

COMODO
Creating Trust Online®



Comodo Internet Security 2013

Software Version 6.0

User Guide
Guide Version 6.0.052113

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ, 07013
United States

Table of Contents

1.Introduction to Comodo Internet Security.....	6
1.1.Special Features.....	10
1.2.System Requirements.....	13
1.3.Installation.....	13
1.3.1.CIS Premium - Installation.....	14
1.3.2.CIS Pro - Installation and Activation.....	24
1.3.3.CIS Complete - Installation and Activation.....	36
1.3.3.1.Installing Comodo Internet Security Complete 2013.....	38
1.3.3.2.Activating Online Backup, TrustConnect and Guarantee.....	49
1.3.3.3.Installing Comodo Backup.....	54
1.3.3.4.Installing Comodo TrustConnect	59
1.3.4.Activating CIS Pro/Complete Services after Installation.....	65
1.3.4.1.Activating Your License.....	66
1.3.4.2.Activating Your Guarantee Coverage.....	69
1.3.4.3.Renewal of Your License.....	74
1.4.Starting Comodo Internet Security.....	74
1.5.The Main Interface	76
1.5.1.The Home Screen.....	76
1.5.2.The Tasks Interface.....	80
1.5.3.The Widget.....	80
1.5.4.The System Tray Icon.....	81
1.6.Understanding Security Alerts.....	83
2.General Tasks - Introduction.....	96
2.1.Scan and Clean Your Computer.....	97
2.1.1.Run a Quick Scan	98
2.1.2.Run a Full Computer Scan.....	103
2.1.3.Run a Rating Scan.....	108
2.1.4.Run a Custom Scan.....	111
2.1.4.1.Scan a Folder	112
2.1.4.2.Scan a File	115
2.1.4.3.Create, Schedule and Run a Custom Scan	118
2.2.Instantly Scan Files and Folders.....	127
2.3.Processing Infected Files.....	130
2.4.Manage Virus Database and Program Updates.....	137
2.5.Manage Quarantined Items.....	140
2.6.View CIS Logs.....	144
2.6.1.Antivirus Logs.....	146
2.6.1.1.Filtering Antivirus Logs.....	147
2.6.2.Firewall Logs.....	150
2.6.2.1.Filtering Firewall Logs.....	152
2.6.3.Defense+ Logs.....	157
2.6.3.1.Filtering Defense+ Logs	158
2.6.4.'Alerts' Logs.....	161
2.6.4.1.Filtering 'Alerts Displayed' Logs.....	163

2.6.5.Tasks.....	168
2.6.5.1.Filtering 'Tasks Launched' Logs.....	169
2.6.6.Configuration Changes.....	172
2.6.6.1.Filtering 'Configuration Changes' Logs.....	173
2.7.Manage CIS Tasks.....	177
2.8.View Active Internet Connections.....	182
3.Firewall Tasks - Introduction.....	187
3.1.Allow or Block Internet Access to Applications Selectively	188
3.2.Stealth your Computer Ports	190
3.3.Manage Network Connections.....	191
3.4.Stop all Network Activities.....	192
3.5.Advanced Firewall Settings.....	192
4.Sandbox Tasks - An Introduction	194
4.1.The Virtual Kiosk.....	194
4.1.1.Starting the Virtual Kiosk.....	195
4.1.2.The Main Interface.....	196
4.1.3.Running Browsers inside the Virtual Kiosk.....	199
4.1.4.Opening Files and Running Applications inside the Virtual Kiosk.....	201
4.1.5.Configuring the Virtual Kiosk.....	201
4.1.6.Closing the Virtual Kiosk.....	203
4.2.Run an Application in the Sandbox	203
4.3.Reset the Sandbox.....	208
5.Advanced Tasks - An Introduction	210
5.1.Create a Rescue Disk	211
5.1.1.Downloading and Burning Comodo Rescue Disk.....	212
5.2.Remove Deeply Hidden Malware	217
5.3.Submit Files.....	220
5.4.Identify and Kill Unsafe Running Processes.....	223
6.Advanced Settings.....	226
6.1.General Settings.....	227
6.1.1.Customize User Interface.....	228
6.1.2.Configure Program and Virus Database Updates.....	232
6.1.3.Log Settings.....	235
6.1.4.Manage CIS Configurations.....	236
6.1.4.1.Comodo Preset Configurations.....	237
6.1.4.2.Importing/Exporting and Managing Personal Configurations.....	238
6.2.Security Settings.....	244
6.2.1.Antivirus Settings.....	246
6.2.1.1.Real-time Scanner Settings.....	246
6.2.1.2.Scan Profiles.....	249
6.2.1.3.Exclusions.....	257
6.2.2.Defense+ Settings.....	269
6.2.2.1.HIPS Behavior Settings.....	270
6.2.2.2.Active HIPS Rules.....	276
6.2.2.3.HIPS Rule Sets.....	285
6.2.2.4.Protected Files and Folders.....	288

6.2.2.4.1.Protected Files.....	289
6.2.2.4.2.Blocked Files.....	296
6.2.2.5.Protected Registry Keys.....	298
6.2.2.6.Protected COM interfaces.....	303
6.2.2.7.Behavior Blocker.....	308
6.2.2.7.1.The Sandbox - An Overview.....	314
6.2.2.7.2.Unknown Files: The Auto-Sandboxing and Scanning Processes.....	314
6.2.2.8.Configure the Sandbox.....	316
6.2.3.Firewall Settings.....	322
6.2.3.1.Firewall Behavior Settings.....	323
6.2.3.2.Application Rules.....	329
6.2.3.3.Global Rules.....	341
6.2.3.4.Firewall Rule Sets.....	343
6.2.3.5.Network Zones.....	345
6.2.3.5.1.Network Zones.....	346
6.2.3.5.2.Blocked Zones.....	351
6.2.3.6.Port Sets.....	354
6.2.4.Manage File Rating.....	357
6.2.4.1.File Rating Settings.....	358
6.2.4.2.Trusted Files.....	359
6.2.4.3.Unrecognized Files.....	362
6.2.4.4.Submitted Files.....	366
6.2.4.5.Trusted Vendors List.....	367
7.Comodo GeekBuddy.....	373
7.1.Overview of Services.....	374
7.2.Activation of Service.....	374
7.3.Launching the Client and Using the Service.....	377
7.4.Accepting Remote Desktop Requests.....	380
7.5.Chat History.....	383
7.6.Starting and Using AntiError.....	384
7.7.Uninstalling Comodo GeekBuddy.....	389
8.TrustConnect Overview.....	390
8.1.Microsoft Windows - Configuration and Connection.....	392
8.2.Mac OS X - Configuration and Connection.....	395
8.3.Linux / Open VPN - Configuration and Connection.....	395
8.4.Apple iPhone / iPod Touch - Configuration and Connection.....	397
8.5.Android Devices - Configuration and Connection.....	398
8.6.Windows Mobile Devices - Configuration and Connection.....	405
8.7.TrustConnect FAQ.....	413
9.Comodo Dragon.....	419
Appendix 1 - CIS How to... Tutorials.....	422
Enabling / Disabling AV, Firewall and Behavior Blocker Easily.....	423
Setting up the Firewall For Maximum Security and Usability.....	424
Blocking Internet Access while Allowing Local Area Network (LAN) Access.....	432
Setting up the HIPS for Maximum Security and Usability.....	438
Setting up the Behavior Blocker for Maximum Security and Usability.....	441

Password Protect Your CIS Settings	442
Reset Forgotten Password (Advanced).....	444
Running an Instant Antivirus Scan on Selected Items.....	447
Creating an Antivirus Scanning Schedule.....	449
Running Untrusted Programs In the Sandbox.....	455
Running Browsers inside Sandbox.....	460
Running Untrusted Programs Inside Virtual Kiosk.....	461
Running Browsers Inside the Virtual Kiosk.....	463
Restoring Incorrectly Quarantined Item(s).....	465
Submitting Quarantined Items to Comodo for Analysis.....	466
Enabling File Sharing Applications like BitTorrent and Emule.....	468
Blocking any Downloads of a Specific File Type.....	474
Disabling Behavior Blocker and Auto-Sandboxing on a per-application basis	477
Enabling Full Virtualization for Auto-Sandboxed Applications (Advanced).....	480
Switching Between Complete CIS Suite and Individual Components (just AV or FW).....	484
Switch Off Automatic Antivirus and Software Updates.....	488
Suppressing CIS Alerts Temporarily while Playing Games.....	492
Renewing or Upgrading your License.....	493
Appendix 2 - Comodo Secure DNS Service.....	496
Router - Manually Enabling or Disabling Comodo Secure DNS Service.....	496
Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service.....	498
Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service.....	502
Appendix 3 - CIS Versions.....	508
About Comodo.....	509

1. Introduction to Comodo Internet Security

Overview

Comodo Internet Security 6.0 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. See '[CIS Versions](#)' for further information. 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 6.0 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.
 - **Behavior Blocker** - 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.
- **Virtual Kiosk** - New to CIS 6.0, the Virtual Kiosk 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 kiosk 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
- **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.
- **Comodo Dragon** - Fast and versatile Internet Browser based on Chromium, infused with Comodo's unparalleled level of Security.
- **GeekBuddy** (*Pro and Complete versions only*) - 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 we'll 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 be accessed only by the user from any Internet connected computer in the world (10GB 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 next four sections of the guide cover every aspect of the configuration of Comodo Internet Security.

- **General Tasks - Introduction**
 - **Scan and Clean your Computer**
 - **Run a Quick Scan**
 - **Run a Full Computer Scan**
 - **Run a Rating Scan**
 - **Run a Custom Scan**

- Instantly Scan Files and Folders
- Processing Infected Files
- Manage Virus Database and Program Updates
- Manage Quarantined Items
- View CIS Logs
- Manage CIS Tasks
- View Active Internet Connections
- Firewall Tasks - Introduction
 - Allow or Block Internet Access to applications Selectively
 - Stealth your Computer Ports
 - Manage Network Connections
 - Stop all Network Activities
 - Advanced Firewall Settings
- Sandbox Tasks - An Introduction
 - The Virtual Kiosk
 - Starting the Virtual Kiosk
 - The Main Interface
 - Running Browsers inside the Virtual Kiosk
 - Opening Files and Running Applications inside Virtual Kiosk
 - Configuring the Virtual Kiosk
 - Closing the Virtual Kiosk
 - Run an Application in the Sandbox
 - Reset the Sandbox
- Advanced Tasks - An Introduction
 - Create a Rescue Disk
 - Downloading and Burning Comodo Rescue Disk
 - Remove Deeply Hidden Malware
 - Submit Files
 - Identify and Kill Unsafe Running Processes
- Advanced Settings
 - General Settings
 - Customize User Interface
 - Configure Program and Virus Database Updates
 - Log Settings
 - Manage CIS Configurations
 - Security Settings
 - Antivirus Settings
 - Real-time Scanner Settings
 - Scan Profiles
 - Exclusions
 - Defense+ Settings
 - HIPS Behavior Settings
 - Active HIPS Rules
 - HIPS Rule Sets
 - Protected Files and Folders

- Protected Registry Keys
- Protected COM interfaces
- Behavior Blocker
 - The Sandbox - An Overview
 - Unknown Files: The Sand-boxing and Scanning Processes
- Configure the Sandbox
- Firewall Settings
 - Firewall Behavior Settings
 - Application Rules
 - Global Rules
 - Firewall Rule Sets
 - Network Zones
 - Port Sets
- Manage File Rating
 - File Rating Settings
 - Trusted Files
 - Unrecognized Files
 - Submitted Files
 - Trusted Vendors List

The final sections contain configuration and technical help for **GeekBuddy** and **TrustConnect**.

- **Comodo GeekBuddy**
 - Overview of Services
 - Activation of Service
 - Launching the Client and Using the Service
 - Accepting Remote Desktop Requests
 - Chat History
 - Starting and Using AntiError
 - Uninstalling Comodo GeekBuddy
- **TrustConnect Overview**
 - Microsoft Windows - Configuration and Connection
 - Mac OS X - Configuration and Connection
 - Linux / Open VPN - Configuration and Connection
 - Apple iPhone / iPod Touch - Configuration and Connection
 - Android Devices - Configuration and Connection
 - Windows Mobile Devices - Configuration and Connection
 - TrustConnect FAQ
- **Comodo Dragon**
- **Appendix 1 - CIS How to... Tutorials**
 - Enabling / Disabling AV, Firewall and Behavior Blocker Easily
 - Setting up the Firewall For Maximum Security and Usability
 - Blocking Internet Access while Allowing Local Area Network (LAN) Access
 - Setting up the HIPS for Maximum Security and Usability
 - Setting up the Behavior Blocker for Maximum Security and Usability
 - Password Protect Your CIS Settings
 - Reset Forgotten Password (Advanced)

- [Running an Instant Antivirus Scan on Selected Items](#)
- [Creating an Antivirus Scanning Schedule](#)
- [Running Untrusted Programs In the Sandbox](#)
- [Running Browsers inside Sandbox](#)
- [Running Untrusted Programs Inside Virtual Kiosk](#)
- [Running Browsers Inside the Virtual Kiosk](#)
- [Restoring Incorrectly Quarantined Item\(s\)](#)
- [Submitting Quarantined Items to Comodo for Analysis](#)
- [Enabling File Sharing Applications like BitTorrent and Emule](#)
- [Blocking any Downloads of a Specific File Type](#)
- [Disabling Behavior Blocker and Auto-Sandboxing on a per-application basis](#)
- [Enabling Full Virtualization for Auto-Sandboxed Applications \(Advanced\)](#)
- [Switching Between Complete CIS Suite and Individual Components \(just AV or FW\)](#)
- [Switch Off Automatic Antivirus and Software Updates](#)
- [Suppressing CIS Alerts Temporarily while Playing Games](#)
- [Renewing or upgrading your License](#)
- [Appendix 2 - Comodo Secure DNS Service](#)
- [Appendix 3 - CIS Versions](#)

1.1. Special Features

Behavior Blocker

- 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
- Includes auto-sandbox feature to completely isolate untrusted files from the rest of your computer

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 Kiosk

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

Comprehensive Antivirus Protection

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

Intuitive Graphical User Interface

- Summary screen gives an at-a-glance snapshot of your security settings;
- Easy and quick navigation between each 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 Dragon

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

- Improved Privacy over Chromium
- Easy SSL Certificate Identification
- Fast Website Access
- Greater Stability and Less Memory Bloat
- Incognito Mode Stops Cookies, Improves Privacy
- Very easy to switch from your Browser to the Dragon

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.

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

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, TrustConnect, 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 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>.

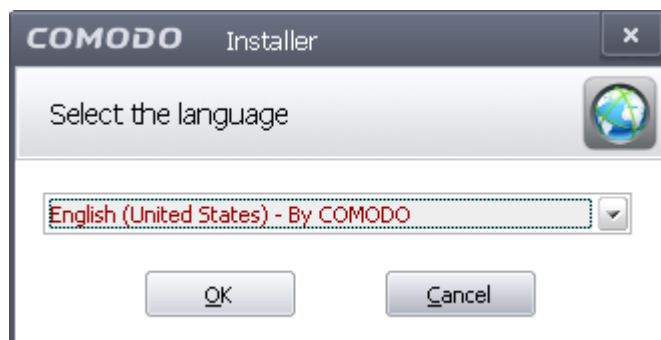
- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and 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. Please note, Comodo TrustConnect (secure wireless connectivity service) will be installed along with CIS. With TrustConnect installed, you are automatically warned whenever CIS detects that you have joined an unsecured/public wireless network. TrustConnect then offers you the opportunity to activate/login to your account and therefore secure the connection.

Step 1 - Choosing the Interface Language

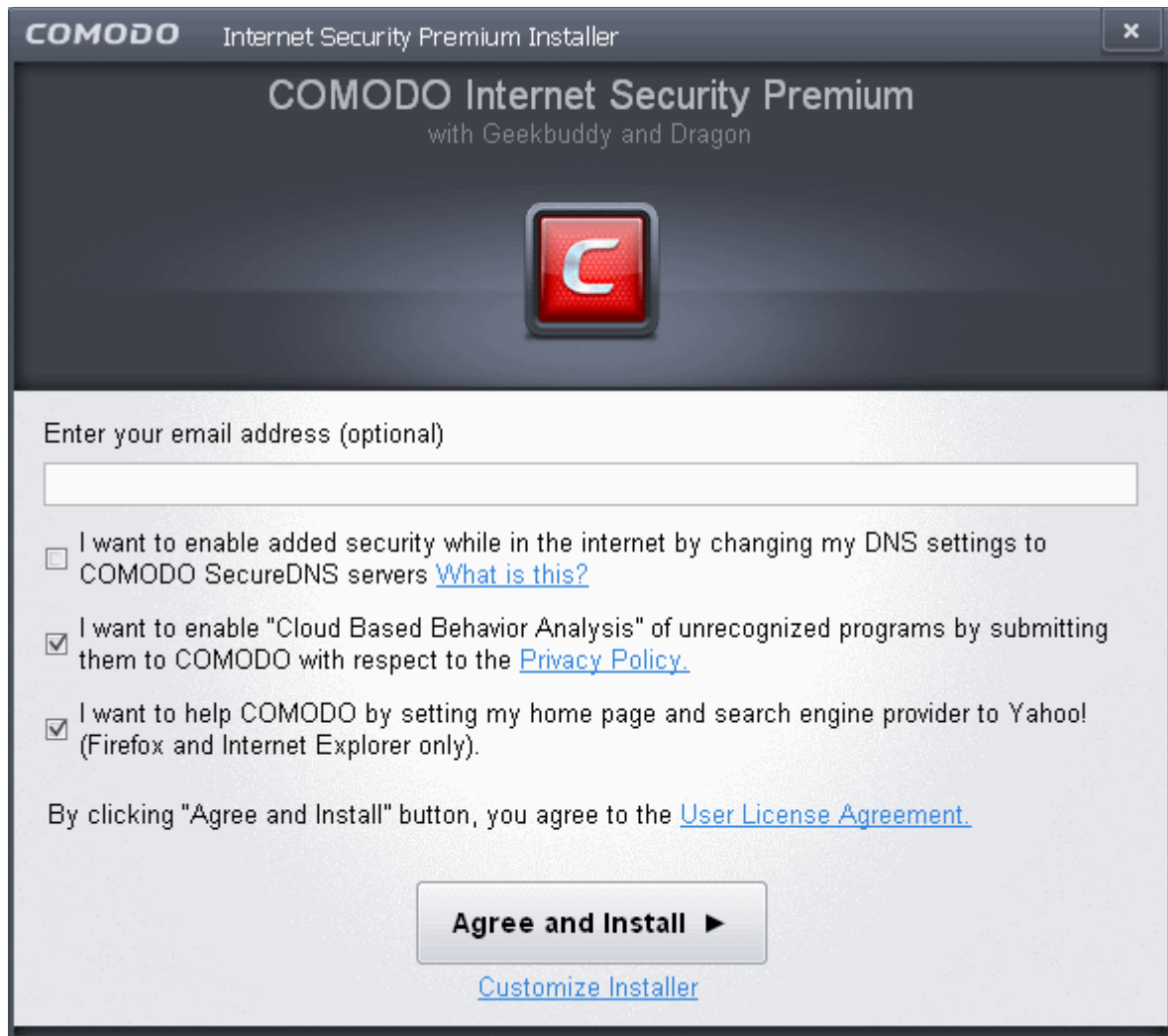
The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



- 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.



- Please review and/or modify the settings in the dialog. Once you are satisfied with your settings, click 'Agree and Install' to **begin installation**.
- If you click 'Customize Installer' 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.

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.

Cloud Based Behavior Analysis

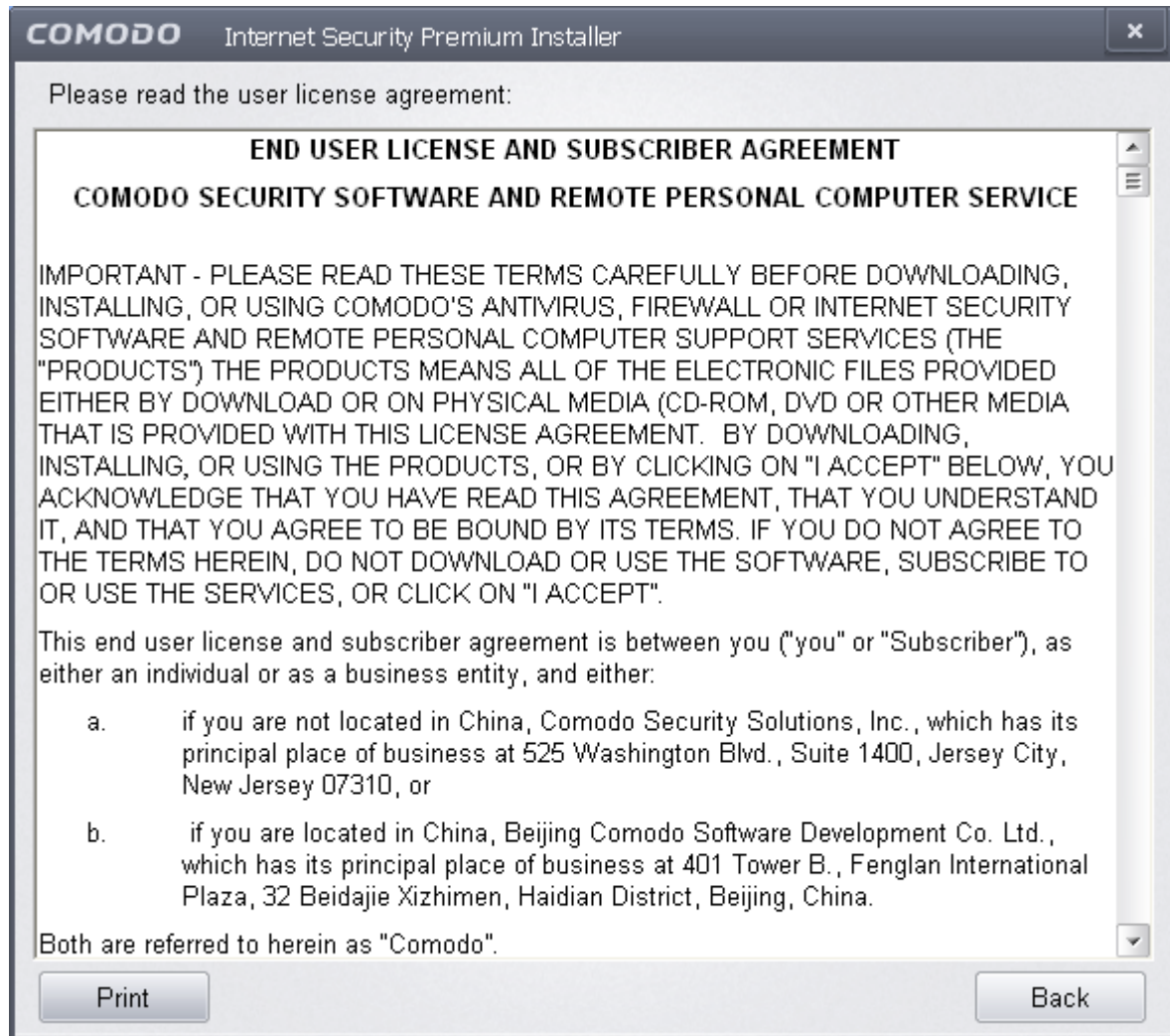
Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Browser Homepage

Your default home page and search engine will be set to Yahoo!

End User License Agreement

Read the complete User License Agreement by clicking the 'User License Agreement' link before proceeding with the installation.



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

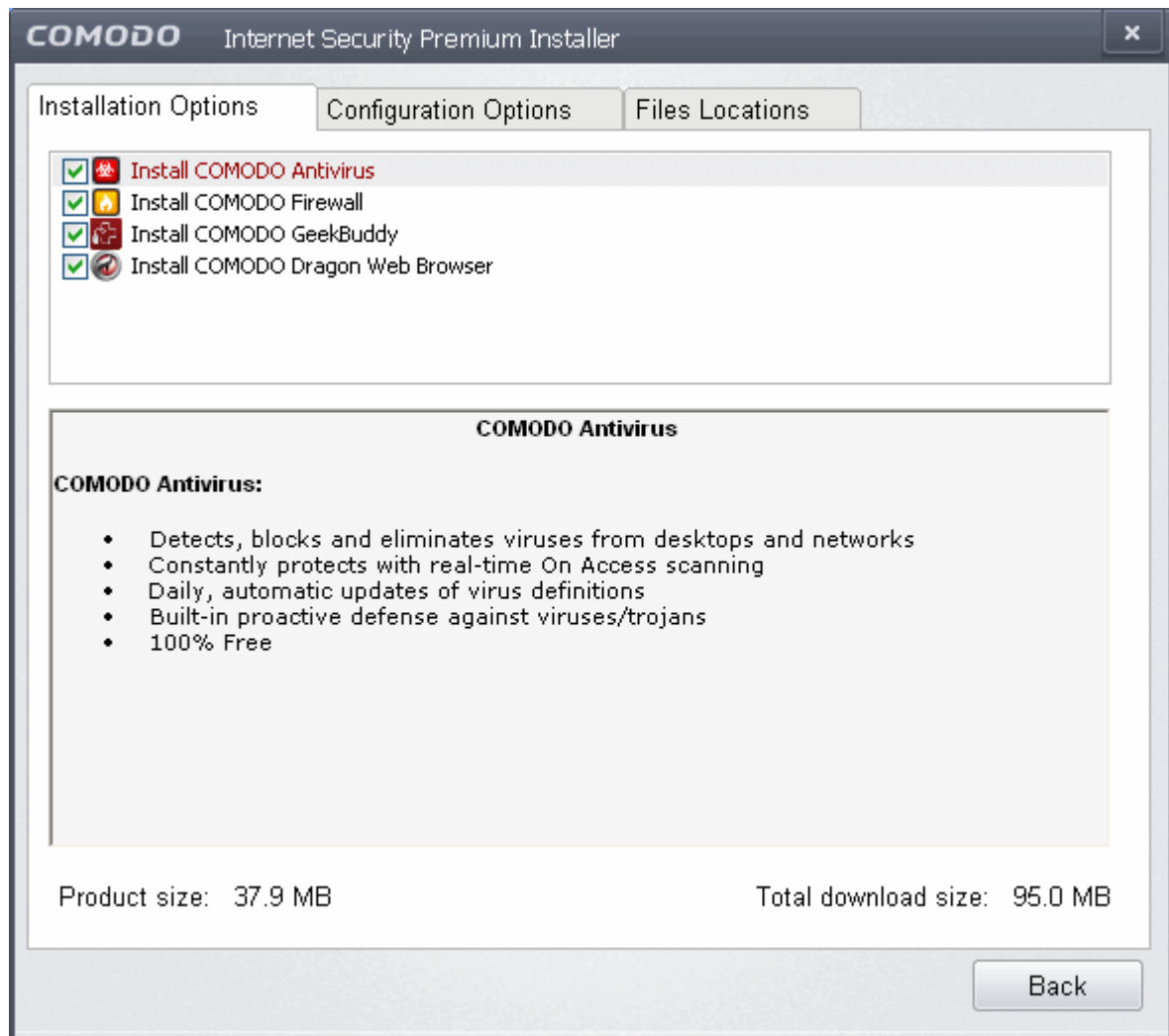
Once back at the main installer screen, if you wish to configure advanced options, click '[Customize Installer](#)'. Otherwise, click 'Agree and Install' to [begin installation](#).

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 full benefit of the product.

Select Components to Install ([Click to go back to Step 2](#))

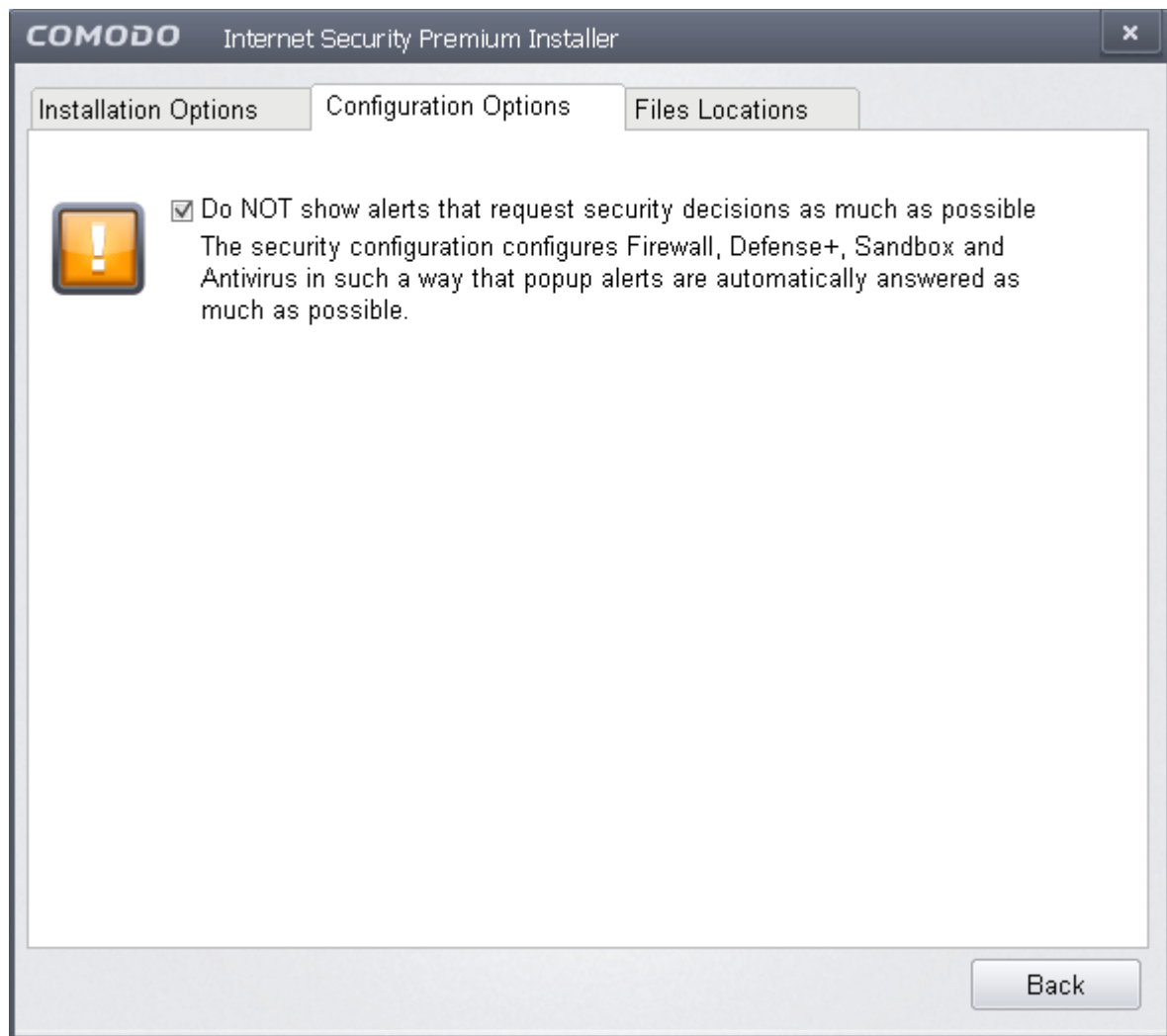
Click the 'Installation Options' tab to select the components to be installed.



- **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 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 COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section **Comodo Dragon** for more details.

Configuration Options

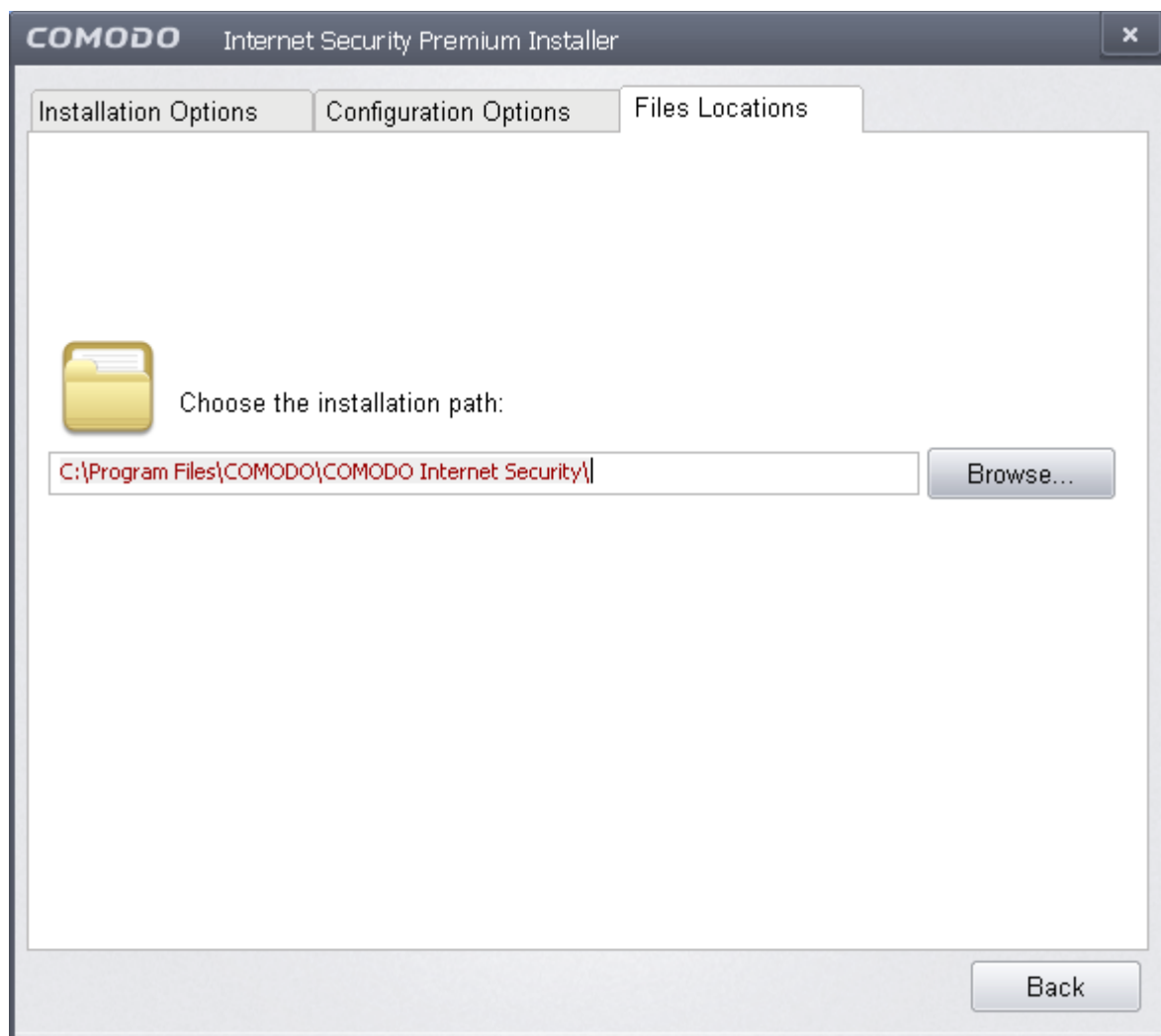
Click the 'Configuration Options' tab to configure pop-up alert options.



- **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.

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

Step 3 - Installation Progress [\(Click to go back to Step 2\)](#)

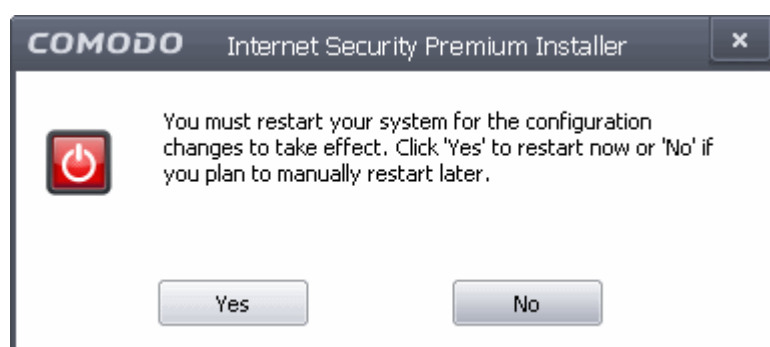
The installation progress will be displayed...



...and on completion, the restart dialog will be displayed.

Step 4 - Restarting Your System

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



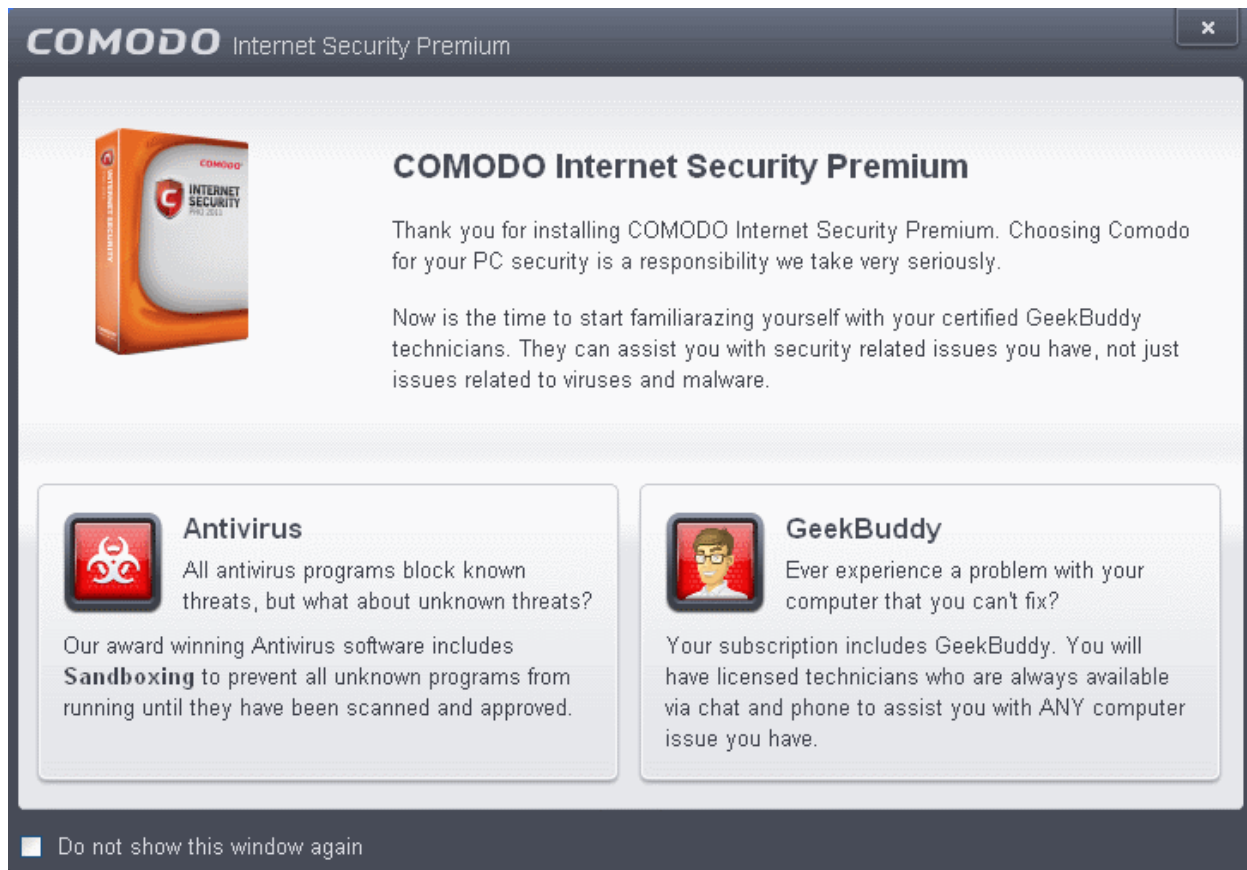
Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

Step 5 - After Restarting Your System

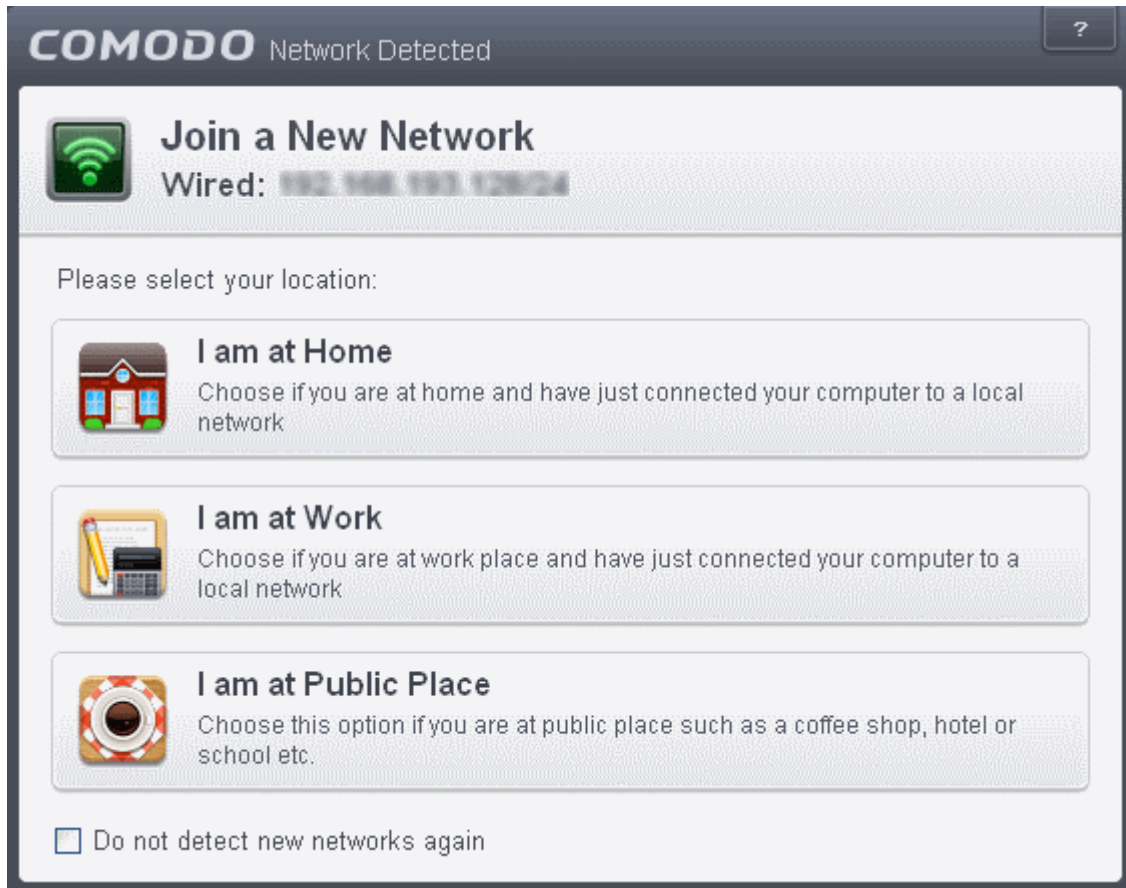
After restarting, a 'thankyou' screen will appear. This contains a summary of the components you chose to install as well as

some friendly advice.



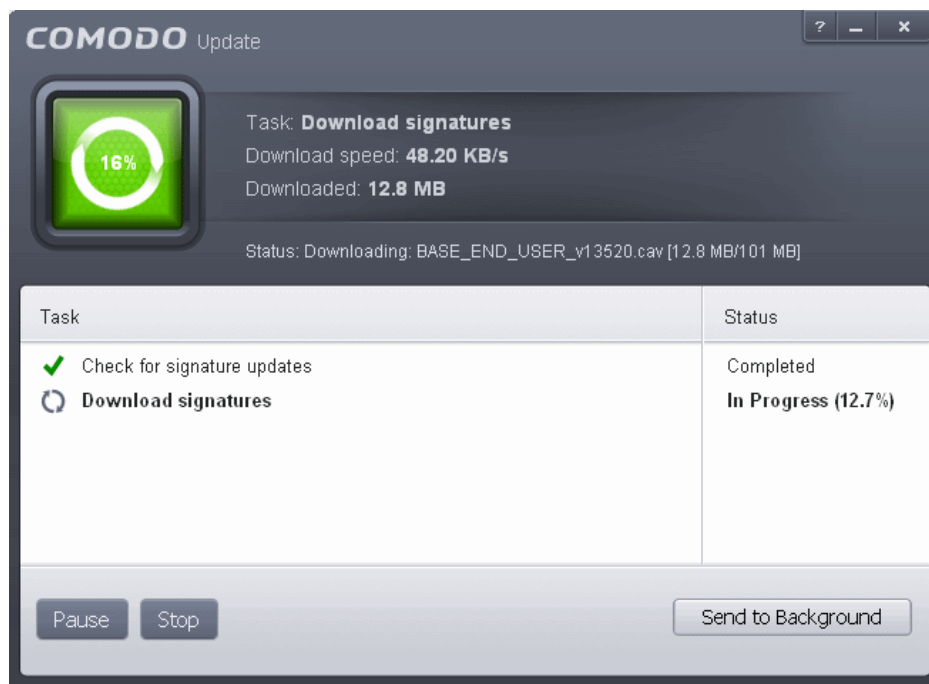
This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

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



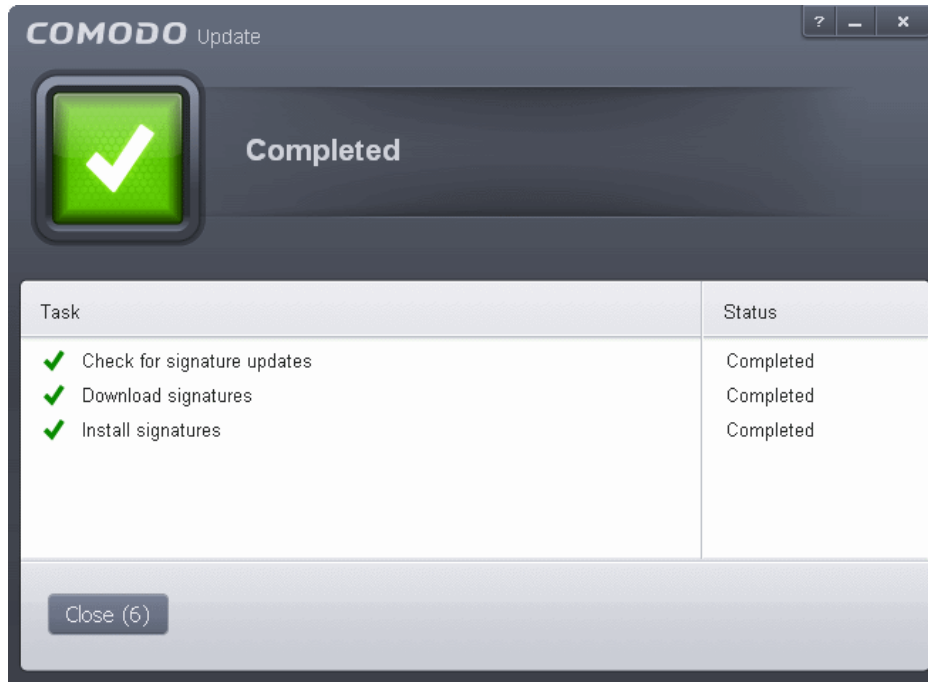
- Select your location from the three options above
- Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in **'Network Zones'** and through the **'Stealth Ports Wizard'**)

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

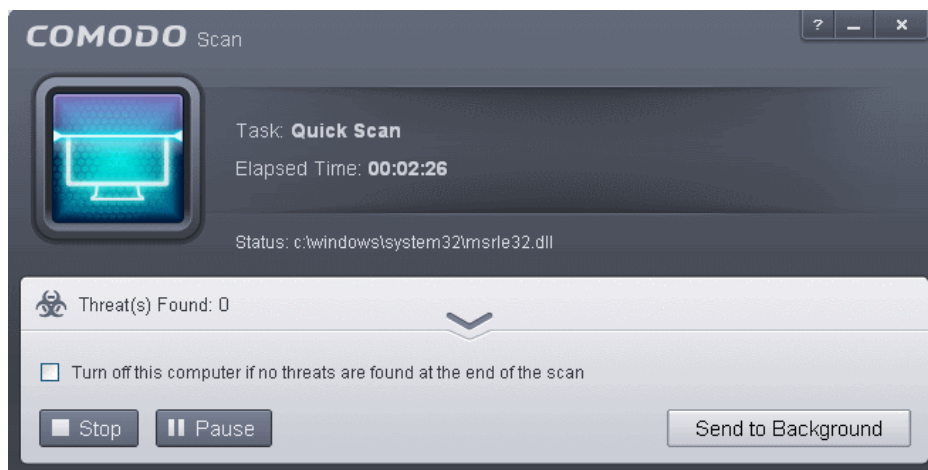


The screen will display details such as download speed, how much has been downloaded and the progress of the process. You

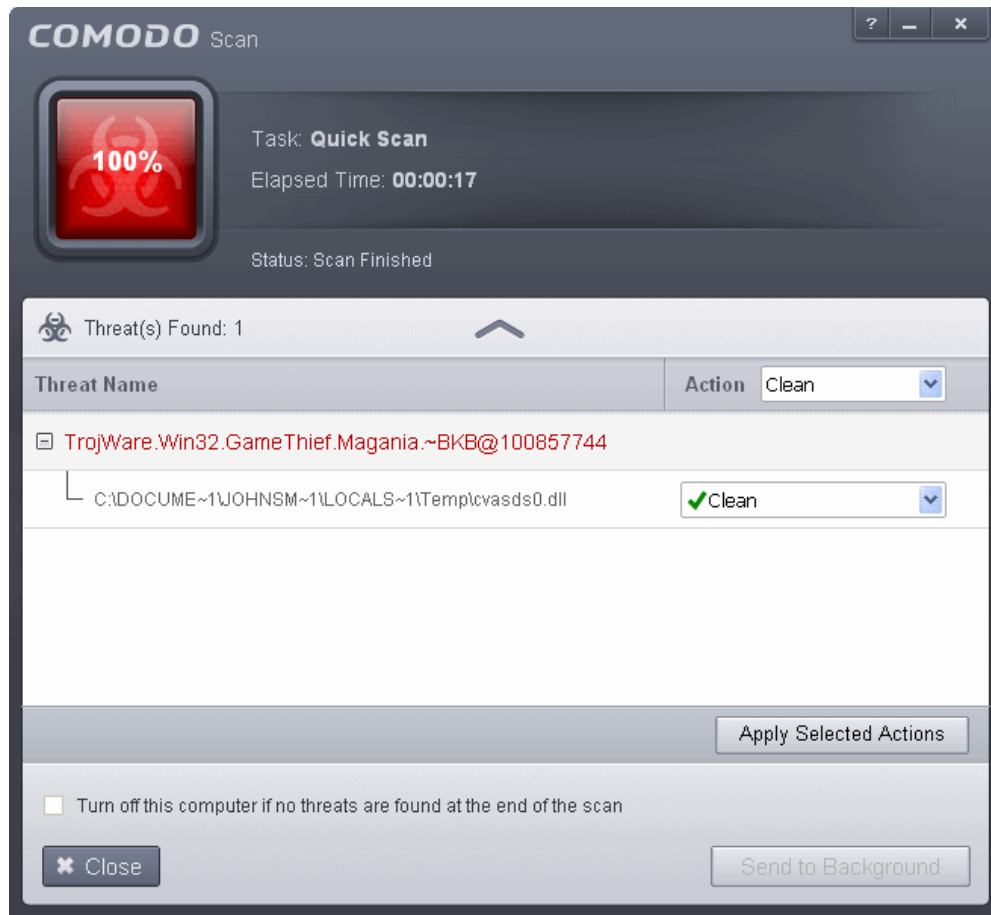
can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '**Manage CIS Tasks**' for more details. When the virus database has been downloaded, the 'Completed' dialog will be displayed.



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 Scan' button. After the scanning is complete, the results screen will be displayed.



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.

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.

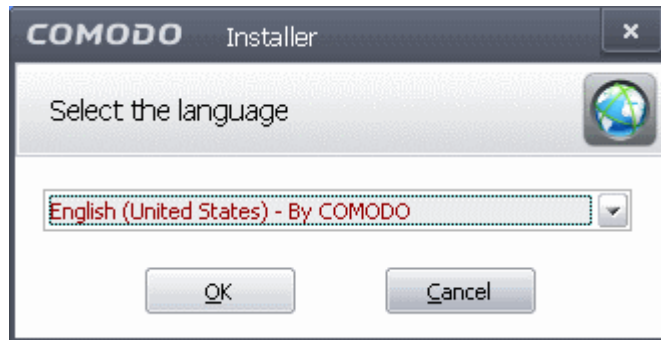
Comodo Internet Security Pro 2013 can be downloaded from <http://www.comodo.com/home/download/download.php?prod=cis-pro> after signing up for subscription and includes, **Comodo Dragon**, **GeekBuddy** and the **Comodo Guarantee**.

- 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. With TrustConnect installed, you are automatically warned whenever CIS Pro detects that you have joined an unsecured/public wireless network and offered the opportunity to login to your account.

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 - Validating Your License and Installation Configuration

The next step is entering the License key and configuring the installation. You should have received your License key through email.



Tip: If you don't have the subscription key handy at the time of installation, you can activate your subscription and guarantee at a later time from the main interface of CIS. For more details refer to **Activating your CIS Pro and CIS Complete Services after Installation**.

- Please review and/or modify the settings in the dialog. Once you are satisfied with your settings, click 'Agree and

Install' to **begin installation**.

- If you click 'Customize Installer' 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.

Cloud Based Behavior Analysis

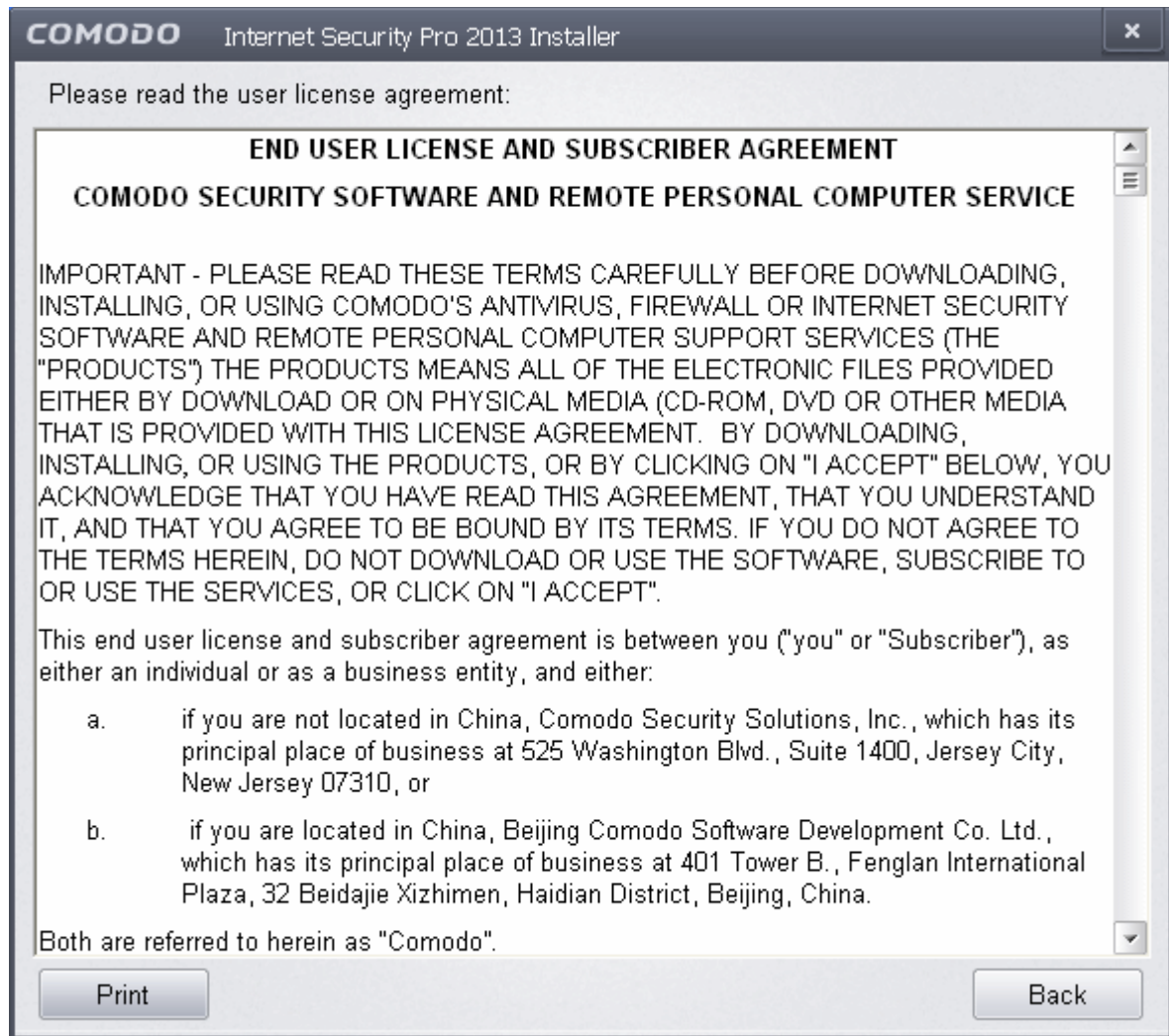
Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Browser Homepage

Your default browser home page and the search engine will be set as Yahoo!

End User License Agreement

Read the complete User License Agreement by clicking the 'User License Agreement' link before proceeding with the installation.



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

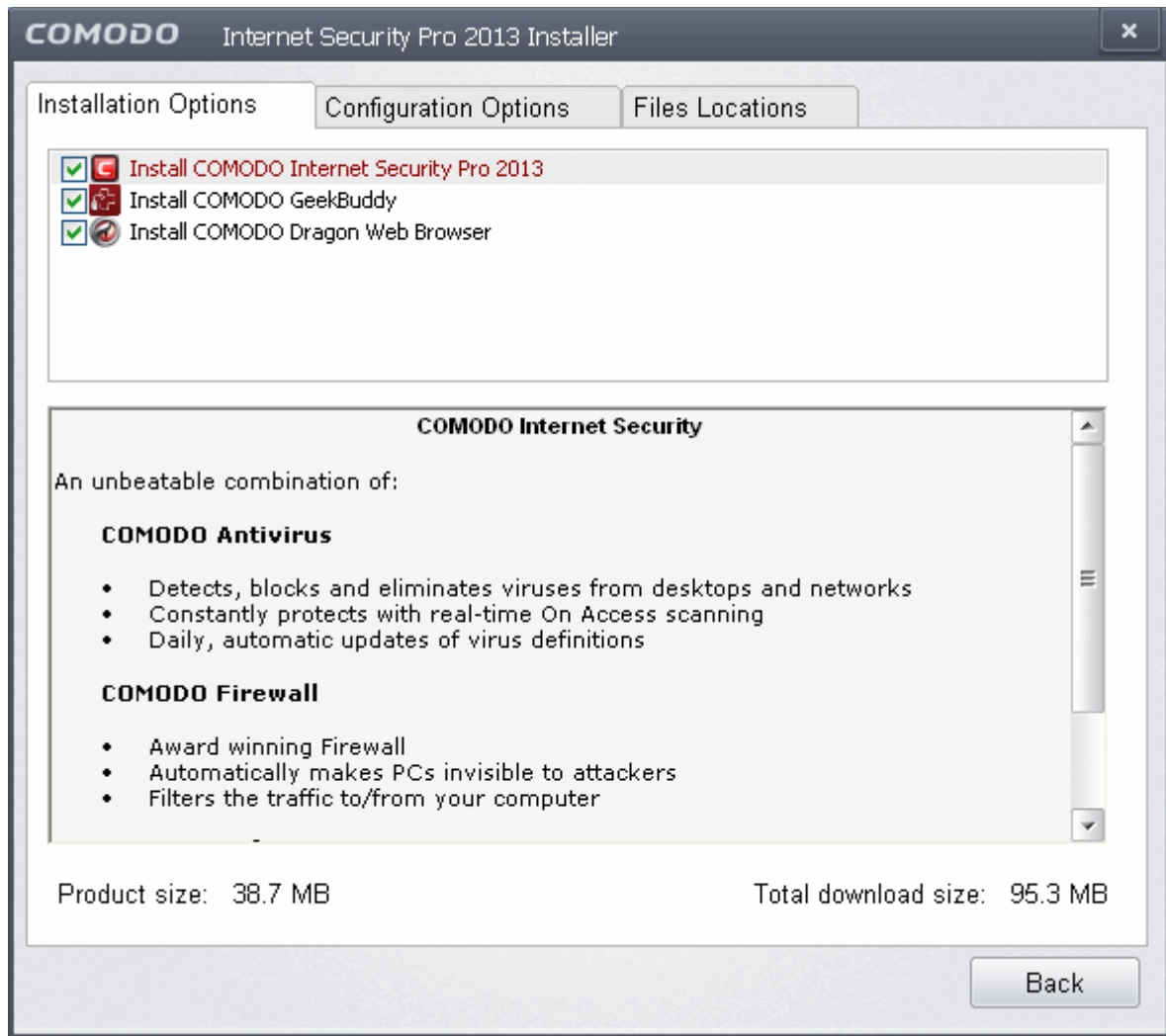
Once back at the main installer screen, if you wish to configure advanced options, click '[Customize Installer](#)'. Otherwise, click 'Agree and Install' to [begin installation](#).

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](#))

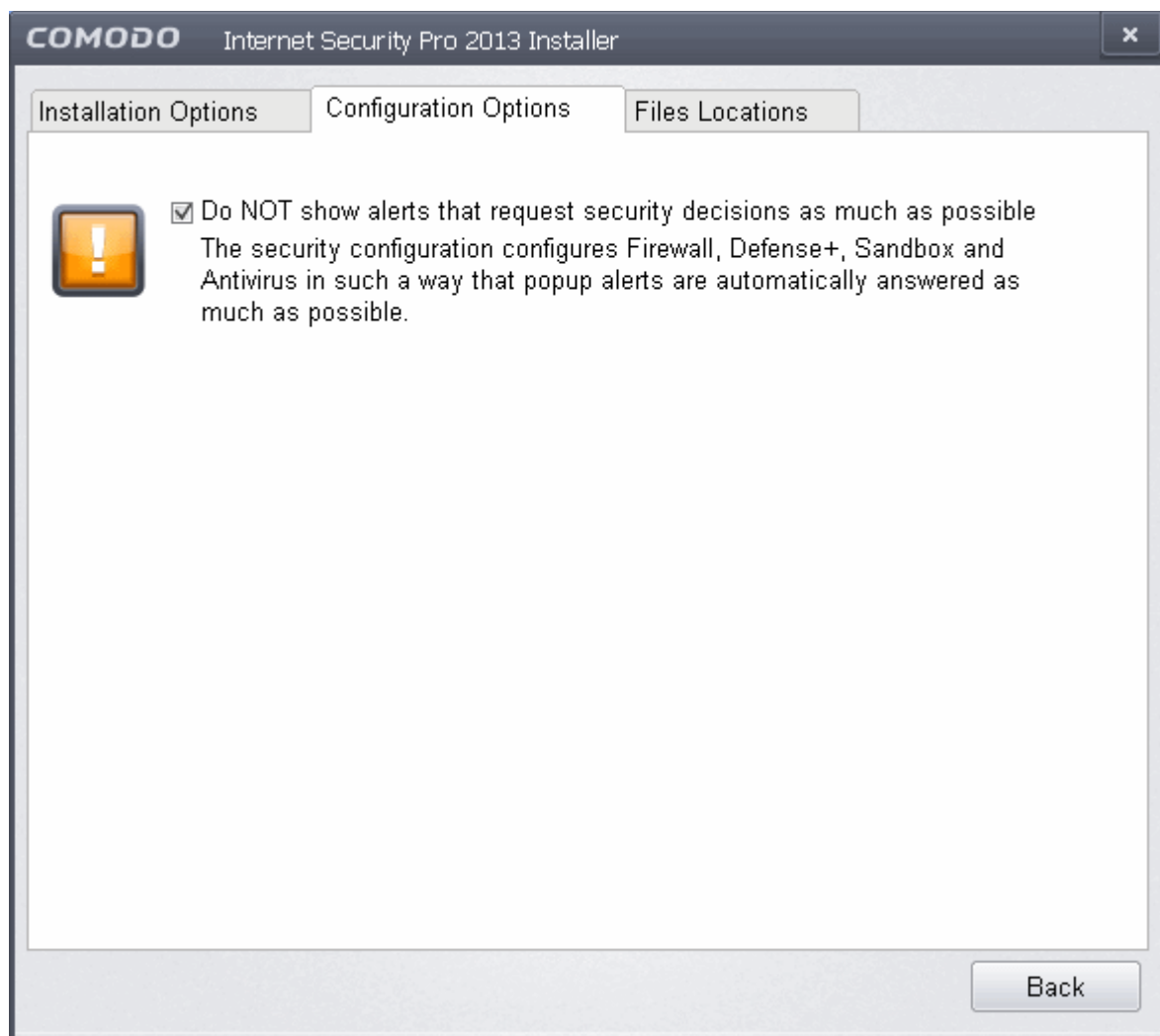
Click the 'Installation Options' tab to select the components to be installed.



- **Install COMODO Internet Security Pro 2013** - Selecting this option installs Comodo Antivirus, Comodo Firewall and Defense+ components. Installing CIS Pro 2013 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 COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section [Comodo Dragon](#) for more details.

Configuration Options

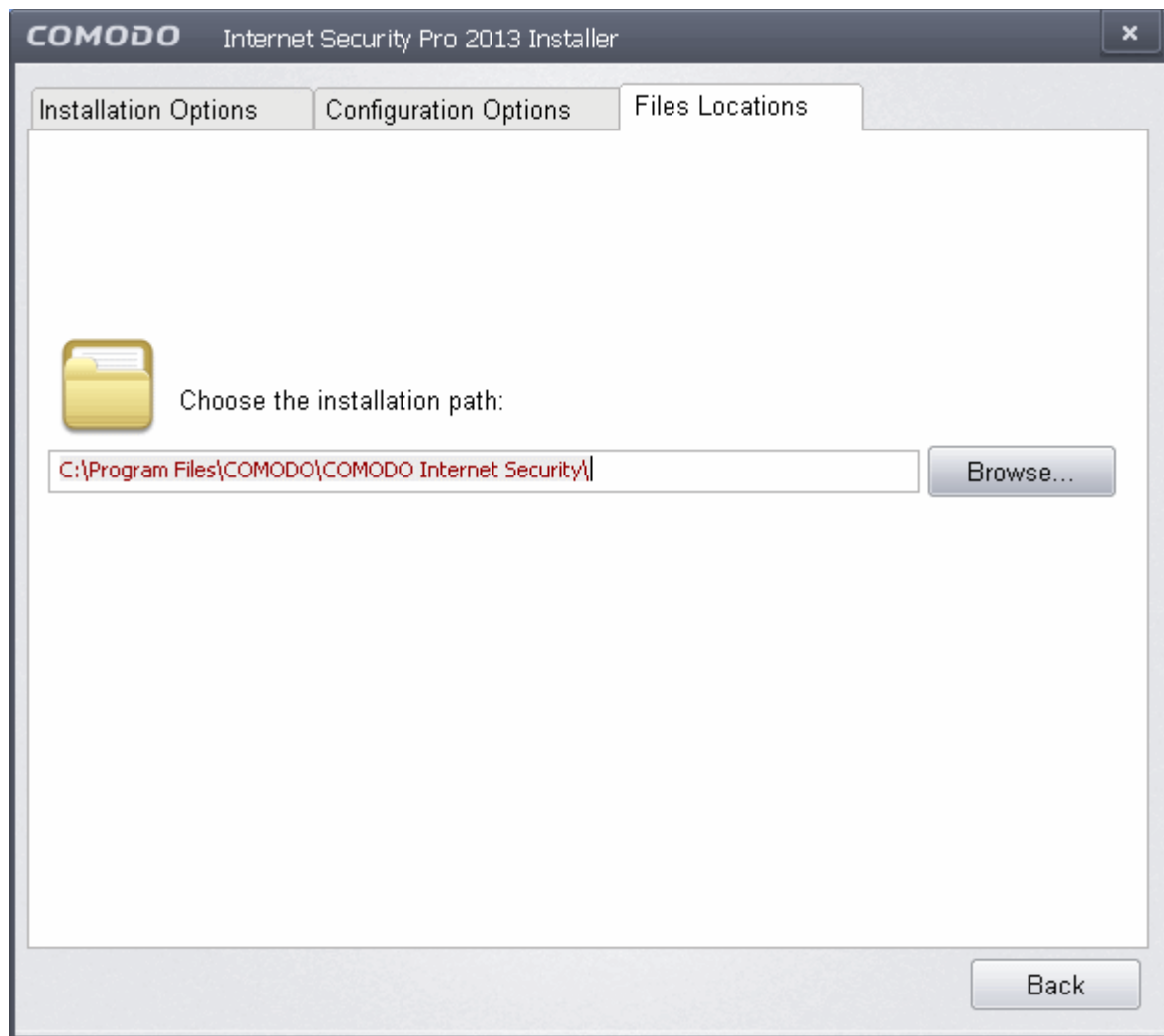
Click the 'Configuration Options' tab to configure pop-up alert options.



- **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.

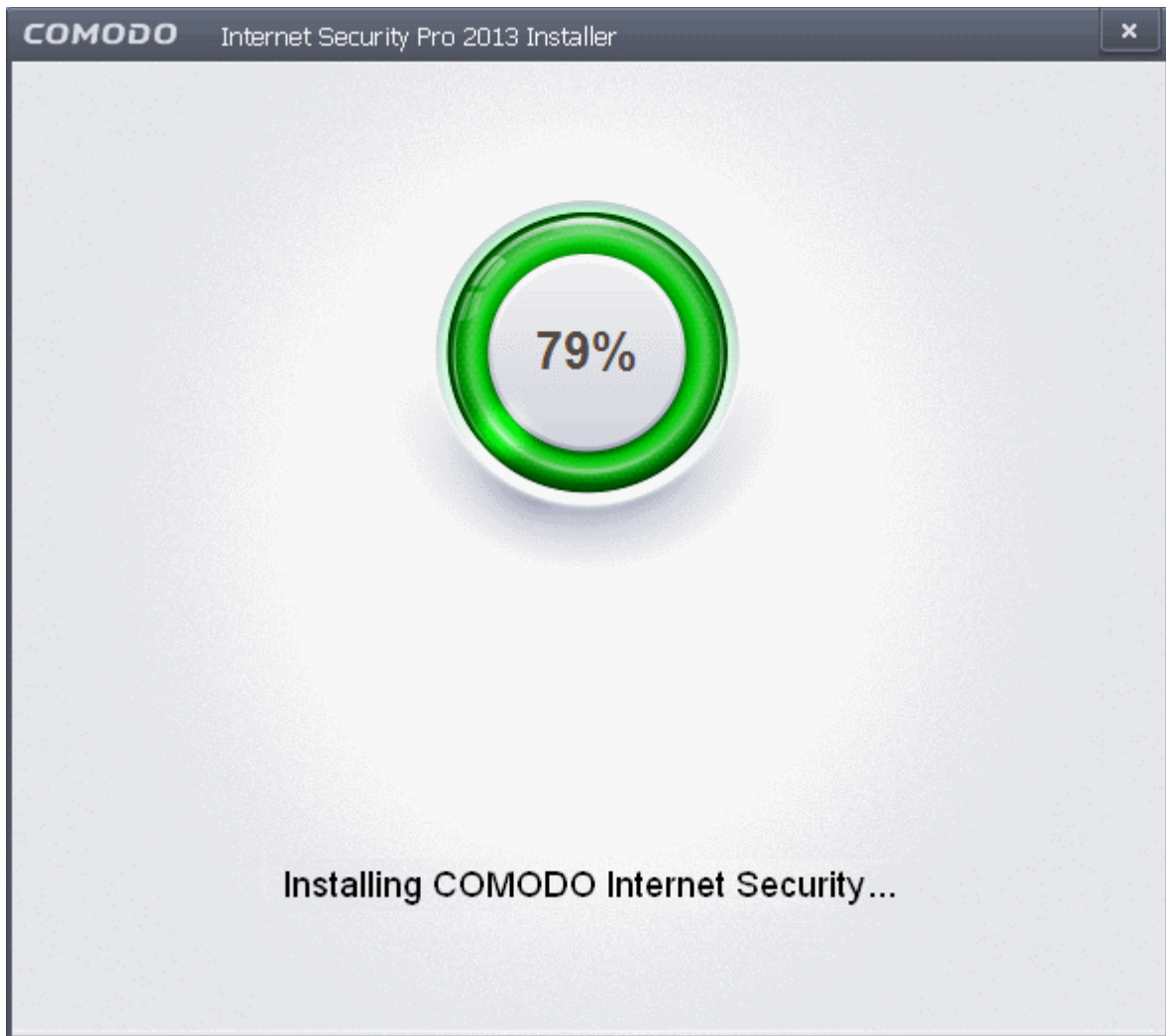
Enter the License key that you received through email.

Copy and save your licence key in a safe place, as you will need it for installation in other machines (your license entitles you for installing the product and obtaining the services on upto three machines).

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

Step 3 - Installation Progress [\(Click to go back to Step 2\)](#)

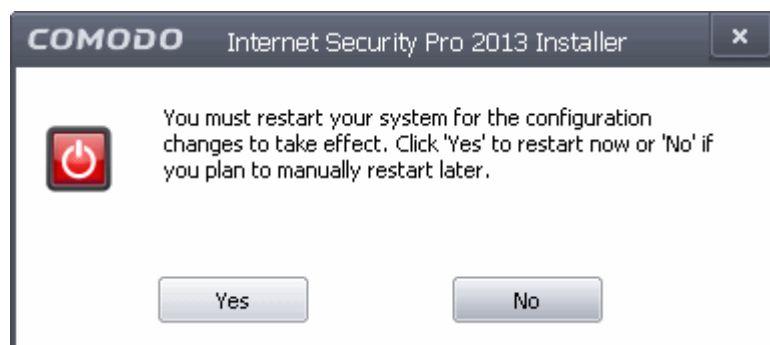
Your License key will be validated and the installation progress will be displayed...



...and on completion, the restart dialog will be displayed.

Step 4 - Restarting Your System

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



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

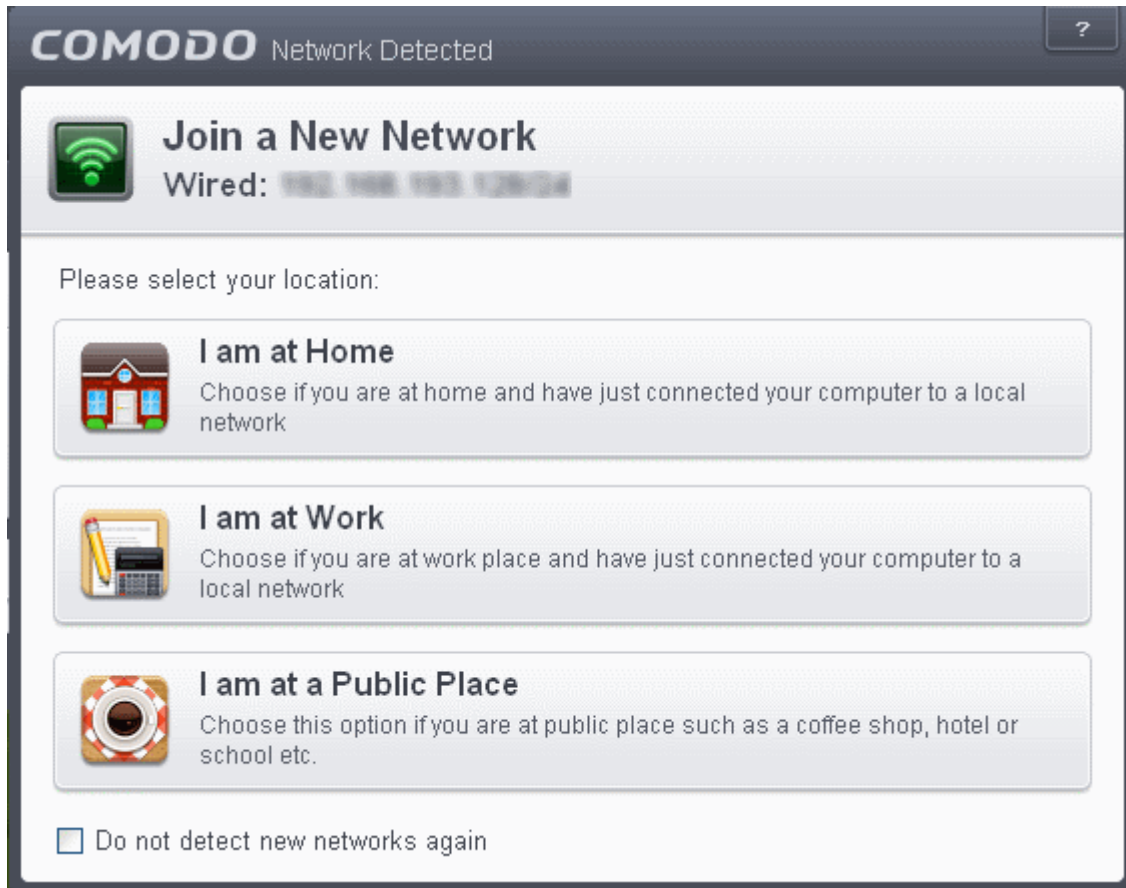
Step 5 - After Restarting Your System

After restarting, a 'thankyou' 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.



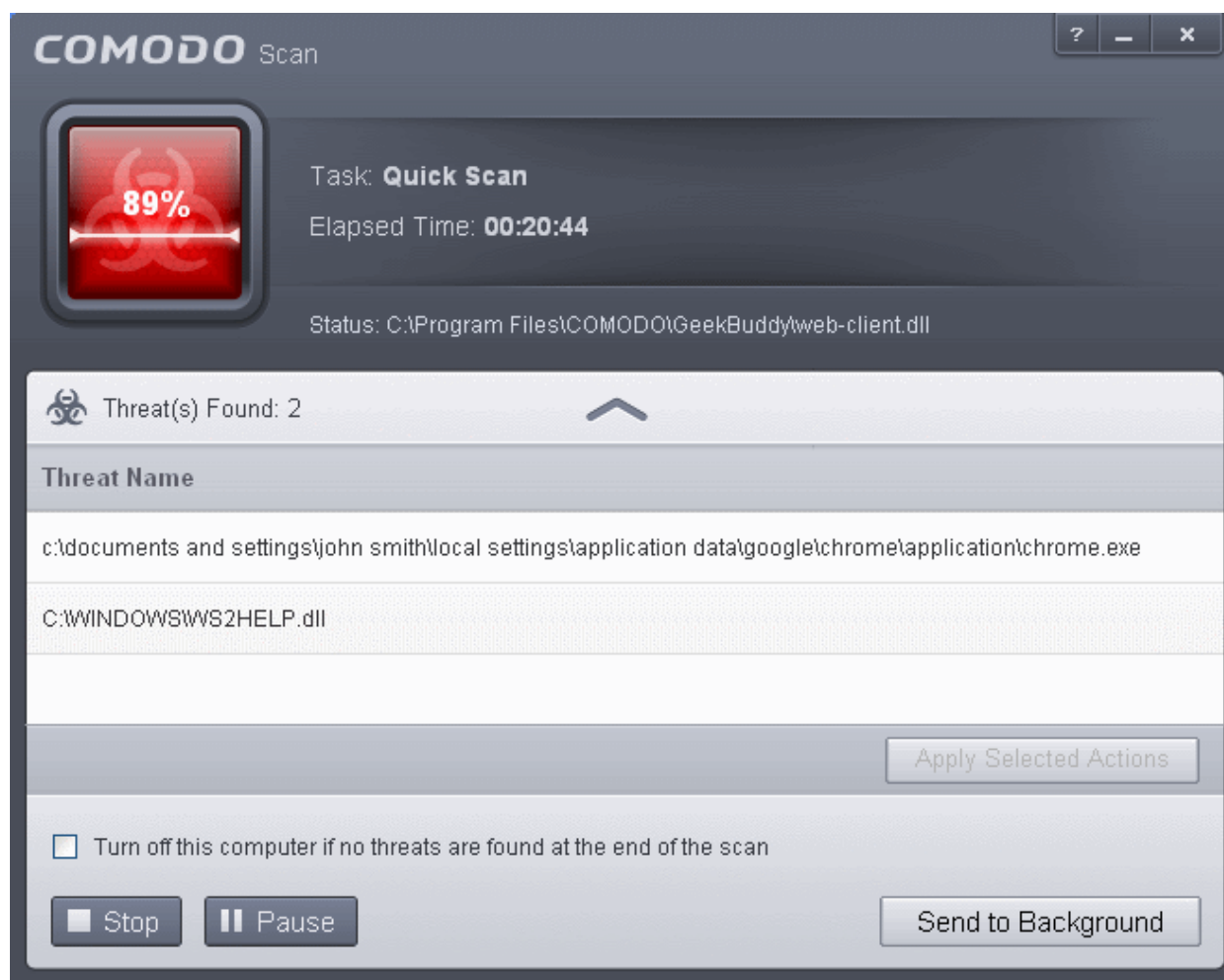
- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '[Network Zones](#)' and through the '[Stealth Ports Wizard](#)')

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



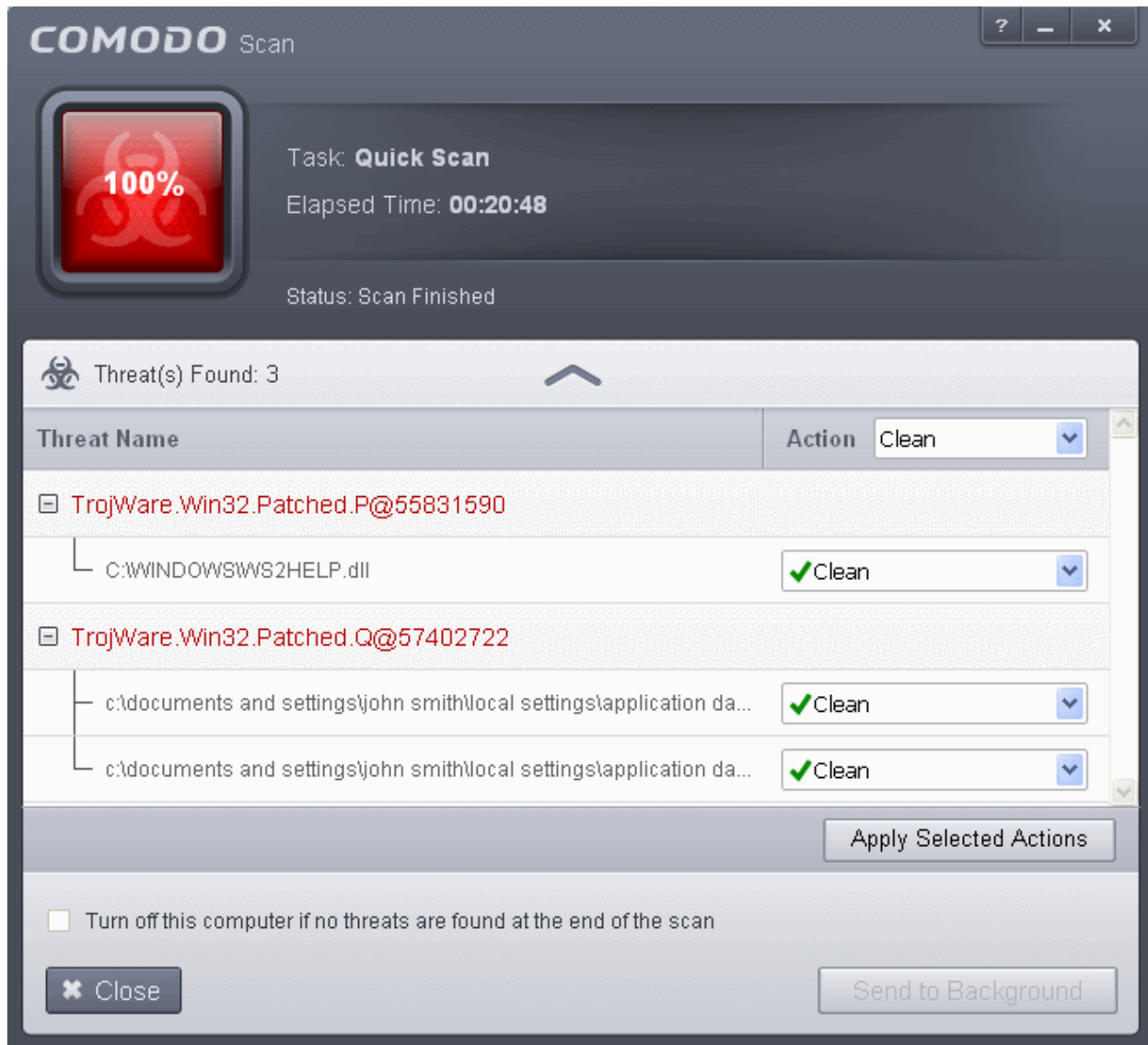
The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '[Manage CIS Tasks](#)' 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, the results screen will be displayed.



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.

Important Note: In order to get your Guarantee coverage, you need to activate your guarantee after successful installation of the application suite and activation of the license.

- 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

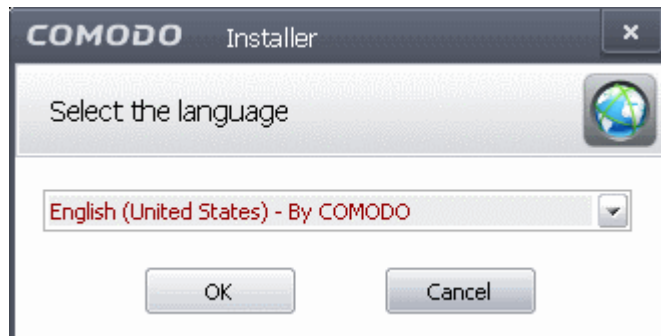
Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. [Click here](#) to read the full note.

Comodo Internet Security 2013 Complete is distributed on DVD and includes [Comodo GeekBuddy](#), [Online BackUp](#), [TrustConnect](#), [Comodo Dragon](#) and the [Comodo Guarantee](#).

After inserting the DVD, the setup program will start automatically.

Tip: If the setup program does not start automatically, click Start > My Computer and double click on the your DVD drive in the Windows Explorer window.

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'.

The following window is displayed.



Install Internet Security Complete 2012 - If you have not yet installed CIS then you should first select 'Install Comodo Internet Security Complete 2012'.

- [Click here for more details on installing Comodo Internet Security Complete 2013](#)

Activate Online Backup and TrustConnect - Begins the activation processes for your online storage space account, TrustConnect account and for your Comodo Guarantee. Please locate your License Key before starting (this is either printed on the DVD itself or printed on an insert included in the box packaging). After entering a valid license key, you will be taken to a Comodo web-form to start the account registration process.

- [Click here for full details on services activation](#)

Install Online Backup - Begins the Comodo BackUp installation procedure. Once installed, you will be able to schedule regular backups to local and network drives. You also get 10GB of secure online backup space (access this by entering your Comodo account username and password in the Comodo BackUp interface).

- [Click here for more details on installing Comodo Backup](#)
- [Click here if you wish to view the Comodo BackUp User Guide](#)

Install TrustConnect - Begins the Comodo TrustConnect setup procedure. TrustConnect usage can be managed by logging into your account at <https://accounts.comodo.com>.

- [Click here to read more about TrustConnect](#)
- [Click here for more details on Installing Comodo TrustConnect.](#)

1.3.3.1. Installing Comodo Internet Security Complete 2013

Click 'Install Internet Security Complete 2013' from the main Comodo Internet Security Complete 2013 Installer screen. The installation wizard for CIS 2013 , GeekBuddy and Dragon will start immediately.

Step 1 - Validating your License and Installation Configuration

The initial phase of installation requires validating your license and configuring the installation of CIS Complete.

The License key is printed on the DVD itself or printed on an insert included in the box packaging.

Enter the license key fully.



Your License key will be validated immediately. On successful validation of the entered key, a green check mark will be

displayed.

Tip: You can skip this step if you don't have the subscription key handy or you are not connected to Internet at the time of installation. In order to continue the installation without entering the key, proceed with configuring the installation as explained below and clicking 'Agree and Install'. You can activate your subscription and guarantee at a later time from the main interface of CIS. For more details refer to [Activating your CIS Pro and CIS Complete Services after Installation](#)'.

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.

Cloud Based Behavior Analysis

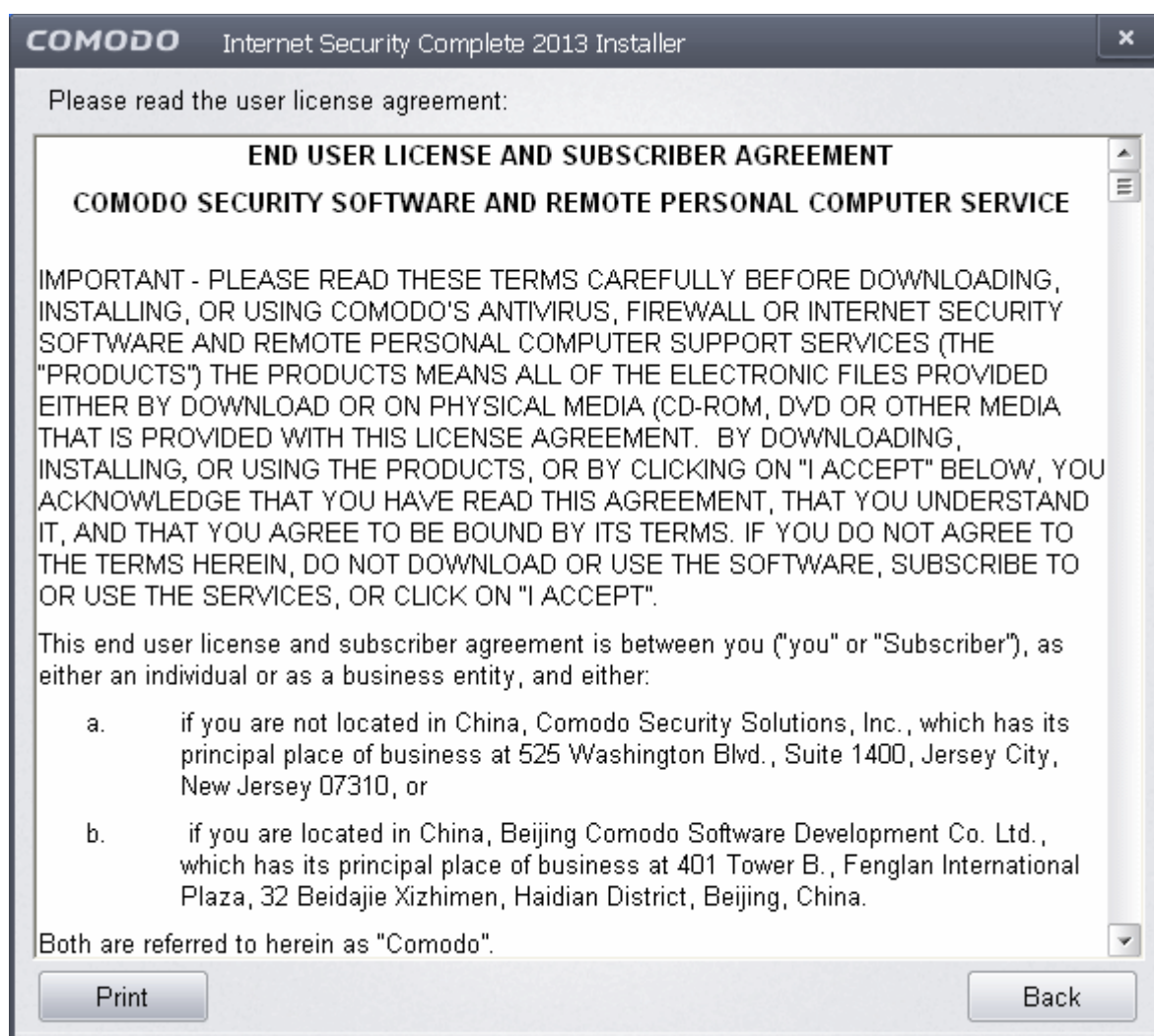
Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

Browser Homepage

Your default browser home page and the search engine will be set as Yahoo!

End User License Agreement

Read the complete User License Agreement by clicking the 'User License Agreement' link before proceeding with the installation.



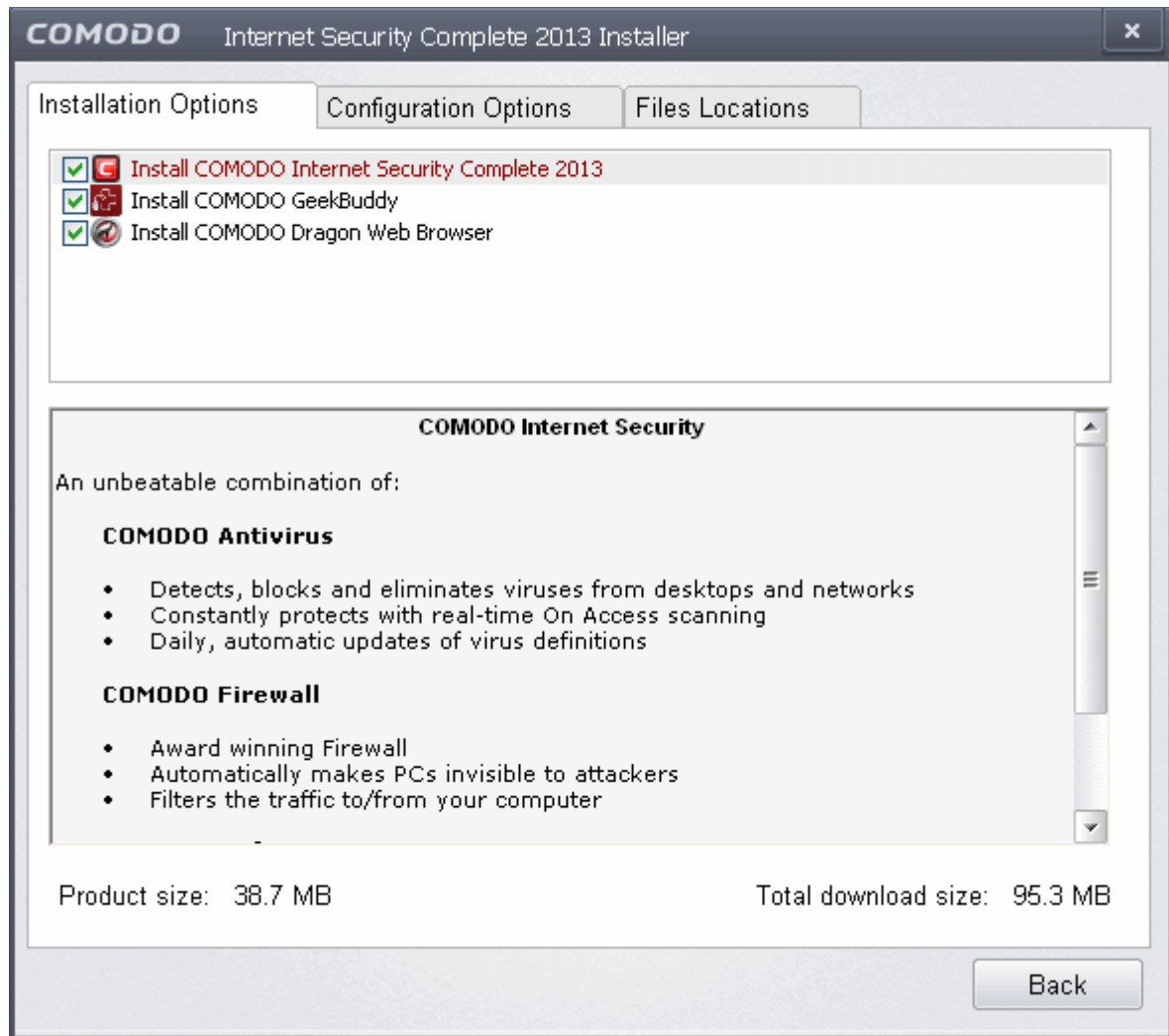
After reading the agreement, click the 'Back' button to return to the installation configuration screen.

Customizing Installation

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

Selecting Components to Install

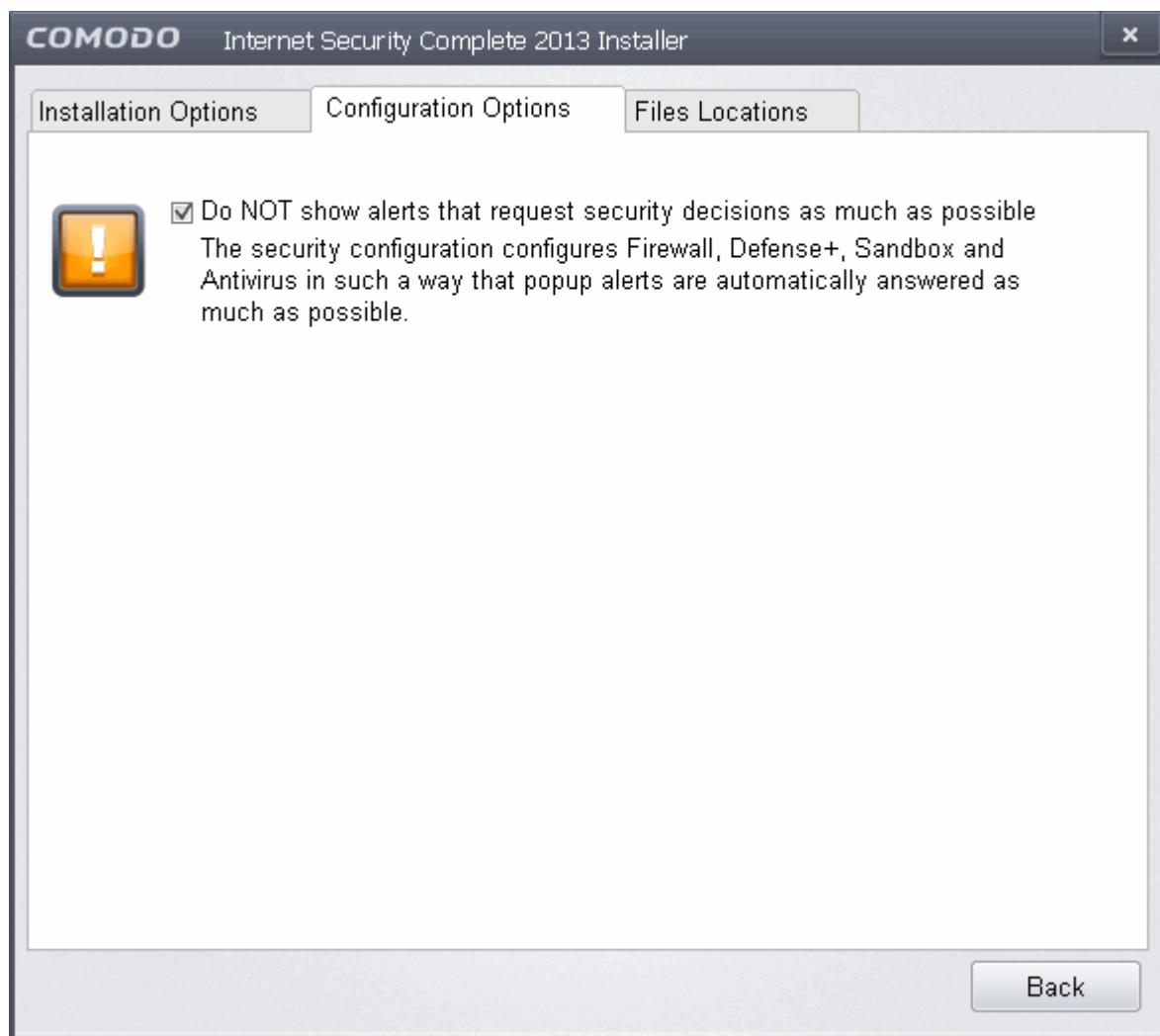
Click the 'Installation Options' tab to select the components to be installed.



- **Install COMODO Internet Security Complete 2013** - Selecting this option installs Comodo Antivirus, Comodo Firewall and Defense+ components. Installing CIS Complete 2012 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 COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section **Comodo Dragon** for more details.

Configuration Options

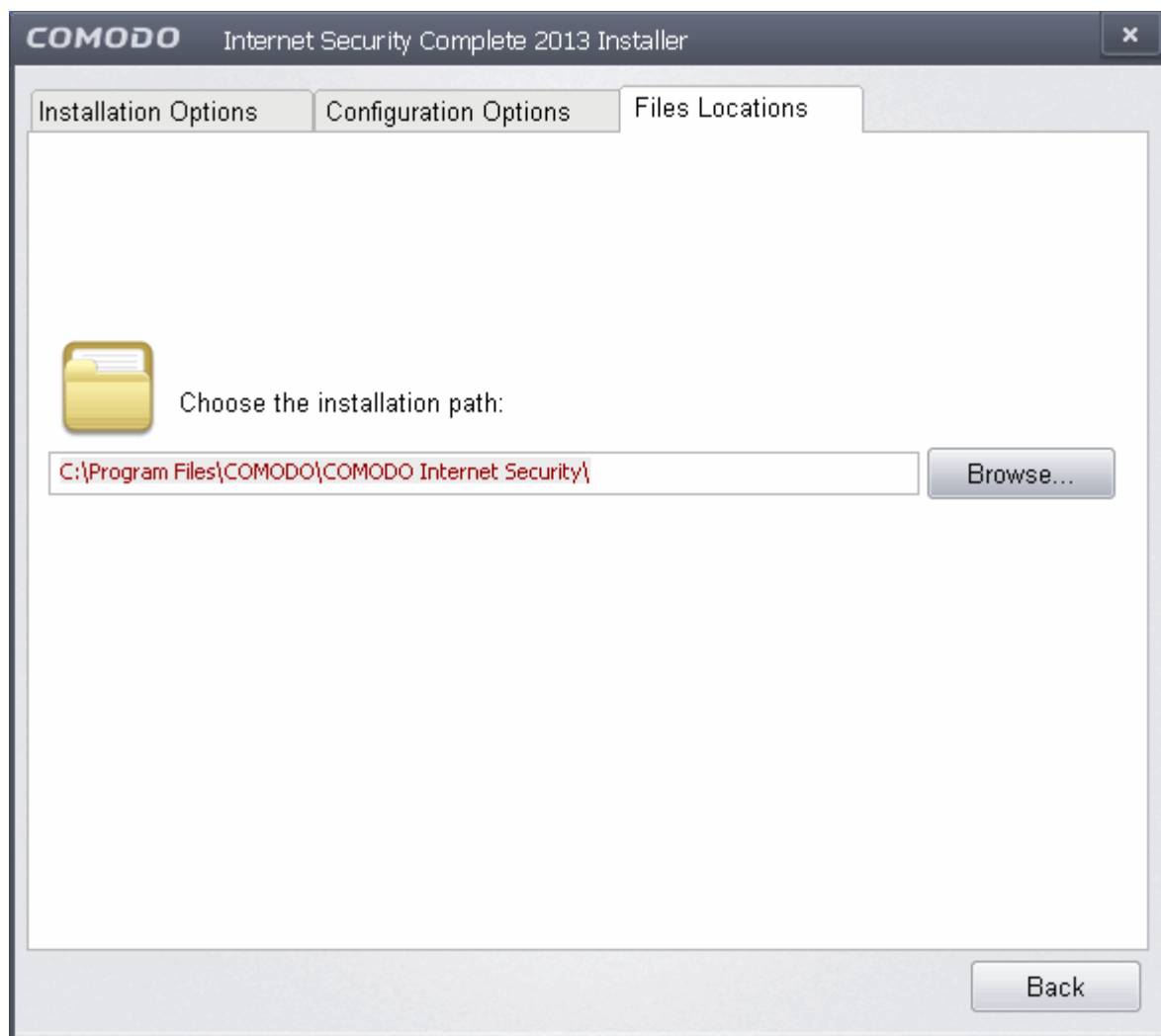
Click the 'Configuration Options' tab to configure pop-up alert options.



- **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.



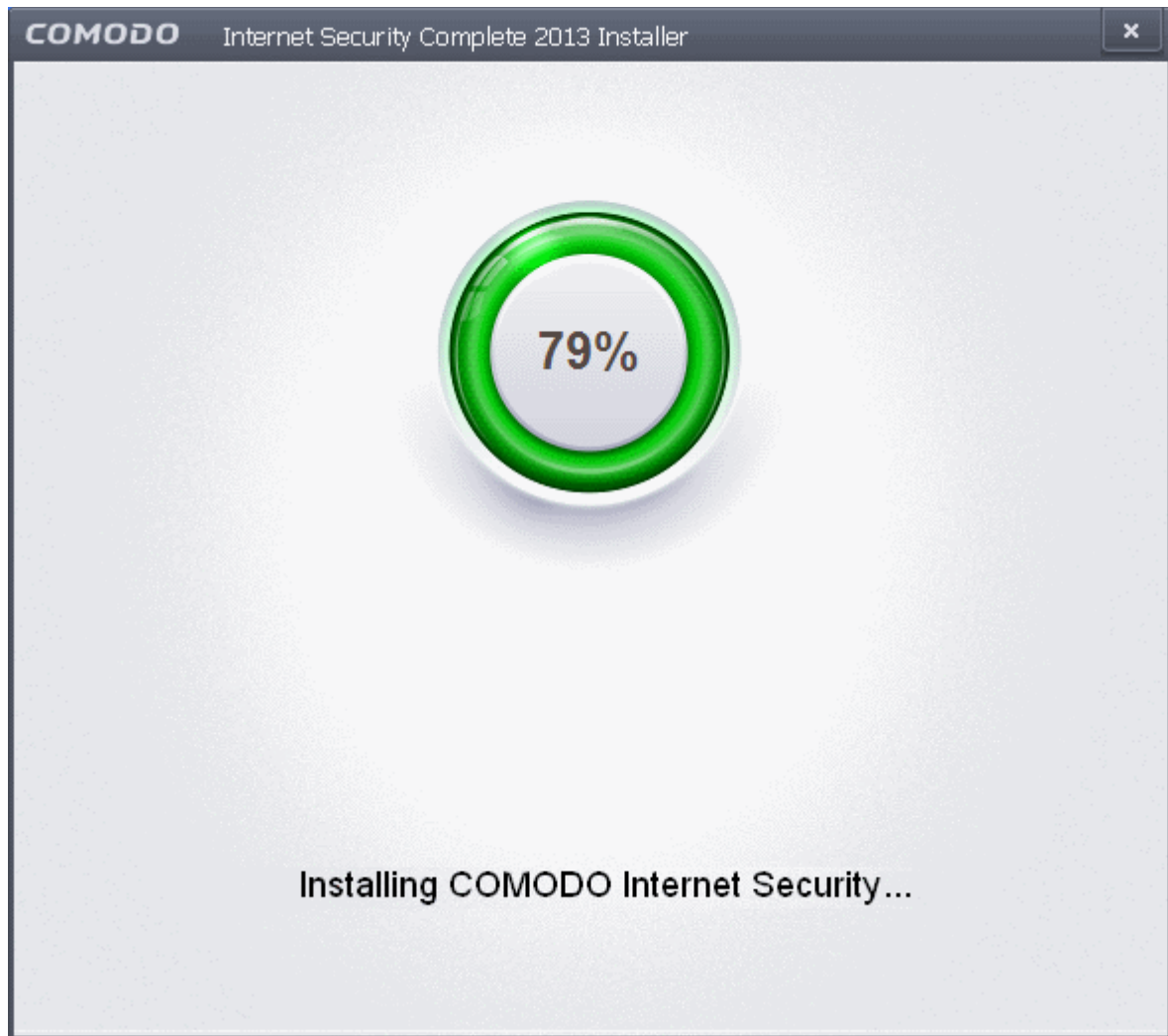
This interface allows you to set the installation folder for Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

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 2 - Installation progress

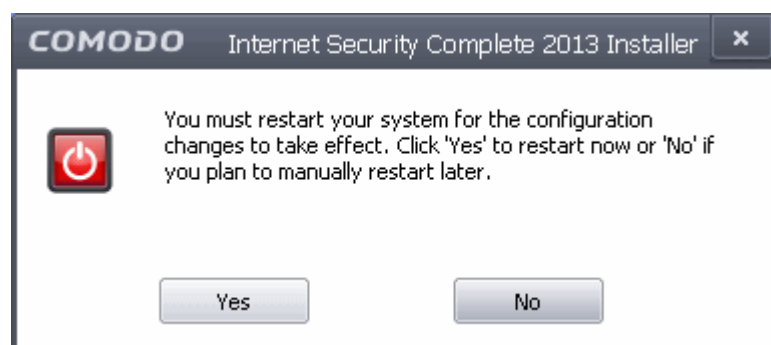
The next step is installation of the product and activation of the license. The progress will be displayed...



...and on completion, the restart dialog will be displayed.

Step 3 - Restarting Your System

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



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

Step 4 - After Restarting Your System

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

some friendly advice.

COMODO Internet Security Complete 2013



COMODO Internet Security Complete 2013

Thank you for installing COMODO Internet Security Complete 2013. Choosing Comodo for your PC security is a responsibility we take very seriously.

Now is the time to start familiarizing yourself with your certified GeekBuddy technicians. They can assist you with security related issues you have, not just issues related to viruses and malware.



Antivirus

All antivirus programs block known threats, but what about unknown threats?

Our award winning Antivirus software includes **Sandboxing** to prevent all unknown programs from running until they have been scanned and approved.



GeekBuddy

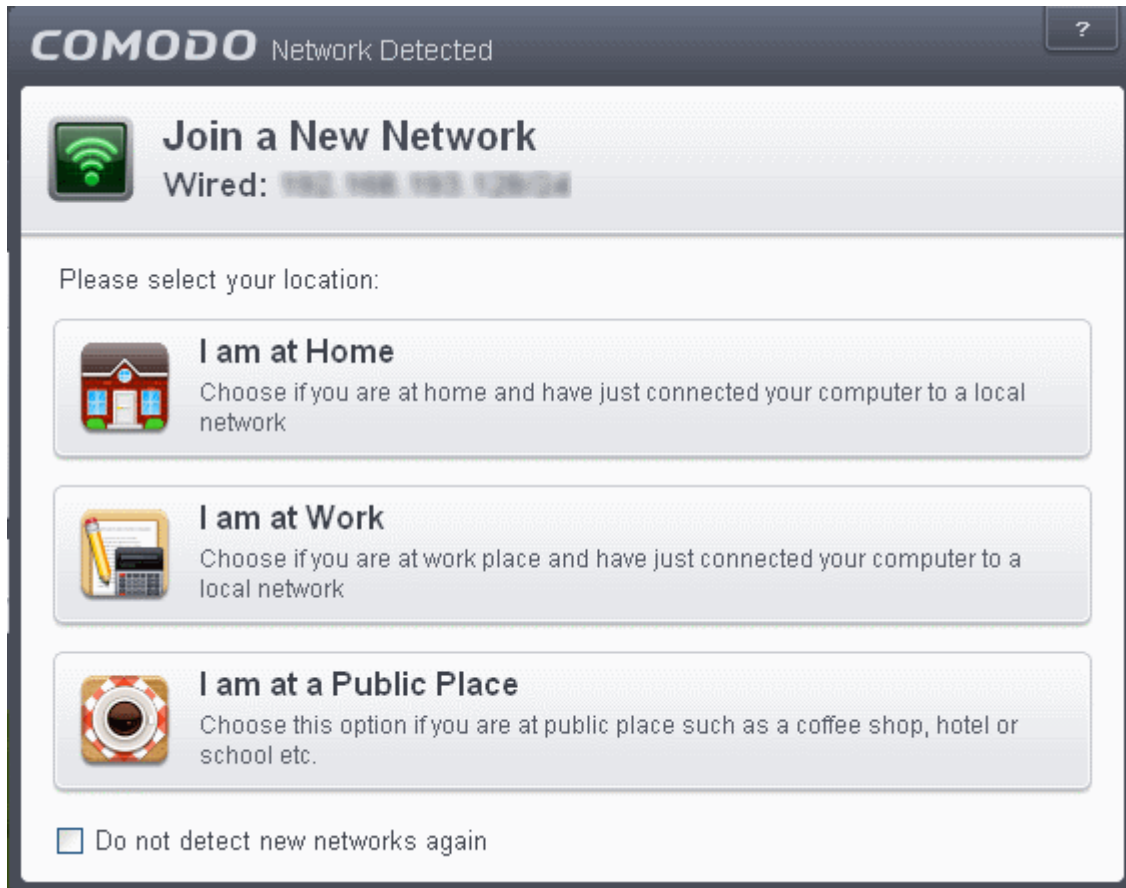
Ever experience a problem with your computer that you can't fix?

Your subscription includes GeekBuddy. You will have licensed technicians who are always available via chat and phone to assist you with ANY computer issue you have.

Do not show this window again

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.



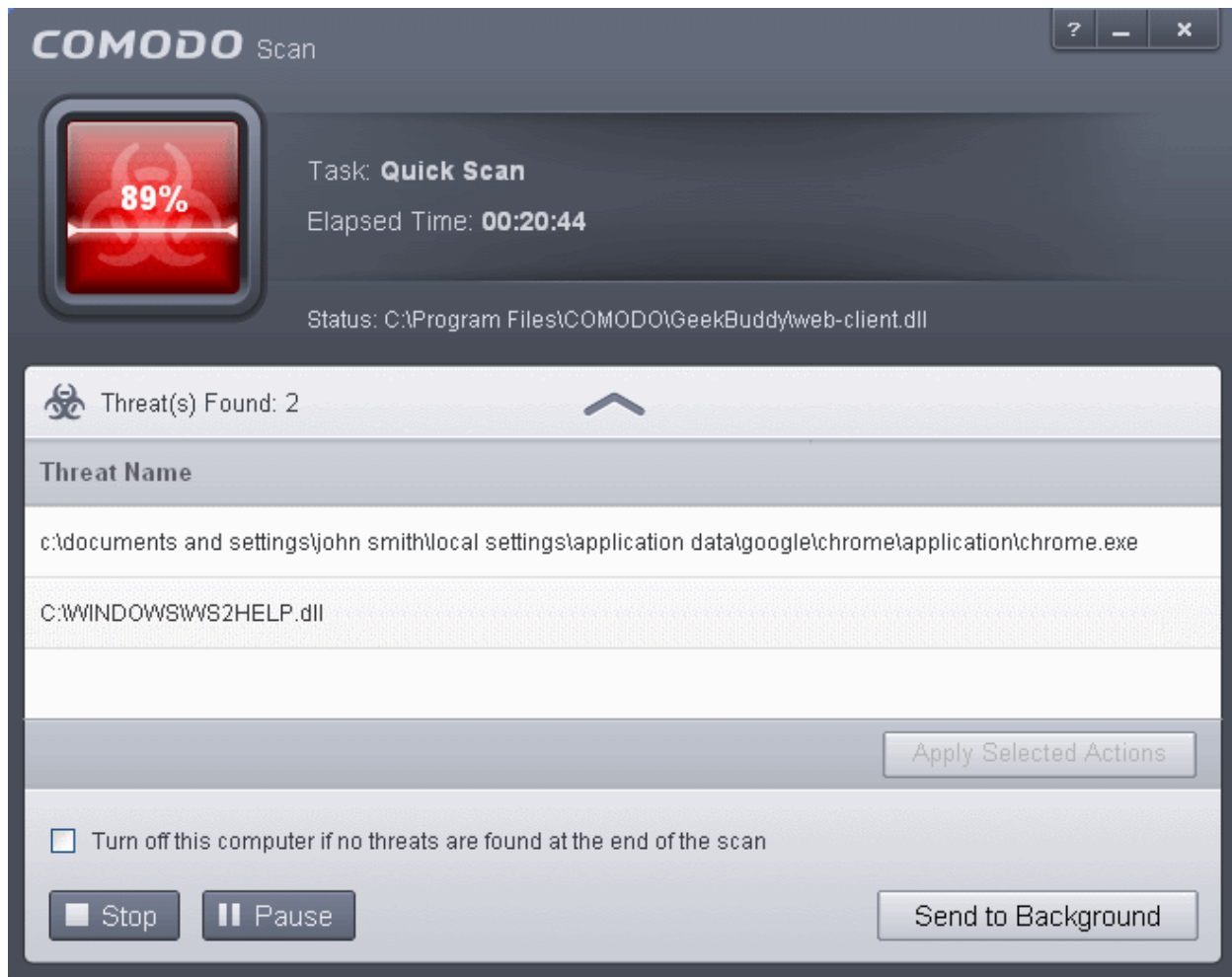
- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '[Network Zones](#)' and through the '[Stealth Ports Wizard](#)').

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



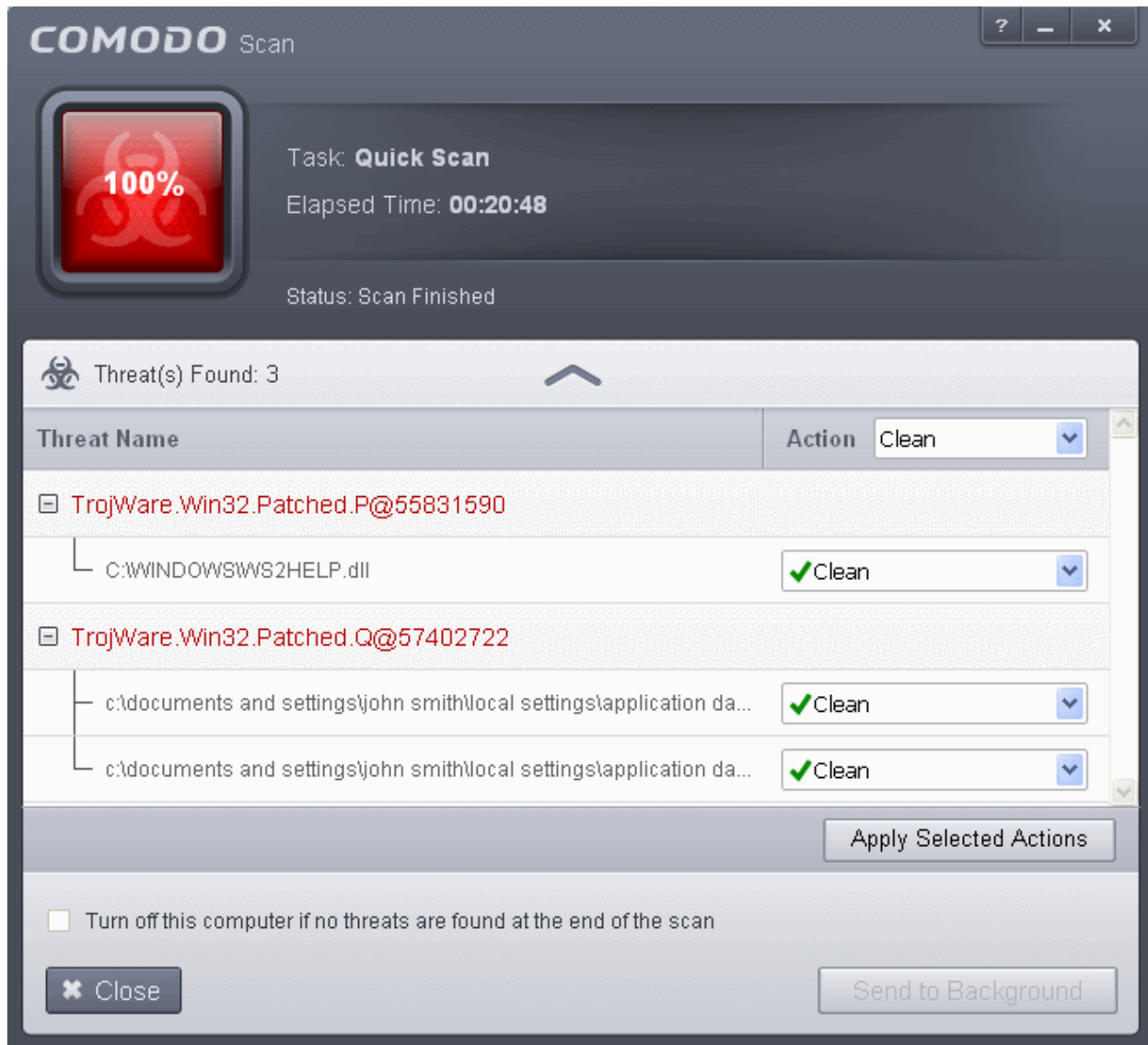
The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '[Manage CIS Tasks](#)' 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, the results screen will be displayed.



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.

Important Note: In order to get your Guarantee coverage, you need to activate your guarantee after successful installation of the application suite and activation of the license.

- 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](#).

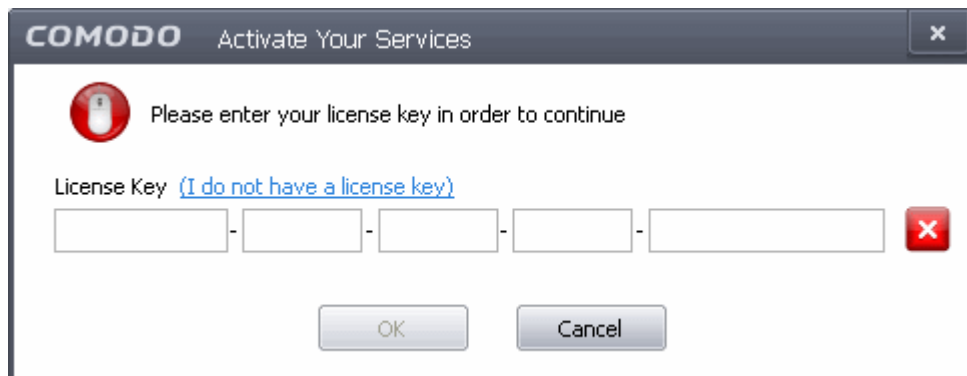
1.3.3.2. Activating Online Backup, TrustConnect and Guarantee

In order to utilize your 10GB online storage space and TrustConnect services, you need to activate the services. Keep the license key handy, before starting this process.

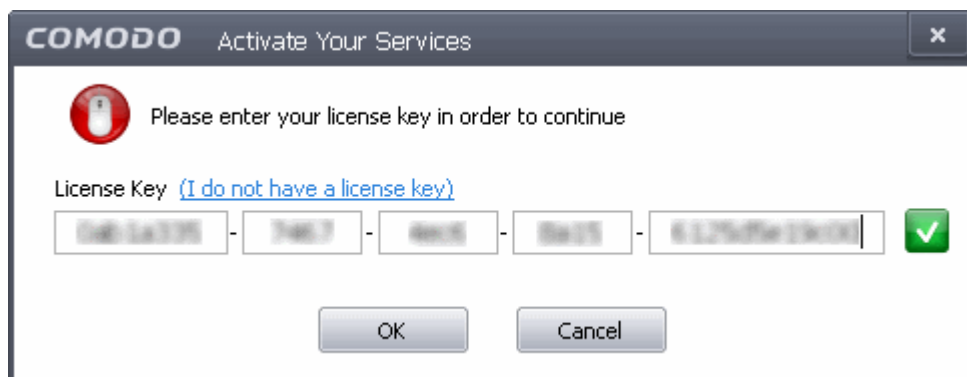
- Reinsert the DVD and click 'Activate Online Backup and TrustConnect' from the main Comodo Internet Security 2013 Complete Installer screen after selecting the language.



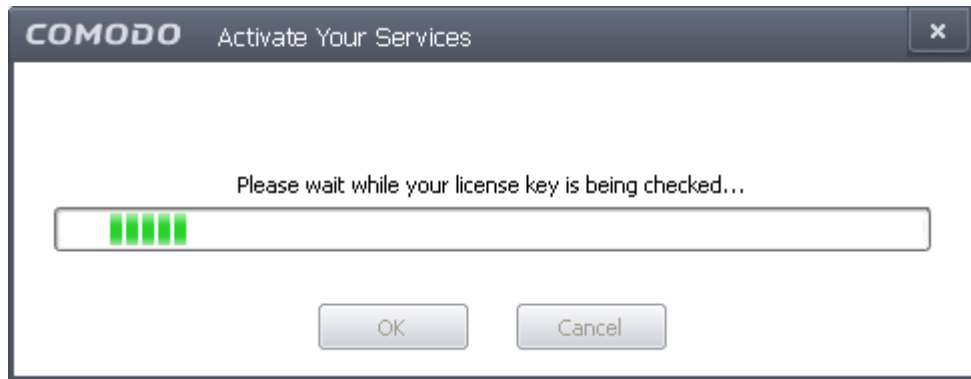
- You will be prompted to enter the your license key.



- Enter the license key provided to you with the CIS product and click OK. The license key will be validated.



- The license key will be validated.



After the License key is verified, the Comodo Sign-Up Page will be displayed.

COMODO | **Comodo Internet Security**
Creating Trust Online*

Comodo Sign-Up Page

License Key*

Customer Information (an * indicates required fields)

User Details

Are you an existing Comodo customer? Yes No

Login* (4 character min.)

Password* (8 characters min.)

Password Confirmation*

First Name*

Last Name*

Email*

Telephone Number

Contact Information

Company Name

Street Address*

Address2

City*

Country*

State or Province

Postal Code*

Communication Options

Yes! Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!

Terms and Conditions

END USER LICENSE AND SUBSCRIBER AGREEMENT
Comodo Internet Security

IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO'S SECURITY SOFTWARE OR USING COMODO'S SECURITY SUITE SERVICES ("PRODUCTS"). BY DOWNLOADING, INSTALLING, OR USING THE PRODUCTS, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT DOWNLOAD OR USE THE SOFTWARE.

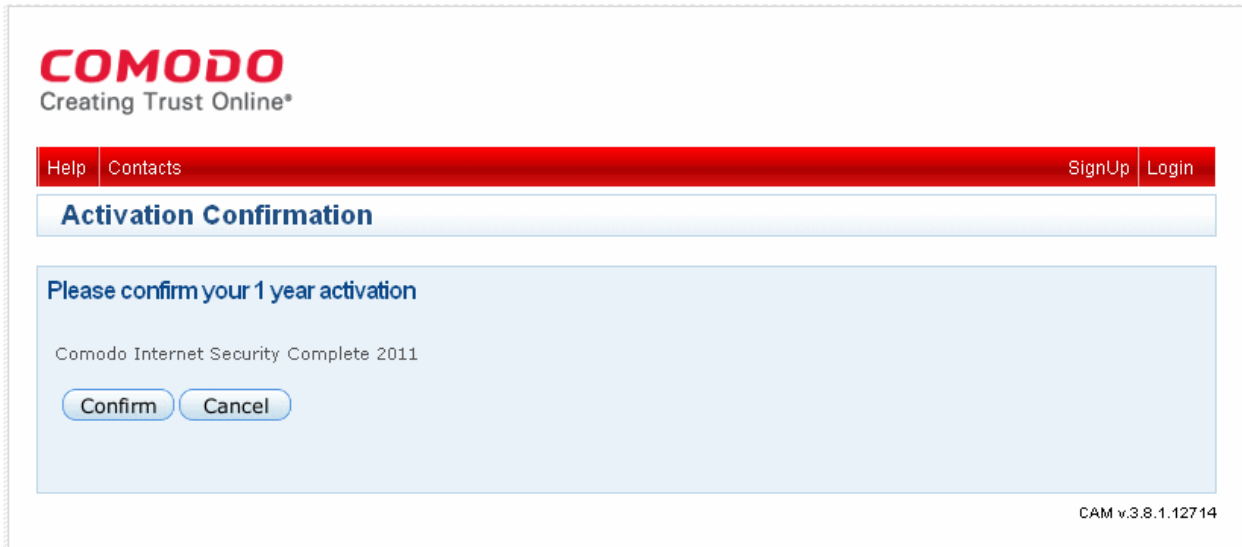
I accept the Terms and Conditions

SIGN UP

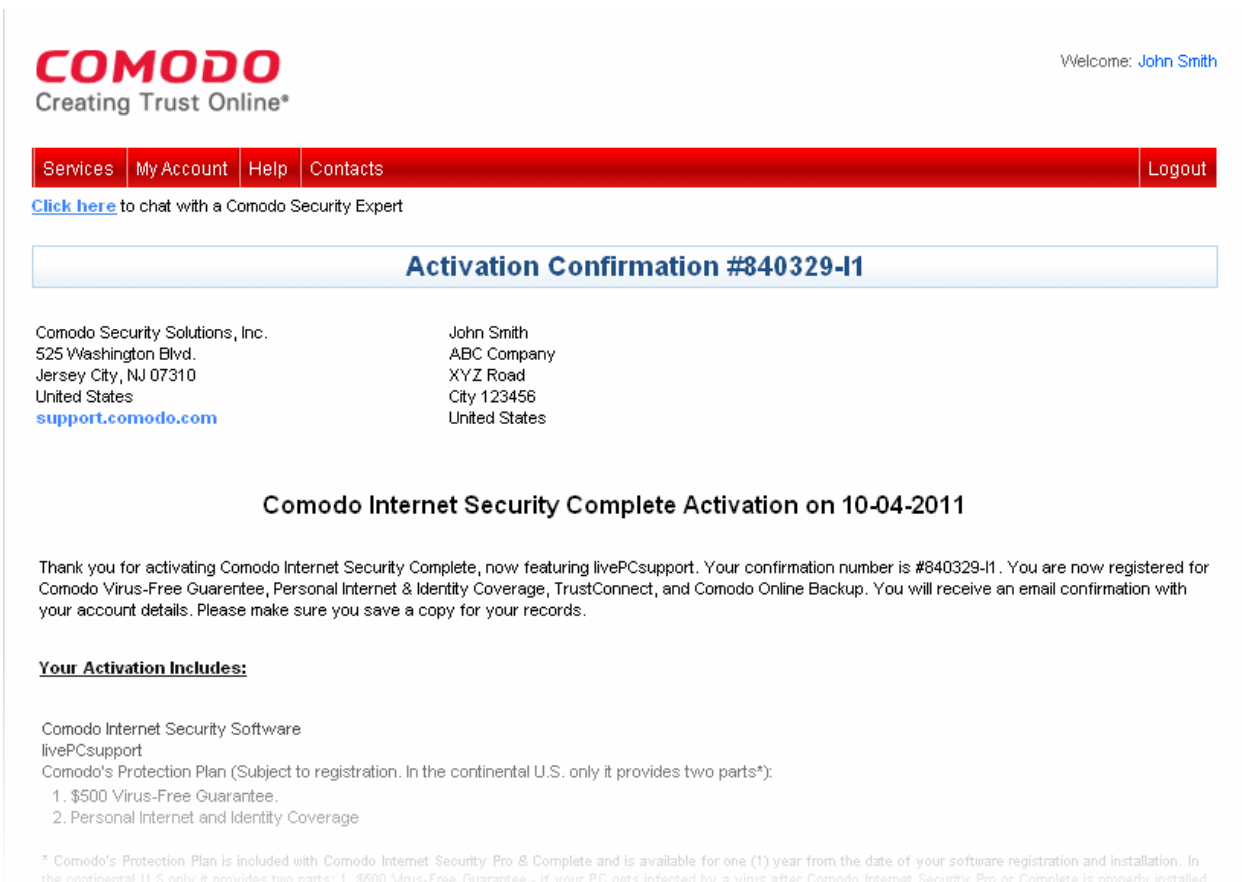
[Terms & Conditions](#) | [Comodo Security Solutions, Inc.'s privacy policy](#) | [Contact Us](#)
©Comodo Security Solutions, Inc.

CAM v.3.0 1.12714

Fill up the required field details and click 'Sign Up' button after selecting the 'I accept the Terms and Conditions' checkbox. The page for Activation Confirmation is displayed. Click the 'Confirm' button to activate the service.



Clicking the 'Confirm' button displays the Activation Confirmation page. The page displays the Activation Confirmation number, your details that you entered while registering, the services you have ordered for, links for downloading the software, your license key and other login details. You will also receive an email regarding the activation of services.



You can now login to your account at <https://accounts.comodo.com>, with the login details you specified during sign-up.

Subscriptions					Search	Create New
Product name	License key	Remediations	Expired At	Status		
Comodo Internet Security Complete 2011	58e45c27-bbfa-48fc-8041-6e1aad107aca	0 remediations	2012-10-04	VALID	Renew	View

1 Found

CAM v.3.8.1.12714

- For using TrustConnect services, you need the Service login and Service Password generated for you. For more details, refer to the chapter [TrustConnect Overview](#).
- For using Online Storage Services, you can use the same login and password you specified during Signing-up for Comodo Account. See [Start Using Online Storage Space](#) for more details.

1.3.3.3. Installing Comodo Backup

In order to store your valuable files to Comodo online storage space for safe-keeping, you need Comodo Backup application installed in your system.

To install Comodo Backup

- Reinsert the DVD and click 'Install Online Backup' from the main Comodo Internet Security 2013 Complete Installer screen after selecting the language. The installation wizard of Comodo Backup will start immediately.

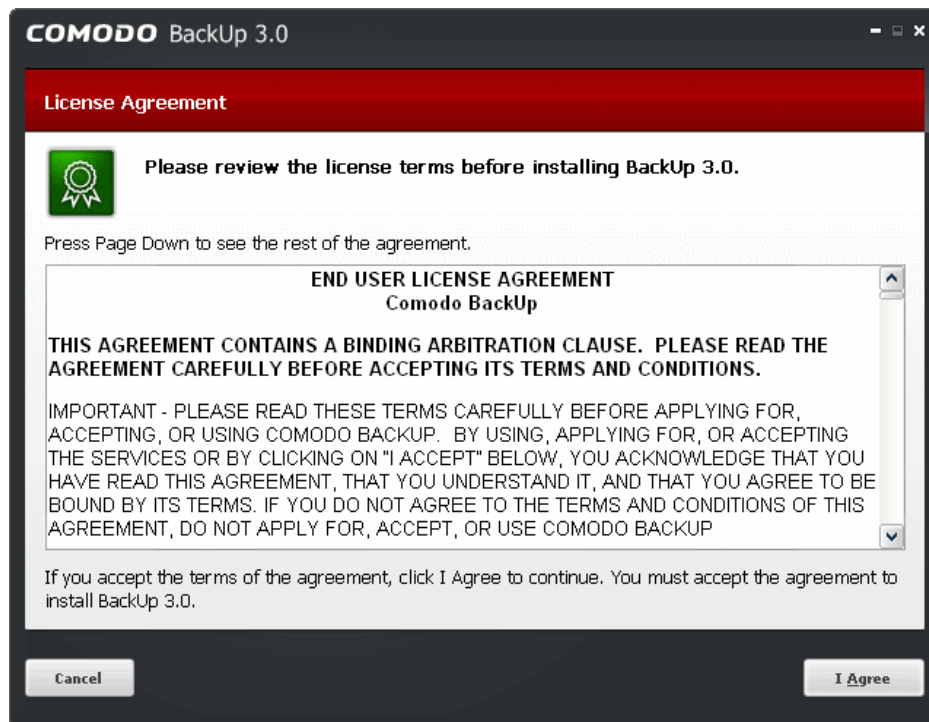
Step 1 - Choosing the Interface Language

The Select Setup language dialog is displayed. Comodo BackUp is available in several languages.



Step 2 - End User License Agreement

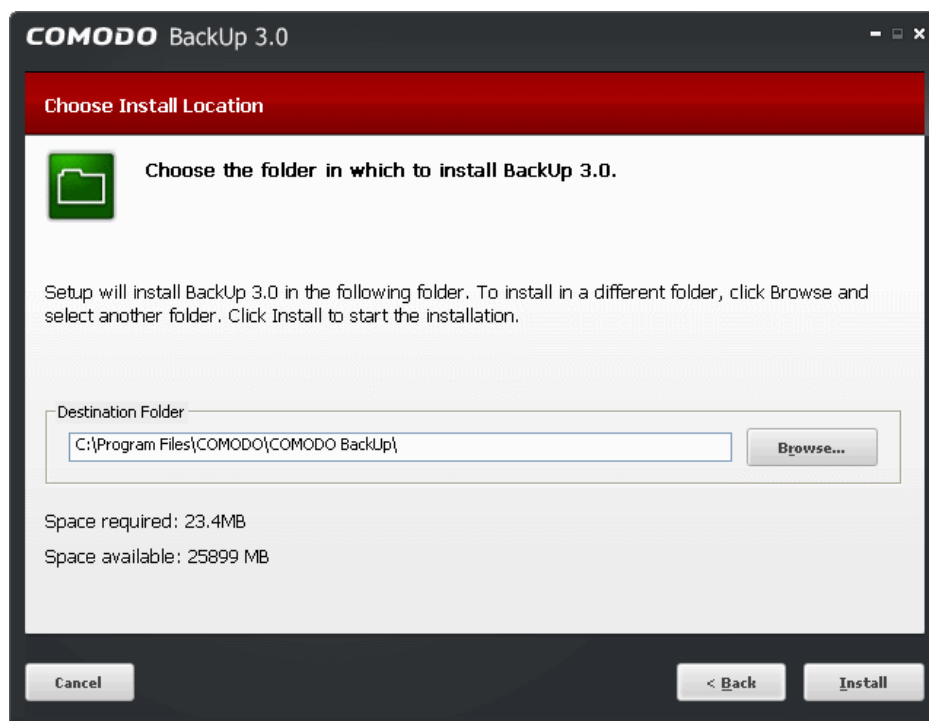
Complete the initialization phase by reading and accepting the End User License Agreement (EULA).



- Click 'I Agree' to continue installation. If you want to cancel the installation, click 'Cancel'.

Step 3 - Select Installation Folder

The next screen allows you to select the folder in your hard drive for installing Comodo BackUp. The default path is *C:\Program Files\Comodo\Comodo BackUp*.

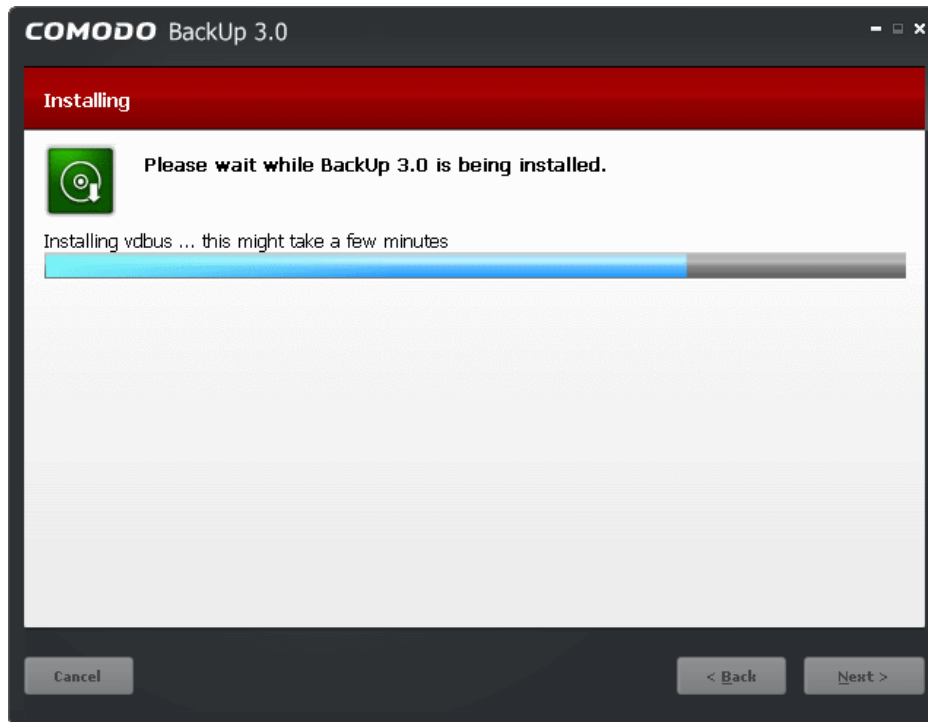


If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

- Click the 'Back' button to review / change any of settings you specified before or press 'Install' to continue with installation process.

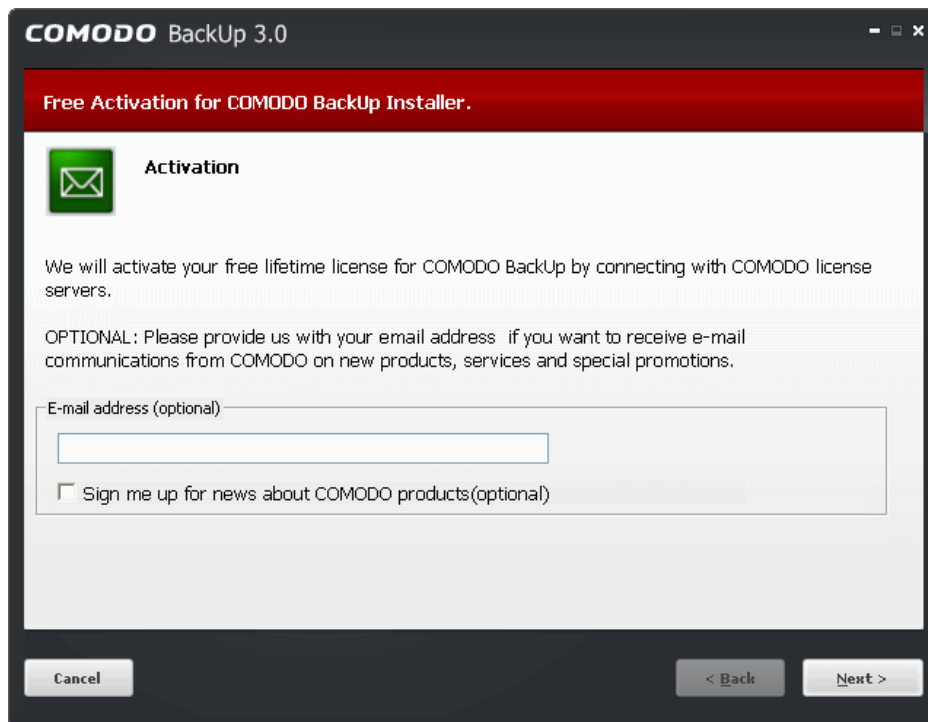
Step 4 - Setup Progress

A setup status dialog box is displayed. You can see a progress bar indicating that the files are being installed.



Step 5 - Product Activation

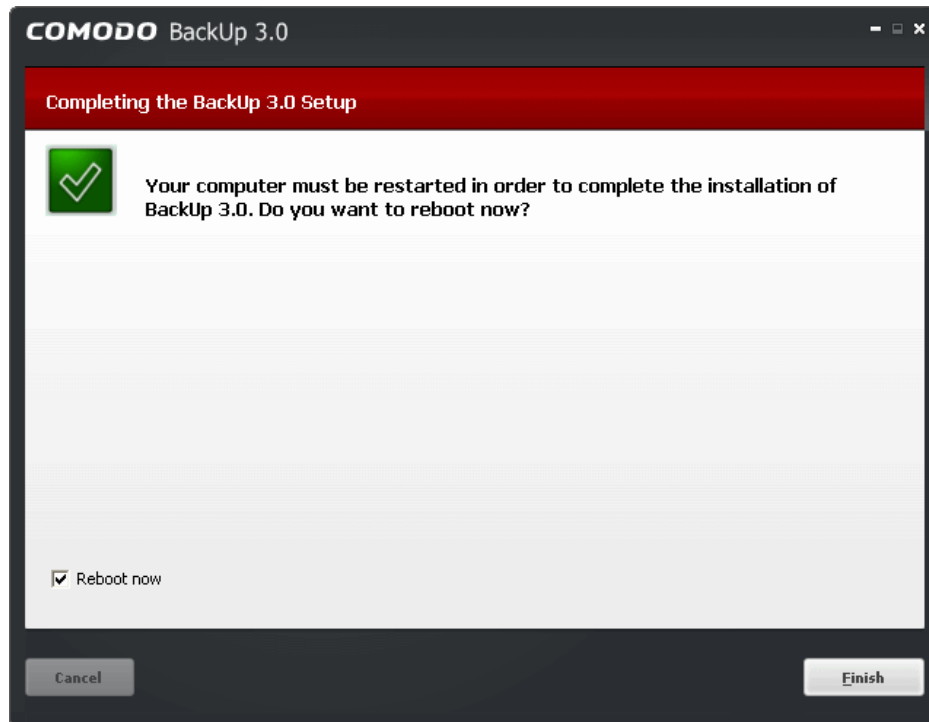
On completion of Installation, the product Activation dialog is displayed. Comodo BackUp is activated at free of cost for lifetime usage. If you wish to sign up for news about Comodo products then enter your email address in the space provided and select **Sign me up for news about Comodo products**.



This is optional. Click 'Next'.

Step 6 - Installation Complete

The Installation Completion dialog is displayed indicating the successful completion of installation. For the installation to take effect, the system has to be restarted.

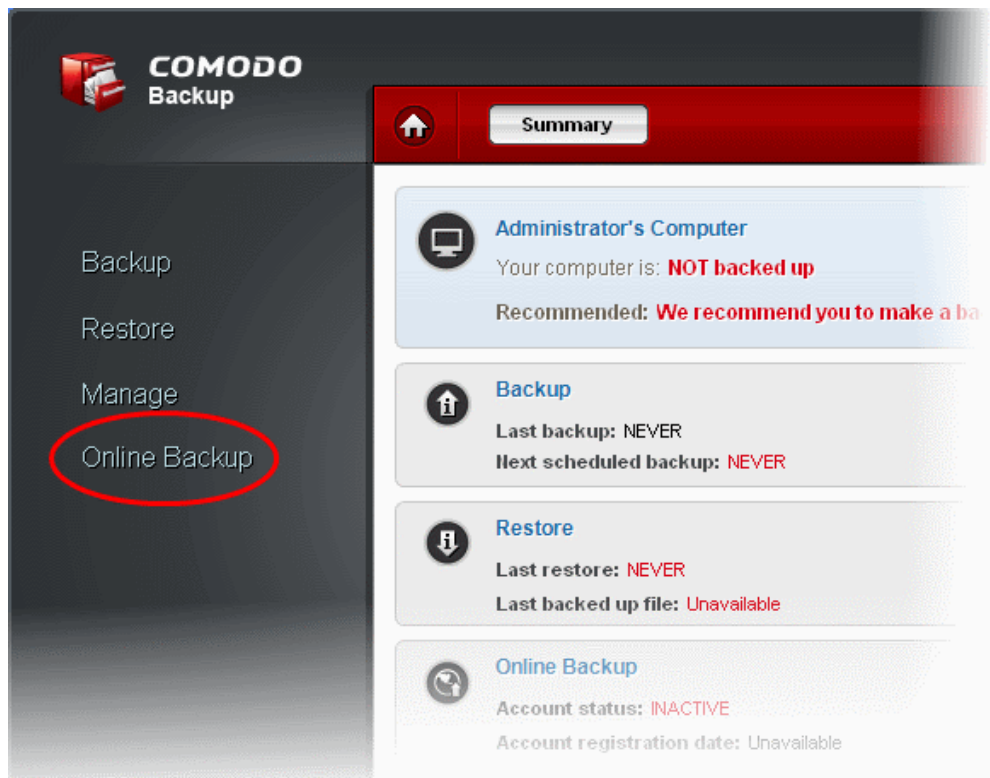


Please save any unsaved data, leave 'Reboot now' checkbox selected and click 'Finish'. If you want to restart the system at a later time, uncheck 'Reboot now' checkbox click 'Finish'.

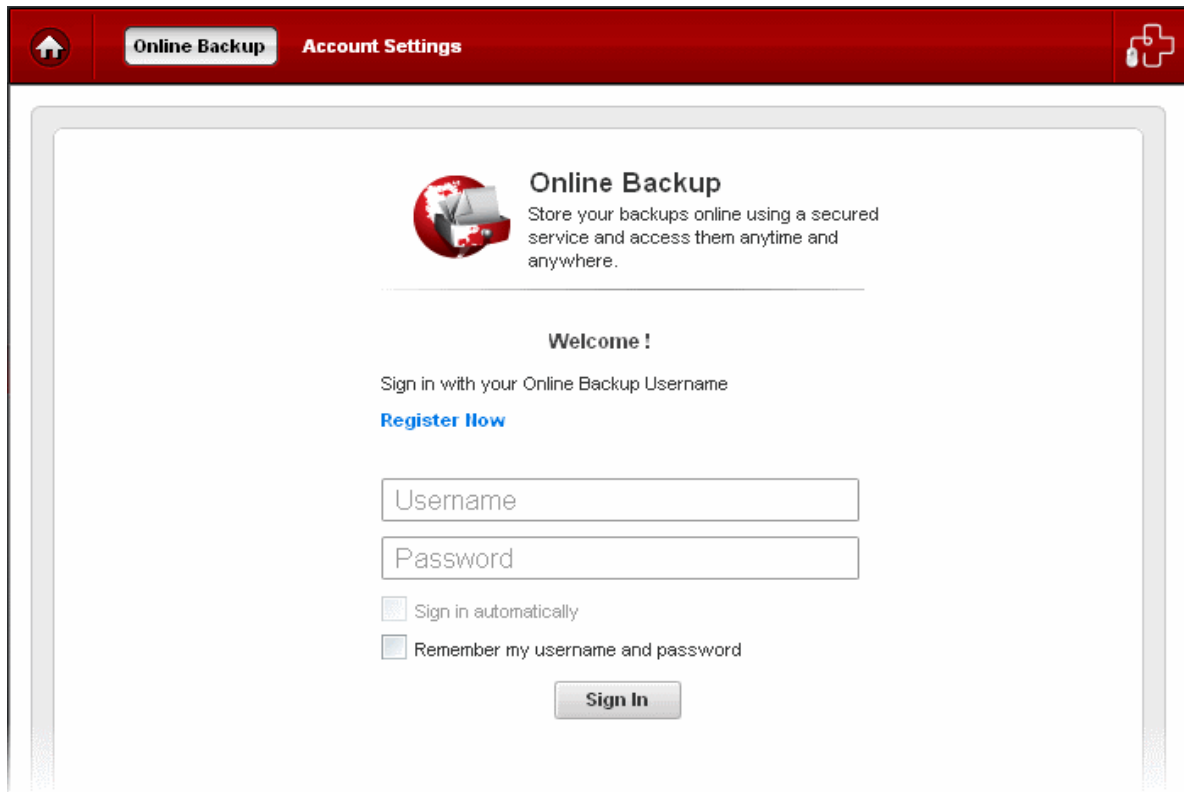
Note: The installation will take effect only after restarting the computer.

Start Using Your Online Storage Space

After successful installation of Comodo Backup, start the application and click Online Storage from Left Hand Side Navigation of its main interface.



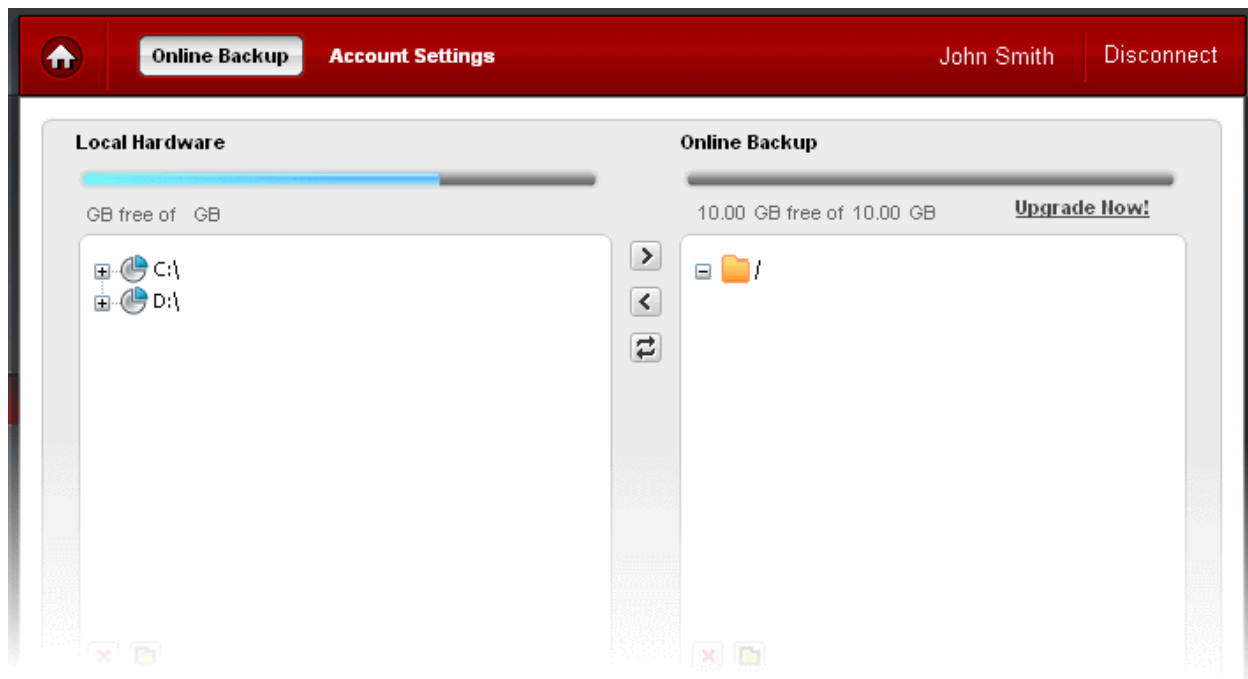
The Online Backup interface will open.



- Sign in using the login and password that you specified in the User Details area of the Comodo Sign-Up page .

After successful login, your username is displayed at the top of the interface. Your local disks, files and folders are displayed in the left hand pane while your online storage files/folder are displayed in the right hand side pane. You can drag and drop files and folders between the two windows.

Comodo BackUp can also be used to create scheduled backups to your online space and offers a wide range of backup types - including synchronized, differential and incremental backup.



Full details on using Comodo BackUp can be found in the Comodo BackUp user-guide available at

<http://help.comodo.com/product-9-Comodo-Backup.html>

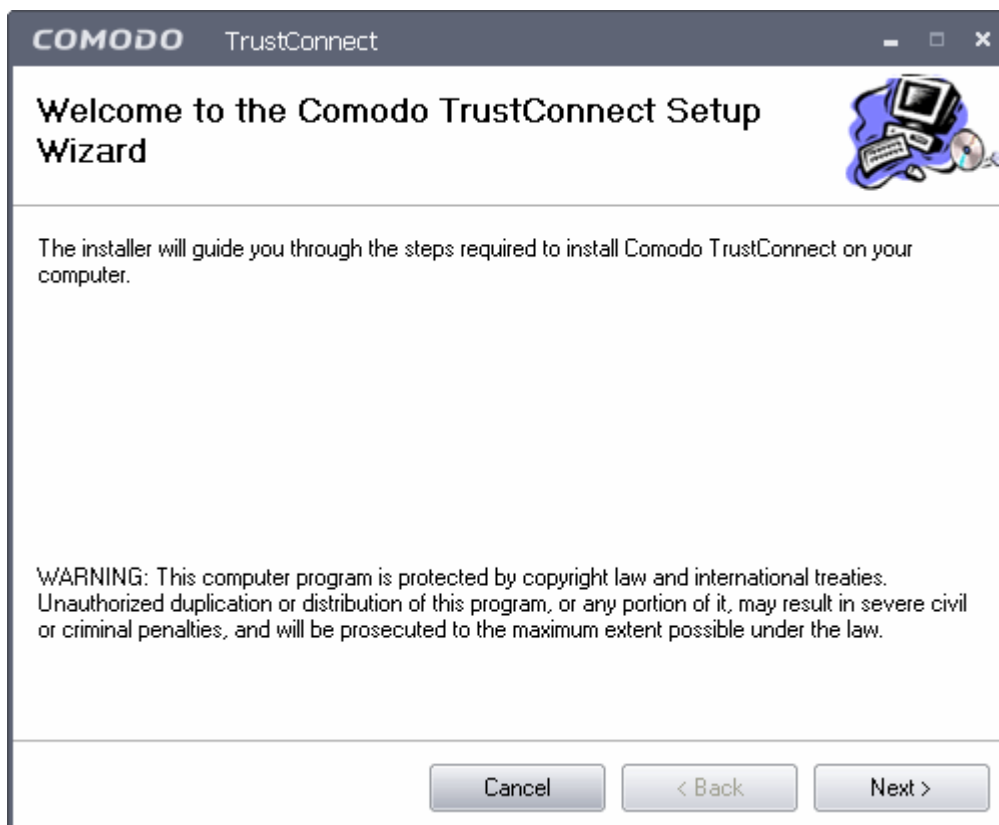
1.3.3.4. Installing Comodo TrustConnect

TrustConnect makes surfing secure from public Wi-Fi locations such as Internet cafes and airports. To install and activate the application, please follow these instructions:

- Click 'Install TrustConnect' from the main Comodo Internet Security 2013 Complete Installer screen. The installation wizard of Comodo TrustConnect will start immediately.

Step 1 - Welcome Screen

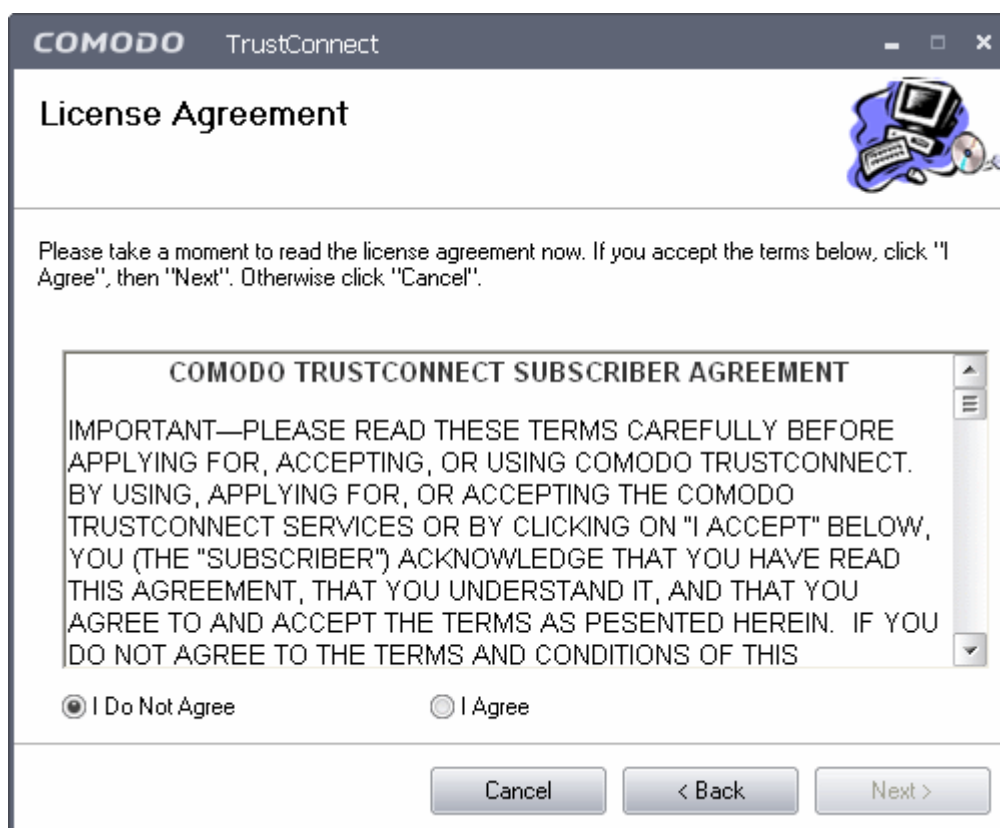
The welcome screen of the wizard will be displayed.



Click 'Next' to continue.

Step 2 - Subscriber License Agreement

Complete the initialization phase by reading and accepting the License Agreement.

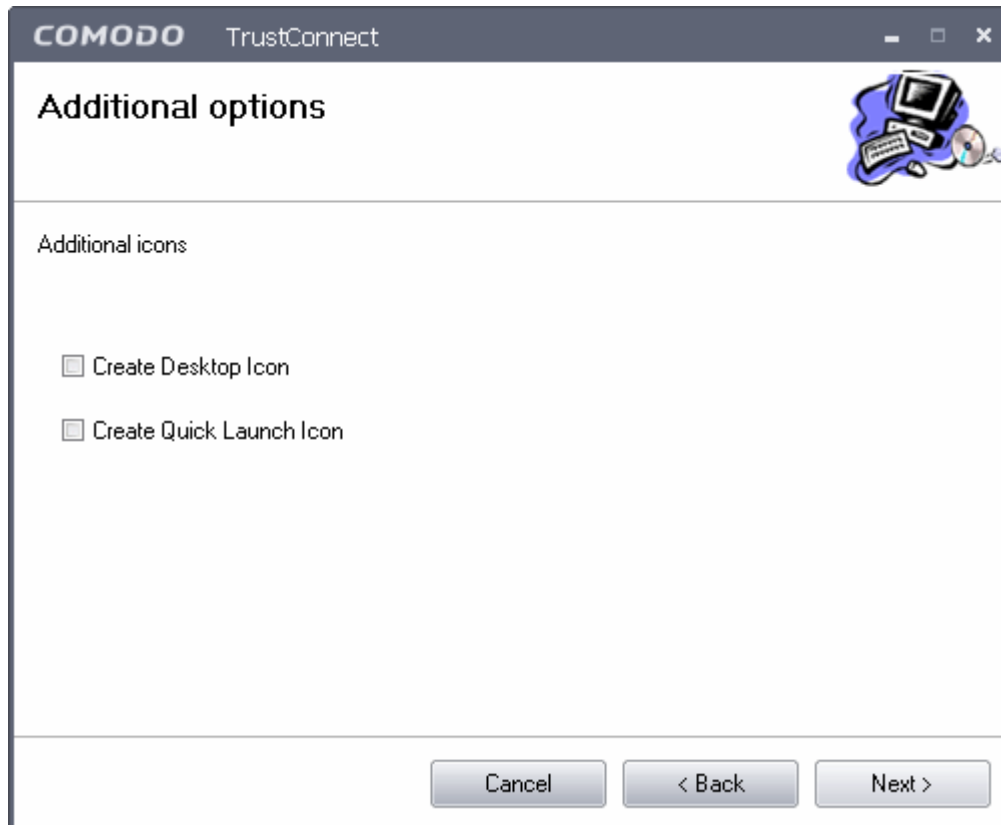


- Select 'I Agree' to continue the installation.
- If you want to cancel the installation at this stage, select 'I Do Not Agree'.

Click 'Next' to continue.

Step 3 - Additional Options

The next stage allows you to select for creation of TrustConnect Desktop icon and TrustConnect quick launch icon, for starting the client from the system tray.



Make your selections and click 'Next' to continue.

Step 4 - Select Installation Folder

The next screen allows you to select the folder in your hard drive for installing Comodo TrustConnect. The default path is *C:\Program Files\Comodo\TrustConnect*.



If you want to install the client in a location other than the default location, click 'Browse' to choose a different location.

- Click 'Next' to continue.

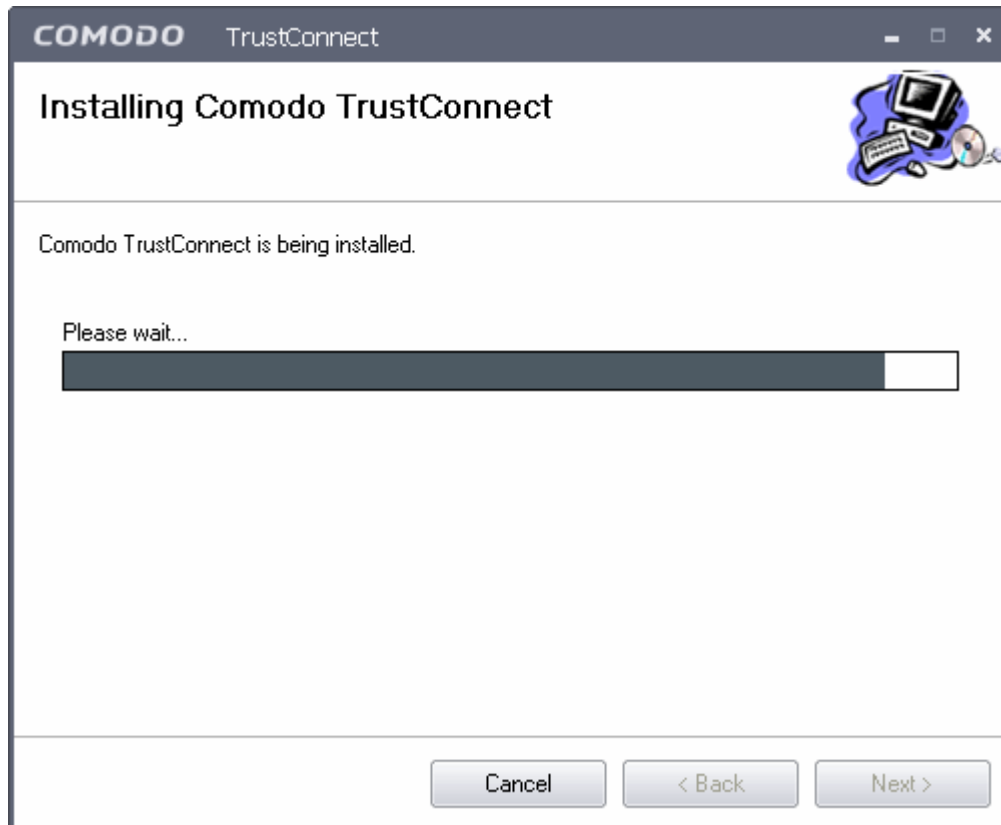
Step 5 - Installation Progress

After completing the configuration options to your satisfaction the setup wizard will ask for confirmation before commencing the installation procedure.

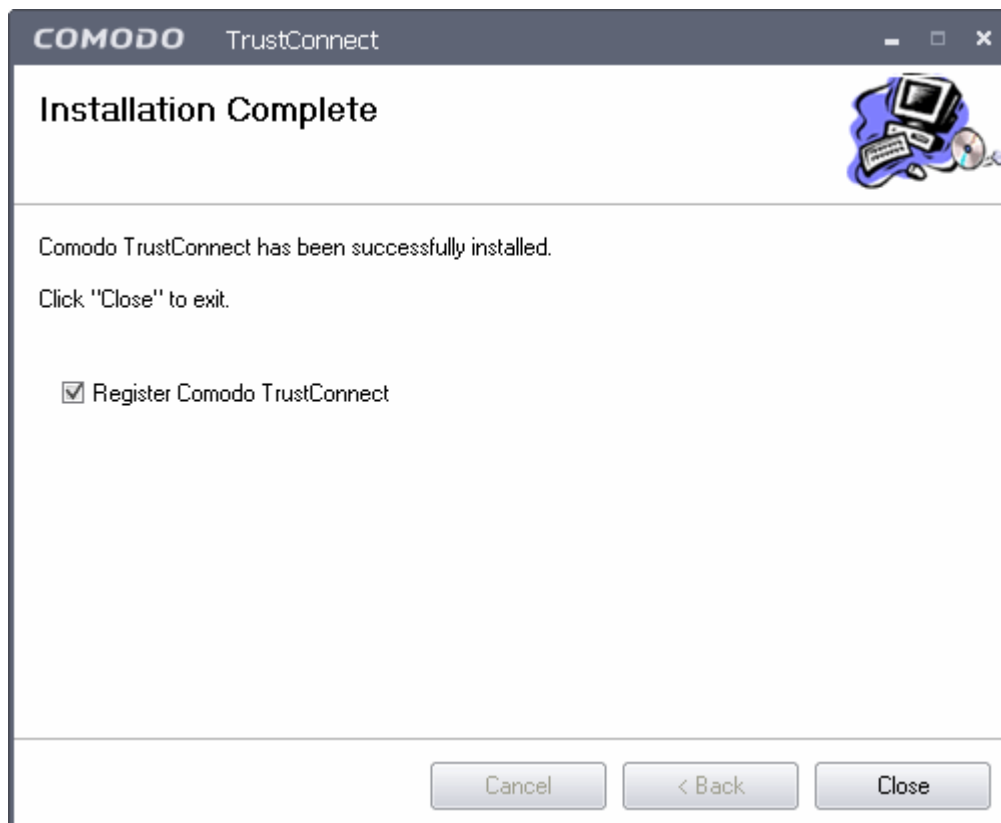


- Click the 'Back' button to review and/or modify any of settings you have previously specified. To confirm your choices and begin the installation of Comodo Internet Security, click 'Next'.

The installation progress will be displayed.

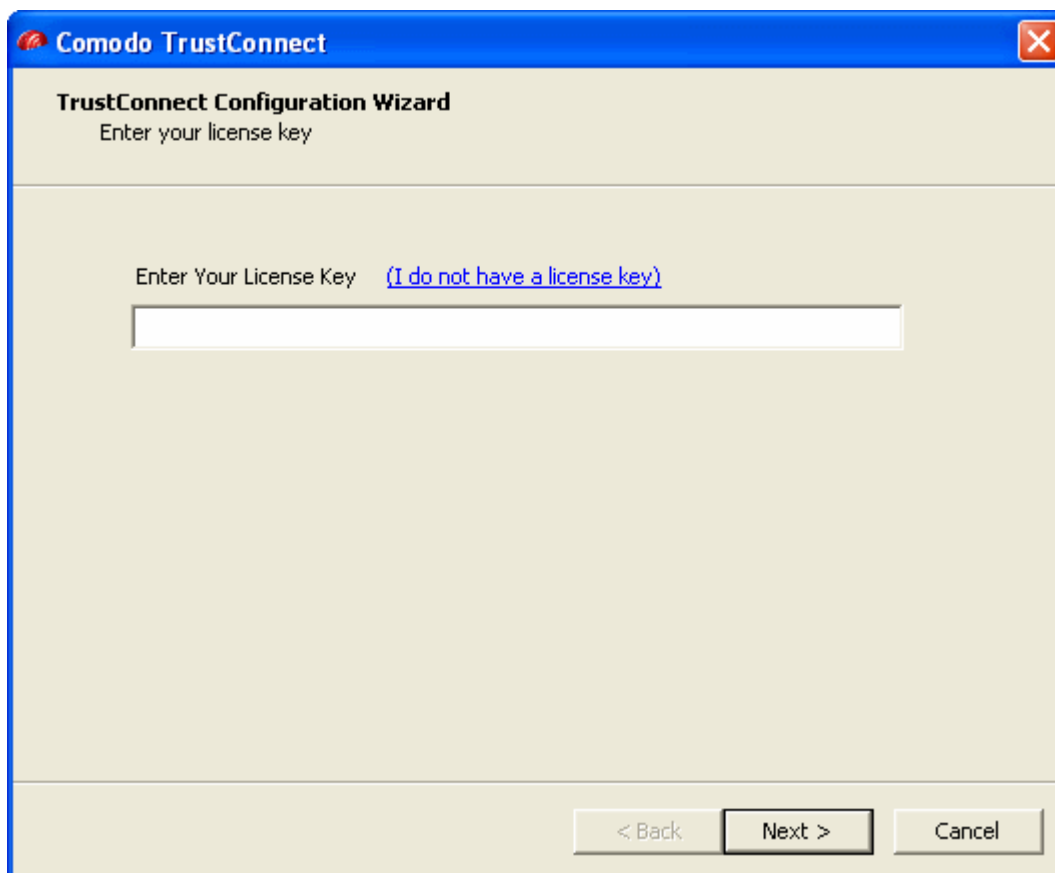


- If any Hardware Installation dialog appears, click 'Continue Anyway'
- On completion, the Installation Complete dialog will be displayed.



- If you have already registered for TrustConnect service through Activate Online Backup and TrustConnect, uncheck the checkbox Register Comodo Trust Connect and click 'Close'. The Installation will be completed.

- If you haven't registered for TrustConnect service through Activate Online Backup and TrustConnect, keep the checkbox Register Comodo Trust Connect checked and click 'Close'. The Registration dialog will be displayed.



- Enter your License Key and click 'Next'.

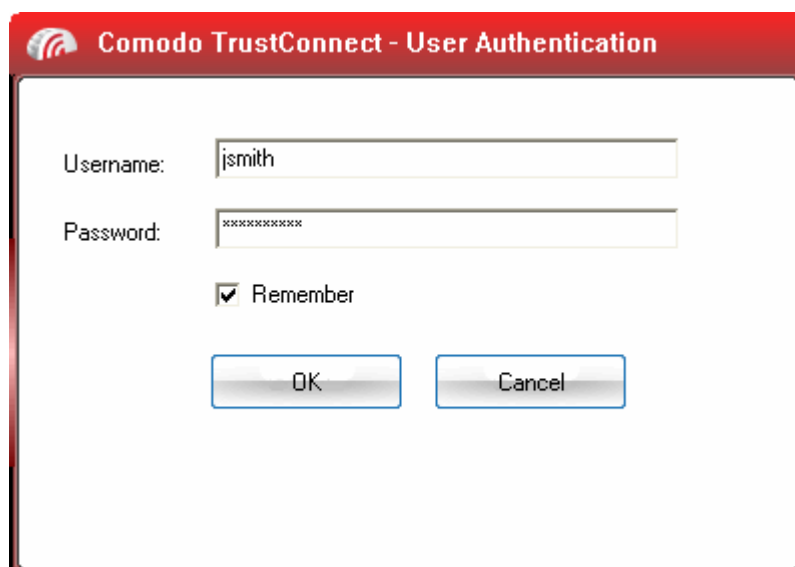
Your key will be validated and activated.



Store the account details in a safe place. You can use TrustConnect in another computer with the same credentials.

- Click 'Finish' to complete the installation.

'Comodo TrustConnect' is now successfully installed in your system.



Full details on using Comodo TrustConnect can be found in the [TrustConnect](#) section of this guide.

1.3.4. Activating CIS Pro/Complete Services after Installation

CIS Pro and CIS Complete enable activation of the license and guarantee coverage even after installation. This is useful in cases where you skipped the process of validating your license during the installation process. Click the links below for detailed explanations:

- [Activating Your License](#);
- [Activating Your Guarantee Coverage](#);
- [Renewal of Your License](#).

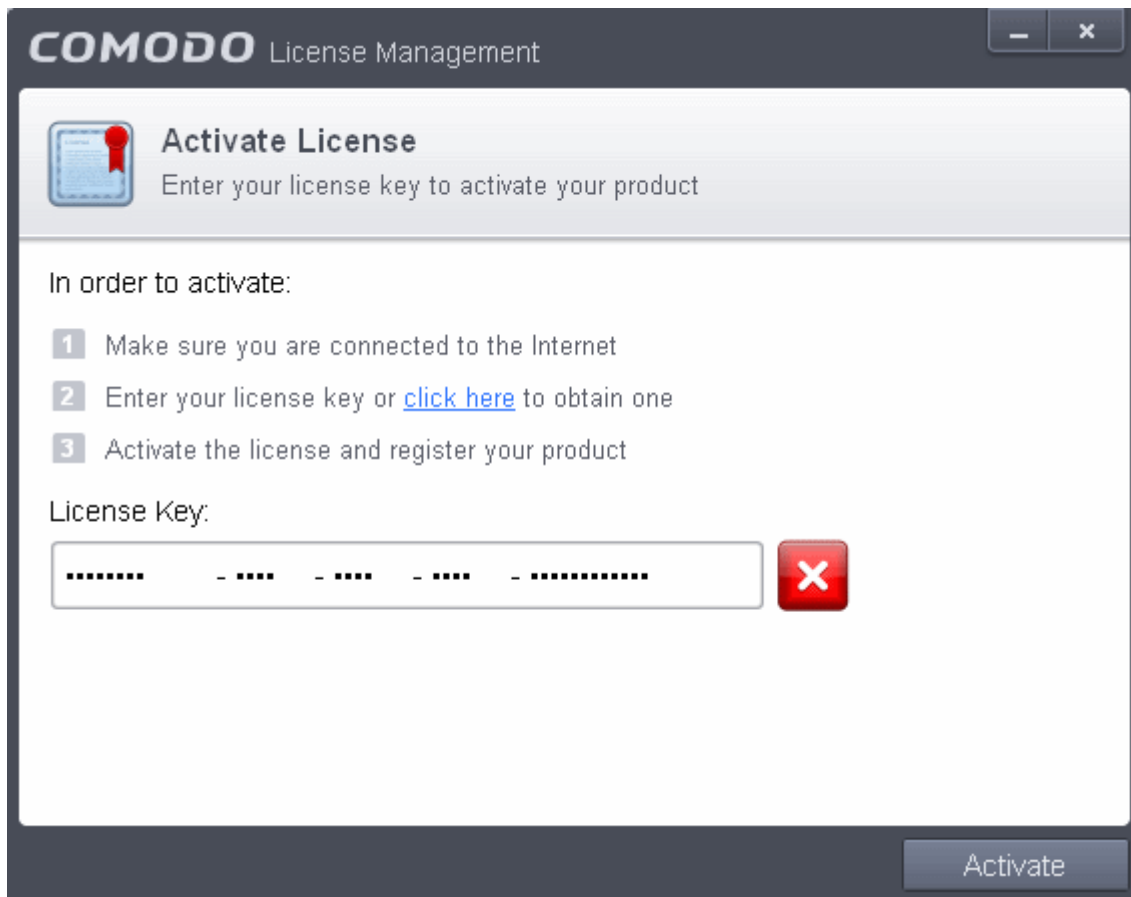
1.3.4.1. Activating Your License

- Start the Comodo Internet Security 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.

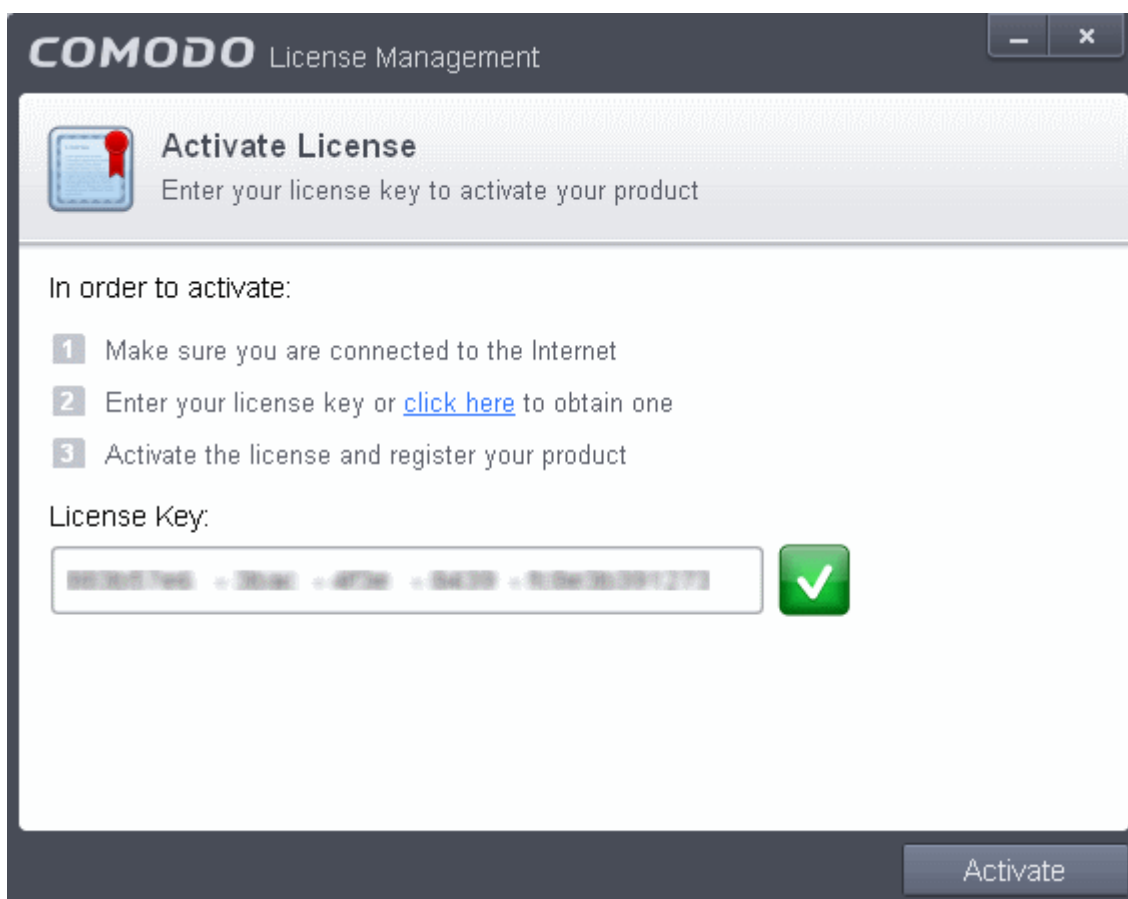


The License Activation Wizard will start.

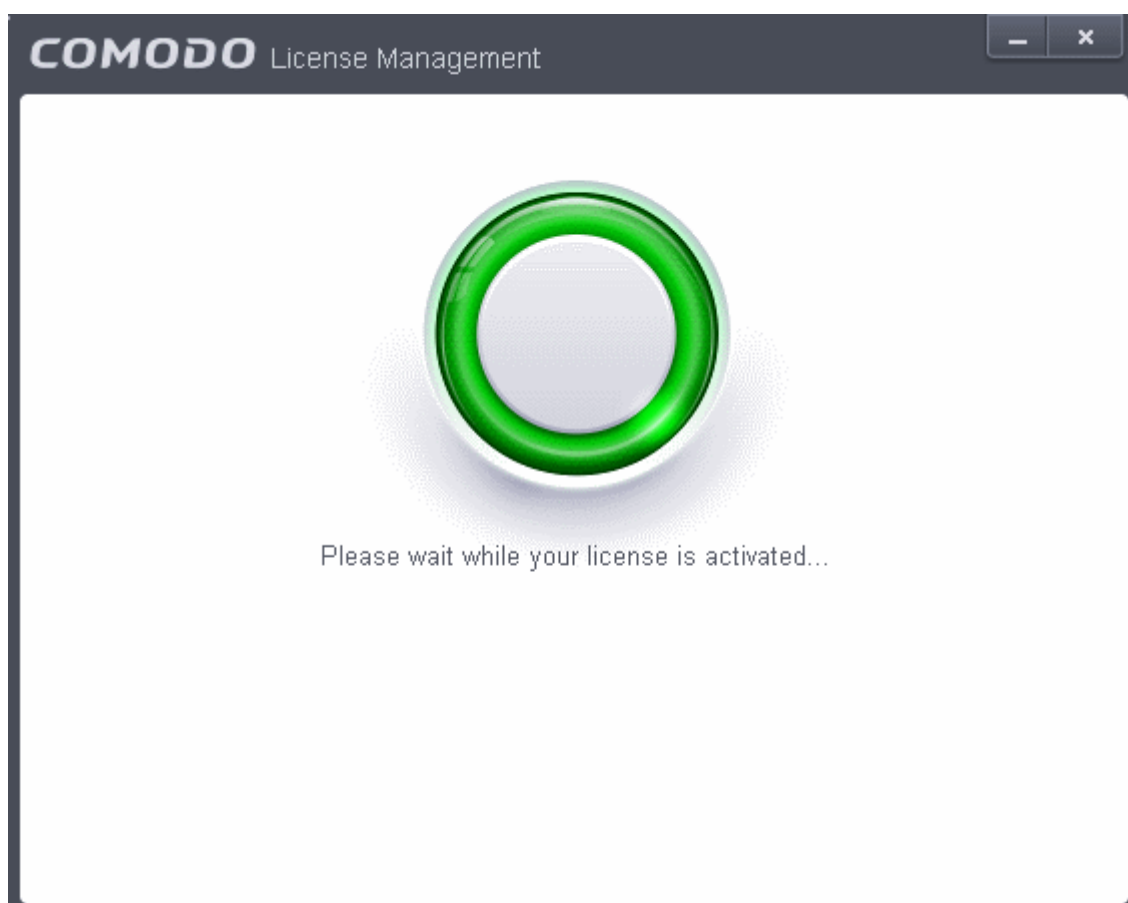


- You should have received your License key through email if you have purchased CIS Pro. For CIS Complete, the license key is available on the DVD itself or printed on an insert included in the box packaging. Enter the license key and click 'Activate'.

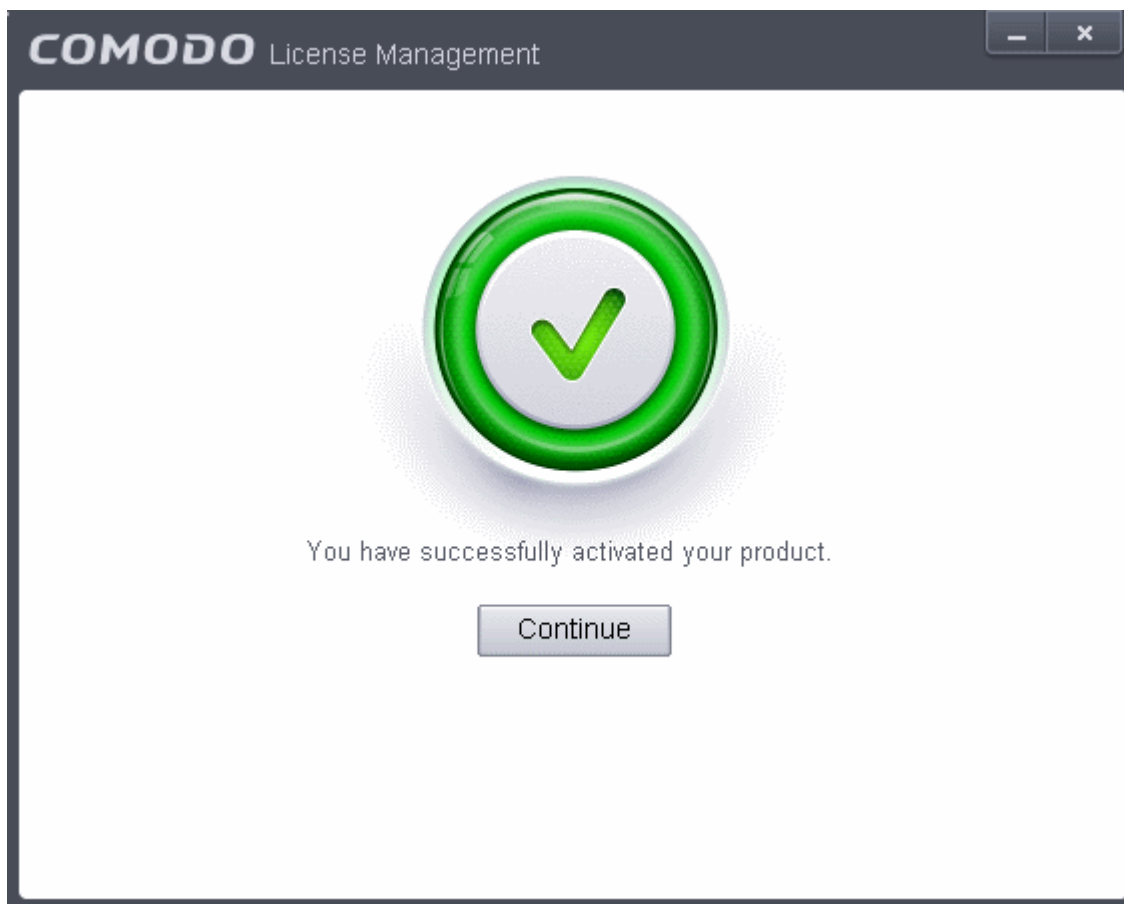
Tip: If you haven't subscribed for Comodo Internet Security - Pro or Complete so far, click the 'click here' link. You will be taken to the Comodo website enabling you to purchase the license.



- The wizard starts validating your key.



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



Click 'Continue' to exit the wizard.

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.

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 for CIS Pro can be found in **CIS Pro - Installation and Activation** and **CIS Complete - Installation and Activation** and in **Activating Your License**.

- 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**).

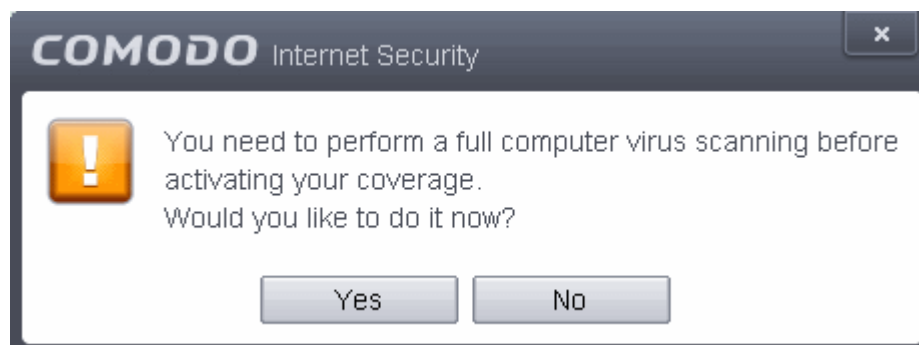
Important Note: Before activating the guarantee, it is essential to run a full computer AV scan with the latest version of the

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.



A full system scan to remove all known viruses is a mandatory requirement if your computer is to be eligible for guarantee coverage. If this step has already been performed (and your system is clean), then the process moves to **step 2**.



Click 'Yes' to run a full computer 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.

Step 2: The next stage is to run the Guarantee Activation Wizard again.

- Click 'Not Activated' beside 'Guarantee:' again. The Guarantee Activation Wizard will start.

http://accounts.comodo.com'. A legend indicates '* Mandatory Field'. A 'Register' button is located at the bottom right of the form."/>

COMODO License Management

Register Product
Enter user details to register your product

* First Name * Last Name

* Email Address

Country City State

Address

Choose a username and password and create a COMODO account. You can use your account to manage your licenses through <http://accounts.comodo.com>

* Username * Password

* Mandatory Field

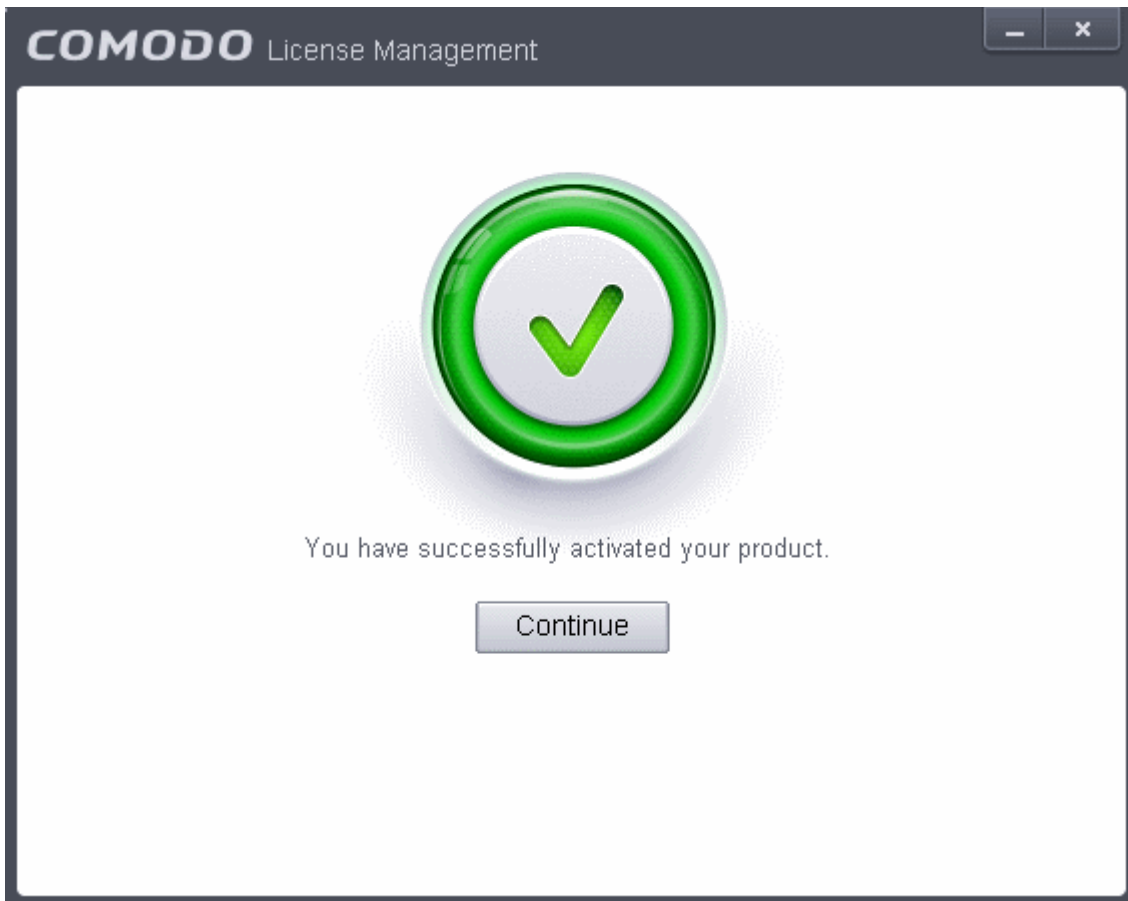
Register

- Fill up the registration form with the login details and password of 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
Create a new COMODO Account	
<ul style="list-style-type: none"> • Enter the login (your email address) and password you submitted while signing up for CIS Pro/Complete 2013 • If you have not signed up for an account, enter your username and password to create a new Comodo account with Comodo Accounts Manager (CAM) 	

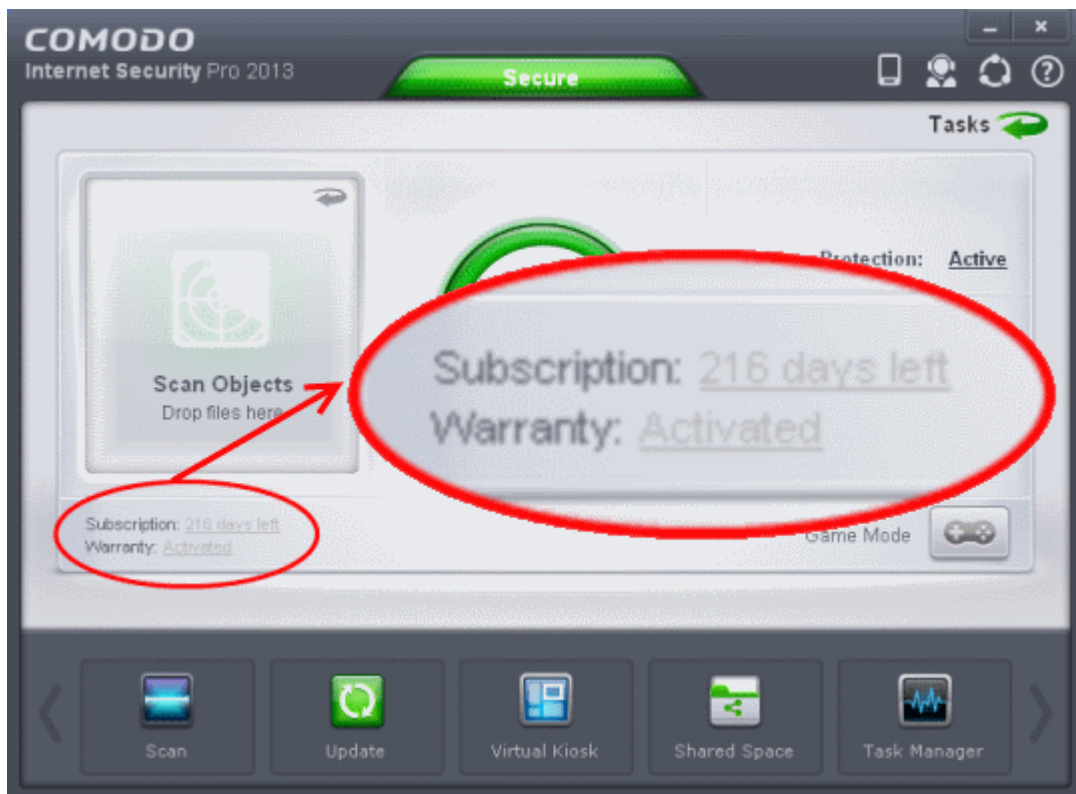
- Click 'Register'

Your guarantee coverage will be registered and on completion, a final confirmation screen indicating successful activation of the Guarantee will be displayed.



- Click 'Continue' to complete the activation wizard

Successfully activating your Guarantee will change the information displayed in the bottom left of the main interface.

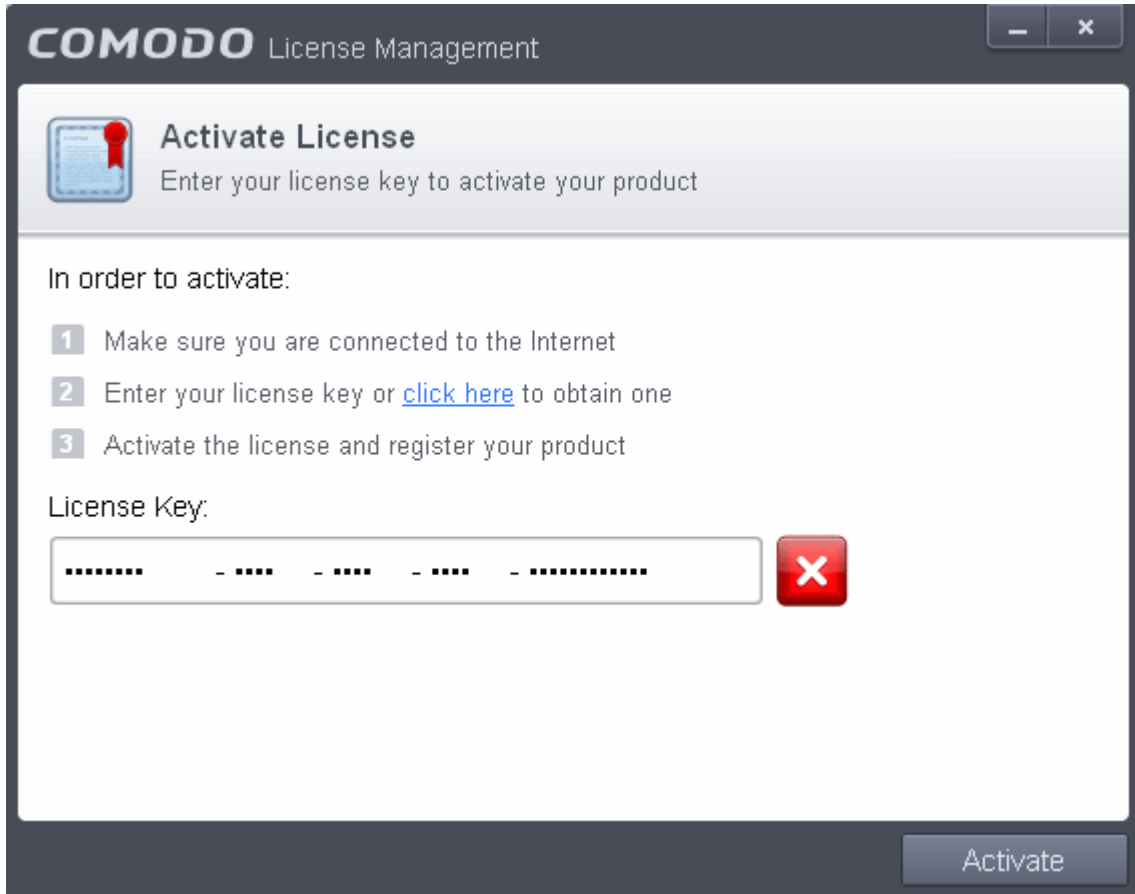


1.3.4.3. Renewal of Your License

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 your license, click 'Activate Now' beside 'License:' from the bottom left corner of the main interface.

