COMODO
Creating Trust Online®

Comodo
Antivirus for Servers

Software Version 8.1

User Guide

Guide Version 8.1.082919

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

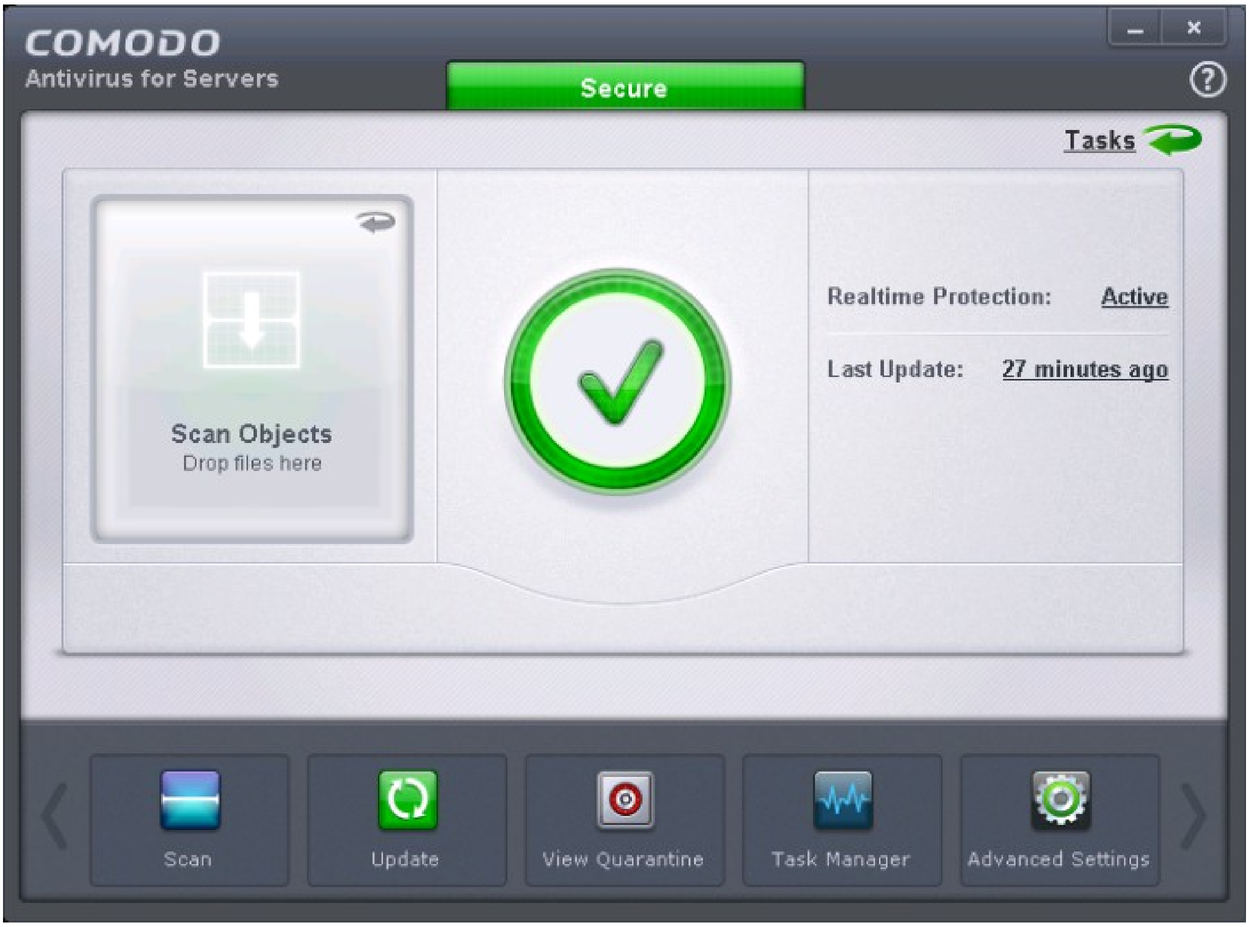
Table of Contents

1. Introduction to Comodo Antivirus for Servers

Overview

Comodo Antivirus for Servers offers 360° protection against internal and external threats by combining a powerful antivirus and an advanced host intrusion prevention system called Defense+.

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



Realtime Protection: Active

Last Update: 27 minutes ago

Comodo Antivirus for Servers - Special Features:

- **Antivirus -** Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the powerful on-demand, on-access and scheduled scan capabilities, CAVS users can now simply drag-and-drop items onto the home screen to run an instant virus scan.
- **Defense+ -** A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
    - **Sandbox -** Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be auto-sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

    - **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your server. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **Virtual Desktop -**The Virtual Desktop is a sandboxed operating environment inside of which you can run programs and browse the Internet without fear that those activities will damage your real computer. Featuring a virtual keyboard to thwart key-loggers, home users will find the virtual desktop is ideally suited to sensitive tasks like online banking. Advanced users will appreciate the ability to run beta-software in an environment that will not upset the stability or file structure of their production systems.
- **Rescue Disk** - Built-in wizard that allows you to burn a boot-disk which will run antivirus scans in a pre-Windows / pre-boot environment.
- **Additional Utilities -** The advanced tasks section contains links that allow you to install other, free, Comodo security products - including Comodo Cleaning Essentials and KillSwitch.

Guide Structure

This introduction is intended to provide an overview of the basics of Comodo Antivirus for Servers and should be of interest to all users.

The next three sections of the guide cover every aspect of the configuration of Comodo Antivirus for Servers.

The Appendix 1 contains quick guidance for commonly performed tasks.

- **Appendix 2 - Glossary of Common Terms**

1.1. Key Features

Host Intrusion Prevention System

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

Comprehensive Antivirus Protection

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

Intuitive Graphical User Interface

- Advanced and Compact View summary screens gives an at-a-glance snapshot of your security settings;
- Easy and quick navigation between each module of the 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.

1.2. Supported Servers

Comodo Antivirus for Servers supports the following MS Server operating systems:

1. Windows Server 2003
2. Windows Small Business Server 2003
3. Windows Server 2008

4. Windows Small Business Server 2008
5. Windows Server 2008 R2
6. Windows Small Business Server 2011
7. Windows Server 2012

1.3. Installation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus products that are on your server. More specifically, remove any other products of the same type as those Comodo products you plan to install. For example, if you plan to install only the antivirus then you do not need to remove 3rd party firewall solutions and vice-versa. Failure to remove products of the same type could cause conflicts that mean CAVS will not function correctly.

The CAVS application can be installed on your server in two ways, through:

- **the command line**
- **the installation wizard as a standalone guide**

To install CAVS via the command line interface

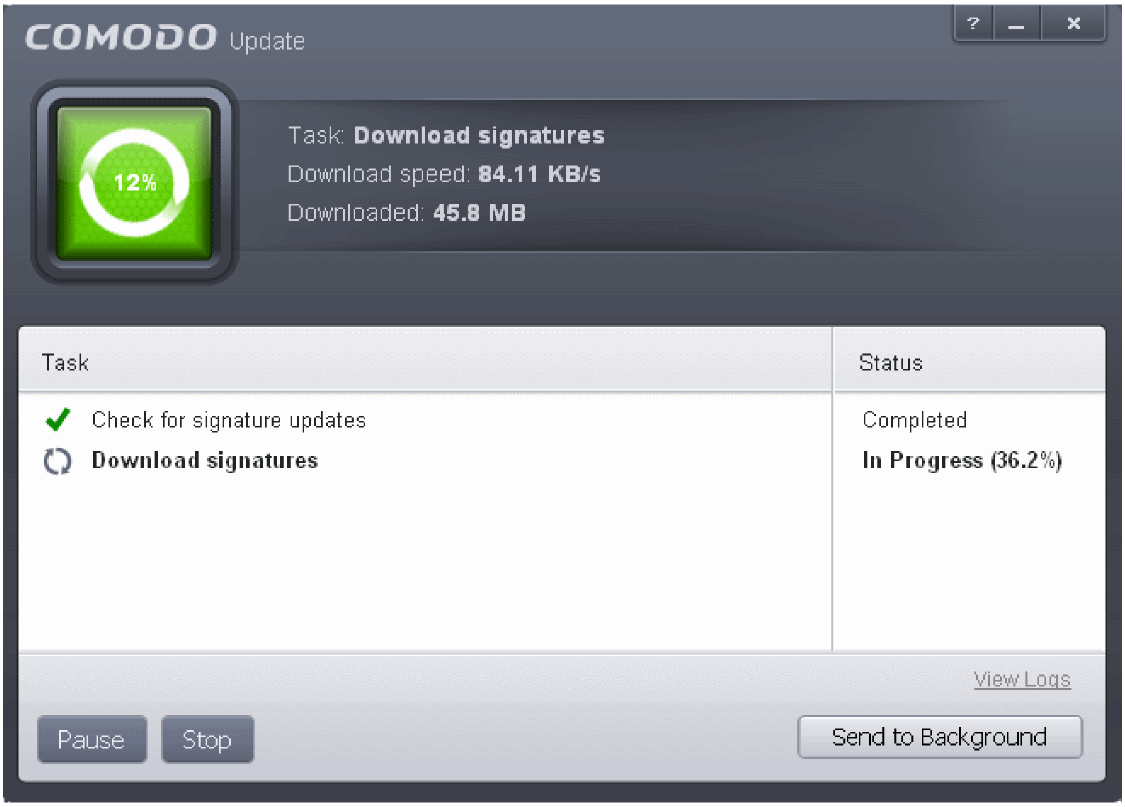
After the installation is complete, the server will restart automatically. So please make sure that the installation does not interrupt other server activities. The command line for installing CAVS is given below:

<Path of the setup file>\<name of the setup file> AV_FOR_SERVERS=1 INSTALLFIREWALL=0 -quiet

For example:

C:\CIS\CIS_Setup_R60AUG_6.3.291358.2908_x86.msi AV_FOR_SERVERS=1 INSTALLFIREWALL=0 -quiet

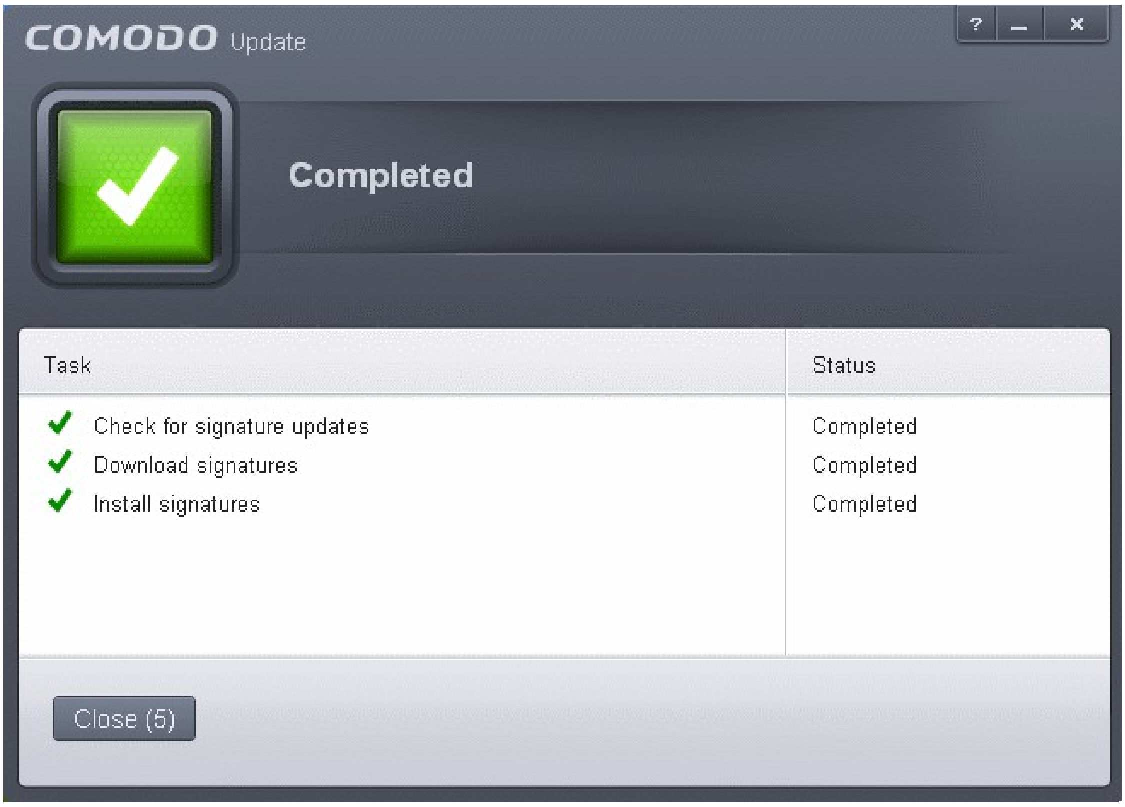
The virus database will be updated automatically for the first time after installation.



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

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

The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section '**Manage CAVS Tasks**' for more details. When the virus database has been downloaded, the 'Completed' dialog will be displayed.

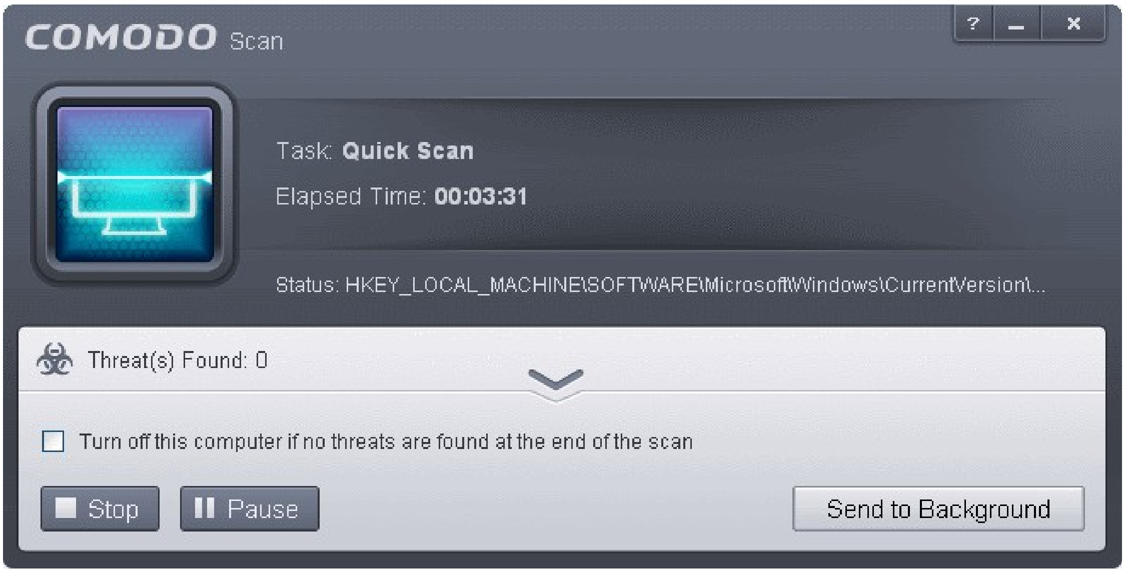


COMODO Update

Completed

Task	Status
✓ Check for signature updates	Completed
✓ Download signatures	Completed
✓ Install signatures	Completed

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



COMODO Scan

Task: **Quick Scan**

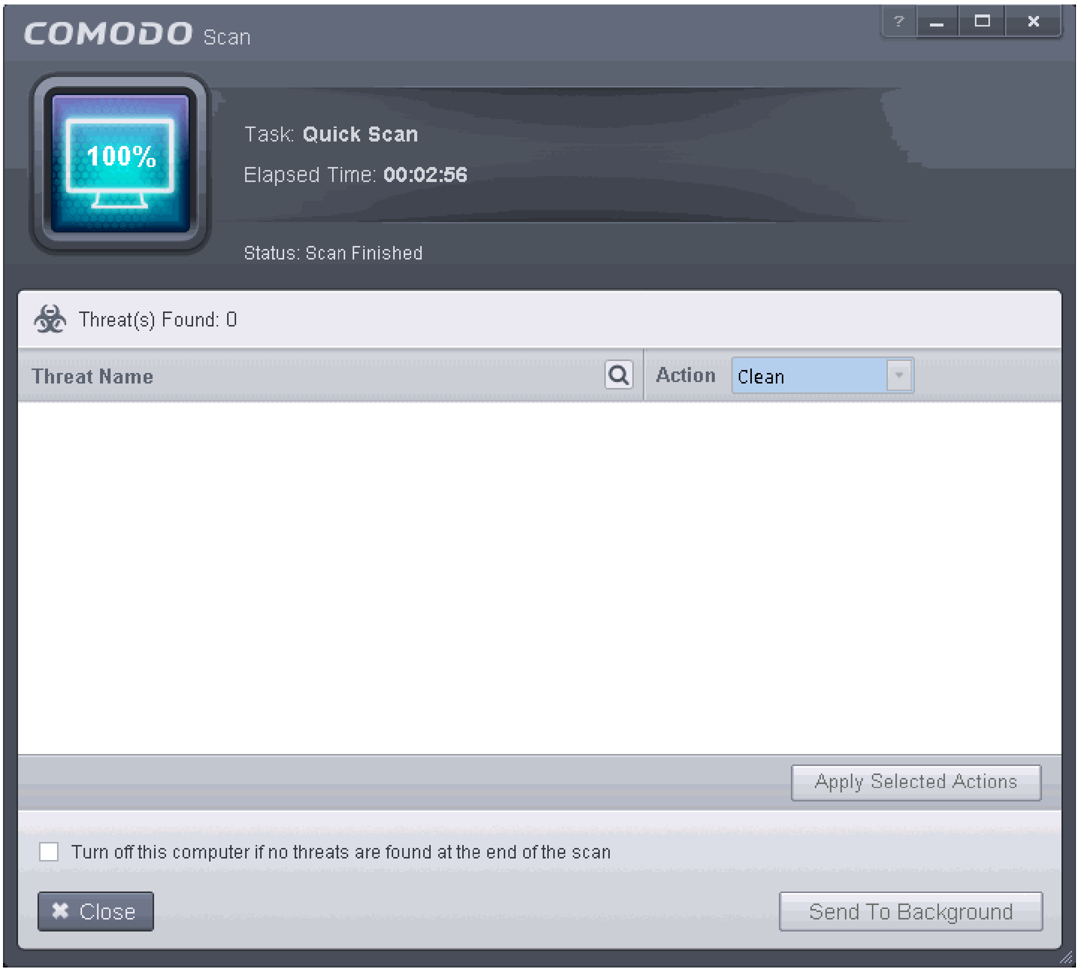
Elapsed Time: **00:03:31**

Status: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\...

Threat(s) Found: 0

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

If you do not want the scan to continue at this time, click the ‘Stop’ button. After the scanning is complete, the results screen will be displayed.



Task: **Quick Scan**

Elapsed Time: **00:02:56**

Status: Scan Finished

Threat(s) Found: 0

Threat Name	Action: Clean

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

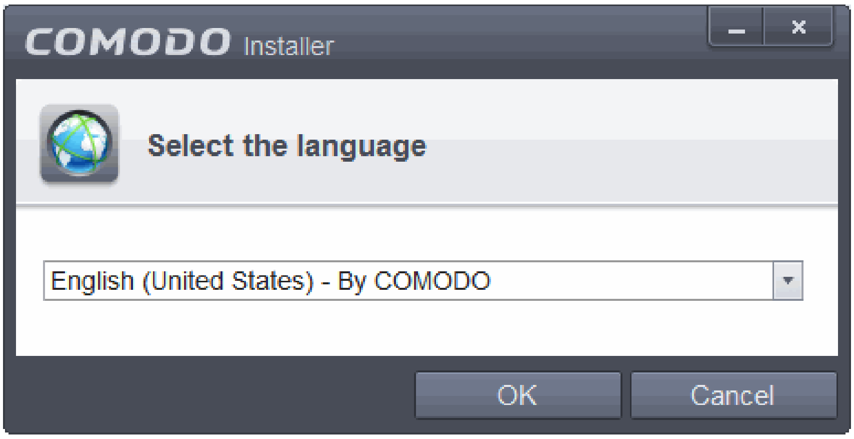
The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to the section '**Processing Infected Files**' for more details.

To install CAVS using installation wizard

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

Step 1 - Choosing the Interface Language

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



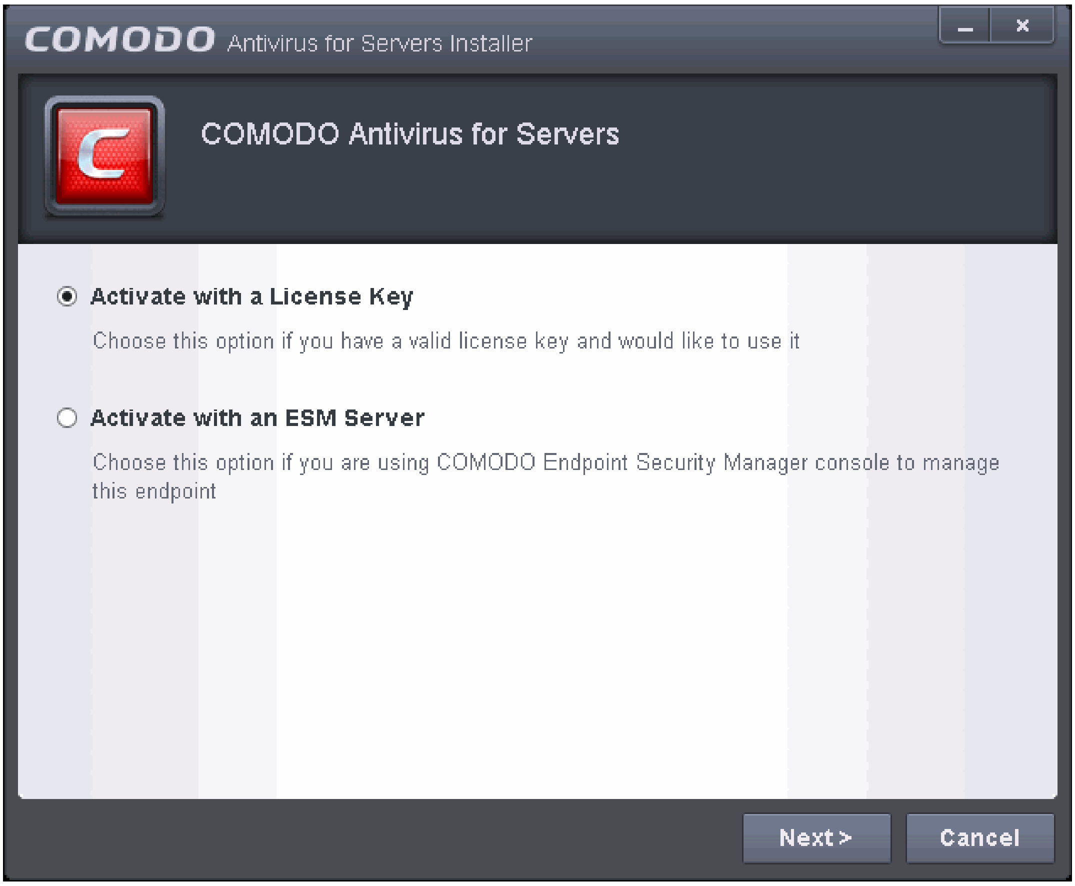
Select the language

English (United States) - By COMODO

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

Step 2 – CAVS Activation

You have the option to activate CAVS using the **license keys** or via the **ESM server** that you want to connect the endpoint to.


COMODO Antivirus for Servers Installer
COMODO Antivirus for Servers
Next >
Cancel

● Activate with a License Key

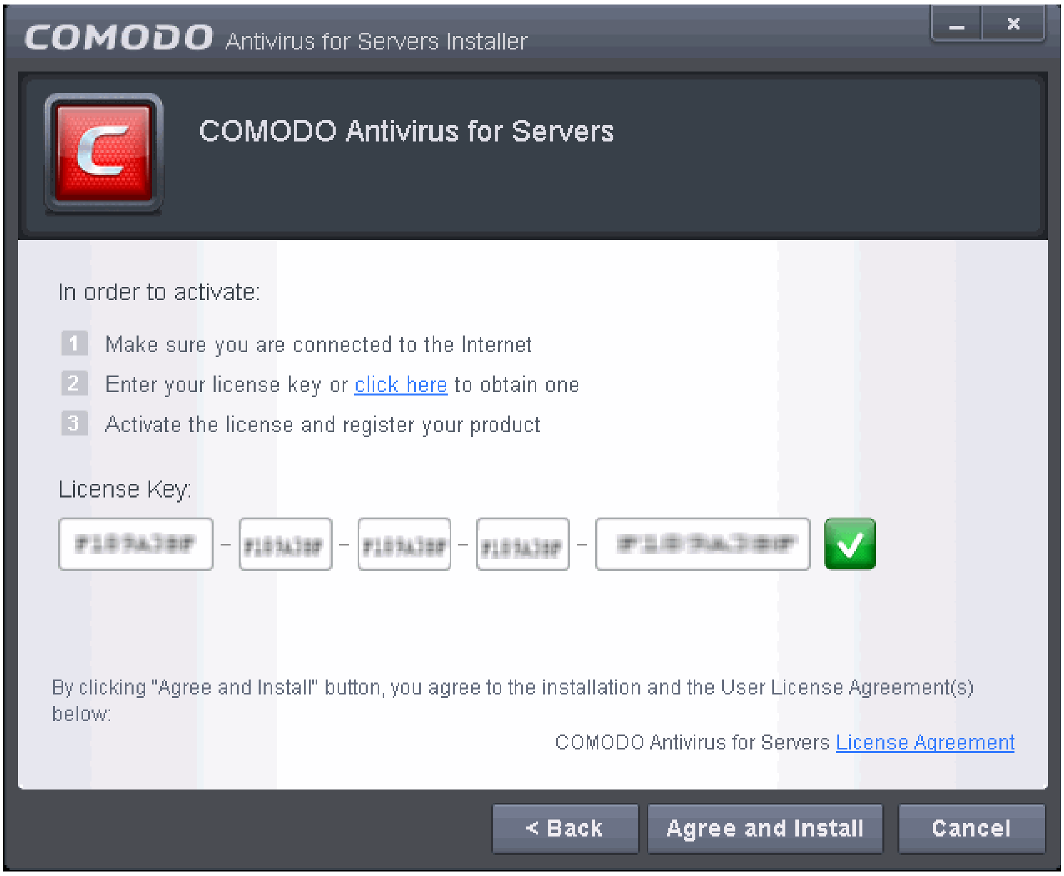
Choose this option if you have a valid license key and would like to use it

○ Activate with an ESM Server

Choose this option if you are using COMODO Endpoint Security Manager console to manage this endpoint

Option 1 – Using the license key:

- Choose Activate with a License Key and click 'Next'



COMODO Antivirus for Servers Installer

COMODO Antivirus for Servers

In order to activate:

1 Make sure you are connected to the Internet

2 Enter your license key or click here to obtain one

3 Activate the license and register your product

License Key:

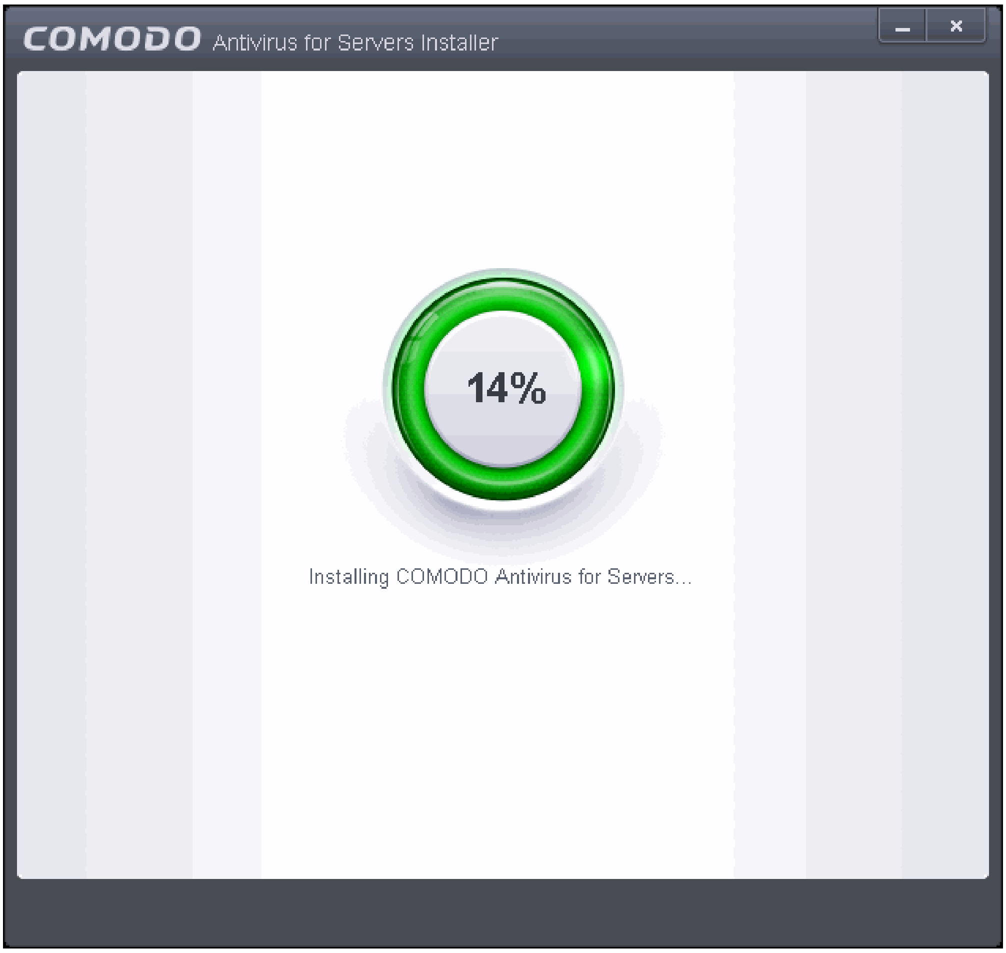
By clicking "Agree and Install" button, you agree to the installation and the User License Agreement(s) below:

COMODO Antivirus for Servers License Agreement

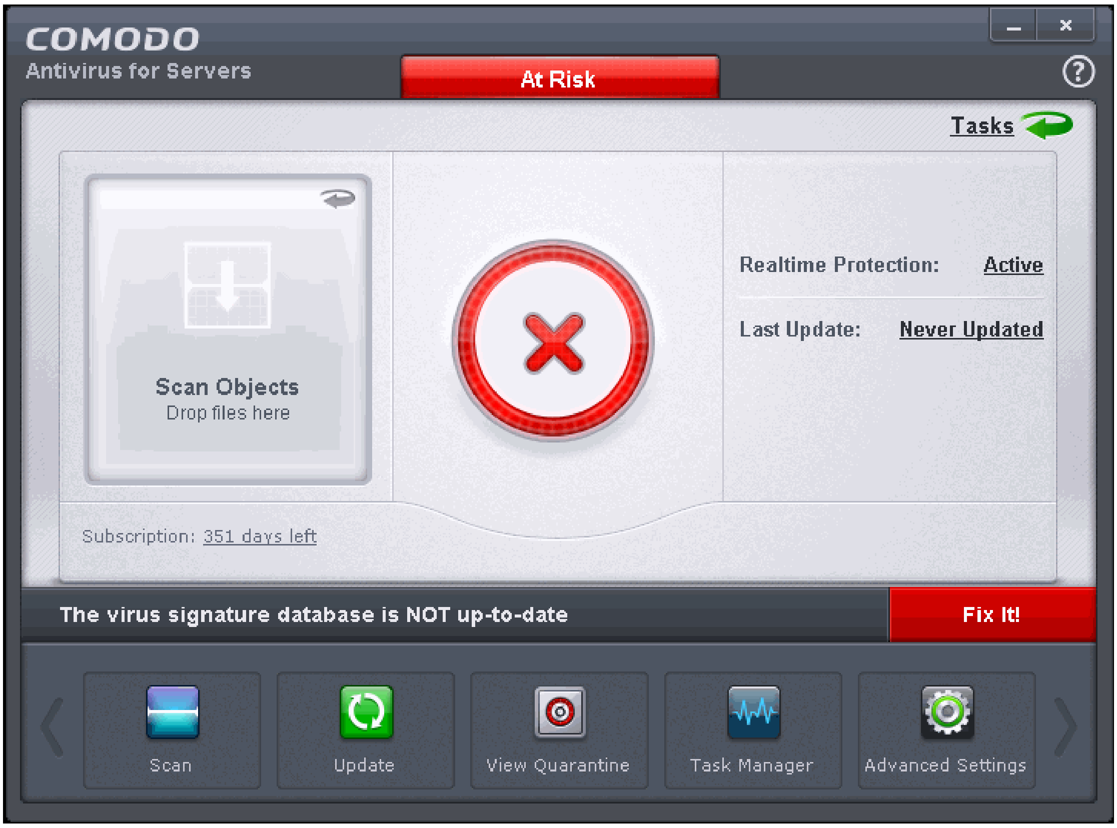
- Click the 'License Agreement' link, read the 'License Agreement' fully and click 'Back'.
- Click 'Agree and Install'

Step 3 – CAVS Installation

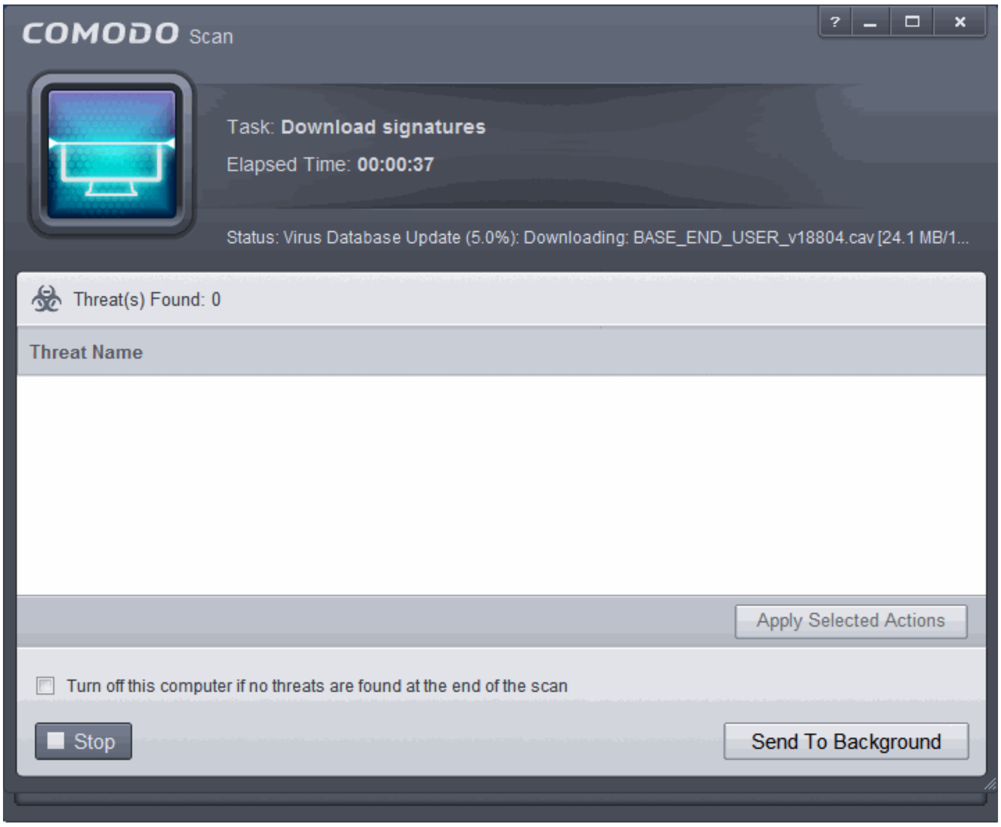
The installation progress will be displayed...


