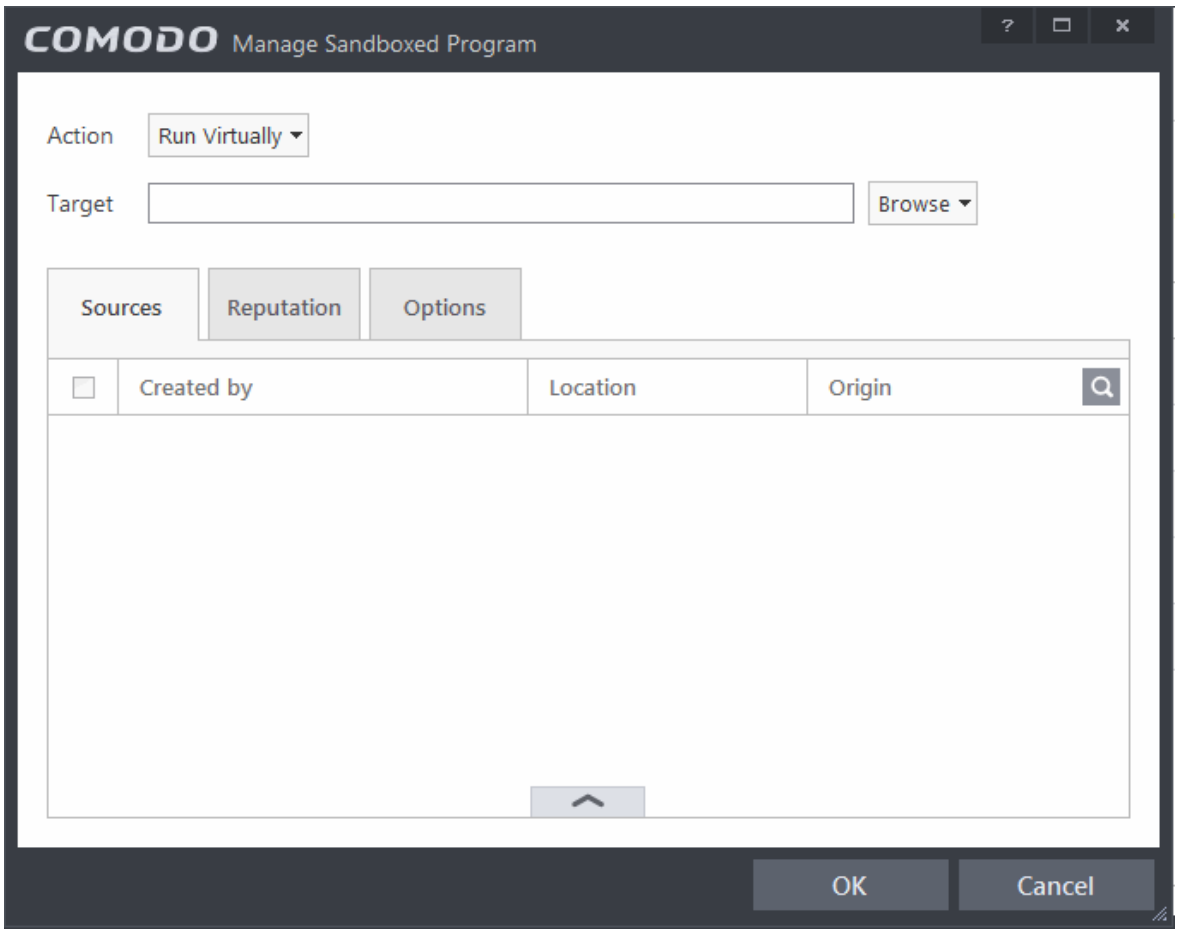
- **Add** - Allows you to add a new sandbox rule. See the section **'Adding an Auto-Sandbox Rule'** for guidance on creating a new rule.
- **Edit** - Allows you to modify the selected sandbox rule. See the section **'Editing an Auto-Sandbox Rule'** for more details.
- **Remove** - Deletes the selected rule.

Users can also re-prioritize the sandbox rules by using the 'Move Up' and 'Move Down' buttons.

Adding an Auto-Sandbox Rule

Auto-sandbox rules can be created for a single application, for all applications in a folder or file group, from running processes or for applications based on their file or process hash. 'Source', 'Reputation' and 'Options' allow you to add detailed filters to your rule. They are, however, optional, so you can create a very simple rule to run an application in the sandbox just by specifying the action and the target application.

- Click the Add button from the options.

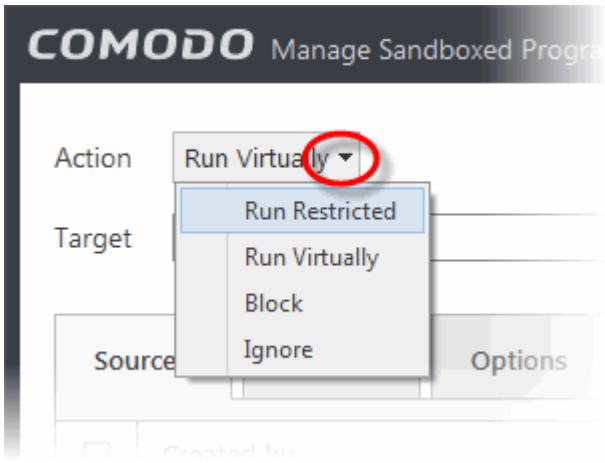


The Manage Sandboxed Program screen will be displayed.

- **Step 1** - Select the Action
- **Step 2** - Select the Target
- **Step 3** - Select the Sources
- **Step 4** - Select the File Reputation
- **Step 5** - Select the Options

Step 1 - Select the Action

The options under the Action drop-down button combined with the Set Restriction Level setting in the Options tab determine the amount of privileges an auto-sandboxed application has access to other software and hardware resources on your computer.



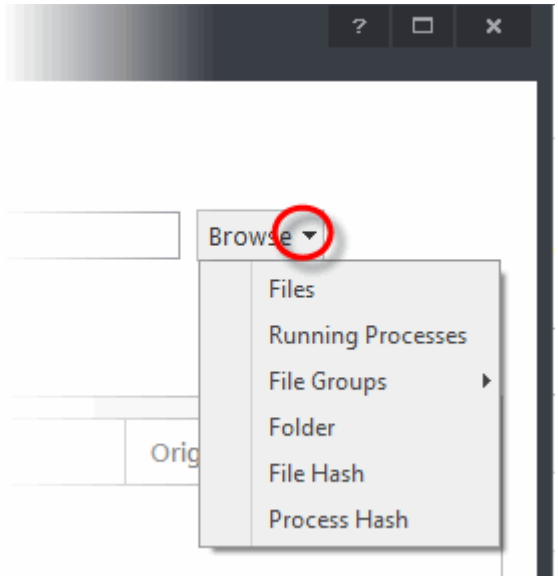
The options available under the Action button are:

- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Run Restricted** - The application is allowed to access 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 sandboxed and allowed to run with all privileges.

Select the action from the options.

Step 2 - Select the Target

The next step is to select the target to which the auto-sandbox rule is to be applied. Click the Browse button beside the Target field.

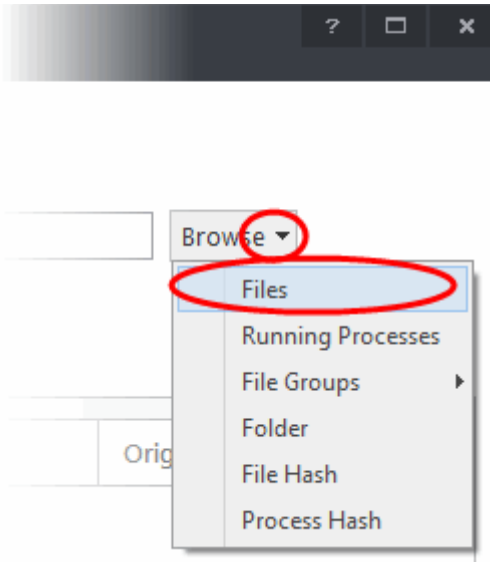


You have six options available to add the target path.

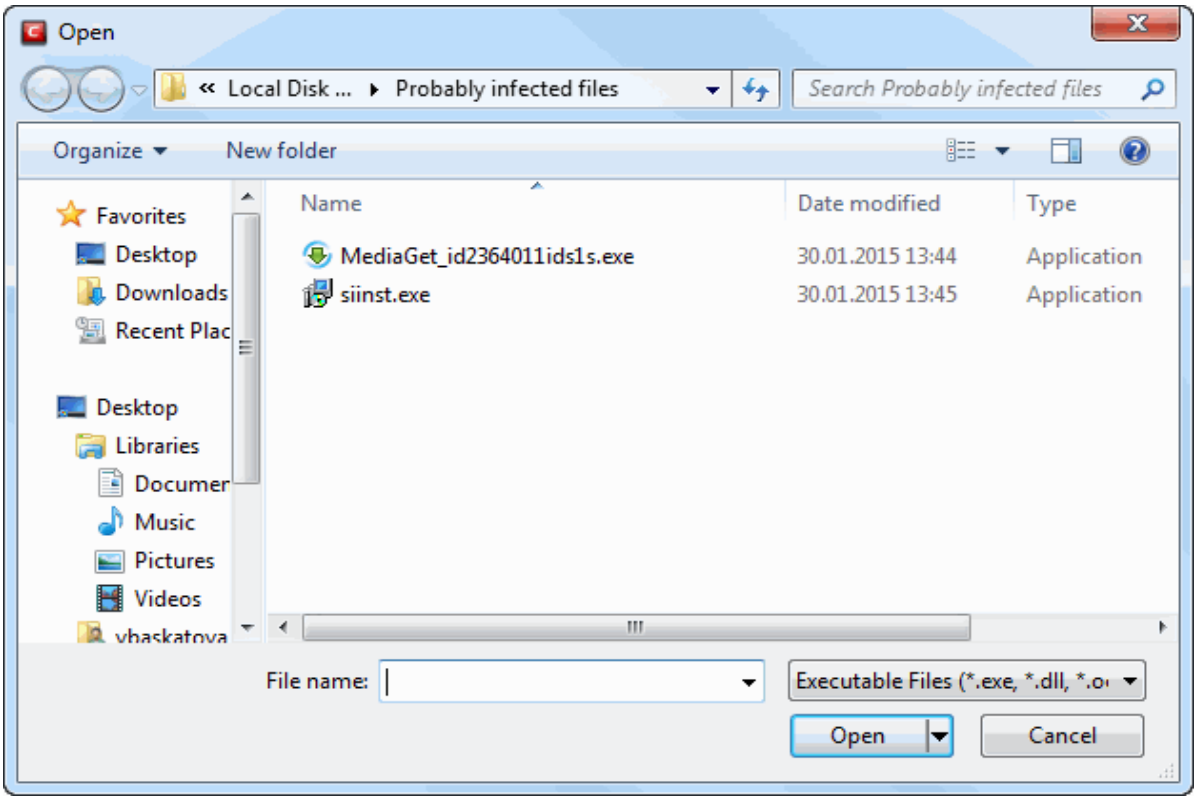
- **Files** - Allows to add individual files as target.
- **Running Processes** - As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** - Allows to add predefined File Groups as target. To add or modify a predefined file group refer to the section **File Groups** for more details.
- **Folder** - Allows you to add a folder or drive as the target
- **File Hash** - Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

Adding an individual File

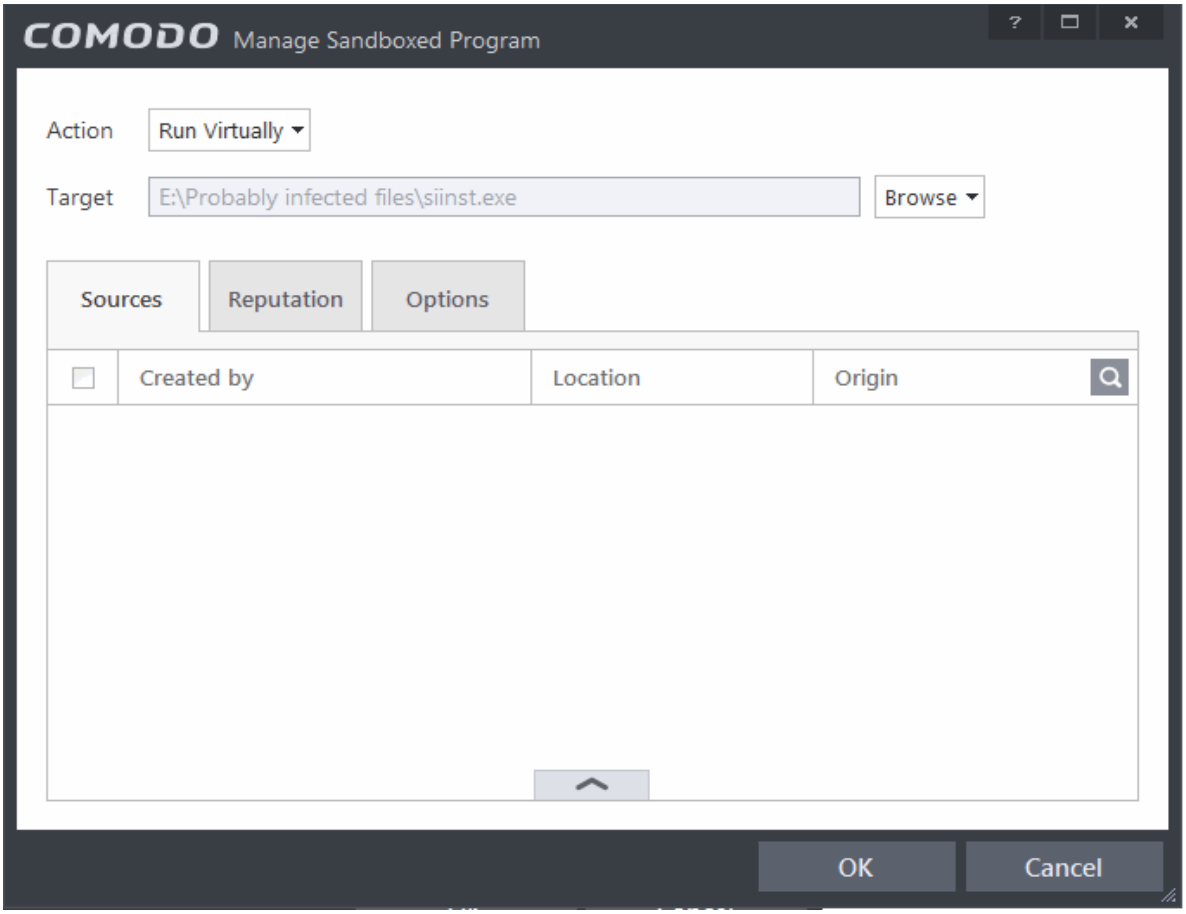
- Choose 'Files' from the 'Browse' drop-down.



- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'



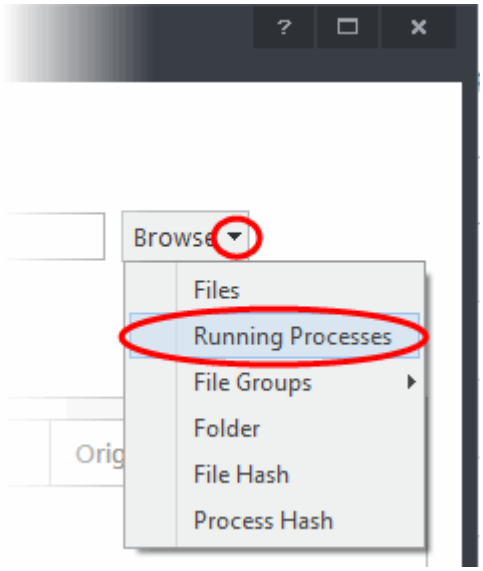
The file will be added as target and will be run as per the action chosen in **Step 1**.



If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

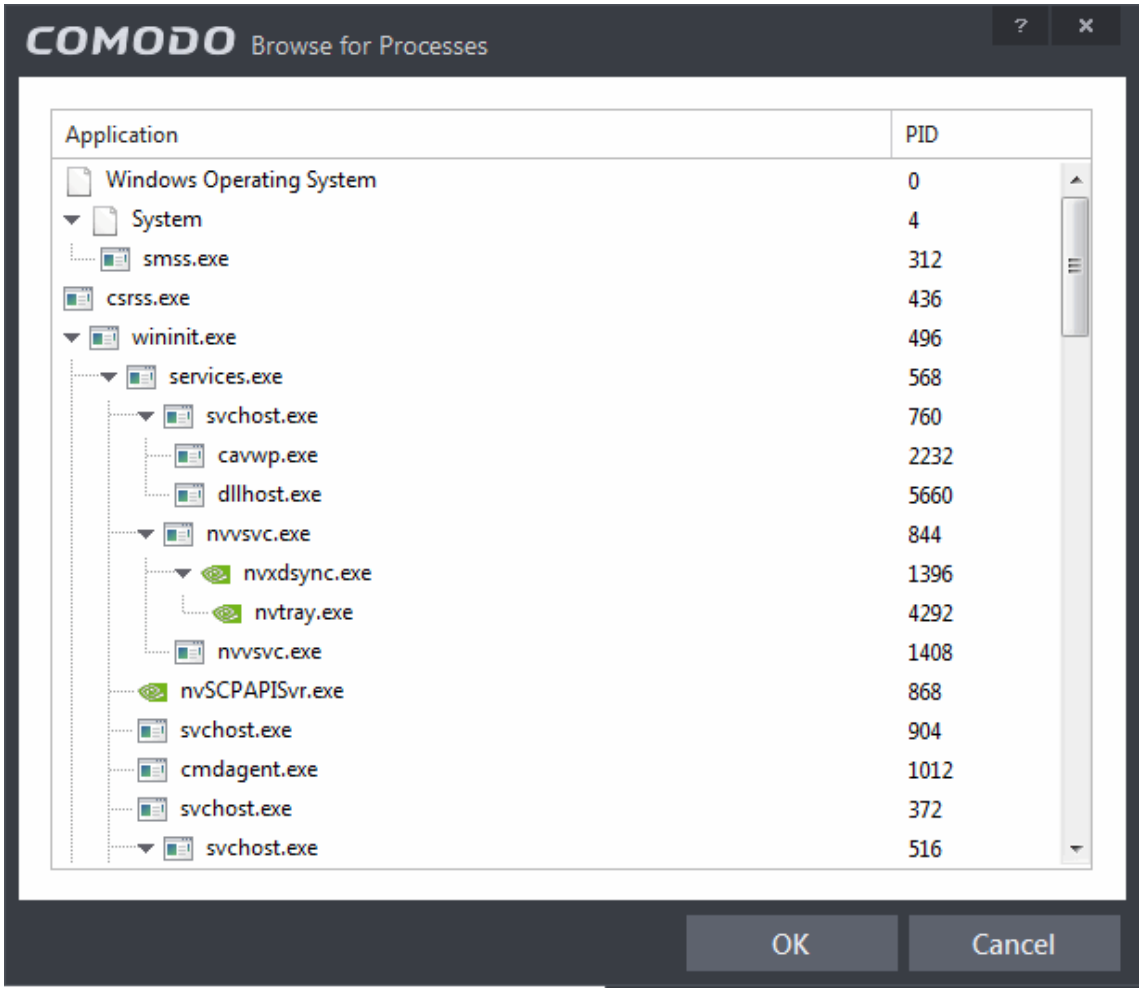
Adding an application from a running processes

- Choose 'Running Processes' from the 'Browse' drop-down.

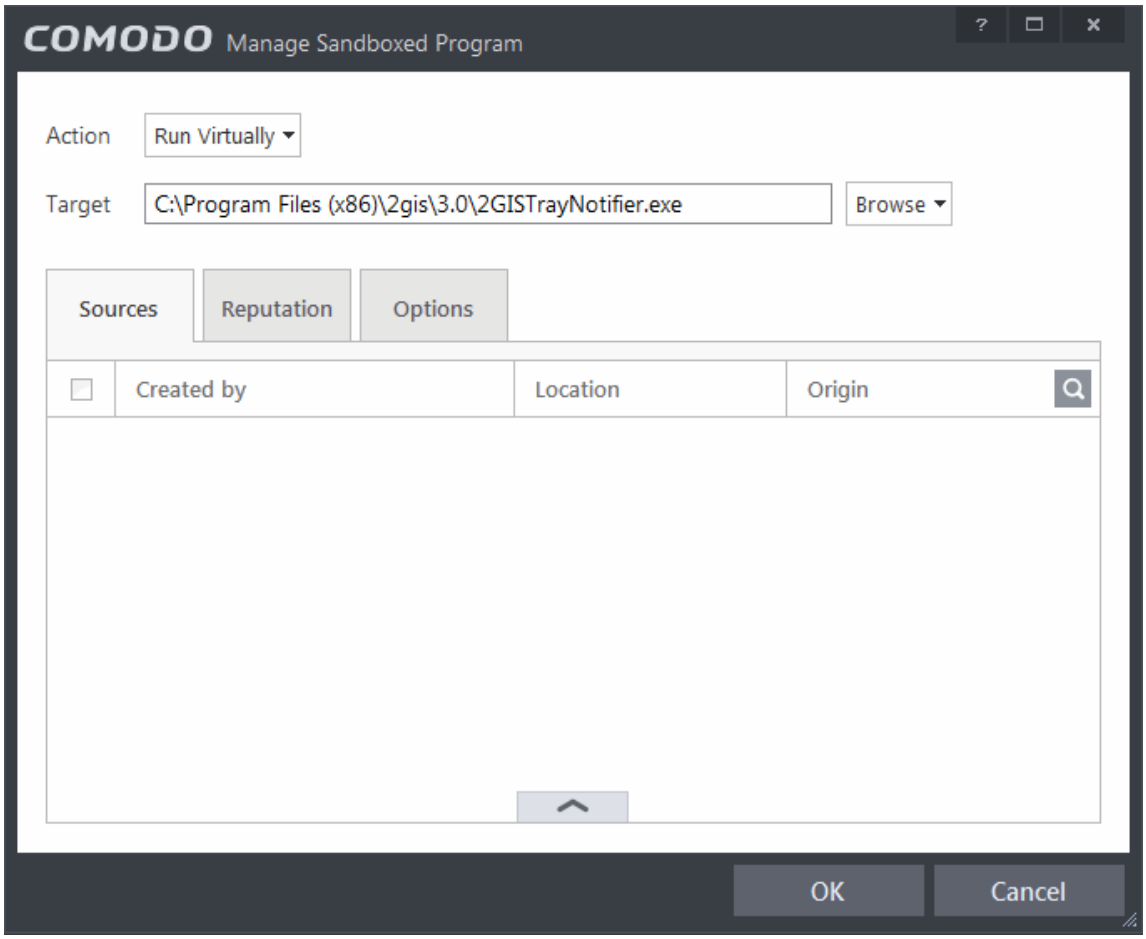


A list of currently running processes in your computer will be displayed.

- Select the process, whose target application is to be added to target and click 'OK' from the Browse for Process dialog.



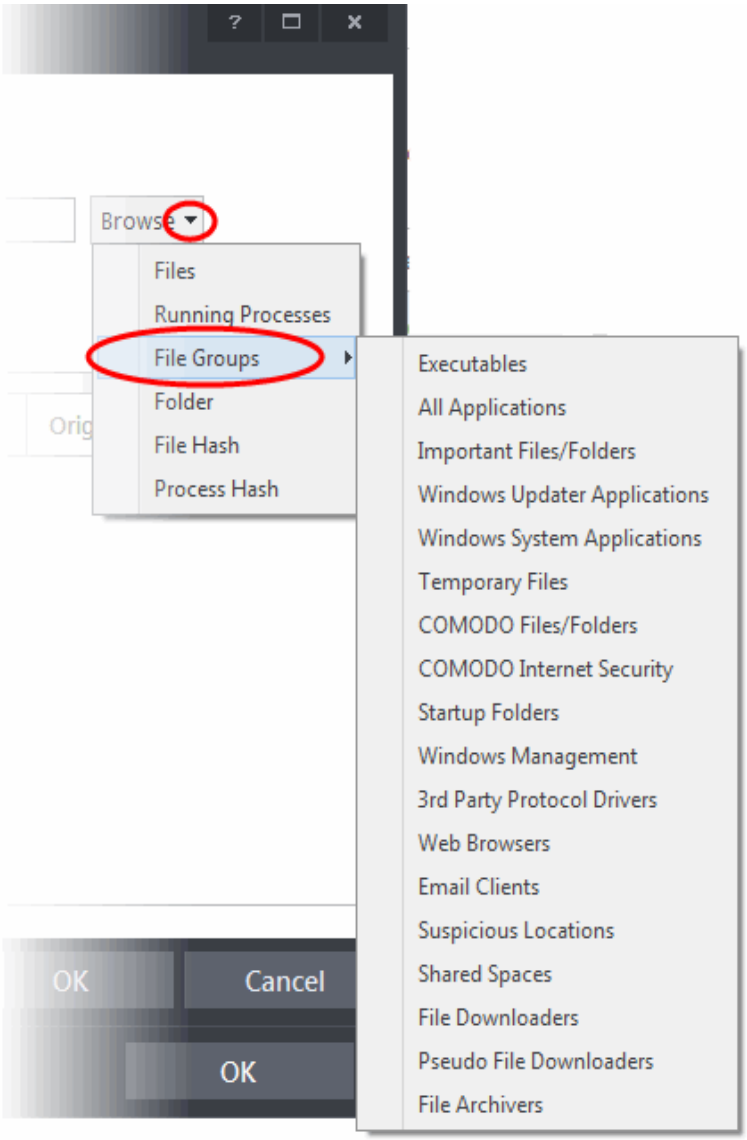
The file will be added as target and will be run as per the action chosen in **Step 1**.



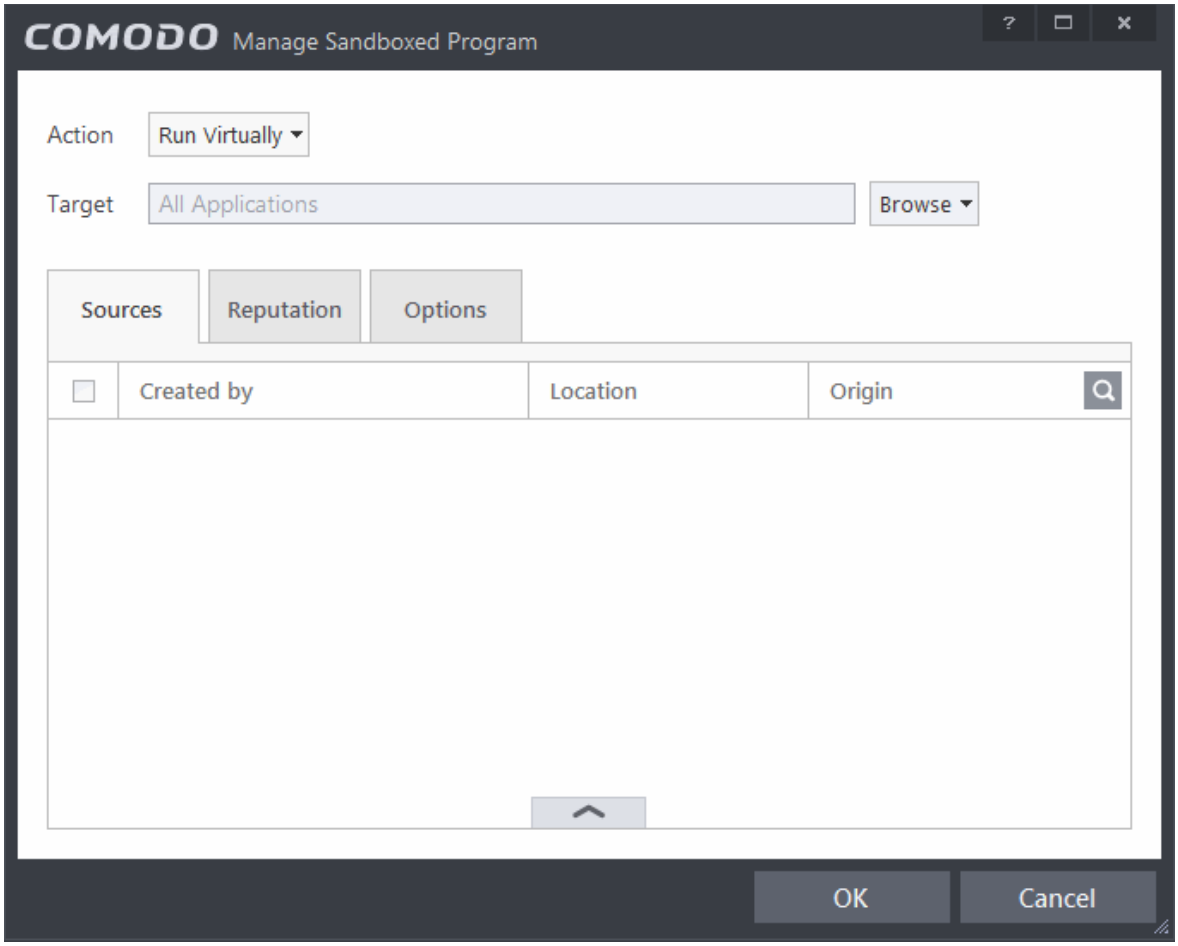
If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Adding a File Group

- Choose 'File Groups' from the 'Browse' drop-down. Choosing File Groups allows you to include a category of pre-set files or folders. For more details on how to manage file groups refer to the section **File Groups**.



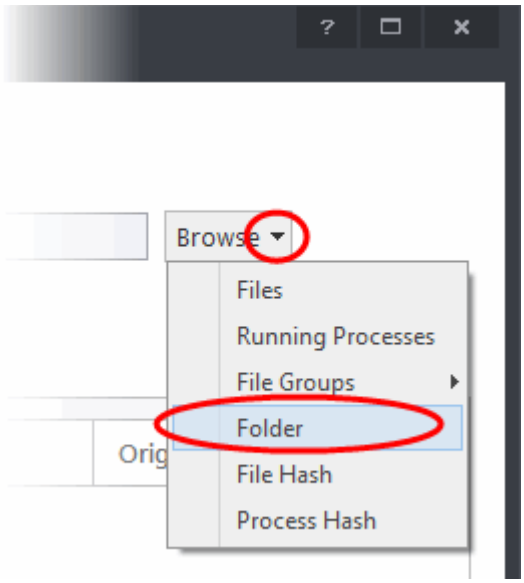
- Select the preset file group from the options.
- The file group will be added as target and the applications inside it will be run as per the action chosen in **Step 1**.



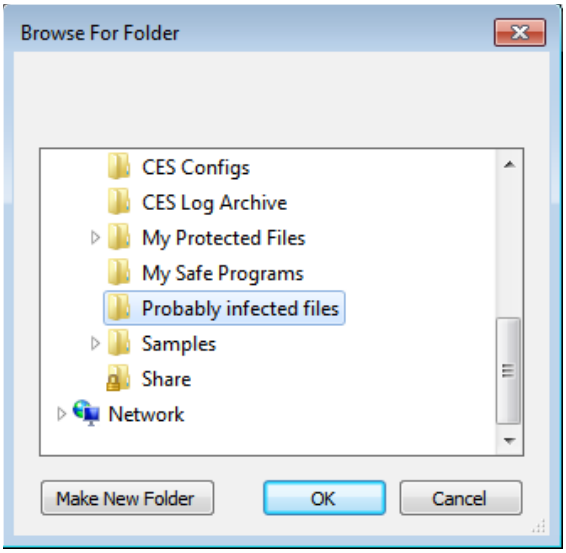
If you want to just add the applications in the file group for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Adding a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.

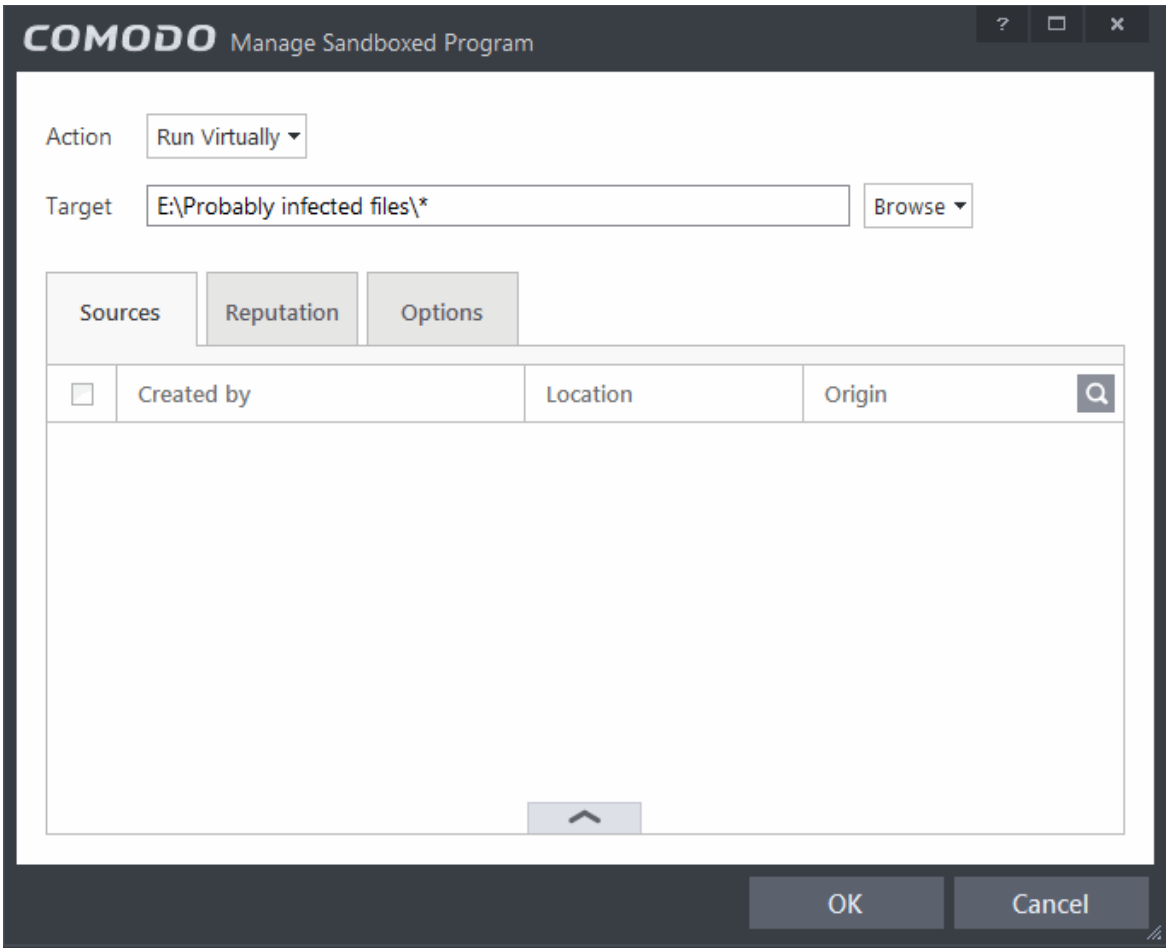


The 'Browse for Folder' dialog will appear.



- Navigate to the drive partition or folder you want to add as target and click OK

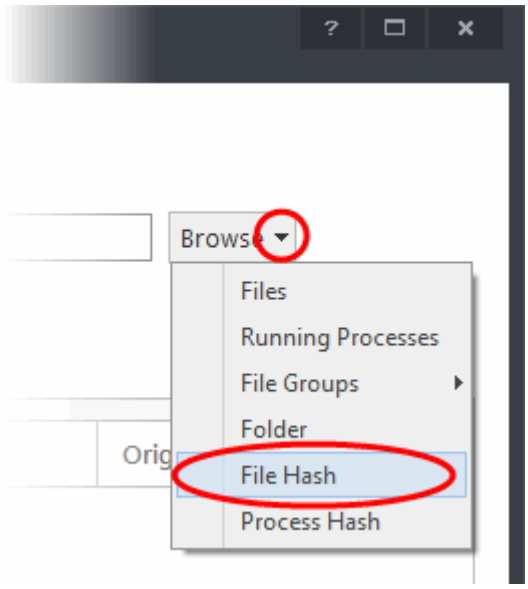
The drive partition/folder will be added as target and will be run as per the action chosen in **Step 1**.



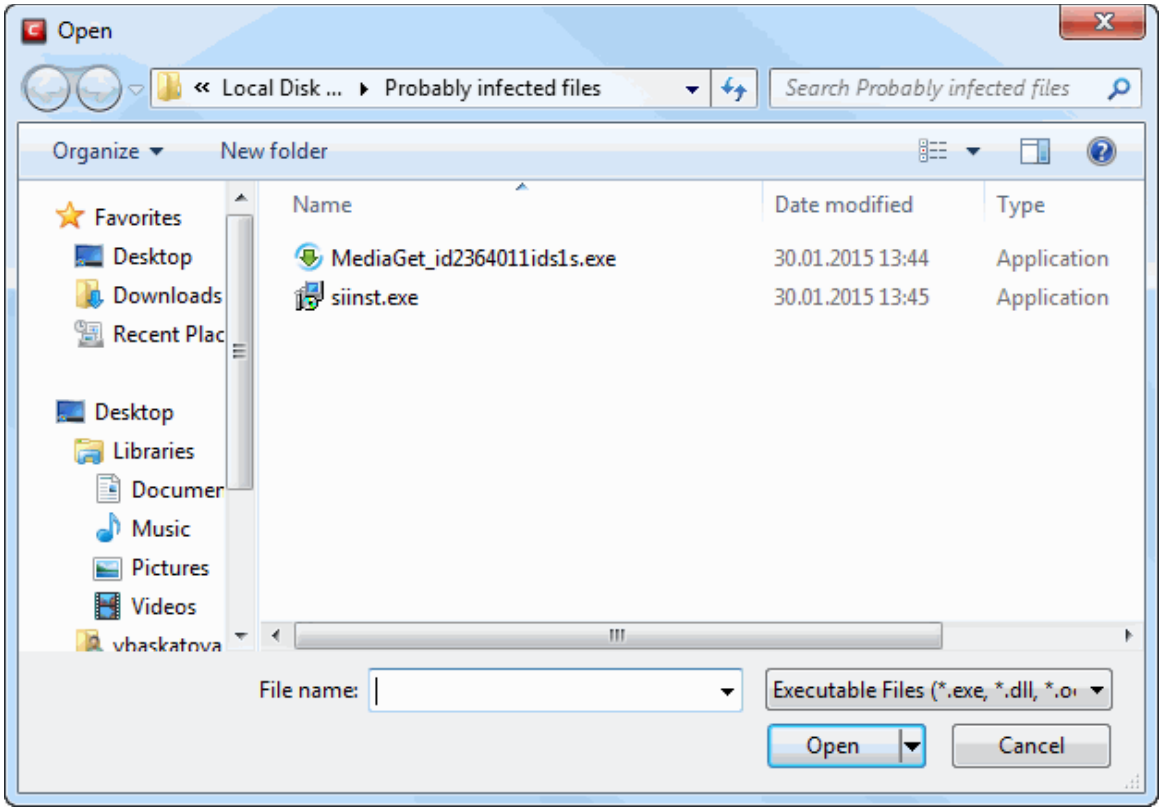
If you want to just add the applications in the drive partition/folder for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Adding a file based on its hash value

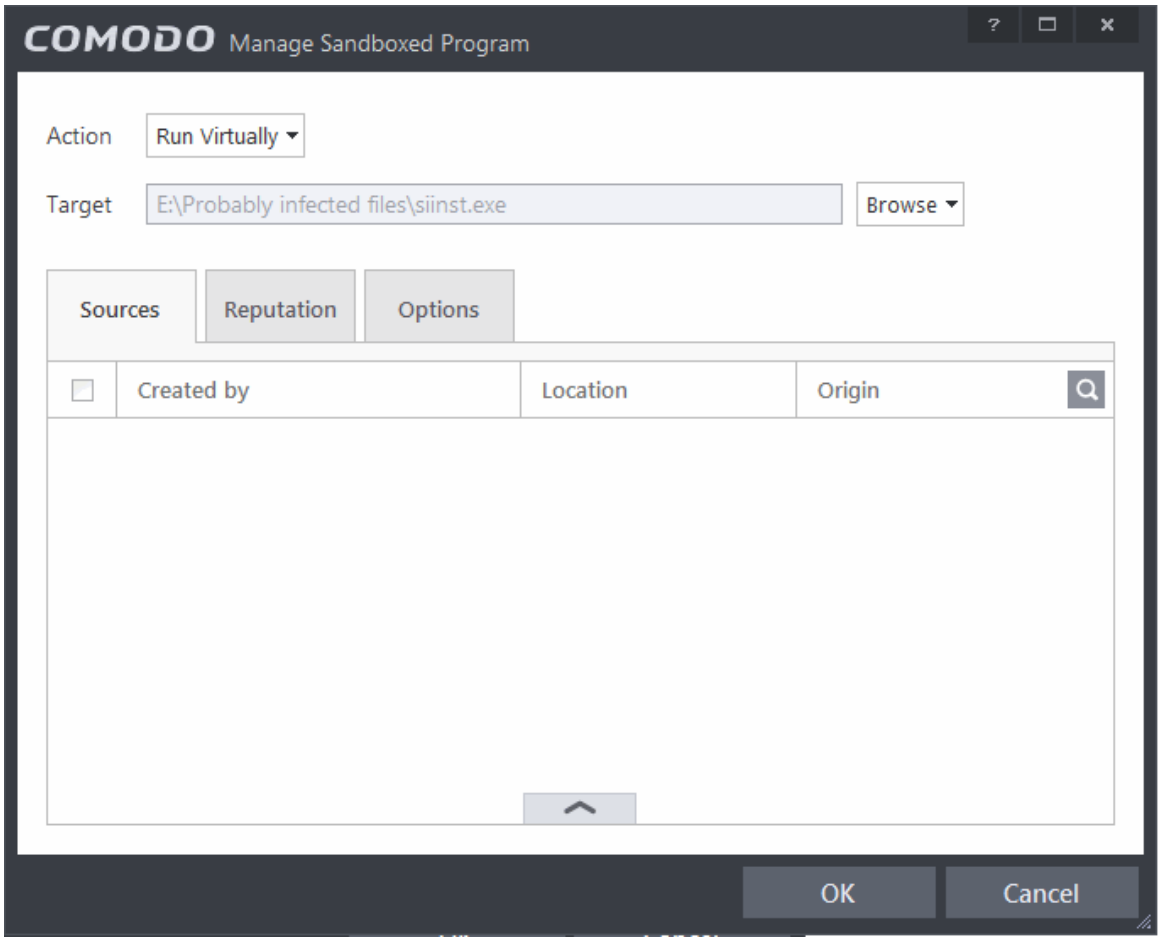
- Choose 'File Hash' from the 'Browse' drop-down.



- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'



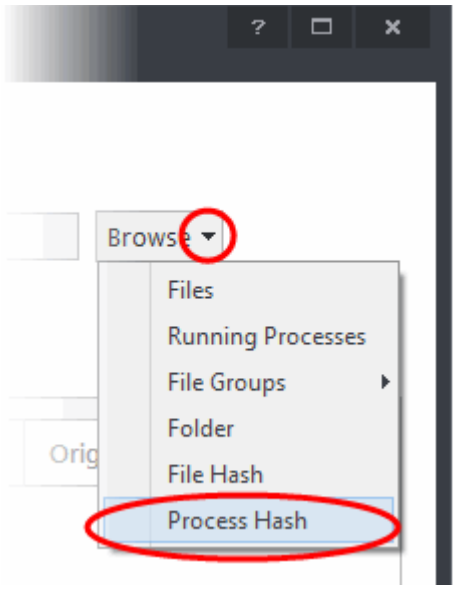
The file will be added as target and will be run as per the action chosen in **Step 1**.



If you want to just add the hash value of an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

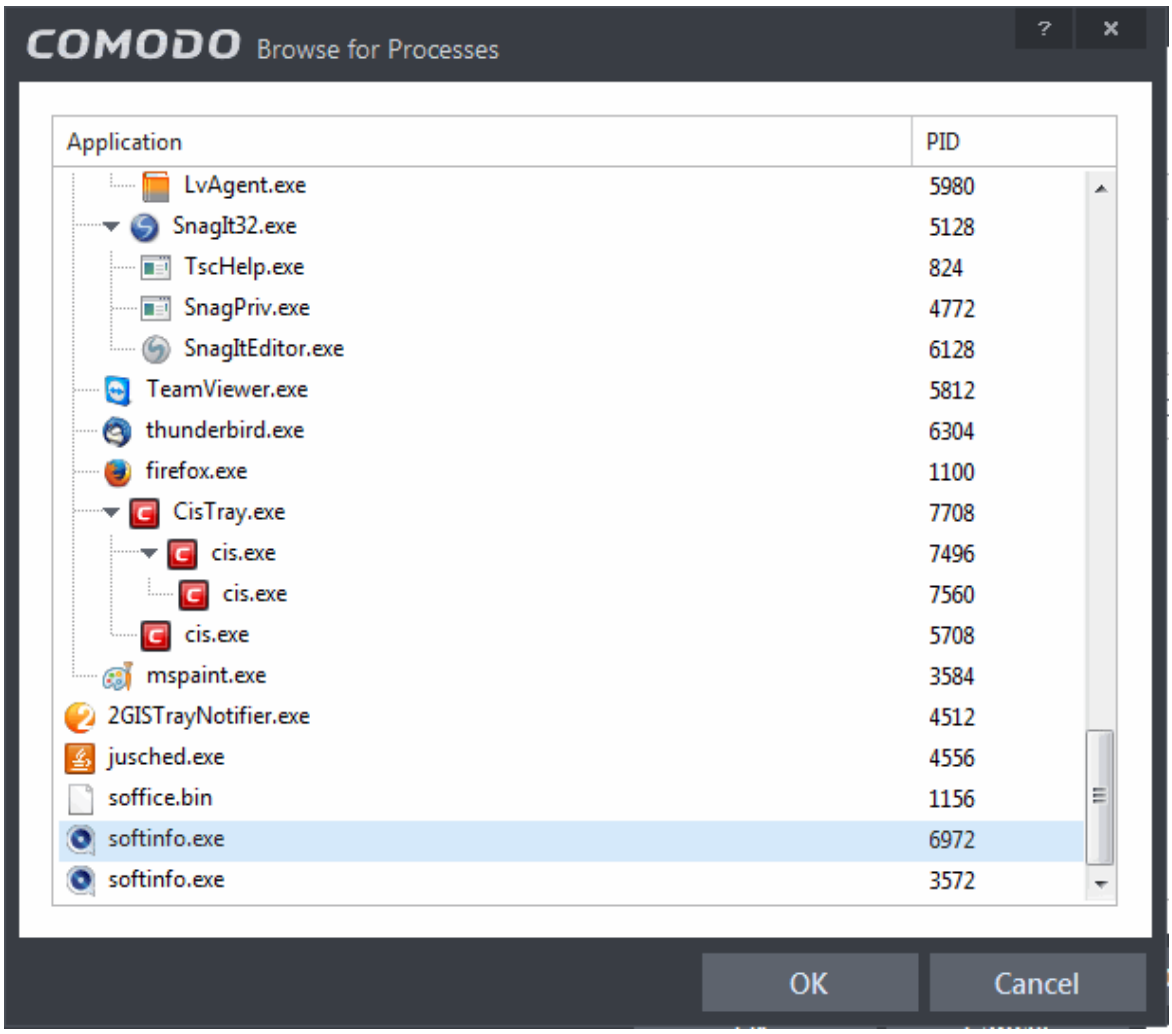
Adding an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.

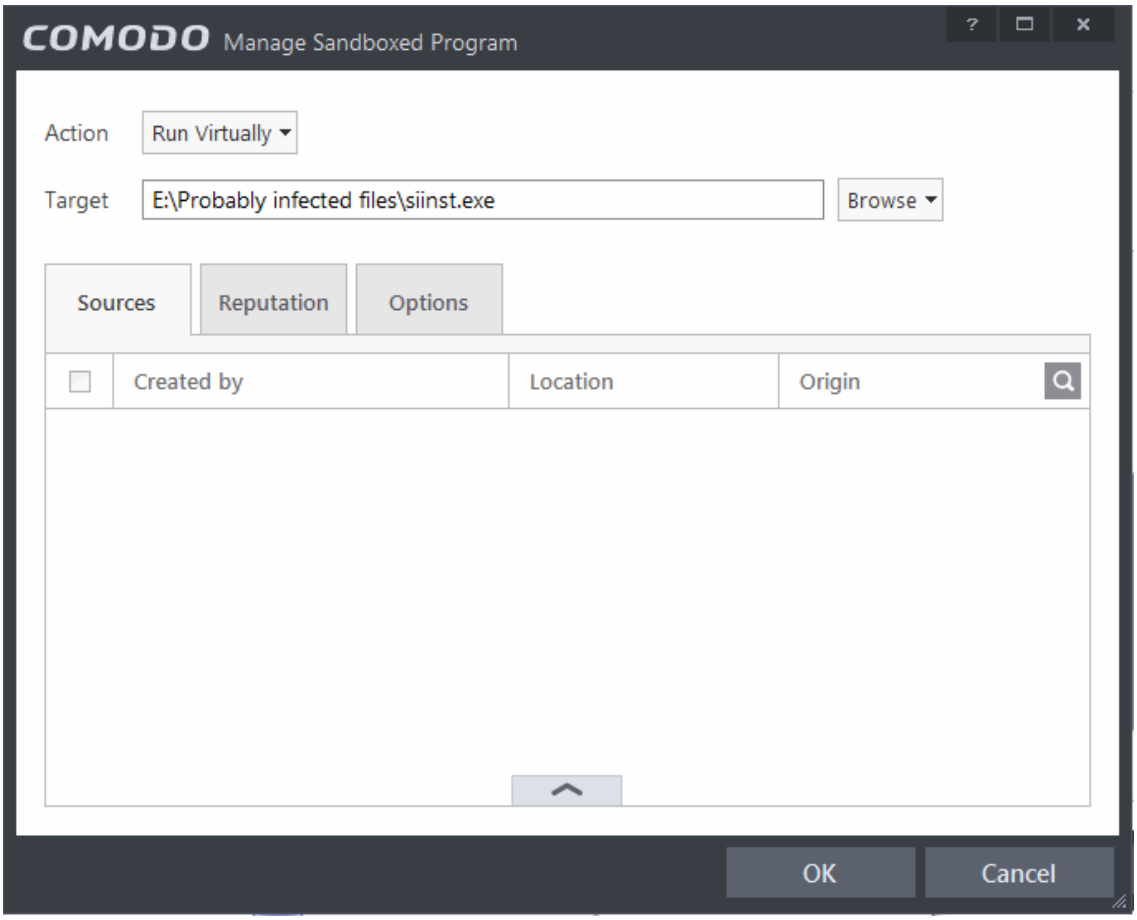


A list of currently running processes in your computer will be displayed.

- Select the process, whose hash value of the target application is to be added to target and click 'OK' from the Browse for Process dialog.



The file will be added as target and will be run as per the action chosen in **Step 1**.



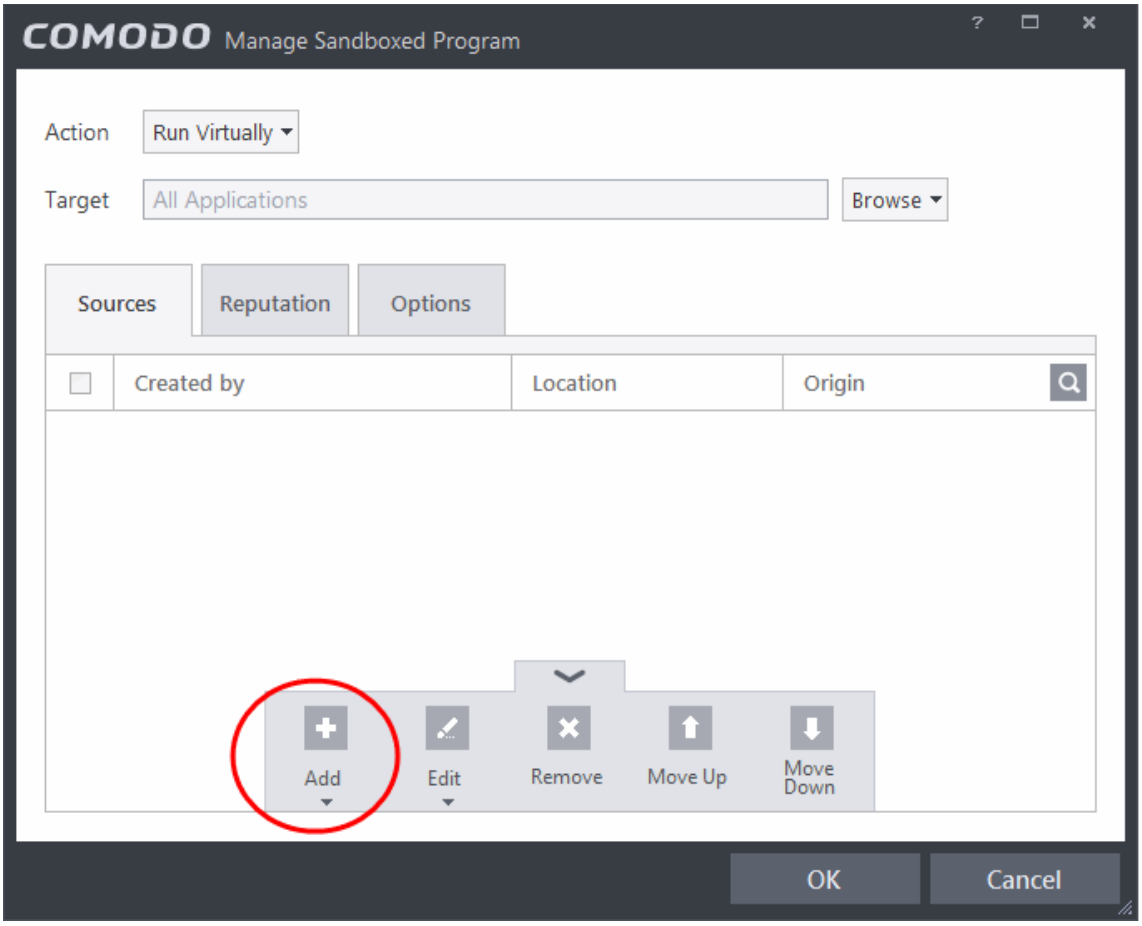
If you want to just add the process hash value of an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Step 3 - Select the Sources

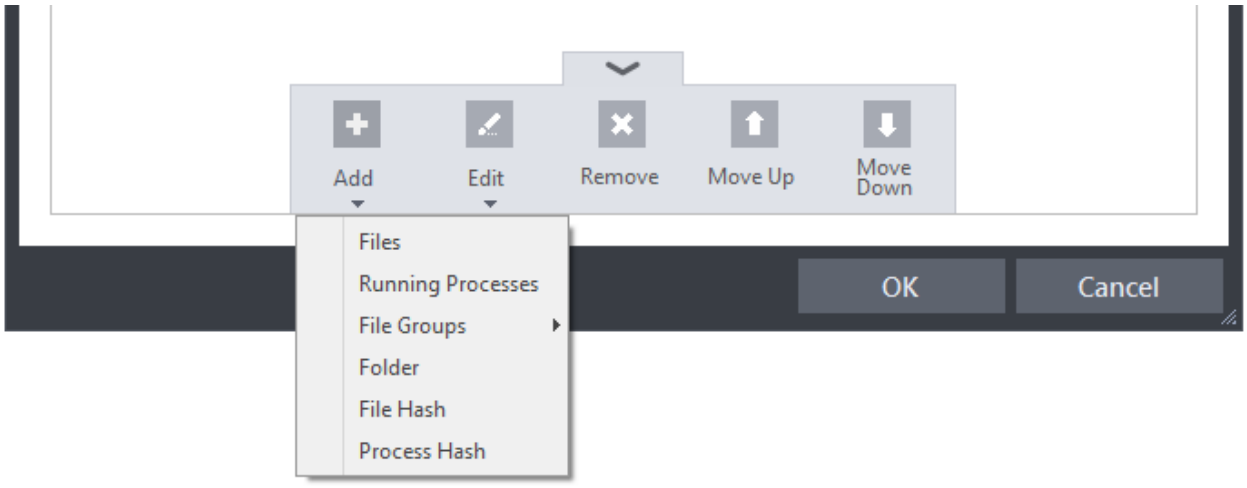
If you want to include a number of items for a rule but want the rule to be applied for certain conditions only, then you can do this in this step. For example, if you include all executables in the Target but want the rule to be applied for executables that were downloaded from the internet only, then the filter can be applied in the Sources. Another example is if you want to run unrecognized files from network share, you have to create an ignore rule with All Applications as target and source located on network drives.

To add a source

- Click the handle at the bottom and then click Add from the options.



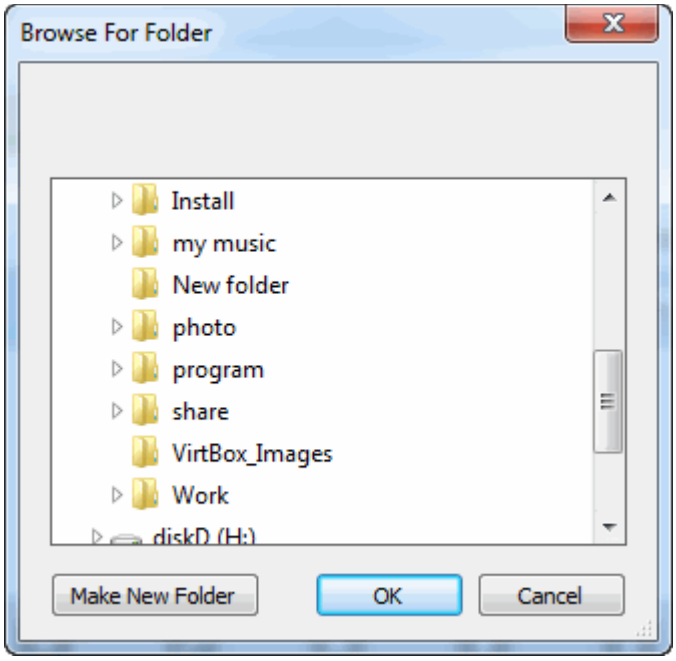
The options available are available are same as available under the Browse button beside Target as explained in **Step 2**. Refer to previous section for each of options for more details.



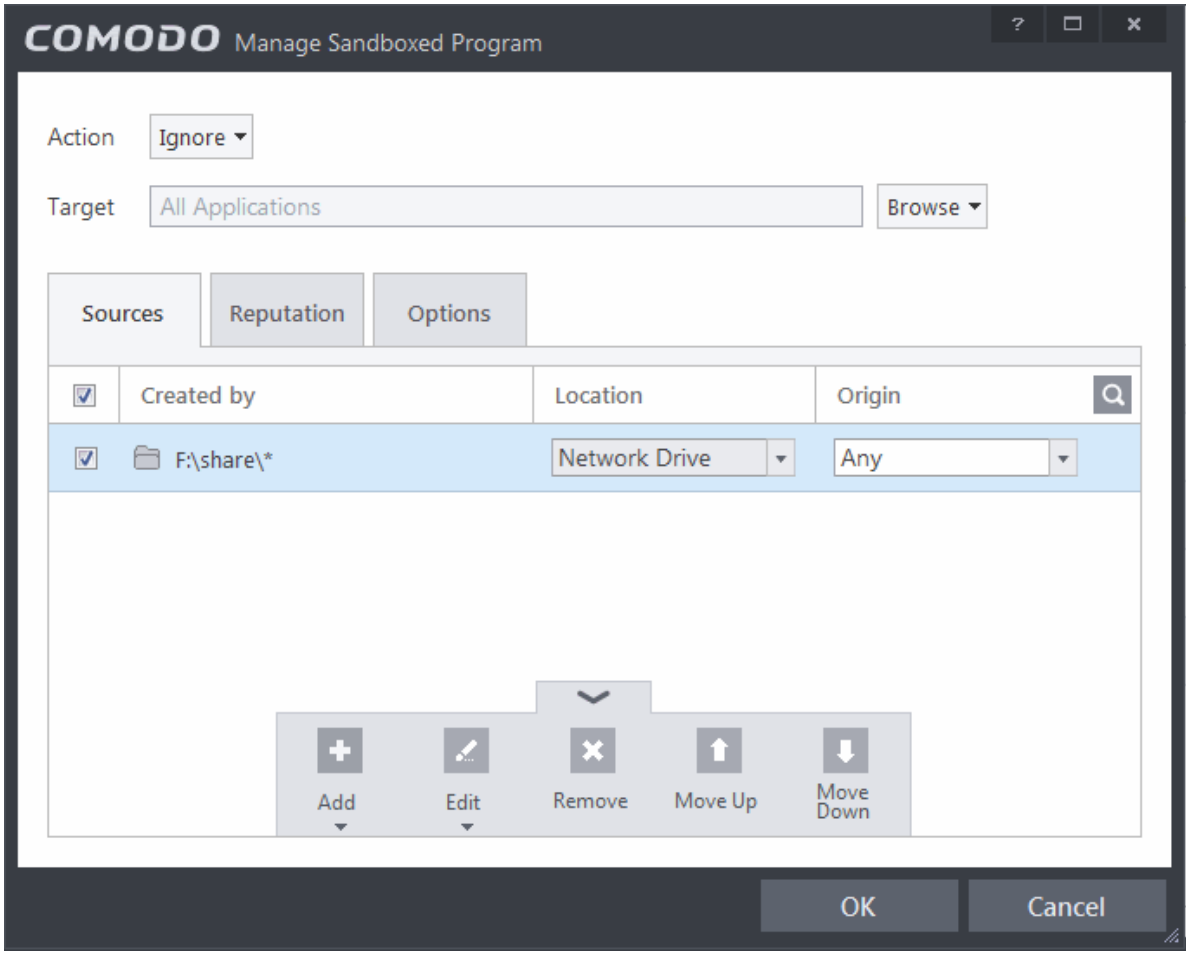
The following example describes how to add a Ignore rule for Unrecognized files from a network source:

- In **Step 1**, select the action as Ignore
- In **Step 2**, select the Target as All Applications in File Groups
- In **Step 3**, click Folder from the Add options.

The Browse For Folder dialog will be displayed.



- Navigate to the source folder in the network, select it and click 'OK'.



The selected network source folder will be added under the 'Created by' column and the screen displays the options to specify the location and from where the files were downloaded.

- **Location** - The options available are:
  - Any

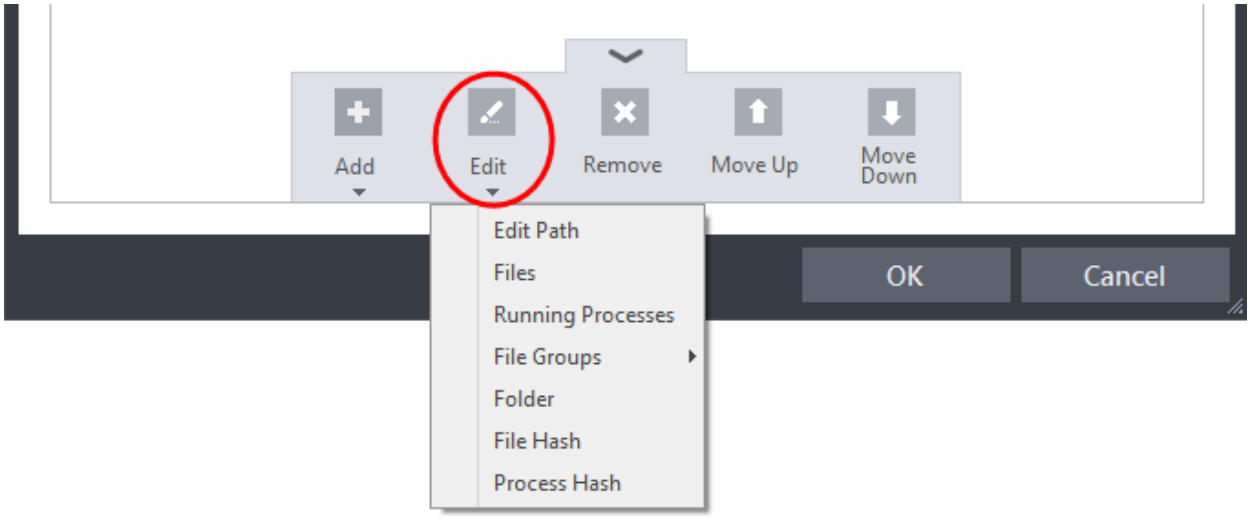
- Local Drive
- Removable Drive
- Network Drive

Since the source is located in a network, select Network Drive from the options.

- **Origin** - The options available are:
  - Any - The rule will apply to files that were downloaded to the source folder from both Internet and Intranet.
  - Internet - The rule will apply to files that were downloaded to the source folder from Internet only.
  - Intranet - The rule will apply to files that were downloaded to the source folder from Intranet only.

Repeat the process to add more source folders.

- Click the Edit button to change the source path from the options:



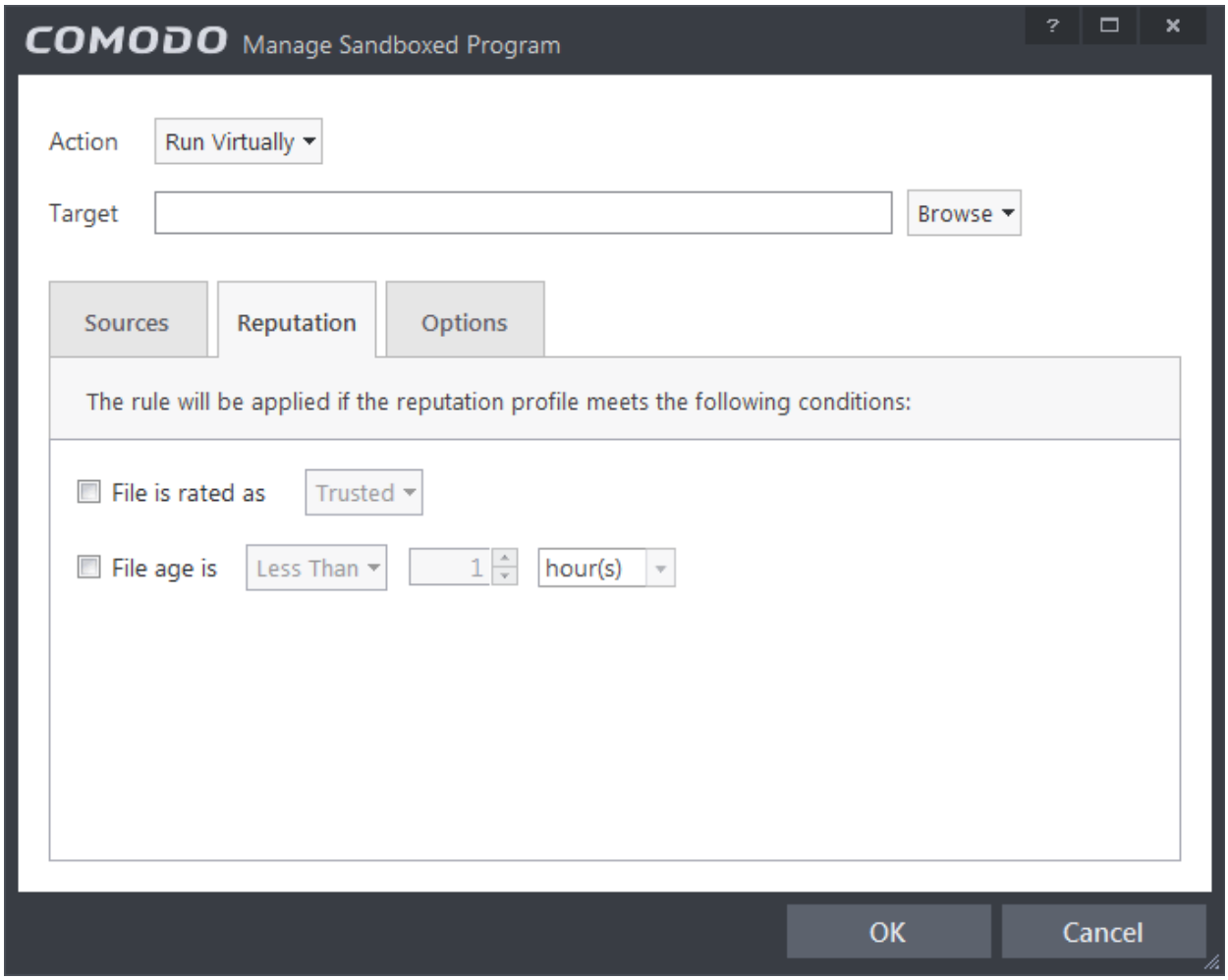
- To remove a source from the list, select it and click the Remove button.
- Use the 'Move Up' and 'Move Down' buttons to specify the order of source path.

If you want to just add the Sources for a particular action as selected in **Step 1** without specifying rating of the file or options, then click 'OK'. The default values for Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Reputation** filters and **Options** for the rule.

Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options in **Step 4**.

Step 4 - Select the File Reputation

- Click the Reputation tab in the Manage Sandboxed Program interface.



By default, the file rating is not selected meaning the rating could be Any. The options available are:

- **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by Defense+. Refer to the sections **File Rating Settings** and **Trusted Files** for more information.
- **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section **File List** for more information.
- **Malware** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. Refer the section **Unknown Files - The Scanning Process** for more information.

By default, file age is not selected, so the age could be Any. The options available are:

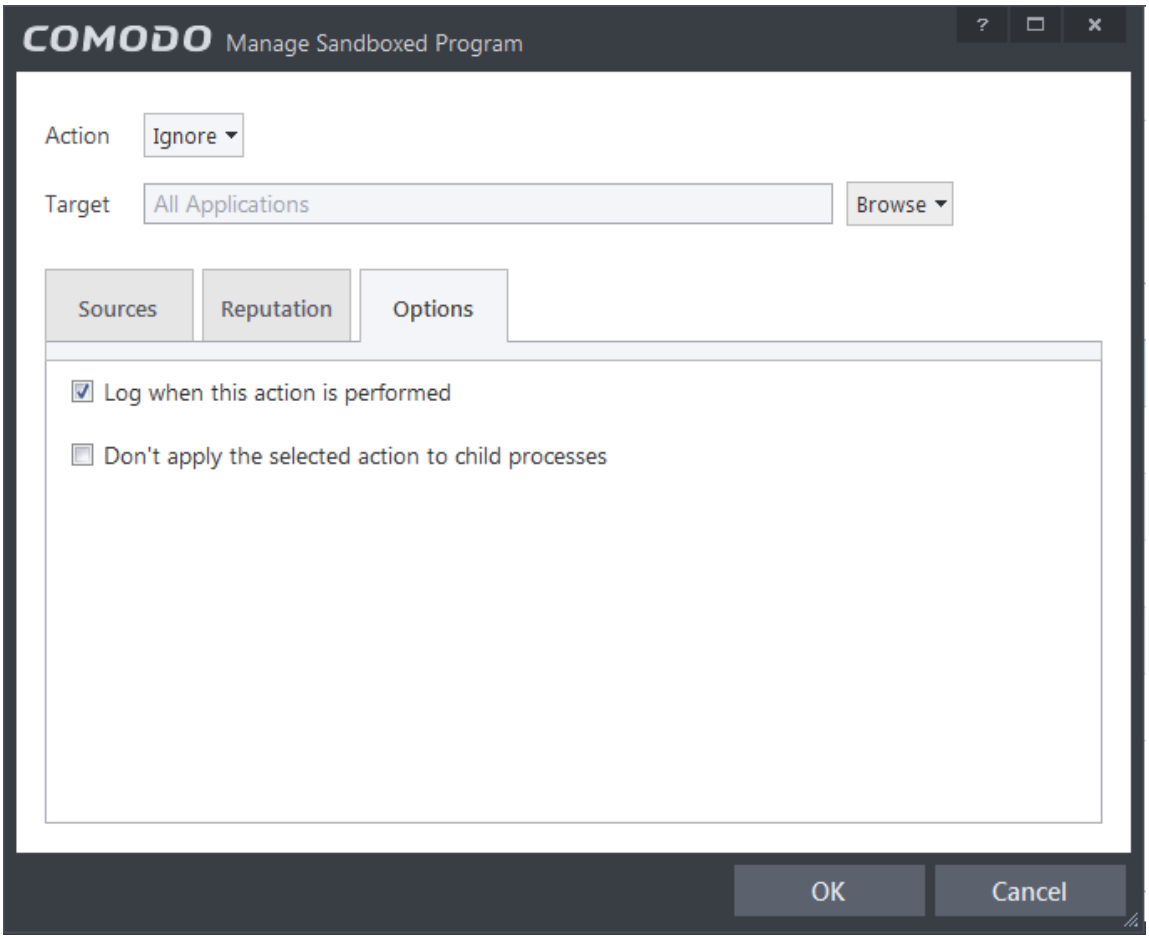
- Less Than – CIS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (***Default and recommended = 1 hours)***
- More Than - CIS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 1 hours)***

Select the category from the options. Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options.

If you want to just add the Sources and Reputation for a particular action as selected in **Step 1** without specifying the options, then click 'OK'. The default values for Options will be 'Log when this action is performed'. If required you can configure **Options** for the rule.

Step 5 - Select the Options

- Click the Options tab in the Manage Sandboxed Program interface.



By default, the 'Log when this action is performed' The options available for Ignore action are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Skip child processes** - Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CIS treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
    - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
    - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox rules individually applied as per their file rating.

The 'Skip child processes' option is available for the Ignore action only. For actions - Run Restricted and Run Virtually - the following options are available:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Set Restriction Level** - When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
    - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(***Default***)
    - **Limited -** Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
    - **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
    - **Untrusted -** The application is not allowed to access any operating system resources. The application is not

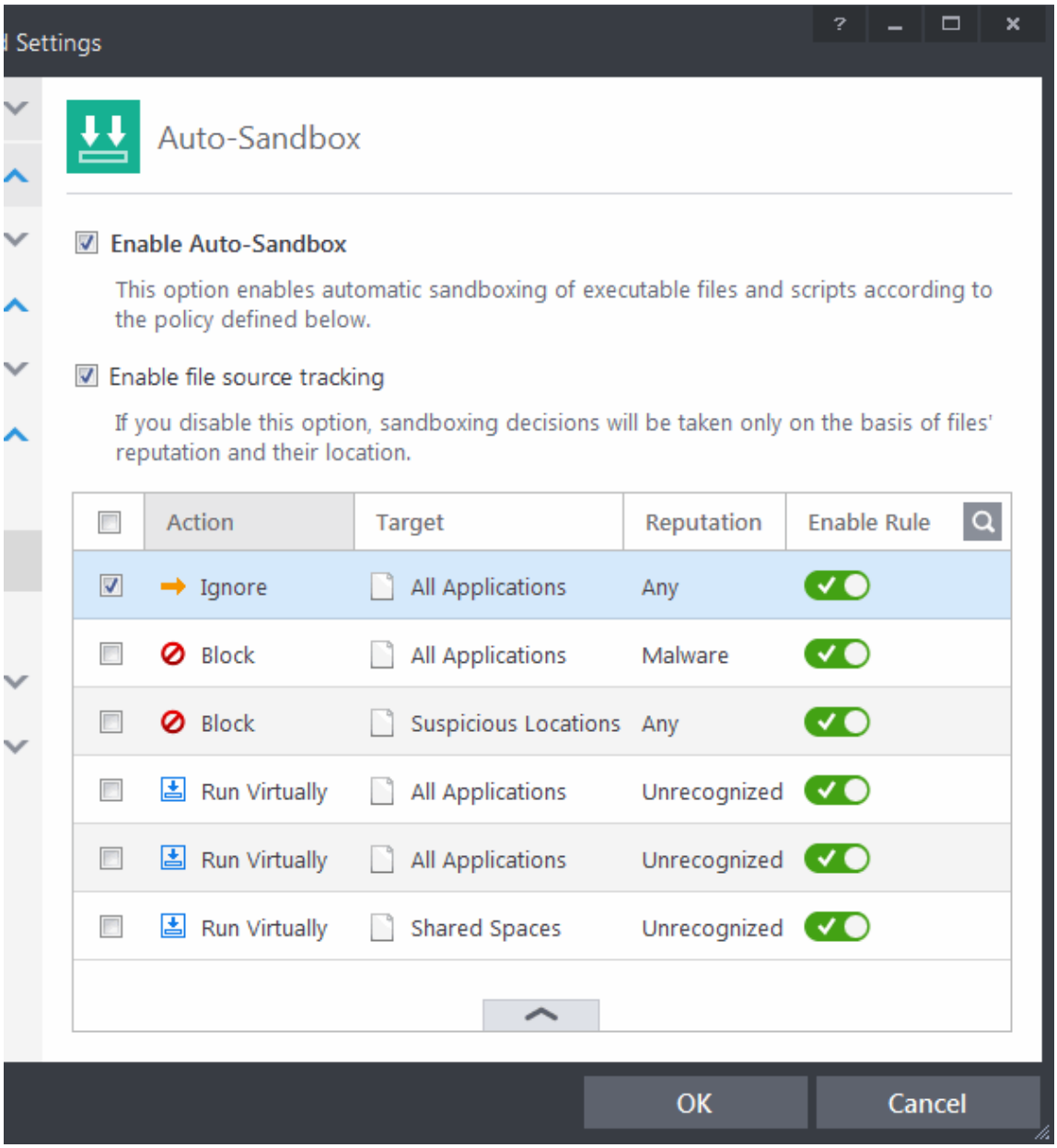
allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.

- **Limit maximum memory consumption to** - Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** - Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For Block action, the following options are available:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Quarantine program** - If checked, the programs will be automatically quarantined. Refer to the section **Manage Quarantined Items** for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



Editing an Auto-Sandbox Rule

- To edit an auto-sandbox rule, select it from the list and click 'Edit' from the options.

The Manage Sandboxed Program interface will be displayed. The procedure is similar to adding Adding an **Auto-Sandbox Rule**.

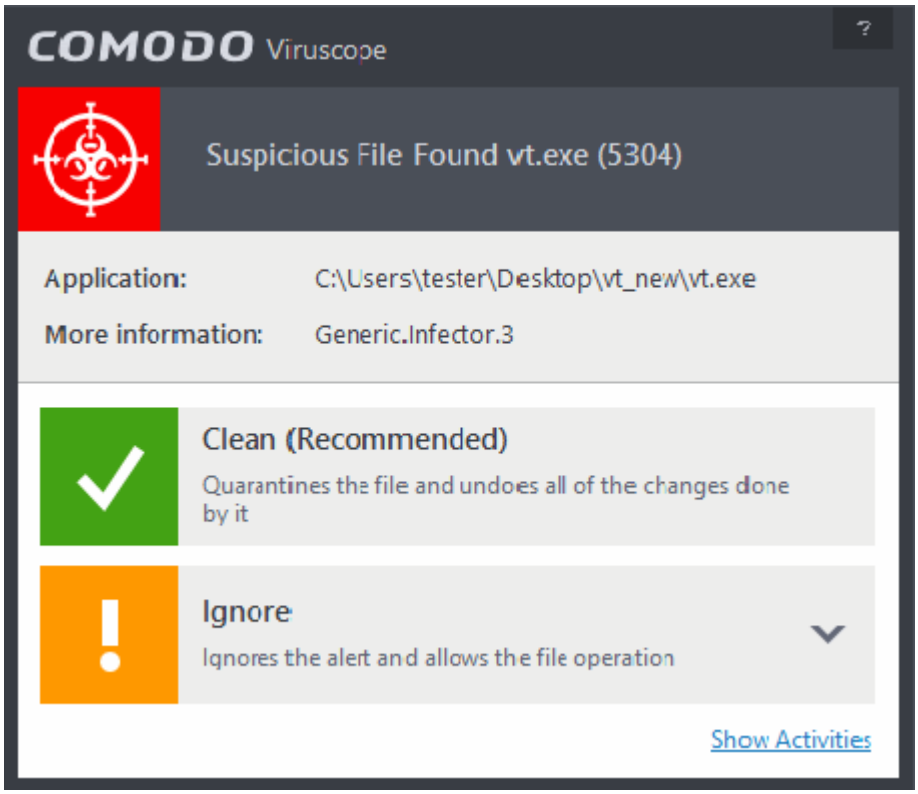
- Click 'OK' to save the changes to the rule.

Important Note: Please make sure the auto-sandbox rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail.

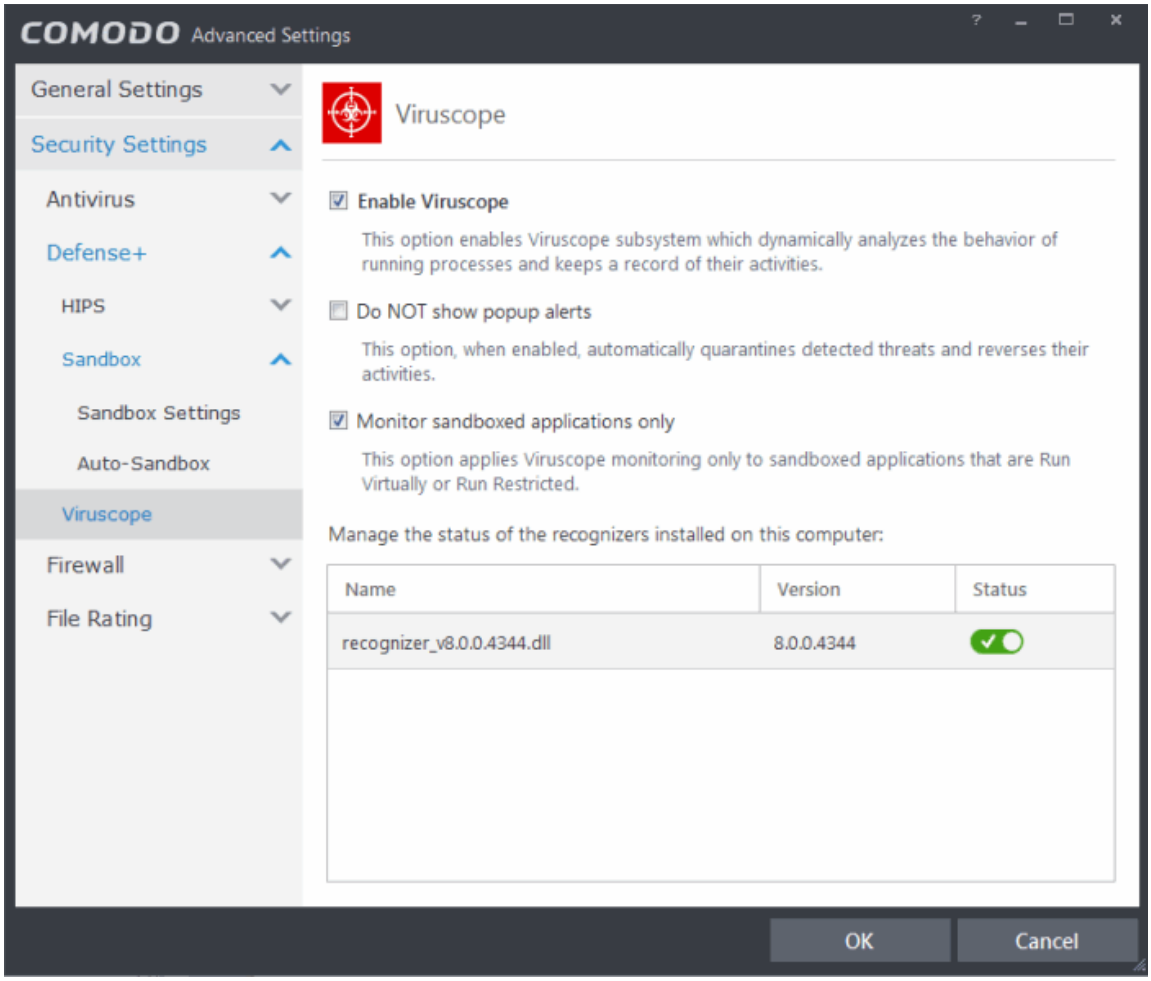
6.2.2.9. Viruscope

Viruscope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the Defense+ by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented in order to run correctly.

Viruscope alerts give you the opportunity to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer.



The 'Viruscope' configuration panel can be accessed by clicking 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Defense + > Viruscope'.



Viruscope Settings

Viruscope is capable of monitoring all running processes and, if suspicious activity is detected, can generate alerts that let you quarantine the application and undo its activities.

- **Enable Viruscope (Recommended)** - Allows you to enable or disable Viruscope. If enabled, Viruscope monitors the activities of running processes and generates alerts if suspicious activity is detected. (***Default = Enabled***)
- **Do NOT show pop-up alerts** - Allows you to configure whether or not CIS should show an alert if Viruscope detects a suspicious activity. Choosing 'Do not show pop-up alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed. (***Default = Disabled***)
- **Monitor sandboxed applications only** - If enabled, Viruscope will only monitor and generate alerts for processes running in the sandbox. (***Default = Enabled***)

Manage the status of recognizers

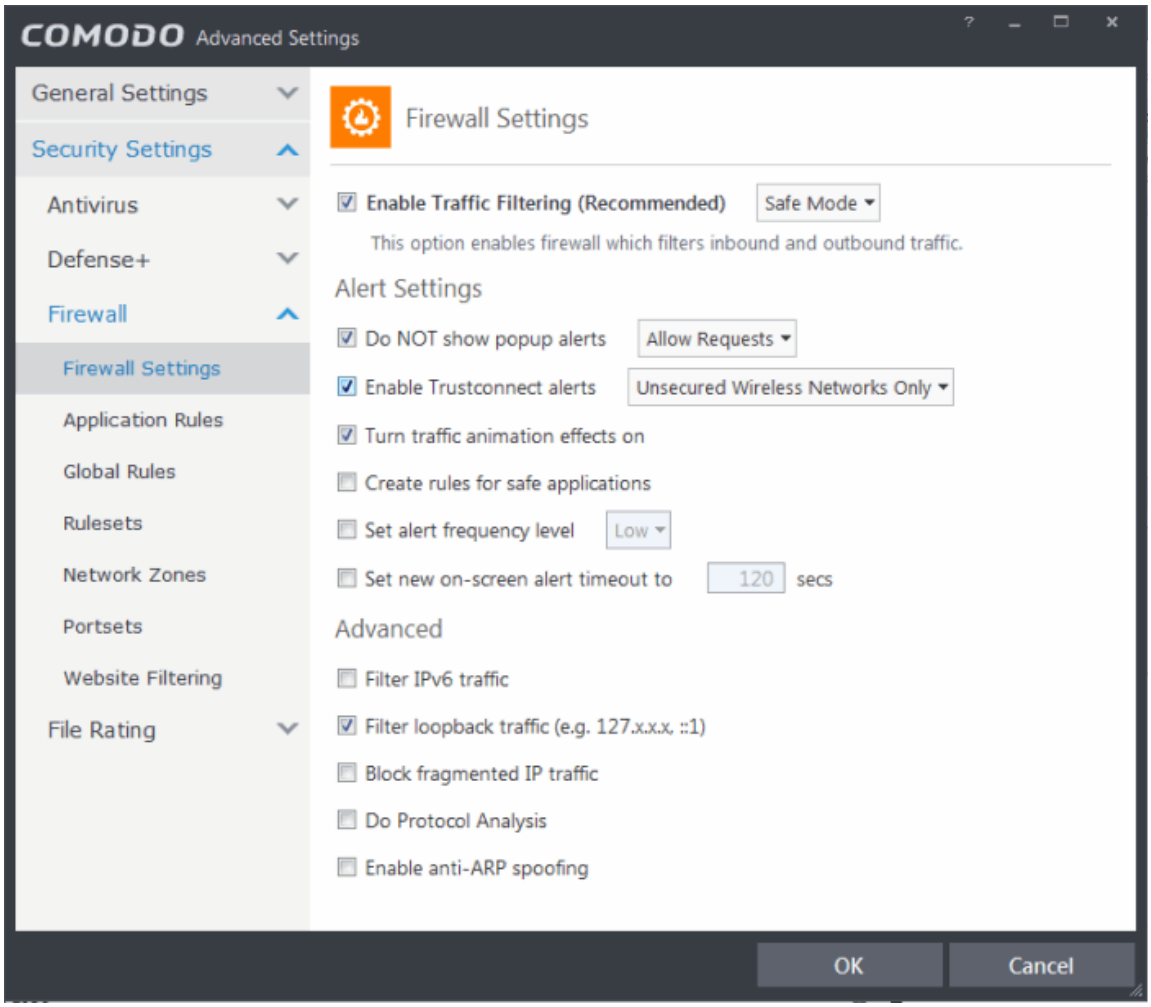
Viruscope detects zero-day malware by analyzing the behavior and actions of an application. If the detected behavior corresponds to that of known malware, then Viruscope will generate an alert which allows you to quarantine the application and reverse any changes that it made.

A 'recognizer' file contains the sets of behaviors that Viruscope needs to look out for. If you disable a particular recognizer, then Viruscope will no longer raise an alert if an application exhibits the behaviors referenced in the file. We recommend most users to leave the 'Status' of recognizers at their default settings. Advanced users, however, may want to try disabling recognizers if they are experiencing a large number of Viruscope false positives.

6.2.3. Firewall Settings

The Firewall component of Comodo Internet Security offers the highest levels of security against inbound and outbound threats. It checks that all network traffic in and out of your computer is legitimate, it stealths your computer's ports against hackers and it blocks malicious software from transmitting your confidential data over the Internet. Comodo Firewall also makes it easy for you

to specify exactly which applications are allowed to connect to the Internet and immediately warns you when there is suspicious activity. Also you can configure rules to allow or block access to specific websites for particular users of your computer.



The 'Firewall Settings' area has several sub-sections that allow you to configure overall behavior; configure network zones and portsets and (for advanced users) to configure and deploy traffic filtering rules on an application specific and global basis.

Click the following links to jump to the section you need help with:

- **Firewall Settings** - Configure settings that govern the overall behavior of the firewall component.
- **Application Rules** - View, create and modify rules that determine the network access privileges of individual applications or specific types of application
- **Global Rules** - View, create and modify rules that apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Predefined collections of firewall rules that can be applied, out-of-the-box, to Internet capable applications such as browsers, email clients and FTP clients.
- **Network Zones** - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Predefined groups of regularly used ports that can used and reused when creating traffic filtering rules.
- **Website Filtering** - Create website filtering rules which let you determine which sites certain users can or cannot access.

Background note on rules: Both application rules and global rules are consulted when the firewall is determining whether or not to allow or block a connection attempt.

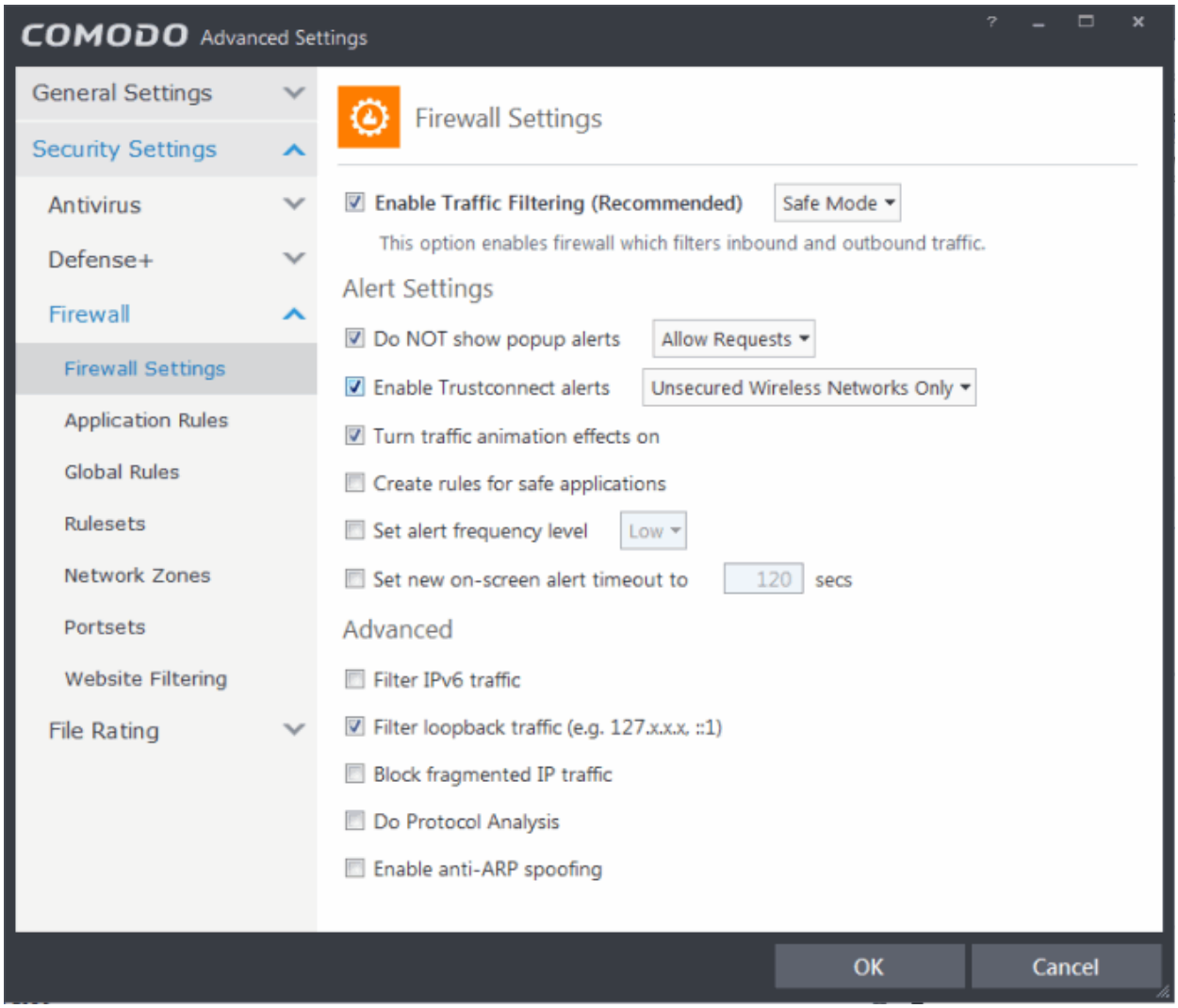
- For Outgoing connection attempts, the application rules are consulted first then the global rules.

- For Incoming connection attempts, the global rules are consulted first then application specific rules.

6.2.3.1. Firewall Settings

Firewall Settings panel allows you to quickly configure overall Firewall settings and is divided into three main areas:

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

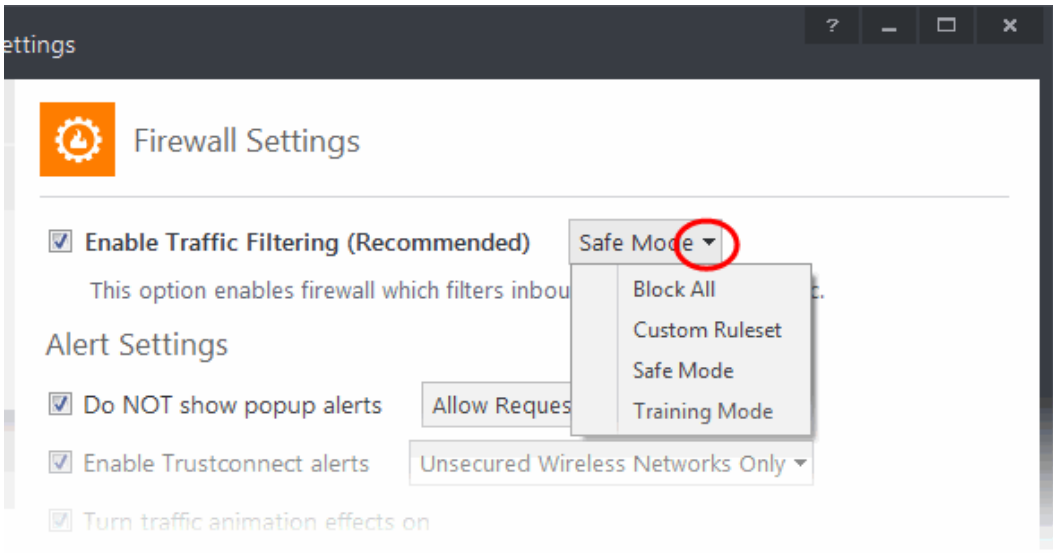


General Settings

- **Enable Firewall** - Allows you to enable or disable Firewall protection.(***Default and recommended =Enabled***)

Note: The Firewall configuration settings can also be modified in the 'Advanced View' of the Home screen by clicking the status link beside Firewall in the Firewall pane.

If enabled, you can also choose the security level from the accompanying drop-down menu:



The choices available are:

- **Block All:** The firewall blocks all traffic in and out of your computer regardless of any user-defined configuration and rules. The firewall does not attempt to learn the behavior of any application and does not automatically create traffic rules for any applications. Choosing this option effectively prevents your computer from accessing any networks, including the Internet.
- **Custom Ruleset Mode:** The firewall applies ONLY the custom security configurations and **network traffic rules** specified by the user. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. You will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, you have specified rules and policies that instruct the firewall to trust the application's connection attempt).

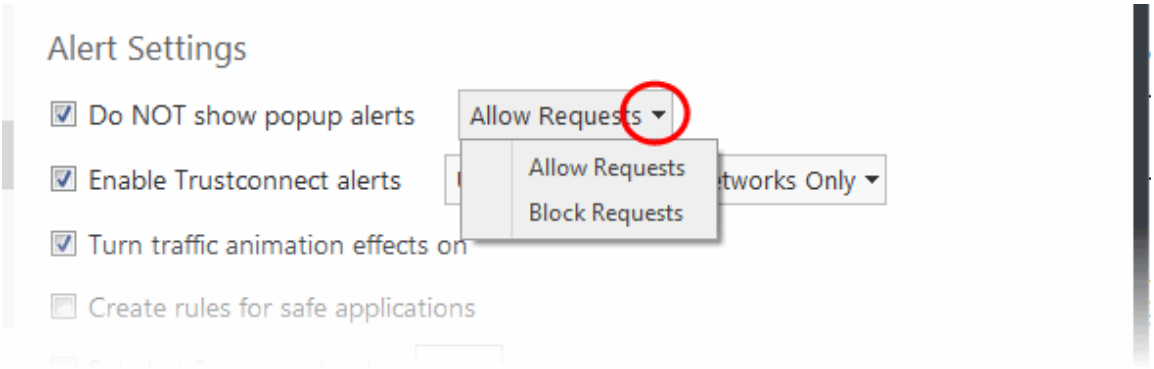
  If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.
- **Safe Mode *(Default)***: While filtering network traffic, the firewall automatically creates rules that allow all traffic for the components of applications certified as 'Safe' by Comodo, if the checkbox **Create rules for safe applications** is selected. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This deploys the **predefined firewall ruleset** 'Trusted Application' onto the application.

  'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.
- **Training Mode** : The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the **correct network access rights**.

Alert Settings

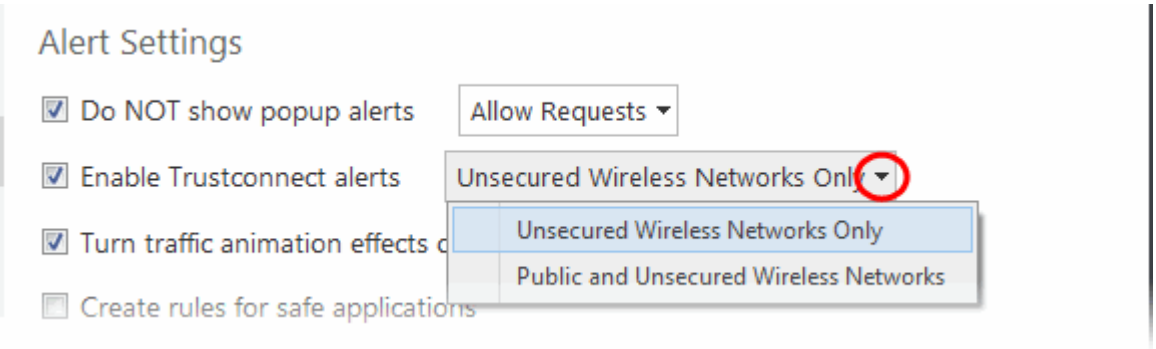
- **Do NOT show popup alerts** - Configure whether or not you want to be notified when the firewall encounters a request for network access. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness. (***Default = Enabled***)

  If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Requests' or 'Allow Requests'.



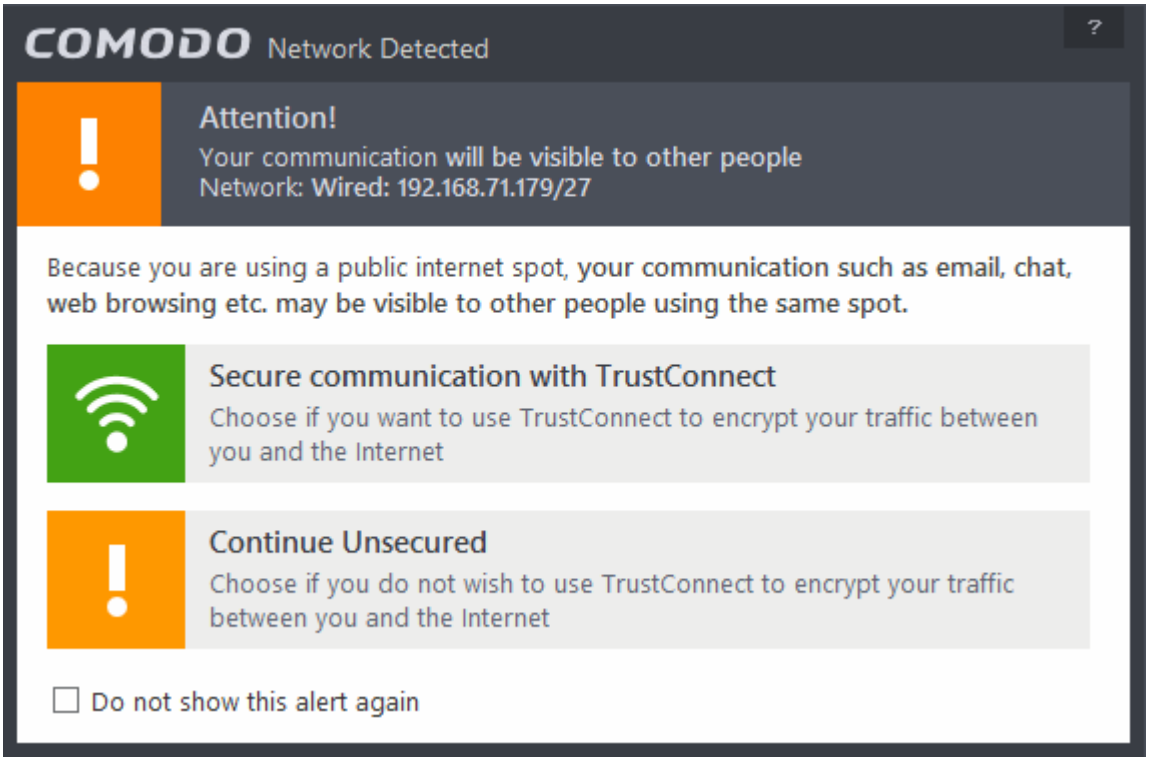
- **Enable Trustconnect Alerts** - If you are connecting to Internet at a public place like an airport or a coffee shop then you are potentially exposing yourself to danger. Unsecured public networks can allow other people to easily eavesdrop on your communications or even gain access to your computer to steal your confidential information. In order to safeguard against such attempts, Comodo recommends you encrypt your connection in public hotspots using TrustConnect - a secure Internet proxy service.

  If selected, Comodo Firewall will display an alert if it detects you are connected to the Internet through an unsecured network (***Default=Enabled***).The drop-down options allow you to select the conditions under which you want alerts to be displayed:



  - **Unsecured Wireless Networks Only (Default) -** TrustConnect alerts are displayed only if you are connecting to an unencrypted wireless network.
  - **Public and Unsecured Wireless Networks only** - TrustConnect alerts are displayed whenever you connect to a public wireless network irrespective of whether the connection is encrypted

You will be alerted and offered the opportunity to secure the connection via the following notification:



- **Turn traffic animation effects on** - By default, the Comodo Internet Security's tray icon displays a small animation whenever traffic moves to or from your computer.

If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the icon. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer. Clear this check box If you would rather not see this animation ***(Default = Enabled)***.

- **Create rules for safe applications** - Comodo Firewall trusts the applications if:
  - The application/file is included in the Trusted Files list under File Rating Settings;
  - The application is from a vendor included in the **Trusted Software Vendors** list under File Rating Settings;
  - The application is included in the extensive and constantly updated Comodo safelist.

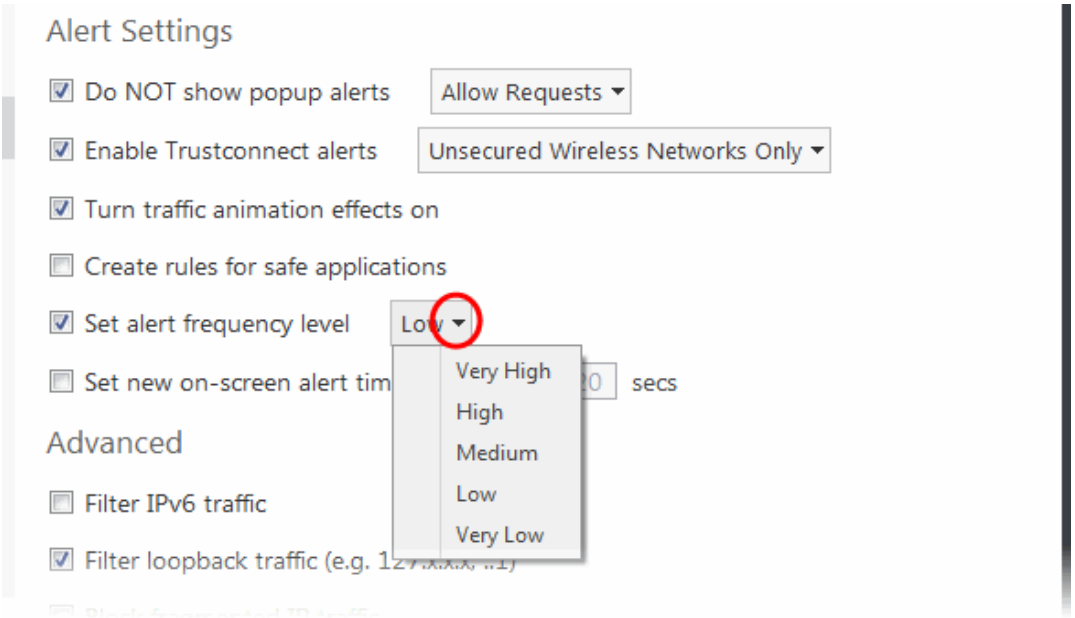
  By default, CIS does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

  Enabling this checkbox instructs CIS to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the **Application Rules** interface. The Advanced users can edit/modify the rules as they wish ***(Default = Disabled).***

Background Note: Prior to version 4.x , CIS would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CIS version 3.x).

- **Set alert Frequency level** - Enabling this option allows you to configure the amount of alerts that Comodo Firewall generates, from the drop-down. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the

default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages. (***Default=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 have not (yet) decided to trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.

- **Set new on-screen alert time out to**: Determines how long the Firewall shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced Settings

Comodo Firewall features advanced detection settings to help protect your computer against common types of denial of service (DoS) attack. When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server.

- **Filter IP v6 traffic** - If enabled, CIS will filter IPv6 network traffic in addition to IPv4 traffic.(***Default = Disabled***).

Background Note: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available. This hard limit has already led to the development of 'work-around' solutions such as Network Address Translation (NAT), which enable multiple hosts on private networks to access the Internet using a single IP address.

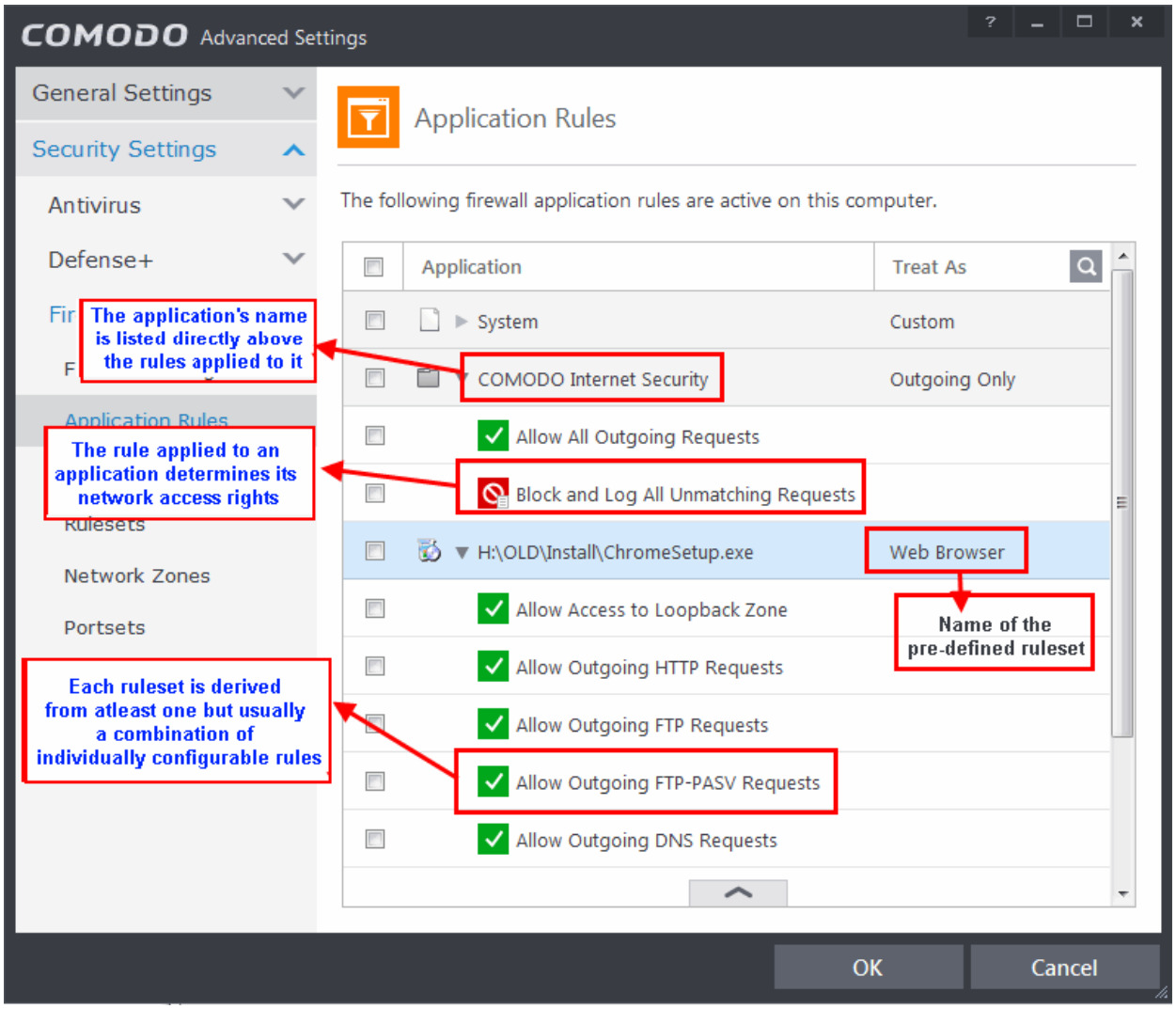
IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

- **Filter loopback traffic**: Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately received by it. This involves no connection outside your computer to the Internet or a local network. The IP address of the loopback network is 127.0.0.1, which you might have heard referred to, under its domain name of 'http://localhost', i.e. the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this option enabled means the firewall will filter traffic sent through this channel. (***Default = Enabled***).
- **Block fragmented 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 (***Default = Disabled***).
- **Do protocol Analysis** - Protocol Analysis is key to the detection of fake packets used in denial of service attacks. Checking this option means Comodo Firewall checks every packet conforms to that protocols standards. If not, then the packets are blocked (***Default = Disabled***).
- **Enable anti-ARP spoofing** - A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update your machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in a machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update your ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in your home network. Enabling this setting helps to block such requests - protecting the ARP cache from potentially malicious updates ***(Default = Disabled).***

6.2.3.2. Application Rules

Overview of Rules and Rulesets

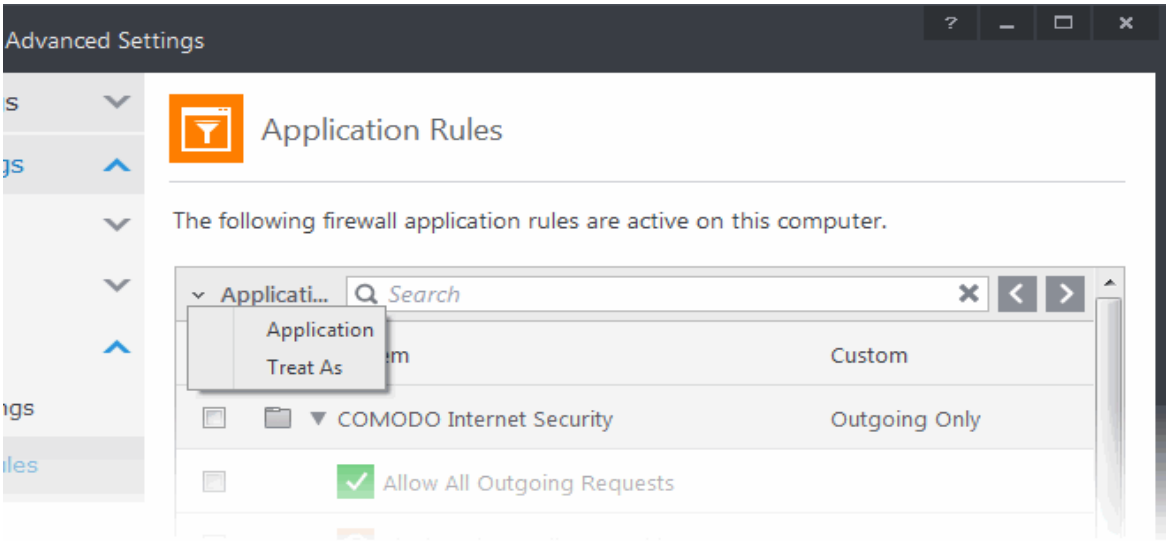
Whenever an application makes a request for Internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Ruleset that has been specified for that application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual network access rule contains instructions that determine whether the application should be allowed or blocked; which protocols it is allowed to use; which ports it is allowed to use and so forth.



The first column, **Application**, displays a list of the applications on your system for which a Firewall ruleset has been deployed. If the application belongs to a file group, then all member applications assume the ruleset of the file group. The second column, **Treat as**, column displays the name of the Firewall ruleset assigned to the application or group of applications in column one.

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

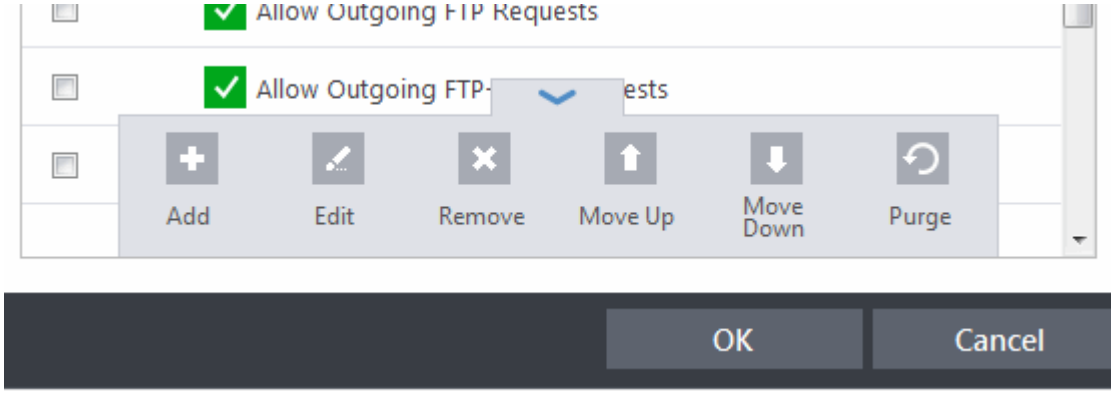
To use the search option, click the search icon at the far right in the column header.