The Product Activation Wizard will start.



- Click the '[click here](https://secure.comodo.com/home/purchase.php?afi=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUizRKY&lid=&)' link. You will be taken to <https://secure.comodo.com/home/purchase.php?afi=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 automatically starts whenever you start Windows and the CIS Widget will be displayed. In order to configure and view settings within Comodo Internet Security, you need to access the main interface.

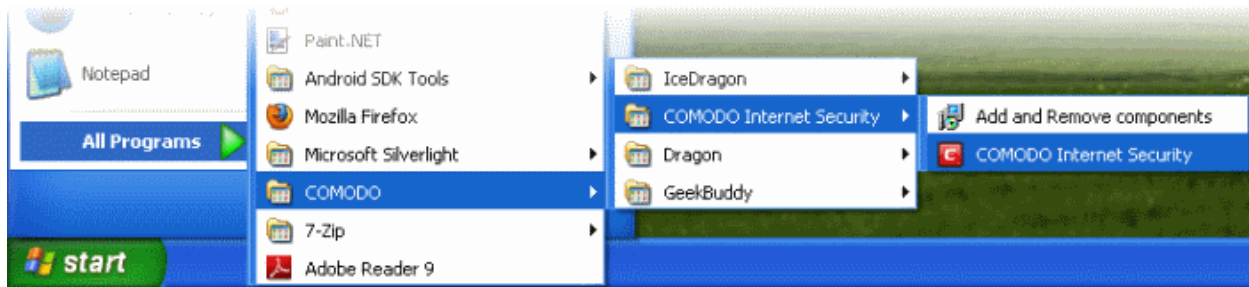
There are 4 different ways to access the main interface of Comodo Internet Security:

- **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**.



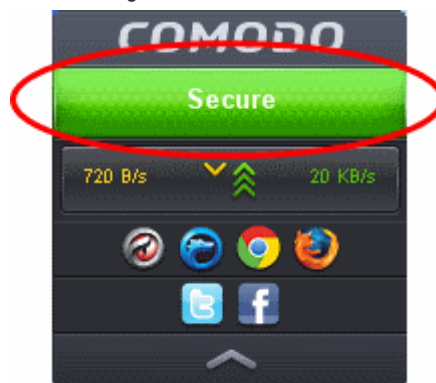
Windows Desktop

- 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.



By right-clicking on the tray icon, you can access short cuts to selected settings such as enabling or disabling Antivirus real-time scan, Firewall, Behavior Blocker, Widget and Game Mode option.

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:

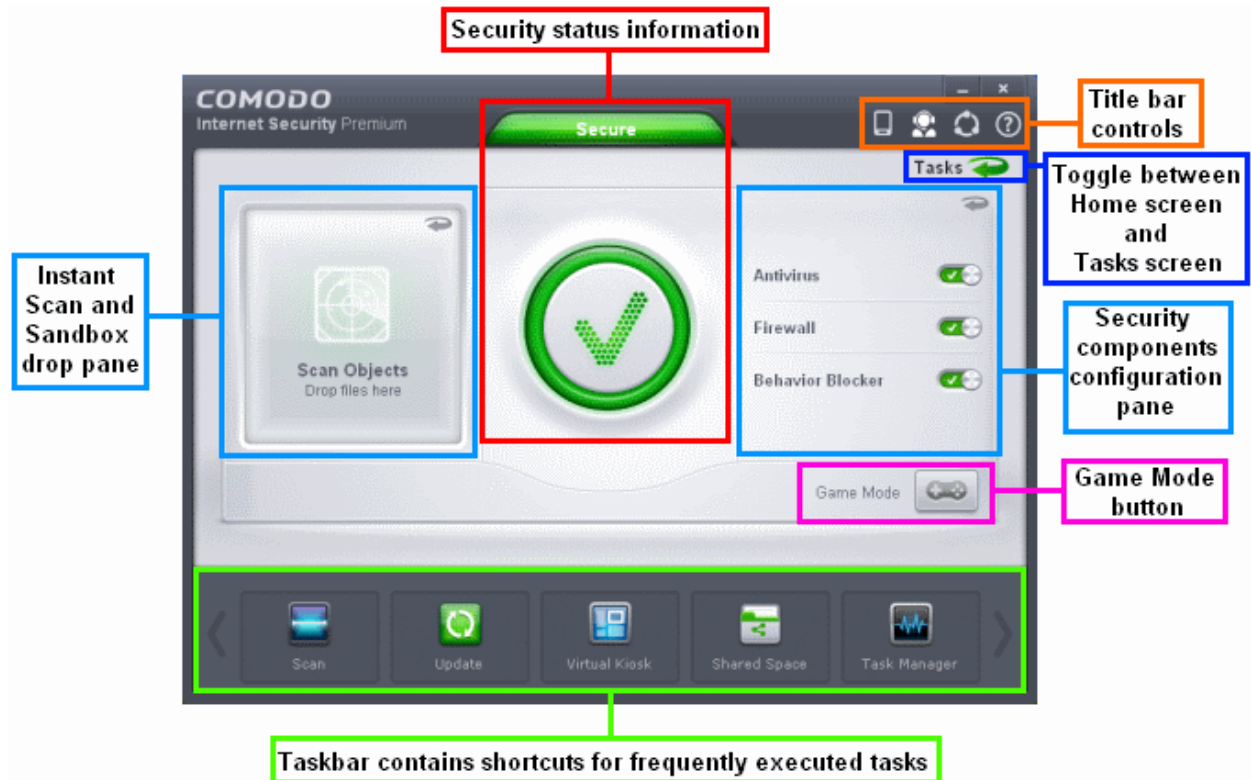
- Defense+/Firewall alerts are suppressed as if they are in training mode;
- AV database updates and scheduled scans are postponed until the gaming is over;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Game Mode to resume alerts and scheduled scans.

Widget - [Click here](#) for more details on CIS Widget.

1.5. The Main Interface


The CIS 6.0 interface has been designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Clicking the curved arrowed on the upper right lets you switch between the **home screen** and the more advanced **tasks interface**. You can instantly run a virus scan on a file or folder by dragging it into the scan box while 'Game Mode' means nothing will interrupt you while you play a full screen game. The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the Virtual Kiosk the update checker and the CIS Task Manager.



Click the following links for more information:

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

1.5.1. The Home Screen

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

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

- [Instantly scan objects / run a program in sandbox](#)
- [Enable or disable security components](#)
- [Adding tasks to the Task Bar](#)
- [Title bar controls](#)

- **Game mode**

Instantly scan objects / run a program in sandbox

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



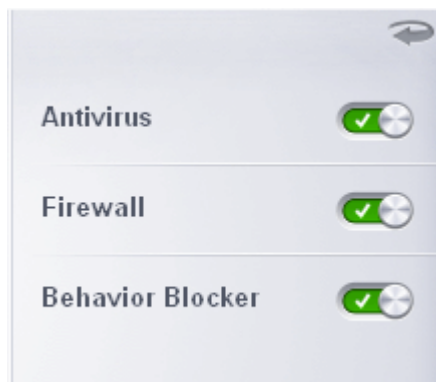
To run an instant scan, navigate to the file/folder that you want to scan and just drag and drop the file into the 'Scan Objects' box. The virus scan will commence immediately. Refer to '[Instantly Scan Individual Files and Folders](#)' for more details.

To run a program in a sandbox, first flip the pane by clicking the curved arrow at the top right side to display 'Sandbox Objects'.

Now, navigate to the program that you want to run in sandboxed environment and just drag and drop it into the box. The program will start as usual but will be run in the CIS sandbox. Refer to '[Run an application in a sandbox](#)' for more details.

Enable or disable security components

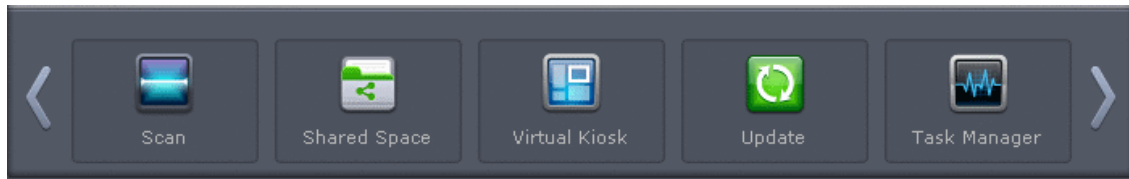
The flippable pane on the right allows you to selectively enable real-time antivirus, the firewall and/or the behavior blocker. The other side of the pane displays the status of real-time protection and when the virus database was updated.




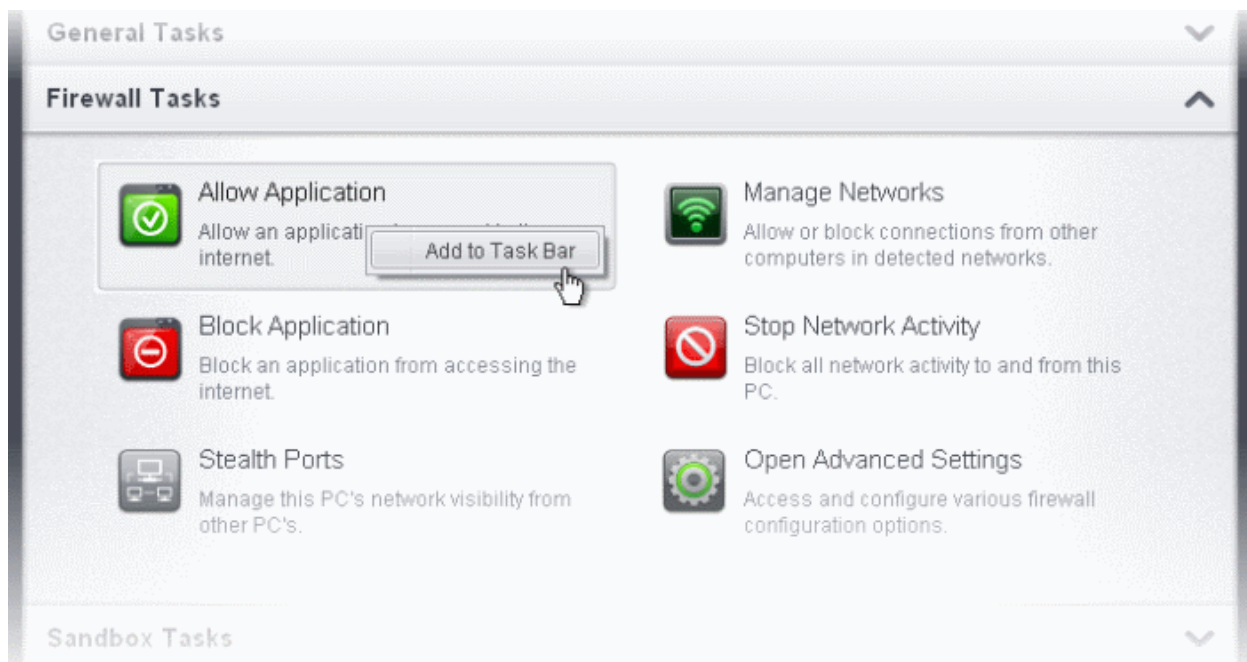
- **Antivirus** - Click the button at the right side of the bar to enable or disable real-time antivirus scanning. Refer to the section '[Real-time Scanner Settings](#)' for more details.
- **Firewall** - Click the button at the right side of the bar to enable or disable firewall protection. Refer to the section '[Firewall Behavior Settings](#)' for more details.
- **Behavior Blocker** - Monitors the behavior of software and files in your system and prevents them from taking actions that would cause damage. Refer to the section '[Behavior Blocker](#)' for more details.

Adding tasks to the Task Bar

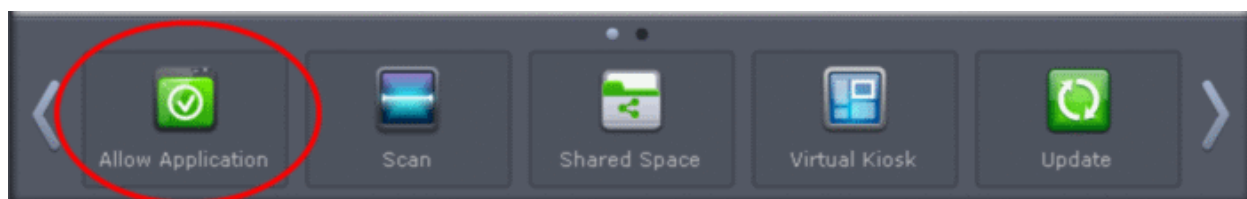
The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles to the left and right sides to scroll through all tasks.



- To add a task to the Task Bar, first open the tasks interface by clicking the curved arrow: 
- Expand any one of the General, Firewall, 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 Settings' then right-click on 'Open Advanced Settings' and select 'Add to Task Bar'.

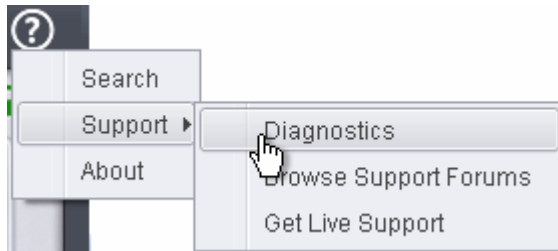
Title bar controls

The title bar (top right) contains shortcuts for:

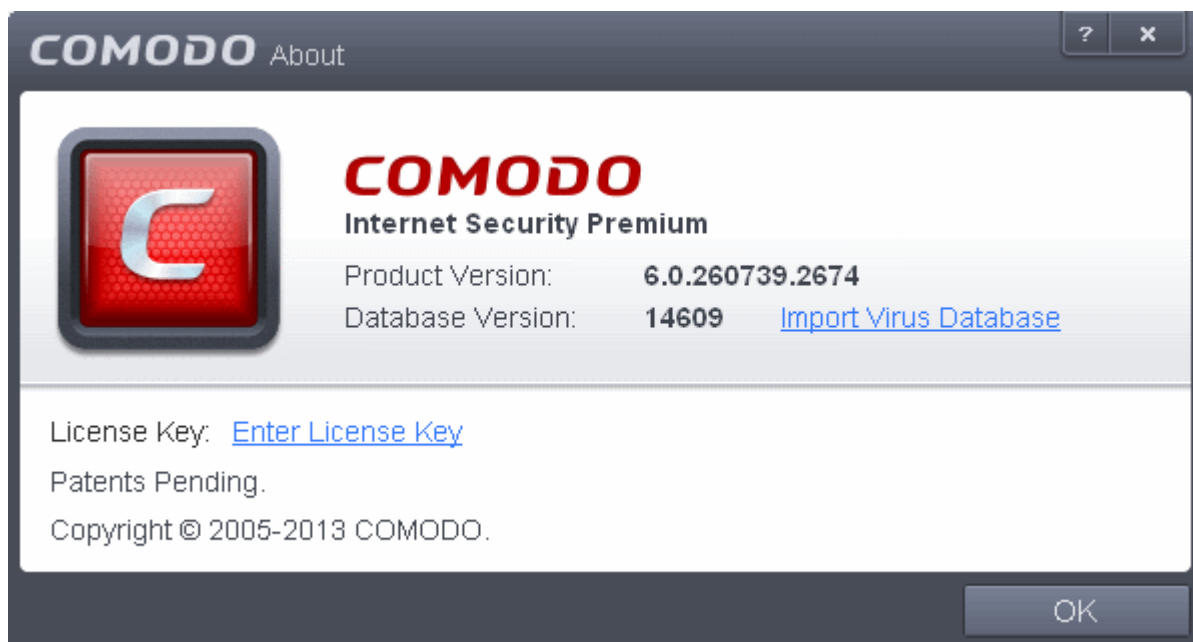
- CIS for Android based Mobile or tablet - Click the mobile icon  and scan the QR code in the image to download the latest Comodo Internet Security Mobile. See <https://m.comodo.com/> for more details.
- Talk to a Certified Technician - Click the  icon to launch the GeekBuddy client and connect to a real-life Comodo security expert. Refer to the topic **Comodo GeekBuddy** for more details..
- Refer your Friends - Click the  icon to open Comodo's Facebook page and refer your friends to Comodo's various

products.

- Get Help - Click the help icon  for the following options:



- **Search** - Opens Comodo Internet Security's online help guide at <http://help.comodo.com/topic-72-1-451-4685-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 product version, virus signature database version and copy-right information of the product. The 'About' dialog also allows you to import a locally stored virus database and to upgrade to CIS Pro version.



- Clicking [Import Virus Database](#) enables you to import a locally stored virus signature database into CIS
- Clicking [Enter License Key](#) allows you to upgrade your product to CIS Pro version. Refer to the section '[Activating CIS Pro/Complete Services after Installation](#)' for more details

Game mode

Switches CIS 2013 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.
- 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.

1.5.2. The Tasks Interface

The links in the 'Tasks' interface allows 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 view running security tasks. 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 advanced 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.

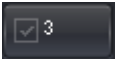

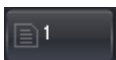
1.5.3. The Widget

The CIS Widget is a handy control that provides at-a-glance information about the security status, speed of outgoing and incoming traffic and links to social networking sites. The Widget starts automatically when CIS is started 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 on right clicking 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. 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 Comodo KillSwitch application, which allows you to identify and terminate unnecessary processes. 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.
- The second button  tells you how many CIS tasks are currently running. Clicking the button opens the Windows [Task Manager](#) interface.
- The third button  displays how many files are added to Unrecognized Files list and are pending for submission to Comodo for analysis. Clicking on it opens the [Unrecognized Files](#) interface which displays the list of Unrecognized files.

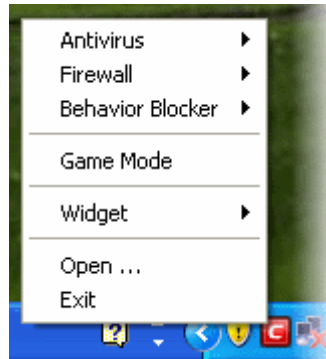
The status row is displayed only if 'Show Status Pane' is enabled under 'Widget options' of CIS tray icon or Widget right click menu. Refer to [The System Tray Icon](#) for more details. (*Default = Disabled*)

- The fourth row contains shortcuts for five common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task. The Common Tasks row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of CIS tray icon or Widget right click menu. Refer to [The System Tray Icon](#) for more details. (*Default = Disabled*)
- The fifth row displays the browsers installed in your computer system. 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 'Widget' options of CIS tray icon or Widget right click menu. Refer to [The System Tray Icon](#) for more details. (*Default = Enabled*)
- The last row in the Widget provides links to social networking sites. The social networking sites row is displayed only if 'Show Connect Pane' is enabled under 'Widget' options of CIS tray icon or Widget right click menu. Refer to [The System Tray Icon](#) for more details. (*Default = Enabled*)
- You can expand or collapse the Widget by clicking the arrow at the bottom.

1.5.4. The System Tray Icon

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

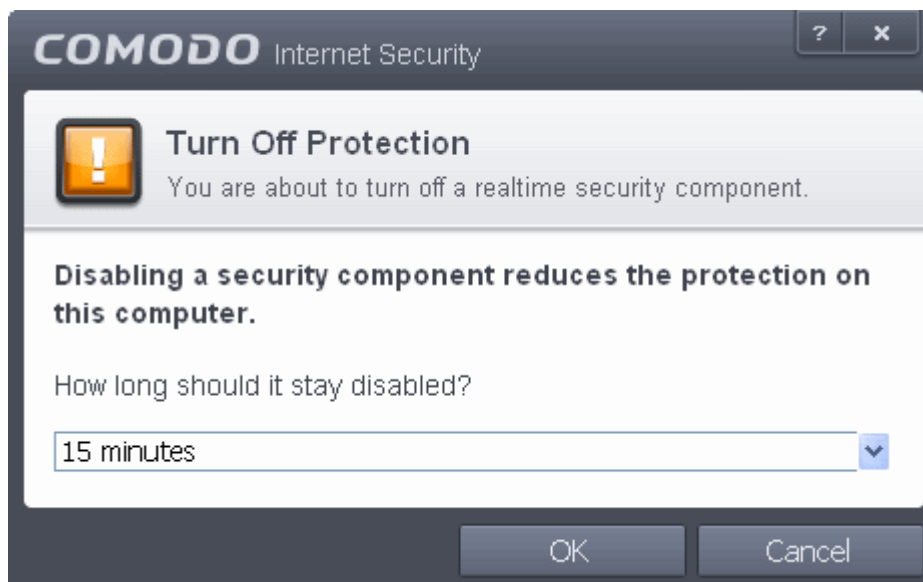
Right-clicking the system tray icon will provide you the option to enable or disable various security settings.



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

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

If any of the above two settings are disabled, immediately the Security Information in the main task interface and the Widget will turn red alerting you of the status. In addition, a pop-up alert will be displayed.



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



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

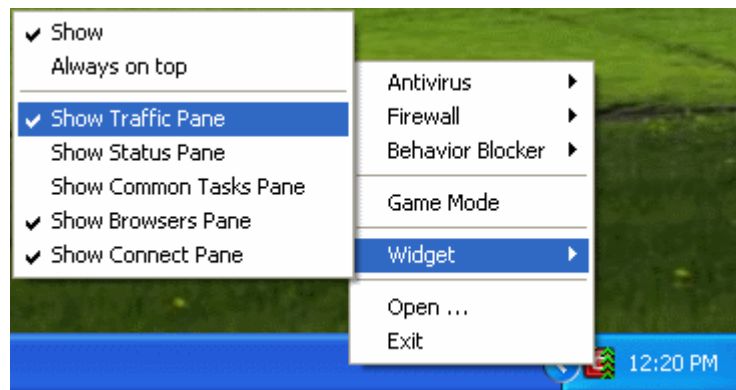
- **Behavior Blocker** - You can enable or disable Behavior Blocker. [Click here](#) to know more about Behavior Blocker.
- **Game Mode** - Switches CIS 2013 to Game Mode to enable you to play your games without any interruptions from various alerts in your computer. The operations that can interfere with users' gaming experience are either suppressed or postponed.

In game mode:

- Defense+/Firewall alerts are suppressed.
- 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** - You can select whether or not the **Widget** is to be displayed and select the components of it to be displayed.



- **Show**: Toggles the display of widget. (*Default = 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 indication row in the widget. (*Default = Enabled*)
- **Show Status Pane**: Displays the row indicating the current status of CIS in the widget. (*Default = Disabled*)
- **Show Common Tasks Pane**: Displays the row containing shortcuts to common CIS tasks in the widget. (*Default = Disabled*)
- **Show Browsers Pane**: Displays the row containing the shortcuts to browsers in your computer. (*Default = Enabled*)
- **Show Connect Pane**: Displays the row containing the shortcuts to social networking sites in the widget. (*Default = Enabled*)
- **Open** - Opens the CIS interface.
- **Exit** - Closes the CIS application.

1.6. Understanding Security Alerts

CIS alerts warn you about security related activities and requests at the moment they occur. Each alert contains information about the particular issue so you can make an informed decision about whether to allow or block it. Alerts also allow you to tell Comodo Internet Security how to behave in future when it encounters activities of the same type.

Type of Alert
Can be Antivirus, Firewall, HIPS, Behavior Blocker or Cloud Scanner

Color indicates severity of the Alert
Both firewall, HIPS and Behavior Blocker alerts are color coded to indicate the risk level

Description of activity or connection attempt

High visibility icons quickly inform you which applications and techniques are involved in an alert. Clicking the name of the executables here opens a window containing more information about the application in question

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

Click these options to allow or block the request

The screenshot shows a 'COMODO Behavior Blocker' alert for 'installer_r20.0.3-windows.exe'. It features a red shield icon with a white cross, indicating a high-risk alert. The alert text states that the application could not be recognized and requests unlimited access to the computer. Below the alert, there are three options: 'Run Isolated(Default)' (with a yellow warning icon), 'Run Unlimited' (with a green checkmark icon), and 'Block' (with a red 'no' icon). A 'Trust this application' checkbox is at the bottom.

Comodo Internet Security alerts come in four main varieties, namely:

- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when **Antivirus is enabled** and the option '**Do not show antivirus alerts**' is disabled in **Real-time Scanner Settings**.
- **Firewall Alerts** - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the **Firewall is enabled** and the option '**Do not show popup alerts**' is disabled in **Firewall Settings**.
- **HIPS Alerts** - Shown whenever an application attempts an unauthorized action or tries to access protected areas. HIPS alerts will only be generated if **HIPS is enabled** and **Do NOT show popup alerts** is disabled.
- **Behavior Blocker / Auto-Sandbox Alerts (including Elevated Privilege Alerts)** - Shown whenever an application tries to modify the Operating System or related files and when the Behavior Blocker automatically sandboxes an unrecognizable file. Behavior Blocker / Auto-Sandbox Alerts will be displayed only when **auto-sandboxing is enabled** under **Behavior Blocker settings**. Privilege Alerts will only be shown **if enabled**.

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

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

Severity Level

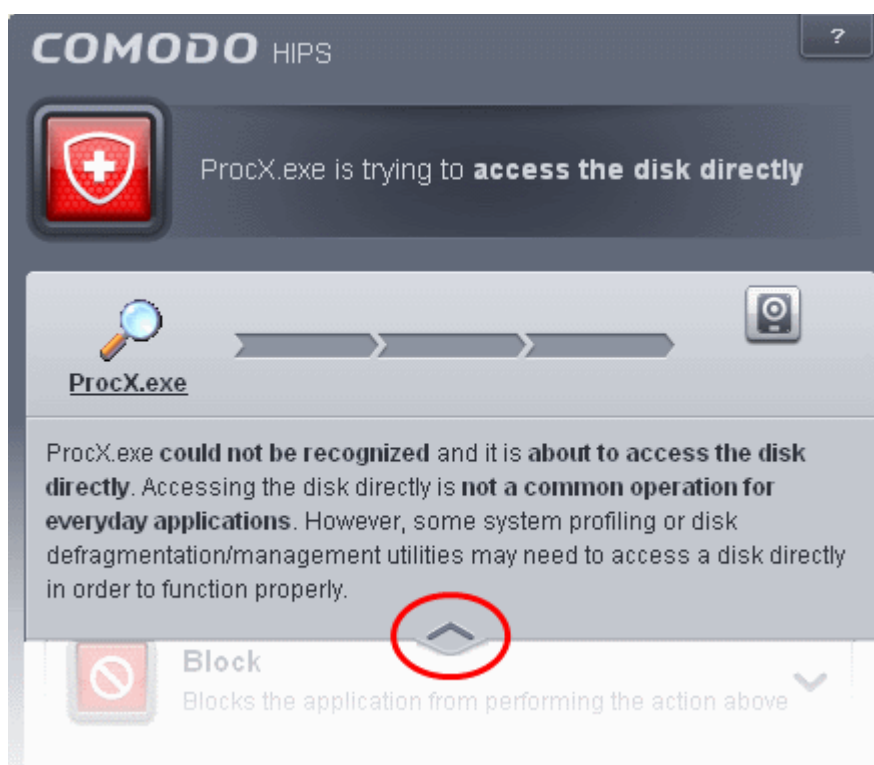
The shield icons at the upper left of each alert are color coded according to the risk level presented by the activity or request. However, it cannot be stressed enough that you should still read the information in order to reach an informed decision on allowing or blocking the activity.

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

Note: Antivirus 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:



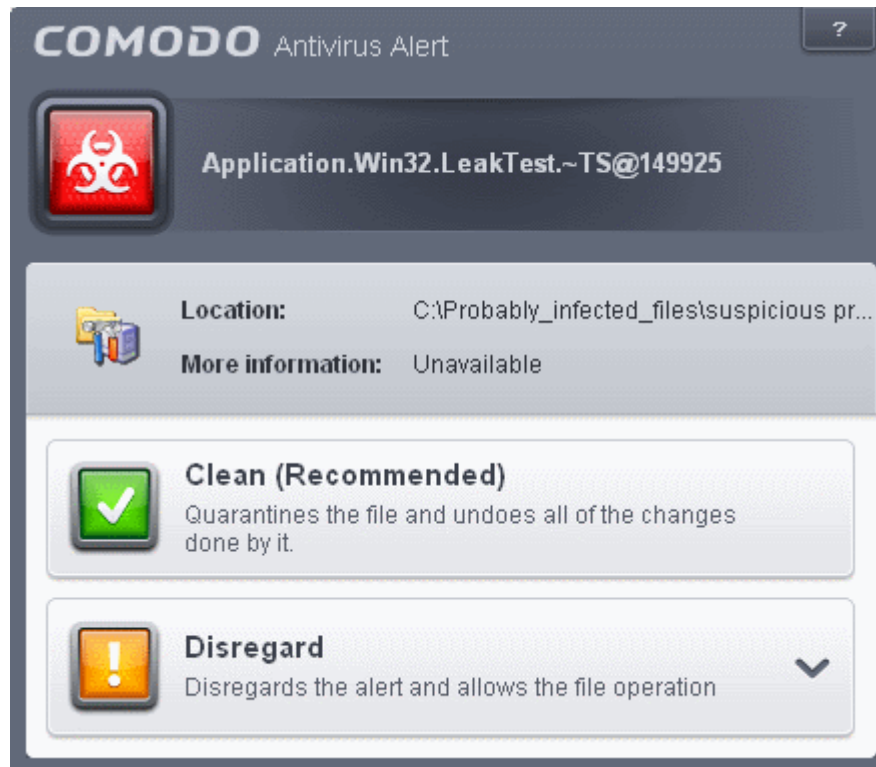
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answering an Antivirus Alert

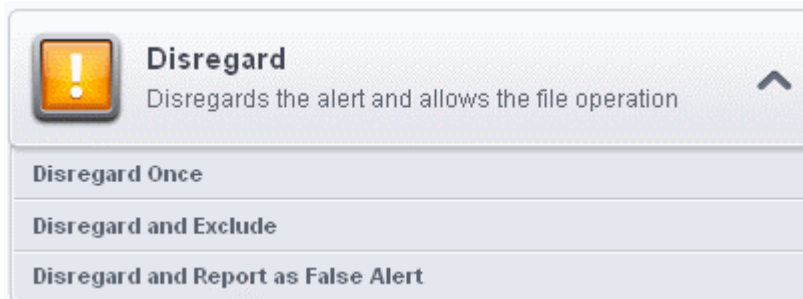
Comodo Internet Security generates an Antivirus alert whenever a virus or virus-like activity is detected on your computer. The alert contains the name of the virus detected and the location of the file or application infected by it. Within the alert, you are also presented with response-options such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

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.



The following response-options are available:

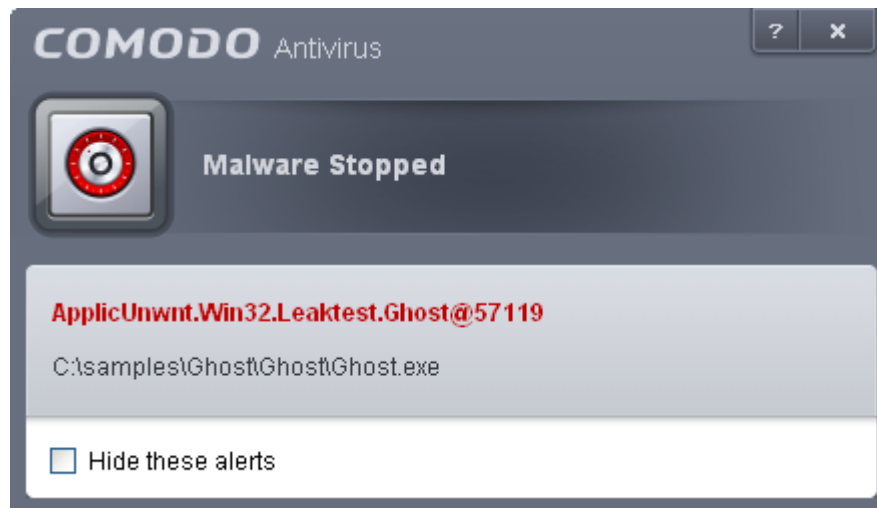
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the **Quarantine** interface. Refer to **Manage Quarantined Items** for more details on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



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

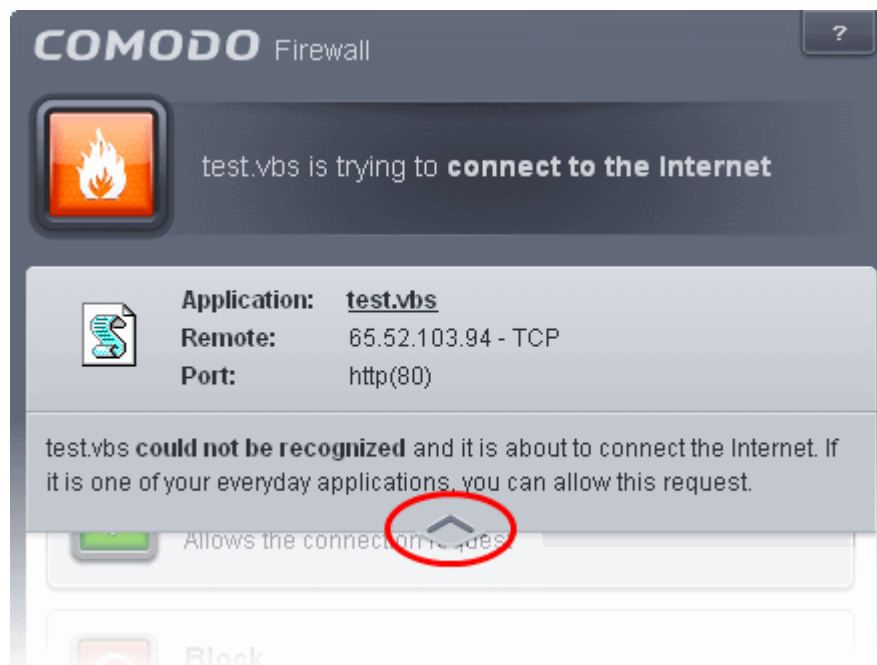


Please note that these antivirus notifications will be displayed only when 'Do not show antivirus alerts' check box in **Antivirus > Real-time Scan settings** screen is selected *and* 'Show notification messages' check box is enabled in **Advanced Settings > User Interface** screen.

Answering Firewall Alerts

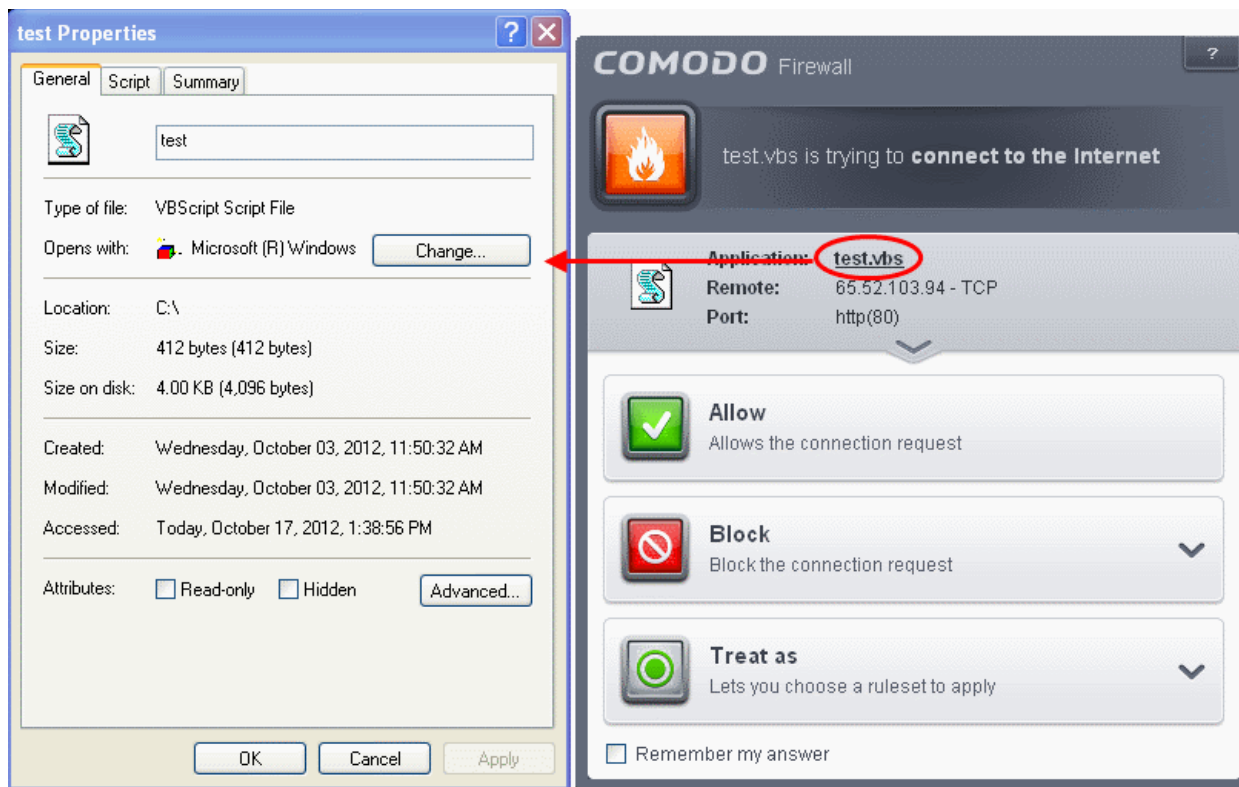
CIS generates a firewall alert when it detects unauthorized network connection attempts or when traffic runs contrary to one of your application or global rules. Each firewall alert allows you to set a default response that CIS should automatically implement if the same activity is detected in future.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

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.

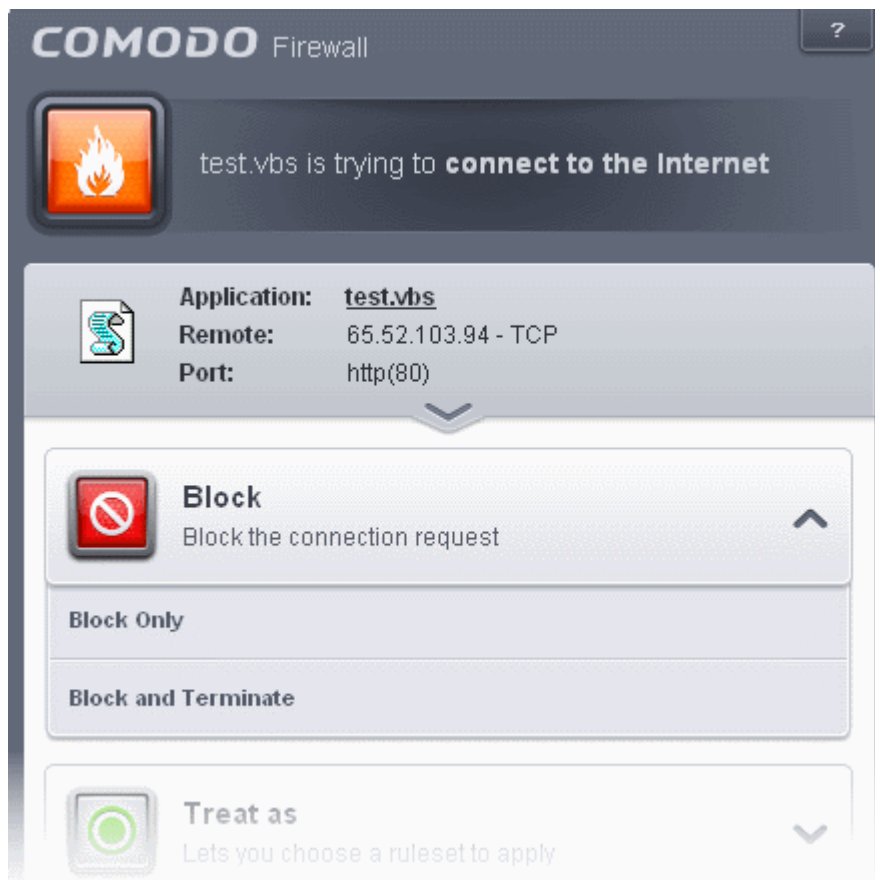


If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.

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

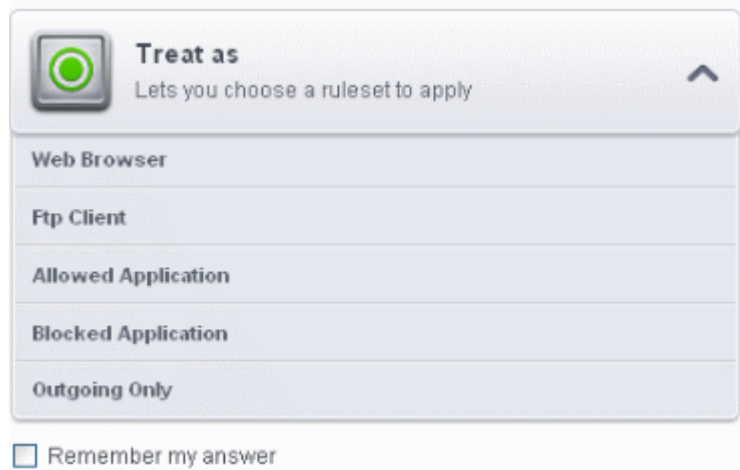


If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand the alert, you can choose to block the connection (connection is not allowed to proceed) or block & terminate (connection is not allowed to proceed and the process/application that made the request is shut down).



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.



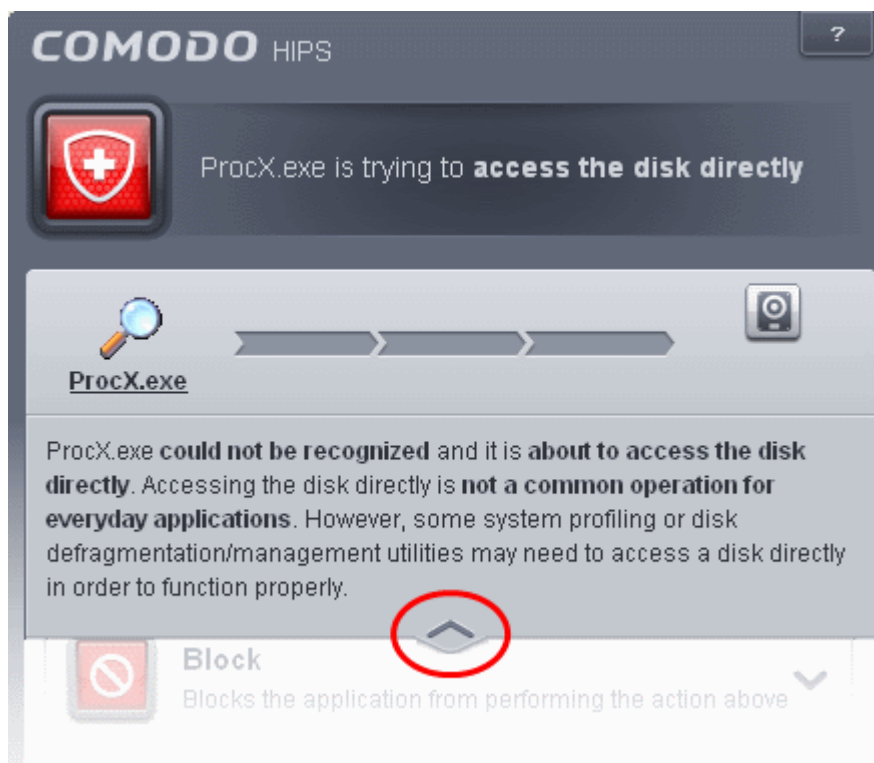
Remember to check the box **Remember My Answer** for the ruleset to be applied in future.

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

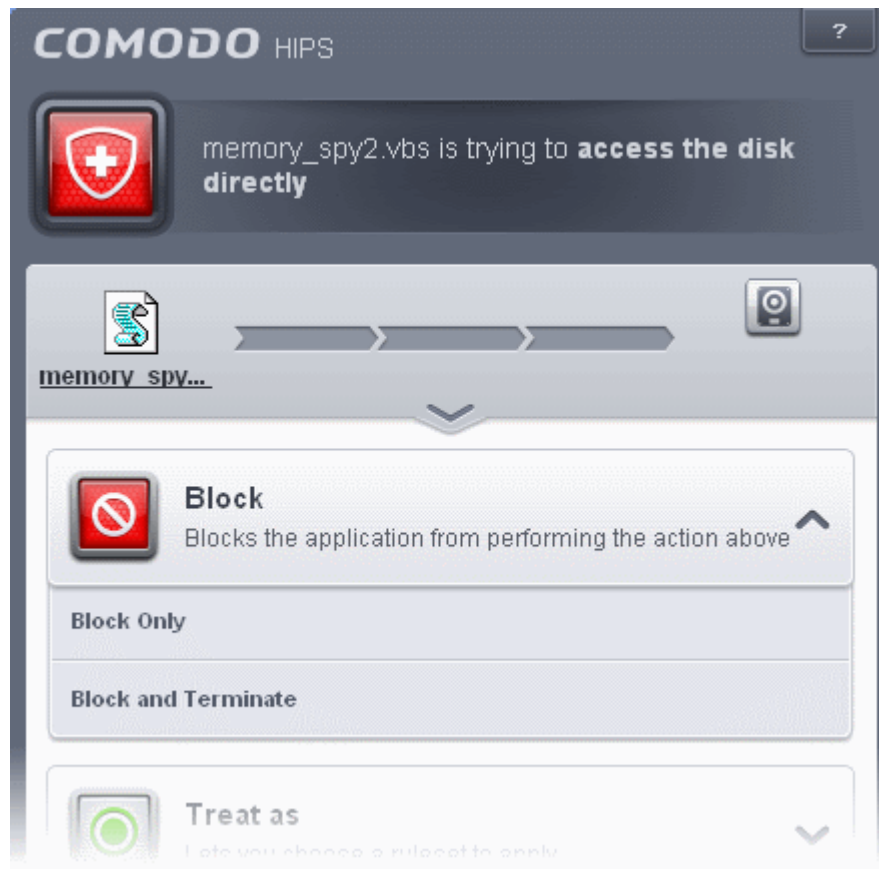
Comodo Internet Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:

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 or to block & terminate.

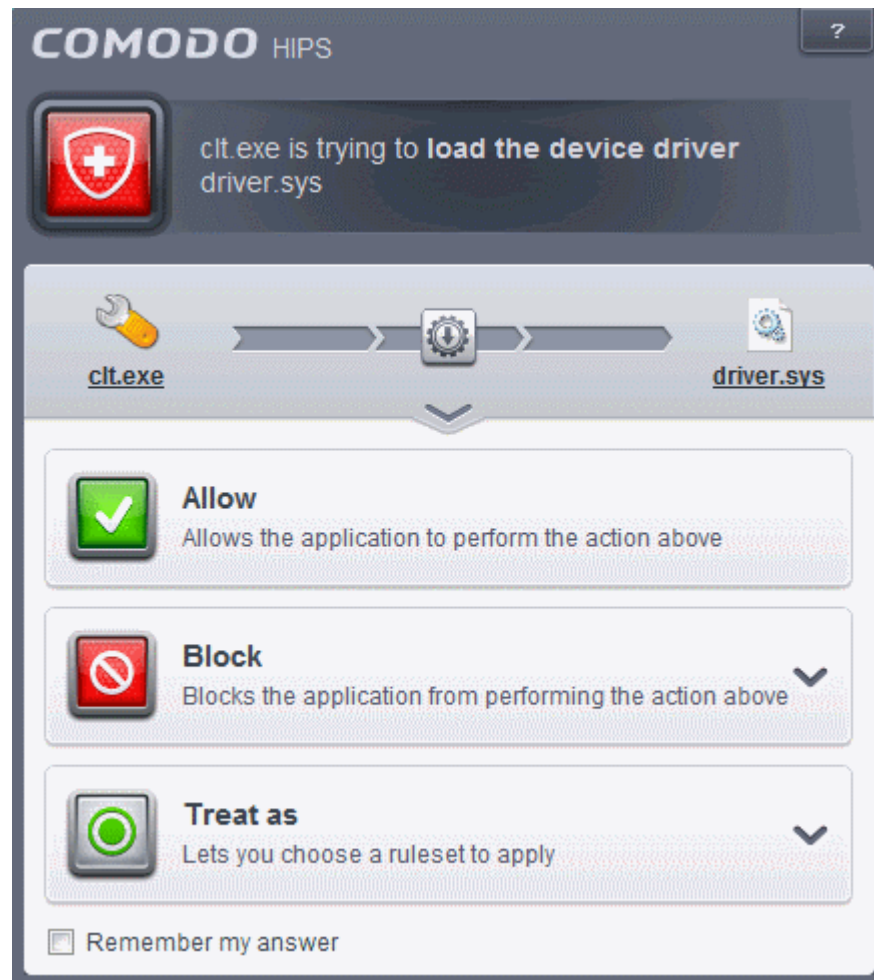


2. If you are sure that it is one of your everyday applications and want to enforce a security policy (ruleset) to it, please use the 'Treat As' option. This applies a **predefined HIPS ruleset** to the target application.

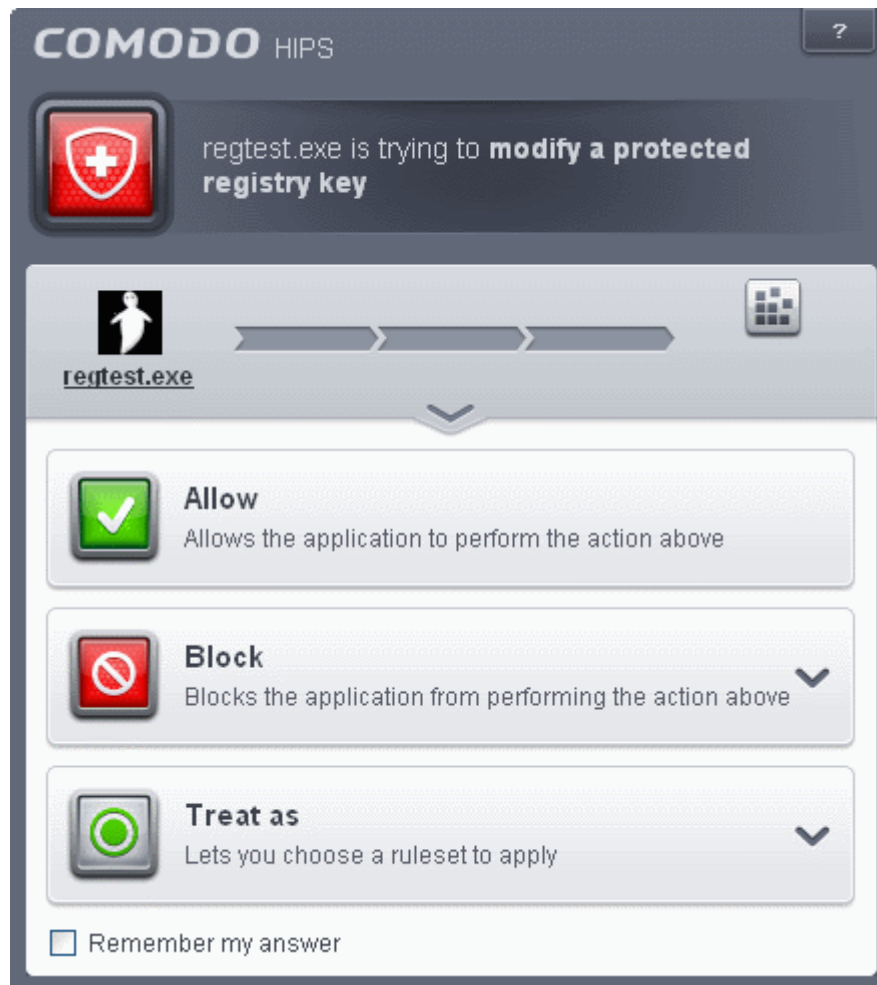


Avoid using the **Installer or Updater** ruleset if you are not installing an application. This is because treating an application as an 'Installer or Updater' grants maximum possible privileges onto to an application - something that is not required by most 'already installed' applications. If you select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

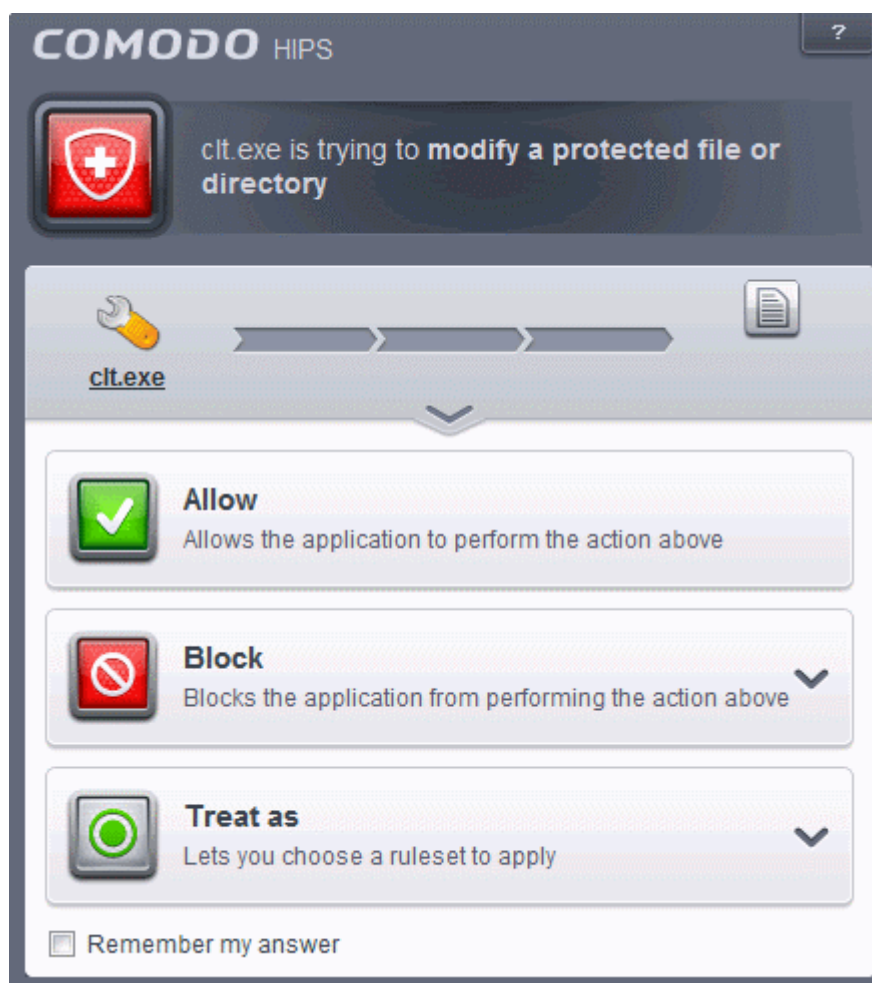
3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity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

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

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

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

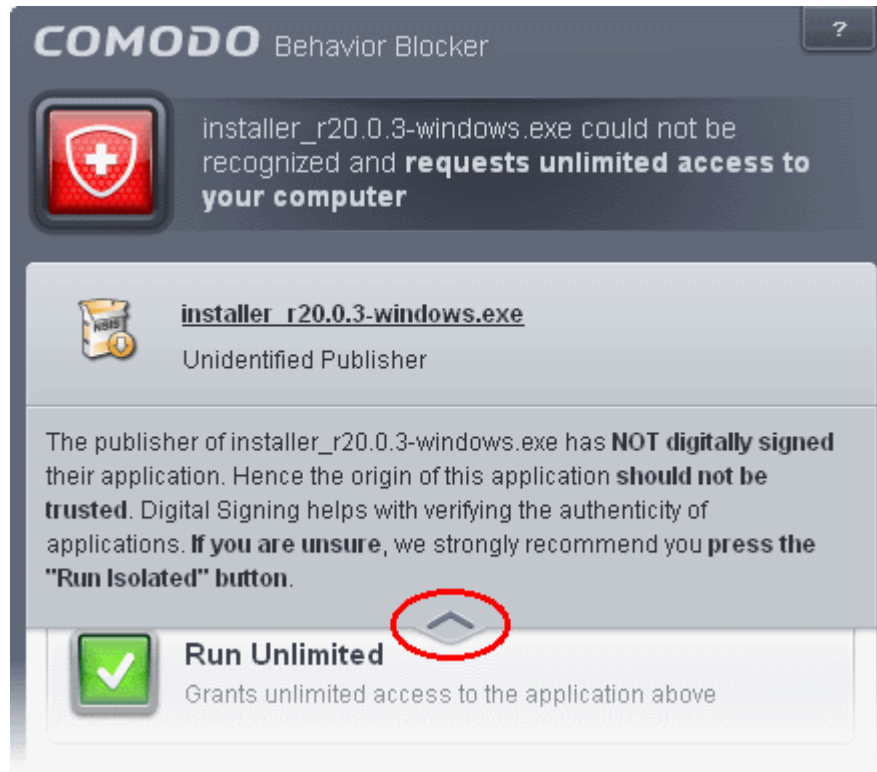
Answering a Behavior Blocker / Auto-Sandbox Alert

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

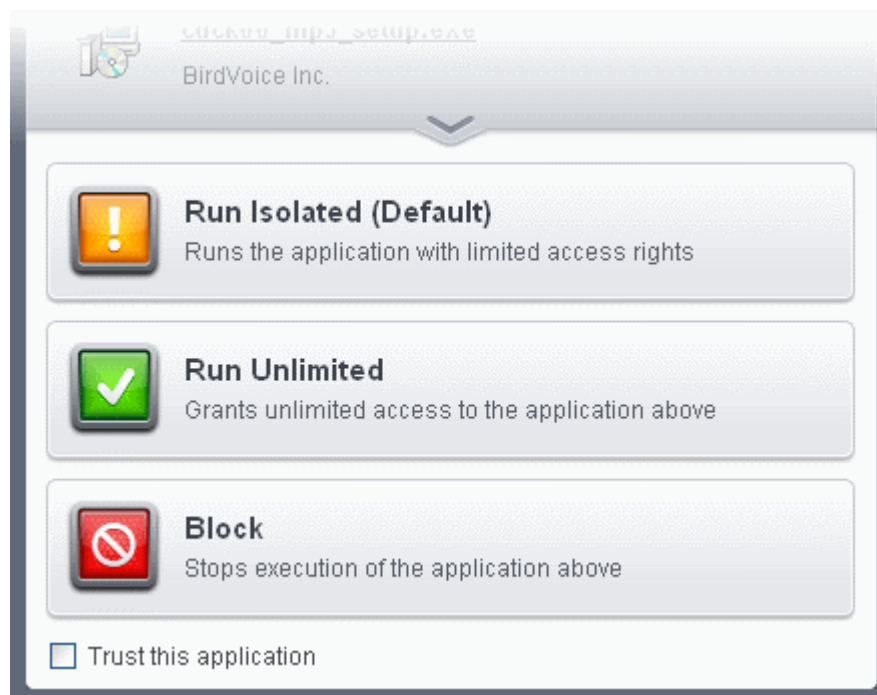
application.

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 Auto-Sandboxing and 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.

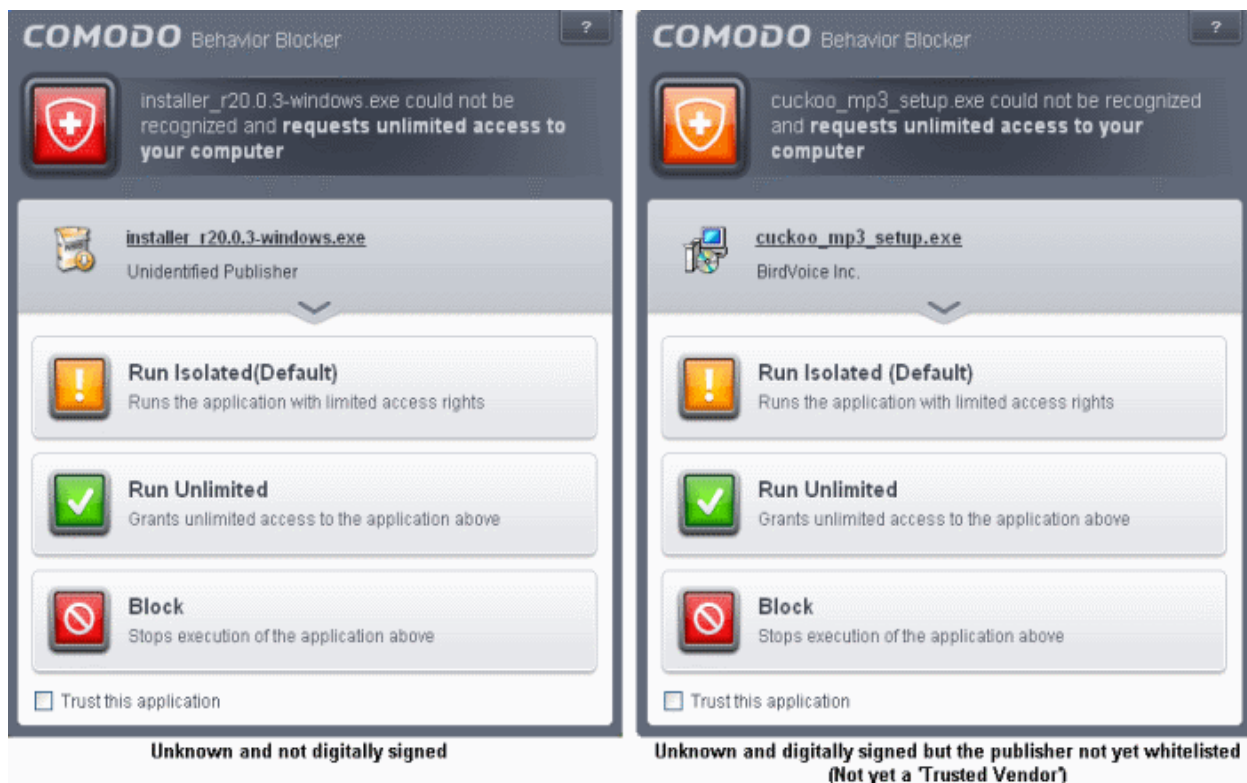
Run with Elevated Privileges Alert

The Behavior Blocker 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+ > Behavior Blocker**'

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').



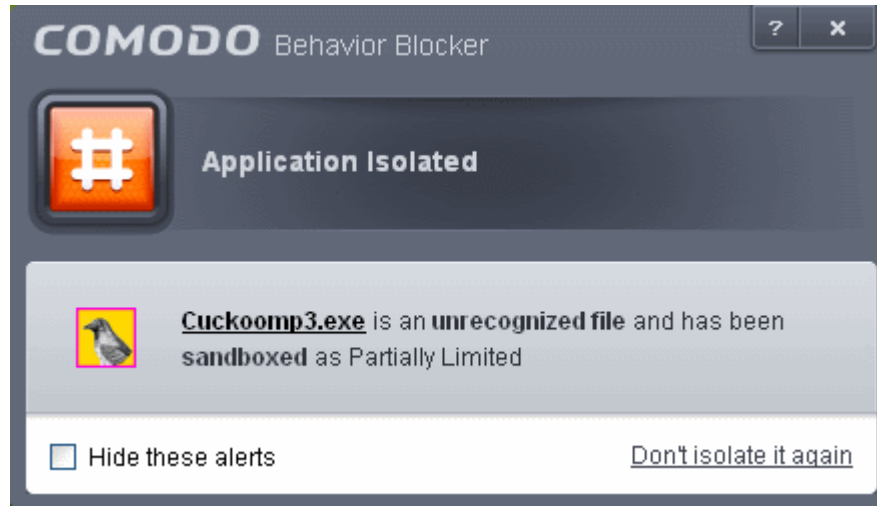
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

- **'Unknown Files: The Auto-Sandboxing and Scanning Processes'** - to understand the decision making process behind why CIS chooses to sandbox certain applications.
- **'Trusted Software Vendors'** - for an explanation of digitally signed files and 'Trusted Software Vendors'.

Auto-Sandbox Alerts

The Behavior Blocker will display an alert 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 **Unrecognized Files** list.

- Clicking the name of the application will open the **Unrecognized Files** interface, that displays a list of the unrecognized files including the currently auto-sandboxed application.
- Clicking Don't isolate it again removes the application from the Unrecognized Files list and adds it to the Trusted Files 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 **'Unrecognized Files'** 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 Auto-Sandboxing and Scanning Processes'** - to understand the decision making process behind why CIS chooses to auto-sandbox certain applications.

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 manage CIS running tasks.

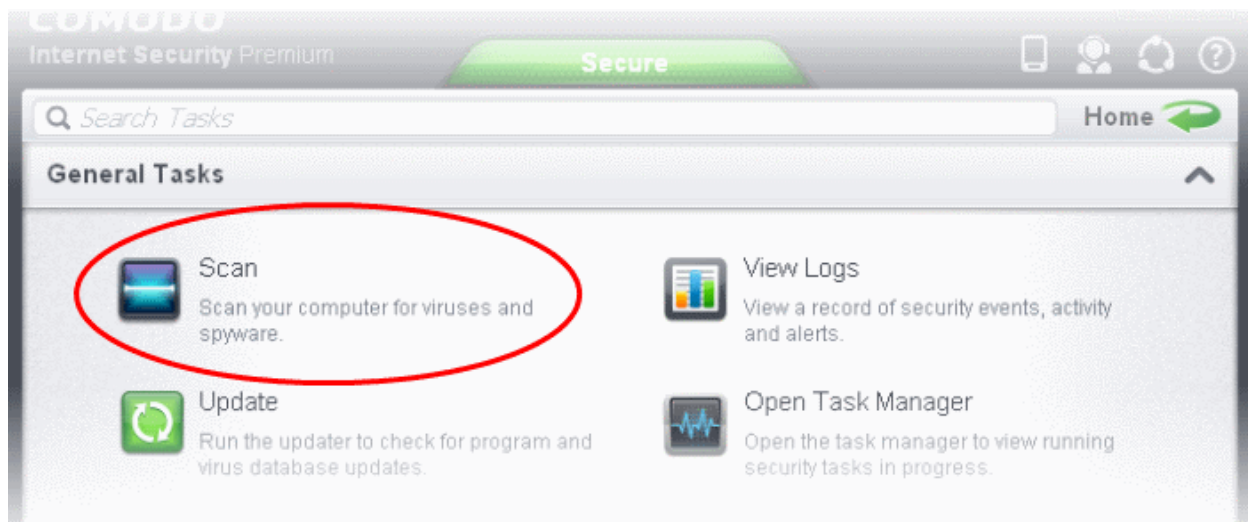


'General Tasks' contains the following areas. Click the links to jump to the help page for that topic.

- [Scan and Clean your Computer](#)
- [Manage Virus Database and Program Updates](#)
- [Manage Quarantined Items](#)
- [View CIS Logs](#)
- [Manage CIS Tasks](#)
- [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](#)

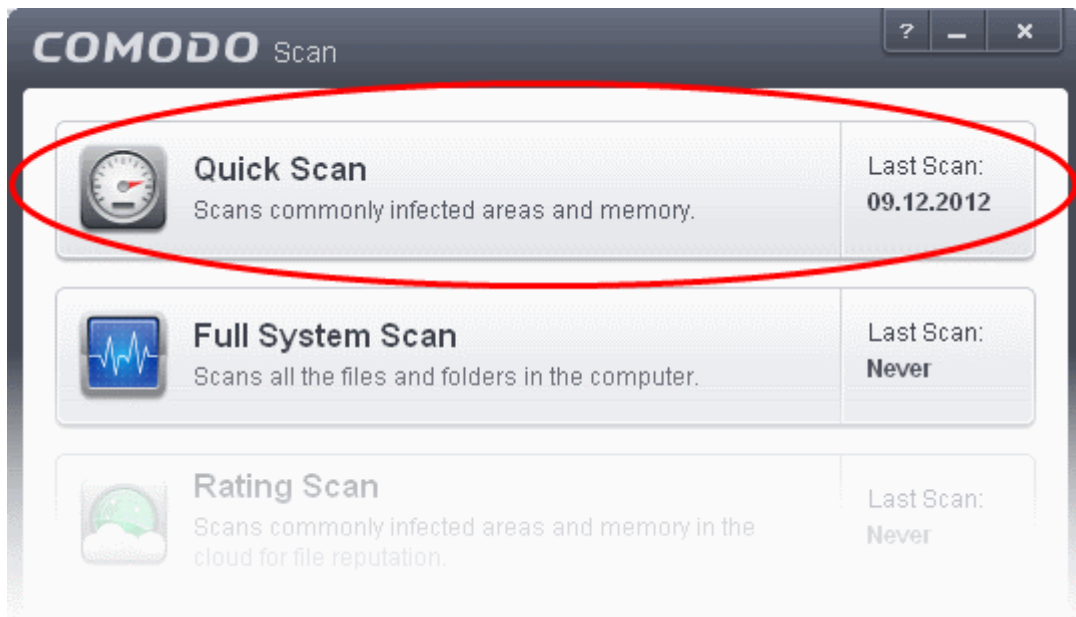
2.1.1. Run a Quick Scan

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.

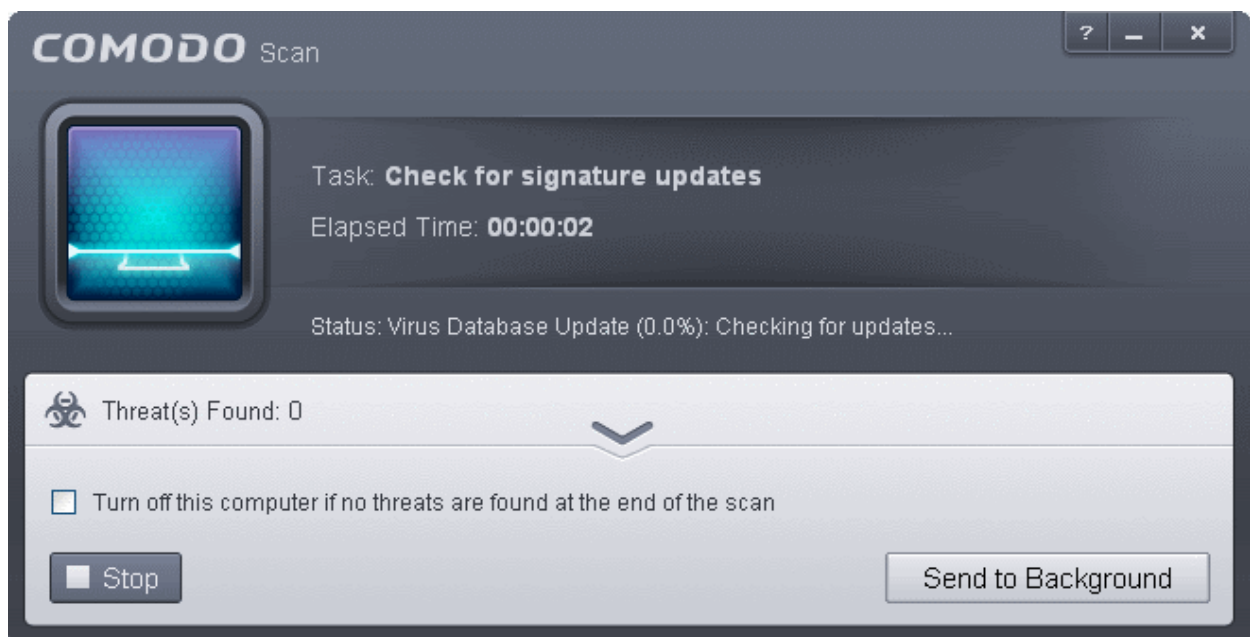
You can customize which items are scanned under a 'Quick Scan' and create a scan schedule from the 'Advanced Tasks' interface. Refer to [Antivirus Settings > Scan Profiles](#) for more details.

To run a Quick Scan

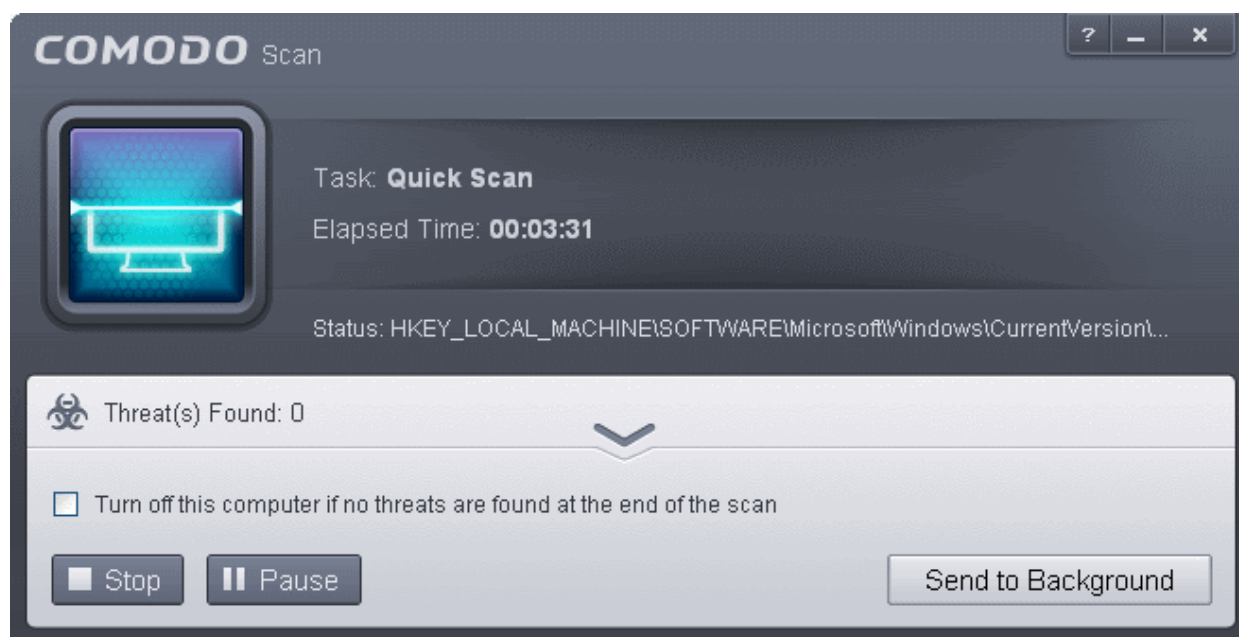
- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



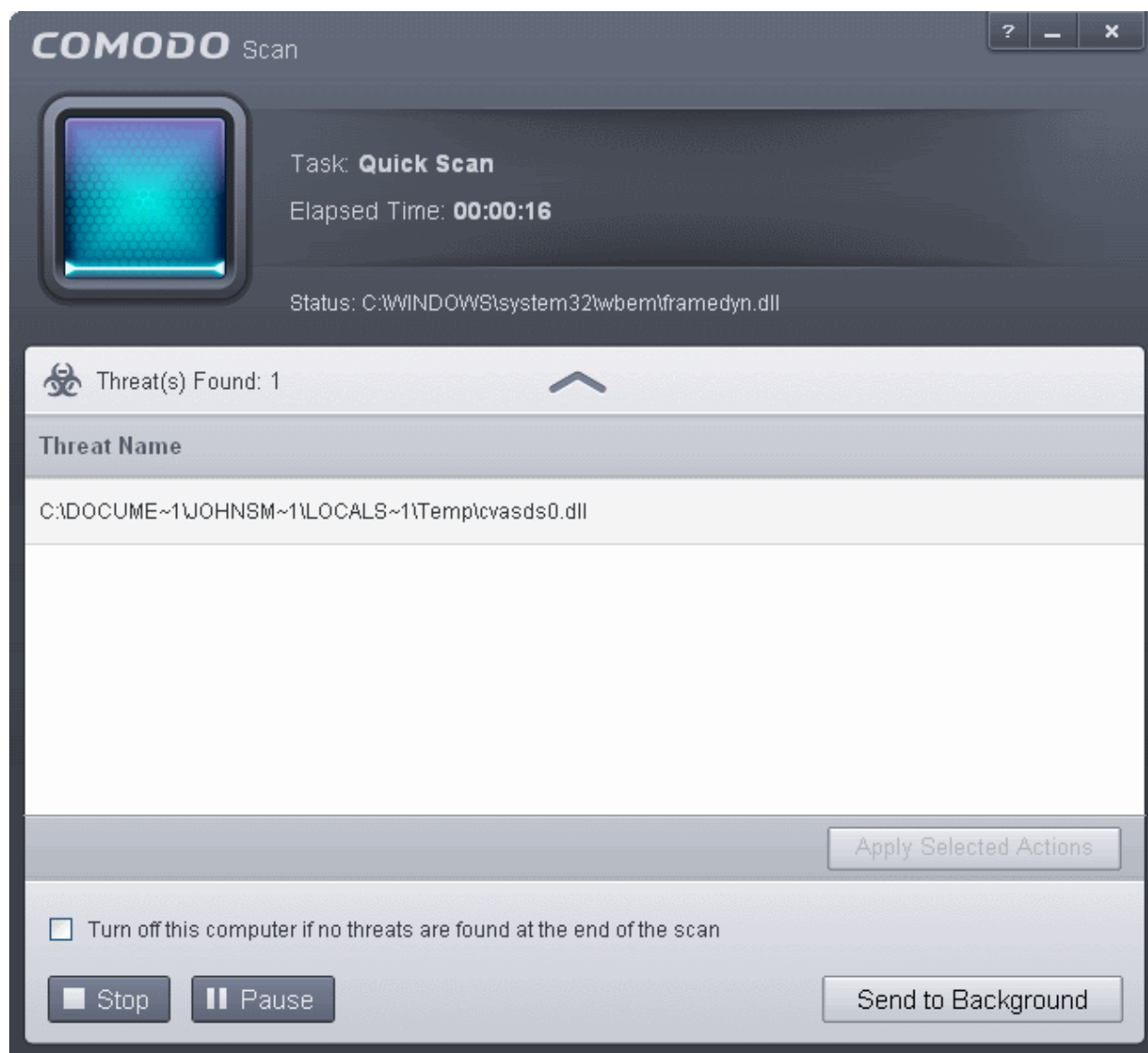
The scanner will start and first check whether your virus signature database is up-to-date:



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

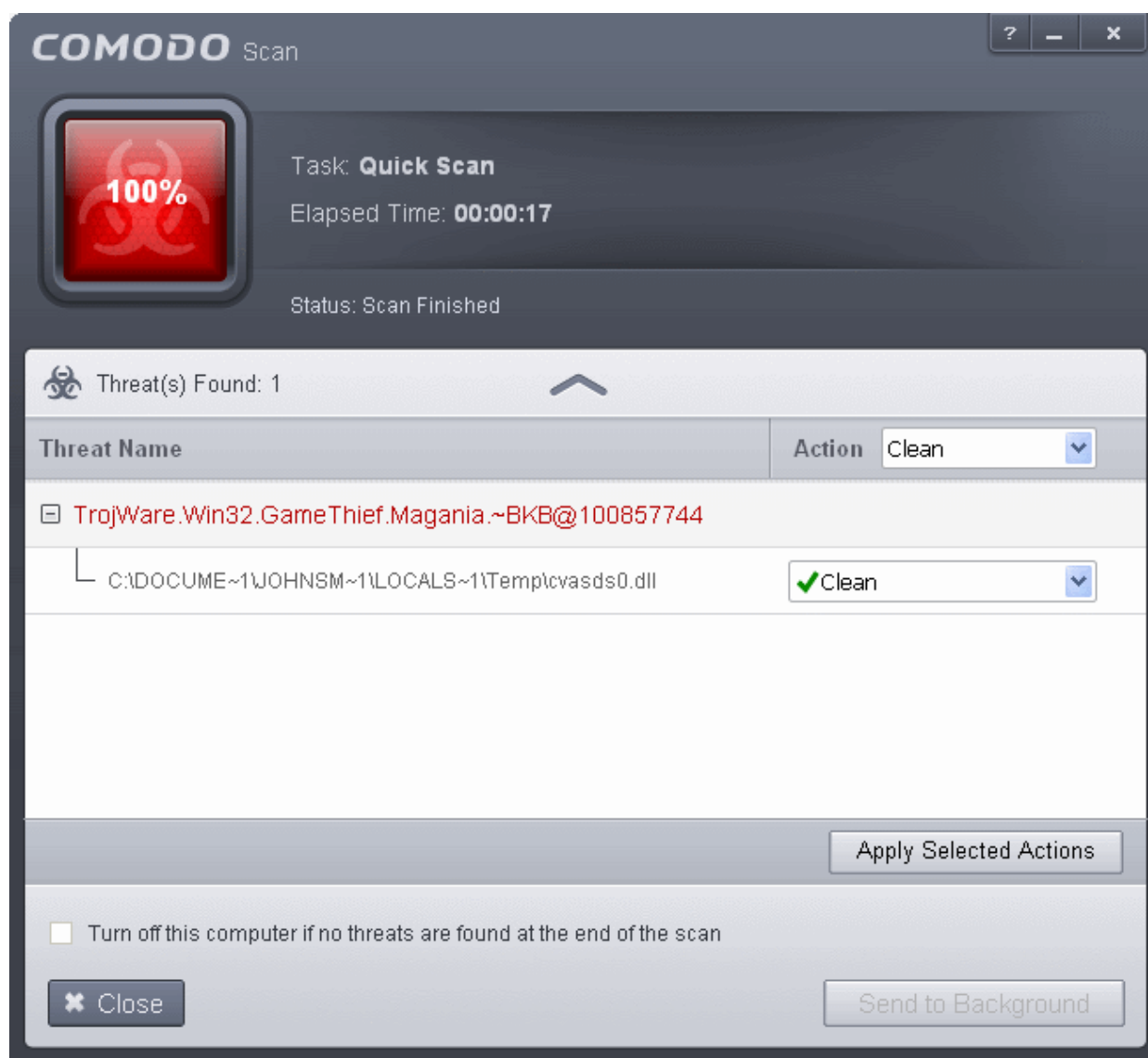


- You can Pause, Resume or Stop the scan by clicking respective buttons. If you want to run the scan in the background, click 'Send to Background'. You can still keep track of the scan progress from the 'Task Manager' interface.

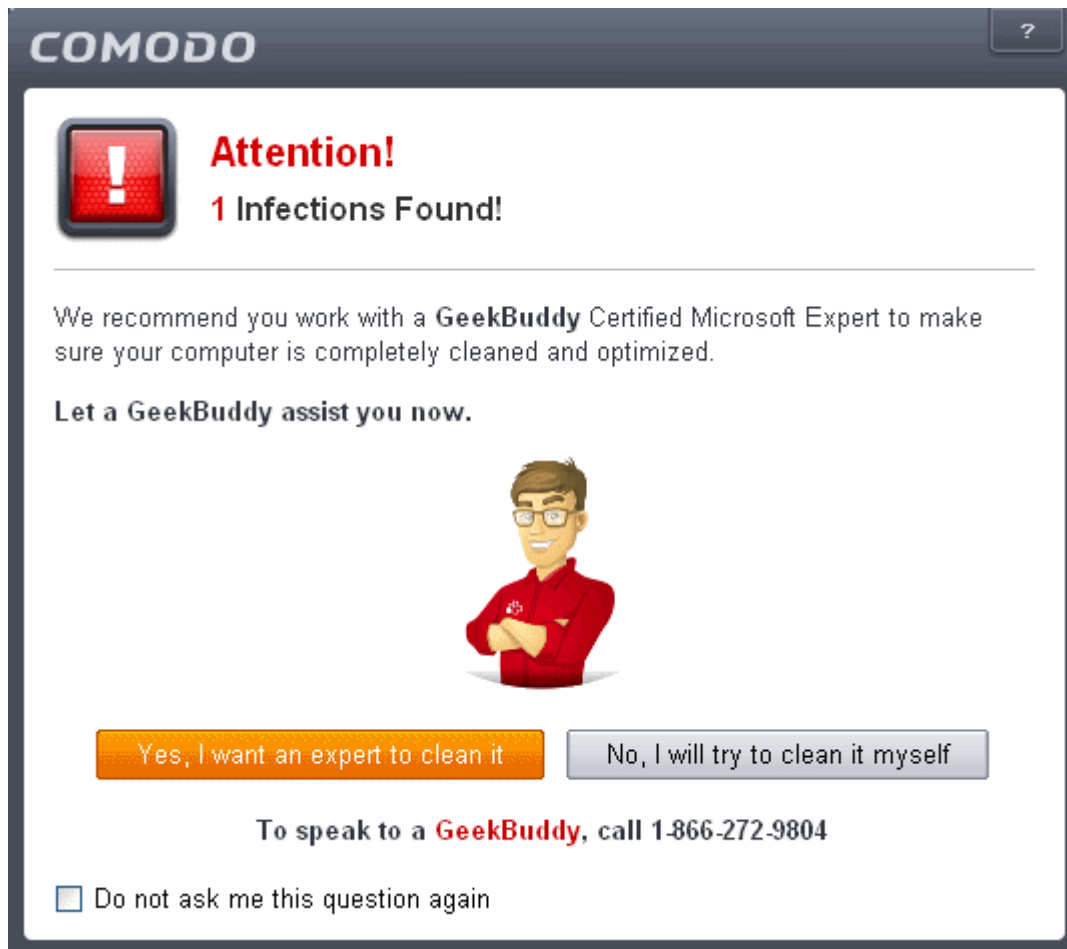


On completion of scanning, the results will be displayed with a list of identified infections:

- To open or close the lower panel that shows the list of infected files detected during the course of scan, click the down/up arrow.



- 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.



COMODO

Attention!
1 Infections Found!

We recommend you work with a **GeekBuddy** Certified Microsoft Expert to make sure your computer is completely cleaned and optimized.

Let a GeekBuddy assist you now.

Yes, I want an expert to clean it **No, I will try to clean it myself**

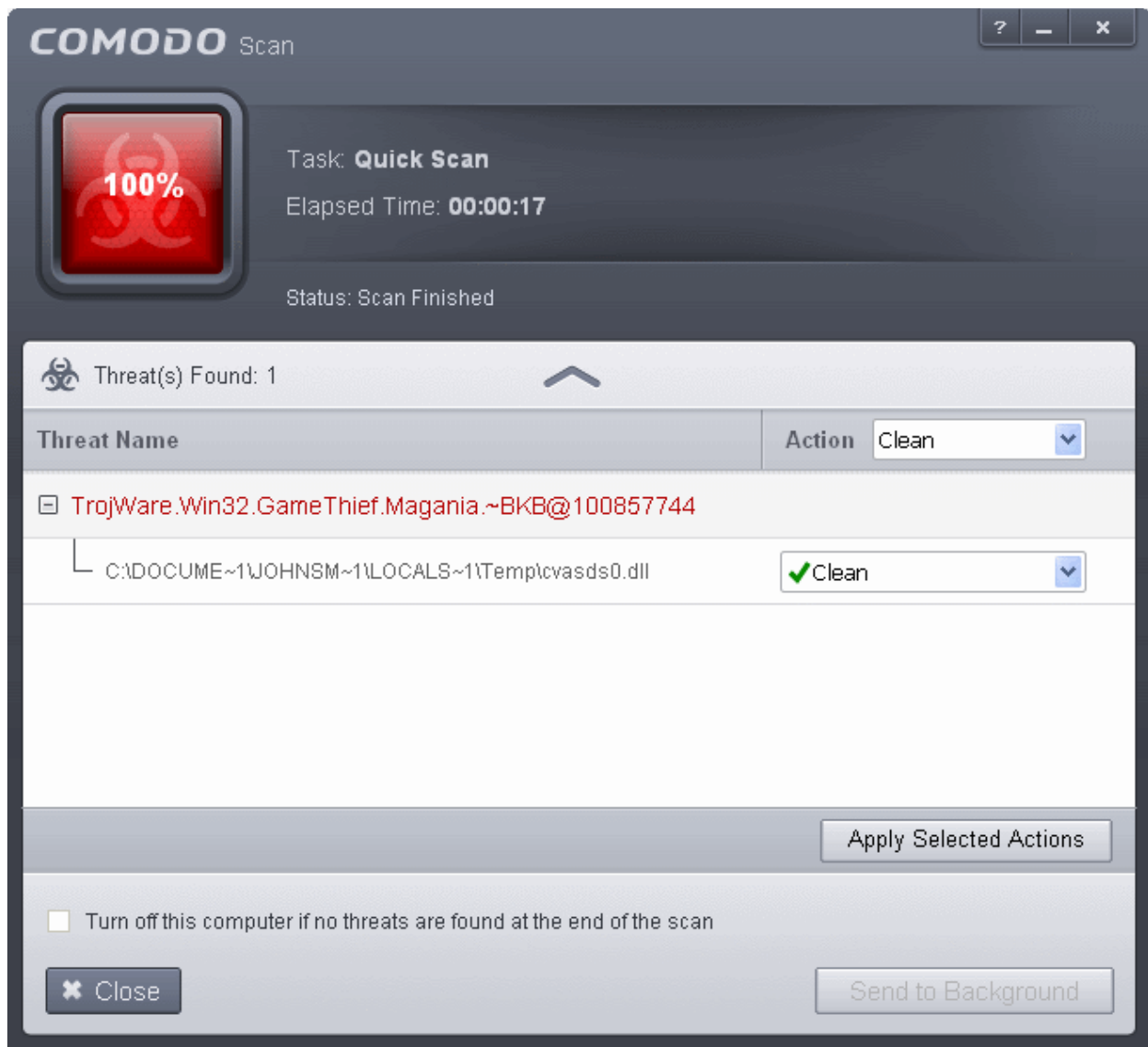
To speak to a **GeekBuddy**, call 1-866-272-9804

Do not ask me this question again

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

2.1.2. Run a Full Computer Scan

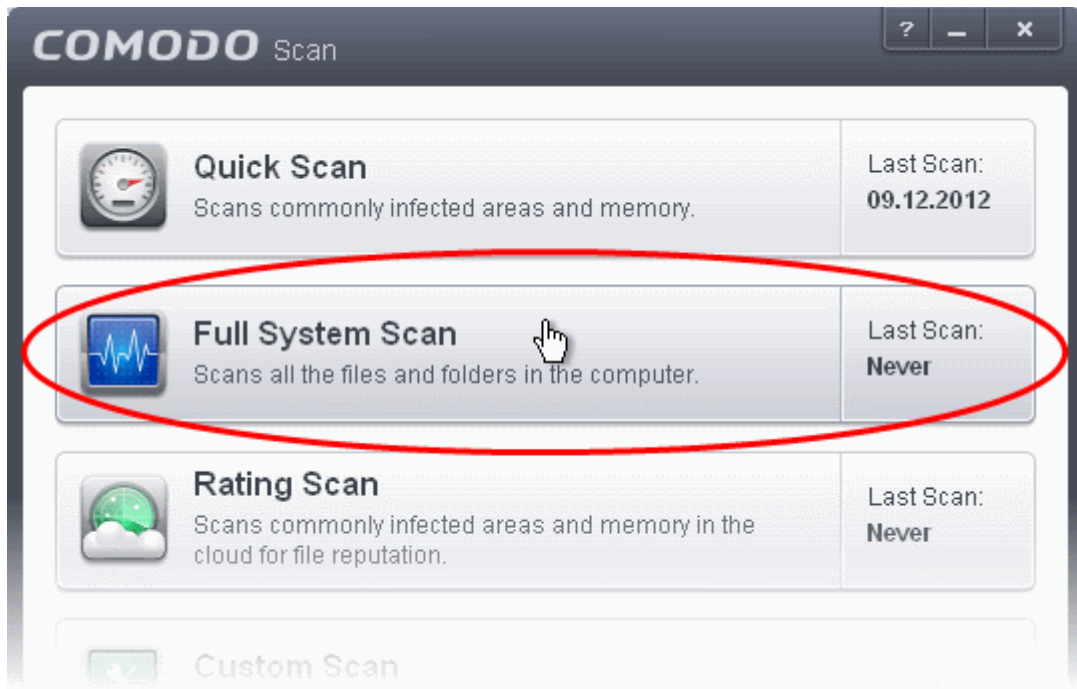
The 'Full System Scan' scans every local drive, folder and file on your system. Any external devices like USB drives, digital camera and so on are also scanned.

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

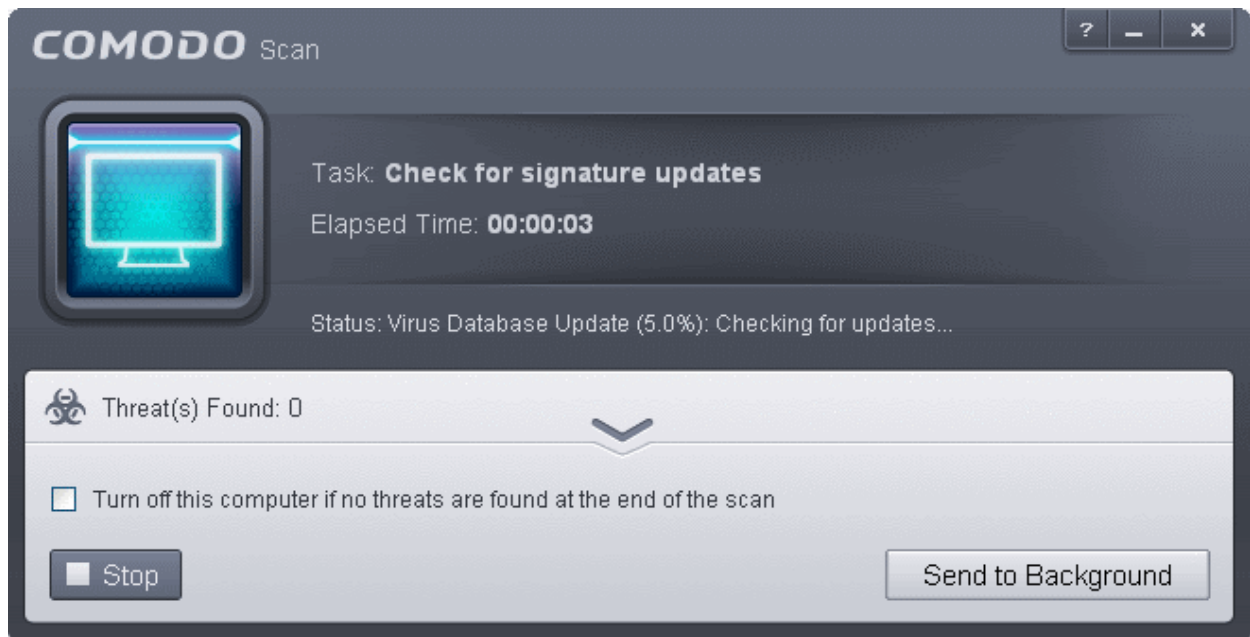
Refer to [Antivirus Settings > Scan Profiles](#) for more details.

To run a Full Computer Scan

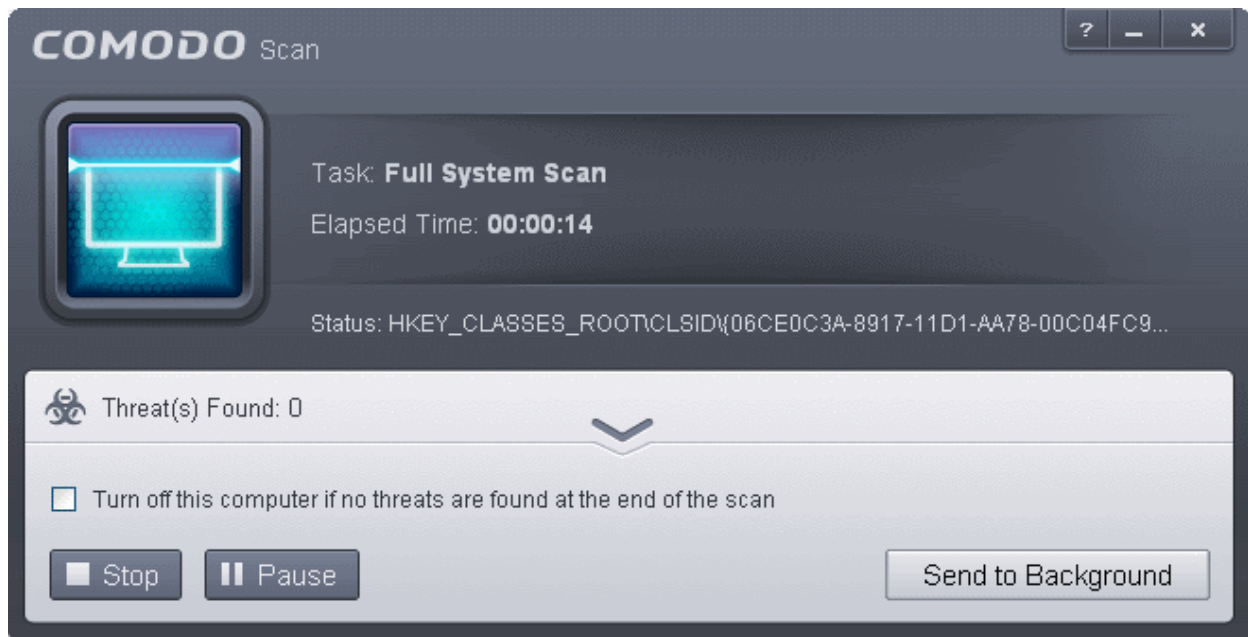
- Click 'Scan' from the General Tasks interface and click 'Full System Scan' from the 'Scan' interface.



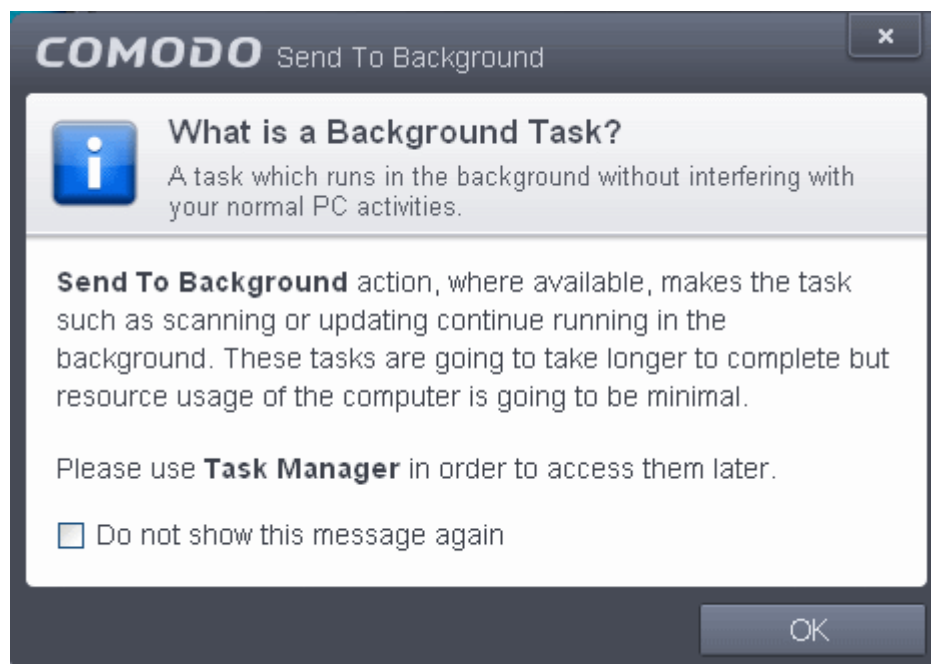
The scanner will start and first check whether your virus signature database is up-to-date.



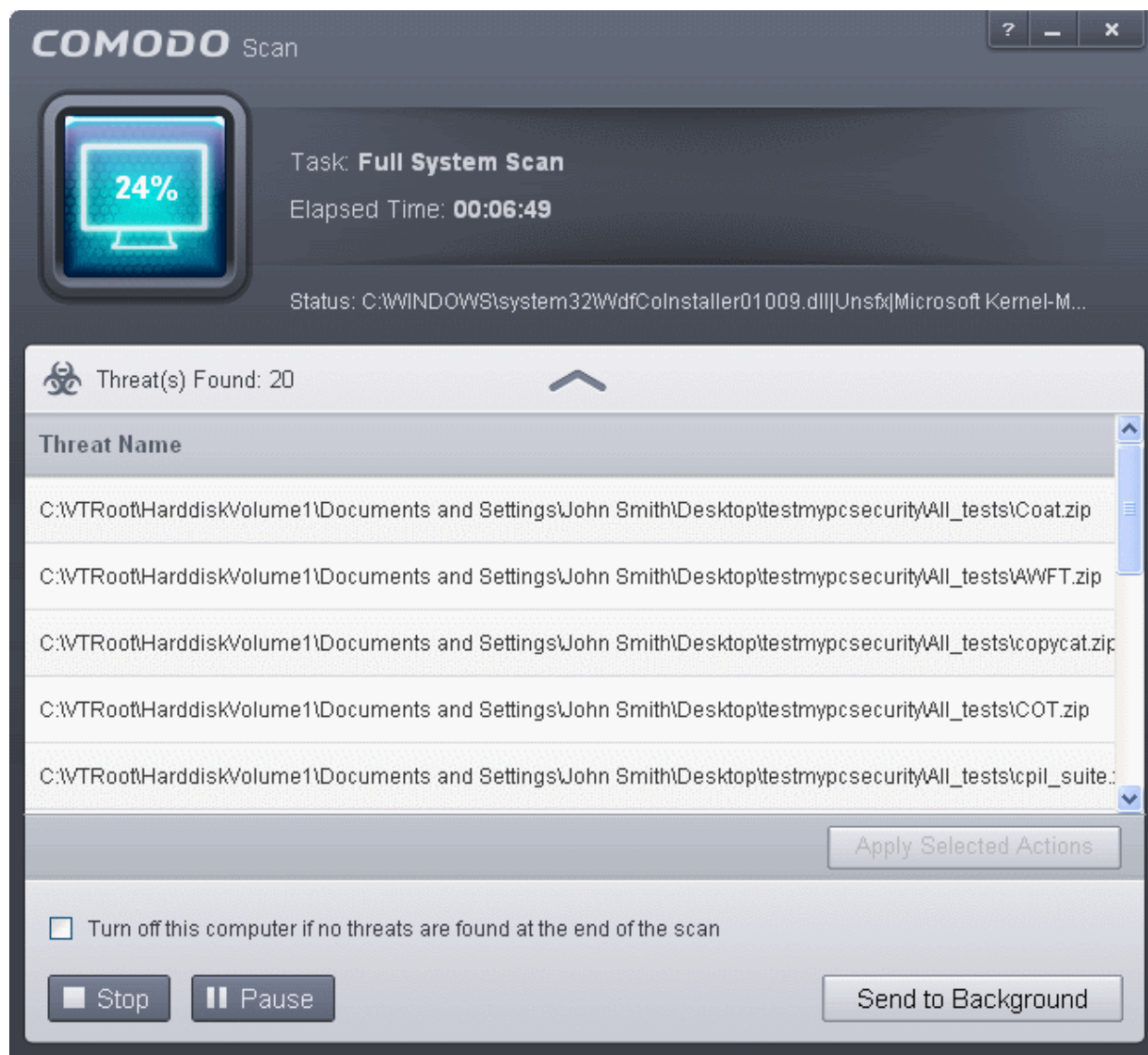
If the database is outdated, CIS will first download and install the latest database before commencing the virus scan.



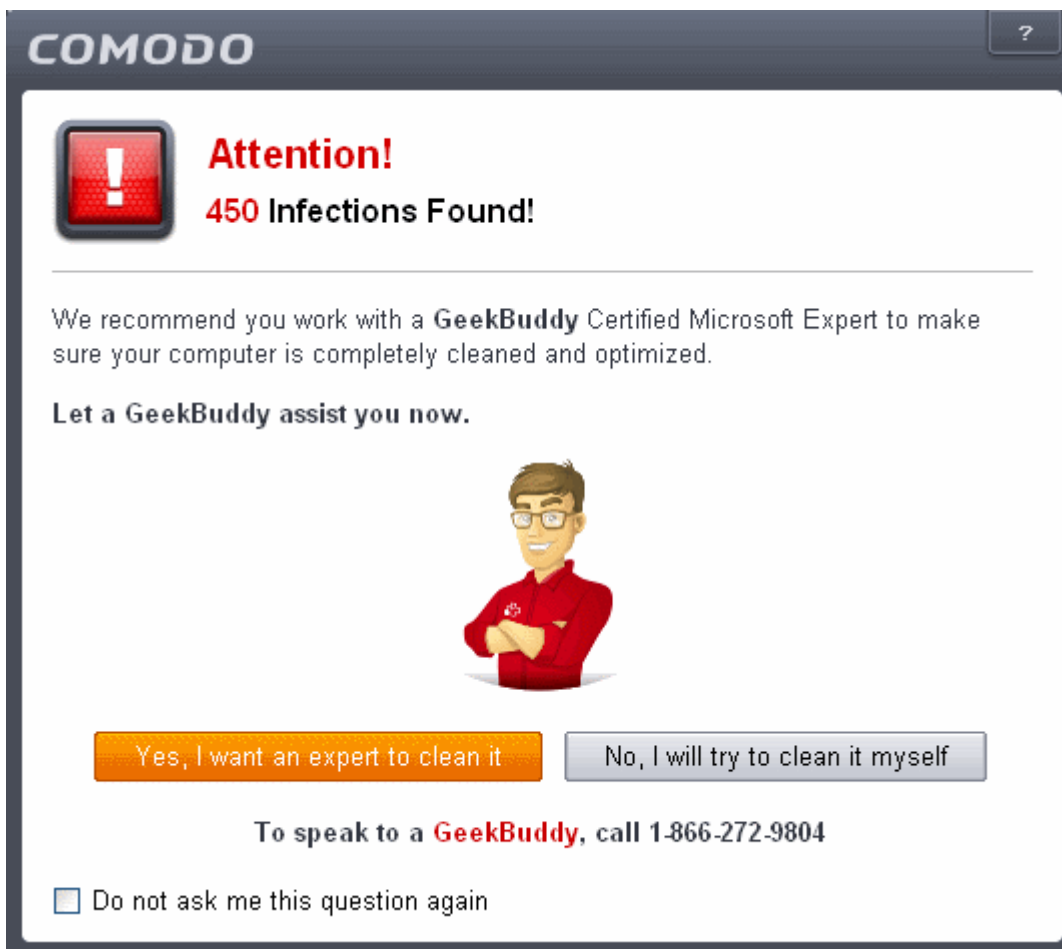
- You can Pause, Resume or Stop the scan by clicking the respective buttons. If you want to run the scan in the background, click 'Send to Background'.



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



- 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.



COMODO

Attention!
450 Infections Found!

We recommend you work with a **GeekBuddy** Certified Microsoft Expert to make sure your computer is completely cleaned and optimized.

Let a **GeekBuddy** assist you now.

Yes, I want an expert to clean it

No, I will try to clean it myself

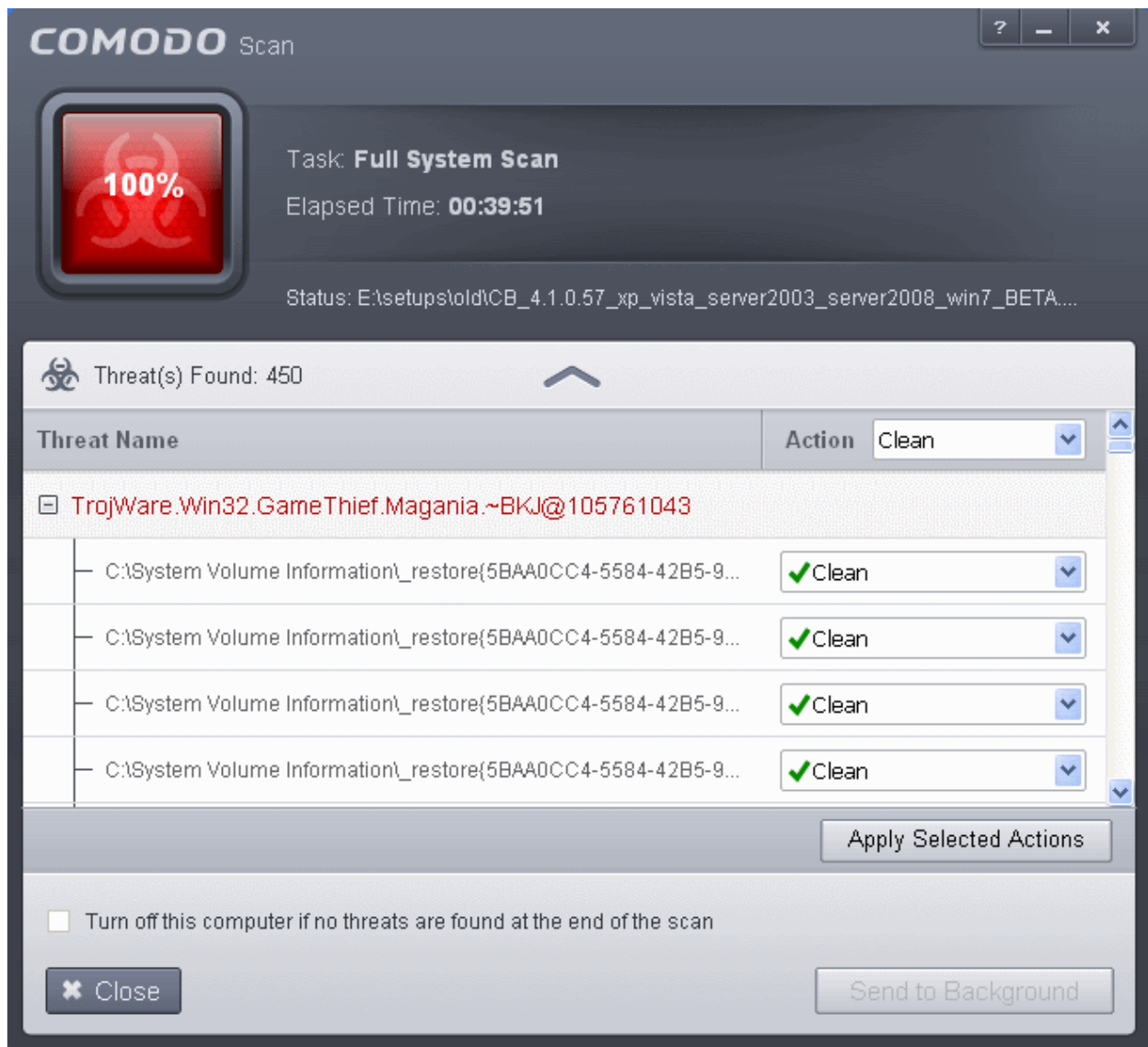
To speak to a **GeekBuddy**, call 1-866-272-9804

Do not ask me this question again

- 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 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

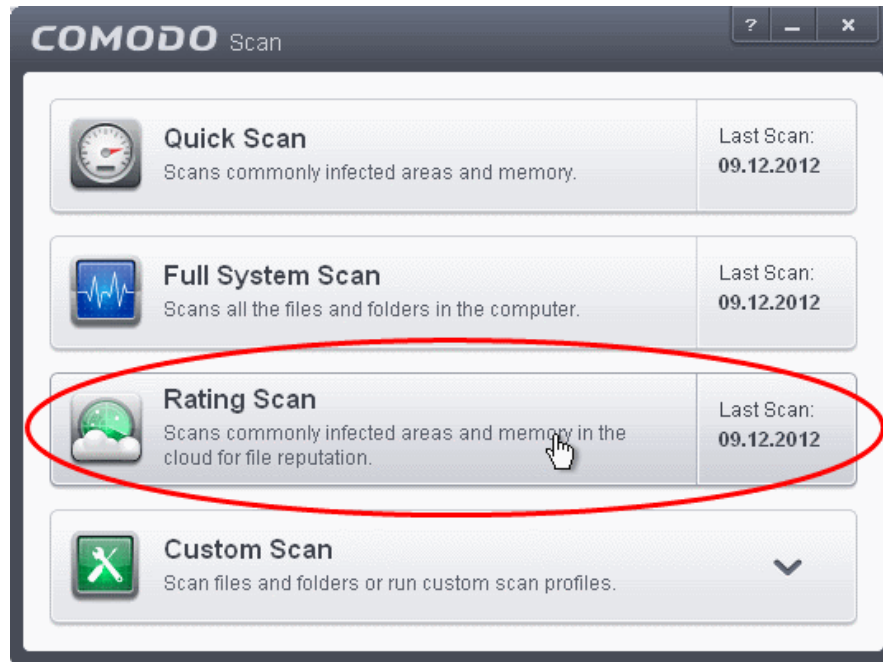
The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

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':

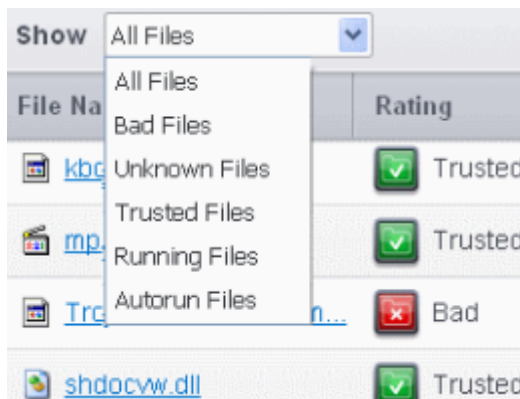


After the cloud scanners have finished their analysis, file ratings will be displayed as follows:

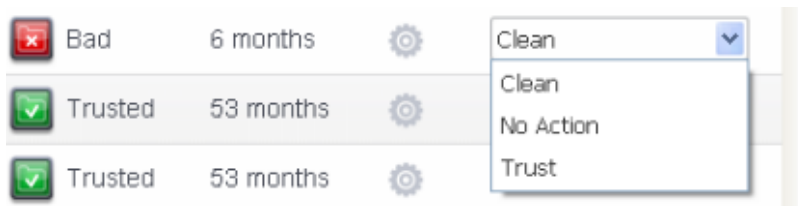


- **File Name:** The file which was scanned
- **Rating:** The rating of the file as per the cloud based analysis
- **Age:** The period of time that the file has been stored on your computer
- **Autorun:** Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous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

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

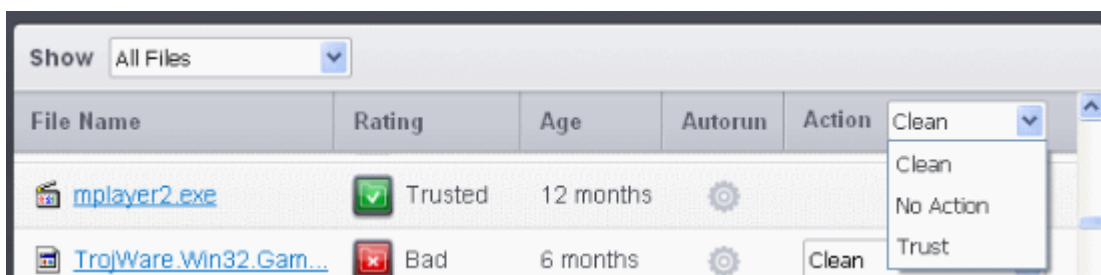


Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'



- **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.

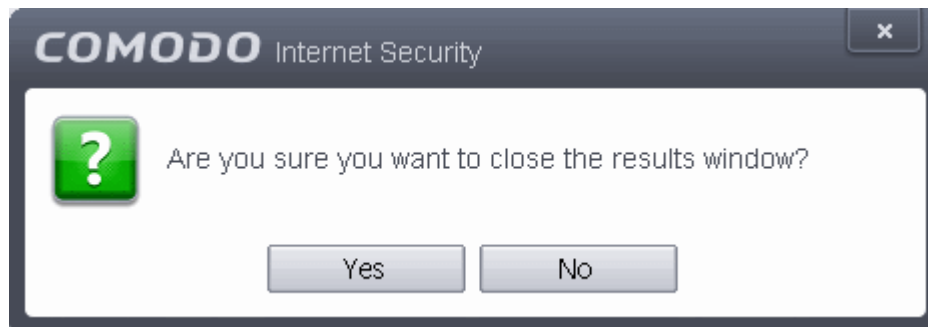
For the same action to be applied to all 'Bad' files, make a selection from the drop-down menu at the top of the 'Action' column.



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

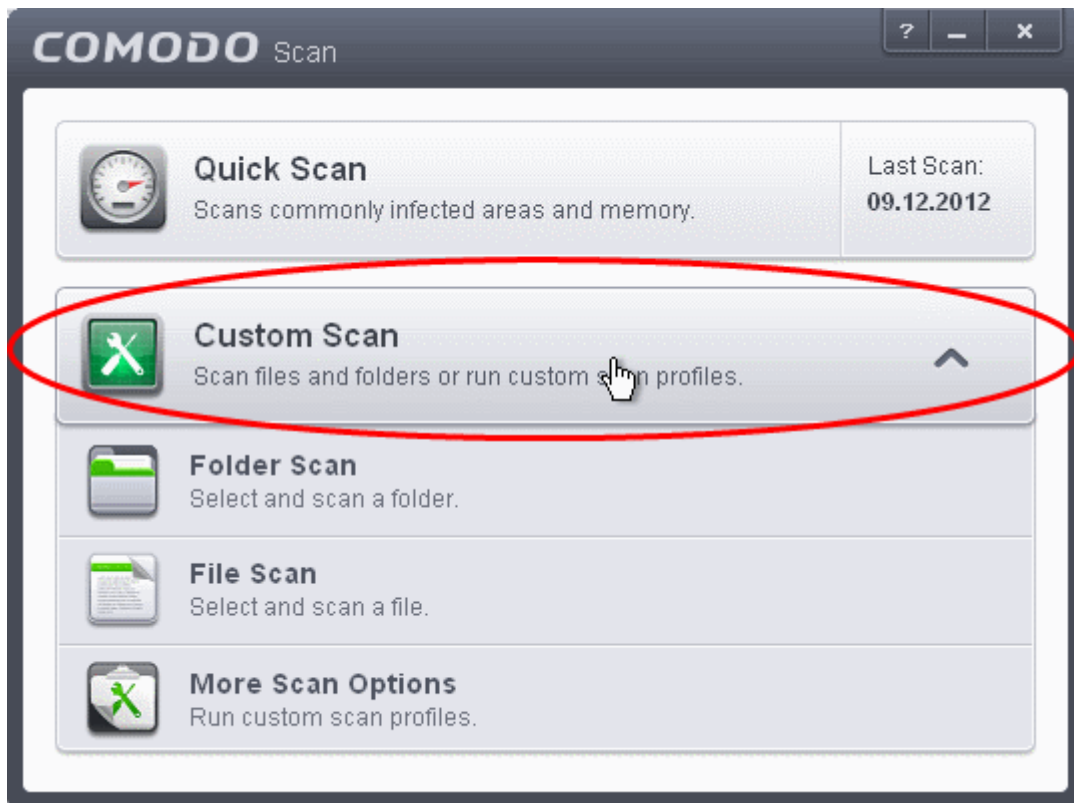


... then click 'Yes' in the confirmation window.

2.1.4. Run a Custom Scan

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

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



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

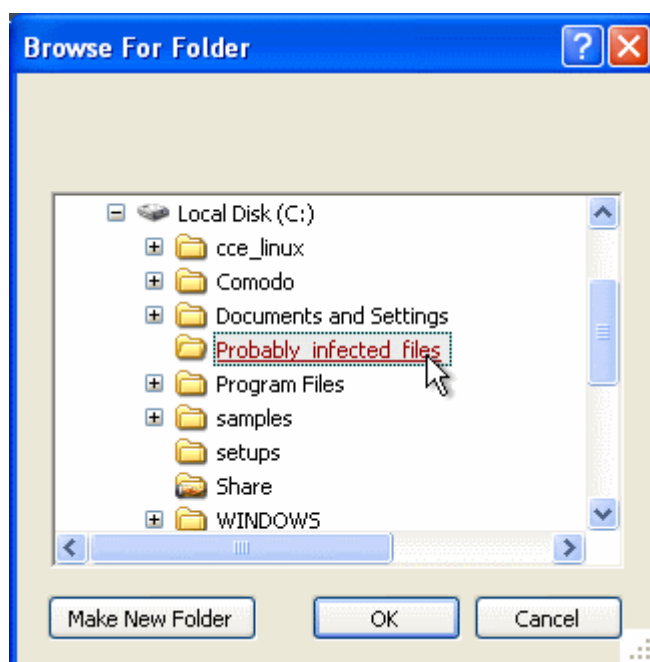
- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file
- **More Scan Options** - create a custom scan profile here

2.1.4.1. Scan a Folder

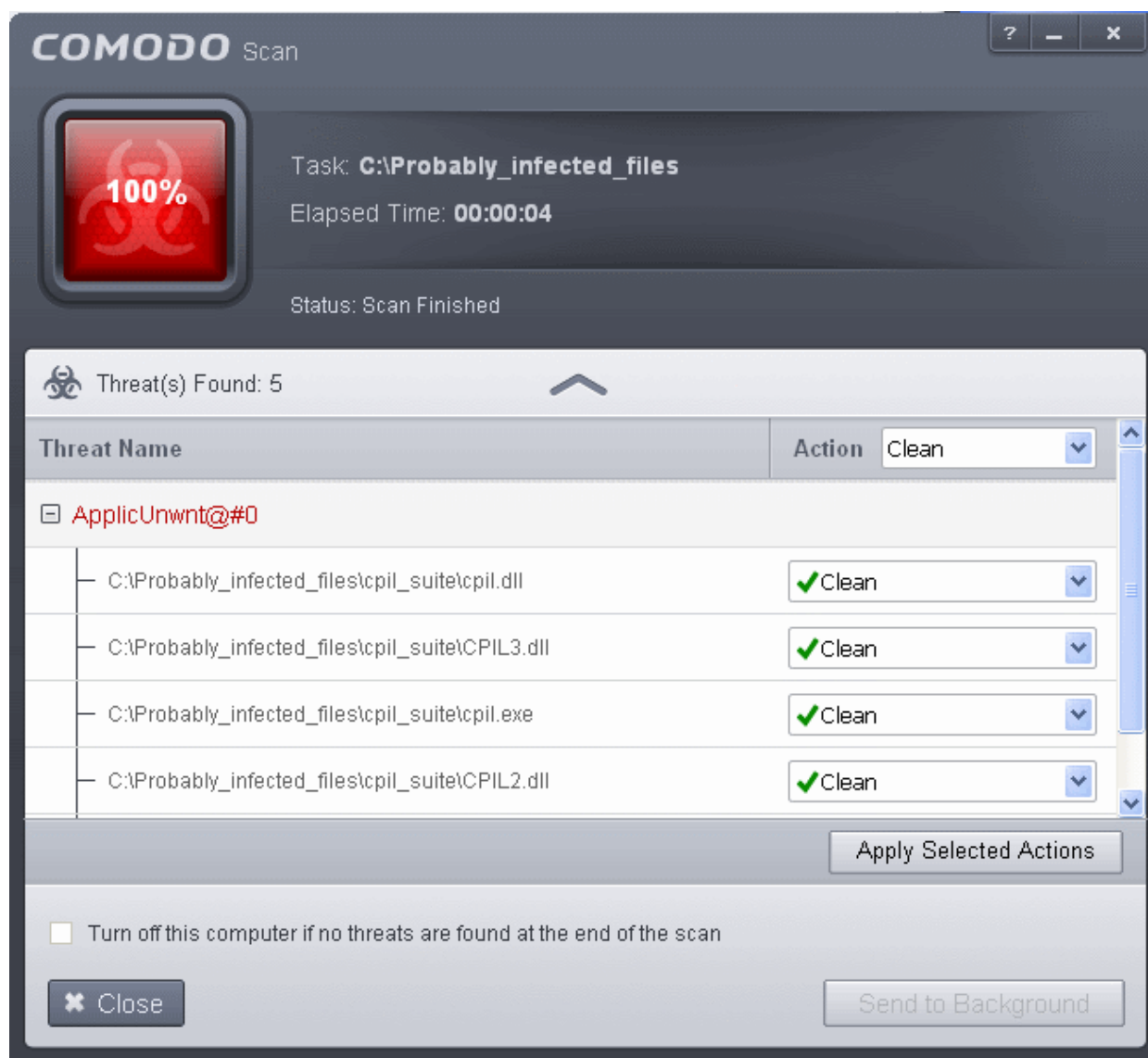
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan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

To scan a specific folder

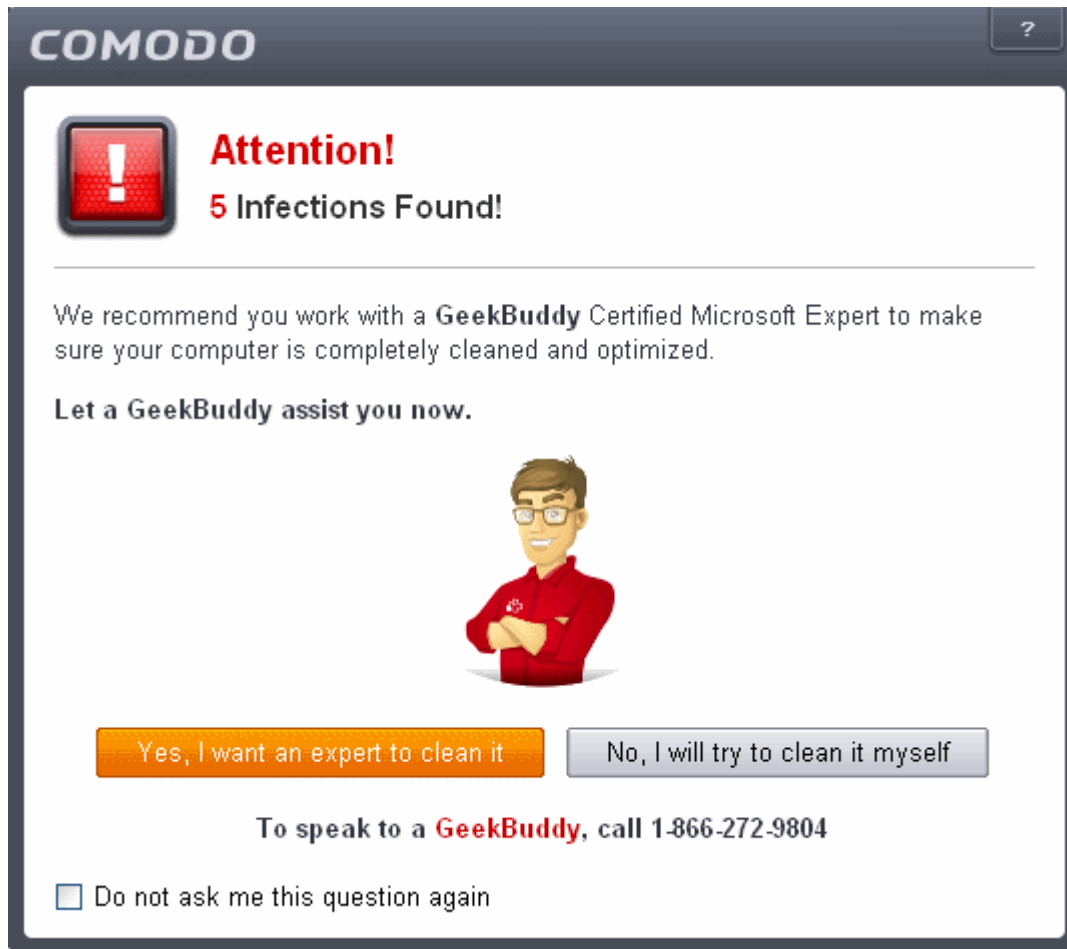
- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'Folder Scan' from the 'Custom Scan' pane
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click OK



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 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 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.

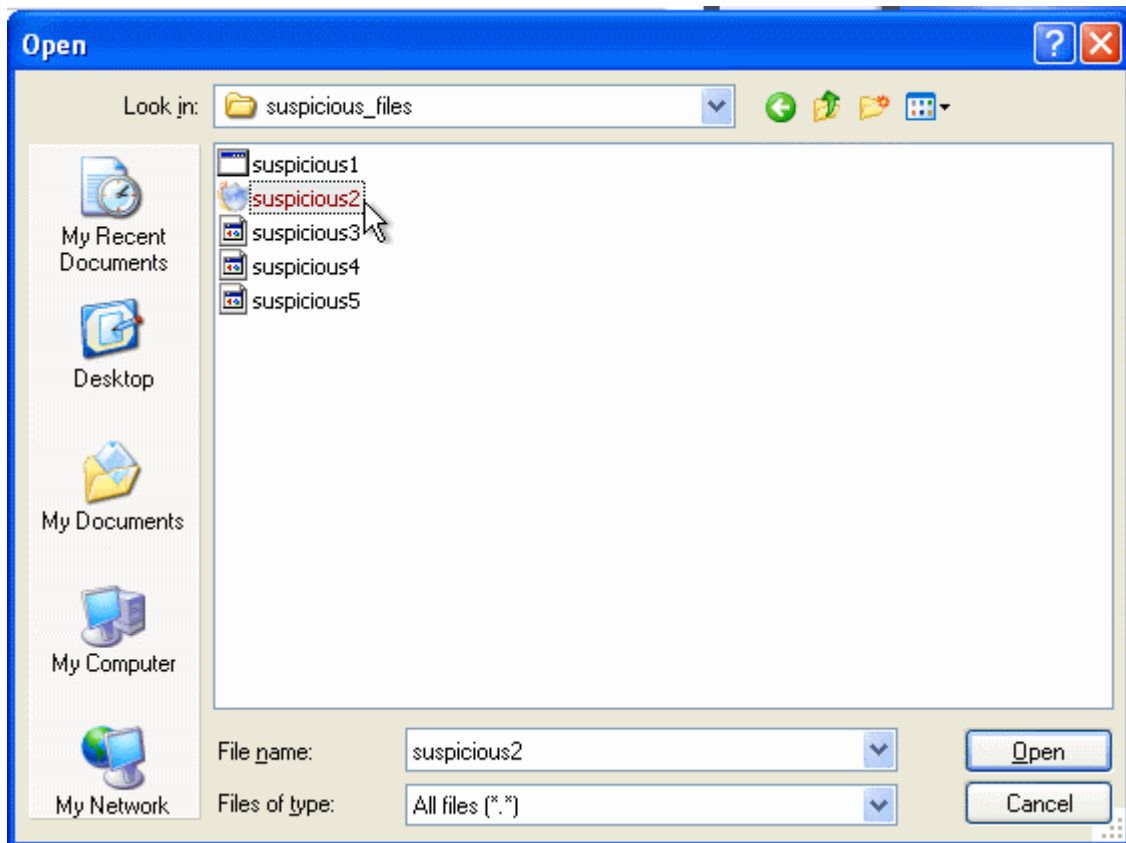
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CIS interface or by right clicking it. Refer to [Scan Individual File/Folder](#) for more details.

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.

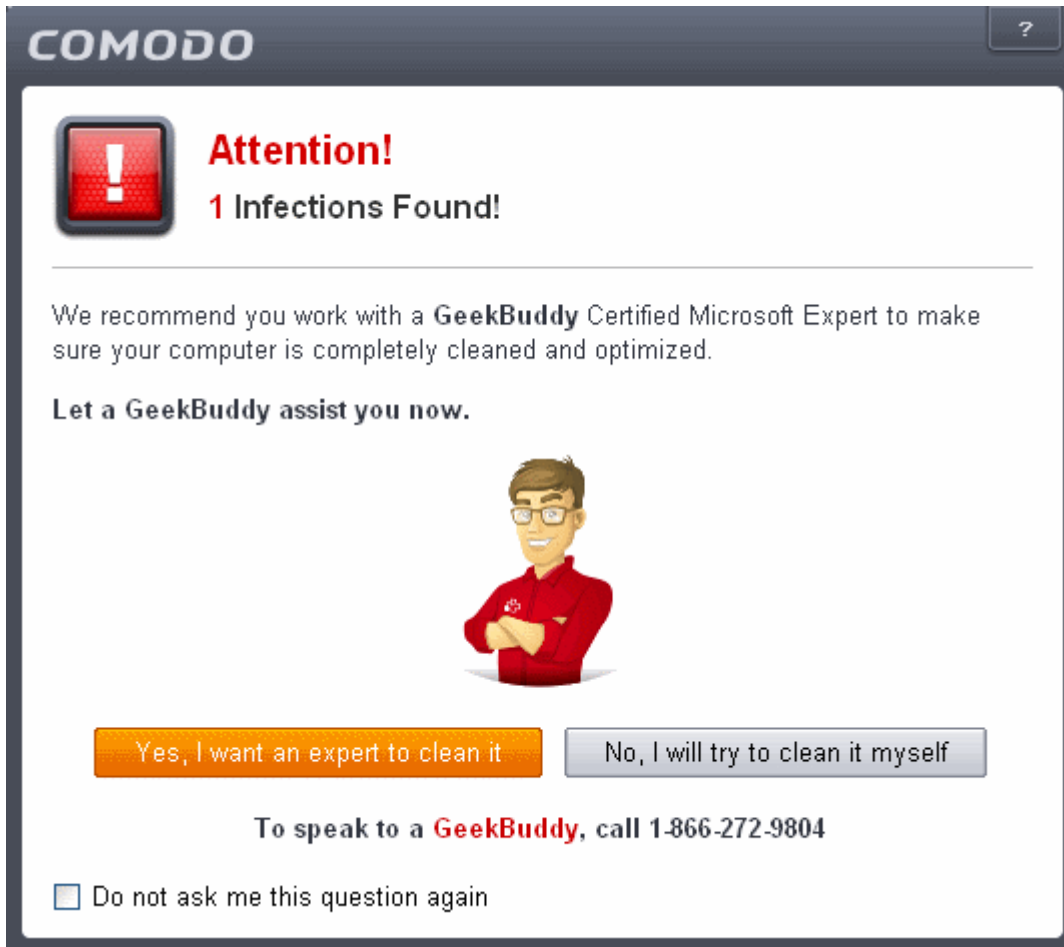
To scan a specific file

- 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.



COMODO

Attention!
1 Infections Found!

We recommend you work with a **GeekBuddy** Certified Microsoft Expert to make sure your computer is completely cleaned and optimized.

Let a GeekBuddy assist you now.

Yes, I want an expert to clean it **No, I will try to clean it myself**

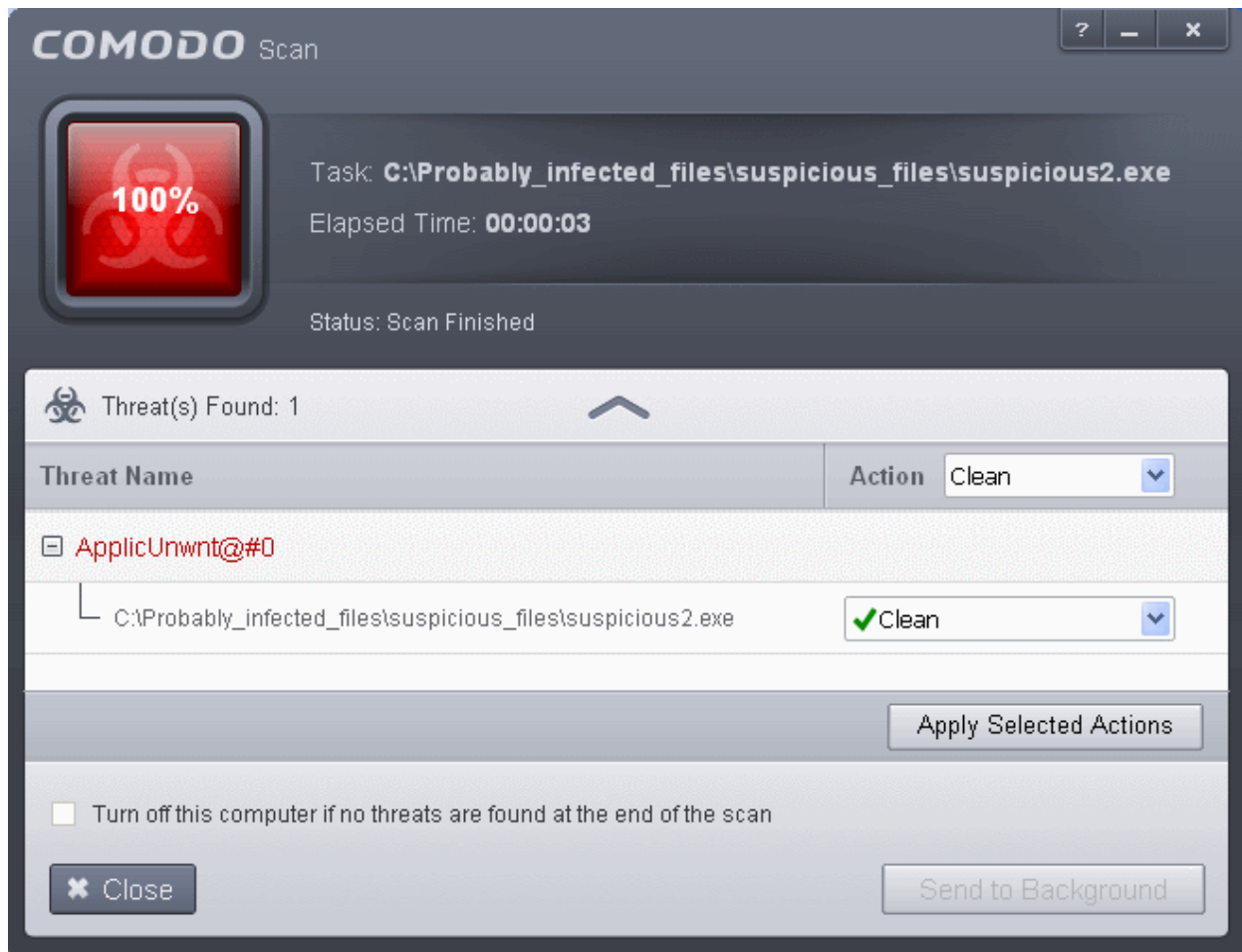
To speak to a **GeekBuddy**, call **1-866-272-9804**

Do not ask me this question again

- 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 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.

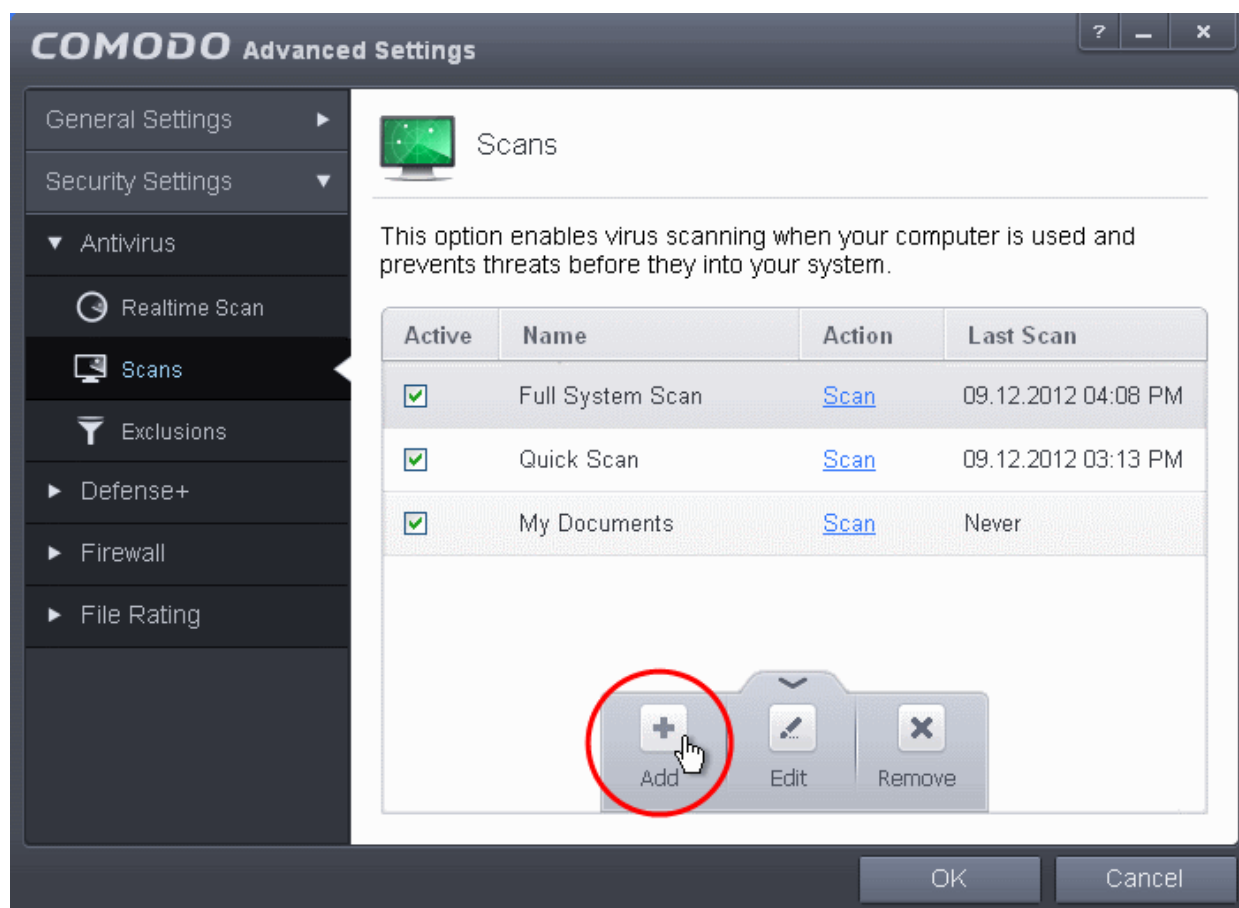
2.1.4.3. Create, Schedule and Run a Custom Scan

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](#)

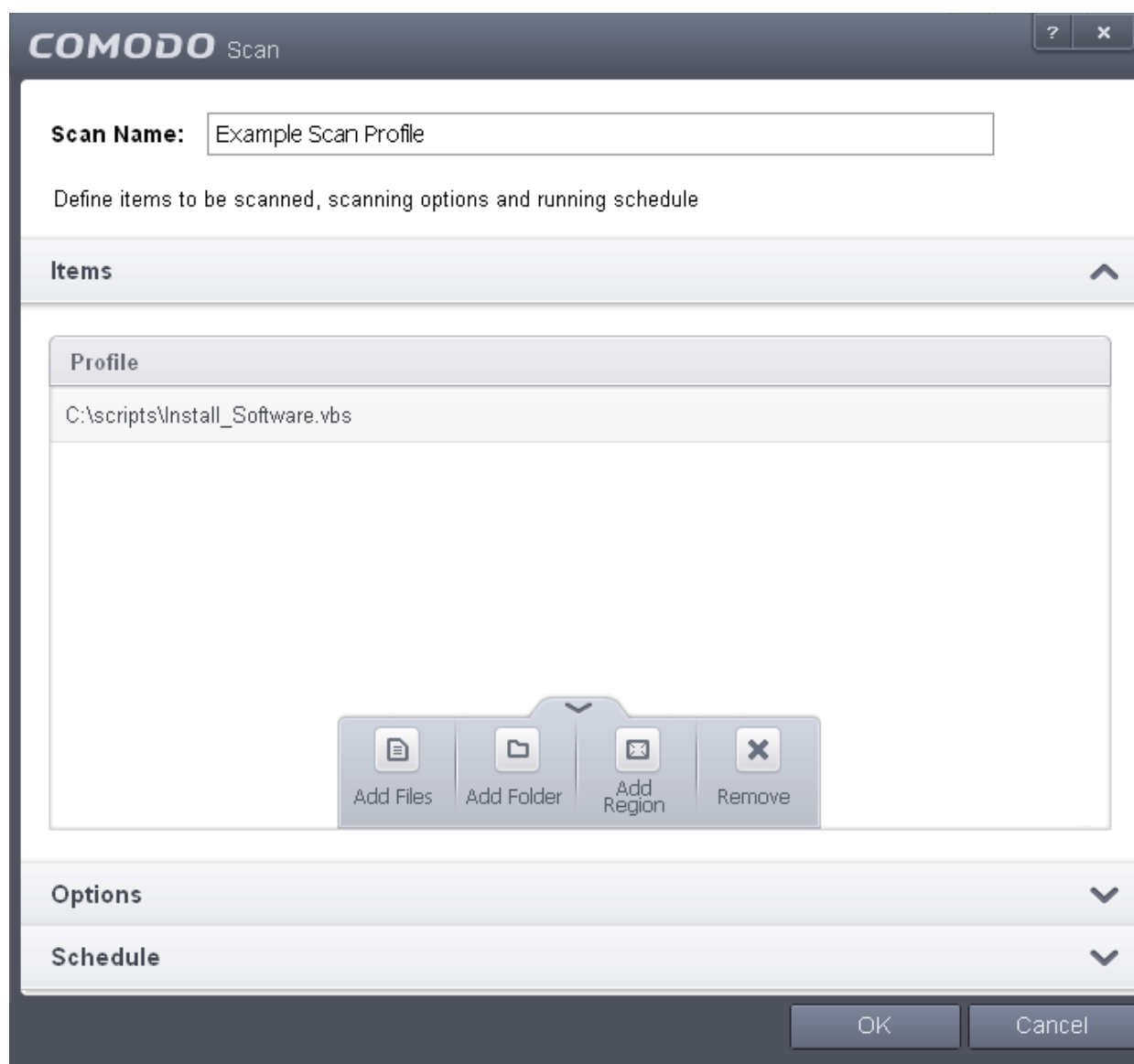
To create a custom profile

- 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.

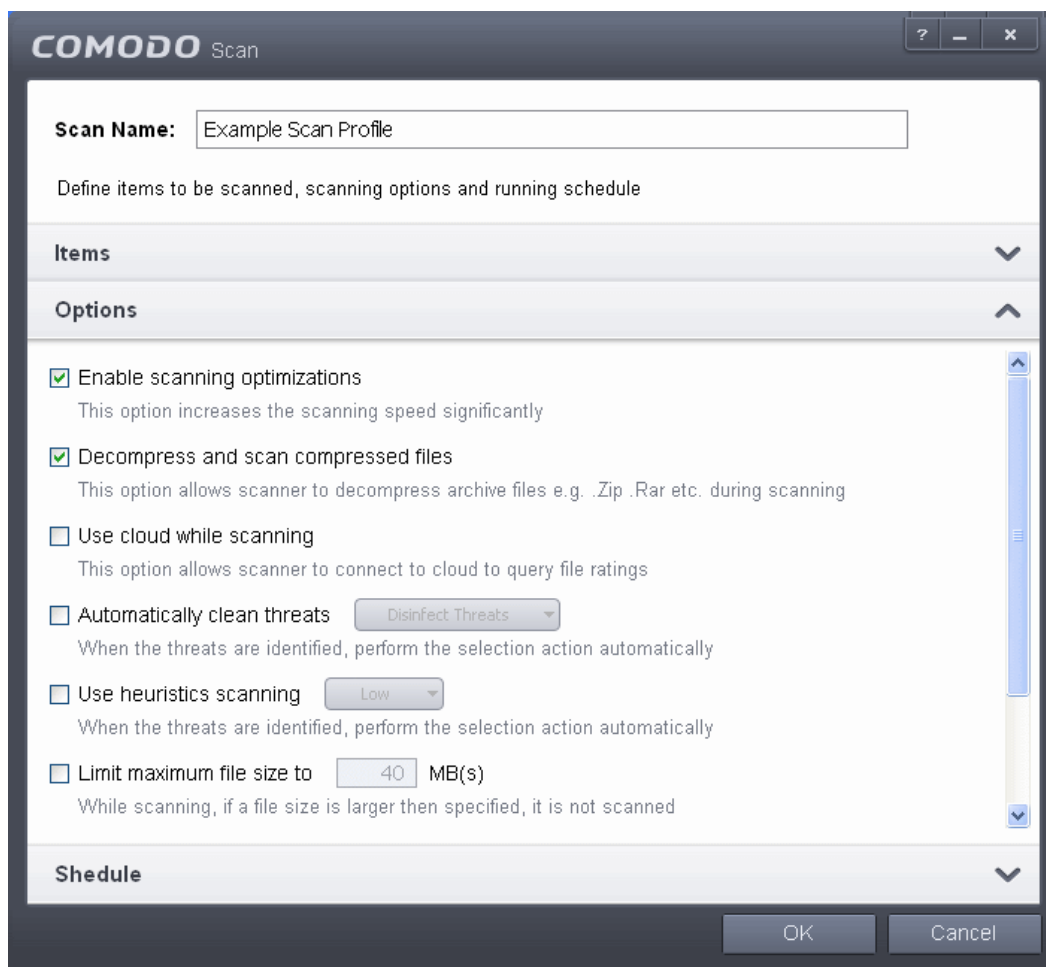
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



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

COMODO Scan

Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Items ▾

Options ▾

Schedule ▴

Frequency:

Do not schedule this task

Every Day

Every Week

Every Month

Start Time: 5:30 AM ▾

Day(s) of Week

Sun Mon Tue Wed Thu Fri Sat

Run only when computer is not running on battery

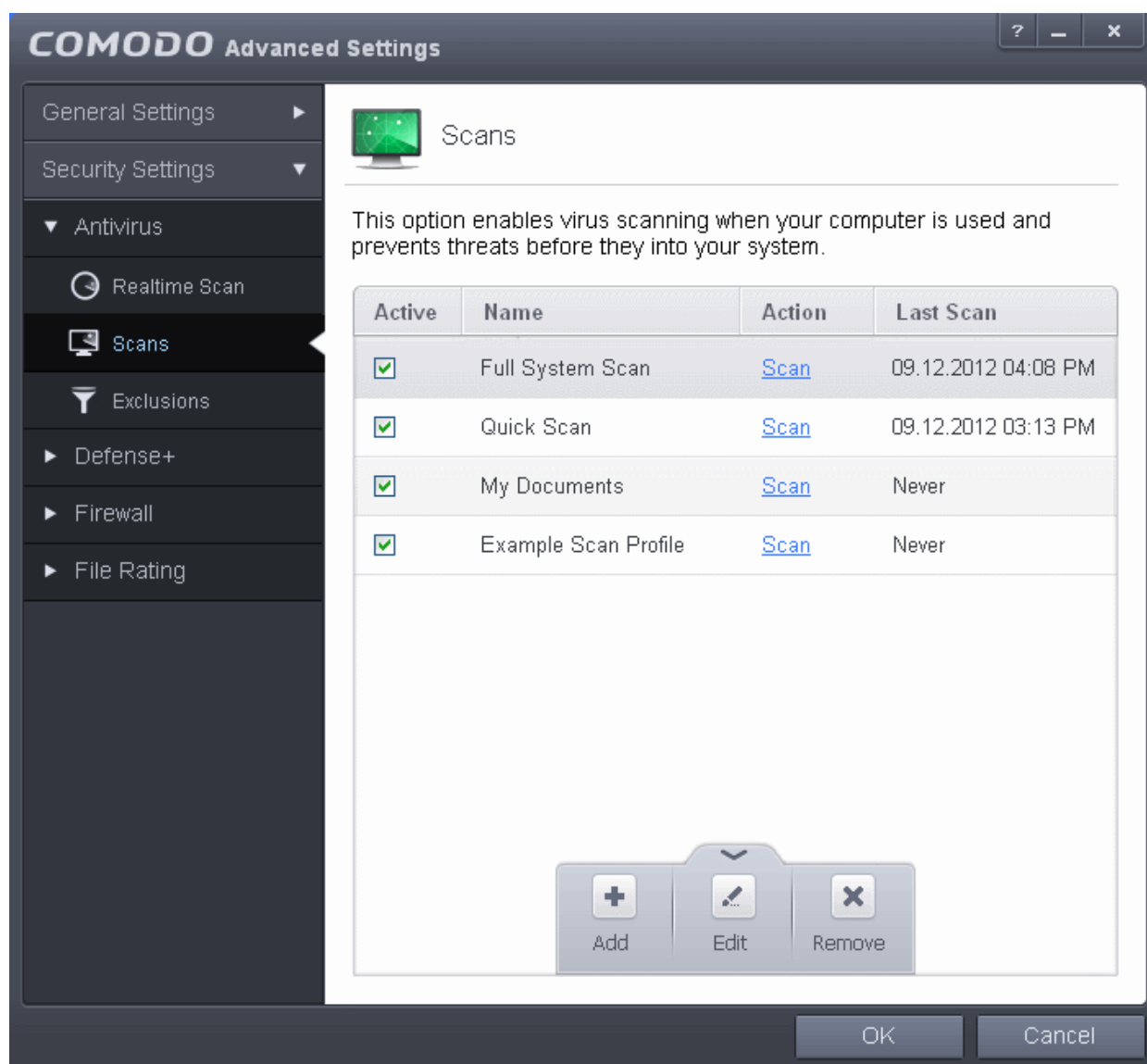
Run only when computer is IDLE

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

OK Cancel

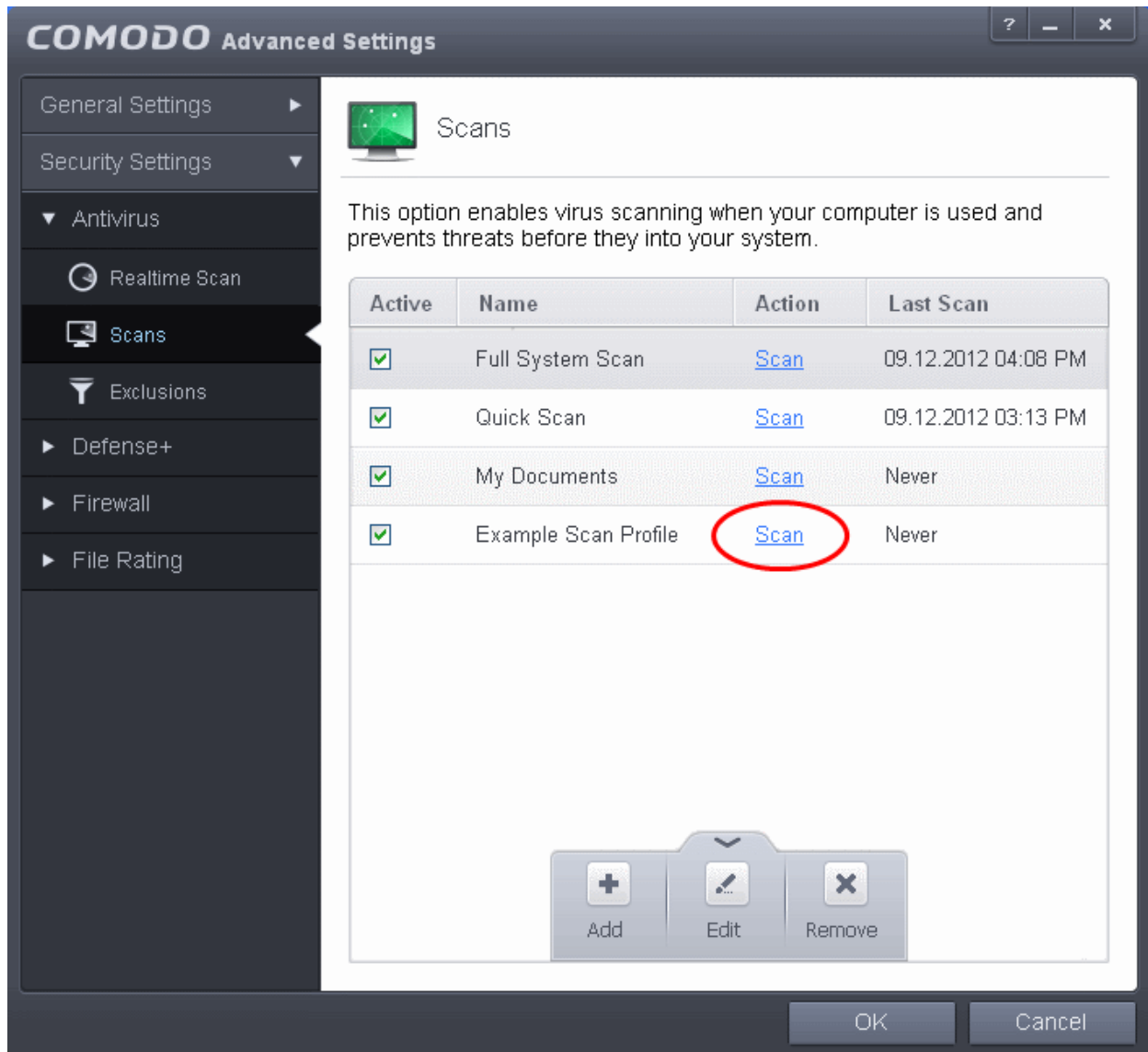
- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
 - **Every Day** - The Antivirus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
 - **Every Week** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
 - **Every Month** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
 - **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adpoter connected to mains supply and not on battery.
 - **Run only when computer id IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
 - **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.
- Click OK to save the profile.

The profile will be available for deployment in future.

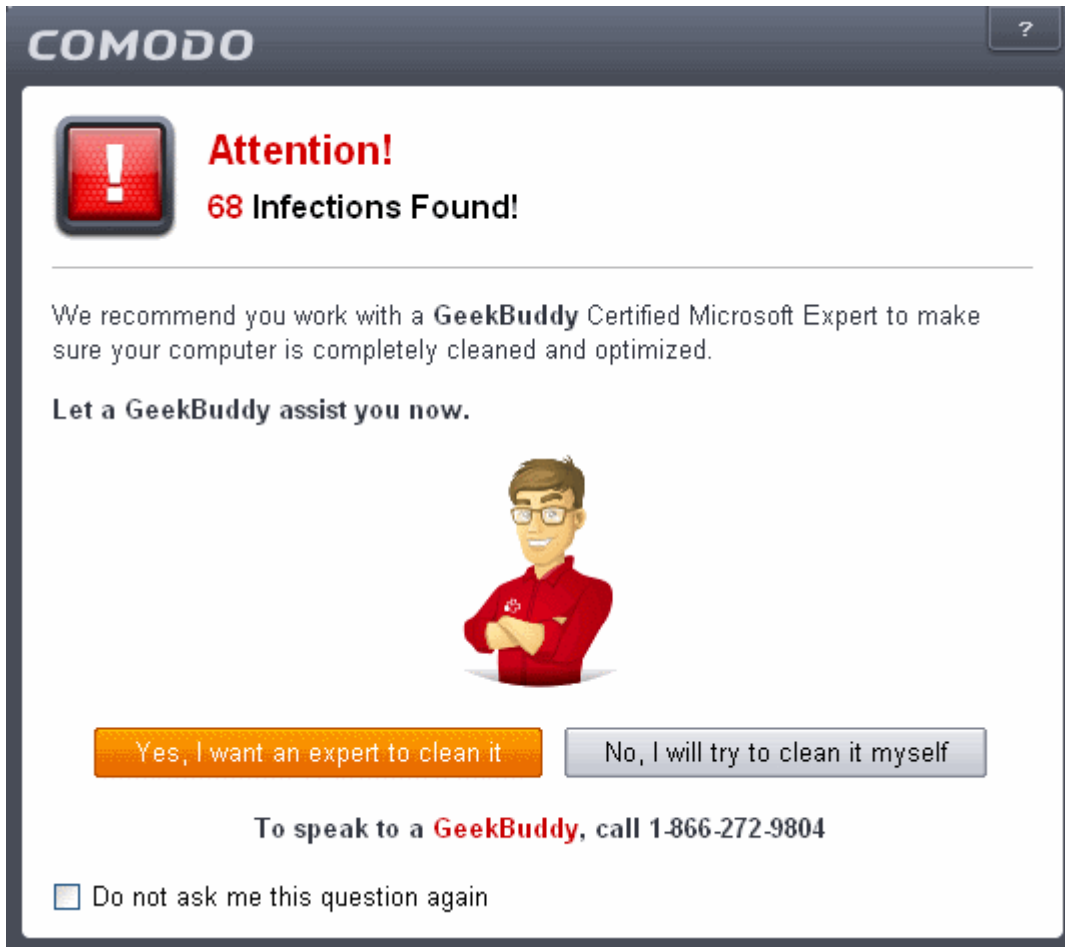


To run a custom scan

- 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.



COMODO

Attention!
68 Infections Found!

We recommend you work with a **GeekBuddy** Certified Microsoft Expert to make sure your computer is completely cleaned and optimized.

Let a **GeekBuddy** assist you now.

Yes, I want an expert to clean it

No, I will try to clean it myself

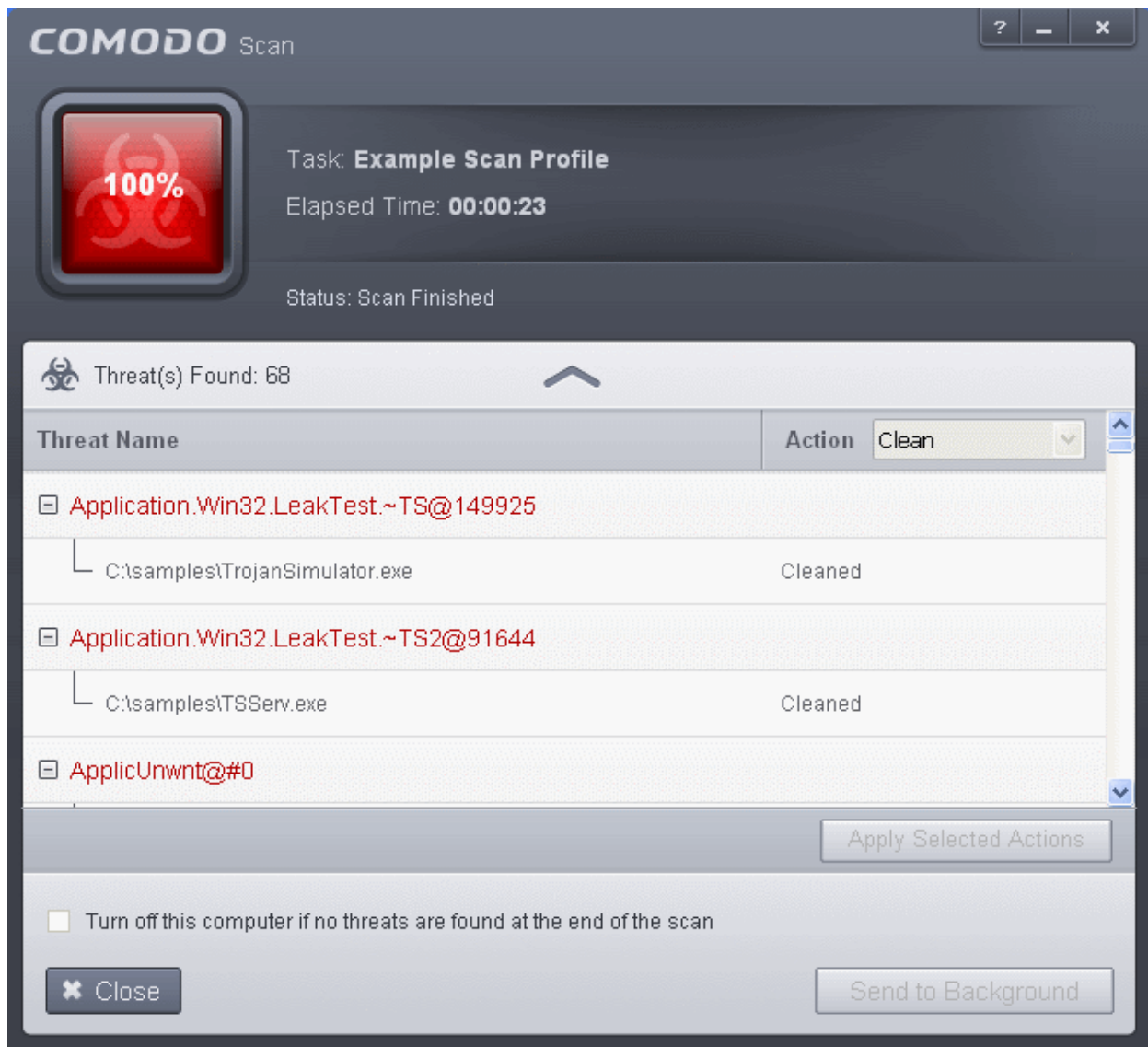
To speak to a **GeekBuddy**, call 1-866-272-9804

Do not ask me this question again

- 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.



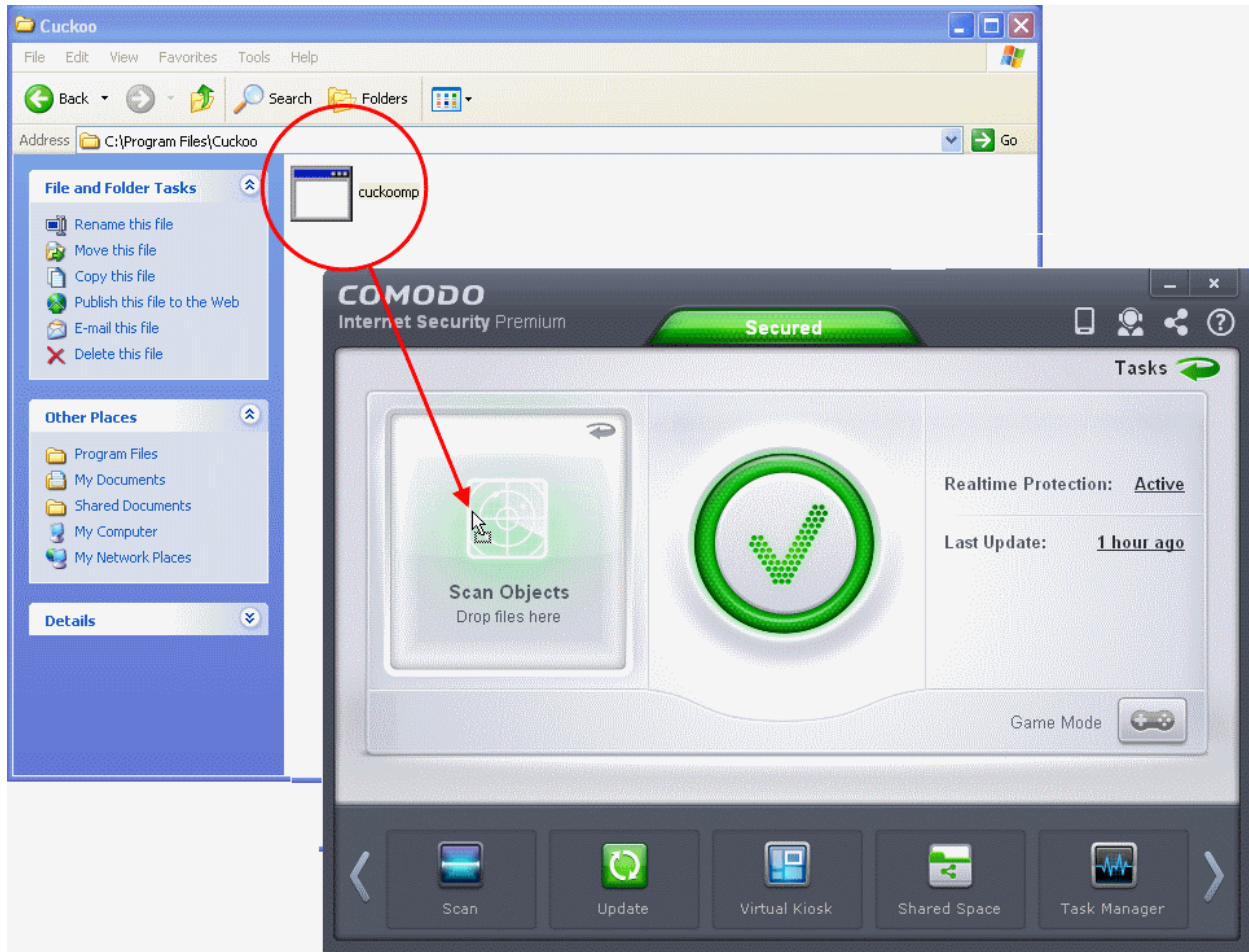
- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

2.2. Instantly Scan Files and Folders

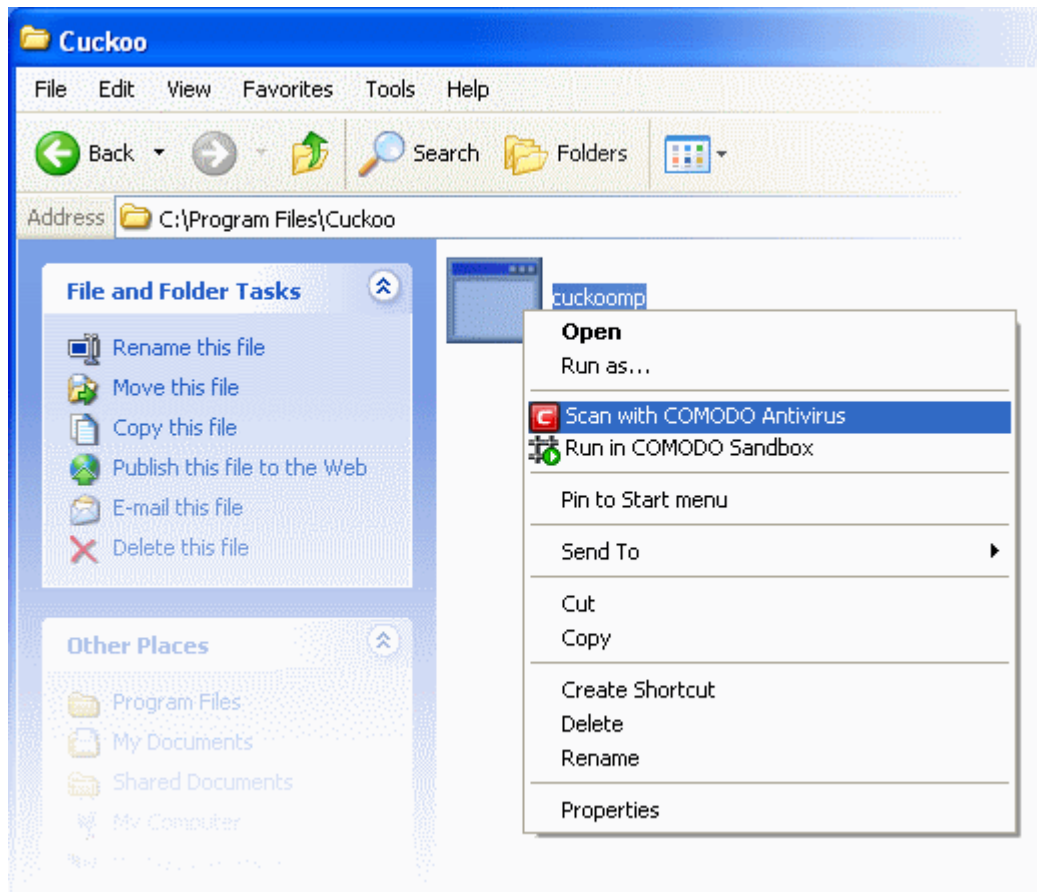
You can scan individual files or folders instantly to check whether it contains any threats or infections. This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from Internet.

To instantly scan an item

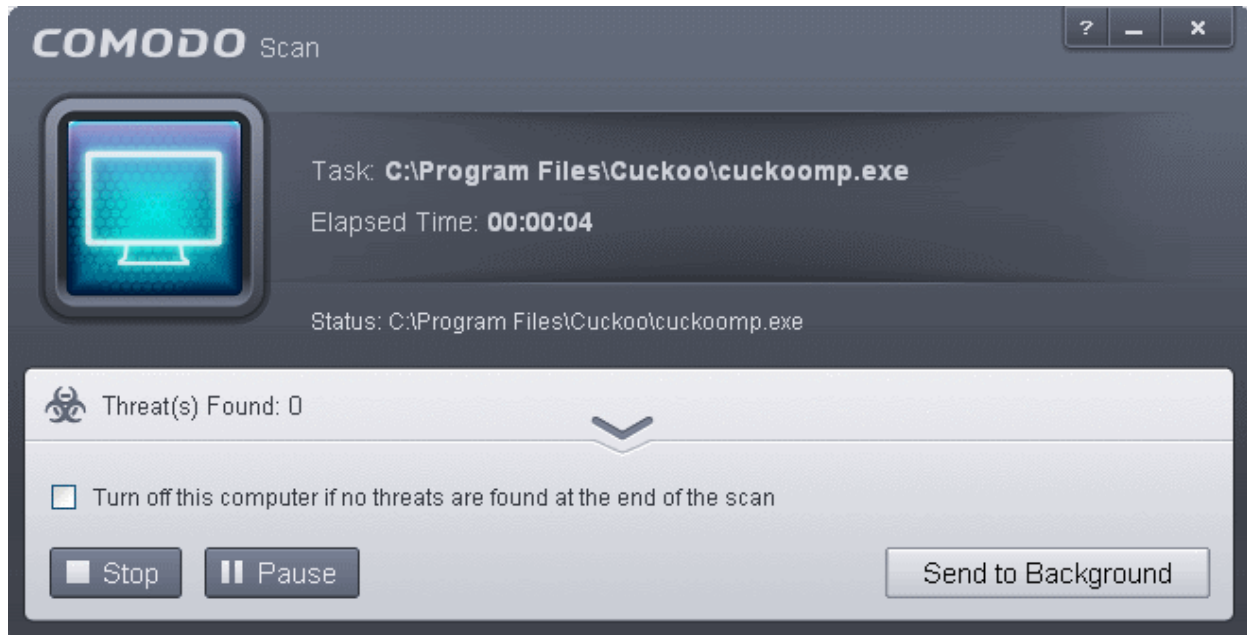
- Drag and drop the item over the area marked 'Scan Objects' in the 'Home' screen of the CIS interface



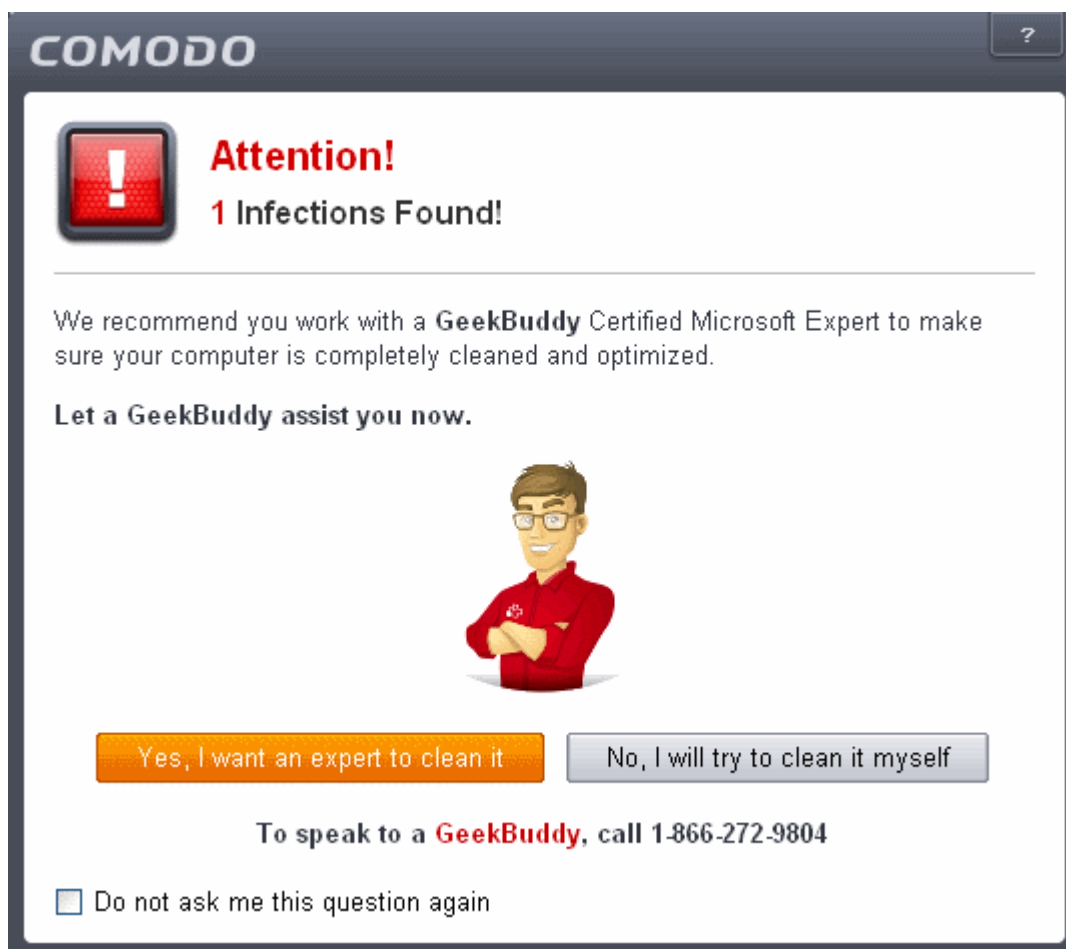
- Alternatively right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



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.

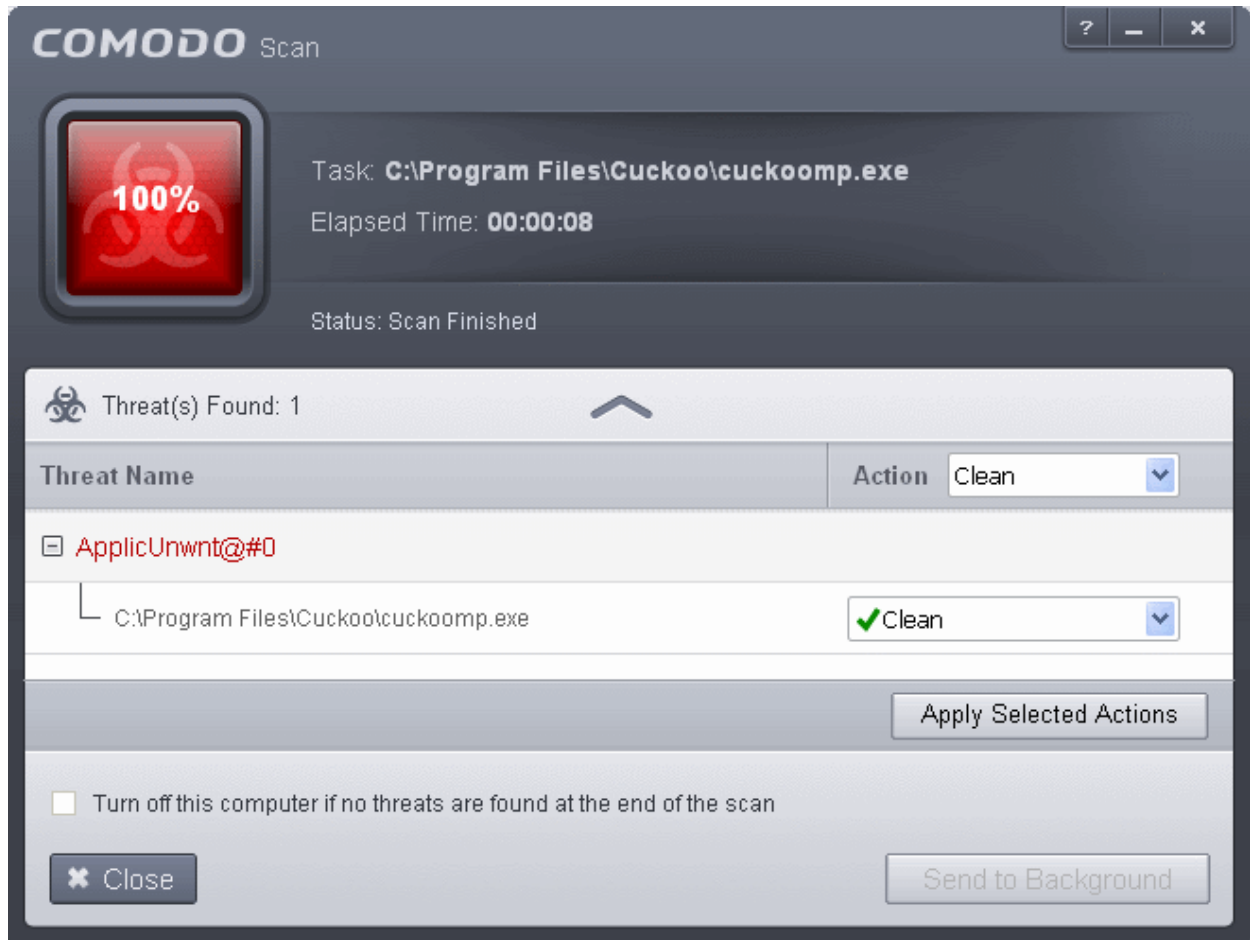


- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up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

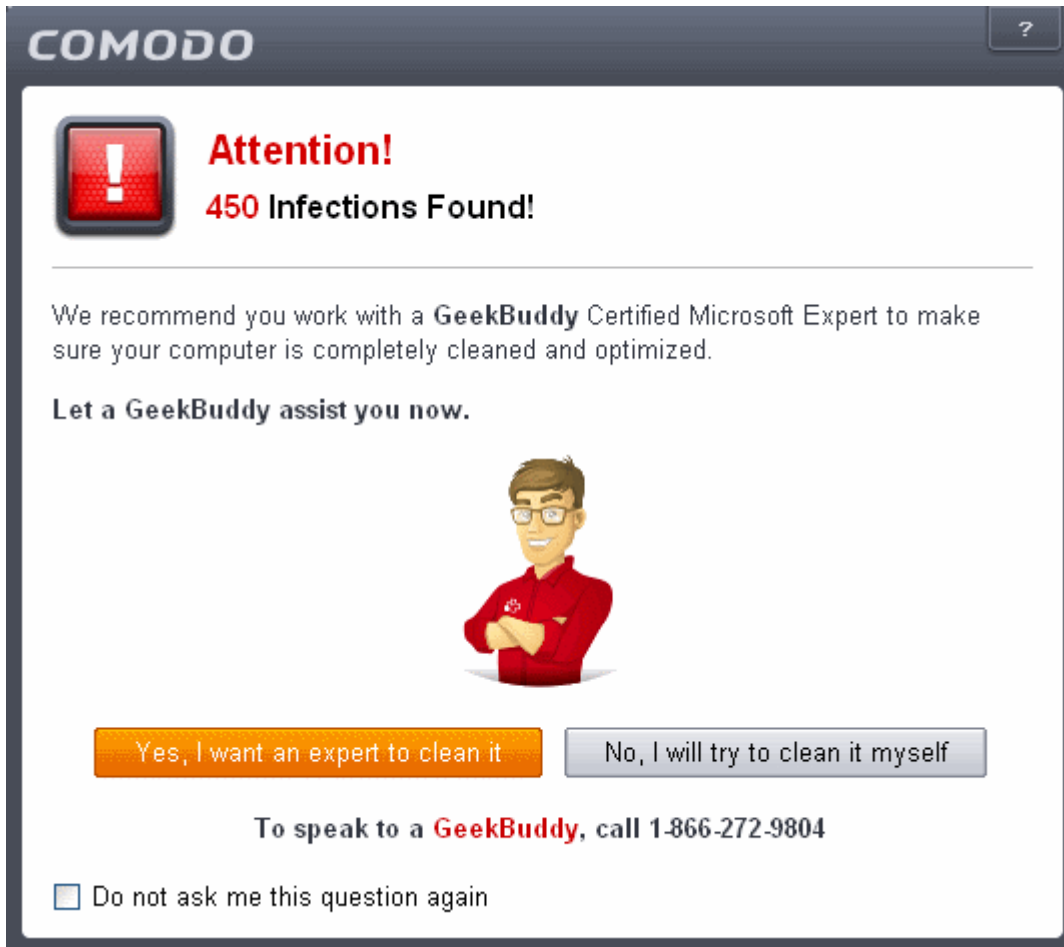
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



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.



COMODO

Attention!
450 Infections Found!

We recommend you work with a **GeekBuddy** Certified Microsoft Expert to make sure your computer is completely cleaned and optimized.

Let a GeekBuddy assist you now.

Yes, I want an expert to clean it **No, I will try to clean it myself**

To speak to a **GeekBuddy**, call **1-866-272-9804**

Do not ask me this question again

- 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](#).

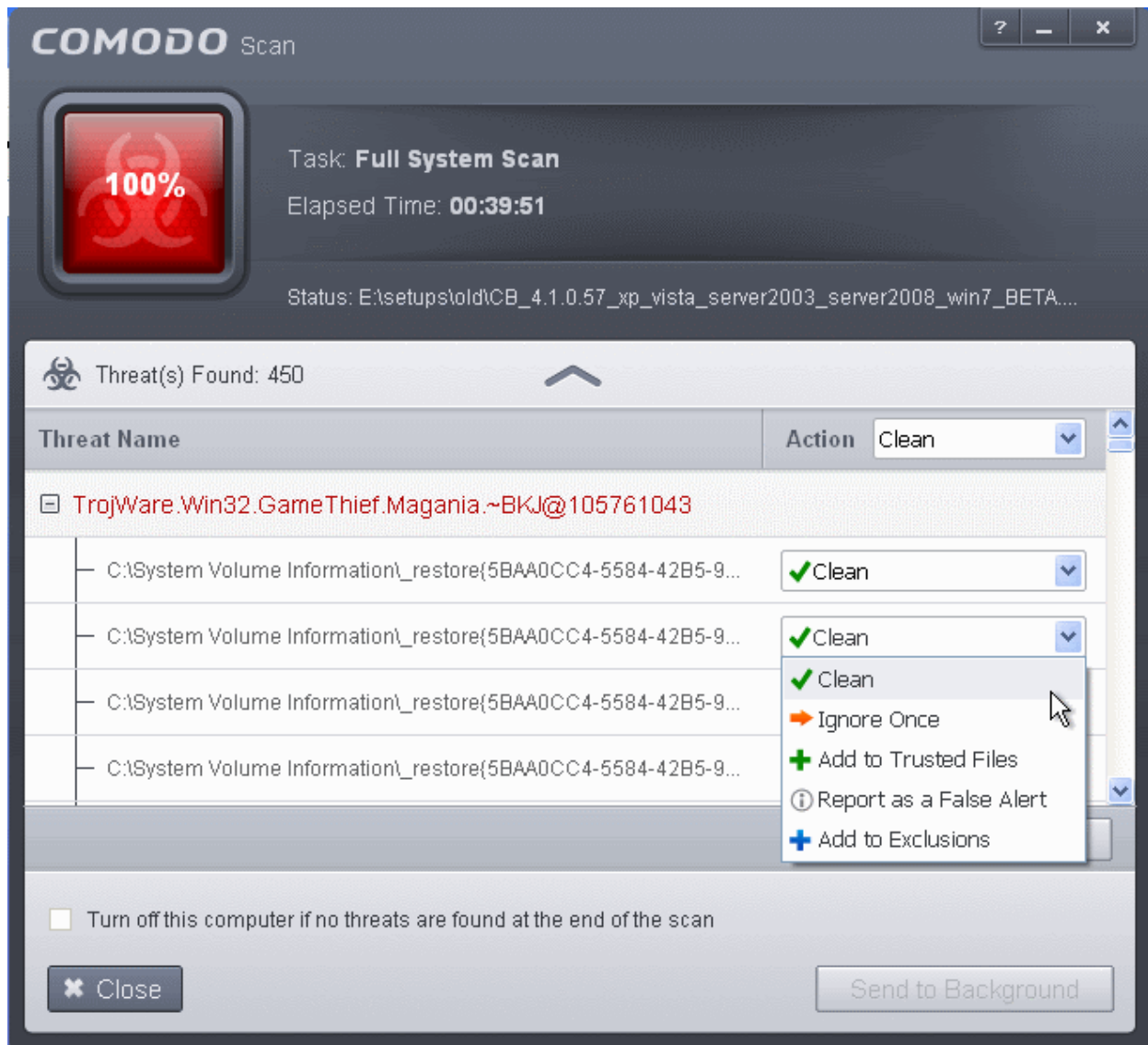
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example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



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

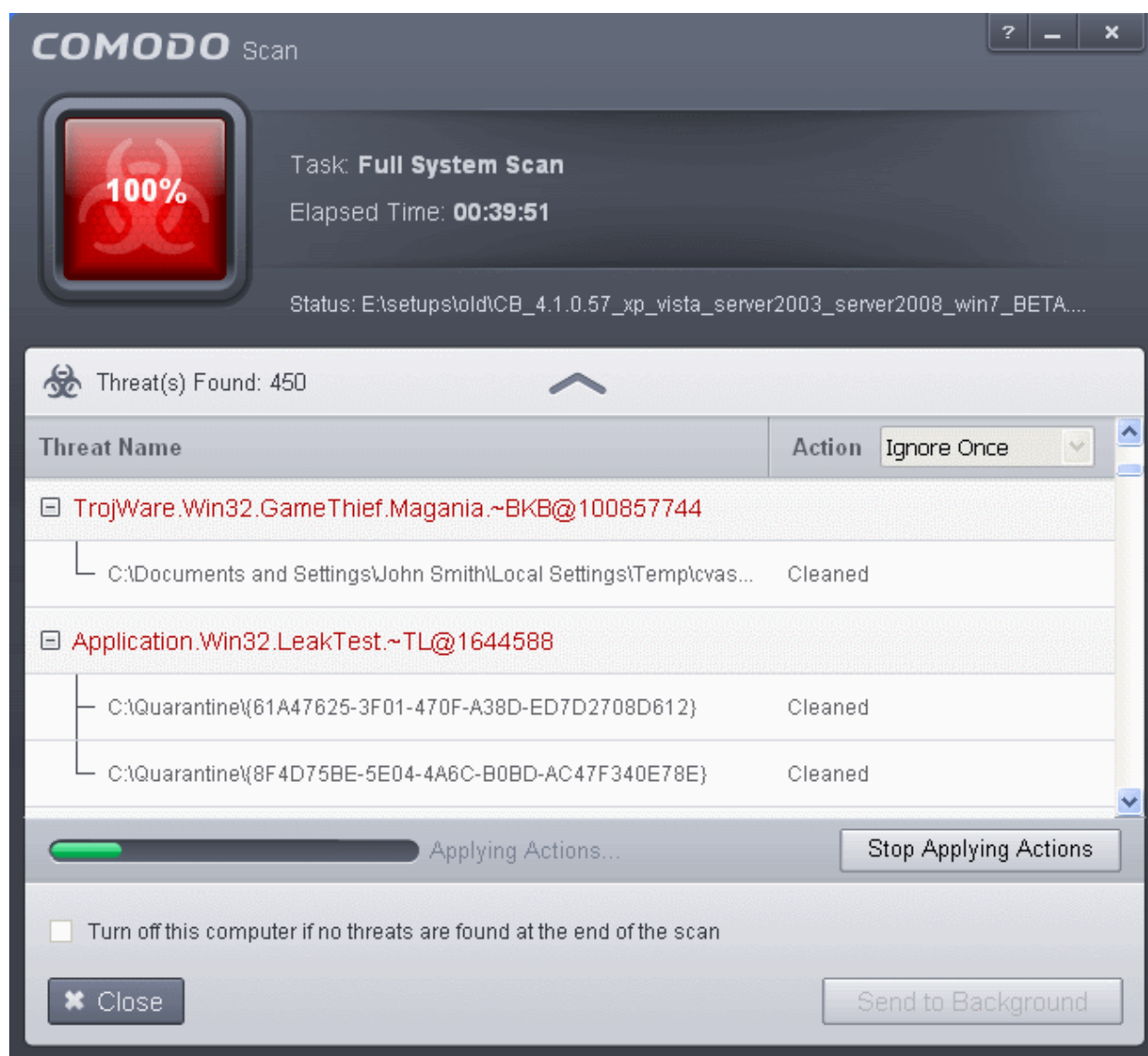


... or the actions to be applied to individual items from the drop-down beside each item.

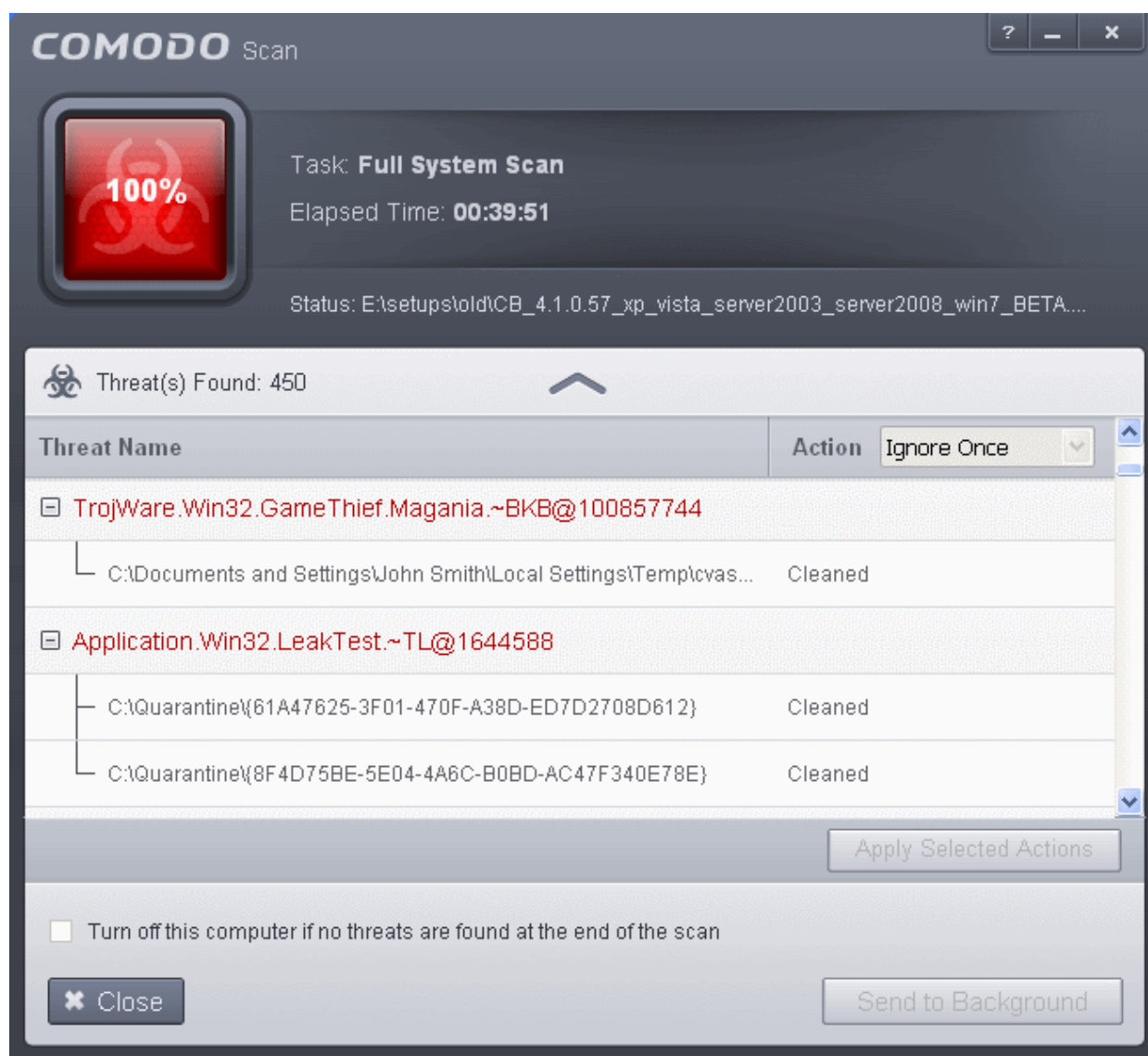


The choices for the actions available are:

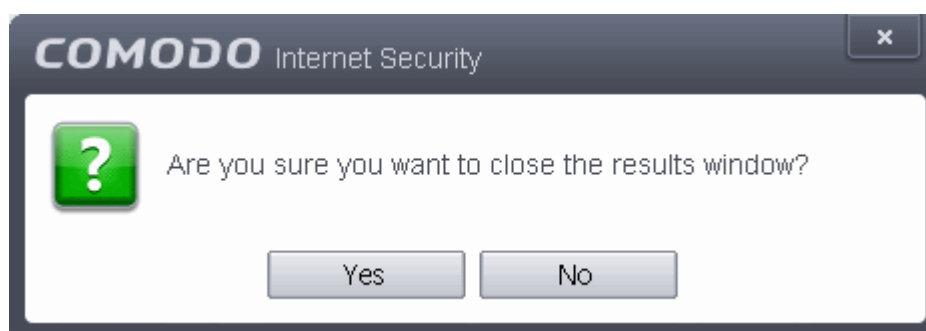
- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application safe. If the disinfection routine is not available, Comodo Antivirus will move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to [Manage Quarantined Items](#).
- **Ignore Once** - If you want to ignore the threat this time only, select 'Ignore Once'. The file will be ignored only at that time. If the same application invokes again, the Antivirus will report it as a threat.
- **Add to Trusted Files** - If you trust the file, select 'Add to Trusted Files'. The file will be 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...



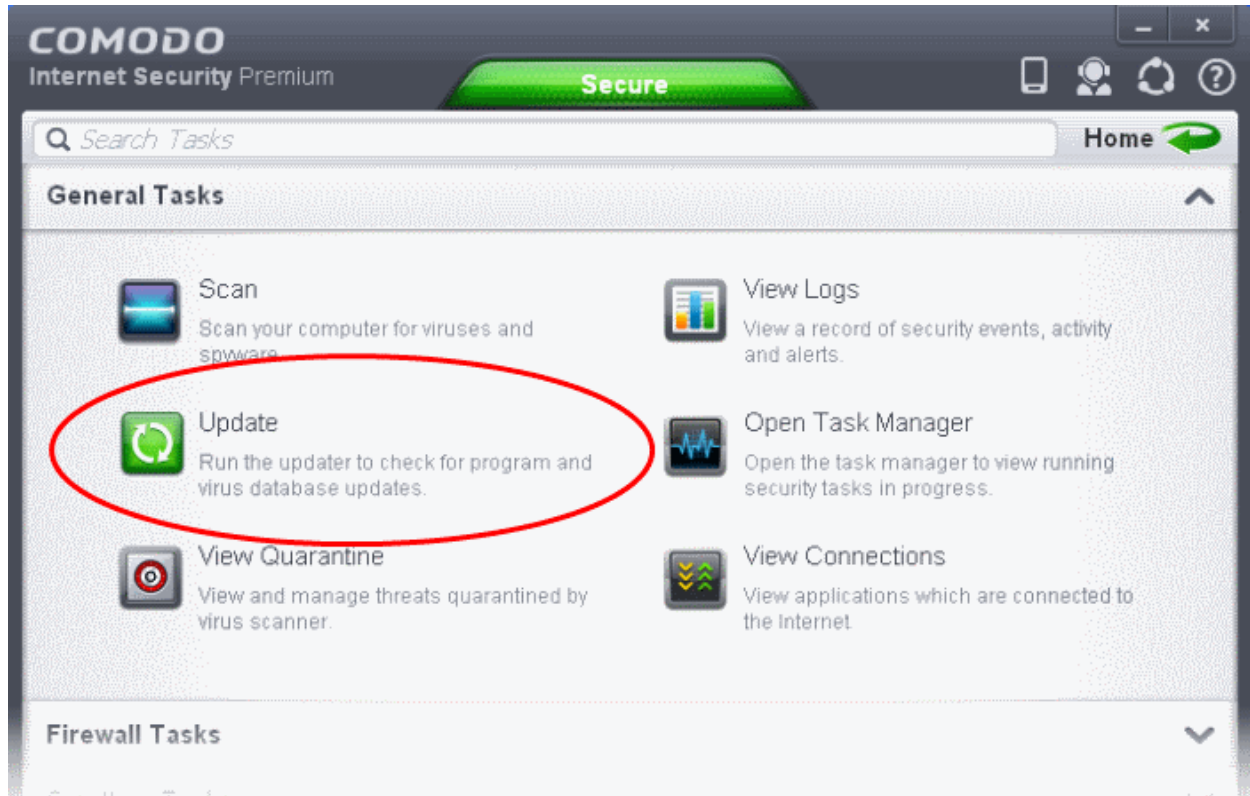
... and click 'Yes' in the confirmation window.