COMODO Antivirus for Servers Installer
14%
Installing COMODO Antivirus for Servers...

...and after completion, the application will start automatically.



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



Task: **Download signatures**

Elapsed Time: **00:00:37**

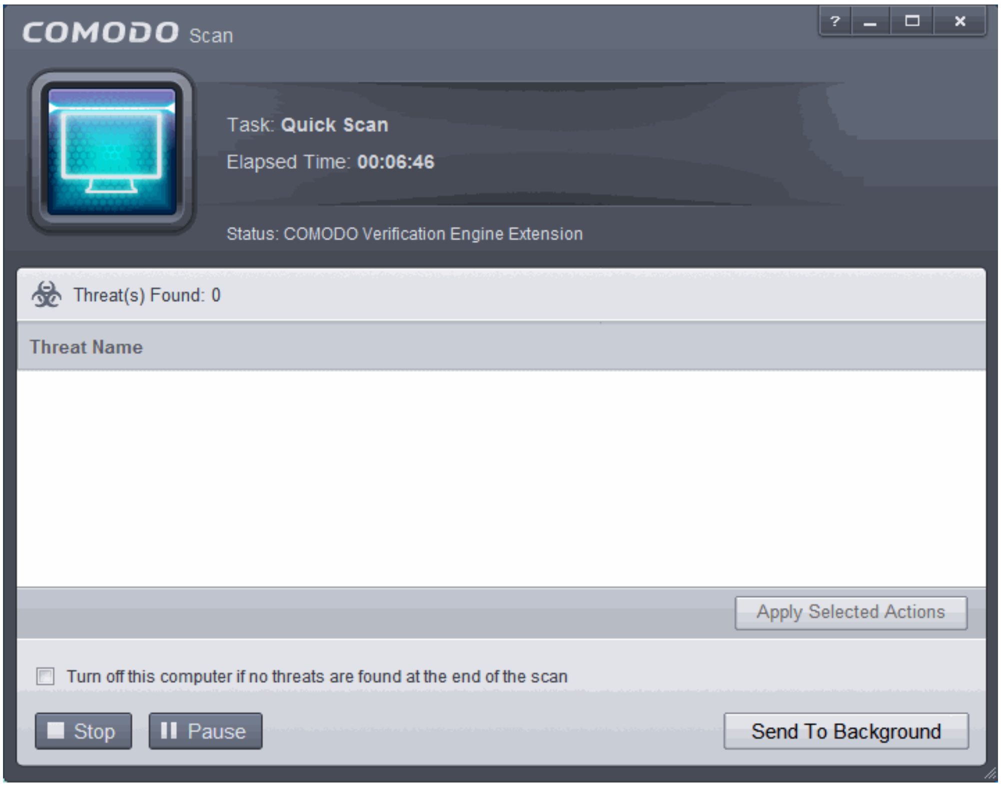
Status: Virus Database Update (5.0%): Downloading: BASE_END_USER_v18804.cav [24.1 MB/1...

Threat(s) Found: 0

Threat Name

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

The screen will display details such as download speed, how much has been downloaded and the progress of the process. You can also send this task to the background by pressing the 'Send to Background' button and retrieve it in the 'Task Manager' interface. Refer to the section **'Manage CAVS Tasks'** for more details. When the virus database has been downloaded, the 'Completed' dialog will be displayed.



Task: **Quick Scan**

Elapsed Time: **00:06:46**

Status: COMODO Verification Engine Extension

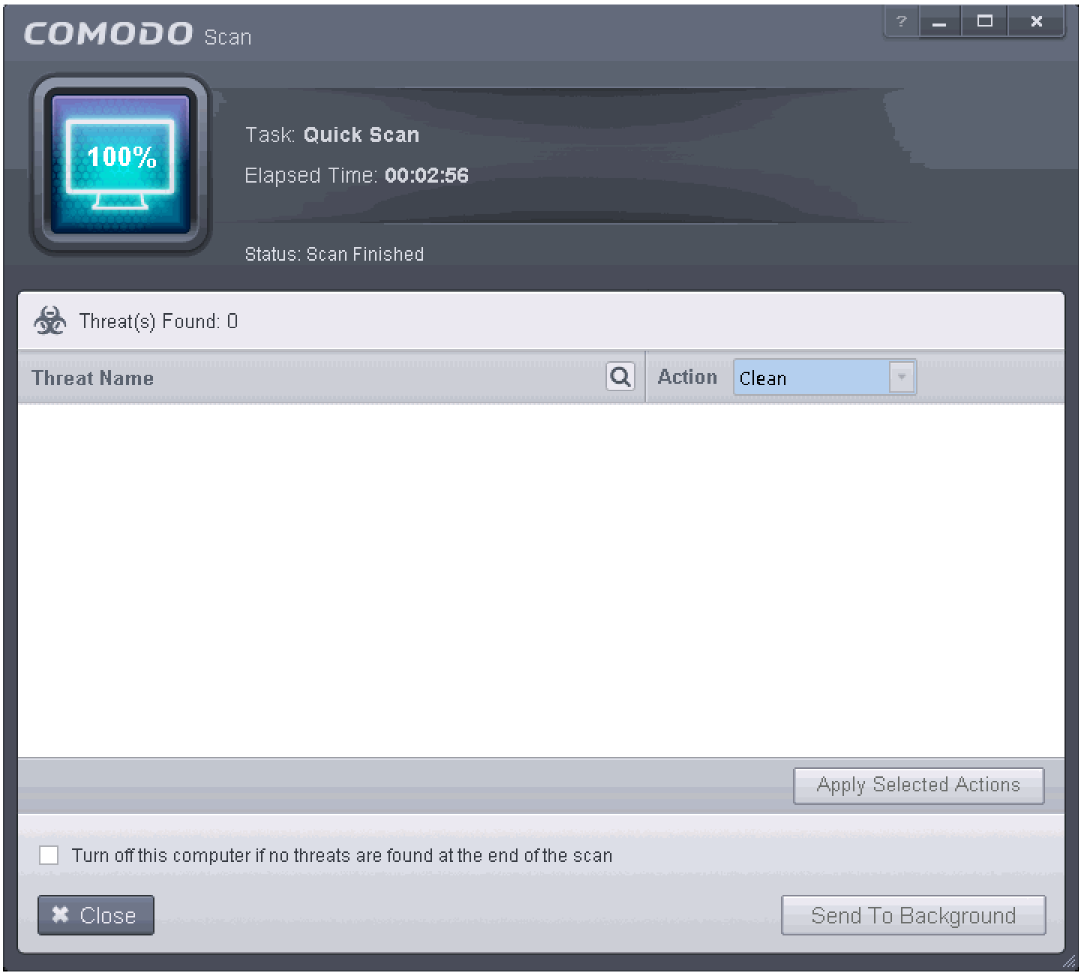
Threat(s) Found: 0

Threat Name

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

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

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



Task: Quick Scan

Elapsed Time: 00:02:56

Status: Scan Finished

Threat(s) Found: 0

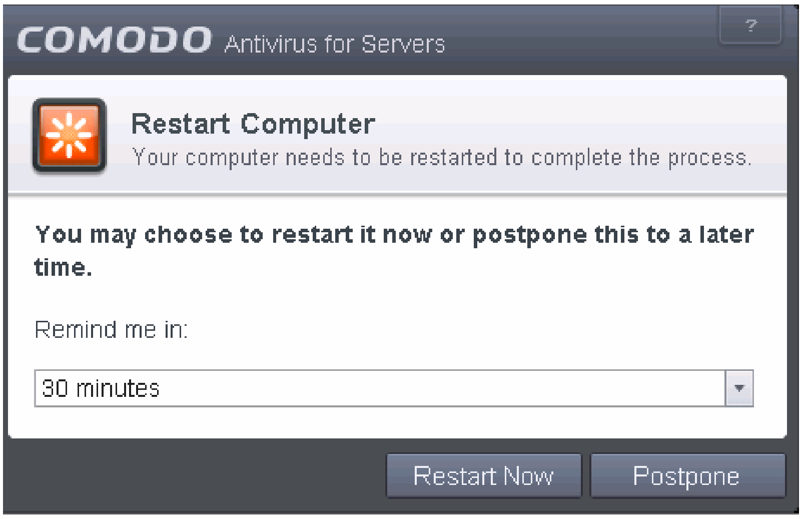
Action: Clean

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

The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to the section '**Processing Infected Files**' for more details.

Step 4 - Restarting Your System

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



Restart Computer

Your computer needs to be restarted to complete the process.

You may choose to restart it now or postpone this to a later time.

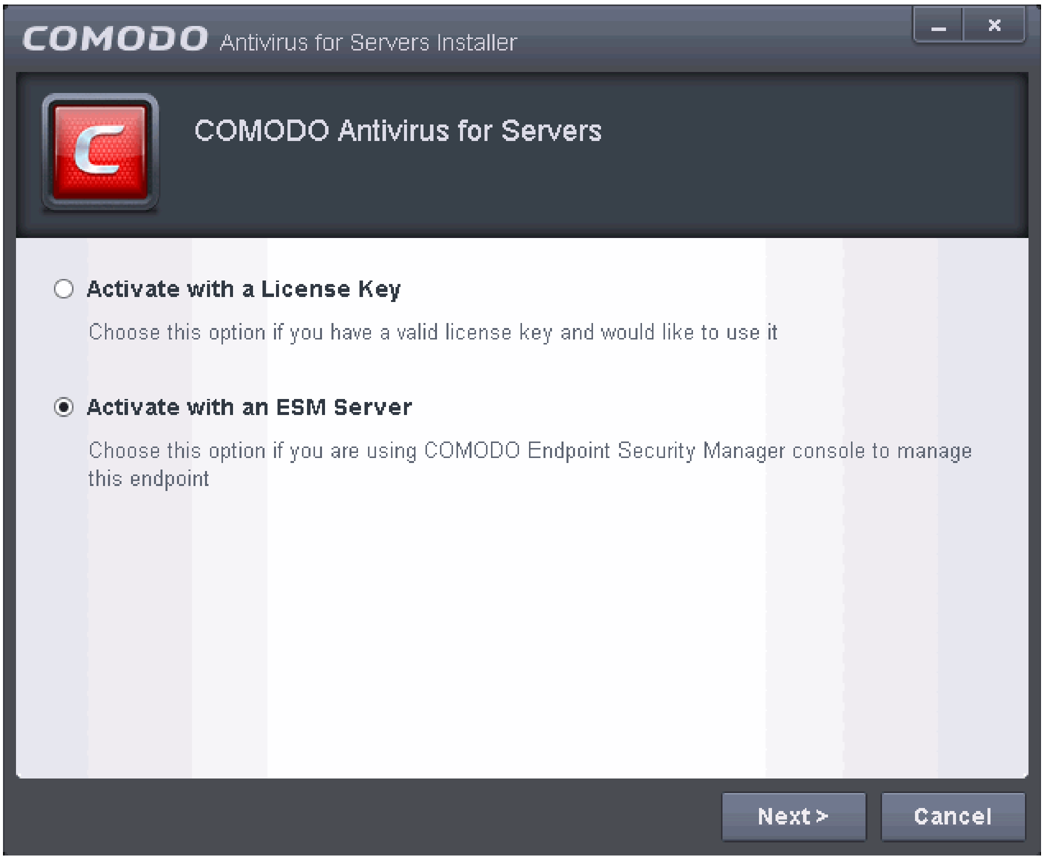
Remind me in:

30 minutes

Please save any unsaved data and click 'Restart Now' to restart the system. If you want to restart the system at a later time, click 'Postpone'. You will be reminded to restart the system as selected from the 'Remind me in:' option.

Option 2 – Activating via CESM

- Choose 'Activate with an ESM Server' and click 'Next'



COMODO Antivirus for Servers Installer

COMODO Antivirus for Servers

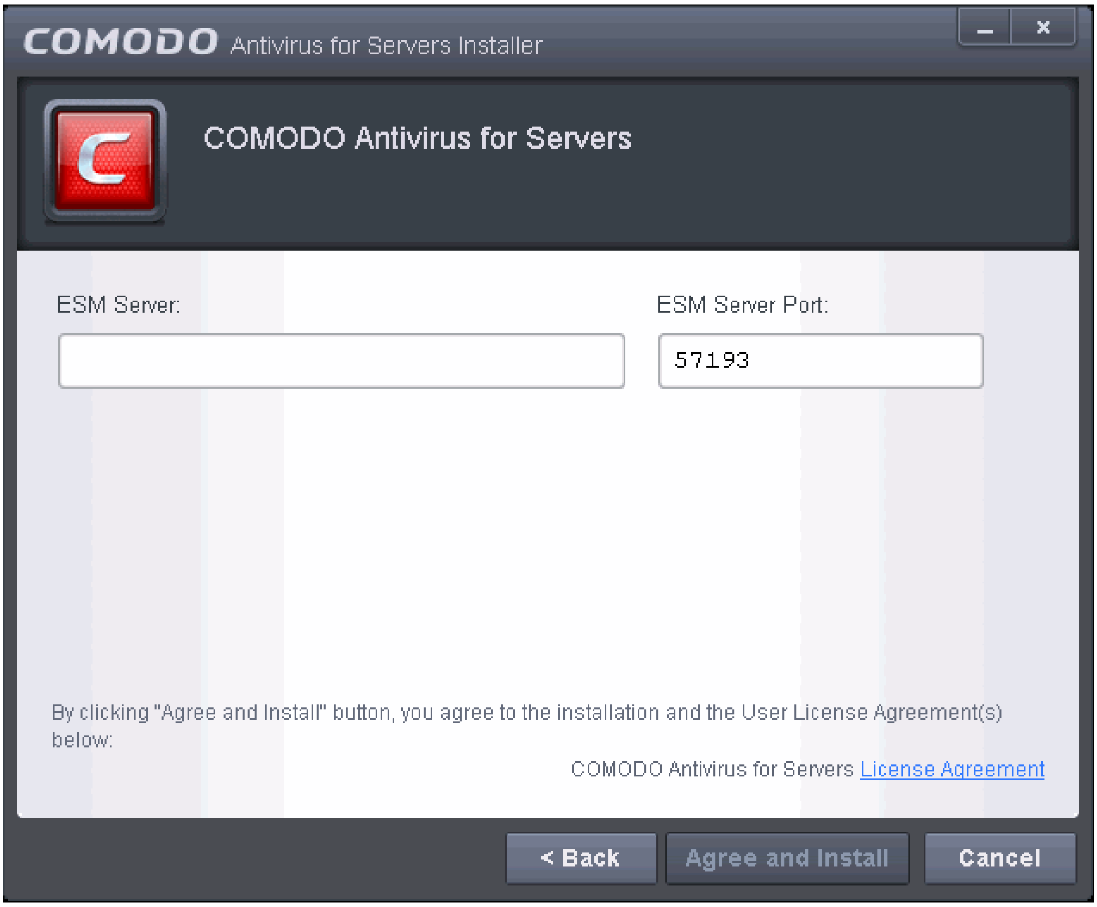
○ **Activate with a License Key**

Choose this option if you have a valid license key and would like to use it

● **Activate with an ESM Server**

Choose this option if you are using COMODO Endpoint Security Manager console to manage this endpoint

The ESM server details that you want to connect the endpoint and the components that you want to activate screen will be displayed.



COMODO Antivirus for Servers Installer
COMODO Antivirus for Servers

ESM Server:

ESM Server Port: 57193

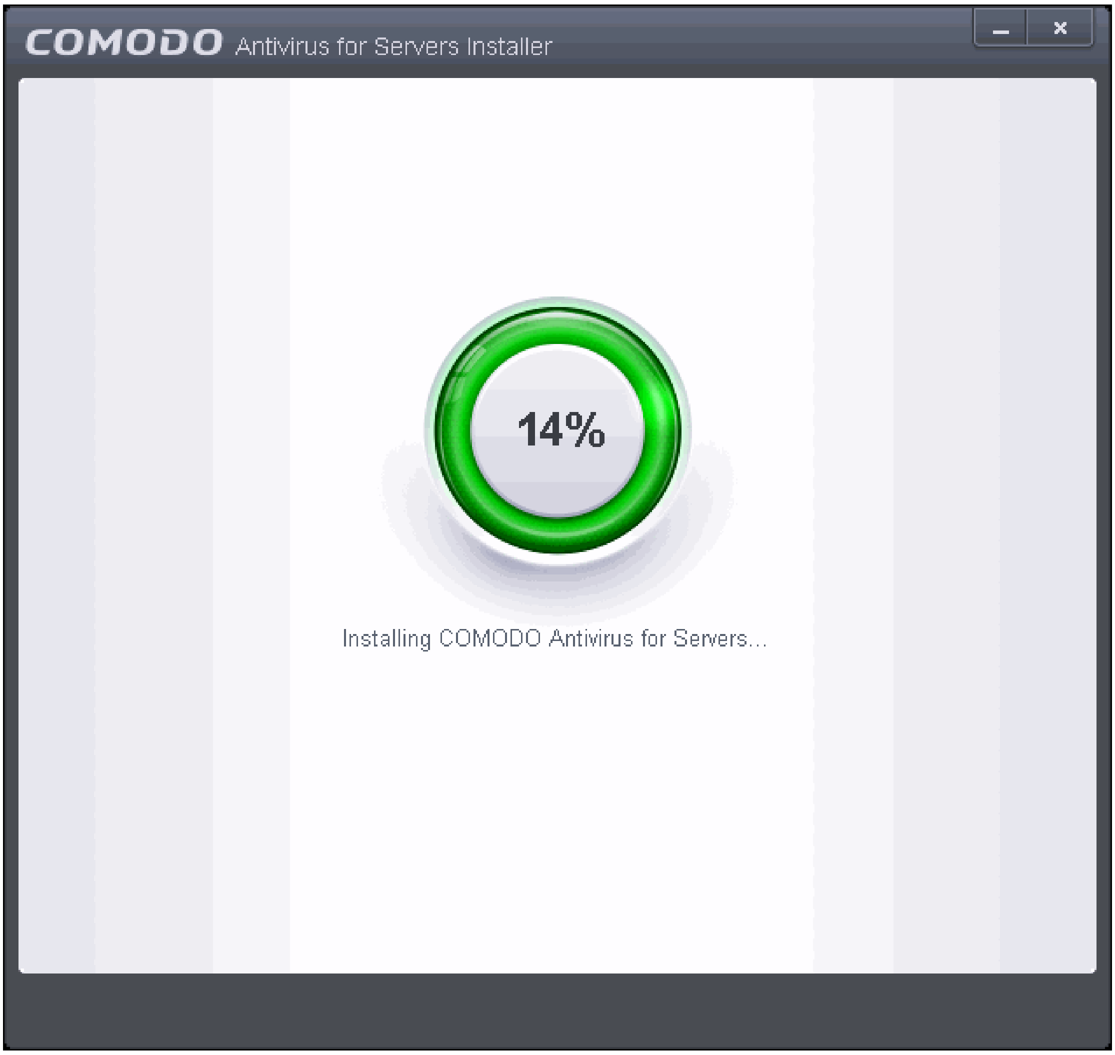
By clicking "Agree and Install" button, you agree to the installation and the User License Agreement(s) below:

COMODO Antivirus for Servers License Agreement

< Back
Agree and Install
Cancel

- Click the 'License Agreement' link, read the Subscriber Agreement fully and click 'Back'.
- Enter the host name or IP Address of the CESM server in the ESM server text box and enter the port through which the server listens for endpoint connections in the ESM server Port text box. (Default = 57193)
- Click 'Agree and Install'

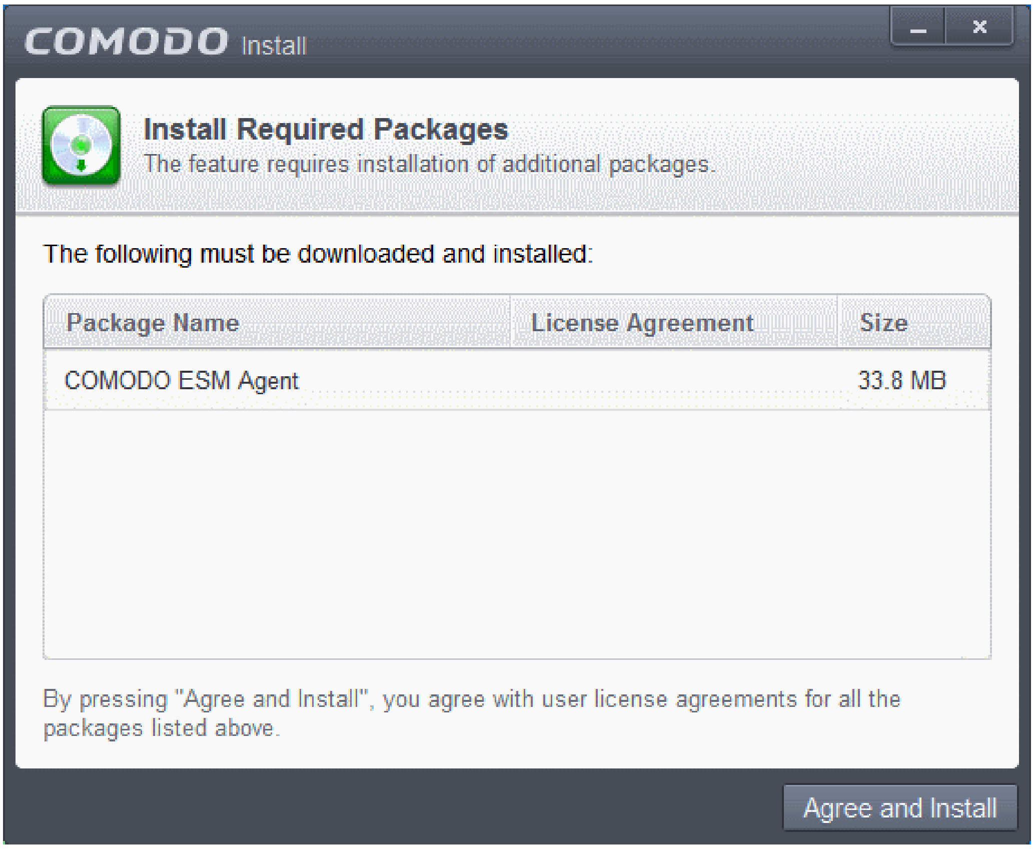
The installation progress will be displayed...



Installing COMODO Antivirus for Servers...

… and after successful completion, the CESM agent installation screen will be displayed.

Background Note on CESM Agent: The CESM agent is a small application installed on every managed endpoint to facilitate communication between the endpoint and the CESM central server. The agent is responsible for receiving tasks and passing them to the endpoint's installation of Comodo Security Software (CES, CAS OR CAV for Mac). Example tasks include changes in security policy, an on-demand virus scan, updates to the local antivirus database or gathering reports that have been requested by the central service. As an additional security feature, endpoint agents can only communicate with the specific instance of the central service which provisioned the agent. This means the agent cannot be reconfigured to connect to any other CESM service. The agent also acts as a tool for endpoint users to interact with the administrators for resolving any issues in their systems.



Install Required Packages

The feature requires installation of additional packages.

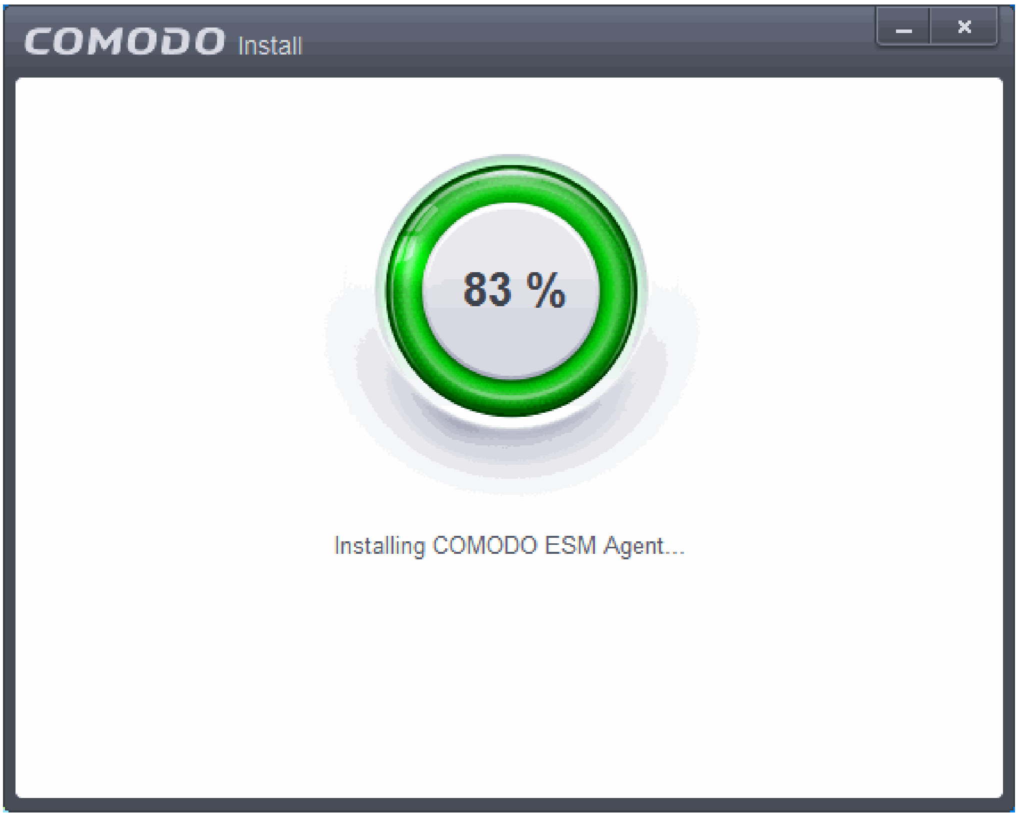
The following must be downloaded and installed:

Package Name	License Agreement	Size
COMODO ESM Agent		33.8 MB

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

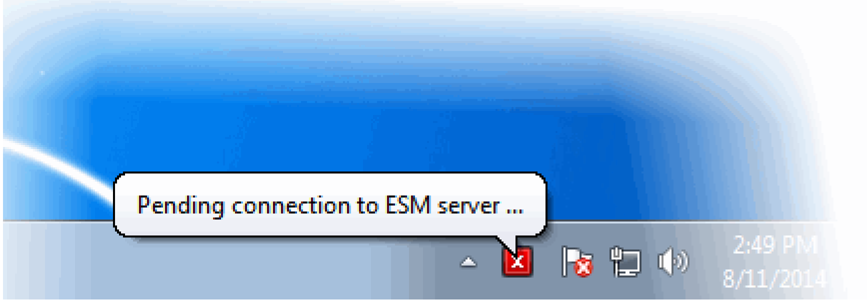
- Click 'Agree and Install'.

The downloading and installing progress will be displayed.



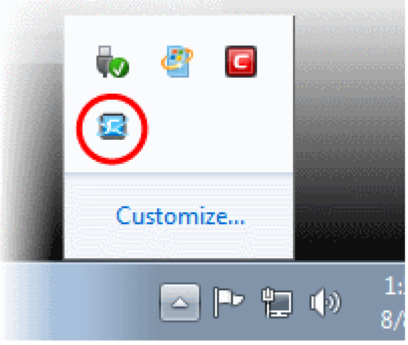
Installing COMODO ESM Agent...

After the agent installation, it will initiate communication with the CESM server from which it was downloaded.



Pending connection to ESM server ...

On completion, the agent icon will be displayed in the system tray....



… and the license will be activated from the CESM server. Your CAVS installation can be remotely managed by the CESM Server now.

- Clicking the CESM Agent system tray icon will open a support chat window that enables you to interact with your administrators for resolving any issues in your system. Refer to the section **Instance User Assistance** for more details.

> **Note:** CAVS 8.0+ features additional functionality that are not supported by Comodo Endpoint Security Manager version 3.1 and lower versions. Please make sure to activate the CAVS 8.0 license from CESM 3.2 and higher versions for full compatibility. The CAVS 8.0 features that are not supported by CESM 3.1 and lower versions are:
>
> - **Sandbox Rules**

1.4. Starting Comodo Antivirus for Servers

After installation, Comodo Antivirus for Servers automatically starts whenever you start server and the CAVS Widget will be displayed. In order to configure and view settings within CAVS, you need to access the main interface.

