

**COMODO**  
Creating Trust Online®



# Comodo Internet Security 2011

Software Version 5.3

## User Guide

Guide Version 5.3.030111

Comodo Security Solutions Inc.  
525 Washington Blvd.  
Jersey City, NJ 07310  
United States

## Table of Contents

<b>1 Introduction to Comodo Internet Security</b> .....	<b>5</b>
1.1 Special Features.....	8
1.2 System Requirements.....	11
1.3 Installation.....	11
1.3.1 CIS Premium - Installation.....	11
1.3.2 CIS Pro- Installation and Activation.....	20
1.3.2.1 Installing Comodo Internet Security 2011 Pro and Live PC Support.....	21
1.3.2.2 Activating TrustConnect and Guarantee.....	27
1.3.3 CIS Complete - Installation and Activation .....	29
1.3.3.1 Installing Comodo Internet Security 2011 Complete and Live PC Support.....	30
1.3.3.2 Activating Online Backup, TrustConnect and Guarantee.....	35
1.3.3.3 Installing Comodo Backup.....	39
1.3.3.4 Installing Comodo TrustConnect.....	45
1.3.3.5 Installing Comodo Dragon Browser.....	52
1.3.4 Activating CIS Pro/Complete Services after Installation .....	57
1.3.4.1 Activating Your Subscription.....	57
1.3.4.2 Activating Your Guarantee Coverage.....	60
1.3.4.3 Renewal of Your Subscription.....	65
1.4 Starting Comodo Internet Security.....	66
1.5 Overview of Summary Screens.....	67
1.5.1 Comodo Internet Security - Summary.....	68
1.5.2 Comodo Antivirus - Summary.....	70
1.5.3 Comodo Firewall - Summary.....	71
1.6 Comodo Internet Security - Navigation .....	72
1.7 Understanding Alerts.....	73
<b>2 Antivirus Tasks - Introduction</b> .....	<b>86</b>
2.1 Run a Scan.....	87
2.2 Update Virus Database.....	97
2.3 Quarantined Items.....	98
2.4 View Antivirus Events.....	100
2.5 Submit Files to Comodo for Analysis.....	110
2.6 Scheduled Scans.....	112
2.7 Scan Profiles.....	114
2.8 Scanner Settings.....	118
2.8.1 Real Time Scanning .....	119
2.8.2 Manual Scanning.....	120
2.8.3 Scheduled Scanning .....	122
2.8.4 Exclusions.....	124
<b>3 Firewall Tasks - Introduction</b> .....	<b>126</b>
3.1 View Firewall Events.....	126
3.2 Define a New Trusted Application.....	133
3.3 Define a New Blocked Application.....	135
3.4 Network Security Policy.....	136
3.4.1 General Navigation.....	137
3.4.2 Application Rules.....	138
3.4.3 Global Rules.....	148
3.4.4 Predefined Policies.....	150

3.4.5 Network Zones.....	151
3.4.6 Blocked Zones.....	155
3.4.7 Port Sets.....	157
3.5 View Active Connections.....	161
3.6 Stealth Ports Wizard.....	162
3.7 Firewall Behavior Settings.....	165
3.7.1 General Settings.....	165
3.7.2 Alert Settings.....	167
3.7.3 Advanced Settings.....	169
<b>4 Defense+ Tasks - Introduction.....</b>	<b>170</b>
4.1 The Sandbox - An Introduction.....	171
4.1.1 Unknown Files: The Sand-boxing and Scanning Processes.....	172
4.2 View Defense+ Events.....	174
4.3 Trusted Files.....	180
4.4 Unrecognized Files.....	181
4.4.1 Unrecognized Files.....	182
4.4.2 Submitted Files.....	185
4.5 Computer Security Policy.....	185
4.5.1 Defense+ Rules.....	186
4.5.2 Predefined Policies.....	191
4.5.3 Always Sandbox.....	192
4.5.4 Blocked Files.....	196
4.5.5 Protected Files and Folders.....	197
4.5.6 Protected Registry Keys.....	200
4.5.7 Protected COM Interfaces.....	203
4.5.8 Trusted Software Vendors.....	205
4.6 View Active Process List.....	210
4.7 Run a Program in the Sandbox.....	211
4.8 Defense+ Settings.....	212
4.8.1 General Settings.....	213
4.8.2 Execution Control Settings.....	215
4.8.3 Sandbox Settings.....	219
4.8.4 Monitoring Settings.....	221
<b>5 More Options-Introduction.....</b>	<b>223</b>
5.1 Preferences.....	223
5.1.1 General Settings.....	224
5.1.2 Parental Control Settings.....	225
5.1.3 Appearance.....	226
5.1.4 Log Settings.....	228
5.1.5 Connection Settings.....	230
5.1.6 Update Settings.....	231
5.2 Manage My Configurations.....	231
5.2.1 Comodo Preset Configurations.....	232
5.2.2 Importing/Exporting and Managing Personal Configurations.....	233
5.3 Diagnostics.....	237
5.4 Check for Updates.....	238
5.5 Browse Support Forums.....	240
5.6 Help .....	241

5.7 About.....	242
<b>6 Comodo GeekBuddy.....</b>	<b>242</b>
6.1 Overview of Services.....	243
6.2 Launching the Client and Using the Service.....	243
6.3 Accepting Remote Desktop Requests.....	247
6.4 Registration.....	249
6.5 Activation of Service.....	249
6.6 Uninstalling Comodo GeekBuddy.....	251
<b>7 Live PC Support.....</b>	<b>253</b>
7.1 Overview of the Services.....	253
7.2 Launching the Client and Requesting the Service.....	254
7.3 Uninstalling Live PC Support Client.....	257
<b>8 TrustConnect Overview.....</b>	<b>258</b>
8.1 Microsoft Windows - Configuration and Connection .....	259
8.2 Mac OS X - Configuration and Connection .....	262
8.3 Linux / Open VPN - Configuration and Connection .....	262
8.4 Apple iPhone / iPod Touch - Configuration and Connection.....	264
8.5 TrustConnect FAQ.....	266
<b>Appendix 1 Comodo Secure DNS Service.....</b>	<b>274</b>
Router - Manually Enabling or Disabling Comodo Secure DNS Service.....	274
Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service.....	276
Windows Vista - Manually Enabling or Disabling Comodo Secure DNS Service.....	280
<b>About Comodo.....</b>	<b>287</b>

# 1 Introduction to Comodo Internet Security

## Overview

Comodo Internet Security 2011 offers 360° protection against internal and external threats by combining a powerful Antivirus protection, an enterprise class packet filtering firewall, and an advanced host intrusion prevention system called Defense+.

CIS is available in Premium (free), Pro and Complete editions. Whilst the core CIS software is identical for all three versions, the Pro and Complete packages each offer a range of additional services. These include services such as **LivePCSupport** (Comodo support experts available 24/7 to fix any problem with your computer); **TrustConnect** (secure Internet proxy service that ensures 128 bit encrypted connectivity from any public wireless hotspot); Online Backup (10GB of online storage space) and the Comodo 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. See terms and conditions for full details. Available to USA residents only). The free, Premium version offers a 60 day free trial of **Comodo GeekBuddy**.

New features in CIS 2011 include Cloud based antivirus scanning and behavior analysis, user-friendly application white-listing, new spyware and rootkit scanners, improved malware cleaning, an all new 'game mode', full support for IPv6, improved Defense+ application compatibility and a completely re-designed interface.

When used individually, each of the Antivirus, Firewall and Defense+ components deliver 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.

The screenshot displays the Comodo Internet Security 2011 Premium interface. The top navigation bar includes tabs for Summary, Antivirus, Firewall, Defense+, and More. The Summary tab is active, showing a dashboard with the following information:

- Antivirus:** Stateful. The virus database has been updated on **Never Updated**. 0 threat(s) detected so far. A **Scan Now** button is present.
- Defense+:** Safe Mode. Defense+ has blocked 0 intrusion(s) so far. 0 unrecognized file(s) observed / will be treated as **Partially Limited**. 0 application(s) currently running in the sandbox.
- Firewall:** Safe Mode. Firewall has blocked 0 intrusion(s) so far. 1 outbound connection(s) and 0 inbound connection(s) are shown. A **Stop All Traffic** button is present.
- Traffic:** System traffic is at 100.0%.

On the left side, a warning icon indicates that the virus signature database is NOT up-to-date, with an **Update Now** button. The bottom left corner shows the version: 5.0.154916.1032 and Antivirus database version: 1.

## Comodo Internet Security Features:

- **Antivirus** - The proactive antivirus system that automatically detects and eliminates viruses, Worms and Trojan horses.
- **Firewall** - The Firewall that constantly defends your system from inbound and outbound Internet attacks with a highly effective packet filtering firewall.
- **Defense+** - A rules based intrusion prevention system that protects your critical operating system files from malicious processes, internal attacks and blocks unknown malware before it ever gets a chance to install. Defense+ now features automated sandboxing of unknown applications. The sandbox ensures untrusted (but harmless) applications are allowed freedom to operate whilst untrusted (and genuinely malicious) applications are prevented from accessing or infecting your computer.
- **Live PC Support** (*Pro and Complete versions only*) - a 24 x 7 online support service in which Comodo experts remotely access your computer when you need it, for:
  - Virus Diagnosis/ Removal;
  - PC Tune-up;
  - Internet Login Protection;
  - Email Account Setup;
  - Software Installation;
  - Printer Setup/ Troubleshooting;
  - Optimizing your computer's power settings;
  - Computer Troubleshooting.
- **Secure Wireless Internet Connectivity** (*Premium, Pro and Complete versions*) - TrustConnect makes surfing the web safe from any public Wi-Fi location (10 GB per month)
- **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. See terms and conditions for full details. Available to USA residents only.
- **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).

Comodo Internet Security can be used 'out of the box' - so even the most inexperienced users need not have to deal with complex configuration issues after installation.

Comodo Internet Security alerts you whenever potential malware attempts to attack or gain access to your system. The alerts are displayed as pop-ups at the right hand corner of your screen and allow you to allow or block the unrecognized activities, processes and connection attempts of running applications (CIS now even protects against 'drive-by-download' buffer overflow attacks.)

## 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**
- **Starting Comodo Internet Security**
- **General Navigation**
- **Understanding Alerts**

The next four sections of the guide cover every aspect of the configuration of Comodo Internet Security. The final two sections contain configuration and technical help for the **Live PC Support** and **TrustConnect**.

- **Antivirus Task Center**
  - [Run a Scan](#)
  - [Update a Virus Database](#)
  - [Quarantined Items](#)
  - [Viewing Antivirus Events](#)
  - [Submit Files to Comodo for Analysis](#)
  - [Scheduled Scans](#)
  - [Scan Profiles](#)
  - [Scanner Settings](#)
    - [Real Time Scanning](#)
    - [Manual Scanning](#)
    - [Scheduled Scanning](#)
    - [Exclusions](#)
- **Firewall Task Center**
  - [Overview of Task Interface](#)
  - [View Firewall Events](#)
  - [Define a New Trusted Application](#)
  - [Define a New Blocked Application](#)
  - [Network Security Policy](#)
    - [General Navigation](#)
    - [Application Rules](#)
    - [Global Rules](#)
    - [Predefined Policies](#)
    - [Network Zones](#)
    - [Blocked Zones](#)
    - [Port Sets](#)
  - [View Active Connections](#)
  - [Stealth Ports Wizard](#)
  - [Firewall Behavior Settings](#)
    - [General Settings](#)
    - [Alert Settings](#)
    - [Advanced Settings](#)
- **Defense+ Task Center**
  - [Overview of Task Interface](#)
    - [The Sandbox - An Introduction](#)
  - [View Defense+ Events](#)
  - [Trusted Files](#)
  - [Unrecognized Files](#)
    - [Unrecognized Files](#)
    - [Submitted Files](#)
  - [Computer Security Policy](#)
    - [Defense+ Rules](#)
    - [Predefined Policies](#)
    - [Always Sandbox](#)
    - [Blocked Files](#)
    - [Protected Files and Folders](#)
    - [Protected Registry Keys](#)
    - [Protected COM Interfaces](#)
    - [Trusted Software Vendors](#)

- [View Active Process List](#)
- [Run a Program in the Sandbox](#)
- [Defense+ Settings](#)
  - [General Settings](#)
  - [Execution Control Settings](#)
  - [Sandbox Settings](#)
  - [Monitoring Settings](#)
- **More... Options**
  - [Preferences](#)
    - [General Settings](#)
    - [Parental Control Settings](#)
    - [Appearance](#)
    - [Log Settings](#)
    - [Connection Settings](#)
    - [Update Settings](#)
  - **Manage My Configuration**
  - [Diagnostics](#)
  - [Check For Updates](#)
  - [Browse Support Forums](#)
  - [Help](#)
  - [About](#)
- **Live PC Support**
  - [Live PC Support](#)
    - [Overview of the Services](#)
    - [Launching the Client and Requesting the Service](#)
    - [Uninstalling Live PC Support Client](#)
- **TrustConnect**
  - [TrustConnect Overview](#)
  - [Windows Configuration](#)
  - [Mac OS X Configuration](#)
  - [Linux / OpenVPN Configuration](#)
  - [Apple iPhone / iPod Touch Configuration](#)
  - [TrustConnect FAQ](#)
- **Appendix 1 Comodo Secure DNS Service**
  - [Comodo Secure DNS Overview](#)
  - [Router Manually Enabling or Disabling Comodo Secure DNS Service](#)
  - [Windows XP Manually Enabling or Disabling Comodo Secure DNS Service](#)
  - [Windows Vista Manually Enabling or Disabling Comodo Secure DNS Service](#)

## 1.1 Special Features

### Defense+ Host Intrusion Prevention System

- Virtually Bulletproof protection against root-kits, inter-process memory injections, key-loggers and more;
- 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 new Sandbox feature to completely isolate untrusted files from the rest of your computer

## 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;
- 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;
- 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 60 day Free Trial (Premium version only)

Comodo Internet Security Premium (Free version) users can get the 60 day trial Comodo GeekBuddy service - Live expert remote support for virtually all of your personal computer issues. Comodo computer experts establish a remote desktop connection to your machine and fix your computer's problems right in front of your 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

**Note:** The trial service is for a period of sixty days only. 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.

## Live PC Support (Pro and Complete versions only)

Comodo Internet Security, Pro and Complete customers receive LivePCSupport - the easiest and most comprehensive way of getting your computer problems fixed. The support services are delivered by a Comodo security expert accessing your computer through a remote desktop. The services include:

- Virus Diagnosis/ Removal
- PC Tune-up
- Internet Login Protection
- Email Account Setup
- Software Installation
- Printer Setup/ Troubleshooting
- Green PC
- Computer Troubleshooting

Please visit <http://livepcsupport.com> for full product details. Please visit <http://personalfirewall.comodo.com> to sign up for CIS Pro package.

## Comodo TrustConnect (Pro and Complete versions only)

Included with a Pro or 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 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 a 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 includes the buffer-overflow protection of Comodo Memory Firewall. On the attempt of a buffer overflow attack, CIS raises a pop-up alert. This provides protection against data theft, computer crashes and system damage, which are possible consequences of a buffer overflow attack.

### '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 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 sandboxing technology 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 7 (Both 32-bit and 64-bit versions), Windows Vista (Both 32-bit and 64-bit versions) or Windows XP (Both 32-bit and 64-bit versions)
- Internet Explorer Version 5.1 or above
- 128 MB available RAM
- 210 MB hard disk space for both 32-bit and 64-bit versions

## 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 LivePCSupport 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 LivePCSupport, TrustConnect, Online Storage and the Comodo Guarantee. Activation of additional services is carried out after the base installation has been completed.

Click the links below for detailed explanations:

- [CIS Premium - Installation](#)
- [CIS Pro - Installation](#)
- [CIS Complete - Installation](#)

### 1.3.1 CIS Premium - Installation

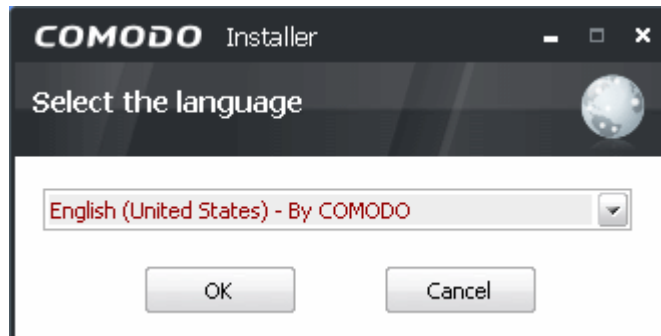
To install, download the Comodo Internet Security setup files to your local hard drive. (setup.exe can be downloaded from <http://www.personalfirewall.comodo.com>)

After downloading the Comodo Internet Security setup file to your local hard drive, double click on

cispremium\_installer.exe  to start the installation wizard.

## Step 1 - Choosing the Interface Language

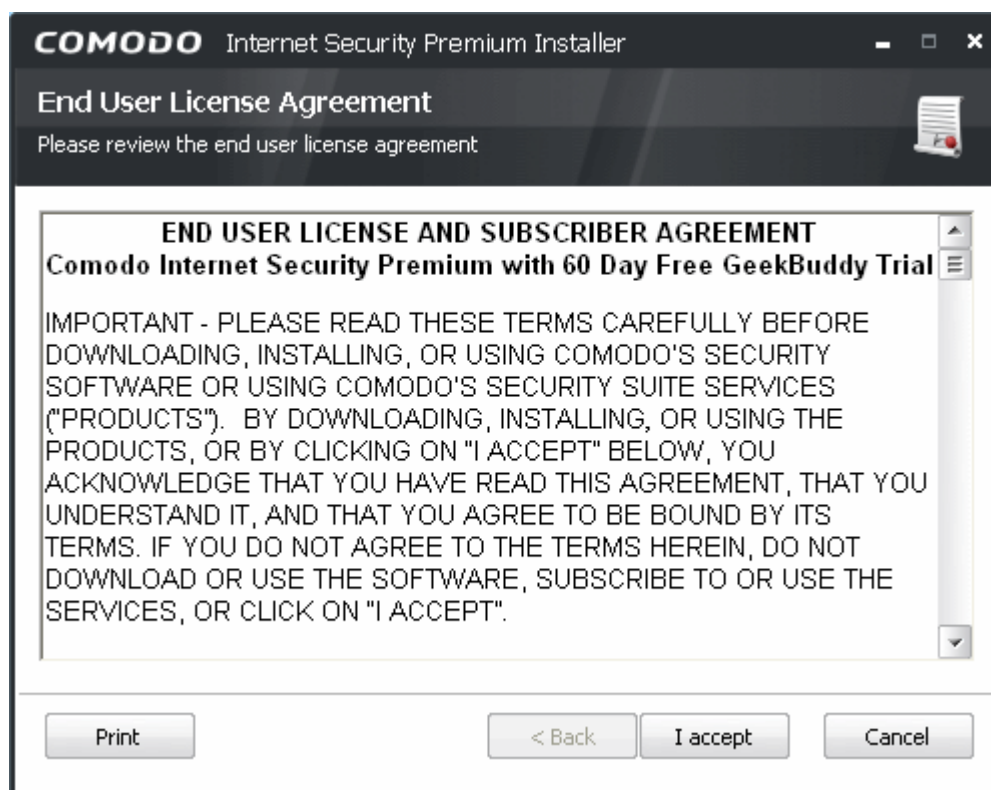
The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



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

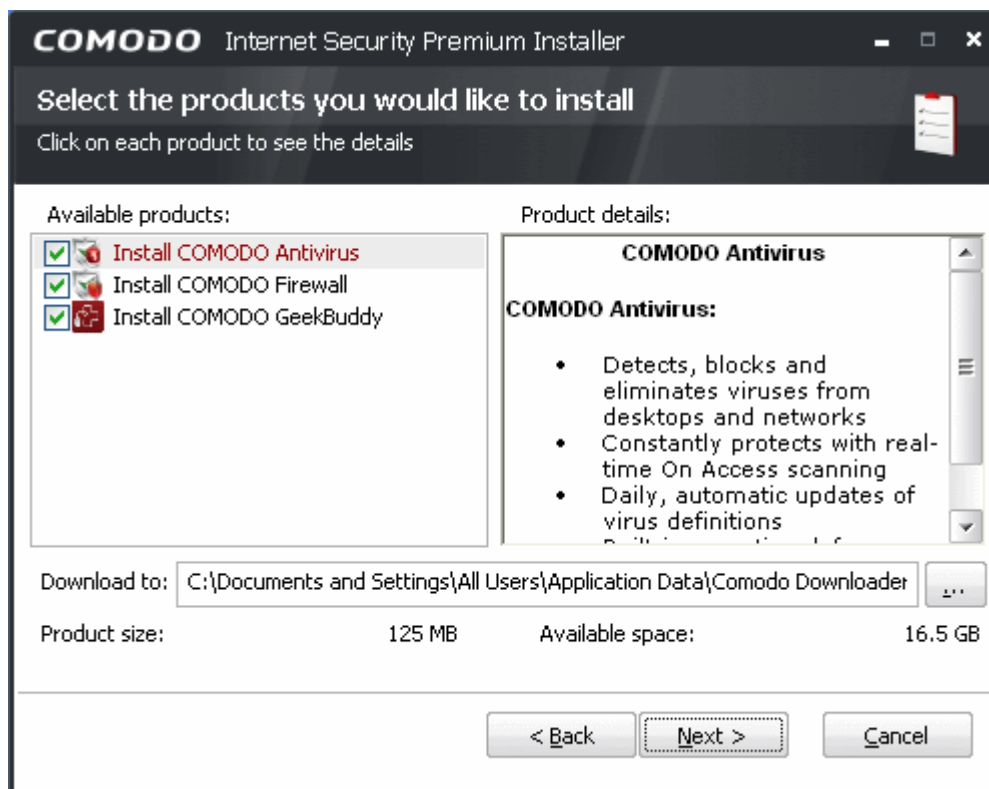
## Step 2 - End User License Agreement

The End-User License Agreement dialog box will be displayed.



To continue with the installation, you must read and then accept the End User License Agreement (EULA). Click 'I accept' to continue the installation. If you want to cancel the installation at this stage, click 'Cancel'.

### Step 3 - Select the Components to Install

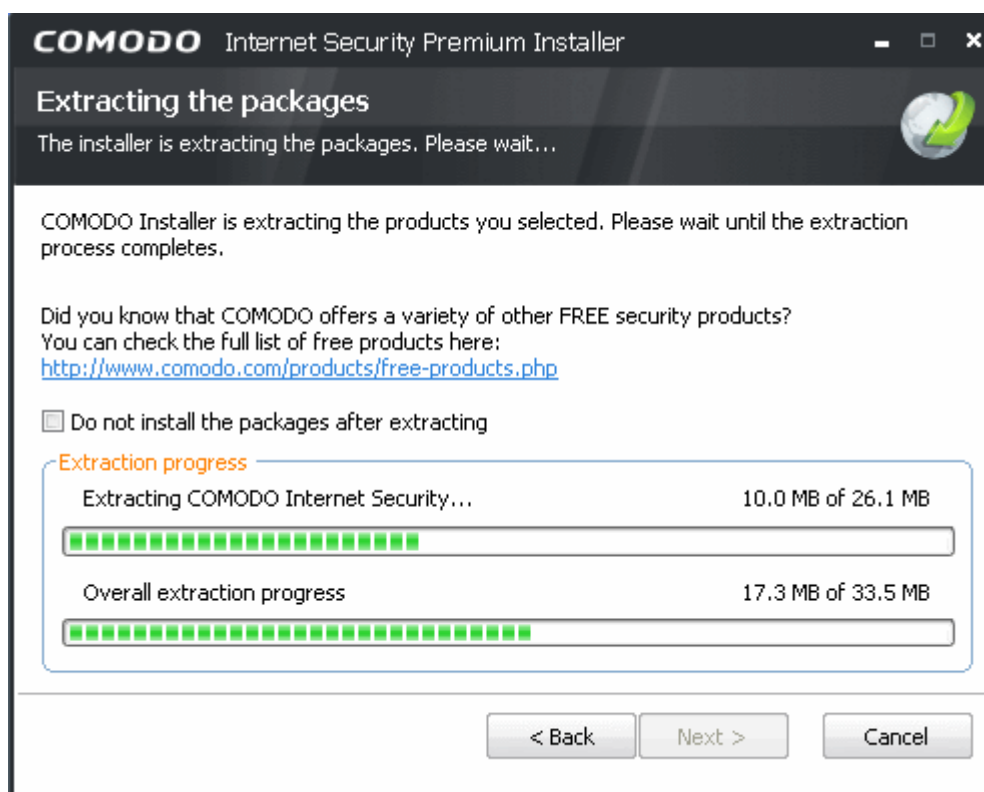


The next step is to choose which elements you would like to install. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select both the Comodo Antivirus and Comodo Firewall options (installation of both is mandatory for Pro and Complete customers). CIS Pro and Complete customers will also need to install Comodo TrustConnect to take advantage of the service (this is optional for users of the free product).

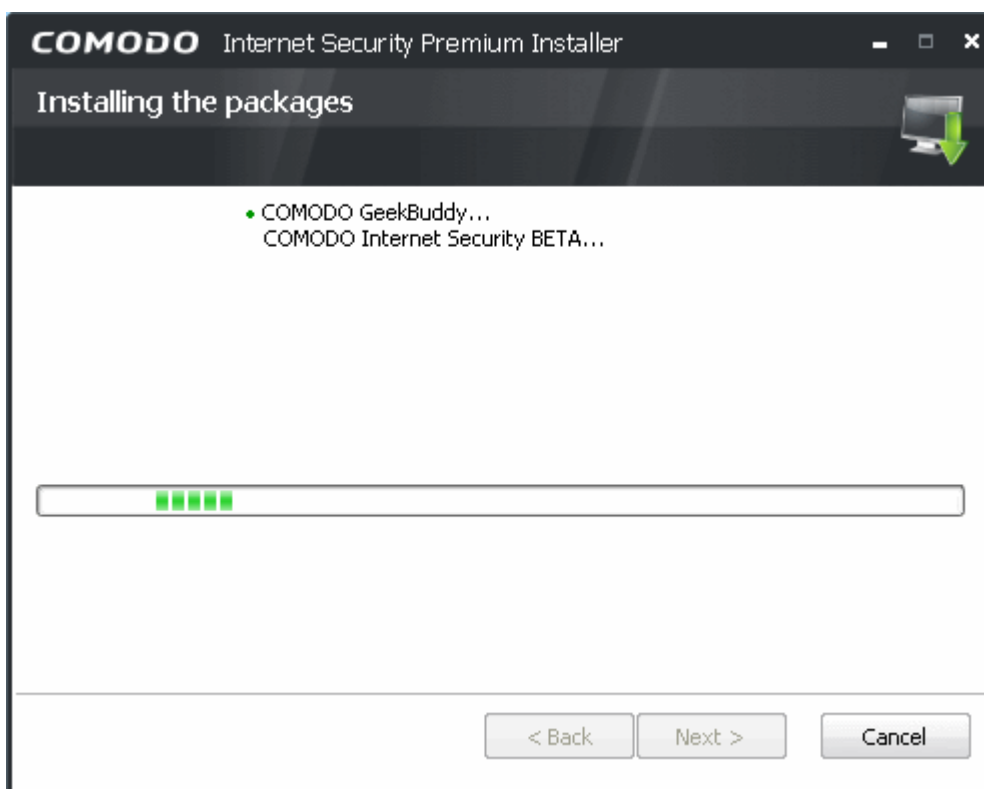
- **Install COMODO Firewall** - Selecting this option installs Comodo Firewall and Defense+ components. De-select this option, if you already have third party Firewall protection activated in your computer system. Installing Comodo Firewall is a mandatory requirement if you are a Premium, Pro or Complete customer. If you choose to install the firewall BUT NOT the antivirus then you will be asked to configure the firewall security settings in Step 6.
- **Install COMODO Antivirus** - Selecting this option installs Comodo Antivirus and Defense+ components. De-select this option, if you already have a third party virus protection activated in your computer system. Installing Comodo Antivirus is a mandatory requirement if you are a Premium, Pro or Complete customer.
- **Install COMODO GeekBuddy** - Selecting this option installs 60 day free trial version of GeekBuddy, a 24 x 7 Remote assistance support service in which Comodo experts remotely access your computer when you need it for getting help with computer related problems. Refer to the section [Comodo GeekBuddy](#) for more details.

### Step 4 - Extracting and Installing the Packages

The setup will extract the files required for installing the selected components...

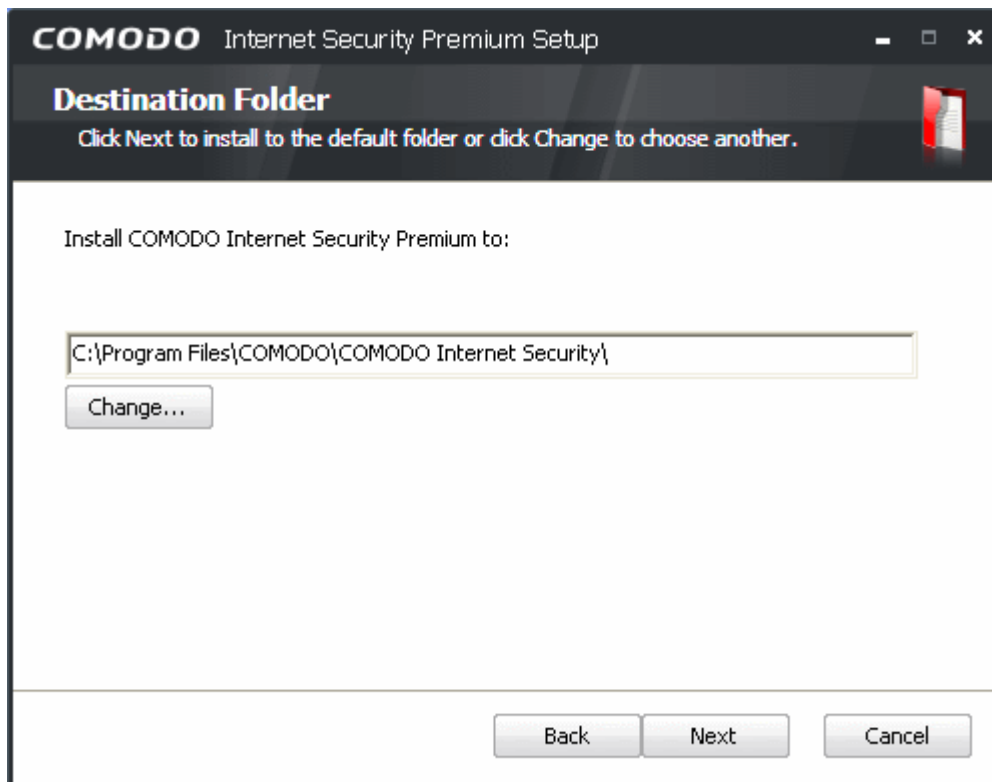


... and will start installing.



## Step 5 - Select Installation Folder

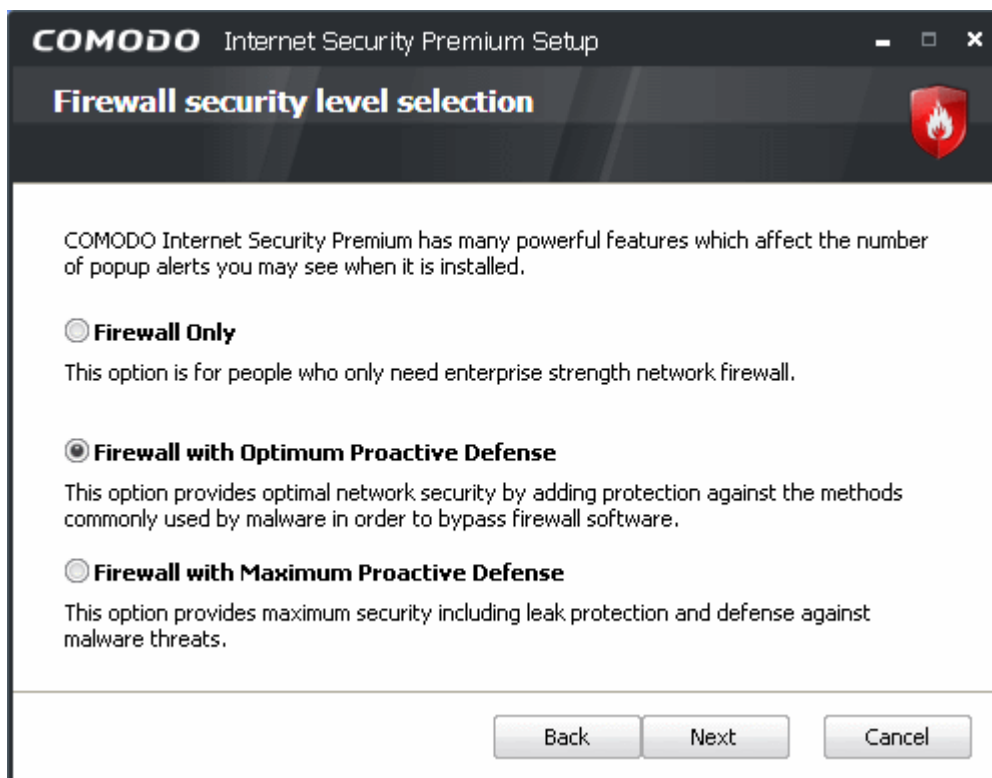
The next screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\Comodo\Comodo Internet Security.



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

## Step 6 - Firewall Configuration

If you chose not to install the antivirus and GeekBuddy components then you are provided with the opportunity to set the security level of the Firewall. If you have chosen to install both antivirus and firewall and GeekBuddy components, the wizard skips this step and goes to [step 7](#).





The options available are;

**Firewall only** - This option is only recommended for *experienced* firewall users that have alternative Host Intrusion Prevention software installed on their systems. Selecting this option will install ONLY the packet filtering network firewall and not Defense+ (Defense+ is essential for blocking malicious software like worms and Trojans from making outgoing connection attempts). This isn't to say this option is an unwise choice (the network firewall is one of the strongest available - offering highly effective and configurable inbound and outbound protection) but it is important to realize that, on it's own, it does not offer the host intrusion protection as afforded by Defense+.

**Firewall with Optimum Proactive Defense** - Selecting this option will install the packet filtering Comodo Firewall with Defense+. Defense+ is installed with optimum protection settings. This also sets the default configuration for security settings to optimum level. [Click here](#) for more details on default protection level.

**Firewall with Maximum Proactive Defense** - This is the most complete option and offers the greatest level of security. Selecting this will install Comodo Firewall with Defense+. Defense+ settings are set to the highest protection levels. This also sets the default configuration for security settings to maximum level. [Click here](#) for more details on default protection level.

Select the option of your choice and click 'Next'.

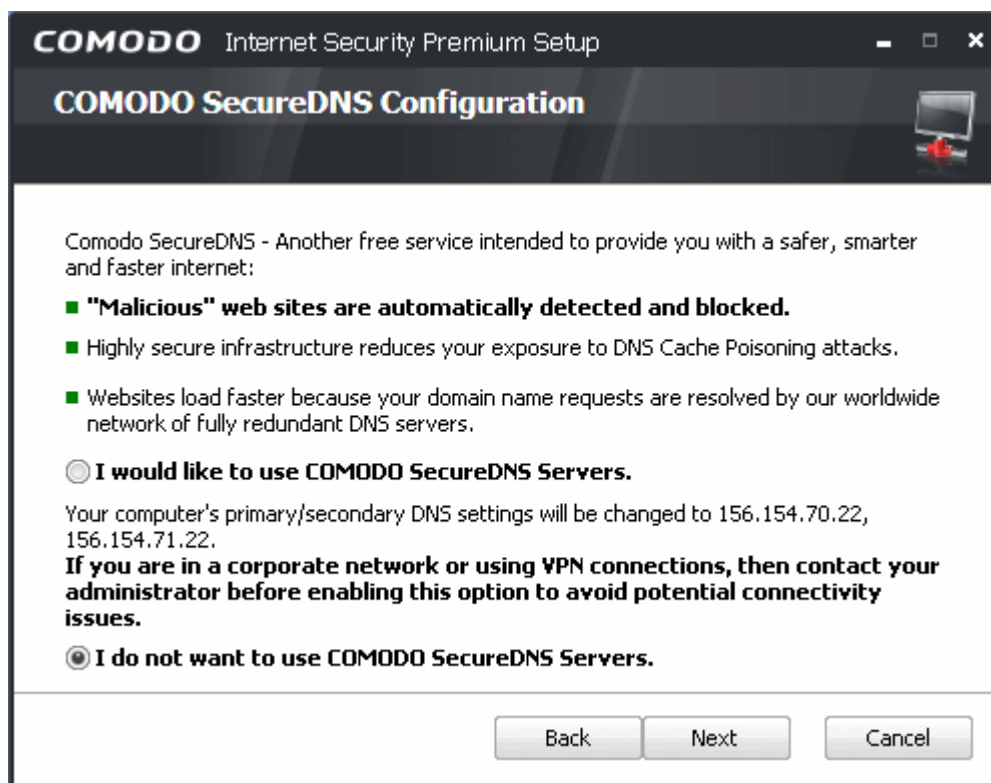
## Step 7 - Configuring your DNS Settings

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 1 Comodo Secure DNS Service](#).

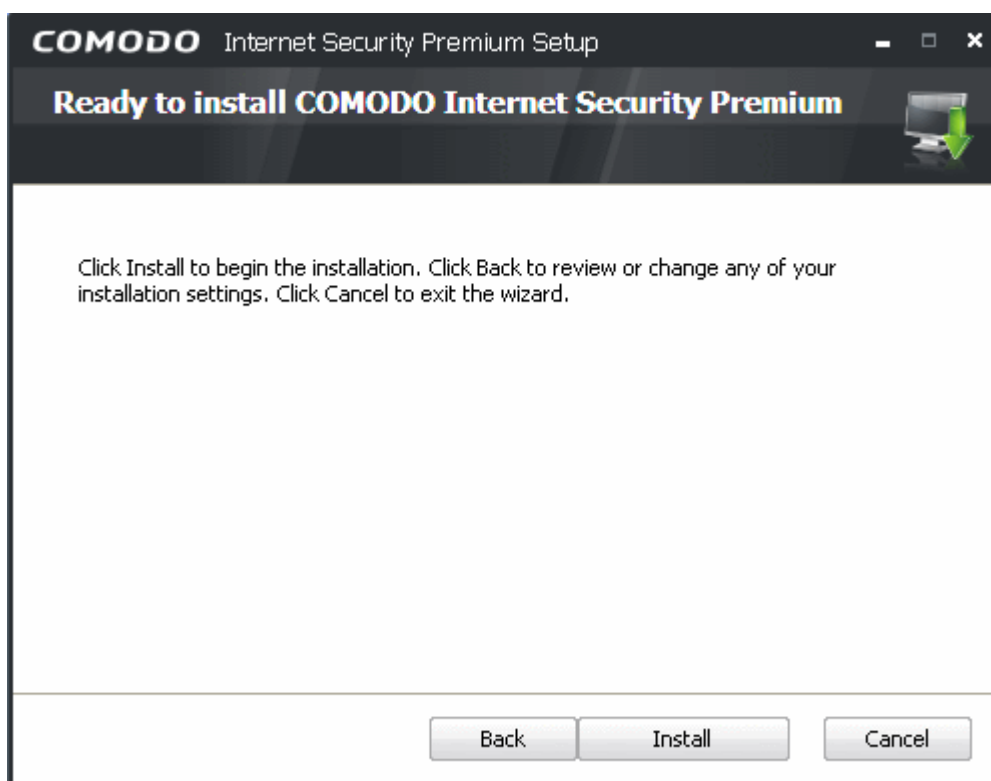


To enable the Comodo Secure DNS Service, select **I Would like to use Comodo Secure DNS Servers** and click 'Next'.

## Step 8 - Installation Progress

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



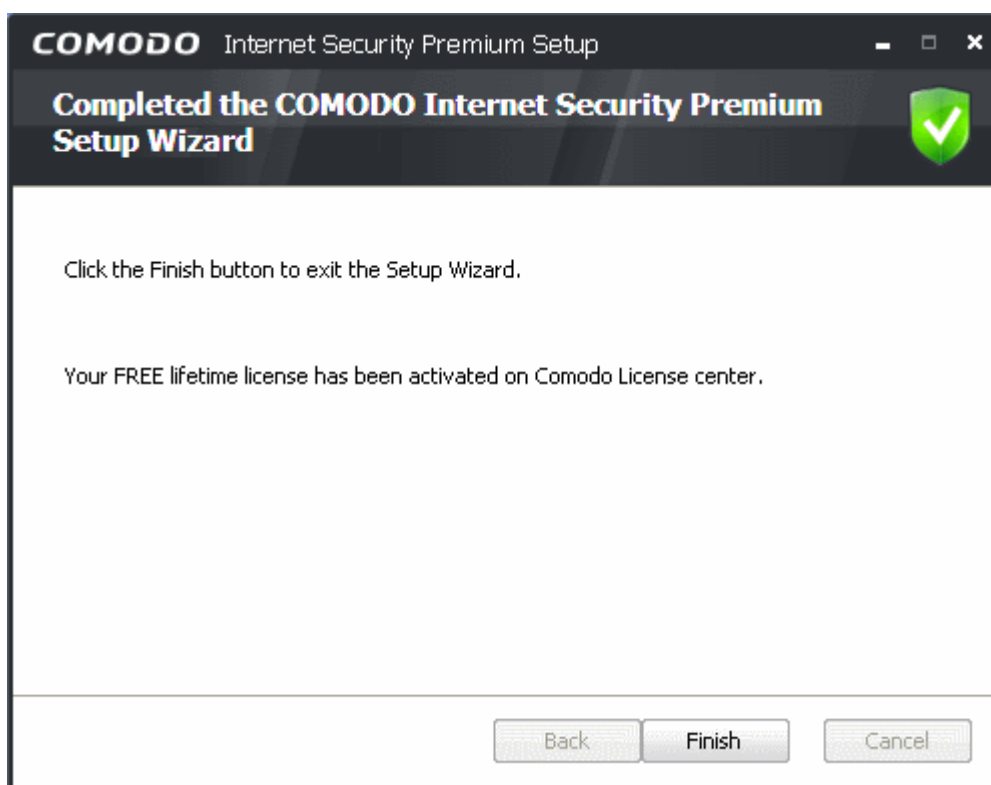


Click the 'Back' button to review and/or modify any of settings you have previously specified. To confirm your choices and begin the installation of Comodo Internet Security, click 'Install'.

The installation progress will be indicated...



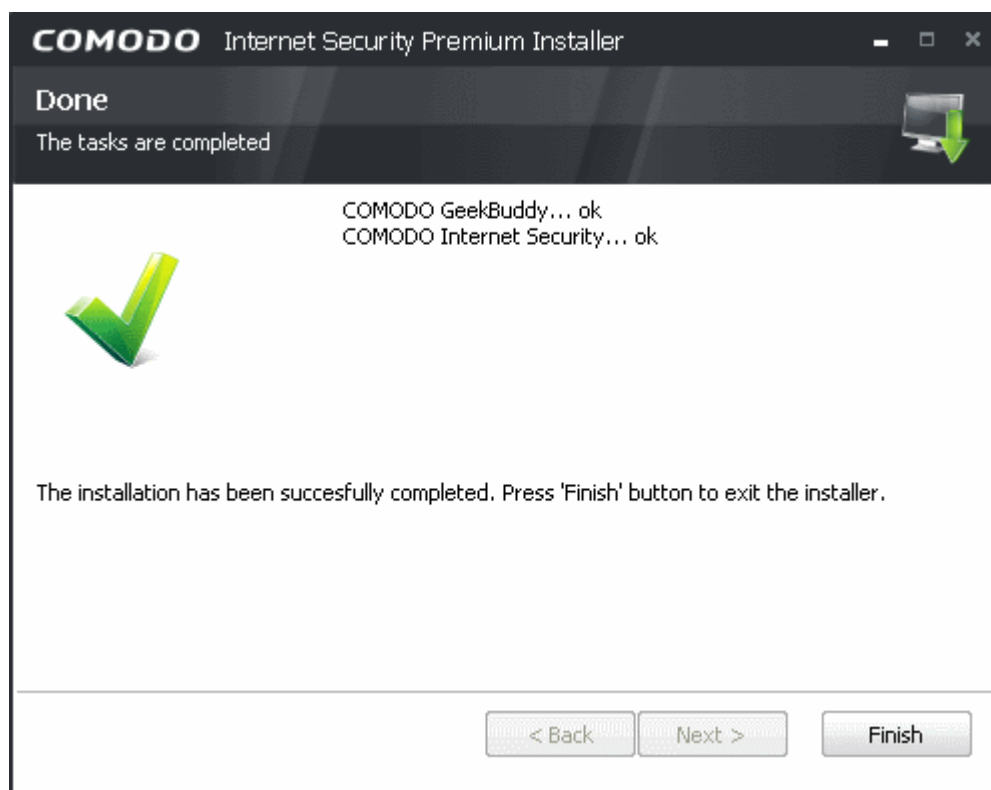
... and on completion, the finish dialogue will be displayed.



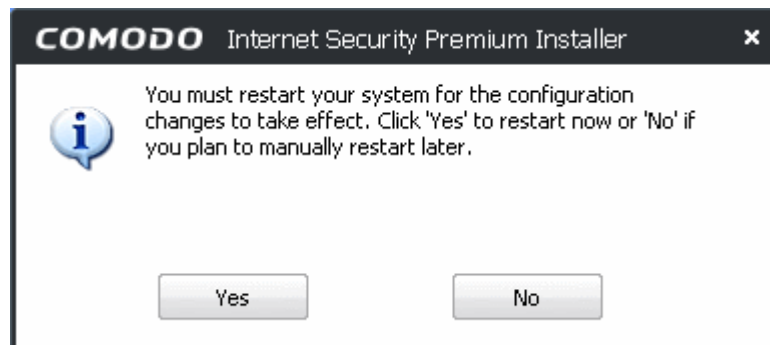
Click 'Finish' .

### Step 9 - Setup Completion and Restarting Your System

On successful setup completion, a confirmation dialog will be displayed.



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

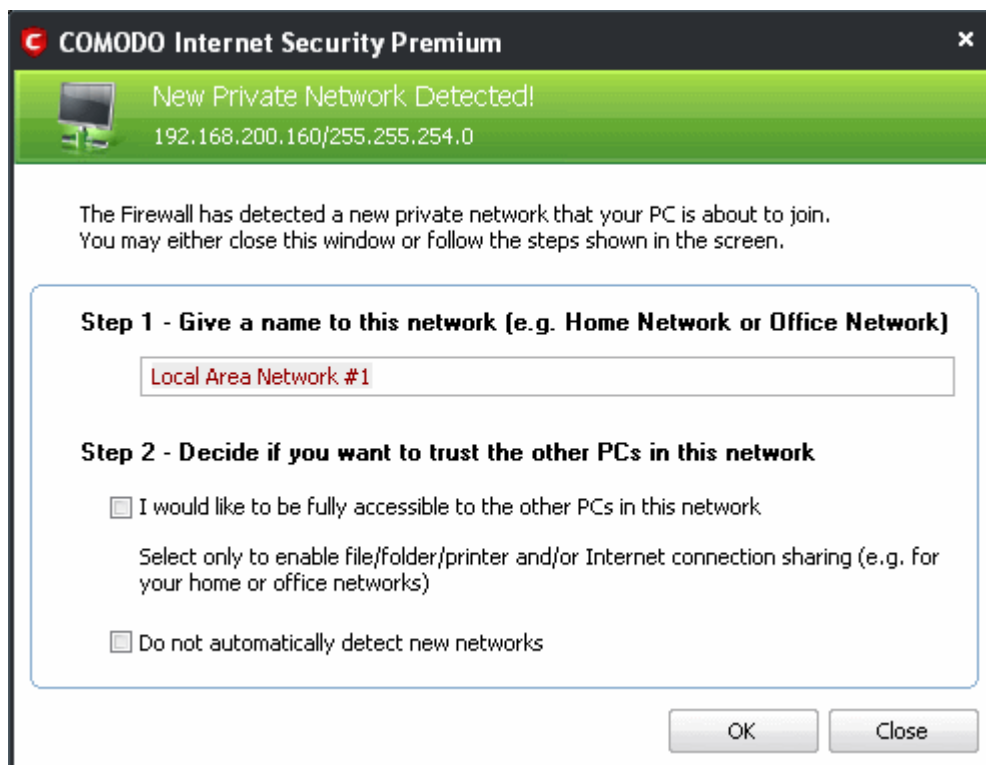


Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

## Step 10 - After Restarting Your System

After restarting, if your computer is connected to a home or work network, then you are prompted to configure it at the 'New Private Network Detected!' dialog:



**Step 1:** Even home users with a single computer have to configure a home network in order to connect to Internet. (this is usually displayed in the Step 1 text field as your network card). Most users should accept this name.

**Step 2:** If you wish your computer to accept connections from other PC's in this network (e.g. a work or home network) or for printer sharing, then check the option 'I would like to be fully accessible to the other PCs in this network'. This then becomes a trusted network. Users that only have a single home computer connecting to the Internet should avoid this setting.

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](#)')

You must click 'OK' to confirm your choice. If you click on 'Close' button, all the network connections are blocked.

## 1.3.2 CIS Pro- Installation and Activation

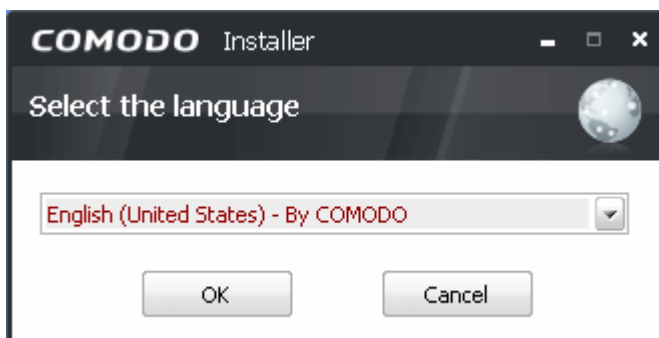
Comodo Internet Security 2011 Pro can be downloaded from <http://personalfirewall.comodo.com/internetsecuritypro/> after signing up for subscription and includes **LivePCSupport**, **TrustConnect** and the **Comodo Guarantee**.

After downloading the Comodo Internet Security setup file to your local hard drive, double click on cispro\_installer.exe



to start the installation.

The Language selection dialog will be 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'.

The following window is displayed.



**Install Comodo Internet Security 2011 Pro** - If you have not yet installed CIS then you should first select 'Install Comodo Internet Security 2011 Pro'.

- [Click here for more details on installing Comodo Internet Security 2011 Pro](#)

**Activate TrustConnect** - Begins the activation processes for your TrustConnect account and for your Comodo Guarantee. Please locate your License Key before starting. You should have received your License Key through email. 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 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.](#)

**Install Dragon Web Browser** - Begins the installation of Dragon web browser. Comodo Dragon is a highly secure, user friendly web browser that makes surfing the web safer, easier and more enjoyable.

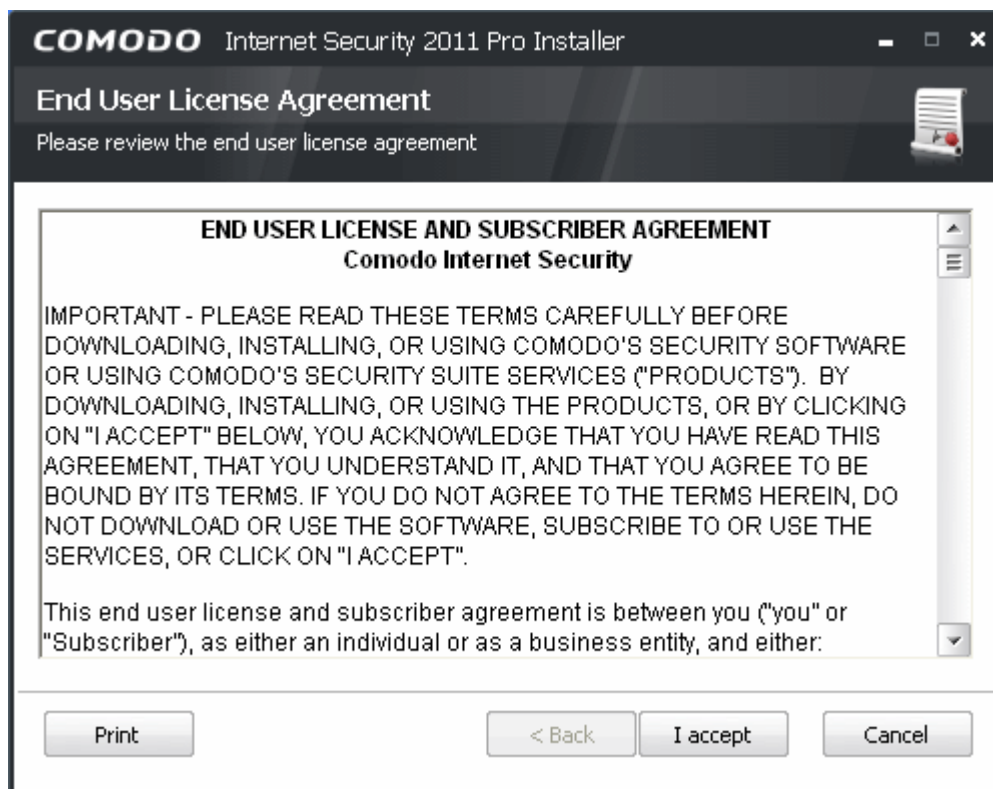
- [Click here for more details on installing Dragon Browser](#)

### 1.3.2.1 Installing Comodo Internet Security 2011 Pro and Live PC Support

Click 'Install COMODO Internet Security 2011 Pro' from the main Comodo Internet Security 2011 Pro Installer screen. The installation wizard for installing CIS 2011 and Live PC Support will start immediately.

#### Step 1 - End User License Agreement

The End-User License Agreement dialog box will be displayed.



To continue with the installation, you must read and then accept the End User License Agreement (EULA). Click 'I accept' to continue the installation. If you want to cancel the installation at this stage, click 'Cancel'.

#### Step 2 - Validating Your License

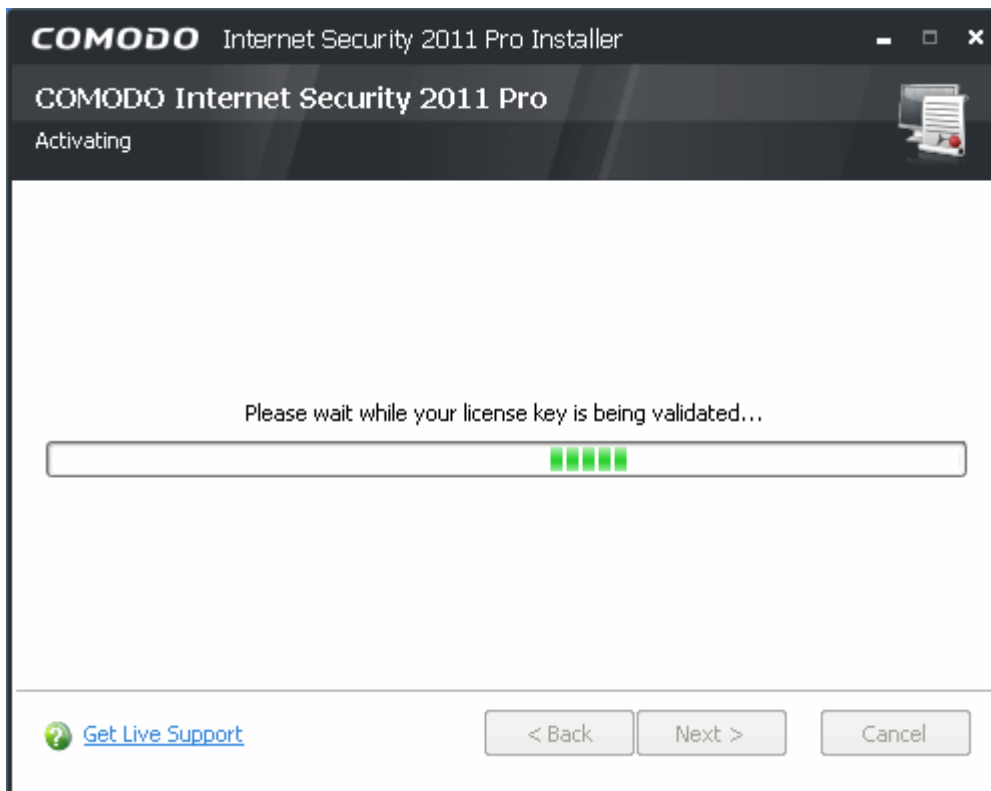
The next step is entering the License key. You should have received your License key through email.



Enter the key fully and click 'Next'.

**Tip:** You can skip this step if you don't have the subscription key handy at the time of installation. In order to continue the installation without entering the key, press 'Next'. 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](#)'.

Your License key will be validated.



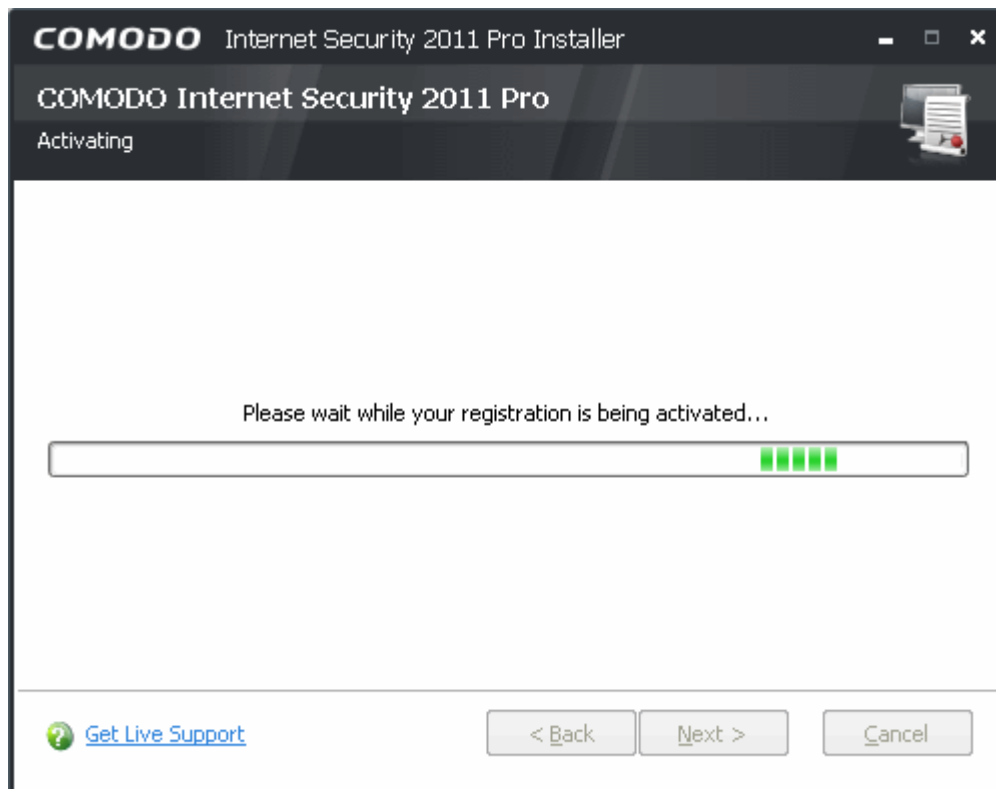
On successful validation of your license key, you need to register your account with Comodo Accounts Manager.



Fill up the registration form with the necessary details. The login and password entered in this form can be used to login into your account with Comodo Account Manager at anytime.

Click 'Next'.

Your registration will be activated.



On successful activation, you will see a final confirmation screen that summarizes your license entitlements:



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).

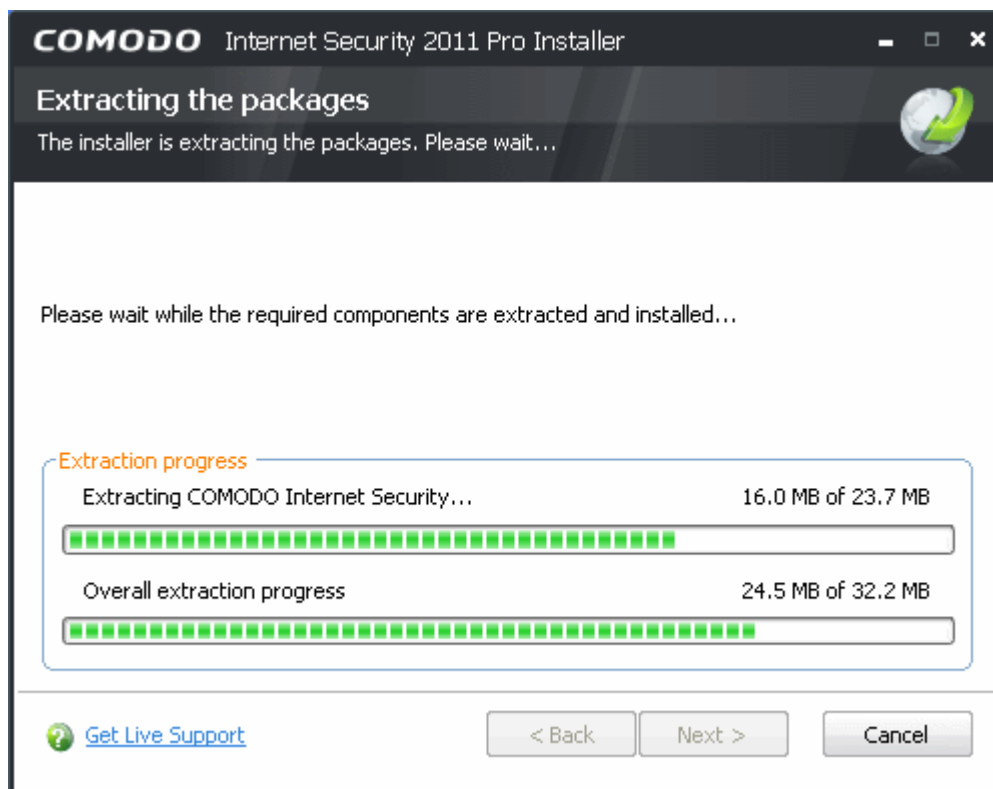
Click 'Next' to continue.



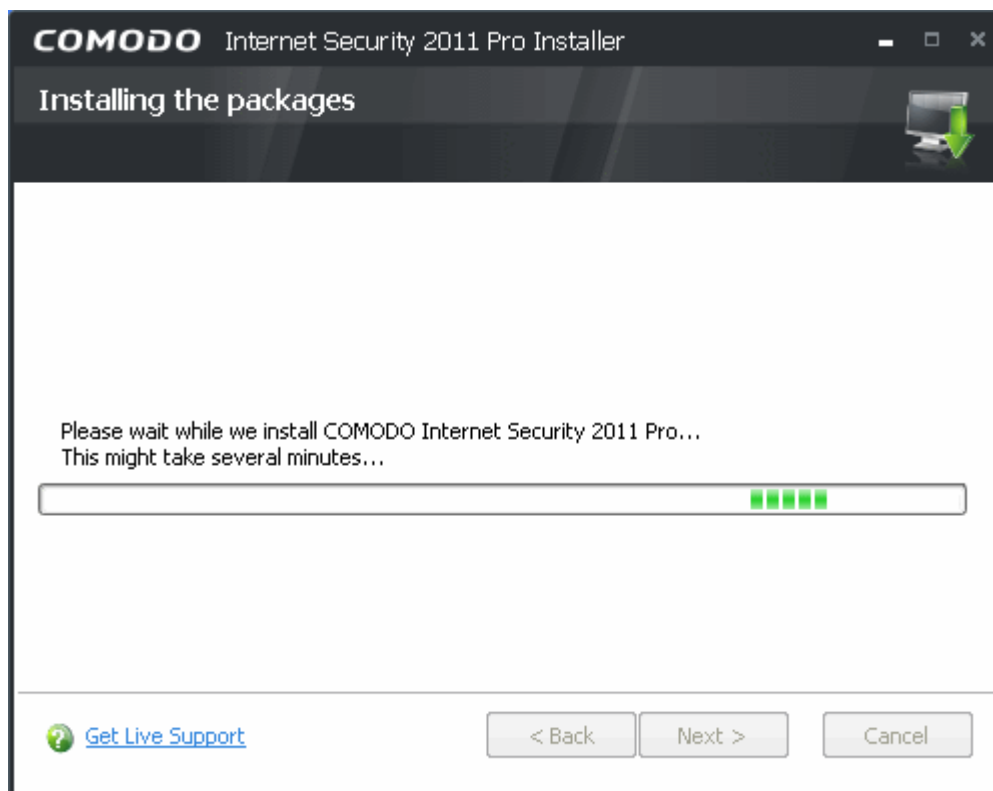
**Important note:** You need to activate your guarantee after completion of installation of CIS. Refer to [Activating Your Guarantee Coverage](#) for more details.

## Step 3 - Installation Progress

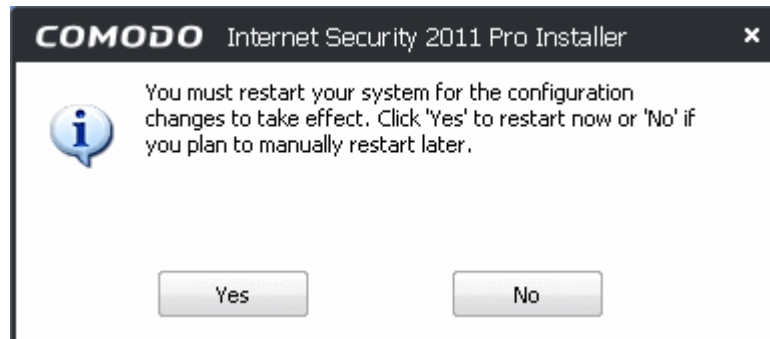
The packages will be extracted...



... and installed. The installation progress will be indicated.



On completion of installation you will be prompted to restart your computer, for the installation to take effect.

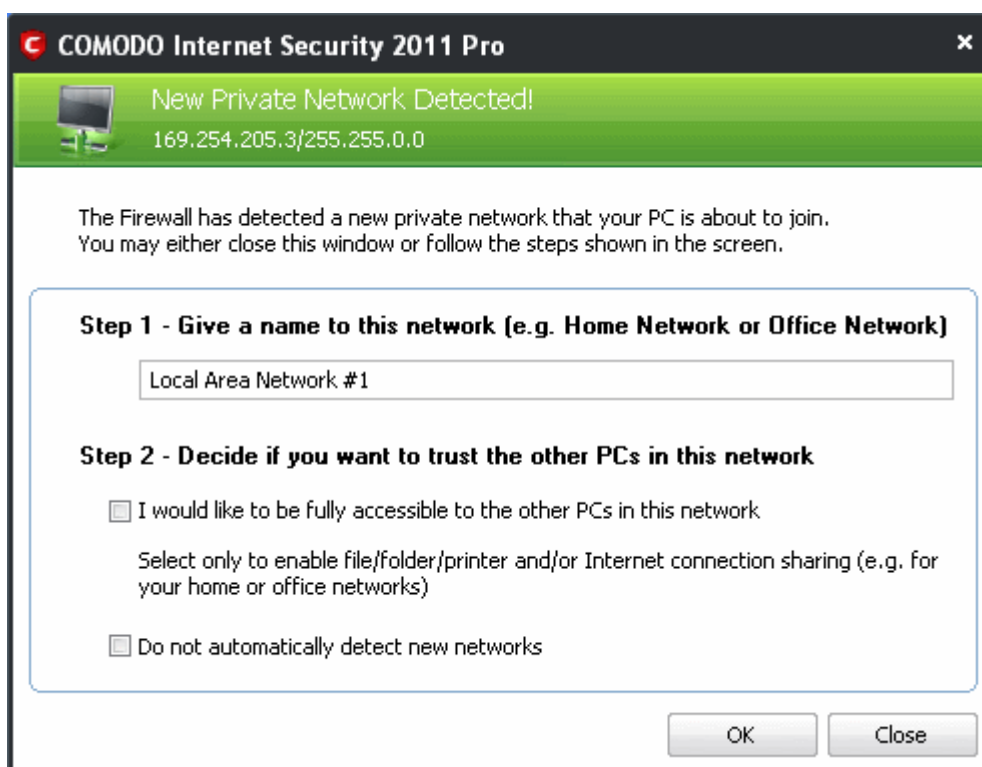


Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

#### Step 4 - After Restarting Your System

After restarting, if your computer is connected to a home or work network, then you are prompted to configure it at the 'New Private Network Detected!' dialog:



**Step 1:** Even home users with a single computer have to configure a home network in order to connect to Internet. (this is usually displayed in the Step 1 text field as you network card). Most users should accept this name.

**Step 2:** If you wish your computer to accept connections from other PC's in this network (e.g. a work or home network) or for printer sharing, then check the option 'I would like to be fully accessible to the other PCs in this network'. This then becomes a trusted network. Users that only have a single home computer connecting to the Internet should avoid this setting.

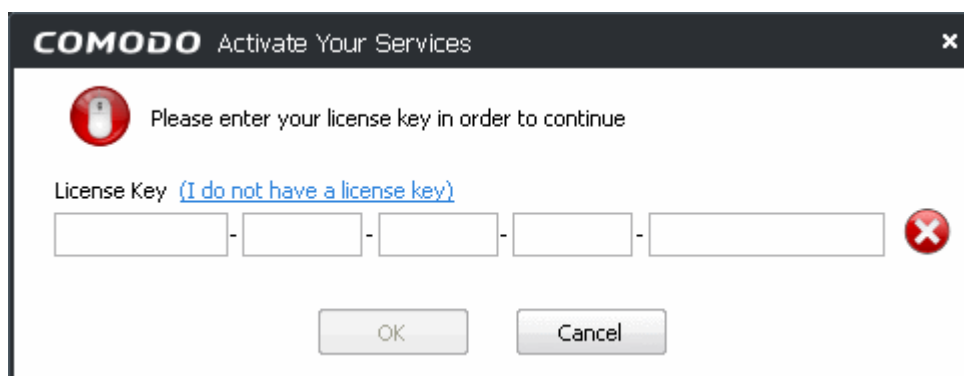
Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '[Network Zones](#)' and through the '[Stealth Ports Wizard](#)')

You must click 'OK' to confirm your choice. If you click on 'Close' button, all the network connections are blocked.

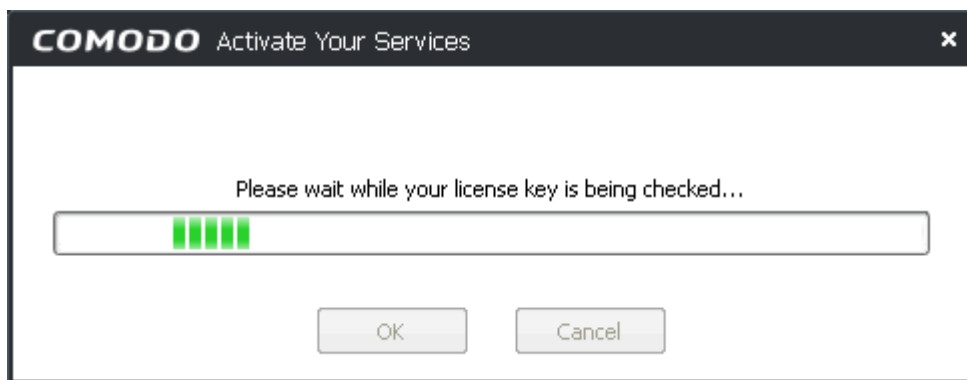
### 1.3.2.2 Activating TrustConnect and Guarantee

In order to utilize TrustConnect services and to get the guarantee coverage, you need to activate the services. Keep the license key handy, before starting this process.

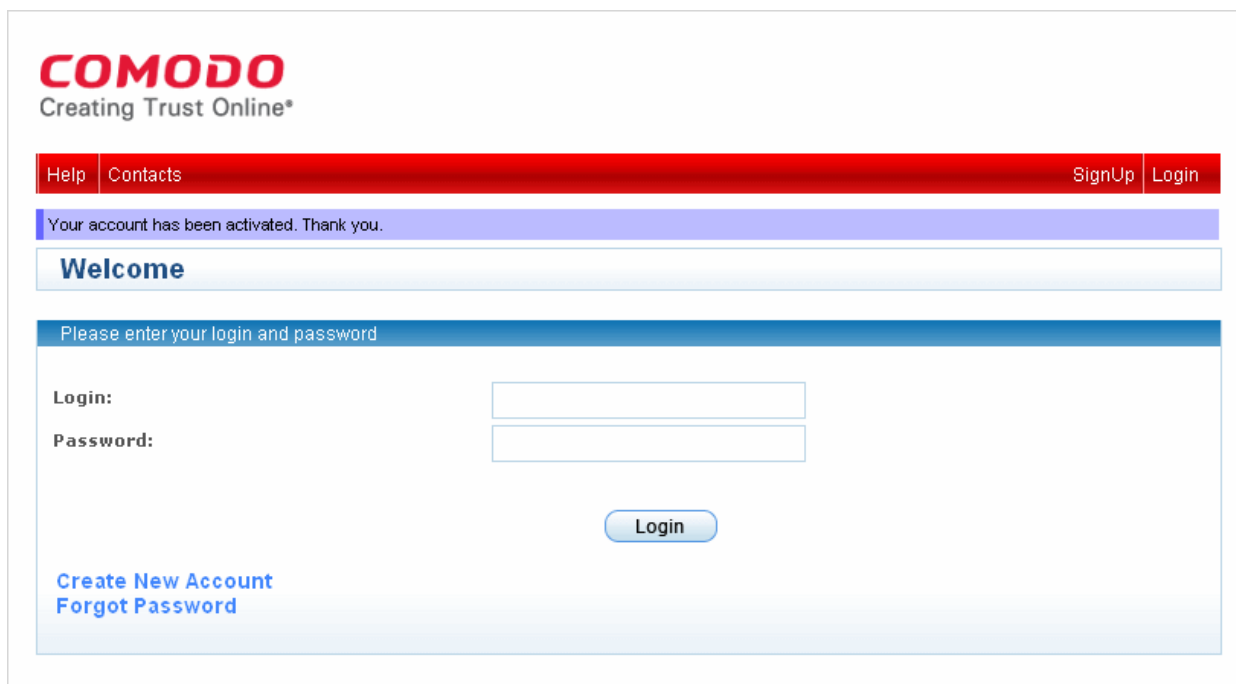
- Click 'Activate TrustConnect' from the main Comodo Internet Security 2011 Pro Installer screen. You will be prompted to enter the your license key in the provided space.



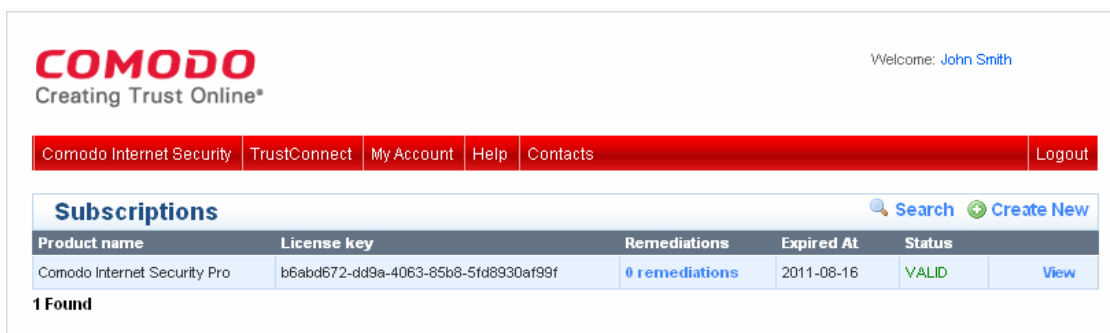
- Enter the license key sent to you by email. The license key will be validated.



After the License key is verified, the Comodo Accounts Manager page is displayed.



Enter your login ID and password for Comodo Accounts Manager (the credentials you defined when **activating your license in Step 2**, during installation). Your account summary will be displayed.



Click on the 'TrustConnect' tab. Your TrustConnect account details will be displayed.

**COMODO**  
Creating Trust Online®

Welcome: [John Smith](#)

Comodo Internet Security | TrustConnect | My Account | Help | Contacts | [Logout](#)

### Comodo TrustConnect

<b>Service Login</b>	jsmith
<b>Service Password</b>	1aB2cdeeFG
<b>License key</b>	e11b3e35-937d-47ef-957d-a2207a4c75b2
<b>Date from</b>	2010-08-16 06:40:09
<b>Date to</b>	2011-08-16 06:40:09

#### Traffic

<b>Limit:</b>	10 GB
<b>Available:</b>	10 GB

**Today**  
No data found.

**This month**  
No data found.

**This year**  
No data found.

In order traffic charts to be displayed correctly, please install [Adobe Flash Player](#) version 9 or higher.

[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™](#)

- Note down the Service Login and Service Password shown in this page. These are the service credentials you need to use for getting the TrustConnect Services. For more details, refer to the chapter [TrustConnect Overview](#).

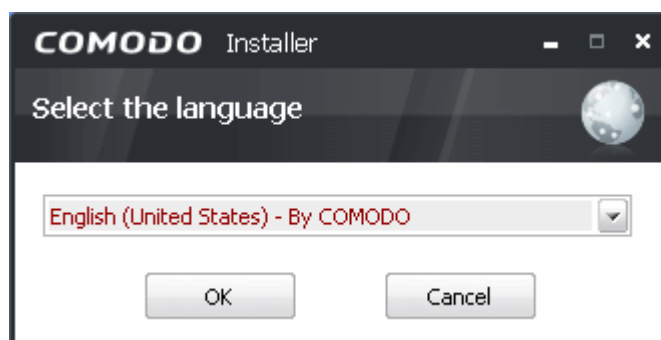
### 1.3.3 CIS Complete - Installation and Activation

Comodo Internet Security 2011 Complete is distributed on DVD and includes [LivePCSupport](#), [Online BackUp](#), [TrustConnect](#) 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 want Comodo Internet Security to be installed from the drop-down menu and click 'OK'.

The following window is displayed.



**Install Comodo Internet Security 2011 Complete** - If you have not yet installed CIS then you should first select 'Install Comodo Internet Security 2011 Complete'.

- [Click here for more details on installing Comodo Internet Security 2011 Complete](#)

**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 download 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.](#)

**Install Dragon Web Browser** - Begins the installation of Dragon web browser. Comodo Dragon is a highly secure, user friendly web browser that makes surfing the web safer, easier and more enjoyable.

- [Click here for more details on installing Dragon Browser](#)

### 1.3.3.1 Installing Comodo Internet Security 2011 Complete and Live PC Support

Click 'Install COMODO Internet Security 2011' from the main Comodo Internet Security 2011 Complete Installer screen.

The installation wizard for installing CIS 2011 and Live PC Support will start immediately.

## Step 1 - End User License Agreement

The End-User License Agreement dialog box will be displayed.



To continue with the installation, you must read and then accept the End User License Agreement (EULA). Click 'I accept' to continue the installation. If you want to cancel the installation at this stage, click 'Cancel'.

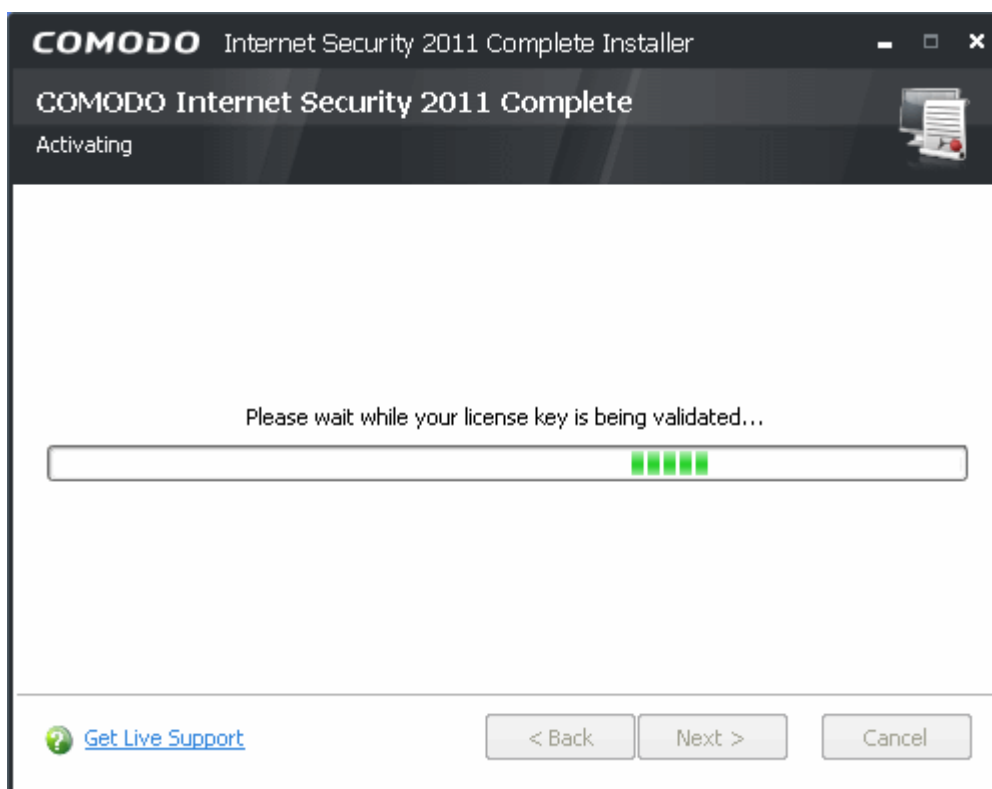
## Step 2 - Validating Your License Key

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



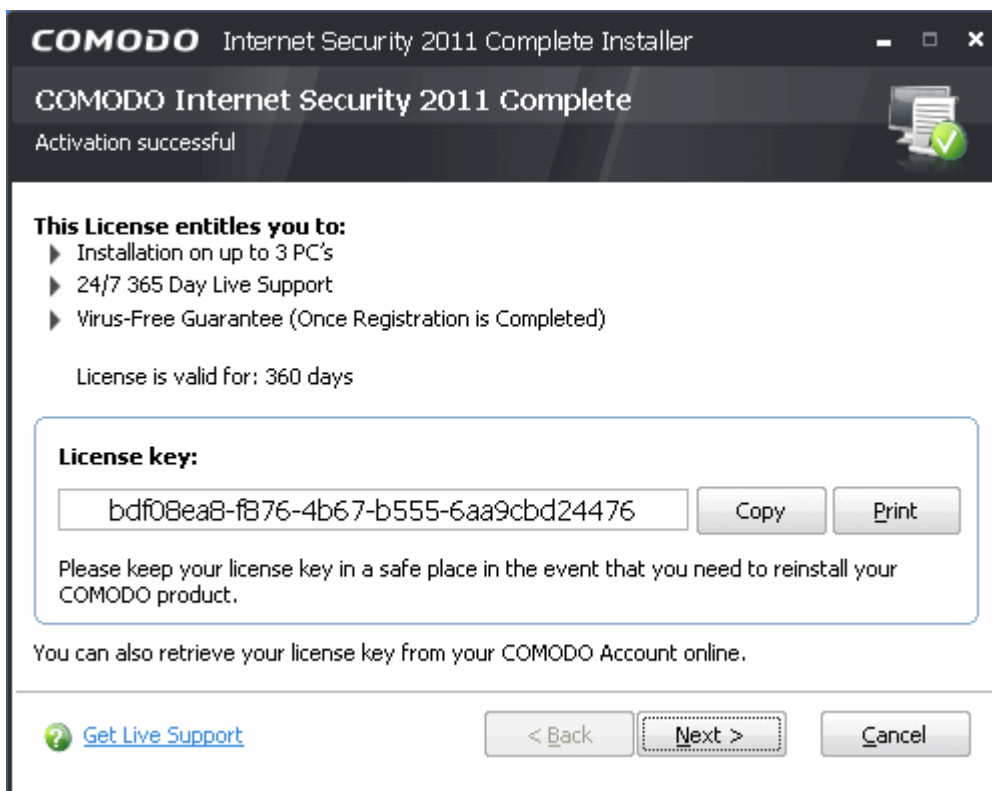
**Tip:** You can skip this step if you don't have the subscription key handy at the time of installation. In order to continue the installation without entering the key, press 'Next'. You can activate your subscription and guarantee at a later time from the main interface of CIS. For more details refer to [Activating your CIS Pro and CIS Complete Services after Installation](#).

Enter the key fully and click 'Next'. Your License key will be validated.





After your license key has been validated, a final confirmation screen will be displayed, that summarizes your license entitlements:



Click 'Next' to continue.

## Step 3 - Installation Progress

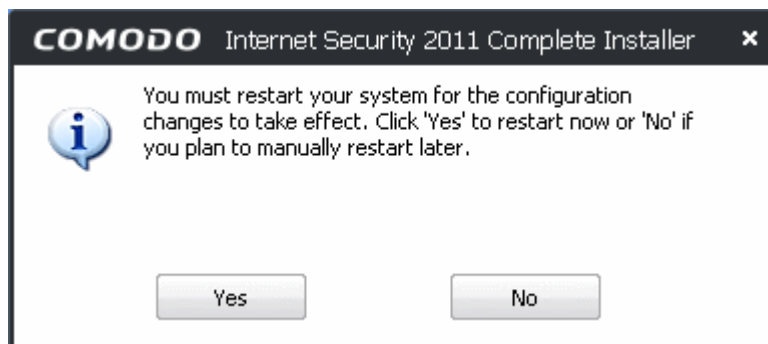
The packages will be extracted...



... and installed. The installation progress will be indicated.



On completion of installation you will be prompted to restart your computer, for the installation to take effect.

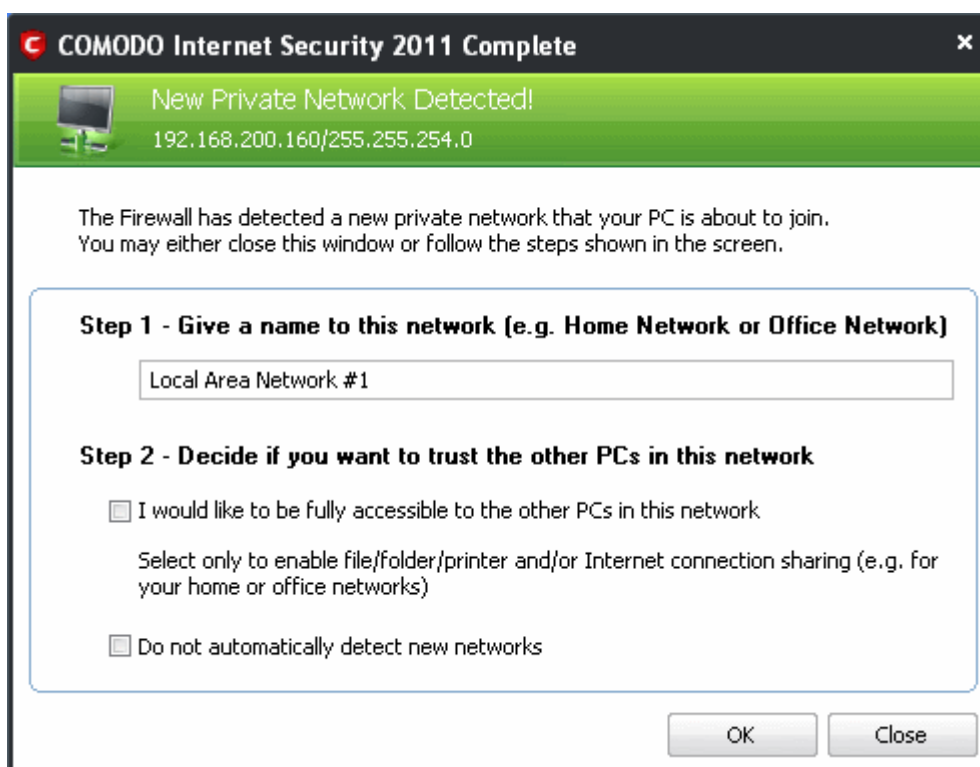


Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

#### Step 4 - After Restarting Your System

After restarting, if your computer is connected to a home or work network, then you are prompted to configure it at the 'New Private Network Detected!' dialog:



**Step 1:** Even home users with a single computer have to configure a home network in order to connect to Internet. (this is usually displayed in the Step 1 text field as you network card). Most users should accept this name.

**Step 2:** If you wish your computer to accept connections from other PC's in this network (e.g. a work or home network) or for printer sharing, then check the option 'I would like to be fully accessible to the other PCs in this network'. This then becomes a trusted network. Users that only have a single home computer connecting to the Internet should avoid this setting.

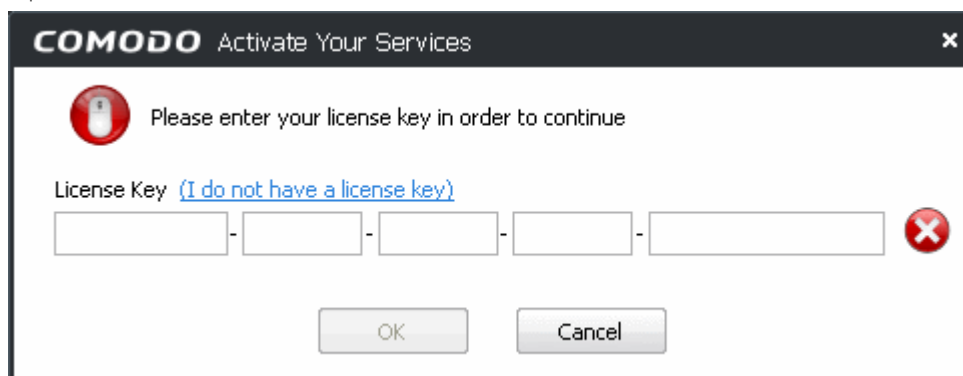
Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in '[Network Zones](#)' and through the '[Stealth Ports Wizard](#)')

You must click 'OK' to confirm your choice. If you click on 'Close' button, all the network connections are blocked.

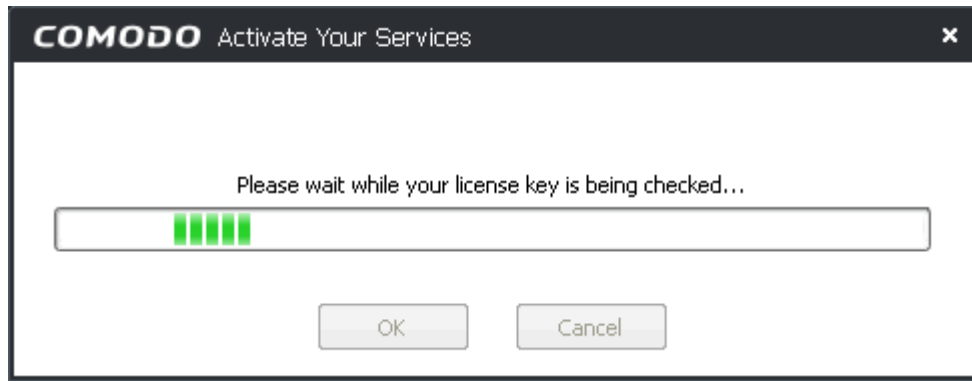
### 1.3.3.2 Activating Online Backup, TrustConnect and Guarantee

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 2011 Complete Installer screen. You will be prompted to enter the your license key in the provided space.



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



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

COMODO  
Creating Trust Online®

## Comodo Internet Security

## Comodo Sign-Up Page

License Key\*

b6abd672-dd9a-4063-85b8-

## Customer Information (an \* indicates required fields)

## User Details

Are you an existing Comodo customer?  Yes  No

Login\*

(4 character min.)

jsmith

Password\*

(6 characters min.)

●●●●●●

Password Confirmation\*

●●●●●●

First Name\*

John

Last Name\*

Smith

Email\*

jsmith@example.com

Telephone Number

18002345614

## Contact Information

Company Name

Company name

Street Address\*

Street name

Address2

Area

City\*

City name

Country\*

United States

State or Province

New York

Postal Code\*

10001

## 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

SUBSCRIBER AGREEMENT  
Comodo livePCsupport

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING IT. IMPORTANT—PLEASE READ THIS AGREEMENT CAREFULLY BEFORE SUBSCRIBING TO OR USING COMODO'S LIVEPC SUPPORT SERVICES ("SERVICES"). BY SUBSCRIBING TO OR USING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT

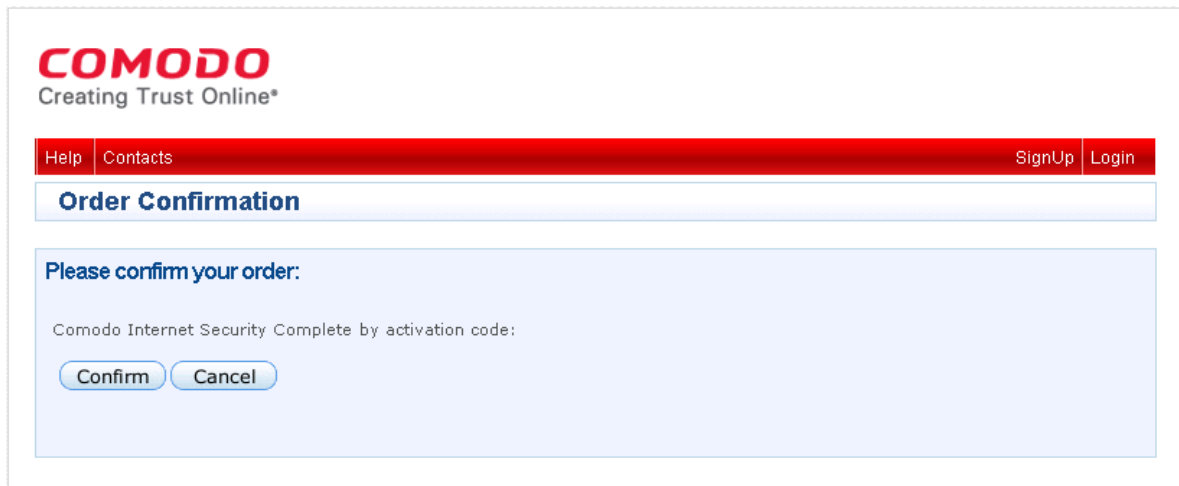
- 1) YOU HAVE READ THIS AGREEMENT,
- 2) YOU UNDERSTAND IT,

 I accept the Terms and Conditions**SIGN UP**

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

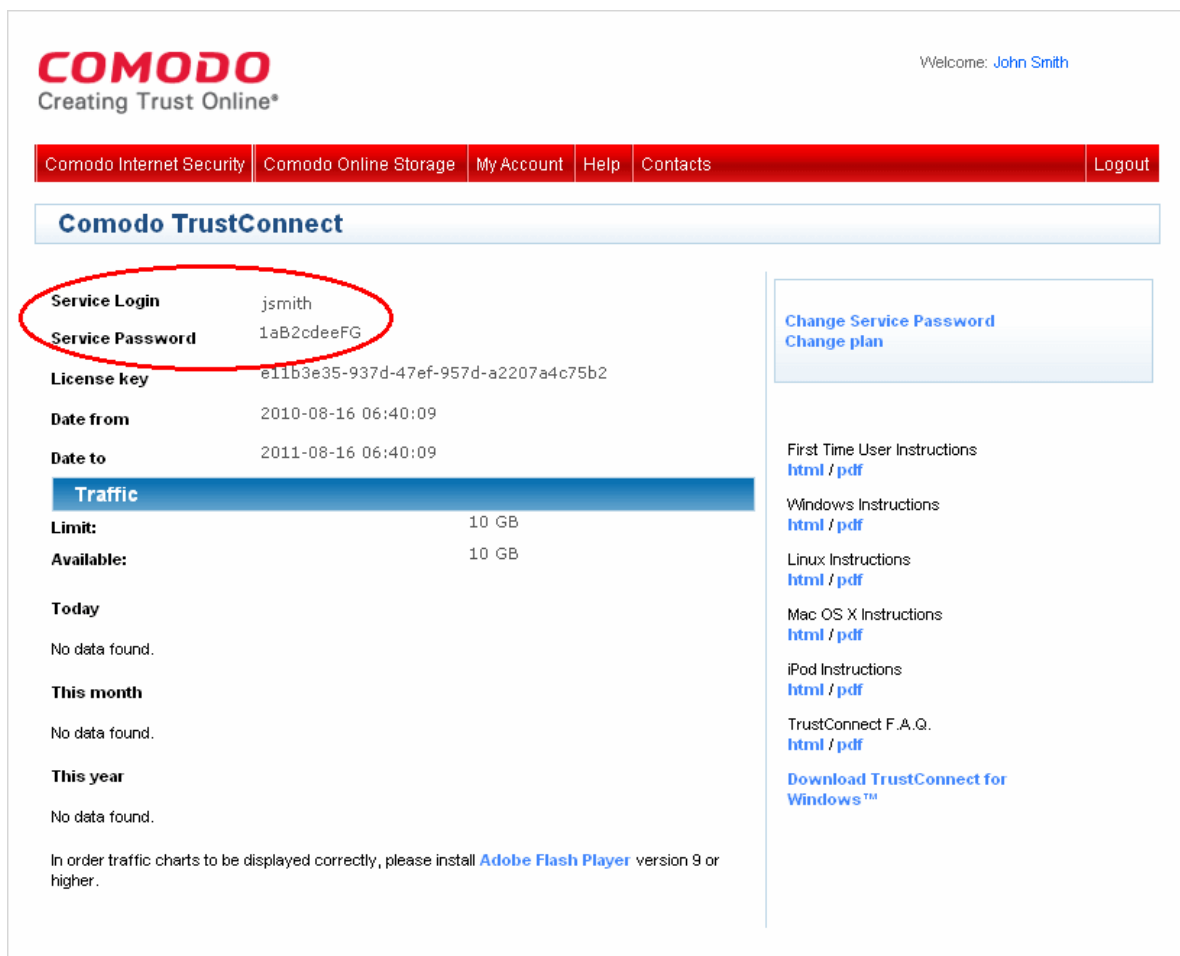
Svn Information

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



Clicking the 'Confirm' button displays the invoice generated for you. The invoice displays 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 can now login to your account at <https://accounts.comodo.com>, with the login details you specified during sign-up.



- For using TrustConnect services, you need the Service login and Service Password generated for you. For more details, refer to the chapter [TrustConnect Overview](#).
- Click the TrustConnect tab from your accounts page and note down the Service Login and Service Password shown in this page.
- 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

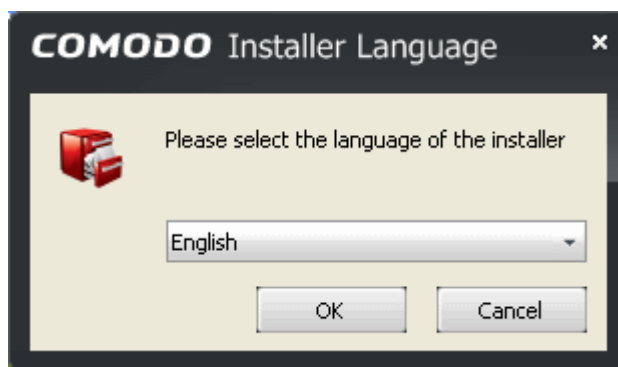
In order to store your valuable files to Comodo online storage space for safe-keeping, you need Comodo Backup application installed in your system.

#### To install Comodo Backup

- Reinsert the DVD and click 'Install Online Backup' from the main Comodo Internet Security 2011 Complete Installer screen. The installation wizard of Comodo Backup will start immediately.

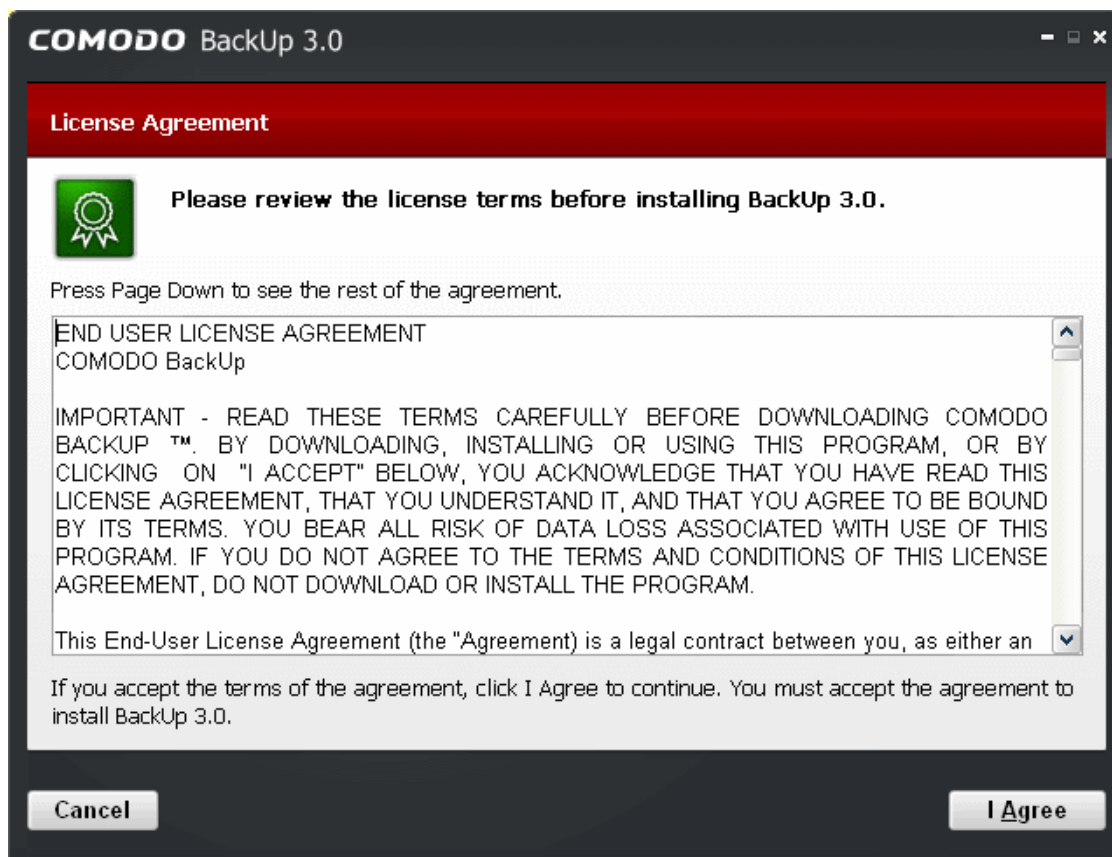
#### Step 1 - Choosing the Interface Language

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



#### Step 2 - End User License Agreement

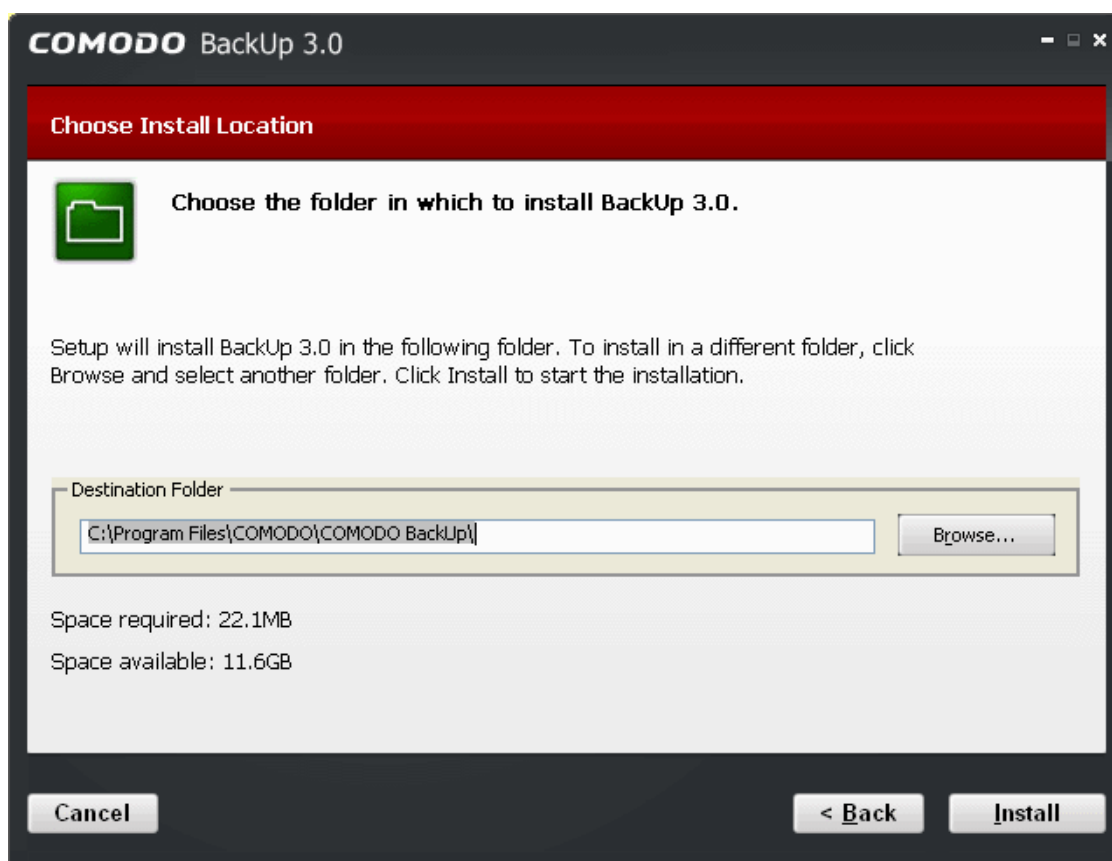
Complete the initialization phase by reading and accepting the End User License Agreement (EULA).



- 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*.



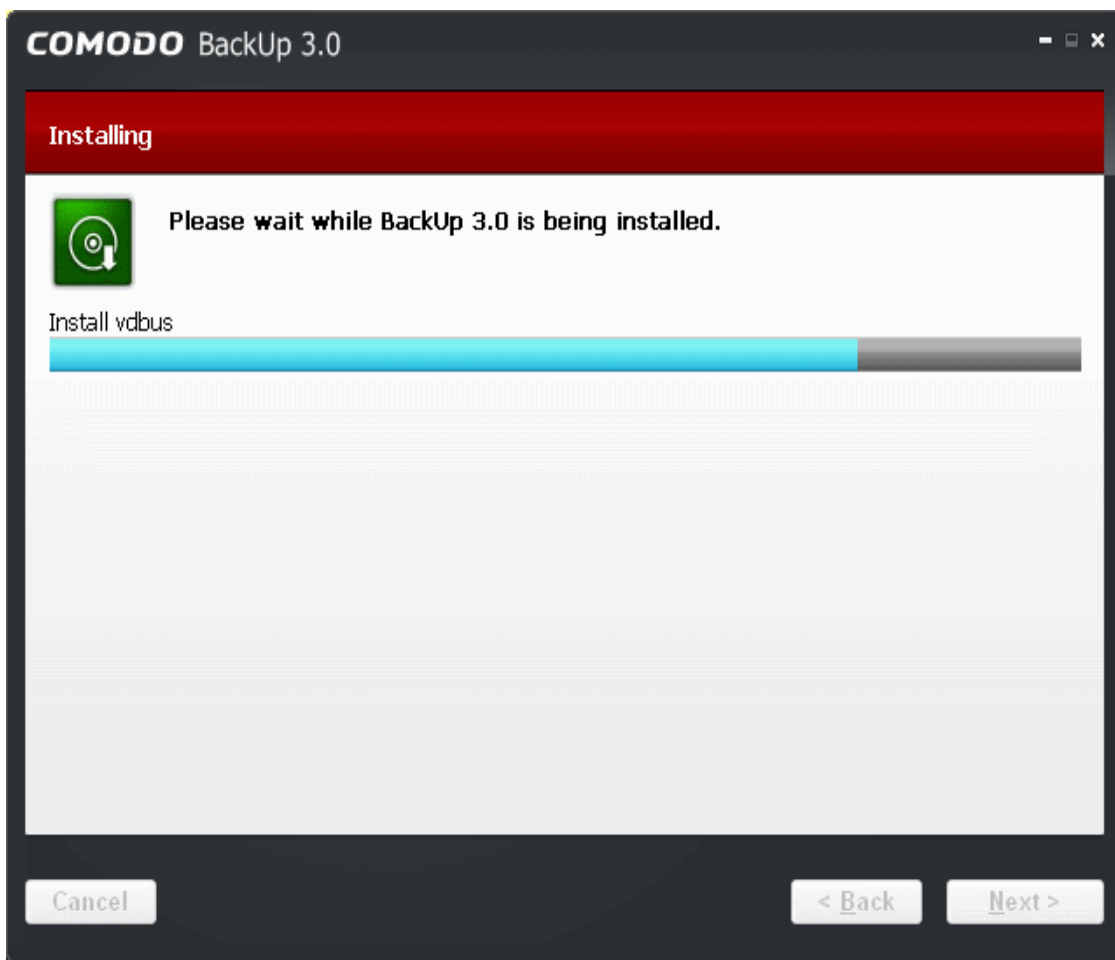
If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

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

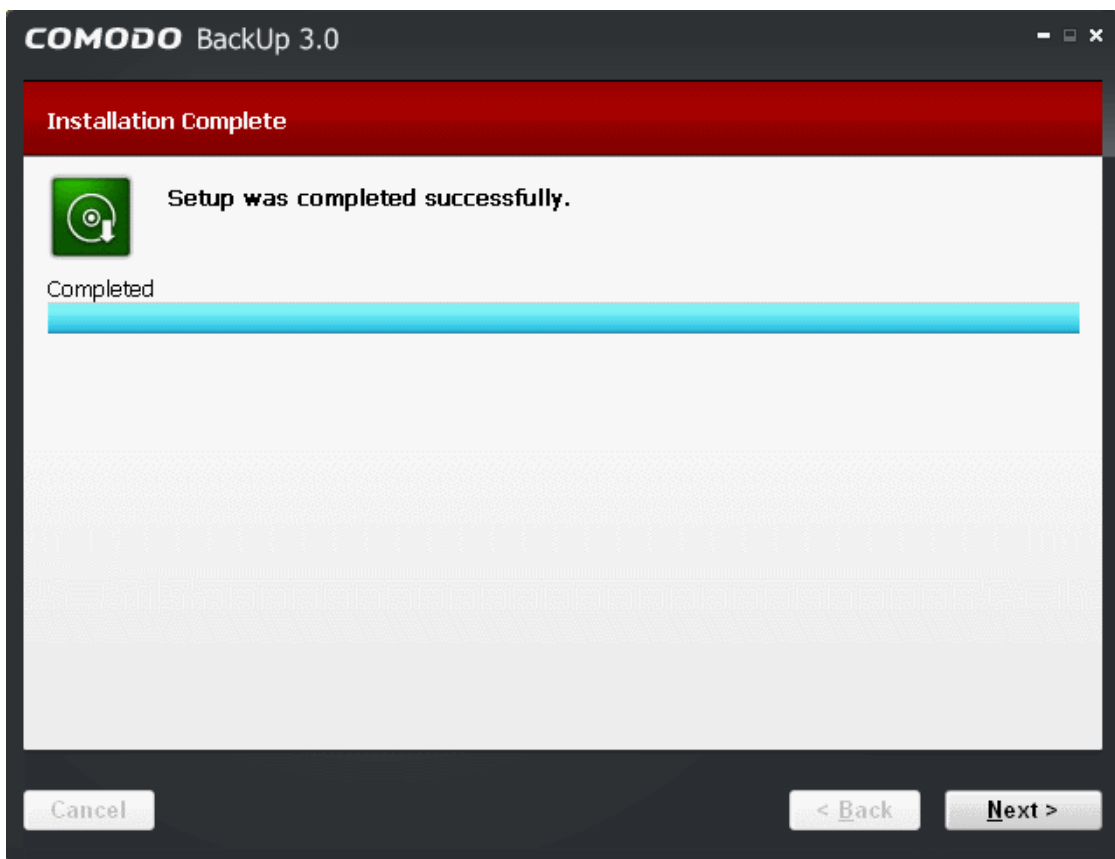
#### Step 4 - Setup Progress

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





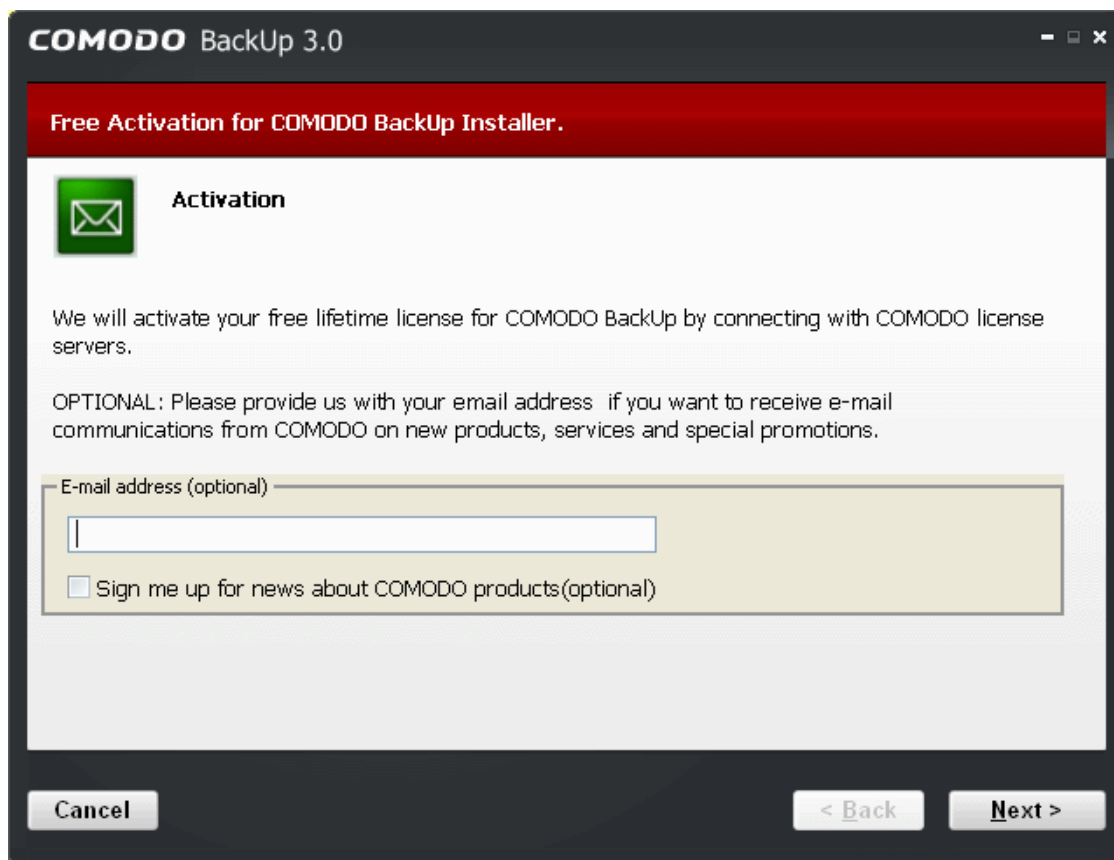
On completion, the 'Installation Complete' dialog will be displayed.