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

General Navigation:

Clicking the handle at the bottom center of the interface opens a rule control panel:



- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the sections **'Creating or Modifying Firewall Rules'** and **'Adding and Editing a Firewall Control Rule'.**
- **Edit** - Allows the user to modify the Firewall rule or ruleset of the selected application. See the sections '**Creating or Modifying Firewall Rules**' and '**Adding and Editing a Firewall Rule**'.
- **Remove** - Deletes the selected ruleset.
- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down** - The traffic is filtered by referring to the rules in order from the top. The Move Up and Move Down buttons enable you to change the priority of a selected rule.

If you wish to modify the **firewall ruleset** for an application:

- Double click on the application name to begin **'Creating or Modifying Firewall Rules'**
- Select the application name click the handle at the bottom right and choose 'Edit' from the options to begin '**Creating or Modifying Firewall Rules**'

If you wish to modify an **individual rule** within the ruleset:

- Double click on the specific rule to begin '**Adding and Editing a Firewall Rule**'
- Select the specific rule and click the handle at the bottom center and choose 'Edit' from the options to begin '**Adding and Editing a Firewall Rule**'

Users can also re-prioritize rulesets by clicking the handle at the bottom center and select 'Move Up' or 'Move Down' from the options.

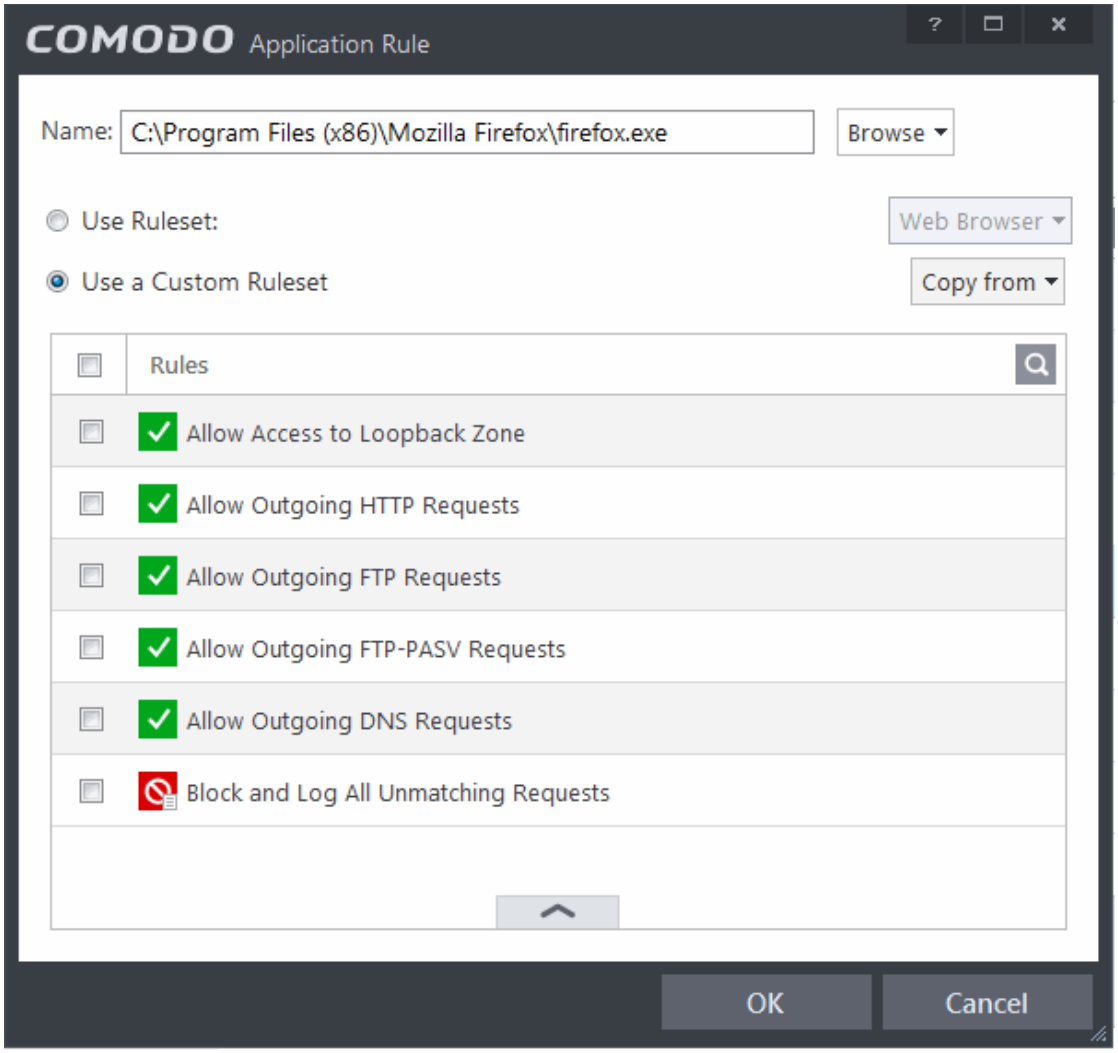
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see **Predefined Rule Sets.**

- See **Application Rule interface** for an introduction to the rule setting interface
- See **Creating and Modifying Firewall Rulesets** to learn how to create and edit Firewall rulesets
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration

Application Rule interface

Firewall rules can be added/modified/removed and re-ordered through the Application Rule interface. Any rules created using **Adding and Editing a Firewall Rule** is displayed in this list.

The Application Rule interface is displayed when you click 'Add' or 'Edit' from the options in 'Application Rules' interface.

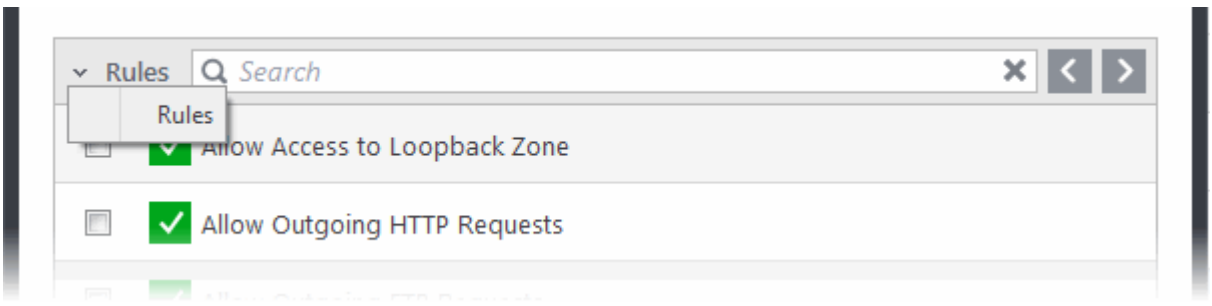


Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see **Understanding Firewall Rules** for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied.

Users can also re-prioritize rulesets by clicking the handle at the bottom center and select 'Move Up' or 'Move Down' from the options. To begin creating Firewall rulesets, first read **'Overview of Rules and Rulesets'** then **'Creating and Modifying Firewall Rulesets**

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

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



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.

- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

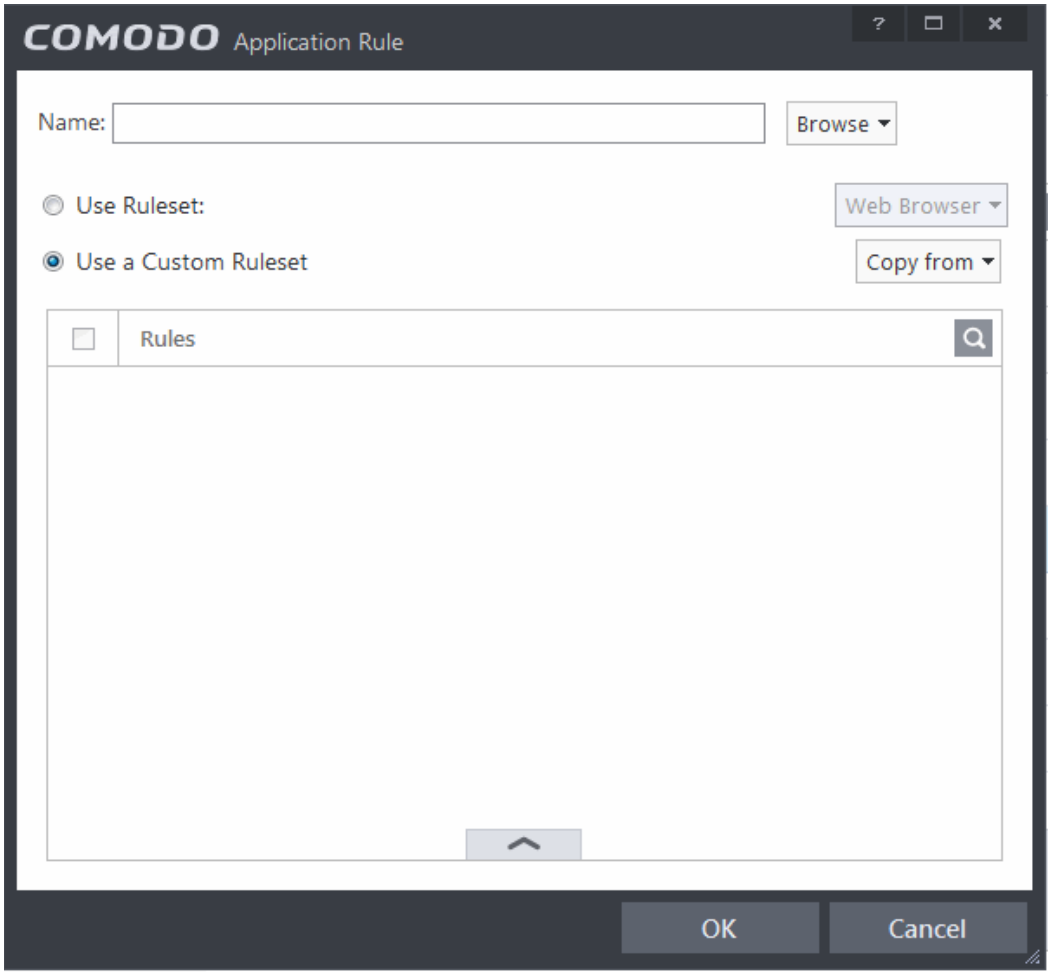
Creating and Modifying Firewall Rulesets

To begin defining an application's Firewall ruleset, you need take two basic steps.

- Step 1 - **Select the application that you wish the ruleset is to be applied.**
- Step2 - **Configure the rules for this application's ruleset.**

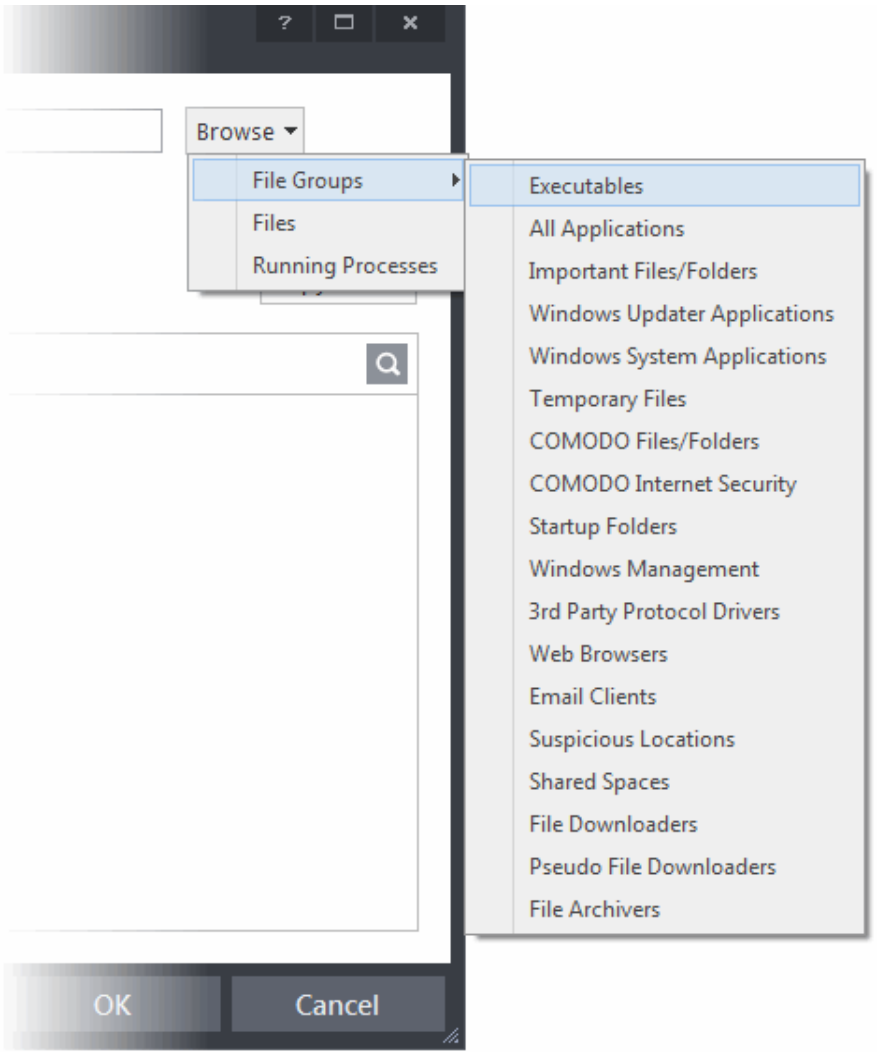
Step 1 - Select the application that you wish the ruleset is to be applied

If you wish to define a ruleset for a new application (i.e. one that is not already listed) then click the handle from the **Application Rules interface** and select 'Add' from the options. This brings up the '**Application Rule**' interface shown below:



Because this is a new application, the 'Application Path' field is blank. (If you are modifying an existing ruleset, then this interface shows the individual rules for that application's ruleset).

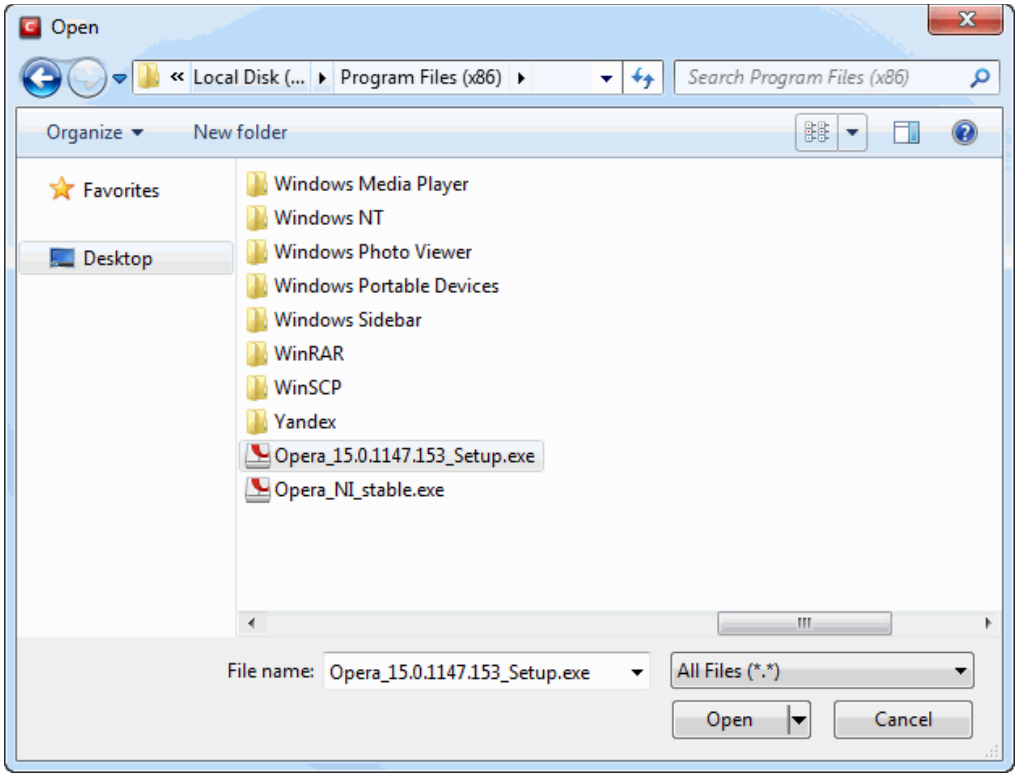
- Click 'Browse' button.



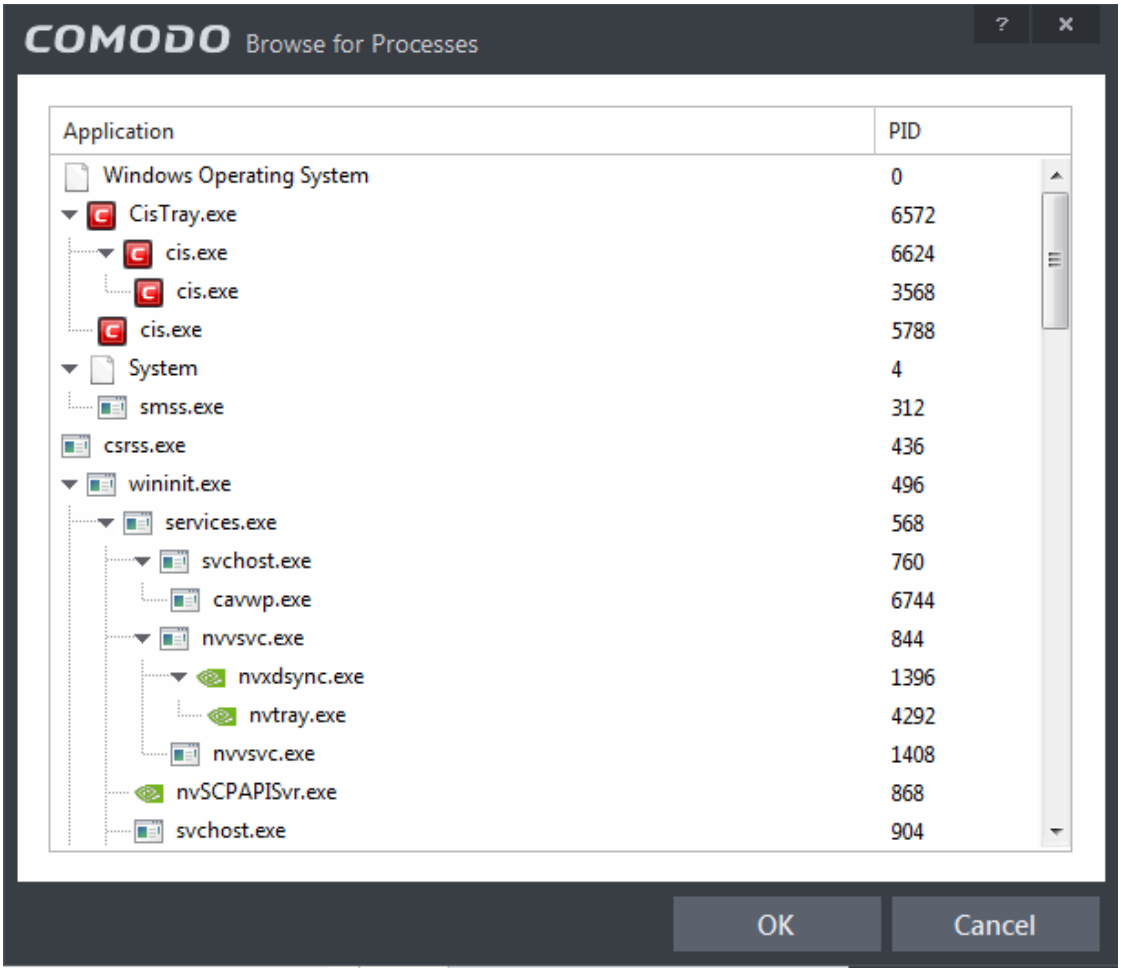
You now have 3 methods available to choose the application for which you wish to create a ruleset - **File Groups**; **Files** and **Running Processes** and

i. **File Groups** - choosing this option allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders. To view the file types and folders that are affected by choosing one of these options, you need to visit the 'Protected Files' of Comodo Internet Security by navigating to: Advanced Settings > Security Settings > Defense+ > HIPS > File Protection> Protected Files and clicking the handle from the bottom center > Groups. For more details on file groups, refer to the section **File Groups**.

ii. **Files -** this option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the firewall ruleset. In the example below, we have decided to create a firewall ruleset for the Opera web browser.



iii. **Running Processes** - as the name suggests, this option allows you to create and deploy firewall ruleset for any process that is currently running on your PC.



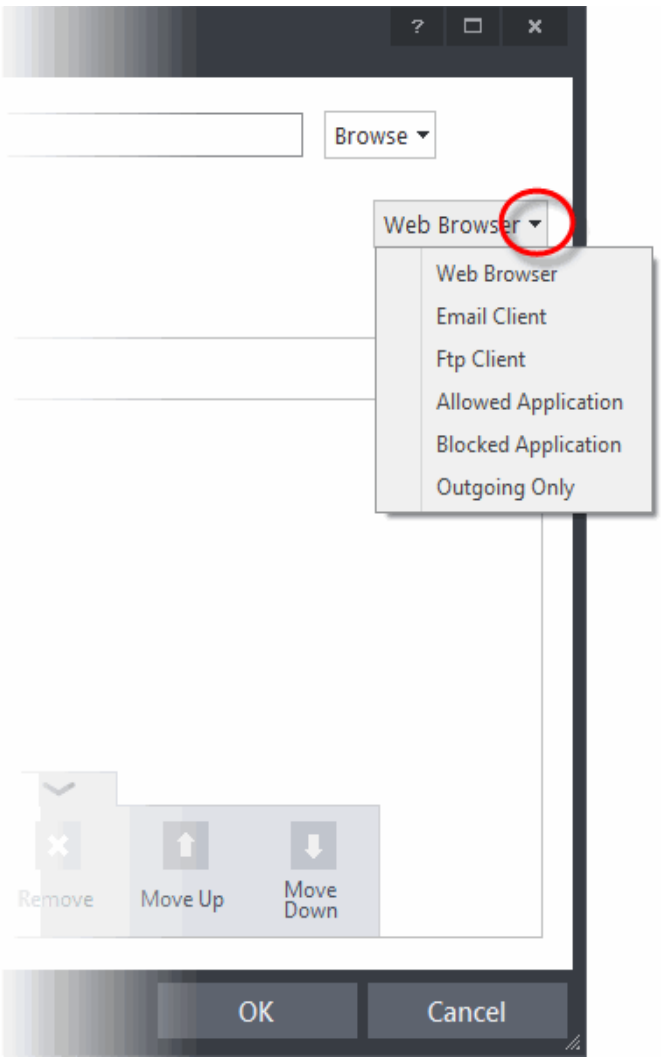
You can choose an individual process or the parent process of a set of running processes. Click 'OK' to confirm your choice.

Having selected the individual application, running process or file group, the next stage is to Configure the rules for this application's Firewall Ruleset.

Step 2 - Configure the rules for this application's ruleset

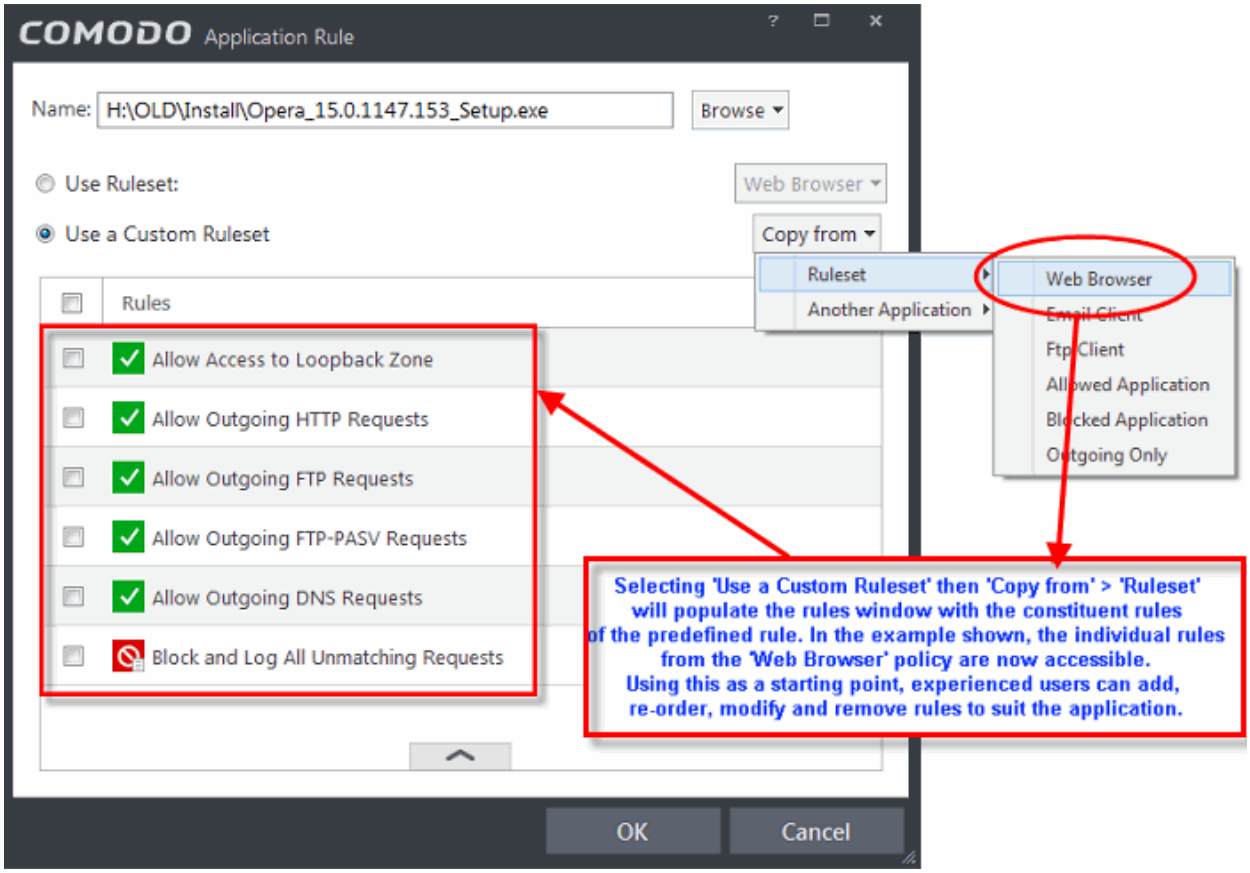
There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset** - Selecting this option allows the user to quickly deploy an existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Opera' browser. The name of the predefined ruleset you choose is displayed in the **Treat As** column for that application in the **interface** ***(Default = Disabled).***



Note: Predefined Rulesets, once chosen, cannot be modified ***directly*** from this interface - they can only be modified and defined using the **Predefined Rulesets** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - designed for more experienced users, the **Custom Ruleset** option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset ***(Default = Enabled)***.



You can create an entirely new ruleset or use a predefined ruleset as a starting point by:

- Clicking the handle from the bottom right and choosing 'Add' from the options to add individual Firewall rules. See '**Adding and Editing a Firewall Rule**' for an overview of the process.
- Use the 'Copy From' button to populate the list with the Firewall rules of a **Predefined Firewall Rule.**
- Use the 'Copy From' button to populate the list with the Firewall rules of another application's ruleset.

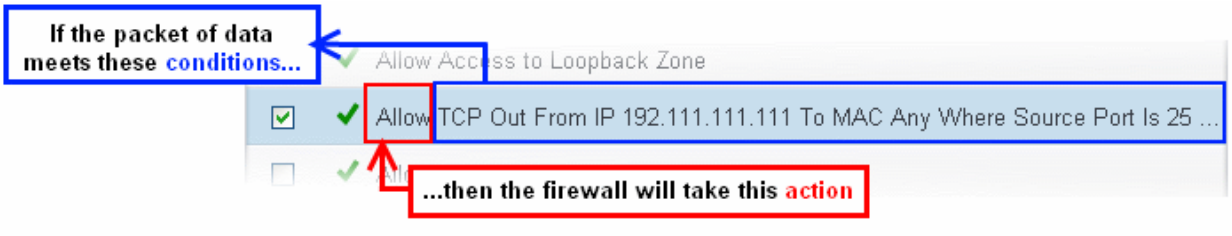
General Tips:

- If you wish to create a reusable ruleset for deployment on multiple applications, we advise you add a new **Predefined Firewall Rules** (or modify one of the existing ones to suit your needs) - then come back to this section and use the '**Ruleset**' option to roll it out.
- If you want to build a bespoke ruleset for maybe one or two specific applications, then we advise you choose the '**Use a Custom Ruleset**' option and create your ruleset either from scratch by adding individual rules or by using one of the built-in rulesets as a starting point.

Understanding Firewall Rules

At their core, each Firewall can be thought of as a simple **IF THEN** trigger - a set of **conditions** (or attributes) pertaining to a packet of data from a particular application and an **action** it that is enforced if those conditions are met.

As a packet filtering firewall, Comodo Firewall analyzes the attributes of *every single* packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a Firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding Firewall rule, then the connection is automatically blocked until a rule is created.



The actual **conditions** (attributes) you see * on a particular Firewall Rule are determined by the protocol chosen in **Adding and Editing a Firewall Rule**

If you chose 'TCP' , 'UDP' or 'TCP and 'UDP', then the rule has the form: **Action** |**Protocol** | **Direction** |**Source Address** | **Destination Address** | **Source Port** | **Destination Port**

If you chose 'ICMP', then the rule has the form: **Action** |**Protocol** | **Direction** | **Source Address** | **Destination Address** | **ICMP Details**

If you chose 'IP', then the rule has the form: **Action** | **Protocol** | **Direction** | **Source Address** | **Destination Address** | **IP Details**

- **Action**: The action the firewall takes when the conditions of the rule are met. The rule shows '**Allow**', '**Block**' or '**Ask**'.**
- **Protocol**: States the protocol that the target application must be attempting to use when sending or receiving packets of data. The rule shows '**TCP**', '**UDP**', '**TCP** or **UDP**', '**ICMP**' or '**IP**'
- **Direction**: States the direction of traffic that the data packet must be attempting to negotiate. The rule shows '**In**', '**Out**' or '**In/Out**'
- **Source Address**: States the source address of the connection attempt. The rule shows '**From**' followed by one of the following: **IP** , **IP range**, **IP Mask** , **Network Zone**, **Host Name** or **Mac Address**
- **Destination Address**: States the address of the connection attempt. The rule shows '**To**' followed by one of the following: **IP**, **IP range**, **IP Mask**, **Network Zone**, **Host Name** or **Mac Address**
- **Source Port**: States the port(s) that the application must be attempting to send packets of data through. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **Destination Port**: States the port(s) on the remote entity that the application must be attempting to send to. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **ICMP Details**: States the ICMP message that must be detected to trigger the action. See **Adding and Editing a Firewall Rule** for details of available messages that can be displayed.
- **IP Details**: States the type of IP protocol that must be detected to trigger the action: See **Adding and Editing a Firewall Rule** to see the list of available IP protocols that can be displayed here.

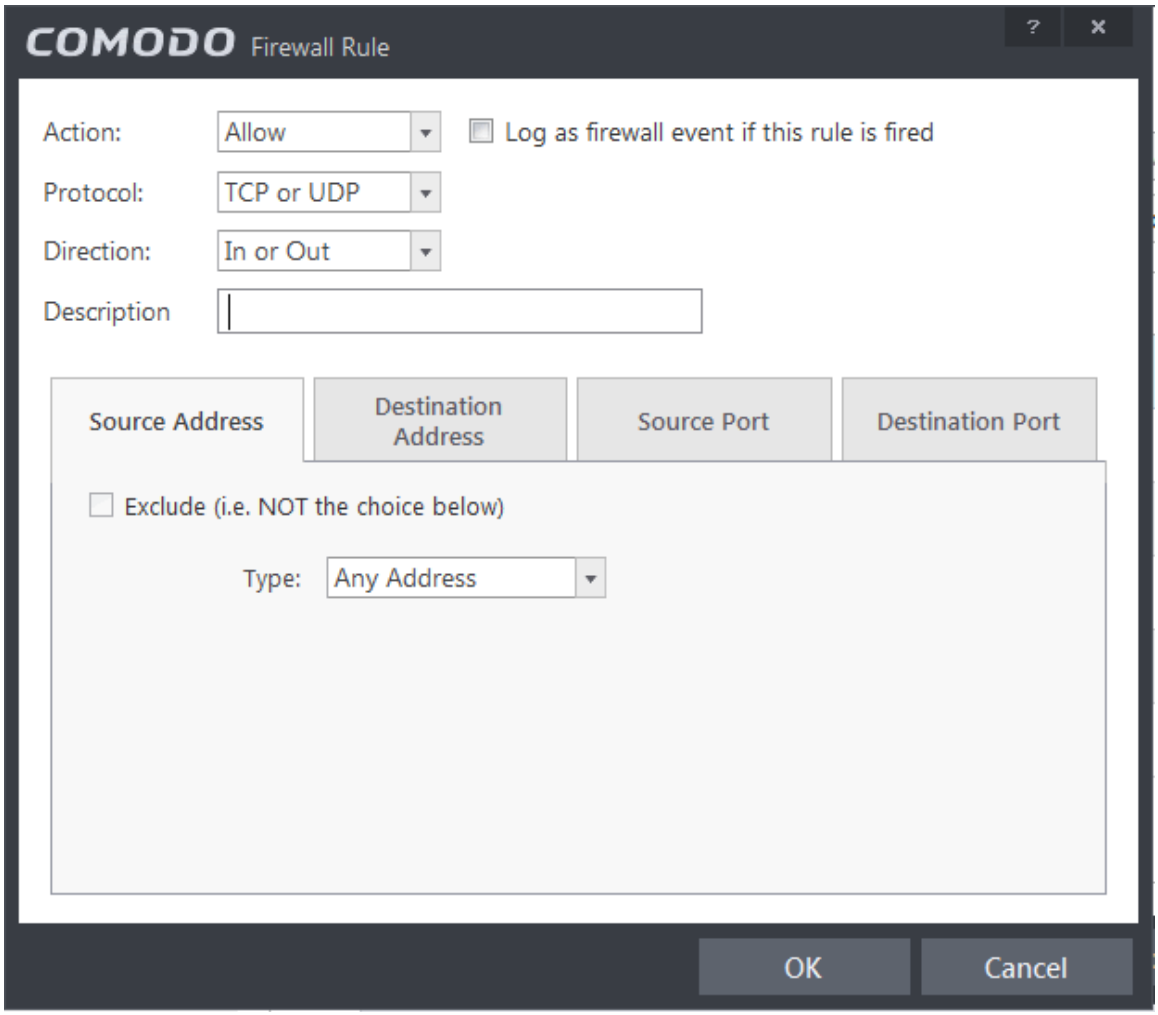
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section '**Global Rules**' to understand the interaction between Application Rules and Global Rules.

* *If you chose to add a descriptive name when creating the rule then this name is displayed here rather than it's full parameters. See the next section, '**Adding and Editing a Firewall Rule**', for more details.*

** *If you selected 'Log as a firewall event if this rule is fired' then the action is postfixed with 'Log'. (e.g. Block & Log)*

Adding and Editing a Firewall Rule

The Firewall Rule Interface is used to configure the actions and conditions of an individual Firewall rule. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading the sections **'Understanding Firewall Rules', 'Overview of Rules and Policies' and 'Creating and Modifying Firewall Rulesets'**



General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' ***(Default)***, '**Block**' or '**Ask**'.
- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' ***(Default)***, '**ICMP**' or '**IP**' .

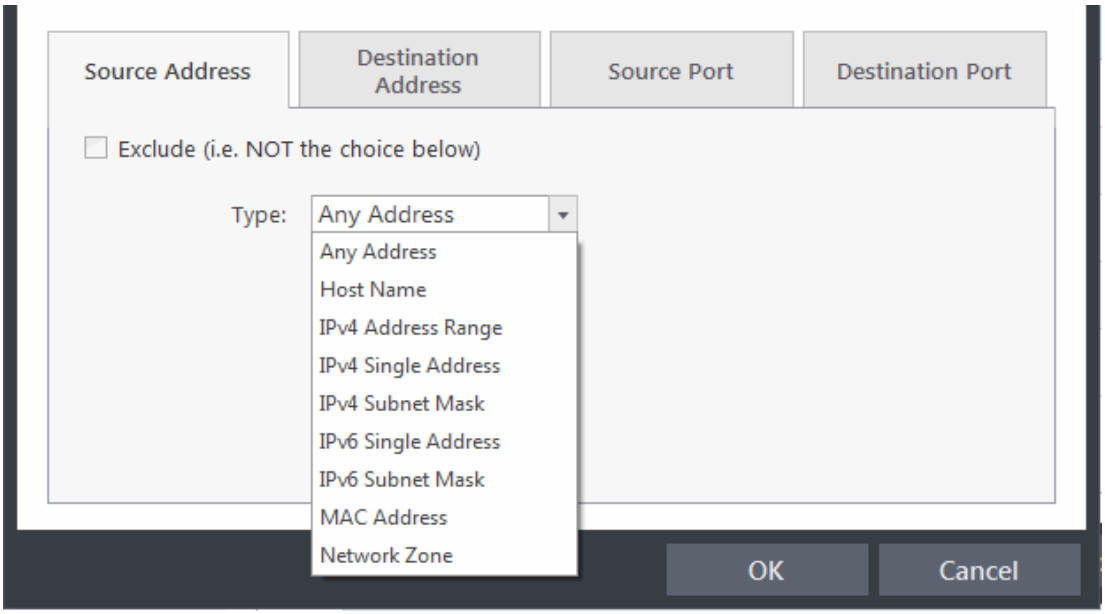
Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out'** ***(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the **firewall event log viewer** whenever this rule is called into operation. (i.e. when ALL conditions have been met) ***(Default = Disabled).***
- **Description**: Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is displayed to represent instead of the full actions/conditions in the main **Application Rules interface** and the **Application Rule interface**.

Protocol

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

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information.



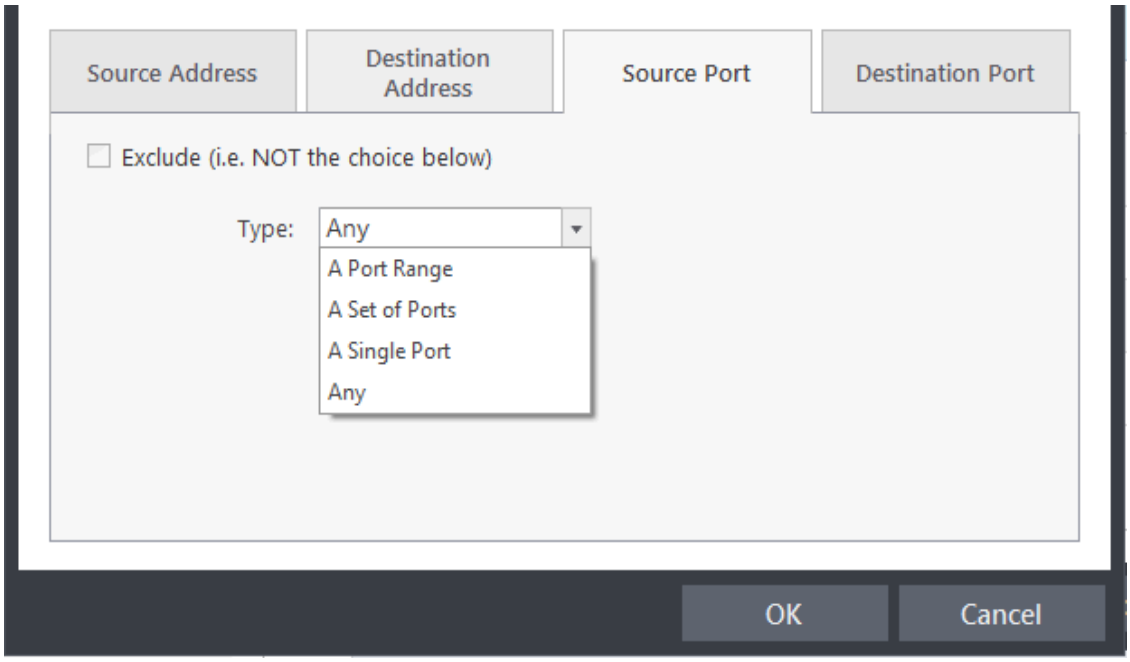
Source Address and Destination Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.
9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.



1. You can choose any port number by selecting Any - set by default , 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a predefined **Port Set** by choosing A Set of Ports. If you wish to create a custom port set then please see the section '**Port Sets**'.

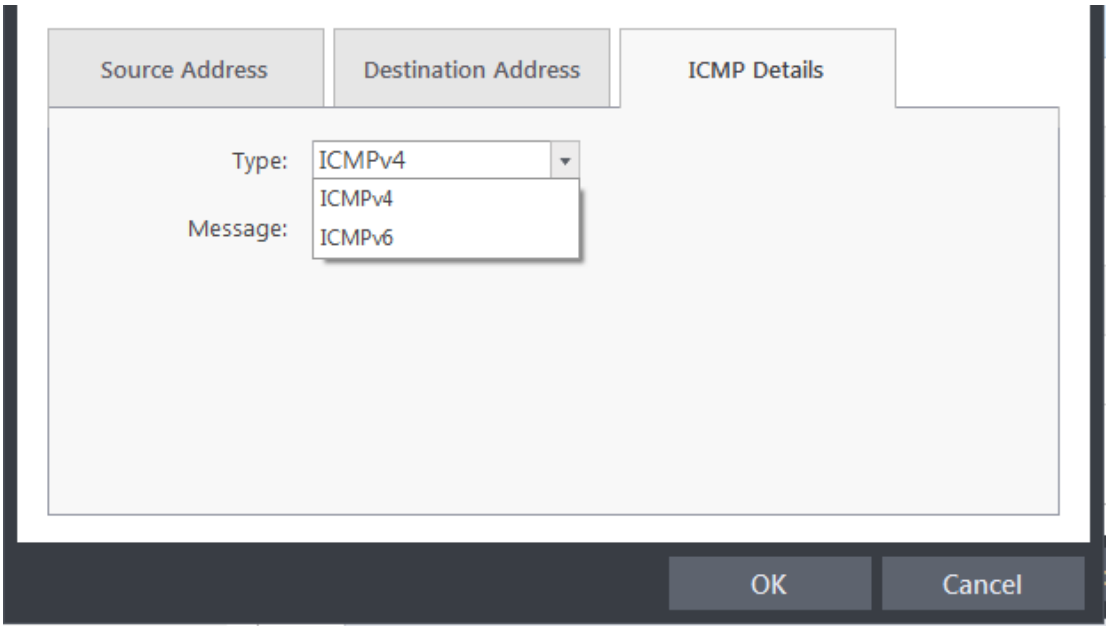
ii. **ICMP**

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

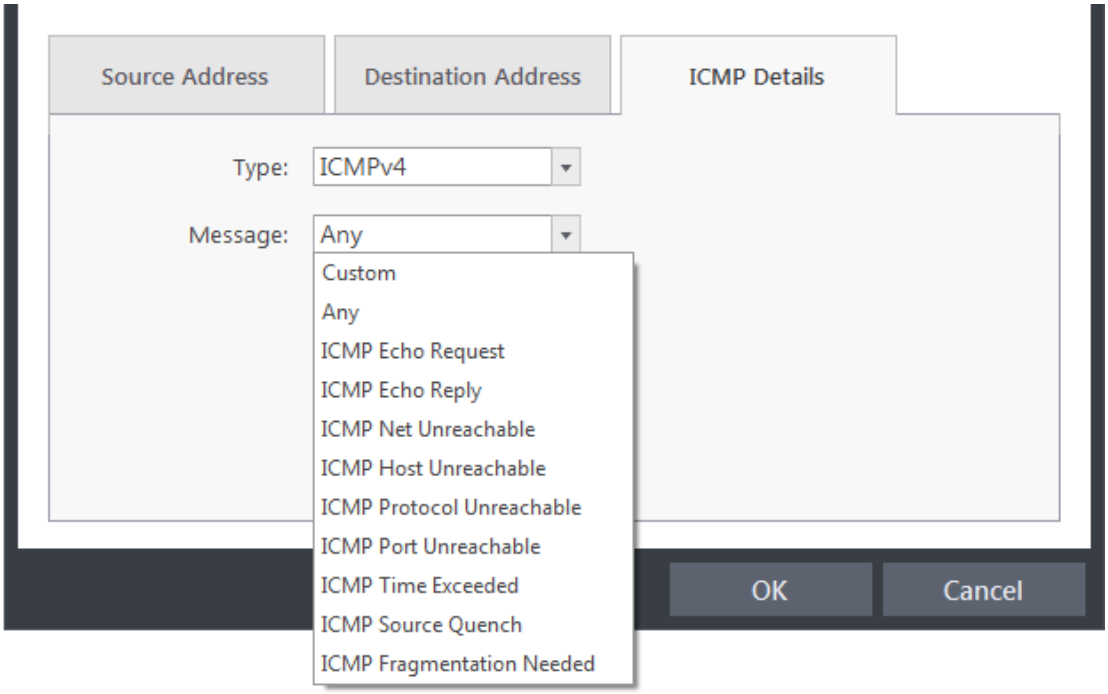
- **ICMP Details**

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.
2. Under the 'ICMP Details' tab, choose the ICMP version from the 'Type' drop-down.

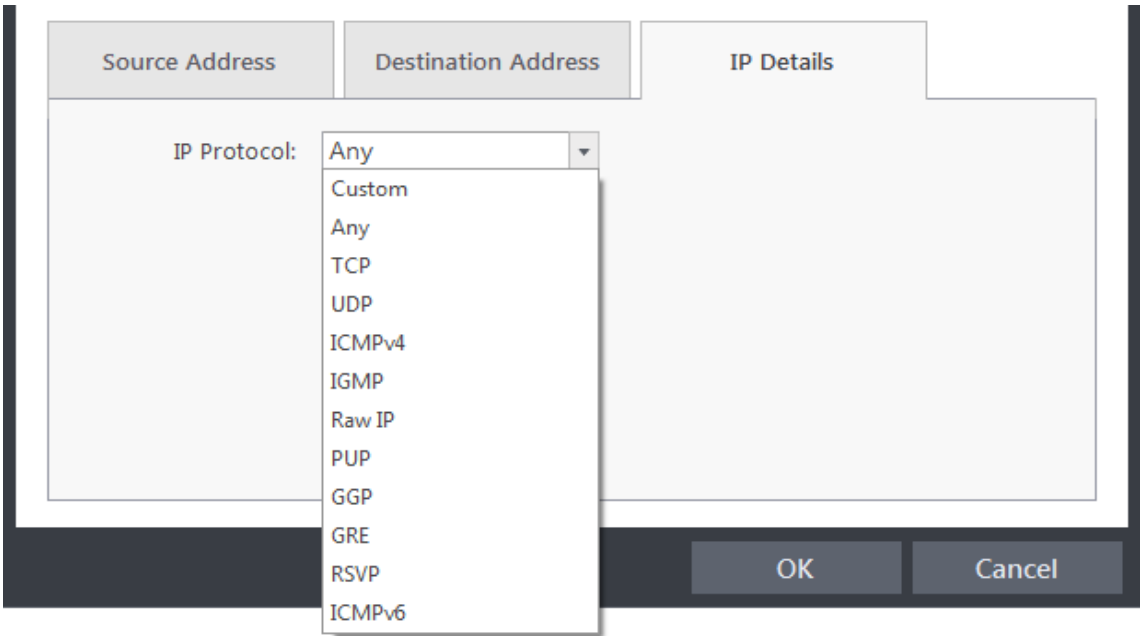


3. Specify ICMP Message , Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.
When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.



iii. **IP**

When you select IP as the protocol in **General Settings**, you are shown a list of IP message type in the 'IP Details' tab alongside the **Source Address and Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.



- **IP Details**

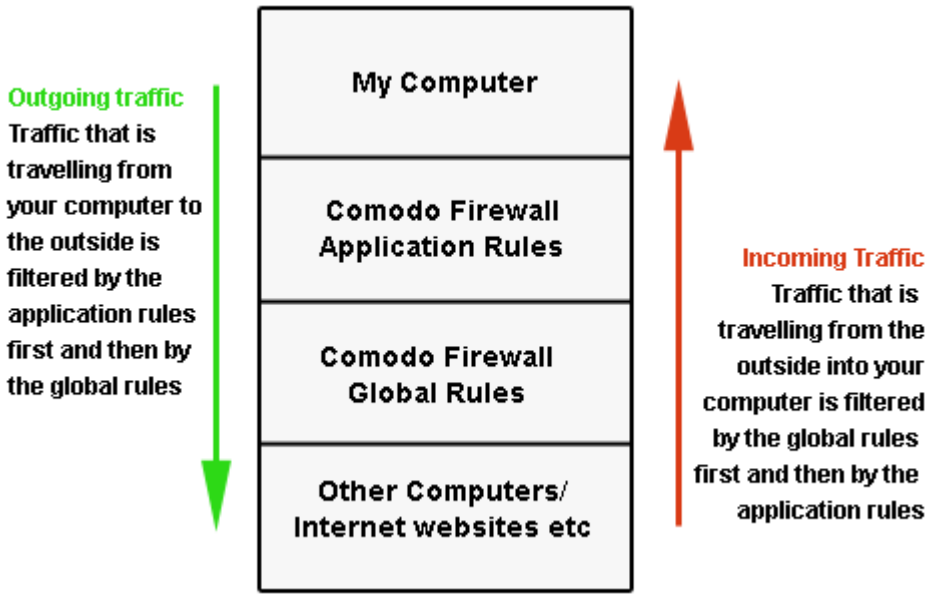
Select the types of IP protocol that you wish to allow, from the ones that are listed.

6.2.3.3. Global Rules

Unlike Application rules, which are applied to and triggered by traffic relating to a specific application, Global Rules are applied to all traffic traveling in and out of your computer.

Comodo Firewall analyzes every packet of data in and out of your PC using combination of Application and Global Rules.

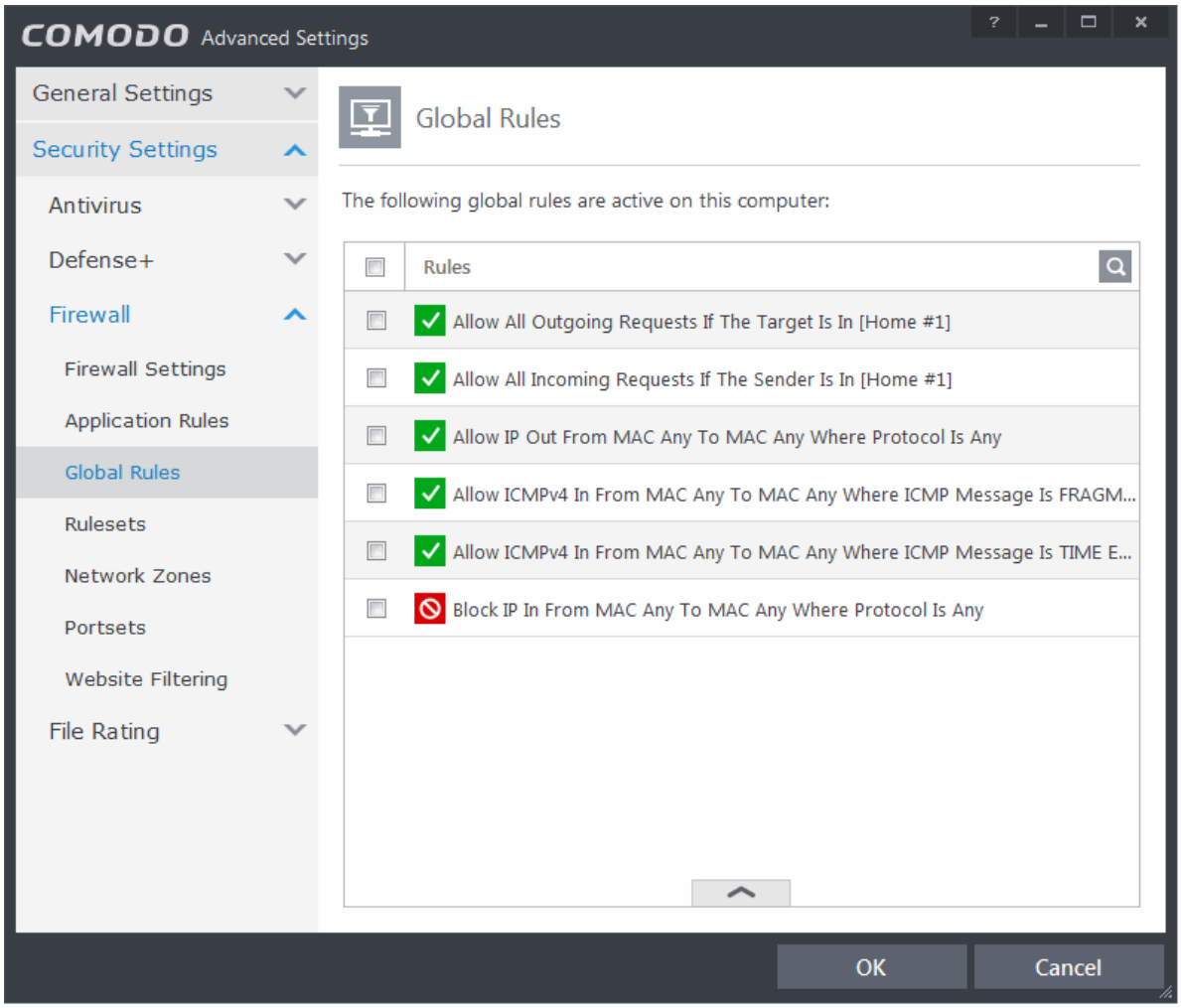
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.



Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.

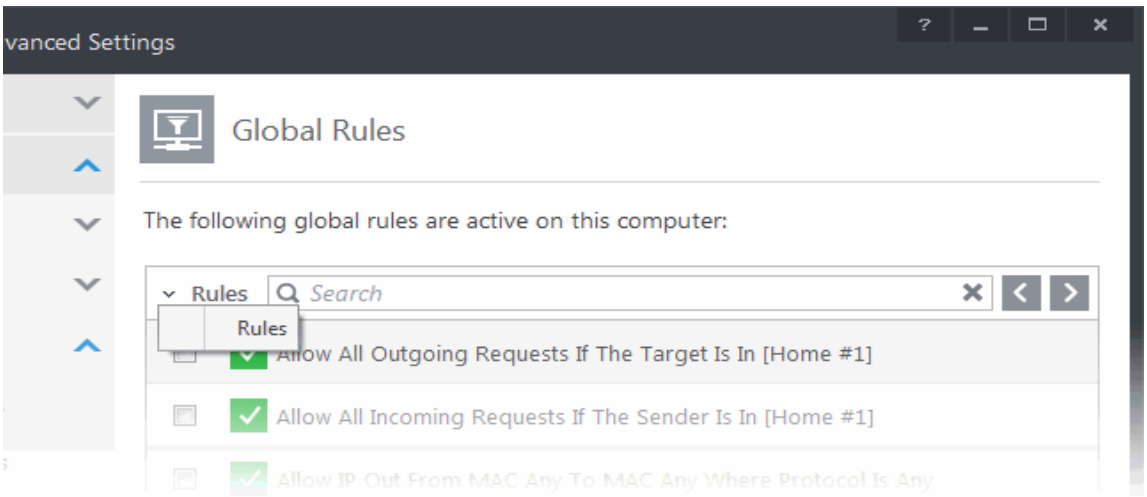
Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

- The Global Rules panel, accessible by clicking Security Settings > Firewall > Global rules tab from the Advanced tasks interface, allows you to view, add and manage the rules



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

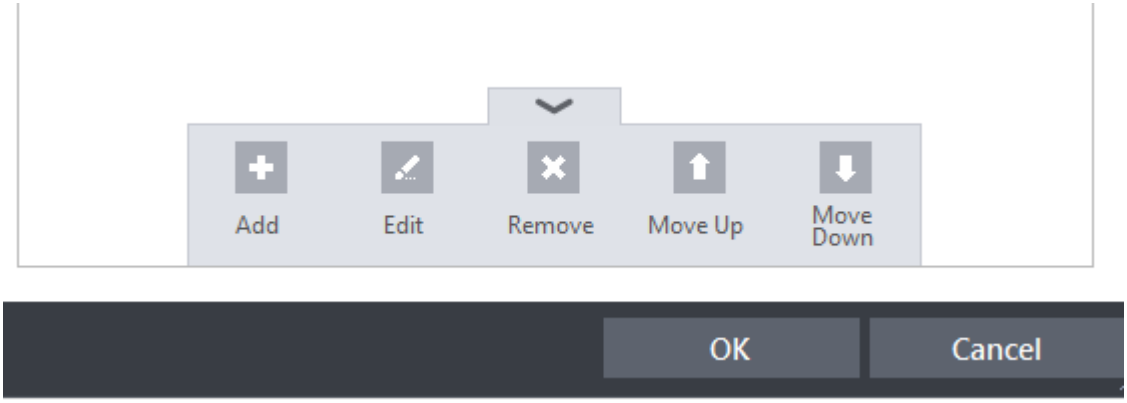
To use the search option, click the search icon at the far right in the column header.



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

General Navigation:

Clicking the handle at the bottom center of the interface opens an option panel with the following options:



- **Add** - Allows you to add a new global rule. See the section **'Adding and Editing a Firewall Rule'** for guidance on creating a new rule.
- **Edit** - Allows you to modify the selected global rule. See the section **'Adding and Editing a Firewall Rule'** for guidance on editing a new rule.
- **Remove** - Deletes the selected rule.
- **Purge** - Runs a system check to verify that all the applications for which rules are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.
- **Move Up and Move Down** - The traffic is filtered by referring to the rules in order from the top. The Move Up and Move Down buttons enable you to change the priority of a selected rule.

The configuration of Global Rules is identical to that for application rules. To add a global rule, click the 'Add...' button on the right. To edit an existing global rule, right click and select 'edit'.

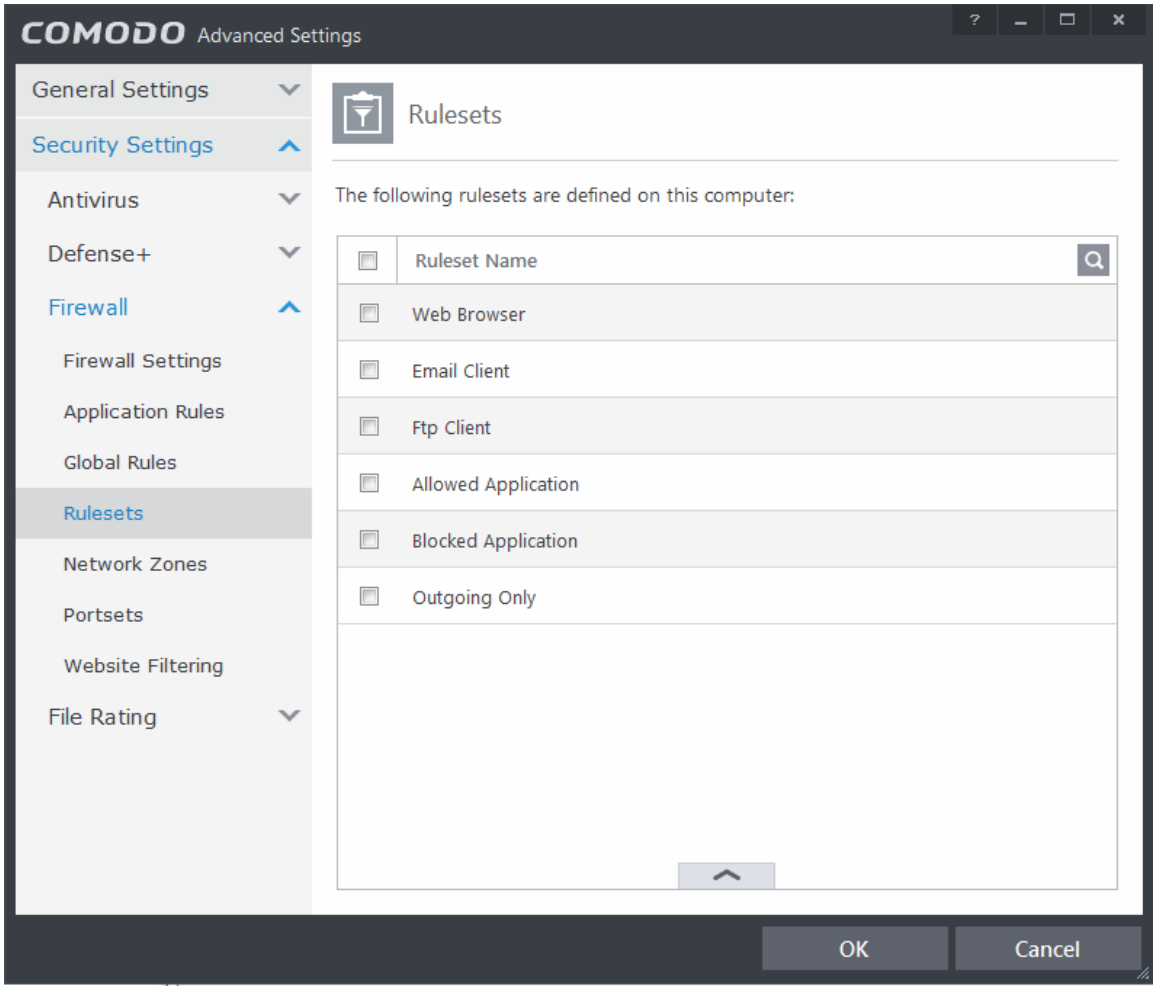
- See **Application Rules** for an introduction to the rule setting interface.
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration.

6.2.3.4. Firewall Rule Sets

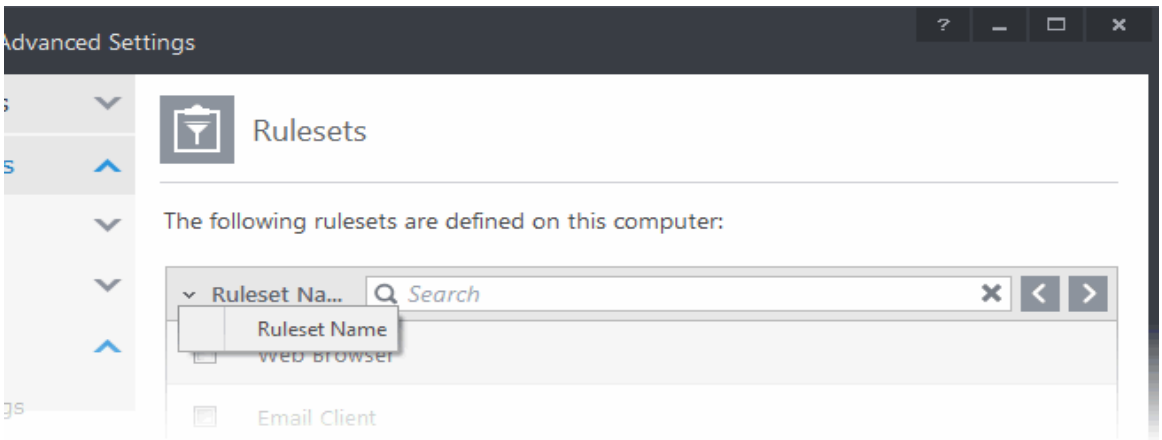
As the name suggests, a firewall Ruleset is a set of one or more individual Firewall rules that have been saved and which can be re-deployed on multiple applications. This section contains advice on the following:

- **Predefined Rulesets**
- **Creating a new ruleset**

The Predefined rulesets interface can be accessed by clicking Security Settings > Firewall > Rulesets from the 'Advanced Settings' interface.



You can use the search option to find a specific ruleset in the list by clicking the search icon at the far right in the column header.



- Enter the name of the item to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Predefined Rulesets

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may

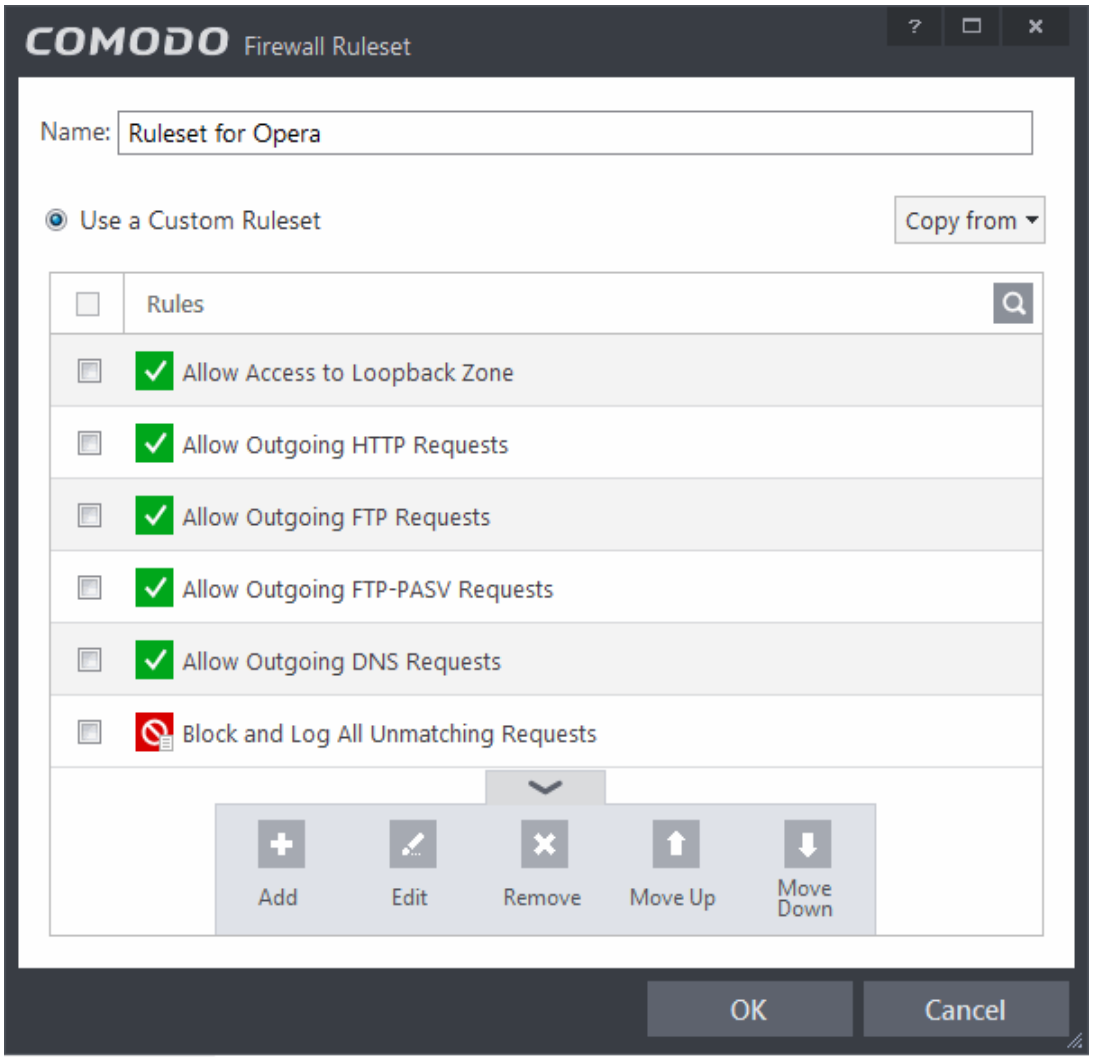
choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined policies to suit their environment and requirements. (for example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of it rules).

Creating a new ruleset

You can create new rulesets with network access control rules customized as per your requirements and can roll out them to required applications while **creating Firewall ruleset** for the applications individually.

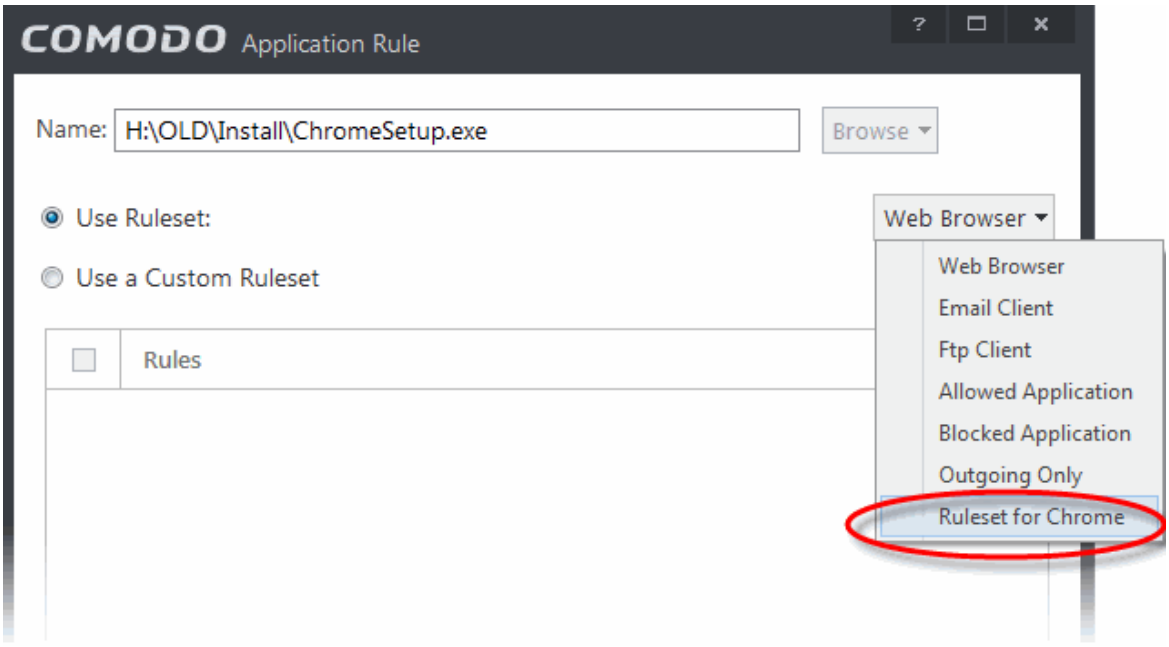
To add a new Ruleset

- Click the handle from the bottom center and select 'Add' from the options



- As this is a new ruleset, you need to name it in the text field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for. Next you should add and configure the individual rules for this ruleset. See '**Adding and Editing a Firewall Rule**' for more advice on this.

Once created, this ruleset can be quickly called from 'Use Ruleset' when **creating or modifying a Firewall ruleset**.



To view or edit an existing predefined Ruleset

- Double click on the Ruleset Name in the list

  or

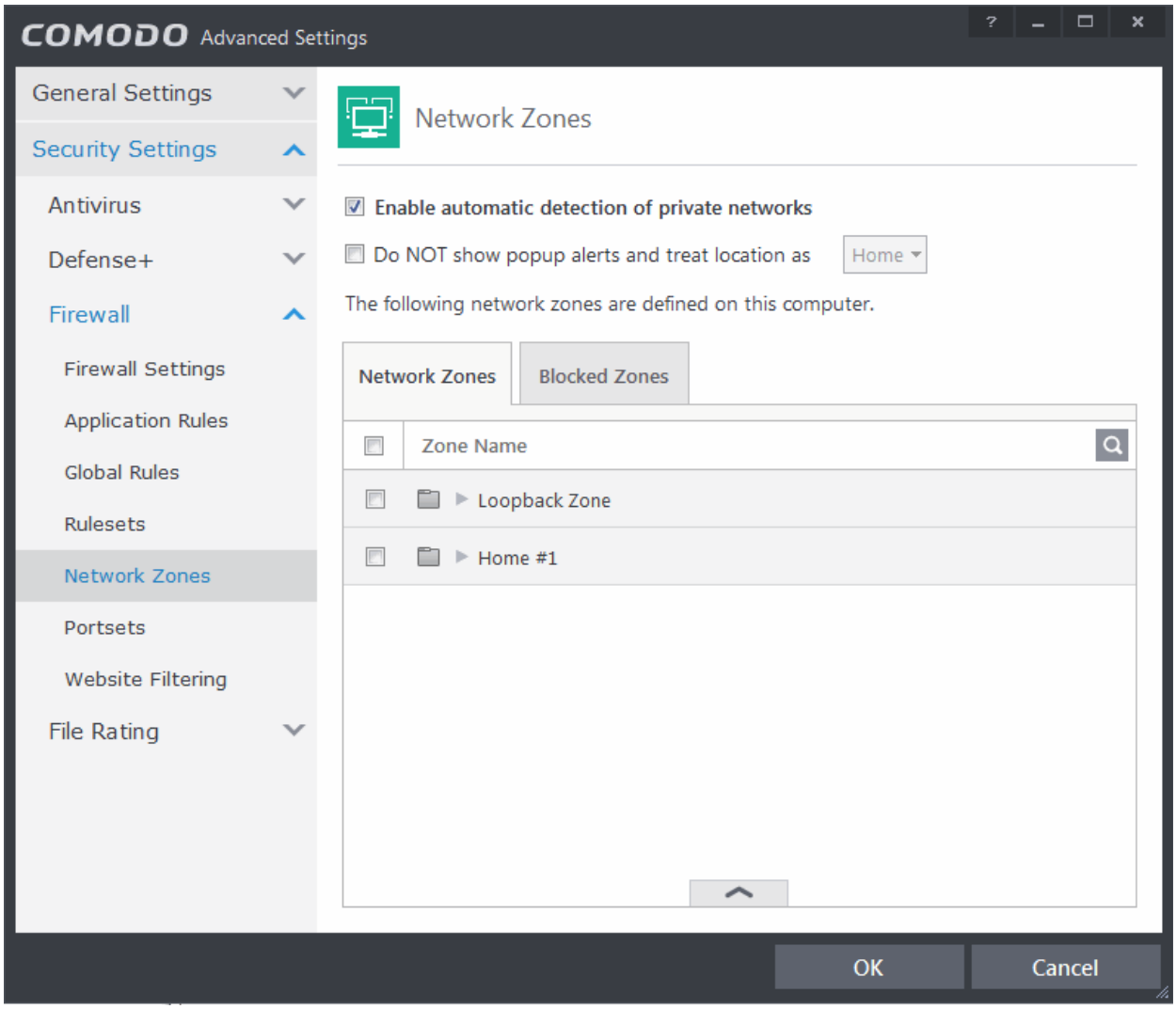
- Select the Ruleset Name, click the handle from the bottom center and select Edit from the options
- Details of the process from this point on can be found **here**.

6.2.3.5. Network Zones

The Network Zones panel allows you to:

- Configure to detect any new network (wired or wireless) that your computer is trying to connect and provide alerts for the same
- Define network zones that are trusted, and to specify access privileges to them
- Define network zones that are untrusted, and to block access to them

The Network Zones panel can be accessed by clicking Security Settings > Firewall > Network Zones from the 'Advanced Settings' interface.



- **Enable automatic detection of private networks** - Instructs Comodo Firewall to keep monitoring whether your computer is connected to any new wired or wireless network ***(Default = Enabled).*** Deselect this option if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in **'Network Zones'** and through the **'Stealth Ports Wizard'**)
- **Do NOT show popup alerts and treat location as** - If enabled, the new network connection alert will not be displayed and the network location will be saved as selected from the drop-down options - Home, Work and Public. ***(Default = Enabled with location as Work)***

If automatic detection of new networks is enabled and pop up alert is disabled, then the following alert will be displayed whenever your system is trying to connect to any new wired or wireless network.

You can select the type of new network you are connected to, so that the firewall configuration is optimized for the type of connection.

- Select 'Do not automatically detect new networks again' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in **'Network Zones'** and through the **'Stealth Ports Wizard'**

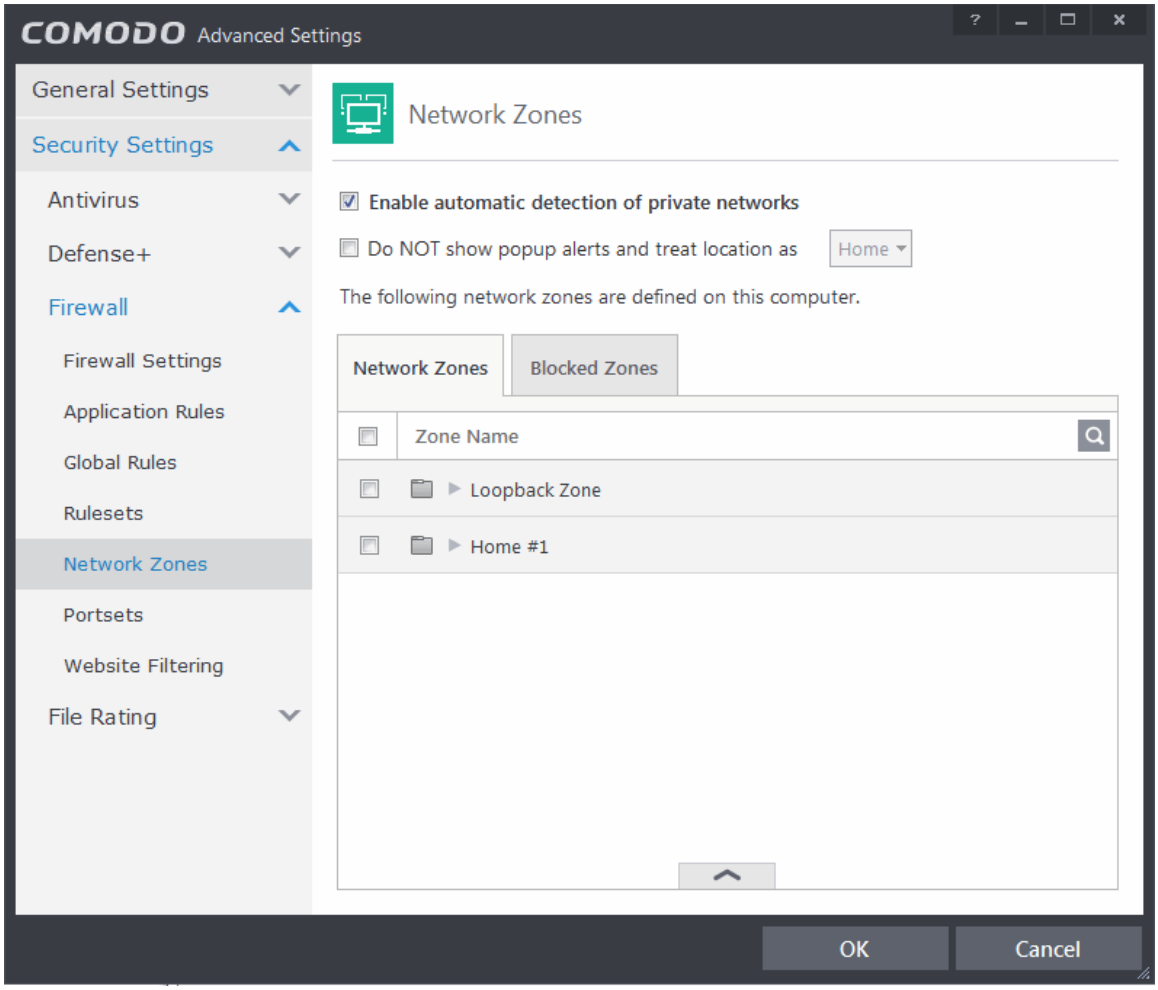
The panel has two tabs:

- **Network Zones** - Allows you to define network zones and to allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.
- **Blocked Zones** - Allows you to define trusted networks that are not trustworthy and to block access to them.

6.2.3.5.1. Network Zones

A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied.

Background Note: A computer network is a connection between computers through a cable or some type of wireless connection. It enables users to share information and devices between computers and other users within the network. Obviously, there are certain computer networks where you need to grant access to, including your home or work network. Conversely, there may be other networks where you want to restrict communication with - or even block entirely.



Note 1: Adding a zone to this area does not, in itself, define any permission levels or access rights to the zone. This area allows to define the zones so you can quickly assign such permissions **in other areas of the firewall**.

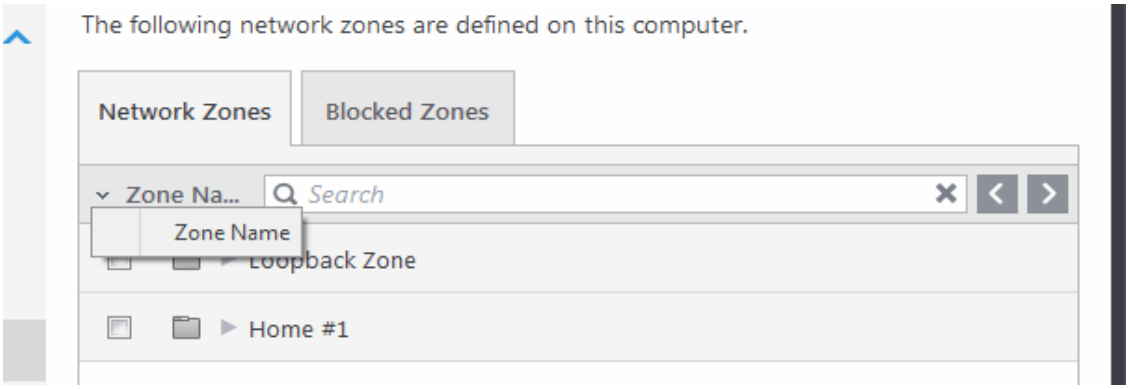
Note 2: A network zone can be designated as 'Trusted' and allowed access from the '**Manage Network Connections**' interface (An example would be your home computer or network).

Note 3: A network zone can be designated as 'Blocked' and denied access by using the '**Blocked Zones**' interface. (An example would be a known spyware site).

Note 4: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rule** can be assigned to a network zone to all activity 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 the search option to find a network zone in the list by clicking the search icon at the far right in the column header.



- Enter the name of the item to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

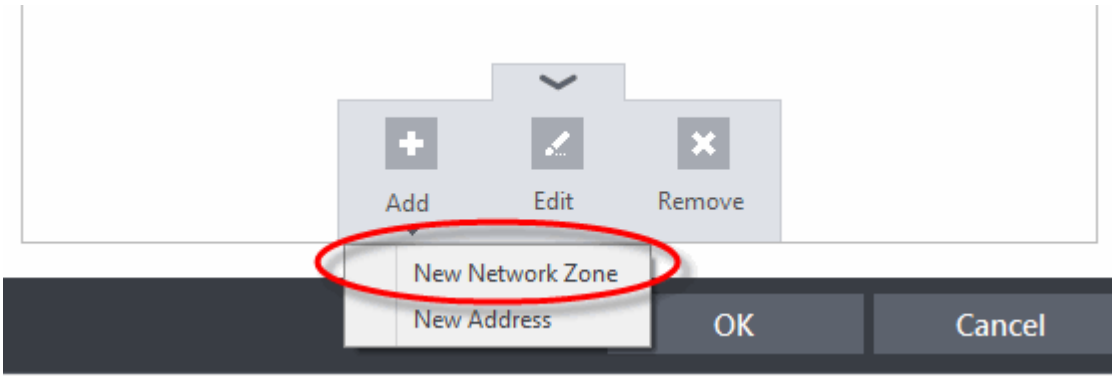
Defining a new Network Zone

To add a new network zone:

- Step 1 - **Define a name for the zone**.
- Step 2 - **Select the addresses to be included in this zone**.

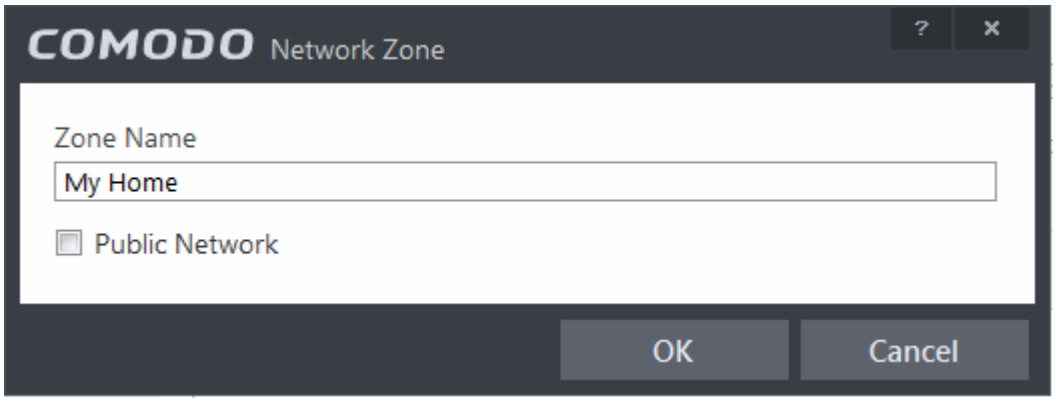
Step 1 - Define a name for the zone

1. Click the handle from the bottom center select 'Add' > 'New Network Zone'.



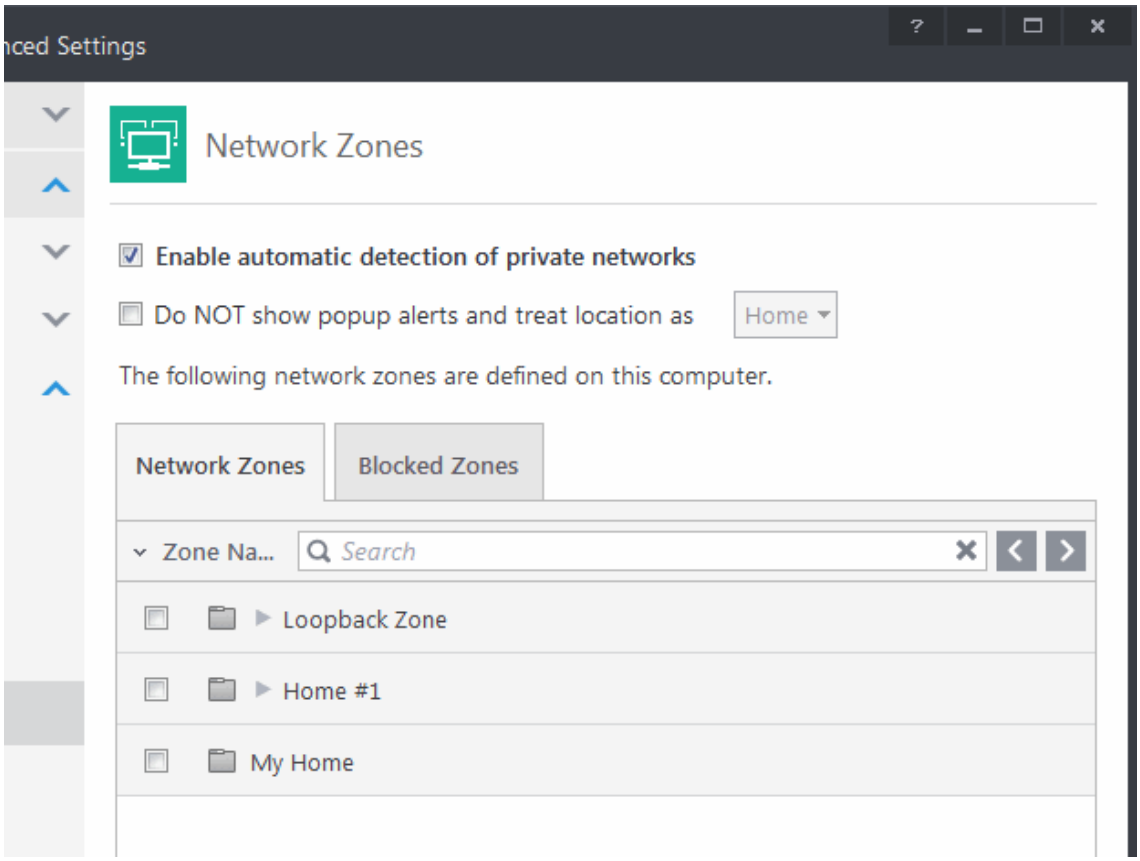
A dialog box will appear, prompting you to specify a name for the new zone.

2. Choose a name that accurately describes the network zone you are creating.



3. Select the checkbox 'Public Network' if you are defining a network zone for a network in a public place, for example, when you are connecting to a Wi-Fi network at an airport, restaurant etc., so that Comodo Firewall will optimize the configuration accordingly.
4. Click 'Apply' to confirm your zone name.

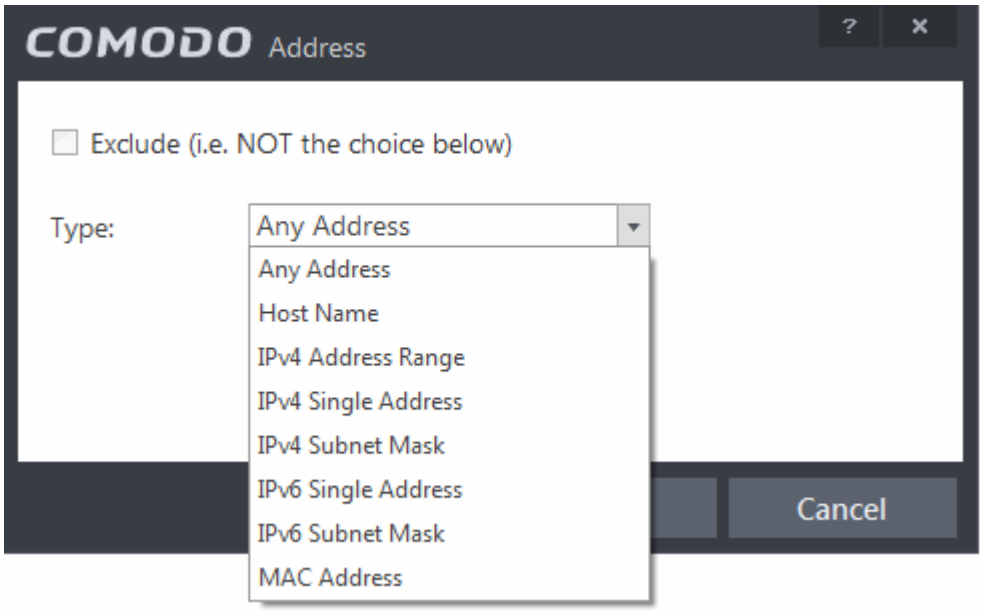
This adds the name of your new zone to the Network Zones list.



Step 2 - Select the addresses to be included in this zone

1. Select the network name, click the handle at the bottom center and choose 'Add' > 'New Address' from the options or click the + button beside the new network zone name and double click on '(add addresses here)'

   The 'Address' dialog allows you to select an address from the Type drop-down box shown below ***(Default = Any Address)***. The Exclude check box will be enabled only if any other choice is selected from the drop-down box.



Select Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to

an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.

2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

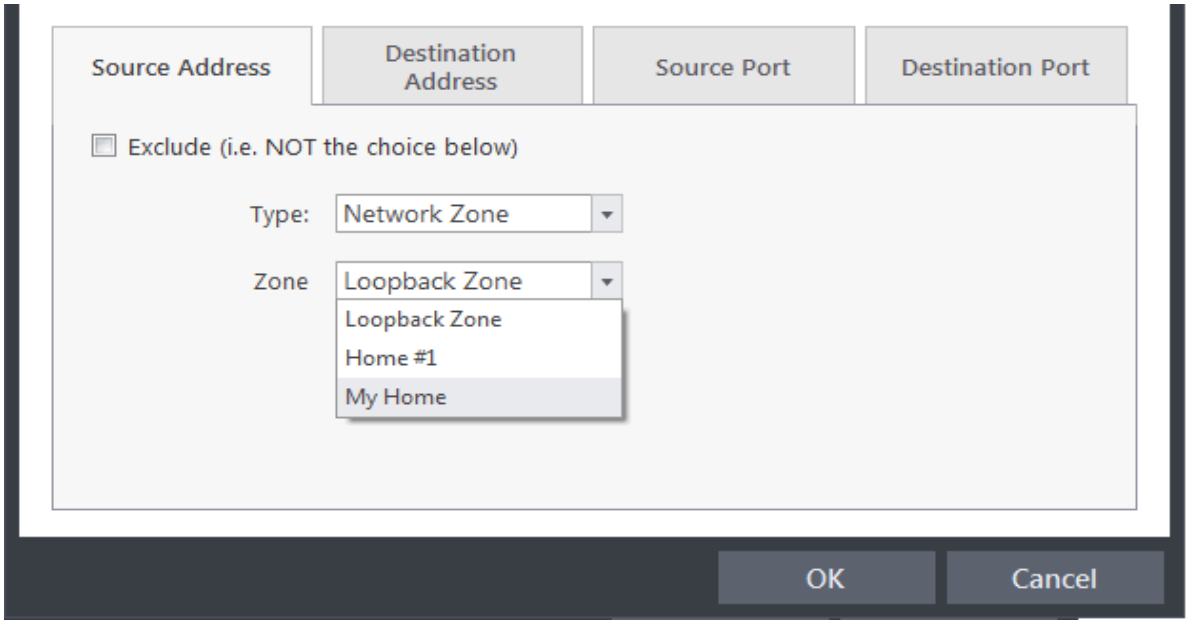
- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

2. Click 'OK' to confirm your choice.
3. Click 'OK' in the 'Network Zones' interface.

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

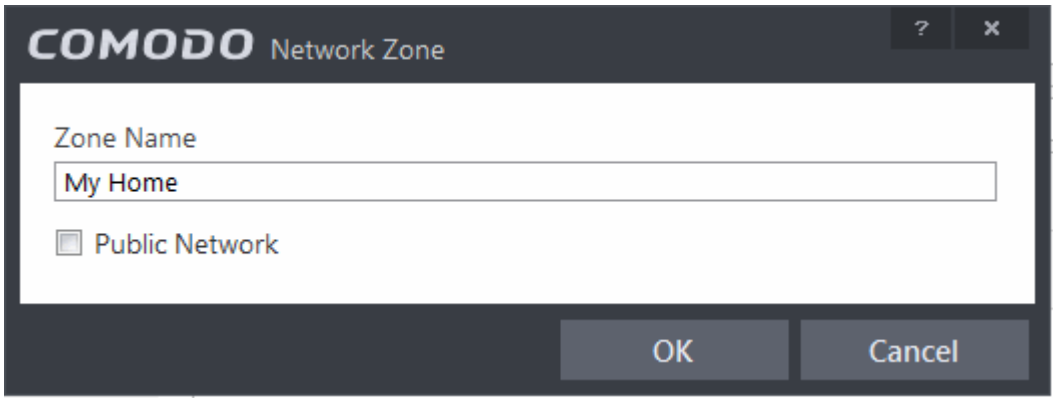
- Quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**



- Quickly called and designated as a blocked zone from the '**Blocked Zones**' interface

To edit the name of an existing Network Zone

1. Select the name of the zone in the list (e.g. My Home), click the handle at the bottom center and choose 'Edit' from the options or double click on the network zone name.



2. Edit the name of the zone.

To add more addresses to an existing Network Zone

- Select the network name, click the handle at the bottom center and choose 'Add > A new Address' from the options
- Add new address from the **'Address' interface**.

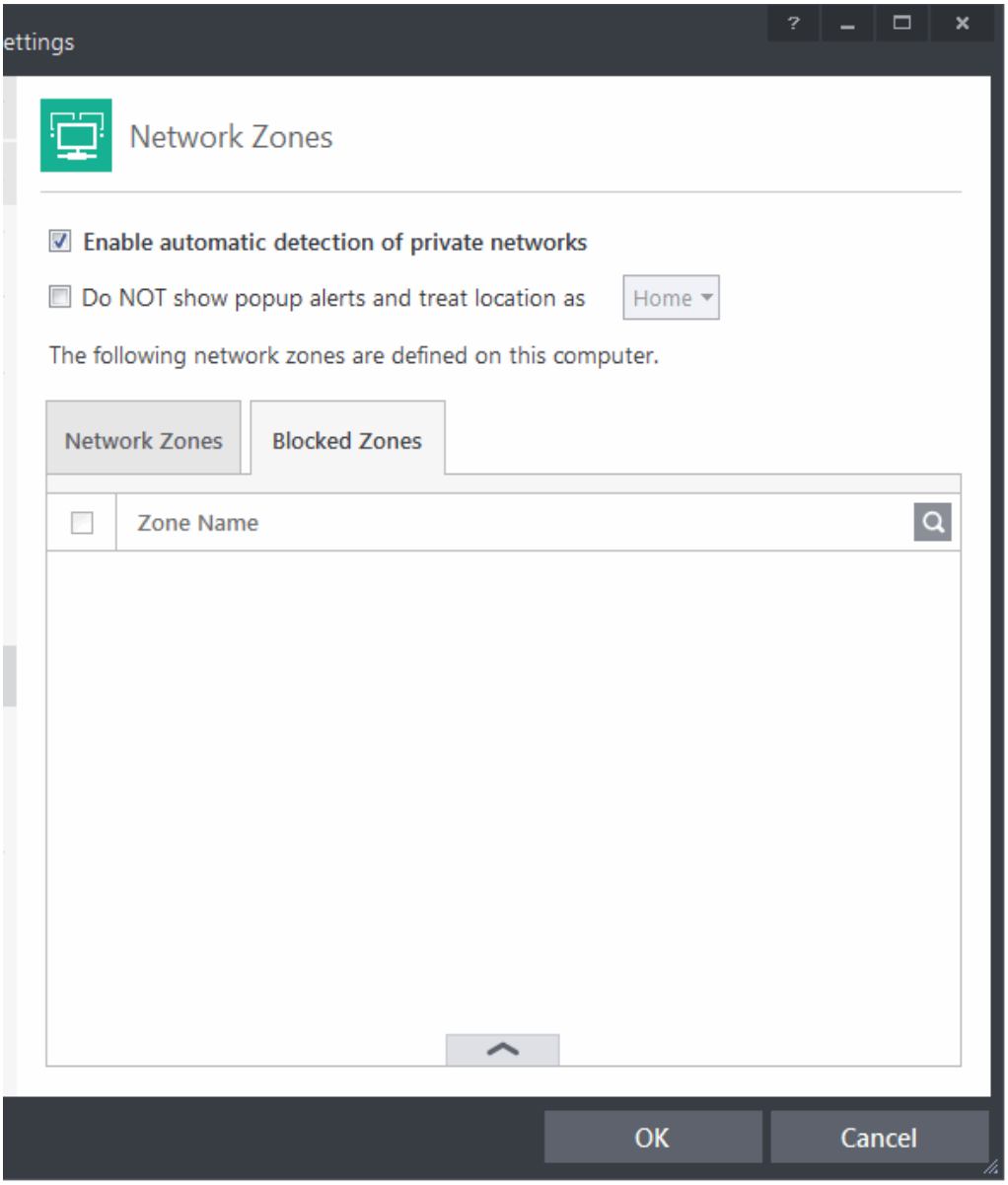
To modify or change the existing address in a zone

- Click the + button beside the network zone name to expand the addresses
- Double click on the address to be edited or select the address, click the handle from the bottom center and choose Edit from the options
- Edit the address from the **'Address' interface**.

6.2.3.5.2. Blocked Zones

A computer network enables users to share information and devices between computers and other users within the network. Obviously, there are certain computer networks that you need to 'trust' and grant access to - for example your home or work network. Unfortunately, there may be other, untrustworthy networks that you want to restrict communication with - or even block entirely.

Note: We advise new or inexperienced users to first read '**Network Zones**' , '**Stealth Ports Wizard**' and '**Application Rules**' before blocking zones using this interface.



The 'Blocked Network Zones' tab allows you to:

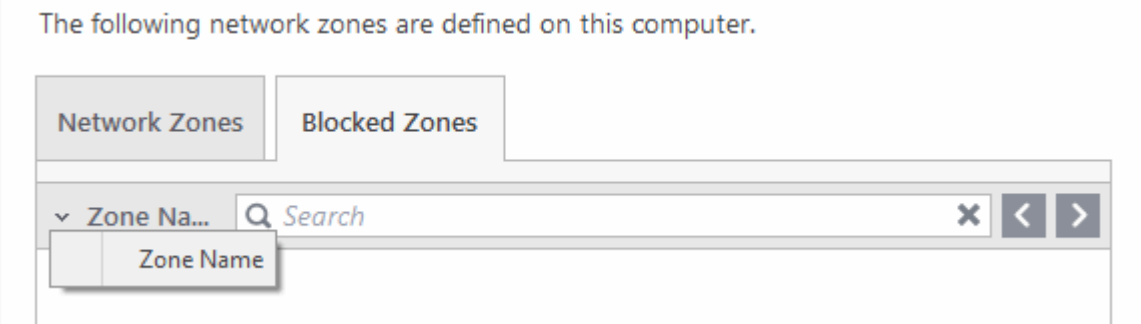
- **Deny access to a specific network by selecting a pre-existing network zone and designating it as blocked**
- **Deny access to a specific network by manually defining a new blocked zone**

Note 1: You must create a zone before you can block it. There are two ways to do this;

1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

Note 2: You cannot reconfigure *pre-existing* network zones from this interface. (e.g., to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

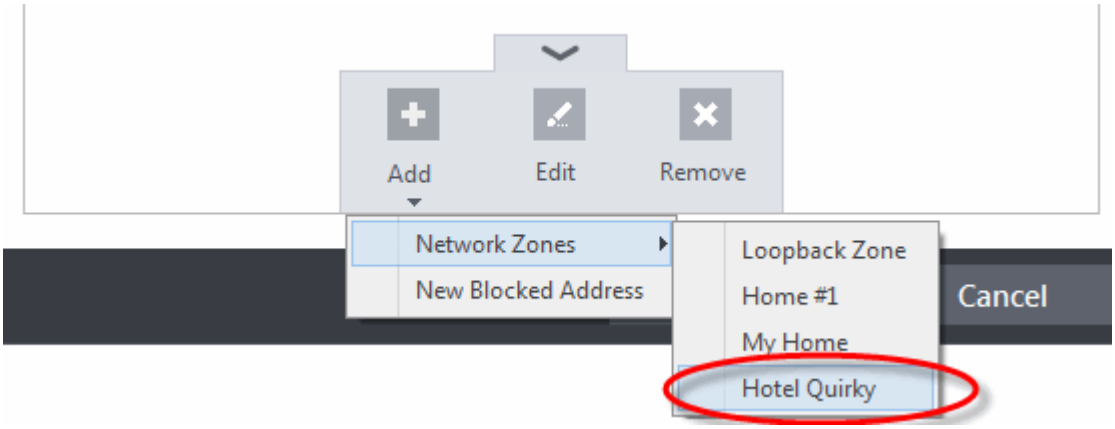
You can use the search option to find a blocked zone in the list by clicking the search icon at the far right in the column header.



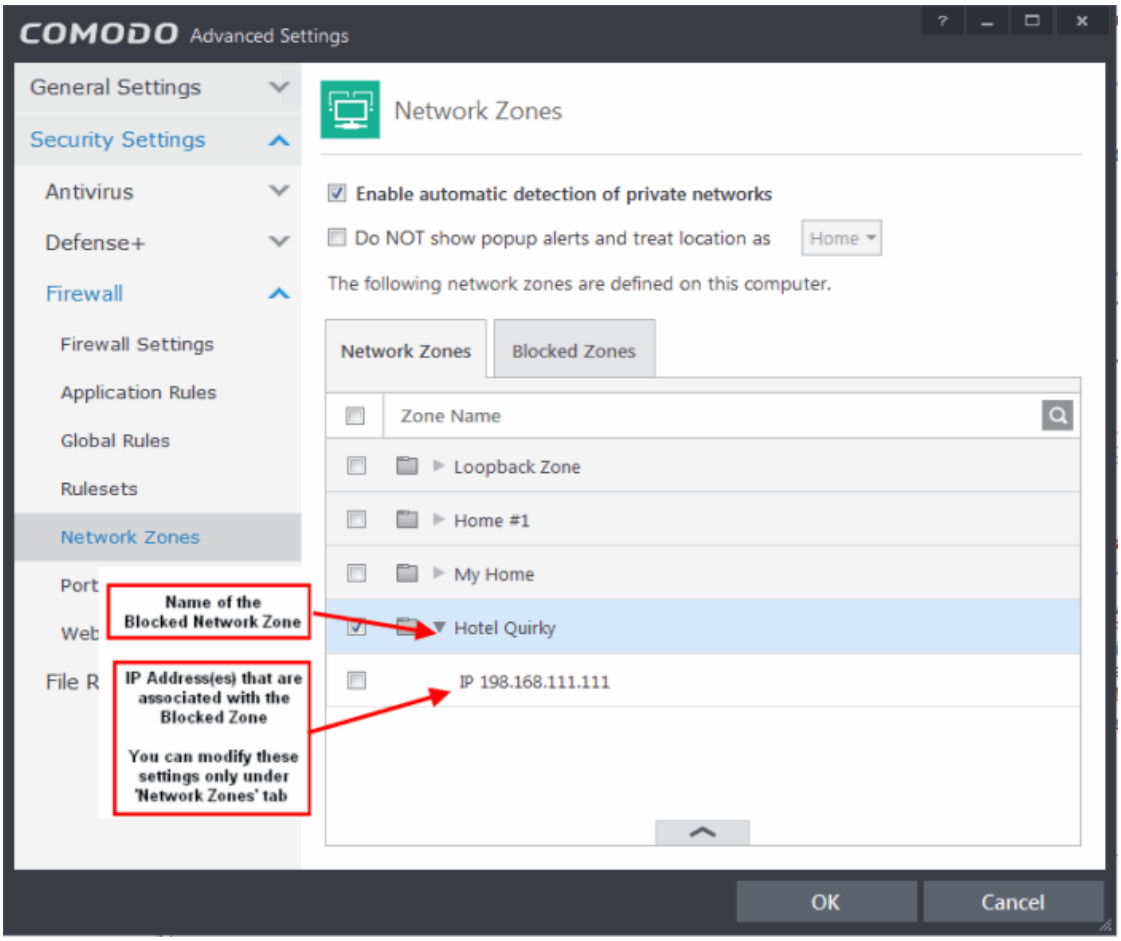
- Enter the name of the zone to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

To deny access to a specific network by selecting a pre-existing network zone and designating it as blocked

1. Click the handle from the bottom center and choose 'Add' > 'Network Zones' from the options
2. Select the particular zone you wish to block.



The selected zone will appear in the 'Blocked Zones' interface.

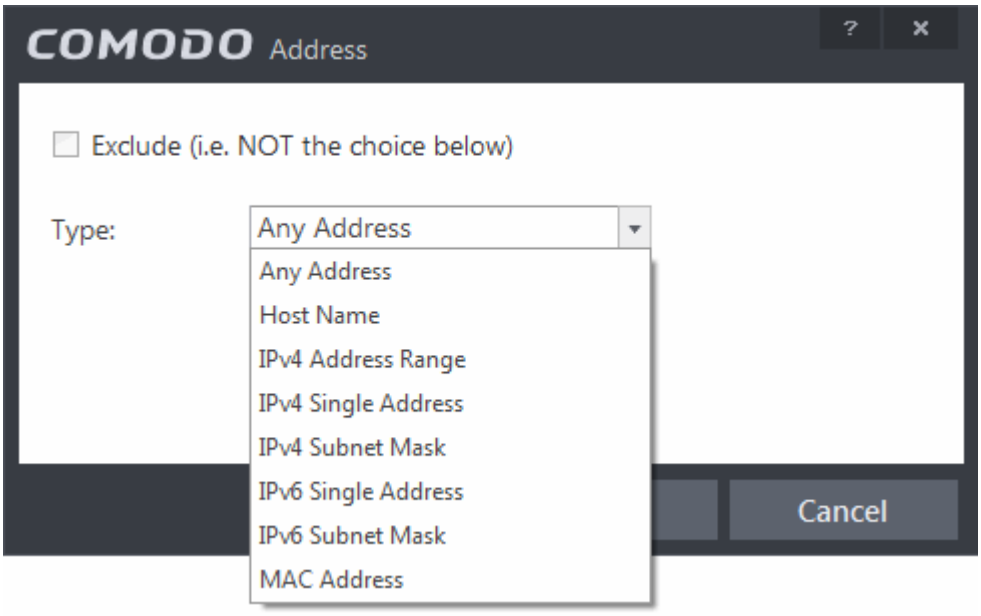


3. Click 'OK' to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

To deny access to a specific network by manually defining a new blocked zone

1. Click the handle from the bottom center and choose 'Add' > 'New Blocked Address' from the options.

The Address dialog will appear. The 'Address' dialog allows you to select an address from the Type drop-down box shown below ***(Default = Any Address)***.



Select Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

2. Select the address to be blocked and click OK

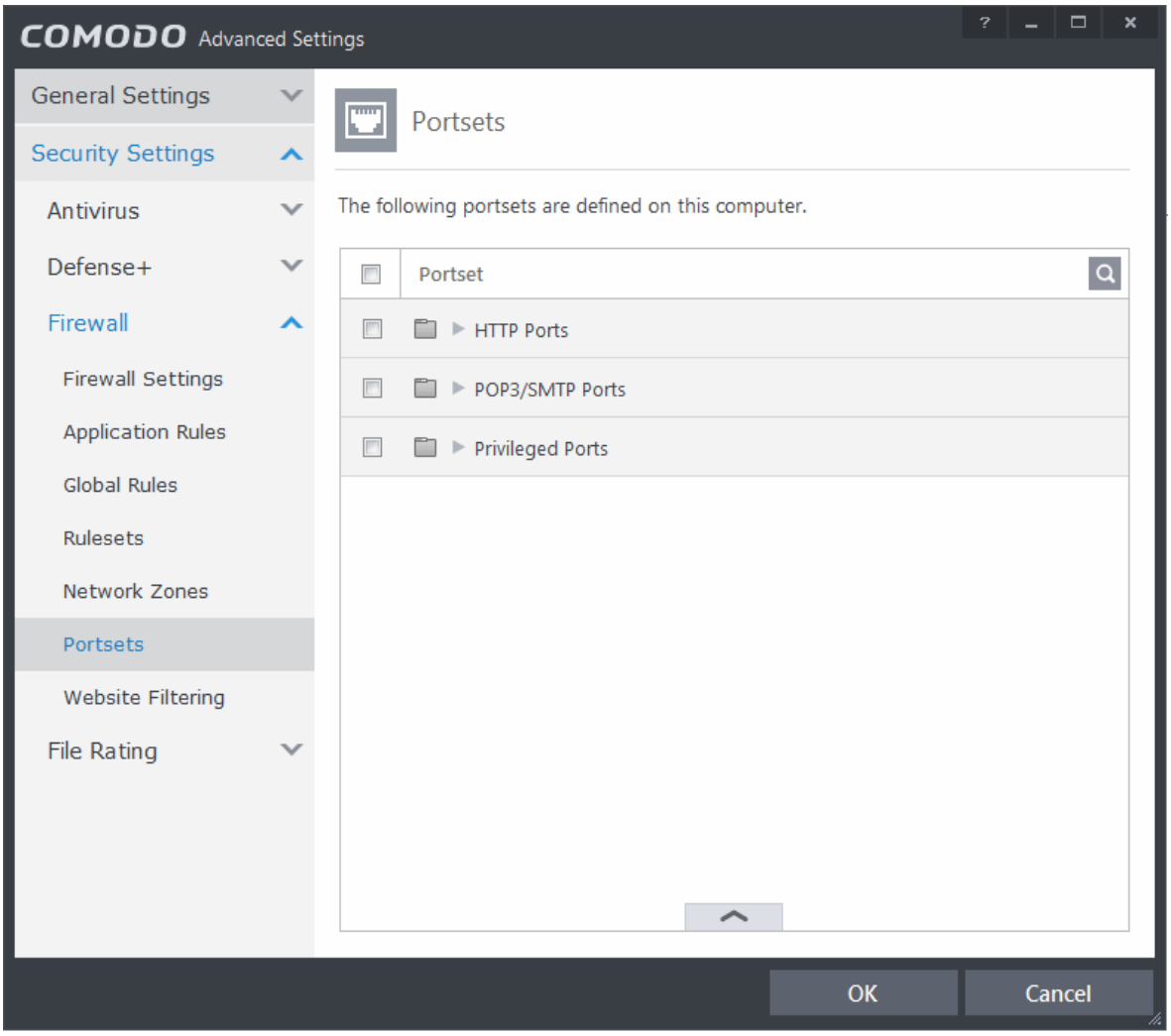
   The address(es) you blocked will appear under the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.

3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

6.2.3.6. Port Sets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple **Application Rules** and **Global Rules**.

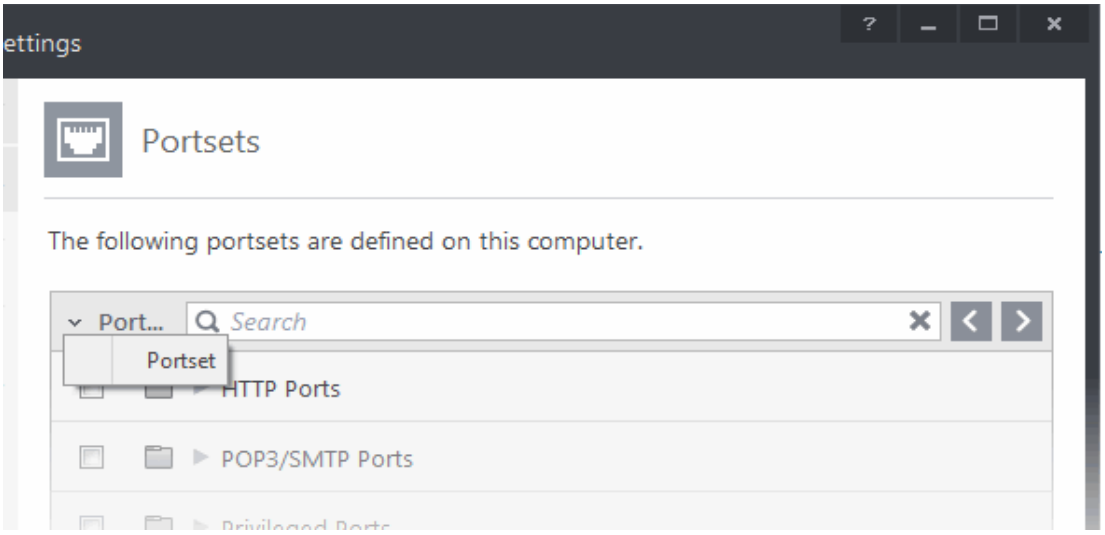
- The Port Sets panel enables you to view and manage pre-defined port sets and t add new port sets
- The Port Sets panel can be accessed by clicking Security Settings > Firewall > Portsets from the Advanced Tasks interface



The Port Sets are displayed as a tree structure. Clicking the + button beside the port set name expand the list of ports defined in it. The default port sets shipped with Comodo Internet Security are:

- **HTTP Ports**: 80, 443 and 8080. These are the default ports for http traffic. Your Internet browser uses this ports to connect to the Internet and other networks.
- **POP3/SMTP Ports**: 110, 25, 143, 995, 465 and 587. These are the ports that are typically used by mail clients like Outlook Express and WinMail for communication using the POP3, SMTP and IMAP protocols.
- **Privileged Ports:** 0-1023**.** This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports.

You can use the search option to find a specific port set in the list by clicking the search icon at the far right in the column header.