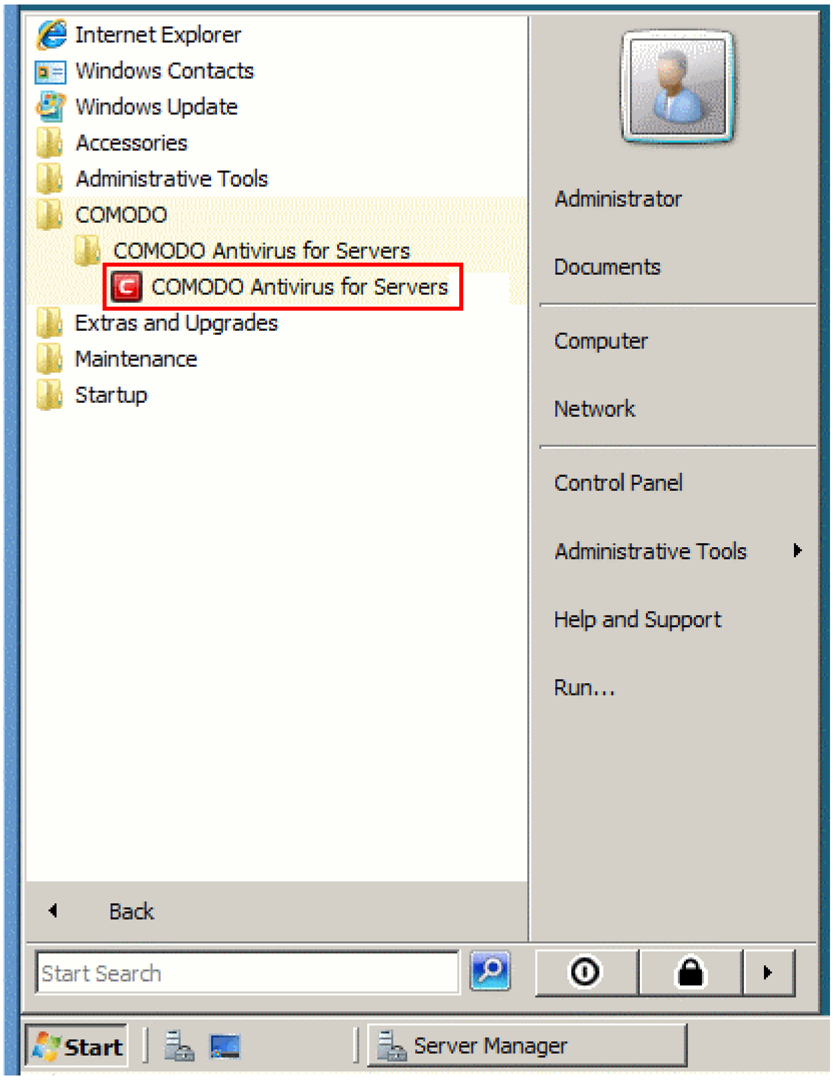
There are 4 different ways to access the main interface of CAVS:

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

Start Menu

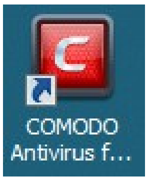
You can access Comodo Antivirus for Servers via the Start Menu.

- Click **Start** and select **All Programs** > **Comodo** > **COMODO Antivirus for Servers** > **COMODO Antivirus for Servers**



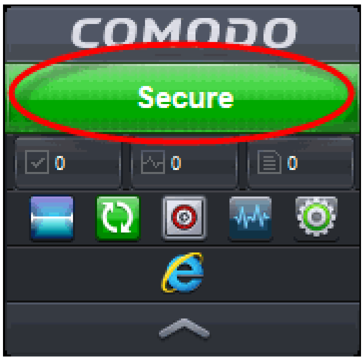
Desktop

- Just double click the shield icon in the desktop to start CAVS.



Widget

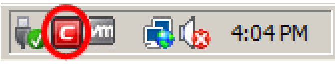
- Just click the information bar in the widget to start CAVS.



You can also view other details in the widget such as number of tasks running and shortcuts to common CAVS tasks. Refer to the section '**The Widget**' for more details.

CAVS Tray Icon

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

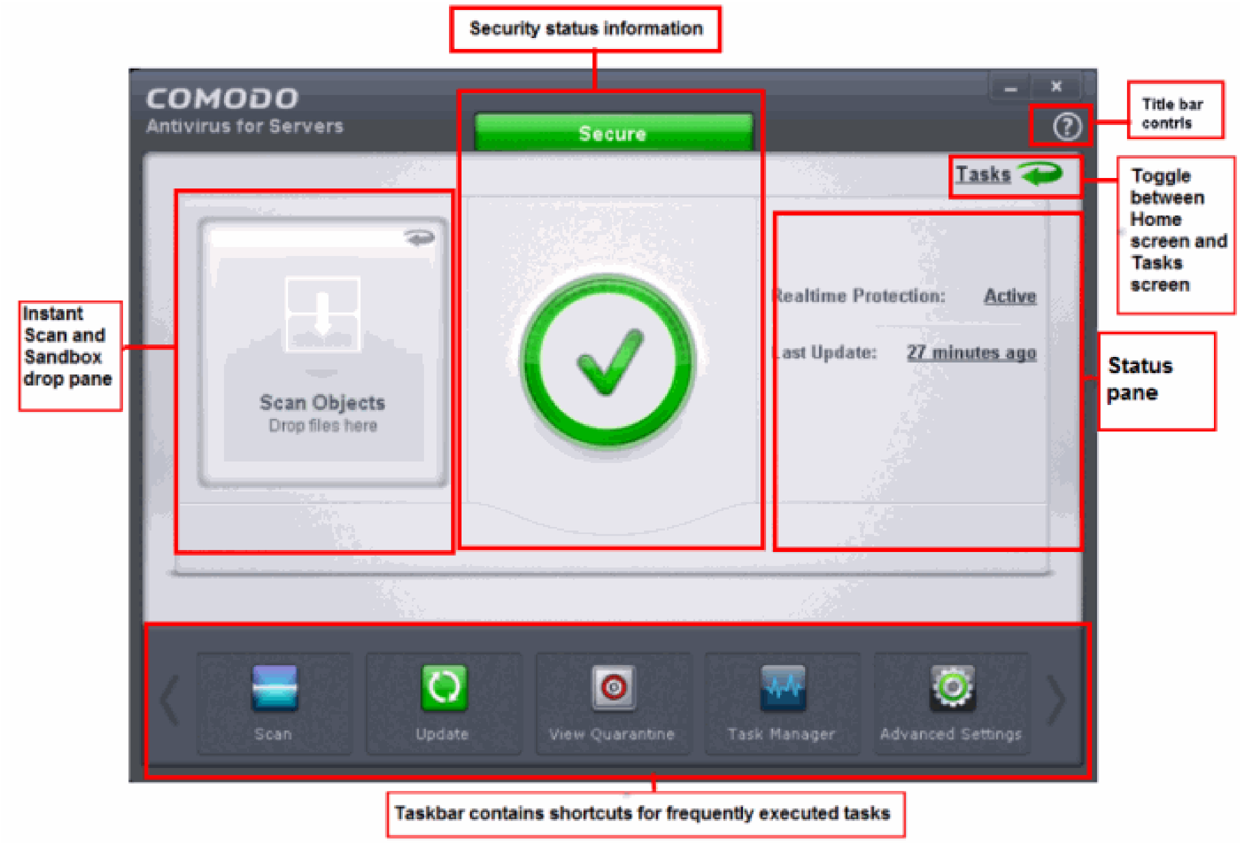


By right-clicking on the tray icon, you can access short cut to Widget settings, open and exit CAVS interface.

1.5. The Main Interface

The CAVS interface has been designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Clicking the curved arrowed on the upper right lets you switch between the **home screen** and the more advanced **tasks interface**. You can instantly run a virus scan on a file or folder by dragging it into the scan box. The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the update checker and the CAVS Task Manager.

The home screen has been designed in such a way that you can flip the view between Compact View and Advanced View by using the toggle button at the top left side of the interface. The Compact View, as the name suggests, is compact and allows you to run instant scans by dropping files or folders.


Security status information
Title bar contrls
Toggle between Home screen and Tasks screen
Status pane
Instant Scan and Sandbox drop pane
Taskbar contains shortcuts for frequently executed tasks
COMODO
Antivirus for Servers
Secure
Tasks
Scan Objects
Drop files here
Realtime Protection: Active
Last Update: 27 minutes ago
Scan
Update
View Quarantine
Task Manager
Advanced Settings

Click the following links for more information:

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

- **Instant Assistance**

1.5.1. The Home Screen

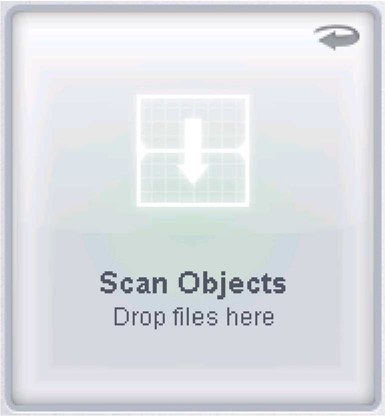
The main interface can be switched to display the 'Home' screen or the 'Tasks' interface. Click the curved green arrow at the upper right of the interface to switch between them:

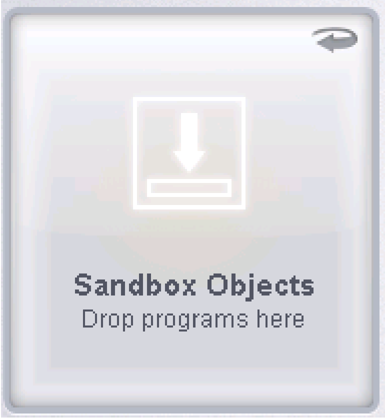
The home screen of CAVS allows you to carry out various tasks and also provides information about security components. In the middle-left of the home screen there is an instant virus scan box into which you can drag-and-drop files, folders or drives. If you flip this box, you can drag-and-drop programs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

- **Instantly scan objects**
- **Enable or disable security components**
- **Adding tasks to the Task Bar**
- **Title bar controls**

Instantly scan objects

The pane on the left side of the home screen allows you to run instant scans of files or folders.





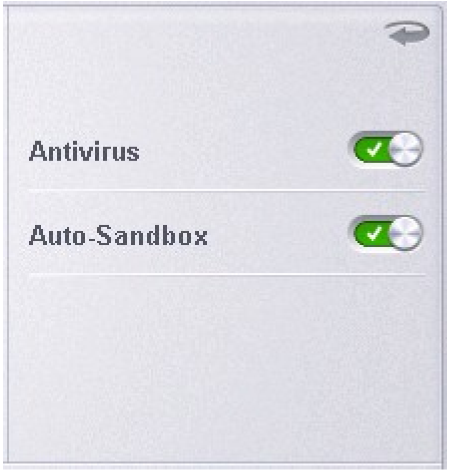
To run an instant scan, navigate to the file/folder that you want to scan and just drag and drop the file into the 'Scan Objects' box. The virus scan will commence immediately. Refer to '**Instantly Scan Individual Files and Folders**' for more details.

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

Now, navigate to the program that you want to run in sandboxed environment and just drag and drop it into the box. The program will start as usual but will be run in the CAVS sandbox. Refer to '**Run an Application in a Sandbox**' for more details.

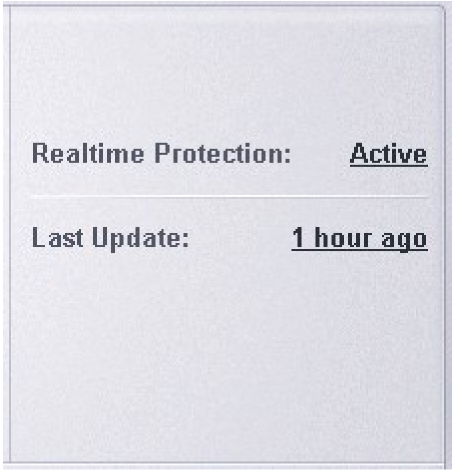
Enable or disable security components

The flippable pane on the right allows you to selectively enable or disable real-time antivirus and the Auto-Sandbox. The other side of the pane displays the status of real-time protection and when the virus database was updated.



Antivirus ✓

Auto-Sandbox ✓



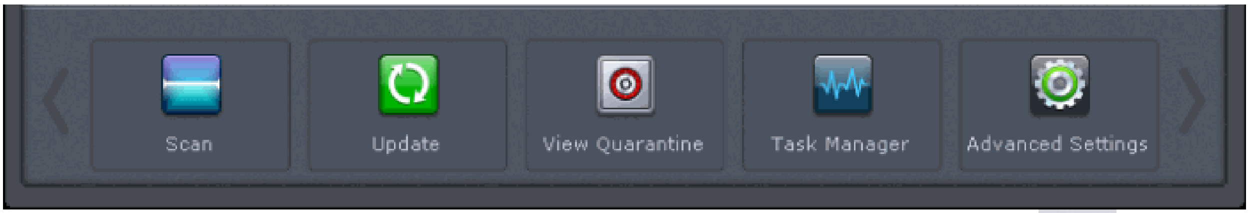
Realtime Protection: Active

Last Update: 1 hour ago

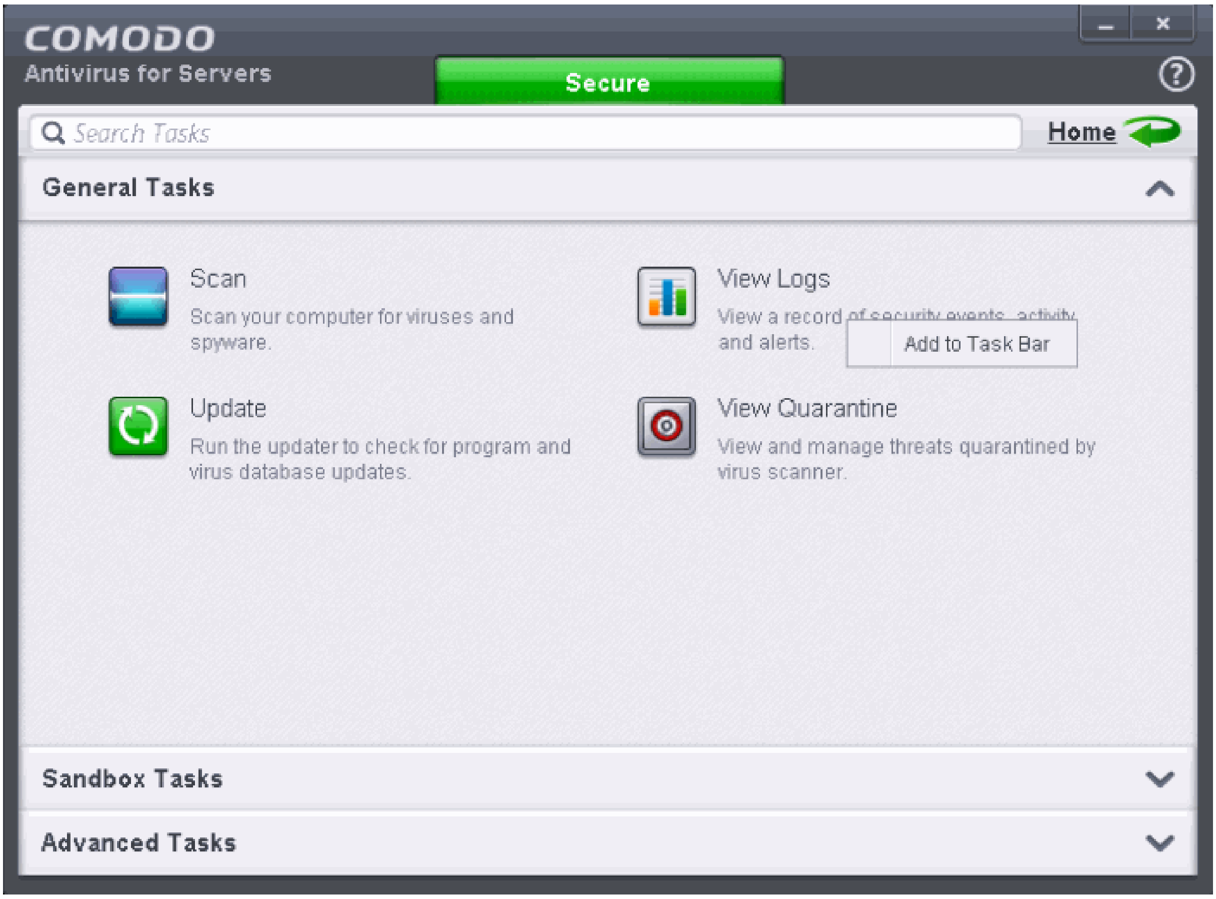
- **Antivirus** - Click the button at the right side of the bar to enable or disable real-time antivirus scanning. Refer to the section '**Real-time Scanner Settings**' for more details.
- Auto-Sandbox - Monitors the behavior of software and files in your system and prevents them from taking actions that would cause damage. Refer to the section '**Configuring Rules For Auto-Sandbox**' for more details.
- **Realtime Protection** - Displays the status of antivirus settings.
- **Last Update** - Displays the last updated time of the virus database. Click on the text link to update the virus database.

Adding tasks to the Task Bar

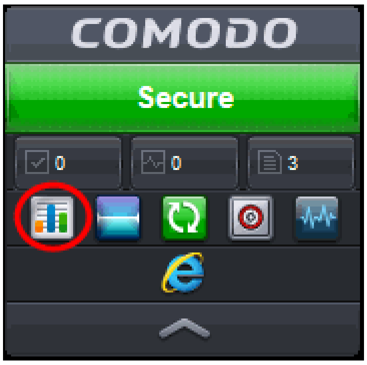
The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles to the left and right sides to scroll through all tasks.

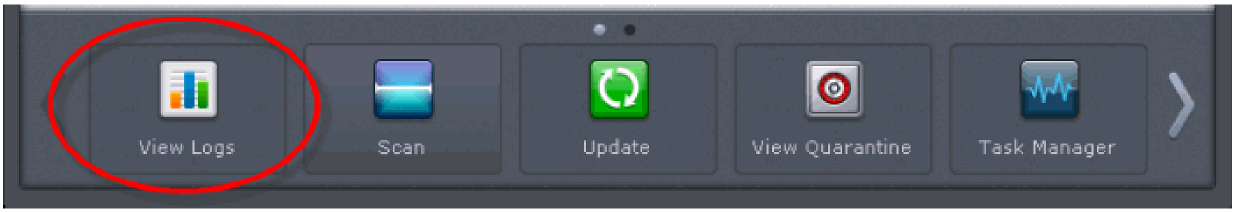


- To add a task to the Task Bar, first open the tasks interface by clicking the curved arrow:
- Expand any one of the General or Advanced Tasks menus.
- Right-click on the task you wish to add then click the message 'Add to Task Bar'.

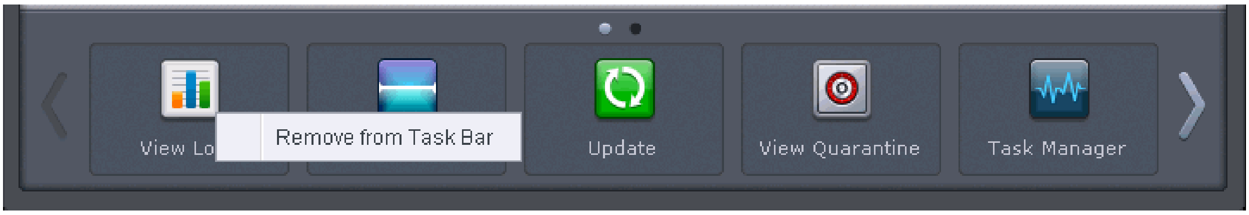

COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Add to Task Bar
Update
Run the updater to check for program and virus database updates.
View Quarantine
View and manage threats quarantined by virus scanner.
Sandbox Tasks
Advanced Tasks

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





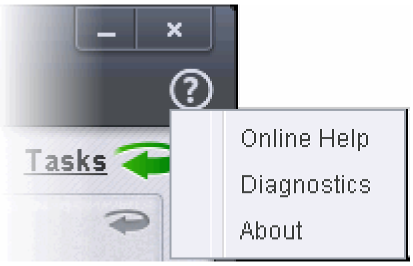
- To remove a task shortcut from the Task Bar, right click on it and choose 'Remove from task bar'.



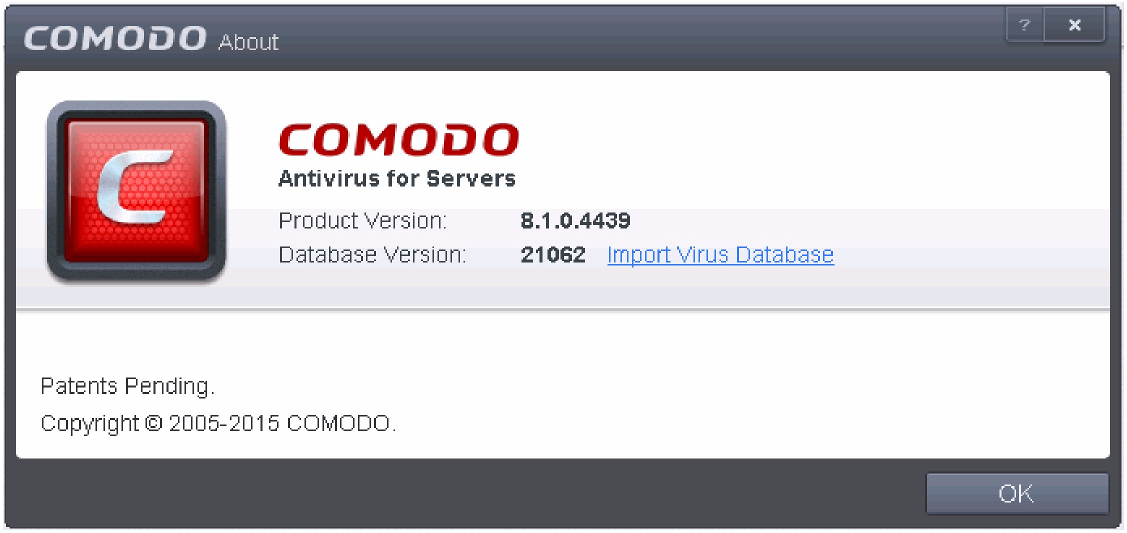
Tip - Many will find it useful to add 'Open Advanced Settings' to the task-bar as it contains several areas important to the configuration of CAVS. To do this, from the 'Home' screen, click the 'Tasks' arrow at upper-right, click 'Advanced Settings' then right-click on 'Open Advanced Settings' and select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

Title bar controls

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



- **Online Help** - Opens Comodo Internet Security's online help guide at **https://help.comodo.com/topic-213-1-517-5965-Introduction-to-Comodo-Antivirus-for-Servers.html**
- **Diagnostics** - Helps to identify any problems with your installation.
- **About** - Displays the product version, virus signature database version, website database version (website filtering URLs) and copyright information. The 'About' dialog also allows you to import a locally stored virus database into CAVS.



Product Version: 8.1.0.4439

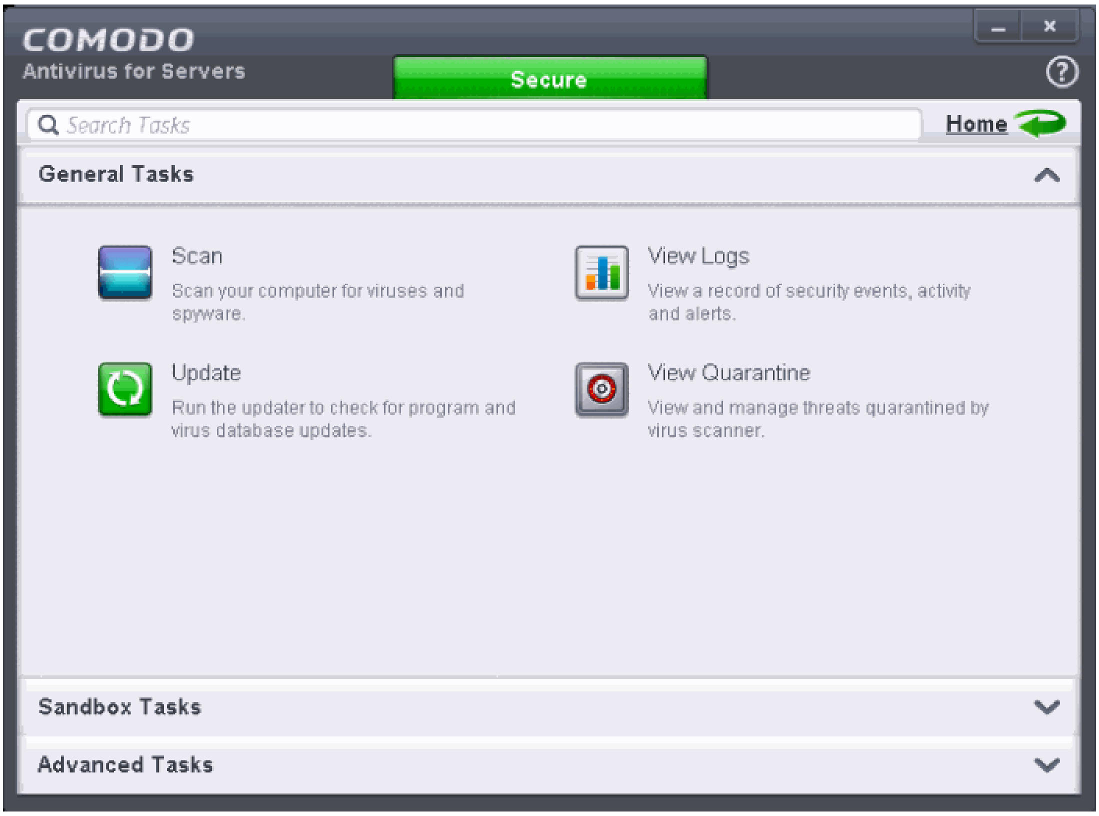
Database Version: 21062 Import Virus Database

Patents Pending.

Copyright © 2005-2015 COMODO.

1.5.2. The Tasks Interface

The links in the 'Tasks' interface allows you to configure every aspect of CAVS.


COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Quarantine
View and manage threats quarantined by virus scanner.
Sandbox Tasks
Advanced Tasks

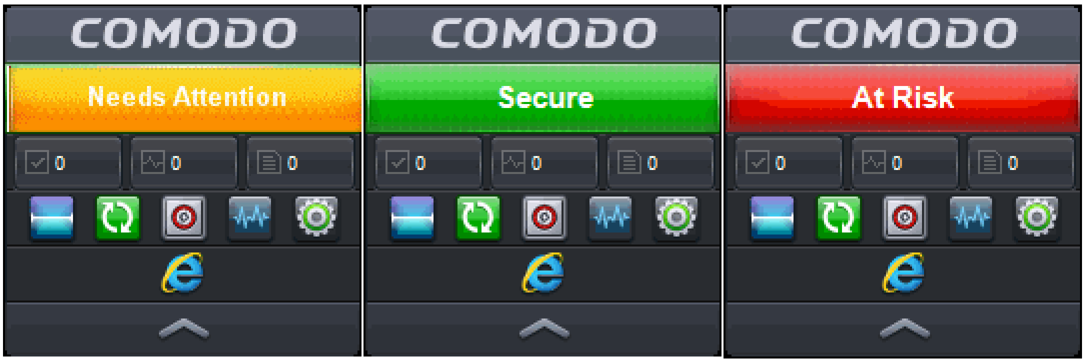
Tasks are broken down into two main sections. Click the following links for more details on each:

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

1.5.3. The Widget

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

Right clicking on the Widget opens a context sensitive menu similar to the one displayed on right clicking the CAVS system tray icon. The context sensitive menu allows you to enable or disable the widget or its components. Refer to section **The System Tray Icon** for more details.

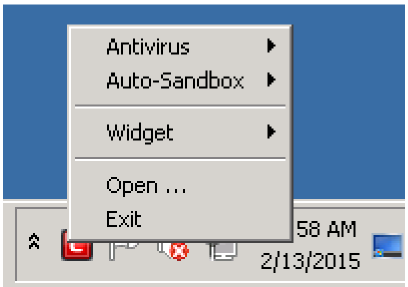


- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' opens the appropriate interface for you to take action immediately.
- The second row tells you current status of the CAVS application:
  - The first button displays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

  The status row is displayed only if 'Show Status Pane' is enabled under 'Widget options of CAVS tray icon or Widget right click menu. Refer to **The System Tray Icon** for more details. (***Default = Disabled***)
- The forth row contains shortcuts for five common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task. The Common Tasks row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of CAVS tray icon or Widget right click menu. Refer to **The System Tray Icon** for more details.
- You can expand or collapse the Widget by clicking the arrow at the bottom.

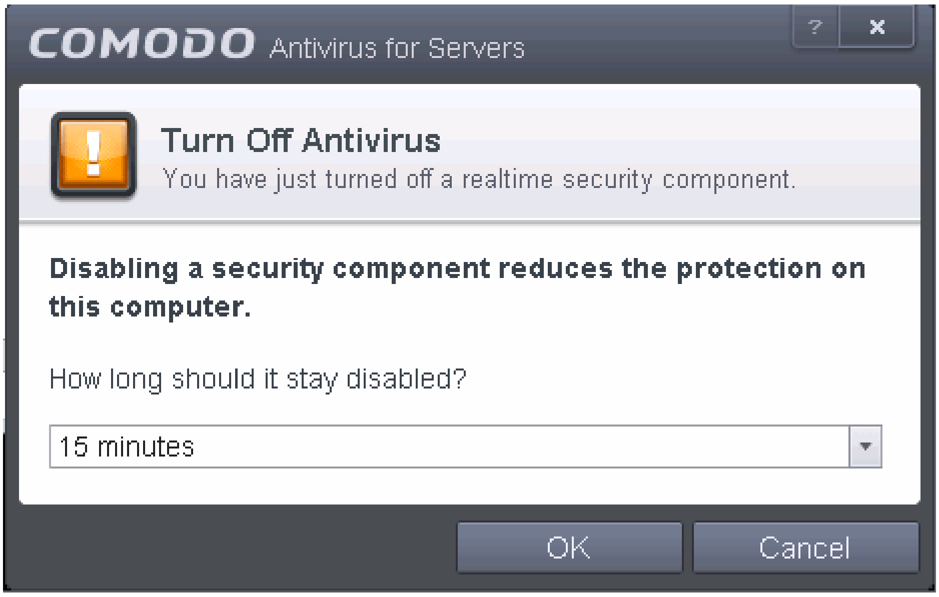
1.5.4. The System Tray Icon

In addition to providing a fast way of starting CAVS, the system tray icon also contains short cuts that allow you to configure the Widget settings. Right click on the icon to access the menu:



- **Antivirus -** You can enable or disable Real-time antivirus scan
- **Auto-Sandbox** - You can enable or disable Auto-Sandbox. You can create rules for running potentially risky applications on an isolated environment. Refer to the sections **Sandbox** and **Configuring Rules for Auto-Sandbox** for more details.

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



COMODO Antivirus for Servers

Turn Off Antivirus

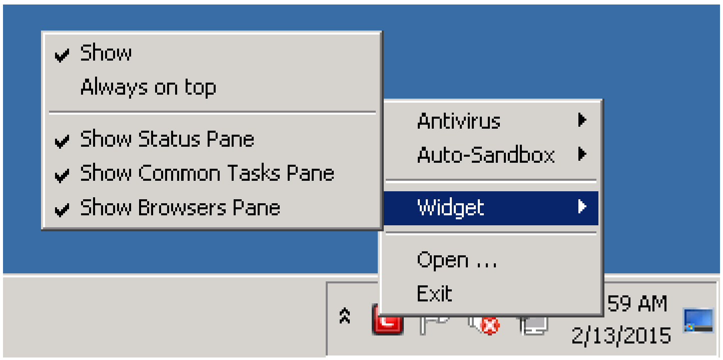
You have just turned off a realtime security component.

Disabling a security component reduces the protection on this computer.

How long should it stay disabled?

15 minutes

- **Open -** Opens CAVS interface if it is minimized or closed.
- **Exit** - Closed the CAVS application.
- **Widget** - You can select whether or not the **Widget** is to be displayed and select the components of it to be displayed.