2.4. Manage Virus Database and Program Updates

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

To manually check for the latest virus Database and program updates

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



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



If the updates are available, they will be downloaded.

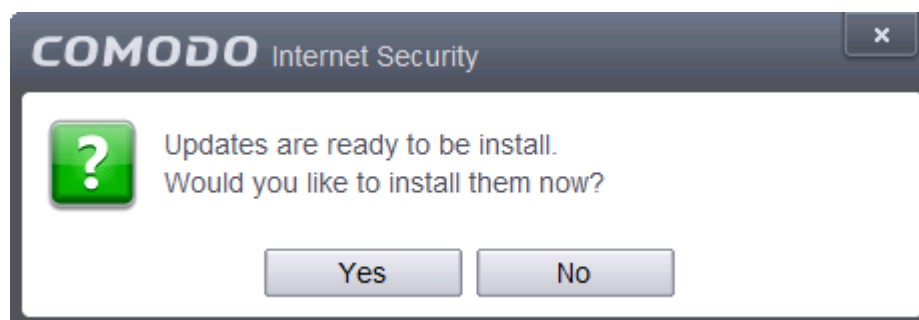


Note: You must be connected to Internet to download the updates.

The virus signature database will be updated on completion.



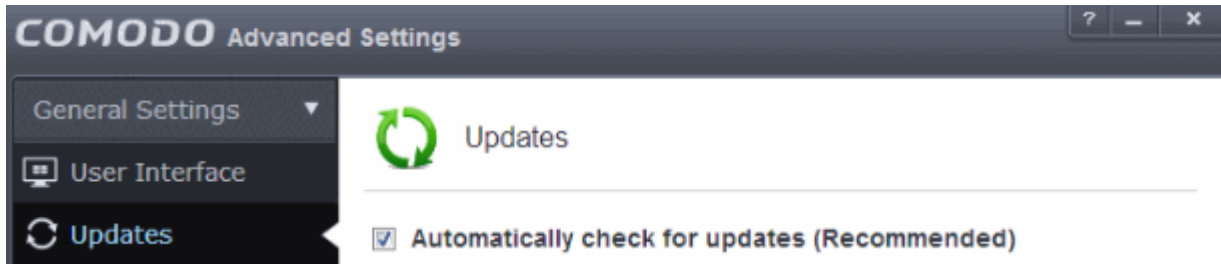
If any program updates are available, they will be downloaded and a confirmation dialog will be displayed before installing them.



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

Automatic Updates

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

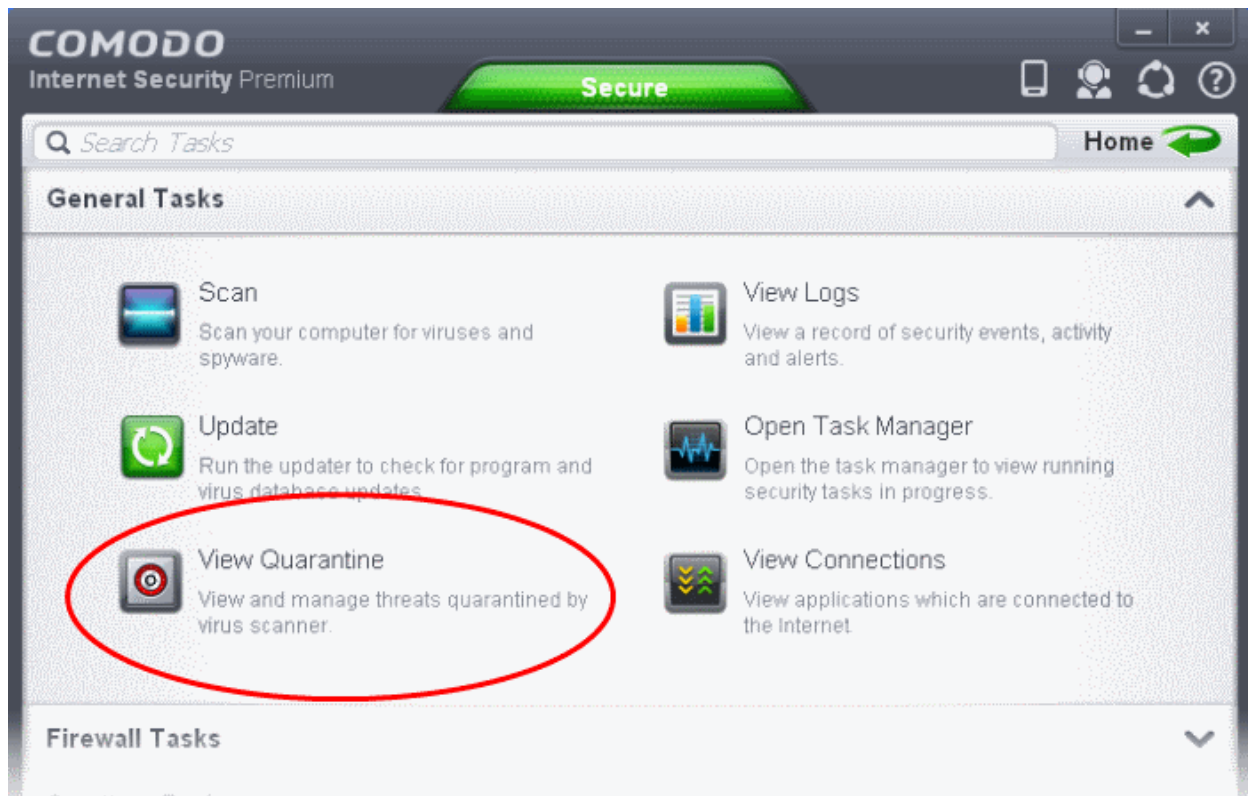


You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. Refer to [Scan Profiles](#) for more details.

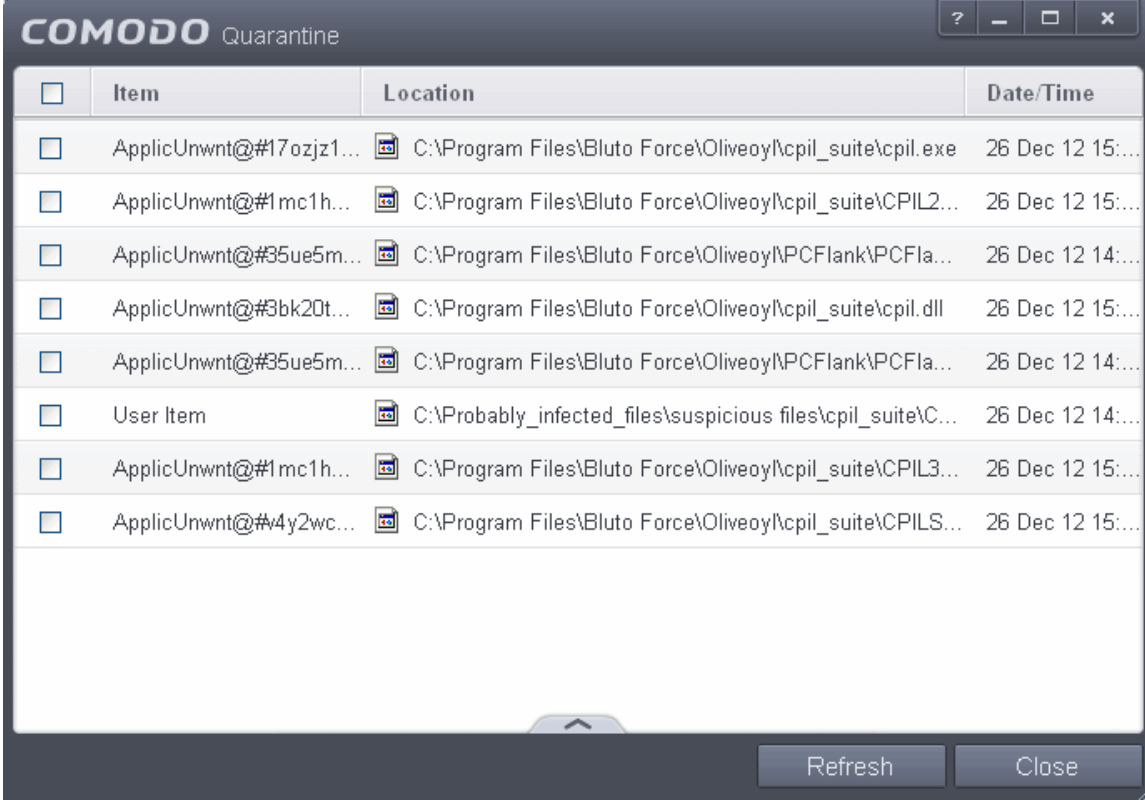
2.5. Manage Quarantined Items

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.



<input type="checkbox"/>	Item	Location	Date/Time
<input type="checkbox"/>	ApplicUnwnt@#17ozjz1...	C:\Program Files\Bluto Force\Oliveoy\cpil_suite\cpil.exe	26 Dec 12 15:...
<input type="checkbox"/>	ApplicUnwnt@#1mc1h...	C:\Program Files\Bluto Force\Oliveoy\cpil_suite\CPIL2...	26 Dec 12 15:...
<input type="checkbox"/>	ApplicUnwnt@#35ue5m...	C:\Program Files\Bluto Force\Oliveoy\PCFlank\PCFla...	26 Dec 12 14:...
<input type="checkbox"/>	ApplicUnwnt@#3bk20t...	C:\Program Files\Bluto Force\Oliveoy\cpil_suite\cpil.dll	26 Dec 12 15:...
<input type="checkbox"/>	ApplicUnwnt@#35ue5m...	C:\Program Files\Bluto Force\Oliveoy\PCFlank\PCFla...	26 Dec 12 14:...
<input type="checkbox"/>	User Item	C:\Probably_infected_files\suspicious files\cpil_suite\C...	26 Dec 12 14:...
<input type="checkbox"/>	ApplicUnwnt@#1mc1h...	C:\Program Files\Bluto Force\Oliveoy\cpil_suite\CPIL3...	26 Dec 12 15:...
<input type="checkbox"/>	ApplicUnwnt@#4y2wc...	C:\Program Files\Bluto Force\Oliveoy\cpil_suite\CPILS...	26 Dec 12 15:...

Refresh Close

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](#).

The Quarantined Items interface also allows you to:

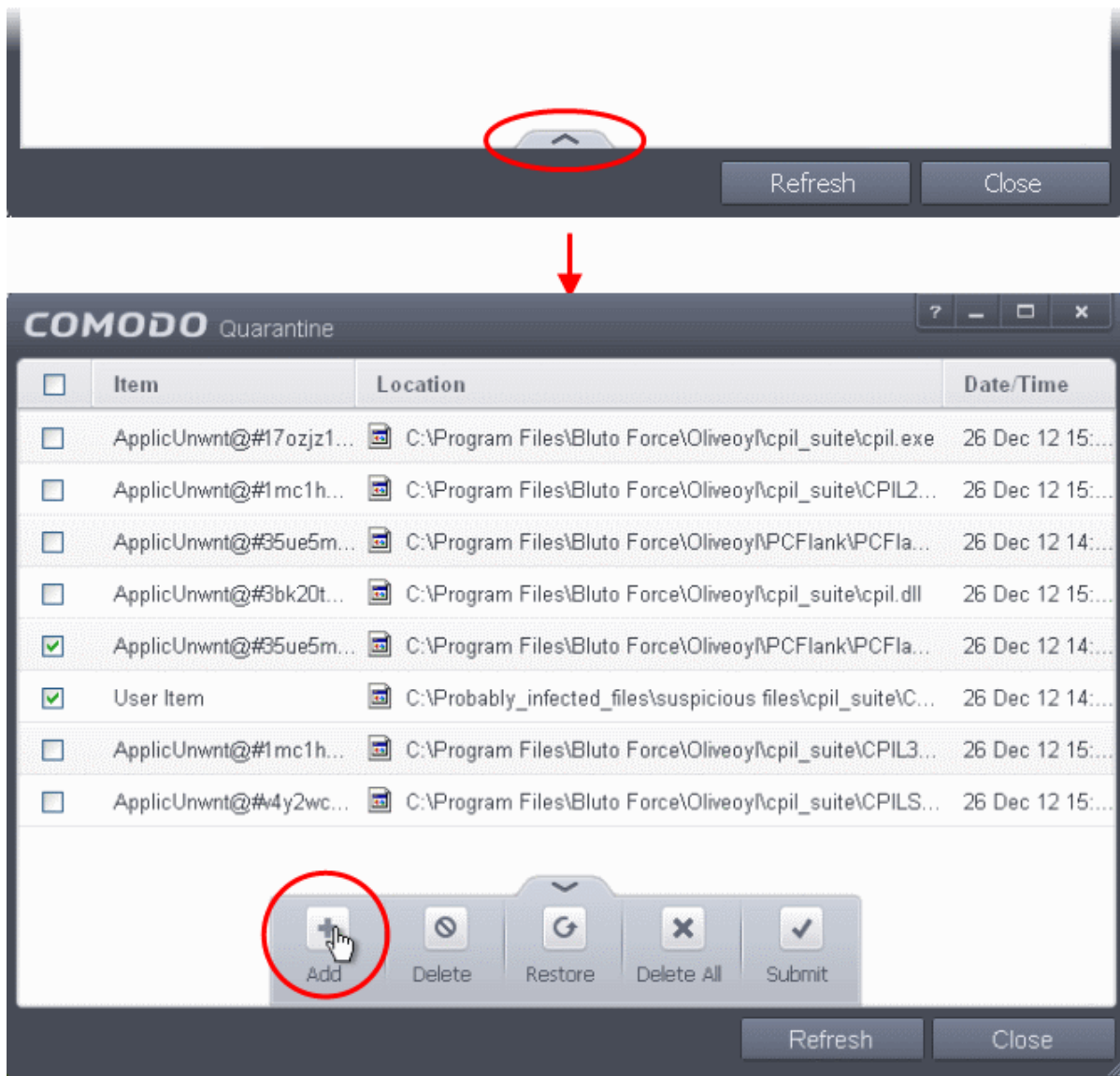
- **Manually add applications, executables or other files, that you do not trust, as a Quarantined item**
- **Delete a selected quarantined item from the system**
- **Restore a quarantined item to oits original location**
- **Delete all quarantined items**
- **Submit selected quarantined items to Comodo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

Manually adding files as Quarantined Items

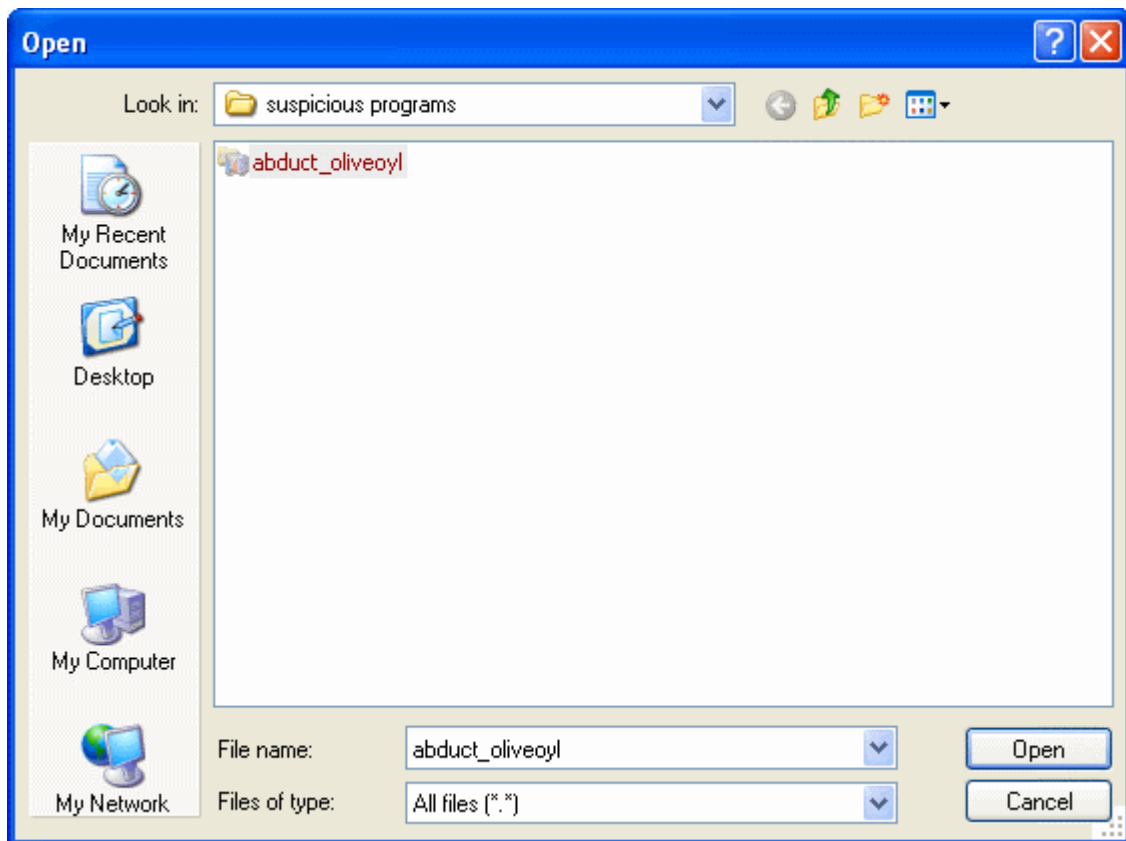
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

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.

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.

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

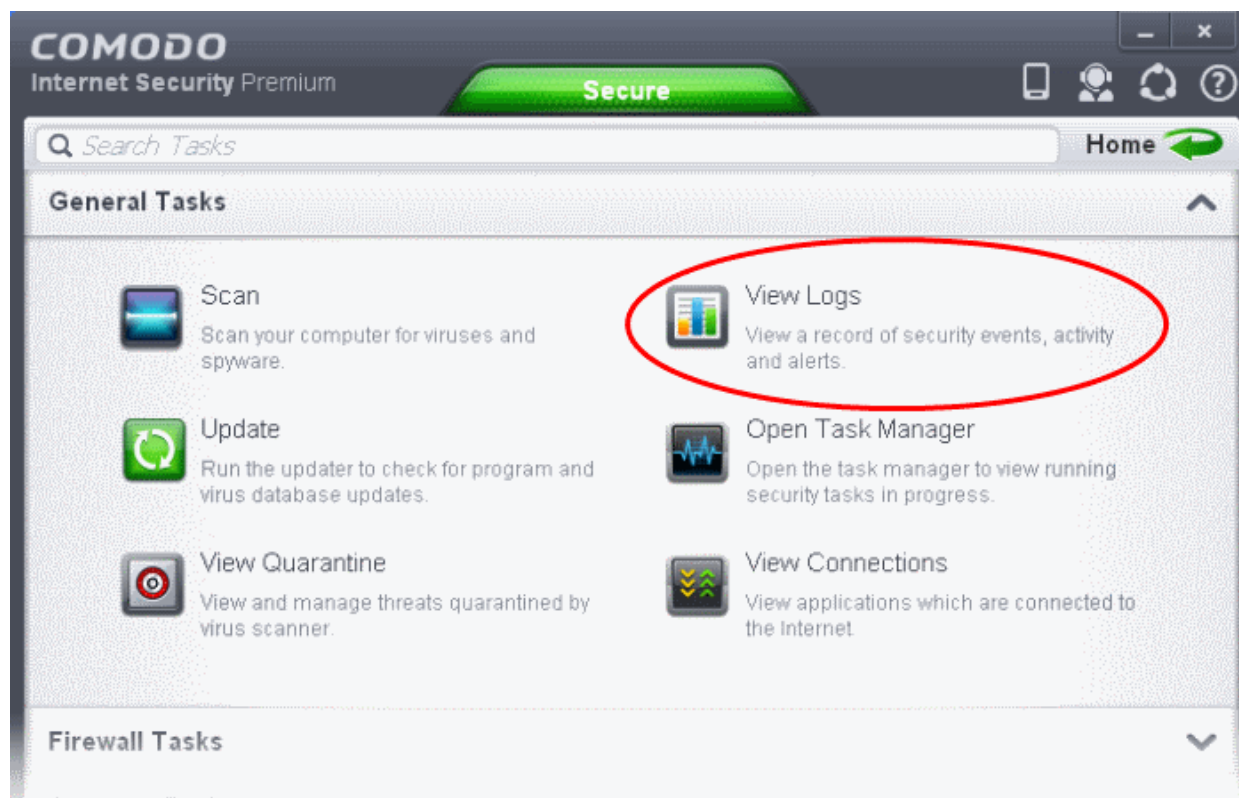
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

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](#)
- [Firewall](#)
- [Defense+](#)

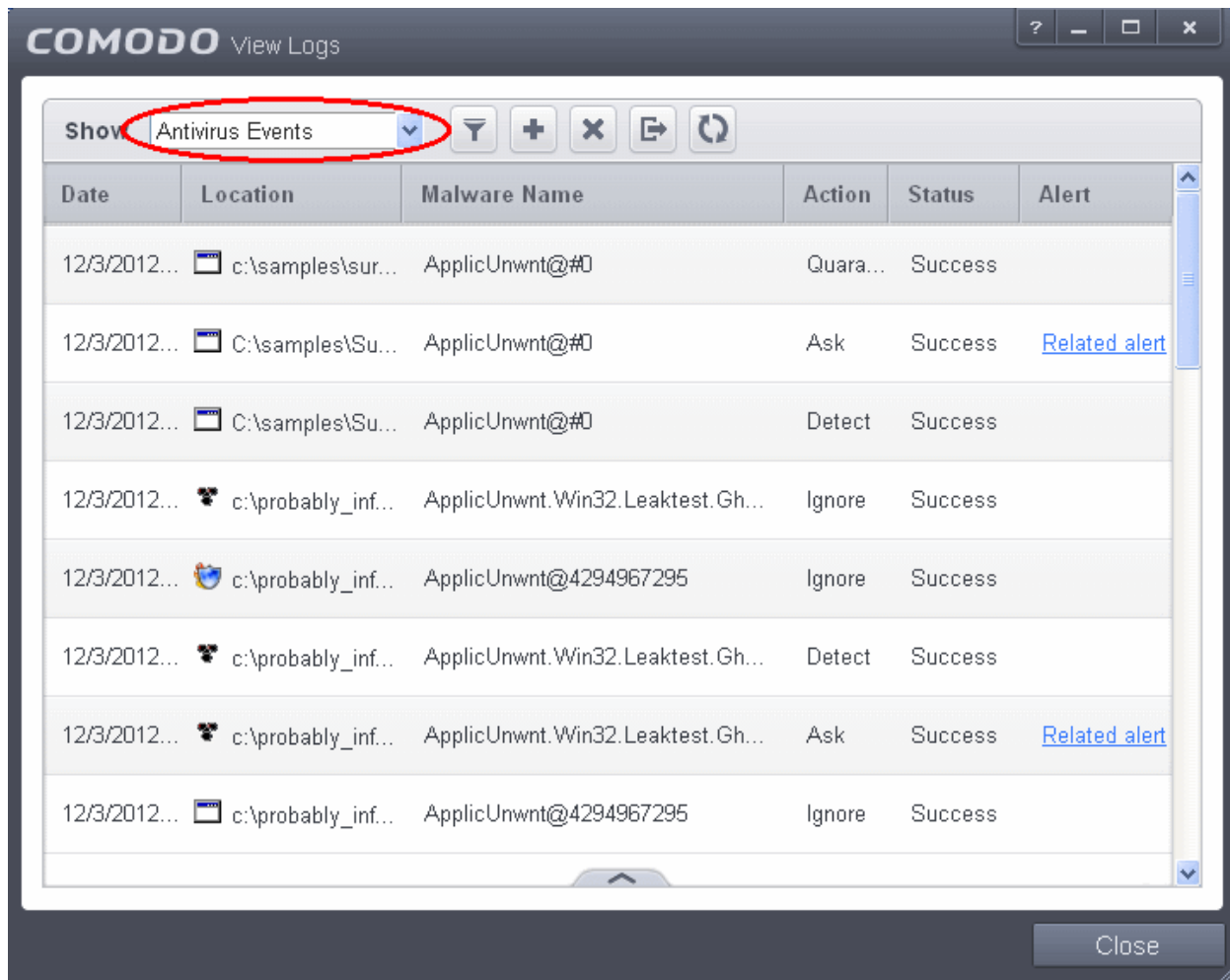
'Other Logs':

- [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.




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

- To export the Antivirus logs as a HTML file click the 'Export' button .

- To open a stored CIS log file, click the 'Open' button .

- To refresh the Antivirus logs, click the 'Refresh' button .

- To clear the Antivirus logs click the 'Clear' button .

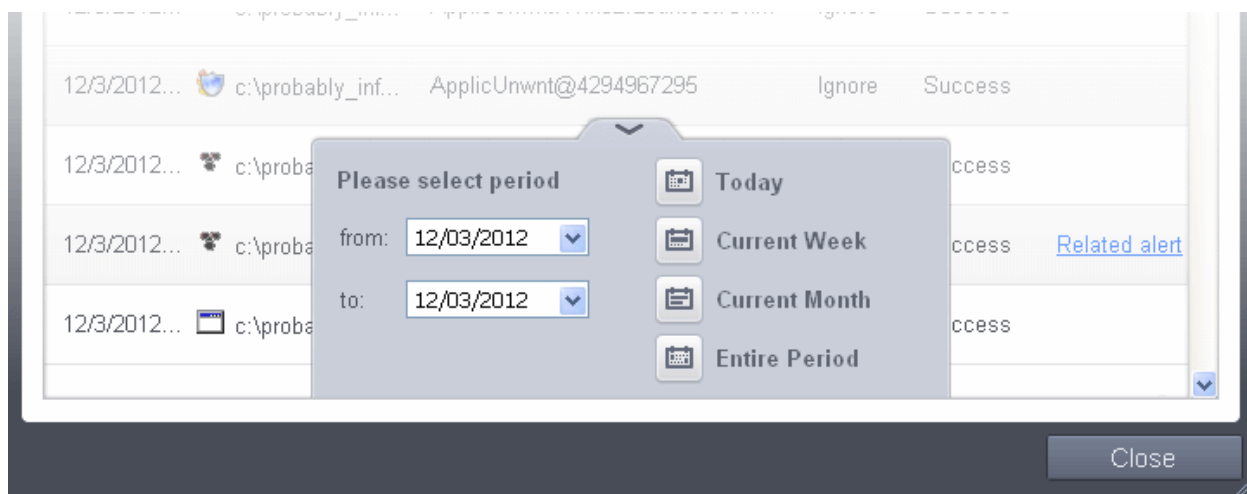
2.6.1.1. Filtering Antivirus Logs

Comodo 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'

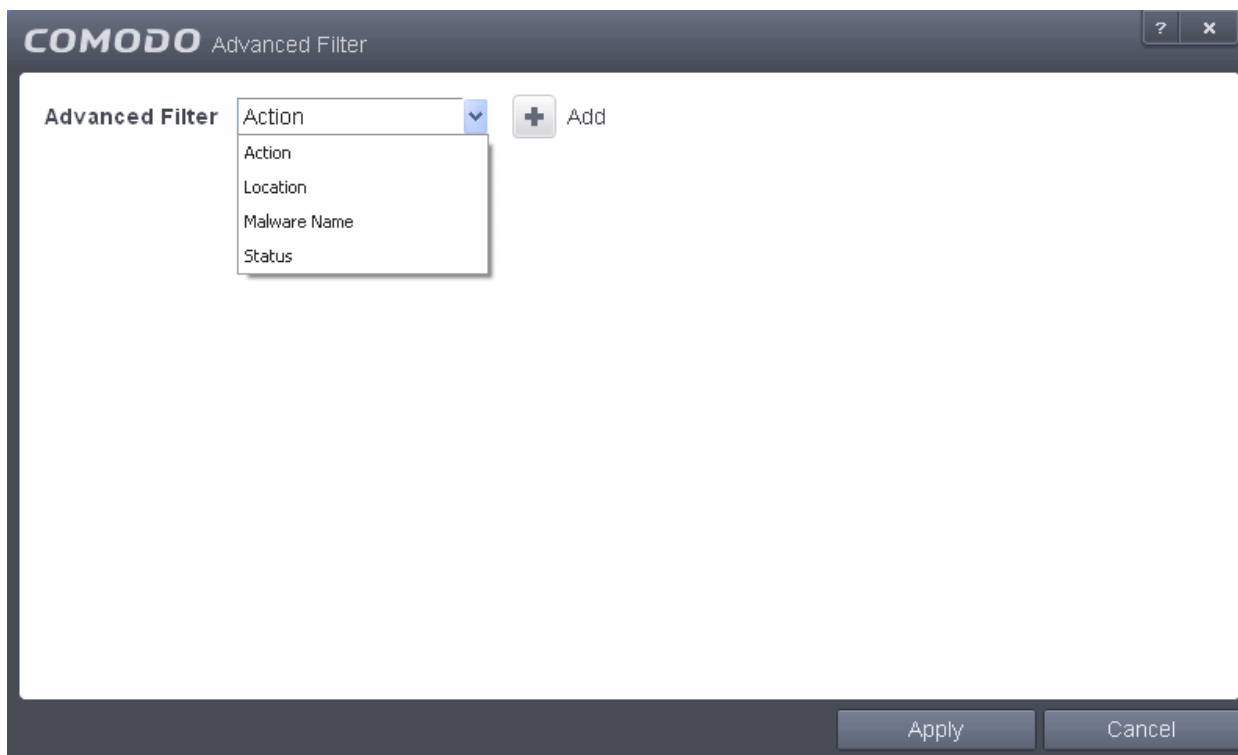
Advanced Filters:

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

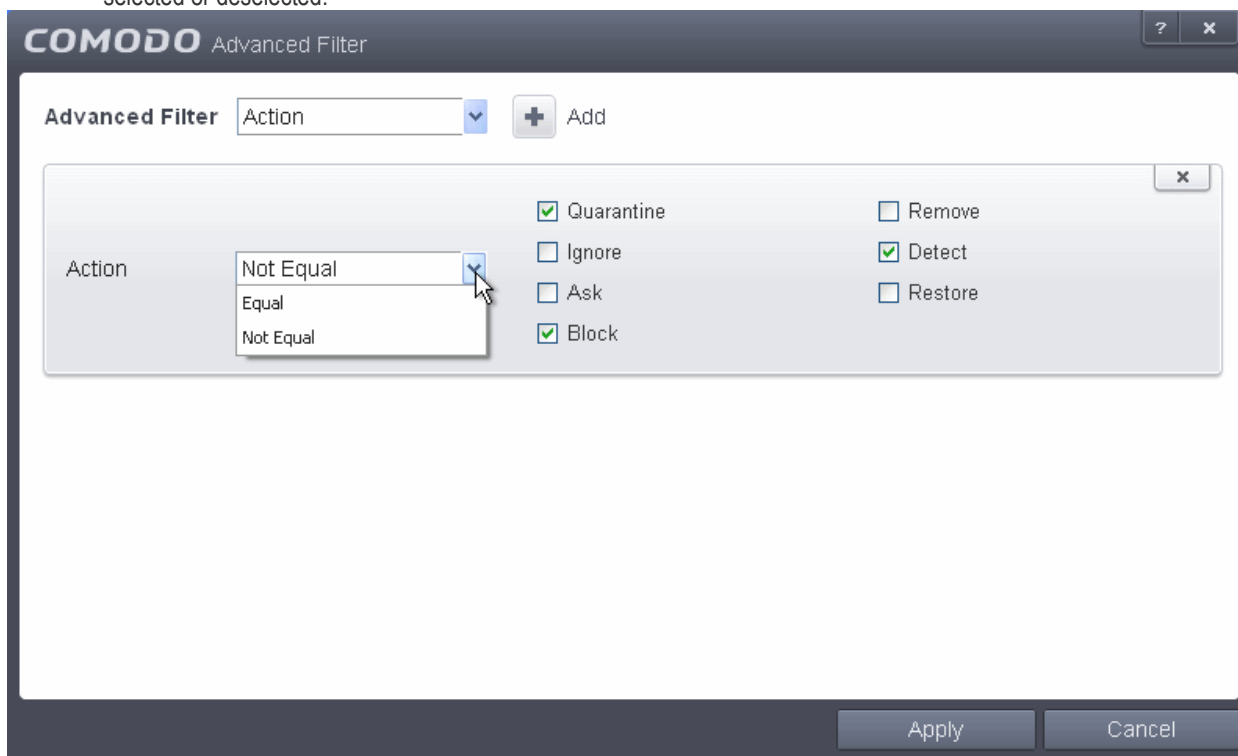
- Click the funnel button  from the title bar. The Advanced Filter interface for AV events will open
- Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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.

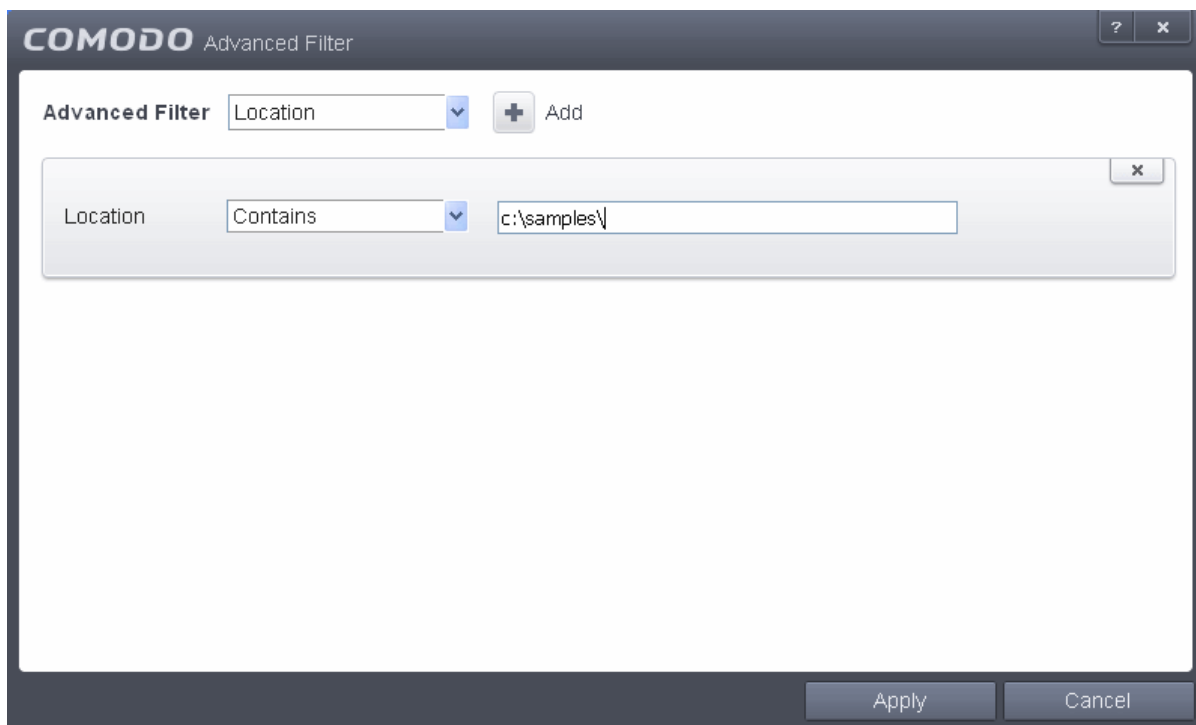


- a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- 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.

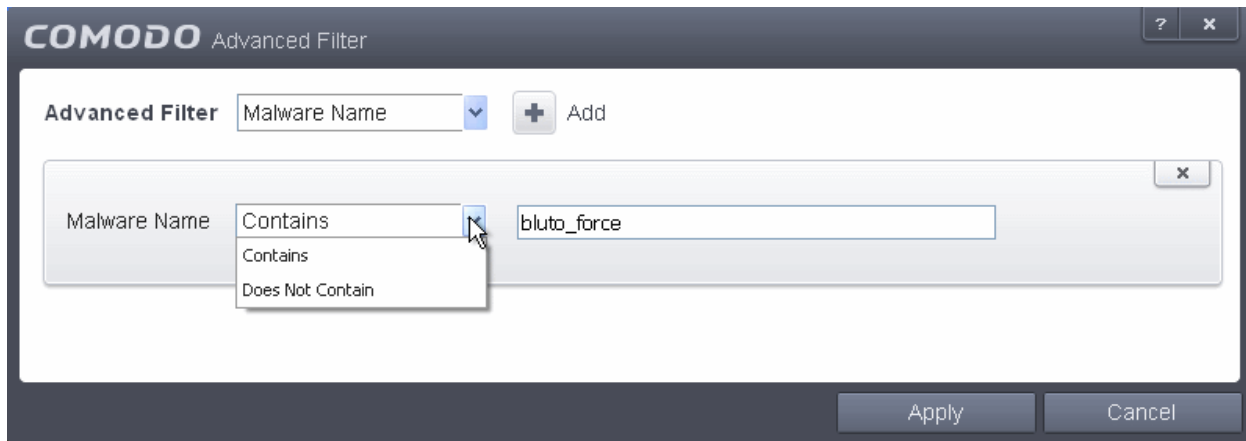
- Location:** The 'Location' option enables you to filter the log entries related to events logged from a specific location. Selecting the 'Location' option displays a drop-down field and text entry field.



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

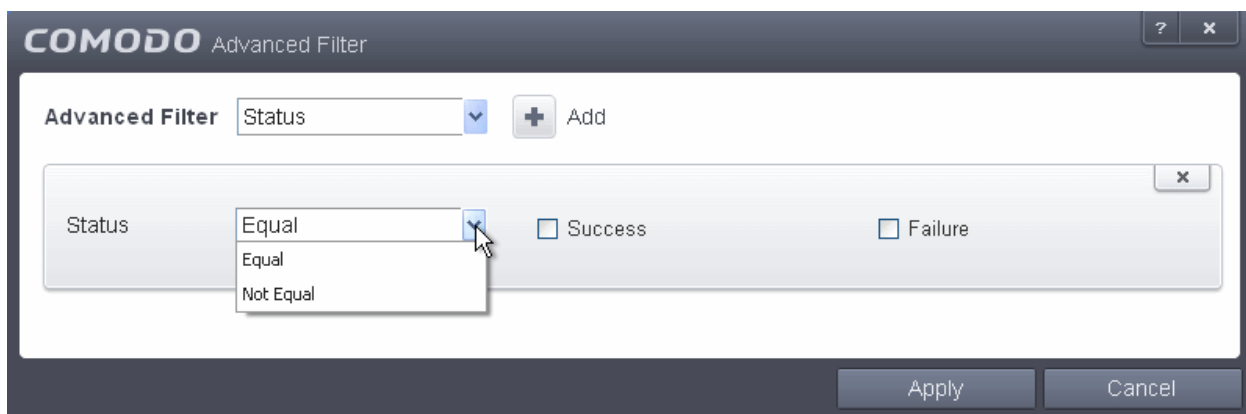
- Malware Name:** The 'Malware Name' option enables you to filter the log entries related to specific malware. Selecting the 'Malware Name' option displays a drop-down field and text entry field.



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

- iv. **Status:** The 'Status' option allows you to filter the log entries based on the success or failure of the action taken against the threat by 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)

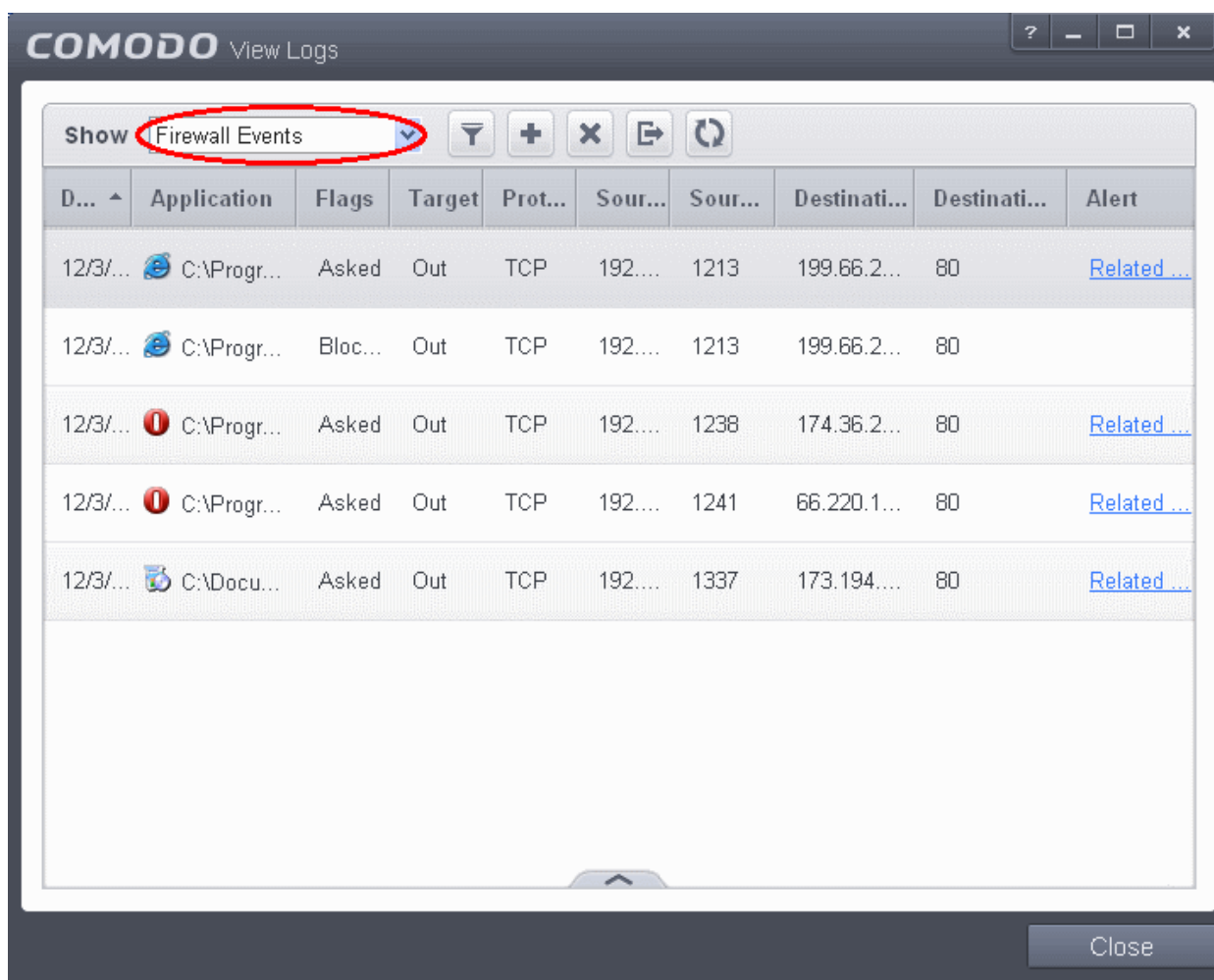
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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.

2.6.2. 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.



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. **Flags** - 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 .

- To open a stored CIS log file, click the Open button .

- To refresh the Firewall logs, click the Refresh button .

- To clear the Firewall logs click the Clear button .

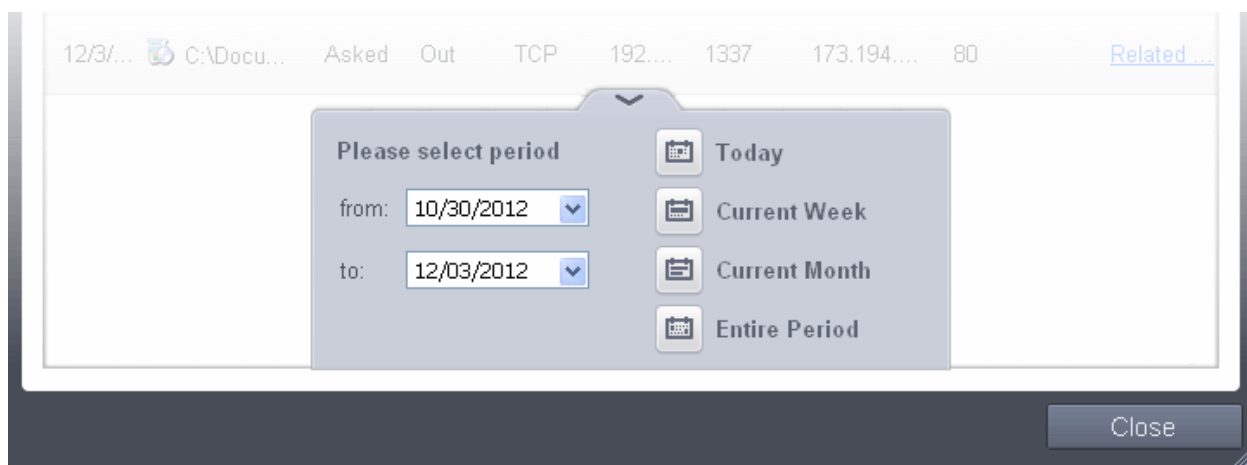
2.6.2.1. Filtering Firewall Logs

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'


Advanced Filters

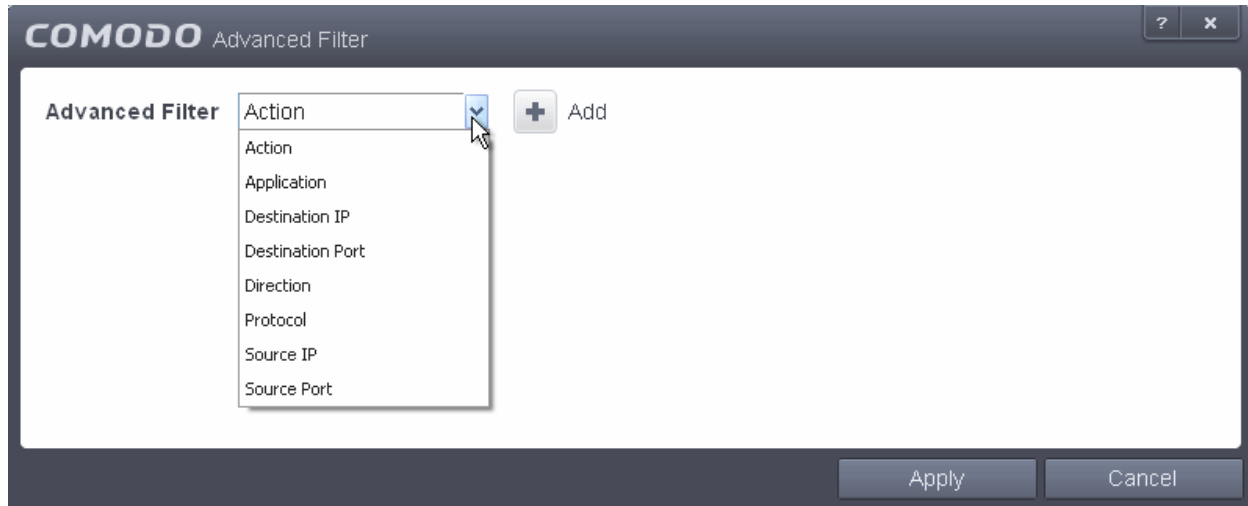
Having chosen a **preset time filter**, you can further refine the displayed events according to specific filters. Following are available filters for Firewall logs and their meanings:

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

- **Source Port** - Displays only the events that originated from a specific port number

To configure Advanced Filters for Firewall events

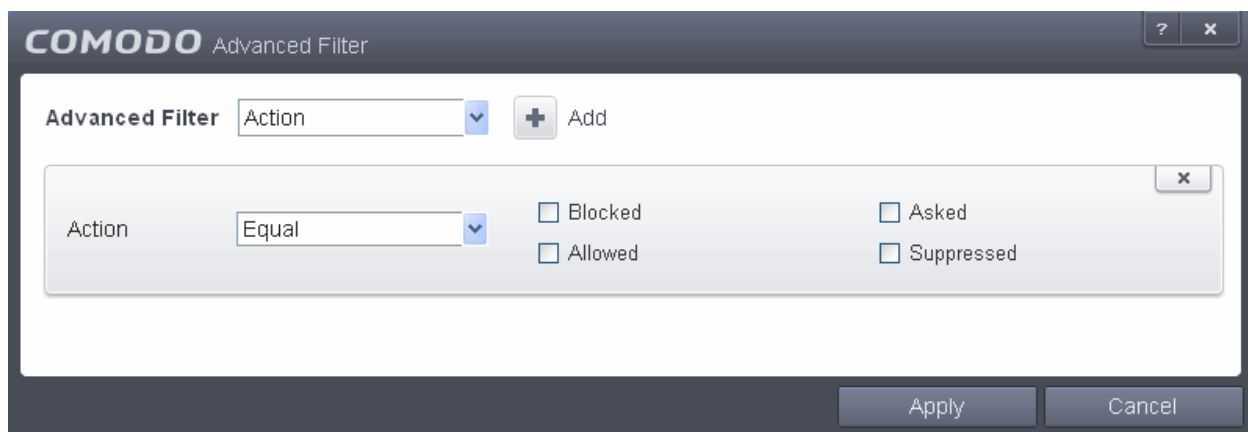
1. Click the funnel button  from the title bar. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



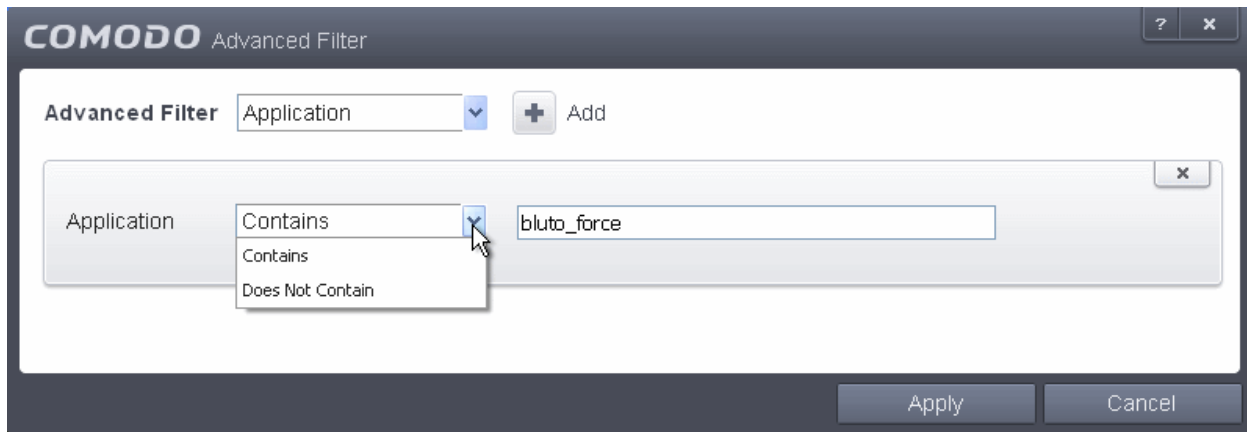
You have 8 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

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

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



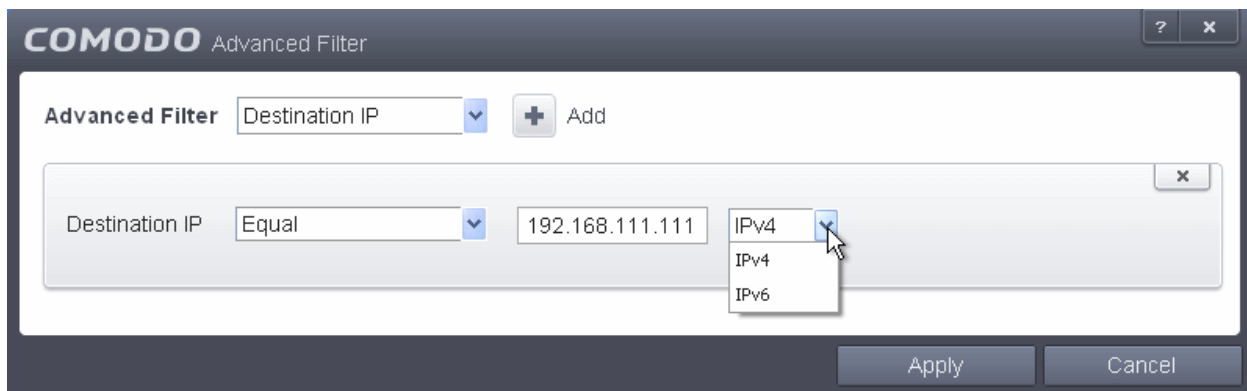
- Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
 - Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
 - **Blocked:** Displays list of events that were blocked
 - **Allowed:** Displays 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
- 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 select 'Contains' option from the drop-down field and enter the phrase 'bluto-force' in the text field, then all events containing the entry 'bluto-force' in the 'Application' column will be displayed. If you select 'Does Not Contain' option from the drop-down field and enter the phrase 'bluto-force' in the text field, then all events that do not have the entry 'bluto-force' in the 'Application' column will be displayed.

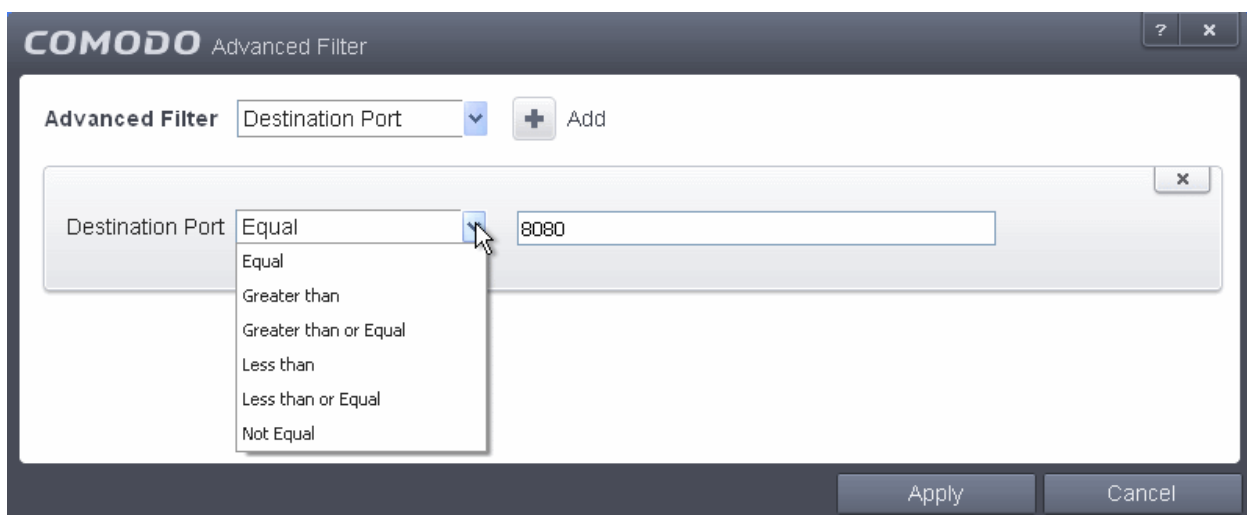
- iii. **Destination IP:** Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.



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

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

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

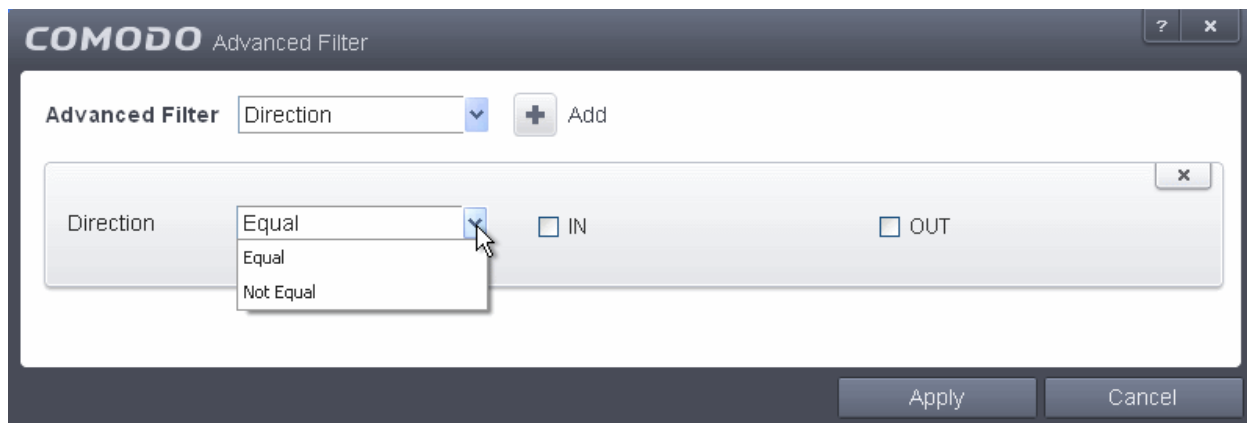


- a) Select any one of the following option the drop-down box.
- Equal
 - Greater than
 - Greater than or Equal
 - Less than
 - Less than or Equal
 - Not Equal

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

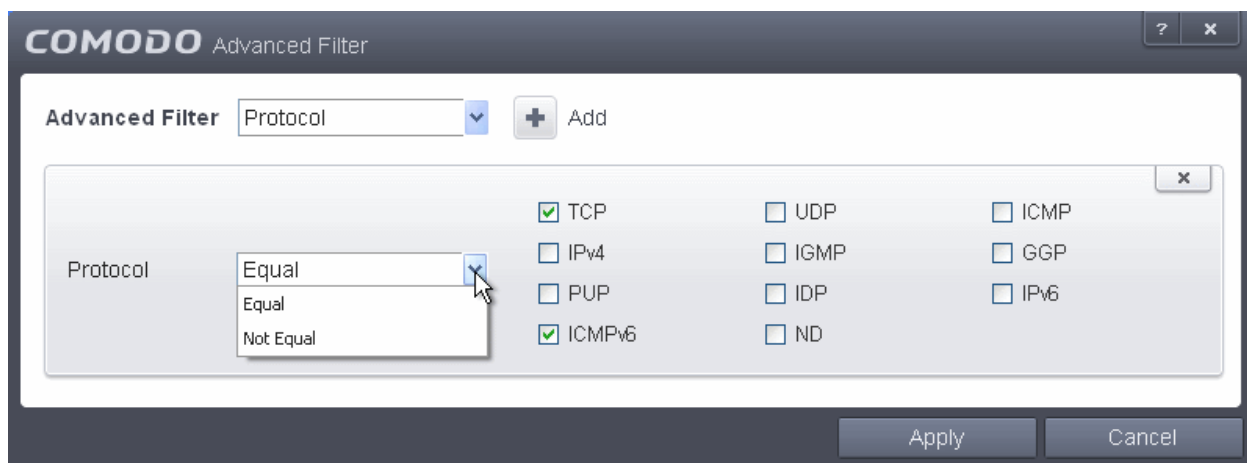
For example, if you select 'Equal' option from the drop-down field and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

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



- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Now select the check box of the specific filter parameters to refine your search. The parameter available are:
- In: Displays a list of events that were directed into the system
 - Out: Displays a list of events that were directed out of the system

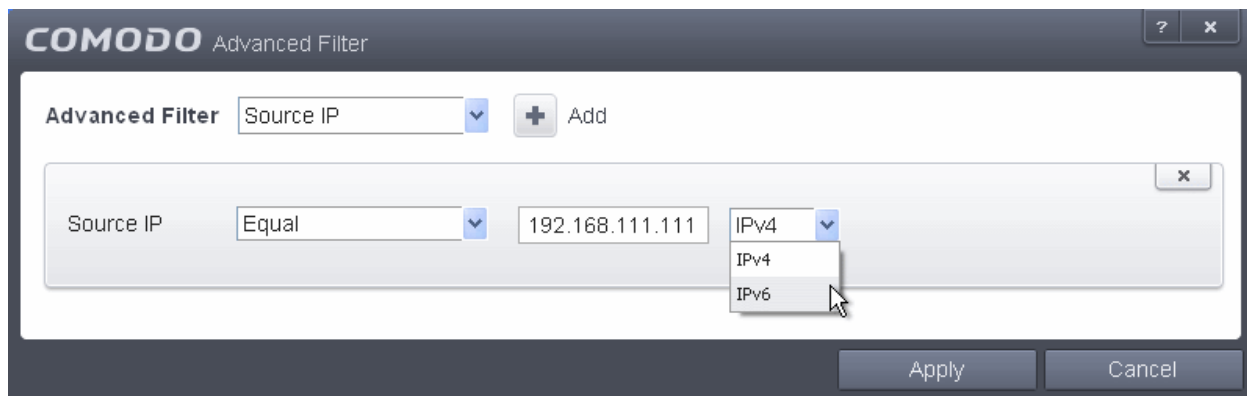
- vi. **Protocol:** Selecting the 'Protocol' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



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

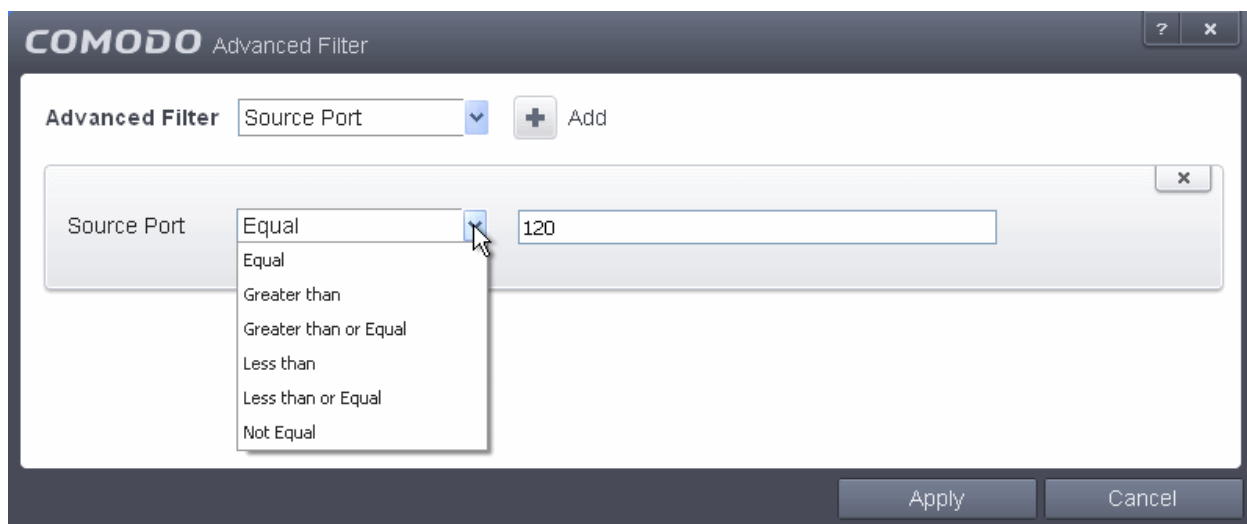
- IPV4
- IGMP
- GGP
- PUP
- IDP
- IPV6
- ICMPV6
- ND

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



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

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



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

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

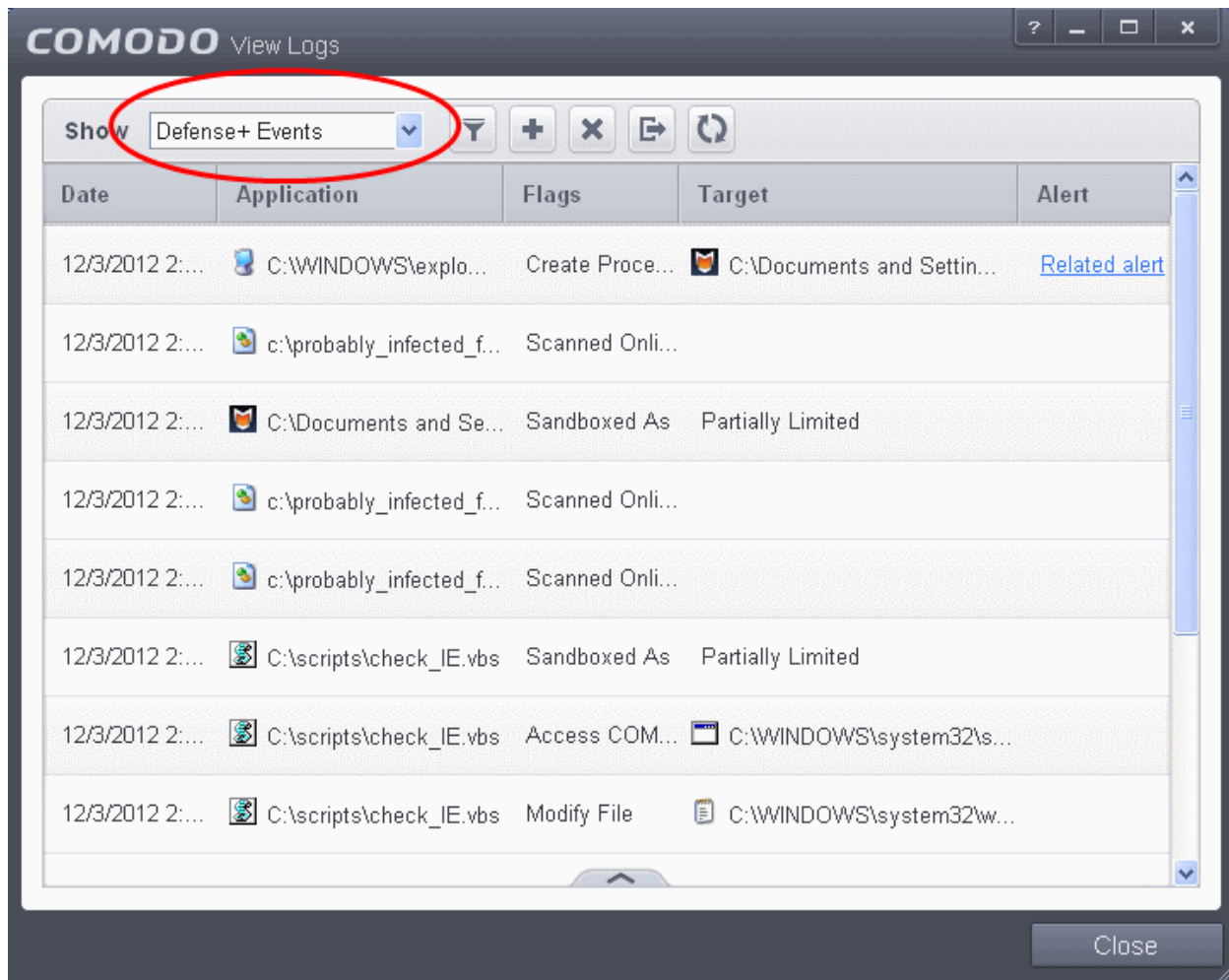
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.3. 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.



Column Descriptions

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

- To export the Defense+ logs as a HTML file click the 'Export' button .
- To open a stored CIS log file, click the 'Open' button .
- To refresh the Defense+ logs, click the 'Refresh' button .
- To clear the Defense+ logs click the 'Clear' button .

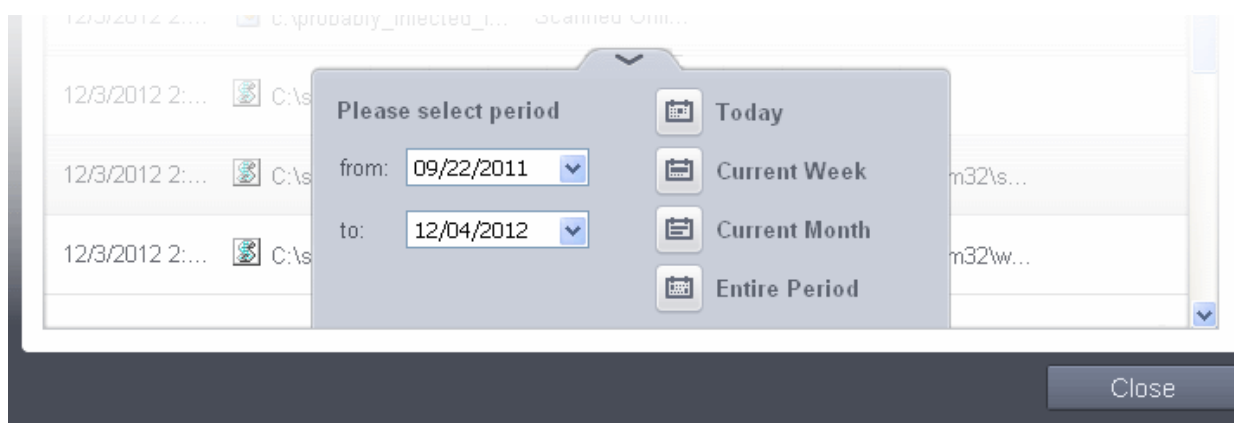
2.6.3.1. Filtering Defense+ Logs

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'

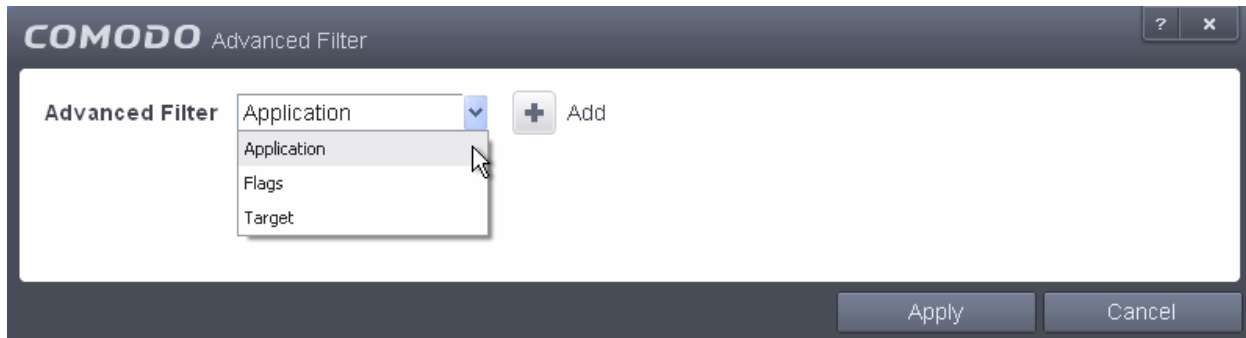
Advanced Filters

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

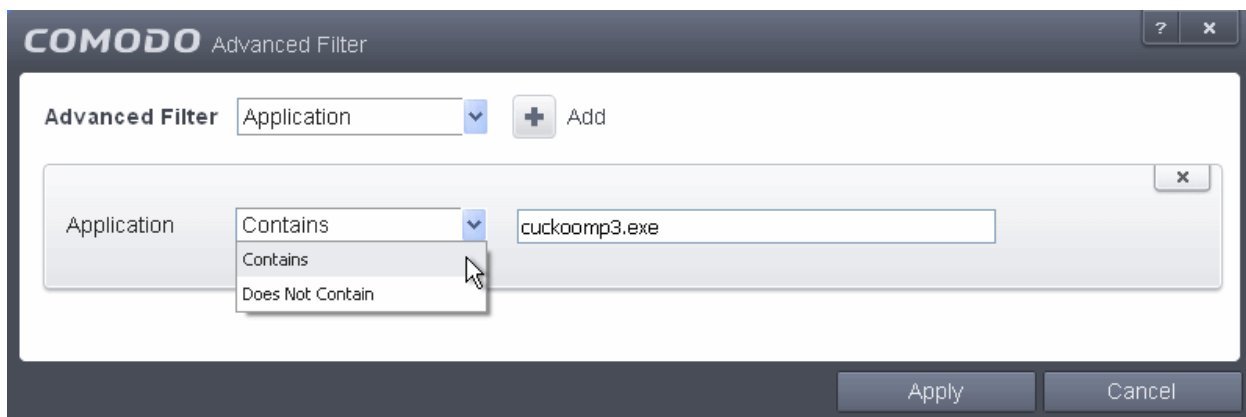
To configure Advanced Filters for Defense+ events

1. Click the funnel button  from the title bar. 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:

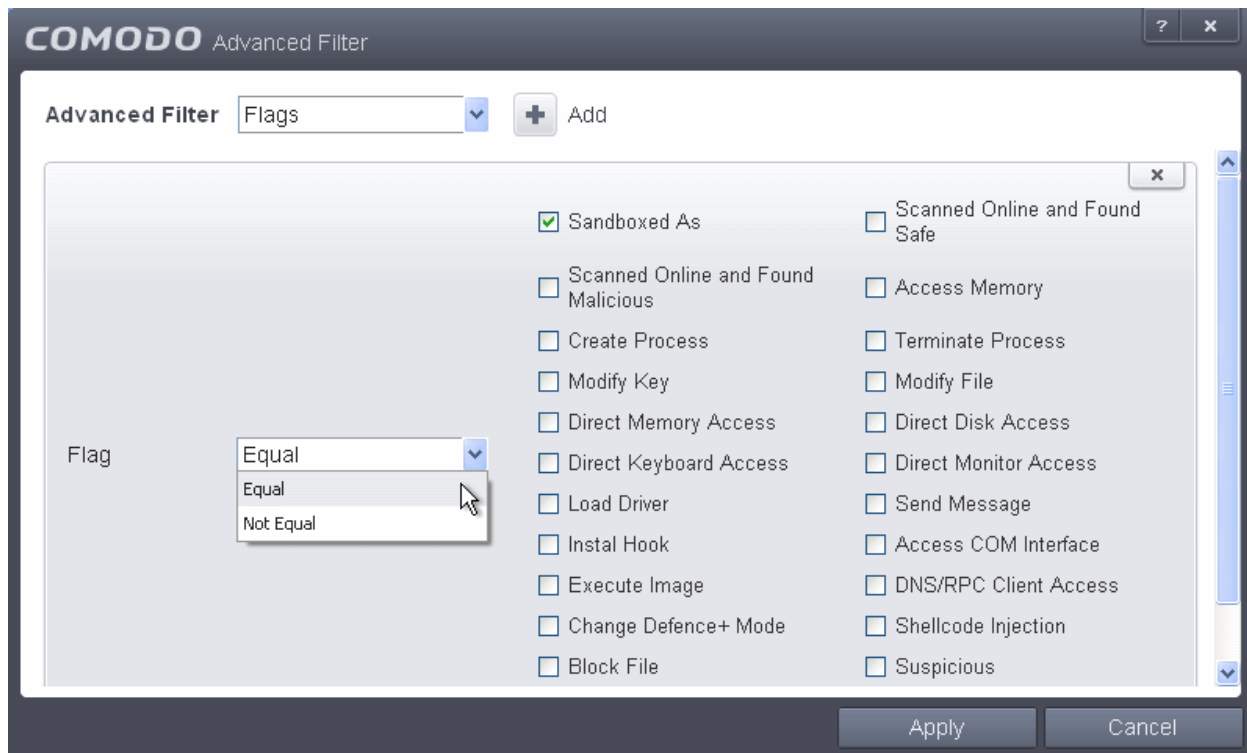
- i. **Application:** Selecting the 'Application' option displays a drop-down field and text entry field.



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

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

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

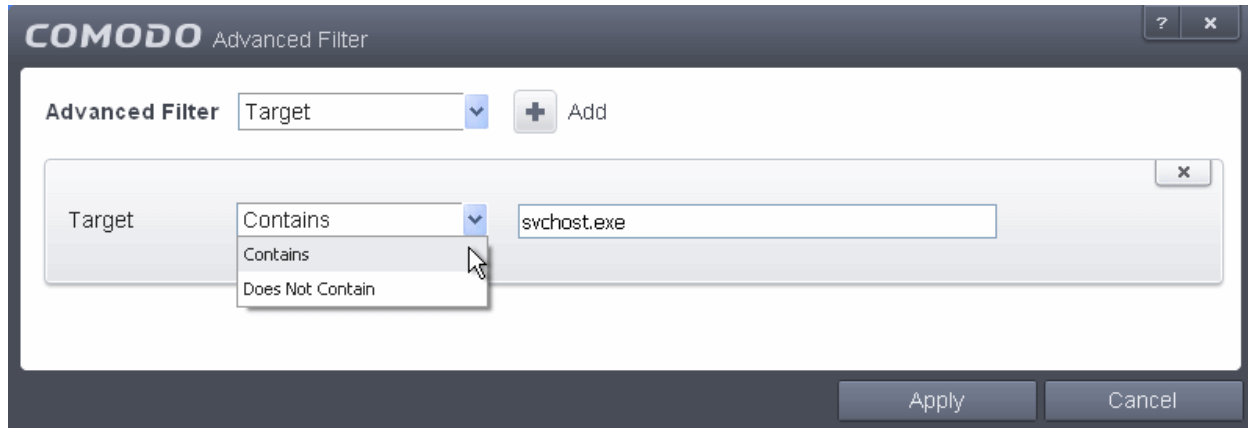


- c) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- d) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

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

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



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

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

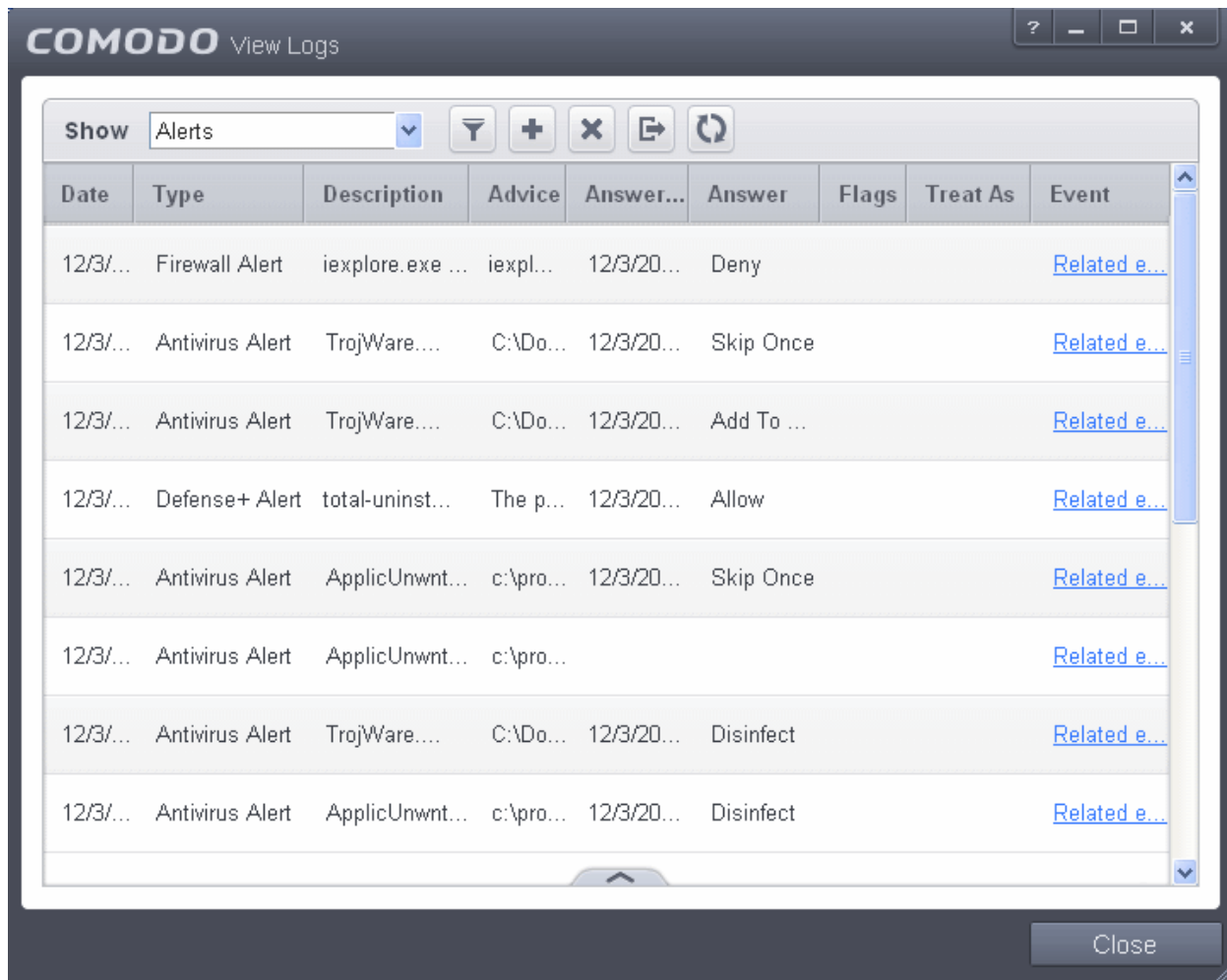
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.4. '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 .
- To open a stored CIS log file, click the 'Open' button .
- To refresh the Alerts logs, click the 'Refresh' button .
- To clear the Alerts logs click the 'Clear' button .

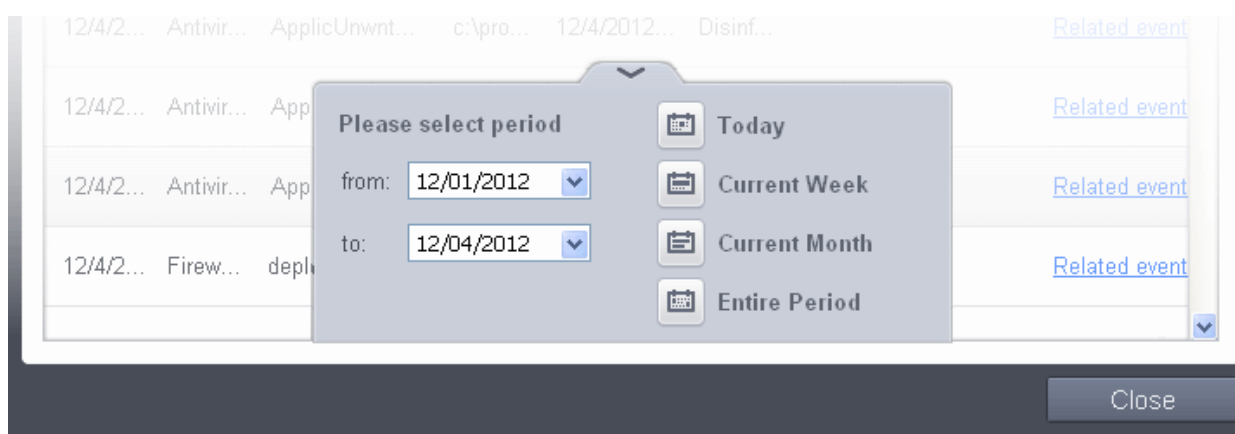
2.6.4.1. Filtering 'Alerts Displayed' Logs

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'

Advanced Filters

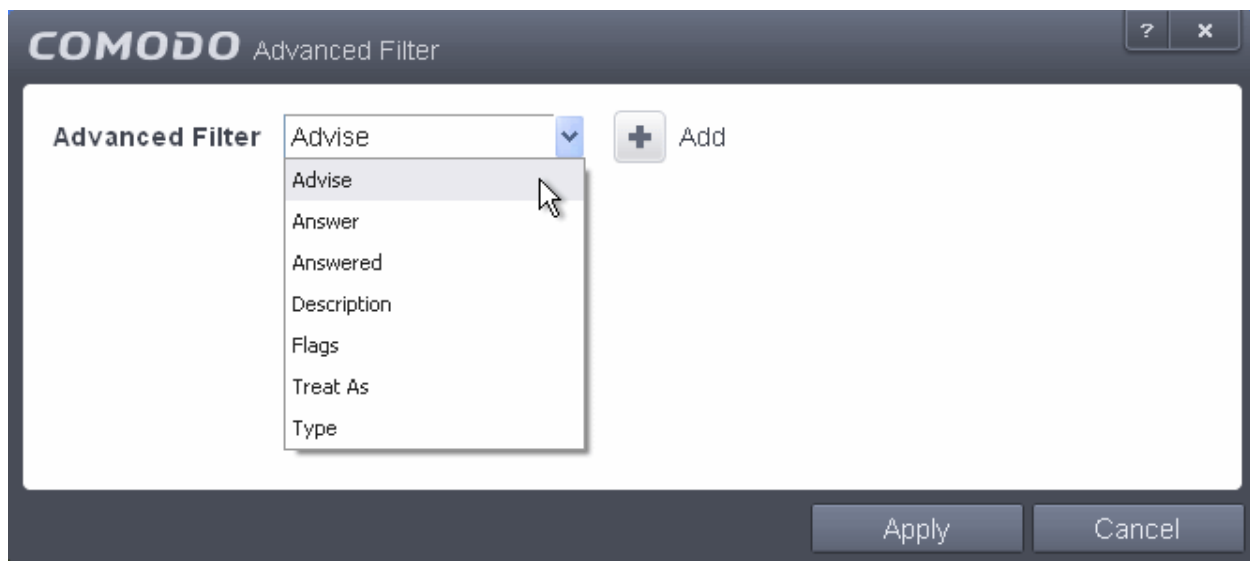
You can further refine the displayed events according to specific filters. Following are available filters for 'Alerts' logs and their meanings:

- **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. The Advanced Filter interface for 'Alerts' logs will open.

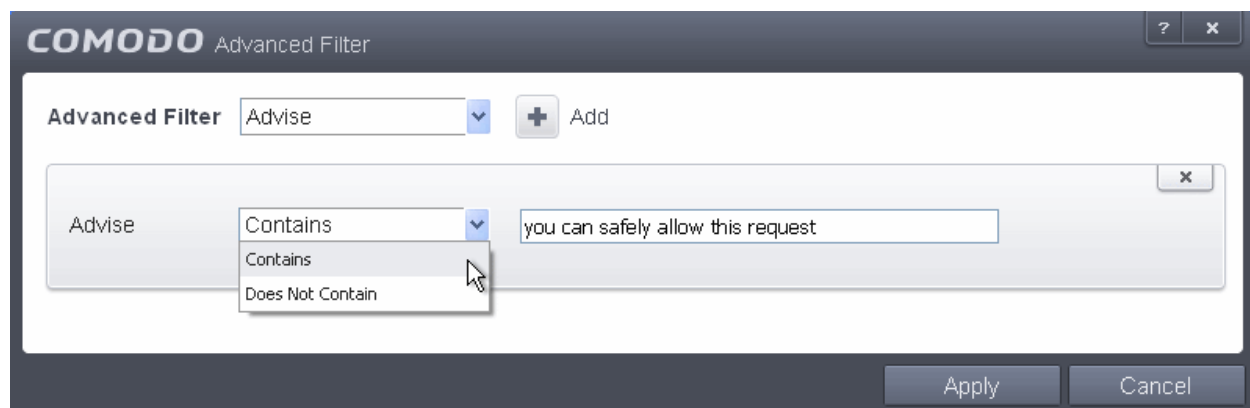
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

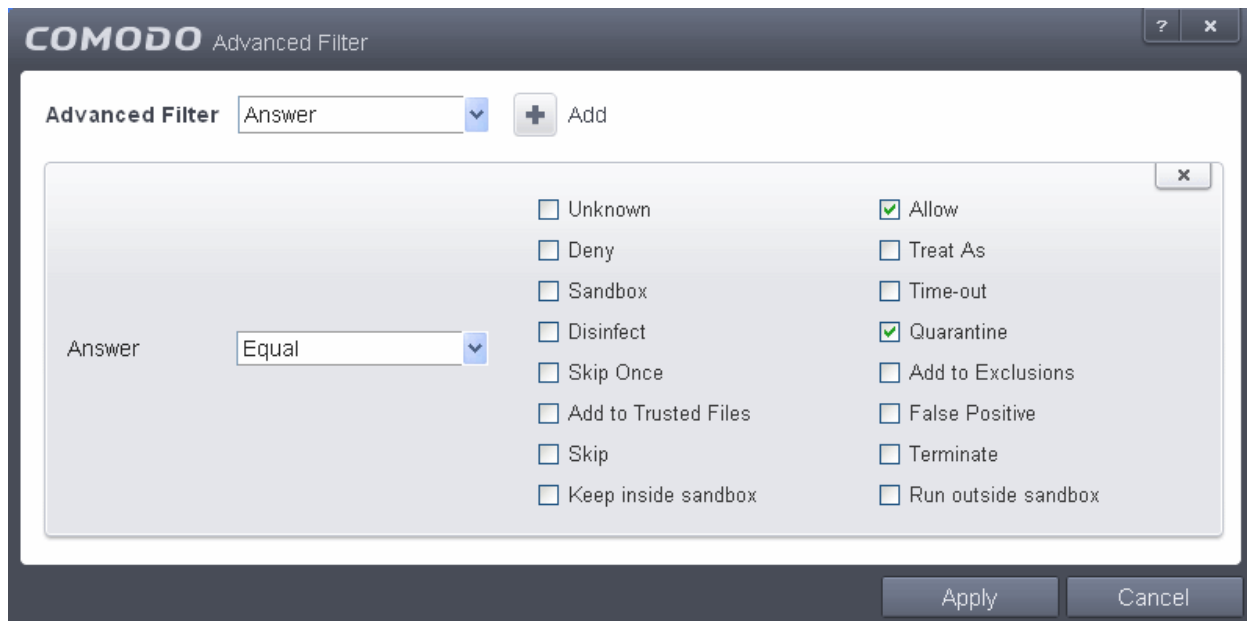
- i. **Advice:** The 'Advice' option enables you to filter the alerts based on advices given by CIS in the alert. Selecting the 'Advice' option displays a drop-down field and text entry field.



- 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 select 'Contains' option from the drop-down field 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 'Advice' 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.

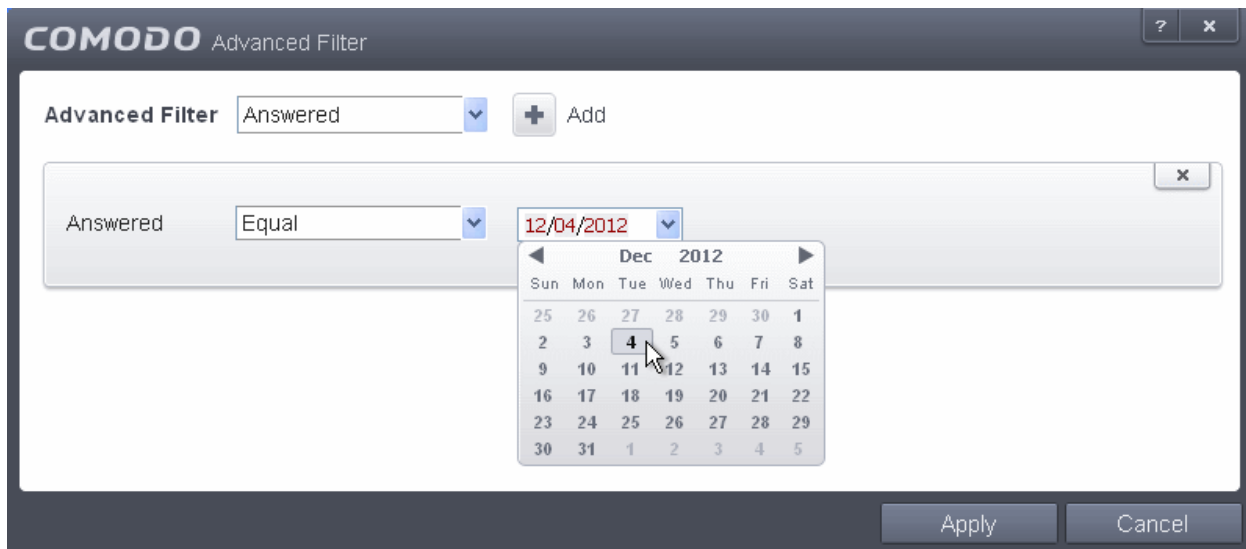


- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- 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 select 'Equal' from the drop-down and select 'Add to Exclusions' checkbox, only the log of Antivirus alerts for which you answered as 'Disregard' > 'Disregard and Exclude' 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 '12/04/2012' , only the log of alerts answered on 12/04/2012 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.

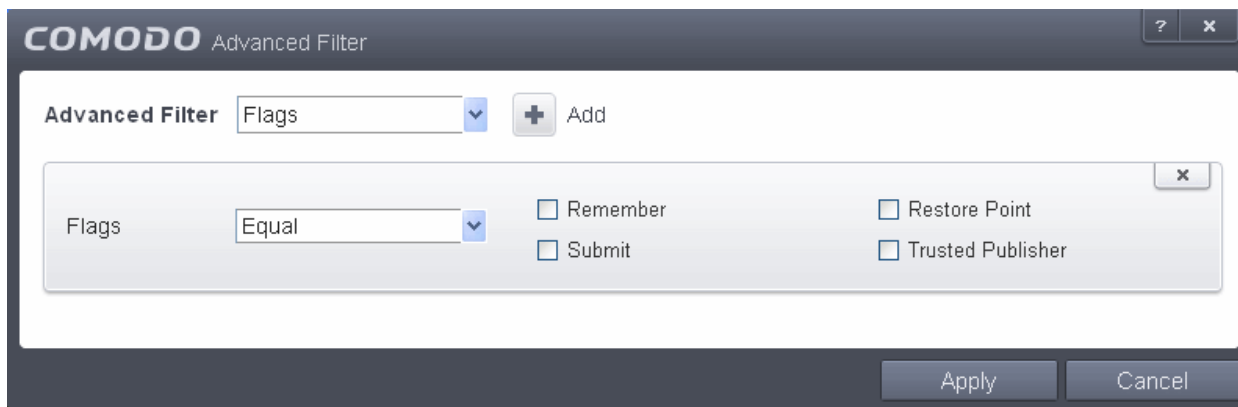


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

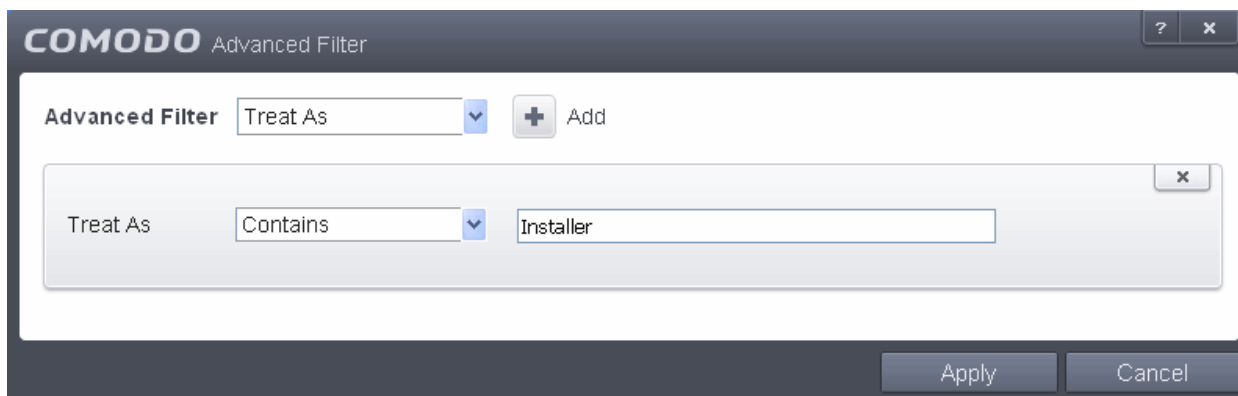
b) Enter the text or word as your filter criteria.

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.

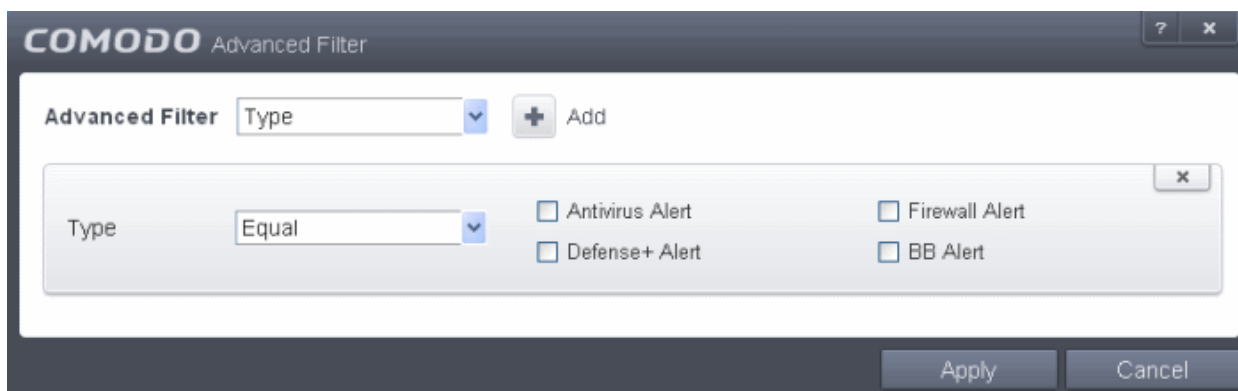
v. **Flags:** The 'Flags' option enables you filter the entries based on the flags set for the kinds of actions against the event triggered by the file. Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.



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



- a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
 - b) Enter the text or word as your filter criteria
- For example, if you have chosen 'Contains' from the drop-down and entered 'Installer' in the text field, only the entries containing the phrase 'Installer' in the 'Treat As' column will be displayed.
- vii. **Type:** The 'Type' option enables you to filter the entries based on the component of 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 Alerts' checkbox, only the log of Antivirus alerts will be displayed.

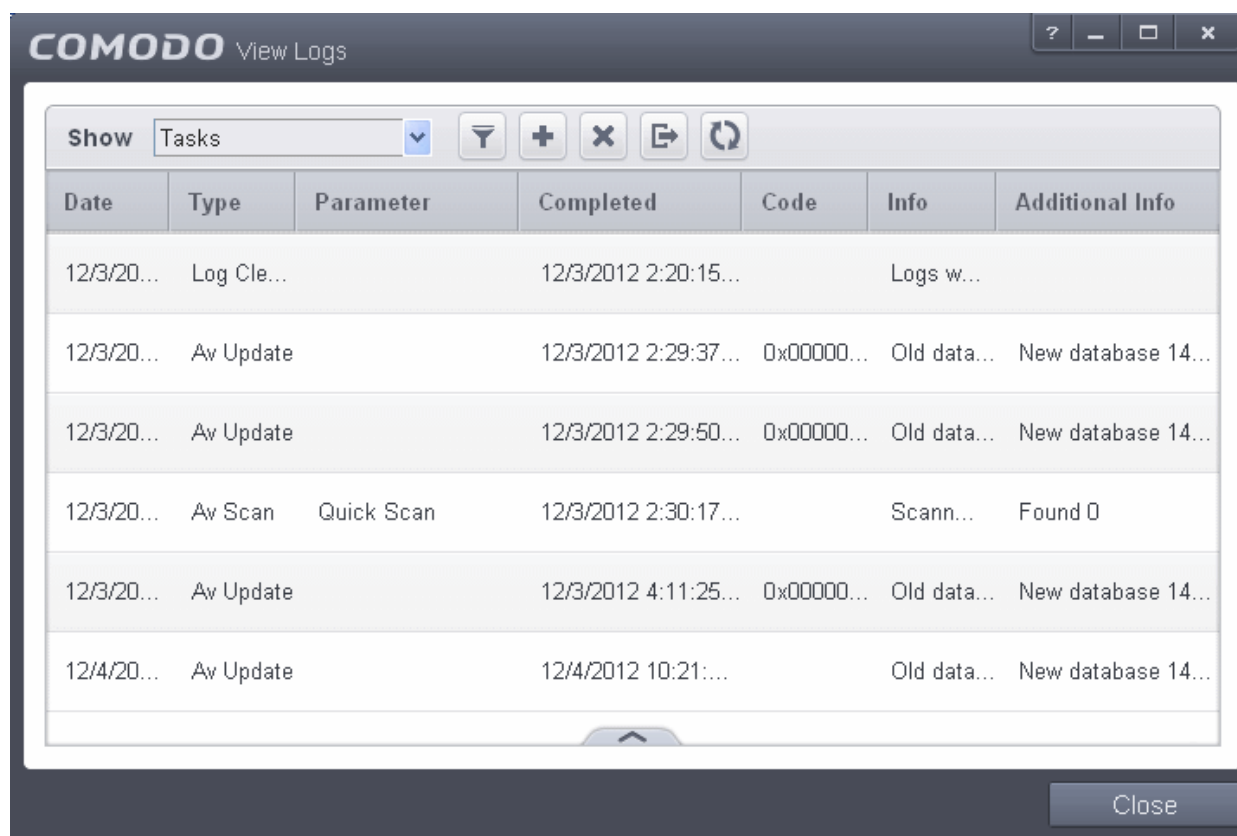
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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.

2.6.5. 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 .
- To open a stored CIS log file, click the 'Open' button .
- To refresh the Tasks logs, click the 'Refresh' button .
- To clear the Tasks logs click the 'Clear' button .

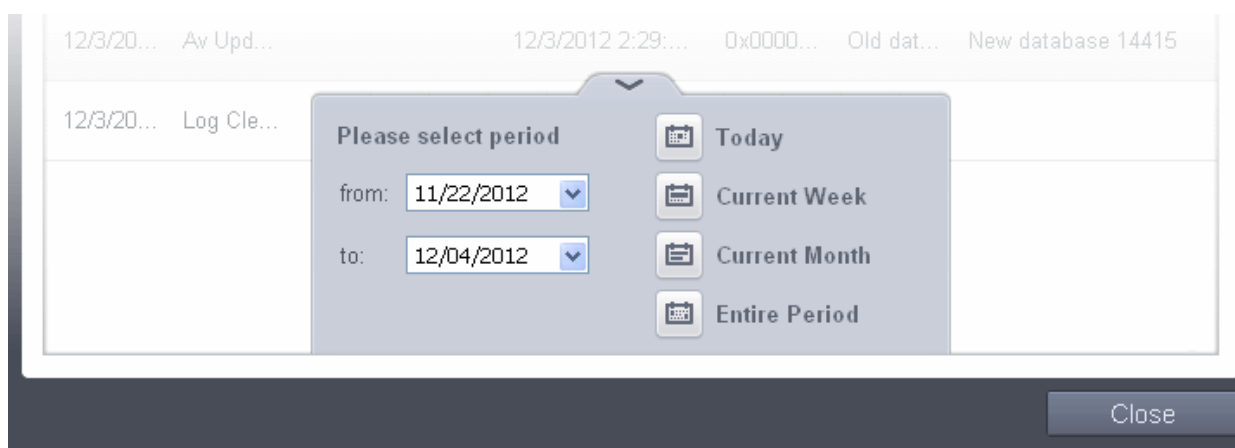
2.6.5.1. Filtering 'Tasks Launched' Logs

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'

Advanced Filters


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

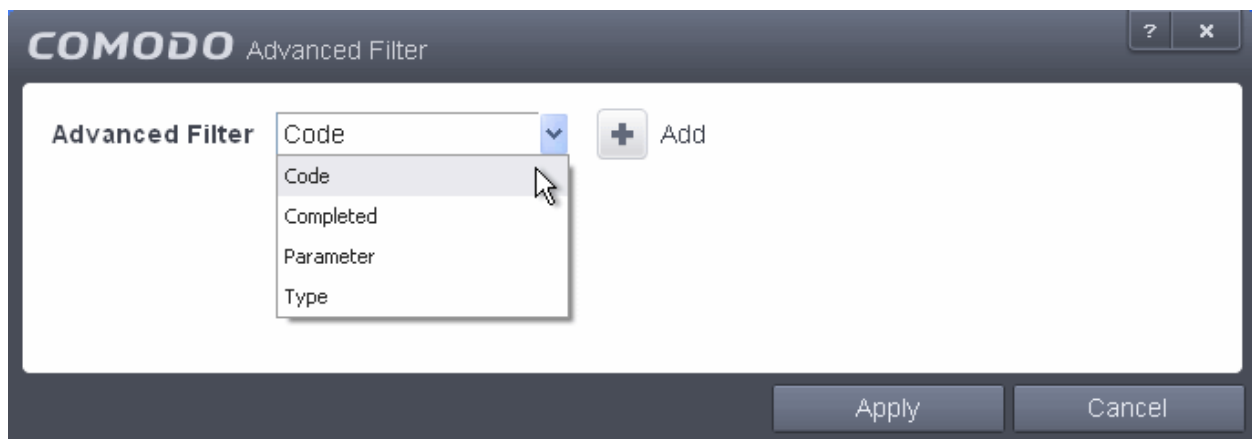
- **Code** - Displays the tasks based on the entered code value
- **Completed** - Displays the tasks completed on entered date.
- **Parameter** - Displays only the tasks launched that include the selected parameter, like scan profile or the locations

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

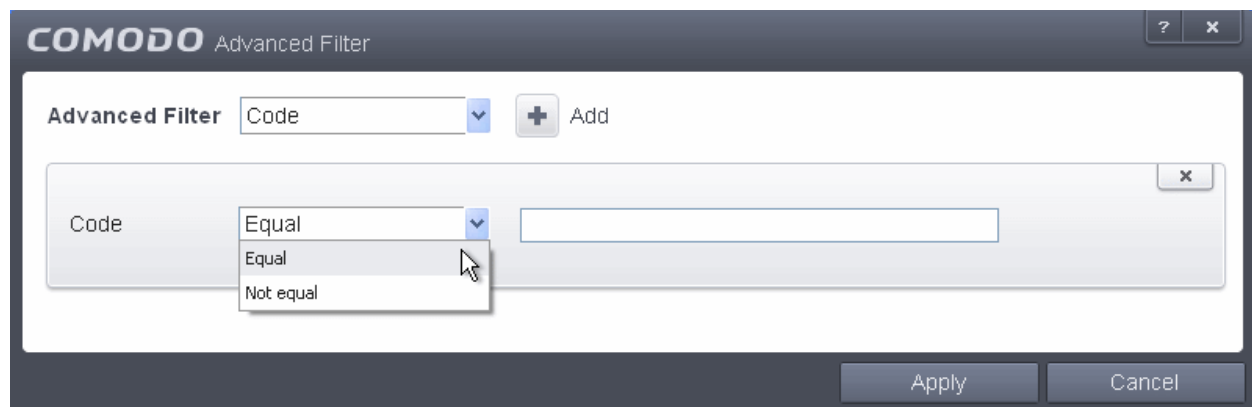
1. Click the funnel button  from the title bar. The Advanced Filter interface for Tasks log viewer will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



You can choose 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:

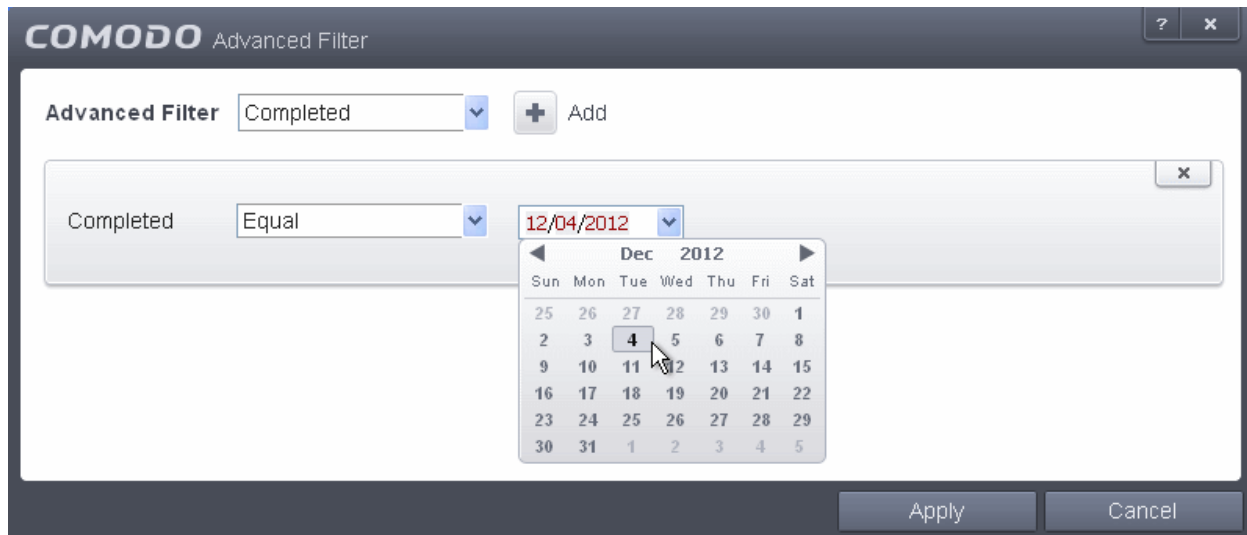
- Code:** The Code option enables you to filter the tasks based on their code value. Selecting the 'Code' option displays a drop-down field and text entry field.



- 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.

- 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.



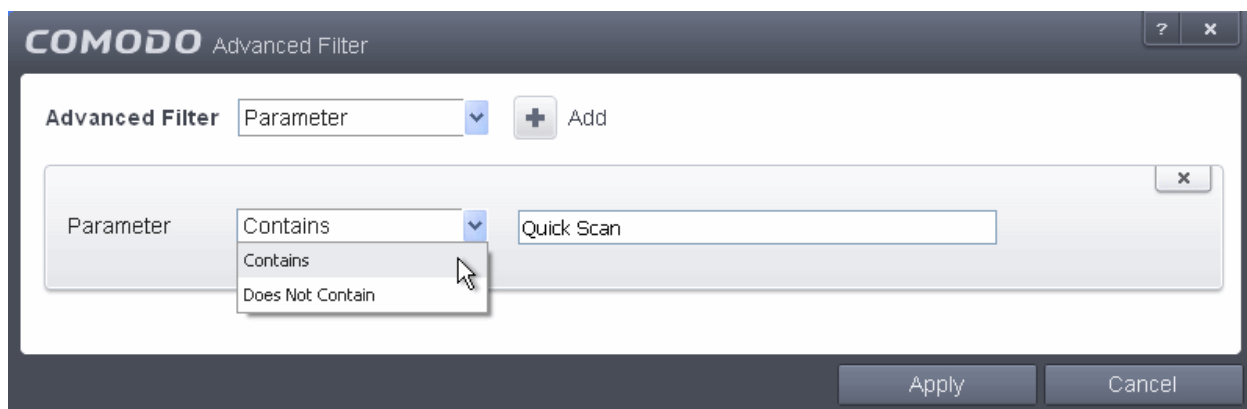
a) Select any one of the following option the drop-down box.

- 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 '12/04/2012' , only the log of Tasks completed on 12/04/2012 will be displayed.

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

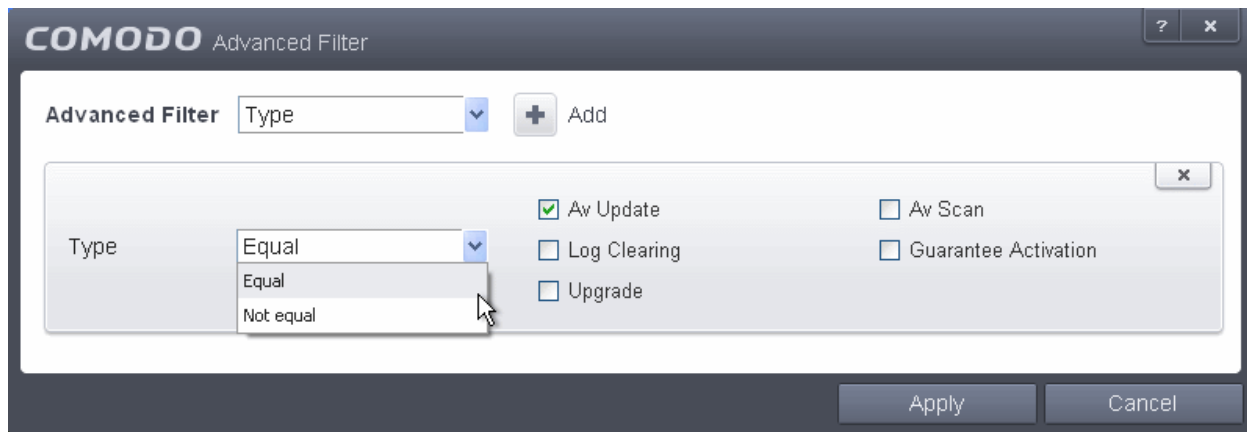


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

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



- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:
 - AV virus signature database update
 - AV Scan
 - Clearing Logs
 - Activation of guarantee
 - Version upgrade

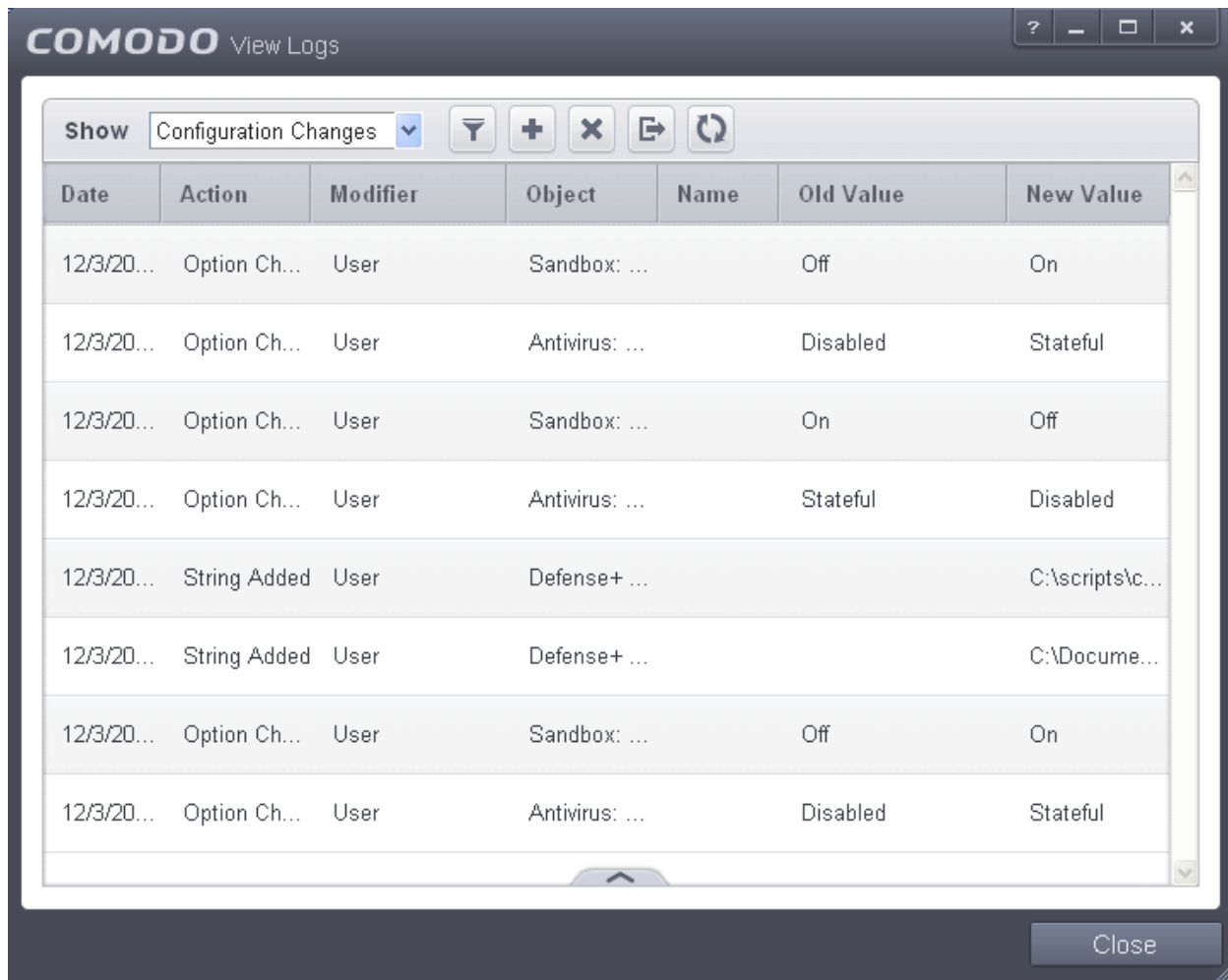
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6.6. 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 parameter changed.
6. **Old value** - Indicates the value of the parameter before the configuration change.
7. **New value** - Indicates the value of the parameter after the configuration change.

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

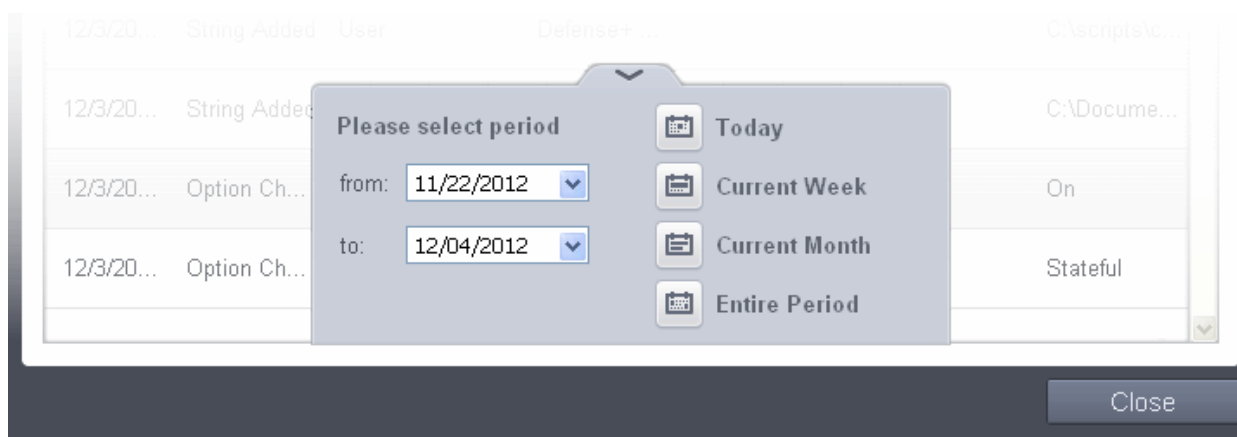
2.6.6.1. Filtering 'Configuration Changes' Logs

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'

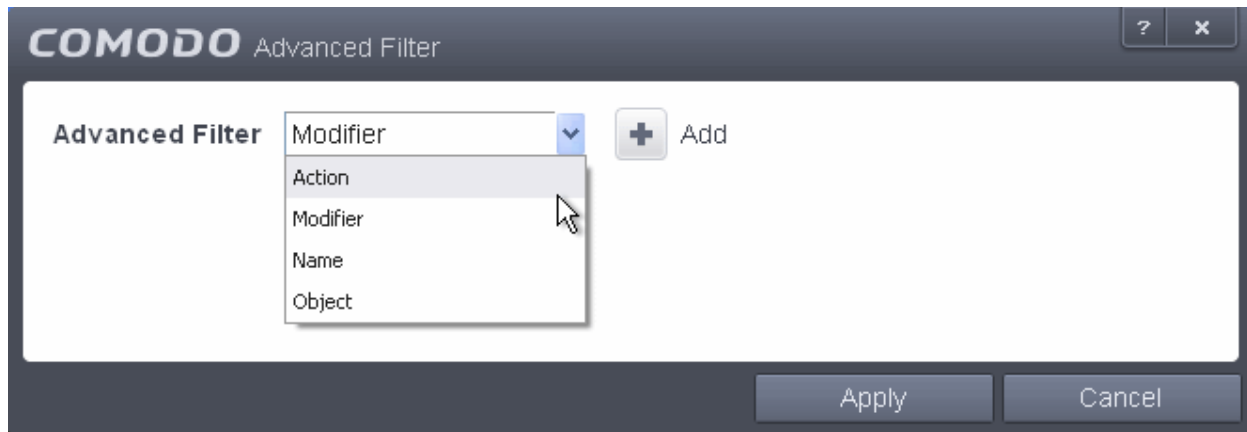
Advanced Filters

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

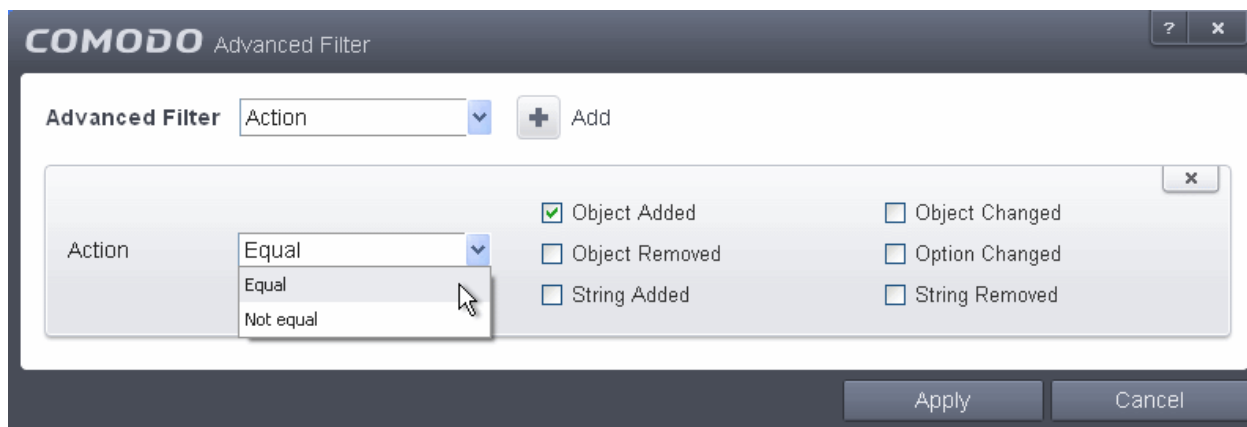
To configure Advanced Filters for Configuration Changes Logs

1. Click the funnel button  from the title bar. 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 choose 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:

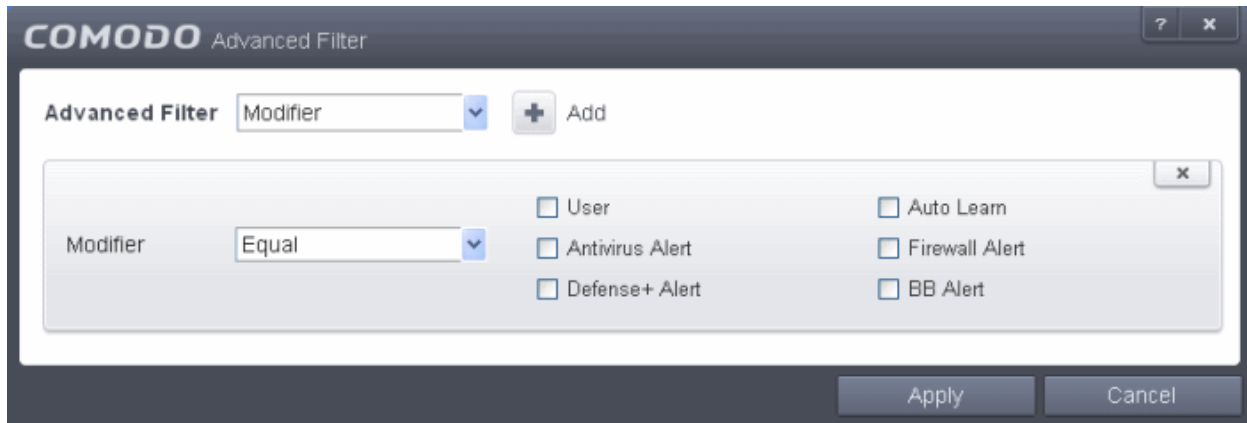
- i. **Action:** The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



- 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
 - String Added
 - String Removed

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

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

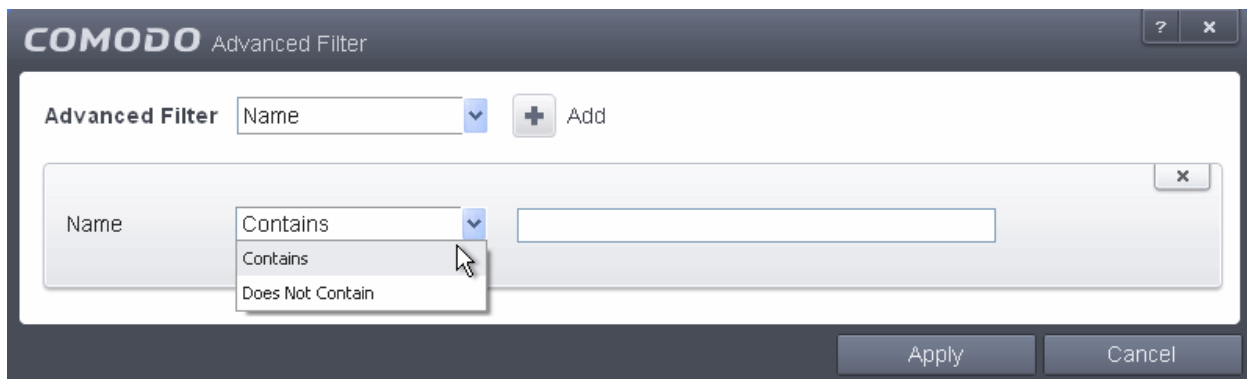


- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:

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

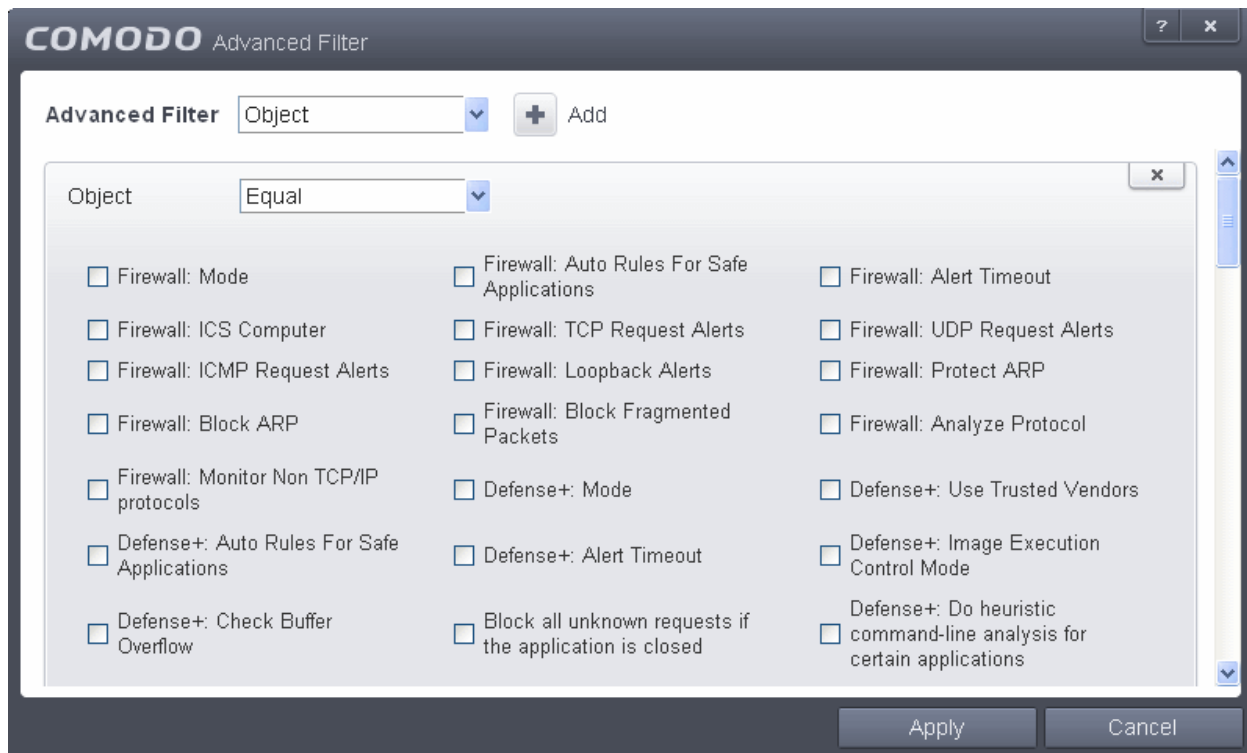
For example, if you have selected Equal in the drop-down and selected 'Antivirus Alert' checkbox, then, only the log entries related to the configuration changes effected by responses to Antivirus Alerts will be displayed.

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



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

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



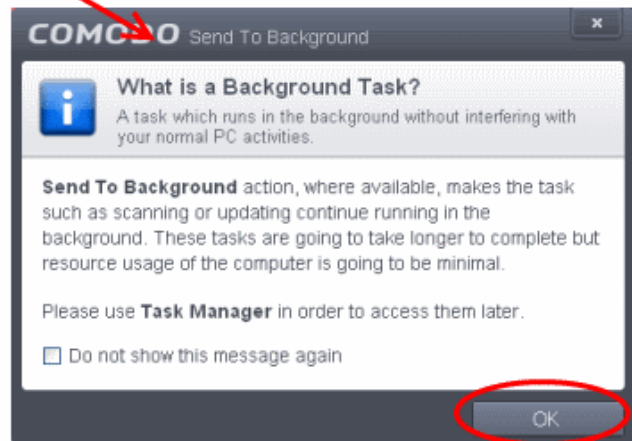
- a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
- b) Now select the check-boxes of the specific objects as filter parameters to refine your search. Scroll the window to the right to see all the parameters options.

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

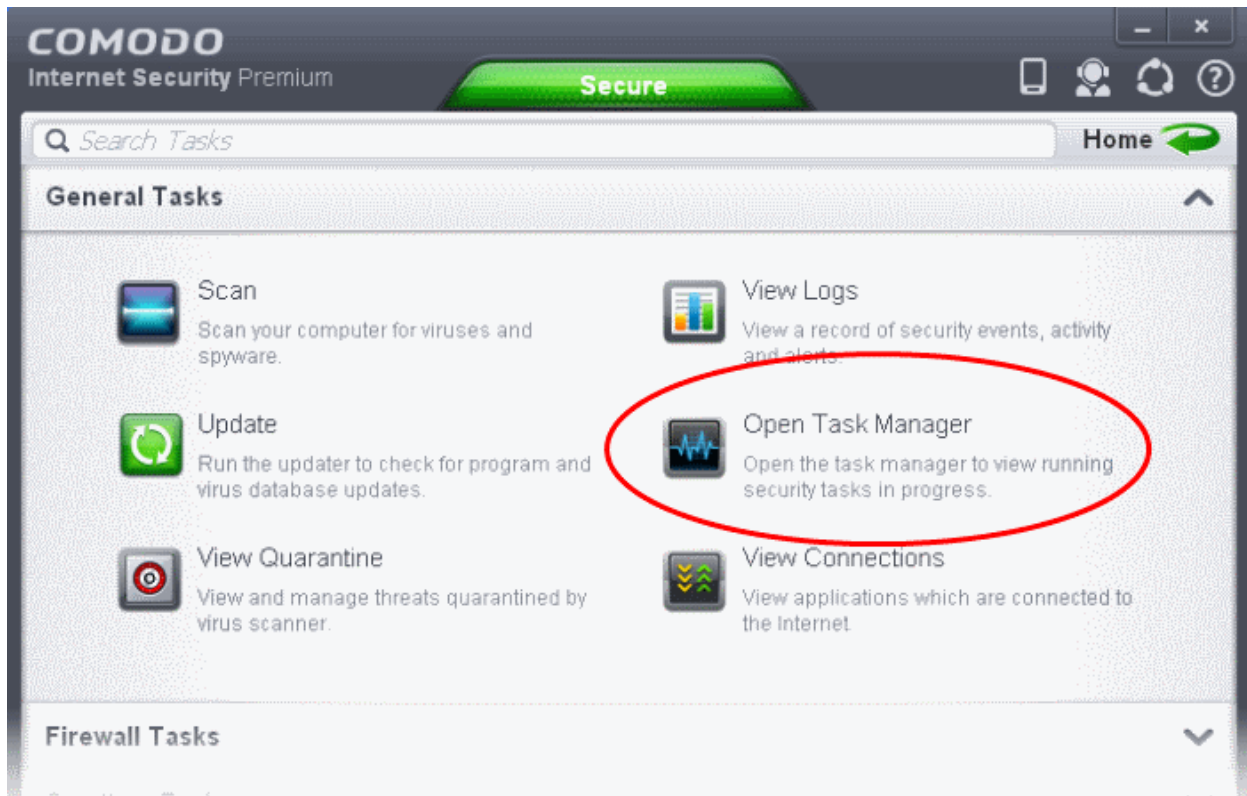
- Click 'Apply' for the filters to be applied to the Configuration Changes log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.

2.7. 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.

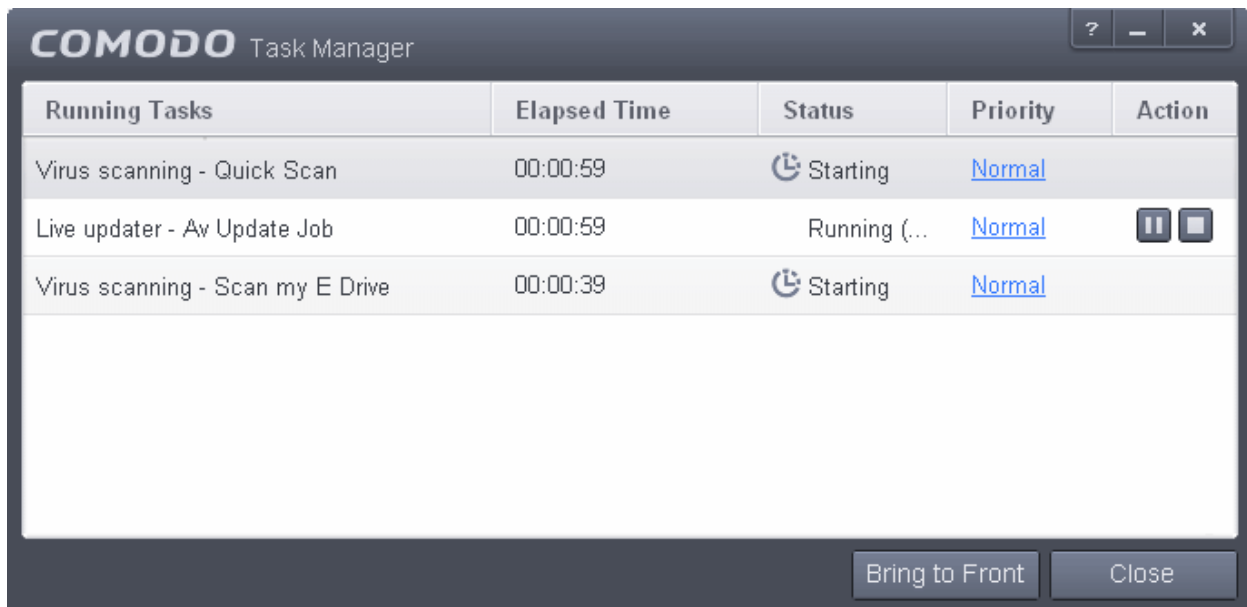


These tasks can be managed, through the Task manager interface that can be accessed at anytime by clicking Open Task Manager from the General Tasks interface.



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:

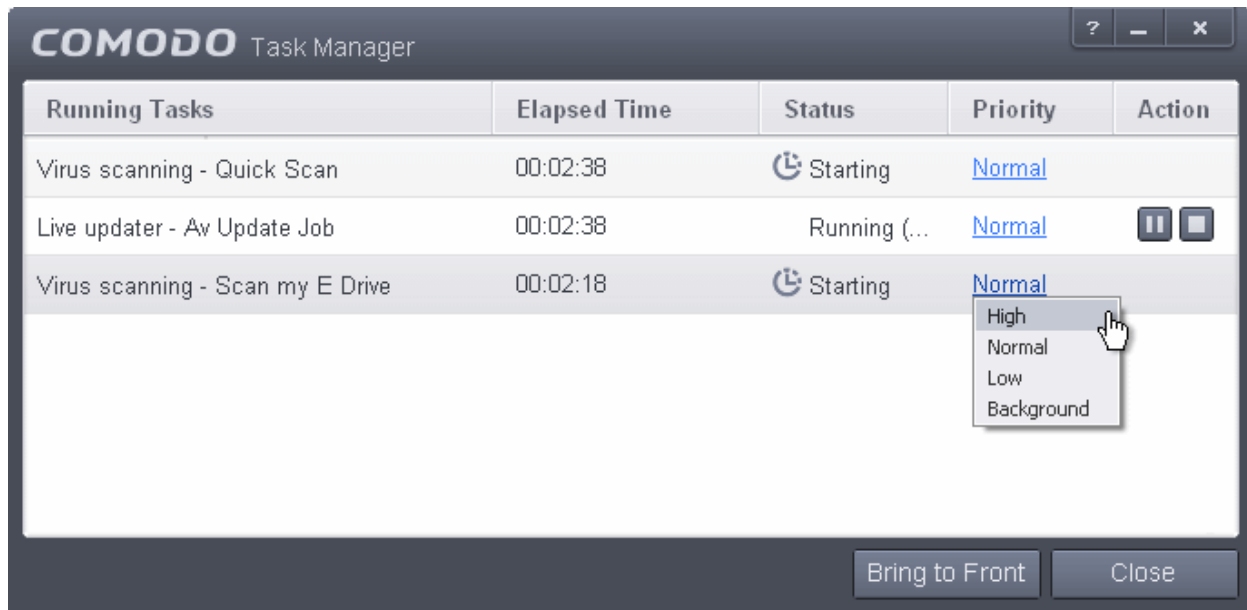
- **Reassign priorities to the tasks**
- **Pause/Resume or Stop a running task**
- **Bring a selected task to foreground**

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

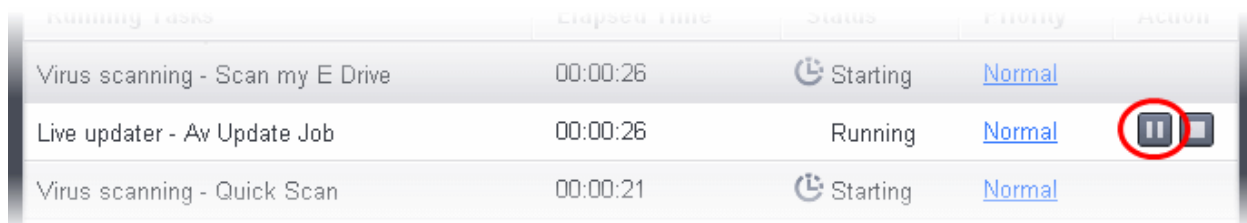
- Click on the current priority and select the priority you want to assign from the options.



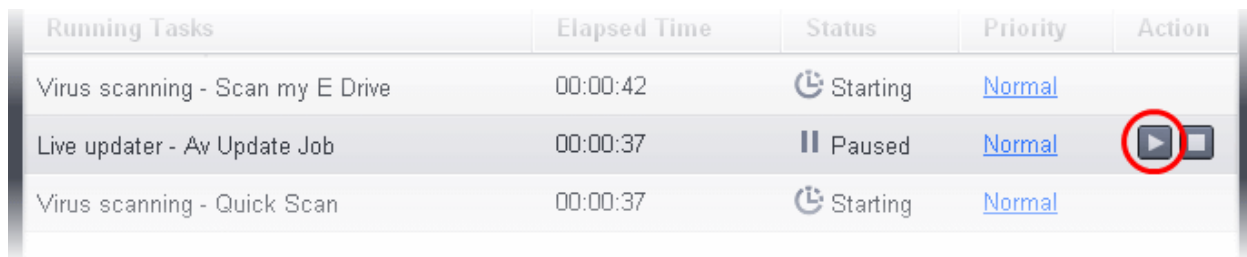
Pausing/Resuming or Stopping running tasks

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

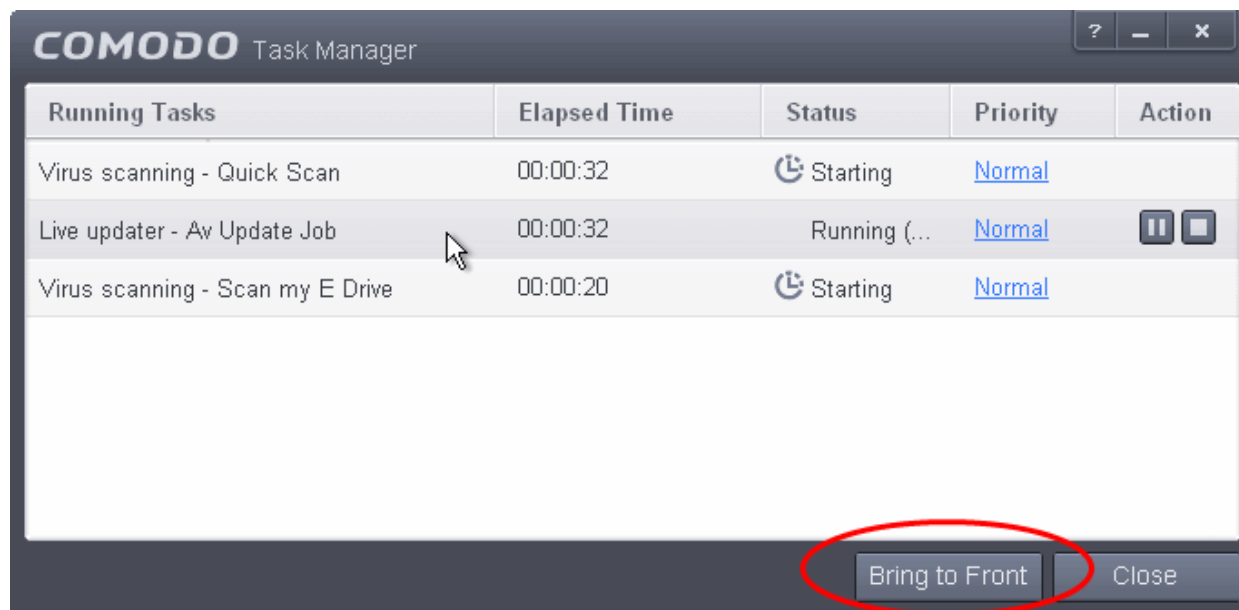


- To stop a running task, click the stop button

Virus scanning - Scan my E Drive	00:00:56	Starting	Normal	
Live updater - Av Update Job	00:00:39	Running (...)	Normal	
Virus scanning - Quick Scan	00:00:52	Starting	Normal	

Bringing a running task to foreground

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



The progress window of the task will be displayed. If the task is completed, the results window will be displayed.

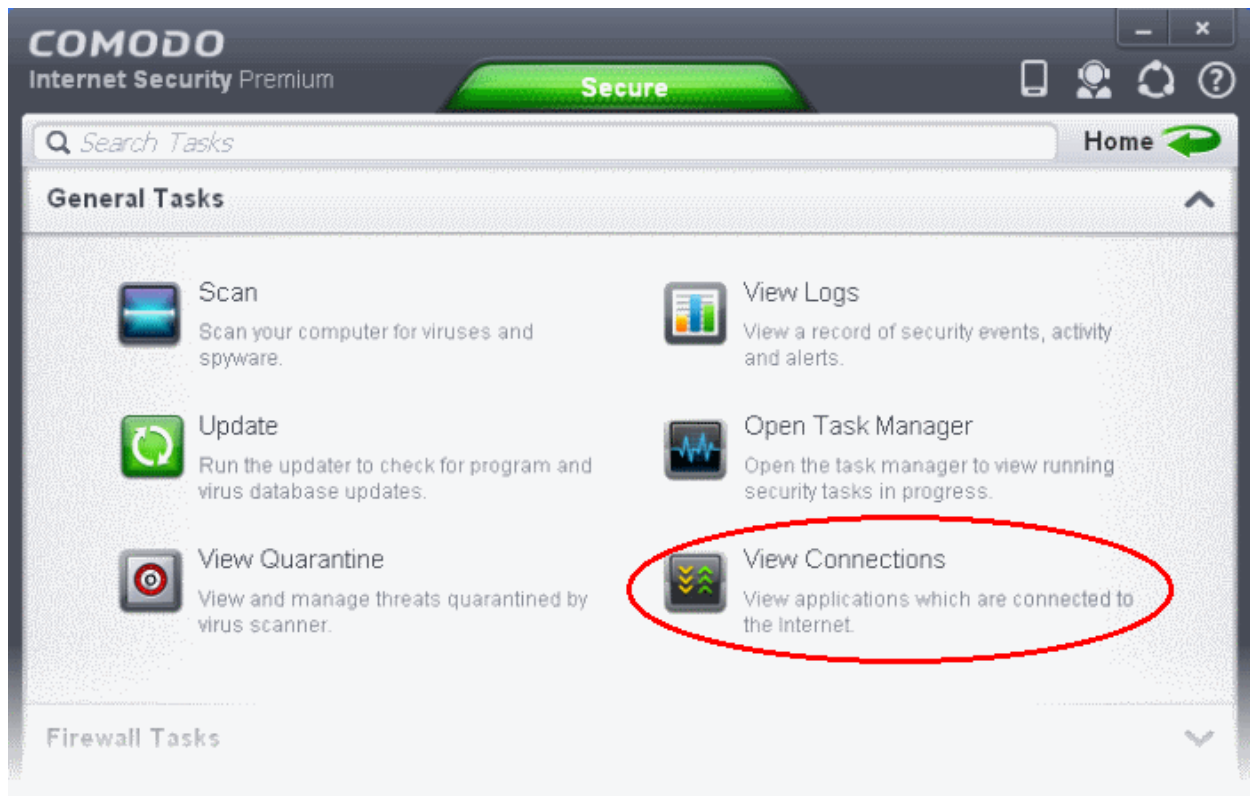


2.8. View Active Internet Connections

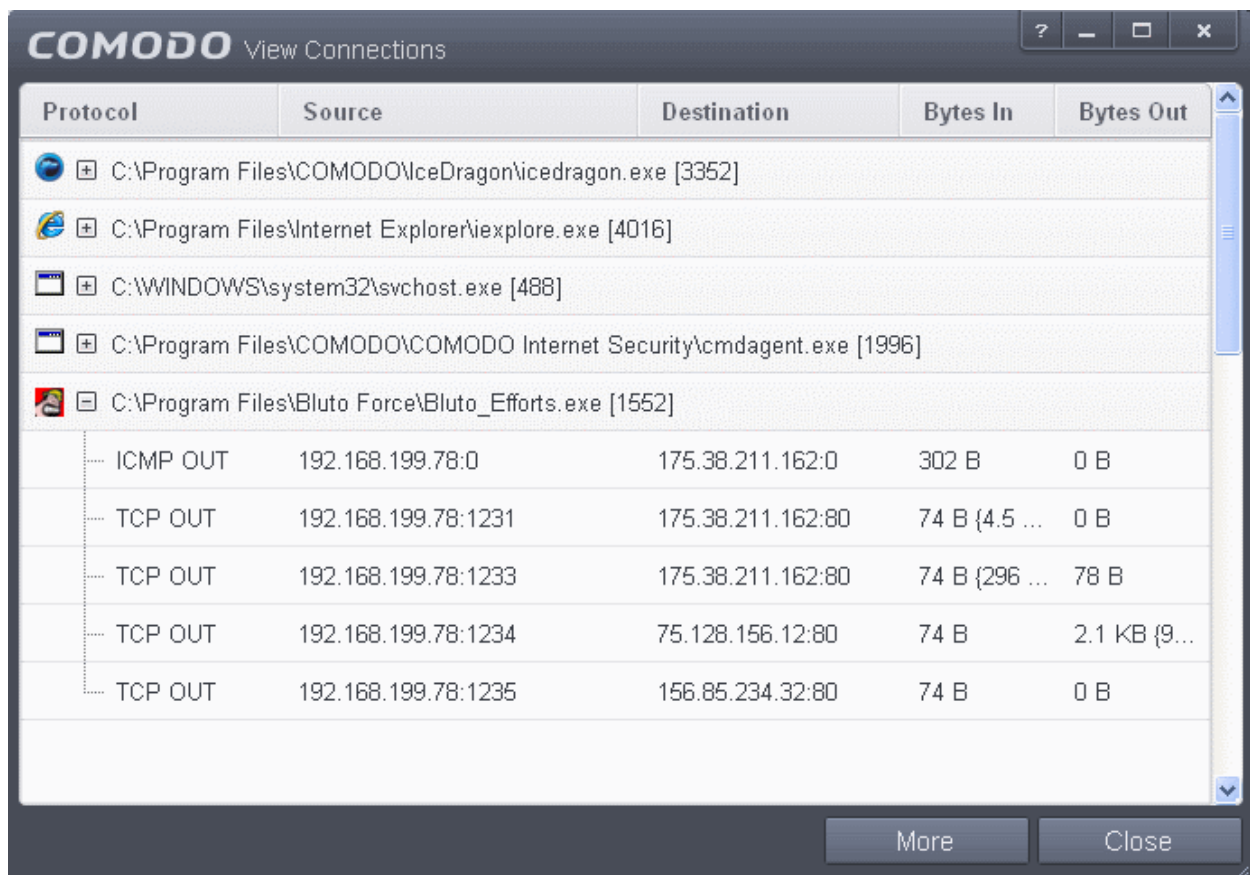
The 'View Connections' interface displays an at-a-glance summary of all currently active Internet connections on a per-application basis. You can view all the applications that are connected; all the individual connections that each application is responsible for; the direction of the traffic; the source 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.



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



Column Descriptions

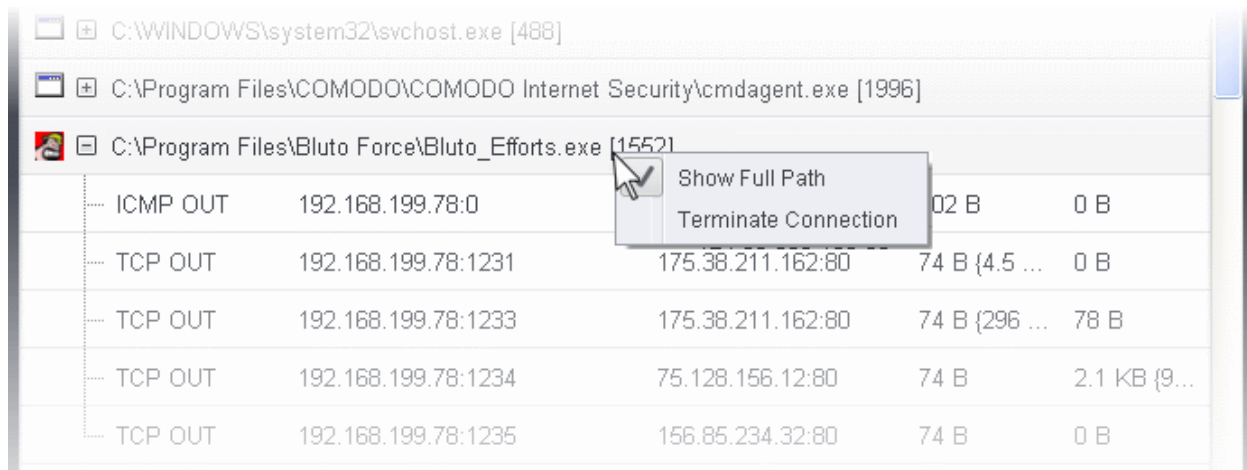
- **Protocol** - Shows the application that is making the connection, the protocol it is using and the direction of the traffic.

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.



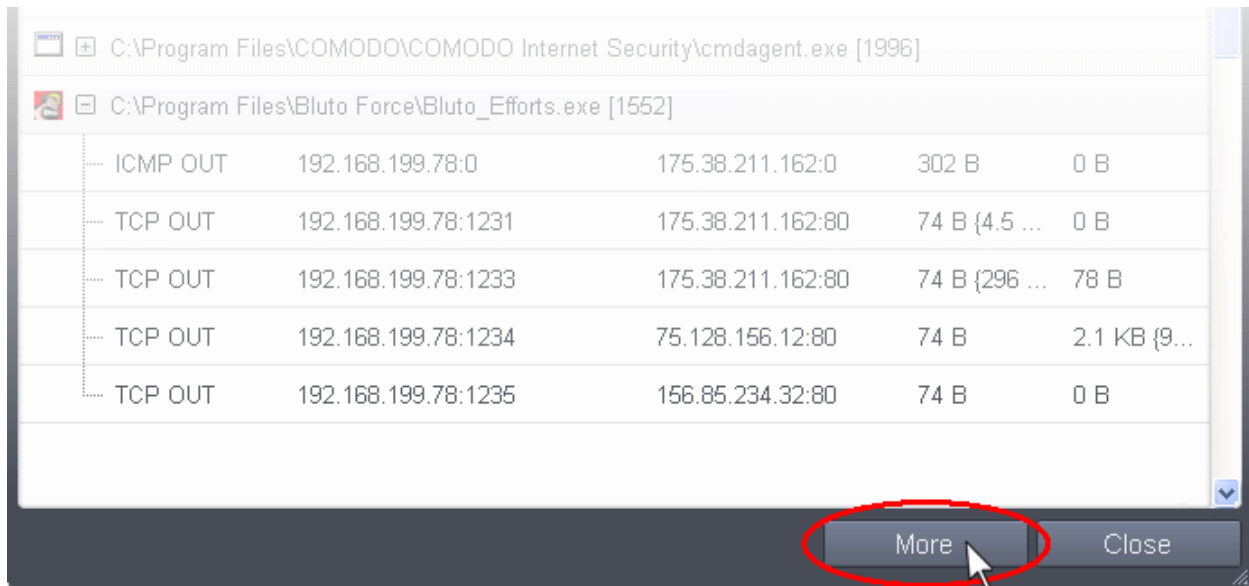
- If you wish to view the full path of the application, right click on the application name and select 'Show Full Path'.
- If you wish to terminate a connection belonging to an application, right click on the specific connection and click 'Terminate Connection'.

Identify and Kill Unsafe Network Connections

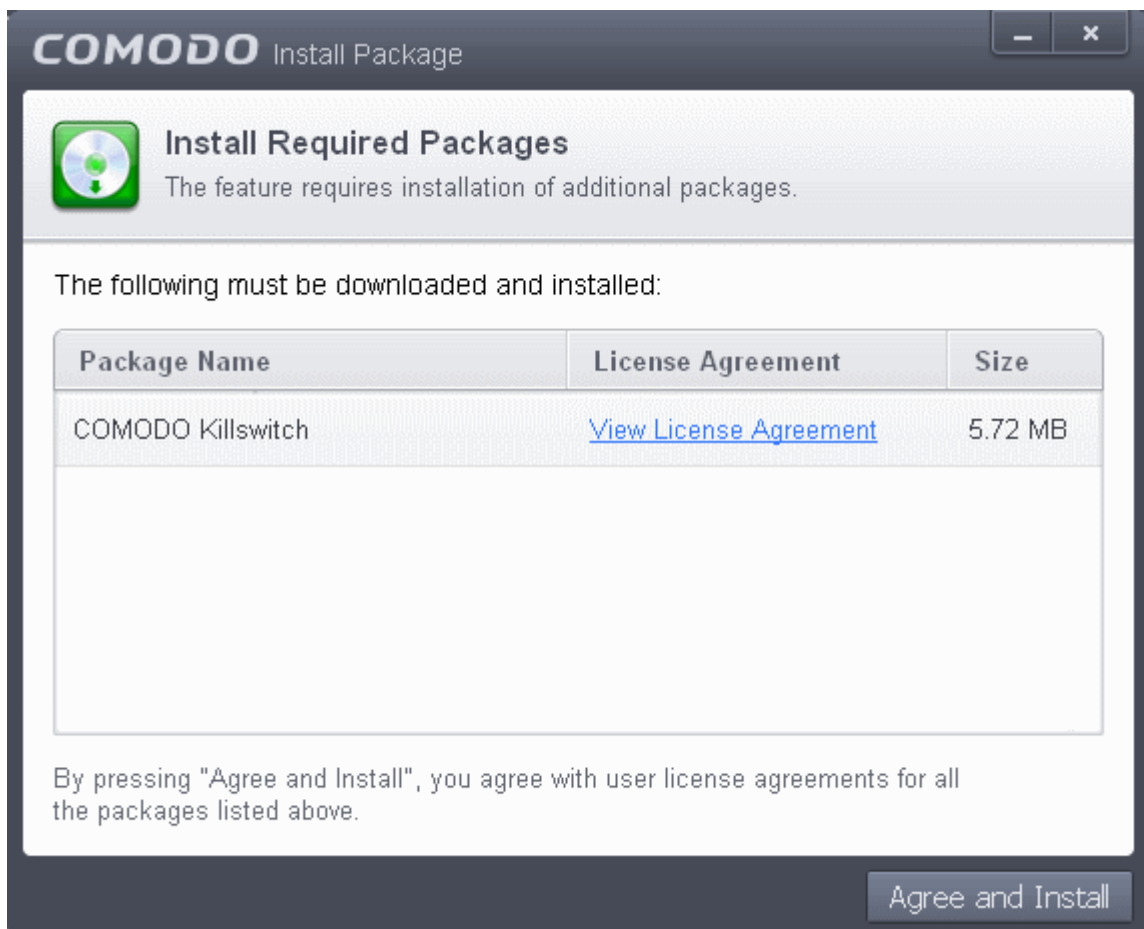
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes and network connections that are running on their system. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides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

Comodo KillSwitch can show ALL running processes with their granular details— exposing even those that were invisible or very deeply hidden. It allows you to identify which of those running processes are unsafe and 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 'View Connections' by clicking the 'More' button.



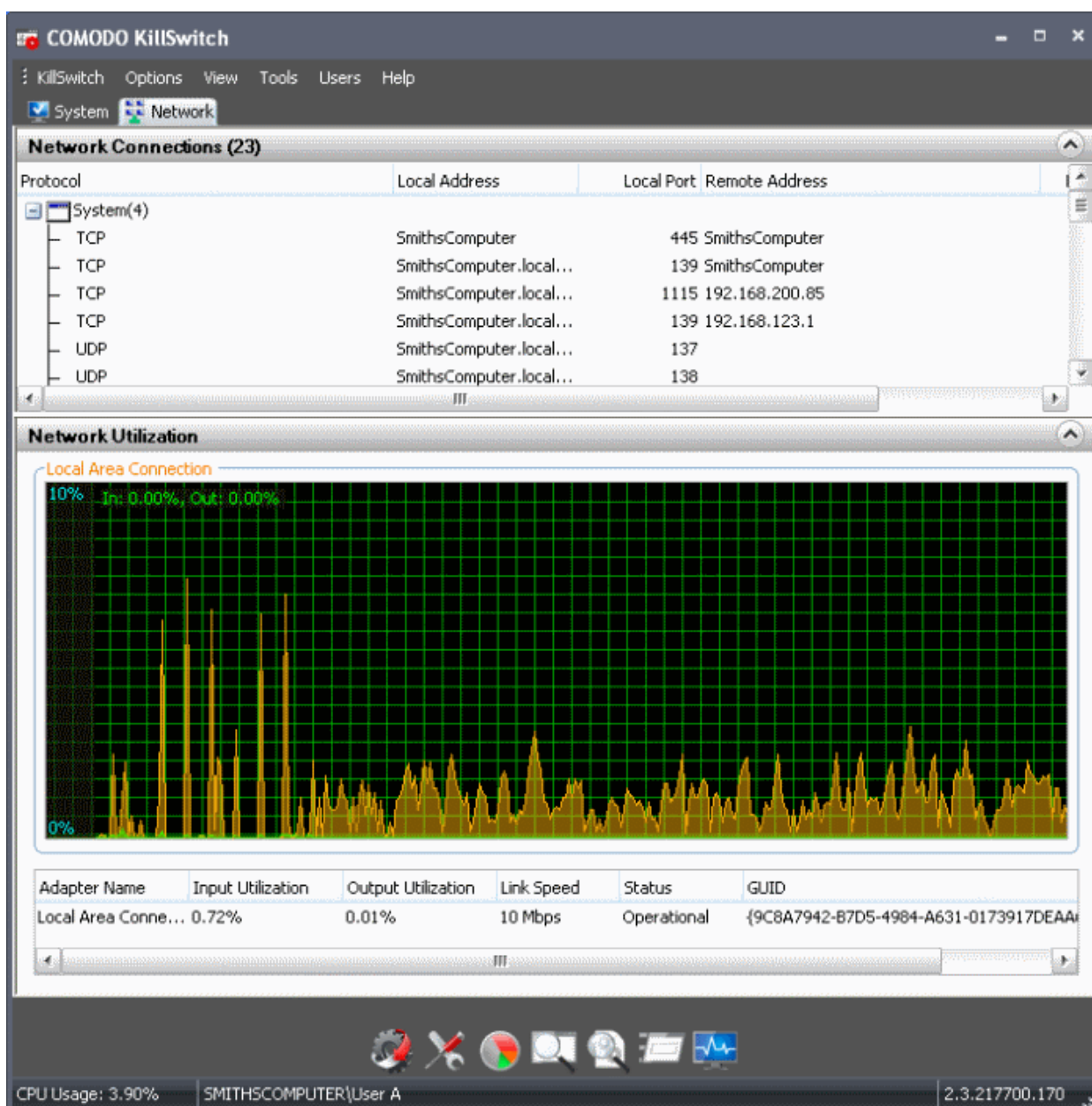
If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



- 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 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>

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:

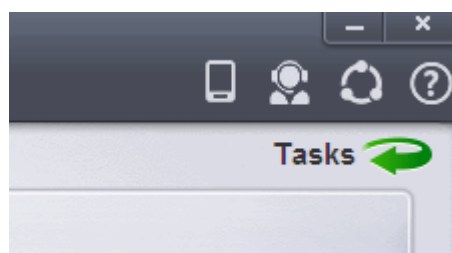
- [Allow or block Internet access to applications selectively](#)
- [Stealth your computer ports](#)
- [Manage network connections](#)
- [Stop all network activity](#)
- [Advanced firewall settings](#)

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.

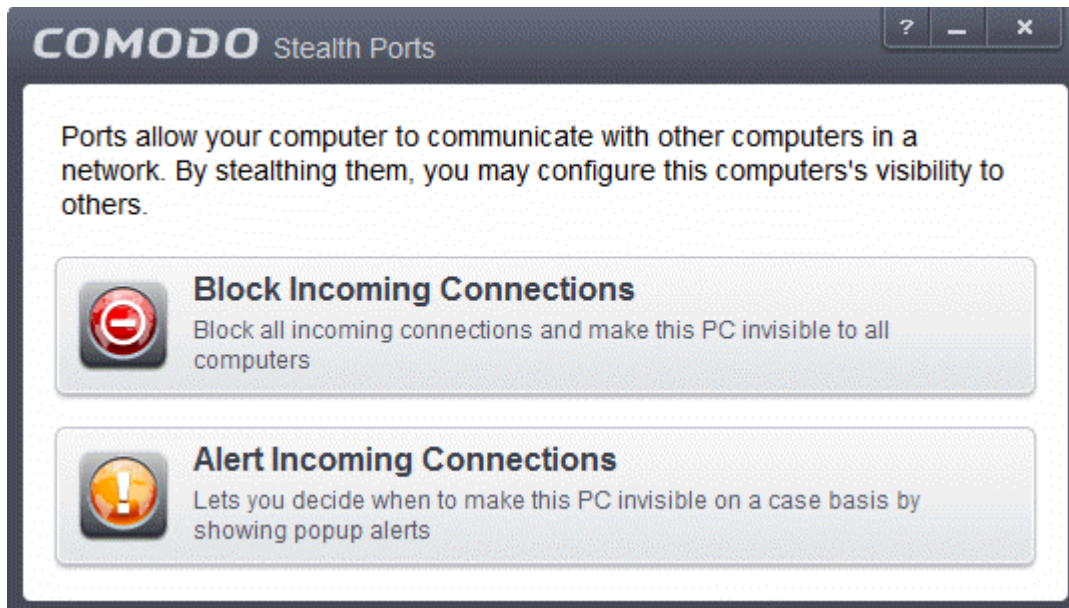
Stealthling a port effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempts ('closed' ports respond with a 'closed' reply- revealing to the hacker that there is actually a PC in existence.) This provides an extremely high 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.

Comodo Firewall provides a user with flexible stealthing options.



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 | In | From Any IP Address | To Any IP Address | Where Protocol is Any

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

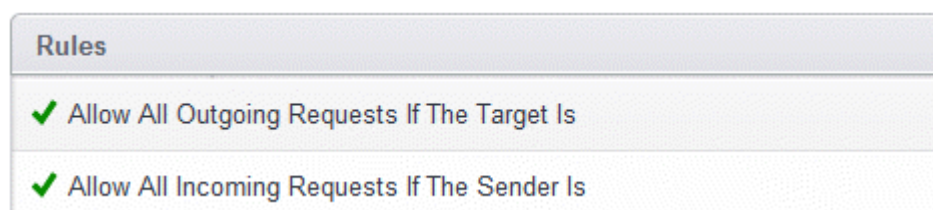
If you would like more information on the meaning and construction of rules, please [click here](#).

Alert incoming connections

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

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

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



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

3.3. Manage Network Connections

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

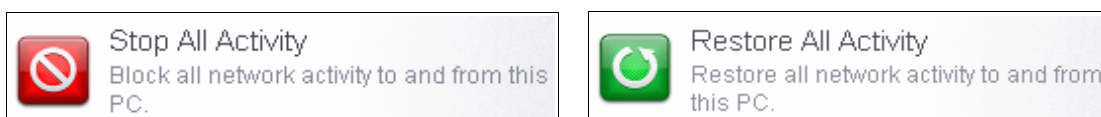
- You can choose to trust or block a network by selecting the appropriate radio button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks.
- Use the handles (< >) to scroll through all available networks or computers
- Use the refresh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



- The 'Manage 'Networks' interface can be opened by clicking 'Tasks > Firewall Tasks > Manage Networks'.
- To view, create or block **Network Zones**, click 'Tasks > Firewall Tasks > Open Advanced Settings > Network Zones'.

3.4. Stop all Network Activities

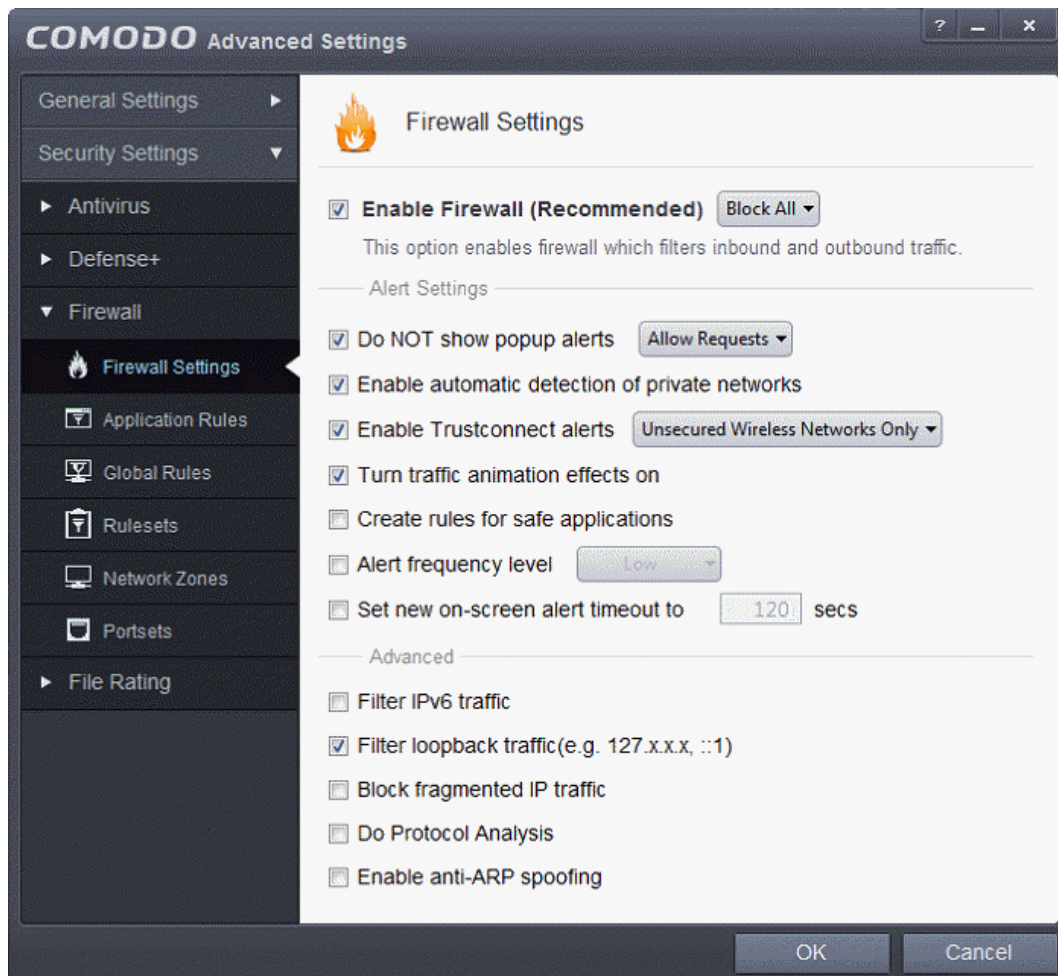
As the name suggests, the 'Stop all network activity' button instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and all available networks (including the Internet). Connections will remain closed until you re-enable them by clicking the button a second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



- Access the network activity 'on/off' button by clicking Tasks > Firewall Tasks
- Disconnect your computer from all networks by clicking 'Stop All Activity' (button will be red)
- Re-enable connectivity by clicking 'Restore All Activity' (button will be green)
- Restoring activity just re-enables your existing firewall rules. Therefore, any networks that you have previously blocked in '**Manage Network Connections**' or '**Network Zones**' will remain blocked.
- You can assign networks into network zones in the '**Network Zones**' area
- You can configure rules per network zone in the '**Global Rules**' area
- You can view all network connections and enable/disable connectivity on a per-network basis in the '**Manage Network Connections**' area

3.5. Advanced Firewall Settings

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

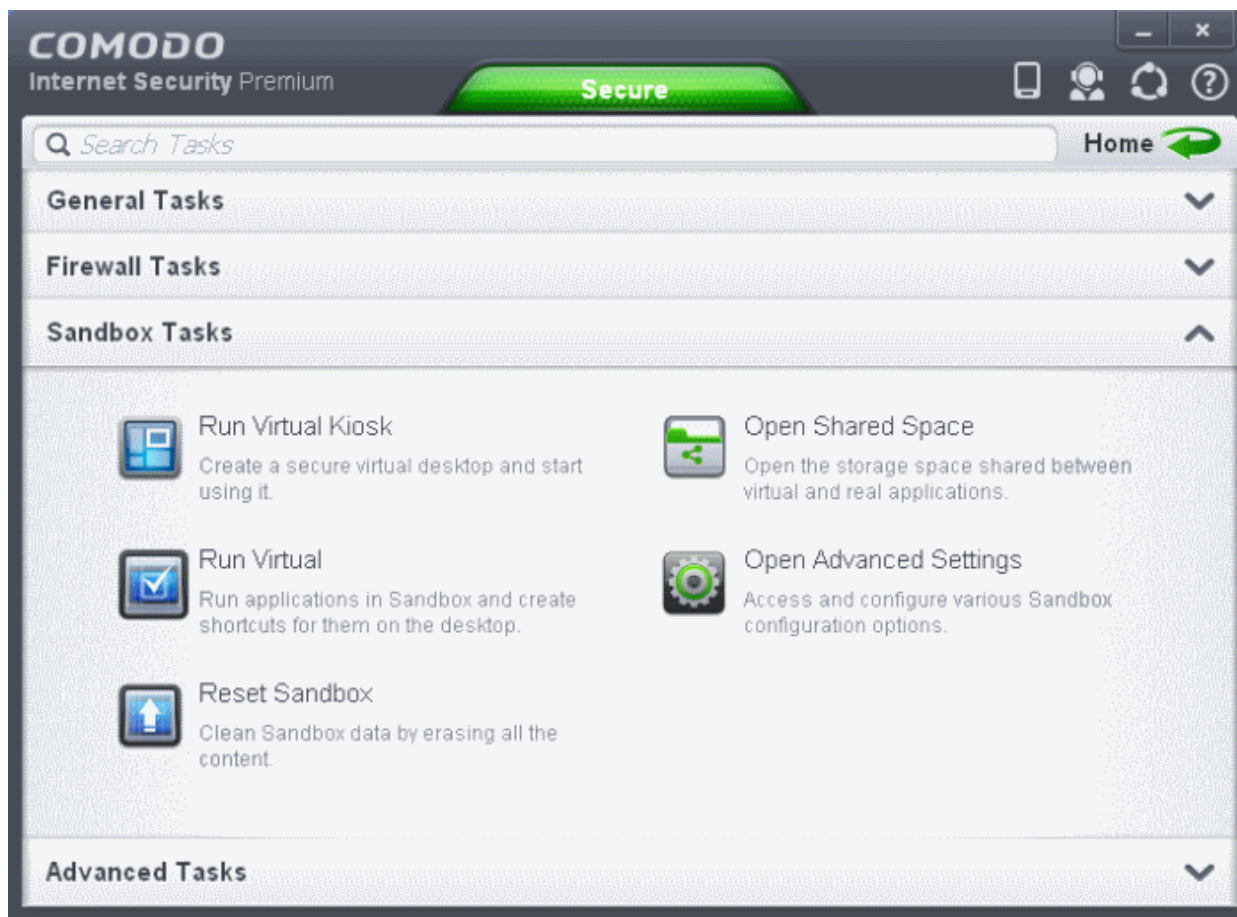


The interface is divided into six main sections - **Firewall Settings**, **Application Rules**, **Global Rules**, **Rulesets**, **Network Zones** and **Portsets**. Click the links below to jump to more details on each section:

- 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.

4. Sandbox Tasks - An Introduction

Comodo Internet Security features a fully functional sandbox called the '**Virtual Kiosk**'- an isolated operating environment for running unknown, untrusted and suspicious applications. Applications executed inside the sandbox/virtual kiosk 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.



Note: The sandbox referred to here is a full environment and is distinct to the 'auto-sandbox' configured under **behavior blocker**.

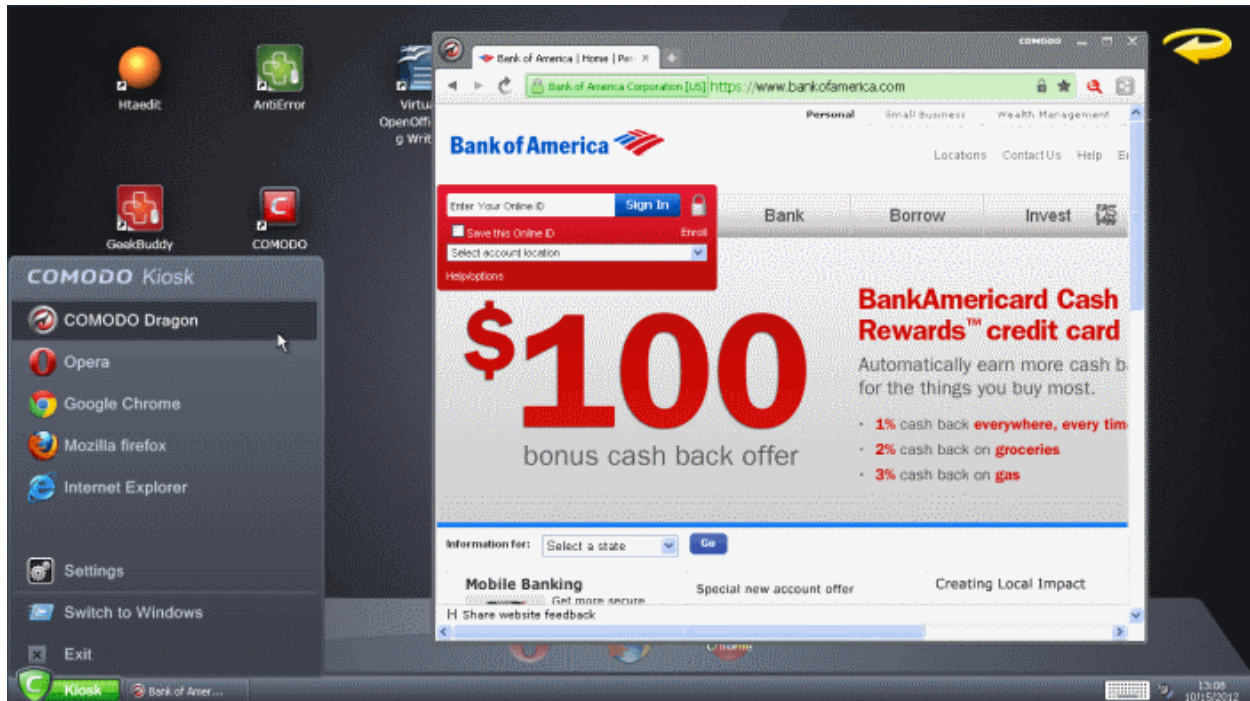
The Sandbox Tasks interface has shortcuts for the following tasks:

- **Run Virtual Kiosk** - Starts the Virtual Kiosk
- **Open Shared Space** - Opens the folder 'Shared Space' which is shared by your host operating system and the Virtual Kiosk. The folder is created by the Virtual Kiosk 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 Kiosk, and enables to share files and applications between the OS and the Kiosk.
- **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
- **Open Advanced Settings** - Add programs that should always run inside the sandbox and access advanced sandbox settings. This is covered in the '**Configure the Sandbox**' section of 'Advanced Settings'

4.1. The Virtual Kiosk

The Virtual Kiosk 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 kiosk 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 Kiosk at a glance:

- The kiosk 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 kiosk will not affect the original versions on your host system. Changes will only be visible in the Kiosk 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 Kiosk can be password-protected for added privacy.
- The virtual keyboard allows you to securely enter confidential passwords without fear of key-logging software.
- The kiosk UI can be used in both 'Classic' (Windows style) and 'Tablet' modes by selecting the mode from **Settings**.
- You can reset the kiosk 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.

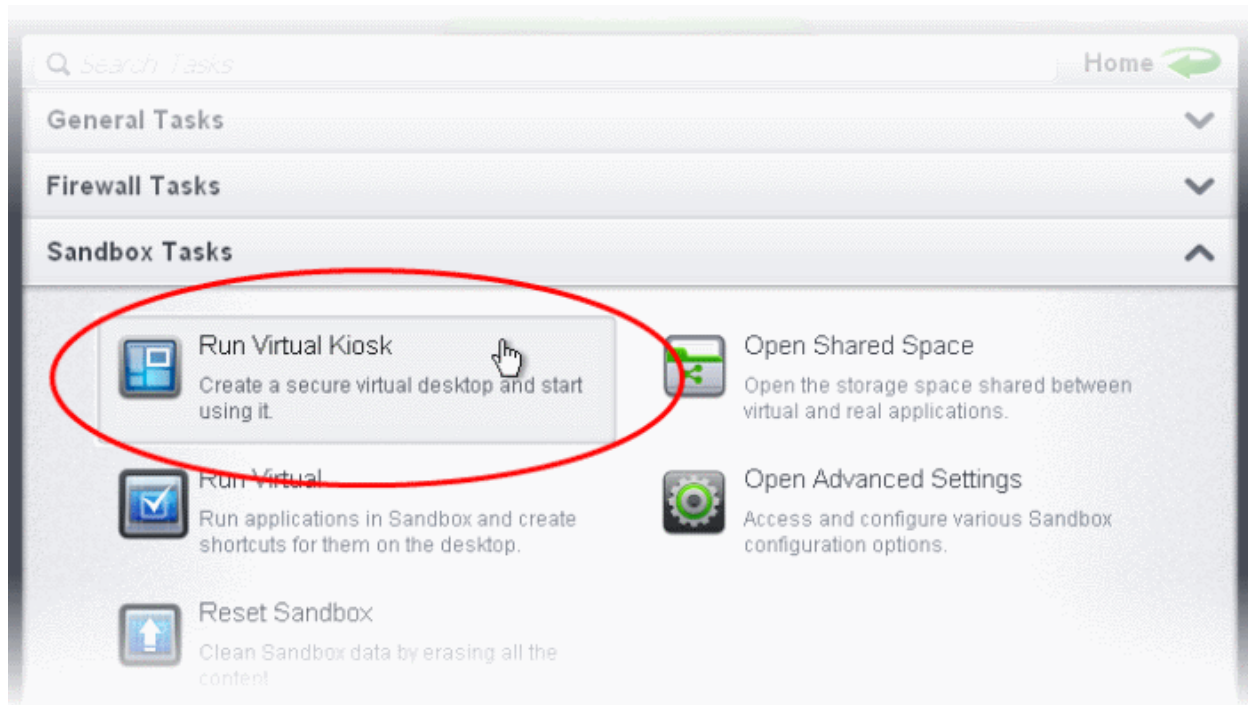
Click the following links to find out more details on:

- [Starting the Virtual Kiosk](#)
- [The Main Interface](#)
- [Run Browsers inside Virtual Kiosk](#)
- [Open Files and Run Applications inside Virtual Kiosk](#)
- [Configuring the Virtual Kiosk](#)
- [Closing the Virtual Kiosk](#)

4.1.1. Starting the Virtual Kiosk

The Virtual Kiosk can be started by:

- Clicking Tasks > Sandbox Tasks > Run Virtual Kiosk

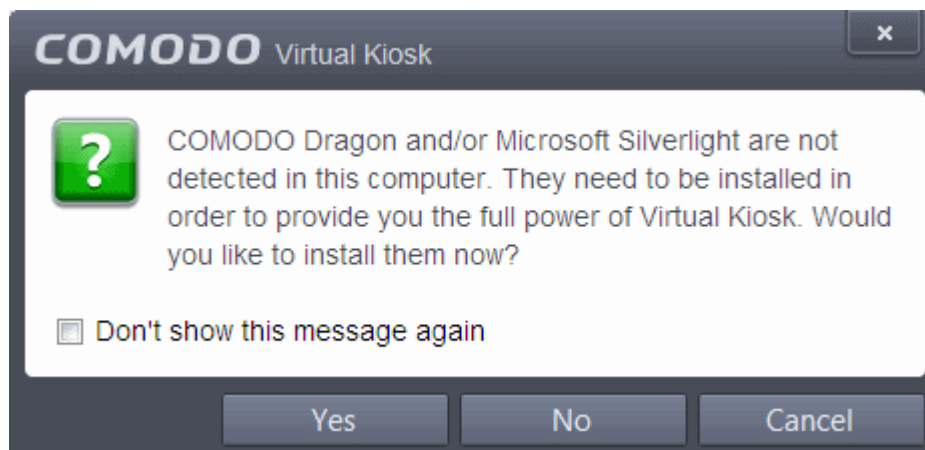


- Or by clicking the Virtual Kiosk shortcut button from the Home Interface

The following software is needed to utilize the Virtual Kiosk to its full potential:

- Comodo Dragon Browser
- Microsoft Silverlight

Whenever you run the kiosk, Comodo Internet Security checks whether these components are installed. If they aren't, you will be prompted to install them.



- If you want Comodo Dragon 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 Kiosk.
- If you do not want the applications to be installed at all, click 'No'.
- On clicking 'Yes', CIS will download and install the software

4.1.2. The Main Interface

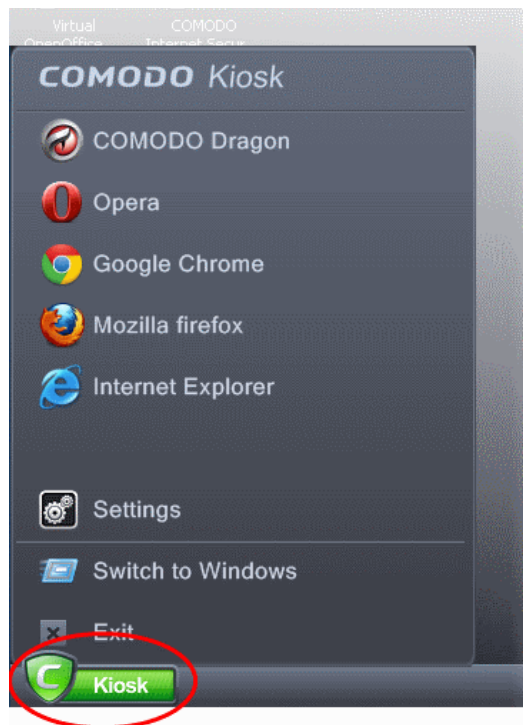
The Virtual Kiosk is presented with two switchable interfaces:

- **Classic Windows style Desktop mode**
- **Tablet mode**

You can switch between these two modes by clicking the green 'Kiosk' button then 'Settings' (**Kiosk > Settings > 'Mode' tab.**) refer to the **table below** for a comparison of different modes of the Kiosk main interface.

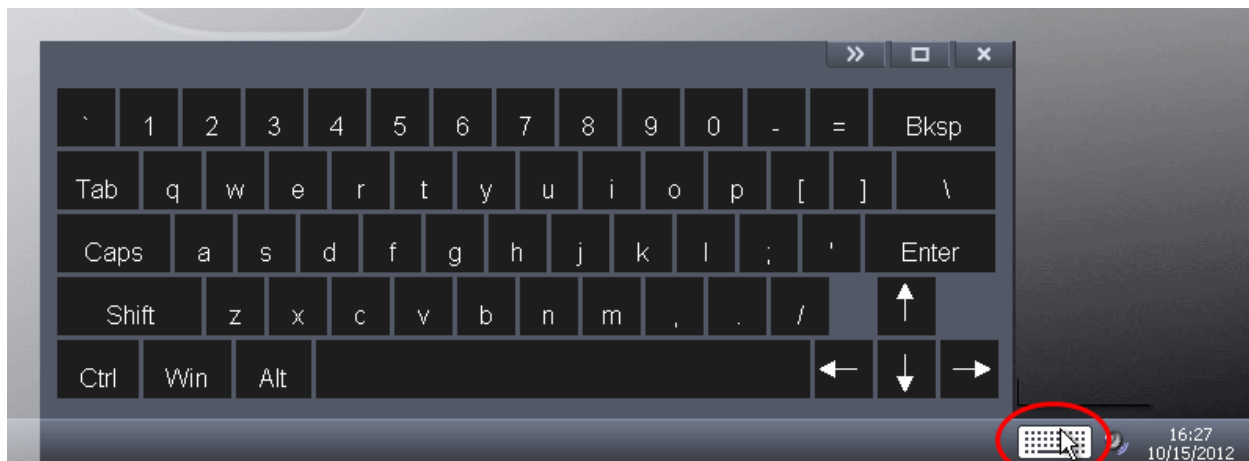
In 'Classic' mode,

- All desktop items of your real system are displayed. Clicking the shortcuts on the kiosk desktop will run the program or file inside the kiosk
- Clicking the 'Kiosk' button at the bottom left will open a Windows style Start Menu style Kiosk menu



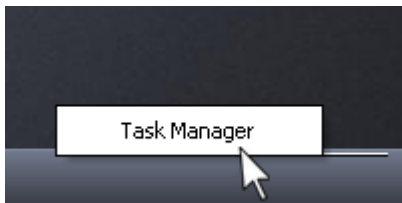
The Kiosk menu allows you to:

- Run browsers that are installed on your system. Refer to **Running Browsers inside the Virtual Kiosk** for more details
- Configure the Virtual Kiosk by clicking 'Settings'. Refer to **Configuring the Virtual Kiosk** 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.



- To display the numeric keypad on the right, click the >> button at the top of the keyboard.

- Clicking the 'Volume Control' icon at the system tray enables you to control the system volume.
- Right-clicking on the task bar and selecting 'Task Manager' 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 'Kiosk' 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 webstore.
2. Mode B - Tablet device + Classic Windows - The home page displays the desktop items from your real system. The task bar from classic mode is present along with the green 'Kiosk' button and the virtual keyboard. The launch strip will display all installed browsers.

You can swap between the two variations by tapping the arrow  at the top right. You can swipe the home screen in both left and right directions to navigate between successive home pages.



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 + Classic
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 Kiosk

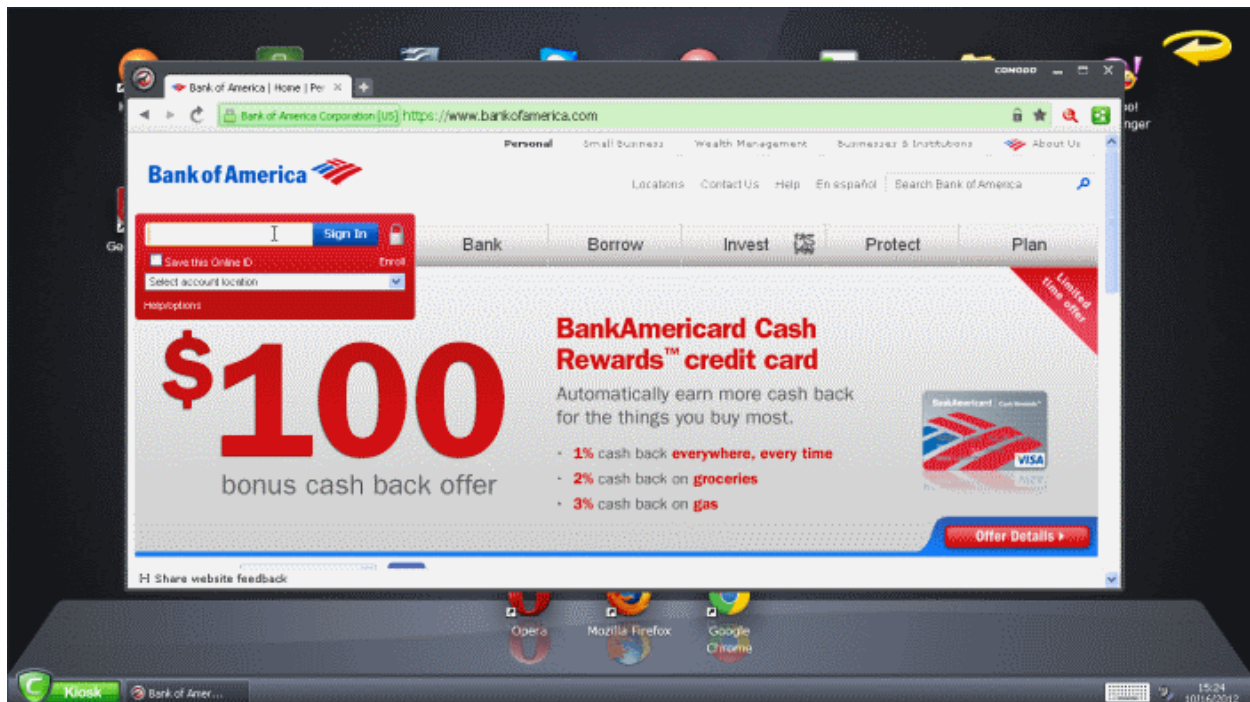
The Virtual Kiosk provides an extremely secure environment for Internet related activities because it isolates your browser from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net inside the Kiosk 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 Kiosk

1. Click the 'Kiosk' menu at the bottom left
2. Select the browser you want to run from the browsers displayed.



The browser will be opened inside the Kiosk.



On completion of your browsing session, no trails like your browsing history will be stored in your computer.

4.1.4. Opening Files and Running Applications inside the Virtual Kiosk

Applications installed or the files stored in your system can be opened inside the Virtual Kiosk 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 Kiosk, in the desktop of your real system. The shortcuts of your real desktop will be available in the Virtual Kiosk desktop. You can double click on the icon to open the respective application of file inside the Virtual Kiosk.

Note: The real computer desktop icons will be available only in the **Classic Windows Mode** and **Tablet + Classic Mode**.

Shared Space

The Virtual Kiosk 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 Kiosk.

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 Kiosk

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 Kiosk'
4. Open Shared Space inside the Virtual Kiosk 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 Kiosk.

The changes you make to the file will be stored to the file only inside the Virtual Kiosk and not in the real computer system.

4.1.5. Configuring the Virtual Kiosk

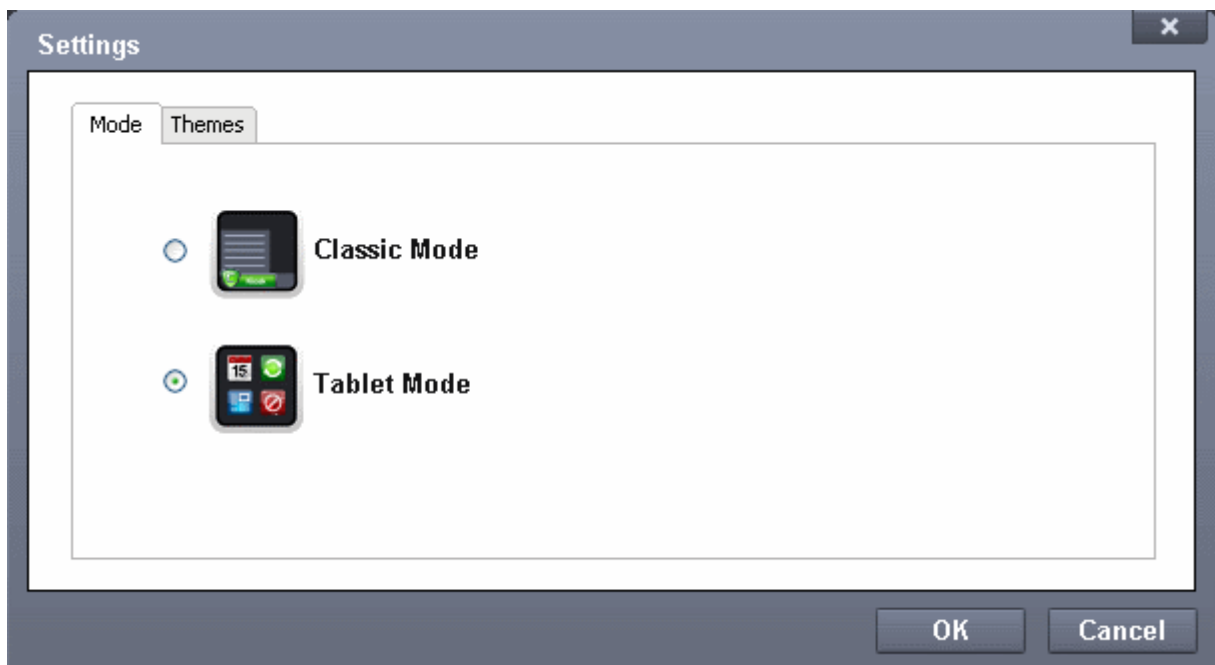
The Settings panel in the Virtual Kiosk allows you to configure the operation mode and look and feel of the Kiosk.

To configure the Virtual Kiosk

1. Click the 'Kiosk' start menu at the bottom left
2. Select 'Settings' from the Kiosk start menu



The Settings panel will open.



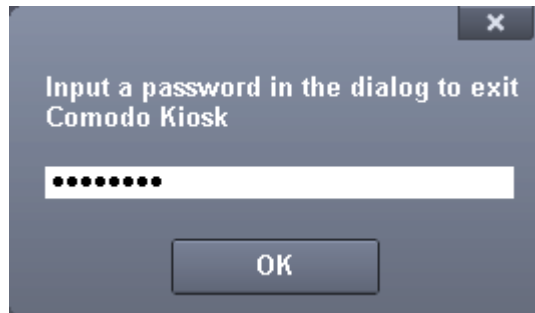
The Settings panel has two tabs:

- **Mode** - Allows you to select the display mode of the Virtual Kiosk between Classic Windows mode and Tablet Mode (Default)
 - **Themes** - Allows you to choose the appearance of the Kiosk
3. Click OK for your settings to take effect

4.1.6. Closing the Virtual Kiosk

To close the Virtual Kiosk and return to your real computer system

1. Click the 'Kiosk' start menu at the bottom left
 - To temporarily switch to your real Windows system, Select 'Switch to Windows'. The Virtual Kiosk will be temporarily closed and you can quickly return to it by clicking 'Open Virtual Kiosk' from the 'Sandbox Tasks' interface.
 - To close the Virtual Kiosk, select 'Exit'. The Virtual Kiosk will be shut down and you will be able to continue with your real system.
2. 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 Kiosk will be closed.



3. Enter the password and click OK.

Note: Remember to save the changes before you exit the Virtual Kiosk. Your changes will be lost if you exit the Kiosk without saving them.

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**).