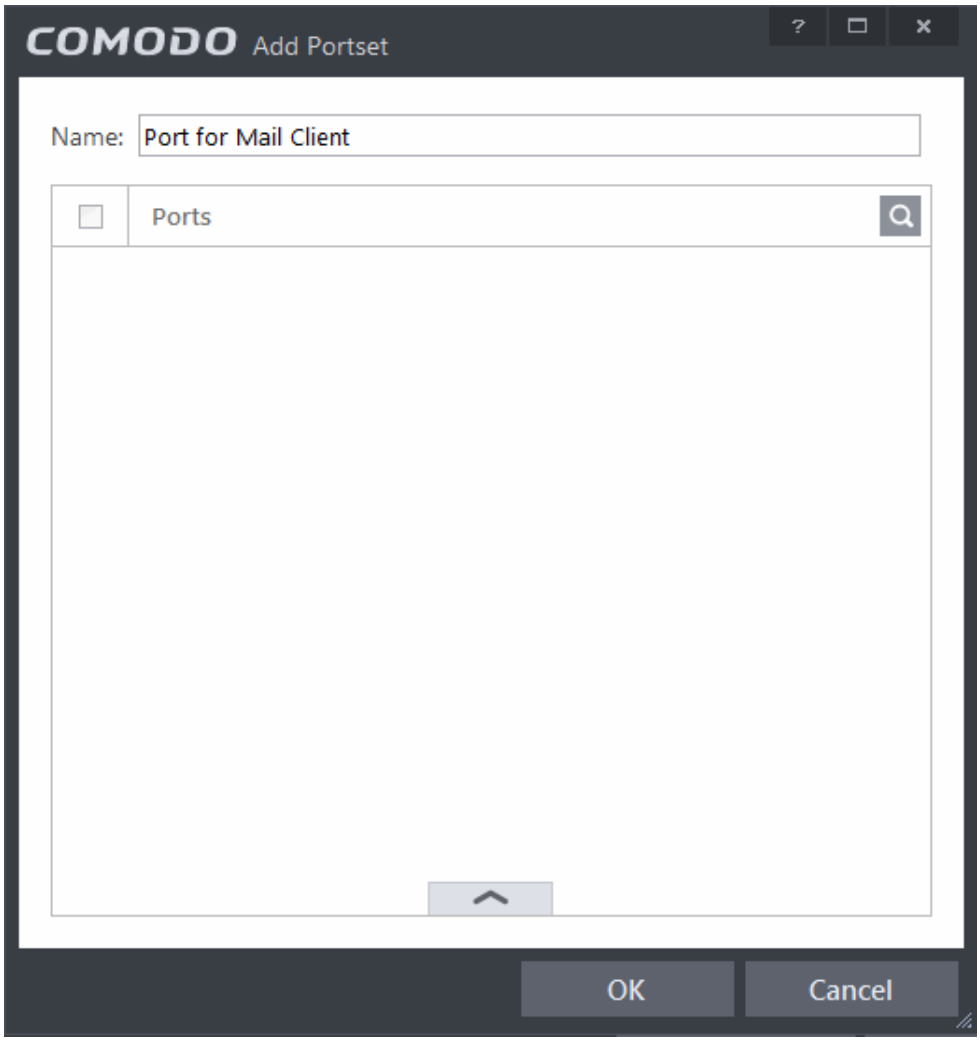
- Enter the name of the port set to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Defining a new Port Set

You can create new portsets and allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.

To add a new portset

1. Click the handle from the bottom center of the Portsets interface and select 'Add' from the options. The 'Add Portset' dialog will open.



2. Enter a name for the new portset in the Name field.
3. To add ports to the new portset, click the handle from the bottom center and choose 'Add' from the options.

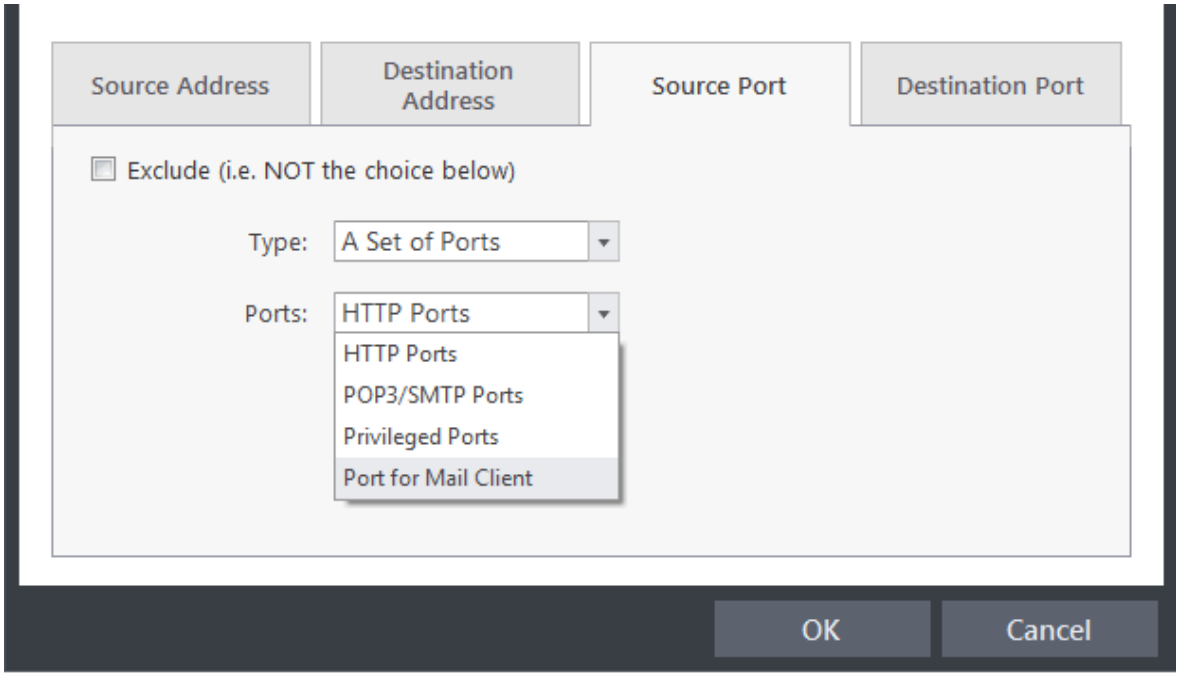
4. Specify the ports to be included in the new portset:
   - **Any -** to choose all ports;
   - **A single port -** Define the port number in the combo box beside;
   - **A port range** - Enter the start and end port numbers in the respective combo boxes.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

5. Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Edit Portset' interface.
6. Click 'OK' in the 'Edit Portsets' interface to create the new portset.

Once created, a Portset can be:

- Quickly called as 'A Set of Ports' when **creating or modifying a Firewall Ruleset**



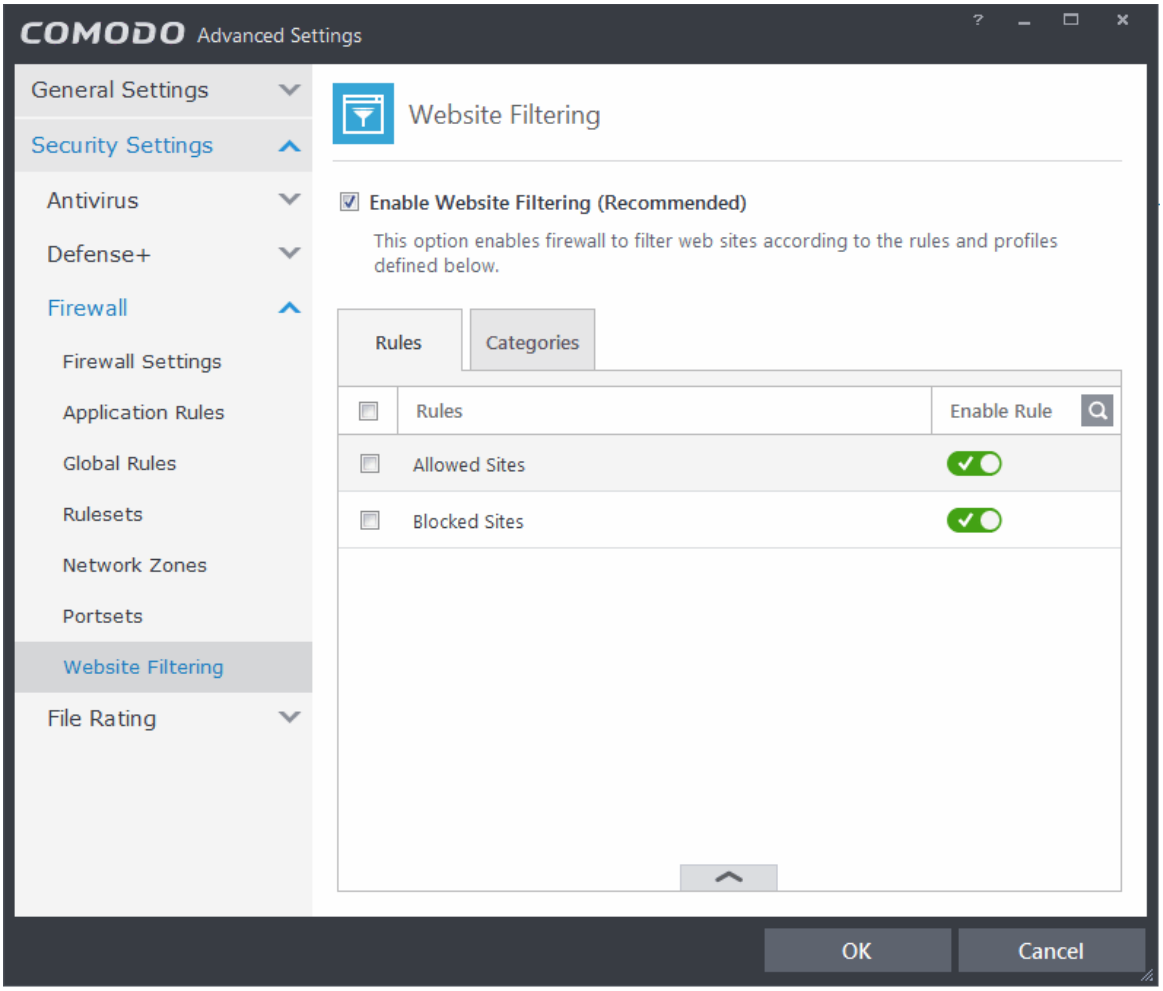
To edit an existing port set

- Select the portset from the 'Portsets' interface, click the handle from the bottom center and select the 'Edit' from the options to bring up the 'Edit Portset' dialog.
- The editing procedure is similar to **adding the portset** explained above.

6.2.3.7. Website Filtering

The Website filtering section allows you to set up rules to allow or block access to specific websites. Rules can be created for particular users of your computer, which makes this feature very useful for both home and work environments. For example, parents can block juvenile users from visiting inappropriate websites while companies can prevent employees from visiting social networking sites during working hours. You also have the option to create a log event whenever a user tries to visit a website which is in conflict with a rule.

The Website Filtering panel can be accessed by clicking Security Settings > Firewall > Website Filtering tab from 'Advanced Settings' interface.



Brief overview:

- Rules are constructed from one or more 'categories'.
- A category is a collection of one or more 'Websites'
- A 'Website' can be specified with its full URL or part of URL with wildcard character (*)
- You must set a rule to be 'Allow', 'Block' or 'Ask' and must specify to which users it should apply.

CIS ships with four preset categories of Websites which can be added to rules that you create. Three of these are non-modifiable lists which are managed by Comodo. These are 'Comodo Safe category', 'Comodo Phishing category' and 'Comodo Malware category'. The fourth preset, 'Exclusions', is empty by default but allows you to specify websites that should be allowed. You should add URLs to the 'Exclusions' category over time if you find you require access to a website which is blocked by a category.

CIS also ships with two predefined rules, 'Allowed Sites' and 'Blocked sites', both of which are modifiable. If switched on, the 'Blocked sites' rule will proactively block access to websites in the 'Comodo defined Malware sites' and 'Comodo defined Phishing Sites' categories. If you wish, you can add other categories to this rule to expand its coverage. The 'Allowed Sites' rule will permit access to websites in the Comodo 'Safe Sites' category and 'Exclusions' categories.

To set up a new rule of your own, click the 'Rules' tab, click 'Add', name your rule, add categories to the rule, specify to which users it should apply and whether it should be 'Allow', 'Block' or 'Ask'.

The 'Website Filtering' panel has two tabs:

- **Rules** - Allows you to define Website Filtering Rules and assign to required users. Refer to the section '**Creating or Modifying Website Filtering Rules**' for more details.
- **Categories** - Allows you to define categories of Websites to be allowed or blocked in Website filtering rules. Refer to the section '**Defining or Modifying Website Categories**' for more details.

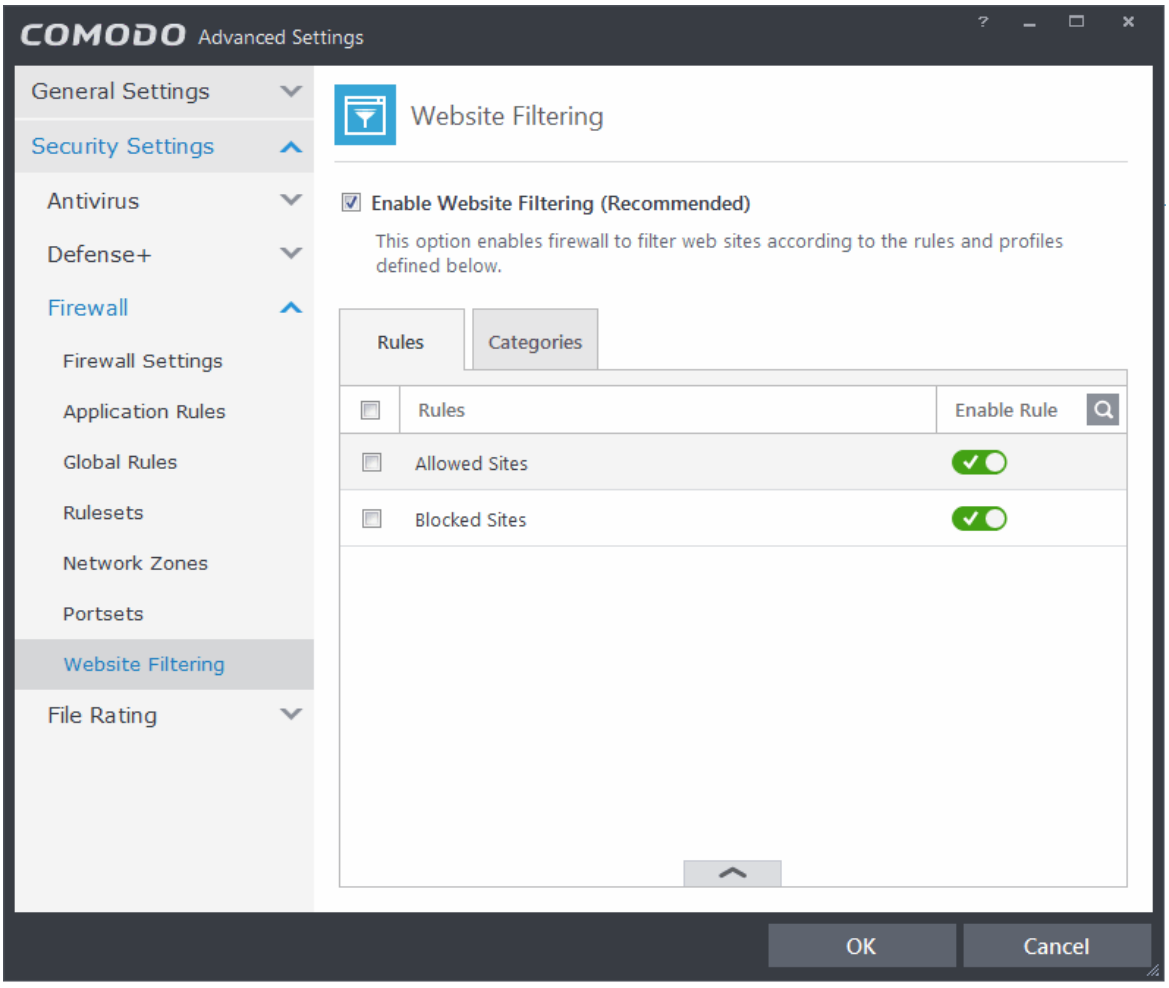
General Advice:

- It is the 'Categories' section where you specify the website(s) you wish to block or allow, not the 'Rules' section. A rule is mainly for specifying the user(s) for whom a category of URLs should be filtered and whether those categories should be allowed or blocked.
- When creating a new rule, you will be required to specify which categories should be included. You can elect to use just the pre-defined Comodo categories but, if you wish to filter specific websites, you will need to create your own category.
- For example, if you wanted to create a category to block youtube.com and certain other leisure websites, you would *click 'Categories' > 'Add Category' > Type name for category > Select your new category in list > 'Add Website' > Type www.youtube.com. Click 'Add Website' again to add more sites.* You will now be able to select this category when creating a rule for a user(s).
- Refer to the section '**Defining or Modifying Website Categories**' for more details on specifying Website categories.

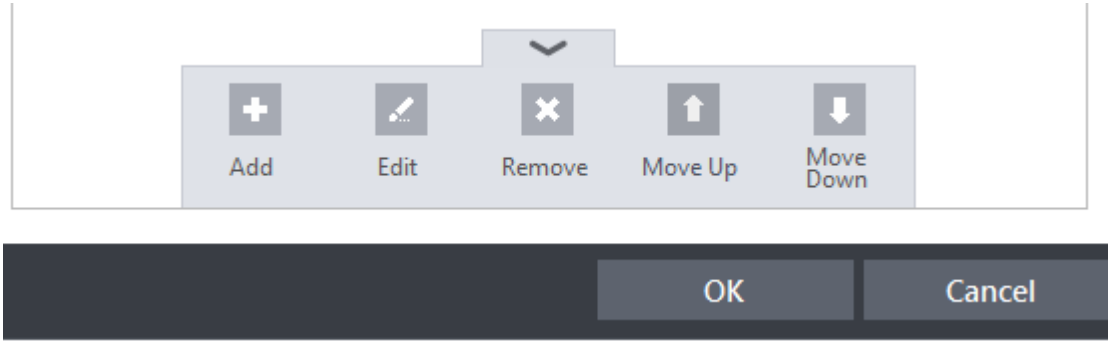
6.2.3.7.1. Creating and Modifying Website Filtering Rules

The 'Rules' tab allows you to create, view, edit and specify exclusions to your website filtering rules. The powerful rule-configuration interface lets you create rules which are as sweeping or as granular as you require. Rules can be created on a per-user basis, allowing you to control exactly which websites certain people can or cannot visit. You can also disable or enable a rule as required at any time.

Comodo Firewall implements rules for the currently logged-in user based on the order they are in this list. Should a conflict exist between individual rules, then the rules at the top takes priority. Click the handle and use the 'Move Up' or 'Move Down' buttons to change a rule's priority.



- The switches in the 'Enable Rule' column enable you to quickly turn a rule on or off
- The check-boxes next to a rule name allow you to select it for editing, removing or re-prioritizing using the controls at the bottom of the interface:



You can search for a specific rule by clicking the search icon at the far right in the column header.

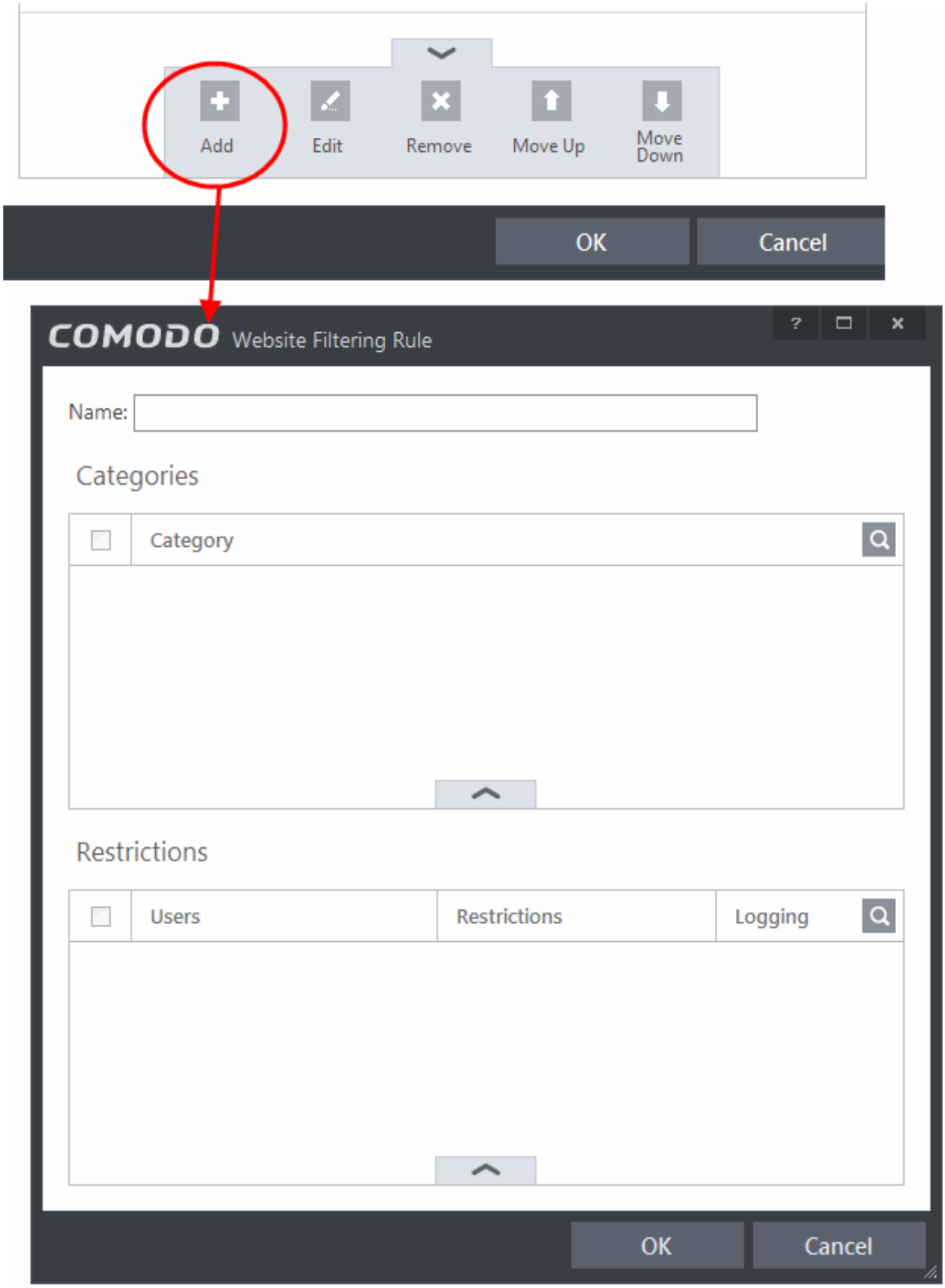
- Enter full or part of the name of the rule in the search field.
- Click the right or left arrow at the far right to begin the search.
- Click the icon in the search field to close the search option.

The Rules interface allows you to:

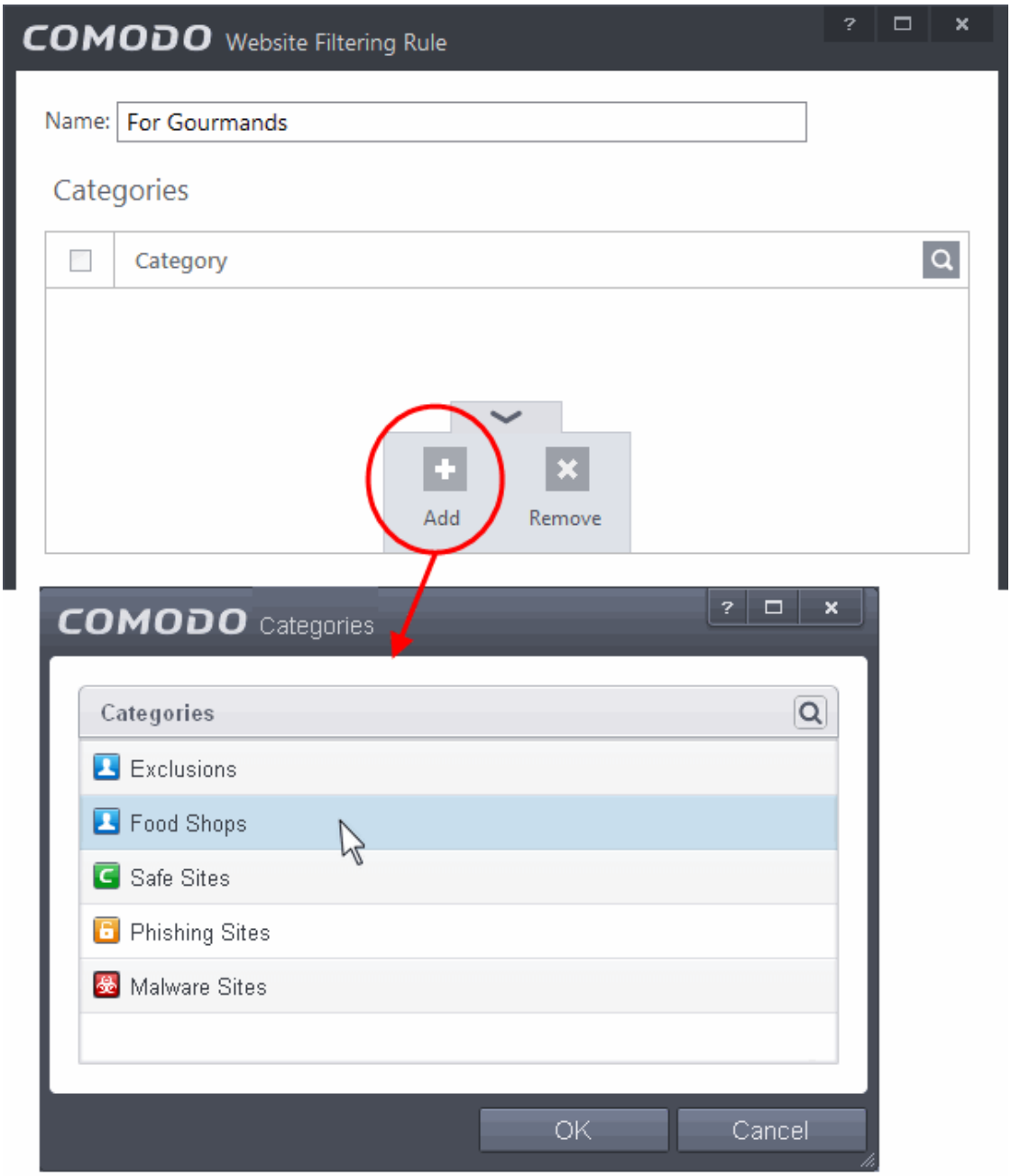
- **Create new Website filtering Rules**
- **Edit existing rules**
- **Change priority of the rules**
- **Remove unwanted rules**

To create a new Website Filtering rule

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the handle at the bottom of the Rules interface and select 'Add'.



3. Enter a name for your new filter.
4. Select the categories that should be added to the filter:
    - Click the handle at the bottom of the 'Category' pane and choose 'Add'.



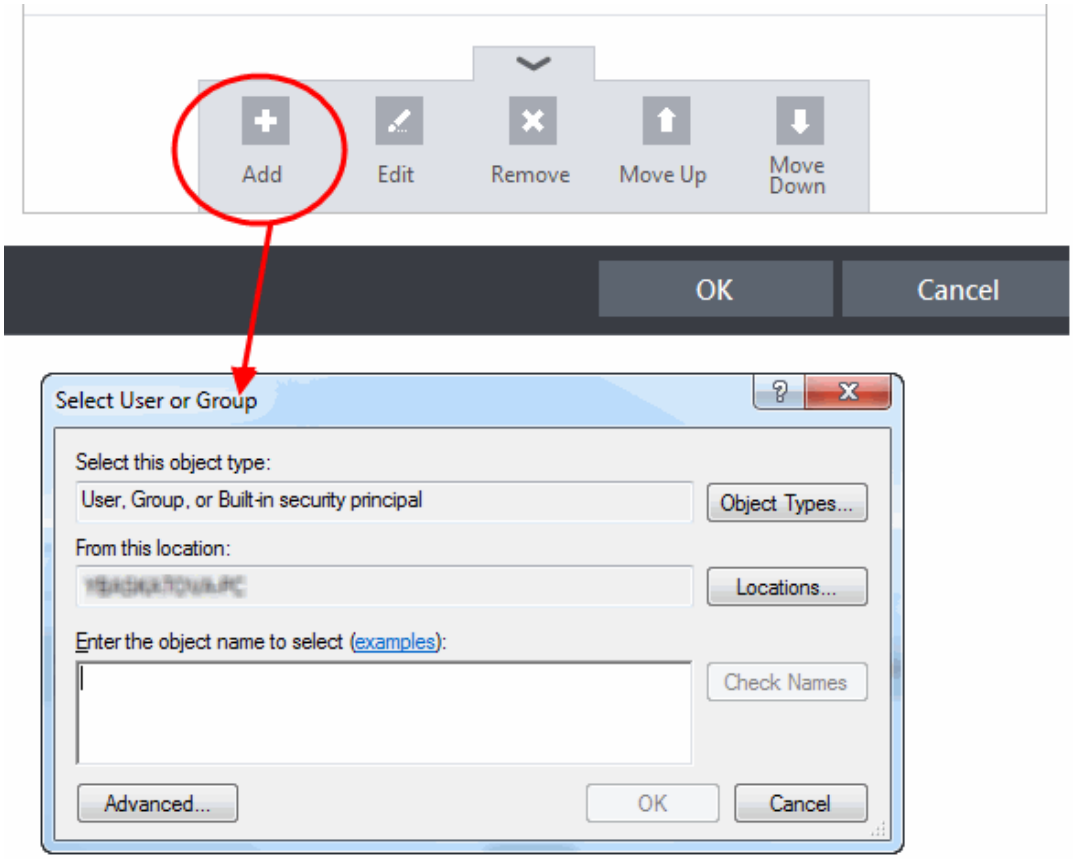
Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

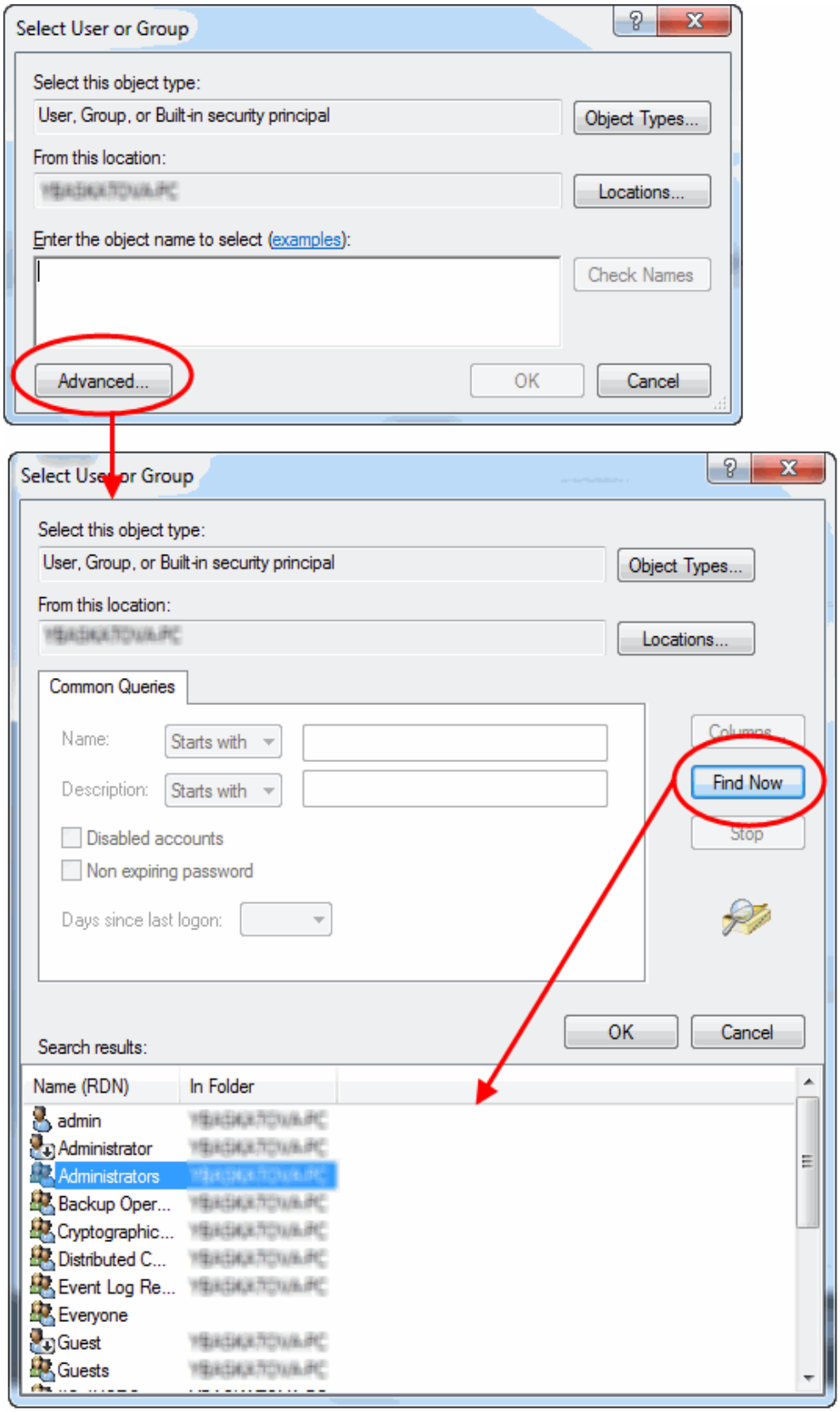
- **Comodo Safe Sites** - Websites that are considered safe according to global whitelist
- **Comodo Phishing Sites** - Websites that lead to phishing websites, as per dynamically updated Comodo Blacklist
- **Comodo Malware Sites** - Websites that may inject malware into your system, as per dynamically updated Comodo Blacklist

For more details on creating and modifying user specified categories, Refer to the section **Defining or Modifying Website Categories**

5. Add Users or User Groups to whom the rule should be applied:
   - Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:



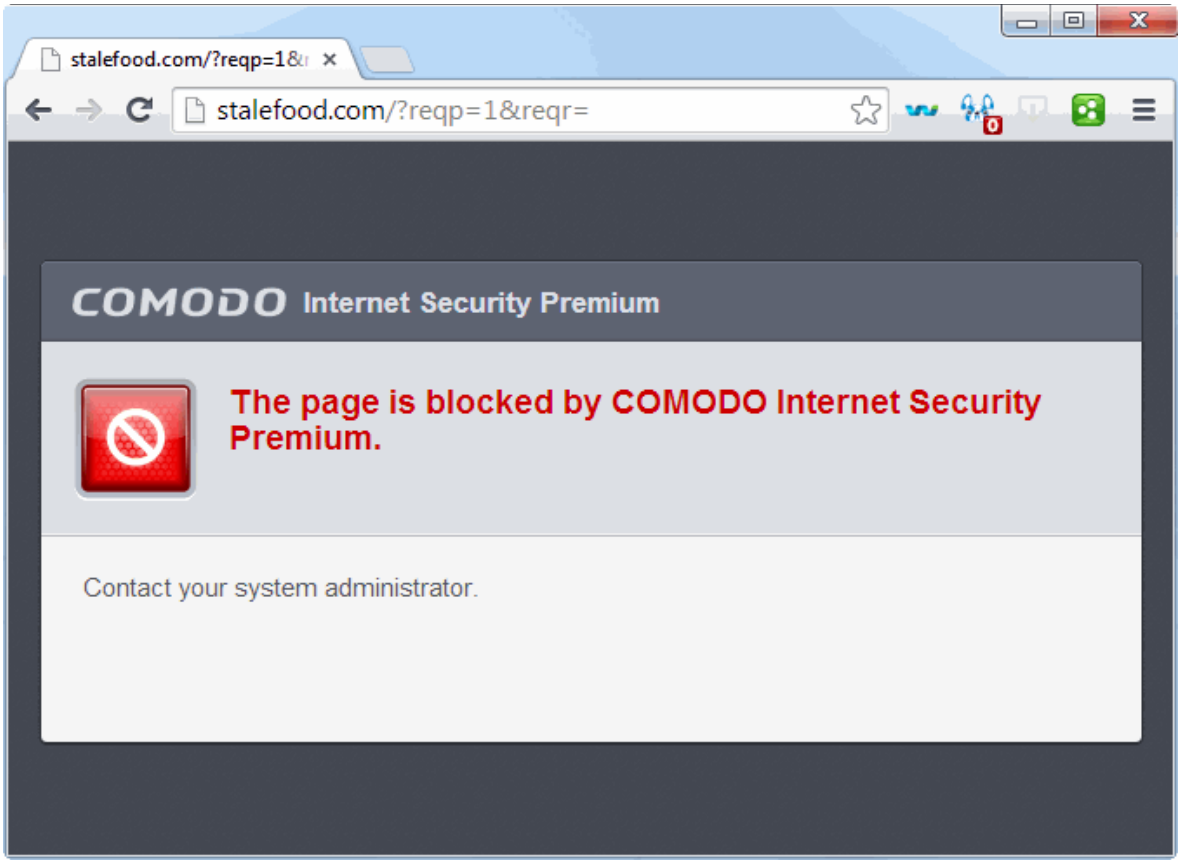
- Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format <domain name>\<user/group name> or <user/group name>@<domain name>. Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



After adding target users or groups, you next need to specify whether those users should be allowed or blocked from viewing the websites in the category or they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:

- **Allow** - The websites in the categories can be accessed by the user.
- **Block** - The websites in the categories cannot be accessed by the user.
- **Ask** - An alert will be displayed in the browser (shown below) if the user tries to access any of the websites

in the category. The user can decide whether or not to continue.



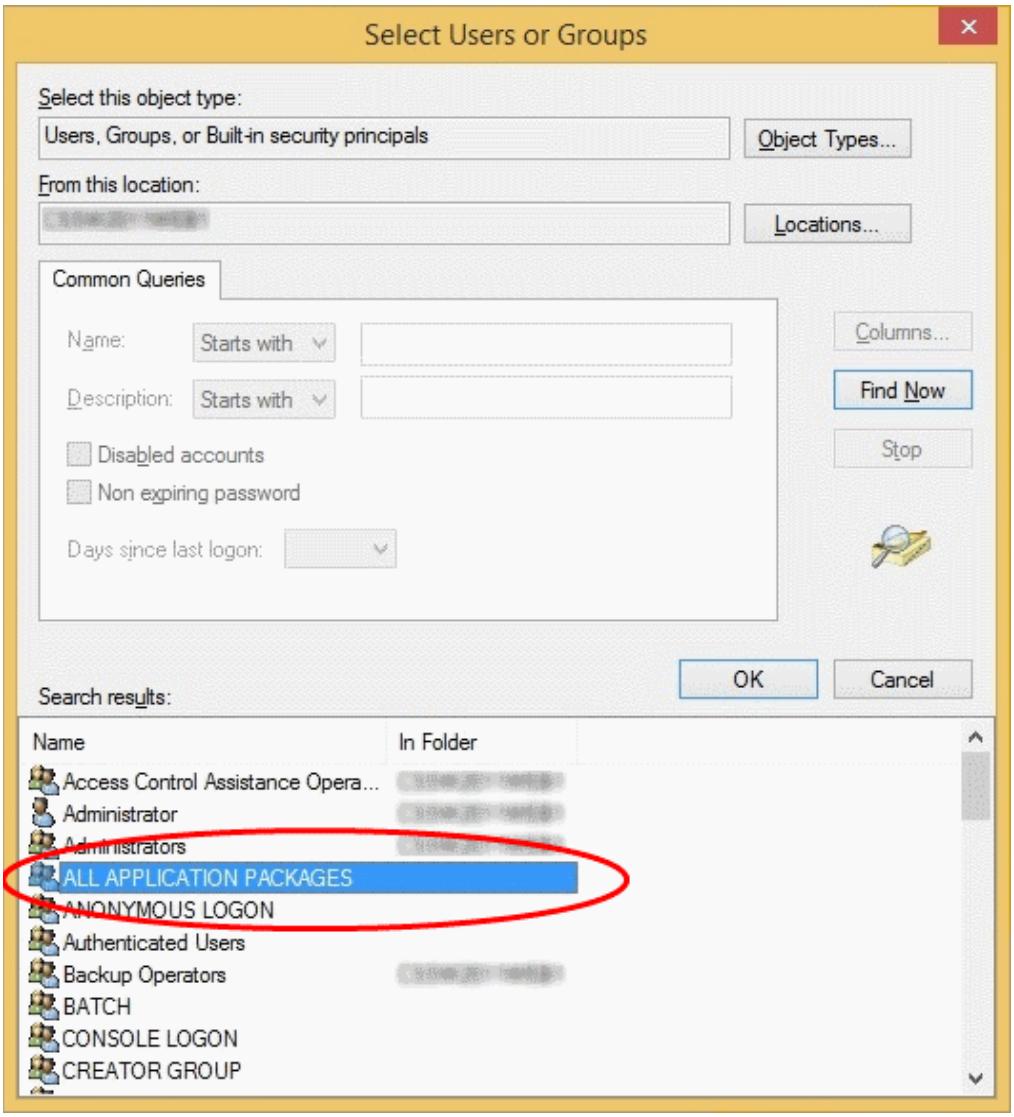
6. Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.
7. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
8. Make sure that the rule is enabled using the toggle switch under the Enable Rule column 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.

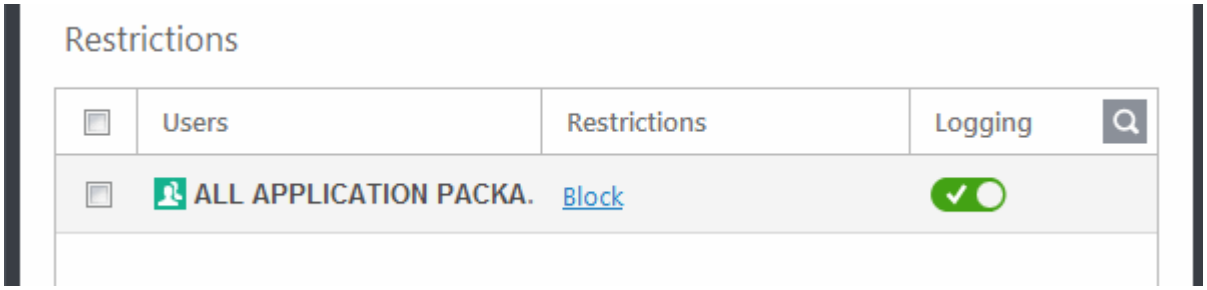
If you or other users access websites using Internet Explorer 11 on Windows 8/8.1, then you must add this user group or your rules will have no effect. For example, users will still be able to access blocked websites.

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



To edit existing rules

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule to be edited under the 'Rules' tab by selecting the checkbox beside the rule.
3. Click the handle from the bottom center of the Rules interface and choose 'Edit' from the options.

The ' Website Filtering Rule' interface for the selected rule will open. You can add/remove categories, add/remove users or change the restriction for selected users from this interface. Refer to **To create a new Website Filtering Rule** for more details

on this interface.

To remove a Website Filtering Rule

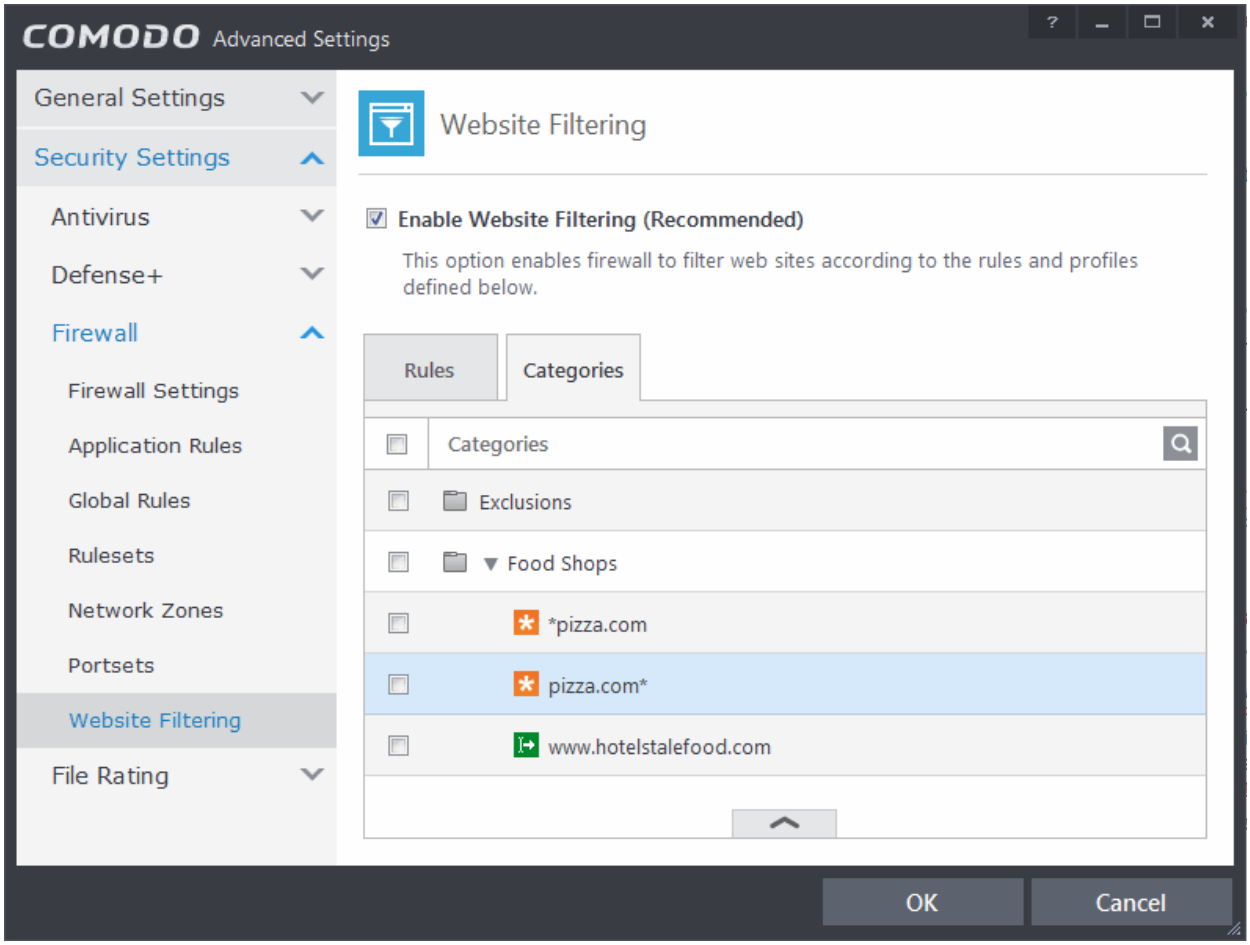
1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule(s) to be removed under the 'Rules' tab by selecting the checkbox(es) beside them.
3. Click the handle from the bottom center of the Rules interface and choose 'Remove' from the options.

To change the priority of Website Filtering Rules

1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule to be moved under the 'Rules' tab by selecting the checkbox beside the rule.
3. Click the handle from the bottom center of the Rules interface and choose 'Move Up' or 'Move Down' option to change the order of the rules in the interface.

6.2.3.7.2. Defining or Modifying Website Categories

The 'Categories' pane displays a list of user-defined categories that can be added to rules. A category can be a list of one or more URLs and/or part of URL with wildcard character. You can search for a specific category by clicking the search icon at the far right in the column header.

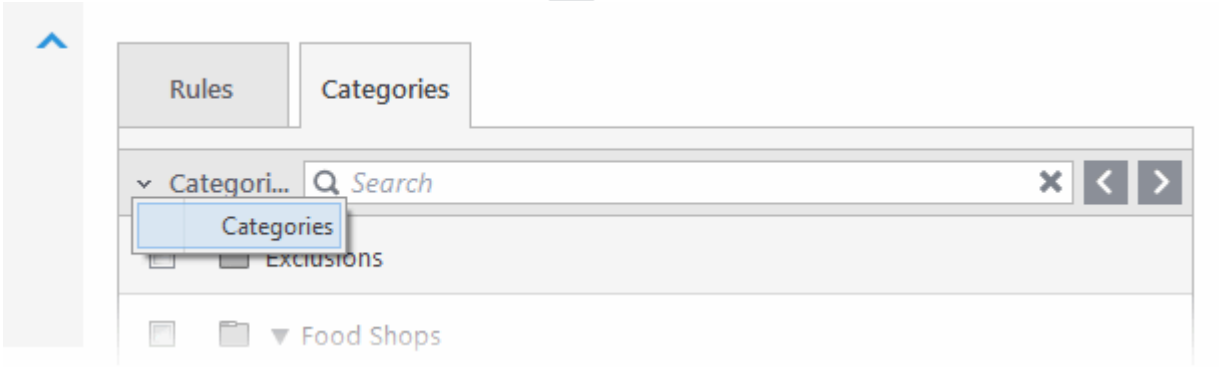


The 'Categories' pane allows you to:

- **Add a new category of Websites**
- **Rename a Category**
- **Remove unwanted Websites from a category**

- **Remove a Category**

To search for a specific category, click the search icon at the far right in the column header.



- Enter full or part of the name of the category in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

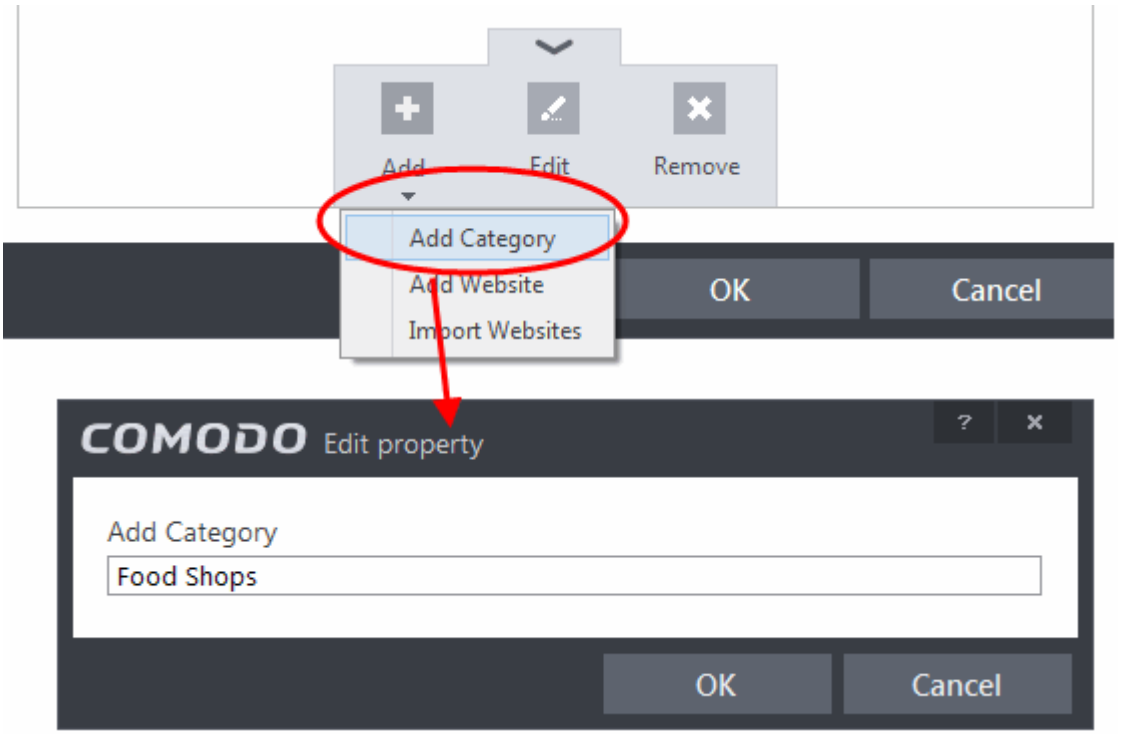
Adding a New Category of Websites

Adding a new category involves two steps:

- Step 1 - Define a name for the category
- Step 2 - Add Websites to be included to the category

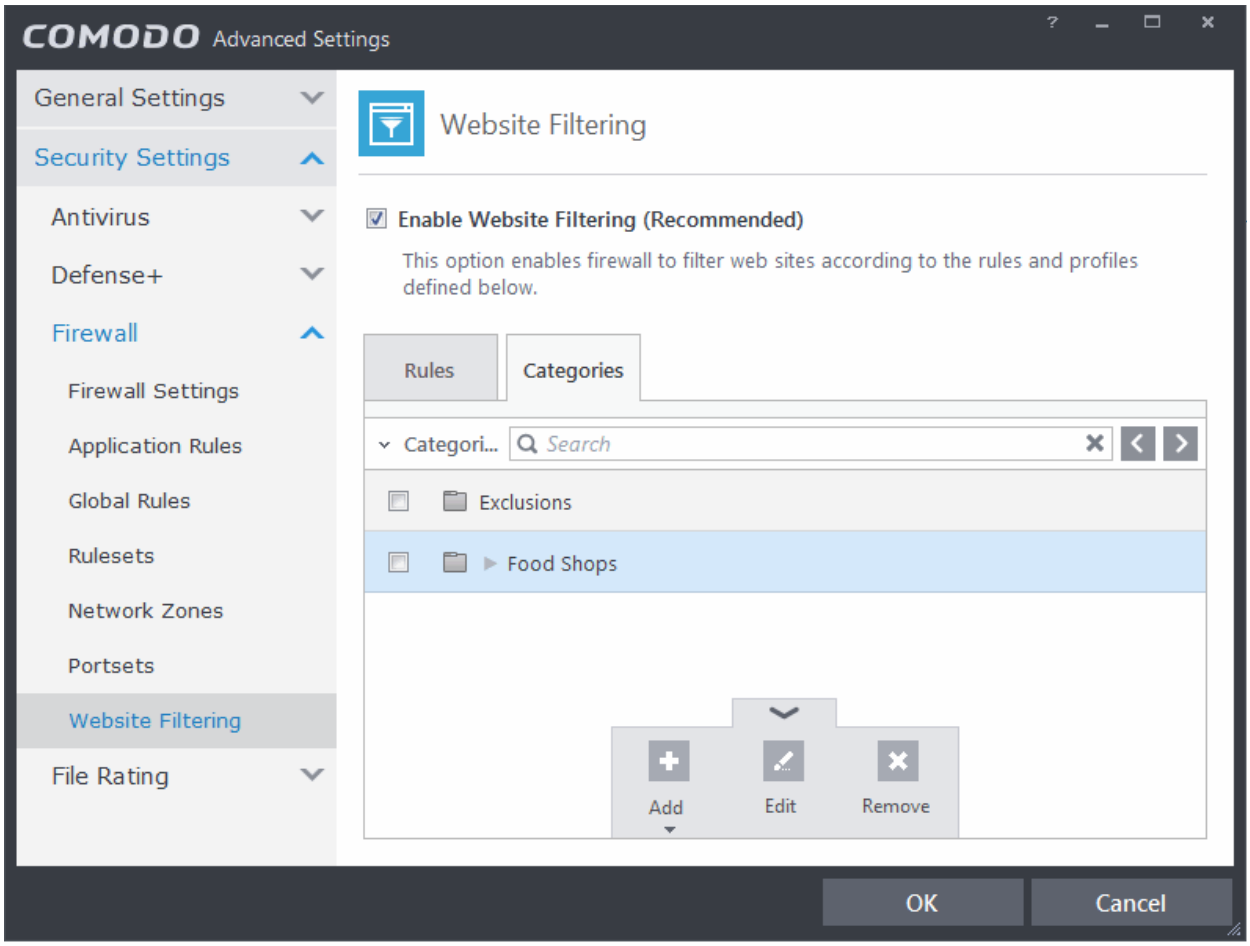
Step 1 - Define a name for the category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Click the handle from the bottom center of the 'Categories' pane, click 'Add' from the options and choose 'Add Category' from the drop-down. The 'Edit Property' dialog will open.



4. Enter a name for the category and click OK

The new category will be created and added under the 'Categories' tab.



You can add URLs of websites to be included in the category.

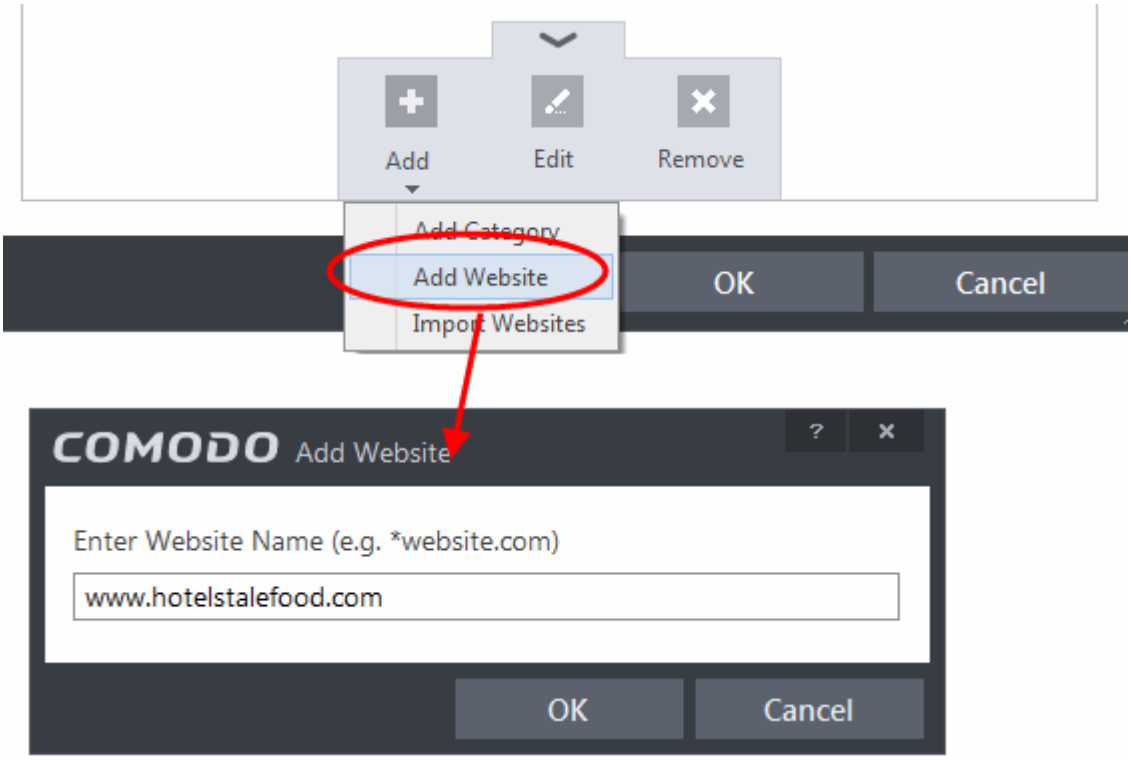
Step 2 - Add URLs to be included to the category

You can add websites to a category in two ways:

- **Manually Specify Websites**
- **Upload Website URLs from a text file**

To manually specify websites

1. Select the Category under the 'Categories' tab.
2. Click the handle at the bottom of the 'Categories' pane, click 'Add' then choose 'Add Website' from the drop-down menu. The 'Add Website' dialog will open:

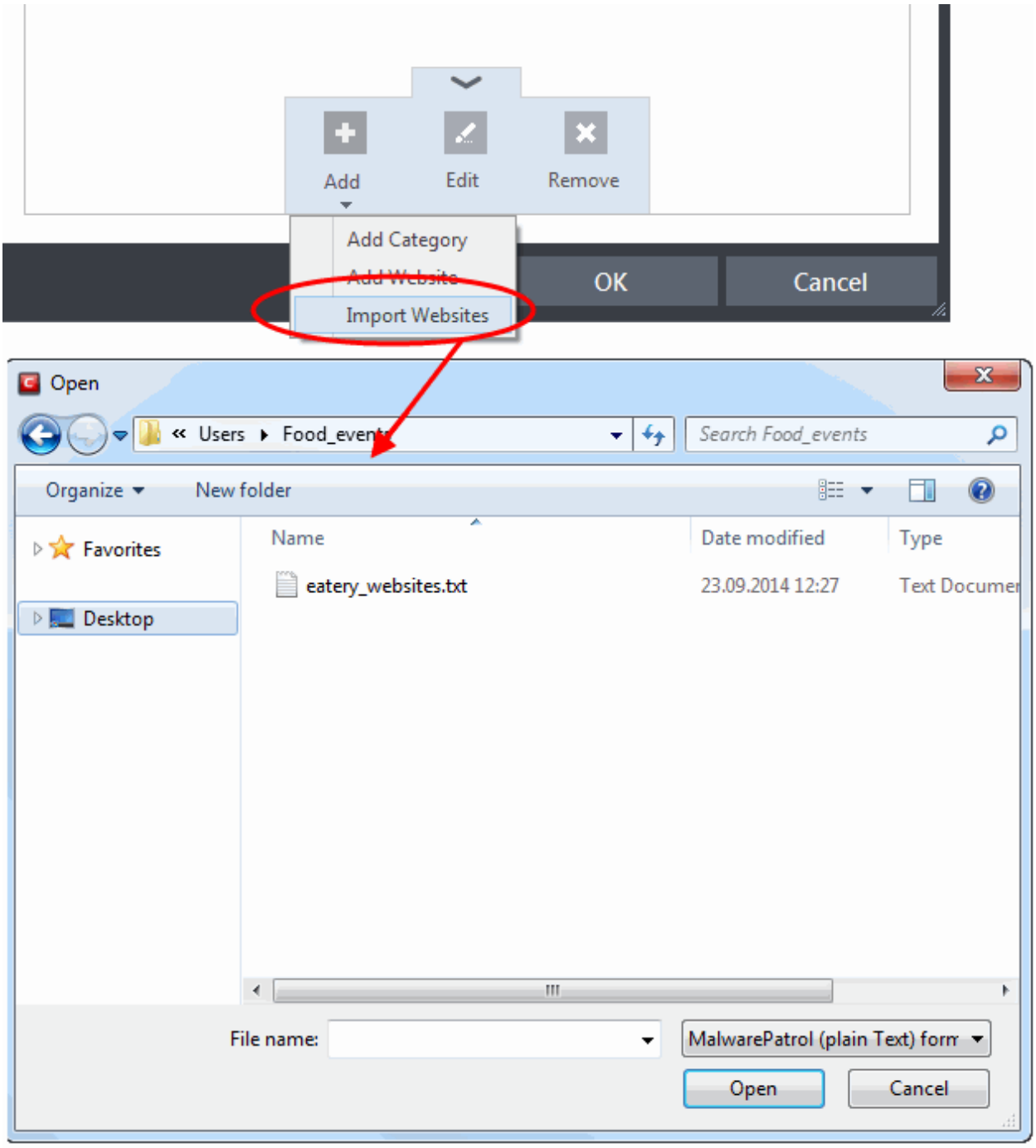


3. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
    - To add a specific website/webpage, enter the full URL of the website/webpage
    - To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
    - To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.
    - To include all the websites with URLs that contain a specific string, add the wildcard character befor and after the string. For example, "*pizza*" will cover hotpizza.com, spicypizza.com and so on.

    The website will be added to the category.
4. Repeat the process to add more websites.

To upload a list of websites from a text file

1. Select the target category from the 'Categories' tab.
2. Click the handle at the bottom of the 'Categories' pane then click 'Add' and choose 'Import'
3. Navigate to the file containing your list of URLs.



Note: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.

4. Click 'Open'.

CIS will automatically add the websites specified in the text file into the selected category.

To rename a category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Select the category to be renamed.

4. Click the handle from the bottom center of the 'Categories' pane and choose 'Edit' from the options. The 'Edit Property' dialog will open.
5. Enter the new name for the category and click OK

The category will be renamed immediately both under the Categories tab and in the Website Filtering Rules to which it is applied.

To remove a Website from a category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Click the + button beside the category to be edited to expand the website list
4. Select the Website(s) to be removed
5. Click the handle from the bottom center of the 'Categories' pane and choose 'Remove' from the options.

To remove a Category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Select the Category to be removed
4. Click the handle from the bottom center of the 'Categories' pane and choose 'Remove' from the options.

Note: You cannot remove a category which is currently applied in a Website Filtering Rule. Before removing a category, make sure you remove the category from the rules to which it is applied.

6.2.4. Manage File Rating

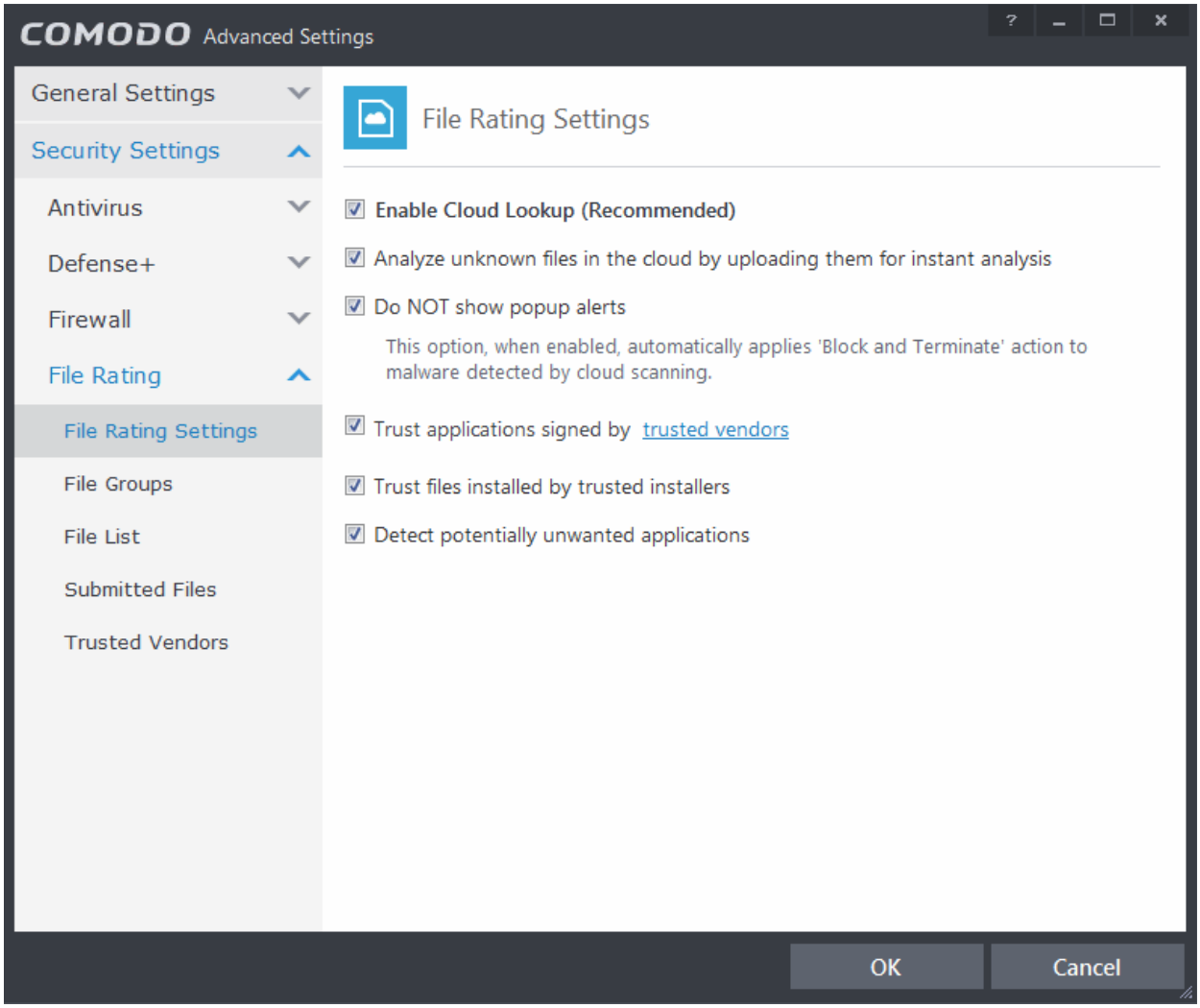
The CIS file rating system is a cloud-based file look-up service (FLS) that attempts to ascertain the reputation of files on your computer by consulting a global database. Whenever a file is first accessed, CIS will check the file against our master whitelist and blacklists and will award it trusted status if:

- The application/file is awarded 'Trusted' status in the **File List**
- The application is from a vendor included in the **Trusted Software Vendors** list;
- The application is included in the extensive and constantly updated Comodo safelist.

Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource consumption. On the other hand, files which are identified as definitely harmful will be awarded a status of 'Malicious' and quarantined or deleted automatically. Files which could not be recognized by the rating system are awarded 'Unrecognized' status'. You can review unrecognized files in the **File List** interface and manually trust/block/delete them. The interface also allows you to view more details on the file, to submit them to Comodo for further analysis or to run an on-demand file-lookup.

The 'Manage File Rating' area allows you to view and manage the list of Trusted Files and Unrecognized Files and also allows you to:

- Manually add files and executables to Trusted Files list.
- Submit unrecognized files for look-up and view the list of files you have submitted previously.
- View and manage the Trusted Software Vendor list.



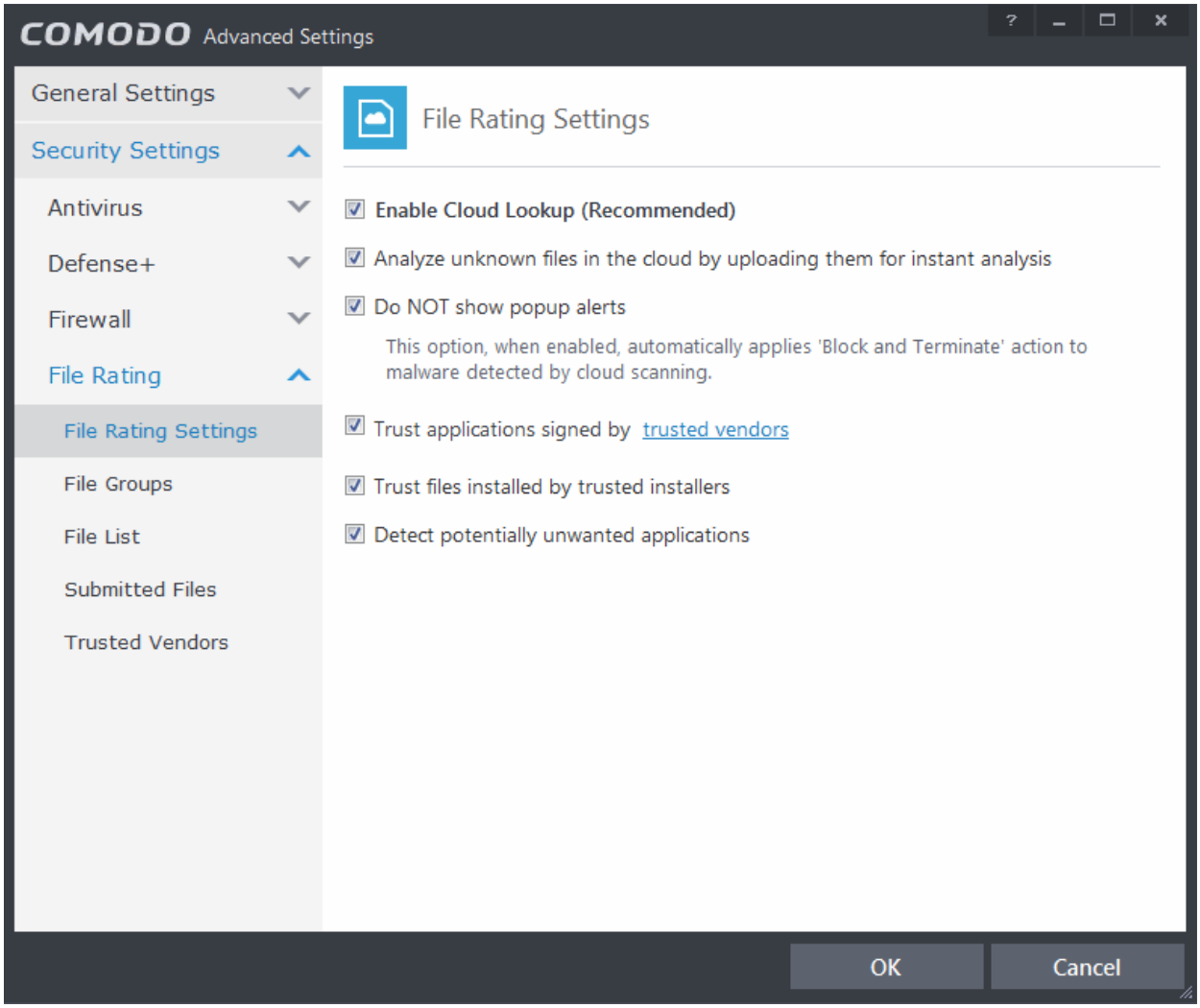
Click the following links to jump to the section you need help with:

- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **File Groups** - Create predefined groups of one or more file types.
- **File List** - View, manage and investigate executable files on your computer and their current trust rating.
- **Submitted Files** - View any files already submitted to Comodo for analysis.
- **Trusted Vendors** - View the list of trusted software vendors and manually add vendors.

6.2.4.1. File Rating Settings

The file ratings 'Settings' panel allows you to configure the overall behavior of the feature.

- The File Rating Settings panel can be accessed by clicking Security Settings > File Rating > File Rating Settings tab from 'Advanced Settings' interface



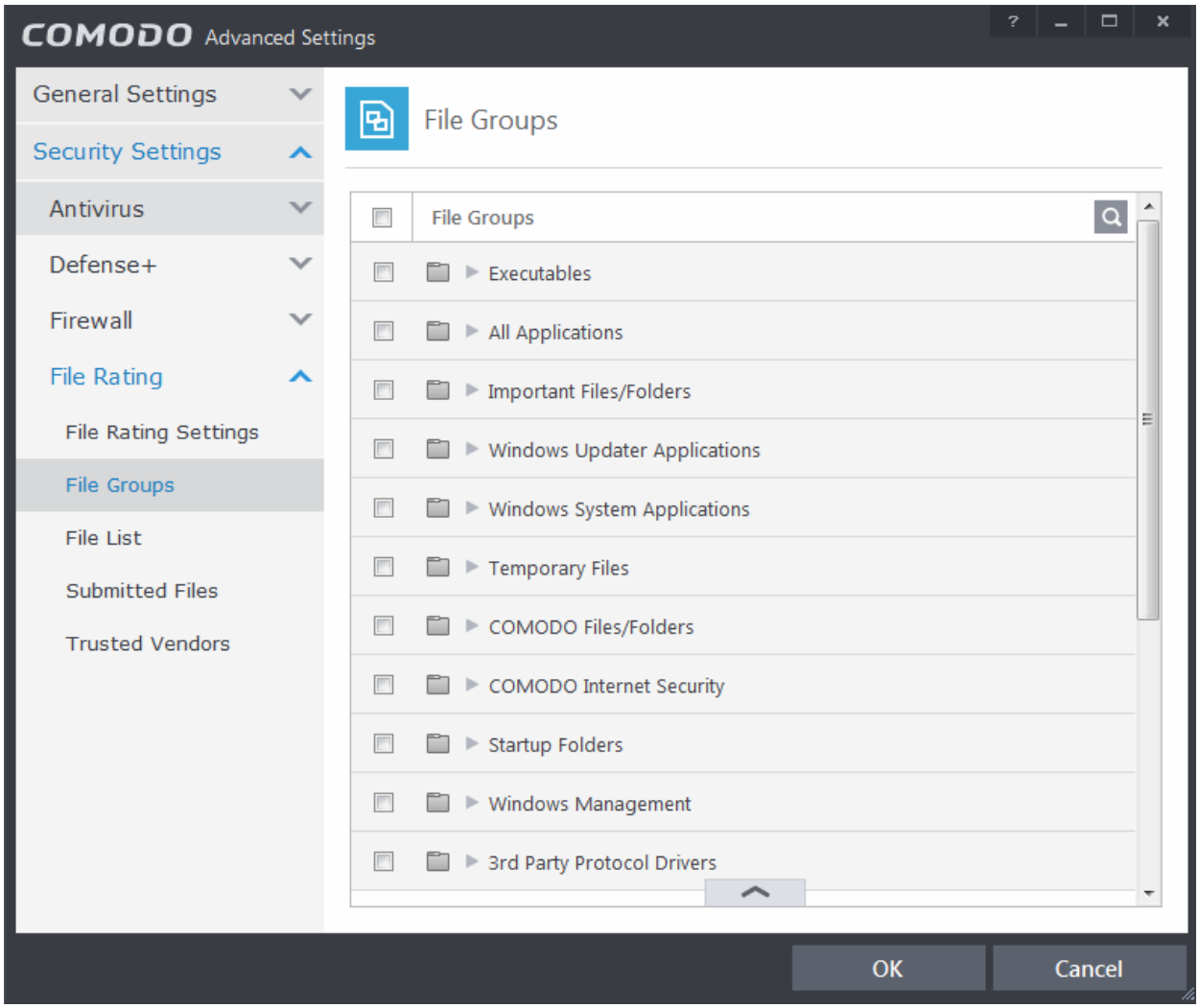
- **Enable Cloud Lookup** - Allows you to enable or disable File Rating.(***Default and recommended =Enabled***)
- **Analyze unknown files in the cloud by uploading them for instant analysis** - Instructs CIS to automatically submit to Comodo those files whose trustworthiness could not be assessed by cloud look-up. Comodo Technicians will analyze the file and add it to future blacklists if found to be malicious. (***Default =Enabled***)
- **DO NOT show popup alerts** - This option allows you to configure whether or not to show firewall alerts when malware is encountered. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show popup alerts then you have a choice of default responses that CIS should automatically take - either 'Block Requests' or 'Allow Requests'. ***(Default =Enabled)***
- **Trust applications signed by trusted vendors** - If enabled, CIS will award trusted status to executables and files that are code-signed by vendors in the Trusted Vendors list. Click the words 'trusted vendors' to open the **Trusted Vendors** panel. (***Default =Enabled***)
- **Trust files installed by trusted installers** - If enabled, CIS will trust executables and files whose parent applications are listed under the 'Installer or Updater' rule in **HIPS Rules**. (***Default =Enabled***)
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet ***(Default =Disabled).***

6.2.4.2. File Groups

File Groups are handy, predefined groupings of one or more file types which make it easy to add an entire class of file types to

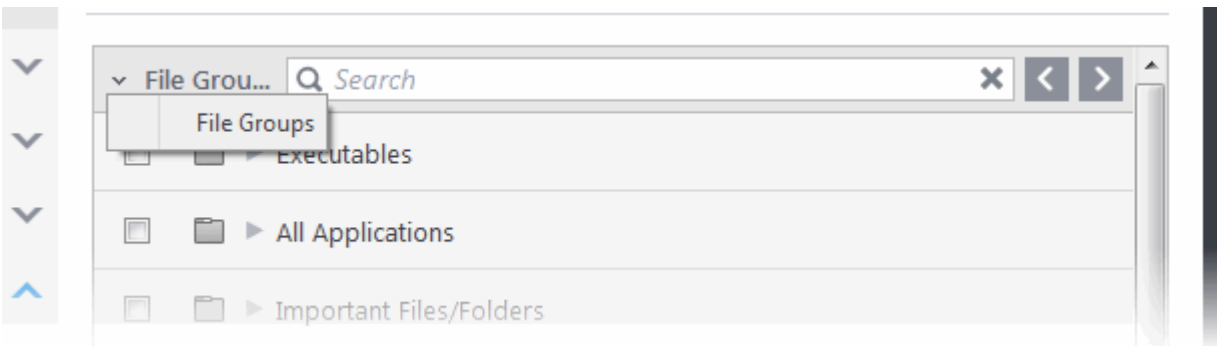
CIS Exclusions, HIPS Rules, Auto-Sandbox and so on. CIS ships with a set of predefined File Groups and, if required users, can add new File Groups and edit existing groups.

- The File Groups panel can be accessed by clicking Security Settings > File Rating > File Groups from the Advanced Tasks interface.



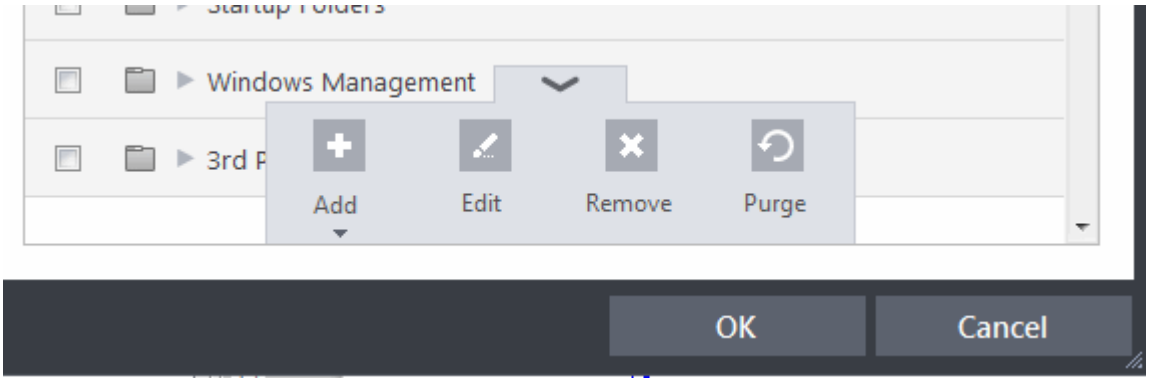
You can use the search option to find a specific name in the list.

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



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

Clicking the handle at the bottom of the interface opens an options panel:



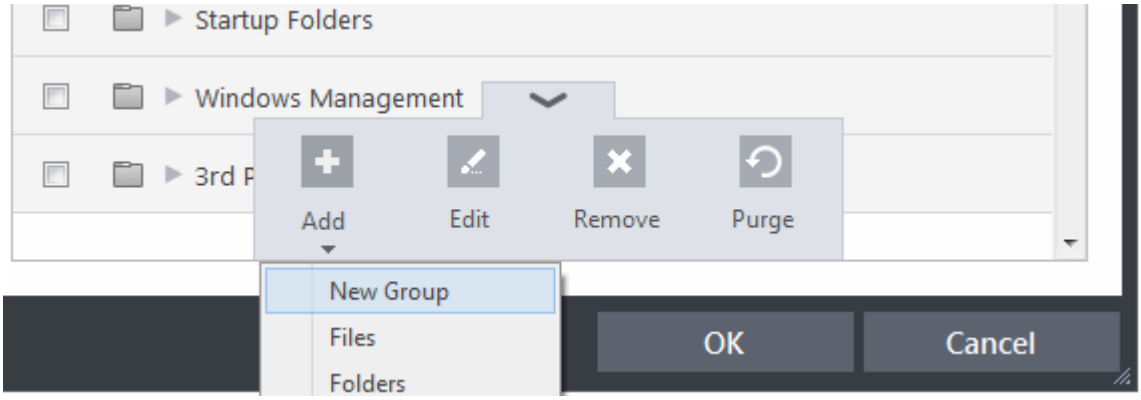
- **Add** - Allows you to add new groups, add individual files ,folders or running process to File Groups.
- **Edit** - Allows you to edit the name of file groups and edit file path of items under a file group.
- **Remove** - Allows you to delete a File Group or item(s) under a file group.
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

This interface allows you to

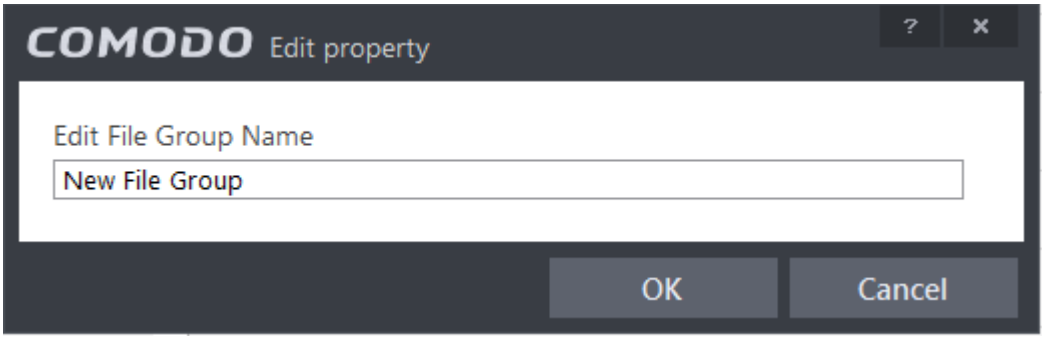
- **Create a new File Group**
- **Edit the names of an Existing File Group**
- **Add a file to an existing file group**
- **Remove existing file group(s) or individual file(s) from existing group**

Adding a File Group

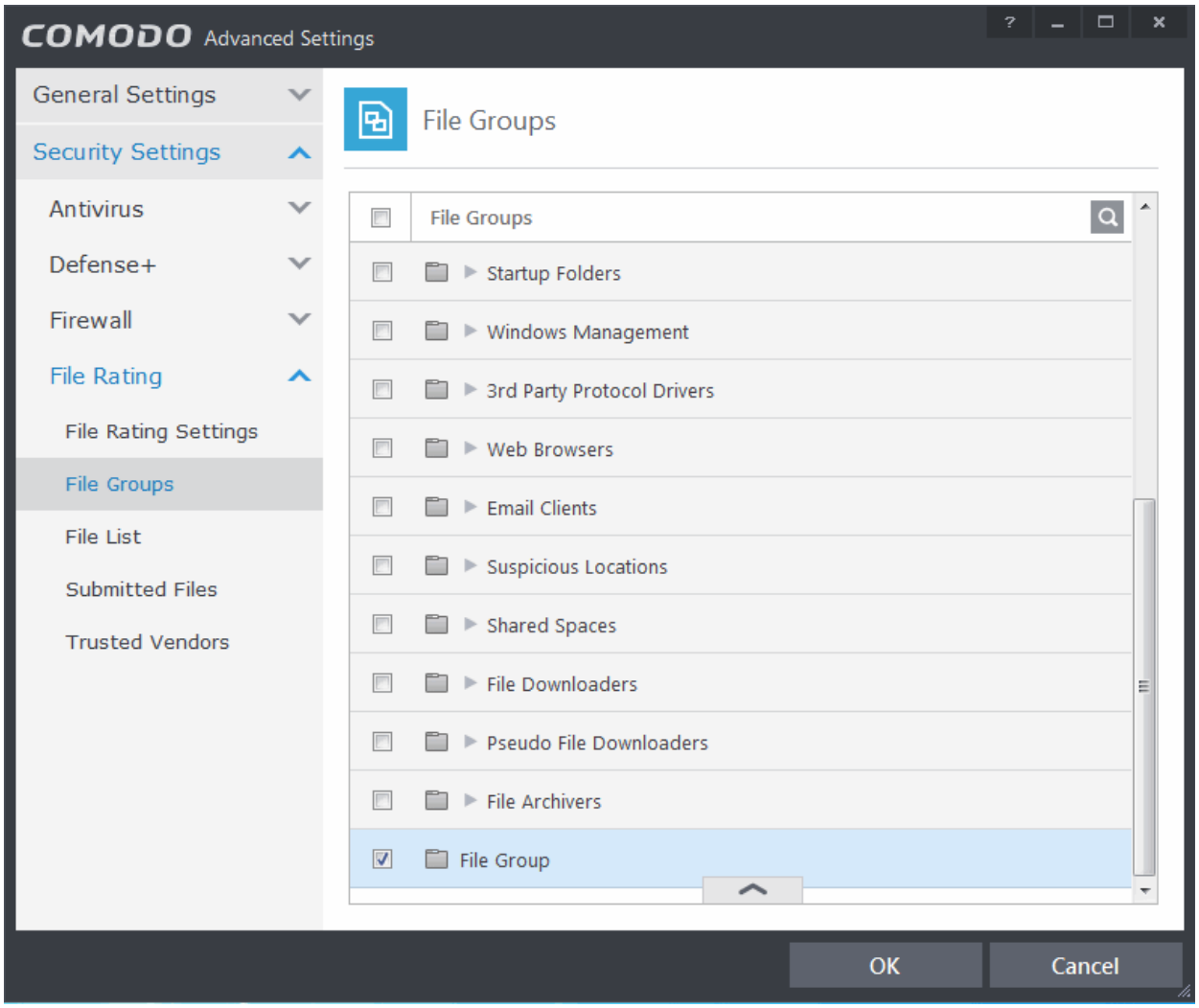
- To add a new File group or add files to an existing group, click the handle from the bottom and click 'Add'.



- Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK



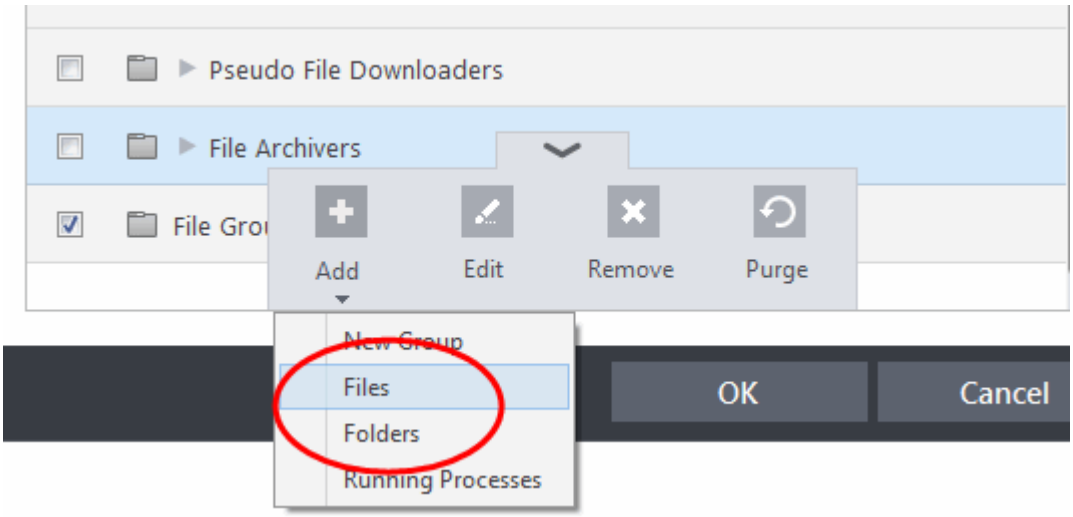
The File Group will be added and displayed in the list.



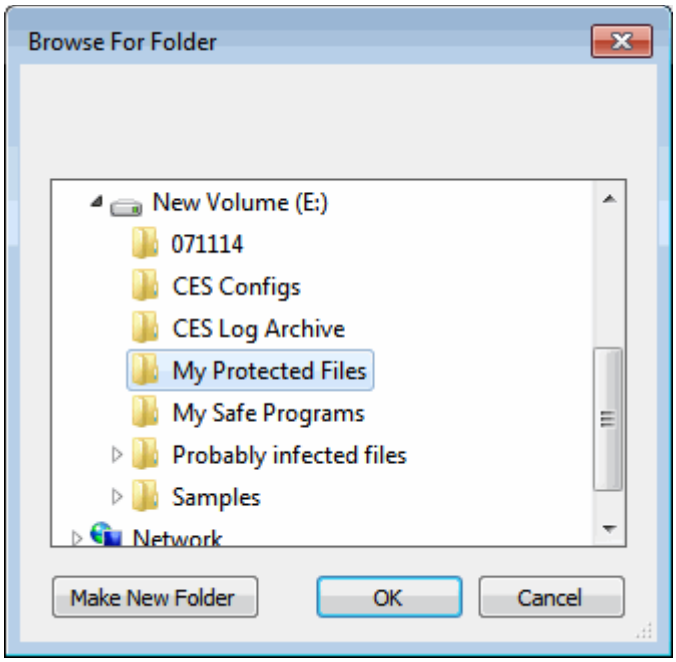
- To edit the name of an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog.

Add individual files or folder to a group

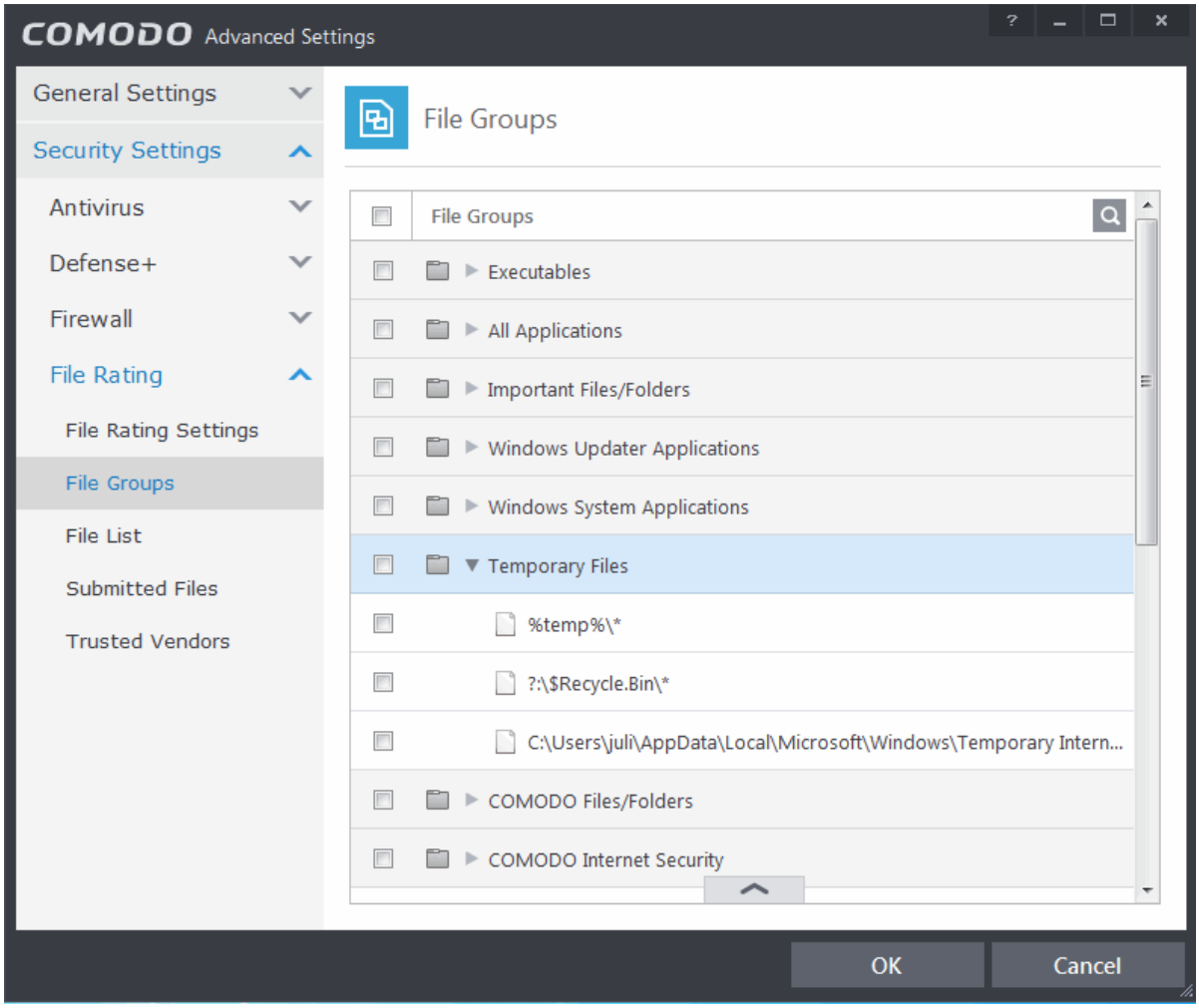
- Select the Group, click the handle and click Add. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes.
  - To add a file or folder, choose 'Files' or 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will open.



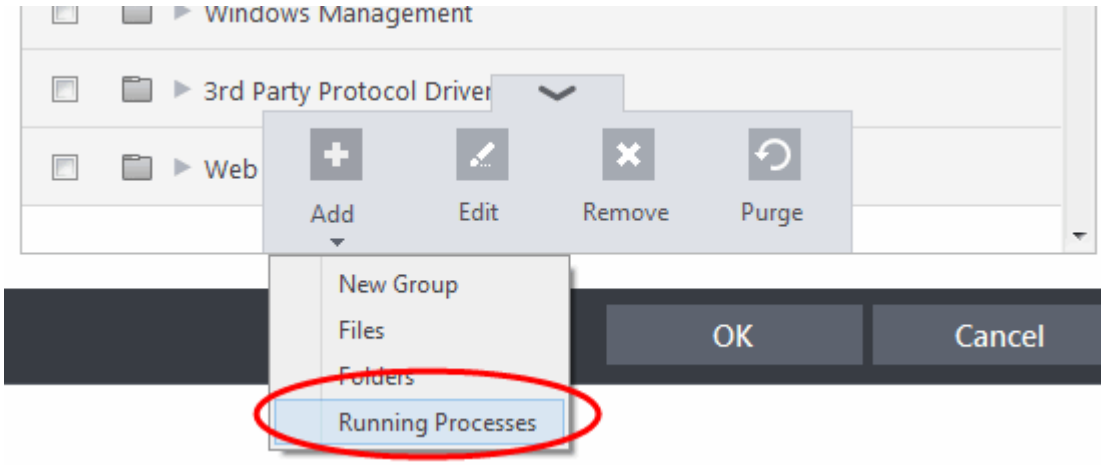
- Navigate to the individual file or folder you want to add to Files Groups and click OK



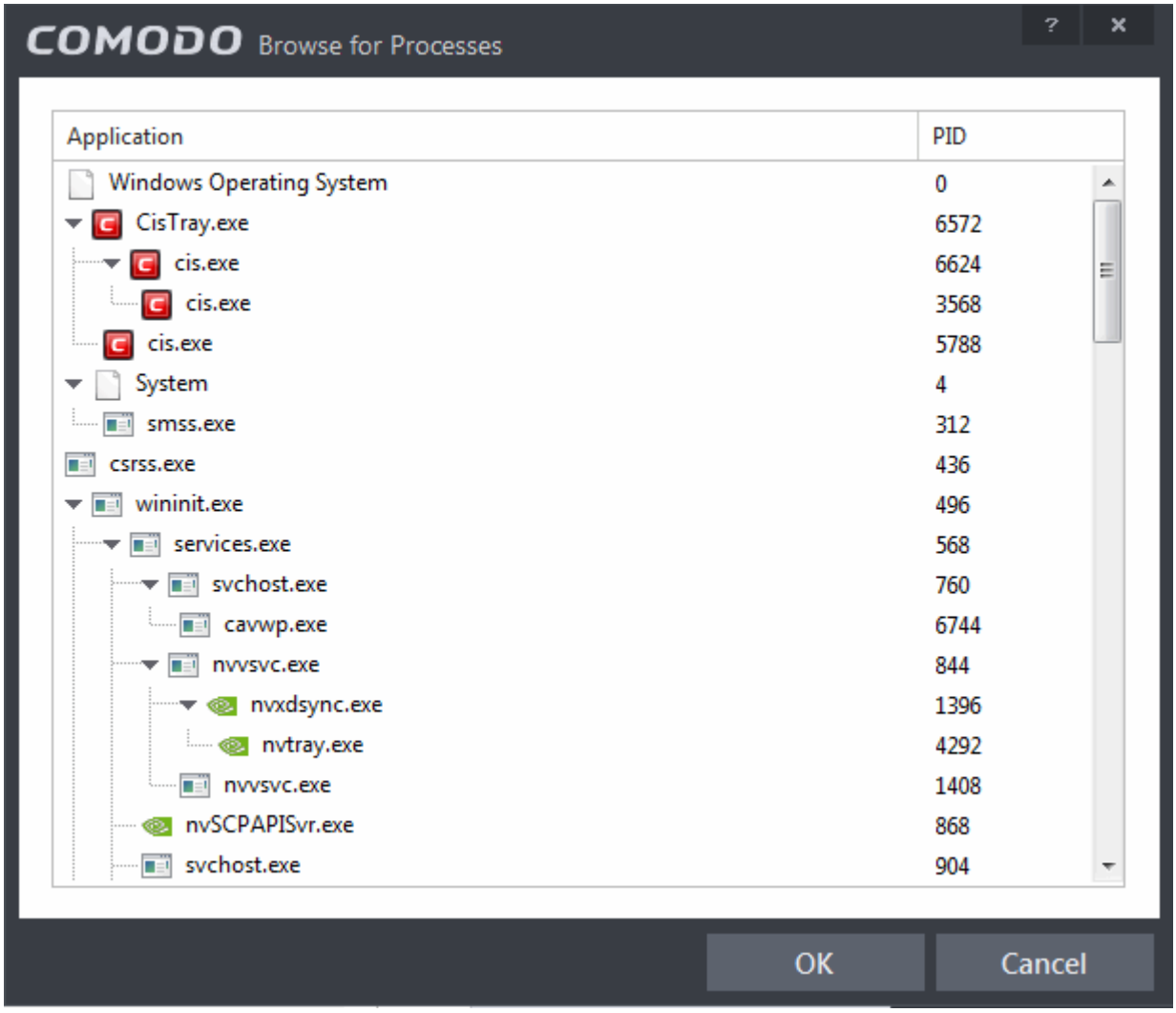
The drive file/folder will be added to File Groups. Repeat the process to add more individual files or folders.

Add an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down



A list of currently running processes in your computer will be displayed.

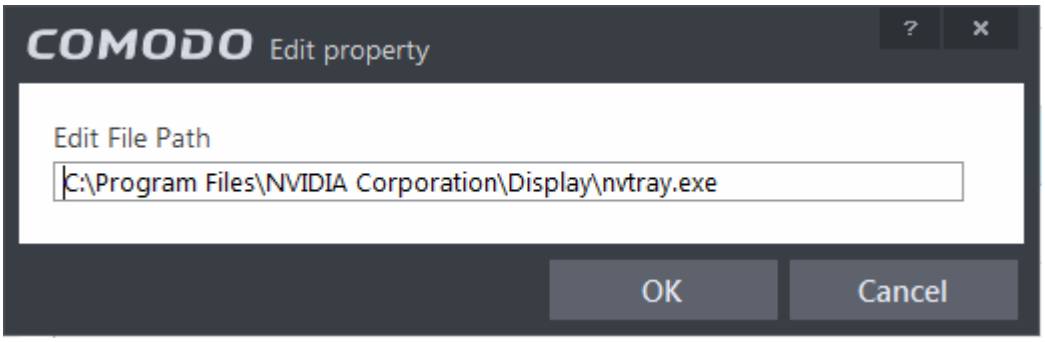


- Select the process, whose target application is to be added to Files Groups and click OK from the Browse for Process dialog.

The application will be added to File Groups.

To edit an item in the Files Groups list

- Select the item from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click OK

To delete existing file group(s) individual file(s) from existing group

- To remove a group, select the group, click the handle and choose Remove.

To remove an individual file from a group, click + at the left of the group to expand the group, select the file to be removed, click

the handle and choose 'Remove'.

6.2.4.3. File List

The 'File List' pane displays a list of executable files, programs and applications and executable files discovered in your system with their file rating. CIS rates the files as:

- **Trusted**
- **Unrecognized**
- **Malicious**

Trusted Files

Files with 'Trusted' rating are automatically given Defense+ trusted status. Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, CIS will check the file against our master whitelist and blacklists and will award it trusted status if:
  - The application is from a vendor included in the **Trusted Software Vendors** list;
  - The application is included in the extensive and constantly updated Comodo safelist.
- Administrator rating
- User Rating – You can provide Trusted status to your files in two ways:
  - If an executable is unknown to the Defense+ safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, you could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted'.
  - You can assign 'Trusted' rating to any desired file from the Files List interface. Refer to the description of **changing the file rating** under the section **File Details** for more details.

  For the files assigned with 'Trusted' status by the user, CIS generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. By this way, even if the file name is changed later, it will retain its Trusted status as the hash remains same.

  By granting 'Trusted' status to executables (including sub folders containing many components) you can reduce the amount of alerts that HIPS generates whilst maintaining a higher level of Defense+ security. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

  Creating your own list of Trusted Files allows you to define a personal safe list of files to complement the default Comodo safe list.

Unrecognized Files

Once installed, the HIPS watches all file system activity on your computer. Every new executable file introduced to the computer, is first scanned against the Comodo certified safe files database. If they are not safe, they are given 'Unrecognized' file rating for users to review and set their own rating. Apart from new executables, any executables that are modified are also given the 'Unrecognized' status.

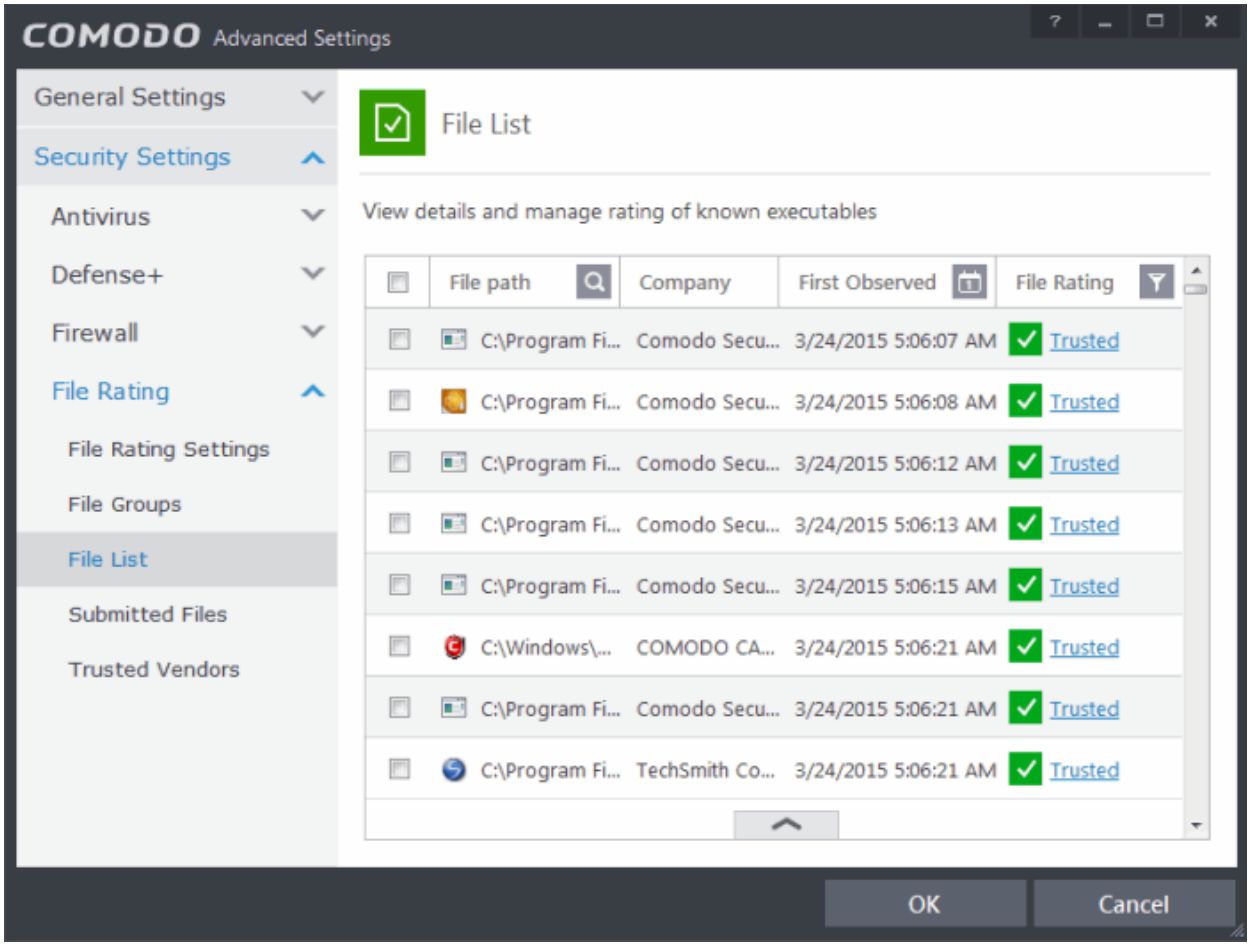
You can assess the pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be given the 'Trusted' rating. Refer to the description of **changing the file rating** for more details. You can also submit the files to Comodo for analysis. Experts at Comodo will analyze the files and add them to global white-list or black-list accordingly.

'Unrecognized Files' is specifically important while HIPS is in 'Clean PC Mode'. In Clean PC Mode, the files in 'Unrecognized Files' are NOT considered safe. For more information, please check '**Clean PC Mode' on the HIPS settings page**.

Malicious Files

Files that are identified as malicious from the FLS will be given 'Malicious' rating and will not be allowed to run by default.

The Trusted Files panel can be accessed by clicking 'Security Settings' > 'File Rating' > 'File List' from the Advanced Settings interface.



The pane displays the list of applications, programs and executable files discovered on your computer.

Column Descriptions:

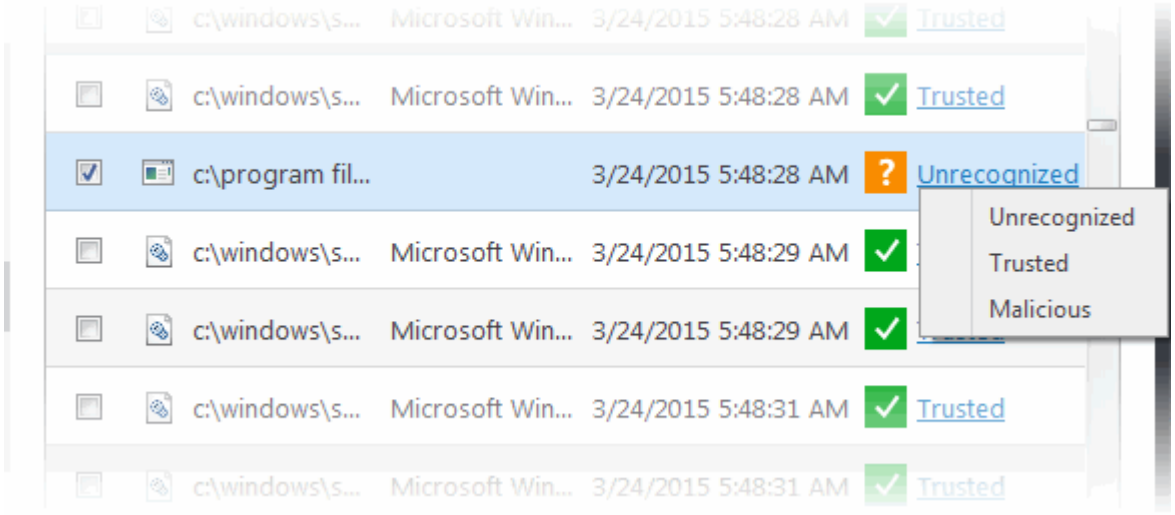
- **File Path**- Indicates installation or storage path of the file;
- **Company** – Shows the publisher of the file;
- **First Observed** - Indicates date and time at which the file was first discovered by CIS. For the files installed or stored before the installation of CIS, it shows the first execution time of CIS, when the file was discovered. For the files installed or stored after installation of CIS, it shows when the file was stored.
- **File Rating** - Indicates the current CIS rating of the file. The possible values are:
  - **Trusted**
  - **Unrecognized**
  - **Malicious**

The files are rated based on the following, in order of priority:

1. Administrator rating (Applicable only if your CIS installation is remotely managed by your CIS administrator).
2. User rating (Rating as set by the user, if modified from the default rating)
3. FLS rating

The File rating can be modified by the user in two ways:

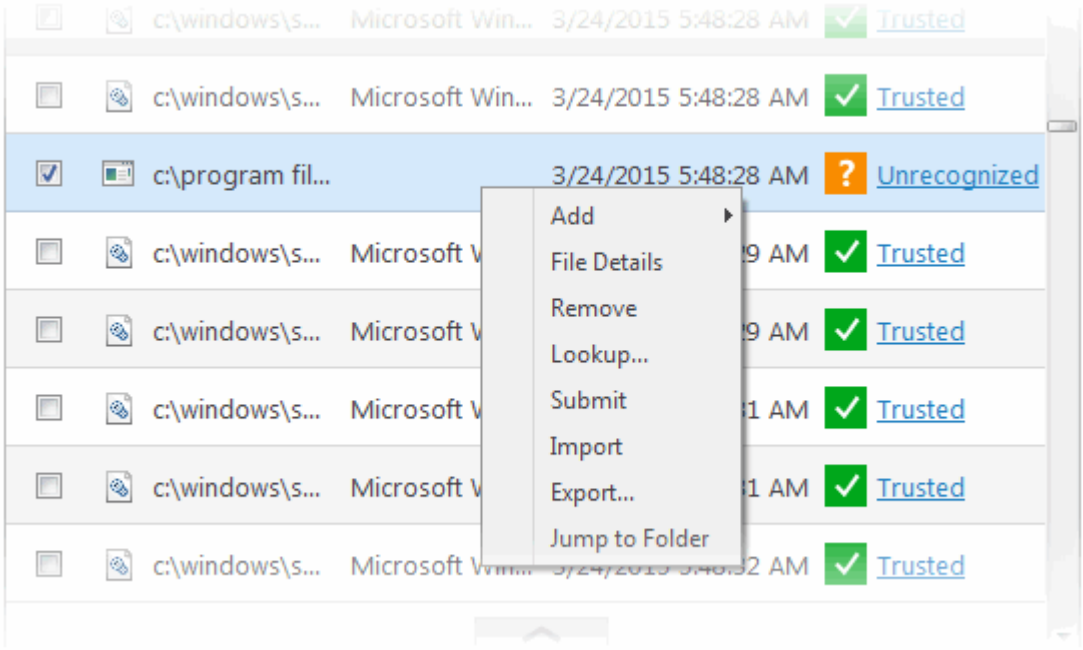
- By clicking on the displayed rating in the row of the desired file and choosing the rating from the context sensitive menu.



- From the 'File Details' dialog of the desired file by selecting it, clicking the handle from the bottom and choosing 'File Details' from the options. Refer to the description of **changing the file rating** under the section **File Details** for more details.

Context Sensitive Menu

Right clicking on a file opens a context sensitive menu that allows you to view the 'File Details' dialog, remove the file from the list, submit the file to Comodo for analysis and more.



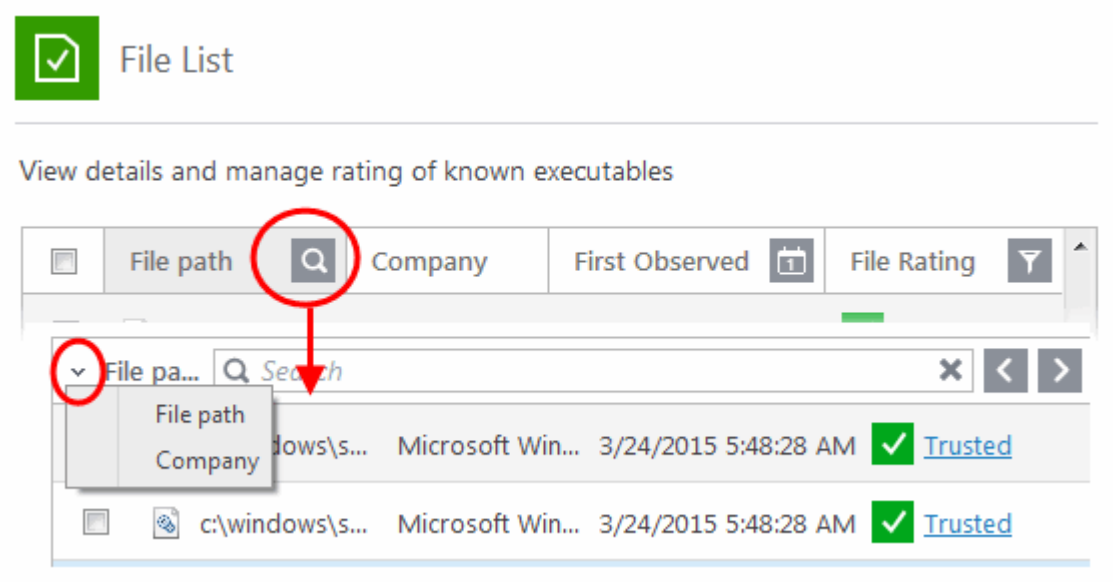
- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the file submission process.
- **Import** - Enables you import a file list from an XML file
- **Export** - Enables you export the current file list with existing ratings to an XML file
- **Jump to Folder** – Opens the folder containing the file in Windows Explorer.