Click 'Next' to continue.

## Step 5 - Product Activation

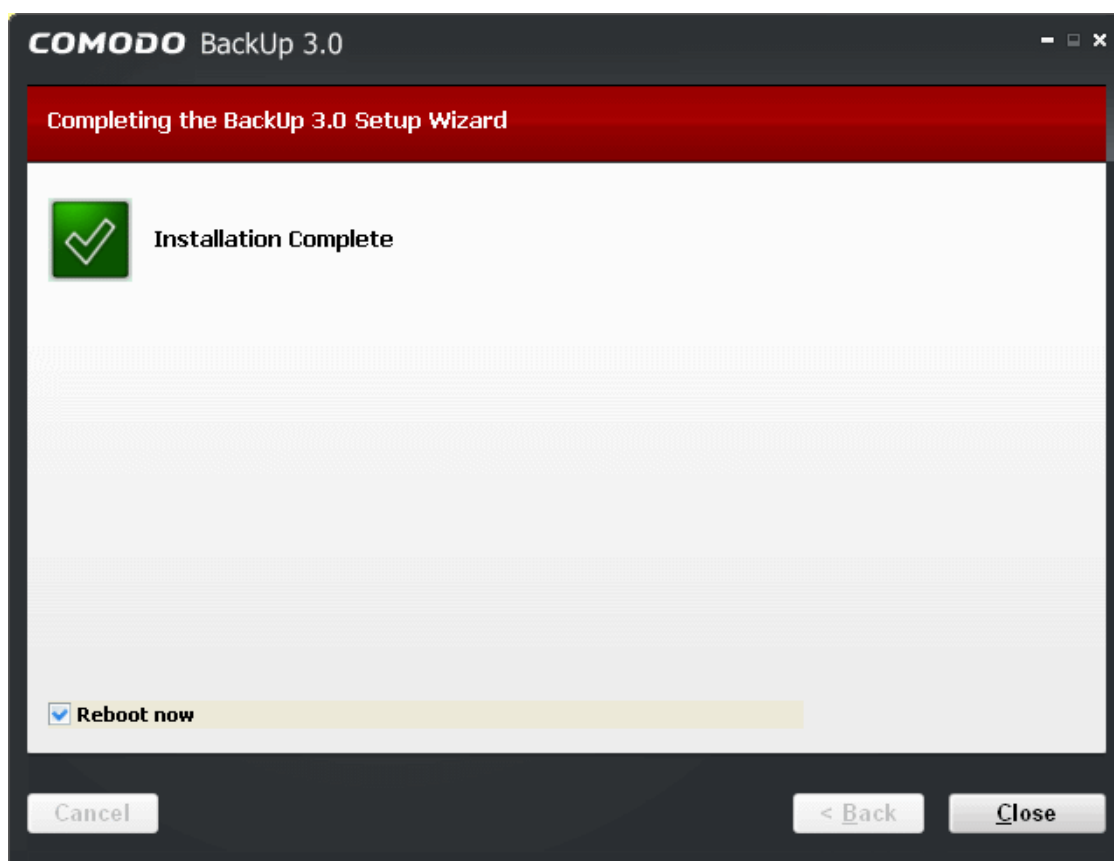
On completion of Installation, the product Activation dialog is displayed. Comodo BackUp is activated at free of cost for lifetime usage. If you wish to sign up for news about Comodo products then enter your email address in the space provided and select **Sign me up for news about Comodo products**.



This is optional. Click 'Next'.

## Step 6 - Installation Complete

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

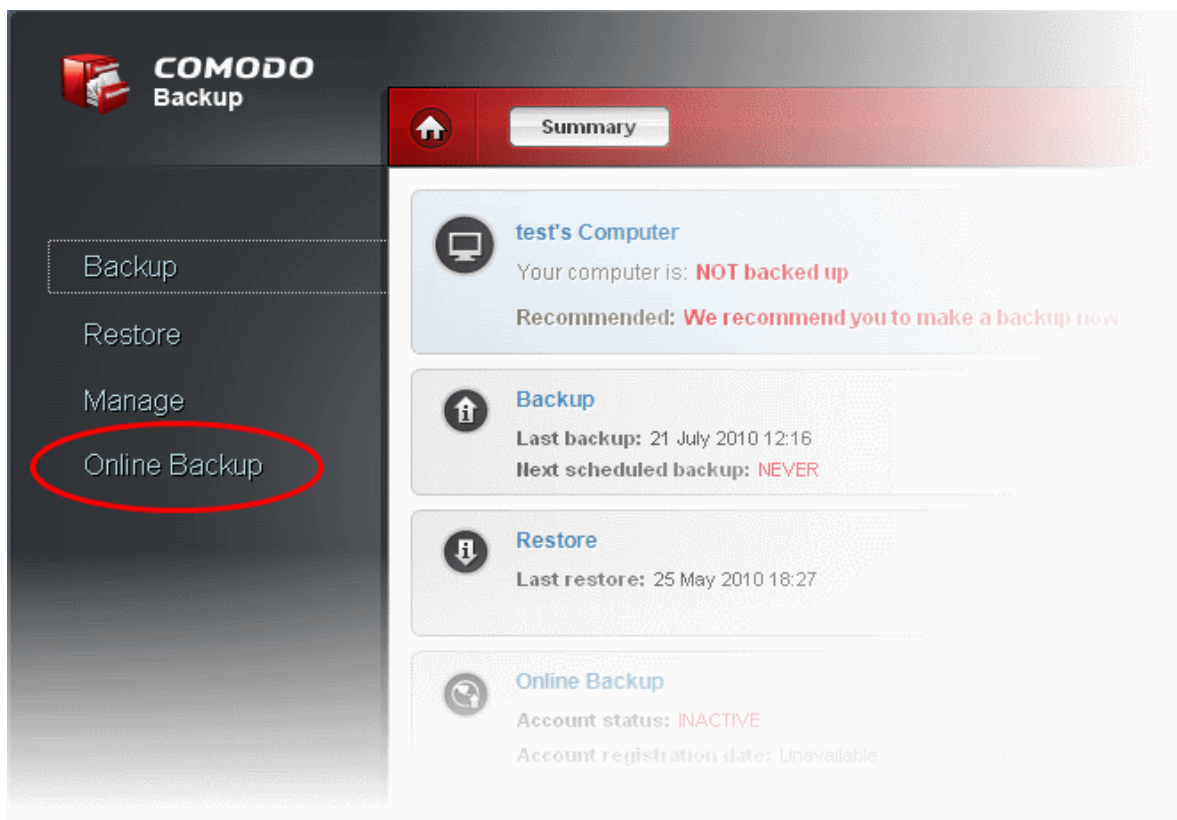


Please save any unsaved data, leave 'Reboot now' checkbox selected and click 'Close'. If you want to restart the system at a later time, uncheck 'Reboot now' checkbox click 'Close'.

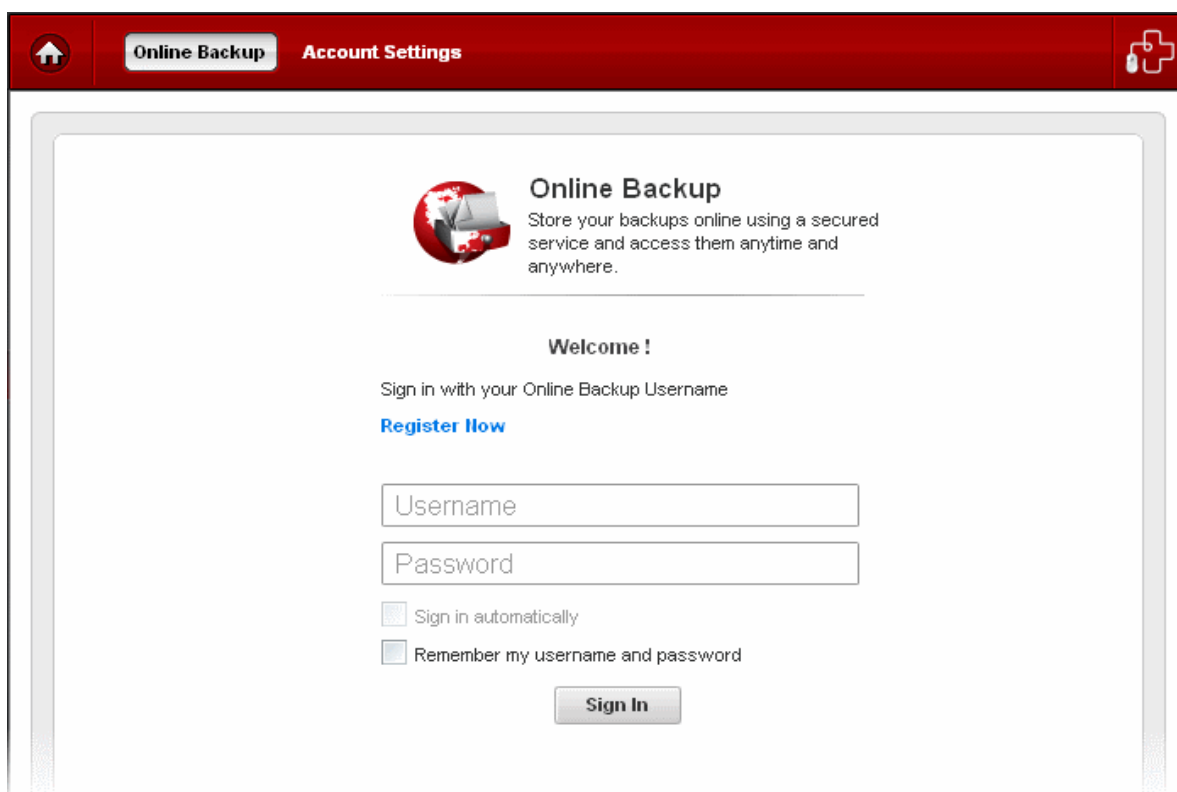
**Note:** The installation will take effect only after restarting the computer.

### 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.



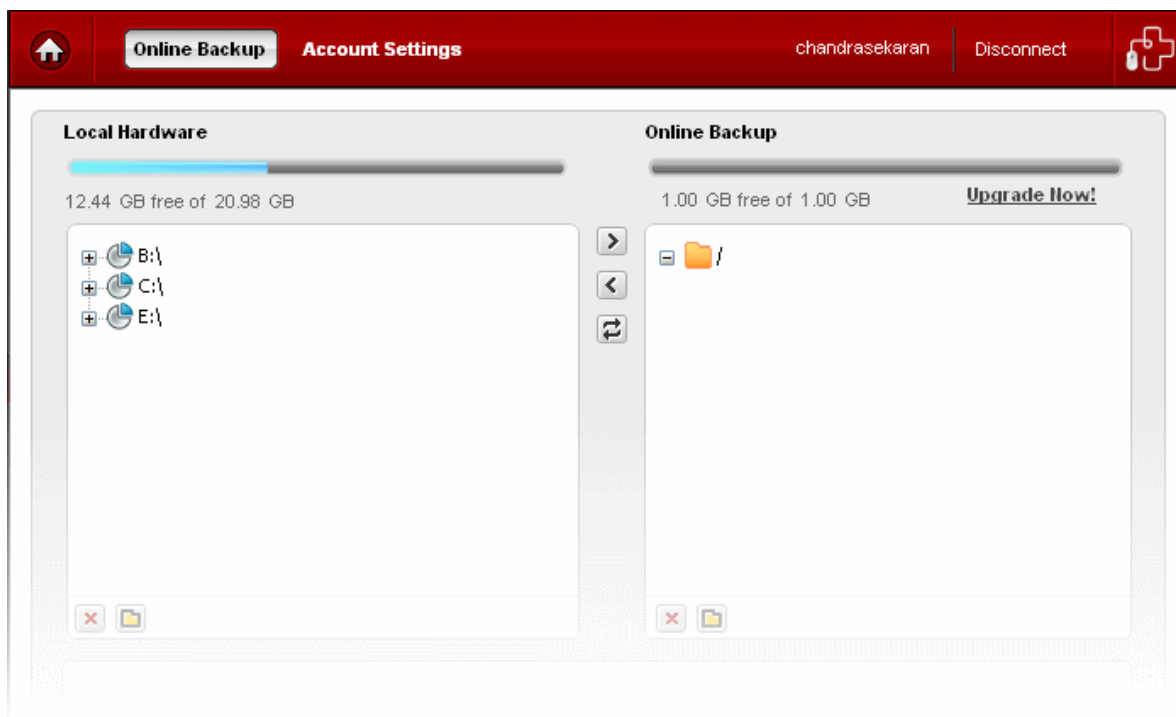
The Online Backup interface will open.



- Enter your Login ID and password with Comodo Account Manager in the Username and Password fields respectively and click Sign In.

After successful login, your username is displayed in the tab structure area and the disk partitions and folders of your system are displayed as a tree structure in the left hand side pane and the folders and files in your online storage space

are displayed as a tree structure in the right hand side pane. You can drag and drop files and folders between the two windows.



For more details on using your online storage space, refer to Comodo Backup User guide available at [http://backup.comodo.com/comodo\\_backup\\_user\\_manual.pdf](http://backup.comodo.com/comodo_backup_user_manual.pdf)

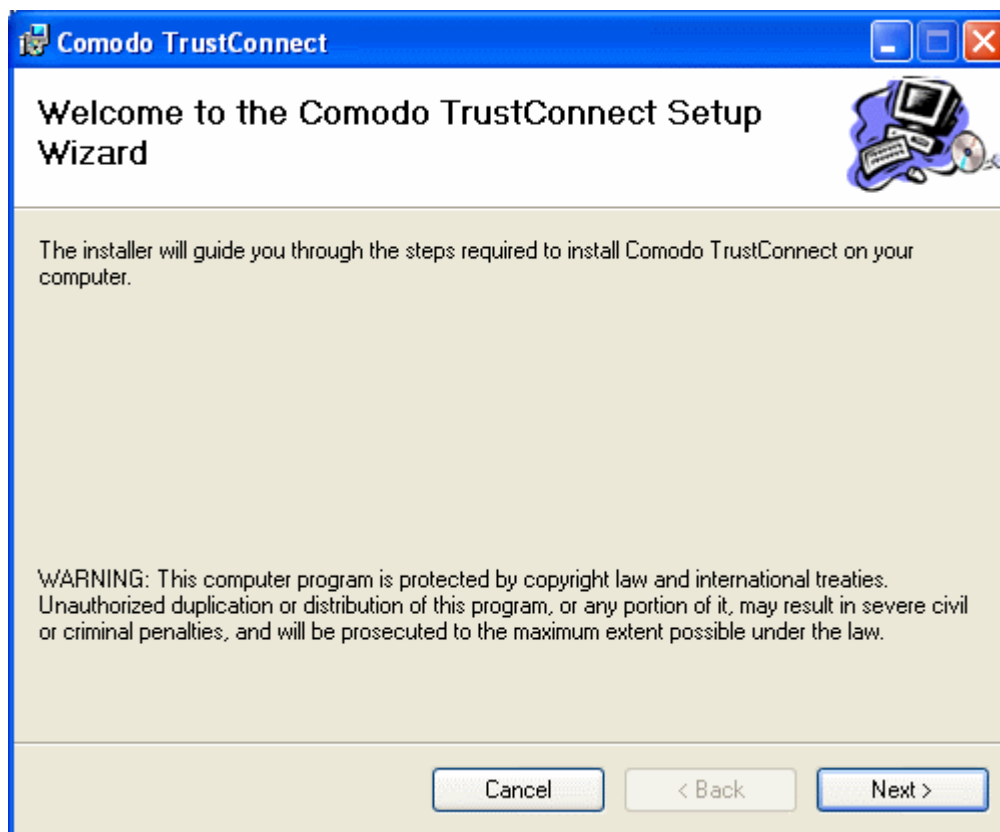
### 1.3.3.4 Installing Comodo TrustConnect

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 2011 Pro/Complete Installer screen. The installation wizard of Comodo TrustConnect will start immediately.

#### Step 1 - Welcome Screen

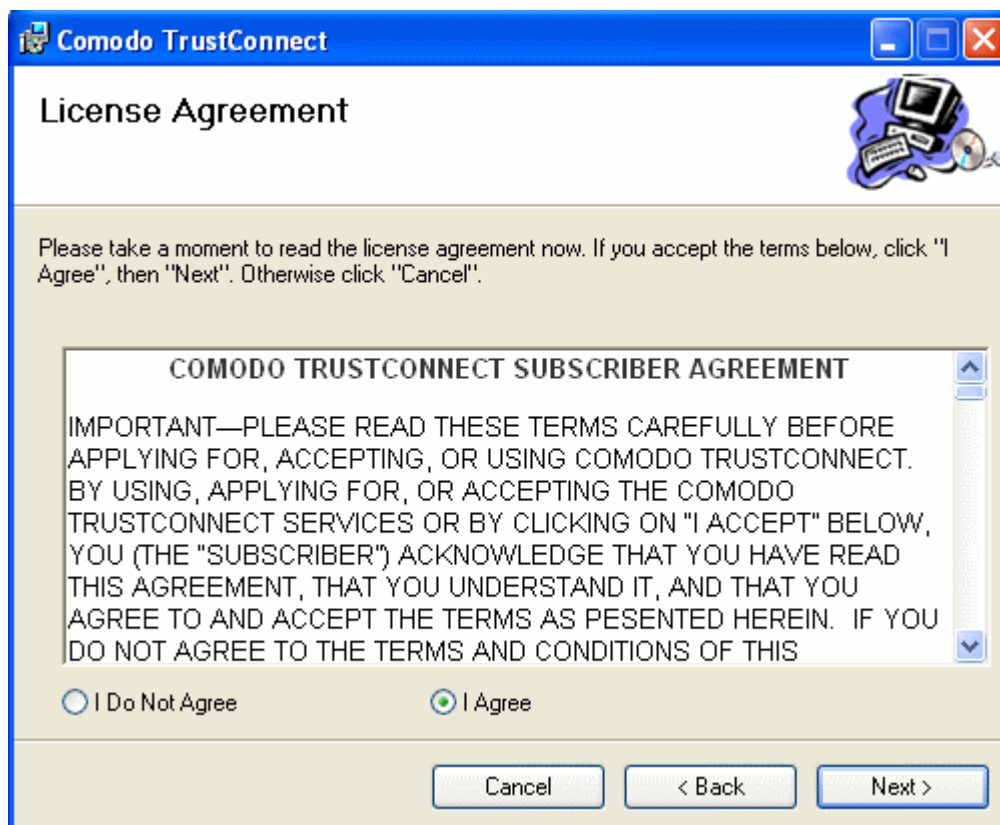
The welcome screen of the wizard will be displayed.



Click 'Next' to continue.

## Step 2 - Subscriber License Agreement

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

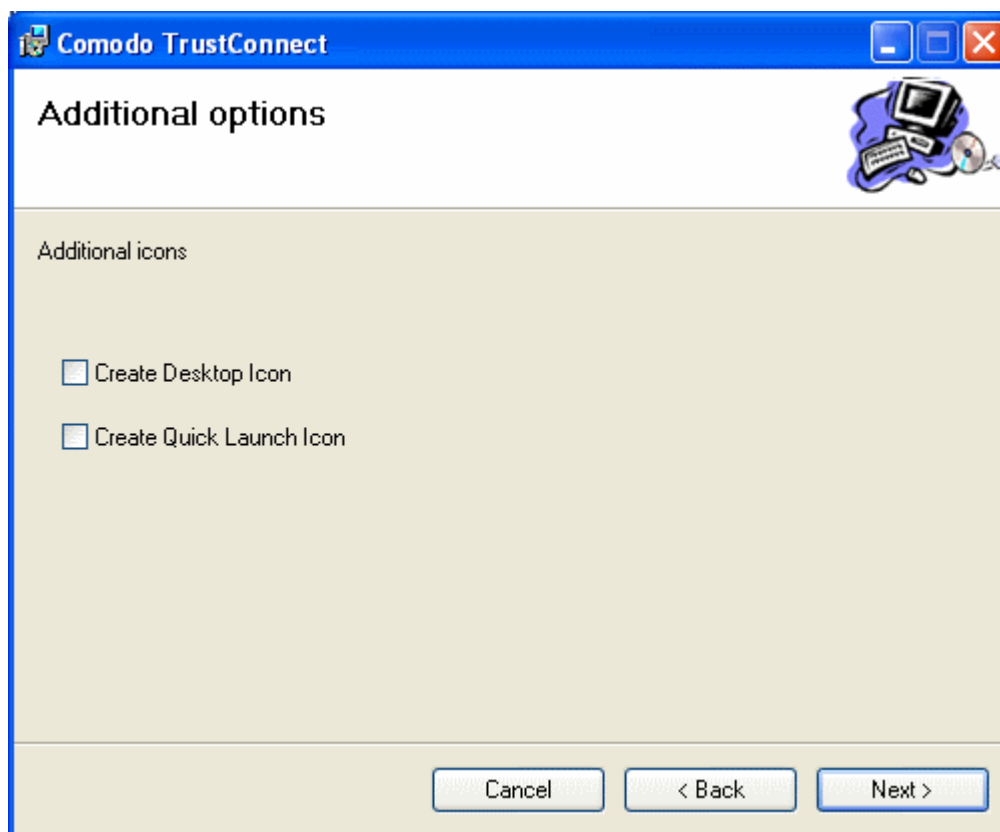


- Select I Agree to continue the installation.
- If you want to cancel the installation at this stage, select I Do Not Agree.

Click 'Next' to continue.

## Step 3 - Additional Options

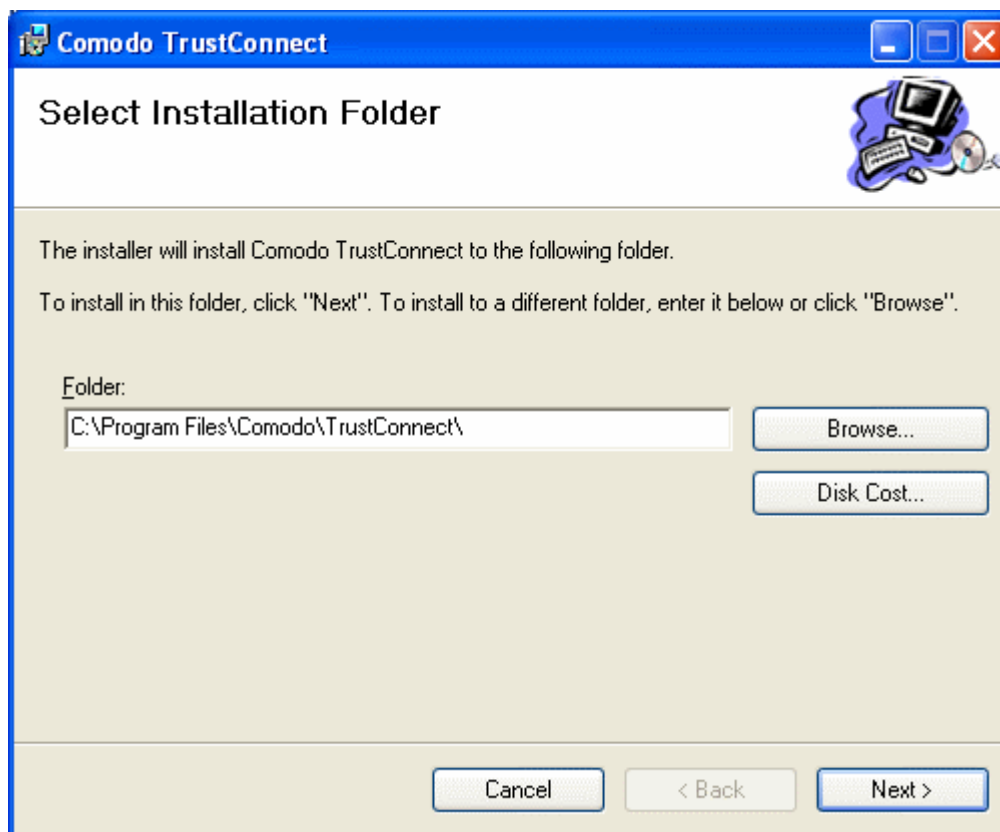
The next stage allows you to select for creation of TrustConnect Desktop icon and TrustConnect quick launch icon, for starting the client from the system tray.



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*.



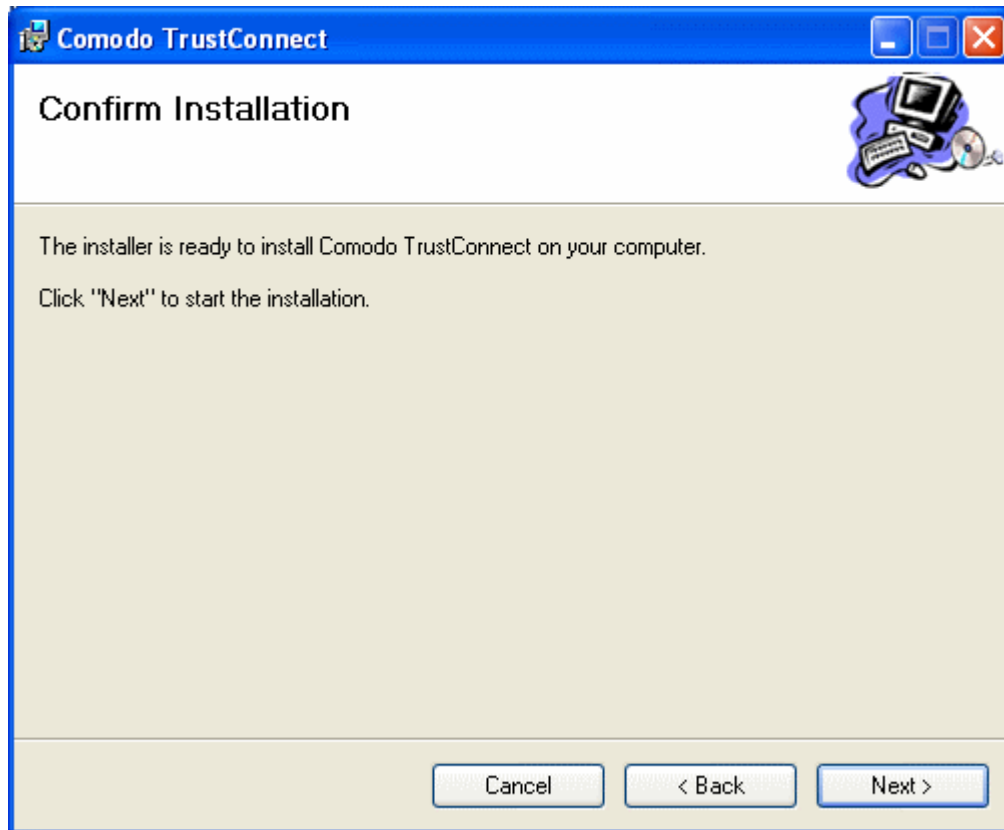
If you want to install the client in a location other than the default location, click 'Browse' to choose a different location.

Click 'Next' to continue.

### Step 5 - Installation Progress

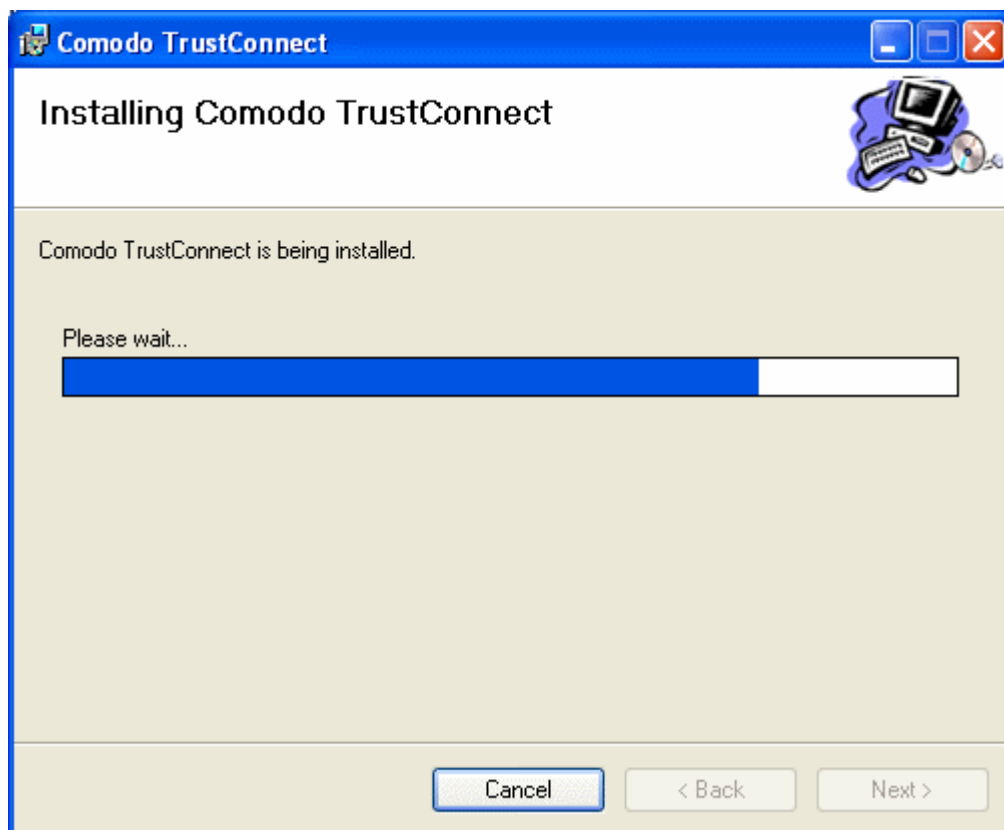
After completing the configuration options to your satisfaction the setup wizard will ask for confirmation before commencing the installation procedure.



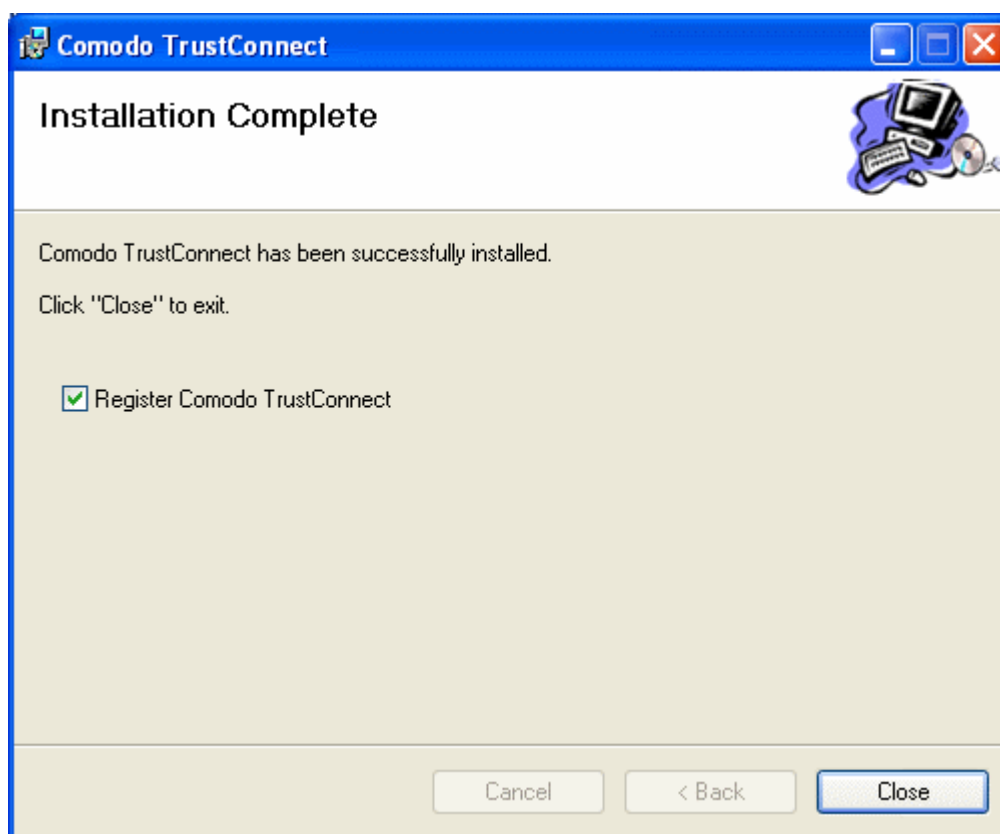


Click the 'Back' button to review and/or modify any of settings you have previously specified. To confirm your choices and begin the installation of Comodo Internet Security, click 'Next'.

The installation progress will be displayed...



...and 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.



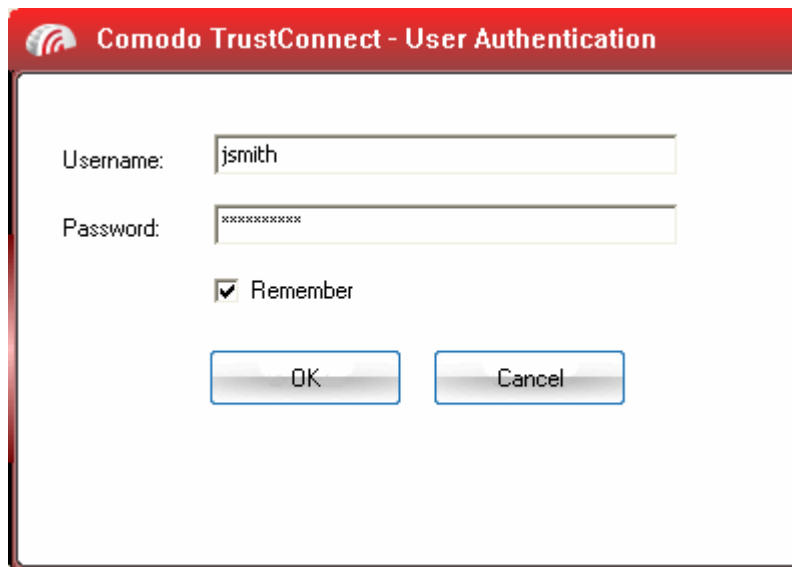
Enter your License Key and click Next.

Your key will be validated and a registration confirmation dialog will be displayed.



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

Click Finish to exit the wizard and start using TrustConnect.



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

### 1.3.3.5 Installing Comodo Dragon Browser

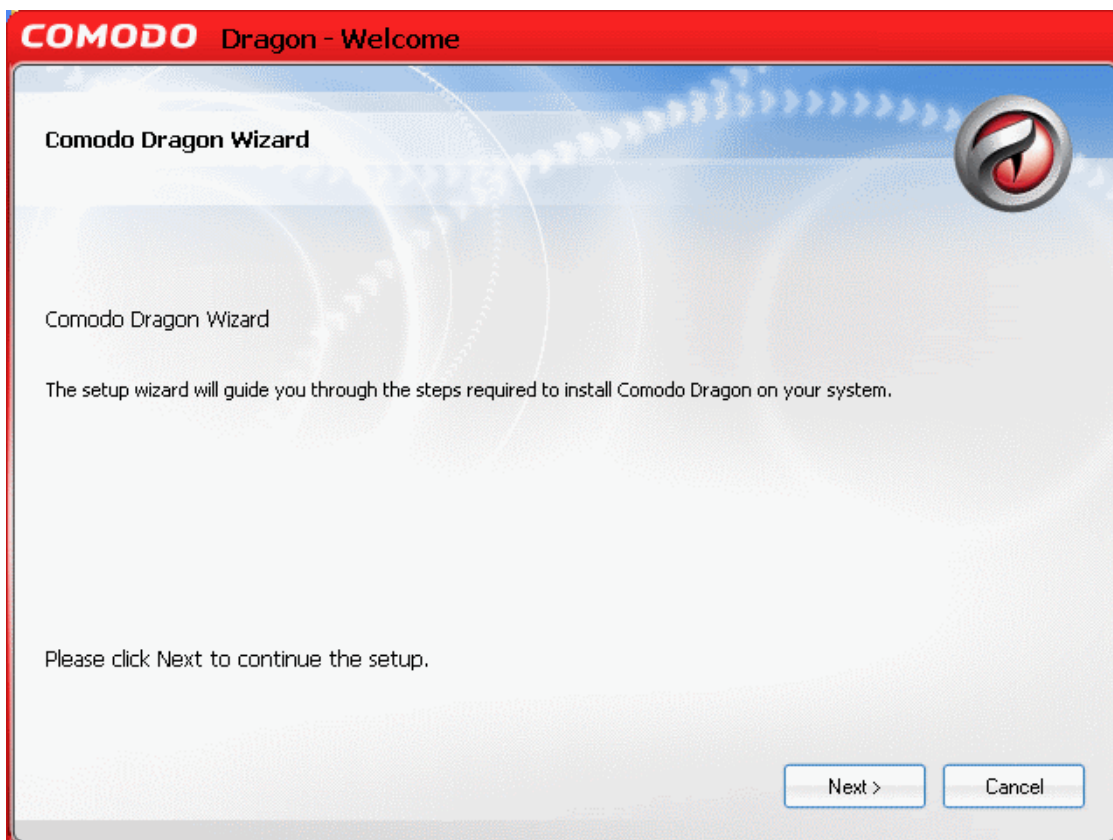
Comodo Dragon is a highly secure, user friendly web browser that makes surfing the web safer, easier and more enjoyable.

#### To install Comodo Dragon

- Click 'Install Dragon Web Browser' from the main Comodo Internet Security 2011 Pro/Complete Installer screen. The installation wizard of Comodo Dragon will start immediately.

#### Step 1 - Welcome Screen

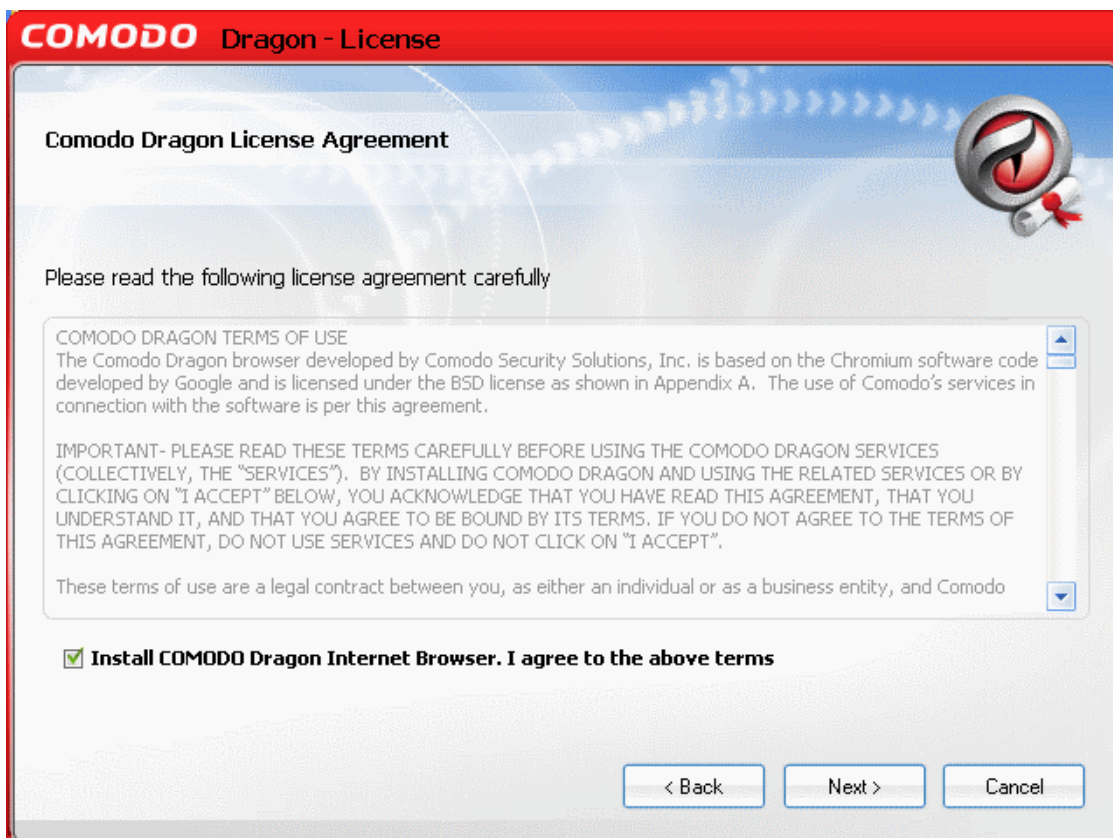
The welcome screen of the wizard will be displayed.



Click 'Next' to continue.

## Step 2 - License Agreement

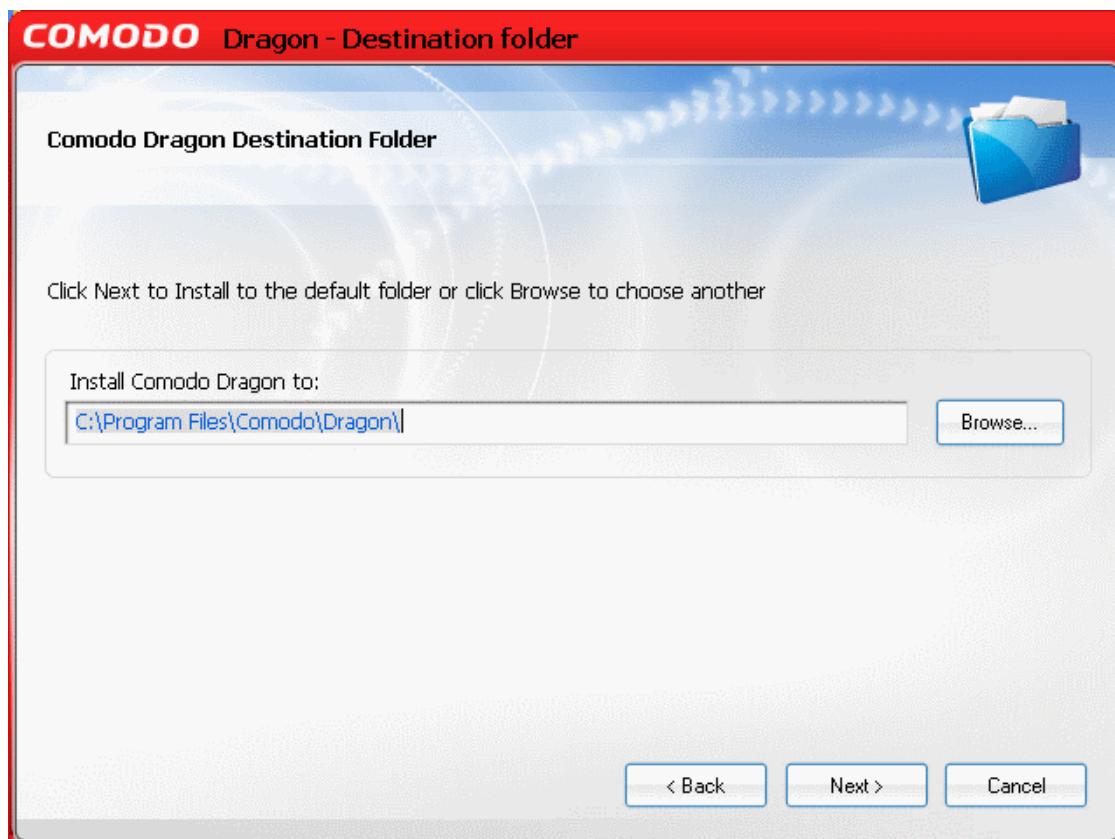
Complete the initialization phase by reading and accepting the License Agreement.



Select the checkbox 'Install Comodo Dragon Internet Browser'. I agree to the above terms and click 'Next'.

## Step 3 - Select Installation Folder

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

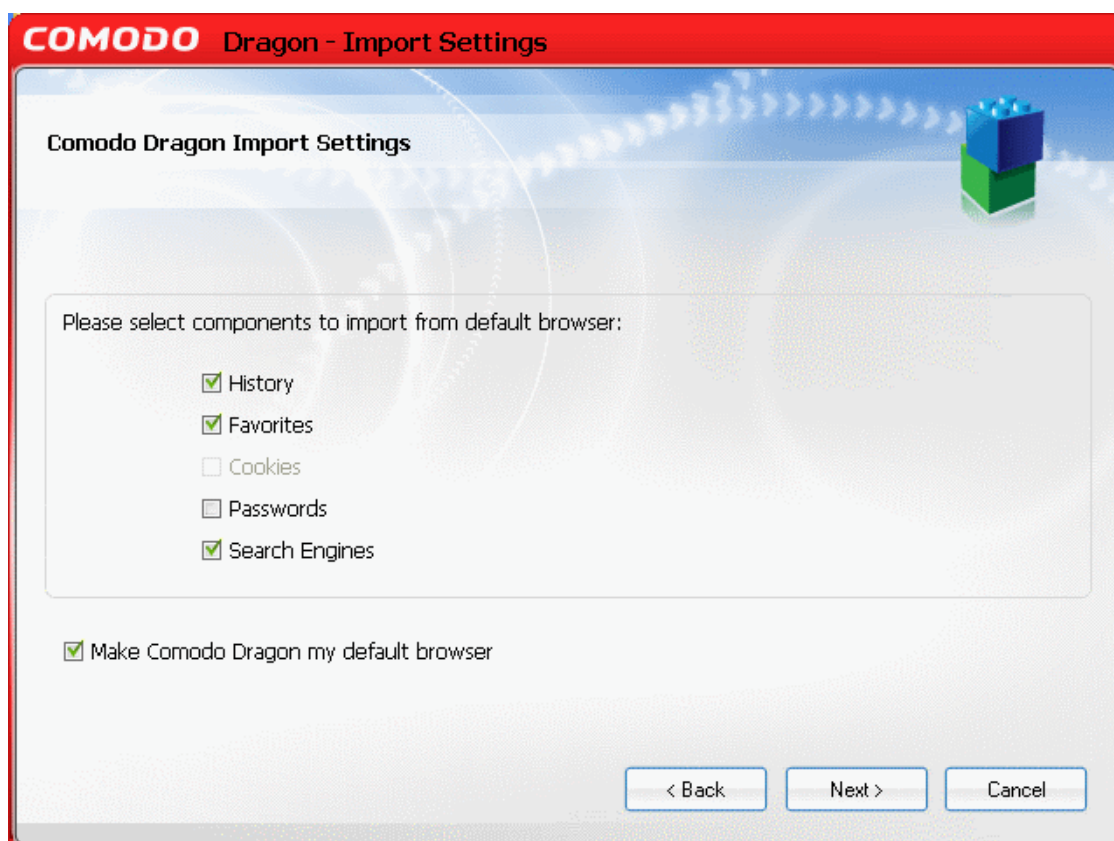


If you want to install the client in a location other than the default location, click 'Browse' to choose a different location. Click 'Next' to continue.

## Step 4 - Import Settings

The next step allows you select the browsing data from your default browser. You can choose to import to your browsing History, stored Favorites, Cookies, saved passwords, favorite search engines. This stage also allows to select Dragon as your default browser.

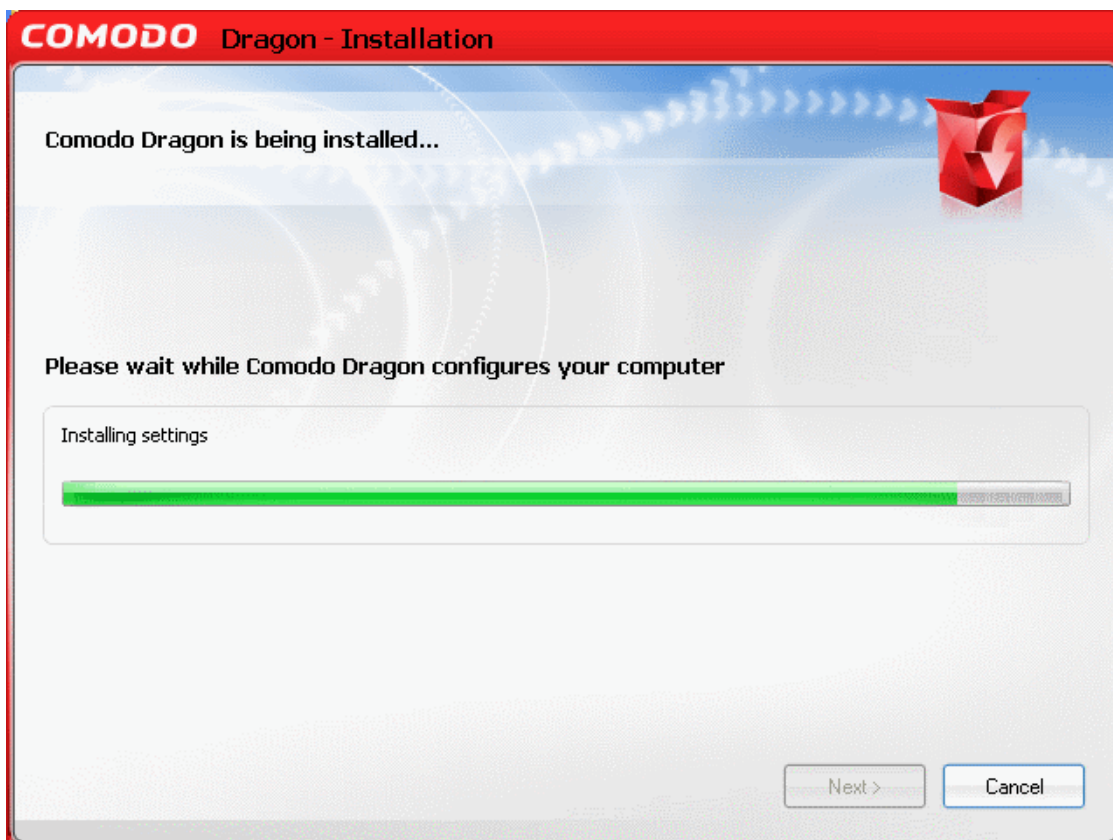




Make your selections and click 'Next'.

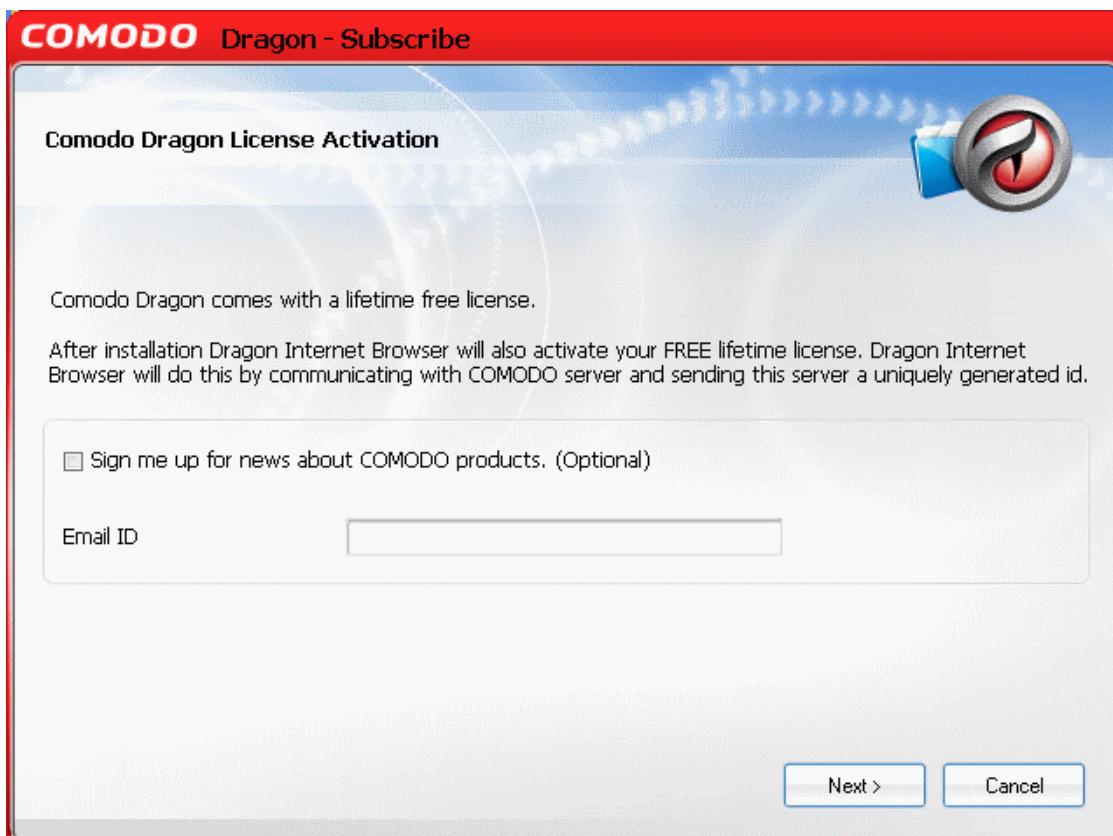
### Step 5 - Installation Progress

The wizard starts installing Dragon. The installation progress will be indicated.



## Step 6 - Product Activation

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

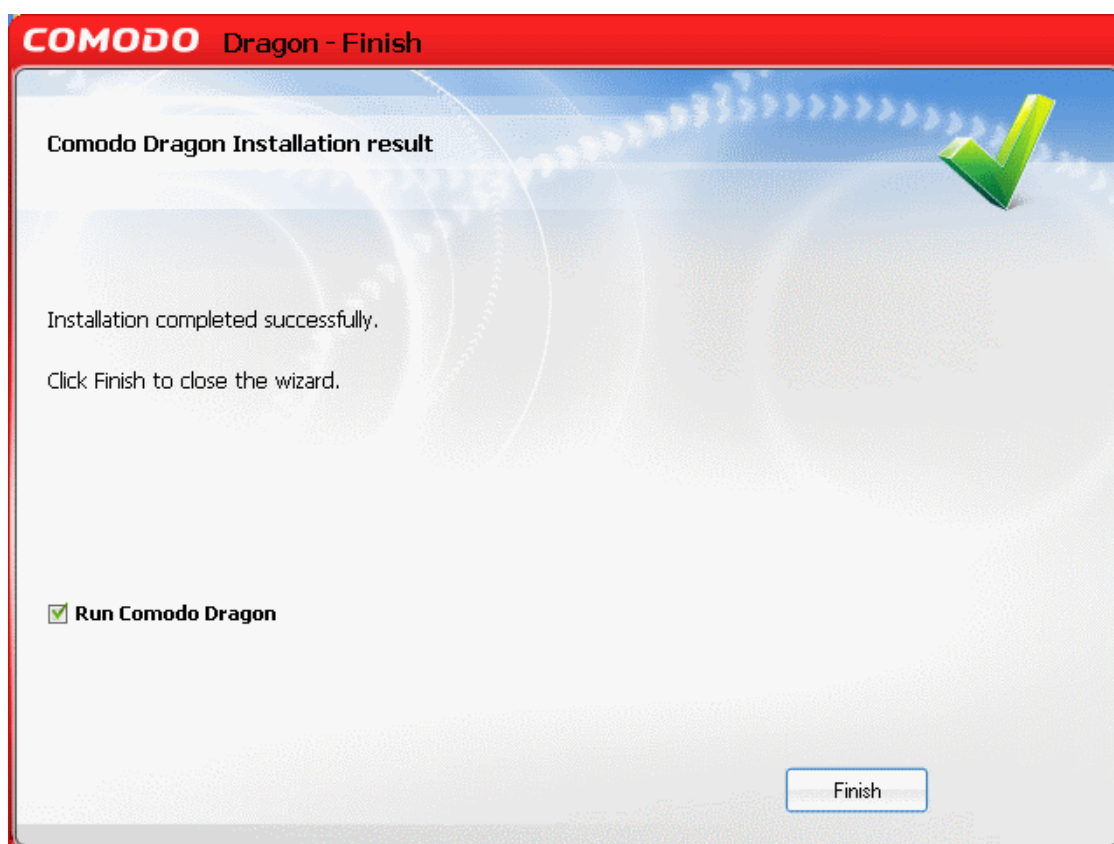




This is optional. Click 'Next'.

## Step 7 - Installation Complete

The Installation Complete dialog is displayed indicating the successful completion of installation.



If you want to run Comodo Dragon Browser immediately, keep the check box 'Run Comodo Dragon' checked, else uncheck it and click 'Finish' to exit the wizard.

### 1.3.4 Activating CIS Pro/Complete Services after Installation

CIS Pro and CIS Complete enable activation of the subscription 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:

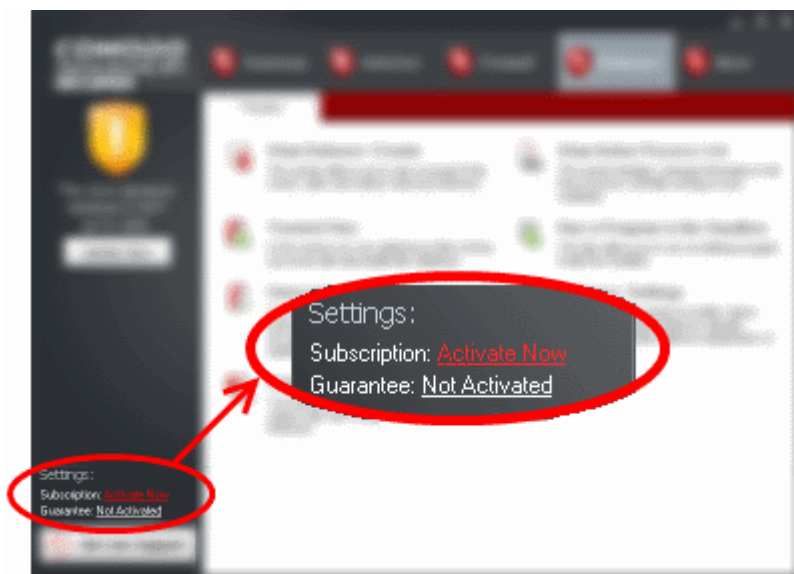
- [Activating your Subscription;](#)
- [Activating your guarantee coverage;](#)
- [Renewal of your Subscription.](#)

#### 1.3.4.1 Activating Your Subscription

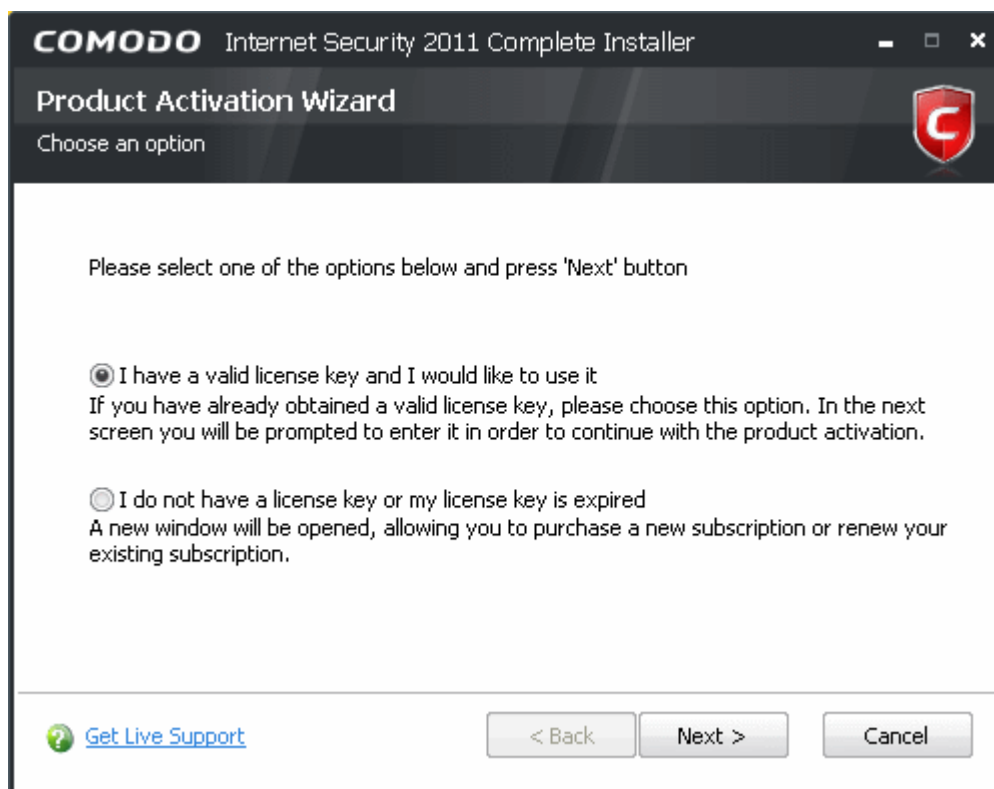
- Start the Comodo Internet Security application as explained in the section [Starting Comodo Internet Security](#).

On the bottom left corner of the main interface, you will see the 'Settings' area.

- Click the link Activate Now link beside Subscription:



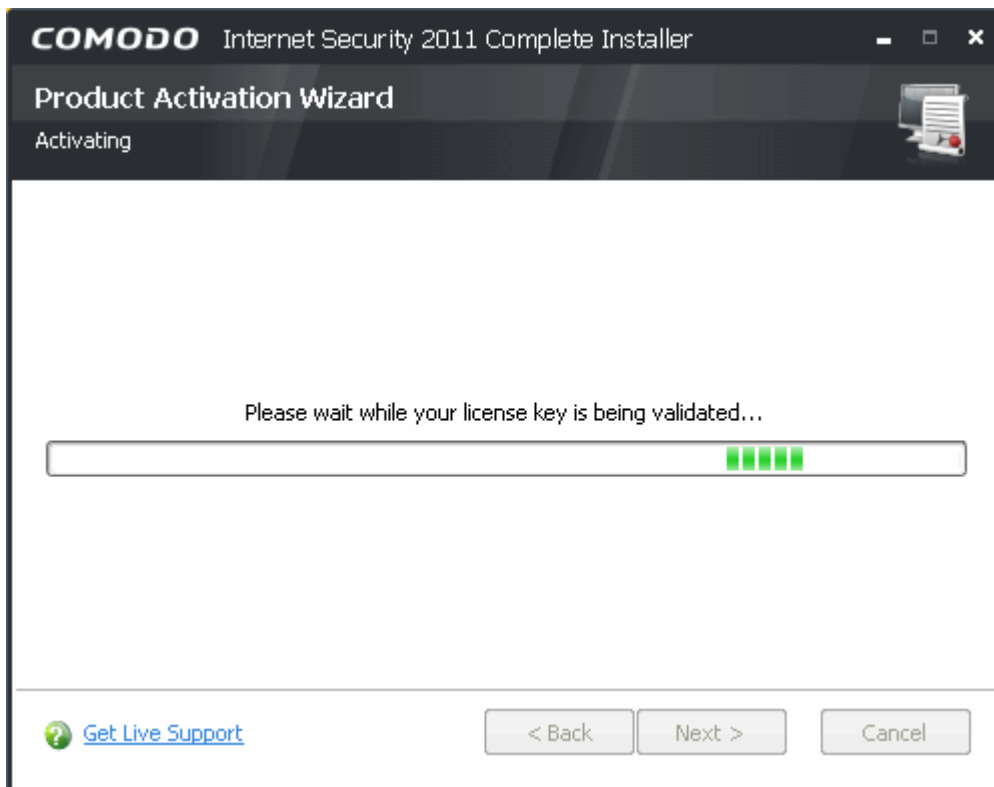
The Product Activation Wizard will start.



- Select 'I have a valid license key and I would use it for activation your new installation' and click 'Next'.



Enter your license key and click 'Next'. The wizard starts validating your license.



On successful validation, your subscription will be activated and a confirmation screen will be displayed with a summary of your license entitlements:



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 'Finish' to exit the wizard.

### 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 subscription. Full details on activating a subscription for CIS Pro can be found in CIS Pro - Installation and Activation and CIS Complete - Installation and Activation.

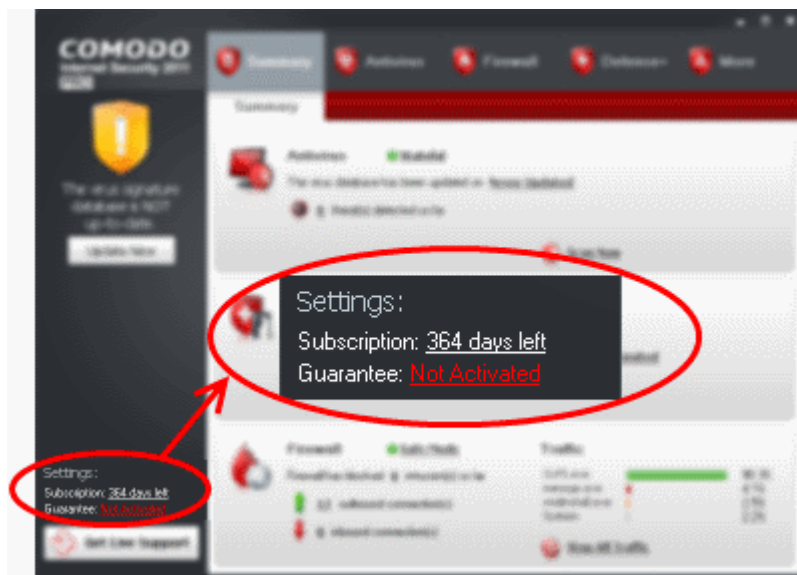
- Please note that if you wish to use and activate the Comodo guarantee then you must have installed Comodo Internet Security (both Antivirus and Firewall components) and Comodo LivePCSupport. You must also have run and passed a Comodo Antivirus scan using the latest signature database. The guarantee is only available if you are a resident of the United States.

**Limits:** The guarantee is limited to the lesser of:

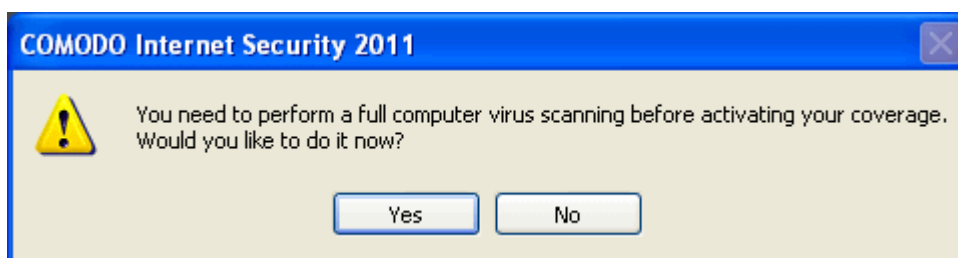
- The actual cost of the computer;
- An aggregate total of \$500 for all claims paid under a single license key, and
- The actual cost of a Comodo specified and authorized third party provider to repair the computer to an operating condition ( Guarantee Limit ).
- The guarantee is limited to repairing 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 End User License Agreement (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 1 of the Installation process of **CIS Pro** or **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](#).

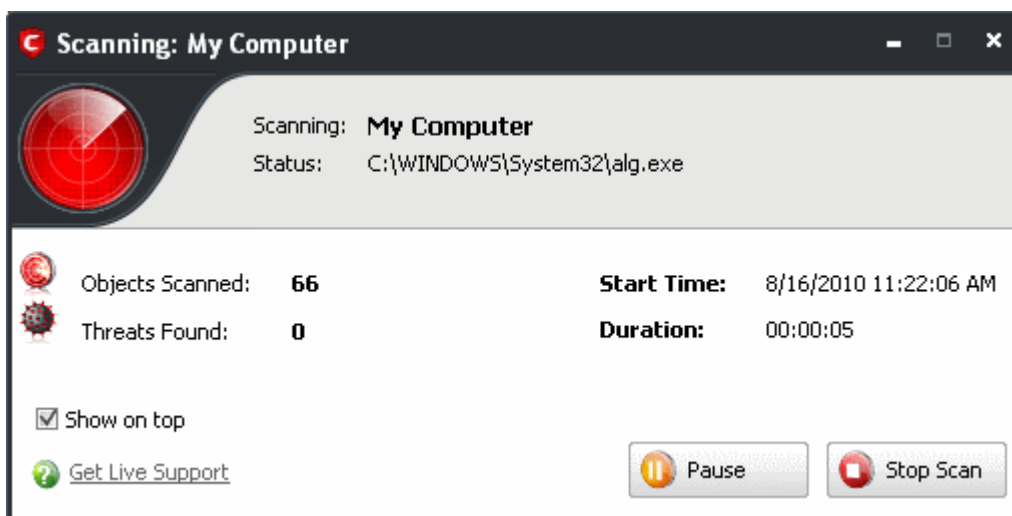
**Step 1:** To activate your guarantee coverage, click 'Not Activated' beside 'Guarantee:' from the Settings area at the bottom left corner of the main interface.



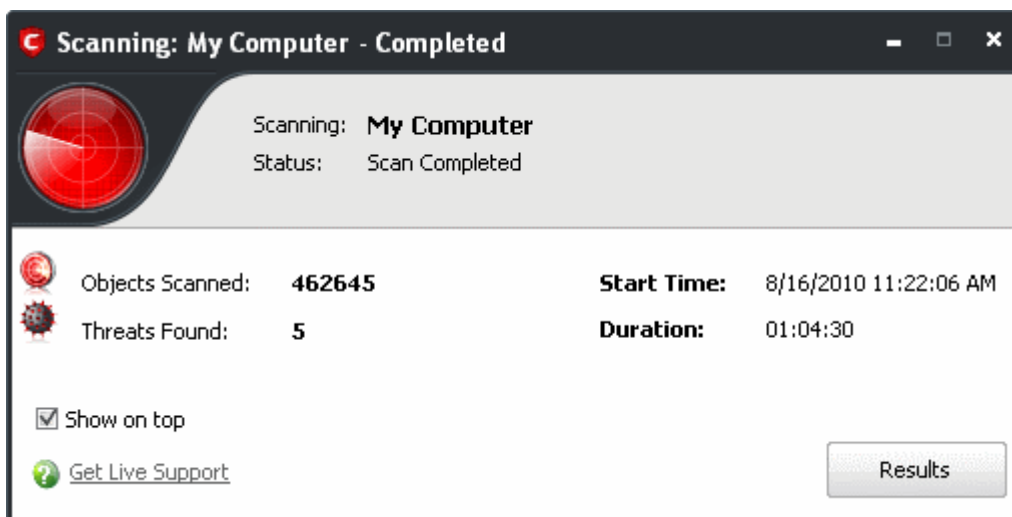
If you have not yet run a full virus scan with the latest signature database (as mentioned [above](#)), you will be asked to do so. A full system scan to remove all known viruses is a mandatory requirement if your computer is to be eligible for guarantee coverage. If this step has already been performed (and your system is clean), then the process moves to [step 2](#).



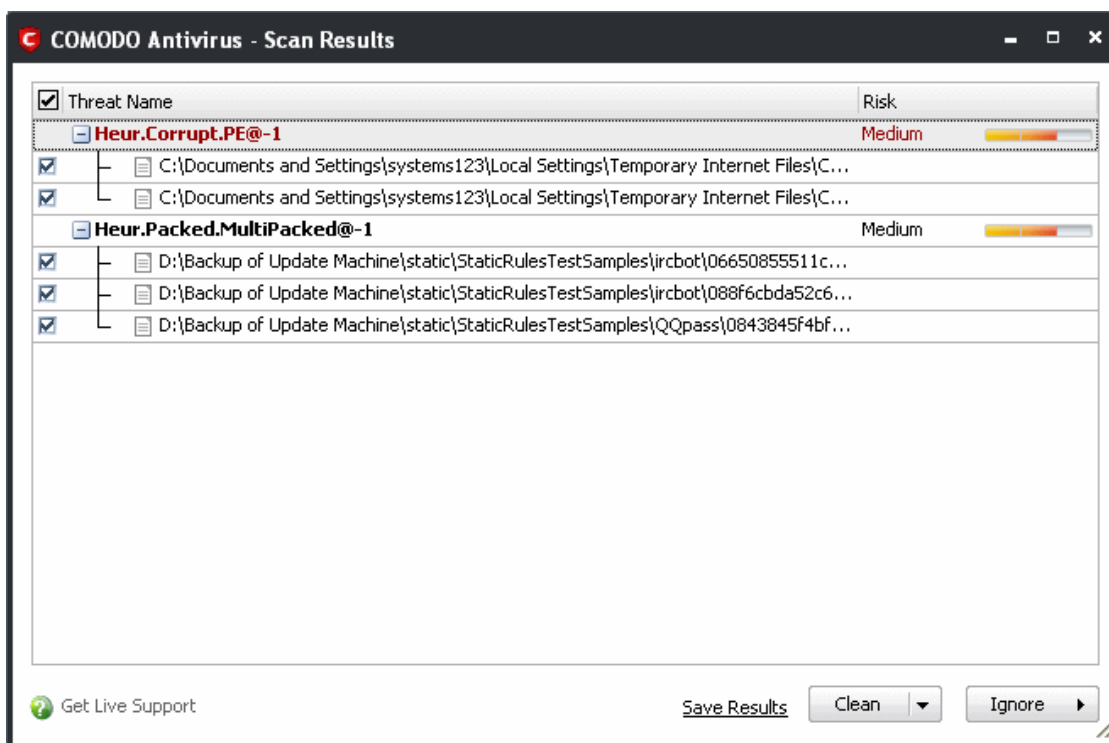
Click 'Yes' to start the scanning.



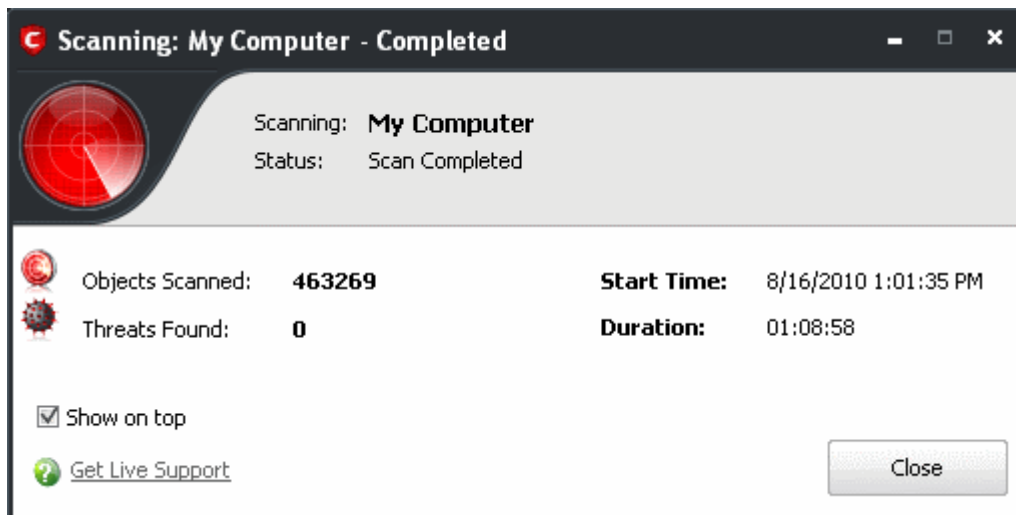
On completion of scanning, the 'scanning completed' window is displayed.



- Click 'Results' to view the Scan Results window. If malicious executables are discovered on your system, the scan results window displays the number of objects scanned and the number of threats (Viruses, Malware and so on).

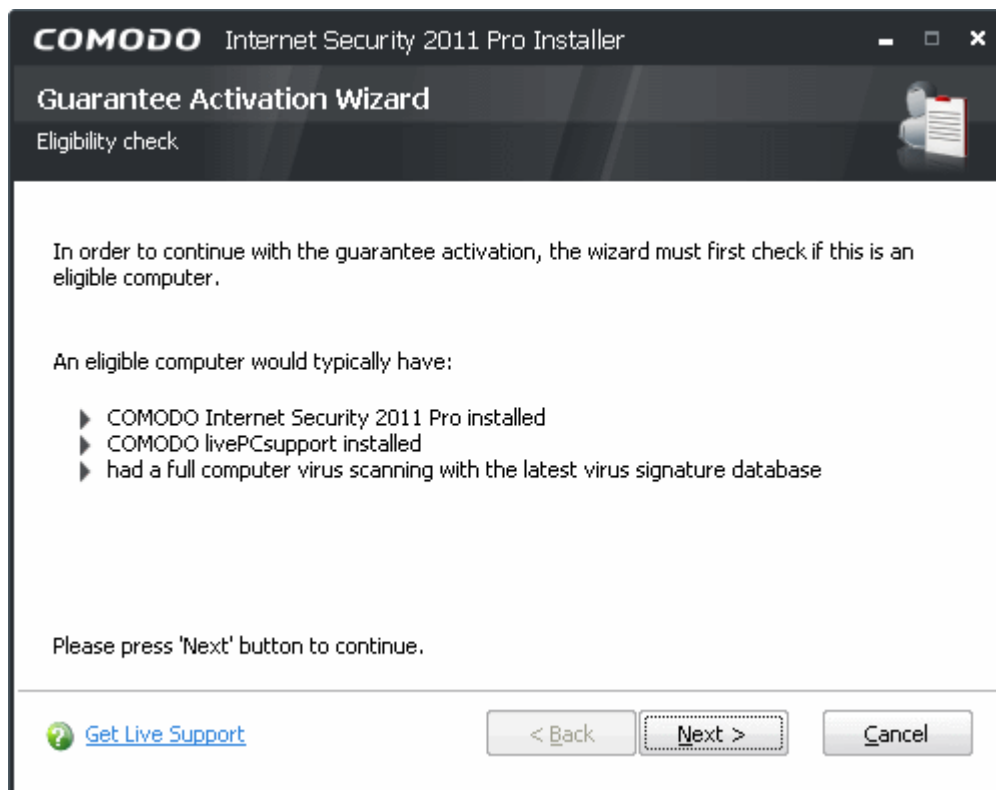


- Click Clean to remove the threats from your computer.
- If No threats are found, click the 'Close' button to return to the main CIS interface.



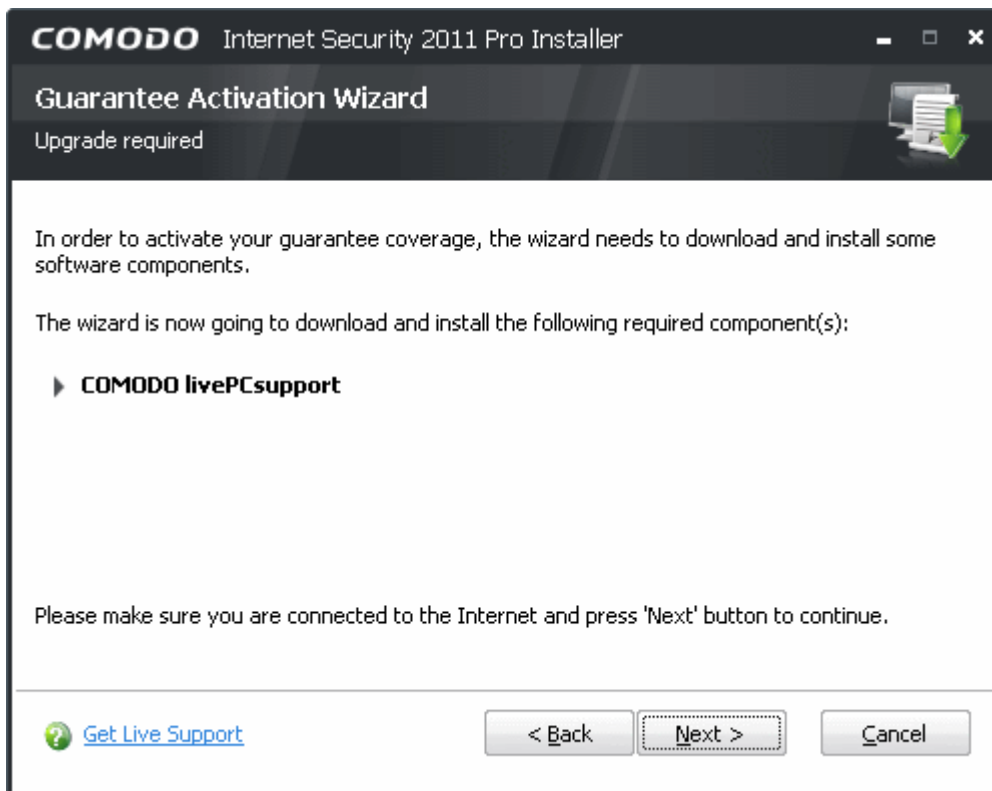
**Step 2:** The next stage is to run the Guarantee Activation Wizard again.

- Click 'Not Activated' beside 'Guarantee:' from the Settings area at the bottom left corner of the main interface.



- Click Next to continue. The wizard will check whether your computer meets the prerequisites for guarantee coverage. The prerequisites are:
  - Comodo Internet Security 2011 (Pro or Complete) is fully installed (both Firewall and Antivirus)
  - Comodo LivePCSupport is installed
  - That your computer has undergone and passed a full virus scan using the latest signature database

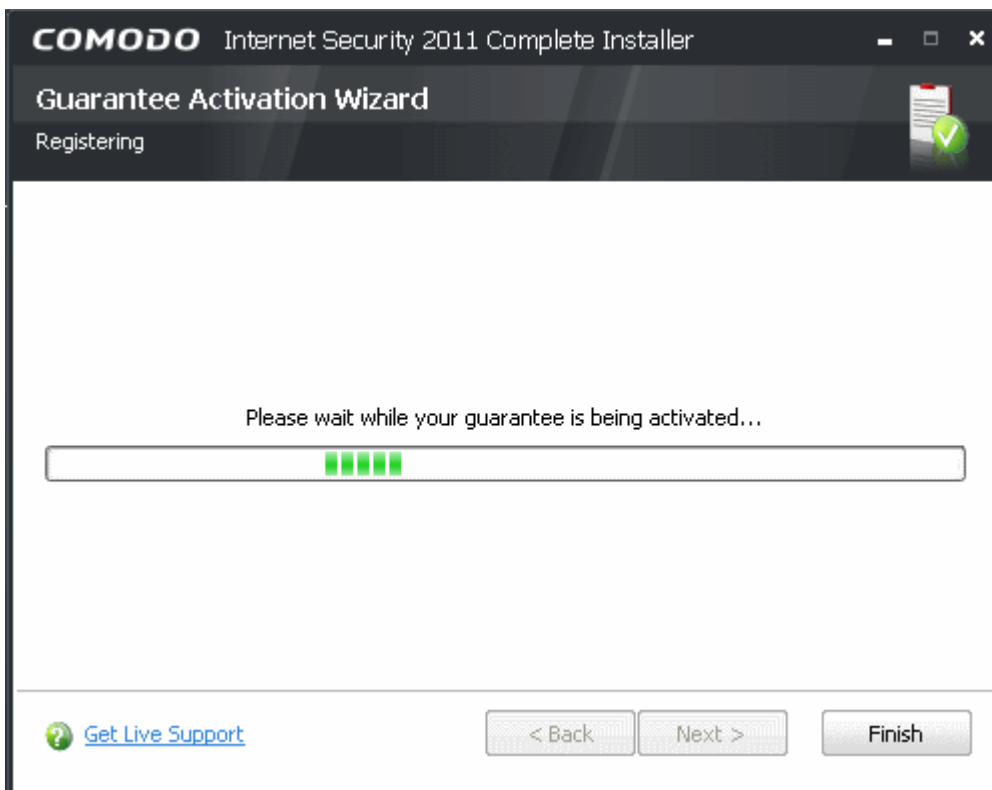
If any of the items listed above are not detected then the next stage of the wizard will implement them (for example, it will install any missing components and start a full virus scan). If all components are present then the process moves to **step 3**.



- Click 'Next' to continue. The wizard will start downloading and installing the components automatically.

### Step 3: Registering Your Guarantee

Your guarantee coverage will be registered...



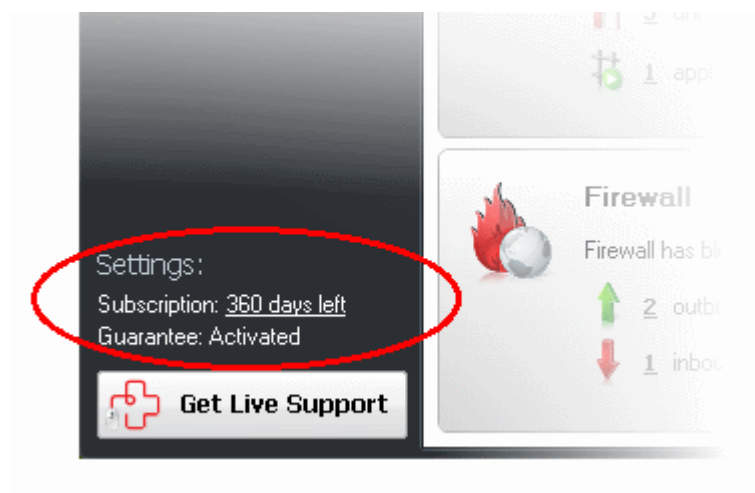
... and on completion, a final confirmation screen indicating successful activation of the Guarantee will be displayed.





- Click 'Finish' to complete the activation wizard.

Successfully activating your Guarantee will change the information displayed in the 'Settings' area:

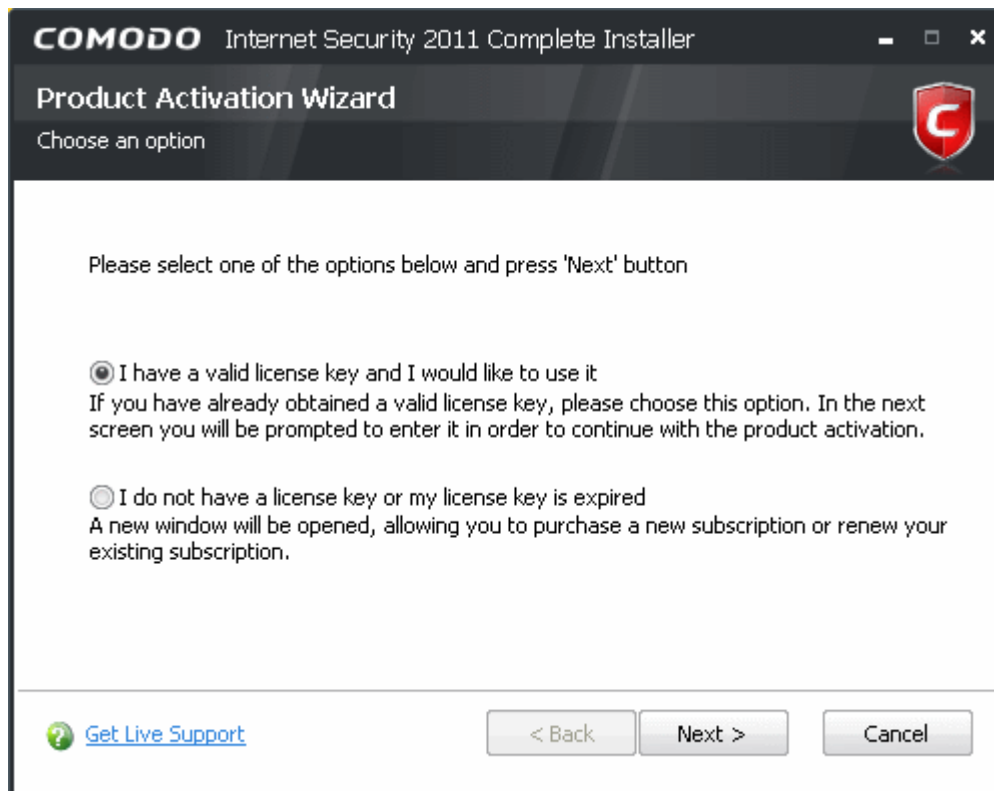


### 1.3.4.3 Renewal of Your Subscription

Your CIS Pro or CIS Complete subscription is valid for one year only. In order to enjoy continuous services from Comodo, you need to renew your subscription.

To renew your subscription click 'Activate Now' beside 'Subscription:' from the Settings area at the bottom left corner of the main interface.

The Product Activation Wizard will start.



- Select 'I do not have a license key or my license key is expired' and click 'Next'.

You will be taken to <https://accounts.comodo.com/cfp/management/signup>.

- Select your CIS Package.
- Select 'Yes' to the question Are you an existing Comodo customer? in Customer information area, enter your login and password and complete the payment procedures.

The Subscription key will be sent to you by email. **Activate your subscription** 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. In order to configure and view settings within Comodo Internet Security, you need to access the management interface.

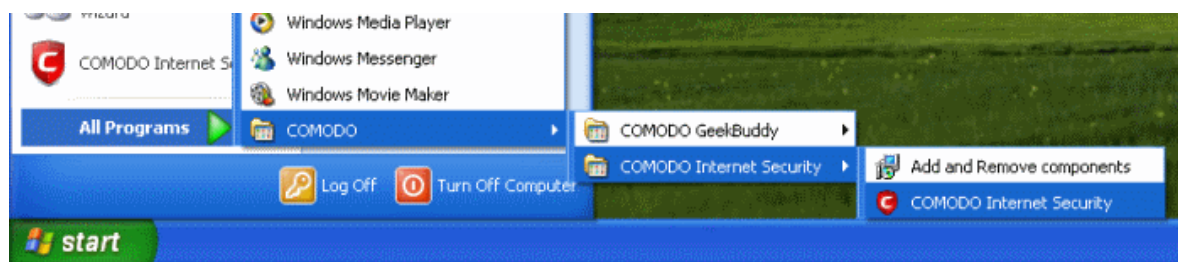
There are 3 different ways to access the management interface of Comodo Internet Security:

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

### Start Menu

You can also 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.



## 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 Antivirus Security Level, Firewall security Level, Defense+ Security Level, Sandbox Security Level, Configuration including Game Mode option.

**Antivirus Security Level** - [Click here](#) for more details on Antivirus Security Level setting

**Firewall Security Level** - [Click here](#) for more details on Firewall security Level setting

**Defense+ Security Level** - [Click here](#) for more details on Defense+ Security Level setting

**Sandbox Security Level** - [Click here](#) for more details on Sandbox Security Level

**Configuration** - [Click here](#) for more details on Configuration settings

**Game Mode** - Switches CIS 2011 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.

## 1.5 Overview of Summary Screens

By default, the management interface displays the 'Summary' area information. You can access this area at any time by selecting the 'Summary' tab as shown in [General Navigation](#).

The specific layout of the summary screen that you see is dependent on the type of installation you chose. Click the links below to view an outline of the summary screen that applies to your installation:

- [COMODO Internet Security with both Antivirus and Firewall](#)
- [COMODO Firewall only](#) or
- [COMODO Antivirus only](#)

## 1.5.1 Comodo Internet Security - Summary



## Summary screen shows the following

## 1. System Status

On the left-hand side of the main interface the status of the system will be displayed and recommendations on actions you need to perform.

## 2. Antivirus

The Antivirus summary box contains:

## i. The Status of Realtime Virus Scanning

The status of the virus scanning setting is displayed as a link (*Stateful* in this example). On clicking this link, the Virus Scanner Settings panel is opened allowing you to quickly set the level of Real Time Scanning, by moving the status slider. For more details on Virus Scanner Settings, refer [Scanner Settings](#).

## ii. When the Virus Database was Last Updated

The day and time at which the virus database was last updated is displayed as a link. On clicking the link, the update of the virus database is started and the current date and time are displayed on completion of the process.

## iii. Number of Detected Threats

The number of threats detected so far from the start of the current session of Comodo Antivirus is displayed here as a link. On clicking the link, Antivirus Events panel is opened. For more details on viewing Antivirus events, refer [Antivirus Events](#).

## iv. Scan Now

The 'Scan Now' link in this box allows you to **Run a Scan**, when clicked.

## 3. Defense+

The Defense+ summary box contains:

## i. Number of Blocked Suspicious Attempts

The number of suspicious attempts blocked by Defense+ from the start of the current session is

displayed as a link . On clicking this link, View Defense+ events is opened. For more details on viewing Defense+ events, refer [View Defense+ events](#).

ii. **Your Current Defense+ Security Level**

Your current Defense+ security level (or Defense+ setting) is displayed as a link (Safe *Mode* in this example). On clicking this link, the Defense+ settings panel is opened to allow you to quickly customize the Defense+ security level by moving the Defense+ security level slider to preset security levels. For a more details on Defense+ settings, refer [Defense+ Settings](#).

iii. **Number of Unrecognized Files**

A numerical summary of all the unrecognized files that are running on your computer is displayed here as a link and how the files are to be treated as set in [Execution Control Settings](#). On clicking the numerical link, **Unrecognized Files** pop-up is displayed with details of each process/application.

You can see in-depth details of all running processes by clicking [View Active Processes](#) in Defense+ center.

iv. **Number of Applications Running in the Sandbox**

The number of files that are currently running in the sandbox is displayed here. For more details on this refer to the sections [Always Sandbox](#) and [Run a Program in the Sandbox](#).

4. **Firewall**

The Firewall summary box contains:

i. **Number of Blocked Intrusion Attempts**

The total number of intrusion attempts blocked by firewall since start of current session of Comodo Internet Security is displayed here as a link. On clicking the link, Firewall Events panel is opened. For more details on viewing Firewall events, refer [View Firewall Events](#).

ii. **Current Firewall Security Level**

Your current Firewall Security Level (or 'Firewall Behavior Setting') is displayed as a link (Safe *Mode* in this example). On clicking this link, the Firewall Behavior Settings panel is opened allowing you to quickly customize the firewall security by moving the Firewall Security Level slider to preset security levels. For more details on Firewall settings, refer [Firewall Behavior Settings](#).

iii. **Inbound/Outbound Connections**

A numerical summary of currently active inbound and outbound connections to and from your computer is displayed here. The numbers are displayed as links. On clicking any number, **Active Connections** panel is opened. For more details on viewing active connections, refer [View Active Connections](#).

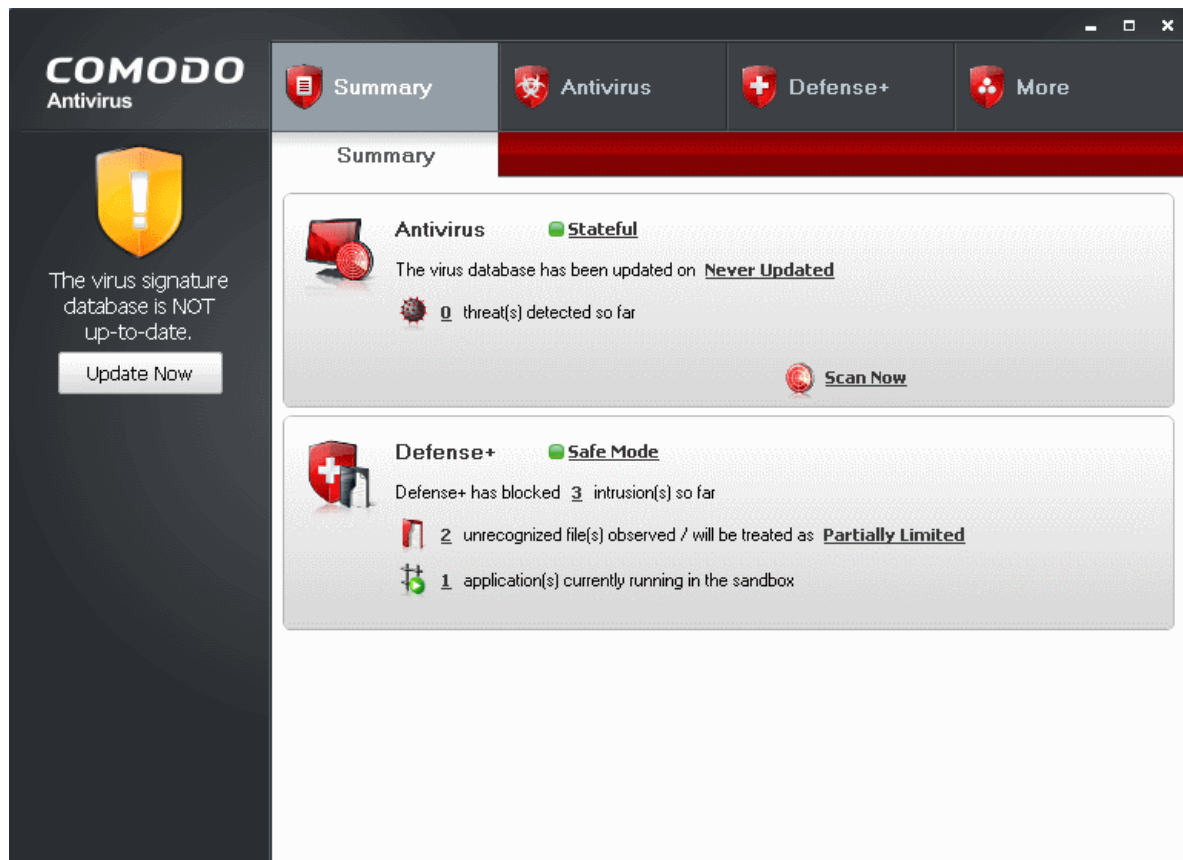
iv. **Traffic**

The Traffic area in the Summary screen of Comodo Firewall displays a bar graph showing the applications that are currently connected to the Internet and are sending or receiving data. The summary also displays the % of total traffic each application is responsible for and the file name of the executable. Clicking on any application name opens View Active Connections interface.

v. **Stop All Traffic/Restore All Traffic**

This link allows you to toggle network activity between **on** and **off**. Specifically, clicking **Stop All Traffic** instantly blocks all incoming and outgoing network connections, placing the firewall in the '**Block All Mode**' of [Firewall Behavior Settings](#). Similarly, clicking **Restore All Traffic** re-implements your previous [Firewall Security Level](#).

## 1.5.2 Comodo Antivirus - Summary

**Summary screen shows the following**1. **System Status**

On the left-hand side of the main interface the status of the system will be displayed and recommendations on actions you need to perform.

2. **Antivirus**

The Antivirus summary area contains:

i. **The Status of Realtime Virus Scanning**

The status of the virus scanning setting is displayed as a link (*Stateful* in this example). On clicking this link, the Virus Scanner Settings panel is opened allowing you to quickly set the level of Real Time Scanning, by moving the status slider. For more details on Virus Scanner Settings, refer to **Scanner Settings**.

ii. **When the Virus Database was Last Updated**

The day and time at which the virus database was last updated is displayed as a link. On clicking the link, the update of the virus database is started and the current date and time are displayed on completion of the process.

iii. **Number of Detected Threats**

The number of threats detected so far from the start of the current session of Comodo Antivirus is displayed here as a link. On clicking the link, Antivirus Events panel is opened. For more details on viewing Antivirus events, refer **Antivirus Events**.

iv. **Scan Now**

The 'Scan Now' link in this box allows you to **Run a Scan**, when clicked.

3. **Defense+**

The Defense+ summary box contains:

i. **Number of Blocked Suspicious Attempts**



The number of suspicious attempts blocked by Defense+ from the start of the current session is displayed as a link. On clicking this link, View Defense+ events is opened. For more details on viewing Defense+ events, refer [View Defense+ events](#).

ii. **Your Current Defense+ Security Level**

Your current Defense+ security level (or Defense+ setting) is displayed as a link (Safe Mode in this example). On clicking this link, the Defense+ settings panel is opened to allow you to quickly customize the Defense+ security level by moving the Defense+ security level slider to preset security levels. For a more details on Defense+ settings, refer [Defense+ Settings](#).

iii. **Number of Unrecognized Files**

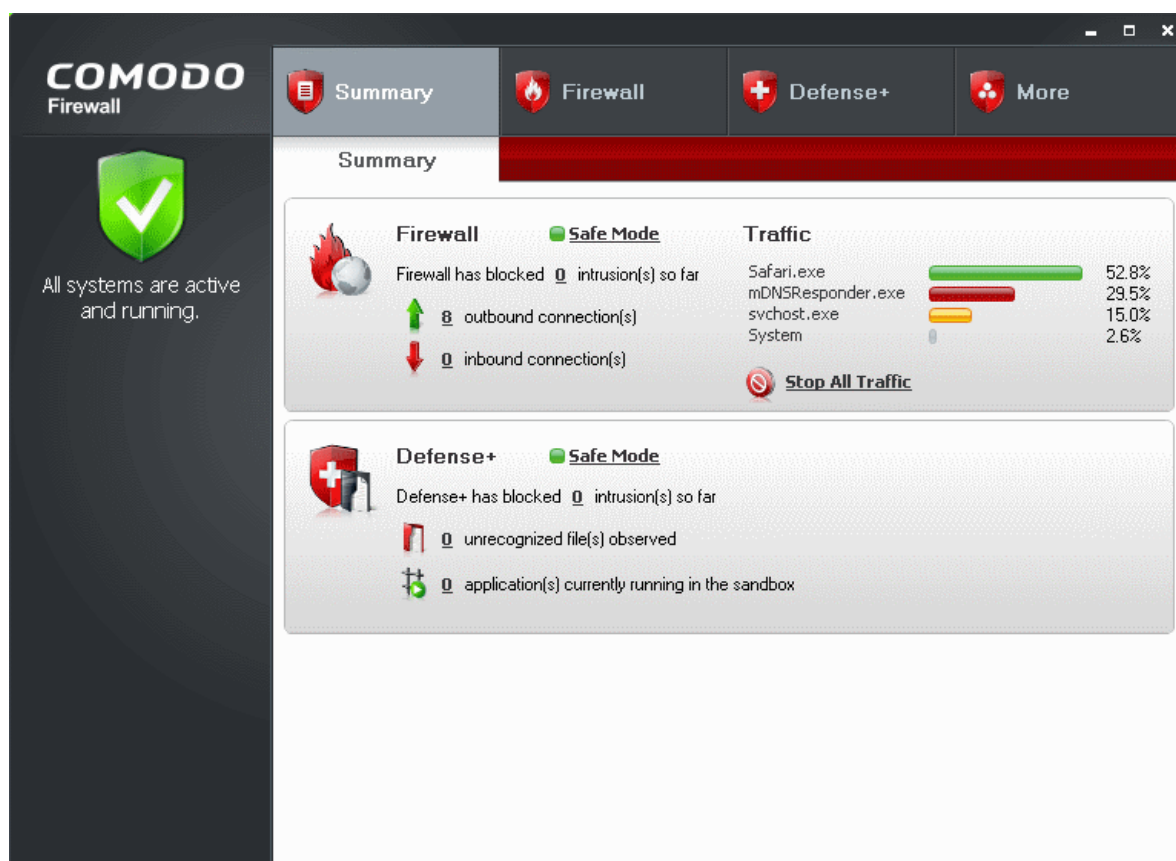
A numerical summary of all the unrecognized files that are running on your computer is displayed here as a link and how the files are to be treated as set in [Execution Control Settings](#). On clicking the numerical link, **Unrecognized Files** pop-up is displayed with details of each process/application.

You can see in-depth details of all running processes by clicking [View Active Processes](#) in Defense+ center.

iv. **Number of Applications Running in the Sandbox**

The number of files that are running currently in the sandbox is displayed here. For more details on this refer [Always Sandbox](#) and [Run a Program in the Sandbox](#).

### 1.5.3 Comodo Firewall - Summary



#### Summary screen shows the following

1. **System Status**

On the left-hand side of the main interface the status of the system will be displayed.

2. **Firewall**

The Firewall summary box contains:

i. **Number of Blocked Intrusion Attempts**

The total number of intrusion attempts blocked by firewall since start of current session of Comodo Internet Security is displayed here as a link. On clicking the link, Firewall Events panel is opened. For more details on viewing Firewall events, refer [View Firewall Events](#).

- ii. **Current Firewall Security Level**

Your current Firewall Security Level (or 'Firewall Behavior Setting') is displayed as a link (*Safe Mode* in this example). On clicking this link, the Firewall Behavior Settings panel is opened allowing you to quickly customize the firewall security by moving the Firewall Security Level slider to preset security levels. For more details on Firewall settings, refer [Firewall Behavior Settings](#).
  - iii. **Inbound/Outbound Connections**

A numerical summary of currently active inbound and outbound connections to and from your computer is displayed here. The numbers are displayed as links. On clicking any number, **Active Connections** panel is opened. For more details on viewing active connections, refer [View Active Connections](#).
  - iv. **Traffic**

The Traffic area in the Summary screen of Comodo Firewall displays a bar graph showing the applications that are currently connected to the Internet and are sending or receiving data. The summary also displays the % of total traffic each application is responsible for and the file name of the executable. Clicking on any application name opens View Active Connections interface.
  - v. **Stop All Traffic/Restore All Traffic**

This link allows you to toggle network activity between **on** and **off**. Specifically, clicking **Stop All Traffic** instantly blocks all incoming and outgoing network connections, placing the firewall in the '**Block All Mode**' of [Firewall Behavior Settings](#). Similarly, clicking **Restore All Traffic** re-implements your previous [Firewall Security Level](#).
3. **Defense+**
- The Defense+ summary box contains:
- i. **Number of Blocked Suspicious Attempts**

The number of suspicious attempts blocked by Defense+ from the start of the current session is displayed as a link . On clicking this link, View Defense+ events is opened. For more details on viewing Defense+ events, refer [View Defense+ events](#).
  - ii. **Your Current Defense+ Security Level**

Your current Defense+ security level (or Defense+ setting) is displayed as a link (*Safe Mode* in this example). On clicking this link, the Defense+ settings panel is opened to allow you to quickly customize the Defense+ security level by moving the Defense+ security level slider to preset security levels. For a more details on Defense+ settings, refer [Defense+ Settings](#).
  - iii. **Number of Unrecognized Files**

A numerical summary of all the unrecognized files that are running on your computer is displayed here as a link and how the files are to be treated as set in [Execution Control Settings](#). On clicking the numerical link, **Unrecognized Files** pop-up is displayed with details of each process/application.

You can see in-depth details of all running processes by clicking [View Active Processes](#) in Defense+ center.
  - iv. **Number of Applications Running in the Sandbox**

The number of files that are currently running in the sandbox is displayed here. For more details on this refer [Always Sandbox](#) and [Run a Program in the Sandbox](#).

## 1.6 Comodo Internet Security - Navigation

After installation, Comodo Internet Security automatically protects any computer on which it is installed. You do not have to start the program to be protected.

See [Starting Comodo Internet Security](#) if you are unsure of how to access the main interface.

### Persistent Navigation

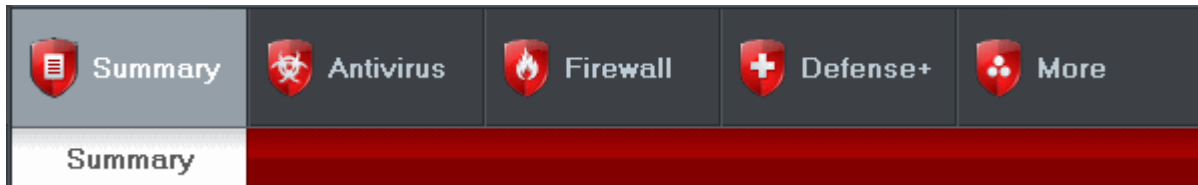
Comodo Internet Security is divided into five main areas indicated by the tabs with respective icons at the top right hand side of the main interface screen.

- [Summary](#)
- [Antivirus](#)
- [Firewall](#)



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

Each of these areas contains several sub-sections that provide total control over configuration of the security Suite. These icons are ever-present and can be accessed at all times.



- **Summary** - Contains at-a-glance details of important settings, activity and other information. The summary screen differs for different types of installation, namely:
  - [Comodo Internet Security](#)
  - [Comodo Antivirus](#)
  - [Comodo Firewall](#)

See the [Overview of summary screens](#) section for more details on this area.

- **Antivirus** - Clicking this icon opens [Antivirus Tasks](#) configuration screen.
- **Firewall** - Clicking this icon opens [Firewall Tasks](#) configuration screen. Advanced users are advised to first visit the [Network Security Policy](#) area for an introduction to firewall policies and rule creation.
- **Defense+** - Clicking this icon opens [Defense+ Tasks](#) configuration screen. Advanced users are advised to first visit the [Computer Security Policy](#) area for an introduction to Defense+ policies, rule creation and Sandboxing features.
- **More** - Clicking this icon opens [More](#) options screen which contains several options relating to overall configuration of Comodo Internet Security.

## 1.7 Understanding Alerts

After first installing Comodo Internet Security, it is likely to see a number of pop-up alerts. This is perfectly normal and indicates that the security suite is learning the behavior of your applications and establishing which programs need privileges such as 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 allow you to instruct Comodo Internet Security on how it should behave in future when it encounters activities of the same type.

**Buffer Overflow Protection Feature** - Buffer overflow attack occurs when a malicious program or script deliberately sends more data to its memory buffer than the buffer can handle. Defense+ provides [alerts](#) on attempt of most types of buffer overflow attacks and provides protection against data theft, computer crashes and system damage. For more details, please refer [Defense+ Settings](#) > [Execution Control Settings](#) > [Detect Shell Code Injections](#).