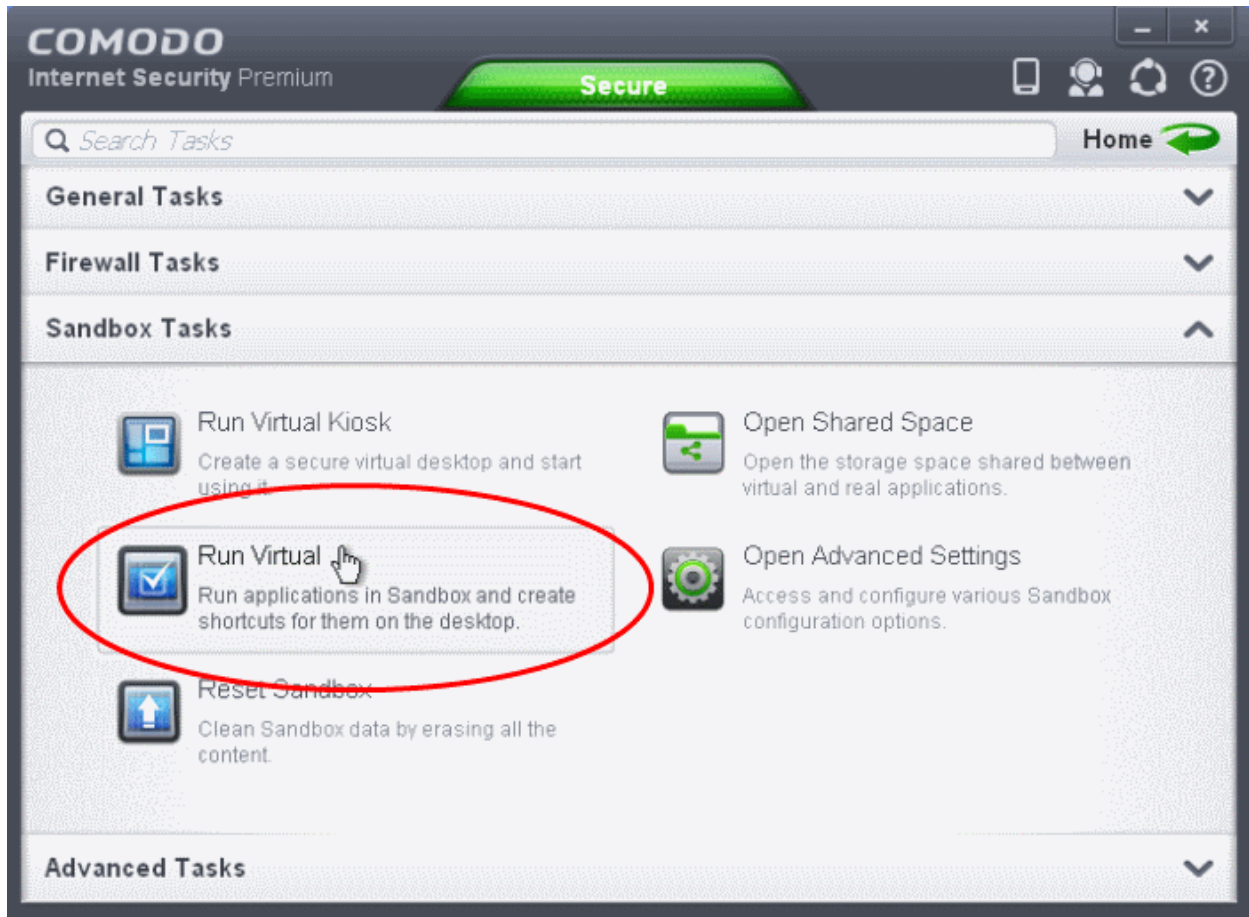
You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



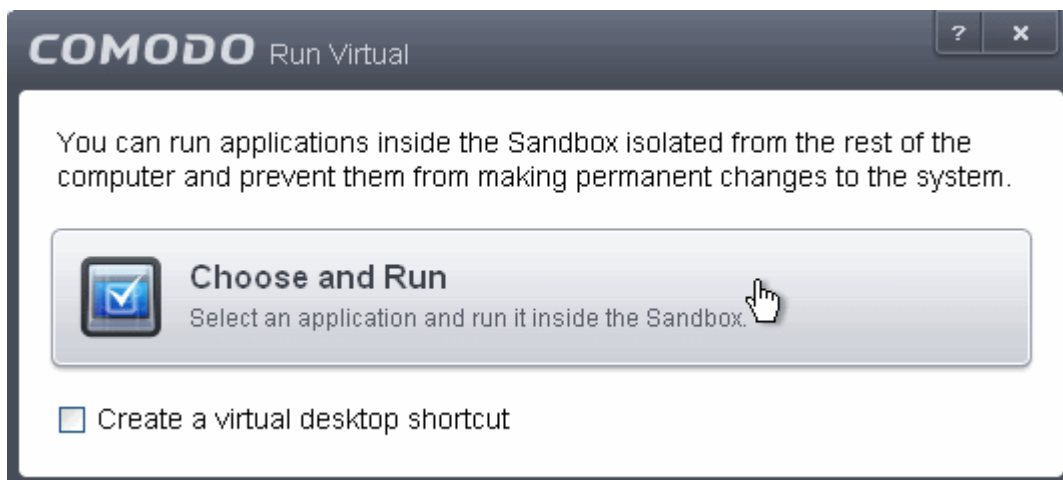
Note: If you wish to run an application in the sandbox on a long-term/permanent basis then **add the file to the Sandbox**.

To run an application in the Sandbox

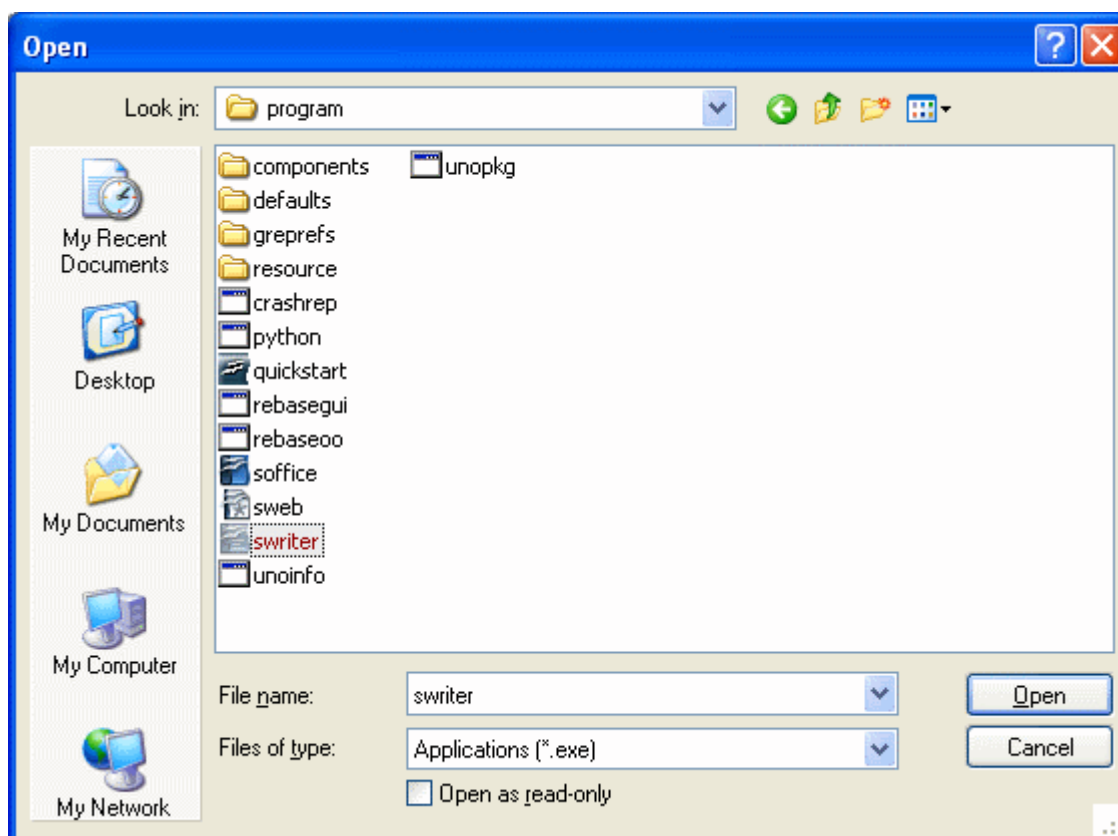
1. Open the Sandbox Tasks interface and Click 'Run Virtual'.



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

The Home screen of the CIS interface has a flippable pane at the left side allowing you to run instant scans or run a program in sandbox. To flip the pane to carry out these tasks, just click the curved arrow at the top right side of the pane.



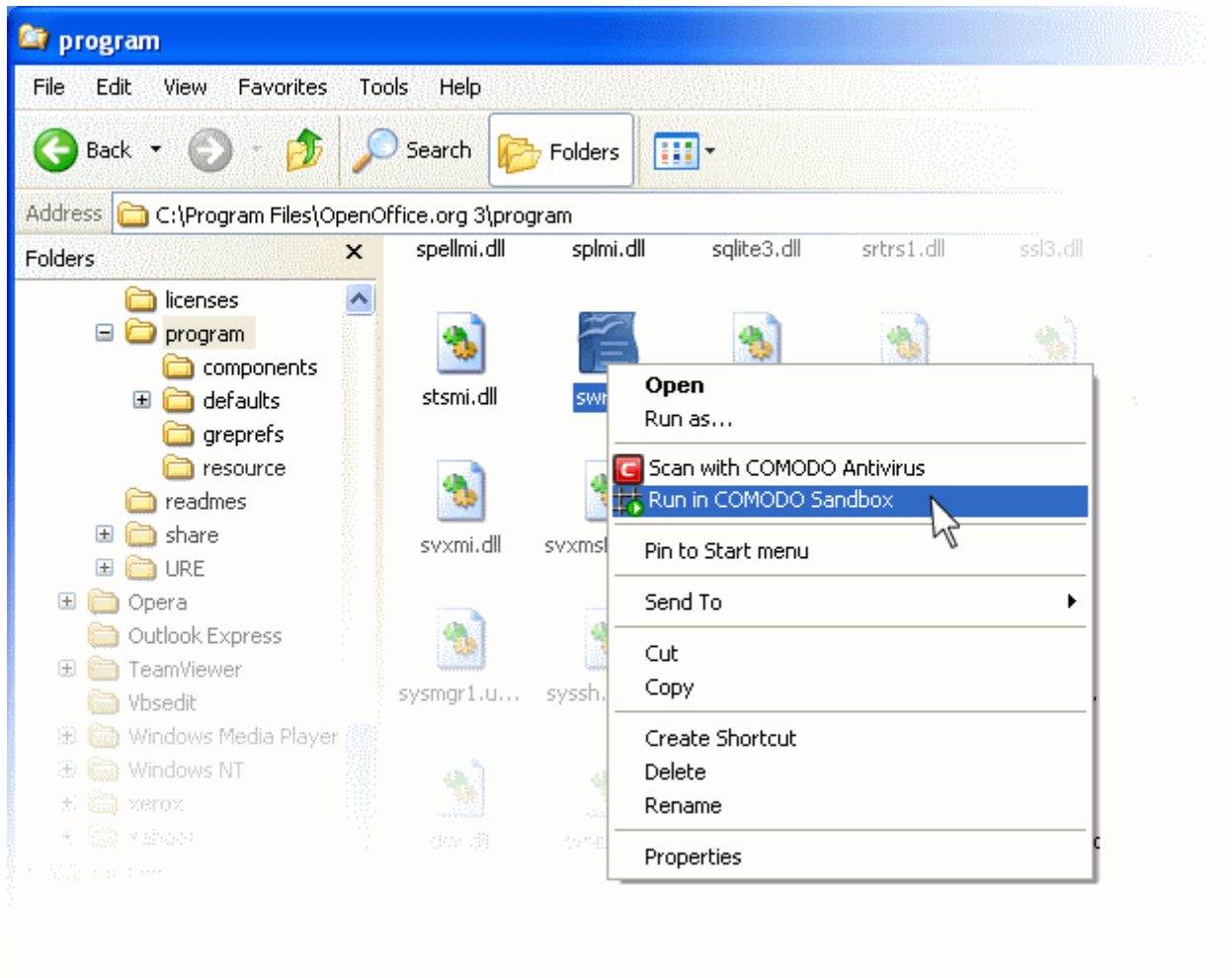
To run a program in a sandbox, first flip the pane by clicking the curved arrow at the top right side to display 'Sandbox Objects'.



Now, navigate to the program in your system that you want to run in sandboxed environment and just drag and drop into the box.

Running a program from the context sensitive menu

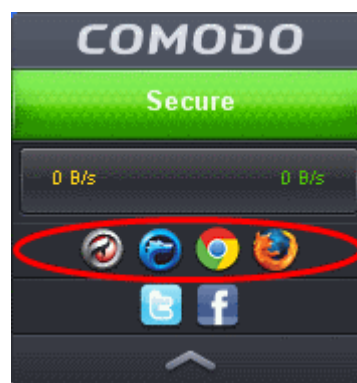
- Navigate to the program in your system that you want to run in sandboxed environment and right click on it



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

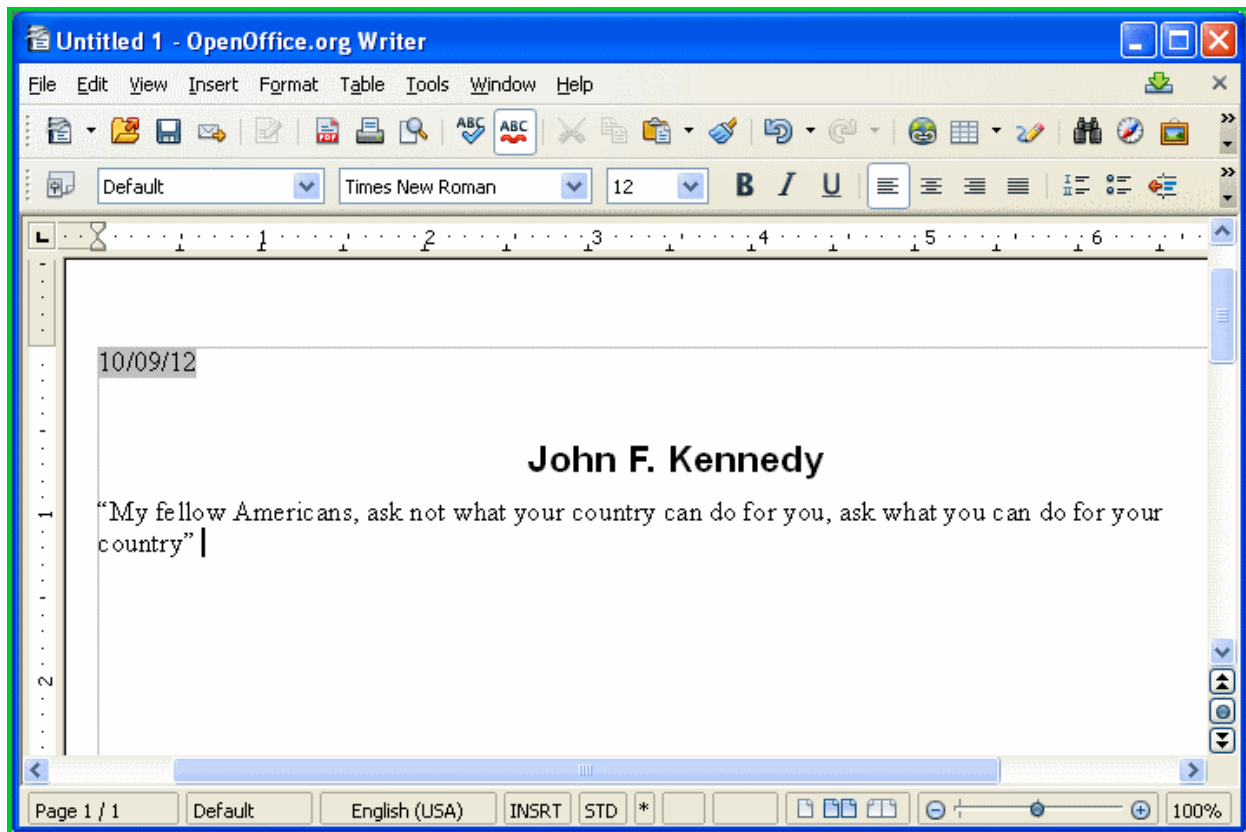
Running Browsers inside the Sandbox

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 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**.

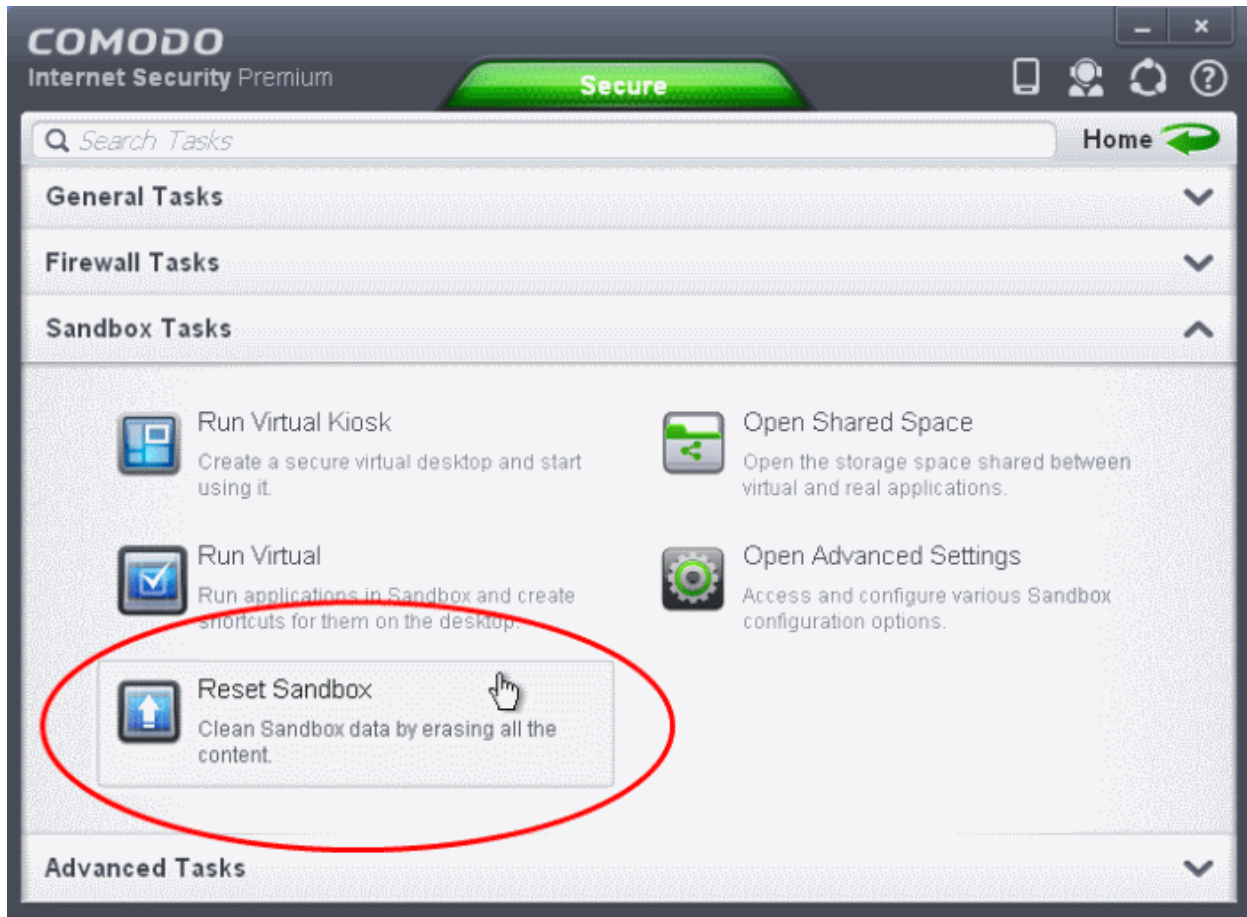
4.3. Reset the Sandbox

Programs running inside the Virtual Kiosk 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 Kiosk 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 Kiosk 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

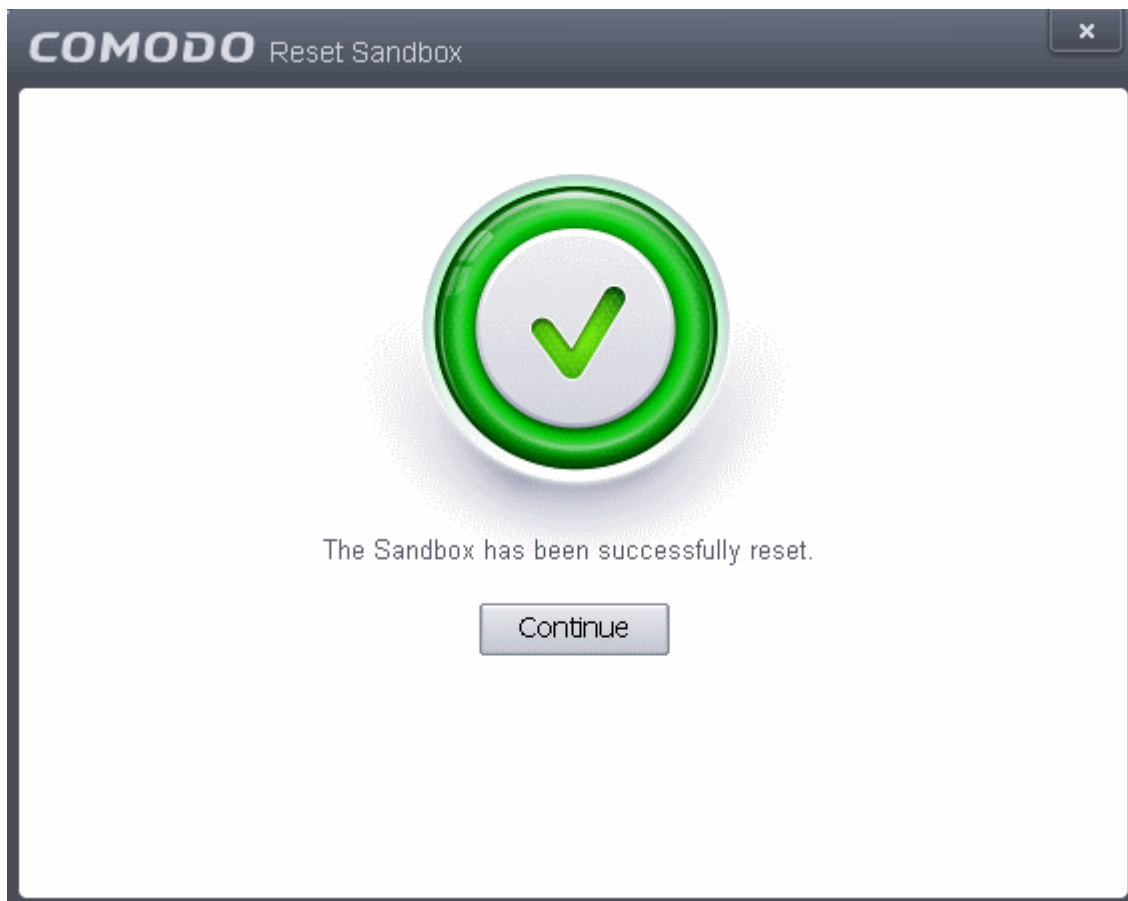
- Click on the 'Sandbox Tasks' bar from the Tasks interface and then click 'Reset Sandbox'



The 'Reset Sandbox' dialog will appear.



- Click 'Erase Changes'. The contents in the sandbox will be deleted immediately.



5. Advanced Tasks - An Introduction

The 'Advanced Tasks' area allows you modify the overall configuration of CIS 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](#)
- [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

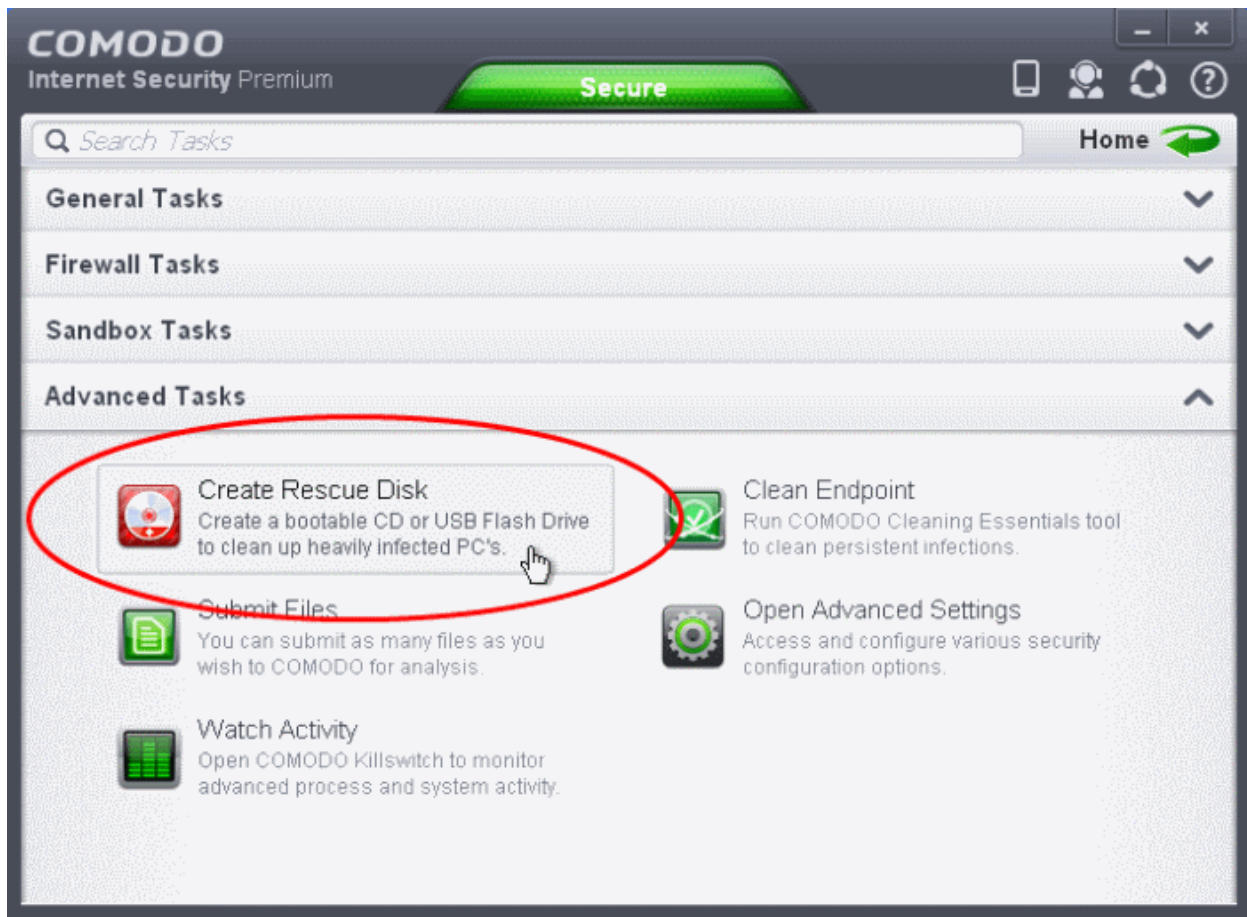


After you have burned the ISO, you need to boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

- 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-170-1-414-4583-Changing-Boot-Order.html>
- Details of how to initiate CRD after booting can be found at: <http://help.comodo.com/topic-170-1-414-4584-Booting-to-and-starting-Comodo-Rescue-Disk.html>
- Details of how to start running scans on your pre-boot environment begin here <http://help.comodo.com/topic-170-1-414-4581-Starting-Comodo-Cleaning-Essentials.html> and here <http://help.comodo.com/topic-170-1-414-4582-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 Comodo Rescue Disk interface displays the steps involved in creation of a new Rescue Disk on a CD/DVD or in a USB drive.

Step 1- Select the ISO file

This step allows you to select the Comodo Rescue Disk image file in .iso format stored in your hard drive, if you have already

downloaded the same from Comodo servers or copied from another computer. Pre-storing the .iso file and burning the rescue disk from it conserves your Internet connection bandwidth usage. This step is optional. If you haven't downloaded the iso file, it will be automatically downloaded from Comodo Servers prior to execution of Step 3 - Burning the Rescue Disk.

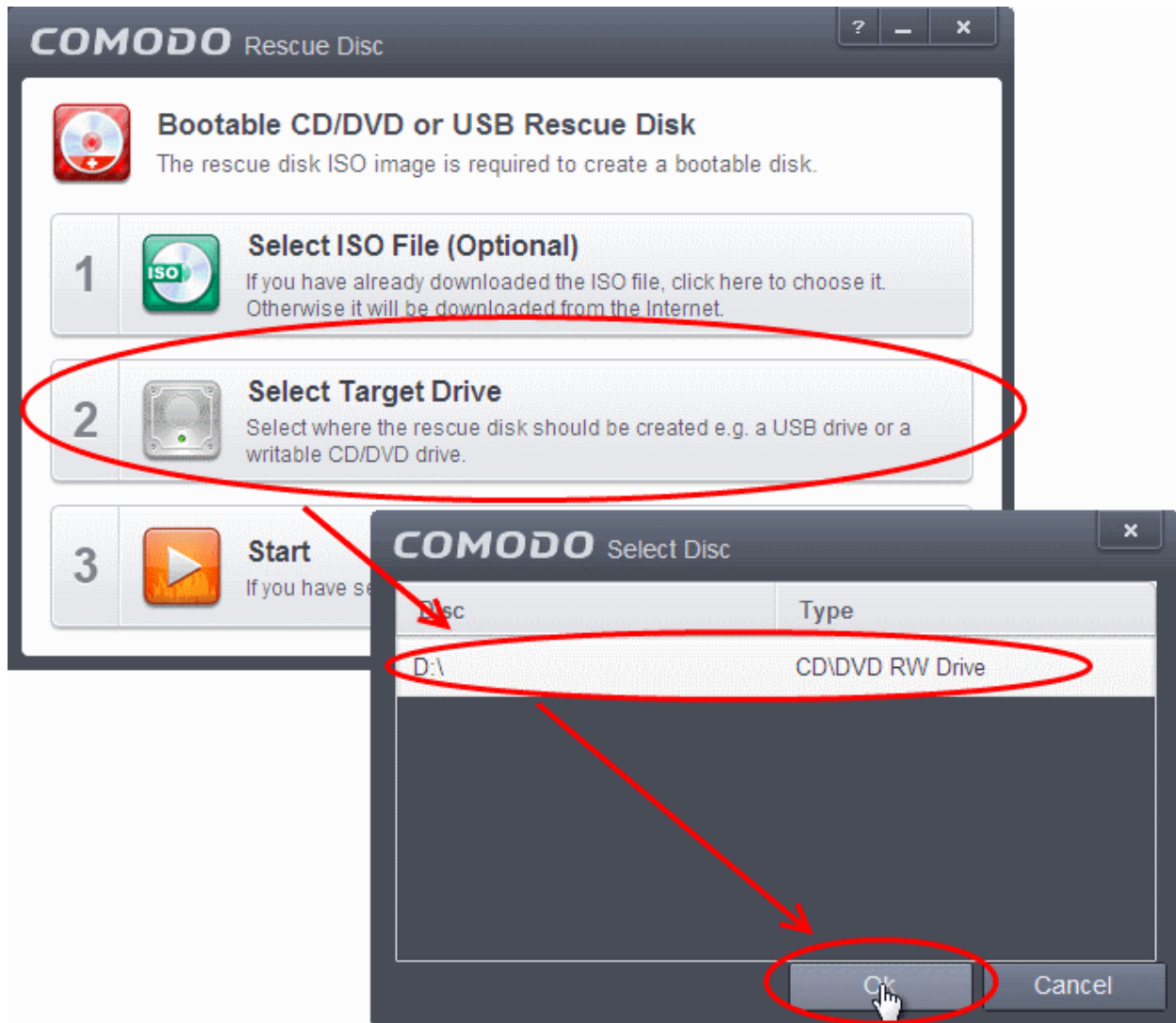
- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

This step allows you to select the CD/DVD drive or the USB drive to burn the Rescue Disk.

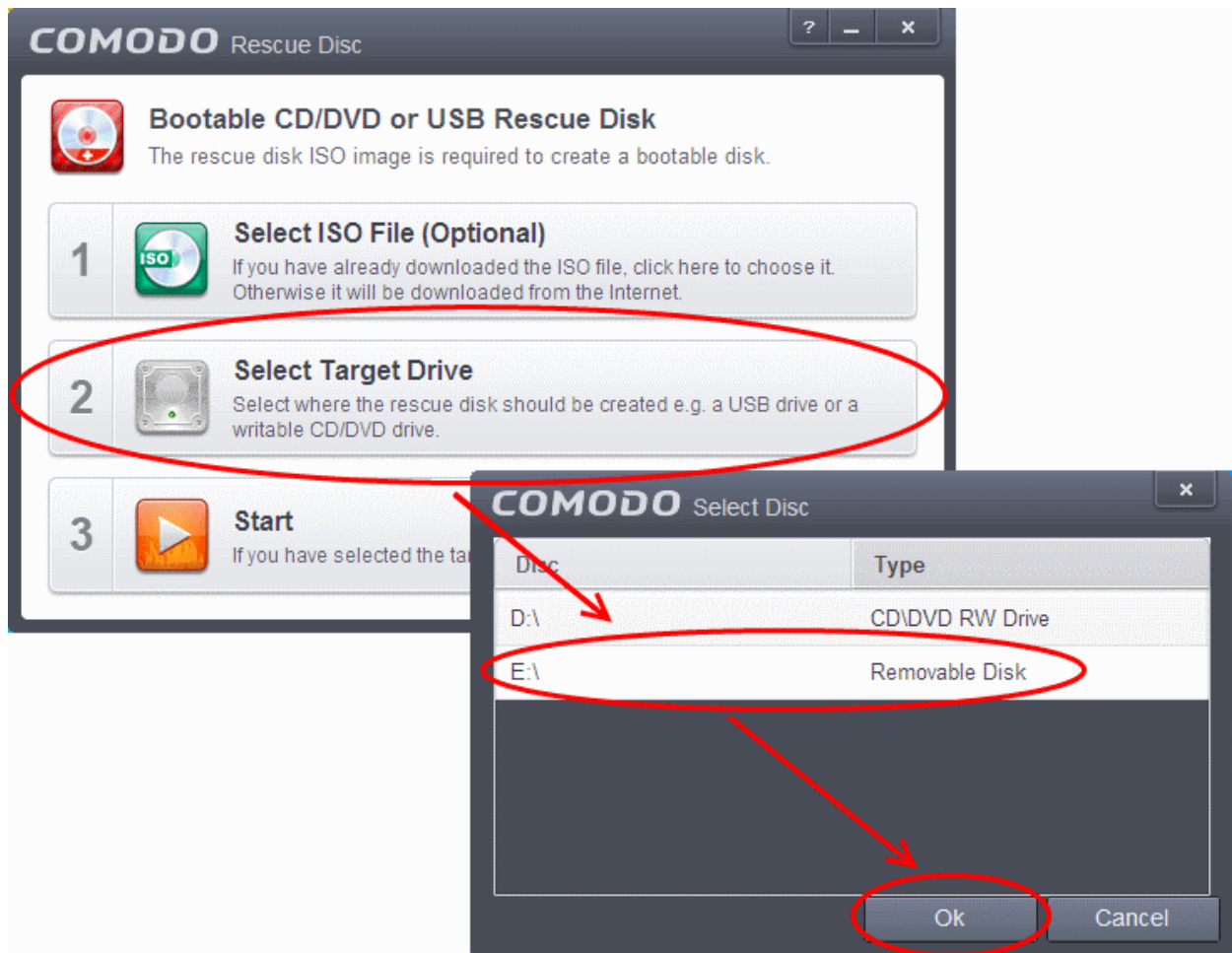
To burn the Rescue disk on a CD or a DVD

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



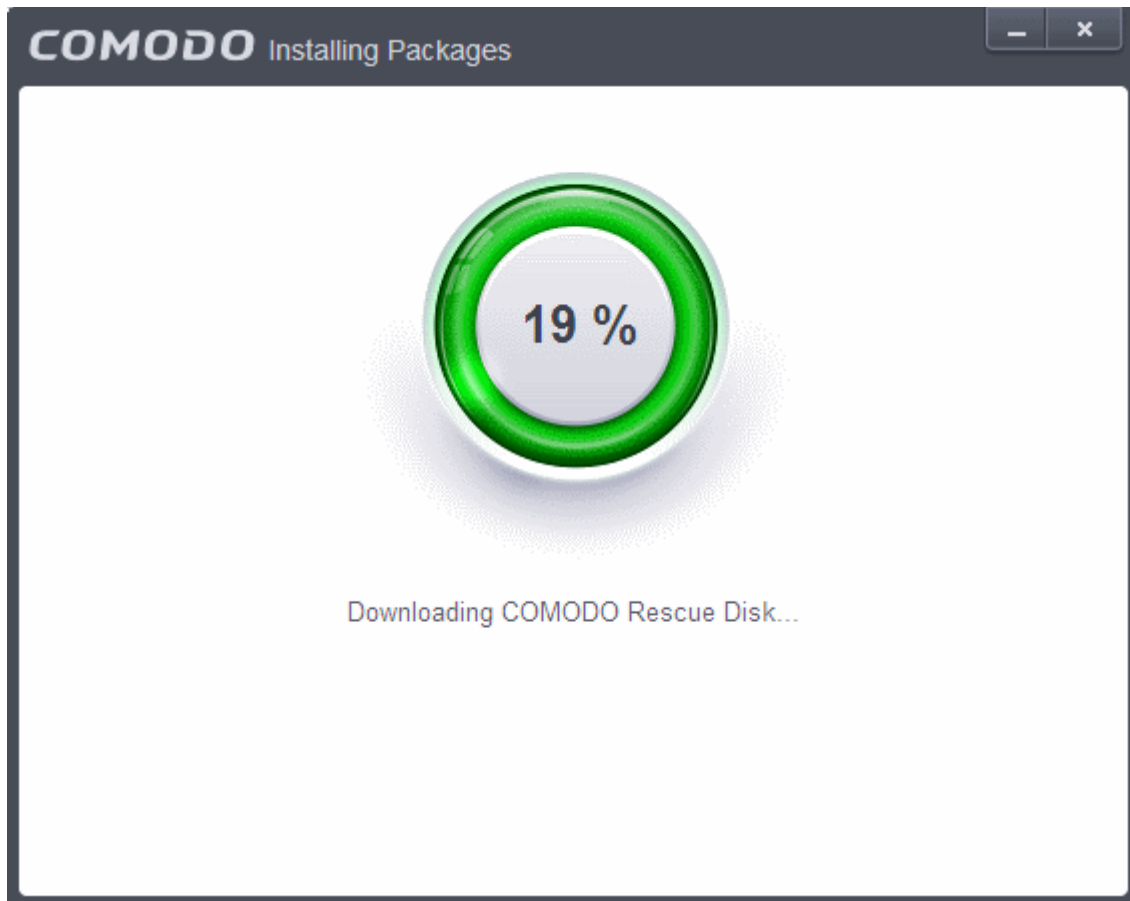
To burn the Rescue disk on a USB Drive

- 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 Disc dialog

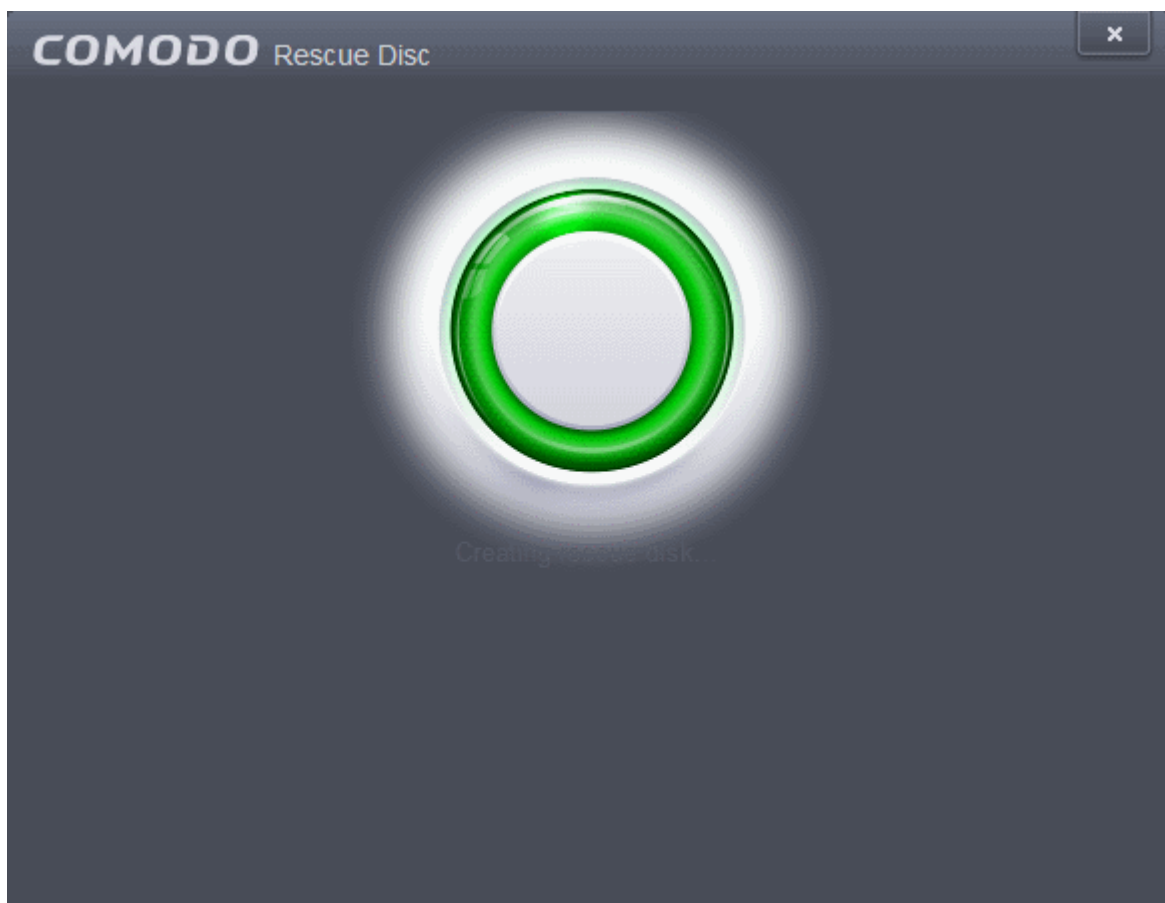


Step 3 - Burn the Rescue Disk

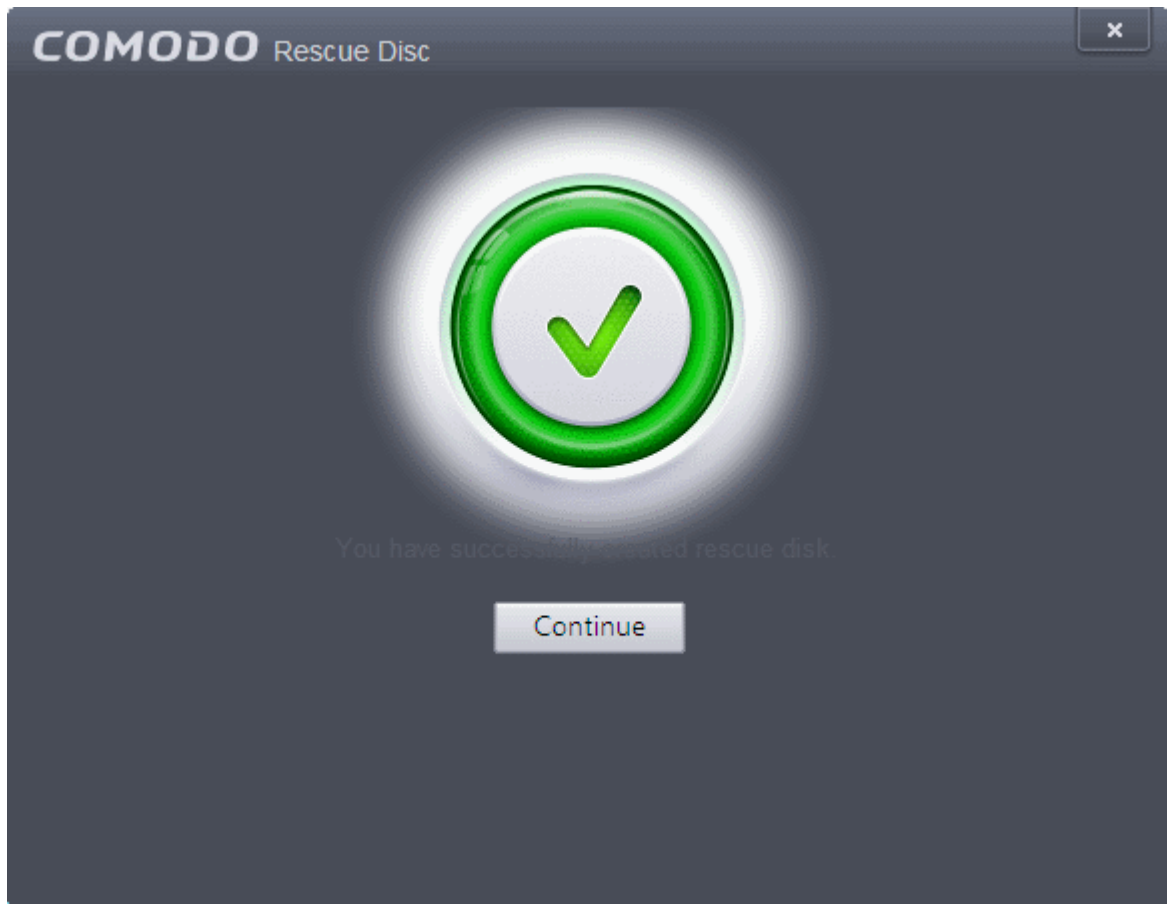
- After you selected the target drive, click 'Start'. If you have selected an .iso file from your hard disk, the burning of the disk will start immediately. Else, the .iso file will be downloaded from Comodo Servers.



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.

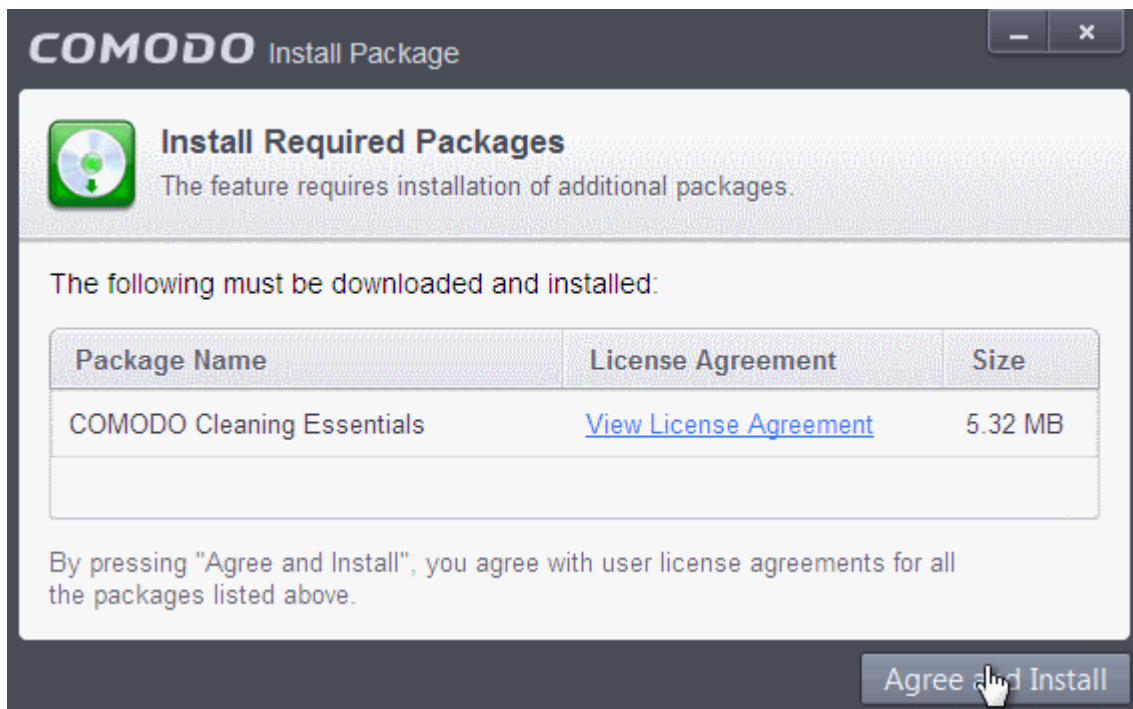
CCE enables home users to quickly and easily run scans and operate the software with the minimum of fuss. More experienced users will enjoy the high levels of visibility and control over system processes and the ability to configure customized scans from the granular options menu.

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>.

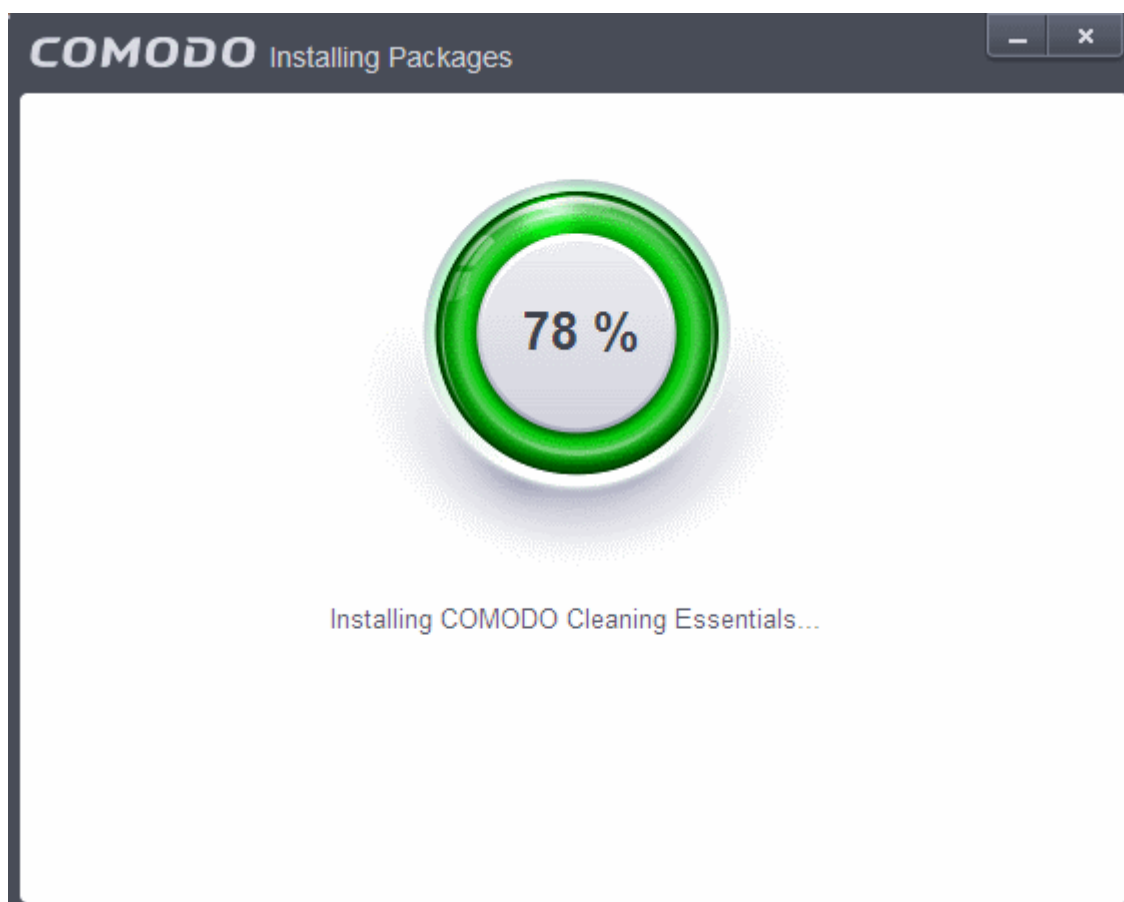
Comodo Cleaning Essentials can be directly accessed from the CIS interface by clicking the 'Clean Endpoint' button in the 'Advanced Tasks' interface.



- 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>

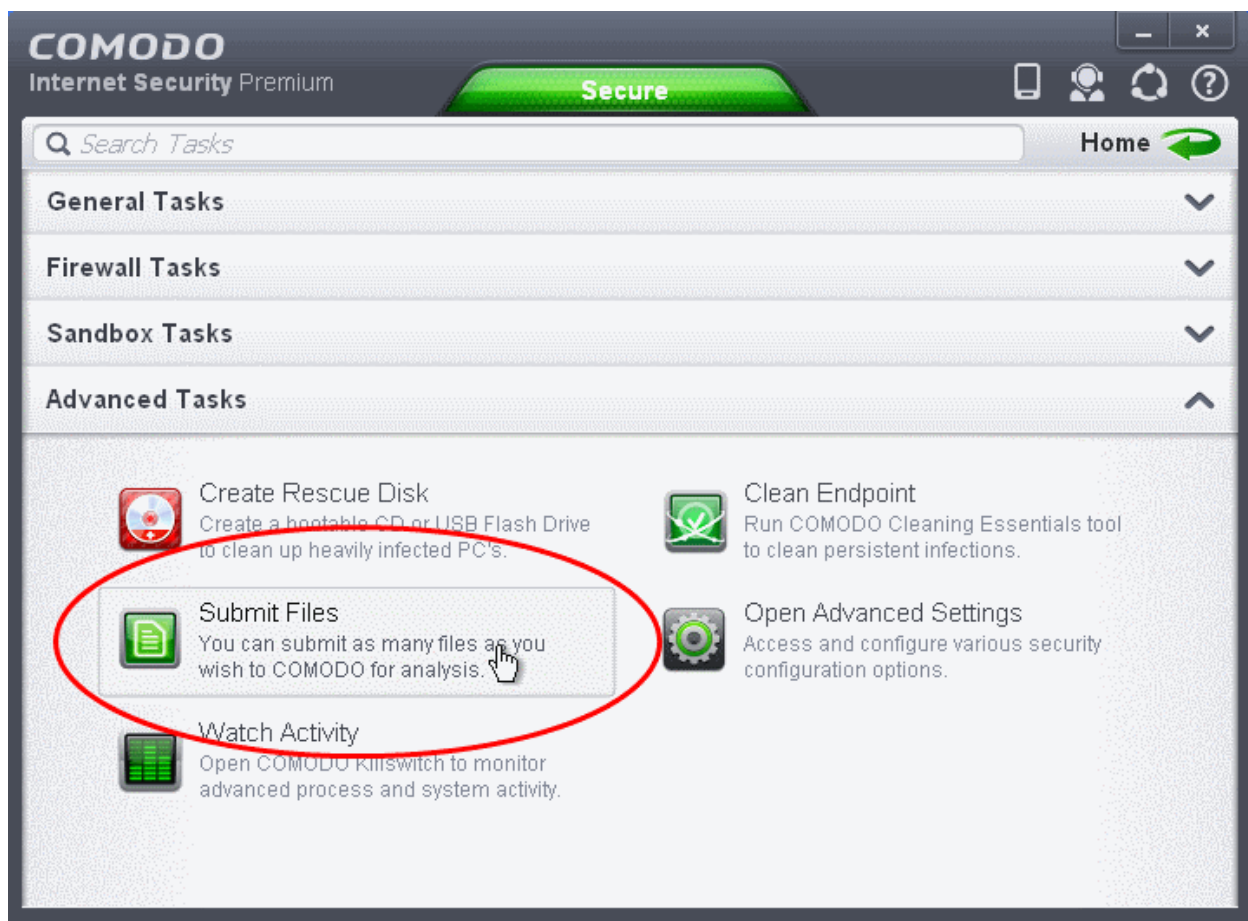
- On clicking the 'Clean Endpoint' button from next time onwards, Comodo Cleaning Essentials will be opened.

5.3. Submit Files

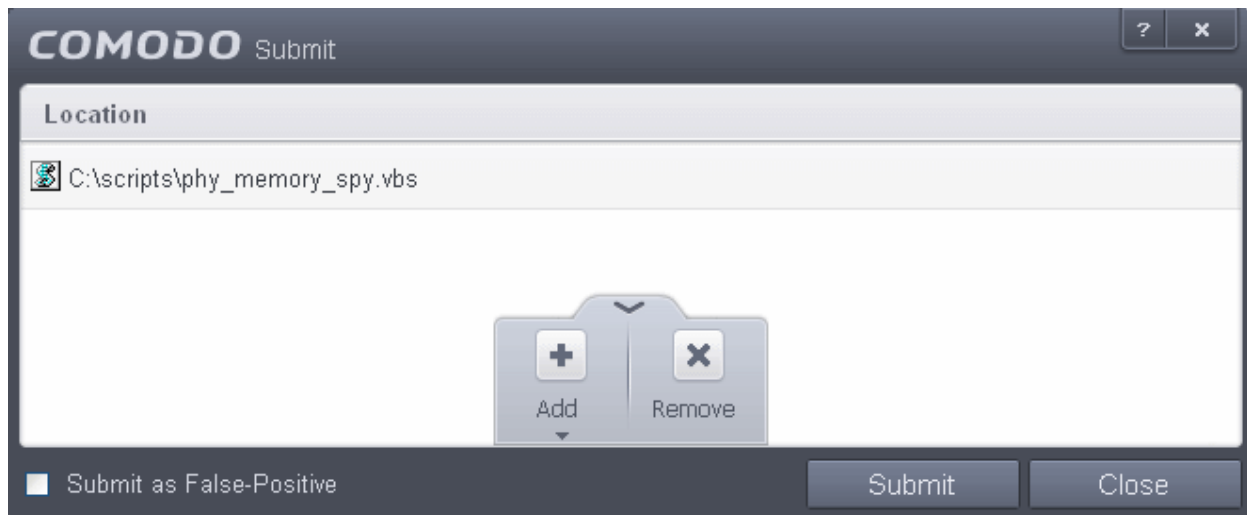
As the name suggests, the 'Submit Files' interface allows you to send as many files as you wish to Comodo for analysis. Files which CIS classifies as 'Unknown' or 'Unrecognized' are not in the Comodo safe list but have also not been identified as known malware. By sending these files to Comodo, you allow 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 '**Unrecognized Files**' interface should you prefer.

To open the 'Submit Files' interface, click 'Tasks' on the home screen followed by 'Advanced Tasks' > 'Submit Files'



The 'Submit' interface will open.

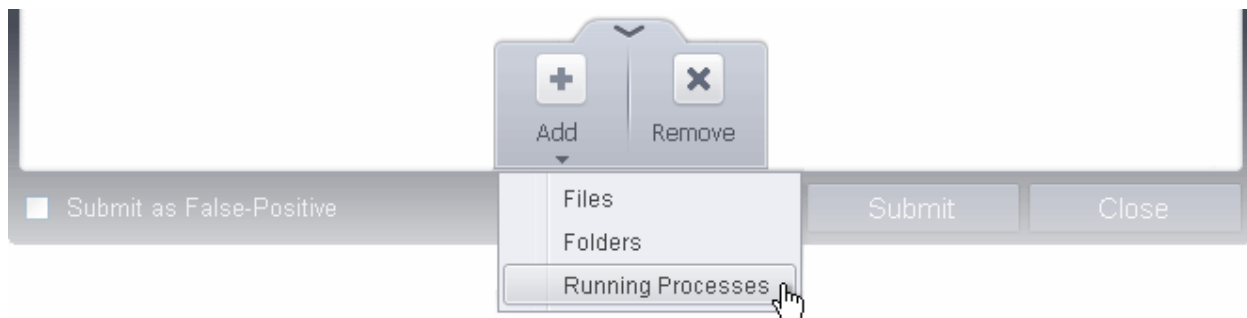


Clicking the handle at the bottom center of the panel opens the following options:

- **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-

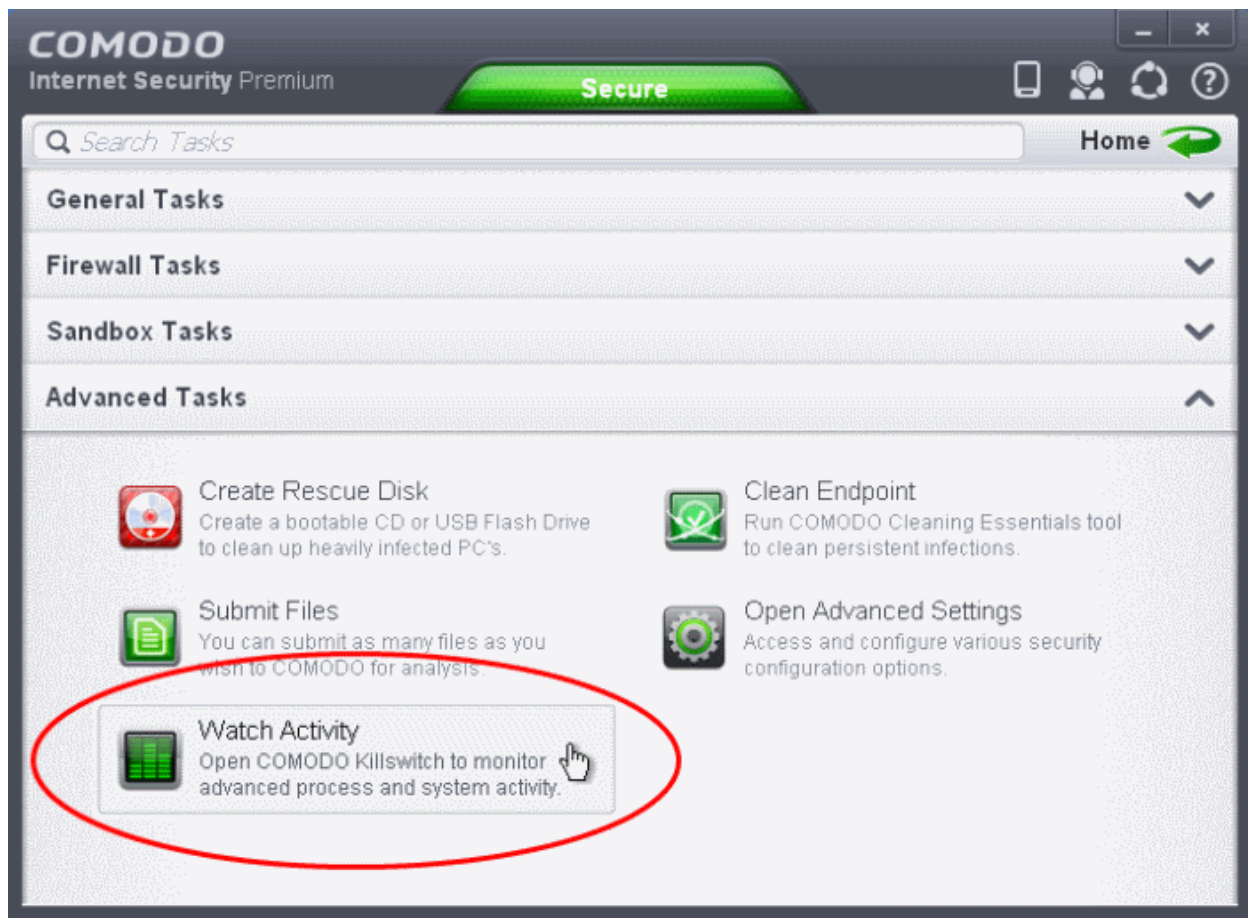
listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed). The list of files submitted from your computer can be viewed from the **Submitted Files** interface.

5.4. Identify and Kill Unsafe Running Processes

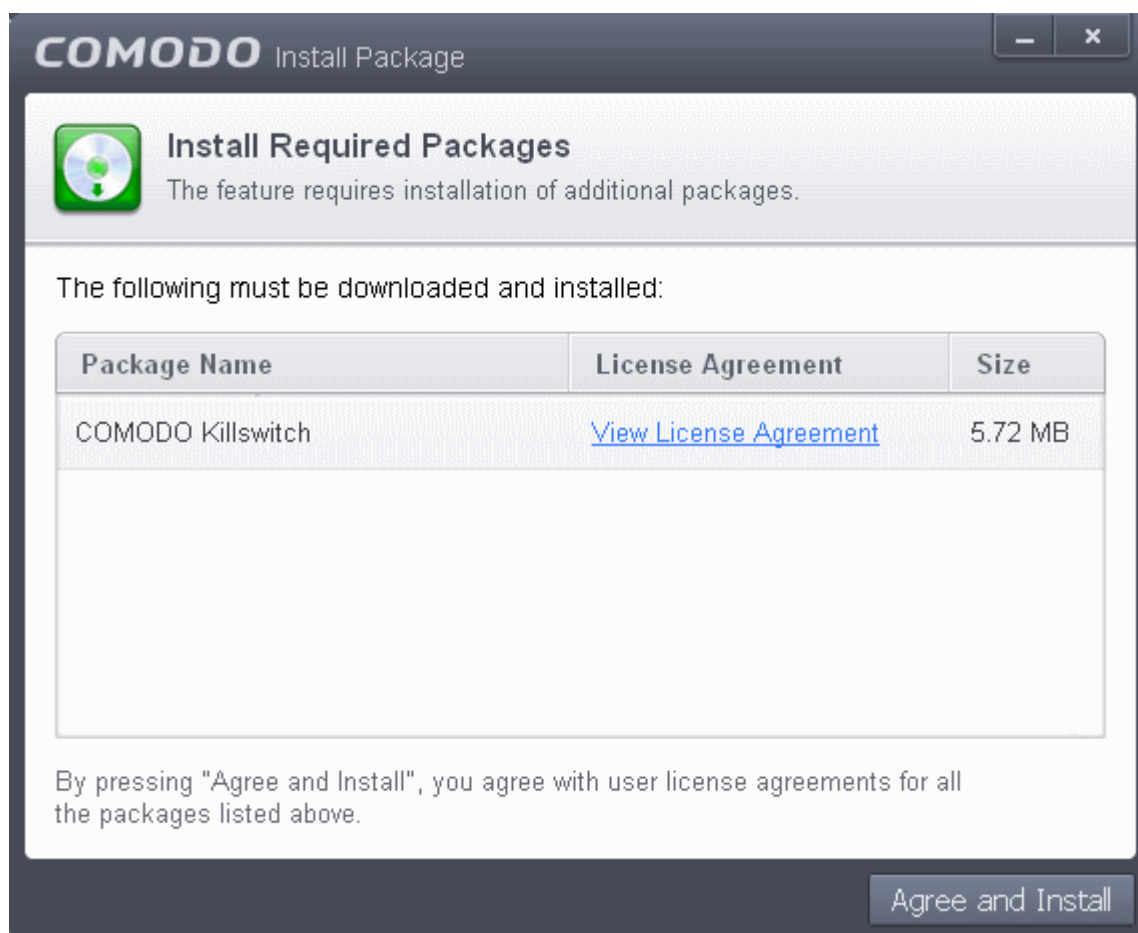
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer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



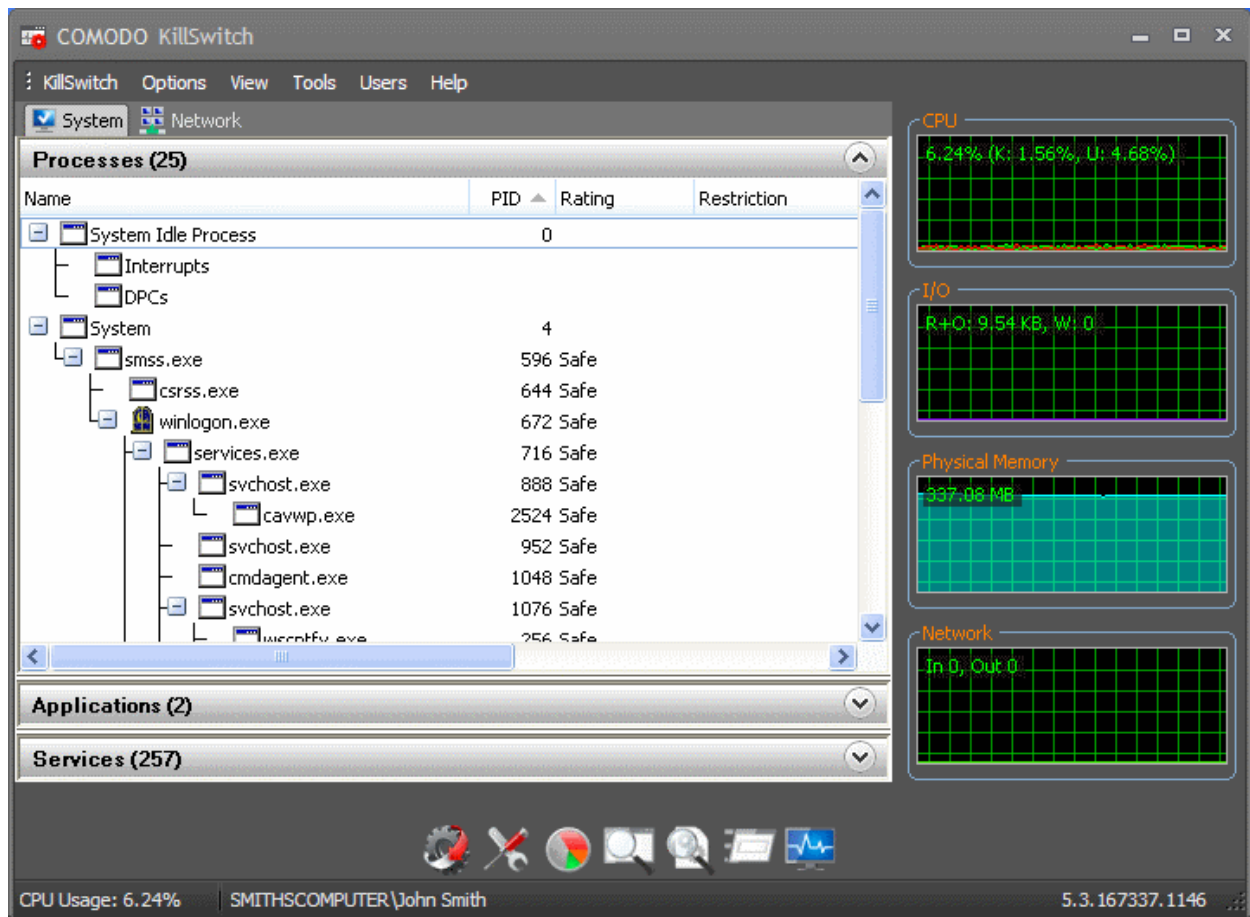
- Clicking the 'Watch Activity' for the first time, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



- 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.

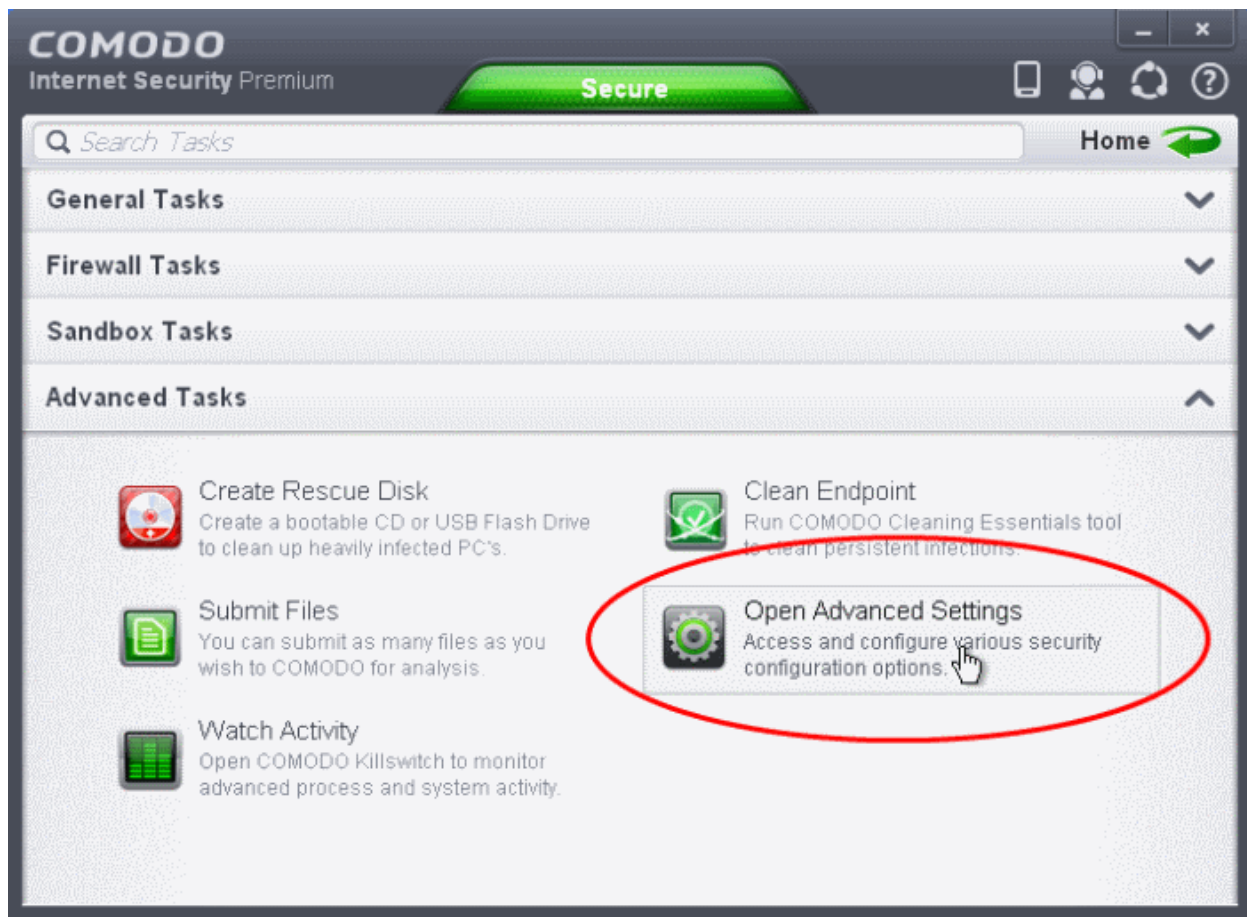
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at <http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html>

6. Advanced Settings

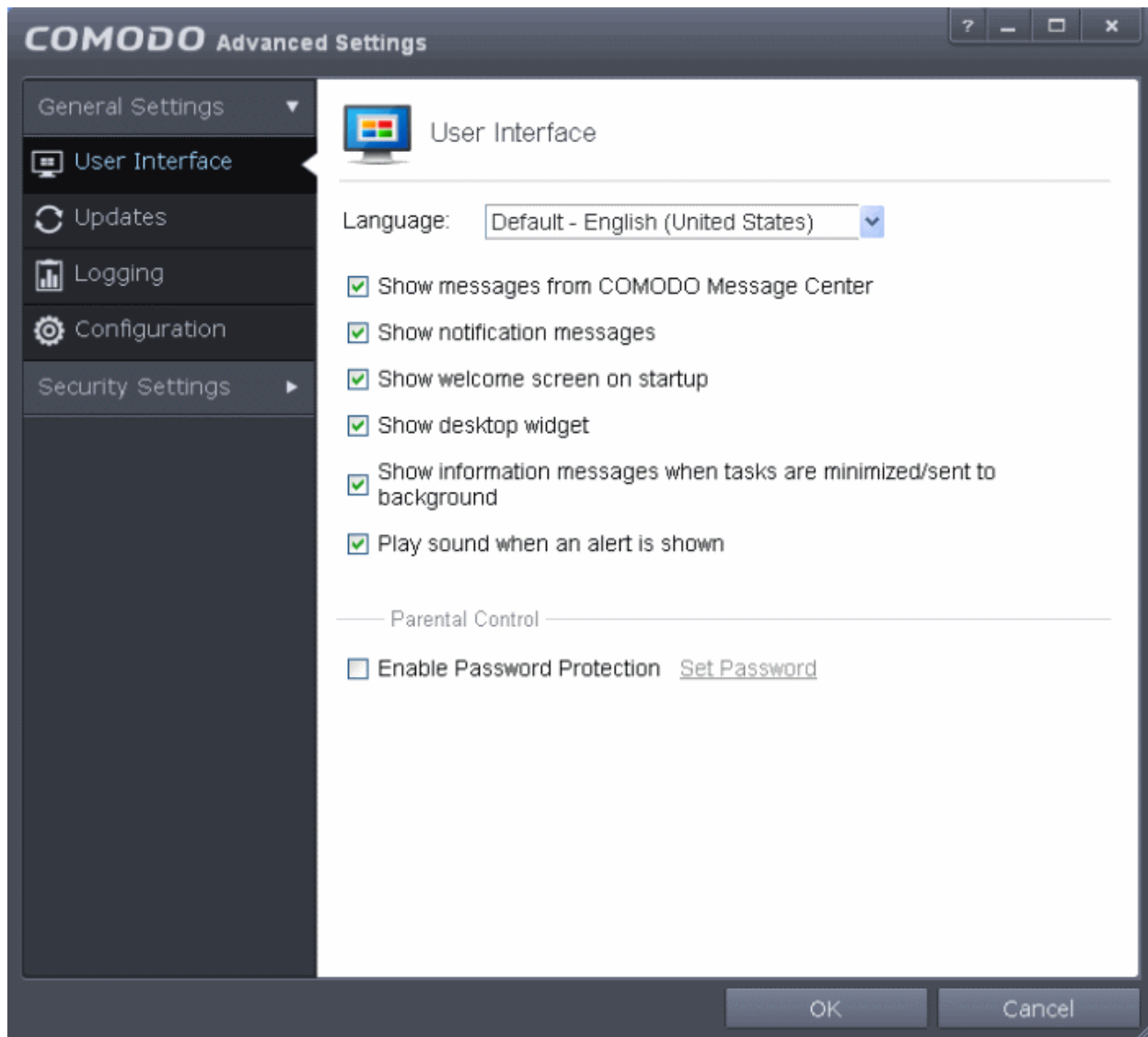
The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Internet Security. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced 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:

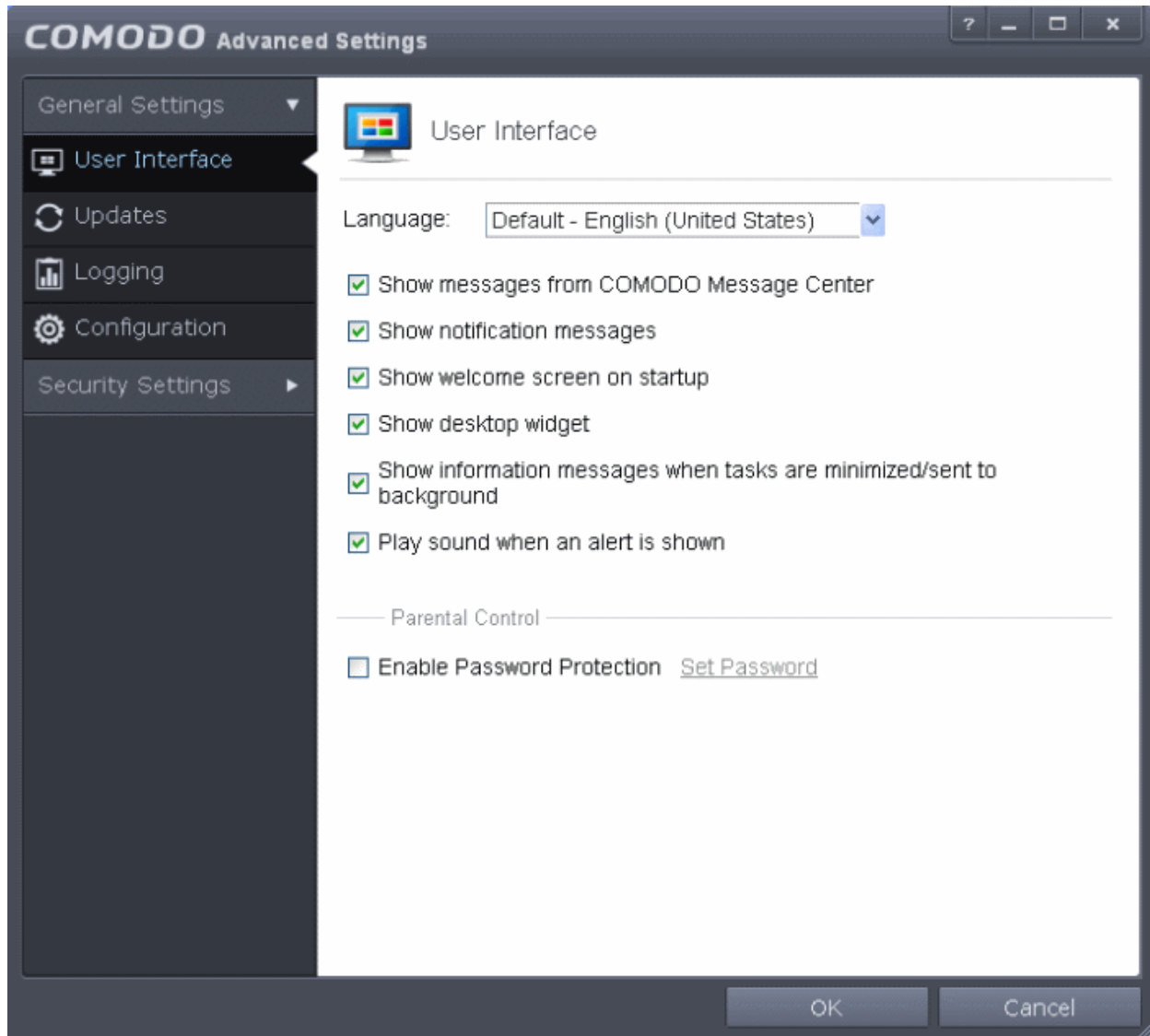


Please click the following links to find out more about each section:

- **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.

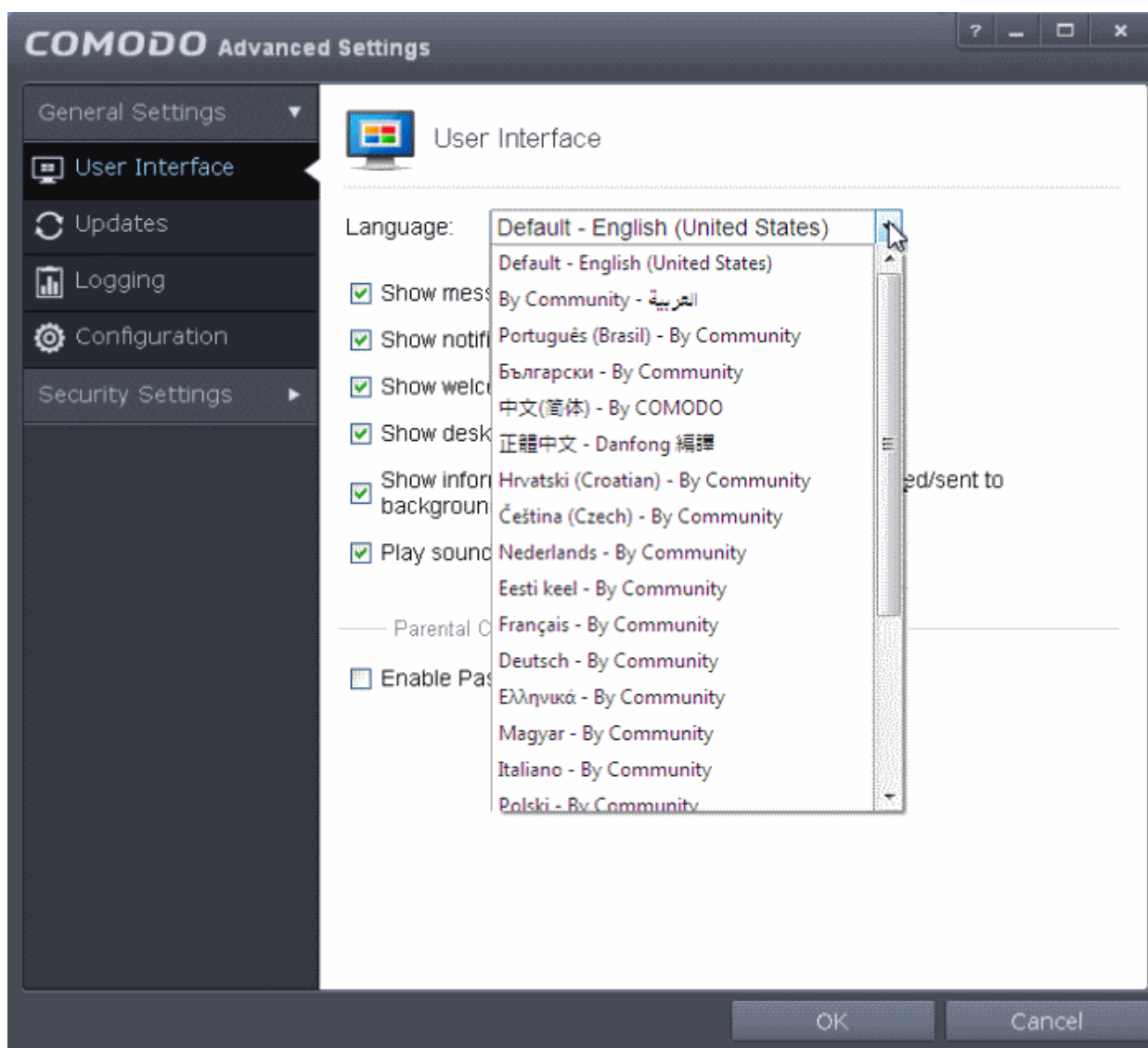


The category has the following sections:

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

6.1.1. Customize User Interface

The 'User Interface' tab lets you choose the interface language and customize the look and feel of Comodo Internet Security according to your preferences. You can also configure how messages are displayed and enable password protection for your settings.



- **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.

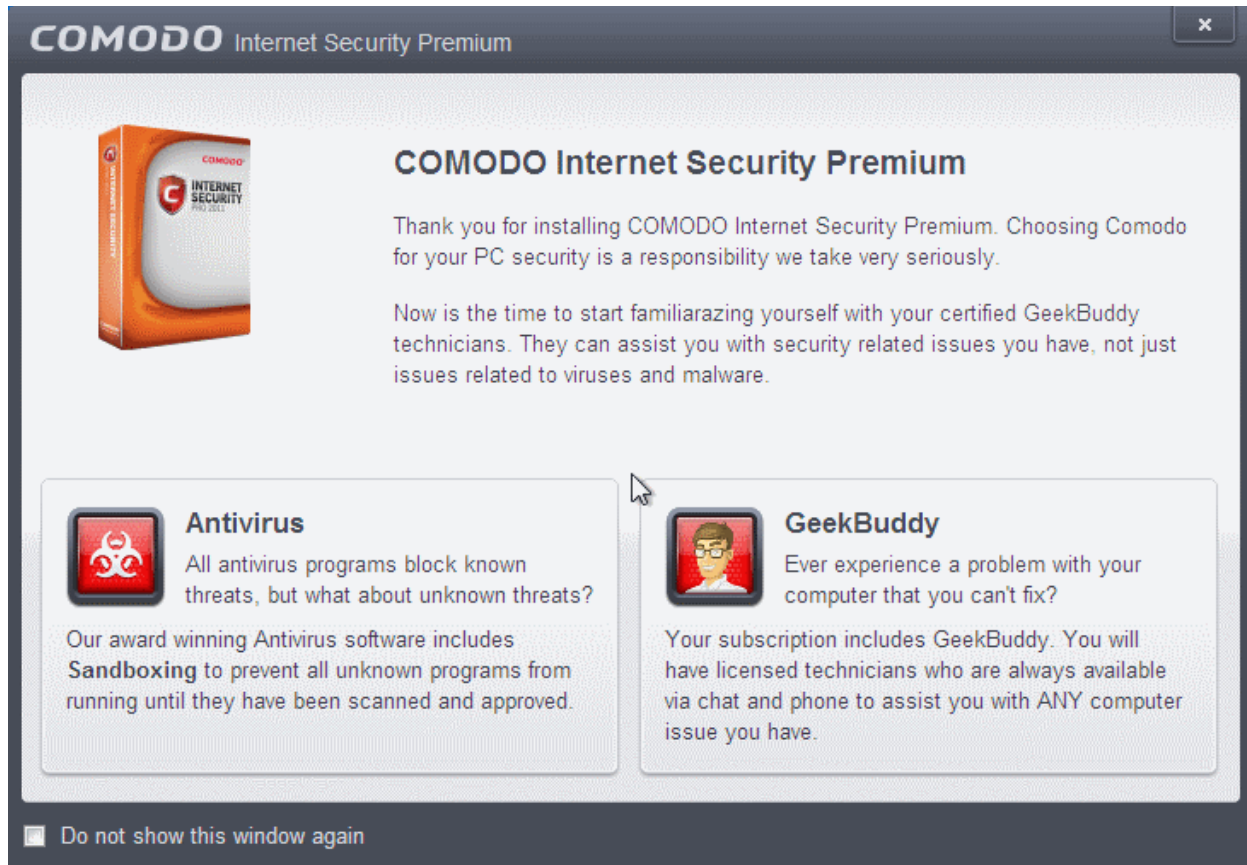


They contain news about product updates, occasional requests for feedback, info about other Comodo products you may be interested to try and other general news. (*Default = Enabled*).

- **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

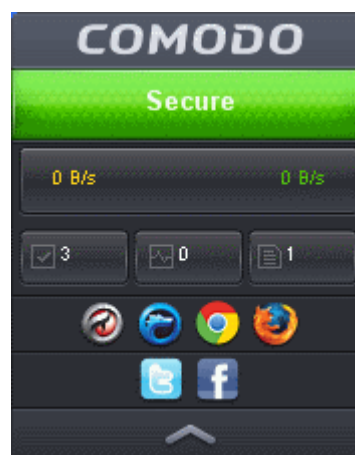
activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in **Antivirus > Real-time Scan settings** screen. Clear this check box if you do not want to see these system messages (*Default = 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.

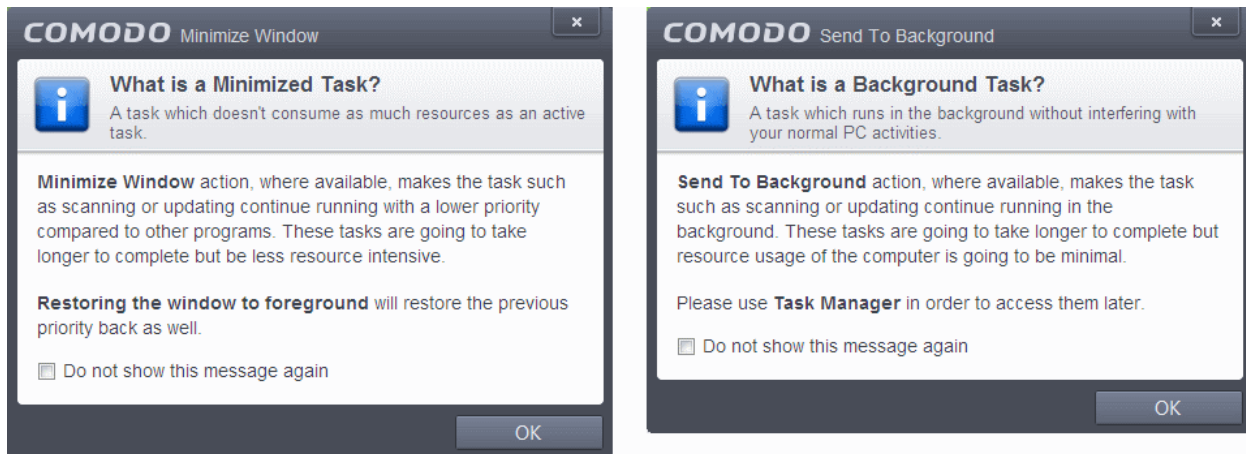


The widget also acts as a shortcut to open the CIS main interface, the Task Manager, your browsers and so on. If you do not want the widget to be displayed on your desktop, clear this checkbox. (*Default = Enabled*).

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*).

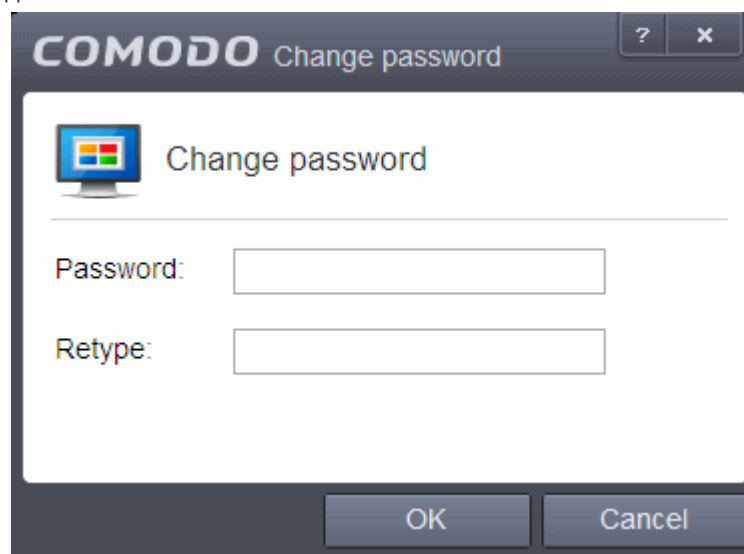
Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **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*)
- **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.



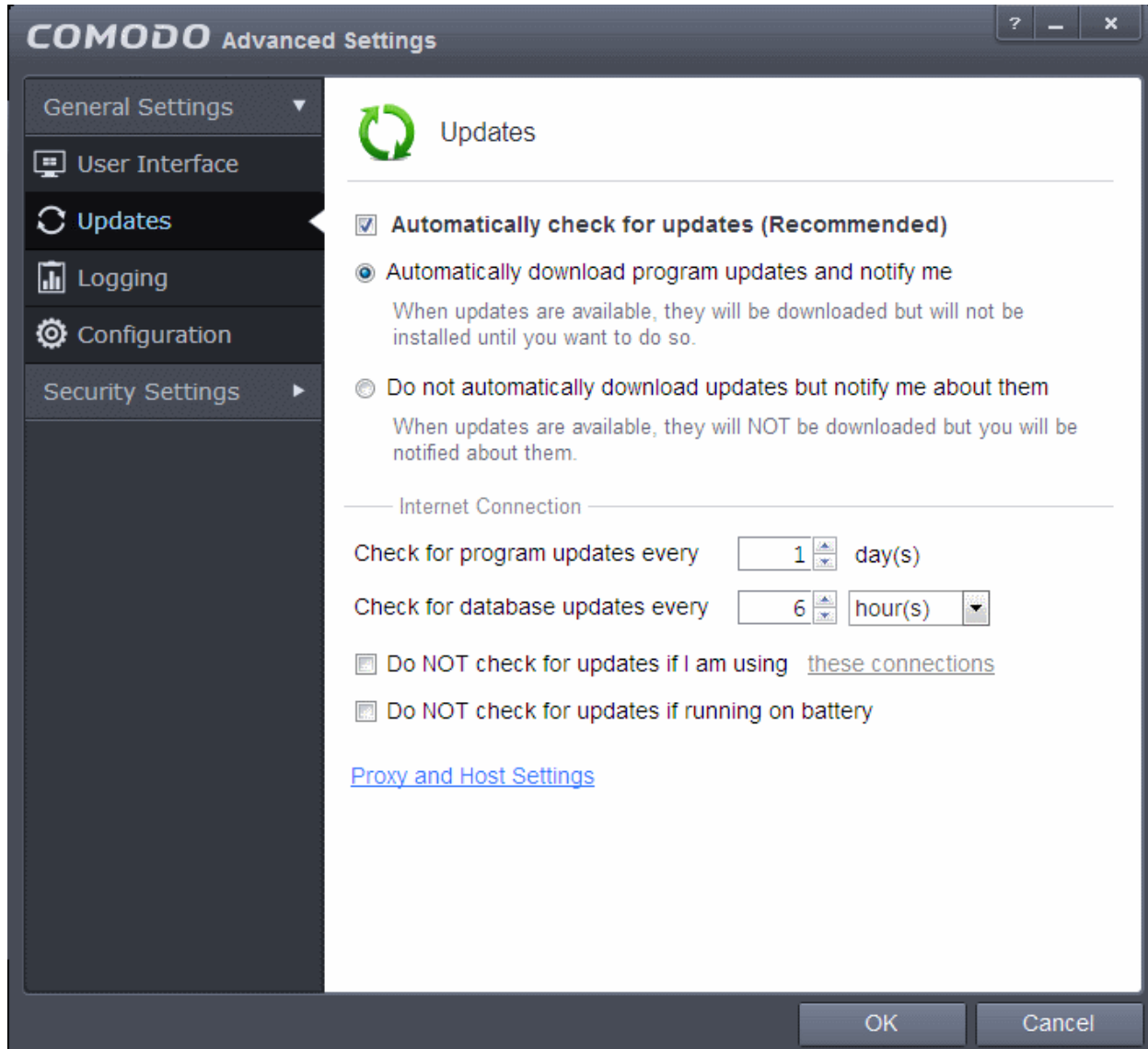
- Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by

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':

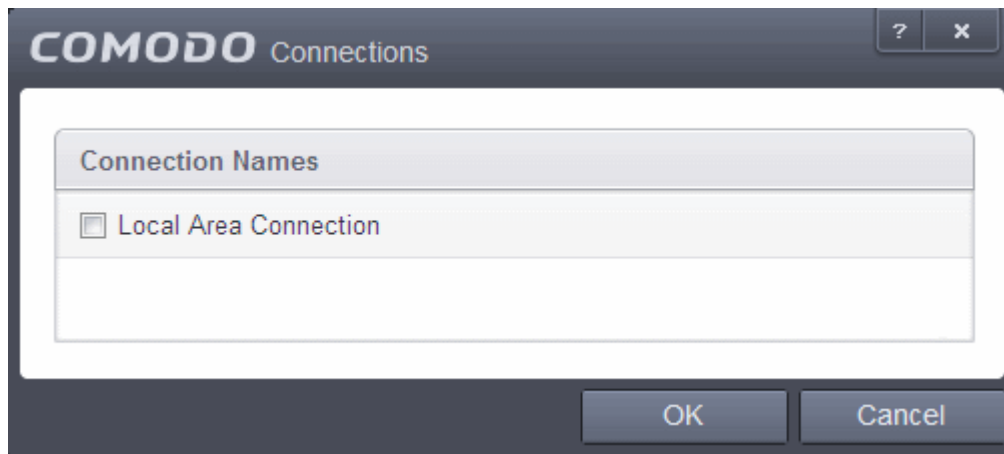


- **Automatically check for updates** - If this option is enabled, CIS automatically checks for program and database updates at the intervals shown further down this interface. You can also specify which servers and connections to use for updates. Comodo recommends automatic update checks are left enabled to ensure your system enjoys maximum protection against the latest threats. (*Default=Enabled*)
 - **Automatically download program updates and notify me** - Instructs CIS to automatically download virus database updates as soon as they are available then notify you that they are ready for installation. (*Default=Enabled*)
 - **Do not automatically download updates but notify me about them** - Selecting this option means CIS will notify you when updates are available but will not download them until after your approval.
- **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*)
- **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.

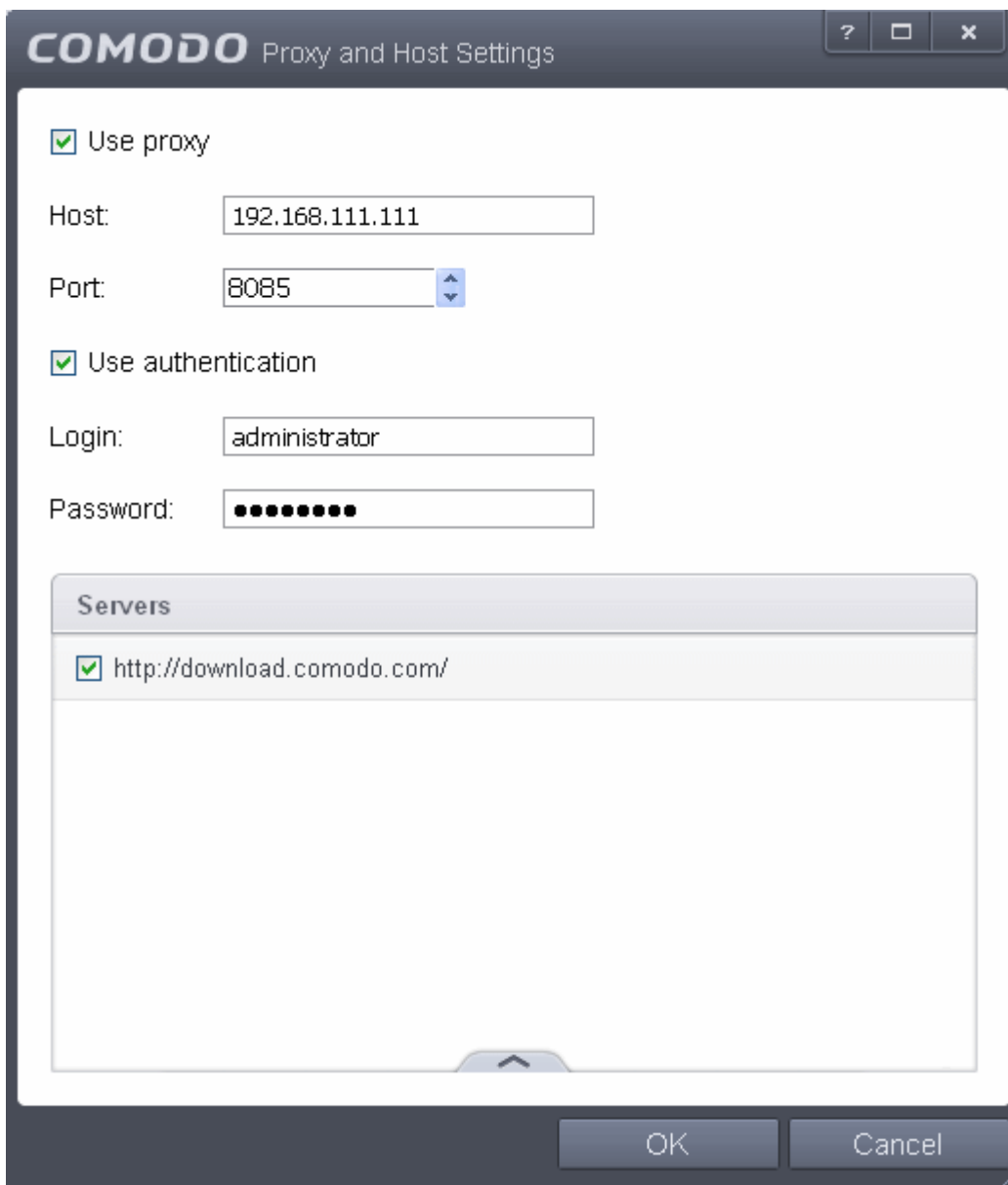


- Select the connection through which you do not want CIS to check for updates and click OK.
- **Do NOT check for updates if running on battery** - If enabled, CIS will not download updates if it detects your computer is running from battery power. This is intended to extend battery lifetime on laptops. (*Default = Disabled*)
- **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.

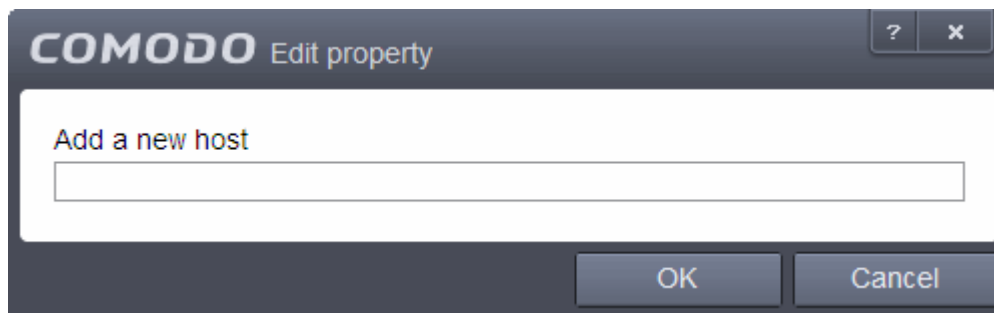
Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from <http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php>

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.



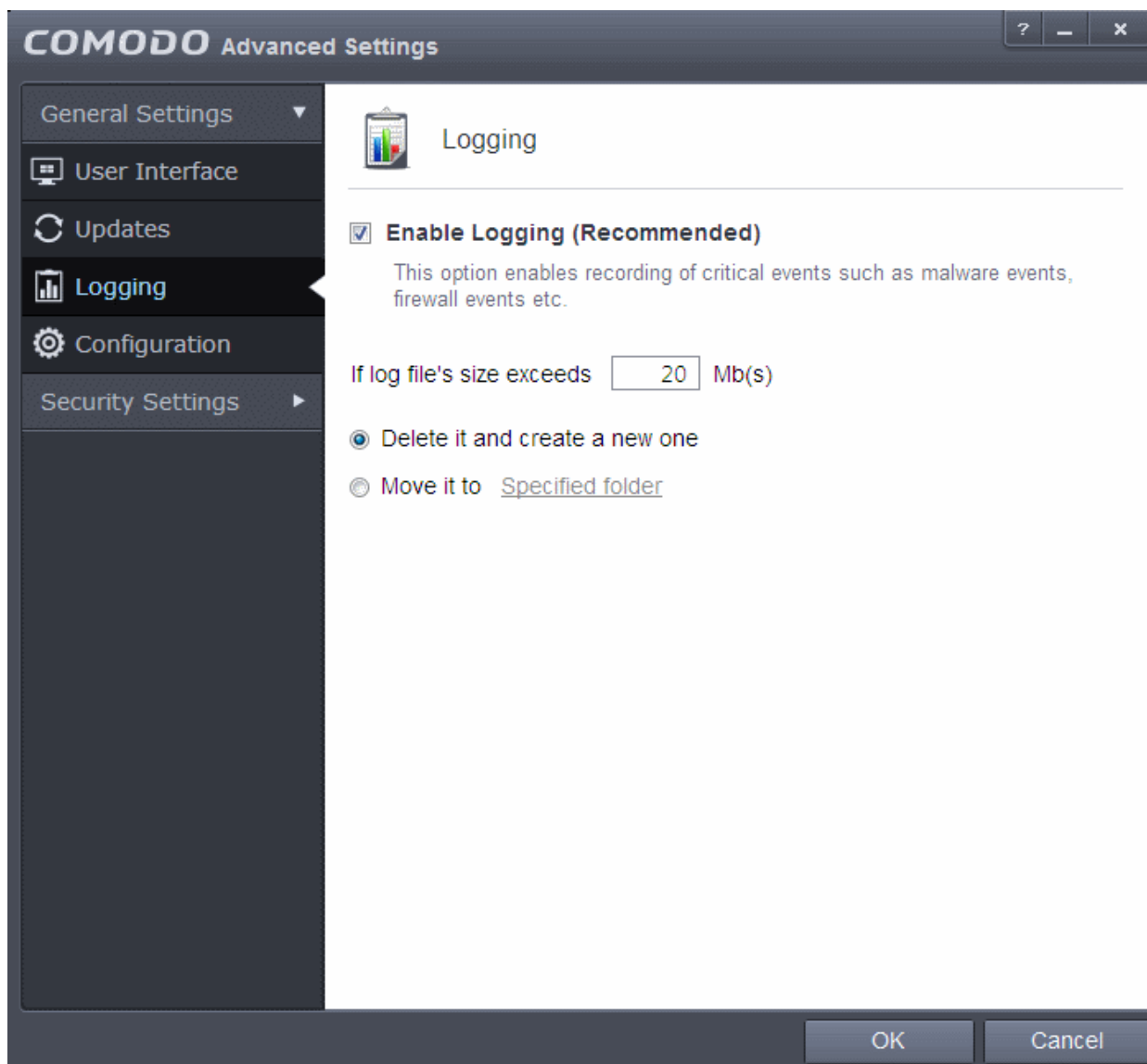
- If you specify multiple servers:
- Activate or deactivate each update server by selecting or deselecting the check-box alongside it
- Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CIS will commence downloading from the first server 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'.

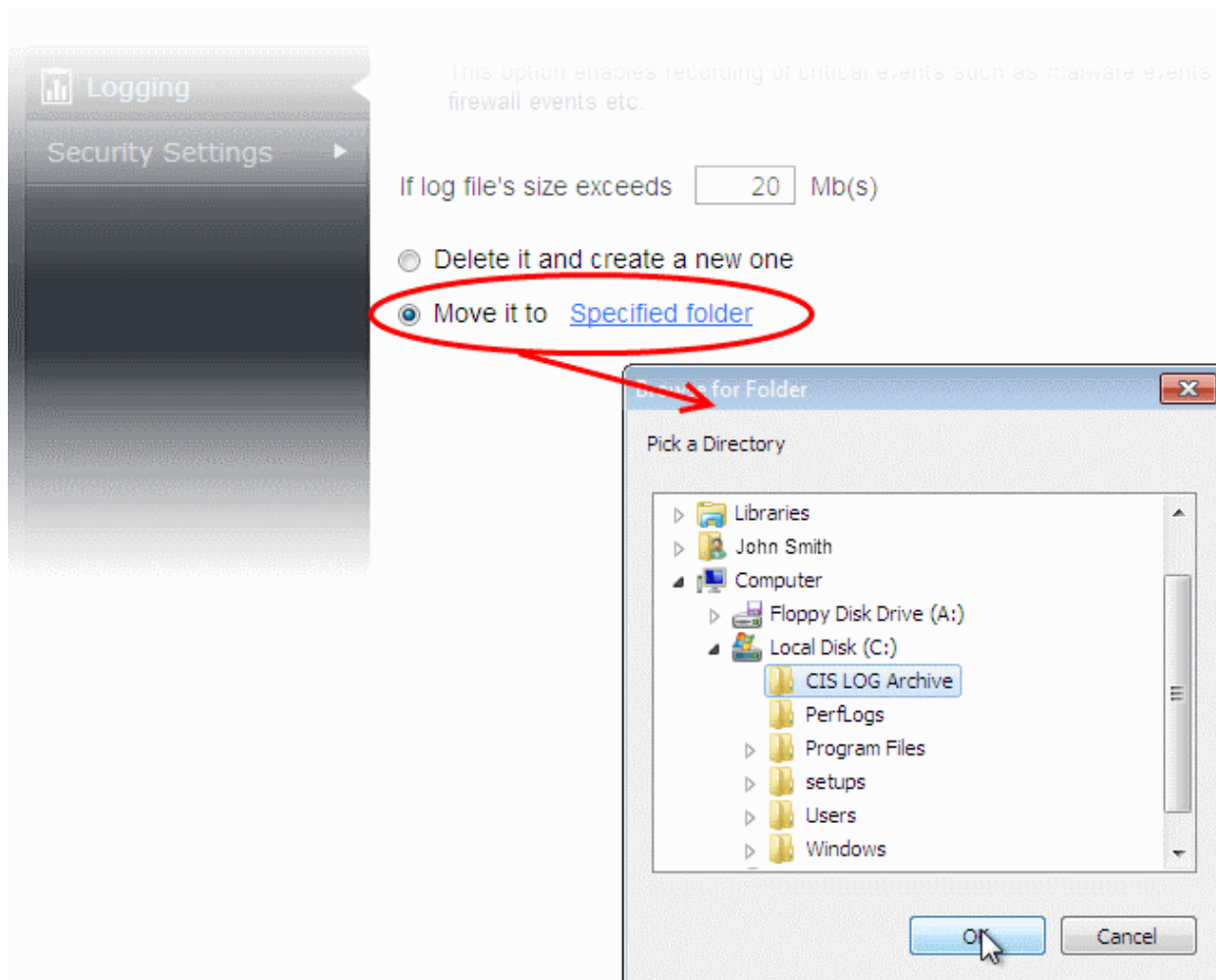
- This 'Logging' interface allows you to specify whether you want to enable logging; the maximum size of the log file and how CIS should react if the maximum file size is exceeded.
- Note: If you wish to actually view, manage and export logs, then you need to open the '**View Logs**' interface under 'General Settings' (Tasks > General Settings > View Logs)



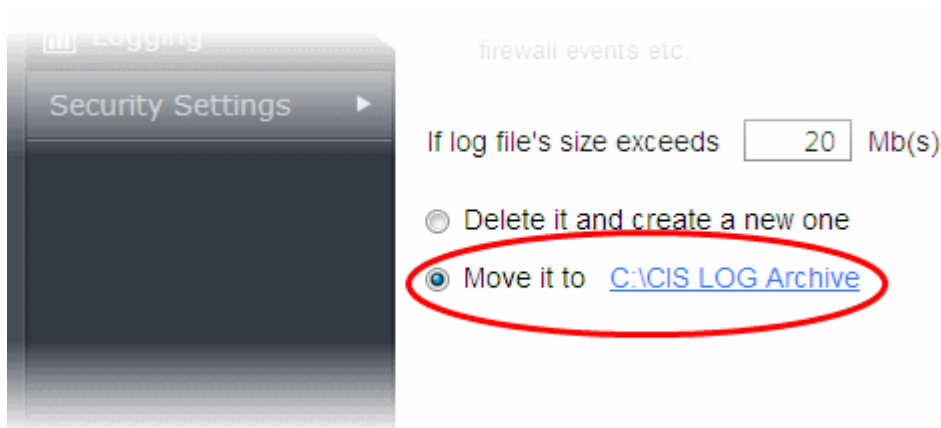
- **Enable Logging** - CIS logs events only if this setting is enabled. (*Default = Enabled*)
- **If the log file's size exceeds (Mb(s))** - Enables you to specify behavior when the log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending 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.

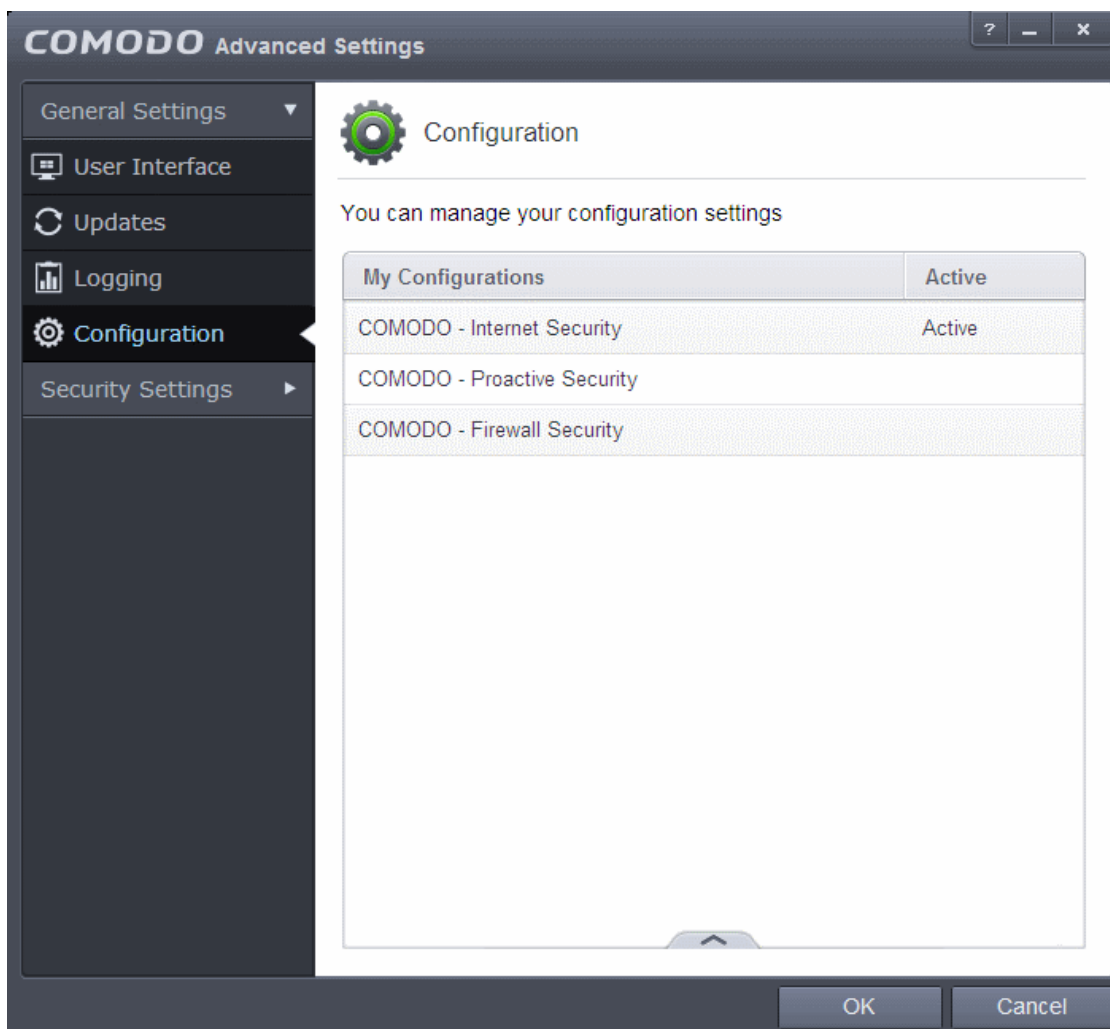
6.1.4. Manage CIS Configurations

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

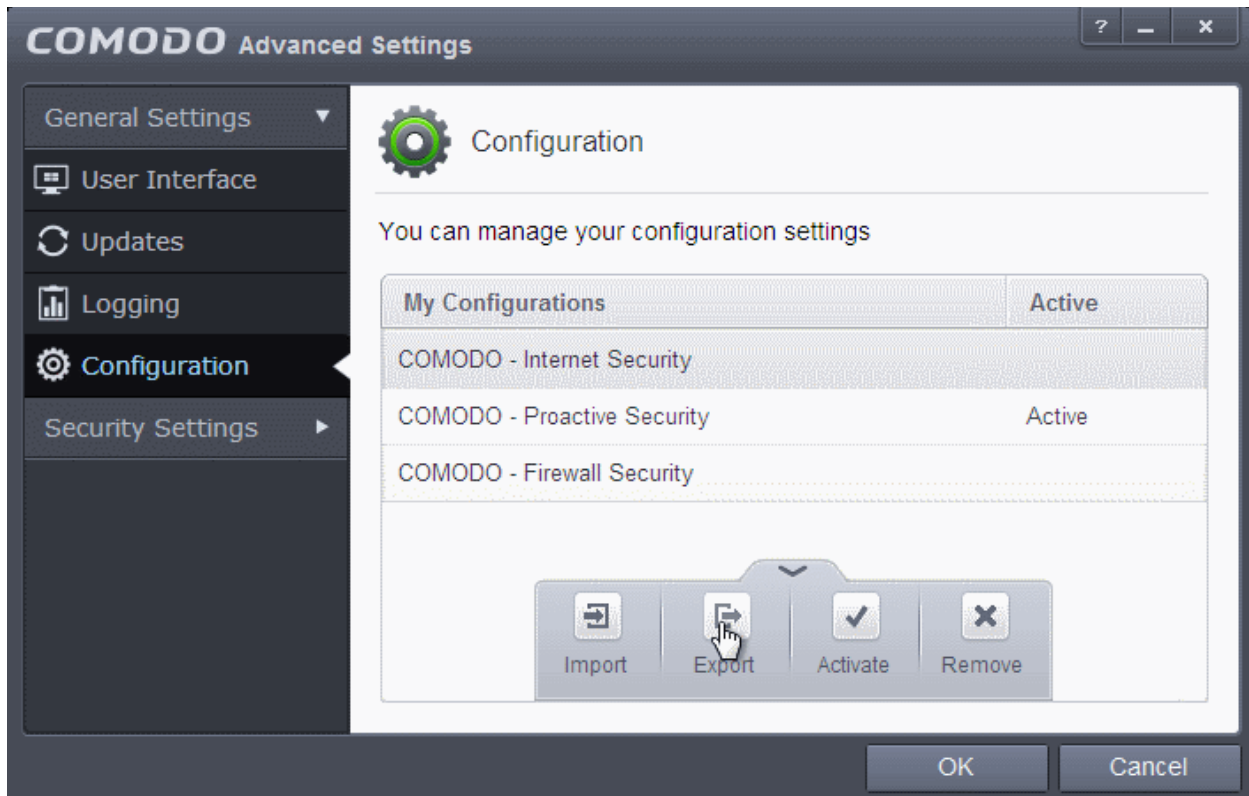
The CIS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Configuration' tab under 'General Settings' in 'Advanced Settings' interface.

Click the area on which you would like more information:

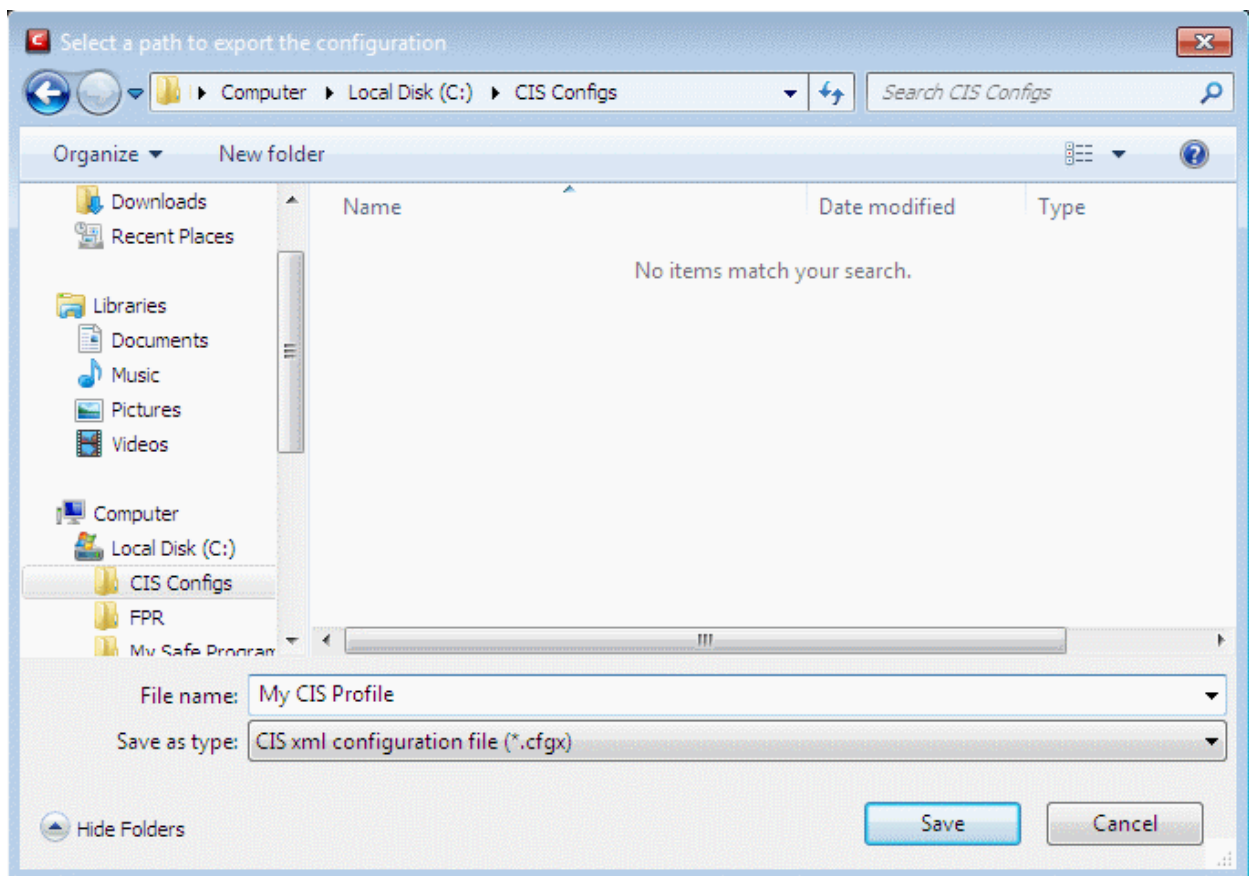
- **Export a stored configuration to a file**
- **Import a saved configuration from a file**
- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

Exporting a stored configuration to a file

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface

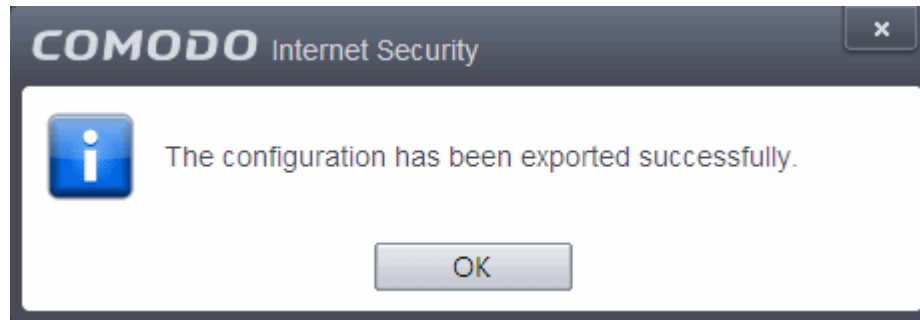


2. Select the configuration, click the up arrow from the bottom center and choose 'Export'. The Select a path to export the configuration dialog will open.



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.

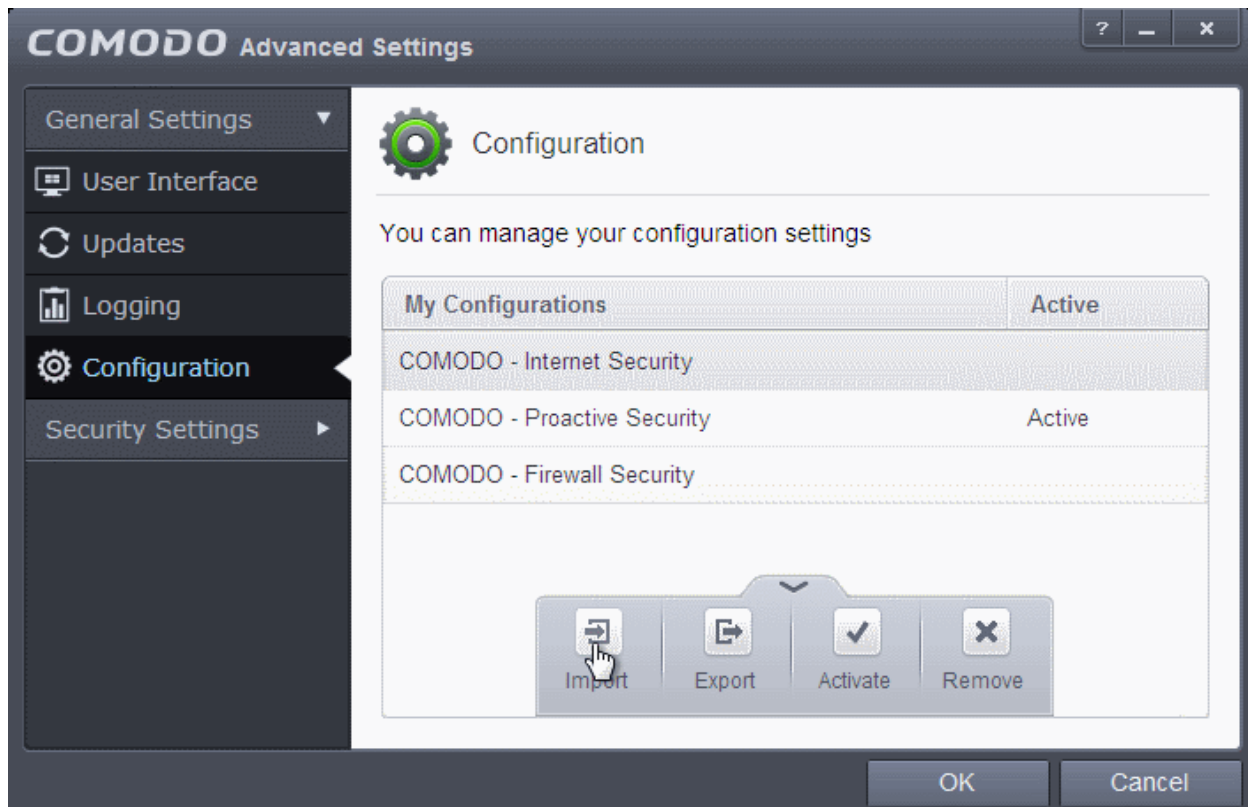


Importing a saved configuration from a file

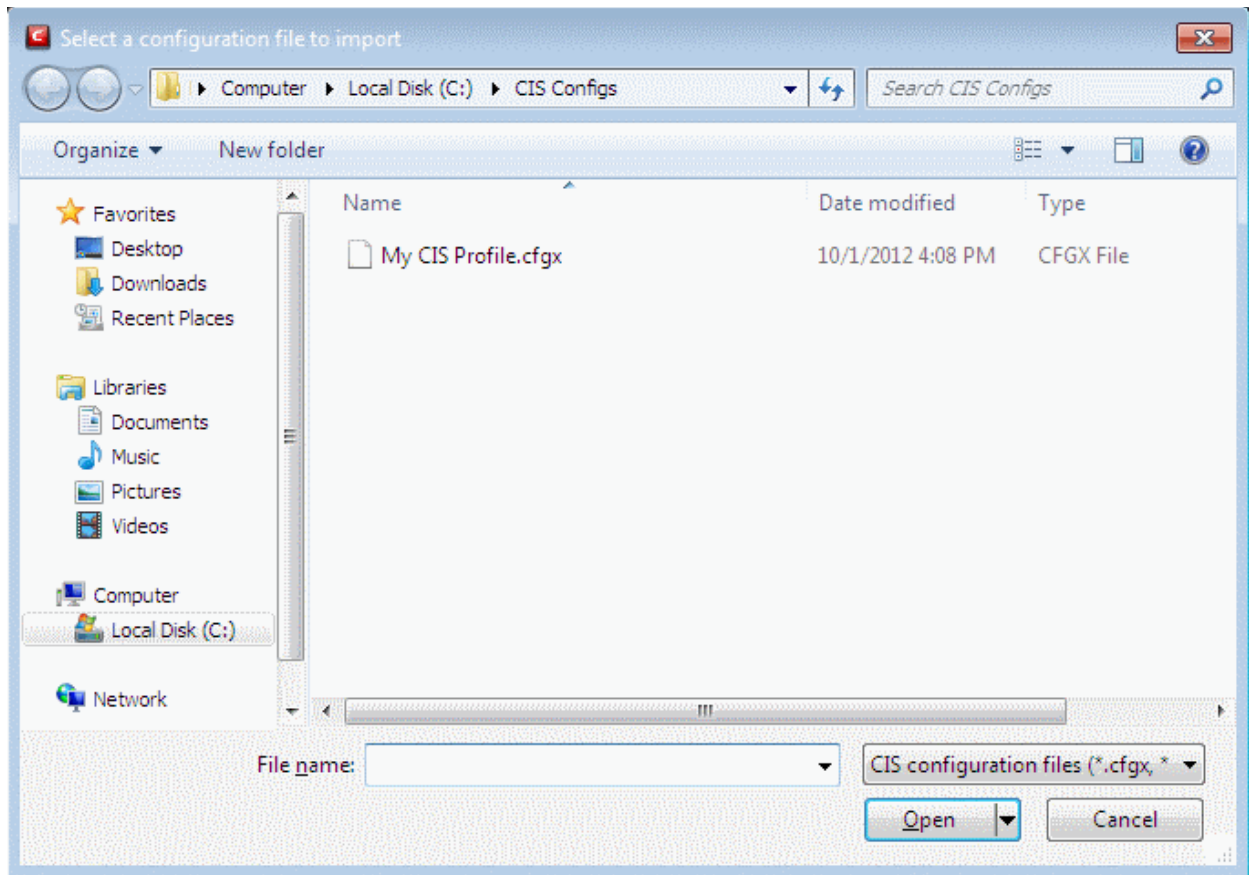
Importing a configuration profile allows you to store any profile within Comodo Internet Security. Any profiles you import do not become active until you **select them for use**.

To import a profile

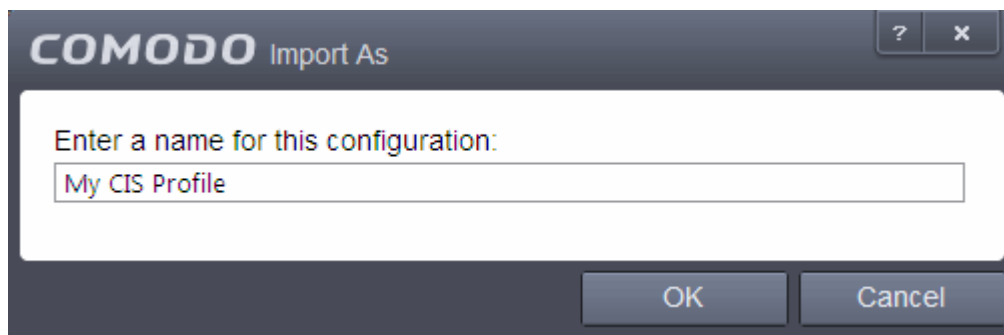
1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface, click the up arrow from the bottom center and choose Import from the options.



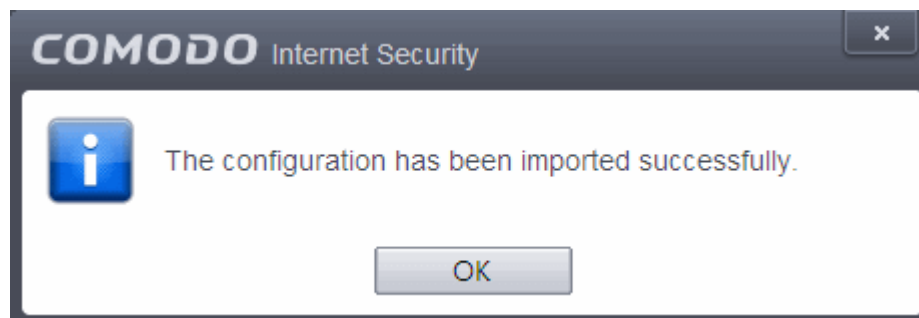
The 'Select a configuration file to import' dialog will open.



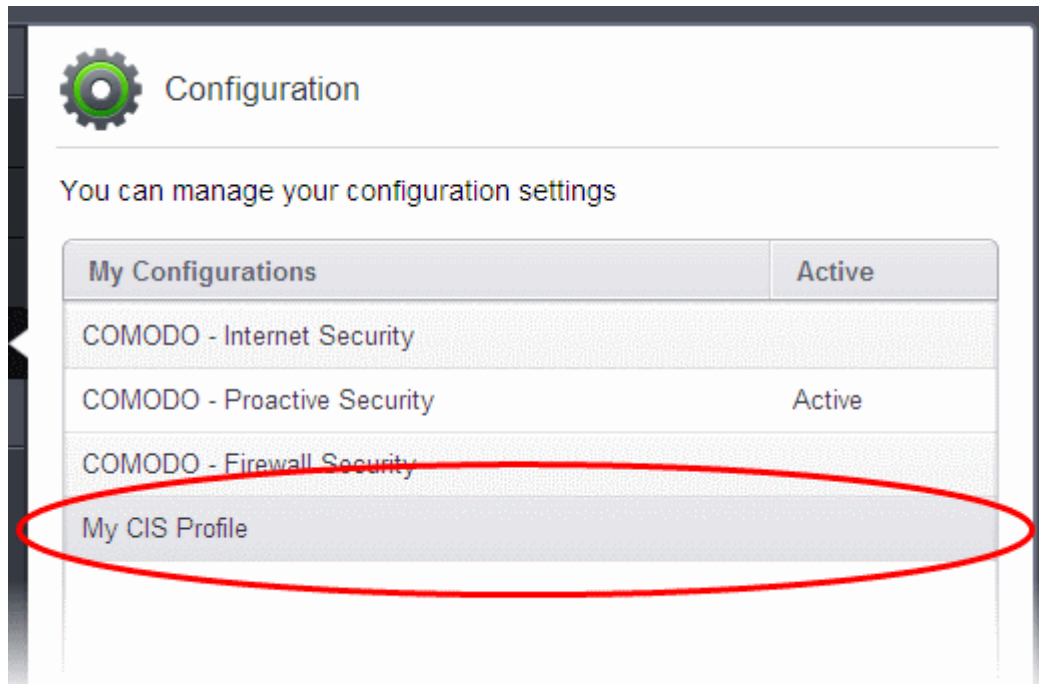
2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



A confirmation dialog will appear indicating the successful import of the profile.



Once imported, the configuration profile is available for deployment by **selecting it**.

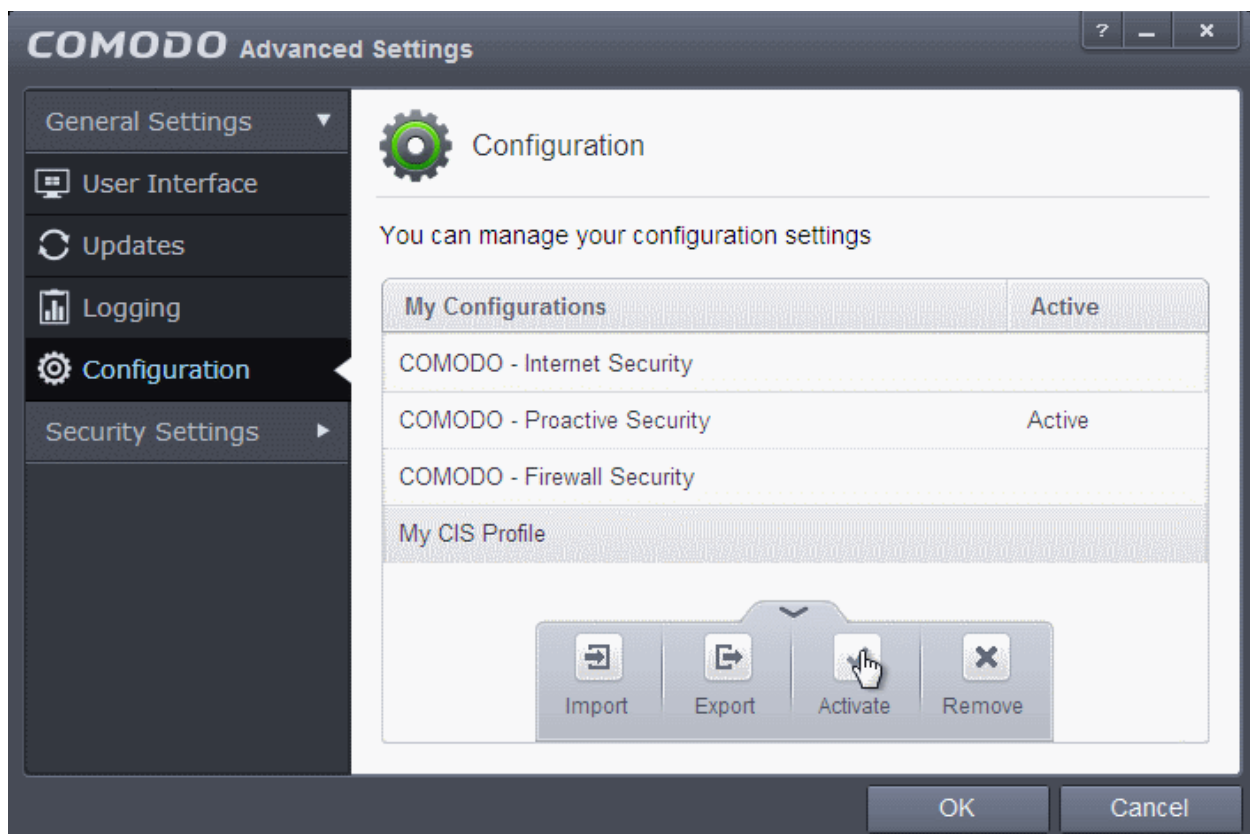


Selecting and Implementing a different configuration profile

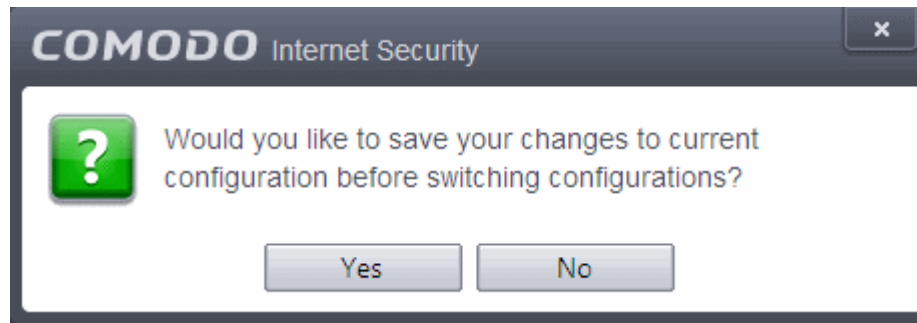
You can change the configuration profile active in CIS at any time from the 'Configurations' panel

To change the active configuration profile

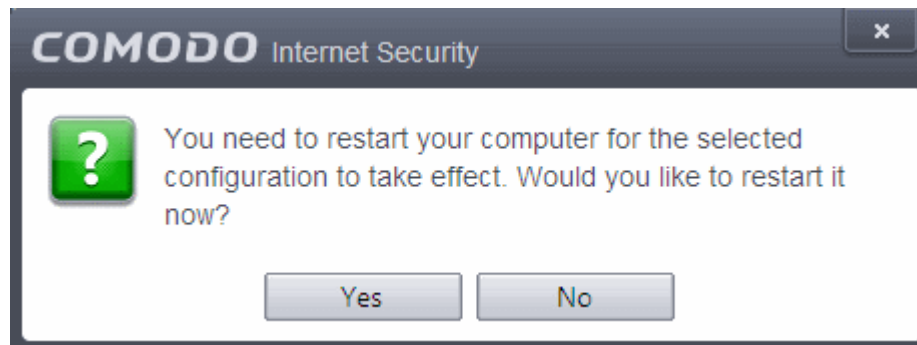
1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to activate, click the up arrow from the bottom center and choose Activate from the options.



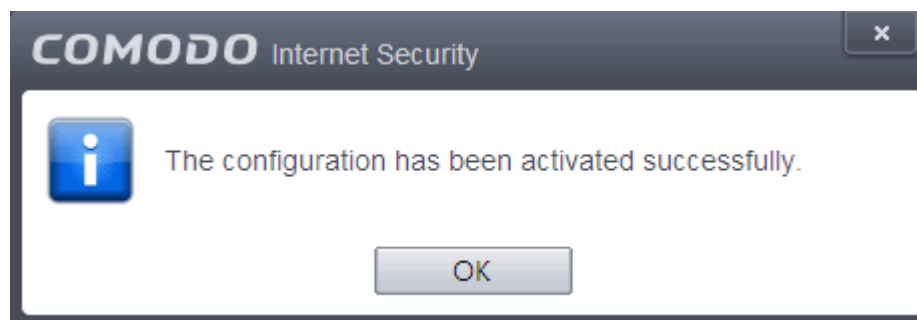
You will be prompted to save the changes to the settings in your current profile before the new profile is deployed.



3. if you choose to save the changes your computer should be restarted for the application of the new profile.



- Click Yes. Your computer will be restarted and the new configuration profile will be installed.
4. If you choose not to save the changes. The new profile will be implemented immediately and the confirmation dialog will be displayed.

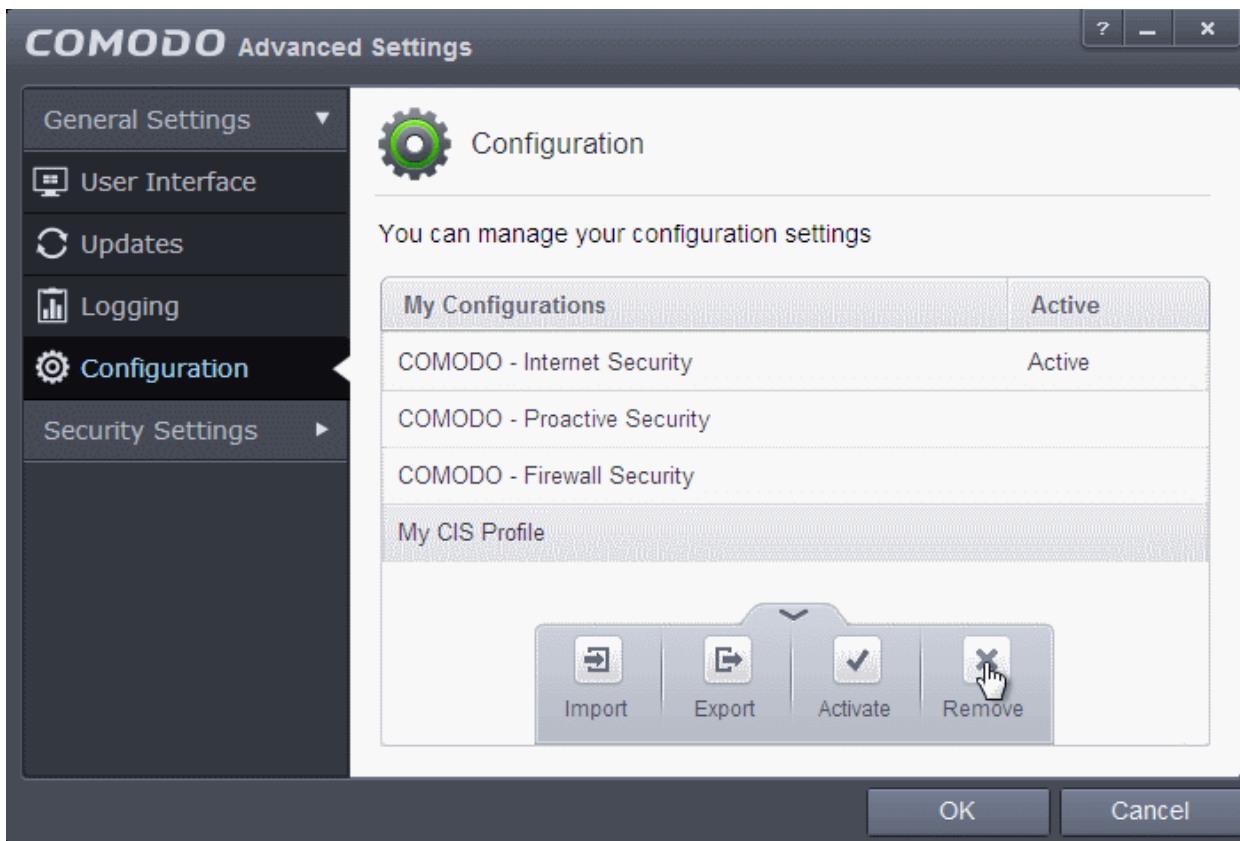


Deleting an inactive configuration profile

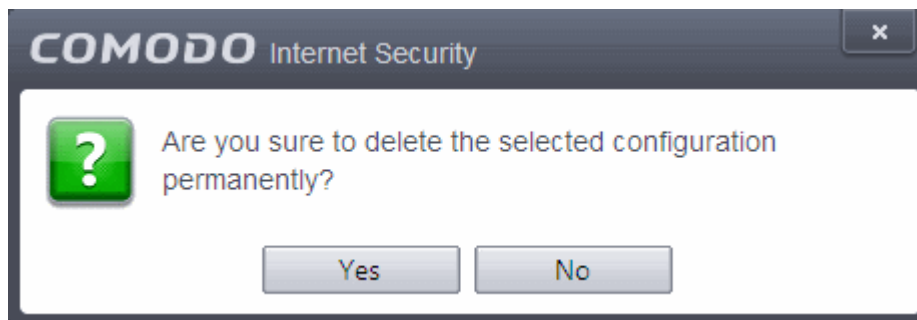
You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that Comodo Internet Security is currently using - only the inactive ones. For example if the COMODO - Internet Security is the active profile, you can only delete the inactive profiles, 'COMODO - Proactive Security', 'My_CIS_Configuration' and so on.

To remove an unwanted profile

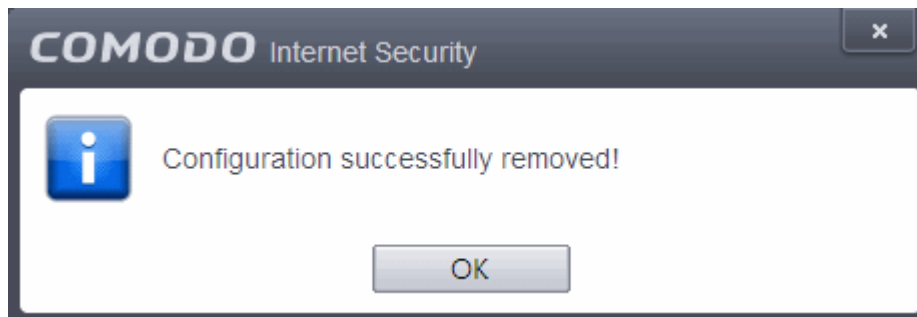
1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to delete, click the up arrow from the bottom center and choose Remove from the options.



A confirmation dialog will be displayed.



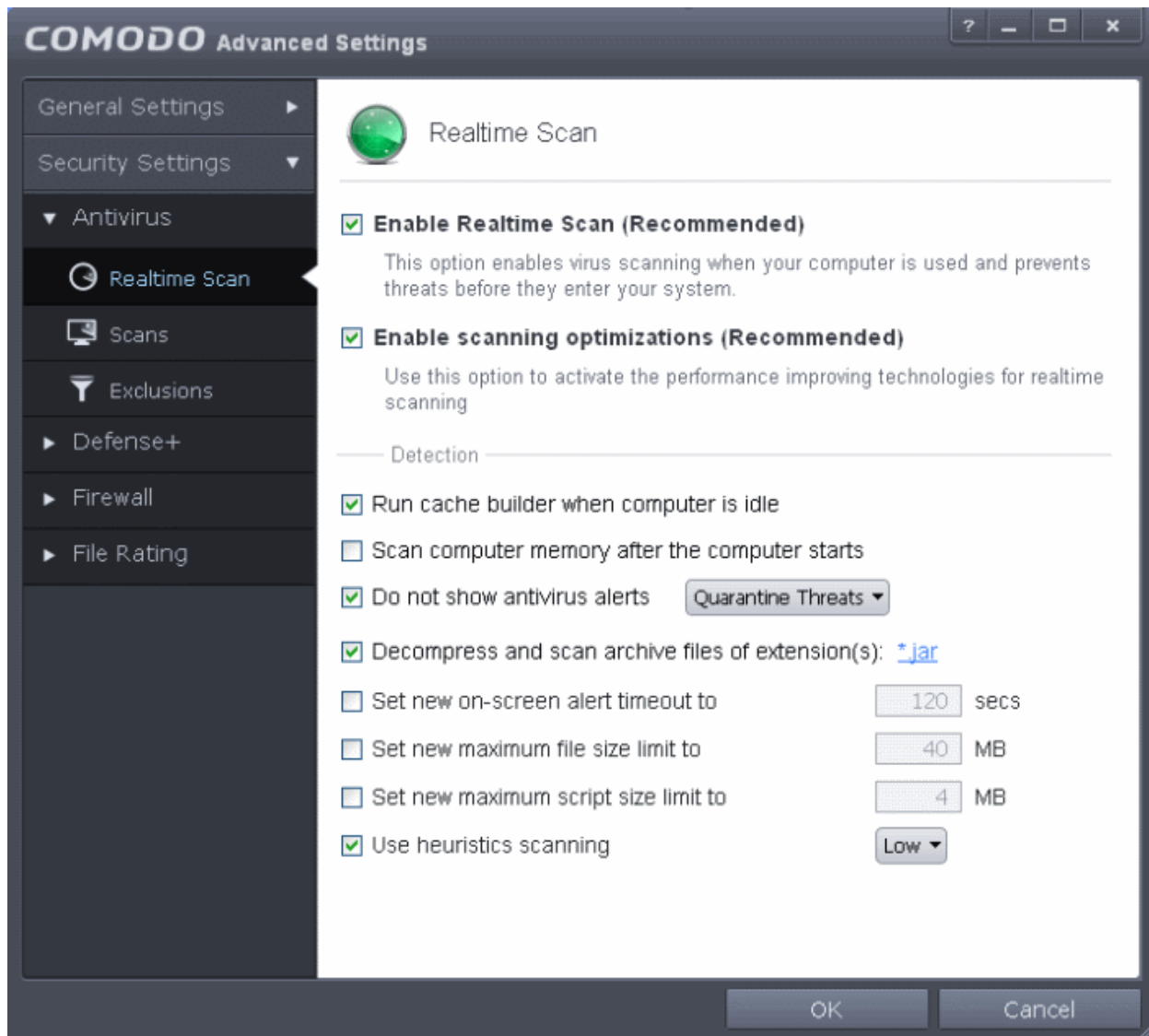
3. Click 'Yes'. The configuration profile will be deleted from your computer.



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 6.0 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 Behavior Settings**
 - **Active HIPS Rules**
 - **Predefined HIPS Rule Sets**
 - **Protected Files and Folders**
 - **Protected Registry Keys**
 - **Protected COM interfaces**
 - **Behavior Blocker**
 - **Sandbox Settings**
- **Firewall Settings**
 - **Firewall Behavior Settings**

- [Application Rules](#)
- [Global Rules](#)
- [Predefined Rule Sets](#)
- [Network Zones](#)
- [Port Sets](#)
- [Manage File Rating](#)
 - [File Rating Settings](#)
 - [Trusted Files](#)
 - [Unrecognized Files](#)
 - [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.

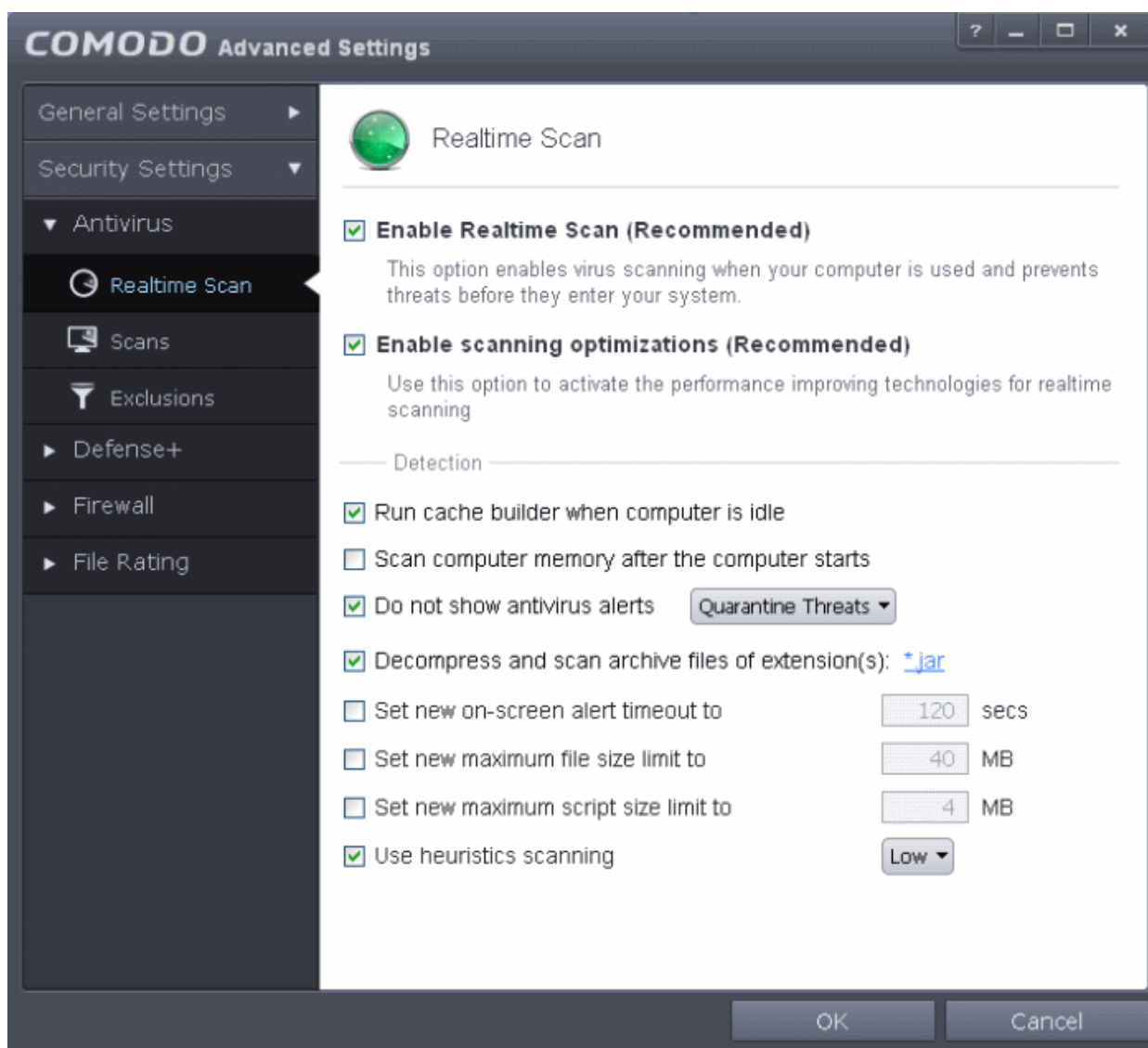
6.2.1.1. Real-time Scanner Settings

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*)

Detection Settings

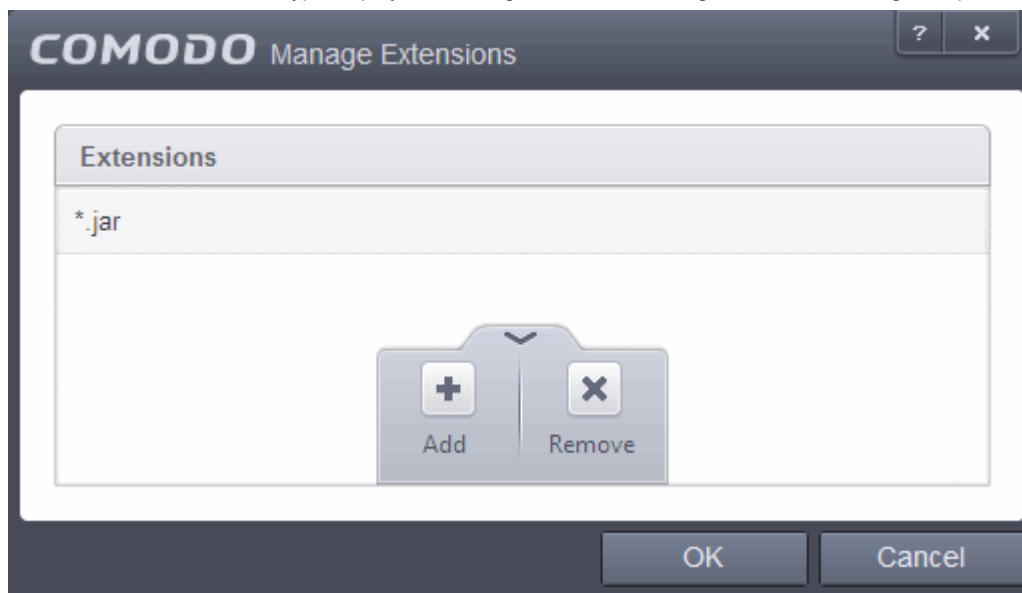
- **Run cache builder when computer is idle** - CIS runs the Antivirus Cache Builder whenever the computer is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (*Default = Enabled*).
- **Scan computer memory after the computer starts** - When this 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.

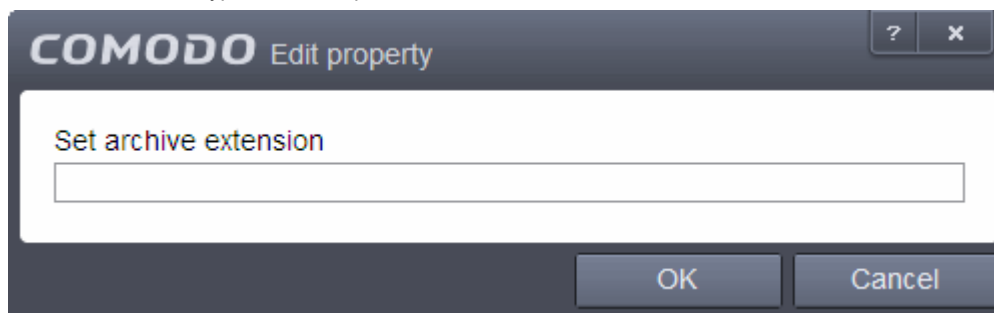
- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. (*Default = 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.



- 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 scanned. (*Default = 40 MB*)
- Set new maximum script size to - This box allows you to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (*Default = 4 MB*)
- **Use heuristics scanning** - Allows you to enable or disable Heuristics scanning and define scanning level. (*Default = 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.

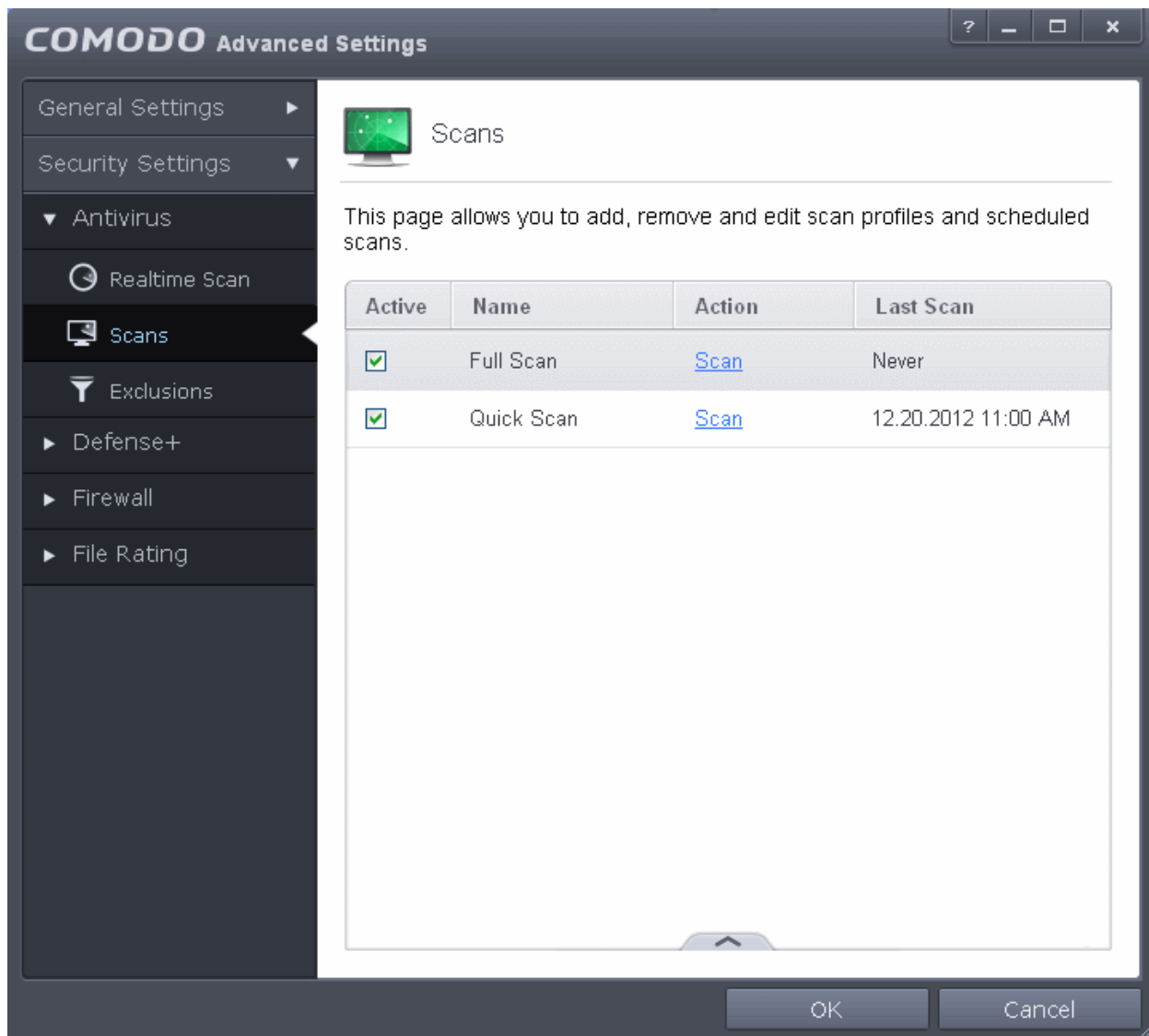
6.2.1.2. Scan Profiles

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.

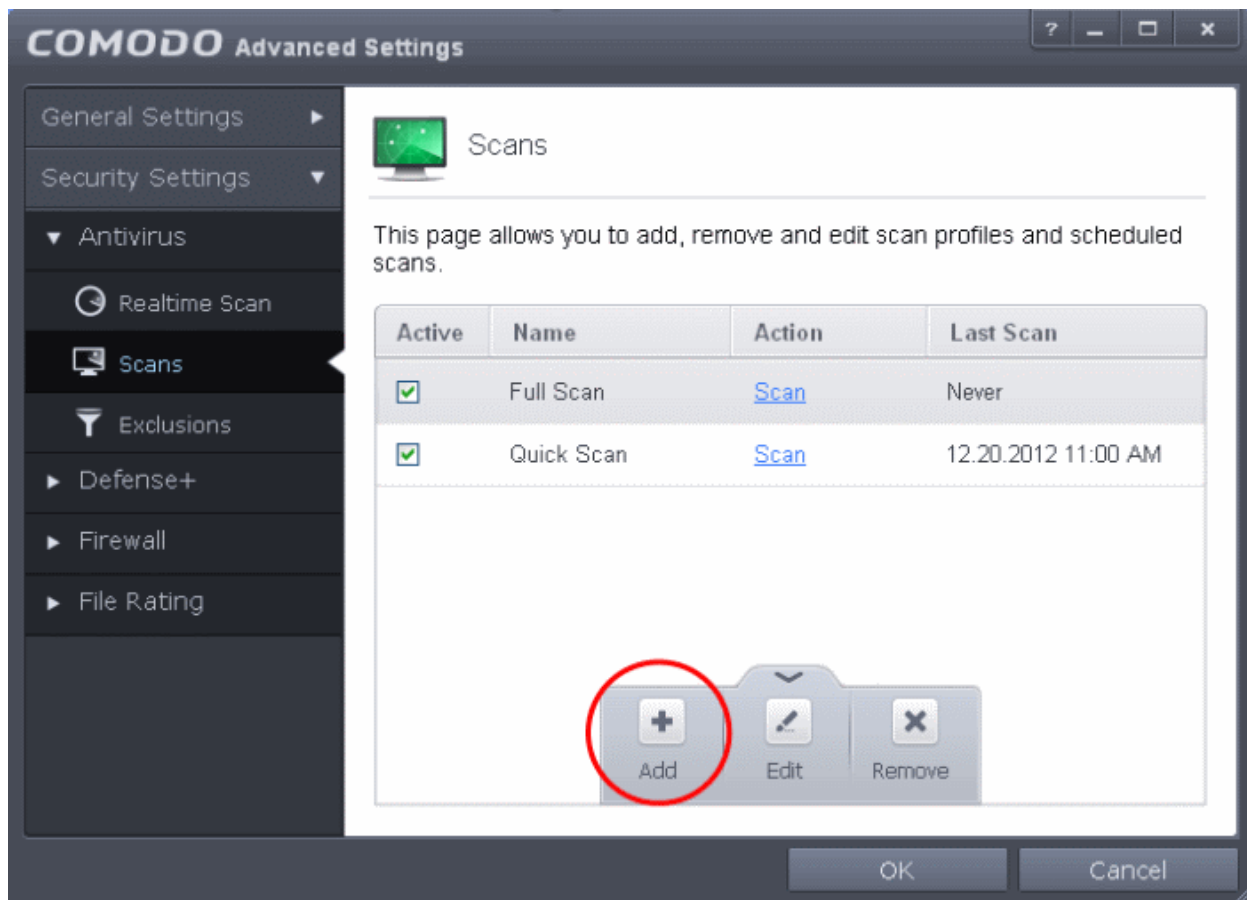
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

- [Creating a Scan Profile](#)
- [Running a custom scan](#)

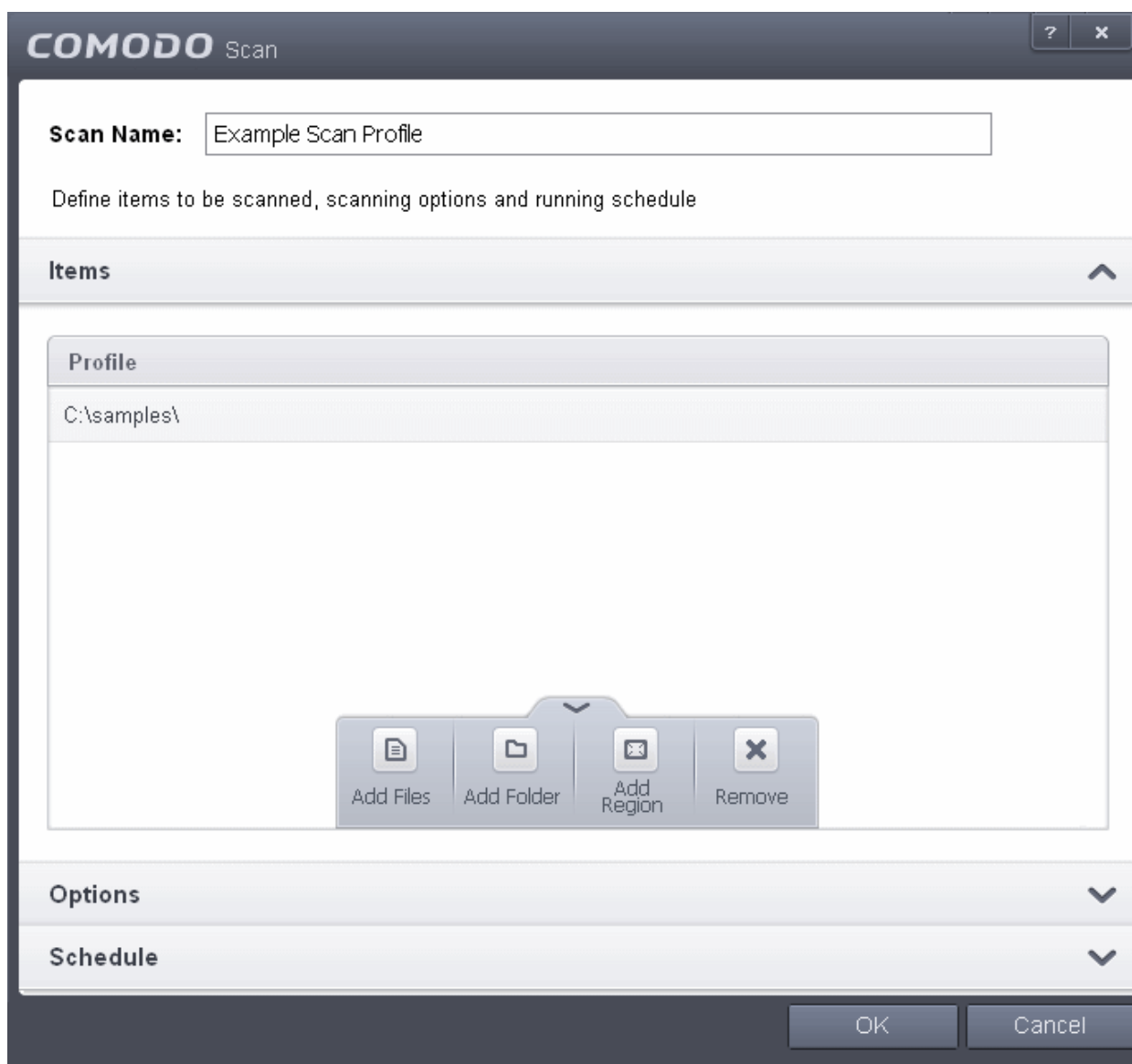
To create a custom profile

- Click the handle at the bottom of the interface then click the 'Add' button:

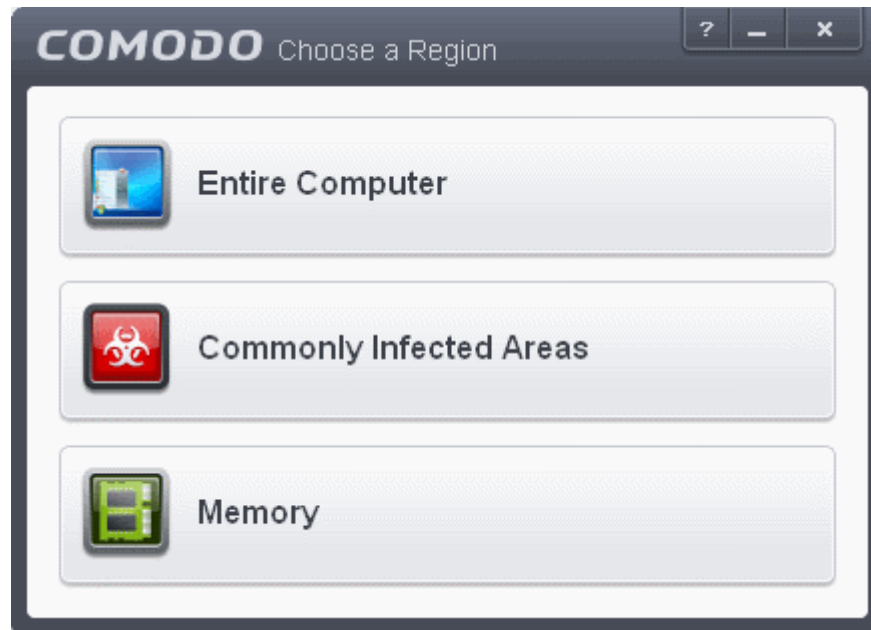


The scan profile interface will be displayed.

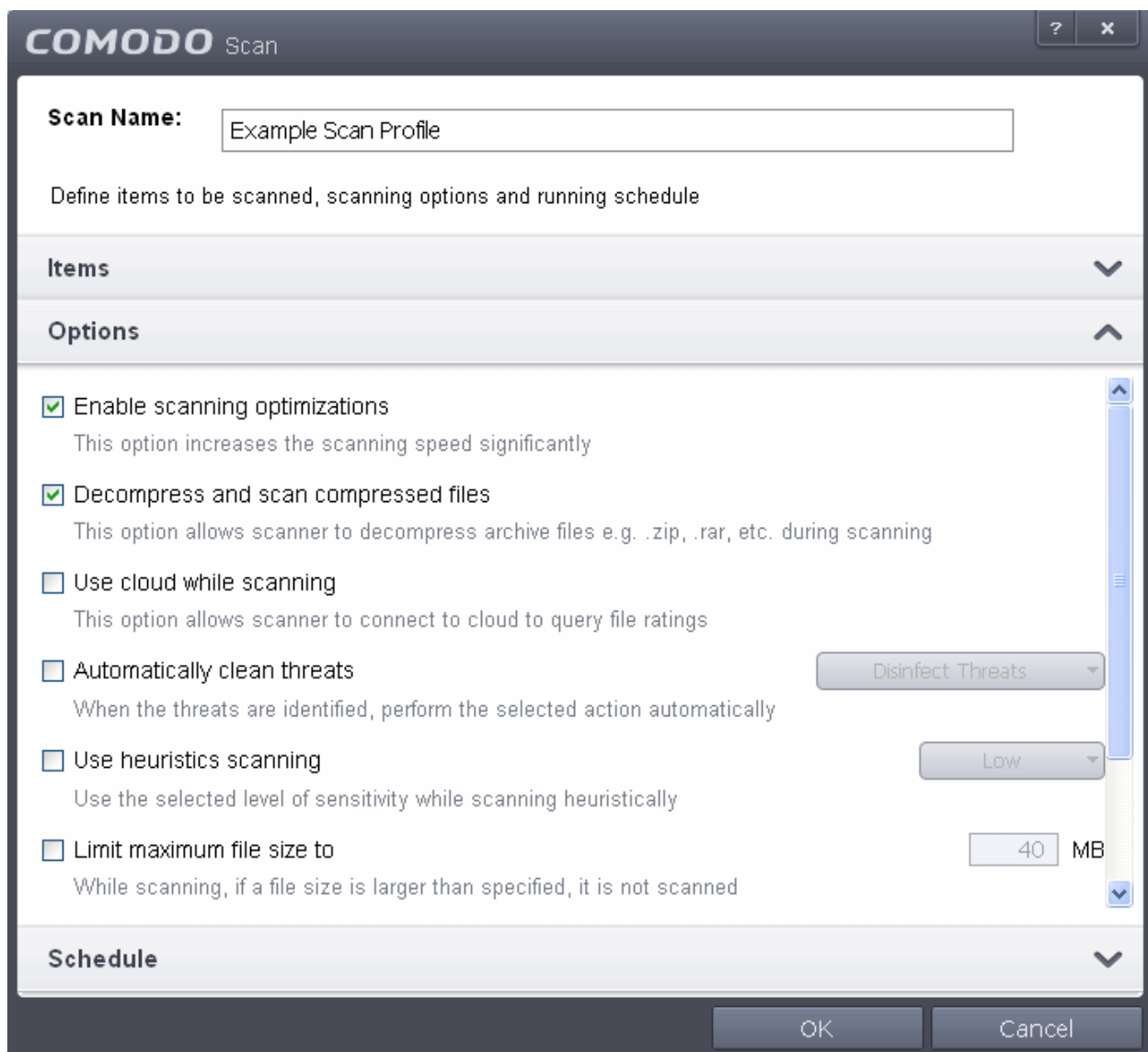
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items that should be included in the profile



- **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 and 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 = Disabled)*.
- If you want the scan to be performed periodically, set a Schedule for the custom scan by clicking 'Schedule'

COMODO Scan

Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Items ▼

Options ▼

Schedule ▲

Frequency:

Do not schedule this task

Every Day

Every Week

Every Month

Start Time: 5:30 AM

Day(s) of Week

Sun Mon Tue Wed Thu Fri Sat

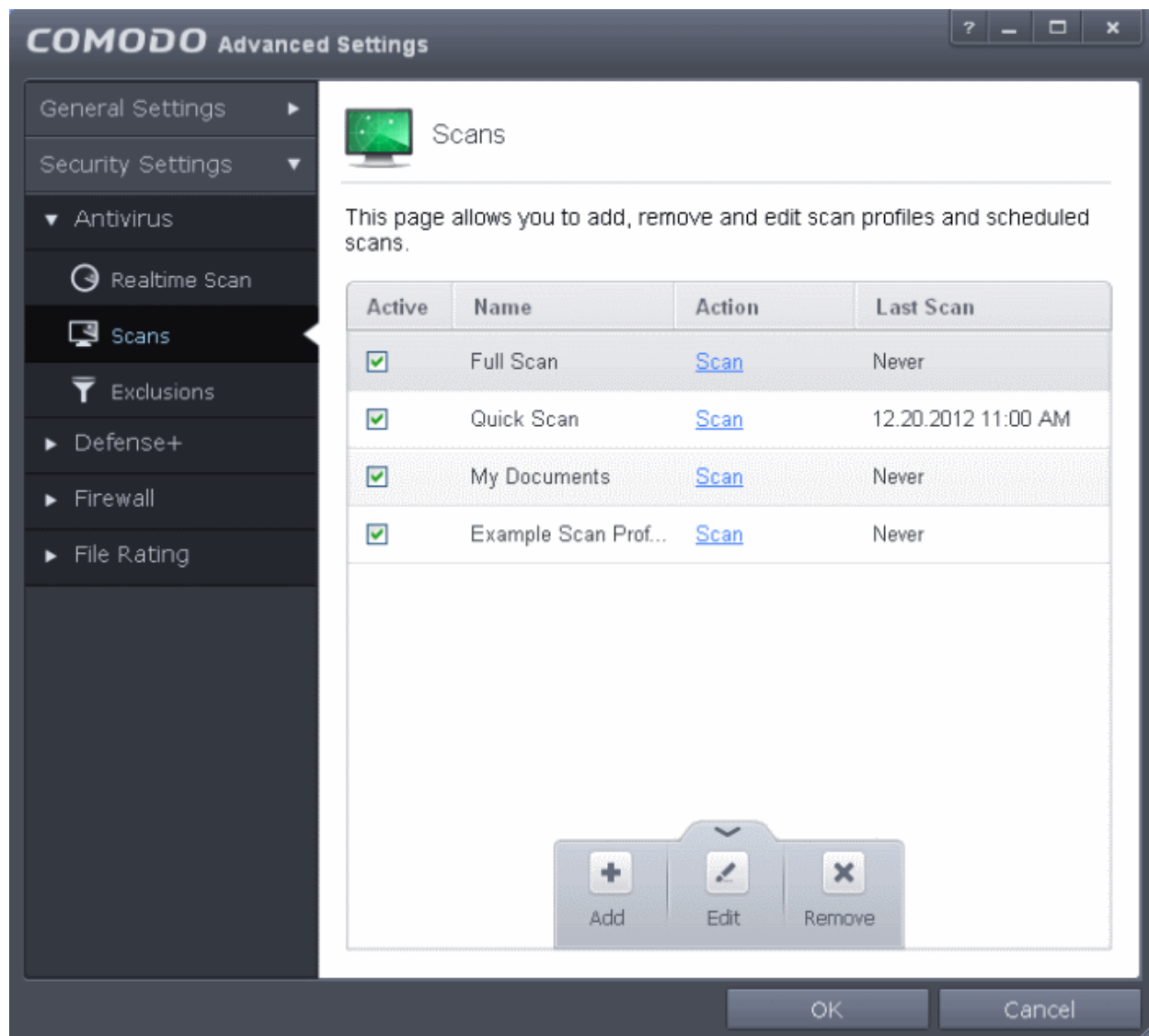
Run only when computer is not running on battery

Run only when computer is IDLE

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

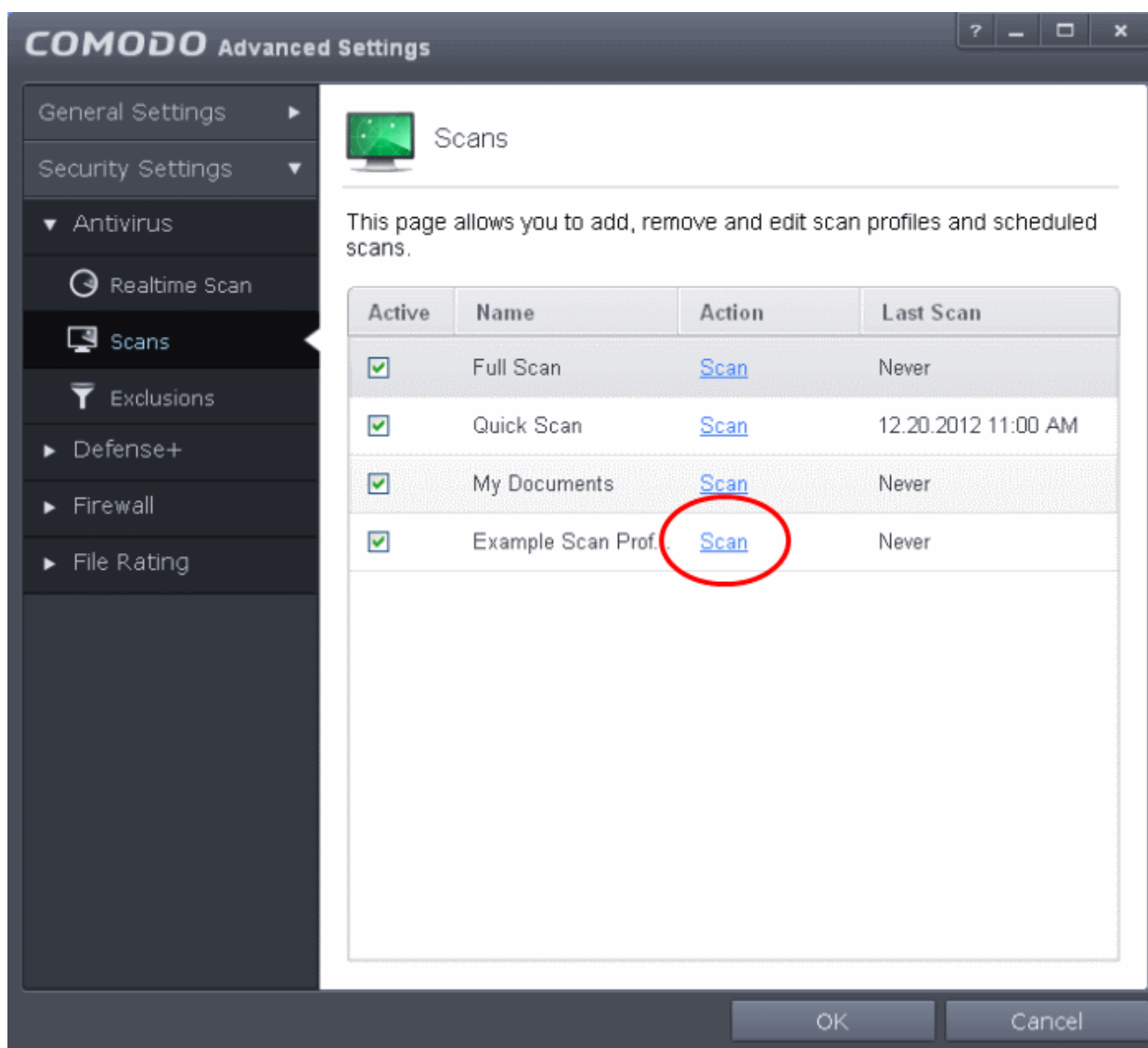
OK Cancel

- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - 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 adapter connected to mains supply and not on battery.
- **Run only when computer is IDLE** - Select this option if you do not want to be disturbed when involved in computer related activities. The scheduled scan 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.

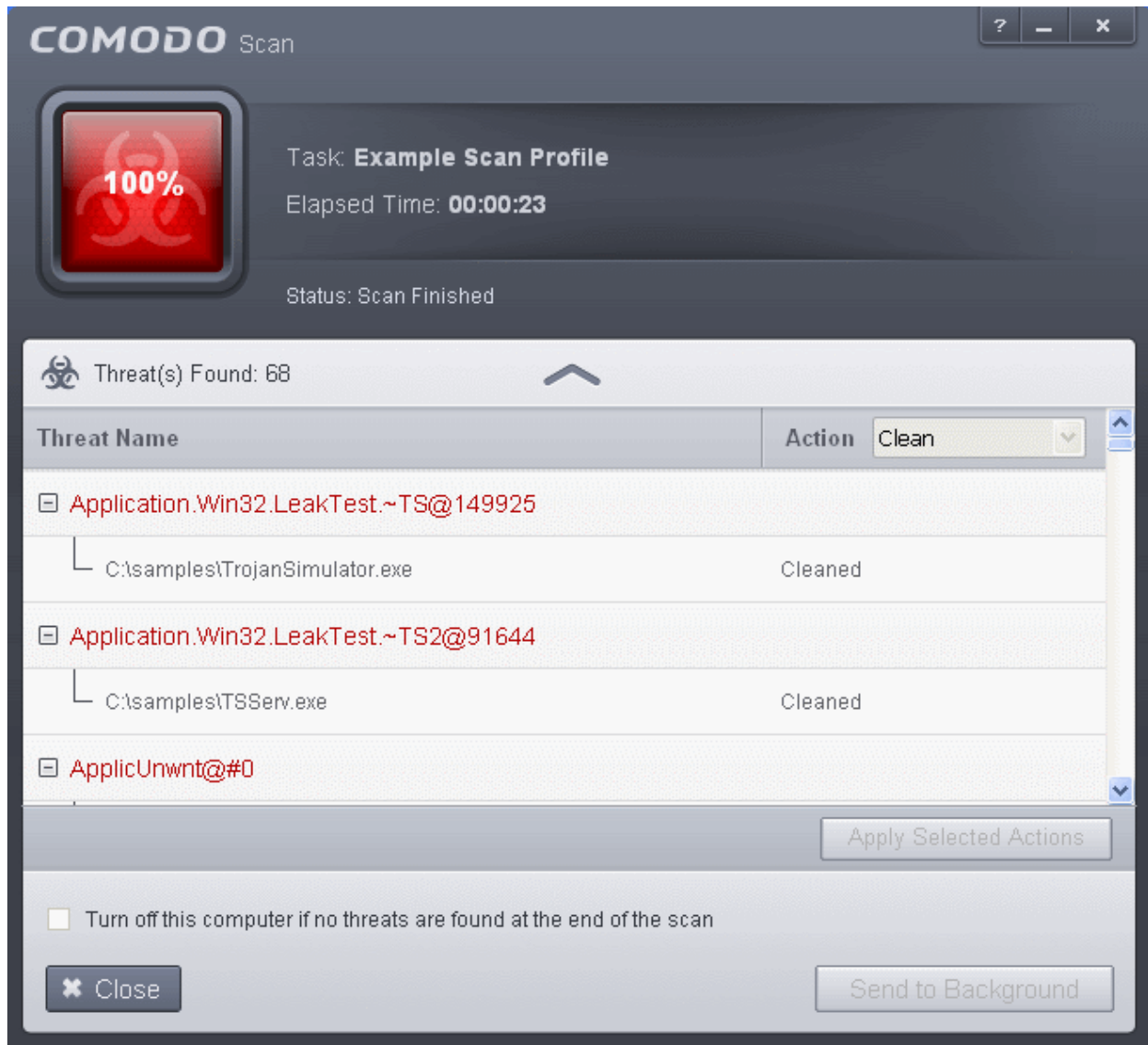


To run a custom scan as per scan profile

- 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.



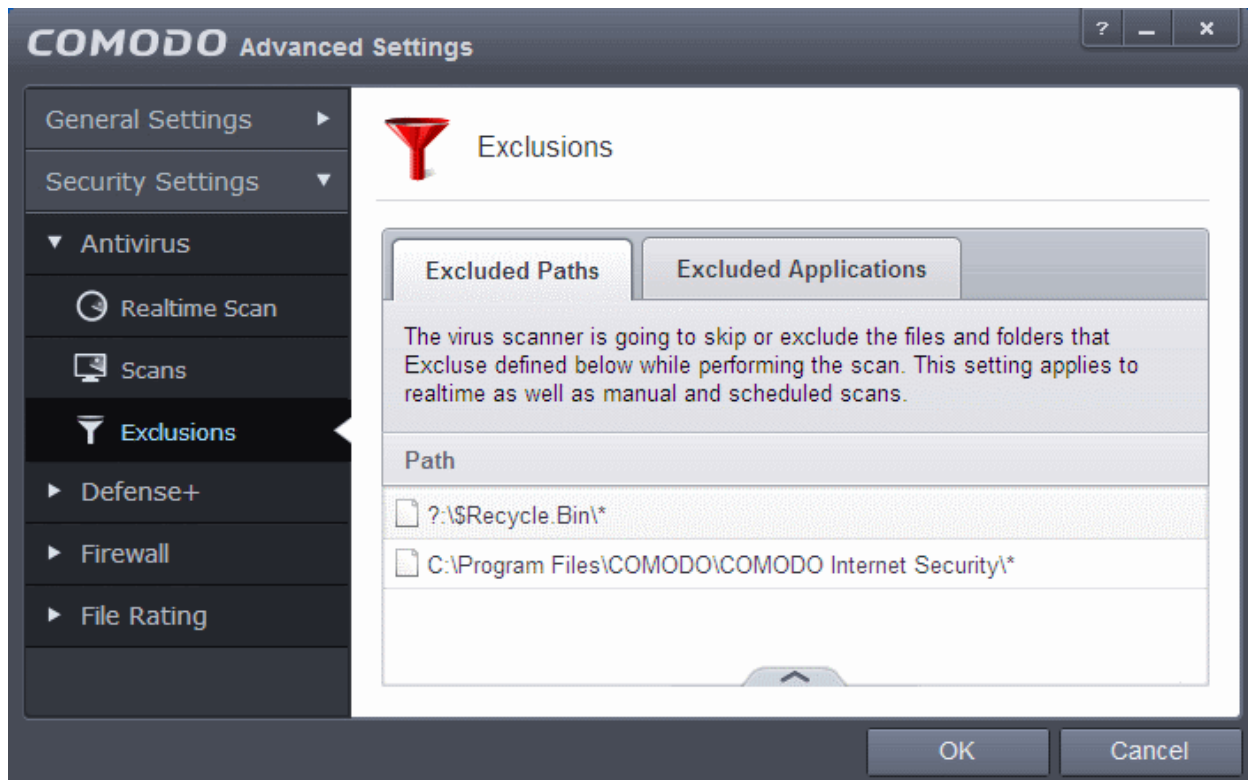
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to [Processing the infected files](#) for more details.

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.

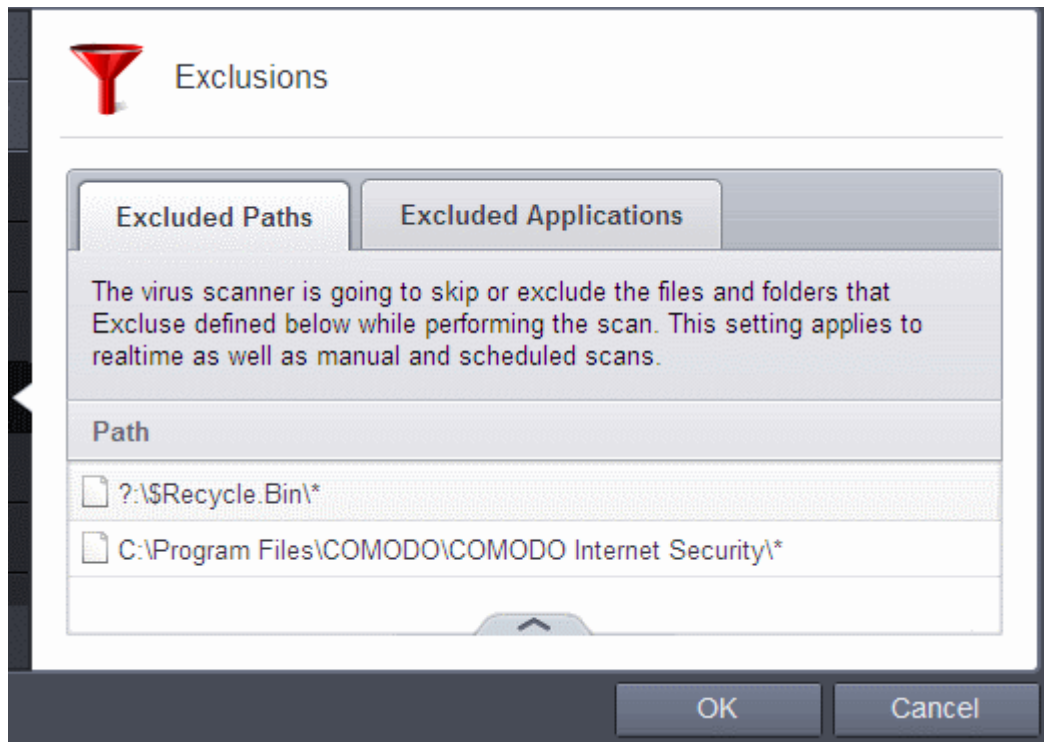


The Exclusions panel has two tabs:

- **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 scans but will be scanned on running on-demand scans. Refer to the section [Excluding Programs/Applications from real-time scans](#) for more details on manually adding and removing exclusion items in this interface.

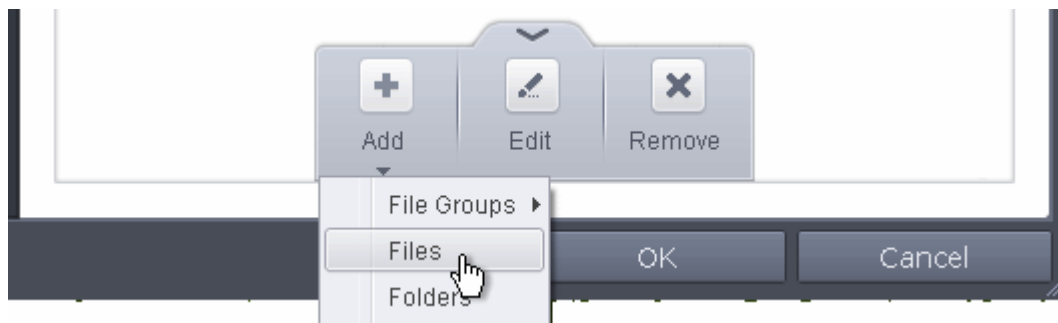
Excluding Drives/Folders/Files from all types of scans

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.



To add item(s) to excluded paths

- Click the handle from the bottom center and click on 'Add' from the options

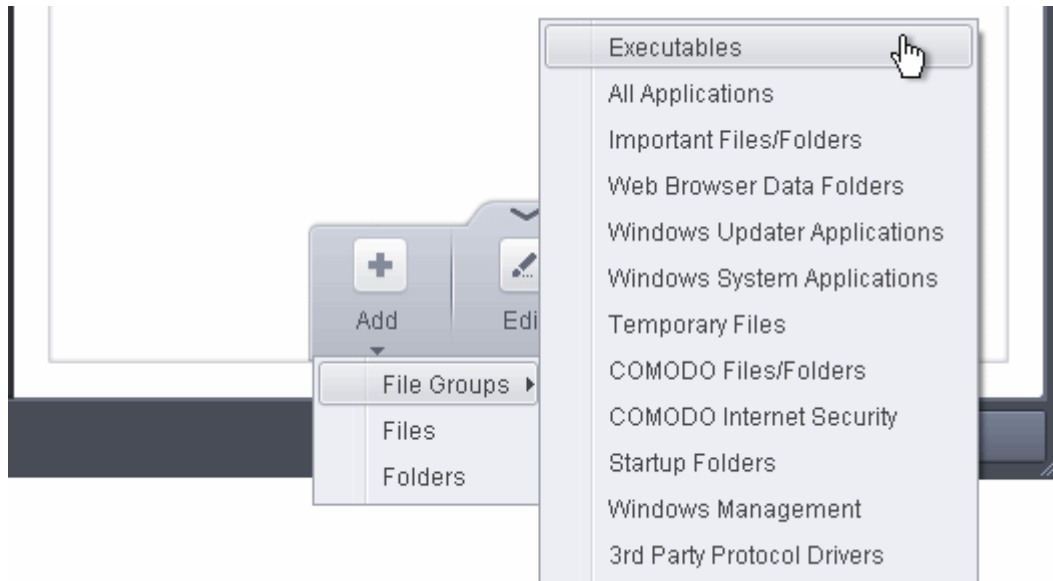


You can choose to add a:

- **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.

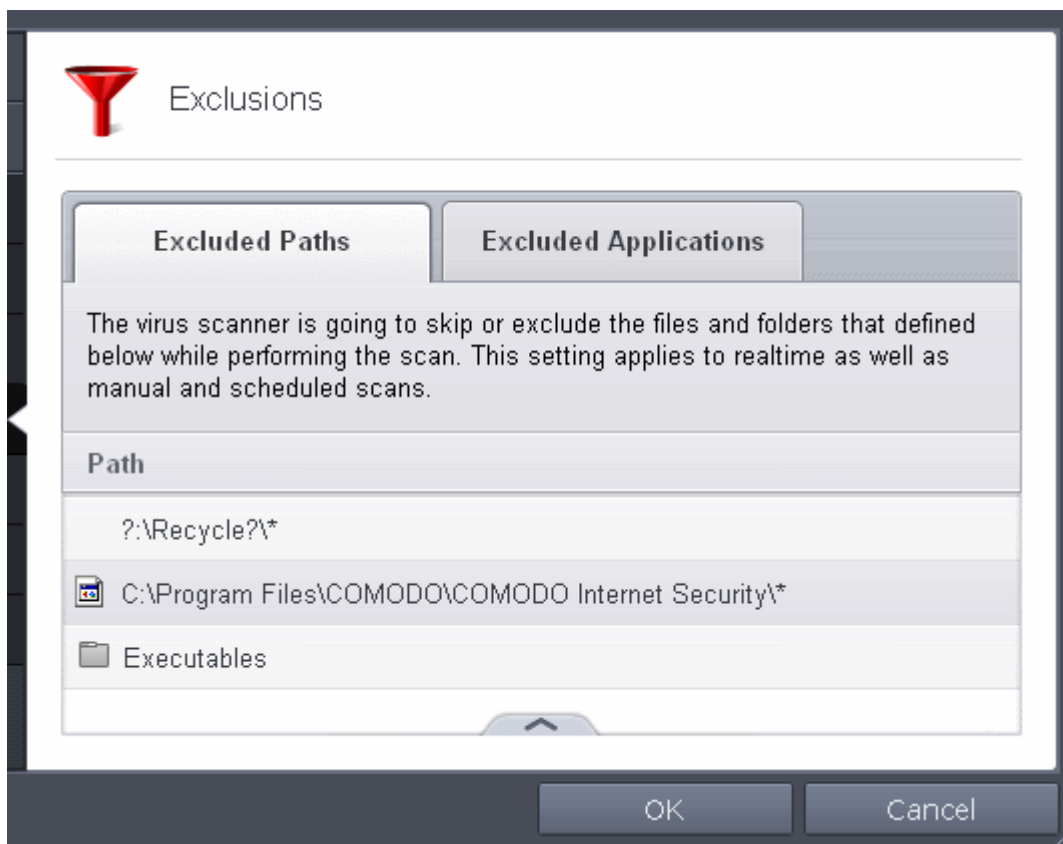


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

The 'File Groups' interface can be accessed by the following method:

- Navigate to **Advanced Settings > Defense+ > HIPS > Protected Files**, click the up arrow from the bottom of the interface and select **'Groups'** from the options.