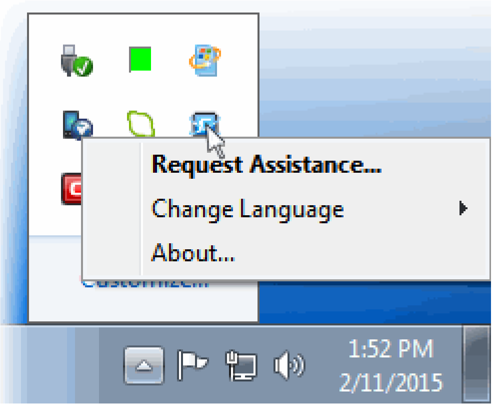


- **Show**: Toggles the display of widget. ***(Default = Disabled)***
- **Always on top**: Displays the widget on top of all windows currently running on your server. ***(Default = Disabled)***
- **Show Status Pane**: Displays the row indicating the current status of CAVS in the widget. ***(Default =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

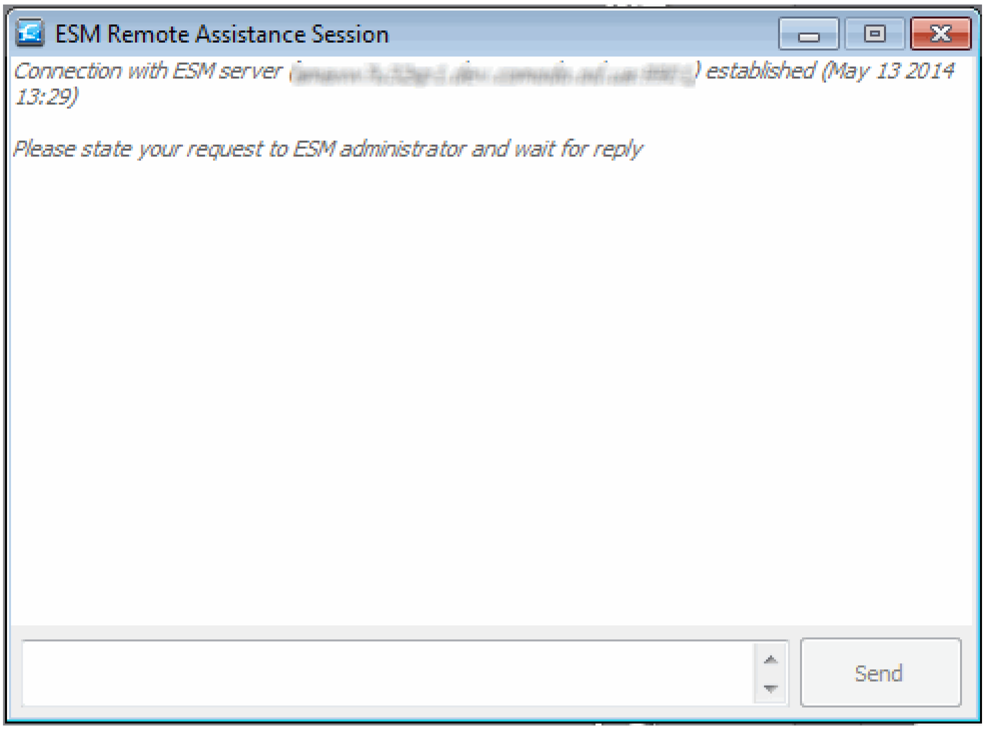
1.5.5. Instant Assistance

The 'Request Assistance...' features allows you to open a chat session with your local administrator or tech support should you need help with problems on your computer. The chat interface allows you to describe your problem and, if required and you agree, will allow the technician to remote desktop into your machine to directly resolve problems.

To request assistance from your administrator, please right-click on the CESM icon in your system tray. If the tray icon is not visible, please contact your administrator, who may have to install some software on your machine.



- Select 'Request Assistance...' to open a chat session. The chat interface works like most instant messaging programs. Simply describe the issue you are experiencing in the field provided and click 'Send'.



Connection with ESM server ([redacted]) established (May 13 2014 13:29)

Please state your request to ESM administrator and wait for reply

1.6. Understanding Security Alerts

Alerts Overview

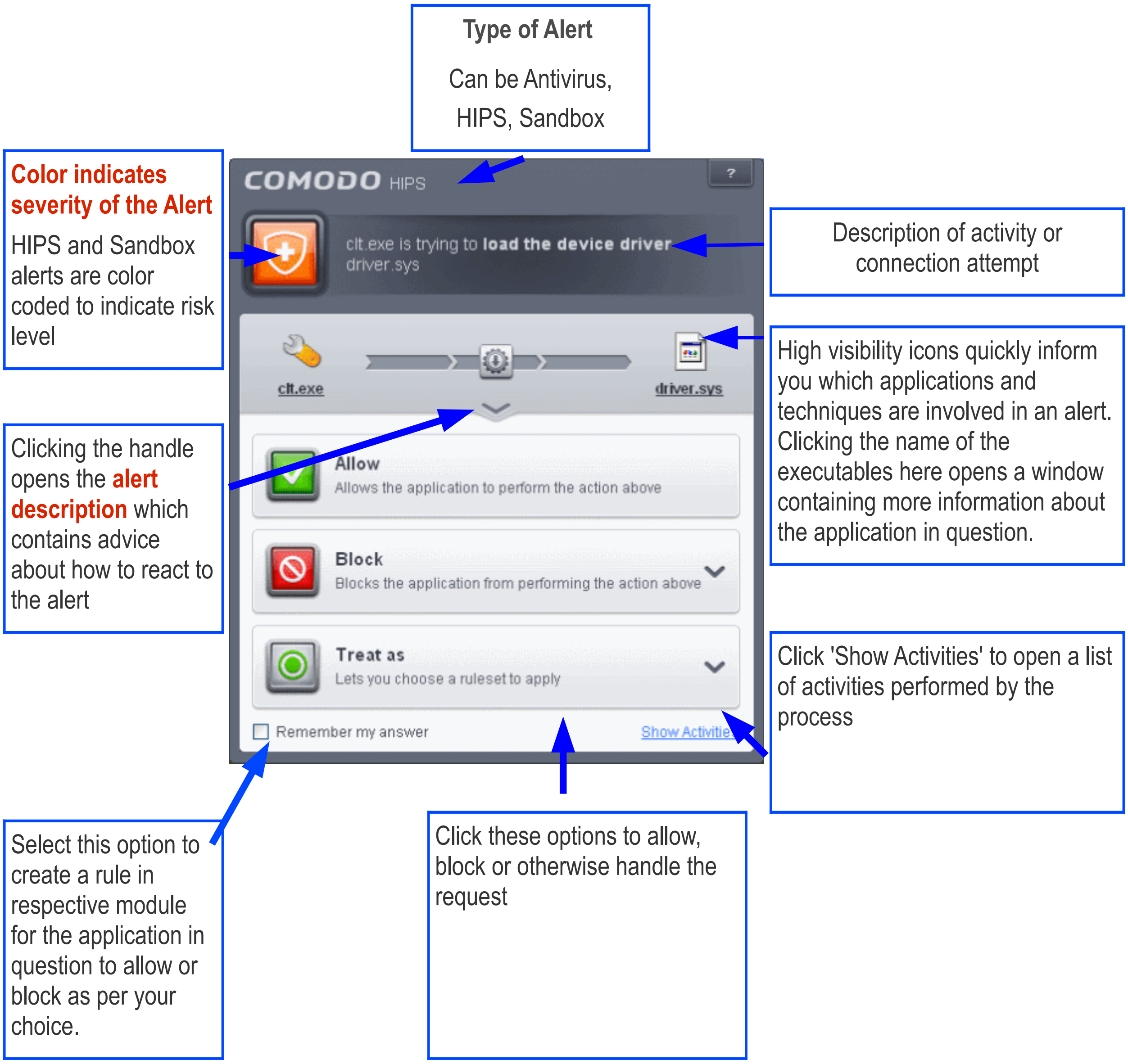
- **Alert Types**
- **Severity Levels**
- **Descriptions**

- **Antivirus Alerts**
- **HIPS Alerts**
  - **Device Driver Installation and Physical Memory Access Alerts**
  - **Protected Registry Key Alerts**
  - **Protected File Alerts**

- Sandbox Alerts
    - Sandbox Notification
    - Elevated Privilege Alerts

Alerts Overview

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



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

Allow Allows the application to perform the action above

Block Blocks the application from performing the action above

Treat as Lets you choose a ruleset to apply

□ Remember my answer

Type of Alert

Can be Antivirus, HIPS, Sandbox

Color indicates severity of the Alert

HIPS and Sandbox alerts are color coded to indicate risk level

Description of activity or connection attempt

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

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

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

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

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

Alert Types

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

- **Antivirus Alerts** - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when **Antivirus is enabled** and the option '**Do not show antivirus alerts**' is disabled in **Real-time**

Scanner Settings.

- **HIPS Alerts** - Shown whenever an application attempts an unauthorized action or tries to access protected areas. HIPS alerts will only be generated if **HIPS is enabled** and **Do NOT show popup alerts** is disabled.
- **Sandbox Alerts** (including **Elevated Privilege Alerts**)- Shown whenever an application tries to modify the Operating System or related files and when the Defense+ automatically sandboxes an unrecognizable file. Sandbox Alerts will be displayed only if privilege elevation alerts **is enabled** under **Sandbox Settings**.

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

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

Severity Level

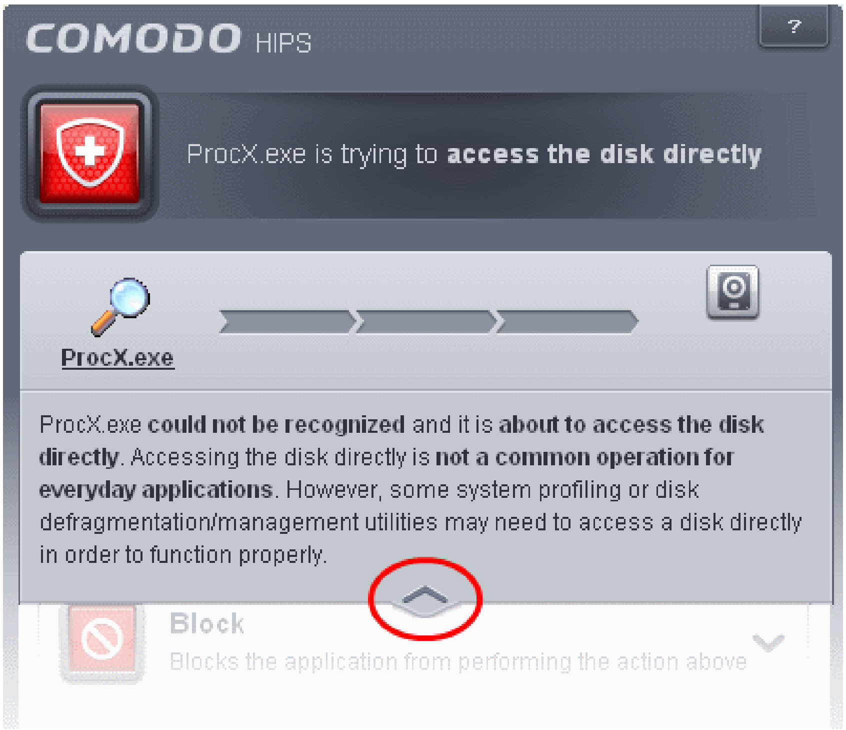
The shield icons at the upper left of each alert are color coded according to the risk level presented by the activity or request. However, it cannot be stressed enough that you should still read the information in order to reach an informed decision on allowing or blocking the activity.

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

Note: Antivirus alert is not ranked in this way. It always appears with a red icon.

Alert Description

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



COMODO HIPS
?
ProcX.exe is trying to **access the disk directly**
ProcX.exe

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

Block
Blocks the application from performing the action above

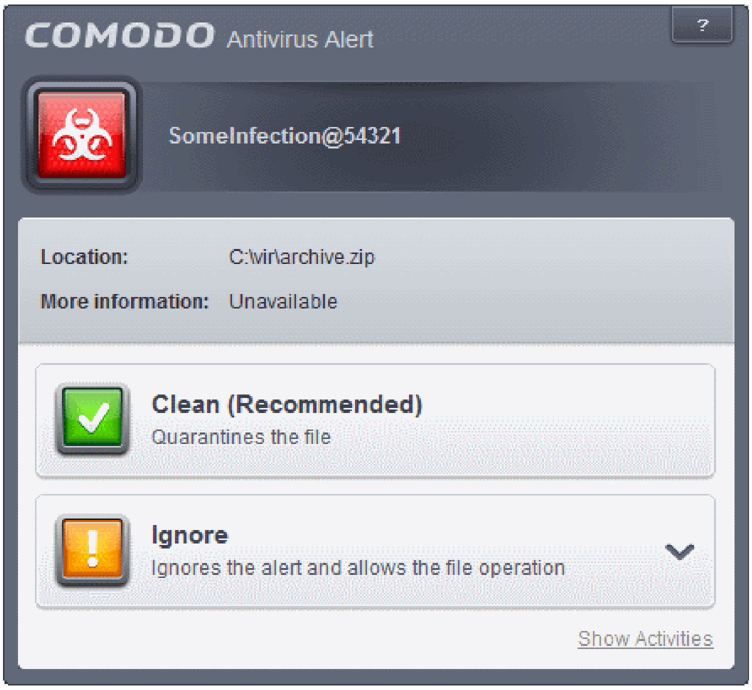
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answering an Antivirus Alert

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

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



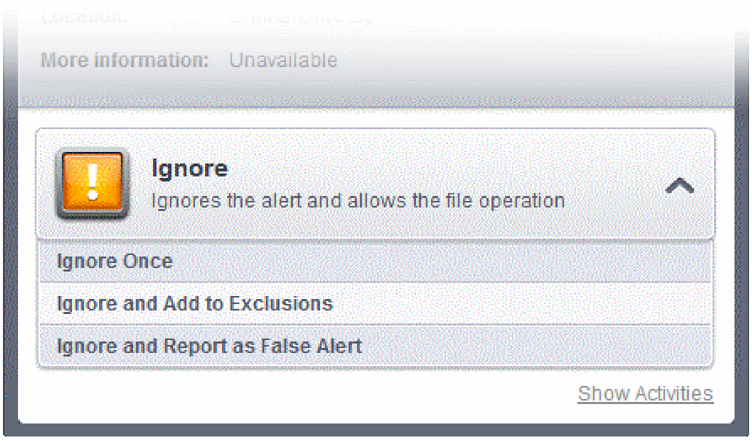
SomeInfection@54321

Location: C:\wir\archive.zip

More information: Unavailable

The following response-options are available:

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



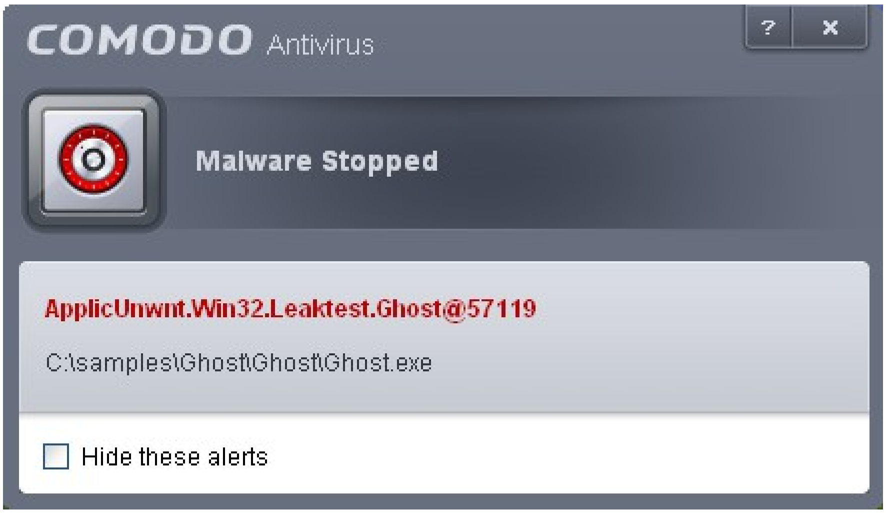
More information: Unavailable

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

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

Antivirus Notification

If CES detects a virus or other malware, it will immediately block it and provide you with instant on-screen notification:



COMODO Antivirus

Malware Stopped

ApplicUnwnt.Win32.Leaktest.Ghost@57119

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

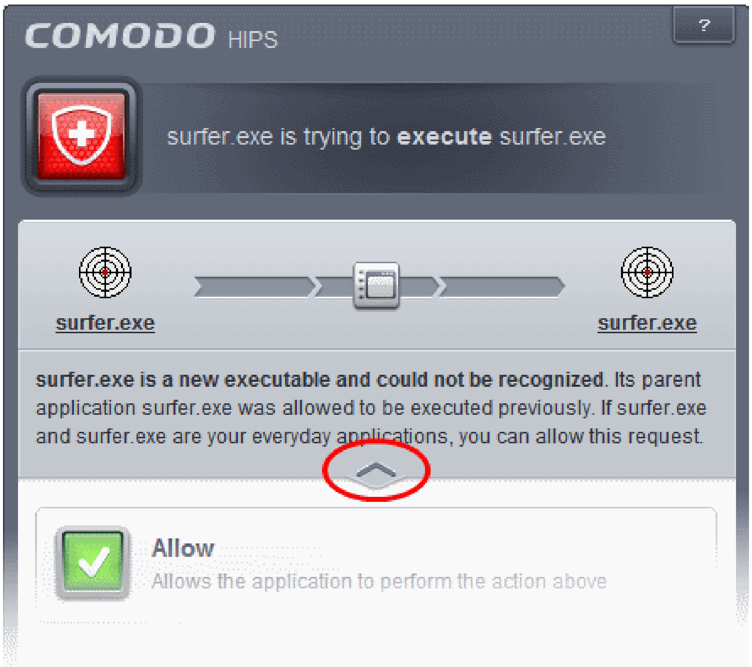
☐ Hide these alerts

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

Answering HIPS Alerts

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

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



COMODO HIPS

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

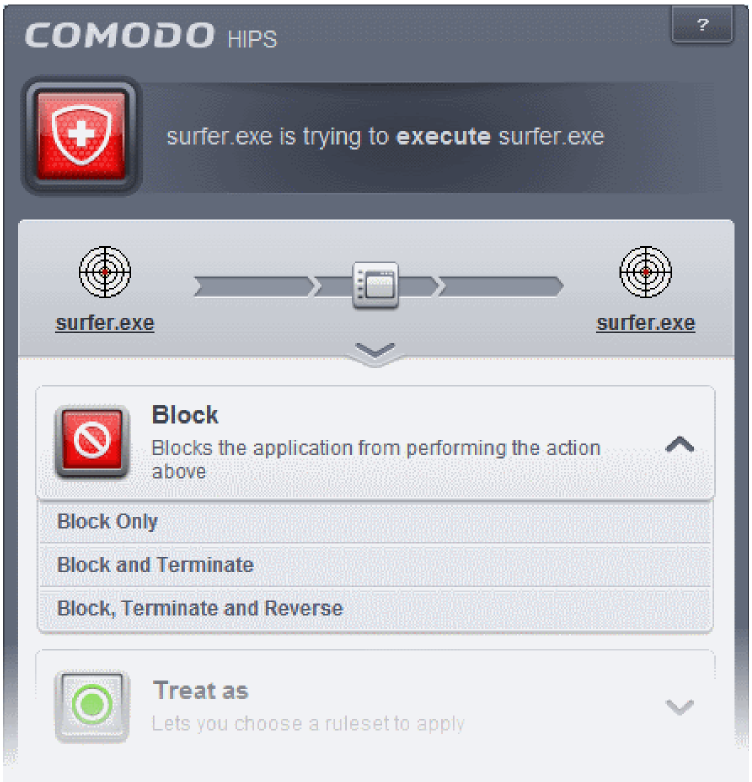
surfer.exe is a new executable and could not be recognized. Its parent application surfer.exe was allowed to be executed previously. If surfer.exe and surfer.exe are your everyday applications, you can allow this request.

Allow

Allows the application to perform the action above

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

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



COMODO HIPS

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

Block

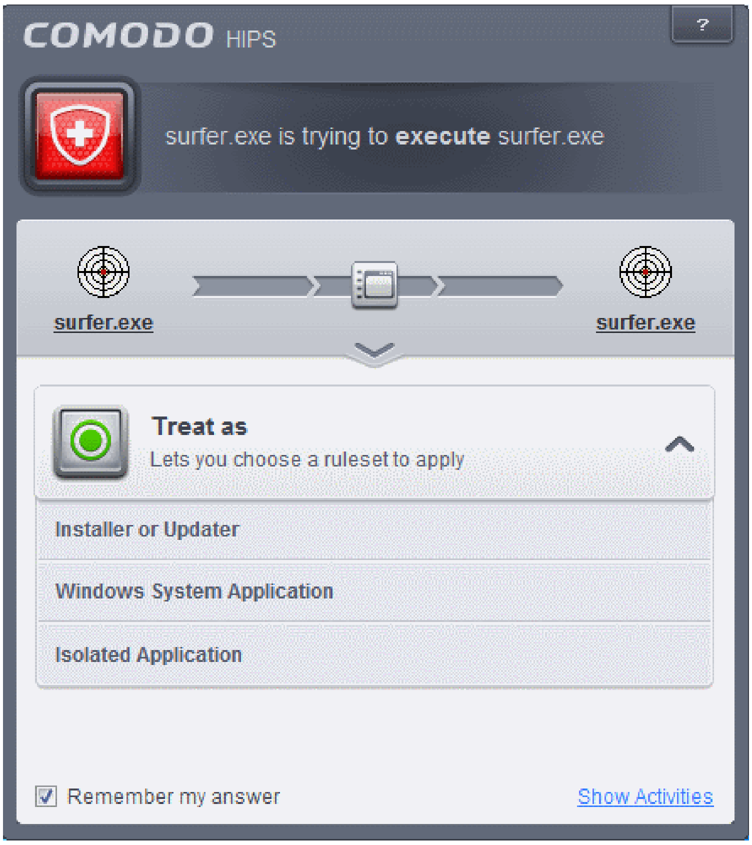
Blocks the application from performing the action above

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

Treat as

Lets you choose a ruleset to apply

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



COMODO HIPS

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

Treat as

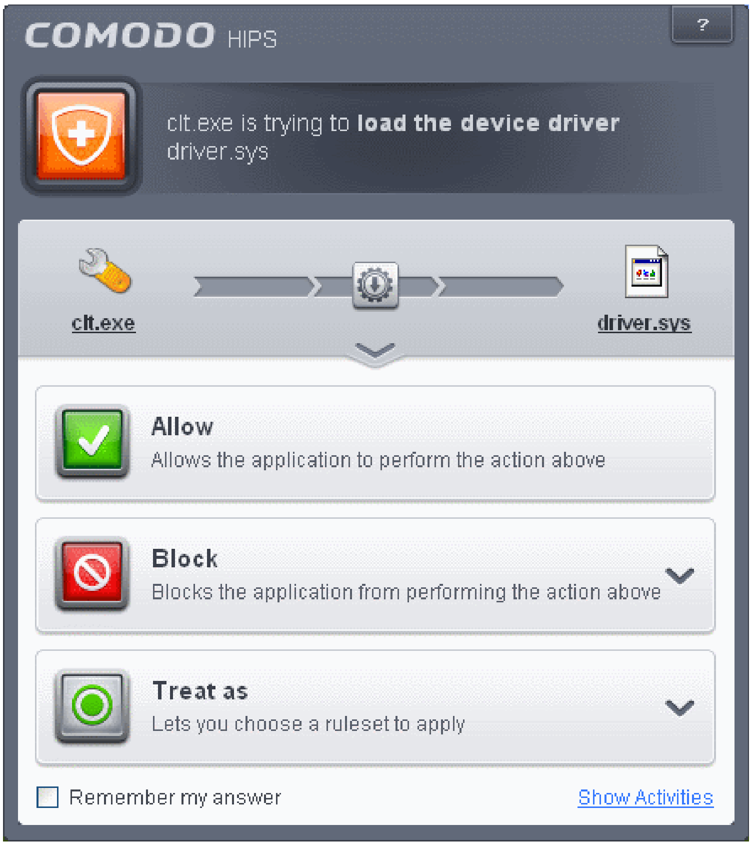
Lets you choose a ruleset to apply

- Installer or Updater
- Windows System Application
- Isolated Application

☑ Remember my answer

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

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


COMODO HIPS

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

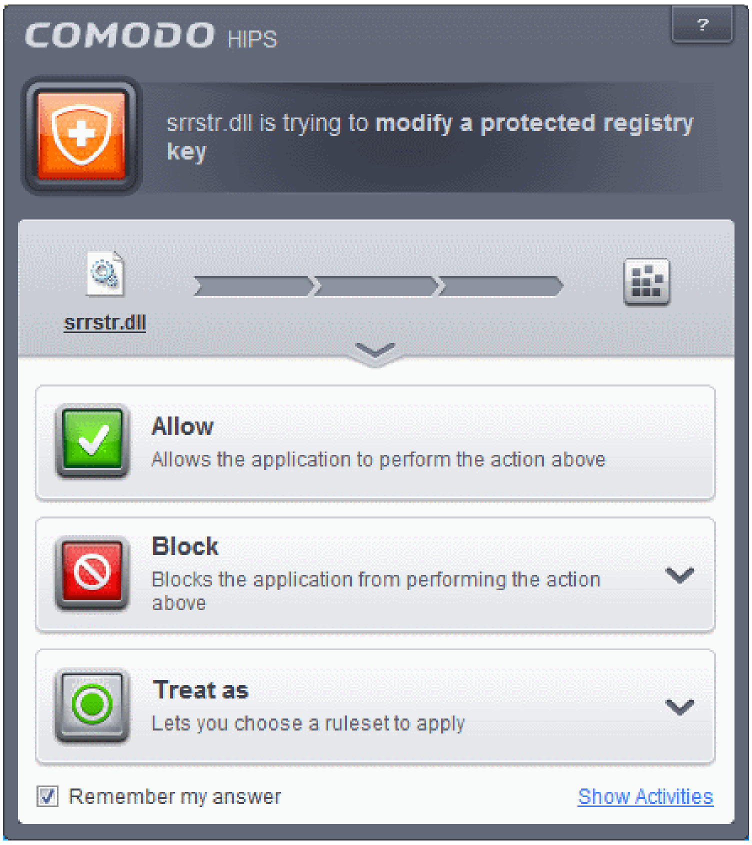
Allow
Allows the application to perform the action above

Block
Blocks the application from performing the action above

Treat as
Lets you choose a ruleset to apply

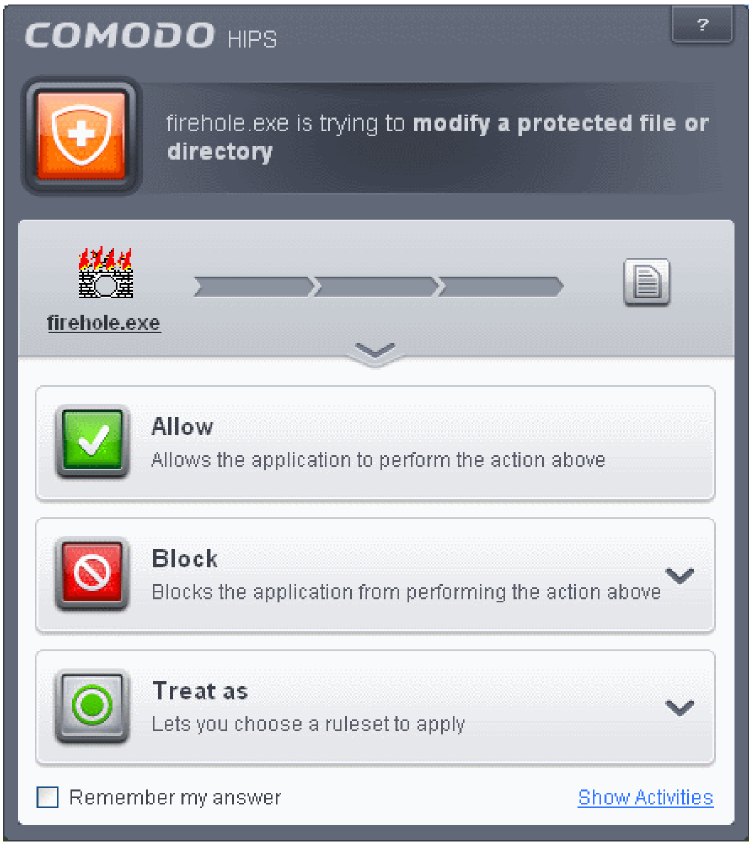
□ Remember my answer

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



COMODO HIPS
?
srrstr.dll is trying to **modify a protected registry key**
srrstr.dll
Allow
Allows the application to perform the action above
Block
Blocks the application from performing the action above
Treat as
Lets you choose a ruleset to apply
☑ Remember my answer
Show Activities

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



COMODO HIPS
?
firehole.exe is trying to **modify a protected file or directory**
firehole.exe
Allow
Allows the application to perform the action above
Block
Blocks the application from performing the action above
Treat as
Lets you choose a ruleset to apply
□ Remember my answer
Show Activities

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

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

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

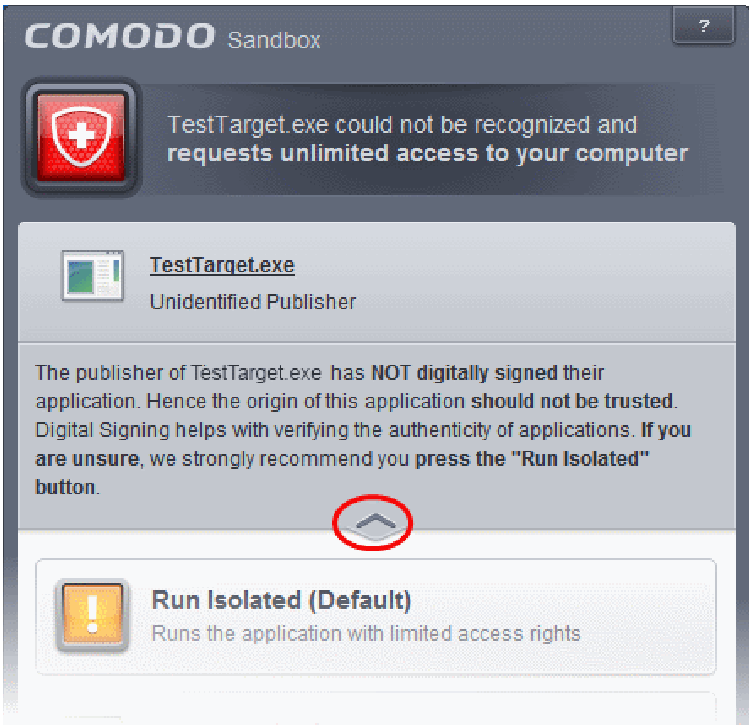
6. If a HIPS alert reports a malware behavior in the security considerations area then you should **Block the request** permanently by selecting **Remember My Answer** option. As this is probably a virus, you should also submit the application in question, to Comodo for analysis.
7. Unrecognized applications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

Answering a Sandbox Alert

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

Please read the following advice before answering a Sandbox alert:

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



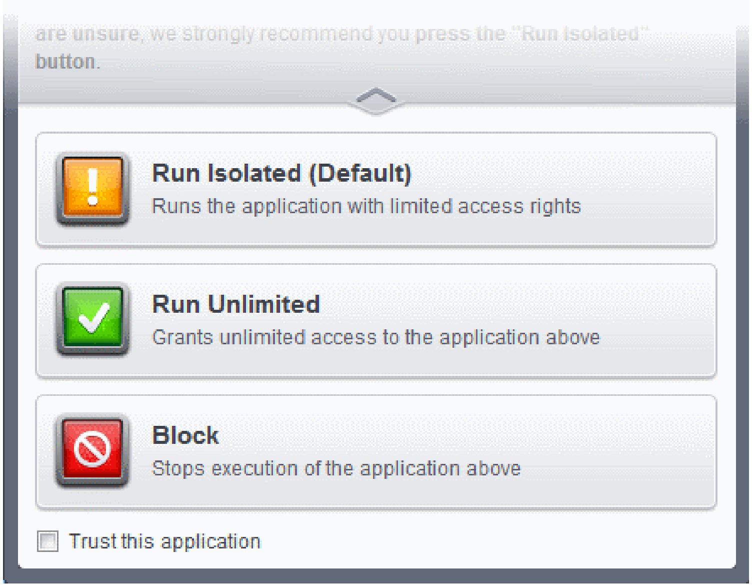
COMODO Sandbox

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

TestTarget.exe
Unidentified Publisher

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

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



are unsure, we strongly recommend you press the "Run Isolated" button.
Run Isolated (Default)
Runs the application with limited access rights
Run Unlimited
Grants unlimited access to the application above
Block
Stops execution of the application above
□ Trust this application

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

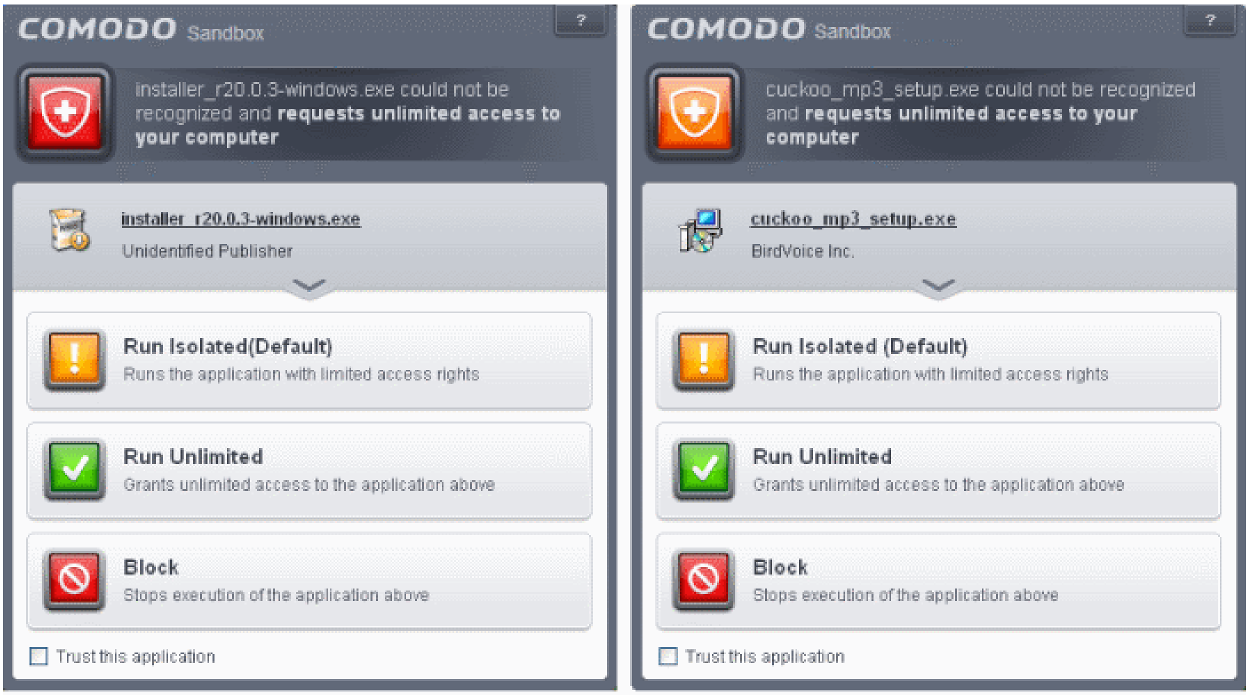
Run with Elevated Privileges Alert

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

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

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

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



COMODO Sandbox

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

installer_r20.0.3-windows.exe
Unidentified Publisher

Run Isolated(Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

COMODO Sandbox

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

cuckoo_mp3_setup.exe
BirdVoice Inc.