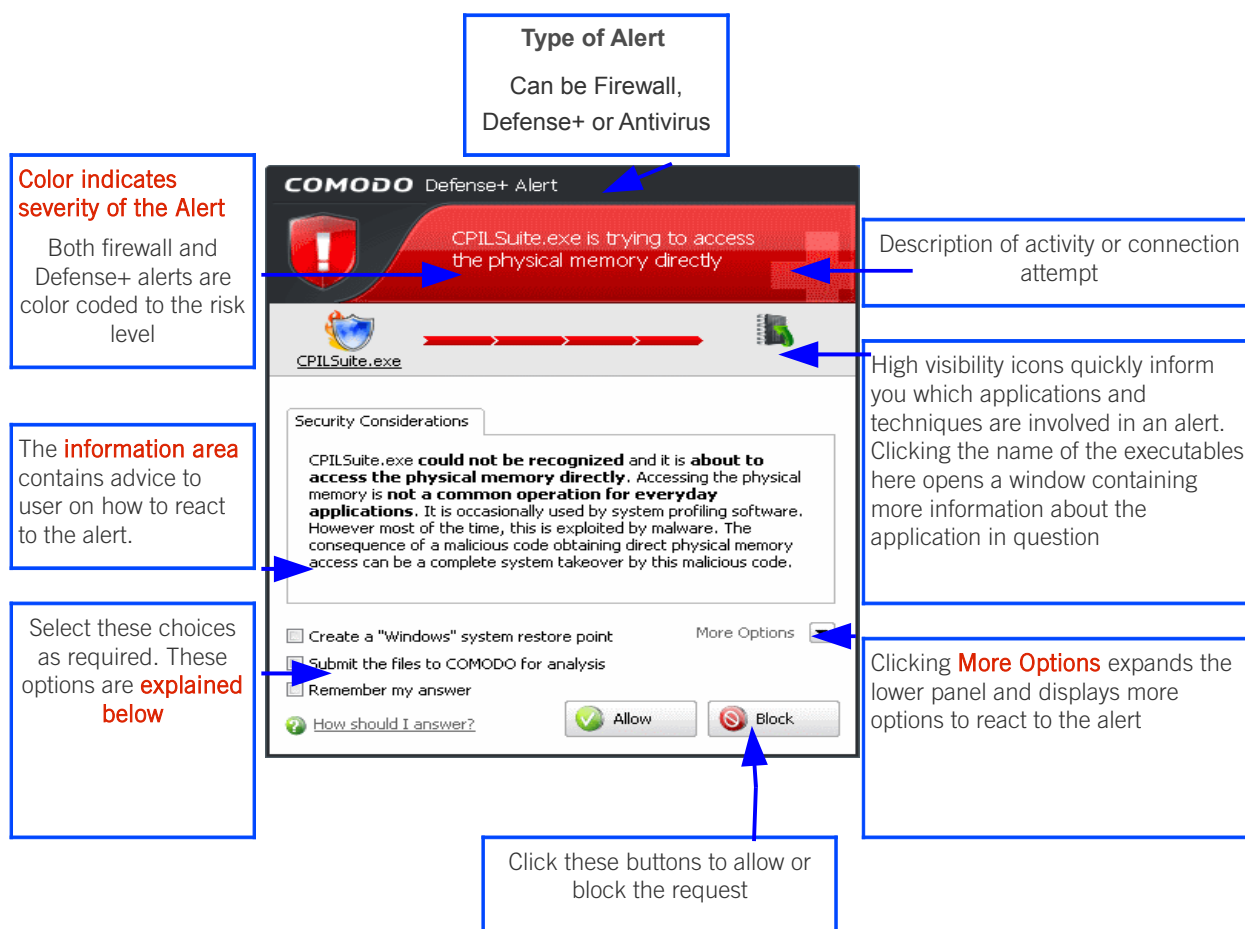
### Alerts Overview

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

- [Antivirus Alerts](#)
- [Firewall Alerts](#)
- [Defense+ Alerts](#) (including [Elevated Privilege Alerts](#))
- [Sandbox Alerts](#)

Broadly speaking, Antivirus alerts inform you when a virus or malware is executed into your system, Firewall alerts inform you about network connection attempts and Defense+ alerts tell you about the behavior of application on your system. In all the three cases, the alert can contain very important security warnings or may simply occur because you are running an application for the first time. Your reaction should depend on the information that is presented at the alert.

An example alert is shown below.



## Severity Level

The upper strip of both Defense+ and Firewall alerts are color coded according to risk level. This provides a fast, at-a-glance, indicator of the severity of the alert. However, it cannot be stressed enough that you should still read the 'Security Considerations' section in order to reach an informed decision on allowing or blocking the activity.

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

- **Yellow Alerts** - Low Severity - In most cases, you can safely approve these connection request or activity. The 'Remember my answer for this application' option is automatically pre-selected for safe requests
- **Orange Alerts** - Medium Severity - Carefully read the 'Security Considerations' section 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 Alerts** - 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.

## Information on the Alert

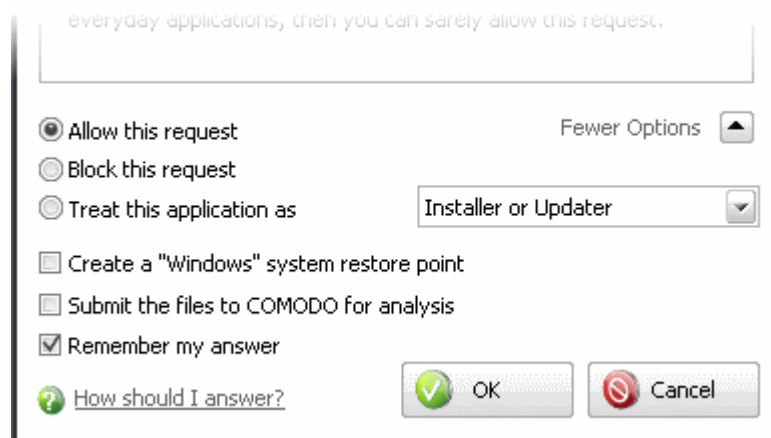
**Security Considerations:** The Security Considerations area contains a description of the nature of the alert. It tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find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



- **Remember my answer** - Select this option if you want Firewall to implement the same decision for identical requests in future - meaning you are not prompted if same type of activity or connection attempt arises in future. The response you made this time is applied automatically to the all the similar activities or connection attempts.

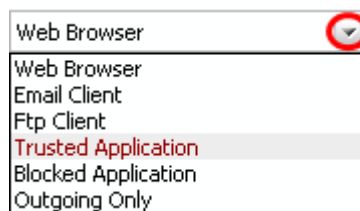
### More Options

Clicking the More Options in the Firewall alert expands the lower panel and displays more options for reacting to the alert.



The first three options enable you to select your reaction to the activity or connection attempt requested.

- **Allow this request** - Allows the requested activity or connection attempt
- **Block this request** - Denies the requested activity or connection attempt.
- **Treat this application as** - Enables you to select a predefined security policy to be deployed on to the application in question. Select this option and select a predefined policy depending on the trustworthiness and type of the application.



Refer to [Predefined Firewall Policies](#) and [Predefined Computer Security Policies](#) for more details.

- **Submit the files to COMODO for analysis** - Select this option if you suspect that the application that has raised this alert as a malware. Comodo Internet Security sends the application to Comodo automatically, irrespective of your Allow or Block response. Comodo analyzes the application and includes it in the safe list or black list accordingly.
- **Create a "Windows" system restore point** - Selecting this option instructs your Windows Operating System to create a restore point. This enables you to safely rollback your system to the previous system state if you encounter problems because of allowing or blocking this request.
  - If you have Comodo Time Machine (CTM) installed then CIS creates a Time Machine restore point.
  - If you do not have Comodo Time Machine installed, then CIS creates a regular Windows System Restore point.

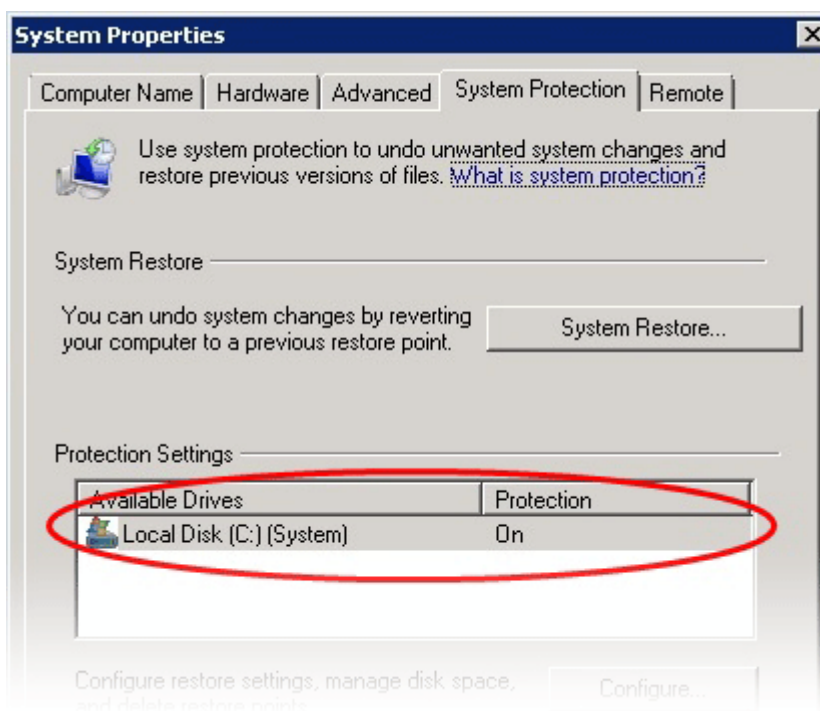
**Note:** This option is only available if Windows System Restore is enabled in your system. You can check whether system restore is enabled by visiting the Windows control panel:

- [Click here if you are using Windows 7](#)
- [Click here if you are using Windows Vista](#)
- [Click here if you are using Windows XP](#)

## Windows 7

### To ensure that Windows system restore is enabled

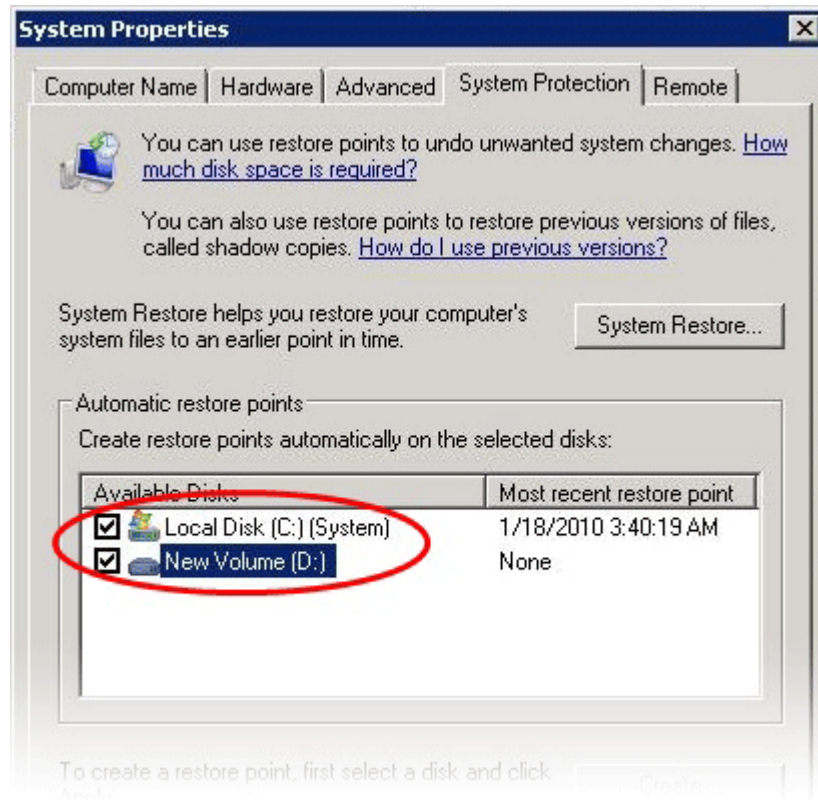
1. Click Start > Control Panel > System > System Protection
2. Make sure that the Protection status of the hard disk drive partition(s) is set to 'On' under 'Protection Settings'.



## Windows Vista

### To ensure that Windows system restore is enabled

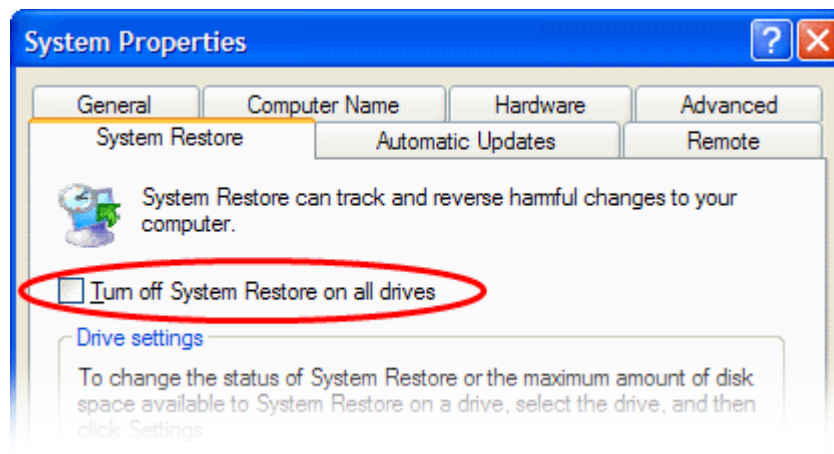
1. Click Start > Control Panel > System > System Protection
2. Make sure that the checkbox(es) beside the hard disk drive partition(s) under 'Automatic restore points > Create restore points automatically on the selected disks' are selected.



## Windows XP

### To ensure that Windows system restore is enabled

1. Click Start > Control Panel > System > System Restore tab
2. Make sure that the checkbox 'Turn off System Restore on all drives' is NOT selected.



If Comodo Time Machine (CTM) is installed in your system, the restore point is created by it irrespective of whether the Windows Restore Point is enabled in your system or not.

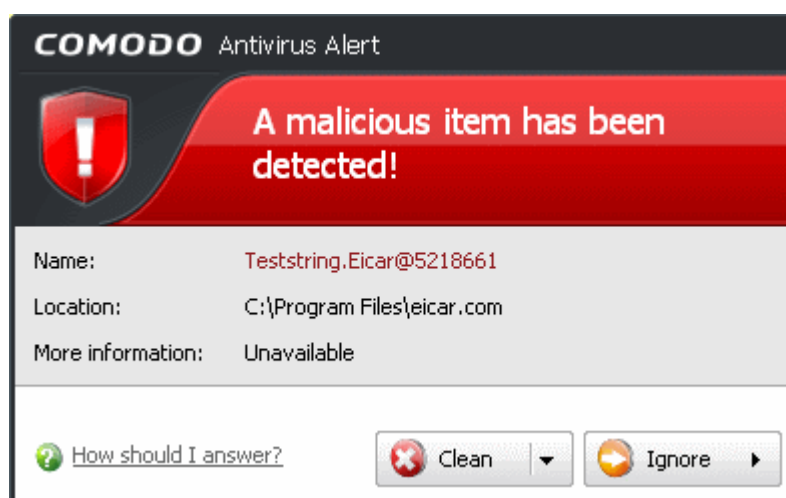
**Background Note:** Comodo Time Machine is a powerful system rollback utility that allows you to quickly restore your computer to an earlier point in time. The software is free of charge and allows you to quickly recover your computer to its last working state in the event of malware attacks or system crashes. Find out more and download the application from <http://www.comodo.com/home/data-storage-encryption/data-recovery.php>.

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

### Answering an Antivirus Alert

Comodo Internet Security generates an Antivirus alert whenever a virus or malware tries to be copied or executed without your knowledge and displays the alert at the bottom right hand side of your computer screen. These alerts are a valuable source of real-time information that helps the user to immediately identify which particular files are infected or are causing problems and the choices for actions to be taken.

The alert contains the name of the virus detected and the location of the file or application infected by it.

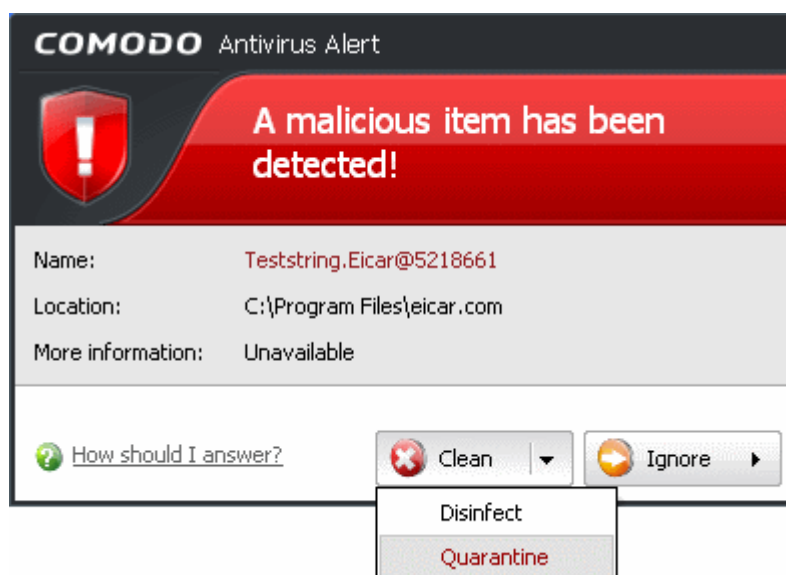


You can take one of the following steps to answer the Antivirus alert.

- Move the file or application to **Quarantined Items** for later analysis, if you feel that the virus appears to be suspicious.
- Disinfect the file if there exists a disinfection routine for the detected file.
- Delete the file or application from your system if you do not trust the application.
- Ignore the alert only if you trust the application or the source of application by clicking 'Ignore'.

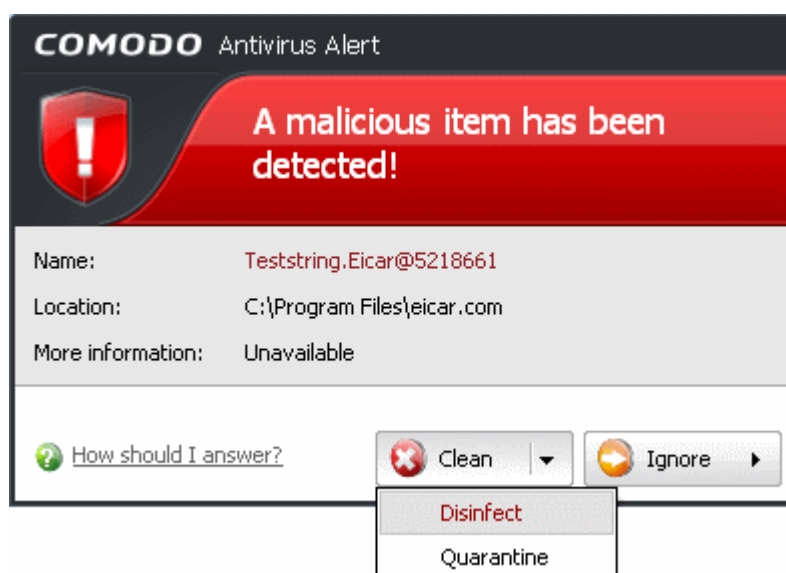
### To move the file or application to Quarantine

- Click the drop-down arrow beside the 'Clean' button and select 'Quarantine' from the 'Clean' options.



### To disinfect the file/application

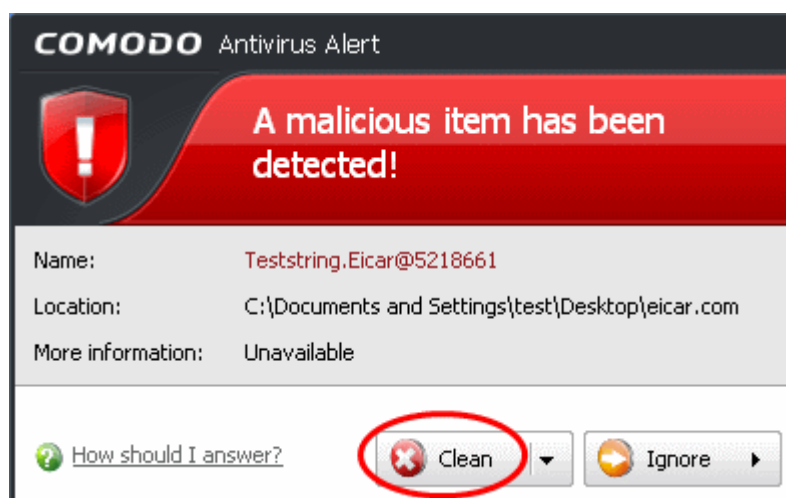
- Click the drop-down arrow beside the 'Clean' button and select 'Disinfect' from the 'Clean' options.



### To permanently delete the file or application

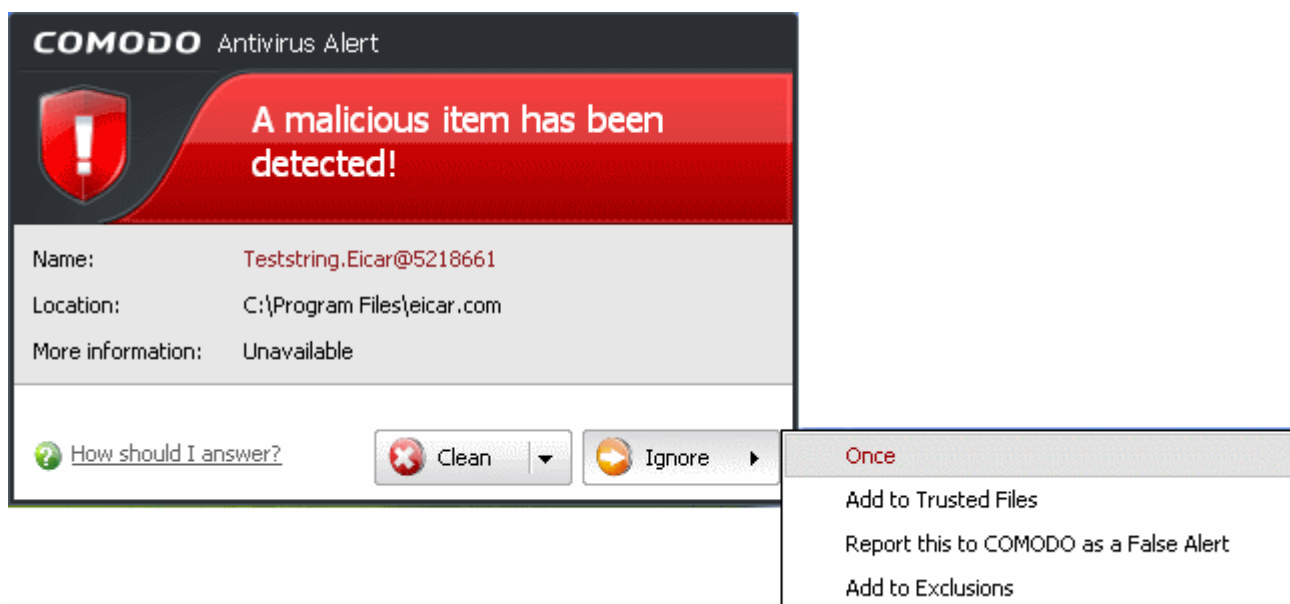
- Click the 'Clean' button





### To ignore the alert if you trust the file/application

- Click 'Ignore'. Selecting Ignore provides you with four options.



- Once.** If you click 'Once', the virus is ignored only at that time only. If the same application invokes again, an Antivirus alert is displayed.
- Add to Trusted Files.** If you click 'Add to Trusted Files', the virus is moved to **Trusted Files** area. The alert is not generated if the same application invokes again.
- Report this to COMODO as a False Alert.** If you are sure that the file is safe, select 'Report this to COMODO as a False Alert'. The Antivirus sends the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.
- Add to Exclusions.** If you click 'Add to Exclusions', the virus is moved to **Exclusions** list. The alert is not generated if the same application invokes again.

### Answering Firewall Alerts

Comodo Internet Security generates a Firewall alert on network connection attempts. The followings steps will help you answer a Firewall alert: :

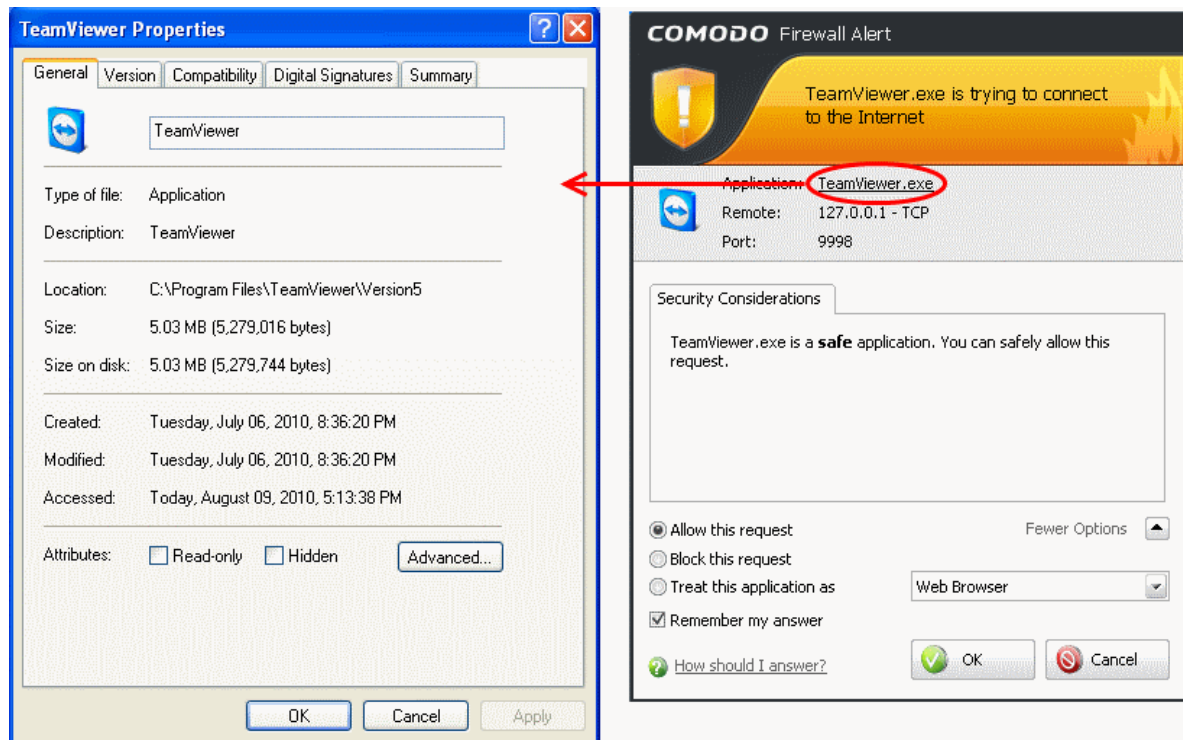
- Carefully read the 'Security Considerations' section. The Firewall can recognize thousands of safe applications. (For example, Internet Explorer and Outlook are safe applications). If the application is known to be safe - it is written directly in the security considerations section along with advice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



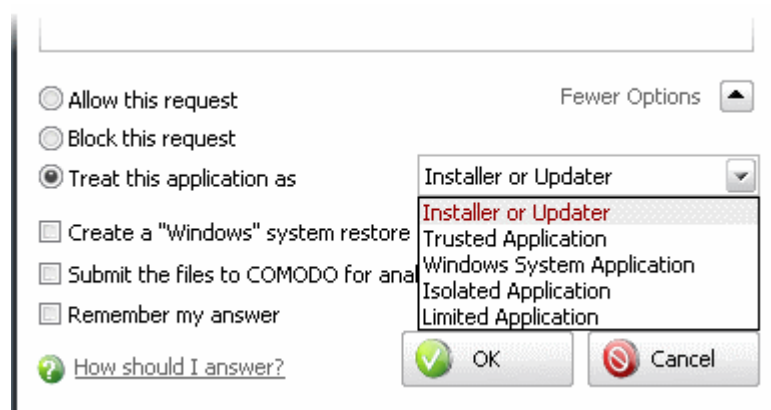
If it is one of your everyday applications that you want to grant Internet access to then you should select **Allow This Request** (it may be the case that the application has not yet been added to the safe application database yet).

If you don't recognize the application then we recommend you select **Block This Request**, but do not select the **Remember My Answer** option.

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



2. If you are sure that it is one of your everyday application, try to use the **Treat This Application As** option as much as possible. This deploys a **predefined firewall policy** 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 policy has been specifically designed by Comodo to optimize the security level of a certain type of application.



If you do not see the **Treat this Application As** option, you should click **More Options**. Remember to check the box **Remember My Answer**.

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 click **Remember My Answer** to make the setting permanent.

## Answering Defense+ Alerts

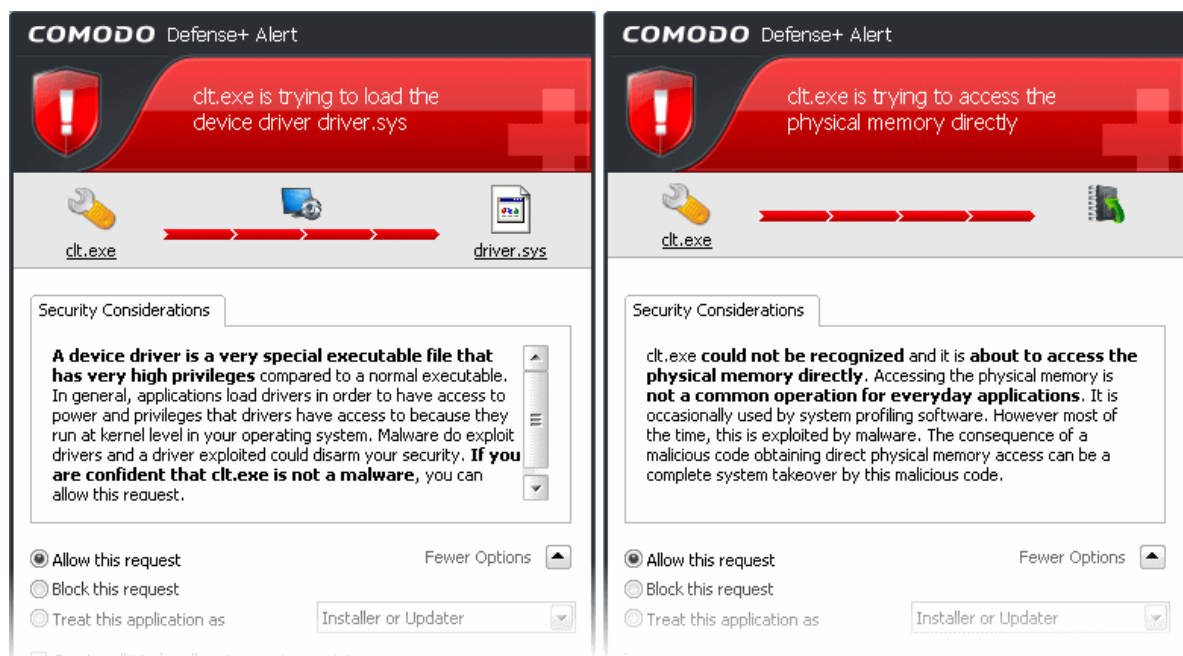
Comodo Internet Security generates a Defense+ Alert based on behavior of applications running in your system. Following are the steps to be followed to answer a Defense+ alert:

1. As with Firewall Alerts, carefully read the 'Security Considerations' section. 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 that you want to grant execution rights to then you should select **Allow This Request**.

If you don't recognize the application then we recommend you select **Block This Request** but do not select **Remember My Answer** check box.

2. Avoid using the **Installer or Updater** policy 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.

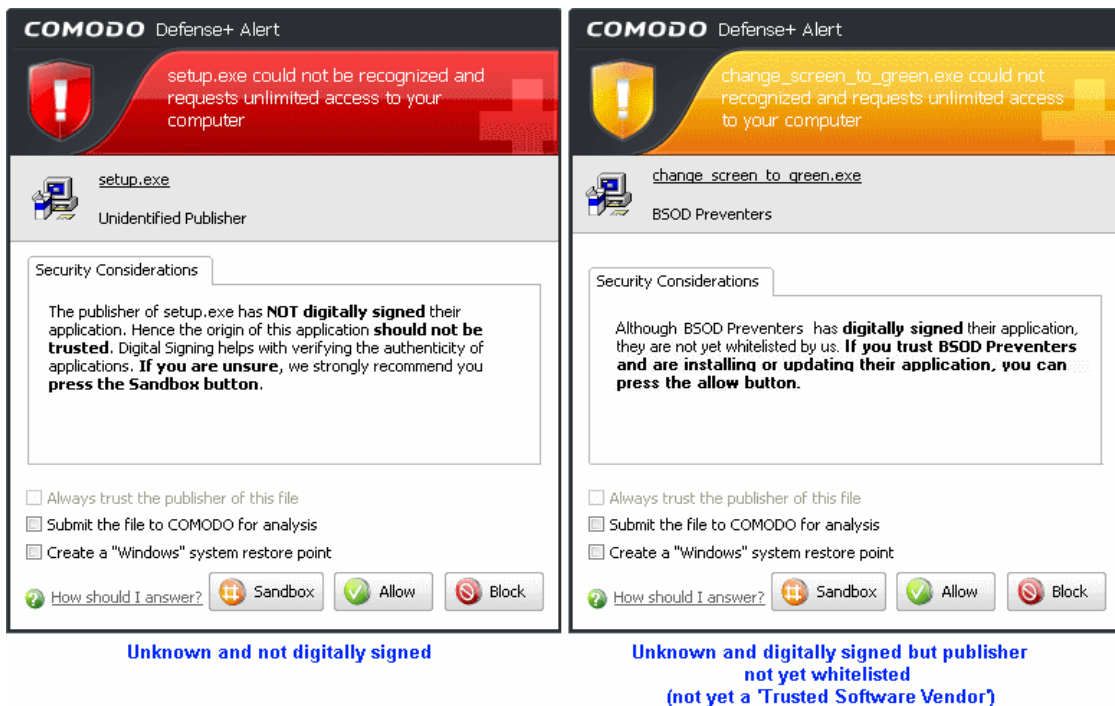


5. **Run with elevated Privileges.** CIS will display this kind of alert when the installer of an unknown application requires administrator, or elevated, privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry.
- If you have good reason to trust the publisher of the software then you can click the 'Allow' 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 in the sandbox** by clicking the 'Sandbox' 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 'Always trust the publisher of this file' then CIS will treat all files from this installer as safe and no future alerts will be generated when you run executables by this publisher.
  - In all cases, please remember to select 'Submit this file to Comodo for analysis' so that our researchers can establish whether the application is safe or not. If it is found to be safe, we shall add it to the global safelist (whitelist). If it is found to be malicious we will add it to our global list of malware signatures (blacklist). Comodo will then distribute the updated lists to all users of CIS.

You will see this type of alert if:

- The sandbox is enabled  
*and*
- 'Automatically detect and run installers outside the sandbox' is enabled. These settings can be modified in **Defense+ Tasks > Defense+ Settings > Sandbox Settings**.

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



- Unknown and unsigned installers should be either sandboxed or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be sandboxed if you would like to evaluate the behavior of the application.
- In both instances, select 'Submit the file to Comodo for analysis' so that we can effectively categorize the file and add it to our global white-list or blacklist.

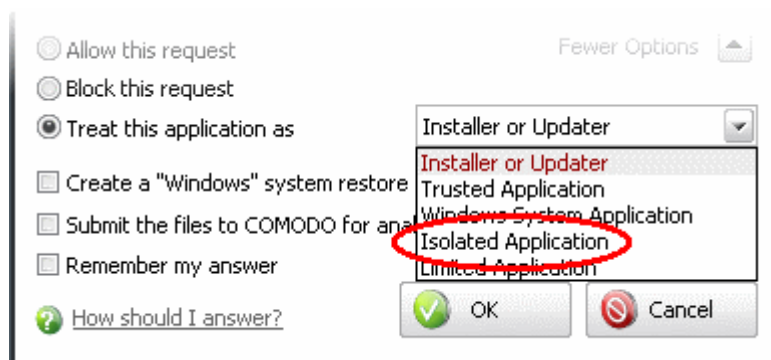
Also see:

- '[Answering a Sandbox Alert](#)' to see how CIS handles unknown applications that are *not* detected as being an installer or updater program.
  - '[Unknown Files: The Sand-boxing 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'.
6. **Protected File Alerts** usually occur when you try to download or copy files or when you update an already installed application.

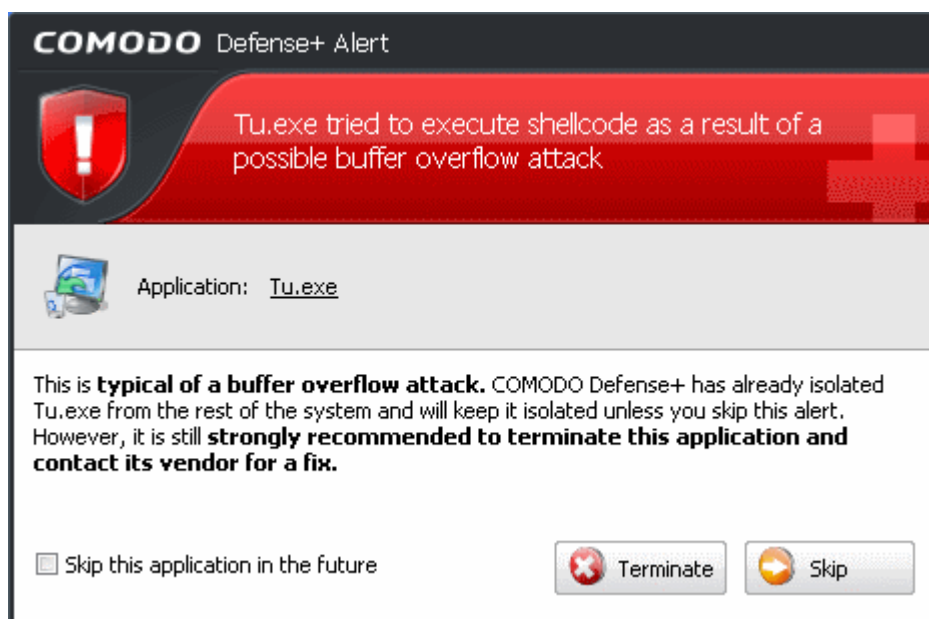
Were you installing new software or trying to download an application from the Internet? If you are downloading a file from the 'net, try to use **Allow without Remembering** option to cut down on the creation of unnecessary rules within the firewall.

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 select **Block This Request** 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 selecting **Treat As Isolated Application** (fourth down in the graphic below).



7. A **Buffer overflow** Alert is generated when an application tries to send more data to its memory buffer than that the buffer can handle. This may be a possible hacking attempt.



If you click **Terminate**, the application is denied access to execute.

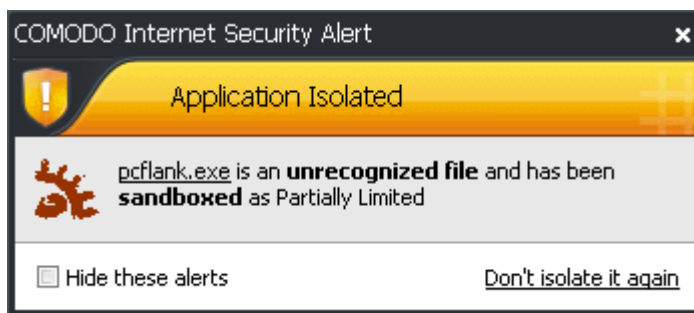
If you click **Skip**, the application is excluded from monitoring for the moment and is allowed access. But on the next attempt of attack the alert is generated again.

If you select 'Skip this application in the future', and click **Skip**, the application is excluded from monitoring permanently and allowed access all the times. Do this only if the application is from a trusted vendor.

8. If a Defense+ 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.
9. 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.
10. If Defense+ 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.
11. Avoid using **Trusted Application** or **Windows System Application** policies for your email clients, web browsers, IM or P2P applications. These applications do not need such powerful access rights.

### Answering a Sandbox Alert

By default, CIS will display an alert whenever it runs an unknown application in the sandbox:



The alert will show the name of the executable that has been isolated in the sandbox. 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 sandboxed application.
- Clicking Don't isolate it again removes the application from the Unrecognized Files list and adds it to the Trusted Files list, enabling the application to run outside the sandbox. 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:

- '**Run with elevated Privileges**' alerts.
- '**Unknown Files: The Sand-boxing and Scanning Processes**' - to understand the decision making process behind why CIS chooses to sandbox certain applications.

## 2 Antivirus Tasks - Introduction

The Antivirus Task Center allows you to quickly and easily configure all aspects of the Antivirus component of Comodo Internet Security (hereafter known simply as 'Comodo Antivirus').

Comodo Antivirus leverages multiple technologies, including Real-time/On-Access Scanning, On Demand Scanning and a fully featured Scan Scheduler 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 which can be re-used across all scan types and features full event logging, quarantine and file submission facilities.

Comodo Antivirus detects and removes threats that are present on your machine and forms an additional layer of security on top of the threat prevention offered by the Firewall and Defense+ components. The heuristics scanning capability of the application identifies previously unknown viruses and Trojans.

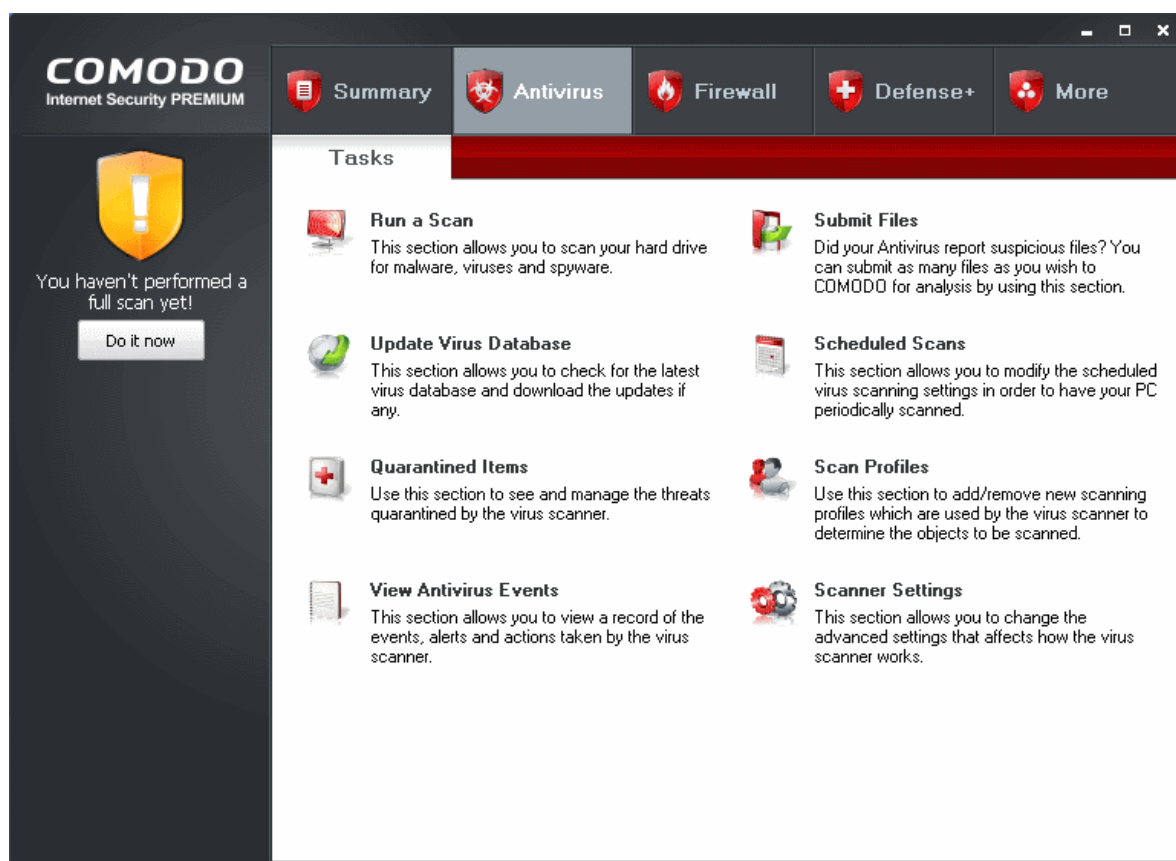
In order to maintain maximum security levels, Comodo advises you to run regular Antivirus scans.

On-Demand scanning is also seamlessly integrated into the Windows operating system. Users can scan specific objects 'on the fly' by simply right-clicking on a file, folder or drive and selecting **Scan with Comodo AntiVirus** from the **context sensitive menu**.



The Antivirus tasks center can be accessed at all times by clicking on the Antivirus tab from the navigation panel.





The Antivirus main configuration area provides easy access to all the features. Click the links below to see detailed explanations of each area in this section.

- [Run a Scan](#)
- [Update Virus Database](#)
- [Quarantined Items](#)
- [View Antivirus Events](#)
- [Submit Files](#)
- [Scheduled Scans](#)
- [Scan Profiles](#)
- [Scanner Settings](#)

## 2.1 Run a Scan

When you want to check a disk or folder for possible infection from viruses and malware, you can launch an **On-Demand Scan** using the **Run a Scan** option. This executes an instant virus scan on the selected item. You can also check a wide range of removable storage devices such as CD's, DVD's, external hard-drives, USB connected drives, digital cameras - even your iPod!!

You have two options available when you choose to run an On-Demand Scan:

1. Scan a **preselected area**; or
2. Define a custom scan of the areas you choose, by **creating a Scan Profile**.
  - Apart from running an On-Demand scan from Run a Scan interface, you can also scan specific objects using **Context Sensitive Scan**.

### Scanning Preselected Areas

Comodo Antivirus has three pre-defined scan profiles to run On-Demand Scan on preselected areas on your system. Comodo Antivirus contains three default Scan Profiles - 'My Computer', 'Critical Areas' and Spyware Scan. These

predefined profiles cannot be edited or removed. They are:

- i. **My Computer (Default)** - When this Profile is selected, Comodo Antivirus scans every local drive, folder and file on your system.
- ii. **Critical Areas** - When this profile is selected, Comodo Antivirus scans the Program Files Folder and WINDOWS Folder of the Operating System of your computer.
- iii. **Spyware Scan** - Spyware is a type of malware that gathers data from your system and transmits it to a 3rd party without your knowledge. Spyware is almost always hidden away on your system so it can carry out such tasks without you noticing (and often, without affecting the performance of your computer in any significant way). The most dangerous type of spyware will use a variety of techniques to steal vital information from your computer such as passwords, credit card numbers and other confidential information. An example would be a 'keylogger', which records every stroke you make on the keyboard and sends this information to an hacker or other unknown third party.

The Spyware Scan feature in Comodo Antivirus scans your Windows registry and system files to check whether your computer is infected with such malware and alerts you. This scanning feature improves the detection and successful cleaning rate of already infected systems.

## Custom Scan

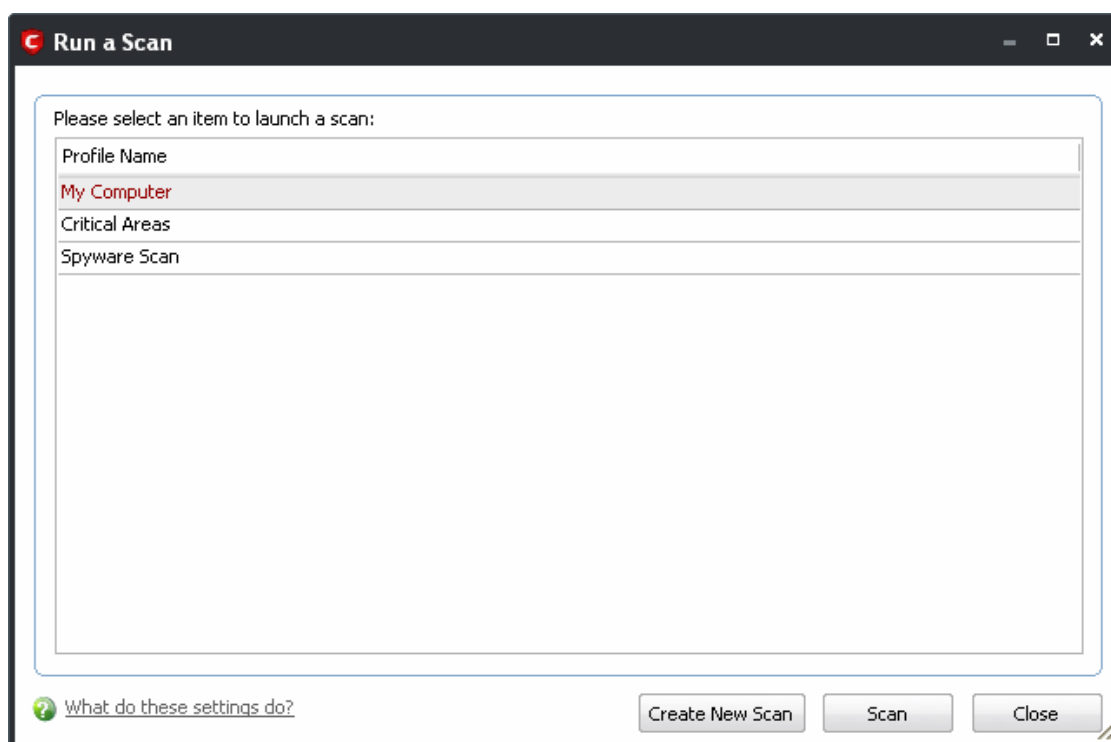
You can run the virus scan on selected disks or folders by setting the scan profiles beforehand. For more details on Scan profiles, refer to [Antivirus Tasks > Scan Profiles](#). You can also [Create a Scan Profile](#) from the **Run a Scan** option.

Comodo Antivirus also scans the archive files such as .ZIP, .RAR, and so on, on running an on-demand scanning.

## To start an On-Demand scanning

1. Click 'Run a Scan' in the main Antivirus Task Manager Screen.

The 'Run a Scan' panel appears.



From the 'Run a Scan' panel you can

- [Run a scan one of the items listed in the panel](#)
- [Add a new item to scan by creating a new scan profile](#)
- [Save the Scan results as text file](#)

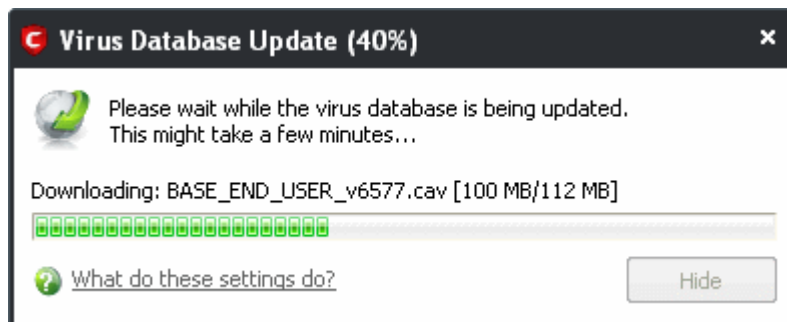


- Move any threats identified by the scan into quarantine
- Disinfect the selected file/application if an exclusive disinfection routine is available
- Delete any infected files, folders or applications
- Exclude an application you consider as safe from the threat list

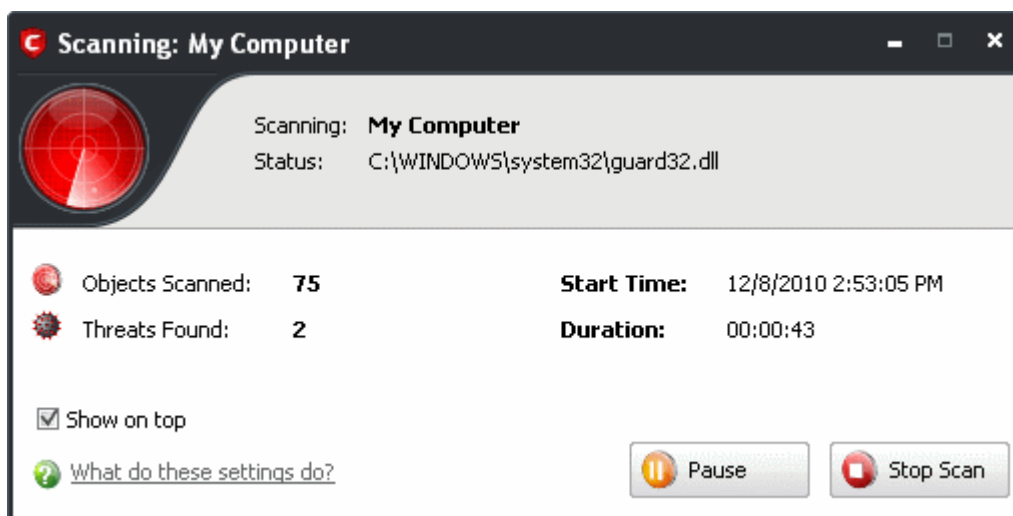
## To scan your system for viruses and malware

1. Click 'Run a Scan' in the Antivirus screen.
2. Select a Scan Profile name and click 'Scan'.

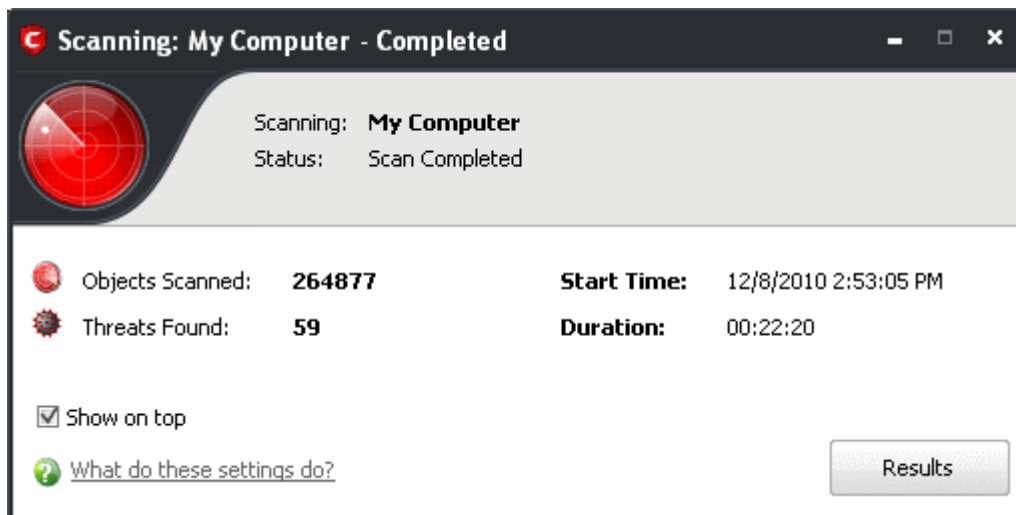
Comodo Antivirus checks for AV database updates and if available, updates the virus database in your system.



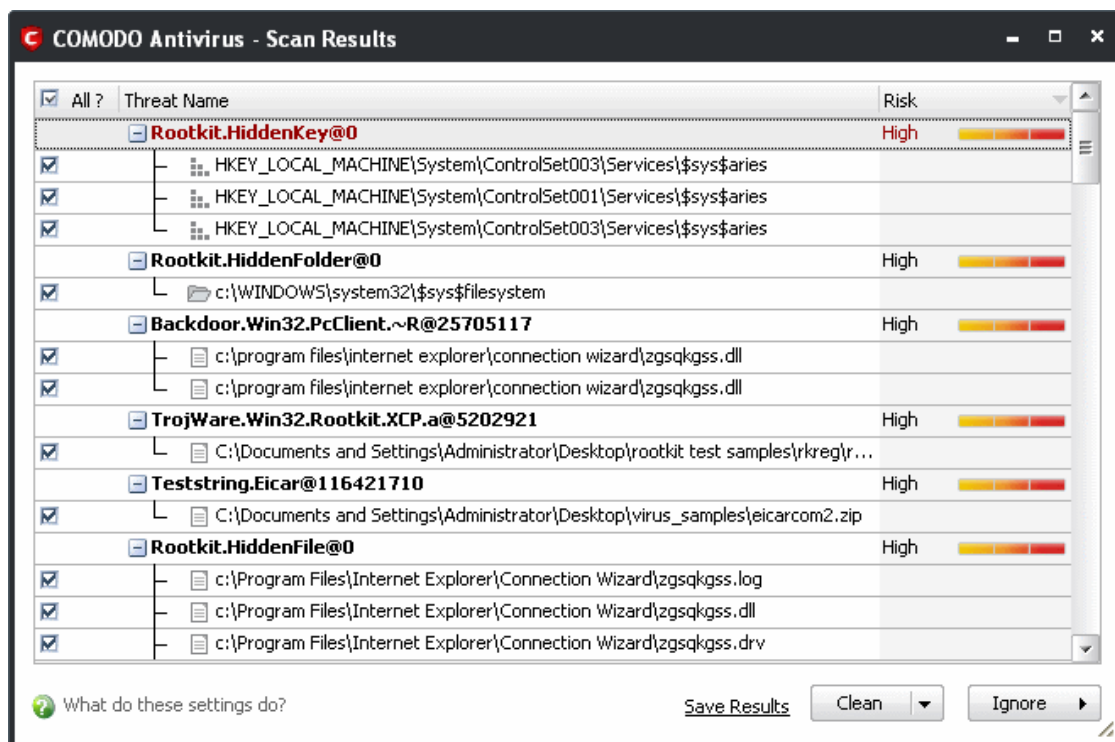
Then Comodo Antivirus starts to scan the items, based on the scan profile you have selected.



On completion of scanning, the 'scanning completed' window is displayed.



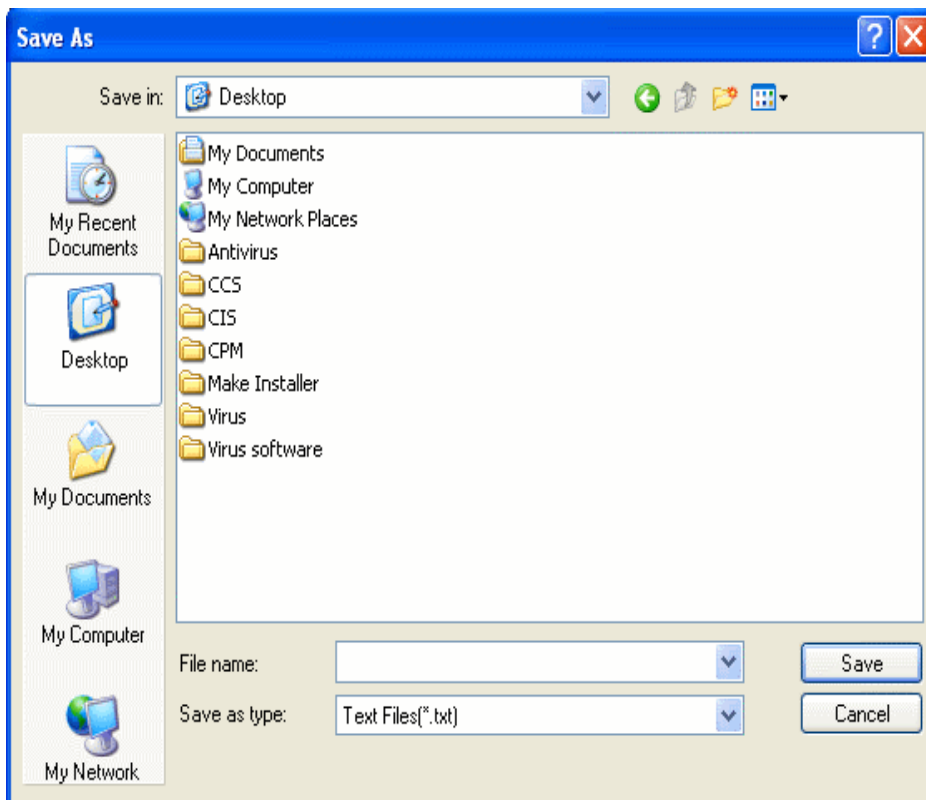
- Click 'Results' to view the Scan Results window. If malicious executables are discovered on your system, the scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on).



**Tip:** You can sort the scan results by alphabetical order by clicking the 'Threat Name' column header. Similarly you can sort the scan results based on the risk level by clicking the 'Risk' column header. To select all the entries for actions such as moving them to quarantine or disinfect, select the check box beside the 'Threat name'.

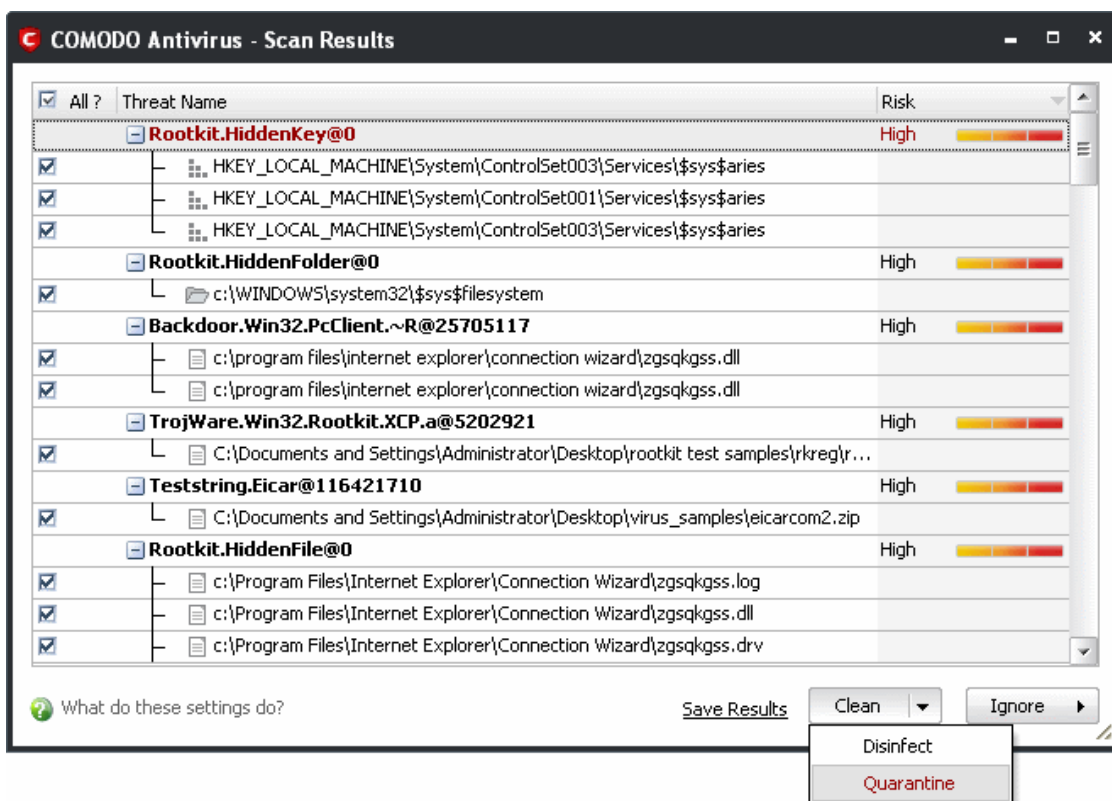
## To save the Scan Results as a Text File

- Click 'Save' and enter the location in the 'Save As' dialog box.

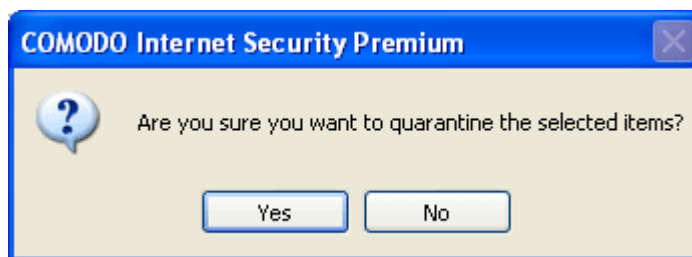


## To move selected executables detected with threats to Quarantined Items

1. Select the application from the results, click the drop-down button beside 'Clean' and select 'Quarantine'.



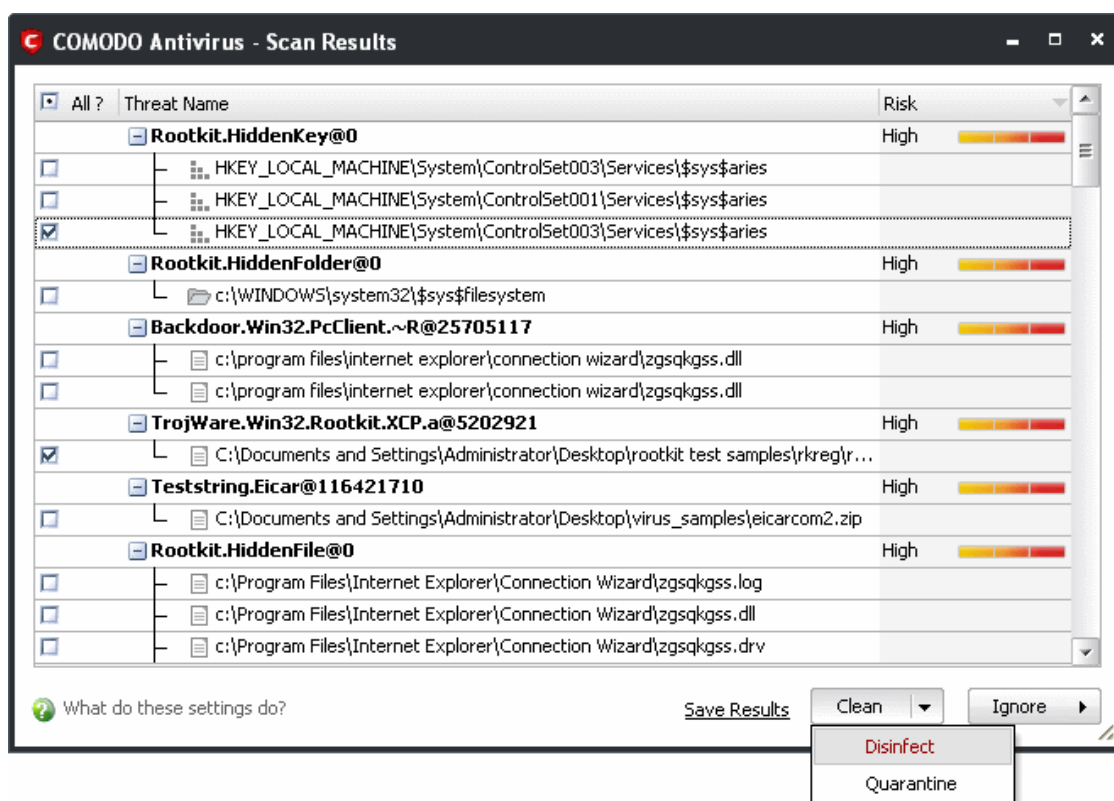
2. Click 'Yes' in the confirmation dialog box.



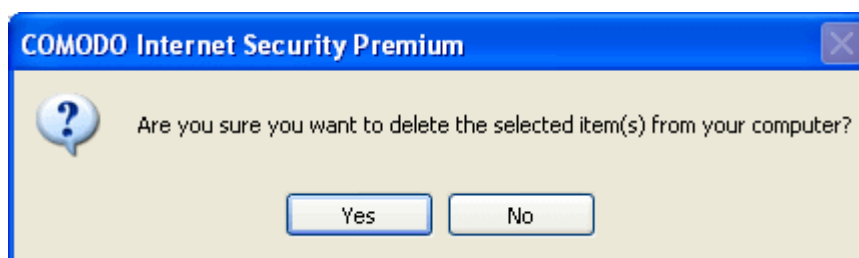
The selected application is moved to the Quarantined items. For more details on quarantined applications, refer to [Antivirus Tasks > Quarantined Items](#).

## To disinfect the file / application detected with a threat

1. Select the application from the results, click the drop-down button beside the 'Clean' button and select 'Disinfect'.



2. Click 'Yes' in the confirmation dialog box.

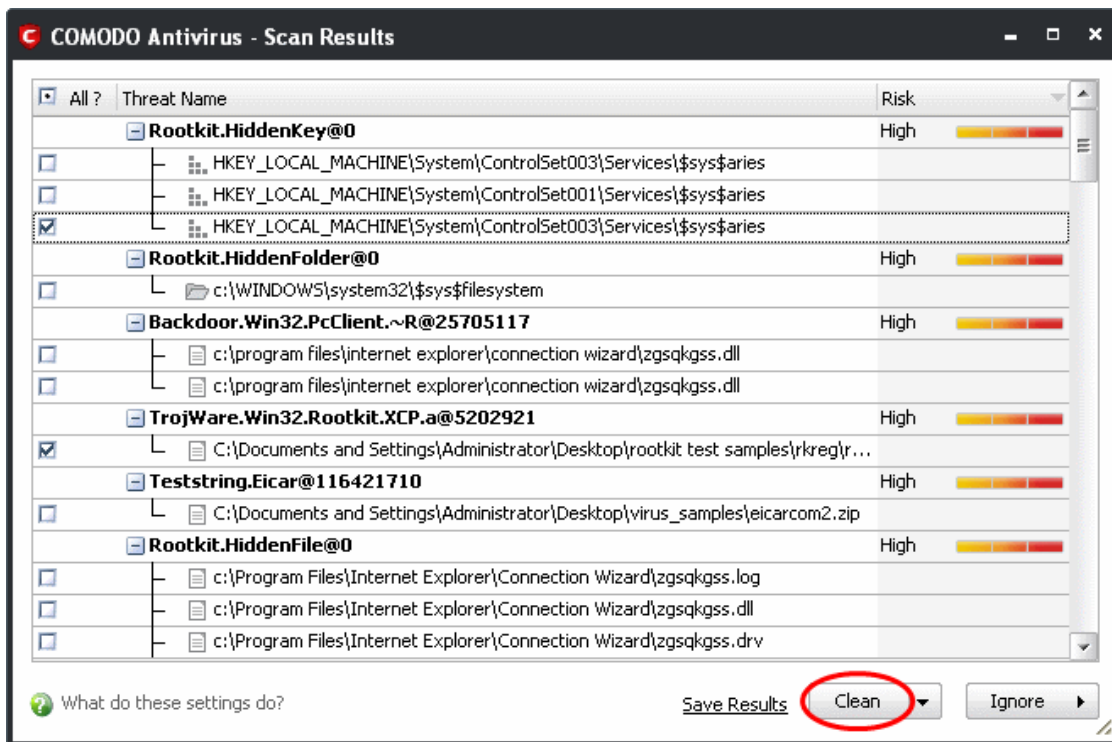


The antivirus disinfects the file if there exists a disinfection routine defined for the file and the file is recovered to its pre-

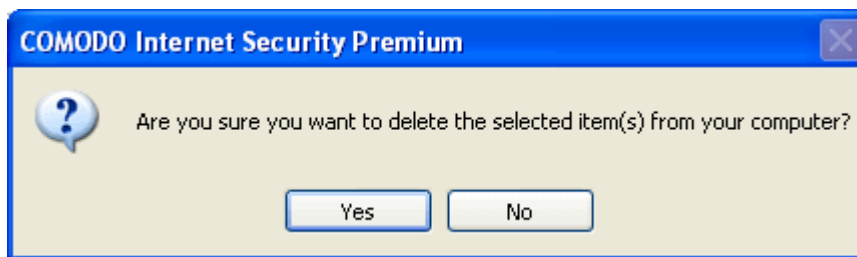
viral state. If no any disinfection routine is available, the file is deleted permanently from your system.

## To delete an application detected with a threat

1. Select the application from the results, click the 'Clean' button.

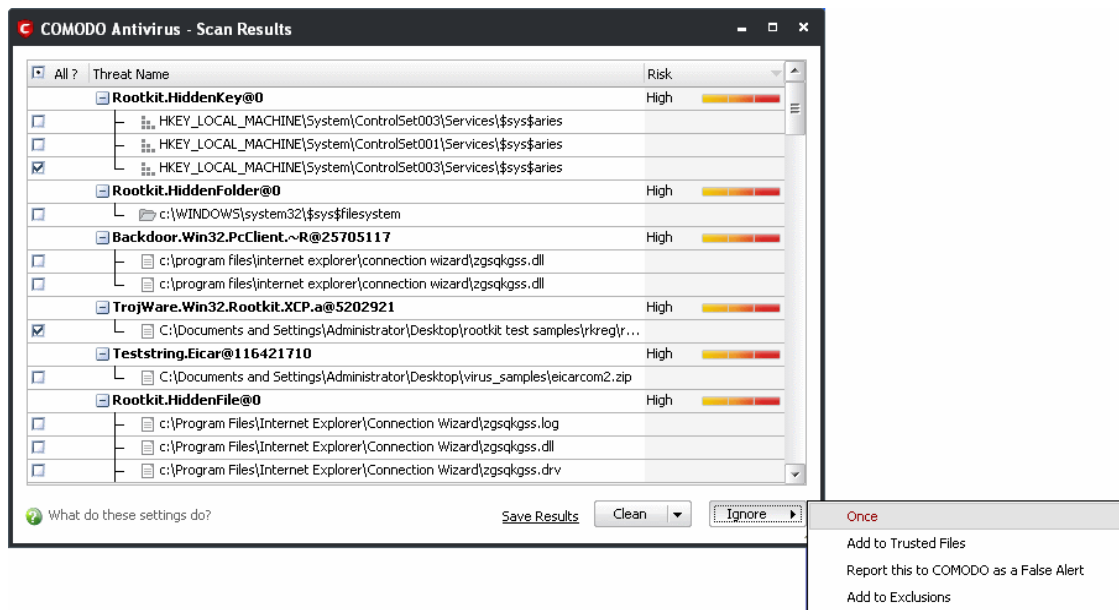


2. Click 'Yes' in the confirmation dialog box.



## To ignore an application / file you consider as safe from the threat list

- Click the 'Ignore' button



Selecting Ignore provides you with four options.

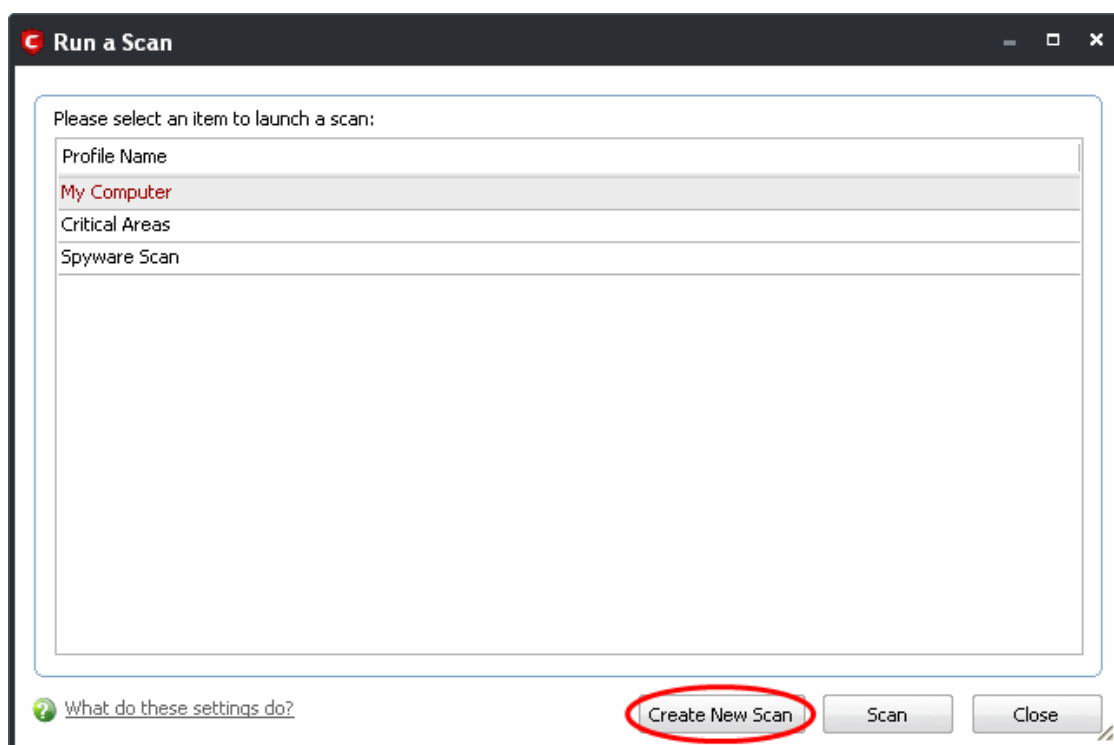
- **Once** - If you click 'Once', the virus is ignored only at that time only. If the same application invokes again, an Antivirus alert is displayed.
- **Add to Trusted Files** - If you click 'Add to Trusted Files', the virus is moved to **Trusted Files** area. The alert is not generated if the same application invokes again.
- **Report this to COMODO as a False Alert** - If you are sure that the file is safe, select 'Report this to COMODO as a False Alert'. The Antivirus sends the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safelist.
- **Add to Exclusions** - If you click 'Add to Exclusions', the virus is moved to **Exclusions** list. The alert is not generated if the same application invokes again.

## Creating a Scan profile

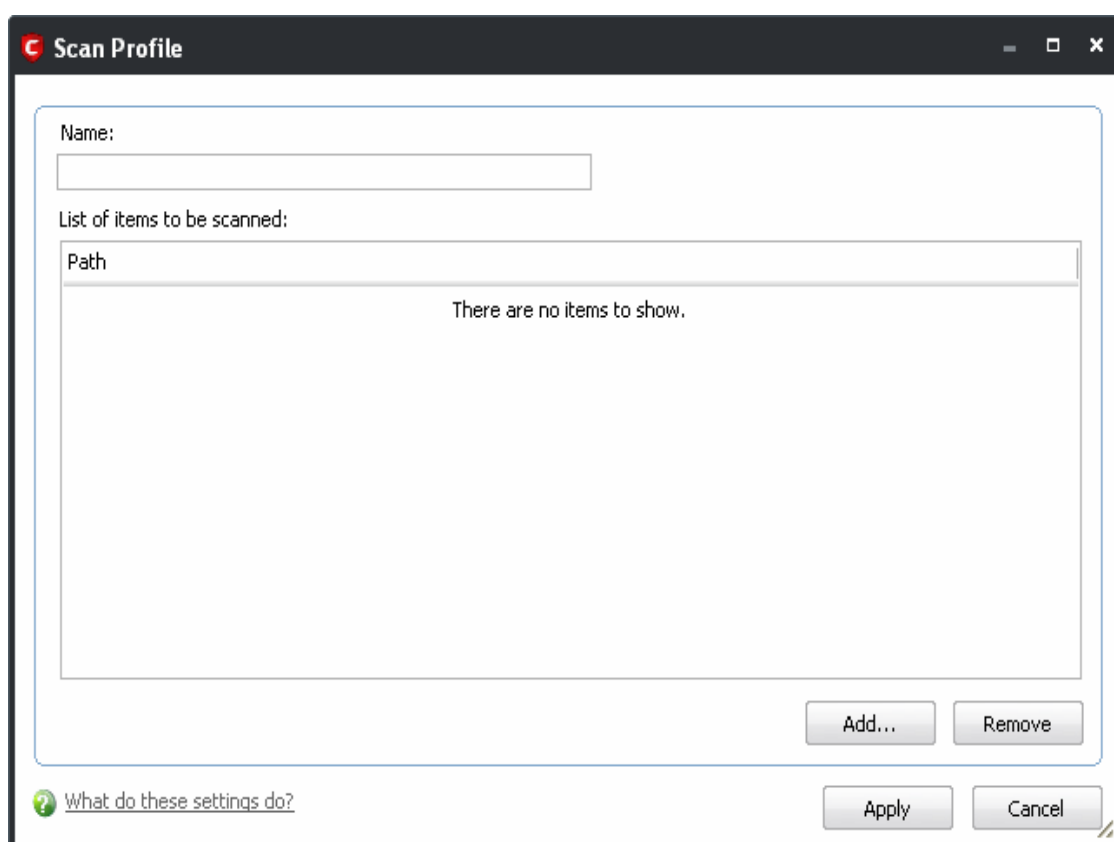
Scan Profiles are the user-defined profiles containing specific areas on your system that you wish to scan and can be re-used for all future scans.

### To create a new scan profile

1. Click 'Create New Scan' in the 'Run a Scan' interface.

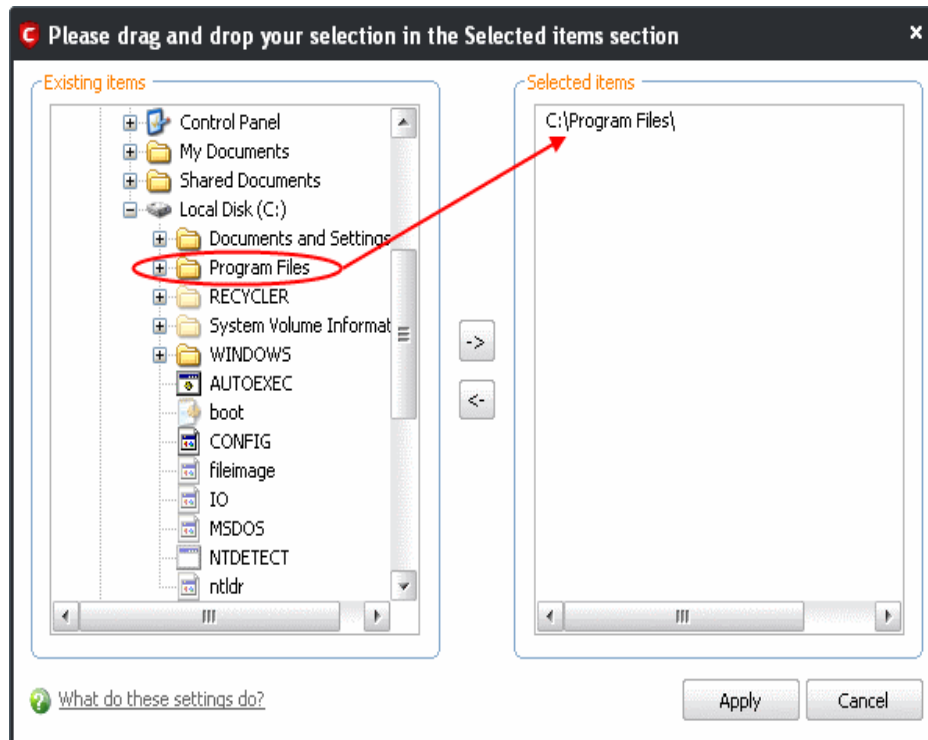


A 'Scan Profile' configuration appears.



2. Type a name for the scan profile to be created in the 'Name' box.
3. Click 'Add'.

A configuration screen appears, prompting you to select the locations to be scanned when the newly created scan profile is selected.



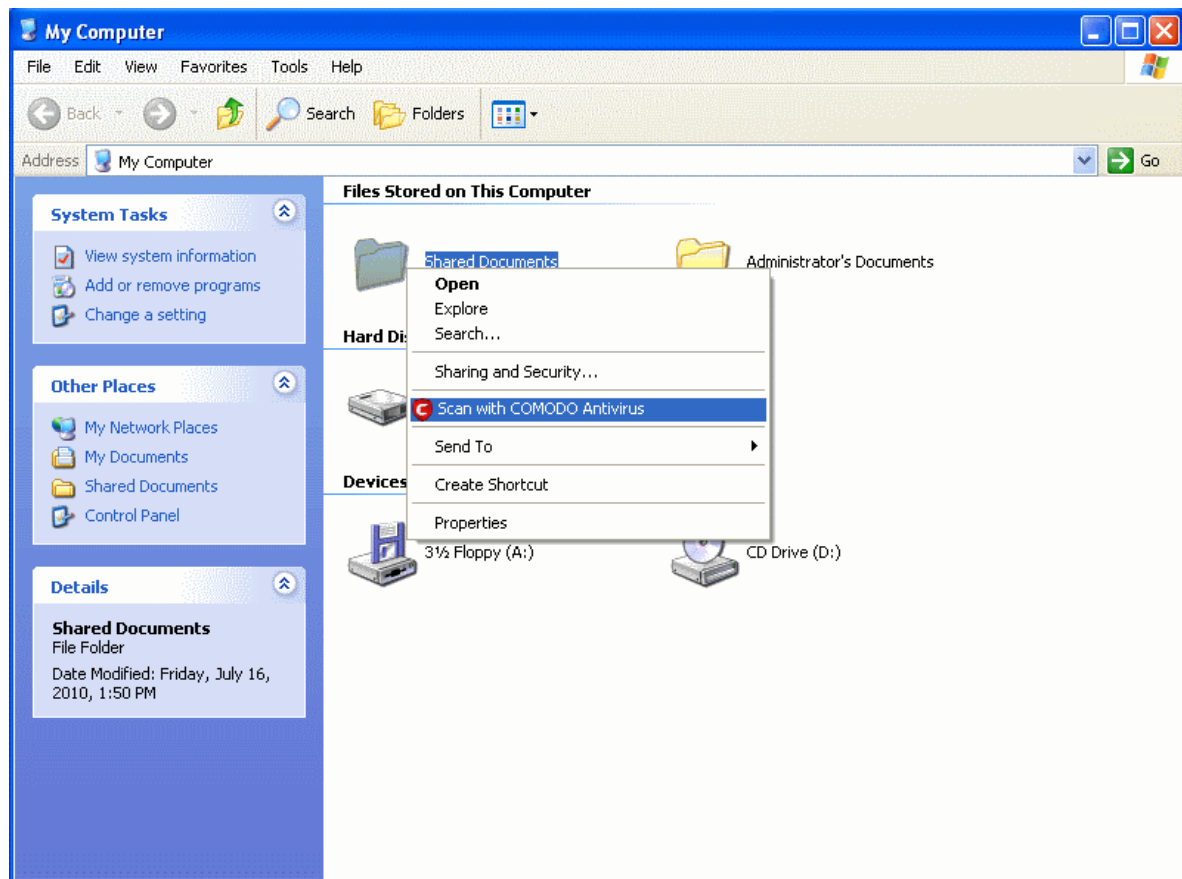
4. Select the locations from the left column, drag and drop to the right column or select the locations and click right arrow to move selected folders to right column.
5. Click 'Apply'.
6. Repeat the process to create more Scan Profiles.

**Note:** You can also create new Scan Profiles by accessing **Scan Profiles** in the Antivirus Screen.

### Context Sensitive Scan

You can right click any item i.e. a drive, folder or a file in Windows Explorer and select 'Scan with COMODO Antivirus' from the context sensitive menu to perform a virus scan selectively on the item. This is useful when you suspect a particular item might contain virus due to newly downloaded or copied folder/file.





## 2.2 Update Virus Database

In order to guarantee the relevance of your antivirus software, it is imperative that your virus databases are updated as regularly as possible.

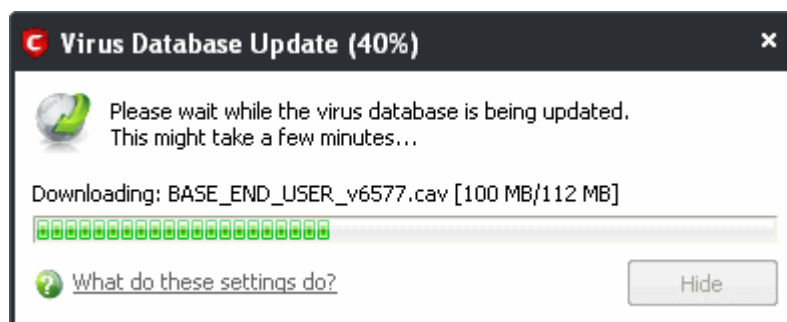
Our anti-virus database is maintained and updated around the clock by a team of dedicated technicians, providing you with the solutions to the latest virus outbreaks. Updates can be downloaded to your system **manually** or **automatically** from Comodo's update servers.

### To manually check for the latest virus Database and then download the updates

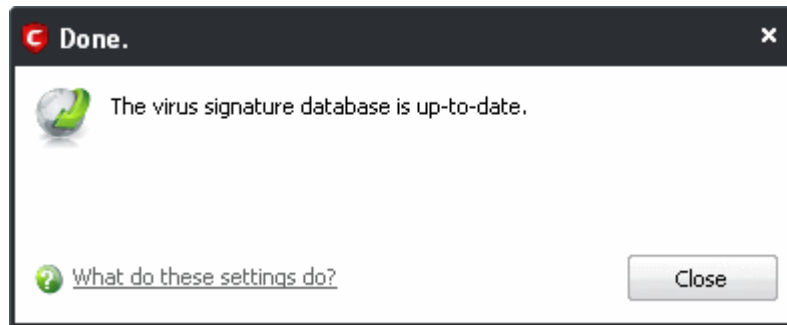
1. Click on the 'Update Virus Database' from the main Antivirus Task Manager Screen.

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

A dialog box appears, showing you the progress of update process.



On completion, your virus database is made up to date.



When infected or possibly infected files are found, if the anti-virus database has been not updated for a critically long time, or your computer has not been scanned for a long time, the main window of Comodo Antivirus recommends a course of action and gives a supporting explanation. We have customized our application to achieve optimal performance based on the extensive expertise of Comodo in the anti-virus protection business.

### Automatic Updates

Comodo AntiVirus checks for latest virus database updates from Comodo website and downloads the updates automatically. You can configure Comodo Antivirus to download updates automatically in the Scanner Settings for Real Time Scanning (On-Access Scanning) and Scheduled Scanning. Refer to [Real Time Scanning Settings](#) and [Scheduled Scanning Settings](#).

## 2.3 Quarantined Items

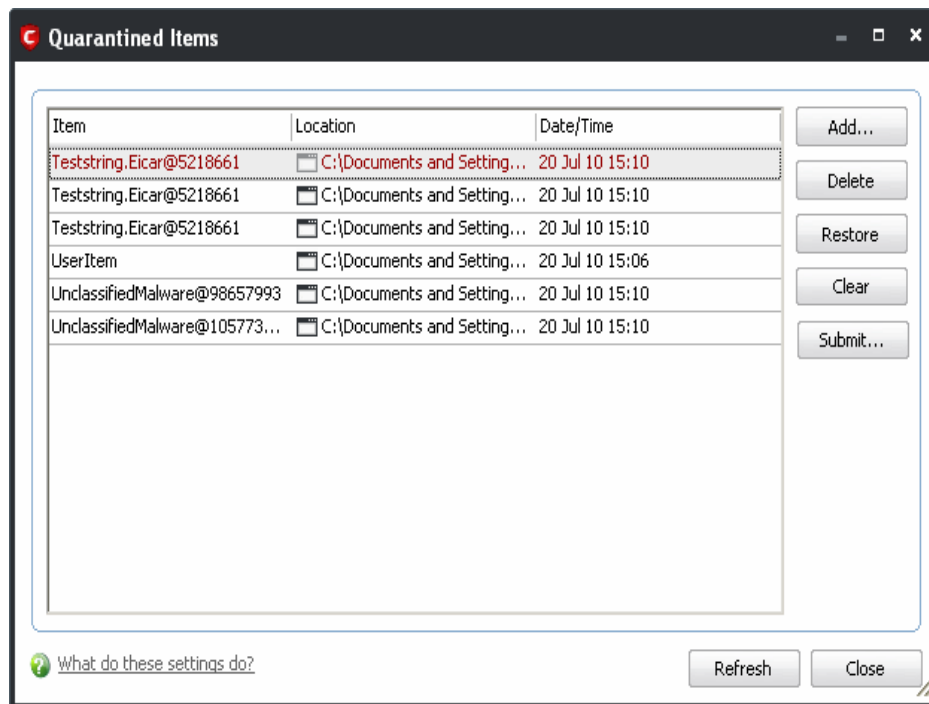
The quarantine facility removes and isolates suspicious files into a safe location before analyzing them for possible infection. Any files transferred in this fashion are encrypted- meaning they cannot be run or executed. This isolation prevents infected files from affecting the rest of your PC. If a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

For adding executables to Quarantined items, refer to [Antivirus Tasks > Run a Scan](#). You can also:

- [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](#)
- [Delete all quarantined items](#)
- [Submit selected quarantined items to Comodo for analysis](#)

### To view the list of Quarantined Items

- Click 'Quarantined Items' from the main Antivirus Task Manager Screen.



### 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.

### 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

- Click **Add** and select the file from **Open** dialog box.

#### To delete a quarantined item from the system

- Select the item and Click 'Delete'.

This deletes the file from the system permanently.

#### To restore a quarantined item to its original location

- Select the item and click 'Restore'.

If the restored item does not contain a malware, it operates as usual. But if it contains a malware, it is 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 'Clear'.

This deletes all the quarantined items from the system permanently.

#### To submit selected quarantined items to Comodo for analysis

- Select the item from the list and click 'Submit'.

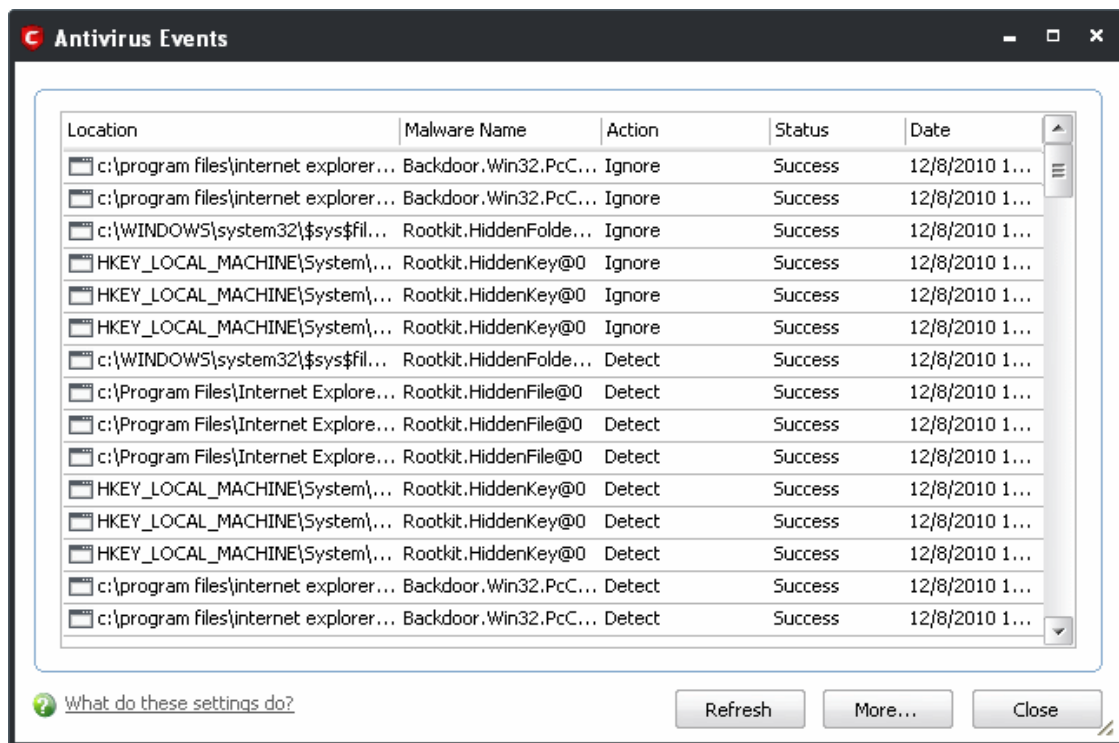
**Note:** Quarantined files are stored using a special format and do not constitute any danger to your computer.

## 2.4 View Antivirus Events

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 anti-virus database and application modules.

### To view a log of Antivirus Events

- Click 'View Antivirus Events' from the main Antivirus Task Manager Screen.



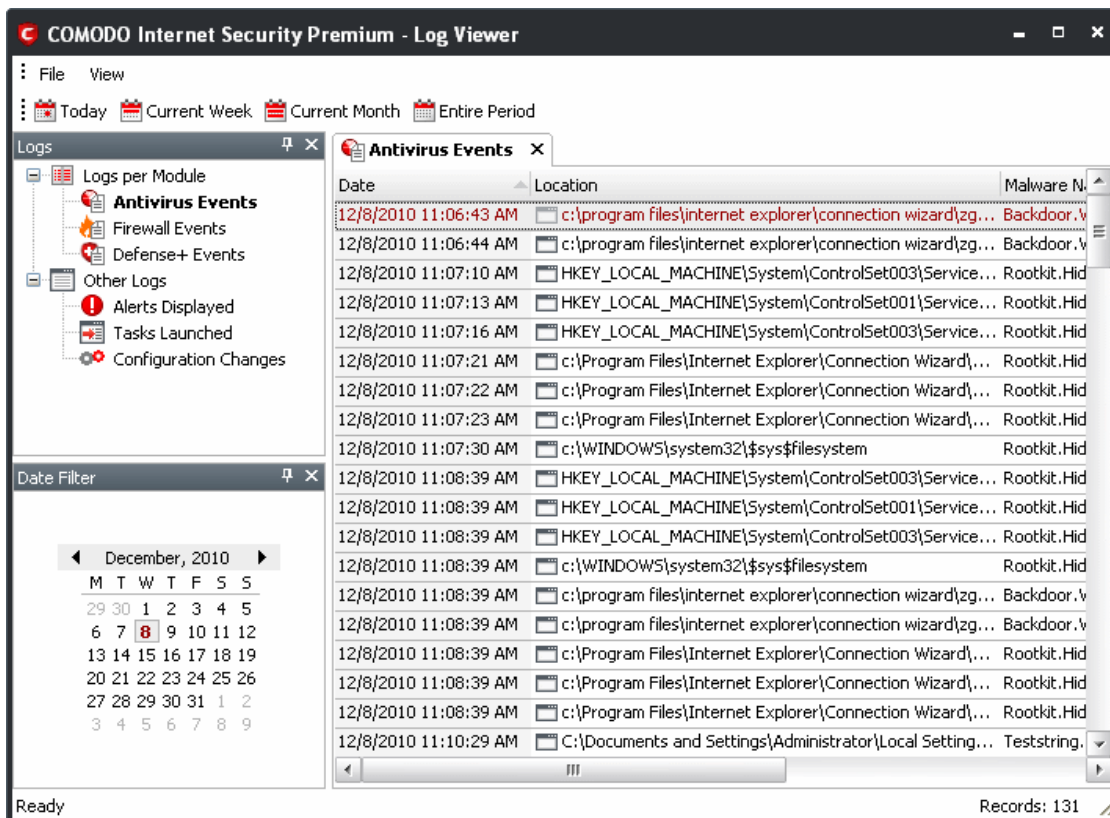
### Column Descriptions

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

Click 'More' to load the full, Comodo Internet Security Log Viewer module.

This window contains a full history of logged events in two categories: Logs per Module and Other Logs.

It also allows you to build custom log files based on **specific filters** and to **export log files** for archiving or troubleshooting purposes.



The Log Viewer Module is divided into three sections. The top panel displays a set of handy, predefined time Filters. The left panel the types of Logs. The right hand side panel displays the actual events that were logged for the time period you selected in the top panel and the type of log selected in the left panel (or the events that correspond to the filtering criteria you selected).

The Logs per Module option contains the logged events of Firewall, Defense+ and Antivirus modules and Other Logs options contains logged events of the following:

- **Alerts Displayed:** Displays the list of various alerts that were displayed to the user, the response given by the user to those alerts and other related details of the alert.
- **Tasks Launched:** Displays the various Antivirus tasks such as updates and scans that have taken place. This area will contain a log of all on demand and scheduled AV scans and the result of that scan.
- **Configuration Changes:** Displays a log of all configuration changes made by the user in the CIS application.

## Filtering Log Files

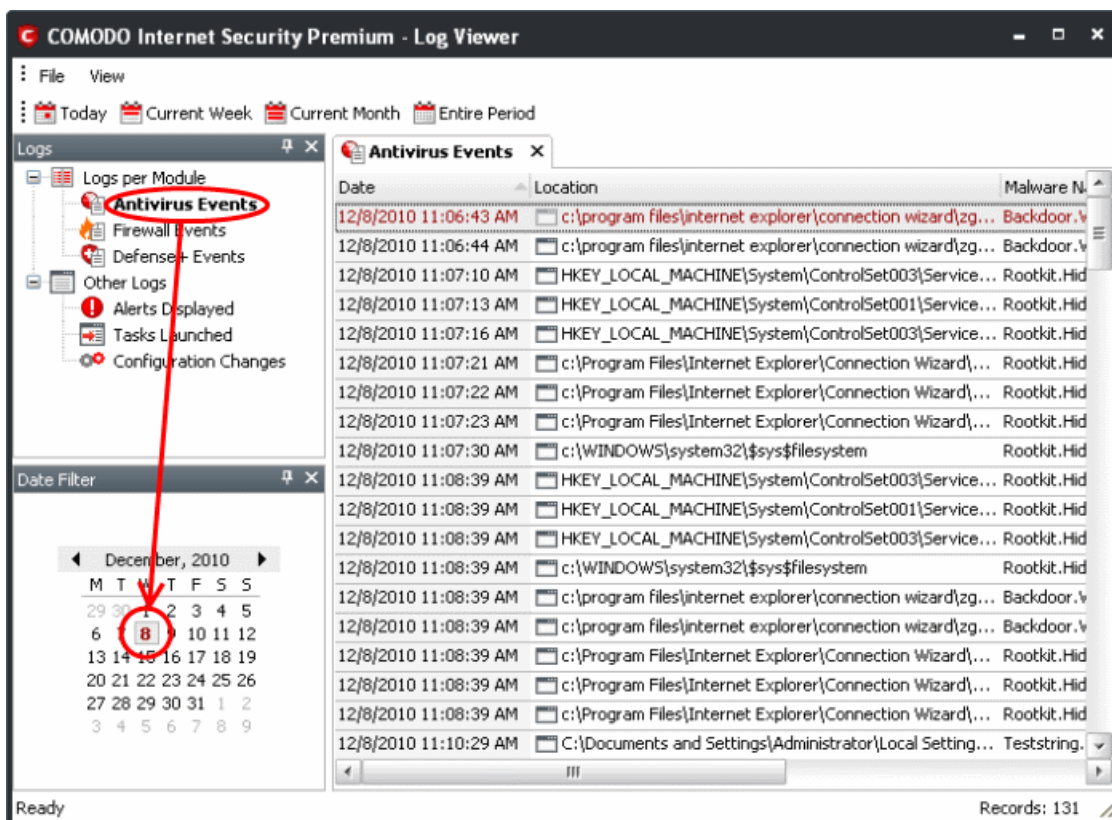
Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria.

### Preset Time Filters:

Clicking on any of the preset filters in the top panel alters the display in the right hand panel in the following ways:

- **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).

The example below shows an example display when the Antivirus Events for 'Today' are displayed.



**Note:** The type of events logged by the Antivirus, Firewall and Defense+ modules of Comodo Internet Security differ from each other. This means that the information and the columns displayed in the right hand side panel change depending on which type of log you have selected in the top and left hand side panel. For more details on the data shown in the columns, see [View Firewall Events](#) or [View Defense+ Events](#).

### User Defined Filters:

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. The type of filters available for Firewall logs differ to those available for Defense+ logs. The table below provides a summary of available filters and their meanings:

Available Filters - Logs per Module		
Antivirus Filter	Firewall Filters	Defense+ Filters
<b>Action</b> - Displays events according to the response (or action taken) by the Antivirus	<b>Action</b> - Displays events according to the response (or action taken) by the firewall	<b>Application</b> - Displays only the events propagated by a specific application
<b>Location</b> - Displays only the events logged from a specific location	<b>Application</b> - Displays only the events propagated by a specific application	<b>Flags</b> - Displays events according to the response (or action taken) by Defense+
<b>Malware Name</b> - Displays only the events logged corresponding to a specific malware	<b>Destination IP</b> - Displays only the events with a specific target IP address	<b>Target</b> - Displays only the events that involved a specified target application
<b>Status</b> - Displays the events according to the status after the	<b>Destination Port</b> - Displays only the	

Available Filters - Logs per Module		
action taken. It can be either 'Success' or 'Fail'	events with a specific target port number	
	<b>Direction</b> - Indicates if the event was an Inbound or Outbound connection	
	<b>Protocol</b> - Displays only the events that involved a specific protocol	
	<b>Source IP address</b> - Displays only the events that originated from a specific IP address	
	<b>Source Port</b> - Displays only the events that originated from a specific port number	

### Creating Custom Filters

Custom Filters can be created through the Advanced Filter Interface. You can open the Advanced Filter interface either by using the View option in the menu bar or using the context sensitive menu.

- Click View > Advanced Filter to open the 'Advanced Filter' configuration area.

Or

- Right click on any event and select 'Advanced Filter' option to open the corresponding configuration area.

The 'Advanced Filter' configuration area is displayed in the top half of the interface whilst the lower half displays the Events, Alerts, Tasks or Configuration Changes that the user has selected from the upper left pane. If you wish to view and filter event logs for other modules then simply click log name in the tree on the upper left hand pane.

The Advanced Log filter displays different fields and options depending on the log type chosen from the left hand pane (Antivirus, Defense+, Firewall).

This section will deal with Advanced Event Filters related to 'Antivirus Events' and will also cover the custom filtering that can be applied to the 'Other Logs' (namely 'Alerts Displayed', 'Tasks' Launched' and 'Configuration Changes'). The Firewall and Defense+ Advanced Event Filters are dealt with in their respective sections.

### Antivirus Events - Advanced Filters

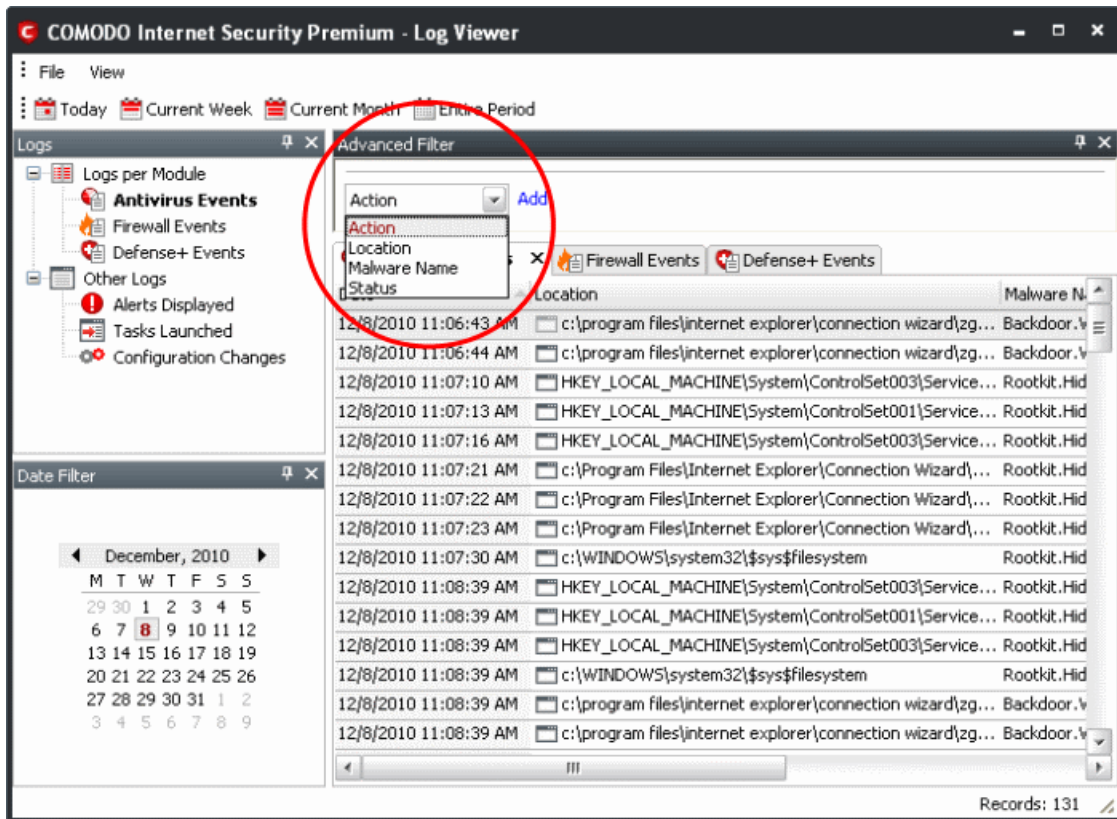
#### To configure Advanced Filters for Antivirus events

1. Select 'View > Advanced Filter'
2. Select 'Antivirus Events' under 'Logs Per Module'

You have 4 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.

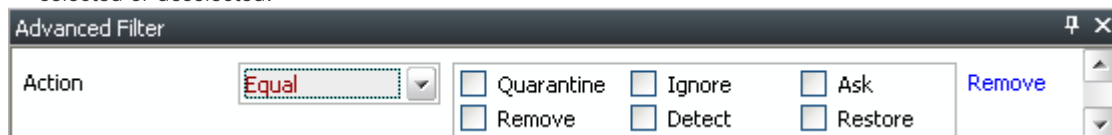
3. Click the 'Add' button when you have chosen the category upon which you wish to filter.





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

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

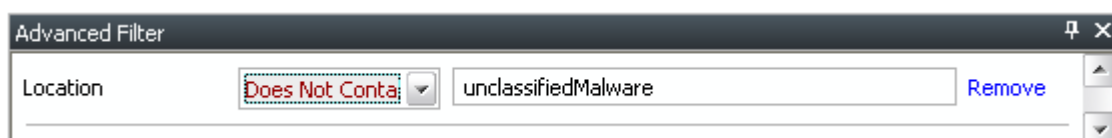


- a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
  - Quarantine: Displays events where the user chose to quarantine a file
 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

The filtered entries are shown directly underneath.

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

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



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

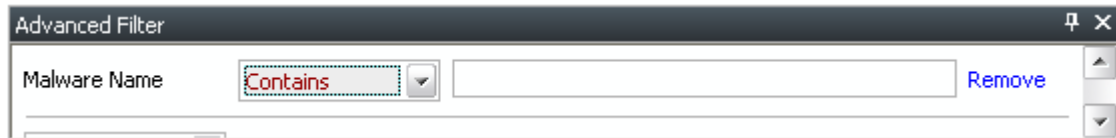


- b) Enter the text or word that needs to be filtered.

The filtered entries are shown directly underneath.

For example, if you select 'Contains' option from the dropdown field and enter the word 'unclassifiedMalware' in the text field, then all events containing the word 'unclassifiedMalware' in the Location field will be displayed directly underneath. If you select 'Does Not Contain' option from the drop-down field and enter the word 'System' in the text field, then all events that do not have the word 'System' will be displayed directly underneath.

- iii. **Malware Name:** Selecting the 'Malware' option displays a dropdown 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.

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Location' option for better understanding.

- iv. **Status:** 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 dropdown 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 database was successfully updated)
- Failure: Displays Events that failed to execute (for example, the database failure to update correctly)

The filtered entries are shown directly underneath.

Refer to the **example** given for 'Action' option for better understanding.

**Note:** More than one filters can be added in the 'Advanced Filter' pane. After adding one filter type, the option to select the next filter type automatically appears. You can also remove a filter type by clicking the 'Remove' option at the end of every filter option.

## Other Logs - Advanced Filters

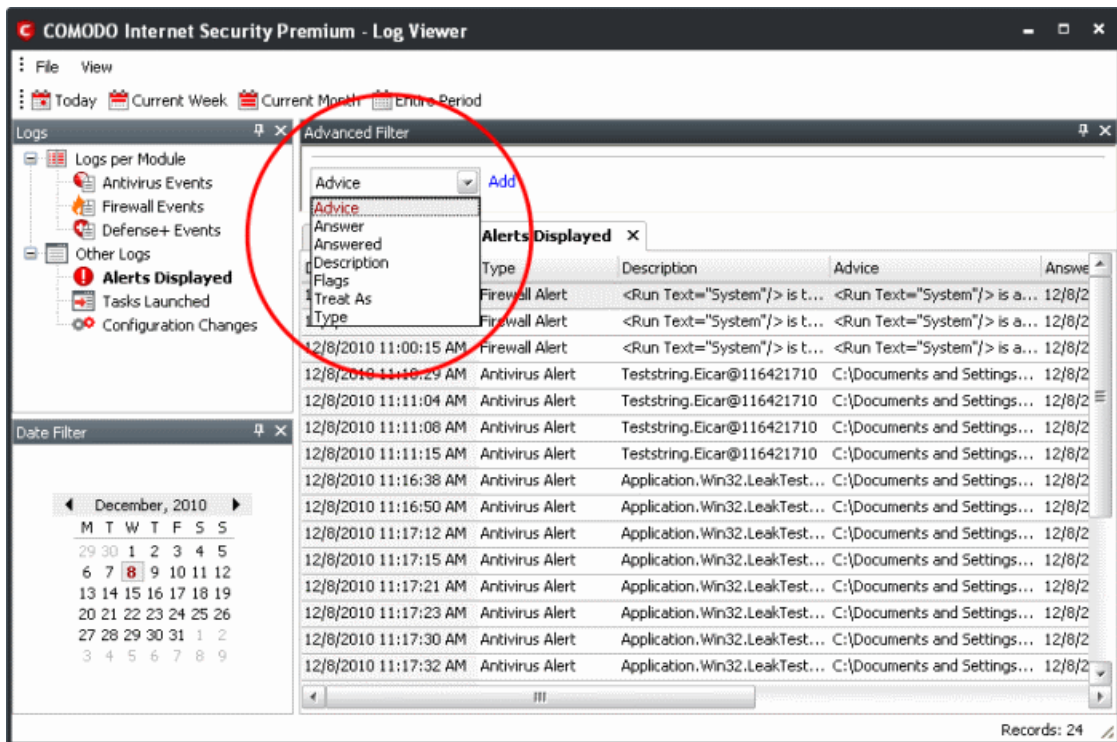
The Advanced Filter function for Alerts Displayed, Tasks Launched and Configuration Changes are the same in Antivirus interface, Firewall interface and Defense+ Interface.

### To configure Advanced Filters for Alerts Displayed

1. Select 'View > Advanced Filter'.
2. Under 'Other Logs', select 'Alerts Displayed'.

This will open the Advanced Filter pane to the upper right. From here, 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.