Searching and Filtering options

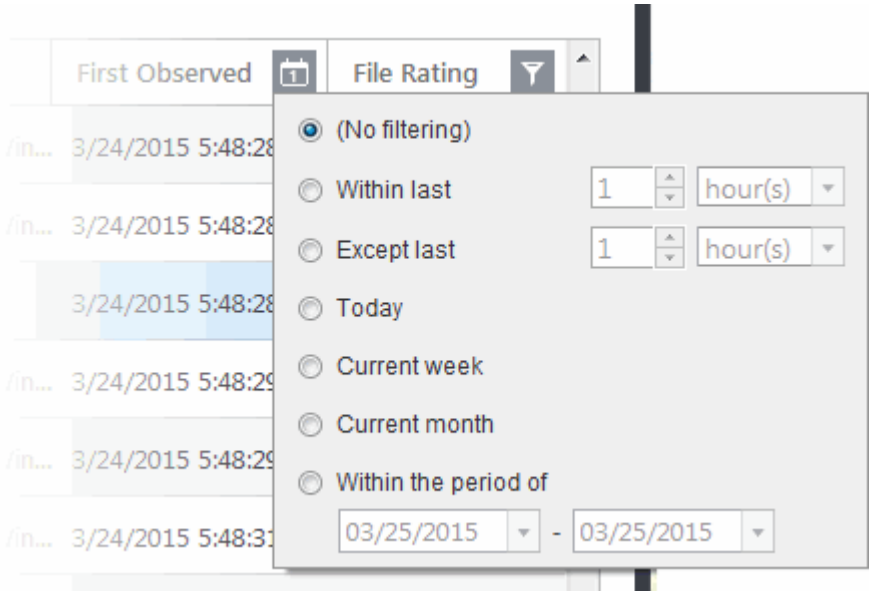
You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and File rating.

To use the search option, click the search icon at the far right in the 'File path' column header.

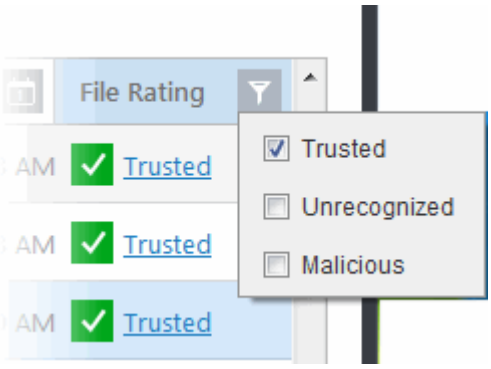
- Click the chevron on the left side of the column header and select the search criteria from the drop-down.



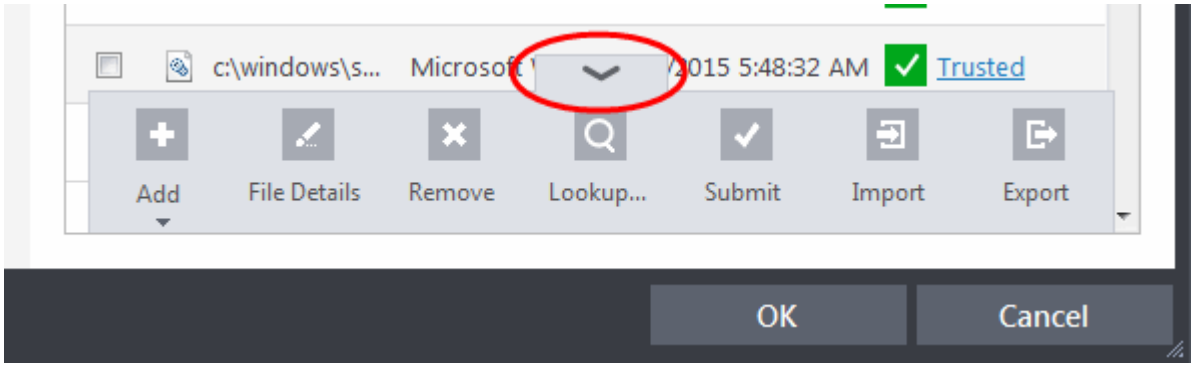
  - Enter the file path or the name of company in part or full as per the selected criteria in the search field and press 'Enter' to begin the search.
- To filter the list based on the date of installation or storage of the files, click the calendar icon at the right of the 'First Observed' column header and choose the time/date/period.



- To filter the list based on the file rating, click the funnel icon at the right of the 'File Rating' column header and select the ratings to display only the files with the selected rating(s).



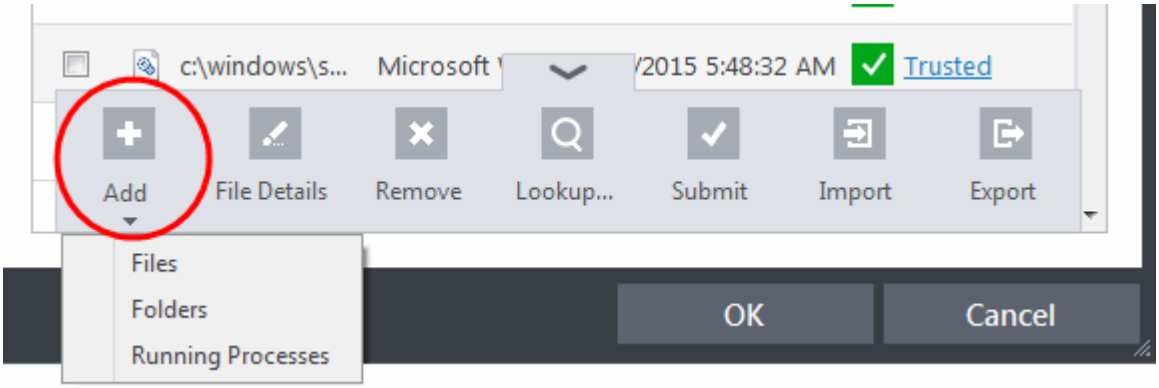
Clicking the handle at the bottom of the panel opens the following options:



- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the file submission process.
- **Import** - Enables you import a file list from an XML file
- **Export** - Enables you export the current file list with existing ratings to an XML file

To manually add files to 'File list'

- Click the handle from the bottom and choose 'Add'

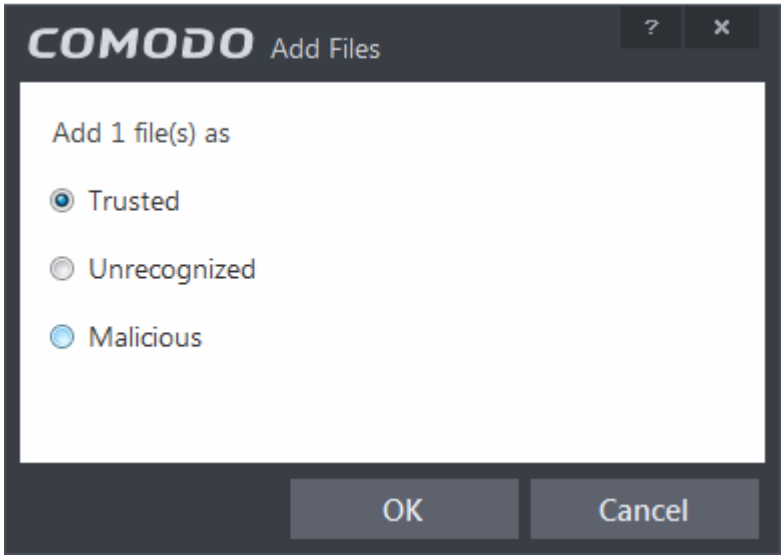


Tip: Alternatively, right click inside the File List page and choose 'Add' from the context sensitive menu.

- You can add files to the File list by three ways:

- **Files** - Allows you to navigate to the file or executable of the program you wish to add and assign a rating.
- **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'File List' with the rating you assign.
- **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'File List' with the rating you assign.

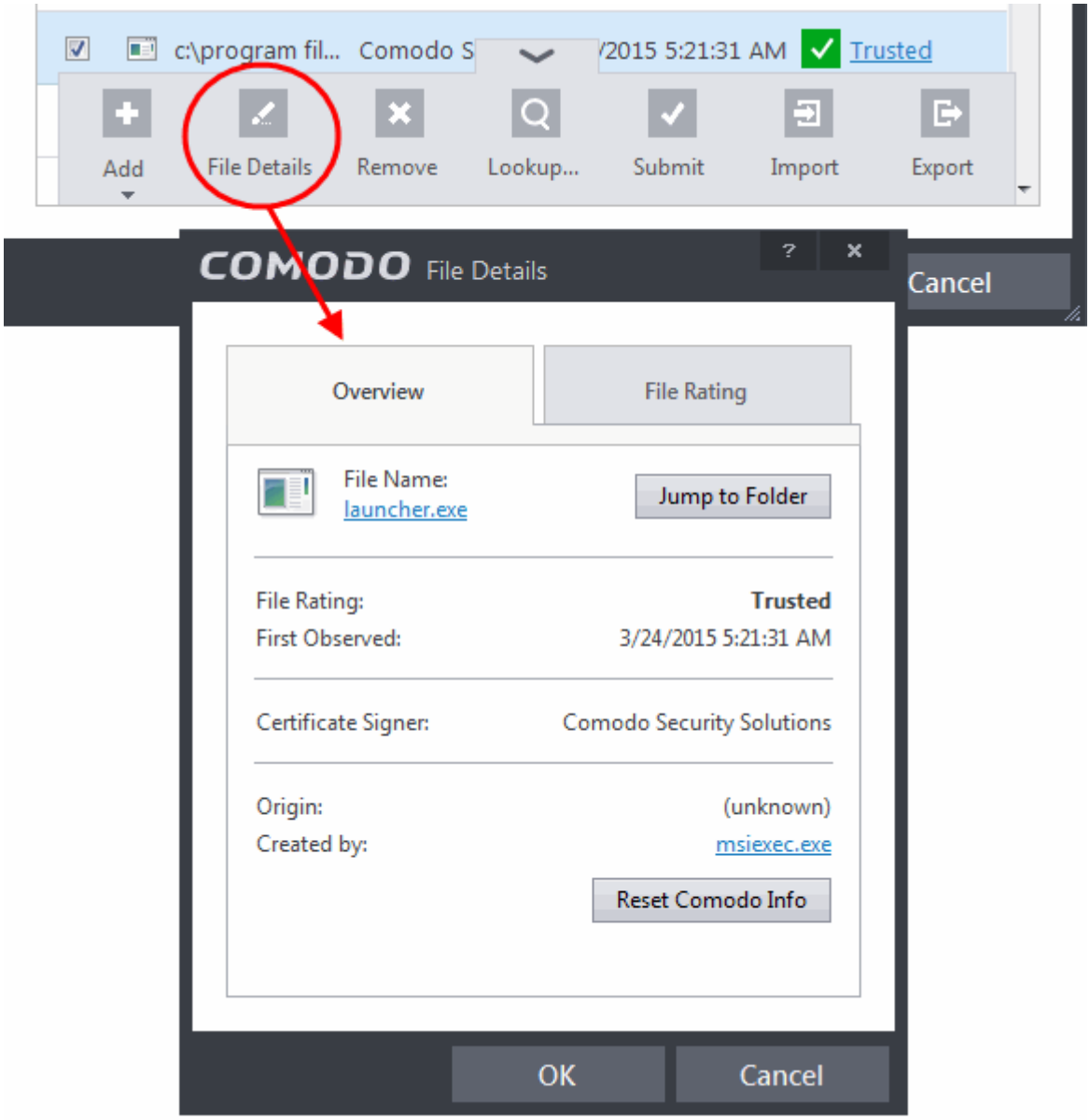
Once you have chosen the file(s) or the folder, you can assign the rating for the file(s) to be added.



- Choose the rating to be assigned to the file(s). The available options are:
  - Trusted – The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
  - Unrecognized – The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
  - Malicious – The file will not be allowed to run.
  - Click OK in the 'Add Files' dialog
- Click 'OK' in the 'Advanced Settings' for your changes to take effect.

To view the 'File Details' and change the rating

- Choose the file to view its details
- Click the handle from the bottom and choose 'File Details'



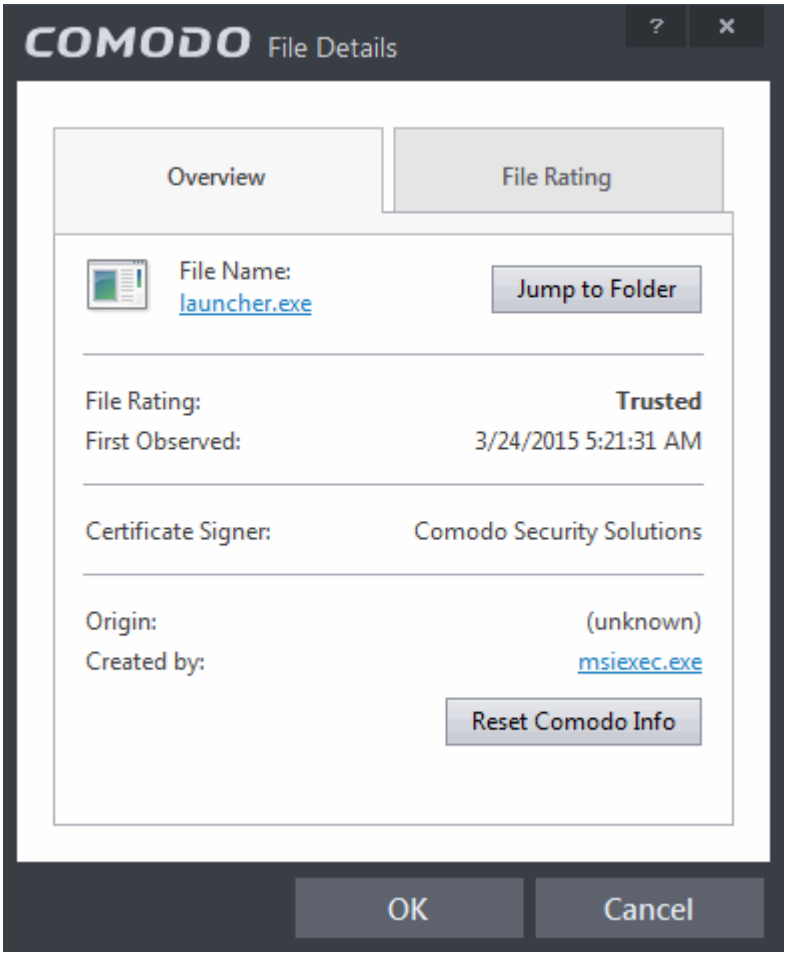
Tip: Alternatively, right click on the selected file inside the File List page and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog contains two tabs:

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

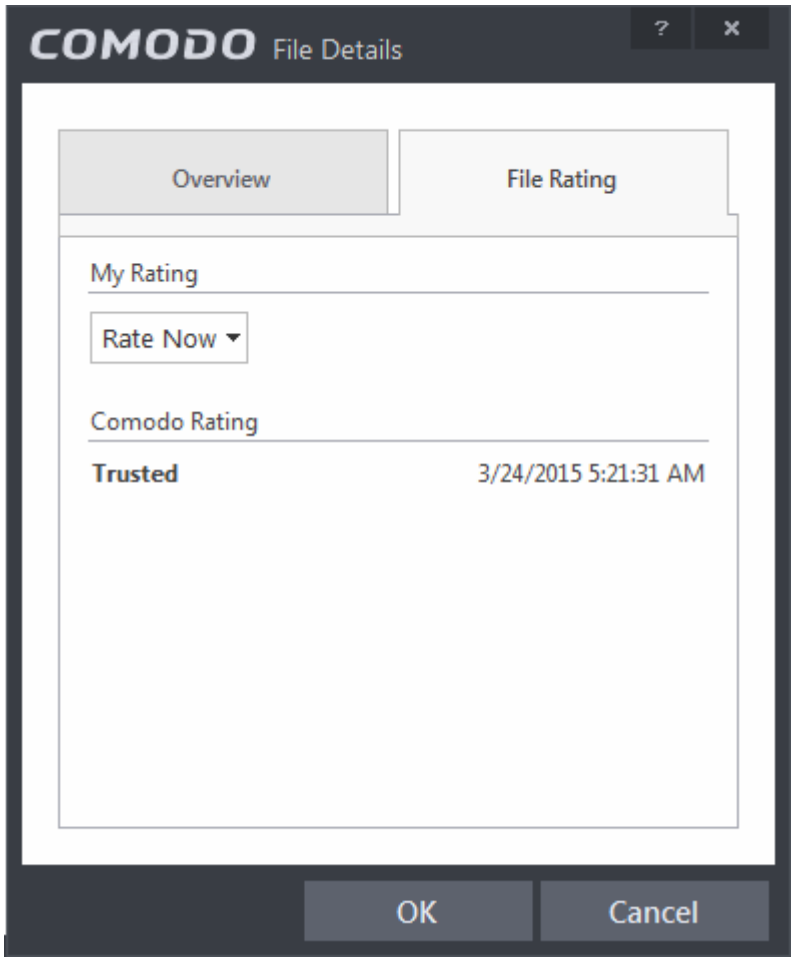
Overview

The Overview tab displays the general details of the file and the publisher details.



- Clicking the file name opens the Windows 'File Properties' dialog.
- Clicking 'Jump to folder' opens the folder containing the file in Windows Explorer, with the respective file selected.

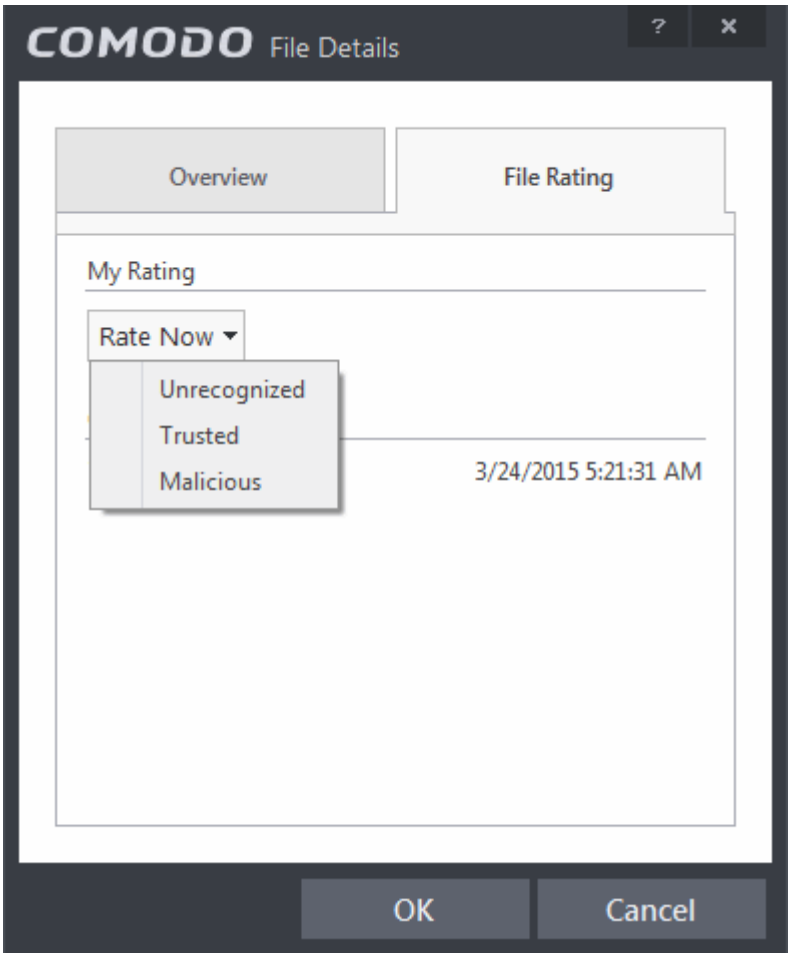
File Rating



The 'File Rating' tab enables you to change the current rating of the file and displays the current rating as per the analysis result from Comodo.

To change the user rating of the file

- Select the file from the 'File List' pane, click the handle from the bottom and choose File Rating from the options
- Click the File Rating tab from the File Details tab
- Click 'Rate Now' and choose the rating from the drop-down



The options available are:

- Trusted – The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- Unrecognized – The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- Malicious – The file will not be allowed to run.

- Click 'OK' in the 'Files Details' dialog

- Click 'OK' in the 'Advanced Settings' interface to save your settings.

To remove files(s) from the File list

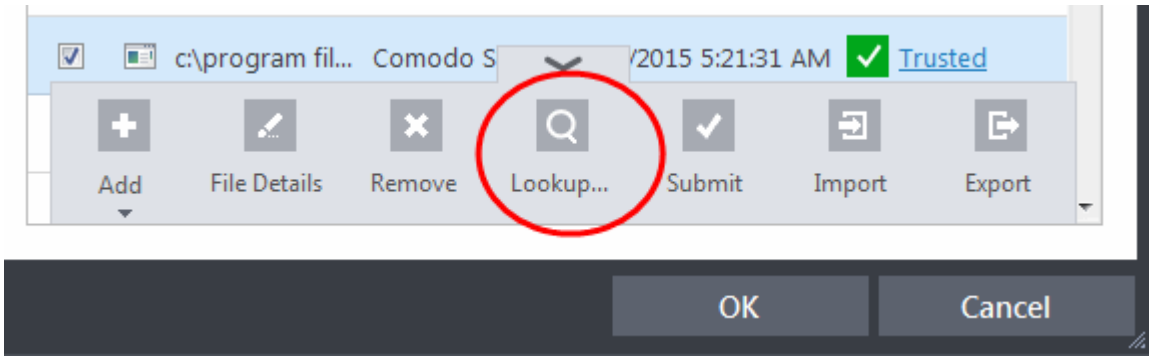
- Select the file(s) to be removed from the 'File List' pane. You can select several entries to be removed at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Remove'. The file is only removed from the list and not deleted from your system.

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Remove' from the context sensitive menu.

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

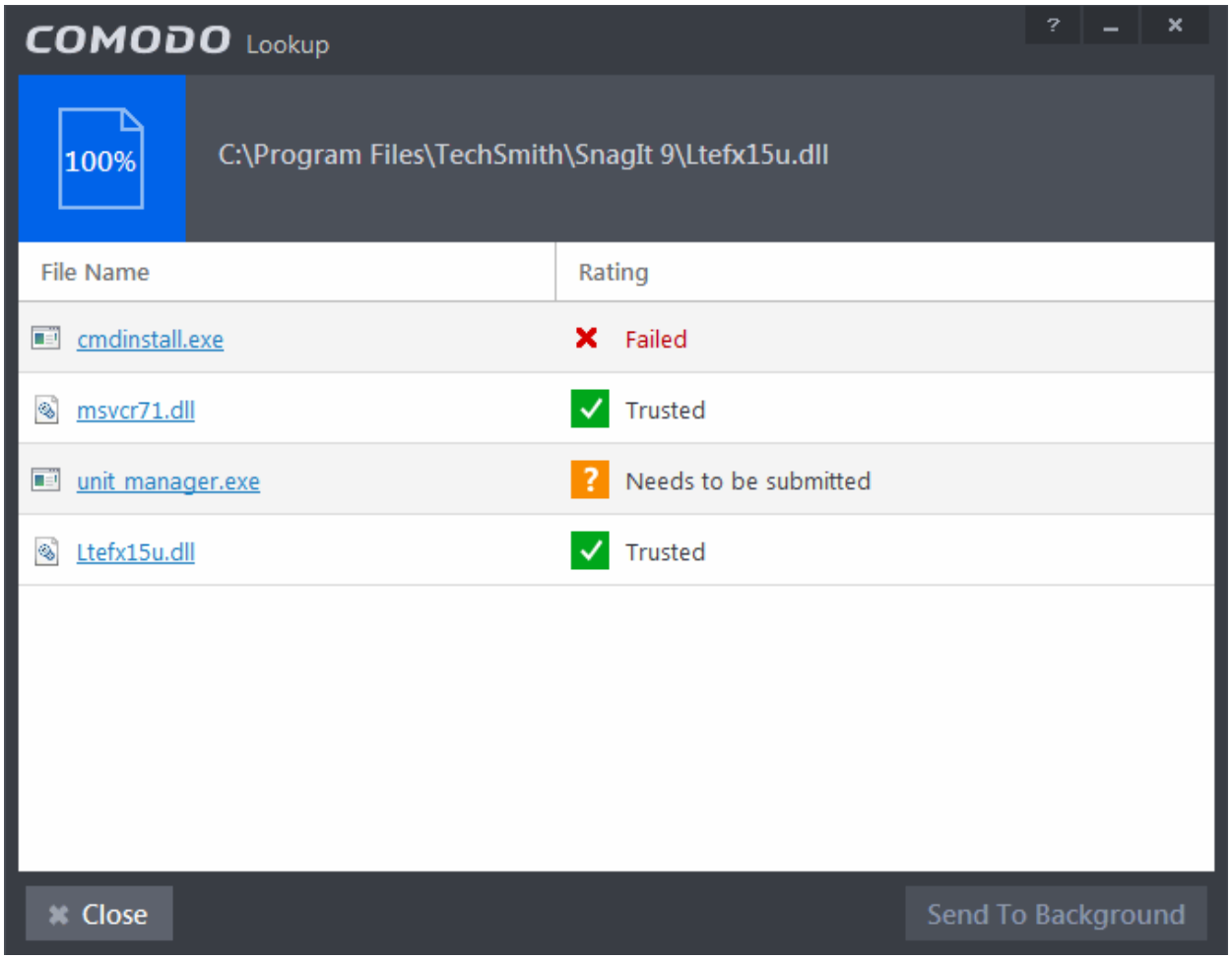
To perform an online lookup for files

- Select the files to be checked from the 'File list' pane. You can select several entries at once by marking the check-boxes beside the entries.
- Click the handle from the bottom and choose 'Lookup...'.

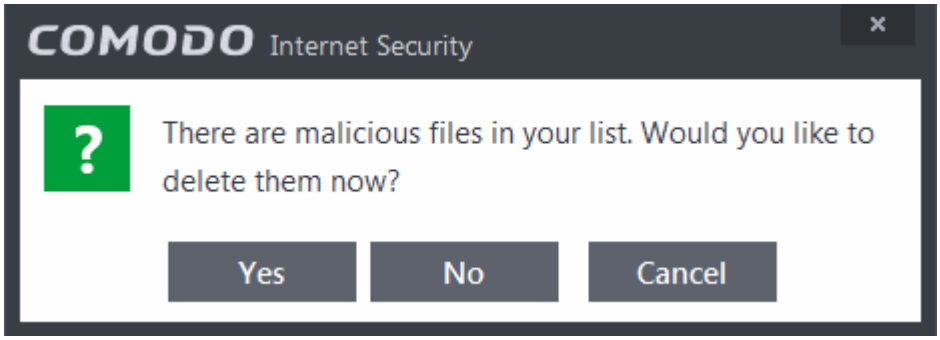


Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Lookup' from the context sensitive menu.

Comodo servers will be contacted immediately to conduct a search of Comodo's master safe list database to check if any information is available about the files in question and the results will be displayed.



If any malicious or unwanted file(s) is/are found, you will be given an option to delete the file from your computer on closing the dialog.



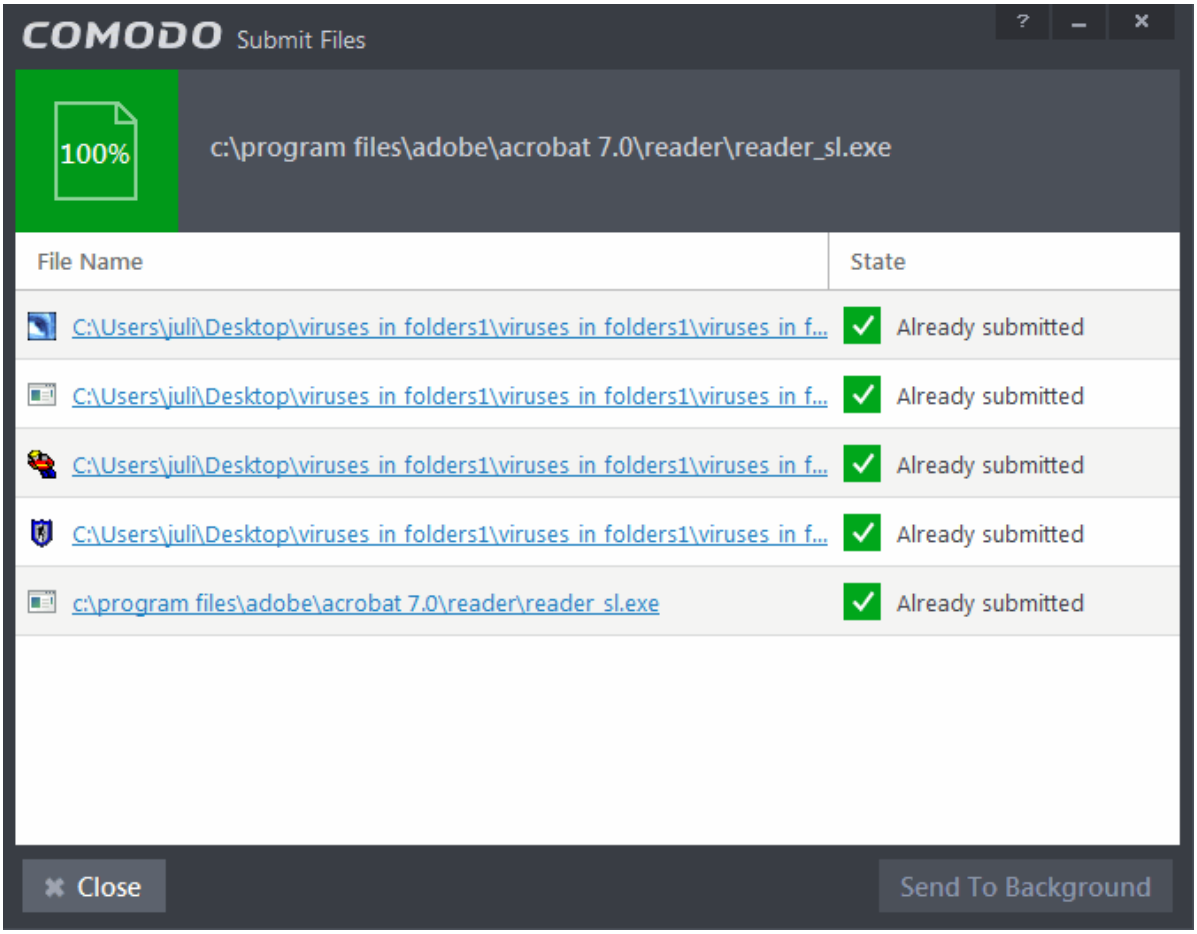
- Click 'Yes' to permanently delete the malicious file(s) from your computer.

- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. Refer to the description of **changing the file rating** under the section **File Details** for more details.
- If no information is available, it will be indicated as 'Unknown' with a yellow icon. You can submit the file to Comodo for analysis. Refer to the **explanation below** for more details.

To manually submit files to Comodo

- Select the file(s) to be submitted from the 'File List' pane. You can select several entries to be sent at once by marking the check-boxes beside the entries.
- Click the handle from the bottom and choose 'Submit'. The file(s) will be immediately sent to Comodo.

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Submit' from the context sensitive menu.



You can view the list of files you submitted so far, from the **Submitted Files** panel.

Exporting and Importing the File List

You can export the list of files with their currently assigned file ratings to an XML file and store the list on a safe place. This is useful to restore your File List, in case you are reinstalling the CIS application for some reasons.

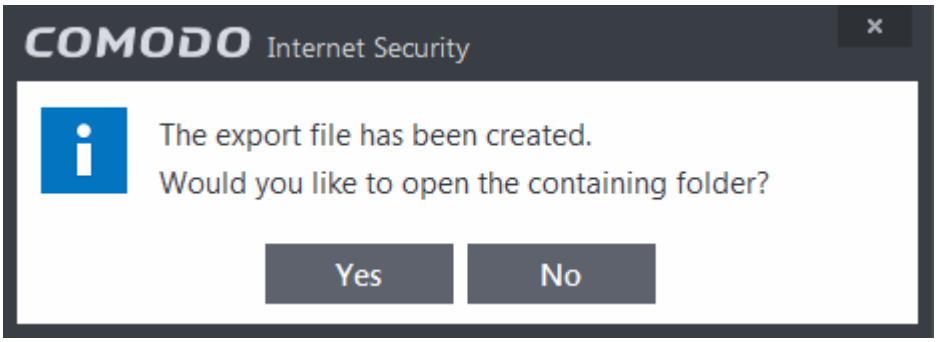
To export the File List

- Click the handle from the 'File List' pane and choose 'Export' from the options

Tip: Alternatively, right click inside the 'File List' page and choose 'Export' from the context sensitive menu.

- Navigate to the location to store the XML file containing the file list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.



To import a saved file list

- Click the handle from the 'File List' pane and choose 'Import' from the options

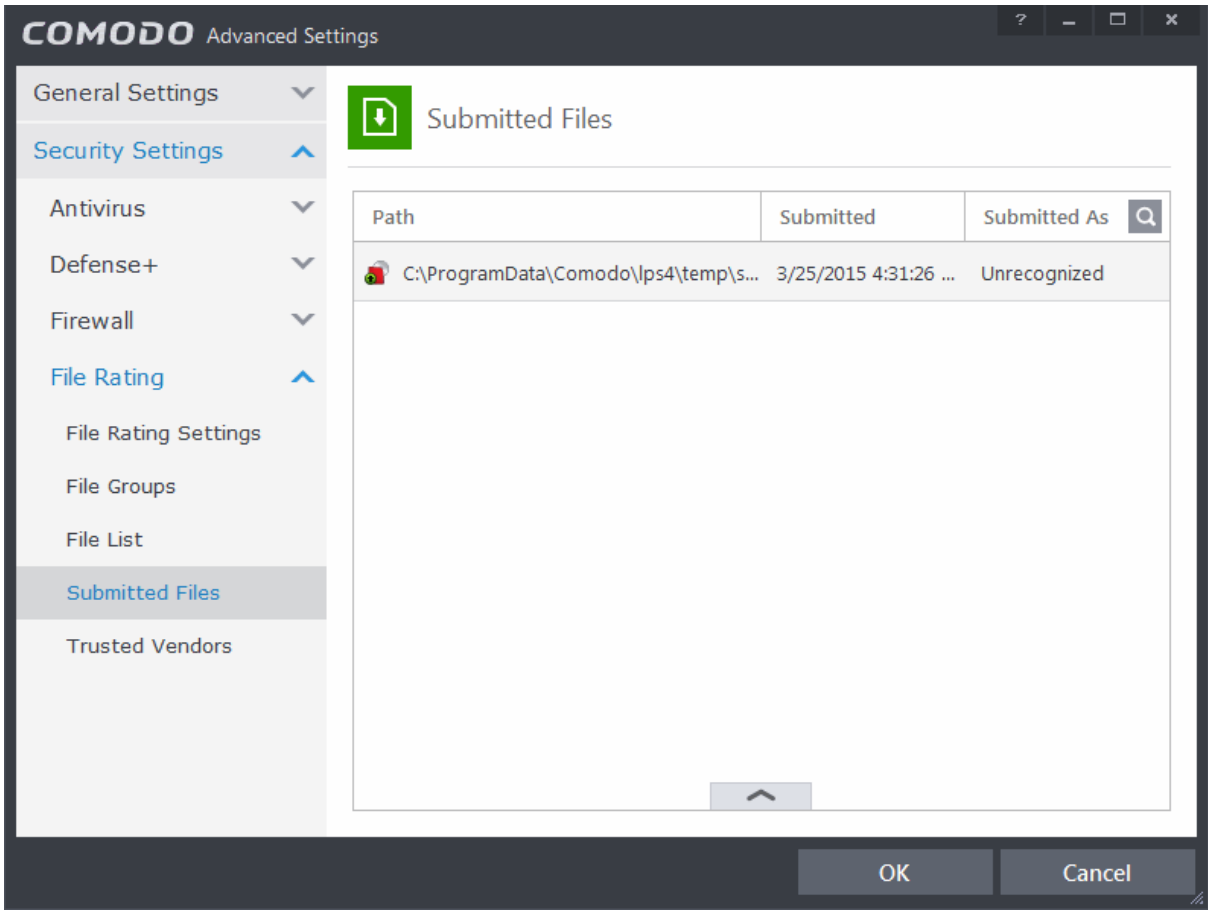
Tip: Alternatively, right click inside the 'File List' page and choose 'Import' from the context sensitive menu.

- Navigate to the location of the XML file containing the file list and click 'Open'.

The 'File List' will be populated as per the imported 'File List'.

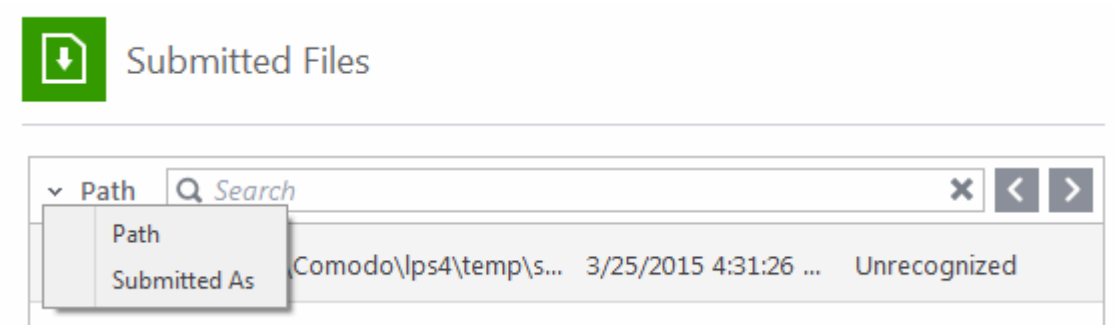
6.2.4.4. Submitted Files

The Submitted Files panel displays a list of files you have submitted so far for analysis to Comodo.



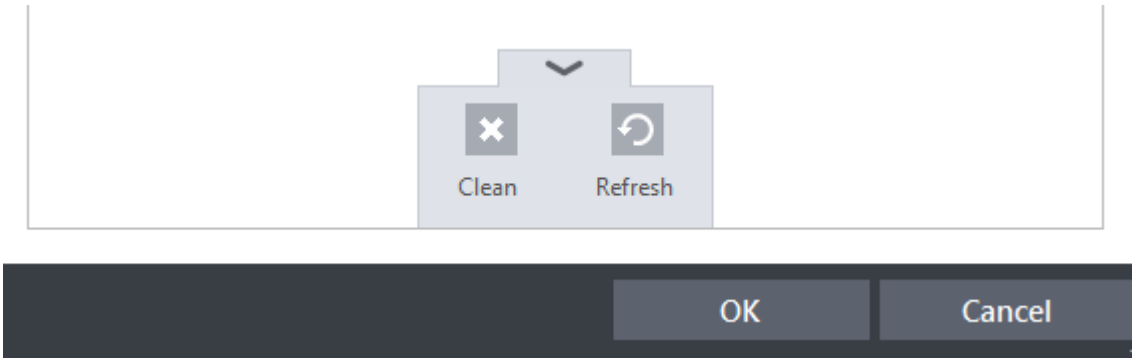
You can use the search option to find a specific file in the list.

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



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

Clicking the handle at the bottom center of the panel opens the following options:



- **Clean** - Clears the list
- **Refresh** - Reloads the list to add items that are submitted recently

6.2.4.5. Trusted Vendors List

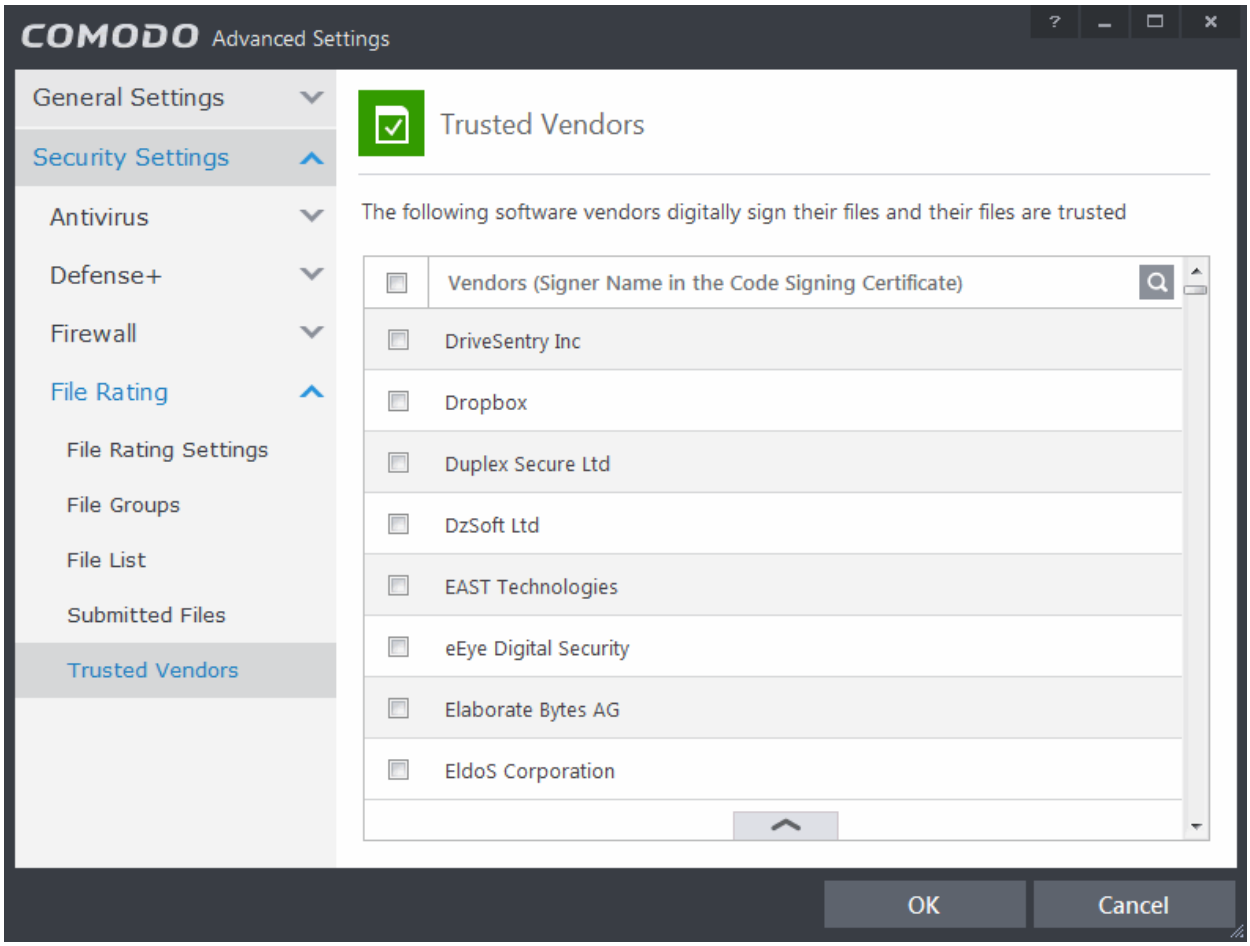
In Comodo Internet Security, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

From this point:

- IF the vendor is on the Trusted Software Vendor List AND the user has enabled '**Trust Applications signed by Trusted Vendors**' in the File Rating Settings panel, THEN the application will be trusted and allowed to run.
- IF the vendor is not on the Trusted Software Vendor List OR the user has not enabled 'Trust Applications signed by Trusted Vendors' THEN the application will be sandboxed. If the application in question is an installer then CIS will generate an elevated privilege alert.

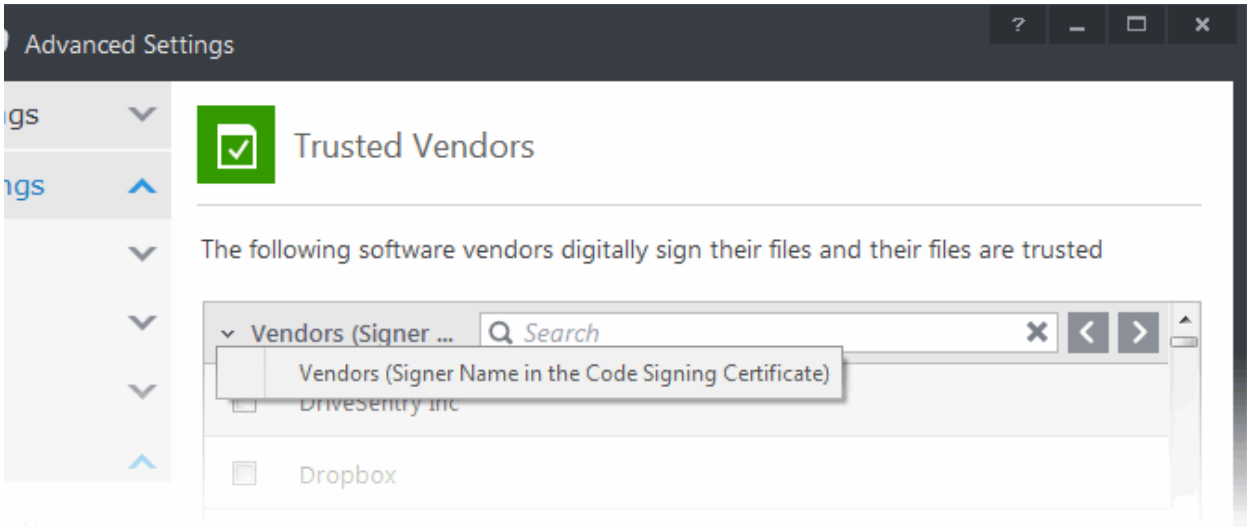
Software publishers may be interested to know that they can have their signatures added, free of charge, to the 'master' Trusted Software Vendor List that ships to all users with CIS. Details about this can be found at the foot of this page.

The 'Trusted Software Vendors' panel can be opened by clicking Security Settings > File Rating > Trusted Vendors.



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

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



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

Click here to read background information on digitally signing software

Click here to learn how to Add / Define a user-trusted vendor

Software Vendors - click here to find out about getting your software added to the list

Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

i. **Content Source**: The software they are downloading and are about to install ***really comes from the publisher that signed it.***

ii. **Content Integrity**: That the software they are downloading and are about to install ***has not be modified or corrupted since it was signed.***

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

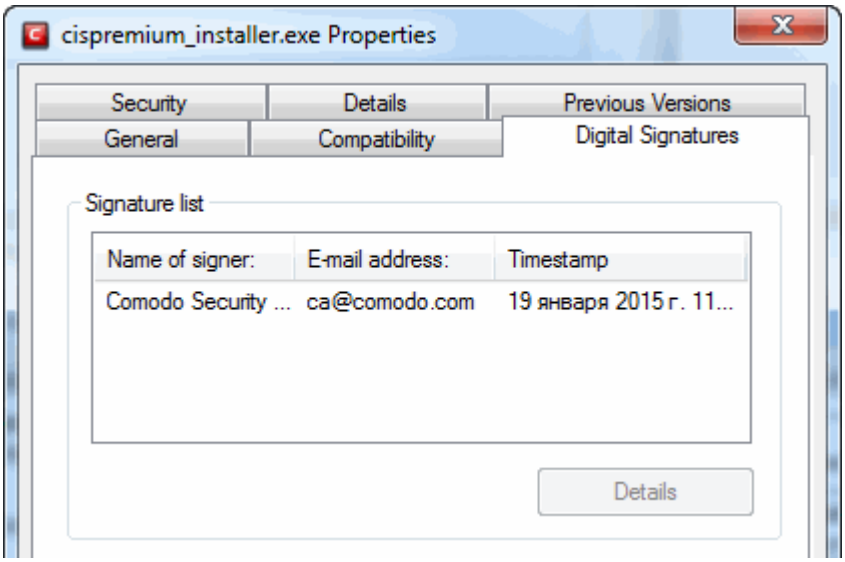
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Internet Security (if you would like to read more about code signing certificates, see **http://www.instantssl.com/code-signing/**).

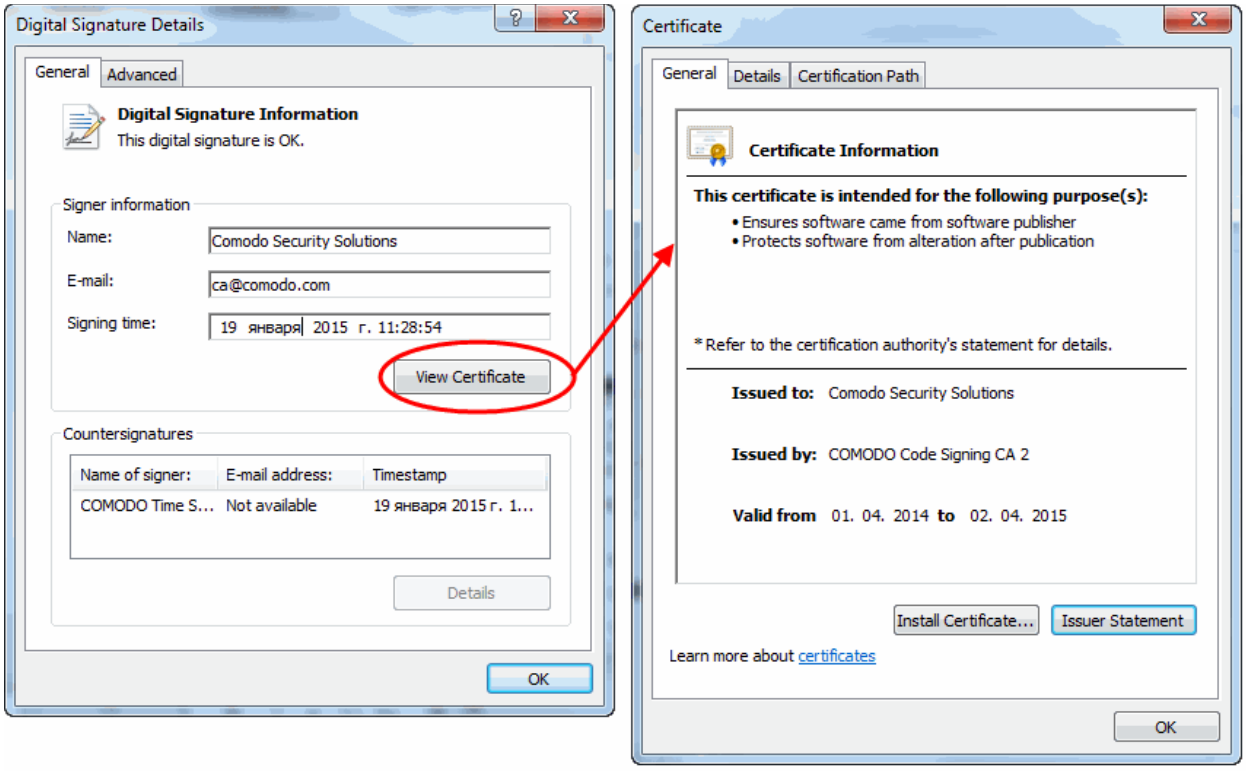
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Internet Security is called 'cis.exe' and has been digitally signed.

- Browse to the (default) installation directory of Comodo Internet Security.
- Right click on the file cis.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

This displays the name of the CA that signed the software as shown below:



Click the 'Details' button to view digital signature information. Click 'View Certificate' 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. **See this example** for more details.

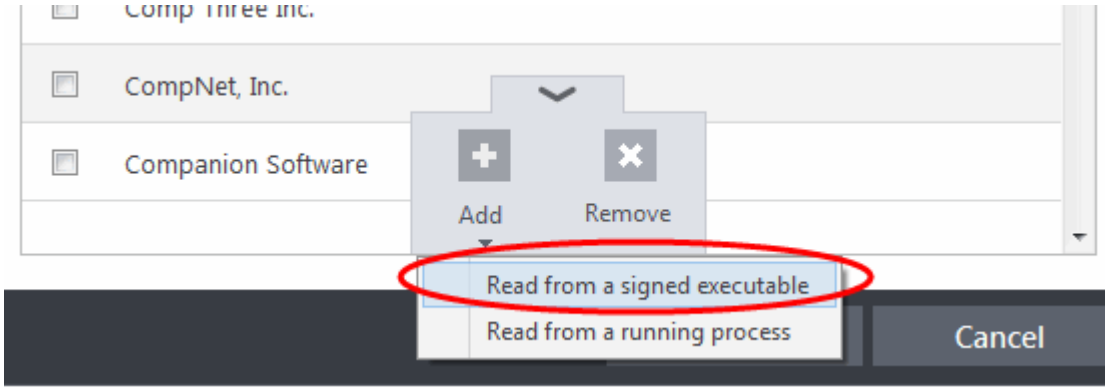
Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

- **By reading the vendor's signature from an executable file on your local drive**
- **By reading the vendor's signature from a running process**

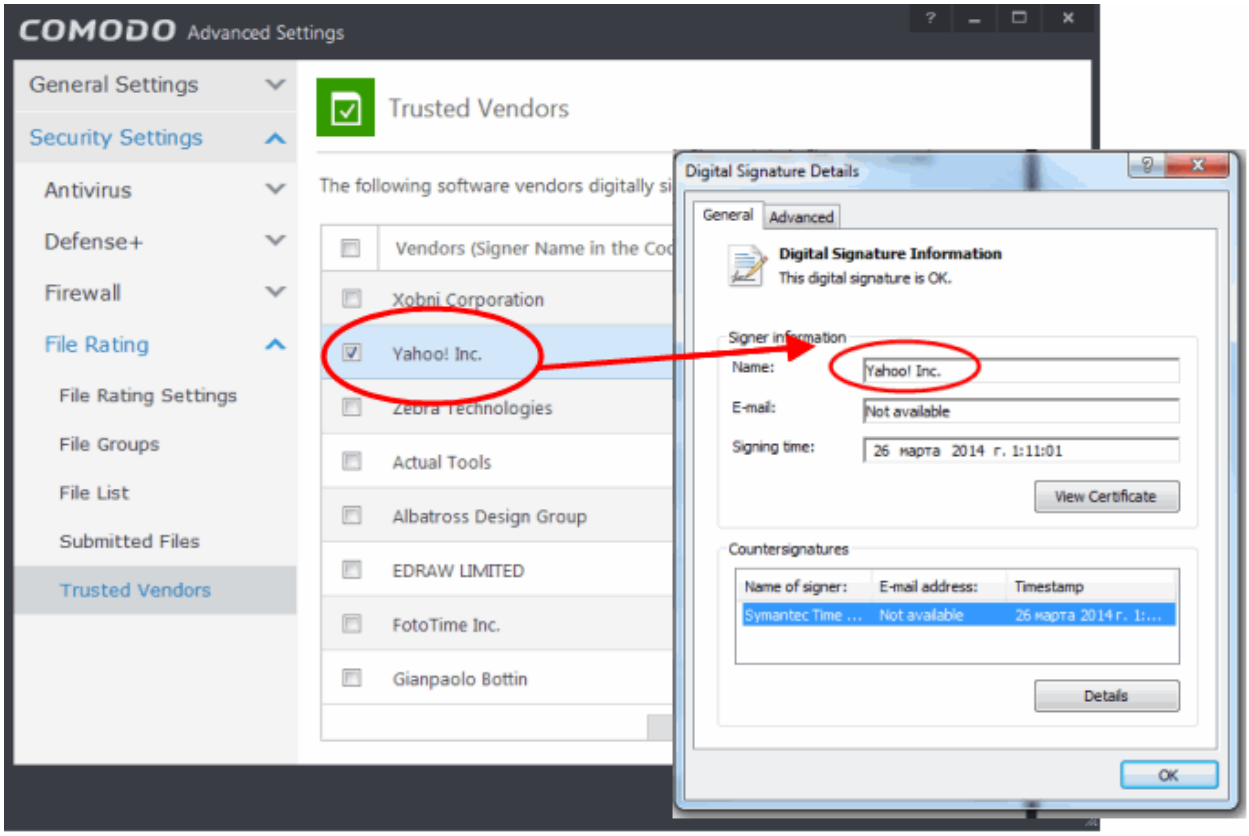
To add a trusted vendor by reading the vendor's signature from an executable

- Click the handle from the bottom center and choose 'Add' > 'Read from a signed executable'



- Browse to the location of the executable your local drive. In the example below, we are adding the executable 'YahooMessenger.exe'.

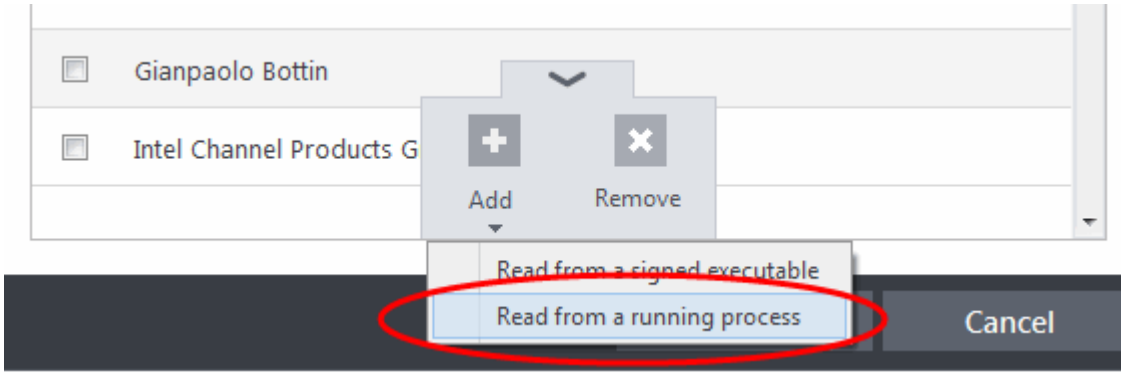
On clicking 'Open', Comodo Internet Security checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the Trusted Vendor list (TVL):



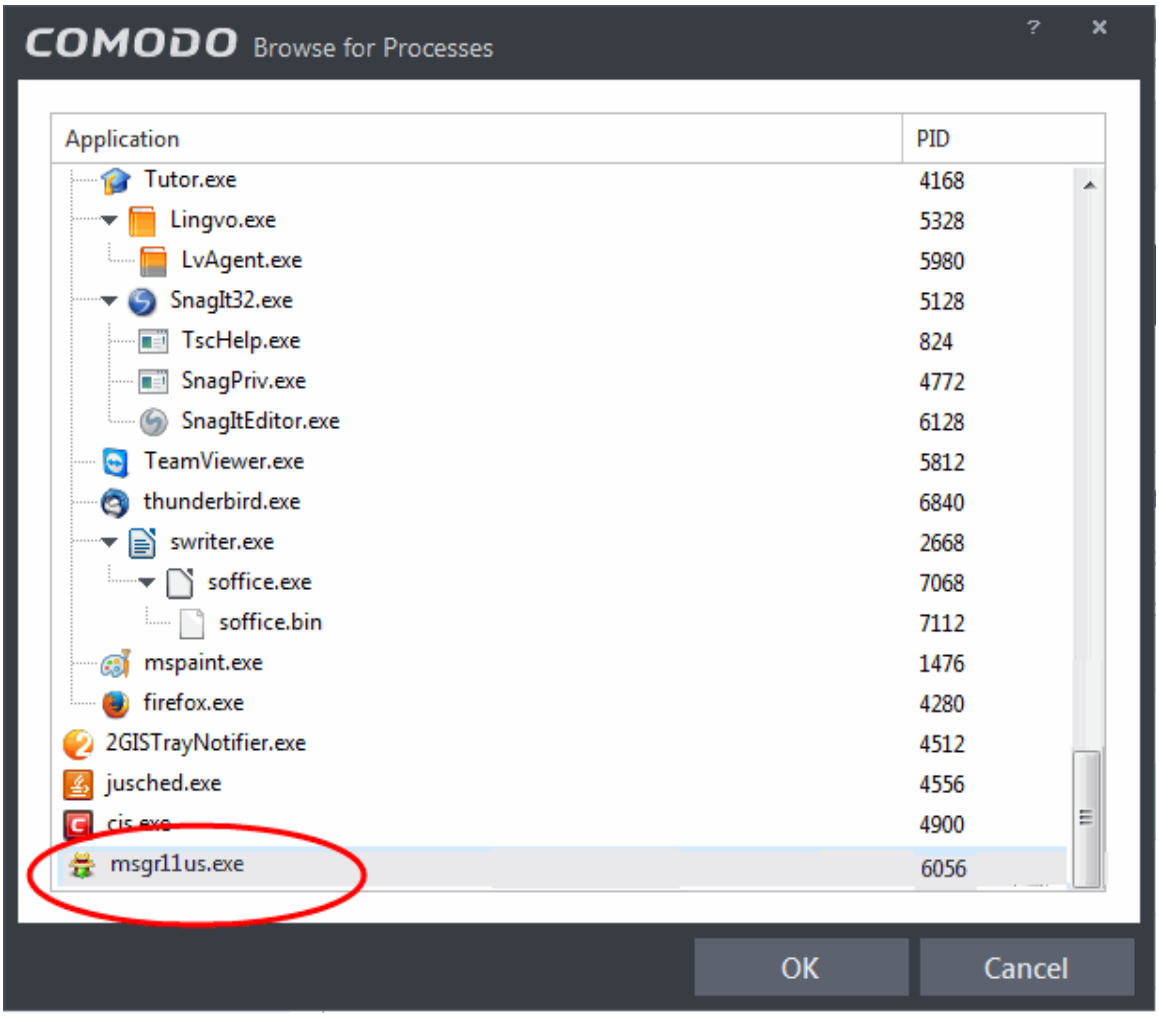
In the example above, Comodo Internet Security was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to the list. All future software that is signed by the vendor 'Yahoo! Inc.' is automatically added to the Comodo Trusted Vendor list UNLESS you change **this setting in File Rating Settings**.

To add a trusted vendor from a currently running process

- Click the handle from the bottom center and choose 'Add' > 'Read from a running process'

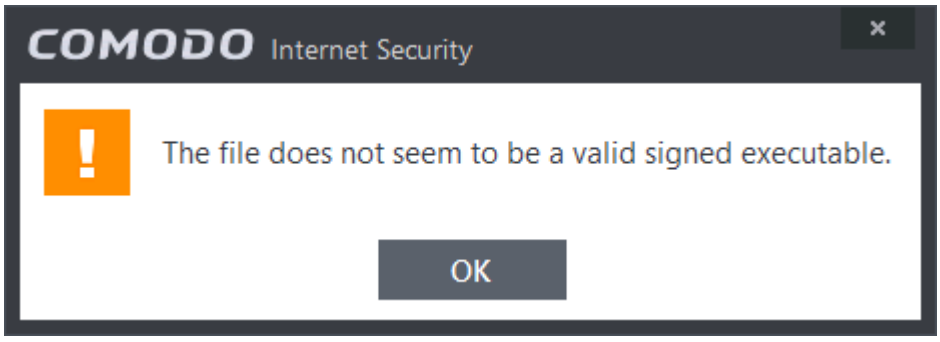


- Select the signed executable that you want to trust and click the 'OK' button.



Comodo Internet Security performs the same certificate check as described above. If the parent application of the selected process is signed, CIS adds the vendor to the Trusted Software Vendors list.

If Comodo Internet Security cannot verify that the software certificate is signed by a Trusted CA then it does not add the software vendor to the list of 'Trusted Vendors'. In this case, you can see the following error message.



Note: The 'Trusted Software Vendors' list displays two types of software vendors:

- User defined trusted software vendors - As the name suggests, these are added by the user via one of the two methods outlined earlier. These vendors can be removed by the user by selecting and clicking the 'Remove' button.
- Comodo defined trusted software vendors - These are the vendors that Comodo, in it's capacity as a Trusted CA, has independently validated as legitimate companies. If the user needs to remove any of these vendors from the list, it can be done by selecting the vendor, clicking 'Remove' and restarting the system. Please note that the removal will take effect only on restarting the system.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default Trusted Vendor List that is shipped with Comodo Internet Security. This service is free of cost and is also open to vendors that have used code signing certificates from any Certificate Authority. Upon adding the software to the Trusted Vendor list, CIS automatically trusts the software and does not generate any warnings or alerts on installation or use of the software.

The vendors have to apply for inclusion in the Trusted Vendors list through the sign-up form at **http://internetsecurity.comodo.com/trustedvendor/signup.php** and make sure that the software can be downloaded by our technicians. Our technicians check whether:

- The software is signed with a valid code signing certificate from a trusted CA;
- The software does not contain any threats that harm a user's PC;

before adding it to the default Trusted Vendor list of the next release of CIS.

More details are available at **http://internetsecurity.comodo.com/trustedvendor/overview.php**.

7.Comodo GeekBuddy

Comodo GeekBuddy is a personalized computer support service provided by friendly computer experts at Comodo. If you experience any issues at all with your computer, simply click the GeekBuddy icon to establish a chat session with one of our technicians.

After requesting your permission, they'll establish a remote connection to your PC and fix the problems right in front of your eyes. No longer do you need to make time consuming calls to impatient help desk support staff. Instead, just sit back and relax while our friendly technicians do the work for you. Visit **http://www.geekbuddy.com/** for more details.

One of the great features of the CIS interface is that you can immediately launch a chat with a qualified computer support technician by clicking 'Help' icon  > Support > Get Live Support. If you have opted not to include GeekBuddy during CIS installation, choosing Get Live Support will start the installation automatically.

GeekBuddy is included with CIS Pro and Complete versions and is available with CIS Premium. The GeekBuddy section of this guide is broken down into the following sections:

- **Overview of the Services**
- **Activation of Service**
- **Launching the Client and Using the Service**
- **Accepting Remote Desktop Requests**
- **Chat History**
- **Using Free Diagnostic Reports**
- **Uninstalling Comodo GeekBuddy**

7.1.Overview of Services

Comodo GeekBuddy includes the following services:

- **Virus & Malware Removal** - Our technicians remotely clear any detected viruses or malware that is found on your PC.
- **Internet and Online Identity Security** - Optimization of your computer's security settings to prevent loss of sensitive data and identity theft.
- **Printer or Email Account Setup** - Installation or updating of printer software and/or drivers, checking ink levels and configuring your printer to work on a wireless or wired network. We set up your Internet-based email account - any

provider, any account. Great for new computers and novice email users.

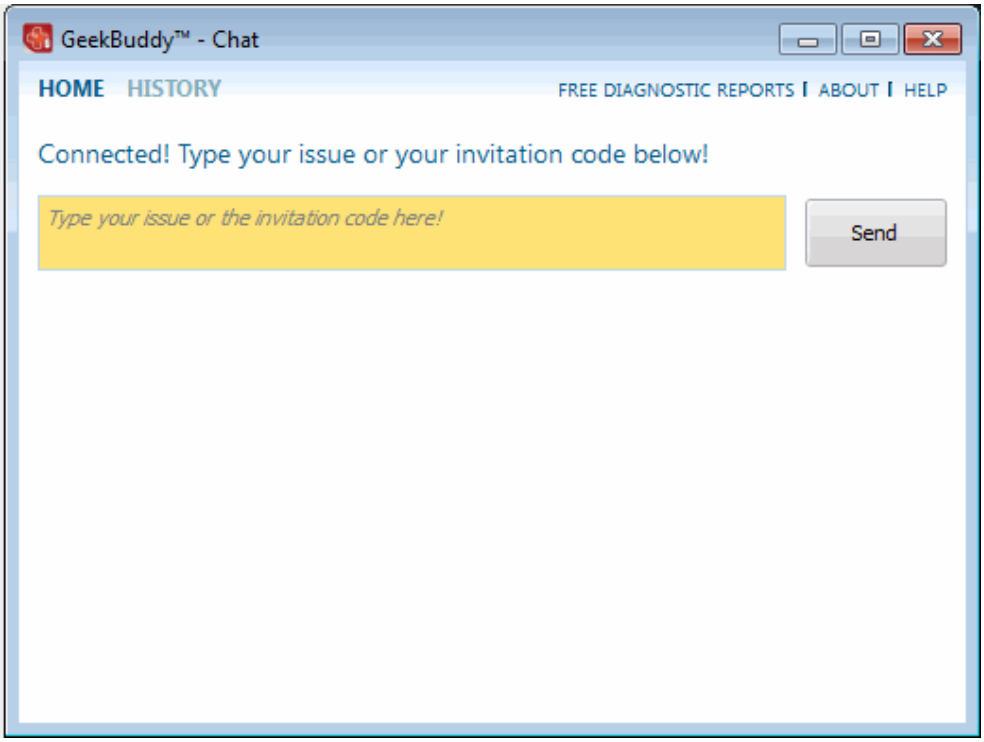
- **Software Activation** - Installation, configuration, and activation of third party software in your system.
- **General PC Troubleshooting** - Detailed system check to identify and eliminate basic hardware and software conflicts in your Windows PC.
- **Computer Power Setting Optimization** - Optimization of your power management settings based on how you use your computer. Your Geek will help you go green and save money on your electric bill.
- **Comodo Software Installation and Set up** - Installation and support of software supplied by Comodo.
- **Comodo Account Questions** - Clarification of any doubts regarding your account in Comodo.

7.2. Activation of Service

GeekBuddy is included in CIS Pro and Complete versions and users who purchased either of these CIS versions can skip this section and move on to the next section '**Launching the Client and Using the Service**'. GeekBuddy client is downloaded along with CIS Premium (a free version) with a trial license, but to use the full service, you have to purchase and activate it.

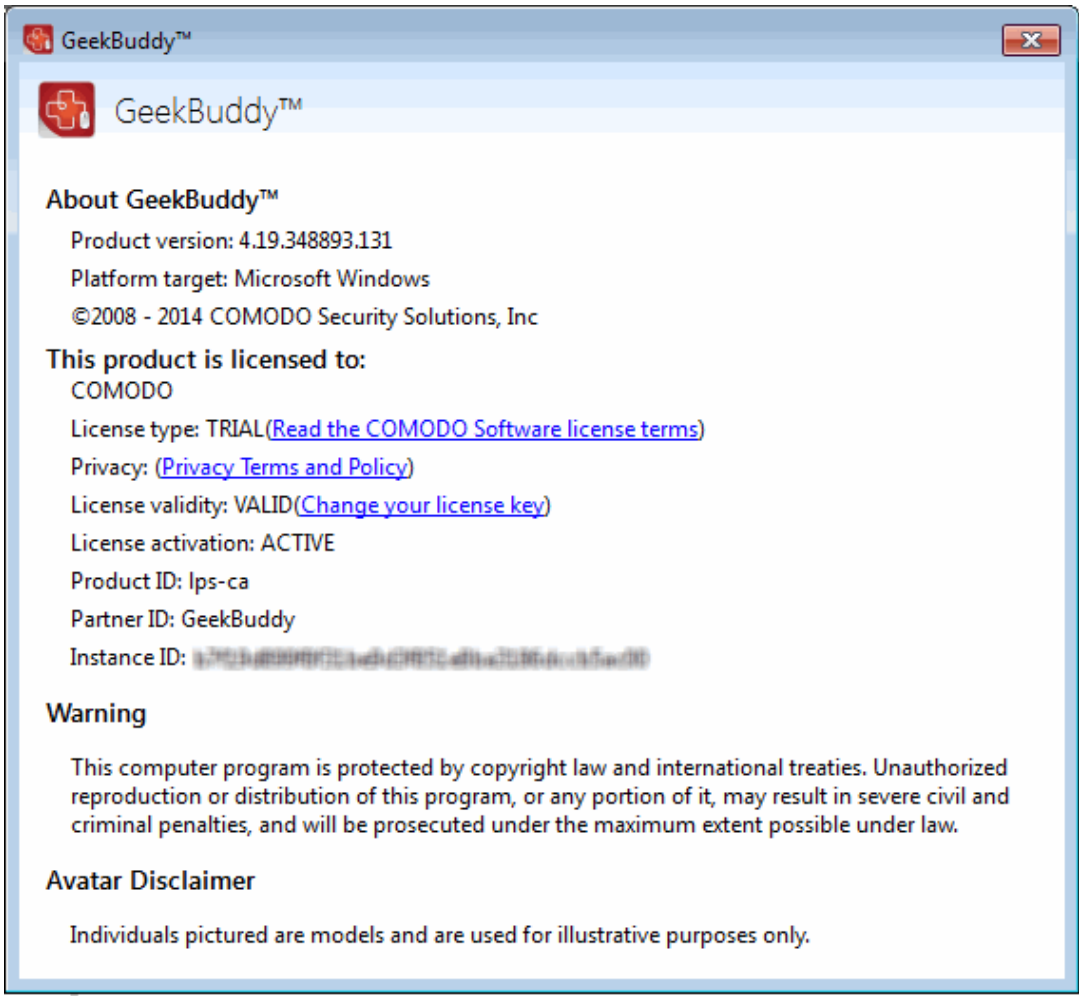
Start the GeekBuddy client by clicking the desktop shortcut icon  or from the 'Start Menu'.

The GeekBuddy Chat screen will be displayed.



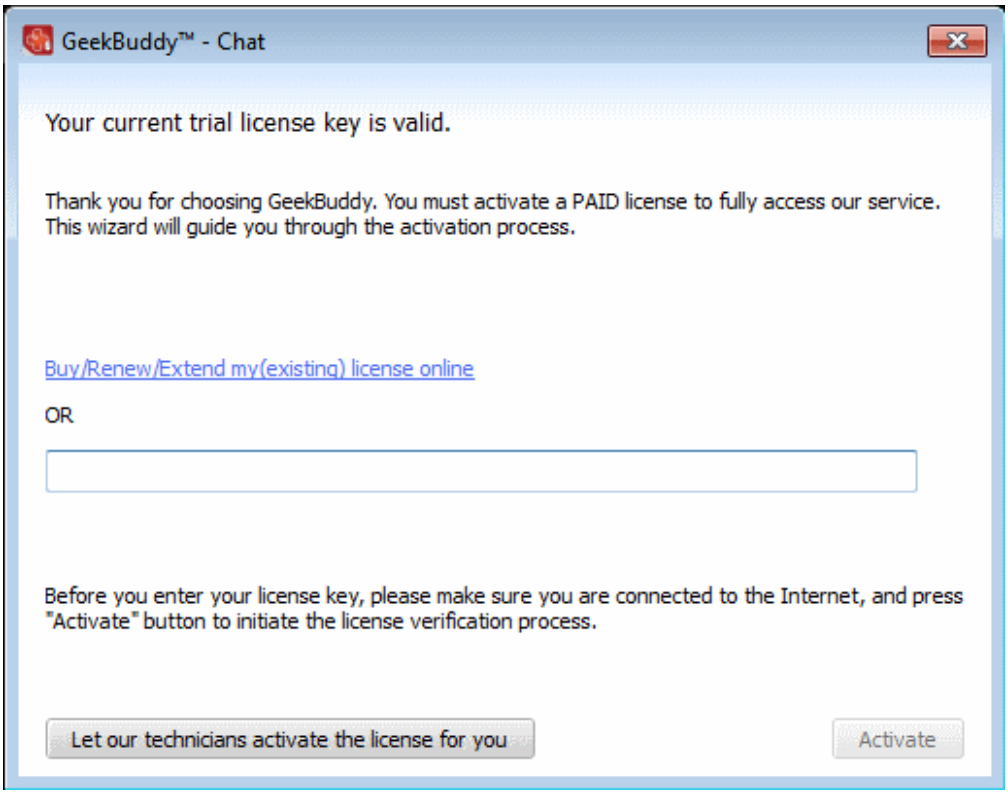
- Click the 'About' link at the top right of the screen.

The About GeekBuddy screen will be displayed.

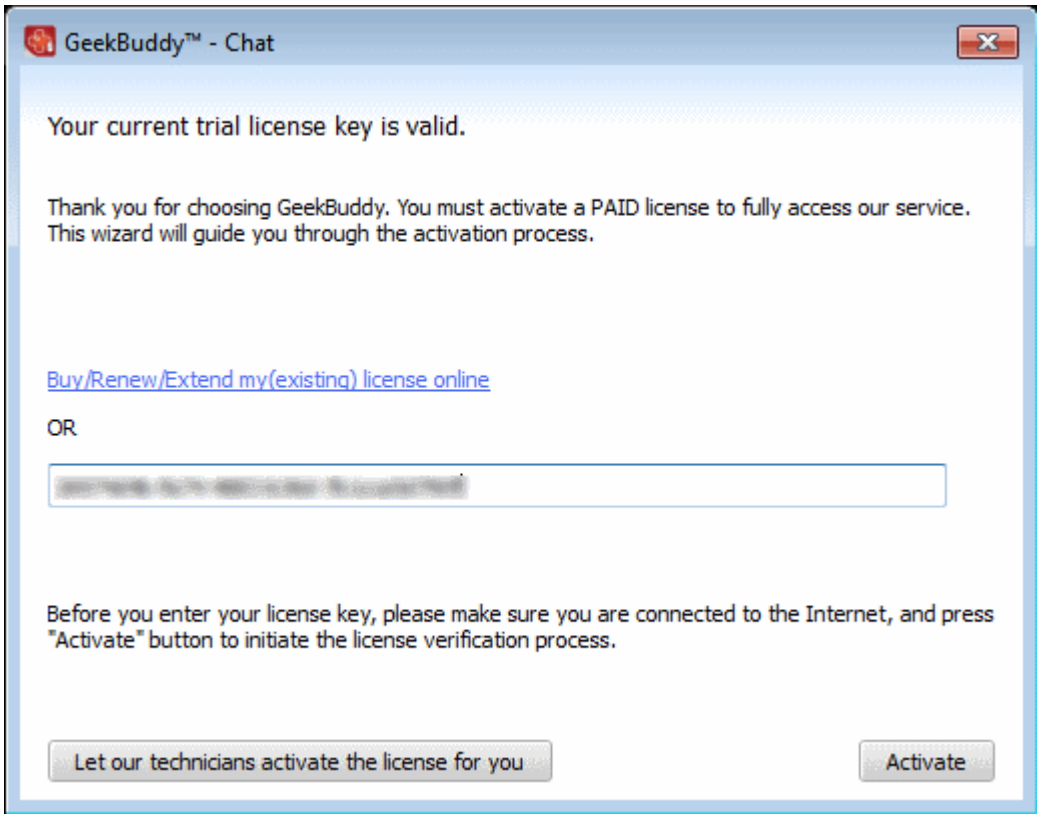


- Click the 'Change your license key' link in the screen.

The 'Activate your License' screen will be displayed.

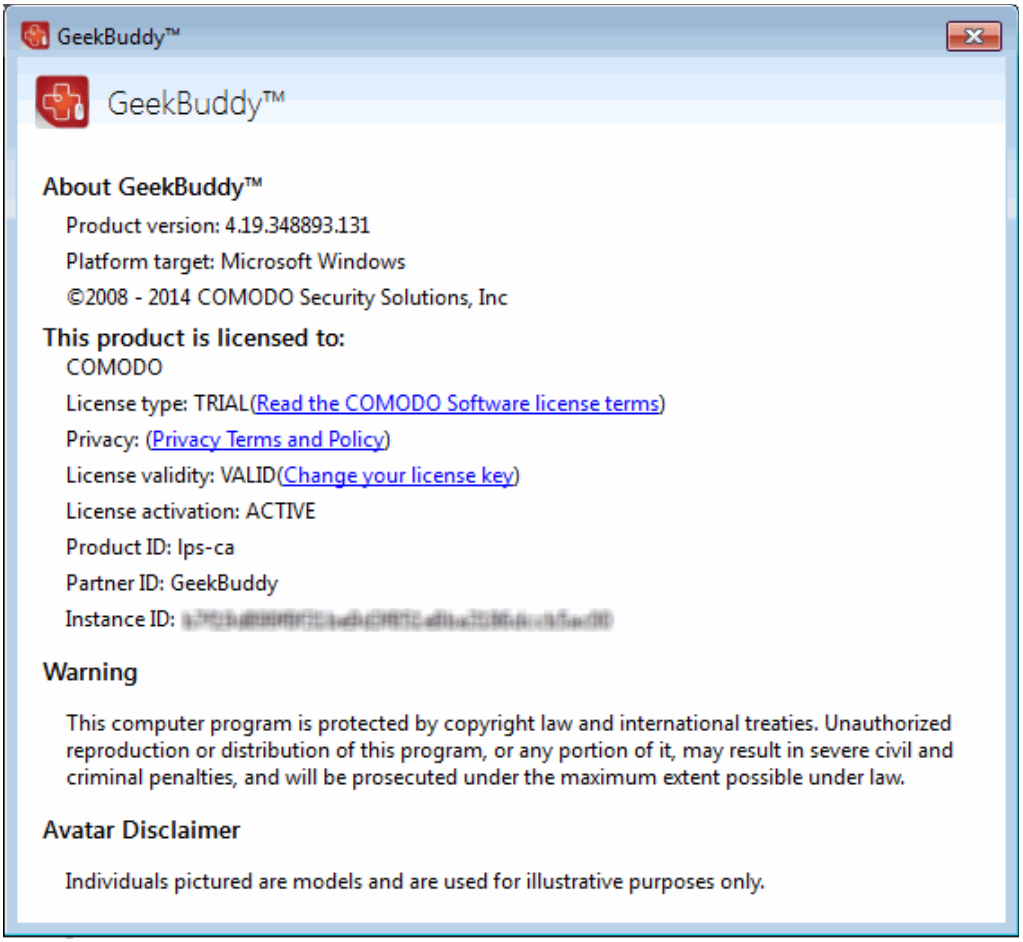


- Enter the License Key from your GeekBuddy retail package or the key you received through your email (for online purchases).



- Click the 'Activate' button or if you need more help on this click the 'Let our technicians activate the license for you' button.

The license key will be checked and if correct, the home screen will be displayed. To check whether the license is activated, you can view the 'About' dialog by clicking 'About' at the top right.



Now you can start using it and seek the help of an expert to resolve your computer problems.

Click the following links for more details on how to start and using them:

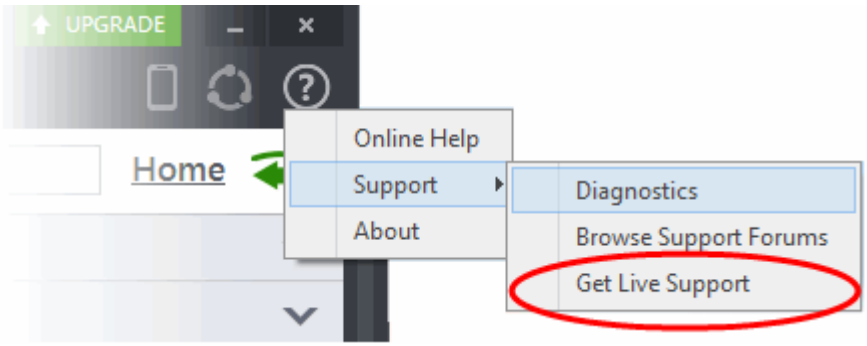
- **Launching the Client and Using the Service**
- **Using Free Diagnostic Reports**

7.3. Launching the Client and Using the Service

The GeekBuddy client required for the services is installed in your system automatically along with CIS Pro and Complete. For CIS Premium, it is installed automatically if you have selected the option Install Comodo GeekBuddy during installation .

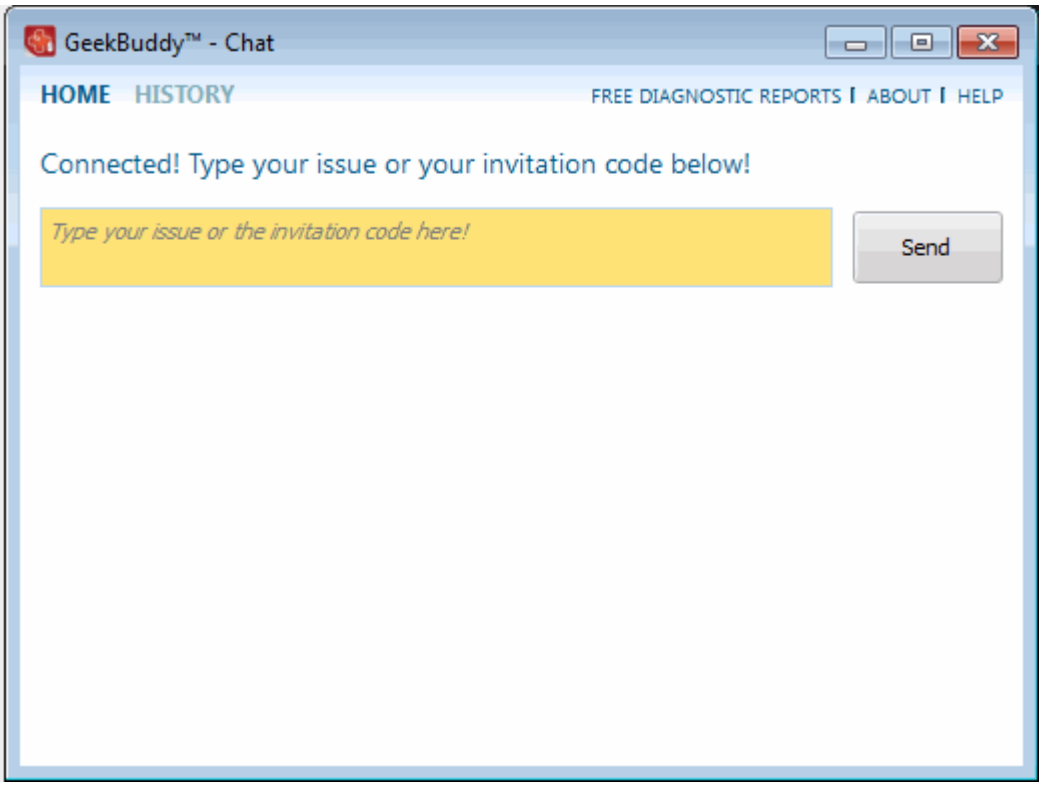
You can start the client and start a live chat session with a GeekBuddy expert using any one of the following methods:

- Double click the GeekBuddy desktop icon 
- Launch a chat with a qualified computer support technician by clicking Help > Support > Get Live Support at the top right side of the main interface.



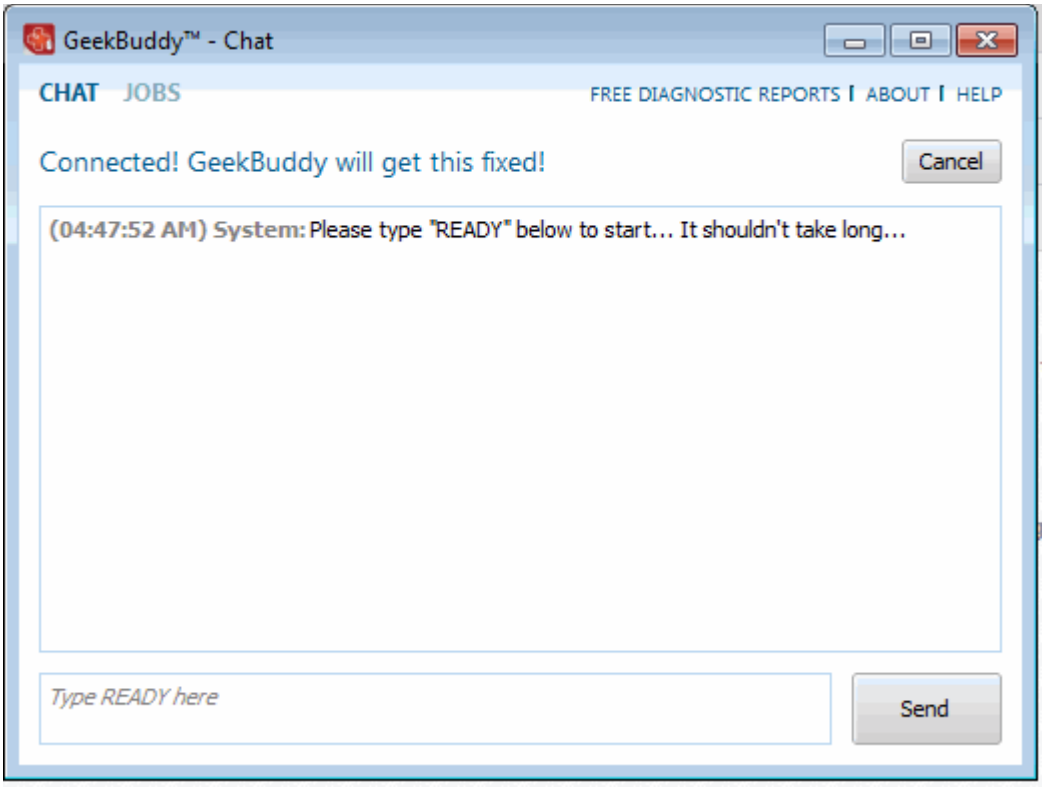
- Launch the GeekBuddy client directly from the Windows Start Menu - Click Start > All Programs > Comodo > GeekBuddy > GeekBuddy.

The GeekBuddy Home screen will open.

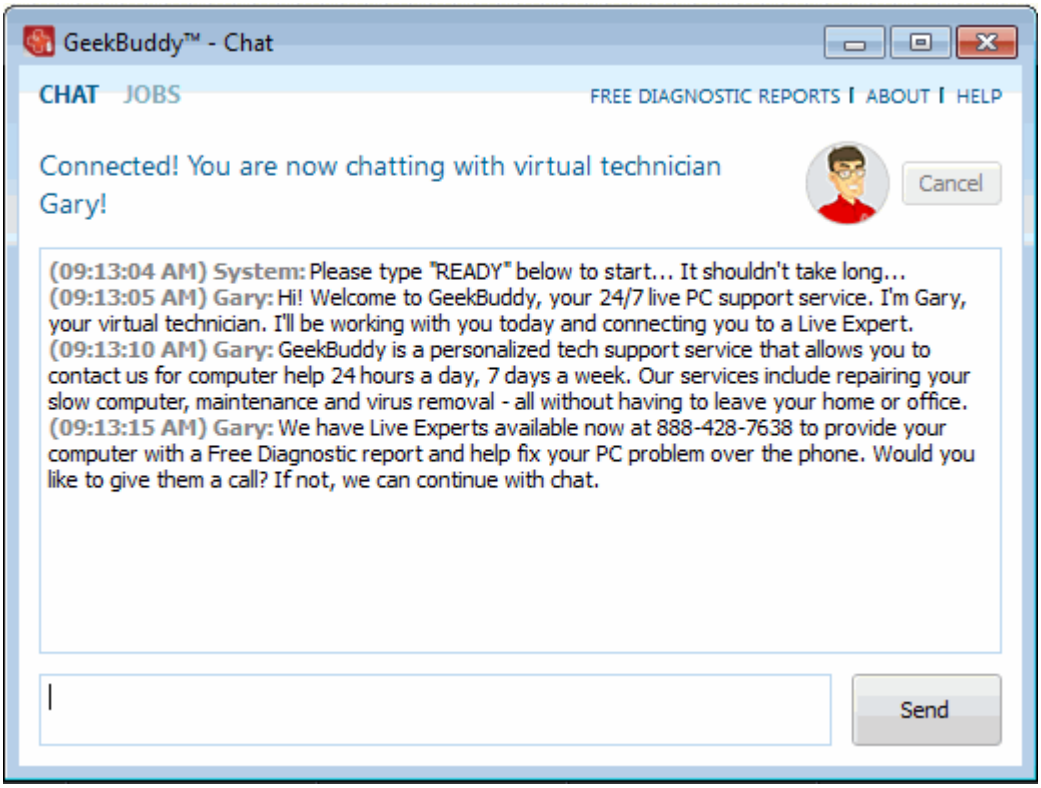


- To contact a support technician, type your issue in the field or enter the invitation code if you have it and click the 'Send' button.

You will be connected to a GeekBuddy…



...and once the connection is established, our support technician will initiate a chat with you.

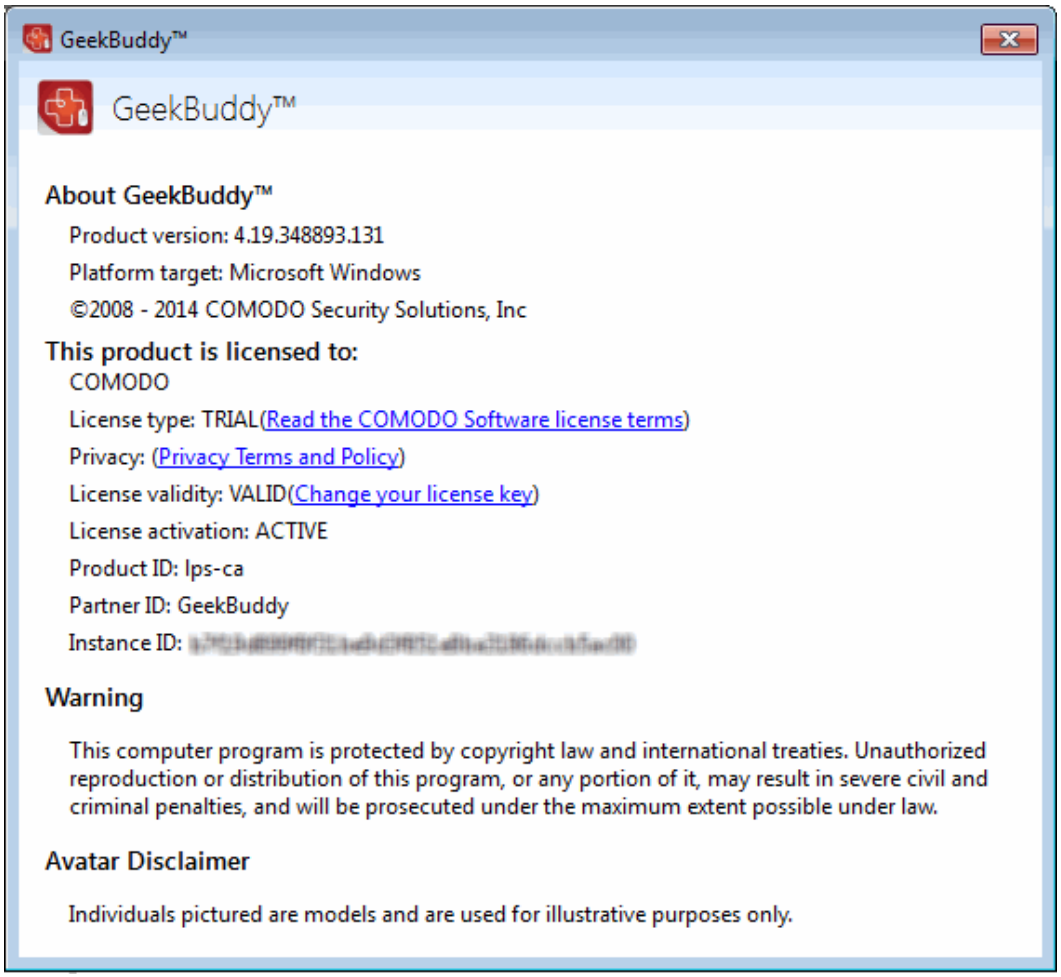


- Proceed to chat now.
- Explain your problem. The technician will assess your problem with you and work with you to fix any issues.

About GeekBuddy

- Click the 'About' link at the top far right of the screen.

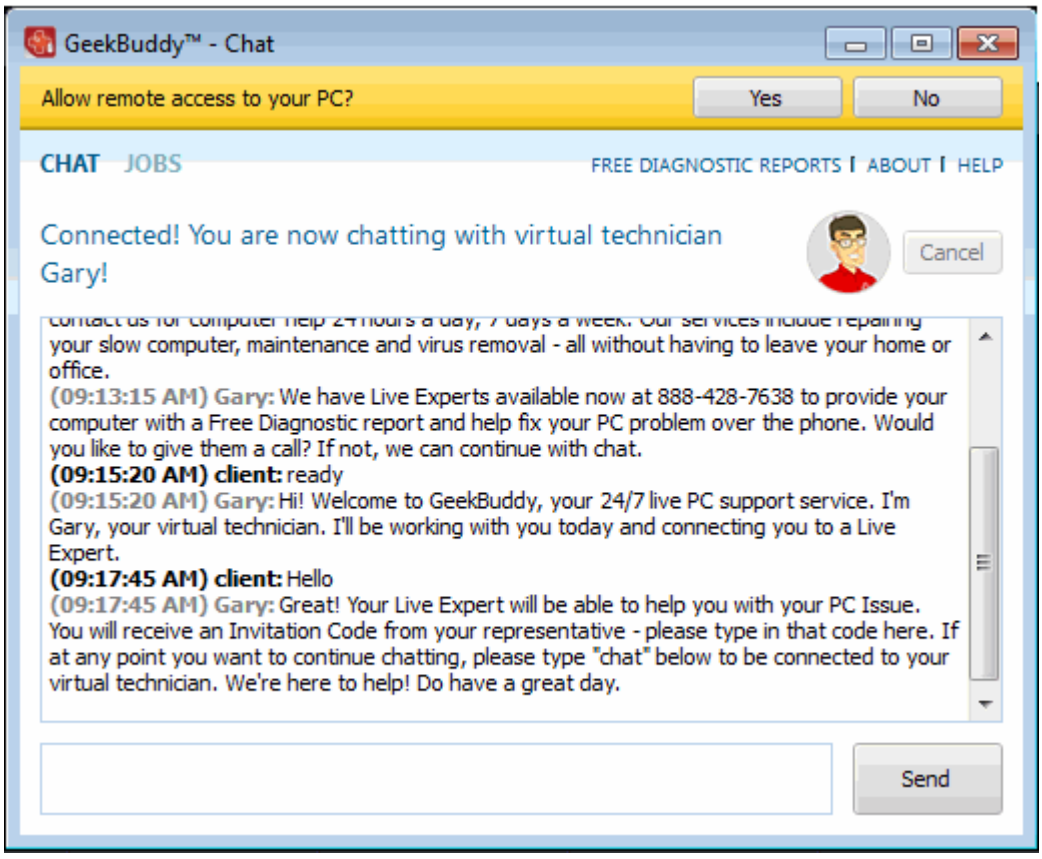
The About GeekBuddy information screen will be displayed.



The 'About' dialog displays the copyright and product version information. The screen also displays information about the licensee, its validity and to change the license key or activate the account.

7.4. Accepting Remote Desktop Requests

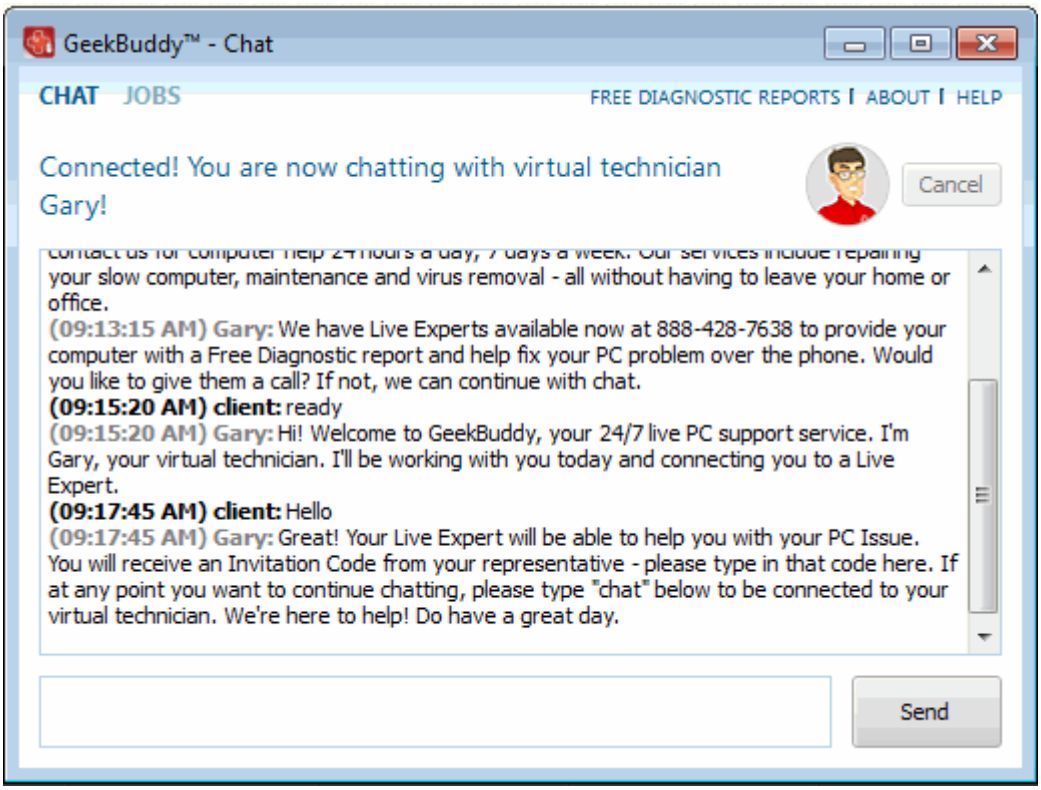
In order to solve certain issues, the support technician may need to directly connect to your computer via a remote connection. Remote control can only go ahead if you grant permission for this to happen. Our technicians will always request your permission via the chat window.



- Click the 'Yes' button at the top of the interface in order to allow the technician to connect to your computer.

The technician will ask your permission before he or she makes any changes to your machine. Such changes might include installing programs, creating system restore points or deleting unnecessary or infected files. You can approve the requests directly by typing your message and clicking 'Send'.

Upon completion of their work, the technician will disconnect from your computer, inform you that the requested tasks have been completed and ask whether you would like help with anything else.



- To disconnect the remote desktop session, click the 'Disconnect' button at the top and confirm it in the next screen to end the session with our GeekBuddy.

Congratulations, you just finished your first GeekBuddy support session. We hope you enjoy using your trouble-free computer.

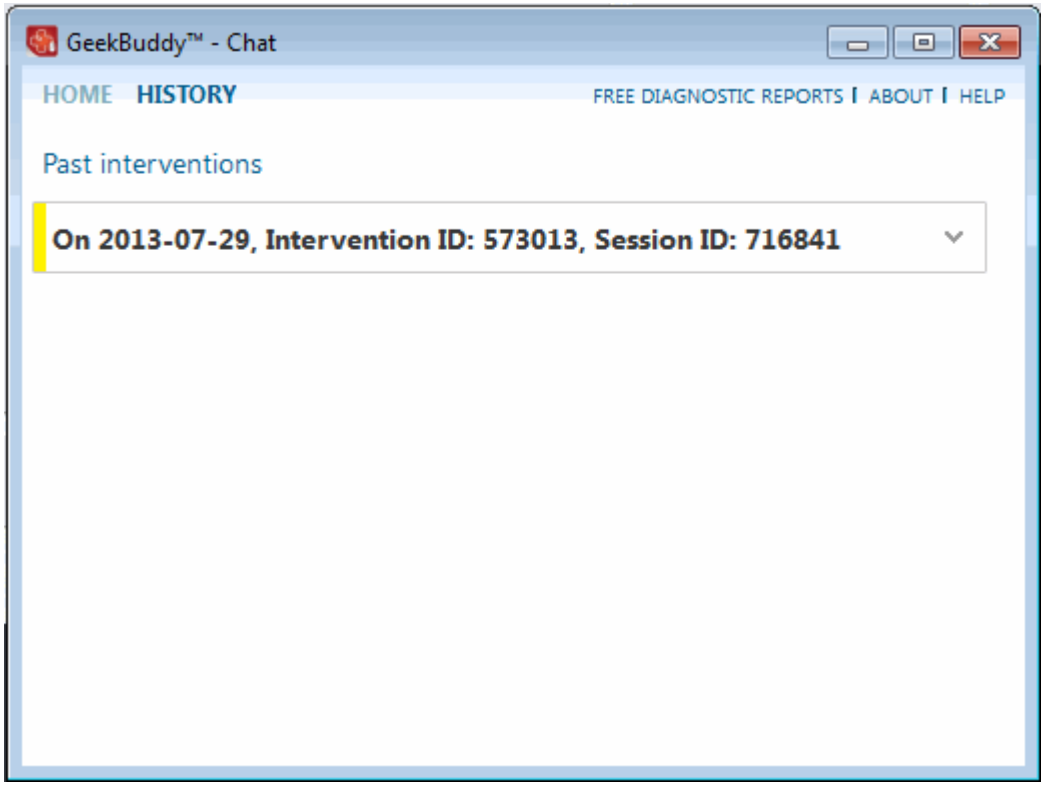
7.5. Chat History

GeekBuddy keeps a local record of every chat session you have with a Comodo technician. Clicking the 'History' link at the top of the interface will display all chat sessions that you had with our technician. This helps you keep track of previous computer issues and chats and can be useful as a reference when trying to fix future issues.

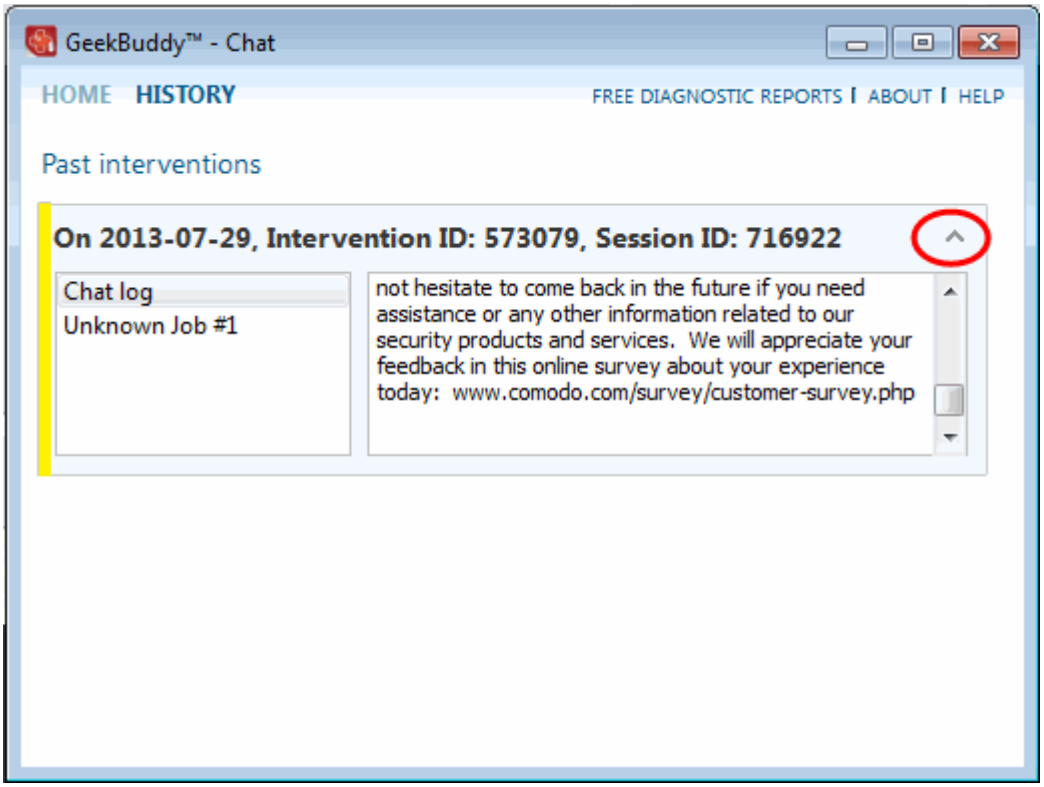
To view history of chat sessions

- Click the 'History' link at the top of the interface.

All the sessions will be displayed.



- Click on the arrow button at the far end of the session history box that you want to view or double-click anywhere on the box. The chat session that you had with our technician will be displayed on the right side.



- The chat session that you had with our technician will be displayed on the right side. Similarly you can view the chat history of other sessions also.

7.6. Using Free Diagnostic Reports

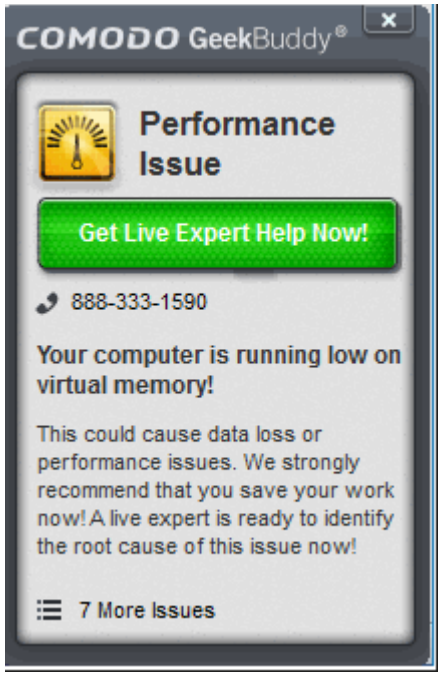
Free Diagnostic Reports helps you maintain the security and efficiency of your computer by automatically identifying problems on your computer and helping you to fix them. For example, Free Diagnostic Reports will alert you if you have too many startup programs/services (can cause computer slow down); an inefficient registry (can also cause slow down and crashes) or your hard drive contains files that might compromise your privacy. In many cases you will be presented with a simple wizard that will allow you to deal with the issue quickly and easily. If the problem is beyond the scope of Issuer Tracker, you will be offered the opportunity to contact a GeekBuddy representative who will help resolve the issues.

The Free Diagnostic Reports can be started in two ways:

- **From the Pop-up Alert**
- **From the GeekBuddy interface**

Popup Alert

At the time of starting your computer, Free Diagnostic Reports will detect problems in your system and provide an alert at the bottom right side of the screen.

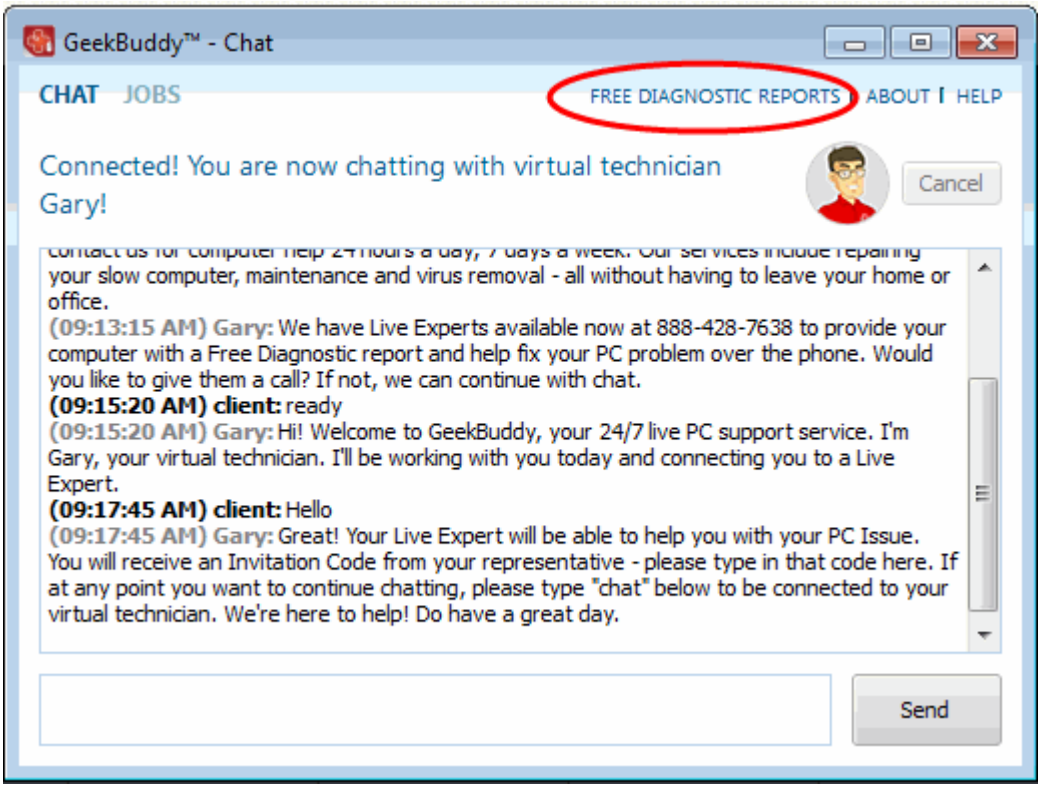


- Click the Fix issues to open the Free Diagnostic Reports interface.

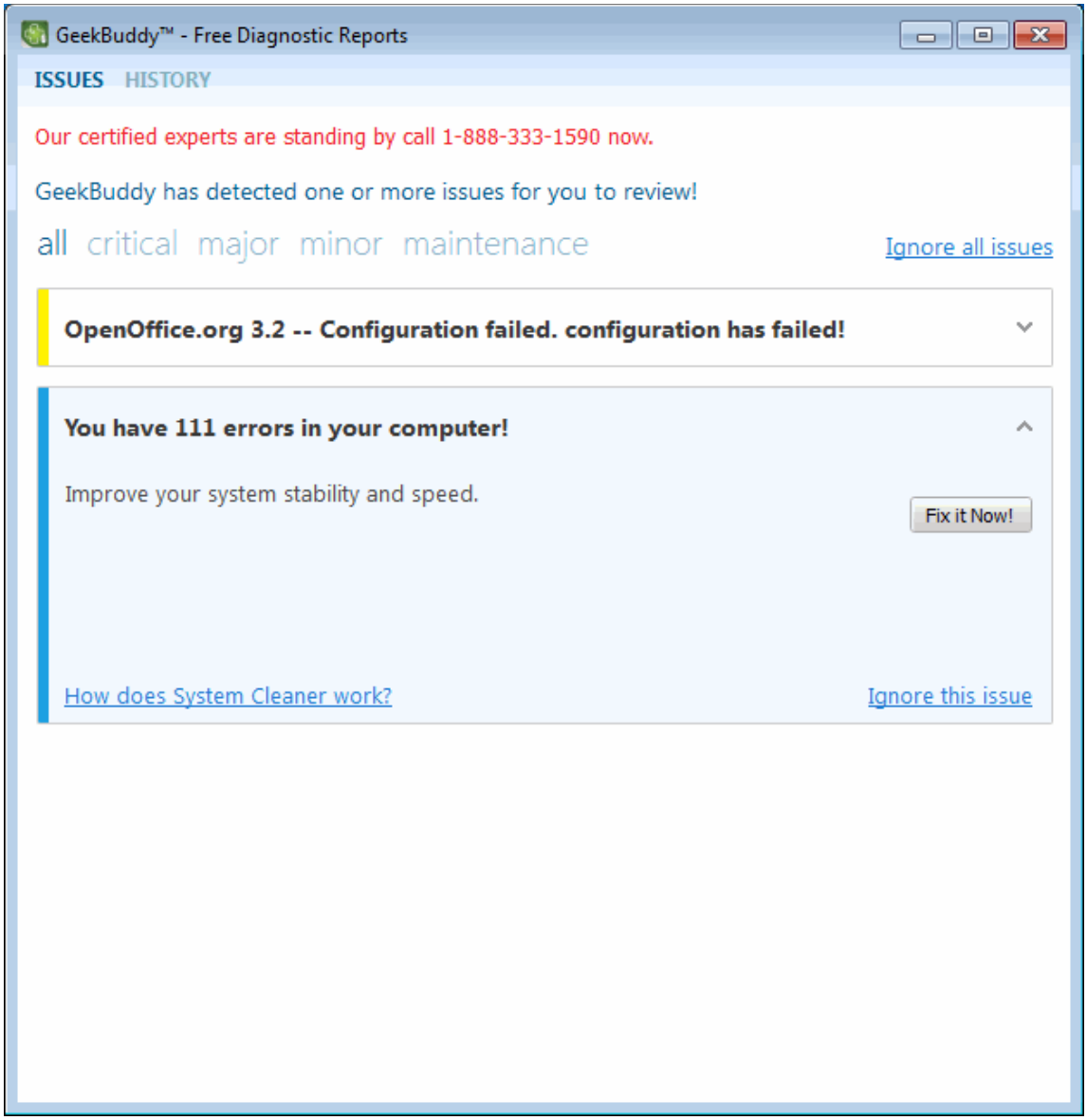
The Free Diagnostic Reports interface will list the problems that it has detected.

GeekBuddy Interface

To start the Free Diagnostic Reports, click the 'Free Diagnostic Reports' link on the right top in the user interface.



The Free Diagnostic Reports interface will list the problems that it has detected.