Run Isolated (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

Unknown and not digitally signed

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

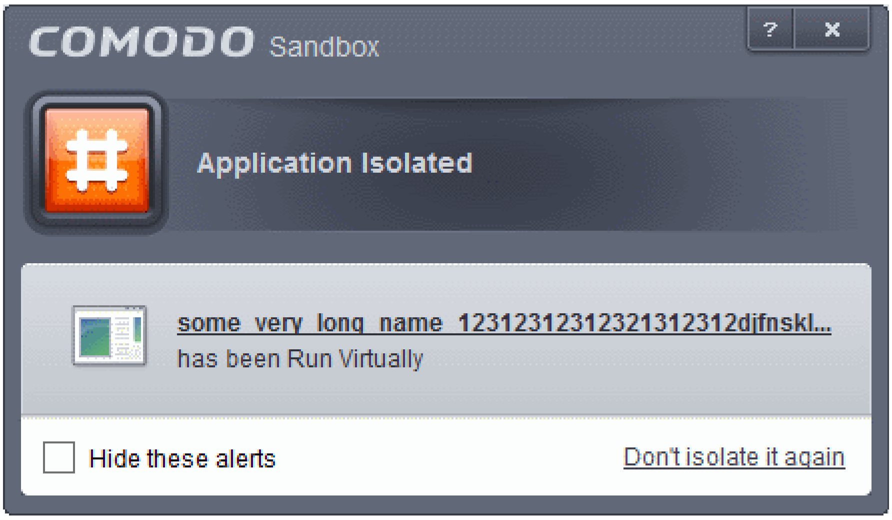
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

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

Sandbox Notification

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



some_very_long_name_1231231231232131231 2djfnskl...
has been Run Virtually

□ Hide these alerts

Don't isolate it again

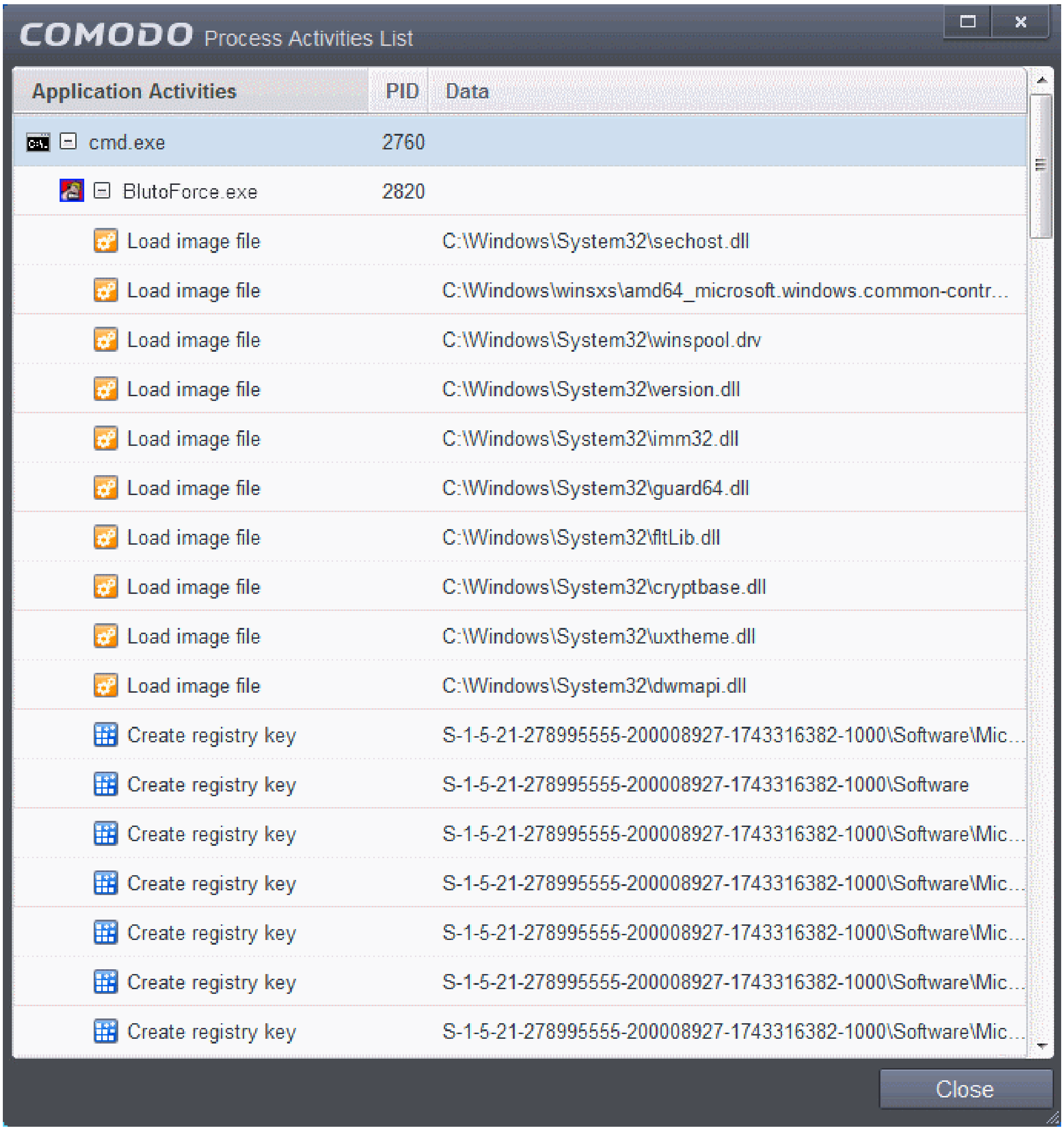
The alert will show the name of the executable that has been auto-sandboxed. The application will be automatically added to the **File List** with the 'Unrecognized' rating.

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

Users are also reminded that they should submit such unknown applications to Comodo via the '**File List**' interface. This will allow Comodo to analyze the executable and, if it is found to be safe, to add it to the global safe list. This will ensure that unknown but ultimately safe applications are quickly white-listed for all users.

Also see:

- **'Unknown Files: The Scanning Processes'** - to understand process behind how CAVS scans files
- To view the activities of the processes, click the Show Activities link at the bottom right. The Process Activities List dialog will open with a list of activities exhibited by the process.



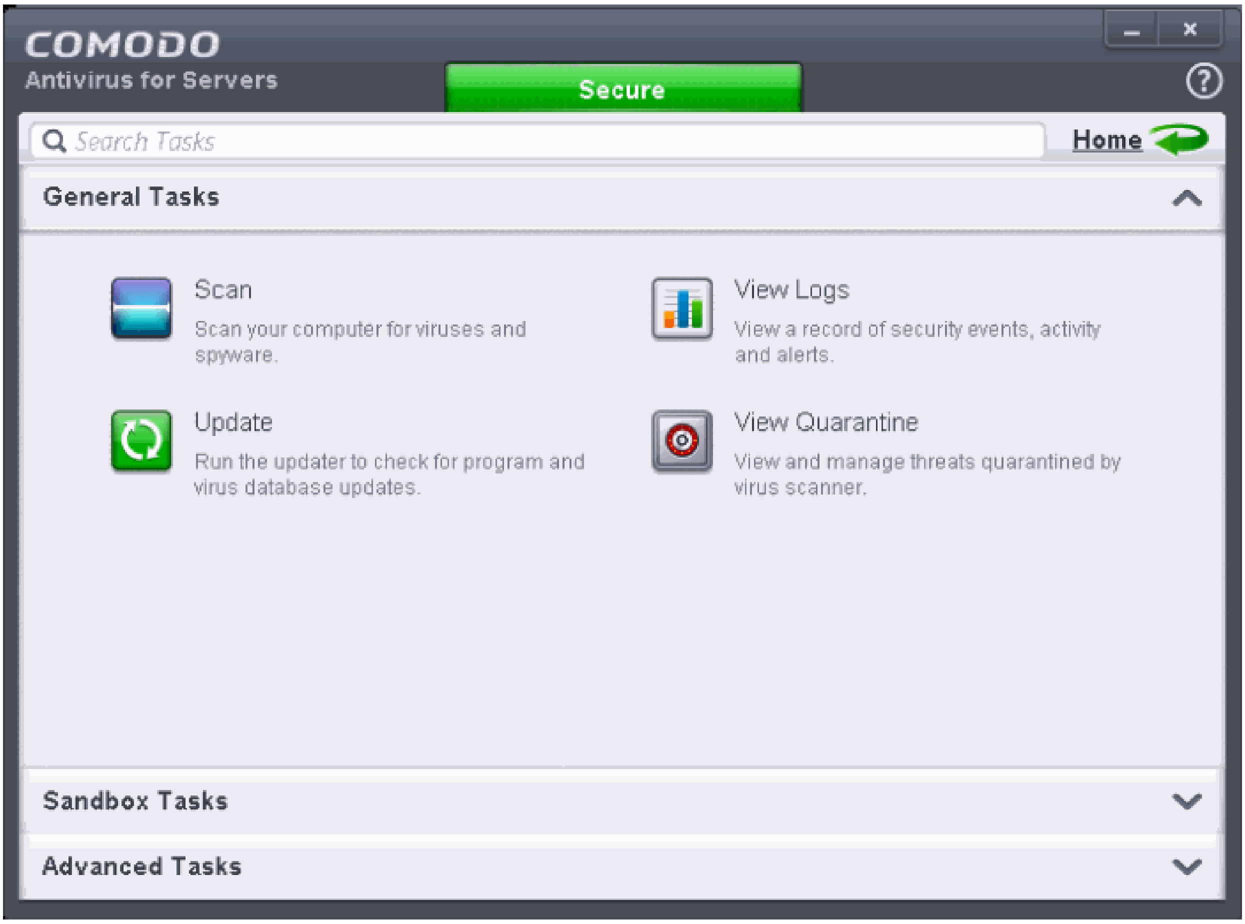
Application Activities	PID	Data
cmd.exe	2760	
BlutoForce.exe	2820	
Load image file		C:\Windows\System32\sechost.dll
Load image file		C:\Windows\winsxs\amd64_microsoft.windows.common-contr...
Load image file		C:\Windows\System32\winspool.drv
Load image file		C:\Windows\System32\version.dll
Load image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

Column Descriptions

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

2. General Tasks – Introduction

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



Scan
Scan your computer for viruses and spyware.

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

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

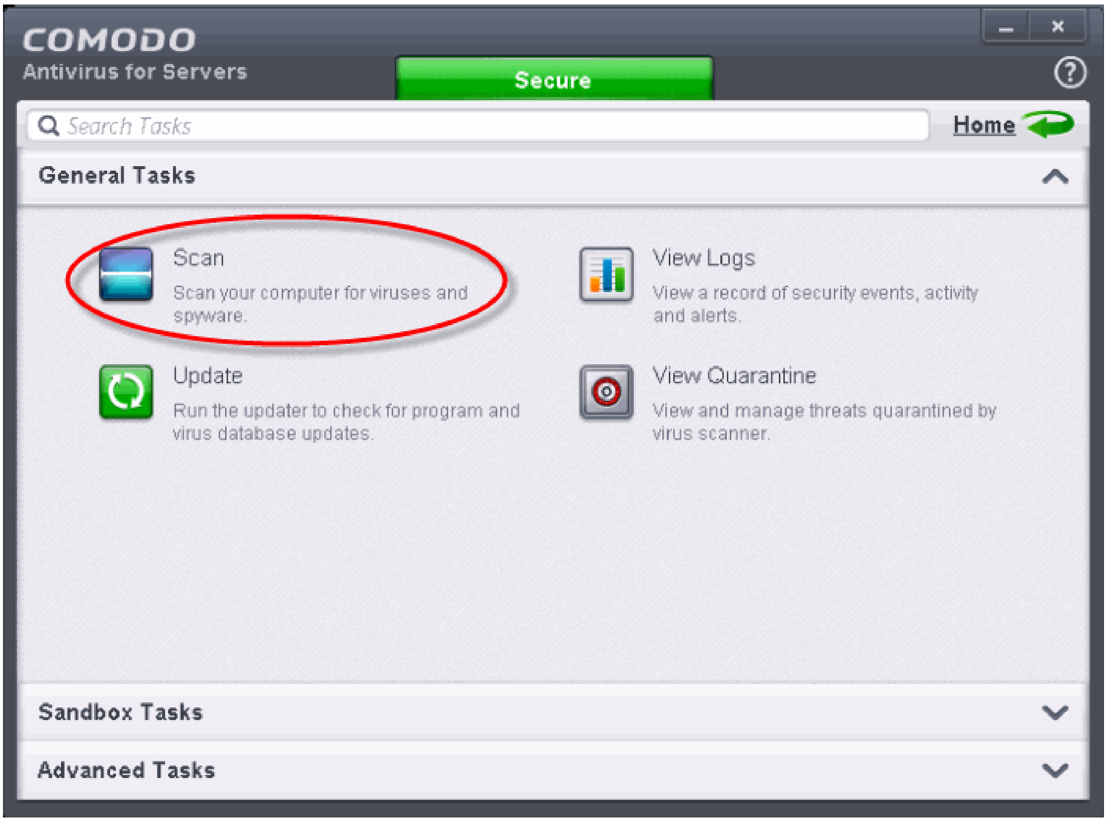
View Quarantine
View and manage threats quarantined by virus scanner.

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

- **Scan and Clean your Server**
- **Instantly Scan Files And Folders**
- **Processing Infected Files**
- **Manage Virus Database and Program Updates**
- **View CAVS Logs**
- **Manage Quarantined Items**

2.1. Scan and Clean Your Server

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



Scan
Scan your computer for viruses and spyware.

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

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

View Quarantine
View and manage threats quarantined by virus scanner.

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

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

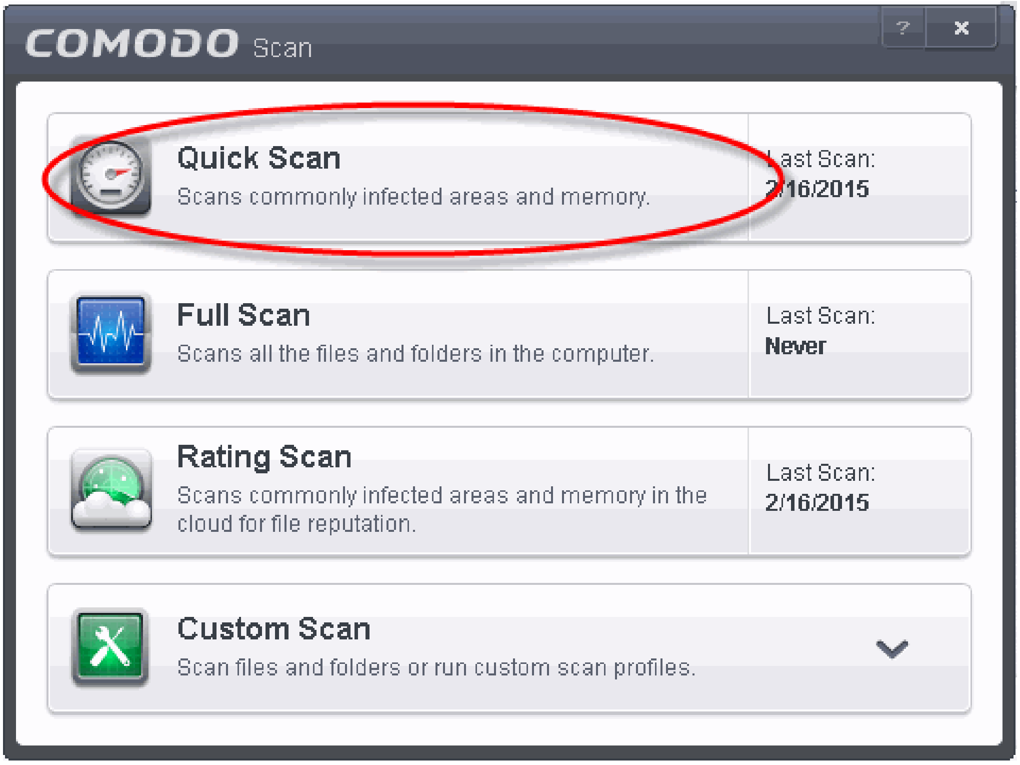
2.1.1.Run a Quick Scan

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

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

To run a Quick Scan

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



COMODO Scan

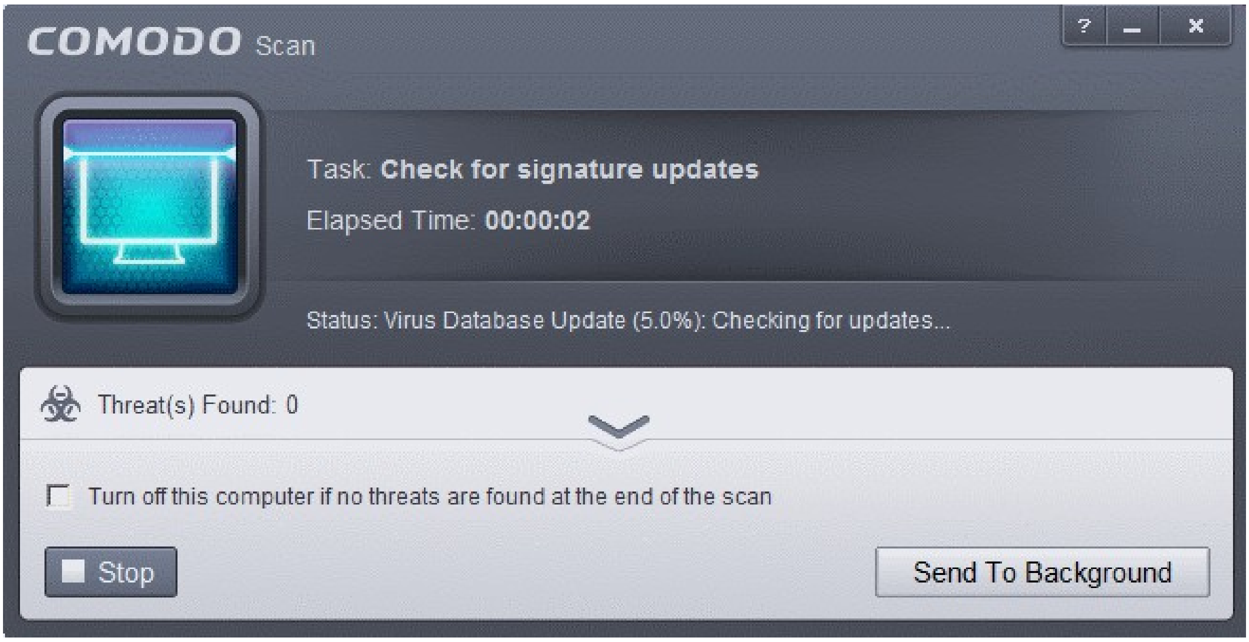
Quick Scan
Scans commonly infected areas and memory.
Last Scan: 2/16/2015

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

Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
Last Scan: 2/16/2015

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

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



COMODO Scan

Task: **Check for signature updates**

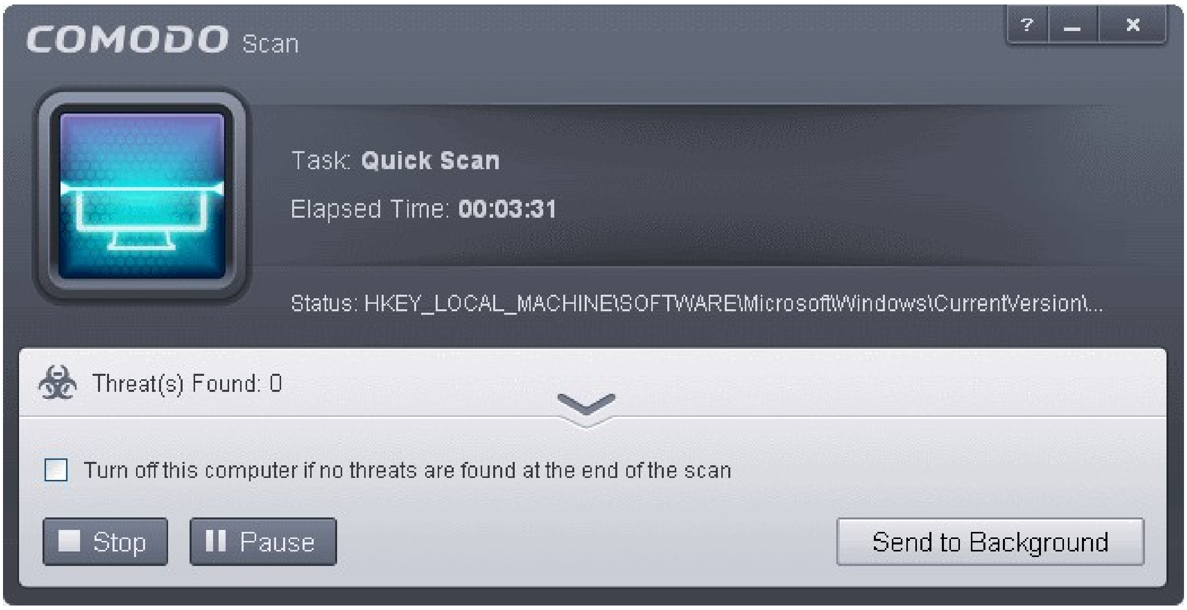
Elapsed Time: **00:00:02**

Status: Virus Database Update (5.0%): Checking for updates...

Threat(s) Found: 0

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

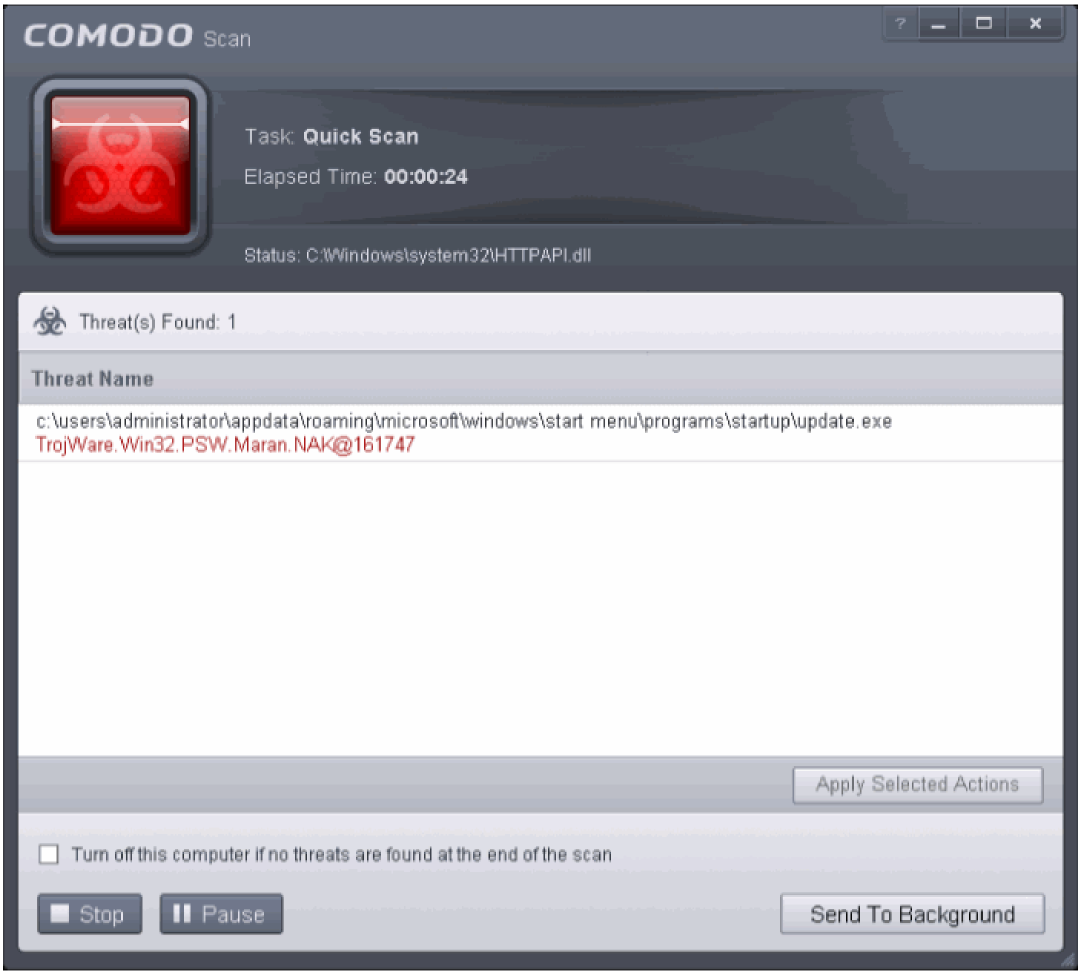
If the database is outdated, the scanner will first download and install the latest database. Once CAVS has the latest database, the scanner starts the scan and the progress will be displayed:



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

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

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



Threat Name
c:\users\administrator\appdata\roaming\microsoft\windows\start menu\programs\startup\update.exe TrojWare.Win32.PSW.Maran.NAK@161747

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

The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

2.1.2. Run a Full Server Scan

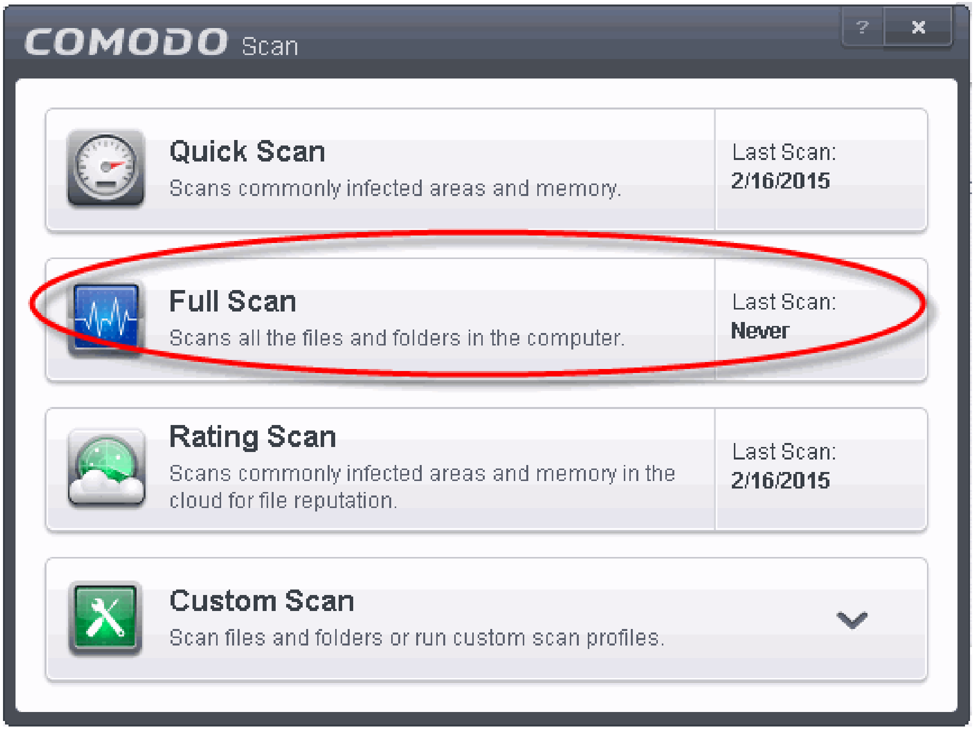
The 'Full System Scan' scans every local drive, folder and file on your server. Any external devices like USB drives, digital camera and so on are also scanned.

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

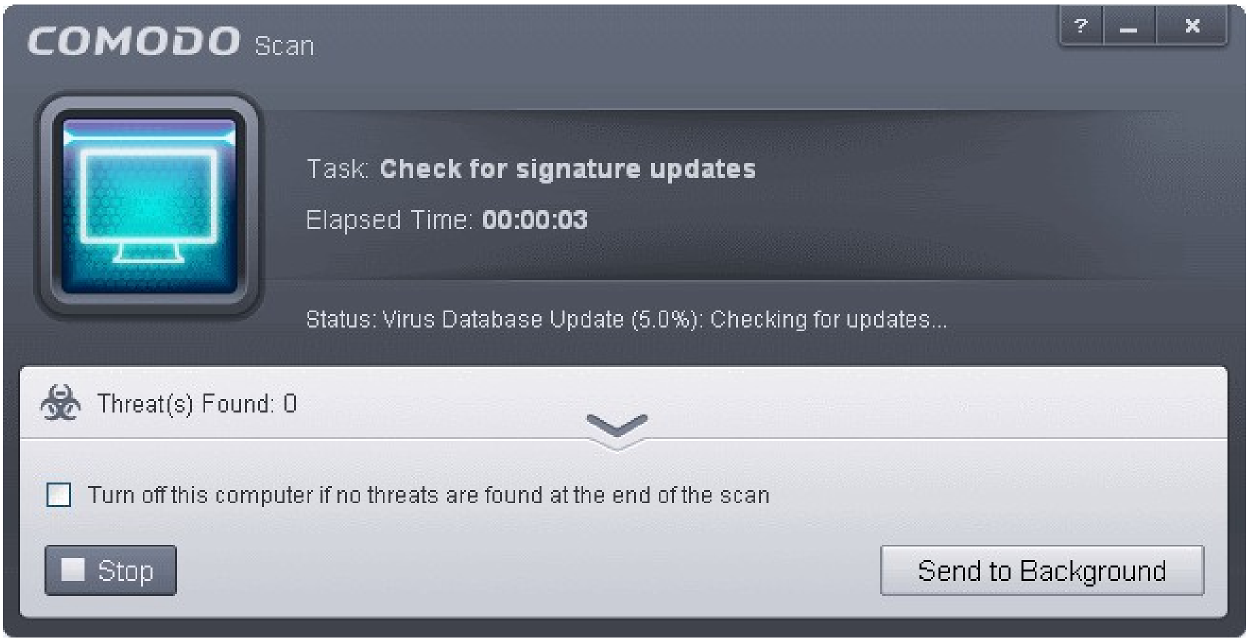
Refer to **Antivirus Settings > Scan Profiles** for more details.

To run a Full Server Scan

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


COMODO Scan
?
×
Quick Scan
Scans commonly infected areas and memory.
Last Scan:
2/16/2015
Full Scan
Scans all the files and folders in the computer.
Last Scan:
Never
Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
Last Scan:
2/16/2015
Custom Scan
Scan files and folders or run custom scan profiles.