- Click 'Add' when you have chosen the category upon which you wish to filter.



The following table lists the various filter categories and parameters for 'Alerts Displayed'.

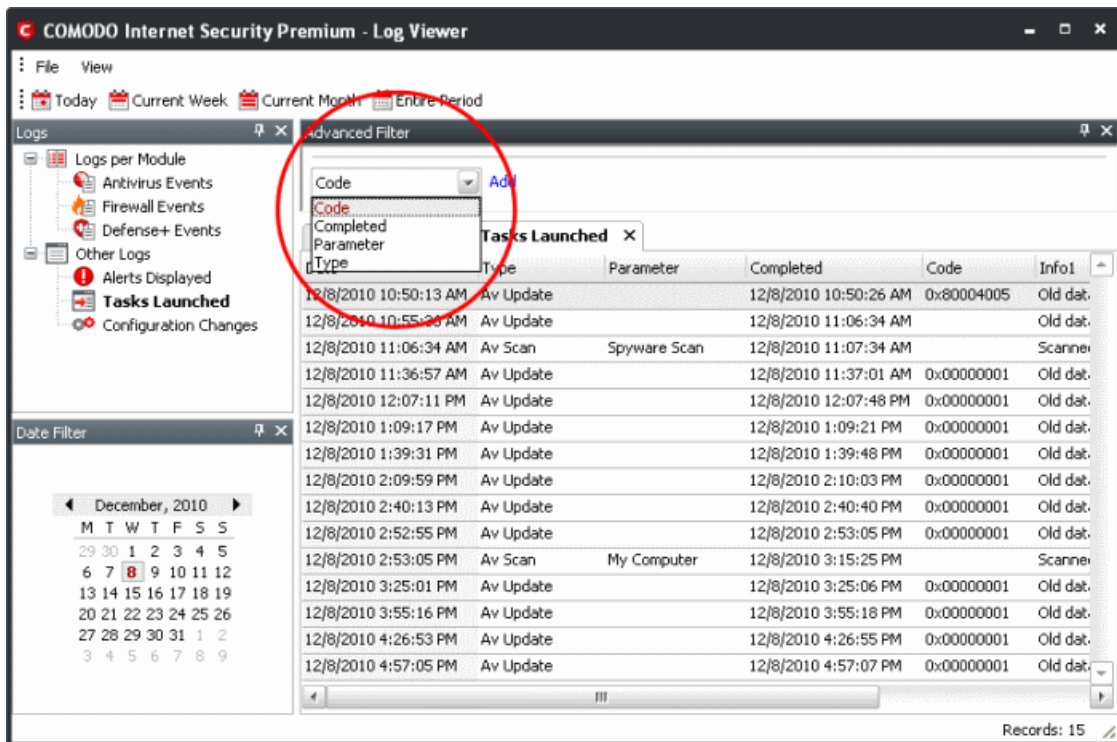
Available Filters - Other Logs - Alerts Displayed	
Filter Option	Description
Type	Displays the type of alert. It can be a Firewall, Defense+ or Antivirus alert
Description	Displays the name of the event
Advice	Suggests an advice that can be executed by the user for that event
Answered	Displays the date and time on which the alert was answered
Flags	Filters the events based on the flags set for them.
Answer	Displays the answer that was given by you for the alert
Treat As	Displays the type of policy, if any, for the corresponding event type

## To configure Advanced Filters for Tasks Launched

- Select 'View > Advanced Filter'.
- Under 'Other Logs', select 'Tasks Launched'.

This will open the Advanced Filter pane to the upper right. From here, 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.

- Click 'Add' when you have chosen the category upon which you wish to filter.



The following table lists the various filter categories and parameters for 'Tasks Launched'.

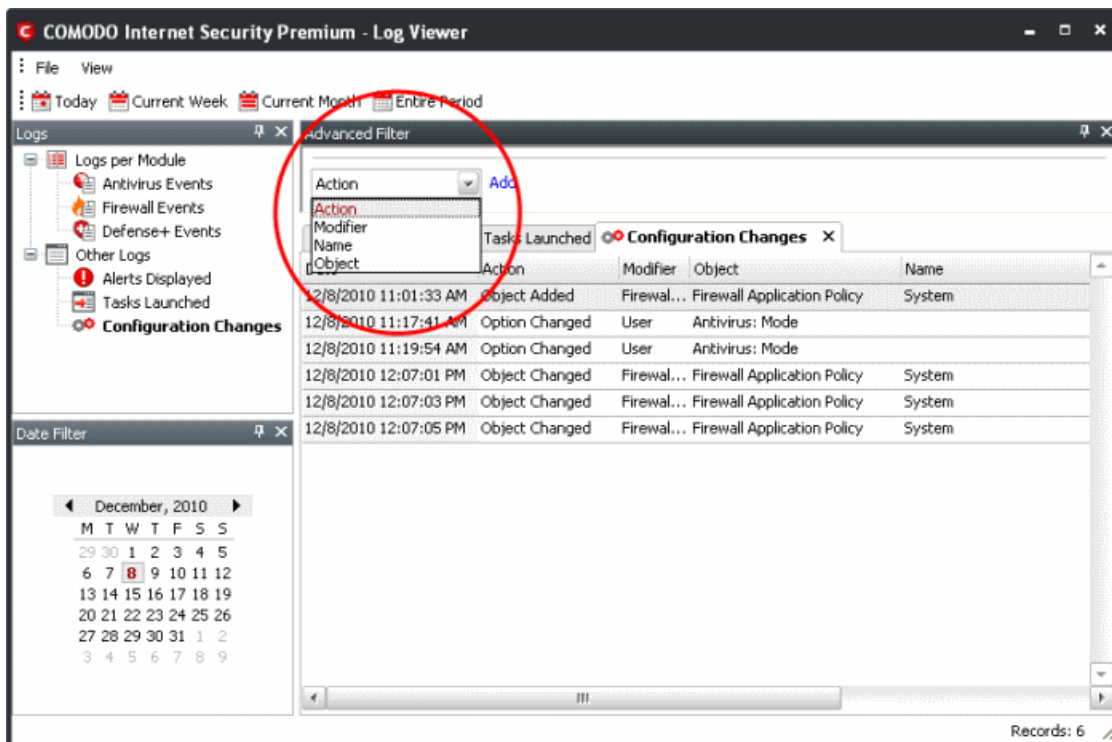
Available Filters - Other Logs - Tasks Launched	
Filter Option	Description
Type	Displays the type of task. It can be an antivirus update or scan type.
Parameter	Displays the name of the scan profile. This column is populated only if 'Av Scan' option is displayed in 'Type' column.
Completed	Displays the date and time at which the task was executed.
Code	Displays a code value if the task was not performed successfully and for task updates it shows a standard value: 0x00000001 if base is up to date

### To configure Advanced Filters for 'Configuration Changes'

- Select 'View' > 'Advanced Filter'
- Under 'Other Logs', select 'Configuration Changes'

This will open the Advanced Filter pane to the upper right. From here, you can chose the category of filter from a drop down box. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided.

- Click 'Add' when you have chosen the category upon which you wish to filter.

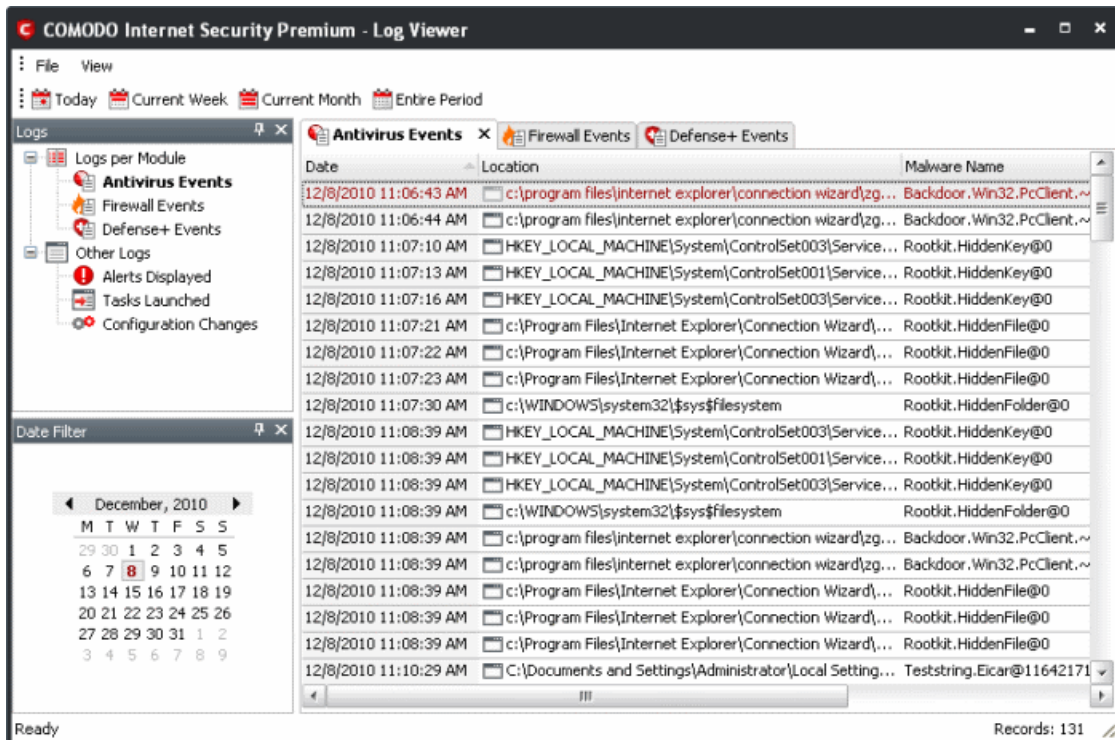


The following table lists the various filter categories and parameters for 'Configuration Changes'.

Available Filters - Other Logs - Configuration Changes	
Filter Option	Description
Action	Displays events according to the response (or action taken) by Defense+
Modifier	Displays events sorted based on whether the configuration was changed by the User, Antivirus alert, Firewall alert or Defense+ alert. It could also be a Buffer Overflow alert, Auto learn or Execution alert.
Object	Displays the object for which the configuration change took place.
Name	Displays the name of the configuration entry, if it can be determined

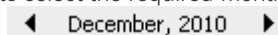
## Date Filter

The Date Filter can be seen in the lower left hand pane. Using the Date Filter you can easily see the events on a particular date or on a date range.

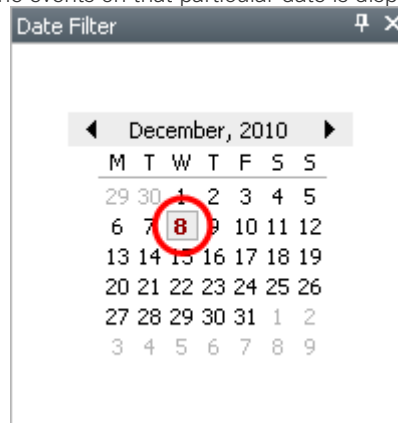


## To view the events on a particular date

1. Click the right arrow or the left arrow to select the required month and year.

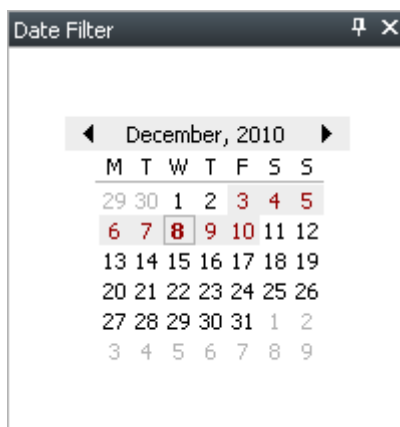


2. Now, click the required date. The events on that particular date is displayed.



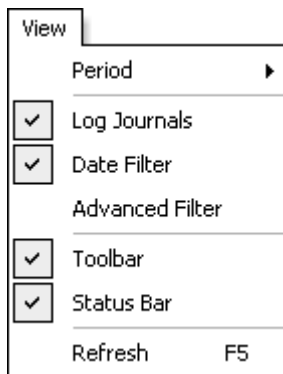
## To view the events on a date range

1. Click the right arrow or the left arrow to select the required month and year.
2. Select the start date from which you wish to view the events. Hold the shift key and click the end date till which you wish to view the events. The events for that particular date range is displayed.



### To close the Date Filter

- Click the 'X' symbol in Date Filter.  
Or
- Click 'View' in the menu bar and click the 'Date Filter' option. This is a toggle command and you can repeat this step to make the Date Filter appear.



### Exporting Log Files to HTML

Exporting log files is useful for archiving and troubleshooting purposes. After making your choice and setting the filters, the log displayed can be directly exported as HTML file. There are two ways to export log files in the Log Viewer interface - using the context sensitive menu and via the 'File' menu option.

#### i. File Menu

1. Select the event for which the log report is to be taken.
2. Click 'Export' from the File menu.
3. Select the location where the log report has to be saved, provide a file name and click 'Save'.

#### ii. Context Sensitive Menu

1. Right click in the log display window to export the currently displayed log file to HTML.

You can export a custom view that you created using the available Filters by right clicking and selecting 'Export' from the context sensitive menu. Again, you are asked to provide a file name and save location for the file.

## 2.5 Submit Files to Comodo for Analysis

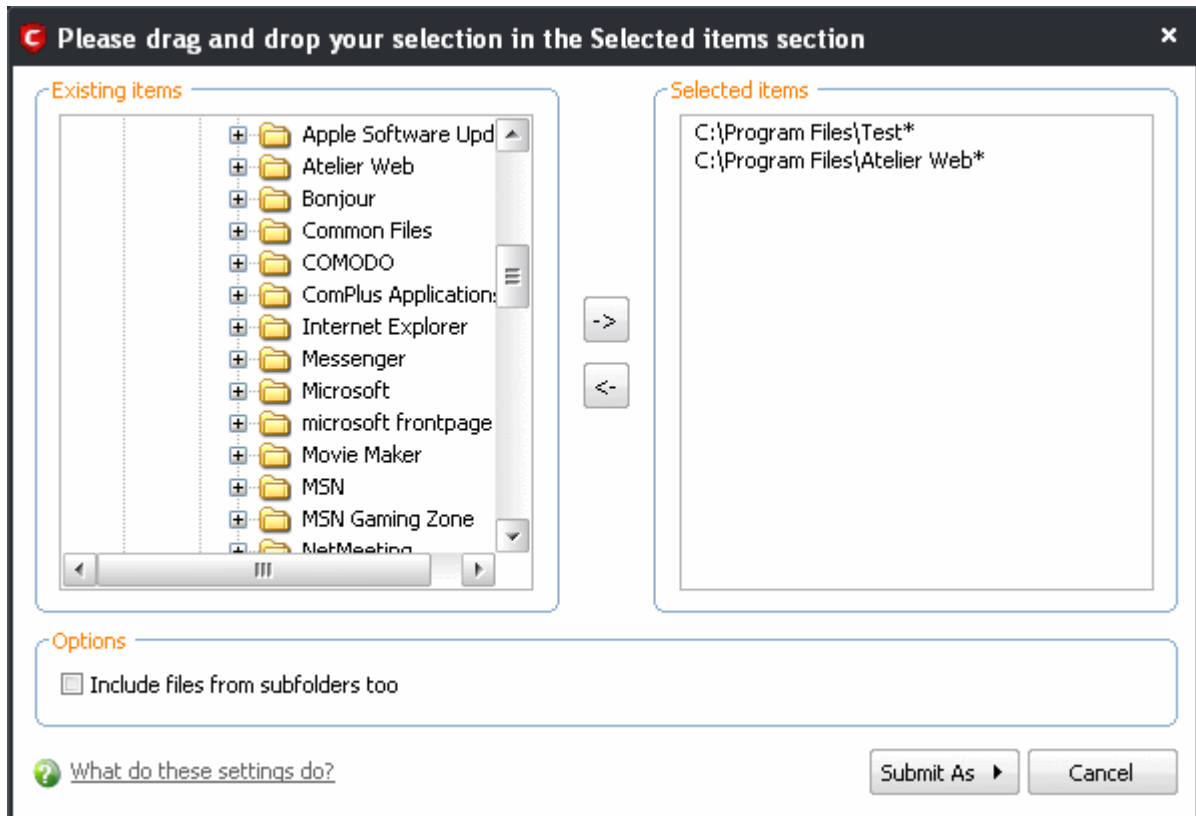
Files which are not in the Comodo safe list and are also unknown to the user can be submitted directly to Comodo for analysis and possible addition to the safe list. Files can also be submitted by clicking 'Submit' button in the **Unrecognized Files** interface.



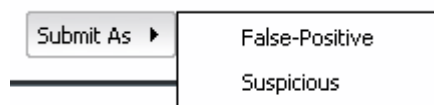
You can submit the files which you suspect to be a malware or the files which you consider as safe but identified as malware by Comodo Antivirus (False Positives). The files are analyzed by experts in Comodo and added to white list or black list accordingly.

### To submit files to Comodo

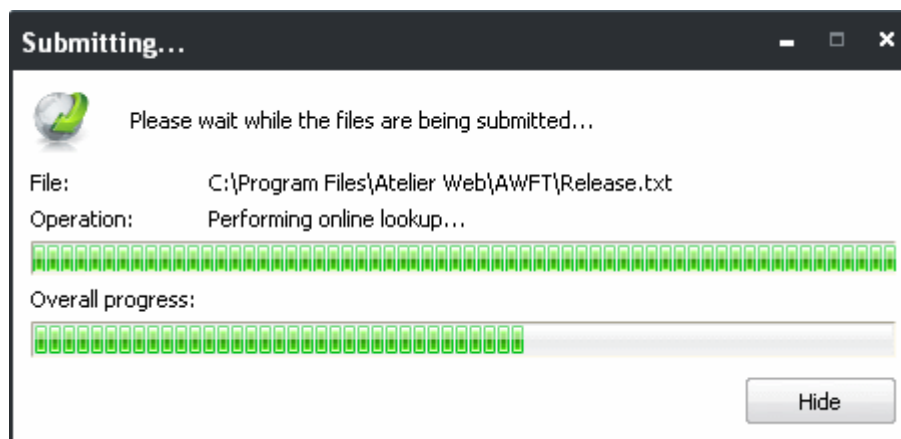
1. Click on the 'Submit Files' link from the main Antivirus Task Manager screen. The Browser dialog opens.



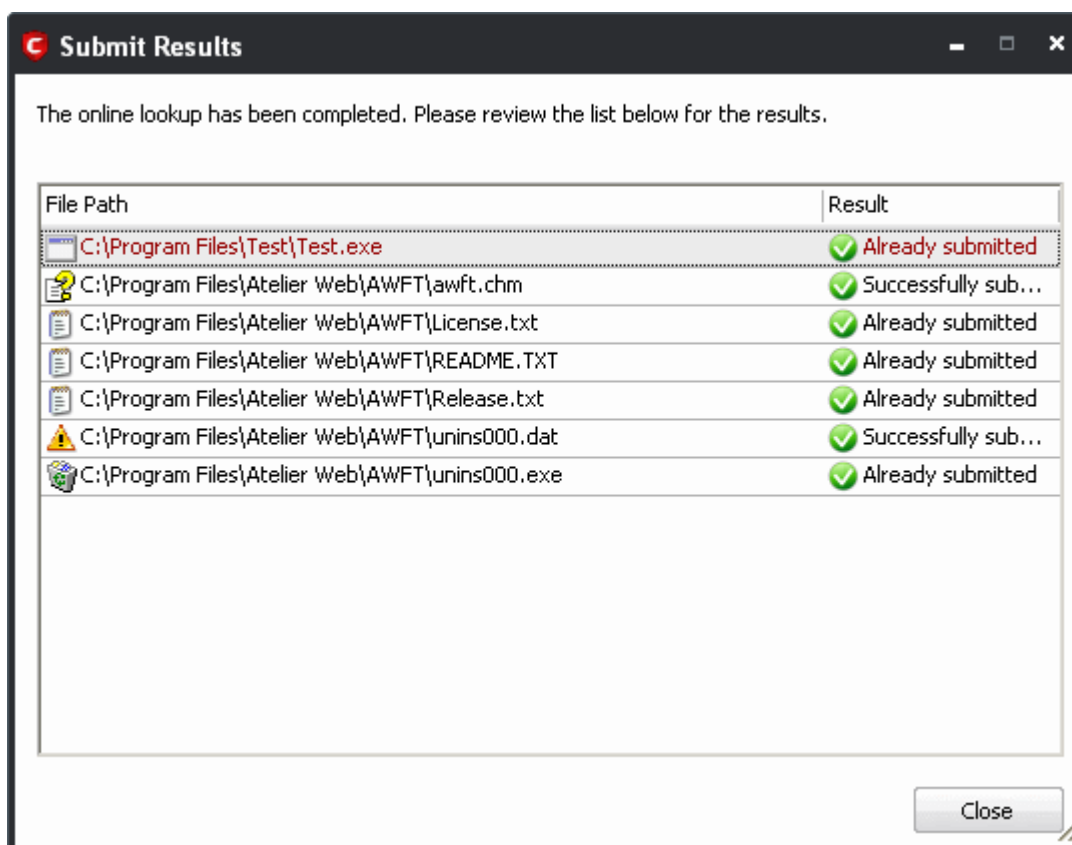
2. Select the items (files or folders) you wish to submit to Comodo for analysis from the right hand pane and move them to left hand pane by clicking the right arrow one by one. (If you want to revert a file, select the file from the left hand pane and click the left arrow)
3. Click 'Submit As' and select :
  - 'False-Positive' for files you consider to be safe or
  - 'Suspicious' for files you suspect to be malware from the submit options.



Progress bars indicate the progress of the files submission to Comodo.



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:



- 'Successfully submitted' - 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).

## 2.6 Scheduled Scans

Comodo Antivirus features a highly customizable scheduler that lets you timetable scans according to your preferences. Comodo Antivirus automatically starts scanning the entire system or the disks or folders contained in the profile selected for that scan.



You can add an unlimited number of scheduled scans to run at a time that suits your preference. A scheduled scan may contain any profile of your choice.

You can choose to run scans at a certain time on a daily, weekly, monthly or custom interval basis. You can also choose which specific files, folders or drives are included in that scan.

Perhaps you wish to check your entire system first thing in the morning; maybe you prefer the middle of the night!! Comodo Antivirus gives you the power to choose, allowing you to get on with more important matters with complete peace of mind.

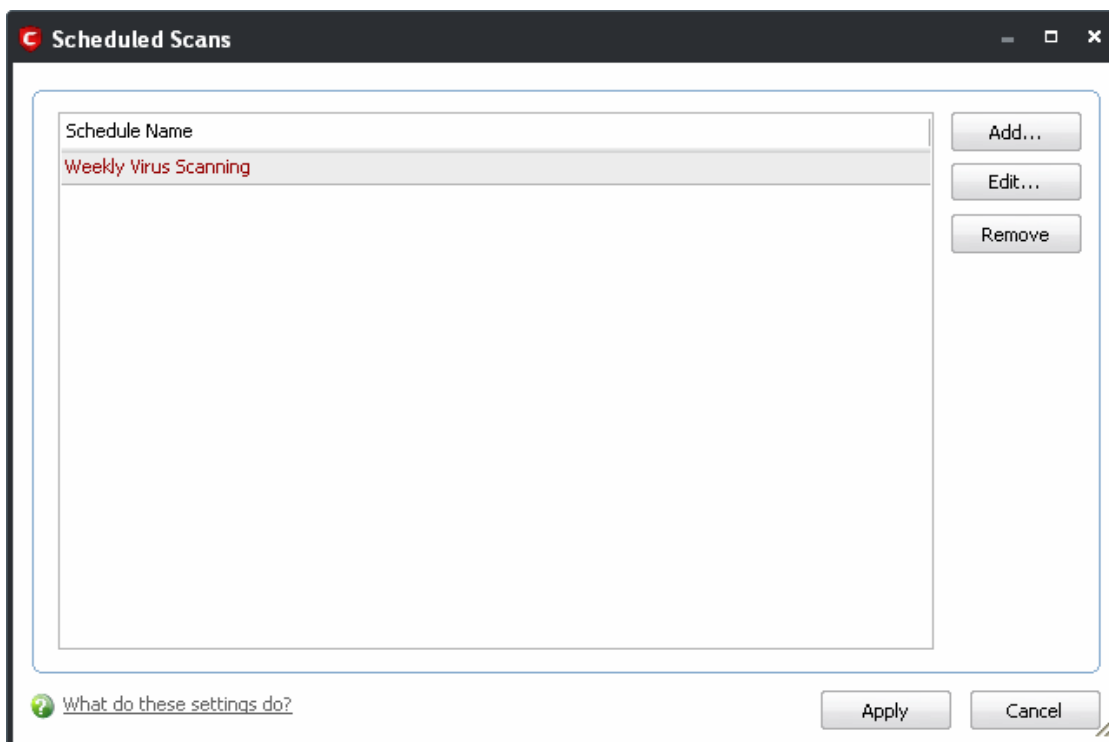
From the 'Scheduled Scans' panel, you can

- **Set a new scheduled scan**
- **Edit a pre-scheduled scan** and
- **Cancel a pre-scheduled scan**

The detection settings for the Scheduled Scans can be configured under the **Scheduled Scanning** tab of the **Scanner Settings** interface.

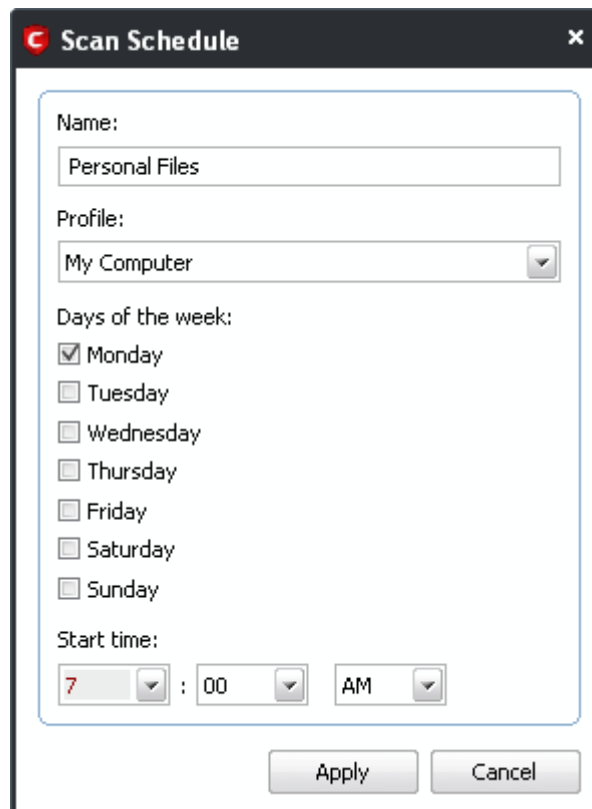
## To set a Scheduled Scan

1. Click on the Scheduled Scans link in the main Antivirus Task Manager screen.



A default schedule 'Weekly Virus Scanning' is displayed. This schedule is set so that your computer is scanned on every Sunday at 12:00am. You can edit this schedule by selecting it and clicking the 'Edit' button.

2. Click 'Add'. The 'Scan Schedule' panel opens.



3. Type a name for the newly scheduled scan in the 'Name' box.
4. Select a scanning profile from the list of preset scanning profiles by clicking at the drop-down arrow, in the 'Profile' box. (For more details on creating a custom Scan Profile that can be selected in a scheduled scan, see [Antivirus Tasks > Scan Profiles](#).)
5. Select the days of the week you wish to schedule the scanning from 'Days of the Week' check boxes.
6. Set the starting time for the scan in the selected days in the 'Start time' drop-down boxes.
7. Click 'Apply'.

Repeat the process to schedule other scans with other predefined scan profiles.

### To edit a Scheduled Scan

1. Select the schedule from the list.
2. Click 'Edit' in the 'Scheduled Scans' setting panel.
3. Edit the necessary fields in the 'Scan Schedule' panel.
4. Click 'Apply'.

### To cancel a pre-scheduled scan

1. Select the Scan Schedule you wish to cancel in the 'Scheduled Scans' settings panel.
2. Click 'Remove'.

## 2.7 Scan Profiles

Creating a Scan Profile allows you to instruct Comodo Antivirus scan selected areas, folders or selected drives of your system. You will be asked to select a profile whenever you click the 'Scan Now' link on the Summary Screen.

You can create custom scan profiles, to define selected disks or folders to be scanned and the created scan profile can be

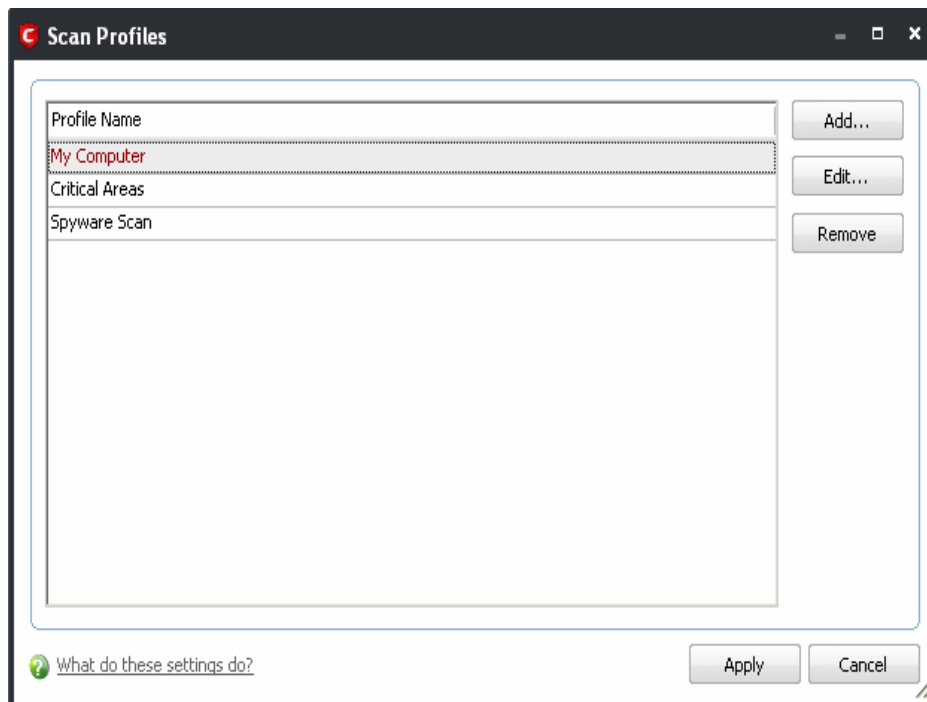
re-used for any desired scan event i.e. Run a Scan (On-Demand Scanning) and Scheduled Scans. You can create as many number of custom scan profiles as you wish according to the usage of your system. A Scan Profile allows you to scan only a selected area of your storage, saving time and resources.

- New scan profiles can be created by clicking the '**Create New Scan**' button in the '**Run a Scan**' panel or by clicking the 'Add button' in the 'Scan Profiles' area.
- New scan profiles can then be referenced when creating a new '**Scheduled Scan**' and as the target of an on-demand scan in the '**Run a scan**' area.

Just to clarify, AntiVirus scan profiles are purely concerned with the location of a scan, not the parameters of the scan. All scan profiles use the parameters as determined in the specific '**Scanner Settings**' tab of that type of scan.

### To access the Scan Profiles interface

- Click 'Scan Profiles' from the main Antivirus Tasks Manager Screen.



Comodo Antivirus contains three default Scan Profiles 'My Computer', 'Critical Areas' and Spyware Scan. These three profiles are predefined and cannot be edited or removed.

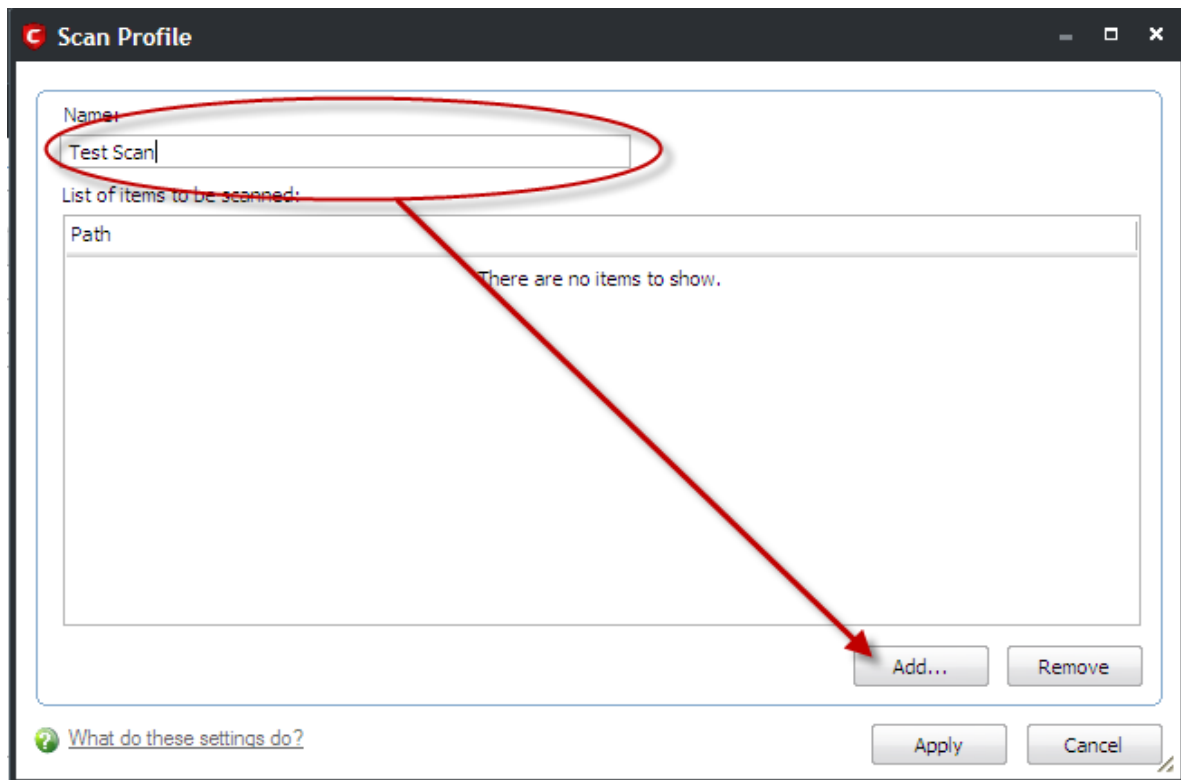
- **My Computer (Default)** - On selecting this, the Antivirus scans all drives on your machine
- **Critical Areas** - On selecting this, the Antivirus scans "Windows", "Program Files", and "Document and Settings" folders.
- **Spyware Scan** - Spyware is a type of malware that gathers data from your system and transmits it to a 3rd party without your knowledge. Spyware is almost always hidden away on your system so it can carry out such tasks without you noticing (and often, without affecting the performance of your computer in any significant way). The most dangerous type of spyware will use a variety of techniques to steal vital information from your computer such as passwords, credit card numbers and other confidential information. An example would be a 'keylogger', which records every stroke you make on the keyboard and sends this information to an hacker or other unknown third party.

The Spyware Scan feature in Comodo Antivirus scans your Windows registry and system files to check whether your computer is infected with such malware and alerts you. This scanning feature improves the detection and successful cleaning rate of already infected systems .

You can select any one of these Scan Profiles if you want to scan the respective areas.

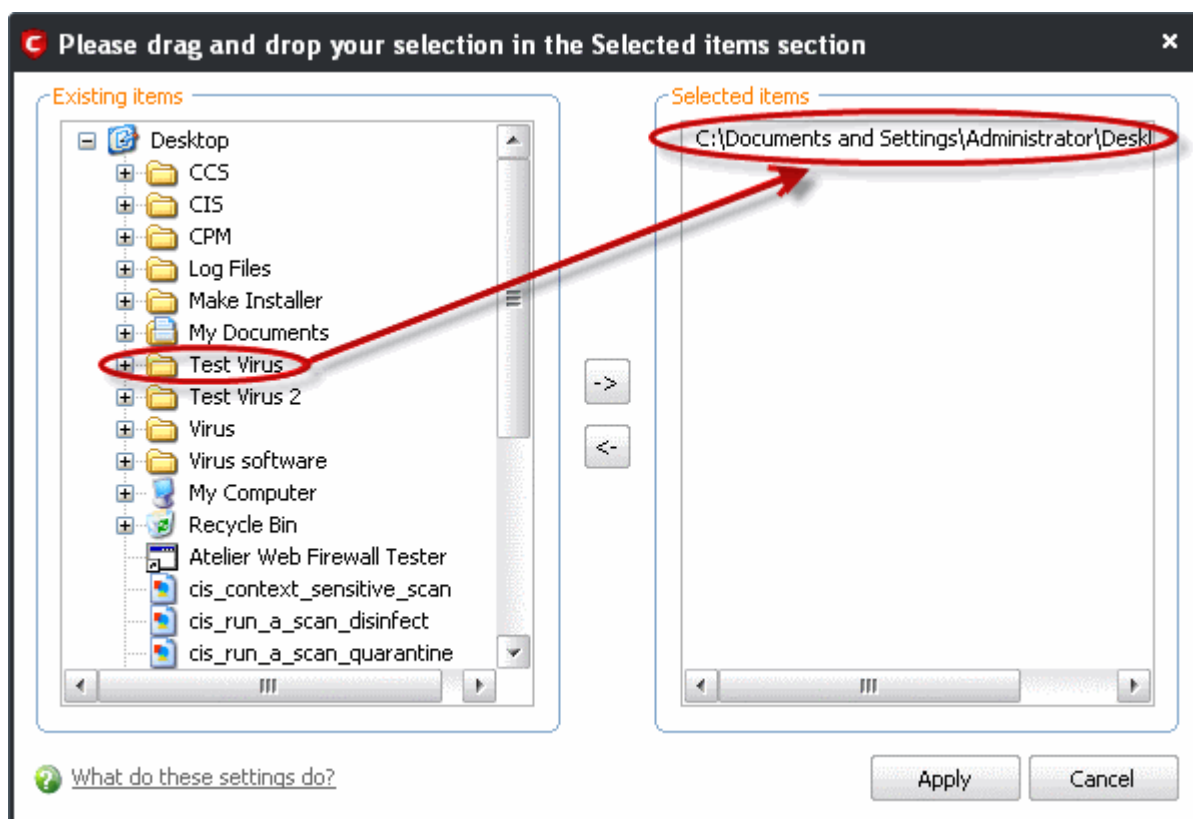
### To create a new scan profile from Scan Profiles option

1. Click 'Scan Profiles' from the main Antivirus Tasks Manager Screen.
2. Click 'Add'. The 'Scan Profile' dialog appears.
3. Type a name for the scan profile to be created in the 'Name' box and click 'Add'.



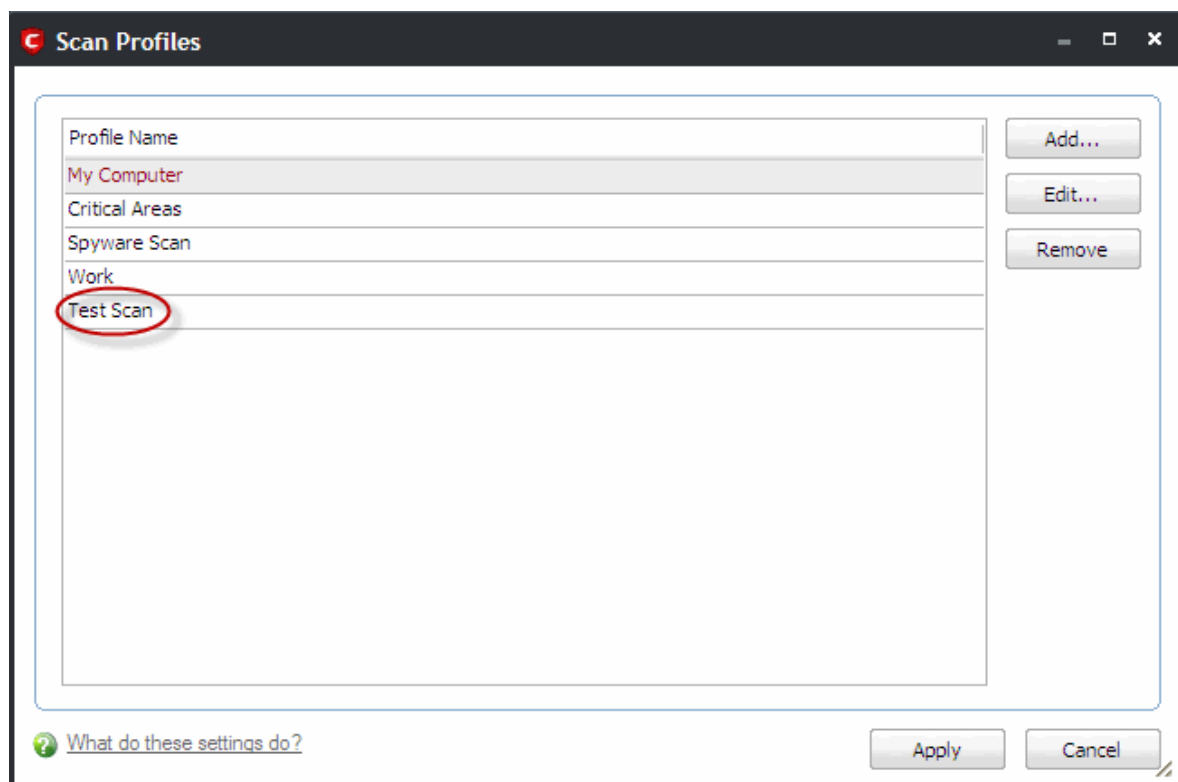
A configuration screen appears, prompting you to select the locations to be scanned when the newly created scan profile is selected. The left column displays all possible items (drives, folders and files) on your system for which scanning is available.

4. Browse to the folder location in the left column and select the folder.
5. Drag and drop all the files, folders and/or drives you require, into the right hand panel or select the files or folders and move them to left-hand pane by clicking the right arrow one by one. (If you want to revert a file, select the file from the left hand pane and click the left arrow)

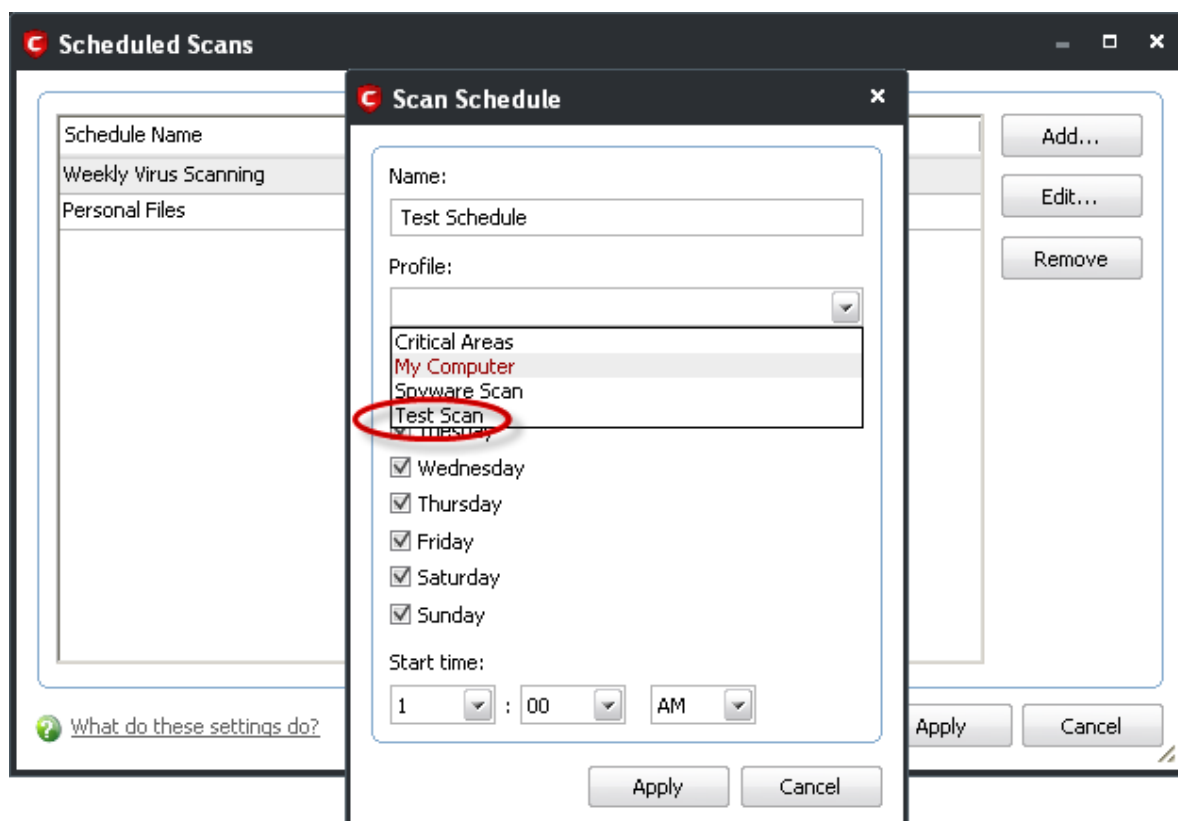


6. Click 'Apply'.
7. Repeat the process to create more Scan Profiles.
8. Click 'Apply' in the Scan Profile interface for the created profiles to take effect.

You can see that the Scan Profile you have created, appearing as a target profile in the 'Run a Scan' panel...



...it is also available for selection during a scheduled scan in the drop-down.



- To edit a Scan Profile, select the profile and click 'Edit'.
- To delete a Scan Profile, select the profile and click 'Remove'.

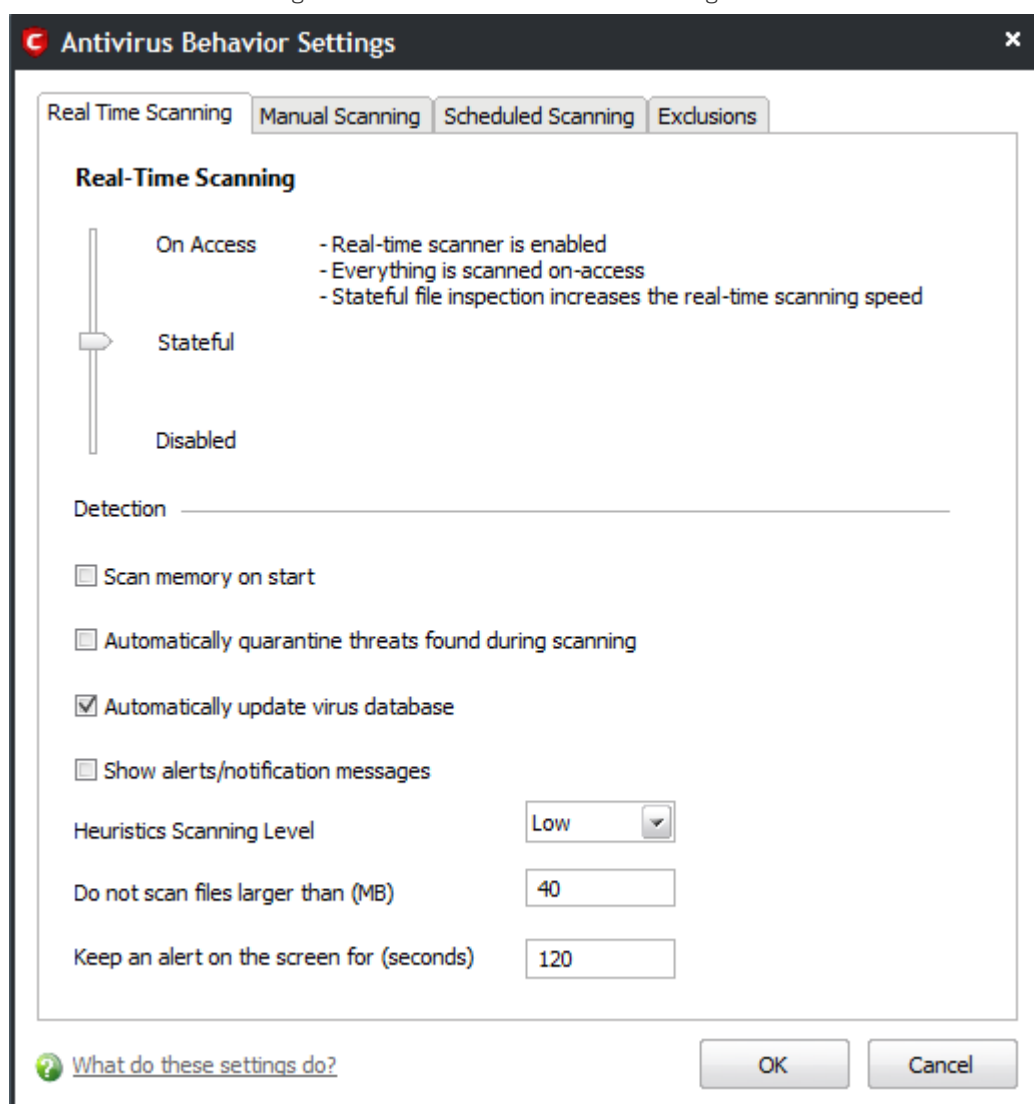
## 2.8 Scanner Settings

The Settings configuration panel allows you to customize various options related to Real Time Scanning (On-Access Scanning), Manual Scanning, Scheduled Scanning and Exclusions (a list containing the files you considered safe and ignored the alert during a virus scan).

- The settings made for each type of the scan applies to all future scans of that type.
- All items listed and all items added to the 'Exclusions' list is excluded from all future scans of all types.

### To open Virus Scanner Settings panel

- Click on 'Scanner Settings' link in the main Antivirus Tasks Management Screen.



The options that can be configured using the settings panel are

- **Real Time Scanning** - To set the parameters for on-access scanning;
- **Manual Scanning** - To set the parameters for manual Scanning (Run a Scan);
- **Scheduled Scanning** - To set the parameters for scheduled scanning;
- **Exclusions** - To see the list of ignored threats and to set the parameters for Exclusions.

## 2.8.1 Real Time Scanning

The Real time Scanning (aka 'On-Access Scanning') 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.

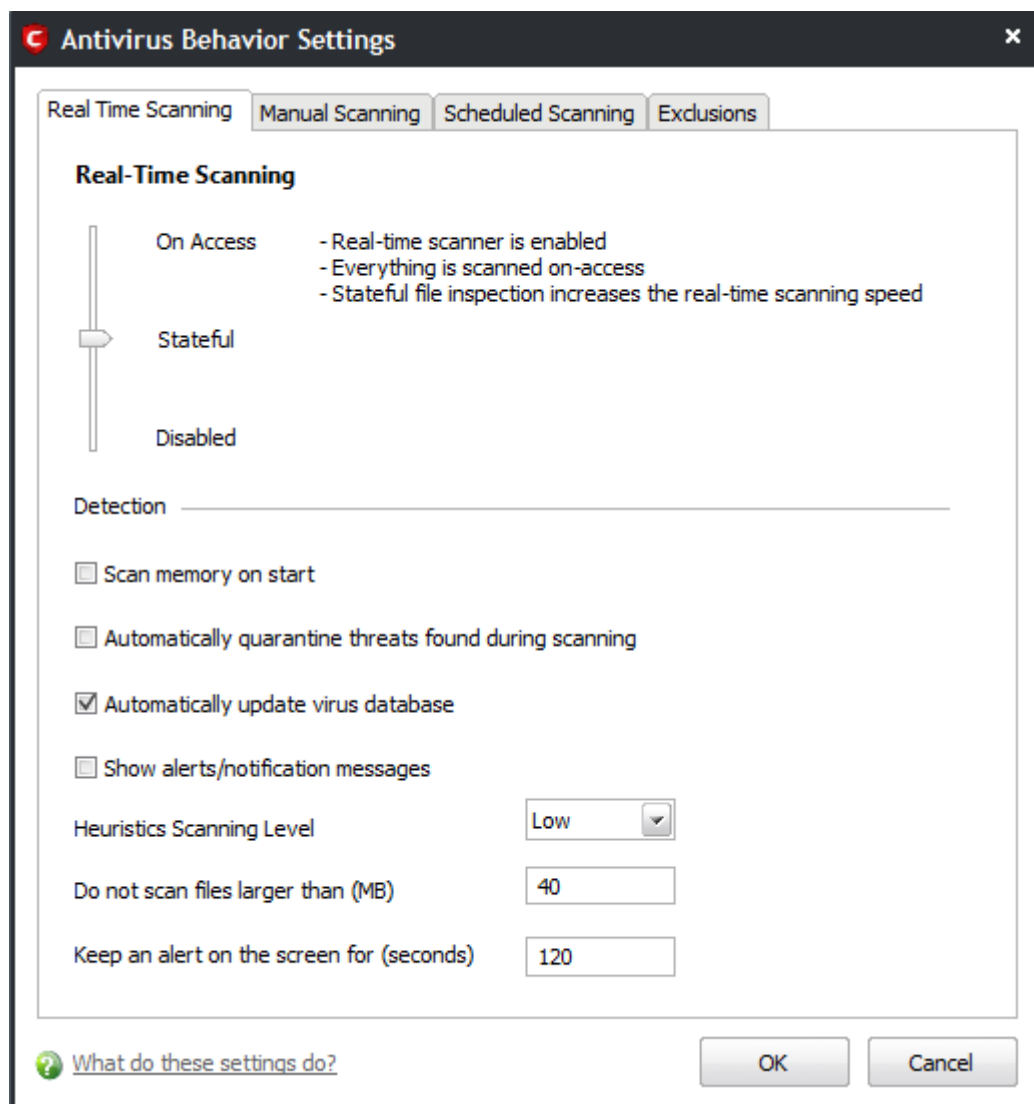
The Real Time Scanner also scans the system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately - giving you real time protection against threats.

You also have options to automatically remove the threats found during scanning and to update virus database before scanning. It is highly recommended that you enable the Real Time Scanner to ensure your system remains continually free of infection.

The Real Time Scanning setting allows you to switch the On Access scanning between **Disabled**, **Stateful** and **On Access** and allows you to specify detection settings and other parameters that are deployed during on-access scans.

### To set the Real Time Scanning level

- Click on the 'Real Time Scanning' tab in the 'Scanner Settings' panel.
- Drag the real time Scanning slider to the required level. The choices available are **Disabled** (not recommended), **Stateful** (*default*) and **On Access**. The setting you choose here are also displayed in the Summary screen.



- **On Access** - Provides the highest level of On Access Scanning and protection. Any file opened is scanned before it is run and the threats are detected before they get a chance to be executed.
- **Stateful (Default)** - Not only is Comodo Internet Security one of the most thorough and effective AV solutions available, it is also very fast. CIS employs a feature called Stateful File Inspection for real time virus scanning to minimize the effects of on-access scanning on the system performance. Selecting the 'Stateful'

option means CIS scans only files that have not been scanned since the last virus update - greatly improving the speed, relevancy and effectiveness of the scanning.

- **Disabled** - The Real time scanning is disabled. Antivirus does not perform any scanning and the threats cannot be detected before they impart any harm to the system.

#### Detection Settings

- **Scan memory on start** - When this check box is selected, the Antivirus scans the system memory during system start-up (*Default = Disabled*).
- **Automatically quarantine threats found during scanning** - When this check box is selected, the Antivirus moves the file detected to be containing the malware, to Quarantined Items. From the quarantined items the files can be restored or deleted at your will (*Default = Disabled*).
- **Automatically update virus database** - When this check box is selected, Comodo Internet Security checks for latest virus database updates from Comodo website and downloads the updates automatically, on system start-up and subsequently at regular intervals (*Default = Enabled*).
- **Show alerts/notification messages** - Alerts are the pop-up notifications that appear in the lower right hand of the screen whenever the on-access scanner discovers a virus on your system. These alerts are a valuable source of real-time information that helps the user to immediately identify which particular files are infected or are causing problems. Disabling alerts does not affect the scanning process itself and Comodo Antivirus still continues to identify and deals with threats in the background. For more details on Antivirus alerts, [click here](#) (*Default = Enabled*).
- **Heuristics Scanning/Level** - Comodo AntiVirus 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 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 matches 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.

The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

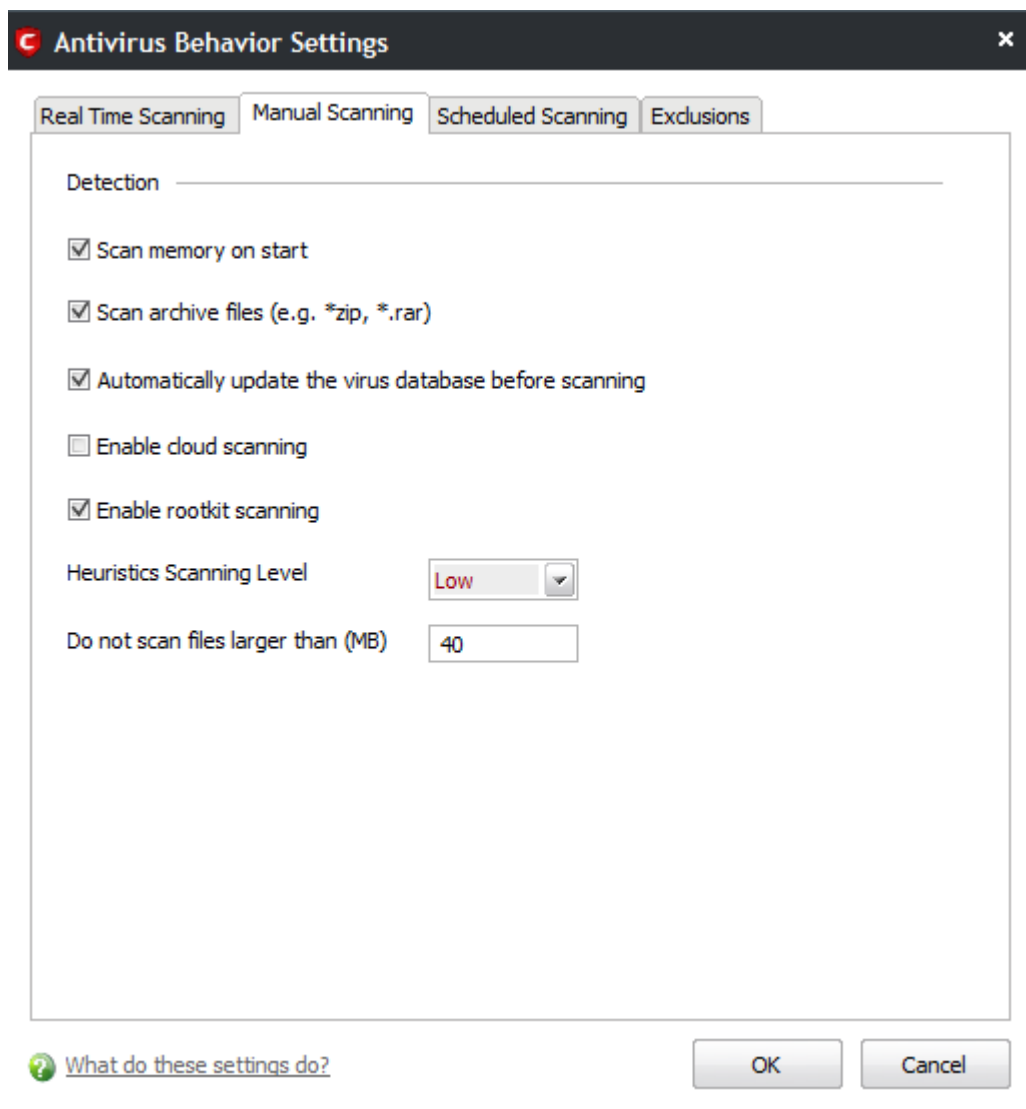
- **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
- **Low (Default)** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false 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. .
- **Do not scan files larger than** - 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, are not scanned. (*Default = 40 MB*).
- **Keep an alert on the screen for** - This box allows you to set the time period (in seconds) for which the alert message should stay on the screen (*Default = 120 seconds*).

Click 'OK' for the settings to take effect.

## 2.8.2 Manual Scanning

The Manual Scanning setting allows you to set the properties and parameters for Run a Scan (On Demand Scan).





- **Scan memory on start** - When this check box is selected, the Antivirus scans the system memory while starting a manual scan i.e. **Run a Scan** option (**Default = Enabled**).
- **Scan archive files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. You are alerted to the presence of viruses in compressed files before you even open them. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (**Default = Enabled**).
- **Automatically update virus database before scanning** - Instructs Comodo Internet Security to check for latest virus database updates from Comodo website and download the updates automatically before starting an on-demand scanning (**Default = Enabled**).
- **Enable Cloud Scanning** - Instructs Comodo Internet Security to perform cloud based antivirus scanning. Selecting this option enables CIS 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**).
- **Submit unknown files for analysis** - Files that are classified as unknown even after cloud scanning will be automatically submitted to Comodo for analysis for inclusion in blacklist or whitelist accordingly when this option is selected. This option will be enabled only when Enable cloud scanning is enabled (**Default = Disabled**).
- **Enable rootkit scanning** - Instructs Comodo Internet Security to scan the file system and Windows registry for (malicious) files or registry values that have been hidden by rootkits. If any such Rootkits are found, they are listed in the scan results - enabling you to remove them from your system (**Default = Disabled**).

**Background Note:**

A rootkit is a type of malware that is designed to conceal the fact that the user's system has been compromised. Once installed, they camouflage themselves as (for example) standard operating system files, security tools and APIs used for diagnosis, scanning, and monitoring. Rootkits then store hidden malicious files into the Window's file system and/or store hidden registry values into the Window's Registry. These malicious files and registry values can be used by hackers to steal user passwords, credit card information, computing resources, or conduct other unauthorized activities.

Rootkits are usually not detectable by normal virus scanners as they camouflage themselves as system files. However, Comodo AntiVirus features a dedicated Rootkit detection scanner that identifies rootkits and, if any, the hidden files and the registry keys stored by them. Any discovered rootkits, hidden malicious files or registry values are listed along with the Antivirus Scan results at the end of each manual scan.

- **Heuristics Scanning/Level** - 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 typical of a virus. If it is found to do so then the application deletes the file or recommend it for quarantine. 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 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.

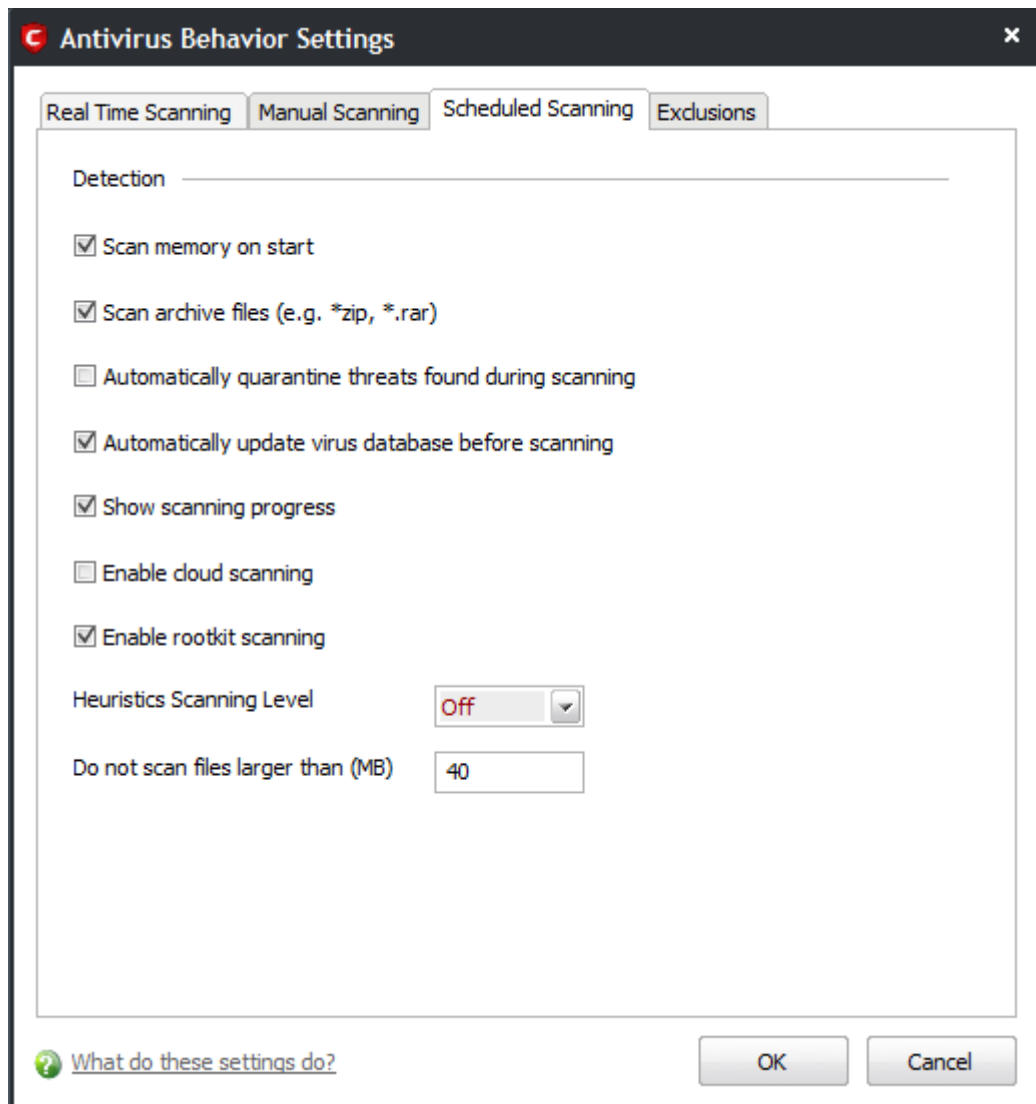
The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

- **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the traditional virus signature database to determine whether a file is malicious or not.
- **Low (Default)** - '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.
- **Do not scan files larger than** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during manual scanning. Files larger than the size specified here, are not scanned (**Default = 40 MB**).

Click 'OK' for the settings to take effect .

### 2.8.3 Scheduled Scanning

The Scheduled Scanning setting panel allows you to customize the scheduler that lets you timetable scans according to your preferences.



You can choose to run scheduled scans at a certain time on a daily, weekly, monthly or custom interval basis. You can also choose which specific files, folders or drives are included in that scan by choosing the scan profiles.

The detection settings are as follows:

- **Scan memory on start** - When this check box is selected, the Antivirus scans the system memory during the start of any scheduled scan (*Default = Enabled*).
- **Scan archive files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files during any scheduled scan. You are alerted to the presence of viruses in compressed files before you even open them. These include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (*Default = Enabled*).
- **Automatically quarantine threats found during scanning** - When this check box is selected, the Antivirus moves the file detected to be containing the malware, to Quarantined Items. From the quarantined items the files can be restored or deleted at your will (*Default = Disabled*).
- **Automatically update virus database before scanning** - When this check box is selected, Comodo Internet Security checks for latest virus database updates from Comodo website and downloads the updates automatically, before the start of every scheduled scan (*Default = Enabled*).
- **Show Scanning progress** - When this check box is selected, a progress bar is displayed on start of a scheduled scan. Clear this box if you do not want to see the progress bar (*Default = Enabled*).
- **Enable Cloud Scanning** - Instructs Comodo Internet Security to perform cloud based antivirus scanning. Selecting this option enables CIS 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*).
- **Submit unknown files for analysis** - Files that are classified as unknown even after cloud scanning will be automatically submitted to Comodo for analysis for inclusion in blacklist or whitelist accordingly when this

option is selected. This option will be enabled only when Enable cloud scanning is enabled (**Default = Disabled**).

- **Enable rootkit scanning** - Instructs Comodo Internet Security to scan the file system and Windows registry for (malicious) files or registry values that have been hidden by rootkits. If any such Rootkits are found, they are listed in the scan results - enabling you to remove them from your system (**Default = Disabled**).

#### Background Note:

A rootkit is a type of malware that is designed to conceal the fact that the user's system has been compromised. Once installed, they camouflage themselves as (for example) standard operating system files, security tools and APIs used for diagnosis, scanning, and monitoring. Rootkits then store hidden malicious files into the Window's file system and/or store hidden registry values into the Window's Registry. These malicious files and registry values can be used by hackers to steal user passwords, credit card information, computing resources, or conduct other unauthorized activities.

Rootkits are usually not detectable by normal virus scanners as they camouflage themselves as system files. However, Comodo AntiVirus features a dedicated Rootkit detection scanner that identifies rootkits and, if any, the hidden files and the registry keys stored by them. Any discovered rootkits, hidden malicious files or registry values are listed along with the Antivirus Scan results at the end of each manual scan.

- **Heuristics Scanning/Level** - 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 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 matches 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.

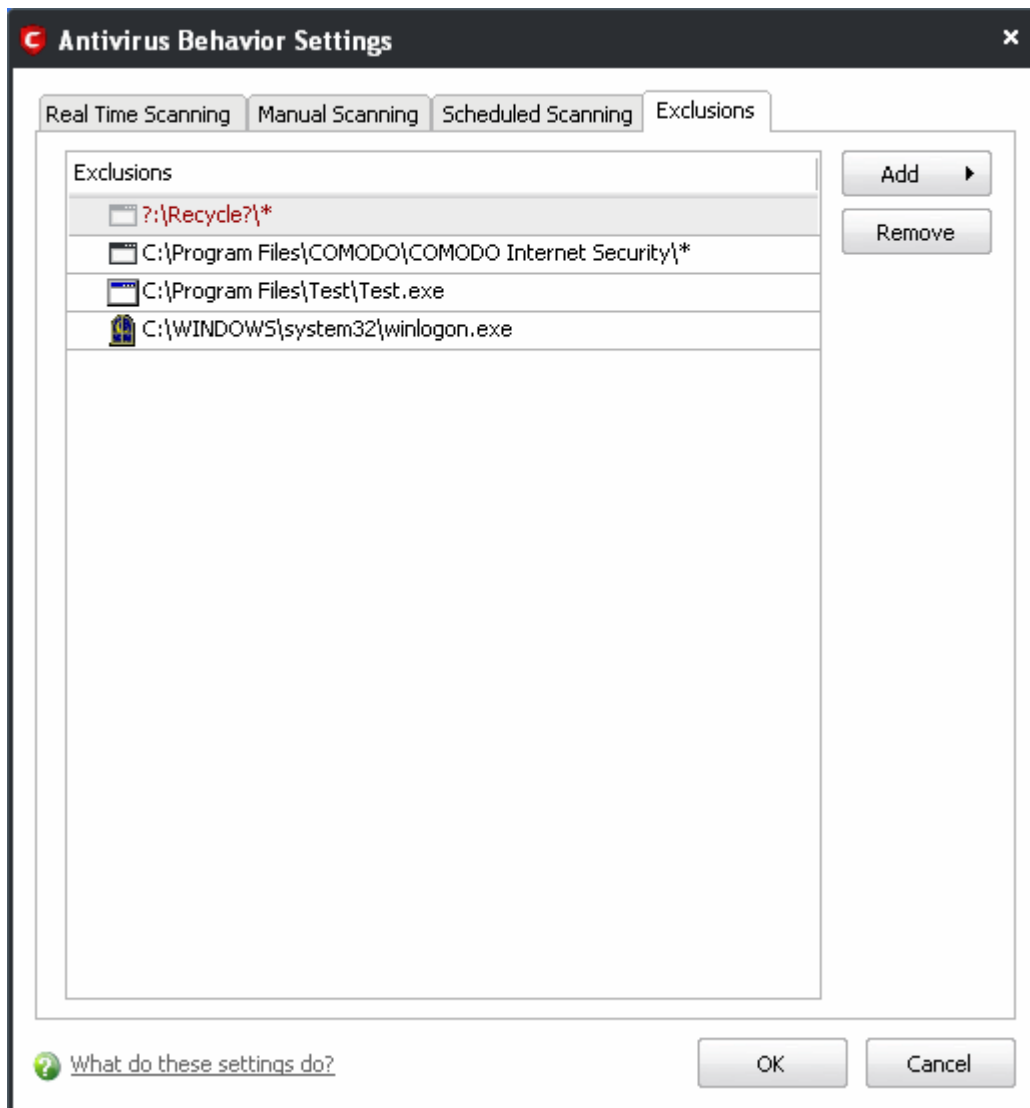
The drop-down menu allows you to select the level of Heuristic scanning from the four levels:

- **Off** - Selecting this option disables heuristic scanning. This means that virus scans only uses the 'traditional' virus signature database to determine whether a file is malicious or not.
- **Low (Default)** - '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.
- **Do not scan files larger than** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during scheduled scanning. Files larger than the size specified here, are not scanned (**Default = 40 MB**).

Click 'OK' for the settings to take effect.

## 2.8.4 Exclusions

The Exclusions tab in the Scanner Settings panel displays a list of applications/files for which you have selected **Ignore** in the **Scan Results** window of Run a Scan option or added to the Exclusions from an antivirus alert.



All items listed and all items added to the 'Exclusions' list is excluded from all future scans of all types.

Also, you can manually define trusted files or applications to be excluded from a scan .

### To define a file/application as trusted and to be excluded from scanning

1. Click 'Add'.

You now have 2 methods available to choose the application that you want to trust - '**Browse Files...**' and '**Browse Running Processes**'.

- **Browse Files...** - 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.
- **Browse Running Processes** - As the name suggests, this option allows you to choose the target application from a list of processes that are currently running on your PC.

When you have chosen the application using one of the methods above, the application name appears along with its location.

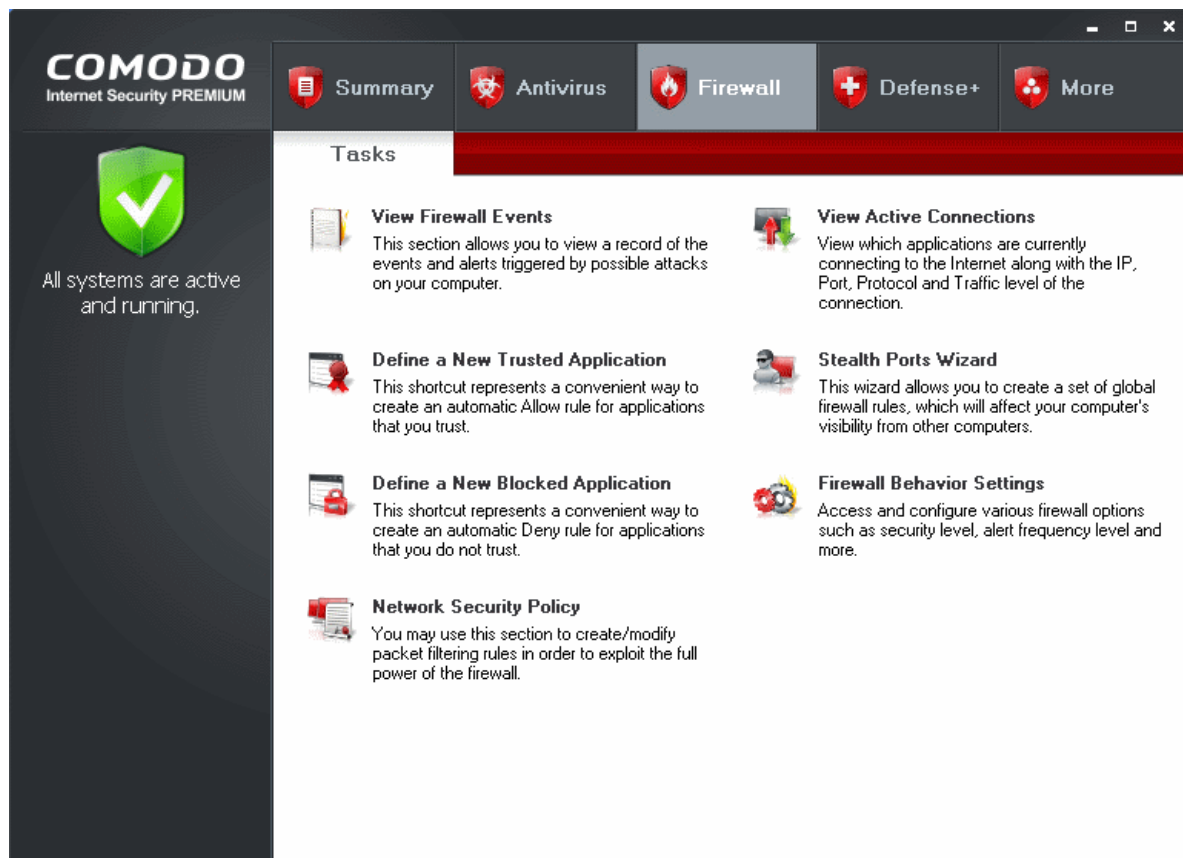
2. Click 'OK' for the settings to take effect.

## 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 link from the Navigation panel.



The Firewall main configuration area provides easy access to all the features and allows you to create rules for applications and network connections through a series of shortcuts and wizards. Click on the links below to see detailed explanations of each area in this section.

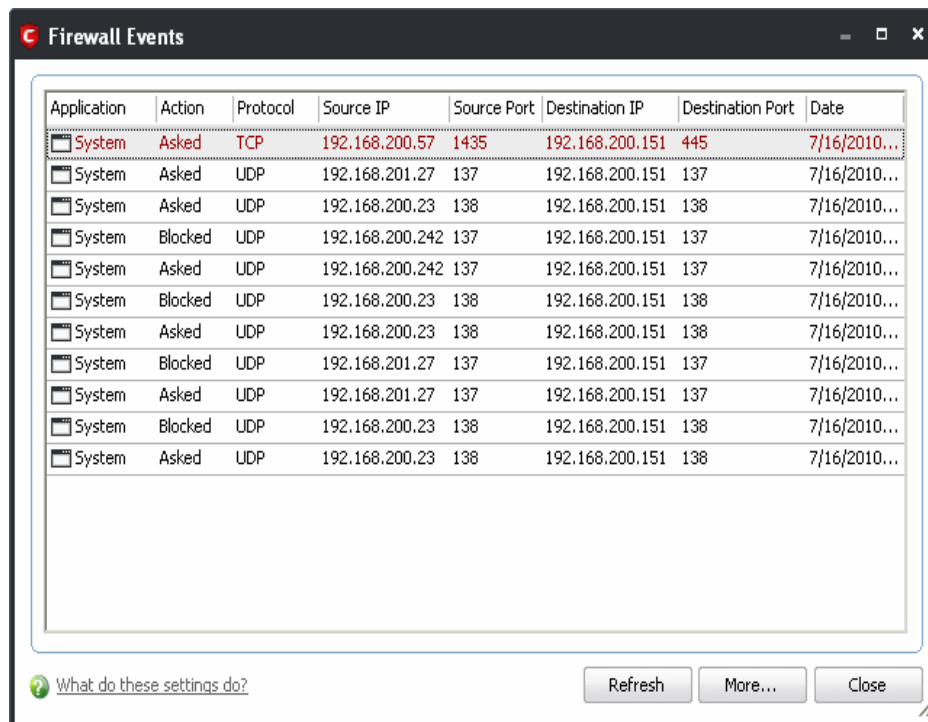
- [View Firewall Events](#)
- [Define a New Trusted Application](#)
- [Define a New Blocked Application](#)
- [Network Security Policy](#)
- [View Active Connections](#)
- [Stealth Port Wizard](#)
- [Firewall Behavior Settings](#)

### 3.1 View Firewall Events

The 'View Firewall Events' area contains logs of actions taken by the firewall. A 'Firewall Event' is recorded whenever an application or process makes a connection attempt that contravenes a rule your Network Security Policy.

## To view Firewall events

- Click 'View Firewall Events' in the common tasks of Firewall task center.



## Column Descriptions

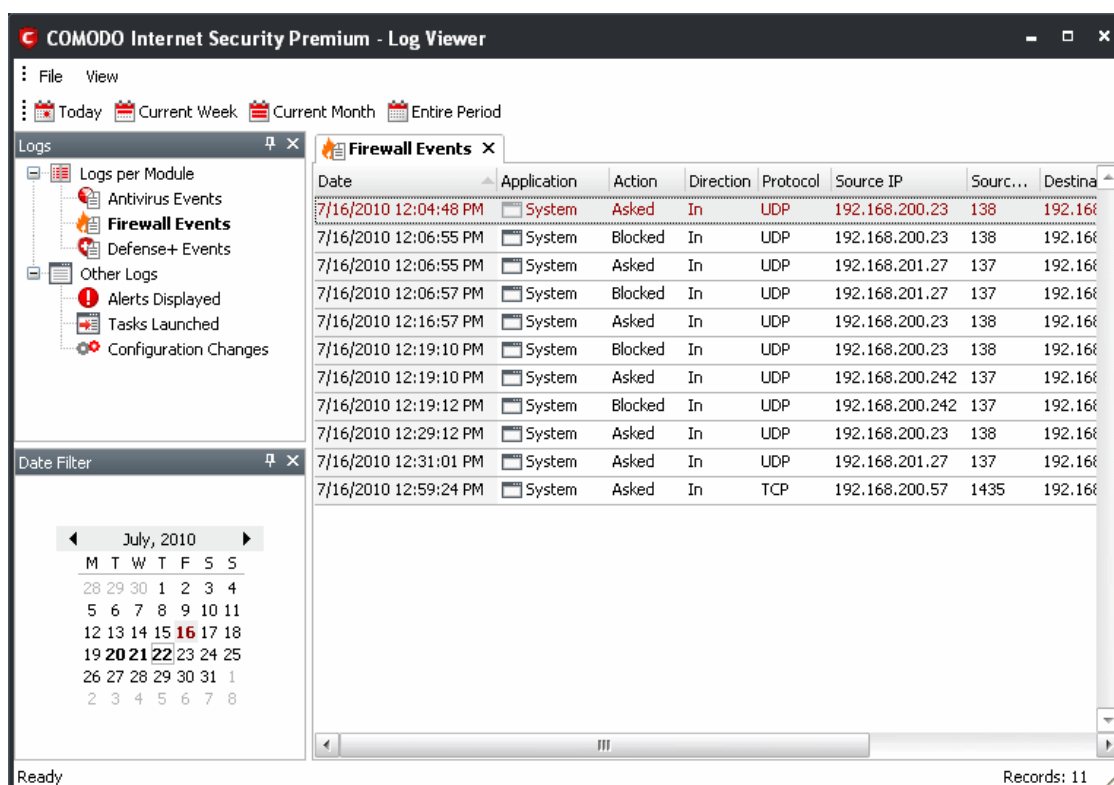
- Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used;
- Action** - Indicates how the firewall has reacted to the connection attempt.
- Protocol** - Represents the Protocol application attempted to use to create the connection. This is usually TCP/IP or UDP - which are the most heavily used networking protocols.
- 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.
- Source Port** - States the port number on the host at the source IP which was used to make this connection attempt.
- 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.
- Destination Port** - States the port number on the host at the destination IP to which the connection attempt was made.
- Date/Time** - Contains precise details of the date and time of the connection attempt.
  - Click 'Refresh' to reload and update the displayed list, to include all events generated since the time you first accessed the 'Firewall Events' area.
  - Click 'More' to load the full, Comodo Internet Security Log Viewer module. See below for more details on this module.

## Log Viewer Module

This window contains a full history of logged events in two categories: Logs per Module and Other Logs.

It also allows you to build custom log files based on **specific filters** and to **export log files** for archiving or troubleshooting purposes.





The Log Viewer Module is divided into three sections. The top panel displays a set of handy, predefined time **Filters**. The left panel the types of Logs. The right hand side panel displays the actual events that were logged for the time period you selected in the top panel and the type of log selected in the left panel (or the events that correspond to the filtering criteria you selected).

The Logs per Module option contains the logged events of Firewall, Defense+ and Antivirus modules and Other Logs options contains logged events of the following:

- **Alerts Displayed:** Displays the list of various alerts that were displayed to the user, the response given by the user to those alerts and other related details of the alert.
- **Tasks Launched:** Displays the various Antivirus tasks such as updates and scans that have taken place. This area will contain a log of all on demand and scheduled AV scans and the result of that scan.
- **Configuration Changes:** Displays a log of all configuration changes made by the user in the CIS application.

## Filtering Log Files

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

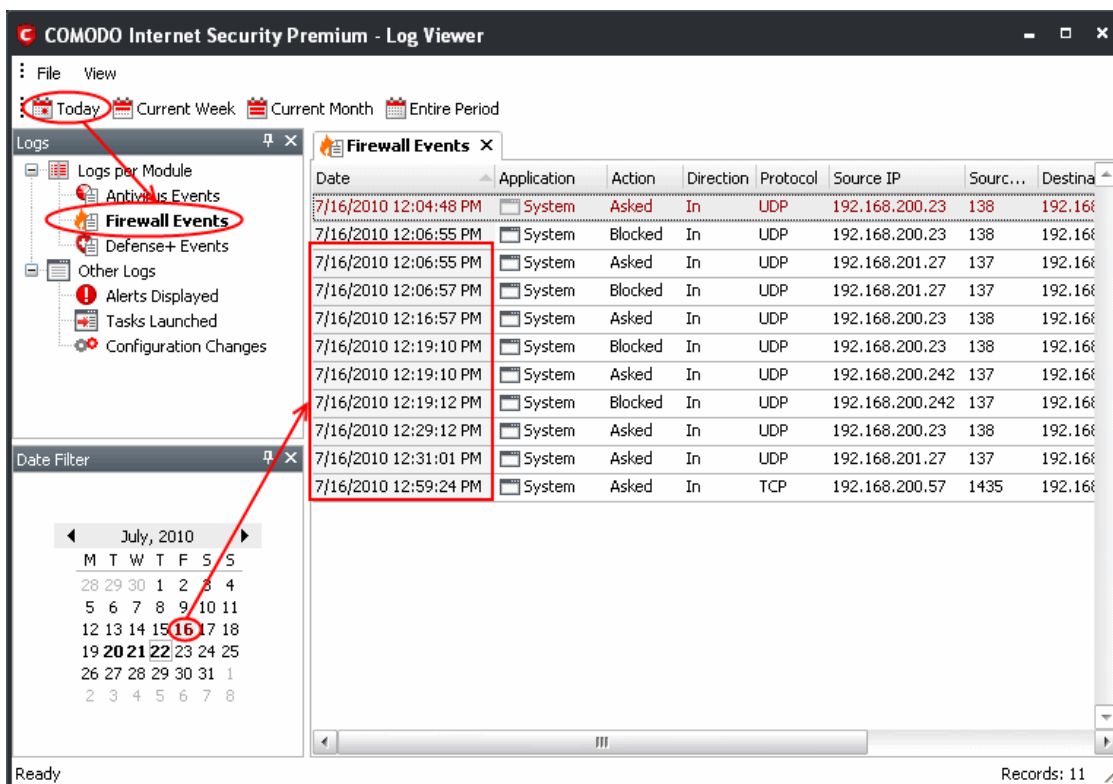
### Preset Time Filters:

Clicking on any of the preset filters in the top panel alters the display in the right hand panel in the following ways:

- **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).

The example below shows an example display when the Defense+ Logs for 'Today' are displayed.





**Note:** The type of events logged by the Antivirus, Firewall and Defense+ modules of Comodo Internet Security differ from each other. This means that the information and the columns displayed in the right hand side panel change depending on which type of log you have selected in the top and left hand side panel. For more details on the data shown in the columns, see [View Antivirus Events](#) or [View Defense+ Events](#).

## User Defined Filters:

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. The type of filters available for Firewall logs differ to those available for Defense+ logs. The table below provides a summary of available filters and their meanings:

Available Filters - Logs per Module		
Antivirus Filter	Firewall Filters	Defense+ Filters
<b>Action</b> - Displays events according to the response (or action taken) by the Antivirus	<b>Action</b> - Displays events according to the response (or action taken) by the firewall	<b>Application</b> - Displays only the events propagated by a specific application
<b>Location</b> - Displays only the events logged from a specific location	<b>Application</b> - Displays only the events propagated by a specific application	<b>Flags</b> - Displays events according to the response (or action taken) by Defense+
<b>Malware Name</b> - Displays only the events logged corresponding to a specific malware	<b>Destination IP</b> - Displays only the events with a specific target IP address	<b>Target</b> - Displays only the events that involved a specified target application
<b>Status</b> - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'	<b>Destination Port</b> - Displays only the events with a specific target port number	

Available Filters - Logs per Module		
	<b>Direction</b> - Indicates if the event was an Inbound or Outbound connection	
	<b>Protocol</b> - Displays only the events that involved a specific protocol	
	<b>Source IP</b> - Displays only the events that originated from a specific IP address	
	<b>Source Port</b> - Displays only the events that originated from a specific port number	

## Creating Custom Filters

Custom Filters can be created through the Advanced Filter Interface. You can open the Advanced Filter interface either by using the View option in the menu bar or using the context sensitive menu.

- Click View > Advanced Filter to open the 'Advanced Filter' configuration area.
- Or
- Right click on any event and select 'Advanced Filter' option to open the corresponding configuration area.

The 'Advanced Filter' configuration area is displayed in the top half of the interface whilst the lower half displays the Events, Alerts, Tasks or Configuration Changes that the user has selected from the upper left pane. If you wish to view and filter event logs for other modules then simply click log name in the tree on the upper left hand pane.

The Advanced Log filter displays different fields and options depending on the log type chosen from the left hand pane (Antivirus, Defense+, Firewall).

This section will deal with Advanced Event Filters related to 'Antivirus Events' and will also cover the custom filtering that can be applied to the 'Other Logs' (namely 'Alerts Displayed', 'Tasks' Launched' and 'Configuration Changes'). The Firewall and Defense+ Advanced Event Filters are dealt with in their respective sections.

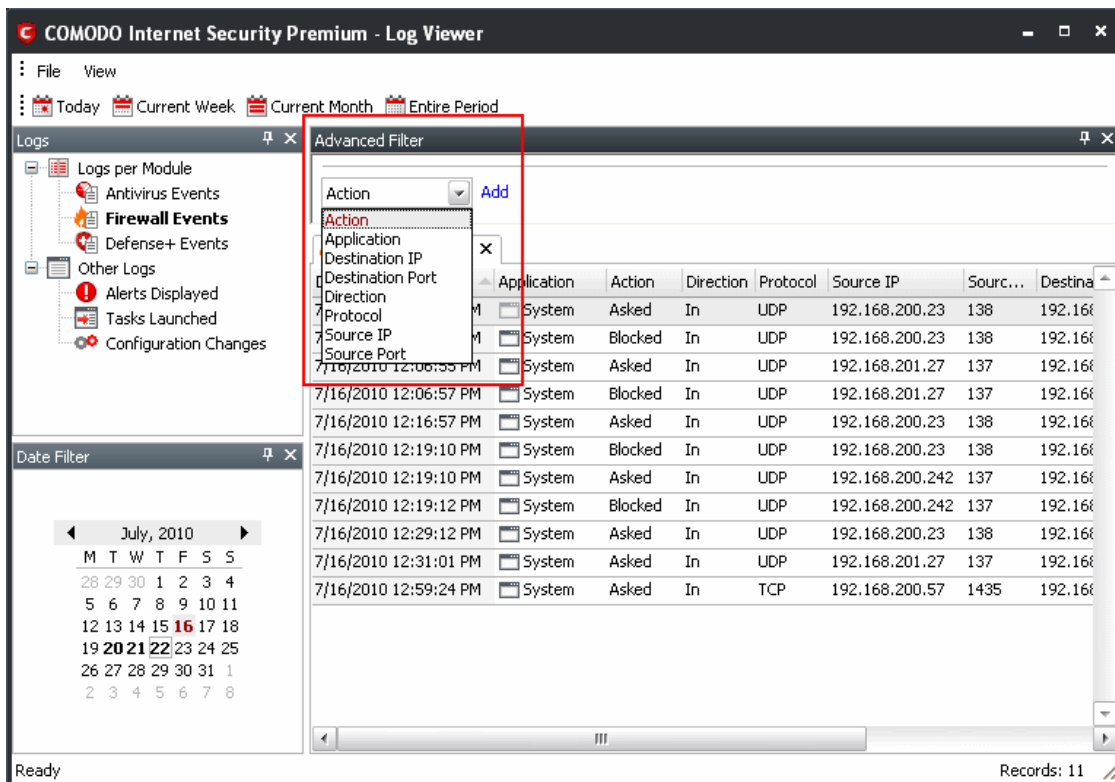
## Firewall Events - Advanced Filters

### To configure Advanced Filters for Firewall events

1. Select 'View > Advanced Filter'
2. Select 'Firewall Events' under 'Logs Per Module'

You have 8 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.

3. Click the 'Add' button when you have chosen the category upon which you wish to filter.



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

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

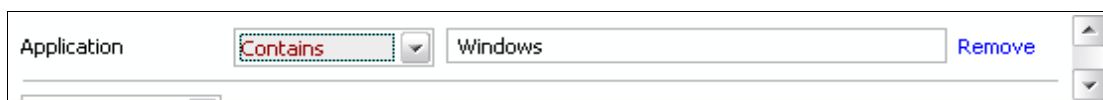


- a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
- b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

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

The filtered entries are shown directly underneath.

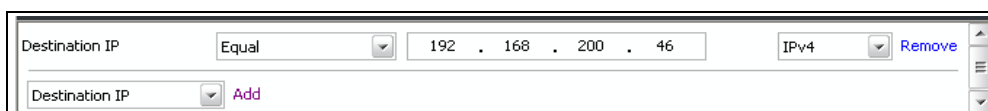
- ii. **Application:** Selecting the 'Application' option displays a drop-down box and text entry field.



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

The filtered entries are shown directly underneath.

- 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.

The filtered entries are shown directly underneath.

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.

The filtered entries are shown directly underneath.

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

The filtered entries are shown directly underneath.

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

The filtered entries are shown directly underneath.

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.

The filtered entries are shown directly underneath.

- 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.

The filtered entries are shown directly underneath.

**Note:** More than one filters can be added in the 'Advanced Filter' pane. After adding one filter type, the option to select the next filter type automatically appears. You can also remove a filter type by clicking the 'Remove' option at the end of every filter option.

## Other Logs - Advanced Filters

Refer to [Antivirus Tasks > View Antivirus Events > Log Viewer > Creating Custom Filters > Other Logs - Advanced Filters](#) for the process of Creating Custom Filters for Alerts Displayed, Task Launched and Configuration Changes.

## Date Filter

[Click here](#) to know more about Date Filter functionality.

## Exporting Log Files to HTML

Exporting log files is useful for archiving and troubleshooting purposes. There are two ways to export log files in the Log Viewer interface - using the context sensitive menu and via the 'File' menu option. After making your choice, you are asked to specify a name for the exported HTML file and the location you wish to save it to.

- i. **File Menu**
  1. Select the event for which the log report is to be taken.
  2. Click 'Export' from the File menu.
  3. Select the location where the log report has to be saved, provide a file name and click 'Save'.
- ii. **Context Sensitive Menu**
  1. Right click in the log display window to export the currently displayed log file to HTML.

You can export a custom view that you created using the available Filters by right clicking and selecting 'Export' from the context sensitive menu. You will be asked to provide a file name and save location for the file.

## 3.2 Define a New Trusted Application

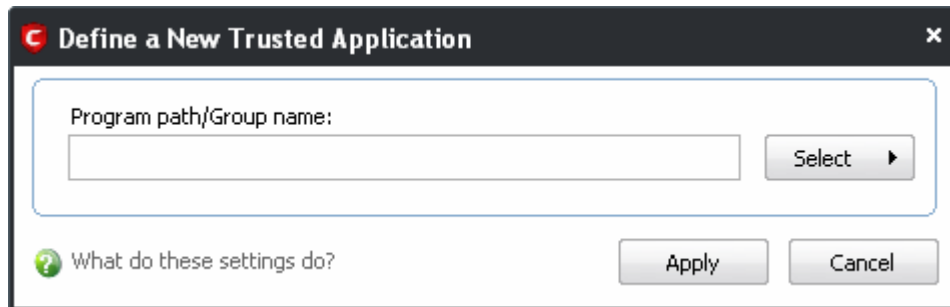
Comodo Firewall allows you to prepare a list of trusted applications and configure their access rights to networks and the

Internet. This shortcut represents a convenient way to create an automatic 'Allow Requests' rule for an individual application - meaning that inbound and outbound connections are automatically permitted.

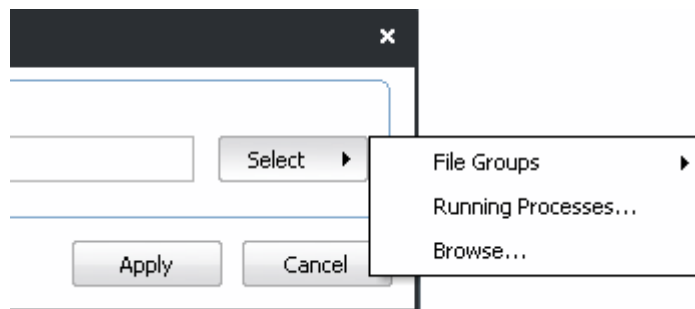
Advanced users can reconfigure the parameters of this rule in the section '[Network Security Policy](#)'.

### To begin defining a new trusted application

1. Click on 'Define a New Trusted Application' link in Firewall Tasks .
2. A dialog box appears prompting you to select the application you want to trust.



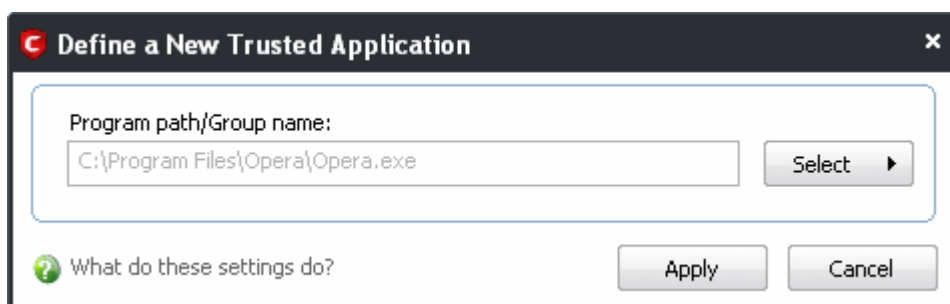
3. Click the 'Select' button.



4. You now have 3 methods available to choose the application that you want to trust - 'File Groups'; 'Running Processes' and 'Browse...'.
  - **File Groups** - Choosing this option allows you to choose your application from a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create an allow rule 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' and so on - each of which provide a fast and convenient way to batch select important files and folders.
  - **Running Processes** - as the name suggests, this option allows you to choose the target application from a list of processes that are currently running on your PC.
  - **Browse...** - this option is the easiest for most users and simply allows you to browse to the location of the application which you want to trust.

When you have chosen the application using one of the methods above, the application name appears along with its location:

5. Click 'Apply' to confirm your choice.



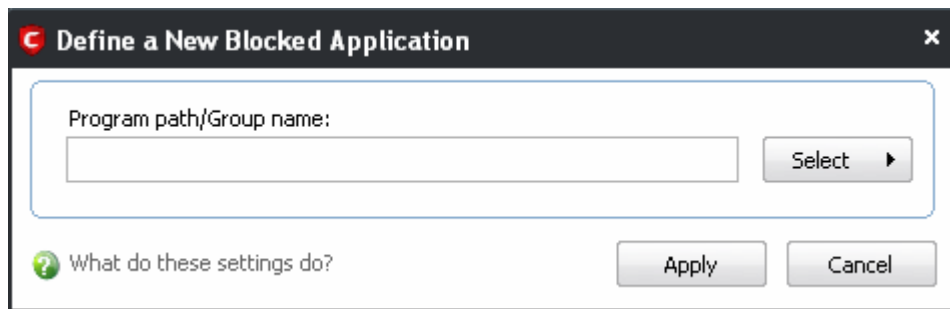
## 3.3 Define a New Blocked Application

Comodo Firewall allows you to prepare a list of blocked applications that you do not want to access the Internet. This shortcut represents a convenient way to create such an automatic 'block and log' rule - meaning that inbound and outbound connections are automatically blocked to this application. Any connection attempts by the application is also logged in the **View Firewall Events** interface.

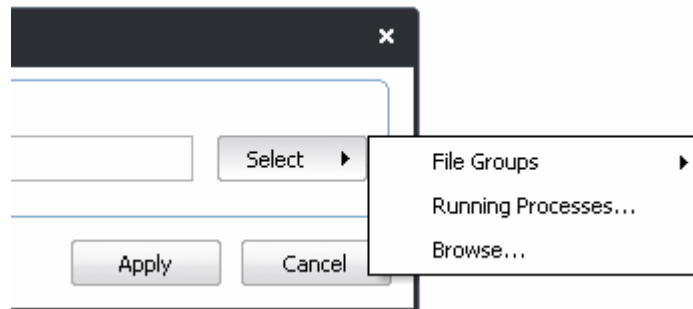
Advanced users can view and edit the parameters of this new rule in '**Network Security Policy**'. (for example, you later realize that a program really ought to be allowed some level of Internet access)

### To begin defining a new blocked application

1. Click the 'Define a New Blocked Application' link in Firewall Tasks.
2. A dialog box appears prompting you to select the application that you want to be blocked.

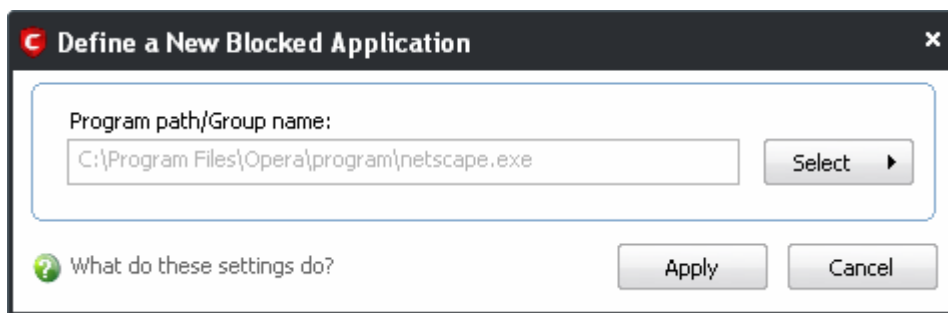


3. Click the 'Select' button:



4. You now have 3 methods available to choose the application that you want to block - 'File Groups'; 'Running Processes' and 'Browse...'.
  - **File Groups** - Choosing this option allows you to choose your application from a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a block rule 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' and so on - each of which provide a fast and convenient way to batch select important files and folders.
  - **Running Processes** - as the name suggests, this option allows you to choose the target application from a list of processes that are currently running on your PC.
  - **Browse...** - this option is the easiest for most users and simply allows you to browse to the location of the application which you want to block.
5. When you have chosen the application using one of the methods above, the application name appears along with its location:





6. Click 'Apply' to confirm your choice. The new block and log rule for the application takes effect immediately. When this application seeks Internet access, Comodo Internet Security automatically denies it and records an entry in the [View Firewall Events](#) interface.

## 3.4 Network Security Policy

The Network Security Policy interface 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.

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 Network Security Policy interface also allows users to define the Network Zones for specifying access privileges on them and Port Sets, which are predefined groupings of one or more ports of the system that can be deployed across multiple traffic filtering rules.

The interface is divided into six main sections - [Application Rules](#), [Global Rules](#), [Predefined Polices](#), [Network Zones](#), [Blocked Zones](#) and [Port Sets](#).

The **Application Rules** tab allows users to view, manage and define the network and Internet access rights of *applications* on your system.

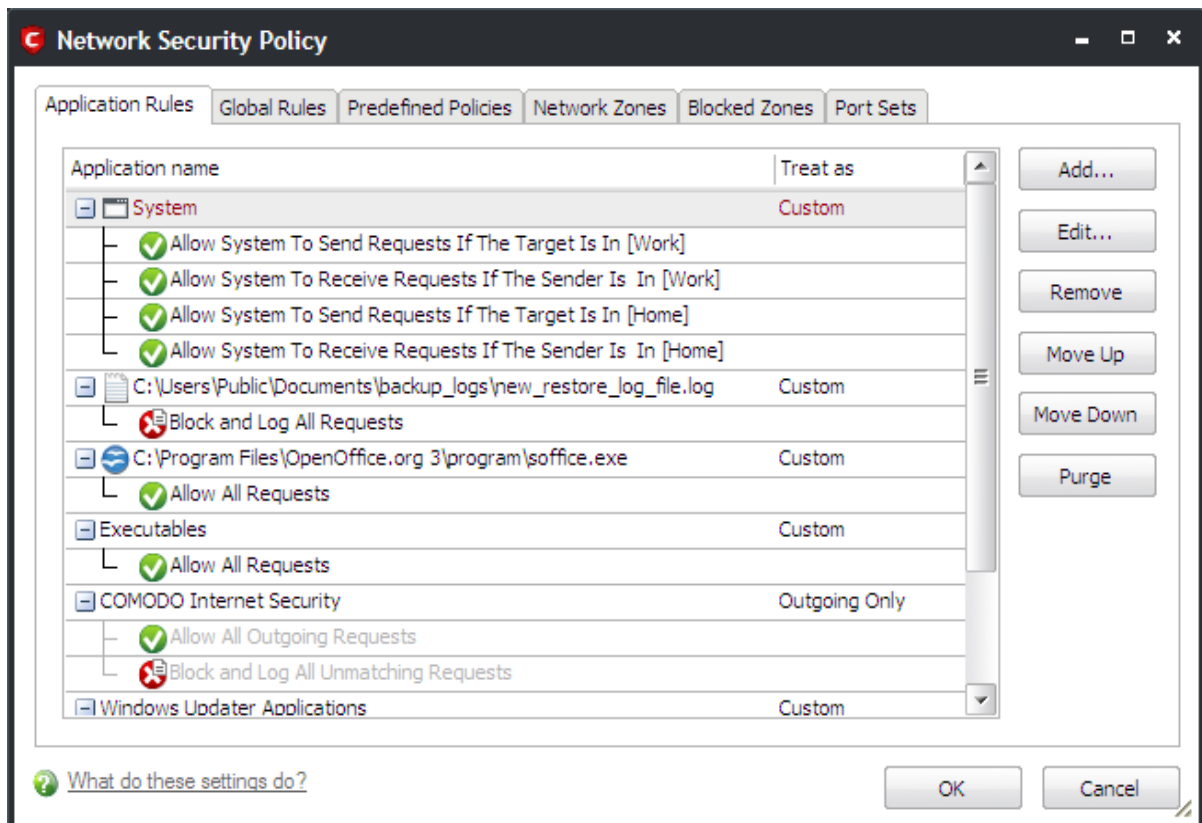
The **Global Rules** tab allows users view, manage and define overall network policy that applies to your computer and is independent of application rules.

The **Predefined Policies** tab allows users to view and manage a set of one or more individual network control rules that have been saved and can be re-used and deployed on multiple applications.

The **Network Zones** tab allows the users to define the network zones for applying access privileges for them.

The **Blocked Zones** tab allows the user the configure settings to allow only the desired and trusted networks.

The **Port Sets** tab allows the users to define groups of ports for deploying application specific and global rules.



- See [General Navigation](#) for a summary of the navigational options available from the Application Rules and Global Rules tabs of Network Security Policy interface.
- See the section '[Application Rules](#)' for help to configure application rules and policies.
- See the section '[Global Rules](#)' for help to configure global rules and to understand the interaction between global and application rules.
- See the section [Predefined Policies](#) for help to configure predefined firewall policies.
- See the section [Network Zones](#) for information and help on defining the network zones.
- See the section [Blocked Zones](#) for information and help of configuring the networks to be blocked from accessing your computer.
- See the section [Port Sets](#) for information and help on defining port groups.

### 3.4.1 General Navigation

- **Add...** - On the **Application Rules** tab this button allows the user to **Add a new Application to the list then create it's policy**. On the **Global Rules** tab it enables you to add and configure a new global rule using the **Network Control Rule interface**.
- **Edit...** - Allows the user to modify the selected rule or application policy. See [Overview of Policies and Rules, Creating and Modifying Network Policy](#) and [Understanding Network Control Rules](#)
- **Remove...** - Deletes the currently highlighted policy or rule
- **Move Up** - Raises the currently selected rule or policy up one row in the priority list. Users can also re-prioritize policies or re-assign individual rules to another application's policy by dragging and dropping.
- **Move Down** - Lowers the currently selected rule or policy down one row in the priority list. Users can also re-prioritize policies or re-assign individual rules to another application's policy by dragging and dropping.
- **Purge** - Runs a system check to verify that all the applications for which policies are listed are *actually installed* on the host machine at the path specified. If not, the policy is removed, or 'purged', from the list.

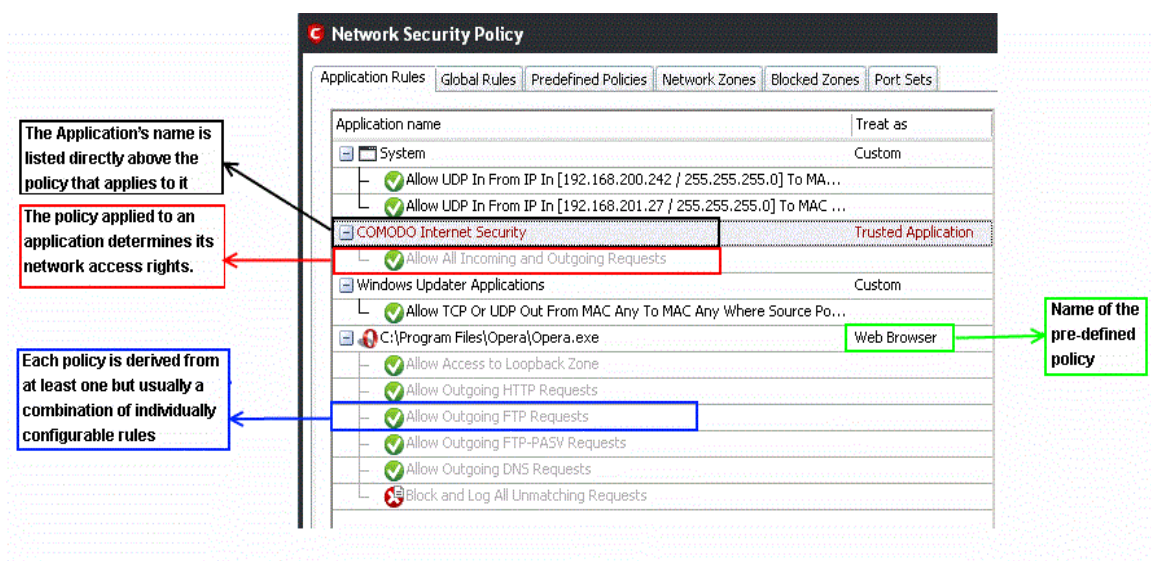
Users can re-order the priority of policies by simply dragging and dropping the rule in question. Alternatively, select the rule you wish to re-prioritize and click either the 'Move Up' or 'Move Down' button.

### 3.4.2 Application Rules

- See [Overview of Policies and Rules](#) for an explanation of rule and policy structure and how these are represented in the main Application Rules interface
- See [Application Network Access Control interface](#) for an introduction to the rule setting interface
- See [Creating and Modifying Network Policies](#) to learn how to create and edit network policies
- See [Understanding Network Control Rules](#) for an overview of the meaning, construction and importance of individual rules
- See [Adding and Editing a Network Control Rule](#) for an explanation of individual rule configuration

#### Overview of Policies and Rules

Whenever an application makes a request for Internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Policy that has been specified for that application. Firewall Policies 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.