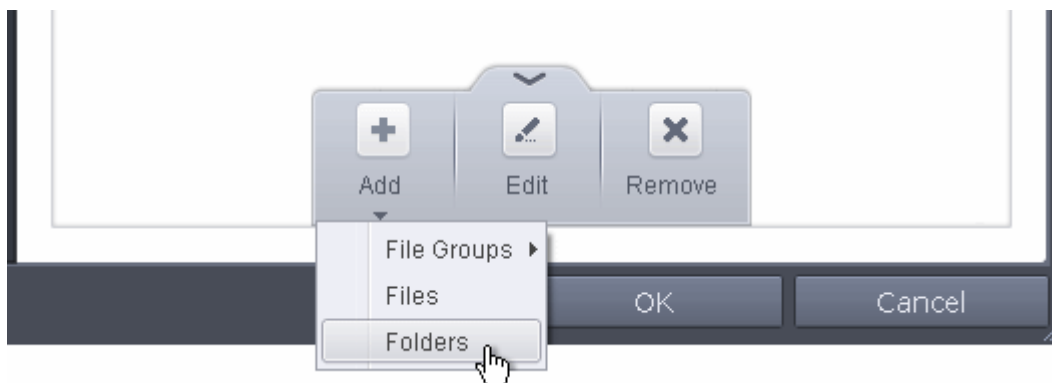
The file groups will be added to Excluded Paths.



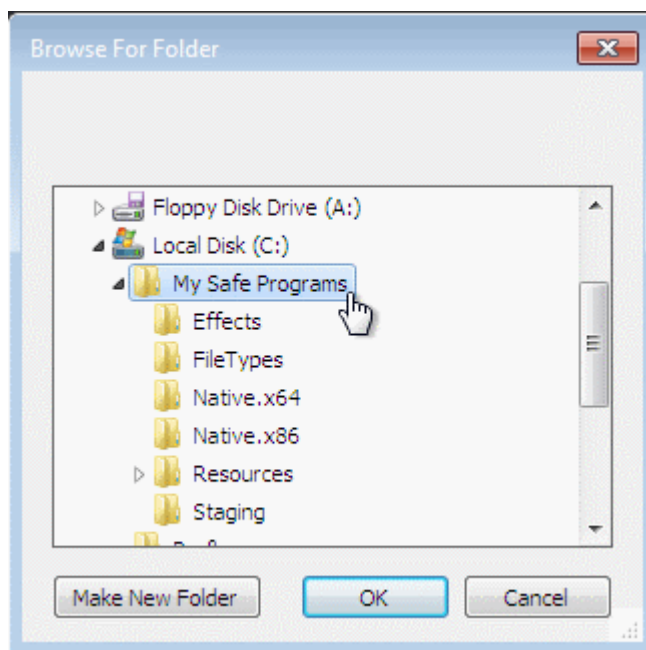
- Repeat process to add more file groups. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding a Drive Partition/Folder

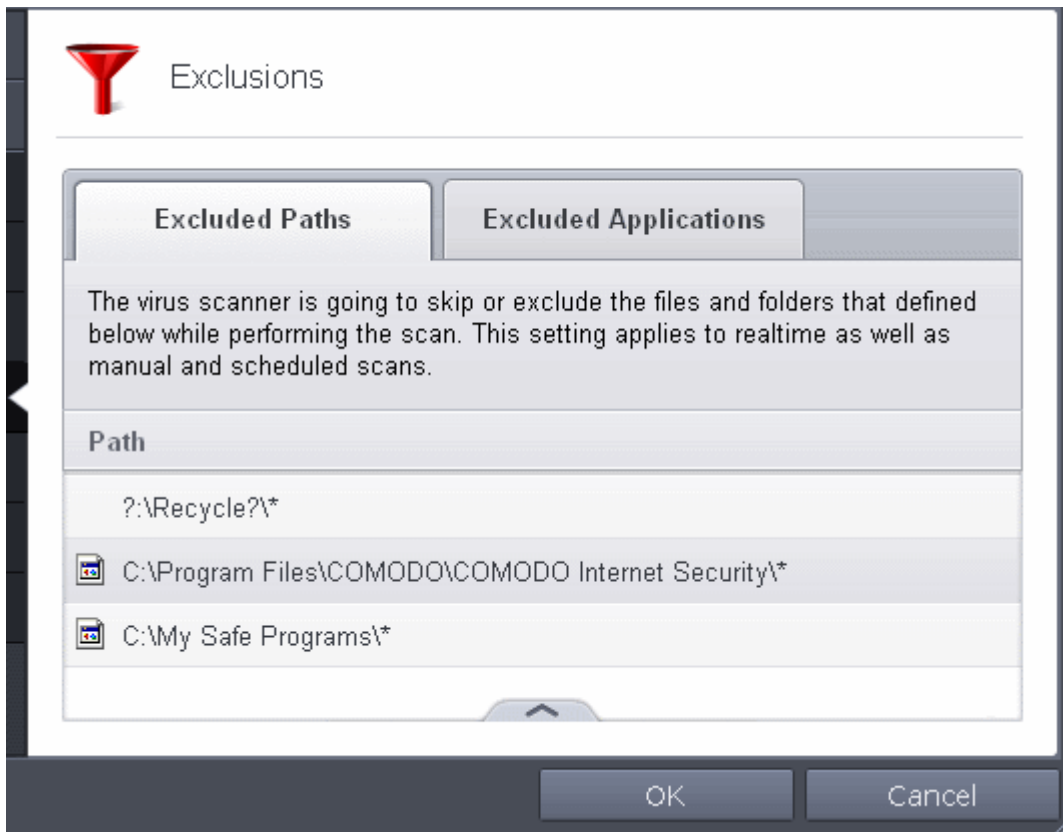
- To add a folder, choose 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will appear.



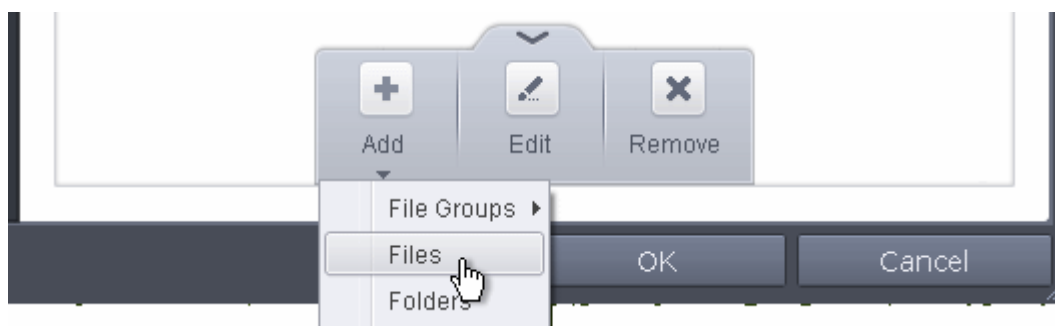
- Navigate to the drive partition or folder you want to add to excluded paths and click OK
The drive partition/folder will be added to Excluded Paths.



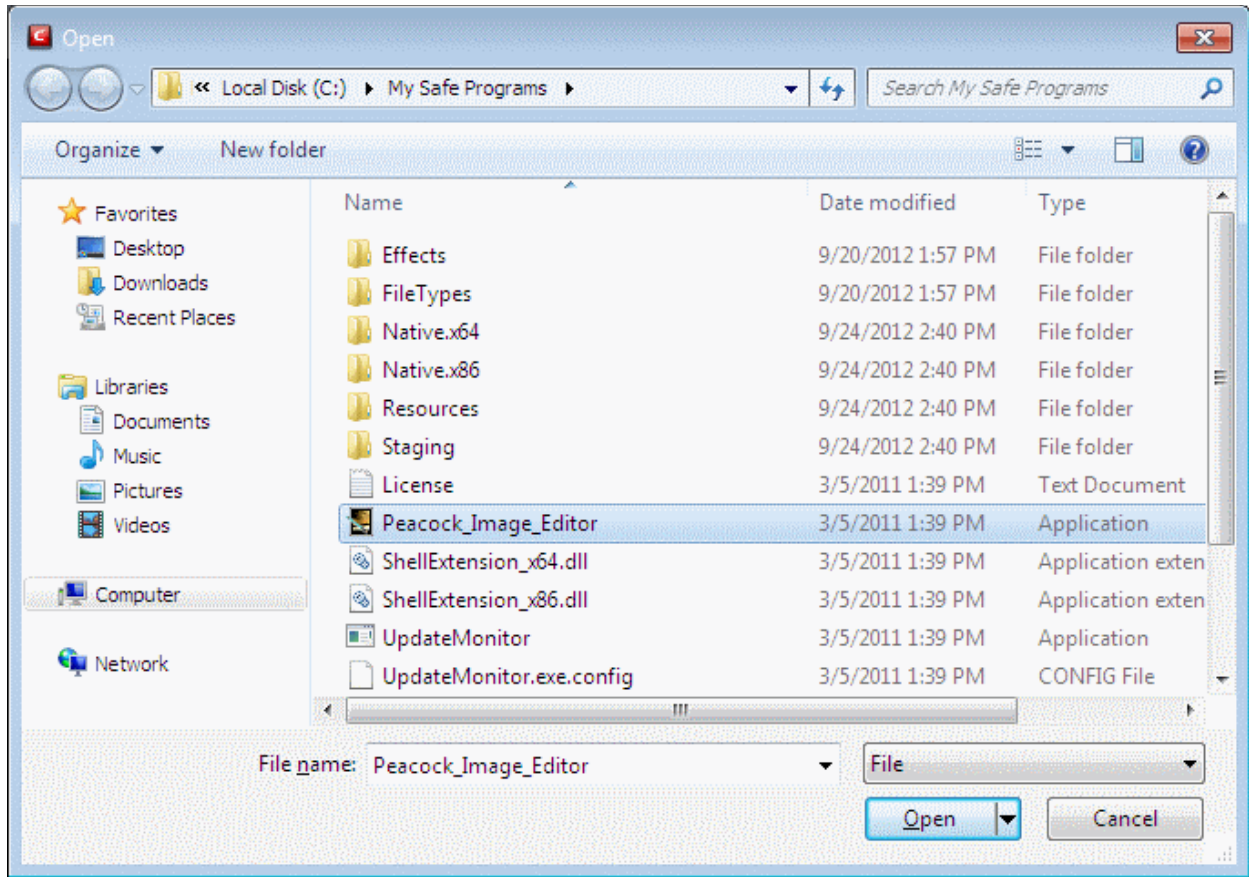
- Repeat process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding an individual File

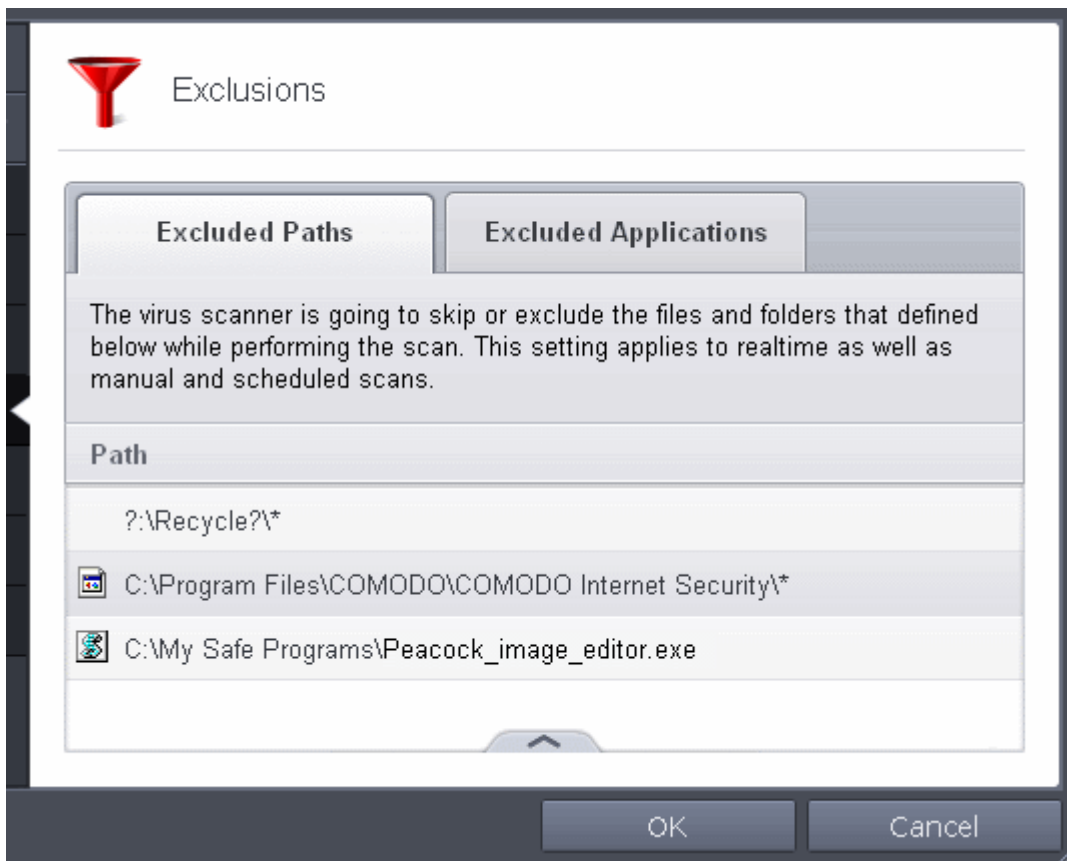
- Choose 'Files' from the 'Add' drop-down.



- Navigate to the file you want to add to Excluded Paths in the 'Open' dialog and click 'Open'



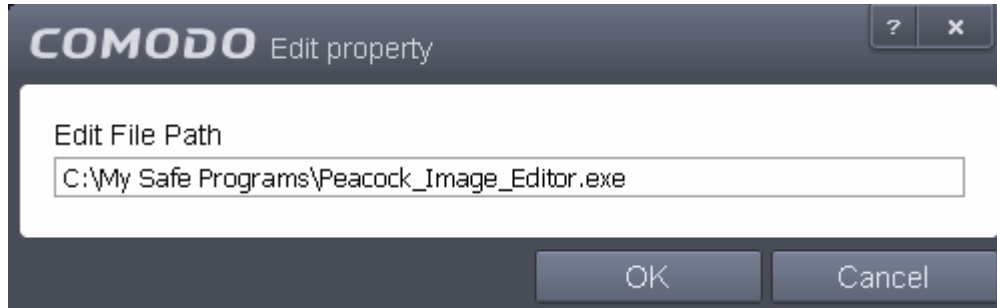
The file will be added to Excluded Paths.



- Repeat process to add more paths. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

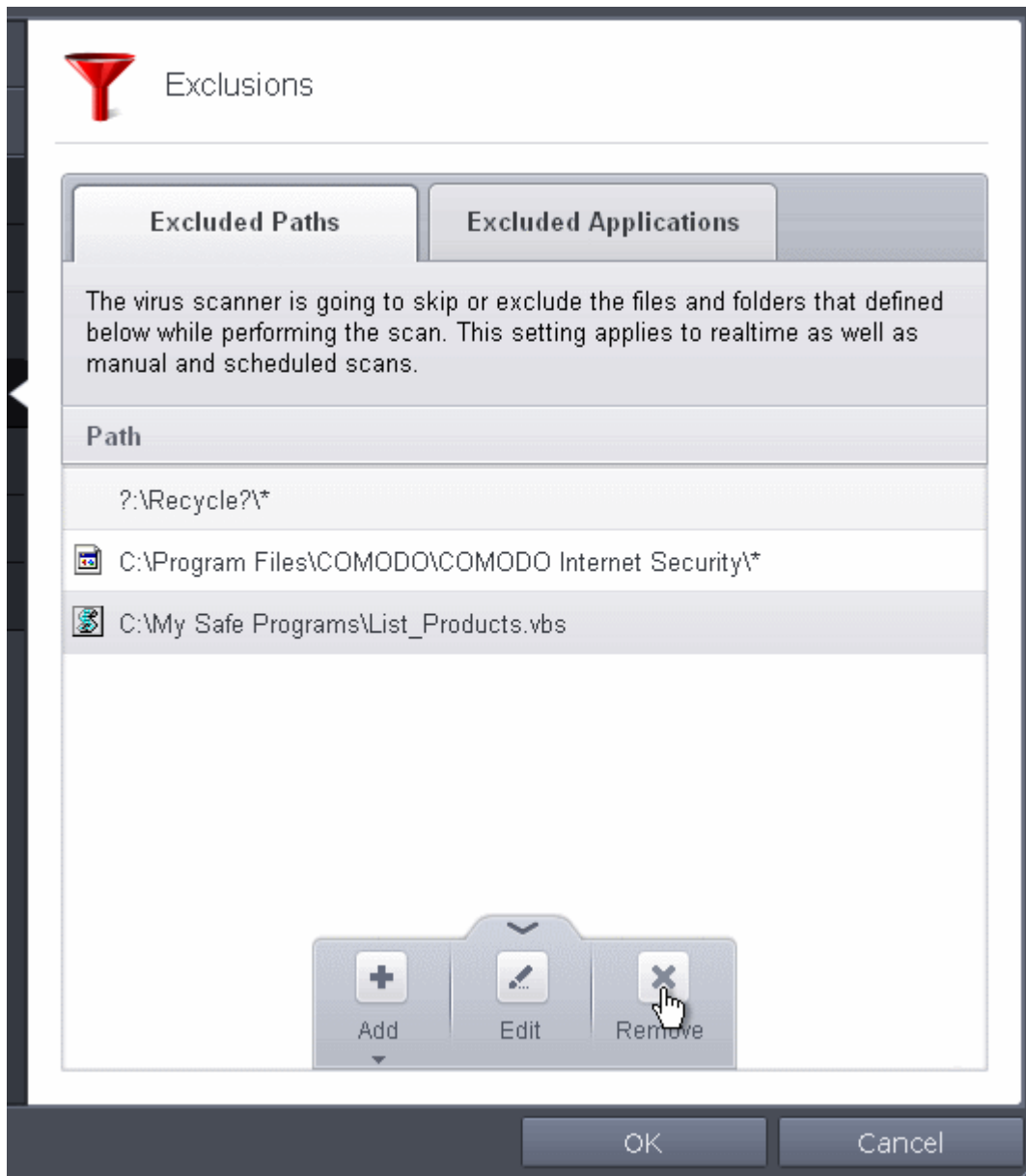
To edit the path of an added item

- 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'.



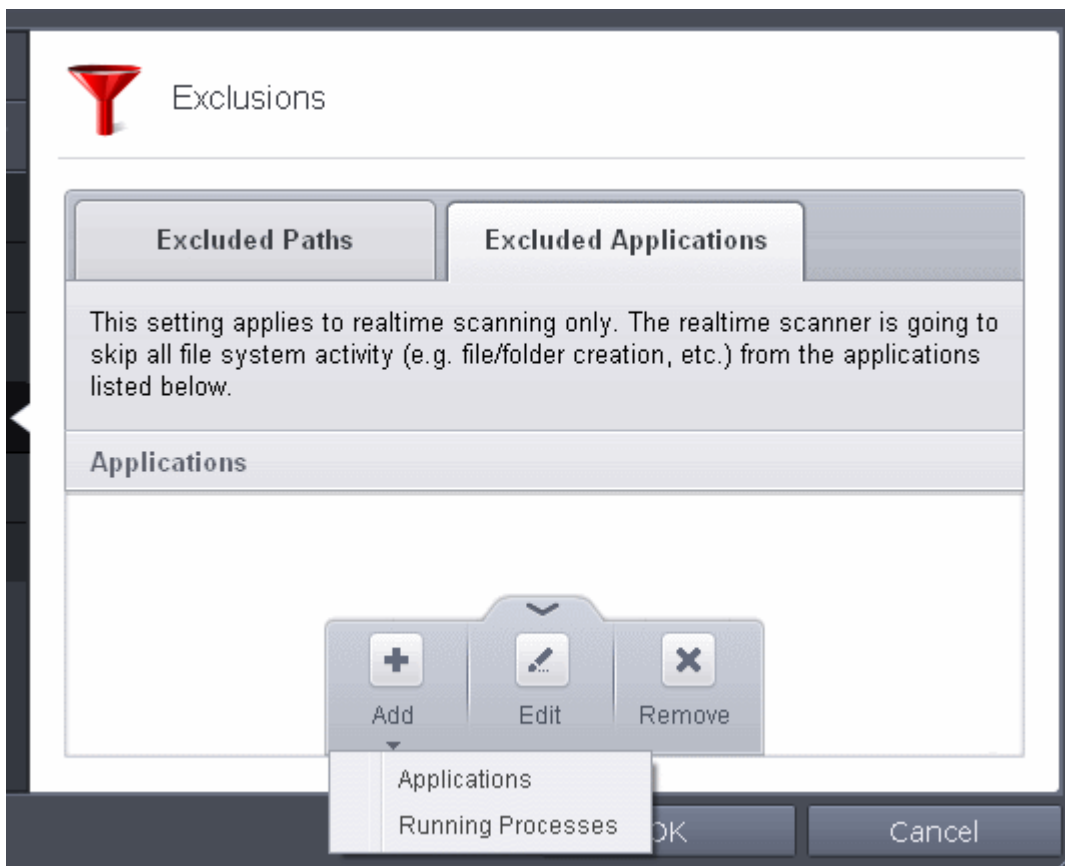
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

In addition to programs, applications or files added to Excluded Applications automatically on selecting Ignore action from the Scan Results window, you can manually add programs, applications or files to Excluded Applications list for excluding them from real-time scans. Also you can remove the items from Excluded Applications that were added by mistake.

To add an item to Excluded Applications

- Click the handle from the bottom center and click on 'Add' from the options

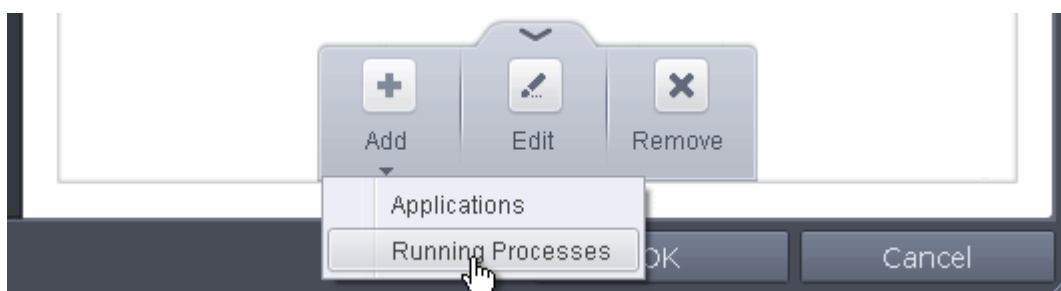


You can choose to add an application by:

- **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.

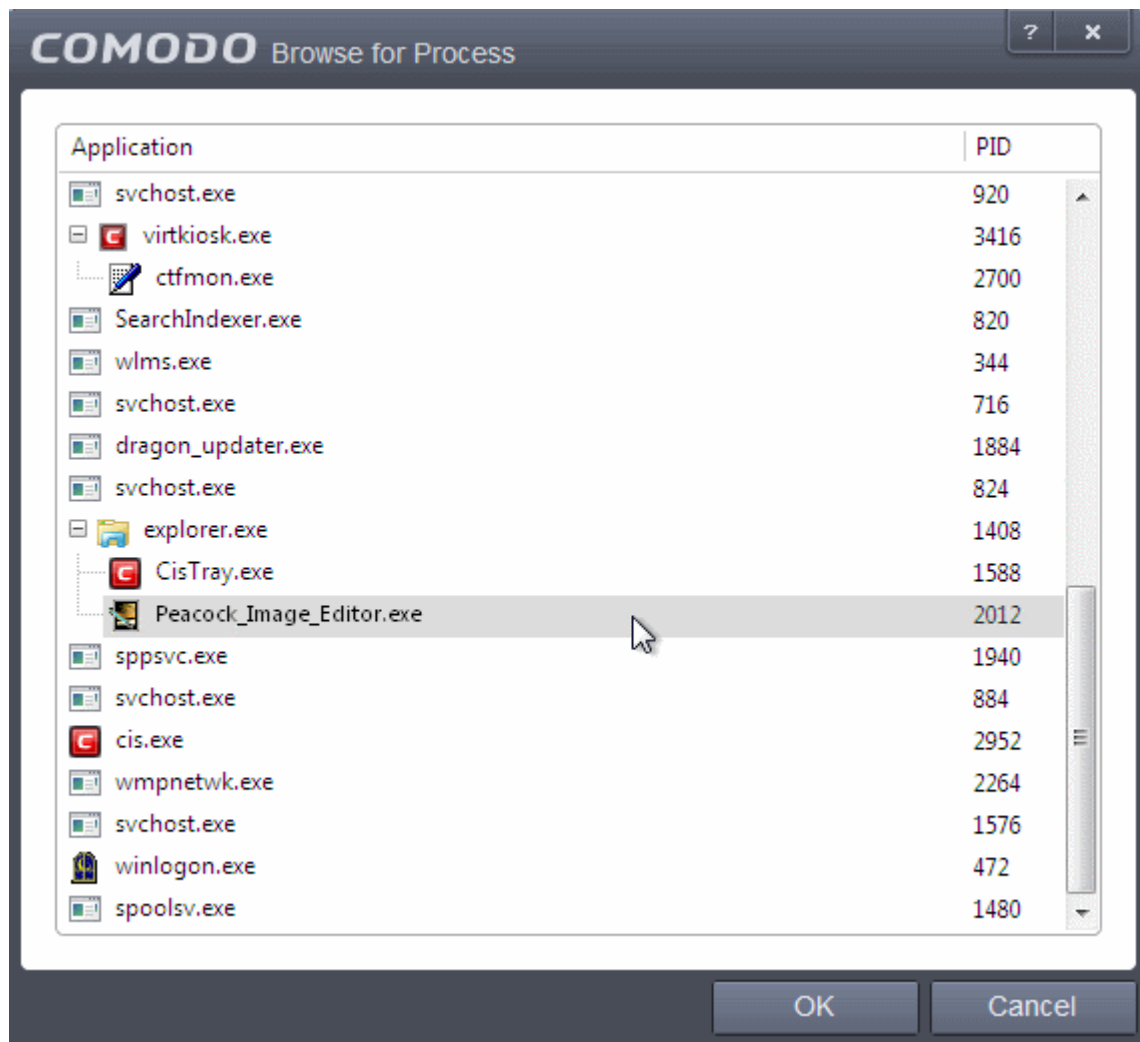
Adding an application from a running processes

- Choose 'Running Processes' from the 'Add' drop-down

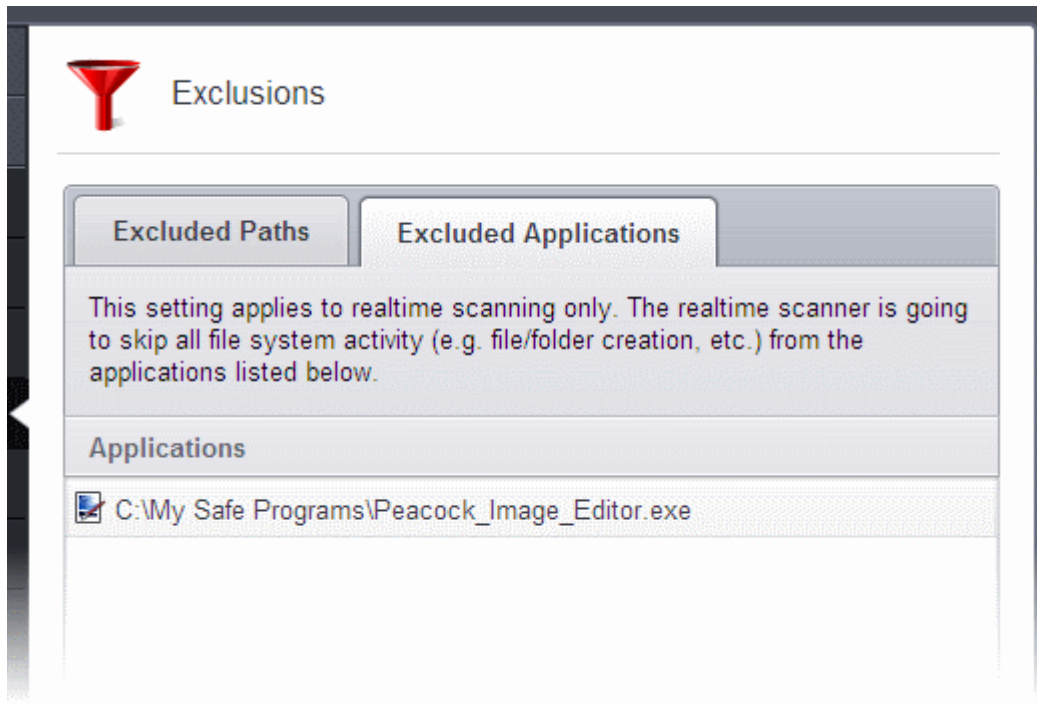


A list of currently running processes in your computer will be displayed

- Select the process, whose target application is to be added to excluded applications and click OK from the Browse for Process dialog.

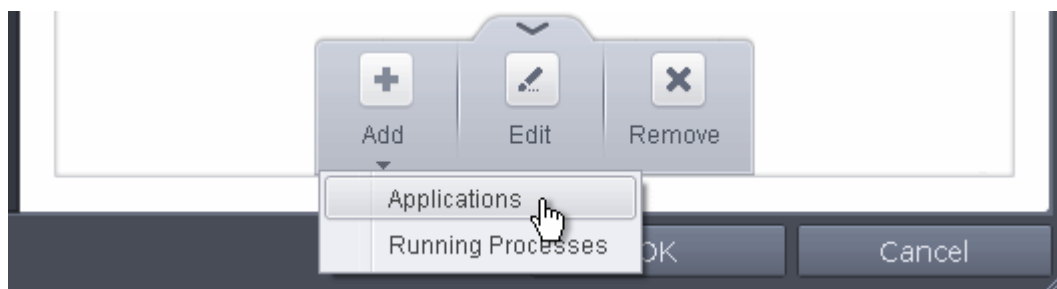


The application will be added to Excluded Applications.

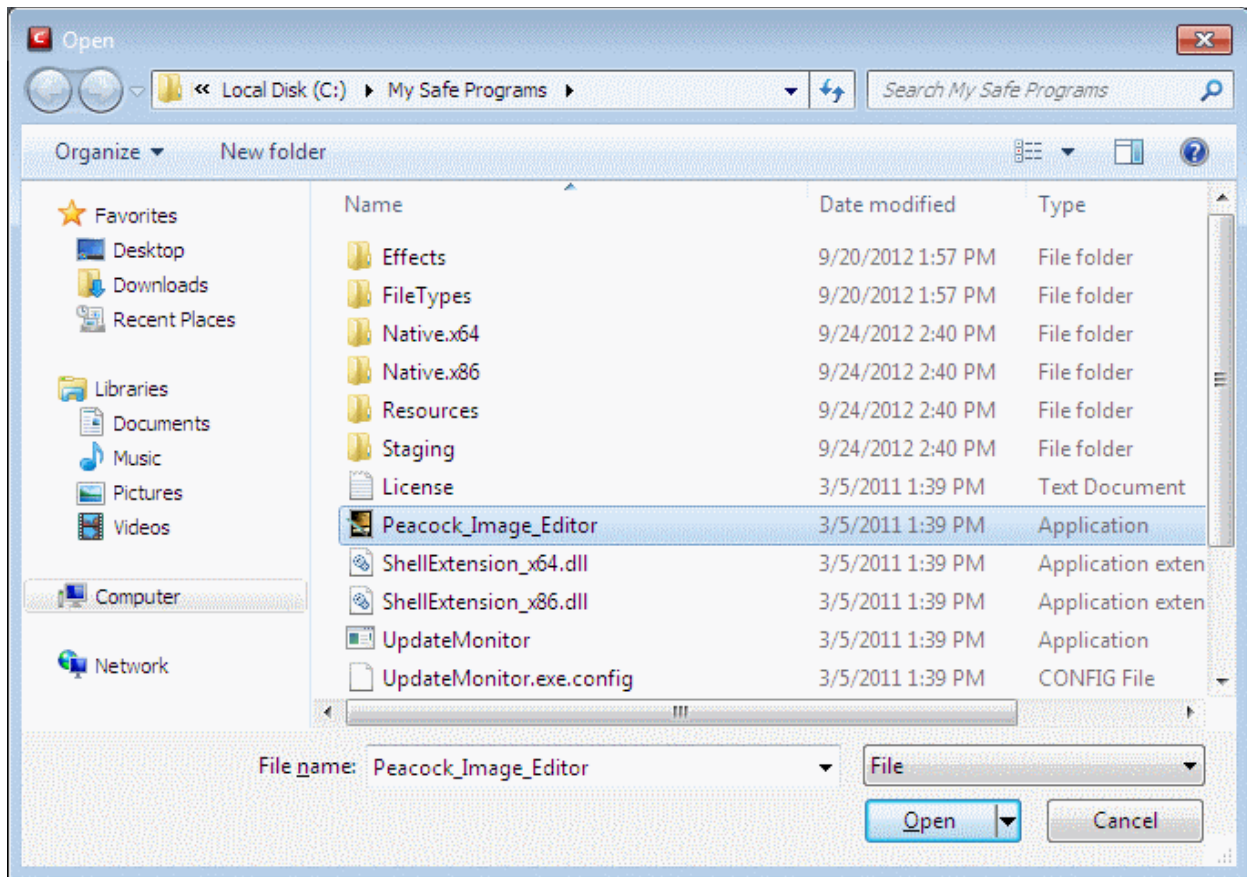


Browsing to the Application

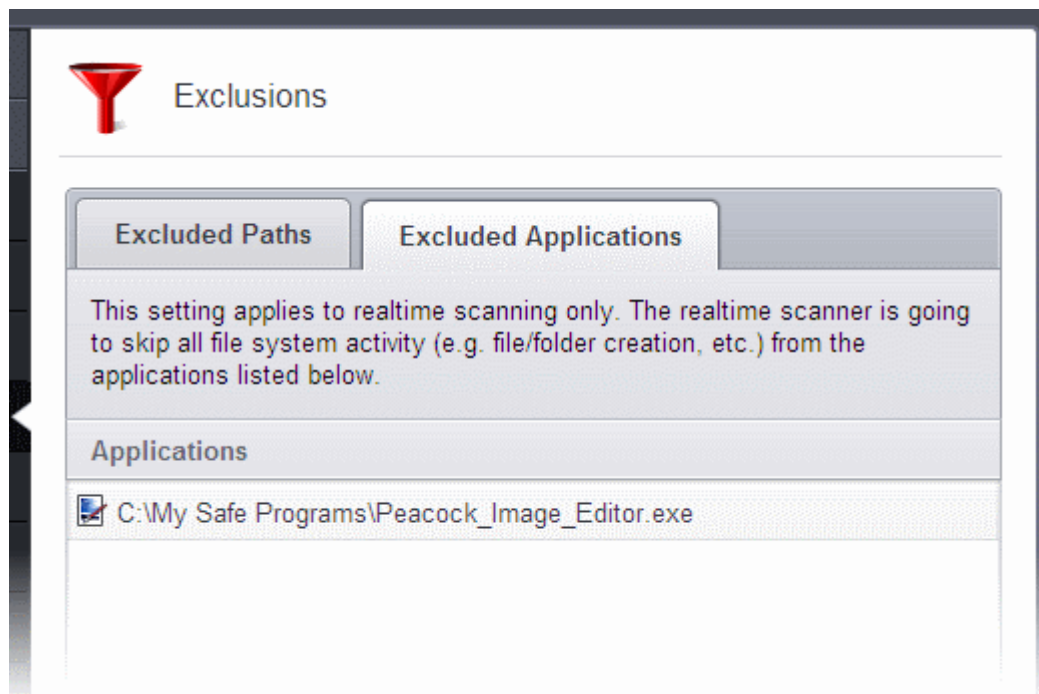
- Choose 'Applications' from the 'Add' drop-down



- Navigate to the file you want to add to Excluded Applications in the 'Open' dialog and click 'Open'



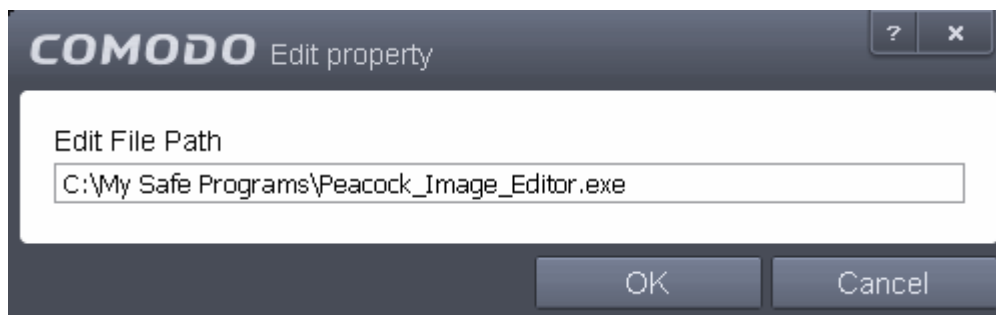
The file will be added to 'Excluded Applications'.



- Repeat process to add more items. The items will be skipped from future real-time scans.

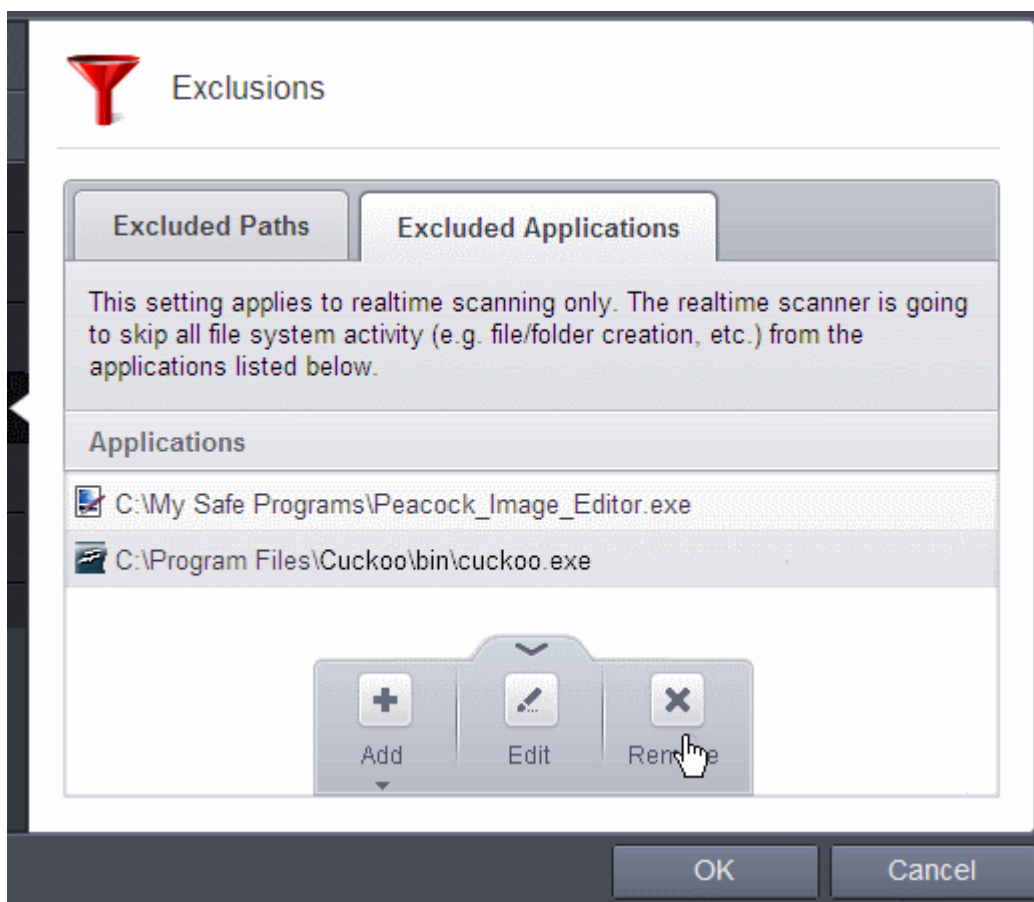
To edit the path of the application added to Excluded Application

- 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

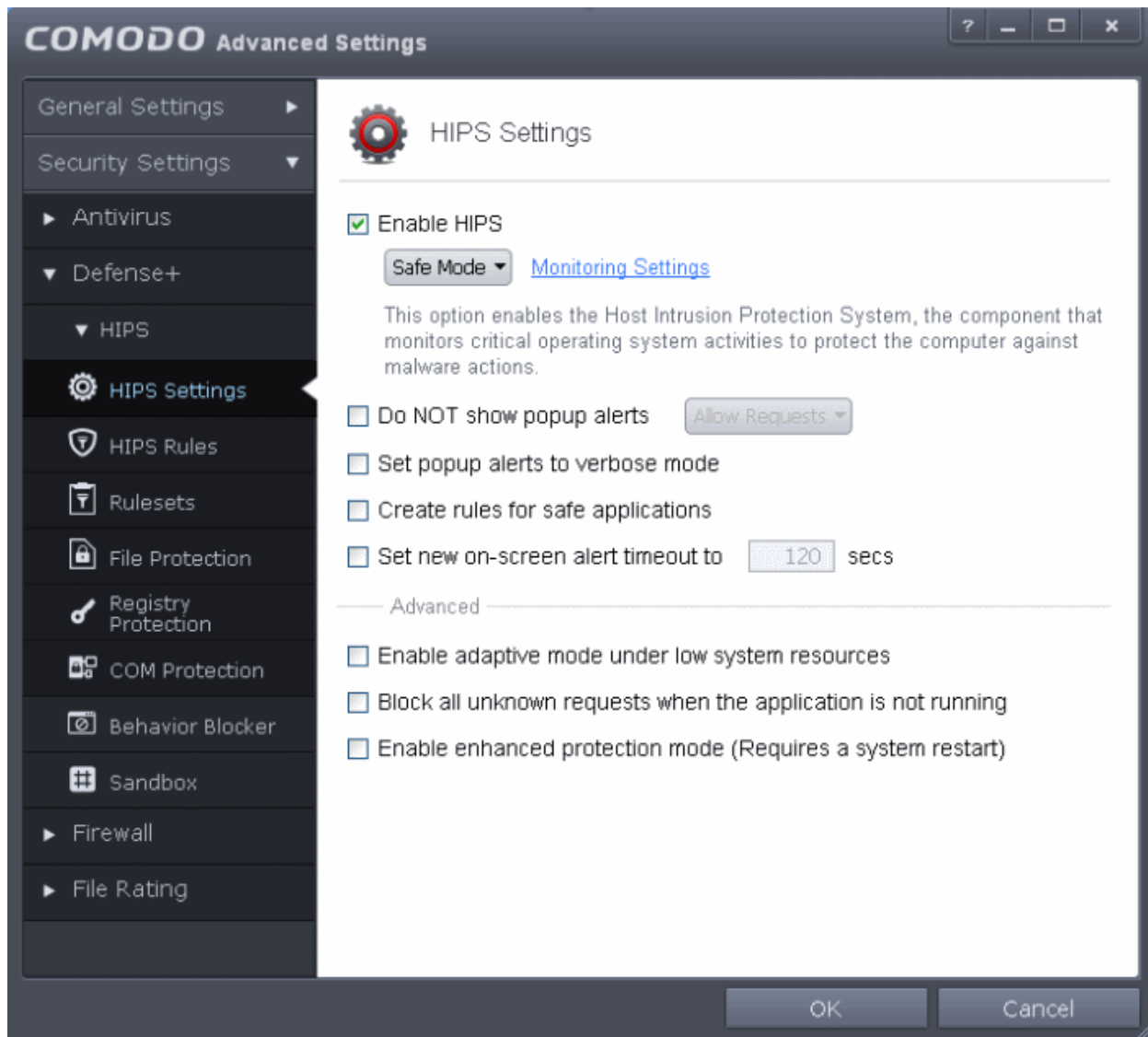
- Select the item, click the handle from the bottom center and select 'Remove'.



- 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 behavior blocker 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 Behaviour Settings**
 - **Active HIPS Rules**
 - **Predefined HIPS Rule Sets**
 - **Protected Files and Folders**
 - **Protected Registry Keys**
 - **Protected COM interfaces**
- **Behavior Blocker**
- **Sandbox Settings**

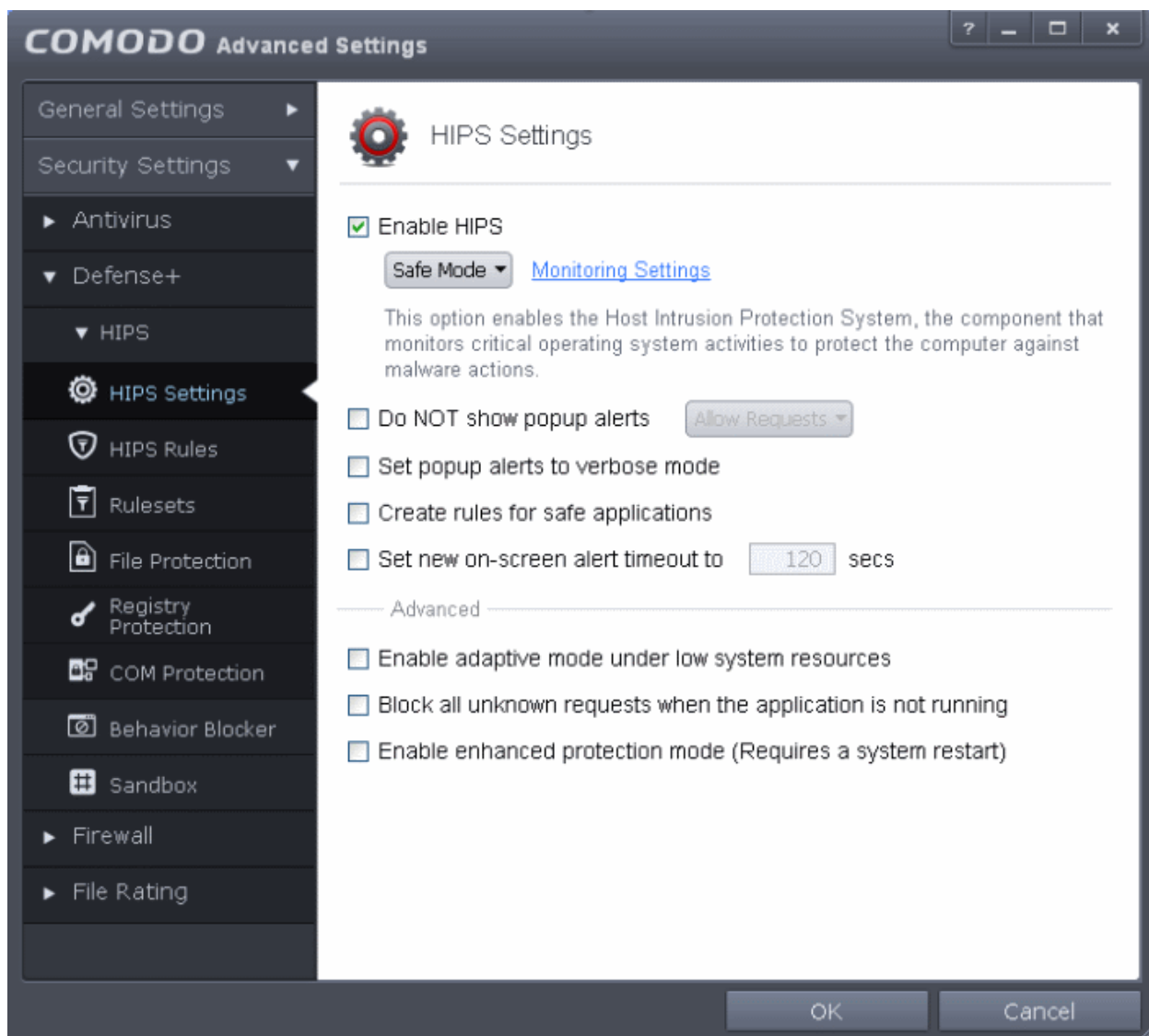
6.2.2.1. HIPS Behavior Settings

HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo 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

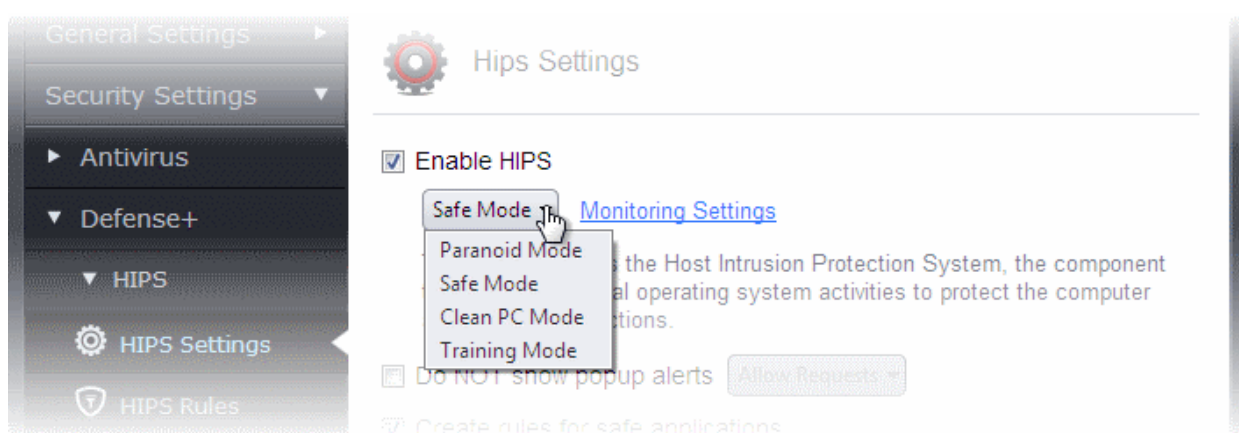


- **Enable HIPS** - Allows you to enable/disable the HIPS protection. (*Default=Disabled*)

If enabled, you can choose the security level and configure the monitoring settings for the HIPS component.

Configuring Security Level of HIPS

The security level can be chosen from the drop-down that becomes active only on enabling HIPS:



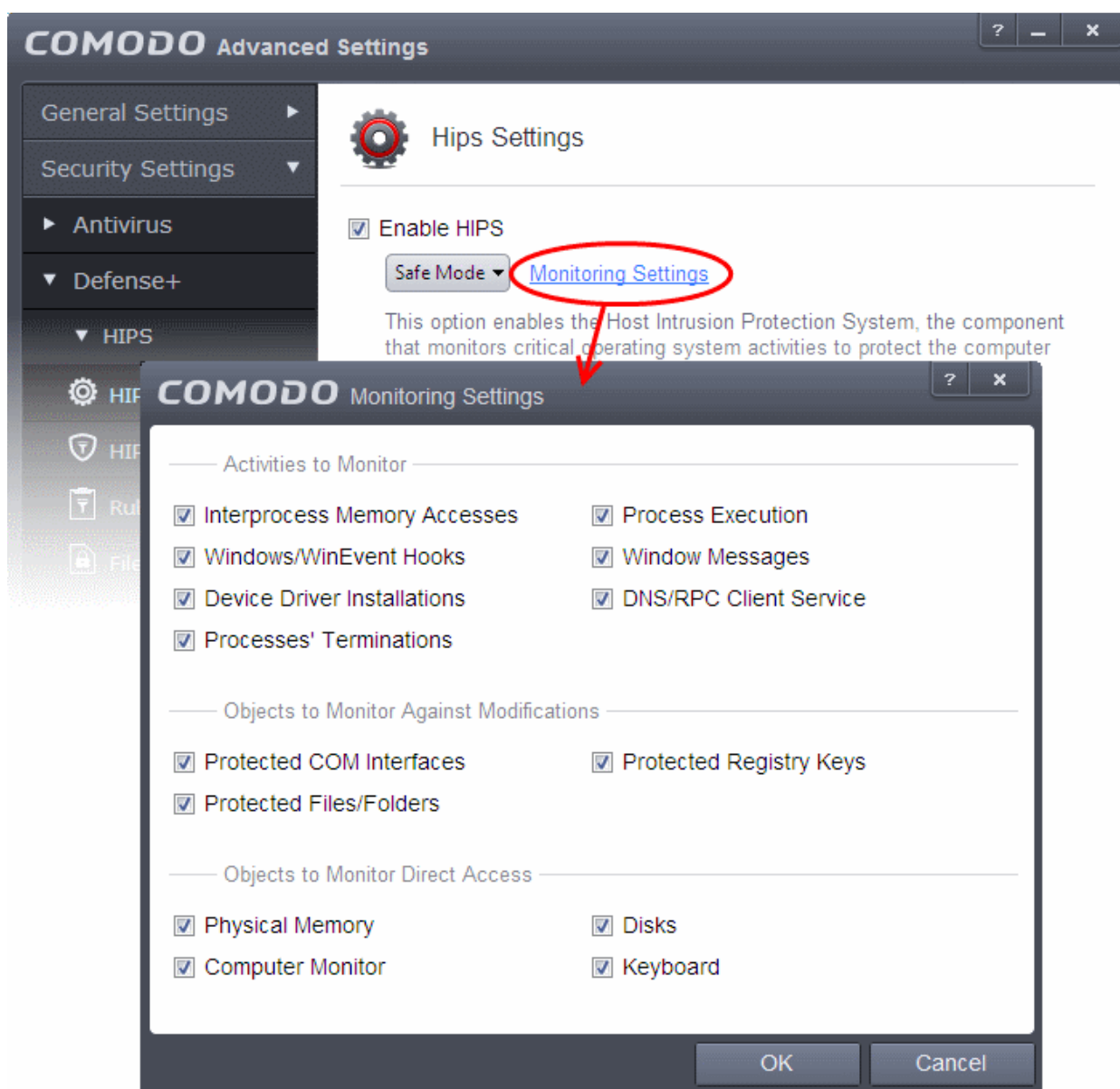
The choices available are:

- 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 computer while all new executables introduced to the system are monitored and controlled. This patent-pending mode of operation is the recommended option on a new computer or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files in '**Unrecognized Files**' 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 be monitored by HIPS can be configured by clicking the [Monitoring Settings](#) link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a *global* basis - effectively creating a universal '**Allow**' rule for that activity. This 'Allow' setting *over-rides* 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:

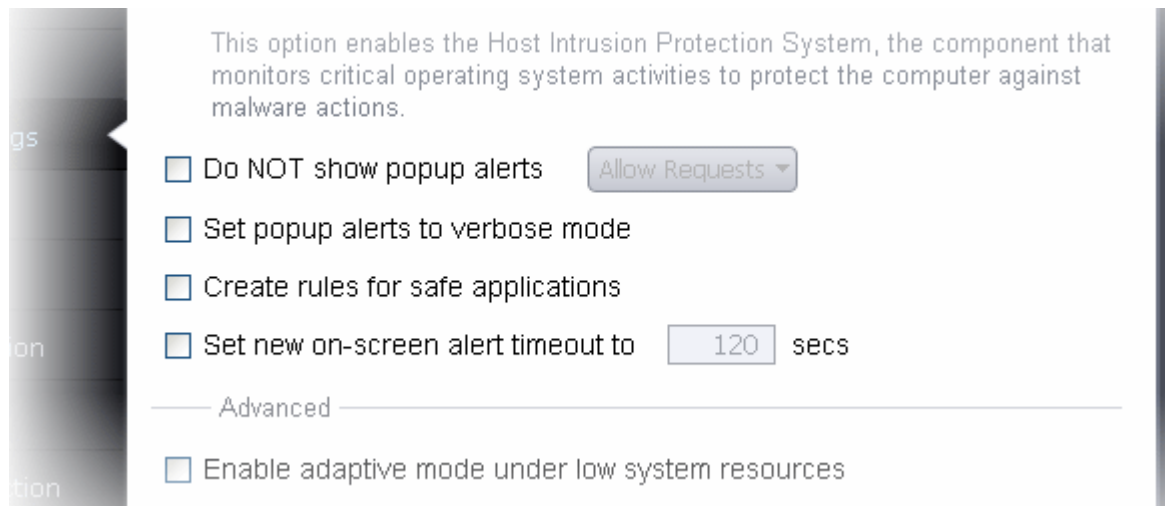
- **Physical Memory:** Monitors your computer's memory for direct access by an applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store 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 = 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'.



- **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
- **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 included in the **Trusted Files** 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).

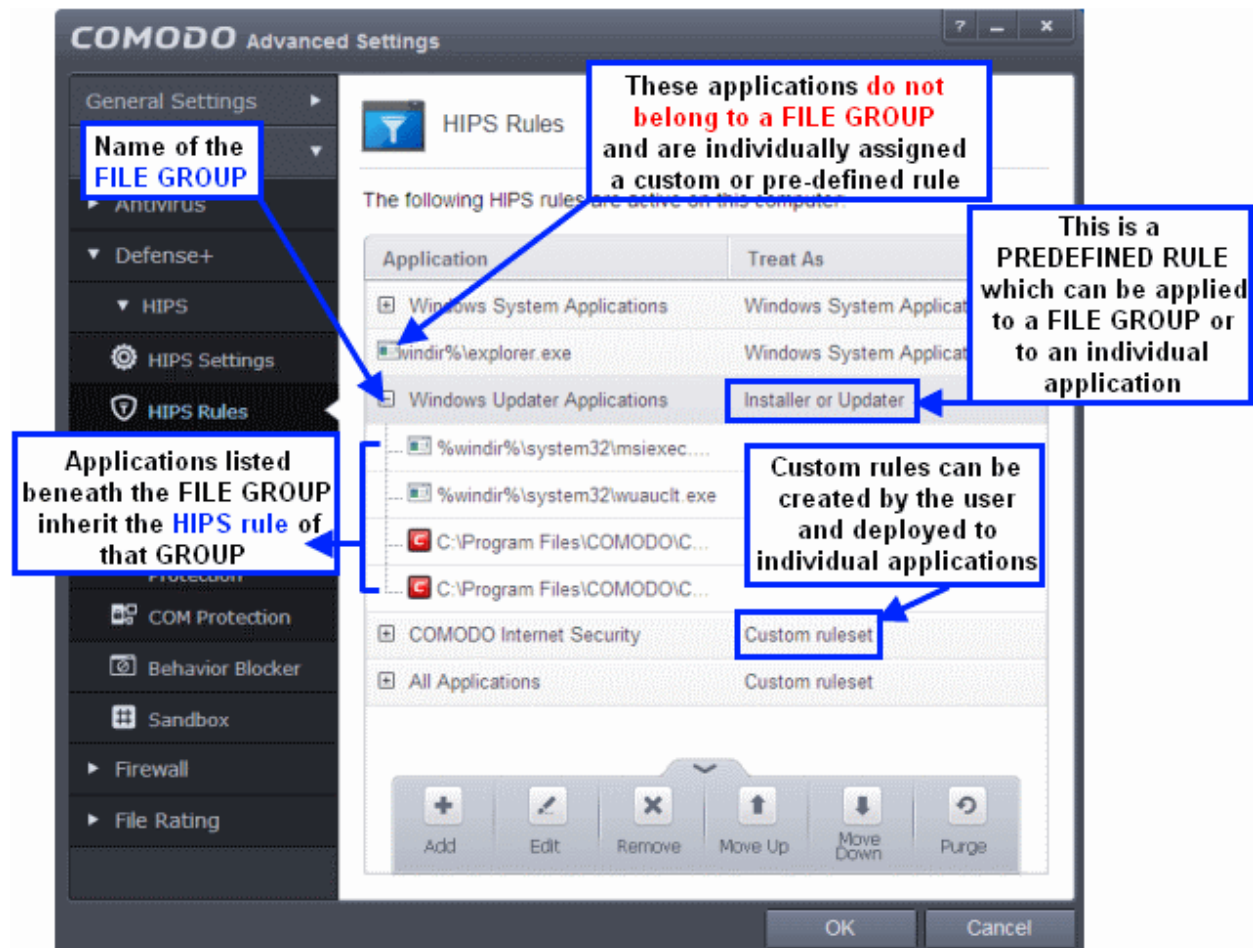
- **Set new on-screen alert time out to:** Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

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 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*)

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.

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.

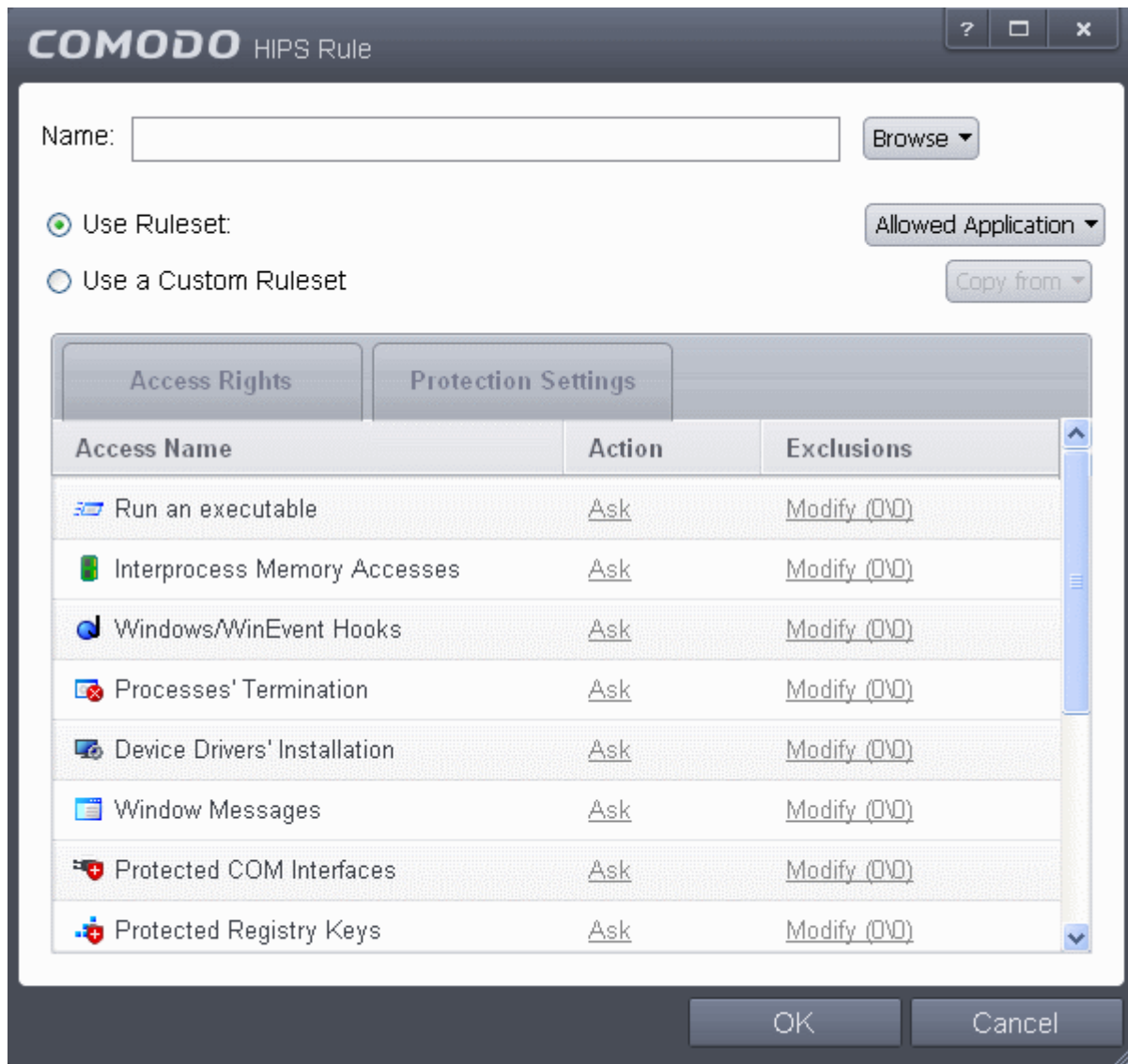
Creating or Modifying a HIPS Ruleset

To begin defining a 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.

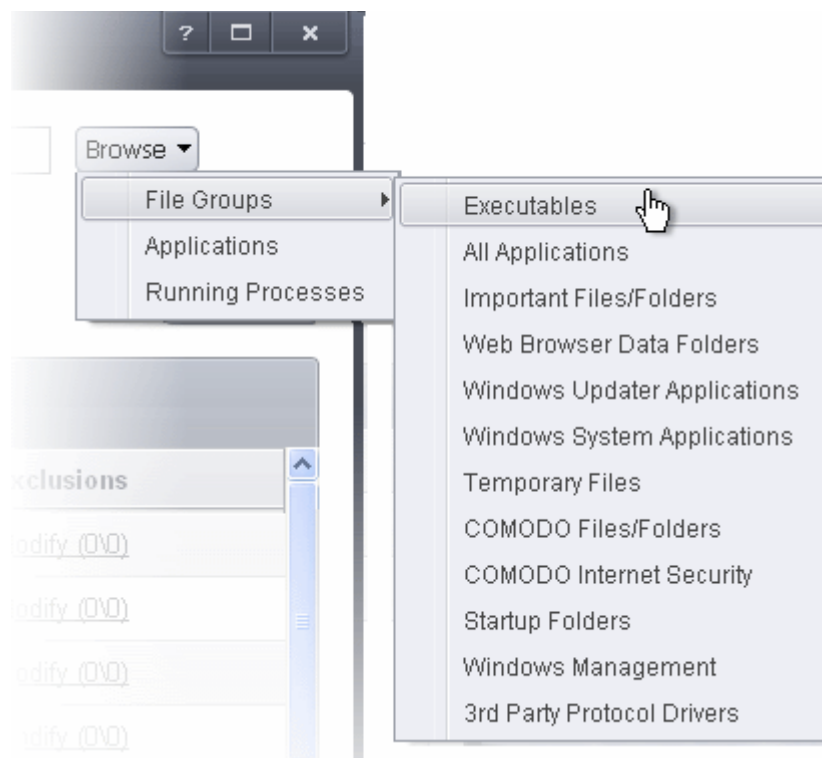


Because you are defining the HIPS rule settings for a new application, you can notice that the 'Name' box is blank. (If you were editing an existing rule instead, then this interface would show that application's name with installation path or application group's name.)

- 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**.

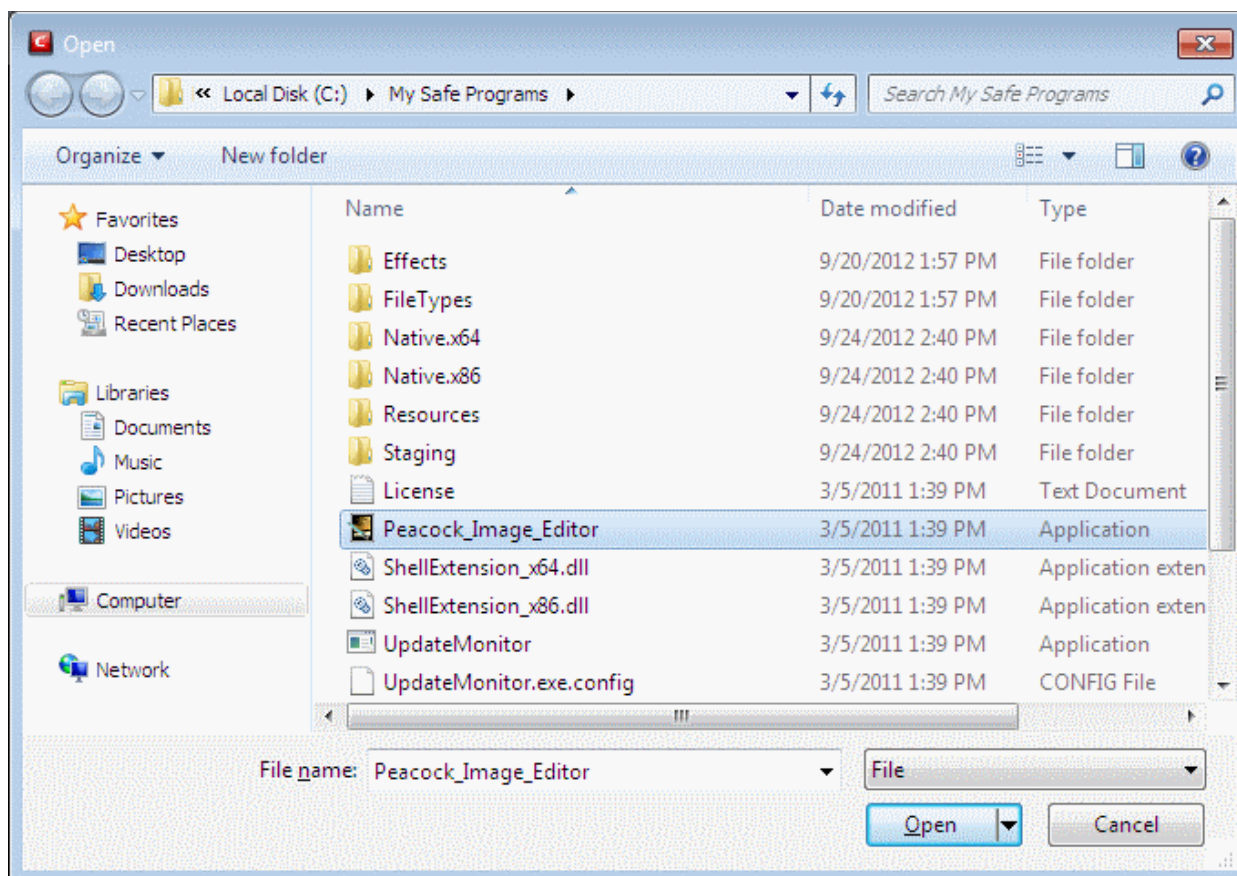
1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available 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.



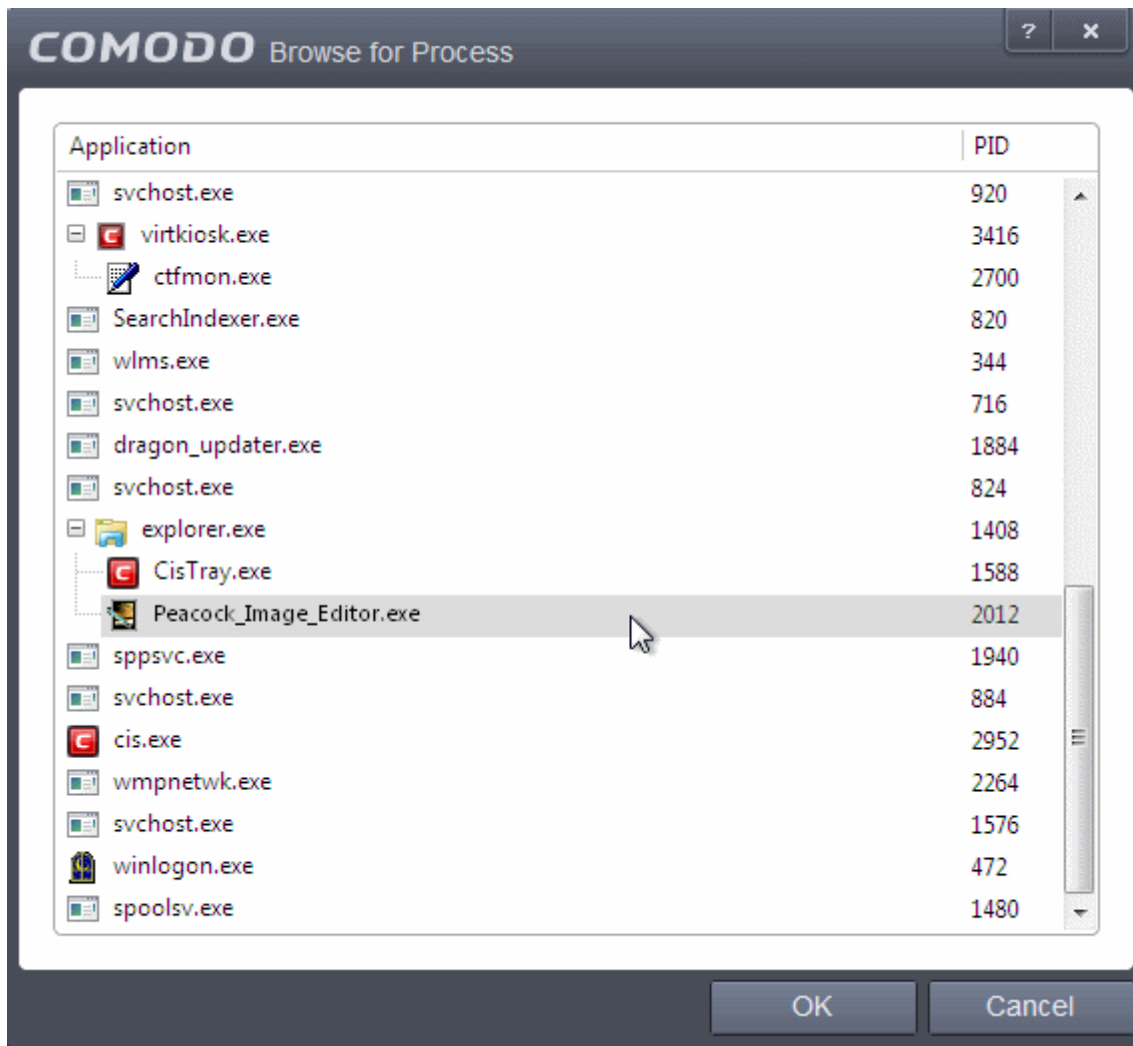
To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

The 'File Groups' interface can be accessed by the following method:

- Navigate to **Advanced Settings > Defense+ > HIPS > Protected Files**, click the up arrow from the bottom of the interface and select '**Groups**' from the options.
- 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.

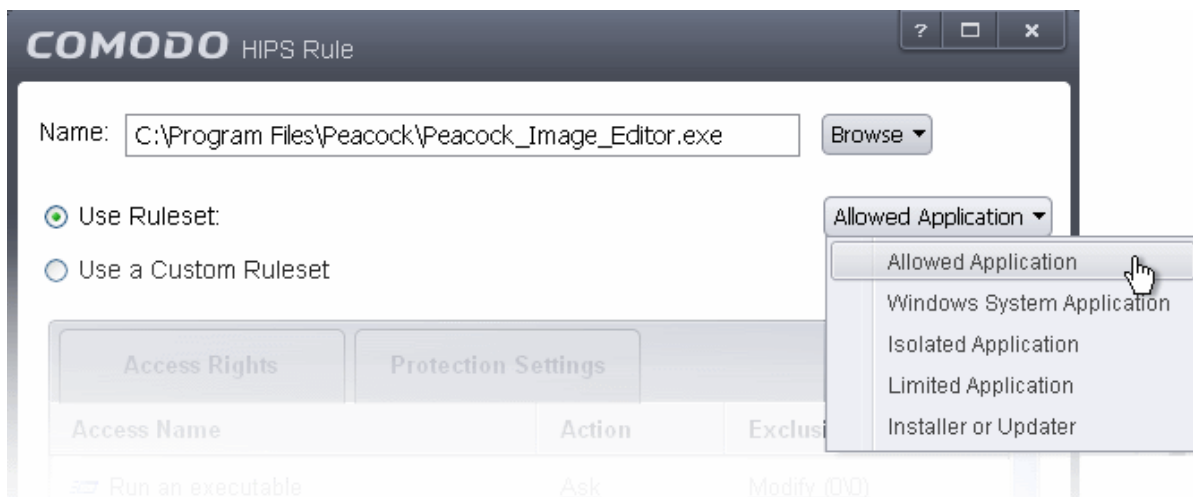


Having selected the individual application, running process or file group, the next stage is to Configure the rules for this ruleset.

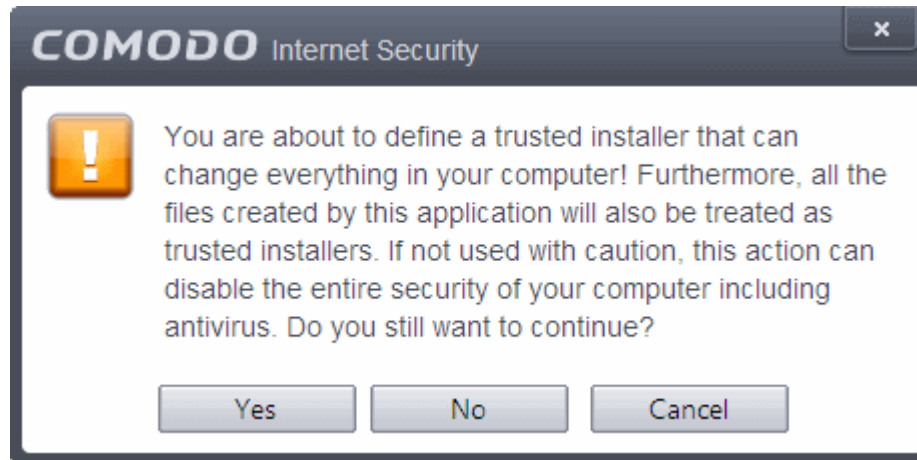
Step 2 - Configure the HIPS Ruleset for this application

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.

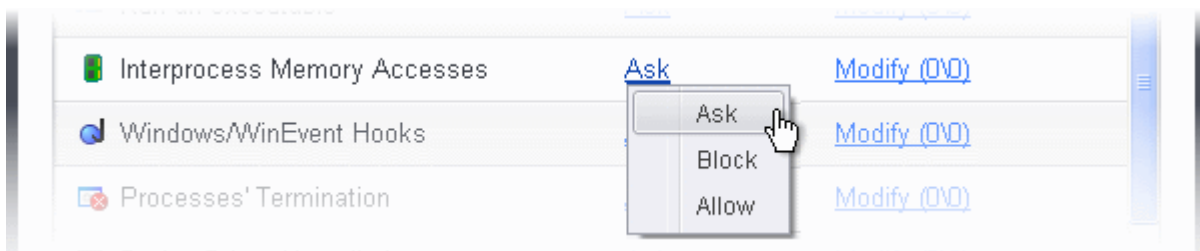
2. **Use a Custom Ruleset** - designed for more experienced users, the 'Custom Ruleset' option enables full control over the configuration specific security ruleset and the parameters of each rule within that ruleset. The Custom ruleset has two main configuration areas - **Access Rights** and **Protection 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.

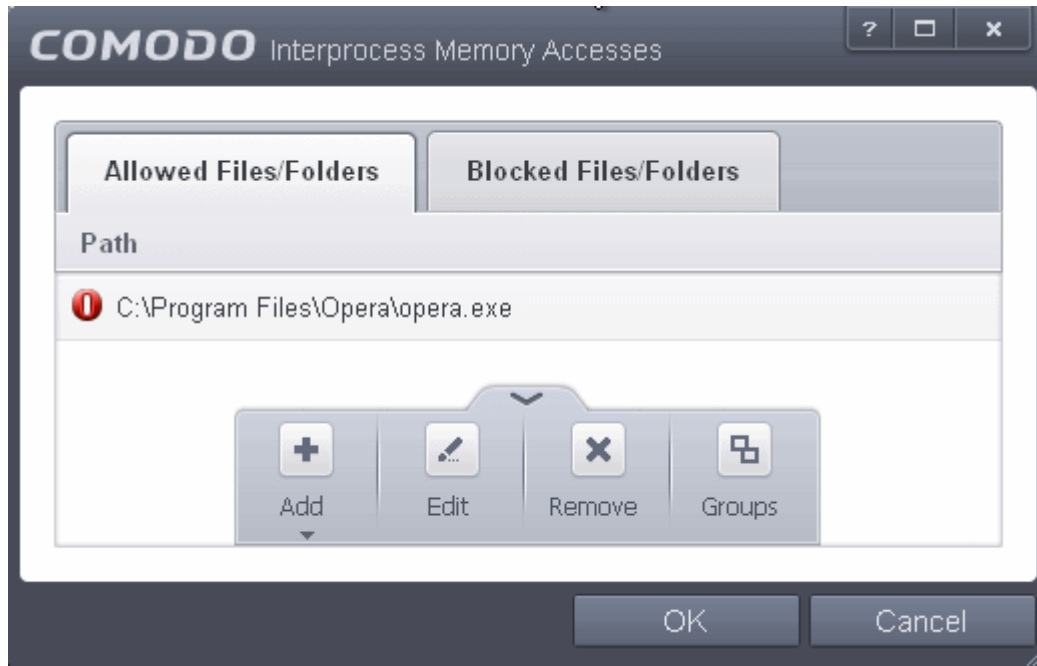
- i. **Access Rights** - The Process Access Rights tab allows you to determine what activities the applications in your custom ruleset are allowed to execute. These activities are called 'Access Names'.



Refer to the section **HIPS Behavior Settings > Activities to Monitor** to view a list of definitions of the Action Names listed above and the implications of choosing the action from 'Ask', 'Allow' or 'Block' for each setting as shown below:



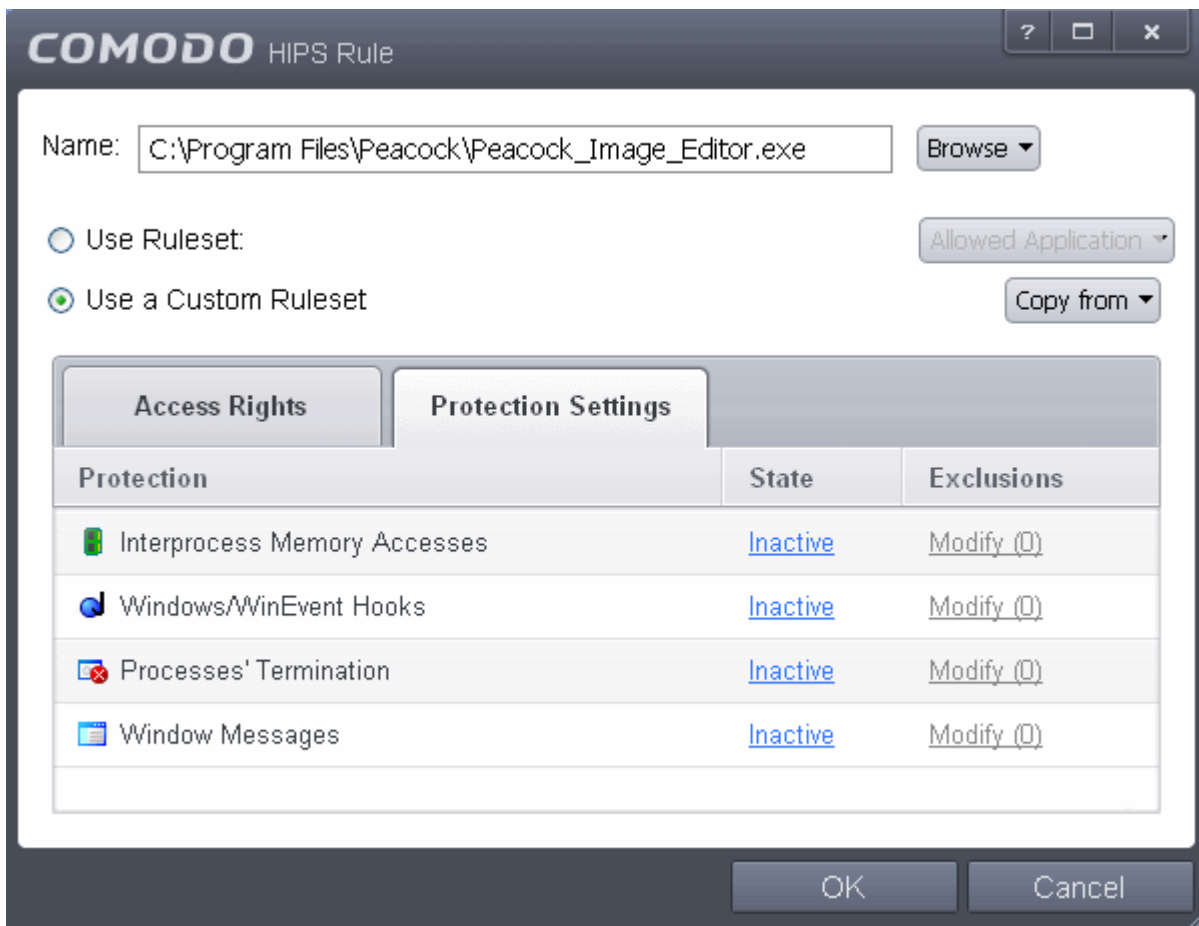
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.



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 'Peacock_Image_Editor.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'opera.exe' to the 'Allowed Applications' tab creates an exception to this rule. Peacock_Image_Editor.exe can now modify the memory space of 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

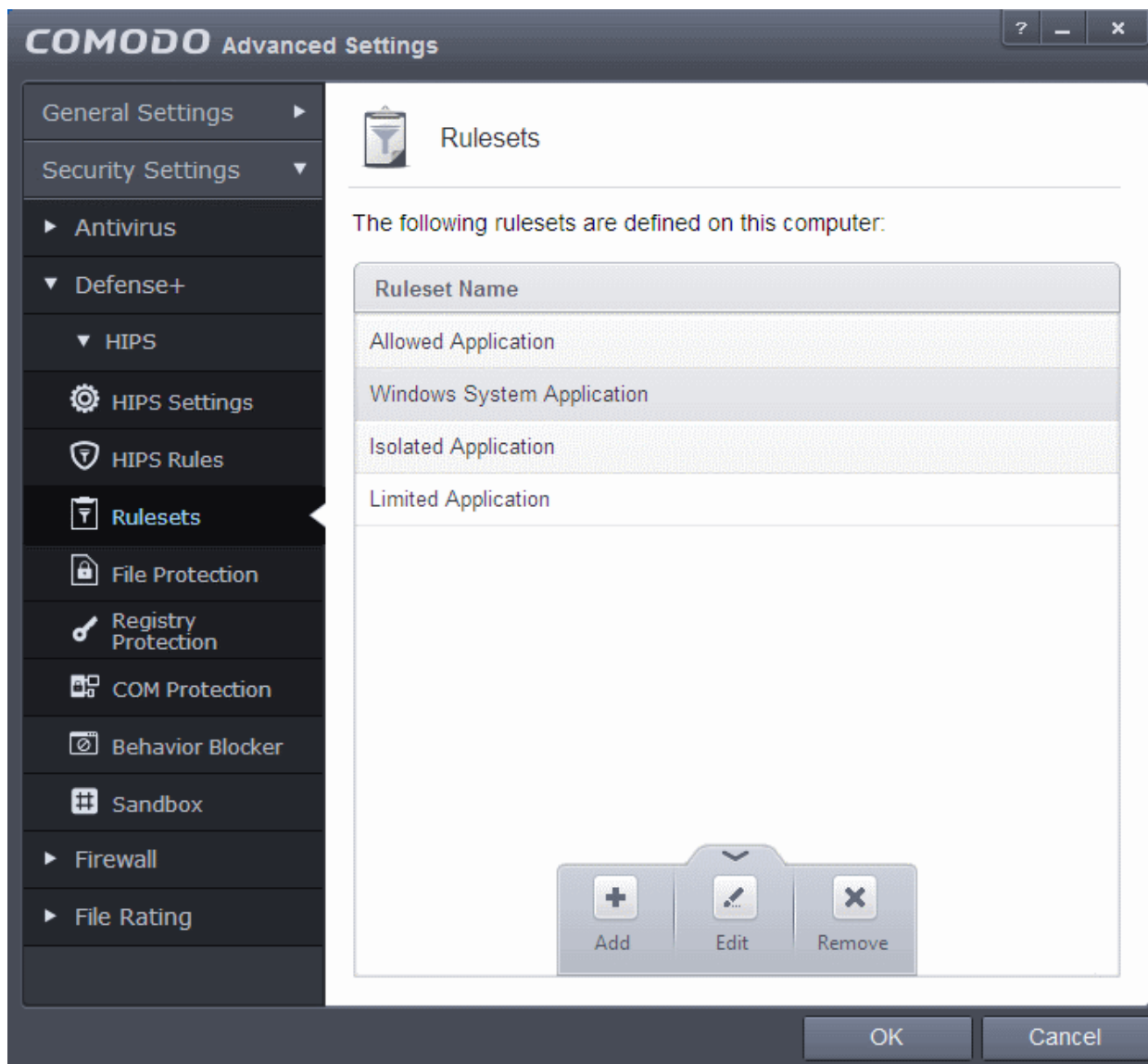
A Pre-defined ruleset is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined 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 'Ruleset Name' column.



To view or edit an existing predefined ruleset

- Double click on the Ruleset in the list
or
- Select the Ruleset, click the handle at the bottom of the interface and choose 'Edit' from the options.

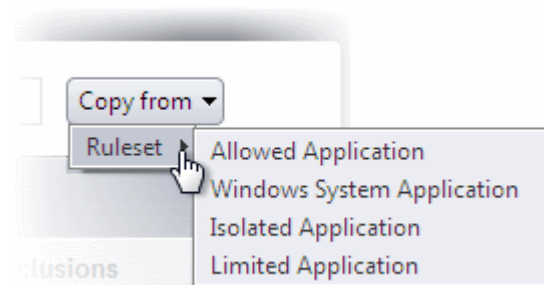
From here, you can modify a ruleset and, if desired, make changes to its **'Access Rights'** and **'Protection Settings'**. Any changes you make here are automatically rolled out to all applications that are currently applied with the ruleset.

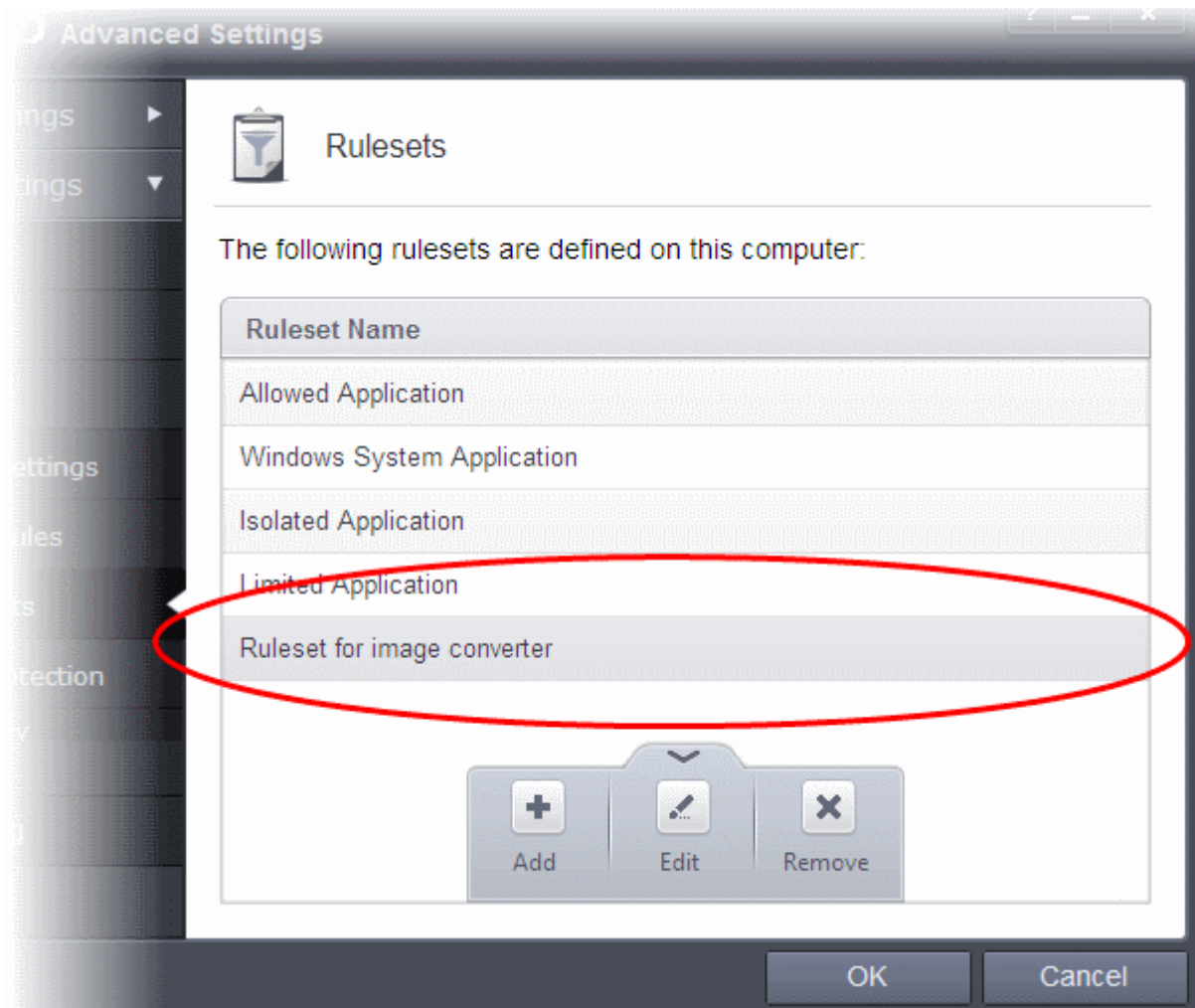
To create a new predefined ruleset

- Click up arrow at the bottom of the interface and choose 'Add' from the options.



- 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.



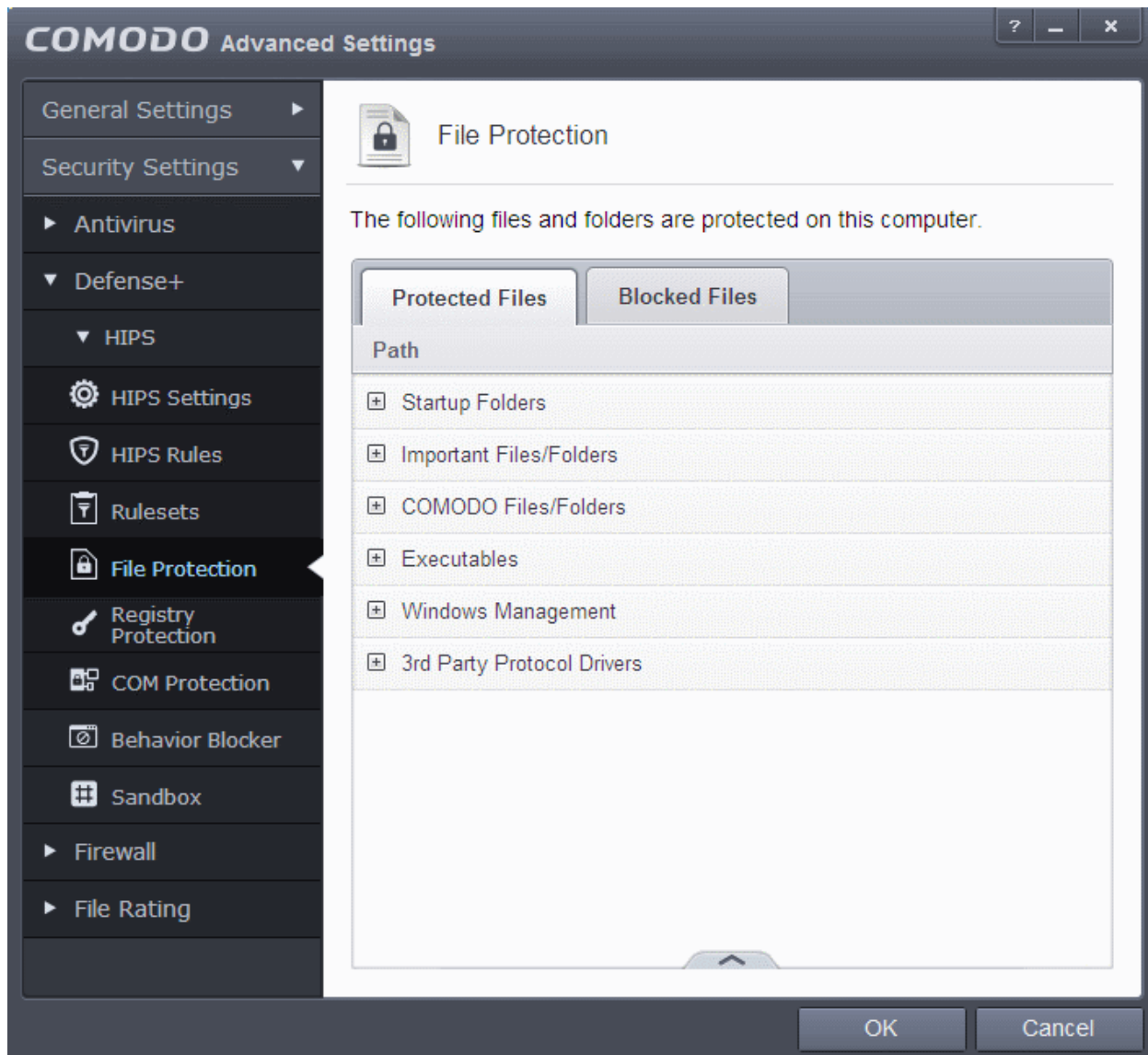


Once created, your ruleset is available for deployment onto specific application or file groups via the **Active HIPS Rules** interface.

6.2.2.4. Protected Files and Folders

The File Protection panel allows you to protect specific files and folders against access or modification by unauthorized processes and services.

The File Protection panel can be accessed by clicking Security Settings > Defense+ > HIPS > File Protection from the Advanced Settings interface.

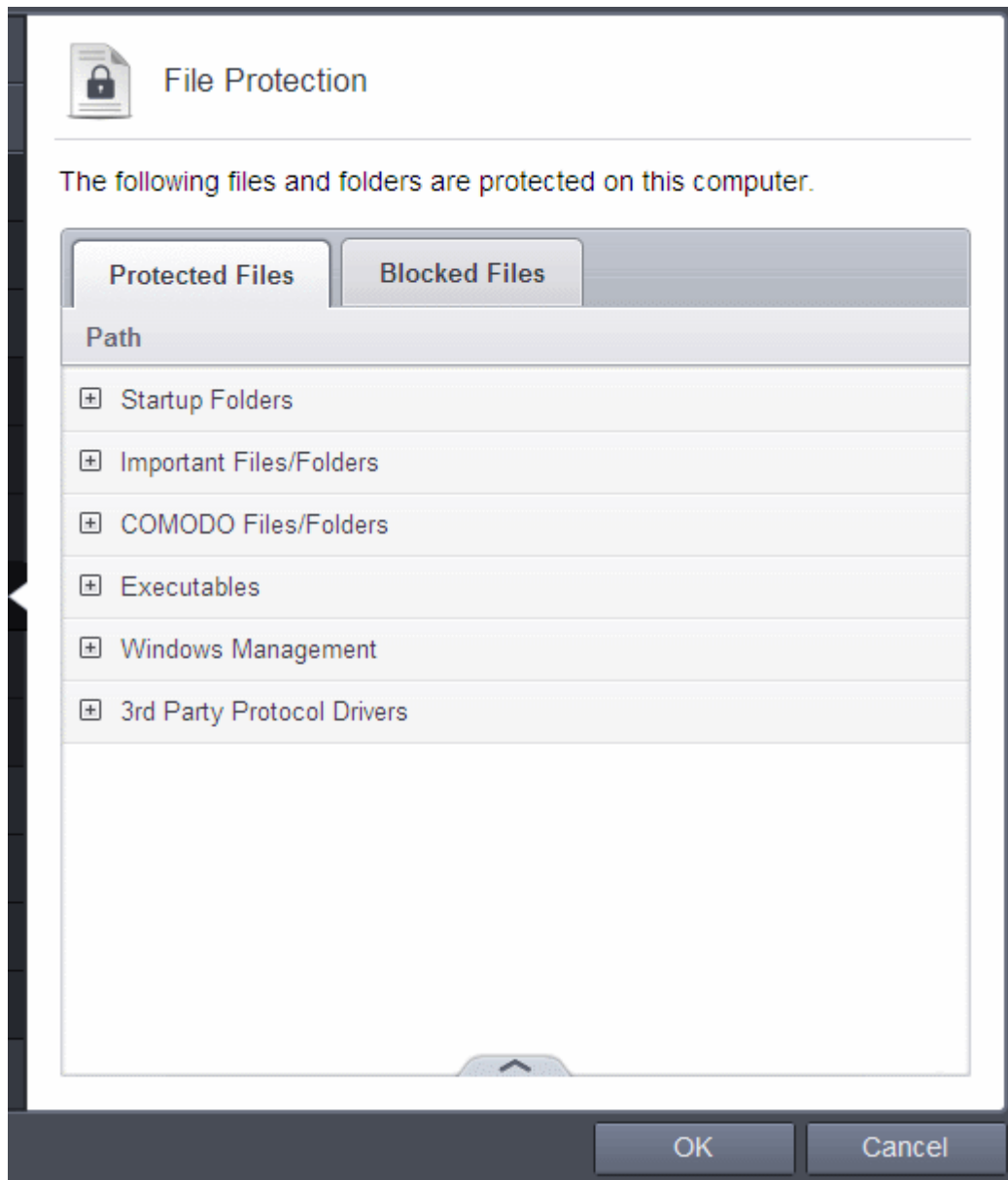


The panel has two tabs:

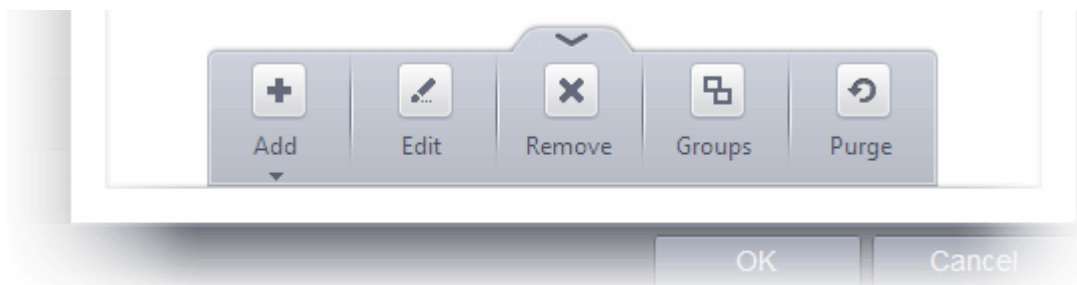
- **Protected Files** - Allows you to specify programs, applications and files that are to be protected from changes
- **Blocked Files** - Allows you to specify programs, applications and files that are to be blocked from execution and opening

6.2.2.4.1. Protected Files

The Protected Files tab displays a list of files and file groups that are protected from access by other programs, especially malicious programs such as virus, Trojans and spyware. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying anyone and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is the your 'hosts' file. (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files 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.



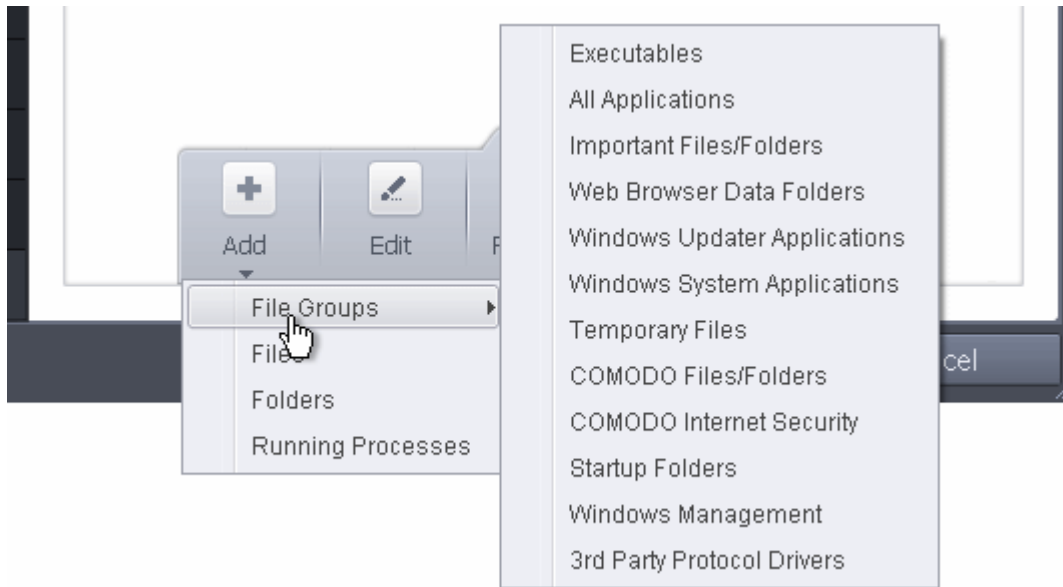
Clicking the handle at the bottom of the interface opens an options panel with the following options:



- **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.
- **Groups** - Opens the Manage Groups interface that allows you to edit pre-defined file groups and define new file groups for inclusion in Protected Files list
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path

specified. If not, the file or the file group is removed, or 'purged', from the list.

To manually add an individual file, folder, file group or process



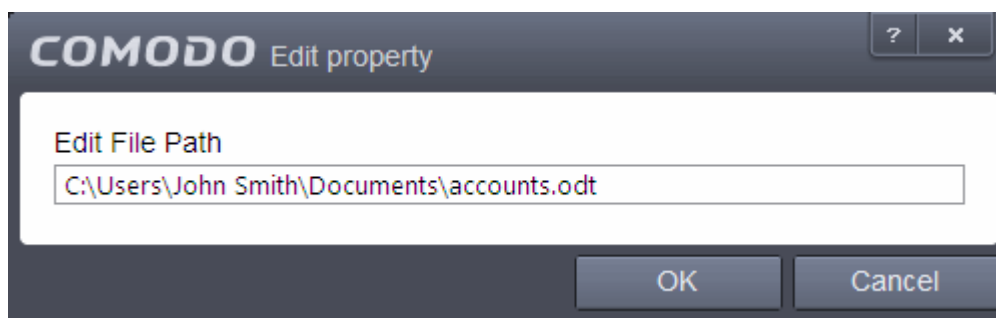
- Click the handle from the bottom center and select 'Add'.

You can add the files by following methods:

- **Selecting from File Groups**
- **Selecting from currently running Processes**
- **Browsing to the File**
- **Browsing to the Folder**

To edit an item in the Protected Files list

- Select the item from the list, click the up arrow from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit the file path, if you have relocated the file and click OK

To delete an item from Protected Files list

- Select the item from the list, click the up arrow from the bottom and select 'Remove'.

The selected item will be deleted from the protected files list. CIS will not generate alerts, if the file or program is subjected to unauthorized access.

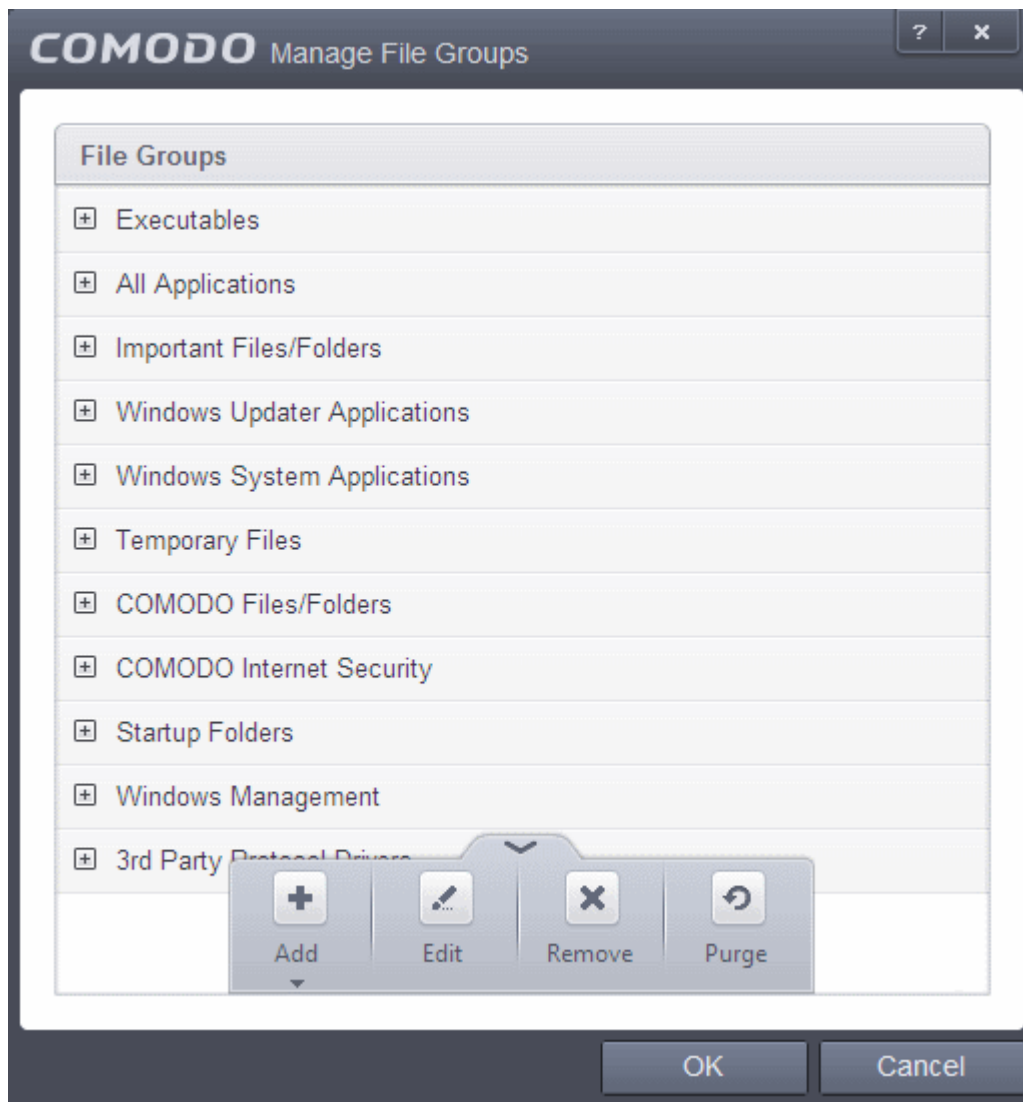
File Groups

File groups are handy, predefined groupings of one or more file types. Creating a file group allows you to quickly deploy a ruleset across multiple file types and applications.

To open the Manage File Groups interface

1. Click the Up arrow from the bottom center of Protected Files interface and select 'Groups'.

The Manage File Groups interface will open.

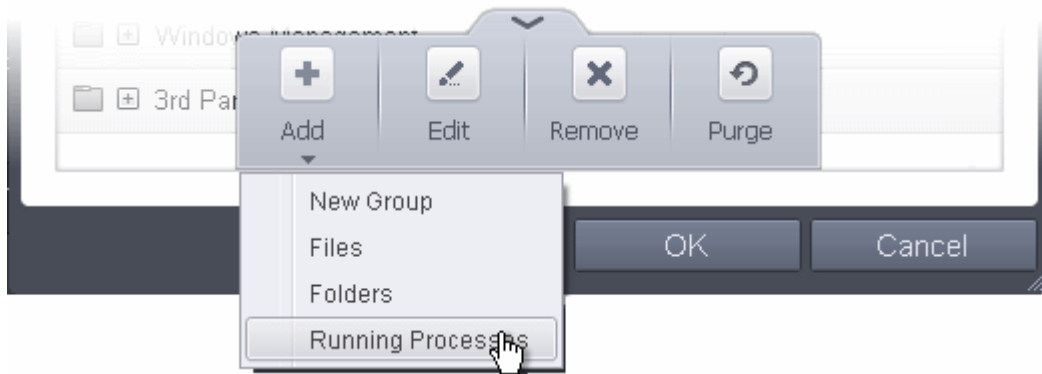


This interface allows you to

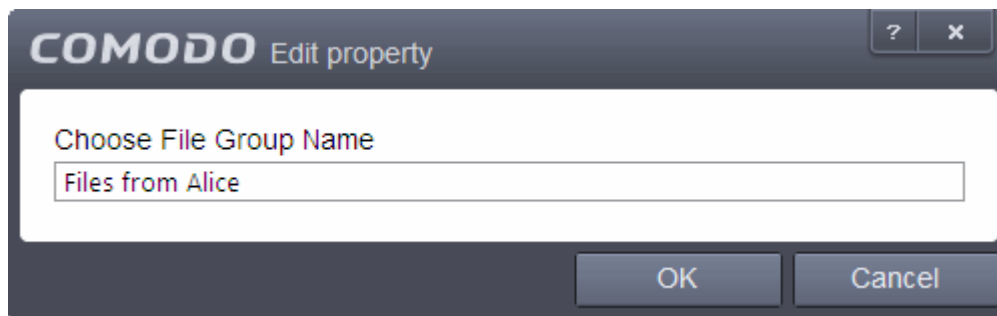
- **Create a new File Group**
- **Edit the names of an Existing File Group**
- **Add a file to an existing file group**
- **Remove existing file group(s) or individual file(s) from existing group**

Note: This area is for the creation and modification of file groups only. You are not able to modify the security ruleset of any applications or files from here. To do that, you should use the **HIPS Rules** interface or the **Predefined Rules** Interface.

- To add a new group or add files to an existing group, click the up arrow 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

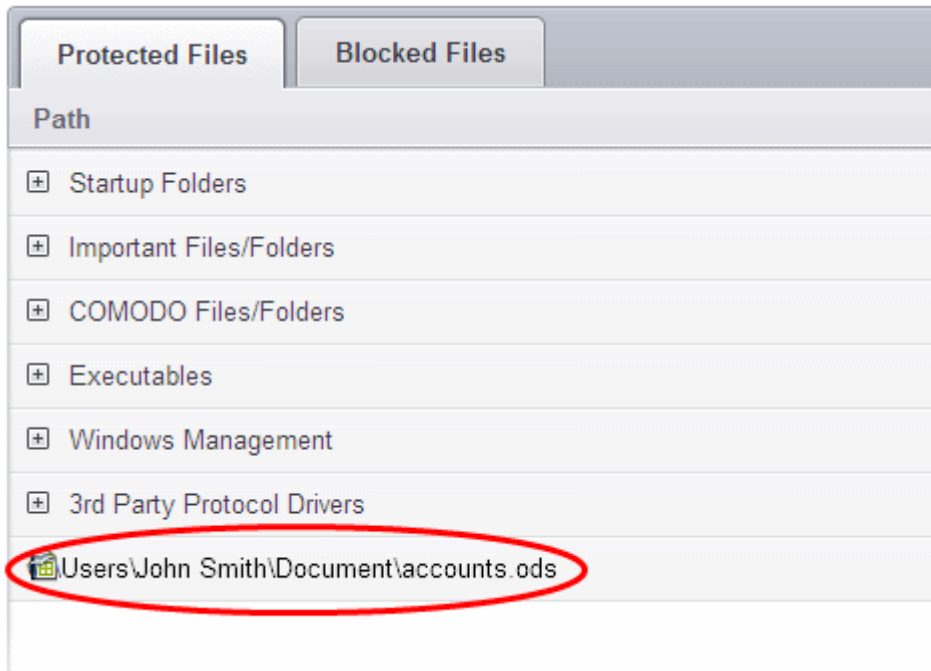


- **Add files to a group** - Select the Group, click the handle and select Add. Choose from 'Files', 'Folders' or 'Running Processes' to add files by **browsing to the file or folder** or from **currently running processes**
- To edit an existing group, select the group, click the handle and choose Edit. 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 file to be removed, click the handle and choose 'Remove'.

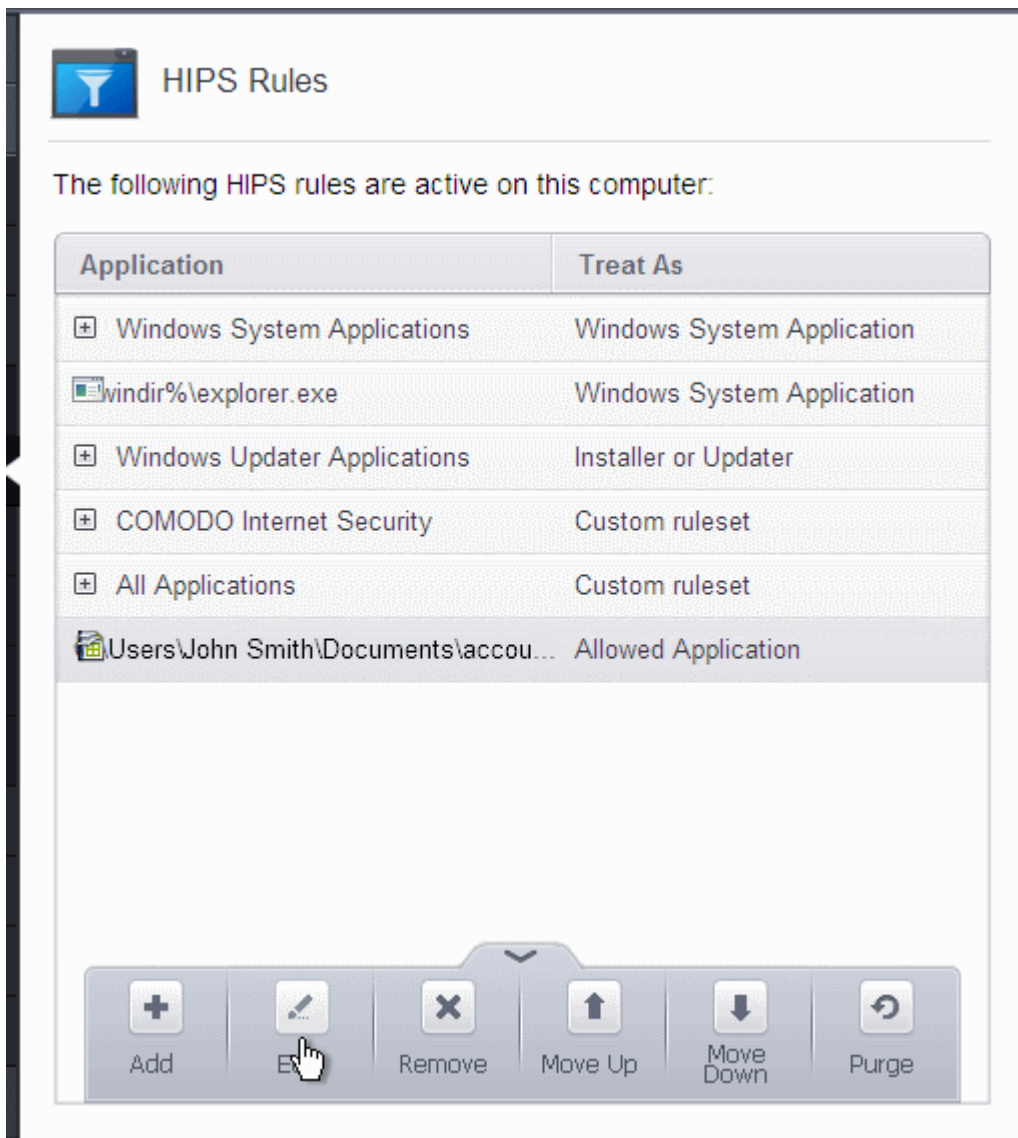
Exceptions

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 'scal' so that it alone could modify 'Accounts.ods'.

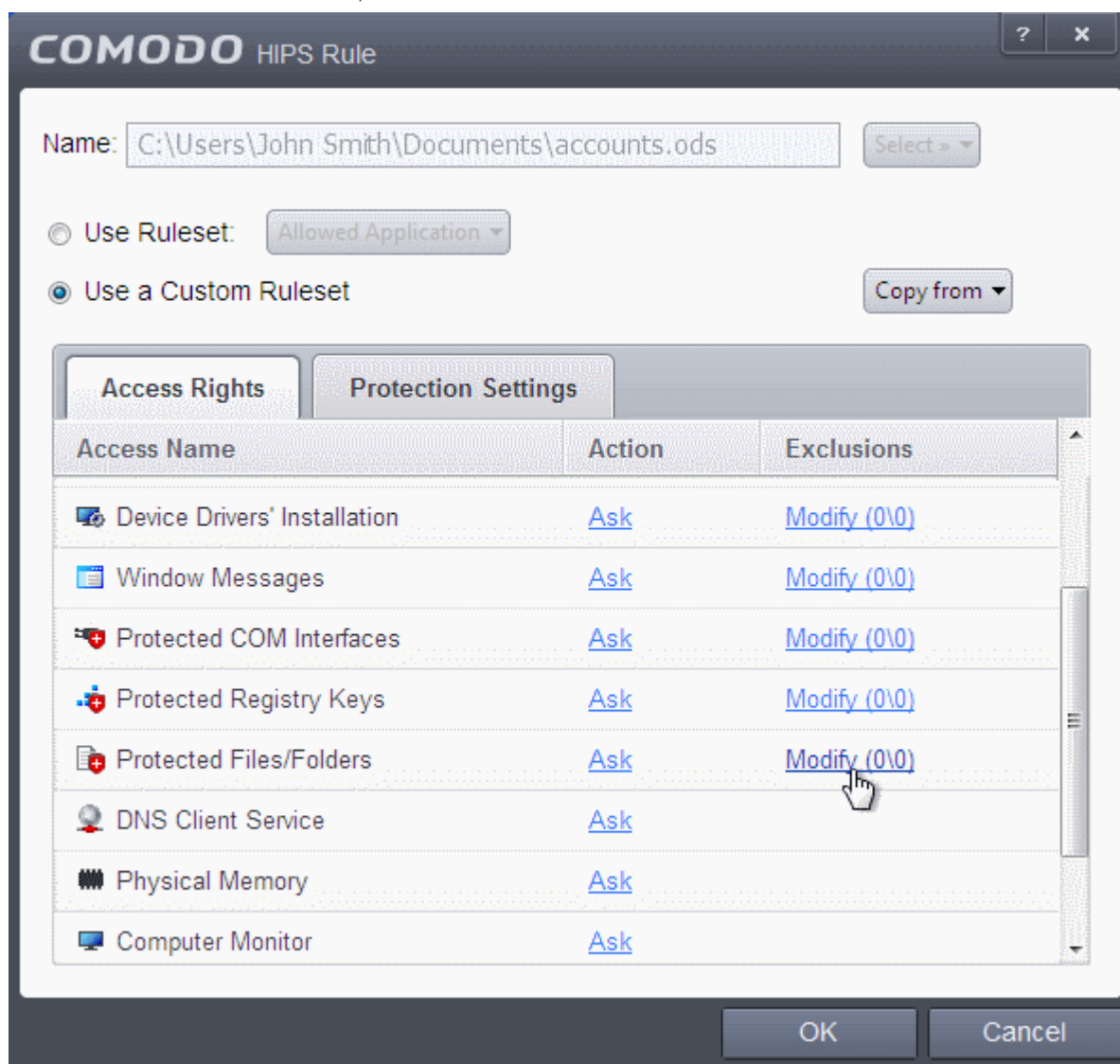
- First add Accounts.odt to Protected Files area.



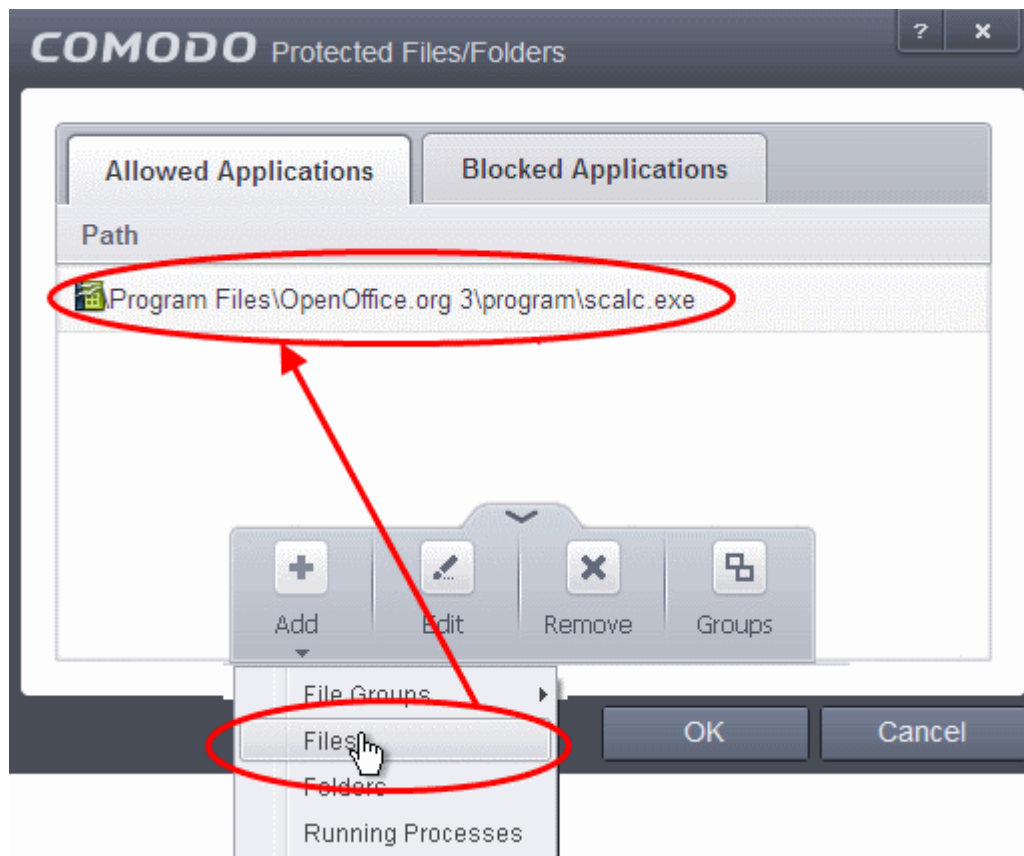
- Then go to HIPS Rules interface and add it to the list of applications. Click the up arrow and choose 'Edit'.



- In the HIPS Rule interface, select 'Use a custom rule set'.



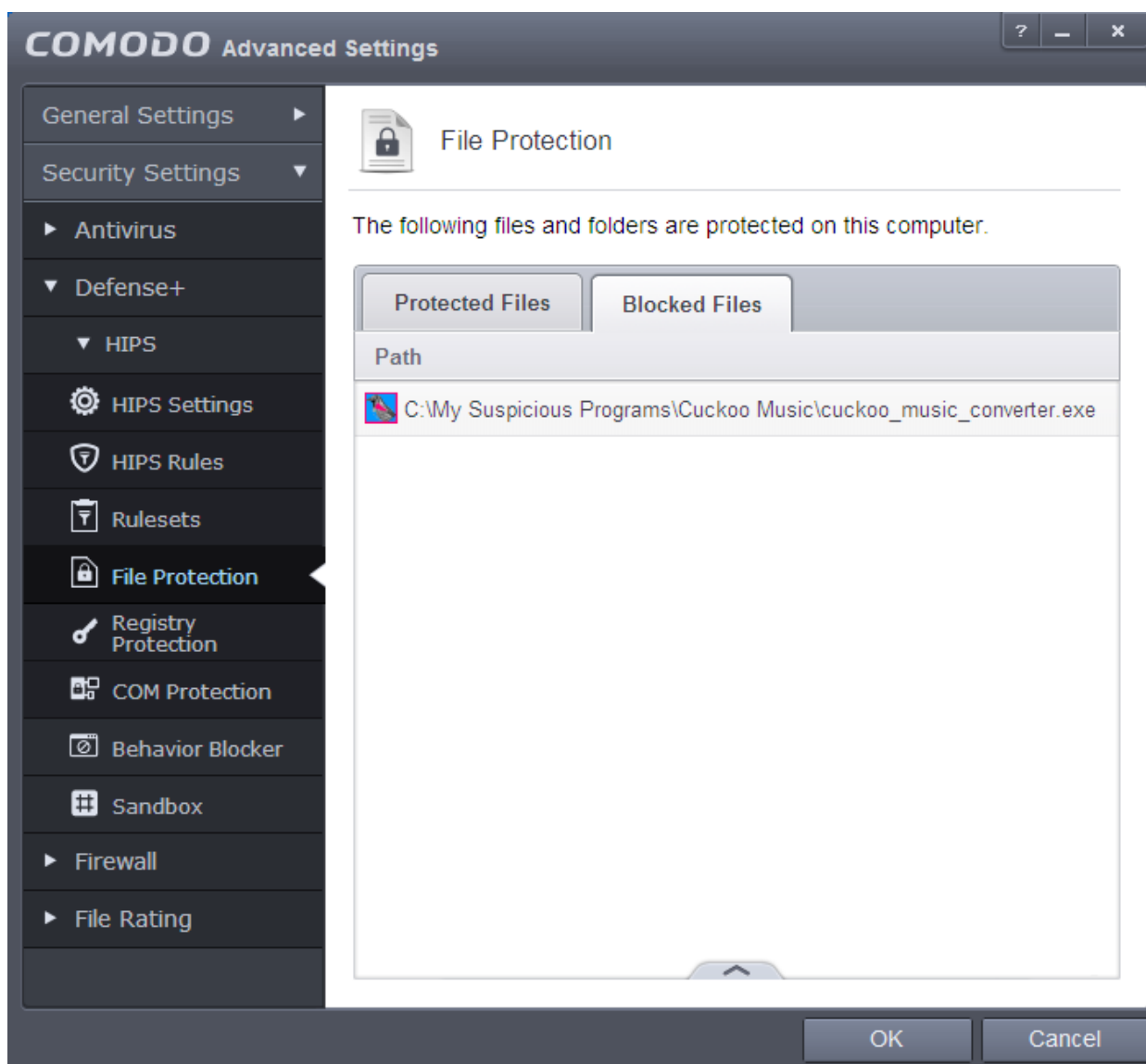
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the 'Access Rights'.



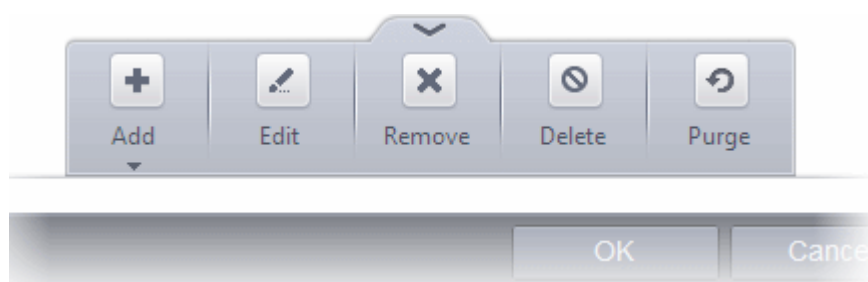
Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add 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:



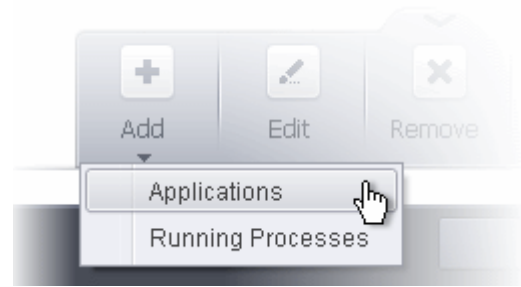
- **Add** - Allows you to add individual files, programs, applications to Blocked Files.
- **Edit** - Allows you to edit the path of the file.
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your computer
- **Purge** - 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.

To manually add an individual file or application

- Click the handle from the bottom center and select 'Add'.

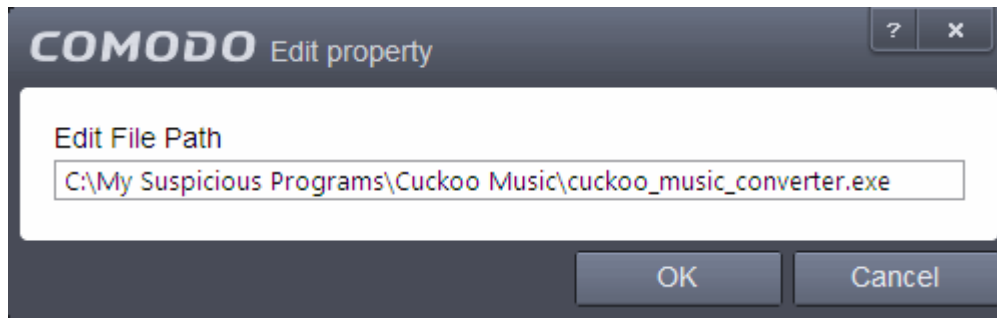
You can add the files by following methods:

- **Selecting from currently running Processes**
- **Browsing to File**



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'.

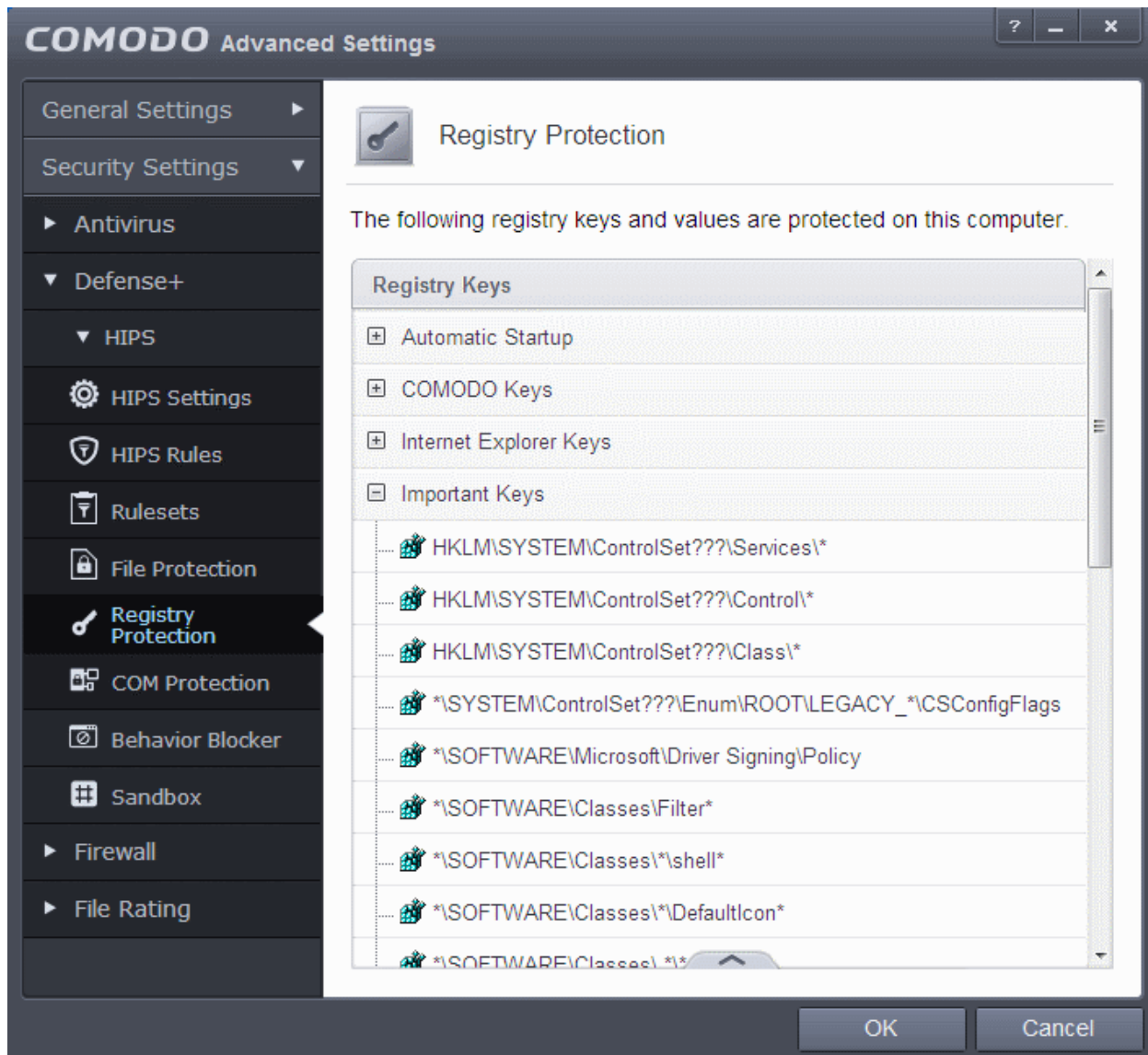
The selected item will be deleted from your computer immediately.

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'.

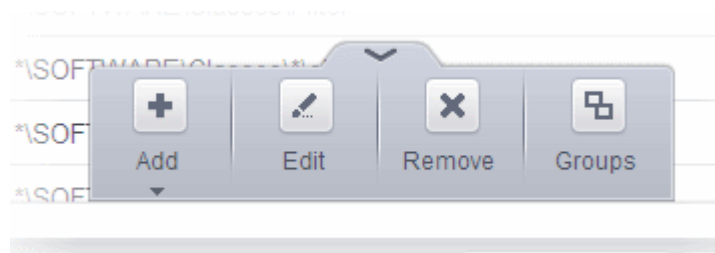
6.2.2.5. Protected Registry Keys

The 'Registry Protection' 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.

The 'Registry Protection' panel can be accessed by clicking Security Settings > Defense+ > HIPS > Registry Protection from the Advanced Settings interface.



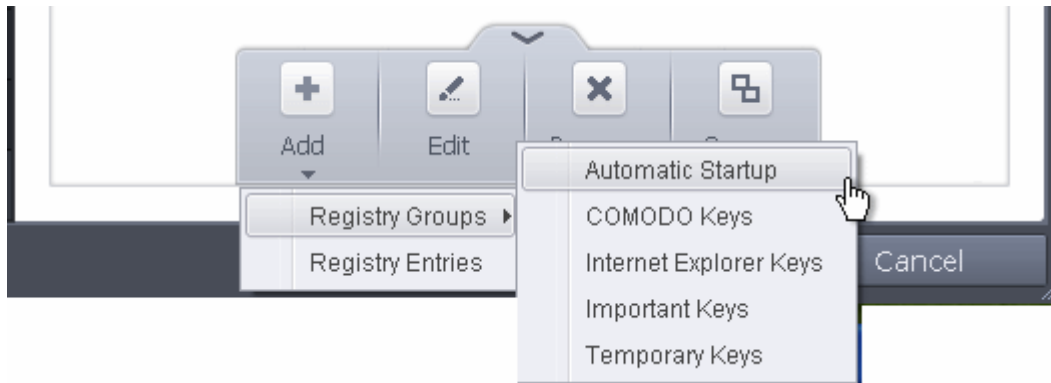
Clicking the handle at the bottom of the interface opens an options panel with the following options:



- **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.
- **Groups** - Opens the Manage Registry Groups interface that allows you to edit pre-defined Registry groups and define new Registry groups for inclusion in Registry Protection list.

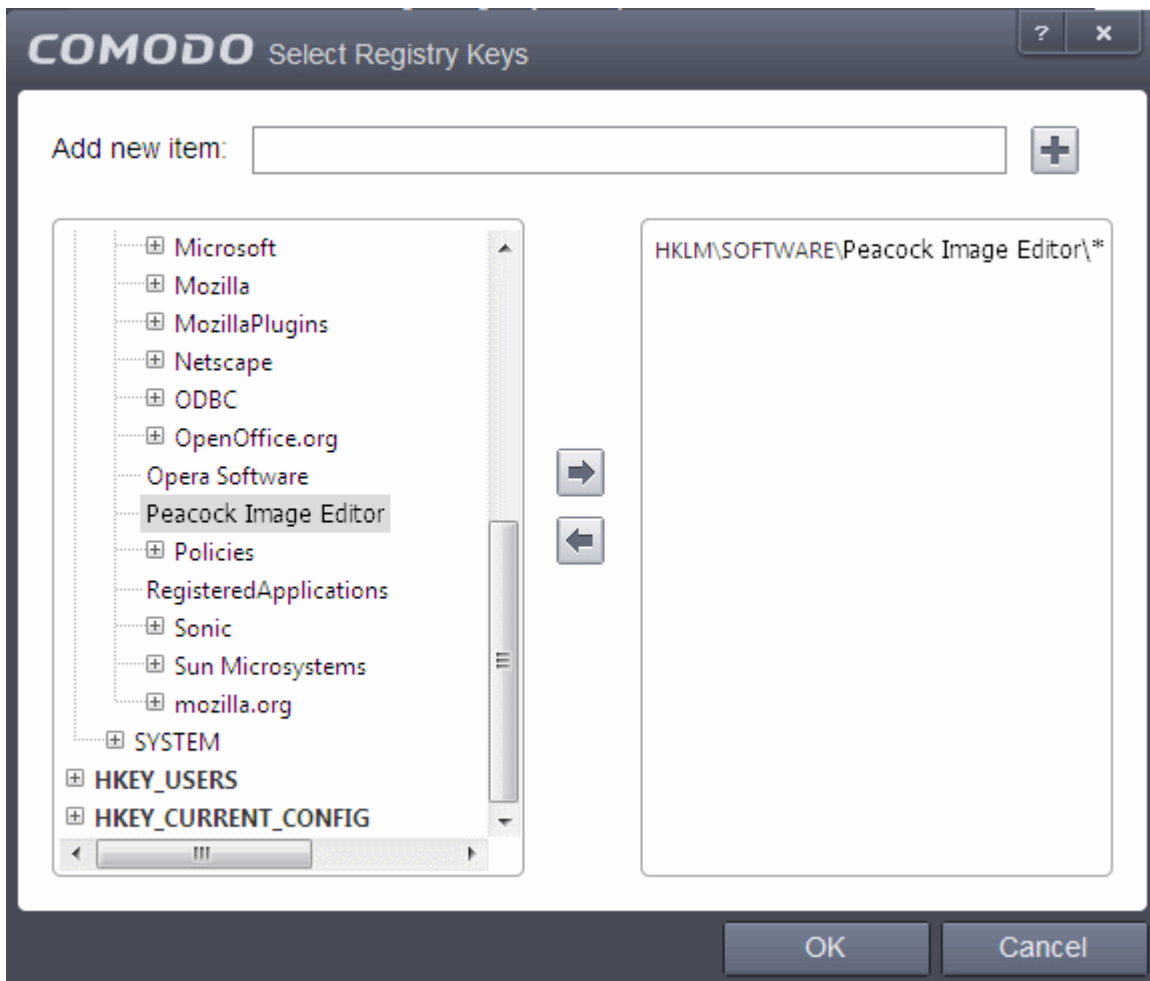
To manually add an individual Registry key or Registry Group

- Click the handle from the bottom center and select 'Add'.



You can add the items by following methods:

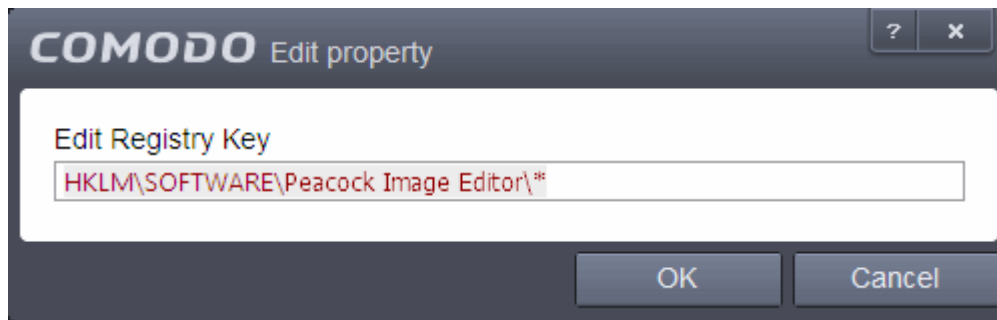
- **Adding Registry Groups** - Selecting Registry Groups allows you to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'. For explanations on editing existing registry groups and creating new groups refer to the section **Registry Groups**.
- **Adding individual Registry Keys** - Selecting 'Registry Entries' opens the 'Select Registry Keys'.



You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the Registry Protection list

- Select the key from the list, click the handle from the bottom and select Edit. The 'Edit Property' dialog will appear.



- Edit 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 the section **Registry Groups** for more details.

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.

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 Manage Registry Groups interface

1. Click the handle from the bottom center of Registry Protection interface and select 'Groups'.

The 'Manage Registry Groups' interface will open.



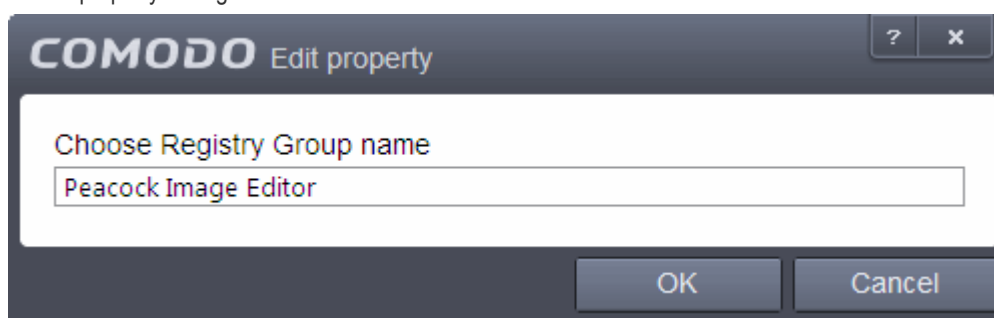
This interface allows you to

- **Create a new Registry Group**
- **Add Registry key(s) to an existing group**

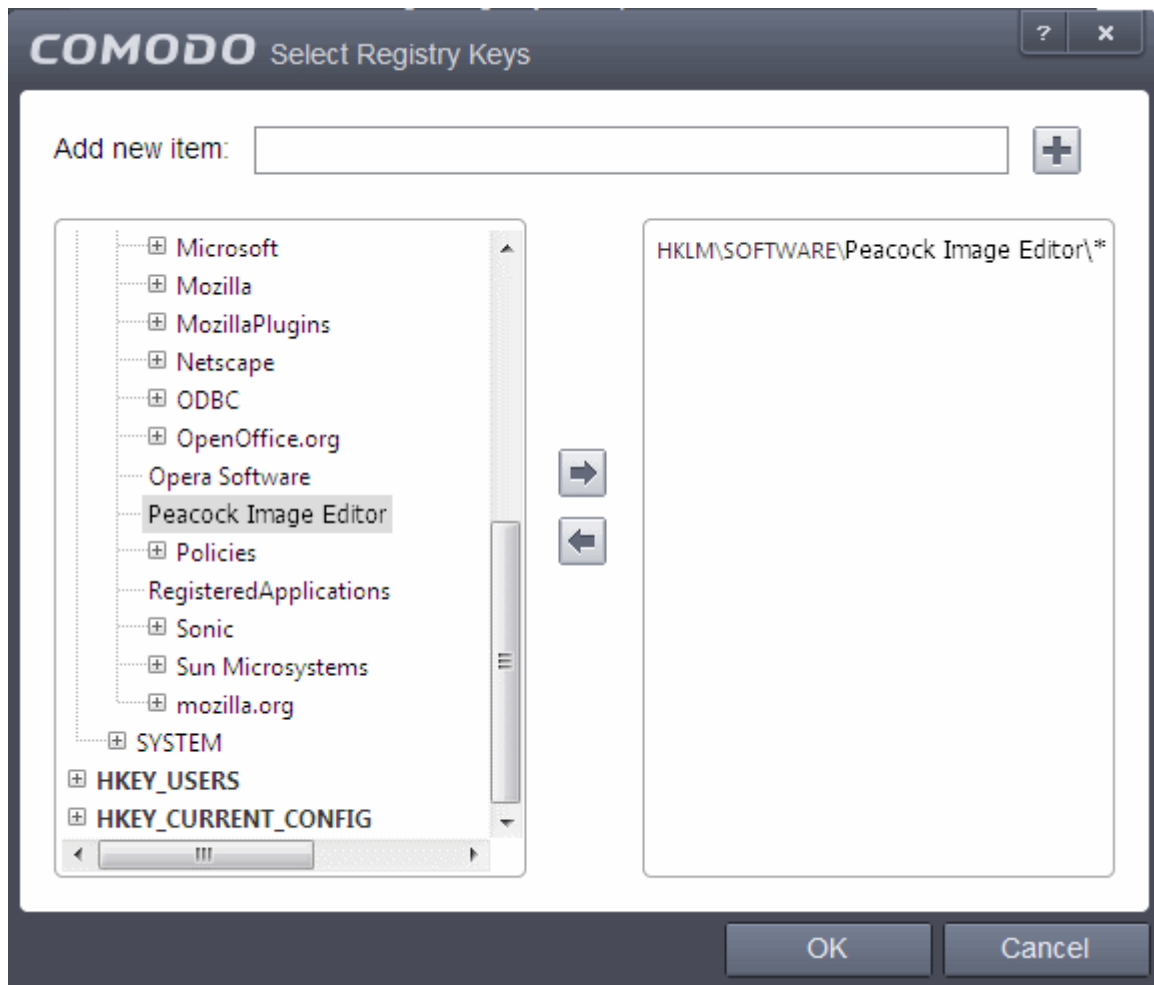
- **Edit the names of an Existing Registry Group**
- **Remove existing group(s) or individual key(s) from existing group**
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



- **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

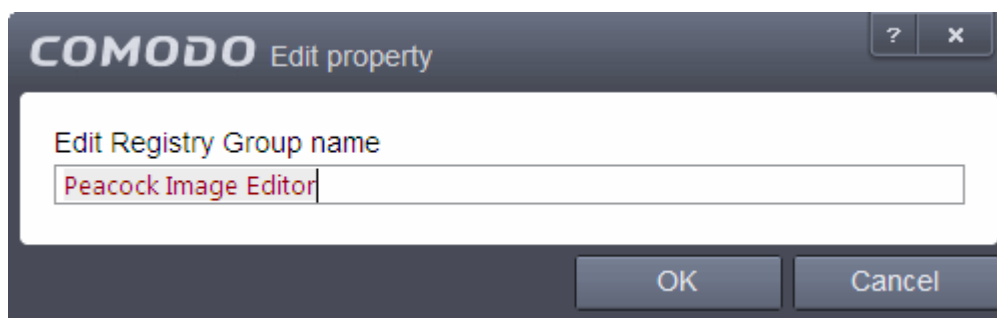


- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



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



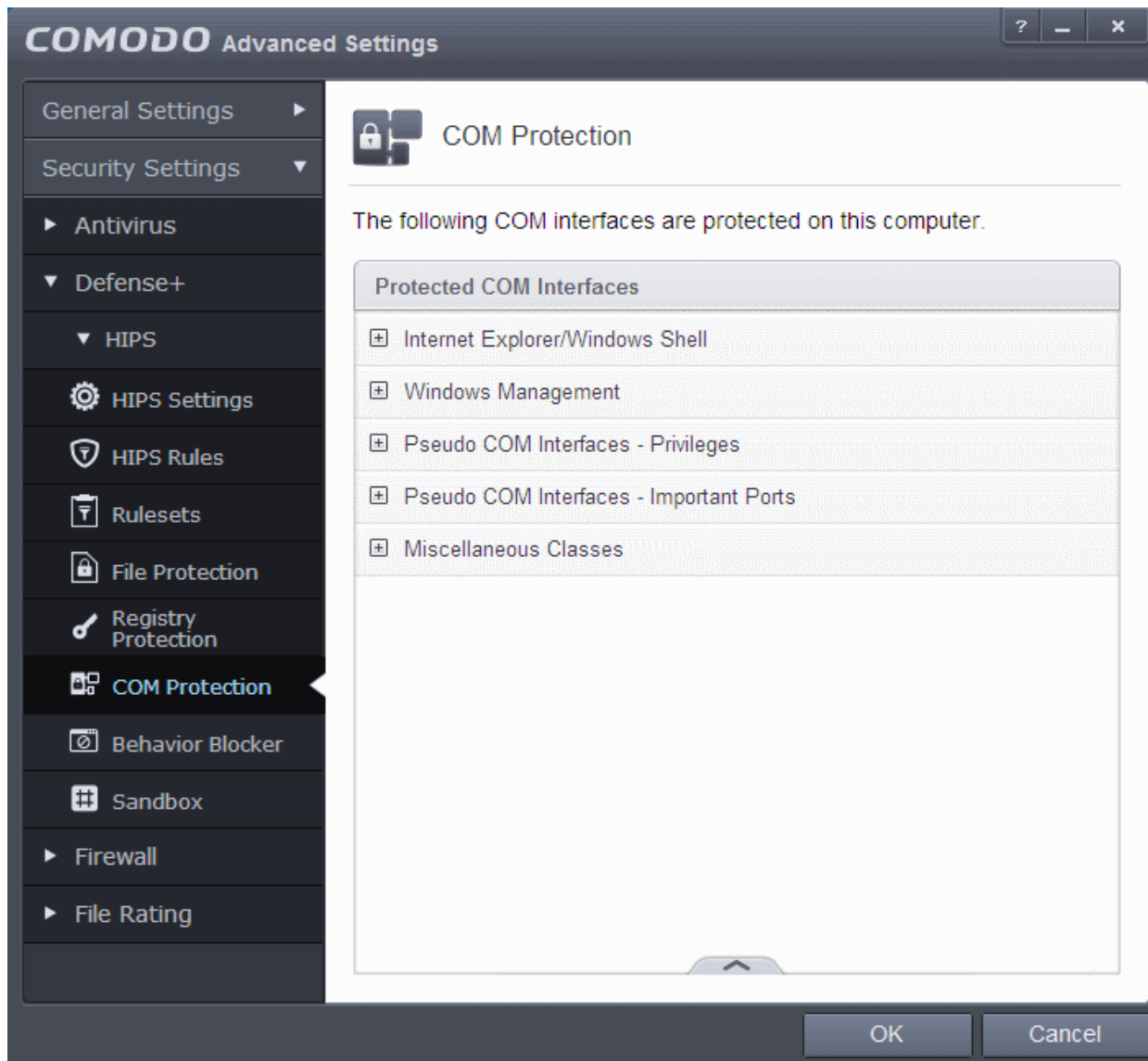
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.6. Protected COM interfaces

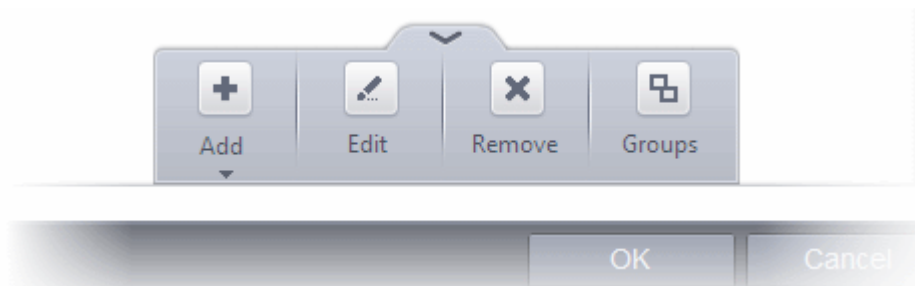
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers 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 Protection' panel 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. The 'COM Protection' panel can be accessed by clicking Security Settings > Defense+ > HIPS > COM Protection from the Advanced Settings interface.



Clicking the handle at the bottom of the interface opens an options panel with the following options:

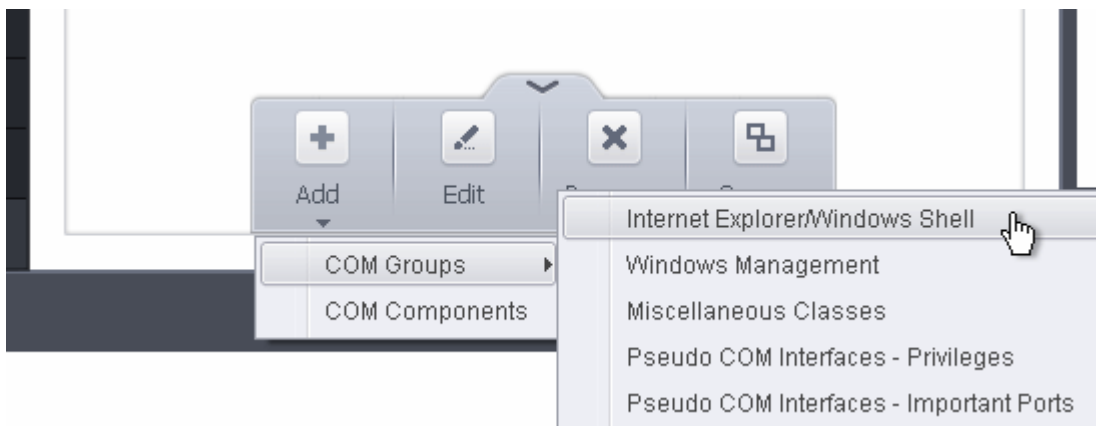


- **Add** - Allows you to add COM groups or individual COM components to COM Protection list.
- **Edit** - Allows you to edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.
- **Groups** - Opens the Manage COM Groups interface that allows you to edit pre-defined COM groups and define new

groups for inclusion in COM Protection list.

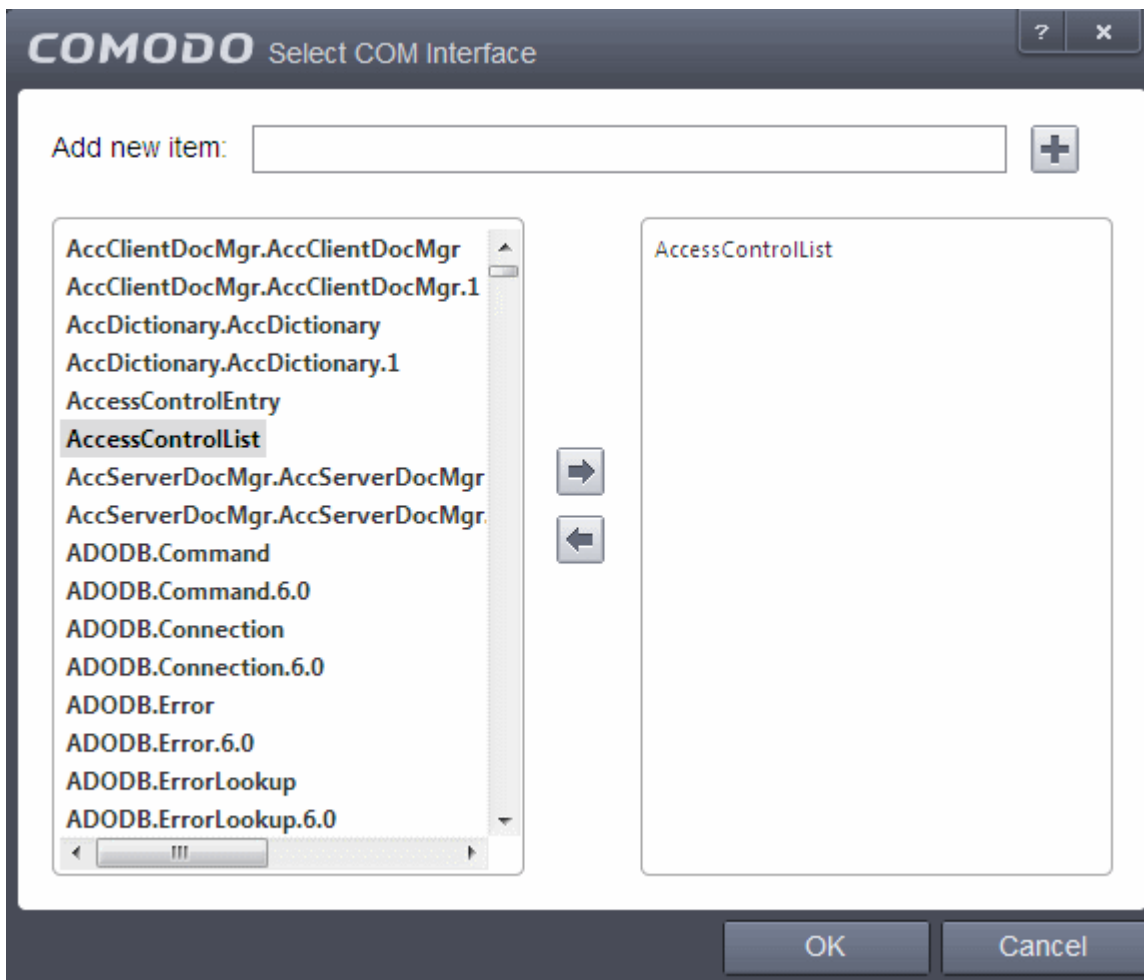
To manually add a COM Group or individual COM component

- Click the handle from the bottom center 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.

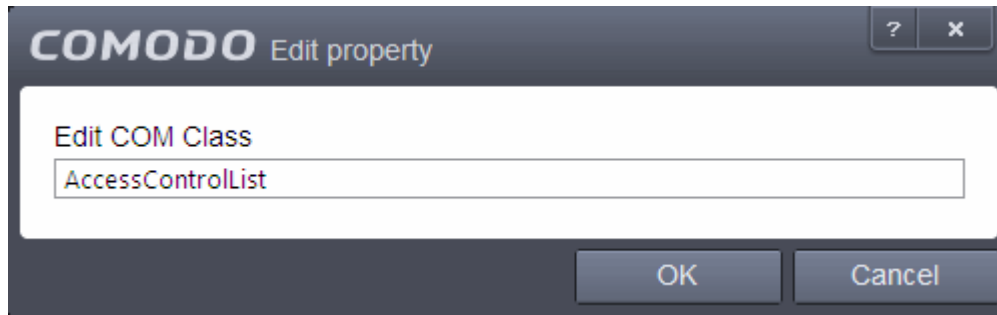


You can add items by selecting from the left hand side pane and moving it to right hand side pane by clicking the right

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.

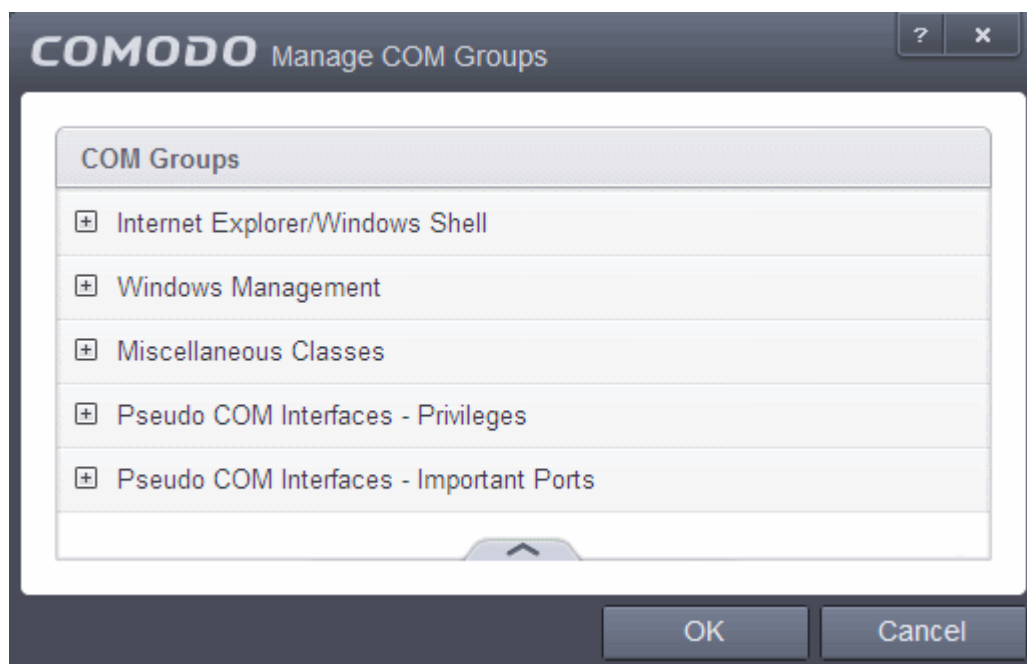
COM Groups

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

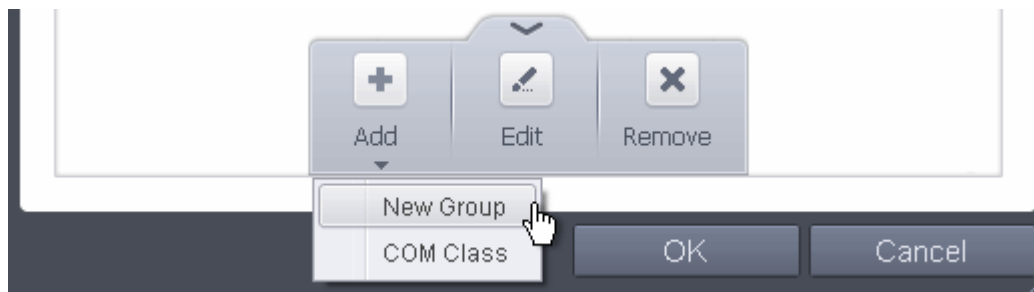
1. Click the handle from the bottom center of COM Protection interface and select 'Groups'.

The 'Manage COM Groups' interface will open.

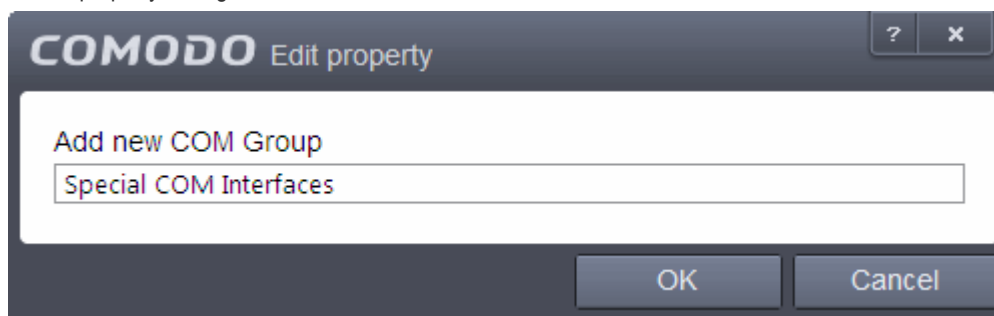


This interface allows you to:

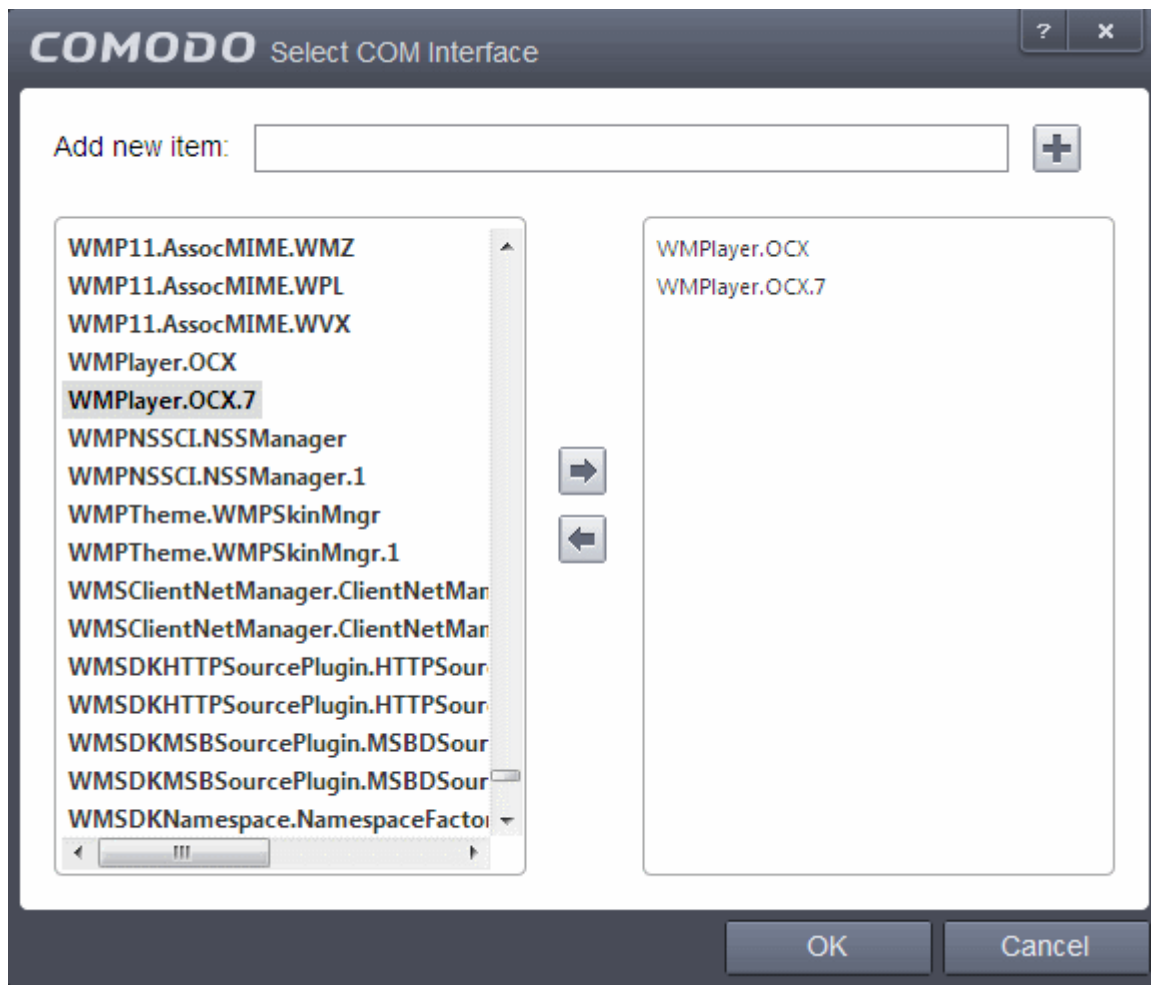
- **Create a new COM Group**
- **Add COM Component(s) to an existing group**
- **Edit the names of an Existing COM Group**
- **Remove existing group(s) or individual COM Component(s) from existing group**
- To add a new group or add new COM Component(s) to an existing group, click the handle from the 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.

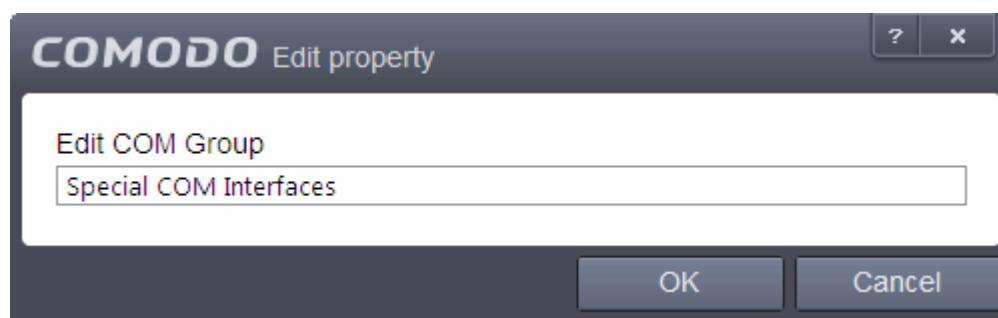


- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class'. The 'Select COM Interface' dialog will be opened.



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

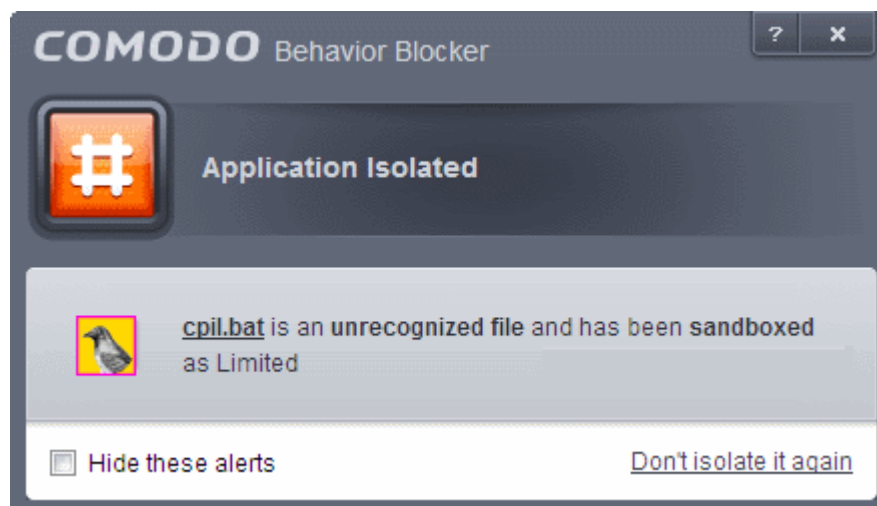
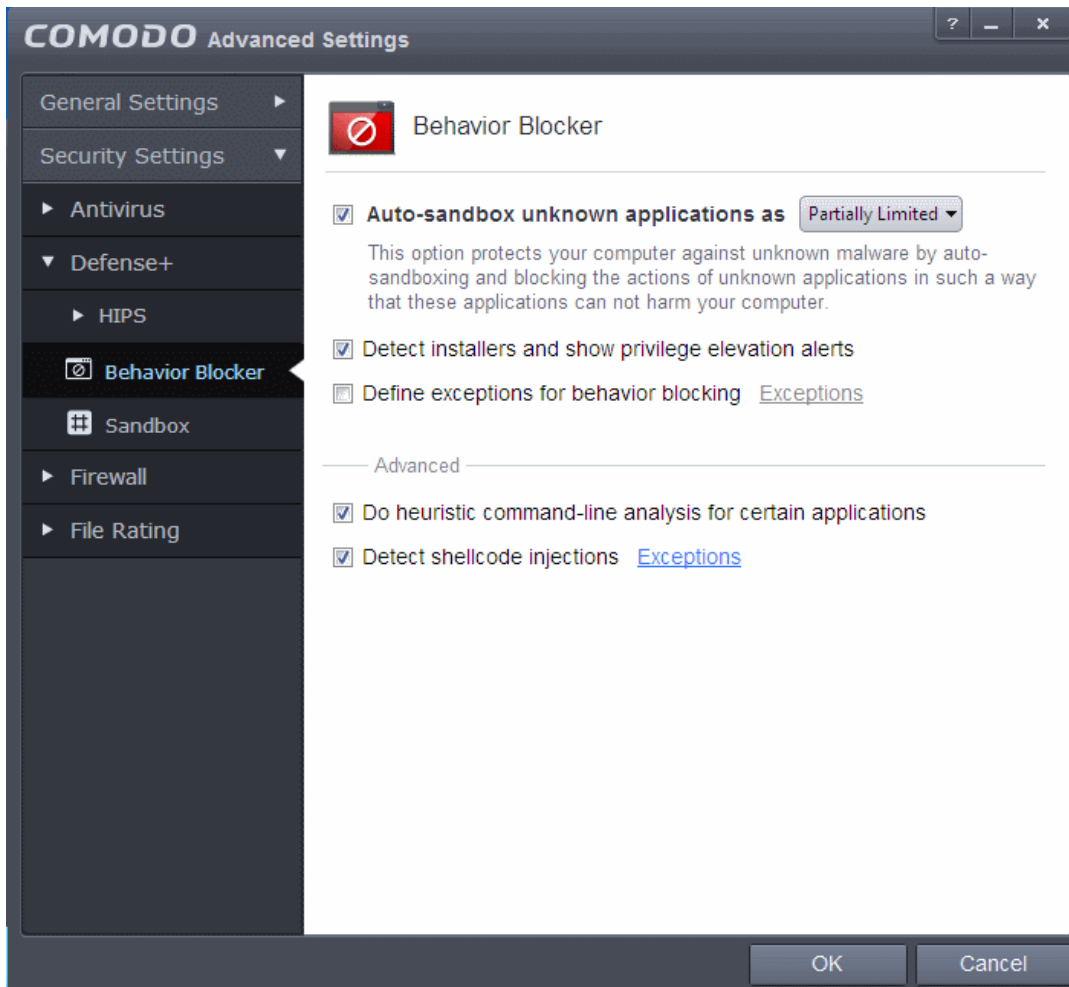


- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual COM Component from a group, click + at the left of the group to expand the group, select the item to be removed, click the handle and choose 'Remove'.

6.2.2.7. Behavior Blocker

The Behavior Blocker is an integral part of the Defense+ engine and is responsible for authenticating every executable image that is loaded into the memory. The Behavior Blocker intercepts all files before they are loaded into memory and intercepts prefetching/caching attempts for those files. It calculates the hash of the executable at the point it attempts to load into the memory. It then compares this hash with the list of known / recognized applications that are on the Comodo safe list. If the hash

matches the one on record for the executable, then the application is safe and the Behavior Blocker allows it to run. If no matching hash is found on the safelist, then the executable is 'unrecognized' and is run inside the auto-sandbox. You will be notified via an alert when this happens.



The 'Behavior Blocker' configuration panel can be accessed by clicking 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Defense + > Behavior Blocker'. This panel allows you to quickly determine how proactive the Behavior Blocker should be and which types of files it should check.

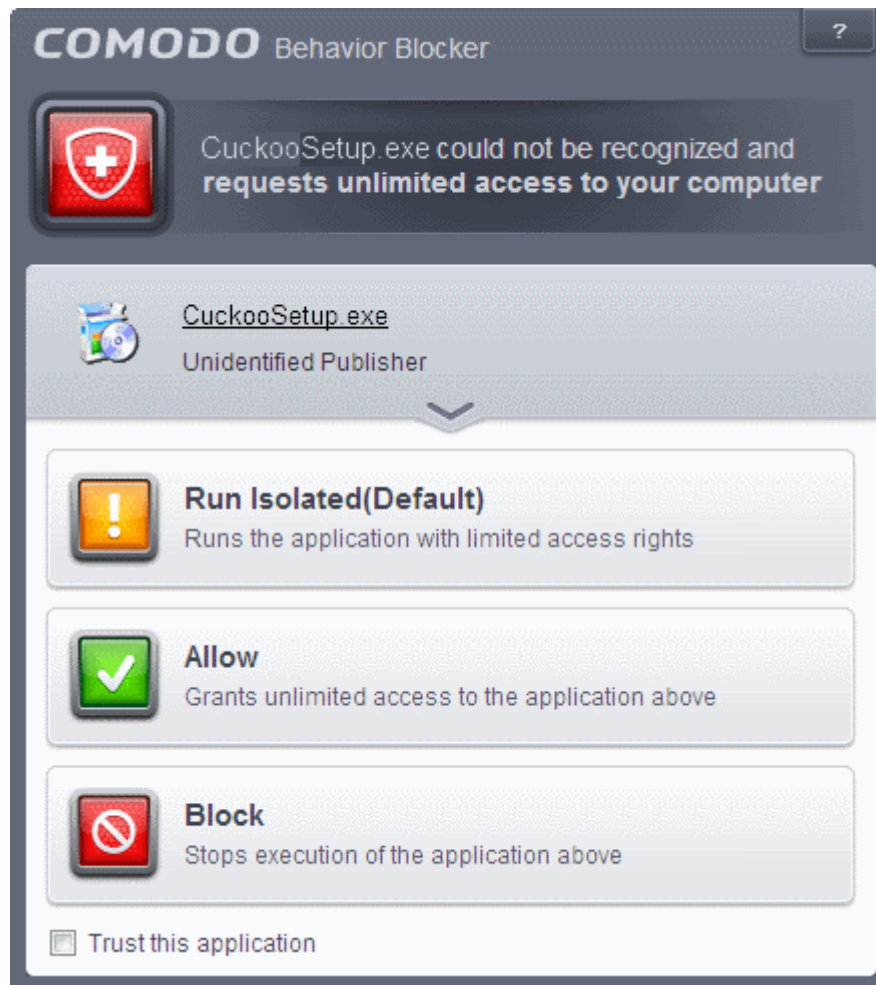
- **Auto-sandbox unknown applications as** - Allows you to enable or disable the Behavior Blocker. If enabled, the Behavior Blocker runs unrecognized applications inside the auto-sandbox with the access restriction as selected in the drop down menu. (Default = 'Enabled' with 'Partially Limited')

Note: The 'auto-sandbox' referred to here is distinct to the fully virtualized sandbox/Virtual Kiosk discussed in [Sandbox Tasks](#). The 'auto-sandbox' is a non-virtual environment under which unrecognized applications are run allowed to run under a set of access restrictions (default='Partially Limited'). These restrictions prevent the application from taking actions that are damaging to your system. Advanced users can, however, make a [registry change to enable 'Full Virtualization'](#) of auto-sandboxed files.

Configuring Access Restriction

Access restriction levels determine the amount of privileges an auto-sandboxed application has to access other software and hardware resources on your computer:

- **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.
- **Blocked** - The application is not allowed to run at all.
- **Fully Virtualized** - This option is not available by default but can be enabled by adding a registry key (advanced users only). To do this, open the registry editor and browse to HKLM > SYSTEM > software > Comodo > Firewall Pro. Add a DWORD key to this hive named EnableDefaultVirtualization and set the value to 1. 'Fully Virtualized' will now be listed in the auto-sandbox restriction level drop down.
- **Detect installers and show privilege alerts:** Allows you to instruct the Behavior Blocker to display alerts when an 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. Refer to the section [Understanding Security Alerts](#) for more details.



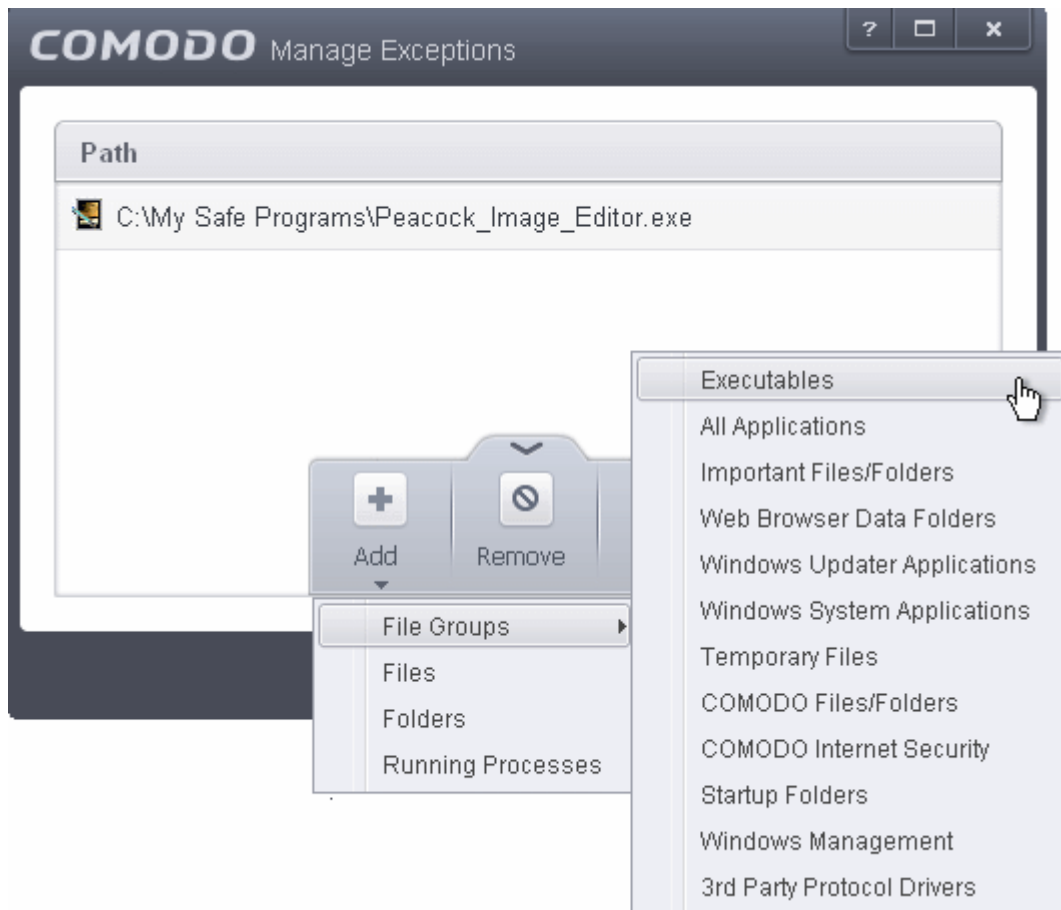
You can decide on whether or not to allow the installer or the unknown application based on your assessment, from the alert itself. (*Default=Enabled*)

- **Define exceptions for behavior blocking** - Allows you to add certain file paths for being excluded from monitoring by the Behavior Blocker. The executables included in the exceptions area are allowed to run without checking of authenticity. (*Default = Disabled*)

Note: The files added through this interface will be exempted only from monitoring by Behavior Blocker. To exclude a file from monitoring by all the components of CIS including Antivirus, Firewall, HIPS and Behavior Blocker, add it to **Trusted Files** list.

To define exceptions

- Select the 'Define exceptions for behavior blocking' checkbox and click the [Exceptions](#) link. The 'Manage Exceptions' dialog will appear.



- Click the handle at 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.
 - **Browse Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
 - **Browse File** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.
- Click 'OK' to implement your settings.

Advanced Settings:

- **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 wscript.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CIS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the Internet, for example, the alert will state 'test.vbs' is attempting to connect to the Internet (**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.

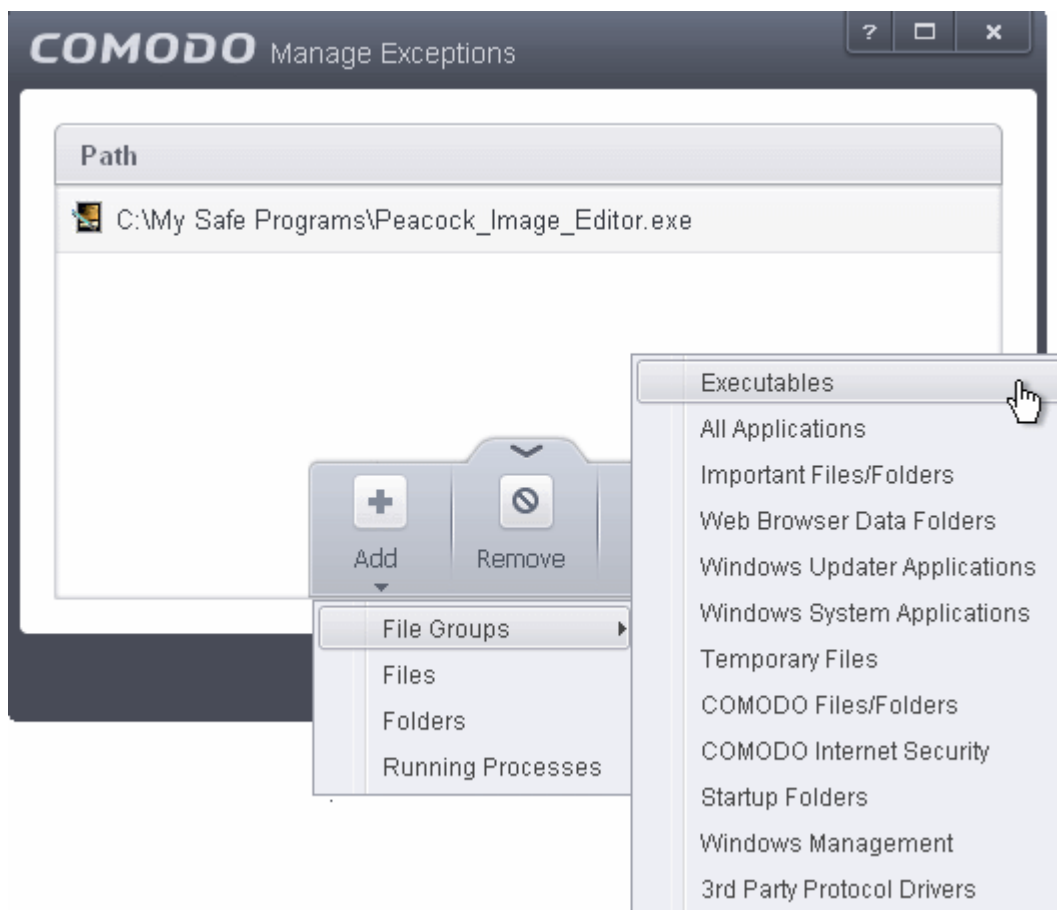
Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow 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. [Click here](#) for more details on the alerts.

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 [Exceptions](#) link. The 'Manage Exceptions' 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.

- **Browse Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
- **Browse File** - 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.

6.2.2.7.1. 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.

The smart application control mechanism performs security inspections whenever you start an application and automatically sandboxes any unknown application so that they can NOT do any harm to your system.

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.

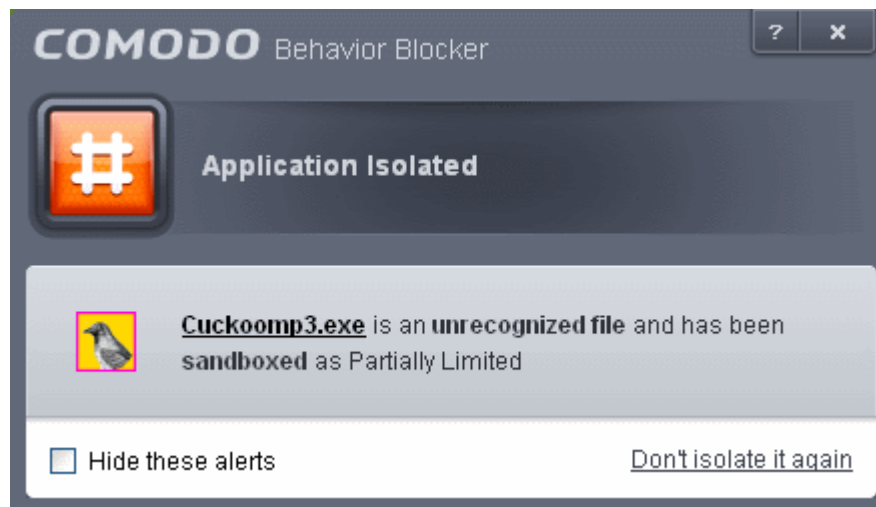
After an unknown application has been placed in the sandbox, CIS also automatically queues it for submission to Comodo Cloud Scanners for automatic behavior analysis. Firstly, the files undergo another antivirus scan on our servers. If the scan discovers the file to be malicious, then it is designated 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 'Unrecognized Files' (for execution within the sandbox) and will be submitted 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 2012 offers improved security, fewer pop-ups and greater ease of use than ever before.

6.2.2.7.2. Unknown Files: The Auto-Sandboxing and 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 added the application to the local **'Trusted Files'**
 - 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 Part 1**
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.
- **Sandbox and Cloud Scanning Part 2**
If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'. CIS simultaneously takes two distinct but complementary actions -
 - (1) It will run the unrecognized file in the auto-sandbox so that it cannot access important operating system files or damage your computer
 - (2) It will leverage Comodo's Cloud Scanning technology to determine whether the file behaves in a malicious fashion.
 - Unrecognized files and applications will be isolated and run in the auto-sandbox. CIS will alert the user that it is going to run the application in the sandbox.



- By default, auto-sandboxed applications are run with 'Partially Limited' restrictions.
More detail: Auto-sandboxed applications are allowed to run under a specific set of conditions or privileges. In CIS, these are known as 'Restriction Levels'. In part, auto-sandbox restriction levels are implemented by enforcing or relaxing the native access rights that Windows can grant to an application. There are five levels - Partially Limited, Limited, Restricted, Untrusted and Blocked. 'Partially Limited' is the default restriction level for auto-sandboxed applications, but you can change this to a different level in the Behavior Blocker Settings panel:
 - 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.

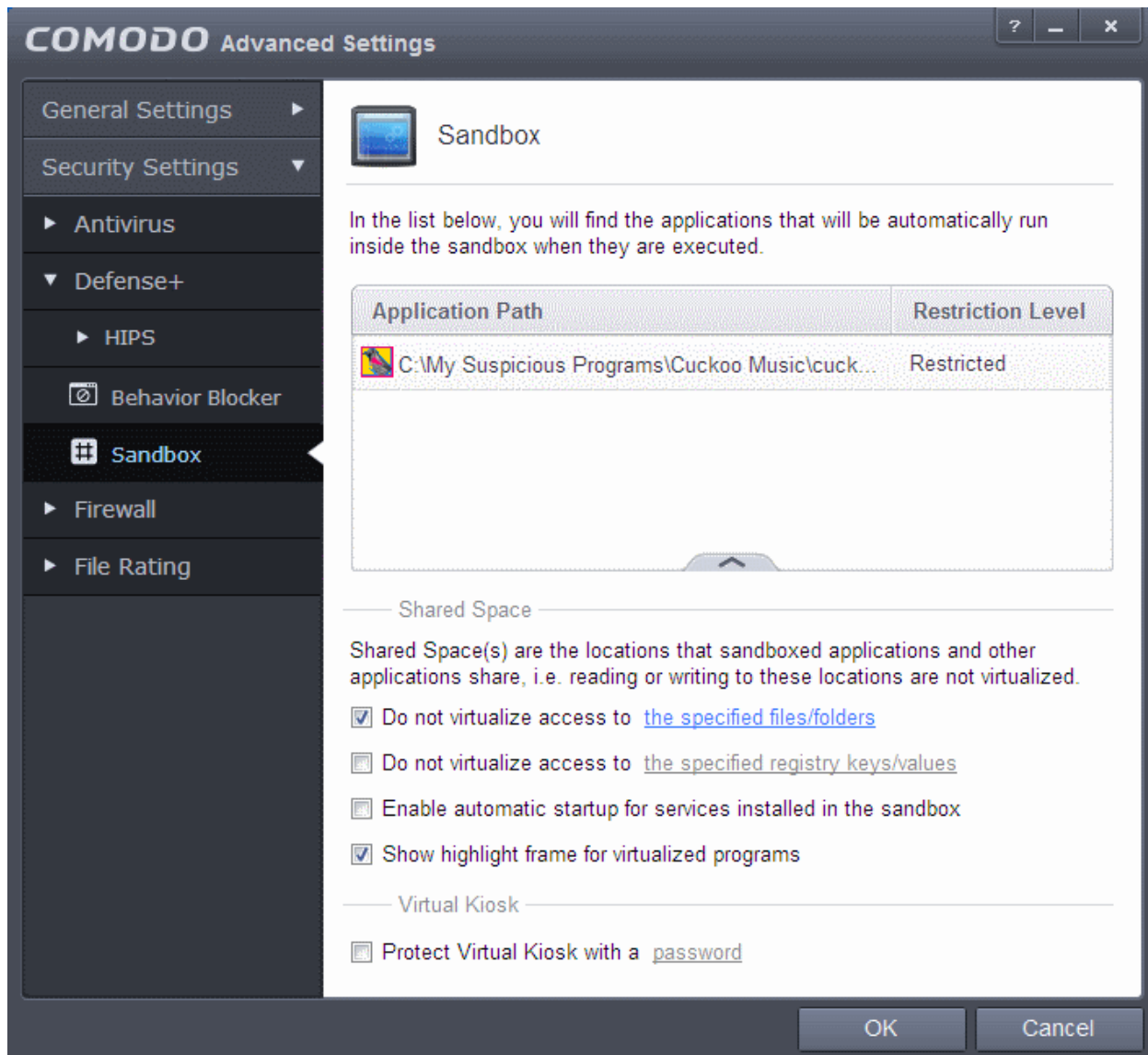
- Untrusted - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
- Blocked - The application is not allowed to run at all.
- 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 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 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.

6.2.2.8. Configure the Sandbox

The 'Sandbox' section of 'Advanced Settings' allows you to view, manage and add applications which should always be run inside the sandbox. A sandboxed application has much less opportunity to damage your computer because it is run in a virtual environment isolated from your operating system and your files. This allows you to safely run applications that you are not 100% sure about. When adding a new application, you can also set that particular application's 'restriction level' (this determines the degree of access that the application has to your 'real' system) and the amount of resources it should be allowed to consume. If you do not select a restriction level then it will run as 'Fully Virtualized'.

The 'Sandbox' area allows you to configure settings that apply to all sandboxed programs. Other sandbox-related options include the ability to password protect the Virtual Kiosk. For easy identification, Comodo Internet Security will show a green border around programs that are running in the sandbox.

- The 'Sandbox' panel can be accessed by clicking 'Tasks > Sandbox Tasks > Open Advanced Settings > Security Settings > Defense+ > Sandbox



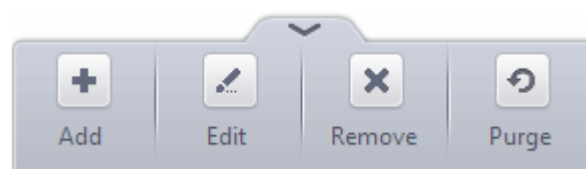
Click the following links to find out more about each section:

- **Sandboxed Programs** - Add and configure programs that should always run sandboxed
- **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 shared space
- **Virtual Kiosk Settings** - Create an 'exit' password for the kiosk. If set, the Kiosk cannot be closed or minimized until the correct password is entered. This prevents guests or younger users from exiting this sandbox environment.

Sandboxed Programs

The upper pane lists all programs that you have added to sandbox along with their installation paths and their access restriction level. Because the sandbox is isolated from your operating system, any programs that are known to be problematic or to cause conflicts with other software can be safely run in the sandbox.

Clicking the handle at the bottom of the pane opens the sandbox tools panel:



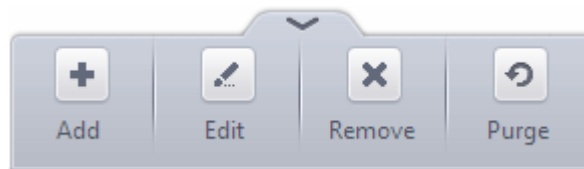
- **Add** - Allows you to add programs that should be run in the sandbox in future.
- **Edit** - Allows you to edit sandbox options for a selected program in the list.
- **Remove** - Releases the currently selected program from the sandbox
- **Purge** - Checks that all files listed are actually installed on your computer at the path specified. If not, the file or the file group is removed (purged) from the list.