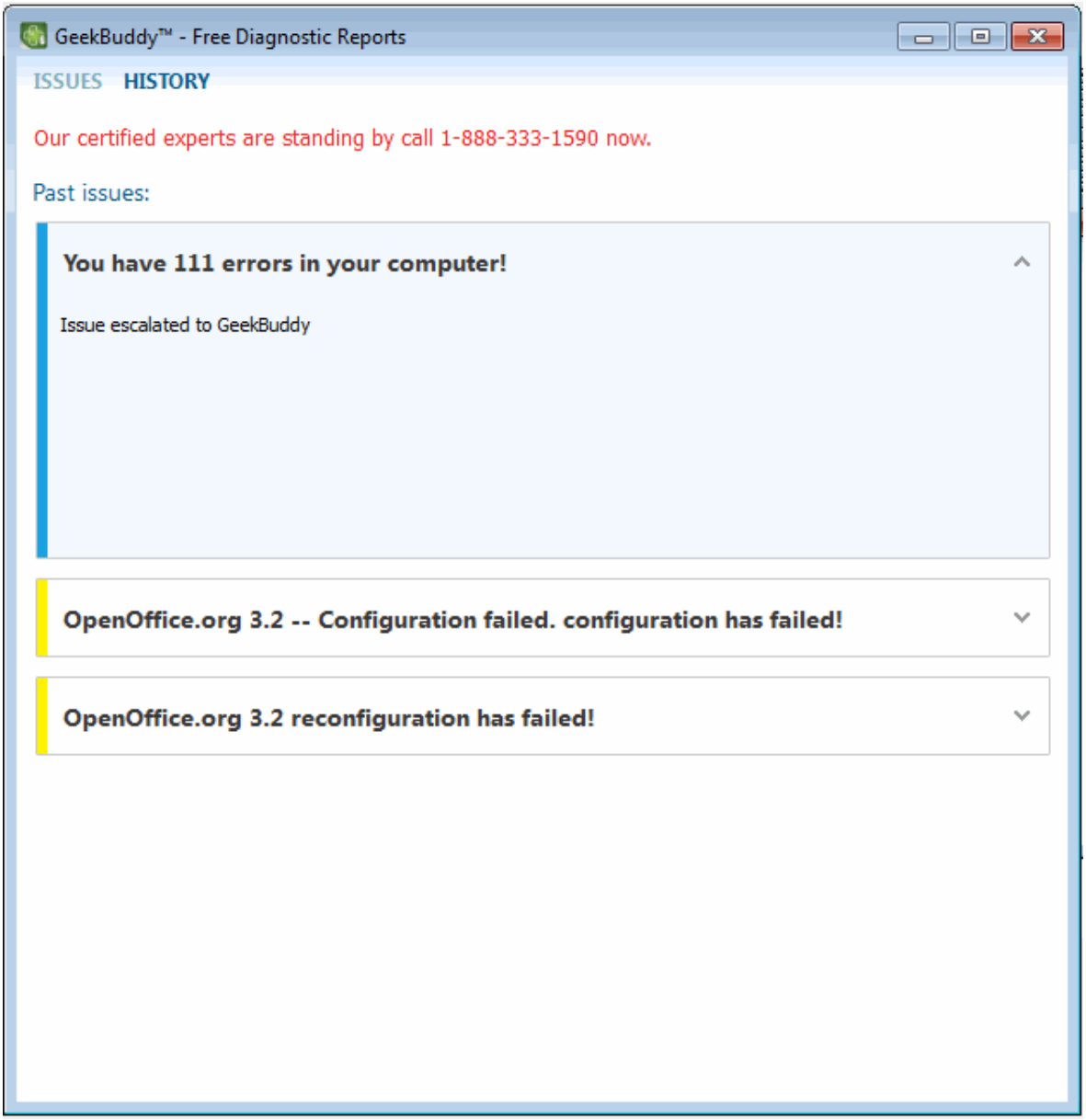
The problems detected will be categorized as critical, major, minor and maintenance issues. Click on the relevant link to view the problem. Clicking the 'All' at the top will display all the problems in your computer and the color code at the left of each issue indicates the category of the issue.

S. No.	Issue	Color Code
1	Critical	Red
2	Major	Orange
3	Minor	Yellow
4	Maintenance	Blue

Some of the common problems that occur in any computer are junk registry entries, slow bootup time and the presence of files that might compromise your privacy.

Each issue discovered will be accompanied with 'solution button' (e.g., 'Fix it Now!'). For example, to improve your system performance in your system and speed because of junk entries in your computer, click this button to resolve the issue by removing the junk entries.

The junk entries will be removed and the successfully completion screen will be displayed.



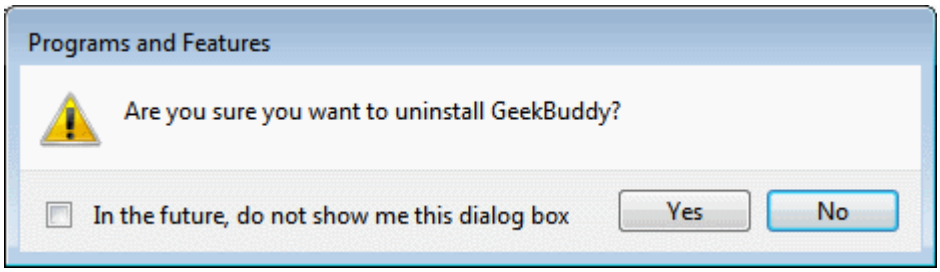
For some of the issues listed, you have to seek the help of an expert technician.

- Click 'Ignore all issues' link to disregard all the issues in your system displayed by Free Diagnostic Reports.
- Click 'Ignore this issue' beside a particular entry to disregard that problem.
- Click 'History' link at the top of the interface to view the actions taken for the problems.
- Click the 'Fix it Now!' button beside an issue to resolve it.

7.7. Uninstalling Comodo GeekBuddy

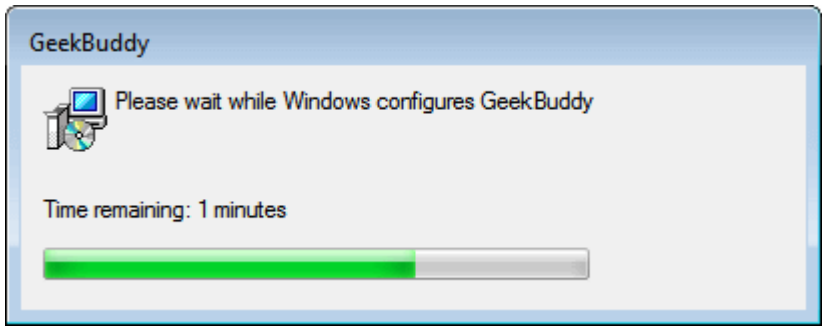
To uninstall Comodo GeekBuddy

- From the Windows Start menu, click 'Control Panel' > 'Programs' > 'Programs and Features' > 'Uninstall a Program'
- From the list of currently installed programs, Select 'GeekBuddy' and click 'Uninstall' at the top. A confirmation dialog will be displayed.



- Click 'Yes' to confirm uninstallation.

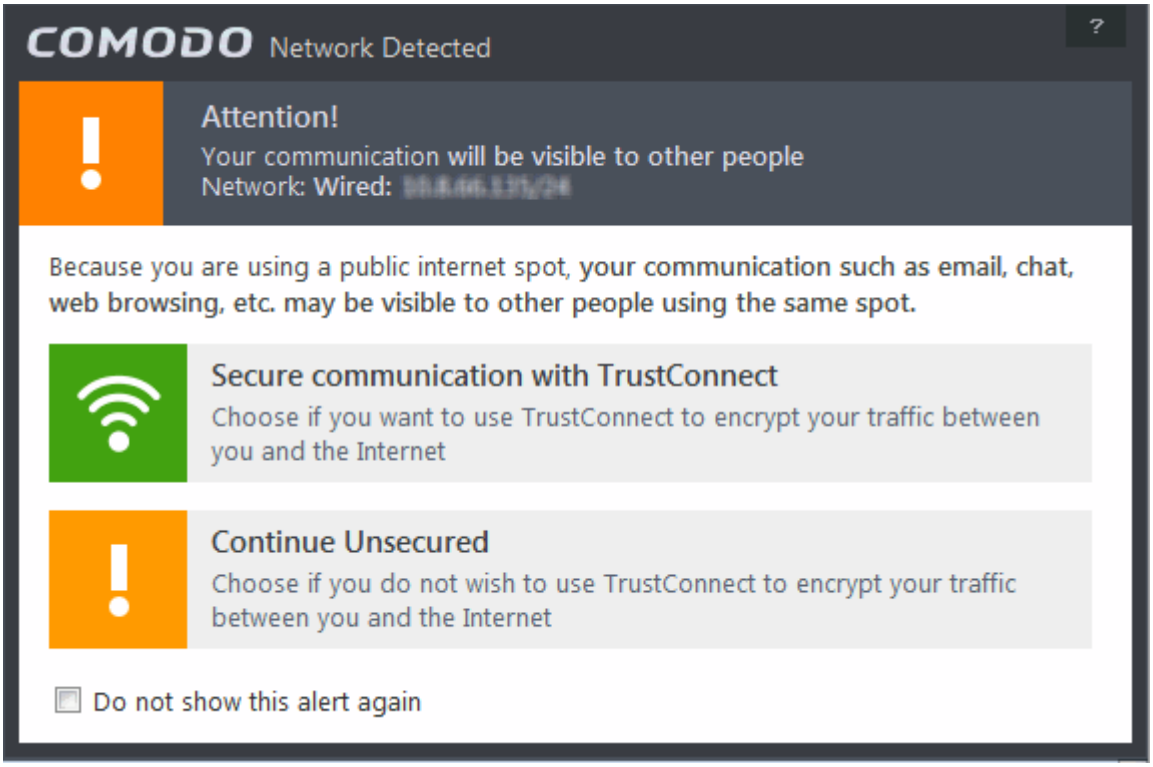
The progress of GeekBuddy removal will be displayed...



... and in a few seconds the uninstallation will be complete.

8. TrustConnect Overview

Comodo TrustConnect is a secure Internet proxy service that creates an encrypted session when users are accessing the Internet over public wireless connections. Since these wireless sessions can be relatively easily intercepted, they present a significant data vulnerability gap for businesses and consumers alike. Whenever Comodo Internet Security detects unsecured wireless connections it will present you with the opportunity to use your TrustConnect account for the connection.



TrustConnect is designed to eliminate these types of data hijacks by preventing criminals from attacking or scanning your system from the local network that you are using to connect to the Internet. It also encrypts all of your traffic destined for the Internet (including Web site addresses, instant messaging conversations, personal information, plain text usernames and passwords and other important information). After connecting to the service, the TrustConnect software indicates that traffic is being encrypted as it leaves your system. Data thieves and hackers cannot 'sniff' or intercept your data - they can't even determine where your information is coming from because, as you are connecting to the Internet through a SSL secured VPN connection to the TrustConnect servers, your requests appear to come from our IP address. Ordinarily, cyber criminals could easily intercept these broadcasts.

Setting up Comodo TrustConnect is easy, as it works on most operating systems (Windows, Mac OS X) as well as with most firewall applications. Typical setup takes less than three minutes. TrustConnect clients are available for Windows, Mac OS, Linux and iPhone mobile devices and can be downloaded by logging into your account at **https://accounts.comodo.com/account/login**. Your Comodo Internet Security Complete confirmation email contains confirmation of your the username that you set up during initial sign up and a subscription ID for the service. Once logged in, click the TrustConnect tab to add subscriptions, change billing and contact information, and review the ongoing status of your service. Your Comodo Internet Security Complete TrustConnect account has a 10 GB/month data transfer limit.

Comodo Internet Security - Complete customers also receive the $99 value 'Live, Expert Computer Support' Comodo GeekBuddy. Please visit **http://www.geekbuddy.com** for full product details.

TrustConnect System Requirements

- Windows 8
- Windows 7
- Windows Vista
- Windows XP
- Mac OS X
- Linux (containing kernel 2.4 or later)
- FreeBSD, OpenBSD

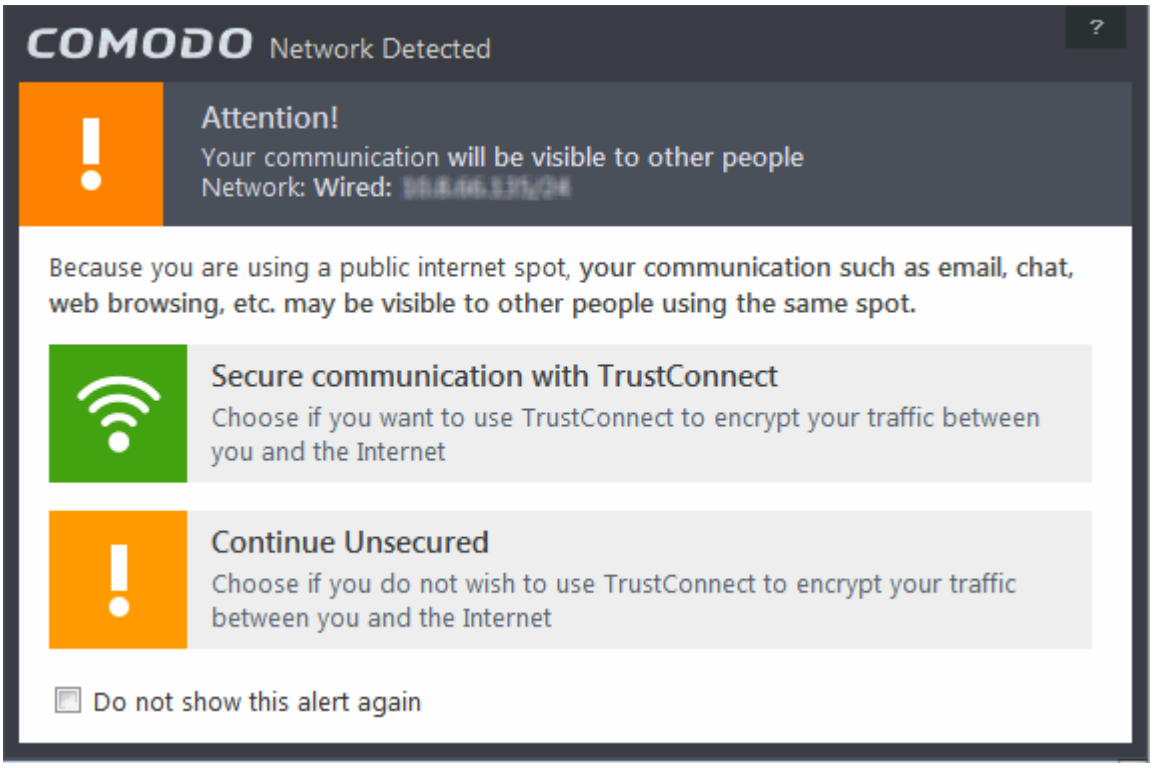
For users of Comodo Internet Security - Complete, TrustConnect is integrated with the application and need not install the TC client in their systems.

Comodo Internet Security Complete Users

CIS Complete product includes TrustConnect service and the application is installed automatically along with CIS. When a new wireless connection is established by your system, a Network Detected dialog will be displayed.

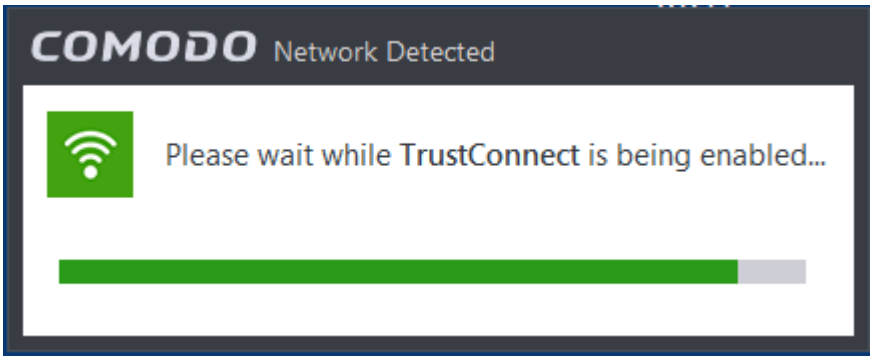
- Select your location from the dialog

A TrustConnect alert will be displayed depending on the settings configured in **Firewall Settings** interface.

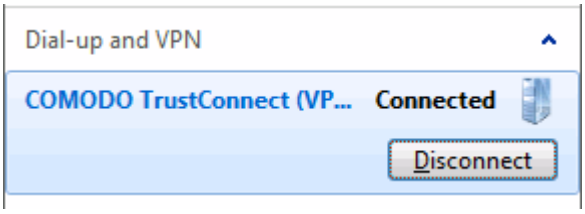


Select whether you want to connect to the Internet via TrustConnect thus encrypting the traffic between your system and the Internet or use the unsecured network.

If you choose 'Secure communication with TrustConnect', CIS will establish the connection via TC...



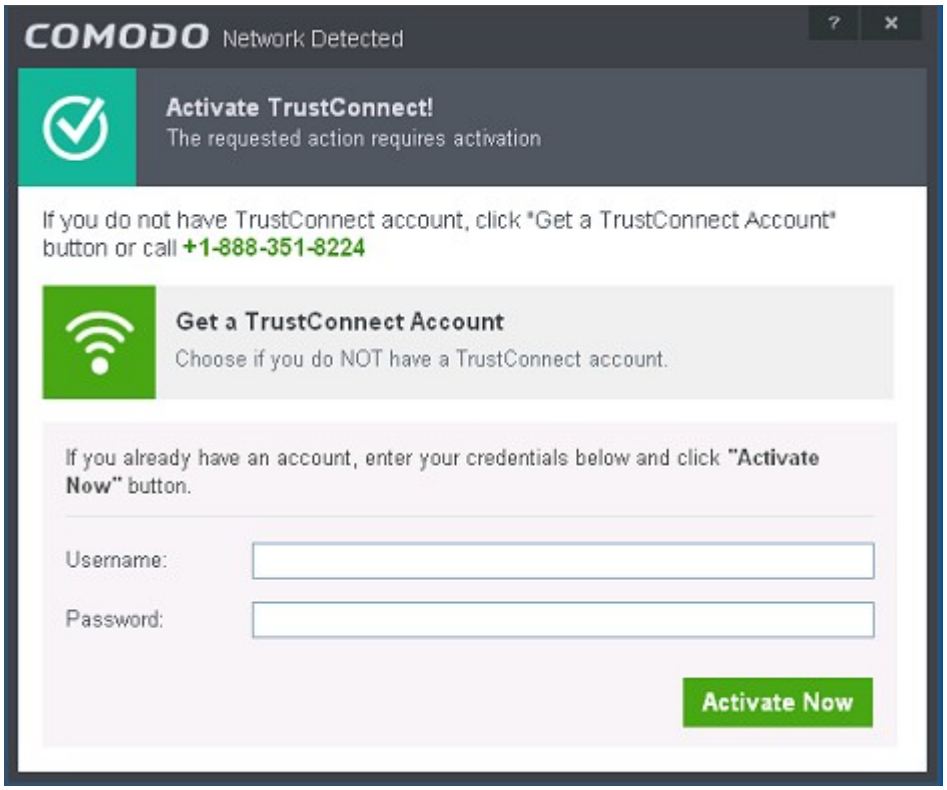
...and on successful connection, you can view the details in the system tray.



Choose 'Continue Unsecured' option if you do not want to establish an encrypted connection.

Comodo Internet Security Pro / Premium Users

TrustConnect service is not included with CIS Pro / Premium and these users should subscribe for using the service. When the option 'Secure communication with TrustConnect is selected, an 'Activate TrustConnect' dialog will be displayed.

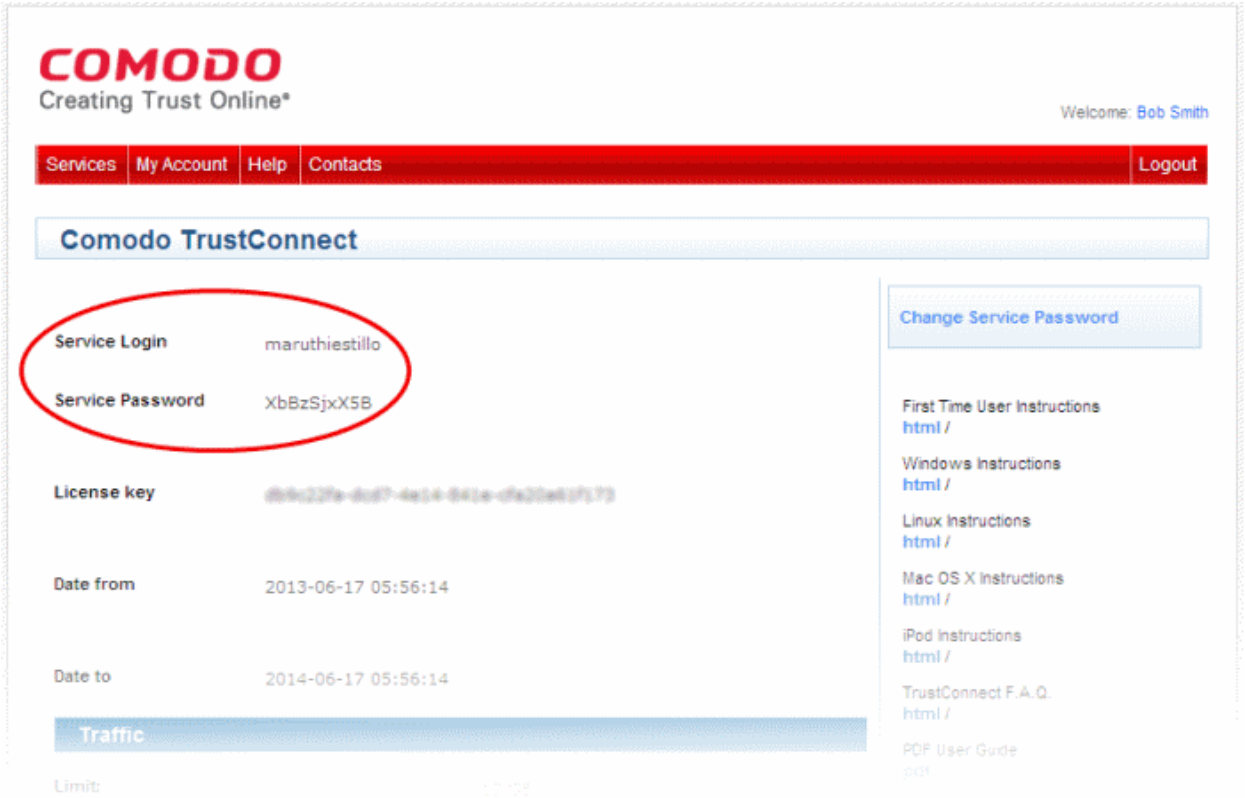


- You can purchase the TC service by clicking the 'Get a TrustConnect Account', enter the TC service credentials and activate the service.
- If you already have a TC account, enter the TC service credentials in the Username and Password fields and click the 'Activate Now' button.

To find your TC service credentials

- In the **https://accounts.comodo.com/** page login to your CAM account using the CAM username and password sent via email at the time of account creation.
- Click 'TrustConnect' in the menu bar or in the drop down from 'Services' tab.

The account details of your TC service will be displayed.



The TC Service Login and Service Password for your account should be entered in the Username and Password fields respectively in the 'Activate TrustConnect dialog.

Please note that this activation dialog will appear only for the first time you are trying to connect via TC. After the activation process is successfully completed, subsequent attempts to connect via TC to the Internet will be automatically established.

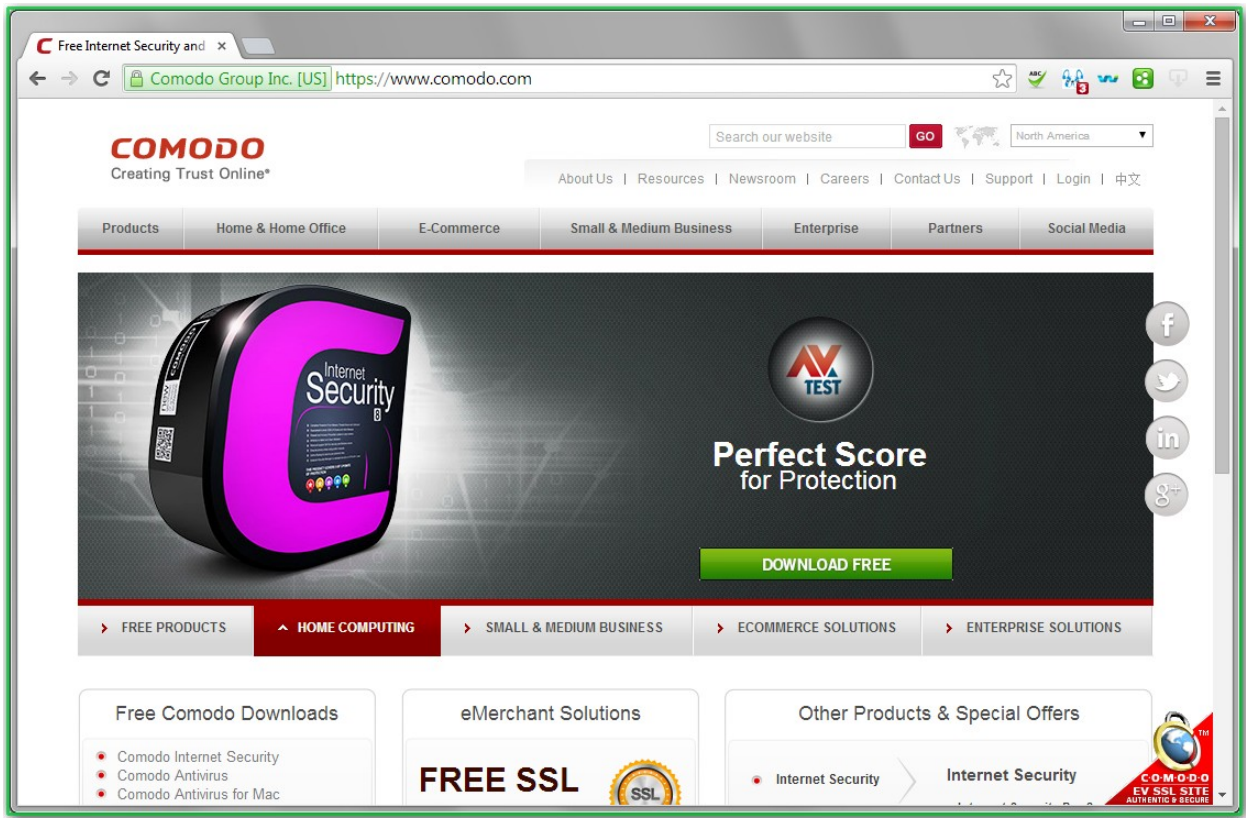
9. Chromodo Browser

Chromodo is a fast and versatile Internet Browser based on Chromium and infused with Comodo's unparalleled level of security.

To help make your Internet browsing experience even safer, Chromodo is installed on your computer as a part of Comodo Internet Security. Chromodo provides the complete complement of features offered by Chromium with superior security and

privacy.

- **Chromodo Features**
- **Starting Chromodo**
- **Chromodo Help**



Features:

- Improved Privacy over Chromium
- Lightning Fast Page Load Times
- Instantly Scan Web Pages for Malware with Web Inspector
- Built-in Media Downloader Allows You To Quickly Save Streaming Video
- PrivDog Extension Automatically Blocks Web Site Trackers
- Greater Stability and Less Memory Bloat
- Incognito Mode Stops Cookies, Improves Privacy
- Very easy to switch from your current browser to Chromodo

Chromodo Security:

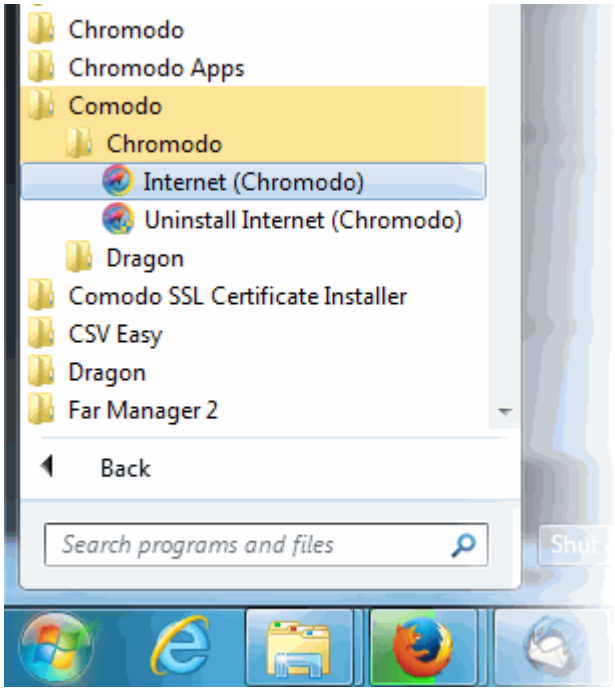
- Has privacy enhancements that surpass those in Chromium's technology
- Has Domain Validation technology that identifies and segregates superior SSL certificates from inferior ones
- Stops cookies and other Web spies
- Prevents all Browser download tracking to ensure your privacy

Starting Chromodo

Chromodo is installed in your computer along with Comodo Internet Security. You can start the browser in two ways:

From the Start menu:

- Click *Start* > *All Programs* > *Comodo* > *Chromodo*> *Internet (Chromodo):*



From the Desktop Icon:

- Double Click on the Chromodo Desktop icon created during the installation:

Chromodo Help

Full details on the use of Chromodo can be found in the online guide at **https://help.comodo.com/topic-249-1-593-6704-Chromodo-Browser---Introduction.html**

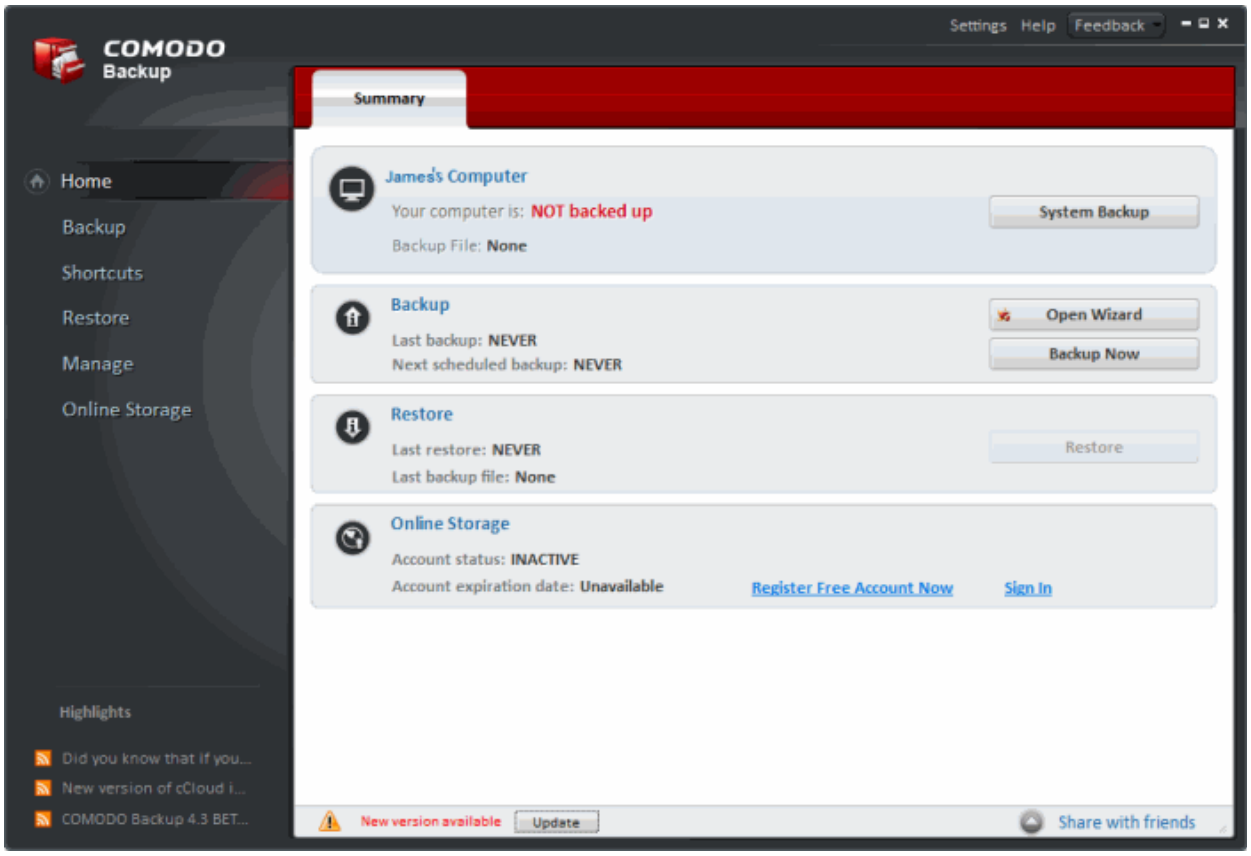
10. Comodo BackUp

Comodo BackUp is a powerful and easy to use desktop application that helps home and business users protect their valuable data against damage or loss. CIS Complete package includes Comodo BackUp with 50 GB of online storage space.

The application's streamlined design and task orientated architecture means even novice users can learn how to create, run and restore their first backup job in a matter of minutes. Other features include full scheduling, password protection, a backup integrity checker and a range of preset backup jobs that allow you to quickly create copies of important data sets such as the Windows Registry, mail accounts and user settings.

Comodo BackUp is also seamlessly integrated to Windows Explorer so that you can just select the folders or files you want to back up, right click on them and quick start the Back Up wizard.

- **Comodo Backup Features**
- **Starting Comodo Backup**
- **Comodo Backup Help**



Comodo Backup Features and Benefits

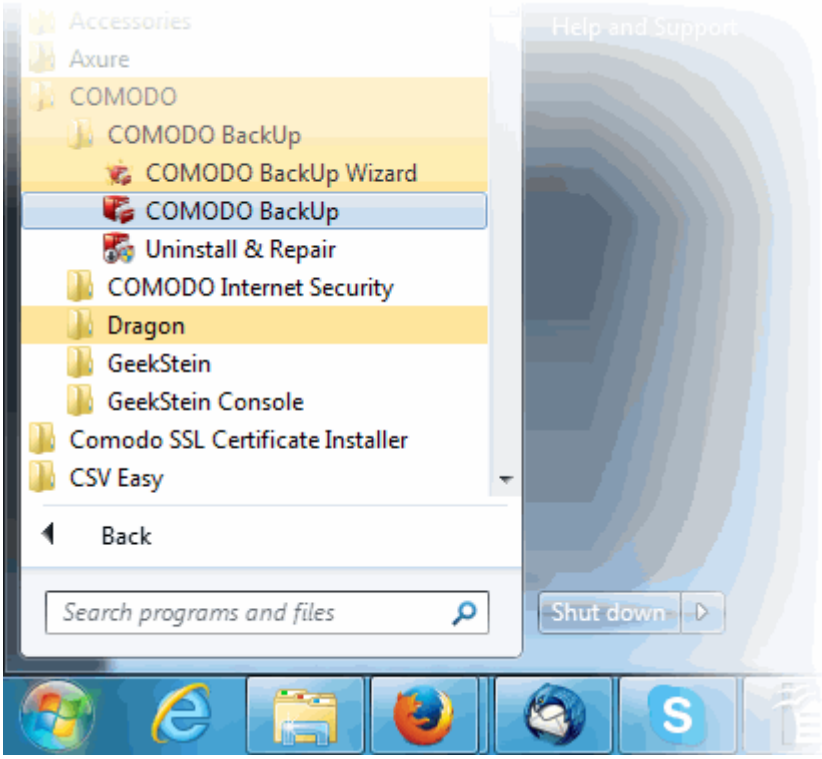
- **Quick backup** of entire drives or individual files or folders to your local computer, network drive, FTP server or Comodo's online server.
- **Step by step wizards** to guide even novice users through the entire backup, restore and scheduling procedures.
- **Flexible storage options** allow you to specify full, incremental or differential backups.
- **Protection** of invaluable personal and business data from loss or corruption.
- **Quick recovery** of files with a few clicks of the mouse.
- **Granular scheduling options** to take automatic backups at a time that suits you.
- **Real-time backups** synchronization feature to get your files copied over as soon as you save them.
- **Built in checker** to confirm the integrity of your backup files before committing to a restore.
- **Backup presets** including mail folders, windows registry, messenger archives and master boot records.
- **Powerful encryption options** to protect your files so that it cannot be accessed by anyone but you.
- **Comodo Cloud -** online file storage service. Backup your files to a highly secure online storage which can also be mounted as a virtual drive in your system.

  CIS Complete package includes 50 GB of online storage space at Comodo's online server. You can log-in to your online storage account with the user name and password that you entered during CIS Complete Registration process. Refer to **Activating Your License** for more details.
- **Command line and scripting support** to automate the online backup and restore operations.

Starting Comodo Backup

From the Start Menu

- Click Start > All Programs > COMODO > COMODO Backup > COMODO Backup:



From the Destop Icon:

- Double Click on the Comodo Backup Desktop icon created during the installation:

Comodo Backup Help

Comodo BackUp's streamlined interface provides fingertip access and control over all functional areas of the software. Please refer to the Comodo Backup online help guide at **http://help.comodo.com/topic-9-1-455-4910-Comodo-BackUp-Introduction.html** for more details on using the product.

Appendix 1 - CIS How to... Tutorials

The 'How To...' section of the guide contains guidance on key tasks of Comodo Internet Security. Use the links below to go to each tutorial's page.

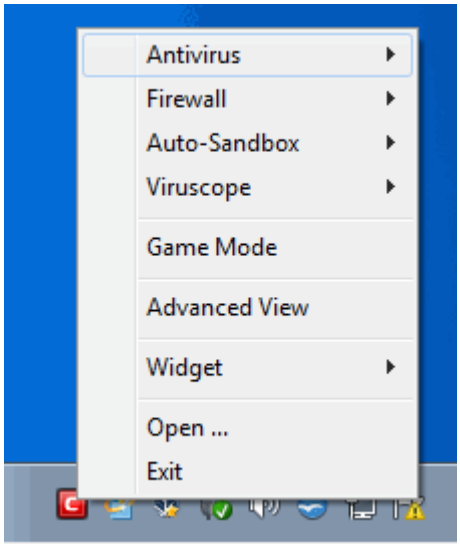
How to...:

- **Enable / Disable AV, Firewall Auto-Sandbox and Viruscope Easily** - Guidance on changing the current enabled/disabled states of Antivirus, Firewall and Defense+.
- **Setup the Firewall for maximum security and usability** - A brief outline of the setting up a secure connection to Internet
- **Block Internet Access while allowing local network (LAN) Access** - guidance on configuring the Firewall to allow only Intranet or LAN connection and to block Internet connection
- **Block/allow websites selectively to users of your computer** - guidance on configuring website filtering rules for different users to selectively allow or block specific websites to them
- **Setup HIPS for maximum security and usability** - A brief outline of how to set Host intrusion Protection for the optimum balance between security and usability

- **Create Rules for Auto-Sandboxing Applications** - A brief outline of how to set create auto-sandbox rules for the maximum security against untrusted applications
- **Password protect your CIS settings** - Explains how to protect your CIS settings
- **Reset a Forgotten Password (Advanced)** - Explains how to create a new password for CIS
- **Run an instant Antivirus scan on selected items** - Guidance on initiating a manual scan on selected folders/files to check for viruses and other malware.
- **Create an Antivirus scanning schedule** - Guidance on time-table scheduling of antivirus scans to be run on selected items at selected intervals
- **Run an untrusted program inside sandbox** - Guidance on executing a program that you do not trust to be safe, inside sandbox to protect any harmful effects of the program upon your system.
- **Run Browsers inside Sandbox** - Guidance on running your browser, inside sandbox when you plan to visit untrusted websites.
- **Run Untrusted Programs inside Virtual Desktop** - Guidance on executing a program that you do not trust to be safe, inside the virtual Desktop.
- **Run Browsers Inside the Virtual Desktop** - Guidance on running your browser, inside virtual Desktop when you plan to do online banking, online shopping and so on.
- **Restore incorrectly quarantined item(s)** - Help to restore files and executables that were moved to quarantine by mistake
- **Submit quarantined items to Comodo for analysis** - Advice on how to send suspicious files/executables to Comodo for analysis
- **Enable file sharing applications like BitTorrent and Emule** - Explains how to configure Comodo Firewall for file sharing through popular software
- **Block any downloads of a specific file type** - Explains how to configure Defense+ to block downloads of files of a specific type
- **Disable Auto-Sandboxing on a Per-application Basis** - Explains how to exclude specific files or file types from the auto-sandboxing process
- **Switch between complete CIS suite and individual components (just AV or FW)** - Explains how to uninstall or install Firewall or Antivirus components after installation.
- **Switch Off Automatic Antivirus and Software Updates** - Explains how to stop automatic software and virus updates
- **Temporarily suppress alerts when playing games** - Helps you to switch off CIS pop-up alerts to avoid interruptions while playing games
- **Renew or upgrade your license** - Explains how to renew or upgrade your license
- **How to use CIS Protocol Handlers** - Explains how to use CIS protocol handlers

Enable / Disable AV, Firewall Auto-Sandbox and Viruscope Easily

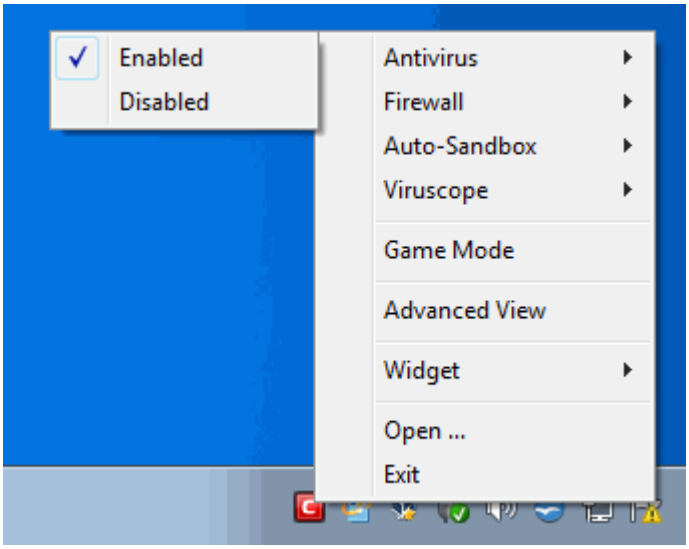
Comodo Internet Security allows users to quickly enable or disable **Antivirus**, **Firewall**, **Auto-Sandbox** or **Viruscope** by right-clicking on the system tray icon. Note - the CIS interface should be in **Compact View**.



Antivirus

To enable/disable the Antivirus

1. Right click on the system tray icon keeping the CIS interface in Compact View.
2. Move the mouse cursor over 'Antivirus'



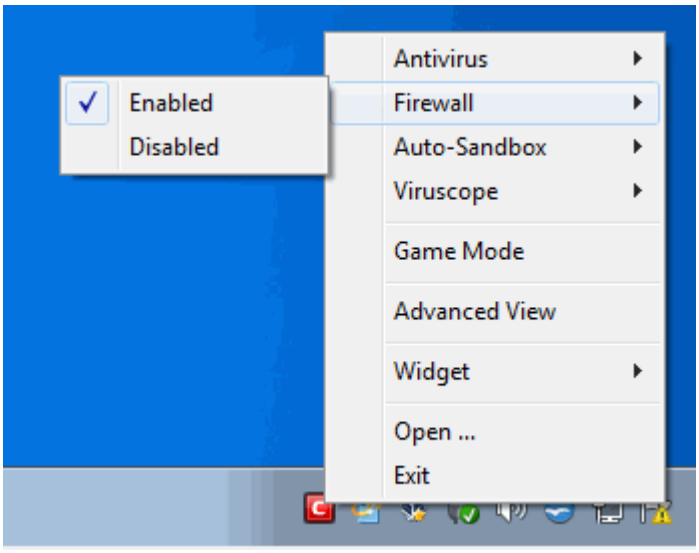
3. Choose 'Enabled' or 'Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Firewall

To enable/disable the Firewall

1. Right click on the system tray icon keeping the CIS interface in Compact View
2. Move the mouse cursor over 'Firewall'



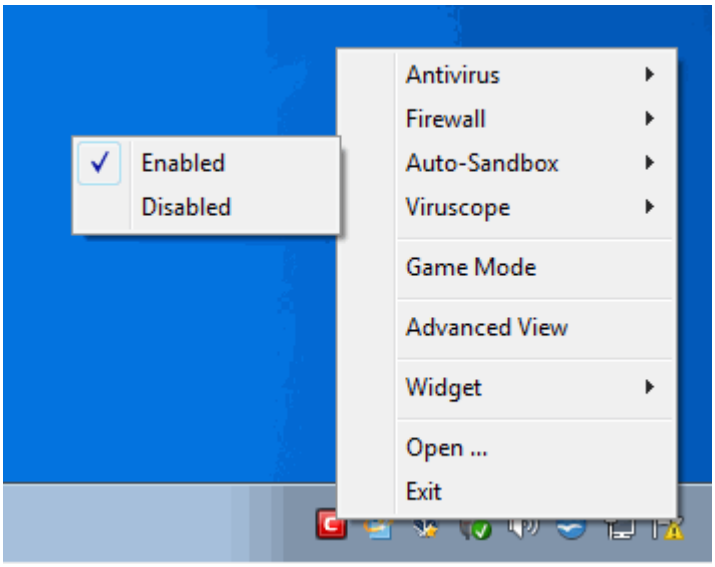
3. Choose 'Enabled' or 'Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Auto-Sandbox

To enable/disable the Auto-Sandbox

1. Right click on the system tray icon keeping the CIS interface in Compact View.
2. Move the mouse cursor over 'Auto-Sandbox'



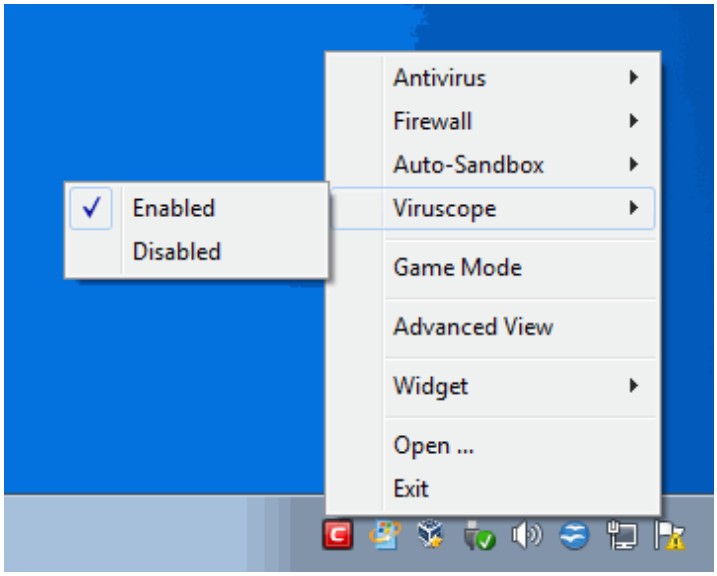
3. Choose 'Enabled' or 'Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Viruscope

To enable/disable the Viruscope

1. Right click on the system tray icon keeping the CIS interface in Compact View.
2. Move the mouse cursor over 'Viruscope'



3. Choose 'Enabled' or 'Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

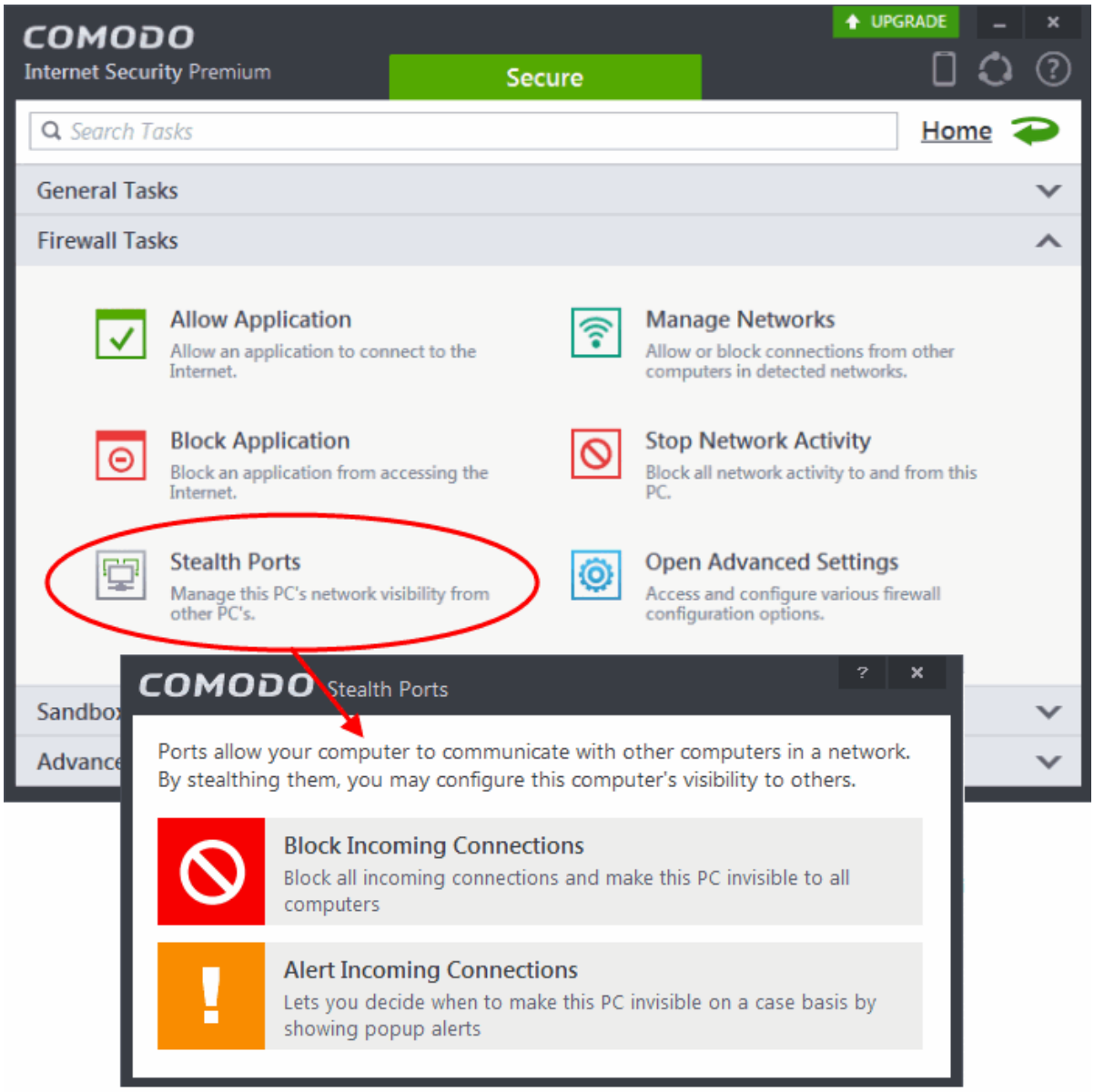
Set up the Firewall For Maximum Security and Usability

This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the Internet.

Stealth Ports Settings

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

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface
3. Open Stealth Ports interface by clicking the 'Stealth Ports' icon  from the Firewall Tasks panel



4. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

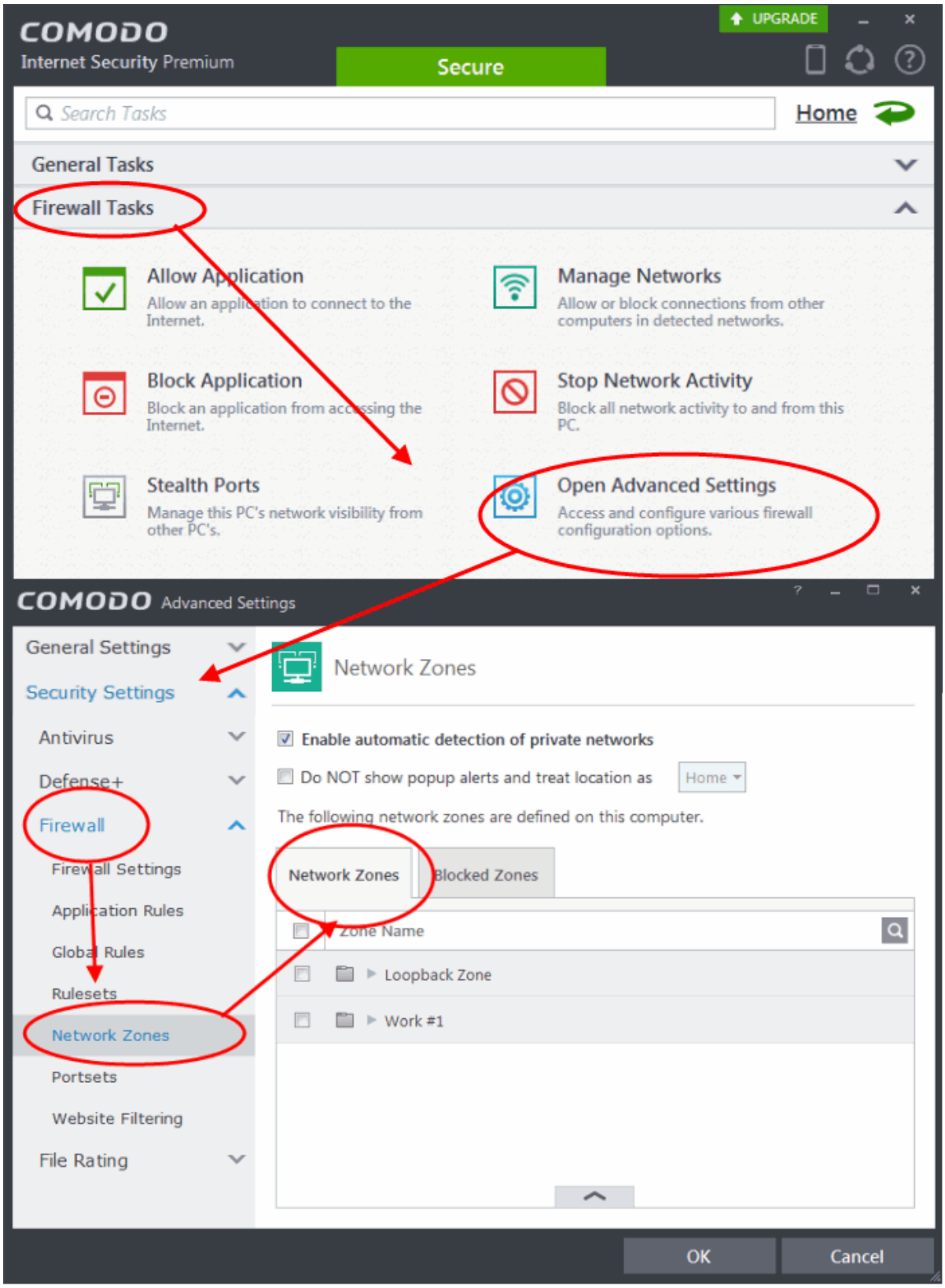
Click here for more details on Stealthing your Computer Ports

Network Zones Settings

The 'Network Zones' settings allow you to configure the protection level for network connection to a Router/home network. (This is usually done **automatically** for you).

To view the configurations

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Network Zones' under Firewall from the left hand side pane
4. Click 'Network Zones' tab from the 'Network Zones' interface



Check the Loopback zone and Local Area Network #1. **In most cases**, the loopback zone IP address should be *127.0.01/255.0.0.0*

In most cases, the IP address of the auto detected Network zone should be *192.168.1.100/255.255.255.0* .

5. Check these addressees and click 'OK'.

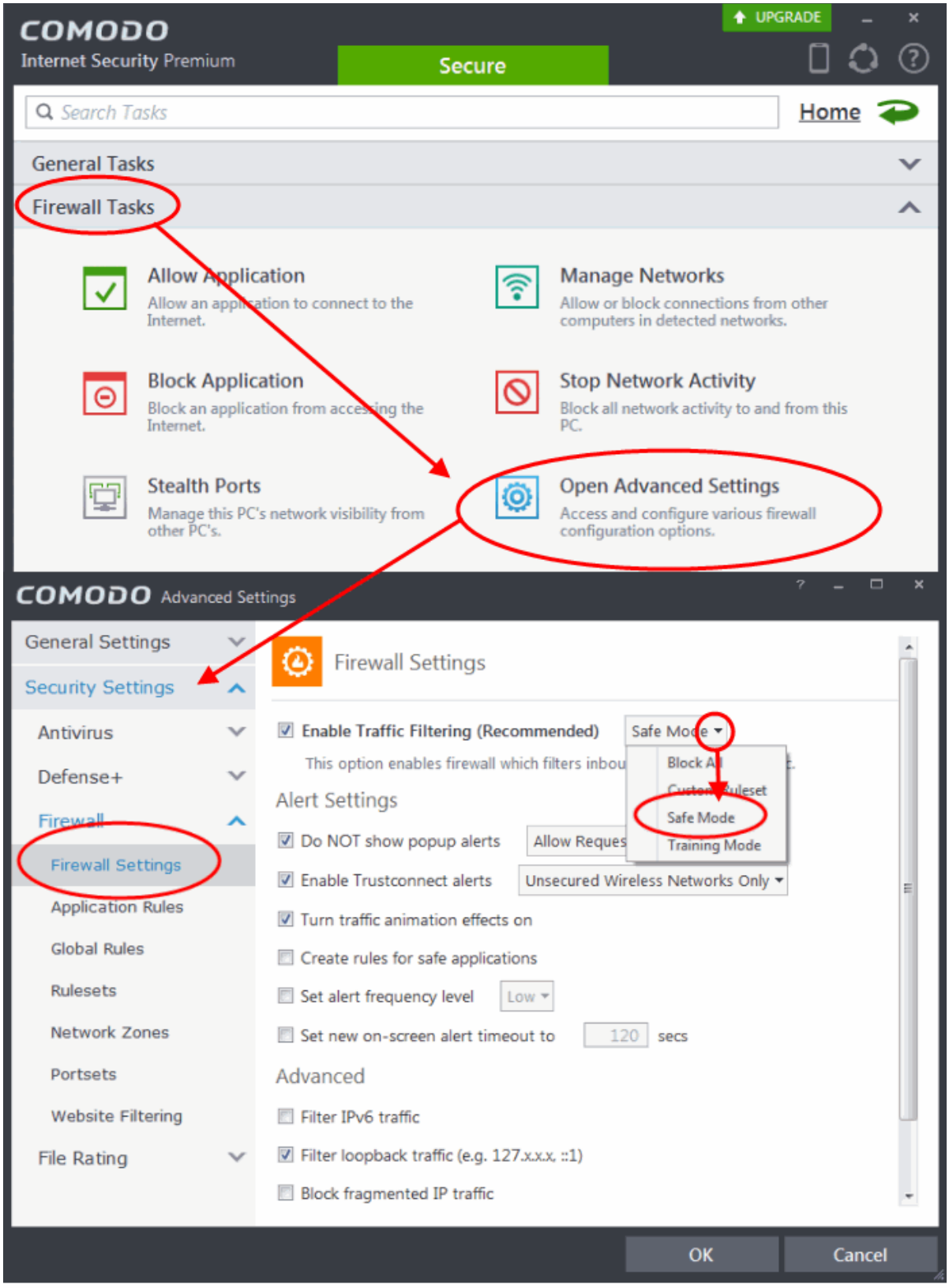
Click here for more details on Network Zones settings

Firewall Settings

The Firewall Settings option allows you to configure the protection level for your Internet connection and the frequency of alerts generated.

To open Firewall Settings panel

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Firewall Settings' under Firewall from the left hand side pane
4. Ensure that 'Enable Firewall' is selected and choose **Safe mode** from the drop-down beside it.

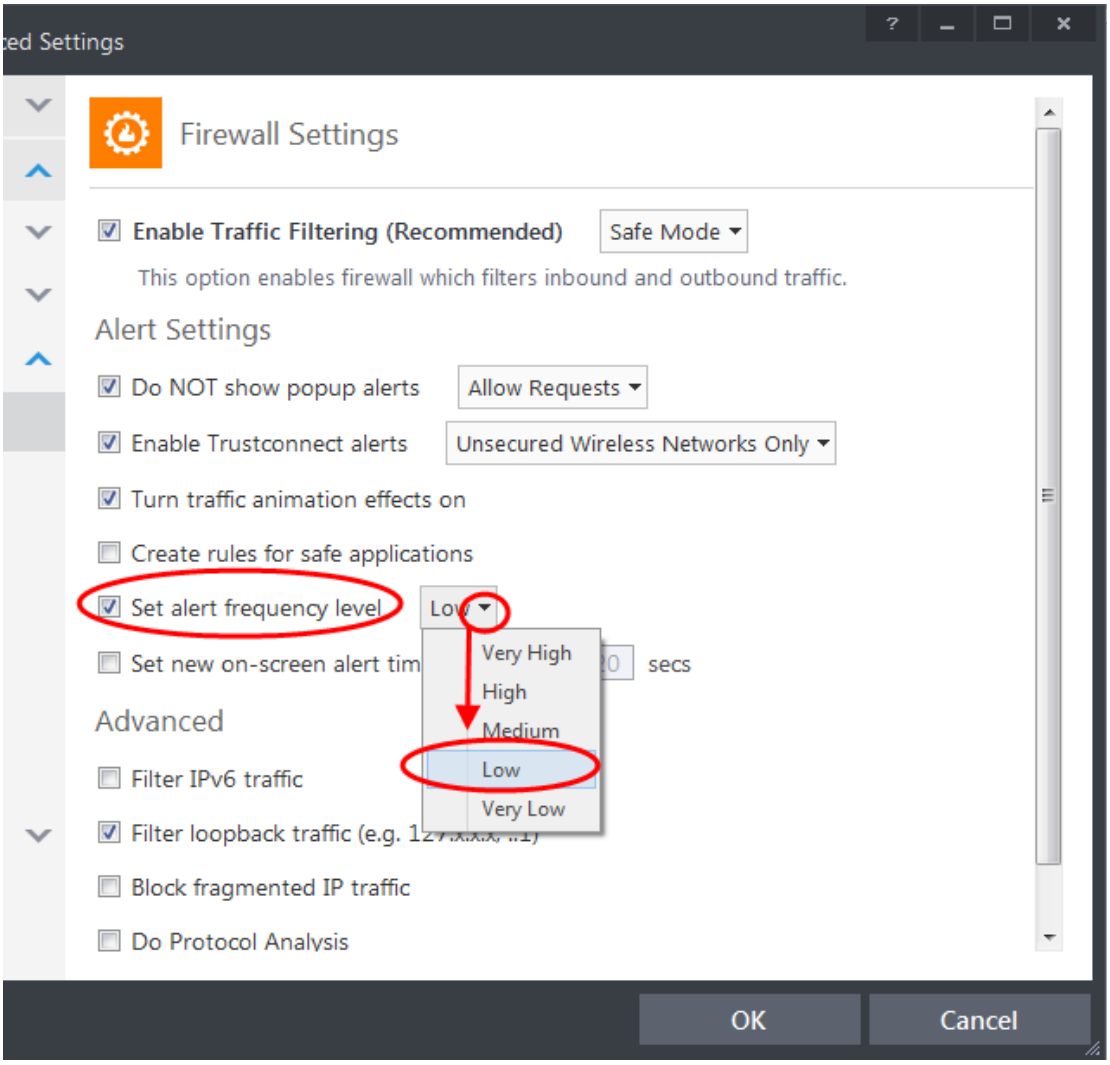


Safe Mode: While filtering network traffic, the firewall will automatically create rules that allow all traffic for the components of applications certified as 'Safe' by Comodo. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

Under 'Alert Settings' in the same interface:

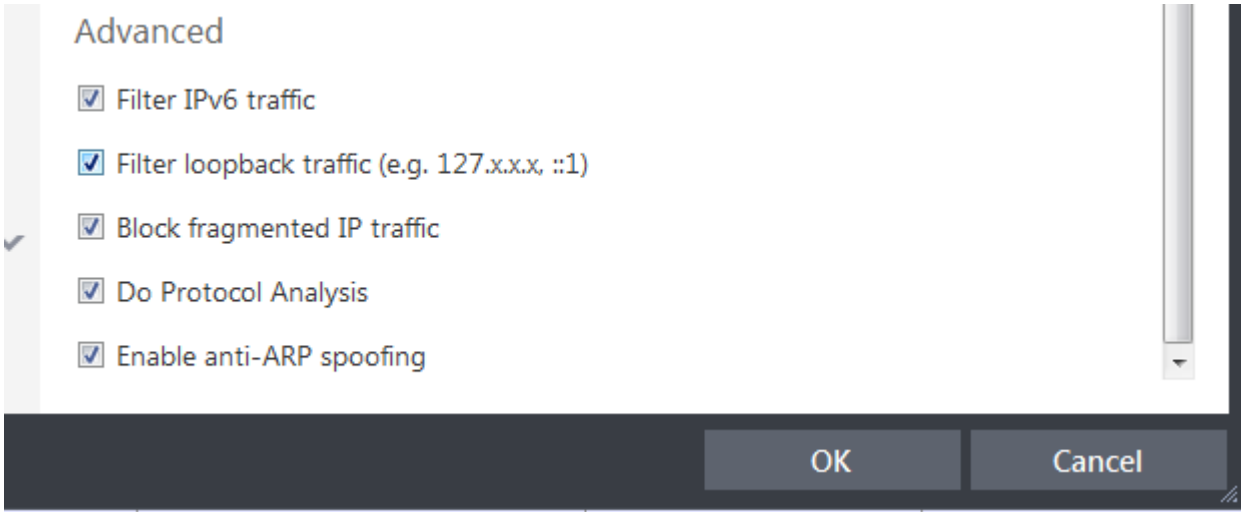
- Deselect Do NOT show popup alerts
- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.



Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- Select **Filter loopback traffic**
- Ensure that the **Block fragmented IP traffic** is selected
    - **Block fragmented IP traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time.
- Select the **Do Protocol Analysis** checkbox to detect fake packets used in denial of service attacks
- Select **Enable anti-ARP spoofing**



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

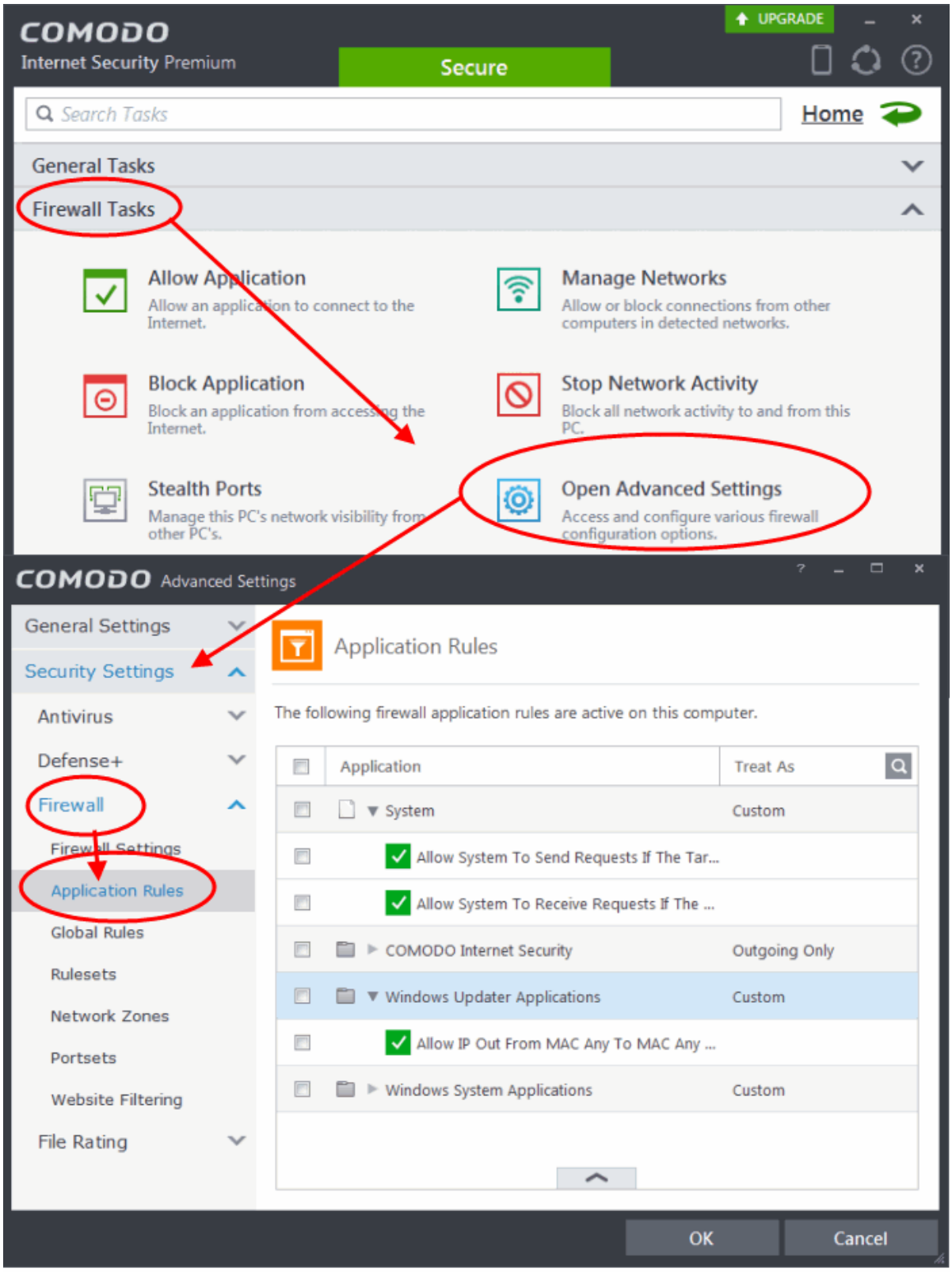
Click here for more details on Firewall Settings

Setting-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules and policies on an application specific and global basis and predefined firewall rulesets.

To view the Application Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Application Rules' under Firewall from the left hand side pane



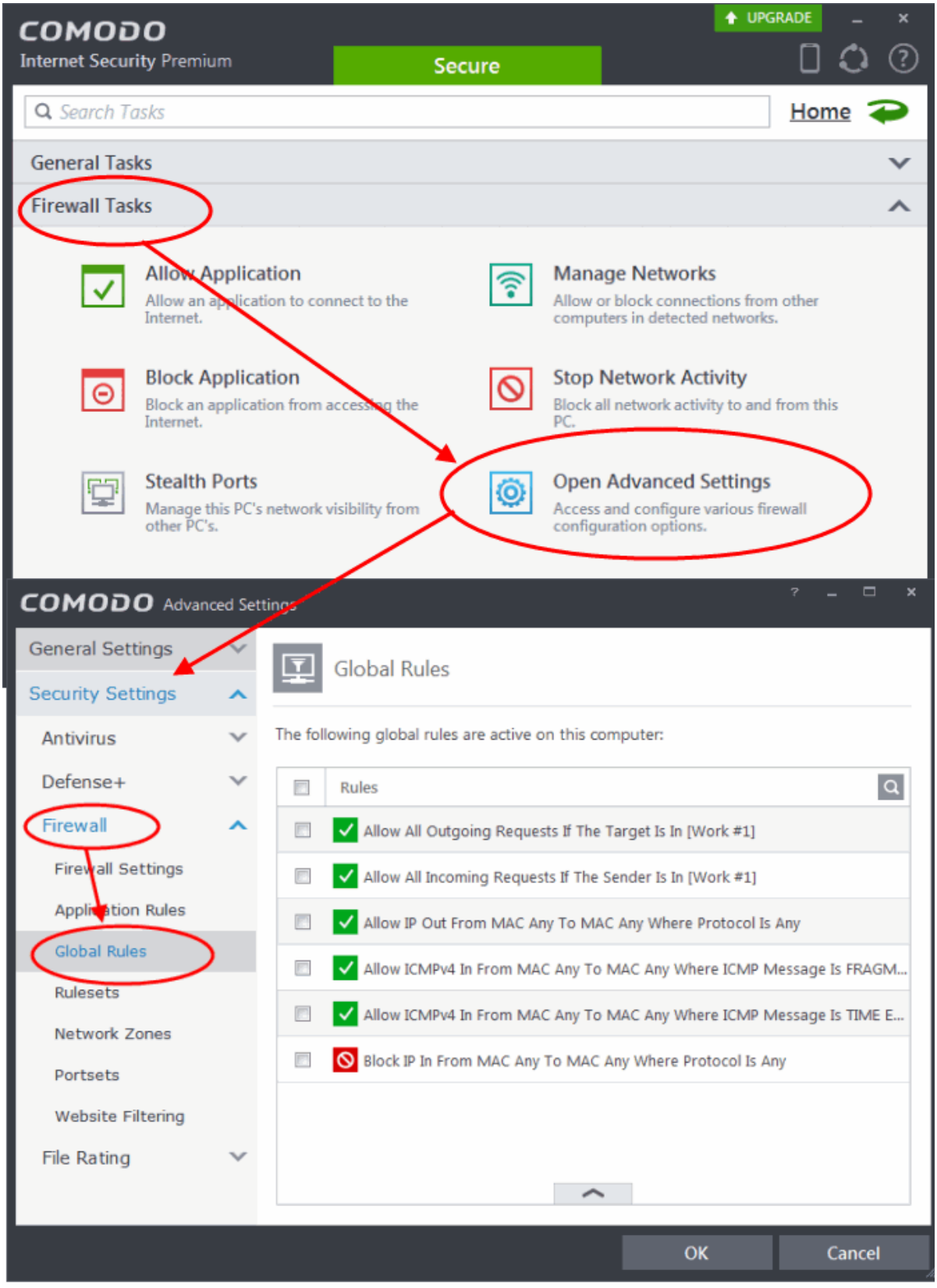
4. Click the handle from the bottom and Add or Edit rules for specific applications manually or remove them.

Click here for more details on Application Rules

To view the Global Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen

2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Global Rules' under Firewall from the left hand side pane

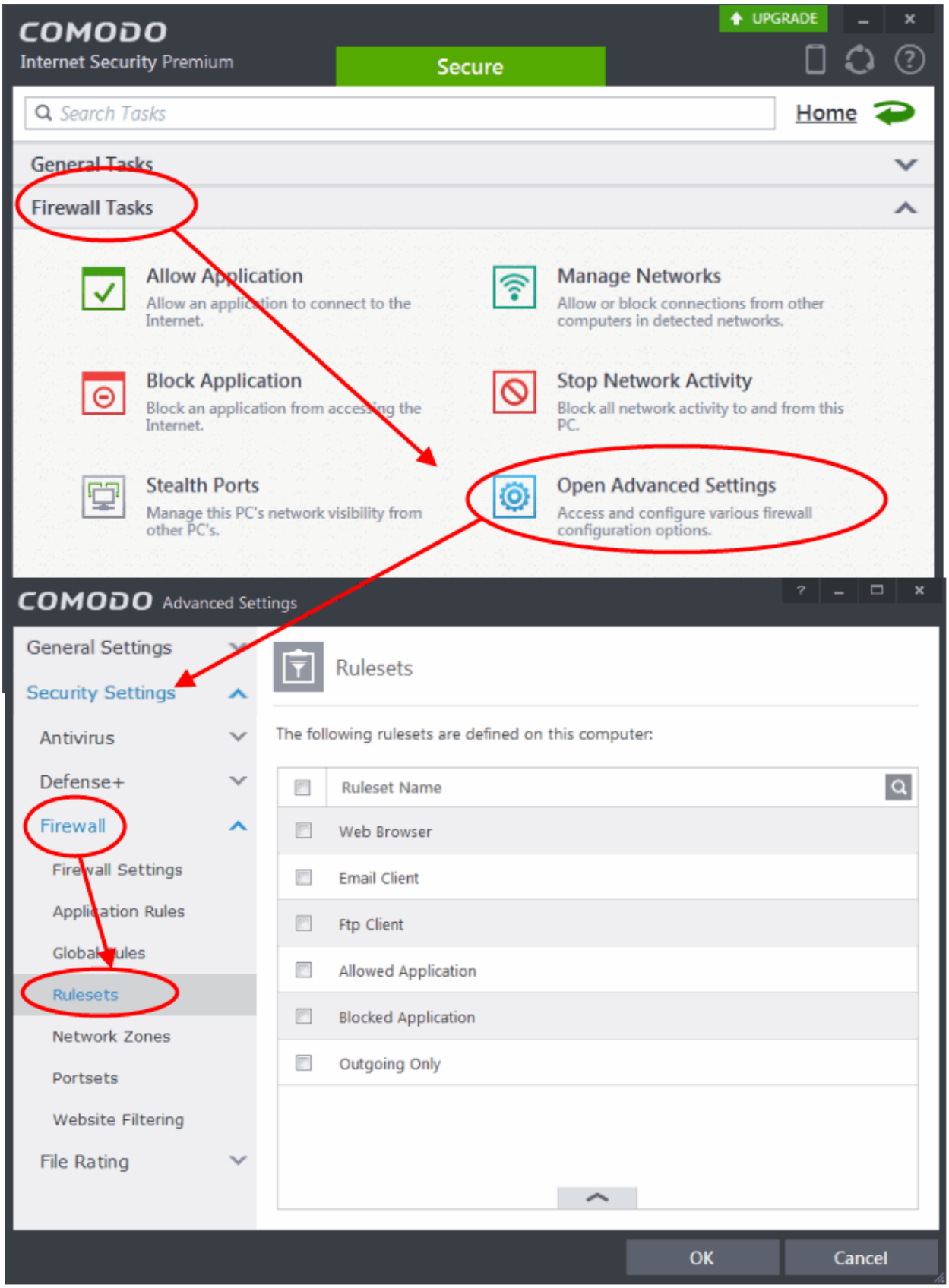


4. Click the handle from the bottom and Add or Edit global rules manually or remove them.

Click here for more details on Global Rules

To view Predefined Firewall rulesets

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Rulesets' under Firewall from the left hand side pane



4. Click the handle from the bottom to and Add, Edit or remove rulesets.

You need not make your own rulesets, the defaults are usually enough.

Click here for more details on pre-defined firewall rulesets

Block Internet Access while Allowing Local Area Network (LAN) Access

You can configure Comodo Firewall to block Internet access while allowing free connections to an internal network (Intranet or LAN).

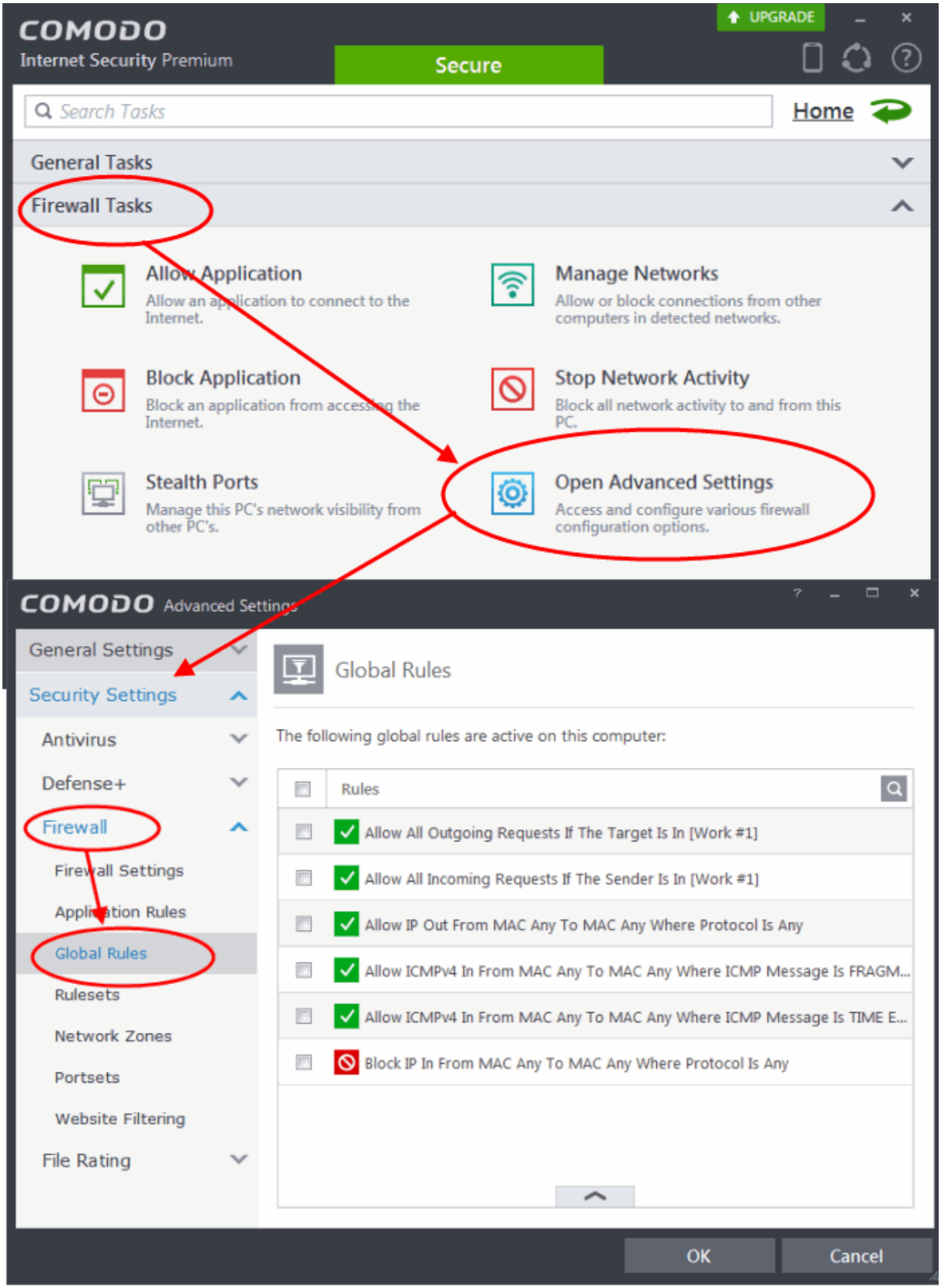
Example scenarios:

- In your network at home, you want your child's computer to connect to other computers at home but disable Internet access to them for safety reasons
- In your corporate network, you want your employee's computers to connect to your local network machines but disable Internet access for them for bandwidth restrictions

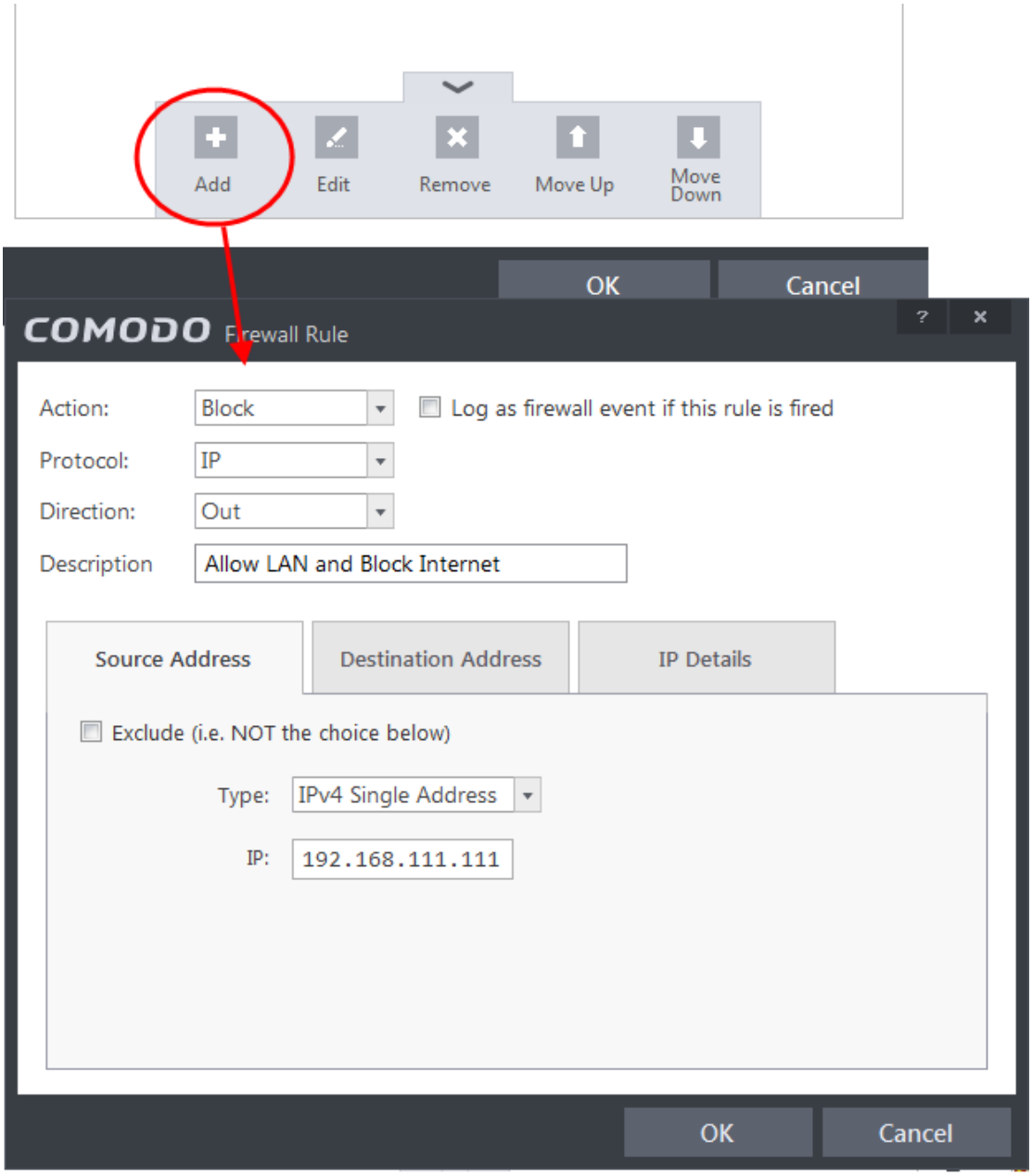
To selectively block connection to Internet whilst allow connection to internal network you need to create a Global Rule under Advanced Firewall Settings and password protect your configuration to prevent others from altering it.

To create a Global Rule

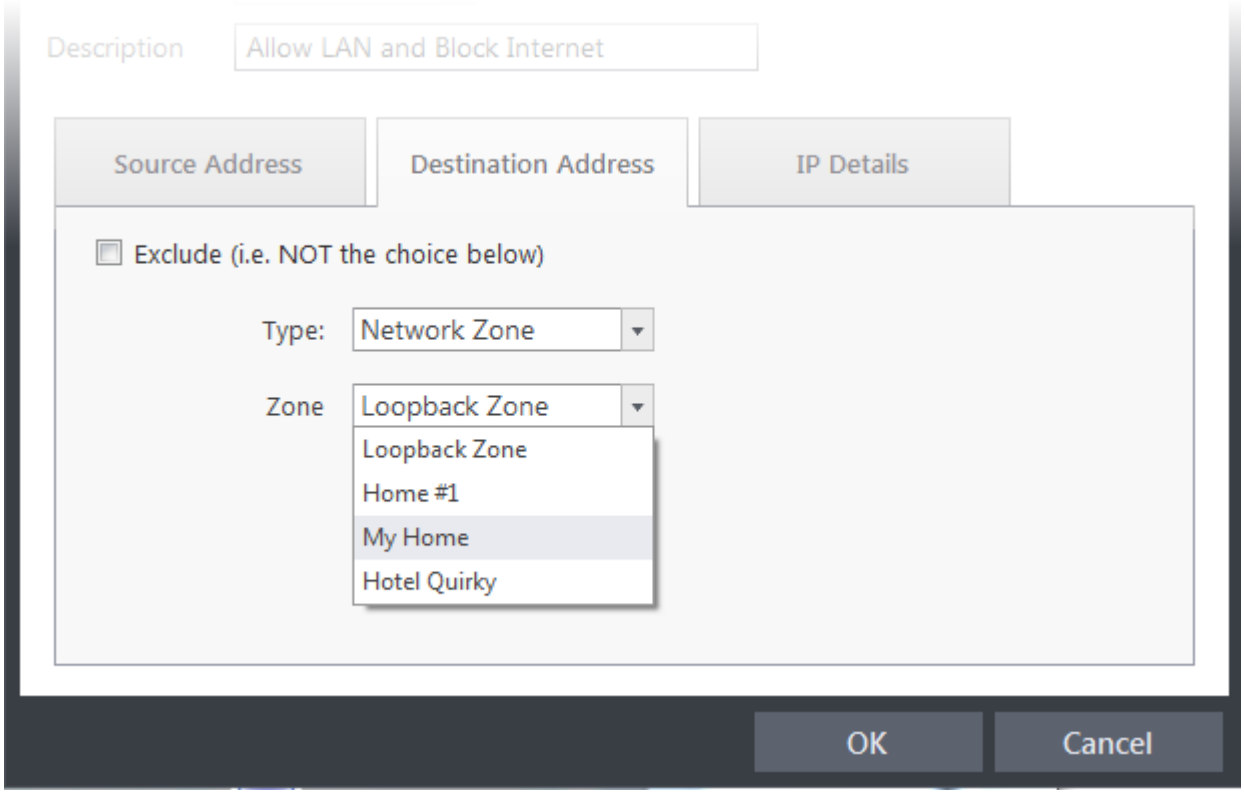
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Global Rules' under Firewall from the left hand side pane



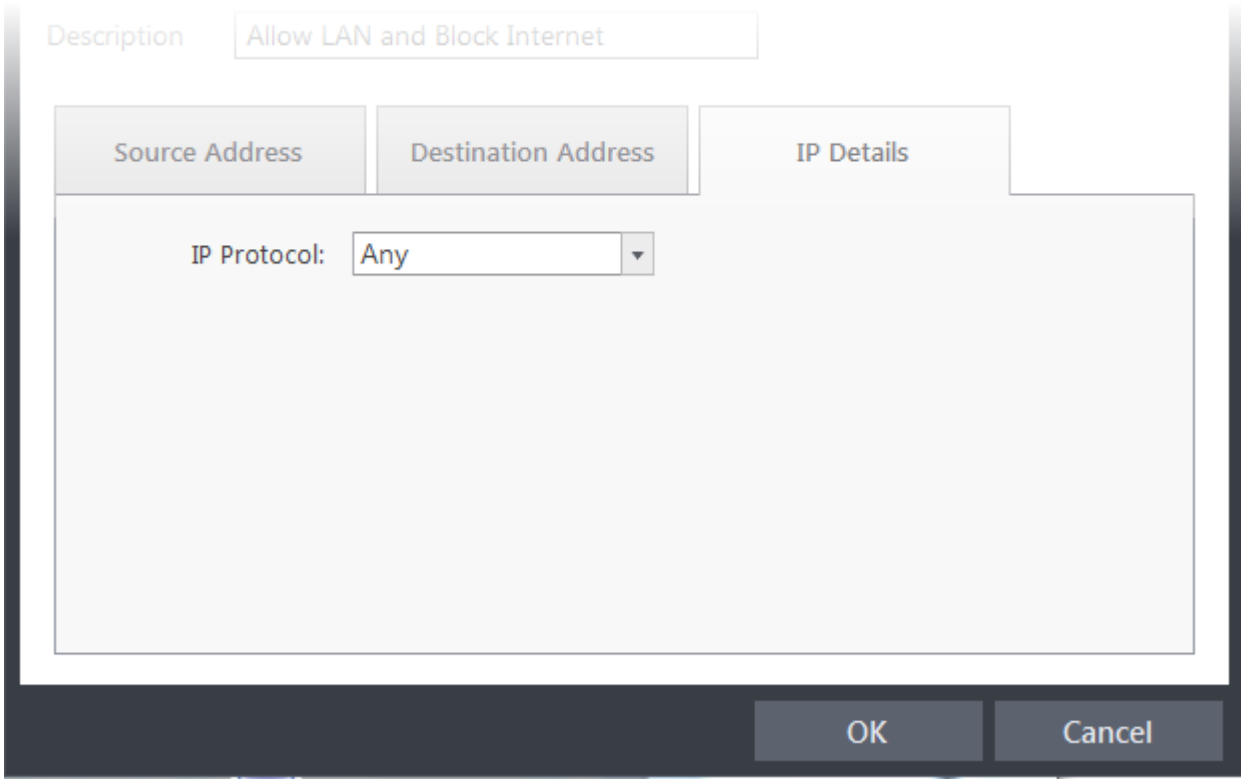
4. Click the handle from the bottom and choose 'Add' from the options. The Firewall Rule interface will open.



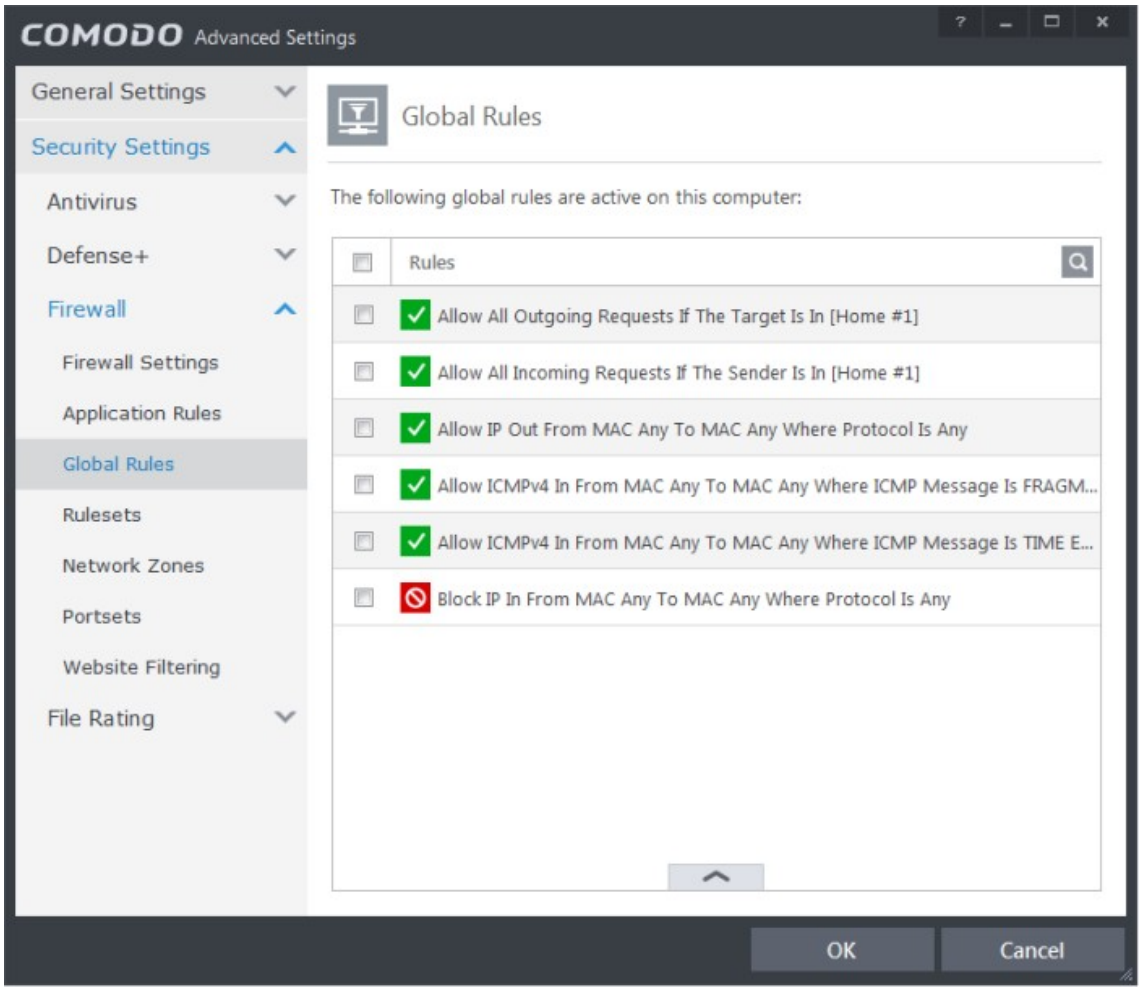
5. Choose the following options from the drop-down menus:
    - Action = Block;
    - Protocol = IP;
    - Direction = Out.
6. Enter a description for the new rule in the Description text box.
7. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network and enter the IP address of the computer in the IP text box.
8. Click the 'Destination Address' tab, choose 'Network Zone' from the Type drop-down and choose your local area network from the 'Zone' drop-down.



9. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.



10. Click 'OK'. The created policy will be added to the list of Global Rules.
11. Select the rule, click the handle from the bottom and click 'Move Up' repeatedly until the rule moves to the first position.

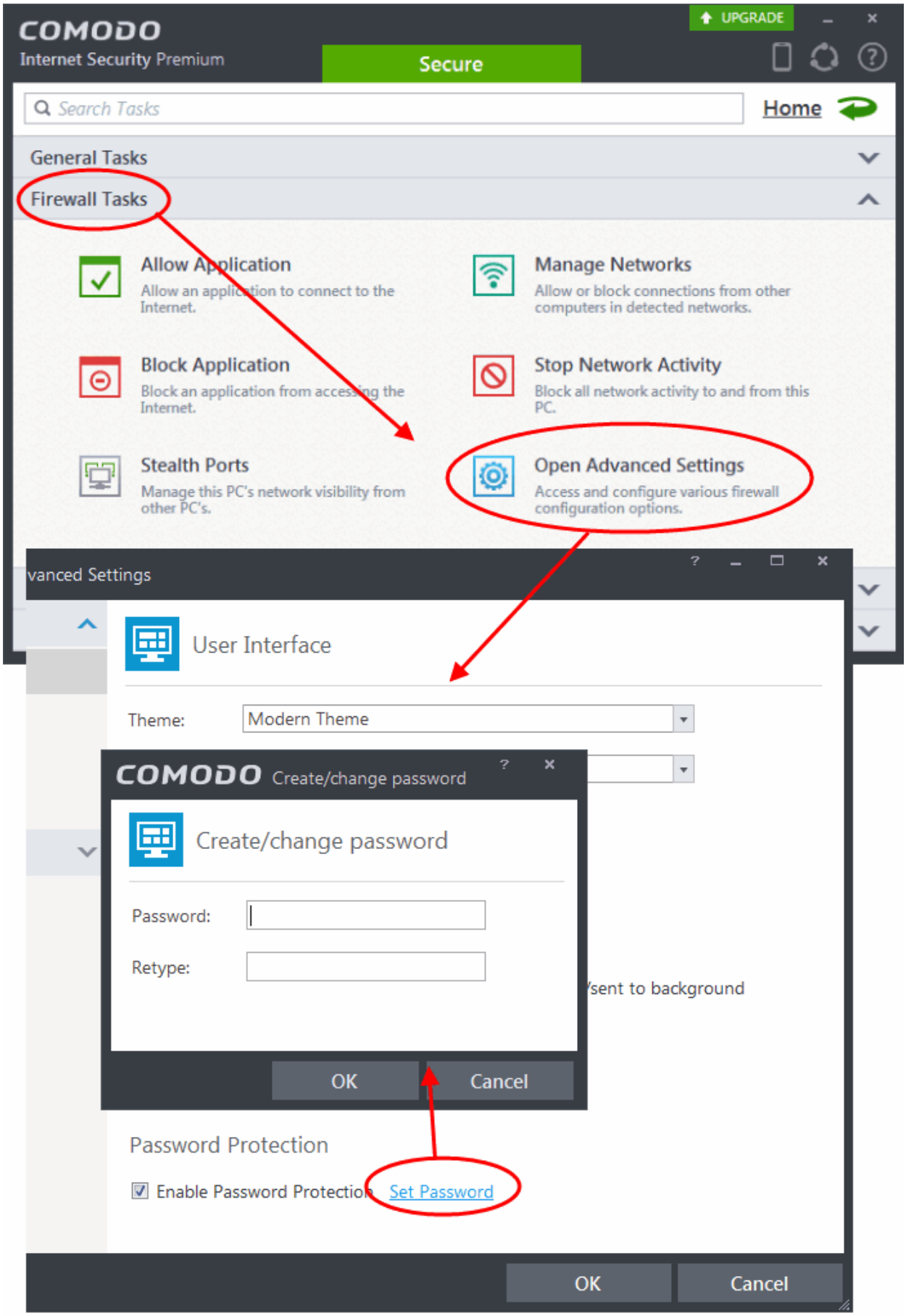


12. Click 'OK' for your configuration to take effect.

Your Firewall is now configured to allow access to internal network but to block Internet access. Now you need to password protect this configuration to prevent others from changing it.

To password protect your configuration

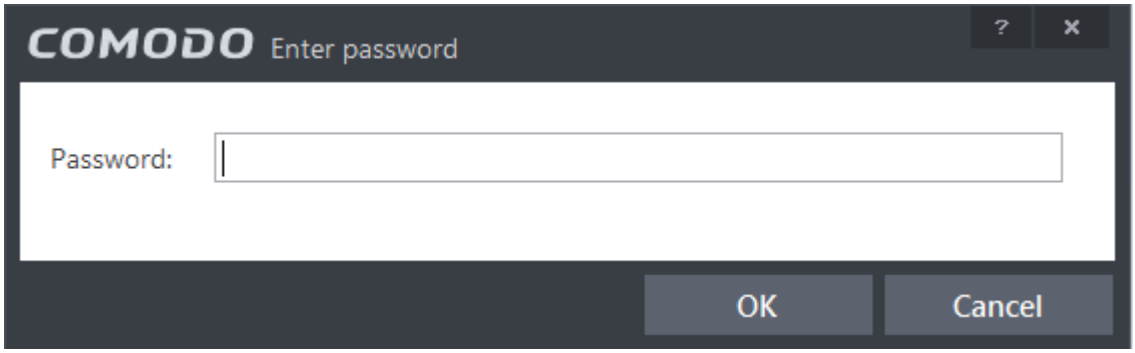
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'User Interface' under General Settings from the left hand side pane



4. Select 'Enable Password Protection' under 'Parental Control' and click 'Set Password' link. The Change password dialog will appear.

5. Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

The configuration is now password protected. From the next attempt to change any configuration changes to CIS, you will be prompted to enter the password to proceed.



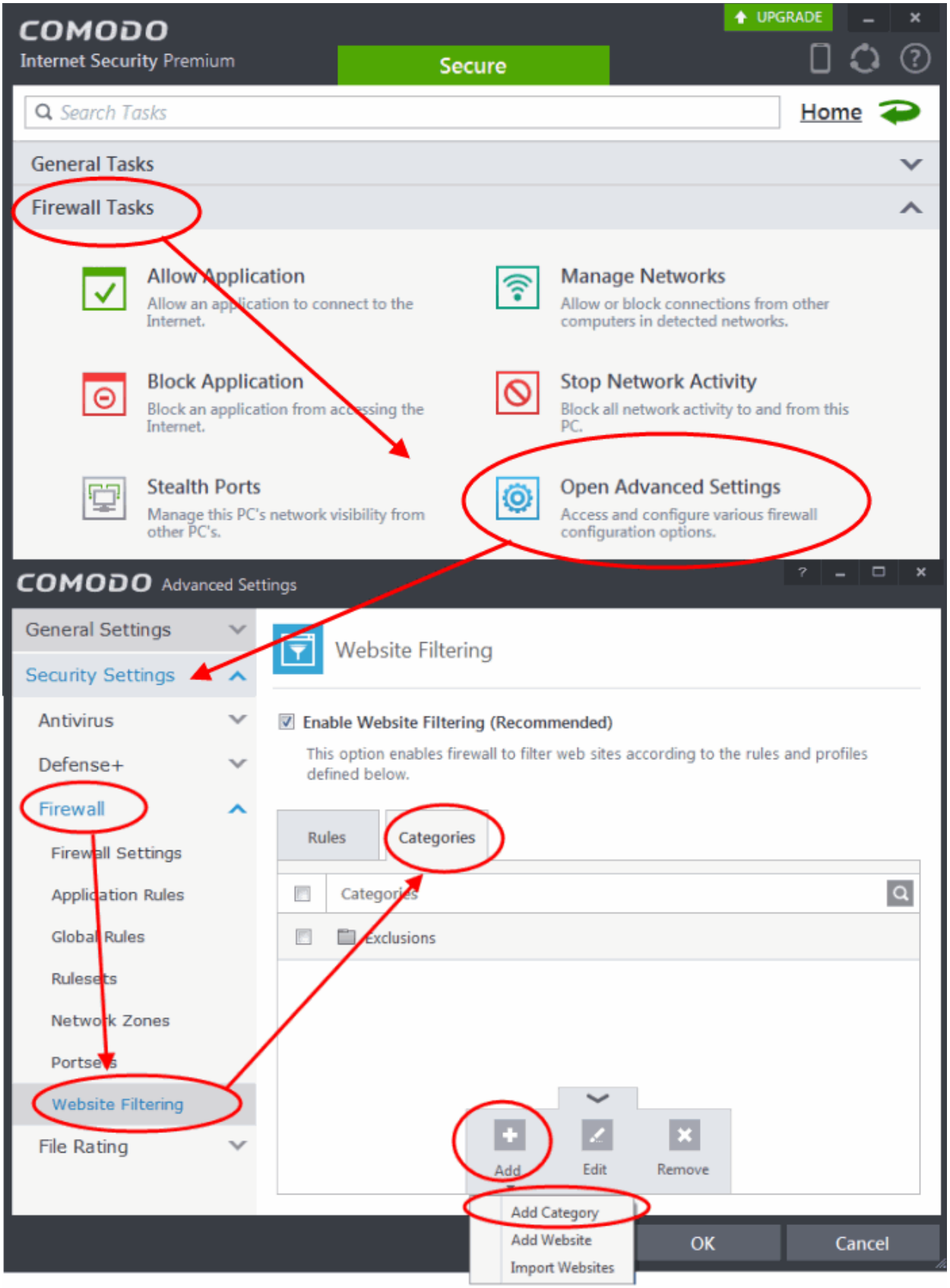
Block/Allow Websites Selectively to Users of Your Computer

Comodo Internet Security allows you to specify websites or groups of website(s) that can be selectively allowed or blocked to different users. This involves two steps:

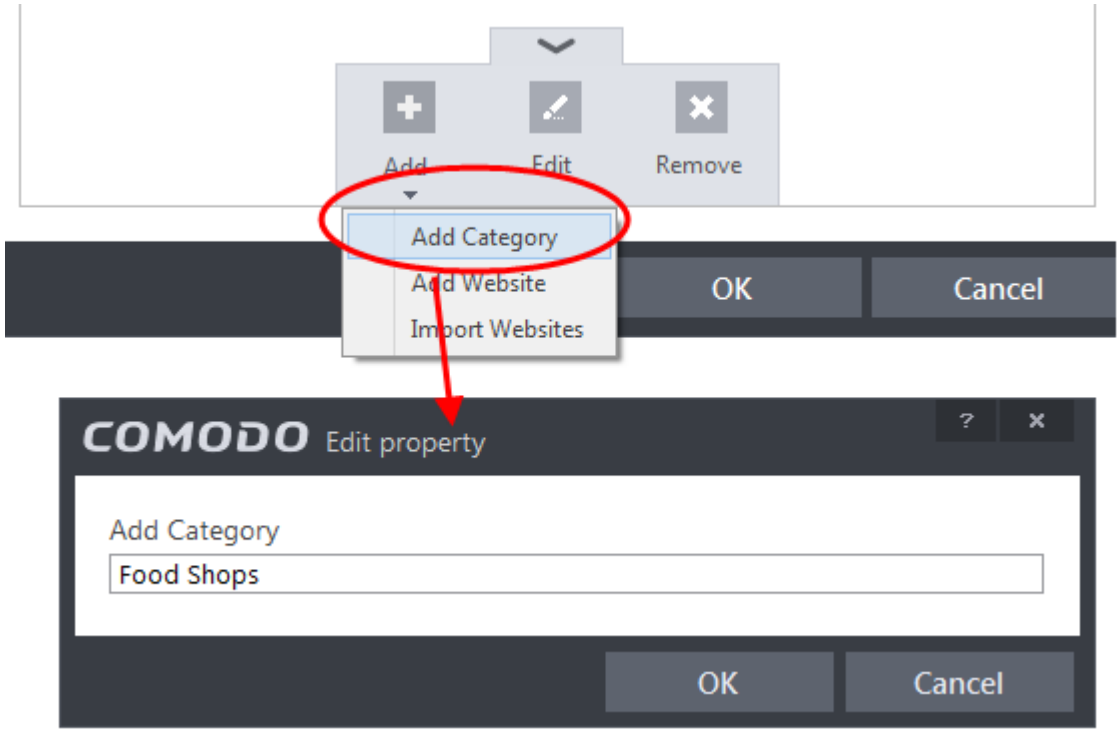
- **Define Website Categories and add websites**
- **Create Firewall rules for allowing or blocking website categories to selected users**

To define website categories

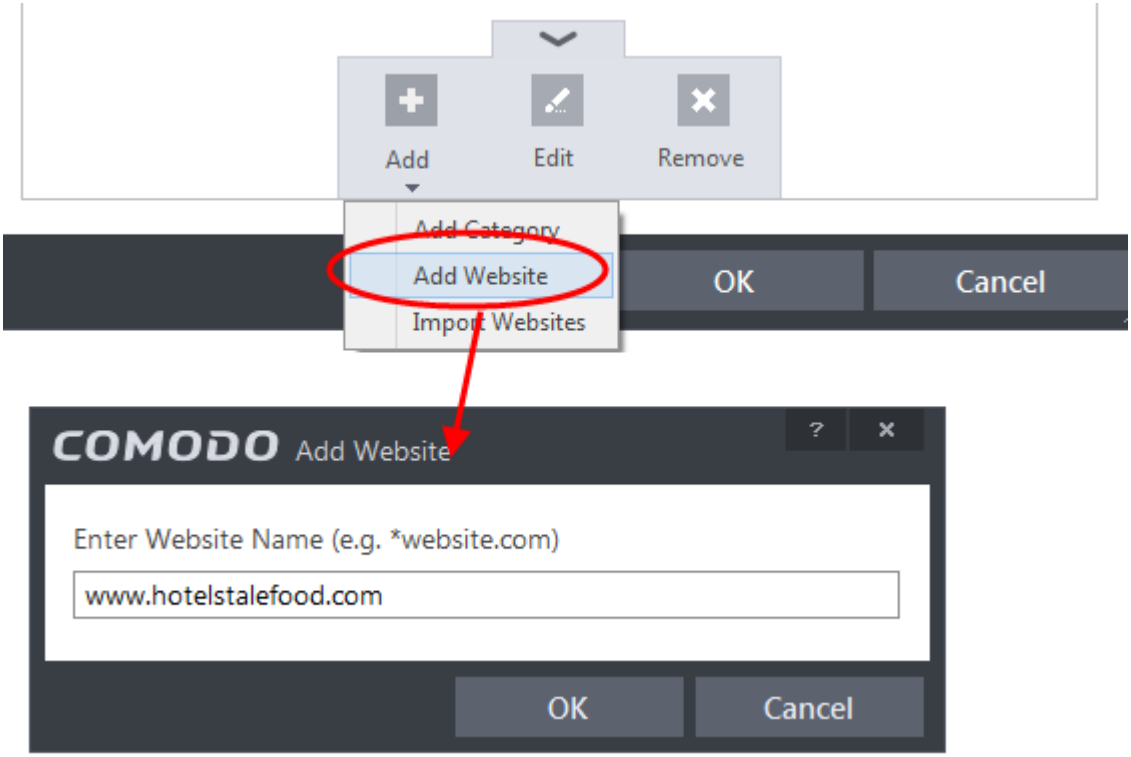
1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen.
2. Click 'Firewall Tasks' from the 'Tasks' interface then click 'Open Advanced Settings'.
3. Click 'Website Filtering' under 'Firewall' in the left hand menu.
4. Ensure that the 'Enable Website Filtering Filtering' checkbox is selected.
5. Click the 'Categories' tab from the 'Website Filtering' interface.



6. Click the handle at the bottom center of the 'Categories' pane, click 'Add' from the options and choose 'Add Category' from the drop-down. The 'Edit Property' dialog will open.



7. Enter a name for the category and click 'OK'. The new category will be created and added under the 'Categories' tab.
8. Select the new category, click the handle at the bottom of the 'Categories' pane, click 'Add' then choose 'Add Website'. The 'Add Website' dialog will open:



9. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
   - To add a specific website/webpage, enter the full URL of the website/webpage
   - To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
   - To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.

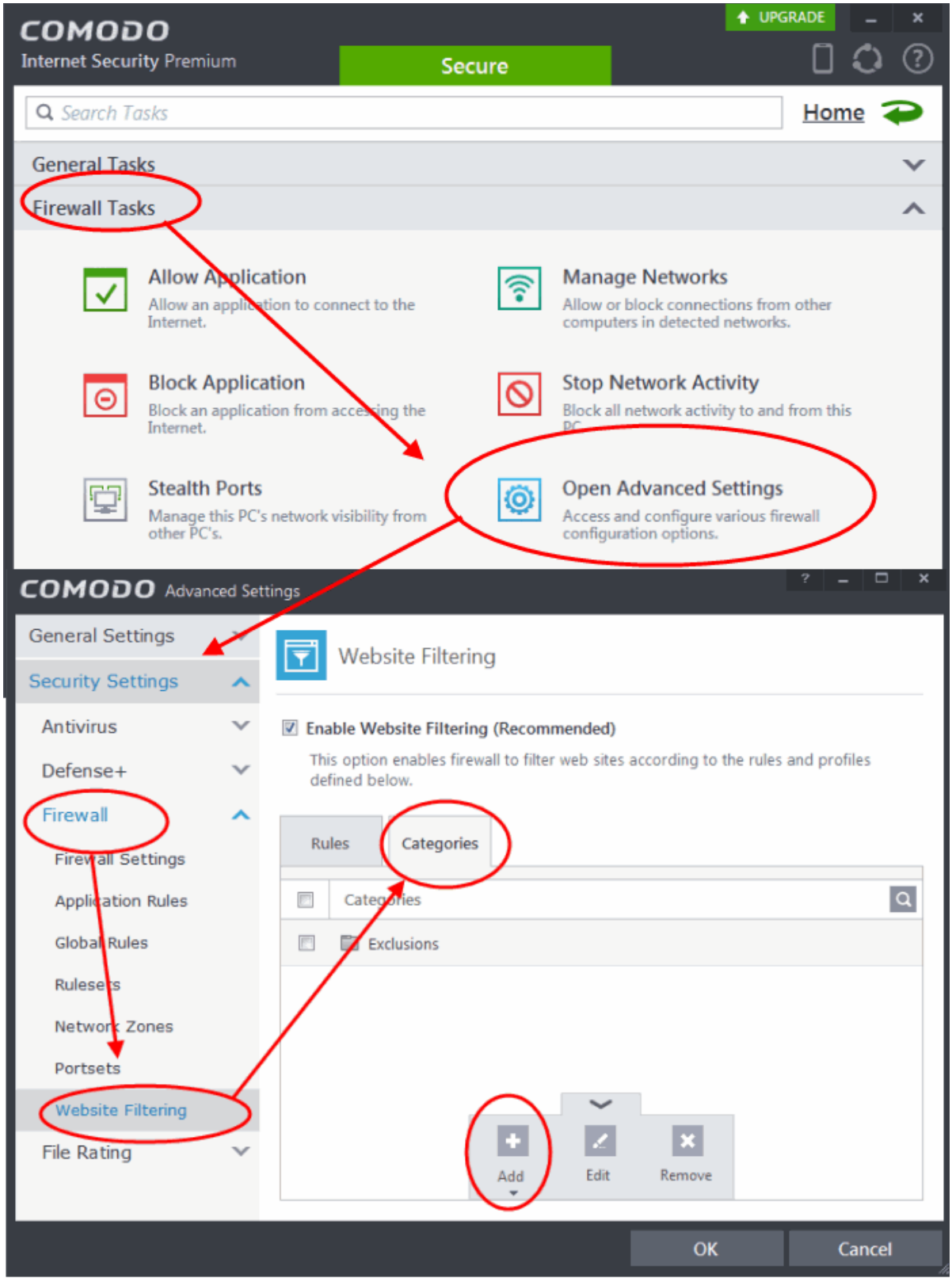
- To include all the websites with URLs that contain a specific string, add the wildcard character befor and after the string. For example, "*pizza*" will cover hotpizza.com, spicypizza.com and so on.

The website(s) will be added to the category.