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

- Double click on the application name to begin '[Creating or Modifying Network Policy](#)'
- Select the application name, right-click and choose 'Edit' to begin '[Creating or Modifying Network Policy](#)'
- Select the application name and click the 'Edit...' button on the right to begin '[Creating or Modifying Network Policy](#)'

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

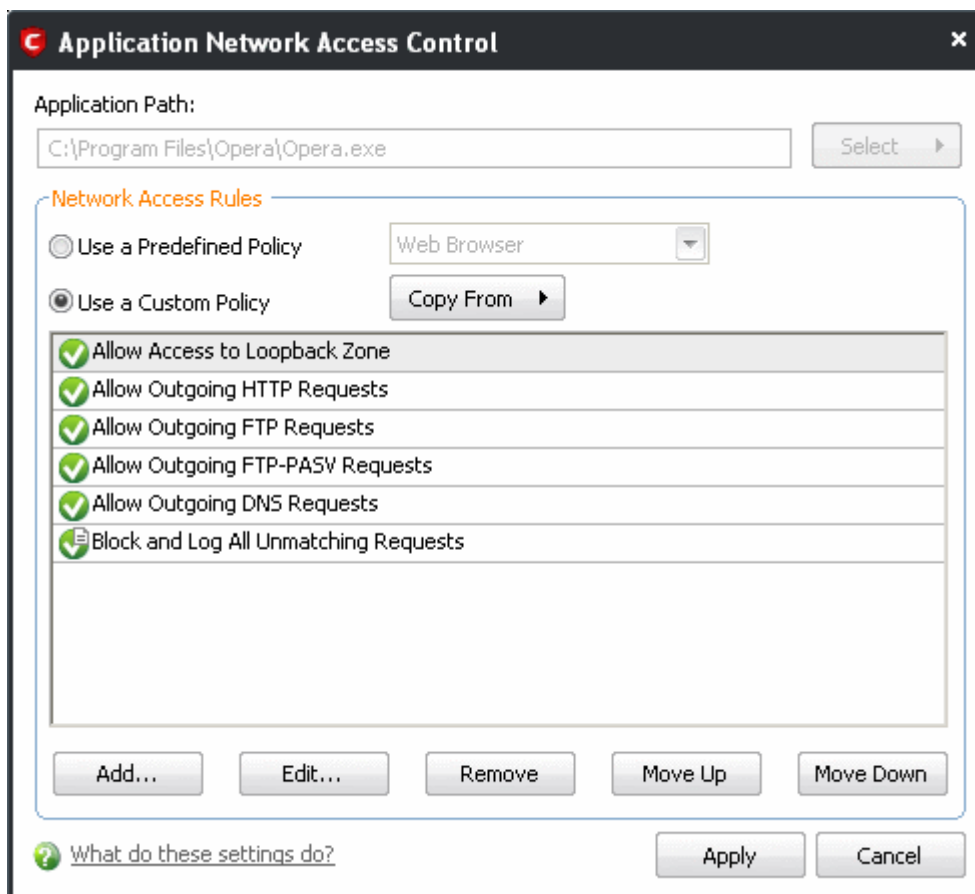
- Double click on the specific rule to begin '[Adding and Editing a Network Control Rule](#)'
- Select the specific rule right-click then choose 'Edit' to begin '[Adding and Editing a Network Control Rule](#)'
- Select the specific rule and click the 'Edit...' button on the right to begin '[Adding and Editing a Network Control Rule](#)'

Users can also re-prioritize policies or re-assign individual rules to another application's policy by dragging and dropping.

Although each policy 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 policies according to broad application category. For example, you may choose to apply the policy 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined policy 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 policies to suit their environment and requirements. For more details, see [Predefined Policies](#).

#### Application Network Access Control interface

Network control rules can be added/modified/removed and re-ordered through the Application Network Access Control interface. Any rules created using [Adding and Editing a Network Control Rule](#) is displayed in this list.



Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see [Understanding Network Control 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 re-order the priority of rules by simply dragging and dropping the rule in question. Alternatively, select the rule you wish to re-prioritize and click either the 'Move Up' or 'Move Down' button. To begin creating network policies, first read '[Overview of Policies and Rules](#)' then '[Creating and Modifying Network Policies](#)'

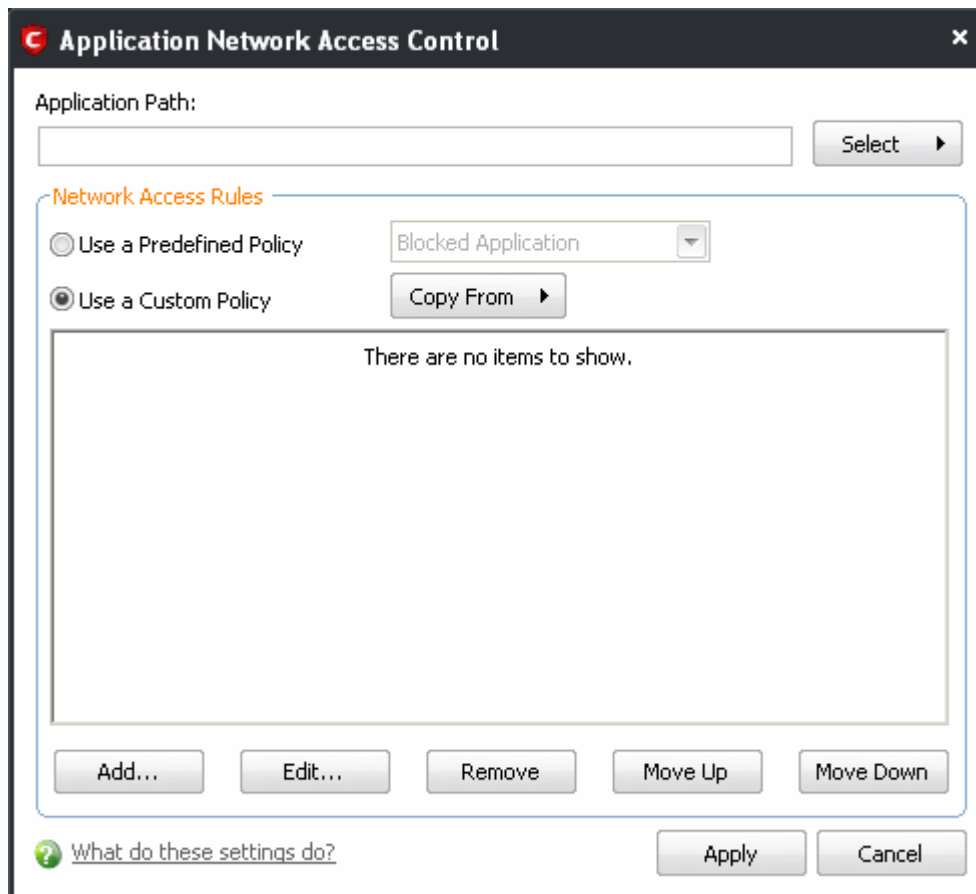
### Creating and Modifying Network Policies

To begin defining an application's network policy, you need take two basic steps.

1. **Select the application that you wish the policy to apply to.**
2. **Configure the rules for this application's policy.**

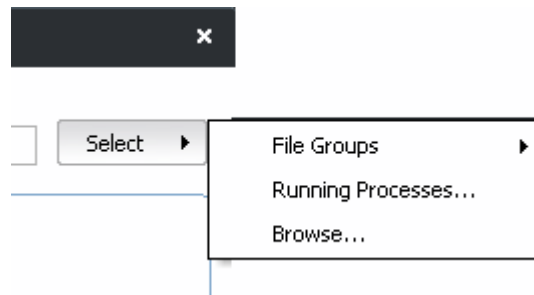
#### 1. Select the application that you wish the policy to apply to

If you wish to define a policy for a new application (i.e. one that is not already listed) then click the 'Add...' button in the main [application rules interface](#). This brings up the 'Application Network Access Control' interface shown below:



Because this is a new application, the 'Application Path' field is blank. (If you are modifying an existing policy, then this interface shows the individual rules for that application's policy).

Click 'Select' button.

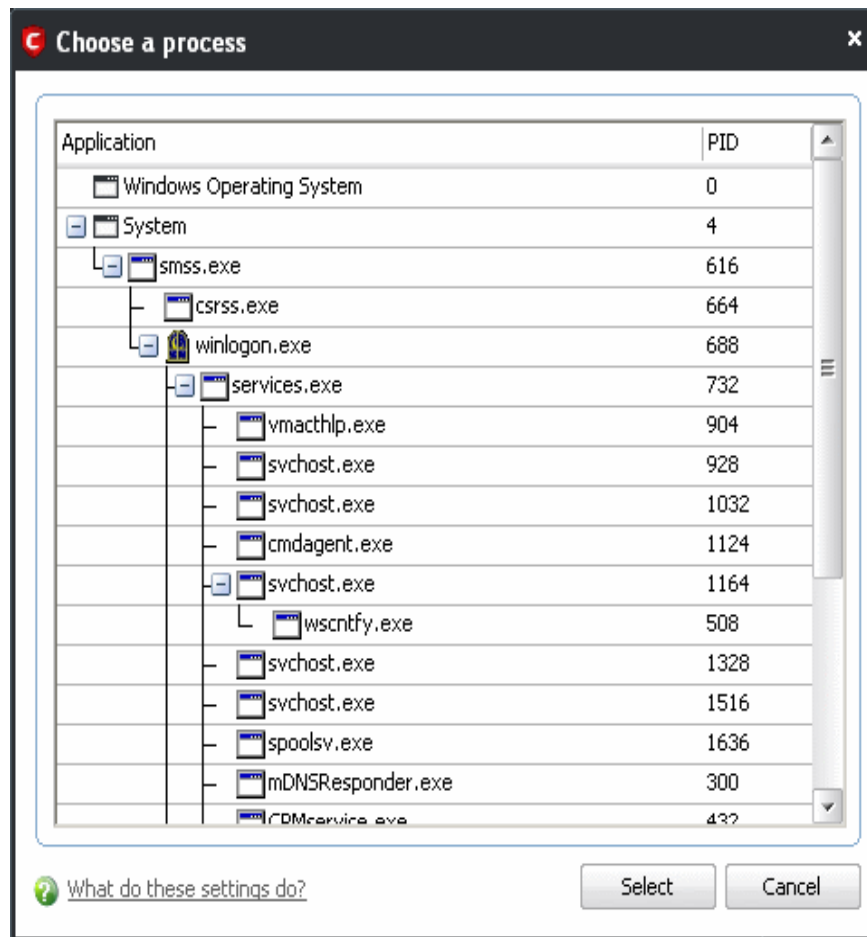


You now have 3 methods available to choose the application for which you wish to create a policy - **File Groups**; **Running Processes** and **Browse...**

- i. **File Groups** - choosing this option allows you to create firewall policy for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a firewall policy 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 policy 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 Defense+ area of Comodo Internet Security by navigating to: Defense+ > Protected Files and Folders> Groups...

More details on Files and File Groupings is available in this help guide in the **Protected Files and Folders** and **Blocked Files** sections.

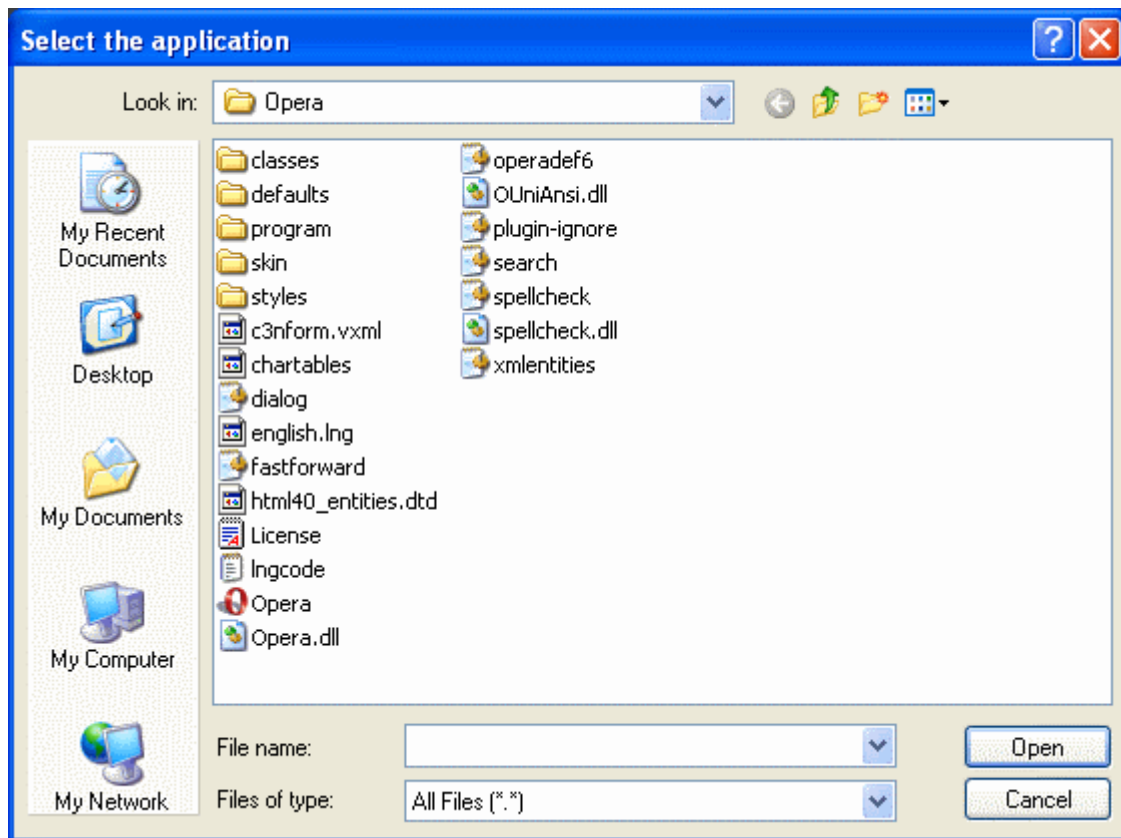
- ii. **Running Processes** - as the name suggests, this option allows you to create and deploy firewall policy for any process that is currently running on your PC.



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

**Note:** A more detailed and powerful 'View Active Process List' is available in the **Defense+ Tasks**.

- iii. **Browse...** - 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 policy. In the example below, we have decided to create a firewall policy for the Opera web browser.



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

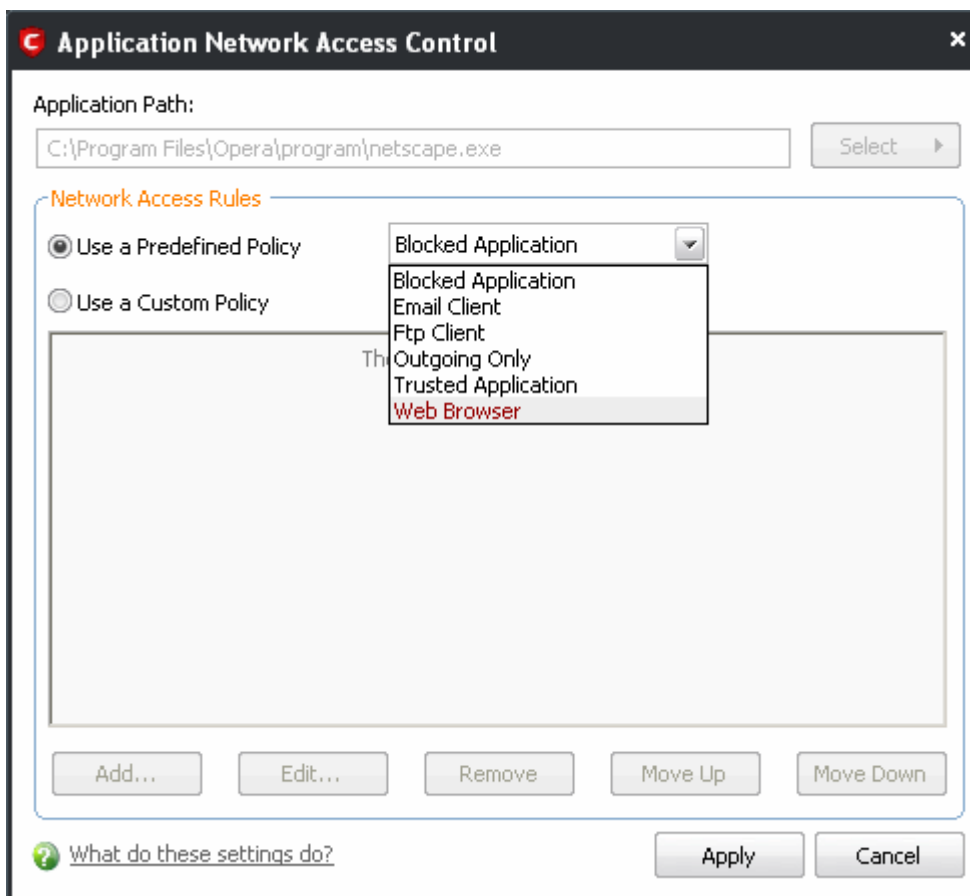
## (2) Configure the rules for this application's policy

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

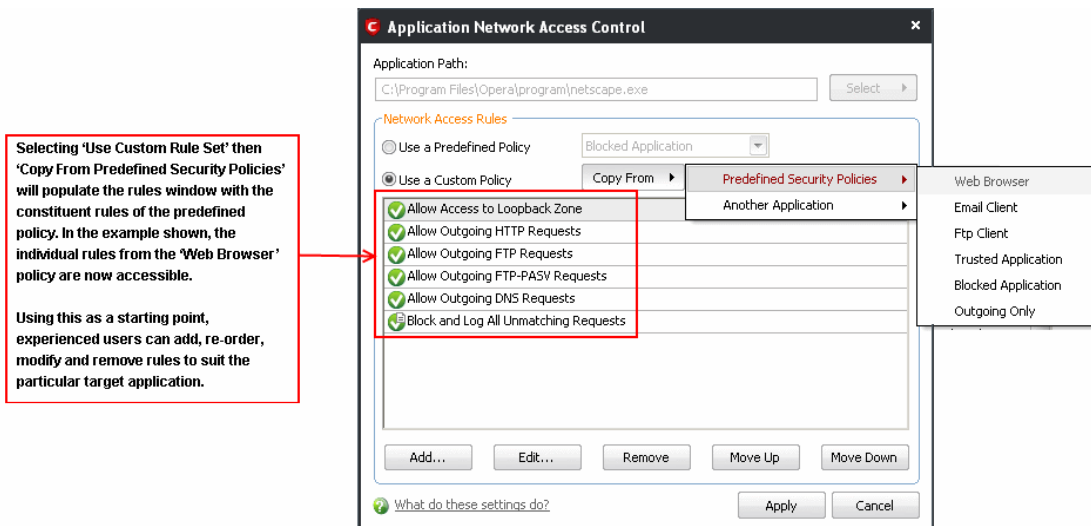
- **Use a Predefined Policy** - Selecting this option allows the user to quickly deploy a existing policy on to the target application. Choose the policy you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a policy for the 'Opera' browser.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

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





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



You can create an entirely new policy or use a predefined policy as a starting point by:

- Clicking the 'Add...' button to add individual network control rules. See '**Adding and Editing a Network Control Rule**' for an overview of the process.
- Use the 'Copy From' button to populate the list with the network control rules of a **Predefined Firewall Policy**.
- Use the 'Copy From' button to populate the list with the network control rules of another application's policy.

**General Tips:**

- If you wish to create a reusable policy for deployment on multiple applications, we advise you add a new **Predefined Firewall Policy** (or modify one of the existing ones to suit your needs) - then come back to this

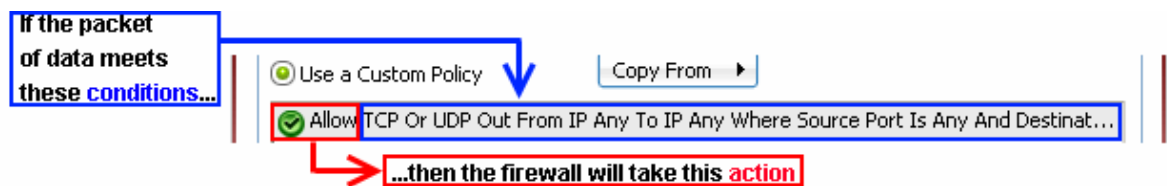
section and use the 'Use Predefined Policy' option to roll it out.

- If you want to build a bespoke policy for maybe one or two specific applications, then we advise you choose the 'Use a Custom Policy' option and create your policy either from scratch by adding individual rules (click the 'Add...' button) or by using one of the built-in policies as a starting point.

## Understanding Network Control Rules

At their core, each network control rule can be thought of as a simple **IF THEN** trigger - a set of **conditions** (or attributes) pertaining to a packet of data from a particular application and an **action** 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 network control 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 network control rule, then the connection is automatically blocked until a rule is created.



The actual **conditions** (attributes) you see\* on a particular Network Control Rule are determined by the protocol chosen in **Adding and Editing a Network Control 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 Network Control 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 Network Control 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 Network Control 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 Network Control Rule

The **Network Control Rule** Interface is used to configure the actions and conditions of an individual network control 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 Network Control Rules'](#), ['Overview of Rules and Policies'](#) and ['Creating and Modifying Network Policies'](#)

### 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*).

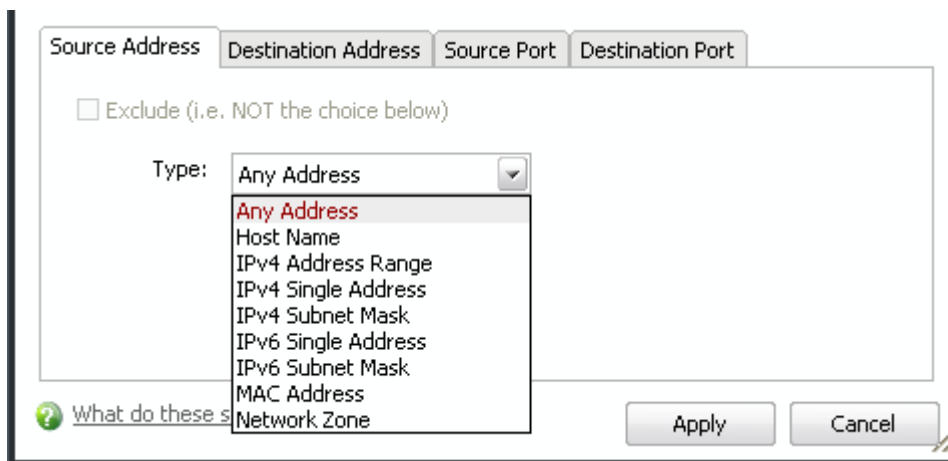
**Log as a firewall event if this rule is fired:** Checking this option creates an entry in the [firewall event log viewer](#) whenever this rule is called into operation. (i.e. when ALL conditions have been met) (*Default = Disabled*).

**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 Network Access Control](#) interface.

### Protocol

- i. TCP', 'UPD' or 'TCP or UDP'

If you select 'TCP', 'UPD' or 'TCP or UDP' as the Protocol for your network, then you have to define the source and destination IP addresses and ports receiving and sending the information.

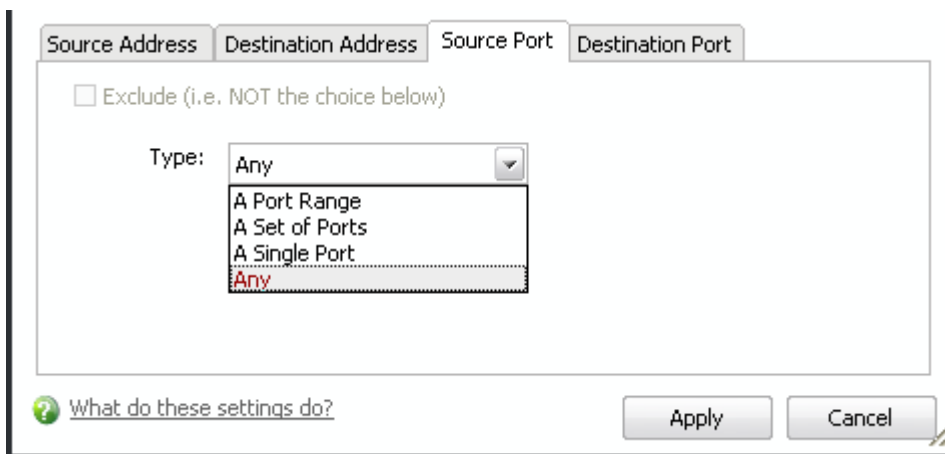


#### Source Address and Destination Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
  2. You can choose a named host by selecting a Host Name which denotes your IP address.
  3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
  4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
  5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
  6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
  7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
  8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.
  9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.
- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

#### Source Port and Destination Port:

Enter the source and destination Port in the text box.



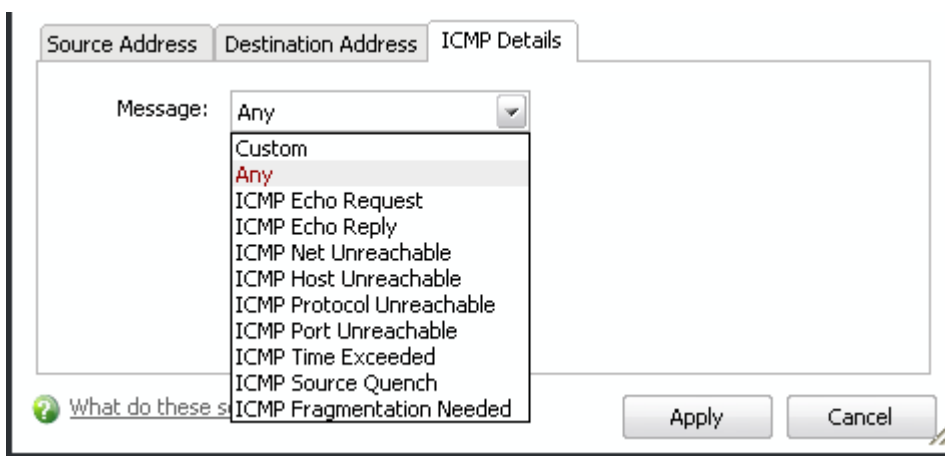
1. You can choose any port number by selecting Any - set by default , 0- 65535.
2. You can choose a Single Port number by selecting Single Port and selecting the single port numbers from the list.
3. You can choose a Port Range by selecting Port Range and selecting the port numbers from the From and To list.
4. You can choose a predefined **Port Set** by choosing A Set of Ports. If you wish to create a 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.

#### iii. 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.

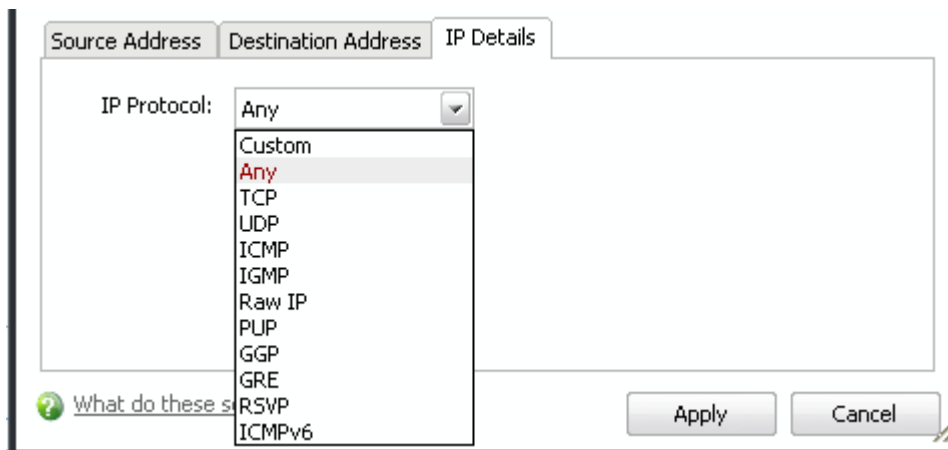


1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.
2. Specify ICMP Message , Types and Codes. An ICMP message includes a Message that specifies the 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.

## 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.

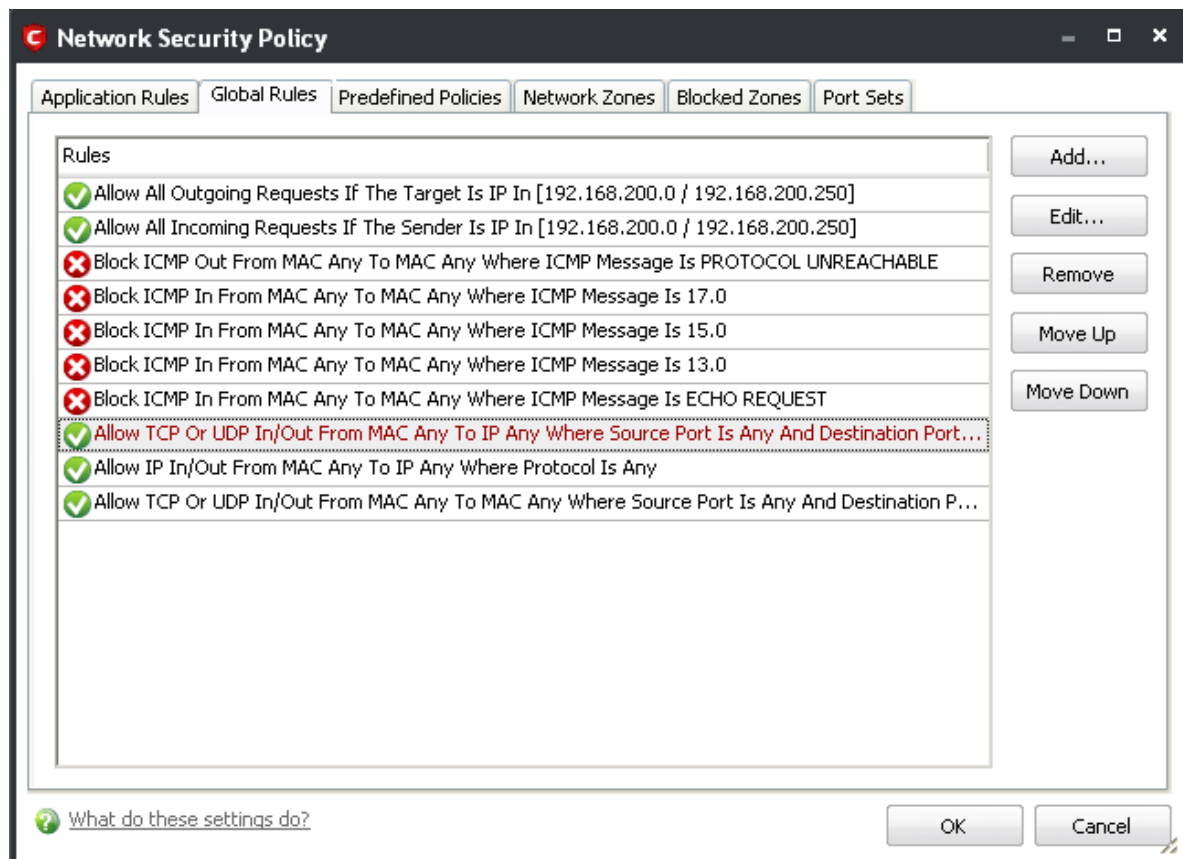


### iv. IP Details

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

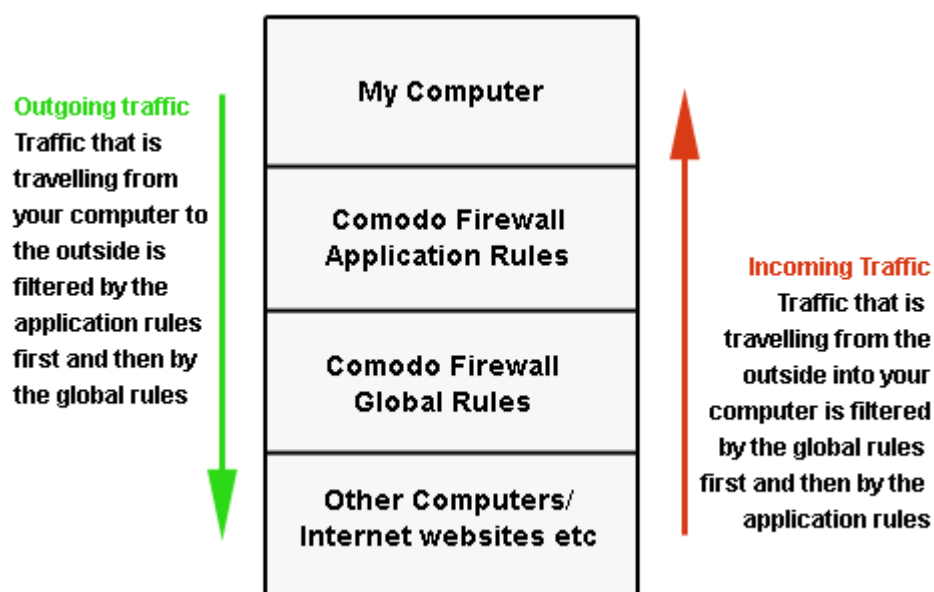
## 3.4.3 Global Rules

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 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 Network Access Control interface](#) for an introduction to the rule setting interface.

See [Understanding Network Control Rules](#) for an overview of the meaning, construction and importance of individual rules.

See [Adding and Editing a Network Control Rule](#) for an explanation of individual rule configuration.

### 3.4.4 Predefined Policies

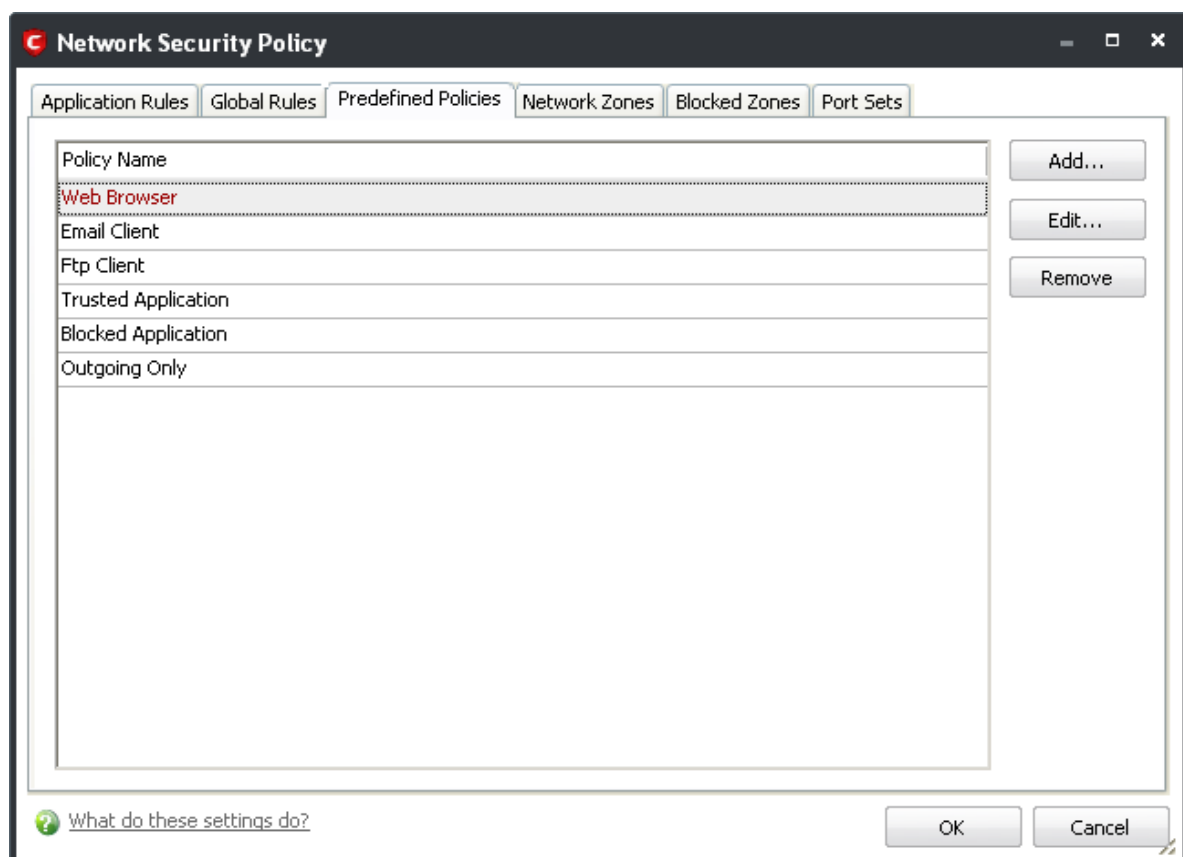
As the name suggests, a predefined firewall policy is a set of one or more individual network control rules that have been saved and can be re-used and deployed on multiple applications.

**Note:** This section is for advanced and experienced users. If you are a novice user or are new to Comodo Firewall, we advise you first read the explanations for [Network Security Policies](#), if you have not already done so.

Although each application's firewall policy *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 policies according to broad application category. For example, you may choose to apply the policy 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined policy 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)

#### To access the Predefined Policies interface

1. Click 'Predefined Policies' tab from Firewall Tasks > Network Security Policy interface.

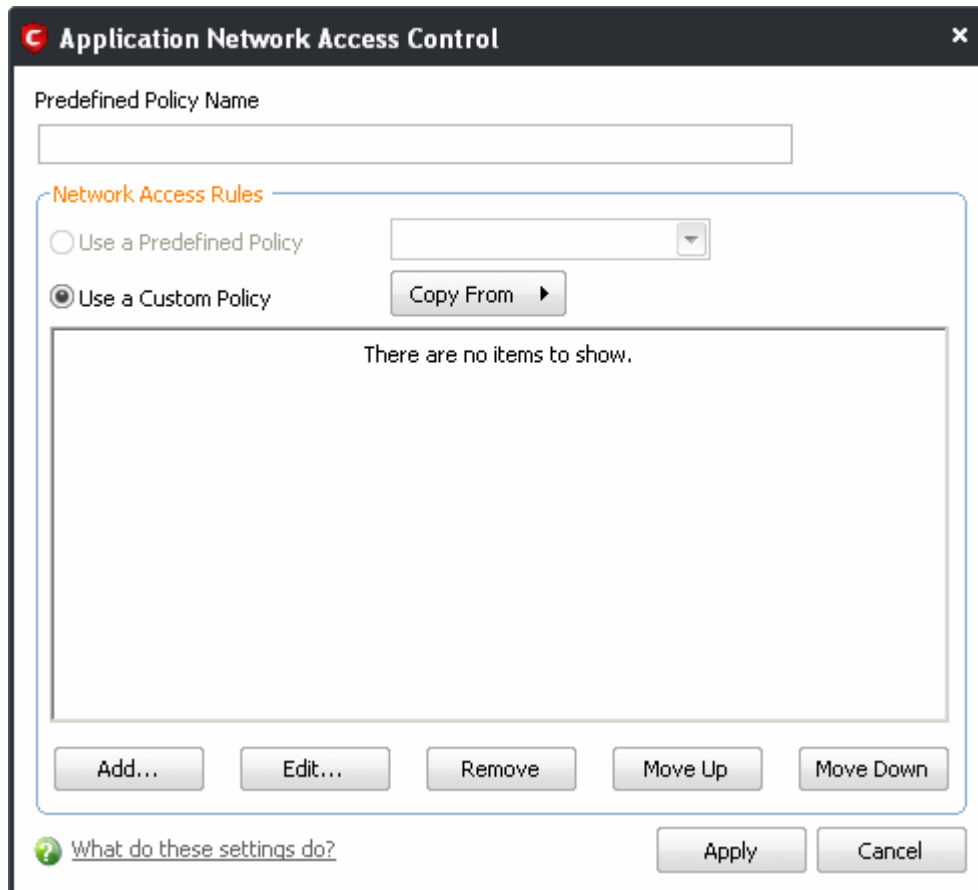


### To view or edit an existing predefined policy

- Double click on the Policy Name in the list
- Select the Policy Name in the list, right-click and choose 'Edit'
- Select the Policy Name and click the 'Edit...' button on the right
- Details of the process from this point on can be found [here](#).

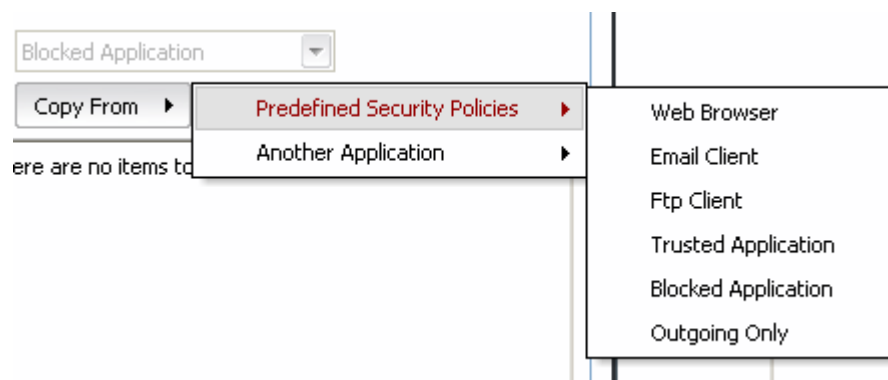
### To add a new predefined policy

- Click the 'Add...' button. This launches the policy creation dialog shown below.



- As this is a new predefined policy, 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 policy for. Next you should add and configure the individual rules for this policy. See '[Adding and Editing a Network Control Rule](#)' for more advice on this.

Once created, this policy can be quickly called as a 'Predefined Policy' when [creating or modifying a network policy](#).



## 3.4.5 Network Zones

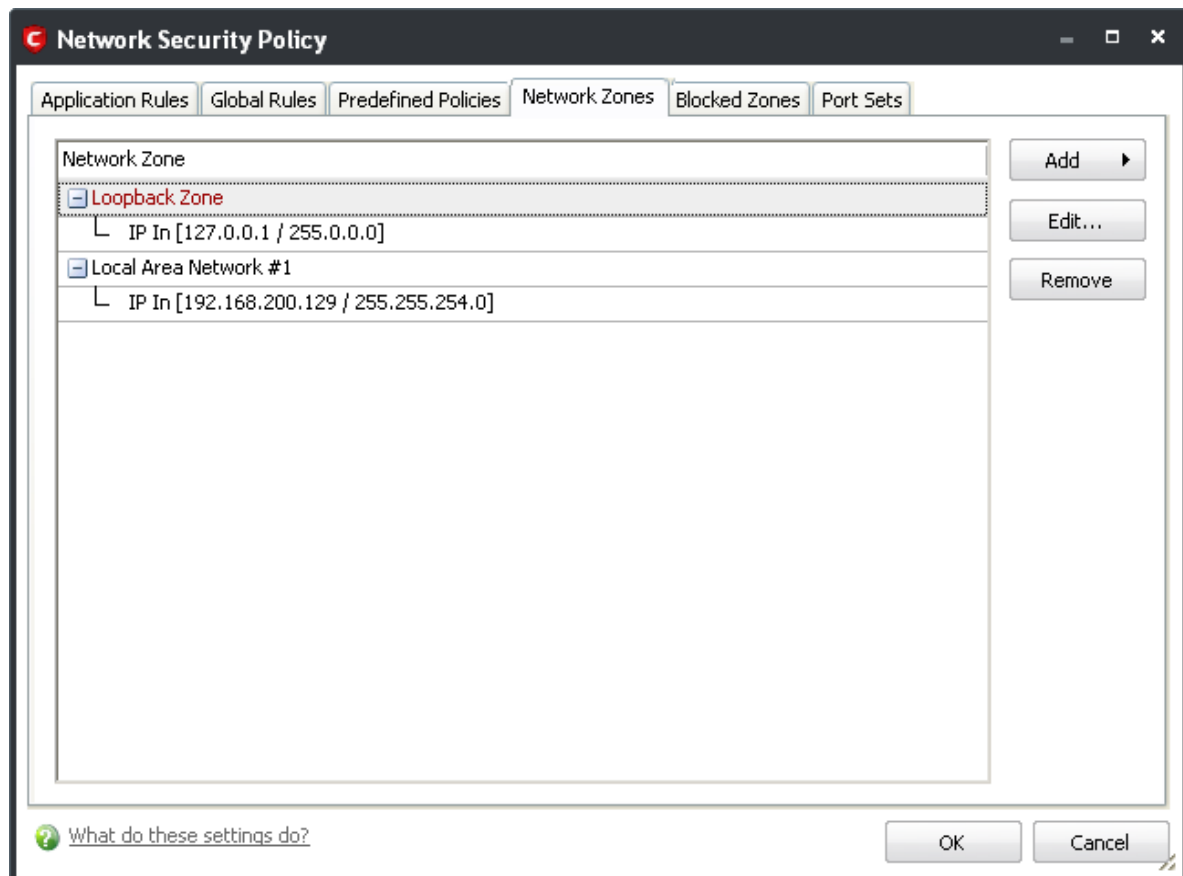
Comodo Firewall allows you to define 'Network Zones' and to specify the access privileges of these zones. A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a network of

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.

## To access the Network Zones interface

- Click 'Network Zones' tab from Firewall Tasks > Network Security Policy interface.



**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 by using the '**Stealth Ports Wizard**' (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). This can be disabled in the **More > Preferences** area of the application.

## To add a New Network Zone

1. **Define a name for the zone.**
2. **Select the addresses to be included in this zone.**

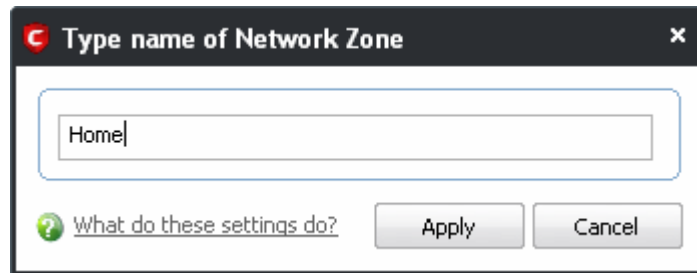
## To define a name for the zone

1. Click 'Add...' button and select 'A New Network Zone...'



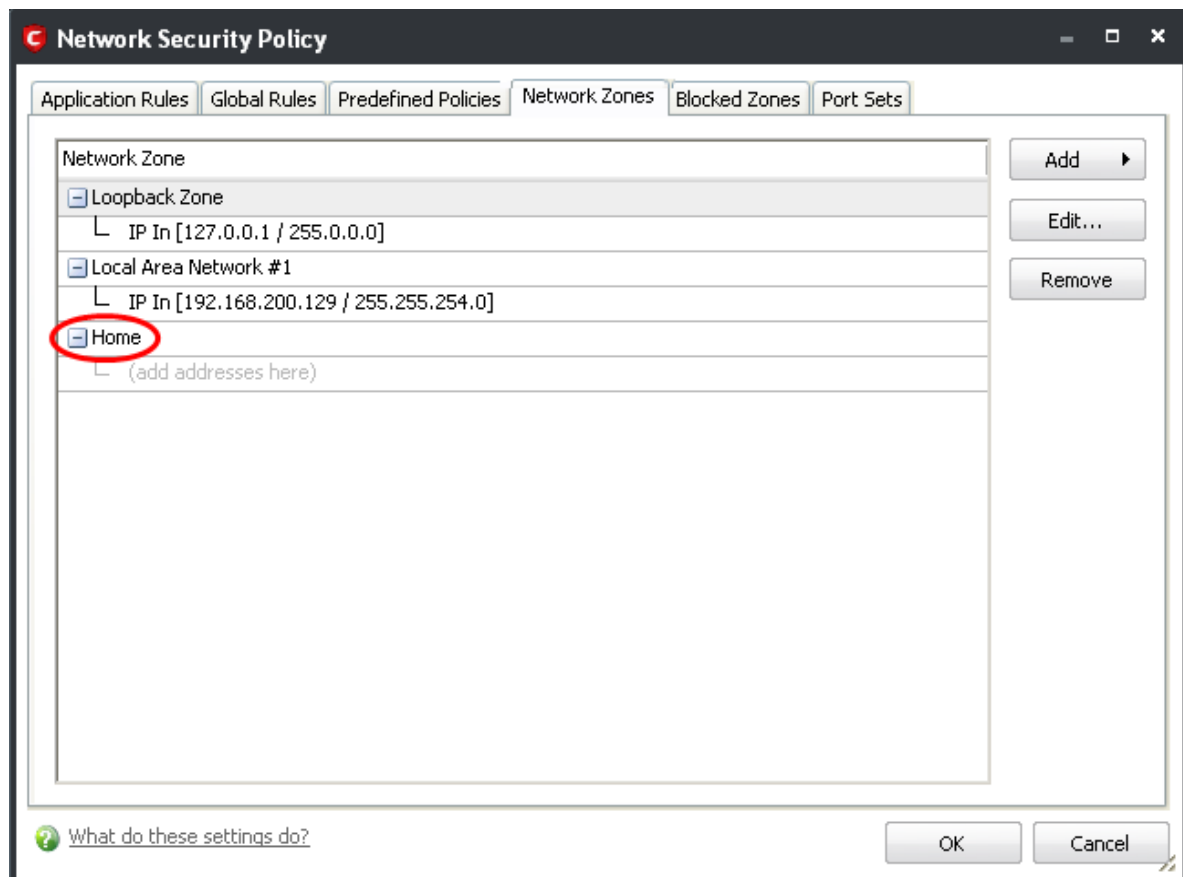
A dialog box will appear, prompting you to specify a name for the new zone.

2. Choose a name that accurately describes the network you are creating.



3. Click 'Apply' to confirm your zone name.

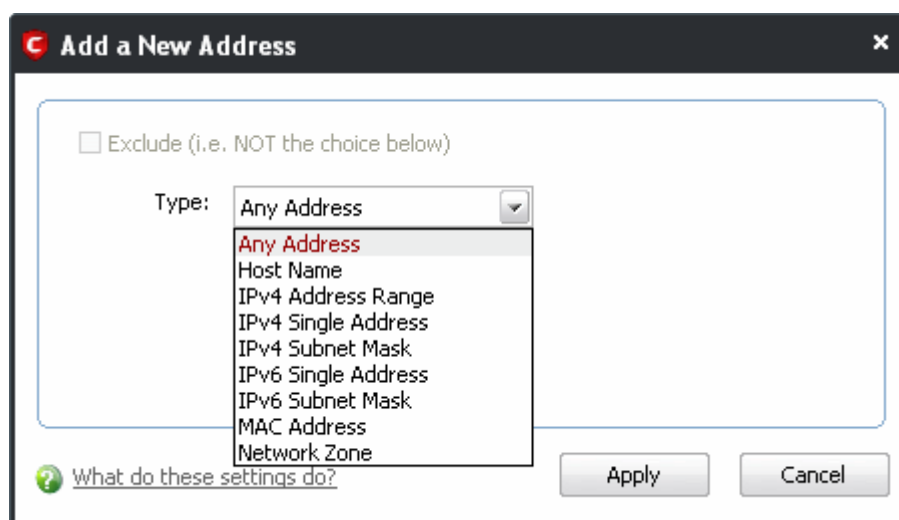
This adds the name of your new zone to the Network Zones list.



### To select the addresses to be included in this zone

1. Select the network name, right click on the name of the new zone and select 'Add...' from the menu.

The 'Add a New 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.

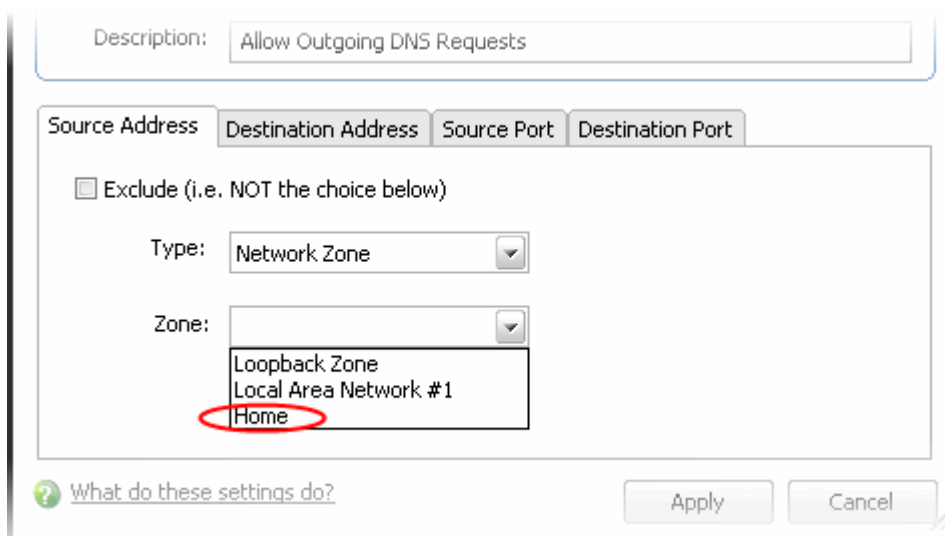


2. Click 'Apply' to confirm your choice.
3. Click 'OK' in the 'Network Zones' interface.

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 network policy**



- Quickly called and designated as a trusted zone from the '**Network Zones**' interface
- 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. Home).
2. Select 'Edit...' to bring up the naming dialog.

### To add more addresses to an existing Network Zone

- Right click on the zone name and click 'Add...' or,
- Select the zone name and click the 'Add...' button on the right and select 'A New Address...' from the drop-down menu.

### To modify or change the existing address in a zone

- Right click on the address (not the zone name) and select 'Edit...' or
- Select the actual address (not the zone name) and click the 'Edit...' button on the right.

### 3.4.6 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.

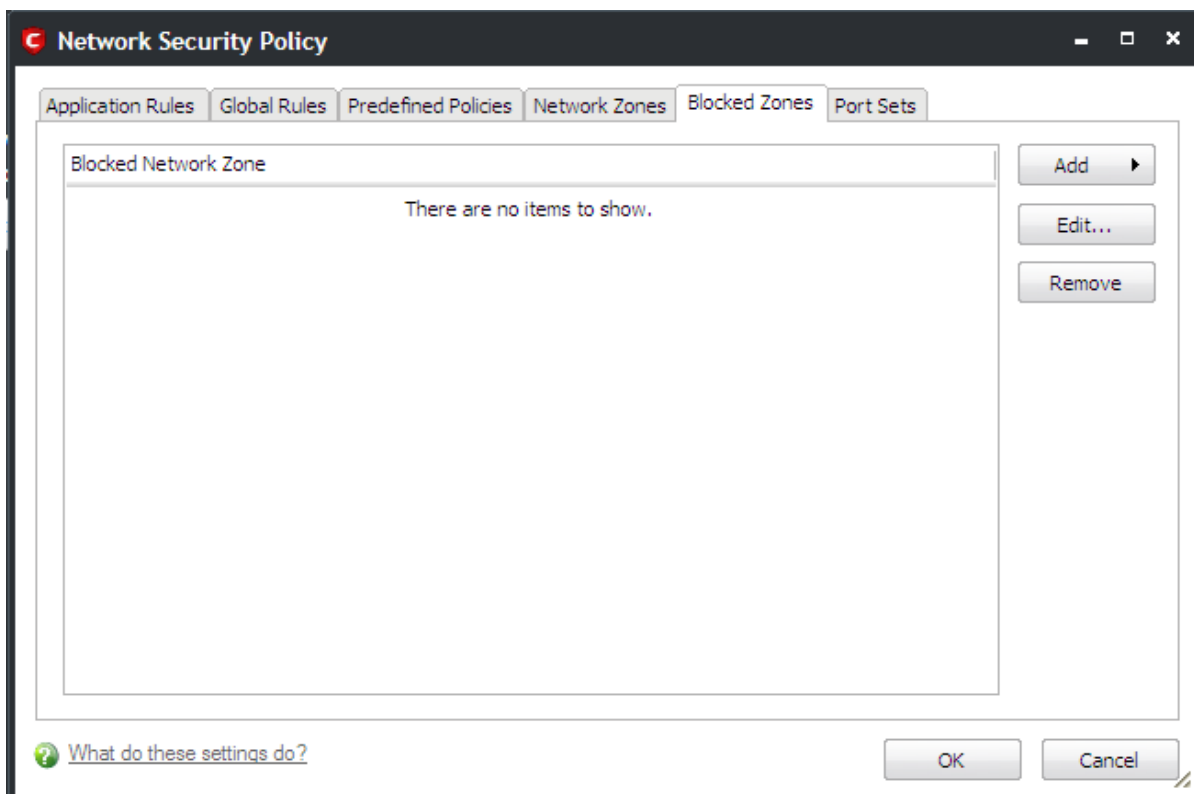
**Note:** We advise new or inexperienced users to first read '[Network Zones](#)', '[Stealth Ports Wizard](#)' and '[Network Security Policy](#)' before blocking zones using this interface.

The 'My Blocked Network Zones' area 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

#### To access the Blocked Zones interface

- Click 'Blocked Zones' tab from Firewall Tasks > Network Security Policy interface.



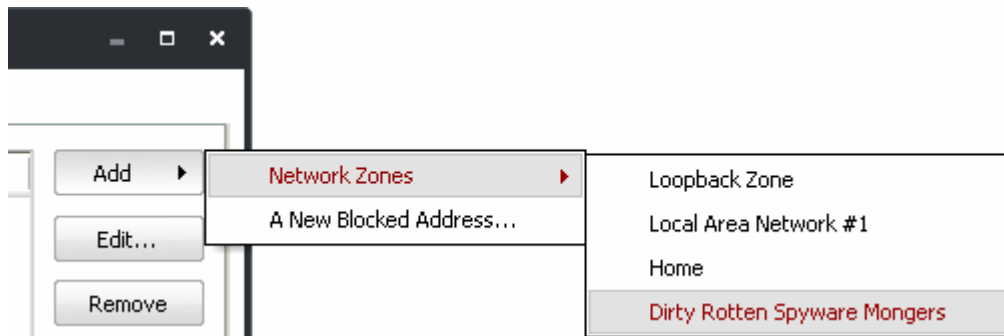
**Note 1:** You must create a zone before you can block it. There are two ways to do this;

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

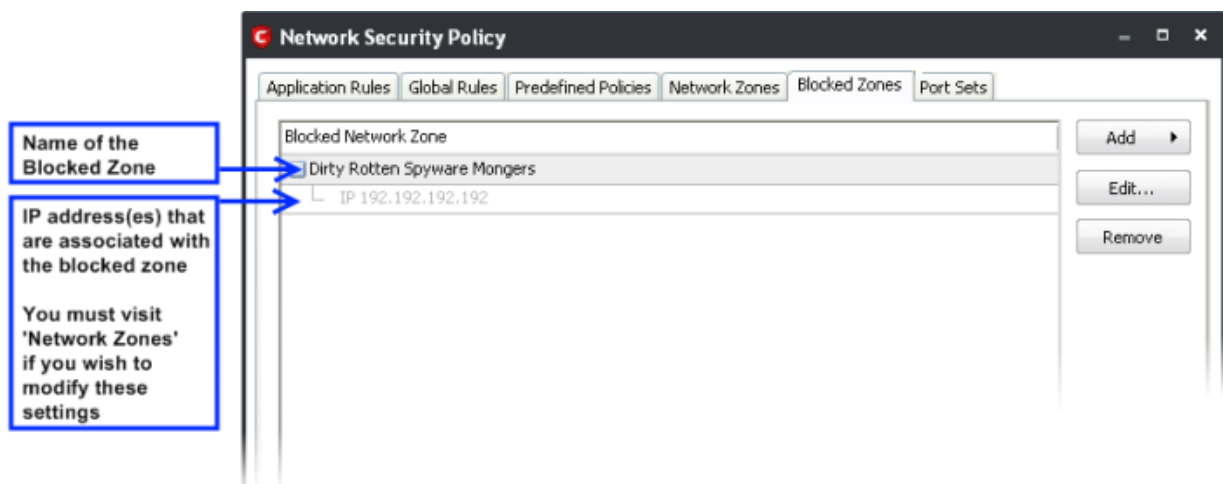
**Note 2:** You cannot reconfigure *pre-existing* network zones from this interface. (e.g., to add or modify IP addresses). You need to use 'My Network Zones' if you want to change the settings of existing zones.

#### To deny access to a specific network by selecting a pre-existing network zone and designating it as blocked

1. Click the 'Add' button at the top right and select 'Network Zones' then the particular zone you wish to block.



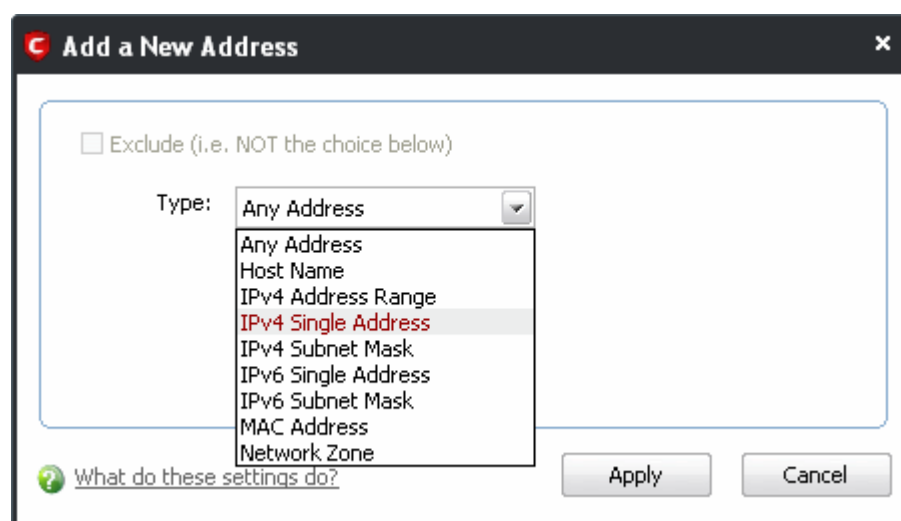
The selected zone appears in the main interface.



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

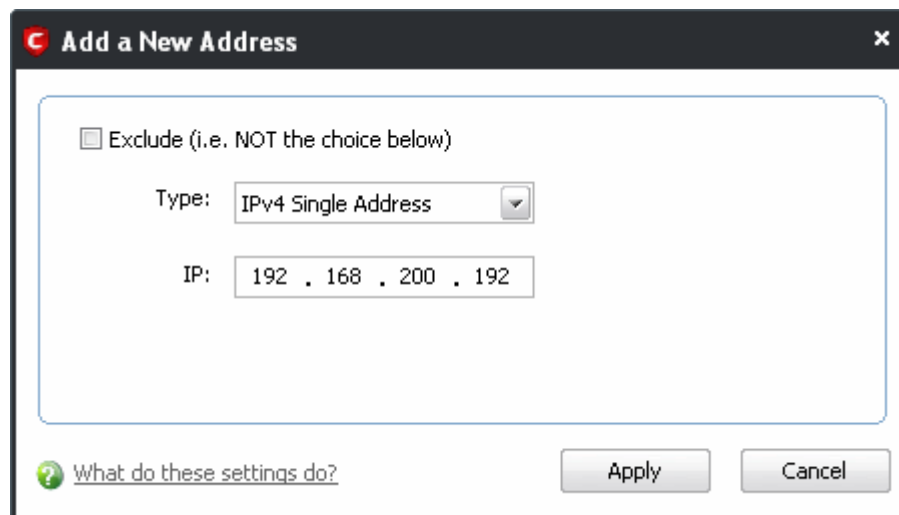
## To deny access to a specific network by manually defining a new blocked zone

1. Click the 'Add' button at the top right and select 'A New Blocked Address' (*Default = Any Address*). The Exclude check box will be enabled only if any other choice is selected from the drop-down box. This launches the following dialog where you can select the IP address(es), IP Subnet Masks, Host Name or MAC address that you wish to block from the Type drop-down box.

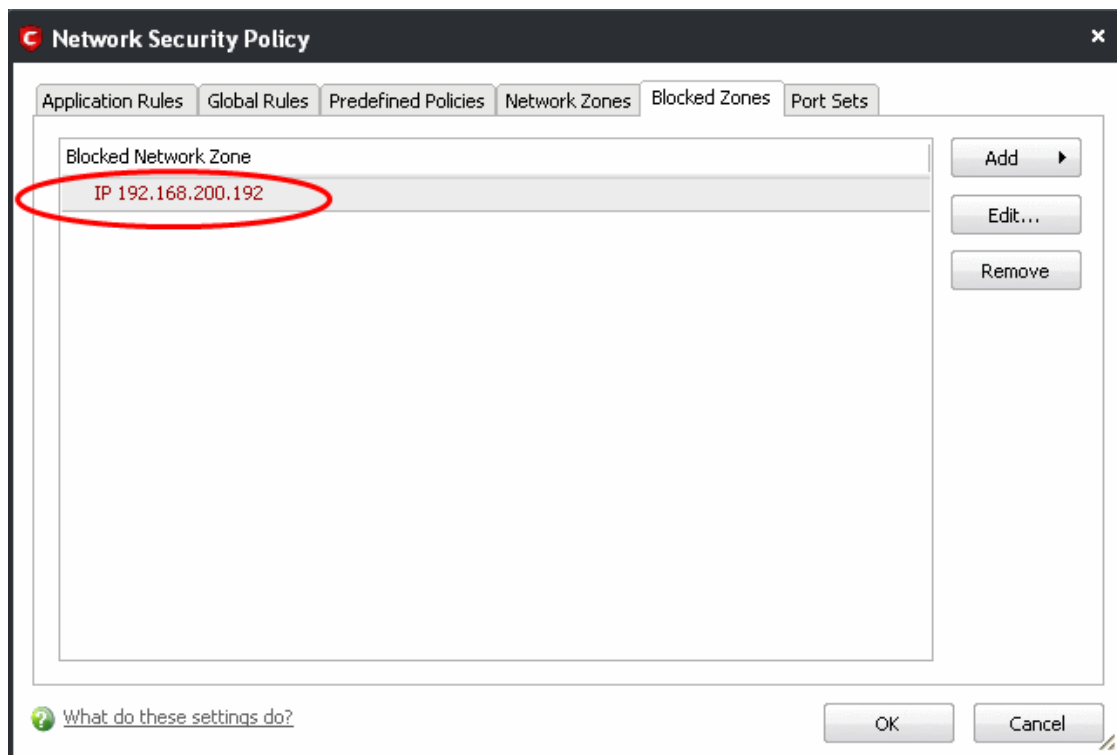


2. Enter the IP address that you wish to block.





After clicking 'Apply' to confirm your choice, the address(es) you blocked appears in the main interface. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.



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

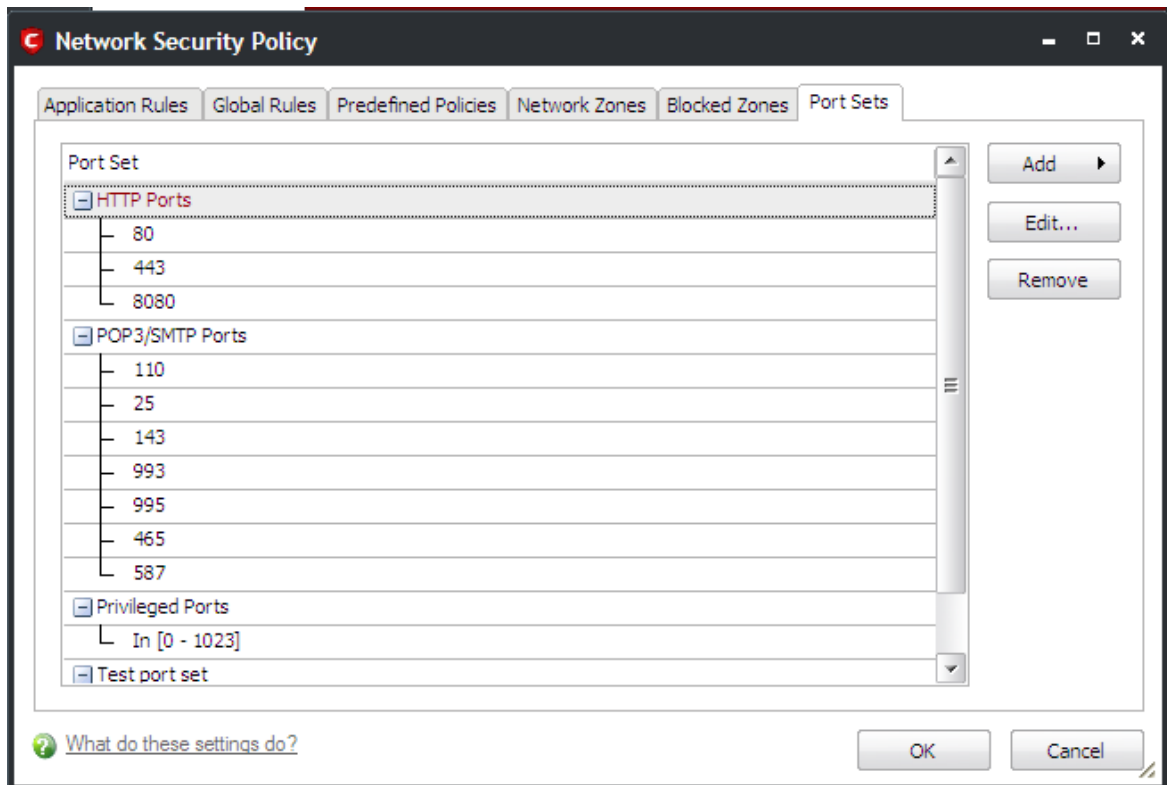
**Special Note:** Creating a blocked network zone implements a 'block all' **global rule** for the zone in question. However, unlike when you create a 'Trusted Zone', this rule is not displayed or editable from the global rules tab of the Network Security Policy interface. This is because you are likely to be trusting only a few zones, there is the potential that you may have to block many. The constant addition of such block rules would make the interface unmanageable for most users.

### 3.4.7 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**.

## To access the 'Port Sets' interface

1. Click 'My Port Sets' tab from Firewall Tasks > Network Security Policy interface.



The name of the port set is shown above the actual port numbers that belong to that set. The default port sets shipped with Comodo Internet Security:

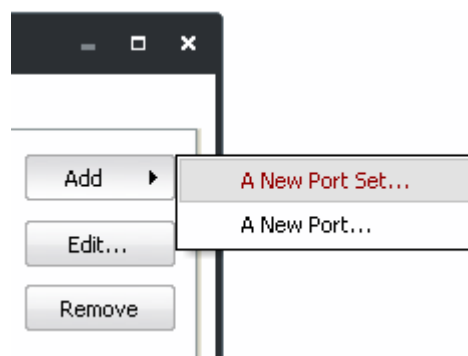
- **HTTP Ports:** 80 and 443. These are the default ports for http traffic. Your Internet browser uses these ports to connect to the Internet and other networks.
- **POP3/SMTP Ports:** 110, 25, 143, 995, 465. These are the ports that are typically used by mail clients like Outlook Express and WinMail for communication using the POP3, SMTP and IMAP protocols.
- **Privileged Ports:** 0-1024. This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1024. 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.

## To add a new port set

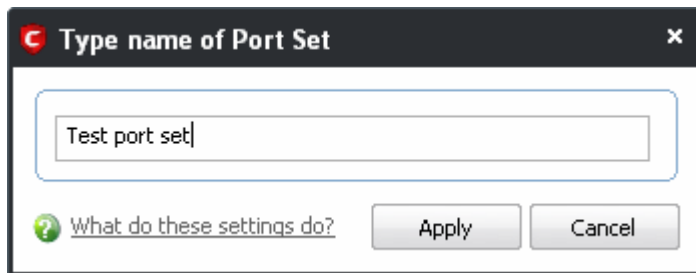
1. **Define a name for the set.**
2. **Select the port numbers you want to belong to this named set.**

## To define a name for the set

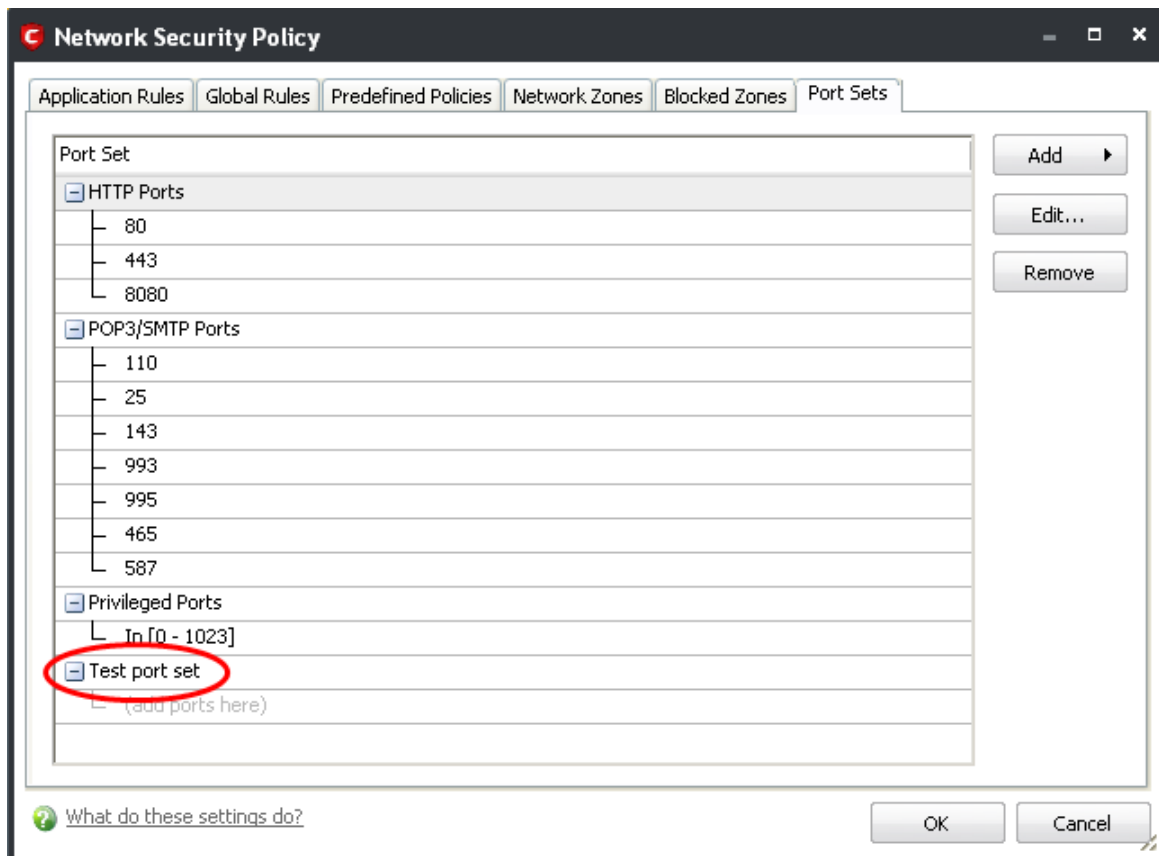
1. Click the 'Add' button on the right hand side and select 'A New Port Set...'



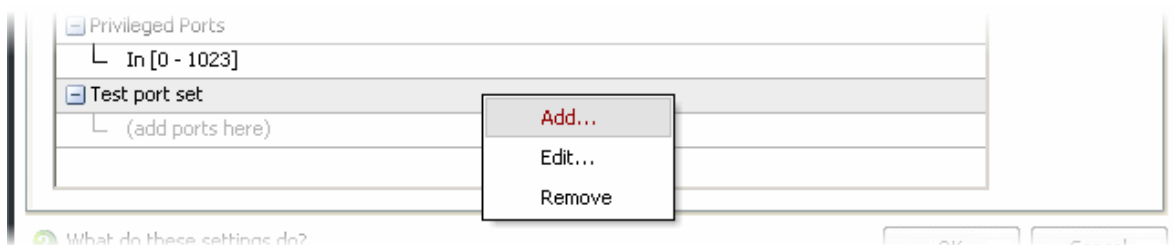
2. Type a name for the port set. In the example below, we have chosen to name our port set A test port set.



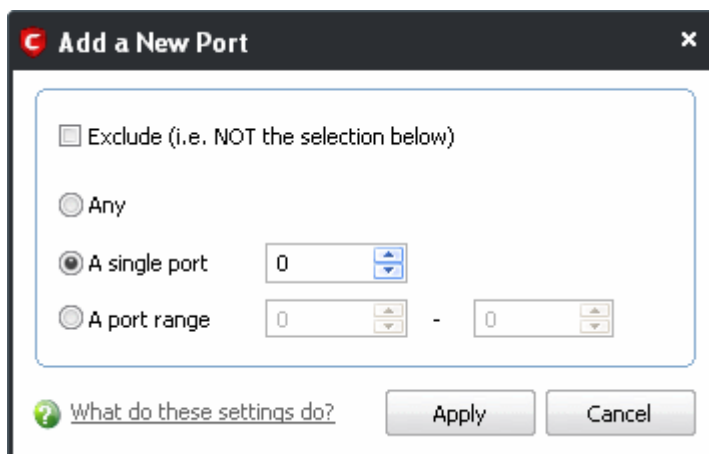
3. Click 'Apply'. The new port set appears in the main port set list:



4. Select the port numbers you want to belong to this named set by right clicking on the name of the new port set and select 'Add...' from the menu.



This opens the port selection dialog.



5. Select the ports by selecting:
  - **Any**, to choose all ports;
  - **A single port** and defining the port in the combo box beside;
  - **A port range** and typing the start and end port numbers in the respective combo boxes.
6. Click 'Apply'.
7. Click 'OK' in the My Port Sets interface

If you wish to add more ports to this set then repeat the process from the fourth step.

### To edit the name of an existing port set

- Select the name of the set in the list (e.g. HTTP Ports) and click 'Edit...' to bring up the naming dialog.

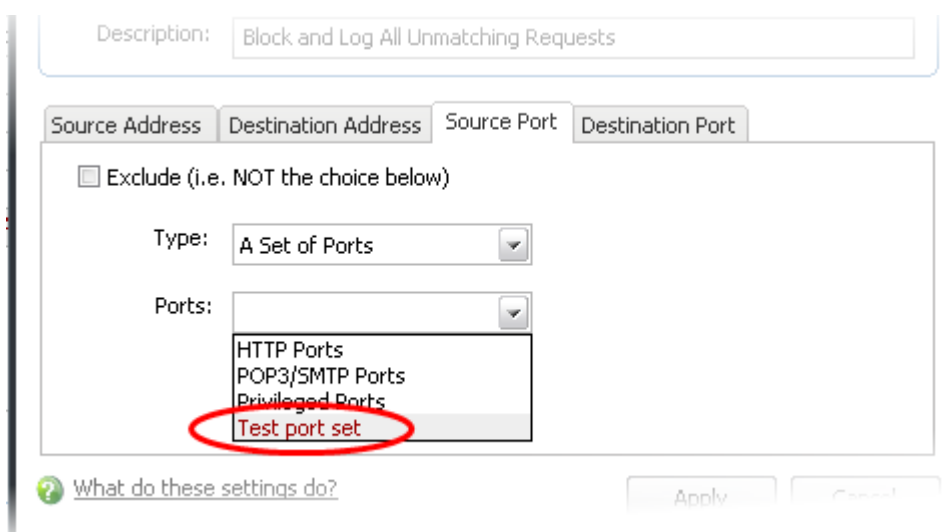
### To add port numbers to an existing port set

- Right click on the set name and click 'Add...' or select the port set name, right click the 'Add...' button and select 'A new port' from the drop-down menu.

### To modify or change the existing port numbers in a port set

- Right click on the port number you wish to change and select 'Edit...' OR select the actual port number (not the port set name), right click on it and Select 'Edit...'.

When **defining or modifying a network control rule**, any port sets listed in this interface, including any new ones you create are available for selection and deployment in the **Source Port** and **Destination Port** tabs on selecting **A set of Ports**.



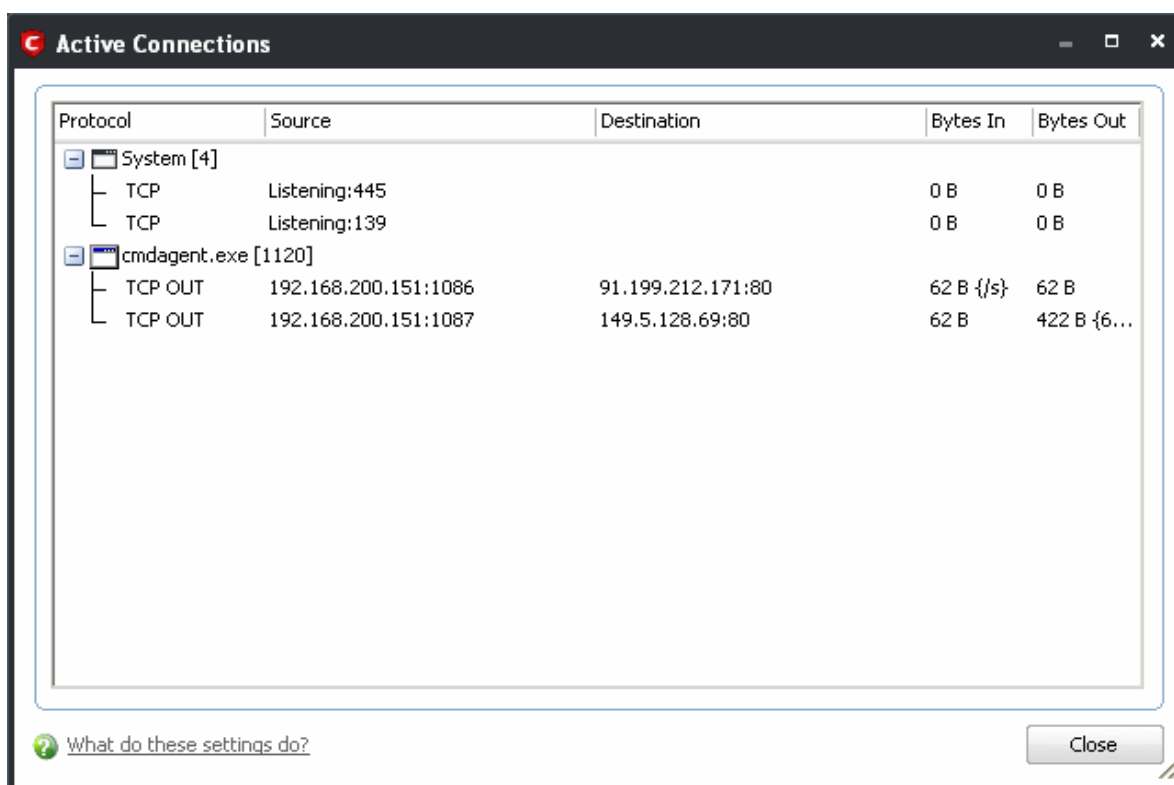
## 3.5 View Active Connections

The Active Connections interface contains an at-a-glance summary of all currently active 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 Active 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.

### To Access View active connections

1. Click on View Active Connections link in Firewall Tasks.

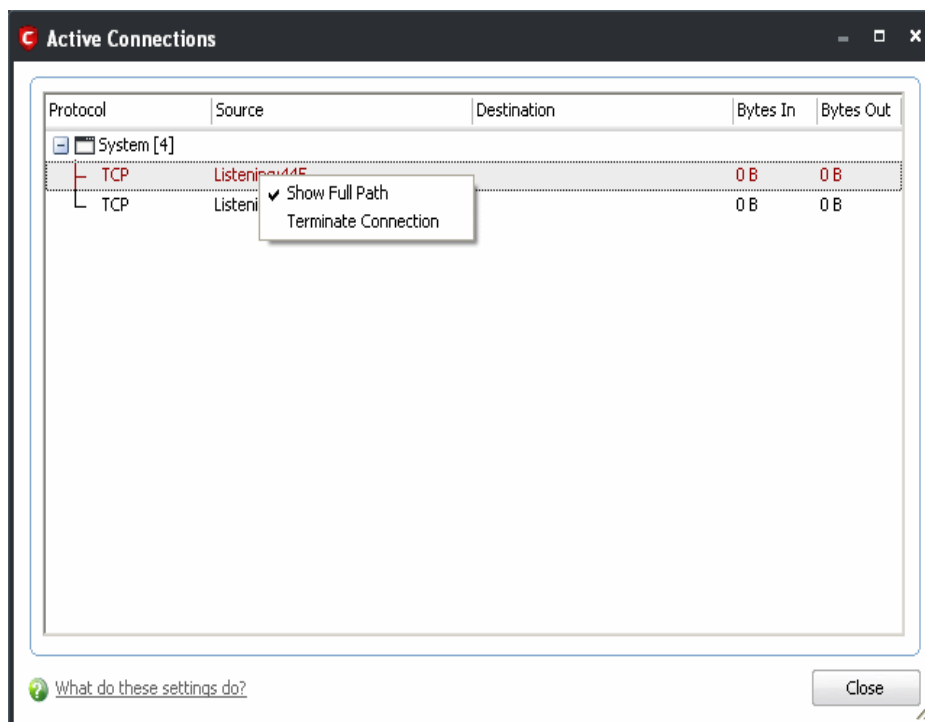


#### Column Description

- **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.
- **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

1. Right click on items in the list to see the context sensitive menu.



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

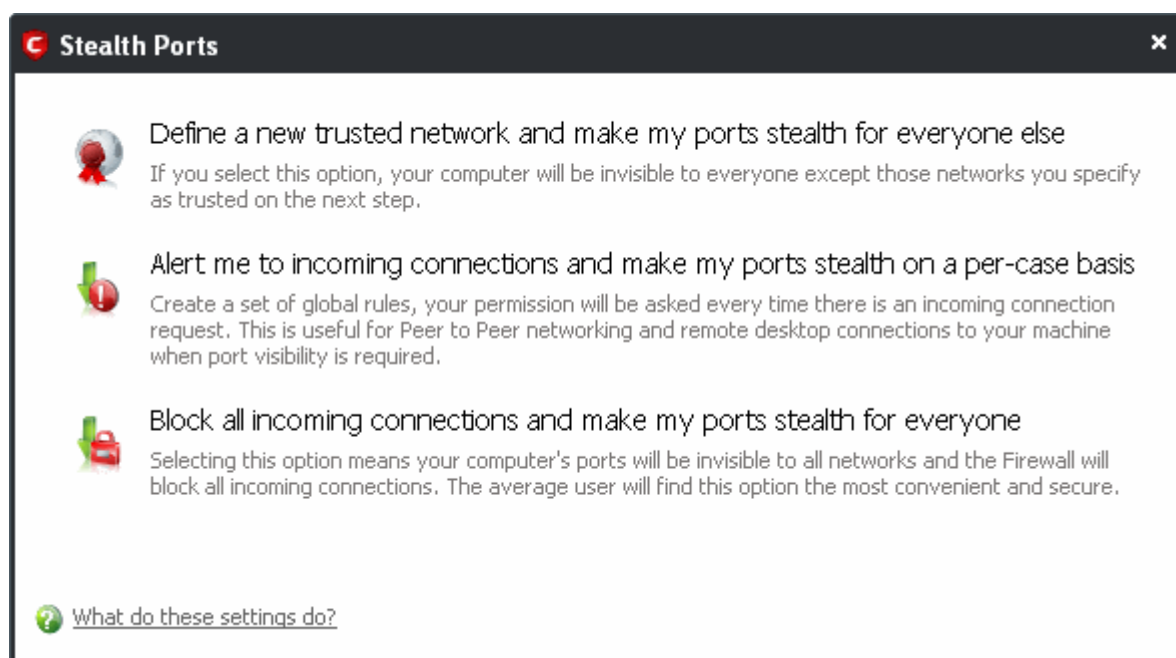
## 3.6 Stealth Ports Wizard

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

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

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

1. Click on 'Stealth Ports Wizard' in Firewall Tasks.
2. You have three options to choose from:
  - Define a new trusted network
  - Alert me to incoming connections
  - Block all incoming connections



Click the option you would like more details on:

- [Define a new trusted network and make my ports stealth for everyone else](#)
- [Alert me to incoming connections and make my ports stealth on a per-case basis](#)
- [Block all incoming connections and make my ports stealth for everyone](#)

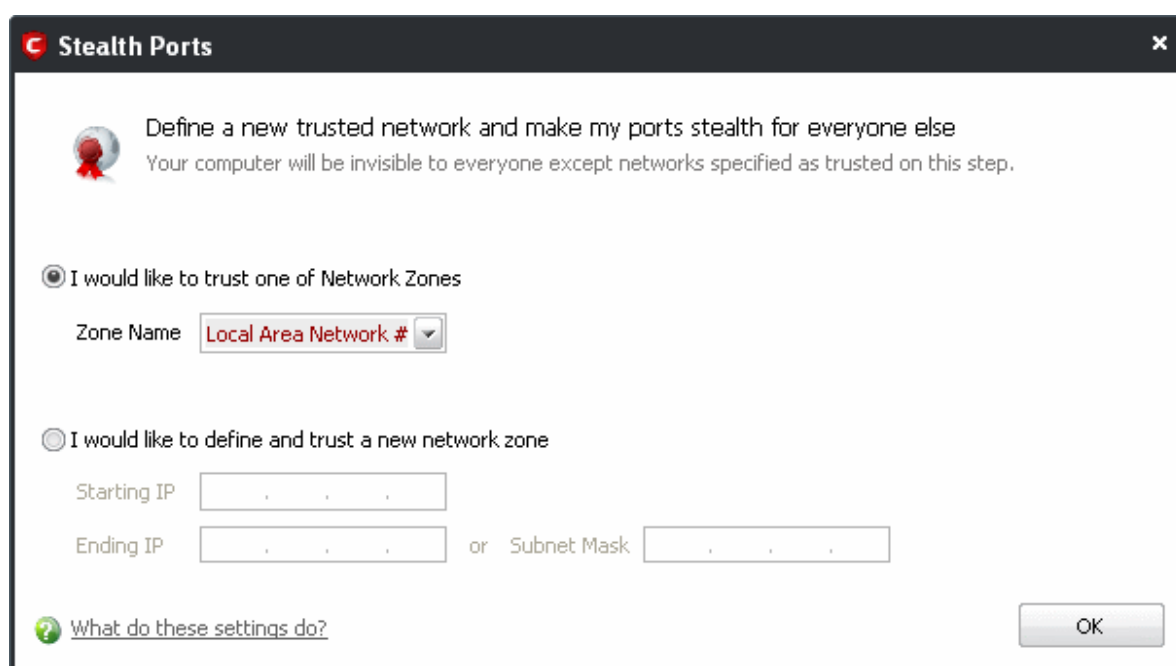
### Define a New Trusted Network and Make my Ports Stealth for Everyone Else

By selecting this option your machine's ports is stealthed (invisible) to everyone EXCEPT those networks that you specify as trusted.

#### To begin the wizard

1. Click 'Define a New Trusted Network and make my ports stealth for everyone else' link.

A dialog box appears, asking you to choose the new trusted zone:

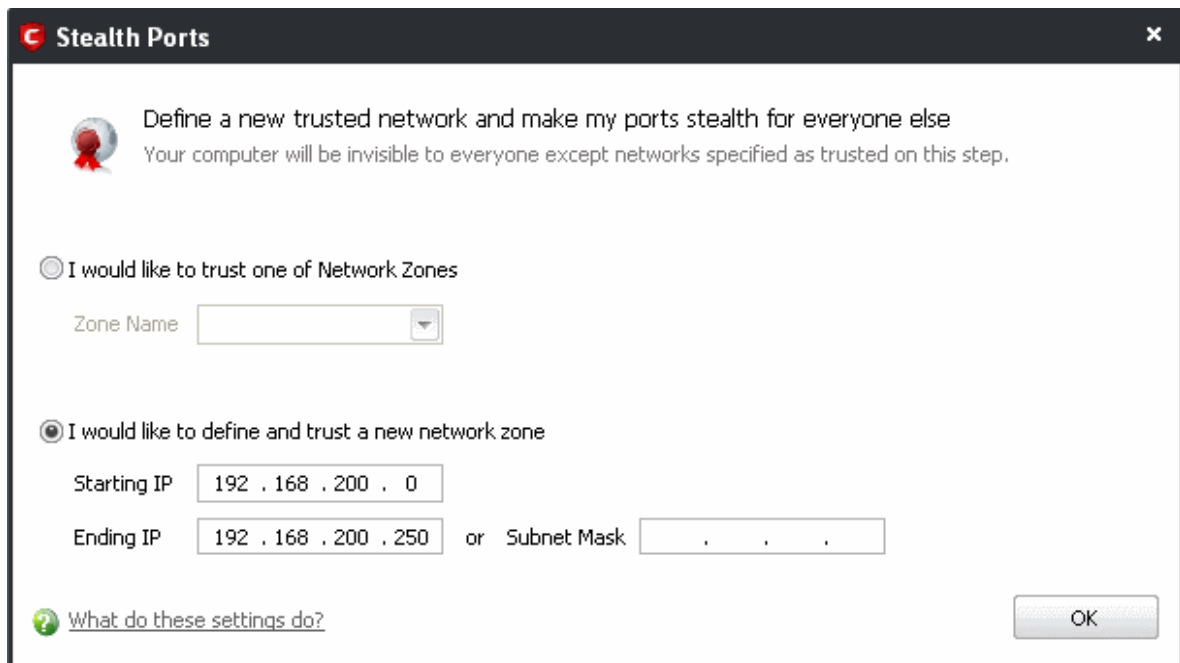


2. If you have already configured a network zone then leave the upper option selected, choose your desired network from the 'Zone Name' drop-down box and click 'OK'.

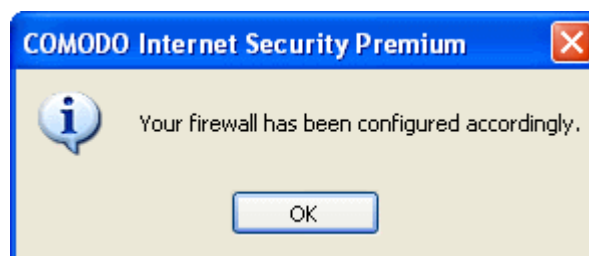
If you have not yet defined a zone you wish to trust, you can do so in '**Network Zones**' area in **Network Security Policy** interface of the firewall or manually define and trust a new zone from this dialog box.

### To manually define and trust a new zone from this dialog box

1. Select 'I would like to define and trust a new network zone'.

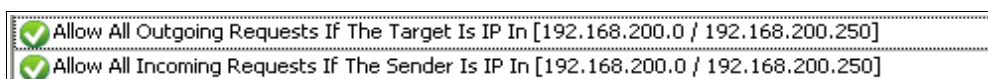


2. Enter the IP range for the zone for which you want your computer to be visible - starting from the Start IP to the End IP (or specify a Subnet Mask)
3. Click 'OK' to create the new Zone rule.



If you wish to add more than one zone, simply repeat this procedure.

Using the 'Define a new trusted network and make my ports stealth for everyone else' option creates a new trusted zone by adding the following rules in the '**Global Rules**' interface:



The specific parameters of the descriptive rule name above are:

**Allow** | IP | Out | From Any IP Address | To <ZONE> | Where Protocol is ANY

**Allow** | IP | In | From <ZONE> | To Any IP Address | Where Protocol is ANY



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

### Alert me to incoming connections and make my ports stealth on a per-case basis

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](#).

### Block all incoming connections and make my ports stealth for everyone

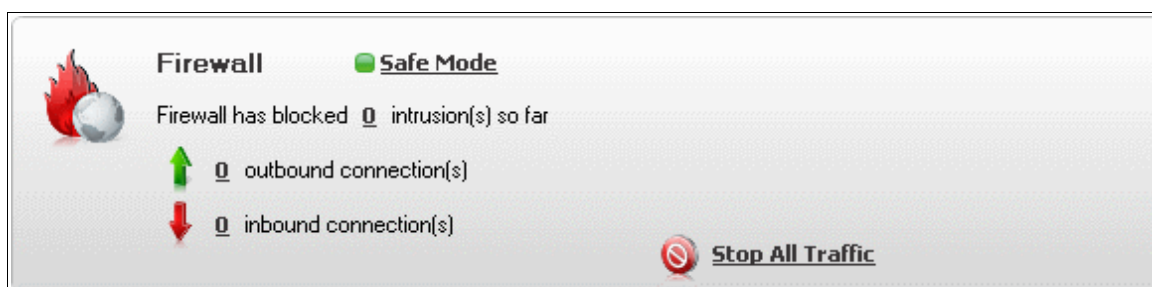
Selecting this option means your computer's ports are invisible to all networks, irrespective of whether you trust them or not. The average home user (using a single computer that is not part of a home LAN) finds this option the more convenient and secure. You are not alerted when the incoming connection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

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

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

## 3.7 Firewall Behavior Settings

Firewall Behavior Settings allows you to quickly configure the security of your computer and the frequency of alerts that are generated. This dialog box can be accessed in the 'Firewall Tasks' and, more immediately, by clicking on security level setting that is displayed (e.g. Safe Mode) in the **Summary Screen** (shown below).



These settings can be done using the tabs listed below.

- **General Settings tab**
- **Alert Settings tab**
- **Advanced Settings tab**

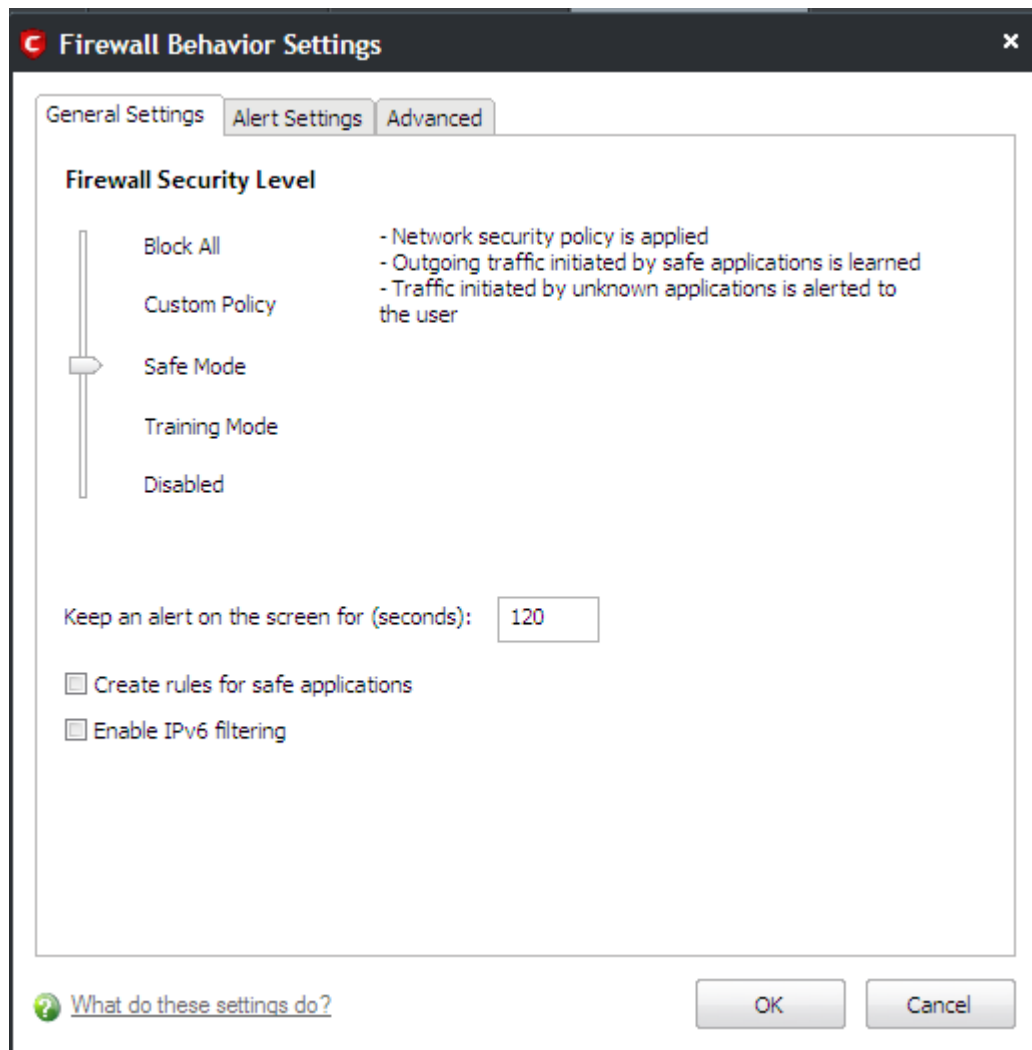
### 3.7.1 General Settings

Comodo Firewall allows you to customize firewall security by using the Firewall Security Level slider to change preset security levels.

The choices available are:

- Block All
- Custom Policy
- Safe Mode (This is default mode)
- Training
- Disabled

The setting you choose here is also displayed on the summary screen.



- **Block All Mode:** 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 applications 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 Policy Mode:** The firewall applies ONLY the custom security configurations and **network traffic policies** 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 policy** '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**.

**Tip:** Use this setting temporarily while playing an online game for the first time. This suppresses all alerts while the firewall learns the components of the game that need Internet access and automatically create 'allow' rules for them. You can switch back to your previous mode later.

- **Disabled:** Disables the firewall and makes it inactive. All incoming and outgoing connections are allowed irrespective of the restrictions set by the user. Comodo strongly advise against this setting unless you are sure that you are not currently connected to any local or wireless networks.

#### Keep an alert on screen for maximum (n) seconds

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.

#### Create rules for safe applications

Comodo Firewall trusts the applications if:

- The application/file is included in the Trusted Files list under Defense+ Tasks;
- The application is from a vendor included in the **Trusted Software Vendors** list under Defense+ Tasks;
- 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 **Network Security Policy > 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, '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).

**Enable IPv6 filtering** - Enabling this options means CIS will filter IPv6 network traffic in addition to IPv4 traffic. (**Default = Disabled**).

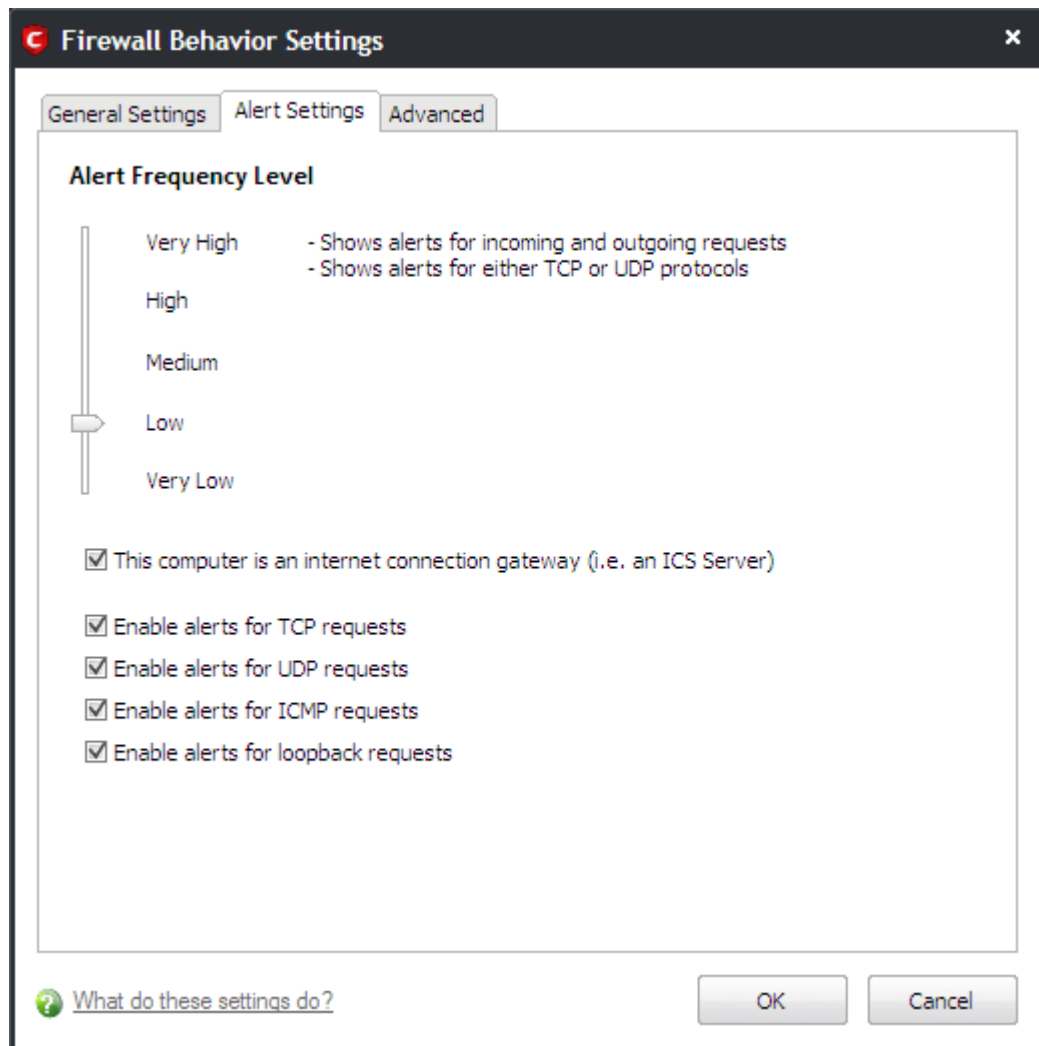
**Background Note:** IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for 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  $3.4 \times 10^{38}$  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.

## 3.7.2 Alert Settings

Users can configure the amount of alerts that Comodo Firewall generates, using the slider on this tab. Raising or lowering the slider changes the amount of alerts accordingly. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in '**Network Security Policy**'). 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.

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.



- **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 (Default):** 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.

#### Check boxes

**This computer is an Internet connection gateway (i.e. an ICS server)** - An Internet Connection Sharing Server (ICS) is a computer that shares its connection to the Internet with other computers that are connected to it by LAN. i.e. the other computers access the Internet through this computer (*Default = Enabled*).

Designating a computer as an ICS server can be useful in some corporate and home environments that have more than one computer but which have only one connection to the Internet. For example, you might have 2 computers in your home but only one connection. Setting one as an ICS server allows both of them to access the Internet.

- Leave this box unchecked if no other computers connect to your computer via Local Area Network to share your connection. This is the situation for the vast majority of home and business users.
- Check this option if this computer has been configured as an Internet Connection Sharing server through

which other computers connect to the Internet.

**Note:** If your computer is indeed an ICS server but you leave this box unchecked then you are likely to see an increase in Firewall alerts. Selecting this checkbox does not decrease the security but tells the firewall to handle ICS requests too. So it just activates some additional functionality and helps reduce the number of alerts.

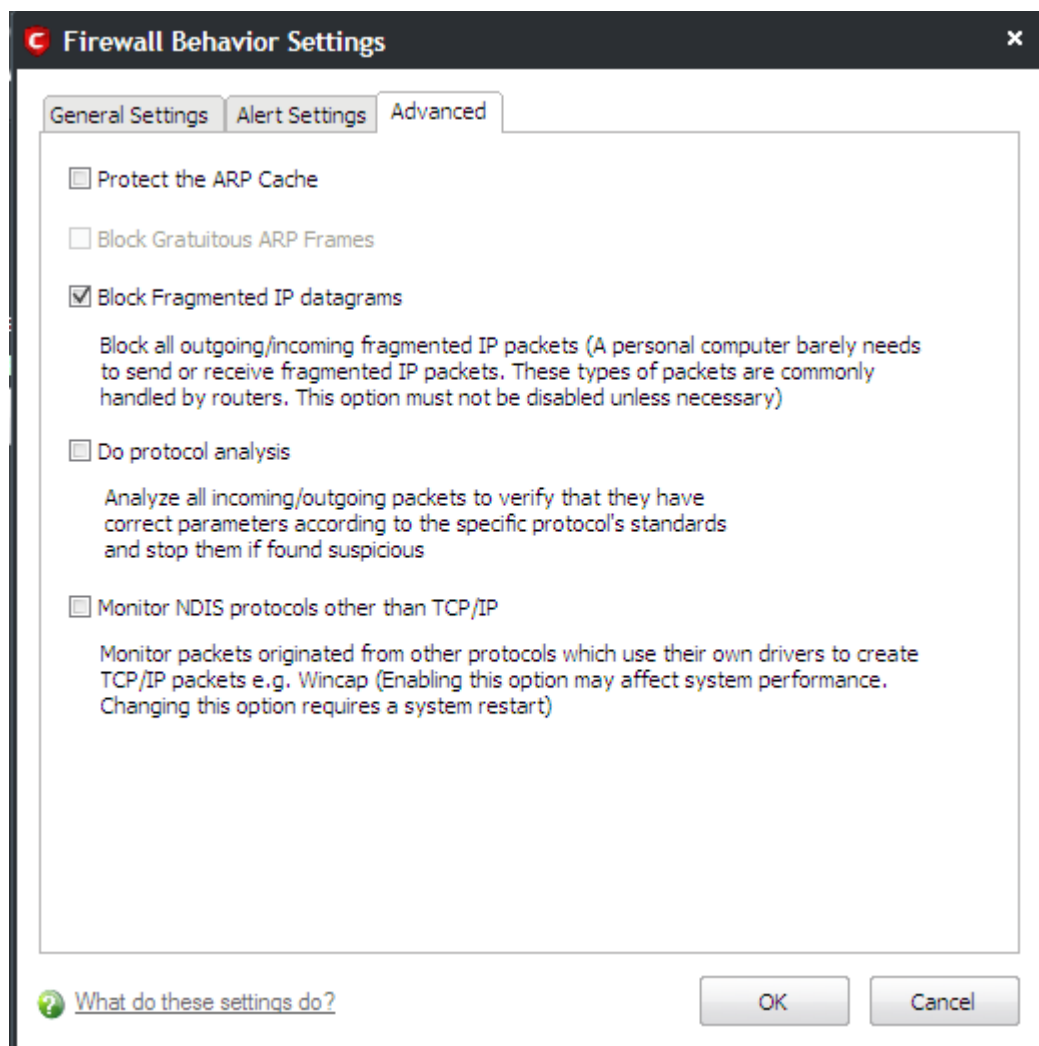
**Q:** 'I have more than one computer in my home and both connect to the Internet. Should I check this box?'

**A:** In most cases no. Having more than one computer in your home, both of which connect to the 'net via a router or wireless connection, is not the same as 'sharing' a connection in the sense that we mean here. Only check this box if you know that you have designated this computer as an ICS server.

**Enable alerts for TCP requests / Enable alerts for UDP requests / Enable alerts for ICMP requests/ Enable Alerts for loopback requests** - In conjunction with the slider, these checkboxes allow you to fine-tune the number of alerts you see according to protocol (*Default = Enabled*).

### 3.7.3 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.



- **Protect the ARP Cache** - Checking this option makes Comodo Firewall to start performing stateful inspection of ARP (Address Resolution Protocol) connections. This blocks spoof ARP requests and protects your computer from ARP cache poisoning attacks (*Default = Disabled*).

The ARP Cache (or ARP Table) is a record of IP addresses stored on your computer that is used to map IP addresses to MAC addresses. Stateful inspection involves the analysis of data within the lowest levels of the

protocol stack and comparing the current session to previous ones in order to detect suspicious activity.

**Background:** Every device on a network has two addresses: a MAC (Media Access Control) address and an IP (Internet Protocol) address. The MAC address is the address of the physical network interface card inside the device, and never changes for the life of the device (in other words, the network card inside your PC has a hard coded MAC address that it keeps even if you install it in a different machine.) On the other hand, the IP address can change if the machine moves to another part of the network or the network uses DHCP to assign dynamic IP addresses. In order to correctly route a packet of data from a host to the destination network card it is essential to maintain a record of the correlation between a device's IP address and its MAC address. The Address Resolution Protocol performs this function by matching an IP address to its appropriate MAC address (and vice versa). The ARP cache is a record of all the IP and MAC addresses that your computer has matched together.

Hackers can potentially alter a computer's ARP cache of matching IP/MAC address pairs to launch a variety of attacks including, Denial of Service attacks, Man in the Middle attacks and MAC address flooding and ARP request spoofing. It should be noted, that a successful ARP attack is almost always dependent on the hacker having physical access to your network or direct control of a machine on your network - therefore this setting is of more relevance to network administrators than home users.

- **Block gratuitous ARP frames** - A gratuitous 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). Enabling this setting helps to block such requests - protecting the ARP cache from potentially malicious updates (*Default = Disabled*).
- **Block fragmented IP Datagrams** - 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 = Enabled*).

Comodo Firewall is set by default to block fragmented IP datagrams i.e the option Block Fragmented IP datagrams is checked by default.

- **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*).
- **Monitor NDIS protocols other than TCP/IP** - This forces Comodo Firewall to capture the packets belonging to any other protocol driver than TCP/IP. Trojans can potentially use their own protocol driver to send/receive packets. This option is useful to catch such attempts. This option is disabled by default: because it can reduce system performance and may be incompatible with some protocol drivers (*Default = Disabled*).

## 4 Defense+ Tasks - Introduction

The Defense+ component of Comodo Internet Security (hereafter known simply as Defense+) is a host intrusion prevention system that constantly monitors the activities of all executable files on your PC. With Defense+ activated, the user is warned EVERY time an unknown application executable (.exe, .dll, .sys, .bat etc) attempts to run. The only executables that are allowed to run are the ones you give permission to.

Defense+ also protects against data theft, computer crashes and system damage by preventing most types of buffer overflow attacks. This type of attack occurs when a malicious program or script deliberately sends more data to its memory buffer than that the buffer can handle. It is at this point that a successful attack can create a back door to the system through which a hacker can gain access. The goal of most attacks is to install malware onto the compromised PC whereby the hacker can reformat the hard drive, steal sensitive user information, or even install programs that transform the machine into a Zombie PC. For more details refer [Execution Control Settings](#).