Note: Programs added to this list will always be executed inside the sandbox. If you want to run an application in the sandbox on a 'one off' basis instead, you can do it in two ways:

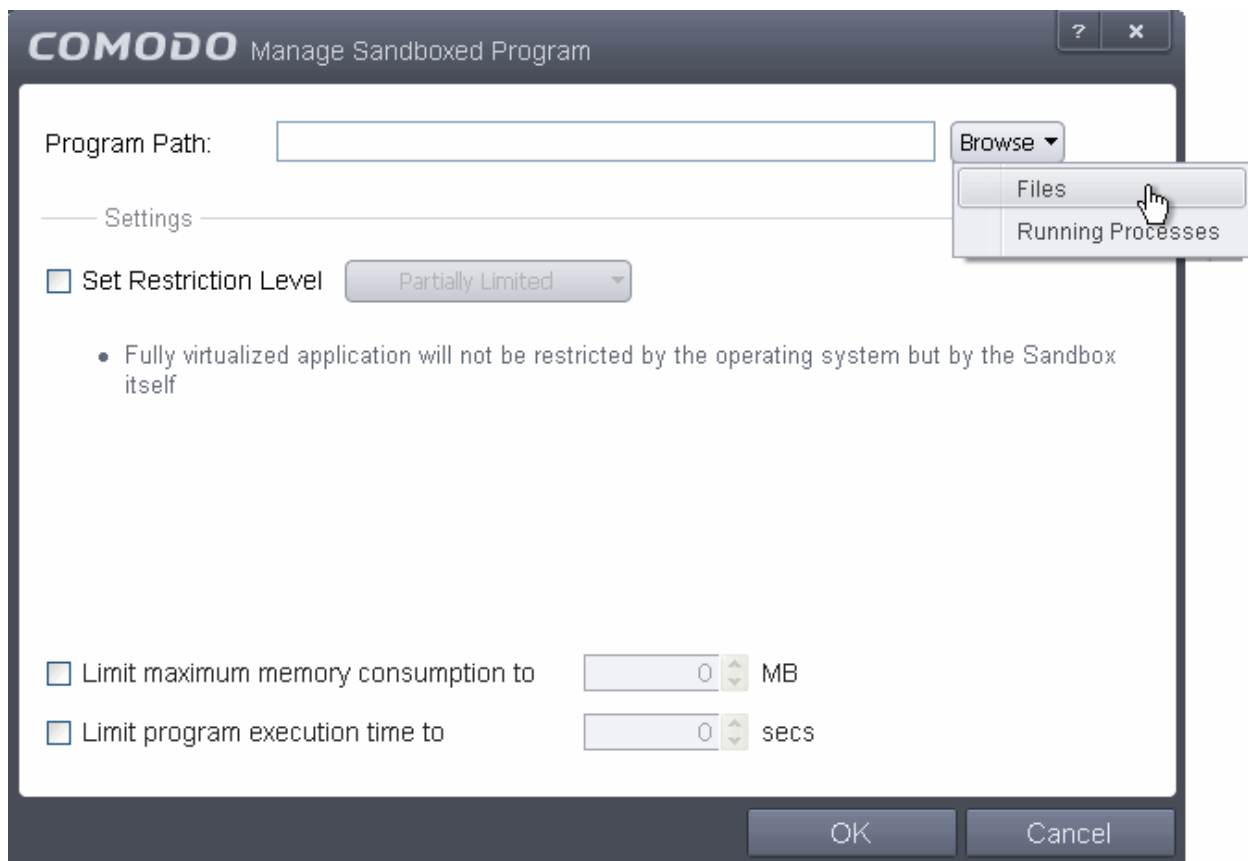
- Right click on the program or file to be opened from the Windows Explorer and select 'Run in Comodo Sandbox'
- or
- Flip the 'Scan objects' pane in the CIS Home screen to show 'Sandbox Objects' and drag and drop the program or file from Windows Explorer to the pane

To manually add a program to Sandbox

- Click the handle at the bottom and select 'Add':



- The 'Manage Sandboxed Program' interface will open:



To add a program, you can manually enter the path to the executable or click 'Browse' to add the program by choosing:

- **Files** - Allows you to navigate to the executable of the program you wish to add.

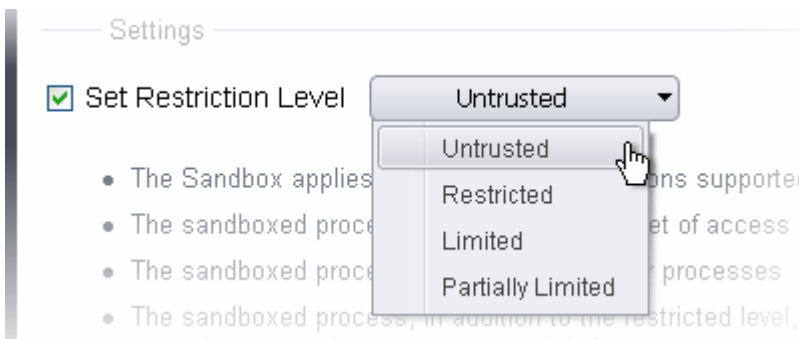
- **Running Processes** - Allows you to add a program to the sandbox by choosing a running process. Note, adding a process to the sandbox will also run it's parent processes in the sandbox.

Settings:

- **Set Restriction Level** - The Access restriction level determines the amount of privileges a sandboxed application has to access other software and hardware resources on your computer. (*Default = Disabled*)

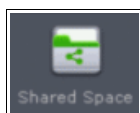
- Set an access restriction level by enabling the 'Set Restriction Level' check-box and choosing a level from the drop-down.

- If you do not set a restriction level, CIS will automatically apply a level of 'Fully Virtualized'.



- **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. Please note, some applications that require user interaction may not work properly under this setting.
- **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. Please note, applications like computer games may not work properly under this setting.
- **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 not allowed to execute actions that require Administrator account privileges. Access to many system resources, like the clipboard, are also prohibited.
- **Partially Limited (Default)**- 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.
- **Limit maximum memory consumption to:** You can define how much system memory can be allocated to the application by selecting this check-box then entering the desired memory (in MB) in the combo box beside it (*Default = Disabled*).
- **Limit the program execution time to:** You can define how long the program is allowed to run by selecting this check-box then entering the time (in seconds). The program will be terminated after this time has elapsed. (*Default = Disabled*).
- Click OK to add the program to the list of sandboxed programs. From this point onwards the application will be run in the sandbox.
- If you wish to remove it at a later date, simply select it in the list and click 'Remove'. Next time you execute this application it will run outside of the sandbox (presuming it is not then detected as malicious or automatically sandboxed as **per the sandboxing process**).
- To edit the restriction settings for an application included in the sandbox, select the application and click 'Edit'. The process is same as explained in **adding a program to sandbox**.

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 Kiosk 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

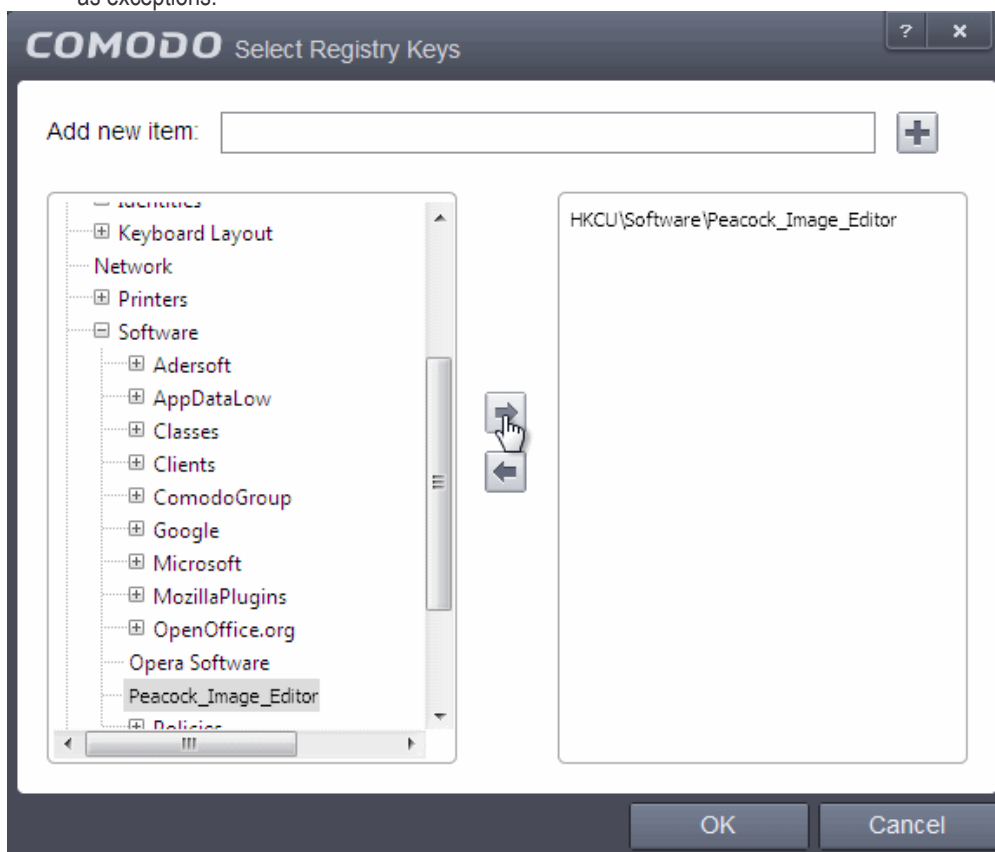
- Clicking 'Shared Space' button on the CIS interface
- Opening 'Sandbox Tasks' from the Tasks interface then clicking 'Open Shared Space'
- By default, sandboxed applications can access folders and files on your 'real' system but cannot save any changes to them. However, you can define exceptions to this rule by using the 'Do not virtualize access to...' links.

To define exceptions for files and folders

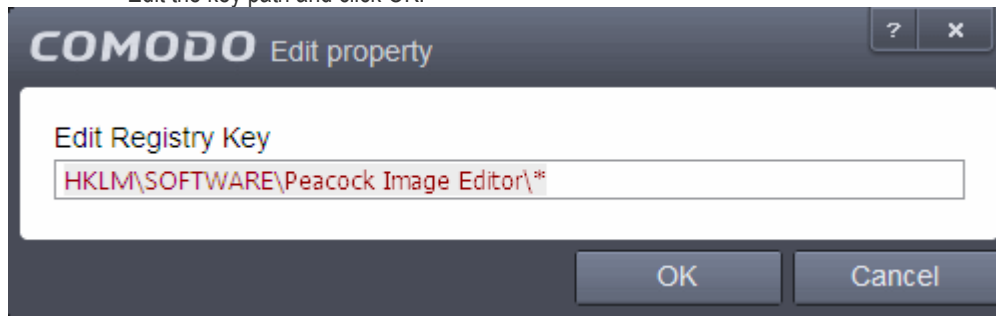
- Enable the 'Do not virtualize access to the specified files/folders' check-box then click on the words the specified files/folders. The 'Manage Exceptions' dialog will appear.
 - Click the handle at the bottom to open the tools menu then click 'Add'.
 - Files** - Allows you to specify files or applications that sandboxed applications are able to access
 - Folders** - Specify a folder that can be accessed by sandboxed applications
 - File Groups** - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl. For more details on file groups, refer to the section **File Groups**.
- To edit an exception, select it from the list, click the handle to open the tools menu then select 'Edit'.
 - Change file or folder location path and click 'OK'
 - Click 'OK' to implement your settings
 - To manage available file groups, click the 'Groups' button from the tools menu. The 'Manage File Groups' dialog allows you to view, add and edit file groups. Please refer to **File Groups** if you need more information with this area.

To define exceptions for specific Registry keys and values

- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the words the specified registry keys/values. The 'Manage Exceptions' dialog will appear.
 - Click the handle at the bottom to open the tools menu then click 'Add'.
 - **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exceptions. For an explanation of 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 exceptions:



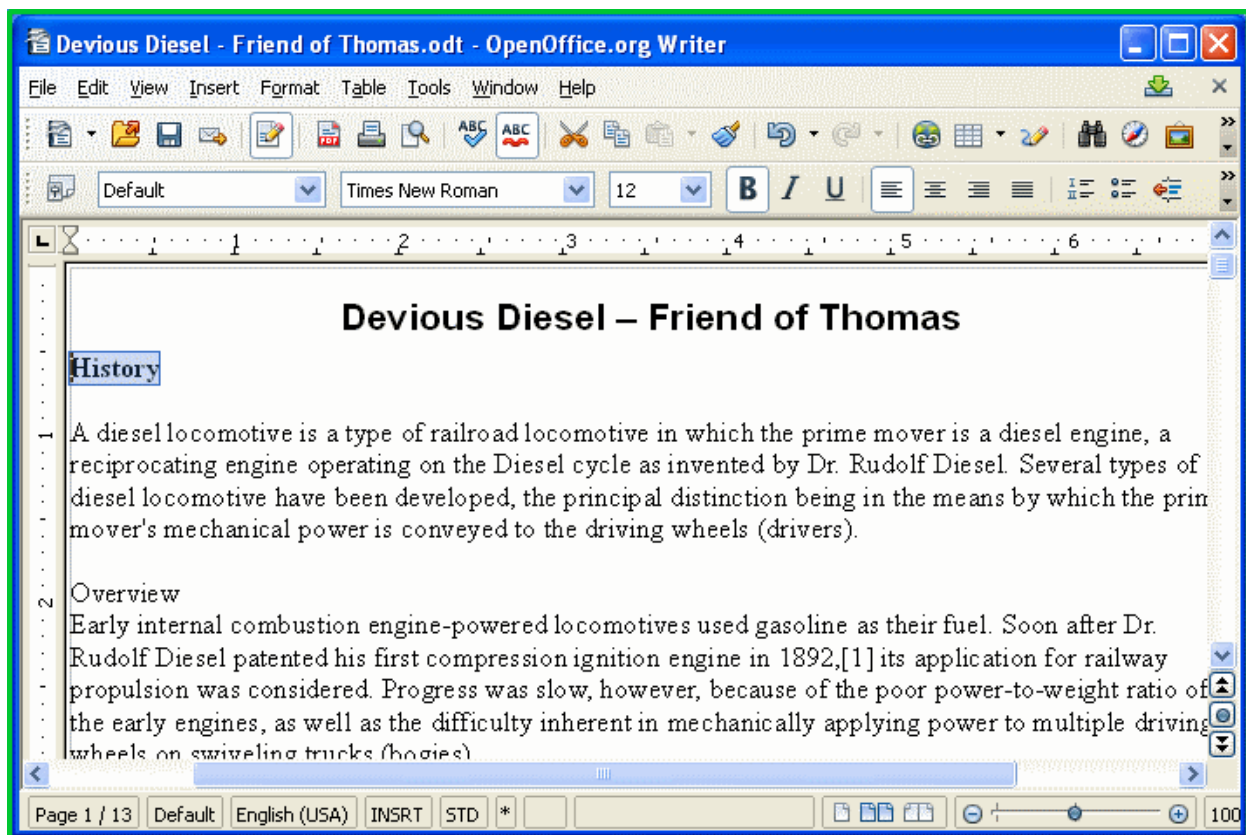
- Click 'OK' to implement your settings.
- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.
 - Edit the key path and click OK.



- To view and manage Registry Groups, click the handle at the bottom and select 'Groups'. From here you can add/remove registry groups, rename a groups and add/remove individual keys to/from a group. Note - any changes you make here are not limited to registry group 'exceptions', they apply to registry groups overall. Refer to the section **Registry Groups** for more details on managing registry groups.

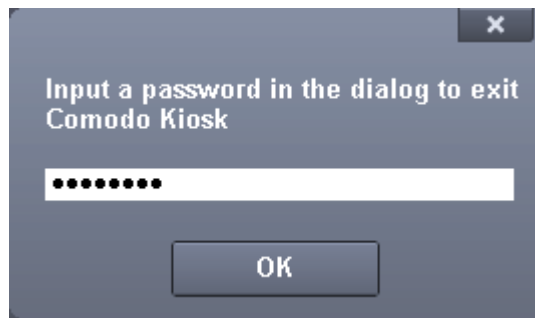
Other Settings:

- **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 = Disabled*)
- **Show highlight frame for virtualized programs** - If enabled, CIS displays a green border around the windows of programs that are running inside the sandbox. The following example shows an .odt document opened with a sandboxed version OpenOffice Writer:



Virtual Kiosk Settings

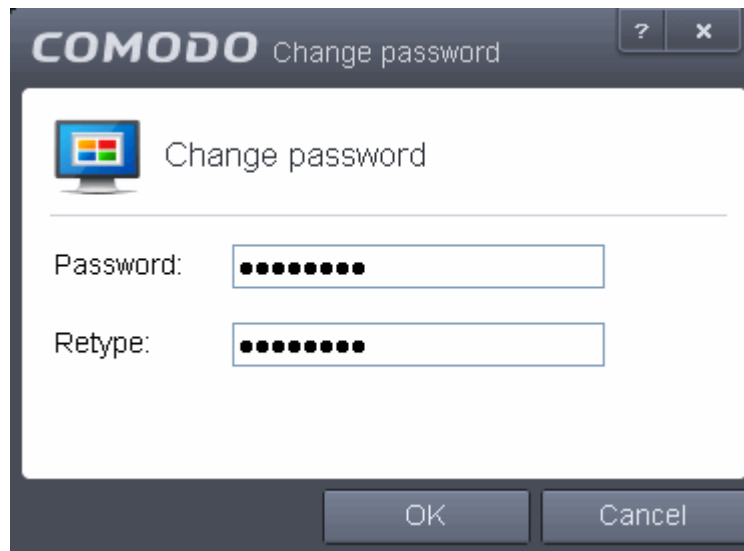
The Virtual Kiosk Settings area allows you to password protect your Virtual Kiosk. Once set, the password has to be entered every time when the Virtual Kiosk is closed.



The exit password for Virtual Kiosk 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 Kiosk:

- Select the 'Protect Virtual Kiosk with a password' check-box then click the words [password](#). The 'Change password' dialog will appear.

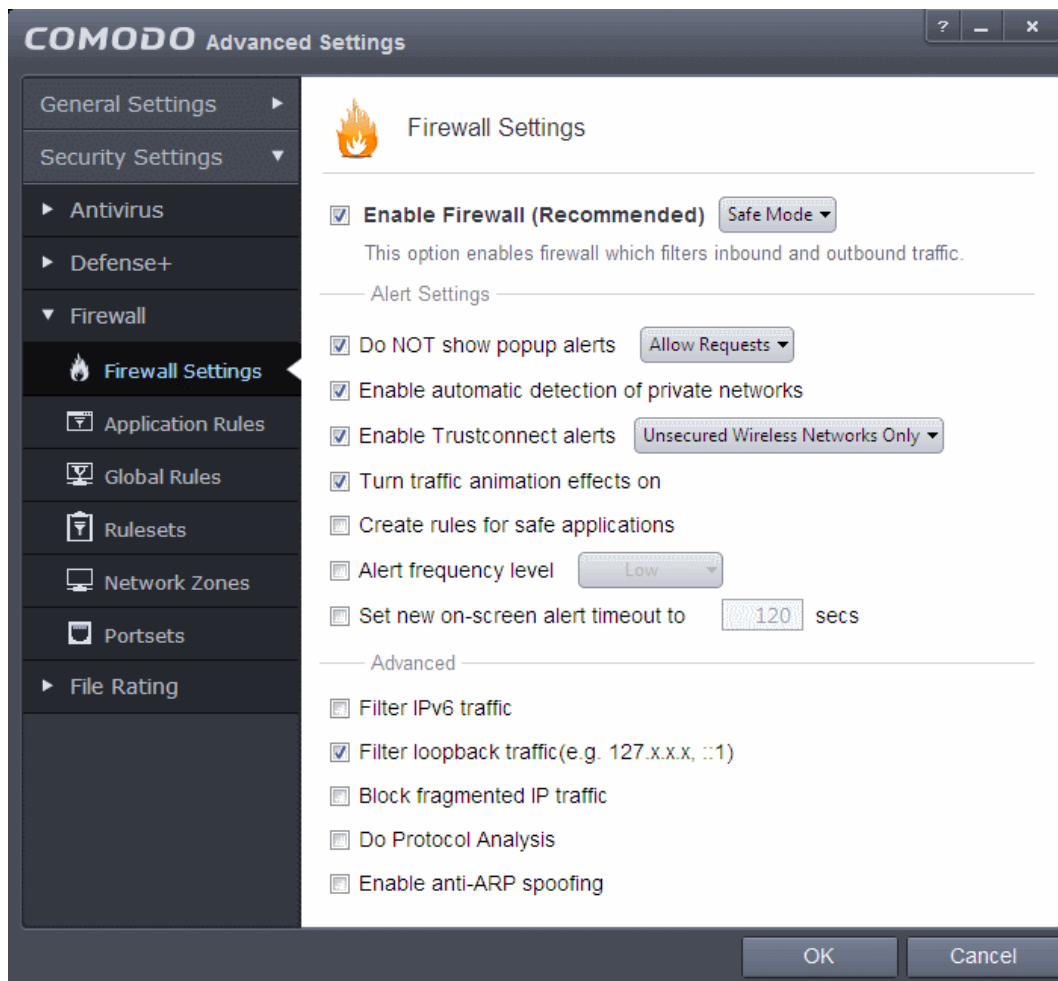


- Type a password which contains a combination of alphabetic and numeric characters and symbols which cannot be easily guessed by others. We recommend a password of at least 8 character in length.
- Re-enter the password in the 'Retype' field then click 'OK'.

You will now be asked for a password every time you exit the Virtual Kiosk.

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.



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 Behavior Settings** - Configure settings that govern the overall behavior of the firewall component.
- **Application Rules** - View, create and modify rules that determine the network access privileges of individual applications or specific types of application
- **Global Rules** - View, create and modify rules that apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Predefined collections of firewall rules that can be applied, out-of-the-box, to Internet capable applications such as browsers, email clients and FTP clients.
- **Network Zones** - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Predefined groups of regularly used ports that can used and reused when creating traffic filtering rules.

Background note on rules: Both application rules and global rules are consulted when the firewall is determining whether or not to allow or block a connection attempt.

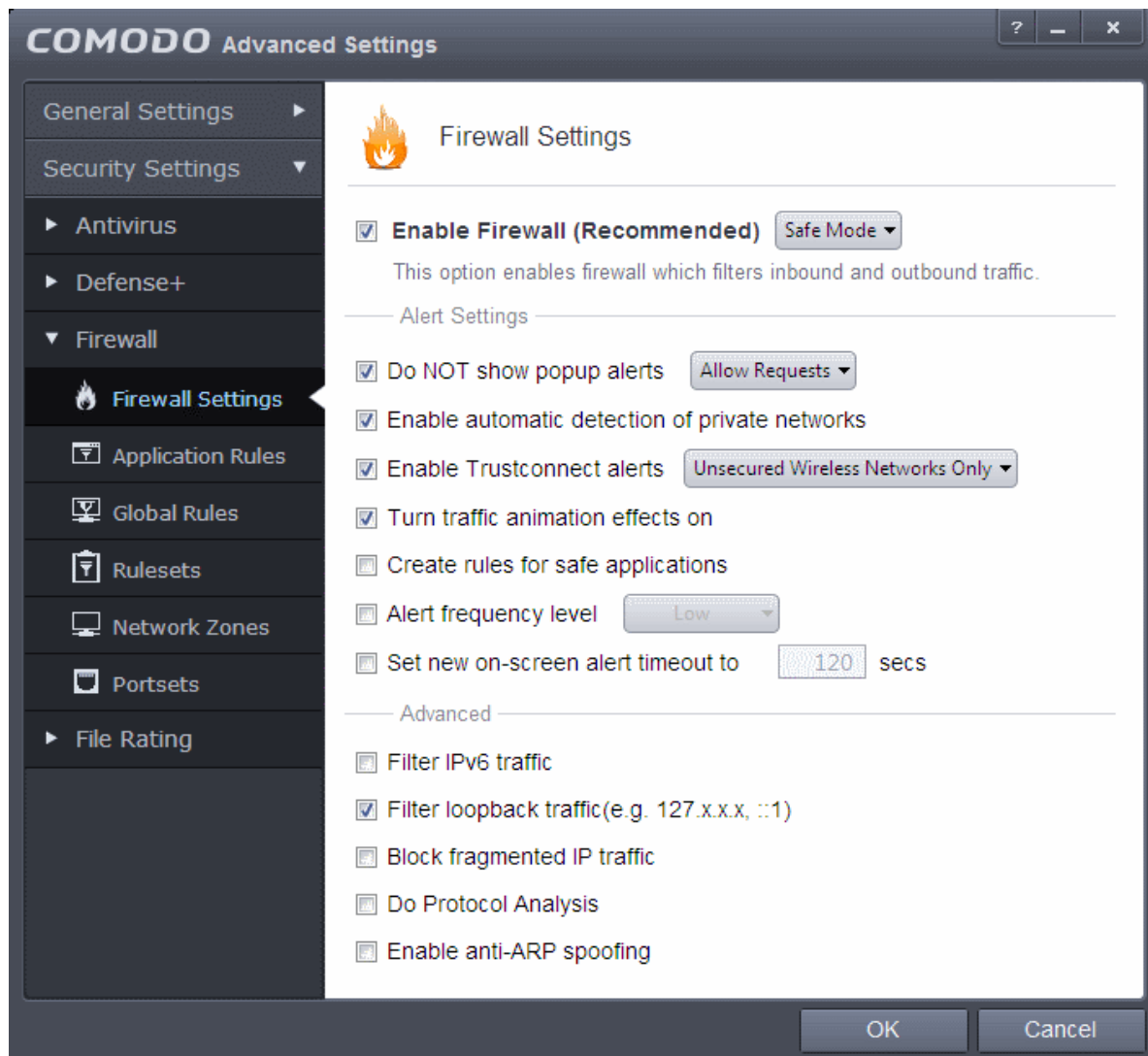
- For Outgoing connection attempts, the application rules are consulted first then the global rules.
- For Incoming connection attempts, the global rules are consulted first then application specific rules.

6.2.3.1. Firewall Behavior Settings

Firewall Settings panel allows you to quickly configure overall Firewall settings and is divided into three main areas:

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

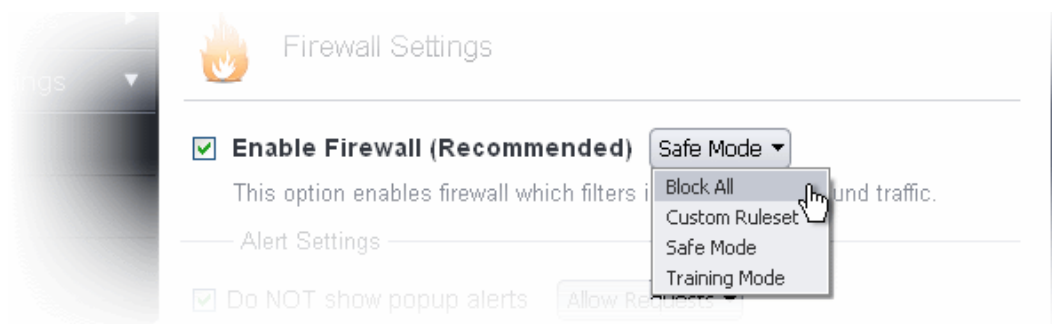
- **Advanced Settings**



General Settings

- **Enable Firewall** - Allows you to enable or disable Firewall protection. (*Default and recommended = Enabled*)

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.

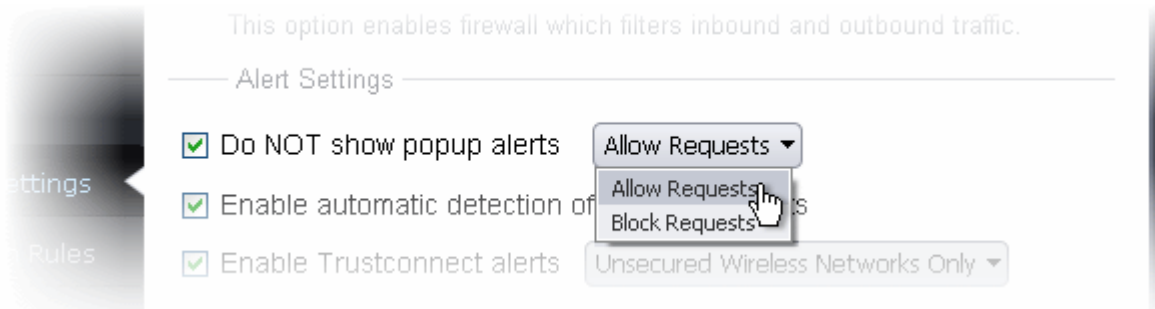
'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.

- **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**.

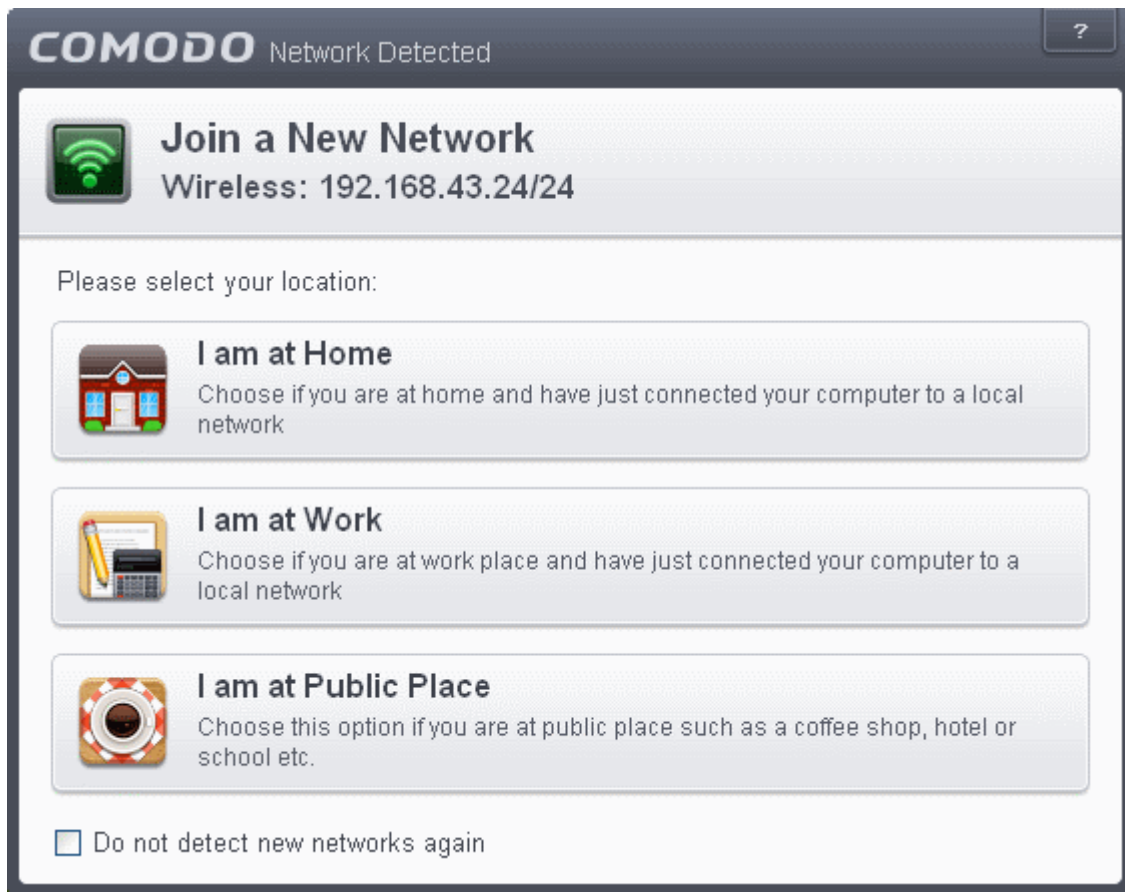
Alert Settings

- **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 automatic detection of private networks** - Instructs Comodo Firewall to keep monitoring whether your computer is connected to any new wired or wireless network. The firewall will display an alert as shown below if it detects a new network (for example, when you connect to a wired home or office network or a Wi-Fi 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. Comodo recommends users to leave this option at its default, enabled setting (**Default = Enabled**).

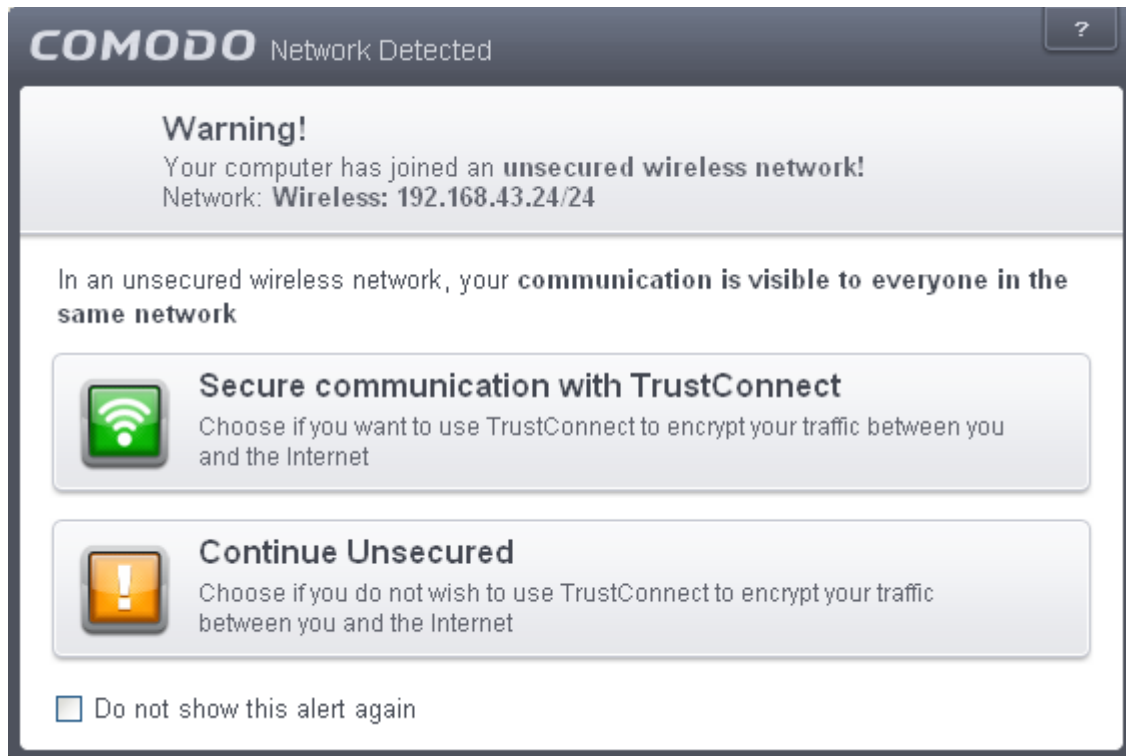
Enable Trustconnect alerts - If you are connecting to Internet at a public place like an airport or a coffee shop then you are potentially exposing yourself to danger. Unsecured public networks can allow other people to easily eavesdrop on your communications or even gain access to your computer to steal 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 'Shield' tray icon displays a small animation whenever traffic moves to or from your computer.



If the traffic is outbound, you can see green arrows moving upwards on the right hand side of the shield. Similarly, for inbound traffic you can see yellow arrows moving down the left hand side. This provides a very useful indicator of the real-time movement of data in and out of your computer. Clear this check box if you would rather not see this animation (*Default = 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).

- **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 3.4×10^{38} unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

- **Filter loopback traffic:** CIS can filter the loopback network traffic applied for testing the transmission or transportation infrastructure. Disable this option if you do not want the loopback traffic to be filtered. (*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.

COMODO Advanced Settings

Application Rules

The following firewall application rules are active on this computer.

Application	Treat As
System	Custom
✓ Allow System To Send Reque...	
✓ Allow System To Receive Req...	
COMODO Internet Security	Outgoing Only
✓ Allow All Outgoing Requests	
⊗ Block and Log All Unmatching...	
Windows Updater Applications	Custom
Windows System Applications	Custom
C:\Program Files\Opera\opera.exe	Web Browser
✓ Allow Access to Loopback Zone	
✓ Allow Outgoing HTTP Requests	
✓ Allow Outgoing FTP Requests	
✓ Allow Outgoing FTP.PA...	

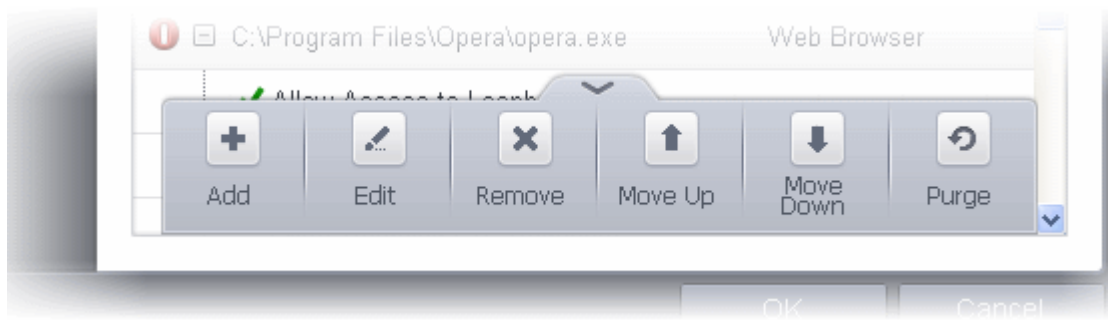
Annotations:

- The application's name is listed directly above the rules applied to it
- The rule applied to an application determines its network access rights
- Each ruleset is derived from at least one but usually a combination of individually configurable rules
- Name of the pre-defined ruleset

The first column, **Application**, displays a list of the applications on your system for which a Firewall ruleset has been deployed. If the application belongs to a file group, then all member applications assume the ruleset of the file group. The second column, **Treat as**, column displays the name of the Firewall ruleset assigned to the application or group of applications in column one.

General Navigation:

Clicking the handle 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 its ruleset. See the sections '[Creating or Modifying Firewall Rules](#)' and '[Adding and Editing a Firewall Control Rule](#)'.
- **Edit** - Allows the user to modify the Firewall rule or ruleset of the selected application. See the sections '[Creating or Modifying Firewall Rules](#)' and '[Adding and Editing a Firewall Rule](#)'.
- **Remove** - Deletes the selected ruleset.
- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

If you wish to modify the **firewall ruleset** for an application:

- Double click on the application name to begin '[Creating or Modifying Firewall Rules](#)'
- Select the application name click the handle at the bottom right and choose 'Edit' from the options to begin '[Creating or Modifying Firewall Rules](#)'

If you wish to modify an **individual rule** within the ruleset:

- Double click on the specific rule to begin '[Adding and Editing a Firewall Rule](#)'
- 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.

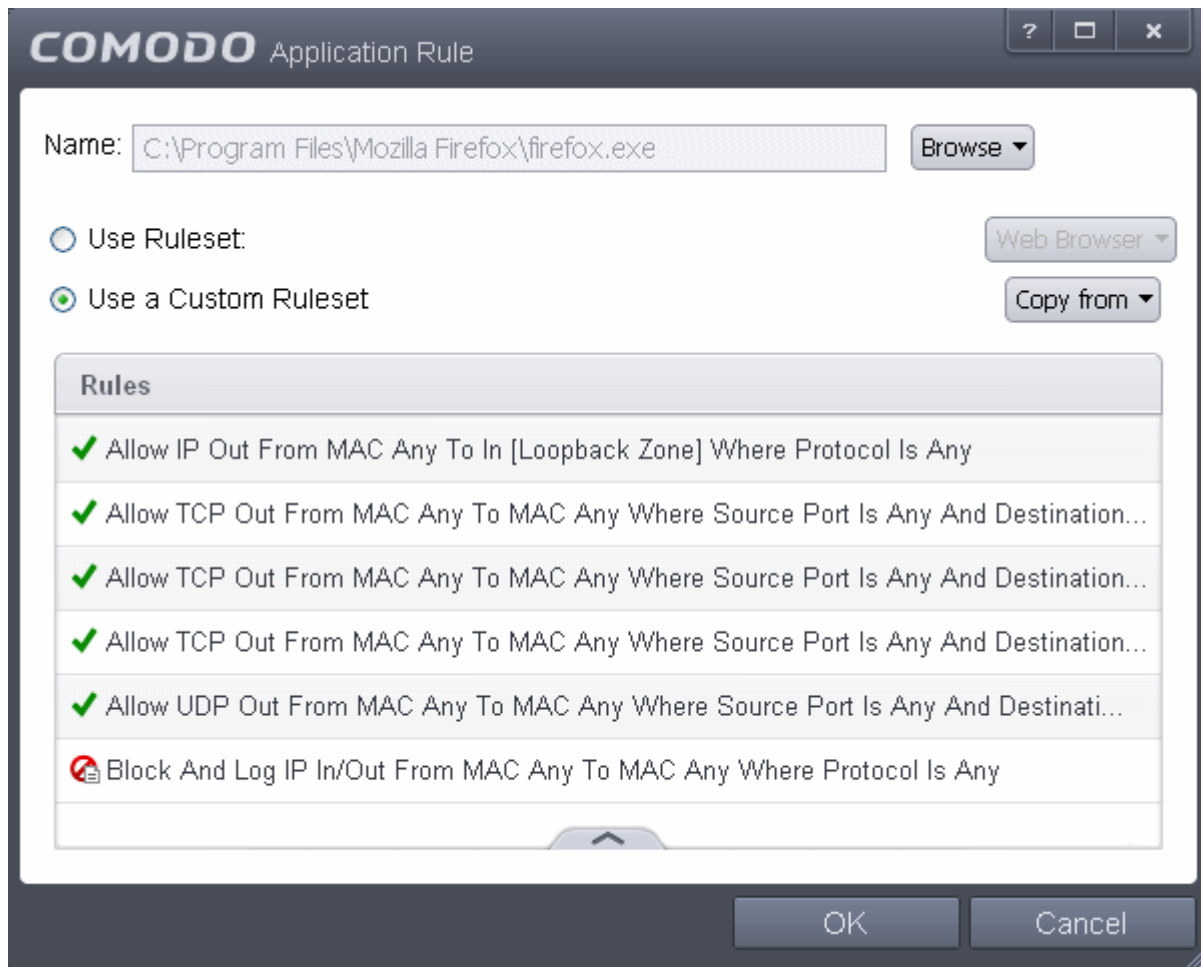
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to 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](#)'

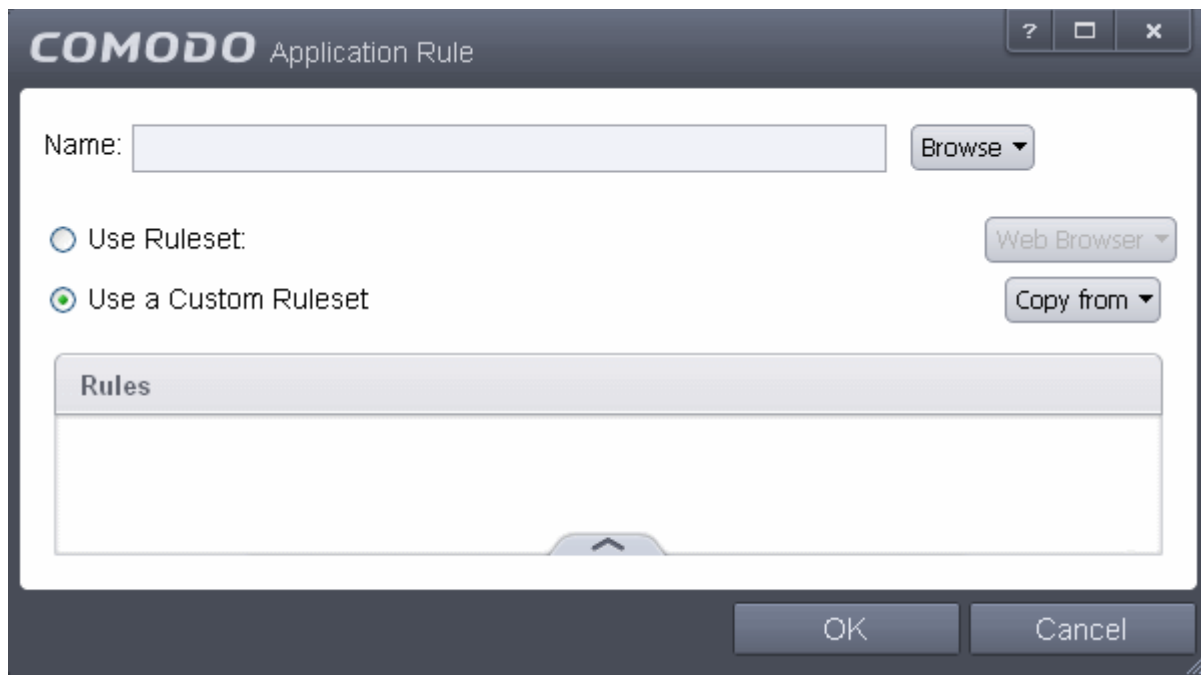
Creating and Modifying Firewall Rulesets

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.**

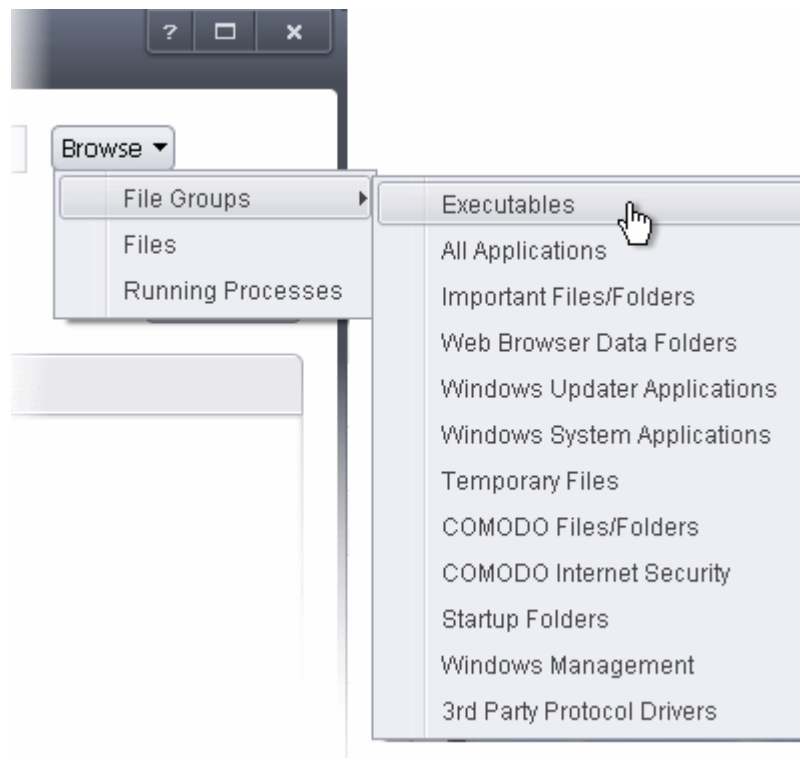
Step 1 - Select the application that you wish the ruleset is to be applied

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.

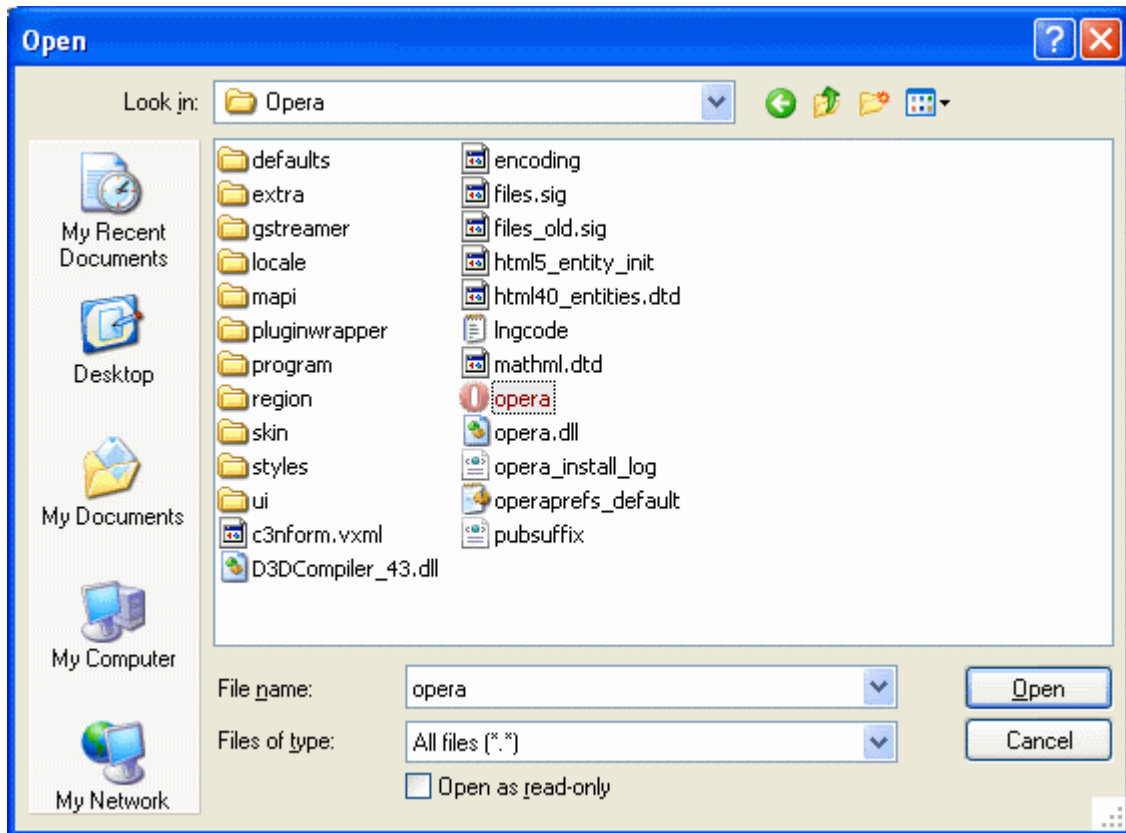


You now have 3 methods available to choose the application for which you wish to create a ruleset - **File Groups**, **Files** and **Running Processes** and

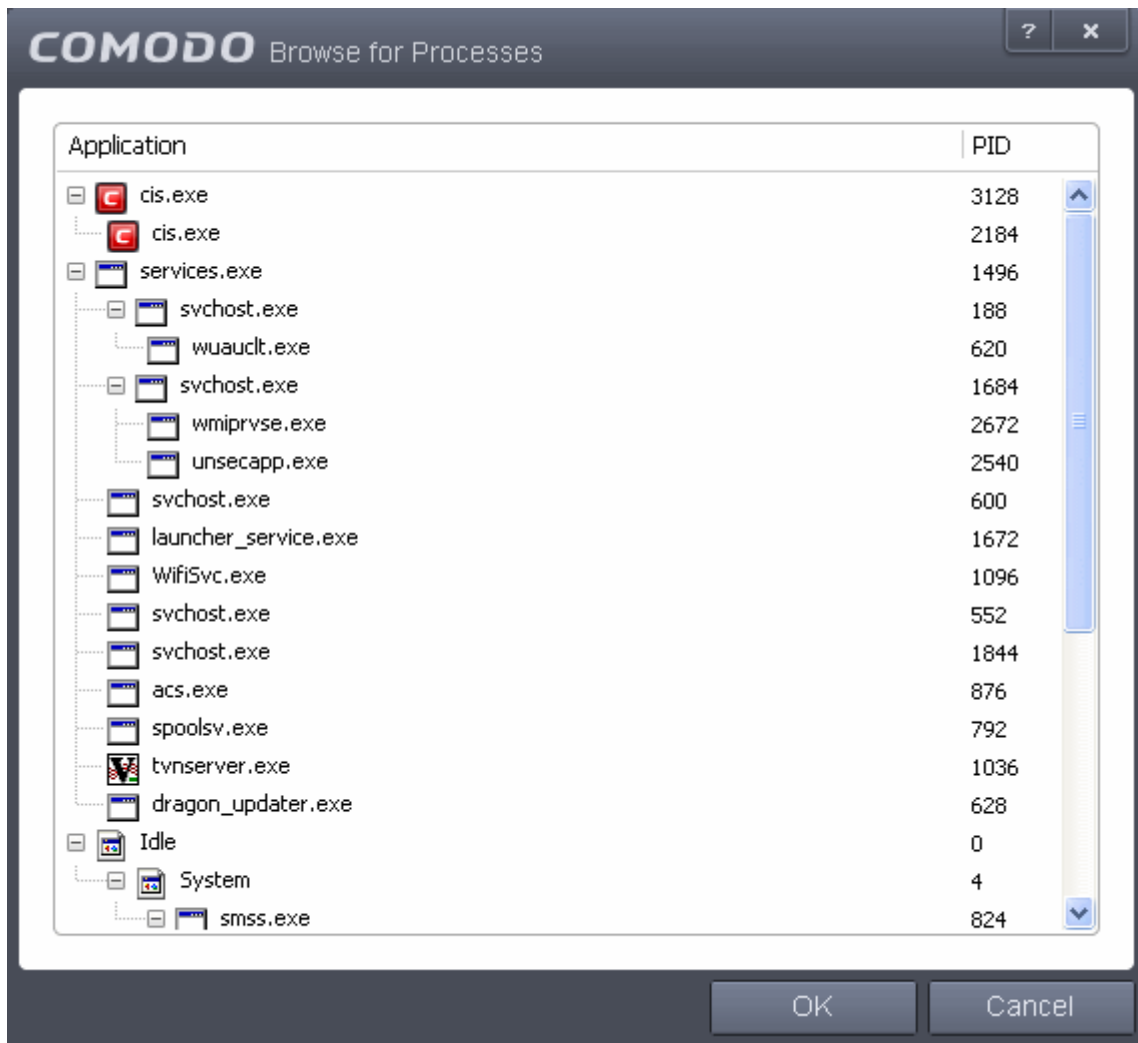
- i. **File Groups** - choosing this option allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .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.



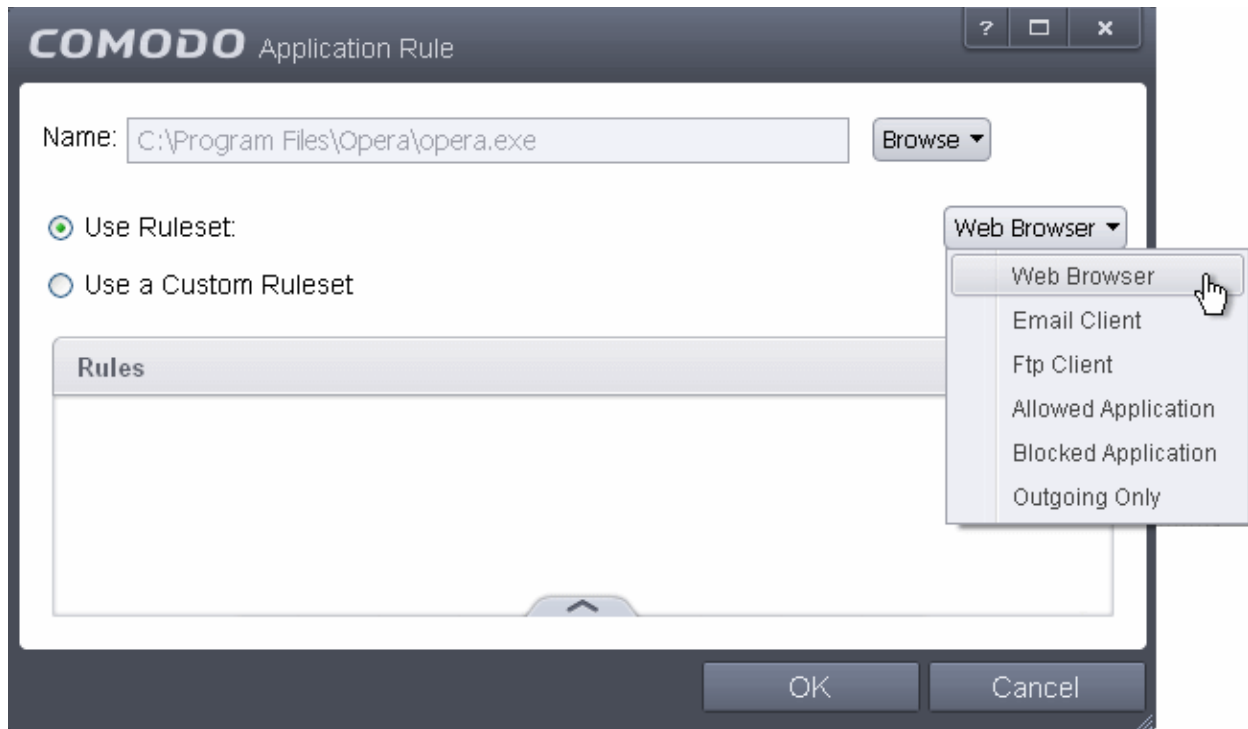
You can choose an individual process (shown above) or the parent process of a set of running processes. Click 'OK' to confirm your choice.

Having selected the individual application, running process or file group, the next stage is to Configure the rules for this application's Firewall Ruleset.

Step 2 - Configure the rules for this application's ruleset

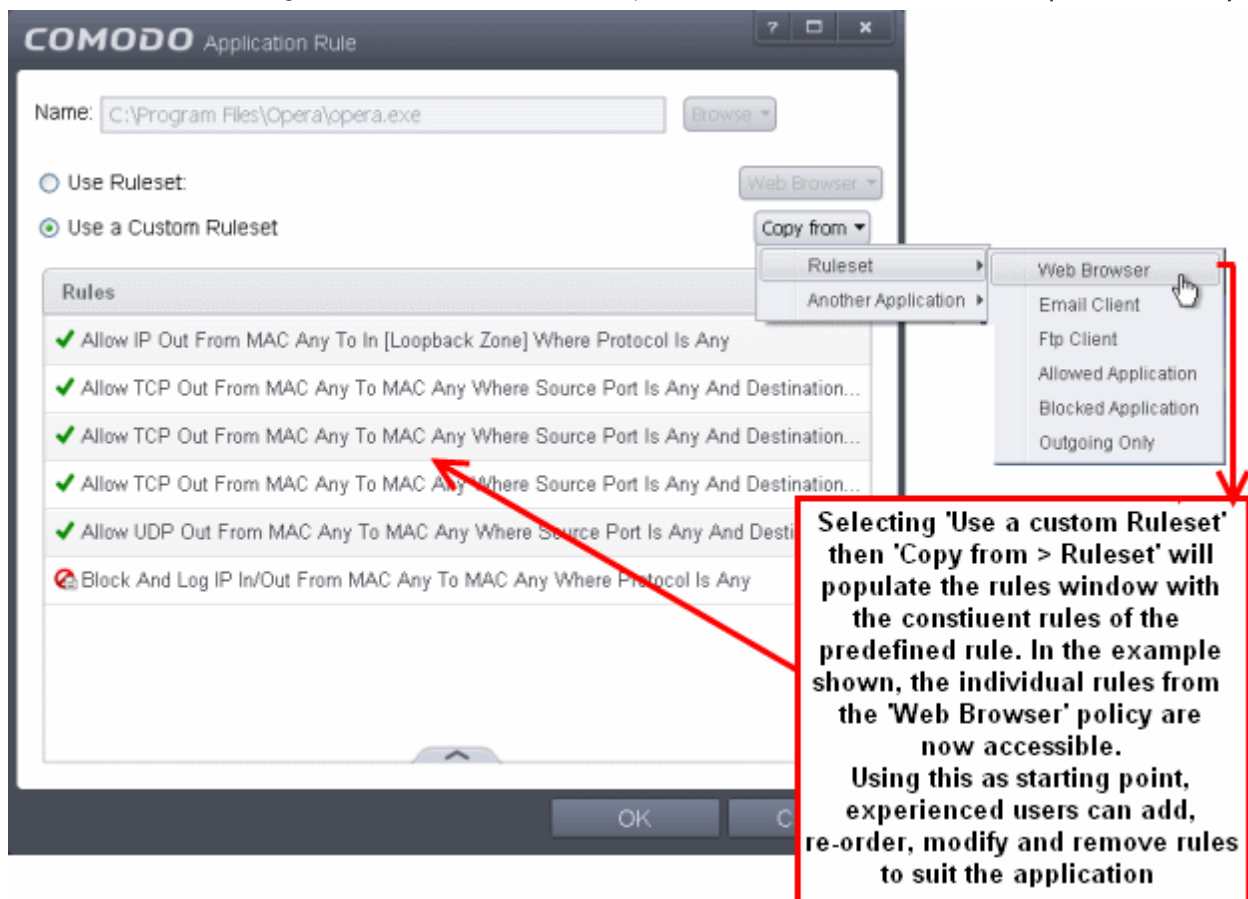
There are two broad options available for creating a ruleset that applies to an application - **Use a Predefined Ruleset** or **Use a Custom Ruleset**.

- **Use a Predefined Ruleset** - Selecting this option allows the user to quickly deploy a existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Opera' browser. The name of the predefined ruleset you choose is displayed in the **Treat As** column for that application in the **interface (Default = Disabled)**.



Note: Predefined Rulesets, once chosen, cannot be modified *directly* from this interface - they can only be modified and defined using the **Predefined Rulesets** interface. If you require the ability to add or modify rules for an application then you are effectively creating a new, custom ruleset and should choose the more flexible **Use Custom Ruleset** option instead.

- **Use a Custom Ruleset** - designed for more experienced users, the **Custom Ruleset** option enables full control over the configuration of Firewall Ruleset and the parameters of each rule within that ruleset (*Default = Enabled*).



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.

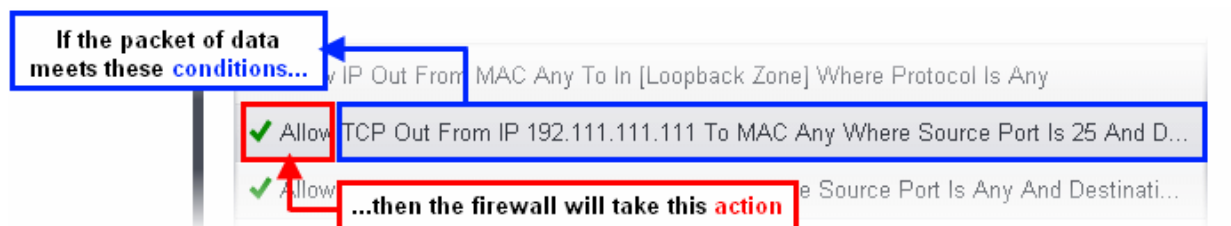
General Tips:

- 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

- 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.

Description:

Source Address	Destination Address	Source Port	Destination Port
<input type="checkbox"/> Exclude (i.e. NOT the choice below)			
Type: <input type="text" value="Any Address"/>			
<ul style="list-style-type: none"> Any Address Host Name IPv4 Address Range IPv4 Single Address IPv4 Subnet Mask IPv6 Single Address IPv6 Subnet Mask MAC Address Network Zone 			

Source Address and Destination Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the

IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.
9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.
 - Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.

Description:

Source Address	Destination Address	Source Port	Destination Port
<input type="checkbox"/> Exclude (i.e. NOT the choice below)			
Type: <input type="text" value="Any"/> <ul style="list-style-type: none"> A Port Range A Set of Ports A Single Port Any 			

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 port set then please see the section '**Port Sets**'.

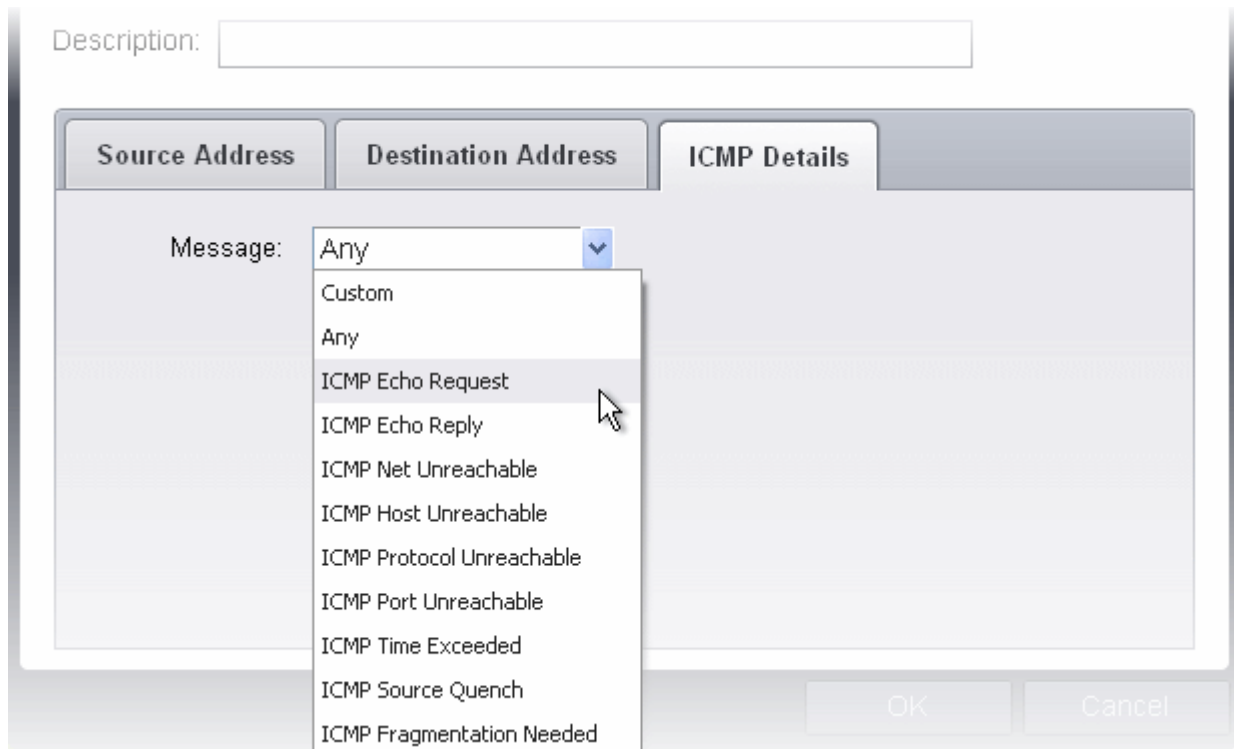
ii. ICMP

When you select ICMP as the protocol in **General Settings**, you are shown a list of ICMP message types in the 'ICMP Details' tab alongside the **Destination Address** tabs. The last two tabs are configured identically to the **explanation above**. You cannot see the source and destination port tabs.

• ICMP Details

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are

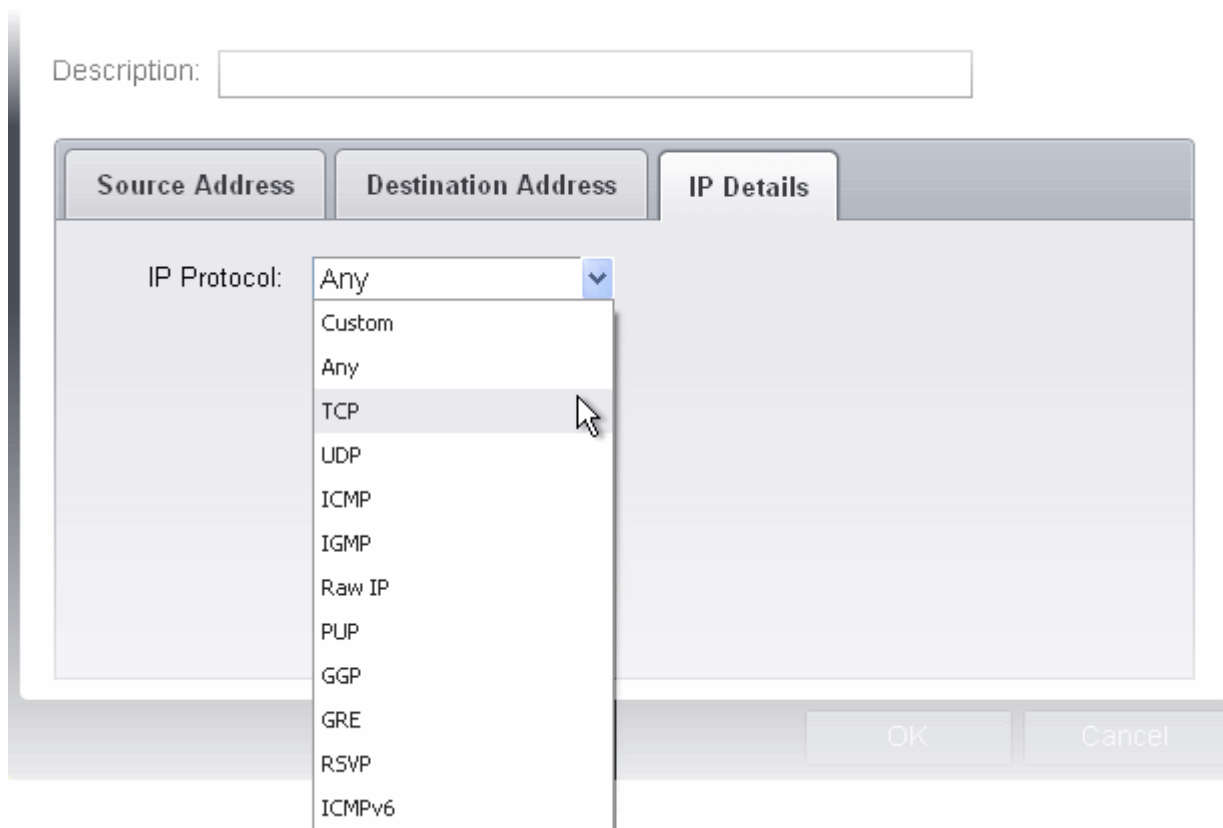
using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.



1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.
2. Specify ICMP Message , Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.
When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

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**

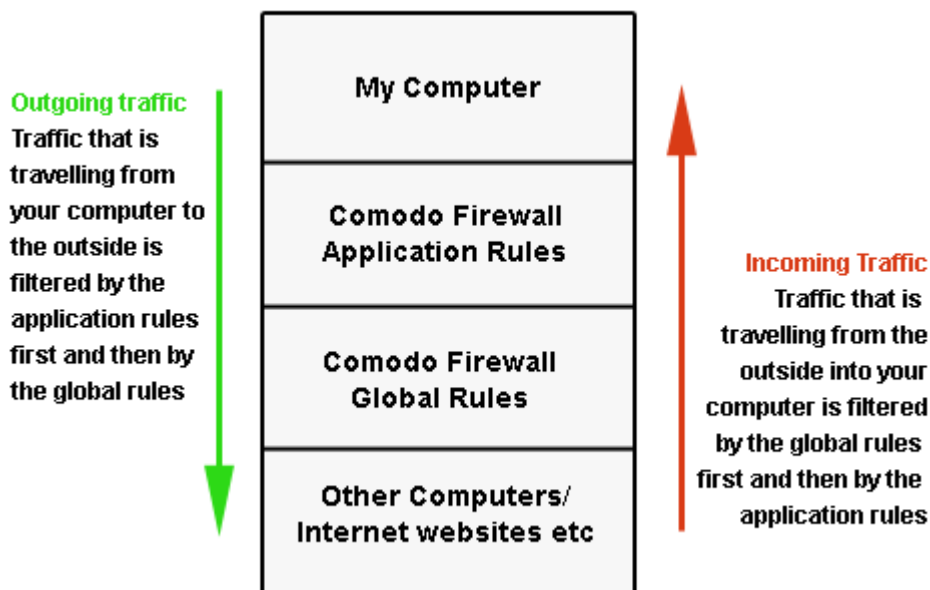
Select the types of IP protocol that you wish to allow, from the ones that are listed.

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.

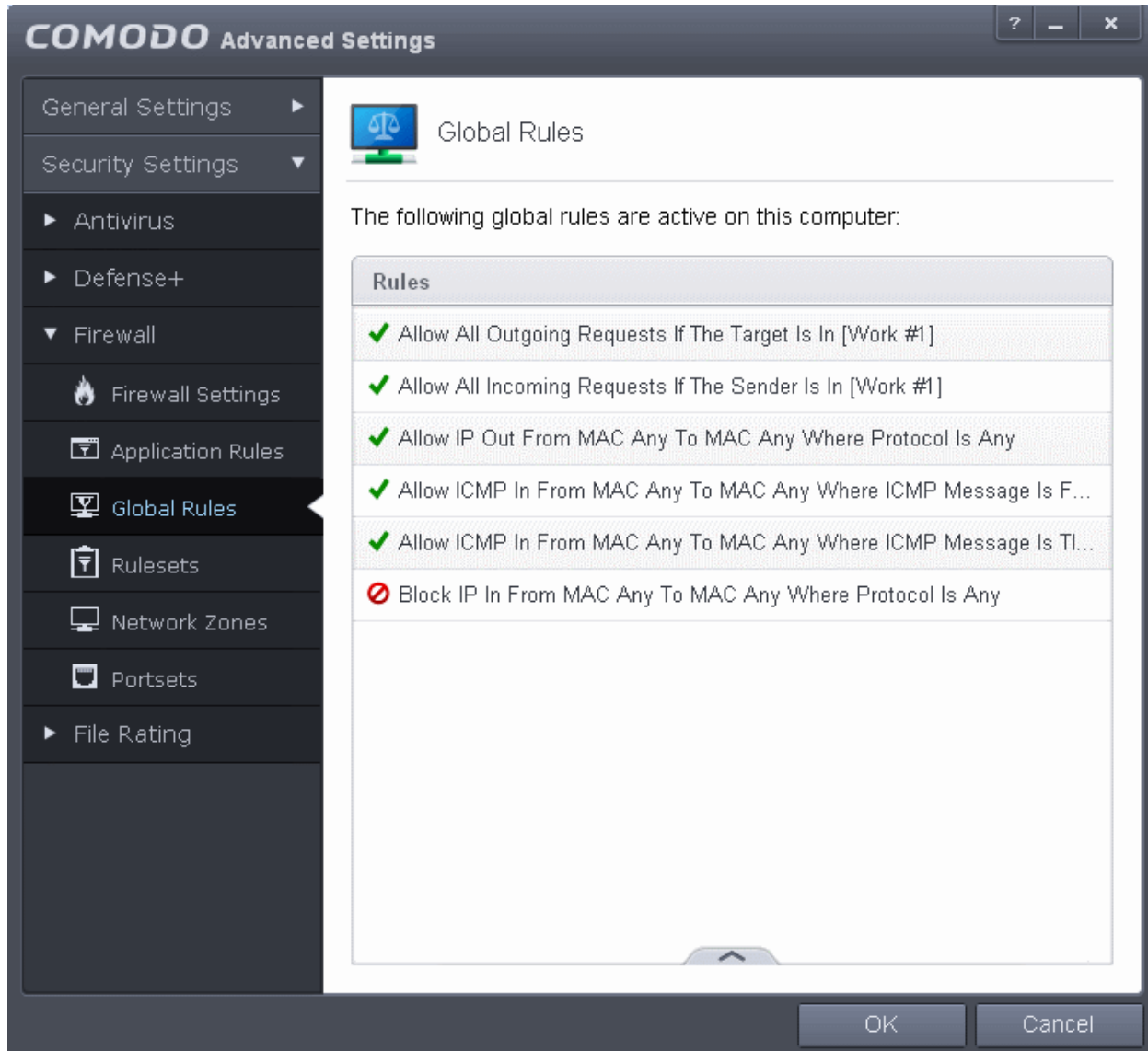
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.



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.

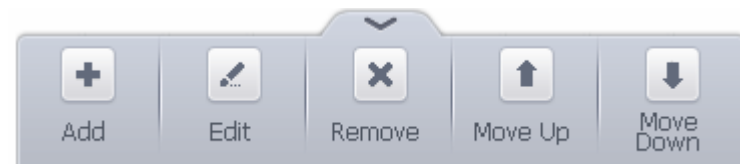
Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

- 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



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.

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'.

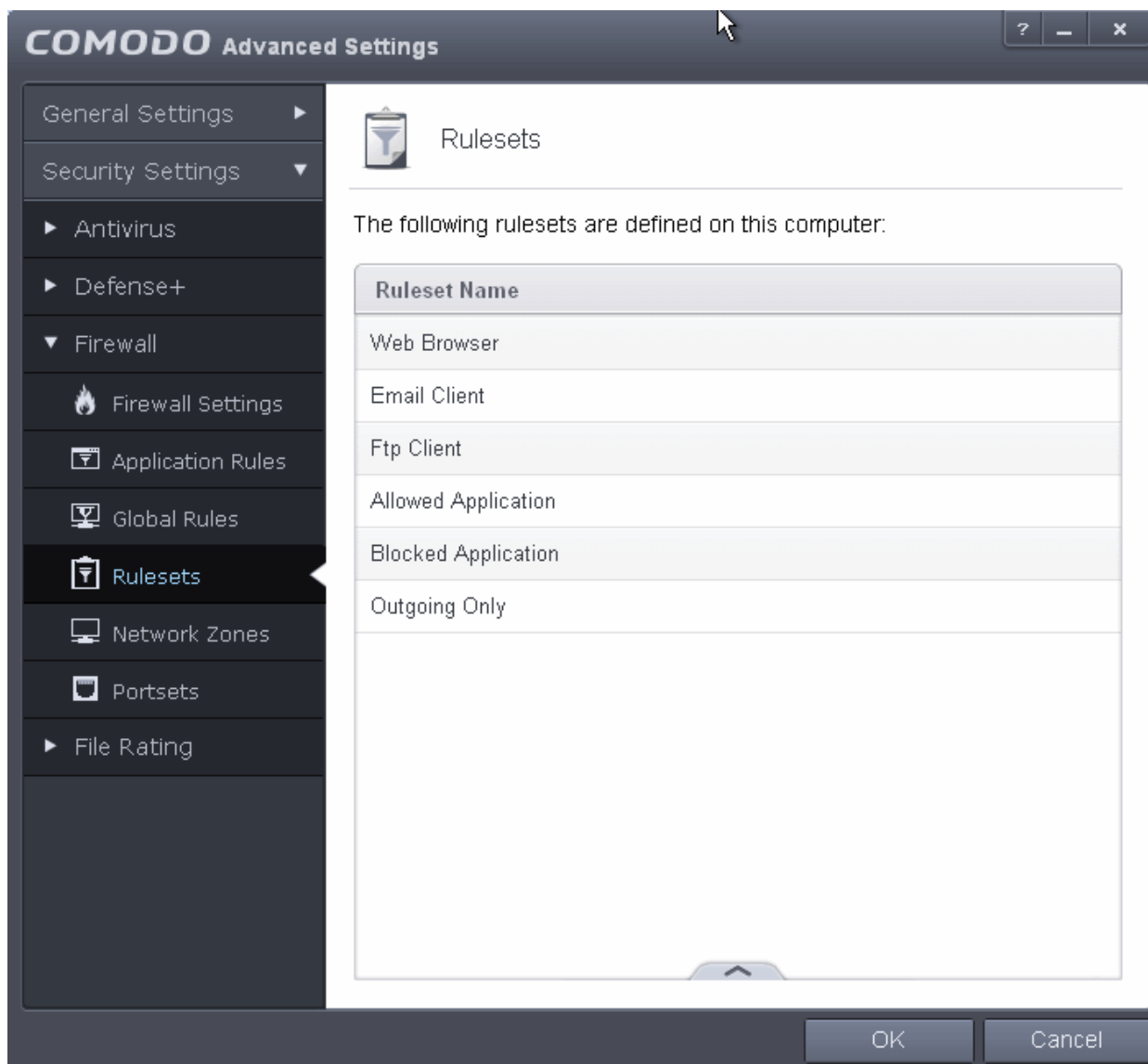
- See [Application Rules](#) for an introduction to the rule setting interface.
- See [Understanding Firewall Rules](#) for an overview of the meaning, construction and importance of individual rules.
- See [Adding and Editing a Firewall Rule](#) for an explanation of individual rule configuration.

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



Predefined Rulesets

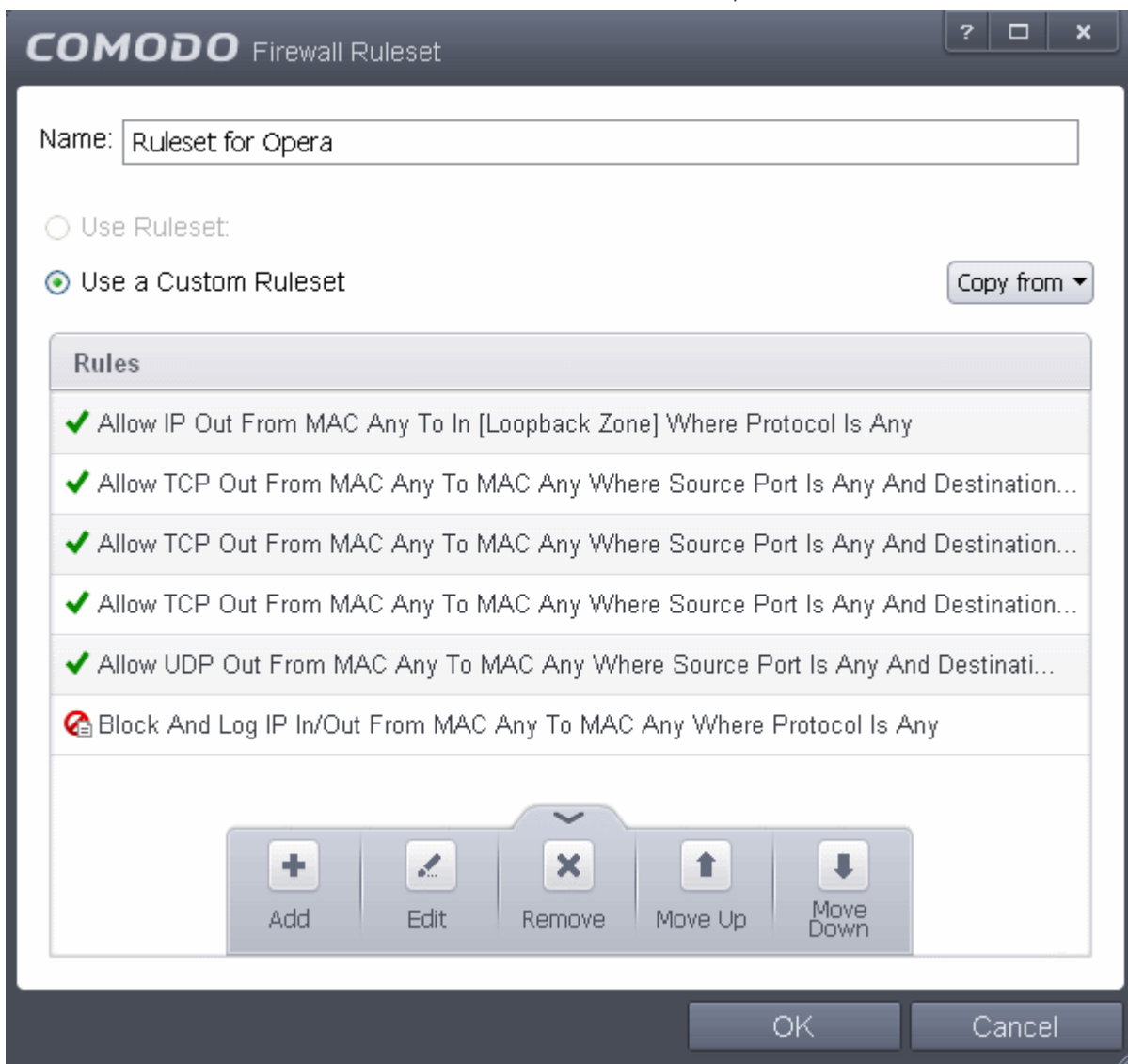
Although each application's firewall ruleset *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined 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.

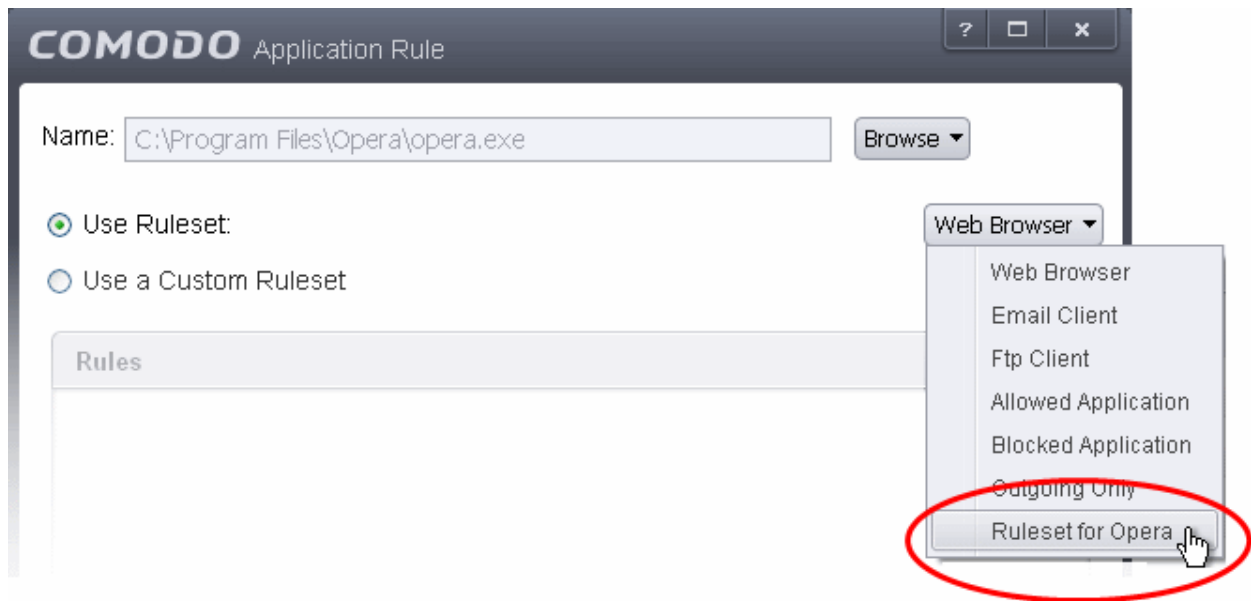
To add a new Ruleset

- 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**

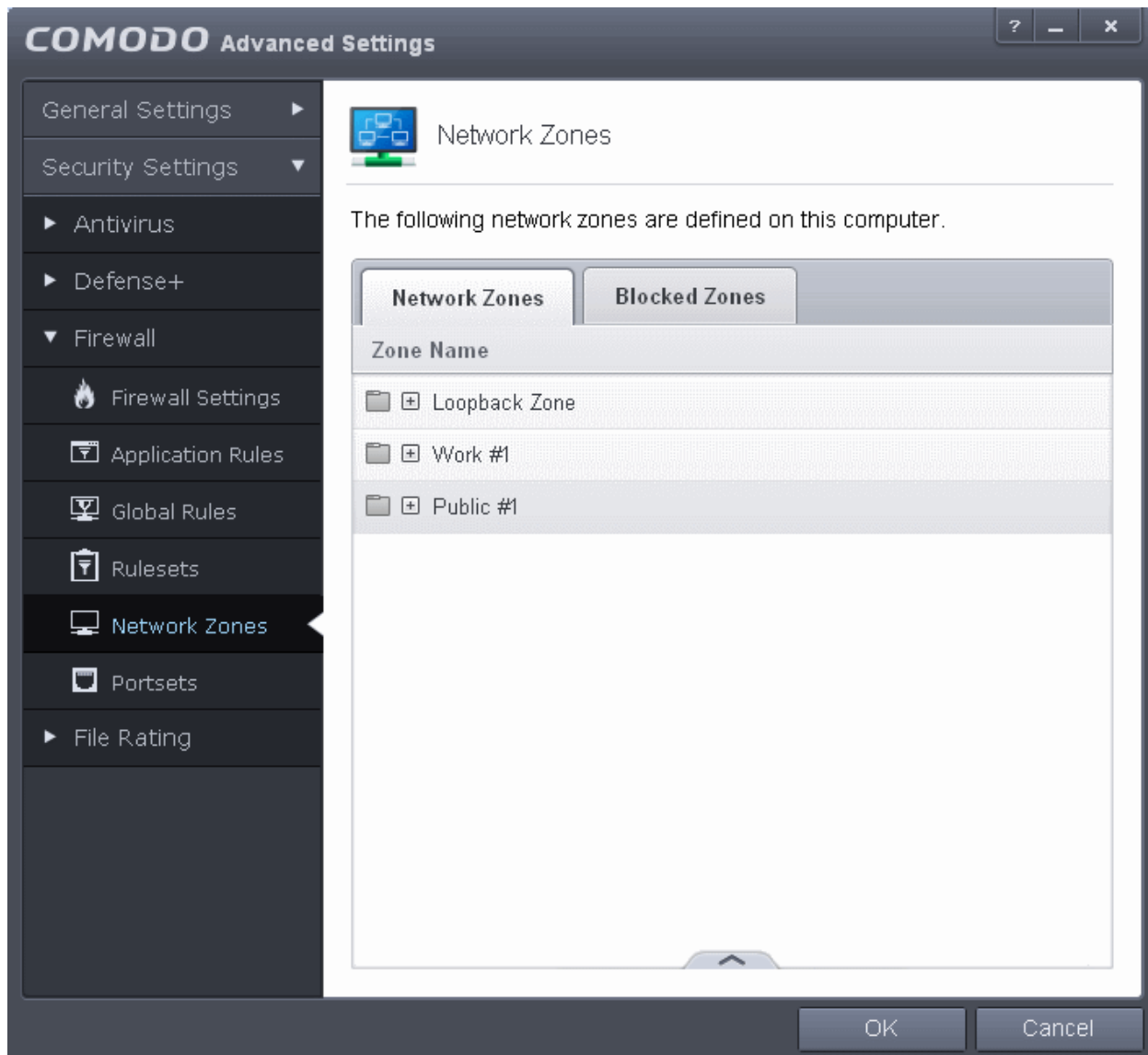
- Double click on the Ruleset Name in the list
or
- Select the Ruleset Name, click the handle from the bottom center and select Edit from the options
- Details of the process from this point on can be found [here](#).

6.2.3.5. Network Zones

The Network Zones panel allows you to:

- 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.



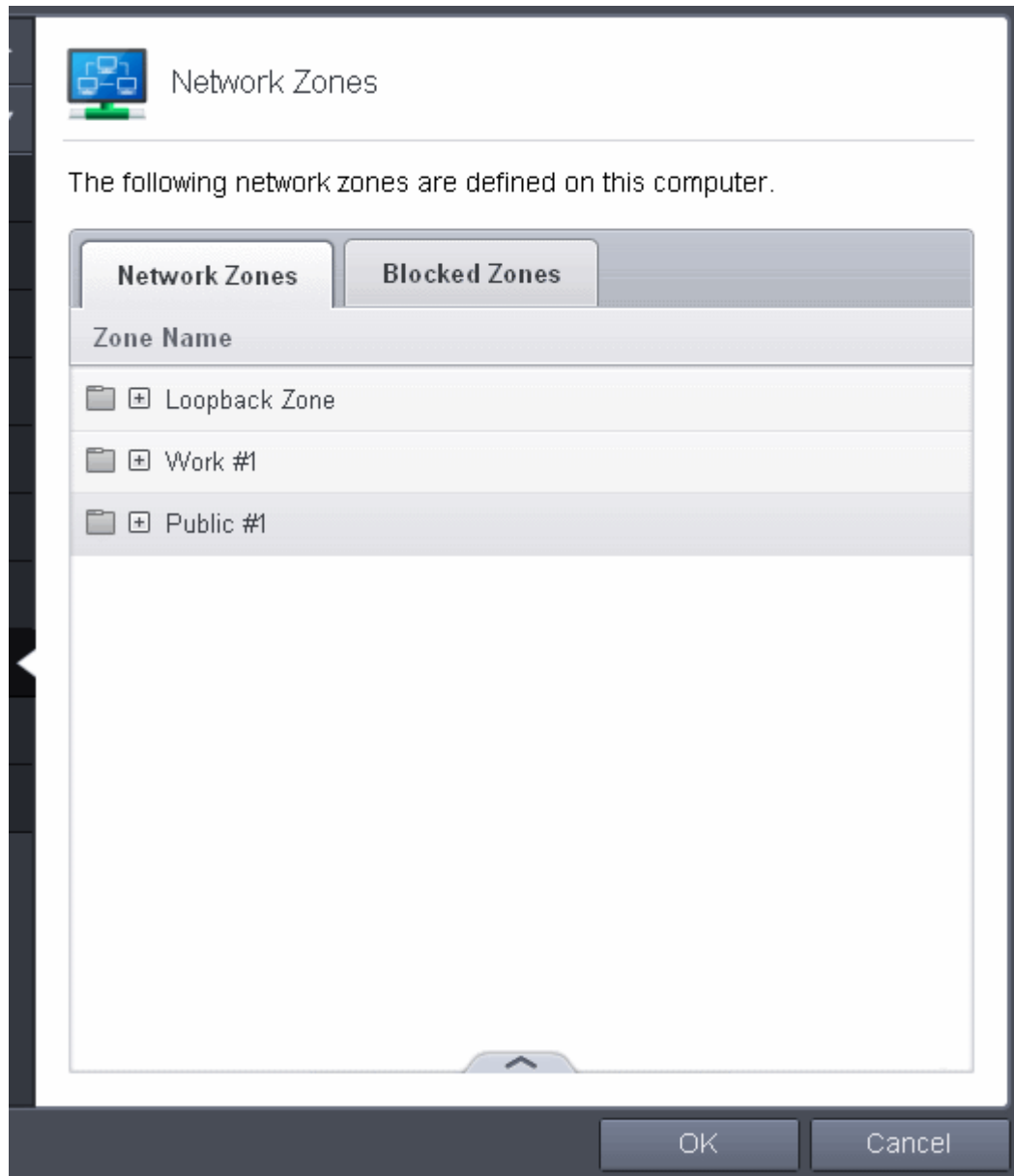
The panel has two tabs:

- **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.

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.**

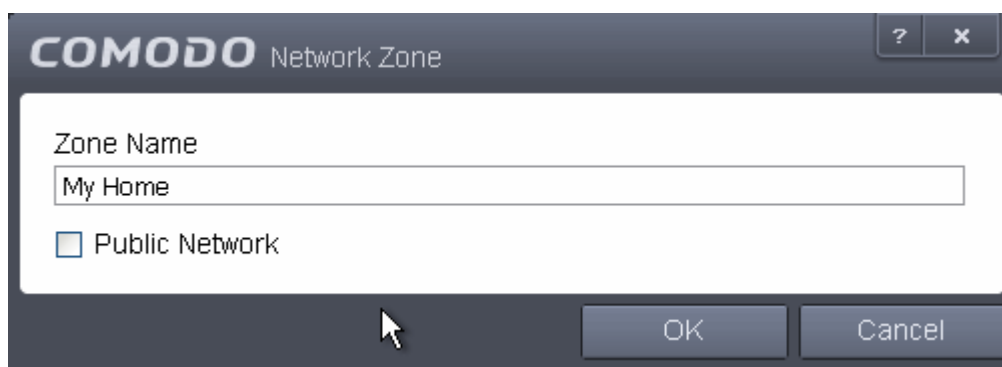
Step 1 - Define a name for the zone

1. Click the handle from the bottom center select 'Add' > 'New Network Zone'.



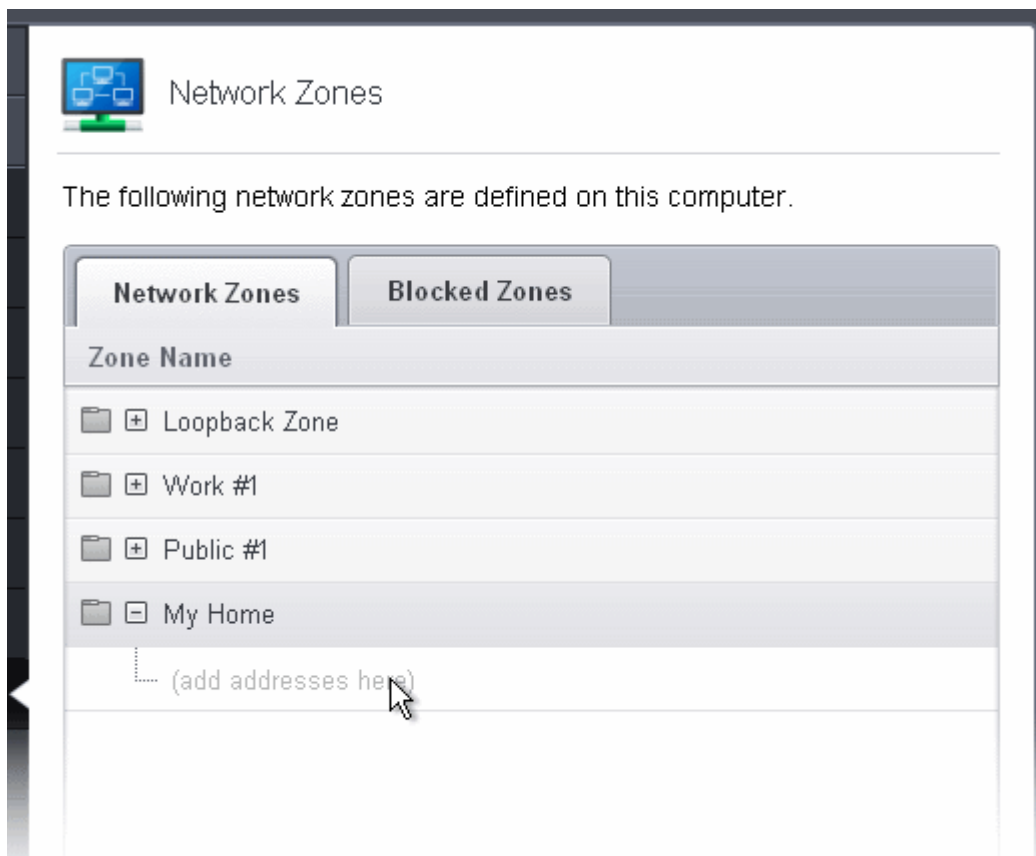
A dialog box will appear, prompting you to specify a name for the new zone.

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.

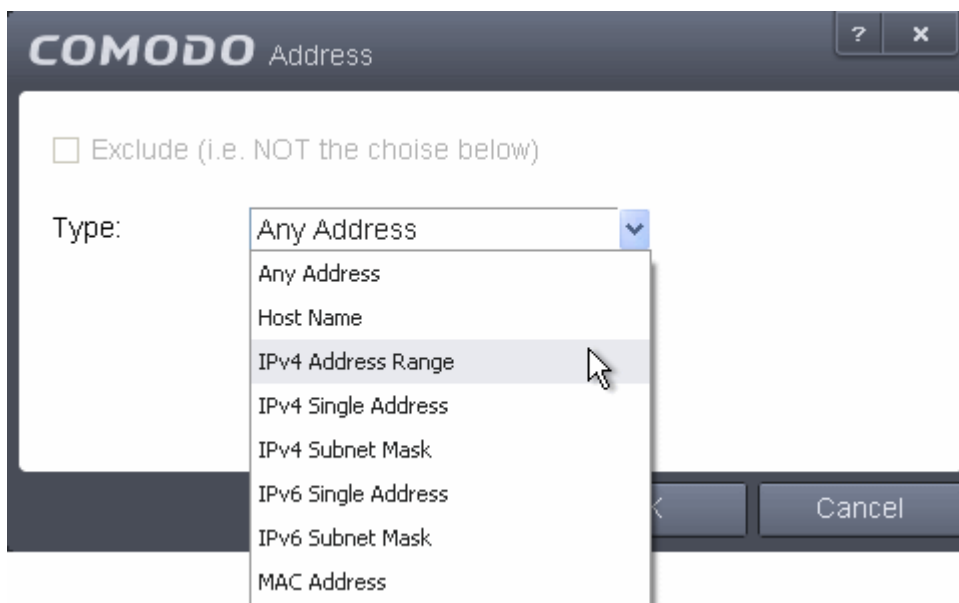
This adds the name of your new zone to the Network Zones list.



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:

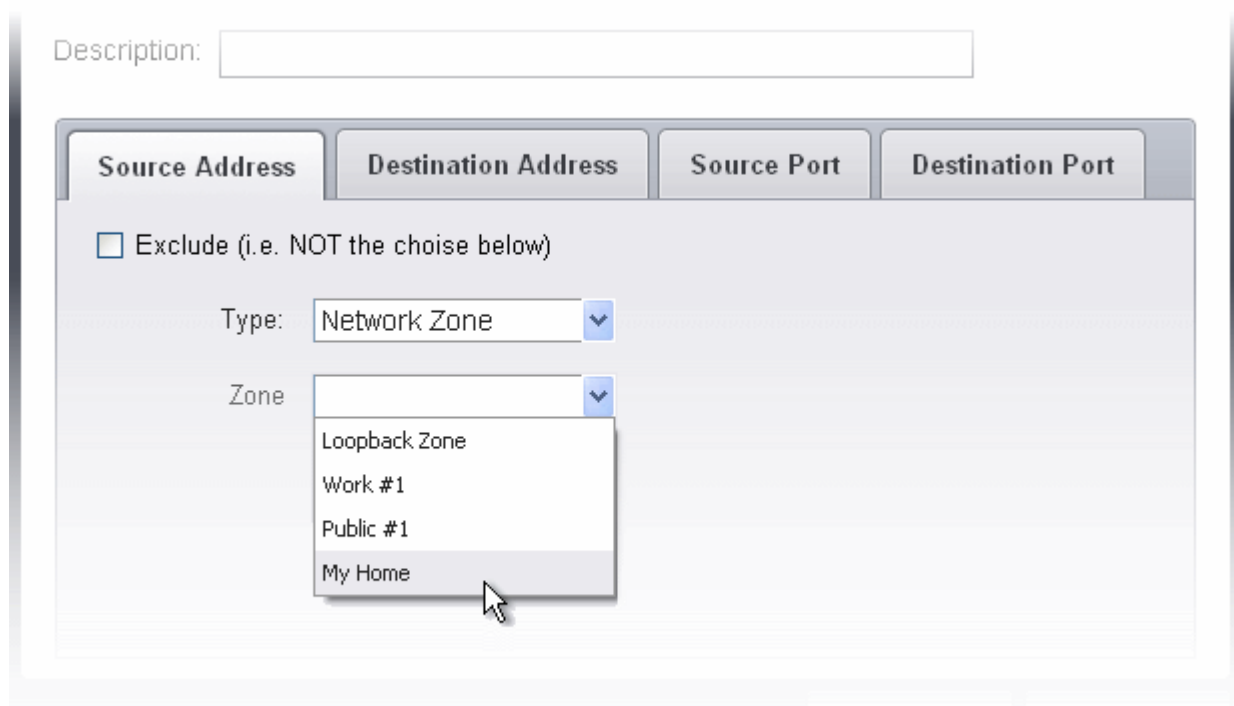
1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.

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:

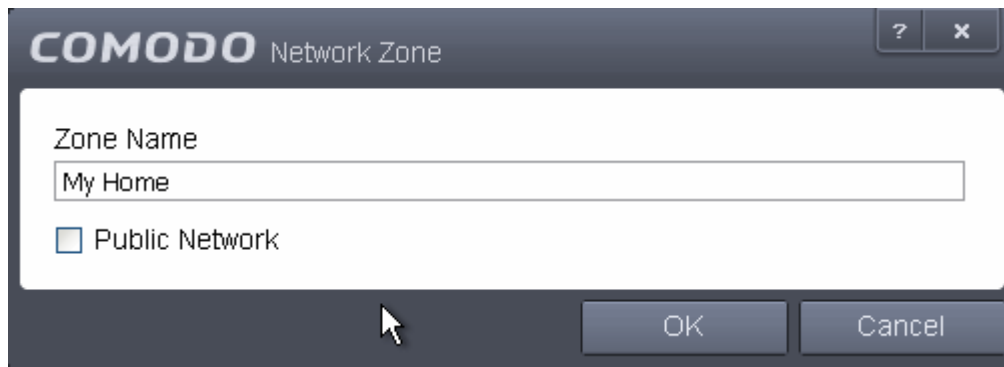
- Quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**



- 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.

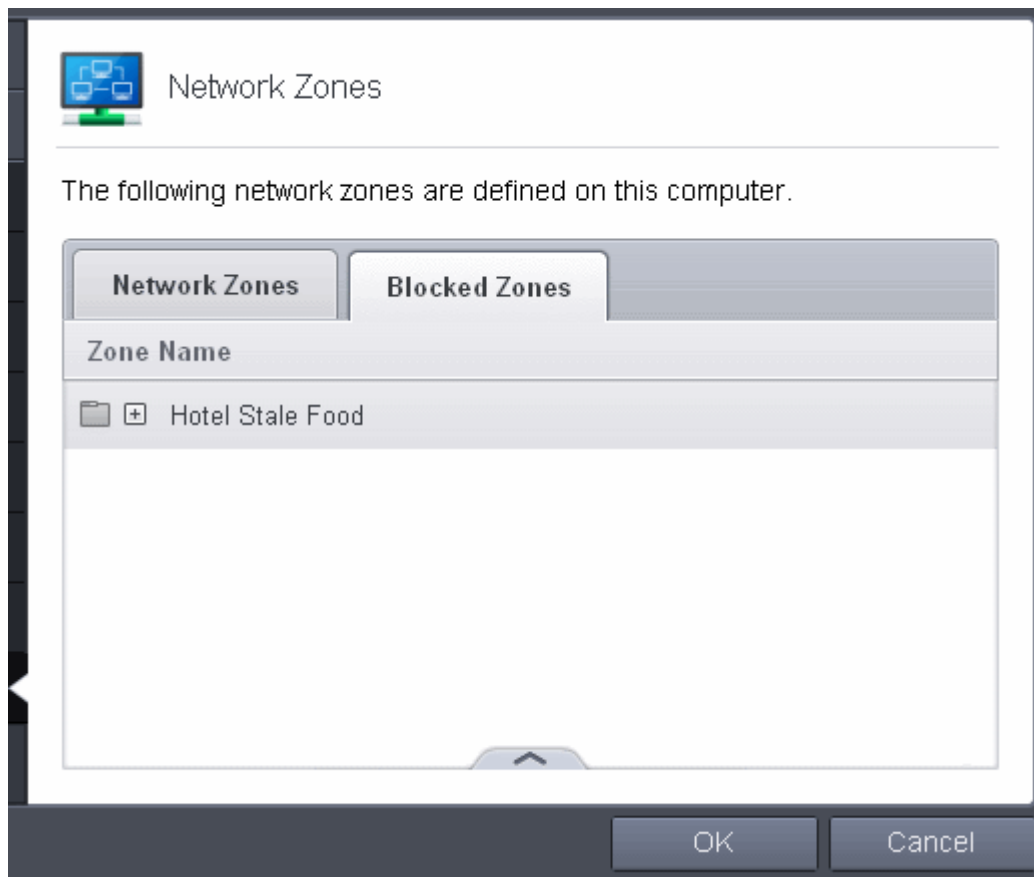
To modify or change the existing address in a zone

- 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

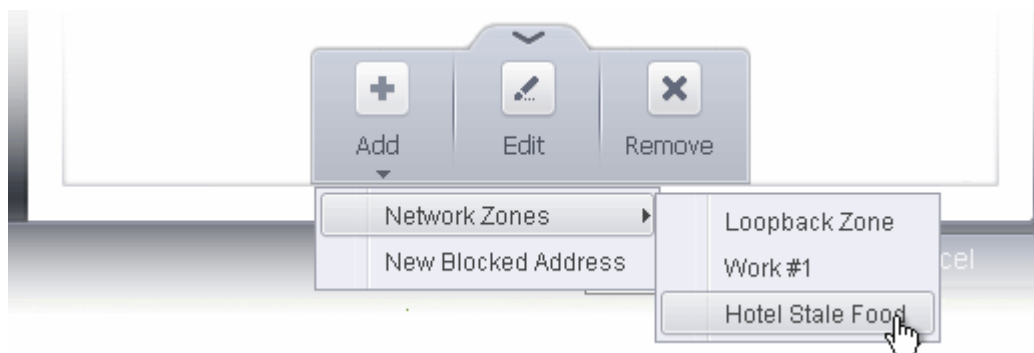
Note 1: You must create a zone before you can block it. There are two ways to do this;

1. Using '**Network Zones**' to name and specify the network you want to block.
2. Directly from this interface using 'New blocked address...'

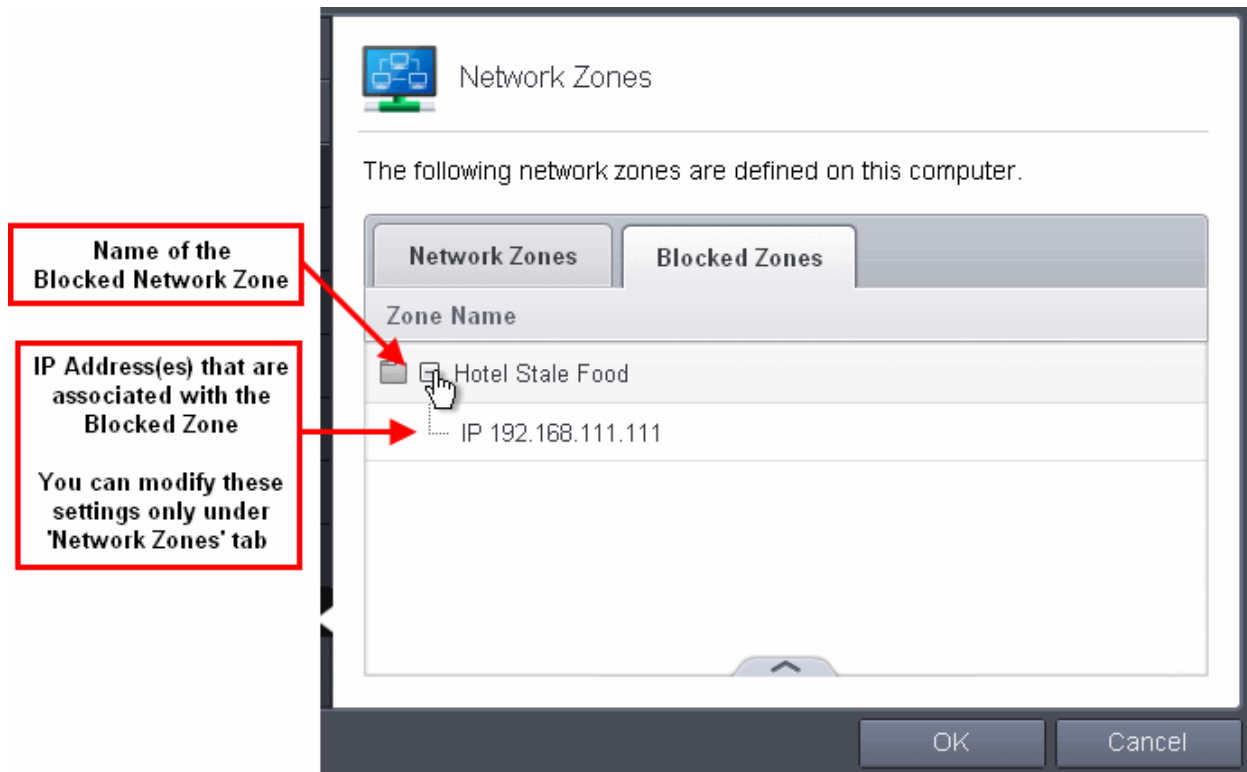
Note 2: You cannot reconfigure *pre-existing* network zones from this interface. (e.g., to add or modify IP addresses). You need to use '**Network Zones**' if you want to change the settings of existing zones.

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.

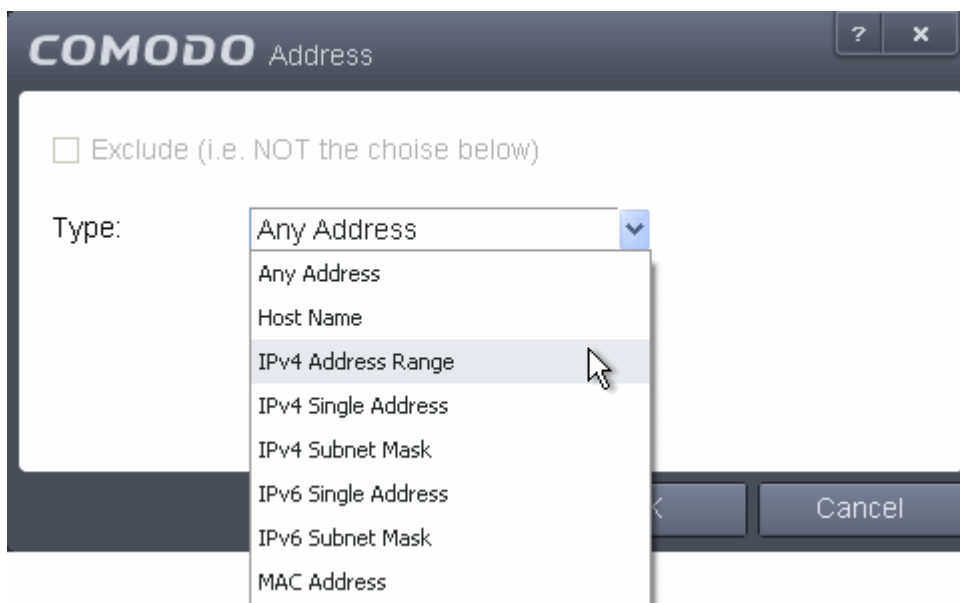


3. Click 'OK' to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

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.

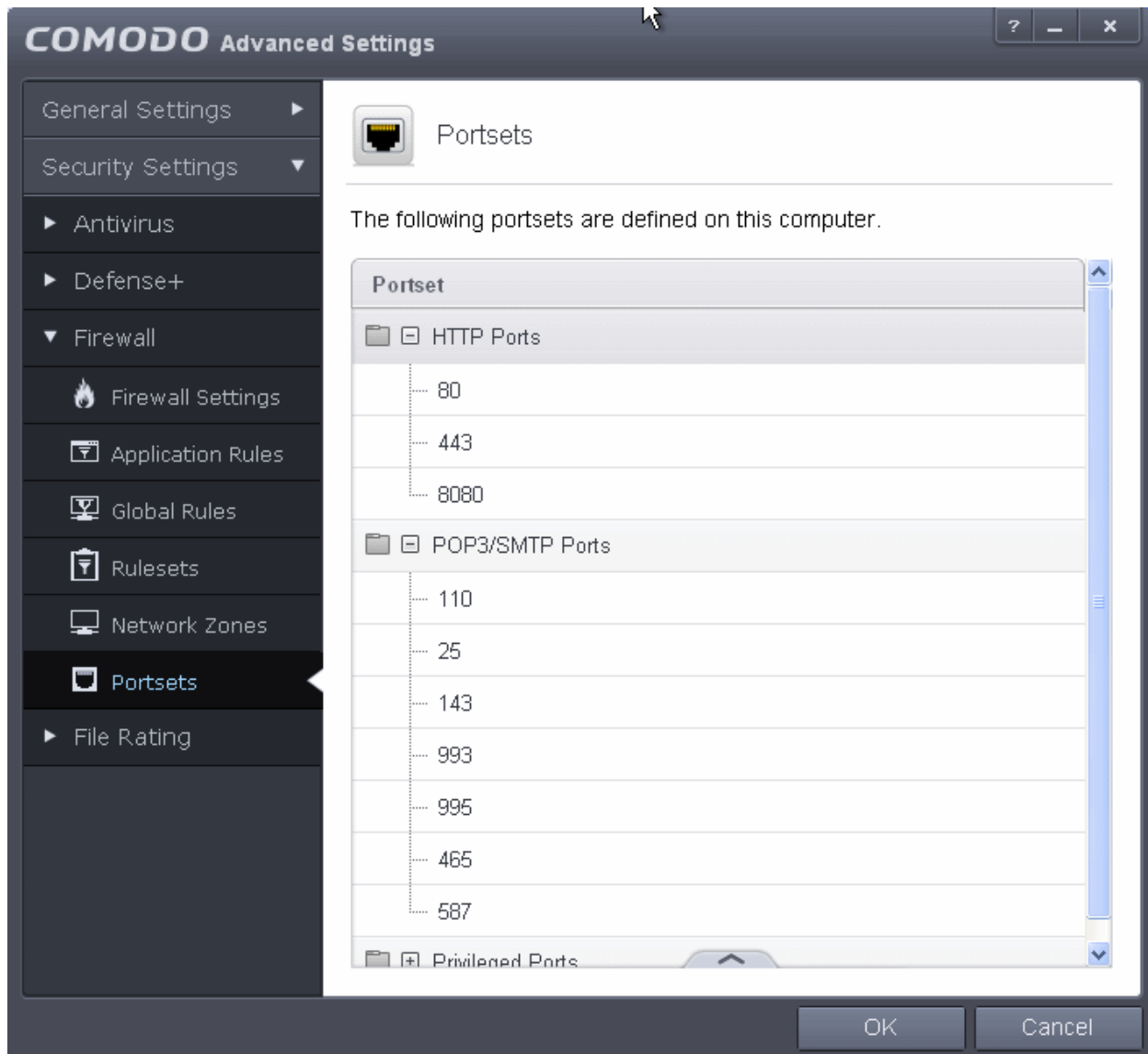
2. You can choose a named host by selecting a Host Name which denotes your IP address.
 3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
 4. You can choose a Single 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 to 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 expands the list of ports defined in it. The default port sets shipped with Comodo Internet Security are:

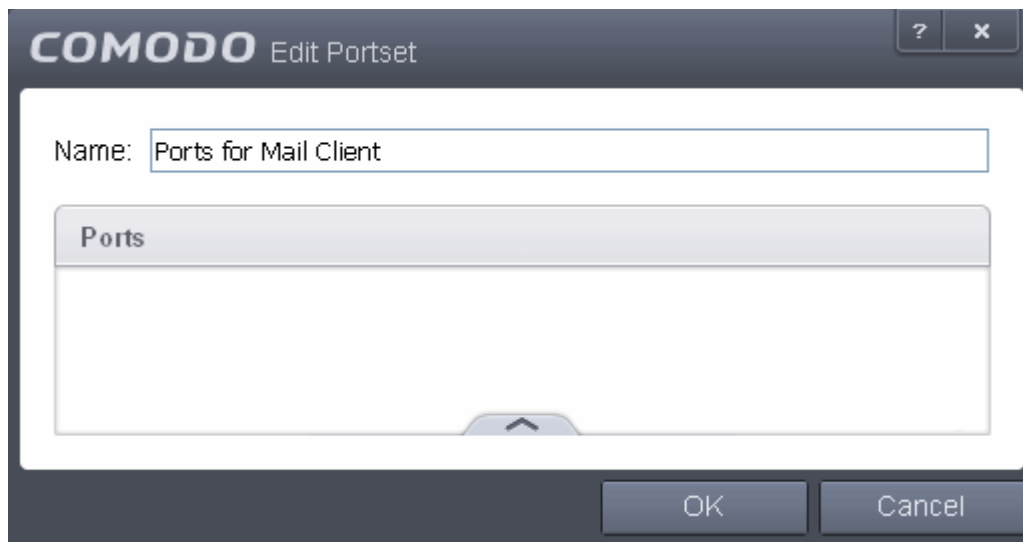
- **HTTP Ports:** 80, 443 and 8080. These are the default ports for http traffic. Your Internet browser uses these ports to connect to the Internet and other networks.
- **POP3/SMTP Ports:** 110, 25, 143, 995, 465 and 587. These are the ports that are typically used by mail clients like Outlook Express 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.

Defining a new Port Set

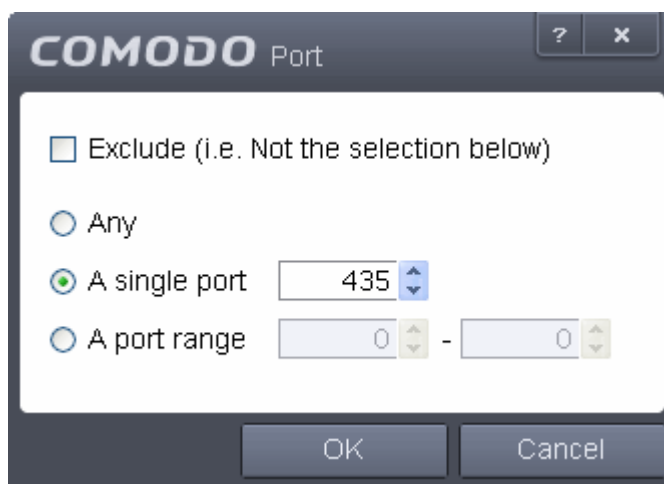
You can create new portsets and allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.

To add a new portset

1. Click the handle from the bottom center of the Portsets interface and select 'Add' from the options. The 'Edit 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 'Edit Portset' dialog. The



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**

Description:

Source Address	Destination Address	Source Port	Destination Port
<input type="checkbox"/> Exclude (i.e. NOT the choice below)			
Type: <input type="text" value="A Set of Ports"/>			
Start Port: <input type="text" value="HTTP Ports"/> <ul style="list-style-type: none"> HTTP Ports POP3/SMTP Ports Privileged Ports Ports for Mail Client 			
			<input type="button" value="OK"/> <input type="button" value="Cancel"/>

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.

6.2.4. Manage File Rating

The CIS rating system is a cloud-based file lookup service (FLS) that ascertains the reputation of files on your computer. Whenever a file is first accessed, CIS will check the file against our master whitelist and blacklists and will award it trusted status if:

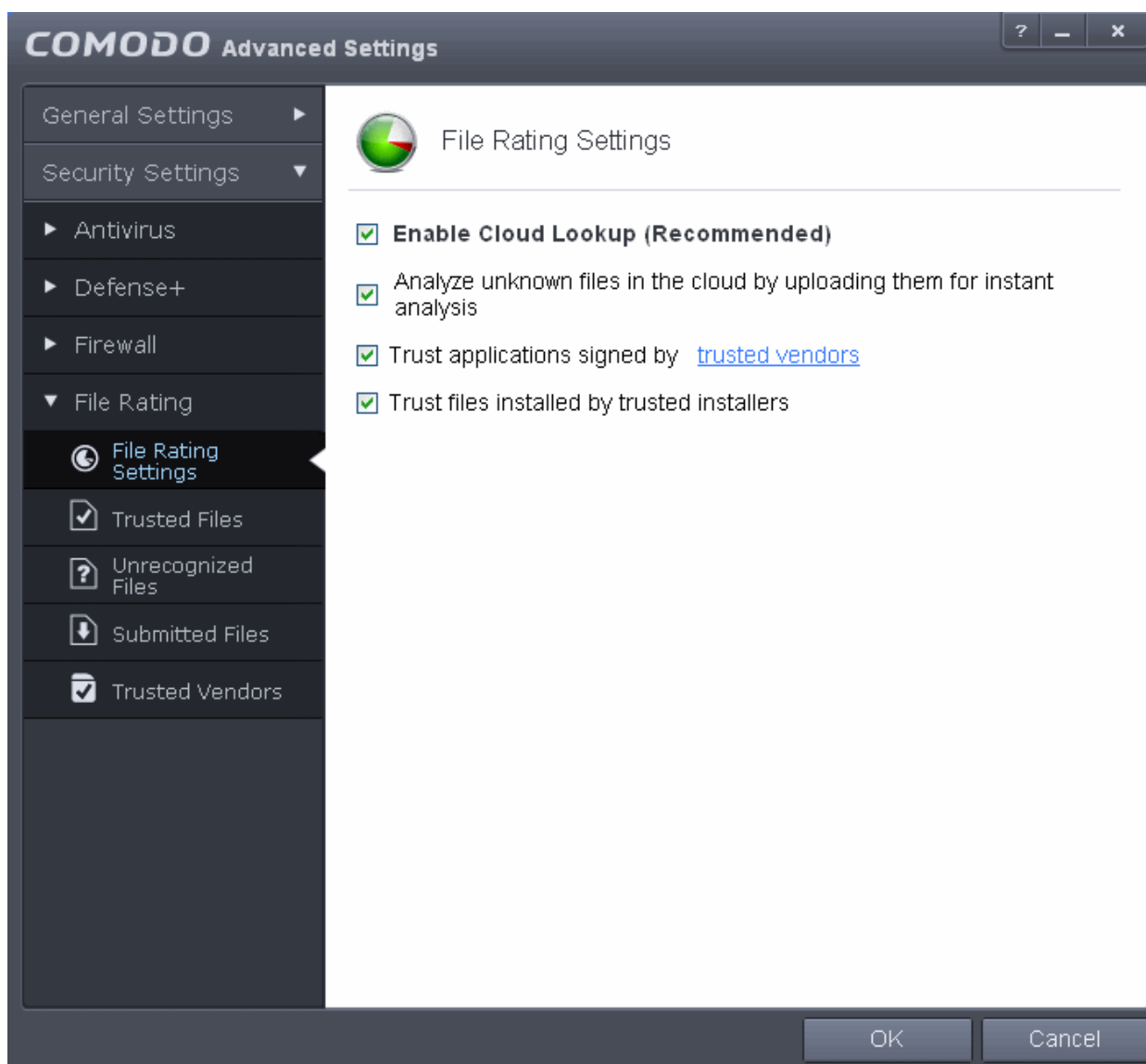
- The application/file is included in the Trusted Files list;
- The application is from a vendor included in the **Trusted Software Vendors** list;
- The application is included in the extensive and constantly updated Comodo safelist.

Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource consumption. On the other hand, files which are identified as malicious will be added to the **Blocked Files** list and denied all access rights from other processes or users - effectively cutting them off from the rest of your system. Files which could not be recognized by the rating system are added to the list of **'Unrecognized Files'**. You can review files on the unrecognized list and manually choose to trust/block/delete them or investigate further by sending them to Comodo for analysis/running another file lookup.

The 'Manage File Rating' area allows you to view and manage the list of Trusted Files and Unrecognized Files. You can also:

- Add files and executables to Trusted Files list manually;
- Submit unrecognized files and view the list of files you submitted;
- View and manage Trusted Software Vendor list;

from this area.



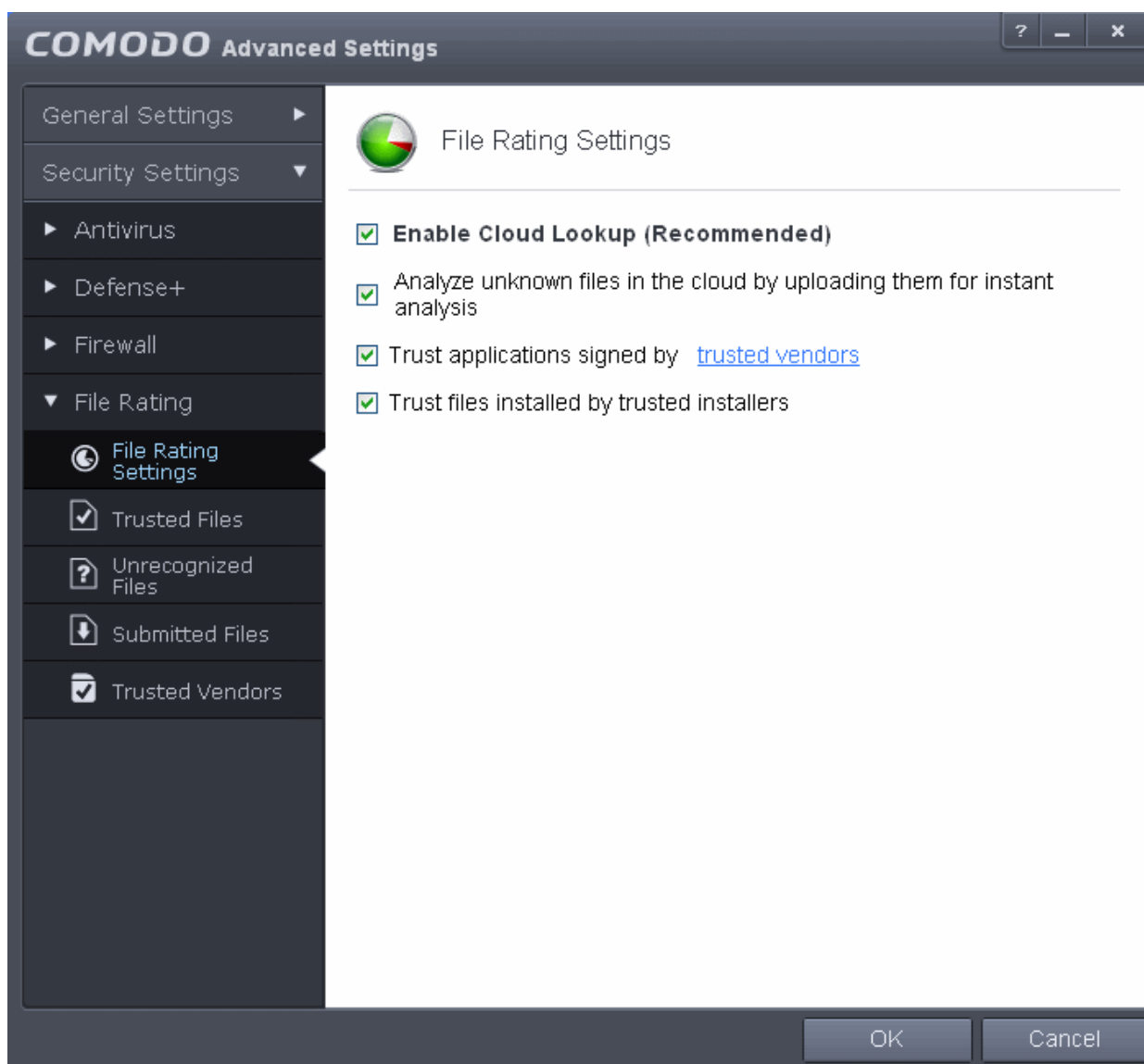
Click the following links to jump to the section you need help with:

- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **Trusted Files** - View the list of trusted files and manually add files to it
- **Unrecognized Files** - View and manage unrecognized items.
- **Submitted Files** - View the list of files submitted for analysis to Comodo.
- **Trusted Vendors** - View the list of trusted software vendors and manually add vendors

6.2.4.1. File Rating Settings

The File Rating Settings panel allows you to configure the overall behavior of File Rating feature of Comodo Internet Security.

- 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 upload files whose trustworthiness could not be assessed by cloud lookup to Comodo for analysis immediately. The experts at Comodo will analyze the file and add to the the whitelist or blacklist according to the analysis. (*Default =Enabled*)
- **Trust applications signed by trusted vendors** - When this option is enabled, CIS will award trusted status to the executables and files that are digitally signed by vendors in the Trusted Vendors list using their code signing certificates. Click the words 'trusted vendors' will open the **Trusted Vendors** panel. (*Default =Enabled*)
- **Trust files installed by trusted installers** - When this option is enabled, CIS will consider the executable and files stored by applications that are assigned with Installer or Updater rule under **HIPS Rules** or the applications. (*Default =Enabled*)

6.2.4.2. Trusted Files

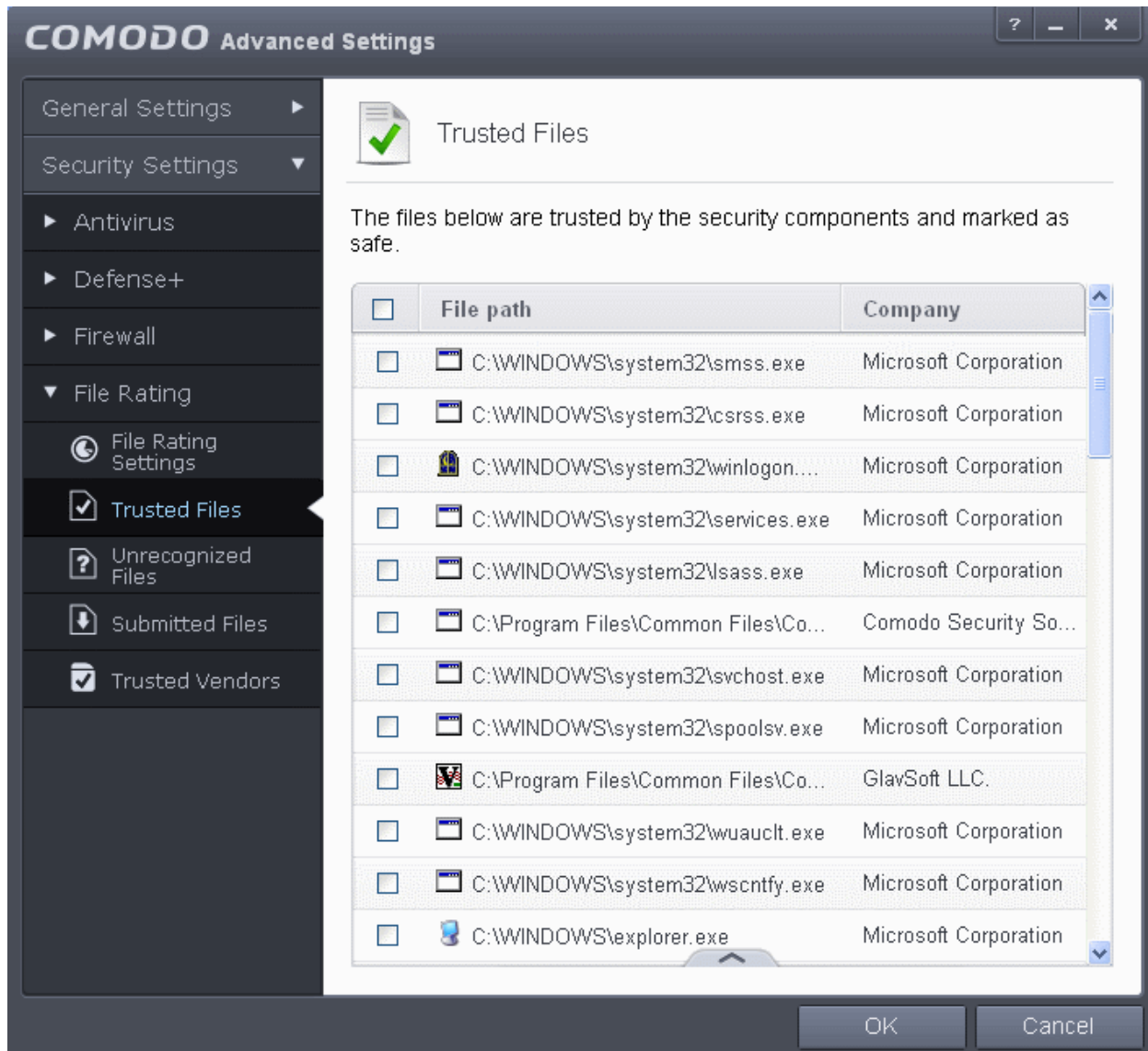
Files added to the Trusted Files list are automatically given Defense+ trusted status. If an executable is unknown to the Defense+ safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, you could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted Files'.

CIS allows you to define a personal safe list of files to complement the default Comodo safe list.

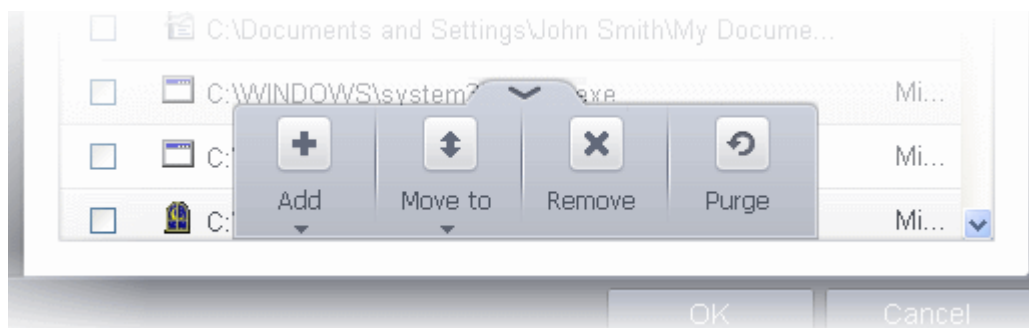
By adding executables to this list (including sub folders containing many components) you can reduce the amount of alerts that HIPS generates whilst maintaining a higher level of Defense+ security. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list. Files can be transferred into this module by

clicking the 'Move to' button in the 'Unrecognized Files' area.

- The Trusted Files panel can be accessed by clicking Security Settings > File Rating > Trusted Files from the Advanced Tasks interface



Clicking the handle at the bottom center of the panel opens the following options:



- **Add** - Allows you to add files to Trusted Files list manually
- **Move** - Allows you to move files from Trusted Files list to Blocked Files or Unrecognized Files list
- **Remove** - Allows you to remove files from Trusted Files list
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path

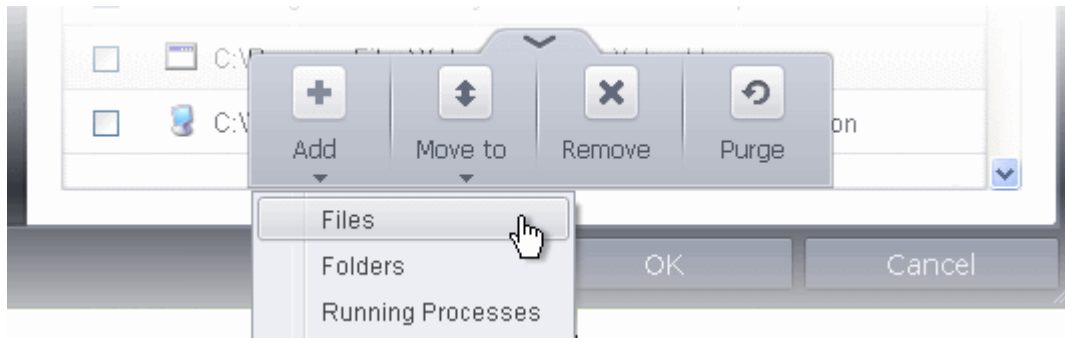
specified. If not, the file is removed, or 'purged', from the list.

Adding files to Trusted Files list

CIS allows you to add files and executables to the list of Trusted Files so that those files will be given Trusted status. For the files added manually, it 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. However you can also add files by their file names, but if you happen to change the file name later, it loses its 'Trusted' status.

To add new file(s) to Trusted Files list

- Click the handle from the bottom center and choose 'Add'

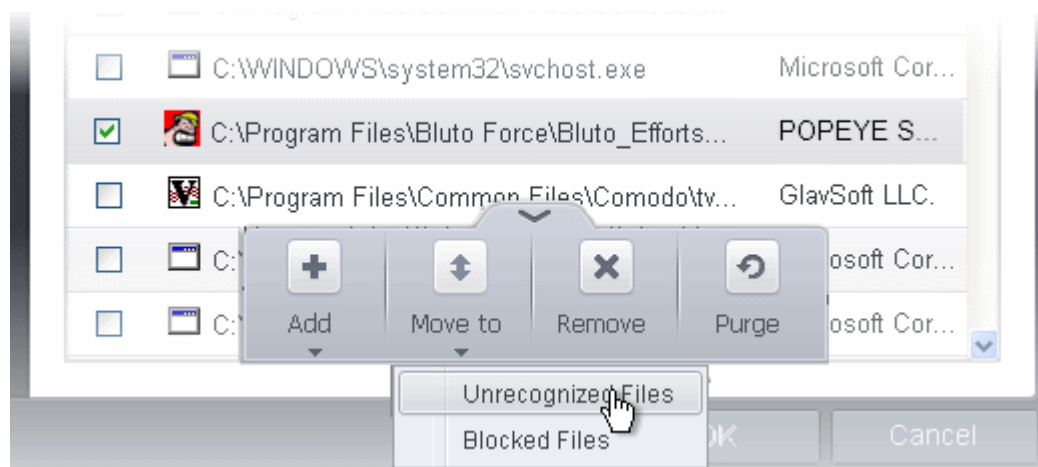


You can add files to the Trusted Files list by three ways:

- 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.
- Click OK for your changes to take effect.

To move an included entry to Unrecognized Files or Blocked Files

- Select the entry to be transferred *out* of the 'Trusted Files' list into either **Unrecognized Files** or **Blocked Files**. You can select several entries to be moved at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Move'



- Choose 'Unrecognized Files' or 'Blocked Files' from the drop-down.
- Click OK for your changes to take effect.

To remove an included entry from the Trusted Files list

- Select the entry to be removed from the 'Trusted Files' list. 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.
- Click OK for your changes to take effect.

6.2.4.3. Unrecognized Files

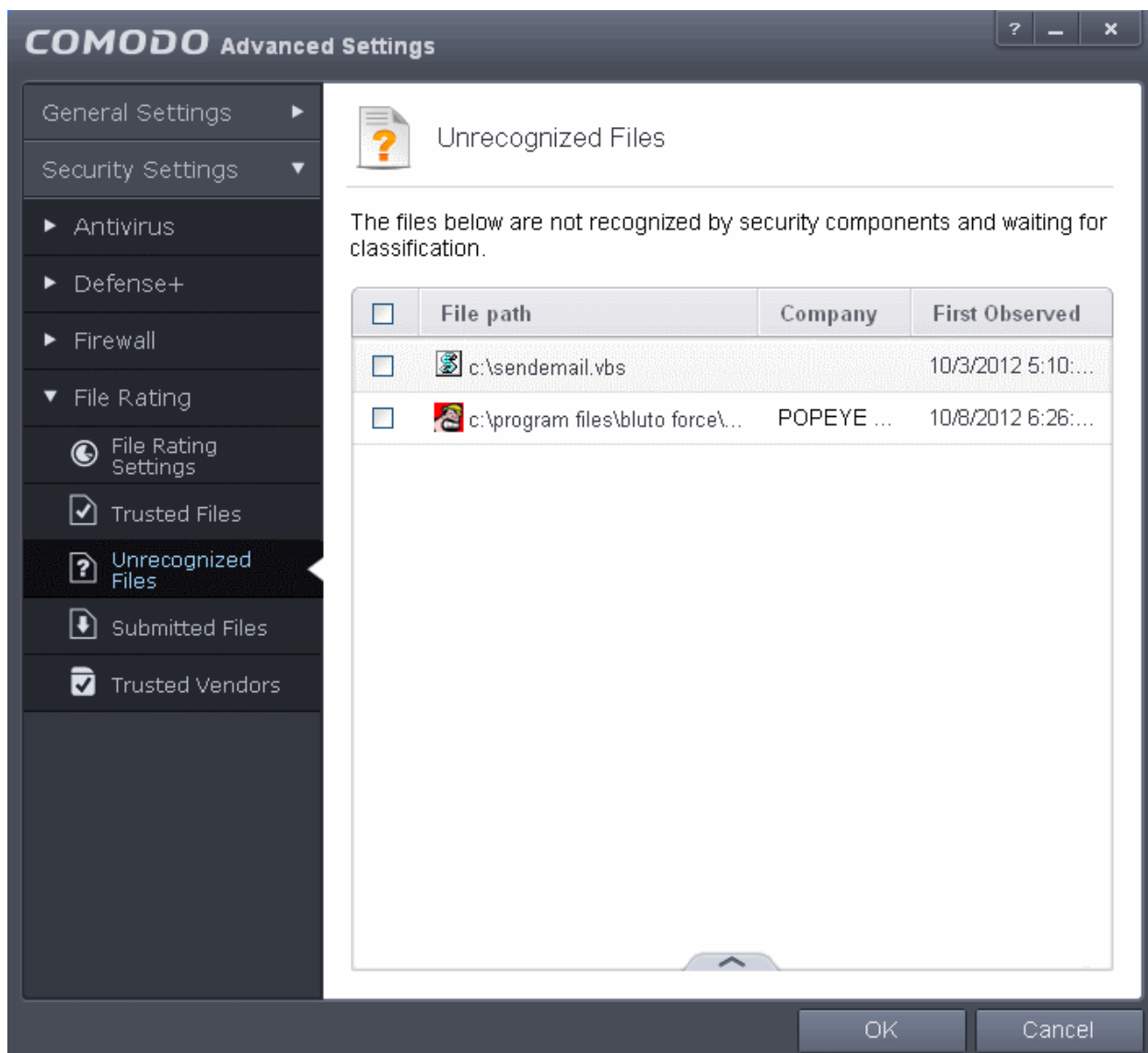
Once installed, the HIPS watches all file system activity on your computer. Every new executable file introduced to the computer, is first scanned against the Comodo certified safe files database. If they are not safe, they are added to the 'Unrecognized Files' for users to review and possibly submit to Comodo. Apart from new executables, any executables that are modified are also moved to the 'Unrecognized Files' area.

'Unrecognized Files' is specifically important while HIPS is in 'Clean PC Mode'. In Clean PC Mode, the files in 'Unrecognized Files' are NOT considered clean. For more information, please check ['Clean PC Mode' on the HIPS settings page](#).

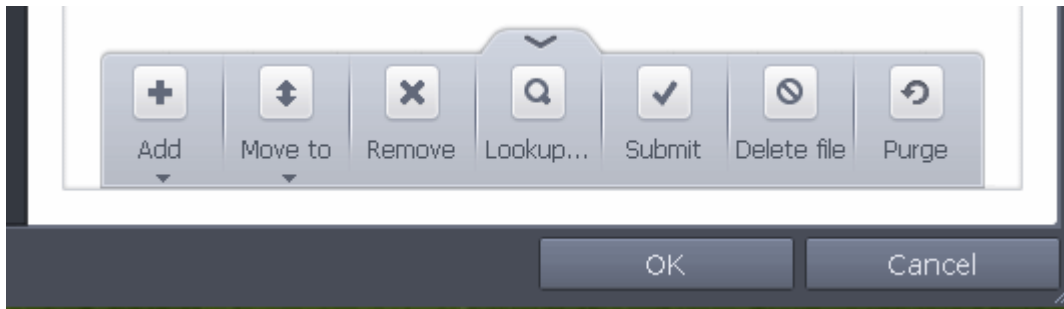
The 'Unrecognized Files' panel displays the list of files added as Unrecognized Files and allows you to assess the pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be moved to 'Trusted Files' using the **'Move to'** button. Similarly, files that are suspicious can be moved to the **'Blocked Files'** area.

You can also add files upon which you are suspicious into 'Unrecognized Files' list to check whether the master Comodo safe list contains more information on them or to 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.

- The Unrecognized Files panel can be accessed by clicking Security Settings > File Rating > Unrecognized Files tab from the Advanced Tasks interface



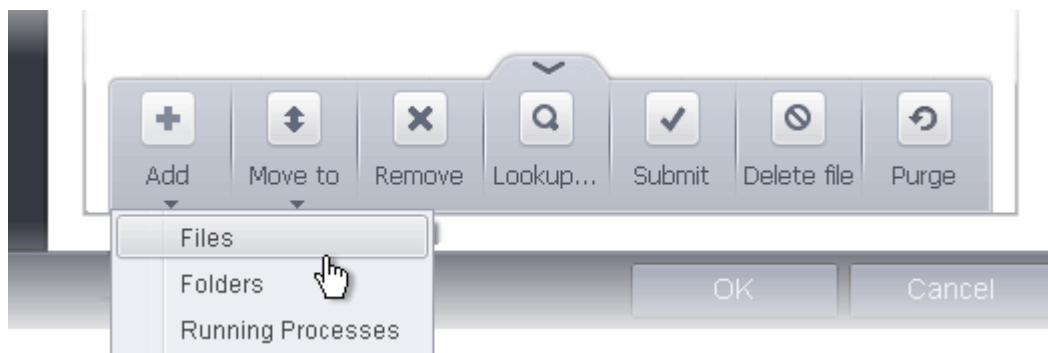
Clicking the handle at the bottom center of the panel opens the following options:



- **Add** - Allows you to add files to 'Unrecognized Files' list manually
- **Move** - Allows you to move files from 'Unrecognized Files' list to Trusted Files or Blocked Files list
- **Remove** - Allows you to remove files from 'Unrecognized Files' 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**.
- Delete file - 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 is removed, or 'purged', from the list.

To manually add files to 'Unrecognized Files' list

- Click the handle from the bottom center and choose 'Add'

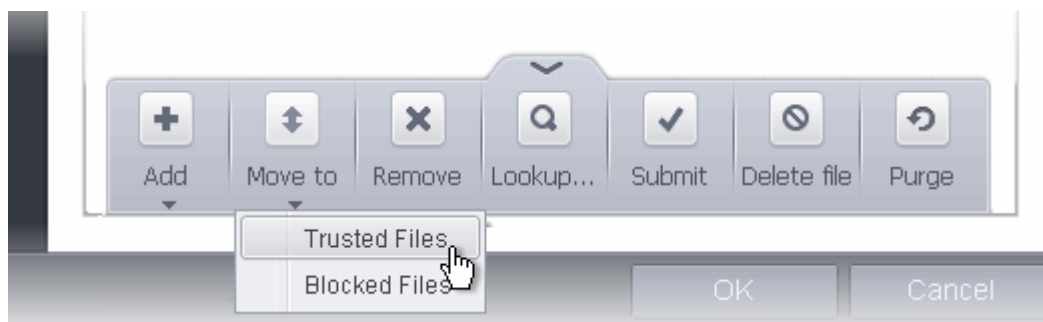


You can add files to the Unrecognized Files list by three ways:

- **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 'Unrecognized 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 'Unrecognized Files' list.
- Click OK for your changes to take effect.

To move an included entry to Trusted Files or Blocked Files

- Select the entry to be transferred *out of* the 'Unrecognized Files' list into either **Trusted Files** or **Blocked Files**. You can select several entries to be moved at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Move'



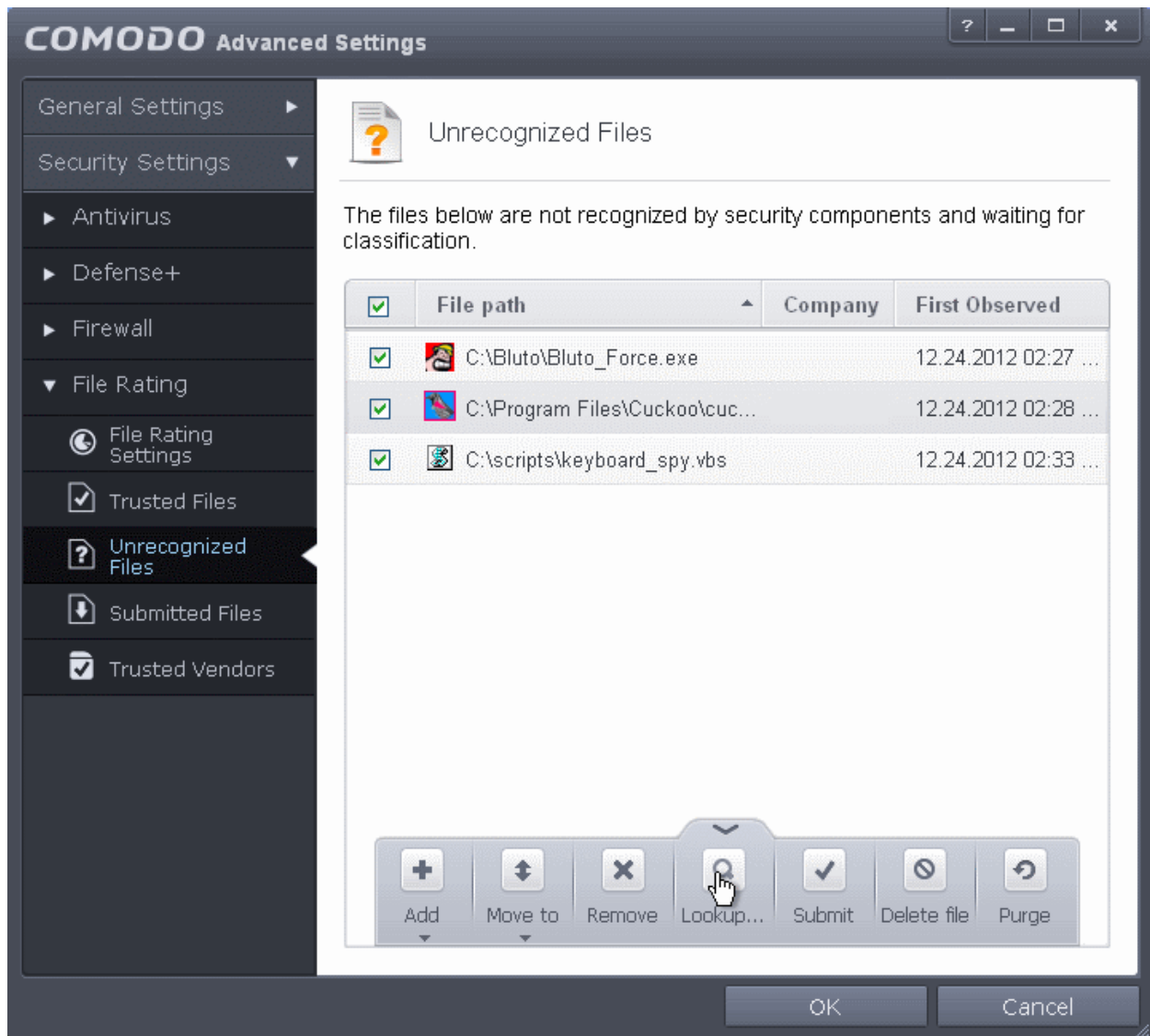
- Choose 'Trusted Files' or 'Blocked Files' from the drop-down.
- Click OK for your changes to take effect.

To remove an included entry from the Unrecognized Files list

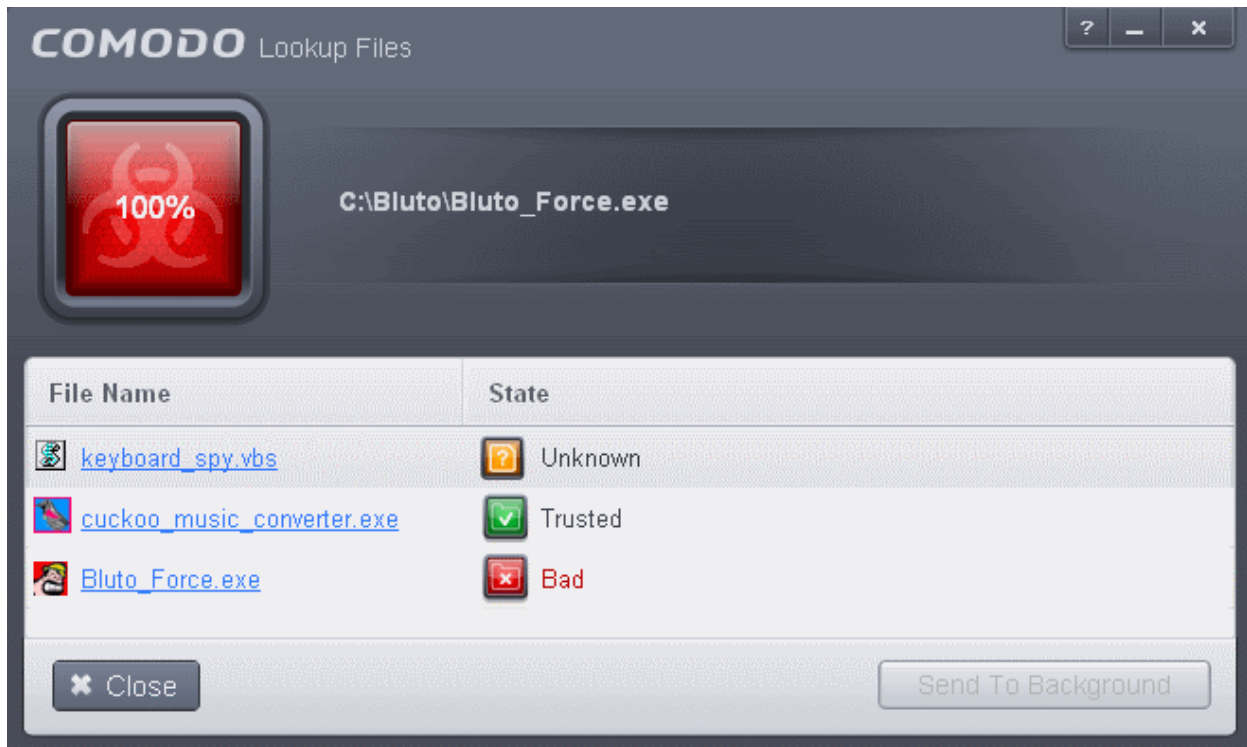
- Select the entry to be removed from the 'Unrecognized Files' list. You can select several entries to be removed at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Remove'. The file is only removed from the list and not deleted from your system.
- Click OK for your changes to take effect.

To perform an online lookup for unrecognized files

- Select the files to be checked from the 'Unrecognized Files' list. You can select several entries at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Lookup...!'



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 a file is found to be malicious, it will be indicated as 'Bad' with a red icon. You can **move it to Blocked Files**.
- If the file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can **move it to Trusted Files**.
- If no information is available, it will be indicated as 'Unknown' with a yellow icon. You can **submit the file to Comodo for analysis**.

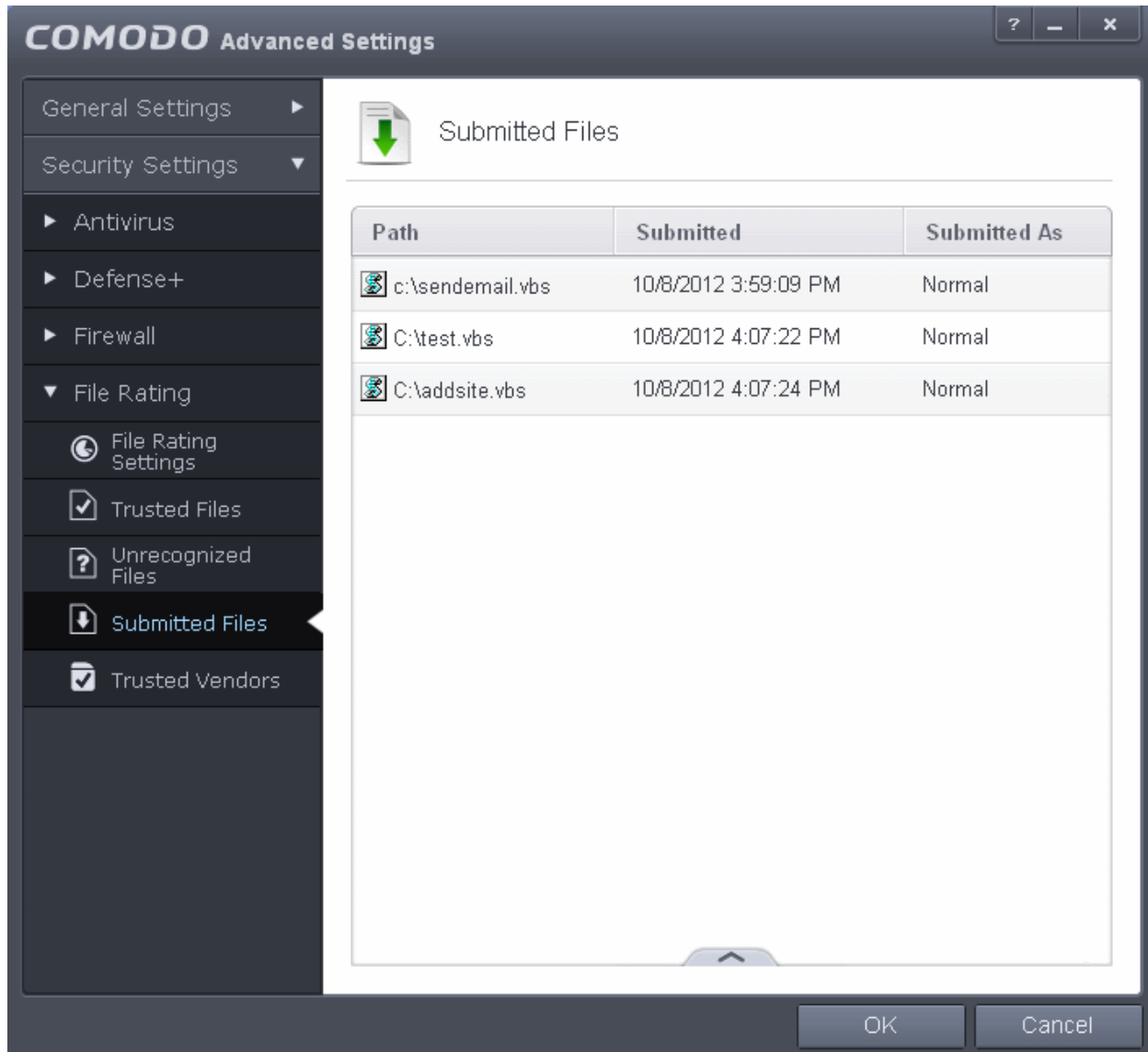
To manually submit files to Comodo

- Select the entry to be submitted from the 'Unrecognized Files' list. You can select several entries to be sent at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Submit'. The file(s) will be immediately sent to Comodo.

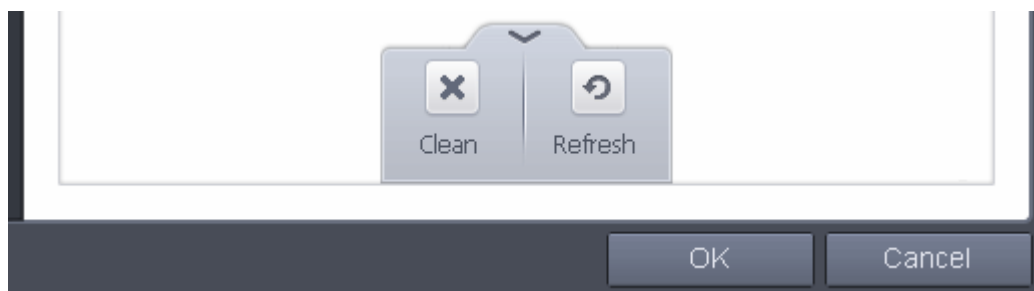
You can view the list of files you submitted so far, from the **Submitted Files** panel.

6.2.4.4. Submitted Files

The Submitted Files panel displays a list of files you have submitted so far for analysis to Comodo.



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:

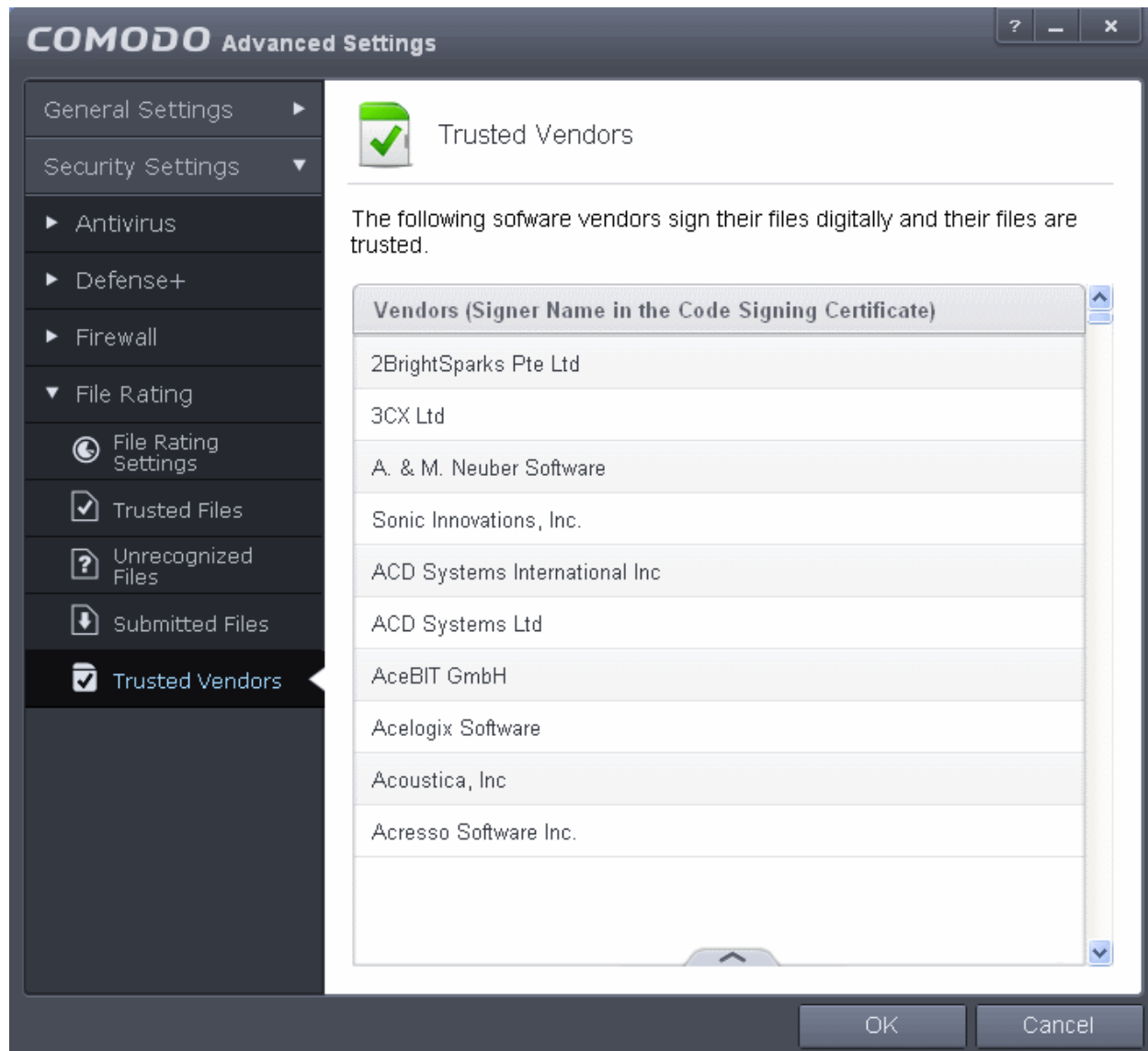
- IF the vendor is on the Trusted Software Vendor List AND the user has enabled '**Trust Applications signed by Trusted**

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.



[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:

- Content Source:** The software they are downloading and are about to install *really comes from the publisher that signed it.*
- Content Integrity:** That the software they are downloading and are about to install *has not be modified or corrupted since it was signed.*

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't

been tampered with - that are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to its probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

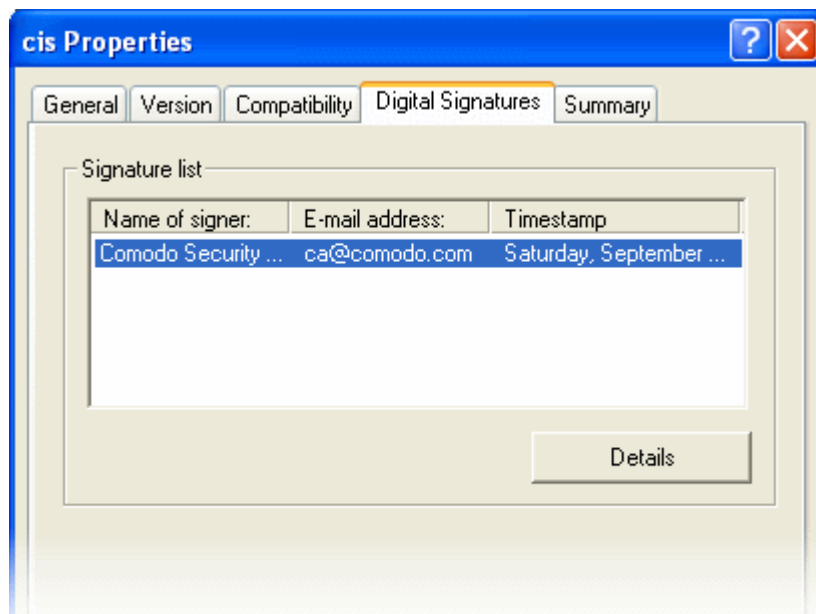
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 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/>).

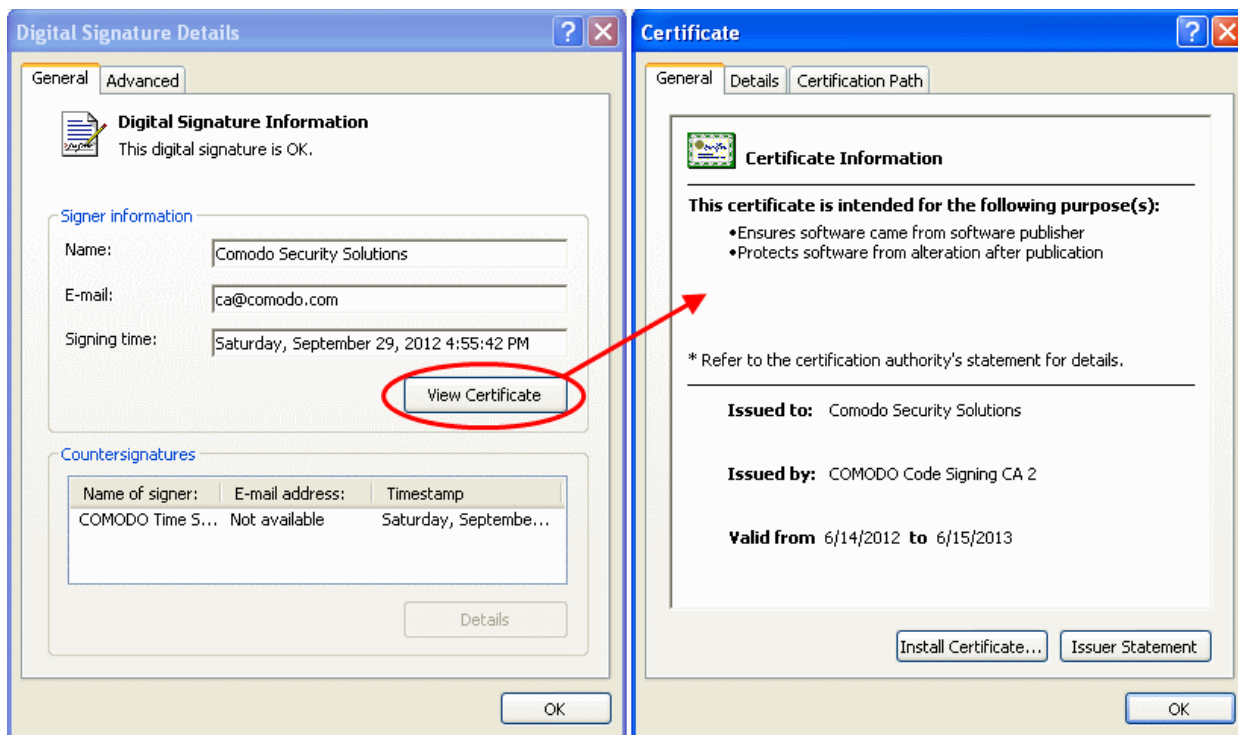
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Internet Security is called 'cfp.exe' and has been digitally signed.

- Browse to the (default) installation directory of Comodo Internet Security.
- Right click on the file cfp.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 'cfp.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.

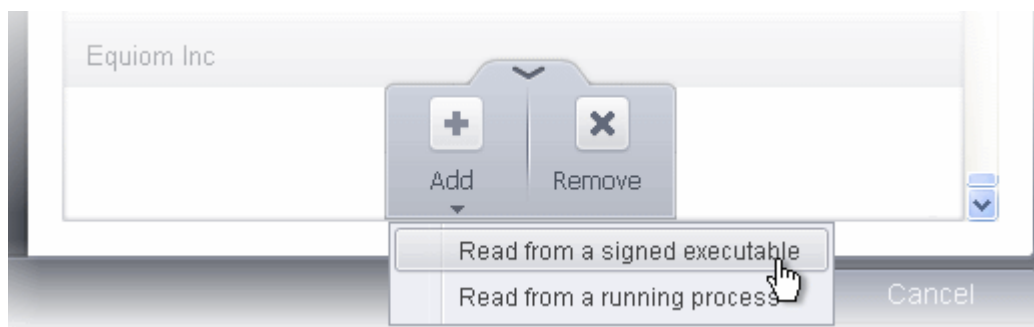
Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

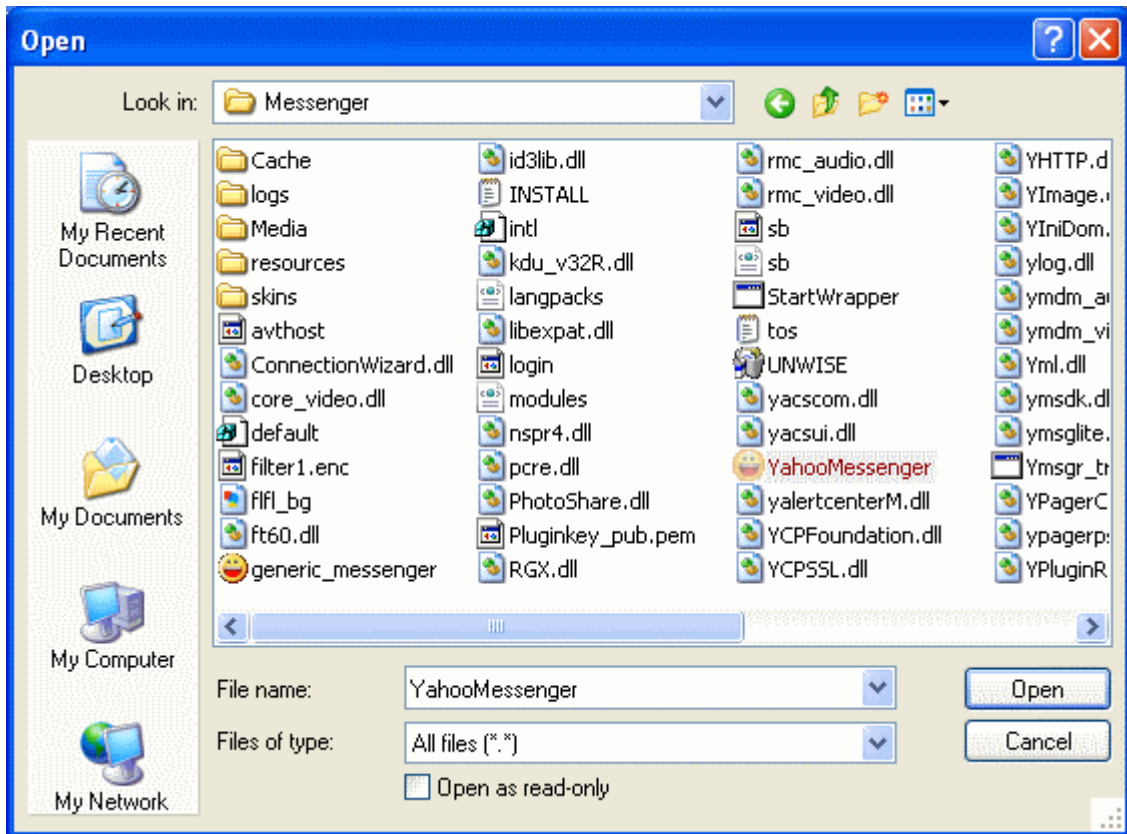
- **By reading the vendor's signature from an executable file on your local drive**
- **By reading the vendor's signature from a running process**

To add a trusted vendor by reading the vendor's signature from an executable

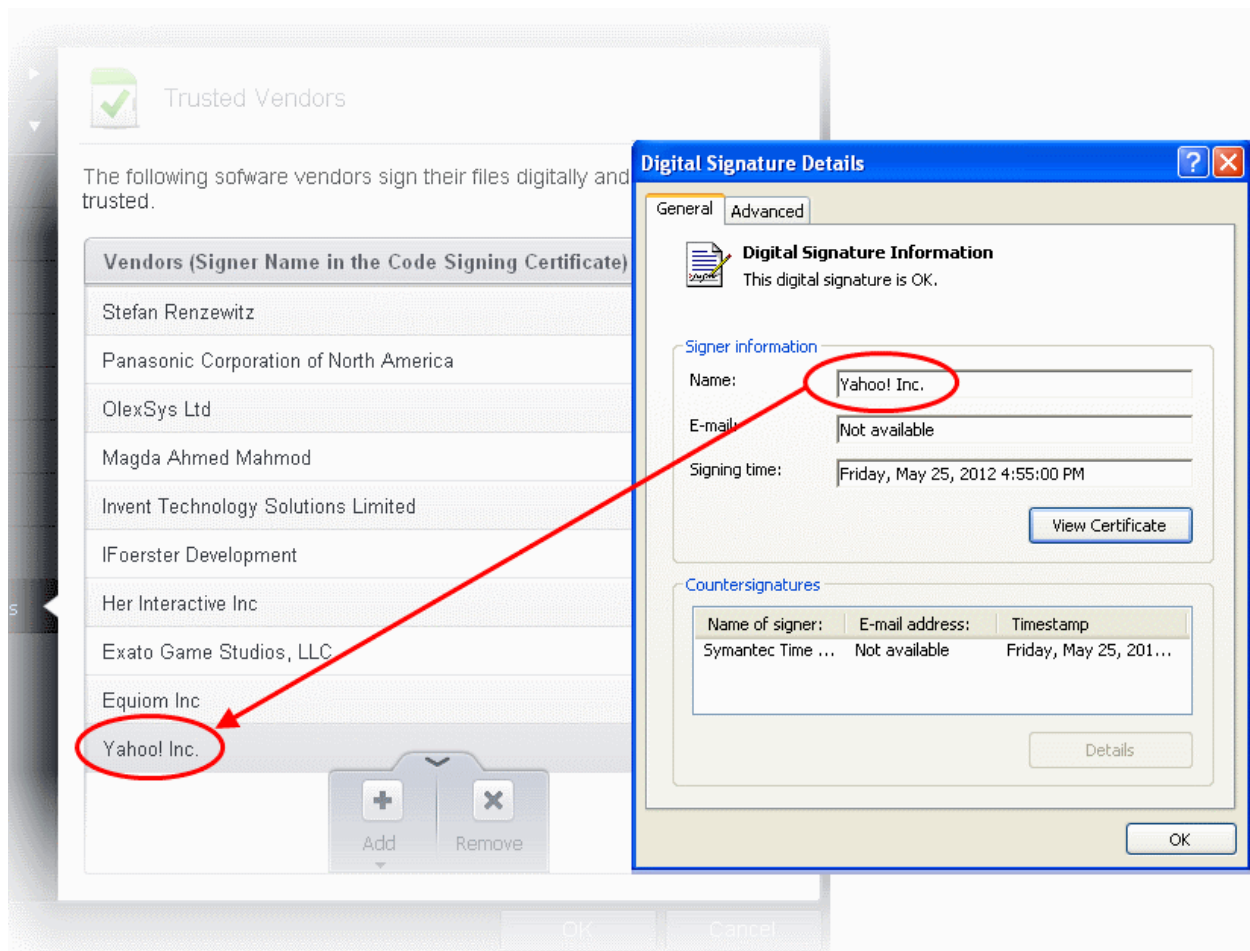
- Click the handle from the bottom center and choose 'Add' > 'Read from a signed executable'



- 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):



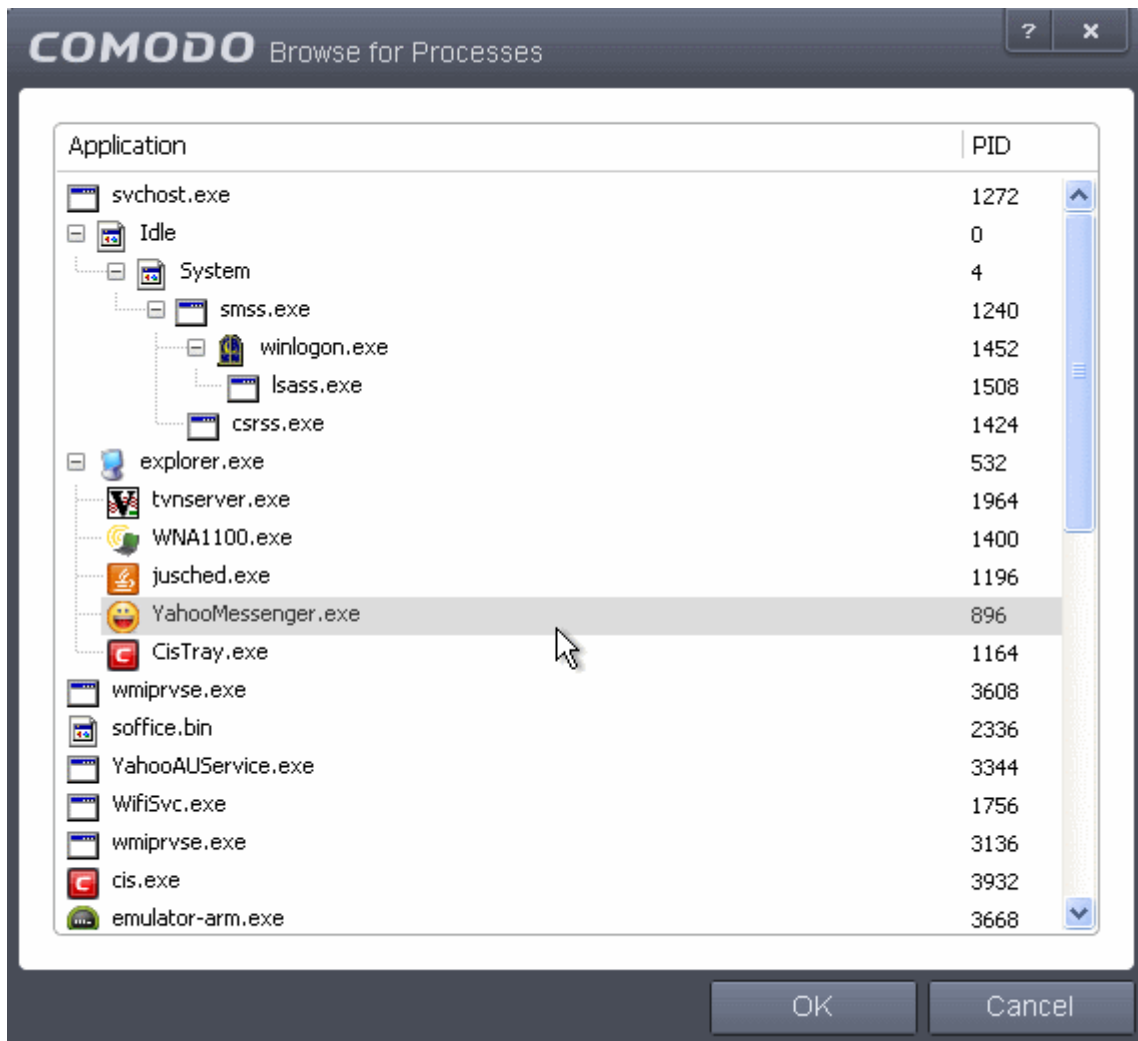
In the example above, Comodo Internet Security was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to the list. All future software that 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'

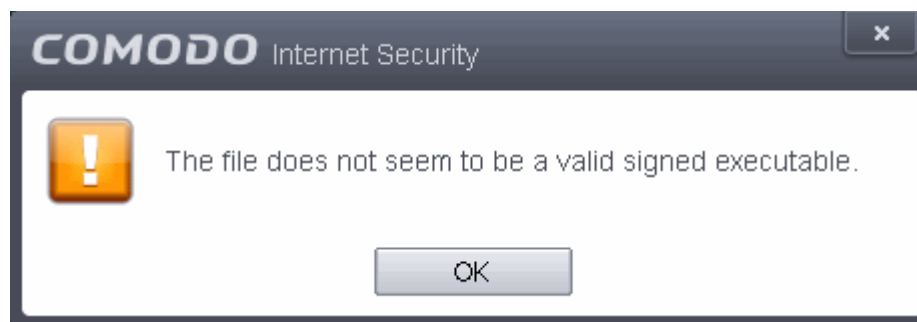


- Select the signed executable that you want to trust and click the 'OK' button.



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 its capacity as a Trusted CA, has independently validated as legitimate companies. If the user needs to remove any of these vendors from the list, it can be done by selecting the vendor, clicking 'Remove' and restarting the system. Please note that the removal will take effect only on restarting the system.

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 new features in CIS 6.0 is that now you can immediately launch a chat with a qualified computer support technician by



clicking this icon in the title bar controls at the top right side of the main interface.

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**
- **Starting and Using AntiError**
- **Uninstalling Comodo GeekBuddy**

7.1. Overview of Services

Comodo GeekBuddy includes the following services:

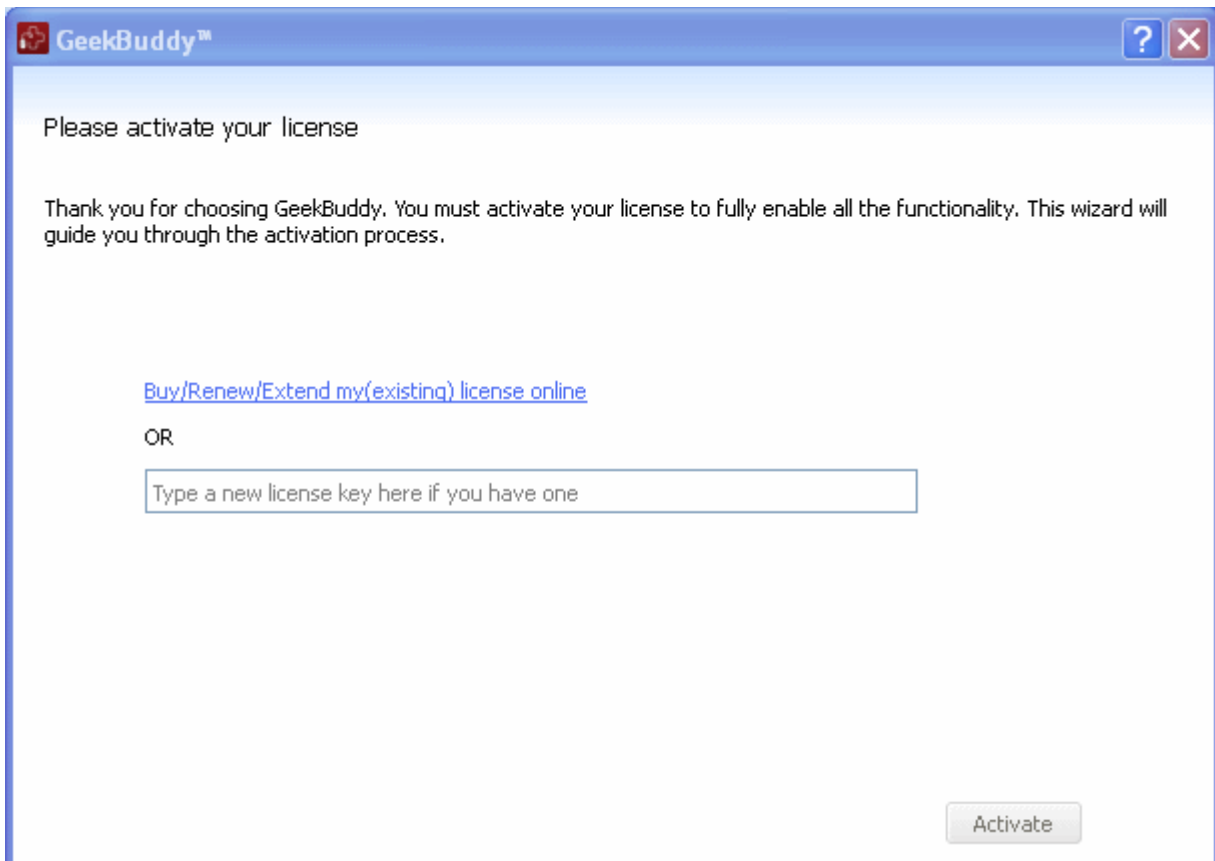
- **Virus & Malware Removal** - Our technicians remotely clear any detected viruses or malware that is found on your PC.
- **Internet and Online Identity Security** - Optimization of your computer's security settings to prevent loss of sensitive data and identity theft.
- **Printer or Email Account Setup** - 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

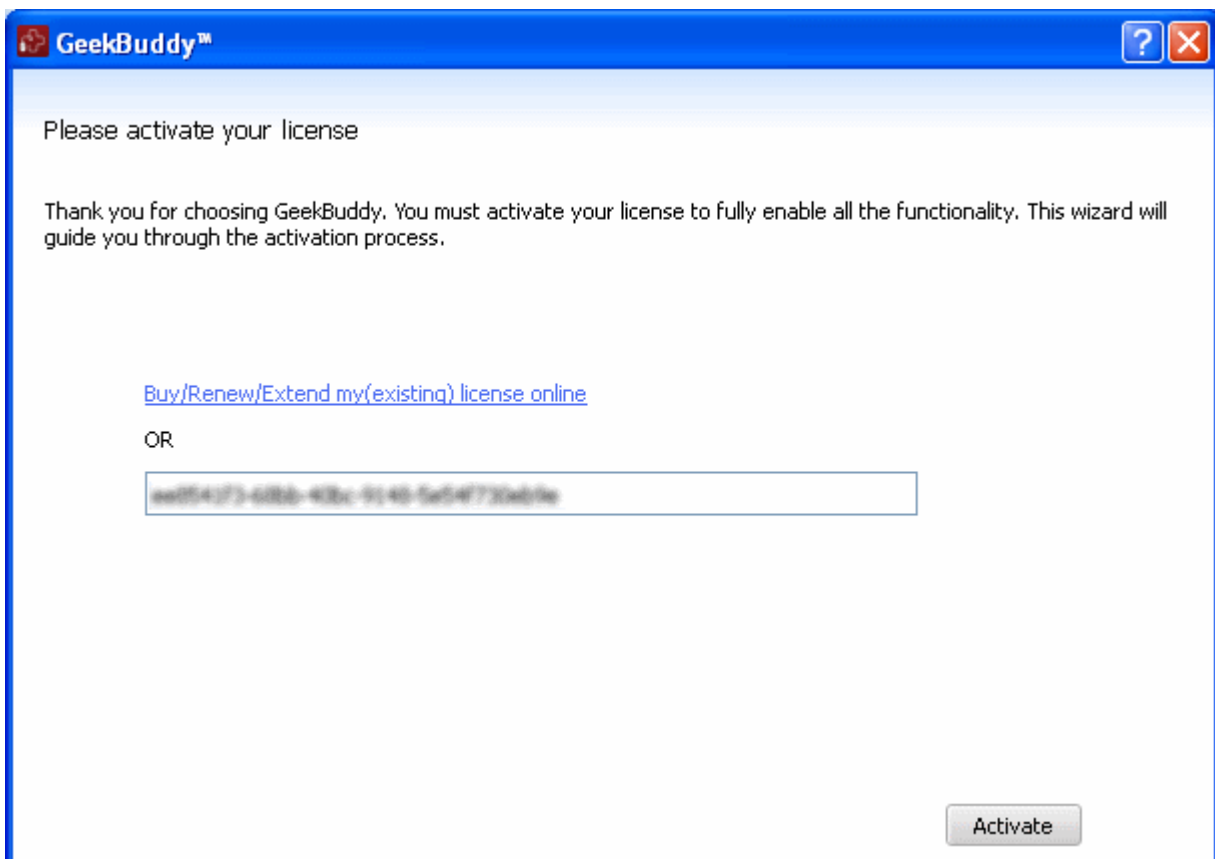
GeekBuddy is included in CIS Pro and Complete versions and users who purchased either of these CIS versions can skip this section and move on to the next section '**Launching the Client and Using the Service**'. GeekBuddy client is downloaded along with CIS Premium (a free version), but to use this service, you have to purchase and activate it.



Start the GeekBuddy client by clicking the desktop shortcut icon  or from the 'Start Menu'. The 'Activate your License' screen will be displayed.

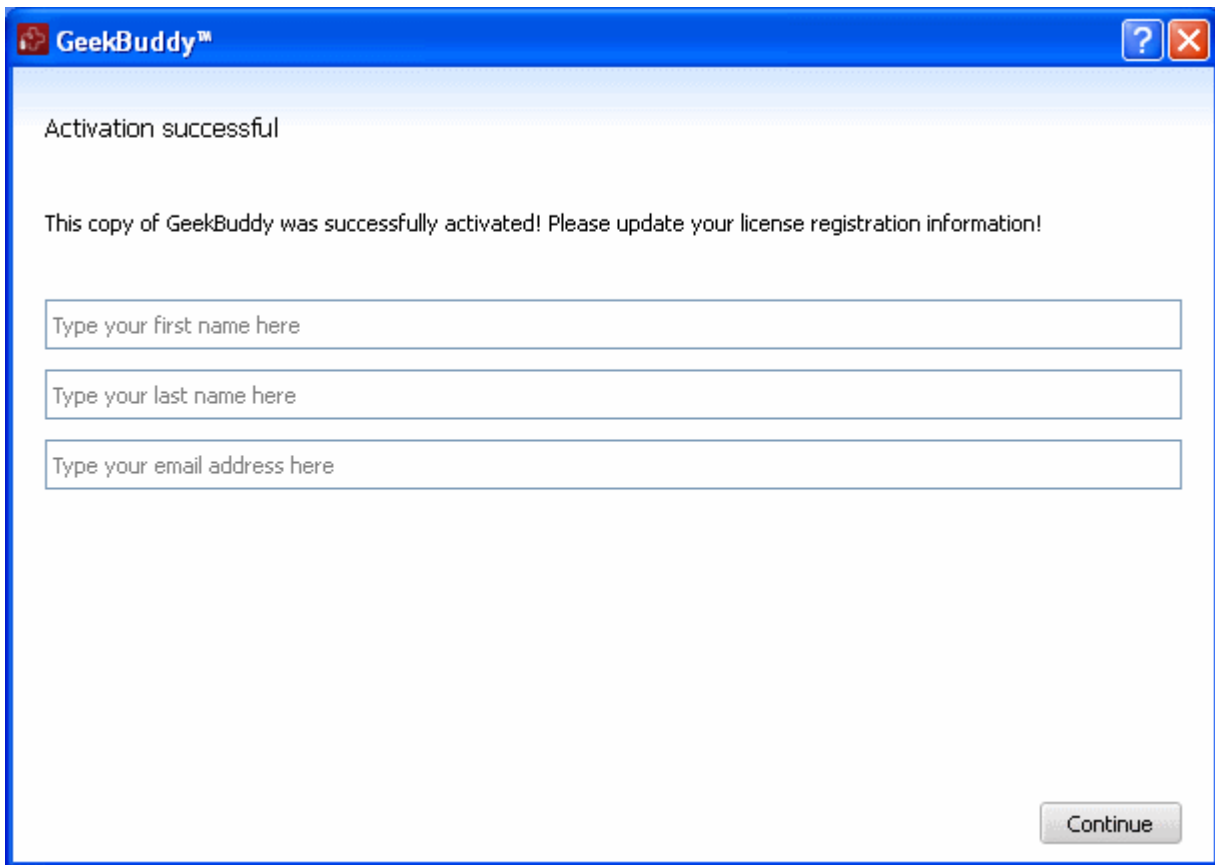


- Enter the License Key from your GeekBuddy retail package or the key you received through your email (for online purchases).

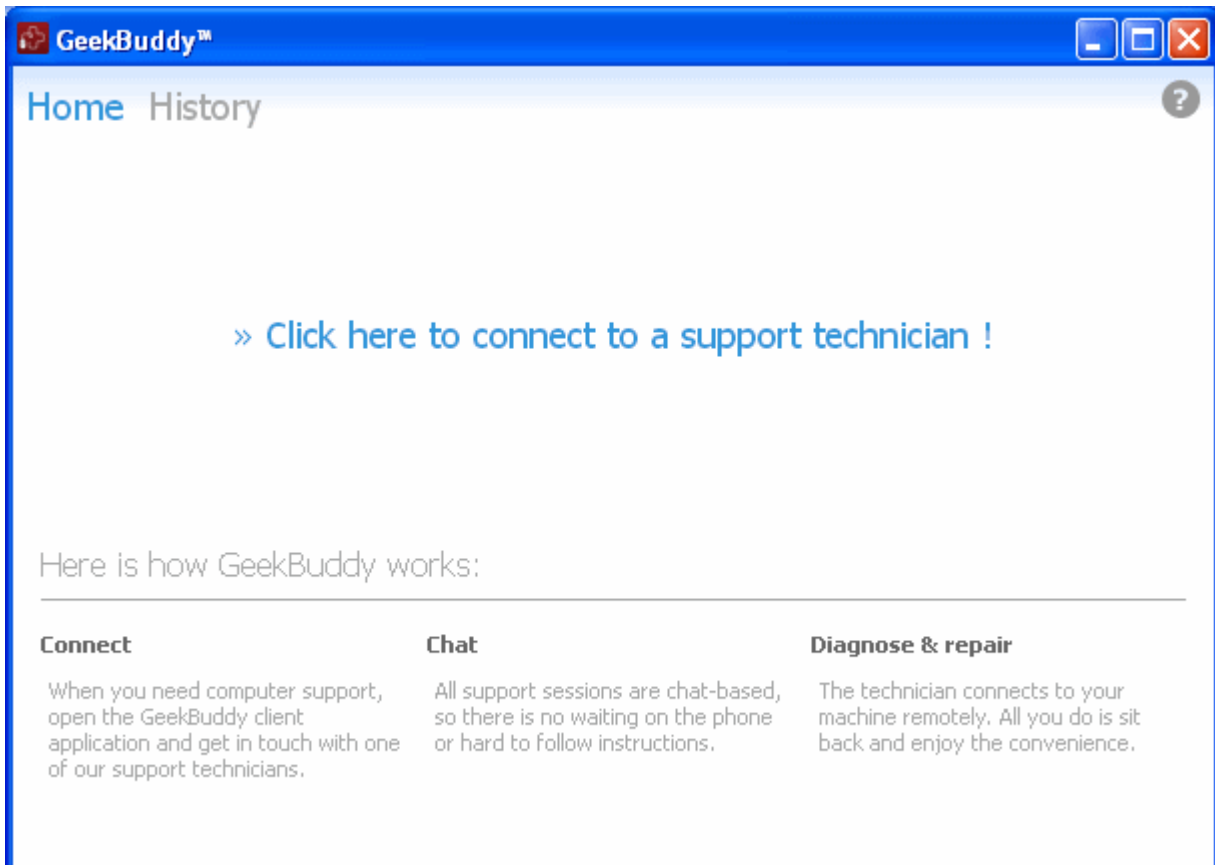


- Click the 'Activate' button.

The license key will be checked and if correct, the 'Activation successful' screen will be displayed.



- Enter the name and email details in the respective fields.
- Click 'Continue'.



The home page of GeekBuddy will be displayed. This screen displays a brief information about how the application works. Now you can start using it and seek the help of an expert to resolve your computer problems.



After activation, you can use both GeekBuddy and AntiError. Click the following links for more details on how to start and using them:

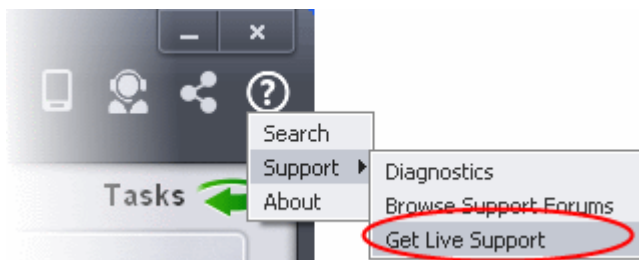
- [Launching the Client and Using the Service](#)
- [Starting and Using AntiError](#)

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 .