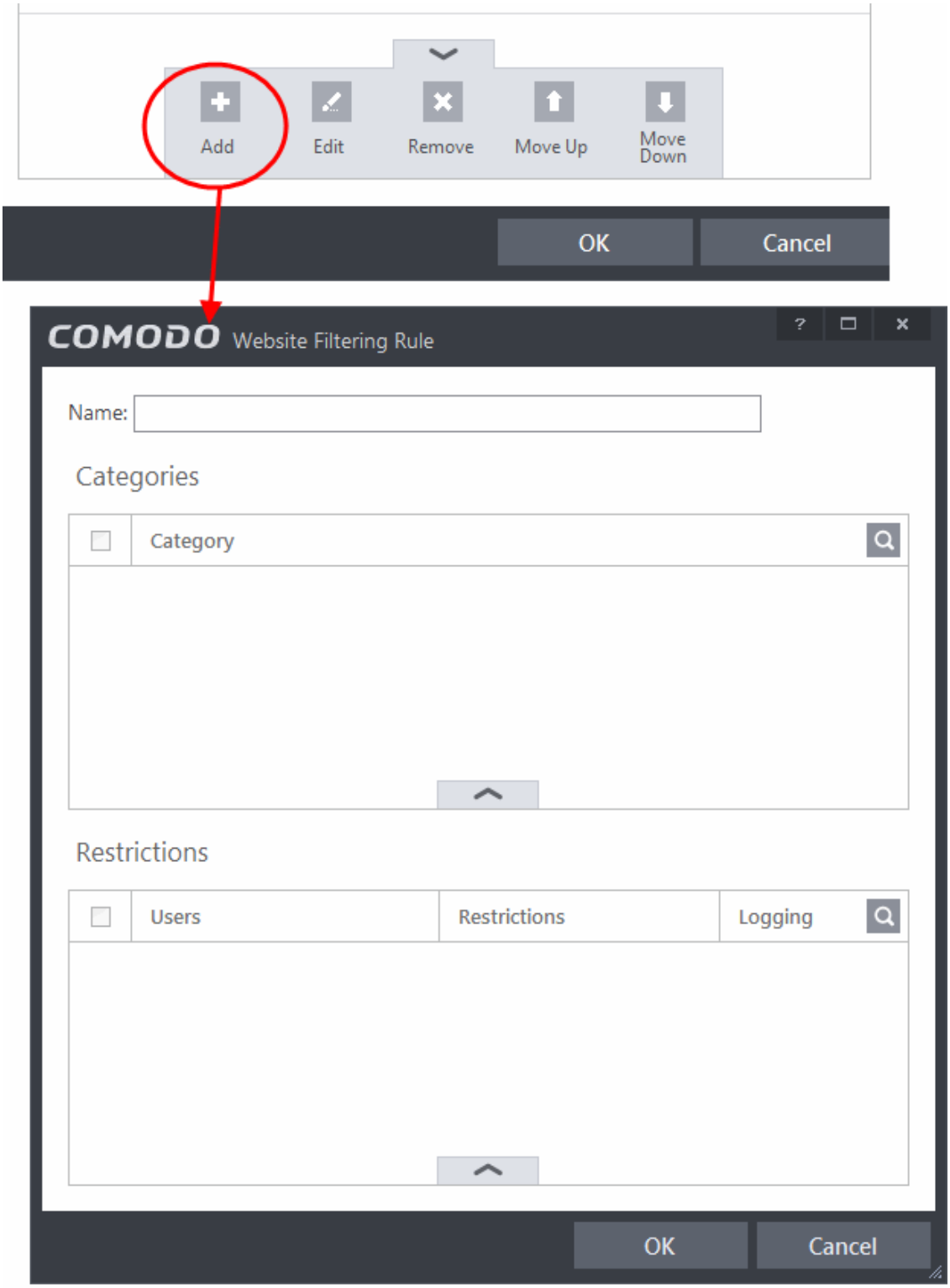
10. Repeat the process to add more websites.
11. Click OK in the 'Advanced Settings' interface to save your settings

To create rules for selectively blocking or allowing websites to users

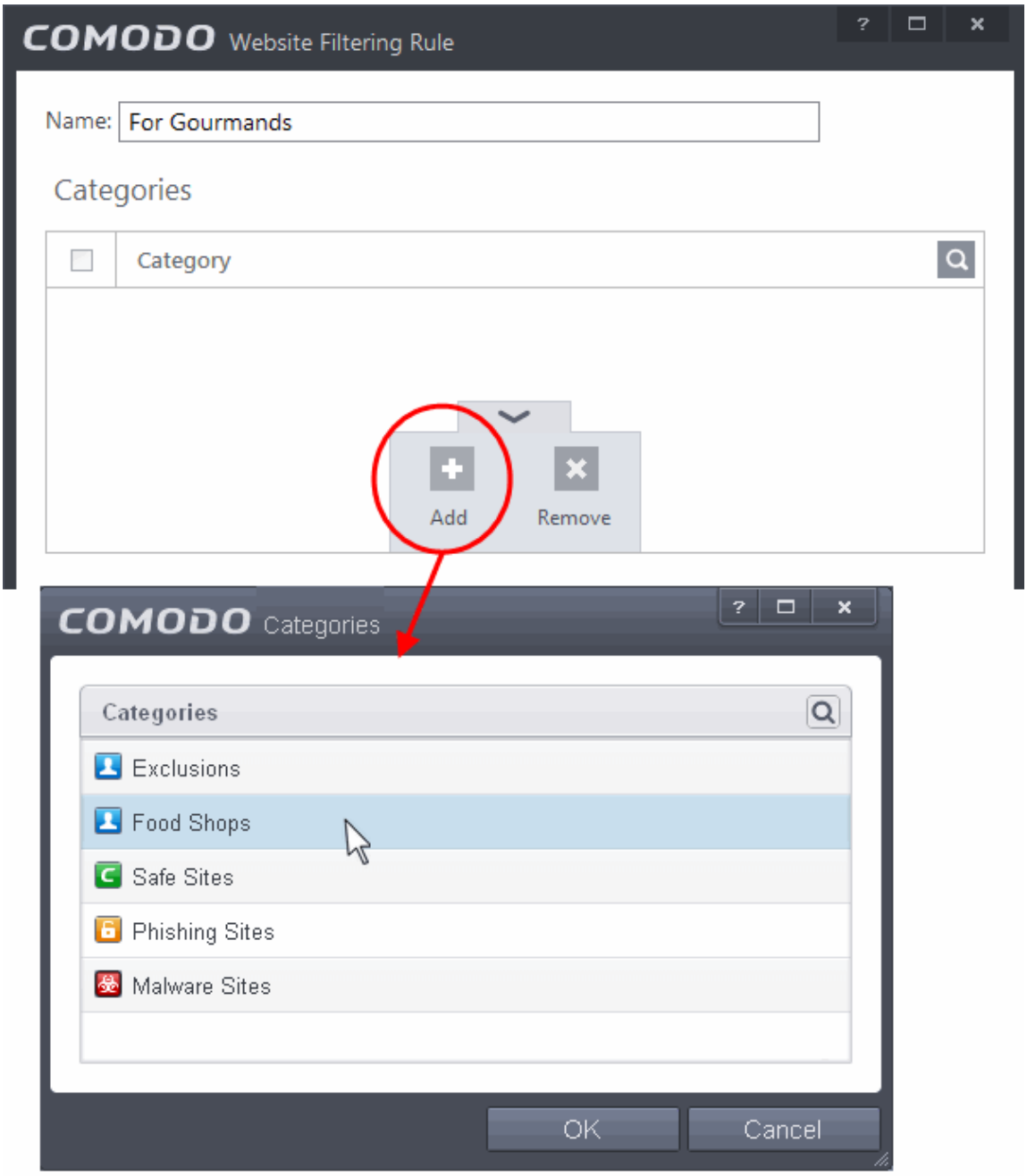
1. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
2. Click 'Website Filtering' under 'Firewall' from the left hand menu.
3. Click the 'Rules' tab
4. Click the handle at the bottom of the interface and select 'Add':



5. Enter a name for your new filter in the 'Website Filtering Rule' dialog.



6. Select the categories that should be added to the filter:
    - Click the handle at the bottom of the 'Category' pane and choose 'Add'.



- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

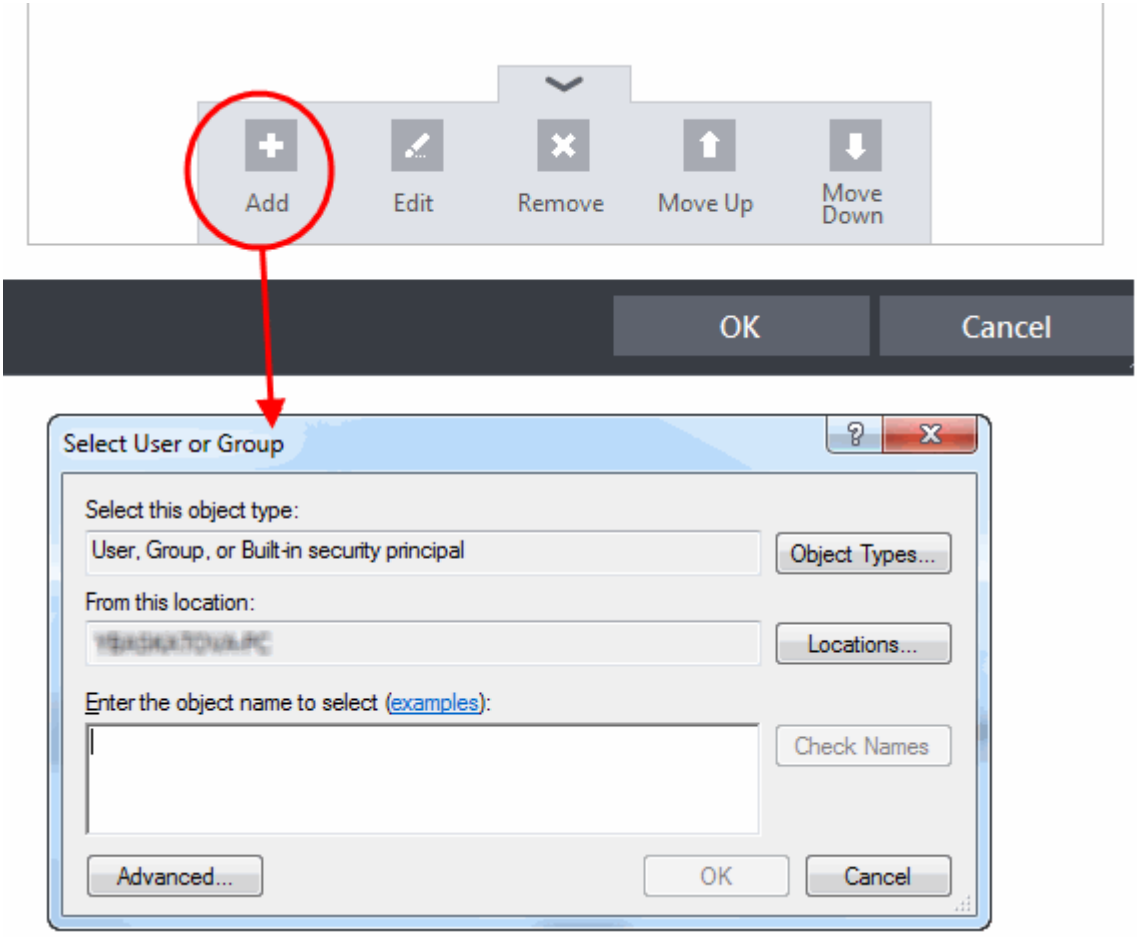
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Comodo Safe Sites** - Websites that are considered safe according to global whitelist
- **Comodo Phishing Sites** - Websites that lead to phishing websites, as per dynamically updated Comodo Blacklist
- **Comodo Malware Sites** - Websites that may inject malware into your system, as per dynamically updated Comodo Blacklist

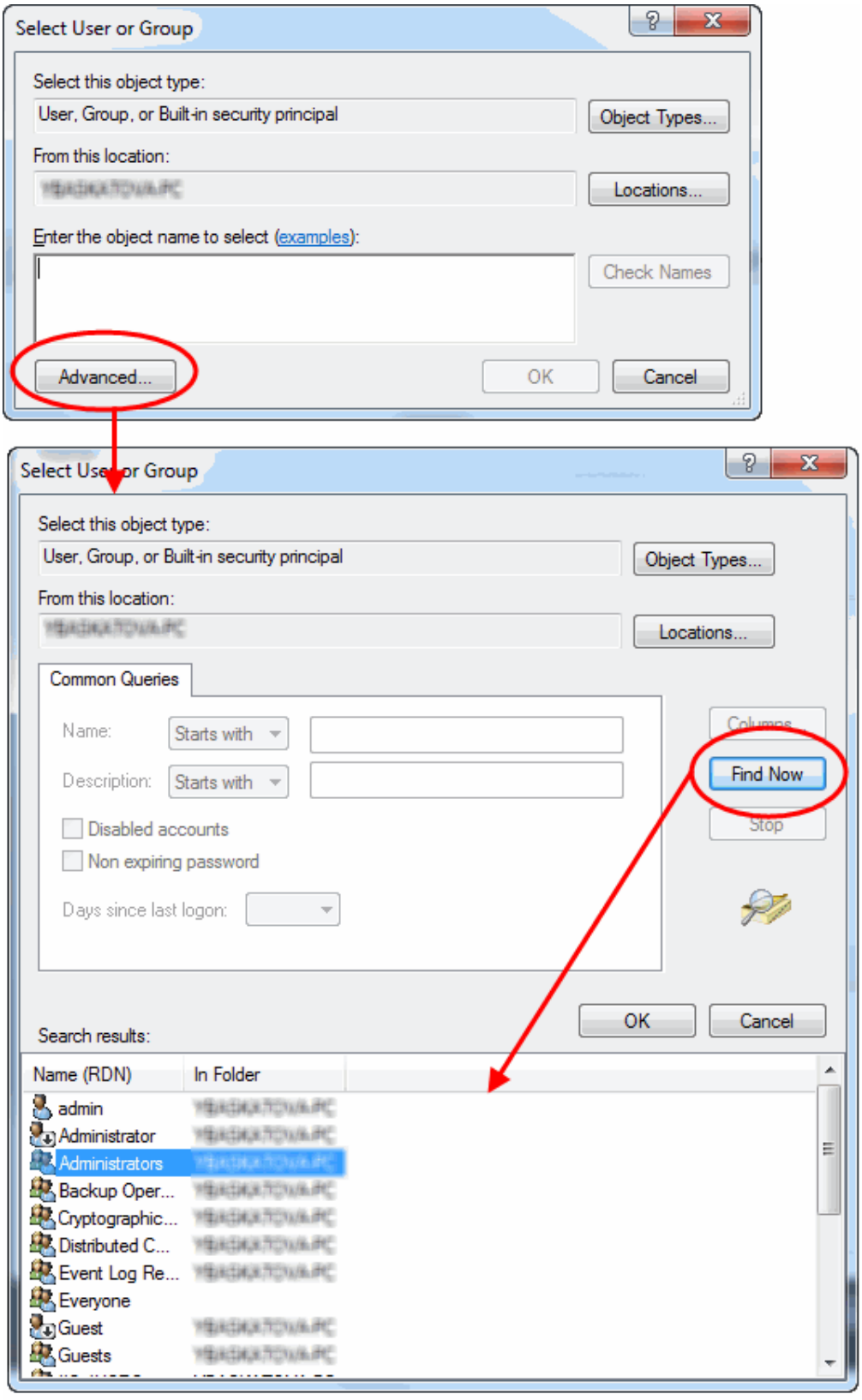
For more details on creating and modifying user specified categories, Refer to the section **Defining or Modifying Website Categories**

7. Add Users or User Groups to whom the rule should be applied:

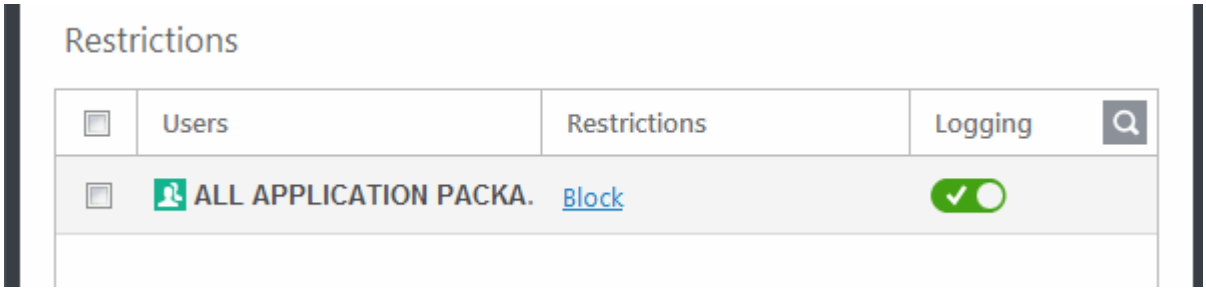
- Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:



- Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format <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.



Important Note to IE 11 users: If you are using Internet Explorer 11 and above, it is mandatory to add the user group 'ALL APPLICATION PACKAGES' to the Restrictions list in addition to the added users for each rule you create.



The rule will take full effect only on adding this user group.

To add 'ALL APPLICATION PACKAGES' to the restrictions list

- Click 'Advanced' in the 'Select User or Group' dialog
- Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom
- Click OK

- After adding target users or groups, you next need to specify whether those users should be allowed or blocked from viewing the websites in the category or they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:

Allow - The websites in the categories can be accessed by the user.

Block - The websites in the categories cannot be accessed by the user.

Ask - An alert will be displayed in the browser if the user tries to access any of the websites in the category. The user can decide whether or not to continue.

- Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.

8. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
9. Ensure that the rule is enabled using the toggle switch under the Enable Rule column for the rule to take effect.

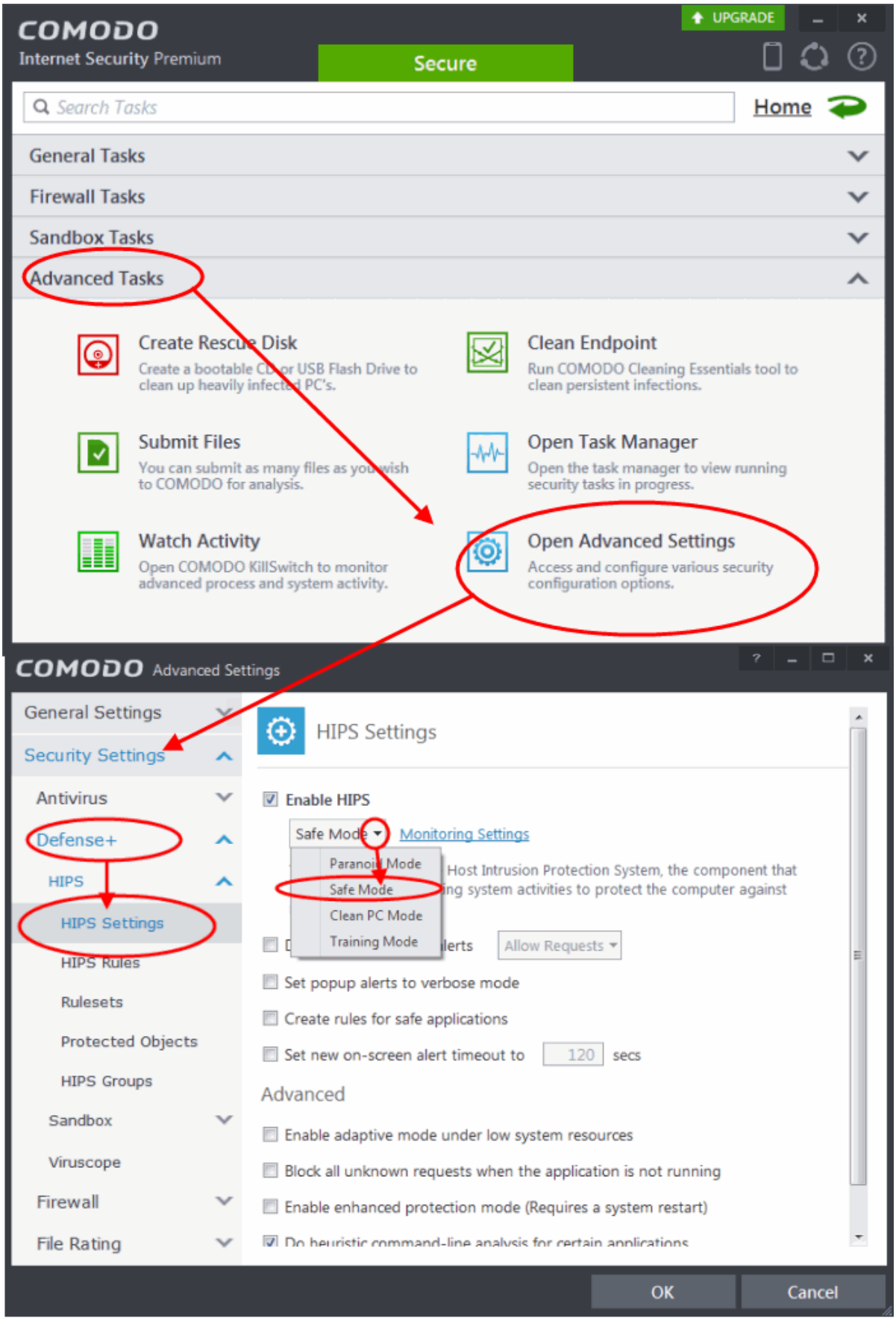
You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Set up the HIPS for Maximum Security and Usability

This page explains on configuring the Host Intrusion Prevention System (HIPS) component of CIS to provide maximum security from the malicious programs that try to execute from within your system and to protect your system from data theft, computer crashes and system damage by preventing most types of buffer overflow attacks, prevent possible attacks from root-kits, inter-process memory injections, key-loggers and more.

To configure HIPS

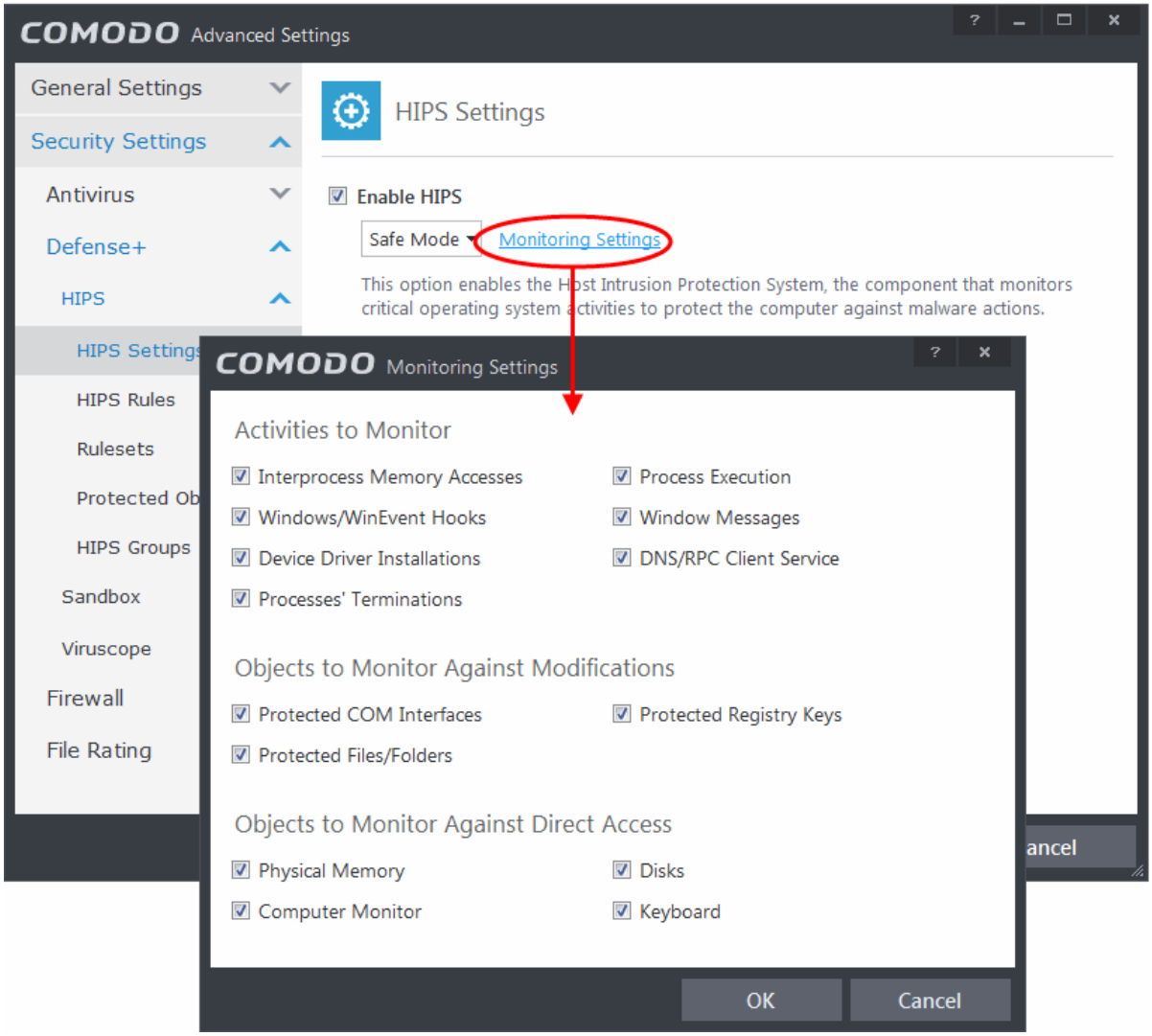
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'HIPS' > 'HIPS Settings' from the left hand side pane



4. Select Enable HIPS
5. Choose 'Safe Mode' from the drop-down below it. Refer to **HIPS Settings** for more details on the Security Levels.

Monitoring Settings

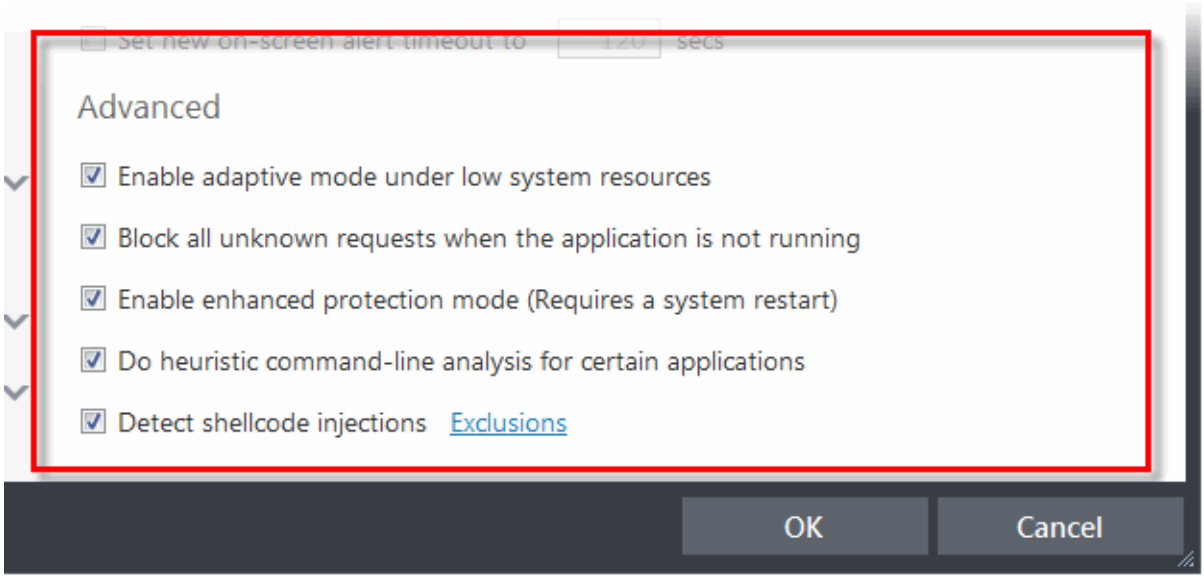
6. Click Monitoring Settings from the HIPS Settings interface



7. Make sure that all the check boxes are selected and click OK

Advanced Settings

8. Make the following settings under Advanced in the HIPS Settings interface



- Optional - Enable 'Block all unknown requests if the application is not running'. Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked.
- If you are using a 64-bit system, in order to maximize the security, it is important to select 'Enable enhanced protection mode (Requires a system restart)' - Enabling this mode will activate additional host intrusion prevention techniques in Defense+ 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 CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS in Defense+.

Click here for more details on HIPS Settings

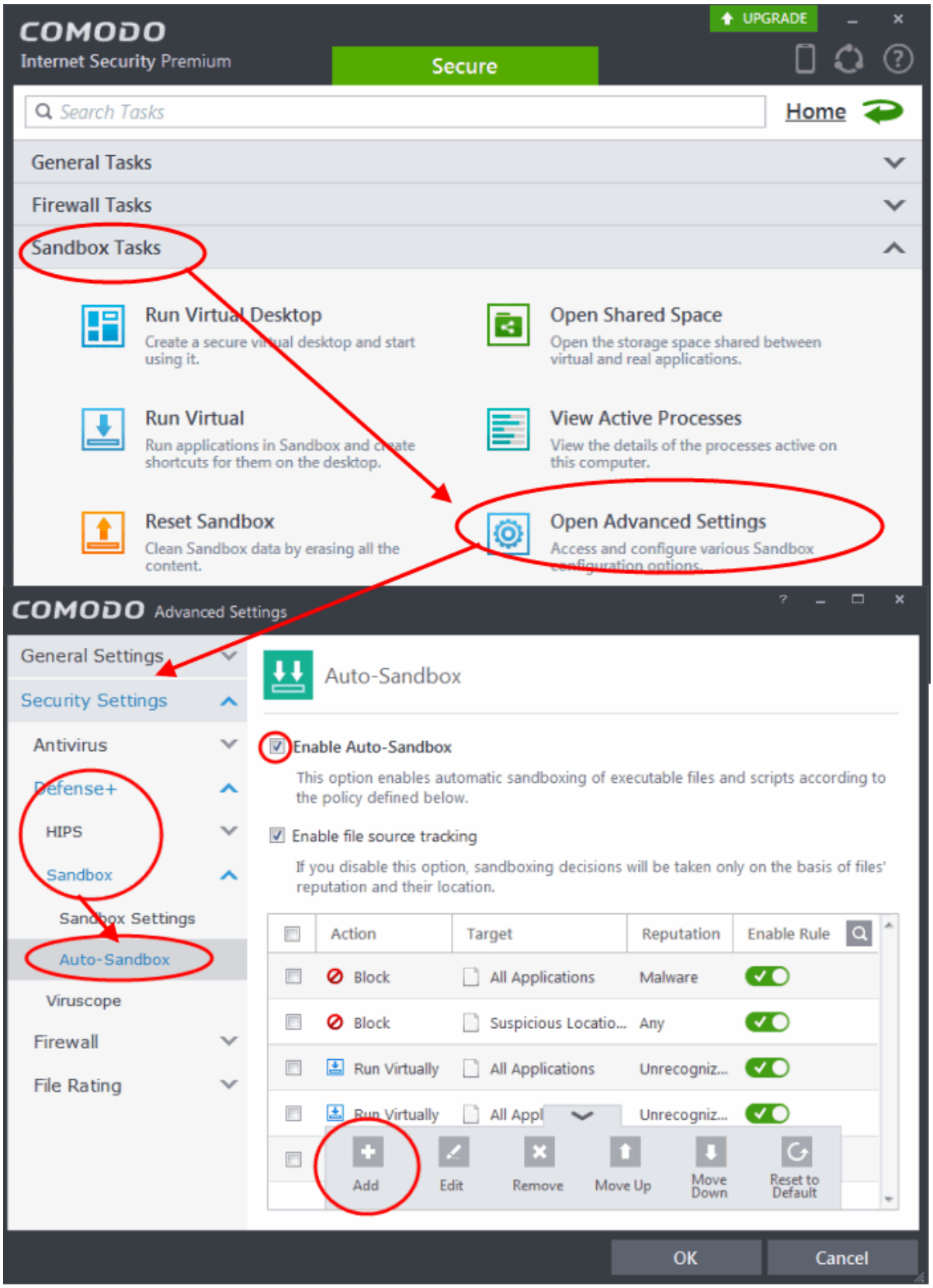
Create Rules for Auto-Sandboxing Applications

You can define rules for programs that should be run in the sandboxed environment. A sandboxed application has much less opportunity to damage your computer because it is run isolated from your operating system and your files.

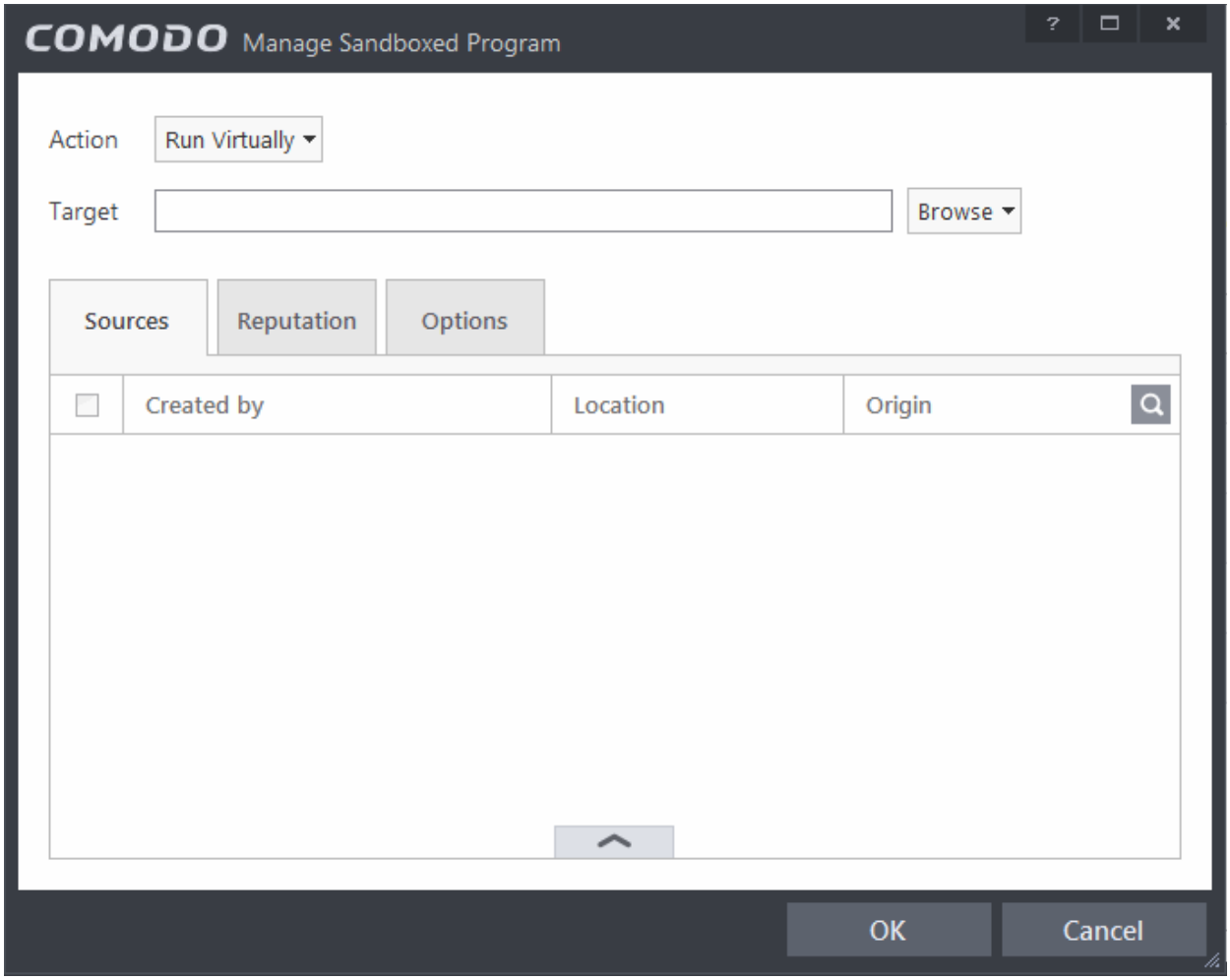
CIS ships with a set of pre-defined auto-sandbox rules that are configured to provide maximum protection for your system. Before creating a rule, check if your requirement is met by the default rules. Refer to the section **Configuring Rules for Auto-Sandbox** for more details.

To create auto-sandbox rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Sandbox Tasks' and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'Sandbox' > 'Auto-Sandbox' from the left hand side pane
4. Click the handle at the bottom of the interface and open the option panel



5. Click the Add button

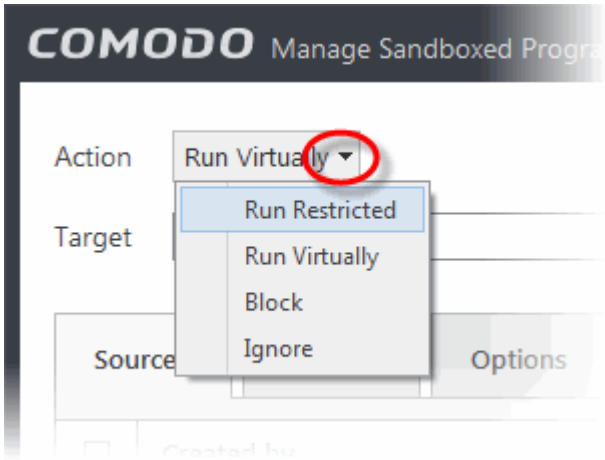


The Manage Sandboxed Program screen will be displayed.

- **Step 1** - Select the Action
- **Step 2** - Select the Target
- **Step 3** - Select the Sources
- **Step 4** - Select the File Reputation
- **Step 5** - Select the Options

Step 1 - Select the Action

The options under the Action drop-down button combined with the Set Restriction Level setting in the Options tab determine the amount of privileges an auto-sandboxed application has access to other software and hardware resources on your computer.

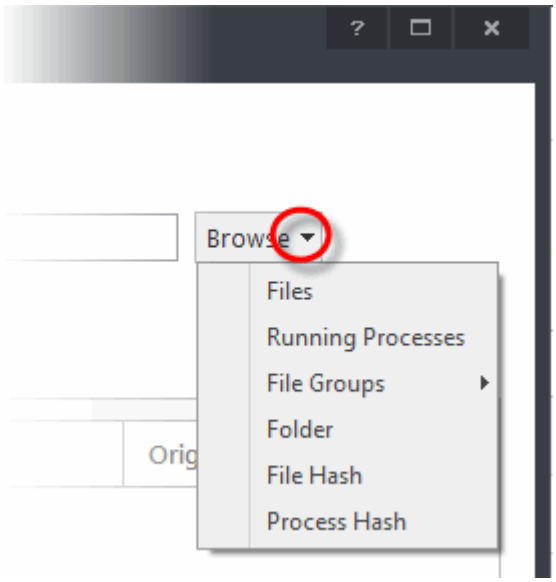


The options available under the Action button are:

- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Run Restricted** - The application is allowed to access 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 sandboxed and allowed to run with all privileges.

Step 2 - Select the Target

The next step is to select the target to which the auto-sandbox rule is to be applied. Click the Browse button beside the Target field.



You have five options available to add the target path.

- **Files** - Allows to add individual files as target.
- **Running Processes** - As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** - Allows to add predefined File Groups as target. To add or modify a predefined file group refer to the section **File Groups** for more details.
- **Folder** - Allows you to add a folder or drive as the target
- **File Hash** - Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

Click here to know more about adding each of the options.

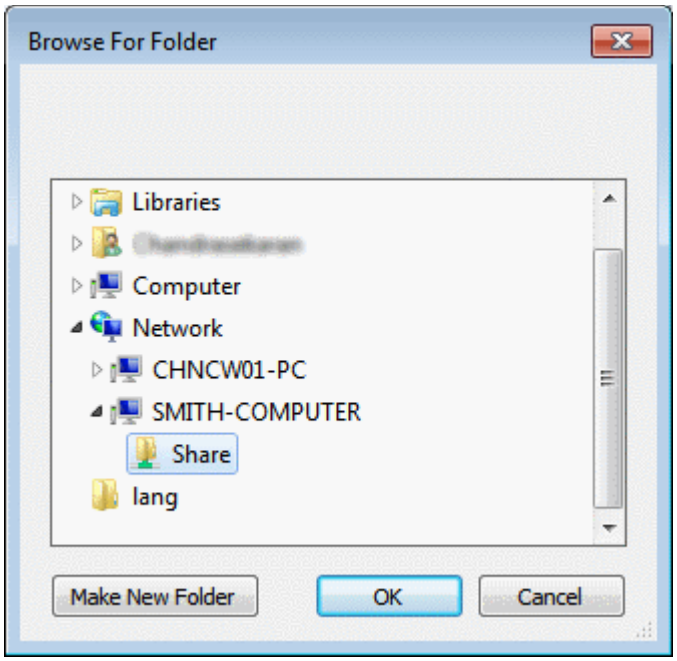
Step 3 - Select the Sources

If you want to include a number of items for a rule but want the rule to be applied for certain conditions only, then you can do this in this step. For example, if you include all executables in the Target but want the rule to be applied for executables that were downloaded from the internet only, then the filter can be applied in the Sources. Another example is if you want to run unrecognized files from network share, you have to create an ignore rule with All Applications as target and source located on network drives.

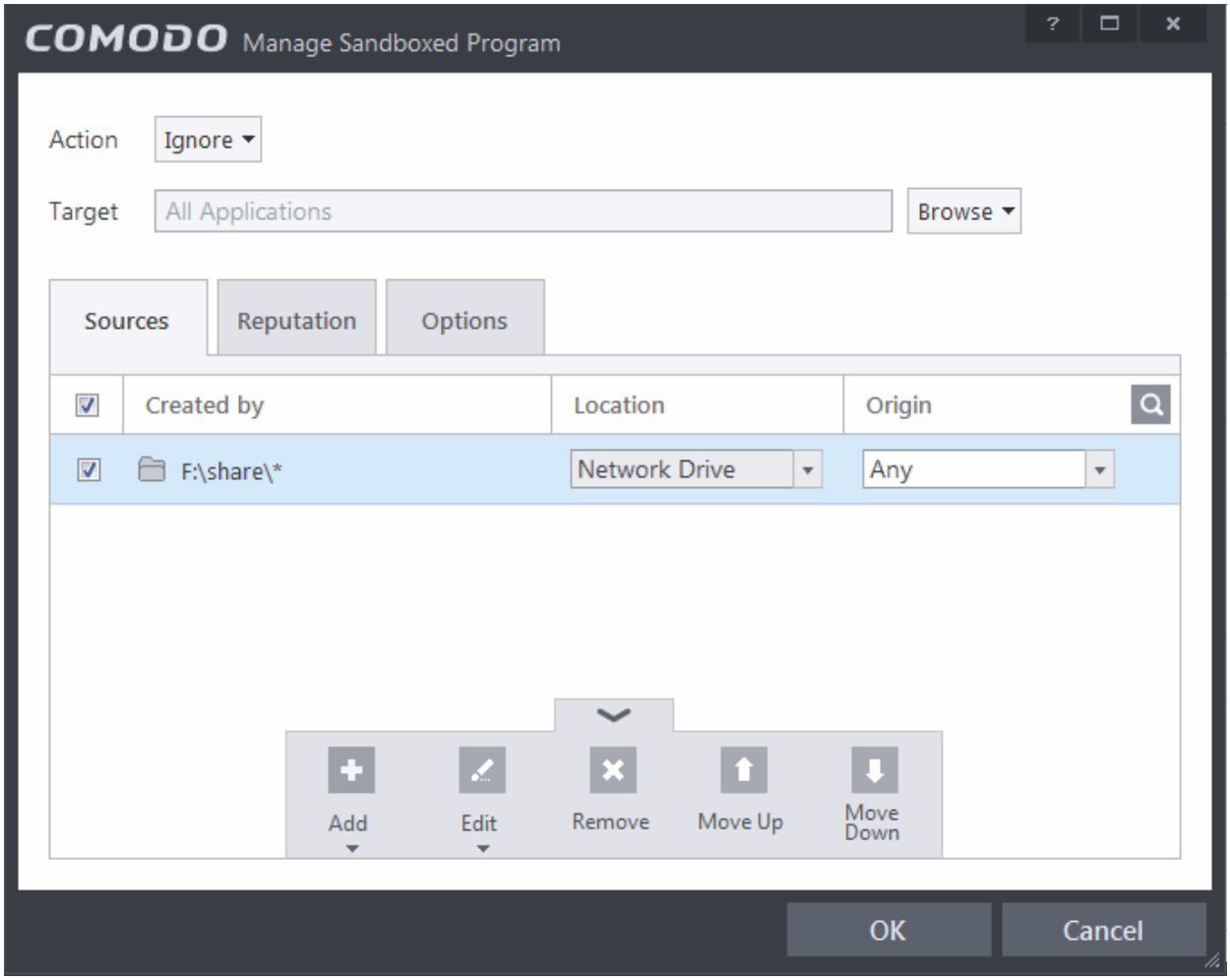
The following example describes how to add an Ignore rule for Unrecognized files from a network source:

- In **Step 1**, select the action as Ignore
- In **Step 2**, select the Target as All Applications in File Groups
- In **Step 3**, click Folder from the Add options.

The Browse For Folder dialog will be displayed.



- Navigate to the source folder in the network, select it and click 'OK'.



The selected network source folder will be added under the 'Created by' column and the screen displays the options to specify the location and from where the files were downloaded.

- **Location** - The options available are:
  - Any
  - Local Drive
  - Removable Drive
  - Network Drive

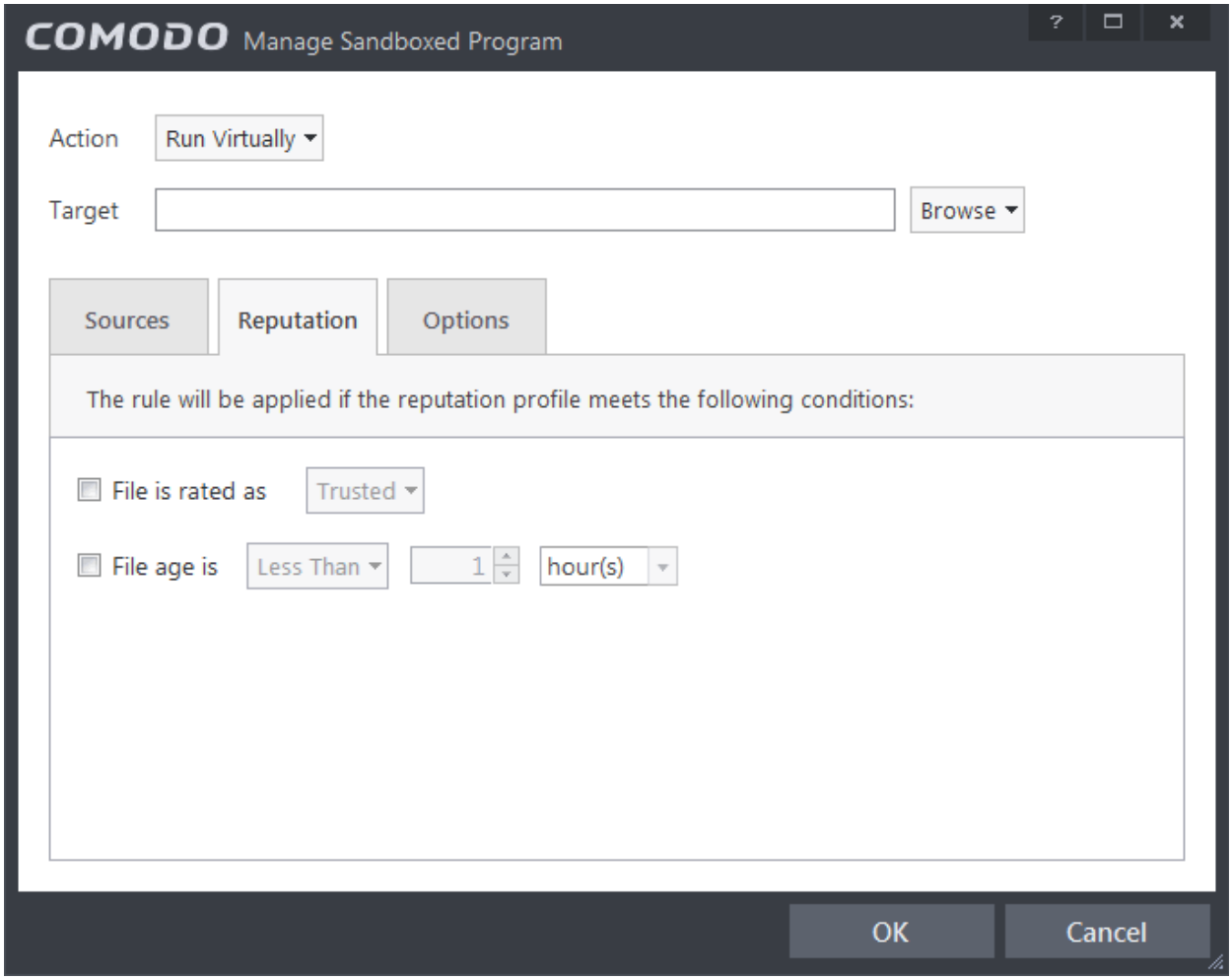
Since the source is located in a network, select Network Drive from the options.

- **Origin** - The options available are:
  - Any - The rule will apply to files that were downloaded to the source folder from both Internet and Intranet.
  - Internet - The rule will apply to files that were downloaded to the source folder from Internet only.
  - Intranet - The rule will apply to files that were downloaded to the source folder from Intranet only.

Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options in **Step 4**.

Step 4 - Select the File Reputation

- Click the Reputation tab in the Manage Sandboxed Program interface.



By default, the file rating is not selected meaning the rating could be Any. The options available are:

- **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by Defense+. Refer to the sections **File Rating Settings** and **Trusted Files** for more information.
- **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section '**File List**' for more information.
- **Malware** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. Refer the section **Unknown Files - The Scanning Process** for more information.

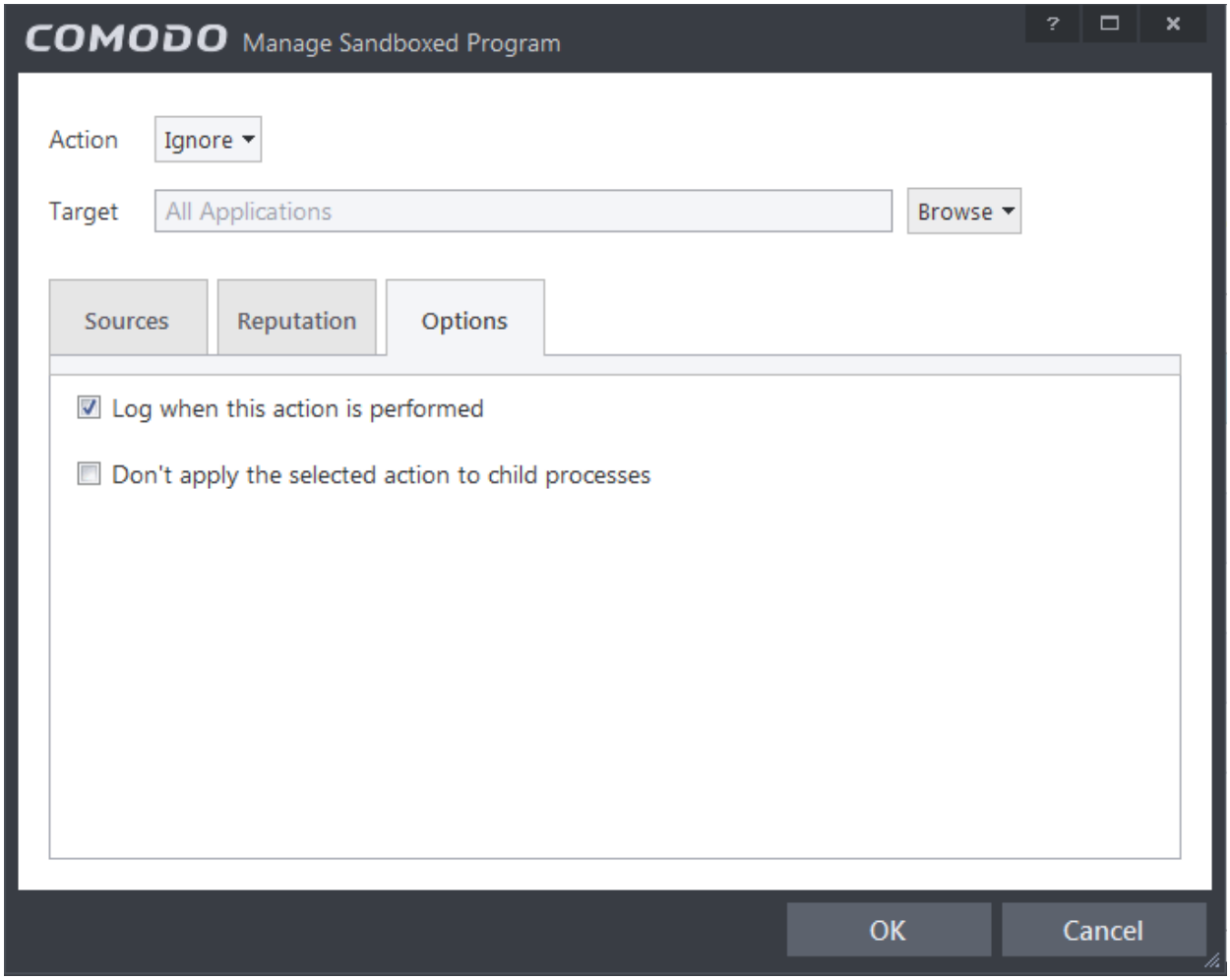
By default, file age is not selected, so the age could be Any. The options available are:

- Less Than – CIS will check for reputation if a file is younger than the age you set here. Select. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 1 hours)***
- More Than - CIS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (***Default and recommended = 1 hours)***

Select the category from the options. Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options.

Step 5 - Select the Options

- Click the Options tab in the Manage Sandboxed Program interface.



By default, the 'Log when this action is performed' The options available for Ignore action are:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** - Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CIS treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
    - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
    - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox 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. For actions - Run Restricted and Run Virtually - the following options are available:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Set Restriction Level** - When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
    - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(***Default***)
    - **Limited -** Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
    - **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.

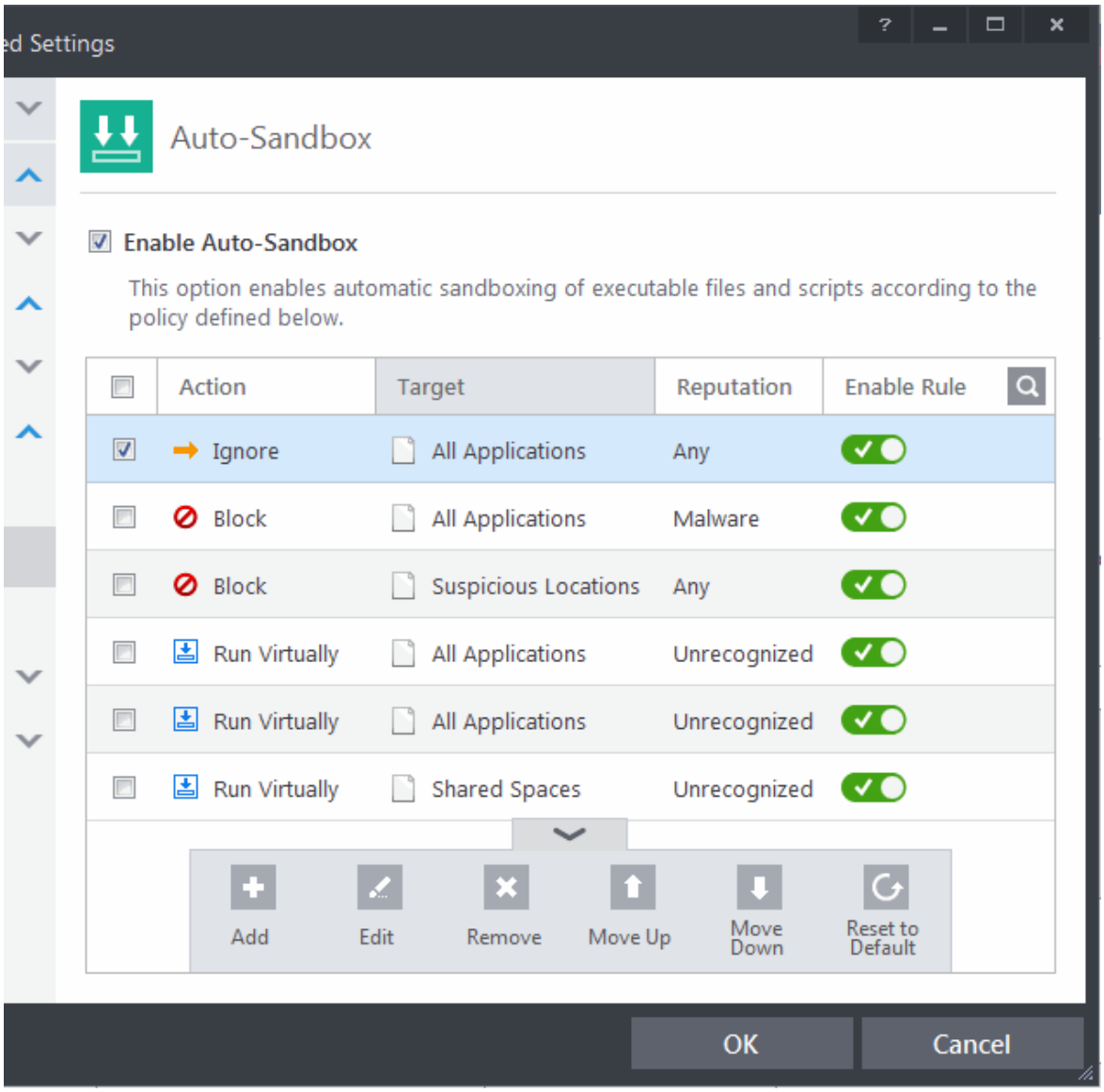
- **Untrusted -** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.

- **Limit maximum memory consumption to** - Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** - Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For Block action, the following options are available:

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Quarantine program** - If checked, the programs will be automatically quarantined. Refer to the section **Manage Quarantined Items** for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



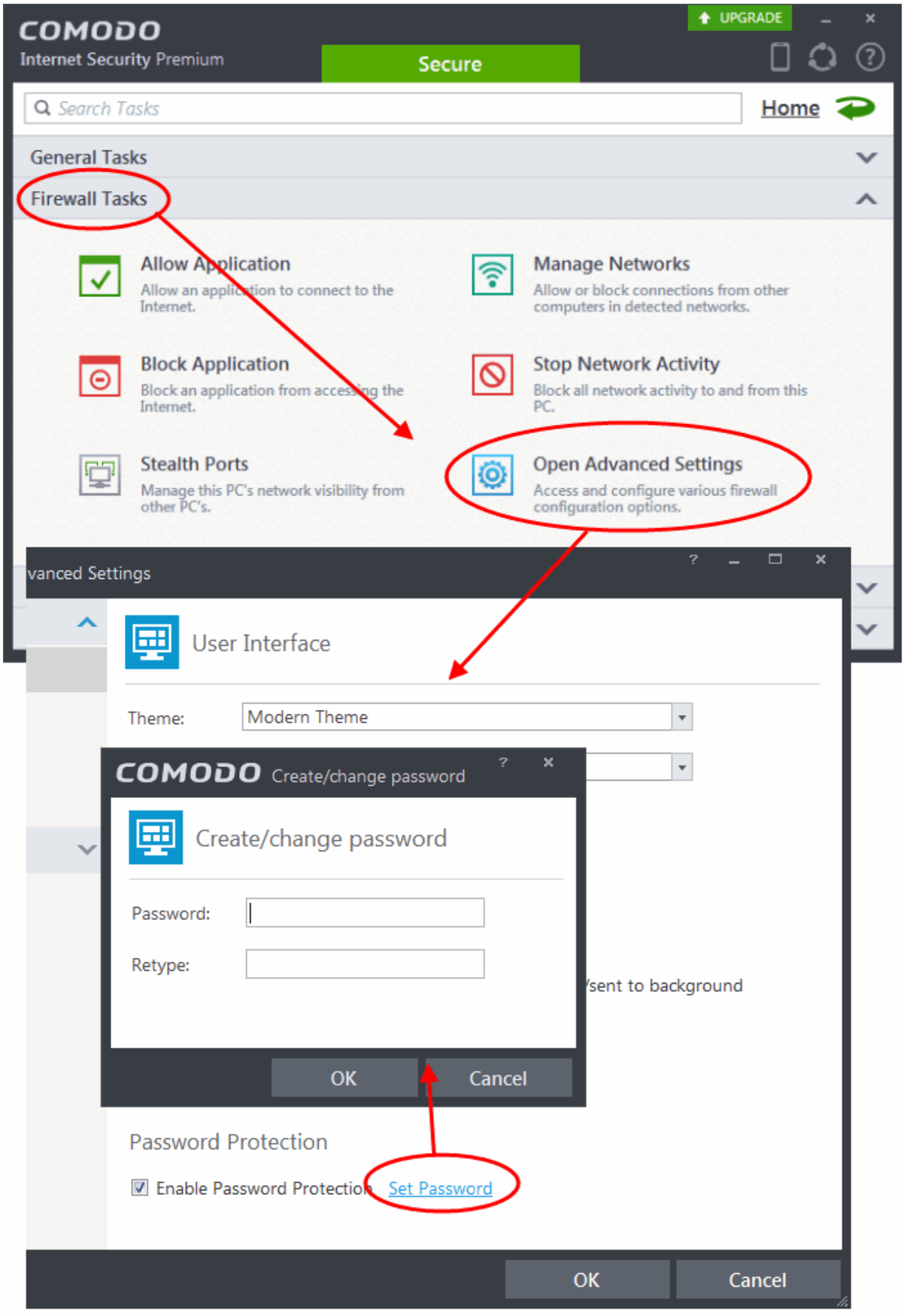
That's it. You have created an Ignore auto-sandbox rule for unrecognized files with a Network drive as source.

Password Protect Your CIS Settings

This page explains how to password protect access to the CIS interface. Implementing the steps explained on this page means another user will not be able to access the CIS interface to modify or over-ride the security settings you have implemented.

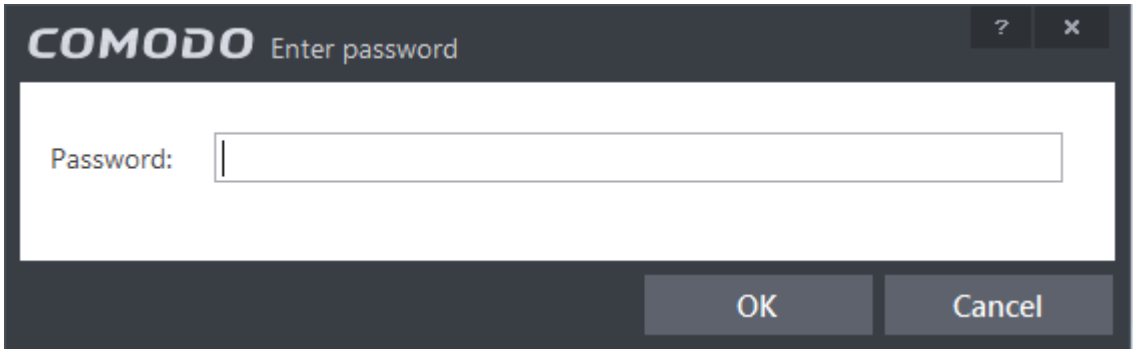
To enable password protection

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'User Interface' under General Settings from the left hand side pane



4. Select 'Enable Password Protection' under 'Parental Control' and click 'Set Password' link. The Change password dialog will appear.
5. Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

The configuration is now password protected. From the next attempt to change any configuration changes to CIS, you will be prompted to enter the password to proceed.



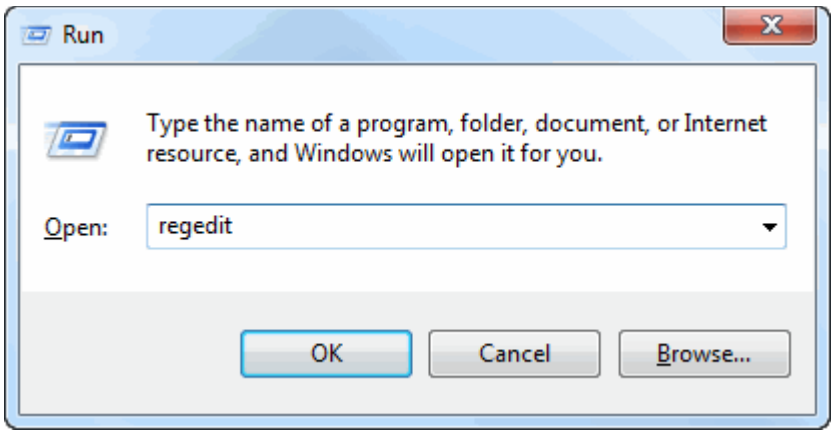
Reset Forgotten Password (Advanced)

This page explains how to remove password protection/reset password just in case you forgot the password you had set for COMODO Internet Security.

Note: It is not possible to 'retrieve' a forgotten password - you can only reset it. To do this involves modification of the Windows registry and is only recommended for experienced users.

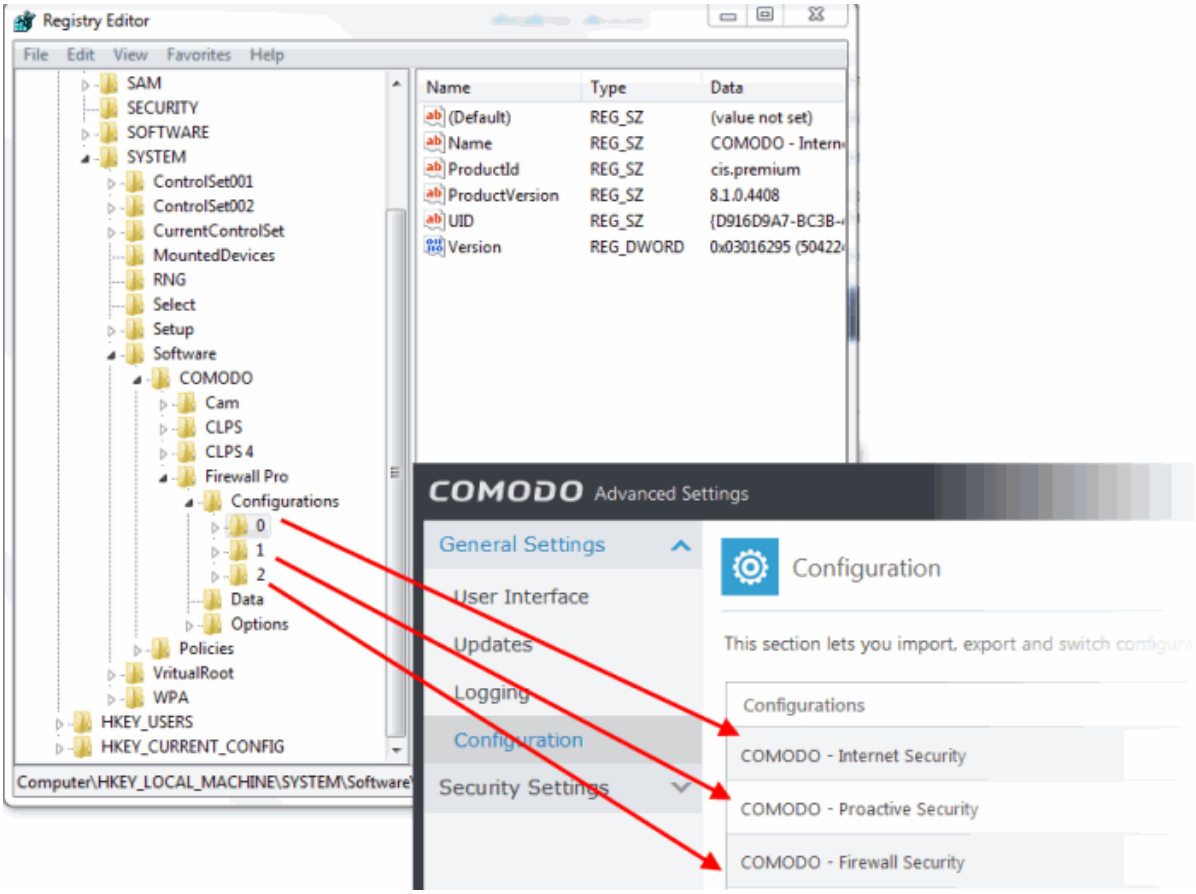
To disable password protection in CIS

1. Click Start > Run, from the Windows Start menu
2. Type 'regedit' in the text box and click 'OK'

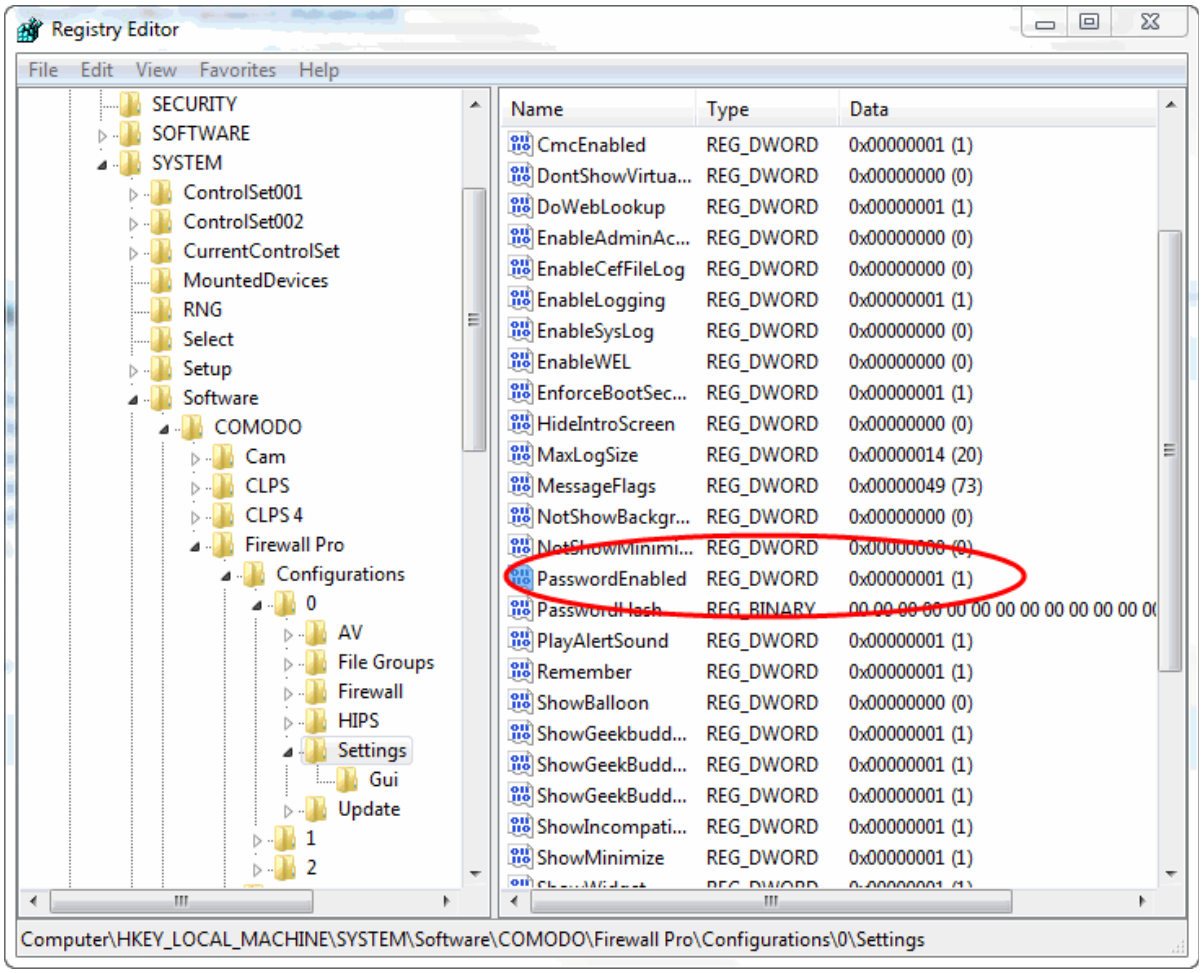


3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\

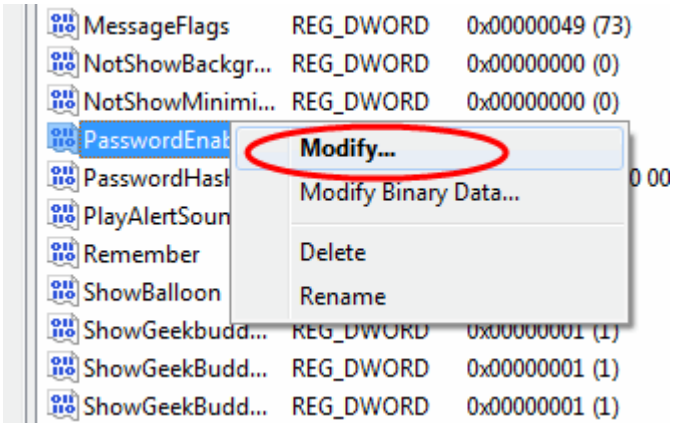
Under the Configurations folder you will see sub-folders named 0,1,2,... depending on the number of preset configurations in CIS. These folders contain registry keys for the settings of the preset configurations in the order of the configurations displayed in **Advanced Settings > General Settings > Configuration** interface. For example, the folder 0 contains the keys for COMODO - Internet Security, the folder 1 contains the keys for COMODO - Proactive Security and so on.



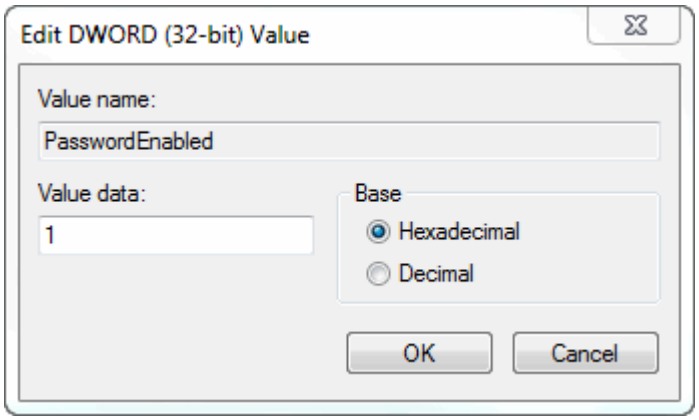
4. Select the folder corresponding to the configuration for which you wish to reset the password and navigate to Settings, for exaregeditmple, navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\0\Settings to reset password in COMODO - Internet Security configuration.



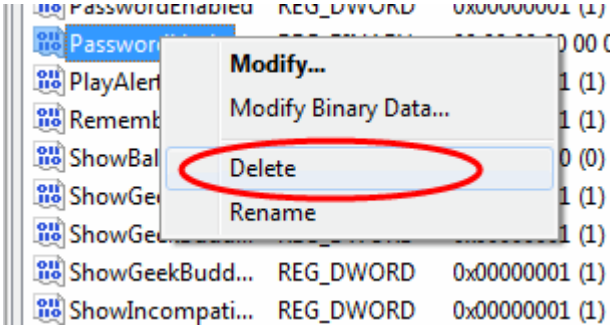
5. Right-click 'PasswordEnabled' key and select 'Modify'



6. In the 'Edit DWORD Value dialog box, change the 'Value data' from 1 to 0



7. Click 'OK'
8. Right-click 'PasswordHash' and select 'Delete'.



9. Restart the system for the changes to take effect

Now you should be able to access all settings, uninstall CIS and set a new password.

Note: If CIS doesn't allow regedit to change those registry items, try to boot in safe mode and repeat the above steps.

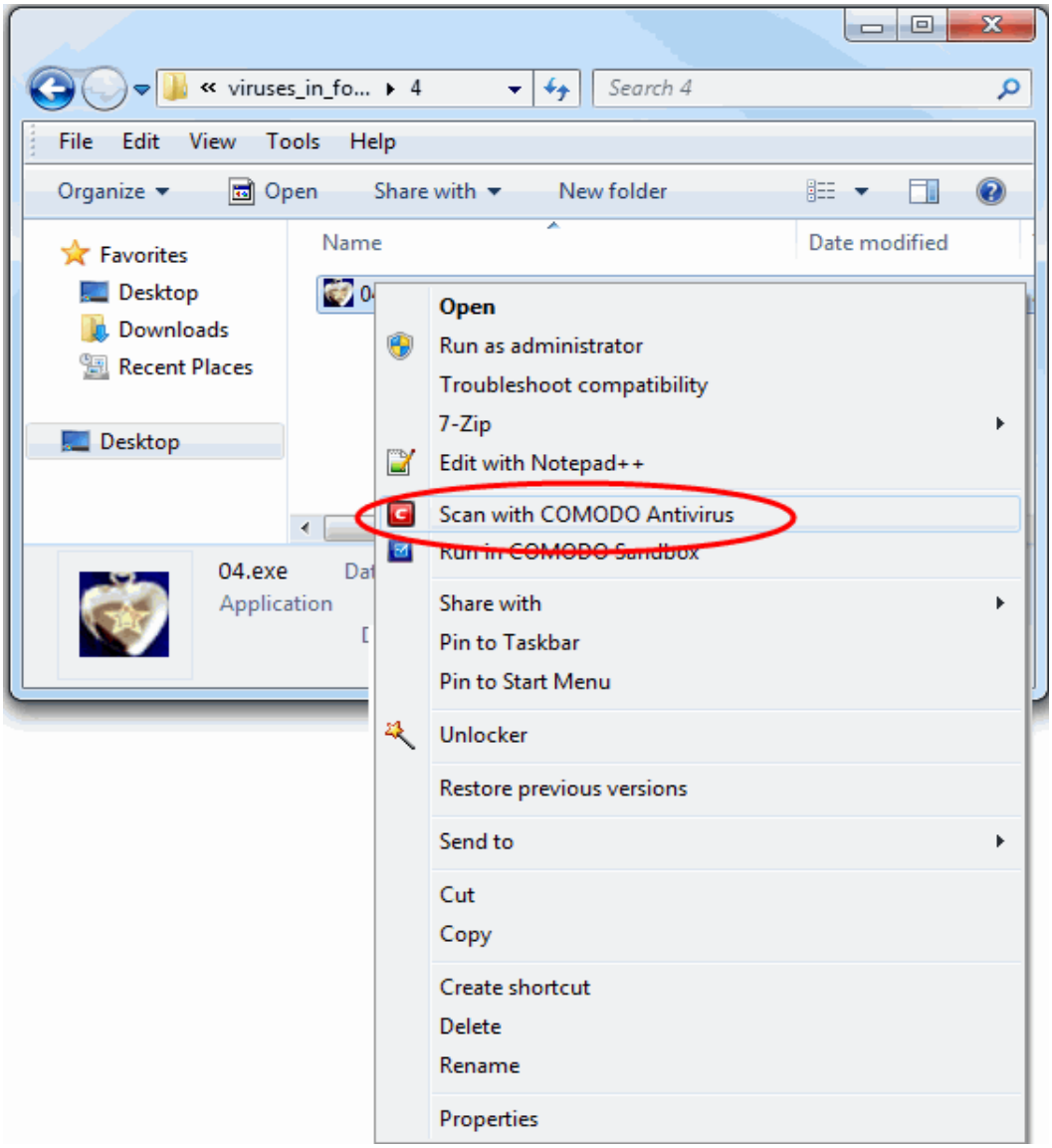
Run an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders files etc. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives, digital cameras - even your iPod and mobile phones too!!! This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from the Internet.

Click here for more details on running on-demand scans.

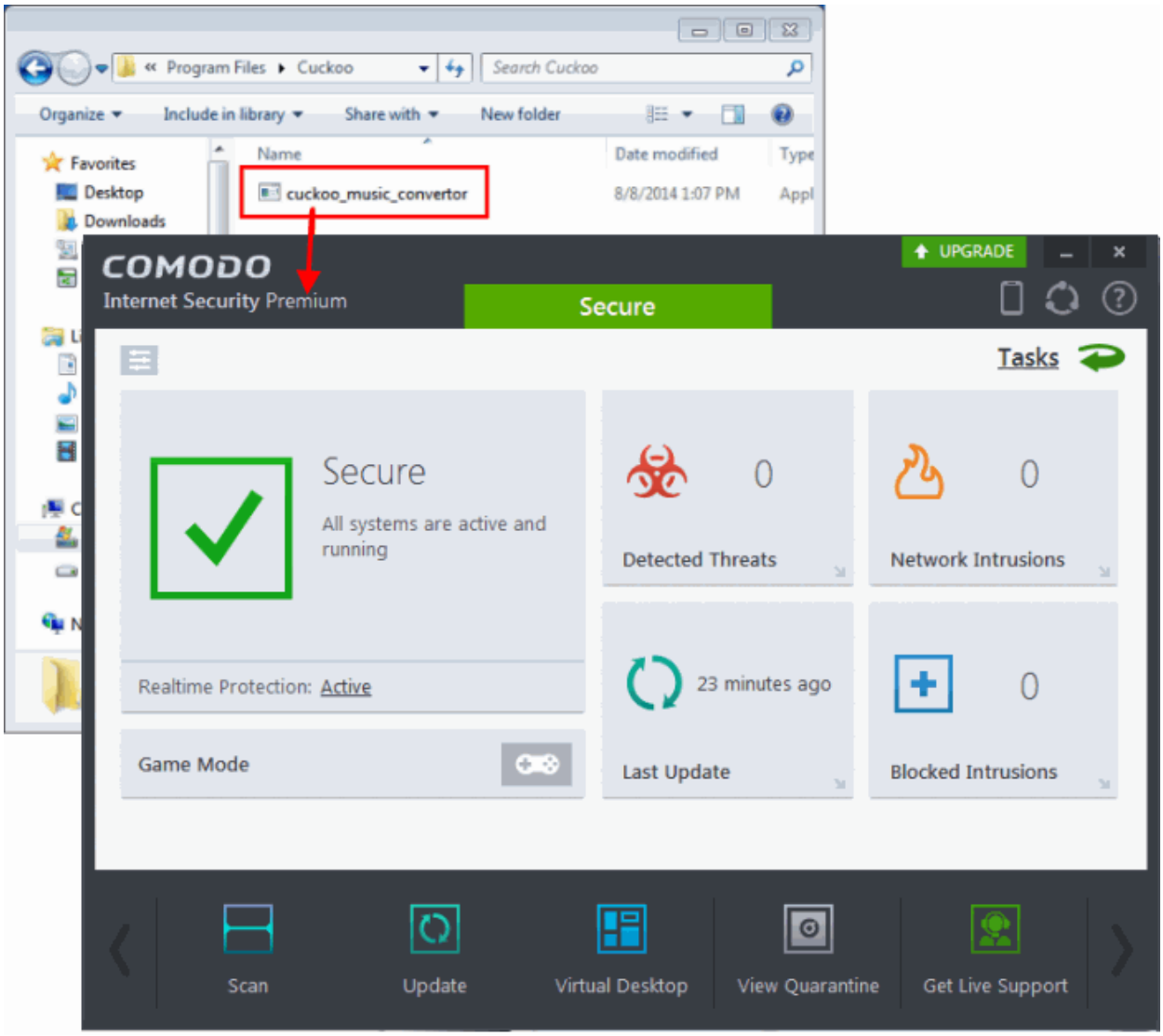
To instantly scan an item

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

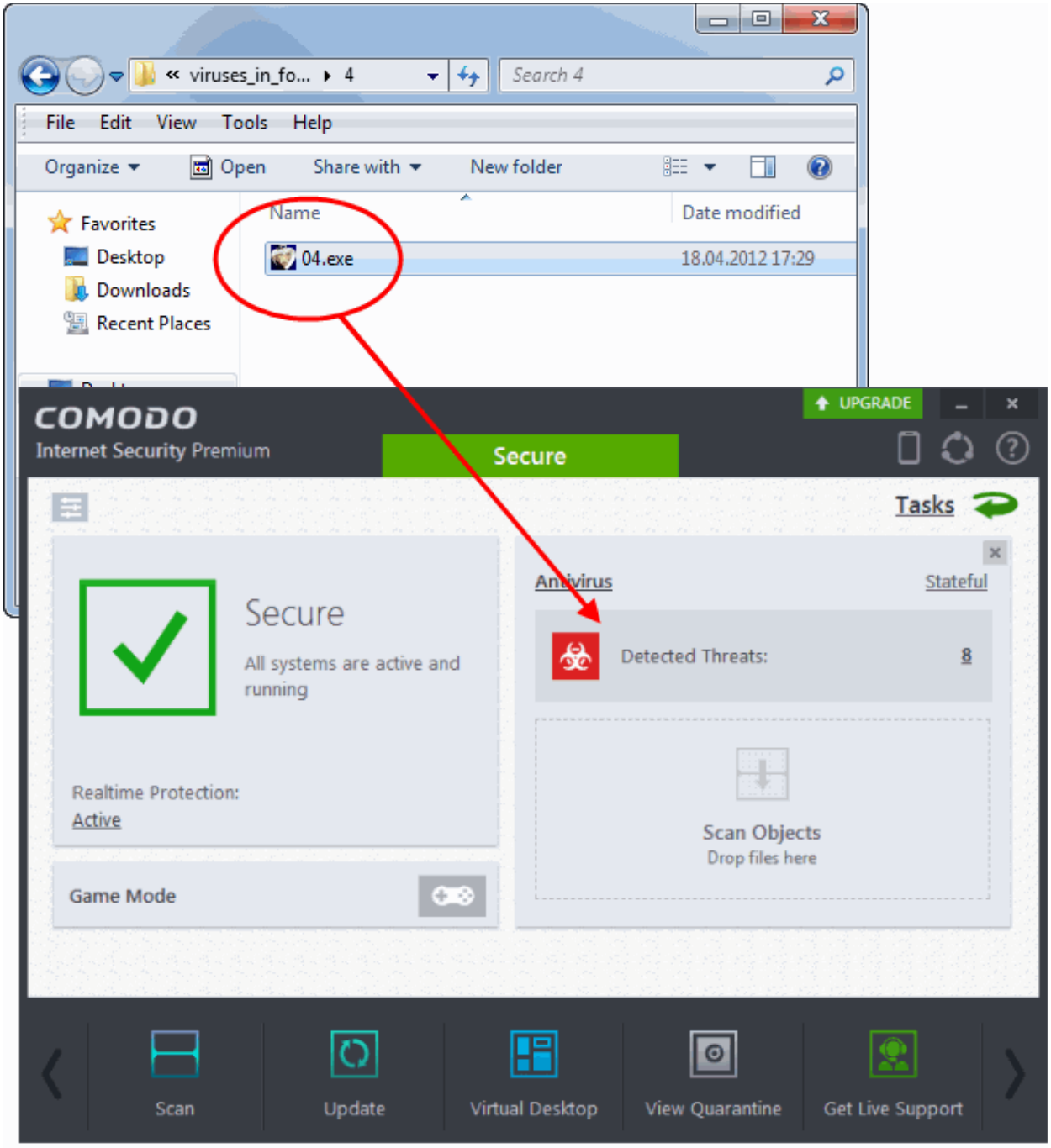


OR

- Click the Antivirus tile at the 'Home' screen in compact view to flip-open the Antivirus pane.

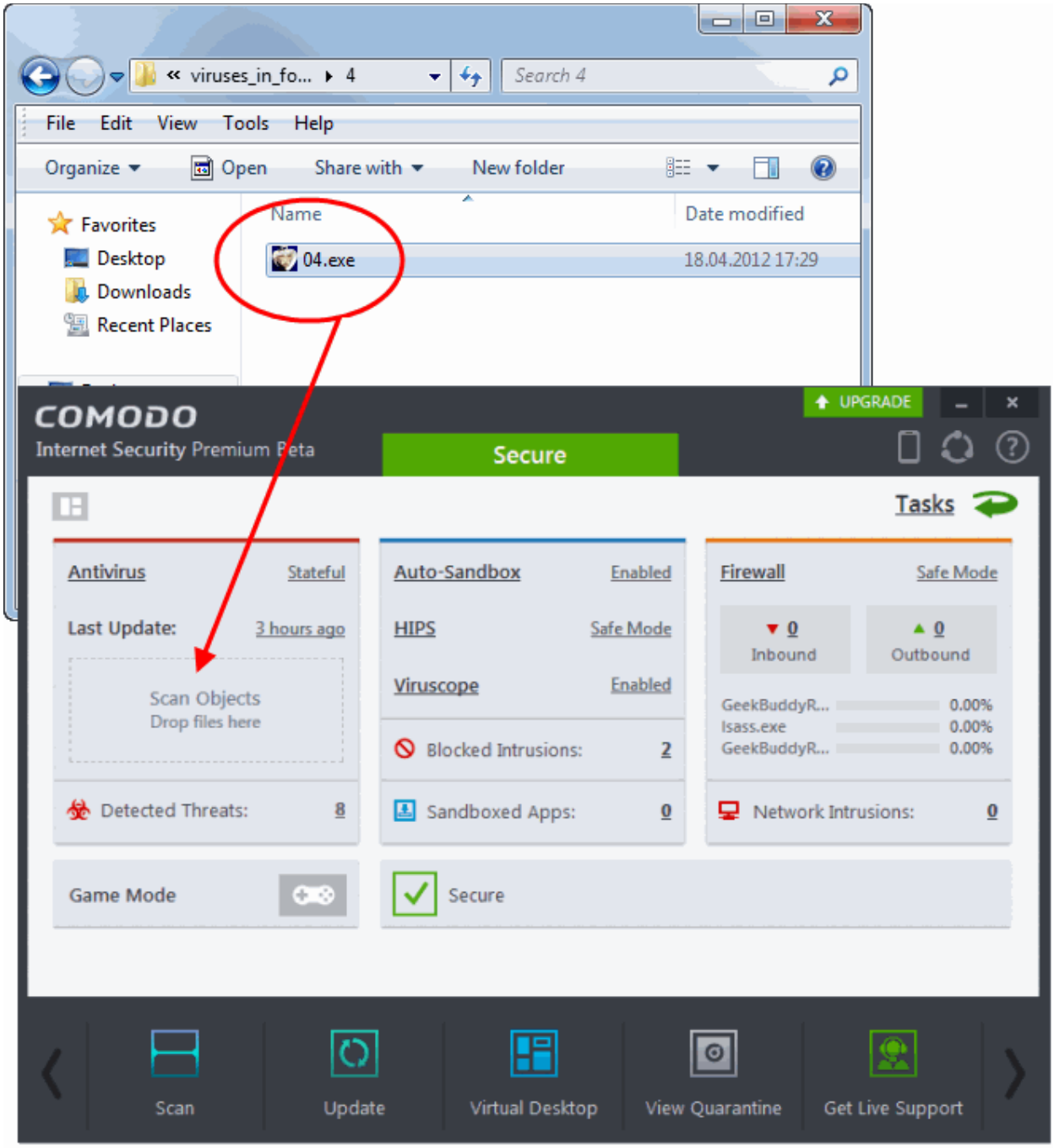


Drag and drop the item over the area marked 'Scan Objects'.

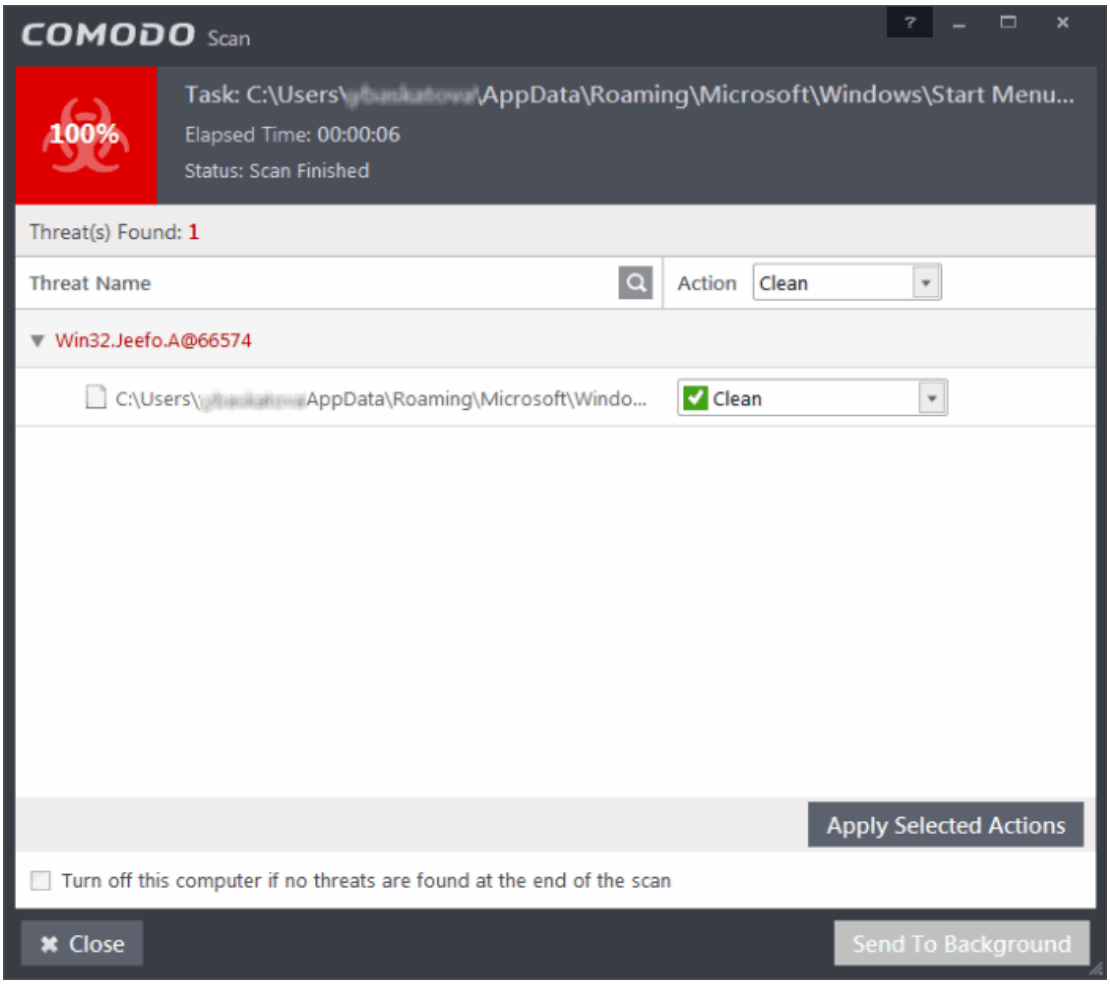


OR

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



The item will be scanned immediately.



...and on completion of scanning, the scan finished dialog be displayed with the number of threats found.

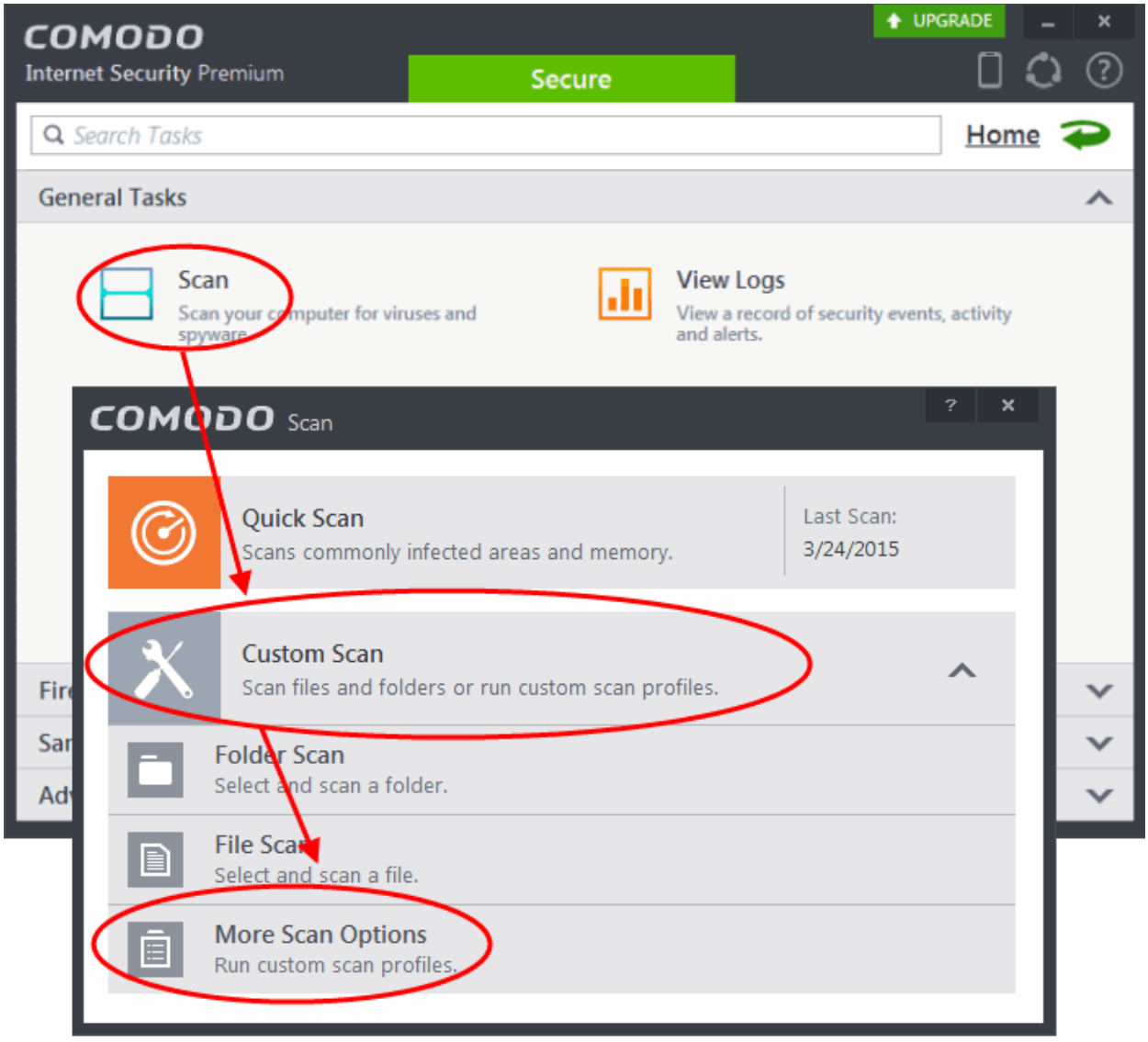
Click here for more details to take action on the infected item(s).

Create an Antivirus Scanning Schedule

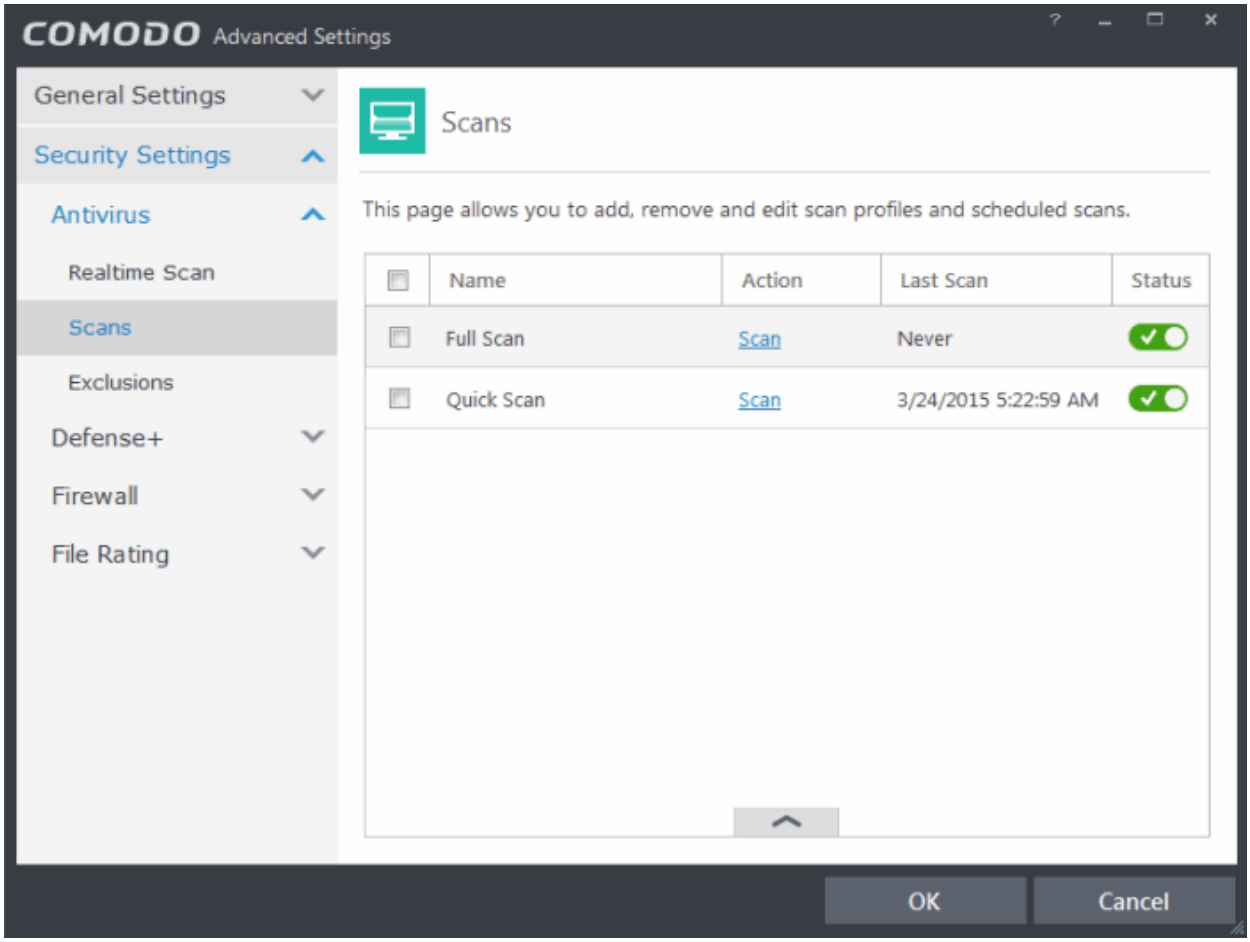
Comodo Internet Security allows you to schedule Antivirus scans on your entire system or on specific areas according to your preferences. You can create a custom scan profile defining exactly which files and folders are to be scanned, when they are to be scanned and how they are to be scanned.

To create an antivirus scanning schedule

- Click the 'Tasks' arrow on the home screen to open the main Tasks menu
- In 'General Tasks', click 'Scan'
- Select 'Custom Scan' then 'More Scan Options'

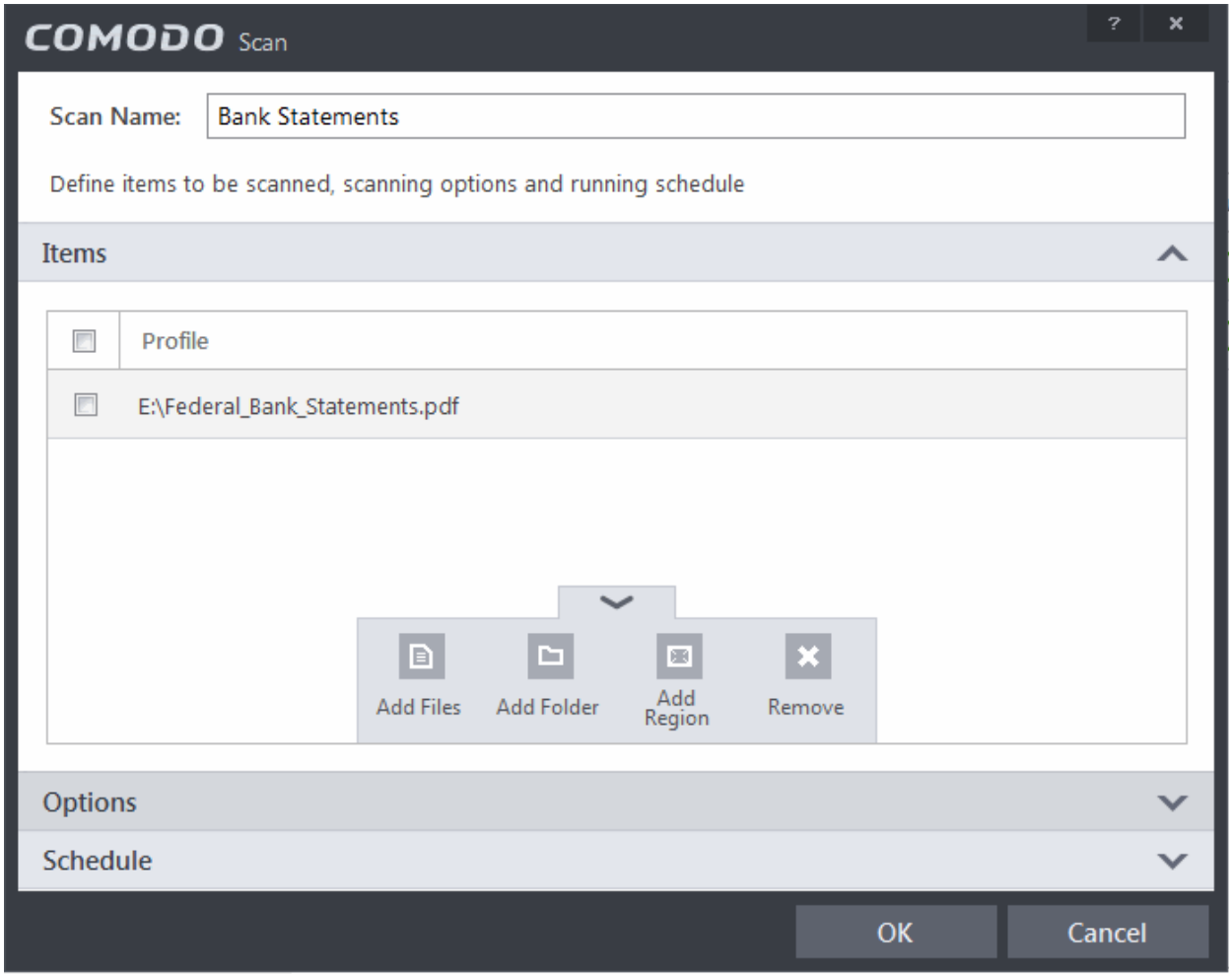


- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened
- Click the handle at the bottom of the interface then select 'Add'

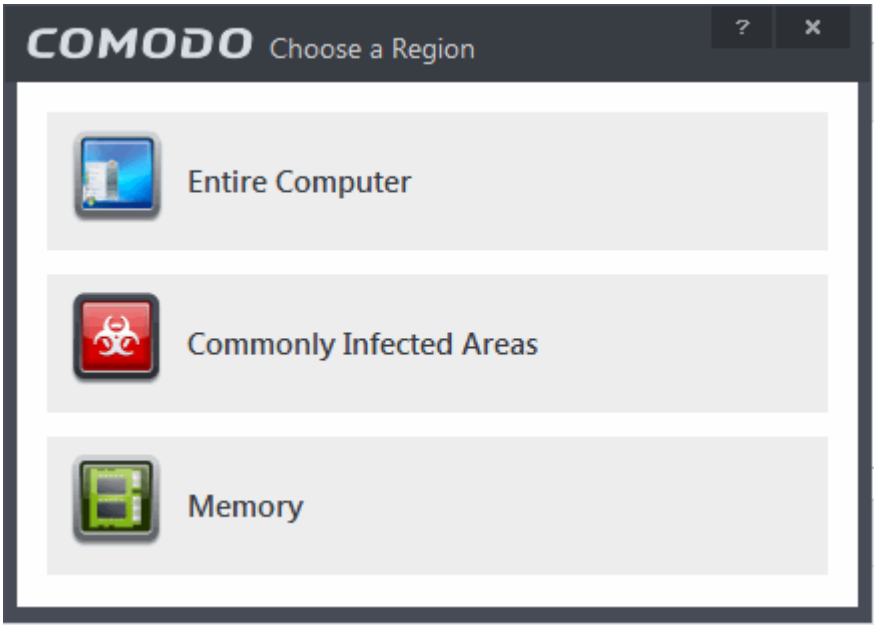


The scan profile interface will be displayed.

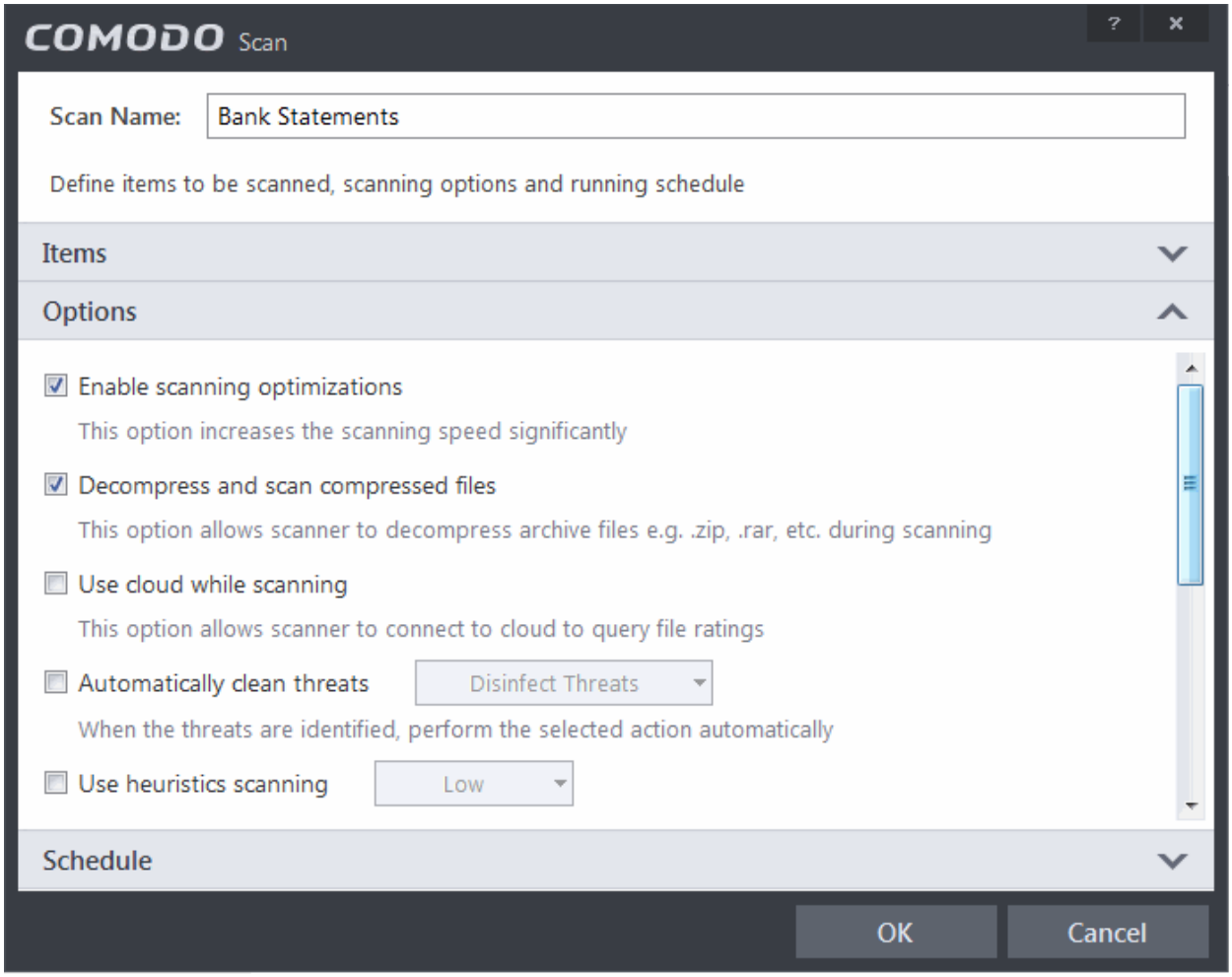
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



- **Add File** - Allows you to add individual files to the profile.
- **Add Folder** - Allows you to select entire folders to be included in the profile
- **Add Region** - Allows you to add pre-defined regions to the profile (choice of 'Full Computer', 'Commonly Infected Areas' and 'System Memory')



- Repeat the process to add more items to the profile. Click 'OK' to confirm your choice.
- Next, click 'Options' to further customize the scan:



- **Options:**
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)*** .
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)*** .
  - **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local anitvirus database is out-dated. ***(Default = Disabled)***.
  - **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine.
  - **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Disabled).***

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

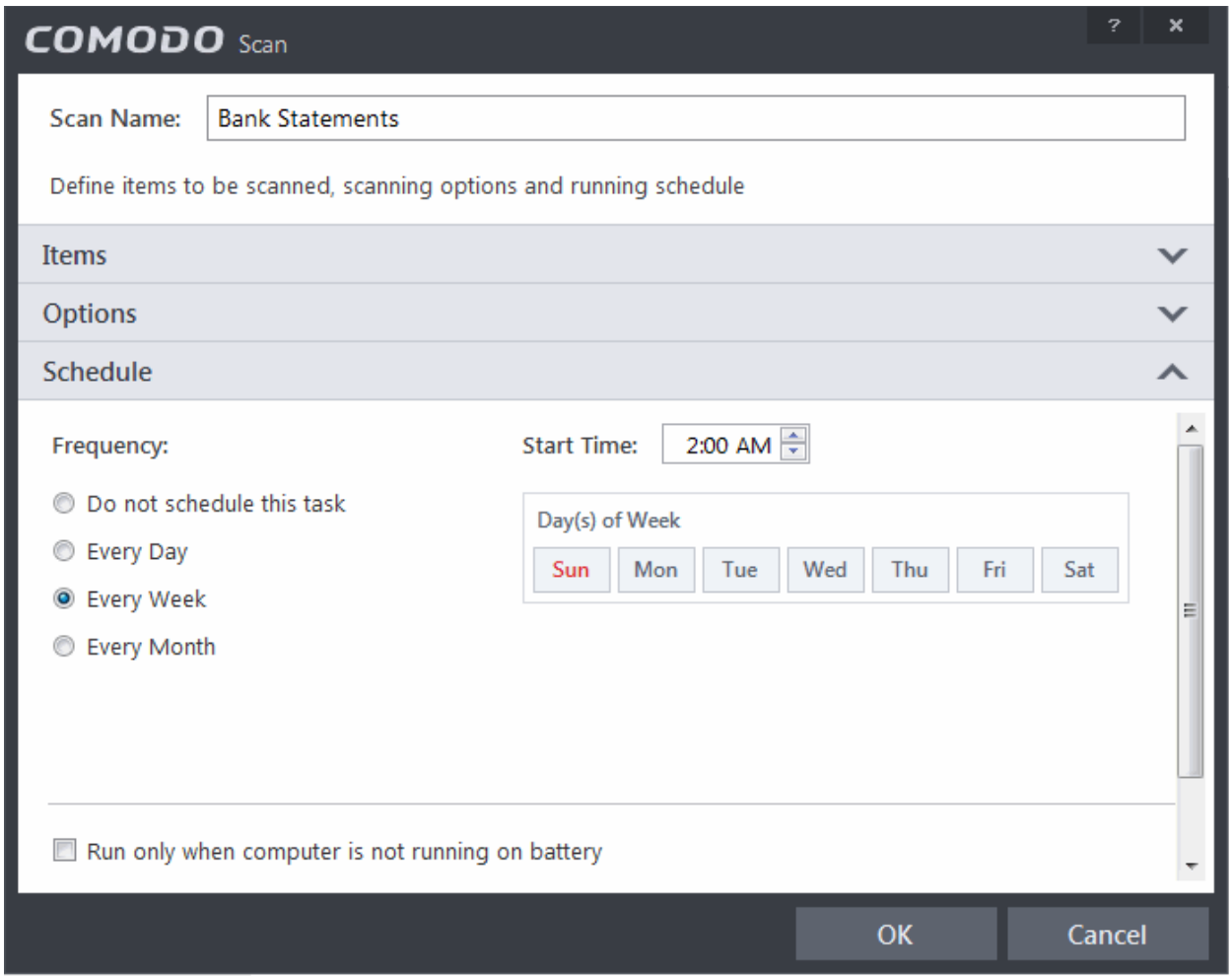
    This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

    - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.