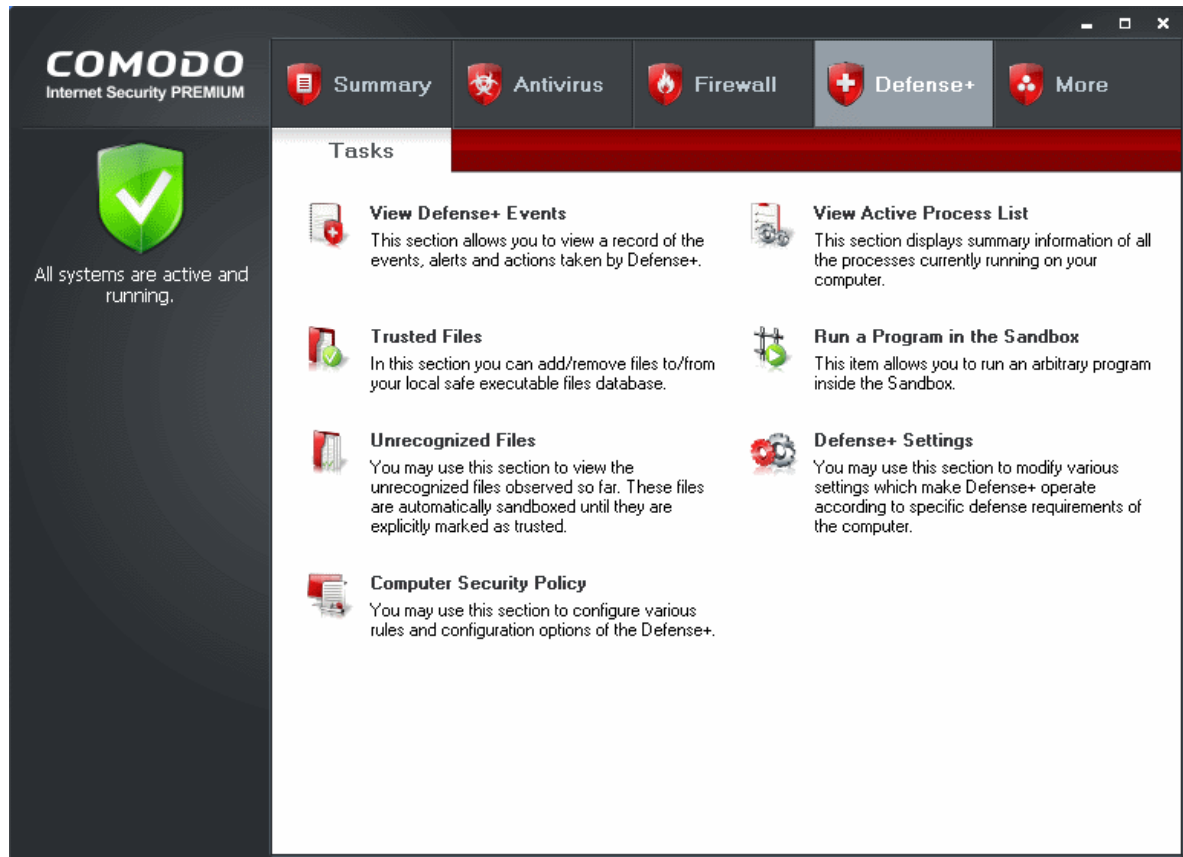
Defense+ boasts a highly configurable security rules interface and prevents possible attacks from root-kits, inter-process memory injections, key-loggers and more. It blocks Viruses, Trojans and Spyware before they can ever get installed on your system and prevents unauthorized modification of critical operating system files and registry entries.



The Sandbox functionality of Defense+ allows you to run suspicious and unknown executables in an isolated environment to safeguard your system from the adverse effects of those executables. This is useful for software testers and users interested in testing out the new software available over Internet.



The Defense+ Tasks area can be accessed at all times by clicking on the Defense+ tab from the navigation panel.



The Defense+ main configuration area provides easy access to all the features and allows you to create rules for applications and sandbox through a series of shortcuts and wizards. Click on the links below to see detailed explanations of each area in this section.

- [View Defense+ Events](#)
- [Trusted Files](#)
- [Unrecognized Files](#)
- [Computer Security Policy](#)
- [View Active Process List](#)
- [Run a Program in the Sandbox](#)
- [Defense+ Settings](#)

## 4.1 The Sandbox - An Introduction

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 sandboxing 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 anti-virus 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 2011 offers improved security, fewer pop-ups and greater ease of use than ever before.

Refer to the following sections for more details on sandbox:

- [The Sand-boxing and Scanning Processes](#)
- [Always Sandbox](#)
- [Run a Program in the Sandbox](#)
- [Sandbox Settings](#)

### 4.1.1 Unknown Files: The Sand-boxing and Scanning Processes

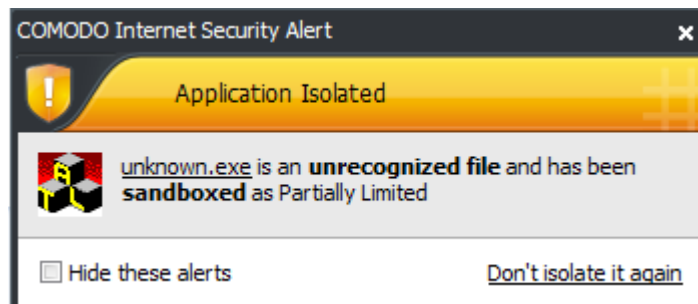
- When an executable is first run it passes through the following CIS security inspections:
  - Antivirus scan
  - Defense+ Heuristic check
  - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CIS (and therefore not 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 sandboxed or sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS policy (See [Computer Security Policy](#) 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 local Sandbox so that it cannot access important operating system files or damage your computer, and
  - (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 locally sandboxed. CIS will alert the user that it is going to run the application in the sandbox.



- Automatically sandboxed applications are run with 'Partially Limited' restrictions. *More detail: Sandboxed applications are allowed to run under a specific set of conditions or privileges. In CIS, these are known as 'Restriction Levels'. There are four levels - Partially Limited, Limited, Restricted and Untrusted ('Partially Limited' is the default level for applications that are automatically placed in the sandbox). In part, sandbox restriction levels are implemented by enforcing or relaxing the native access rights that Windows can grant to an application. For example, the 'Limited' setting applies some of the supported operating system restrictions and grants it access rights similar to if the application was run under a non-admin user account. These restriction levels are fortified with certain Defense + restrictions that apply to all sandboxed applications (for example, they cannot key log or screen grab, set windows hooks, access protected COM interfaces or access non-sandboxed applications in memory. If the user enables virtualization, then sandboxed apps. can't modify registry keys or modify existing protected files either).*
- Automatically sandboxed applications cannot be viewed or modified in the interface. Applications that were automatically sandboxed can only be removed if they become recognized as 'safe' by CIS (see conditions above).
- Unrecognized files are simultaneously uploaded to Comodo's Instant Malware Analysis servers for further checks:
  - Firstly, the files undergo another anti-virus 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.

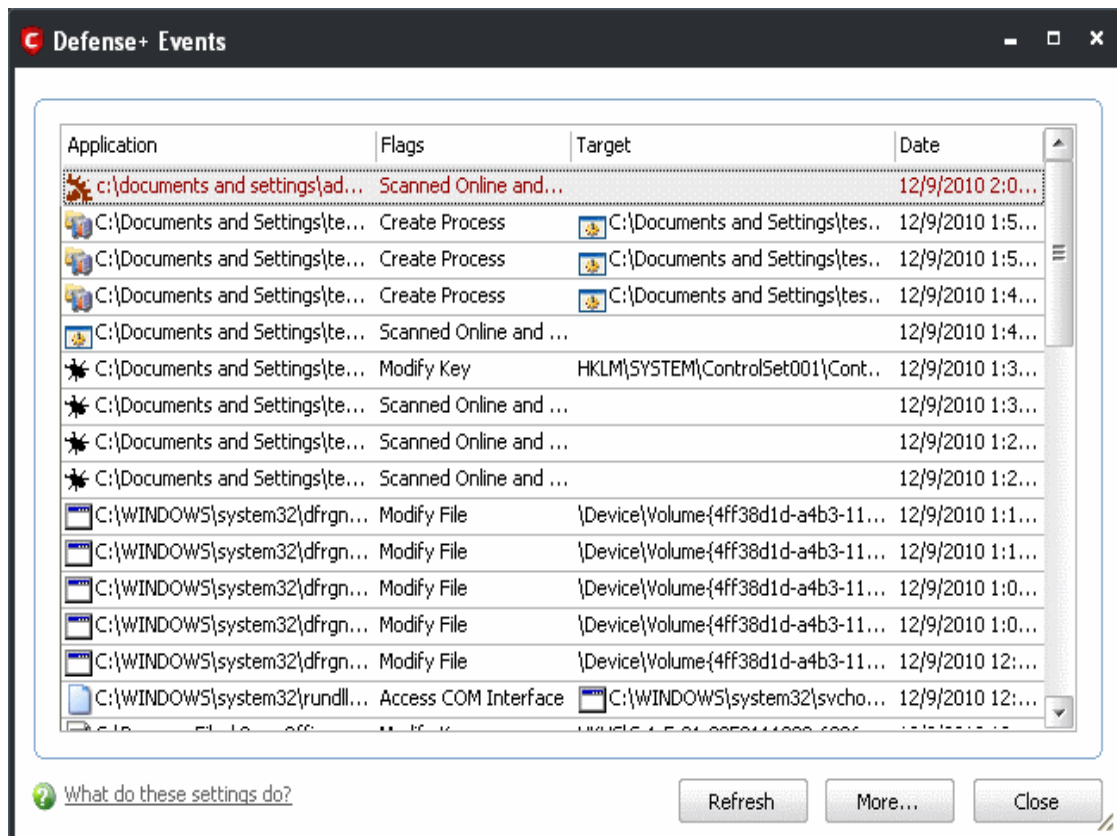
- In either case, the result is reported back to your CIS installation in approximately 15 minutes. If the executable was not found to be malicious then it will be run in the sandbox. It will simultaneously be added to the 'Unrecognized Files' list and uploaded to our technicians for analysis. If it is discovered to be a threat then CIS will show an AV alert to the user. From this alert the user can opt to quarantine, clean (delete) or disinfect the malicious file. This new threat will be automatically added to the global black list database and therefore benefit all CIS users.

#### Sandbox - Other notes

- Applications can be placed in the sandbox automatically by CIS or by the **Always Sandbox** feature. Users also have the option to **run an application in the sandbox** on a 'one-off' basis.
- If a safe or installer application is executed by an application running inside the sandbox, the installer also runs in the sandbox no matter what
- If a user defines an application for sandboxing, this causes any applications (safe or installer) to also be executed inside the sandbox.
- In addition to the Sandbox restriction level set for an application, Defense + also implements the following restrictions. A sandboxed application cannot:
  - Access non-sandboxed applications in memory
  - Access protected COM interfaces
  - Key log or screen capture
  - Set windows hooks
  - Modify protected registry keys (if virtualization is enabled)
  - Modify EXISTING protected file (if virtualization is enabled).

## 4.2 View Defense+ Events

The 'View Defense+ Events' area contains logs of all actions taken by the Defense+. A 'Defense+ Event' is triggered whenever an application makes an attempt to access memory, other programs, the registry etc. that contravenes your **Computer Security Policy**.

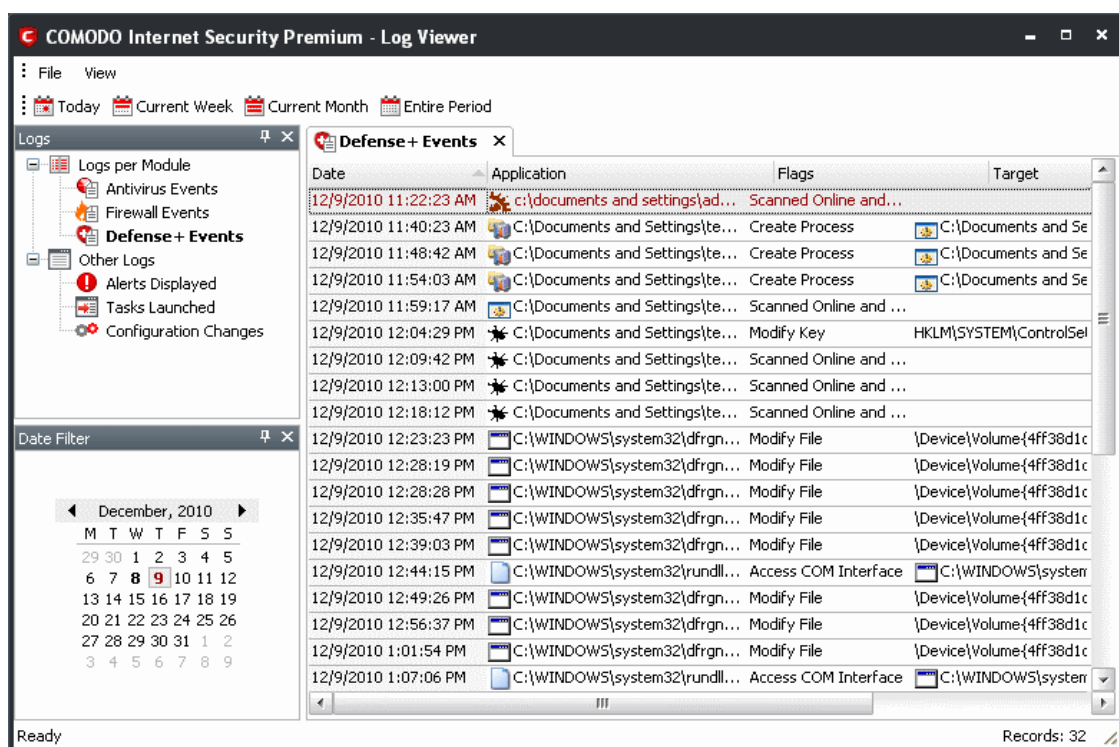


## Column Descriptions

- **Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used.
- **Flags** - Indicates flags set for the kinds of actions against the event triggered by the file.
- **Target** - Represents the location of the target file.
- **Date/Time** - Contains precise details of the date and time of the access attempt.
  - Click **Refresh** to reload and update the displayed list, to include all events generated since the time you first accessed the 'Defense+ Events' area.
  - Click **'More ...'** to load the full, Comodo Internet Security Log Viewer module. See below for more details on this module.

## Log Viewer Module

This window contains a full history of logged events of Firewall, Defense+ and Antivirus modules. It also allows you to build custom log files based on **specific filters** and to **export log file** for archiving or troubleshooting purposes.



The Log Viewer Module is divided into two sections. The left hand panel displays a set of handy, pre-defined time **Filters** for Firewall, Defense+ and Antivirus event log files. The right hand panel displays the actual events that were logged for the time period you selected in the left hand panel (or the events that correspond to the filtering criteria you selected).

## Filtering Log Files

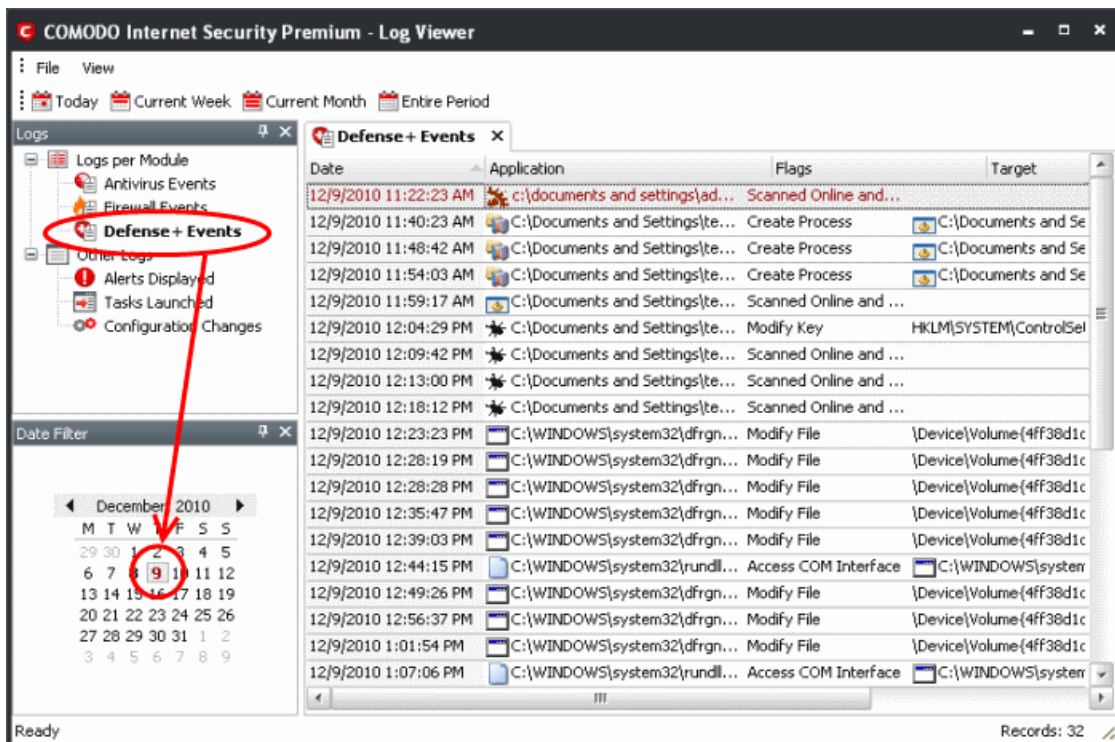
Comodo Internet Security allows you to create custom views of all logged events according to user defined criteria.

### Preset Time Filters:

Clicking on any of the preset filters in the top panel alters the display in the right hand panel in the following ways:

- **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).

The example below shows an example display when the Defense+ Logs for 'Today' are displayed.



**Note:** The type of events logged by the Antivirus, Firewall and Defense+ modules of Comodo Internet Security differ from each other. This means that the information and the columns displayed in the right hand side panel change depending on which type of log you have selected in the top and left hand side panel. For more details on the data shown in the columns, see [View Anti-virus Events](#) or [View Firewall Events](#).

### User Defined Filters:

Having chosen a **preset time filter** from the top panel, you can further refine the displayed events according to specific filters. The type of filters available for Firewall logs differ to those available for Defense+ logs. The table below provides a summary of available filters and their meanings:

Available Filters - Logs per Module		
Antivirus Filter	Firewall Filters	Defense+ Filters
<b>Action</b> - Displays events according to the response (or action taken) by the Antivirus	<b>Action</b> - Displays events according to the response (or action taken) by the firewall	<b>Application</b> - Displays only the events propagated by a specific application
<b>Location</b> - Displays only the events logged from a specific location	<b>Application</b> - Displays only the events propagated by a specific application	<b>Flags</b> - Displays events according to the response (or action taken) by Defense+
<b>Malware Name</b> - Displays only the events logged corresponding to a specific malware	<b>Destination IP</b> - Displays only the events with a specific target IP address	<b>Target</b> - Displays only the events that involved a specified target application
<b>Status</b> - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'	<b>Destination Port</b> - Displays only the events with a specific target port number	

Available Filters - Logs per Module		
	<b>Direction</b> - Indicates if the event was an Inbound or Outbound connection	
	<b>Protocol</b> - Displays only the events that involved a specific protocol	
	<b>Source IP address</b> - Displays only the events that originated from a specific IP address	
	<b>Source Port</b> - Displays only the events that originated from a specific port number	

## Creating Custom Filters

Custom Filters can be created through the Advanced Filter Interface. You can open the Advanced Filter interface either by using the View option in the menu bar or using the context sensitive menu.

- Click View > Advanced Filter to open the 'Advanced Filter' configuration area.

Or

- Right click on any event and select 'Advanced Filter' option to open the corresponding configuration area.

The 'Advanced Filter' configuration area is displayed in the top half of the interface whilst the lower half displays the Events, Alerts, Tasks or Configuration Changes that the user has selected from the upper left pane. If you wish to view and filter event logs for other modules then simply click log name in the tree on the upper left hand pane.

The Advanced Log filter displays different fields and options depending on the log type chosen from the left hand pane (Antivirus, Defense+, Firewall).

This section will deal with Advanced Event Filters related to 'Antivirus Events' and will also cover the custom filtering that can be applied to the 'Other Logs' (namely 'Alerts Displayed', 'Tasks' Launched' and 'Configuration Changes').

## Defense+ Events - Advanced Filters

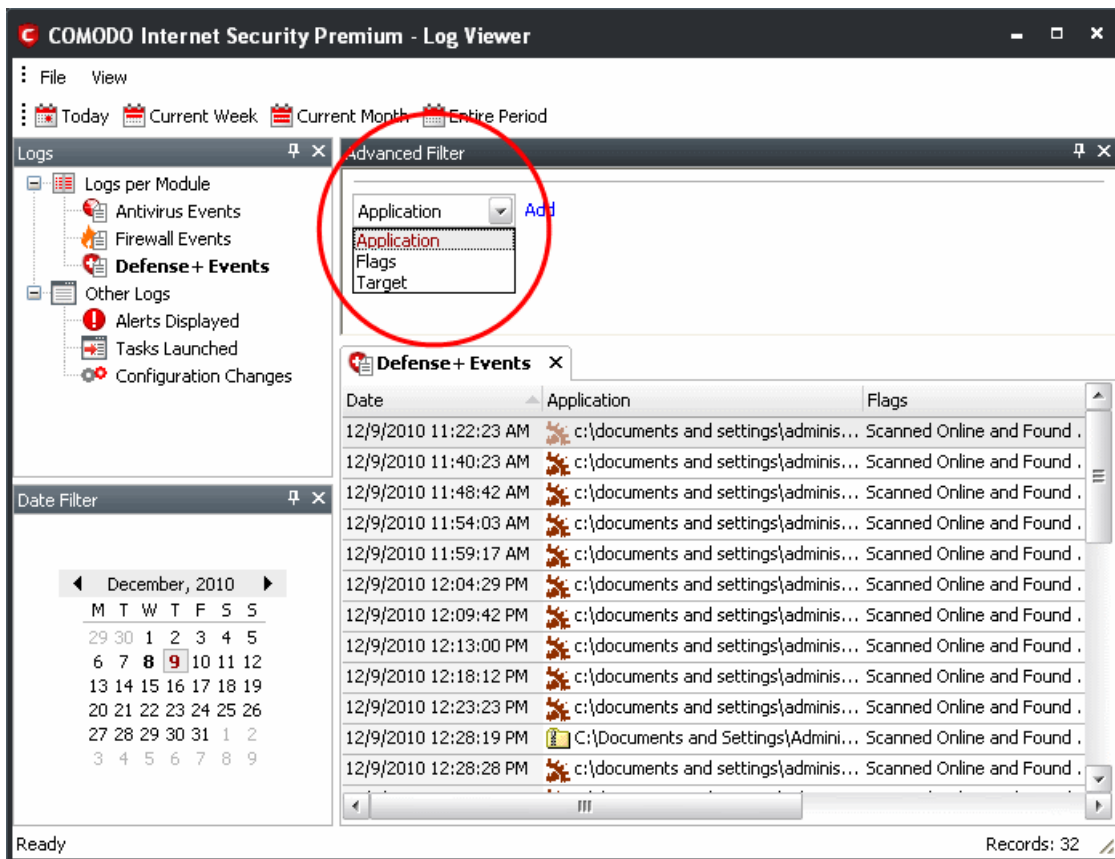
### To configure Advanced Filters for Defense+ events

1. Select 'View > Advanced Filter'
2. Select 'Defense+ Events' under 'Logs Per Module'

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.

3. Click the 'Add' link when you have chosen the category upon which you wish to filter.





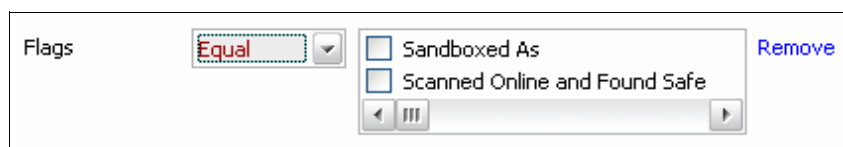
Following are the options available in the 'Add' drop down menu:

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



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

- 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

The filtered entries are shown directly underneath.

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

Target	Contains ▼	Application	Remove
--------	------------	-------------	--------

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

The filtered entries are shown directly underneath.

**Note:** More than one filters can be added in the 'Advanced Filter' pane. After adding one filter type, the option to select the next filter type automatically appears. You can also remove a filter type by clicking the 'Remove' option at the end of every filter option.

## Other Logs - Advanced Filters

Refer to [Antivirus Tasks Overview > View Antivirus Events > Log Viewer > Creating Custom Filters > Other Logs - Advanced Filters](#) for the process of Creating Custom Filters for Alerts Displayed, Task Launched and Configuration Changes.

## Date Filter

[Click here](#) to know more about Date Filter functionality.

## Exporting Log Files to HTML

Exporting log files is useful for archiving and troubleshooting purposes. There are two ways to export log files in the Log Viewer interface - using the context sensitive menu and via the 'File' menu option. After making your choice, you are asked to specify a name for the exported HTML file and the location you wish to save it to.

### i. File Menu

1. Click 'File' Menu.
2. Move cursor to 'Export'
3. Click on any one of 'Firewall Logs', 'Defense+ Logs', 'Antivirus Logs' and 'All', as required.
  - **Firewall Logs** - Exports the Firewall log that is currently being displayed in the right hand side panel.
  - **Defense+ Logs** - Exports the Defense+ log that is currently being displayed in the right hand side panel .
  - **Antivirus Logs** - Exports Antivirus log that is currently being displayed in the right hand side panel.

- **All** - Exports ALL logs for ALL TIME for Firewall, Defense+ and Antivirus logs as a single HTML file.
4. Select the location where the log has to be stored in the 'Save Firewall Log as' window and click 'Save'.
- ii. **Context Sensitive Menu**
1. Right click in the log display window to export the currently displayed log file to HTML.

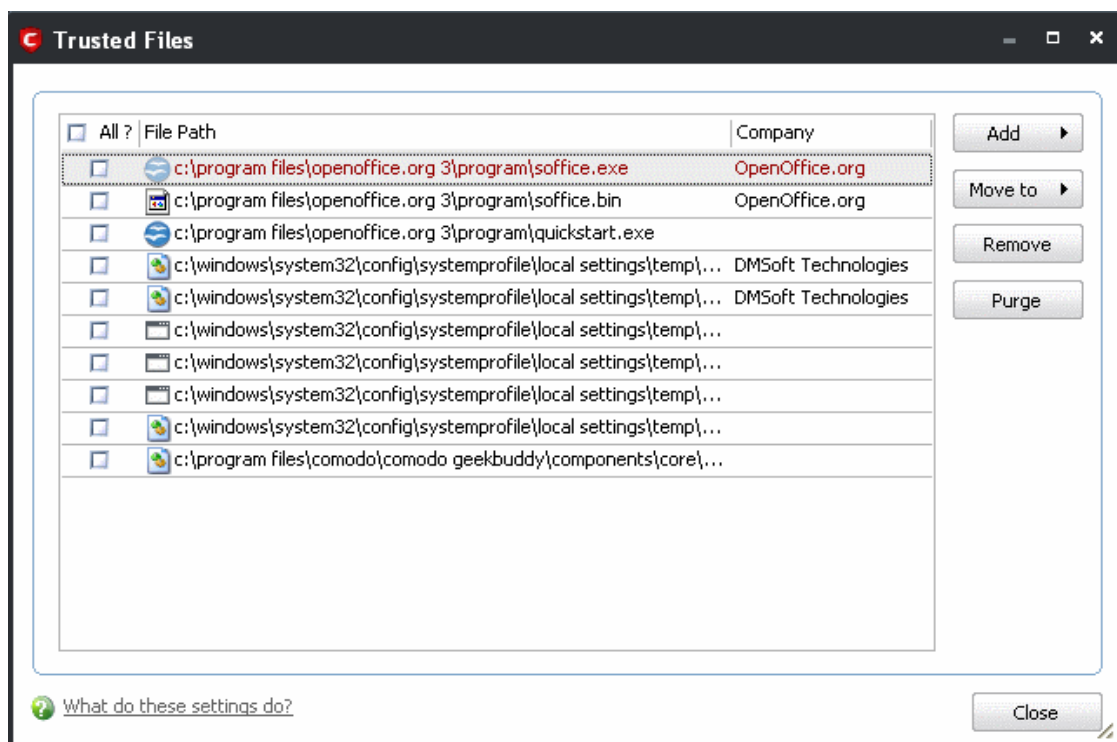
You can export a custom view that you created using the available Filters by right clicking and selecting 'Export' from the context sensitive menu. Again, you are asked to provide a filename and save location for the file.

## 4.3 Trusted Files

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

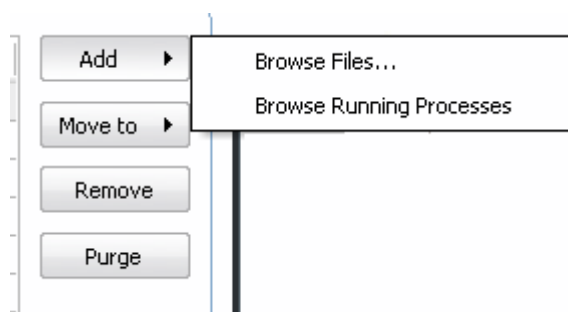
Files added to the Trusted Files area are automatically given Defense+ trusted status. If an executable is unknown to the Defense+ safe list then, ordinarily, it and all its active components generate Defense+ alerts when they run. Of course, you could choose the 'Treat this as a Trusted Application'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

By adding executables to this list (including sub folders containing many components) you can reduce the amount of alerts that Defense+ 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.

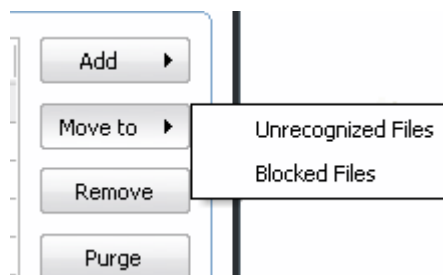


Click the 'Add' button to manually imports files or processes into this area:





The 'Move to...' option allows you to transfer the selected files *out* of the 'Trusted Files' area into either the **Unrecognized Files** or **Blocked Files** areas of Defense+:



### To remove an included entry from the Trusted Files list

- Select the entry and click 'Remove' button. The file is only removed from the list and not deleted from your system.

### To remove invalid entries (programs / files that are not present or uninstalled from your computer) automatically

- Select the entry and click 'Purge' button.

## 4.4 Unrecognized Files

Once installed, Defense+ 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.

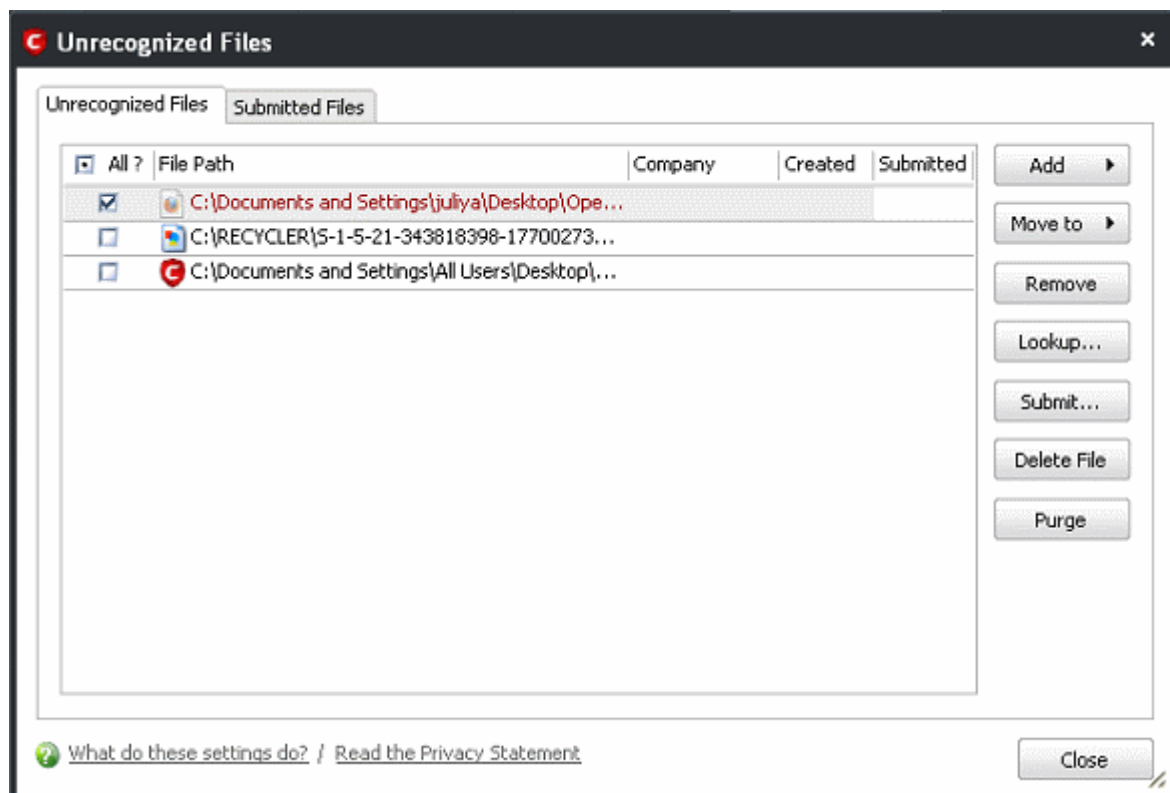
'Unrecognized Files' is specifically important while Defense+ is in 'Clean PC Mode'. In Clean PC Mode, the files in 'Unrecognized Files' are NOT considered clean. For more information, please check ['Clean PC Mode' on the Defense+ settings page](#).

The 'Unrecognized Files' Area allows the user 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.
- Use the **'Lookup...'** feature to see if the master Comodo safe list contains more information.
- Send the file to Comodo for analysis by clicking the 'Submit' button which automatically begins the **file submission process**.
- **Manually add files** to the pending list for look-ups or submitting to Comodo.
- Use the 'Purge' feature to scan the list for files that no longer exist on your system and remove them from the 'Unrecognized Files' list.
- Delete a selected file from the system by clicking 'Delete File' button

### To access Unrecognized Files interface Files

- Navigate to: Defense+ Tasks > Unrecognized Files.

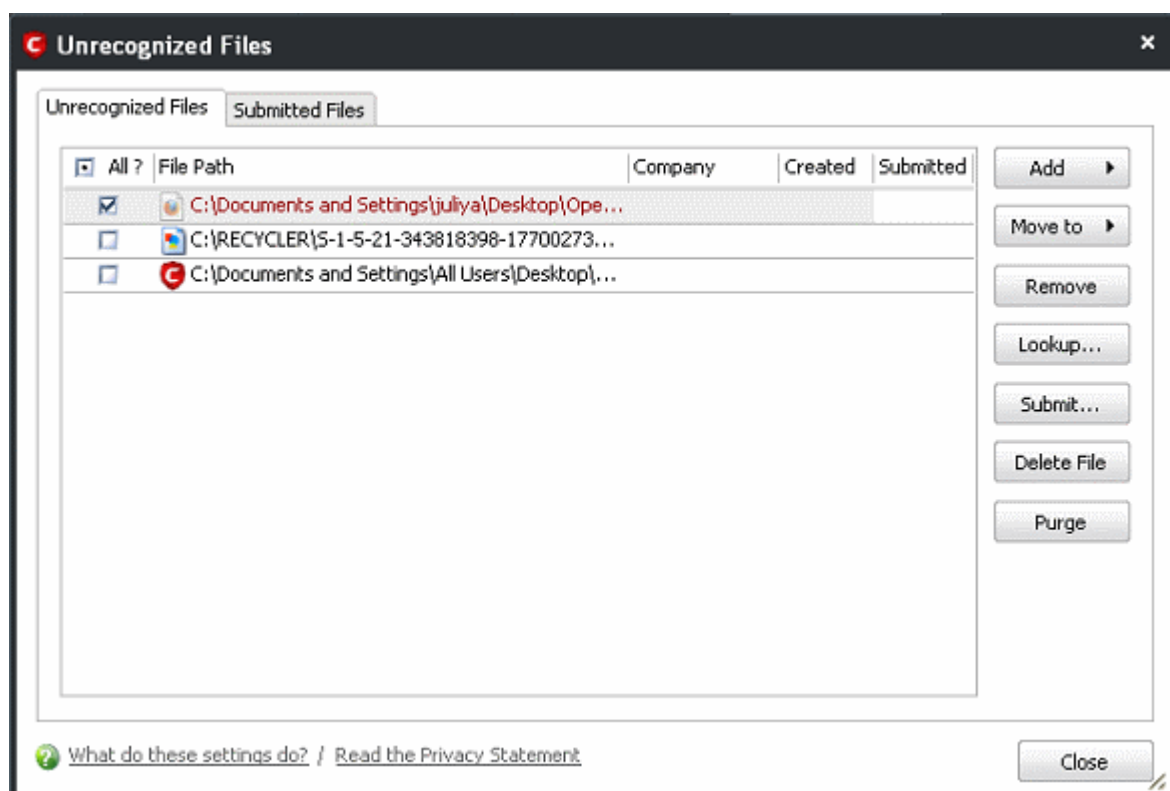


This area contains two tabs:

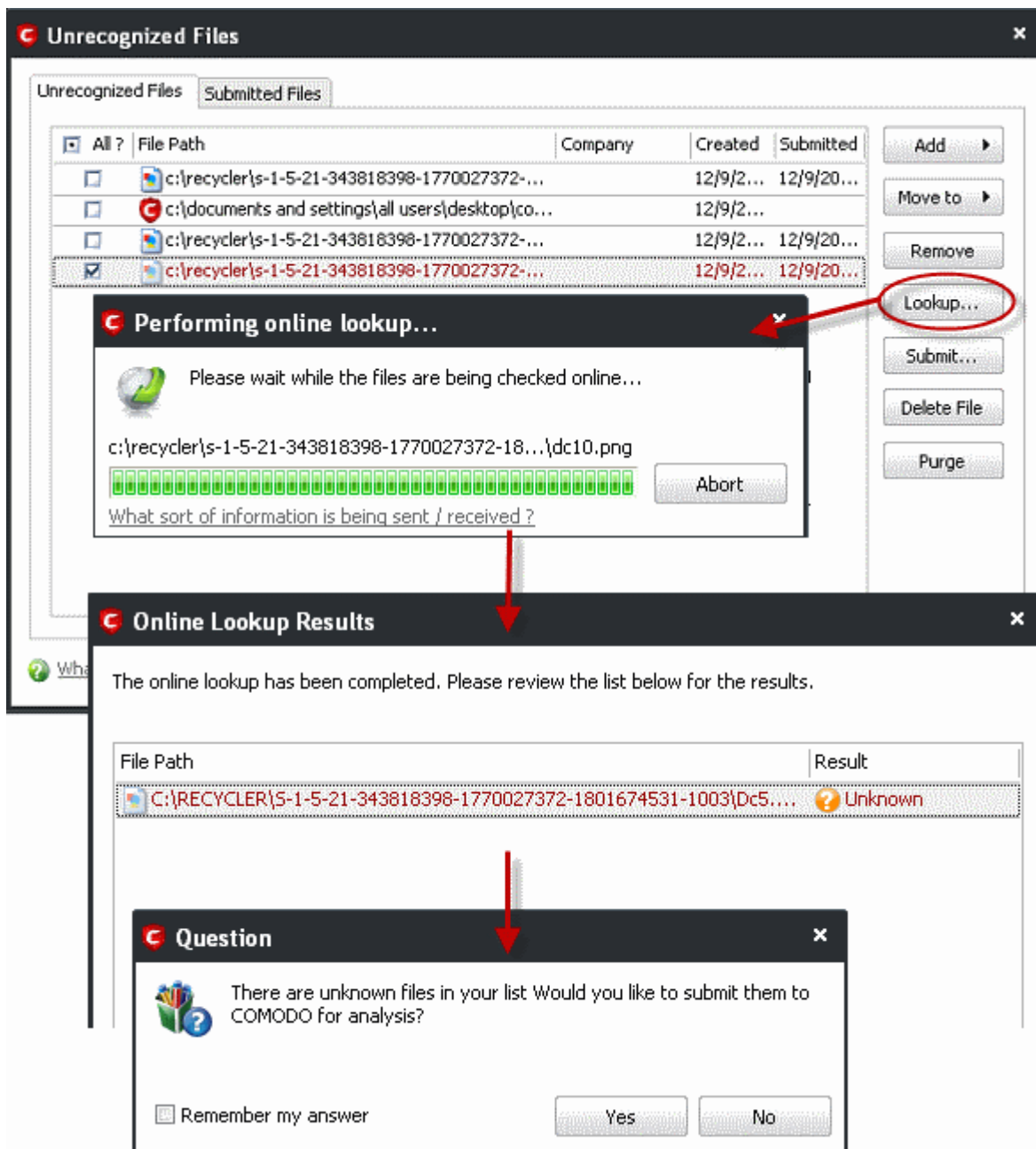
- **Unrecognized files** - Displays a list of files identified as suspicious by Defense+ and the files added to this area manually.
- **Submitted Files** - Displays a list of files that were submitted to Comodo for analysis.

#### 4.4.1 Unrecognized Files

The Unrecognized Files tab displays the list files that are identified as suspicious by Defense+. Also you can manually add suspicious and unclassified files to this area for later submission to Comodo for analysis.



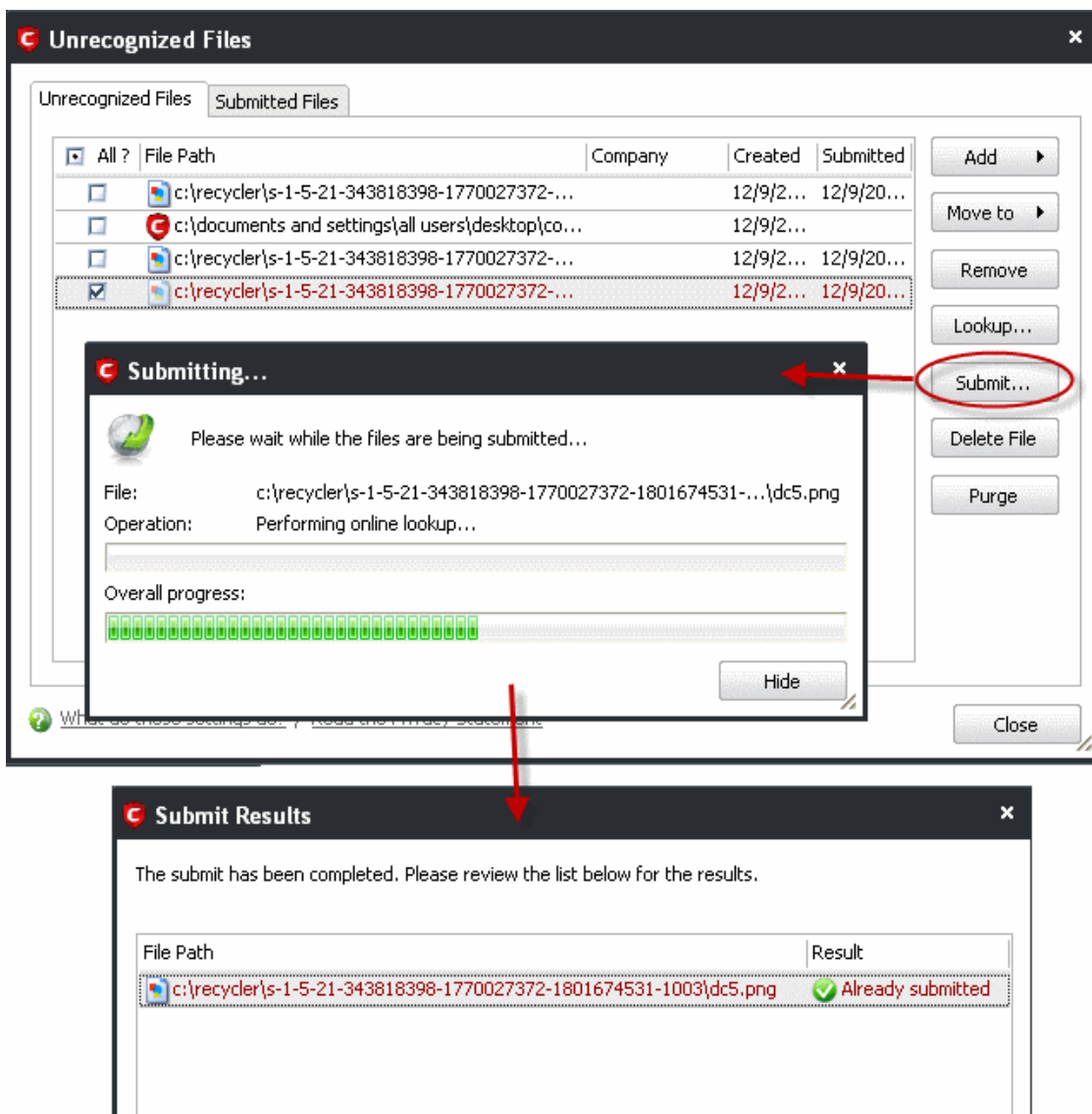
The 'Lookup...' button allows you to check for information on the files by consulting the master Comodo safe list, Select the file(s) you want to check and click the 'Lookup...' button. This contacts Comodo servers to conduct a search of Comodo's master safe list database to check if any information is available about the file in question. If no information is available, you are presented with the option to submit them to Comodo for analysis:



After sending the file to Comodo, our technicians determine whether or not it represents a threat to your security. If it is found to be trustworthy, it is added to the Comodo safe list. You can also directly submit the files to Comodo from this area.

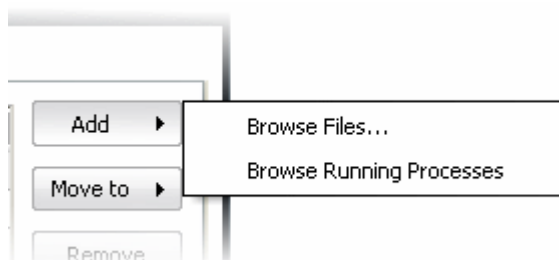
## To manually submit the files to Comodo

Select the file from the list and click 'Submit'...

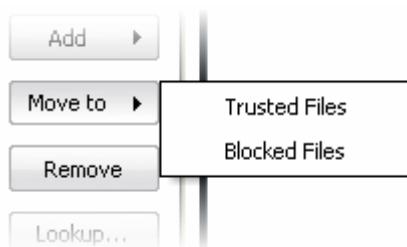


You will see a progress of file submission and on completion, the submission results will be displayed. You can see the file under Submitted files tab.

You can manually add files to the 'Unrecognized Files' list by clicking the 'Add..' button and either browsing to their location on your hard drive or selecting a running process:



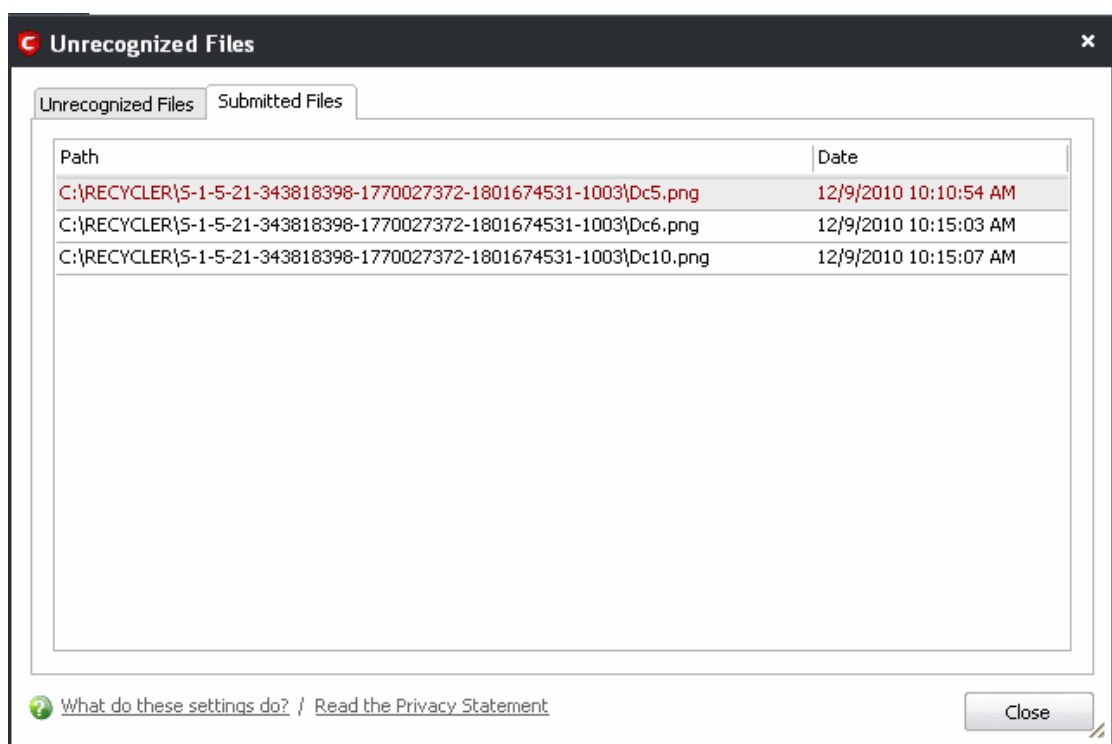
The 'Move to...' option allows you to transfer the files out of the 'My Pending Files' area and into either the **Trusted Files** or **Blocked Files** areas of Defense+:



Files can also be transferred *into* this module by clicking the 'Move to...' button in the 'Trusted Files' area.

## 4.4.2 Submitted Files

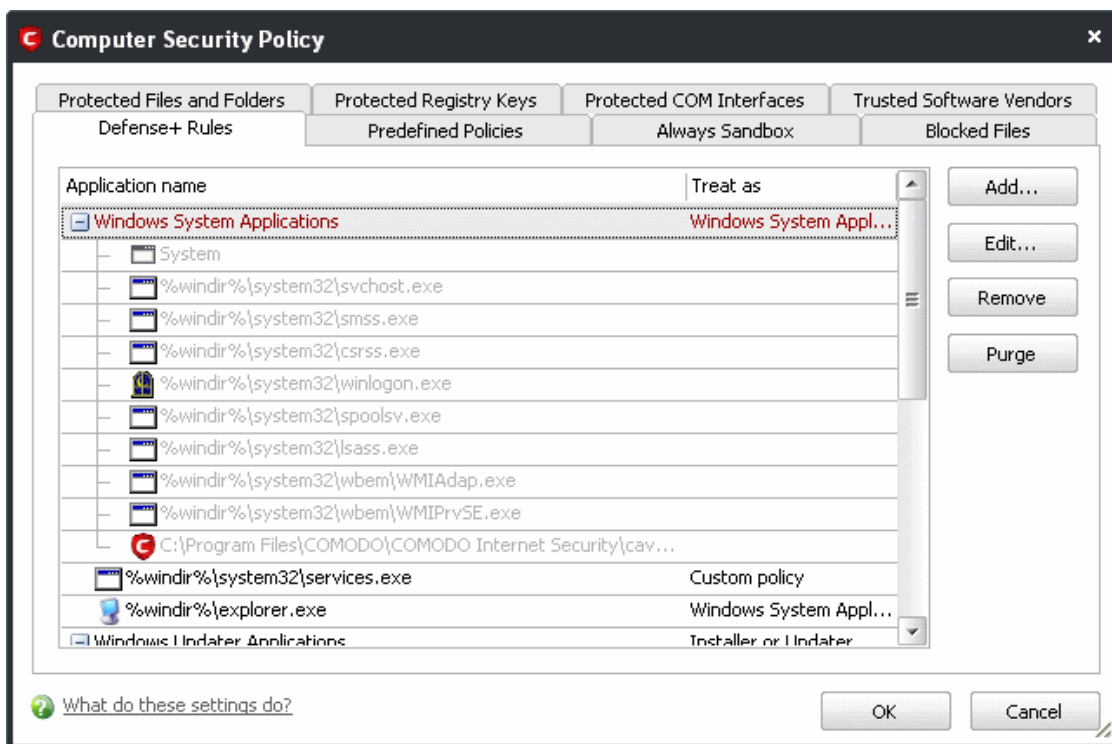
The Submitted files tab in the Unrecognized Files area displays a list of files submitted to Comodo for analysis, both from the [Defense+ Tasks > Unrecognized Files](#) area and [Antivirus tasks > Submit Files](#) area.



## 4.5 Computer Security Policy

The Computer Security Policy area allows the user to view manage and edit the Defense+ security policies that apply to applications, Predefined Security Policies, define protected Files and Folders, Registry Keys, COM interfaces, files to be always sandboxed or blocked, define a list of Trusted Software Vendors etc.

To access the Computer Security Policy area, click [Defense+ Tasks > Computer Security Policy](#).

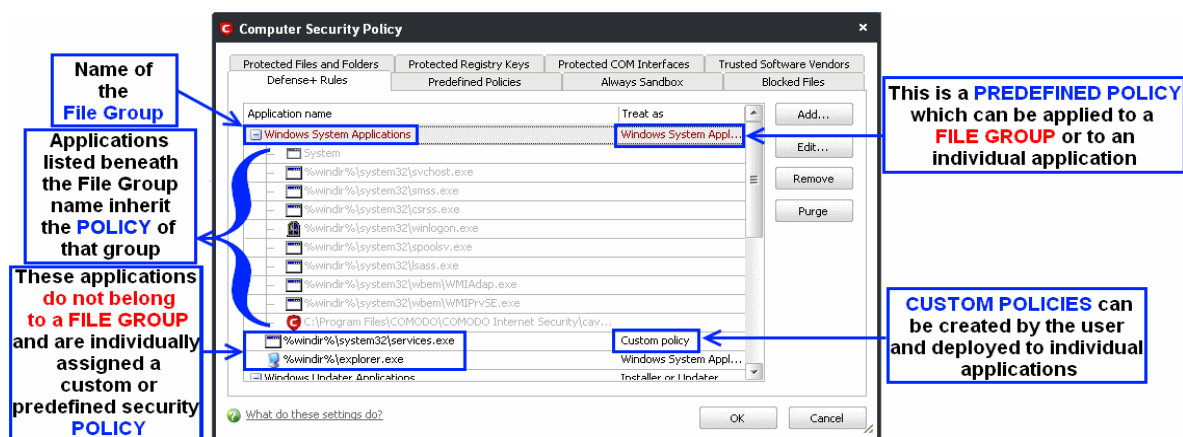


The Computer Security Policy area contains the following tabs:

- **Defense+ Rules**
- **Predefined Policies**
- **Always Sandbox**
- **Blocked Files**
- **Protected Files and Folders**
- **Protected Registry Keys**
- **Protected COM Interfaces**
- **Trusted Software Vendors**

## 4.5.1 Defense+ Rules

The Defense+ Rules tab lists the different groups of applications installed in your system and the security policies applied to them. You can change the policy applied to selected applications and also create custom policies to be applied to selected applications.



The first column, **Application Name**, displays a list of the applications on your system for which a security policy has been deployed. If the application belongs to a file group, then all member applications assume the security policy of the file

group. The second column, **Treat as**, column displays the name of the security policy assigned to the application or group of applications in column one.

#### General Navigation:

- **Add...** - Allows the user to Add a new Application to the list then create it's policy. See the section '[Creating or Modifying a Defense+ Security Policy](#)'.
- **Edit...** - Allows the user to modify the Defense+ security policy of the selected application. See the section '[Creating or Modifying a Defense+ Security Policy](#)'.
- **Remove** - Deletes the current policy.

**Note:** You cannot remove individual applications from a file group using this interface - you must use the '[My File Groups](#)' interface to do this.

- **Purge** - Runs a system check to verify that all the applications for which policies are listed are actually installed on the host machine at the path specified. If not, the policy is removed, or 'purged', from the list.

Users can re-order the priority of policies by simply dragging and dropping the application name or file group name in question. To alter the priority of applications that belong to a file group, you must use the '[My File Groups](#)' interface.

## Creating or Modifying a Defense+ Security Policy

### To begin defining an application's Defense+ policy

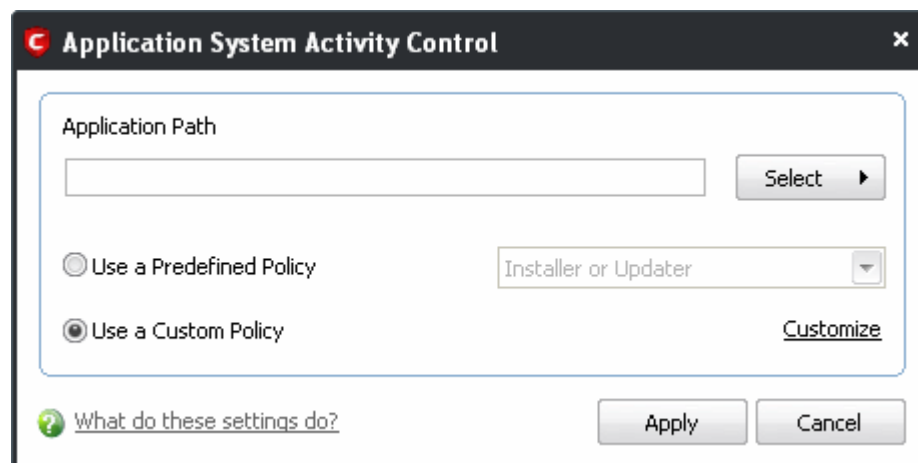
(1) Select the application or file group that you wish the policy to apply to.

(2) Configure the security policy for this application.

(1) Select the application or file group that you wish the policy to apply to

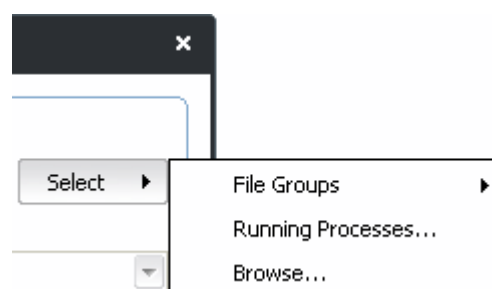
If you wish to define a policy for a new application (i.e. one that is not already listed), click the 'Add...' button in the main [Defense+ Rules interface](#).

This brings up the 'Application System Activity' Control interface shown below.



Because you are defining the Defense+ security settings for a new application, you can notice that the 'Application Path' box is blank. (If you were editing an existing policy instead, then this interface would show that policy's name and path.)

Click 'Select' to begin.





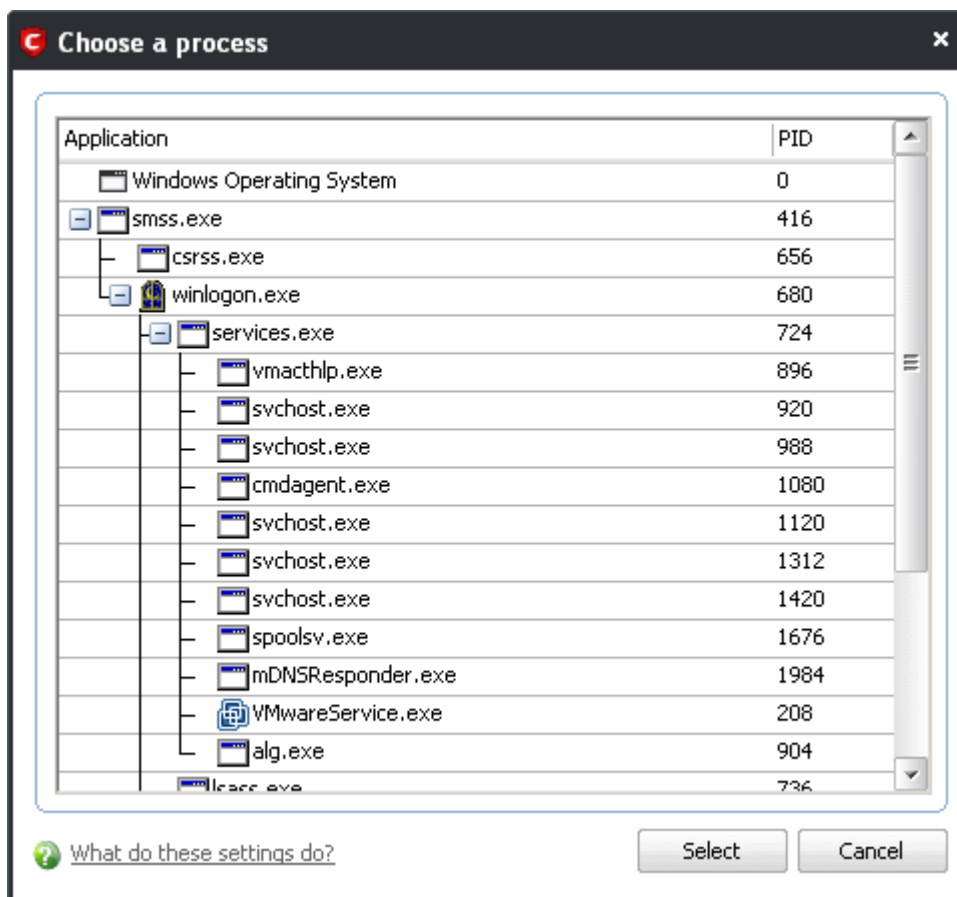
You now have 3 methods available to choose the application for which you wish to create a policy - **File Groups**; **Running Processes** and **Browse**.

1. **File Groups** - choosing this option allows you to create a Defense+ security policy for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Defense+ policy 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 policy 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 'My File Groups' interface.

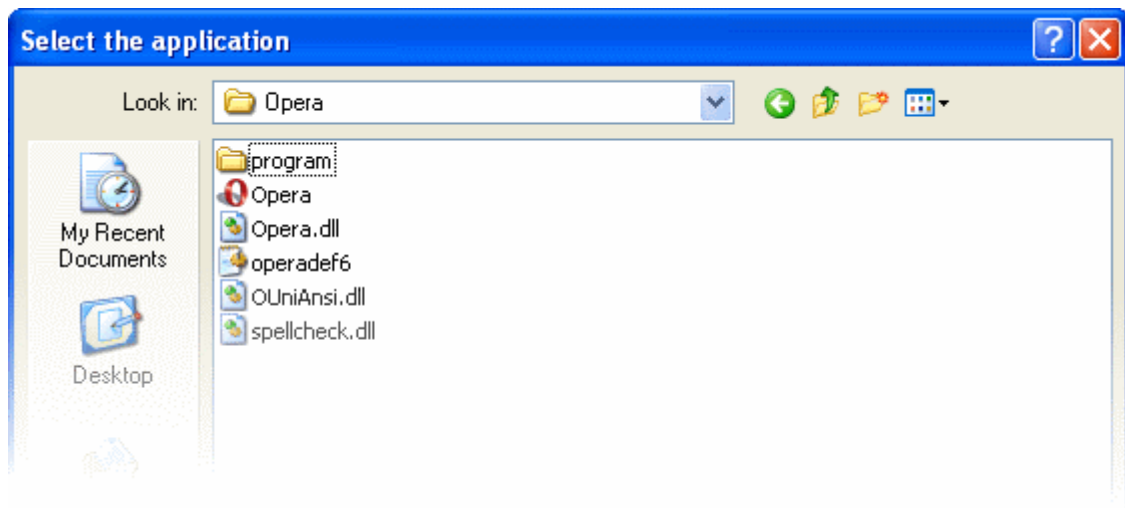
The 'My File Groups' interface can be accessed either of the following methods:

- Navigate to **Defense+ > Computer Security Policy > Protected Files and Folders** then click the 'Groups...' button.
- 2. **Running Processes** - as the name suggests, this option allows you to create and deploy a Defense+ policy 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 'Select' to confirm your choice.

3. **Browse...** - 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 Defense+ security policy.



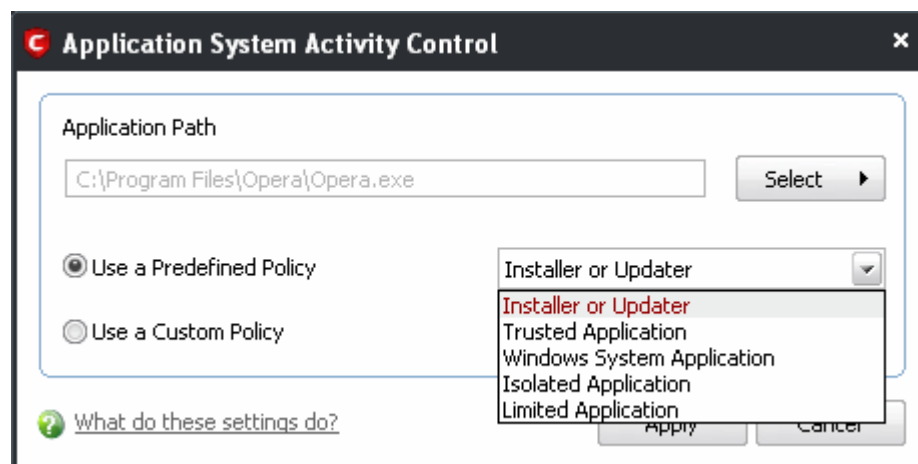
In the example below, we have decided to create a security policy for the Opera web browser.

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

## (2) Configure the security policy for this application

There are two broad options available for selecting a policy that applies to an application - **Use a Pre-defined Policy** or **Use a Custom Policy**.

1. **Use a Predefined Policy** - Selecting this option allows the user to quickly deploy a existing security policy on to the target application. Choose the policy you wish to use from the drop down menu. In the example below, we have chosen 'Limited Application'. The name of the predefined policy you choose is displayed in the 'Treat As' column for that application in the **Computer Security Policy** interface (*Default = Disabled*).

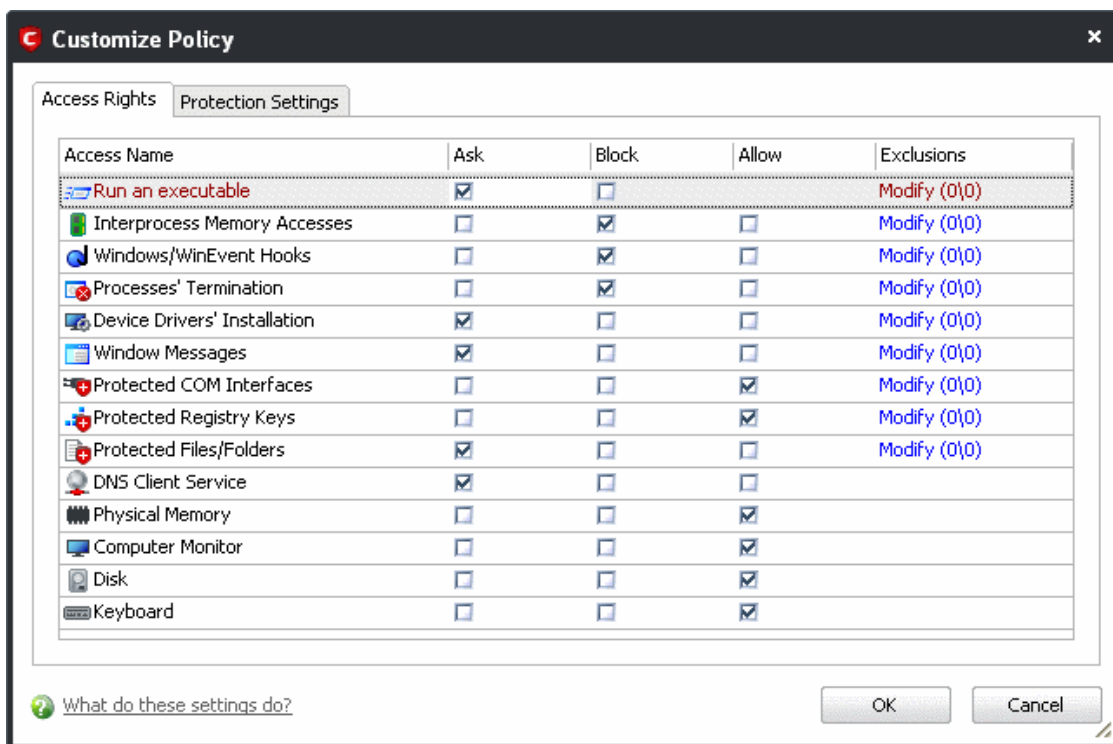


**Note:** Predefined Policies, once chosen, cannot be modified directly from this interface - they can only be modified and defined using the '**Predefined Policies**' interface. If you require the ability to add or modify settings for an specific application then you are effectively creating a new,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

2. **Use a Custom Policy**- designed for more experienced users, the 'Custom Policy' option enables full control over the configuration specific security policy and the parameters of each rule within that policy. The Custom Policy has two main configuration areas - **Access Rights** and **Protection Settings** (*Default = Enabled*).

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.

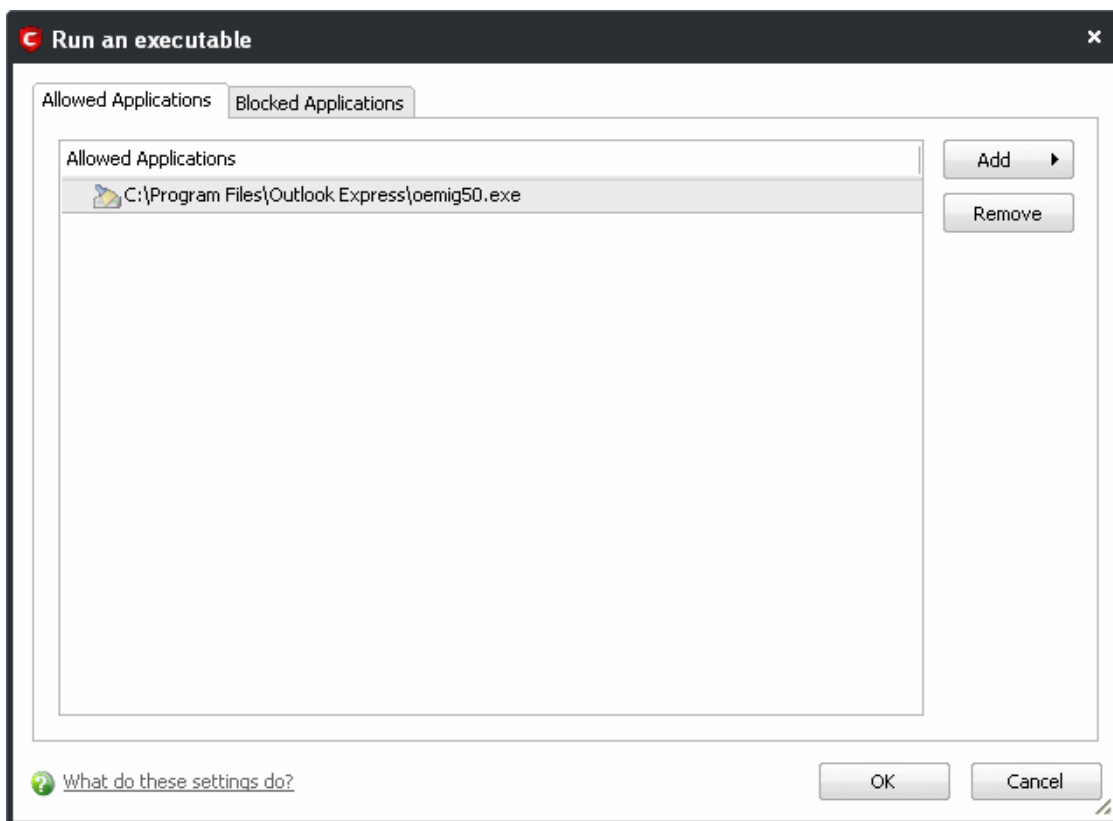
- i. **Access Rights** - The Process Access Rights interface allows you to determine what activities the applications in your custom policy are allowed to execute. These activities are called 'Access Names'.



Click [here](#) to view a list of definitions of the Action Names listed above and the implications of choosing to Ask, Allow or Block for each setting.

Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the policy by clicking the 'Modify' link on the right.:

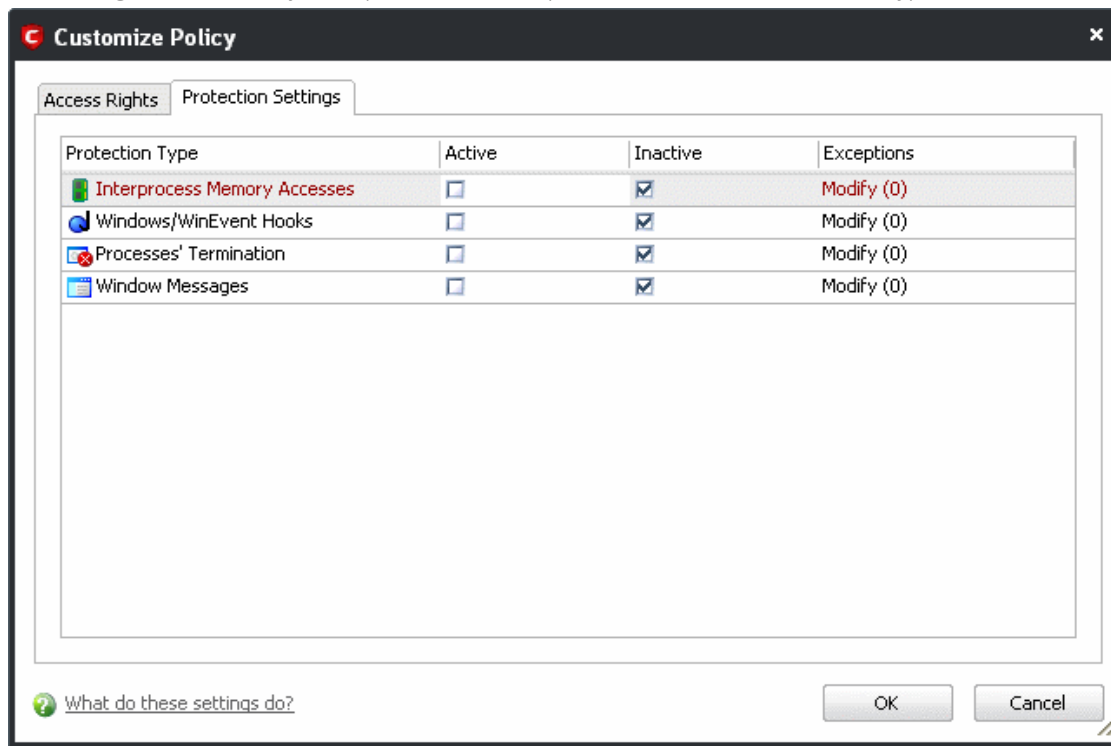
Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.



Clicking '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 'Run as an executable' is 'Ask'. This means Defense+ generates an alert asking your permission if 'Opera.exe' tried to run another program. Clicking 'Modify' then adding 'oemig50.exe' to the 'Allowed Applications' tab creates an exception to this rule. Opera.exe is now allowed to run 'oemig50.exe' but an alert is generated if it tries to run any other application.

- ii. **Protection Settings** - Protection Settings determine how protected the application or file group in your policy is *against* activities by other processes. These protections are called 'Protection Types'.



Select 'Yes' to enable monitoring and protect the application or file group against the process listed in the 'Protection Type' column. Select 'No' 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 'Yes' or 'No' can be specified in the application's policy by clicking the 'Modify...' button on the right.

3. Click 'Apply' to confirm your setting.

## 4.5.2 Predefined Policies

As the name suggests, a predefined computer security policy is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications. Each policy is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined Policies' is a set of policies that concern an application's access rights to memory, other programs, the registry etc.

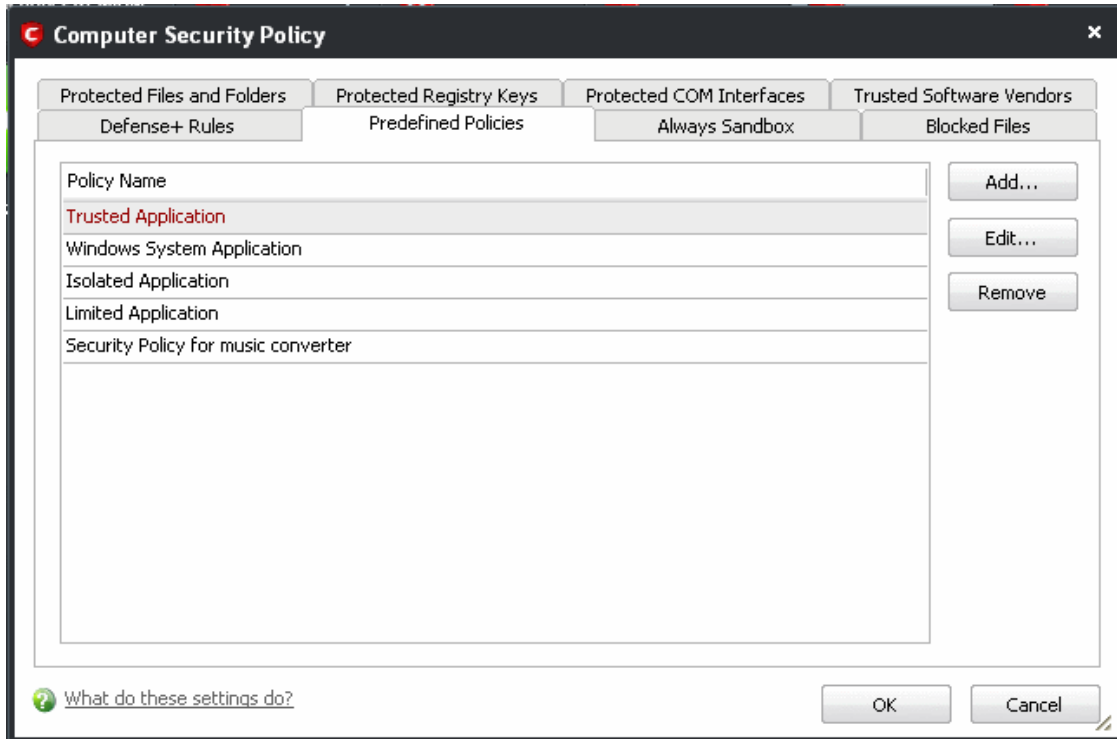
**Note:** This section is for advanced and experienced users. If you are a novice user to Comodo Internet Security, we advise you first read the **Computer Security Policy** section in this help guide if you have not already done so.

Although each application's security policy 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 predefined policies according to broad application categories. Each predefined policy 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.

### To configure this category

- Navigate to: Defense+ Tasks > Computer Security Policy > Predefined Policies. There are four default

security policies listed under the Policy Name column.



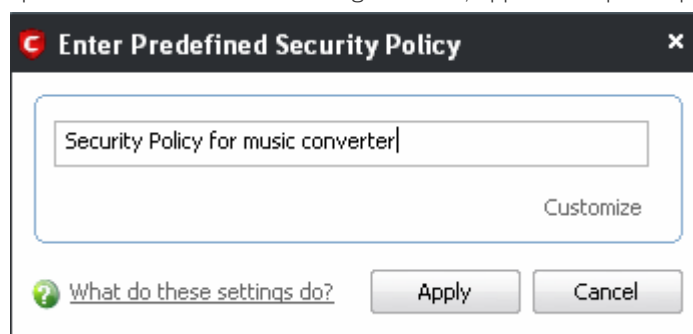
### To view or edit an existing predefined policy

1. Double click on the Policy Name in the list or
2. Select the Policy Name in the list, right-click and choose 'Edit' or
3. Select the Policy Name and click the 'Edit...' button on the right.

From here, you can modify a policy's name and, if desired, make changes to its **'Access Rights'** and **'Protection Settings'**. Any changes you make here are automatically rolled out to all applications currently under that policy.

### To create a new predefined policy

- Click the 'Add...' button, type a name for the policy, click 'Customize' link and then follow the same configuration procedure as outlined for creating a custom, application specific policy. [Click here to view.](#)



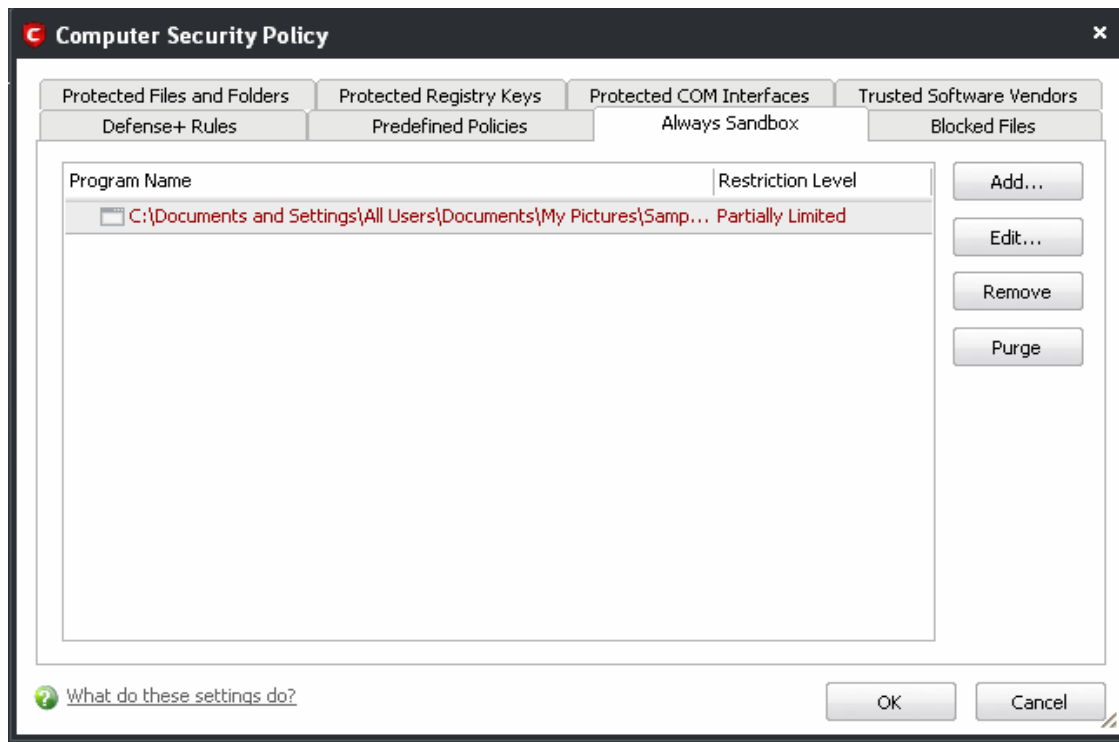
Once created, your policy is available for deployment onto specific application or file groups via the **Computer Security Policy** section of Defense+.

## 4.5.3 Always Sandbox

The 'Always Sandbox' area lists those applications which the user has decided should be executed in the sandbox on a permanent or long term basis. This may include applications that the user suspects are not safe or has other concerns about (for example, you could test beta software by running it in the sandbox). These applications will appear as normal programs in your system but will be run in the sandbox under a restricted set of privileges. They will not be allowed to access files on your real system, alter operating system settings or alter the registry entries corresponding to other

applications

To open the 'Always Sandbox' interface, Click Defense+ > Computer Security policy > Always Sandbox.

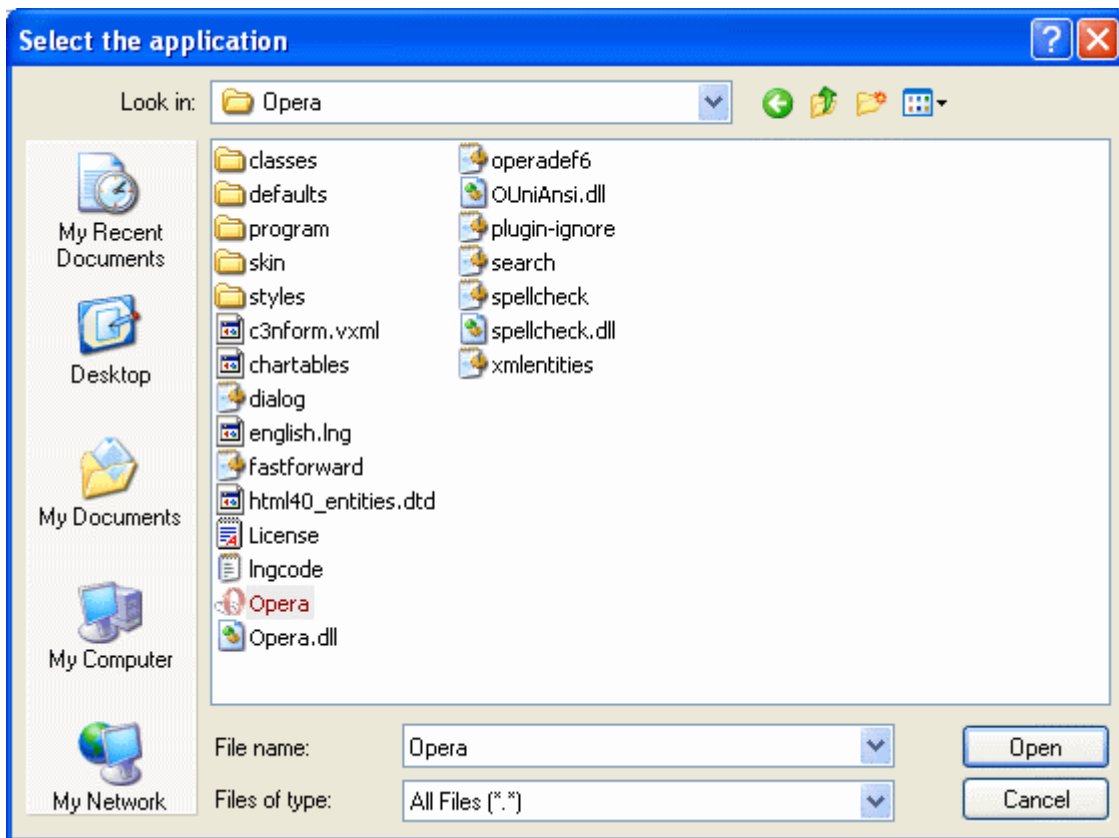


## To (permanently) add programs into the sandbox

1. Click 'Add...' from the 'Always Sandbox' interface. This will open the 'Add a Program to Sandbox' dialog.
2. Click 'Select' and browse to the file or currently running process that you wish to sandbox.



3. Click 'Open'. In the example below, we are adding opera.exe.



4. Choose 'Restriction Settings'

- i. **Untrusted** - The application is not allowed to access any of the 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. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** are imposed.

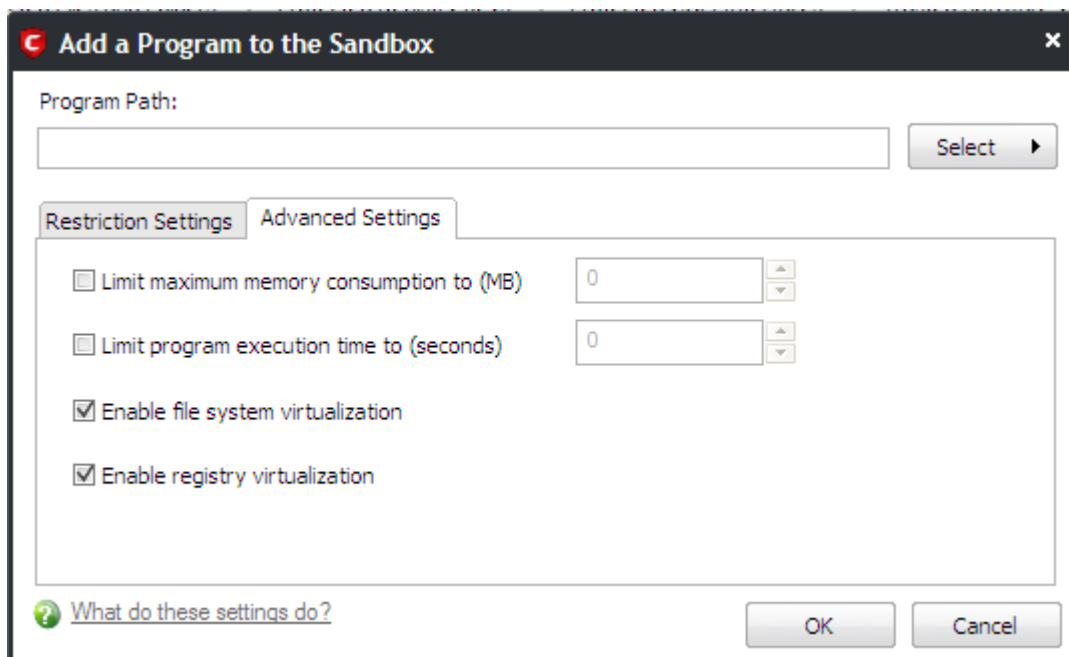
**Note:** Some of the applications that require user interaction may not work properly under this setting.

- ii. **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. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** are imposed.

**Note:** Some of the applications like computer games may not work properly under this setting.



- iii. **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 with out Administrator account privileges. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** are imposed.
  - iv. **Partially Limited (Default)** - The application is allowed to access all the Operating system files and resources like clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. The restrictions on usage of system memory, operation with virtual file system and registry and execution time defined in **Advanced Settings** are imposed.
5. Choose 'Advanced Settings'



The Advanced Settings tab to configure the restrictions on system resource usage and access to other files. Available options are:

- i. **Limit maximum memory consumption** - You can define how much of the system memory can be allocated for the application on execution by selecting this checkbox and entering the memory (in MB) in the combo box beside it (**Default = Disabled**).
- ii. **Limit the program execution time** - You can define how long the program can be allowed to run by selecting this checkbox and entering the time (in seconds) in the combo box beside it (**Default = Disabled**).
- iii. **Enable file system virtualization** -The sandboxed applications are not permitted to modify the files in your 'real' file system. Enabling file system virtualization instructs the Sandbox to create a virtual file system in your system. The application added to the sandbox writes any data only into the created virtual file system, instead of affecting and potentially causing damage to your real file system. If you disable this option, the application may not function correctly because it is not be to create the entries that it needs too (**Default = Enabled**).

**Note for advanced users:** The virtual file system is created inside the Sandbox working folder (e.g. c:\sandbox\

The virtual file system is not created even on enabling this setting here, if file system virtualization is disabled in **Sandbox Settings**.

- iv. **Enable registry virtualization** - The sandboxed applications are not permitted to access and modify the entries in your 'real' Window's Registry hives. Enabling registry virtualization instructs the Sandbox to create a virtual registry hive in your system. The application added to the Sandbox writes any entries pertaining to it only into the created registry hive, instead of affecting and potentially causing damage to your real registry hives. If you disable this option, the application may not function correctly because it is not able to create the entries that it needs too (**Default = Enabled**).

**Note for advanced users:** The virtual registry hive is created as HKEY\_LOCAL\_MACHINE\SYSTEM\Sandbox\ ... for the

sandboxed applications to write their registry values.

The virtual registry hive is not created even on enabling this setting here, if registry virtualization is disabled in **Sandbox Settings**.

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

From this point onwards the application will be run in the sandbox. If you wish to remove it at a later date, simply highlight it in the list and click 'Remove'. If you wanted to run an application in the sandbox on a 'one off' basis instead, then please use **'Run a Program in the Sandbox'** instead.

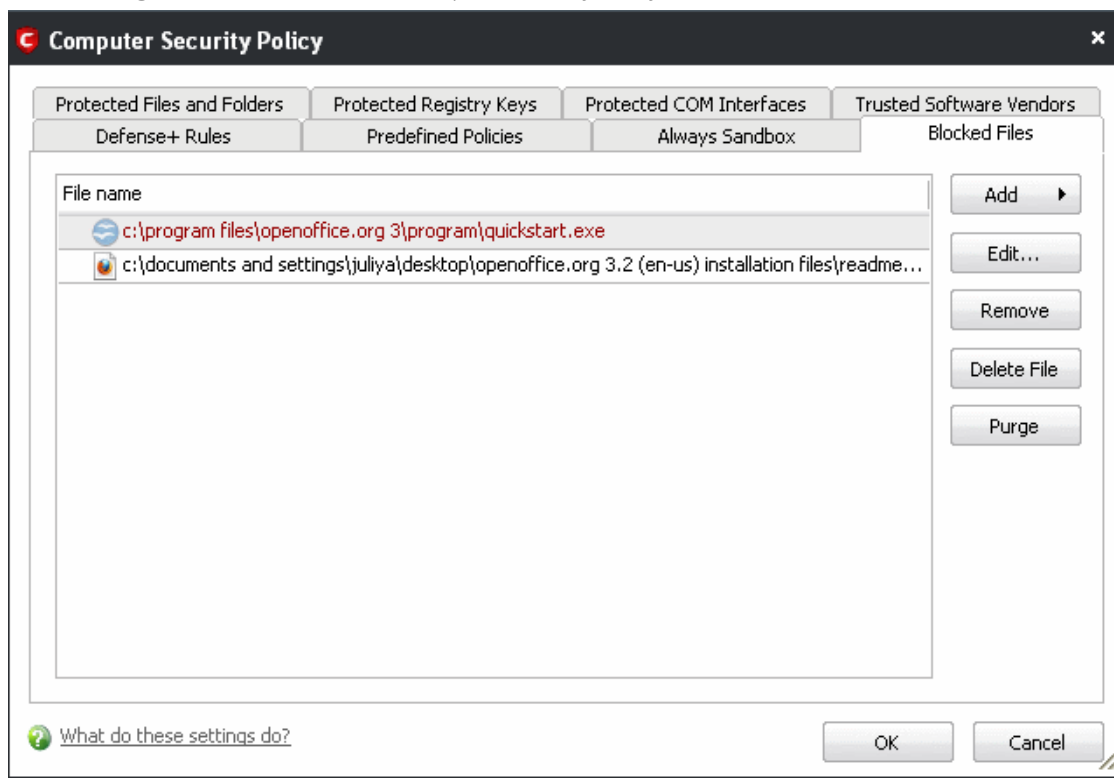
- To edit the restriction settings for an application included in the sandbox, select the application and click 'Edit'.
- To remove an application from the sandbox, select the application and select 'Remove'. Next time you execute this application it will run outside of the sandbox (presuming it is not then detected as malicious or automatically sandboxed as **per the sandboxing process**)
- To remove invalid entries (programs/files that are not present or uninstalled from your computer) automatically, click 'Purge'.

## 4.5.4 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 and Folders', users cannot selectively allow any process access to a blocked file.

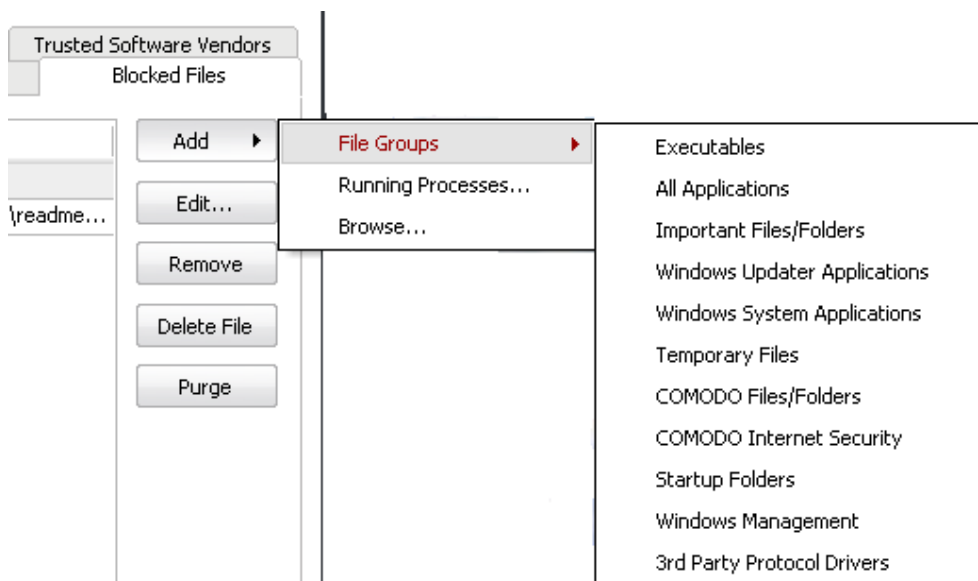
### To access Blocked Files interface

- Navigate to: Defense+ Tasks > Computer Security Policy > Blocked Files.



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

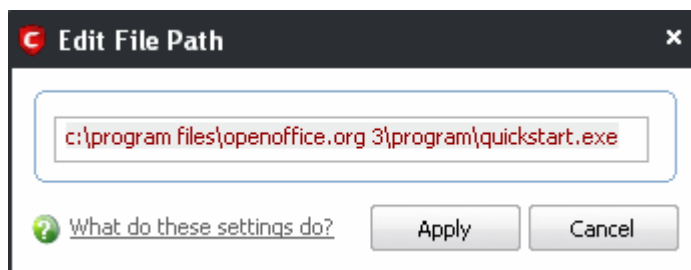
1. Click the 'Add' button. **Click here** for a description of the choices available when selecting a file.



Alternatively, files can be transferred *into* the My blocked Files module using the 'Move to' button in the '**Unrecognized Files**' and '**Trusted Files**' areas.

### To edit the file path of an included entry

1. Select the entry and click 'Edit' button. The 'Edit' dialog opens for changing the file path.



2. Alter the file path as required and click 'Apply'.

### To remove an included entry from Blocked Files

- Select the entry and click 'Remove' button. The file is only removed from the list and not deleted from your system.

### To permanently delete the individual file; file group or executable from your system

- Select the entry and click 'Delete File' button.

### To remove invalid entries (programs / files that are not present or uninstalled from your computer) automatically,

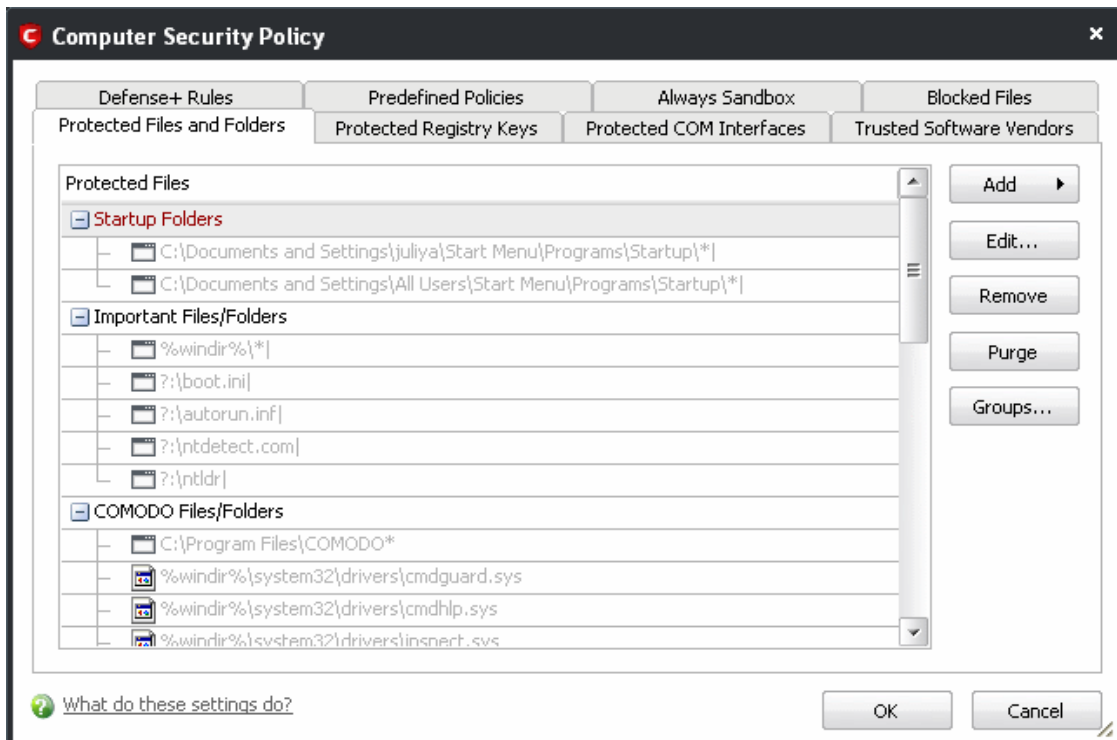
- Click 'Purge' button.
- Click 'OK' to implement your settings.

## 4.5.5 Protected Files and Folders

Protected Files and Folders setting allows you to protect specific files and folders against unauthorized modification especially by 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

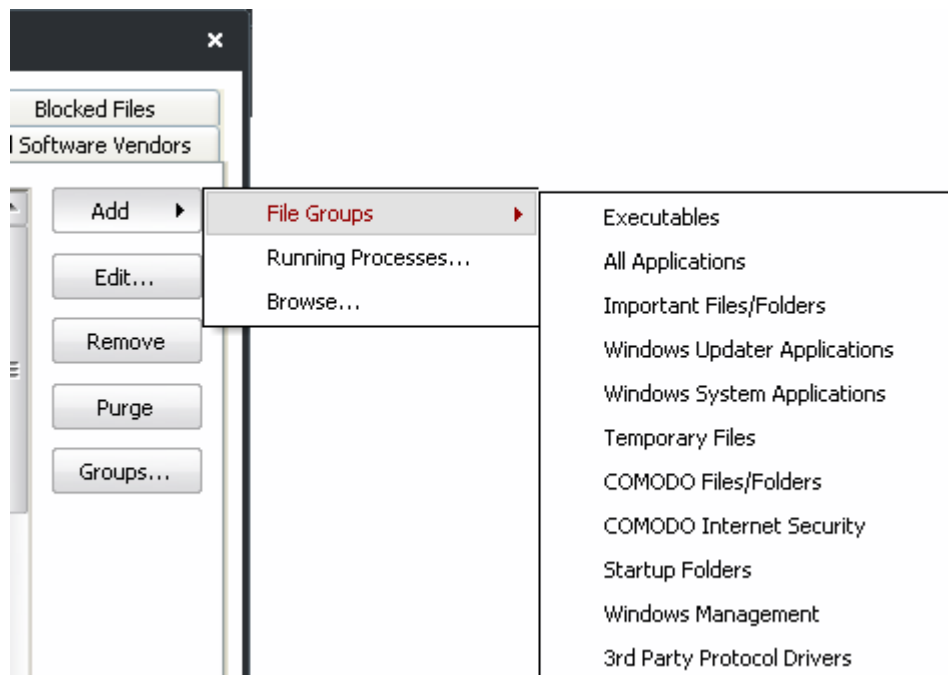
altered. A good example of a file that ought to be protected is the your 'hosts' file. (c:\windows\system32\drivers\etc\hosts). Placing this in the 'My Protected Files and Folders' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Internet Security blocks this attempt and produce a 'Protected File Access' pop-up alert.

To access My Protected Files, navigate to: Defense+ Tasks > Computer Security Policy > Protected Files and Folders.



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

1. Click the 'Add' button. [Click here](#) for a description of the choices available when selecting a file.



## Exceptions

Users can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate Access Right in 'Computer Security Policy'. 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 and

Folders' area by clicking the 'Add' button then 'Browse...' to 'Accounts.ods'. Once added to 'My Protected Files', you would go into 'Computer Security Policy' and create an exception for 'scal.exe' so that it alone could modify 'Accounts.ods'.

**1. First add Accounts.ods to Protected Files and Folders.**  
**2. Then go to Computer Security tab and add scal.exe to the list of applications and click "Edit".**

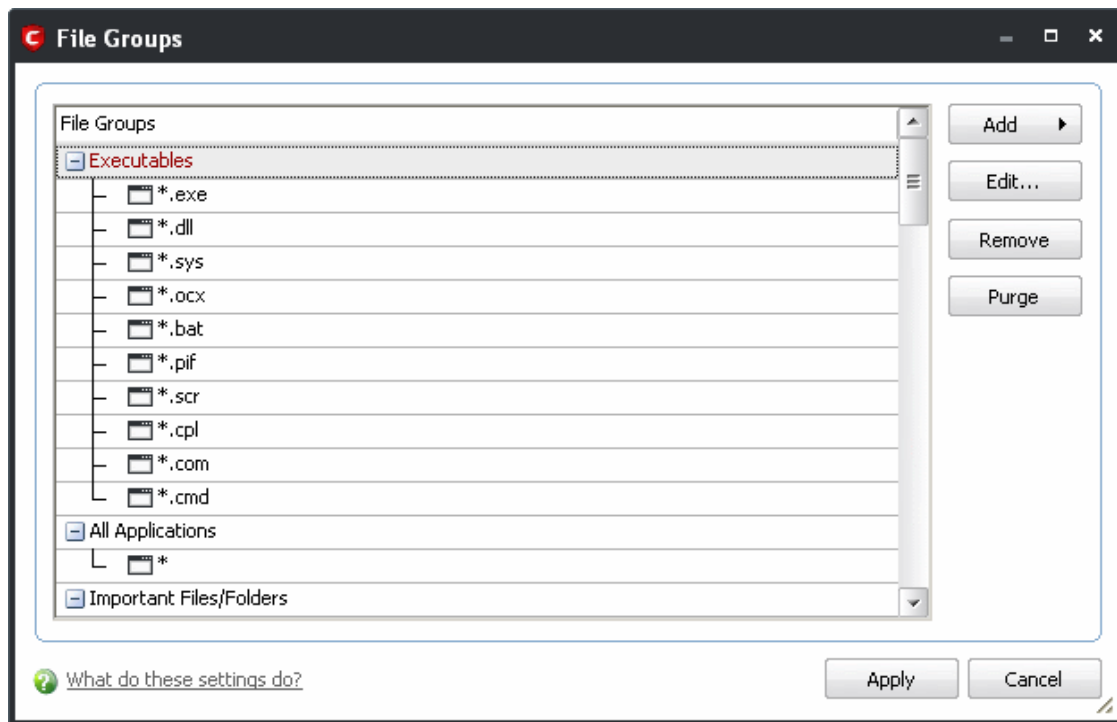
**3. Click the "Customize" link.**

**4. Under the "Access Rights" tab, click the link Modify beside the entry Protected Files/Folders.**

**5. Under the "Allowed Files/Folders" tab, click "Add" then "Browse...". Add "Accounts.ods" and an exception 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 and Folders' area (\* = all files in this directory). Next go to 'Computer Security Policy', 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.

The 'Groups...' button allows the user to access the 'File Groups' interface.



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

This interface allows you to

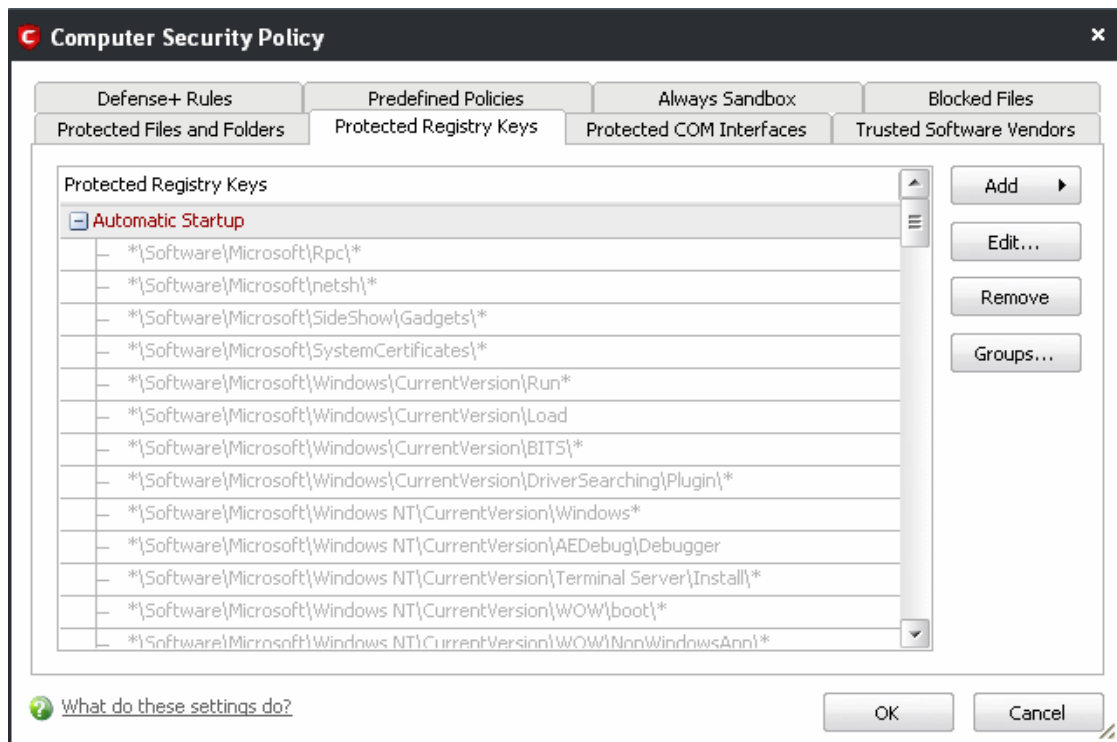
- Create a new File Group by clicking the 'Add' button.
- Edit the names of an Existing File Group or File by right-clicking and selecting the 'Edit' button.
- Add a file to an existing file group by selecting the File Group name from the list then clicking Add > Select From >....'
- Re-assign files to another file group by dragging and dropping.

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

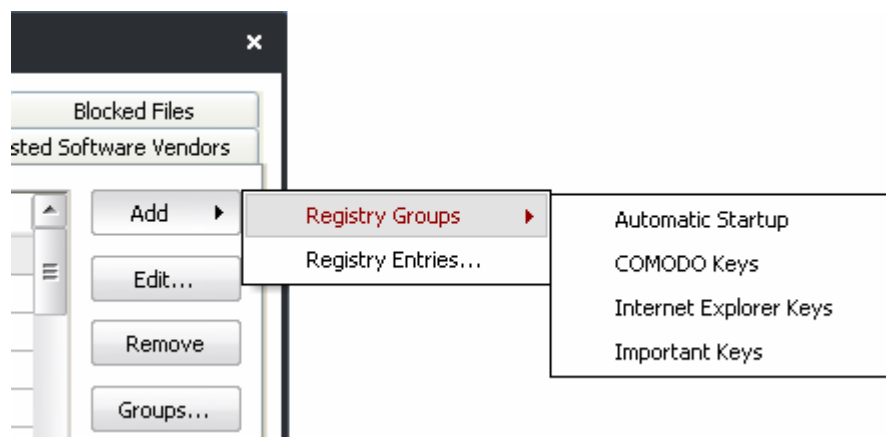
## 4.5.6 Protected Registry Keys

Comodo Internet Security automatically protects 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 attack.

In order to access Protected Registry Keys interface, navigate to: Defense+ Tasks > Computer Security Policy > Protected Registry Keys.



You can import additional registry keys that you wish to protect by clicking the 'Add' button:

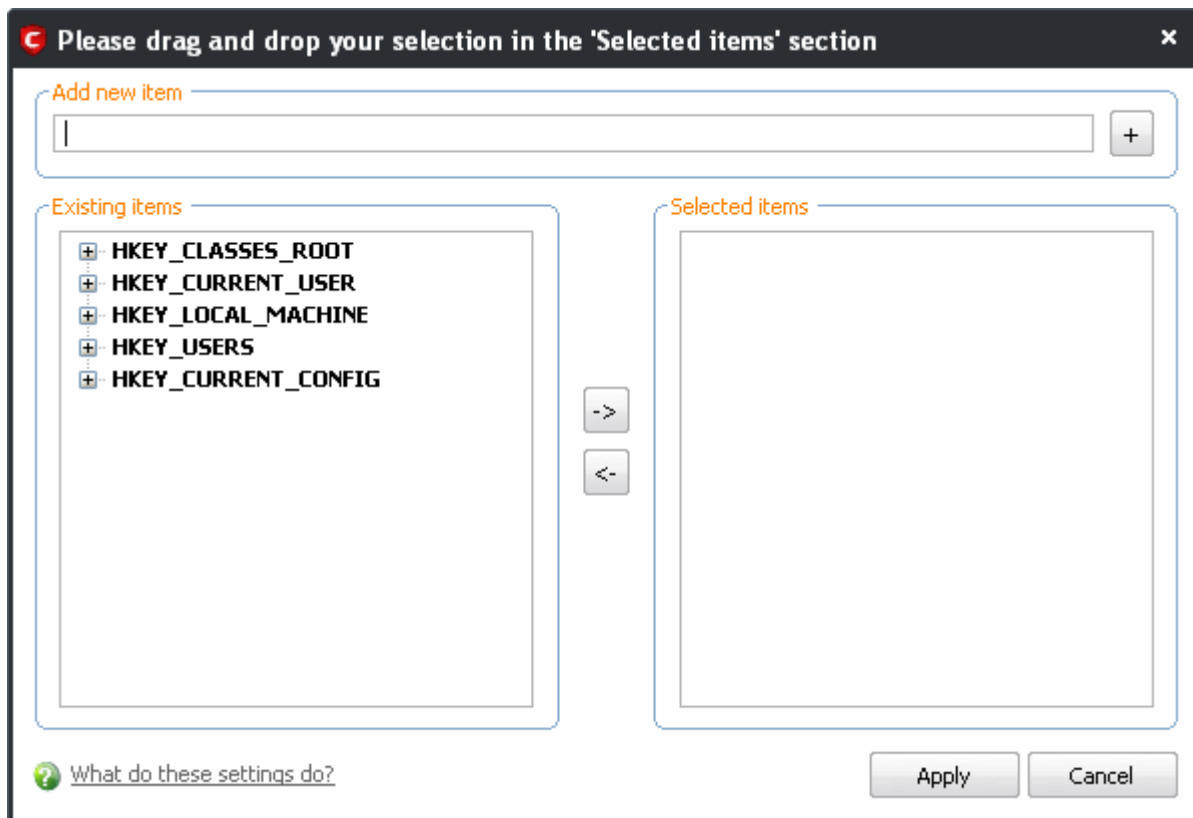


The 'Registry Groups' option allows you to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'.