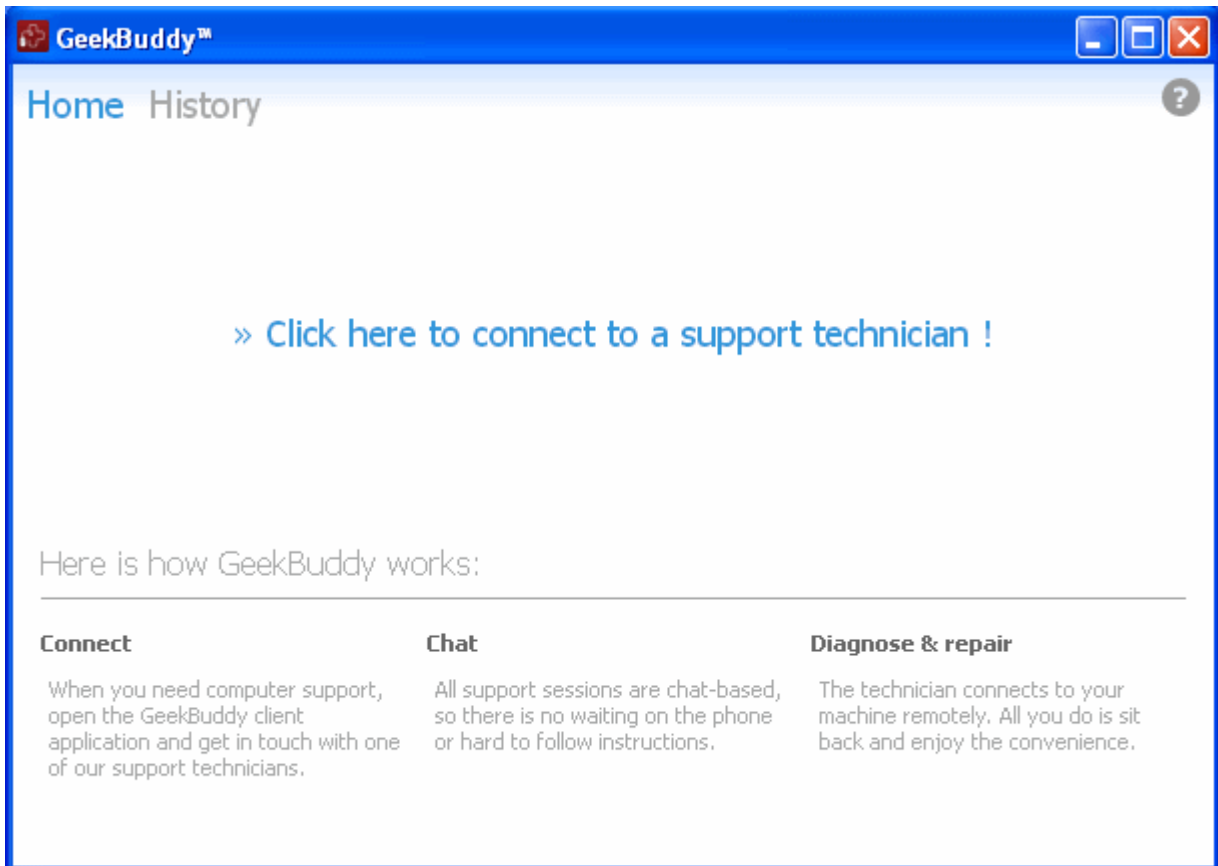
You can start the client and start a live chat session with a GeekBuddy expert using any one of the following methods:

- Double click the GeekBuddy desktop icon 
- Launch a chat with a qualified computer support technician by clicking this  icon in the title bar controls at the top right side of the main interface.
- 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.



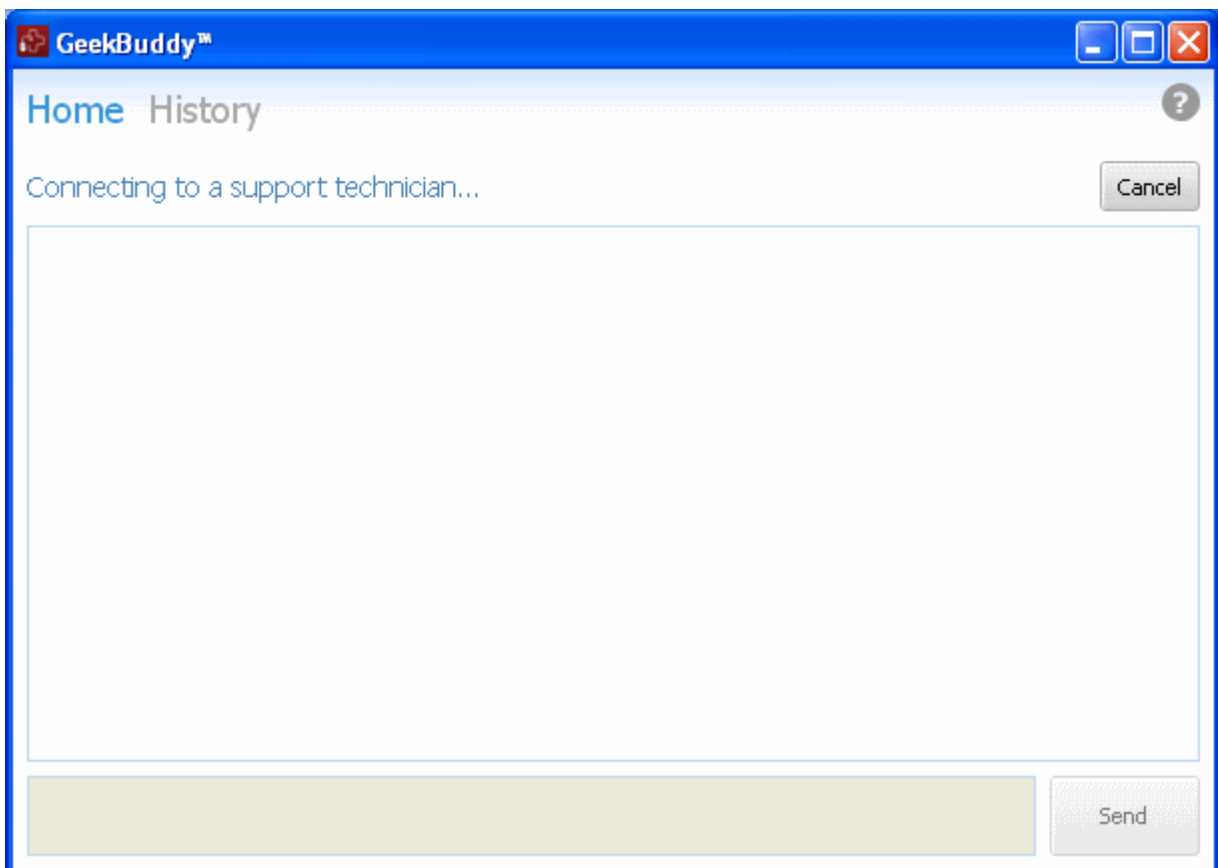
- Launch the GeekBuddy client directly from the Windows Start Menu - Click Start > All Programs > Comodo > GeekBuddy > GeekBuddy.

The 'Click here to connect to a support technician!' dialog will open.

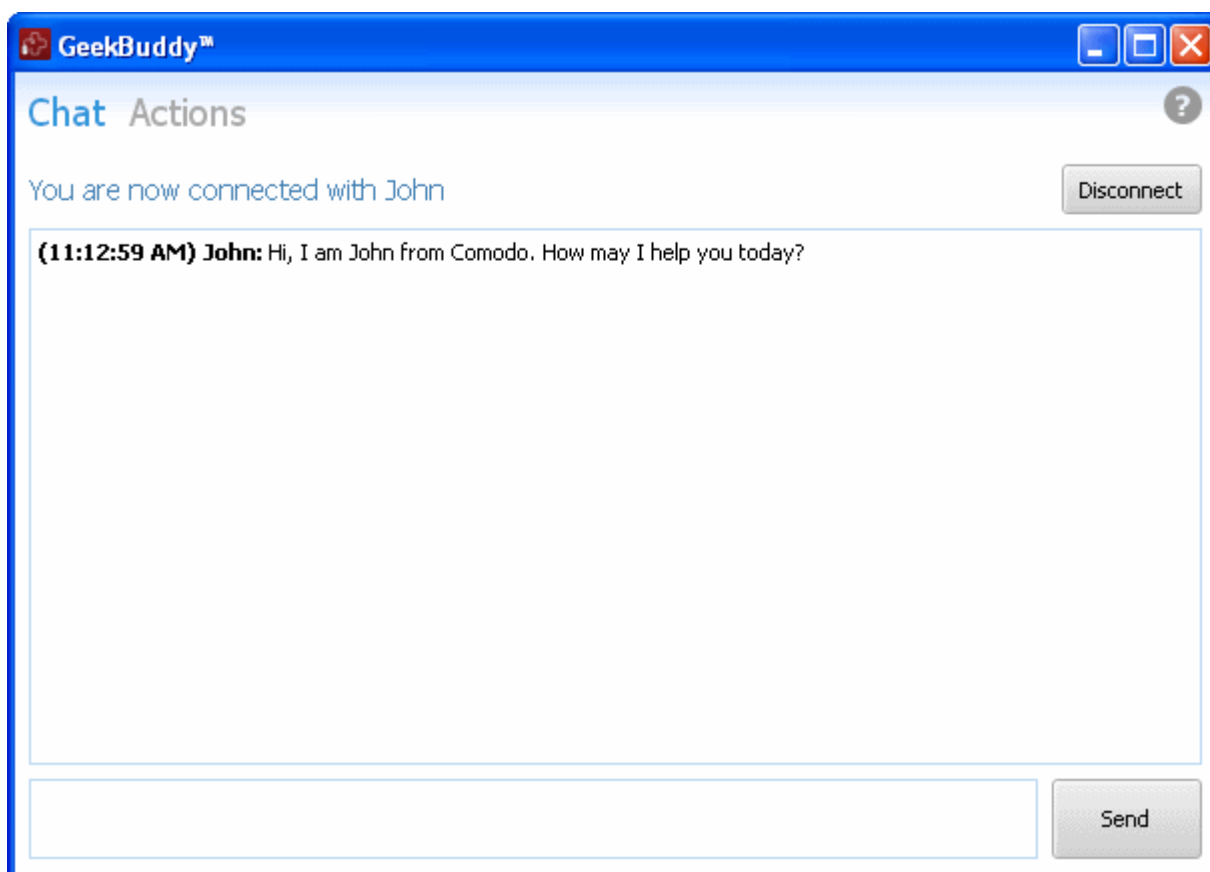


The screen displays a brief information about how GeekBuddy works in the Home screen.

- To contact a support technician, click the link 'Click here to connect to a support technician!' You will be connected to a GeekBuddy...




...and once the connection is established, our support technician will initiate a chat with you.

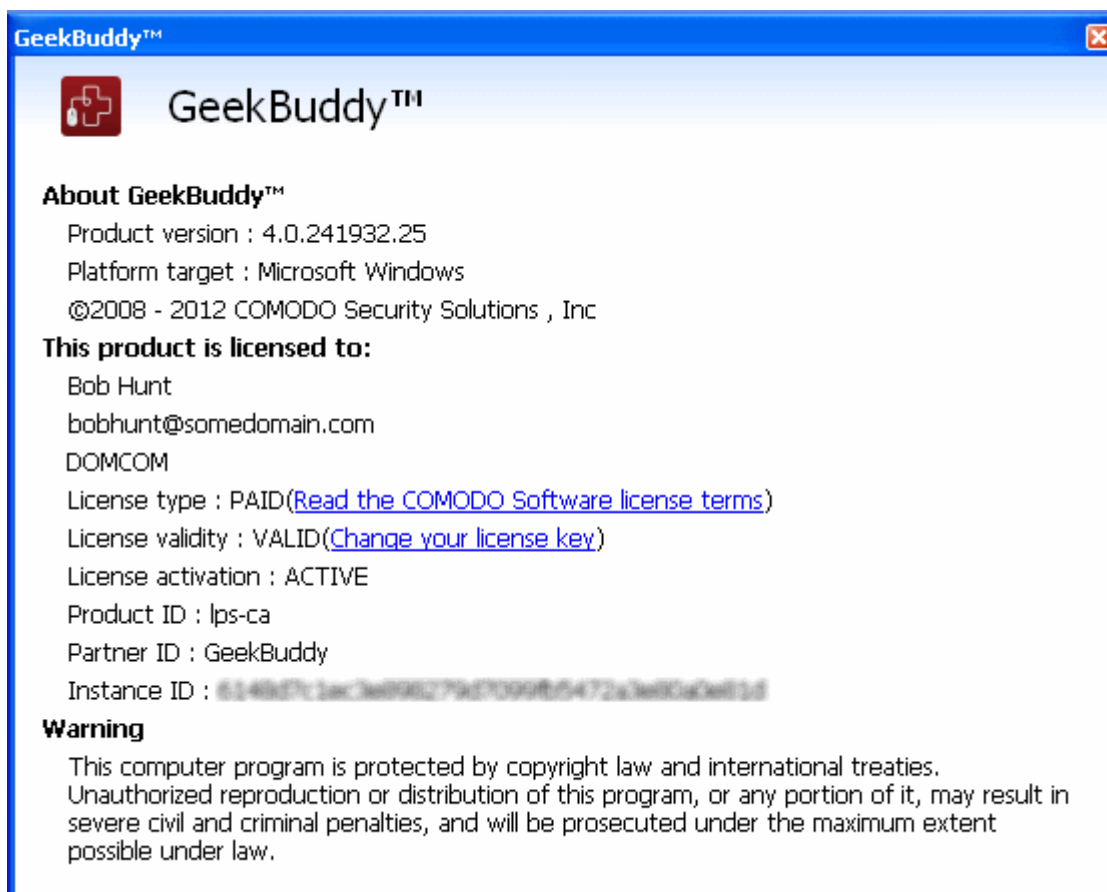


- Proceed to chat now.
- Explain your problem. The technician will assess your problem with you and work with you to fix any issues.

About GeekBuddy

- Click the  icon at the top right side of the interface.

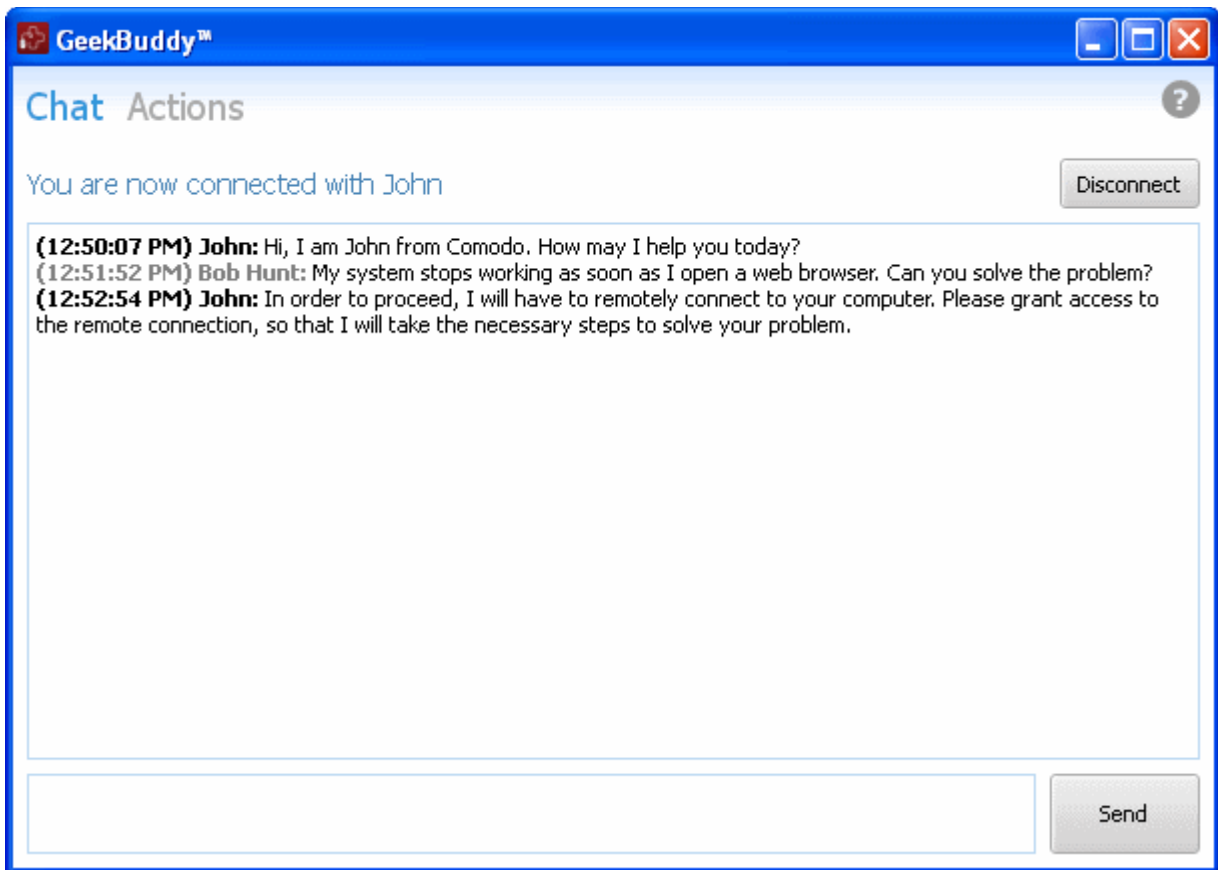
The About GeekBuddy information screen will be displayed.



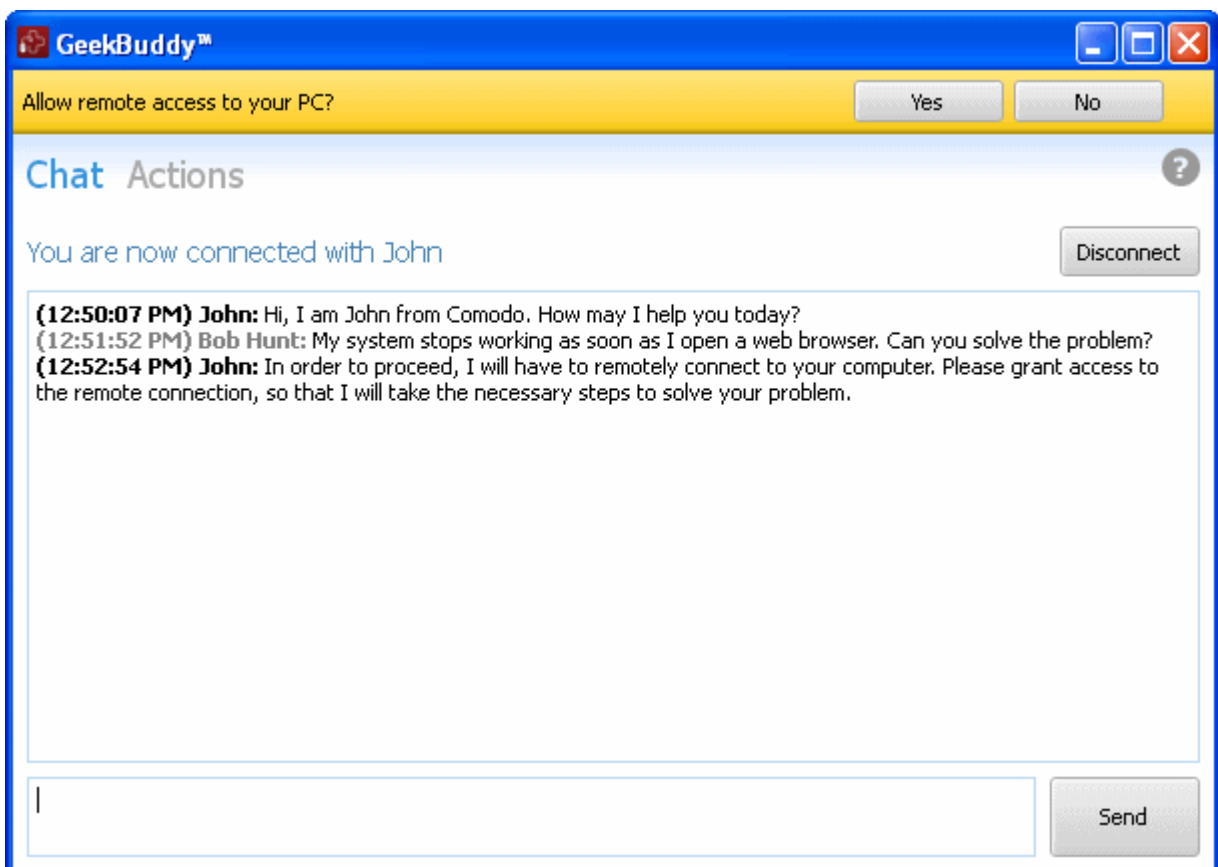
The 'About' dialog displays the copyright and product version information. The screen also displays information about the licensee and its validity.

7.4. Accepting Remote Desktop Requests

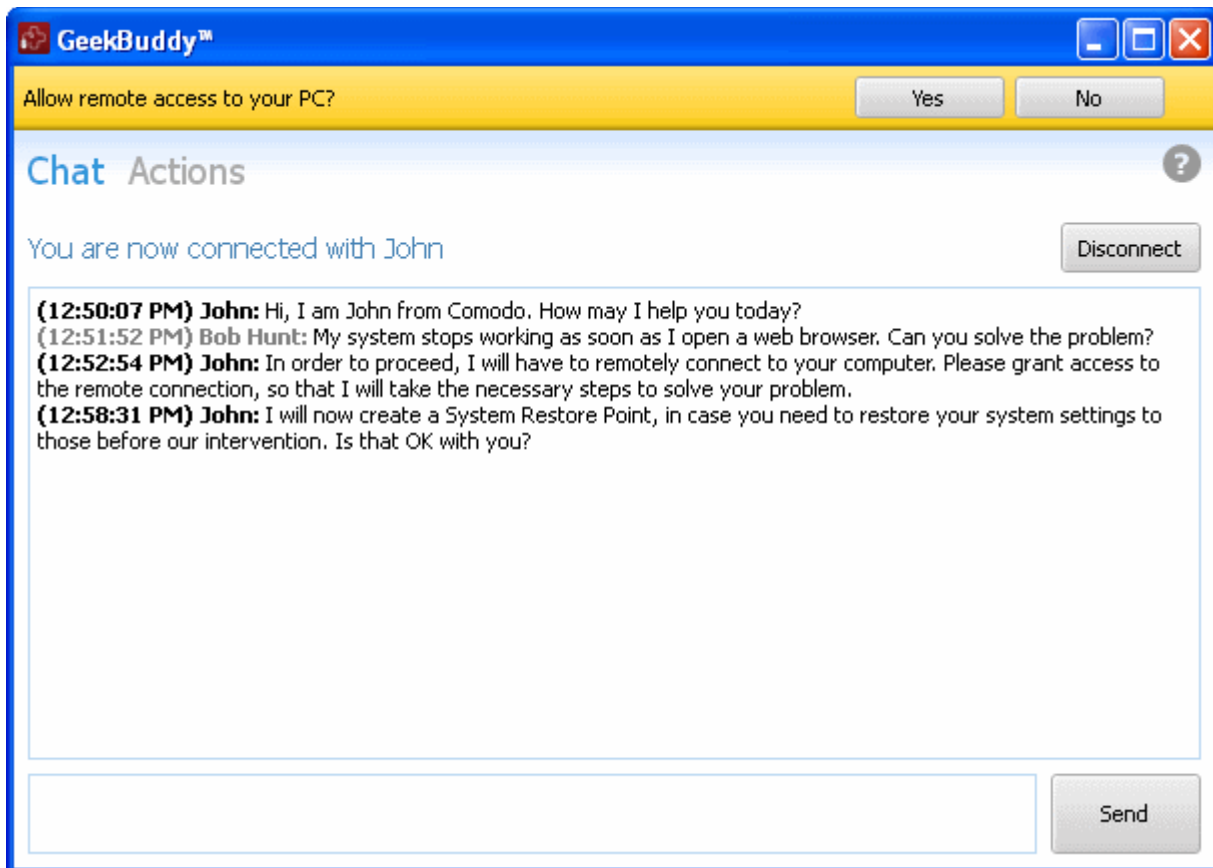
In order to solve certain problems, the support technician may need to observe and directly input data into your computer via a remote connection. Remote control can only go ahead if you grant permission for this to happen. Our technicians will always request your permission via the chat window.



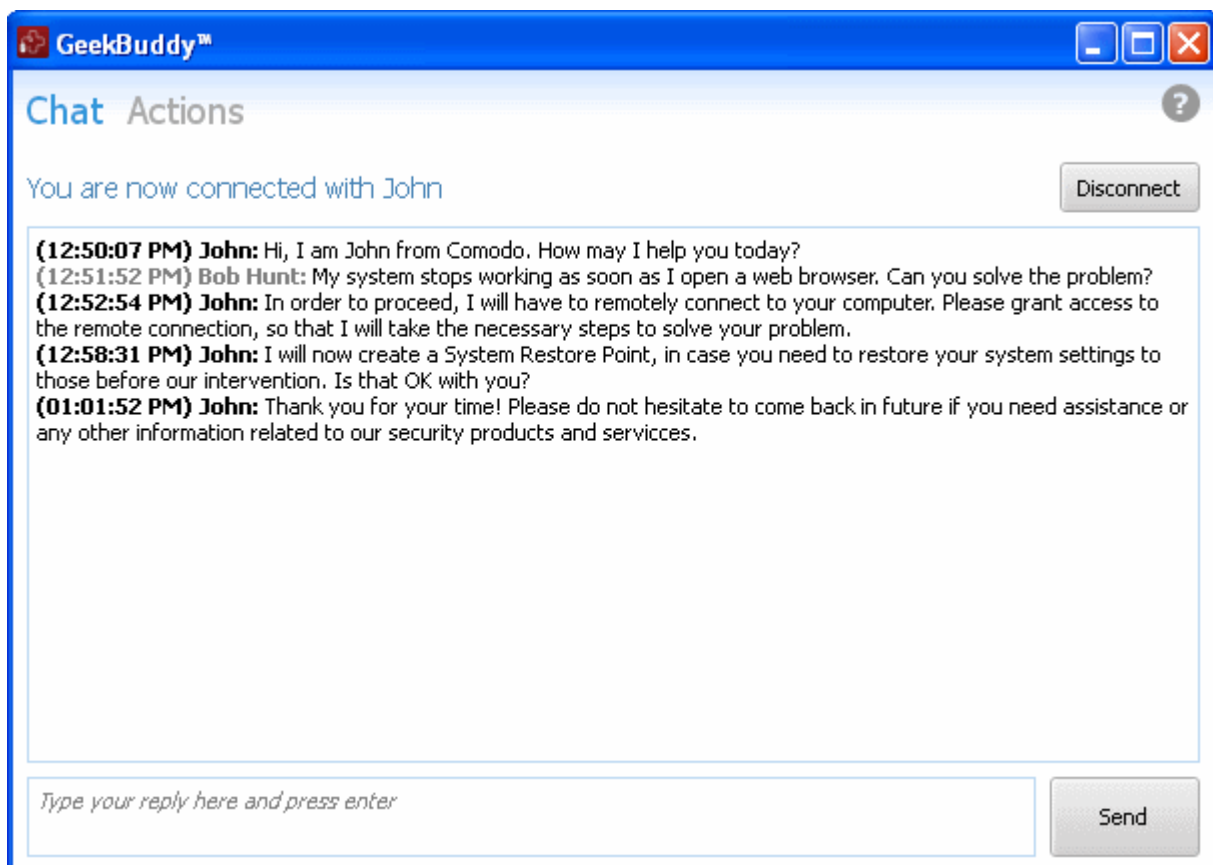
The technician may also ask your permission to make other changes to your machine. Such changes might include installing programs, creating system restore points or deleting unnecessary or infected files.



Click the "Yes" button at the top of the interface in order to allow the technician to connect to your computer.



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.



- Click the 'Disconnect' button 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.

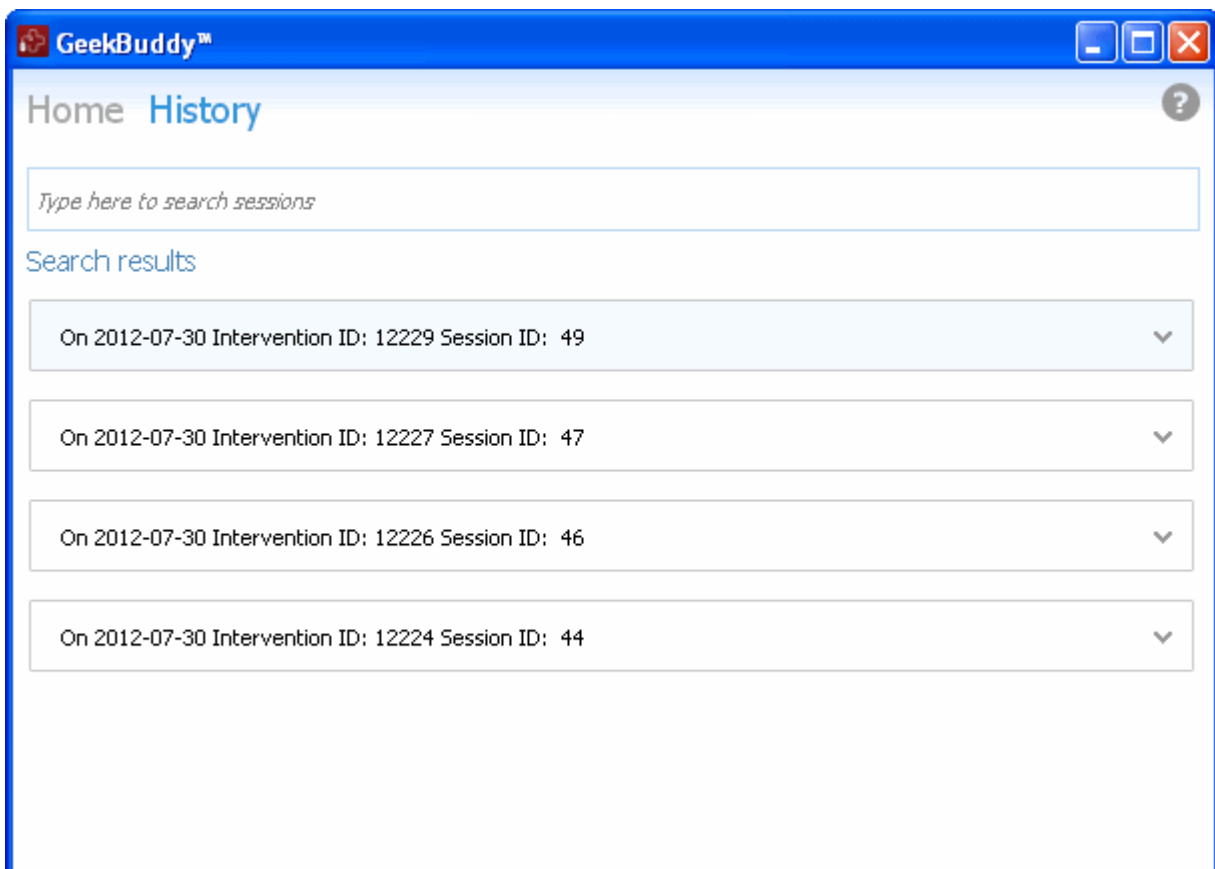
7.5.Chat History

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.

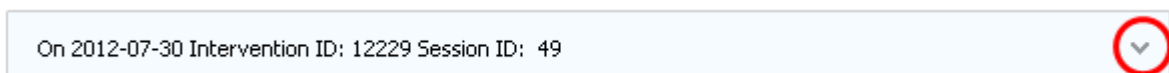
To view history of chat sessions

- Click the 'History' link at the top of the interface.

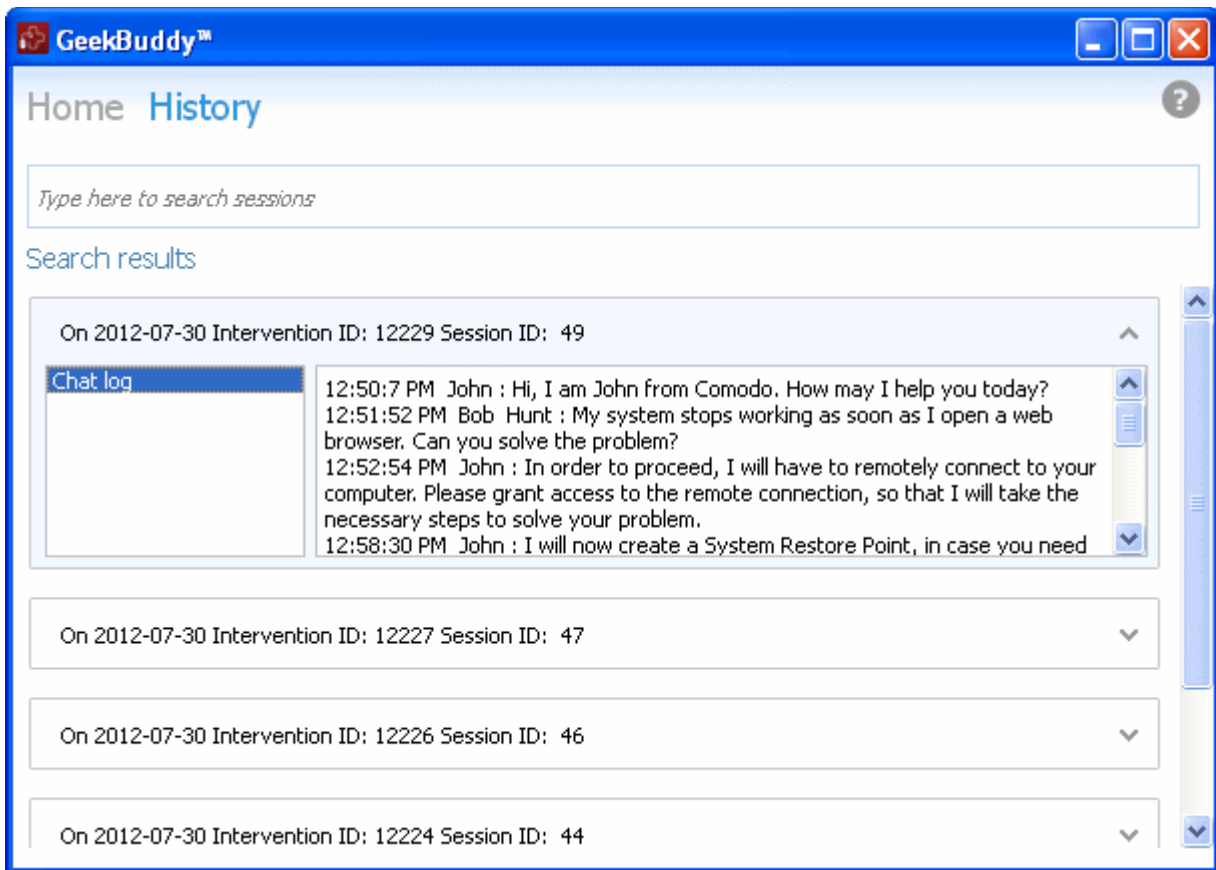
All the sessions will be displayed.



- 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.



- Click on the text 'Chat log' on the left side and 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. Starting and Using AntiError

The AntiError utility helps maintain the security and operational efficiency of your computer by automatically identifying common problems and helping you to fix them. For example, AntiError 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 AntiError, you will be offered the opportunity to contact a GeekBuddy representative who will help resolve the issues.

There are three ways to start AntiError:

- **Desktop Icon**
- **Start Menu**
- **Popup Alert**

Desktop Shortcut Icon



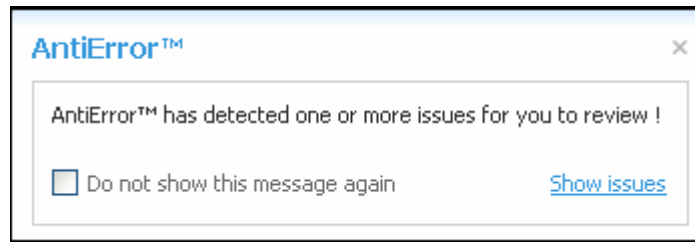
- Double click the shortcut icon  in the desktop.

Start Menu

- Click **Start > All Programs > Comodo > GeekBuddy > AntiError**

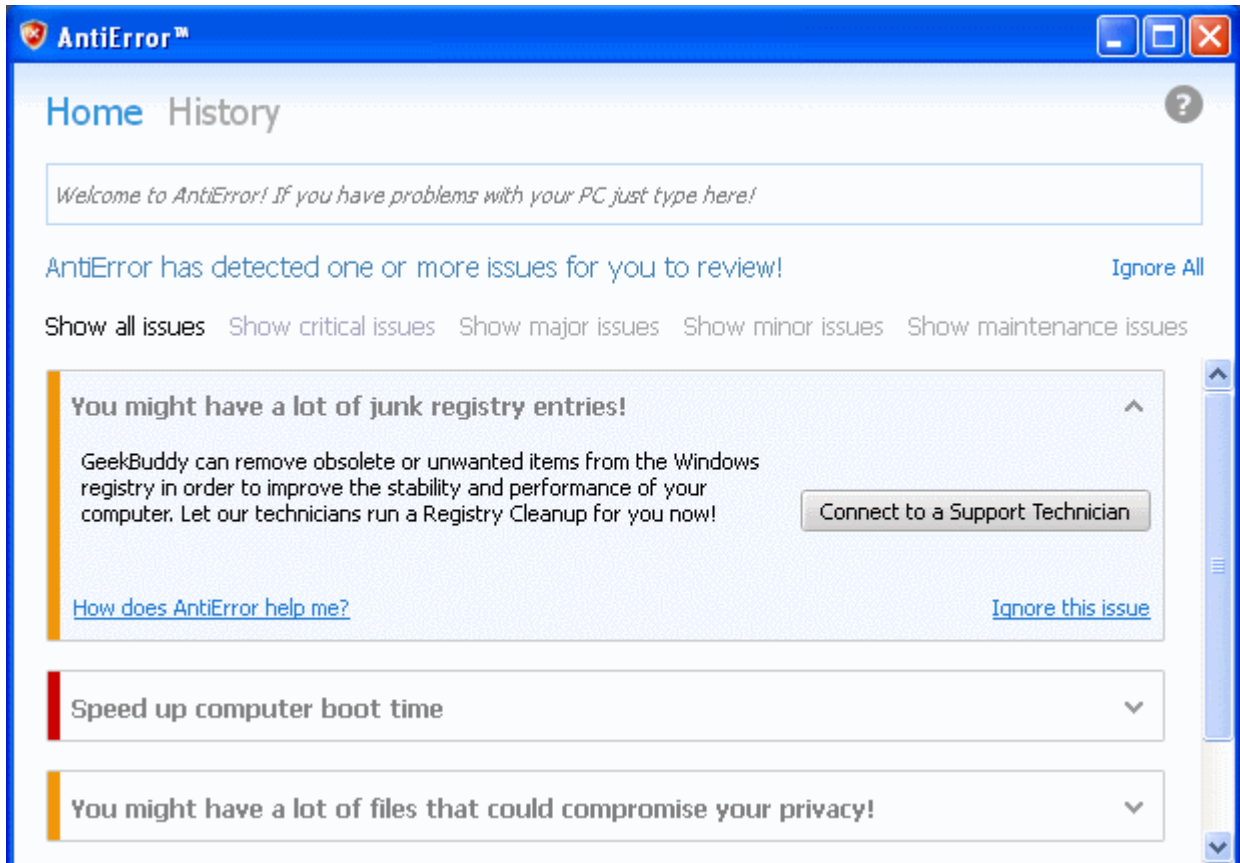
Popup Alert

At the time of starting your computer, AntiError will detect problems in your system and provide an alert at the bottom right side of the screen.



- Click the Show issues to open the AntiError interface.

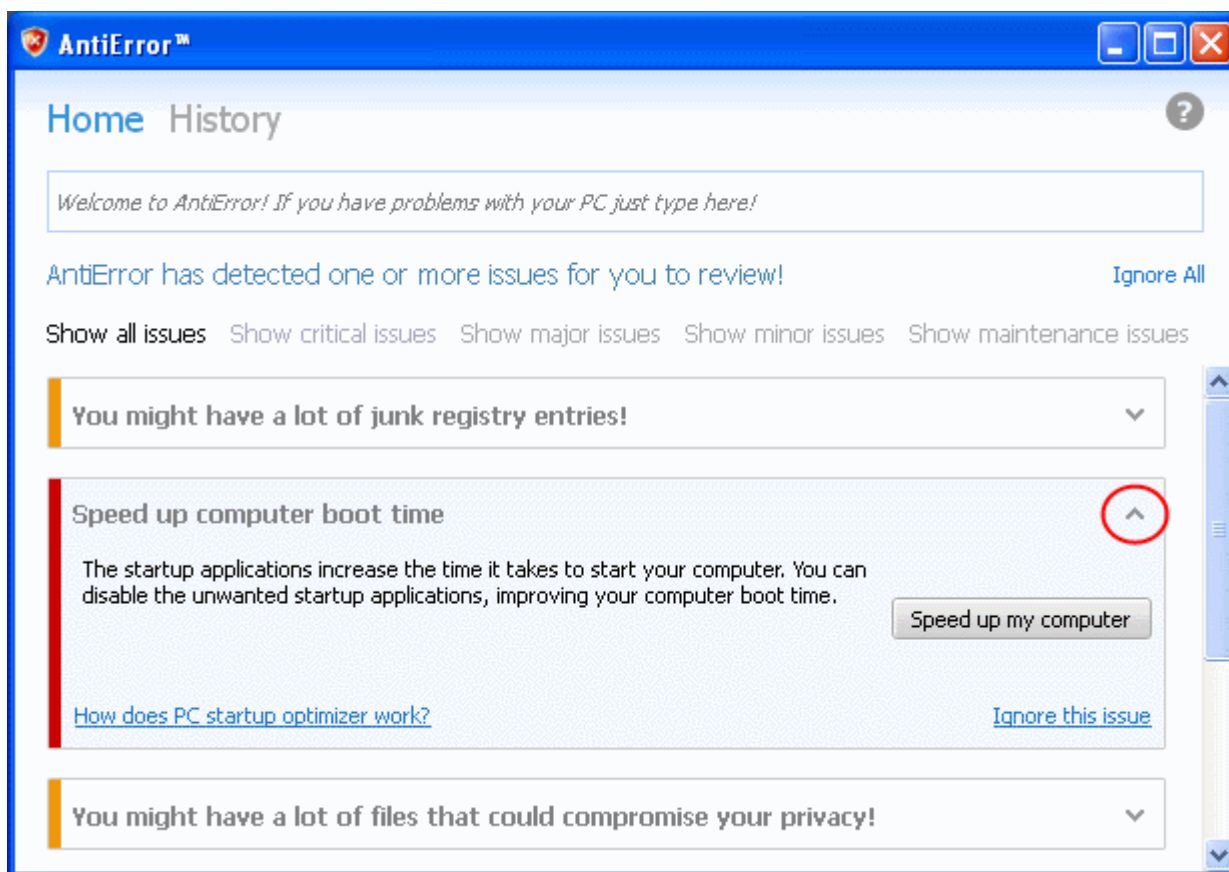
The AntiError interface will list the problems that it has detected.



The problems detected will be categorized as critical, major, minor and maintenance issues. Click on the relevant link to view the problem. Clicking the 'Show all issues' link 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

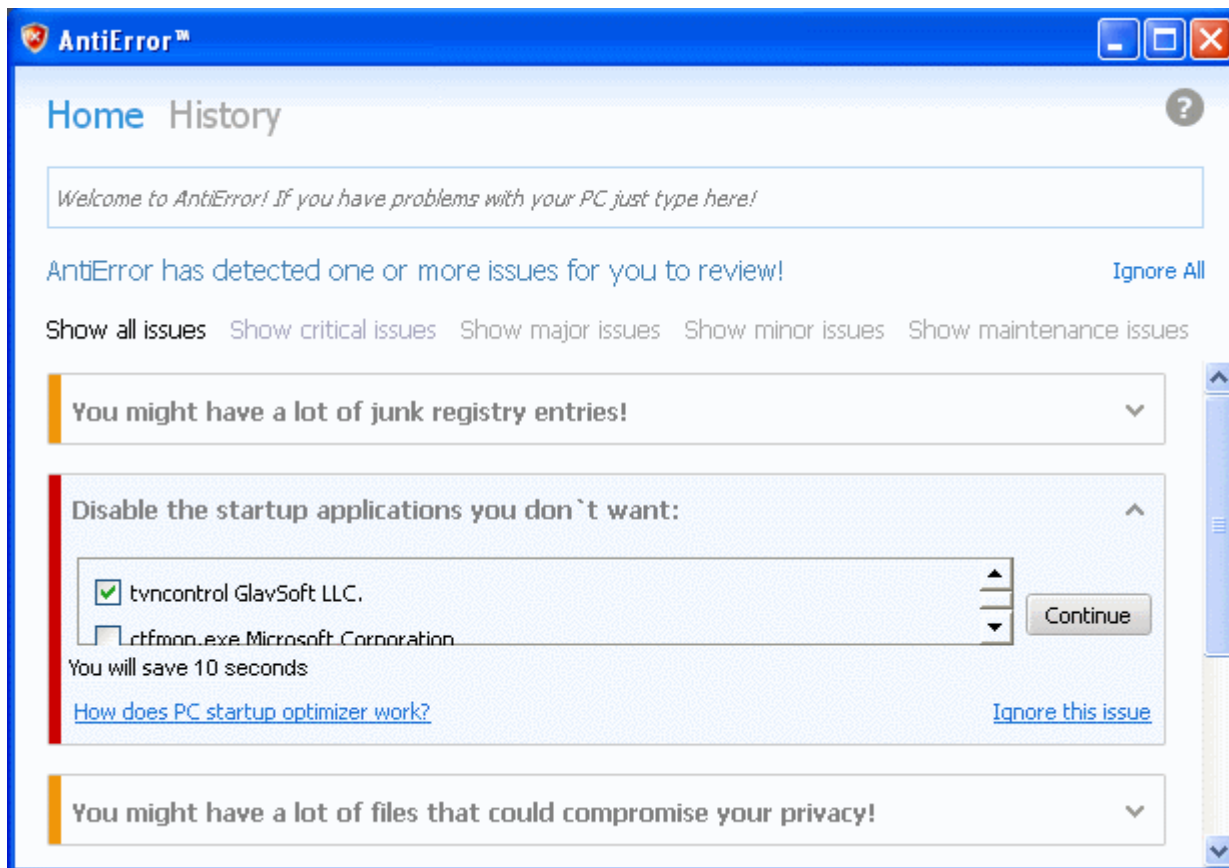
Click on the arrow beside the issue or double click anywhere on the entry to view its details.



Some of the common problems that occurs in any computer are junk registry entries, slow bootup time and presence of files that might compromise your privacy.

Each of the entry will provide a solution for the issue. For example, for the issue of slow bootup time, 'Speed up my computer' button will be displayed.

Clicking this button will display a list of startup programs in your system.

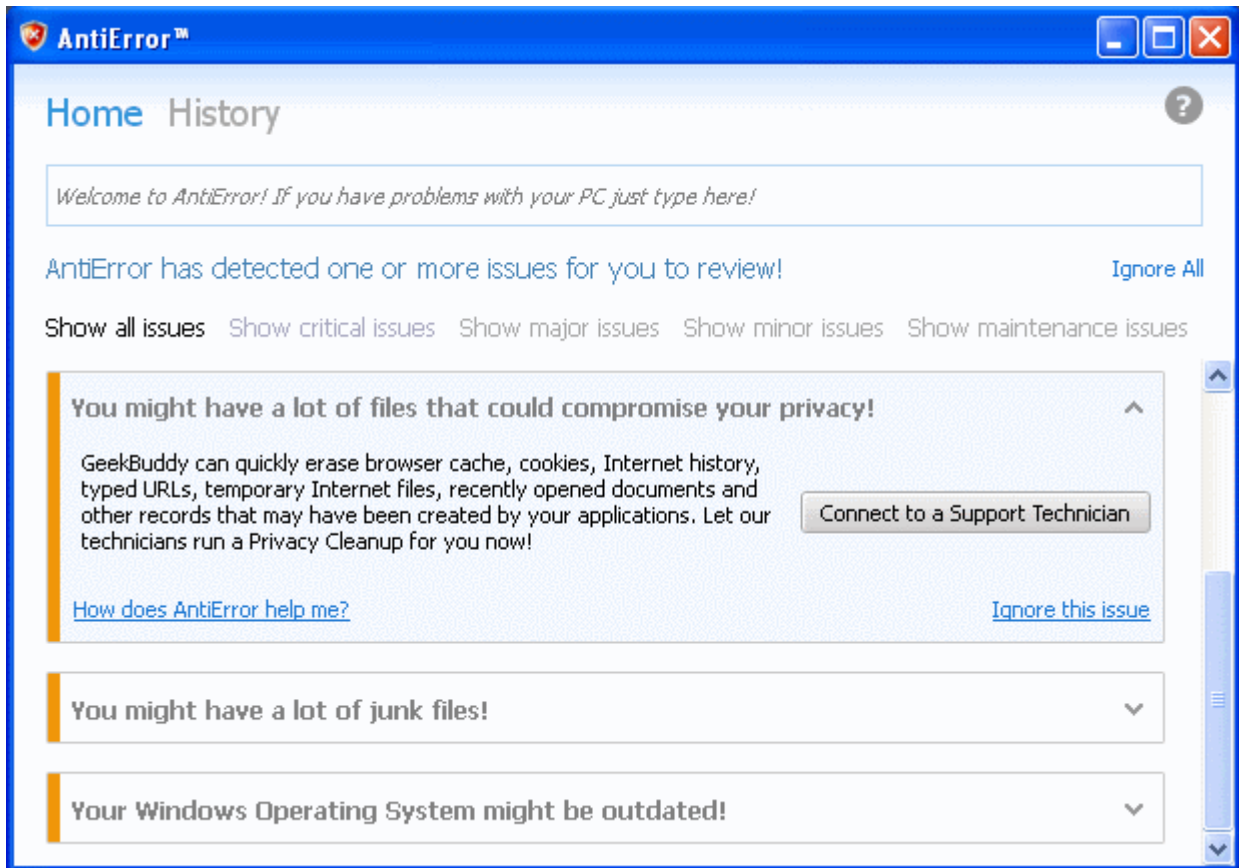


These programs are automatically loaded into the system during Windows start-up and running at the background. You can identify the programs which you do not want to be loaded automatically during system start-up and disable them from this interface. Blocking unwanted programs from running in the background saves system resources and improves the performance of the system. You can view the total time saved below the list for the programs you've selected to be disabled.

- Click 'Continue'.

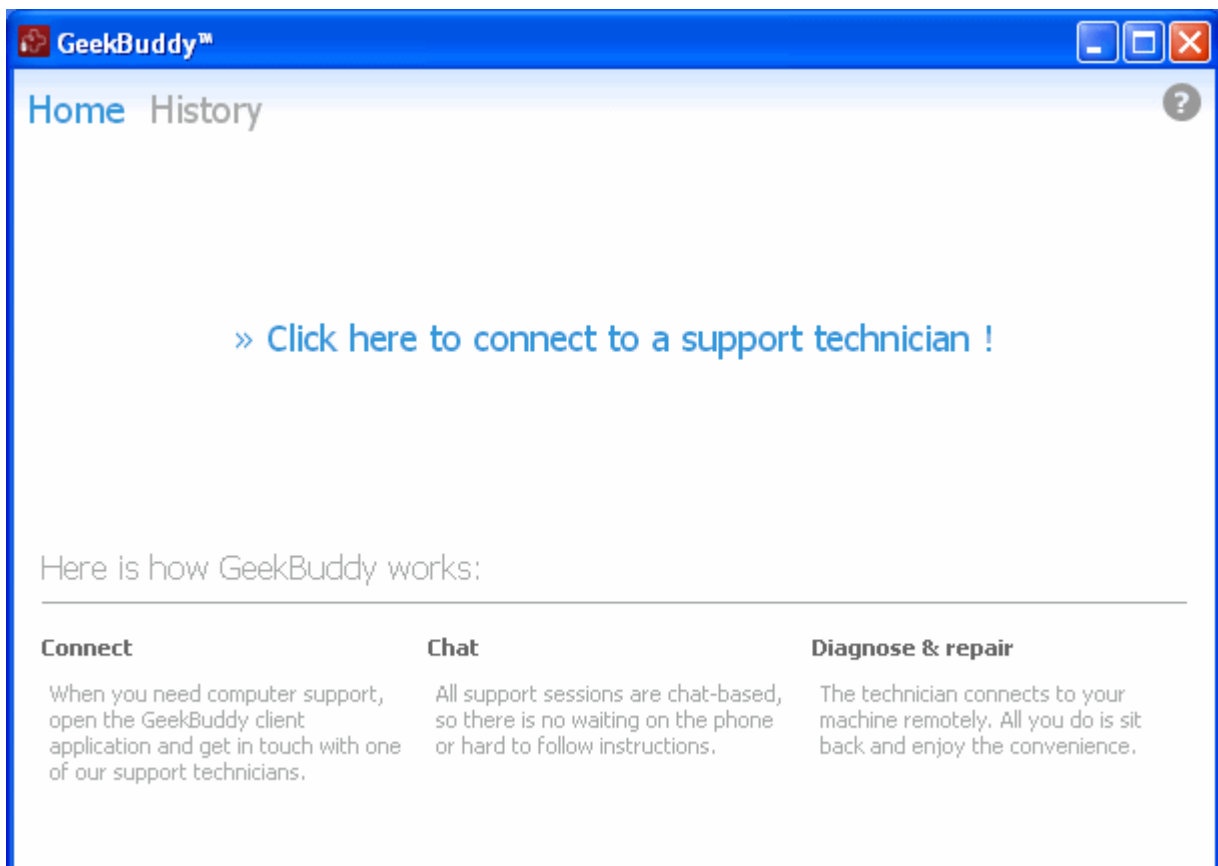
The selected programs will be disabled from running in the background.

For some of the issues listed, you have to seek the help of an expert technician.



- Click the 'Connect to a Support Technician' button.

The GeekBuddy interface will be displayed.



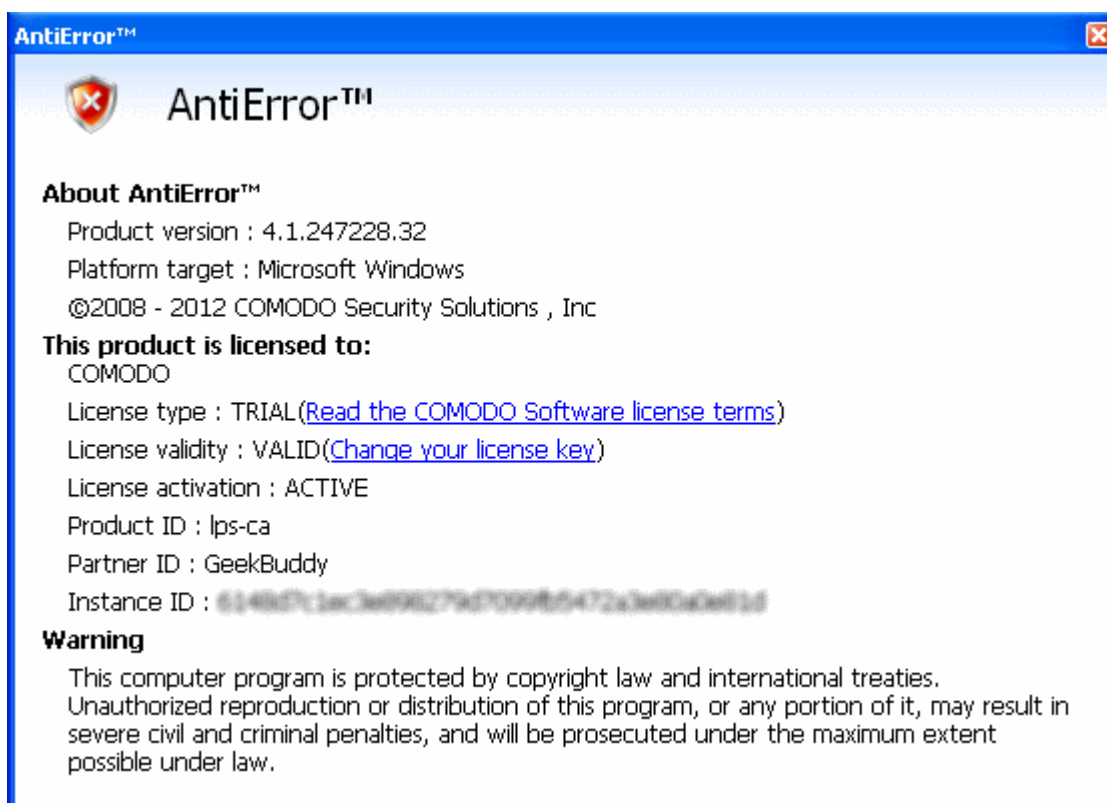
A support technician will chat with you after clicking the 'Click here to connect to a support technician!' link. [Click here](#) for more details.

- Click 'Ignore All' link to disregard all the issues in your system displayed by AntiError.
- 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.

About AntiError

- Click the  icon at the top right side of the interface.

The About AntiError information screen will be displayed.

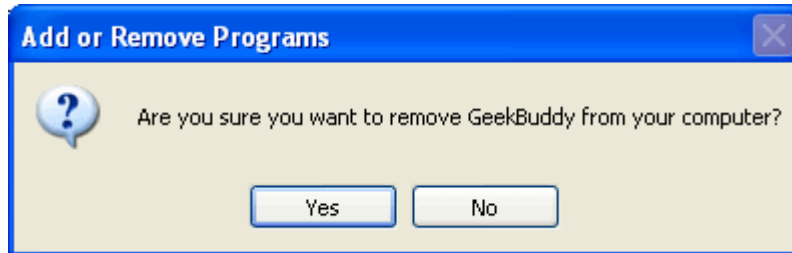


The 'About' dialog displays the copyright and product version information. The screen also displays information about the licensee and its validity.

7.7. Uninstalling Comodo GeekBuddy

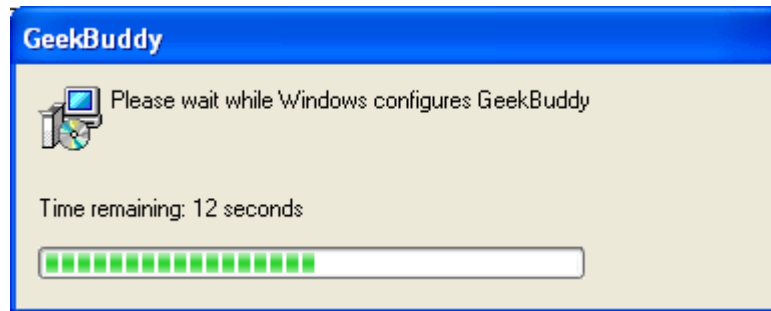
To uninstall Comodo GeekBuddy

- Click Start > Control Panel
- In the Control Panel, double-click Add/Remove Programs
- In the list of currently installed programs, click GeekBuddy
- Click the 'Change/Remove' button.



- Click 'Yes' to confirm uninstallation.

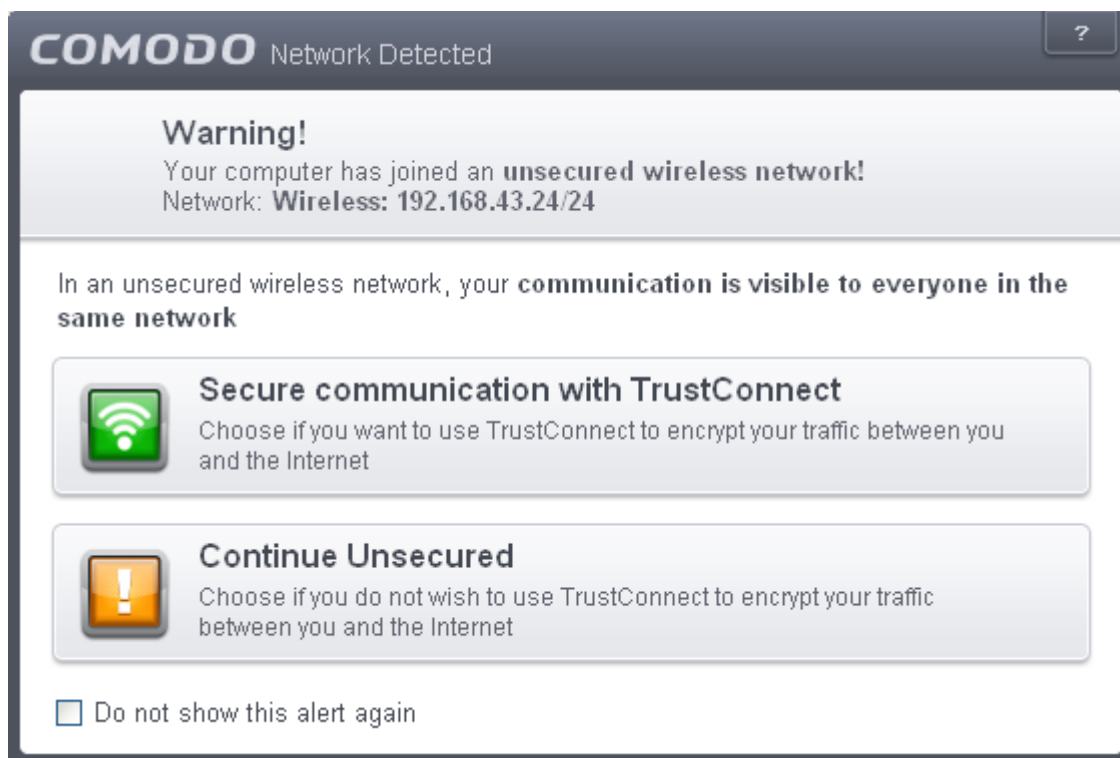
The progress of GeekBuddy removal will be displayed...



---and after a few minutes 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 Vista
- Windows XP
- Mac OS X
- Linux (containing kernel 2.4 or later)
- FreeBSD, OpenBSD

Setting up TrustConnect

- **Microsoft Windows**
- **MAC OS X**
- **Linux**
- **iPhone / iPod Touch**

- [Android Devices](#)
- [Windows Mobile Devices](#)

8.1. Microsoft Windows - Configuration and Connection

This section deals with the configuration and connection of TrustConnect and presumes you already have the software installed. If you have not yet installed the software then:

- Please run the CIS Complete installer and select 'Install TrustConnect' at the options menu
- Alternatively, the TrustConnect client can be downloaded separately from <http://www.comodo.com/trustconnect> or from the 'TrustConnect' area of your Comodo account at <http://accounts.comodo.com/login>
- Installation of TrustConnect is dealt with in Section [1.3.3.4 Installing TrustConnect](#) of this guide.

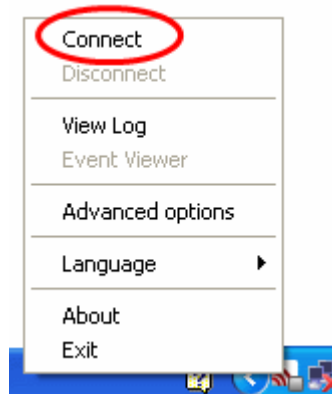
Establish a connection to TrustConnect

Once installation is complete, TrustConnect can be launched in one of the following ways:

- Via the Windows 'Start' menu. Click '**Start > Programs > Comodo > Trust Connect > ComodoTrust Connect**'



- By double clicking the TrustConnect Tray icon:
- By right clicking on the TrustConnect Tray icon and selecting 'Connect':



By default, your TrustConnect client automatically selects the best TrustConnect access server from the servers distributed all over the world depending on your location, distance between you and the servers and their load. You can change the server you want to connect to, through [Advanced Options](#) explained in this section.

After starting TrustConnect you should enter your TrustConnect Service Login and Service Password at the client login box.

Note: This is not the same password as your Comodo Account password. It is a unique, random password that was generated during account creation to authenticate you to the TrustConnect servers. If required, you can change this password to something more memorable by using the 'Change Service Password' button on the right.

COMODO
Creating Trust Online®

Welcome, John

Comodo Internet Security | TrustConnect | My Account | Help | Contacts

Comodo TrustConnect

Service Login jsmith
Service Password 1aB2cdeeFG

License key e11b3e35-937d-47af-957d-a2207a4c75b2

Date from 2010-08-16 06:40:09

Date to 2011-08-16 06:40:09

Traffic

Limit: 10 GB

Available: 10 GB

Today

No data found.

This month

[Change Service Password](#)
[Change plan](#)

[First Time User Instructions](#)
[html / pdf](#)

Comodo TrustConnect - User Authentication

Username:

Password:

Remember

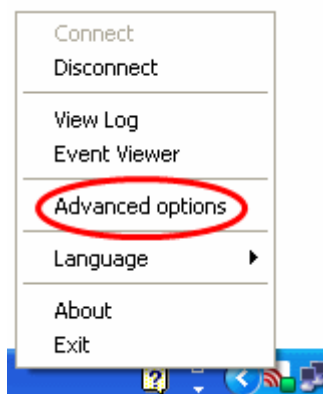
Click 'OK' to confirm and connect. After successful authentication of your user-name and password, the tray icon turns green to indicate that you are successfully connected to TrustConnect:



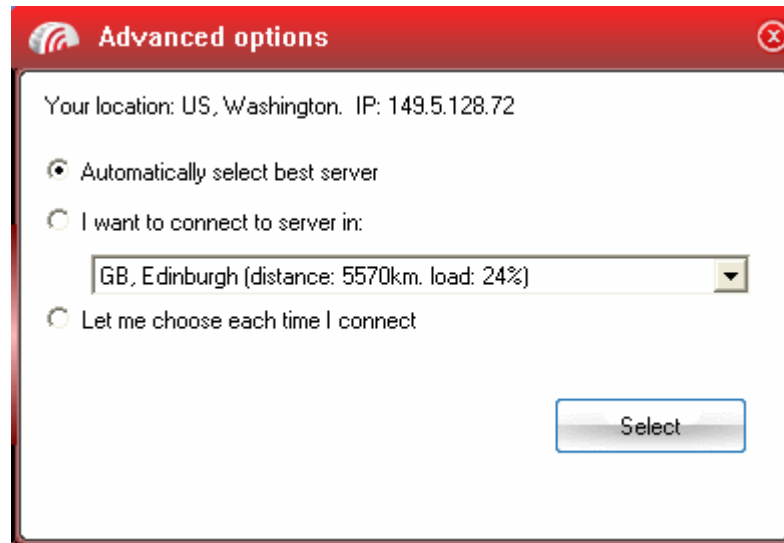
Advanced Options

Comodo TrustConnect allows you to select the TrustConnect access server you want to connect to, through its advanced options. You can set TrustConnect to automatically select the best server, set a default server or choose to select the server manually every time.

To access the Advanced options panel, right click on the TrustConnect Tray icon and select 'Advanced Options'.



The panel displays your current location with the IP address.



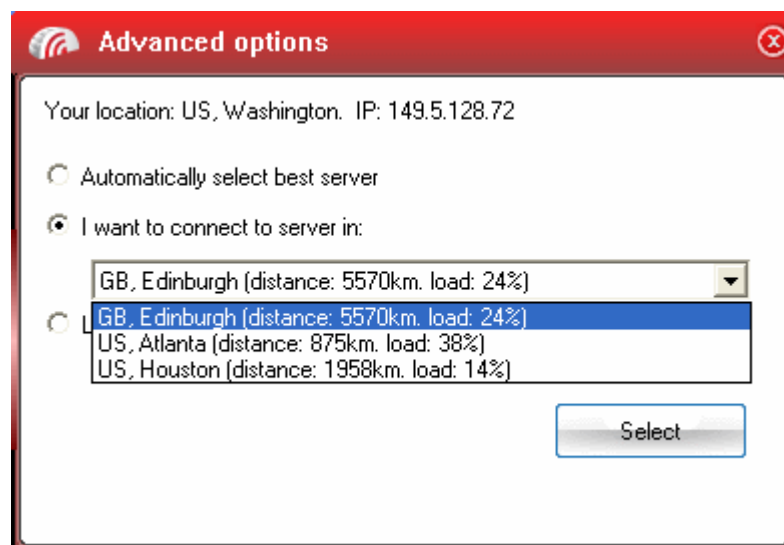
You can configure the server selection from the options :

- **Automatically select the best server;**
- **I want to connect to server in;**
- **Let me choose each time I connect.**

Select the option and click the Select button for your settings to take effect.

Automatically select the best server - Instructs TrustConnect to select the best access server with optimal load and distance to connect to. Your TrustConnect client automatically finds a server nearest to your location and with optimal connection load. This is the default option and is recommended for all users.

I want to connect to server in: Allows you to choose a server and to set it as default, so that every time you start TrustConnect service, you are connected to the selected server irrespective of your location. The drop-down box displays a list of TrustConnect access servers located at different places, all over the world. Each server is indicated with its location (country, state), distance from your current location and the load of the server in percentage.



- Select the server which you want to set as default and click the 'Select' button.

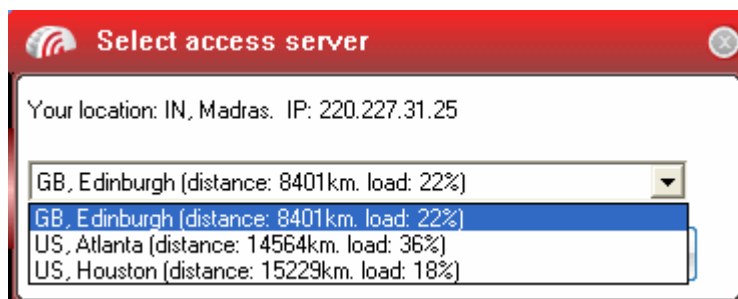
Note: It is always recommended to choose a server nearest to your location for quicker access.

A connection to the selected server is established every time you establish a connection to TrustConnect. You can change this

setting anytime you want, by accessing the Advanced Options in TrustConnect.

Let me choose each time I connect - Allows you to select a different server each time you establishing a connection with TrustConnect.

Every time you start TrustConnect service, you are prompted to select the server which you wish to connect. On establishing a connection to TrustConnect, a 'Select access server' dialog appears.



The drop-down box displays a list of TrustConnect access servers located at different places, all over the world. Each server is indicated with its location (country, state), distance from your current location and the load of the server in percentage.

- Select the server to which you want to connect and click the 'Select' button. A connection with the selected access server is established.

Note: It is always recommended to choose a server nearest to your location for quicker access.

8.2. Mac OS X - Configuration and Connection

Install and configure TrustConnect OpenVPN client

1. Download the TrustConnect OpenVPN client for Mac OS X 10.4 (or above) from the Tunnelblick project site - <http://code.google.com/p/tunnelblick>. The client can be download from the 'Featured downloads' section on the right hand side of the homepage.

Alternatively, it can be downloaded directly by clicking the following link:

http://tunnelblick.googlecode.com/files/Tunnelblick_3.0b26.dmg

2. Install the client. Double click the .dmg file you downloaded in the step above to start the installation process. Once setup is complete, a 'Tunnelblick' icon should appear on your desktop. More details about the Tunnelblick application and its usage is available at the project website located at <http://code.google.com/p/tunnelblick>.
3. Download the correct client configuration file for your TrustConnect package:
 - TrustConnect subscribers download:
<https://accounts.comodo.com/download/trustconnect/client.conf>
4. Rename the file you just downloaded from either 'client.conf' or 'free_client.conf' to 'openvpn.conf'
5. Download the TrustConnect **CA certificate**.
6. Copy the renamed **configuration file** and the root **CA certificate** into the following directory:
`~/Library/Application/Support/Tunnelblick/Configurations`
7. Start **Tunnelblick.app** and choose **Connect 'openvpn'**.
8. Enter your TrustConnect login and password.

8.3. Linux / Open VPN - Configuration and Connection

The following options are available for Linux users:

- [Download and Install the OpenVPN Client](#)
- [Download and Install the RedHat Client](#)

- [Download and Install the Ubuntu Client](#)

Download and Install the TrustConnect OpenVPN Client

To connect to the TrustConnect service you must first download and install the TrustConnect OpenVPN client software.

1. Download the TrustConnect OpenVPN client for Linux. Click [here](#) to download the client directly.
2. Using the RPM package

If you are using a Linux distribution which supports **RPM packages** (SuSE, Fedora, Redhat, etc.), it's best to install using this mechanism. You can **build** your own binary RPM file:

```
rpmbuild -tb openvpn-[version].tar.gz
```

Once you have the RPM file, you can **install** it with:

```
rpm -ivh openvpn-[details].rpm
```

Installing OpenVPN from a binary RPM package has these **dependencies**: openssl, lzo, pam. LZO library can be downloaded [here](#).

3. Without the RPM package

If you are using Debian, Gentoo, or a non RPM based Linux distribution, use your distribution specific packaging mechanism such as 'apt-get' on Debian or 'emerge' on Gentoo. It is also possible to install OpenVPN on Linux using the universal **./configure** method.

First expand the **.tar.gz** file:

```
tar -xzf openvpn-[version].tar.gz
```

Then **cd** to the top level directory and type:

```
./configure
make
make install
```

For more details, visit the official [OpenVPN 2.0 'How To' page](#)

Configuring TrustConnect OpenVPN Client

1. Download the correct client configuration file for your TrustConnect package:
 - TrustConnect subscribers download: <https://accounts.comodo.com/download/trustconnect/client.conf>
2. Download the TrustConnect **CA certificate**.
3. Copy root **CA certificate** and **configuration file** into OpenVPN configuration directory, for example into **/etc/openvpn/**.
4. Start TrustConnect OpenVPN client program:


```
openvpn--openvpn config /etc/openvpn/client.conf
```
5. Enter your TrustConnect **login** and **password**.

Download and Install the TrustConnect RedHat Client

To install TrustConnect client for RedHat (Fedora, RHEL) system

1. Download RPM package here:

<https://accounts.comodo.com/download/trustconnect/tcclient-1.0-1.noarch.rpm>

2. Start console, login as root and execute command:

```
# rpm -Uvh PATH/TO/RPM/tcclient-1.0-1.noarch.rpm
```

Client was tested on the RedHat Fedora 8, 9, 10

Download and Install the TrustConnect Ubuntu Client

To install TrustConnect client for Ubuntu system

1. Download DEB package here:

https://accounts.comodo.com/download/trustconnect/tcclient_1.0-1_all.deb

2. Start console, login as root and execute command:

```
# dpkg -i PATH/TO/DEB/tcclient_1.0-1_all.deb
```

Client was tested on the Ubuntu 8.0, 8.1

Usage:

Run trustconnect client: "Applications Menu" -> "Internet" -> "TrustConnect Client"

8.4. Apple iPhone / iPod Touch - Configuration and Connection

Open VPN account information page. Go to **Setting > General > Network > VPN > Settings**.

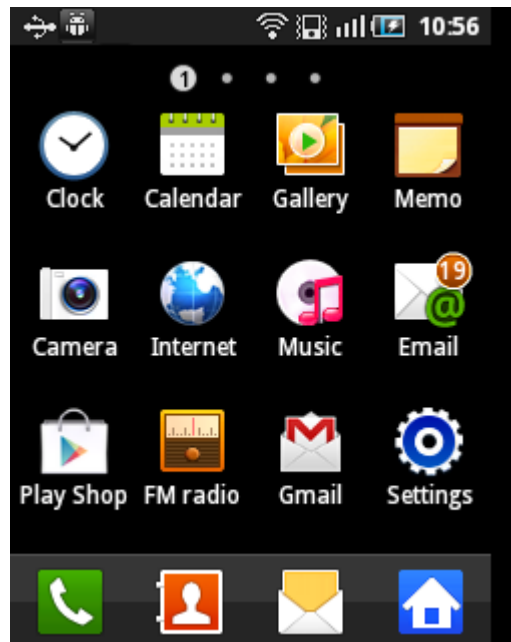
1. Select PPTP and enter TrustConnect VPN account information:
 - In the 'Server' field, please use one of the following addresses:
 - us1.vpn.comodo.com (commercial subscription)
 - us2.vpn.comodo.com (commercial subscription)
 - us3.vpn.comodo.com (free subscription users only)
2. Enter your TrustConnect account and password.



3. Click the 'Save' button and go back to VPN main page (**Setting > General > Network > VPN**).
4. Start Trust Connect VPN connection. Switch 'VPN' to 'ON'.

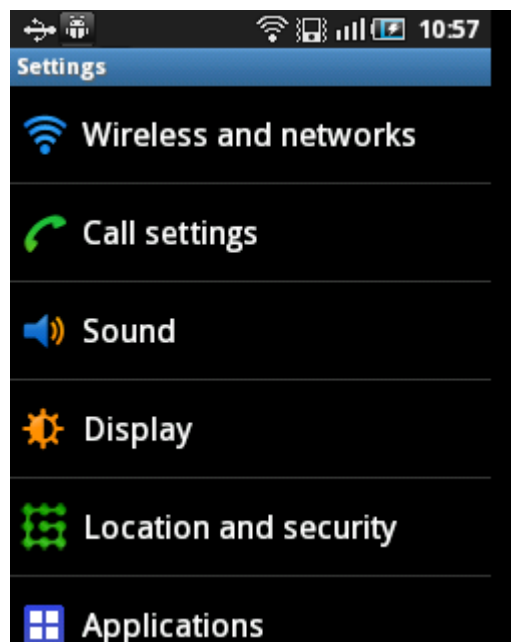
8.5. Android Devices - Configuration and Connection

1. Tap 'Menu' in the home screen of your Android device.



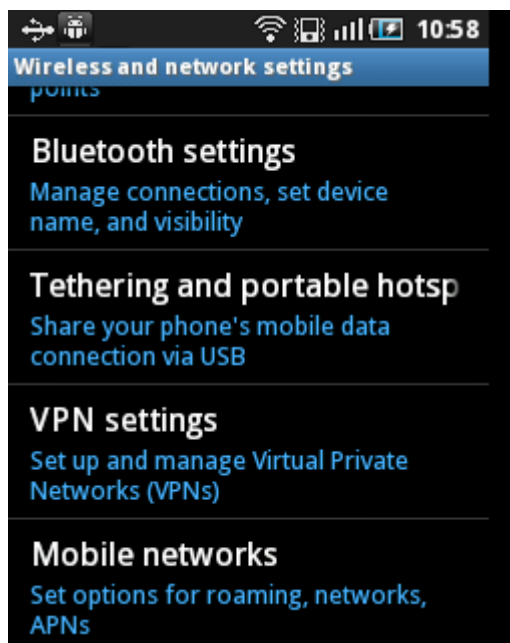
2. Tap 'Settings' in the menu screen.

The settings interface will be displayed. The settings menu screen might look different depending on the Android device you are using. However, the 'Wireless and networks' screen should be fairly common for most of the Android devices.

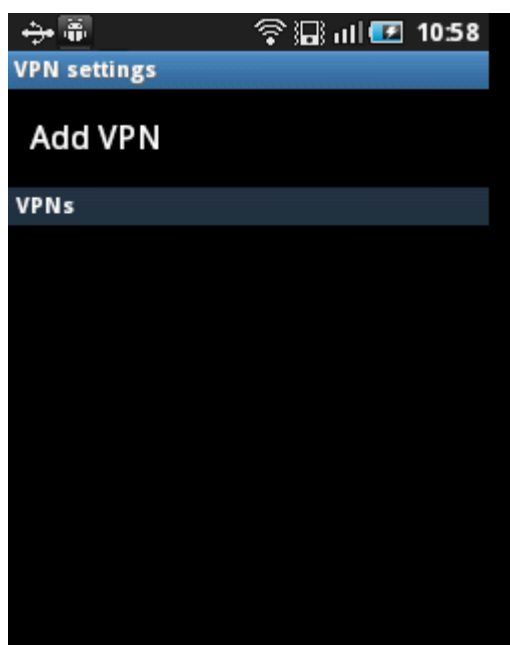


3. Tap 'Wireless and networks' in the Settings interface.

The 'Wireless and network settings' screen will be displayed.



4. Tap 'VPN settings' in the screen.
The VPN settings screen will be displayed.

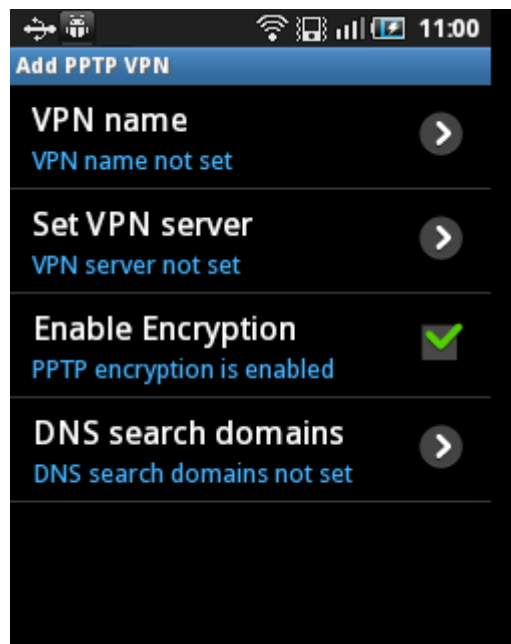


5. Tap 'Add VPN' in the screen.
The 'Add VPN' screen will be displayed.

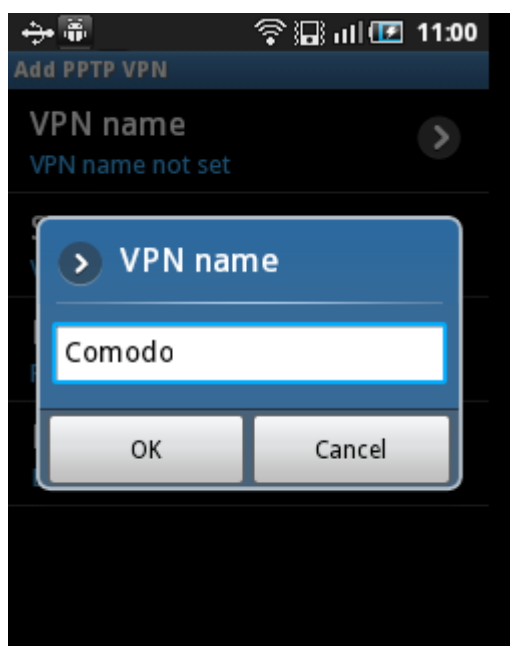


6. Tap 'Add PPTP VPN' the screen.

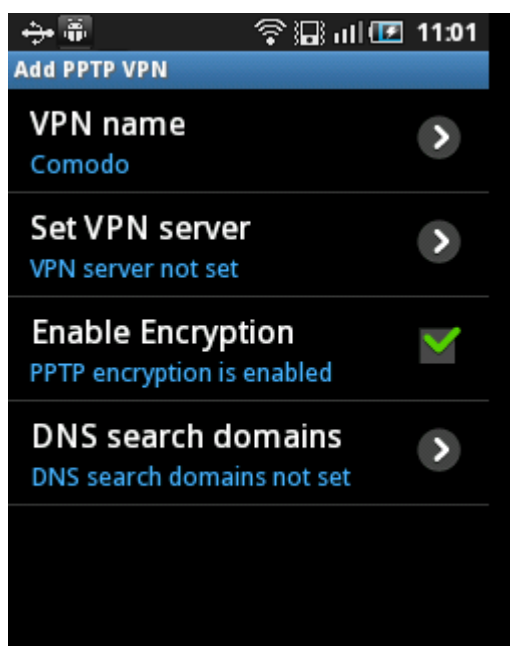
The 'Add PPTP VPN' screen will be displayed.



7. Tap 'VPN name' and enter a name for the VPN and tap 'OK'.

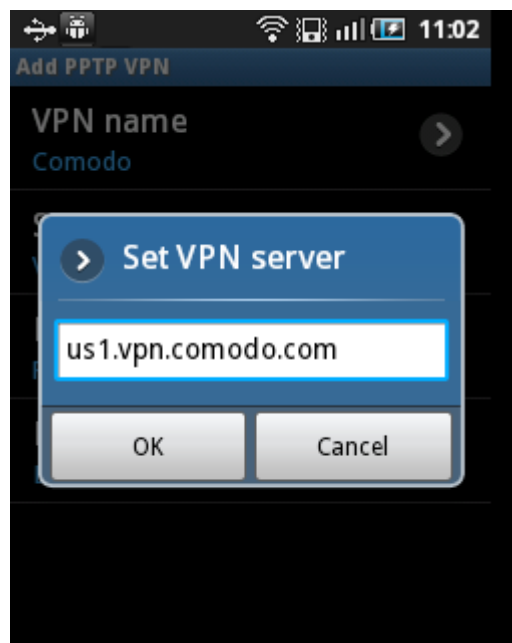


8. Tap 'Set VPN server' in the screen...

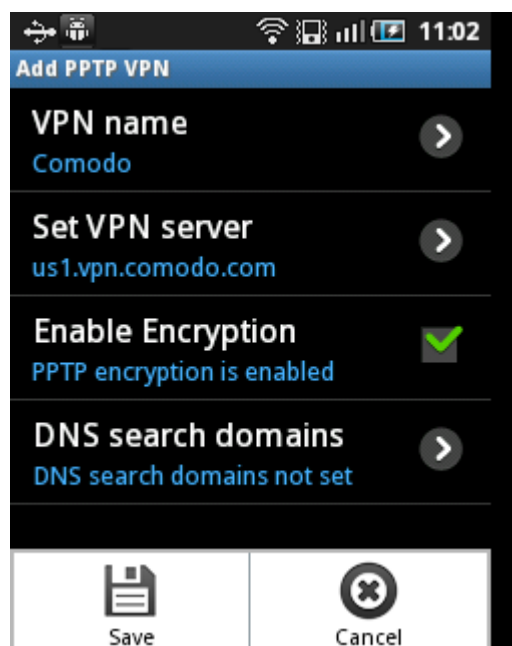


...and enter one of the following addresses in the server field and tap 'OK'.

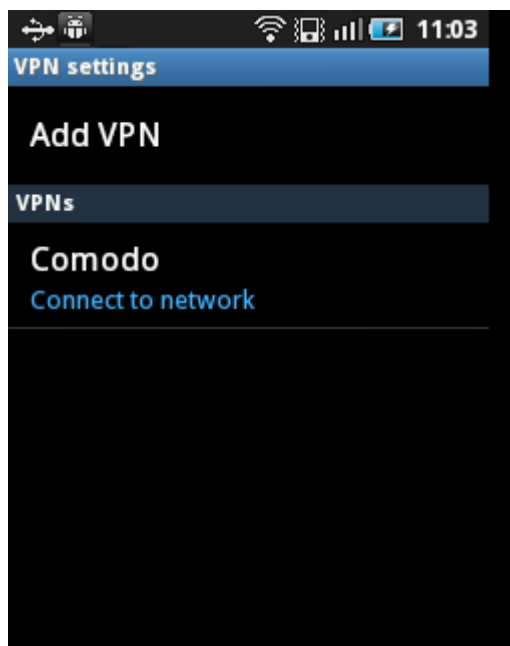
- us1.vpn.comodo.com
- us2.vpn.comodo.com
- uk1.vpn.comodo.com
- uk2.vpn.comodo.com



9. Press options key and tap Save.



The VPN will be added and displayed in the VPN settings screen.



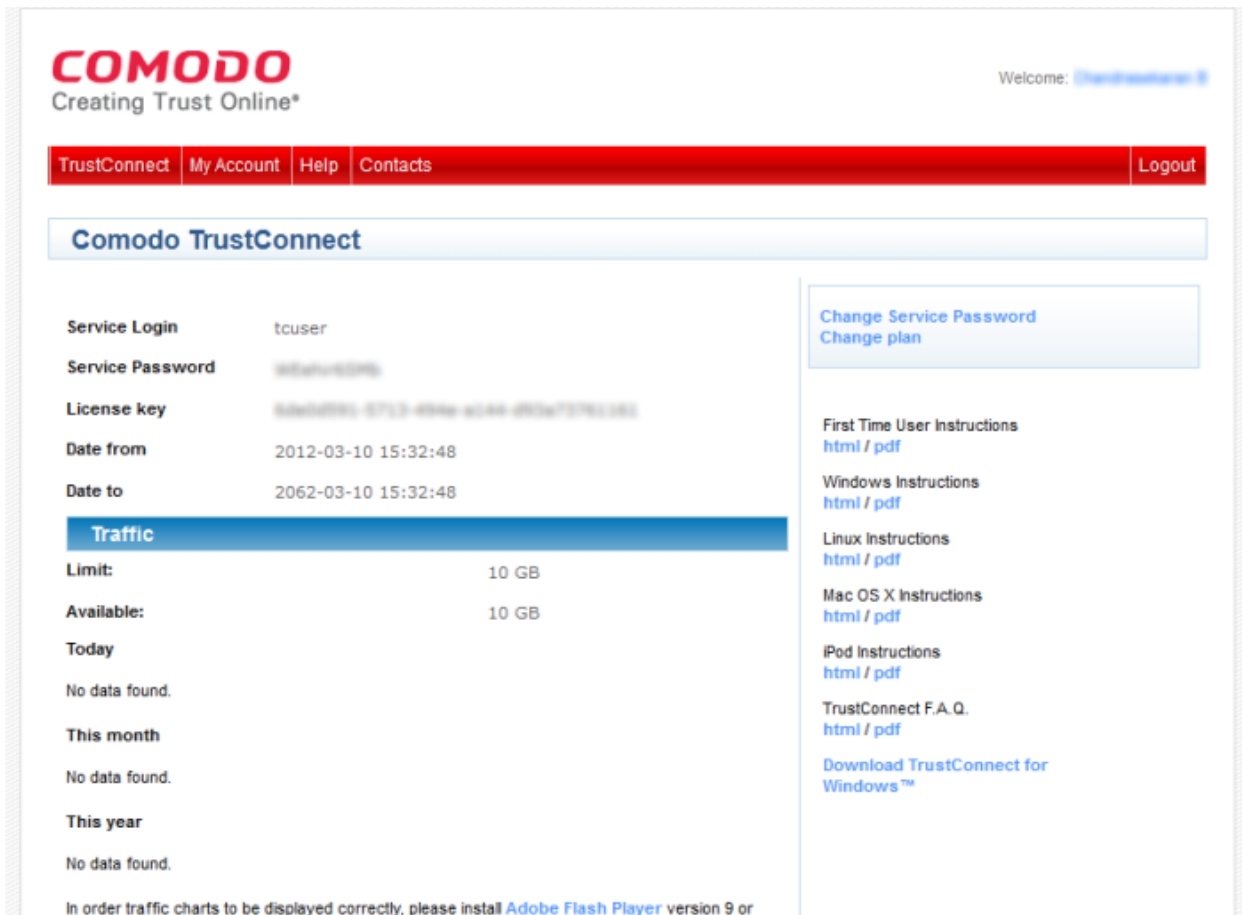
- To connect, tap on the VPN name.



- Enter your TrustConnect username and password.

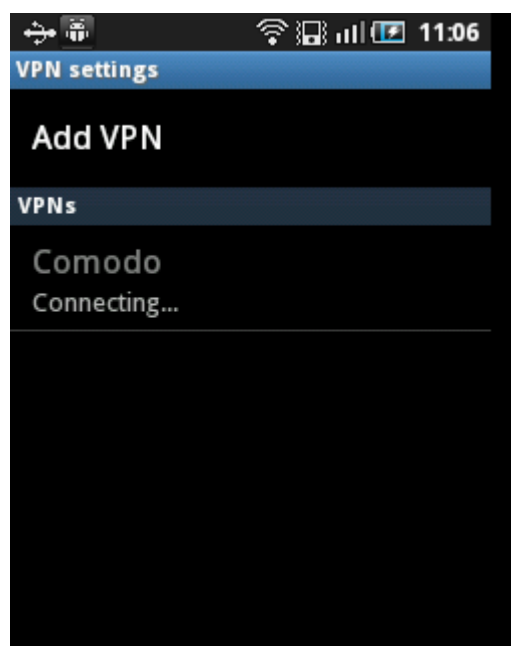
TIP: Select the 'Remember user name' checkbox and you need not enter the login credentials from next time onwards.

You need to enter TrustConnect service password here (Not the CAM password). To know your service password, login to your CAM Account at <https://accounts.comodo.com/account/login> and click TrustConnect in the menu bar.

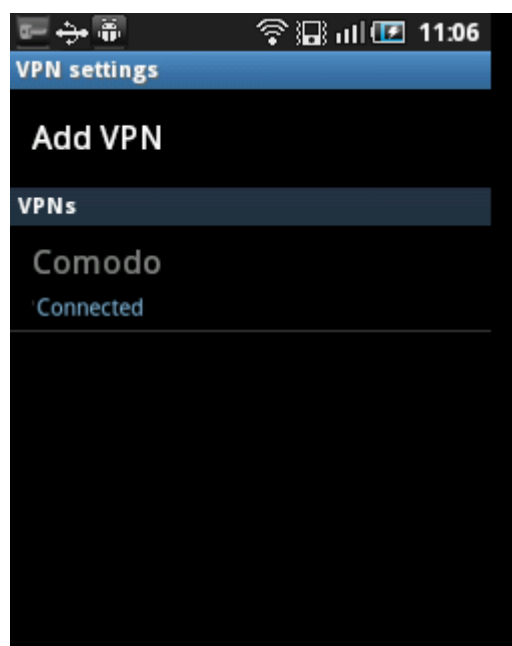


The name, service password and license key details are blurred intentionally in the screenshot above and will be clearly visible when you login to your CAM account.

The connection progress will be displayed...



...and after authenticating the login credentials, your Android device will be connected.



A key icon will be displayed in the notifications area once a successful connection is made.

8.6. Windows Mobile Devices - Configuration and Connection

1. Tap 'Start' in the notifications bar.



2. Tap 'Settings' in the screen.



3. In the 'Settings' screen, tap 'Connections'.



4. In the 'Connections' screen, tap 'Connections' again.



- In the 'Connections Settings' screen, tap the 'Add a new VPN server connection' link.



- In the 'Make New Connections' screen, enter the relevant details:

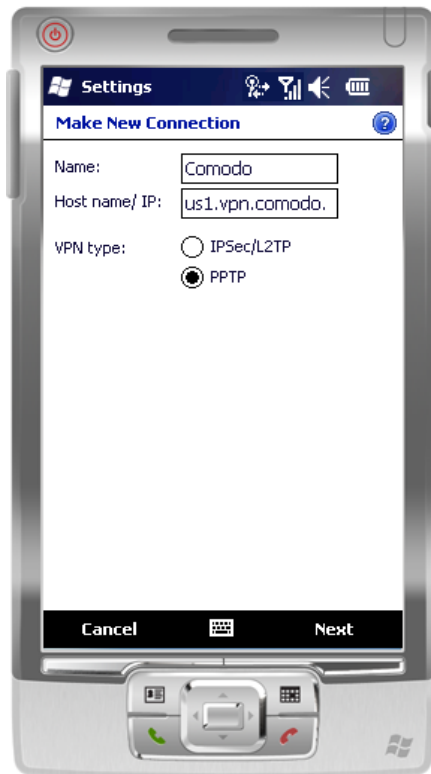
Name: Enter any name in the box.

Host name/IP: Enter any of the following addresses:

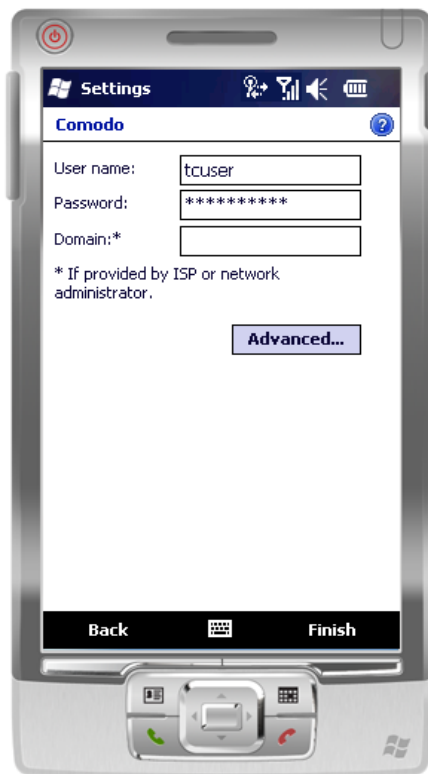
- us1.vpn.comodo.com
- us2.vpn.comodo.com

- uk1.vpn.comodo.com
- uk2.vpn.comodo.com

VPN type: Select 'PPTP'.



7. Tap 'Next'.



8. Enter your TrustConnect user name and password.

You need to enter TrustConnect service password here (Not the CAM password). To know your service password, login to your CAM Account at <https://accounts.comodo.com/account/login> and click TrustConnect in the menu bar.

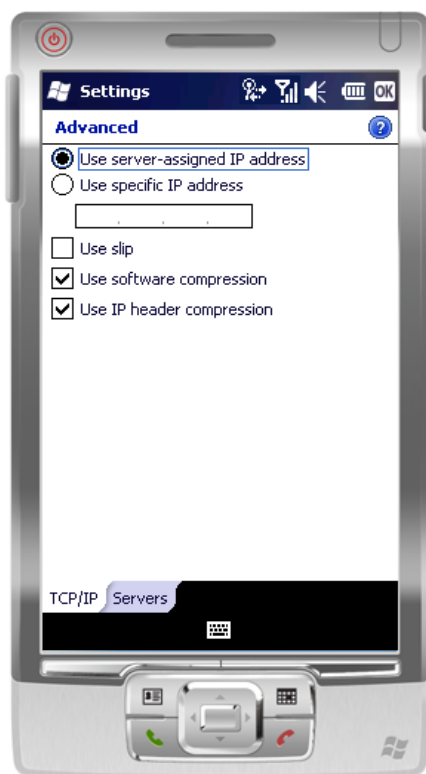
The screenshot displays the Comodo TrustConnect user interface. At the top left is the Comodo logo and tagline 'Creating Trust Online*'. On the top right, it says 'Welcome: [username]'. Below this is a navigation bar with links for 'TrustConnect', 'My Account', 'Help', 'Contacts', and 'Logout'. The main content area is titled 'Comodo TrustConnect' and contains several sections:

- Account Details:**
 - Service Login: tcuser
 - Service Password: [blurred]
 - License key: [blurred]
 - Date from: 2012-03-10 15:32:48
 - Date to: 2062-03-10 15:32:48
- Traffic:**
 - Limit: 10 GB
 - Available: 10 GB
 - Today: No data found.
 - This month: No data found.
 - This year: No data found.
- Right-hand sidebar:**
 - Change Service Password / Change plan
 - First Time User Instructions (html / pdf)
 - Windows Instructions (html / pdf)
 - Linux Instructions (html / pdf)
 - Mac OS X Instructions (html / pdf)
 - iPod Instructions (html / pdf)
 - TrustConnect F.A.Q. (html / pdf)
 - Download TrustConnect for Windows™

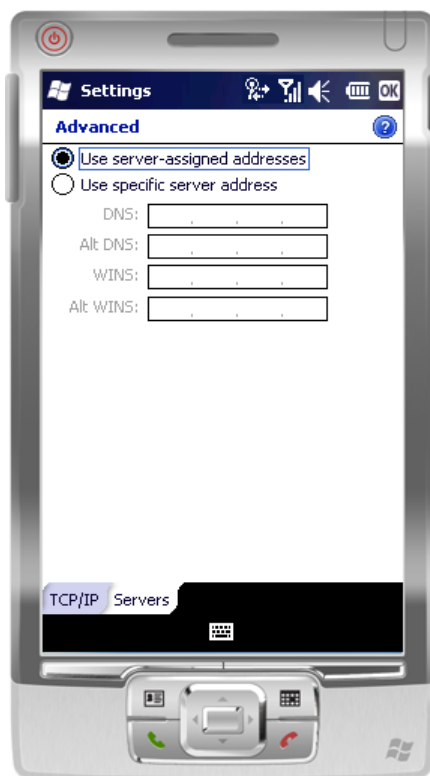
At the bottom of the traffic section, a note reads: 'In order traffic charts to be displayed correctly, please install Adobe Flash Player version 9 or higher'.

The name, service password and license key details are blurred intentionally in the screenshot above and will be clearly visible when you login to your CAM account.

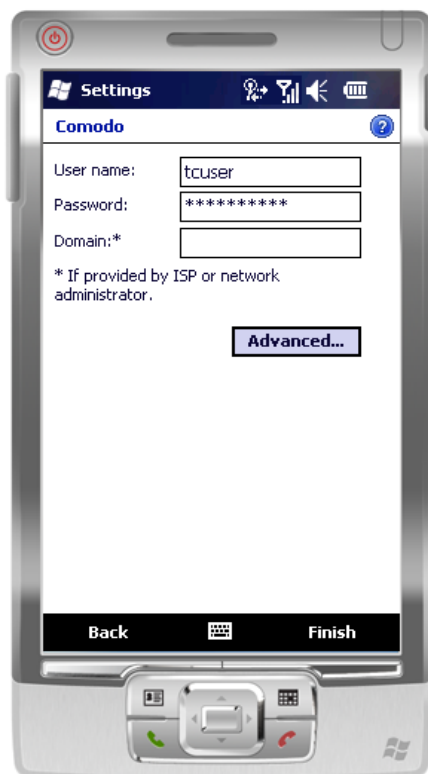
9. Tap 'Advanced' and retain the default settings in the 'TCP/IP' tab as shown below.



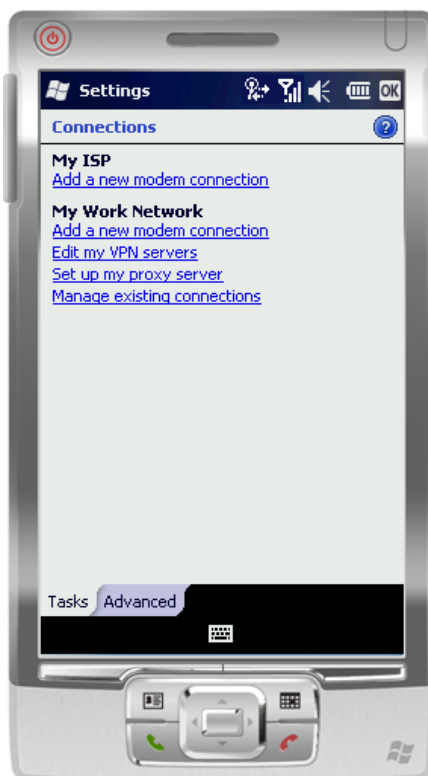
10. Tap the 'Servers' tab and retain the default settings (all the fields should be blank and 'Use server-assigned addresses' selected) as shown below.



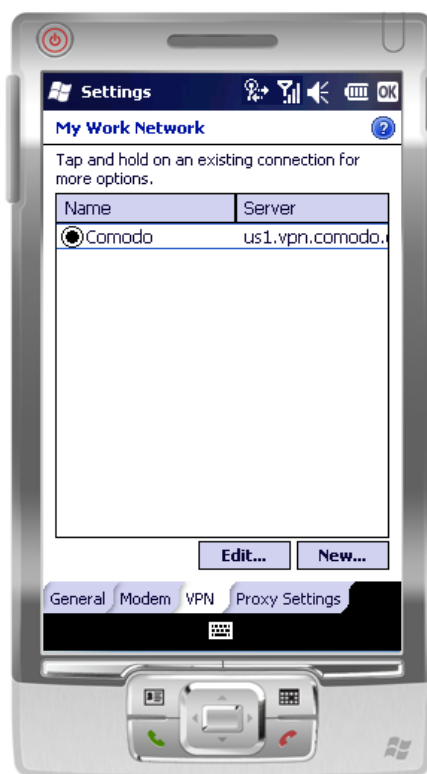
11. Tap 'OK' in the notifications area and tap 'Finish'.



12. Tap 'Edit my VPN servers' link.



13. Tap and hold the newly configured connection.



14. Tap 'Connect' in the drop-down.



The connection progress will be displayed...



...and on successful connection, the details will be displayed.



That's it. Now your Windows mobile device is connected to Comodo TrustConnect.

8.7. TrustConnect FAQ

Common Questions

1. [How do I set up TrustConnect and Log on to the TrustConnect Server?](#)
2. [My User Name and Password don't work - why not?](#)
3. [What Operating Systems does TrustConnect support?](#)
4. [What clients should I use to connect to the TrustConnect Server?](#)
5. [All our Internet \(HTTP & HTTPS\) connections are via a proxy server. How do I connect using TrustConnect in this situation?](#)
6. [Why do I need a Secure Connection like Comodo TrustConnect?](#)
7. [What is a Sniffer?](#)
8. [Do I have to use a wireless connection to use Comodo TrustConnect?](#)
9. [I have a Wi-Fi at home with WEP turned on. Am I safe?](#)
10. [Is the TrustConnect license for only one computer, or can I install it on others in my home network?](#)
11. [What is the typical connection speed through TrustConnect?](#)
12. [How do I cancel my account?](#)
13. [What security measures does TrustConnect use?](#)
14. [Can TrustConnect work on a PC behind a NAT-enabled router?](#)

Windows Configuration

1. [What is the "TAP-Win32 Adapter" that appears in my "Network Connections"?](#)
2. [I'm sure I've done everything correctly but I still cannot connect to the server.](#)
3. [I can connect to the server, but cannot get access to any site. IPCONFIG /ALL shows IP 0.0.0.0 for the TAP adapter. What's wrong?](#)
4. [Do I need my Firewall up while connecting to the WEB via TrustConnect?](#)
5. [What port numbers are used by TrustConnect?](#)

Windows Vista Configuration

1. [I cannot connect to the server. Log file contains the entry "All TAP-Win32 adapters on this system are currently in use." But I cannot find any adapters in my "Network Connections". What is the problem?](#)
2. [All adapters are located in correct place, but I still cannot connect to the server.](#)

iPhone/iPod Client Configuration

1. [The server did not respond when I try to connect.](#)
2. [What are the TrustConnect server addresses?](#)
3. [What port numbers are used by TrustConnect for iPod clients?](#)

Common Questions

How do I set up TrustConnect and Log on to the TrustConnect Server?

1. Firstly, log into your Comodo Account at <https://accounts.comodo.com> with the user name and password that you created during the TrustConnect or CIS Complete enrollment process.
2. Click the 'TrustConnect' tab on the top navigation bar.
3. Download, install and configure the appropriate TrustConnect client software for your operating system. All necessary software and instructions are available on the right hand side of the 'TrustConnect' area of your account. Alternatively, please use the following links:

Windows

[View TrustConnect Windows Client Configuration Guide](#)

[Download the Windows TrustConnect Client](#)

MAC OS X

[View TrustConnect MAC OS X Client Configuration Guide](#)

Linux / OpenVPN

[View TrustConnect Linux Client Configuration Guide](#)

iPhone / iPod Touch

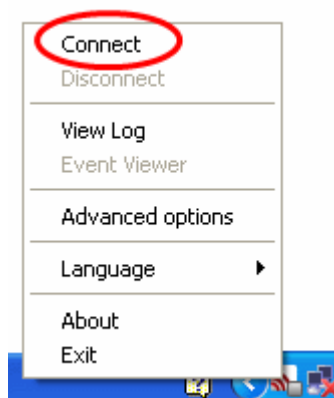
[View TrustConnect iPod Client Configuration Guide](#)

- Once installed, start up the Trust Connect Client.

The following example shows how to connect using the Windows client:

Click **Start > Programs > Comodo > Trust Connect > Trust Connect**

Or, if TrustConnect is already running, right click on the tray icon and select 'Connect':



- At the login box you should enter your **TrustConnect Service Login and Service Password**.

Note: This is not the same password as your Comodo Account password. It is a unique, random password that was generated during account creation to authenticate you to the TrustConnect servers. If required, you can change this password to something more memorable by using the 'Change Service Password' button on the right.

COMODO
Creating Trust Online®

Welcome: John

Comodo Internet Security | TrustConnect | My Account | Help | Contacts

Comodo TrustConnect

Service Login	jsmith
Service Password	1aB2cdeeFG
License key	e11b3e35-937d-47ef-957d-a2207a4c75b2
Date from	2010-08-16 06:40:09
Date to	2011-08-16 06:40:09

[Change Service Password](#)
[Change plan](#)

First Time User Instructions
[html](#) / [pdf](#)

Traffic	
Limit:	10 GB
Available:	10 GB
Today	
No data found.	
This month	

Comodo TrustConnect - User Authentication

Username:

Password:

Remember

6. The TrustConnect tray icon turns green upon successful connection:



Not Connected to TrustConnect	Attempting to connect to TrustConnect	Successfully connected to TrustConnect
-------------------------------	---------------------------------------	--

My User Name and Password don't work - why not?

Make sure that you are entering the TrustConnect Service login details and NOT your Comodo Account Manager login details.

As a TrustConnect customer (or CIS Complete customer which includes TrustConnect service) you have two sets of login details:

Your Comodo Account Login Details. This user name and password enables you to log into your account at <https://accounts.comodo.com> to view and configure account details. You created this on the sign - up form when you enrolled for TrustConnect or CIS Complete.

Your TrustConnect Service Login Details. This user-name and password is used to connect to the TrustConnect server and should be entered at the **client login box**.

To view your TrustConnect Service Login details:

- Login at <https://accounts.comodo.com> with your Comodo Account Login Details
- Click the 'TrustConnect' button on the top navigation
- Your service login and password are listed. You can change this password at any time by clicking the 'Change Service Password' button.

What operating systems does TrustConnect support?

TrustConnect is successfully tested on Windows 2000, Windows XP, Windows Vista, Linux and Mac Os X. It supports mobile devices like iPod/iPhone as well.

What clients should I use to connect to the TrustConnect server?

To start using TrustConnect you must first download and install the appropriate TrustConnect client software for your operating system. Client software for supported operating systems is available for download in the TrustConnect area of your account. Alternatively, use the following links:

Windows

[View TrustConnect Windows Client Configuration Guide](#)

[Download the Windows TrustConnect Client](#)

MAC OS X

[View TrustConnect MAC OS X Client Configuration Guide](#)

Linux / OpenVPN

[View TrustConnect Linux Client Configuration Guide](#)

iPhone / iPod Touch

[View TrustConnect iPod Client Configuration Guide](#)

All our Internet (HTTP & HTTPS) connections are via a proxy server. How do I connect using TrustConnect in this situation?

If you use the Windows client, you should:

- Change the TrustConnect target (command) line:
 - Right click on 'TrustConnect' icon;
 - Select 'Properties' -> 'Shortcut';
 - Add the following text **--allow_proxy 1** into the 'Target' field, so it looks like this:

```
"C:\Program Files\Comodo\TrustConnect\bin\TrustConnect.exe" --allow_proxy 1
```

Target:

- ii. Start TrustConnect client
- iii. Set your proxy settings:
 - Right click on 'TrustConnect' tray icon and select 'Proxy Settings';
 - Select 'Manual Configuration' and enter your proxy settings, for example:
HTTP proxy, Address: 192.168.0.1, Port: 3128
- iv. Connect to TrustConnect.

If you use the Linux/Unix or MAC OS X client, you need only add the http-proxy directive to the client configuration file. For example: http-proxy 192.168.0.1 3128.

If you use iPhone/iPod client:

- Set your proxy settings on the VPN settings: 'Setting' -> 'General' -> 'Network' -> 'VPN' -> 'Settings' -> 'Proxy'

Why do I need a Secure Connection like Comodo TrustConnect?

If you are logging onto the Internet using Wi-Fi public hotspots, then all of your information is in a readable, plain text format that cyber criminals can sniff. In addition, many hotels have sniffable wired networks. When you're traveling, all of your information can be seen, including confidential company and personal information.

What is a Sniffer?

Typically, a computer only receives traffic aimed at its TCP/IP address. Sniffer software allows a computer to record traffic headed to (and from) every computer on the local network.

Do I have to use a wireless connection to use Comodo TrustConnect?

Not at all. Some networks, even if they are physically hard-wired and not wireless, do not have secure connections. You can use Comodo TrustConnect even from a wired connection if you need to encrypt your session or hide your destination. If you'd like another layer of protection, Comodo TrustConnect can provide it.

I have a Wi-Fi at home with WEP turned on. Am I safe?

No. Cyber criminals can break WEP encryption with easy-to-acquire tools that are available on the Internet. Computers without firewalls are even more vulnerable to attack. Comodo TrustConnect helps make your connection secure even on your home-based Wi-Fi connection.

Is the TrustConnect license for only one computer, or can I install it on others in my home network?

You may install TrustConnect client software on any amount of PCs you wish, but you are allowed to connect to TrustConnect service with one of them at a time. For example, you may install TrustConnect on work PC and on your own laptop and connect to TrustConnect from work computer or from laptop, but not simultaneously.

The license agreement can be read here: <https://accounts.comodo.com/trustconnect/management/eula>

What is the typical connection speed through TrustConnect?

All TrustConnect connections are made over 128 bit SSL encrypted connections so typical speeds are between 1.5 - 3.0 Mbps.

How do I cancel my account?

If you would like to cancel your TrustConnect account at any time, please send your request to trustconnectcancel@comodo.com Please remember to include your account user-name (login), email address and order number and a brief reason for cancellation.

What security measures does TrustConnect use?

All connections to TrustConnect are over 128-bit SSL encryption. Additionally, a private VPN session key is re-created every hour.

Can TrustConnect work on a PC behind a NAT-enabled router?

Yes. If your computer is connected to the Internet through a NAT-enabled router, you shouldn't have any problems connecting to

the TrustConnect service.

Microsoft Windows Questions

What is the "TAP-Win32 Adapter" that appears in my "Network Connections"?

The "TAP-Win32 Adapter" is virtual network card that is created by the TrustConnect client during installation. This adapter is required in order to establish a secure tunnel to the TrustConnect Server.

I'm sure I've done everything correctly but I still cannot connect to the server.

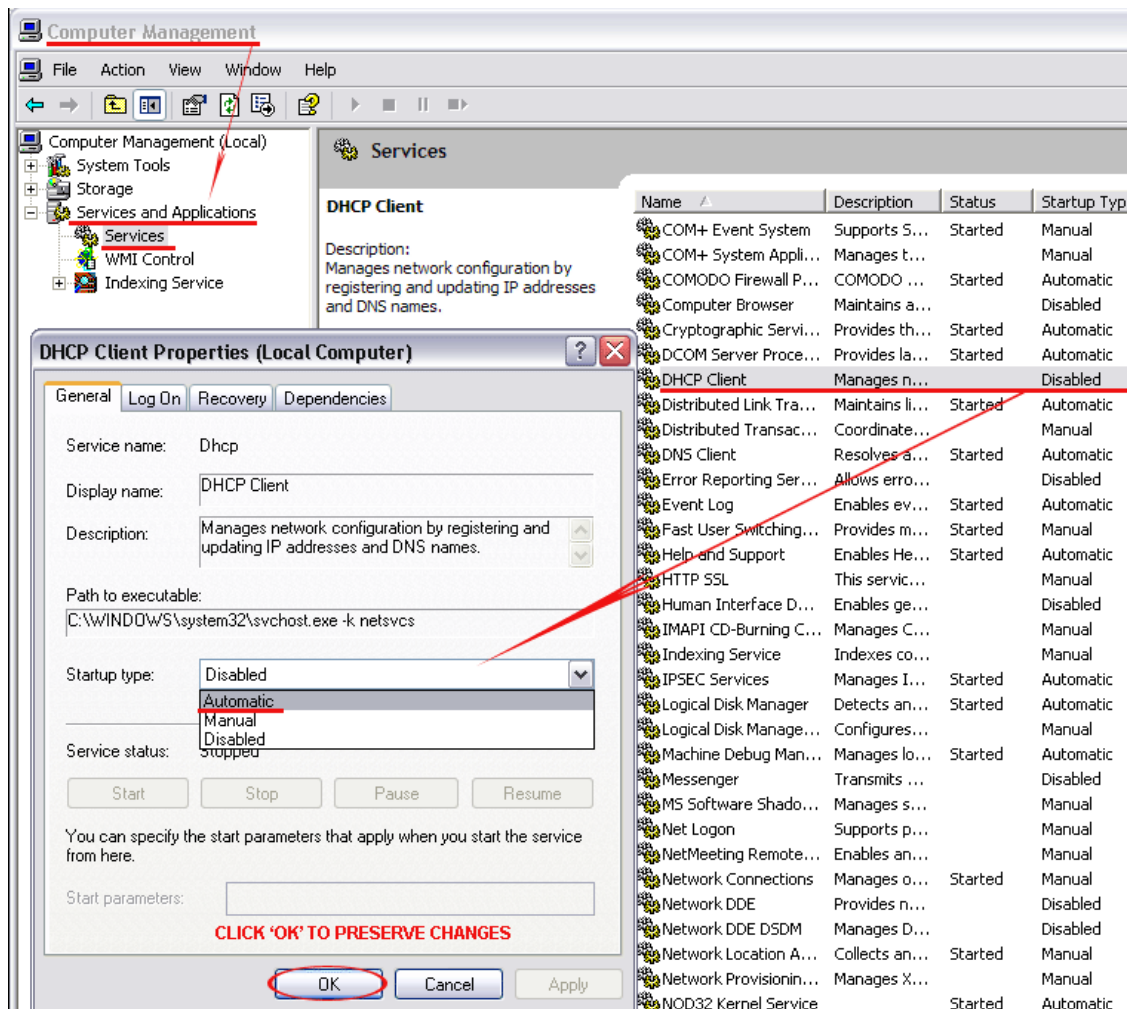
Make sure that you have been correctly entering your Service Login/Password. If it is incorrect you should visit <https://accounts.comodo.com/trustconnect/management> and check your Service Login.

I can connect to the server, but cannot get access to any site. IPCONFIG /ALL shows IP 0.0.0.0 for the TAP adapter. What is wrong?

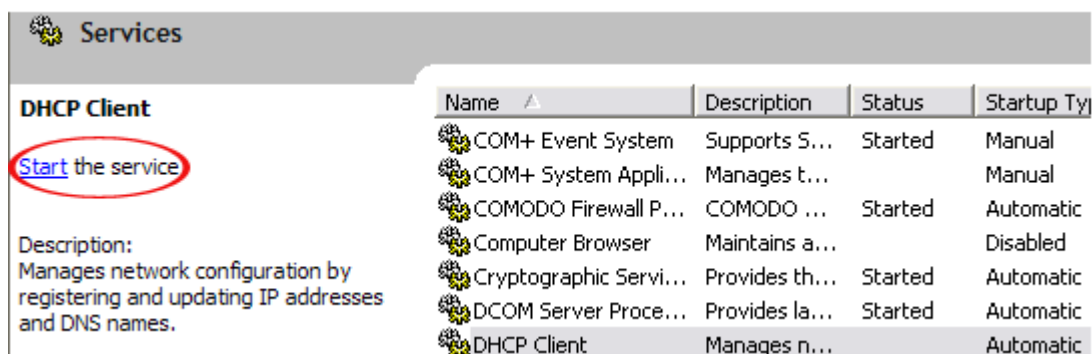
The DHCP Client service MUST be enabled.

To enable this service, you need to:

1. Right click on the Windows "My Computer" icon.
2. Select "Manage" from the context sensitive menu to open the Windows 'Computer Management' utility.
3. Select 'Services and Applications' then 'Services'.
4. Double-click 'DHCP Client' from the list of services that are listed in the right hand pane. This opens the DHCP Client Properties dialog.
5. Make sure 'Start Up Type' is set to 'Automatic'.
6. Click 'OK' to confirm and save your changes.



- The 'Start the service' link is now available. Click on it to run the DHCP Client.



The screenshot shows the Windows Services console. On the left, the 'DHCP Client' service is selected, and a red circle highlights the 'Start the service' link. Below the link, the description reads: 'Manages network configuration by registering and updating IP addresses and DNS names.' On the right, a table lists various services with their names, descriptions, statuses, and startup types.

Name	Description	Status	Startup Ty
COM+ Event System	Supports S...	Started	Manual
COM+ System Appli...	Manages t...		Manual
COMODO Firewall P...	COMODO ...	Started	Automatic
Computer Browser	Maintains a...		Disabled
Cryptographic Servi...	Provides th...	Started	Automatic
DCOM Server Proce...	Provides la...	Started	Automatic
DHCP Client	Manages n...		Automatic

Do I need my Firewall up while connecting to the WEB via TrustConnect?

Yes. TrustConnect ensures secure wireless connectivity to the Internet but does not secure all your computers ports (it is not designed for this purpose). You still need an effective firewall to protect your ports when surfing the 'net. Comodo recommends users install Comodo Internet Security which contains an award winning packet filtering personal firewall and is completely free for home and business users.

What port numbers are used by TrustConnect?

TrustConnect uses only port 443.

Microsoft Windows Vista Questions

I cannot connect to the server. The log file contains the entry "All TAP-Win32 adapters on this system are currently in use." - but I cannot find any adapters in my "Network Connections". What is the problem?

Always install and run TrustConnect under Administrator access rights.

All adapters are located in correct place, but I still cannot connect to the server.

You need to check the box against "Run this program as an administrator":

- Right click on TrustConnect icon;
- Select 'Properties' --> 'Compatibility'.

OR run the application under the Windows Vista "Run As Admin" option.

iPhone/iPod Client Questions

The server did not respond when I try to connect.

Check your network settings and access to Internet.

What are the TrustConnect Server Addresses?

You may use the following addresses when configuring the iPod / iPhone client:

- us1.vpn.comodo.com (commercial subscription)
- us2.vpn.comodo.com (commercial subscription)
- us3.vpn.comodo.com (free subscription)

What port numbers are used by TrustConnect for iPod clients?

TrustConnect for iPod clients uses 1723 port (PPTP service).

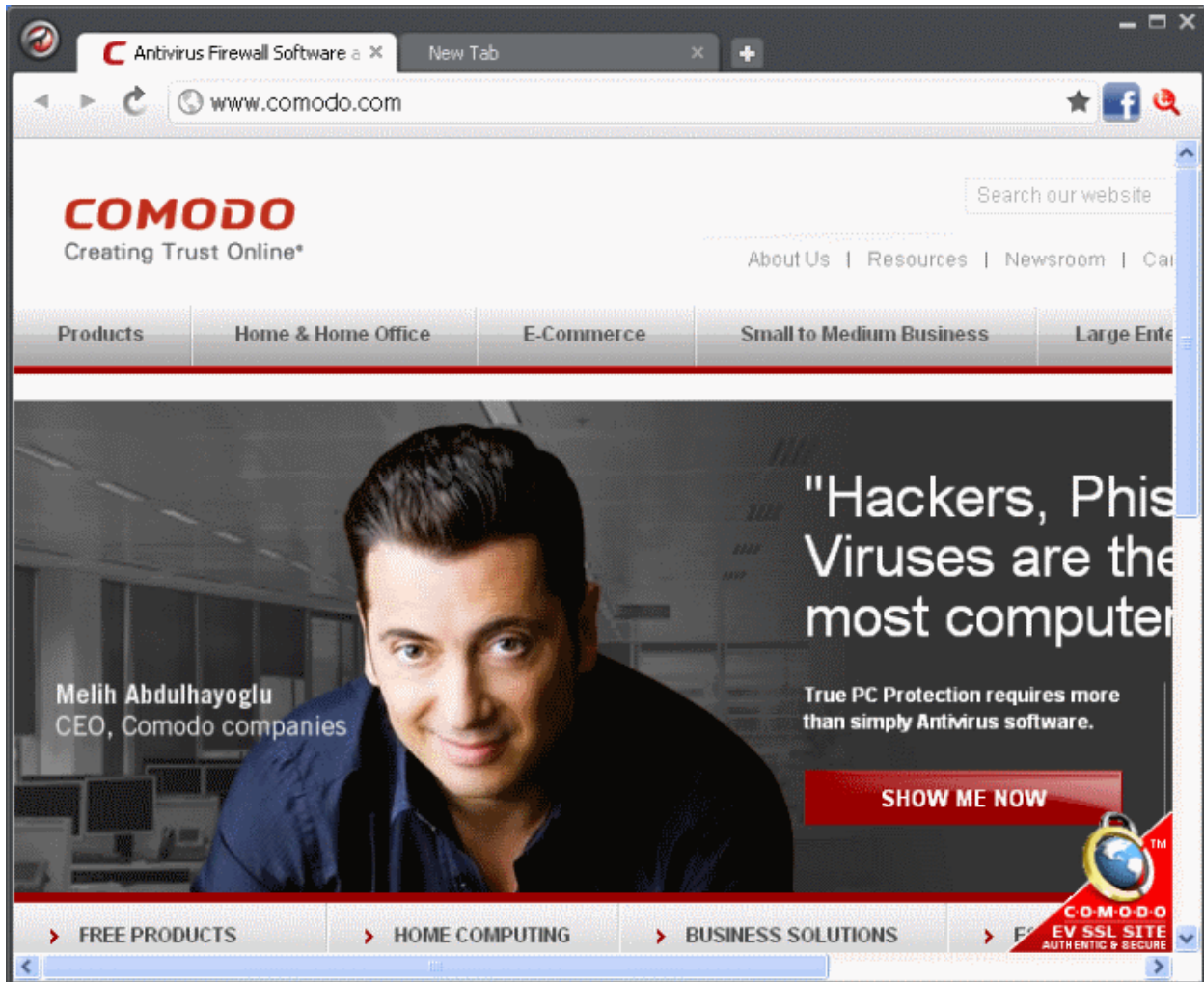
9. Comodo Dragon

Comodo Dragon is a fast and versatile Internet Browser based on Chromium and infused with Comodo's unparalleled level of security.

To help make your Internet browsing experience even safer, Comodo Dragon is installed in your computer as a part of Comodo Internet Security 2012. Comodo Dragon gives you the complete compliment of features offered by Chromium with superior

security and privacy.

- [Comodo Dragon Features](#)
- [Starting Comodo Dragon](#)
- [Comodo Dragon Help](#)



Features:

- Improved Privacy over Chromium
- Easy SSL Certificate Identification
- Fast Website Access
- Greater Stability and Less Memory Bloat
- Incognito Mode Stops Cookies, Improves Privacy
- Very easy to switch from your Browser to the Dragon

Comodo Dragon Security:

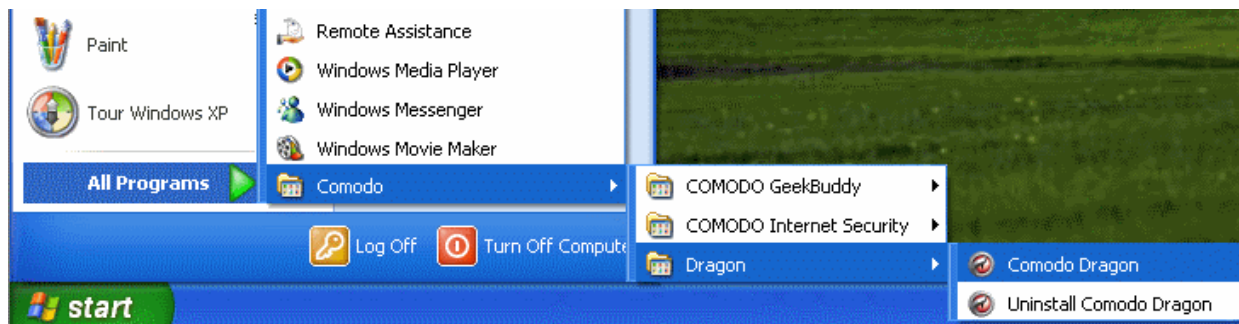
- Has privacy enhancements that surpass those in Chromium's technology
- Has Domain Validation technology that identifies and segregates superior SSL certificates from inferior ones
- Stops cookies and other Web spies
- Prevents all Browser download tracking to ensure your privacy

Starting Comodo Dragon

Comodo Dragon is installed in your computer along with Comodo Internet Security 2013. You can start the browser in two ways:

From the Start menu:

- Click Start > All Programs > Comodo > Dragon > Comodo Dragon:



From the Desktop Icon:

- Double Click on the Comodo Dragon Desktop icon created during the installation:



Comodo Dragon Help

Comodo Dragon's intuitive multi-tabbed interface enables easy and fast access to sophisticated features of the browser. Please refer to the Comodo Dragon online help guide at <http://help.comodo.com/topic-120-1-279-2524-Comodo-Dragon—Introduction.html> for more details on using the browser.

Appendix 1 - CIS How to... Tutorials

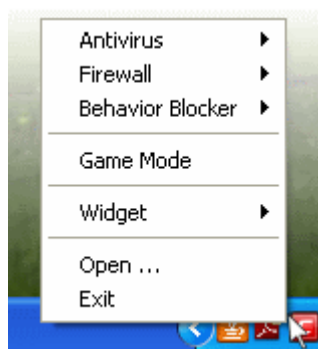
The 'How To...' section of the guide contains guidance on key tasks of Comodo Internet Security. Use the links below to go to each tutorial's page.

How to...:

- **Enable / Disable AV, Firewall and Behavior Blocker 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
- **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
- **Setup Behavior Blocker for maximum security and usability** - A brief outline of how to set Behavior Blocker 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 Kiosk** - Guidance on executing a program that you do not trust to be safe, inside the virtual kiosk.
- **Run Browsers Inside the Virtual Kiosk** - Guidance on running your browser, inside virtual kiosk 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
- **Selectively disable Behavior Blocker and Auto-Sandboxing for specific files** - Explains how to exclude specific files or file types from the auto-sandboxing process
- **Enable Full Virtualization for Auto-Sandboxed Applications (Advanced)** - Explains how to enable Full Virtualization for applications auto-sandboxed by Behavior Blocker
- **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

Enabling / Disabling AV, Firewall and Behavior Blocker Easily

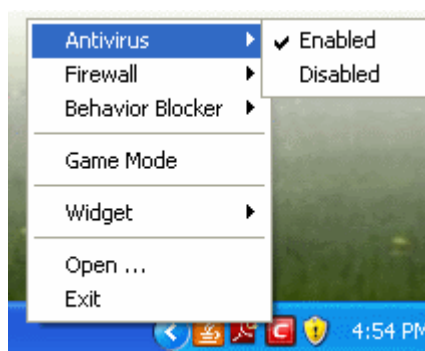
Comodo Internet Security allows users to quickly switch the Enabled/Disabled states of **Antivirus**, **Firewall** and **Behavior Blocker** by right clicking on the system tray icon.



Antivirus

To enable/disable the Antivirus

1. Right click on the system tray icon
2. Move the mouse cursor over 'Antivirus'



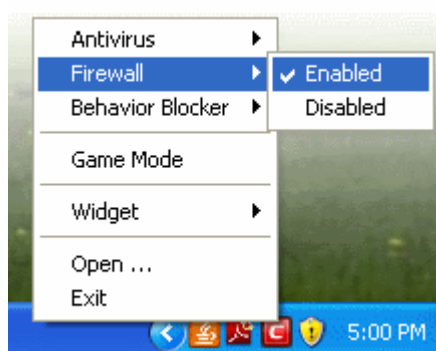
3. Choose 'Enabled or Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Firewall

To enable/disable the Firewall

1. Right click on the system tray icon
2. Move the mouse cursor over 'Firewall'



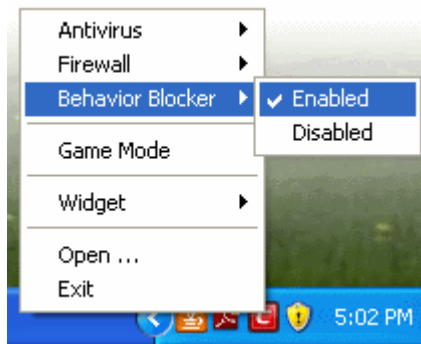
3. Choose 'Enabled or Disabled' as per your choice

You can find the set security level also from [the Home Screen](#).

Behavior Blocker

To enable/disable the Behavior Blocker

1. Right click on the system tray icon
2. Move the mouse cursor over 'Behavior Blocker'



3. Choose 'Enabled or Disabled' as per your choice

You can find the set security level also from [the Home Screen](#).

Setting up the Firewall For Maximum Security and Usability

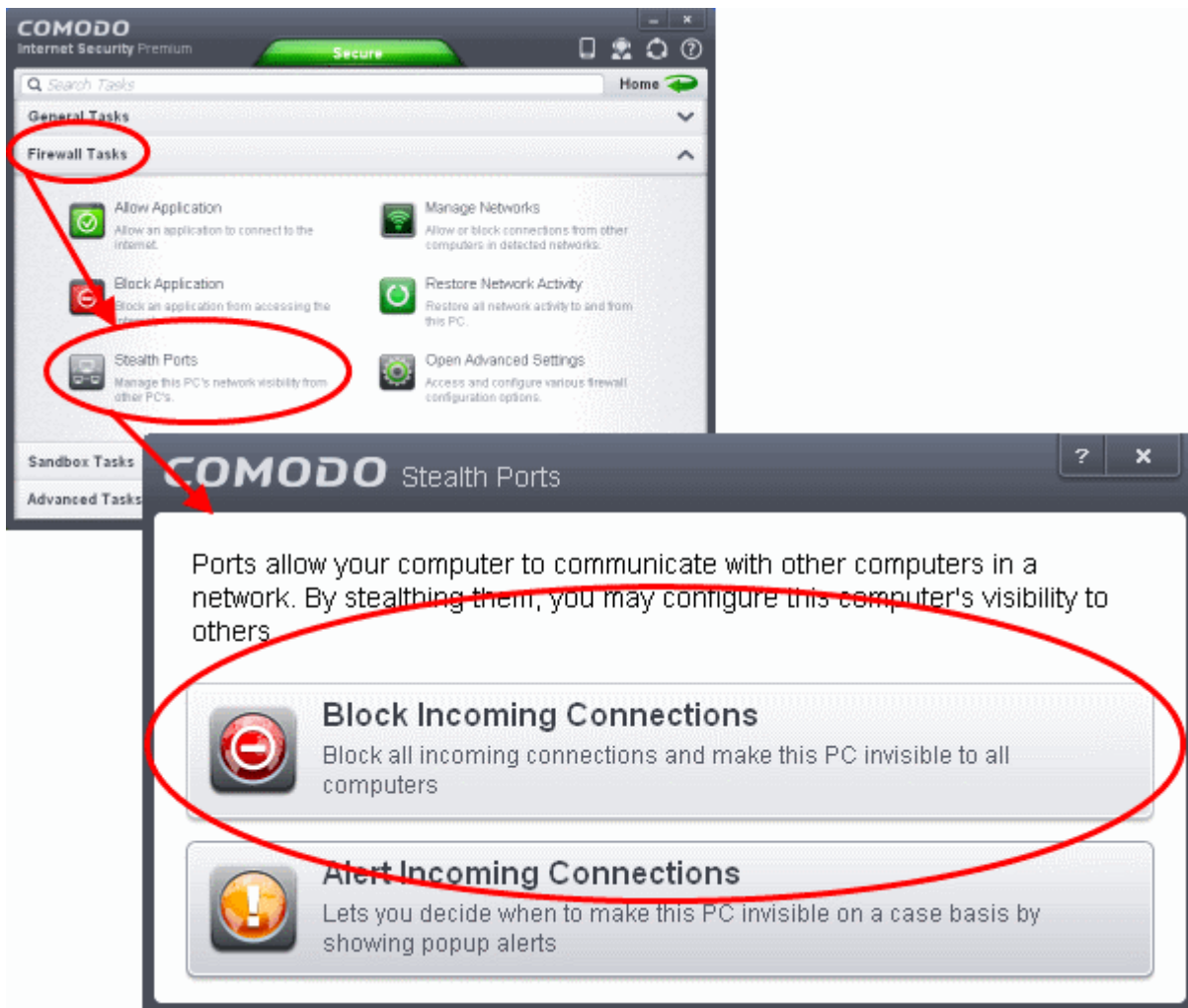
This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the Internet.

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

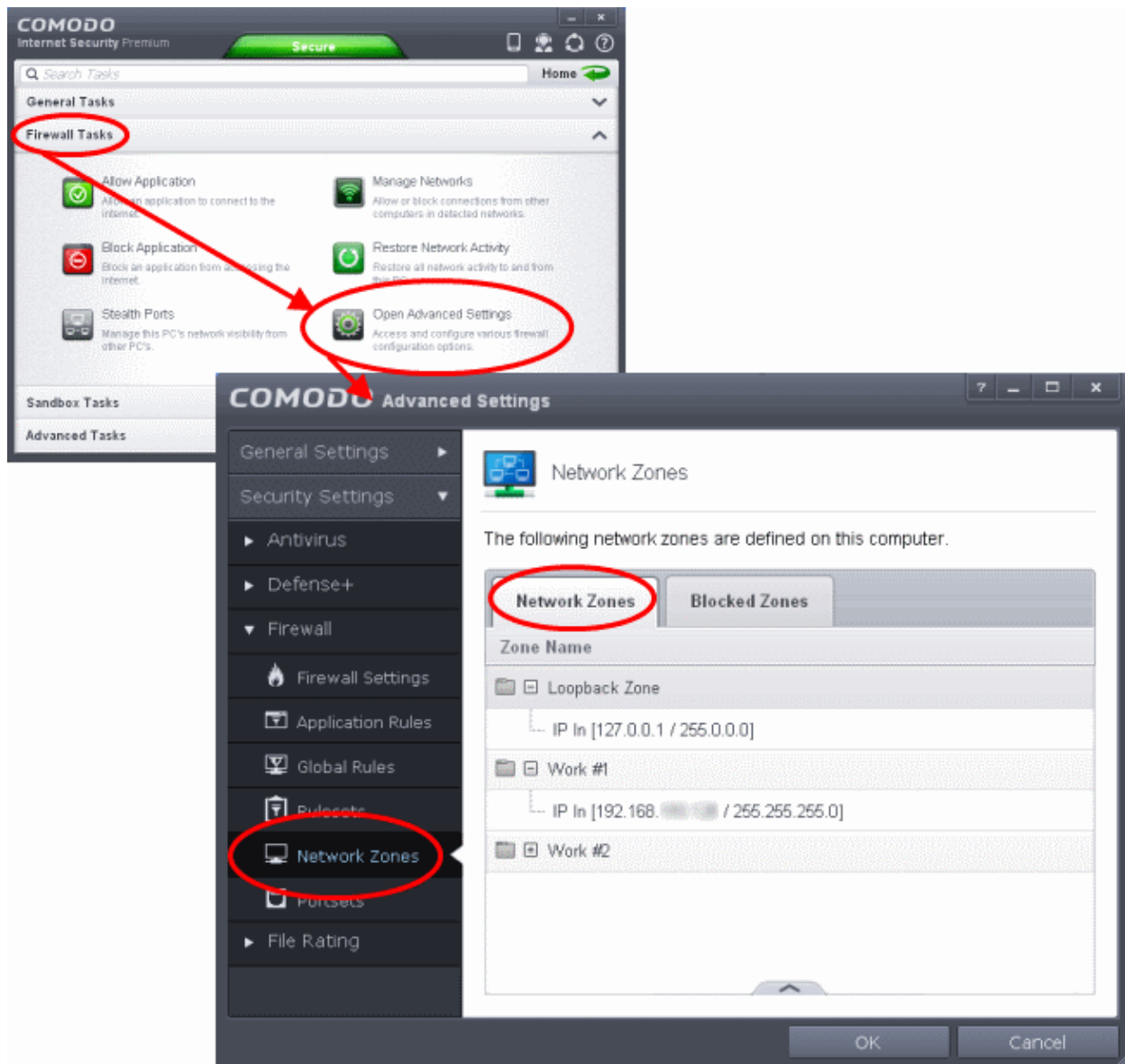
[Click here for more details on Stealthing your Computer Ports](#)

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 *127.0.0.1/255.0.0.0*

In most cases, the IP address of the auto detected Network zone should be *192.168.1.100/255.255.255.0*.

5. Check these addressees and click 'OK'.

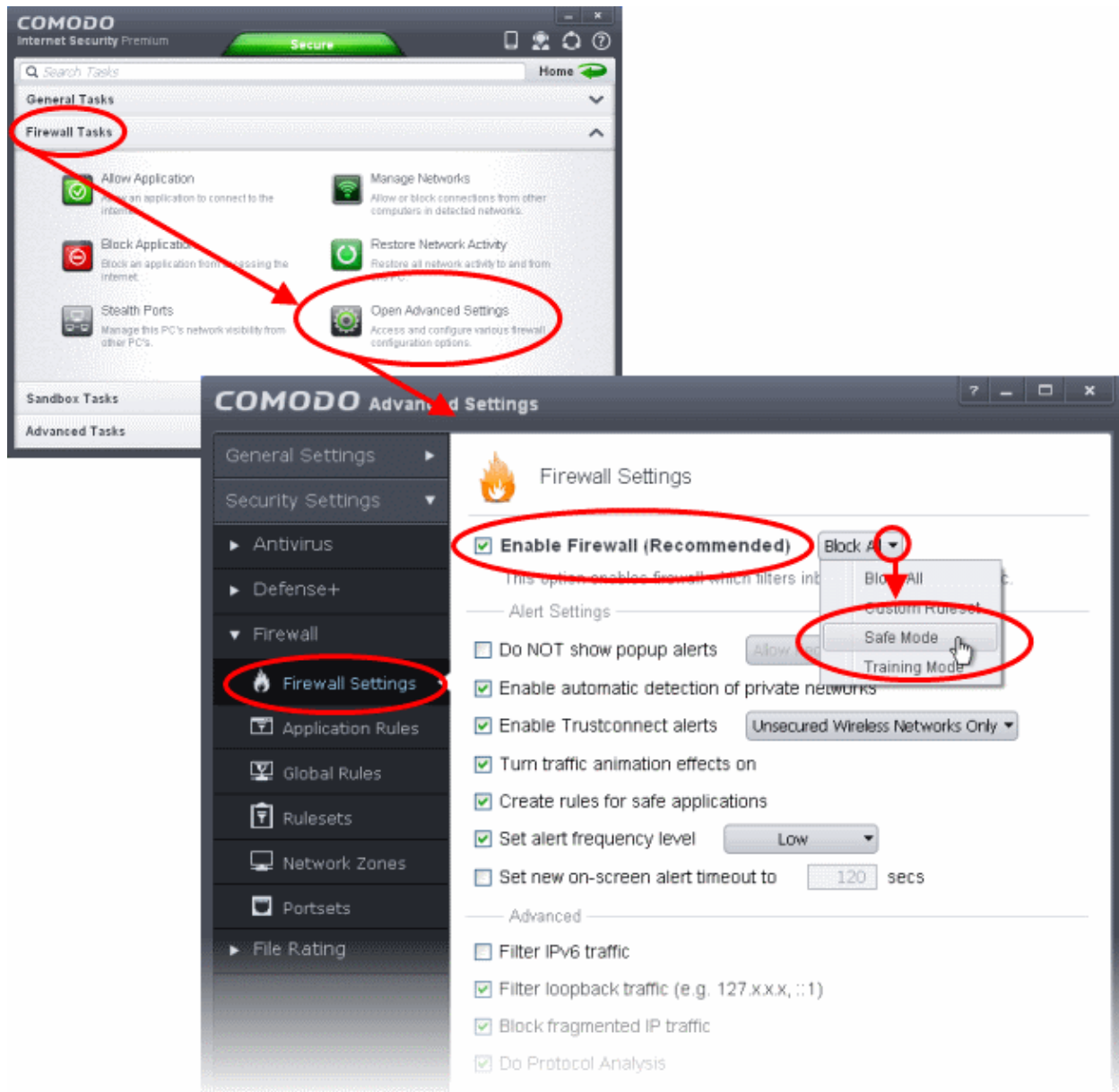
[Click here for more details on Network Zones settings](#)

Firewall Behavior Settings

The Firewall Behavior Settings option allows you to configure the protection level for your Internet connection and the frequency of alerts generated.

To open Firewall Behavior Settings panel

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Firewall Settings' under Firewall from the left hand side pane
4. Ensure that 'Enable Firewall' is selected and choose **Safe mode** from the drop-down beside it.



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

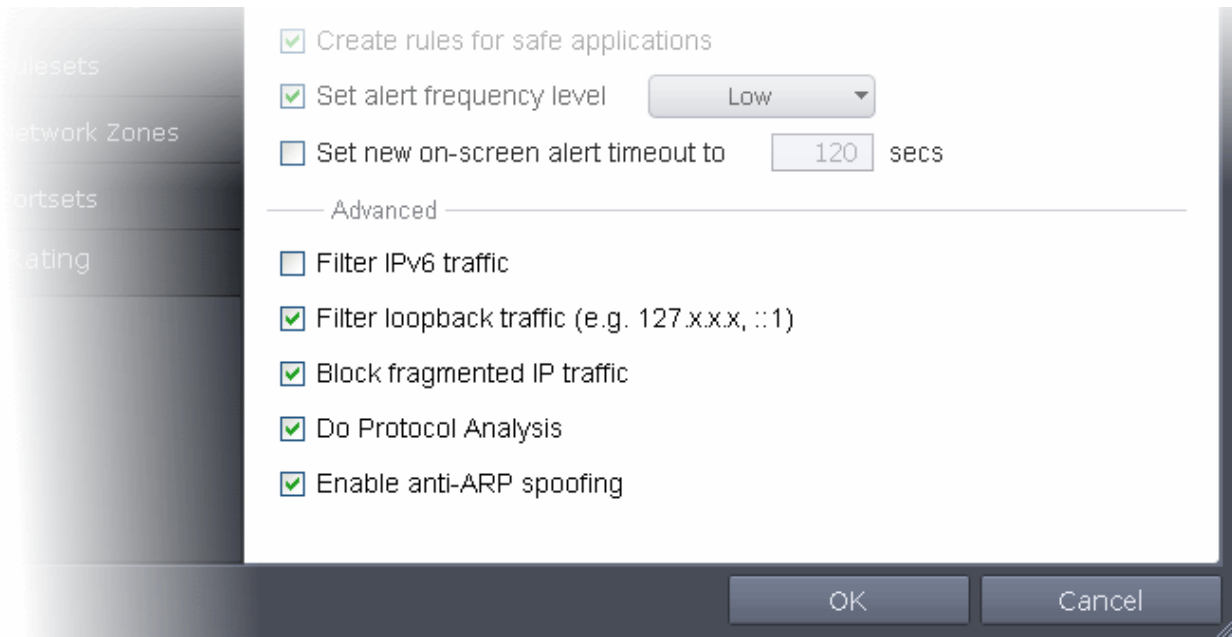
Under 'Alert Settings' in the same interface:

- 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.

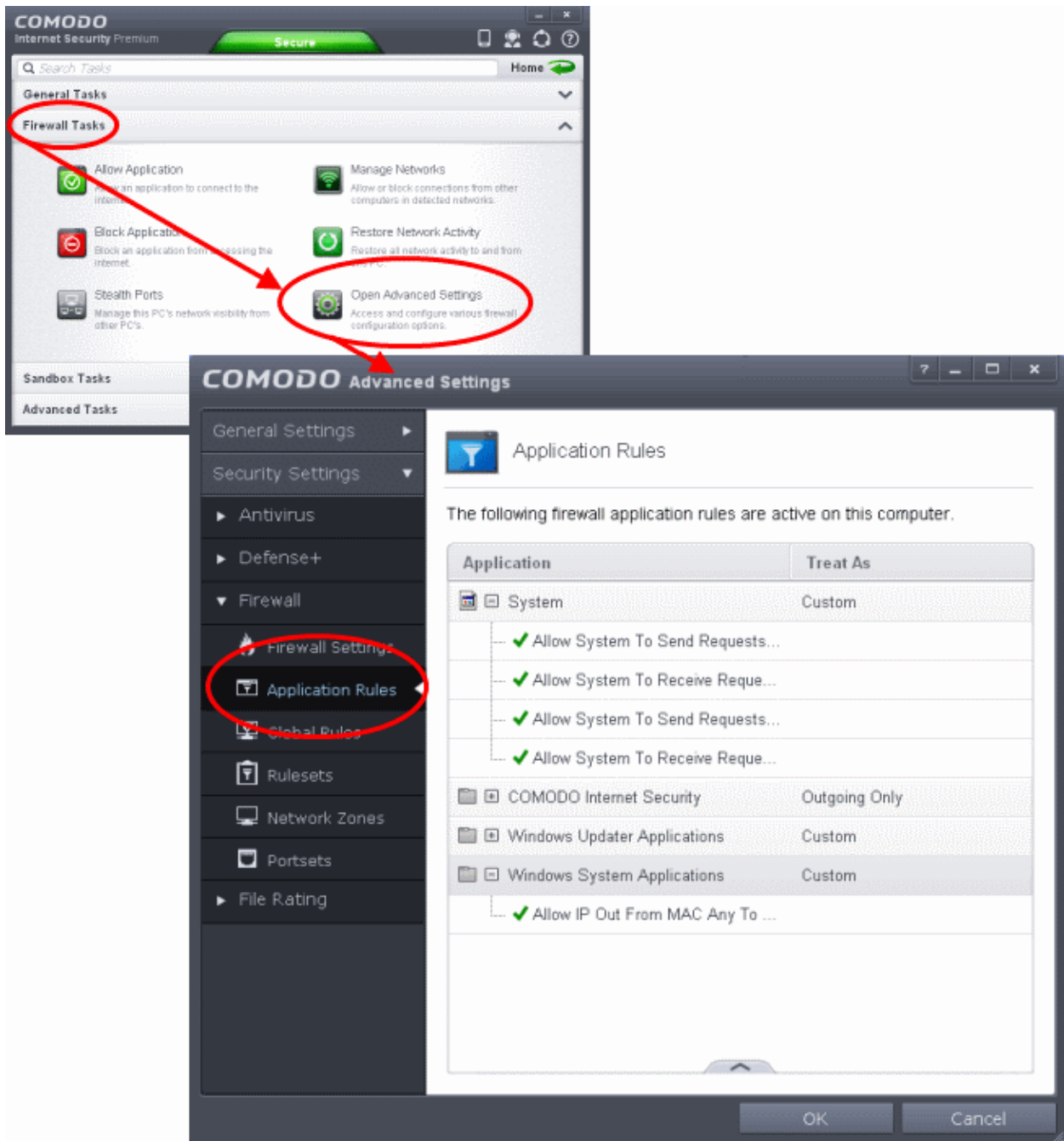
[Click here for more details on Firewall Behavior Settings](#)

Setting-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules and policies on an application specific and global basis and predefined firewall rulesets.

To view the Application Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Application Rules' under Firewall from the left hand side pane

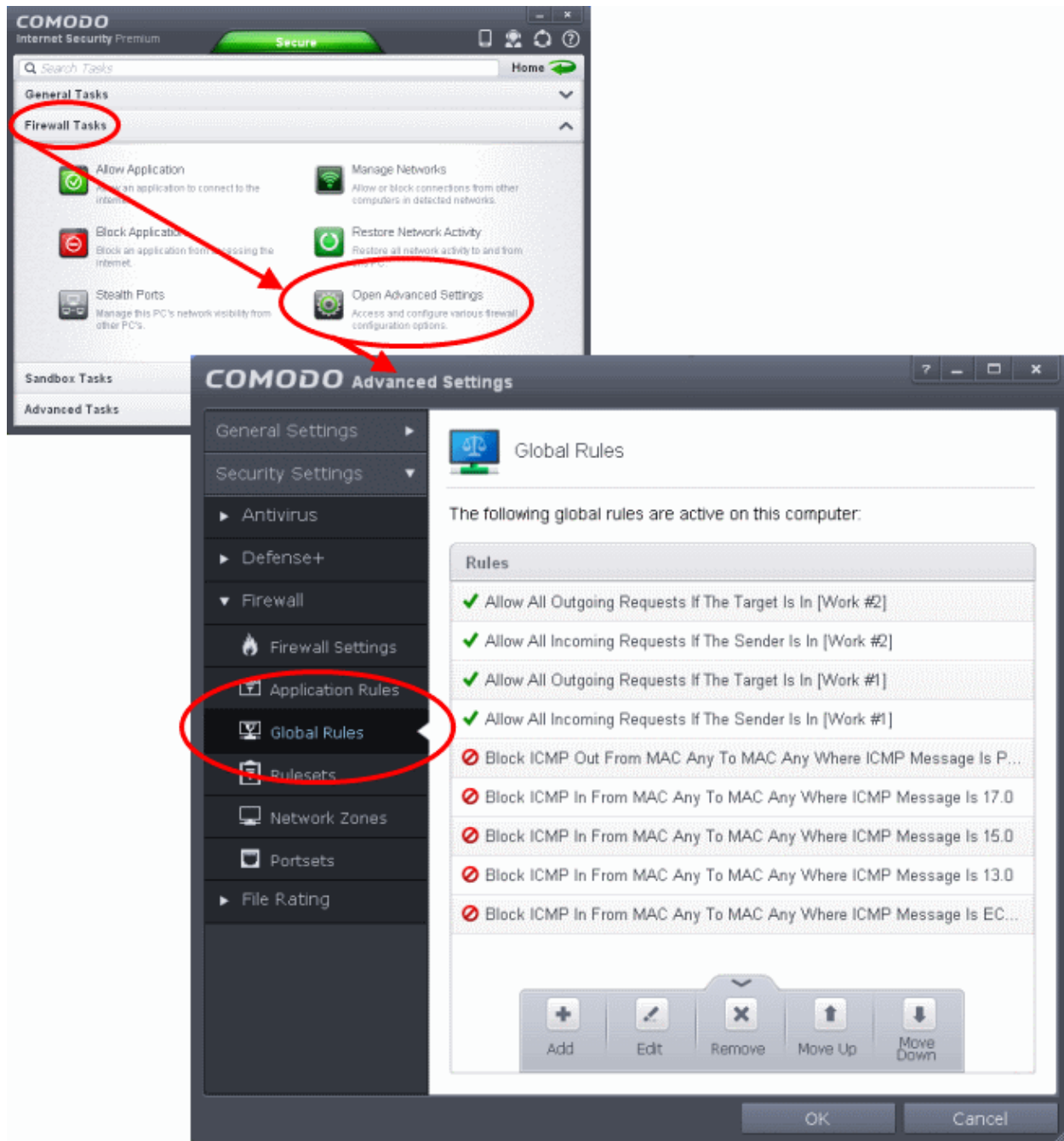


4. Click the handle from the bottom and Add or Edit rules for specific applications manually or remove them.

[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

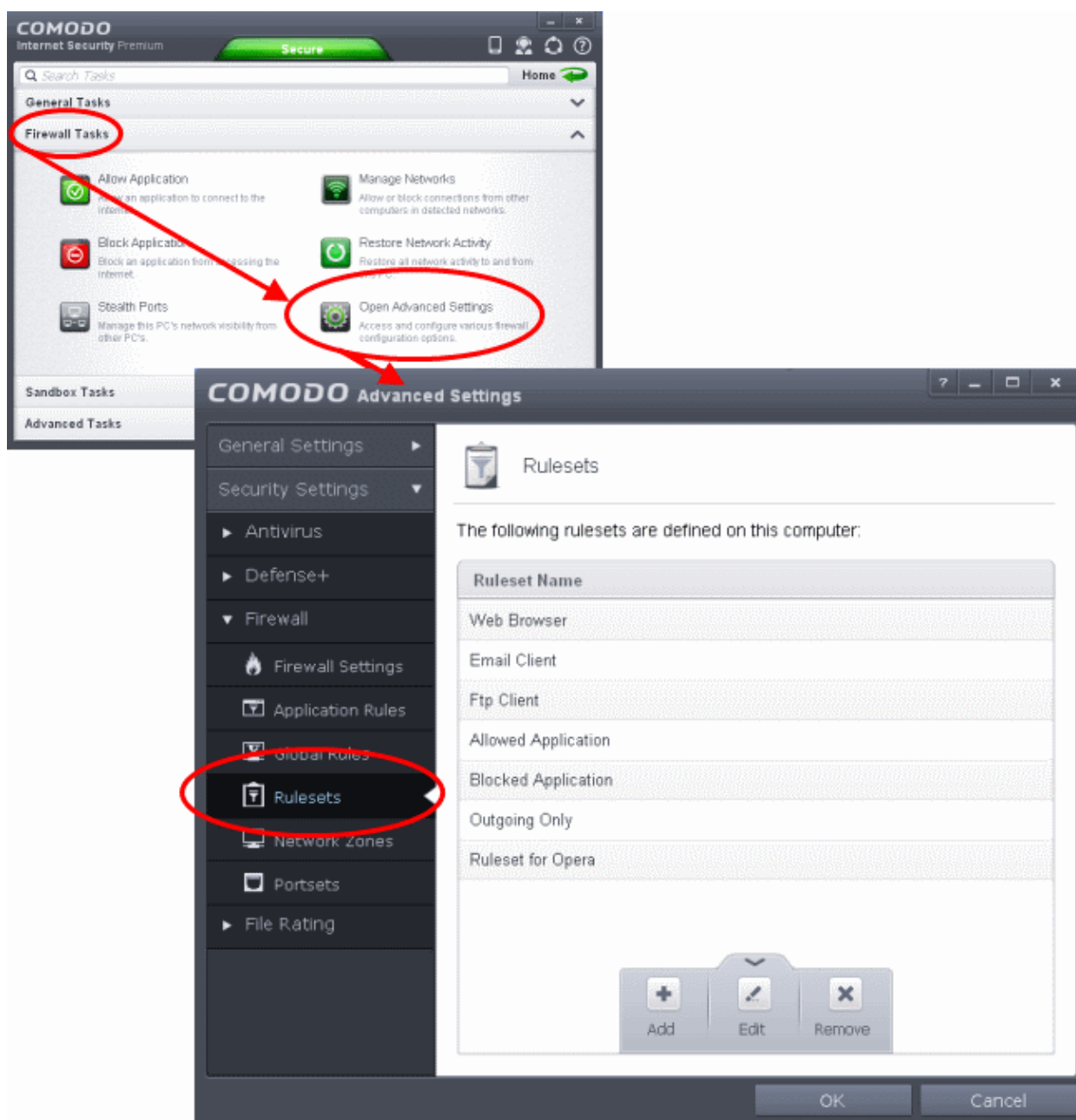


4. Click the handle from the bottom and Add or Edit global rules manually or remove them.

[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 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](#)

Blocking 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:

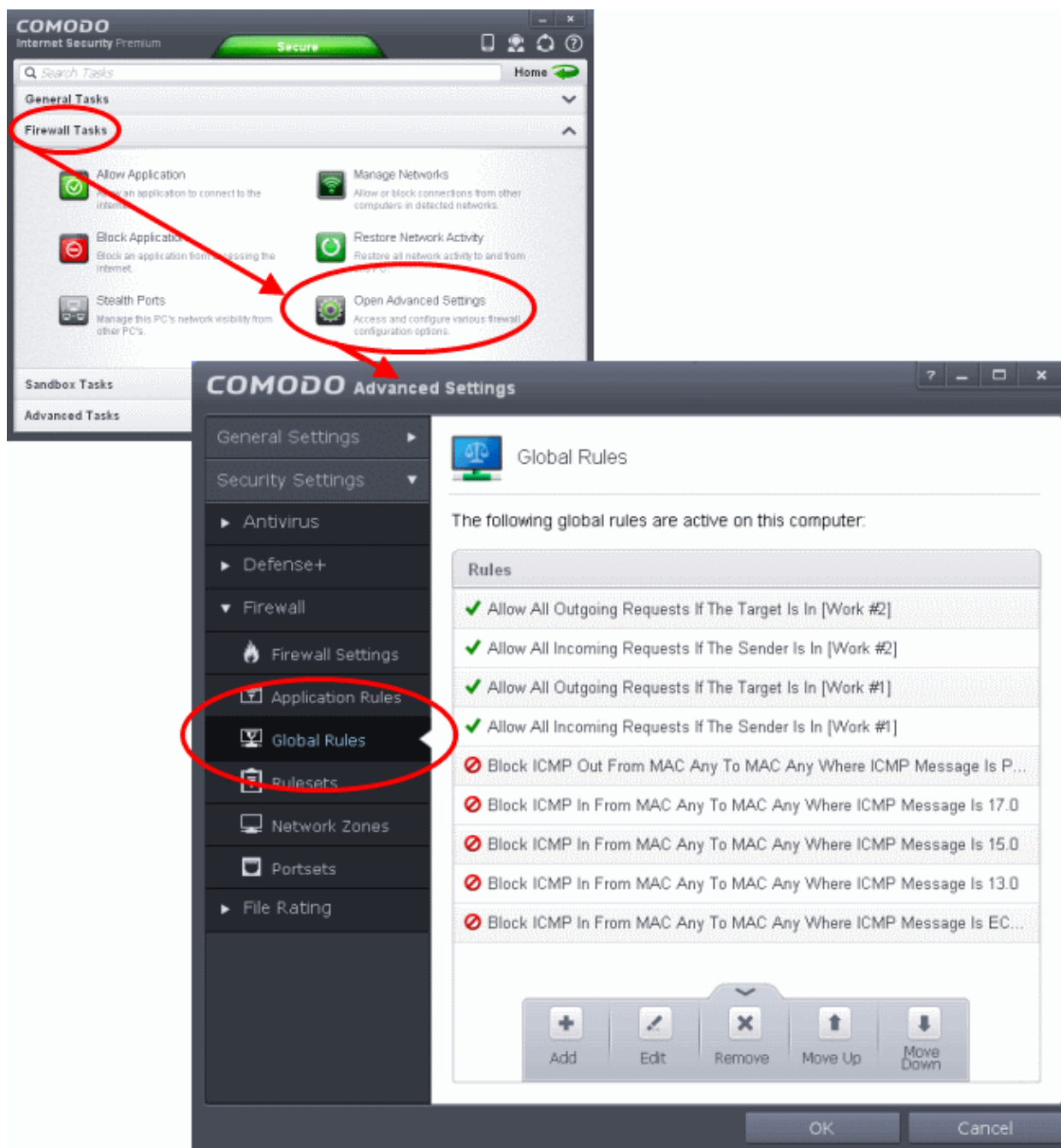
- In your network at home, you want your child's computer to connect to other computers at home but disable Internet access to them for safety reasons
- In your corporate network, you want your employee's computers to connect to your local network machines but disable

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.

COMODO Firewall Rule

Action: Log as firewall event if this rule is fired

Protocol:

Direction:

Description:

Source Address | **Destination Address** | **IP Details**

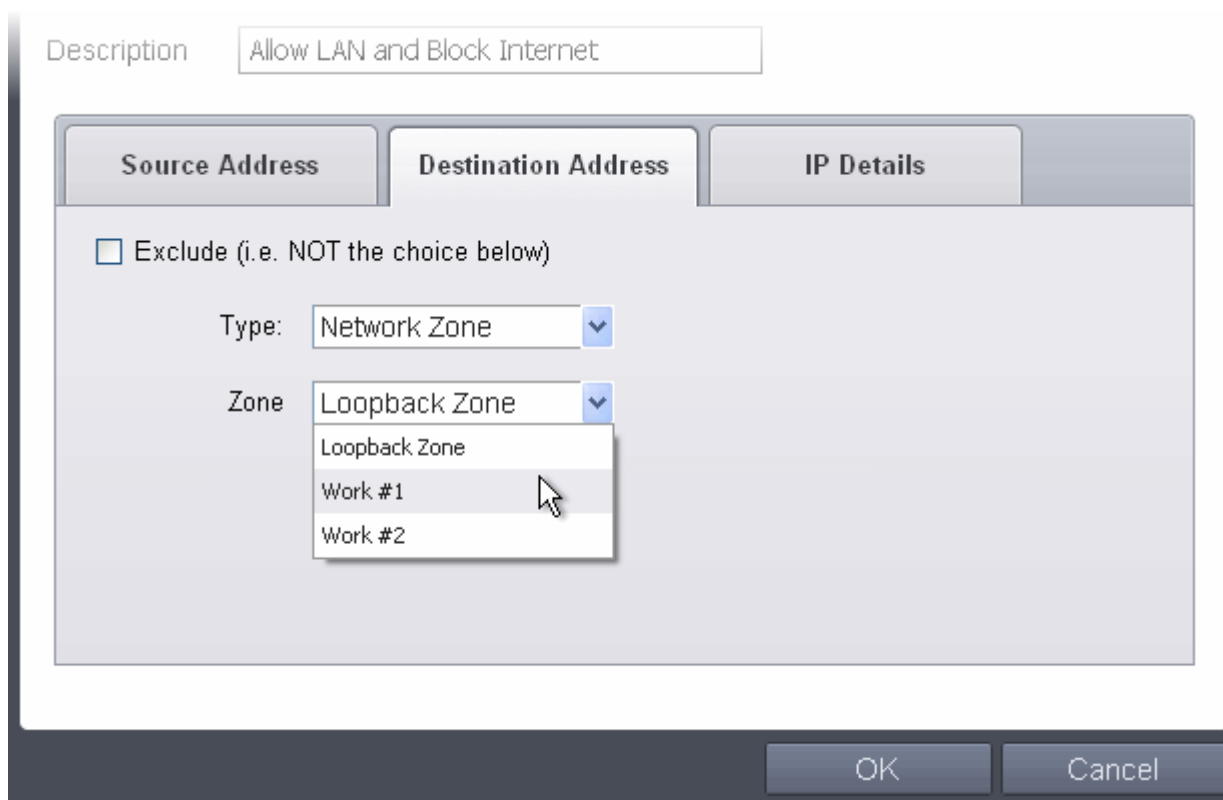
Exclude (i.e. NOT the choice below)

Type:

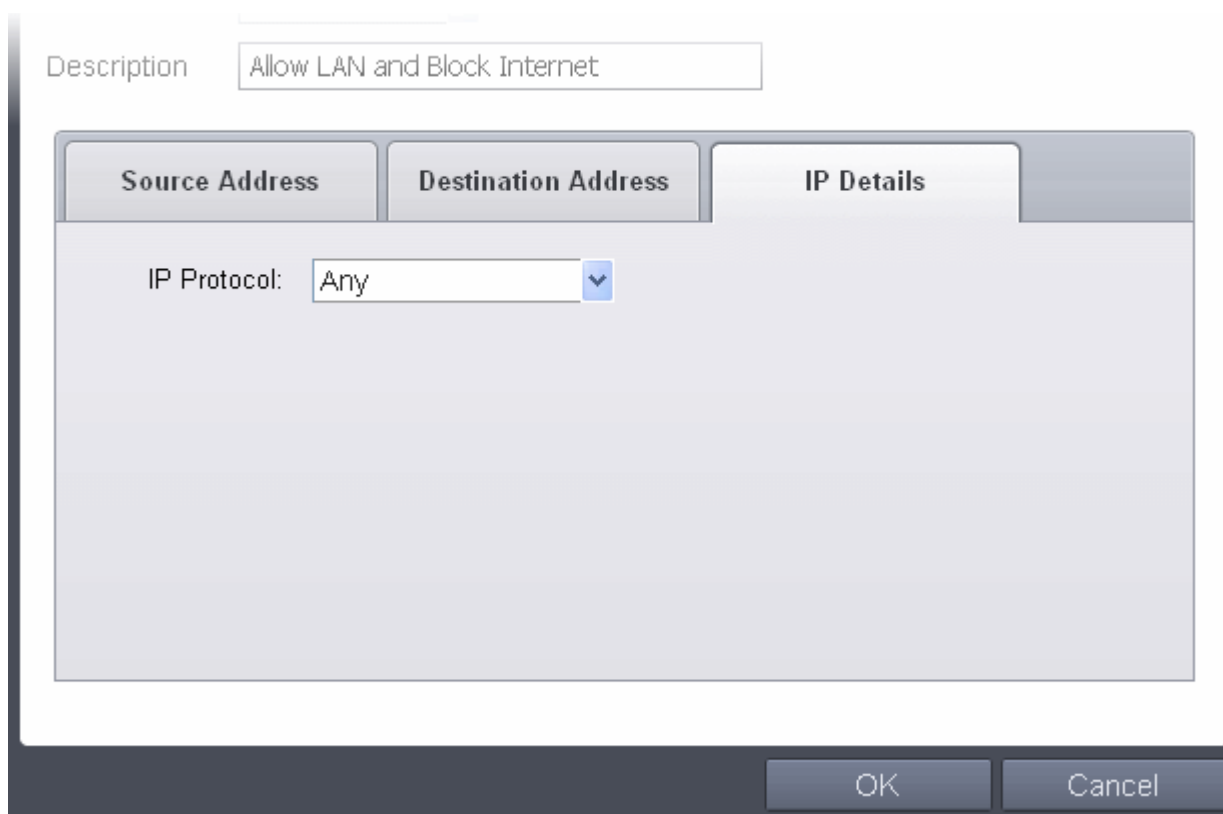
IP:

OK Cancel

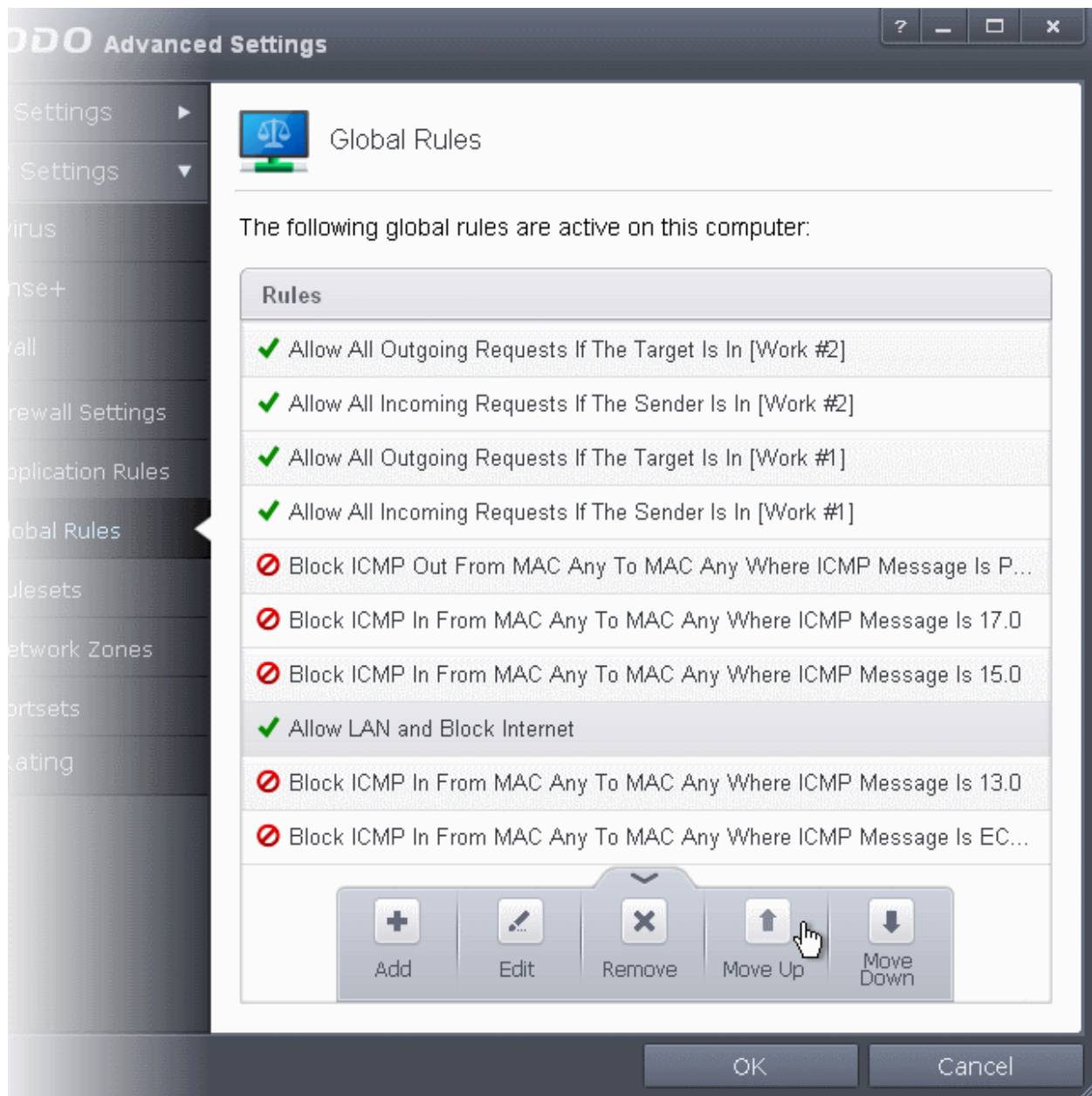
5. Choose the following options from the drop-down menus:
 - Action = Block;
 - Protocol = IP;
 - Direction = Out.
6. Enter a description for the new rule in the Description text box.
7. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network and enter 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.

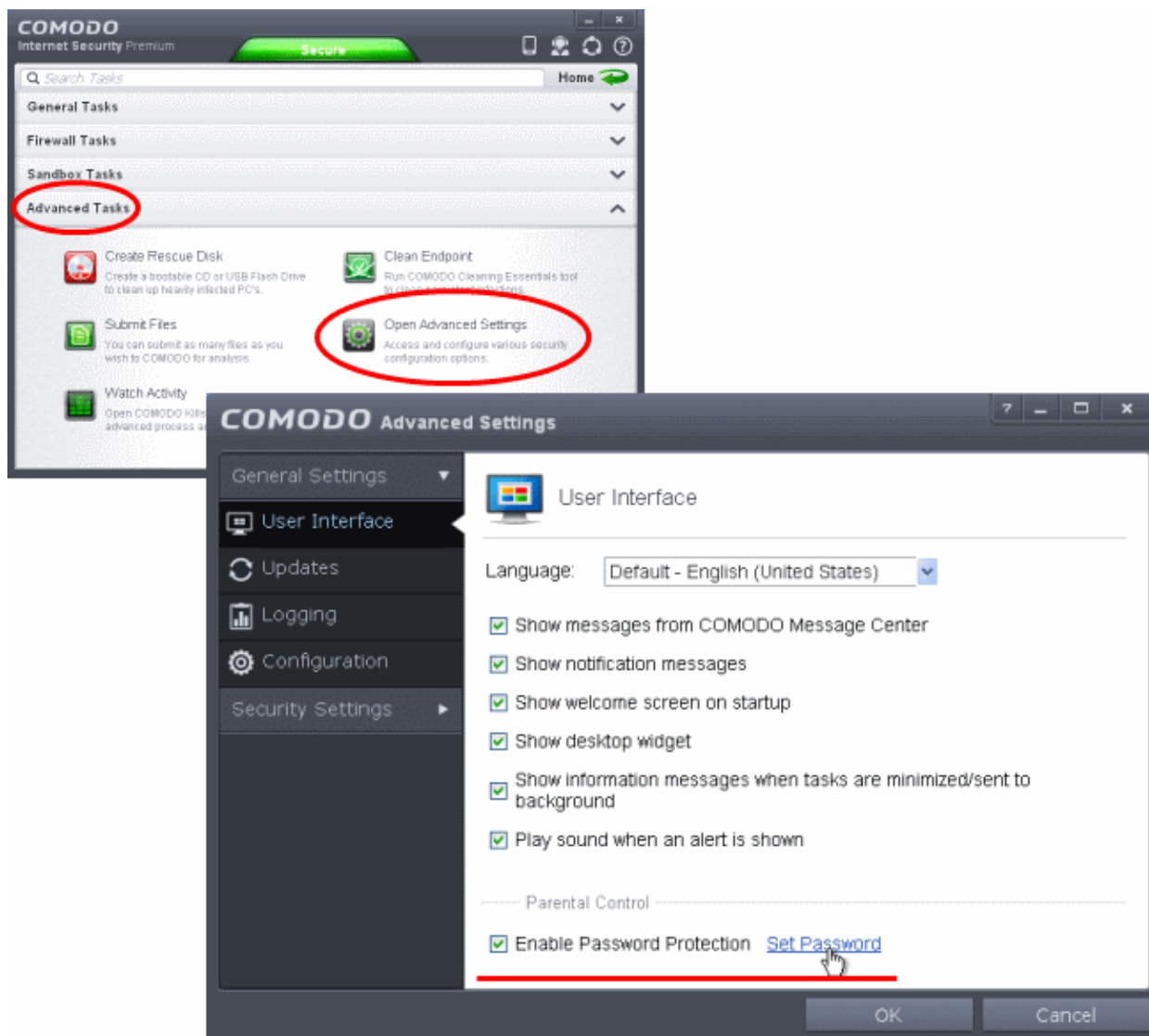


12. Click 'OK' for your configuration to take effect.

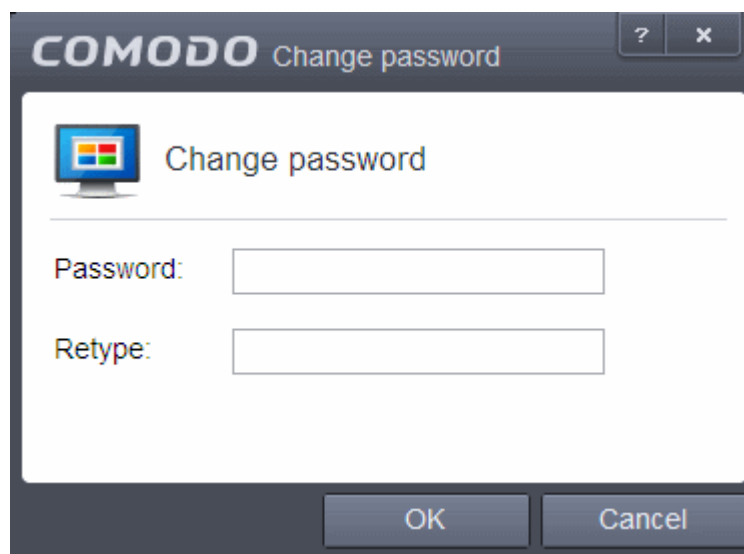
Your Firewall is now configured to allow access to internal network but to block Internet access. Now you need to password protect this configuration to prevent others from changing it.

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



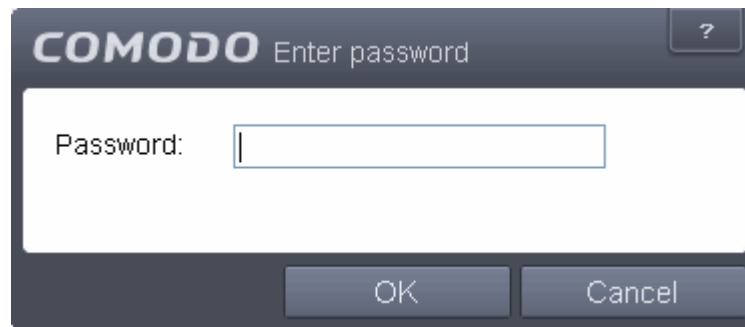
4. Select 'Enable Password Protection' under 'Parental Control' and click 'Set Password' link. The Change password dialog will appear.



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.

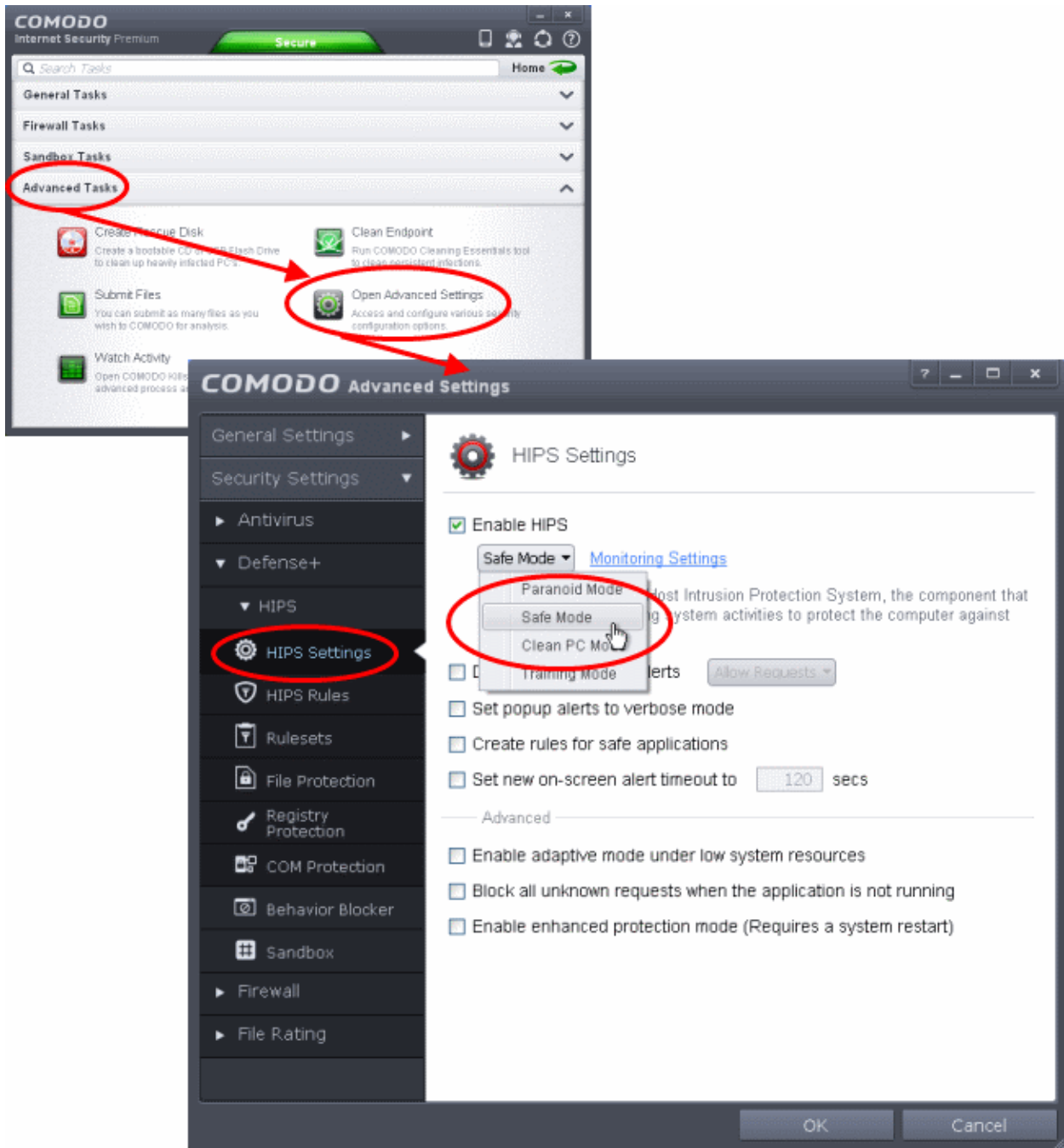


Setting up the HIPS for Maximum Security and Usability

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

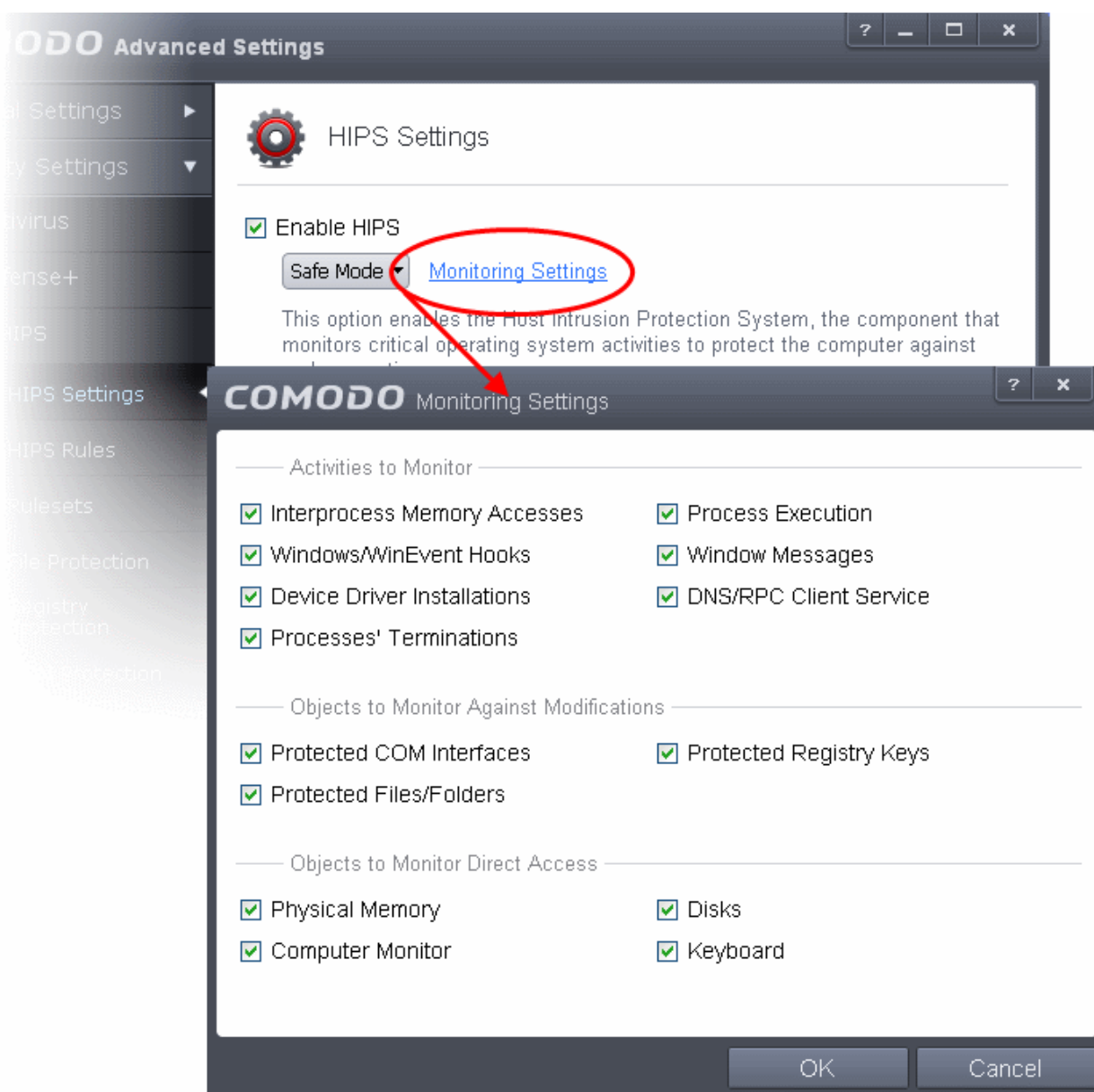
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking 'Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+' > 'HIPS' > 'HIPS Settings' from the left hand side pane



4. Select Enable HIPS
5. Choose 'Safe Mode' from the drop-down below it. Refer to **HIPS Behavior Settings** for more details on the Security Levels.

Monitoring Settings

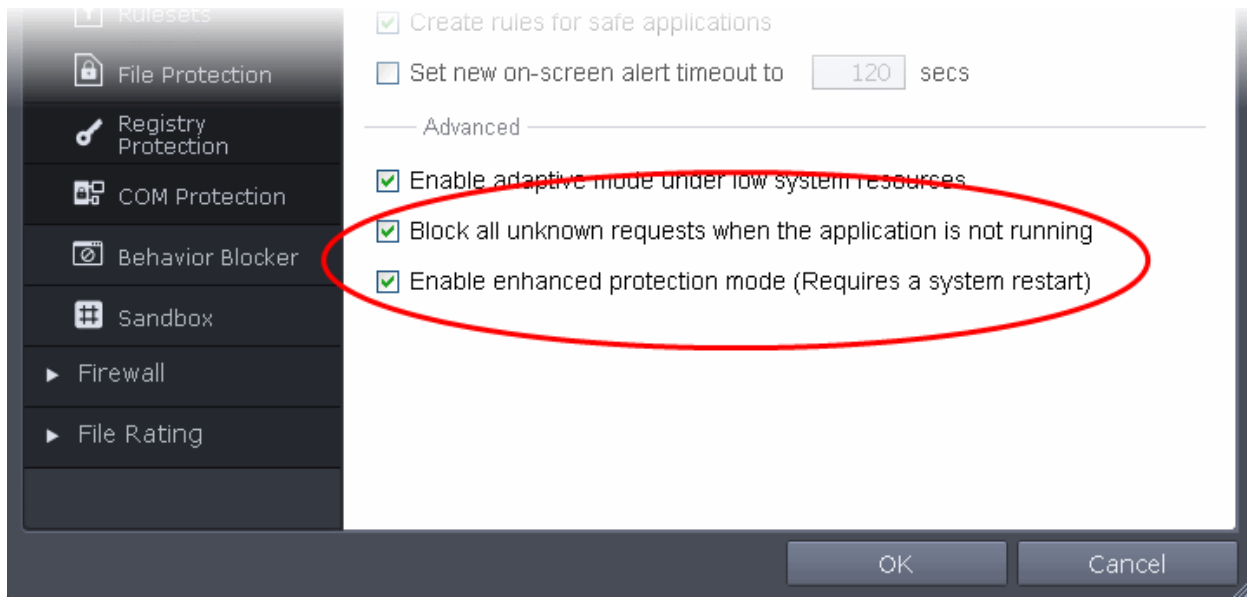
6. Click Monitoring Settings from the HIPS Settings interface



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+.

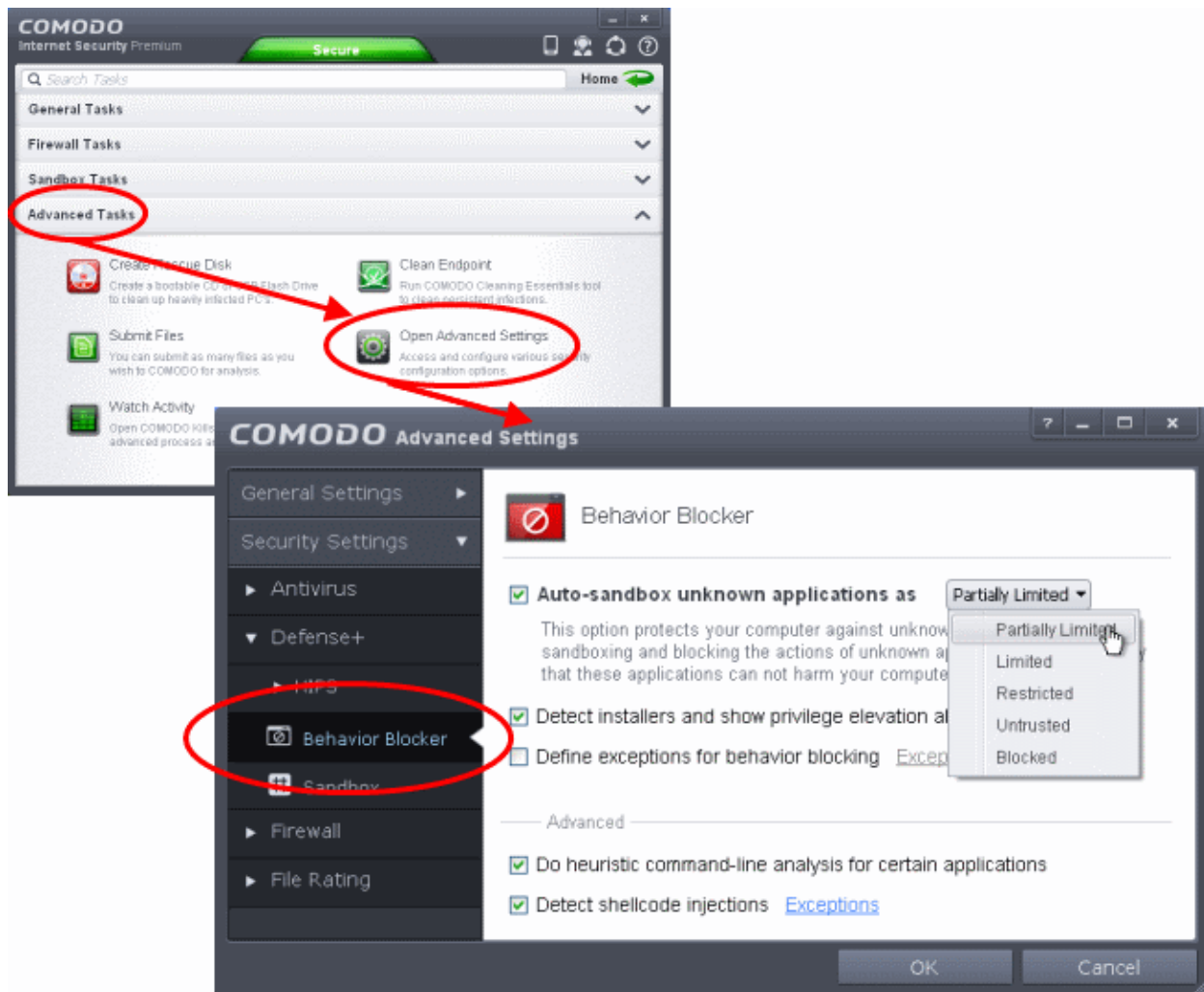
[Click here for more details on HIPS Behavior Settings](#)

Setting up the Behavior Blocker for Maximum Security and Usability

This page explains on configuring the Behavior Blocker to auto-sandbox applications that are unrecognized by CIS to prevent potential damages to your system from untrusted programs.

To configure Behavior Blocker

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+' > 'Behavior Blocker' from the left hand side pane



4. Make sure that the check box 'Auto-sandbox unknown applications as' is selected and choose 'Partially Limited' from the drop-down menu.

Advanced Settings

5. Make sure that both the check boxes:
 - Do heuristic command-line analysis for certain applications;
 - Detect shellcode injections
 ... are selected.

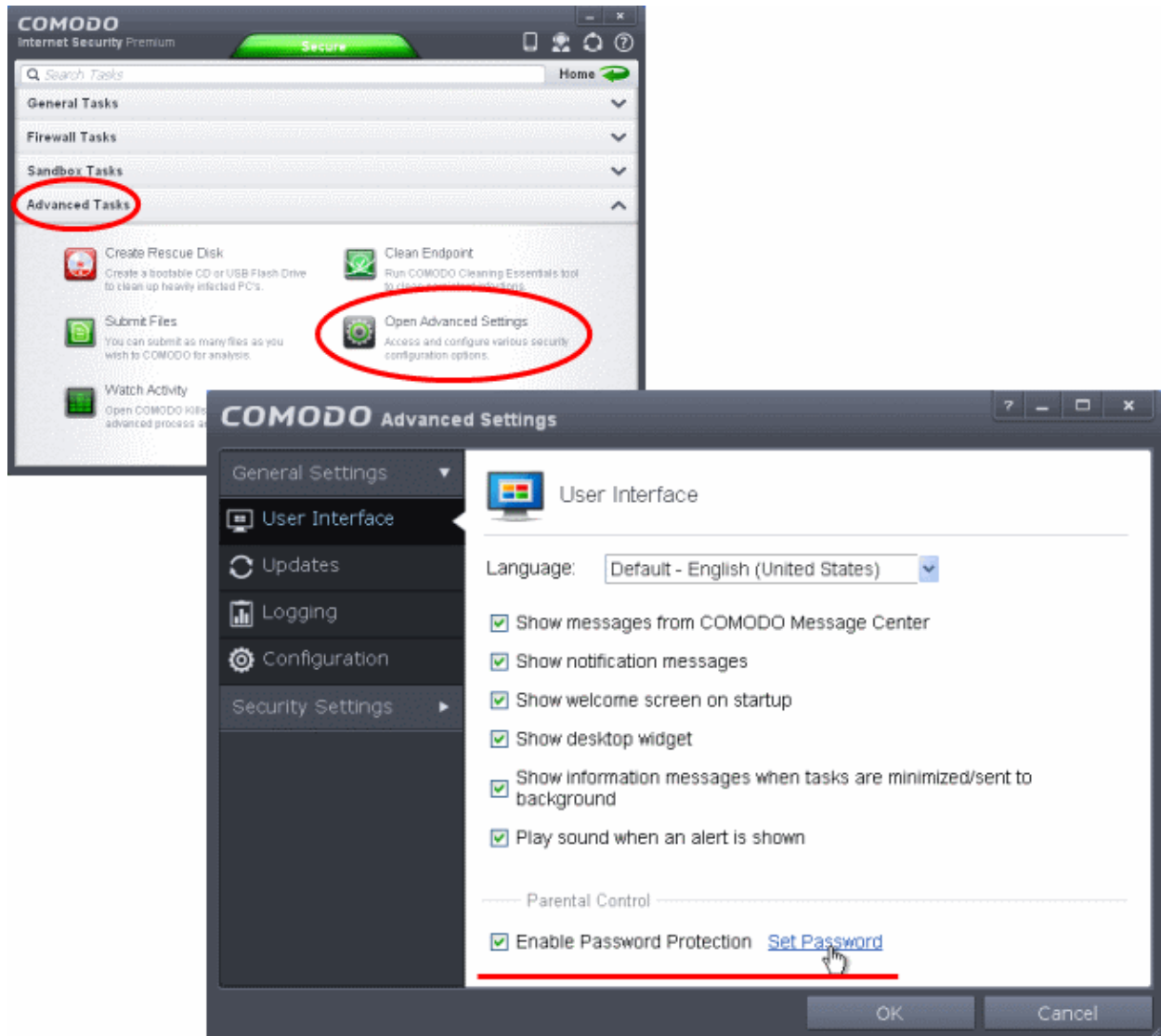
[Click here for more details on Behavior Blocker Settings](#)

Password Protect Your CIS Settings

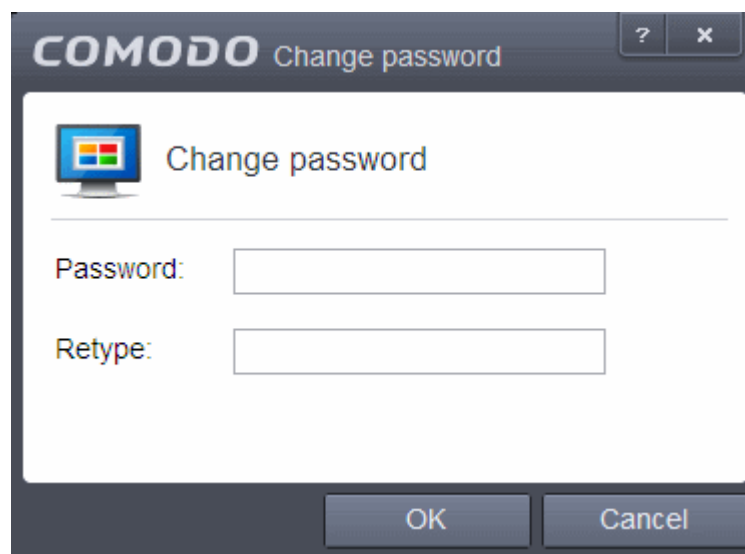
This page explains how to password protect access to the CIS interface. Implementing the steps explained on this page means another user will not be able to access the CIS interface to modify or over-ride the security settings you have implemented.

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



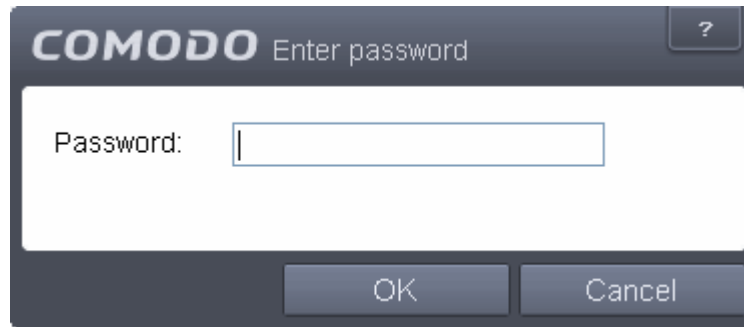
4. Select 'Enable Password Protection' under 'Parental Control' and click 'Set Password' link. The Change password dialog will appear.



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.



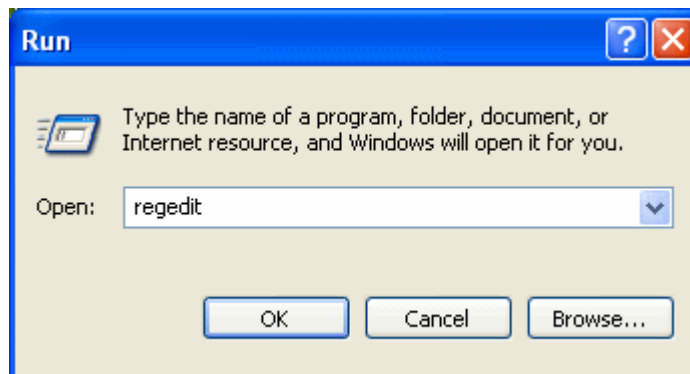
Reset Forgotten Password (Advanced)

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.