- **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run this scan with** - Enables you to set the priority of the scan profile. You can select the priority from the drop-down.(***Default = Disabled***).
- **Update virus database before running** - Instructs Comodo Internet Security to check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning (***Default = Enabled***) .
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. (***Default = Enabled***)

- To schedule the scan to run at set intervals, click 'Schedule':



- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - The Antivurus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
- **Every Week** - The Antivurus starts scans the areas defined in the scan profile on the day(s) of the week specified

in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.

- **Every Month** - The Antivurus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
- **Run only when computer is IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.

- Click OK to save the profile.

The profile will be saved and the selected areas will be scanned repeatedly as per the set schedule.

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

Run Untrusted Programs In the Sandbox

Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:

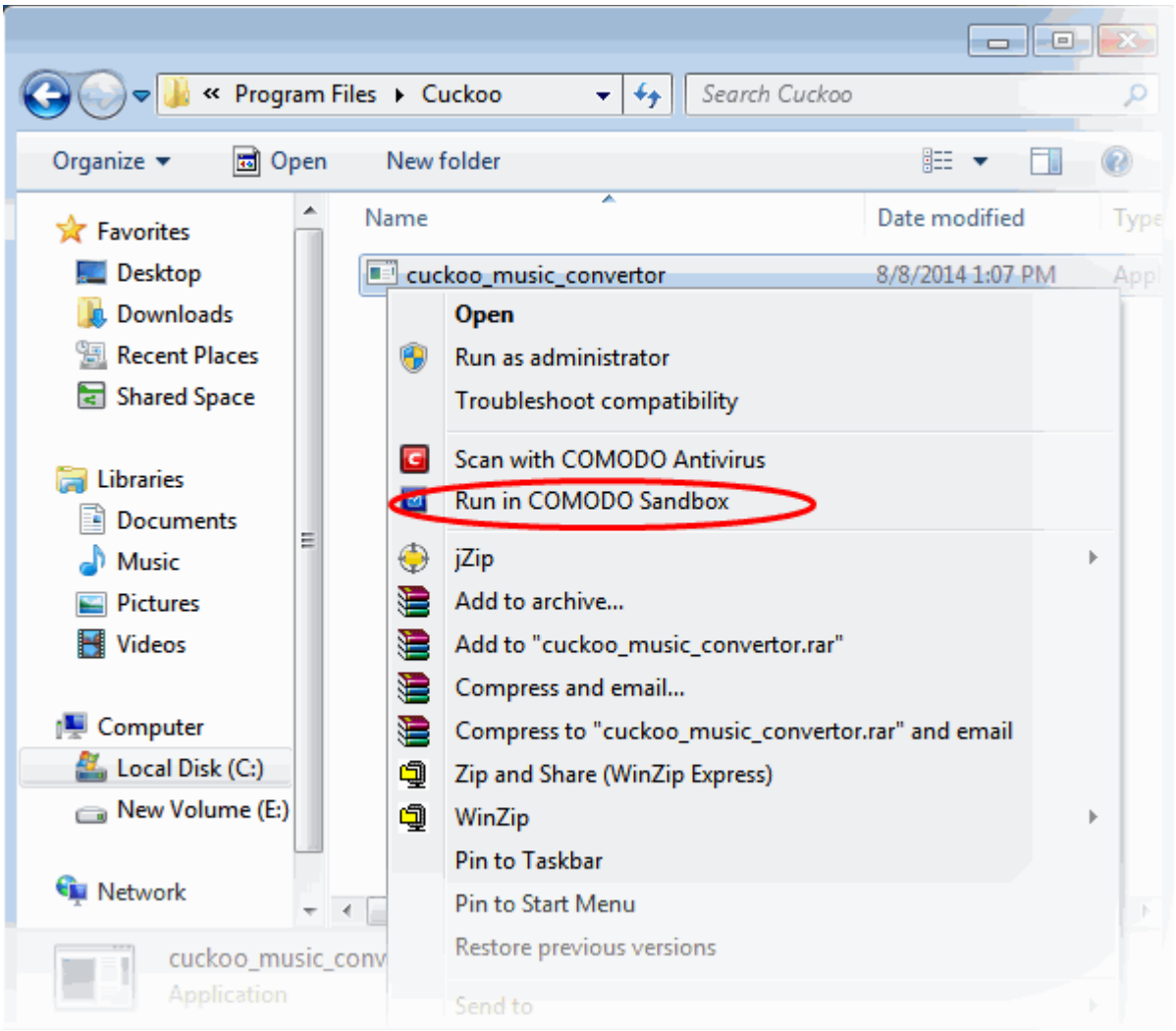
Comodo Internet Security allows you to run a program in the sandbox:

- **From the right click options**
- **From the Sandbox Tasks interface**

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

Run a program inside the sandbox through right click options

1. Browse to the installation folder of the .exe file through Windows Explorer

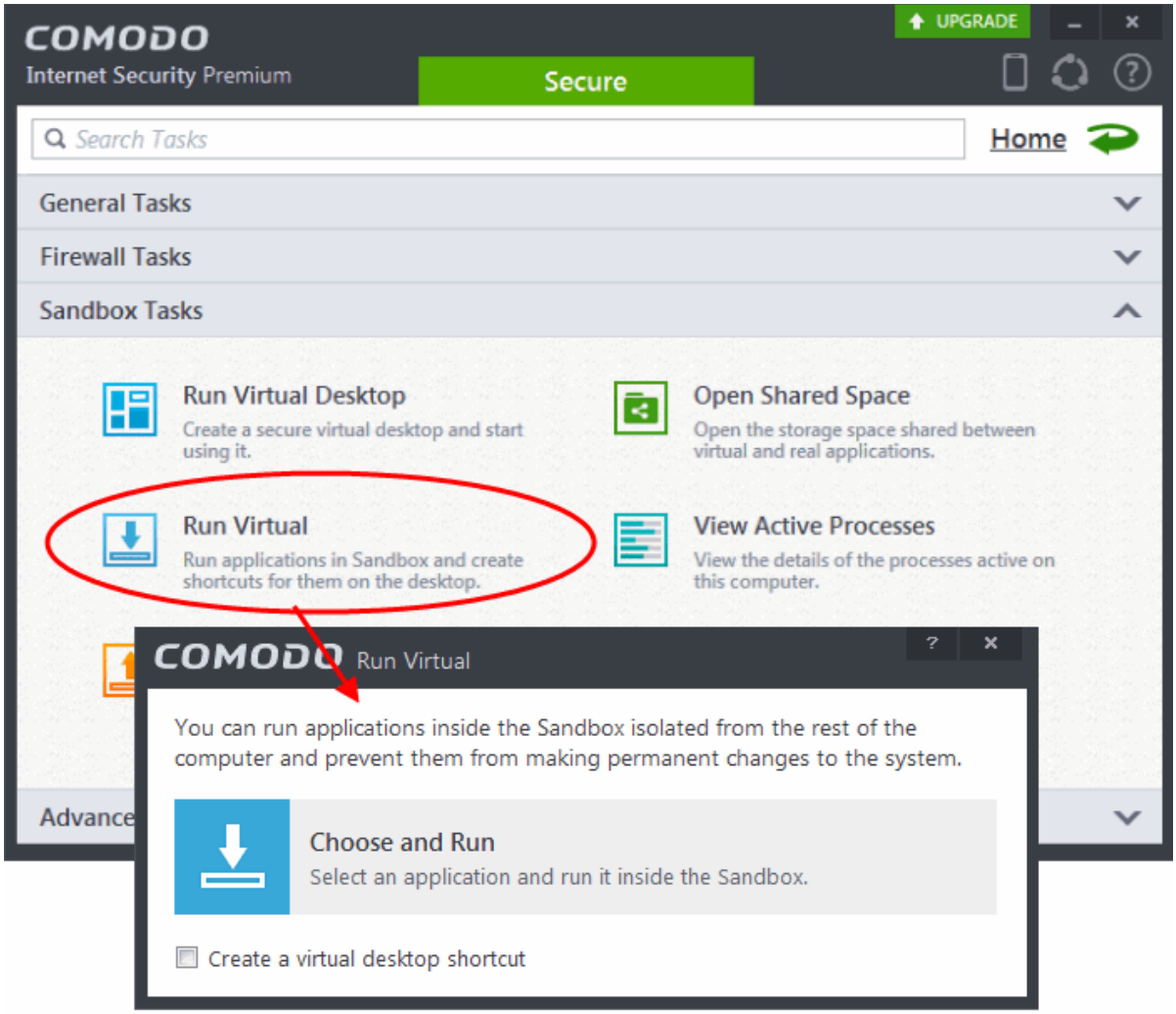


2. Right click on the program that you want to run inside the sandbox

3. Choose 'Run in Comodo Sandbox' from the context sensitive menu

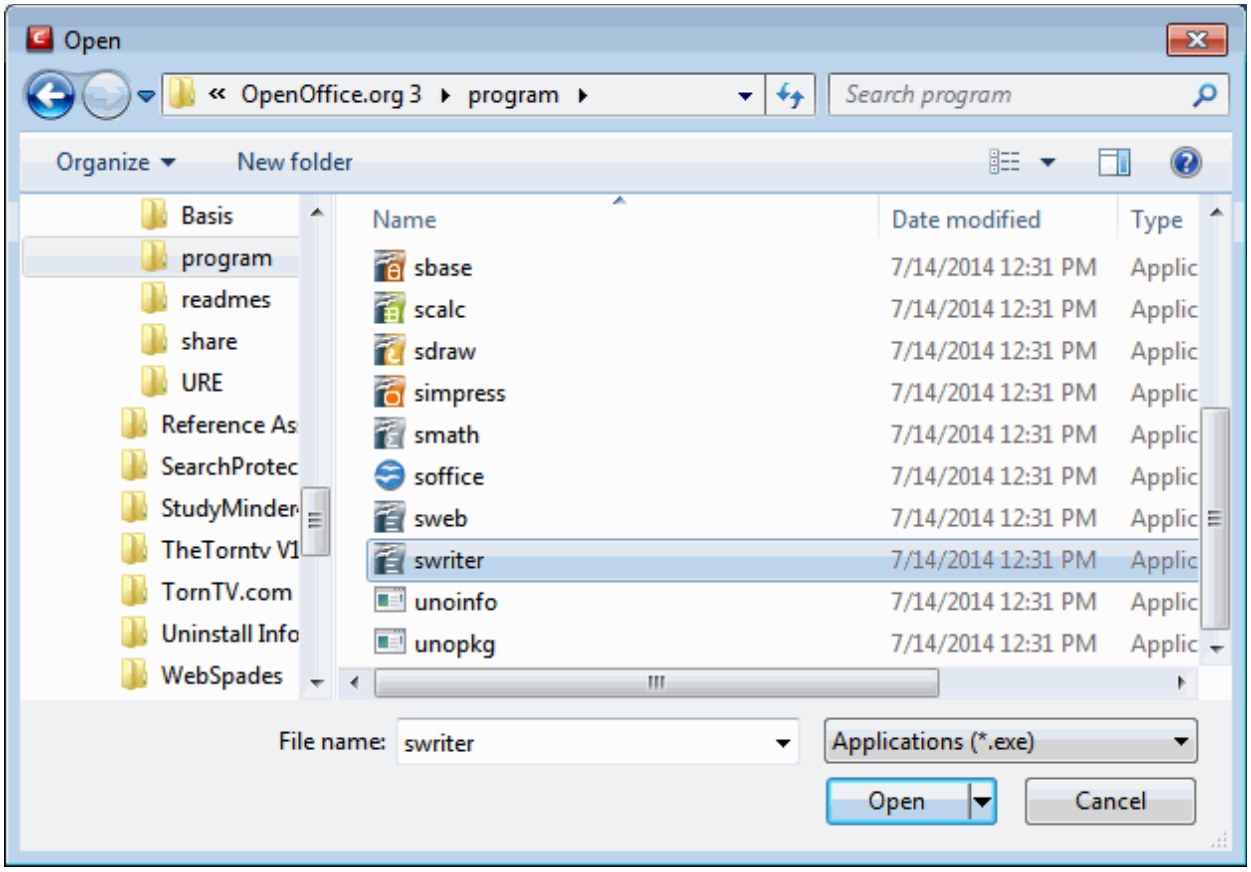
Run a program in sandbox from Sandbox Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Sandbox Tasks' and click 'Run Virtual' from the 'Sandbox Tasks' interface



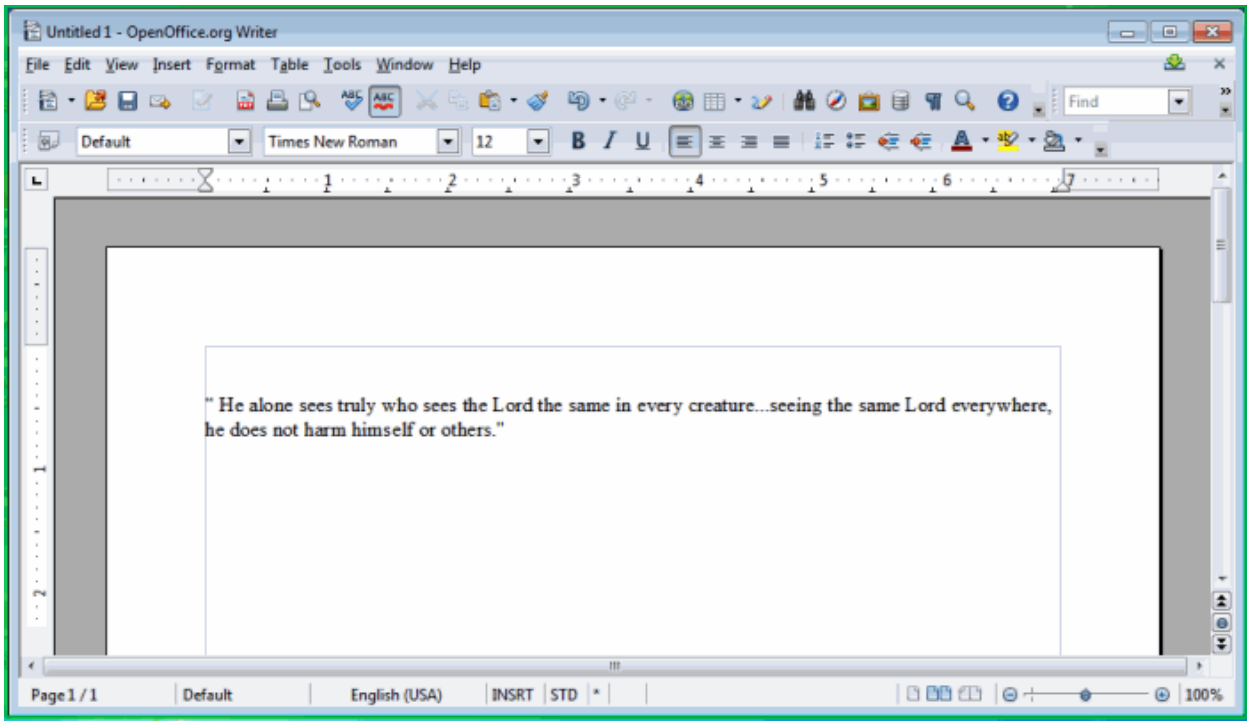
The 'Run Virtual' dialog will be displayed.

3. To run an application inside the sandbox, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is sandboxed. If you wish to run the application in the sandbox in future, then select 'Create a virtual desktop shortcut'.



4. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

The application will run in the Sandbox on this occasion only. If you often want the browser to run sandboxed then create a 'virtual shortcut' for the application by selecting the check-box 'Create a virtual desktop shortcut' in step 2. If you wish to run an application in the sandbox on a long-term/permanent basis then **add the file to the Sandbox**.



Run Browsers Inside Sandbox

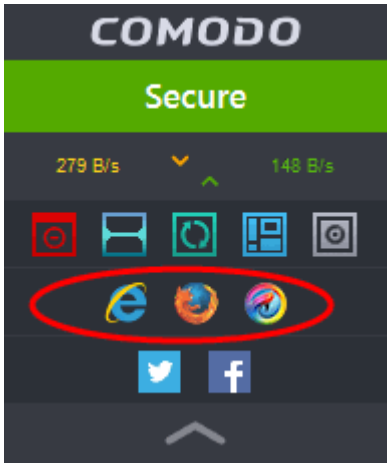
This page explains how to run your Internet browser inside the sandbox. Surfing the Internet with a sandboxed browser is the same as normal, with the benefit that any malicious files you inadvertently download cannot do damage your real computer. You can also create a desktop shortcut to run the browser inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:

Comodo Internet Security allows you to run a browser in the sandbox:

- **From the desktop widget**
- **From the Sandbox Tasks interface**

Starting a browser from the desktop widget

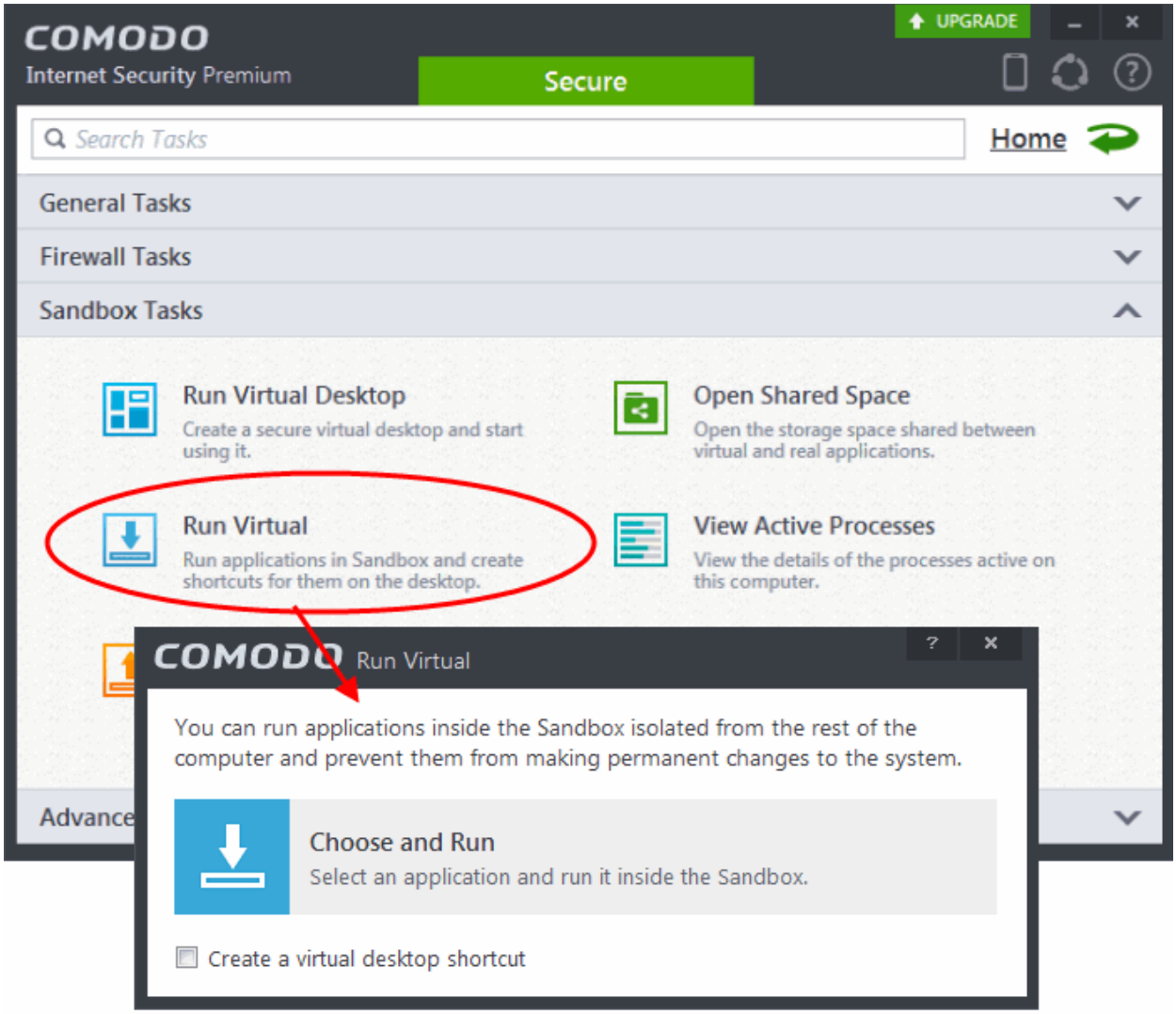
The CIS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- To start a browser inside the sandbox, click on the browser icon.

Starting a browser from the Sandbox Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Sandbox Tasks' and click 'Run Virtual' from the 'Sandbox Tasks' interface



The 'Run Virtual' dialog will be displayed.

3. To run a browser inside the sandbox, click 'Choose and Run', navigate to the installation location of the browser and select the exe file of the browser. If you wish to create a desktop shortcut to run the browser in the sandbox in future, then select 'Create a virtual desktop shortcut'.

The browser will run with a green border indicating that it is sandboxed.

Run Untrusted Programs Inside Virtual Desktop

This page explains how to run untrusted programs inside the Virtual Desktop. Applications running in the virtual desktop also leave no cookies or history behind on your real system, making it ideal for testing out beta/unstable software.

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

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

Desktop Shortcuts

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

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

Shared Space

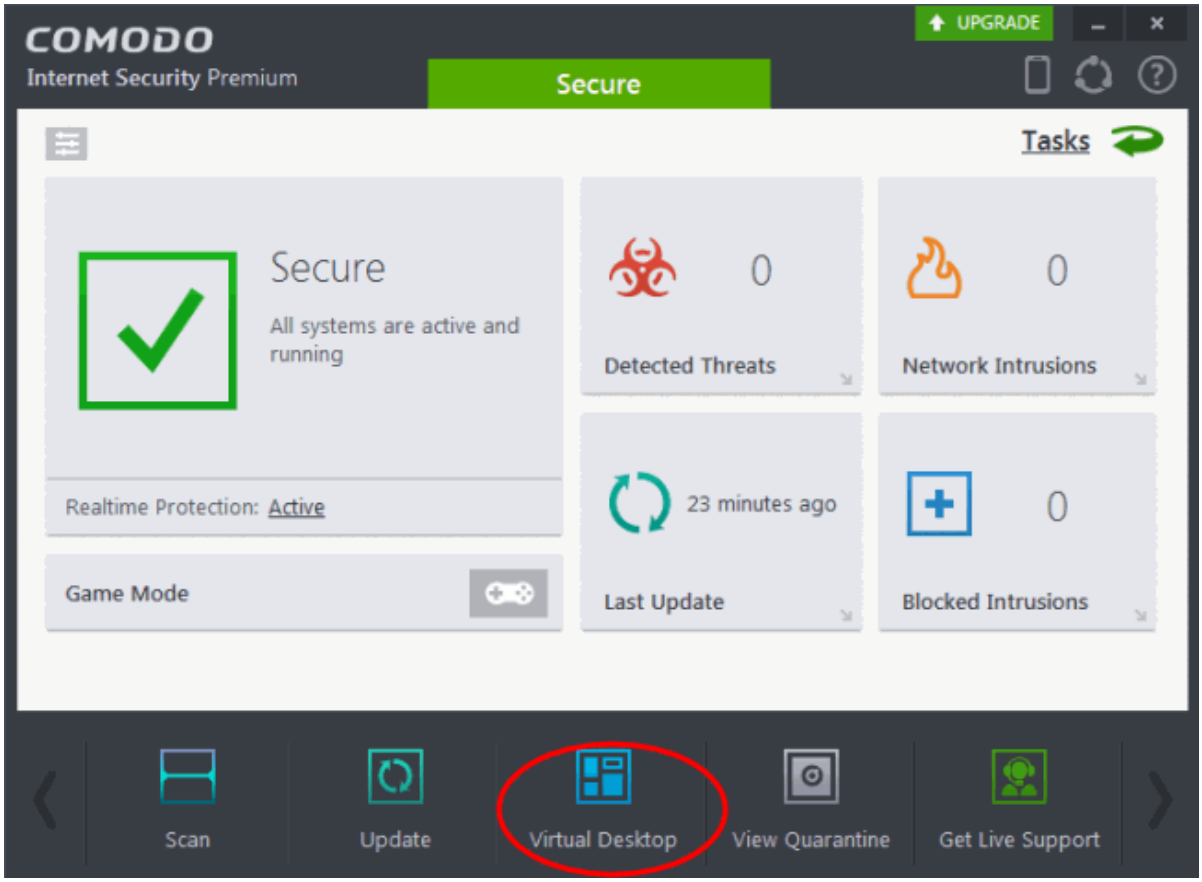
The Virtual Desktop creates a folder Shared Space in the location "C:\Documents and Settings\All Users\Application Data\Shared Space", which can be shared by your host operating system and the Virtual Desktop.

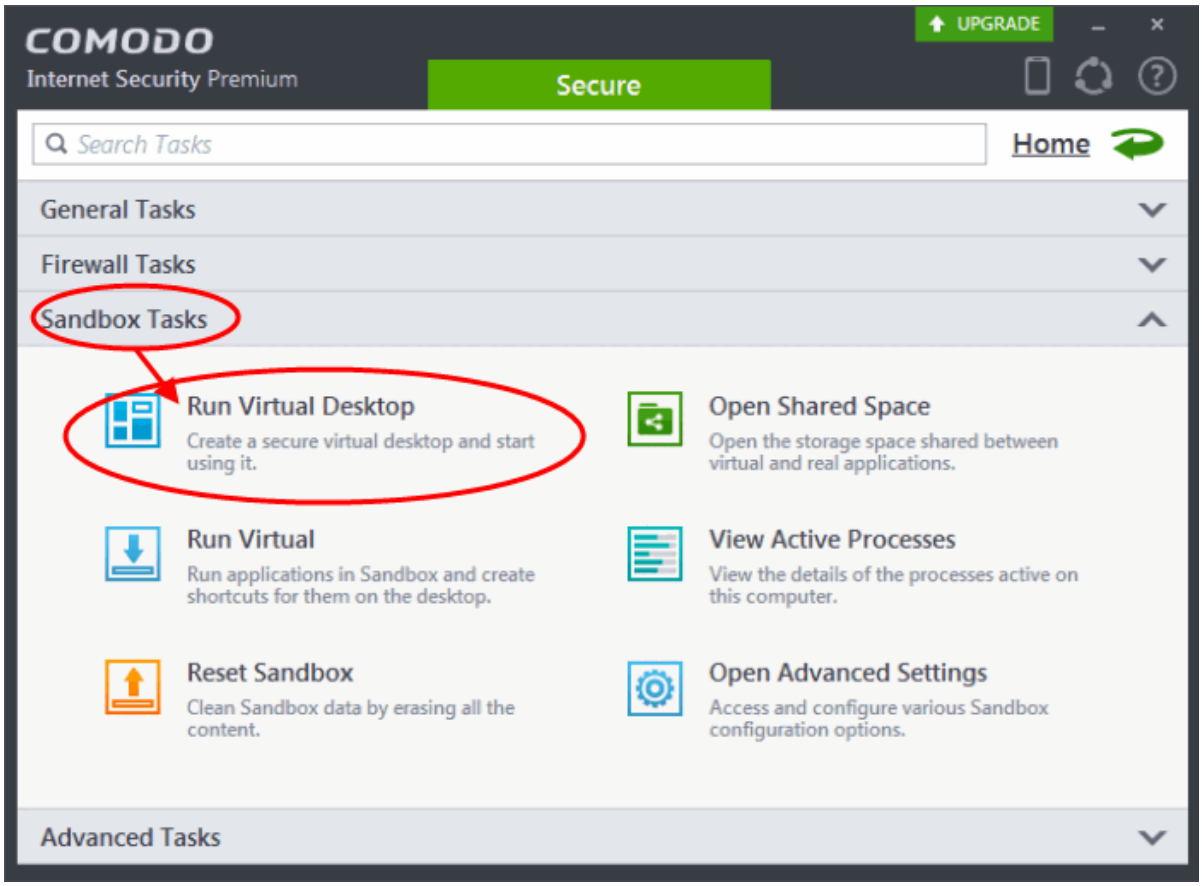
The Shared Space can be accessed in the following ways:

- Click 'Open Shared Space' under 'Sandbox' Tasks in the Tasks Interface
- Click the 'Shared Space' shortcut icon from the home screen of CIS
- Click the 'Shared Space' shortcut icon from the CIS widget
- Click the 'Shared Space' desktop shortcut icon

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

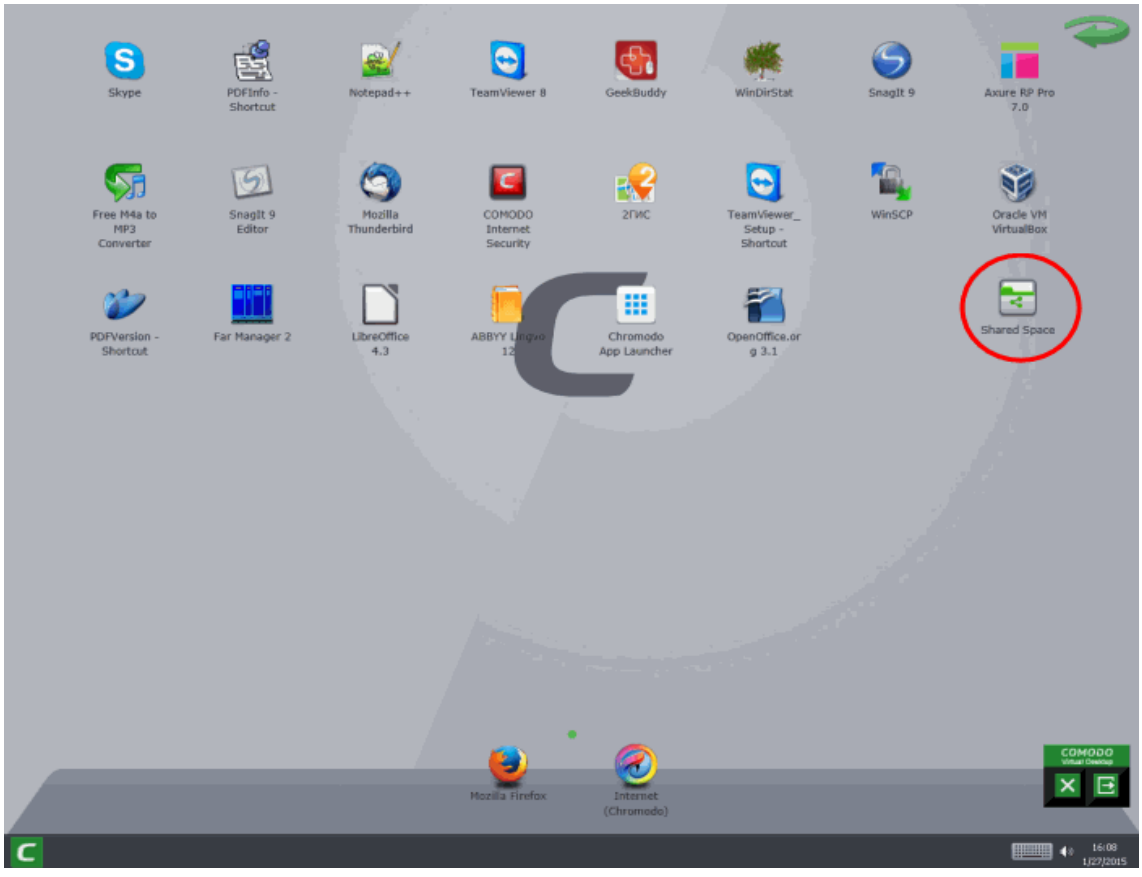
1. Open the 'Shared Space' as mentioned above
2. Copy/Move the application or the file to be opened into the Shared Space
3. Start 'Virtual Desktop' by clicking the Virtual Desktop shortcut in the CIS home screen or by clicking Sandbox Tasks > Run Virtual Desktop from the Tasks interface of CIS.





4. Open Shared Space inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.

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



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

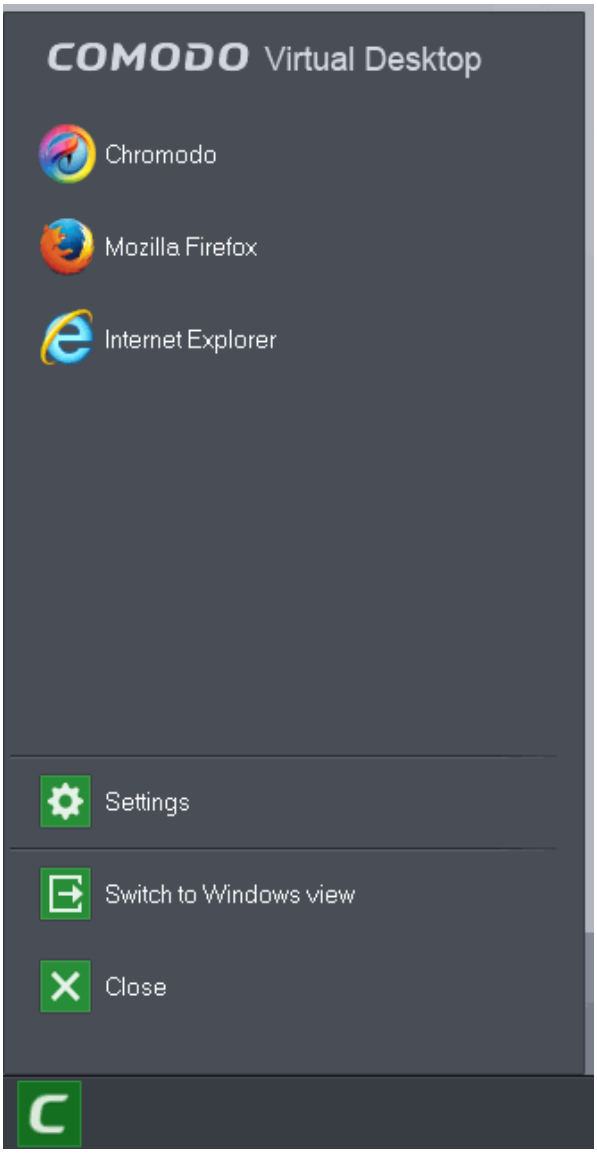
The changes you make to the file will be stored to the file only inside the Virtual Desktop and not in the real computer system.

Run Browsers Inside the Virtual Desktop

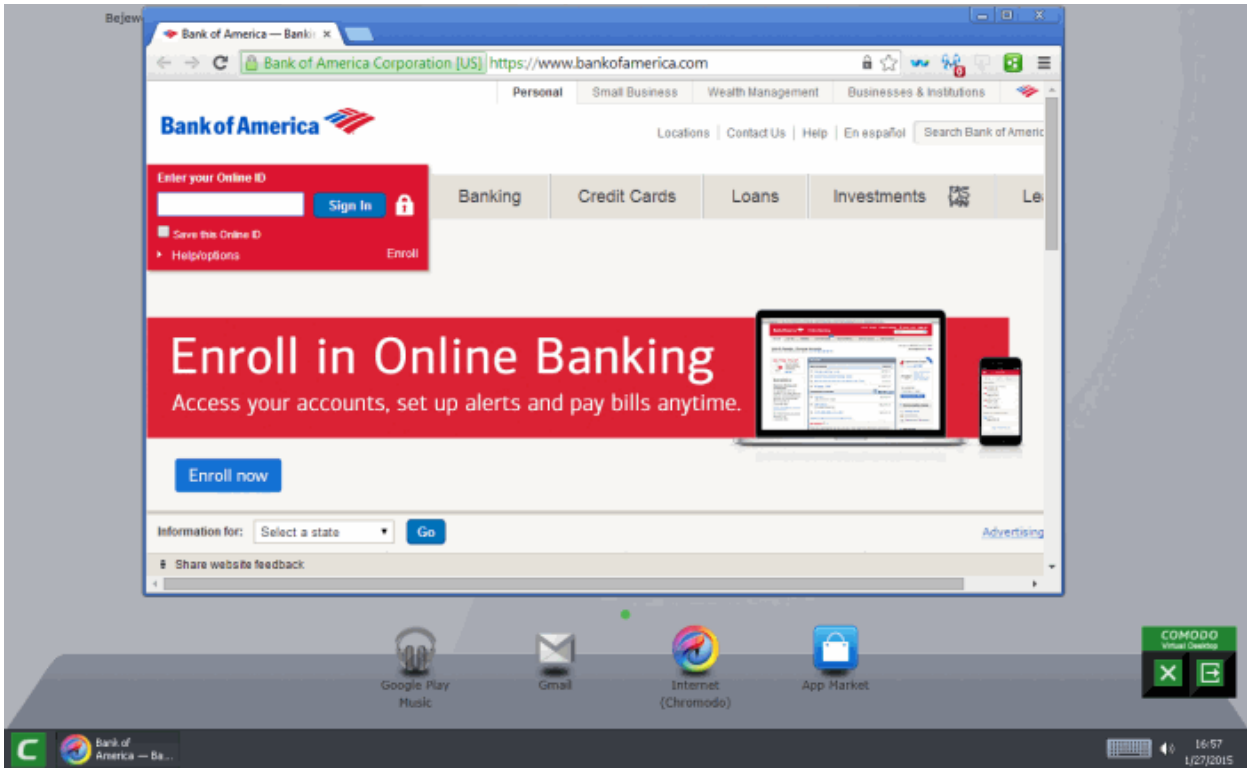
The Virtual Desktop provides an extremely secure environment for Internet related activities because it isolates your browser from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net inside the virtual desktop removes this threat to your machine by preventing any website from installing anything on your real computer. Furthermore, the Virtual Keyboard allows you to securely enter user-names, credit card numbers and passwords without fear of key-logging software recording your physical keystrokes.

To run a browser inside the Virtual Desktop

1. Click the 'C' button
2. Select the browser you want to run from the browsers displayed.



The browser will open inside the Virtual Desktop.



On completion of your browsing session, no trails like your browsing history will be stored in your computer.

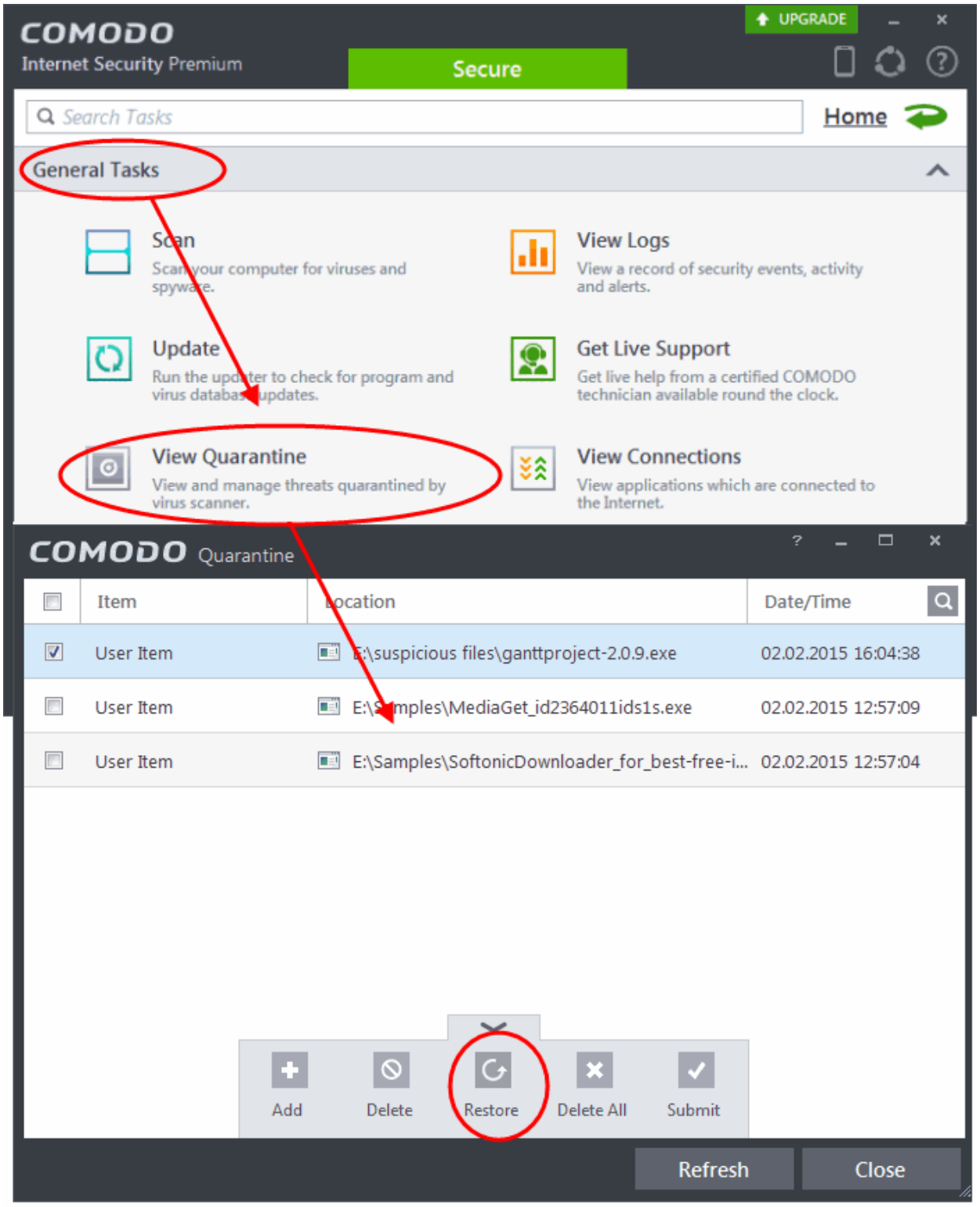
Restore Incorrectly Quarantined Item(s)

If you have incorrectly quarantined item(s) or you feel an item has been incorrectly quarantined by the application (a false positive) then you can restore it/them using the following procedure:

To submit Quarantined items

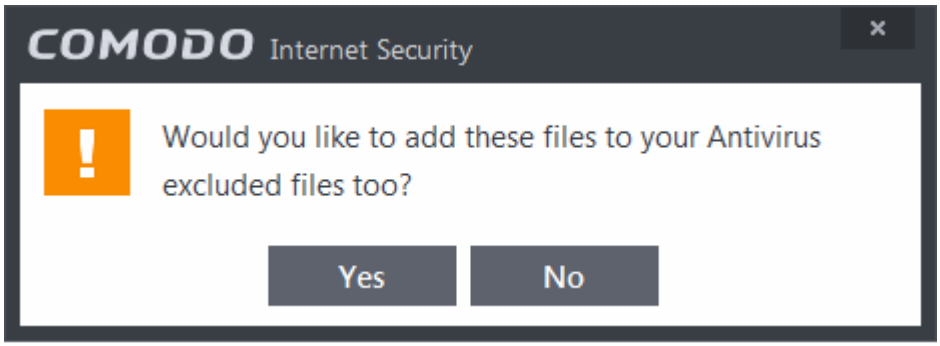
1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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



3. Choose the items to be restored by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Restore'.

An option to add the selected items to AV excluded files will open.



If you select 'Yes', these items will not be included for AV scans. If you select' No', these items will be included for AV scans and quarantined during the next scanning.

All the selected files will be restored to their original locations immediately.

5. Click 'Close' button to exit.

Click here for more details on the Quarantined Items.

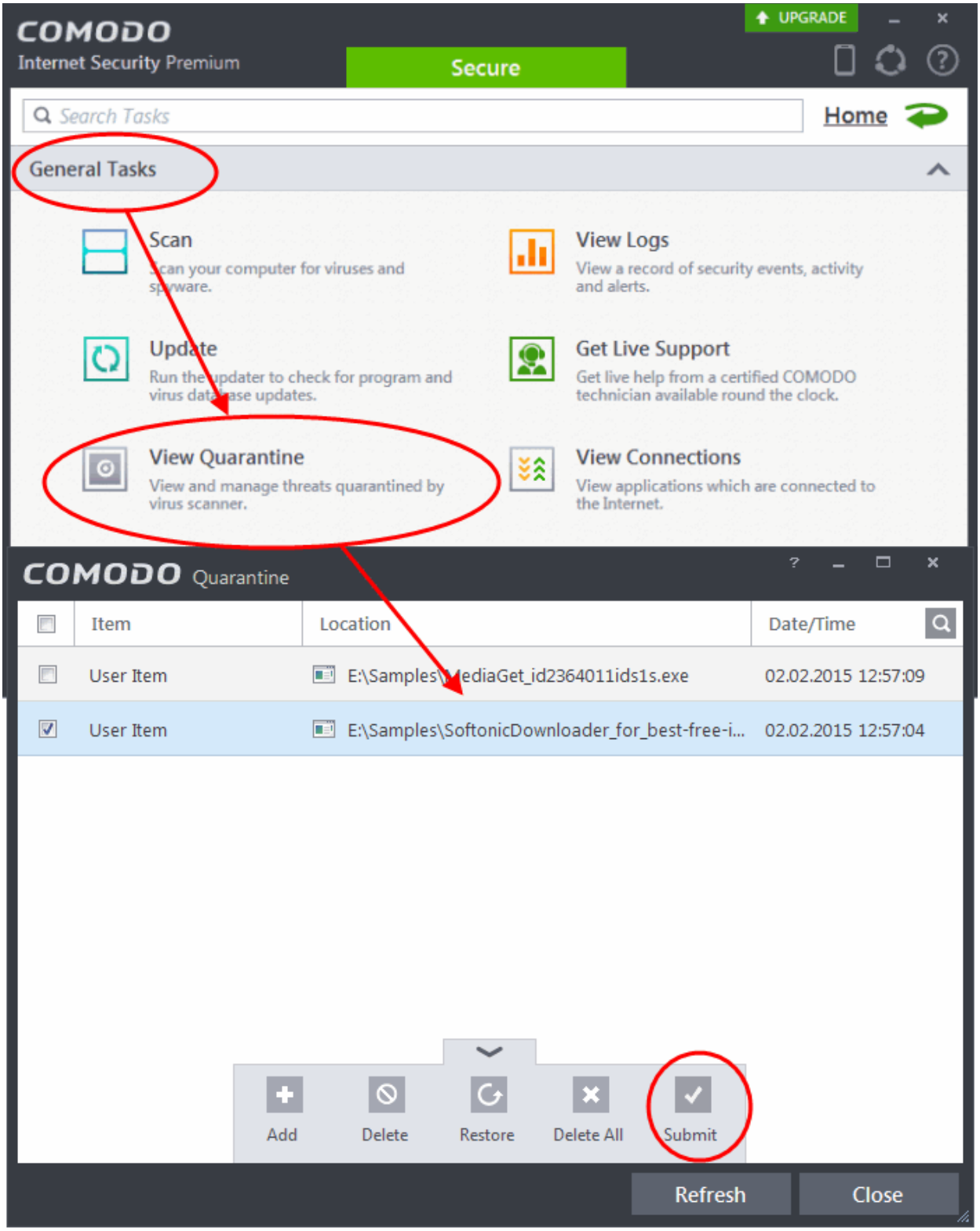
Submit Quarantined Items to Comodo for Analysis

Items which have been quarantined as a result of an On Access, On Demand or Scheduled Scans, can be sent to Comodo for Analysis. After the analysis, if the submitted item is found to be a False Positive, it will be added to Comodo Safe List. Conversely, if it is found to be a malware, it will be added to the anti-malware Black list. This helps Comodo to enhance its virus signature database and helps millions of other CIS users to benefit out of it. **Click here** for more details on Quarantined Items.

To submit Quarantined items

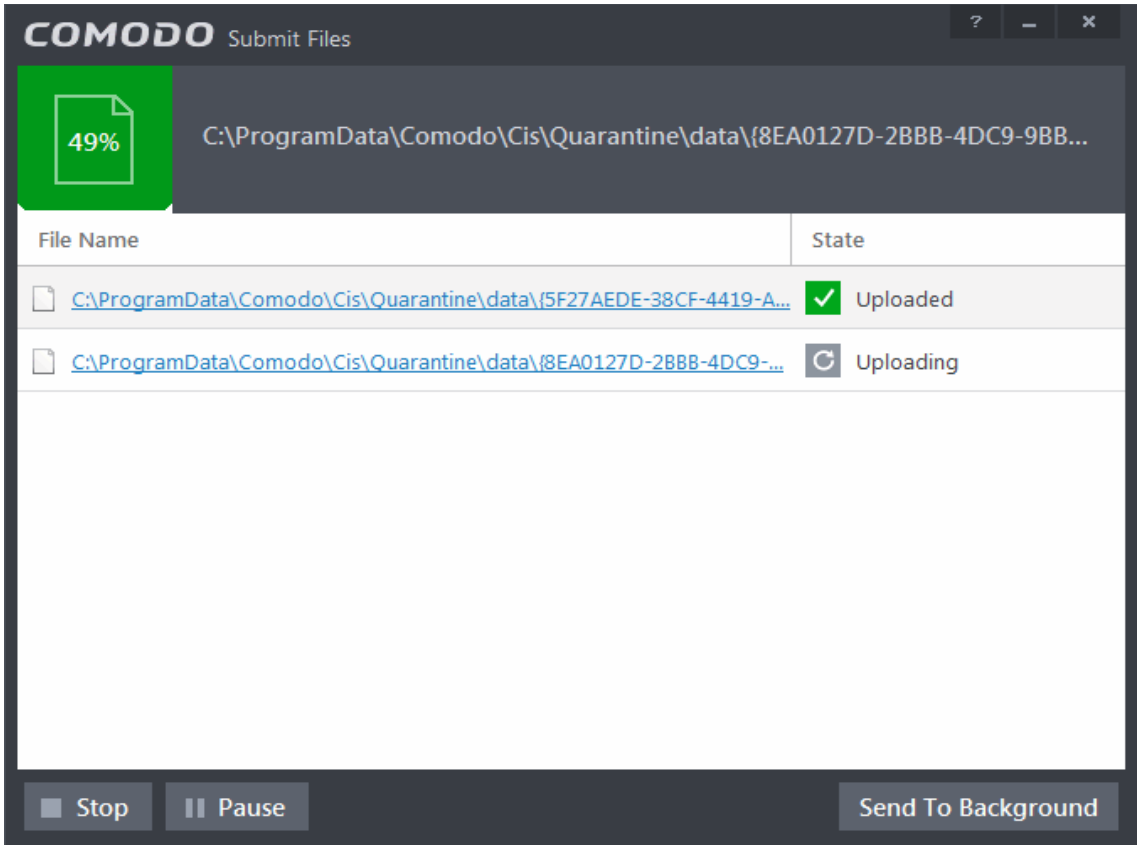
1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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

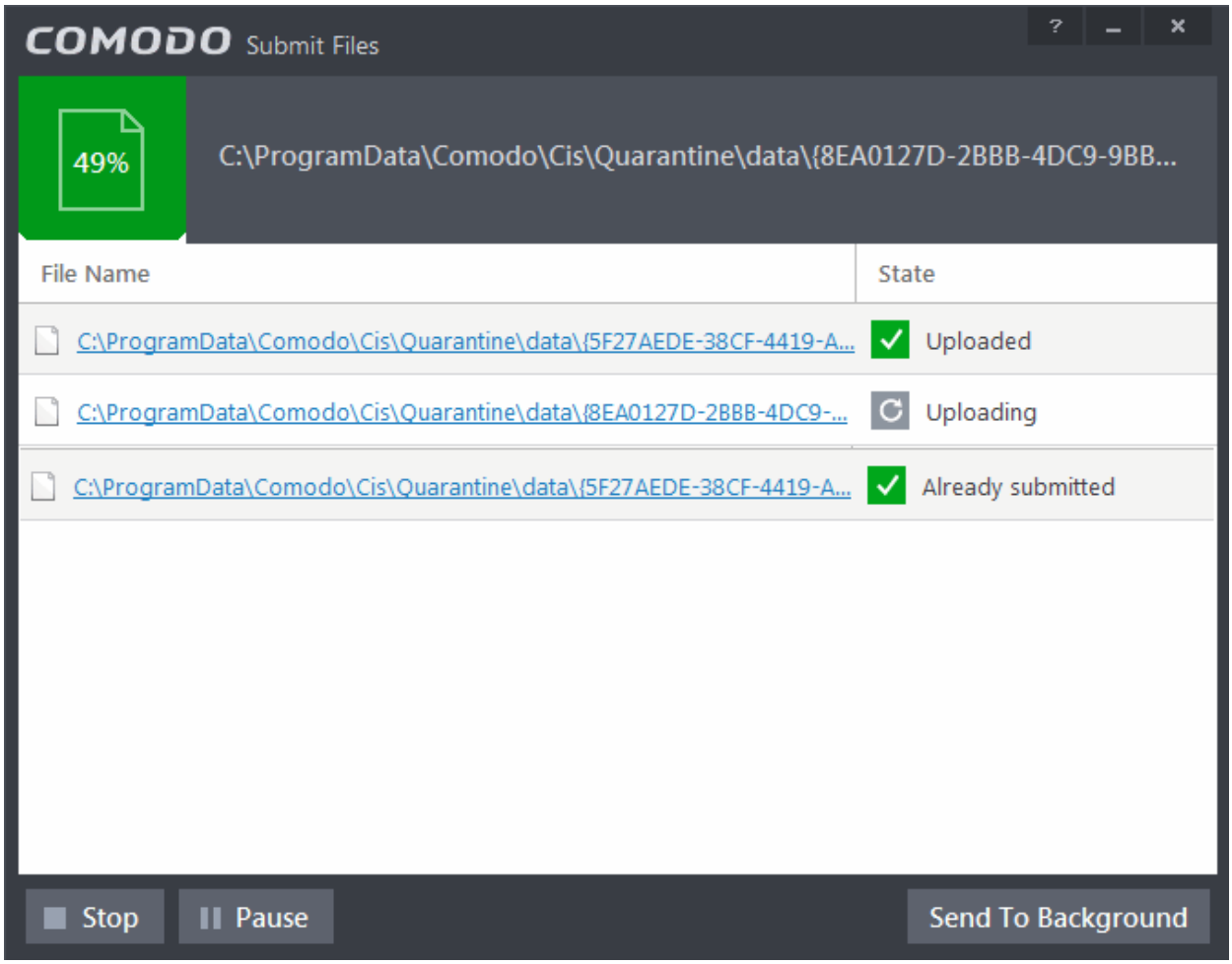


3. Choose the items to be submitted to Comodo for analysis by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Submit'.

The submission progress will be indicated.



On completion, the submission results will be displayed, indicating whether the file is successfully submitted or already submitted by other users and is pending for analysis.



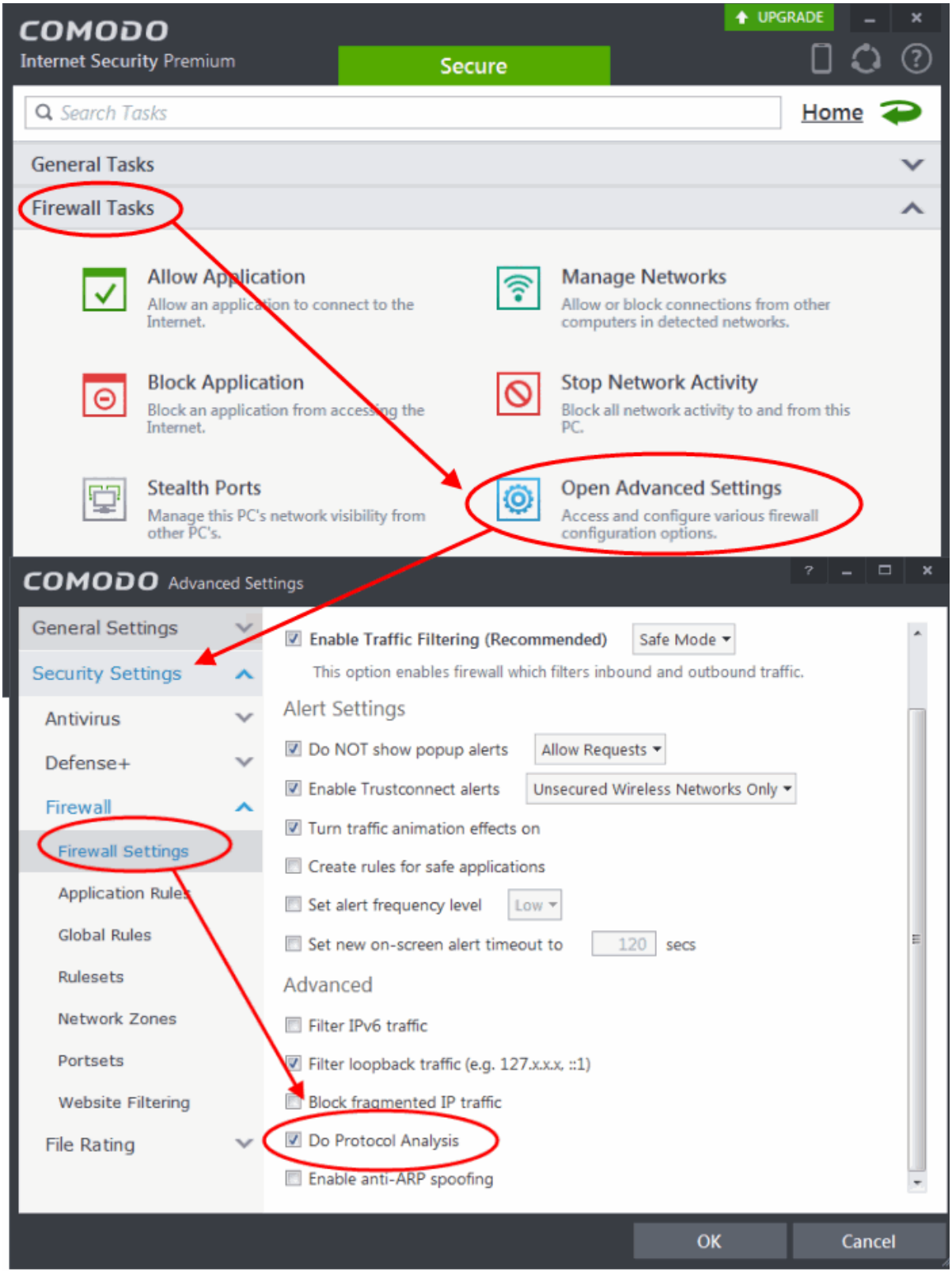
Enable File Sharing Applications like BitTorrent and Emule

This page explains how to configure Comodo Firewall for file sharing applications like Shareaza/Emule and BitTorrent/UTorrent. To allow these file sharing applications, you must:

- **Disable 'Do Protocol analysis'** ***(disabled, by default)***
- **Create a 'Predefined Firewall Ruleset' for Shareaza/Emule**
- **Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent**

To Disable 'Do Protocol analysis'

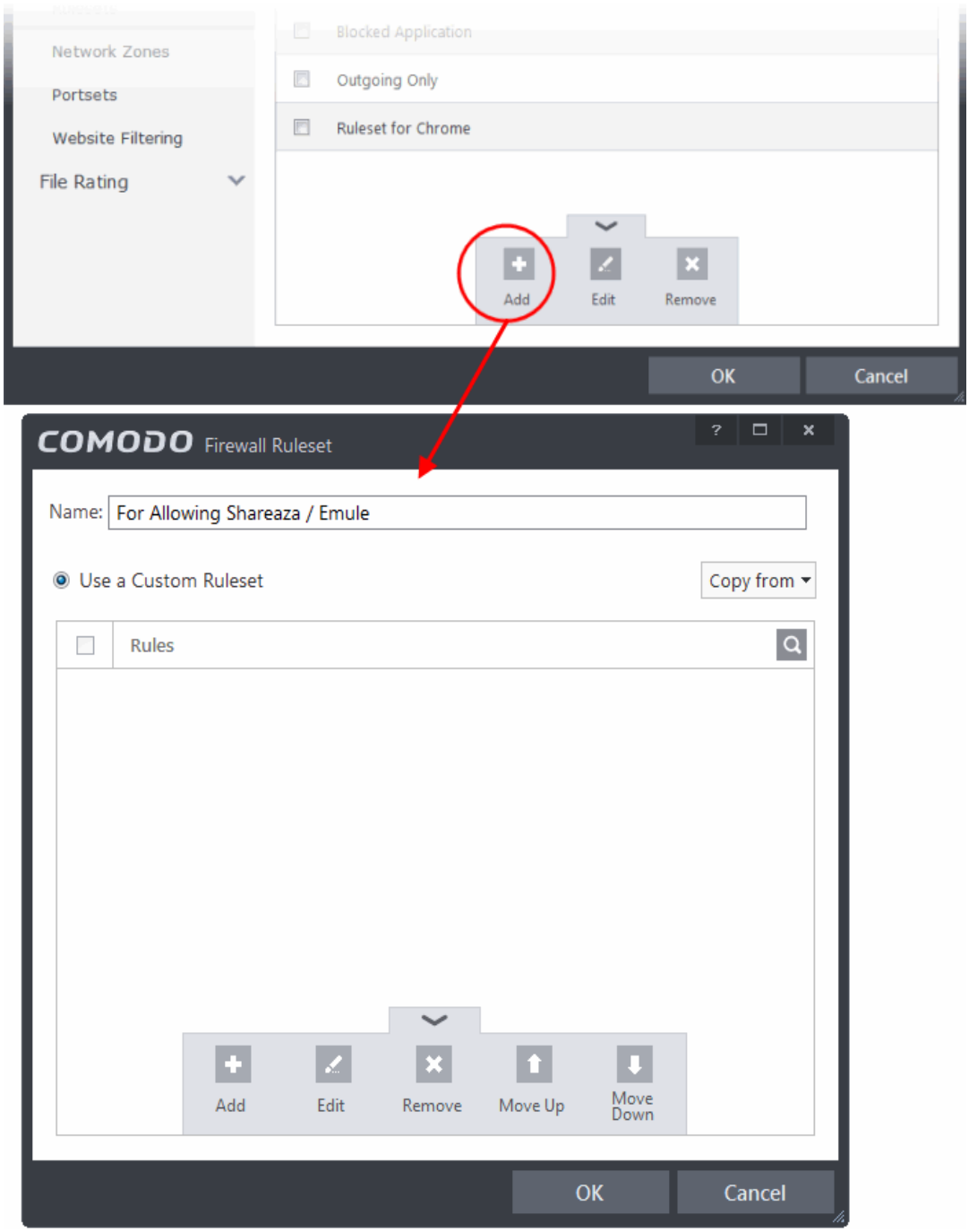
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.



3. Ensure that 'Do Protocol Analysis' checkbox is not selected.

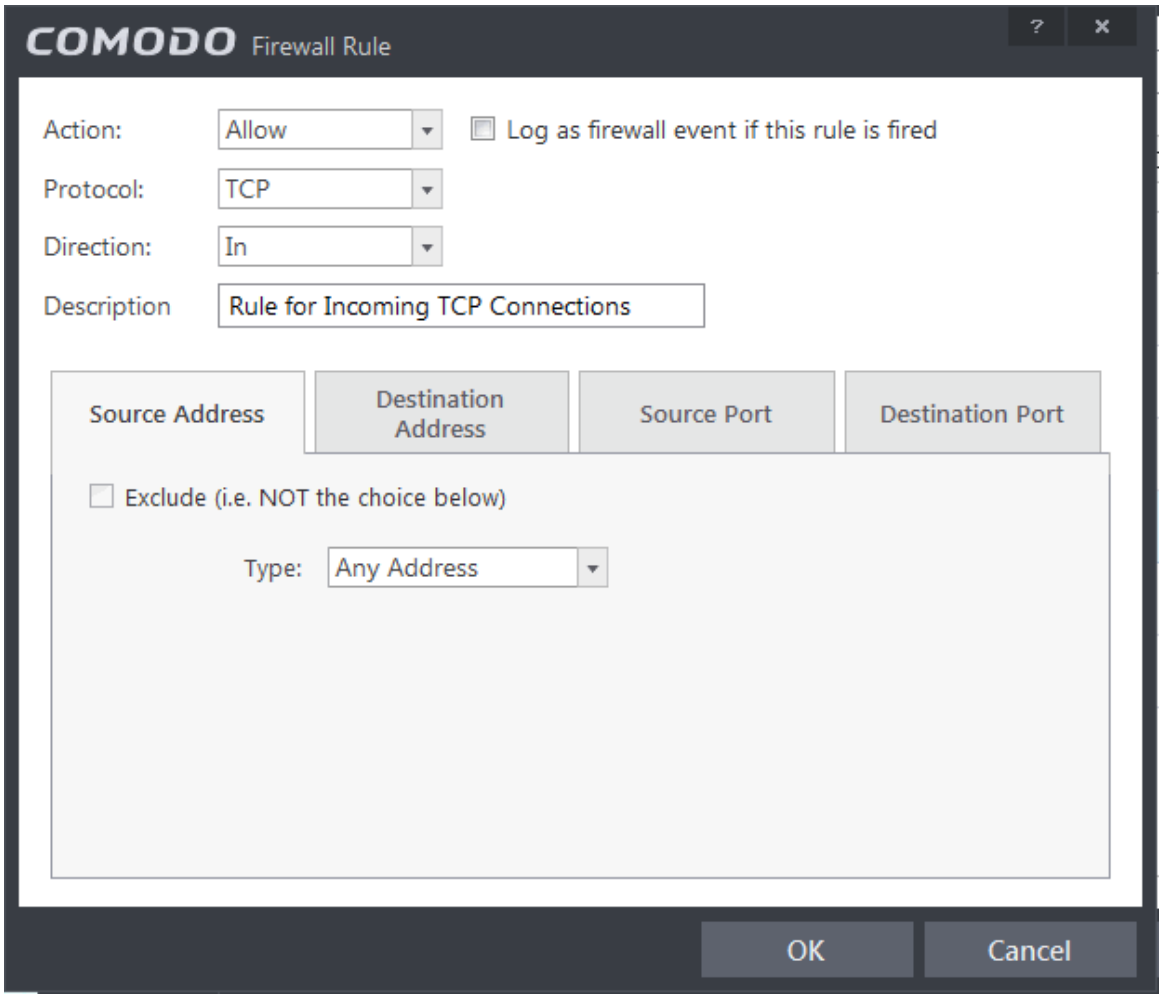
To Create a 'Predefined Firewall Ruleset' for Shareaza/Emule

1. Click 'Rulesets' under 'Firewall' from the LHS navigation pane of 'Advanced Settings' interface to open 'Rulesets' panel
2. Click the handle from the bottom of the panel and choose 'Add'



The 'Firewall Ruleset' interface will open for creating a new set of rules.

3. Click the handle from the bottom and choose 'Add'
4. Enter a descriptive name for the new ruleset to be created in the 'Description' text box (for example: For allowing Shareaza/Emule).
5. Now you need to create six rules for the newly created ruleset. To do so, click 'Add'. The 'Firewall Rule' interface will appear. For creating each rule, select the check box and choose the drop-down options under each tab as given below. After creating each rule, click 'OK' for the rule to be added. Click handle in the 'Firewall Ruleset' interface and choose 'Add' to create the next rule.



Rule 1

- Action : Allow
- Protocol : TCP
- Direction : In
- Description : Rule for incoming TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1025 / End Port = 65535)
- Destination port : A Single Port : (Port : Your TCP port of Shareaza/Emule)

Rule 2

- Action : Allow
- Protocol : UDP
- Direction : In
- Description : Rule for incoming UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1025 / End Port = 65535)
- Destination port : A Single Port : (Port : Your UDP port of Shareaza/Emule)

Rule 3

- Action : Allow
- Protocol : TCP or UDP

- Direction : Out
- Description : Rule for outgoing TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1025 / end port = 65535)
- Destination port : A port range : (start port = 1025 / end port = 65535)

Rule 4

- Action : Allow
- Protocol : ICMP
- Direction : Out
- Description : Ping the server (edk network)
- Source Address : Any Address
- Destination Address : Any Address
- ICMP Details : Message : ICMP Echo Request

Rule 5

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1025 / end port = 65535)
- Destination port : Type : Single Port; (Port : 80)

Rule 6

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.

The new ruleset will be created and added as a Predefined ruleset. Start Shareaza or Emule. When Comodo raises a pop-up alert, choose 'Treat this application as', select the descriptive name you gave for this rule (e.g. For allowing Shareaza/Emule) from the options and select 'Remember my answer'.

To create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Rulesets' under 'Firewall' from the LHS navigation pane of 'Advanced Settings' interface to open 'Rulesets' panel
2. Click the handle from the bottom of the panel and choose 'Add'

The 'Firewall Ruleset' interface will open for creating a new set of rules.

3. Click the handle from the bottom and choose 'Add'
4. Enter a descriptive name for the new ruleset to be created in the 'Description' text box (for example: For allowing BitTorrent/Utorrent).
5. Now you need to create six rules for the newly created ruleset. To do so, click 'Add'. The 'Firewall Rule' interface will appear. For creating each rule, select the check box and choose the drop-down options under each tab as given below. After creating each rule, click 'OK' for the rule to be added. Click handle in the 'Firewall Ruleset' interface and choose 'Add' to create the next rule.

Rule 1

- Action : Allow
- Protocol : TCP or UDP
- Direction : In
- Description : Rule for incoming TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1025 / End port = 65535)
- Destination port : A Single Port (Port: The port of BitTorrent/Utorrent)

Rule 2

- Action : Allow
- Protocol : TCP
- Direction : Out
- Description : Rule for outgoing TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1025 / End port = 65535)
- Destination port : A Port Range : (Start port = 1025 / End port = 65535)

Rule 3

- Action : Allow
- Protocol : UDP
- Direction : Out
- Description : Rule for outgoing UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Single Port: Port: the port of utorrent
- Destination port : A Port Range : (Start port = 1025 / End port = 65535)

Rule 4

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1025 / End port = 65535)
- Destination port ; A Single Port (Port = 80)

Rule 5

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.

The new ruleset will be created and added as a Predefined Firewall ruleset. Start BitTorrent or Utorrent. When Comodo raises a pop-up alert, choose 'Treat this application as', select the descriptive name you gave for this rule (e.g. For allowing

BitTorrent/Utorrent) from the options and select 'Remember my answer'.

Block any Downloads of a Specific File Type

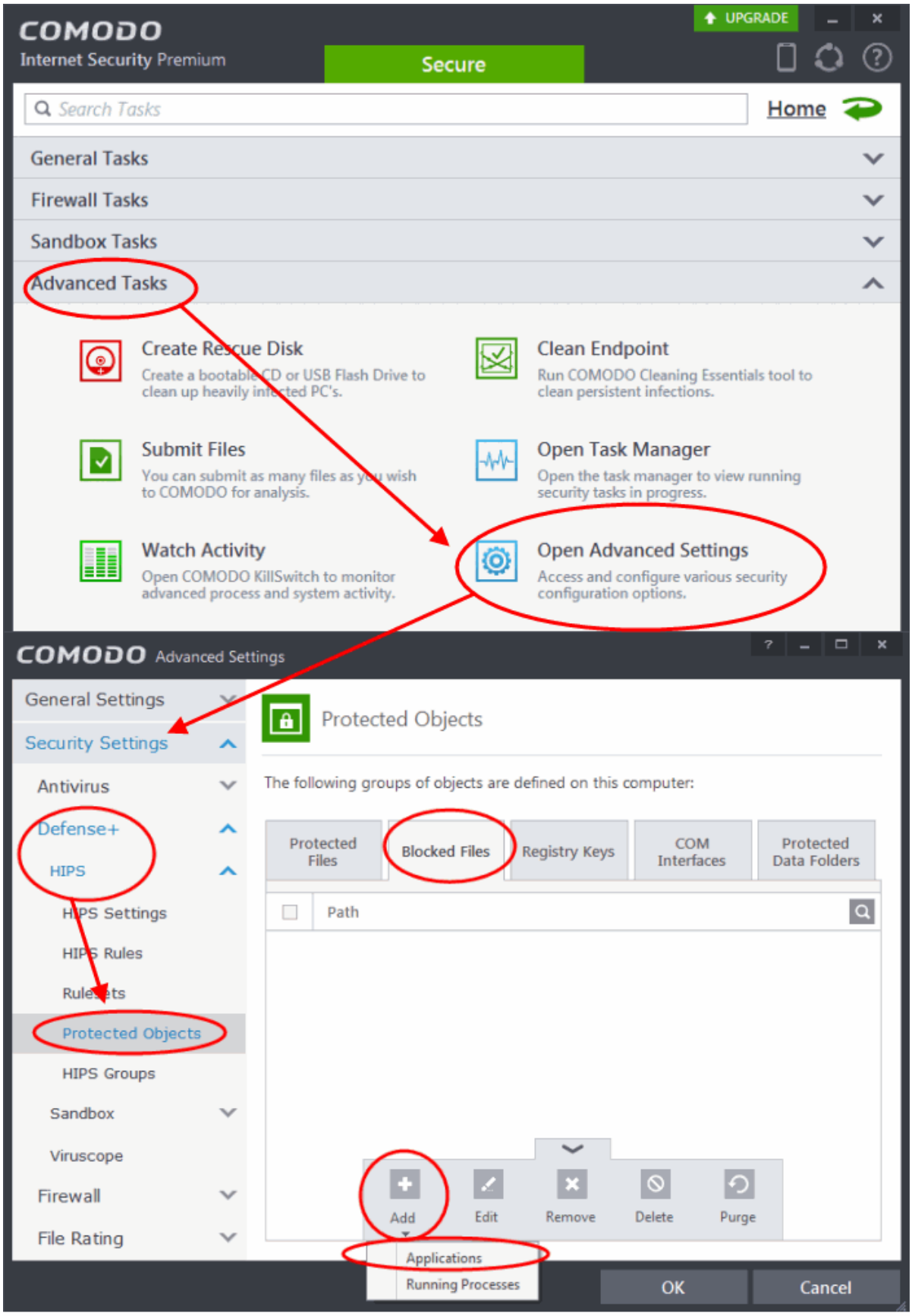
Comodo Internet Security can be configured to block downloads of specific types of file.

Example scenarios:

- Some malicious websites try to push downloads of malware in .exe file format. .exe files are programs which can execute commands on your computer. If the .exe is malicious in intent then these commands could include the installation of key logging programs, initiation of buffer overflow attacks or code to turn your PC into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You want to avoid downloading media files like audio files (e.g. files with extensions .wma, .mp3, .wav, .midi), video files (e.g. files with extensions .wmv, .avi, .mpeg, .swf) or image files (e.g. files with extensions .bmp. .jpg, .png) for your disk space restrictions.

To selectively block downloading of specific file type, you need to configure Defense+ component of CIS to block the specific file type from the default download folder of your browser.

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'HIPS' > 'Protected Objects' from the left hand side pane
4. Click 'Blocked Files' tab

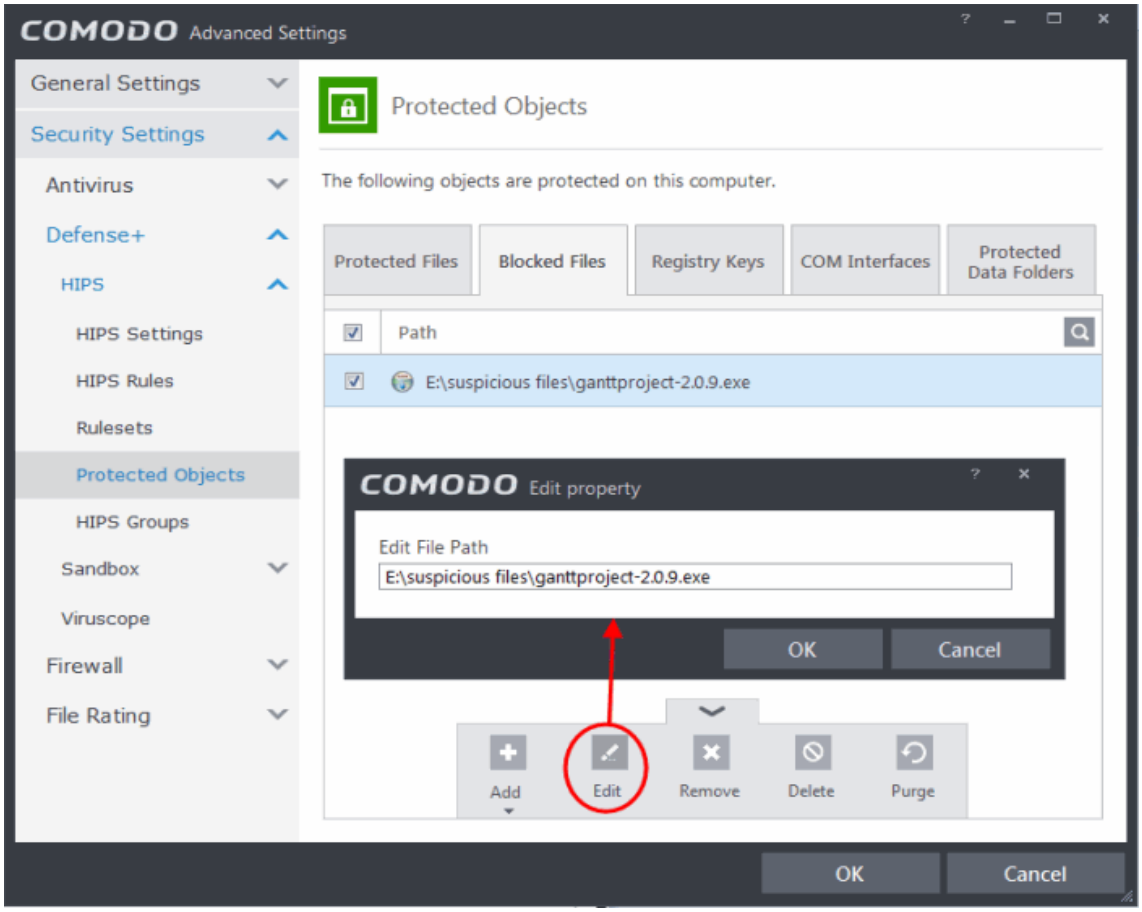


5. Click the handle from the bottom and choose 'Add' > 'Applications'.
6. Browse to the default download folder for that particular file type of your Internet Browser from the Open dialog

- For example, the default download locations for some file types in Internet Explorer are given below:
  - Executable files - C:\Documents and Settings\user name\Local Settings\Temporary Internet Files\
  - Document files - C:\Documents and Settings\user name\My Documents\
  - Image files - C:\Documents and Settings\user name\My Documents\My Pictures\
  - Music files - C:\Documents and Settings\user name\My Documents\My Music\
  - Video files - C:\Documents and Settings\user name\My Documents\My Videos\

7. Select file from the folder and click 'Open'

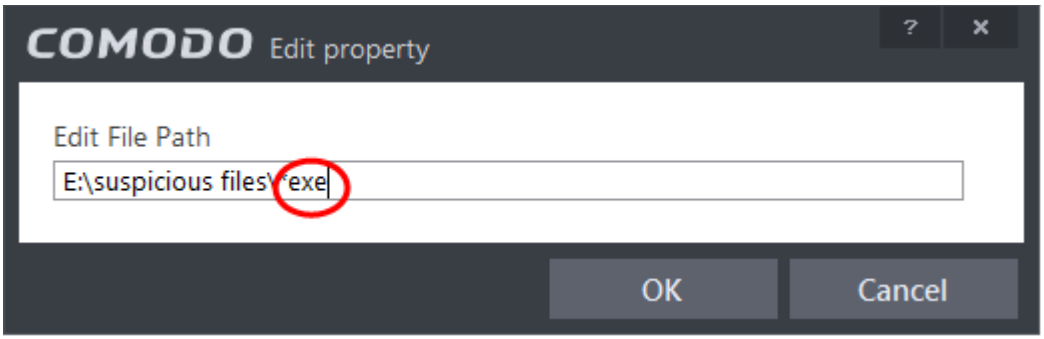
The file will be added to blocked files list.



8. Select the entry from the Blocked Files interface, click the handle from the bottom and choose Edit

The Edit Property dialog will appear.

9. Change the file name at the end of the file path to *.file_extension" (e.g. *.exe, *.jpg)



10. Click OK in the 'Edit Property' dialog
11. Click OK in the Advanced Settings interface to save your settings

The download of the specific file type to the specified folder through the browser will be blocked. If you have more than one browser, repeat the same for the other browsers too.

Note: Blocking files in this way will only block the downloads of the specific file types in the specified folders. If you change the download destination while downloading a file through your web browser, the download will be allowed.

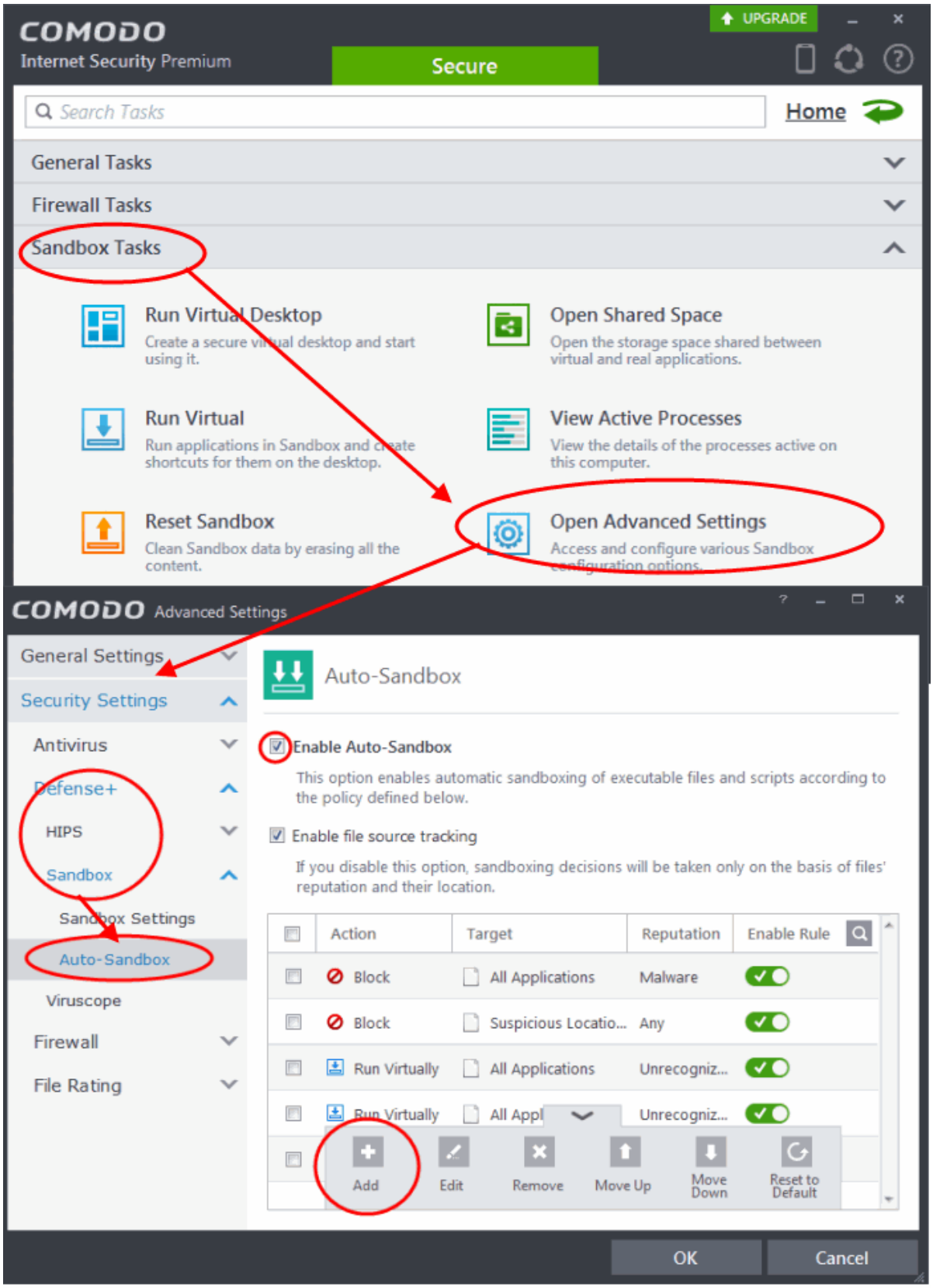
Tip: To unblock the download, Advanced Settings > Defense+ > HIPS > File Protection > Blocked Files, select the file path, click the handle from the bottom and choose 'Remove'.

Disable Auto-Sandboxing on a Per-application Basis

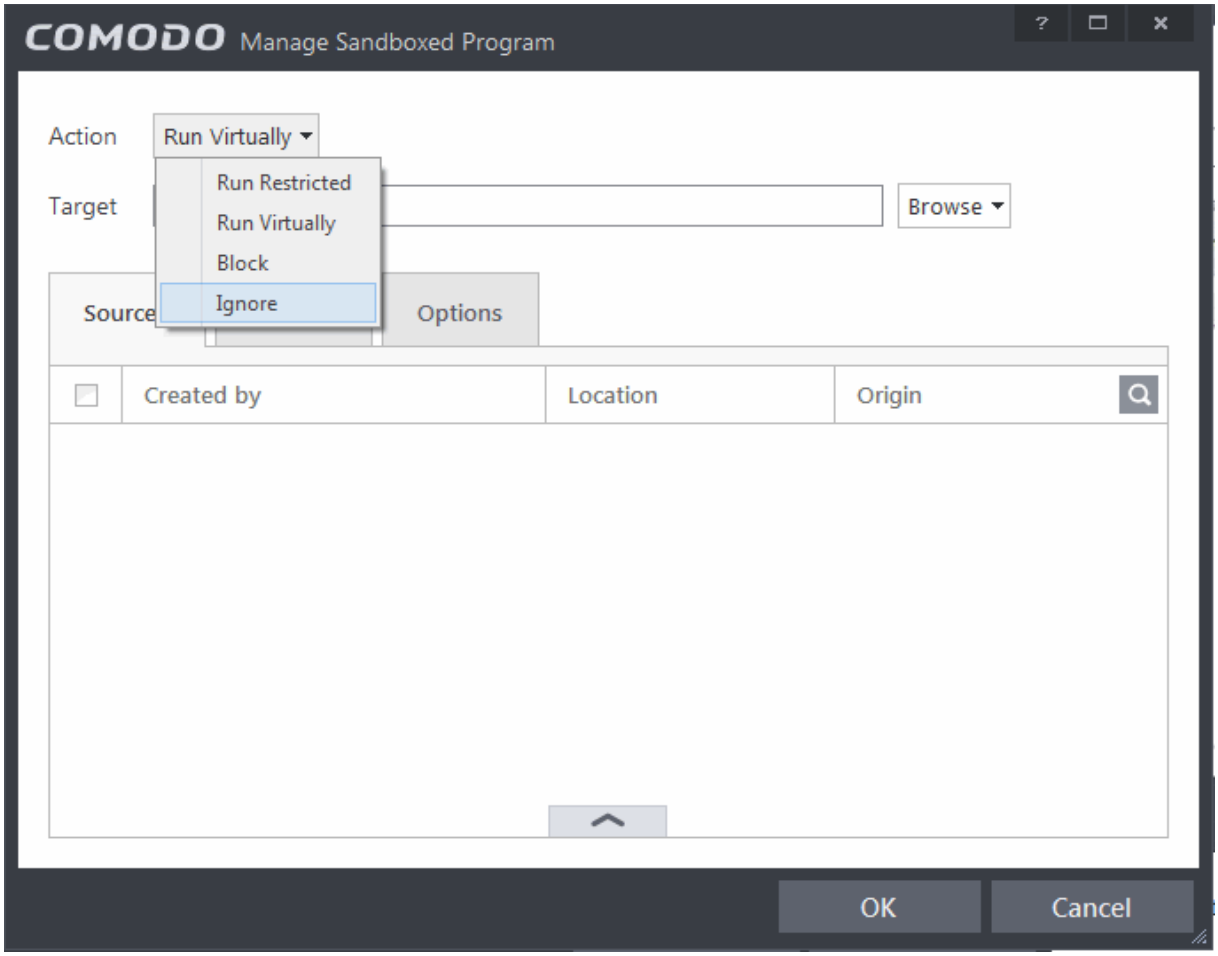
The default auto-sandbox rules will run unknown executables in sandboxed environment and queue them for submission to Comodo Cloud scanners for behavior analysis. Users do, however, have the option to exclude specific files or file types from this auto-sandboxing process by creating a rule. This is particularly useful for developers that are creating new applications which, by their nature, are as yet unknown to the Comodo safe list.

To disable the auto-sandboxing selectively

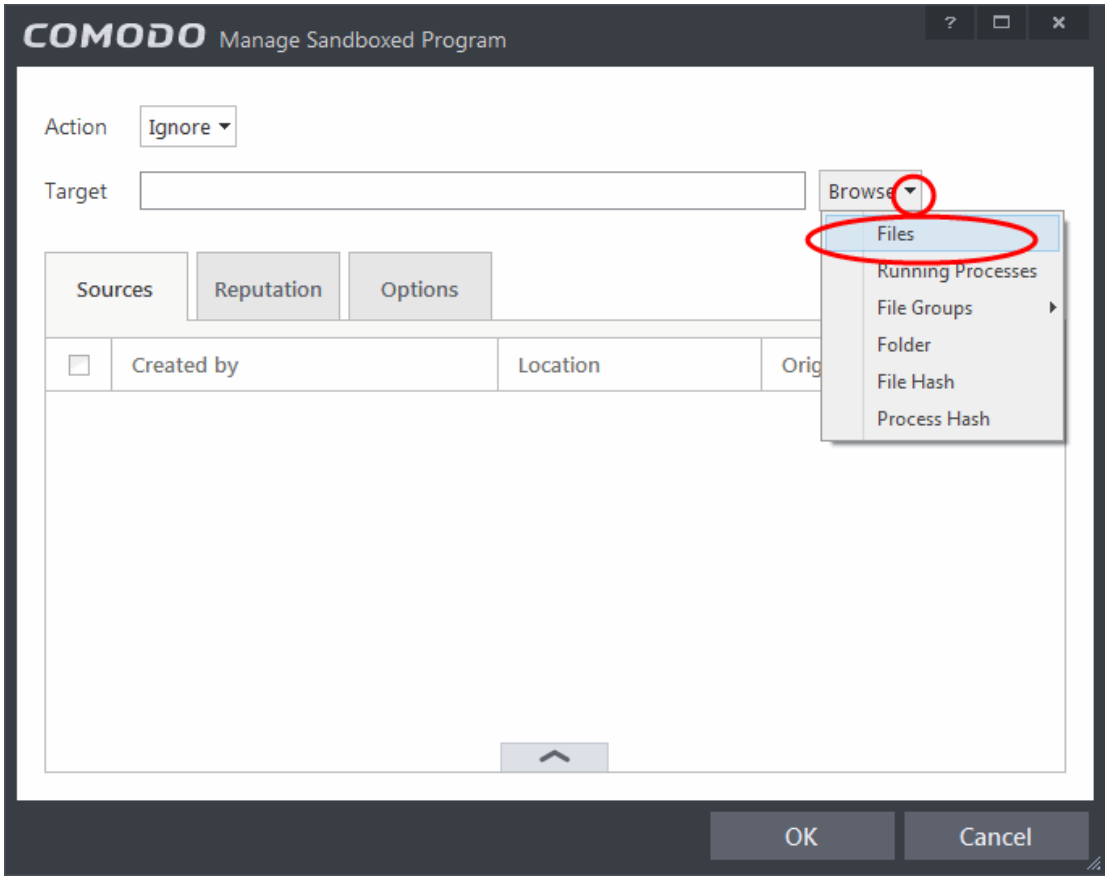
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Sandbox Tasks' and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'Sandbox' > 'Auto-Sandbox' from the left hand side pane
4. Click the handle at the bottom of the interface and open the option panel



5. Click the 'Add' button
6. In the Manage Sandboxed Program interface, select 'Ignore' from the 'Action' drop-down options:

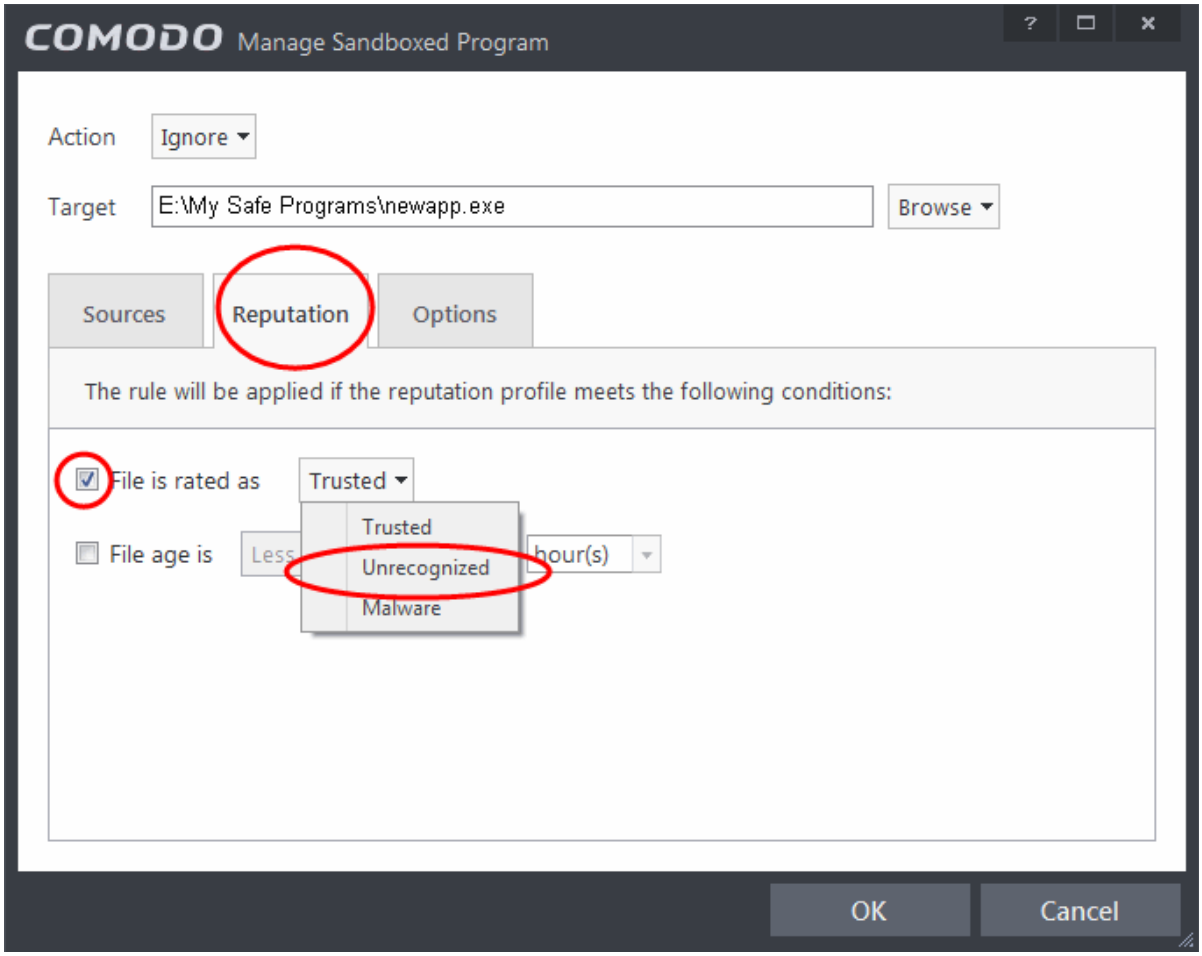


7. By default the Source tab will be selected. Click the Browse button beside the Target field then click Files from the options.

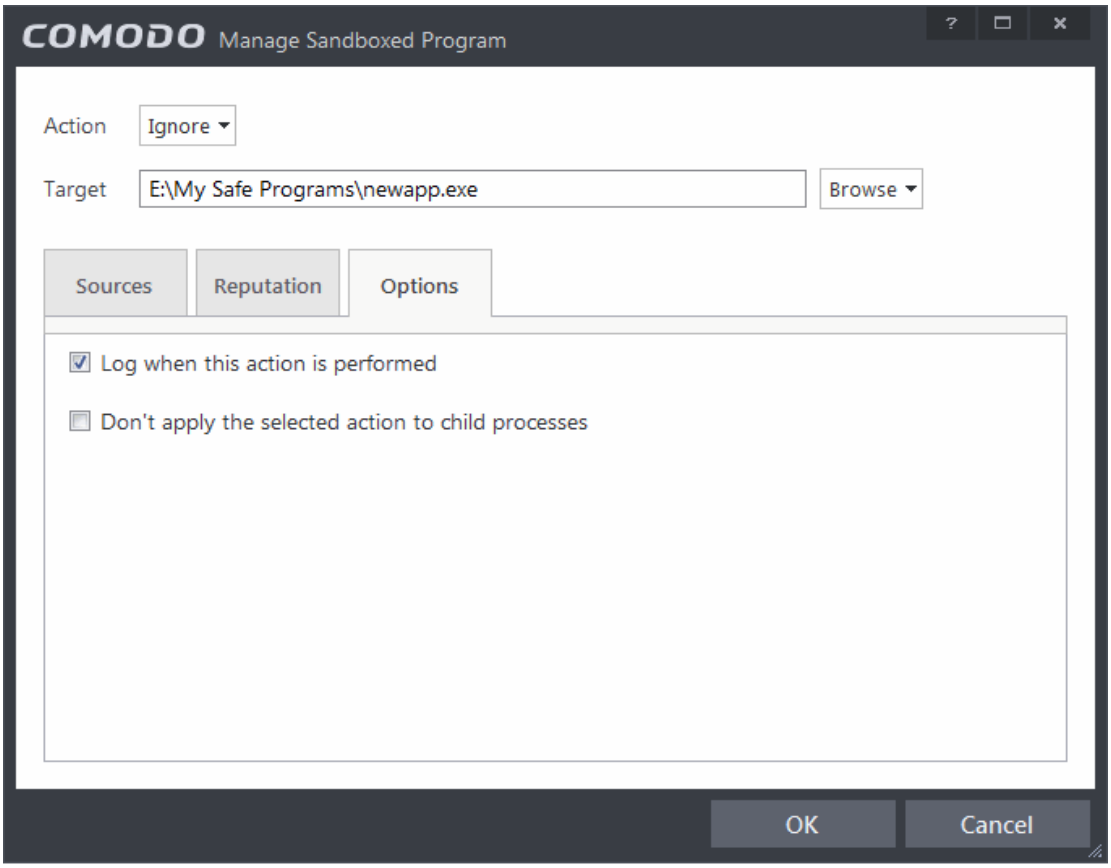


8. Navigate to the location where is the application is installed or stored, select it and click 'Open'. Click here for details about adding to target from other options.

9. Click the Reputation tab, select the checkbox beside 'Select file rating' and click 'Unrecognized' from the drop-down options.



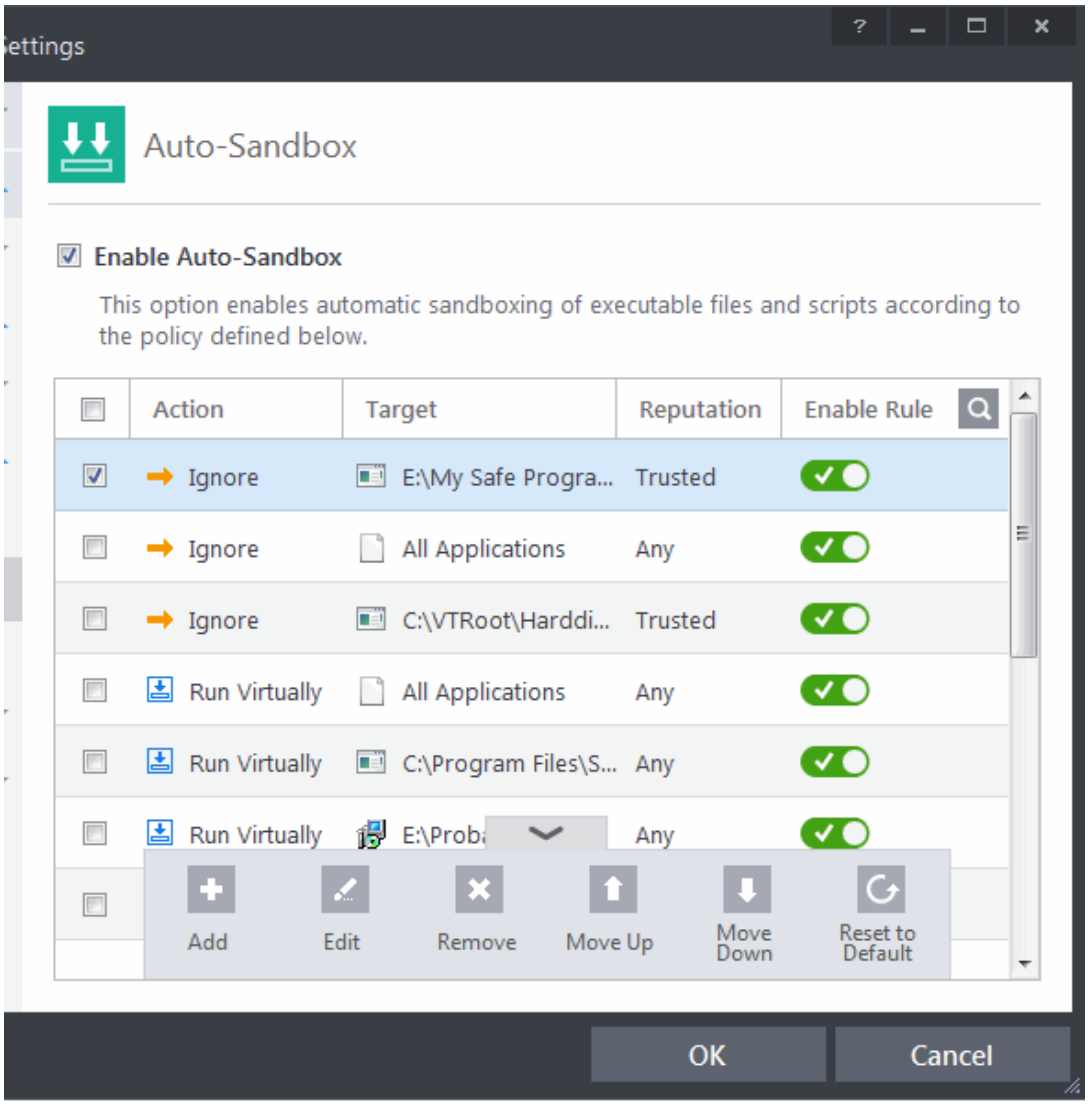
10. Click the Options tab.



By default, 'Log when this action is performed' will be selected.

- **Log when this action is performed** - Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** - Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CIS treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
  - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
  - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox rules individually applied as per their file rating.

11. Select the options as required and click 'OK'.



The Ignore rule will be saved for the specified application and displayed in the Auto-Sandbox screen. Make sure to keep this rule above all other rules for unrecognized files.

Alternatively…

1. Assign Trusted rating to the file from the **File List** interface
2. Digitally sign your files with a code signing certificate from a trusted CA then manually add your organization to the **Trusted Software Vendors** list
3. Disable Behavior Blocker by de-selecting the 'Enable Auto-Sandbox unknown applications as' check box in the Behavior Blocker settings panel. *Not recommended*.

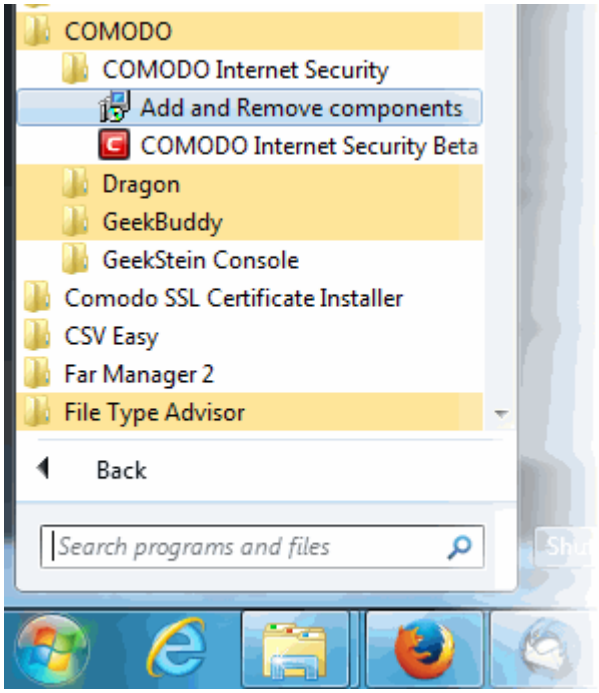
For more details on Auto-Sandboxing process, refer to the section **Unknown Files: The Auto-Sandboxing and Scanning Processes**.

Switch Between Complete CIS Suite and Individual Components (just AV or FW)

Comodo Internet Security provides the flexibility of installation as a complete security suite or as individual components. You can choose the installation type **during the installation** itself. Even after the installation, you can switch the installation type without the requirement of uninstallation of the software, retaining your configuration settings. You might have installed the CIS as complete suite initially but may want to retain the AV part or FW part and uninstall the other or vice -versa. The inbuilt uninstaller of CIS enables to switch your installation type at any point of time.

To switch the installation type

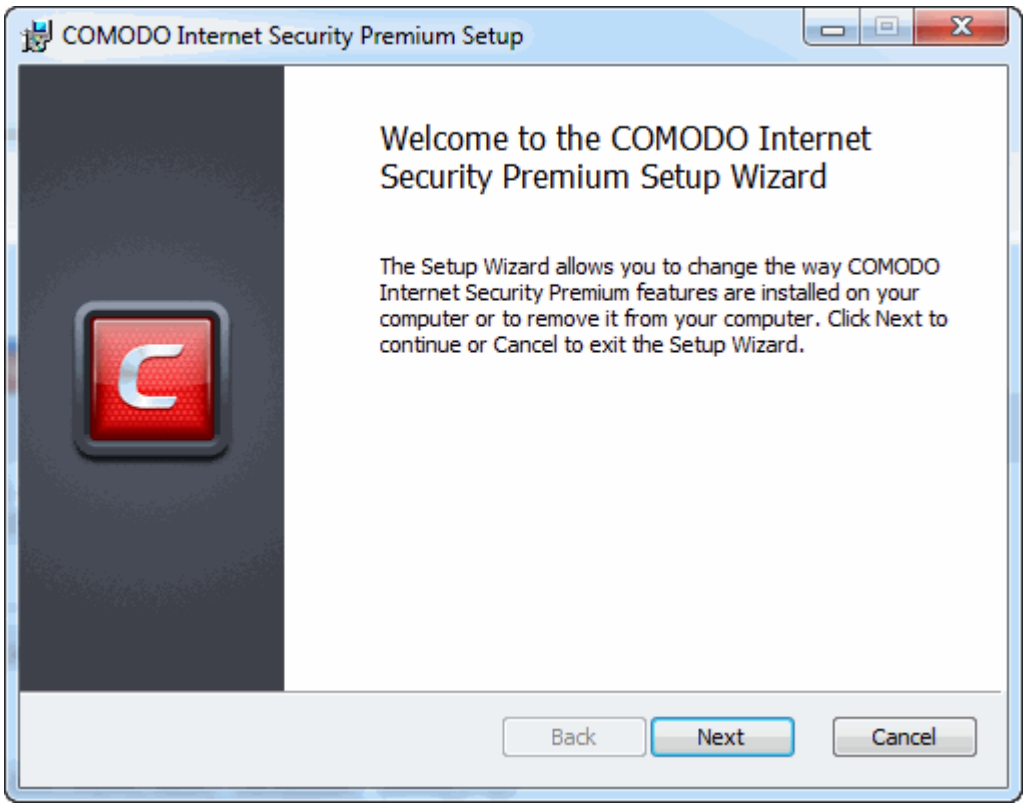
1. Click Start > All Programs > COMODO > COMODO Internet Security > Add and Remove Components



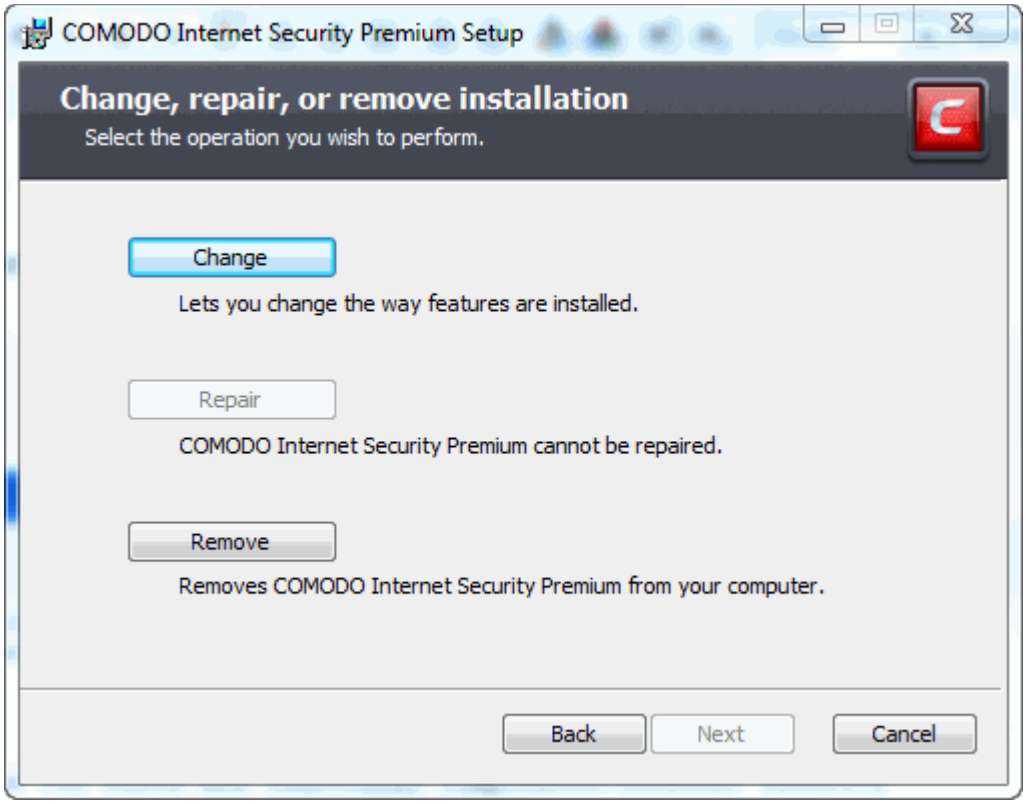
or

Click Start > Control Panel > Control Panel > Comodo Internet Security > Change.

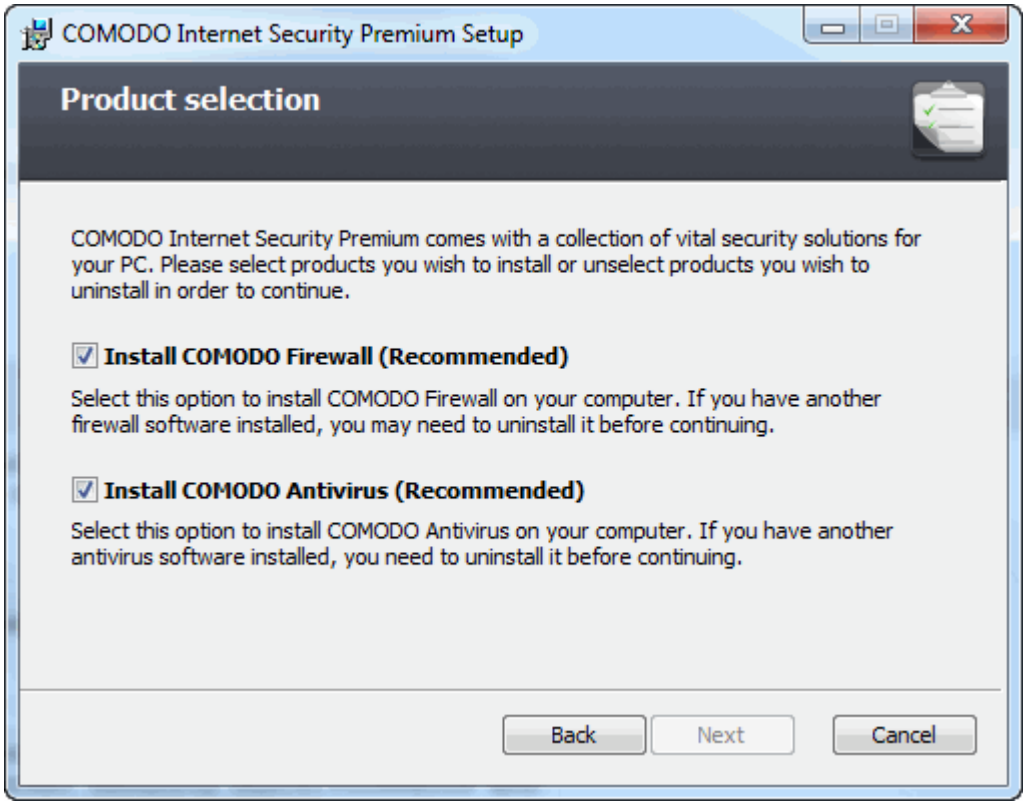
The Configuration Wizard will start.



2. Click 'Next'. The configuration selection screen will appear.



3. Select 'Change' button to change the installed features and click 'Next.' The Product Selection screen will appear.



Select the installation type.

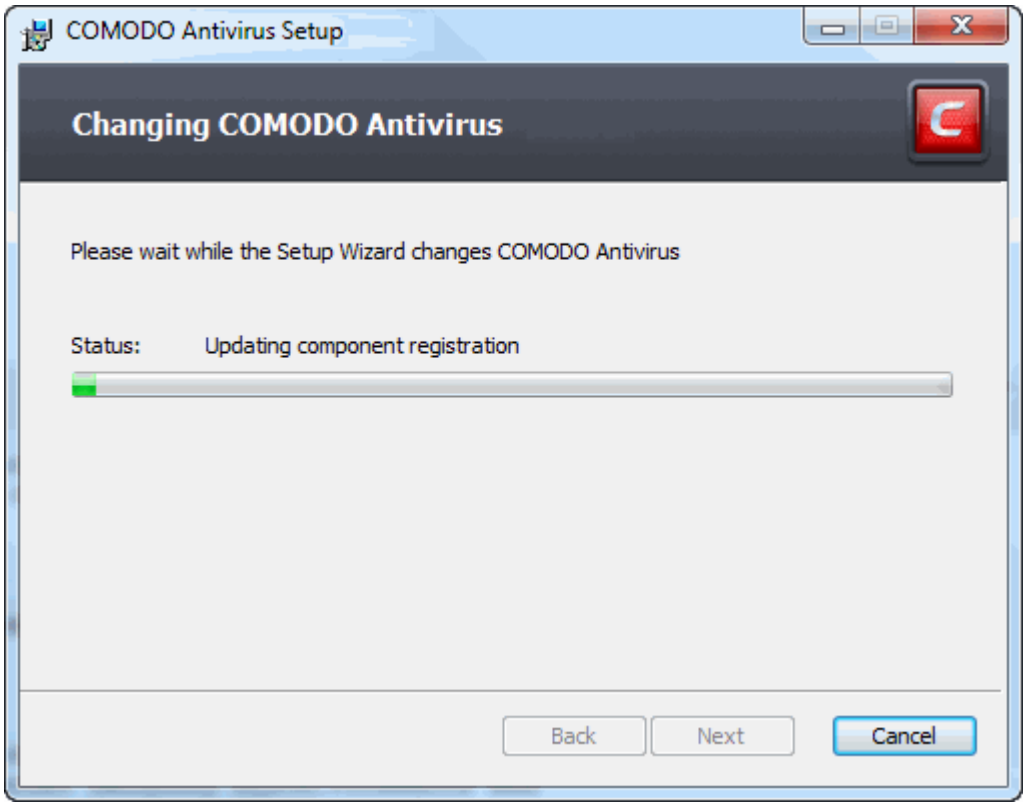
- If you want the complete installation, select both Install COMODO Antivirus and Install COMODO Firewall.
- If you want only the Antivirus part and not the Firewall part, select only the Install COMODO Antivirus and uncheck Install COMODO Firewall.
- If you want only the Firewall part and not the Antivirus part, select only the Install COMODO Firewall and

uncheck Install COMODO Antivirus.