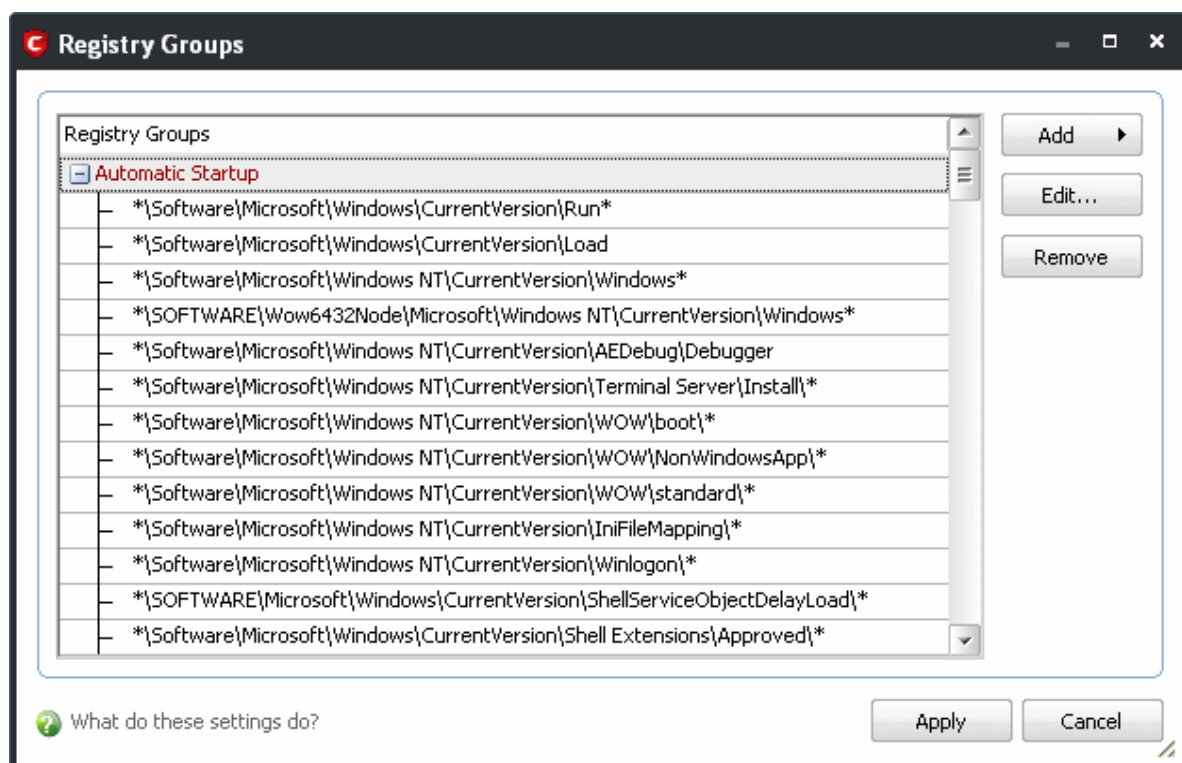
The 'Registry Entries...' option opens the Windows registry editor within the Comodo Internet Security interface and allow you to select individual keys.

You can add items manually by browsing the registry tree in the right hand pane. Drag & drop specific registry keys into the 'Selected Items' pane. To add item manually enter its name in the field and press the '+' button.





The 'Groups...' button allows the user to access the 'My Registry Groups' interface.



Registry groups are handy, predefined groupings of important registry keys.

This interface allows you to:

- Create a new registry key Group by clicking the 'Add' button.
- Add keys to your new group by selecting the Registry Group name from the list then clicking 'Add > Select From > Registry Key...'
- Add keys to a pre-existing group by selecting its name from the list then clicking 'Add > Select From >

Registry Key...'

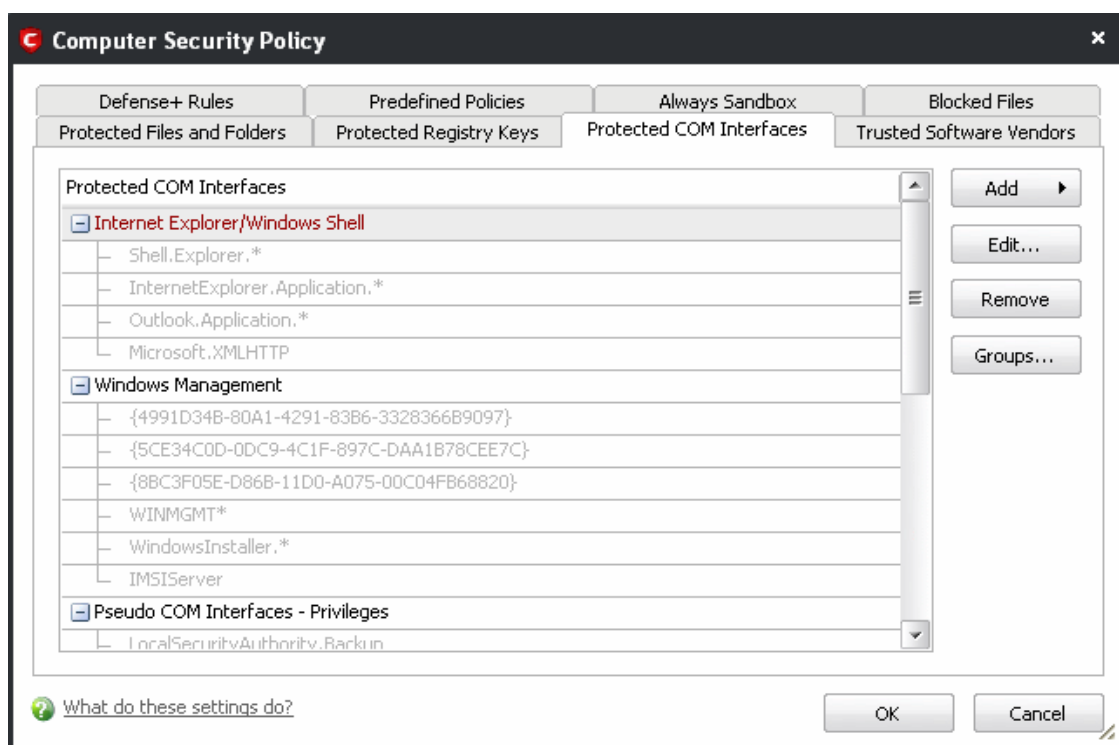
- Edit the names of existing registry key Group or individual key by right-clicking and selecting the 'Edit'.
- Re-assign registry keys to another group by dragging and dropping.

## 4.5.7 Protected COM Interfaces

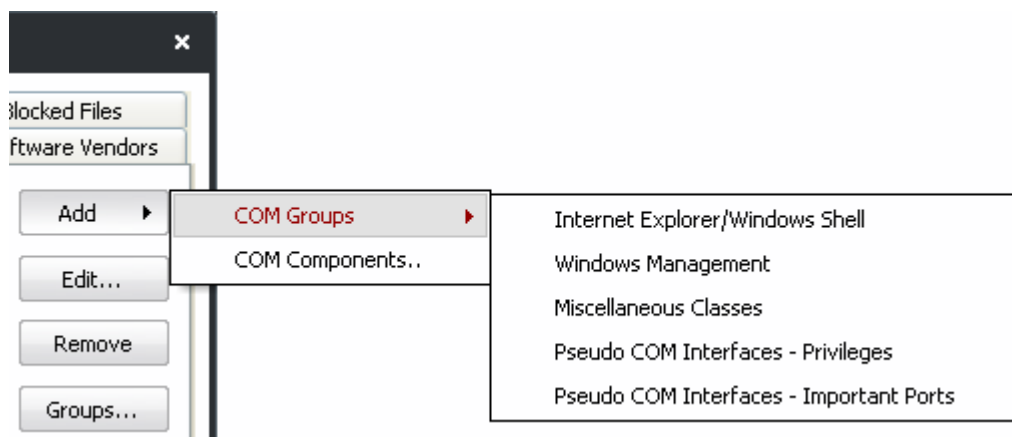
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers 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 modification, corruption and manipulation by malicious processes. The predefined **COM Interface groups** can be accessed by clicking the 'Groups...' button.

In order to access 'Protected COM Components' Interface, navigate to: Defense+ Tasks > Computer Security Policy > Protected COM Interfaces.

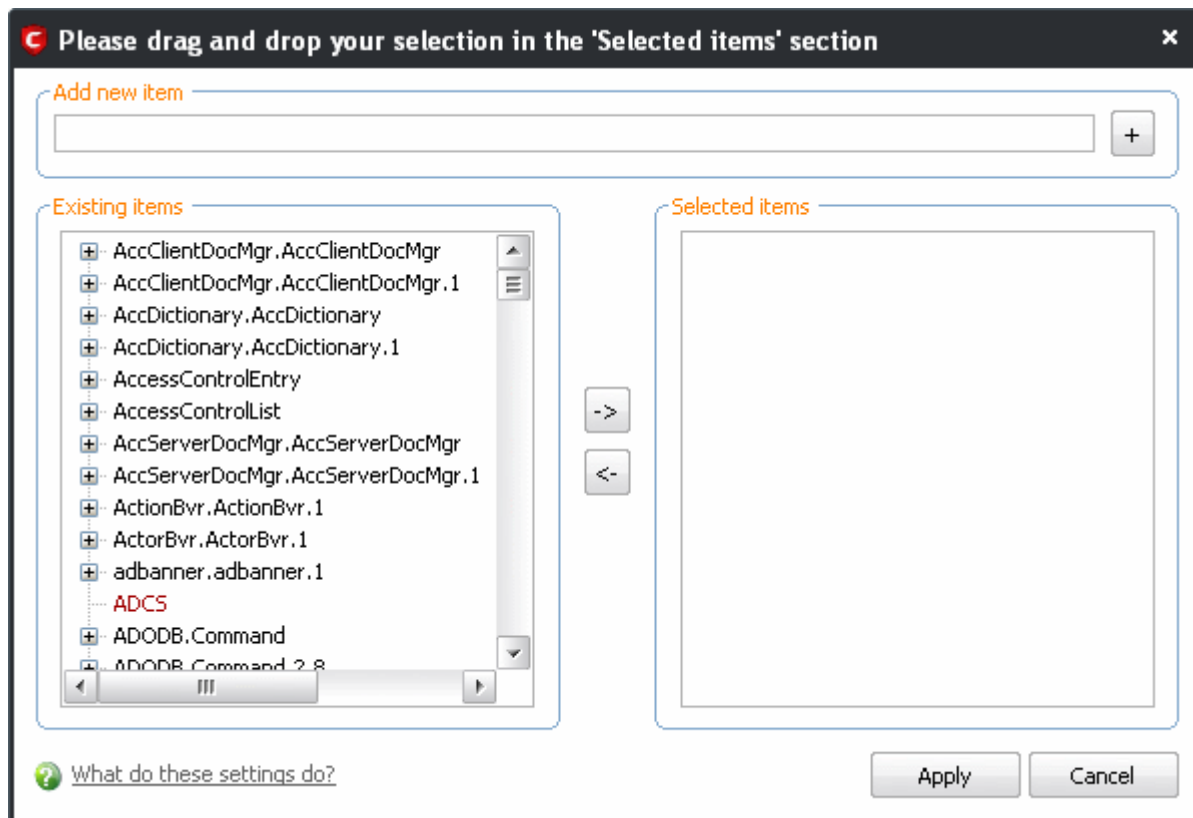


You can import additional COM interfaces that you wish to protect by clicking the 'Add' button.



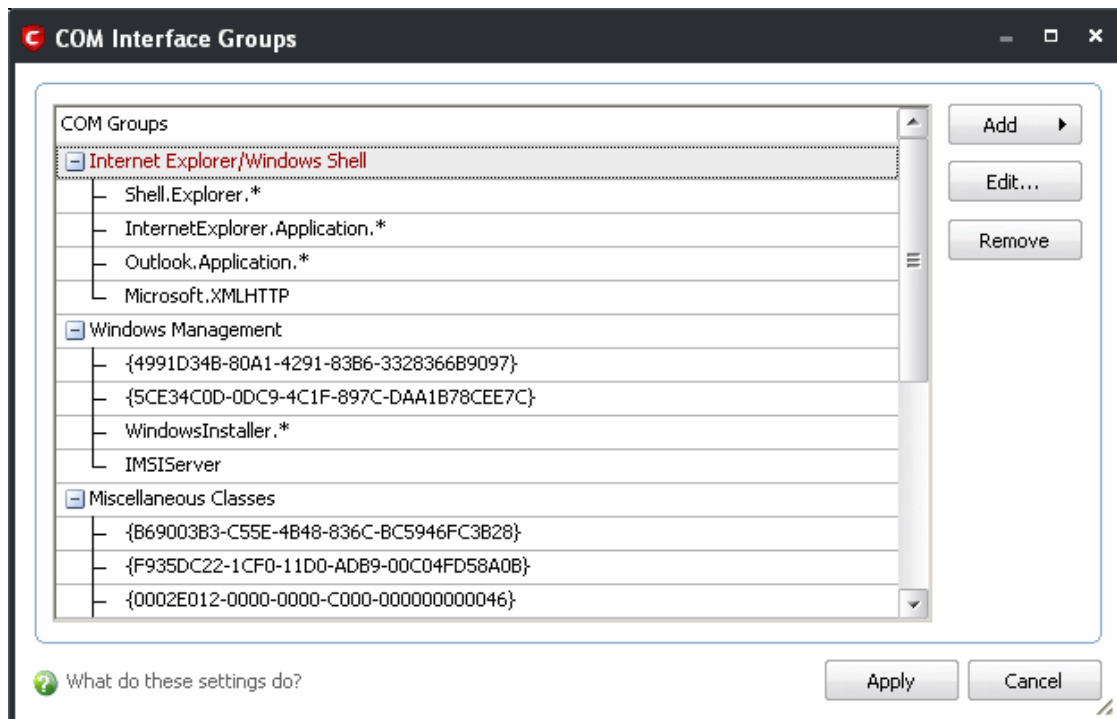
The 'COM Groups' option allows you to batch select and import predefined COM interfaces.

The 'COM Components...' option allows you to add individual COM components. You can add items manually by browsing the components in the right hand pane. Drag & drop specific components into the 'Selected Items' pane. To add manually add a component' enter its name in the field and press the '+' button.



### To access 'COM Interface Groups'

- Click on the 'Groups' button.



COM groups are handy, predefined groupings of COM interfaces.

This interface allows you to:

- Create a new COM Group by clicking the 'Add' button.
- Add components to your new group by selecting the group name from the list then clicking 'Add > Select From > COM components...'

- Add keys to a pre-existing COM group by selecting its name from the list then clicking 'Add > Select From > COM components...'
- Edit the names of existing COM Group or individual component by right-clicking and selecting 'Edit'.
- Re-assign COM components to another group by dragging and dropping.

## 4.5.8 Trusted Software Vendors

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 that are digitally signed by Trusted Software Vendors**' 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 that are digitally signed by Trusted Software 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' area can be opened by navigating to Defense+ Tasks > Computer Security Policy > Trusted Software 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 are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

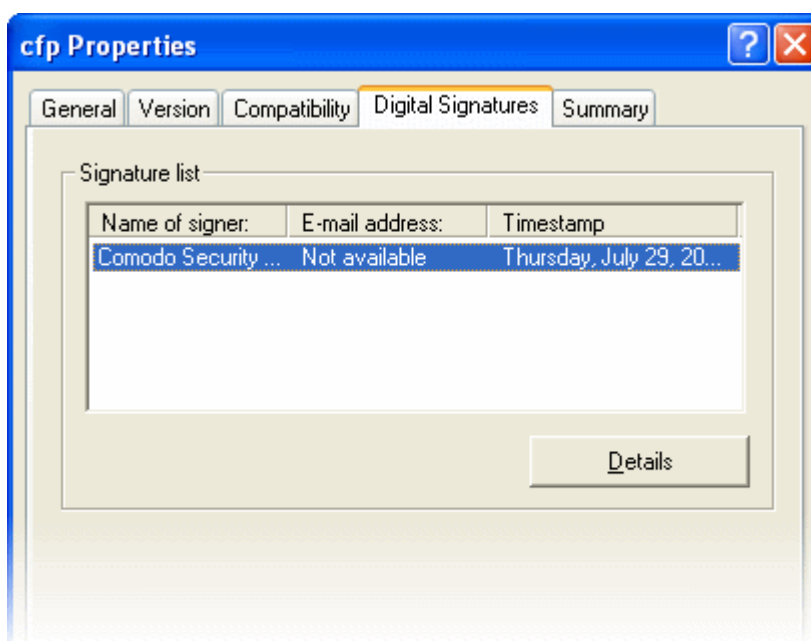
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Internet Security (if you would like to read more about code signing certificates, see <http://www.instantssl.com/code-signing/>).

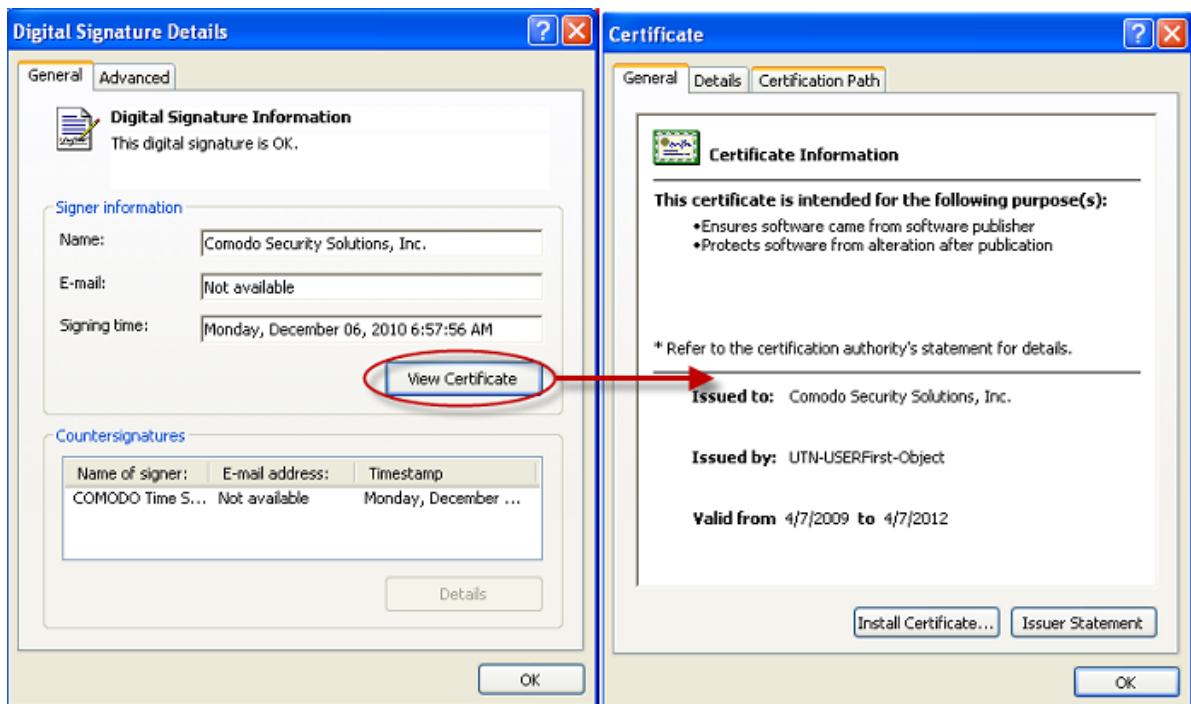
One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Internet Security is called 'cfp.exe' and has been digitally signed.

- 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)

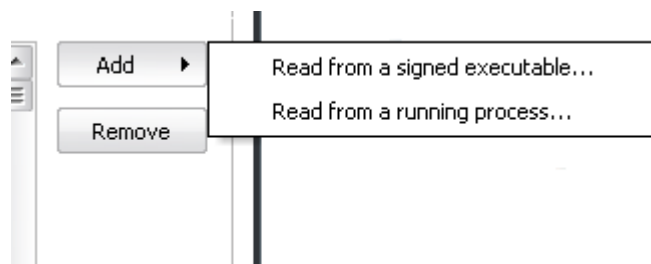


It should be noted that the example above is a special case in that Comodo, as creator of 'cfp.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different. [See this example](#) for more details.

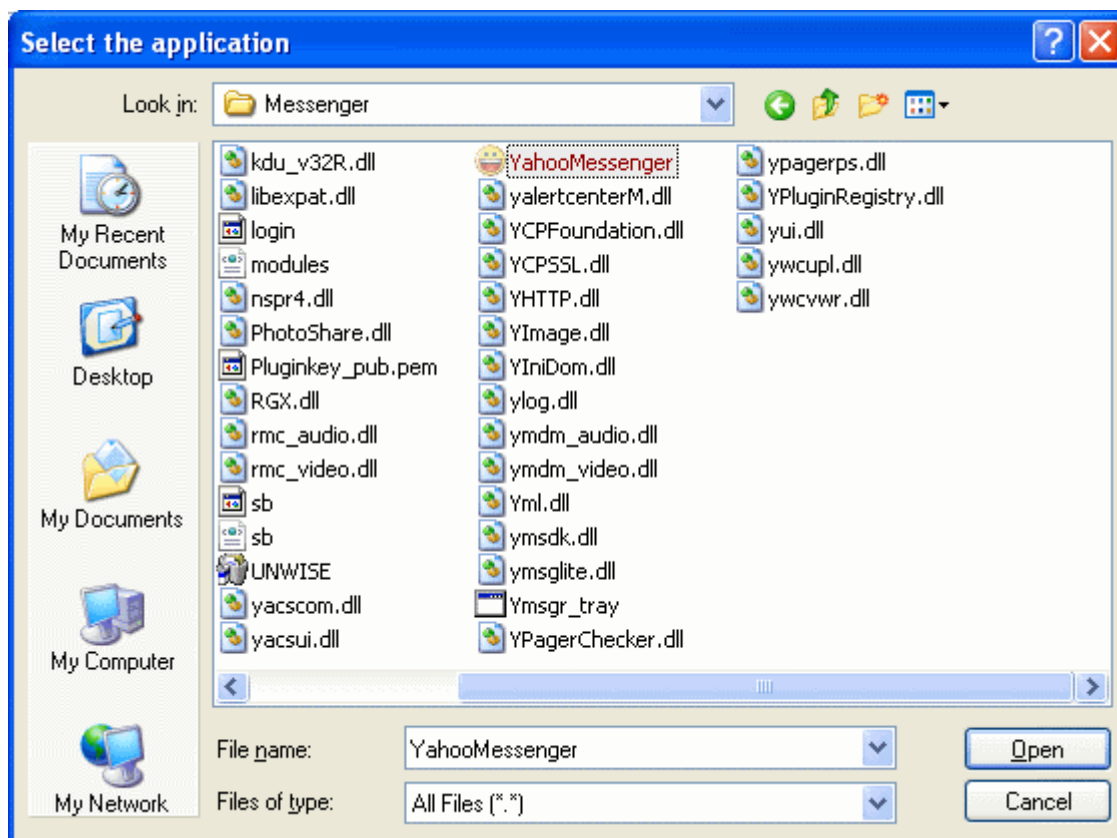
## Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

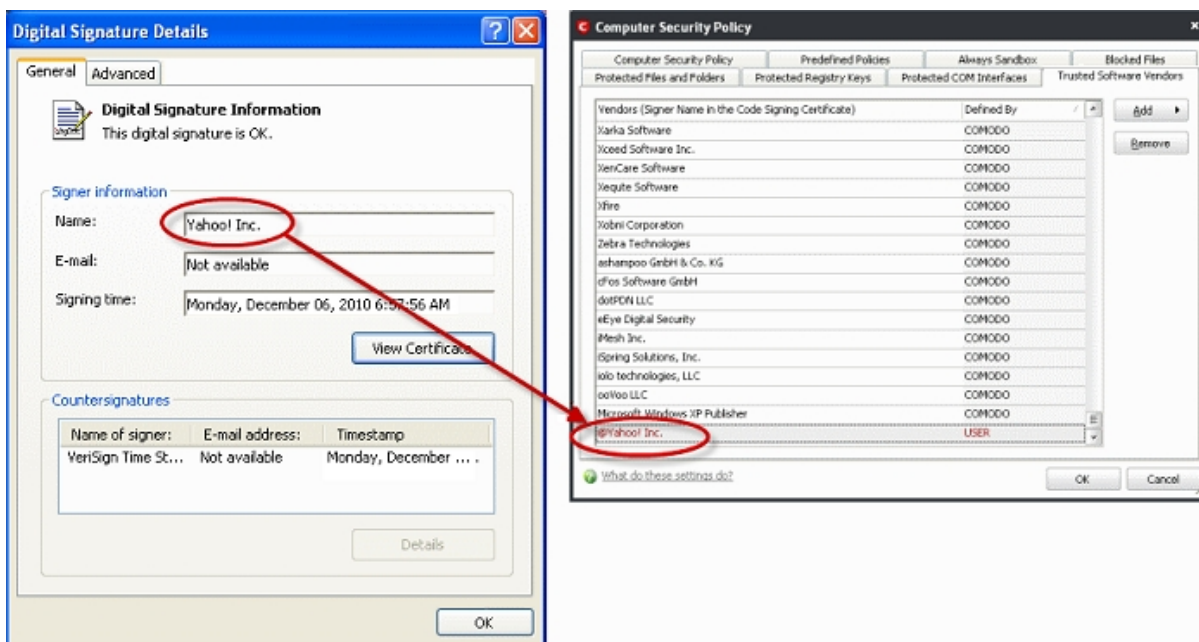
- By reading the vendor's signature from an executable file on your local drive
- By reading the vendor's signature from a running process



Click the add button on the right hand side and select 'Read from a signed executable...'. Browse to the location of the executable your local drive. In the example below, we are adding the executable 'YahooMessenger.exe'.



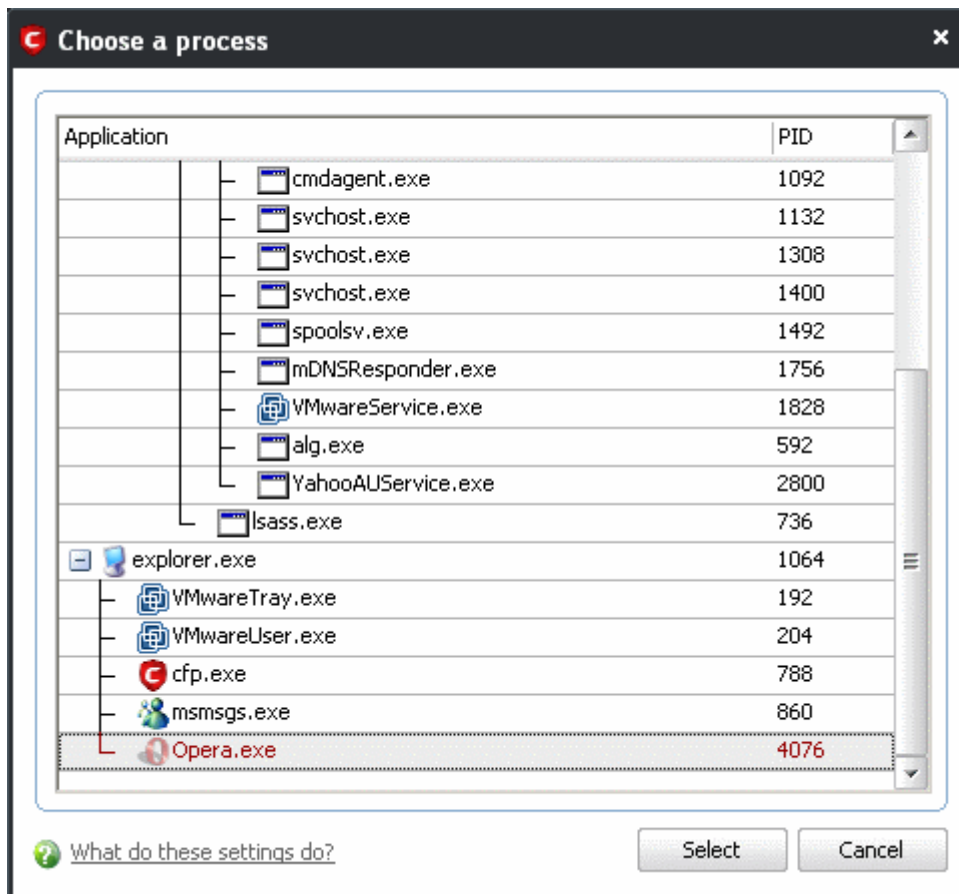
After clicking 'Open', Comodo Internet Security checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the Trusted Vendor list (TVL):



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 'Verisign'. 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 Defense+ Settings > General Settings**.

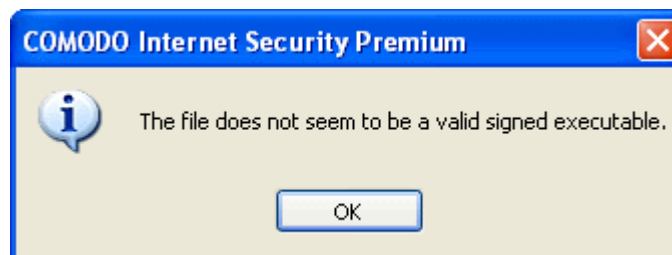
Comodo Internet Security also allows you to add a trusted vendor by selecting from processes that are currently running on your PC. To do this, click the 'Add...' button and select 'Read from a running process...':





Select the signed executable that you want to trust and click the 'Select' button. Comodo Internet Security performs the same certificate check as described above.

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 'My Trusted Vendors'. In this case, you can see the following error message.



**Note:** The 'My 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 a legitimate company. Comodo certified vendors are hard coded into CIS and cannot be removed by the user.

### 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>.

## 4.6 View Active Process List

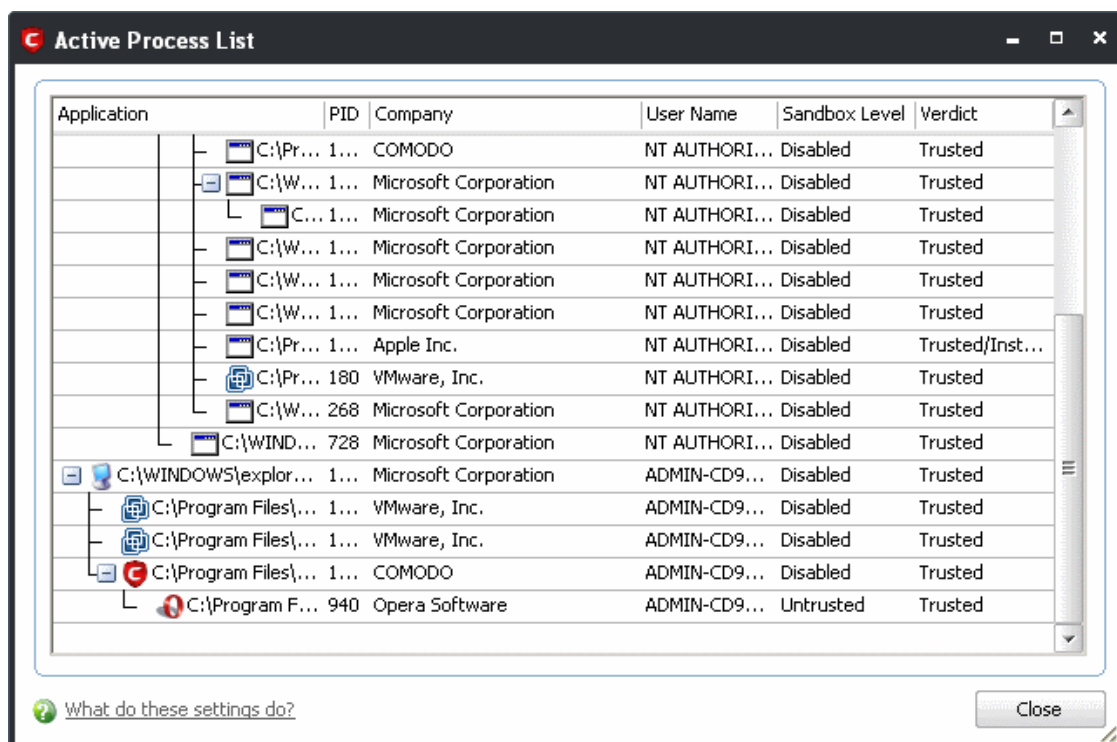
The **Active Process List** interface displays all currently active processes that are running on your PC and the parent application of those processes. By tracing an application's parent process, Defense+ can detect whether a non-trusted application is attempting to spawn an already trusted application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

### To view Active Process list

1. Navigate to Defense+ > Active Process List.

#### Column Descriptions

- **Application** - Displays the names of the applications which are currently running on your PC.
- **PID** - Process Identification Number.
- **Company** - Displays the name of the software developer
- **User Name** - The name of the user that started the process
- **Sandbox Level** - Displays the level of sandbox setting selected for the program
- **Verdict** - Displays whether the application is trusted or not.



Right click on any process to:

- **Show full path:** Displays the location on your location of the the executable in addition to it's name.
- **Show Sandboxed Only:** Displays the details of the sandboxed programs only.
- **Terminate:** Shuts down the currently selected process.
- **Terminate & Block:** Shuts down the currently selected process and places the executable into the **Blocked Files** section of Defense+.

- **Add to Trusted Files:** The selected program is added to Trusted Files list.
- **Online Lookup:** The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- **Submit:** The selected application will be sent to Comodo for analysis.

## 4.7 Run a Program in the Sandbox

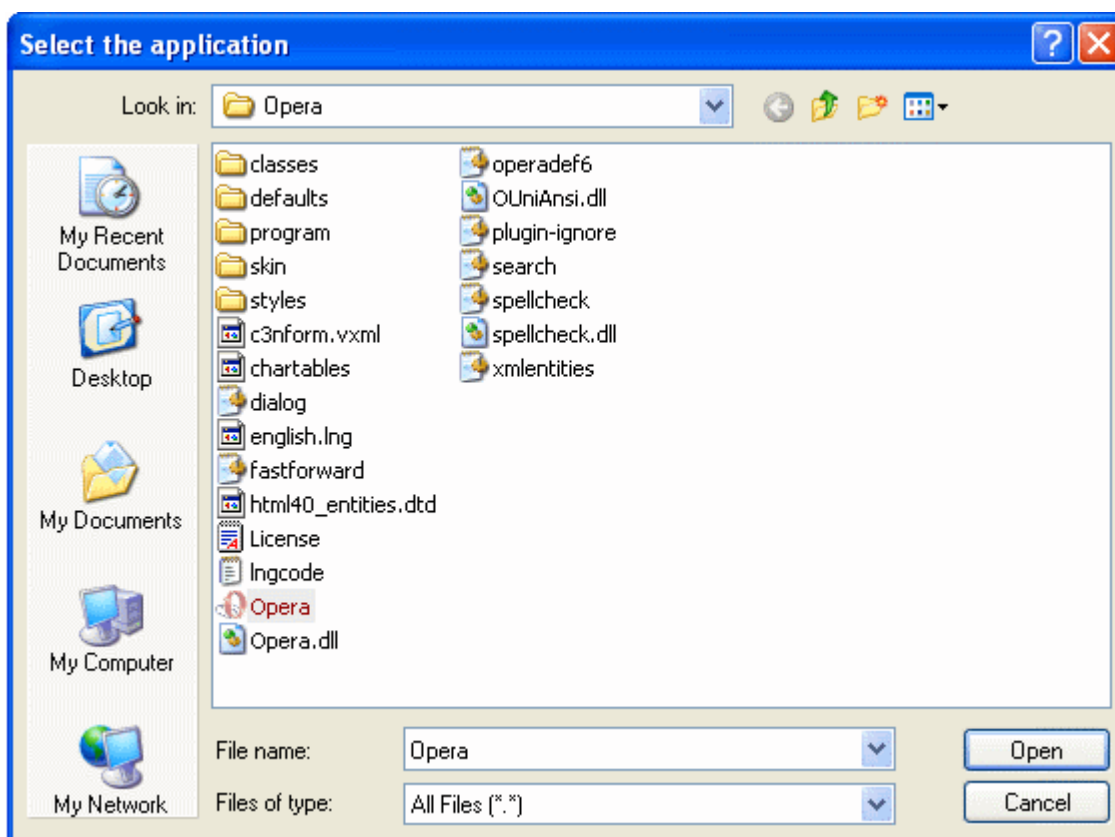
Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. Adding a program in this way means that it will run in the Sandbox this time only. On subsequent executions it will not run in the sandbox (presuming it passes **the sandboxing process**). If you wish to run an application in the sandbox on a long-term/permanent basis then use the **Always Sandbox** interface.

### To run an application in the Sandbox

1. Click the 'Run a Program in the Sandbox' link in the Defense+ interface. The following dialog will open:



2. Click 'Select' to choose the program to be executed in the sandbox.



3. Browse to the application and click 'Open'. In the example above, opera.exe is chosen.



4. Click 'Run As' and select the restriction level you want to apply to the program from the menu.
  - **Untrusted** - The application is not allowed to access any of the 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.

**Note:** Some of the 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.

**Note:** Some of the 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 run with out Administrator account privileges.
- **Partially Limited** - The application is allowed to access all the Operating system files and resources like clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.

The program is executed within the sandbox with the access restriction level that you selected. It will run in the Sandbox on this occasion only.

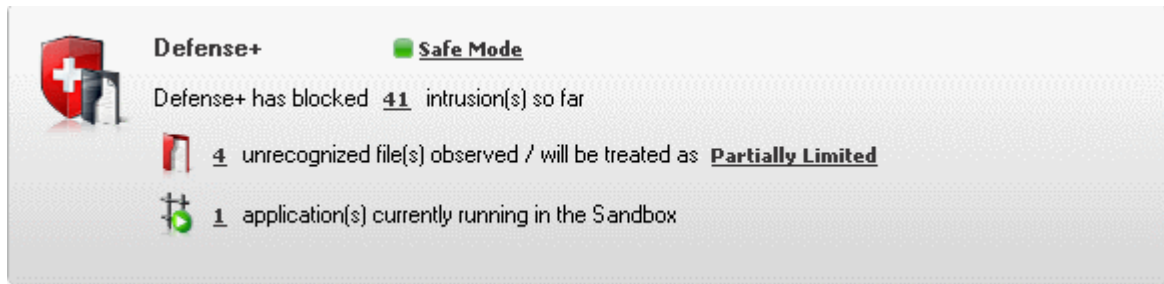
## 4.8 Defense+ Settings

The Defense+ component of Comodo Internet Security is a host intrusion prevention system that constantly monitors the activities of all executable files on your PC. With Defense+ activated, the user is warned EVERY time an unknown application executable (.exe, .dll, .sys, .bat etc) attempts to run. The only executables that are allowed to run are the ones you give permission to. An application can be given such permission to run in a variety of ways including; manually granting them execution rights in **Computer Security Policy**; by deciding to treat the executable as trusted at a **Defense+ alert** or simply because the application is on the Comodo safe list. Defense+ also automatically protects system-critical files and folders such as registry entries to prevent unauthorized modification. Such protection adds another layer of defense to Comodo Internet Security by preventing malware from ever running and by preventing any processes from making changes to vital system files.

**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. Worse still, these programs are explicitly designed to run without you knowing about them. Defense+ is designed to make sure you DO know about them by blocking all unknown executables and alerting you whenever they try to run.

The Defense+ Settings area allows you to quickly configure the security level and behavior of Defense+ during operation. This settings area can be accessed in the '**Defense+**' interface and, more immediately, by clicking on security level setting that is displayed (e.g., Safe Mode) in the **Summary Screen** (shown below).



These settings can be done using the tabs listed below.

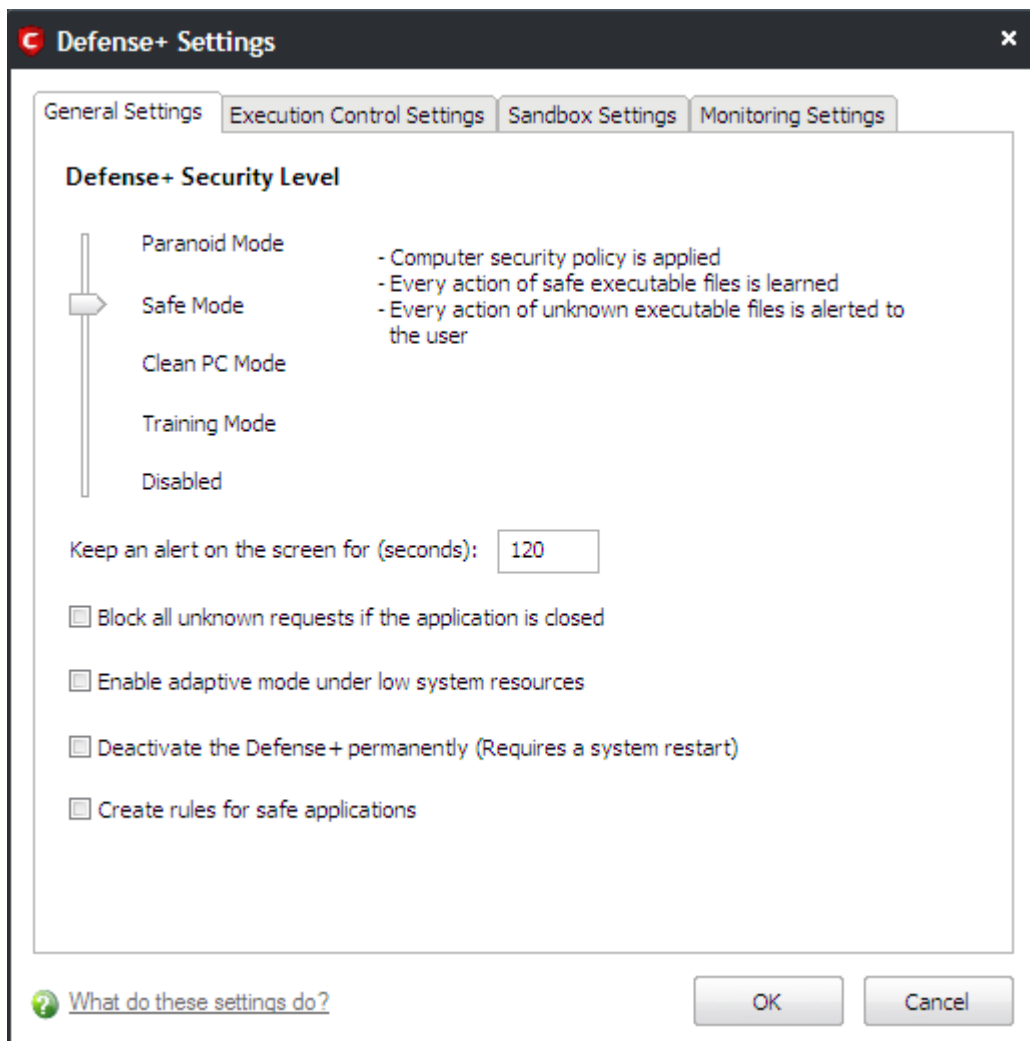
- [General Settings tab](#)
- [Execution Control Settings tab](#)
- [Sandbox Settings tab](#)
- [Monitoring Settings tab](#)

## 4.8.1 General Settings

### Slider Options

Comodo Internet Security allows you to customize the behavior of Defense+ by adjusting a Security Level slider to switch between preset security levels.

The choices available are: **Paranoid Mode**, **Safe Mode**, **Clean PC Mode**, **Training Mode** and **Disabled**. The setting you choose here are also to be displayed on the CIS summary screen.



- **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 Defense+ alert. Choosing this option generates the most amount of Defense+ alerts and is recommended for advanced users that require complete awareness of activity on their system.
- **Safe Mode (Default):** 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 Defense+ 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 Defense+ alerts the user whenever a new, unrecognized application is being installed. In this mode, the files in 'My Pending 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 Defense+ 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.

**Tip:** This mode can be used as the 'Gaming Mode'. It is handy to use this setting temporarily when you are running an (unknown but trusted) application or Games for the first time. This suppresses all Defense+ alerts while Comodo Internet Security learns the components of the application that need to run on your machine and automatically create 'Allow' rules for them. Afterward, you can switch back to 'Train with Safe Mode' mode).

- **Disabled:** Disables Defense+ protection. All executables and applications are allowed to run irrespective of your configuration settings. Comodo strongly advise against this setting unless you are confident that you have an alternative intrusion defense system installed on your computer.

### Checkbox Options

- **Keep an alert on screen for maximum (n) seconds** - Determines how long Comodo Internet Security shows a Defense+ alert without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference (*Default = 120 seconds*).
- **Block all unknown requests if the application is closed** - Checking this box blocks all unknown requests (those not included in your **Computer Security Policy**) if Comodo Internet Security is not running/has been shut down (*Default = Disabled*).
- **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*).
- **Deactivate Defense+ permanently (Requires a system restart)** - Shuts down the Defense+ Host Intrusion element of Comodo Internet Security PERMANENTLY. The firewall and antivirus are not affected and continues to protect your computer even if you deactivate Defense+. Comodo does not recommend users close Defense+ unless they are sure they have alternative Intrusion Prevention Systems installed (*Default = Disabled*).
- **Create rules for safe applications** - Automatically creates rules for safe applications in Computer Security Policy (*Default = Disabled*).

**Note:** Defense+ 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 **Computer Security Policy** 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, '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)

## 4.8.2 Execution Control Settings

Image Execution Control is an integral part of the Defense+ engine. If your Defense+ Security Level is set to **'Training Mode' or 'Clean PC Mode'**, then it is responsible for authenticating every executable image that is loaded into the memory.

Comodo Internet Security calculates the hash of an executable at the point it attempts to load into 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. If no matching hash is found on the safelist, then the executable is 'unrecognized' and you receive an alert.

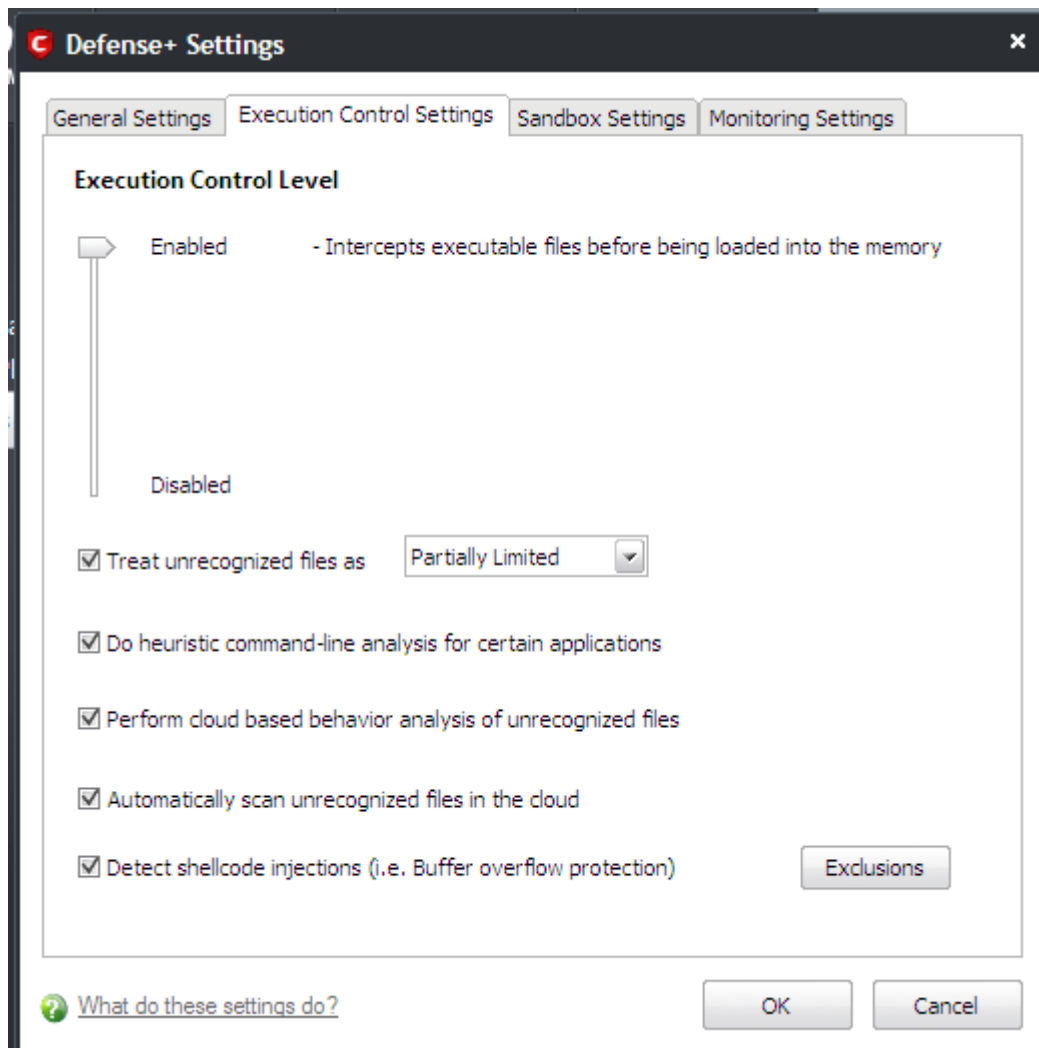
This area allows you to quickly determine how proactive the monitor should be and which types of files it should check.

**Background note:** In this context, an 'image' means an 'Executable Image'. An executable image is a variation on file compression, such as ZIP or RAR files. For example, most program installers are contained in executable images.

### Image Execution Control Level Slider

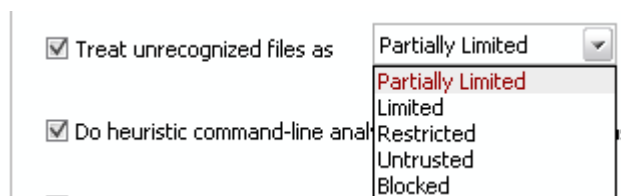
The control slider in the Settings interface allows you to switch the Image Execution settings between **Enabled** and **Disabled** states. The Image Execution Control is disabled irrespective of the settings in this slider, if Defense+ is **permanently deactivated** in the General Settings from the **Defense+ Settings** interface.

- **Enabled (Default)** - This setting instructs Defense+ to intercept the all the files *before* they are loaded into memory and also Intercepts prefetching/caching attempts for the executable files.
- **Disabled** - No execution control is applied to the executable files.



## Check Boxes

**Treat unrecognized files as** - This has five options and the unrecognized files will be run as per the option selected.



- **Partially Limited (Default)** - The application is allowed to access all the Operating system files and resources like clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.
- **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 with out 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.

**Note:** Some of the applications like computer games may not work properly under this setting.



- **Untrusted** - The application is not allowed to access any of the 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.

**Note:** Some of the applications that require user interaction may not work properly under this setting.

- **Blocked** - The application is not allowed to run at all.

**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.

**Perform cloud based behavior analysis of unrecognized files** - When checked, any file that is marked as unrecognized and 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 (**Default = Enabled**).

*More details.* The behavior analysis system is a cloud based service that is used to help determine whether an unknown file is safe or malicious. Once submitted to the system, the unknown executable will be automatically run in a virtual environment and all activities, host state changes and network activity will be recorded. The list of behaviors recorded during this analysis can include information about processes spawned, files and registry keys modified, network activity, and other changes. 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 behavior analysis system takes around 15 minutes to report its results back to CIS. If the executable is deemed a threat then it will be automatically quarantined or deleted. This threat report is also used to update the global black list databases and therefore benefit all CIS users.

**Automatically scan unrecognized files in the cloud** - Selecting this option will automatically submit unrecognized files to our File Lookup Server to check whether or not they are on the master Comodo white list or black-list (White list = files that are known to be safe. Black list = files that are known to be malware) and the files are rated accordingly. The important features of the cloud based scanning are:

- Cloud based Whitelisting: Safe files and trusted vendors and trusted publishers can be easily identified;
- Cloud based Anti virus: Malicious files can be detected even if the users do not have an up-to-date local antivirus database or a local antivirus database at all;
- Cloud Based Behavior Analysis: Zero-day malware can be instantly detected by Comodo's cloud based behavior analysis system, CIMA.

The cloud scanning, complemented by automatic sandboxing and application isolation technologies, is very extremely fast and powerful in preventing PC infection even without a traditional antivirus signature database while keeping the user interaction at minimal levels.

Comodo recommends users leave this setting enabled (*Default = Enabled*).

**Detect Shellcode injections (i.e. Buffer overflow protection)** - Enabling this setting turns-on the Buffer over flow protection.

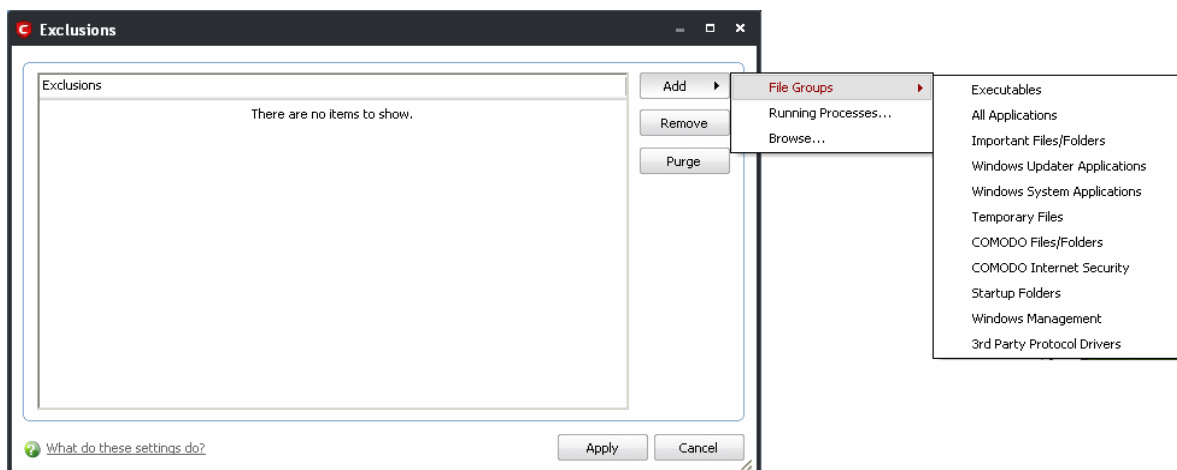
A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may 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.

1. Click on the 'Exclusions' button.



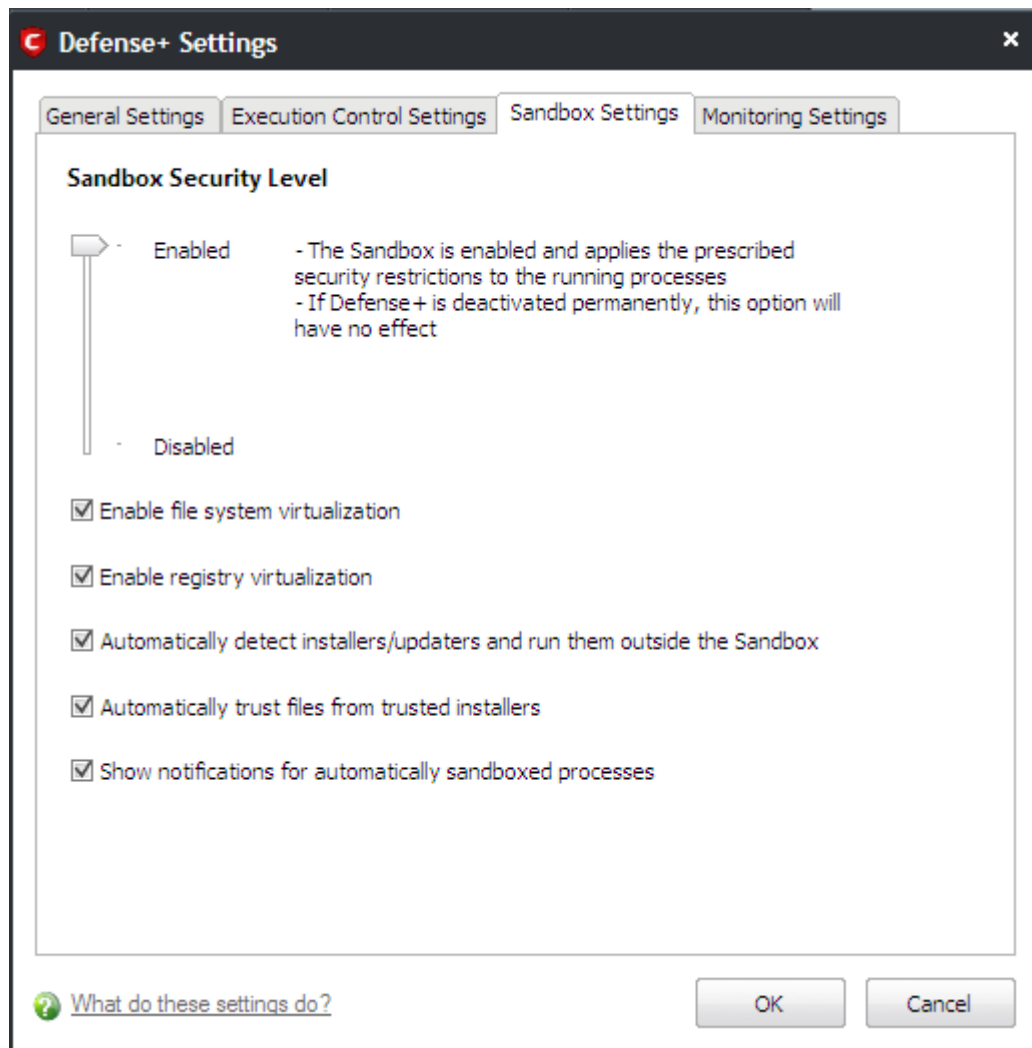
2. Click 'Add' to include file groups or processes to the Exclusions list. Click here for an [outline of the options](#) available when adding file types.
3. Click 'Remove' to remove selected entries from the exclusions list
4. Click 'Purge' to remove invalid entries (programs that are not present or uninstalled from your computer) automatically.

**Note:** These settings are recommended for advanced users only.

5. Click 'Apply' to implement your settings.

### 4.8.3 Sandbox Settings

The Sandbox Settings area allows you to configure the security level and the overall behavior of the sandbox. To access the Sandbox Settings interface, click 'Defense + Settings' then select the 'Sandbox Settings' tab. If you would like some background information on the sandbox before changing these settings then please see section [4.1 - The Sandbox -An Introduction](#).



#### Sandbox Security Level Slider

The Security Level slider in the Settings interface allows you to switch the Sandbox between **Enabled** and **Disabled** states. The programs included in the Sandbox is executed with the set restrictions only if the Sandbox is in Enabled state. If disabled, the programs is run normally without any restrictions. The Sandbox is disabled irrespective of the settings in this slider, if Defense+ is **permanently deactivated** in the General Settings from the **Defense+ Settings** interface.

#### Check Boxes

**Enable file system virtualization** - The sandboxed applications are not permitted to modify the files in your 'real' file system. Enabling file system virtualization instructs the Sandbox to create a virtual file system in your system. The sandboxed applications write any data only into the created virtual file system, instead of affecting and potentially causing damage to your real file system. If you disable this option, the sandboxed applications may not function correctly because they are not able to create the entries that they need too (*Default = Enabled*).

**Note for advanced users:** The virtual file system is created inside the Sandbox working folder (e.g. c:\sandbox\l) to

execute the applications within this file system.

If you disable this option here, the virtual file system is not created even if you have **enabled file system virtualization** for individual applications within the Sandbox.

**Enable registry virtualization** -The sandboxed applications are not permitted to access and modify the entries in your 'real' Window's Registry hives. Enabling registry virtualization instructs the Sandbox to create a virtual registry hive in your system. The sandboxed applications write any entries pertaining to them only into the created registry hive, instead of affecting and potentially causing damage to your real registry hives. If you disable this option, the sandboxed applications may not function correctly because they are not able to create the entries that they need too (**Default = Enabled**).

**Note for advanced users:** The virtual registry hive is created as HKEY\_LOCAL\_MACHINE\SYSTEM\Sandbox\ ... for the sandboxed applications to write their registry values. If you disable this option here, the virtual registry hive is not created even if you have **enabled registry virtualization** for individual applications within the Sandbox.

The table below explains the precedence of the file system virtualization and registry virtualization settings made through this interface and those through **Computer Security Policy > Always Sandbox > Add > Always Sandbox > Advanced Settings**.

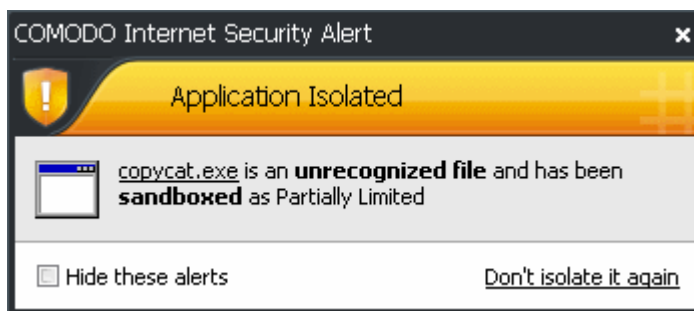
Sandbox Settings	Always Sandbox > Advanced Settings	Is the setting enabled for the specific application?
Yes	Yes	Yes
Yes	No	No
No	Yes	No
No	No	No

**Automatically detect the installers / updaters and run them outside the Sandbox** - On execution of an Installer or an Updater, the application is run outside the Sandbox. Select this option only if you are going to run installers / updaters from trusted vendors (**Default = Enabled**).

**Automatically trust the files from the trusted installers** - Files that are generated by trusted installers are also trusted. This means that they will not be sandboxed (**Default = Enabled**).

**Show notifications for automatically sandboxed processes** - By default, CIS will display an alert whenever it runs an unknown application in the sandbox. Use this control to enable or disable these alerts (**Default = Enabled**).

Click 'OK' for your settings to take effect.



Additional information:

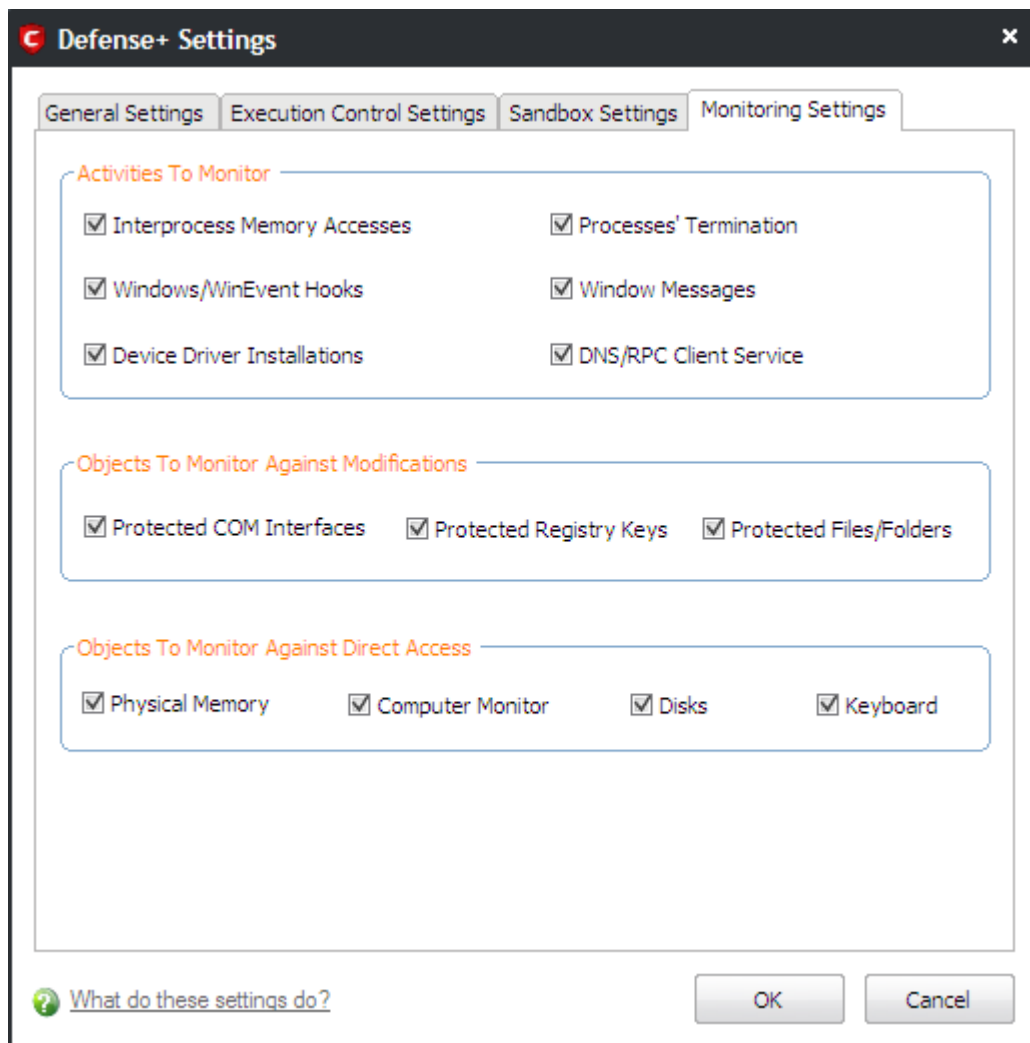
- See '**Sandbox Alerts**' for a explanation of the options available at a Sandbox alert
- See '**Unknown Files: The Sand-boxing and Scanning Processes**' to understand the decision making process behind why CIS chooses to sandbox certain applications.

## 4.8.4 Monitoring Settings

The 'Monitoring Settings' tab allows you configure which activities, entities and objects should monitored by Defense+.

**Note:** The settings you choose here are universally applied.

- If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a *global* basis - effectively creating a universal 'Allow' rule for that activity. This 'Allow' setting *over-rules* any policy 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 Defense+ 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 Defense+ 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 'cfp.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**).
- **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 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 [here](#) (**Default = Enabled**).
- **Protected Registry Keys** enables monitoring of Registry keys you specified [here](#) (**Default = Enabled**).
- **Protected Files/Folders** enables monitoring of files and folders you specified [here](#) (**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**).

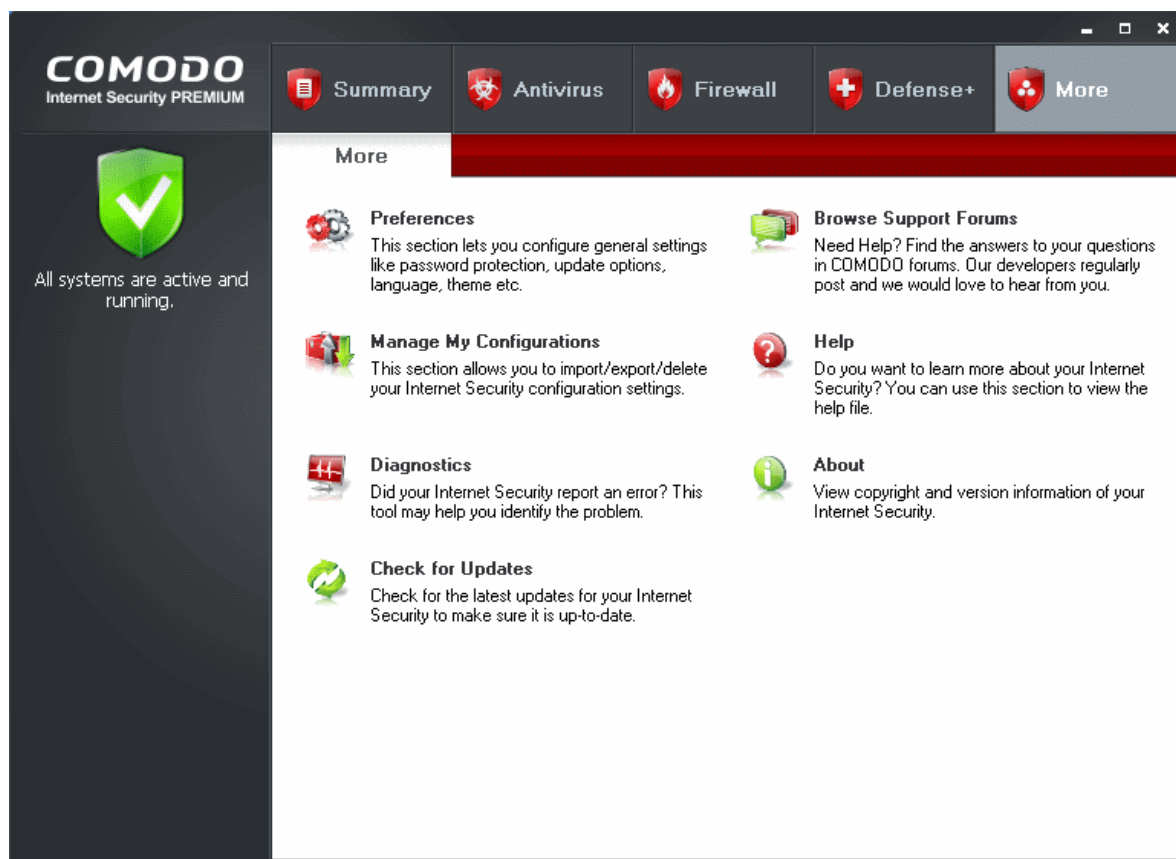


## 5 More Options-Introduction

The **More Options** interface contains several areas relating to overall configuration as well as handy utilities and shortcuts to help enhance and improve your experience with Comodo Internet Security.



It can be accessed at all times by clicking on the 'More' link from the navigation panel.



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

- **Preferences:** Allows the user to configure general Comodo Internet Security settings (password protection, update options, language, theme and so on.)
- **Manage My Configurations:** Allows the user to manage, import and export their Comodo Internet Security configuration profile.
- **Diagnostics:** Helps to identify any problems with your installation.
- **Check For Updates:** Launches the Comodo Internet Security updater.
- **Browse Support Forums:** Links to Comodo User Forums.
- **Help:** Launches the online help guide.
- **About:** Displays version and copy-right information about the product.

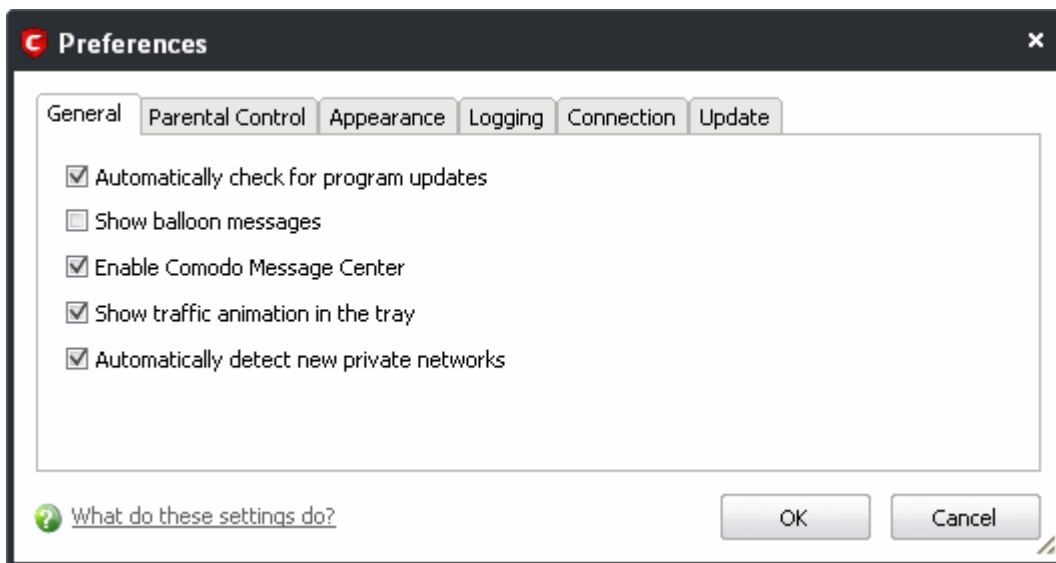
### 5.1 Preferences

The **Preferences** menu in **More** section allows you to configure various options related to the operation of Comodo Internet Security.



## To open Preferences dialog box

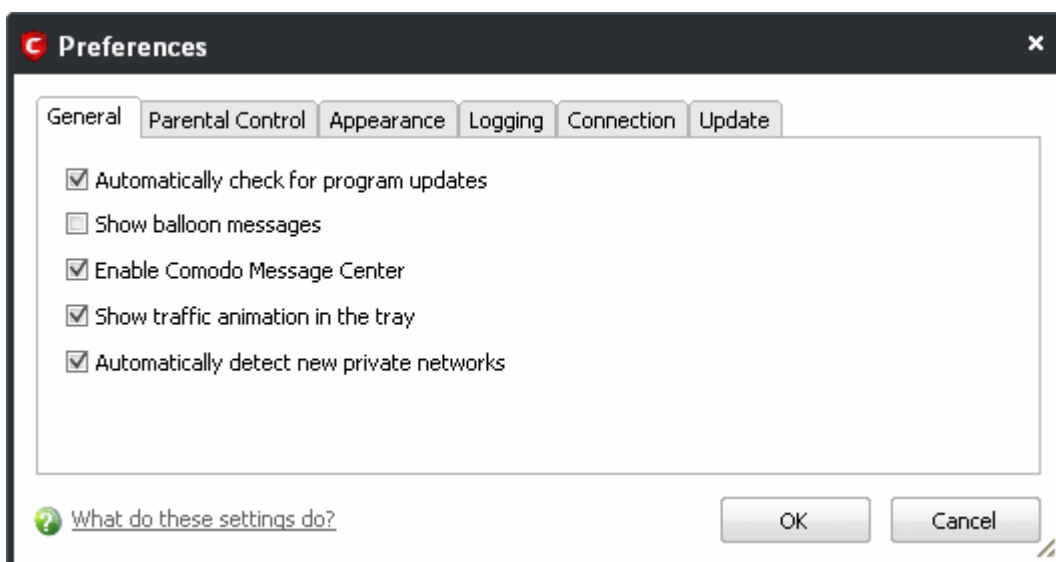
- Click 'Preferences' in 'More' screen.



It has the following tabs to make your settings:

- **General**
- **Parental Control**
- **Appearance**
- **Logging**
- **Connection**
- **Update**

### 5.1.1 General Settings



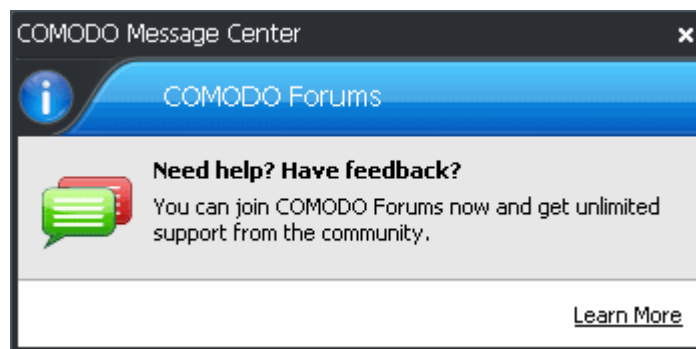
- **Automatically Check for the program updates** - This option determines whether or not Comodo Internet Security should automatically contact Comodo servers for updates. With this option selected, Comodo Internet Security automatically checks for updates every 24 hours AND every time you start your computer. If updates are found, they are automatically downloaded and installed. We recommend that users leave this setting enabled to maintain the highest levels of protection. Users who choose to disable automatic updates can download them manually by clicking '**Check for Updates**' in the 'More...' section (**Default = Enabled**).

- **Show the balloon messages** - These are the notifications that appear in the bottom right hand corner of your screen - just above the tray icons. Usually these messages like 'Comodo Firewall is learning' or 'Defense+ is learning' and are generated when these modules are learning the activity of previously unknown components of trusted applications. Clear this check box if you do not want to see these messages (**Default = Disabled**).
- **Show traffic animation in tray** - 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 red 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**).

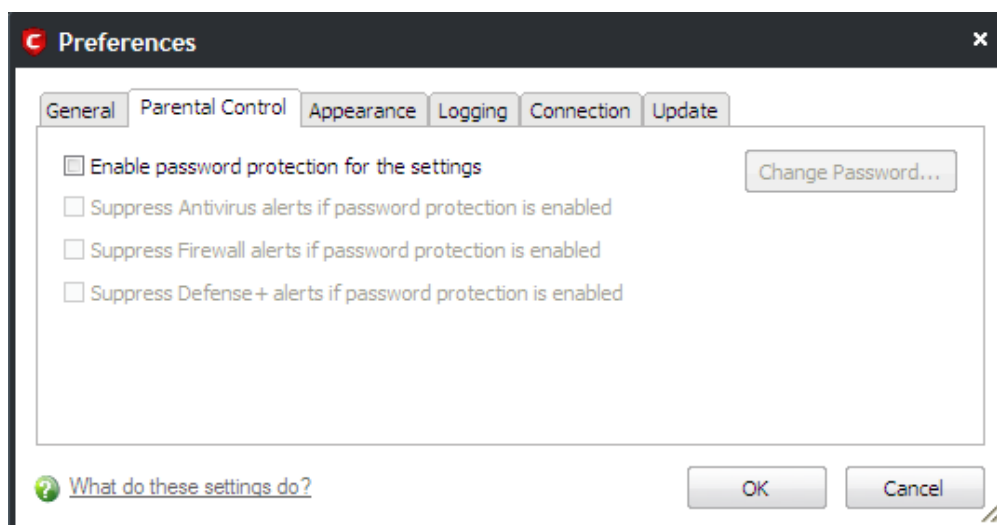
- **Automatically Detect New Private Networks** - Selecting this check box means that the firewall automatically detects any new networks that the computer is connected to. Comodo recommends users to leave this option at its default, enabled setting (**Default = Enabled**).
- **Enable Comodo Message Center** - Comodo Internet Security displays Comodo Message Center window periodically if this option is selected.



The Comodo Message Center window contains information about Security Alerts and News related to Comodo Internet Security and latest critical security updates. Clicking the 'Learn More' link takes you to the Comodo Forums website at <http://forums.comodo.com>. Registration is free and you'll benefit from the expert contributions of developers and fellow users alike (**Default = Enabled**).

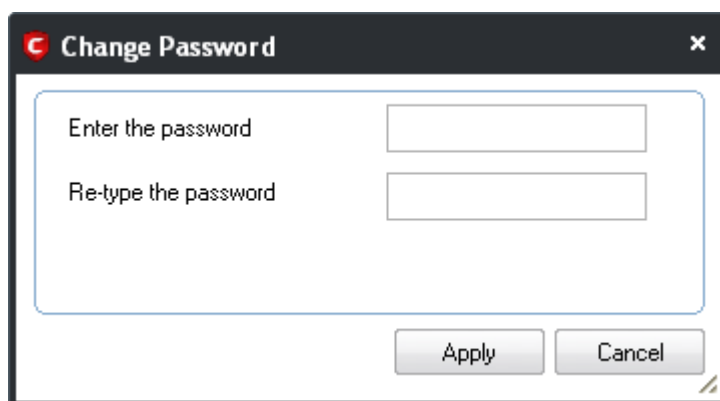
## 5.1.2 Parental Control Settings

The 'Parental Control' tab allows you to configure password protection for Comodo Internet Security.



- **Enable password protection for settings** - Selecting this option activates password protection for all important configuration sections and wizards within the interface. If you choose this option, you must first specify and confirm a password by clicking the 'Change Password...' button. You are asked for this password every time you

try to access important configuration areas (for example, all sections in the **Antivirus Tasks**, **Firewall Tasks** and **Defense+ Tasks** areas require this password before allowing you to view or modify their settings).

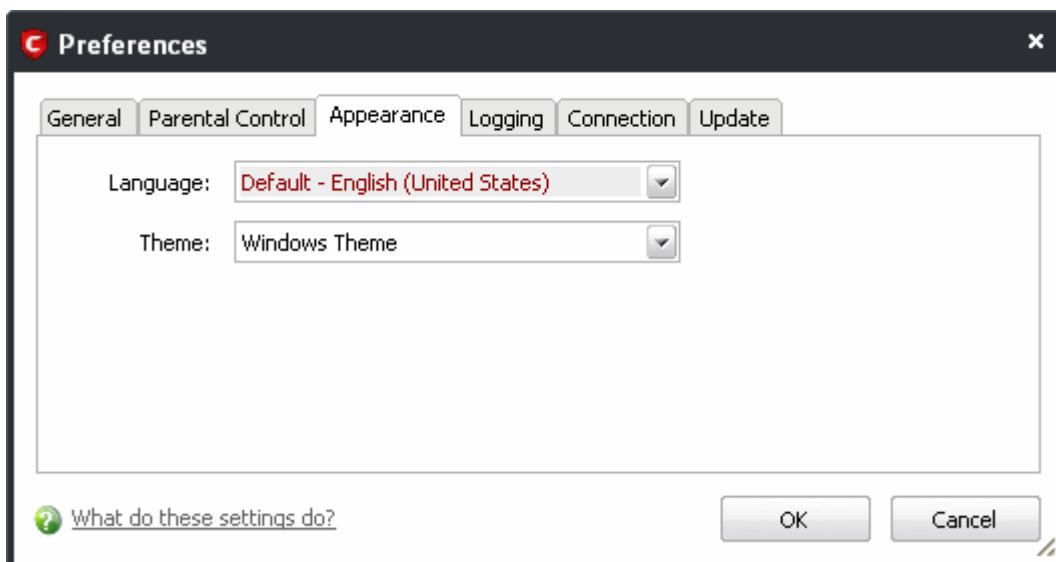


This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and exposing the machine to threats (**Default = Disabled**).

- **Suppress Antivirus alerts when password protection is enabled** - If selected, no Antivirus Alerts are displayed when **password protection** is enabled. Parents and network admins may want to enable this setting if they do not want users to be made aware when an Antivirus alert has been triggered. For example, a virus program may be attempting to copy itself and infect user's computer without permission or knowledge of the user. Usually, the Antivirus would generate an alert and ask the user how to proceed. If that user is a child or an inexperienced user then they may unwittingly click 'allow' just to 'get rid' of the alert and/or gain access to the website in question - thus exposing the machine to attack. Selecting this option **blocks the activity** of the virus but does not generate an alert (**Default = Disabled**).
- **Suppress Firewall alerts when password protection is enabled** - If selected, no Firewall Alerts are displayed when **password protection** is enabled. Parents and network admins may want to enable this setting if they do not want users to be made aware when a Firewall alert has been triggered. For example, a trojan horse program may be attempting to download itself or transmit private information to a third party. Usually, the firewall would generate an alert and ask the user how to proceed. If that user is a child or an inexperienced user then they may unwittingly click 'allow' just to 'get rid' of the alert and/or gain access to the website in question - thus exposing the machine to attack. Selecting this option **blocks the connection** but does not generate an alert (**Default = Disabled**).
- **Suppress Defense+ alerts when password protection is enabled** - If selected, no Defense+ Alerts are displayed when **password protection** is enabled. Parents and network admins may want to enable this setting if they do not want users to be made aware when a Defense+ alert has been triggered. For example, a malware program may be attempting to modify, terminate or delete a critical registry key in order to launch an attack on your machine. Usually, the Defense+ intrusion detection system would generate an alert and ask the user how to proceed. If that user is a child or an inexperienced user then they may unwittingly click 'allow' just to 'get rid' of the alert - thus exposing the machine to attack. Selecting this option **blocks the activity** of the suspected malware but does not generate an alert (**Default = Disabled**).

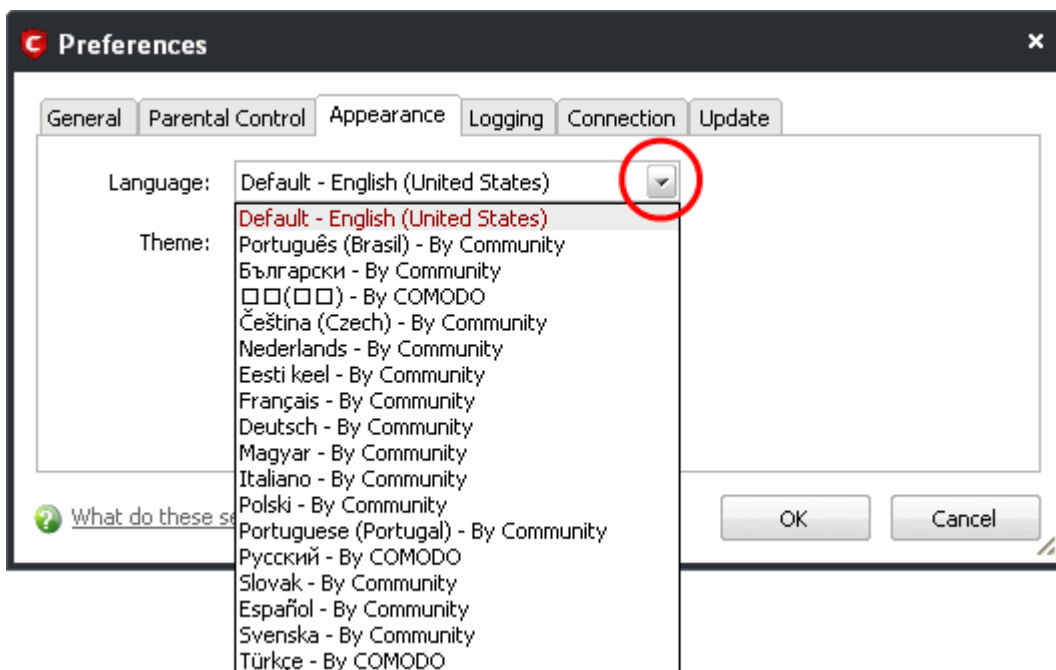
### 5.1.3 Appearance

The **Appearance** tab allows you to choose the interface language and customize the look and feel of Comodo Internet Security according to your preferences. Use the drop-down menu to switch between installed themes.



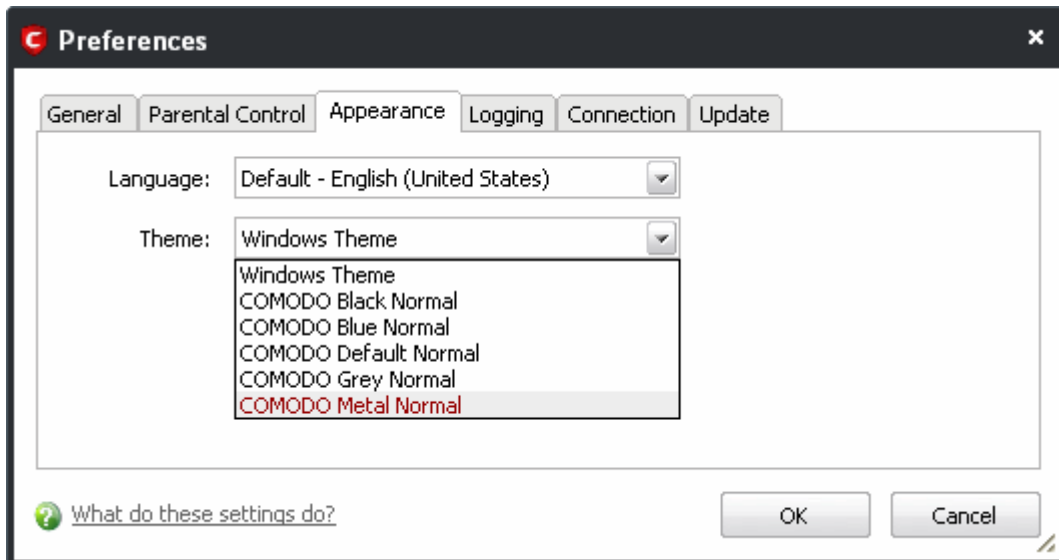
### Language Settings

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)*).

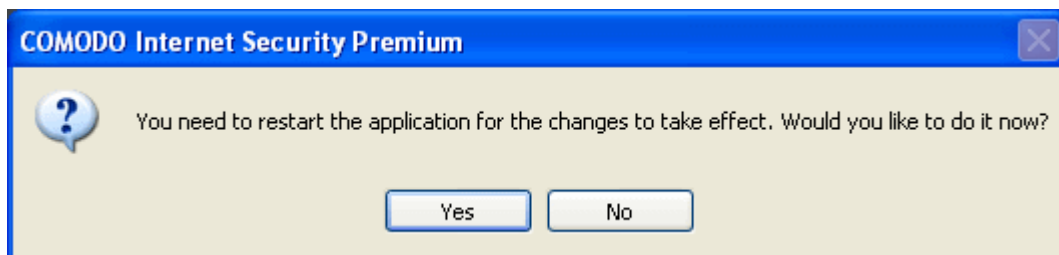


### Themes

The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (*Default = Comodo Default Normal*).



In order for your language and/or theme choices to take effect, you must restart the Comodo Internet Security application.



- Click Yes to restart the application.

You can also do this at a later time by either:

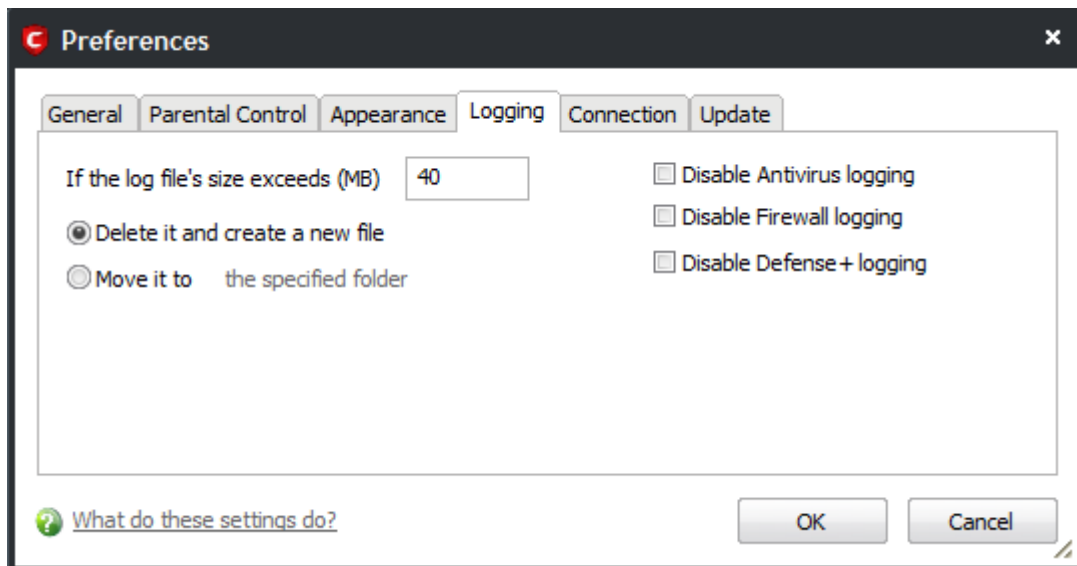
- Restarting your computer (recommended) ; or
- Closing the application by right clicking on the shield tray icon and selecting 'Exit' and then restarting it by navigating through Start > Programs > COMODO > Comodo Internet Security or by double-clicking the desktop icon. The application is in your choice of language the next time you restart the application.

## 5.1.4 Log Settings

Comodo Internet Security maintains a log of all the Antivirus, Firewall and Defense+ events which can be accessible by clicking...

- '**View Antivirus Events**' from the Antivirus Tasks interface;
- '**View Firewall Events**' from the Firewall Tasks interface;
- '**View Defense+ Events**' from the Defense+ Tasks interface.

...respectively. The Logging tab in the More...> Preferences interface allows you to configure the log file settings for Comodo Internet Security.

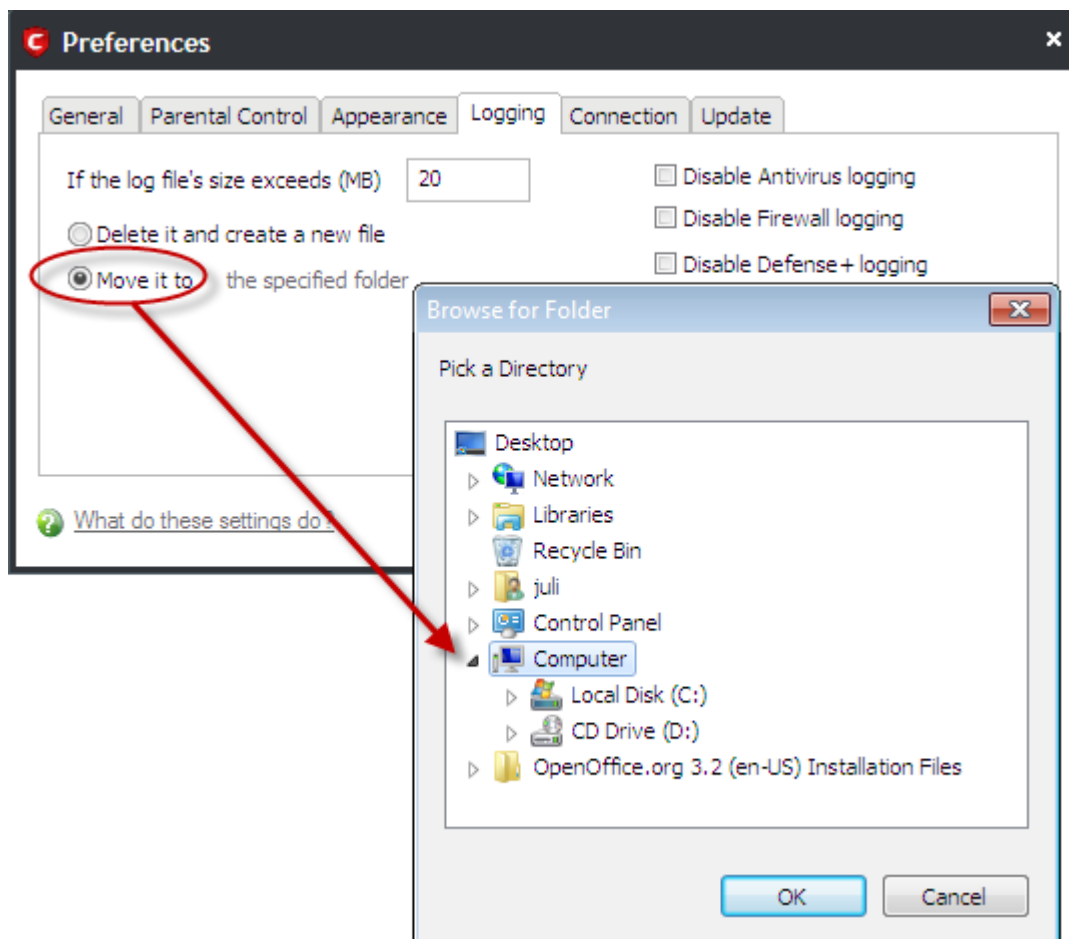


**If the log file's size exceeds (MB):** Enables you to configure for deleting or moving the log file if it reaches a specified size in MB. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.

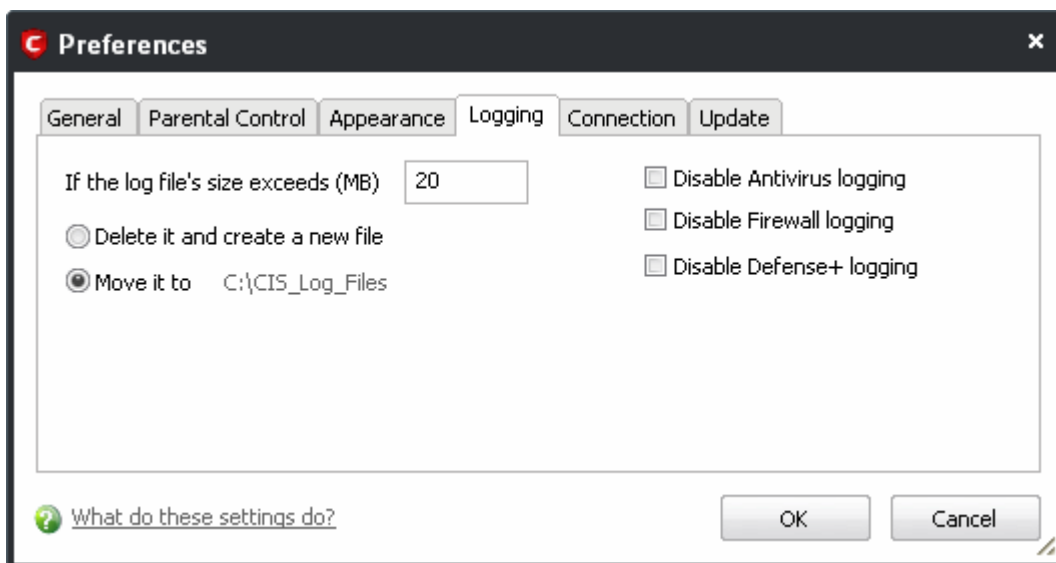
- Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' (*Default = 40MB*).

If you want to discard the log file if it reaches the maximum size, select '**Delete it and create a new file**'. Once the log file reaches the 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.

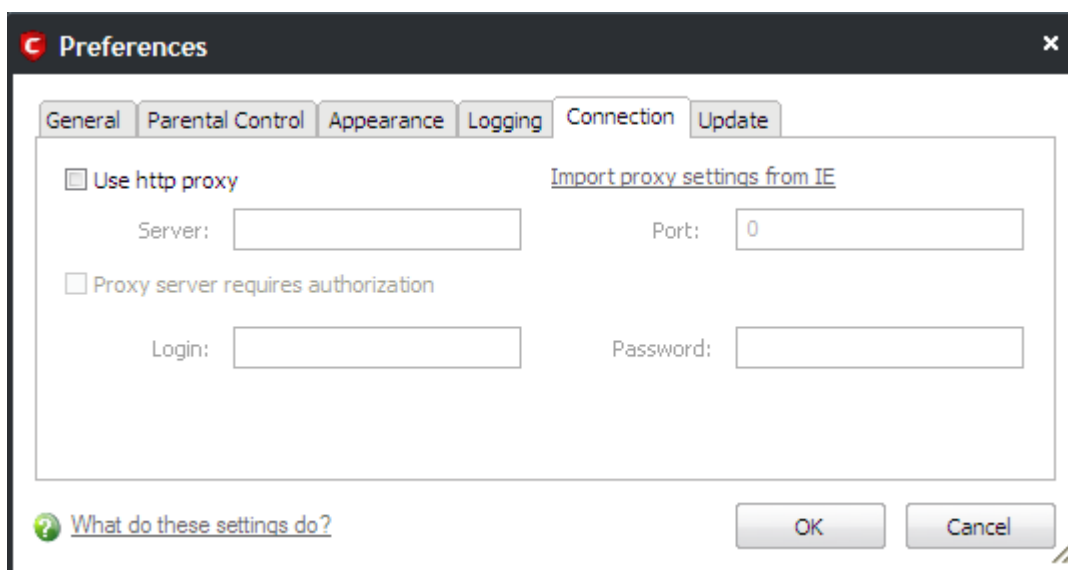
#### Check Boxes:

The check boxes allow you to disable logging of events according to your preferences.

- **Disable Antivirus logging** - Instructs Comodo Internet Security to not to log Antivirus events (*Default = Disabled*).
- **Disable Firewall logging** - Instructs Comodo Internet Security to not to log Firewall events (*Default = Disabled*).
- **Disable Defense+ logging** - Instructs Comodo Internet Security to not to log Defense+ events (*Default = Disabled*).

## 5.1.5 Connection Settings

The Connection tab allows you to configure how Comodo Internet Security should connect to Comodo servers for receiving program updates etc. If you are using a Proxy server in your network and if you want CIS to use the Proxy Server, the Proxy settings can be configured through this settings interface.



- Select 'Use http proxy' if you want Comodo Internet Security to use the Proxy Server. Enter the proxy server

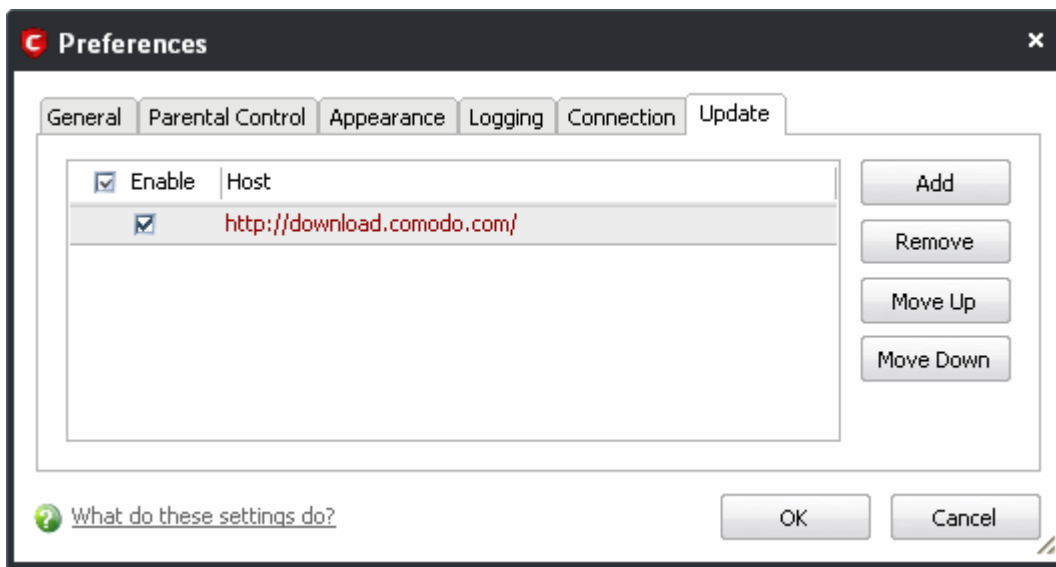


IP address or name in the 'Server' text box and enter the port number in the 'Port' text box (*Default = Disabled*).

- If your Proxy Server needs authentication, Select '**Proxy server requires authorization**'. Type your Login ID in the 'Login' text box and enter the password in the 'Password' text box (*Default = Disabled*).
- If you want Comodo Internet Security to acquire the proxy settings from your Internet Explorer, just click '**Import proxy settings from IE**' link (*Default = Disabled*).

## 5.1.6 Update Settings

The Update tab allows you enable/disable the CIS program updates and to select the host from which the updates are to be downloaded. By default, the URL of the Comodo Server is entered as an available host.



- If you want to download the updates always from the Comodo servers, you can leave the setting as it is (*Default = Enabled*).
- If you are connected to a local network and the CIS program updates are available at an HTTP Server or at any of the other computers in your network running Comodo Offline Updater, you can add the computers as hosts in this area.

**Note:** Comodo Offline Updater allows users to configure a local HTTP server to download and provision updates to networked machines. Advanced users can download the utility from <http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php>

- To add a host click 'Add' and enter the url or IP address of the host in the next row that appears.
- Repeat the process for adding multiple hosts.
- Select the host by using the Move Up and Move Down buttons.
- CIS will automatically check the host specified here and download the updates from the host even when you are offline.
- Click 'OK' for your settings to take effect.

**Note:** CIS program updates can also be checked manually. Click More Options > Check For Updates if you wish to update manually. [Click here](#) to view the help page on manual updates.

## 5.2 Manage My Configurations

Comodo Internet Security allows you to maintain, save and export multiple configurations of your security settings. 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, you can export your configuration settings to a safe place before uninstallation. After re-installation, you can import the configuration settings to take effect in your newly installed Comodo Internet Security. This feature is also a great time saver for anyone with more than one computer because it allows you to quickly implement your security settings on other

computers that you own without having to manually re-configure them.

- [Comodo Preset Configurations](#)
- [Importing/Exporting and Managing Personal Configurations](#)

## 5.2.1 Comodo Preset Configurations

By default Comodo Internet Security has three preset configurations available. Based on the installation option you have selected during setup, one of these choices is set as ACTIVE CONFIGURATION by default. You are able to switch between configurations at any time by right-clicking on the CIS tray icon.

Click the links below to find out more details on each configuration:

- [COMODO - Internet Security](#)
- [COMODO - Proactive Security](#)
- [COMODO - Firewall Security](#)

**Important Note:** Any changes you have made to the Comodo Internet Security settings since installation are recorded in this, active profile.

The detailed descriptions of the default security levels provided by the three preset choices are given below:

**COMODO - Internet Security** - This configuration is activated by default, when both Antivirus and Firewall components are installed, i.e. the complete installation. Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, Defense+ is set to Clean PC mode. Otherwise, the default is Safe mode. In this mode,

- Image Execution Control is disabled.
- Computer Monitor/Disk/Keyboard/DNS Client access/Window Messages are NOT monitored.
- 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 using My Configurations interface.

**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, Defense+ 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 using My Configurations interface.

**COMODO - Firewall Security** - This configuration is activated when the user chooses to install Firewall only and selects optimum protection settings for Defense+ . Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, Defense+ is set to Clean PC mode. Otherwise, the default is Safe mode.

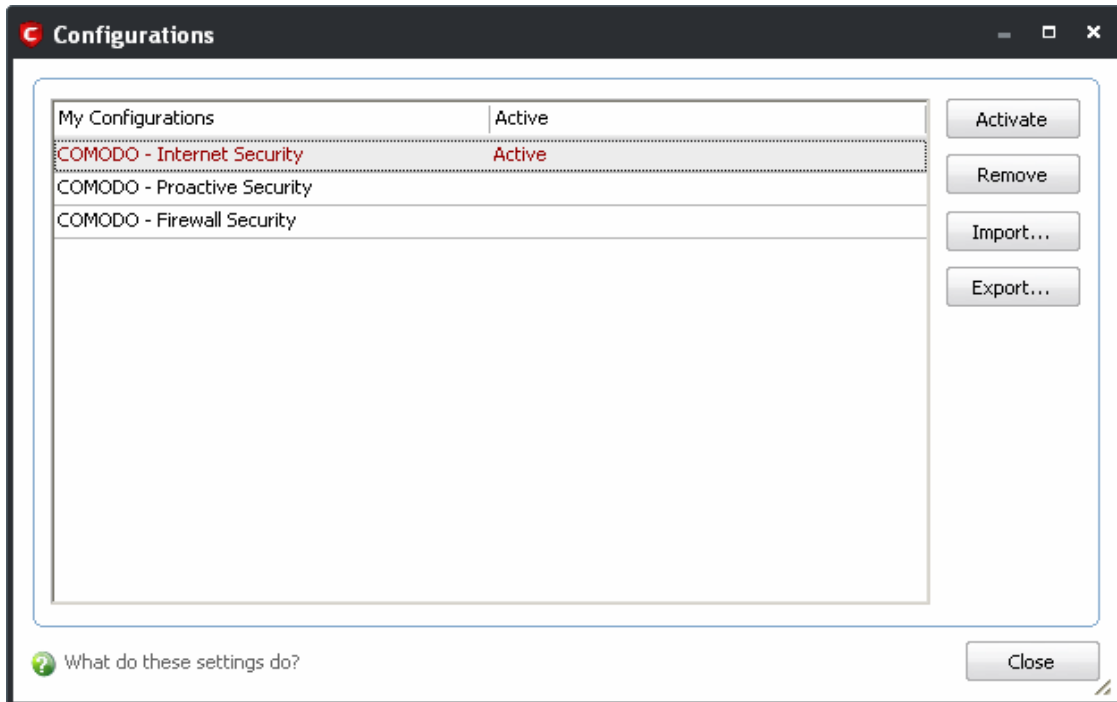
- Image Execution Control checks only applications that are not started manually by the user.
- Computer Monitor/Disk/Keyboard is NOT monitored.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Defense+ is tuned to prevent infection of the system 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 using My Configurations interface.

## 5.2.2 Importing/Exporting and Managing Personal Configurations

### To access Configurations interface

1. Navigate to 'More > Manage My Configurations'.



If this is the first time you have accessed this interface you can see the three preset choices:

- **COMODO - Internet Security**
- **COMODO - Proactive Security**
- **COMODO - Firewall Security**

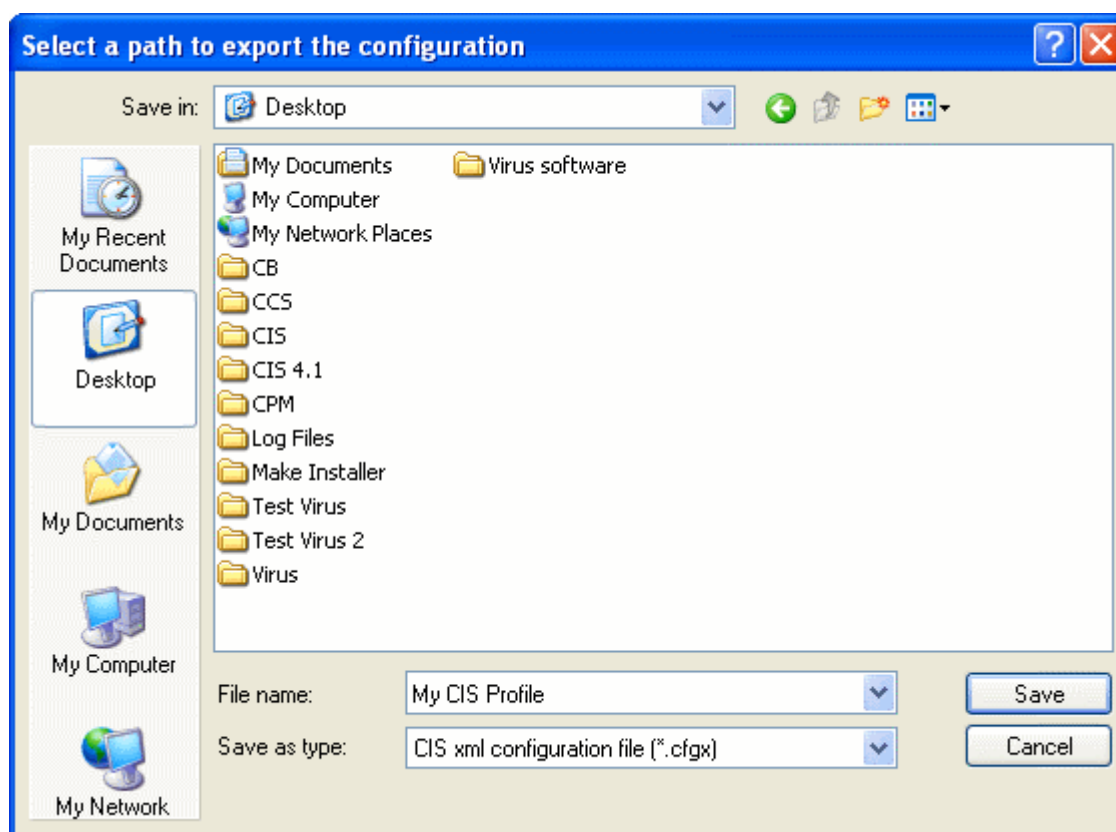
The currently active configuration is indicated as 'Active' in this interface.

2. Click the area on which you would like more information:
  - **Export my configuration to a file**
  - **Import a saved configuration from a file**
  - **Select a different active configuration setting**
  - **Delete a inactive configuration profile**

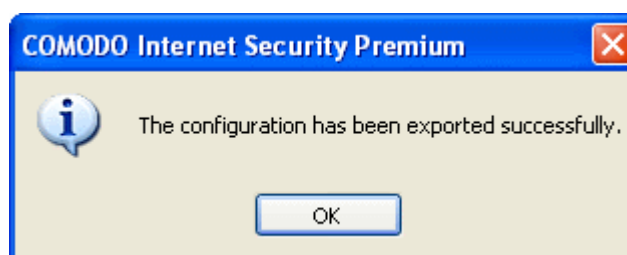
Export my configuration to a file

### To export your currently active configuration

1. Click the 'Export' button .
2. Type a file name for the profile (e.g., 'My CIS Profile') and save to the location of your choice.



A confirmation dialog appears for the successful export of the configuration.