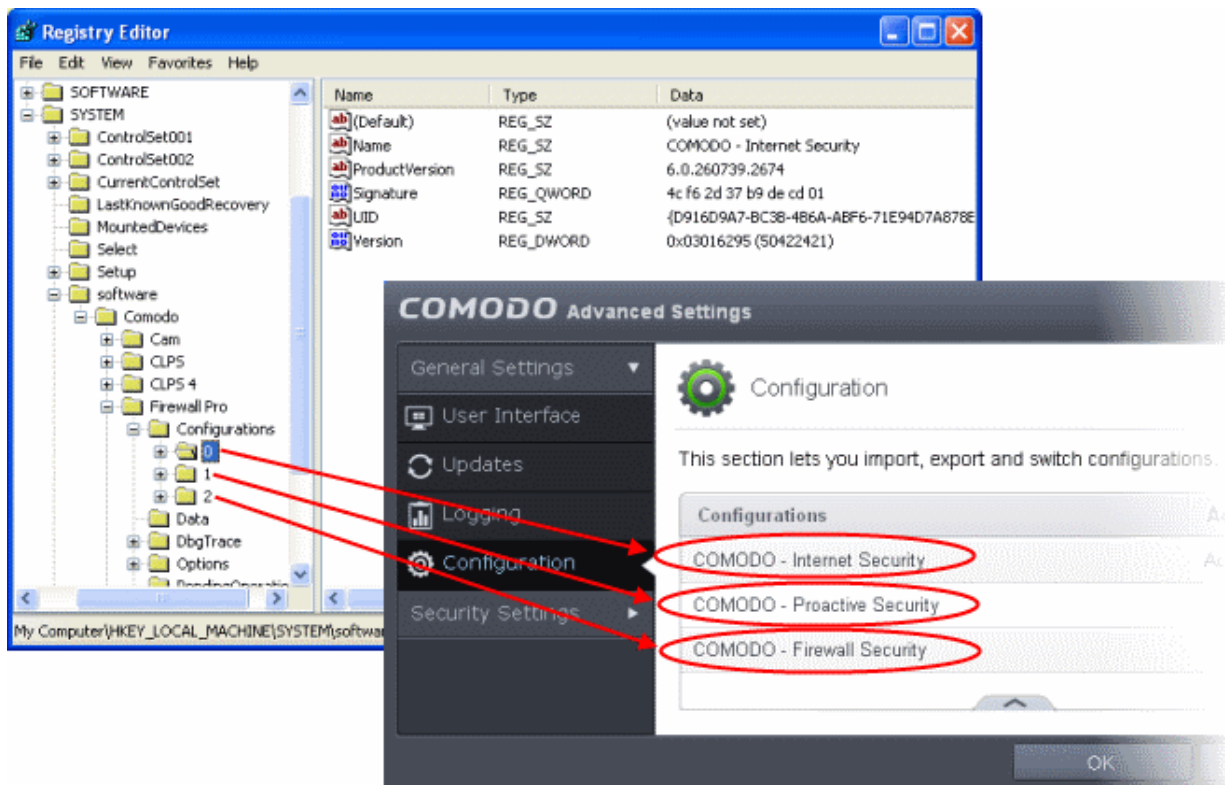
To disable password protection in CIS

1. Click Start > Run, from the Windows Start menu
2. Type 'regedit' in the text box and click 'OK'

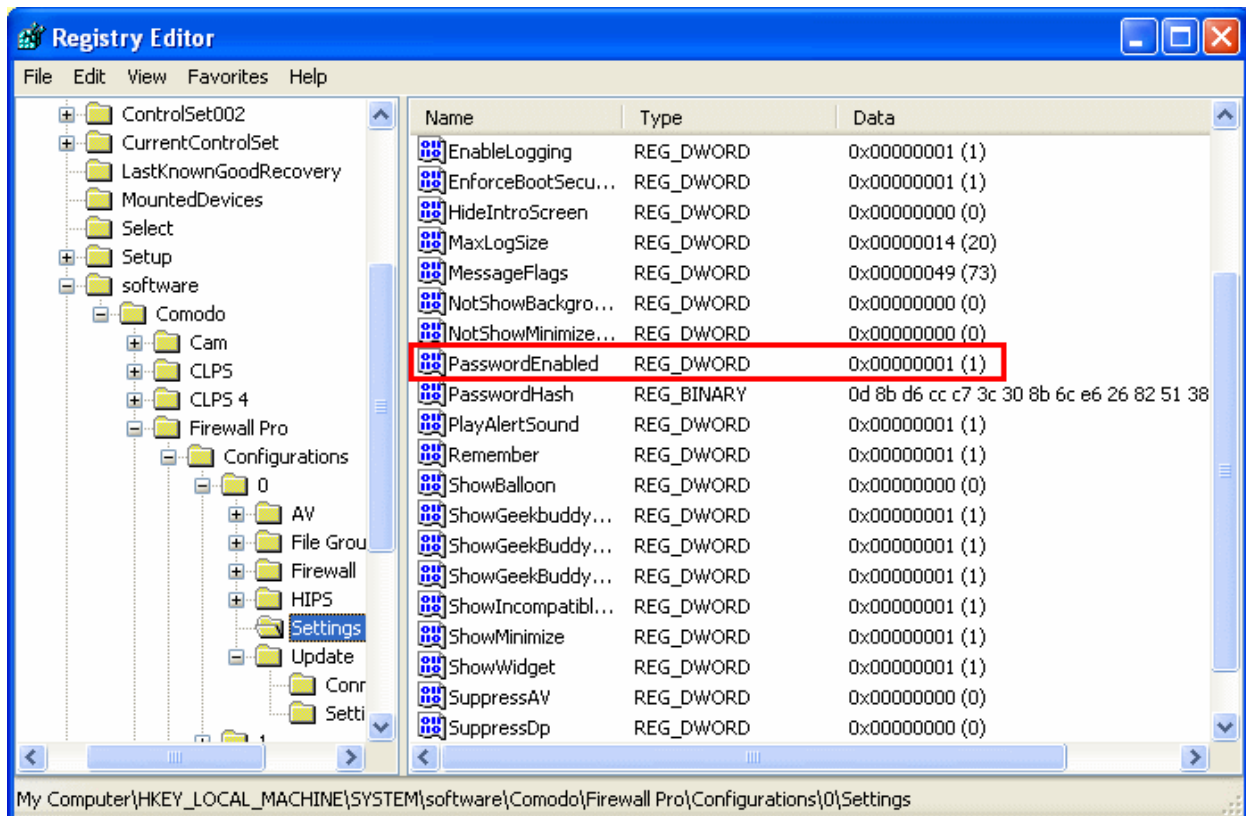


3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\

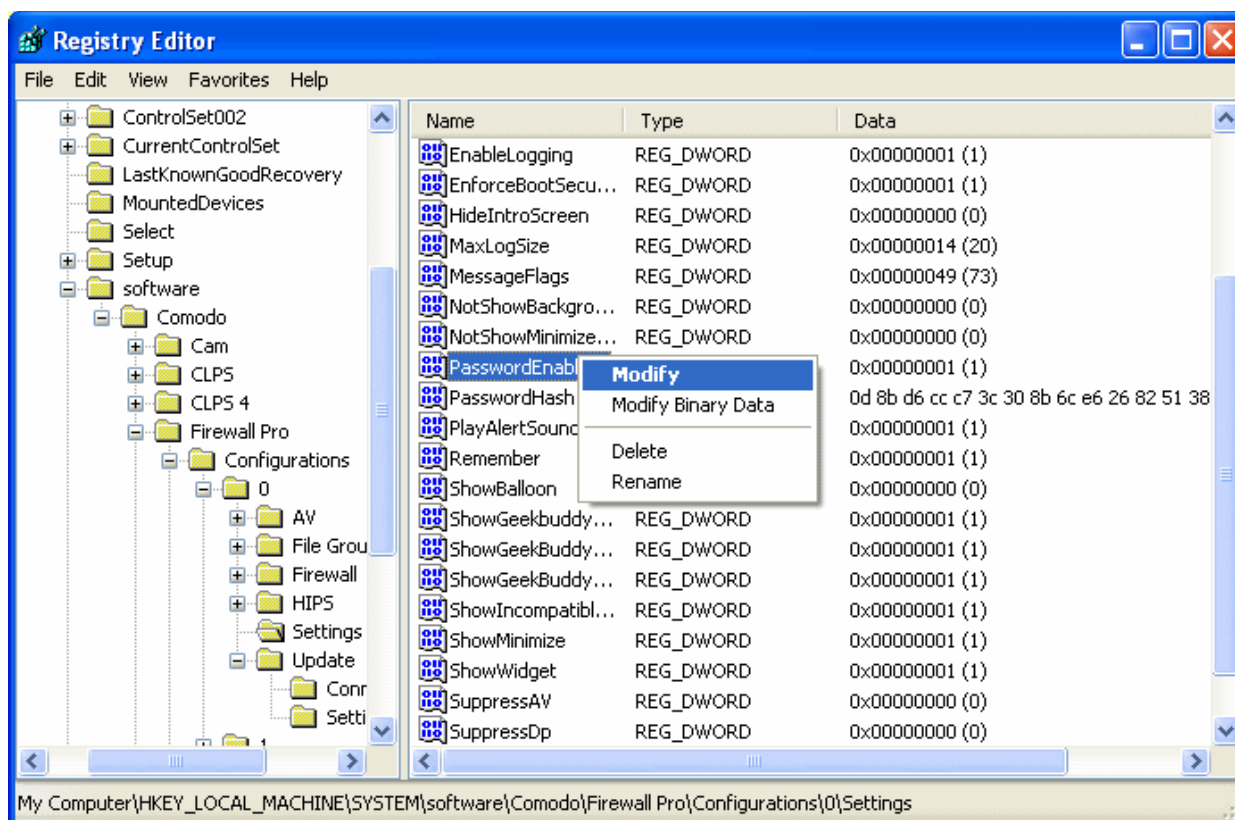
Under the Configurations folder you will see sub-folders named 0,1,2,... depending on the number of preset configurations in CIS. These folders contain registry keys for the settings of the preset configurations in the order of the configurations displayed in **Advanced Settings > General Settings > 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.



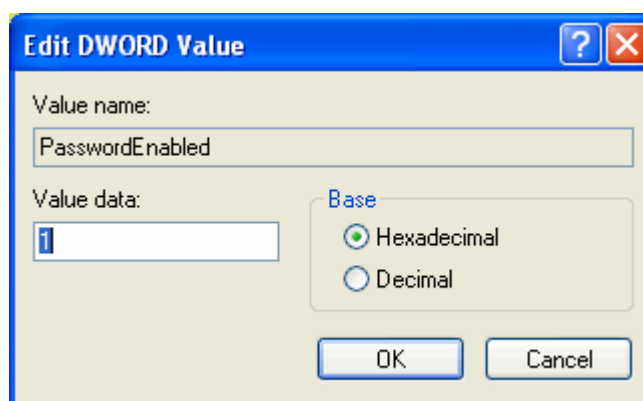
4. Select the folder corresponding to the configuration for which you wish to reset the password and navigate to Settings, for example, navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\0\Settings to reset password in COMODO - Internet Security configuration.



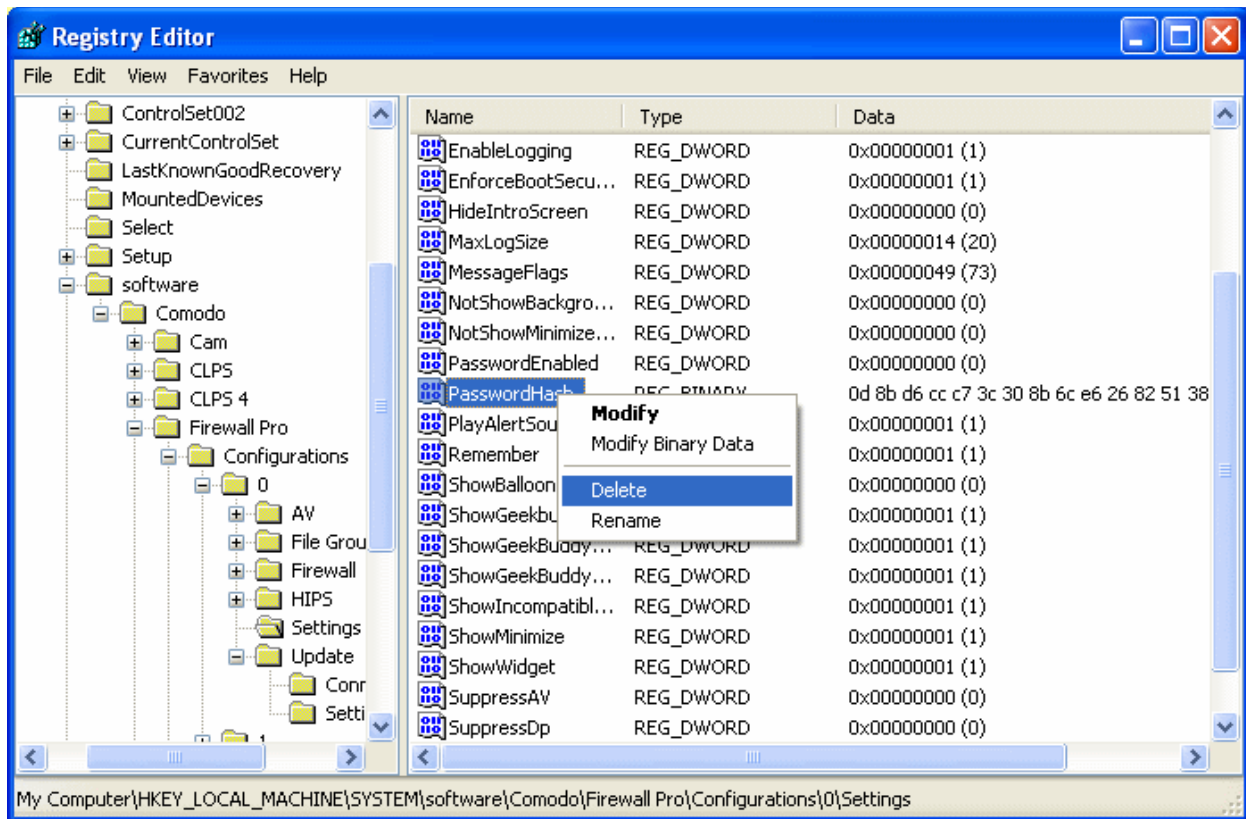
5. Right-click 'PasswordEnabled' key and select 'Modify'



- In the 'Edit DWORD Value' dialog box, change the 'Value data' from 1 to 0



- Click 'OK'
- Right-click 'PasswordHash' and select 'Delete'.



- 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.

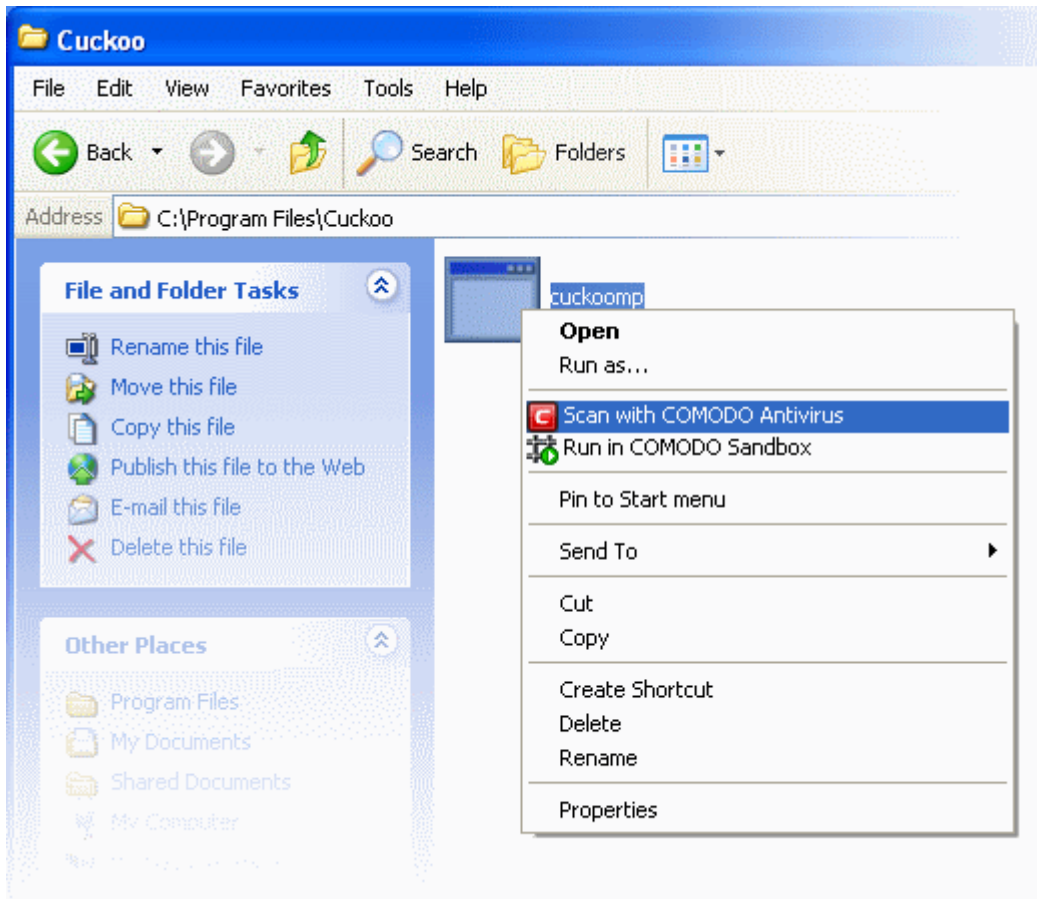
Running an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders files etc. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives, digital cameras - even your iPod and mobile phones too!!! This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from the Internet.

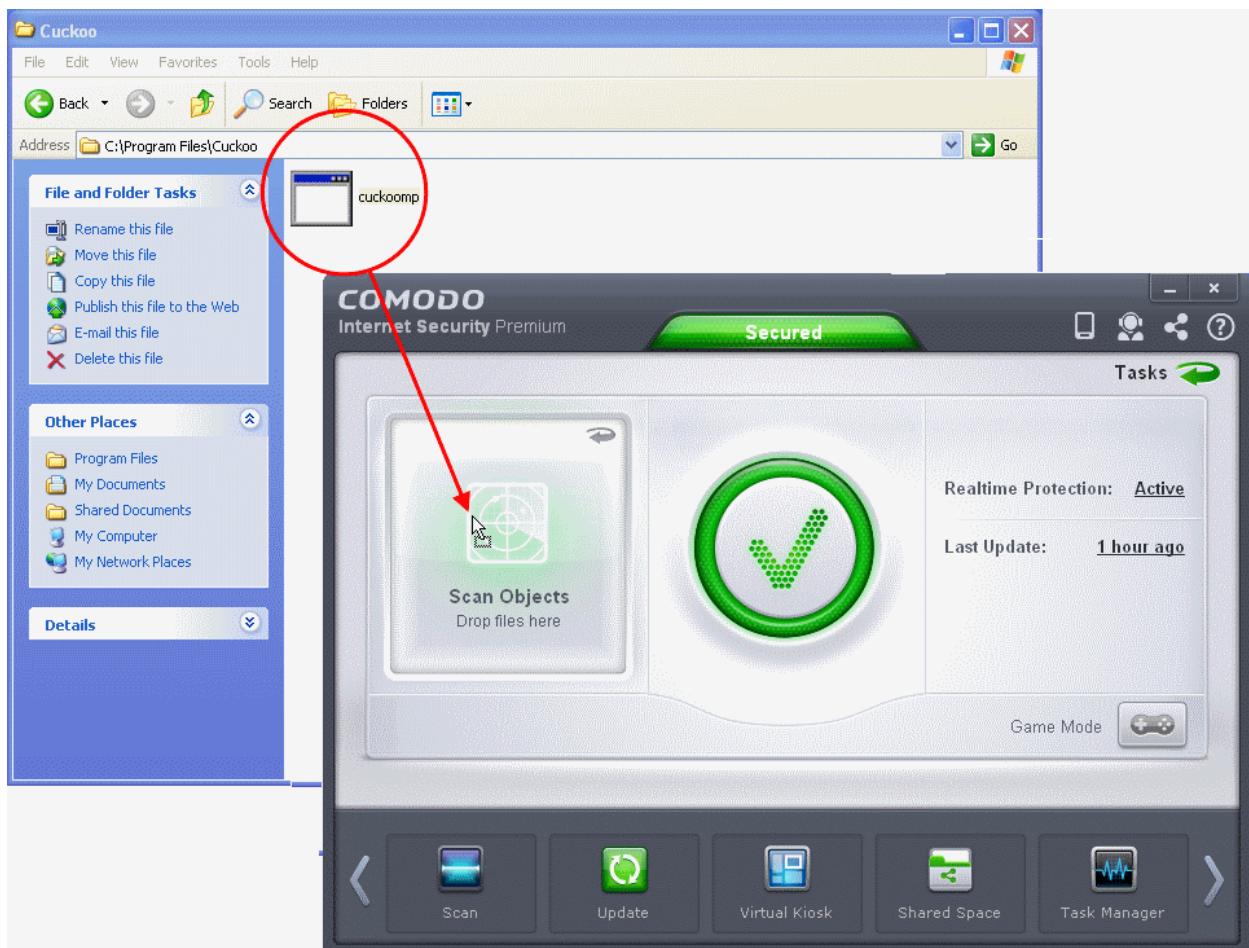
[Click here](#) for more details on running on-demand scans.

To instantly scan an item

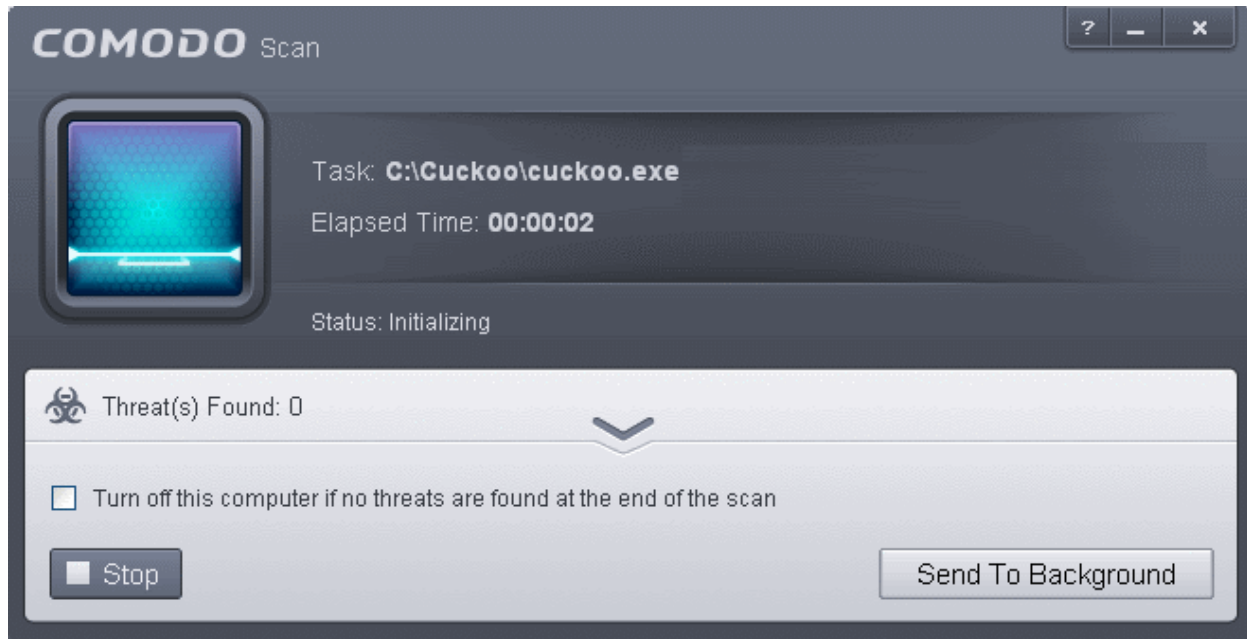
- Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



- Alternatively drag and drop the item over the area marked 'Scan Objects' in the 'Home' screen of the 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.

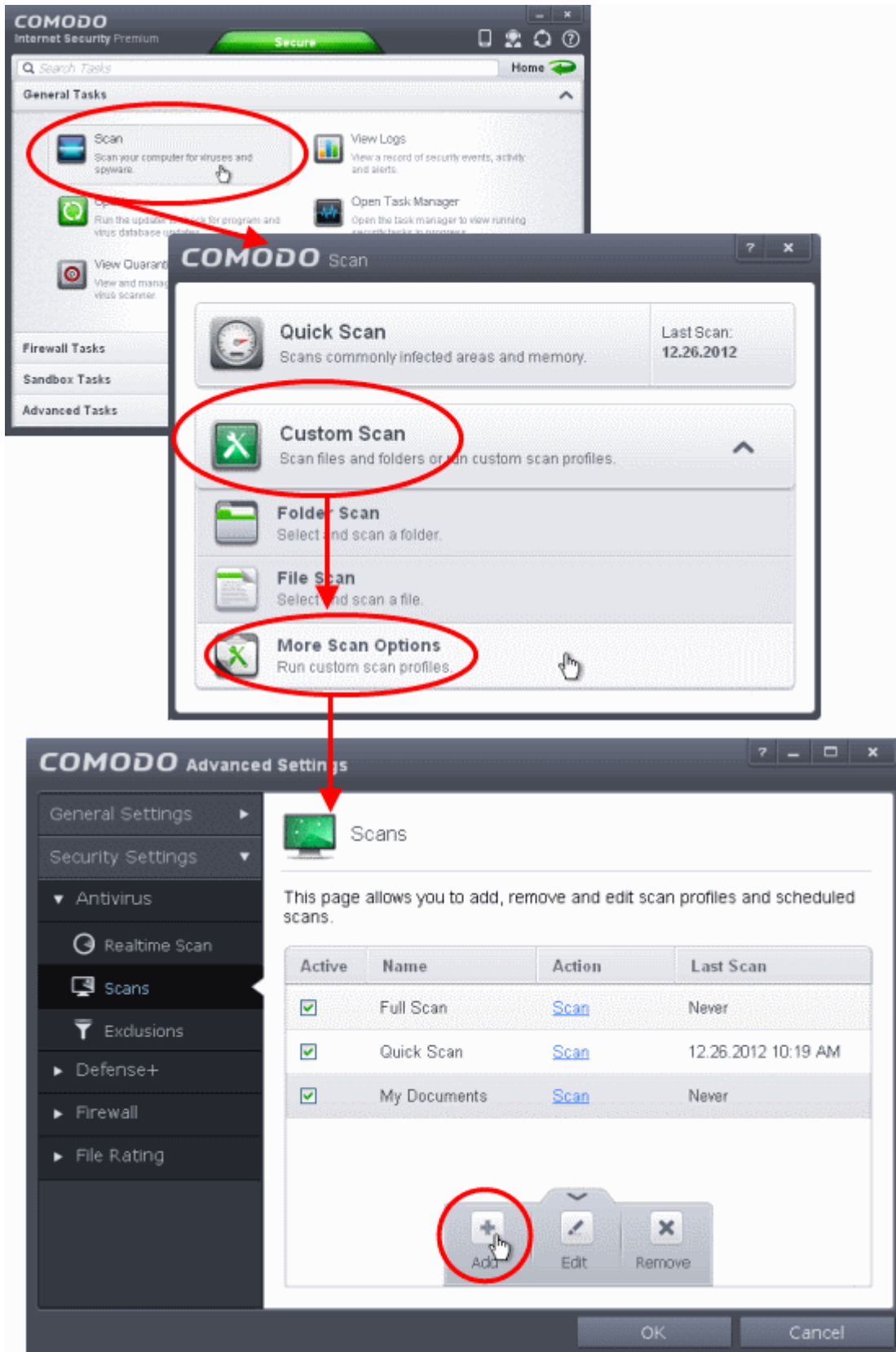
[Click here](#) for more details to take action on the infected item(s).

Creating 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.

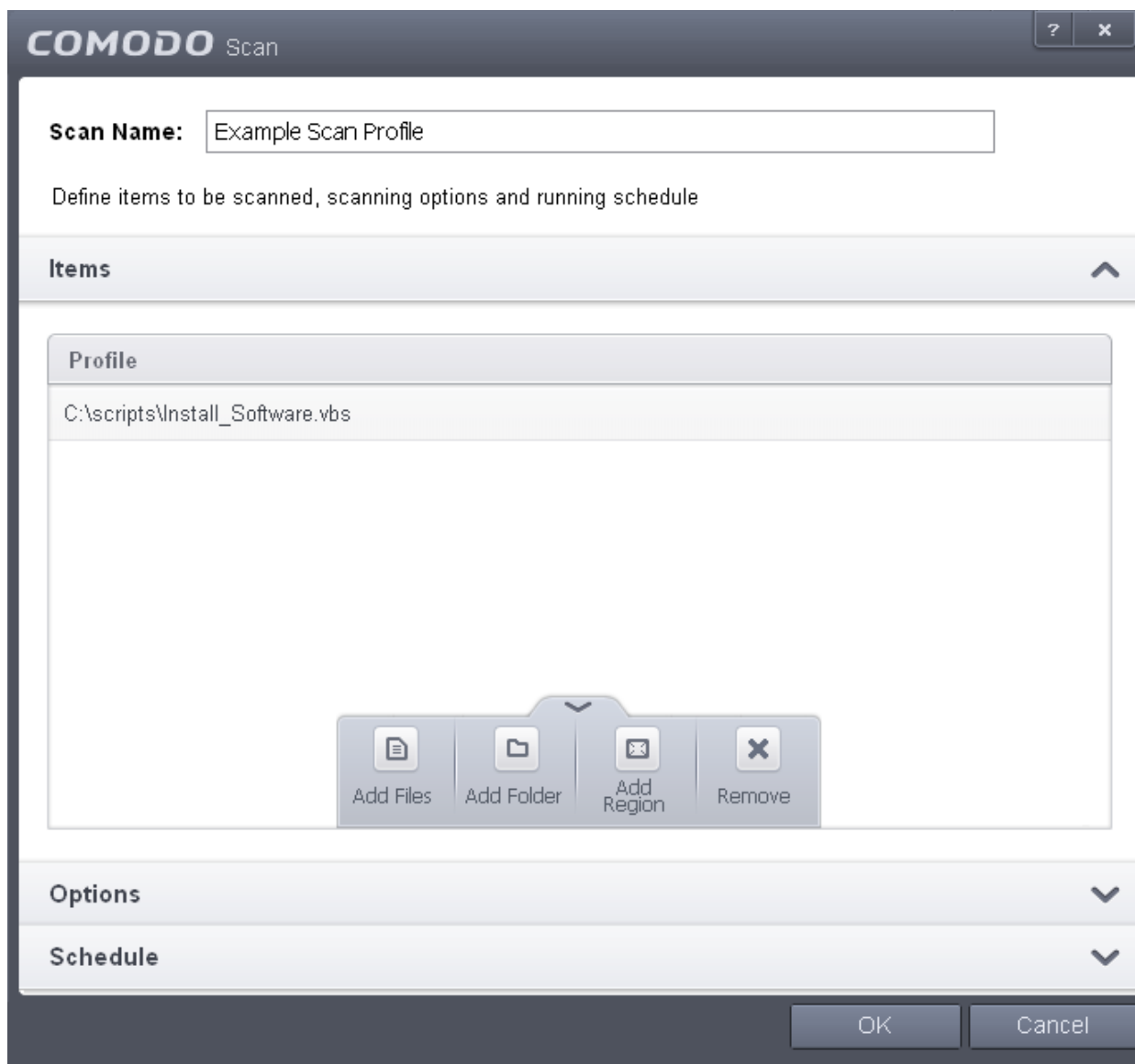
To create an antivirus scanning schedule

- 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'

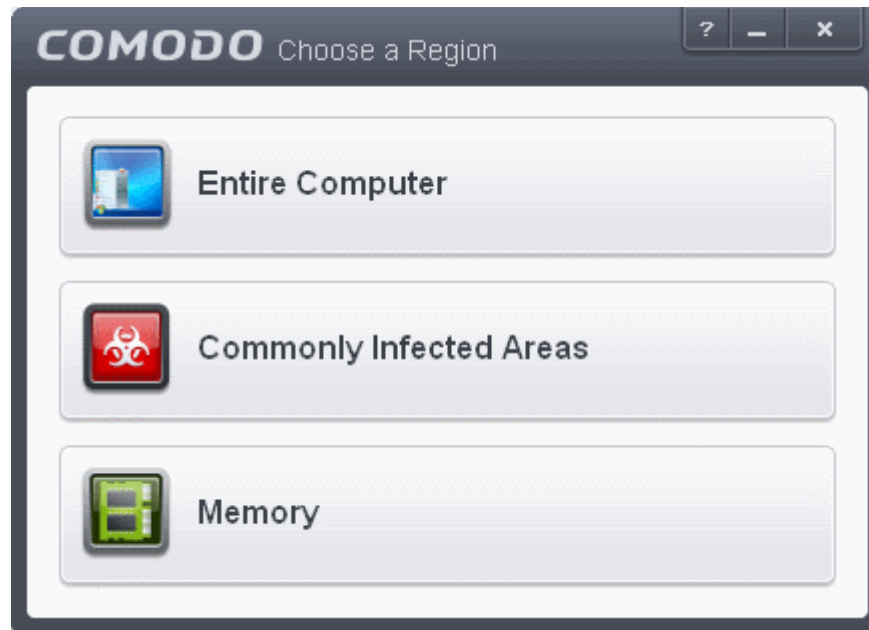


The scan profile interface will be displayed.

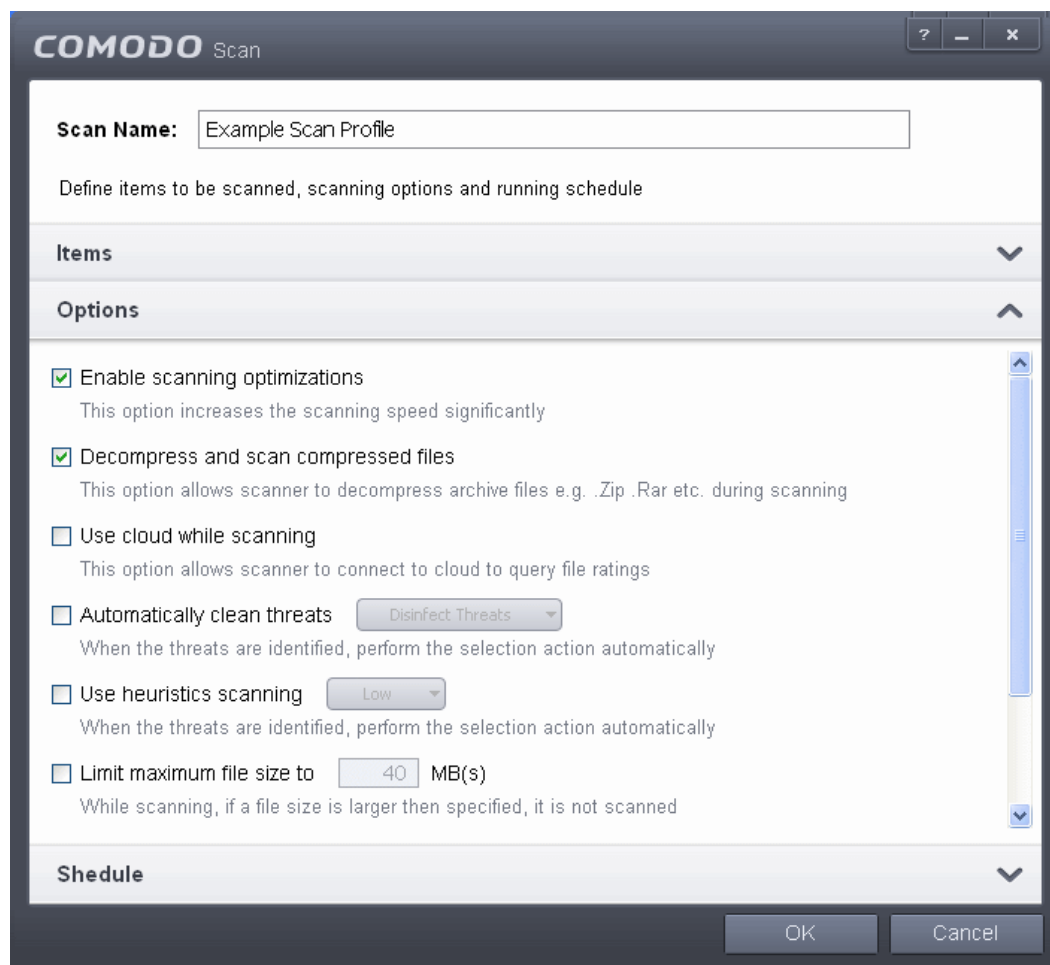
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



- **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:



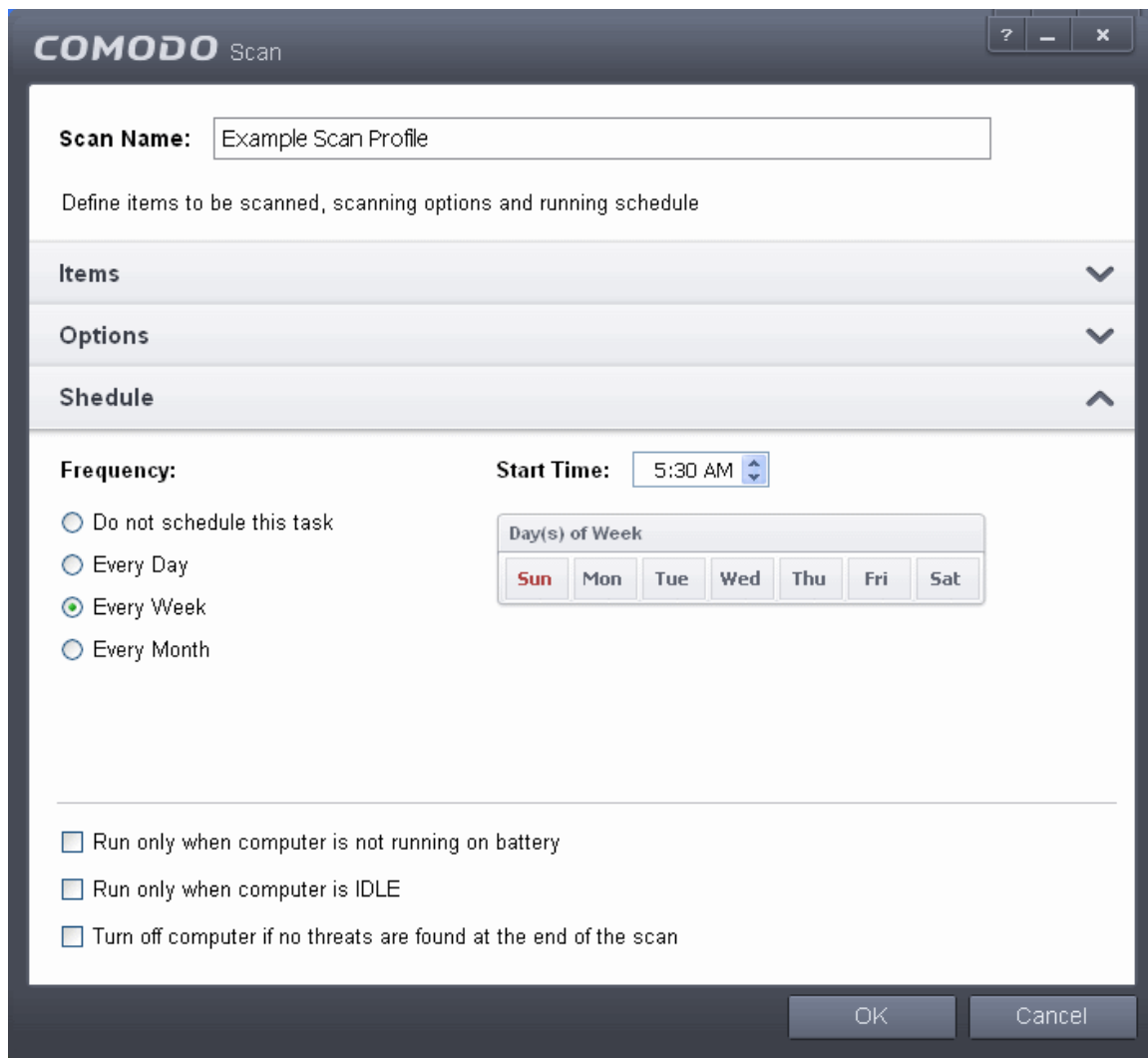
- **Options:**
 - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process (**Default = Enabled**).

- **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 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.
- **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*).
- 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 Antivirus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
- **Every Week** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - The Antivirus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
- **Run only when computer id IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.
- Click OK to save the profile.

The profile will be saved and the selected areas will be scanned repeatedly as per the set schedule.

Running 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 how a 'virtual' shortcut will appear on your desktop:



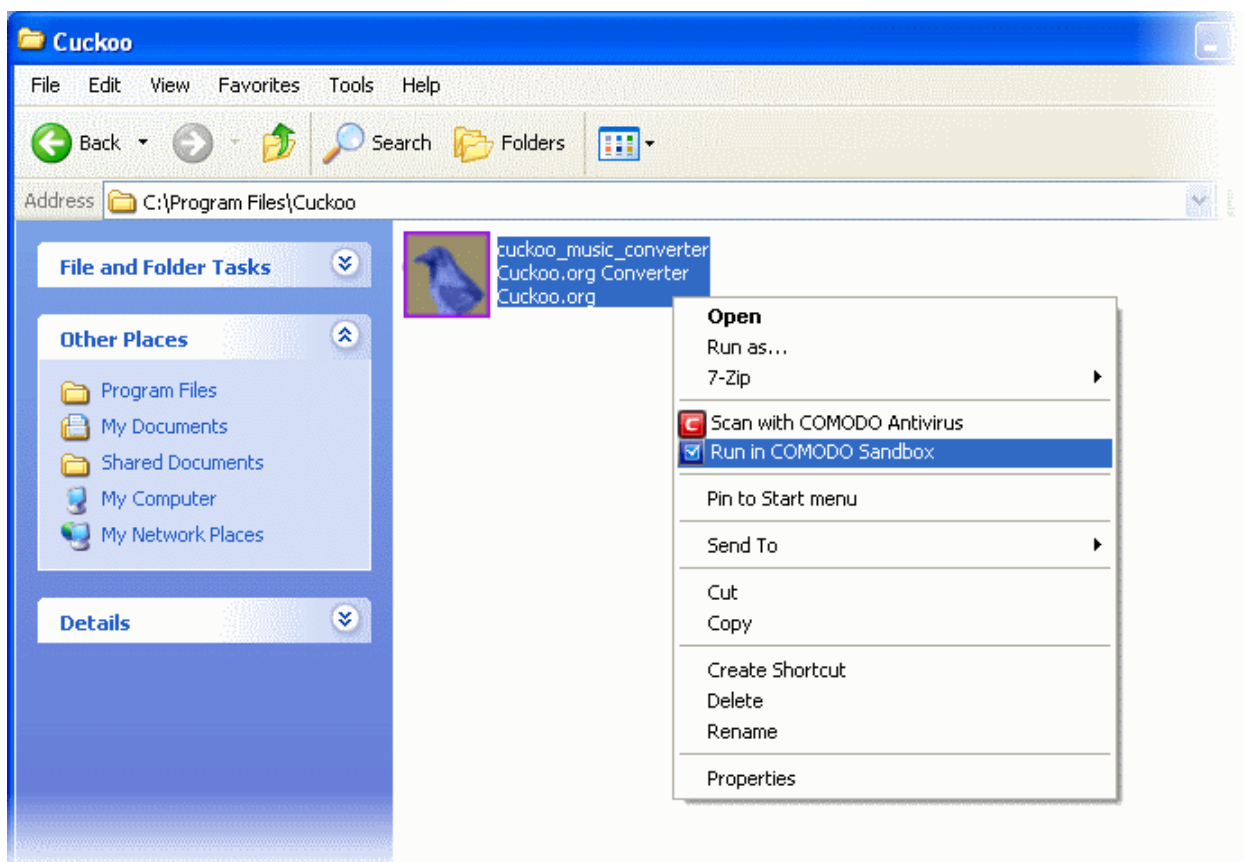
Comodo Internet Security allows you to run a program in the sandbox:

- **From the right click options**
- **By dragging-and-dropping the application on to CIS Home screen**
- **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

Drag-and-drop the application on to CIS Home Screen

The Home screen of the CIS interface has a flippable pane at the left side allowing you to run instant scans or run a program in sandbox. To flip the pane to carry out these tasks, just click the curved arrow at the top right side of the pane.

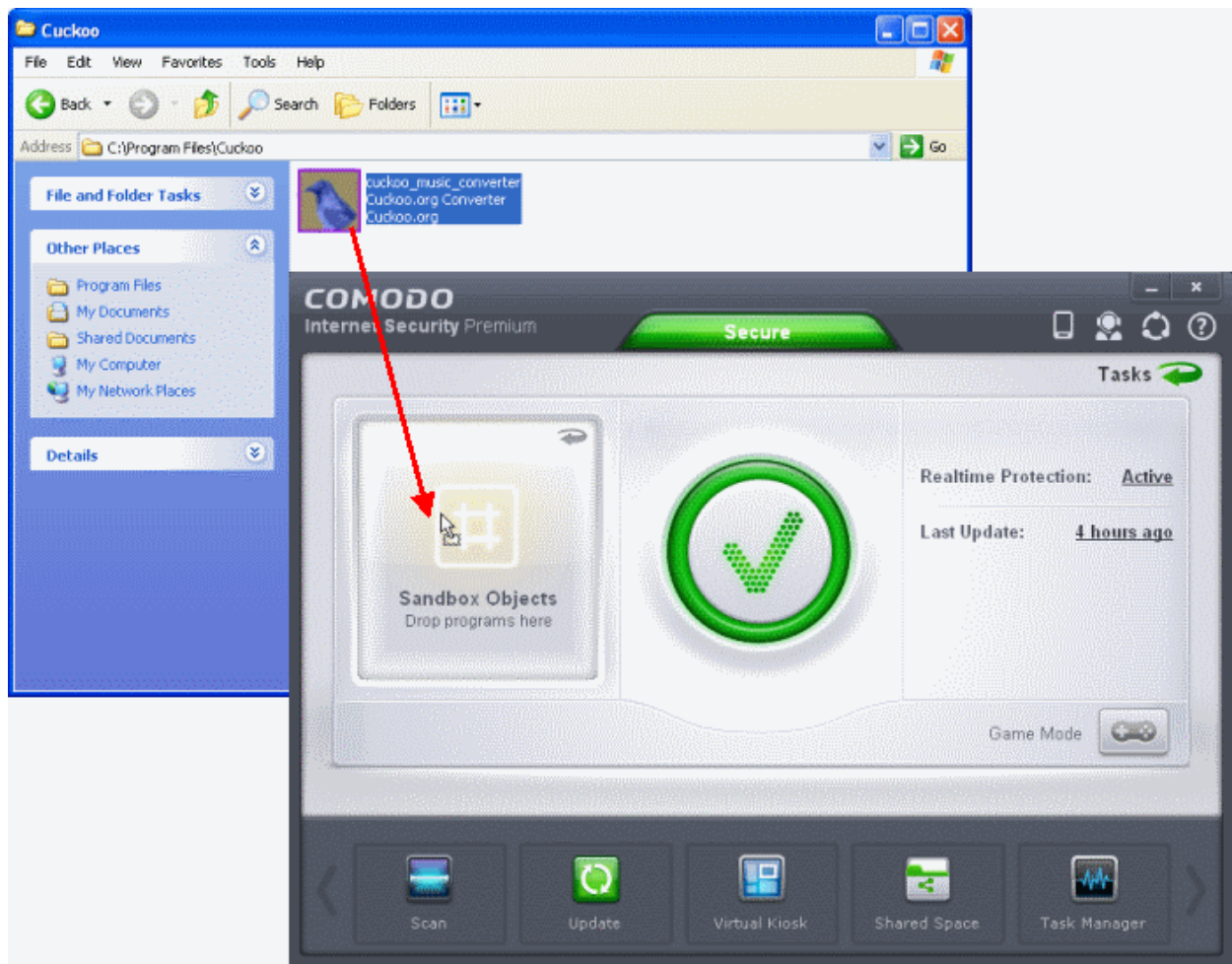


To run a program in a sandbox

1. Flip the pane by clicking the curved arrow at the top right side to display 'Sandbox Objects'.

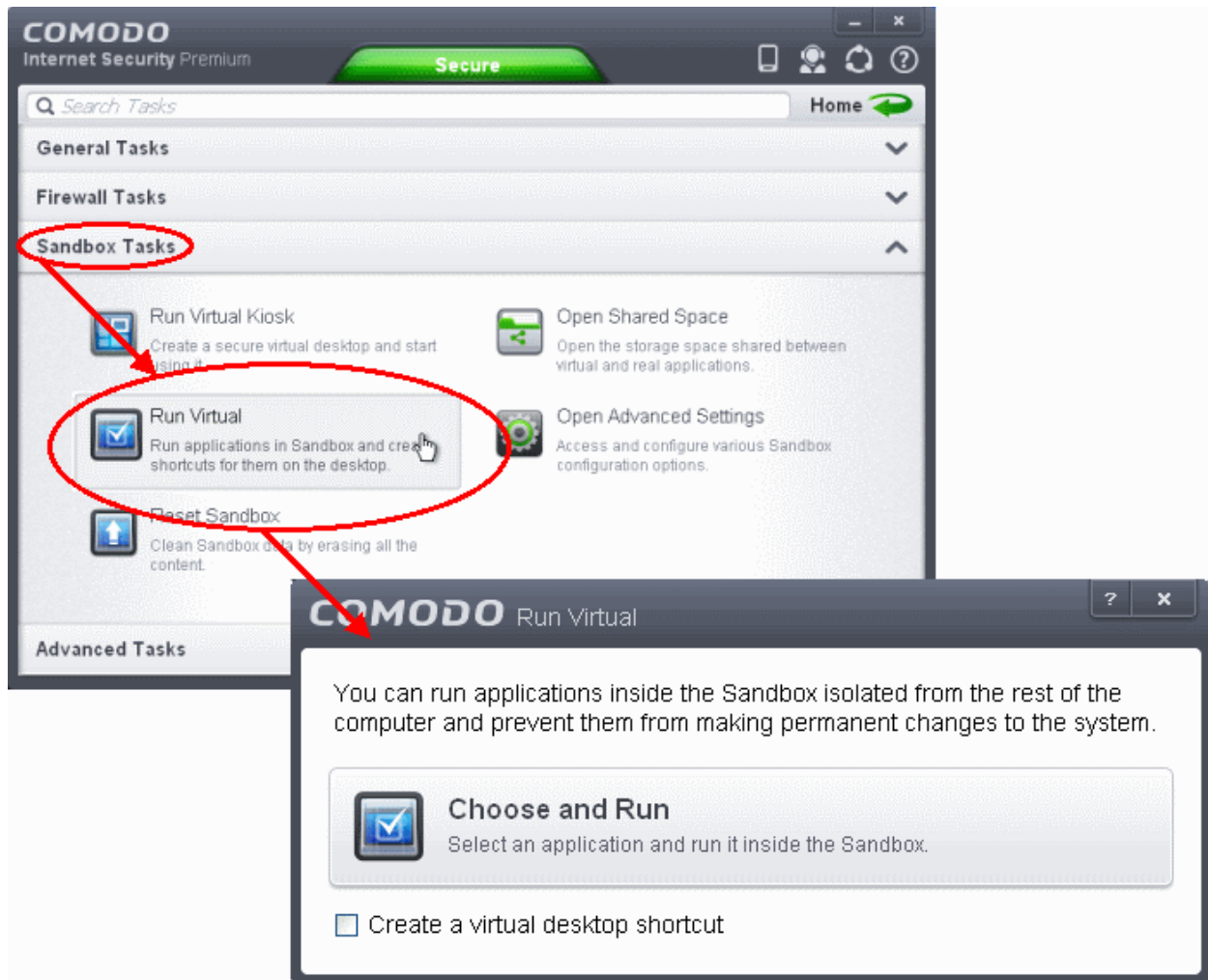


2. Navigate to the program in your system that you want to run in sandboxed environment through Windows Explorer and just drag and drop into the box.



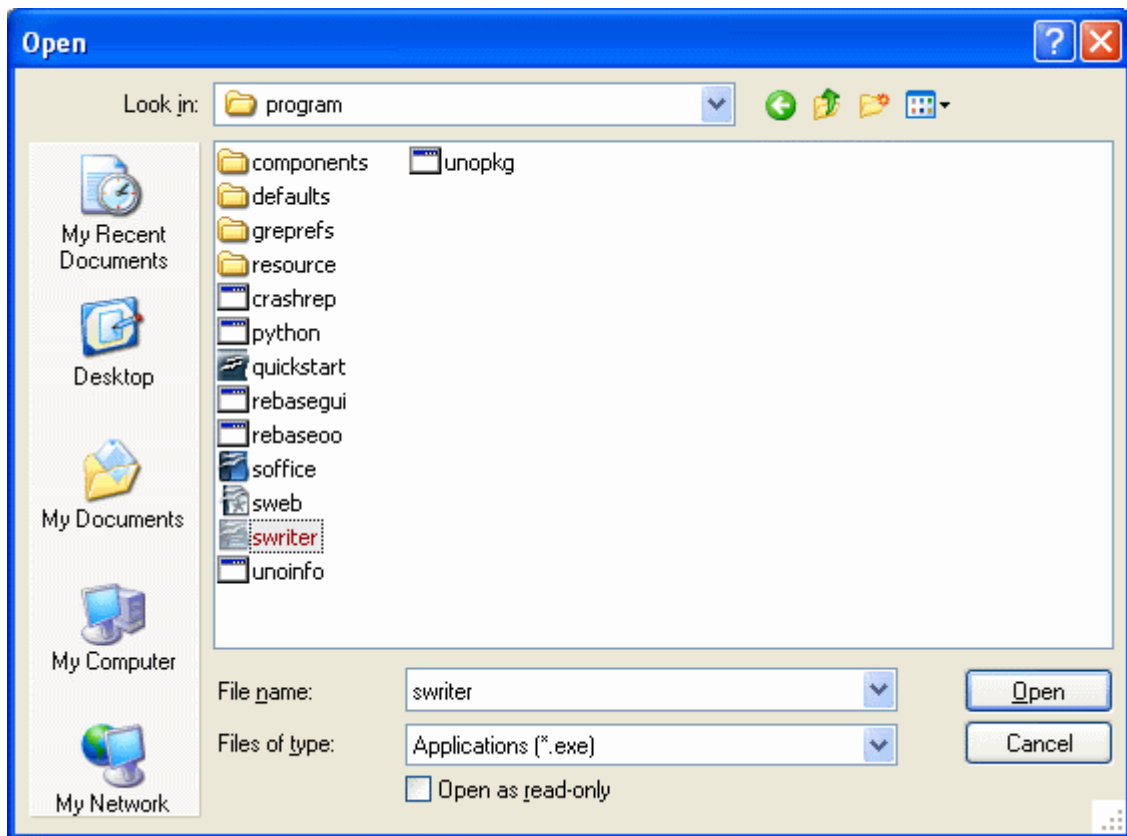
Run a program in sandbox from Sandbox Tasks interface

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



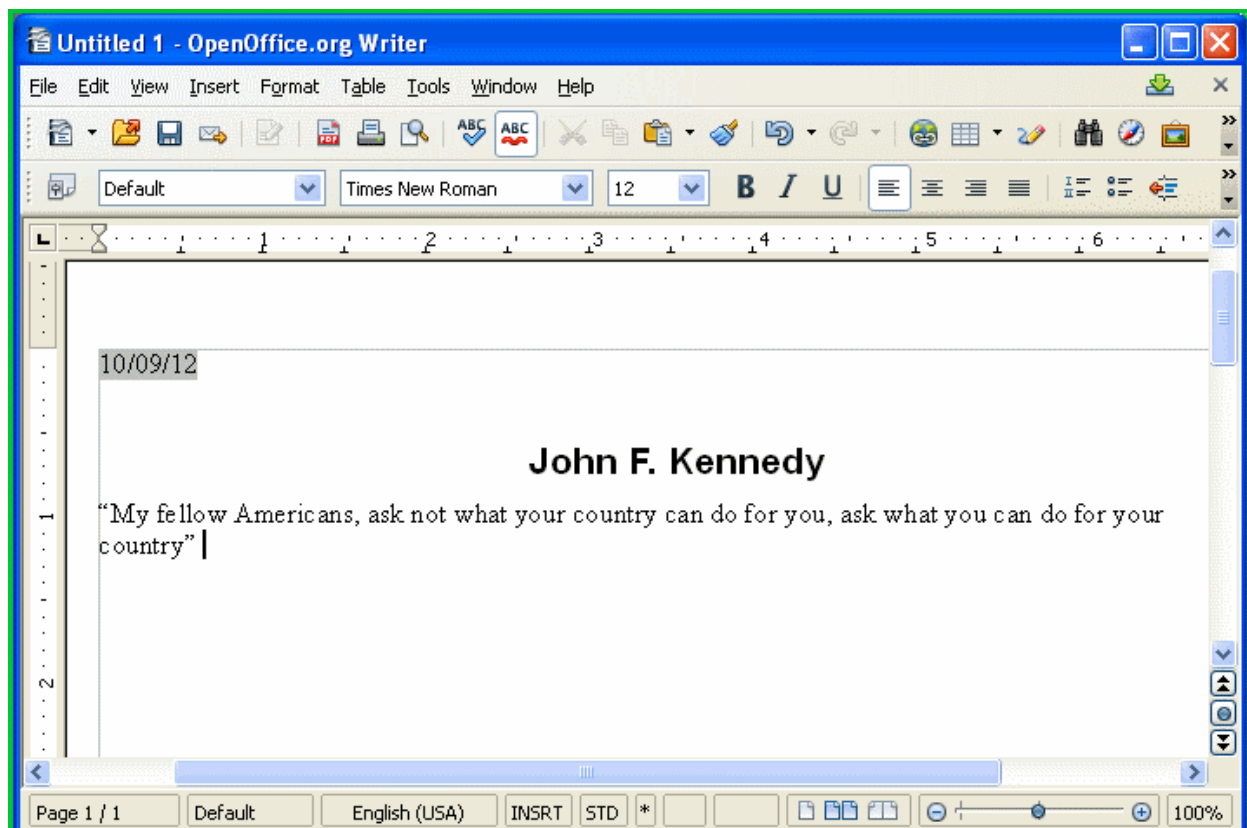
The 'Run Virtual' dialog will be displayed.

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**.



Running 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:

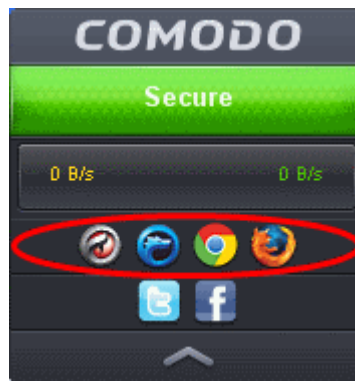


Comodo Internet Security allows you to run a browser in the sandbox:

- **From the desktop widget**
- **From the Sandbox Tasks interface**

Starting a browser from the desktop widget

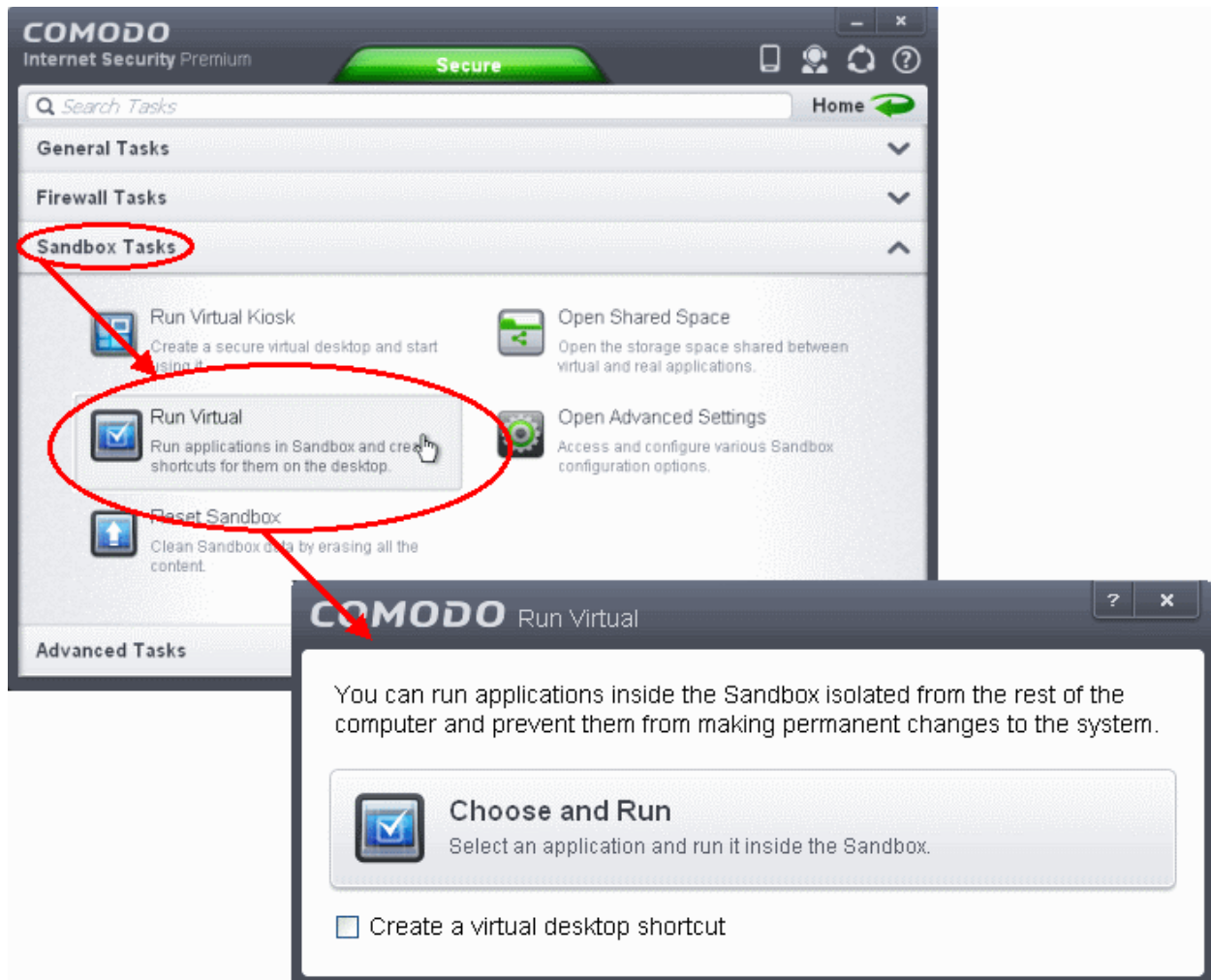
The CIS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- 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.

Running Untrusted Programs Inside Virtual Kiosk

This page explains how to run untrusted programs inside the Virtual Kiosk. Applications running in the kiosk 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 Kiosk 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 Kiosk, in the desktop of your real system. The shortcuts of your real desktop will be available in the Virtual Kiosk desktop. You can double click on the icon to open the respective application of file inside the Virtual Kiosk.

Note: The real computer desktop icons will be available only in the **Classic Windows Mode** and **Tablet + Classic Mode**.

Shared Space

The Virtual Kiosk 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 Kiosk.

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 Kiosk

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 Kiosk' by clicking the Virtual Kiosk shortcut in the CIS home screen or by clicking Sandbox Tasks > Run Virtual Kiosk from the Tasks interface of CIS.



4. Open Shared Space inside the Virtual Kiosk 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 Kiosk.

The changes you make to the file will be stored to the file only inside the Virtual Kiosk and not in the real computer system.

Running Browsers Inside the Virtual Kiosk

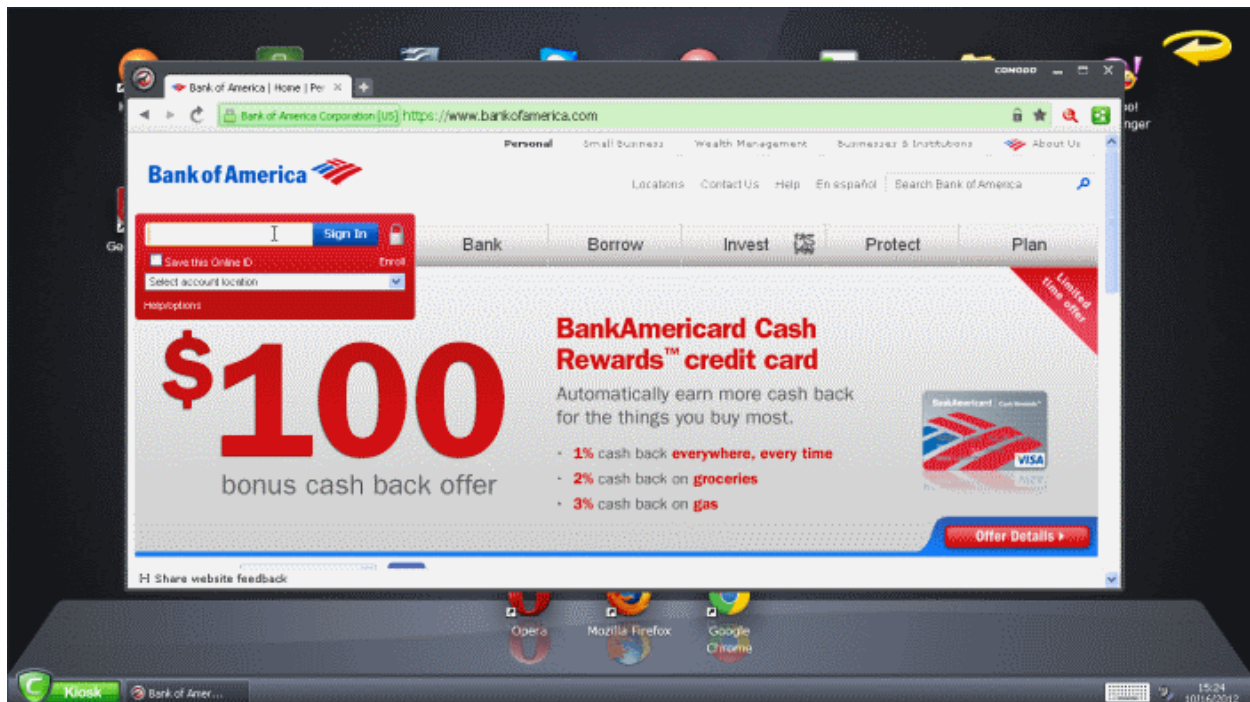
The Virtual Kiosk provides an extremely secure environment for Internet related activities because it isolates your browser from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net inside the Kiosk 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 Kiosk

1. Click the 'Kiosk' menu at the bottom left
2. Select the browser you want to run from the browsers displayed.



The browser will be opened inside the Kiosk.



On completion of your browsing session, no trails like your browsing history will be stored in your computer.

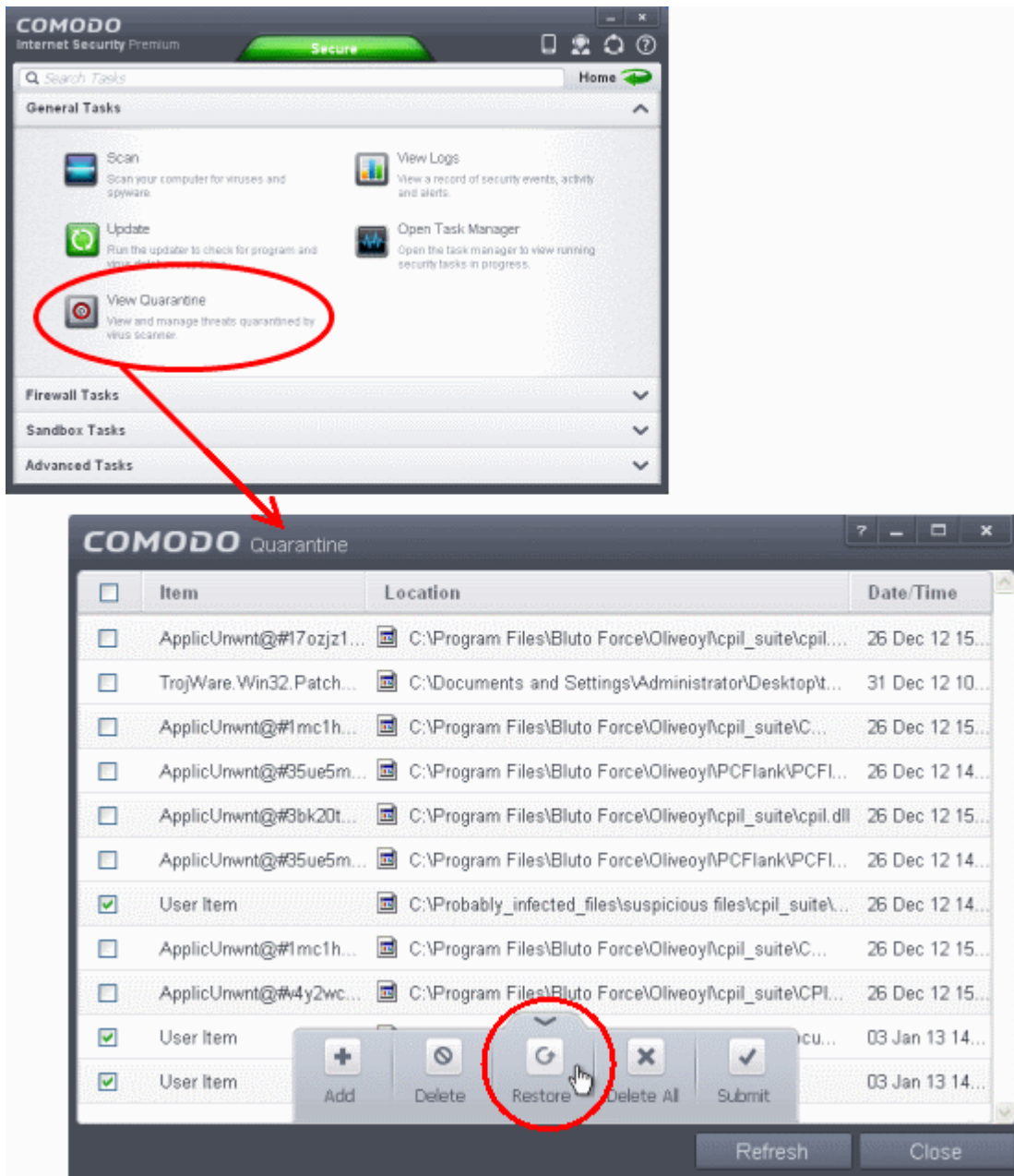
Restoring Incorrectly Quarantined Item(s)

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'.

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.

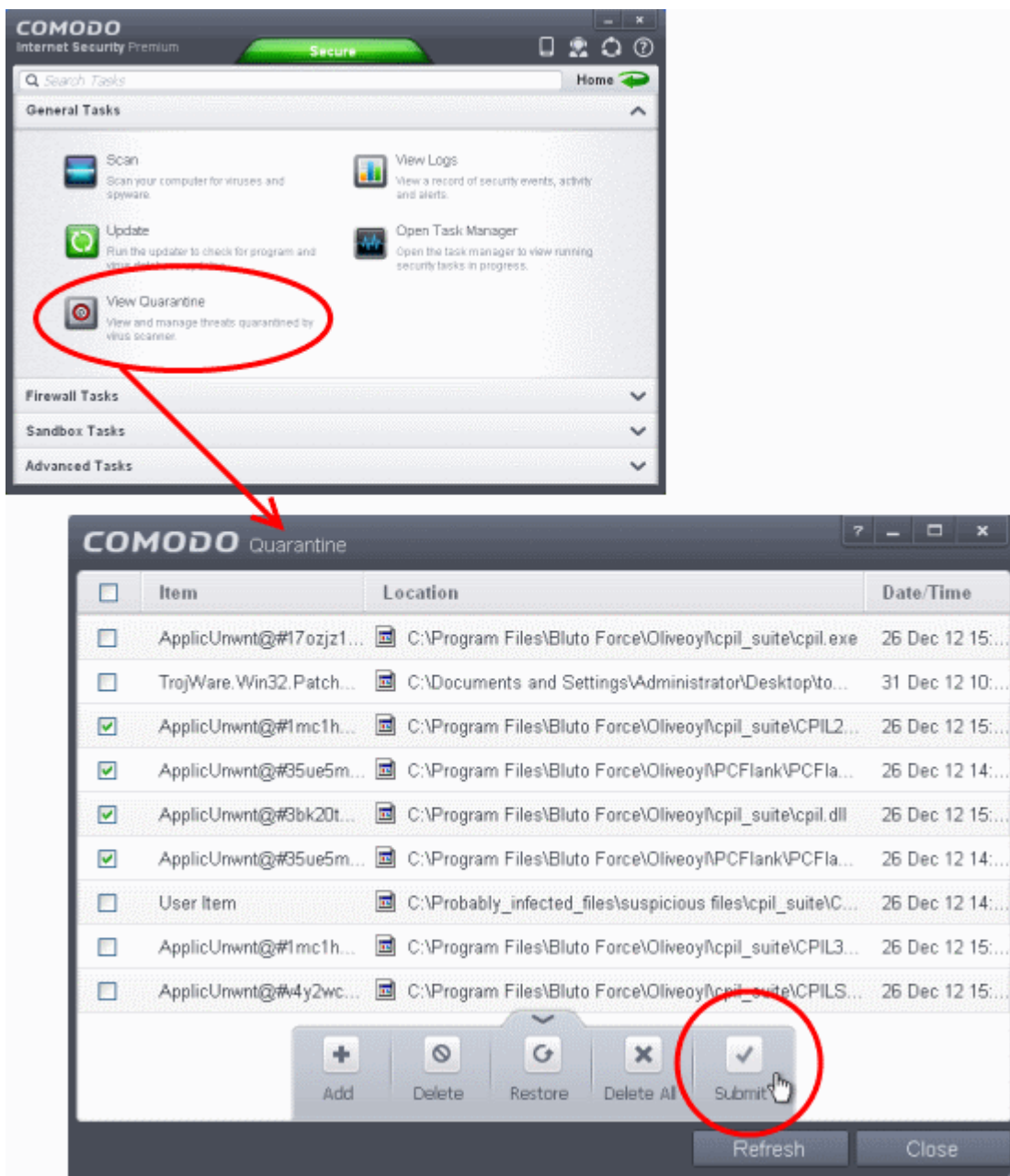
Submitting Quarantined Items to Comodo for Analysis

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

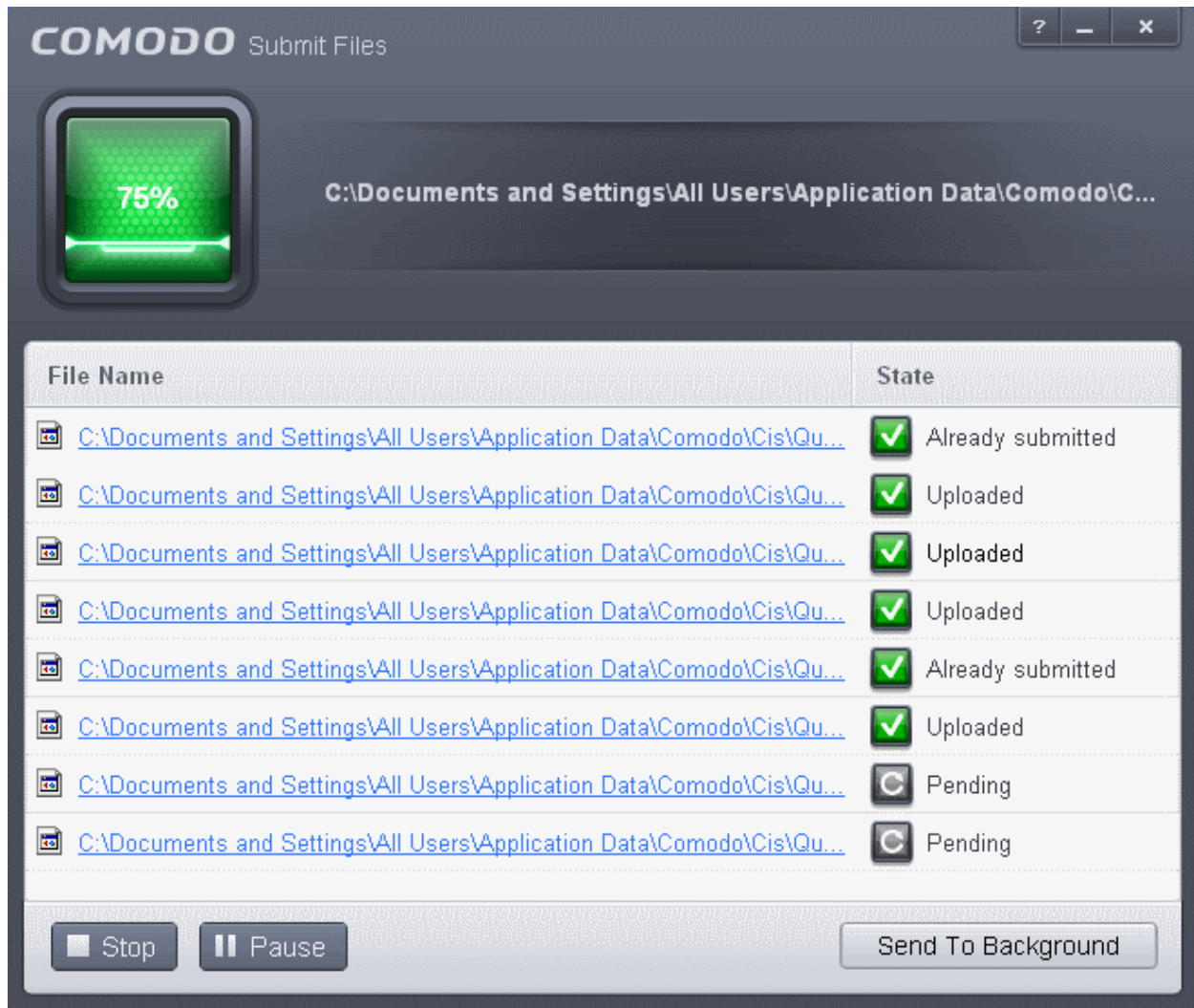
1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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.

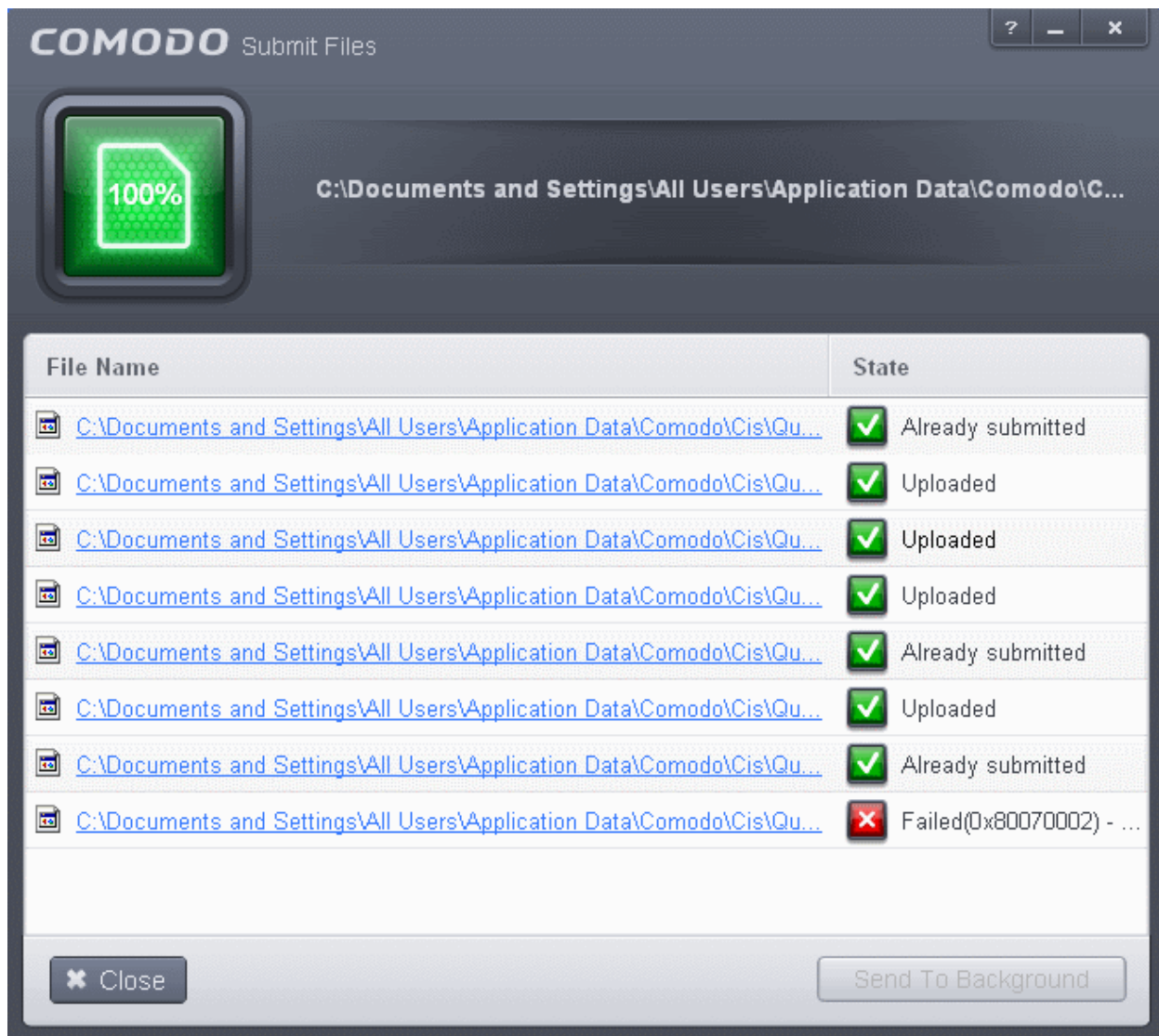


3. Choose the items to be submitted to Comodo for analysis by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Submit'.

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.



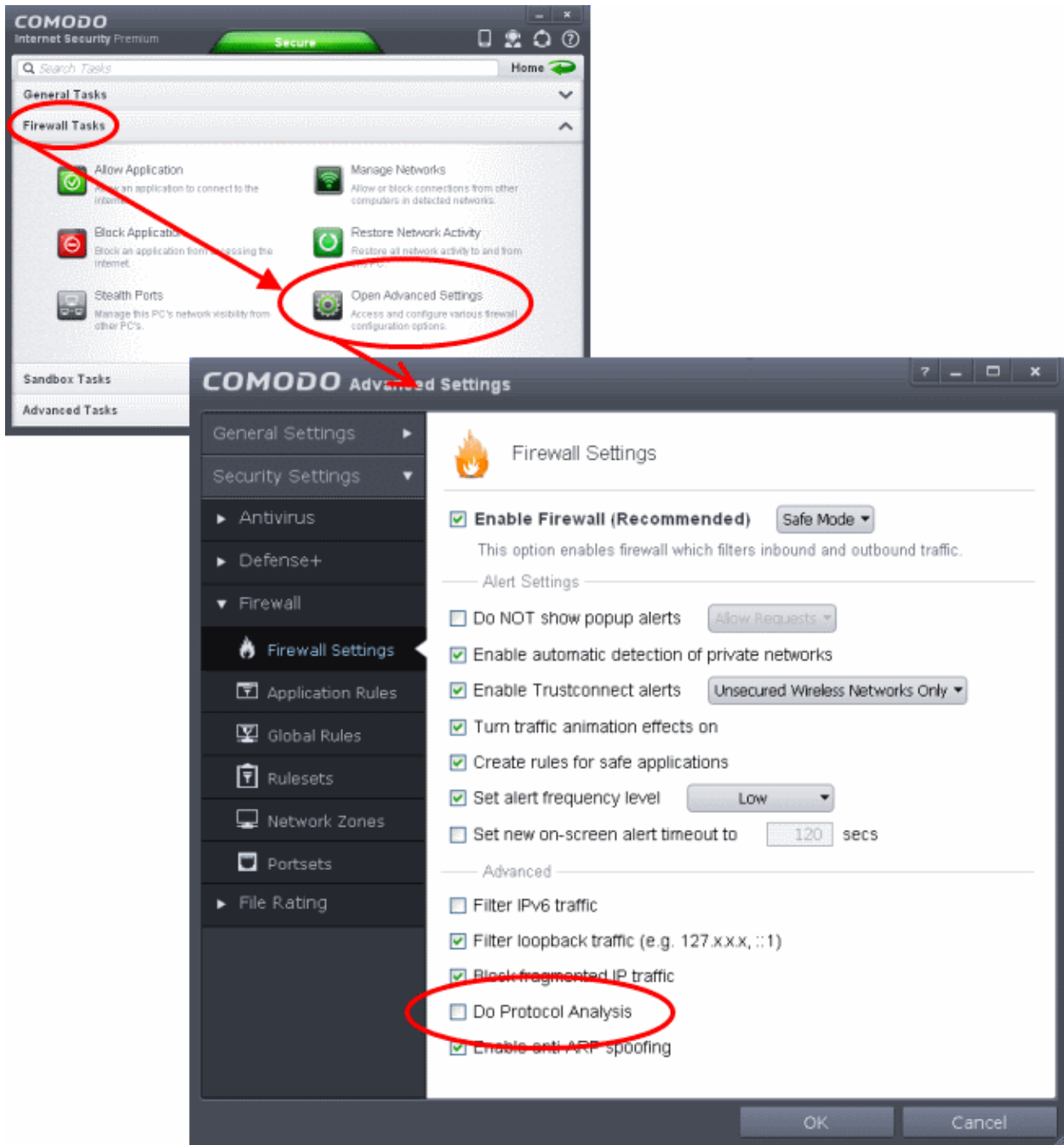
Enabling File Sharing Applications like BitTorrent and Emule

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'

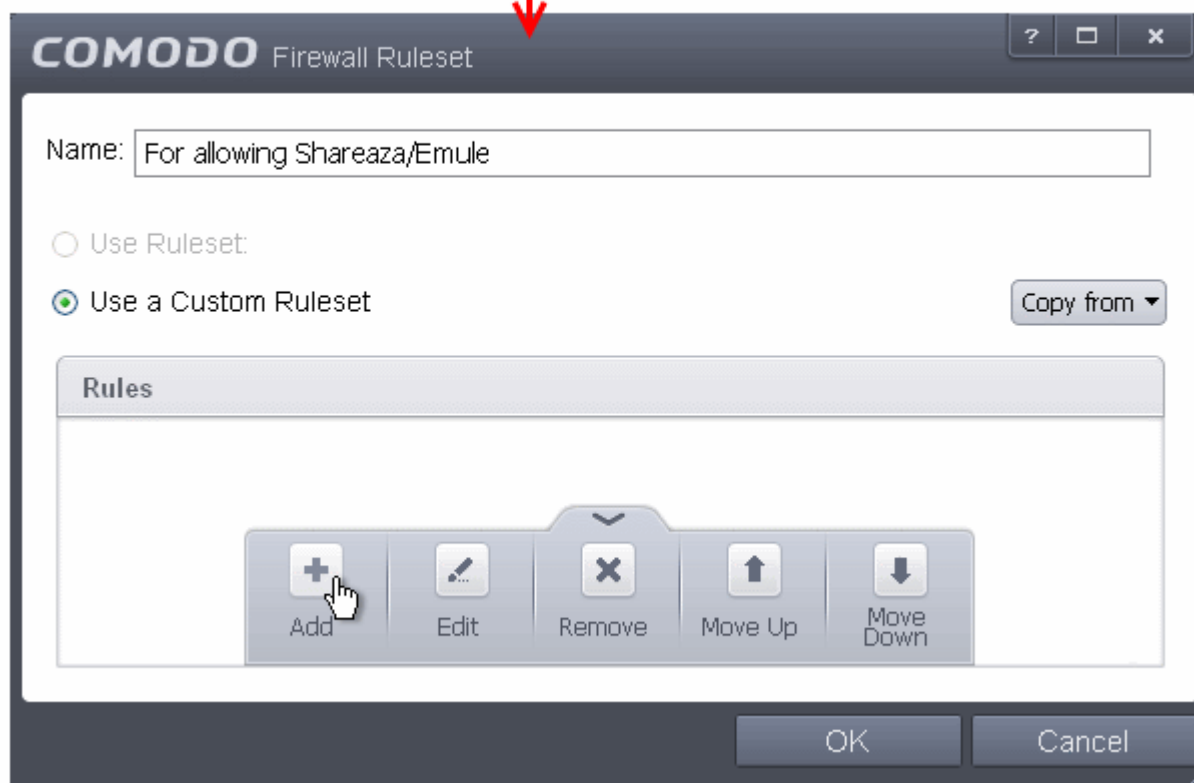
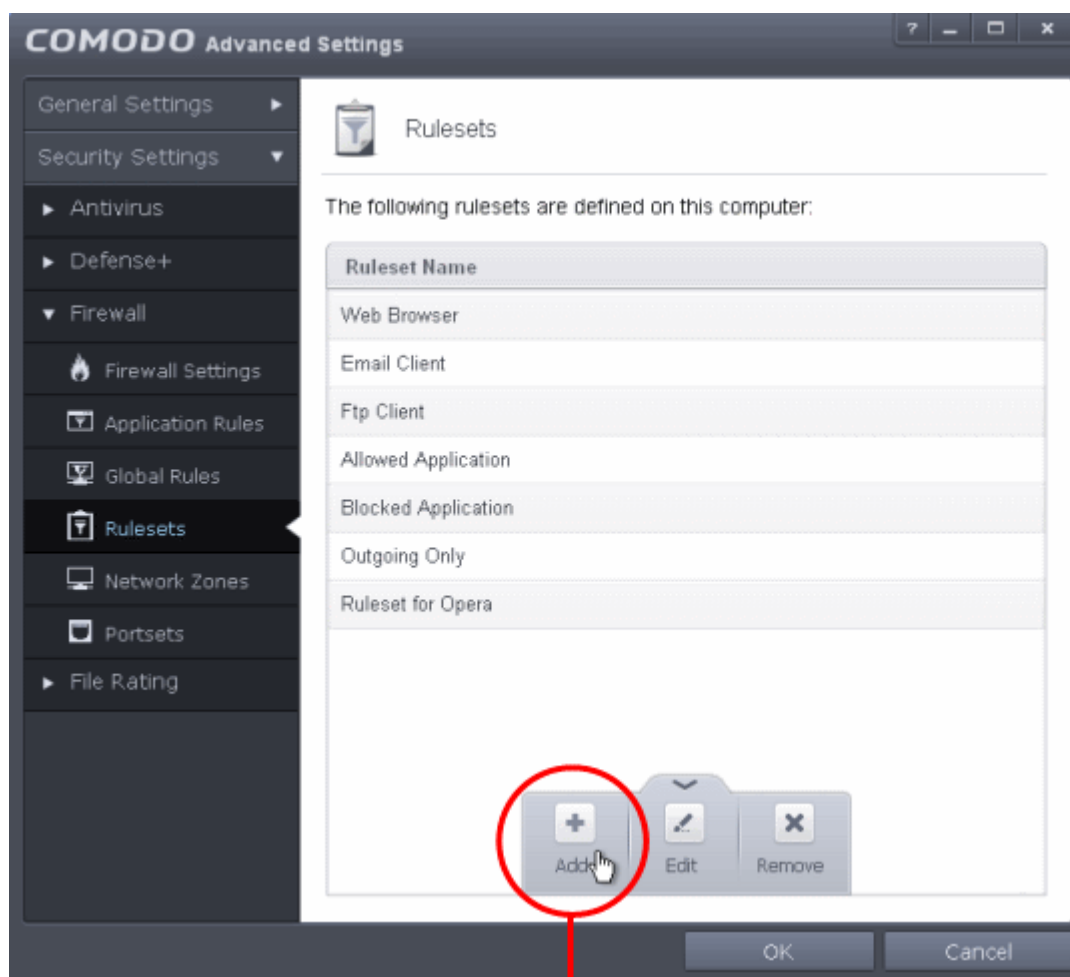
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.



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'.

Blocking any Downloads of a Specific File Type

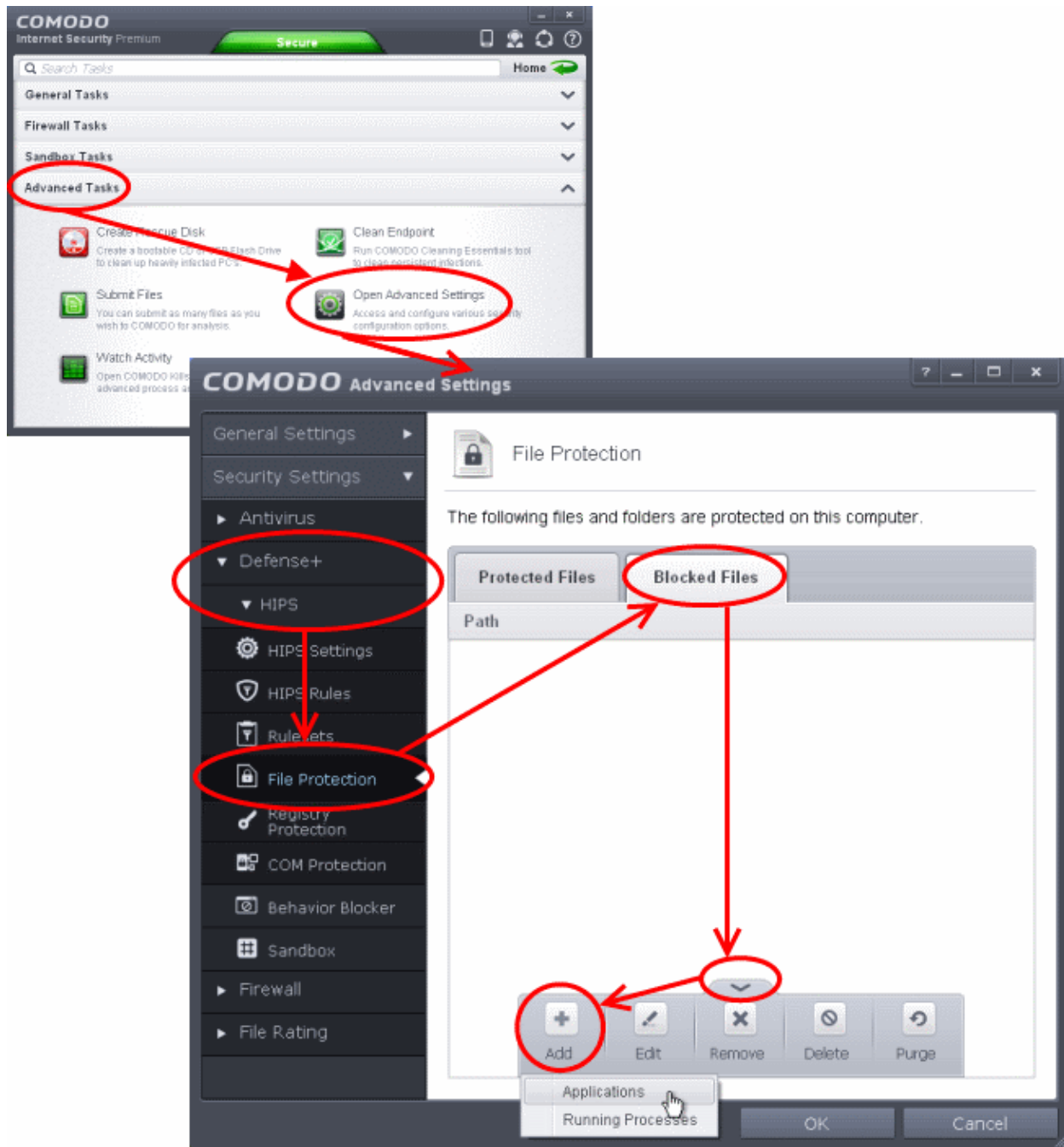
Comodo Internet Security can be configured to block downloads of specific types of file.

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.

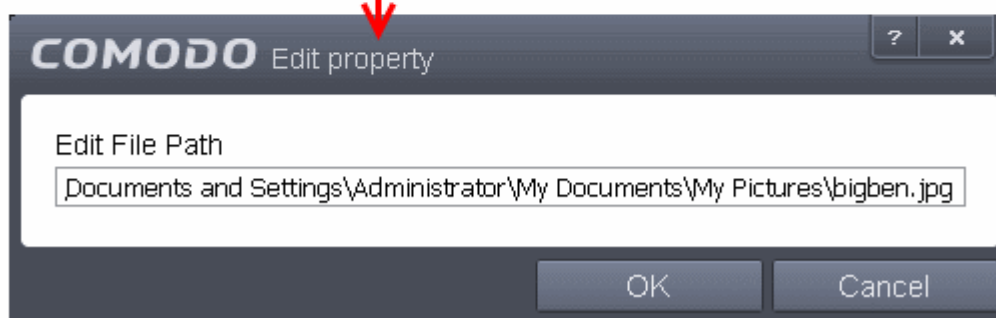
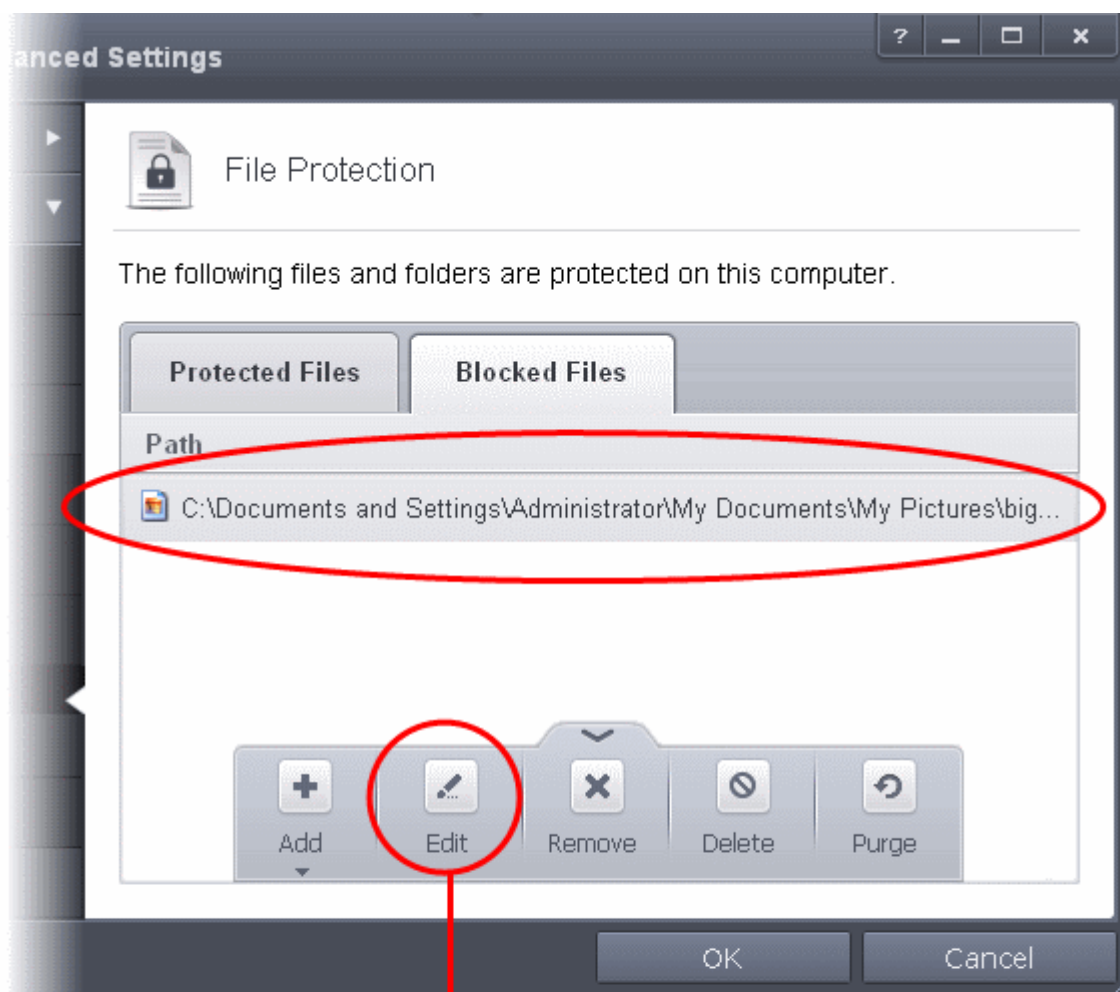
To selectively block downloading of specific file type, you need to configure Defense+ component of CIS to block the specific file type from the default download folder of your browser.

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' > 'File Protection' 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'

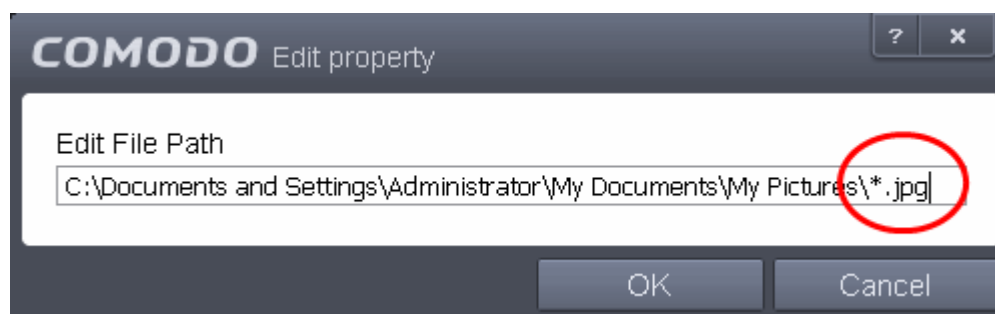
The file will be added to blocked files list.



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.

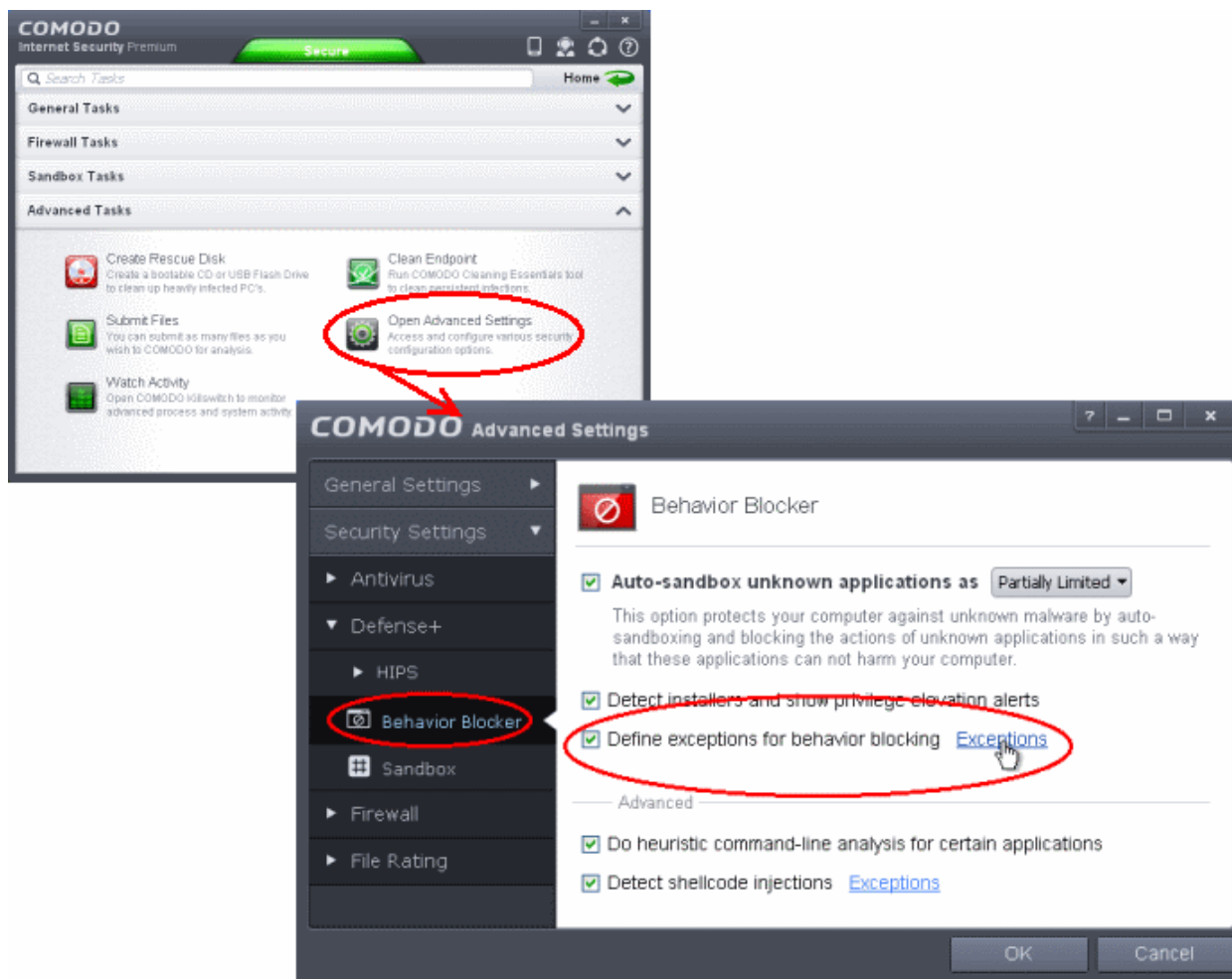
Tip: To unblock the download, Advanced Settings > Defense+ > HIPS > File Protection > Blocked Files, select the file path, click the handle from the bottom and choose 'Remove'.

Disabling Behavior Blocker and Auto-Sandboxing on a per-application basis

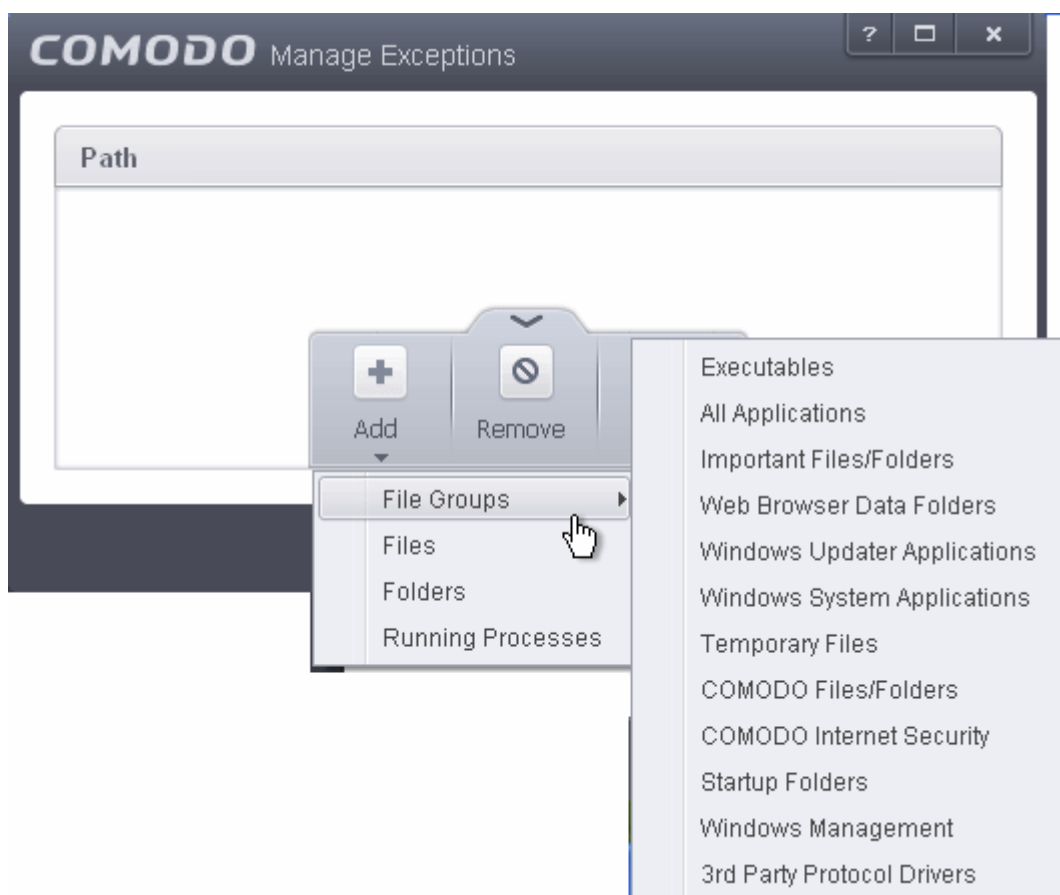
Behavior Blocker will auto-sandbox run unknown executables and queue them for submission to Comodo Cloud scanners for behavior analysis. Users do, however, have the option to exclude specific files or file types from this auto-sandboxing process. This is particularly useful for developers that are creating new applications which, by their nature, are as yet unknown to the Comodo safe list.

To disable the auto-sandboxing selectively

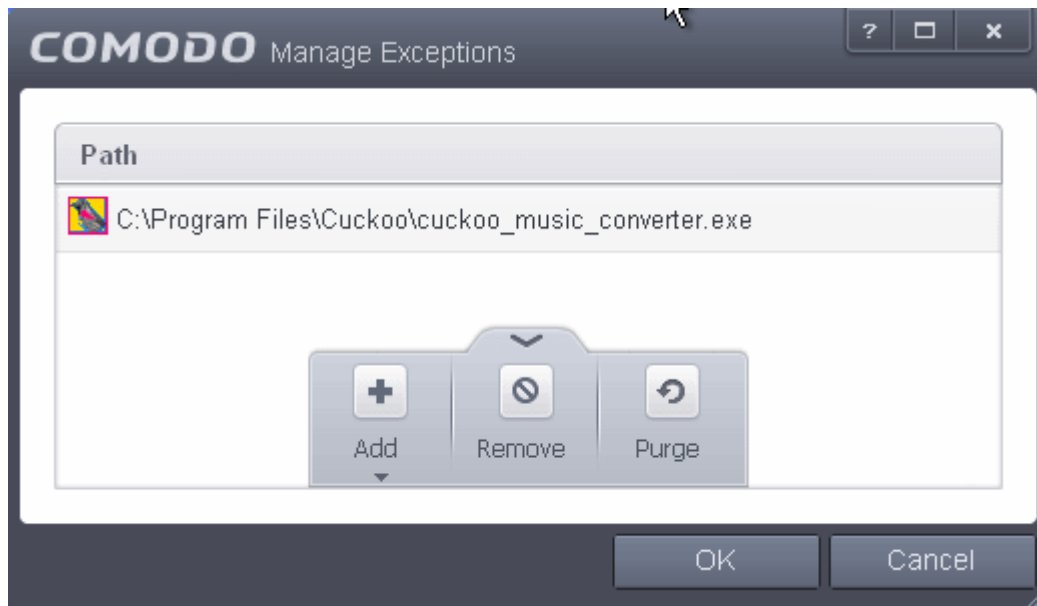
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Security Settings' > 'Defense+' > 'Behavior Blocker' in the left hand side navigation pane of Advanced Settings pane
4. Select the check box 'Define exceptions for behavior blocking and then click on the words 'Exceptions'



The Manage Exceptions interface will open.



5. Click the handle from the bottom and choose 'Add' from the options to add the files/executables to be excluded from monitoring by Behavior Blocker and Auto-Sandboxing.
 - 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**.
 - **Files** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.
 - **Folder** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
 - **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.
6. Click 'OK' in the Manage Exceptions interface.



7. Click OK in the Advanced Settings panel for your settings to take effect.

The selected application will not be auto-sandboxed on its execution.

Alternatively...

1. Add the files to the list of **Trusted Files**
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**.

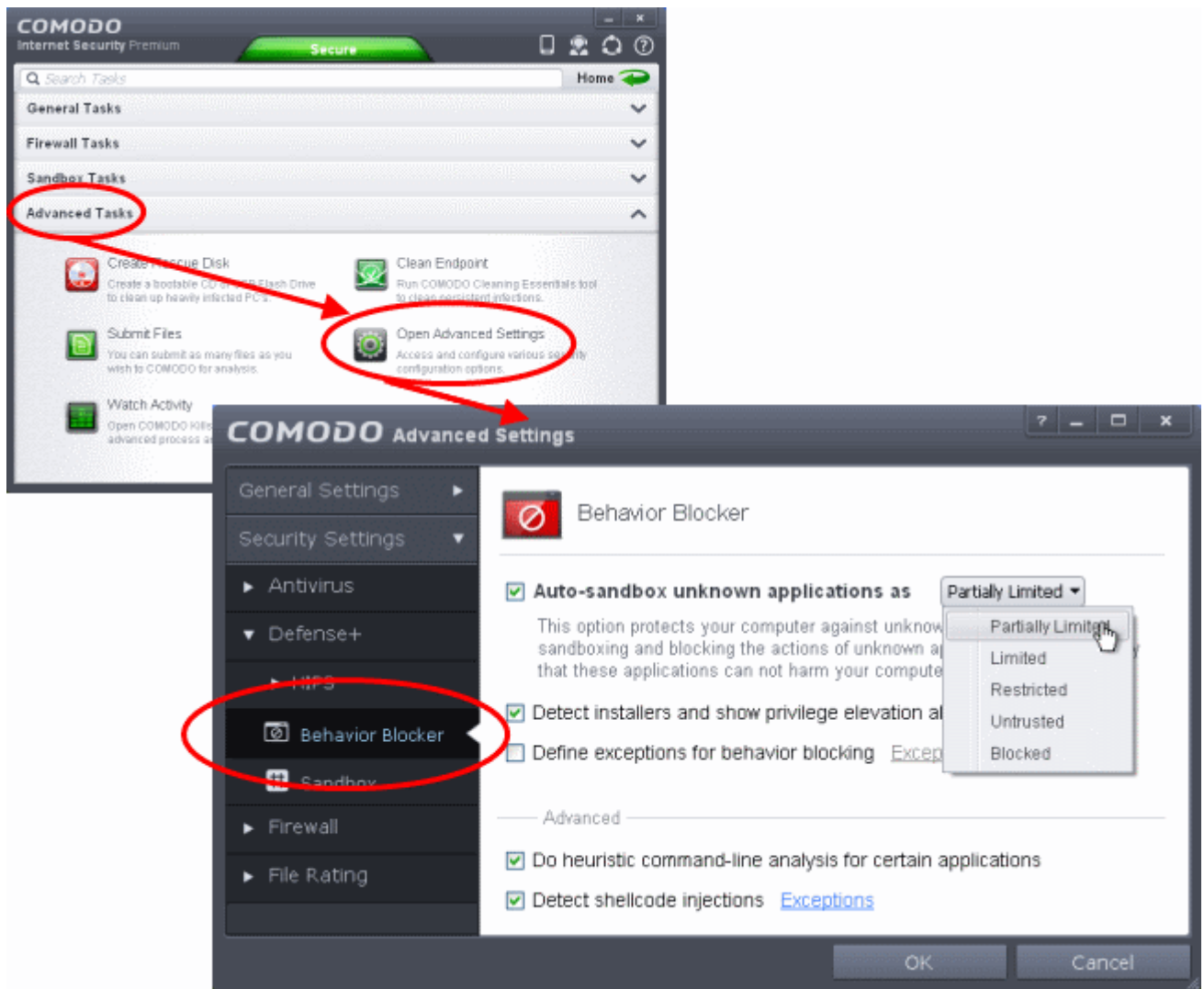
Enabling Full Virtualization for Auto-Sandboxed Applications (Advanced)

The Behavior Blocker will auto-sandbox an unknown executable and restrict its execution privileges according to an access restriction level set by you. The available restriction levels can be viewed in the Behavior Blocker settings panel. This tutorial explains how to add 'Fully Virtualized' to the set of available restriction levels for auto-sandboxed applications. It involves modifications to the Windows registry and should only be attempted by advanced users.

- **Viewing and understanding restriction levels**
- **Adding the 'Fully Virtualized' level**

To view auto-sandbox restriction levels

1. Open the 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Click 'Advanced Tasks' > 'Open Advanced Settings'
3. Click 'Security Settings' > 'Defense+' > 'Behavior Blocker' from the left hand navigation



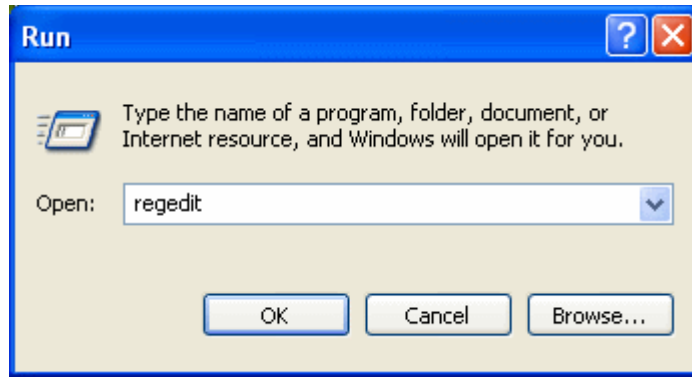
By default, the Behavior Blocker provides five access restriction levels to choose from, for automatically sandboxed applications.

- **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.
- **Blocked** - The application is not allowed to run at all.

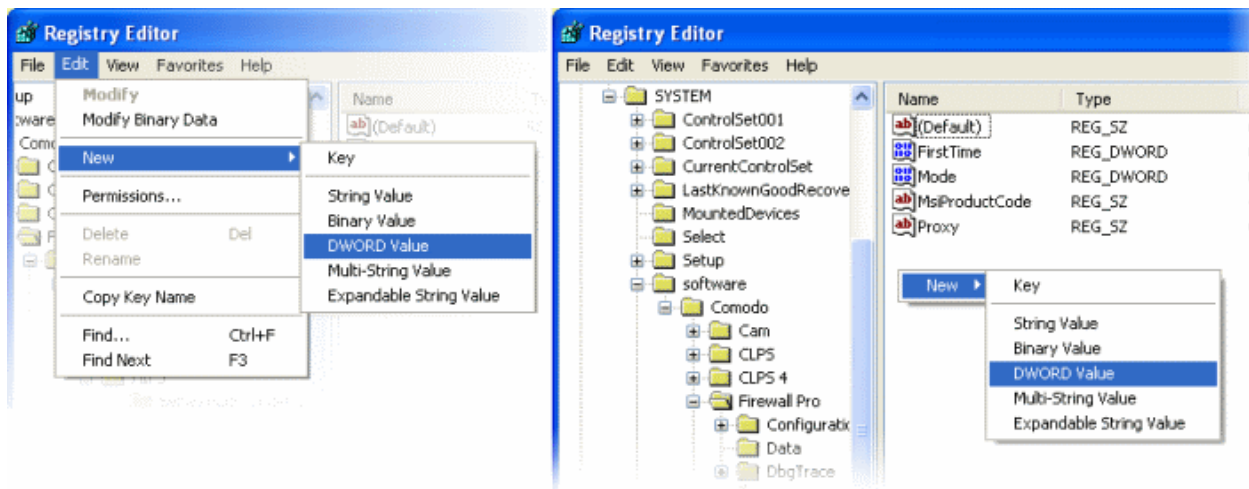
Advanced users can add an additional level '**Fully Virtualized**', in which all functionality of the application will be enabled, but in a virtual environment isolated from the operating system and files in the system. The 'Fully Virtualized' level but can be enabled by adding a registry key.

To add 'Fully Virtualized' level

1. Click 'Start' > 'Run', from the Windows Start menu
2. Type 'regedit' in the text box and click 'OK'

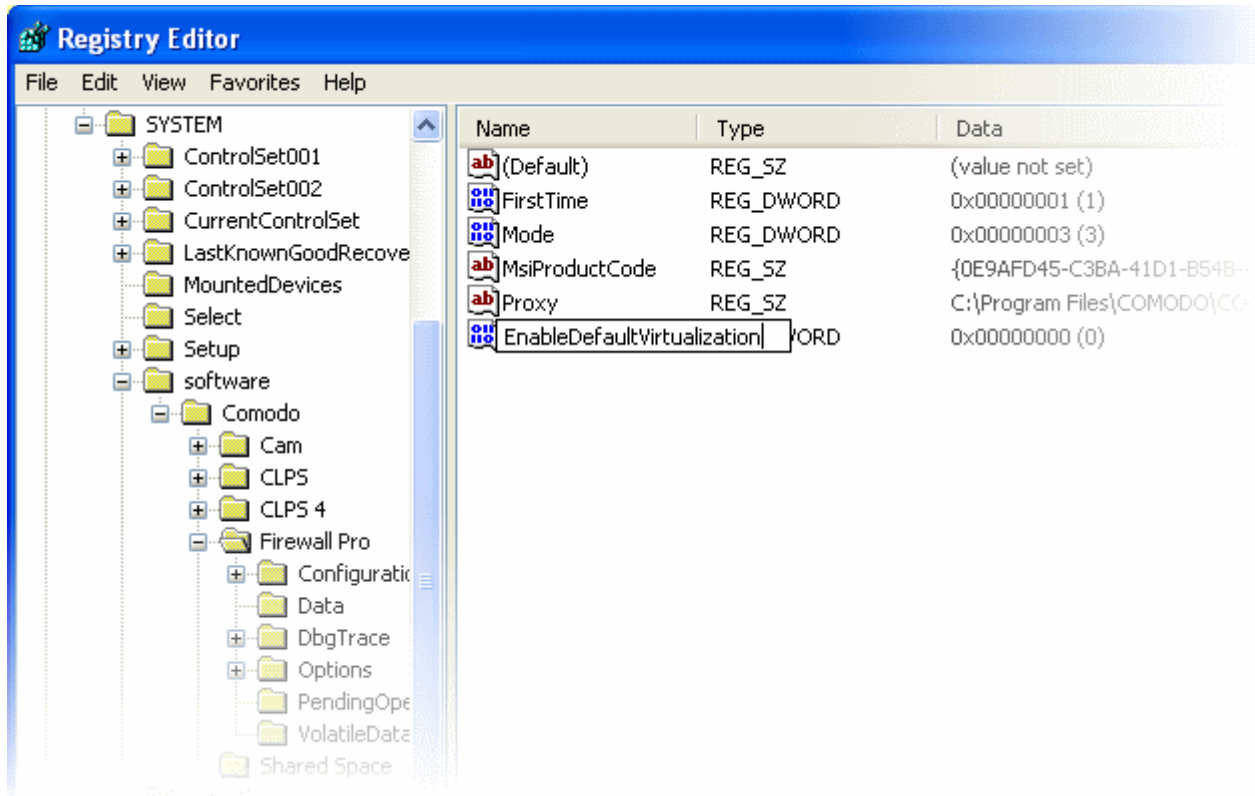


3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro
4. To add a new DWORD Entry, Click 'Edit' from the menu bar and select 'DWORD Value' **OR** right click in the right hand side pane and click 'New' > 'DWORD Value' from the right click options

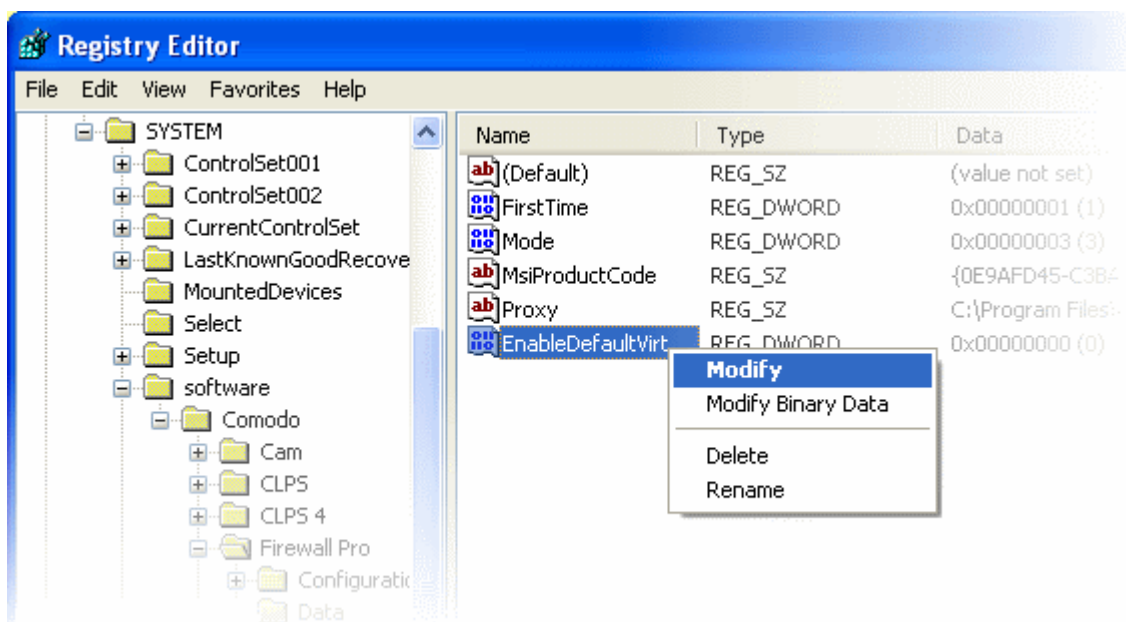


A new registry value will be added with the name 'New Value#1'

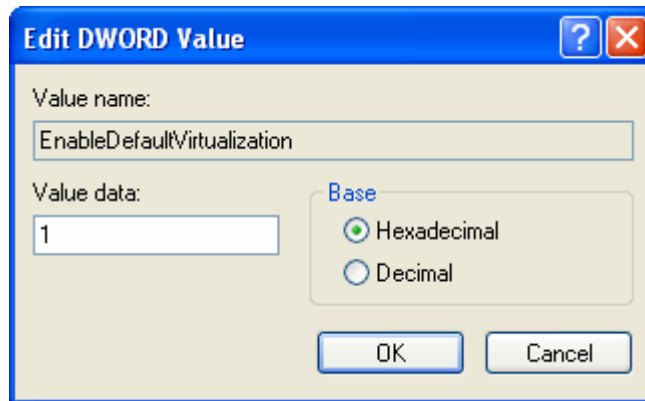
5. Rename the as **EnableDefaultVirtualization**



- Right-click on the value 'EnableDefaultVirtualization' and click 'Modify' from the context sensitive menu

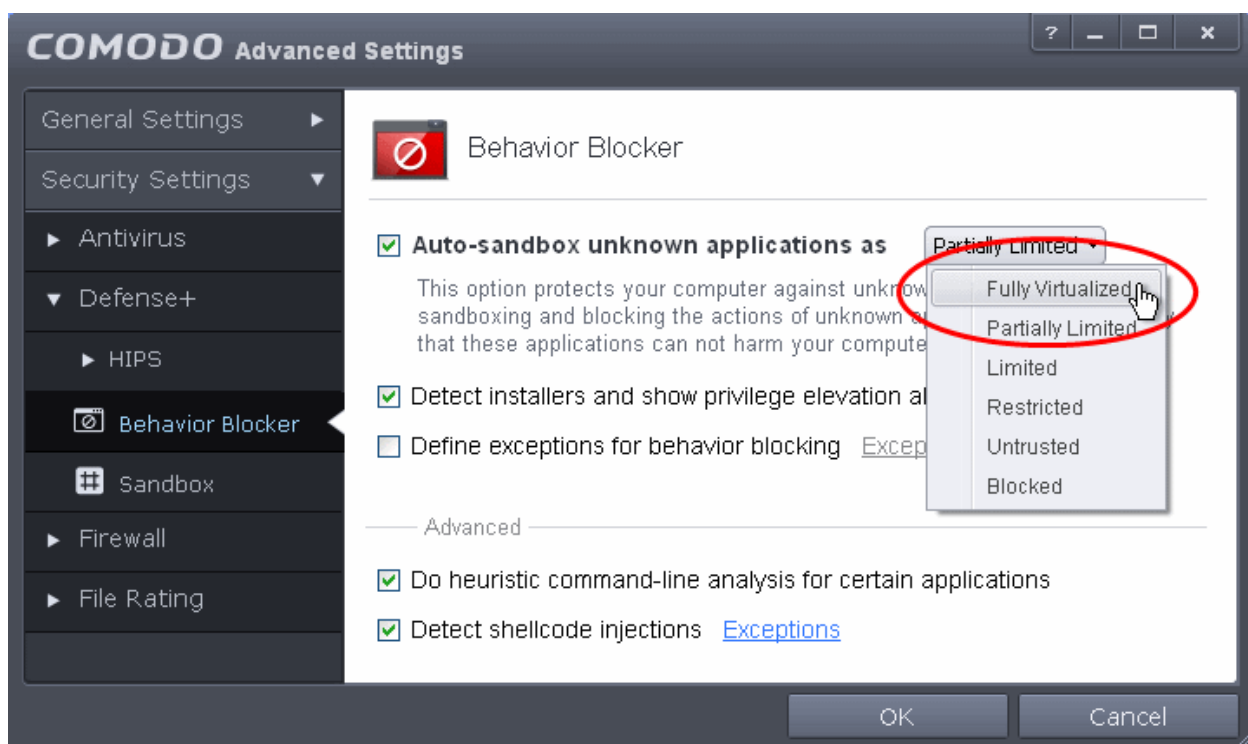


- In the 'Edit DWORD Value dialog box, change the 'Value data' from 1 to 0 and click OK



- Restart the system for the changes to take effect

The level 'Fully Virtualized' will be added and will be available available for selection in the Behavior Blocker Settings panel.



For more details on Auto-Sandboxing process, refer to the section [Unknown Files: The Auto-Sandboxing and Scanning Processes](#).

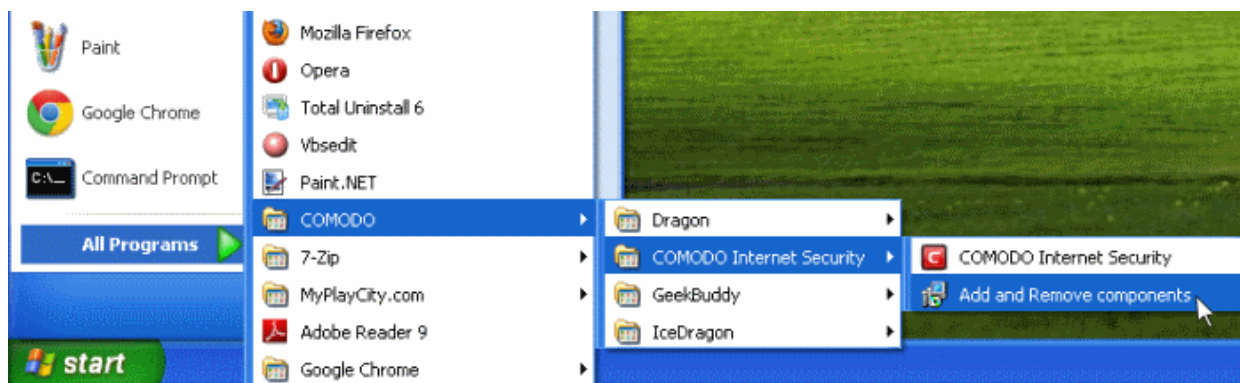
For more details on Behavior Blocker Settings refer to the section [Behavior Blocker](#).

Switching 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.

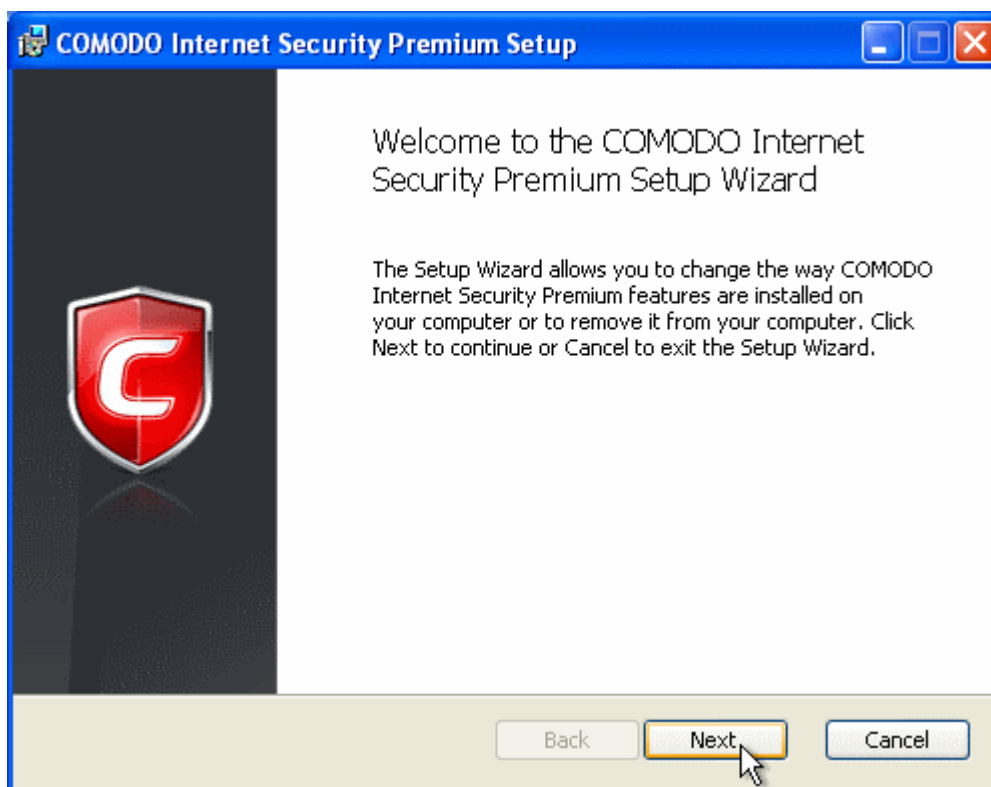
To switch the installation type

- Click Start > All Programs > COMODO > COMODO Internet Security > Add and Remove Components

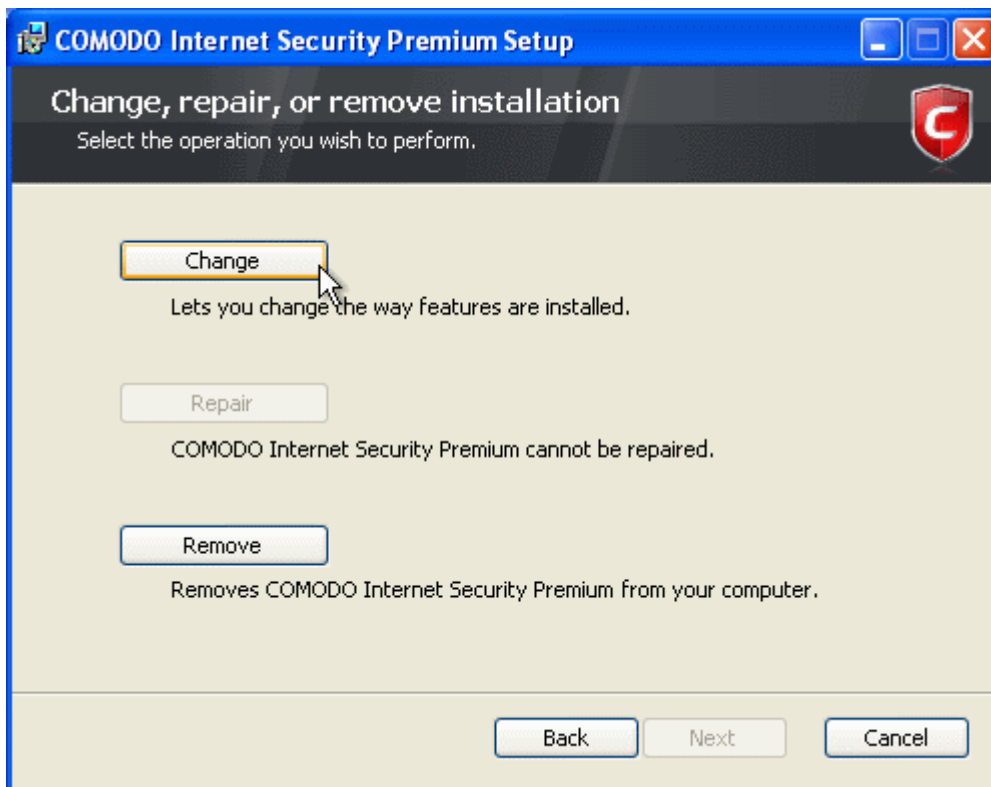


or click Start > Control Panel > Add/Remove Programs > Comodo Internet Security > Change.

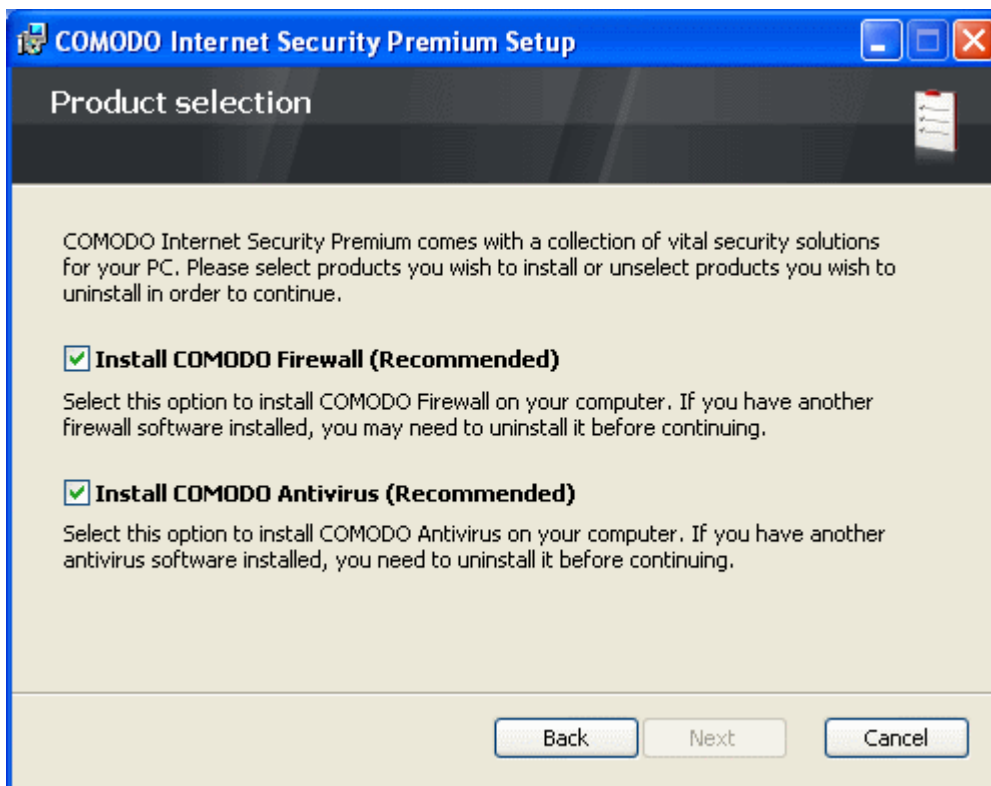
The Configuration Wizard will start.



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.

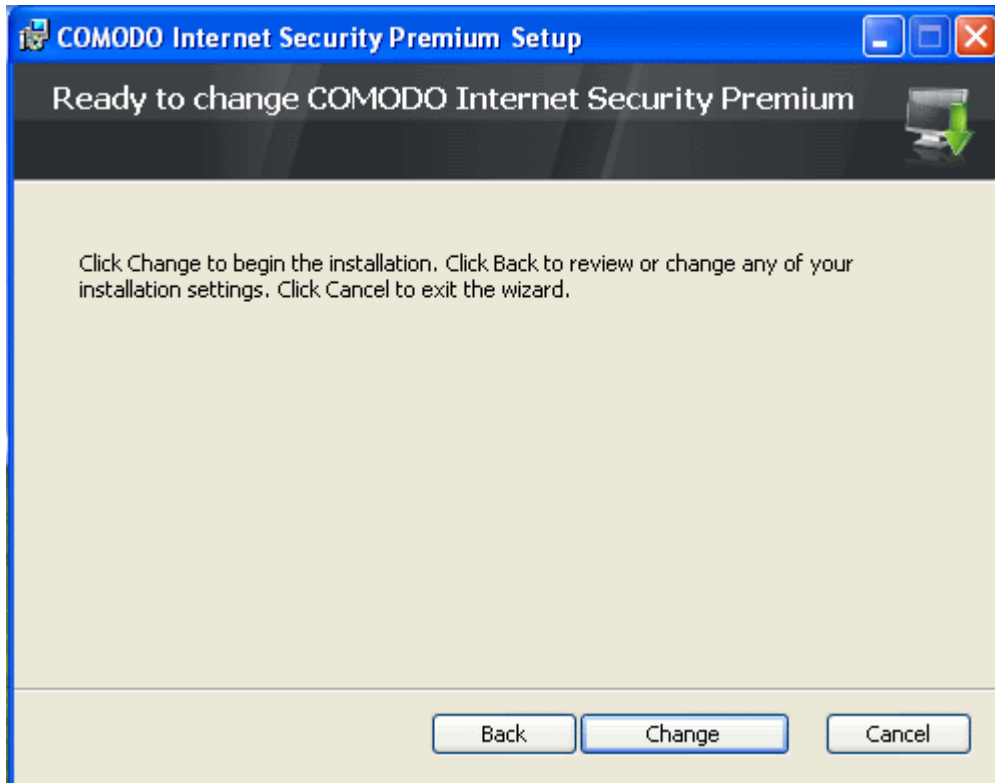
- If you want the complete installation, select both Install COMODO Antivirus and Install COMODO Firewall.
- If you want only the Antivirus part and not the Firewall part, select only the Install COMODO Antivirus and

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.

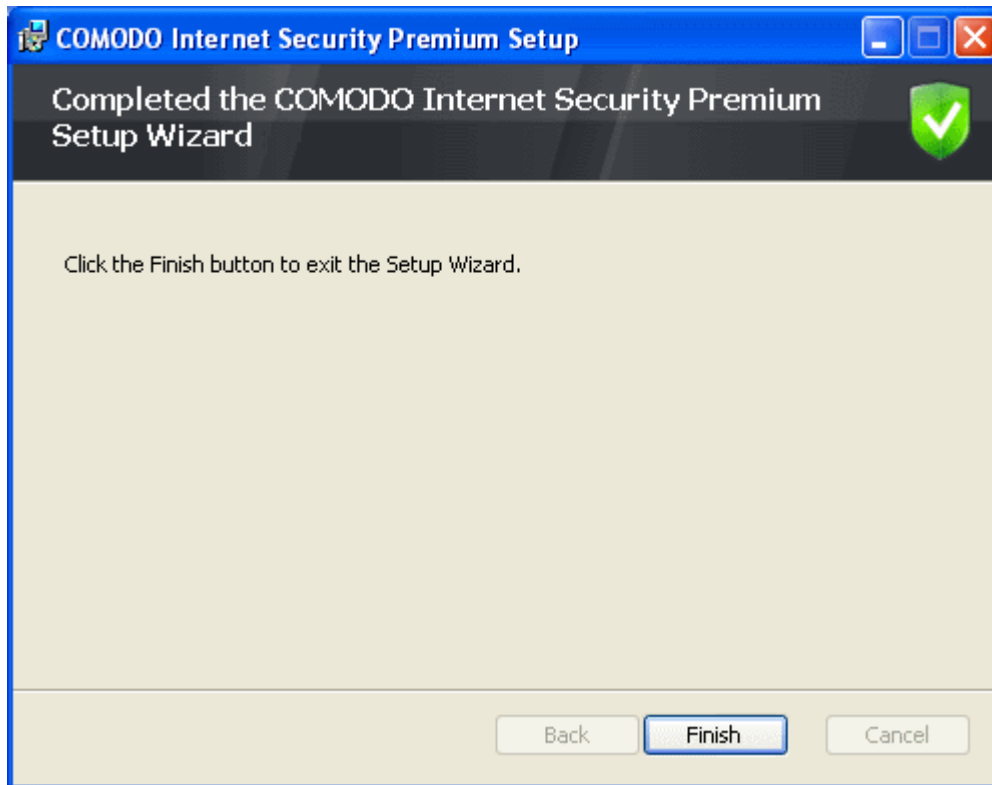
- Click 'Next'. Wait till the CIS is configured and is ready for the change.



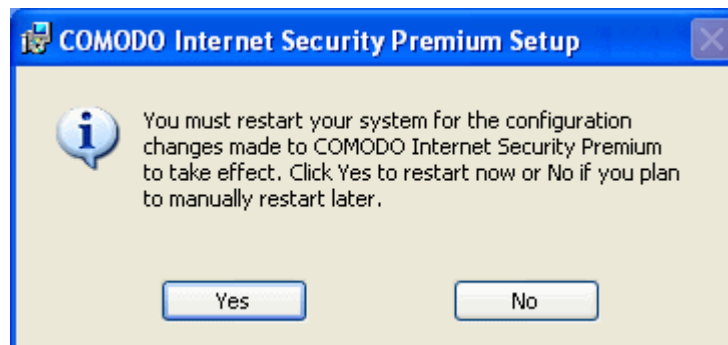
4. Click 'Change' in the next screen. The change progress will be indicated...



... 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.



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

Switch Off Automatic Antivirus and Software Updates

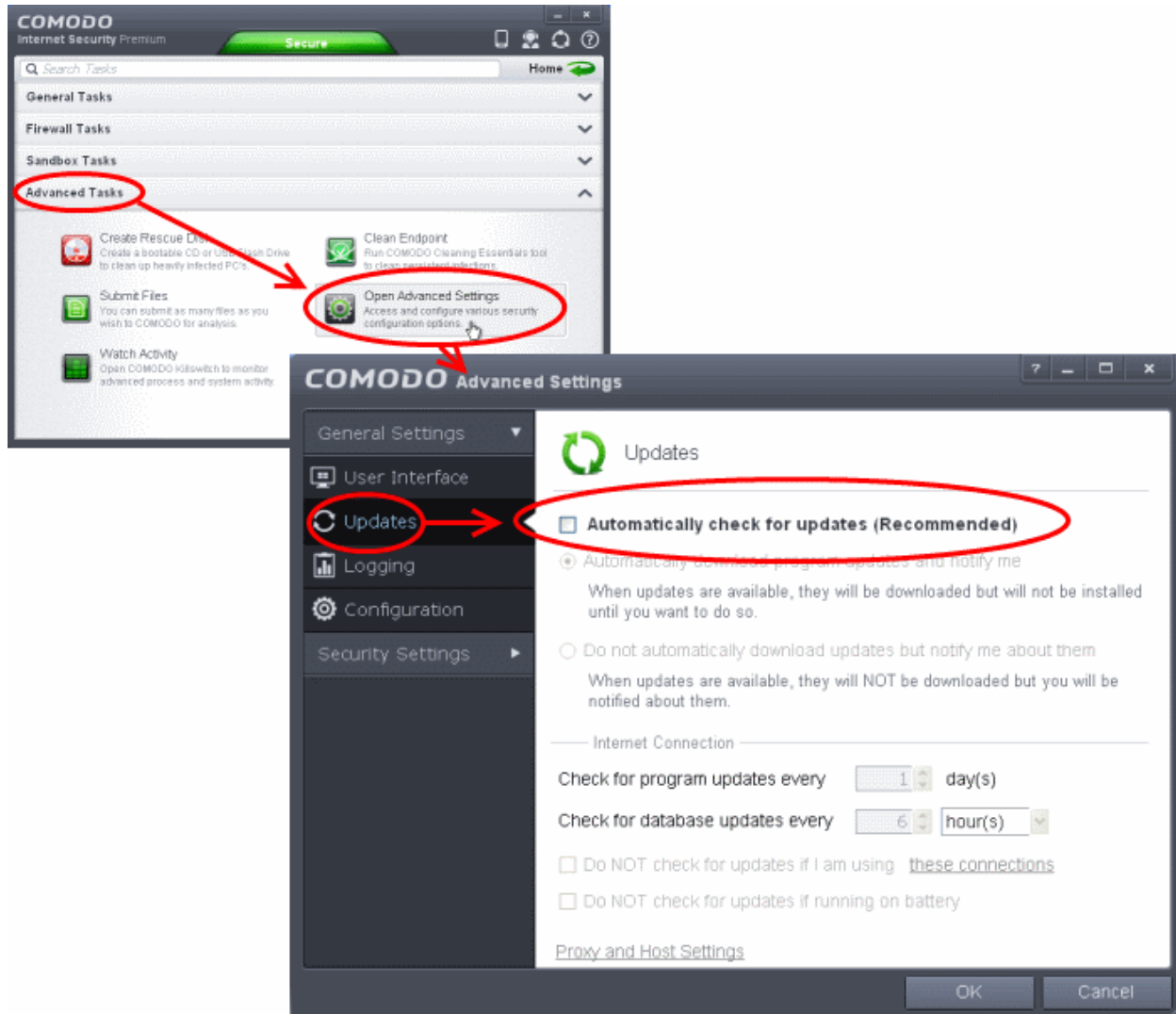
By default, Comodo Internet Security will automatically check for software and Antivirus database updates. However, some users like to have control over what gets downloaded and when it gets downloaded. For example, network administrators may not wish to automatically download because it will take up too much bandwidth during the day. Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.

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:

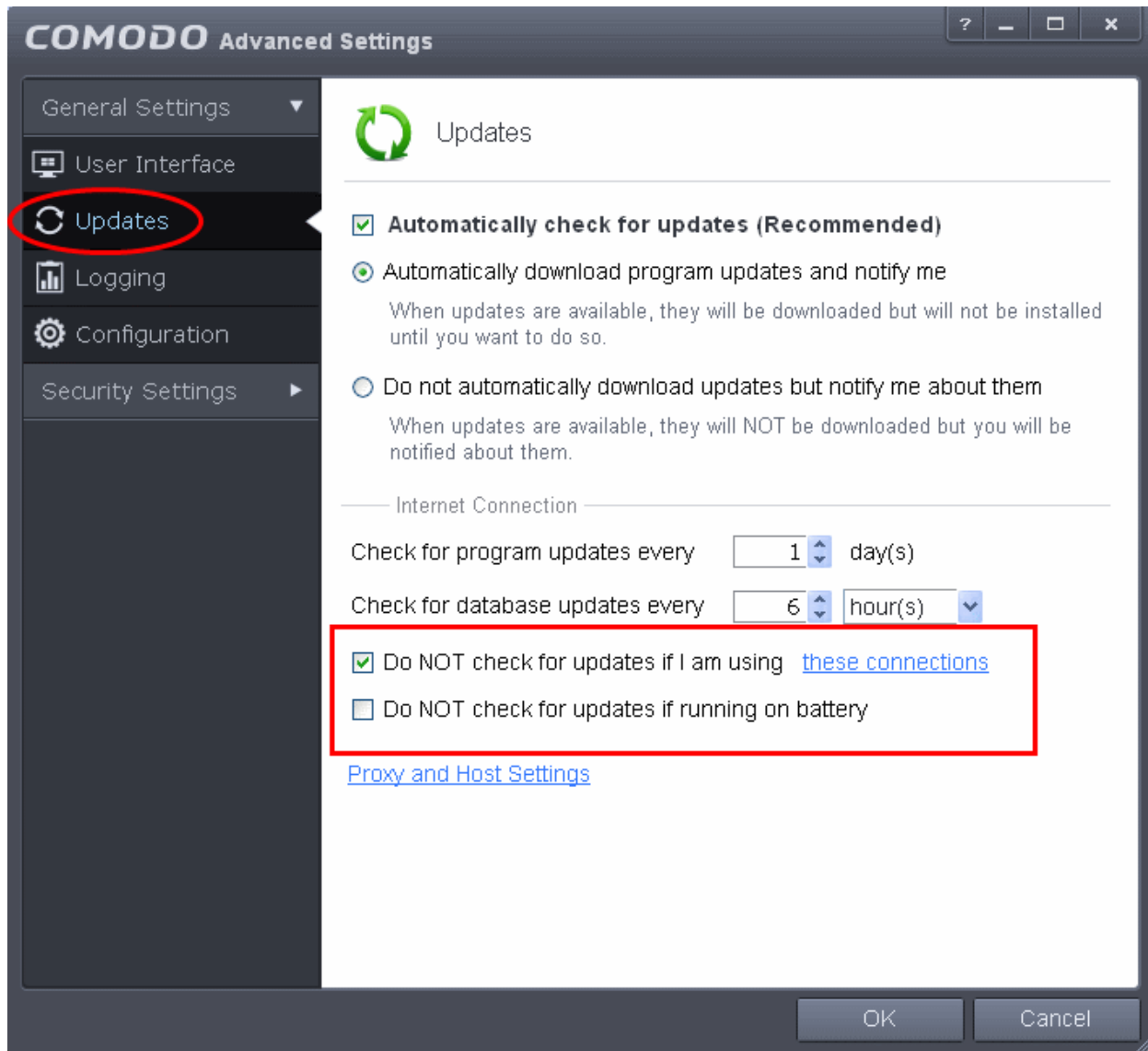
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane
4. Deselect the check box 'Automatically check for updates'



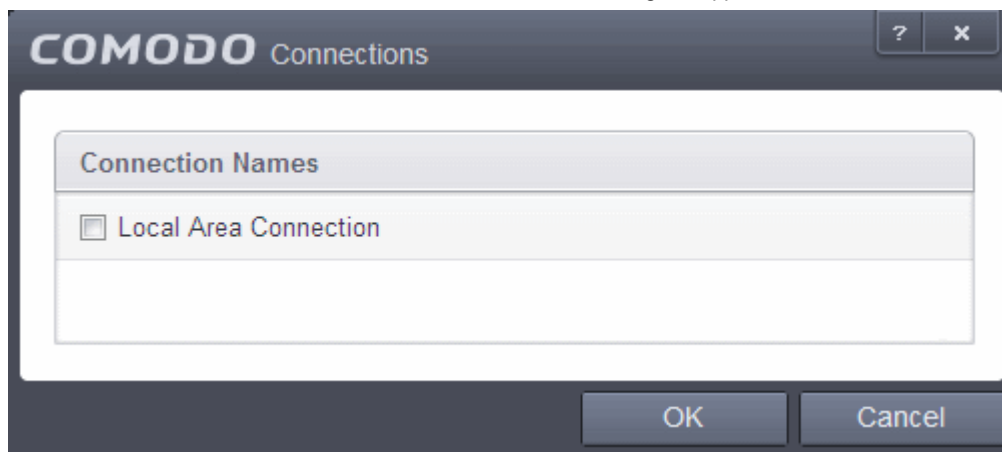
5. Click 'OK' in the Advanced Settings panel.

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



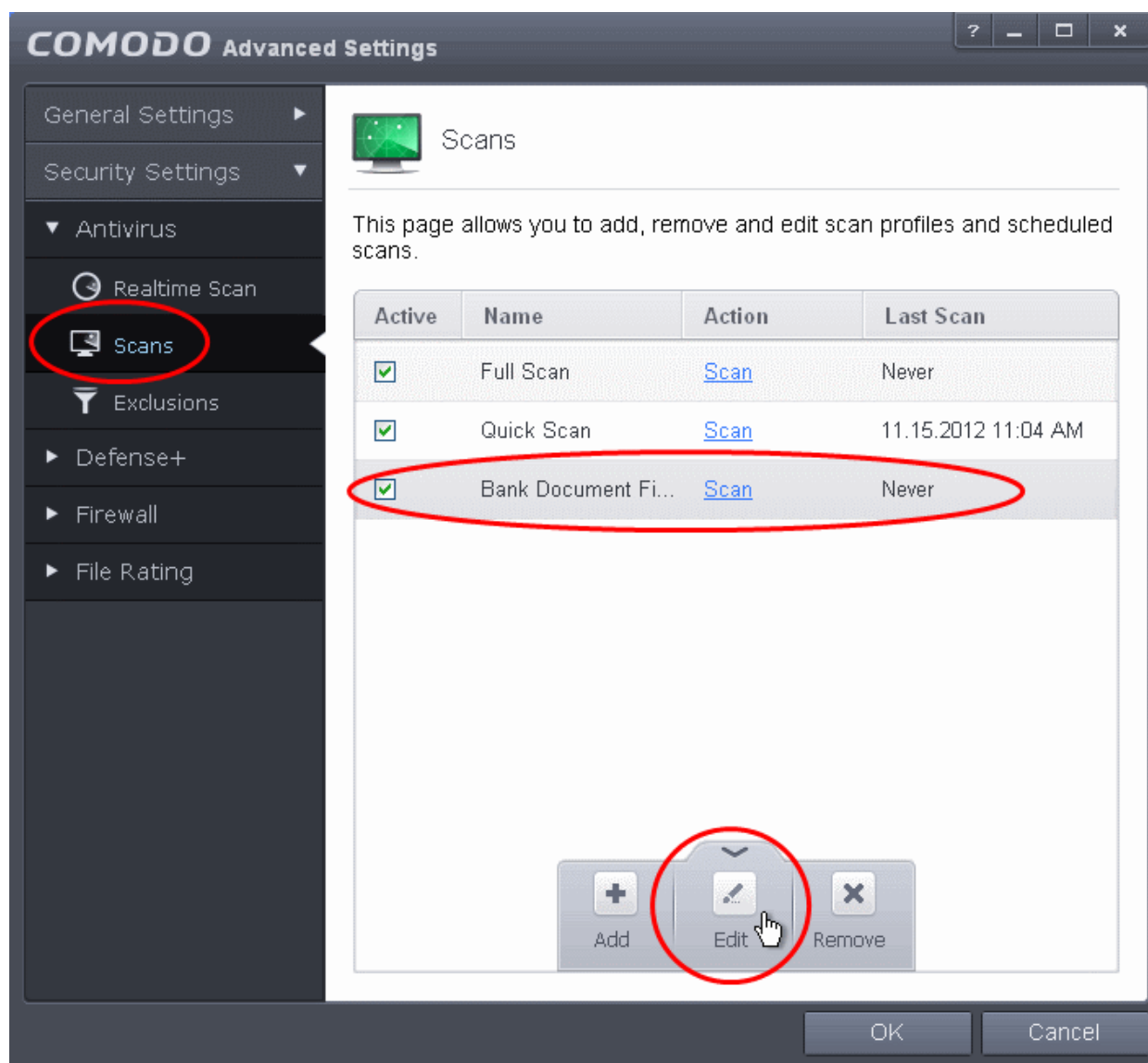
- If you want to suppress automatic updates when you are connected to Internet through certain networks
 - Select the 'Do NOT check updates if am using these connections' check-box
 - Then click the 'these connections'. The 'Connections' dialog will appear with the list of connections you use.



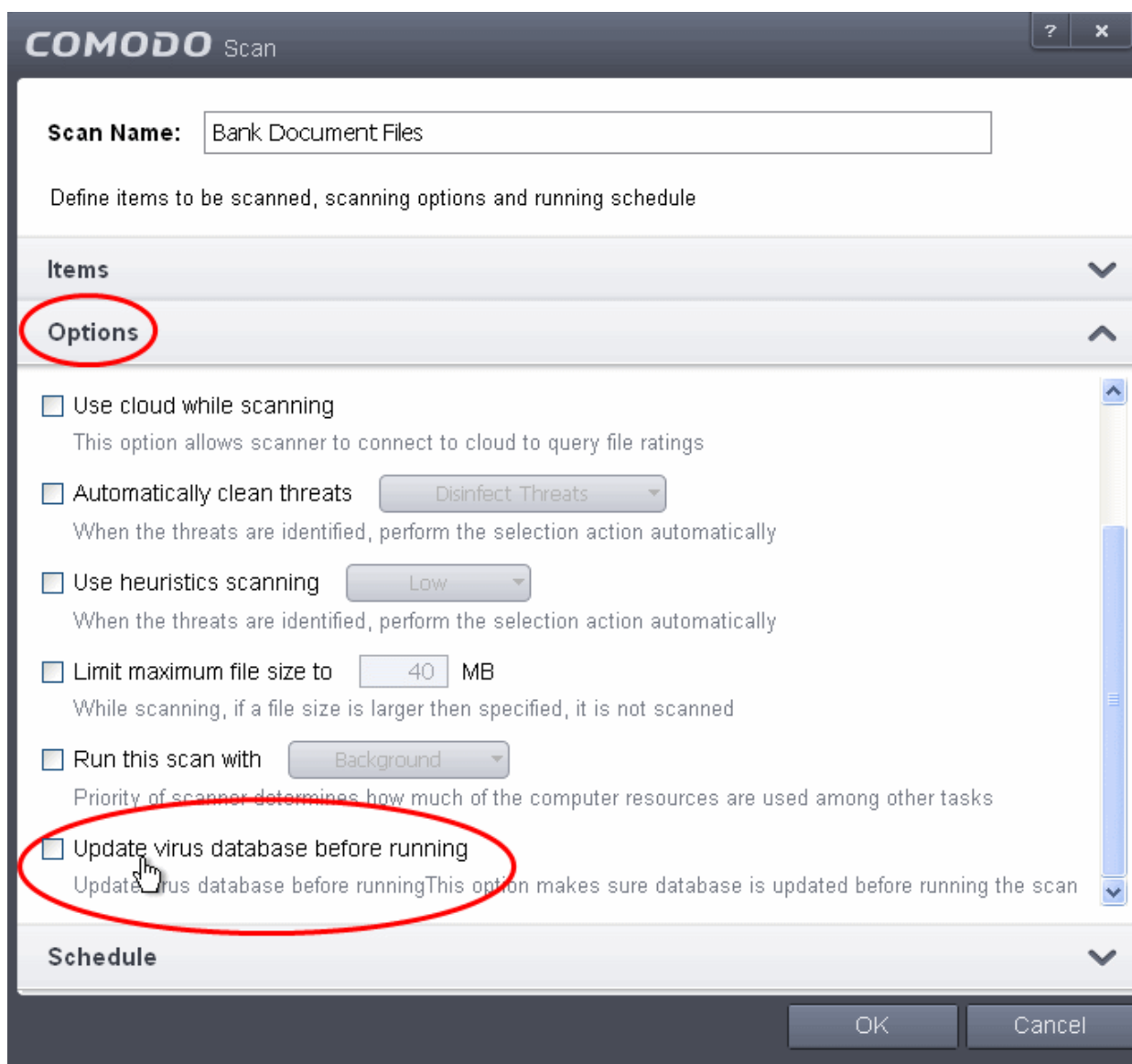
- Select the connection through which you do not want CIS to check for updates and click OK.
- If you want to suppress automatic updates when your computer is running on battery
 - Select the 'Do NOT check for updates if running on battery' checkbox

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



5. Click the handle from the bottom and select 'Edit'



6. Click 'Options' to open the Options pane 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.

Suppressing 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.

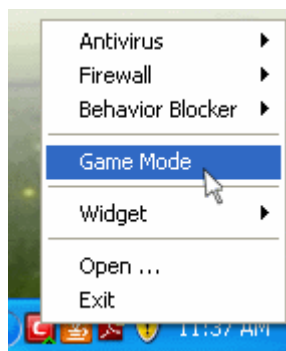
To temporarily stop pop-up alerts

- 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.

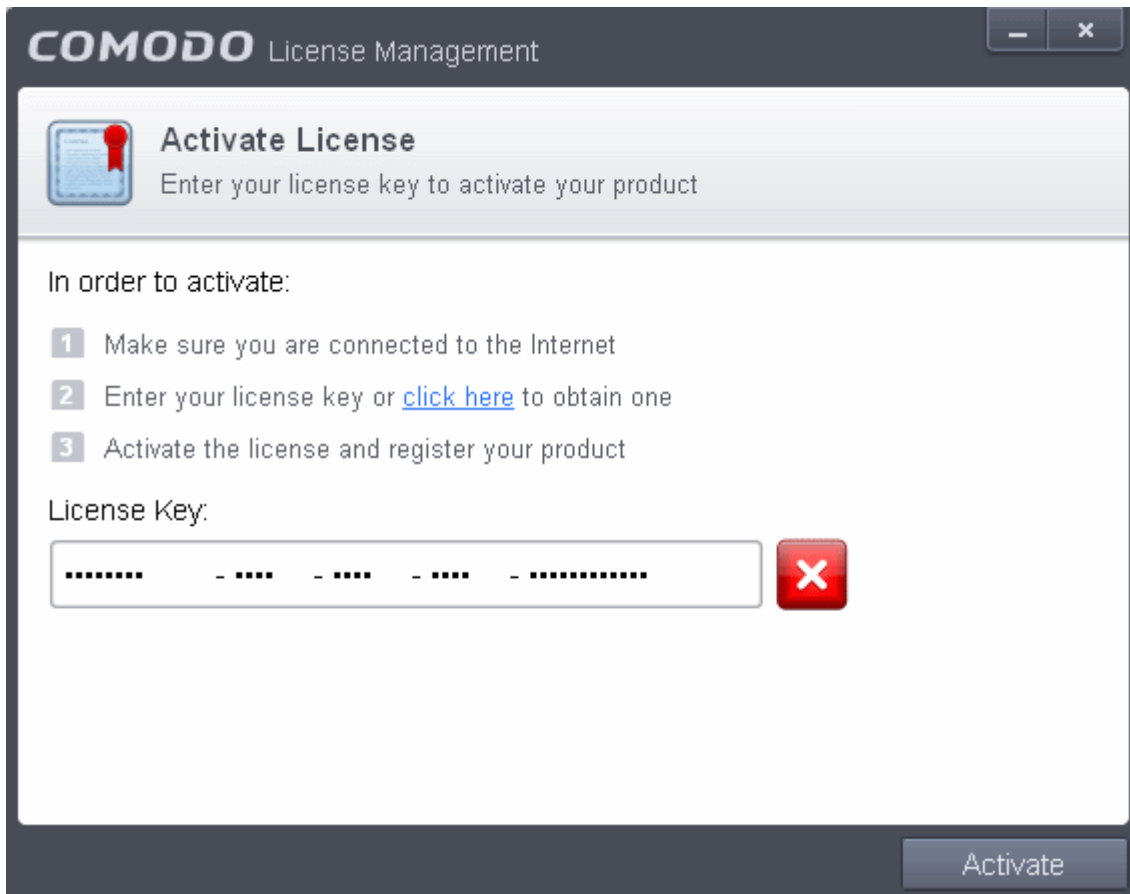
Renewing or Upgrading your License

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?afi=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 the 'Renew Now' button in the alert screen and follow the same purchase and activation procedure explained above.

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).

The screenshot shows a web interface titled "DNS AND ADVANCED SETTINGS". It contains a checkbox labeled "Use these DNS Servers:" which is currently unchecked. Below this are two text input fields: "Primary DNS Server:" and "Secondary DNS Server:". At the bottom left of the form is a blue button labeled "Advanced >>".

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.

The screenshot shows the same "DNS AND ADVANCED SETTINGS" web interface. The checkbox "Use these DNS Servers:" is now checked. The "Primary DNS Server:" field contains the text "8 . 26 . 56 . 26" and the "Secondary DNS Server:" field contains "8 . 20 . 247 . 20". The "Advanced >>" button remains at the bottom left.

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

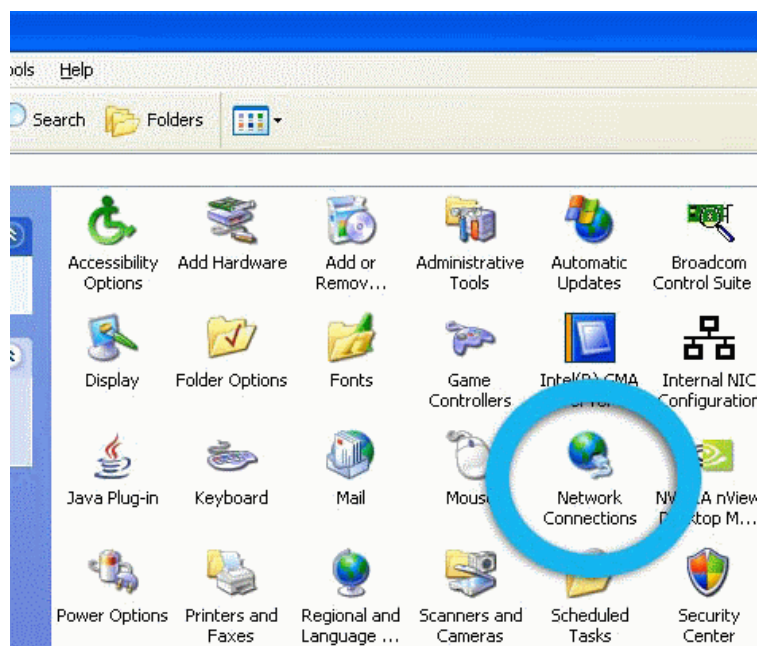
- **Modify the DNS server IP address to your previous settings.**

To modify the DNS settings

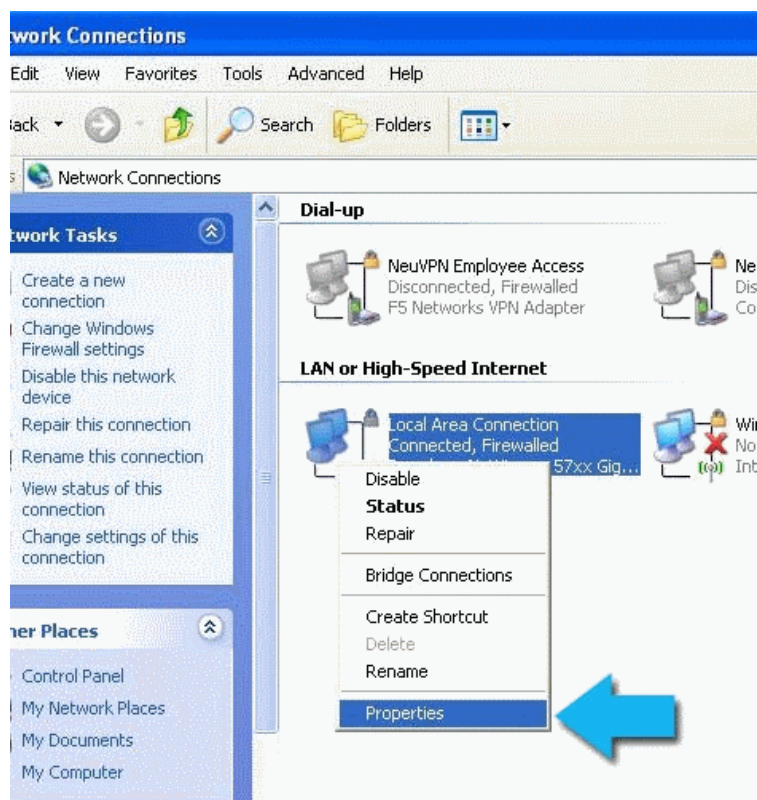
1. Select the 'Control Panel' from the Start Menu.



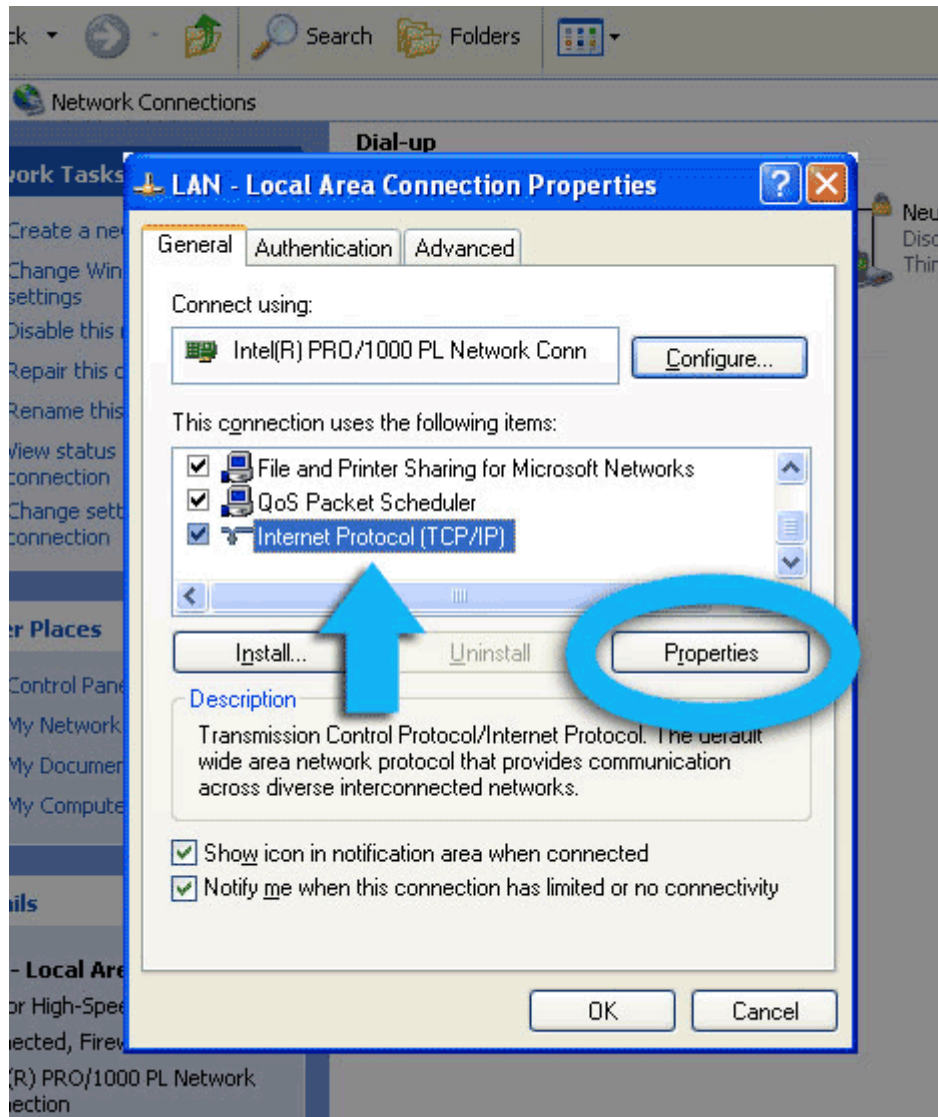
2. Click 'Network Connections' from the Control Panel options.



3. Right click on your connection from the Network Connections window and click 'Properties'.



4. Select 'Internet Protocol (TCP/IP)' and click 'Properties'.

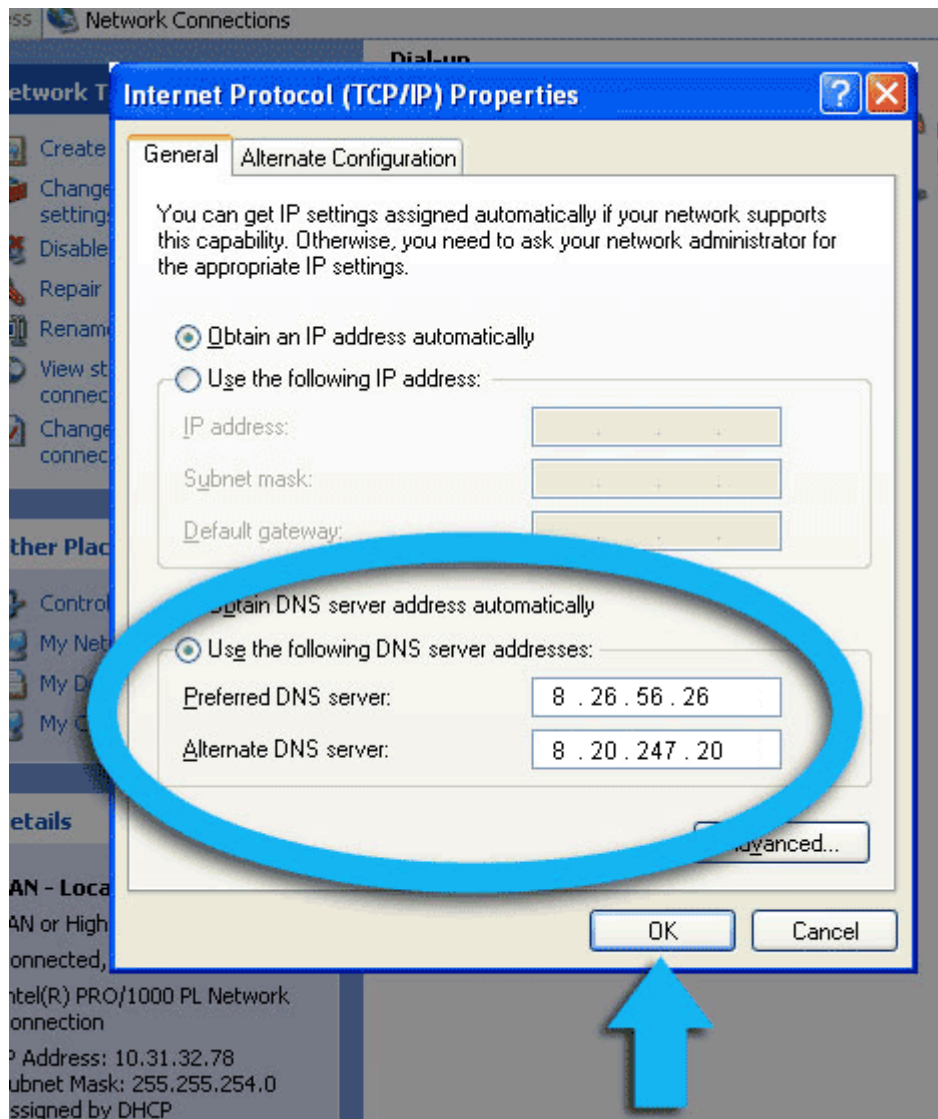


5. Click the radio button Use the following DNS server addresses and type in Comodo Secure DNS addresses in the Preferred DNS server and Alternate DNS server fields.

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.

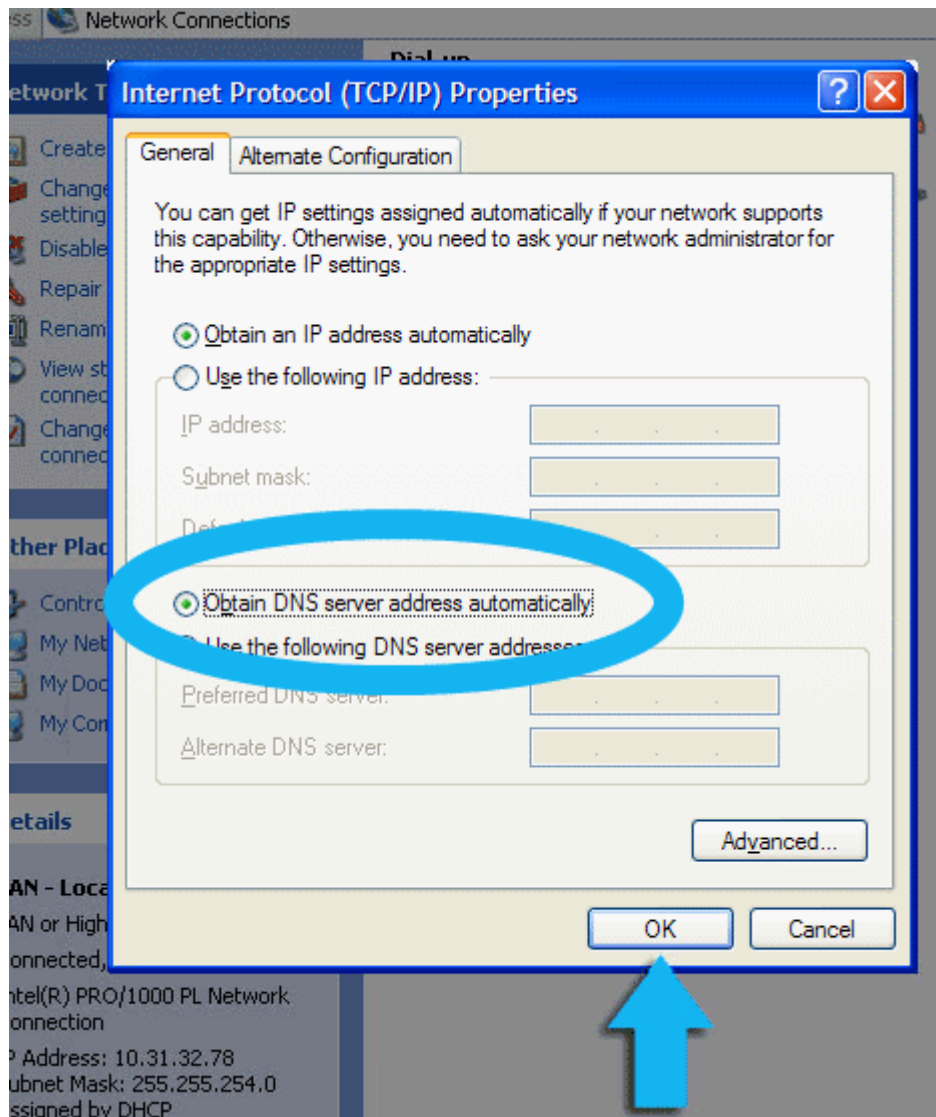
Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26

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:

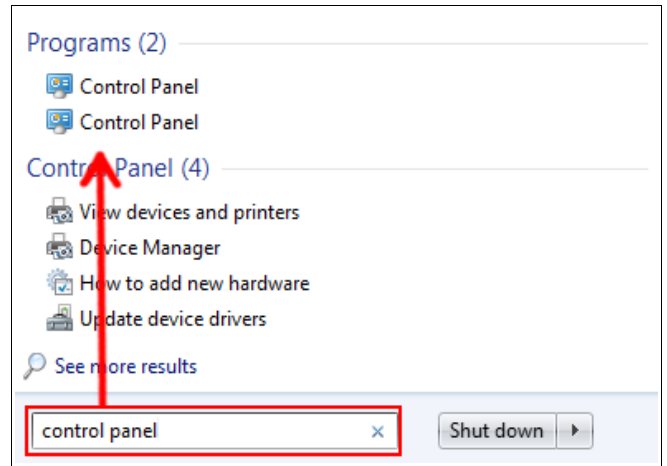
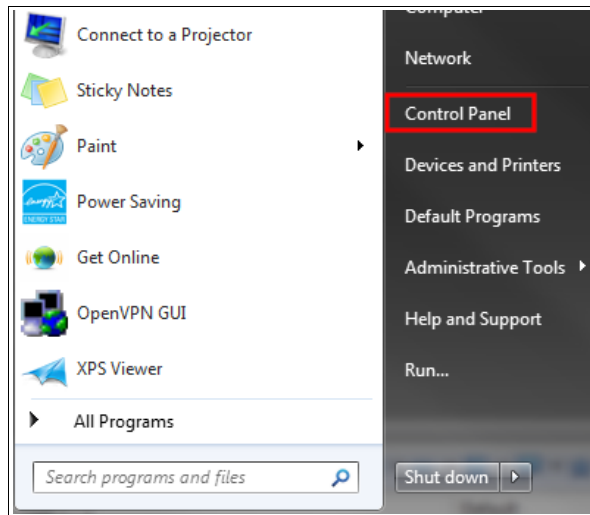
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

Enabling Comodo DNS in Windows 7 / Vista

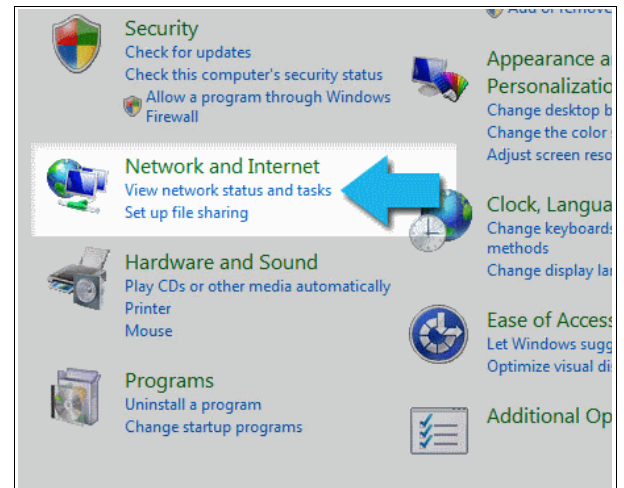
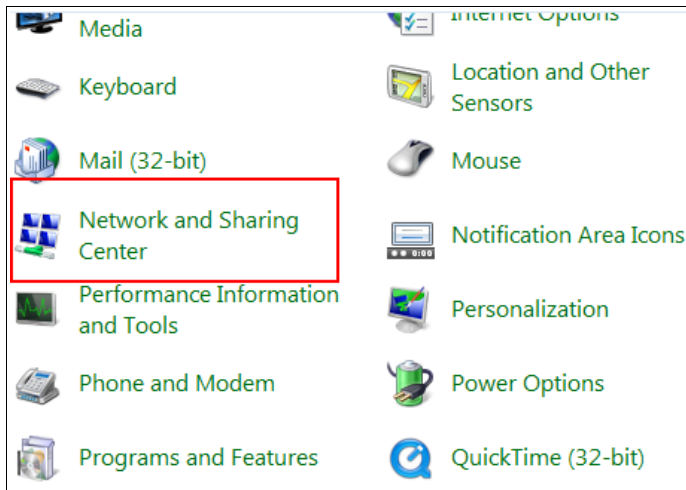
Disabling Comodo DNS in Windows 7 / Vista

Enabling Comodo DNS in Windows 7 / Vista

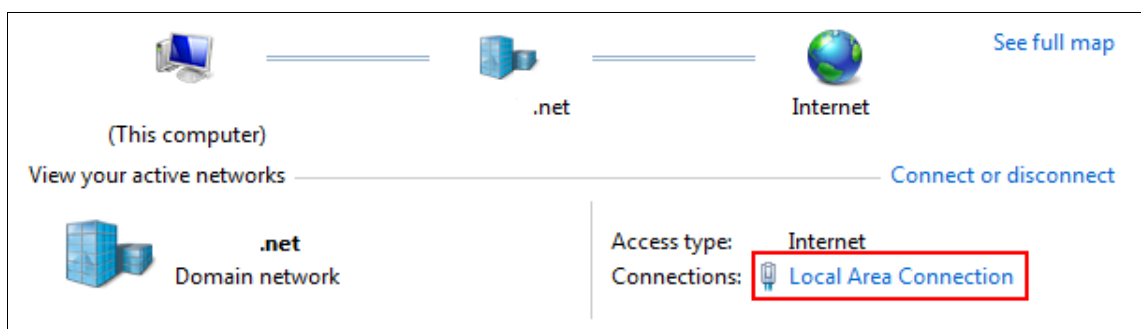
1. Open the control panel by either selecting it from the Windows 'Start' menu or by typing 'control panel' into the search box then clicking the program name.



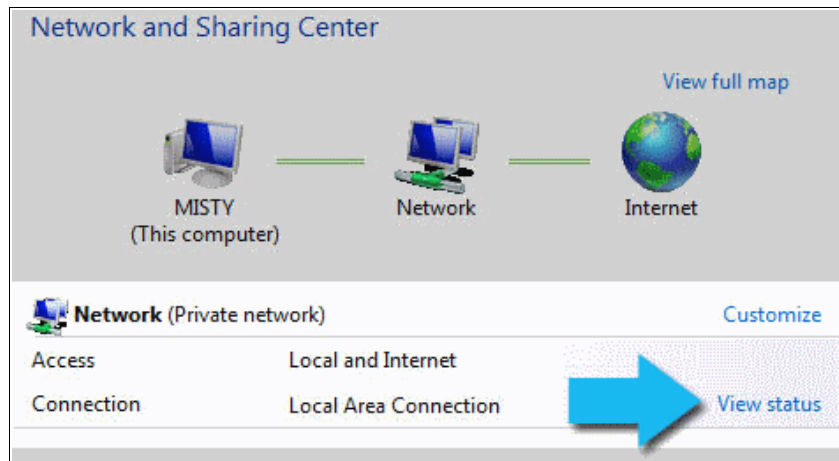
2. From the control panel menu, select 'Network and Sharing Center' (Windows 7) or 'Network and Internet (Vista):



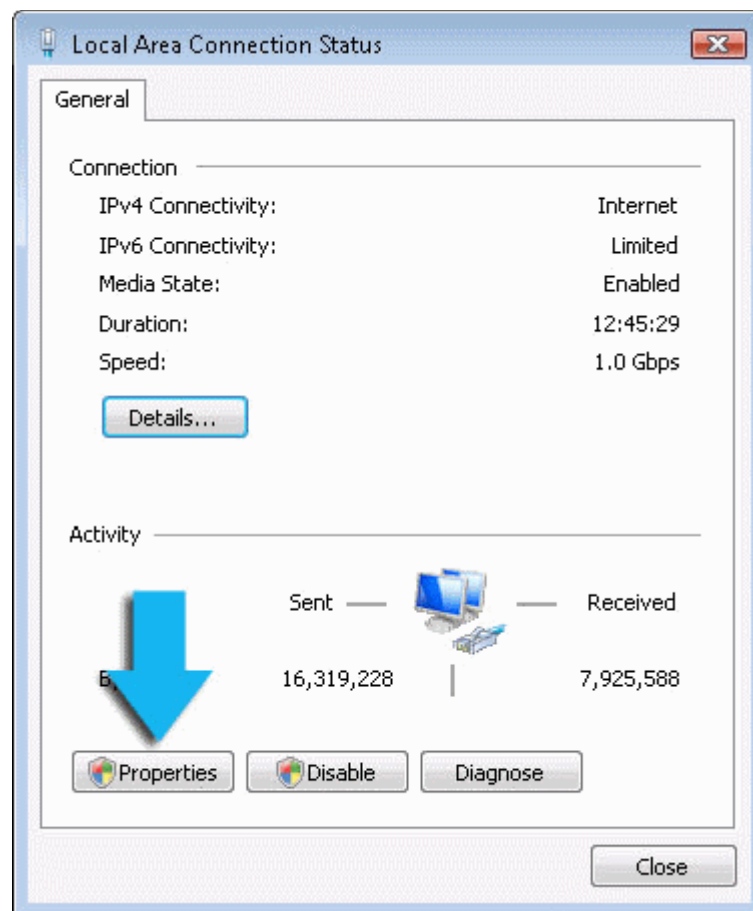
3. In the Network and Sharing center, click the connection type next to 'Connections' (Windows 7):



or 'View Status' (Vista):

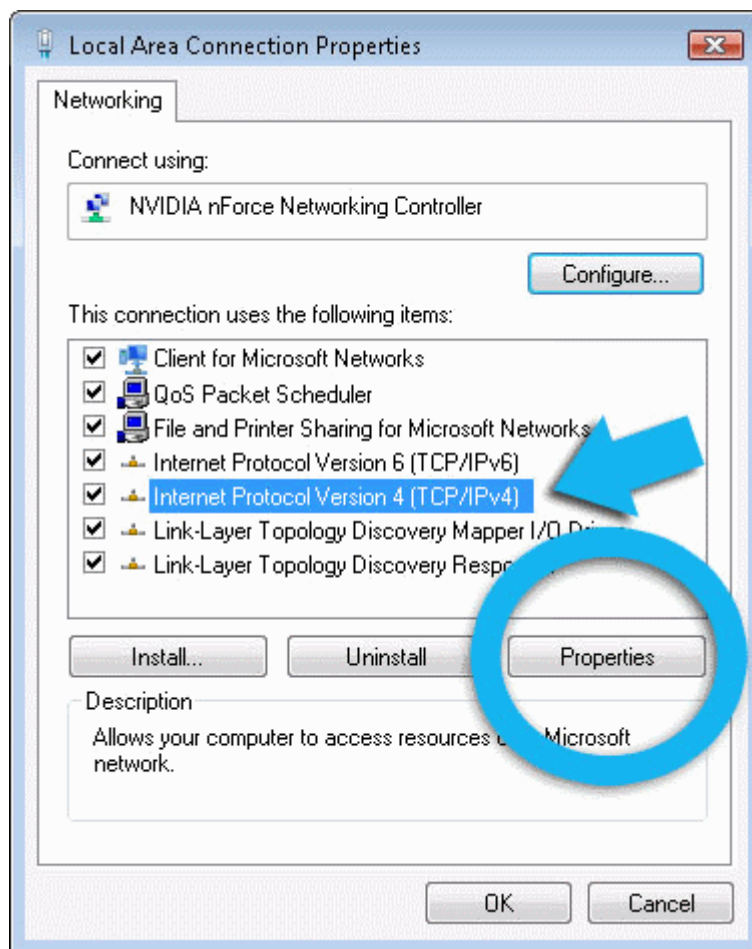


- This will open the 'Local Area Connection Status' dialog. Click the 'Properties' button:

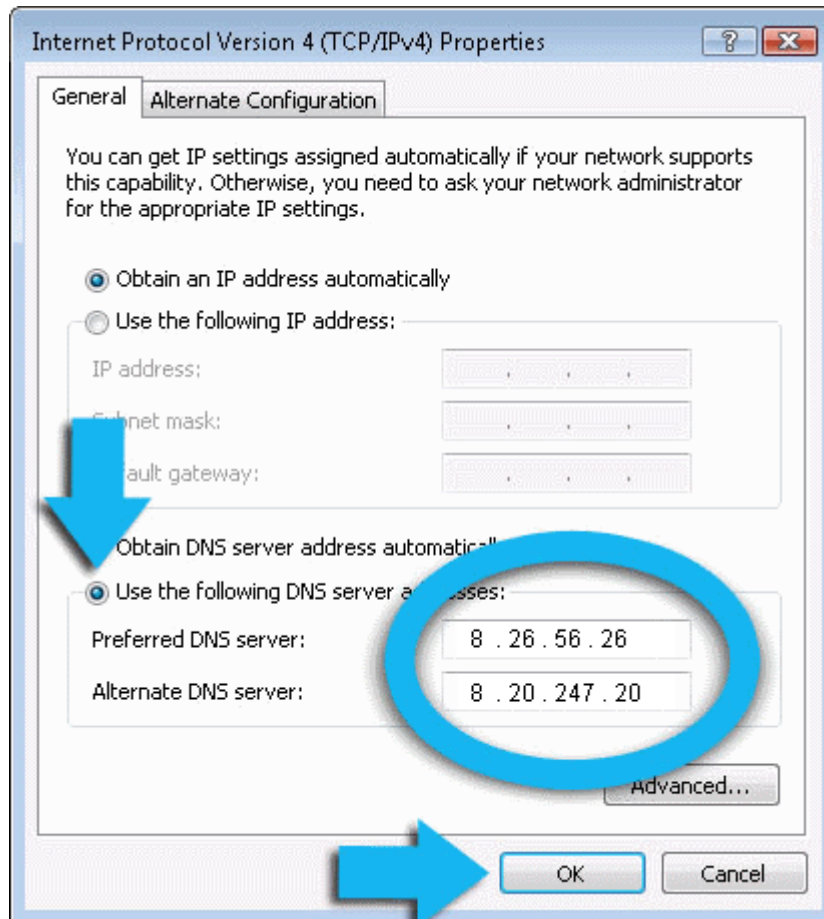


At this point, Windows might ask for your permission to continue or request that you enter an Administrator password.

- Once you have granted permission/entered an admin password, you will be presented with the 'Local Area Connection Properties' dialog. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button:



6. Enable 'Use the following DNS server addresses'. Doing so will allow you to enter the addresses of Comodo DNS servers in the fields provided. Enter the addresses listed below then click 'OK' to activate your settings:
 - Preferred DNS : 8.26.56.26
 - Alternate DNS : 8.20.247.20

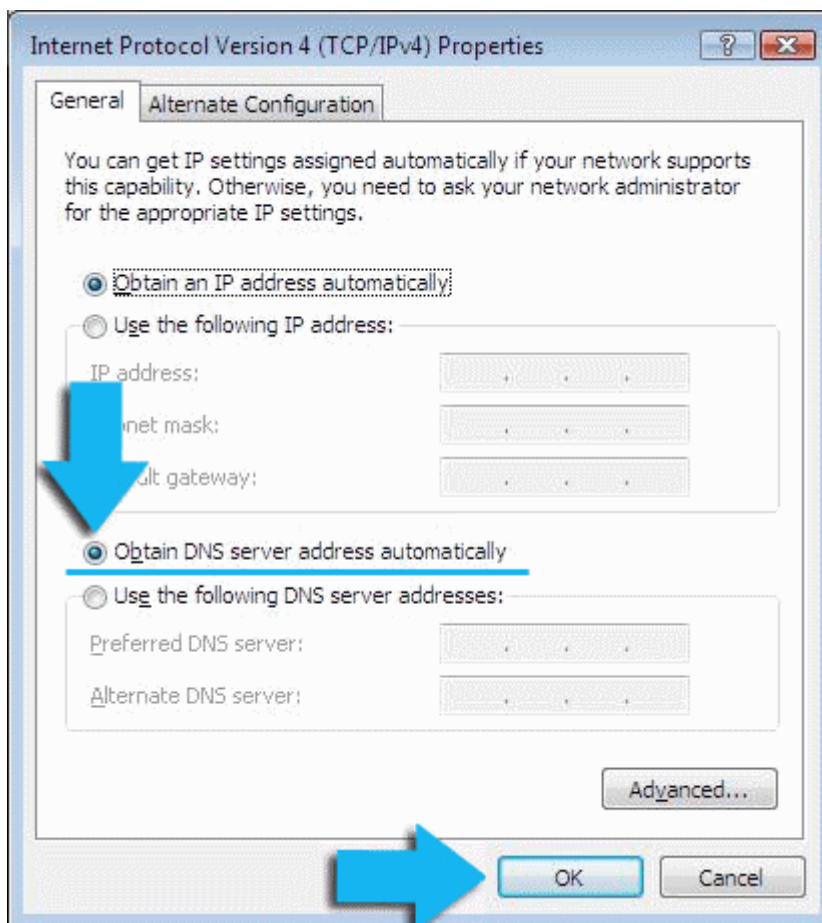


Your computer will now use Comodo DNS as its default domain name resolution service for all applications that connect to the Internet.

Disabling Comodo DNS in Windows 7 / Vista

To disable Comodo DNS, you need to instruct Windows to automatically obtain the address of a DNS server. Doing so means you will use the DNS server provided by your ISP. To do this:

- Follow steps 1 to 7 of the ['Enabling Comodo DNS in Windows 7 / Vista'](#) tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

Appendix 3 - 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 (10GB 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 Version 5.x	✓	✓	✗	✗	✗	✗	✗	Free
CIS Pro 2012	✓	✓	✓	✗	✗	✓	✓	\$49.99/year or \$4.95/month
CIS Complete 2012	✓	✓	✓	✓ (10 GB)	✓ (10 GB)	✓	✓	\$69.99/year or \$6.95/month
CIS Plus 2012	✓	✓	✓	✗	✗	✗	✓	\$39.99 or \$3.95/month
CIS Plus 2012 - International Edition	✓	✓	✓	✓ (10 GB)	✗	✗	✗	\$19.99/year
CAV Free	✓	✗	✗	✗	✗	✗	✗	Free
CAV Advanced 2012 - 30 Day Trial	✓	✗	✗	✗	✗	✗	✗	Free for one 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
STE 100
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>.