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



Task: **Check for signature updates**

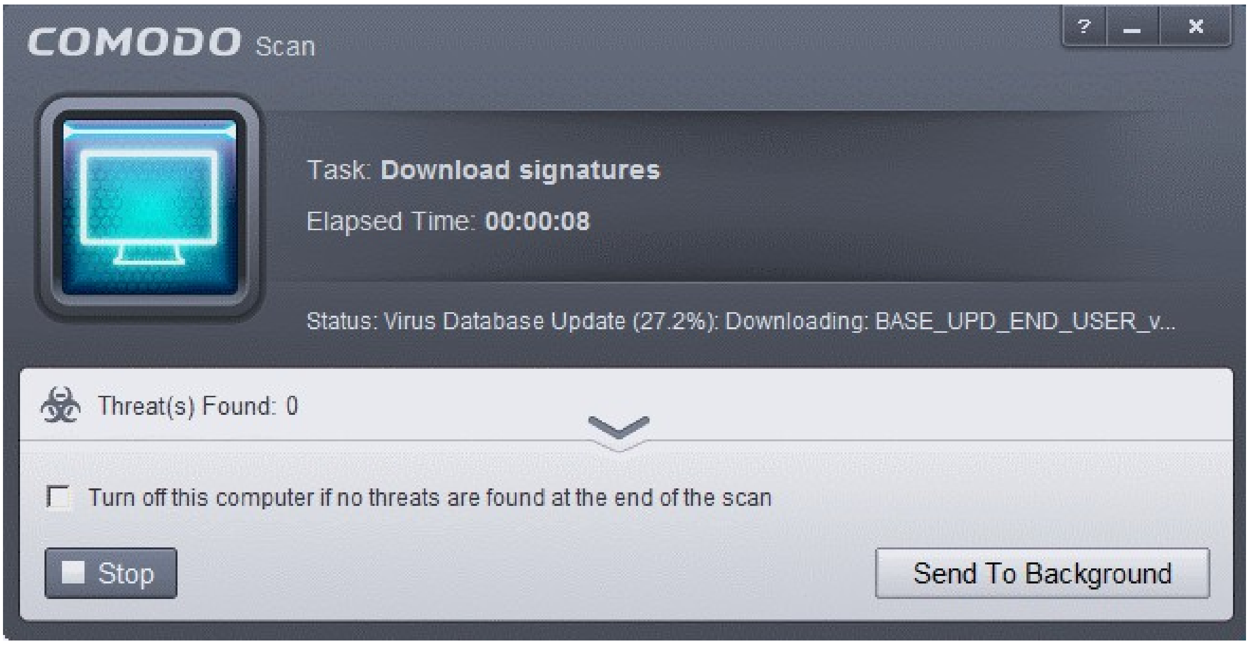
Elapsed Time: **00:00:03**

Status: Virus Database Update (5.0%): Checking for updates...

Threat(s) Found: 0

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

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



Task: **Download signatures**

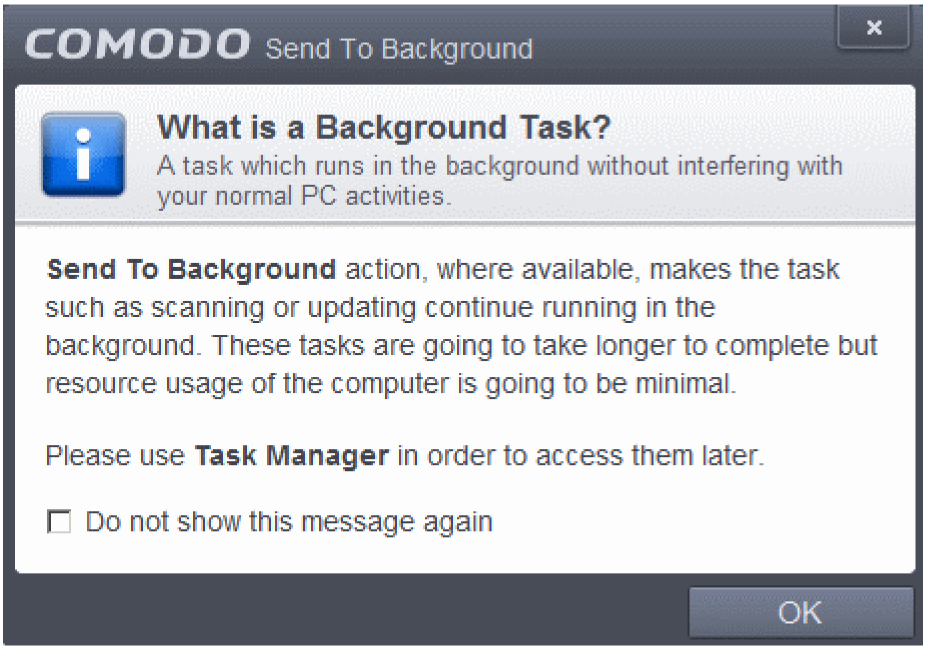
Elapsed Time: **00:00:08**

Status: Virus Database Update (27.2%): Downloading: BASE_UPD_END_USER_v...

Threat(s) Found: 0

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

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



What is a Background Task?

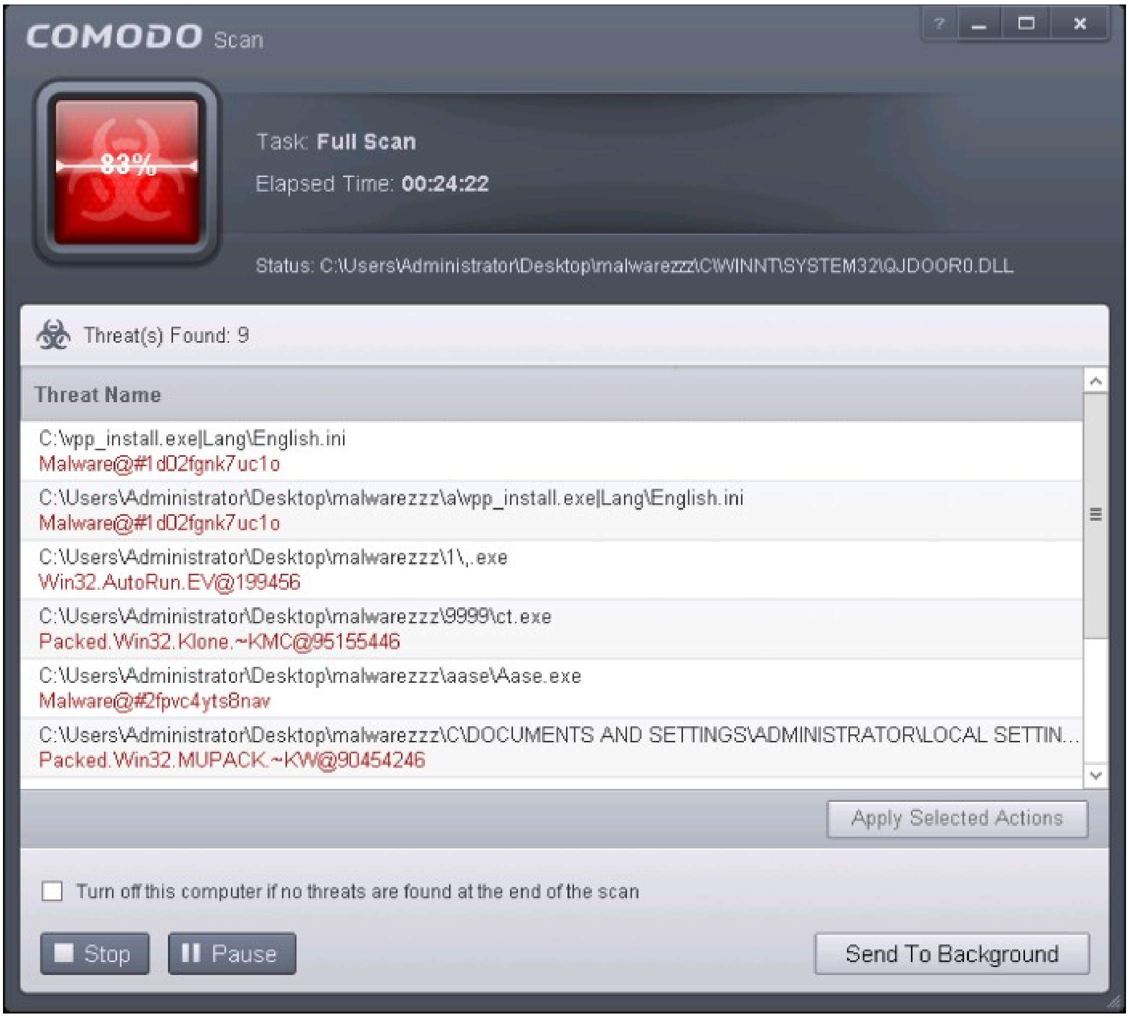
A task which runs in the background without interfering with your normal PC activities.

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

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

□ Do not show this message again

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



Task: **Full Scan**

Elapsed Time: **00:24:22**

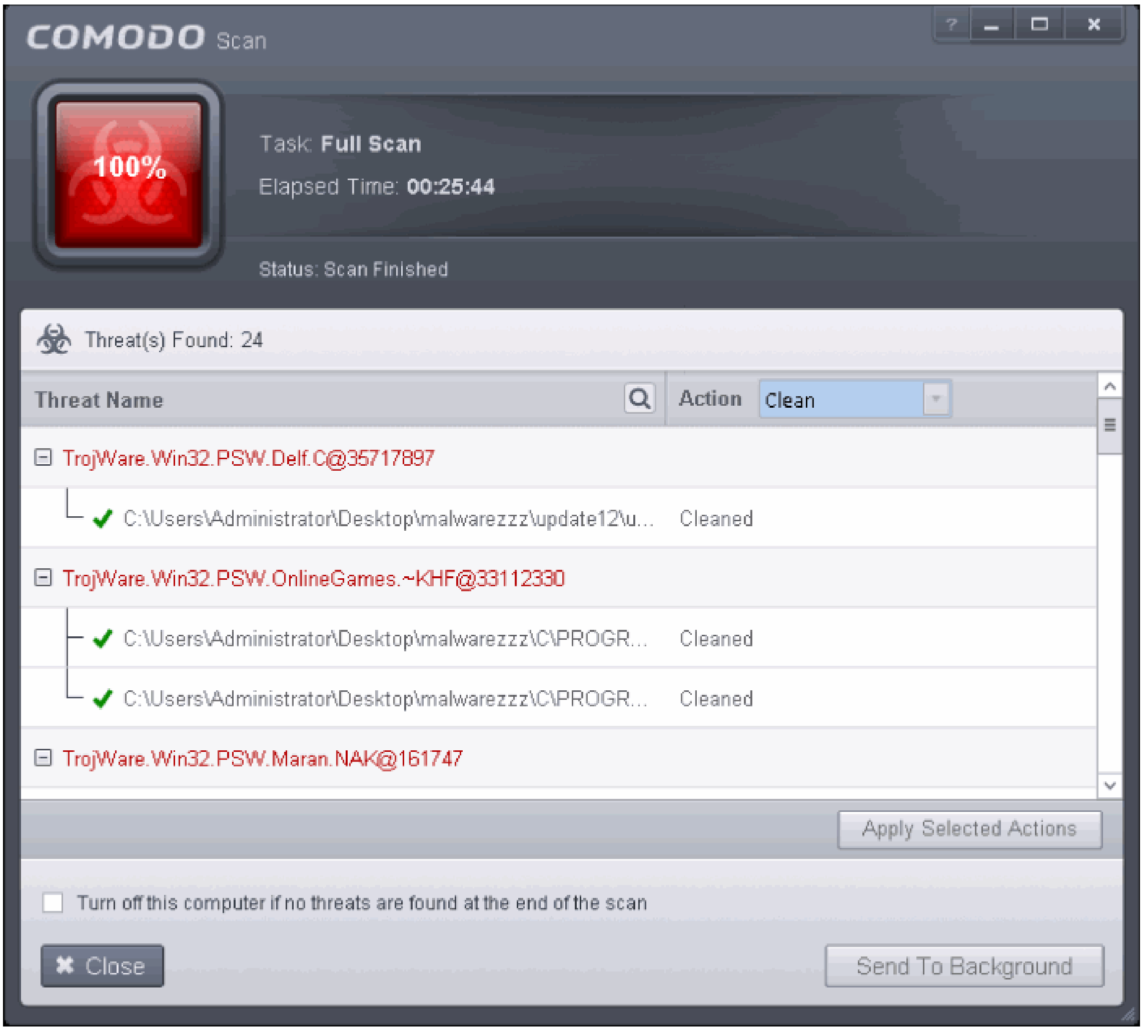
Status: C:\Users\Administrator\Desktop\malwarezzz\C\WINNT\SYSTEM32\QJDOOR0.DLL

Threat(s) Found: 9

Threat Name
C:\wpp_install.exe|Lang\English.ini Malware@#1d02fgnk7uc1o
C:\Users\Administrator\Desktop\malwarezzz\a\wpp_install.exe|Lang\English.ini Malware@#1d02fgnk7uc1o
C:\Users\Administrator\Desktop\malwarezzz\1\,.exe Win32.AutoRun.EV@199456
C:\Users\Administrator\Desktop\malwarezzz\9999\ct.exe Packed.Win32.Klone.~KMC@95155446
C:\Users\Administrator\Desktop\malwarezzz\aase\Aase.exe Malware@#2fpvc4yts8nav
C:\Users\Administrator\Desktop\malwarezzz\C\DOCUMENTS AND SETTINGS\ADMINISTRATOR\LOCAL SETTIN... Packed.Win32.MUPACK.~KW@90454246

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

- On completion of scanning, the scan results screen will be displayed.



Task: Full Scan

Elapsed Time: 00:25:44

Status: Scan Finished

Threat(s) Found: 24

Threat Name	Action: Clean
TrojWare.Win32.PSW.Delf.C@35717897	
✓ C:\Users\Administrator\Desktop\malwarezzz\update12\u...	Cleaned
TrojWare.Win32.PSW.OnlineGames.~KHF@33112330	
✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...	Cleaned
✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...	Cleaned
TrojWare.Win32.PSW.Maran.NAK@161747	

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

The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

2.1.3. Run a Rating Scan

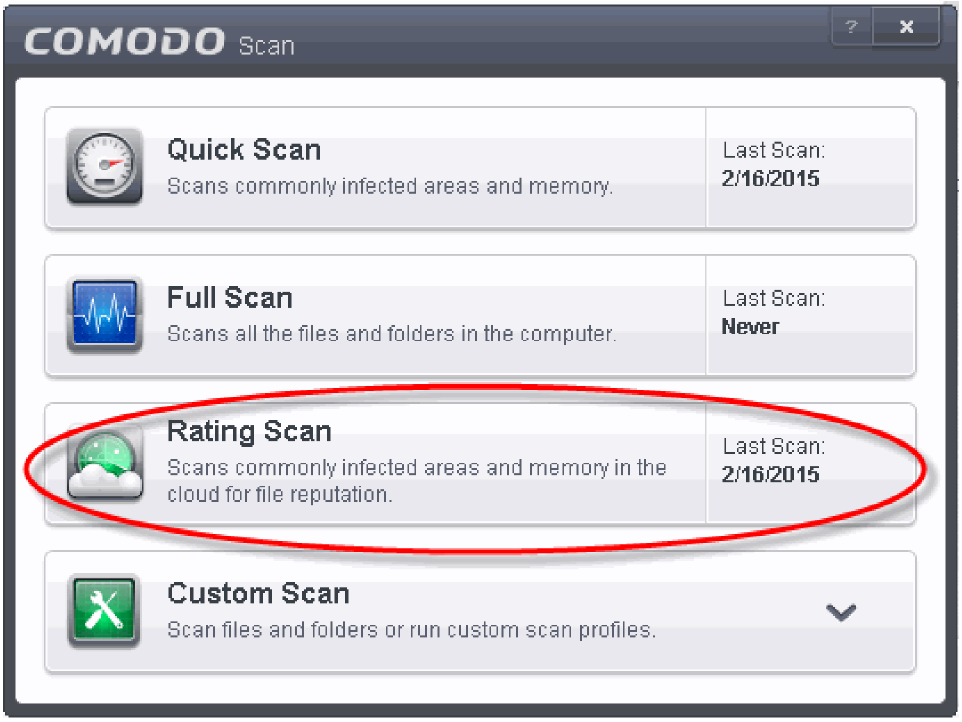
The 'Rating Scan' feature runs a cloud-based assessment on files on your server to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

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

To run a Rating scan

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



COMODO Scan

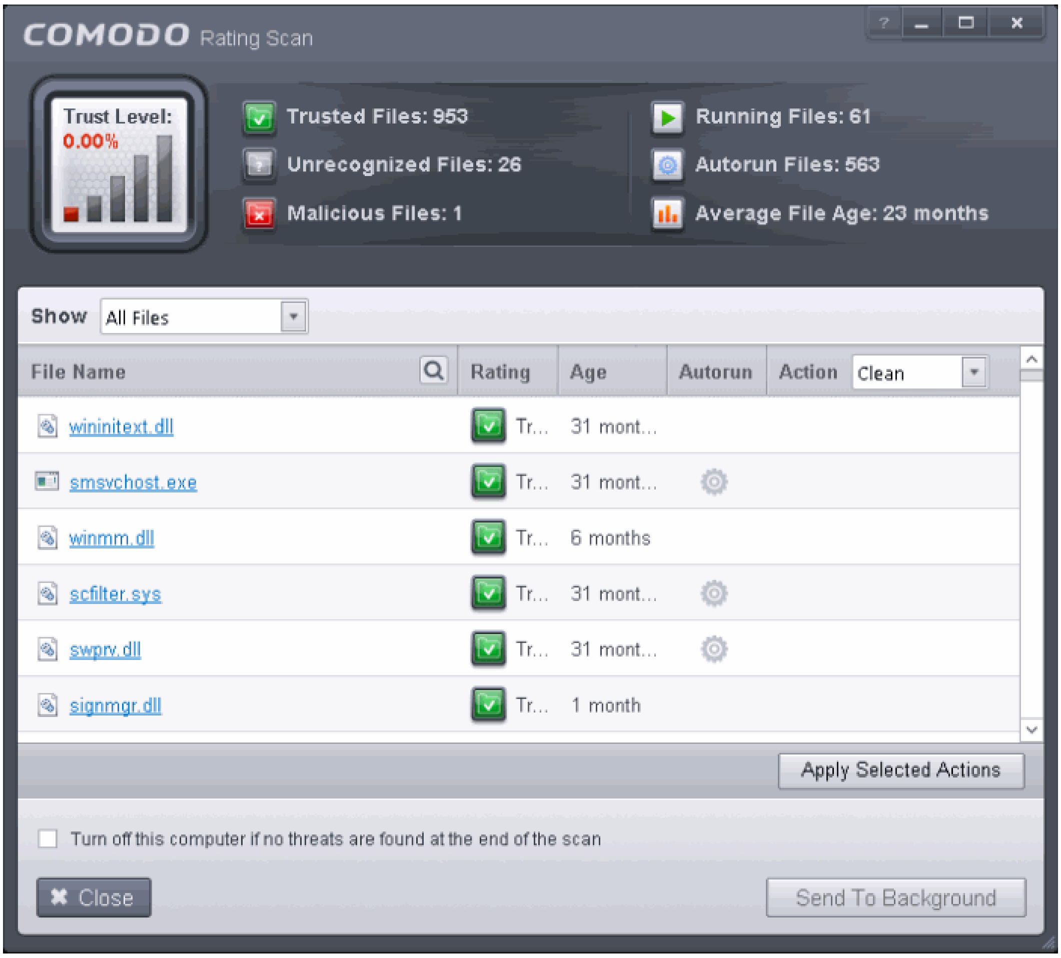
Quick Scan
Scans commonly infected areas and memory.
Last Scan: 2/16/2015

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

Rating Scan
Scans commonly infected areas and memory in the cloud for file reputation.
Last Scan: 2/16/2015

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

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



COMODO Rating Scan

Trust Level: 0.00%

Trusted Files: 953
Unrecognized Files: 26
Malicious Files: 1
Running Files: 61
Autorun Files: 563
Average File Age: 23 months

Show: All Files

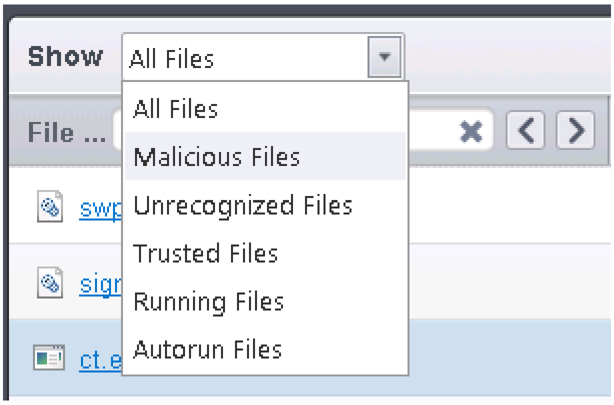
File Name	Rating	Age	Autorun	Action: Clean
wininitext.dll	Tr...	31 mont...		
smsvchost.exe	Tr...	31 mont...	⚙	
winmm.dll	Tr...	6 months		
scfilter.sys	Tr...	31 mont...	⚙	
swprv.dll	Tr...	31 mont...	⚙	
signmgr.dll	Tr...	1 month		

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

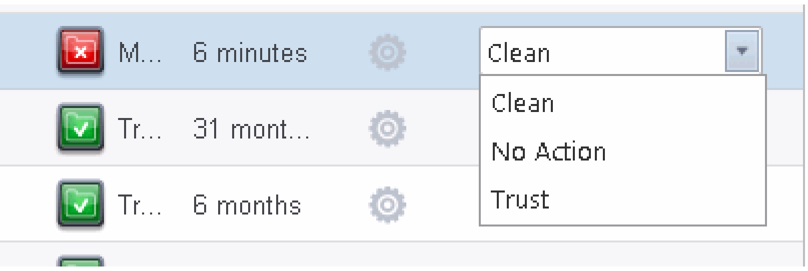
- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your server

- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous to your computer so we advise you clean or quarantine them immediately.

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

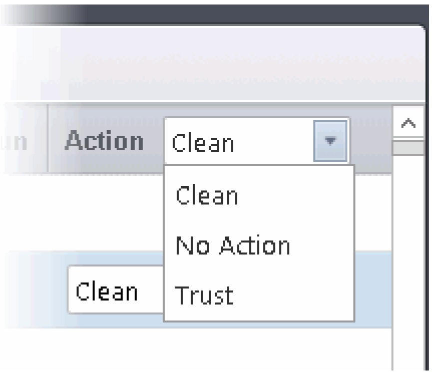


Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

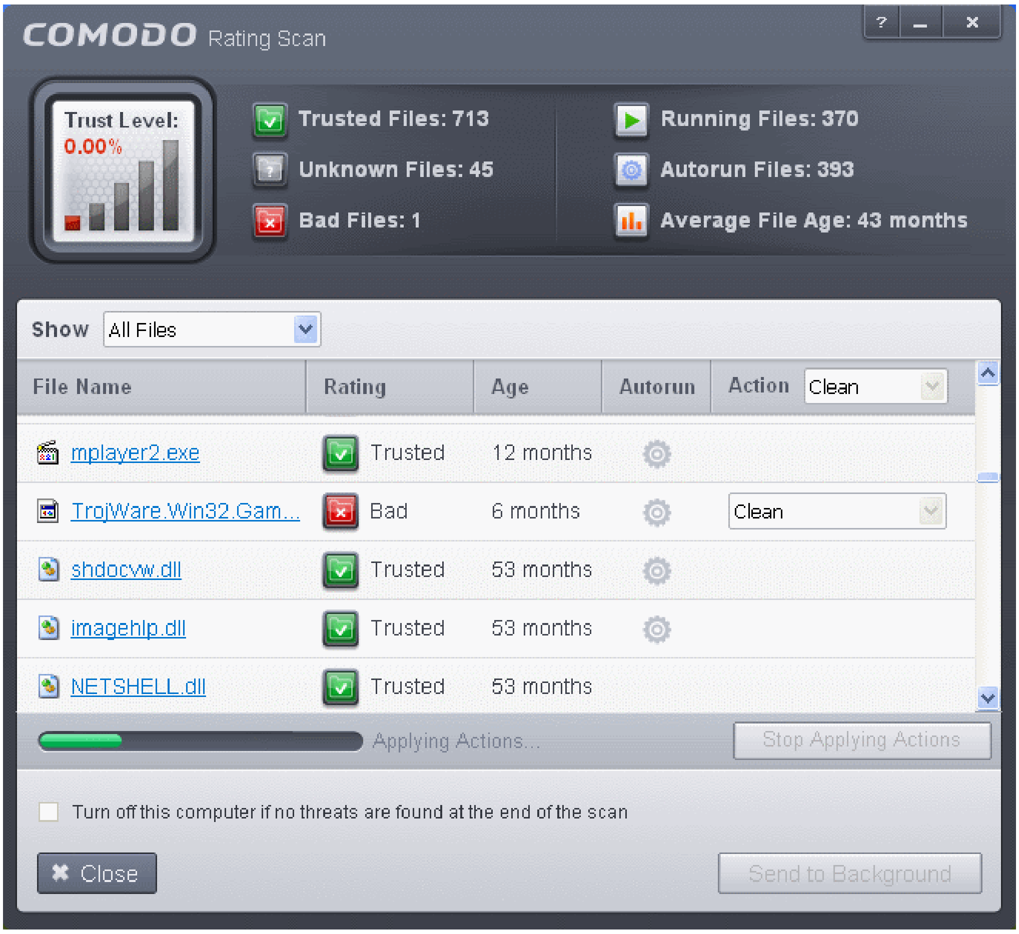


- **Clean -** If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See **Manage Quarantined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

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



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



Trusted Files: 713
Unknown Files: 45
Bad Files: 1
Running Files: 370
Autorun Files: 393
Average File Age: 43 months

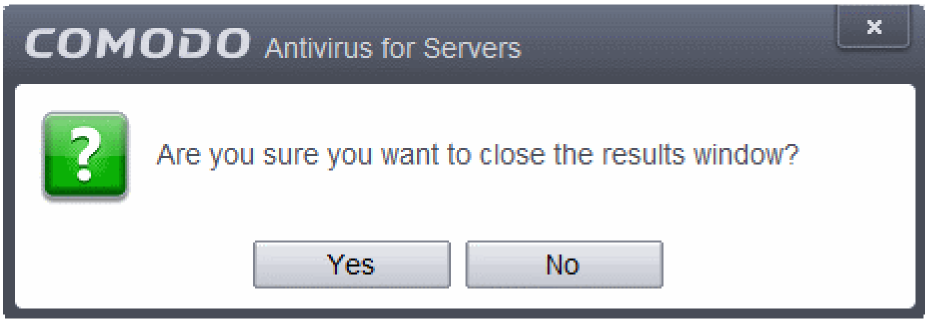
Show: All Files

File Name	Rating	Age	Autorun	Action: Clean
mplayer2.exe	✓ Trusted	12 months	⚙	
TrojWare.Win32.Gam...	✗ Bad	6 months	⚙	Clean
shdocvw.dll	✓ Trusted	53 months	⚙	
imagehlp.dll	✓ Trusted	53 months	⚙	
NETSHELL.dll	✓ Trusted	53 months		

Applying Actions...

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

- Click 'Close' to exit



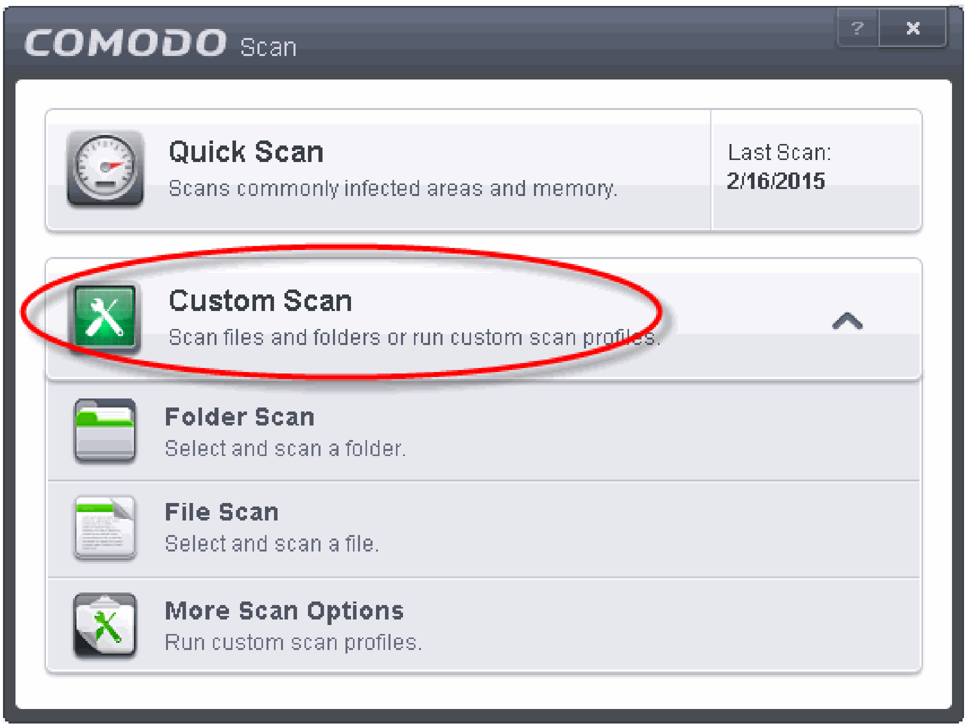
Are you sure you want to close the results window?

… then click 'Yes' in the confirmation window.

2.1.4. Run a Custom Scan

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

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


COMODO Scan
?
×
Quick Scan
Scans commonly infected areas and memory.
Last Scan:
2/16/2015
Custom Scan
Scan files and folders or run custom scan profiles.
Folder Scan
Select and scan a folder.
File Scan
Select and scan a file.
More Scan Options
Run custom scan profiles.