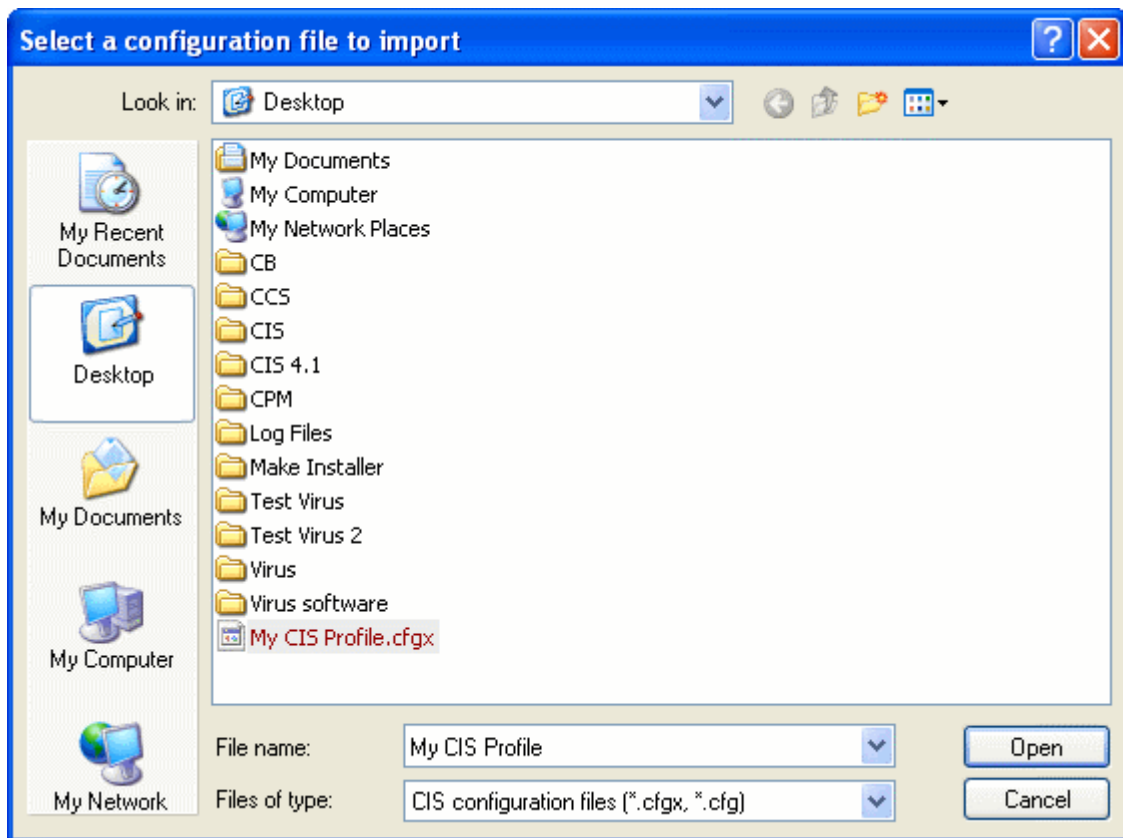


### Import a saved configuration from a file

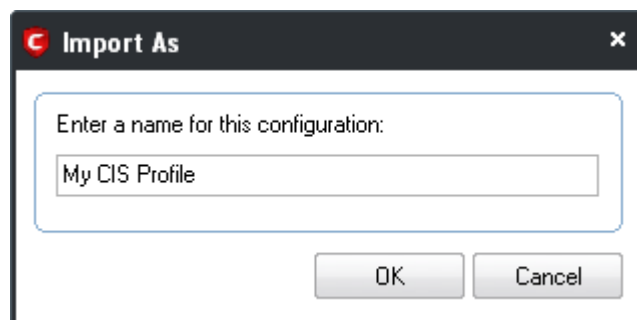
Importing a configuration profile allows you to store any profile within Comodo Internet Security. Any profiles you import do not become active until you **select them for use**.

### To import a profile

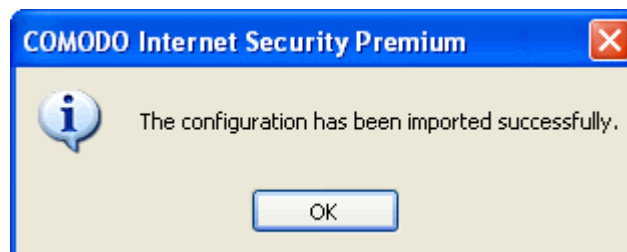
1. Click the 'Import' button.
2. Browse to the location of the saved profile and click 'Open'.



3. In the 'Import As' dialog that appears, assign a name for the profile you wish to import and click 'OK'.



A confirmation dialog appears indicating the successful import of the profile.



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



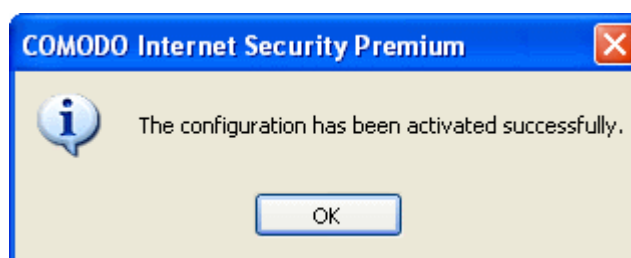
### Select and Implement a different configuration profile

The **Activate** option allows you to quickly switch between configuration profiles.

#### To select a different configuration

1. Click on the profile you want to select and activate.
2. Click the 'Activate' button.

A confirmation dialog appears.



The selected configuration is activated.

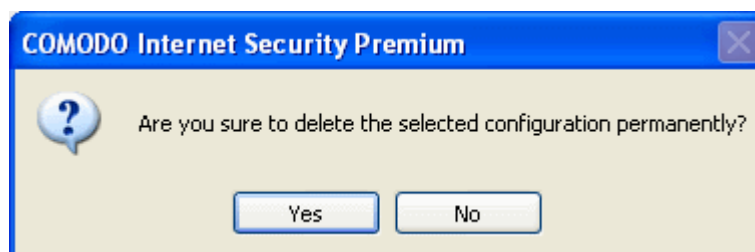


### Delete an inactive configuration profile

You can remove any unwanted configuration profiles using the 'Remove' button. 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. Select the profile and click 'Remove' button. A confirmation dialog appears.



2. Click 'Yes' if you are sure to delete. The selected profile is removed from the list and a confirmation dialog appears.



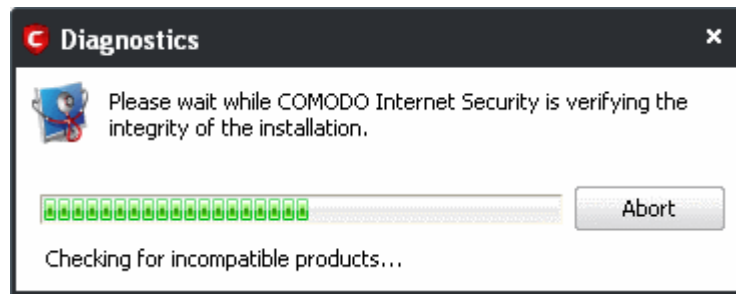
## 5.3 Diagnostics

Comodo Internet Security has its own integrity checker. This checker scans your system to make sure that the application is installed correctly. It checks your computer's:

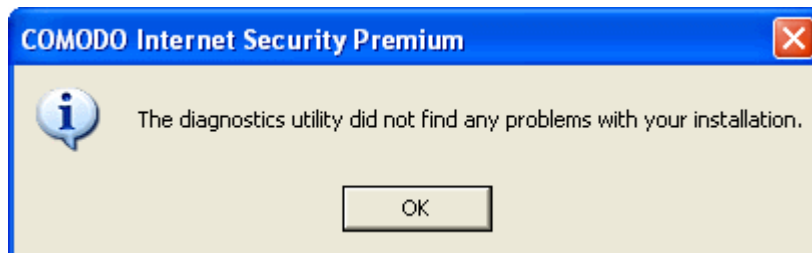
- File System - To check that all of Comodo's system files are present and have been correctly installed.
- Registry - To check that all of Comodo's registry keys are present and in the correctly installed.



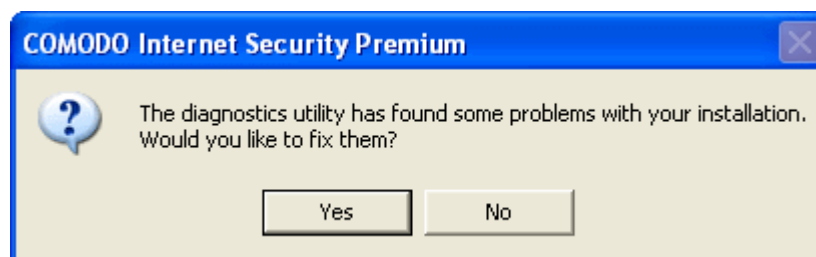
- Checks for the presence of software that is known to have compatibility issues with Comodo Internet Security.



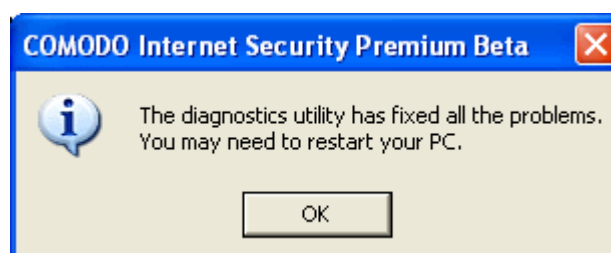
The results of the scan are shown in the following pop-up window. If your installation does not have any errors the following dialog is displayed.



If the diagnostics utility has found some errors in the installation, the following dialog is displayed.



Click 'Yes'. The diagnostics utility automatically fixes the problems and prompts you to restart the computer.



Restart your computer for the changes to take effect.

## 5.4 Check for Updates

Updates on Comodo Internet Security can be downloaded and installed at any time by clicking the 'Check for Updates' link in 'More' Options interface.



## To check for availability of updates

- Click 'Start'.



On completion of checking, the panel shows the availability of updates.



The 'Update Details' link will lead you to the web page that provides release notes for the latest version of the application.

### To initiate the update process

- Click the 'Start' button in the panel.

**Note:** If you want to download and install the updates later, click the 'Cancel' button.

After the installation process is completed, Click 'OK'. You are then asked to restart the system.

- Click 'Yes' to reboot the system now or 'No' to reboot at a later time.

## 5.5 Browse Support Forums

The fastest way to get further assistance on Comodo Internet Security is by posting your questions on Comodo Forums, a message board exclusively created for our users to discuss anything related to our products.

- Click the **Browse Support Forums** link to be taken straight to the website at <http://forums.comodo.com>. Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.

**More**

**Preferences**  
This section lets you configure general settings like password protection, update options, language, theme etc.

**Browse Support Forums**  
Need Help? Find the answers to your questions in COMODO forums. Our developers regularly post and we would love to hear from you.

**COMODO**  
Creating Trust Online®

WELCOME TO THE COMODO FORUM

HOME HELP SEARCH LOGIN REGISTER

USER INFO: Welcome, Guest. Please login or register. August 04, 2010, 05:47:17 AM

LOGIN: Login with username, password and session length

FORUM STATS: 413713 Posts, 45957 Topics, 103928 Members, Latest Member: **saidthrock**

NEWS: Thu, 22 Jul 2010 08:00:00 EST Comodo Ranks # 1 Provider of High Assurance Certificates, Mon, 19 Jul 2010 08:00:00 EST Comodo Targets Web Hosting Companies with New Security Solutions at HostingCon in Austin

Search: Search Advanced search | Tag Cloud Please Join our Forums

## Online Knowledge Base

We also have an online knowledge base and support ticketing system at <http://support.comodo.com>. Registration is free.

## 5.6 Help

Clicking the **Help** link in the **More** section opens the online help guide hosted at <http://help.comodo.com/>. Each area has its own dedicated page containing detailed descriptions of the application's functionality.

Find the desired product help Comodo Internet Security 5.3 English See Help

Comodo Internet Security Version 5.3 English

Introduction To Comodo Internet Security

- Introduction To Comodo Internet Security
  - Special Features
  - System Requirements
- Installation
  - Starting Comodo Internet Security
- Comodo Internet Security - Overview Of Summary Screens
- Comodo Internet Security - Navigation
- Understanding Alerts
- Antivirus Tasks-Introduction
- Firewall Tasks-Introduction
- Defense+ Tasks - Introduction
- More Options-Introduction
- Comodo GeekBuddy
- LivePCSupport
- TrustConnect Overview

## Introduction to Comodo Internet Security

### Overview

Comodo Internet Security 2011 offers 360° protection against internal and external threats by combining a powerful Antivirus protection, an enterprise class packet filtering firewall, and an advanced host intrusion prevention system called Defense+.

CIS is available in Premium (free), Pro and Complete editions. Whilst the core CIS software is identical for all three versions, the Pro and Complete packages each offer a range of additional services. These include services such as [LivePCSupport](#) (Comodo support experts available 24/7 to fix any problem with your computer); [TrustConnect](#) (secure Internet proxy service that ensures 128 bit encrypted connectivity from any public wireless hotspot); Online Backup (10GB of online storage space) and the Comodo 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. See terms and conditions for full details. Available to USA residents only). The free, Premium version offers a 60 day free trial of [Comodo GeekBuddy](#).

New features in CIS 2011 include Cloud based antivirus scanning and behavior analysis, user-friendly application white-listing, new spyware and rootkit scanners, improved malware cleaning, an all new 'game mode', full support for IPv6, improved Defense+ application compatibility and a completely re-designed interface.

When used individually, each of the Antivirus, Firewall and Defense+ components deliver 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.

You can also print or download the help guide in pdf format from the webpage.

## 5.7 About

Click the 'About' option in the 'More' Screen to view the 'About' information dialog.



You can view information about the Version Number of Comodo Internet Security that is installed on your computer and the unique serial number of your installation. The serial number is used to identify your installation and is necessary for support purposes.

## 6 Comodo GeekBuddy

Comodo GeekBuddy is a personal computer support service provided by Comodo computer experts

who establish a remote desktop connection to your machine and fix your computer's 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.

Comodo Internet Security Premium includes 60 day trial version of Comodo GeekBuddy. The users can get the services for free for the first 60 days and have to register for further usage.

- [Overview of the Services](#)
- [Launching the Client and Using the Service](#)
- [Accepting Remote Desktop Requests](#)
- [Registration](#)
- [Activation of Service](#)
- [Uninstalling Comodo GeekBuddy](#)



## 6.1 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.

## 6.2 Launching the Client and Using the Service

The GeekBuddy client required for the services is installed in your system along with CIS Premium if you have selected the option Install Comodo GeekBuddy in **Step 3** 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 
- Click the GeekBuddy system tray icon 
- Launch the GeekBuddy client directly from the Windows Start Menu - Click Start > All Programs > Comodo > Comodo GeekBuddy > Comodo GeekBuddy.

The service support option dialog will open.

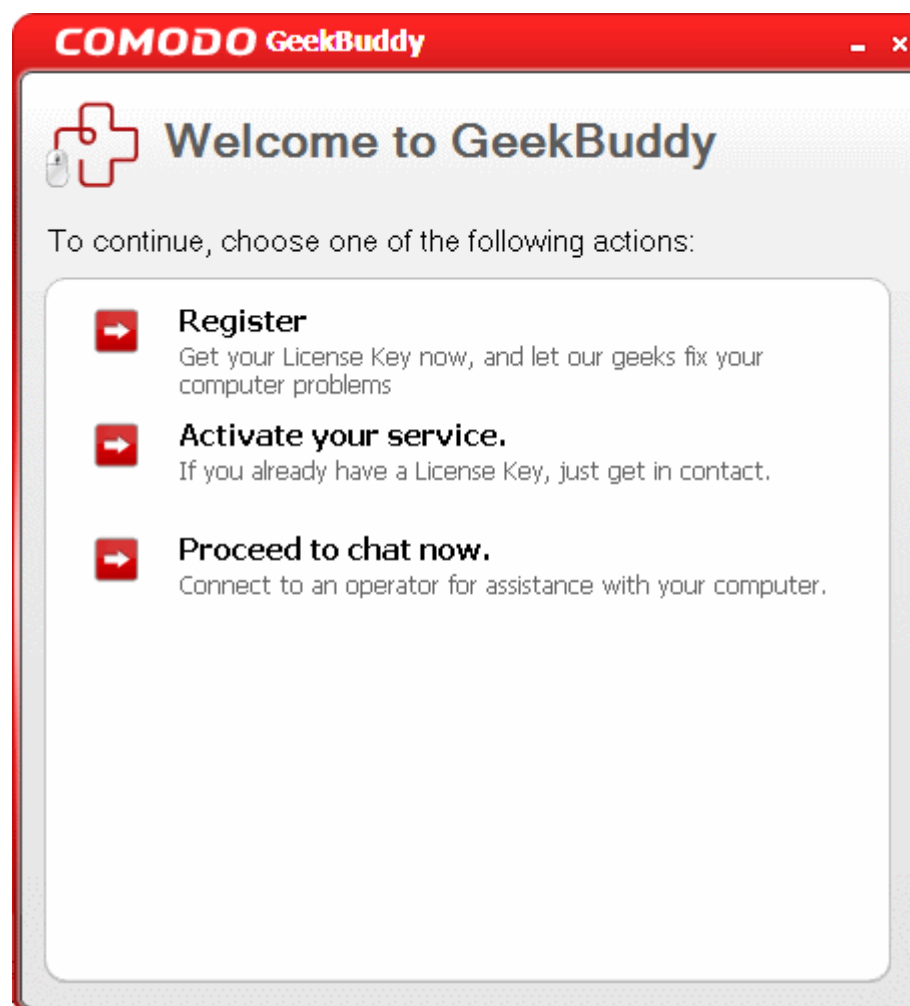


Select the type of service you need:

- **Virus Infection** - Select if you need assistance in removing viruses, malware etc. from your system.
- **Other** - Select if you need assistance with a PC issue that does not fall into any of the other service categories offered, or if you are not sure.
- **Internet and online identity security** - Select if you require assistance optimizing your computer's basic security settings to prevent loss of sensitive data and identity theft.
- **Printer or email account set up** - Select if you need assistance installing or updating printer software and/or drivers, checking ink levels, and/or configuring your printer to work on a wireless or wired network. Our technician will also provide assistance setting up your internet-based email account with any provider and any account.
- **Software activation** - Select if you require assistance installing or activating any third-party software in your system.
- **Other PC troubleshooting** - Select if you need assistance resolving any other problems in your computer.
- **Computer power setting optimization** - Select if you require assistance configuring the power management settings in your computer to save money on your electric bill.
- **Comodo software installation and setup** - Select if you need assistance installing and/or setting up any software products supplied by Comodo.
- **Comodo account questions** - Select if you have any doubts about your account in Comodo or queries about opening an account in Comodo.

You will be connected to a technician trained to provide the precise support you have requested. Clicking any of the options will open the registration screen.

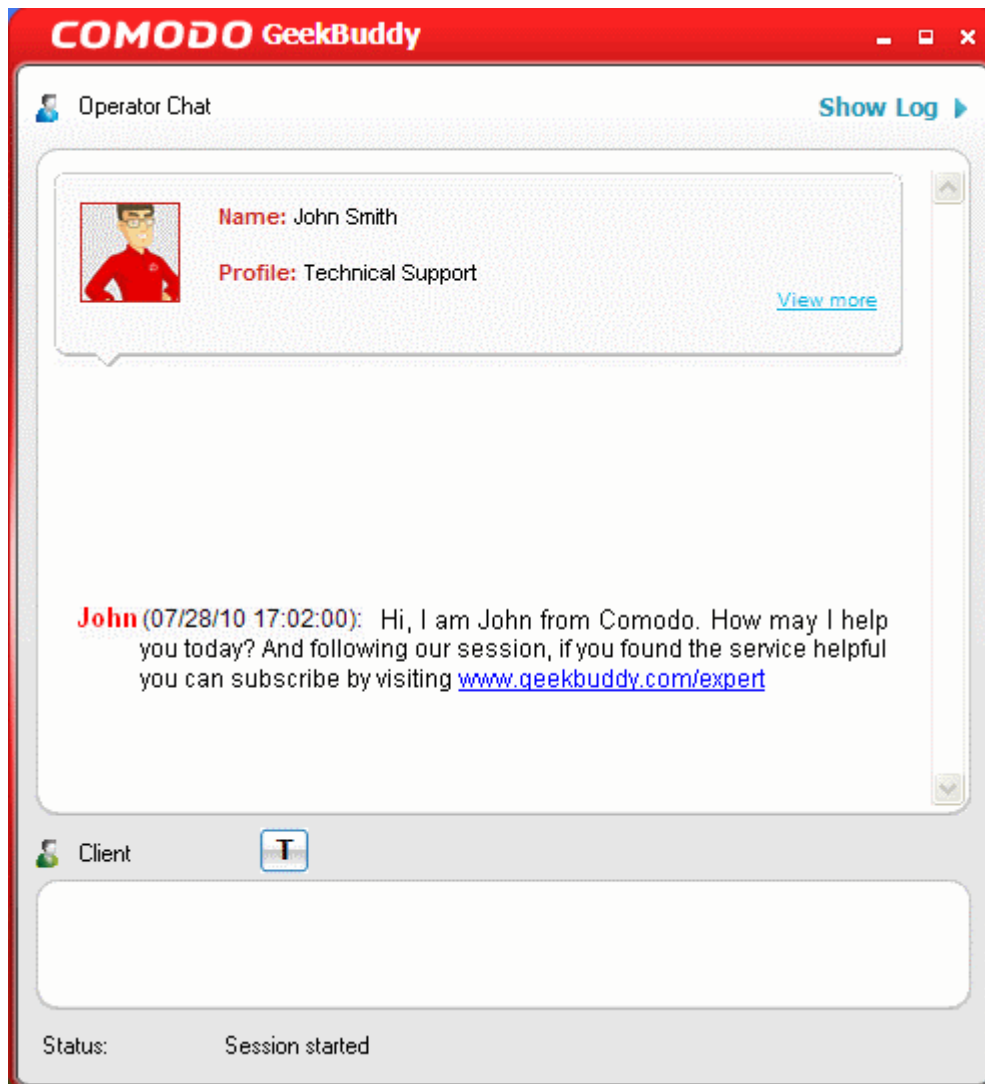




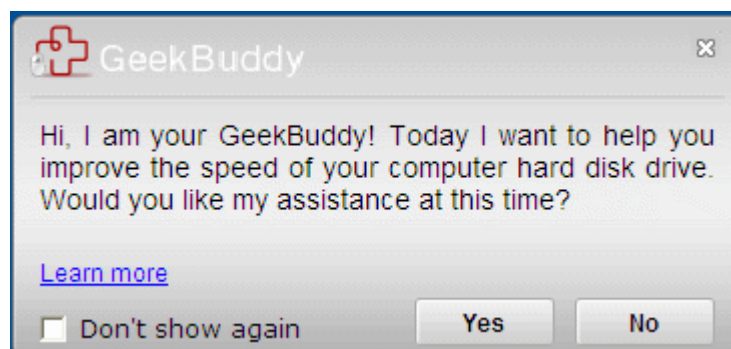
**Proceed to chat now** - The easiest and fastest way to start chatting with an expert technician is by clicking the 'Proceed to chat now' link. Within seconds, a Comodo support technician will respond in a chat window and ask you to describe the problem. Trial service users can go for this option to get the services.

**Note:** The trial service is for a period of sixty days only. 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**.

- Start chatting! Use the chat window to explain any problems you are having with your computer, or to request any of the GeekBuddy services. For your first chat, why not ask the technician to configure Comodo Internet Security (CIS), run a full antivirus check, then optimize your computer for security and performance.



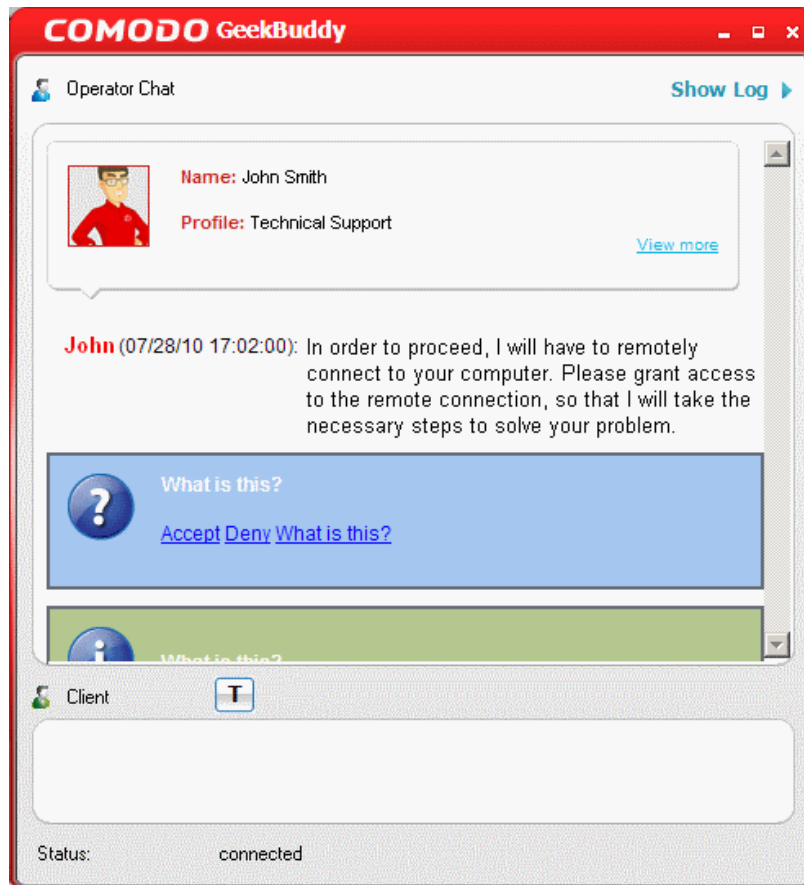
- The technician may request for a remote desktop access of your computer. You need to **accept the remote desktop access request** to enable the technician to solve your problems.
- Occasionally, you will see friendly messages from GeekBuddy which offer to perform useful services such as improving the performance of your computer:



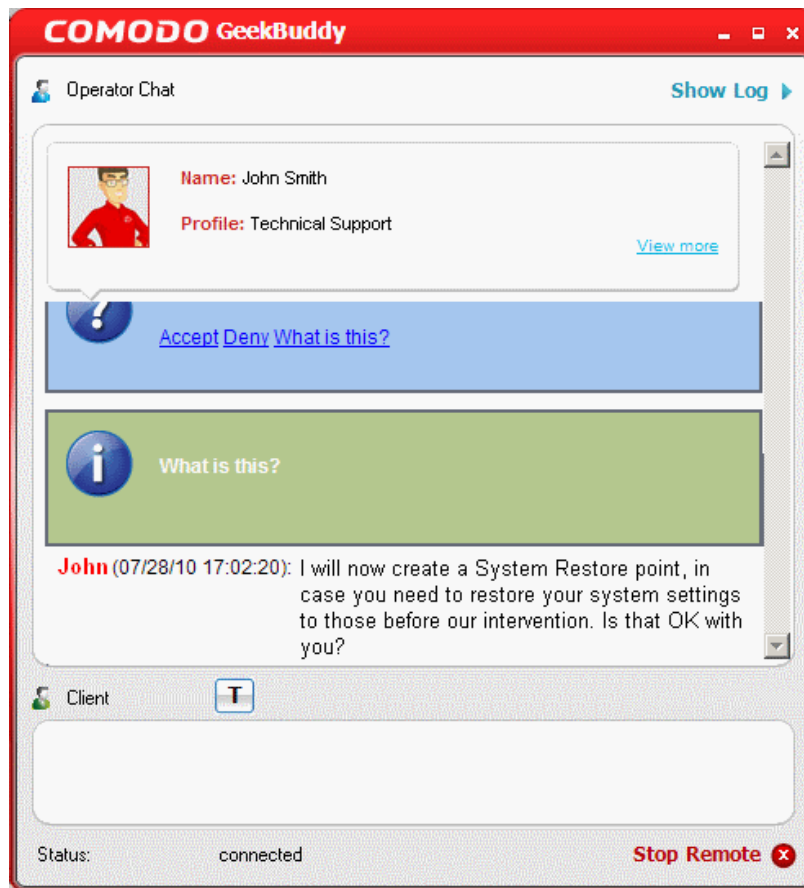
Clicking 'Yes' to these messages will connect you straight to a GeekBuddy operative as if you had clicked 'Proceed to chat now'. Comodo proactively offer these reminders to ensure our customers get the maximum value out of the services we offer.

## 6.3 Accepting Remote Desktop Requests

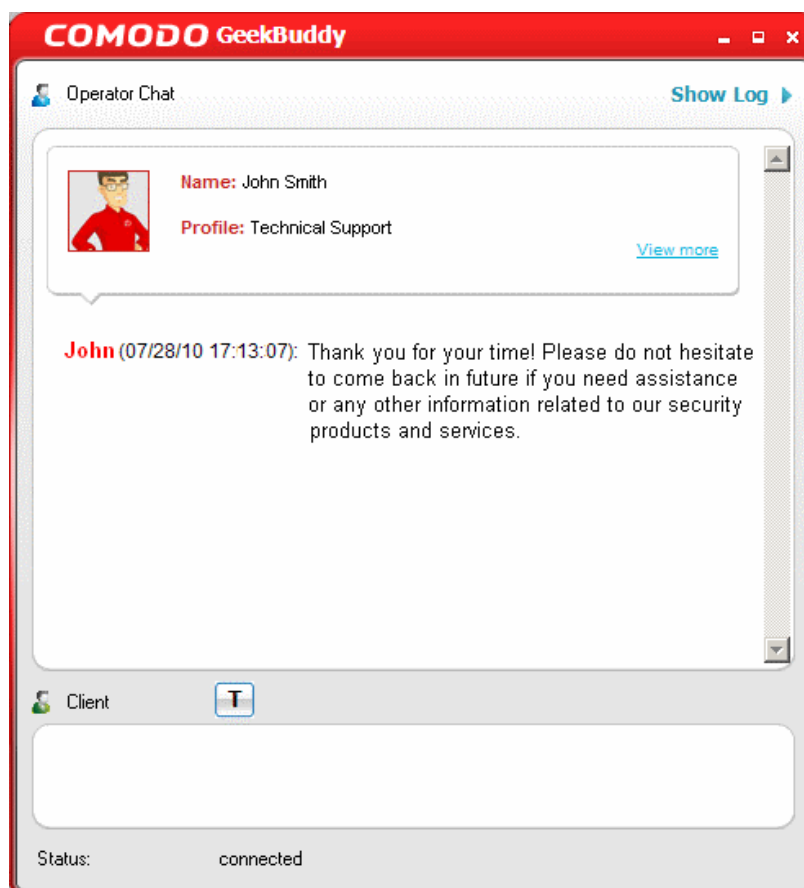
In order to solve certain problems, the support technician may need to connect to your computer via remote desktop connection. This will allow them to directly perform the required services while you watch. Remote desktop control can only go ahead if you grant permission for this to happen. Our technicians will always request your permission via the chat window as shown below:



- Click the 'Accept' link to enable the technician to connect to your computer. The technician will take control over your computer through remote desktop connection and start fixing your problems or performing the service that you requested. 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 malicious files.



On completion of his/her 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.

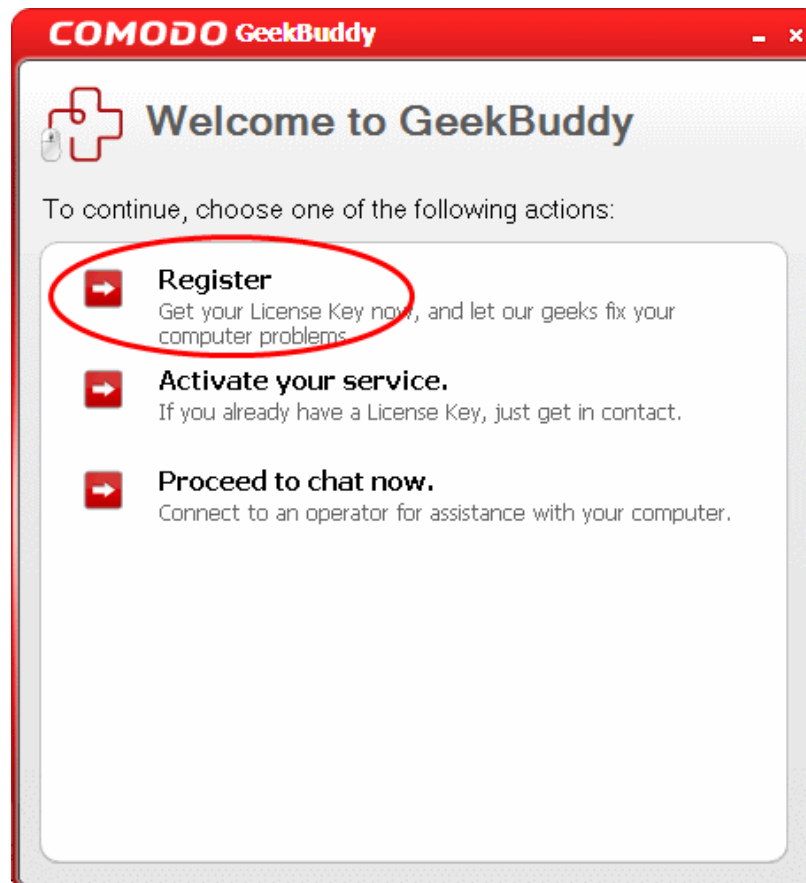


Congratulations, you just finished your first GeekBuddy support session. We hope you enjoy using your trouble-free computer.

## 6.4 Registration

To become a paid subscriber of the Comodo GeekBuddy services, you need to register your account with Comodo using our online registration form.

### To register your account



- Click the 'Register' link and you will be taken to the purchase order form. Fill in the details as required in the order form and follow the process.

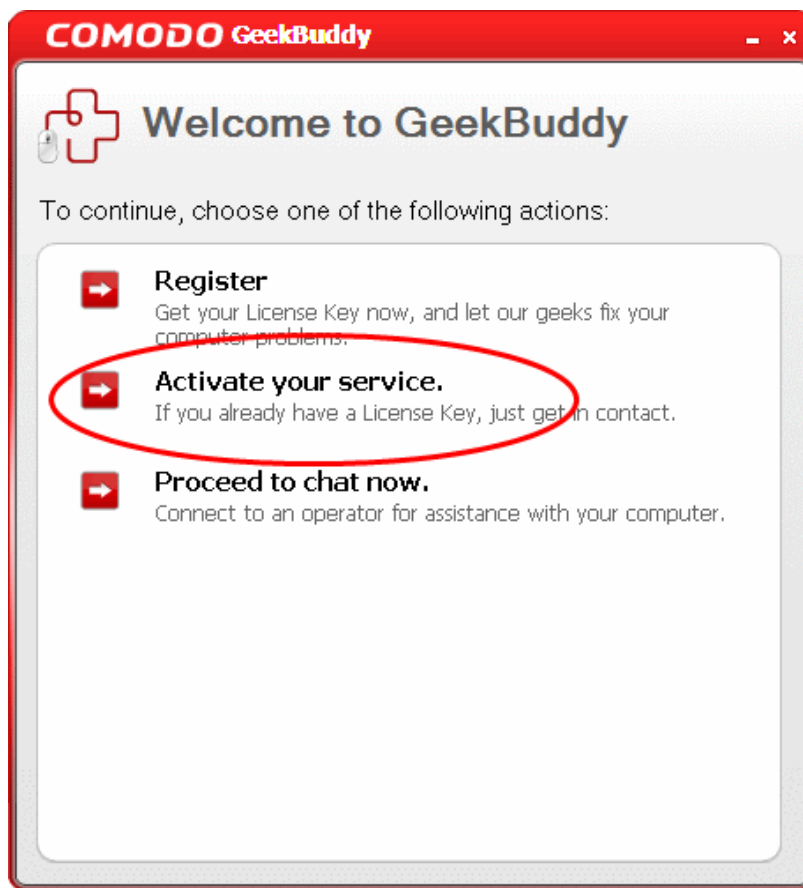
Your account with GeekBuddy will be created and your License Key in the order confirmation will be sent to you to the email address provided in the purchase order form. You need to enter this License Key when you access the service for the first time.

Registration is a one time process for a single machine.

The Comodo GeekBuddy license entitles you to usage of the service on up to three machines. You need to enter the license key when you are installing the client and registering the account from a different machine. So keep the License Key in a safe place.

## 6.5 Activation of Service

To start using the Comodo GeekBuddy service, start the client using any of the methods explained [above](#). Click on any of the service options and the activation screen will open.

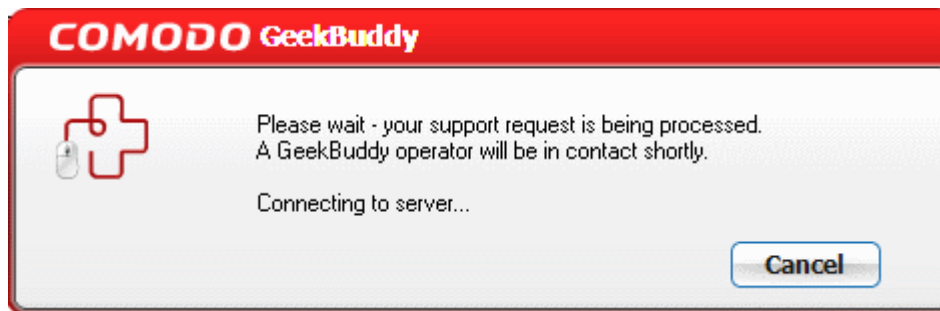


For first time usage, you need to enter the License Key that you received via email. Enter your License Key and click 'Next'.

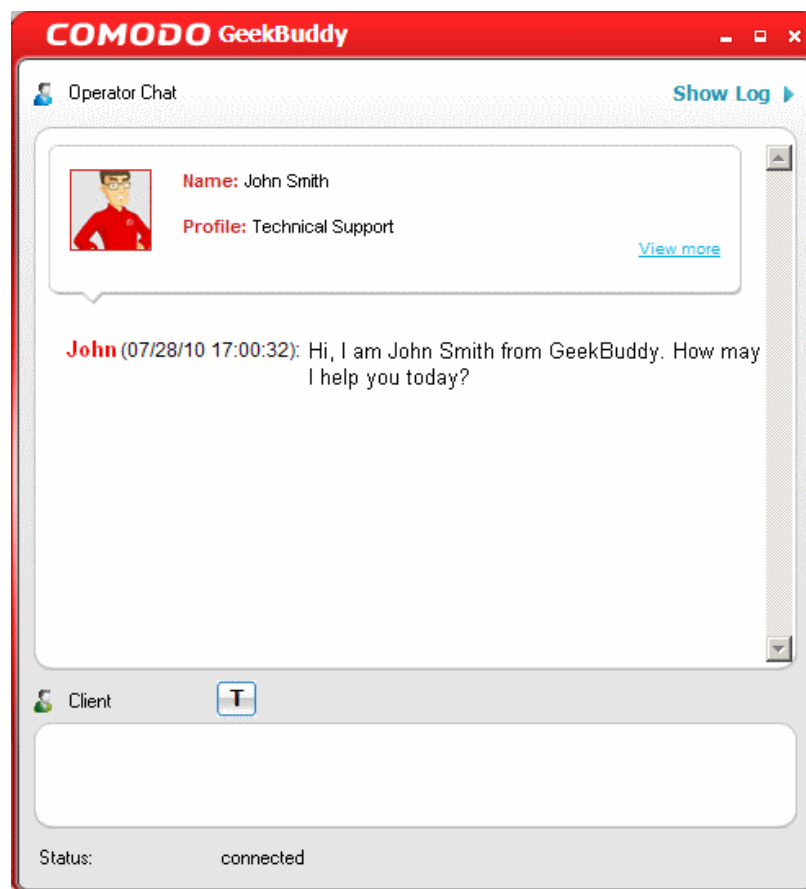


Your account will be verified and activated. The verification and activation is a one-time process. You need not enter the License Key again.

Following activation, you will be connected to the GeekBuddy service...



...and within seconds, a Comodo Support Technician will respond in a chat window and ask you to describe the problem.



- Start chatting! Use the chat window to explain any problems you are having with your computer, or to request any of the GeekBuddy services.

## 6.6 Uninstalling Comodo GeekBuddy

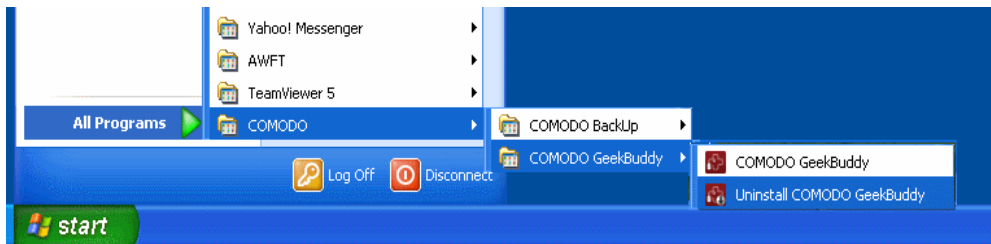
### To uninstall Comodo GeekBuddy:

- Click Start > Settings > Control Panel
- In the Control Panel, double-click Add/Remove Programs
- In the list of currently installed programs, click Comodo GeekBuddy
- Click the 'Change/Remove' button.

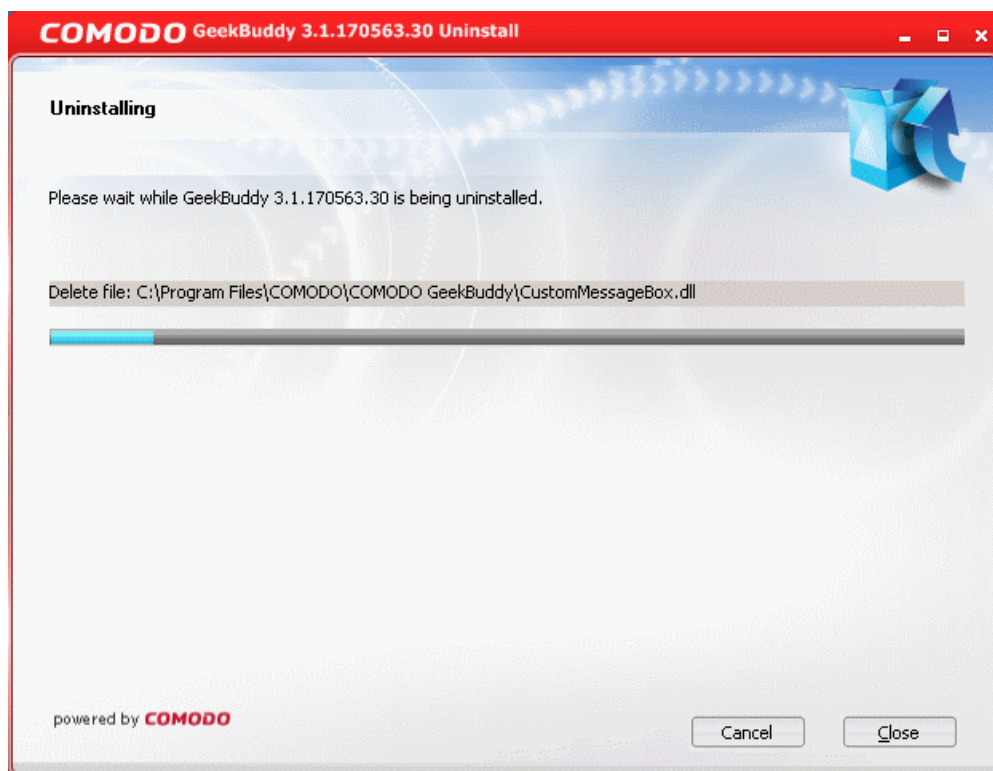


Or

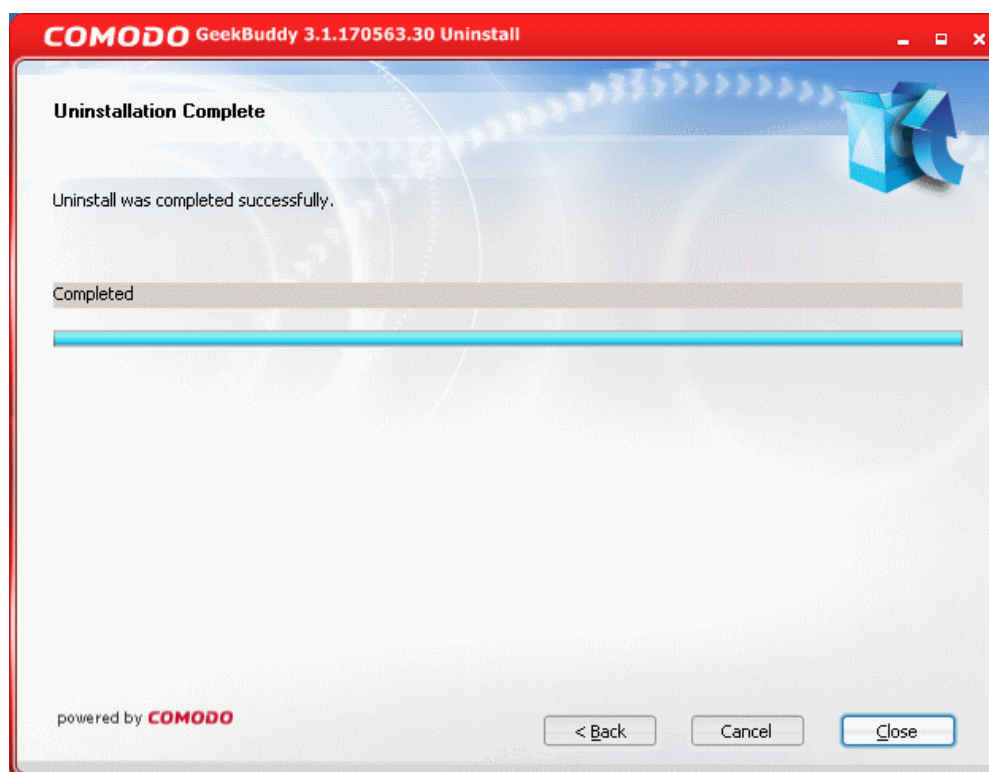
- Click Start > All Programs > Comodo > Comodo BackUp > Uninstall Comodo GeekBuddy



The un-installation wizard will start and the un-installation progress will be displayed...



Upon completion, the 'Uninstallation Complete' dialog will be displayed.



Click 'Close' to finish the process.

## 7 Live PC Support

Comodo Internet Security Pro and Complete customers receive **Live PC Support** - the quickest, most comprehensive way of getting help with your computer problems. Simply clicking the 'Live Support' button will open a chat window with a Comodo security expert where you can ask questions or request that a service be performed on your computer. Services include items such as virus removal and PC troubleshooting and are executed by our expert accessing your computer through a remote desktop connection. Those wishing to test the service should take advantage of the **30 day free trial**.

Please visit <http://www.livepcsupport.com> for full product details. Please visit <http://personalfirewall.comodo.com> to sign up for Comodo Internet Security - Pro.

- [Overview of Services](#)
- [Launching the Client and Requesting the Services](#)
- [Uninstalling the LivePCSupport Client](#)

### 7.1 Overview of the Services

Live PC Support is carried out by Comodo security experts establishing a remote desktop connection to your machine and fixing your computer's 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.

- **Our experts are available 24 hours per day** to perform any service or answer any support question
- **Unlimited incidents on up to 3 home or work PC's.** Each Comodo Internet Security Pro or Complete license allows you to call upon the Live PC Support services listed below as many times as you need them.
- **Initiate an Online Chat session anytime.** If you request it, our technicians will use the chat window to remotely connect to your machine and solve your problem.
- **Enjoy using your problem-free computer once again !!**

Comodo Internet Security Pro and Complete subscribers receive LivePCSupport:

- **Virus Diagnosis / Removal** - Your PC is thoroughly checked for viruses and spyware. If any are discovered then they are expertly removed and your computer restored to its pre-viral state.
- **PC Tune Up** - Expert evaluation of issues affecting your computer's performance. Fine Tuning key areas and improving speed and stability.
- **Internet Login Protection** - Activating your computer's basic security settings to prevent loss of sensitive data and identity theft.
- **Email Account Set Up** - Setting up your Internet-based email account - any provider, any account. Great for new computers and novice email users.
- **Software Installation** - Installing your Comodo products and customizing configuration for maximum security protection and efficiency.
- **Printer Set Up and Troubleshooting** - Installing or updating software and printer drivers, checking ink levels and configuring your printer to work on a wireless or wired network.
- **Green PC** - Optimizing your power management setting based on how you use your computer. Go green and save money on your electric bill.
- **Computer Troubleshooting** - Checking basic hardware conflicts in Windows.



**Note 1:** In all cases, you must have your subscription ID ready. Your subscription ID can be found in your Comodo Internet Security Pro order confirmation email and for the CIS Complete version, the subscription ID is printed on the DVD itself or printed on an insert included in the box packaging.

**Note 2:** The services listed above describe only the LivePCSupport component of Pro and Complete package. [Click here to see full Pro and Complete package details.](#)

## 7.2 Launching the Client and Requesting the Service

The Live PC Support service requires the Live PC Support client installed in your system. The client is installed automatically while installing CIS Pro or CIS Complete. You can start the client and start a live chat session with a Live PC Support expert using any one of the following methods:



- Double click the LivePCSupport desktop icon 
- Click the LivePCSupport system tray icon 
- Launch the LivePCSupport client directly from the Windows Start Menu - Click All Programs > COMODO > LivePCSupport > Comodo LivePCSupport.

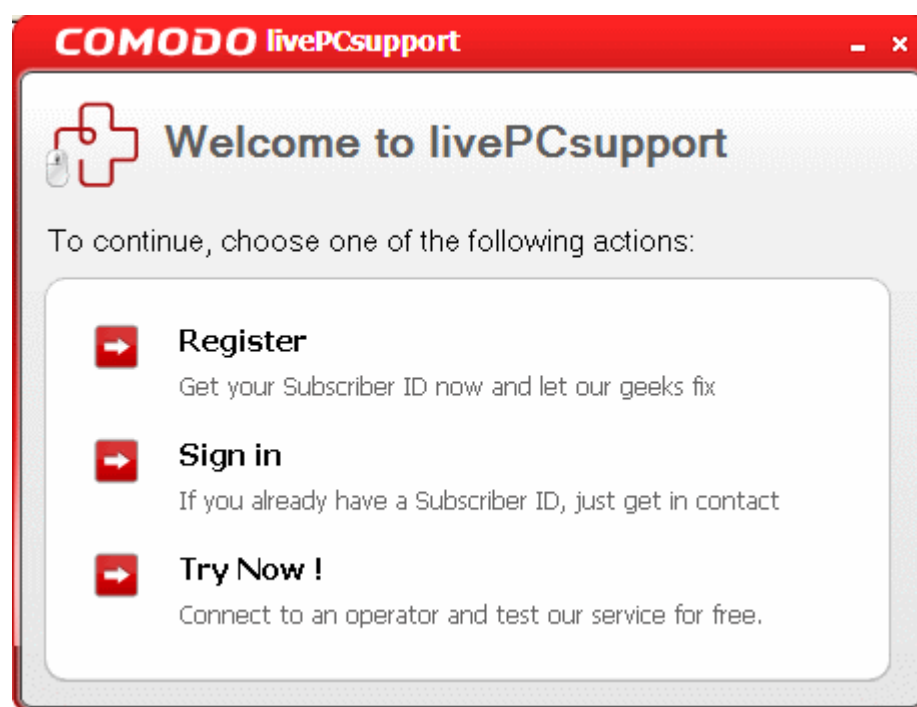
The LivePCSupport login options dialog will be displayed:



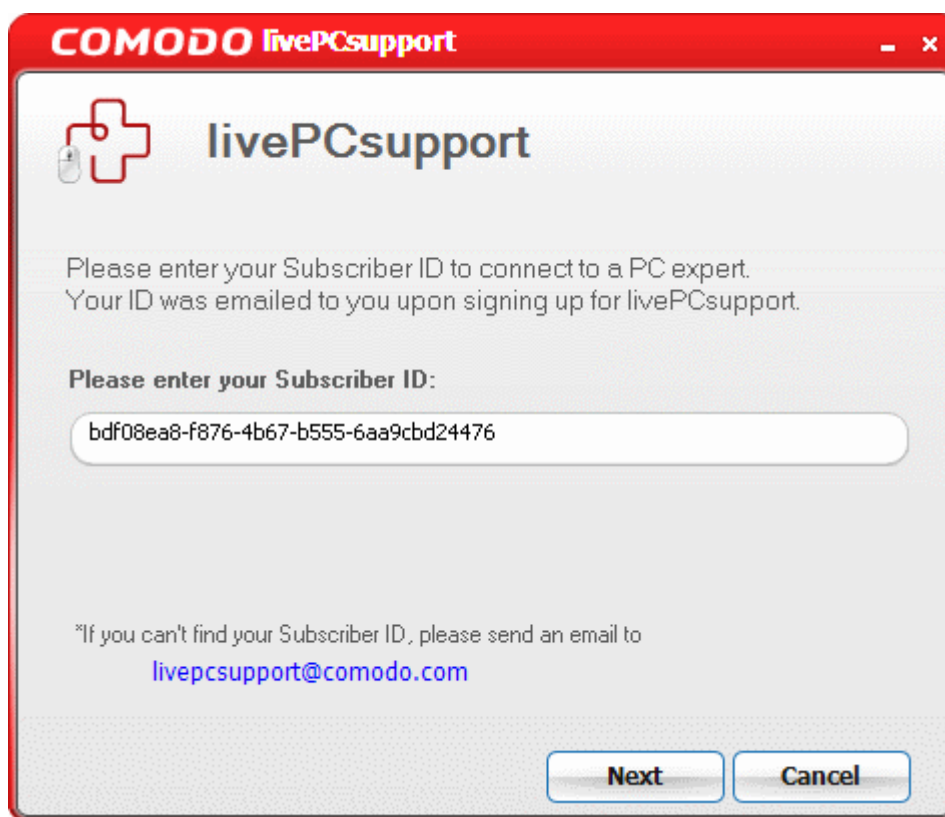
Select the type of service you need:

- **Virus Infection** - Select if you need assistance in removing viruses, malware etc. from your system.
- **Other** - Select if you need assistance in removing registry errors, privacy issues, junk files, and other Windows/System related problems.

You will be connected to the technician skilled in the specific area. Clicking any of the options will open the registration screen.

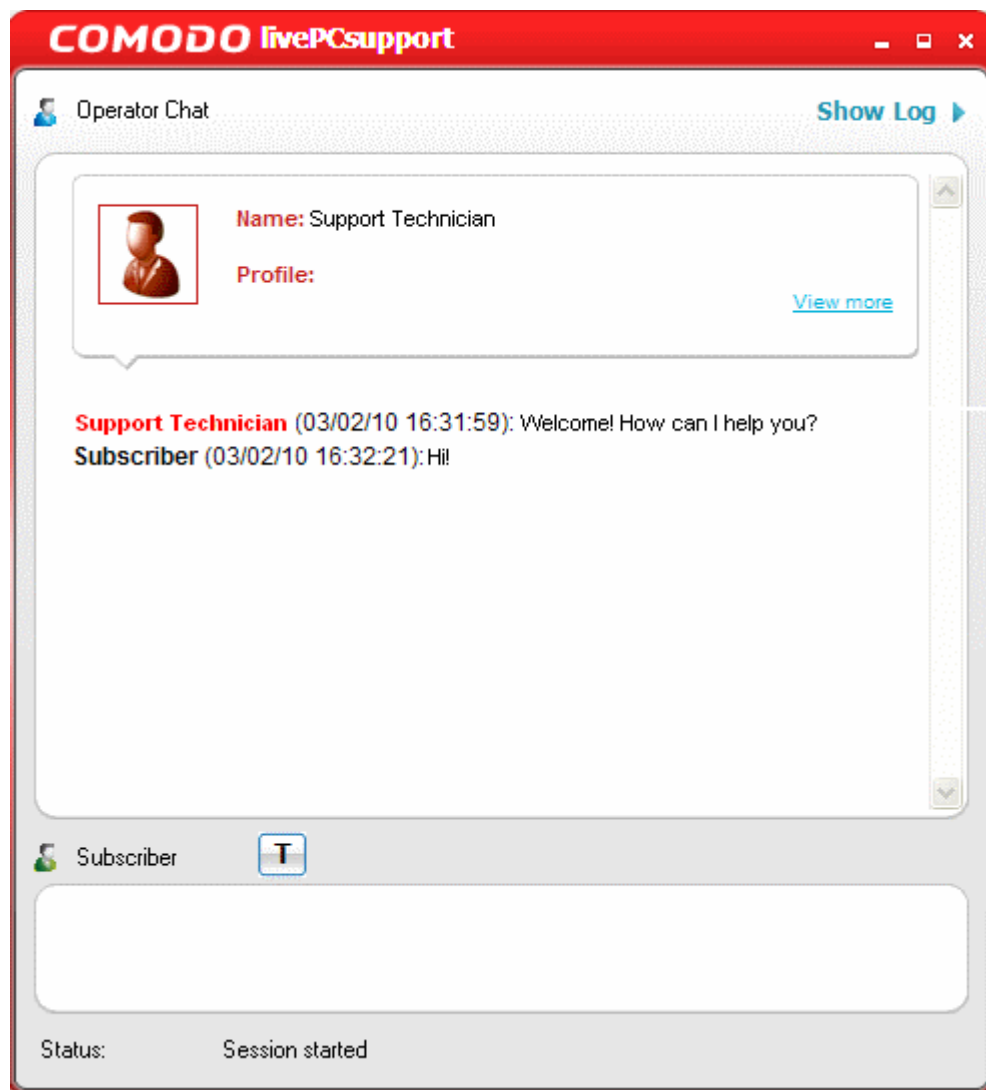


Select 'Sign in'...



...and enter your Subscriber ID in the 'Subscriber ID:' text box and click 'Next'.

Within seconds, a Comodo Support Technician responds in a chat window and ask you to describe the problem.



Type your question in the text box and press Enter key.

The qualified Comodo security technician will help you with any questions you may have. If necessary, they may access your computer through a remote desktop connection to implement the changes and fixes necessary to solve your problem and get your PC working perfectly.

## 7.3 Uninstalling Live PC Support Client

### To Uninstall Live PC Support Client

Click All Programs > COMODO > LivePCSupport > Uninstall.

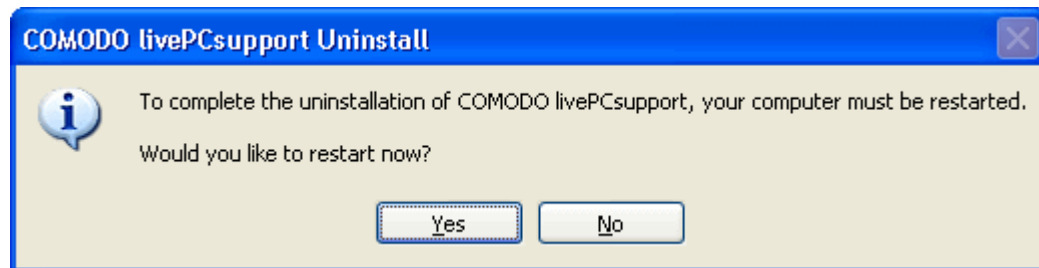
Or

1. Open the Control Panel.
2. Double click 'Add/Remove Programs'.
3. Select 'Comodo LivePCSupport'.
4. Click 'Remove'.

The uninstall confirmation dialog appears.



5. Click 'Yes'. The uninstall progress is indicated. You must restart your system for the uninstallation to take effect.



6. Click 'Yes' for completing the uninstallation process and restarting your system.

You can email any questions to: [cisquestions@comodo.com](mailto:cisquestions@comodo.com)

For technical product questions please visit: <https://support.comodo.com/> (Comodo's Customer Service management system requires you to establish a free service account. Your service account provides access to Comodo's extensive Knowledge base, Customer Forums, and Live Chat support and offers the ability to submit support requests into our service management system.)

## 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.

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 Suite Pro/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 Suite Pro/Complete TrustConnect account has a 10 GB/month data transfer limit.

Comodo Internet Security Pro/Complete customers also receive the \$99 value 'Total Security and Support' LivePCsupport package. Please visit <http://www.livepcsupport.com> for full product details. Please visit <http://personalfirewall.comodo.com> to sign up for Comodo Internet Security Pro.

### 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**

## 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 Pro or 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.

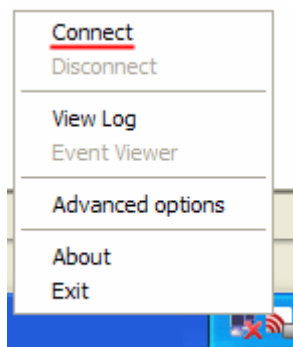
### Establish a connection to TrustConnect

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 > Trust 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 at the foot of this page.

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.



Welcome: John

- Comodo Internet Security
- TrustConnect
- My Account
- Help
- Contacts

## Comodo TrustConnect

<b>Service Login</b>	jsmith
<b>Service Password</b>	1aB2cdeeFG
<b>License key</b>	e11b3e35-937d-47af-957d-a2207a4c75b2
<b>Date from</b>	2010-08-16 06:40:09
<b>Date to</b>	2011-08-16 06:40:09
<b>Traffic</b>	
<b>Limit:</b>	10 GB
<b>Available:</b>	10 GB
<b>Today</b>	
No data found.	
<b>This month</b>	

[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:

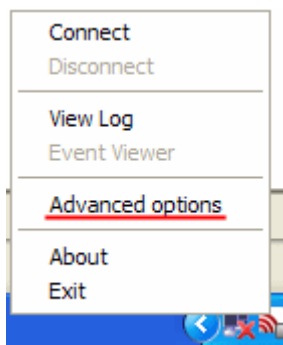


<i>Not Connected to TrustConnect</i>	<i>Attempting to connect to TrustConnect</i>	<i>Successfully connected to TrustConnect</i>
--------------------------------------	--	---

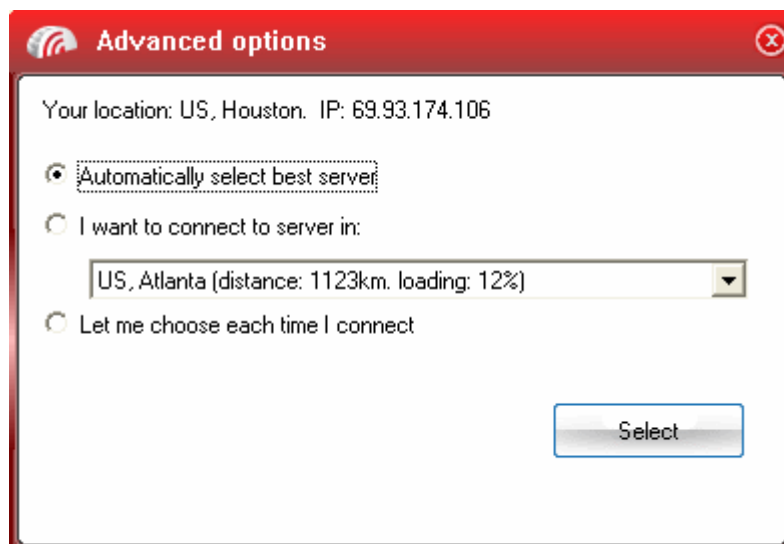
## Advanced Options

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.



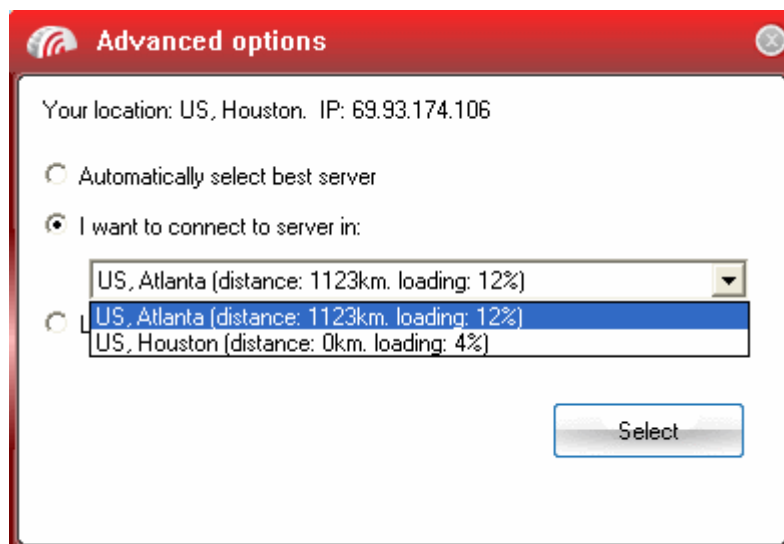
You can configure the server selection from the options :

- **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.

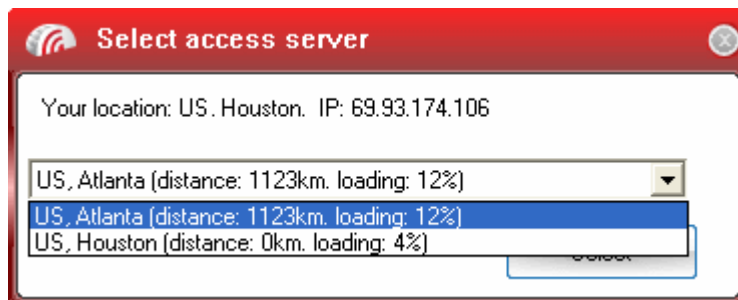
**Note:** It is always recommended to choose a server nearest to your location for quicker access.

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](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 OR 7 day trialists, download: <https://accounts.comodo.com/download/trustconnect/client.conf>
  - Users of TrustConnect FREE service should download: [http://download.comodo.com/trustconnect/free\\_client.conf](http://download.comodo.com/trustconnect/free_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 OR 7 day trialists, download:  
<https://accounts.comodo.com/download/trustconnect/client.conf>
  - Users of TrustConnect FREE service should download:  
[http://download.comodo.com/trustconnect/free\\_client.conf](http://download.comodo.com/trustconnect/free_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

**Note:** The TrustConnect RedHat Client is not available for users of the free service. Users of the free service should download and install the OpenVPN client as detailed earlier in this document.

## 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](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"

**Note:** The TrustConnect Ubuntu Client is not available for users of the free service. Users of the free service should download and install the OpenVPN client as detailed earlier in this document.

## 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 TrustConnect FAQ

### Common Questions

How do I set up TrustConnect and Log on to the TrustConnect Server?

My User Name and Password don't work - why not?

What Operating Systems does TrustConnect support?

What clients should I use to connect to the TrustConnect Server?

All our Internet (HTTP & HTTPS) connections are via a proxy server. How do I connect using TrustConnect in this situation?

Why do I need a Secure Connection like Comodo TrustConnect?

What is a Sniffer?

What types of TrustConnect Accounts are available?

What Subscription Plans are available for the full service?

Can I buy additional traffic when I need it?

What is the difference between the free service and the paid license service?

How do I switch to a full account and remove these limitations?

Do I have to use a wireless connection to use Comodo TrustConnect?

I have a Wi-Fi at home with WEP turned on. Am I safe?

Is the TrustConnect license for only one computer, or can I install it on others in my home network?

What is the typical connection speed through TrustConnect?

What happens at the end of the TrustConnect Trial?

How do I cancel my account?

What security measures does TrustConnect use?

Can TrustConnect work on a PC behind a NAT-enabled router?

### Windows Configuration

What is the "TAP-Win32 Adapter" that appears in my "Network Connections"?

I'm sure I've done everything correctly but I still cannot connect to the server.

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?

Do I need my Firewall up while connecting to the WEB via TrustConnect?

What port numbers are used by TrustConnect?

### Windows Vista Configuration

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?

All adapters are located in correct place, but I still cannot connect to the server.

### iPhone/iPod Client Configuration

The server did not respond when I try to connect.

What are the TrustConnect server addresses?

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 Pro/Complete enrollment process.
2. Click the 'TrustConnect' tab on the top navigation bar.

- 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

[Download TrustConnect Windows Client Configuration Guide \(pdf\)](#)

[Download the Windows TrustConnect Client](#)

## MAC OS X

[Download TrustConnect MAC OS X Client Configuration Guide \(pdf\)](#)

## Linux / OpenVPN

[Download TrustConnect Linux Client Configuration Guide \(pdf\)](#)

## iPhone / iPod Touch

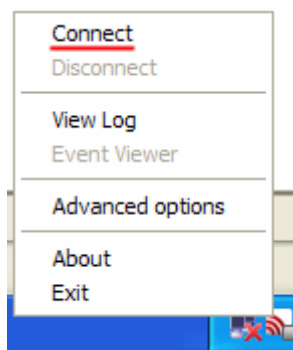
[Download TrustConnect iPod Client Configuration Guide \(pdf\)](#)

- 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.



Welcome, John

- Comodo Internet Security
- TrustConnect
- My Account
- Help
- Contacts

## Comodo TrustConnect

<b>Service Login</b>	jsmith
<b>Service Password</b>	1aB2cdeeFG
<b>License key</b>	e11b3e35-937d-47ef-957d-a2207a4c75b2
<b>Date from</b>	2010-08-16 06:40:09
<b>Date to</b>	2011-08-16 06:40:09

Traffic	
<b>Limit:</b>	10 GB
<b>Available:</b>	10 GB
<b>Today</b>	
No data found.	
<b>This month</b>	

**Comodo TrustConnect - User Authentication**

Username:

Password:

Remember

6. The TrustConnect tray icon turns green upon successful connection:



### 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 Pro/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 Pro/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

[Download TrustConnect Windows Client Configuration Guide \(pdf\)](#)

[Download the Windows TrustConnect Client](#)

#### MAC OS X

[Download TrustConnect MAC OS X Client Configuration Guide \(pdf\)](#)

#### Linux / OpenVPN

[Download TrustConnect Linux Client Configuration Guide \(pdf\)](#)


#### iPhone / iPod Touch

[Download TrustConnect iPod Client Configuration Guide\(pdf\)](#)

### 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:

- i. 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: `stConnect\bin\TrustConnect.exe" --allow_proxy 1`

- 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.

### What are types of TrustConnect accounts are available?

There are 3 main 'types' of TrustConnect Account

- **FULL** - Subscription based. Users get access to all features of the TrustConnect service.
- **TRIAL** - Unlimited 7 day trial which includes all the functionality that is available in the paid service.

- **FREE** - 'Free for life' service that includes certain service restrictions. For more details, see '[What's the Difference between the Free Service and the Paid License Service?](#)'.

## What Subscription Plans are Available for the full service?

The following plans are available for the TrustConnect service:

- Daily Pass - \$3.99 for 24 hours access
- Monthly Plan - \$6.99 per month, 1 user account, unlimited traffic
- Annual Plan - \$49.99 per year, 1 user account, unlimited traffic

The following business packages are also available:

- Corporate Monthly - \$25.00 per month, 5 user accounts, 500 GB total traffic
- Corporate Annual - \$200.00 per year, 5 user accounts, 500 GB total traffic

## Can I buy Additional traffic when I need it?

Yes, additional traffic limit can be added to your account at anytime.

- Login to your Comodo account at <https://accounts.comodo.com> with your user-name and password
- Click the 'TrustConnect' tab on the top navigation bar (or select 'TrustConnect' from the 'Service' menu button)
- Click 'Buy extra traffic' on the right hand side then sign up for the plan that fits your requirements

## What's the Difference between the Free Service and the Paid License Service?

The free service is:

- Limited to 10 GB of traffic per month
- Location services are not available to free users (i.e. users are not able to select which server they connect to in 'Advanced Options')
- Free service features small banner adverts
- Free service does not allow certain protocols to be used. These include FTP, SMTP, NNTP and NTP

**Note:** POP3 and IMAP protocols ARE allowed, so you can check online mail accounts like Gmail or Yahoo mail. Instant Messengers such as MSN and ICQ can also be used.

- The proprietary TrustConnect client for RedHat and Ubuntu Linux distributions is not available for free users. Users are, of course, free to use the OpenVPN client to configure the service.

## How do I switch to a full account and remove these limitations?

If you've already signed up for a free account and want to upgrade to the full service:

- Login to your Comodo account at <https://accounts.comodo.com> with your user-name and password
- Click the 'TrustConnect' tab on the top navigation bar (or select 'TrustConnect' from the 'Service' menu button)
- Click 'Change Plan' then sign up for a subscription plan that fits your requirements

## 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.

## What happens at the end of the TrustConnect Trial?

Once your **7 day trial** period is over you are automatically switched over to the full monthly or annual plan that you enrolled for.

## 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](mailto: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.

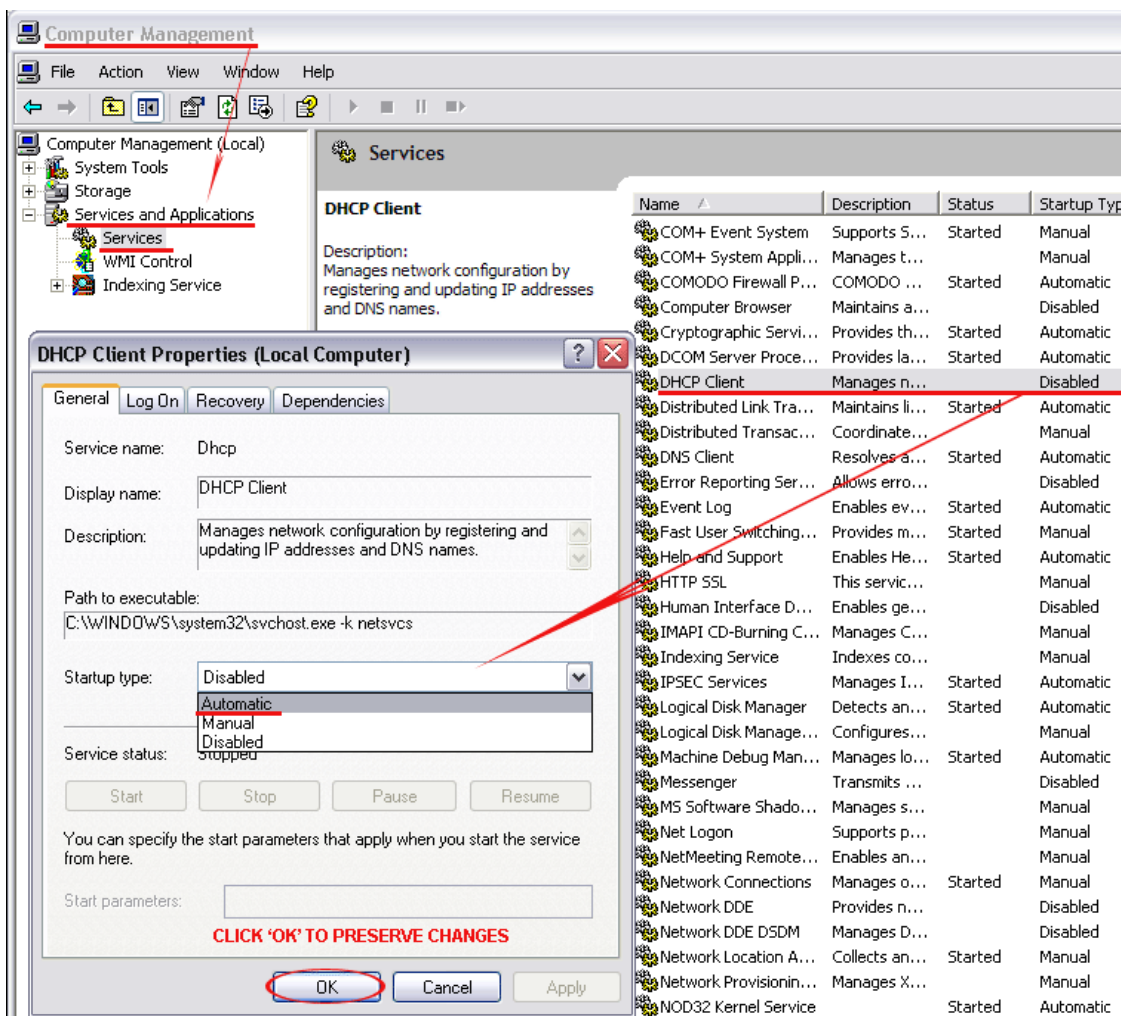
### I can connect to the server, but cannot get access to any site. IPCONFIG /ALL shows IP 0.0.0.0 for the TAP adapter. What is wrong?

The DHCP Client service MUST be enabled.

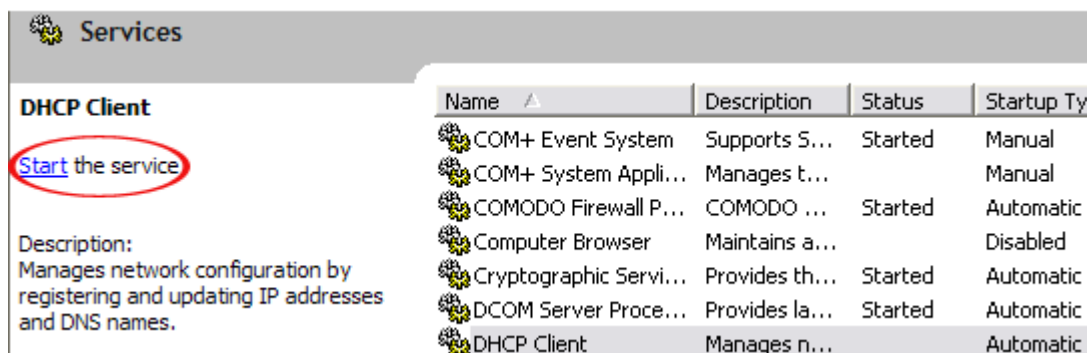
#### To enable this service, you need to:

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.



### 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).

# Appendix 1 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 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 : 156.154.70.22

Secondary DNS : 156.154.71.22

**Important Note:** If you have chosen to install CIS in a language other than English then the DNS Server addresses to be entered are:

Primary DNS : 156.154.70.25

Secondary DNS : 156.154.71.25

## To stop Comodo Secure DNS service

- **Modify the DNS server IP address to your previous settings.**

## To modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

http://192.168.0.1

http://192.168.1.1

http://192.168.10.1

If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).

**DNS AND ADVANCED SETTINGS**

**Use these DNS Servers :**

**Primary DNS Server :**

**Secondary DNS Server :**

**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: 156.154.70.22

Secondary DNS server address for Comodo Secure DNS is: 156.154.71.22

**Important Note:** If you have chosen to install CIS in a language other than English then the DNS Server addresses to be entered are:

Primary DNS Server : 156.154.70.25

Secondary DNS Server : 156.154.71.25

When you are done, the above example would look like this.

**DNS AND ADVANCED SETTINGS**

**Use these DNS Servers :**

**Primary DNS Server :**

**Secondary DNS Server :**

**Advanced >>**

You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.
- or
- Entering different preferred and alternate DNS server IP addresses.

## Windows XP - Manually 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 : 156.154.70.22

Alternate DNS : 156.154.71.22

**Important Note:** If you have chosen to install CIS in a language other than English then the DNS Server addresses to be entered are:

Preferred DNS : 156.154.70.25

Alternate DNS : 156.154.71.25

### To stop Comodo Secure DNS service

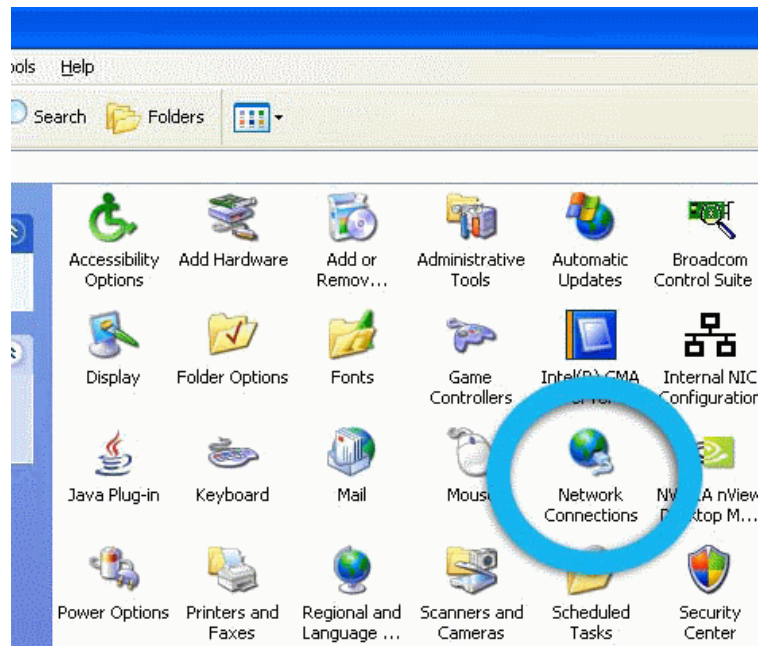
- **Modify the DNS server IP address to your previous settings.**

### To modify the DNS settings

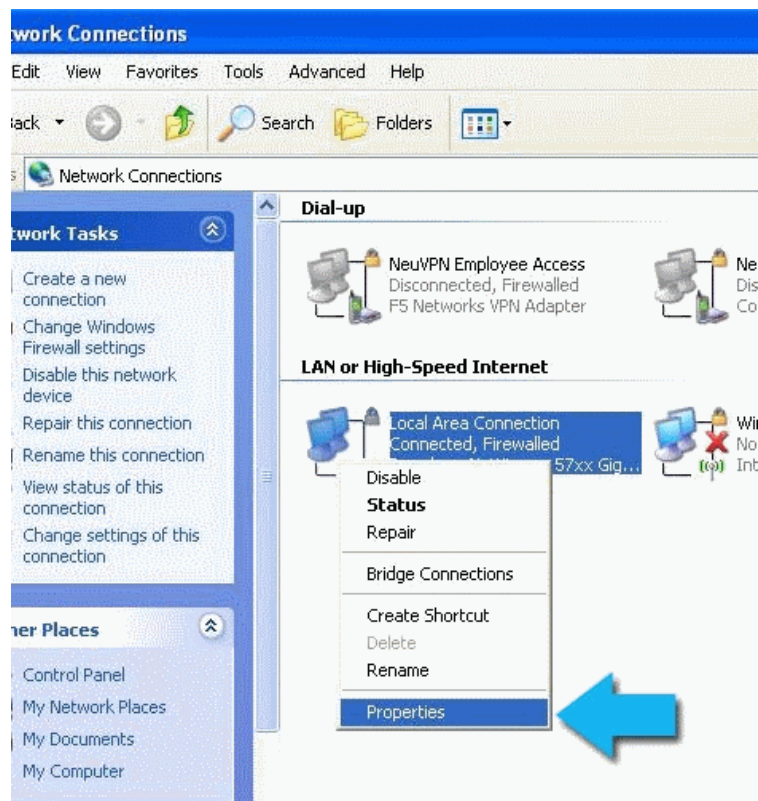
1. Select the 'Control Panel' from the Start Menu.



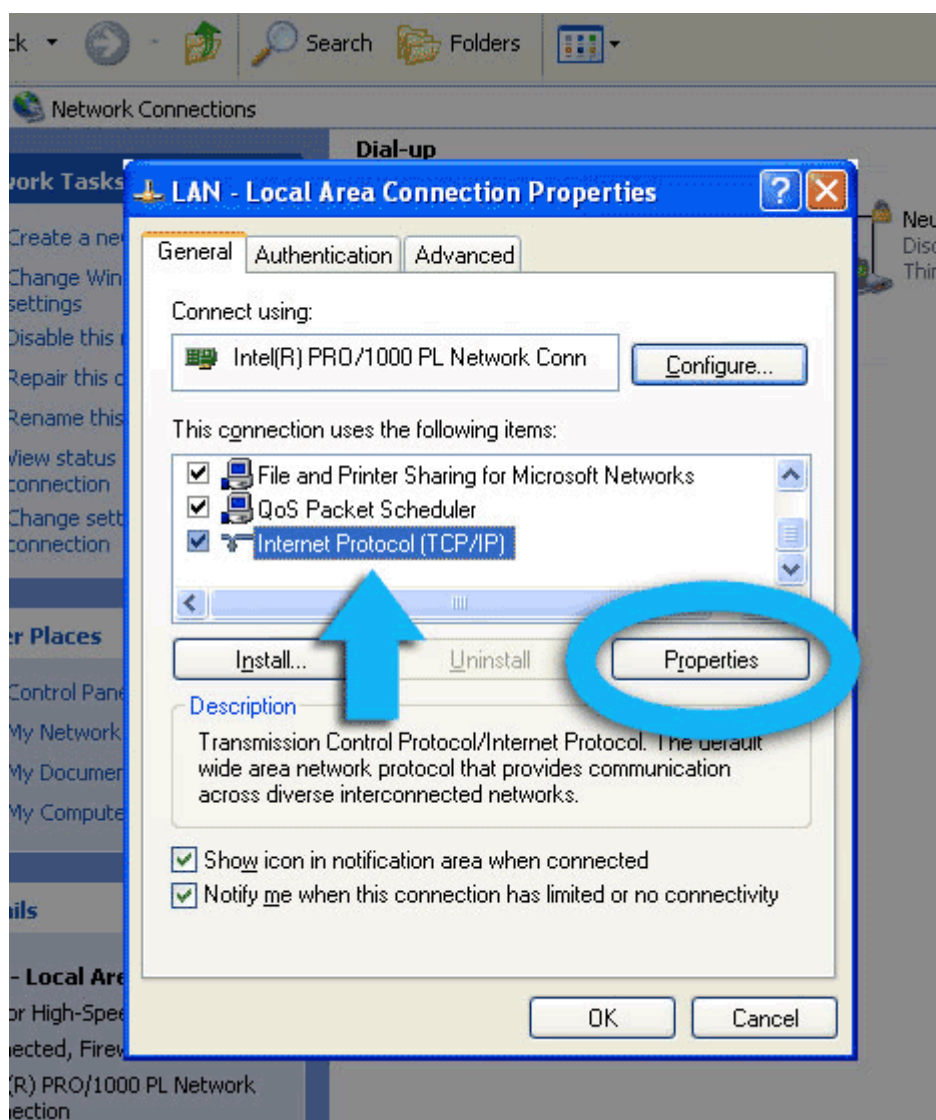
2. Click 'Network Connections' from the Control Panel options.



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: 156.154.70.22

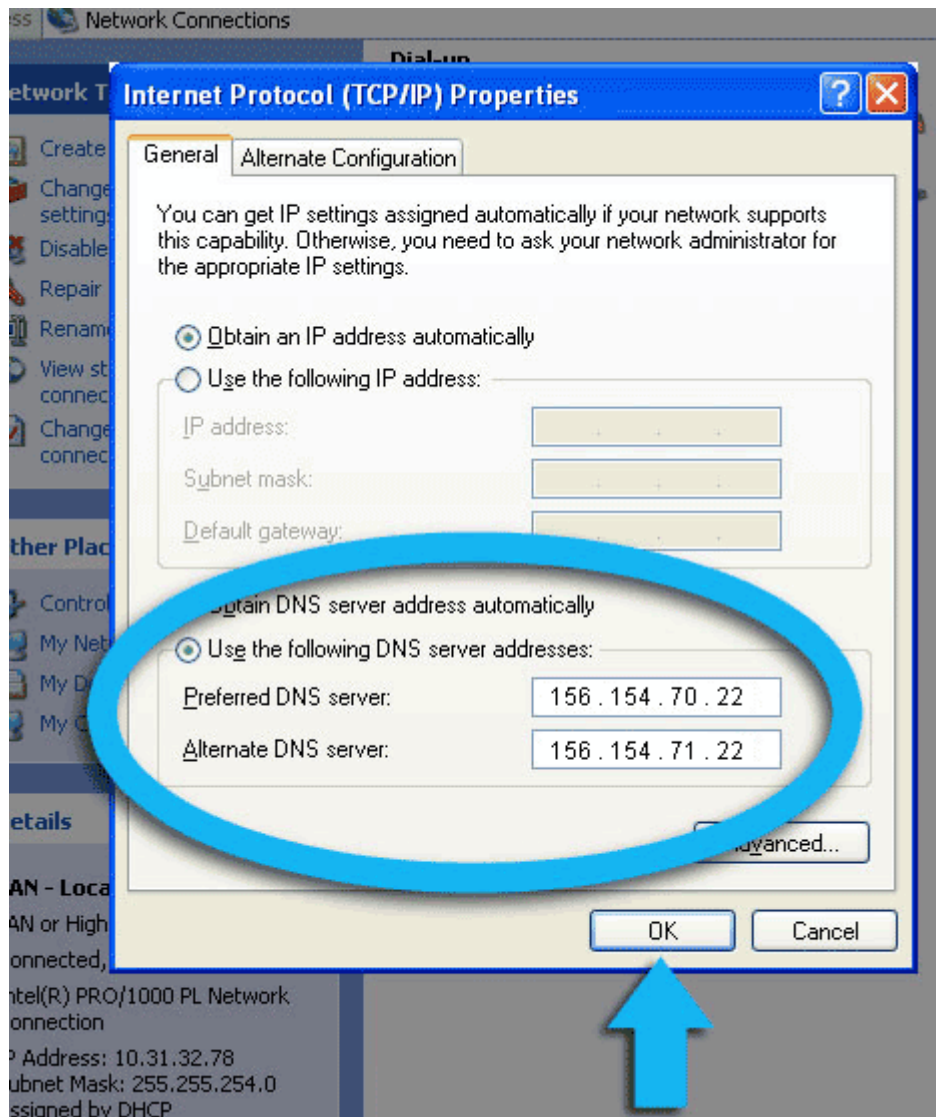
Alternate DNS server address for Comodo Secure DNS is: 156.154.71.22

**Important Note:** If you have chosen to install CIS in a language other than English then the DNS Server addresses to be entered are:

Preferred DNS : 156.154.70.25

Alternate DNS : 156.154.71.25

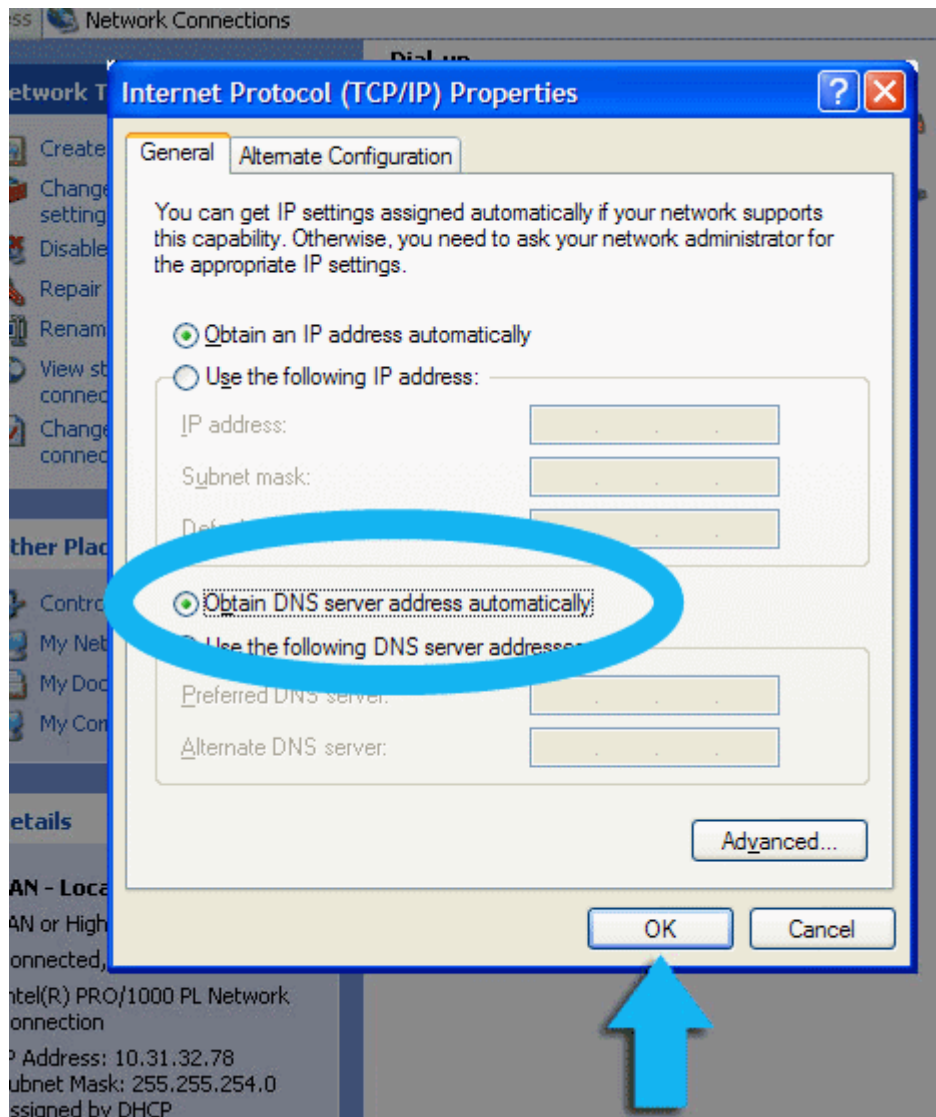




You can disable Comodo Secure DNS by:

- 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 Vista - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Windows Vista computer by modifying the DNS settings accessible through Control Panel > Network and Internet settings.

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 : 156.154.70.22

Alternate DNS : 156.154.71.22

**Important Note:** If you have chosen to install CIS in a language other than English then the DNS Server addresses to be entered are:

Preferred DNS : 156.154.70.25

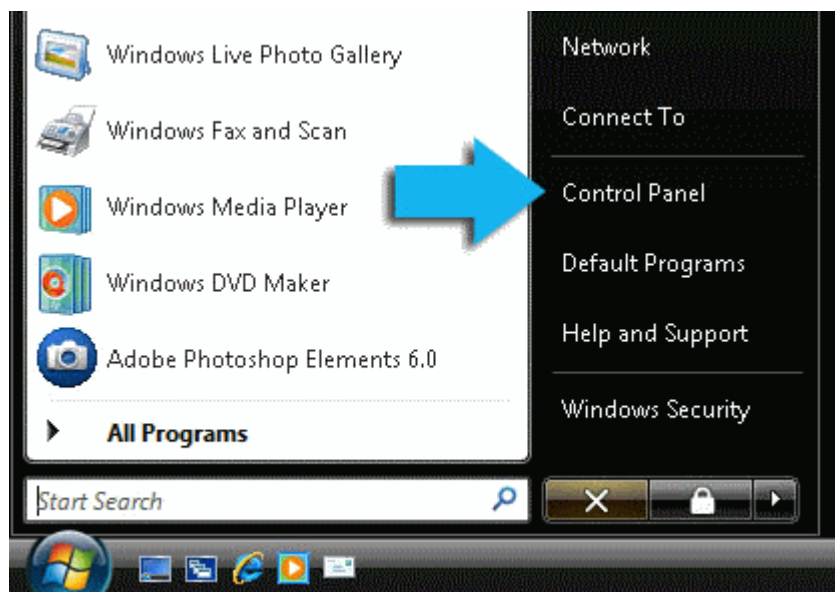
Alternate DNS : 156.154.71.25

### To stop Comodo Secure DNS service

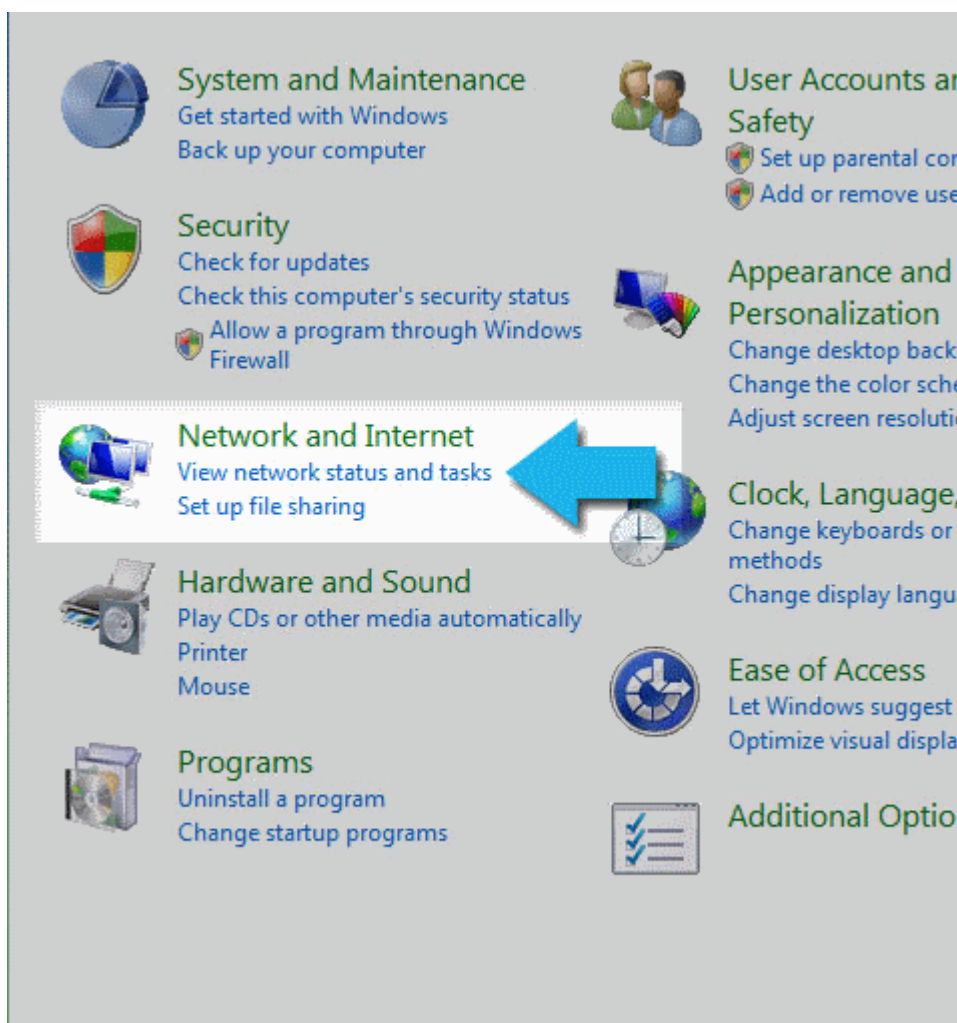
- **Modify the DNS server IP address to your previous settings.**

### To modify the DNS settings

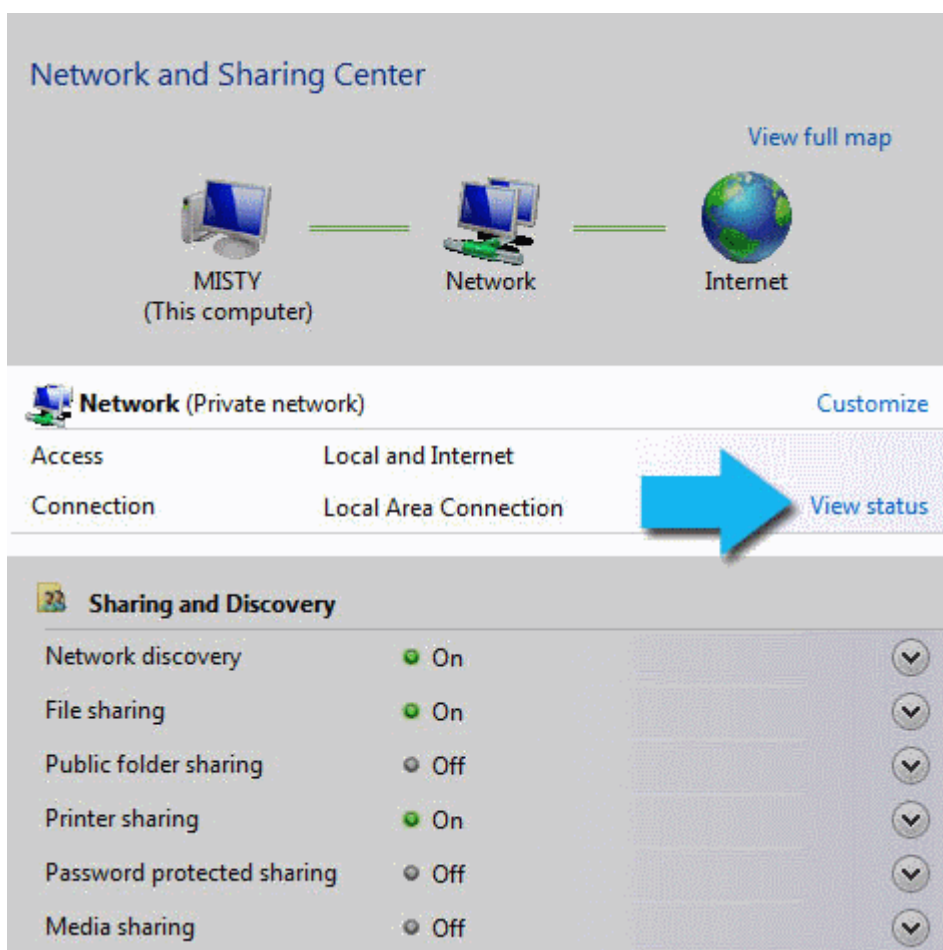
1. Click the 'Start', then select 'Control Panel'.



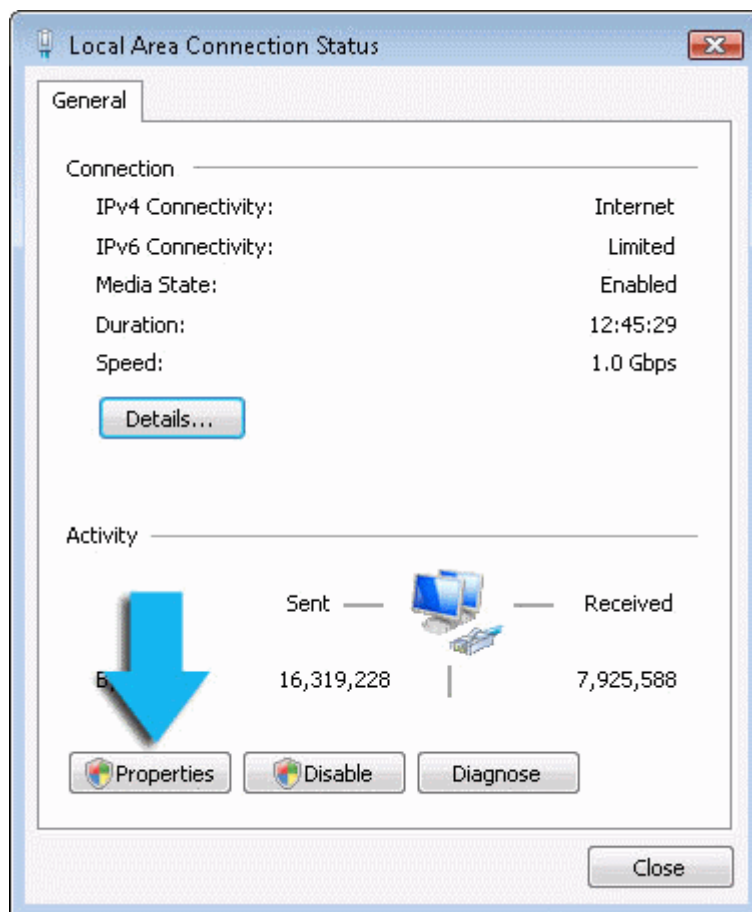
2. Click on 'View network status and tasks'.



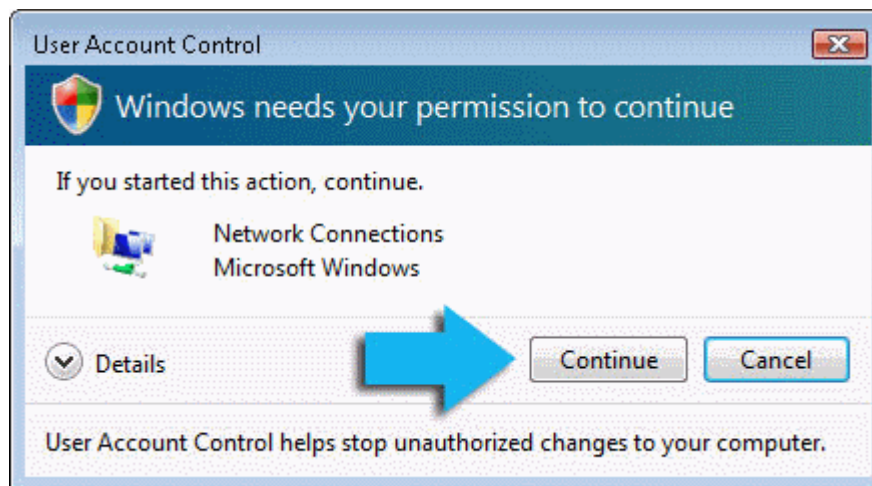
3. Click on 'View Status'.



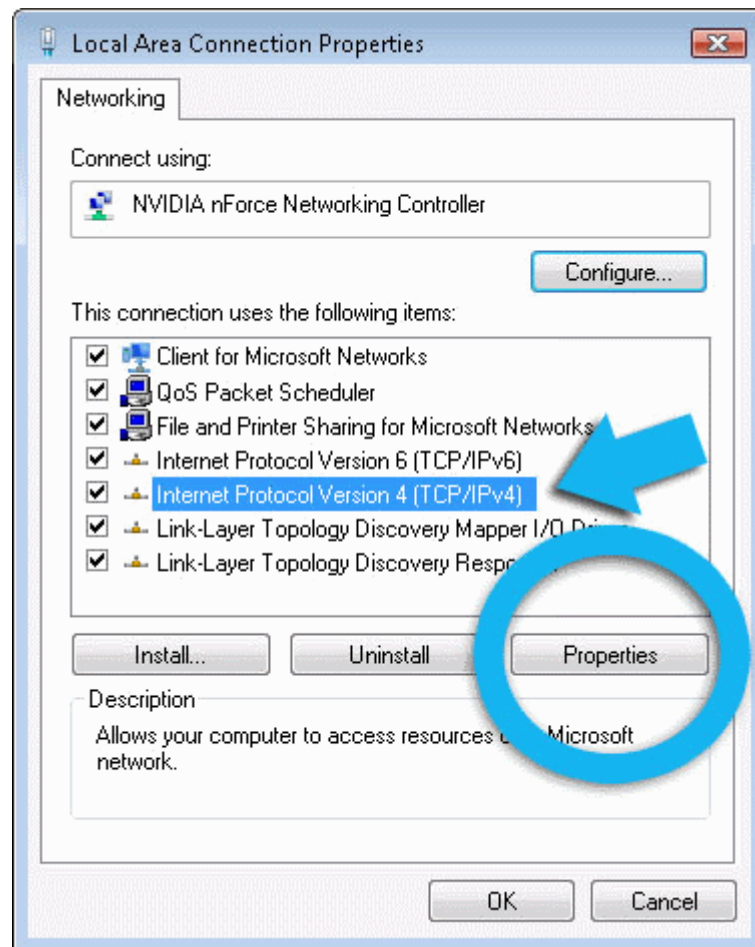
4. Click the 'Properties' button.



5. Vista may ask for your permission to make changes. If so, click the 'Continue' button.



6. Select 'Internet Protocol Version 4 (TCP/IPv4)', then click the 'Properties' button.



7. 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.

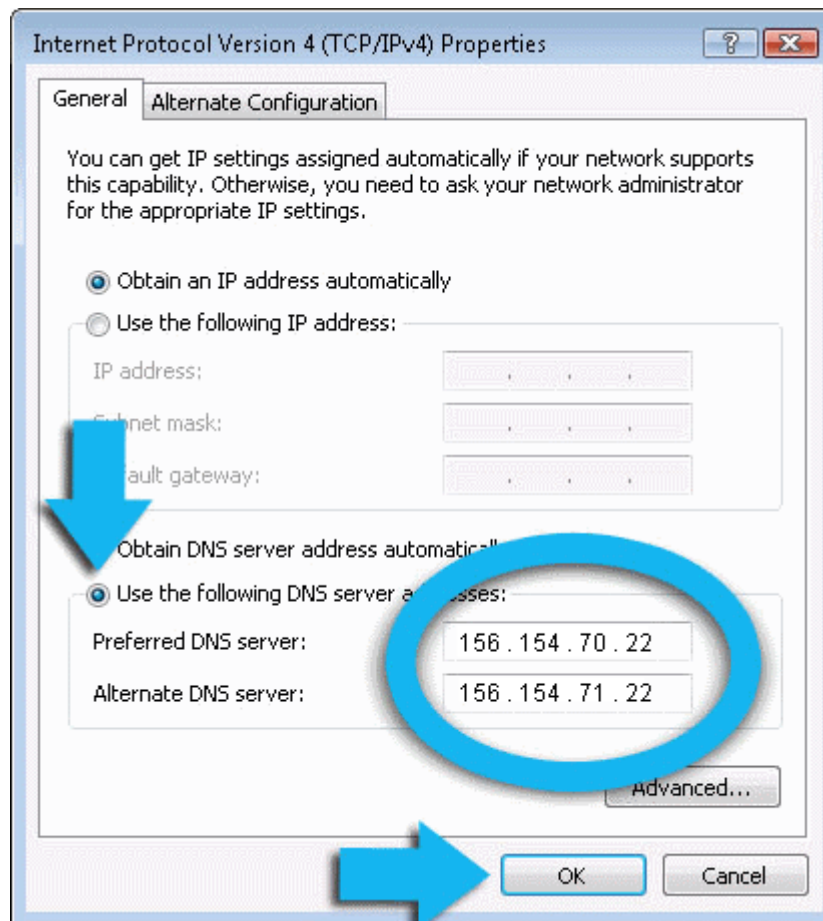
Preferred DNS server address for Comodo Secure DNS is: 156.154.70.22

Alternate DNS server address for Comodo Secure DNS is: 156.154.71.22

**Important Note:** If you have chosen to install CIS in a language other than English then the DNS Server addresses to be entered are:

Preferred DNS : 156.154.70.25

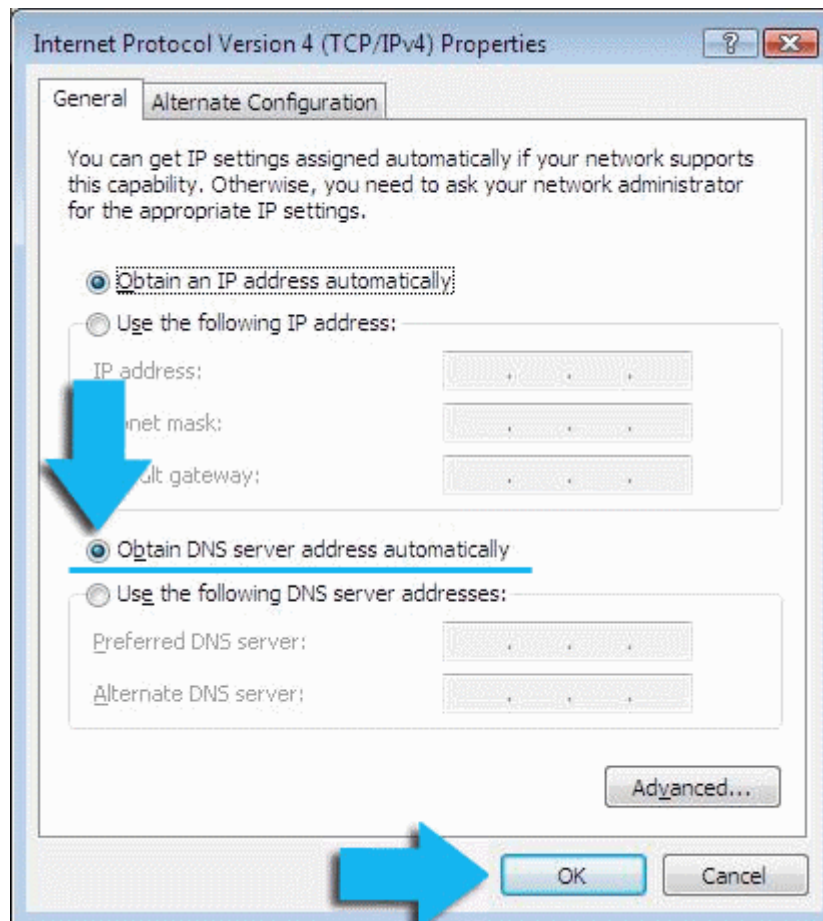
Alternate DNS : 156.154.71.25



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.







## 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.**

525 Washington Blvd.

Jersey City, NJ 07310

United States

Tel : +1.888.266.6361

Email: [Sales@comodo.com](mailto:Sales@comodo.com)

### **Comodo CA Limited**

3rd floor, Office Village Exchange Quay

Trafford Road, Salford, Manchester M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767