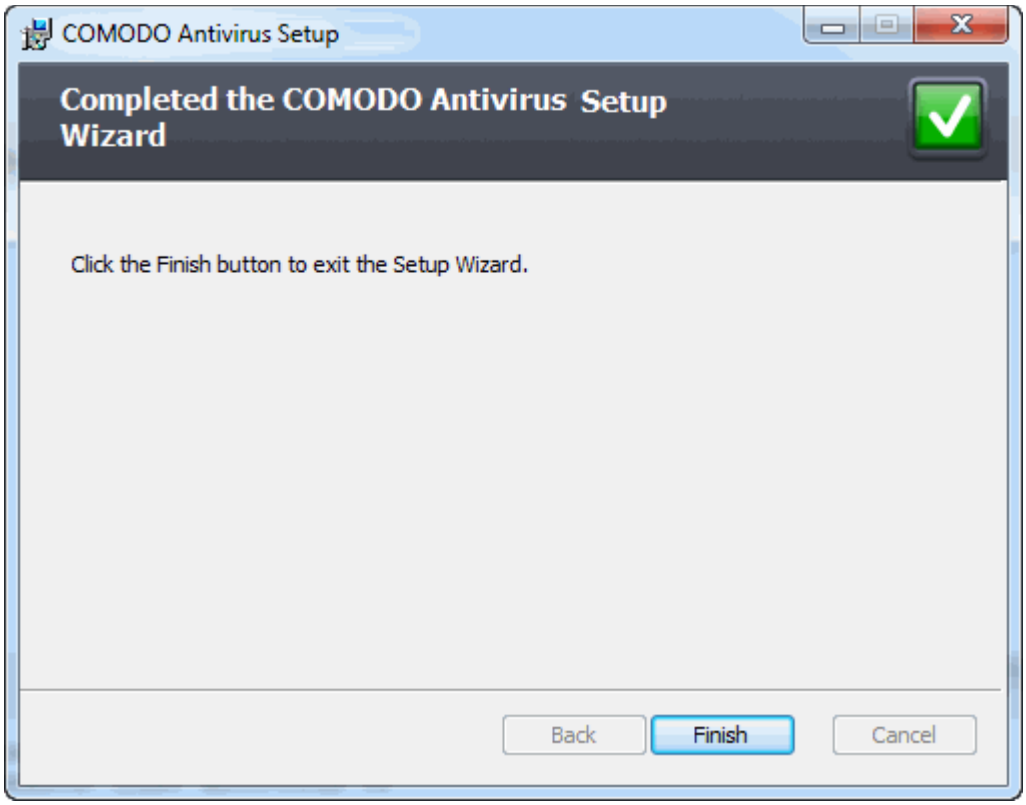
Click here for more details on the installation of individual components.

- Click 'Next'. Wait till the CIS is configured and is ready for the change.

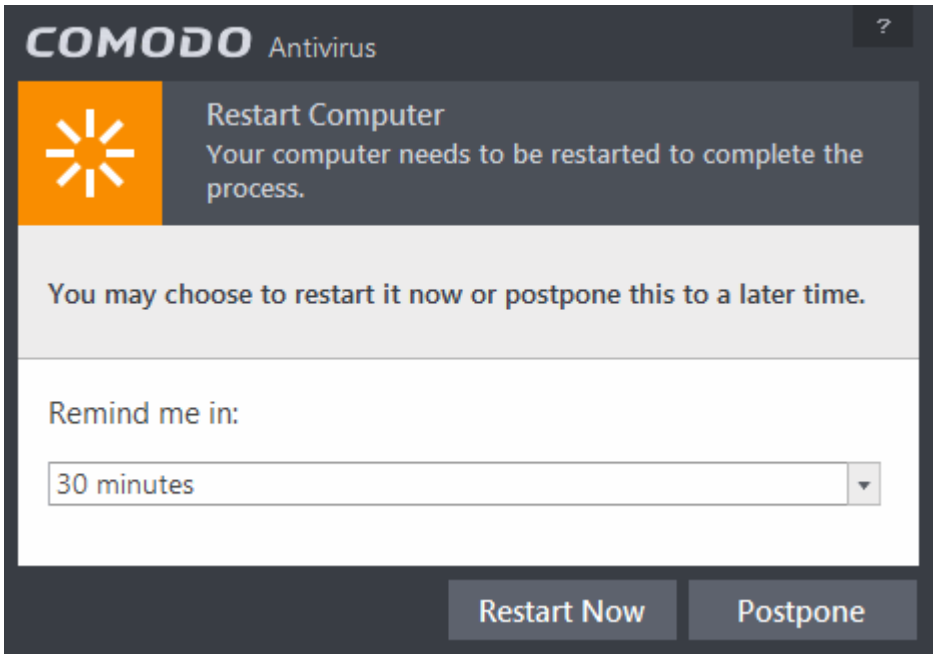
4. Click 'Change' in the next screen. The change progress will be indicated…



... and on completion, Click the Finish button to exit the wizard.



In order for the configuration change to take effect, your computer needs to be restarted. A 'Restart Computer' dialog with a countdown timer will be displayed.



- If you want to restart the system at a later time, click 'No'.
- If you want to restart the system immediately, please save any unsaved data and click 'Yes' or leave the dialog for the system to restart at the end of countdown timer.

Note: The change will take effect only on the next restart of the computer.

Switch Off Automatic Antivirus and Software Updates

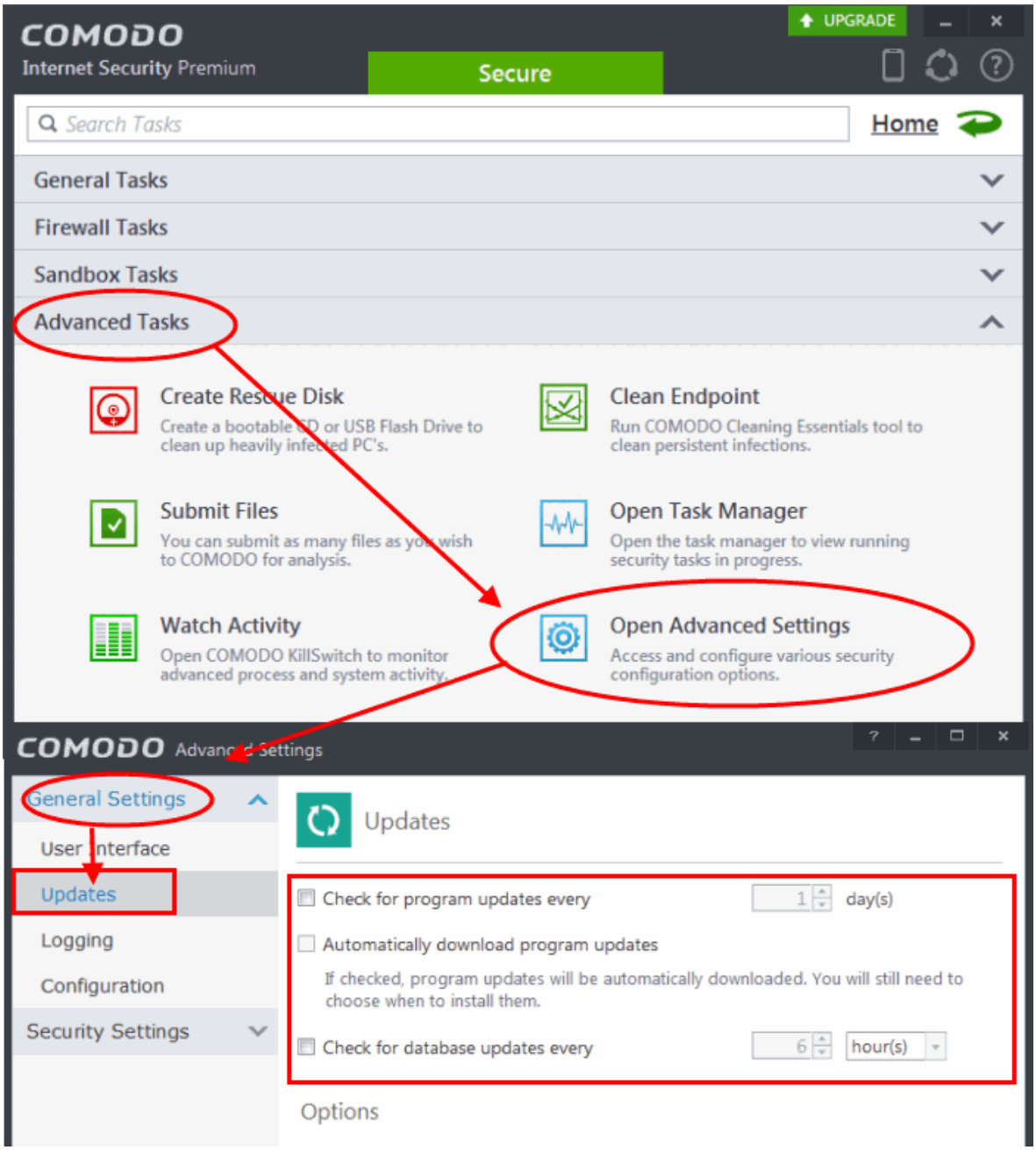
By default, Comodo Internet Security will automatically check for software and Antivirus database updates. However, some users like to have control over what gets downloaded and when it gets downloaded. For example, network administrators may not wish to automatically download because it will take up to much bandwidth during the day. Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.

CIS provides full control over virus and software updates. Click the appropriate link below to find out more:

- **Switch off automatic software and virus signature database updates entirely**
- **Switch off automatic software and virus signature database selectively**
- **Switch off automatic virus signature database updates prior to Antivirus Scans**

To switch off automatic updates entirely:

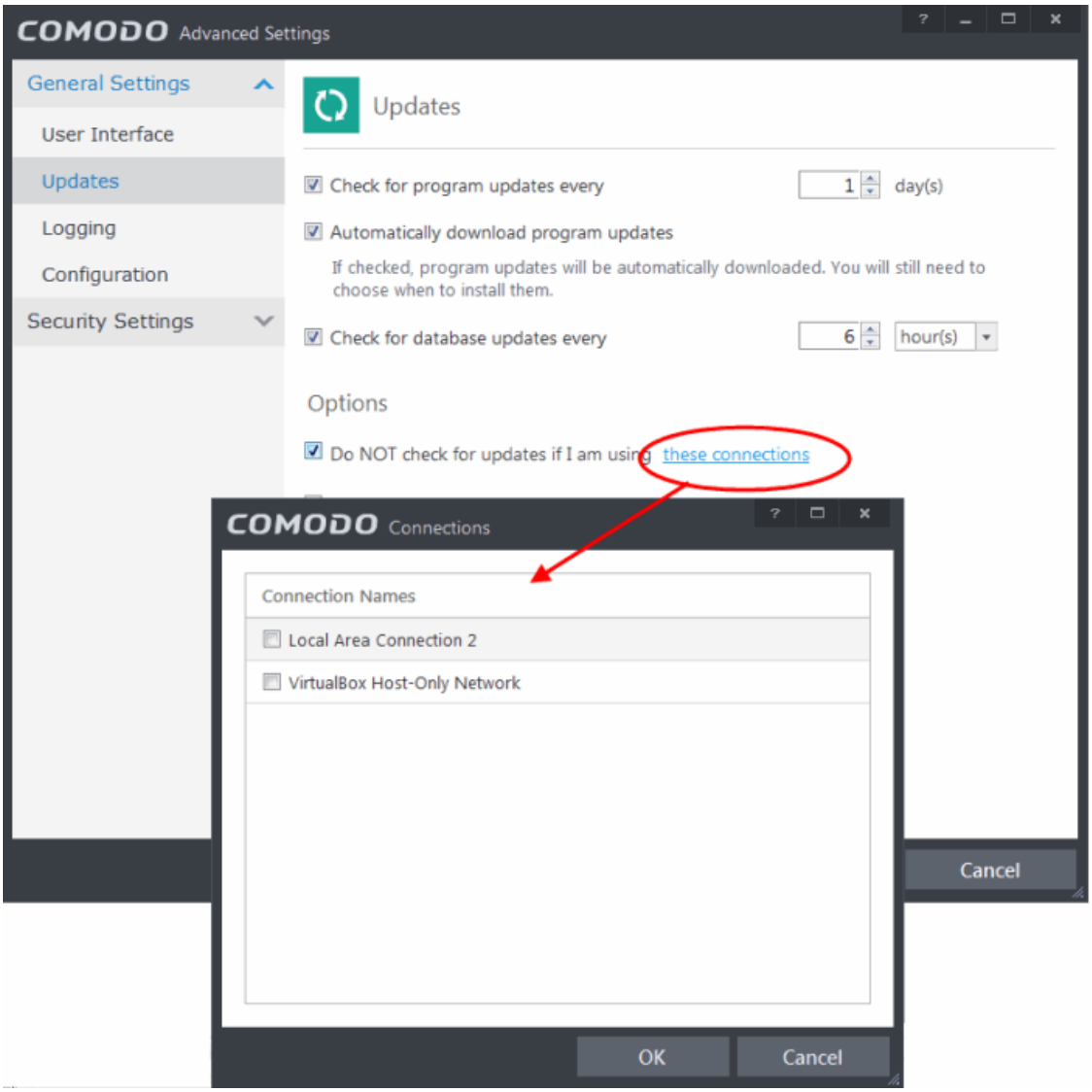
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane
4. Deselect the check boxes 'Check for program updates every xxx day(s)' and 'Check for database updates every xxx hour(s)'



5. Click 'OK' in the Advanced Settings panel.

To switch off automatic updates selectively:

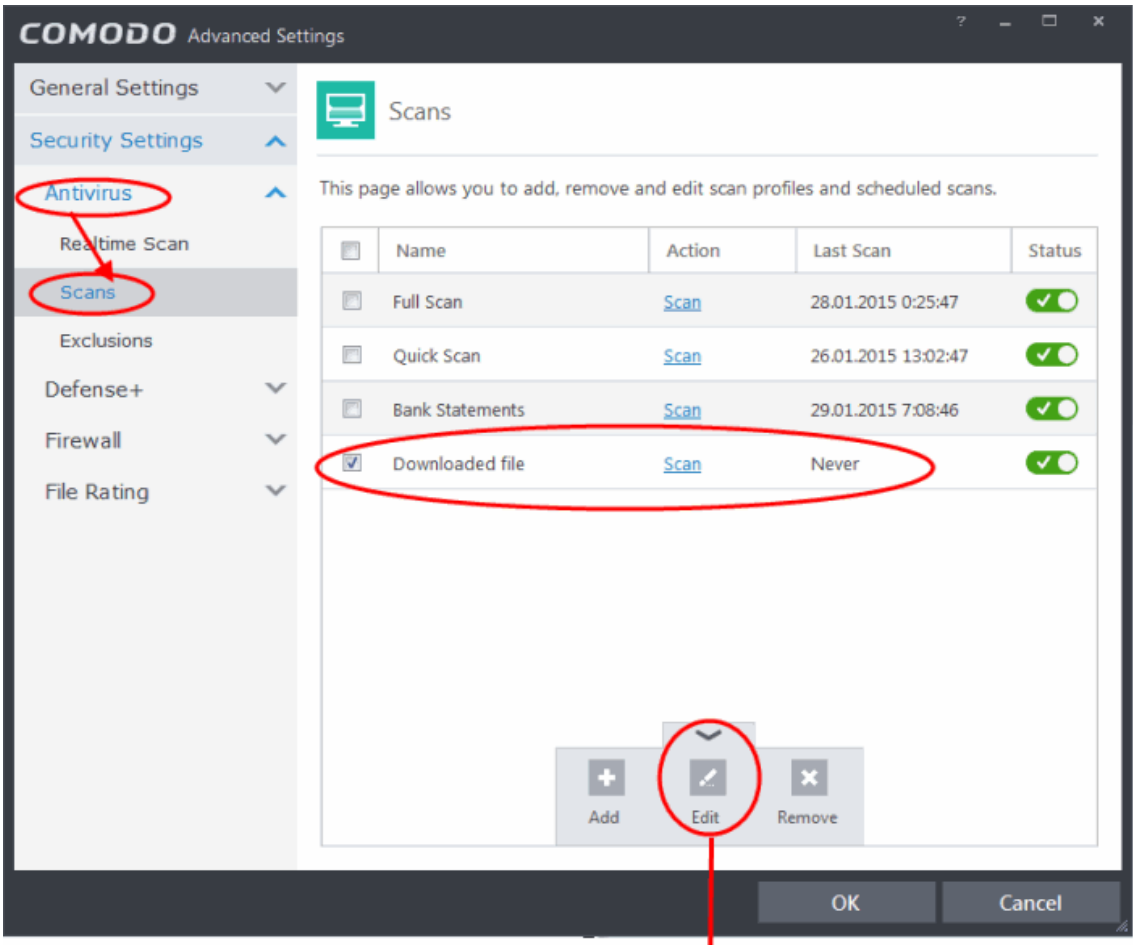
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane

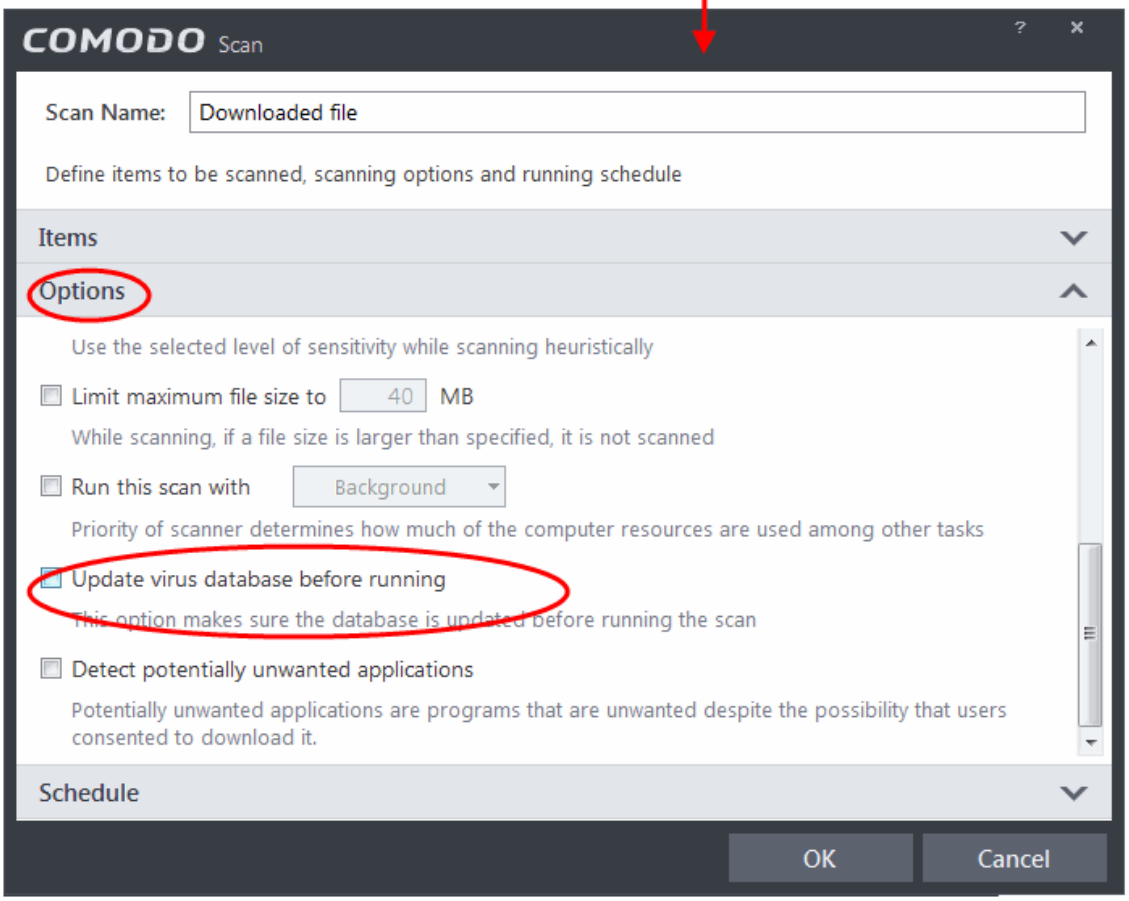


- If you want to suppress automatic updates when you are connected to Internet through certain networks
  - Select the 'Do NOT check updates if am using these connections' check-box
  - Then click the 'these connections'. The 'Connections' dialog will appear with the list of connections you use.
  - Select the connection through which you do not want CIS to check for updates and click OK.
- If you want to suppress automatic updates when your computer is running on battery
  - Select the 'Do NOT check for updates if running on battery' checkbox

To switch off automatic virus signature database updates prior to AV Scans:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Security Settings' > Antivirus' > 'Scans'. A list defined scan profiles will be displayed.
4. Select the scan profile for which you do want the automatic virus database updates prior to the scan


COMODO Advanced Settings
General Settings
Security Settings
Antivirus
Real time Scan
Scans
Exclusions
Defense+
Firewall
File Rating
Scans
This page allows you to add, remove and edit scan profiles and scheduled scans.
Name
Action
Last Scan
Status
Full Scan
Scan
28.01.2015 0:25:47
Quick Scan
Scan
26.01.2015 13:02:47
Bank Statements
Scan
29.01.2015 7:08:46
Downloaded file
Scan
Never
Add
Edit
Remove
OK
Cancel


COMODO Scan
Scan Name:
Downloaded file
Define items to be scanned, scanning options and running schedule
Items
Options
Use the selected level of sensitivity while scanning heuristically
Limit maximum file size to
40
MB
While scanning, if a file size is larger than specified, it is not scanned
Run this scan with
Background
Priority of scanner determines how much of the computer resources are used among other tasks
Update virus database before running
This option makes sure the database is updated before running the scan
Detect potentially unwanted applications
Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download it.
Schedule
OK
Cancel

5. Click the handle from the bottom and select 'Edit'
6. Click 'Options' to open the Options pane, scroll down and deselect 'Update virus database before running' checkbox.
7. Click 'OK' on the 'Scan' interface.
8. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

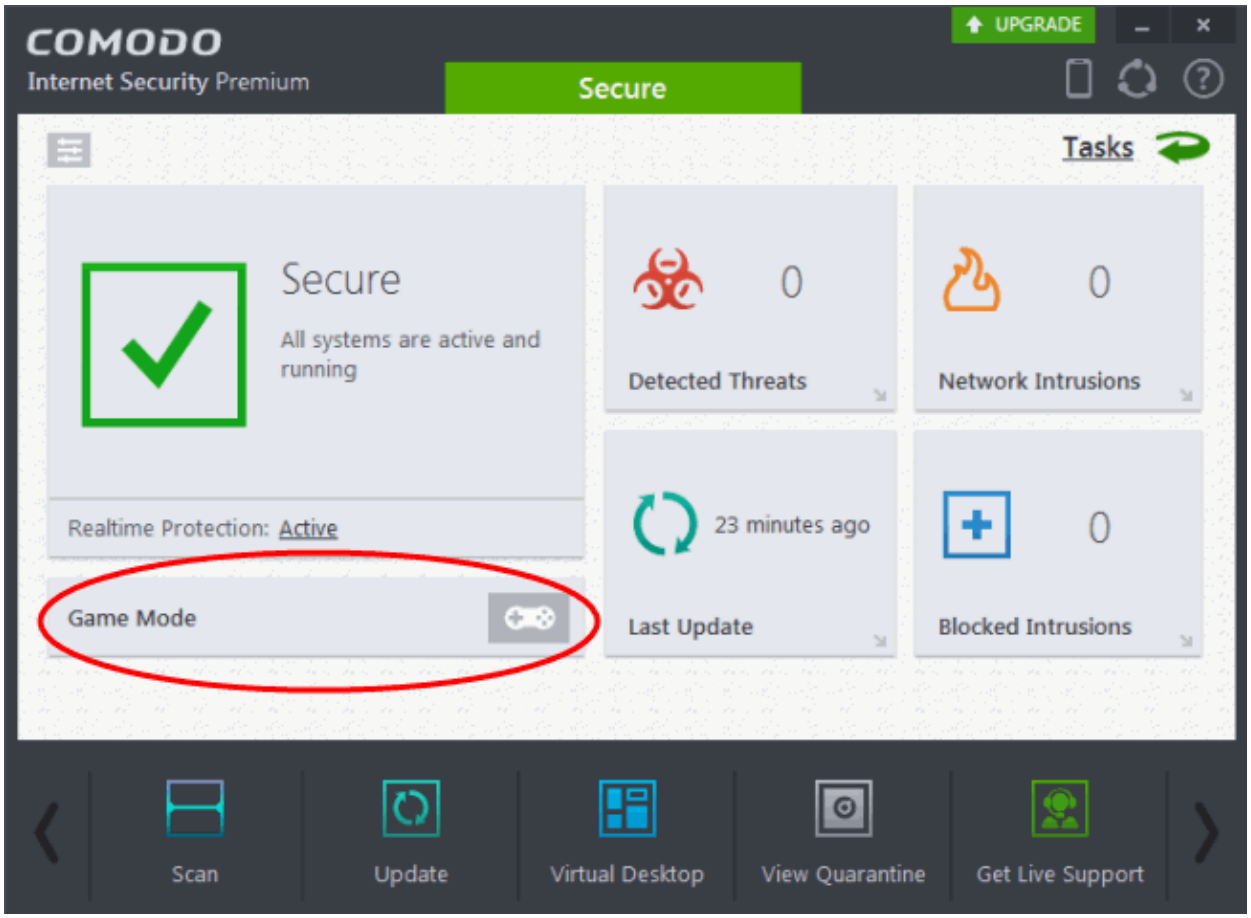
Suppress CIS Alerts Temporarily while Playing Games

Because of continuous monitoring of all your system activities in granular level for implementing Default-Deny Protection, Comodo Internet Security generates pop-up alerts whenever it identifies any event appearing to be a malicious activity or execution of programs that require privileges like Internet access and file access rights. Each alert provides information and options that enable you to make an informed decision on whether you want to allow or block a request or activity. Alerts also to allow you to instruct Comodo Internet Security on how it should behave in future when it encounters activities of the same type.

But at times when you are involved in activities like playing computer games, where you do not want to be interfered with such alerts, you can temporarily stop them from being displayed. require undisturbed environment. During this time, the operations that can interfere with users' gaming experience are either suppressed or postponed.

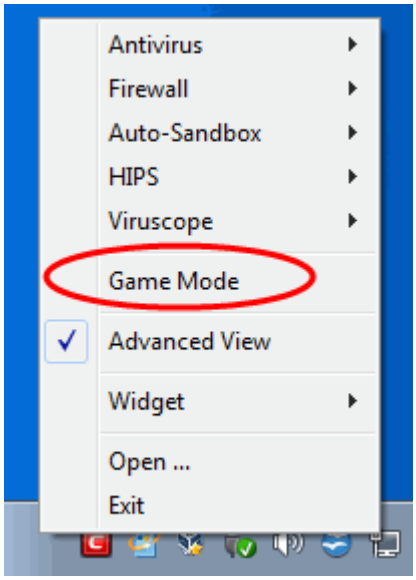
To temporarily stop pop-up alerts

- Click 'Game Mode' button from CIS Home screen



or

- Right click on the CIS System Tray icon and select 'Game Mode' from the options.

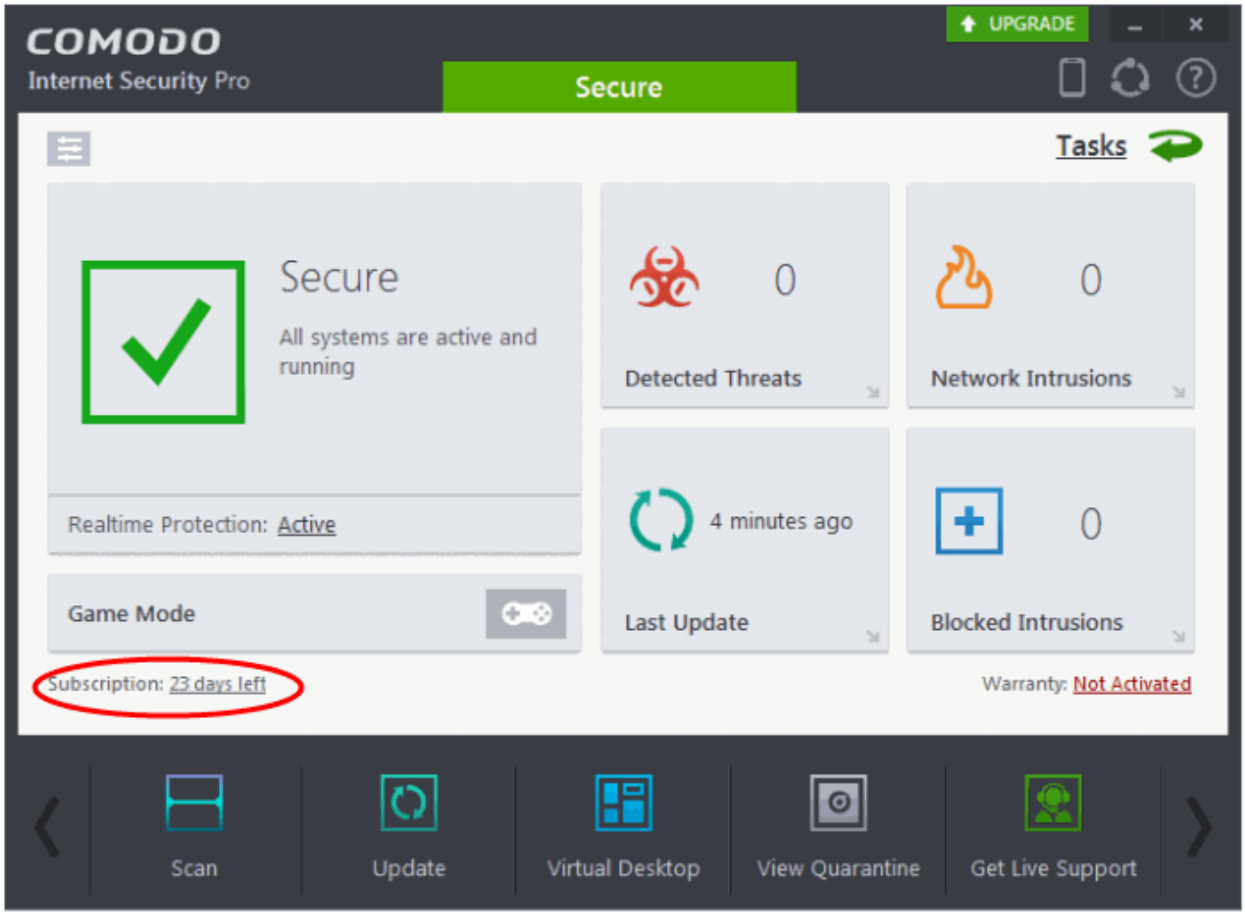


The alerts are now suppressed. To resume alerts and scheduled scans, just de-activate Game Mode from the home screen or the system tray icon right click options.

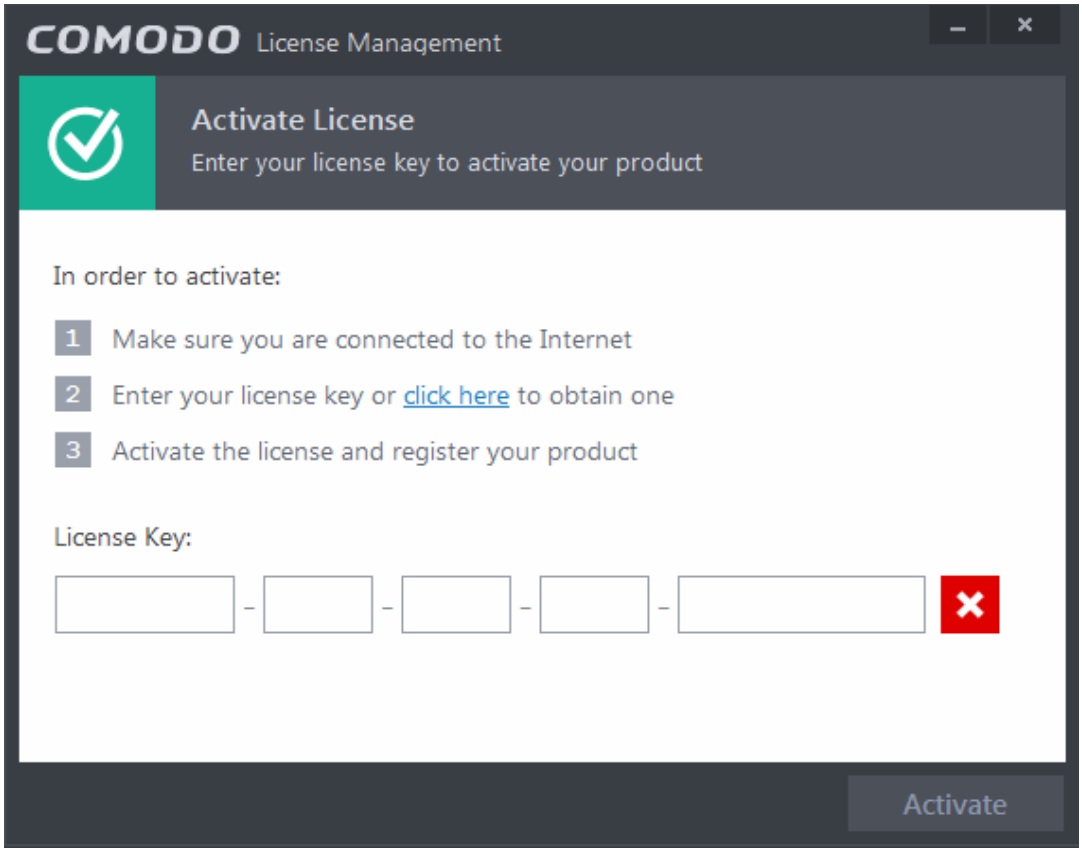
Renew or Upgrade your License

In order to enjoy continued protection from Comodo Internet Security, you will need to renew your license when it is due to expire.

To renew or upgrade your license, click the 'Activate Now' link beside 'Subscription' on the CIS home screen (alternatively, click 'No. of days left')



The Product Activation Wizard will start.



- Click the 'click here' link. You will be taken to the purchase page at **https://secure.comodo.com/home/purchase.php?afl=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUIzRkY&lid=&**
- Select your CIS Package.
- Select 'Existing Comodo User' checkbox in 'Enter Customer Details' area, enter your login and password and complete the payment procedure.
- The License key will be sent to you by email. Enter the license key and click the 'Activate' button.
- After successful validation, your subscription will be activated and a confirmation screen will be displayed.

If you are renewing a license for the same CIS product then entering the license key will upgrade the license without requiring re-installation. If you are upgrading license types, then installation of the new product type will begin automatically. You may need to restart your computer to finalize the upgrade.

If you are using any of the trial versions of CIS, you have to purchase the license at the end of trial period in order to continue using the product. An alert will be displayed after the expiry of trial period.

- Click the 'Renew Now' button in the alert screen and follow the same purchase and activation procedure explained above.

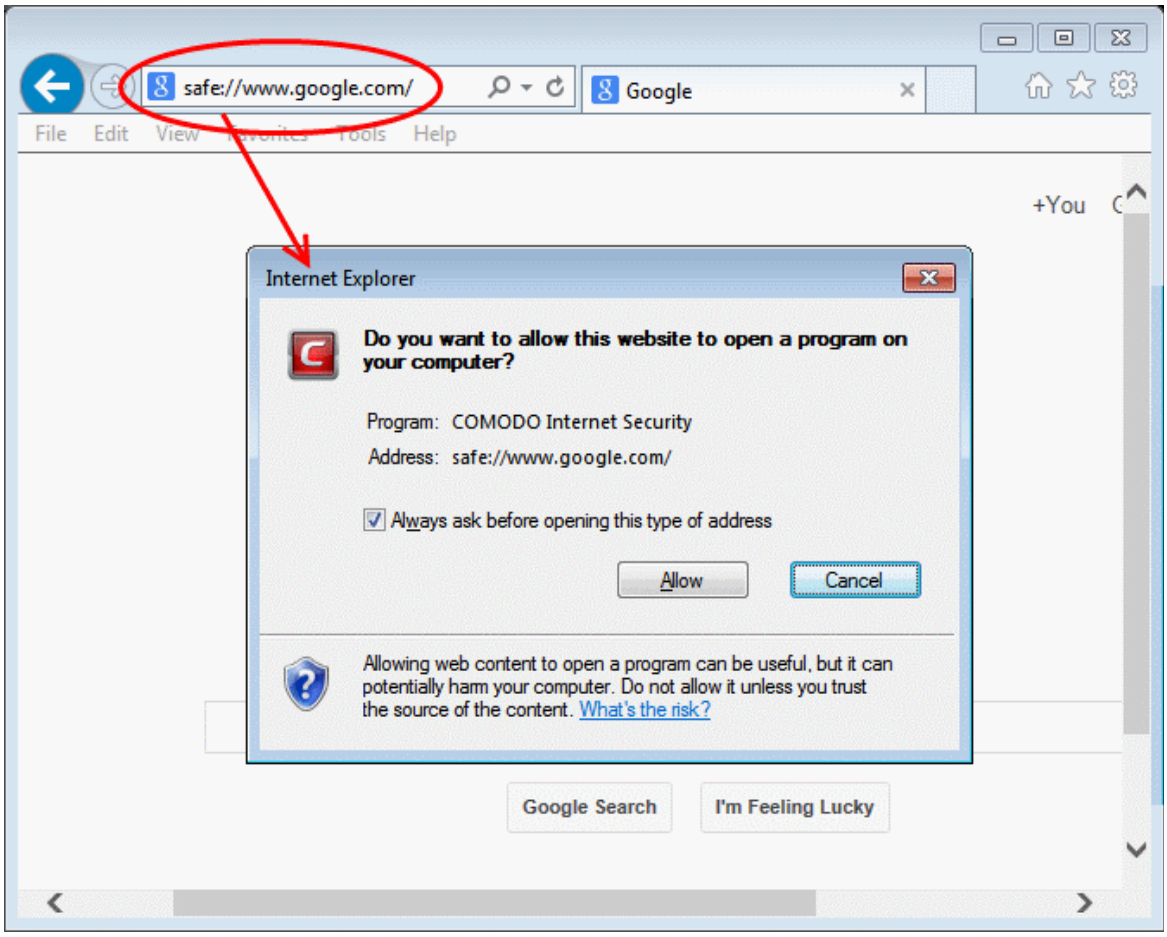
How to Use CIS Protocol Handlers

COMODO Internet Security has its own protocol handlers that allow you to perform certain tasks from a web page. This includes tasks like opening a web page from a sandboxed browser, or starting a virus database update etc. CIS supports several protocol handlers listed below.

1 - safe://

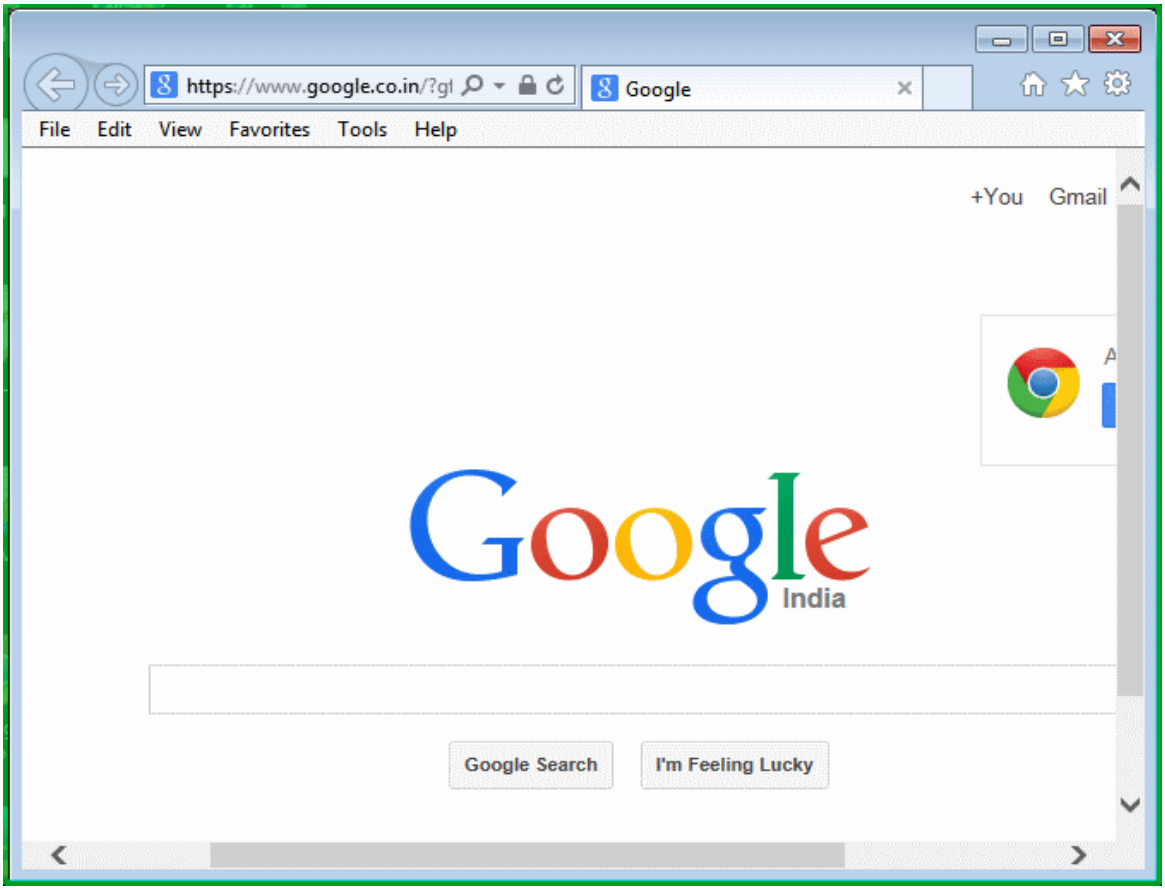
This protocol is used to open any URL with a sandboxed browser.

For example: Try *safe://www.google.com*



- Allow the application

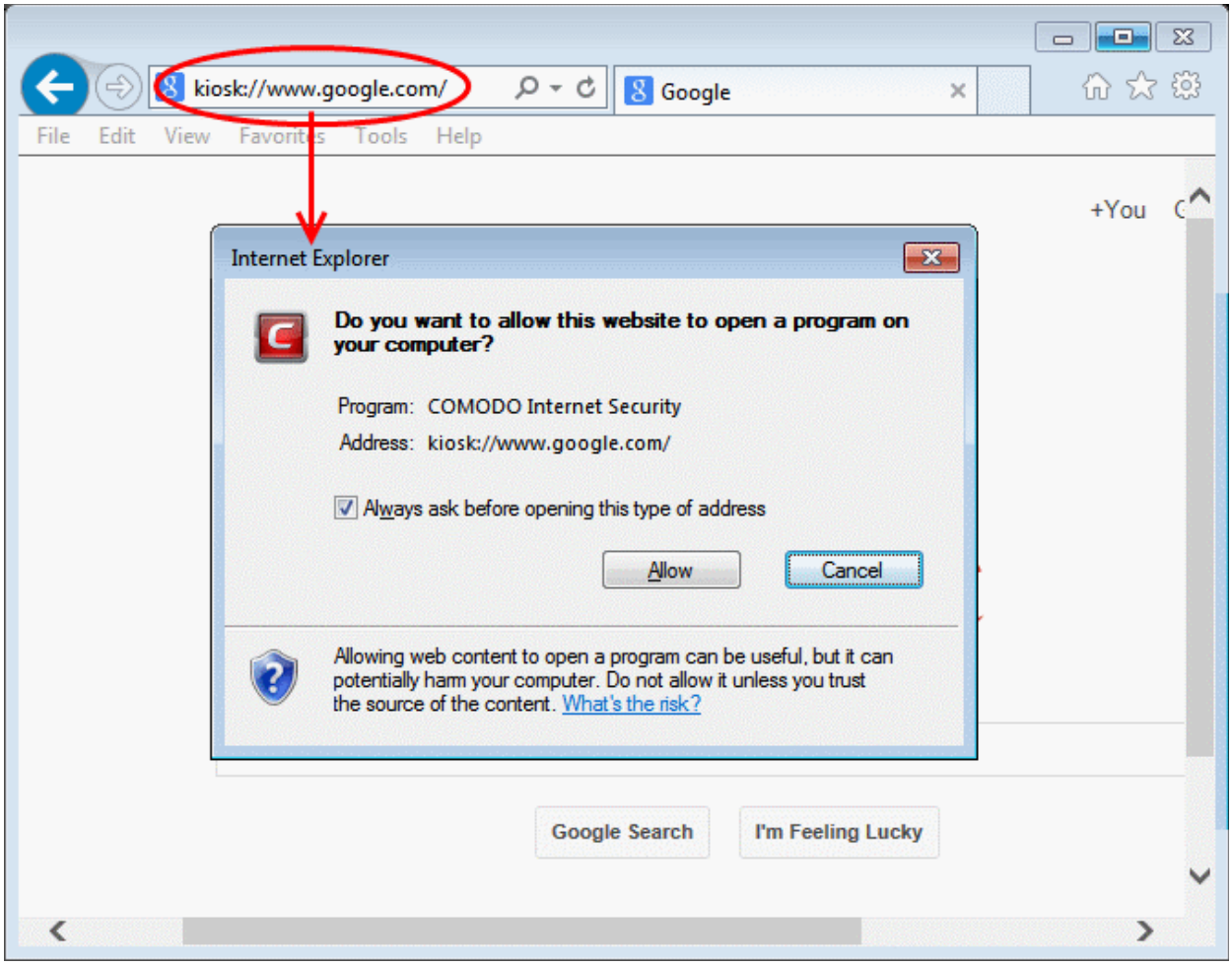
The URL will be open in a sandboxed browser. Note the green border:



2 - kiosk://

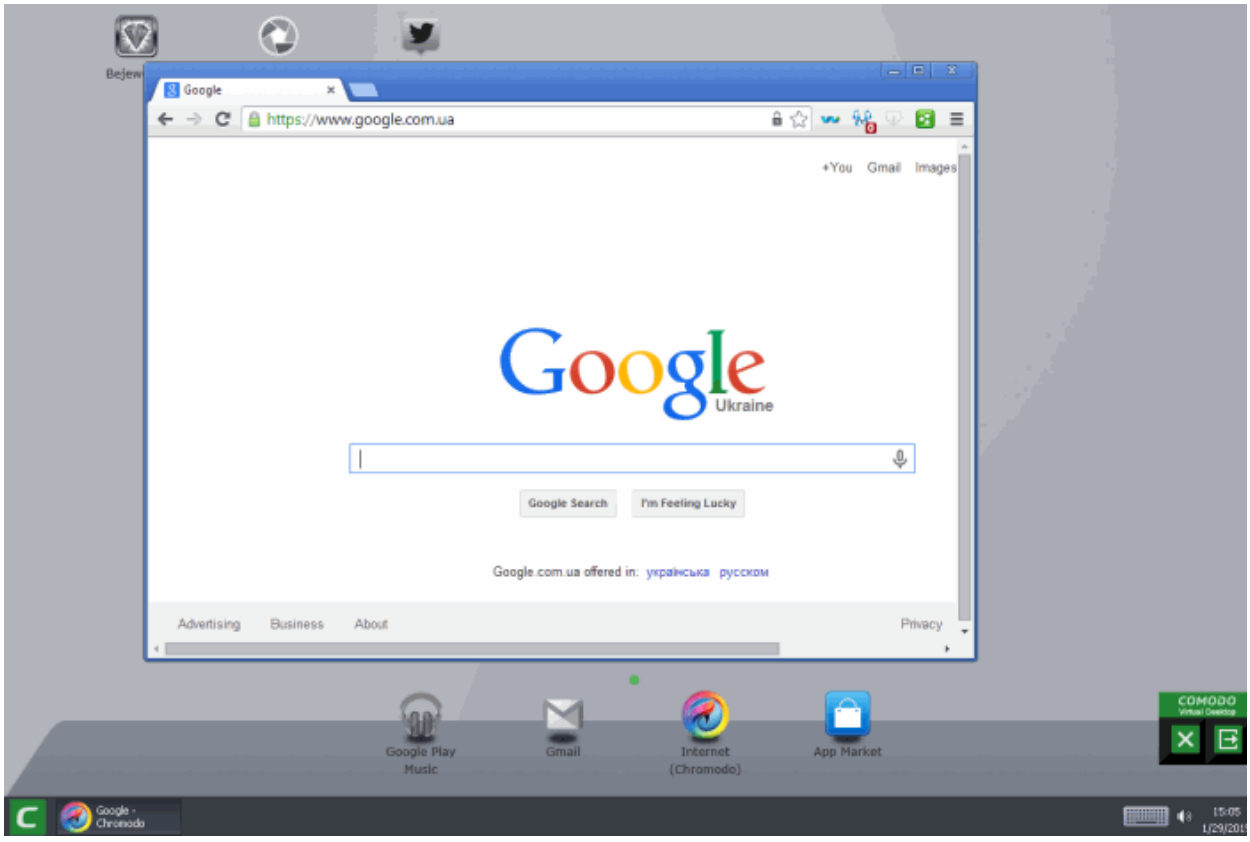
Like the previous one, opens the webpage from COMODO Virtual Desktop.

E.g. Try *kiosk://www.google.com*



- Allow the application

The webpage will be displayed in a browser from the Comodo Virtual Desktop:



Appendix 2 - Comodo Secure DNS Service

Introduction

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Most of the networks use recursive DNS services that are provided by their ISP or that reside on their own set of small DNS servers but it becomes essential to have a secure and broadly distributed DNS service to have a faster and safe DNS resolution.

Background Note: Every device on the Internet is uniquely identified by a 32-bit number (IPv4) or a 128-bit number (Ipv6). While this is perfectly satisfactory for computers, humans are far more comfortable remembering names rather than a string of numbers. The Domain Name System (DNS) provides the translation between those names and numbers. Virtually every piece of software, device, and service on the Internet utilizes DNS to communicate with one another. DNS also makes this information available across the entire span of the Internet, allowing users to find information remotely.

Comodo Secure DNS is a broadly distributed Recursive DNS service that gives you full control to determine how your clients interact with the Internet. It requires no hardware or software and provides reliable, faster, smarter and safer Internet experience.

- Reliable - Comodo Secure DNS Directory Services Platform currently spans across five continents around the world. This allows us to offer you the most reliable fully redundant DNS service anywhere. Each node has multiple servers, and is connected by several Tier 1 carriers to the Internet.
- Faster - Our strategically placed nodes are located at the most optimal intersections of the Internet. Unlike most DNS providers, Comodo Secure DNS Directory Services Platform uses Anycast routing technology - which means that no matter where you are located in the world, your DNS requests are answered by the closest available Comodo Secure DNS set of servers. Combine this with our huge cache and we can get the answers you seek faster and more reliably than anyone else. Furthermore, our "name cache invalidation" solution signals the Comodo Secure DNS recursive servers anytime one of our authoritative customers or partners updates a DNS record, fundamentally eliminating the concept of a TTL.
- Smarter - Comodo's highly structured search and guide pages get you where you want to be, when you inadvertently attempt to go to a site that doesn't exist.
- Safer - As a leading provider of computer security solutions, Comodo is keenly aware of the dangers that plague the Internet today. Secure DNS helps users keep safe online with its malware domain filtering feature. Secure DNS references a real-time block list (RBL) of harmful websites (i.e. phishing sites, malware sites, spyware sites, excessive advertising sites, etc.) and will warn you whenever you attempt to access a site containing potentially threatening content. Additionally, our 'name cache invalidation' solution signals the Comodo Secure DNS recursive servers whenever a DNS record is updated - fundamentally eliminating the concept of a TTL. Directing your requests through highly secure servers can also reduce your exposure to the DNS Cache Poisoning attacks that may affect everybody else using your ISP.

To start Comodo Secure DNS service the DNS settings of your computer has to be modified to point to our server's IP addresses. Comodo Internet Security automatically modifies the DNS settings of your system during its installation to get the services. You can also modify the DNS settings of your system manually, if you haven't selected the option during installation. You can also revert to the previous settings if you want, at anytime.

Click the following links to get the instructions for manually modifying the DNS settings on your router or on your computer.

- **Router**
- **Windows XP**
- **Windows 7/ Windows Vista**

Router - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Router by modifying the DNS settings accessible through DNS Server settings of your router. Comodo recommends making the change on your router so that with one change, all the computers on your network can benefit from Comodo Secure DNS.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Primary DNS : 8.26.56.26

Secondary DNS : 8.20.247.20

To stop Comodo Secure DNS service

- **Modify the DNS server IP address to your previous settings**.

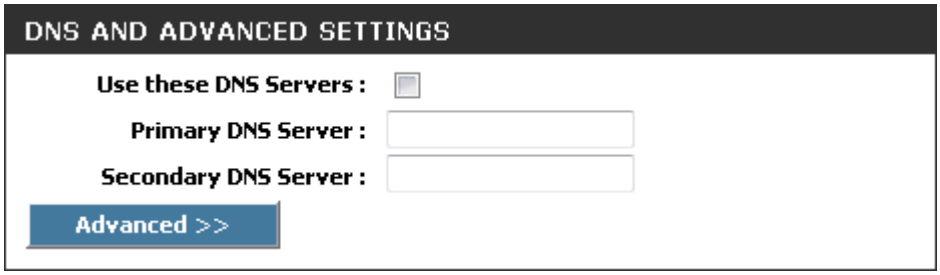
To modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

   http://192.168.0.1
   http://192.168.1.1
   http://192.168.10.1

   If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).

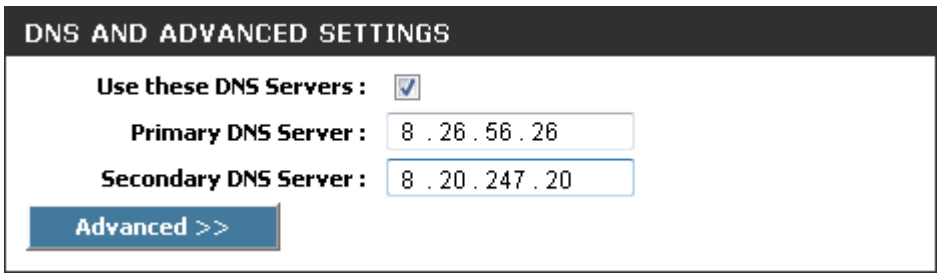


3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

   Primary DNS server address for Comodo Secure DNS is: 8.26.56.26

   Secondary DNS server address for Comodo Secure DNS is: 8.20.247.20

   When you are done, the above example would look like this.



You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.

Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Windows XP computer by modifying the DNS settings accessible through Control Panel > Network Connections.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Preferred DNS : 8.26.56.26

Alternate DNS : 8.20.247.20

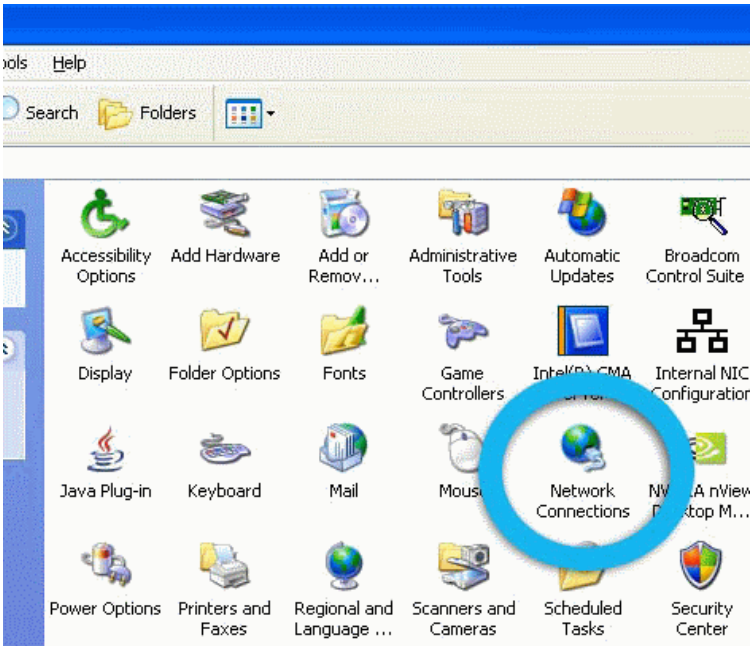
To stop Comodo Secure DNS service

- **Modify the DNS server IP address to your previous settings**.

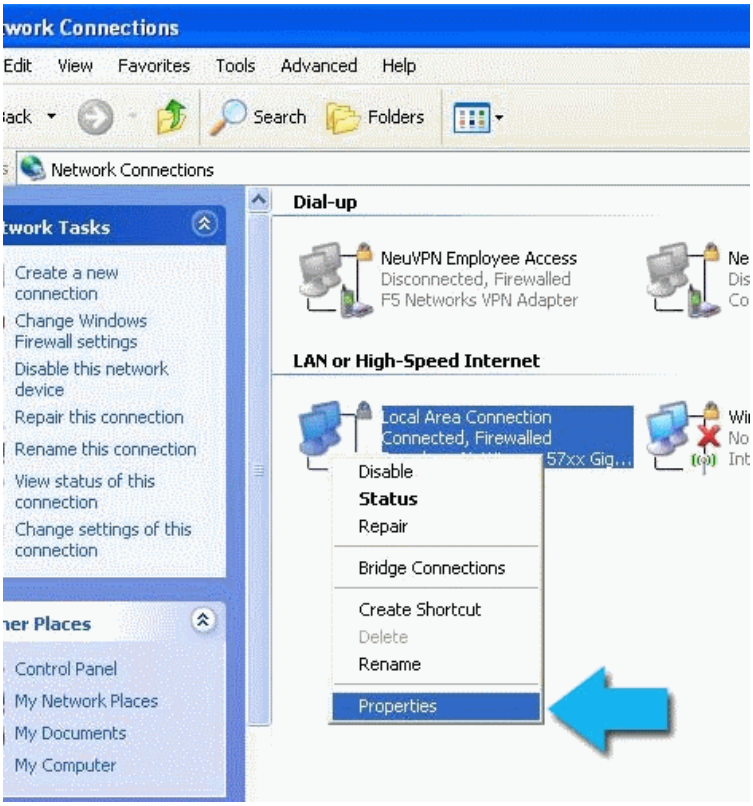
To modify the DNS settings

1. Select the 'Control Panel' from the Start Menu.

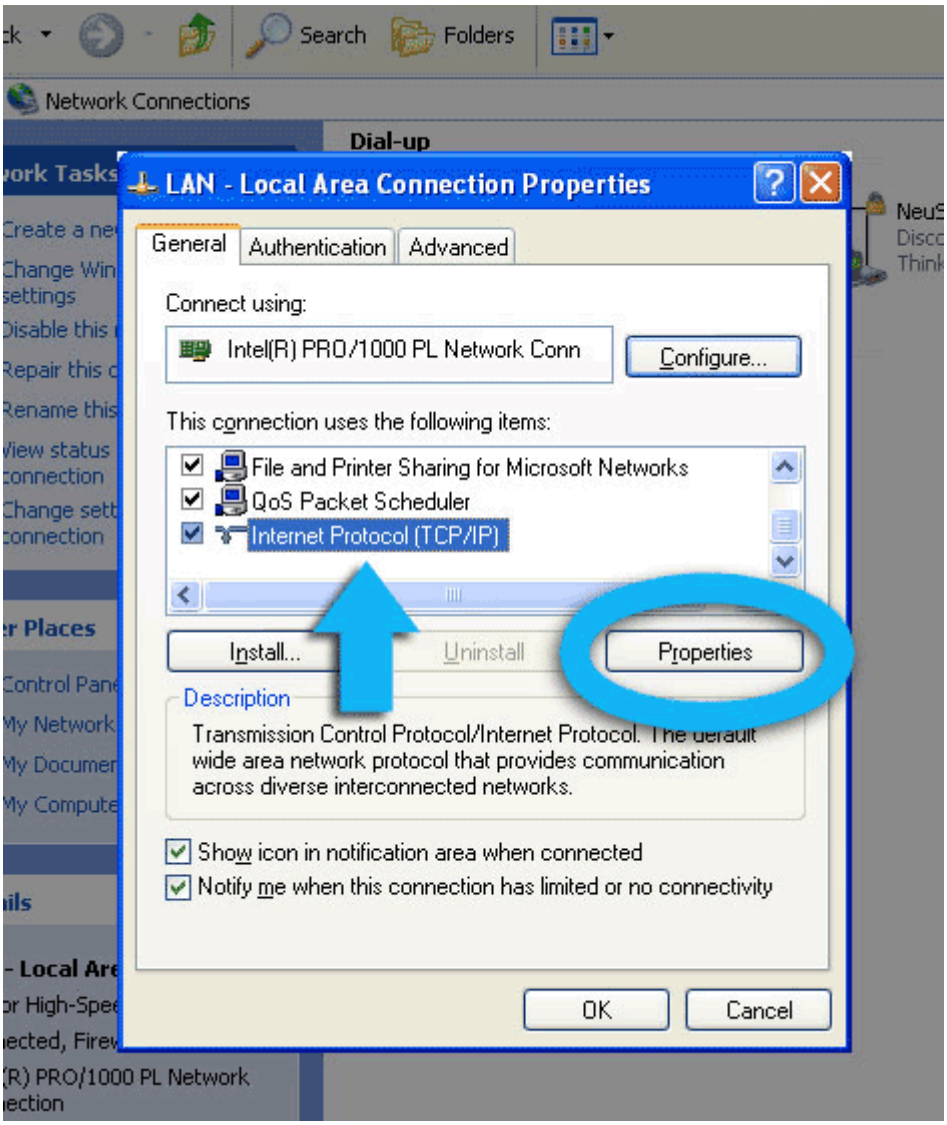
2. Click 'Network Connections' from the Control Panel options.



3. Right click on your connection from the Network Connections window and click 'Properties'.



4. Select 'Internet Protocol (TCP/IP)' and click 'Properties'.

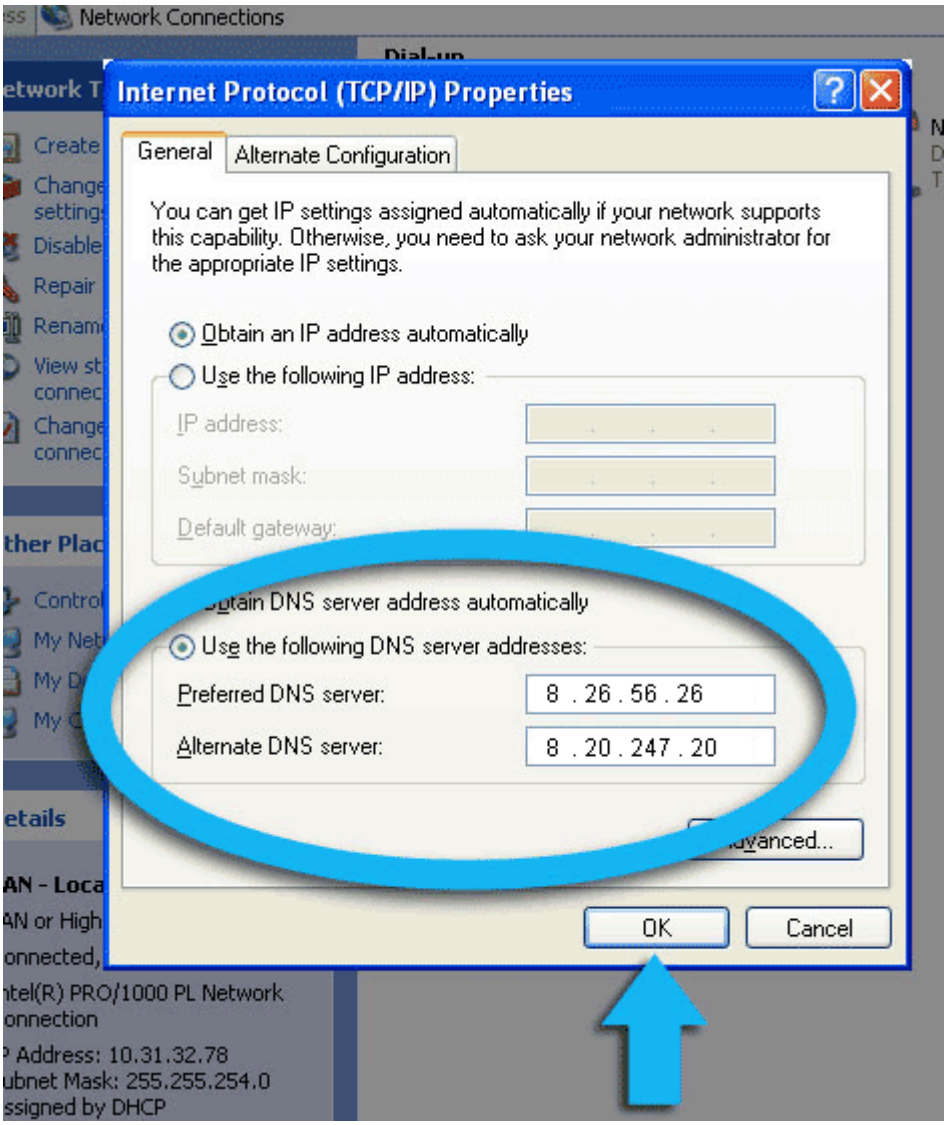


5. Click the radio button Use the following DNS server addresses and type in Comodo Secure DNS addresses in the Preferred DNS server and Alternate DNS server fields.

   Please note down your current DNS settings before switching to Comodo Secure DNS, in case you want to return to your old settings for any reason.

   Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26

   Alternate DNS server address for Comodo Secure DNS is: 8.20.247.20

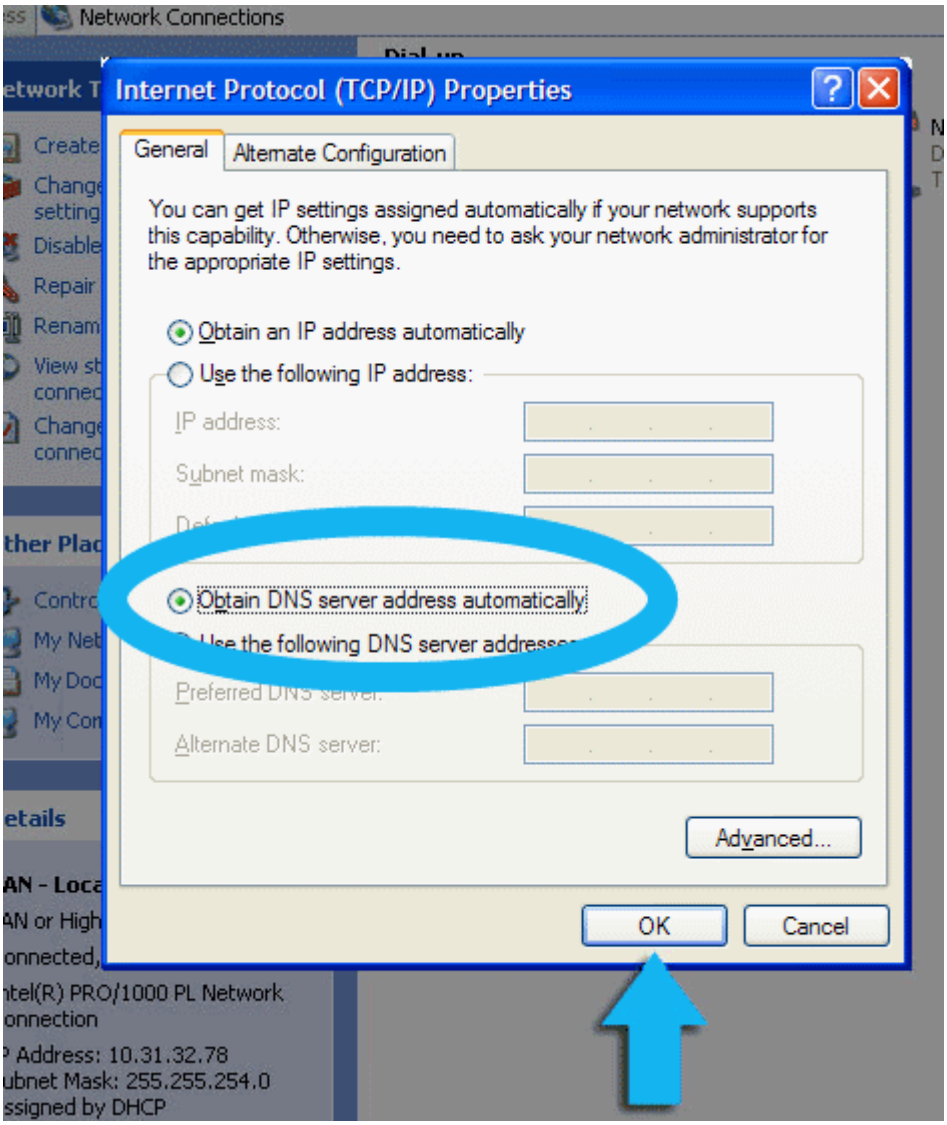


You can disable Comodo Secure DNS by:

- Selecting 'Obtain DNS server address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.



Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable the Comodo Secure DNS service by changing your DNS server addresses to:

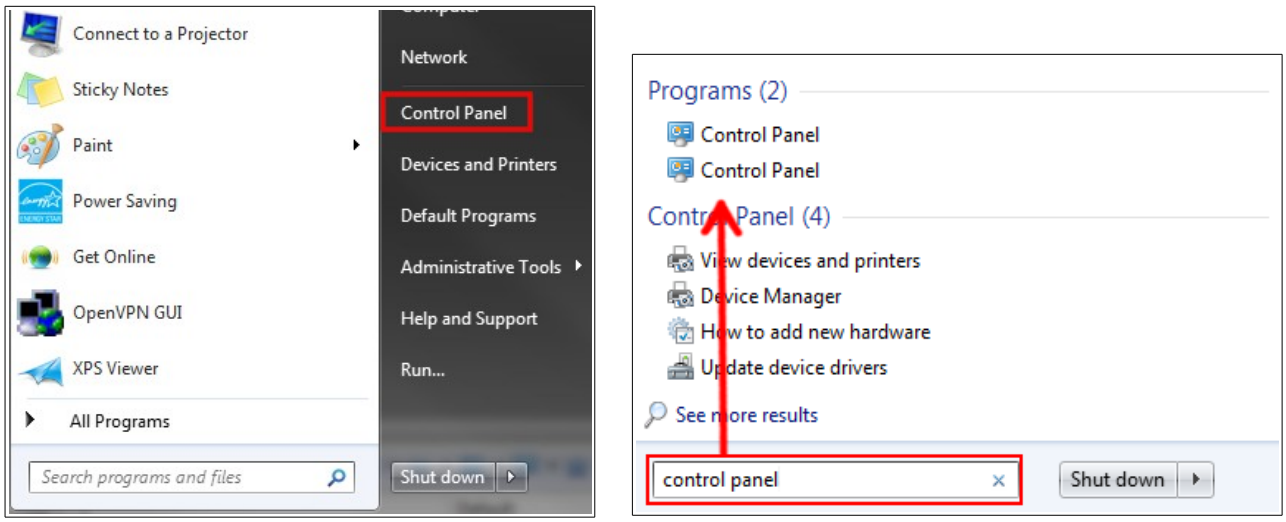
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

Enabling Comodo DNS in Windows 7 / Vista

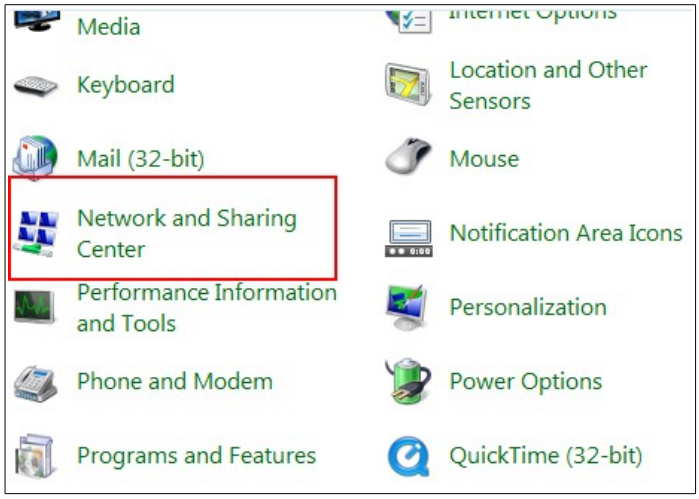
Disabling Comodo DNS in Windows 7 / Vista

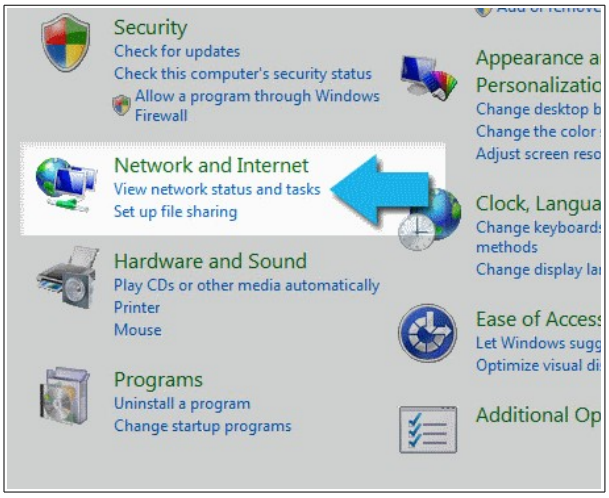
Enabling Comodo DNS in Windows 7 / Vista

1. Open the control panel by either selecting it from the Windows 'Start' menu or by typing 'control panel' into the search box then clicking the program name.

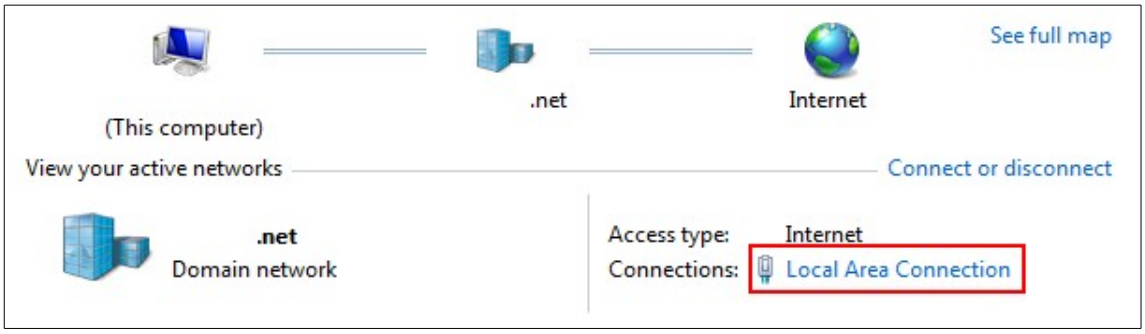


2. From the control panel menu, select 'Network and Sharing Center' (Windows 7) or 'Network and Internet (Vista):

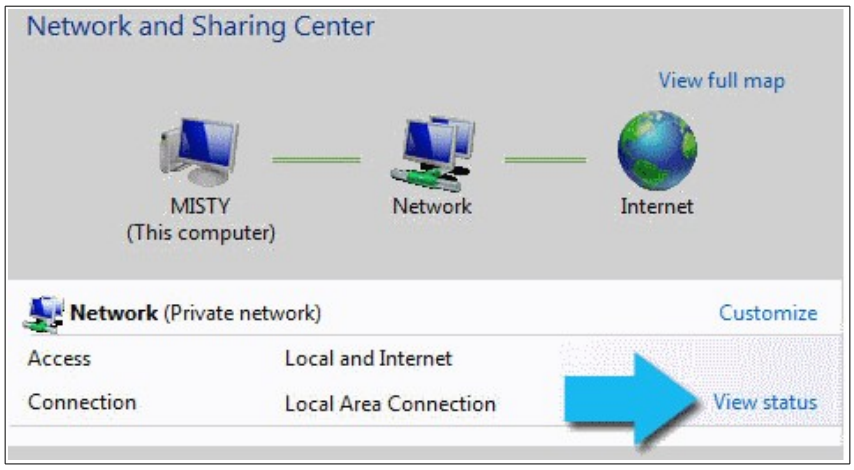




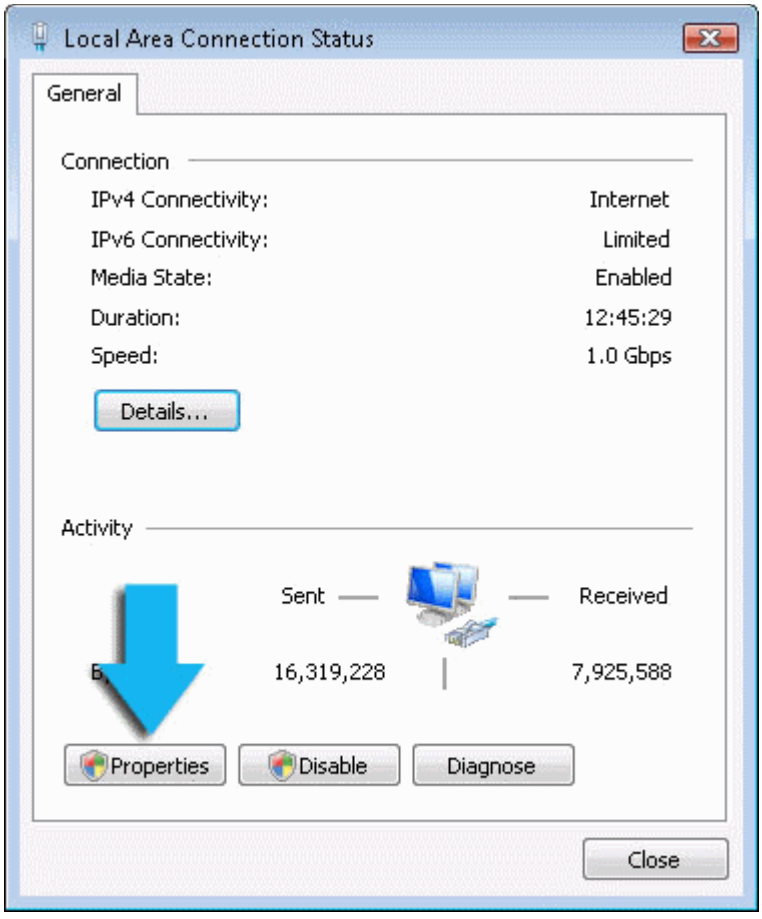
3. In the Network and Sharing center, click the connection type next to 'Connections' (Windows 7):



or 'View Status' (Vista):

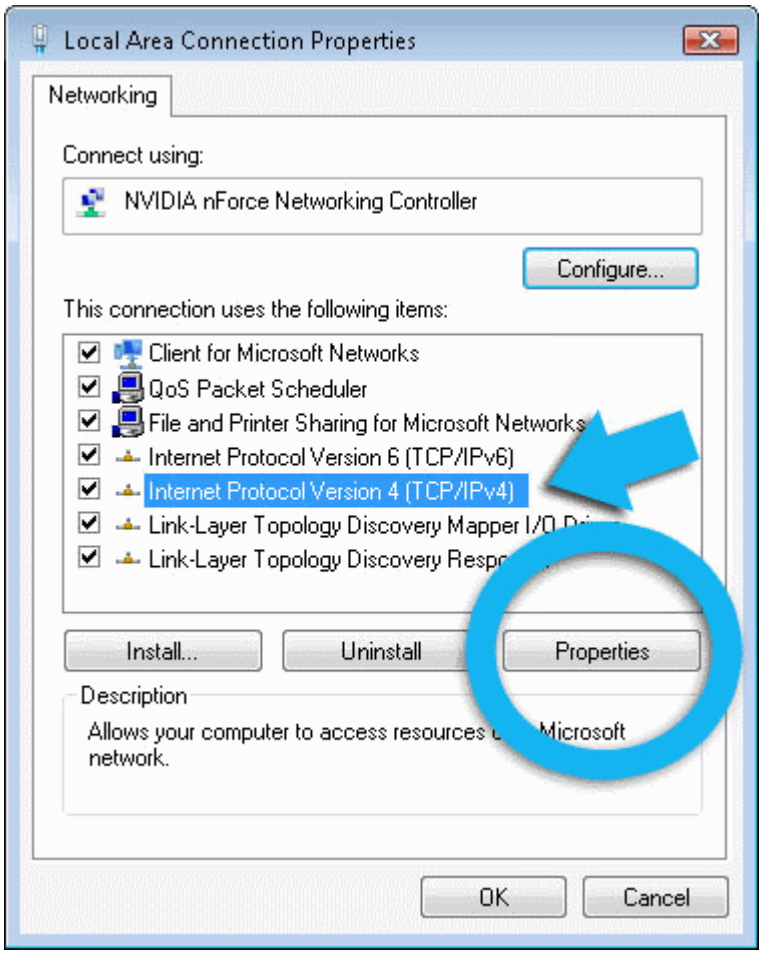


4. This will open the 'Local Area Connection Status' dialog. Click the 'Properties' button:

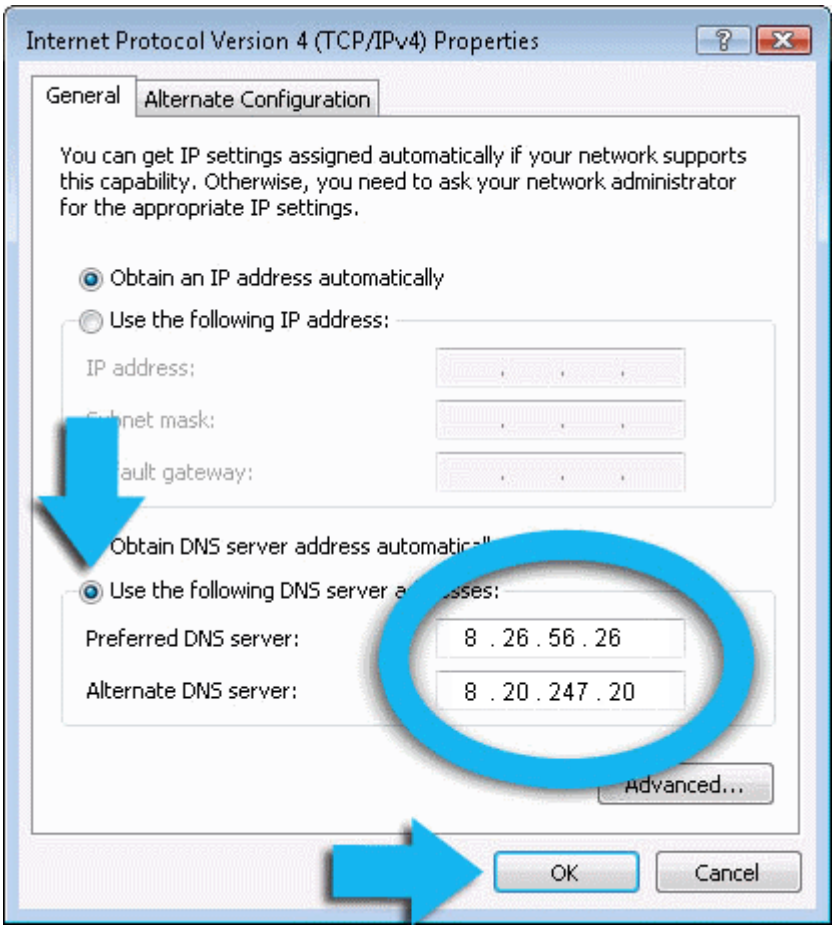


At this point, Windows might ask for your permission to continue or request that you enter an Administrator password.

5. Once you have granted permission/entered an admin password, you will be presented with the 'Local Area Connection Properties' dialog. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button:



6. Enable 'Use the following DNS server addresses'. Doing so will allow you to enter the addresses of Comodo DNS servers in the fields provided. Enter the addresses listed below then click 'OK' to activate your settings:
    - Preferred DNS : 8.26.56.26
    - Alternate DNS : 8.20.247.20

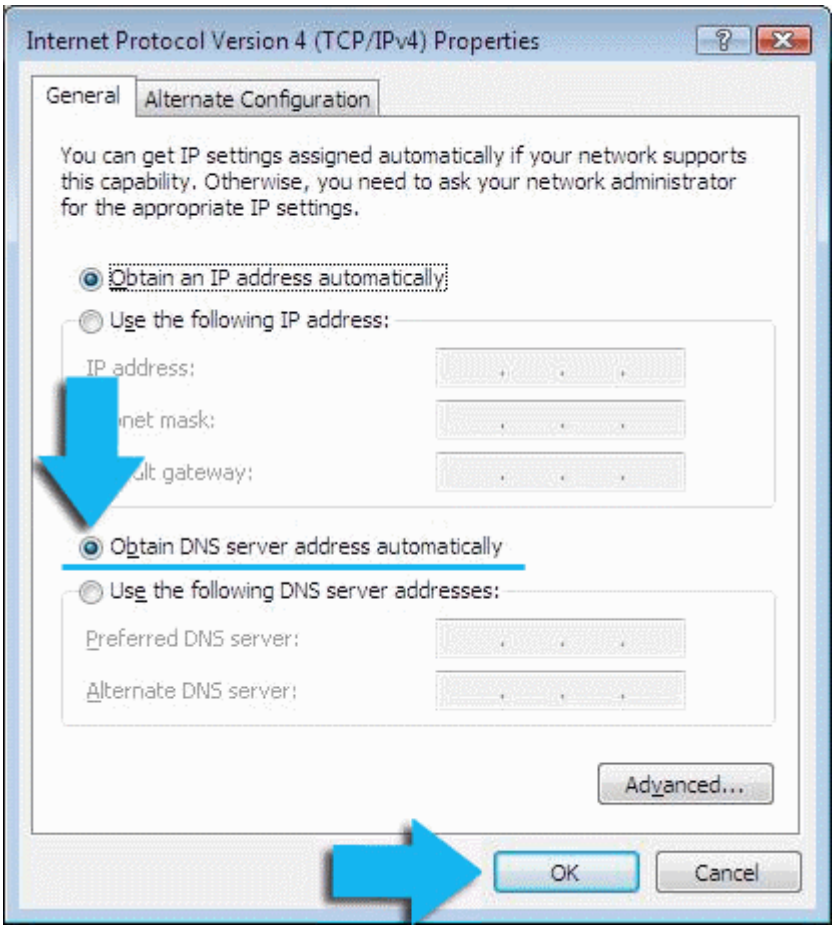


Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the Internet.

Disabling Comodo DNS in Windows 7 / Vista

To disable Comodo DNS, you need to instruct Windows to automatically obtain the address of a DNS server. Doing so means you will use the DNS server provided by your ISP. To do this:

- Follow steps 1 to 7 of the '**Enabling Comodo DNS in Windows 7 / Vista**' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

Appendix 3 - Glossary Of Terms

A B C D E F G H I J K L M N O P Q R S U V W X Y Z

A

ACK

The acknowledgment bit in a TCP packet. (ACKnowledgment code) - Code that communicates that a system is ready to receive data from a remote transmitting station, or code that acknowledges the error-free transmission of data.

Back to the top

Adware

Adware is software which displays advertising content that is unwanted by users and is often installed without their explicit consent as part of another piece of software. Examples of Adware behavior are replacing your home page, redirecting you to web sites you did not request and displaying constant pop-up ads that can adversely impact your online experience.

Back to the top

Antivirus

An antivirus software is an application which is capable of detecting and removing malicious software such as viruses, trojans, worms and scripts from a computer system. A traditional (or 'classic') antivirus relies on a system of 'black-listed' signatures to detect malicious software. Under this system, antivirus vendors create digital signatures of any executable identified as malware. They then send this list of signatures to their customer's local antivirus software via regular (often daily) updates. The customer's antivirus software will then flag as a virus any program with a signature matching a signature on the blacklist.

One drawback with the signature system is its reactive nature - it can only detect 'known' threats. The vendor has to first identify the file as a virus before they can create a signature of it. In many cases, this means the virus has to have already infected someones computer before a signature can be created to combat it.

Because of this limitation, most modern anti-viruses now deploy a wide range of layered technologies to determine the threat level of a particular file. Such technologies include heuristics, behavior analysis, cloud-based scanning, sand-boxing, host intrusion prevention and file-look up services.

Back to the top

Antivirus Scan

An audit performed by an antivirus application in order to detect malware and viruses in the file system and/or memory of a computer.

Back to the top

ARP

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address, also known as MAC address, in an Ethernet local area network.

Back to the top

Attached Resource Computer NETwork (ARCNET)

ARCNET is a local area network (LAN) protocol, similar in purpose to Ethernet or Token Ring. ARCNET was the first widely available networking system for microcomputers and became popular in the 1980s for office automation tasks. It has since gained a following in the embedded systems market, where certain features of the protocol are especially useful.

Back to the top

Auto-sandbox

Auto-sandboxing describes the process whereby applications and processes which are unknown to Comodo Internet Security will be automatically run in a isolated operating environment. Sandboxed applications are run under a set of access restrictions so they cannot cause damage the underlying file structure or operating system. The access restriction level applied to sandboxed applications can be set by the user and includes 'Limited', 'Partially Limited', 'Restricted', 'Untrusted', 'Blocked' and

'Fully Virtualized'.

Conceptually, the auto-sandbox is designed to securely handle 'unknown' executables - those which are not present on Comodo's black-list (definitely malicious) or white-list (definitely safe). If the unknown file turns out to be malicious then it cannot cause any harm because the sand-boxing process denied it access to critical system resources. On the other hand, programs that are unknown but perfectly harmless will run just as well in the sandbox. This allows safe applications the freedom to run as intended while denying malicious applications the ability to cause damage.

The auto-sandbox process is further enhanced if it is married to a system that can subsequently classify these unknown files as either 'safe' or 'malicious'. In Comodo Internet Security, sandboxed files can be submitted to Comodo servers* for automated behavior analysis. If this analysis discovers the file is malicious then it is added to the black-list which is distributed to all CIS users. If the file does not exhibit malicious behavior it is passed to Comodo labs for more in-depth tests and possible inclusion on the white-list.

** if enabled by the user*

Back to the top

B

Behavior Analysis

An activity performed by CIS to determine whether an unknown application in the sandbox is malicious or not. Unknown files are analyzed by Comodo Cloud Scanners and Comodo's Instant Malware Analysis (CIMA) servers. If found to be safe, they will be submitted to Comodo labs for further checks.

Back to the top

Behavior Blocker

A Host Intrusion Protection (HIPS) mechanism that monitors the behavior of software and files in your system and prevents them from taking actions that would cause damage.

Back to the top

Brute-force

Brute-force search is a trivial but very general problem-solving technique, that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

Back to the top

Buffer Overflow

A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations, often causing the process to crash or produce incorrect results. Hackers use buffer overflows as a trigger to execute to execute malicious code.

Back to the top

Bug

Error in a program that cause problems.

Back to the top

C

CA - Certification Authority

A Certificate Authority (CA) is trusted third party that validates ownership information about a web-server then issues an SSL/TLS certificate to the organization that owns the server. The certificate is then placed on the web-server and is used to secure connections between the server and any clients (browsers) that connect to it. For example, an online store would use a certificate to secure its order forms and payment pages.

A Certificate Authority (CA) such as Comodo CA will sign the certificates it issues with their private key. However, for the website's certificate to operate correctly, there is a reciprocal client side requirement - the internet browser that the visitor is using MUST physically contain the certificate authority's 'root certificate'. This root is required to successfully authenticate any website certificates that have been signed by the CA. If the root certificate is not embedded in a browser, then the website's certificate will not be trusted and visitors will see an error message. Certificate Authorities proactively supply browser vendors with their root certificates for inclusion in the browser's 'certificate store' - an internal repository of root certificates that ships with each browser.

Back to the top

CIS Widget

The CIS Widget is a handy control panel that shows information about the security status of your computer, the speed of outgoing and incoming traffic and other useful information. The widget also has shortcuts to common CIS tasks and allows users to launch sandboxed instances of any internet browser they have installed on their system. By default, the widget is displayed on the desktops of Windows computers running CIS version 6.0 and above.

Back to the top

COM Interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on a computer. Comodo Internet Security automatically protects COM interfaces against modification.

Back to the top

Computer Network

A computer network is a connection between computers through a cable or some type of wireless connection. It enables users to share information and devices between computers and other users within the network.

Back to the top

D

Debugging

The process of identifying a program error and the circumstances in which the error occurs, locating the source(s) of the error in the program and fixing the error.

Back to the top

DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices to connect to a network and be automatically assigned an IP address.

Back to the top

Digital Certificate

A digital certificate is a file used to cryptographically bind a company's Public Key to its identity. Like a driving license or passport binds a photograph to personal information about its holder, a digital certificate binds a Public Key to information about that company. They are issued for between 1 and 5 year validity periods.

Digital certificates are issued by a Certificate Authority like Comodo. Each CA acts as a trusted third party and conducts background checks on a company to ensure they are legitimate before issuing a certificate to them. Apart from providing an encrypted connection between a internet browser and a website, digital certificates are intended to reassure website visitors that the company they are about to make a purchase from can be trusted.

To get a digital certificate, a company must first generate a Certificate Signing Request (CSR) on their web-server. This CSR contains their public key and their identity information. They then enroll and pay for the certificate and send their CSR to the CA.

The CA's validation department will check that the identity information in the CSR is correct by conducting background checks and will sometimes request that the company supplies documentation such as articles of incorporation. Once validation is satisfactorily completed, the CA will issue the certificate to the customer. The customer will then install it on their website to secure sensitive areas like payment pages.

Back to the top

Digital Signature

Digital signatures are used for authentication and integrity, meaning it guarantees that the person sending a message is indeed the same person who he/she claims to be and the message has not been altered. To authenticate oneself using a digital signature, a person needs to download and install Digital Certificates in their systems from Certificate Authorities such as Comodo. The client certificate then can be imported into their browsers and email clients. The same certificate can also be used to digitally sign a document before sending it. The recipient can easily find out if the document has been tampered with en-route.

Back to the top

DNS

DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. When a user searches for a website name like 'www.domain.com', their browser will first contact a DNS server to discover the IP address associated with that domain name. Once it has this information, it can successfully connect to the website in question.

Back to the top

Dynamic IP

The procedure of allocating temporary IP addresses as they are needed. Dynamic IP's are often, though not exclusively, used for dial-up modems.

Back to the top

E

Encryption

Encryption is a technique that is used to make data unreadable and make it secure. Usually this is done by using secret keys and the encrypted data can be read only by using another set of secret keys. There are two types of encryption - symmetric encryption and asymmetric encryption.

Symmetric encryption is applying a secret key to a text to encrypt it and use the same key to decrypt it. The problem with this type of encryption lies during the exchange of secret keys between the sender and the recipient over a large network or the Internet. The secret keys might fall into wrong hands during the exchange process.

Asymmetric encryption overcomes this problem by using two cryptographically related keys, a key pair - a public key and a private key. The private key is kept secret in your system and the public key is made available freely to anyone who might want to exchange messages with you. Any message, be it text, documents or binary files that are encrypted using the public key can be decrypted using the corresponding private key only. Similarly anything that is encrypted using the private key can be decrypted using the corresponding public key. Typically public keys are made available to everyone by using Digital Certificates. The certificates are issued by a Certificate Authority (CA), which identifies a server or user and usually contains information such as the CA who issued it, the organization's name, email address of the user and country and the public key of the user. When a secure encrypted communication is required between a client and a server, a query is sent over to the other party for the certificate and the public key can be extracted from it.

Back to the top

End User

The person who uses a program after it's been compiled and distributed.

Back to the top

EPKI Manager

Enterprise Public Key Infrastructure Manager. The EPKI Manager allows you to issue bulk numbers of:

- SSL Certificates for use on domain names owned by your Company;
- SecureEmail Certificates (S/MIME) for use by employees of your Company.

Your nominated EPKI Manager Administrator(s) will be able to manage all the company's Certificates from a central web based console. Additional certificates may be purchased through the console in minutes; ensuring new servers and employee email may be secured in minutes rather than days. For more information about EPKI Manager click **here**.

Back to the top

Ethernet

Ethernet is a frame-based computer networking technology for local area networks (LANs). The name comes from the physical concept of ether. It defines wiring and signaling for the physical layer, and frame formats and protocols for the media access control (MAC)/data link layer of the OSI model. Ethernet is mostly standardized as IEEEs 802.3. It has become the most widespread LAN technology in use during the 1990s to the present, and has largely replaced all other LAN standards such as token ring, **FDDI**, and **ARCNET**.

Back to the top

Executable Files

An 'executable' is a file that instructs a computer to perform a task or function. Every program, application and device run on computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. For example, when Microsoft Word is started, the executable file 'winword.exe' instructs the computer to start and run the Word application. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Back to the top

F

False Positive

When an antivirus scan is run and the scanner reports that some programs are infected with malware which may not be the actual case and the files are safe. This kind of false alert is called 'False Positive'. Too much of False Postive results can be annoying and the user might just ignore legitimate warning or delete legitimate files causing the relevant program or operating system to malfunction.

Back to the top

Firewall

A firewall is an application that helps an user or administrator to have a control over how the system should be connected with other network/systems or over the Internet.

Back to the top

FS type

Type of file system.

Back to the top

FTP

File Transfer Protocol (FTP) is a protocol used for file transfer from computer to computer across a TCP network like the Internet. An anonymous FTP is a file transfer between locations that does not require users to identify themselves with a password or log-in. FTP uses the TCP/IP protocols to enable data transfer. FTP is most commonly used to download files from a server or to upload a file to a server.

Back to the top

G

Graphical User Interface (GUI)

The visual symbols and graphics with which a user controls a piece of software or device. Most software has a GUI that comprises of windows, menus, and toolbars. The user interacts with the GUI by clicking their mouse on a GUI element. Operating systems like Windows use GUI's because most users find them easier to use than less friendly interfaces like a command line.

Back to the top

H

Heuristics

Heuristics is a technique that continuously evolves based on experience for solving problems, discovery and learning. When the term is used in computer security parlance, Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist. Comodo Internet Security applies this technology in the application, which is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

Back to the top

HIPS

A Host Intrusion Protection System (HIPS) is designed to identify and block zero malware by monitoring the behavior of all applications and processes. It is designed to prevent actions that could cause damage to your operating system, system-memory, registry keys or personal data.

Security software using a HIPS system will generally enforce rules prescribing the permitted activities of processes and executables at the point of execution. Examples of such activities can include changes to files or directories, accessing protected COM interfaces, modifications to the registry, starting up another application or writing to the memory space of another application. The precise nature of these rules can be set by the user or pre-configured by the vendor.

If an executable or process attempts to perform an action that transgresses these rules then the HIPS system will block the attempt and generate an alert notifying the user of that action. Most HIPS alerts will also include security advice.

Back to the top

HTTP

HTTP (Hypertext Transfer Protocol) is the foundation protocol of the World Wide Web. It sets the rules for exchanges between browser and server. It provides for the transfer of hypertext and hypermedia, for recognition of file types, and other functions.

Back to the top

I

ICMP

The Internet Control Message Protocol (ICMP) is part of Internet Protocol (IP) suite and used to report network applications communications errors, network congestion, timeouts and availability of remote hosts.

Back to the top

IDS

An Intrusion Detection System (IDS) is software/hardware that detects and logs inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Back to the top

IMAP

Internet Message Access Protocol'. IMAP is a method of distributing email. It is different from the standard POP3 method in that with IMAP, email messages are stored on the server, while in POP3, the messages are transferred to the client's computer when they are read. Thus, using IMAP allows you to access your email from more than one machine, while POP3 does not. This is important because some email servers only work with some protocols.

Back to the top

Information Security Exposure

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

Back to the top

Internet Service Provider (ISP)

A company or organization that provides the connection between a local computer or network, and the larger Internet.

Back to the top

IP - Internet Protocol

The Internet Protocol (IP) is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched network. An IP address is a numeric address that is used to identify a network interface on a specific network or subnetwork. Every computer or server on the Internet has an IP address. When a user types a domain name such as www.domain.com into the address bar of their browser, the browser still needs to find the IP address associated with that domain in order to reach the website. It finds the IP address by consulting with a DNS server.

There are currently two versions of IP in use today - IPv4 and Ipv6.

IPv4 (Internet Protocol version 4) was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available.

IPv6 is intended to replace IPv4, which uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

Back to the top

K

Key Logger

Key logger is a software application or a hardware device that keeps tracks of computer activity in real time including the keys that are pressed. Key loggers are used to troubleshoot technical problems in computer systems. The application can also be used for malicious purposes such as to steal passwords and other sensitive information.

Back to the top

L

LAN

A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology running at 10, 100 or 1,000 Mbit/s (1,000 Mbit/s is also known as 1 Gbit/s).

Back to the top

Leak Test

Leak Test is a way to find out how well your system is protected by your security software from external and internal threats. Typically these tests are down-loadable and should not cause any harm to your system while being run. The Firewall Leak Tests are used to test how effective the firewall component of your security software is at detecting and blocking outgoing connection attempts. If an application is able to connect to the Internet without your knowledge, it poses a real danger meaning it can easily retrieve private and confidential information from your system and transmit it.

Host Intrusion Prevention System (HIPS) tests are designed to test how well your security software is capable of protecting your internal system from malicious attacks such as viruses. A good HIPS system will deny the malware from accessing your critical operating system files, registry keys, COM interfaces and running processes.

Back to the top

License

The official terms of use for a specific program. A software license is a legal document since it formally restricts the rights of the user.

Back to the top

M

MAC Address

A Media Access Control (MAC) address is a number that is hardwired in network adapters and is used to identify the device or system in which it is installed.

Every device on a network has two addresses: a MAC (Media Access Control) address and an IP (Internet Protocol) address. The MAC address is the address of the physical network interface card inside the device, and never changes for the life of the device (in other words, the network card inside the PC has a hard coded MAC address that it keeps even if installed it in a different machine). On the other hand, the IP address can change if the machine moves to another part of the network or the network uses DHCP to assign dynamic IP addresses. In order to correctly route a packet of data from a host to the destination network card it is essential to maintain a record of the correlation between a device's IP address and it's MAC address. The Address Resolution Protocol performs this function by matching an IP address to its appropriate MAC address (and vice versa). The ARP cache is a record of all the IP and MAC addresses that the computer has matched together.

Back to the top

Malicious File

Often called 'Malware', a malicious file is software designed to damage computer systems, steal sensitive information or gain unauthorized access to private computer systems. For example it may be coded to gather sensitive information from a system such as passwords, credit card details and send them back to the creator of the malware.

Back to the top

Malware

Malware is short for 'malicious software'. It is an umbrella term that describes a wide range of malicious software including viruses, trojans, worms, scripts and root kits. When installed on a computer system or network, malware can disrupt operations, steal sensitive and personal information, delete important data, create zombie networks and perform other destructive operations.

Back to the top

N

Network (computer)

Networking is the scientific and engineering discipline concerned with communication between computer systems. Such networks involves at least two computers, which can be separated by a few inches (e.g. via Bluetooth) or thousands of miles (e.g. via the Internet). Computer networking is sometimes considered a sub-discipline of telecommunications.

Back to the top

Network Zone

A Network Zone can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied. The creation of network zones helps an administrator to apply changes for all the computer(s) in selected zone(s).

Back to the top

NIDS

NIDS - Network-Based Intrusion Detection System. Detects intrusions based upon suspicious network traffic. A network intrusion detection system (NIDS) is a system that tries to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic.

Back to the top

NNTP

Network News Transfer Protocol - Refers to the standard protocol used for transferring Usenet news from machine to machine. A protocol is simply a format used to transfer data to two different machines. A protocol will set out terms to indicate what error checking method will be used, how the sending machine will indicate when it is has finished sending the data, and how the receiving machine will indicate that it has received the data.

Back to the top

O

Operating System (OS)

The essential software to control both the hardware and other software of a computer. An operating system's most obvious features are managing files and applications. An OS also manages a computer's connection to a network, if one exists. Microsoft Windows, Macintosh OS, and Linux are operating systems.

Back to the top

P

Ping

Ping is a computer network tool used to test whether a particular host is reachable across an IP network.

Back to the top

PKCS

PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security.

Back to the top

PKCS#7

See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS).

Back to the top

PKCS#10

See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.

Back to the top

PKCS#12

Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

Back to the top

Plugin

A program that allows a Web browser to display a wider range of content than originally intended. For example: the Flash plugin allows Web browsers to display Flash content.

Back to the top

POP2

There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Back to the top

POP3

POP3 is the abbreviation for Post Office Protocol - a data format for delivery of emails across the Internet.

Back to the top

Ports

A computer port is an interface that allows communication between applications or processes running on a host computer and other computers, devices or networks.

Your computer sends and receives data to other computers and to the Internet through a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to Internet using port 80 and port 443. Your e-mail application connects to your mail server through port 25.

Back to the top

Potentially Unwanted Applications

A potentially unwanted application (PUA) is a piece of software that (i) a user may or may not be aware is installed on their computer, and/or (ii) may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. Because of this ambiguity, many antivirus companies use the term 'Potentially Unwanted Application' to identify such software.

Back to the top

Q

Quarantined Files

After an antivirus scan, files that are detected as malware may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any files moved into quarantine are encrypted so they cannot be run or executed. This prevents infected files from corrupting the rest of a computer.

Back to the top

R

Registry Keys

The Windows Registry serves as an archive for collecting and storing the configuration settings of all computer hardware, software and Windows components. Every time an application or hardware is started, it will access the registry keys relating to it. Applications will also access and modify their registry keys constantly during the course of their execution. As the registry is one of the most regularly accessed parts of Windows, it plays a critical role in the stability, reliability and performance of a computer. Indeed, many computer problems are caused by registry errors. Corrupt keys and invalid keys left by uninstalled applications can often cause severe degradation in system performance, crashes and, in extreme cases, can render a system un-bootable. Inexperienced users are, however, discouraged from making manual adjustments to the registry because a single change can have potentially devastating consequences. There are several dedicated registry cleaners available today, including **Comodo PC TuneUp**.

Back to the top

S

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email encapsulated in MIME.

Back to the top

Single User Certificate

A single use certificate refers to the x.509 and associated private key generated by SecureEmail on Alice; stored on SES and downloaded by Bob after a successful SSL client authentication.

Back to the top

SMB

A message format used by DOS and Windows to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include Lan Manager, Windows for Workgroups, Windows NT, and Lan Server. There are also a number of products that use SMB to enable file sharing among different operating system platforms.

Back to the top

SMTP

Simple Mail Transfer Protocol is the most widely used standard for email transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred.

Back to the top

SNMP

Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Back to the top

Spyware

Spyware is a program that performs certain actions without the consent of the user such as displaying advertisements, collecting personal and sensitive information and changing the configuration of the computer. Not all tracking software are malicious since you may have agreed to the conditions as a trade-off for obtaining certain services for free. The tracking software will monitor your online activities to decide what kind of ads should be shown for you.

Back to the top

SSL

Secure Sockets Layer (SSL) is a commonly used protocol for ensuring secure message transmission on the internet. It facilitates an encrypted connection between a web server and an internet browser. It was developed by Netscape in 1994 as a direct response to growing concerns over internet security.

The encryption provided by SSL means that all data passed between a web server and a browser is private and cannot be eavesdropped on. You can tell if you are in an SSL session if the URL begins with https.

SSL is used on the payment pages of millions of websites to protect their online transactions with their customers.

Back to the top

STATIC IP

An IP address which is the same every time you log on to the Internet. See IP for more information.

Back to the top

Stealth Port

Port Stealthing is a security technique whereby ports on an Internet connected PC are hidden so that they provide no response to a remote port scan.

A computer sends and receives data to other computers and to the Internet through an interface called a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, most computers connect to the internet using ports 80 and port 443. Most e-mail applications connect to their mail server through port 25. A 'port scanning' attack consists of sending a message to each port to find out which are open and which are being used by services. With this knowledge, a hacker can determine which attacks are likely to work against a particular

computer. Port stealthing effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt ('closed' ports respond with a 'closed' reply- revealing to the hacker that there is actually a PC in existence).

Back to the top

Stateful Packet Inspection

Stateful Packet Inspection, also known as SPI, is an enhanced firewall technique that uses dynamic packet filtering method over the older method of static packet filtering. SPI scrutinizes the packet contents, monitors traffic and keeps track of the sources of packets. A network administrator can configure the firewall that uses SPI according to the needs of the organization, for example, close ports until requested by legitimate users to open them.

Back to the top

SYN

SYN (synchronize) is a type of packet used by the Transmission Control Protocol (TCP) when initiating a new connection to synchronize the sequence numbers on two connecting computers. The SYN is acknowledged by a SYN/ACK by the responding computer.

Back to the top

T

TCP

TCP stands for Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Back to the top

Token-Ring

LAN technology was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5 by the Institute of Electrical and Electronics Engineers. Initially very successful, it went into steep decline after the introduction of 10BASE-T for **Ethernet** and the EIA/TIA 568 cabling standard in the early 1990s. A fierce marketing effort led by IBM sought to claim better performance and reliability over Ethernet for critical applications due to its deterministic access method, but was no more successful than similar battles in the same era over their Micro Channel architecture. IBM no longer uses or promotes Token-Ring. Madge Networks, a one time competitor to IBM, is now considered to be the market leader in Token Ring.

Back to the top

Trojan

A Trojan is a type of malware that looks like a legitimate piece of software and users are tricked to install and execute in their computers. The malware takes the name from the Greek mythology, Trojan Horse, a wooden horse that was used by the Greeks to infiltrate the city of Troy. Once the malware is activated, it can damage the system, spread other computer viruses and also create a back door so as to allow online fraudsters to take access or control the system.

Back to the top

Trusted Files

In Comodo Internet Security, a trusted file is one that is considered safe and is allowed to run on a user's computer. This type of file can also be referred to as a 'safe' file or a 'white-listed' file.

A file will be treated as safe if it is in the 'Trusted Files' list OR if it is digitally signed by a 'Trusted Software Vendor'. Comodo Internet Security ships with a list of trusted files and a list of Trusted Vendors. Users can add their own trusted files and vendors to their local installation. They can also submit files and vendors to Comodo so they can be considered for inclusion in future safe lists.

Back to the top

Trusted Software Vendor

A Trusted Software Vendor (TSV) is a publisher of software that is automatically trusted by Comodo Internet Security software.

Executable files that have been digitally signed by a TSV will be allowed to run normally and will not be placed in the sandbox.

Many software vendors digitally sign their software with a code signing certificate. Digitally signed software helps a user to identify the publisher and to be sure that the software he/she is downloading is genuine and has not been tampered with. Each code signing certificate is counter-signed by a trusted certificate authority (CA) after the CA has conducted detailed checks that the vendor is a legitimate company.

Back to the top

U

User

A person who uses a computer, including a programmer or **end user**.

Back to the top

V

Virtual Desktop

The Virtual Desktop is a standalone sandbox featured in Comodo Internet Security which allows users to run any applications in a completely virtual environment. Software in the virtual desktop will not affect other processes, programs or data on the user's computer. Similarly, internet browsers running in the virtual desktop leave behind no personally identifying cookies or history on an employee's real system. The virtual desktop also features a virtual keyboard which provides additional security when entering usernames and passwords on website login pages. Although the virtual desktop is primarily intended for users to test unknown or beta software and for launching highly secure browsing sessions, it can be used to run most software. The virtual desktop interface is available in both desktop and tablet optimized versions.

Back to the top

Virtual Machine (VM)

Virtual machine is a software application that emulates a computing environment in which a program or an operating system can be installed and run. There are many advantages in using a VM such as for testing out new applications or procedures without affecting the host system.

Back to the top

Virus

A computer virus is an executable application capable of causing damage to computer files, folders and components. Viruses are also capable of self-replication so can infect multiple items on a system if left unchecked. The malicious activities performed by a virus are wide ranging and include stealing confidential information, modifying user data, overwriting or damaging files and erasing hard disk content.

Back to the top

Viruscope

Viruscope is an innovative subsystem that monitors all the processes running on a computer in real time to find any suspicious actions taken by any of the processes. If a suspicious activity is identified, Viruscope generates an alert. The alert allows the user to quickly block the process, reverse the effects of the action and move the parent application of the process to quarantine, if the activity is found to be malicious, or to allow the process, if the action is found to be legitimate.

Back to the top

Virus Database

A database of the digital signatures of all known computer viruses and malware. This database, sometimes referred to as a 'black list', enables antivirus software to detect any malware running on a customer's computer.

Every time a file or executable is identified as being malware, antivirus companies will create a digital signature of the file and add it to their database of blacklisted files. This database is then distributed to their customers as an update to their antivirus software. If the blacklisted signature of the malware is found anywhere on a customers computer, then the file is flagged as infected and may be quarantined or deleted.

Comodo has a dedicated team of technicians and crawlers that are continually searching for new virus strains to add to our database. Comodo's virus database is available for public download at
http://internetsecurity.comodo.com/updates/vdp/database.php

Back to the top

Vulnerability

In network security, a vulnerability refers to any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network.

Back to the top

W

Website Filtering

Website Filtering is a security technique whereby access to specific websites can be selectively blocked or allowed to particular users of the computer. The website filtering is very useful for parental control as it allows to block inappropriate websites to juvenile users. Also, in work environments, administrators can prevent employees from visiting social networking sites during working hours.

Back to the top

Web server

The term Web server can mean one of two things:

1. A computer that is responsible for accepting **HTTP** requests from clients, which are known as Web browsers, and serving them Web pages, which are usually HTML documents and linked objects (images, etc.).

2. A computer program that provides the functionality described in the first sense of the term.

Back to the top

Worm

A Worm, another type of malware, unlike virus is capable of spreading from computer to computer without any human help. The worm with its capability to replicate itself several times over consumes most of the system memory causing the computer to slow down or crash altogether. It can also cause bandwidth jam while spreading to other computers in the network.

Back to the top

Wildcard

Wildcards are symbols that add flexibility to a keyword search by extending the parameters of a search word. A wildcard item is usually denoted with the asterisk symbol, '*'. This stands for one-or-more characters (useful for all suffixes or prefixes). In digital certification terms, a 'wildcard certificate' means that the certificate will secure the domain plus unlimited sub-domains of that domain. A wildcard certificate is applied for using the format '*.domain.com'.

Back to the top

X

X.509

An internationally recognized standard for certificates that defines their required parts

Back to the top

Z

Zero-Day Malware

Zero-day malware describes new computer viruses or worms that have been discovered in the public realm but which antivirus vendors have not yet created a digital signature for. The term means that the antivirus companies have had 'zero-days' to react. New malware can reasonably be called 'zero-day' for the the length of time between its discovery and the creation of a signature to combat it. For most antivirus vendors, this is usually measured in a matter of hours. Of course, the malware itself may have been at large for a much longer period of time before it was discovered. Because of this window of vulnerability, most security software has grown beyond a reliance on traditional, signature based detection. Most antivirus software now contains layers of prevention-based technologies intended to detect and neutralize 'unknown' malware until such time as a signature can be created. Example technologies include heuristic detection, host intrusion prevention (HIPS), automatic sandboxing and real-time behavior analysis.

Back to the top

Appendix 4 - CIS Versions

Comodo Internet Security is available in three versions - Premium (free), Pro and Complete. The Pro version includes **Comodo GeekBuddy** (Comodo support experts available 24/7 to fix any problem with your computer) and the Virus Free Guarantee (if your computer becomes damaged as a result of malware and Comodo support services cannot return it to a working condition then we'll pay the costs of getting it repaired. Please see the **End User License Agreement** for full details). CIS Complete includes GeekBuddy, the Virus Free Guarantee, **TrustConnect** (a secure Internet proxy service that ensures 128 bit encrypted connectivity from any public wireless hotspot) and a Comodo Online Backup account (50GB of online storage space).

Product	Includes							Price*
	Antivirus	Firewall	GeekBuddy	TrustConnect	Online Storage	Protection Plan Virus Free Guarantee (VFG) / Identity Protection (IDP)	Virus Removal Service	
CIS Premium 8.x	✓	✓	✓	✗	✗	✗	✗	Free
CIS Pro 8.x	✓	✓	✓	✗	✗	✓	✓	$39.99/year or $3.99/month
CIS Complete 8.x	✓	✓	✓	✓ (10 GB / Month)	✓ (50 GB Free. Upgrades available)	✓	✓	$89.99/year or $8.99/month
CAV Free	✓	✗	✗	✗	✗	✗	✗	Free
CAV Advanced	✓	✗	✗	✗	✗	✗	✓	$19.99/year or $3.49/month
Comodo Firewall	✗	✓	✗	✗	✗	✗	✗	Free

* Most CIS products also have discounts for multi-year purchases.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **http://www.comodo.com.**