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

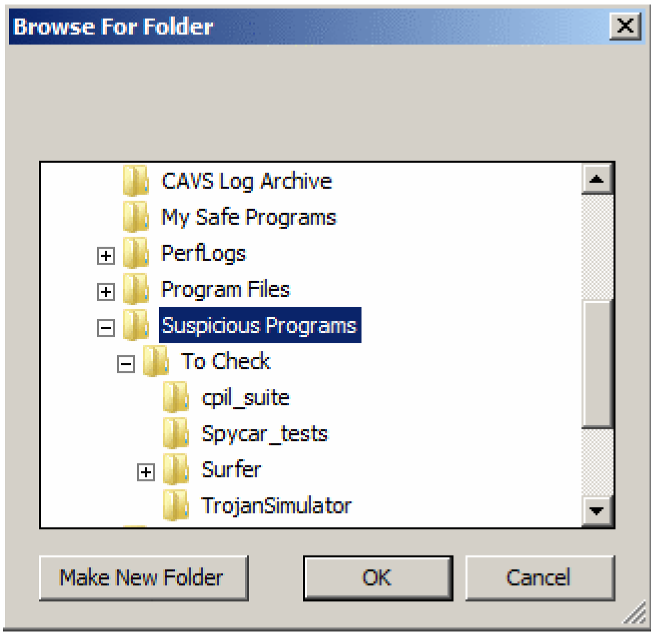
- **Folder Scan** - scan individual folders
- **File Scan** - scan an individual file
- **More Scan Options** - create a custom scan profile here

2.1.4.1. Scan a Folder

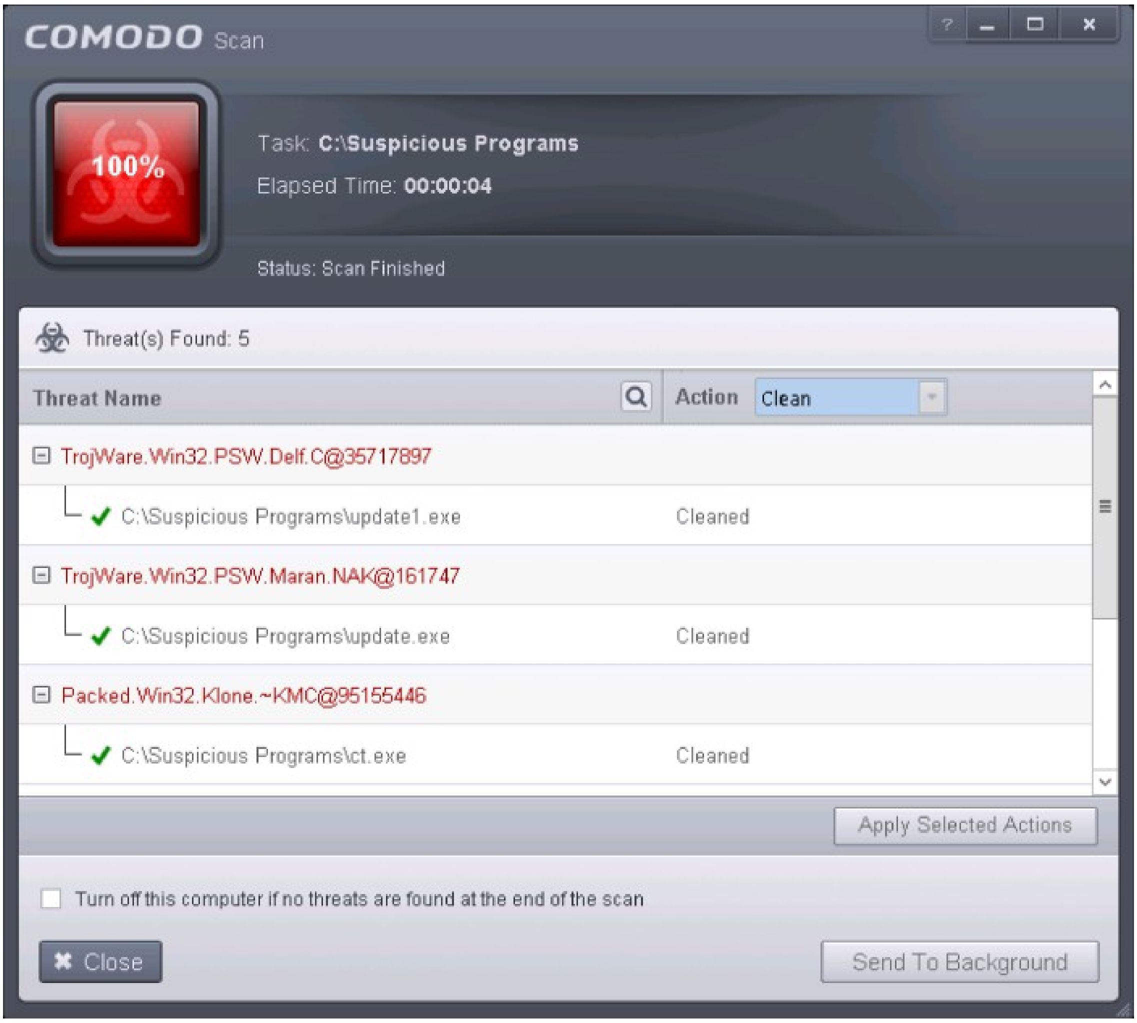
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your server. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan it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

To scan a specific folder

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



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



COMODO Scan

100%

Task: **C:\Suspicious Programs**

Elapsed Time: **00:00:04**

Status: Scan Finished

Threat(s) Found: 5

Threat Name	Action: Clean
TrojWare.Win32.PSW.Delf.C@35717897	
✓ C:\Suspicious Programs\update1.exe	Cleaned
TrojWare.Win32.PSW.Maran.NAK@161747	
✓ C:\Suspicious Programs\update.exe	Cleaned
Packed.Win32.Klone.~KMC@95155446	
✓ C:\Suspicious Programs\ct.exe	Cleaned

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

The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

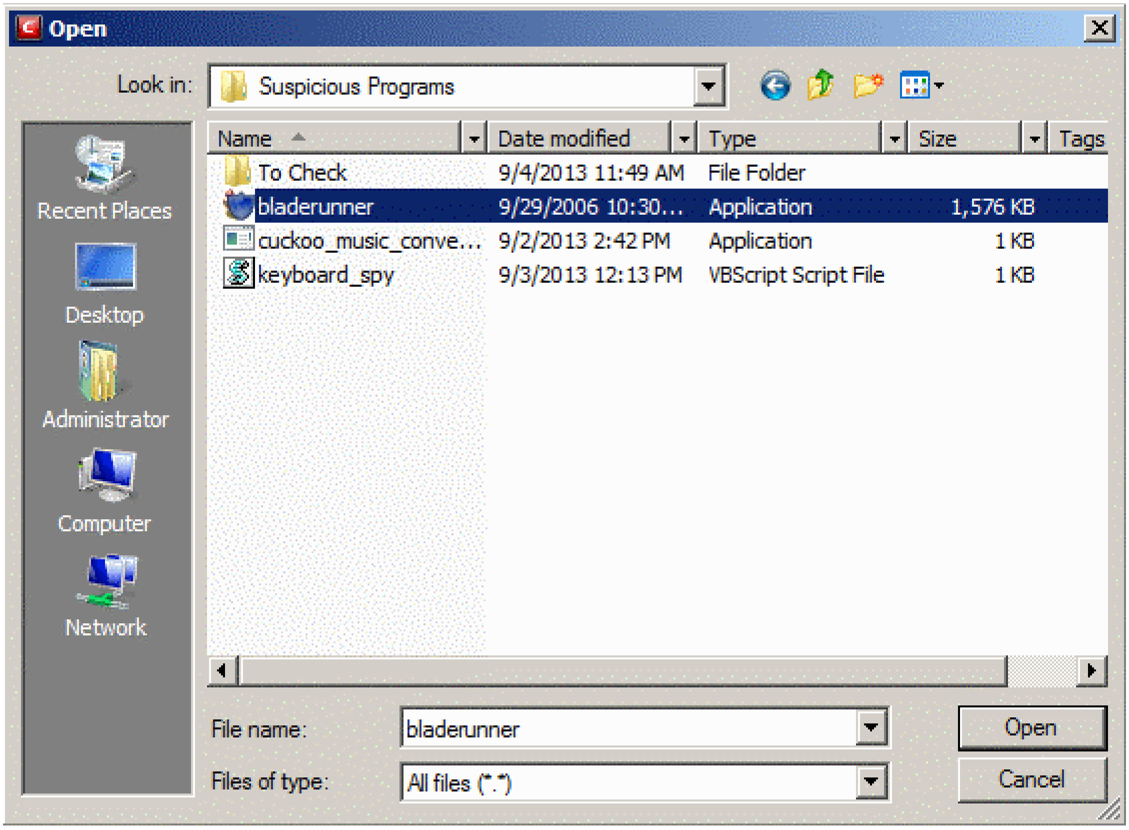
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CAVS interface or by right clicking it. Refer to **Scan Individual File/Folder** for more details.

2.1.4.2. Scan a File

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

To scan a specific file

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



Look in: Suspicious Programs

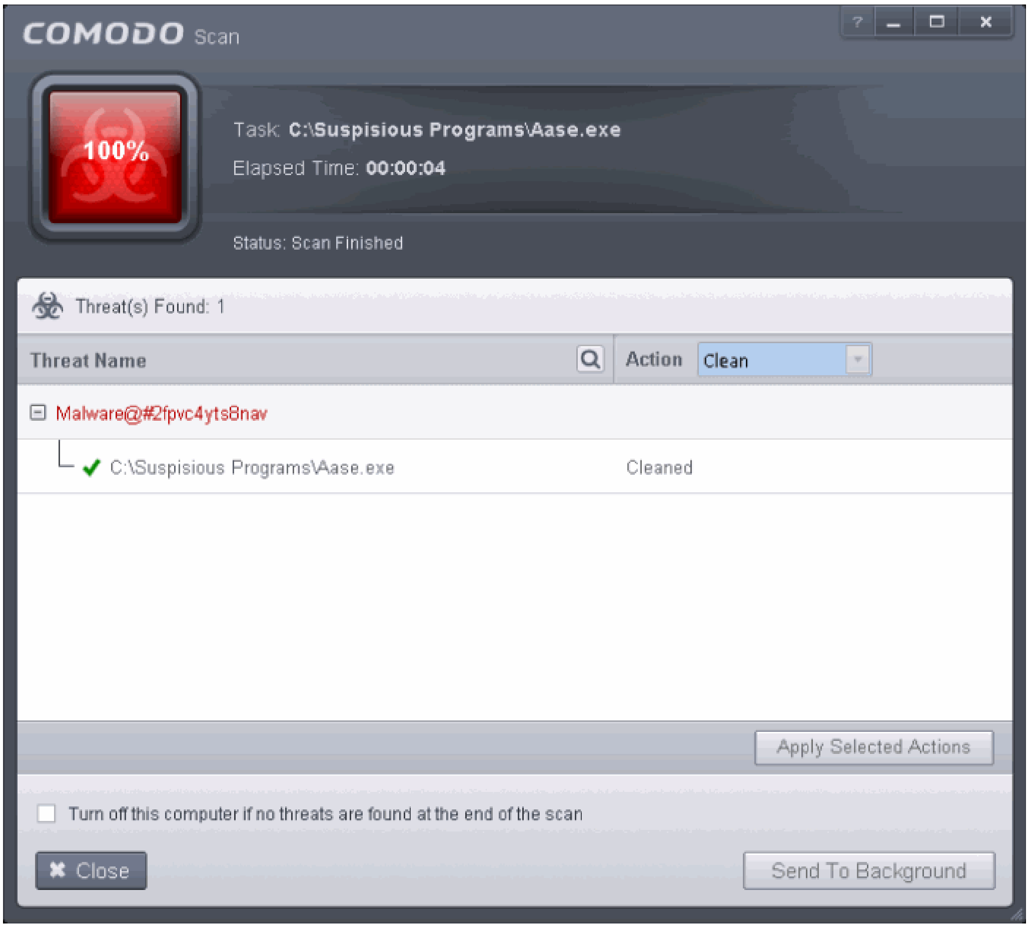
Name	Date modified	Type	Size	Tags
To Check	9/4/2013 11:49 AM	File Folder		
bladerunner	9/29/2006 10:30...	Application	1,576 KB	
cuckoo_music_conve...	9/2/2013 2:42 PM	Application	1 KB	
keyboard_spy	9/3/2013 12:13 PM	VBScript Script File	1 KB	

File name: bladerunner

Files of type: All files (*.*)

The file will be scanned instantly.

- On completion of scanning, the scan results screen will be displayed.



The scan results window will display any threats discovered during the scans (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

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

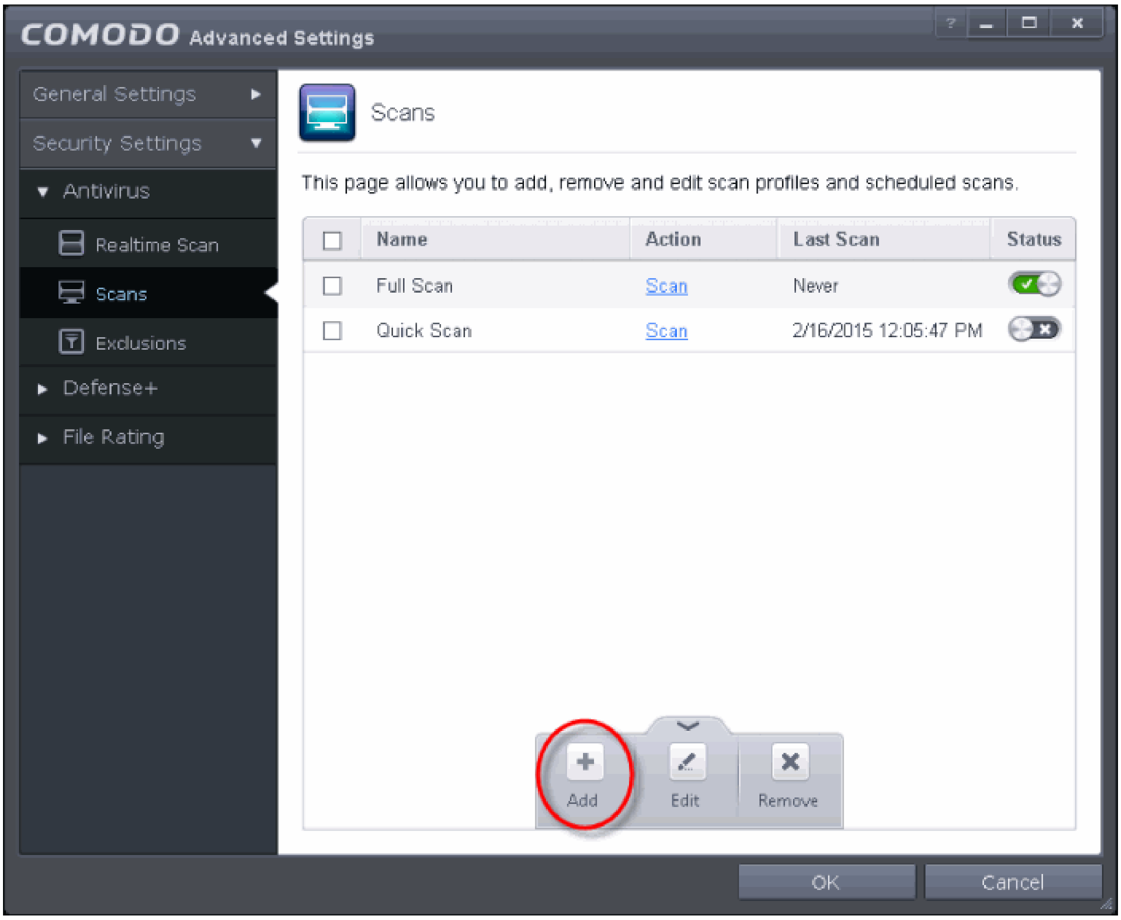
2.1.4.3. Create, Schedule and Run a Custom Scan

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

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

To create a custom profile

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

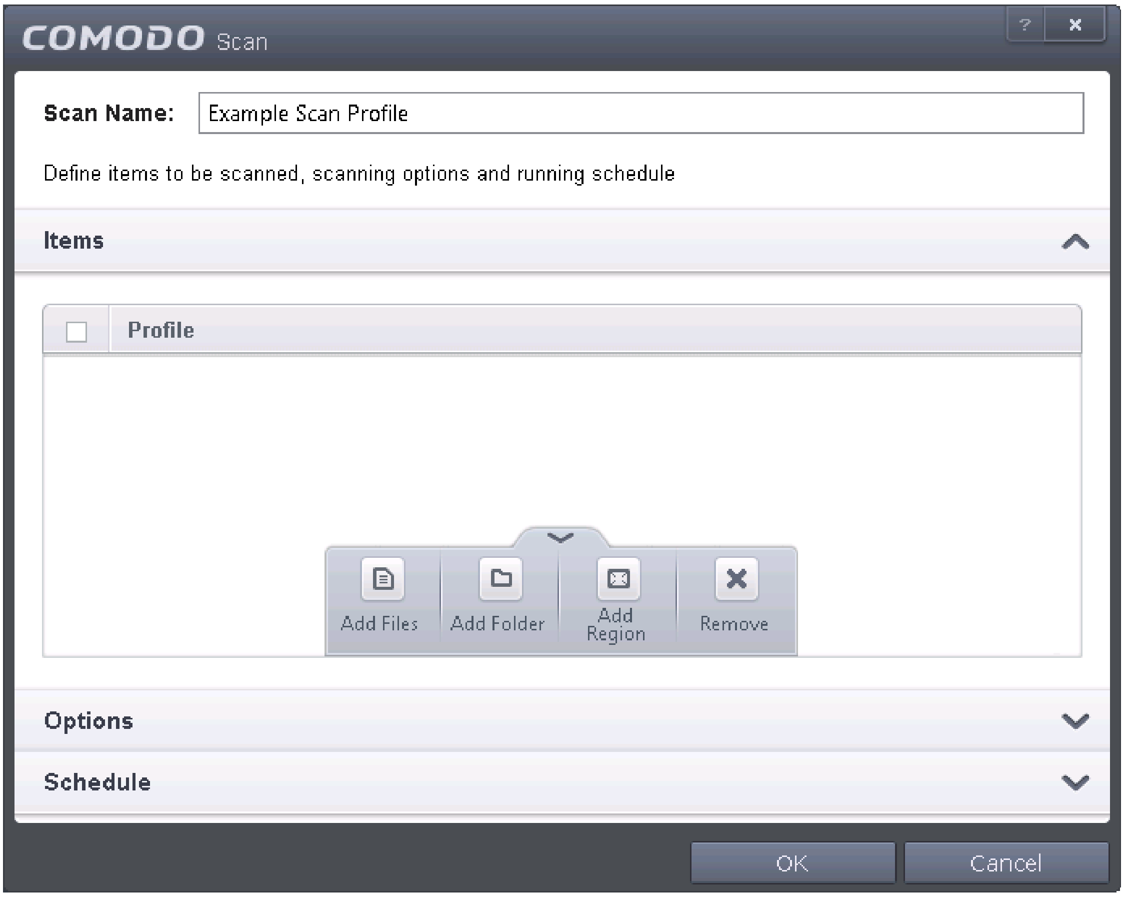


This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗

The scan profile interface will be displayed.

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



COMODO Scan

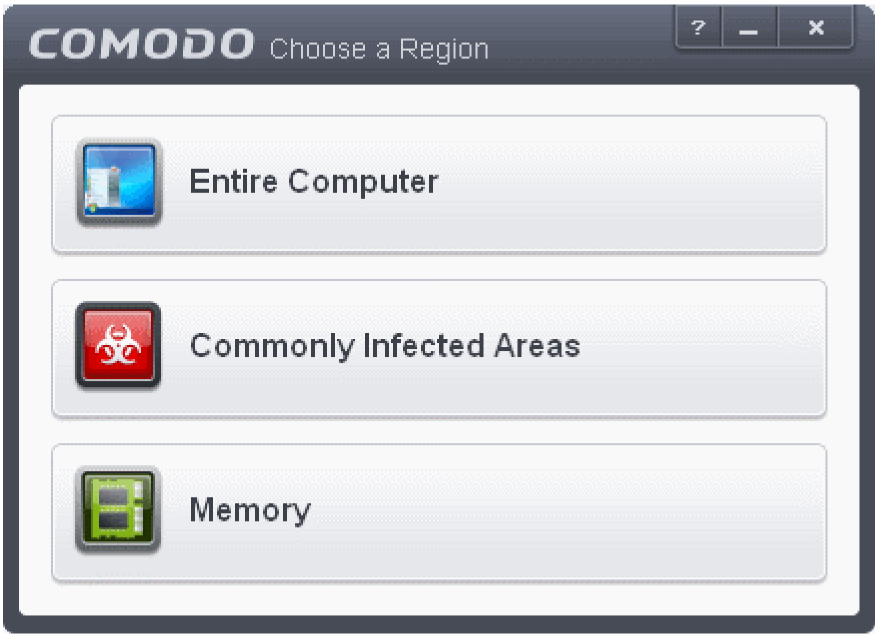
Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Items

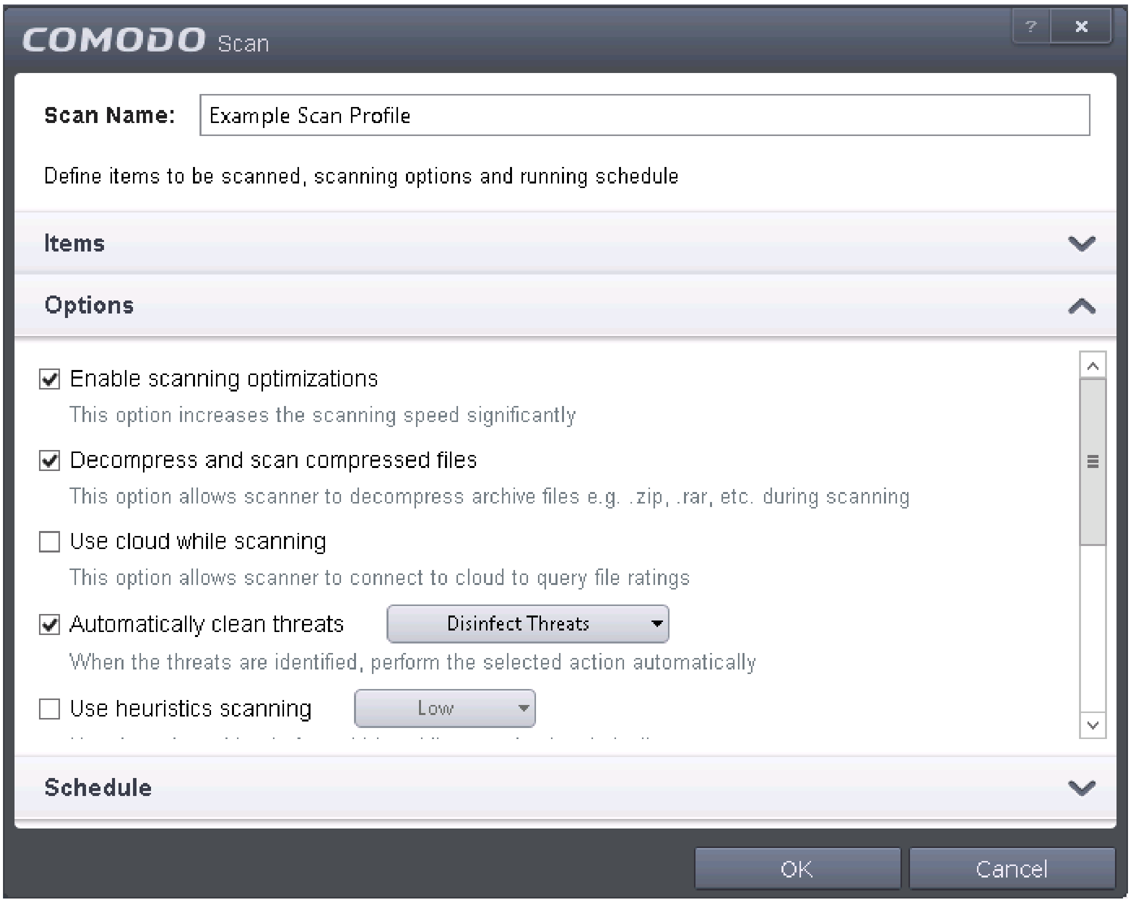
□ Profile

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



COMODO Choose a Region

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



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

☑ Enable scanning optimizations
This option increases the scanning speed significantly

☑ Decompress and scan compressed files
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

☐ Use cloud while scanning
This option allows scanner to connect to cloud to query file ratings

☑ Automatically clean threats: Disinfect Threats
When the threats are identified, perform the selected action automatically

☐ Use heuristics scanning: Low

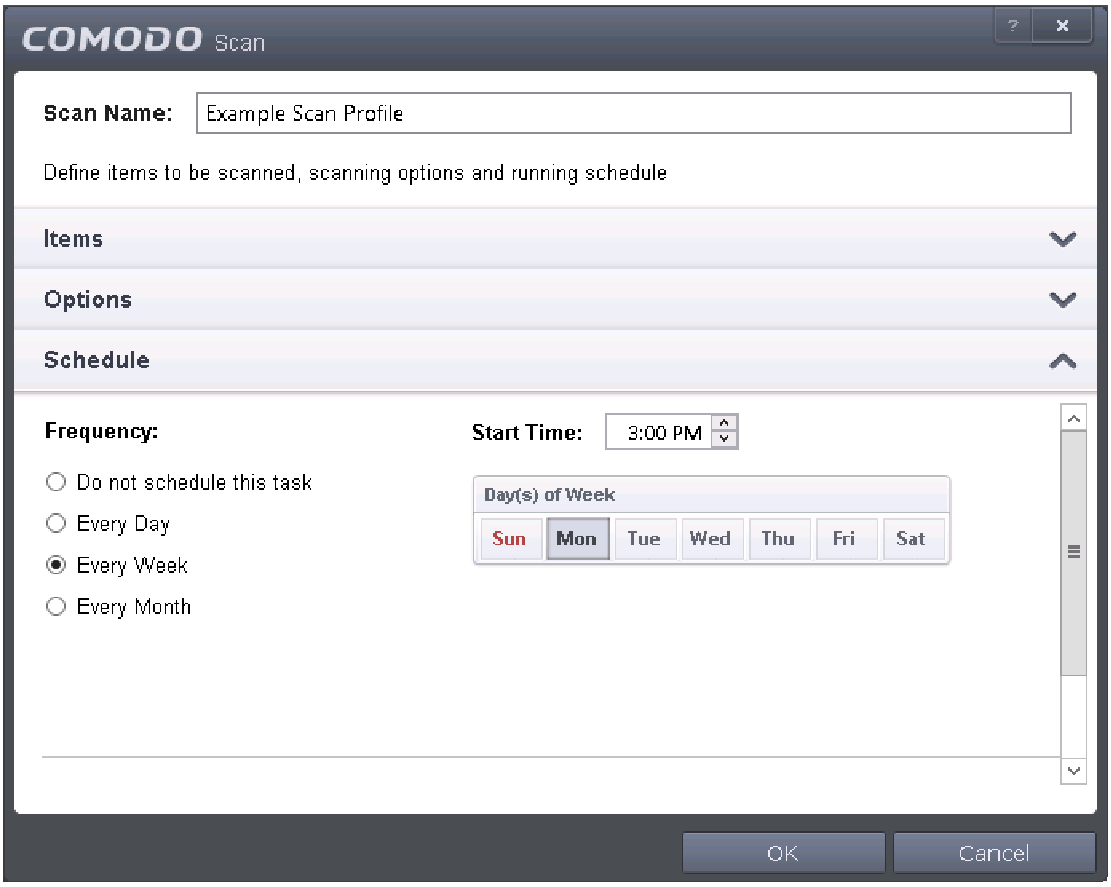
- **Options:**
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)*** .
  - **Decompress and scan compressed files** - When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

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

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

  - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run this scan with** - Enables you to set the priority of the scan profile. You can select the priority from the drop-down.(***Default = Disabled***).
- **Update virus database before running** - Instructs CAVS to check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning (***Default = Enabled***).
- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet (***Default = Disabled***).

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



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Frequency:

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

Start Time: 3:00 PM

Day(s) of Week

Sun	Mon	Tue	Wed	Thu	Fri	Sat

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

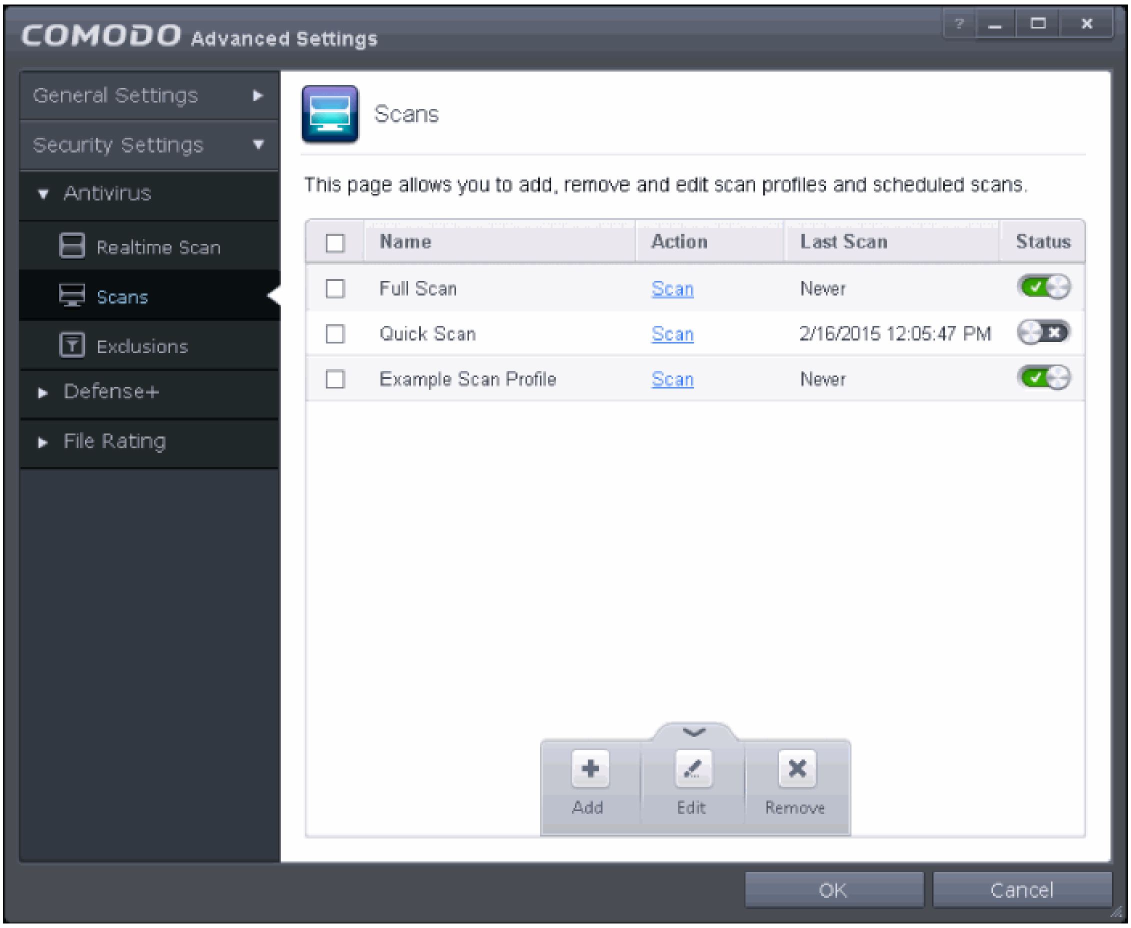
time specified in the Start Time field

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

- Click OK to save the profile.

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

The profile will be available for deployment in future.



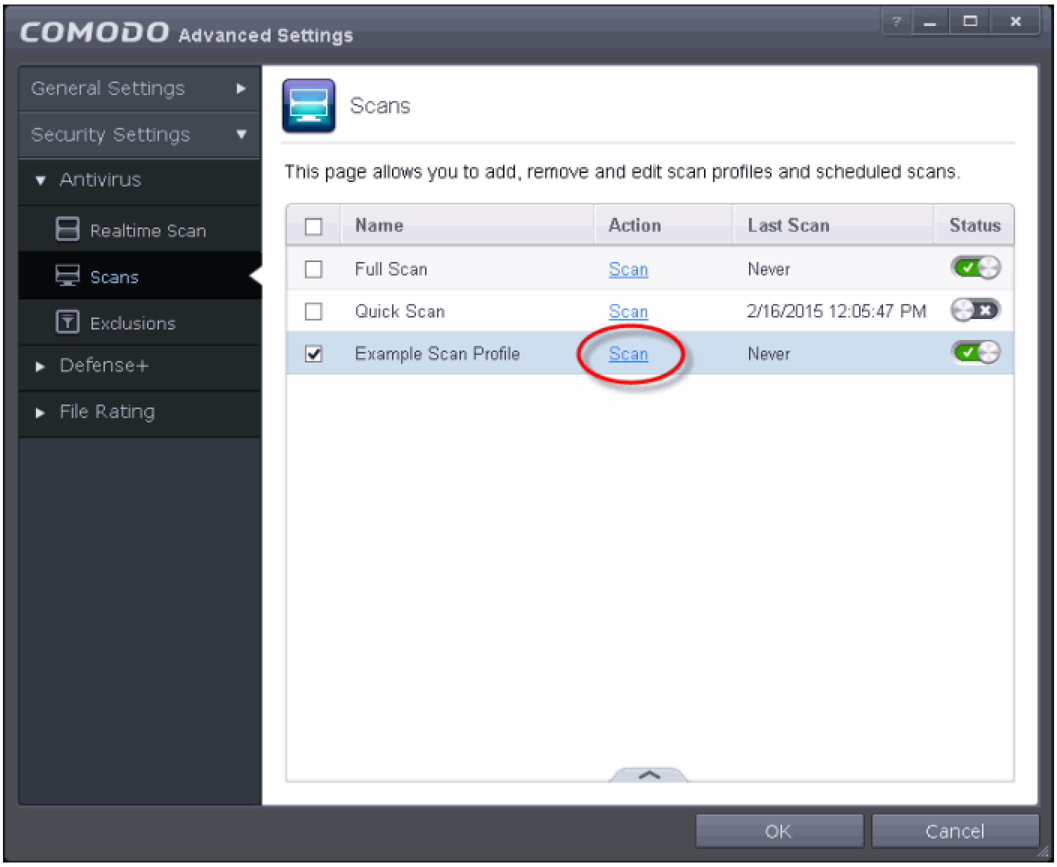
This page allows you to add, remove and edit scan profiles and scheduled scans.

☐	Name	Action	Last Scan	Status
☐	Full Scan	Scan	Never	✓
☐	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗
☐	Example Scan Profile	Scan	Never	✓

To run a custom scan

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

- Click 'Scan' beside the required scan profile.

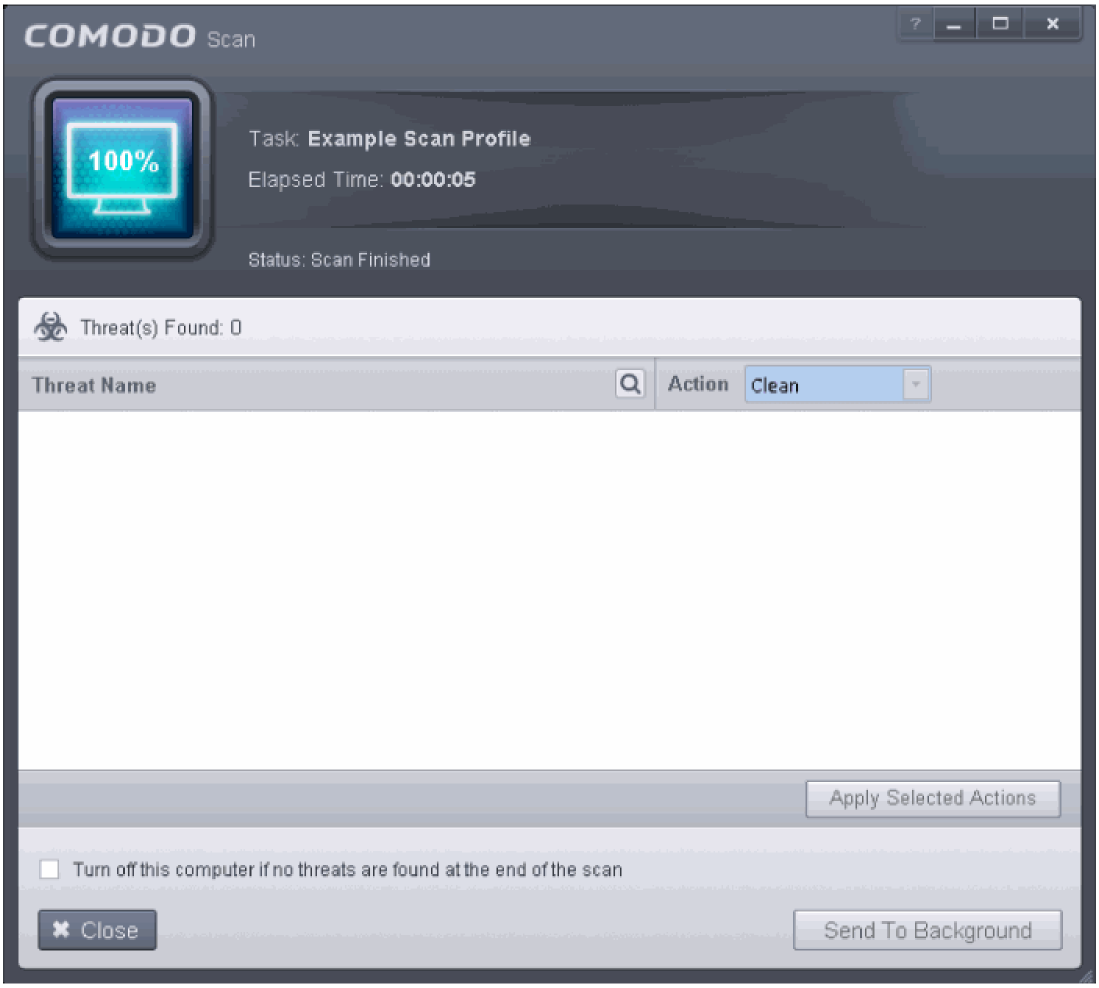


Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗
☑	Example Scan Profile	Scan	Never	✓

- The scan will be started.
- On completion of scanning, the scan results screen will be displayed.



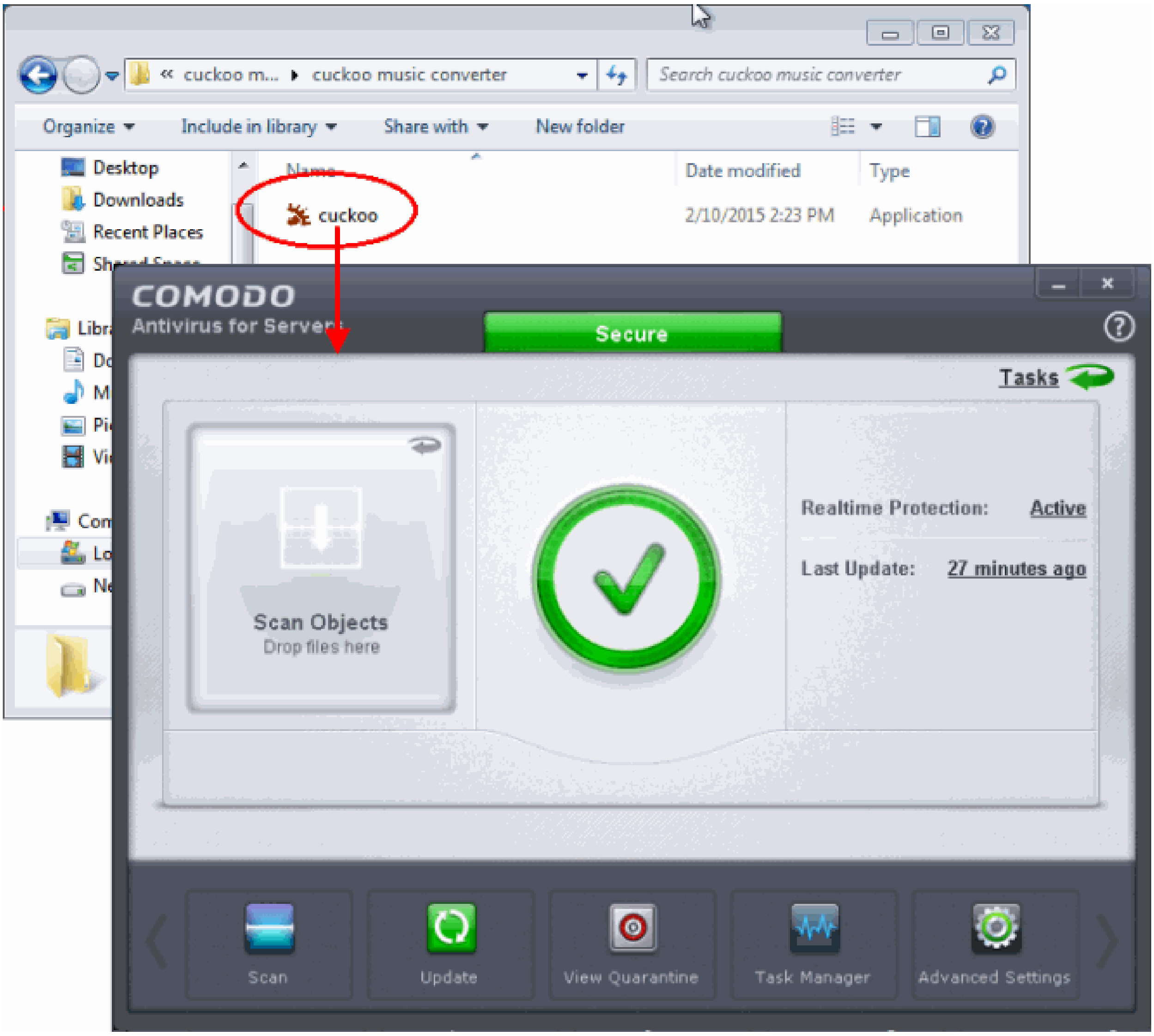
- The scan results window will display any threats discovered during the scans (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

2.2. Instantly Scan Files and Folders

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

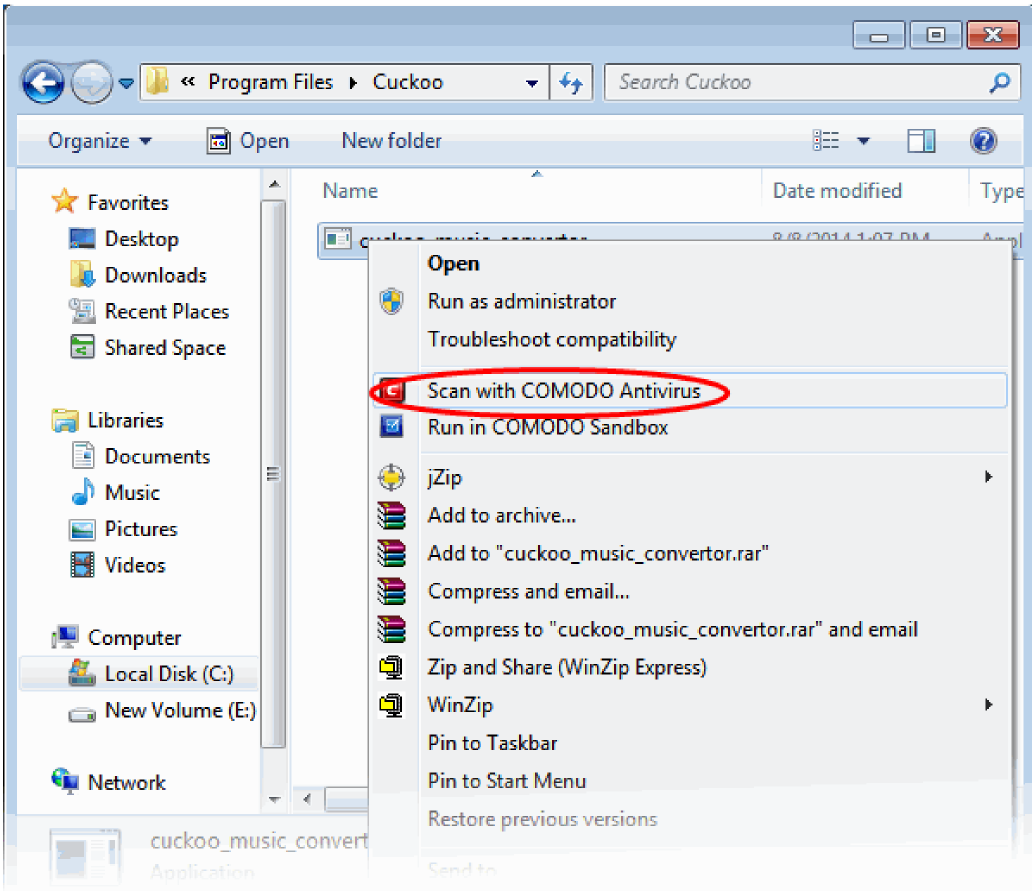
To instantly scan an item

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

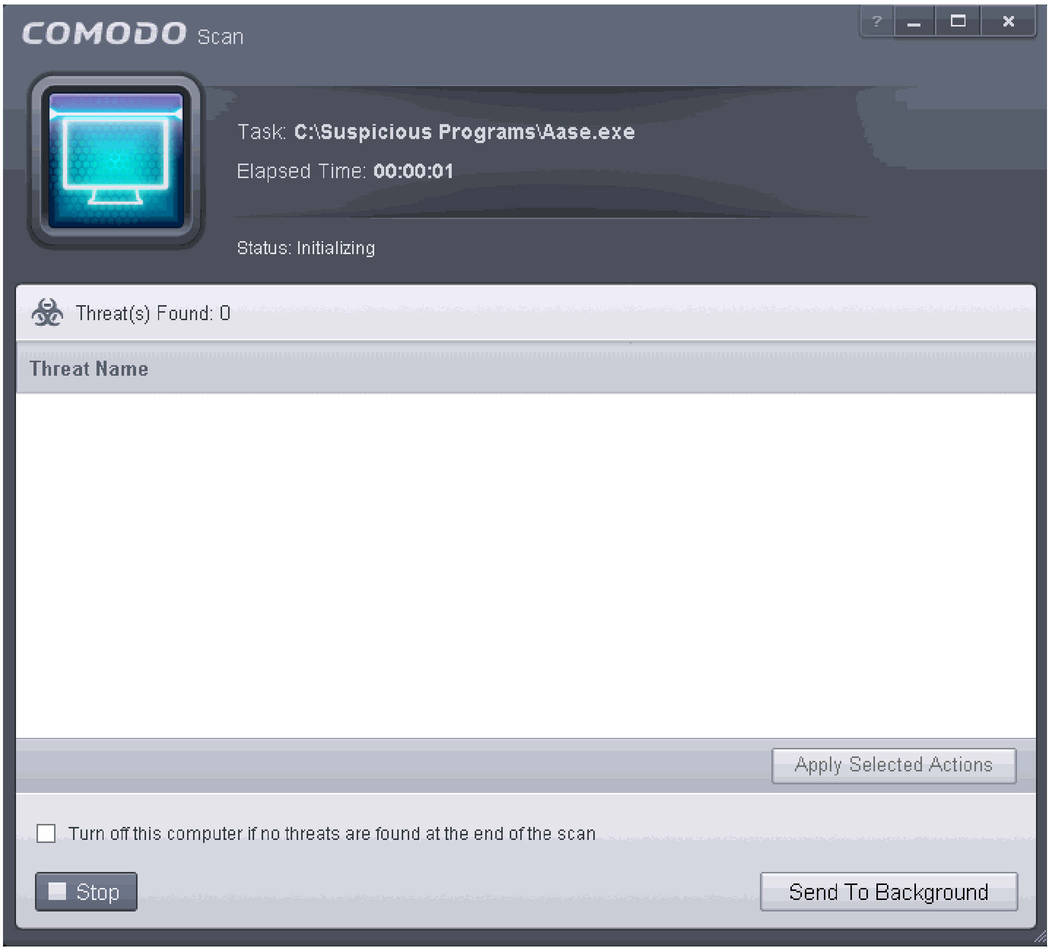


OR

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



The item will be scanned immediately.



Task: C:\Suspicious Programs\Aase.exe

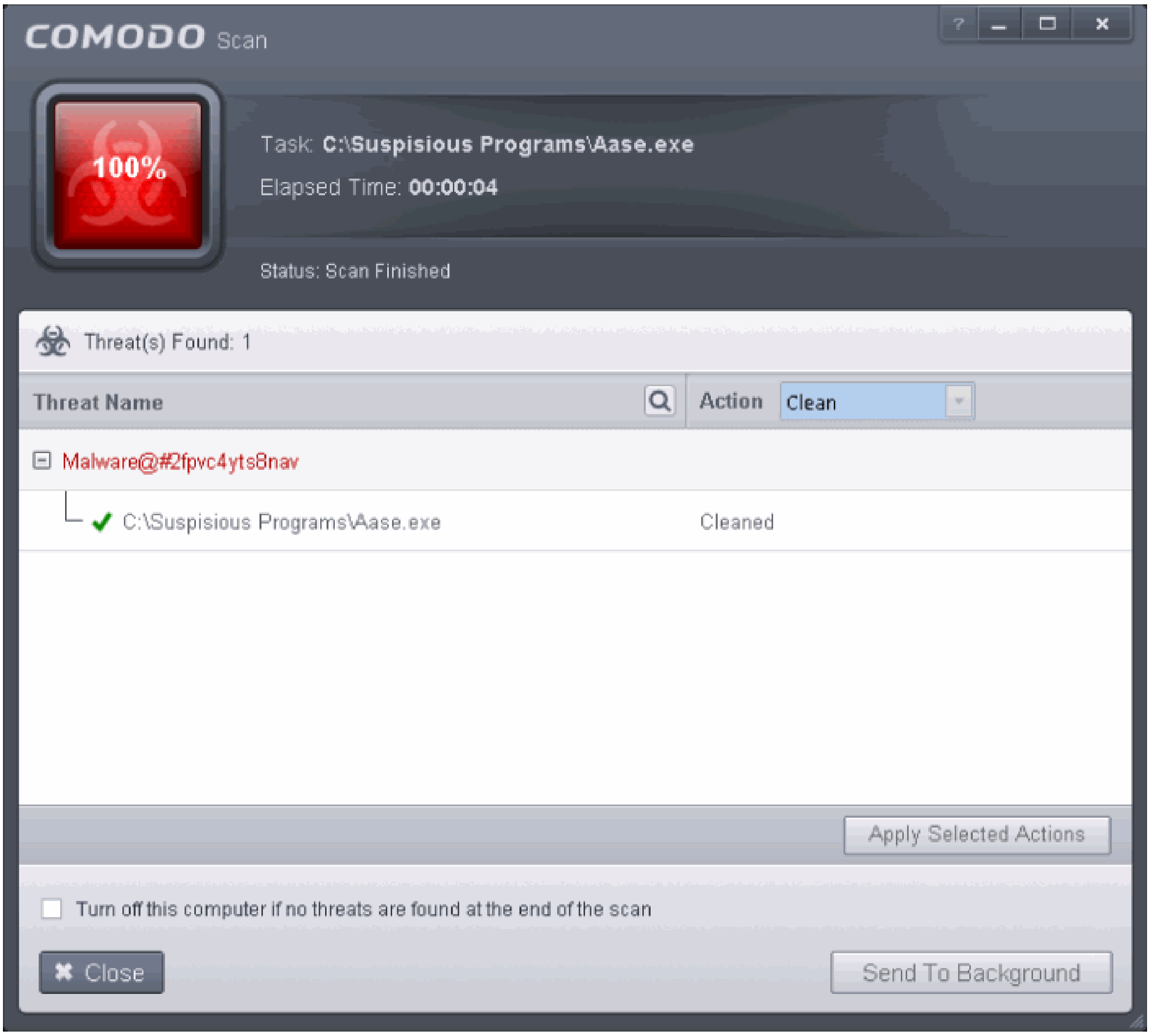
Elapsed Time: 00:00:01

Status: Initializing

Threat(s) Found: 0

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

On completion of scanning, the scan results screen will be displayed.



Task: C:\Suspisious Programs\Aase.exe

Elapsed Time: 00:00:04

Status: Scan Finished

Threat(s) Found: 1

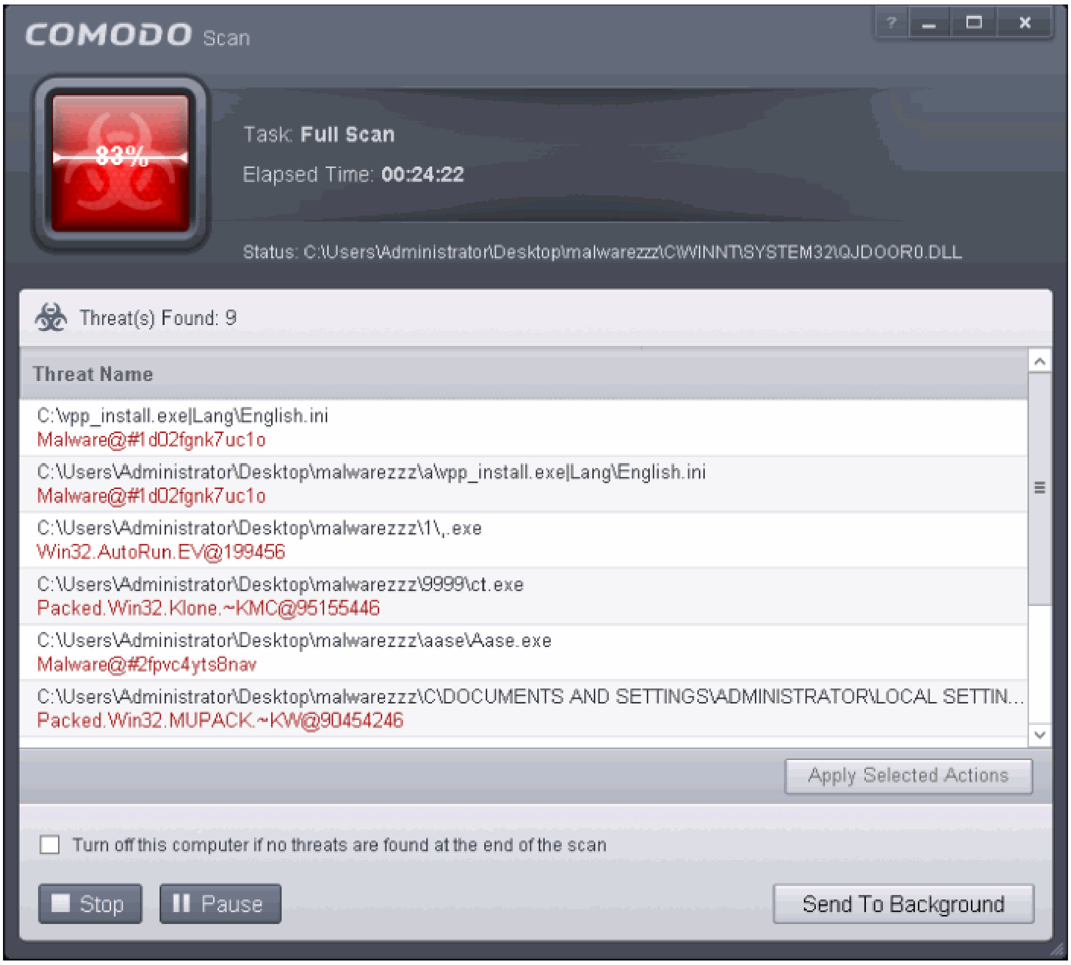
Threat Name	Action: Clean
⊟ Malware@#2fpvc4yts8nav	
✓ C:\Suspisious Programs\Aase.exe	Cleaned

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

The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

2.3. Processing Infected Files

On completion of any on-demand or scheduled scanning, the scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



Task: **Full Scan**

Elapsed Time: **00:24:22**

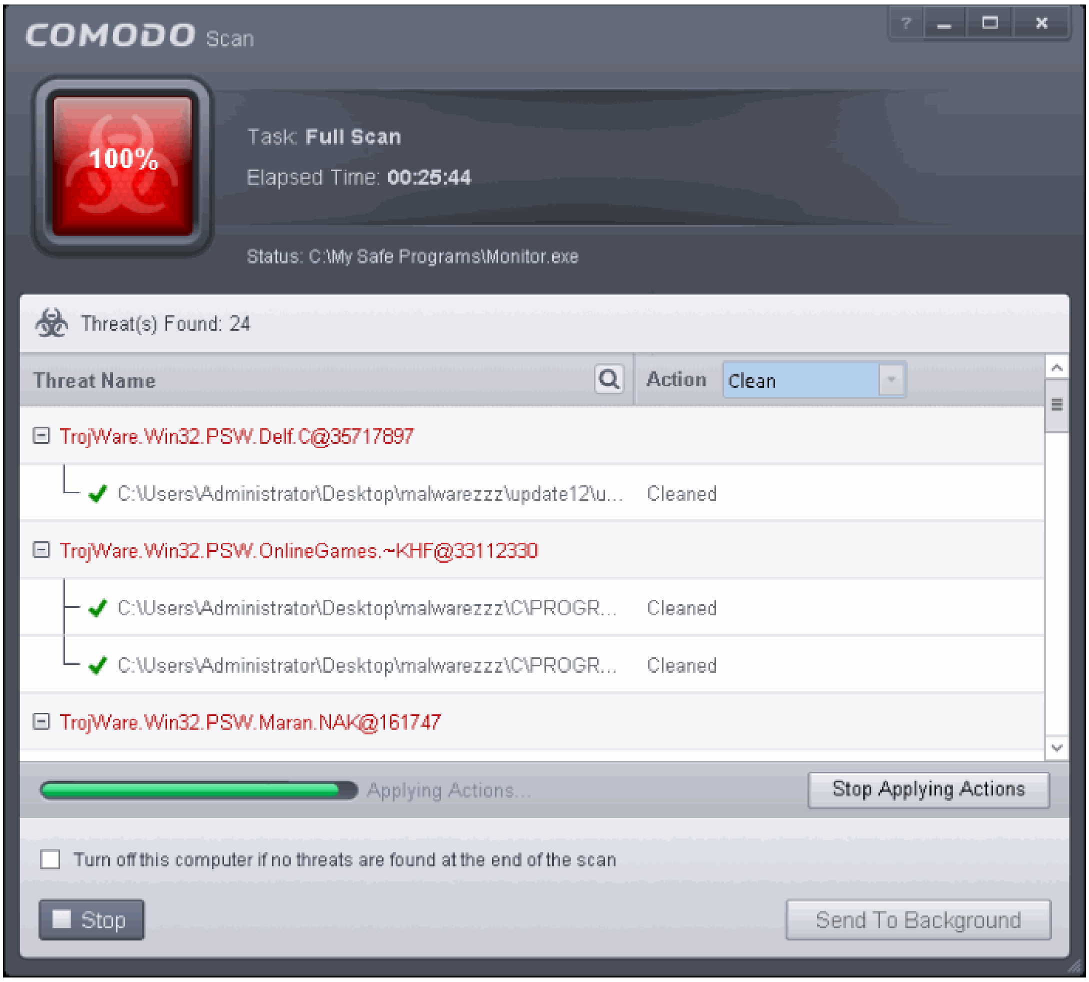
Status: C:\Users\Administrator\Desktop\malwarezzz\C\WINNT\SYSTEM32\QJDOOR0.DLL

Threat(s) Found: 9

Threat Name
C:\wpp_install.exe|Lang\English.ini Malware@#1d02fgnk7uc1o
C:\Users\Administrator\Desktop\malwarezzz\a\wpp_install.exe|Lang\English.ini Malware@#1d02fgnk7uc1o
C:\Users\Administrator\Desktop\malwarezzz\1\,.exe Win32.AutoRun.EV@199456
C:\Users\Administrator\Desktop\malwarezzz\9999\ct.exe Packed.Win32.Klone.~KMC@95155446
C:\Users\Administrator\Desktop\malwarezzz\aase\Aase.exe Malware@#2fpvc4yts8nav
C:\Users\Administrator\Desktop\malwarezzz\C\DOCUMENTS AND SETTINGS\ADMINISTRATOR\LOCAL SETTIN... Packed.Win32.MUPACK.~KW@90454246

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

- The 'Clean' action to be taken on all the detected threats automatically.



Task: **Full Scan**

Elapsed Time: **00:25:44**

Status: C:\My Safe Programs\Monitor.exe

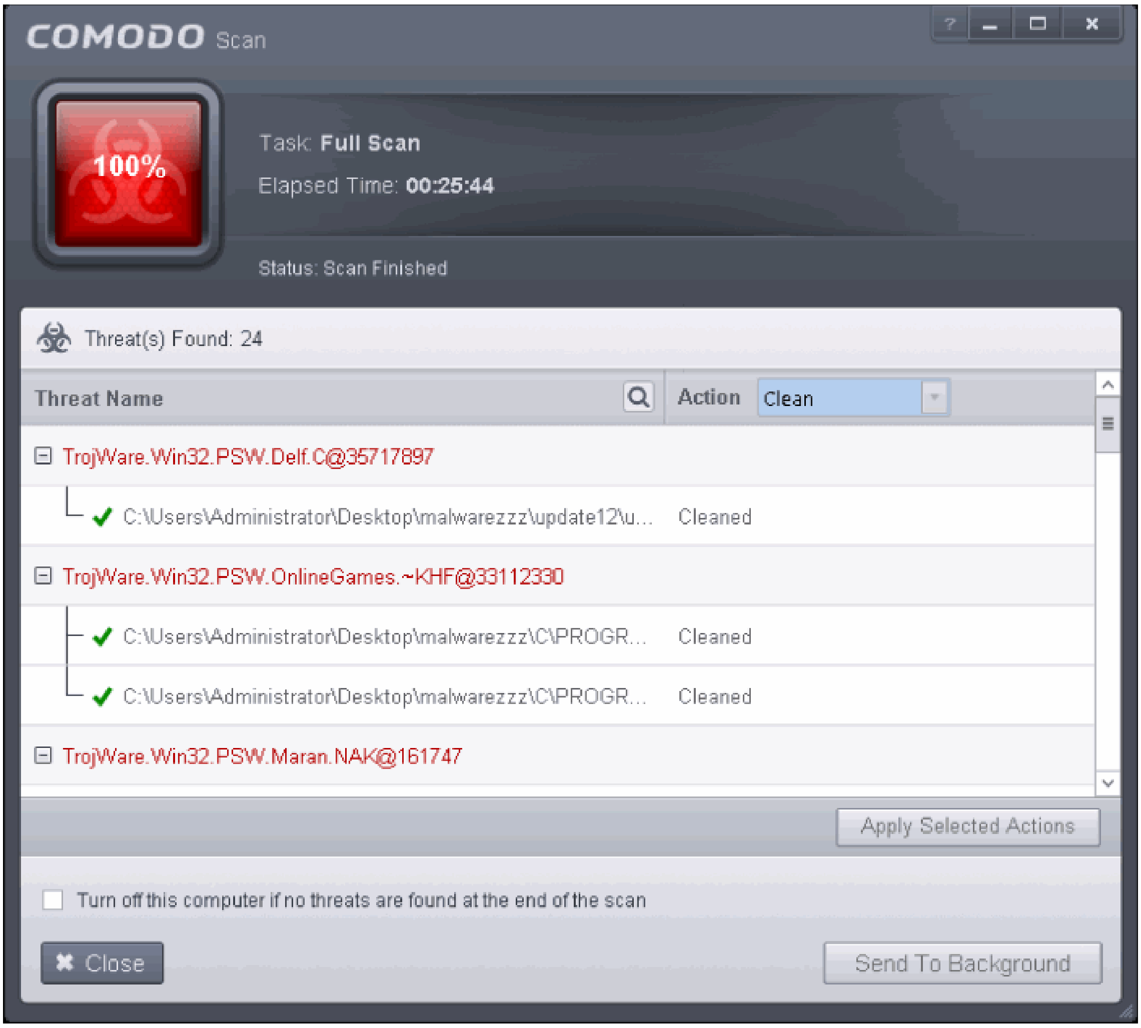
Threat(s) Found: 24

Threat Name	Action: Clean
⊟ TrojWare.Win32.PSW.Delf.C@35717897	
✓ C:\Users\Administrator\Desktop\malwarezzz\update12\u...	Cleaned
⊟ TrojWare.Win32.PSW.OnlineGames.~KHF@33112330	
✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...	Cleaned
✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...	Cleaned
⊟ TrojWare.Win32.PSW.Maran.NAK@161747	

Applying Actions...

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

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



Task: **Full Scan**

Elapsed Time: **00:25:44**

Status: Scan Finished

Threat(s) Found: 24

Threat Name	Action: Clean
⊟ TrojWare.Win32.PSW.Delf.C@35717897	
✓ C:\Users\Administrator\Desktop\malwarezzz\update12\u...	Cleaned
⊟ TrojWare.Win32.PSW.OnlineGames.~KHF@33112330	
✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...	Cleaned
✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...	Cleaned
⊟ TrojWare.Win32.PSW.Maran.NAK@161747	

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

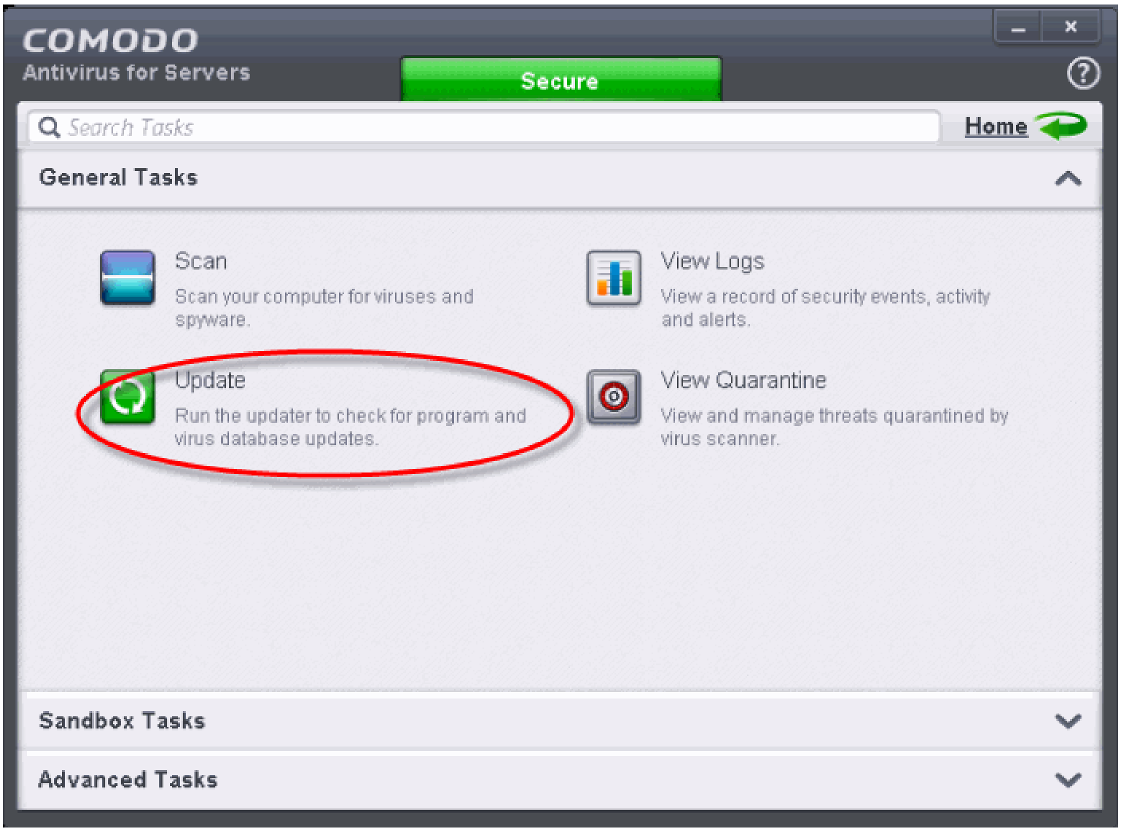
- Click 'Close' to close the results window.

2.4. Manage Virus Database and Program Updates

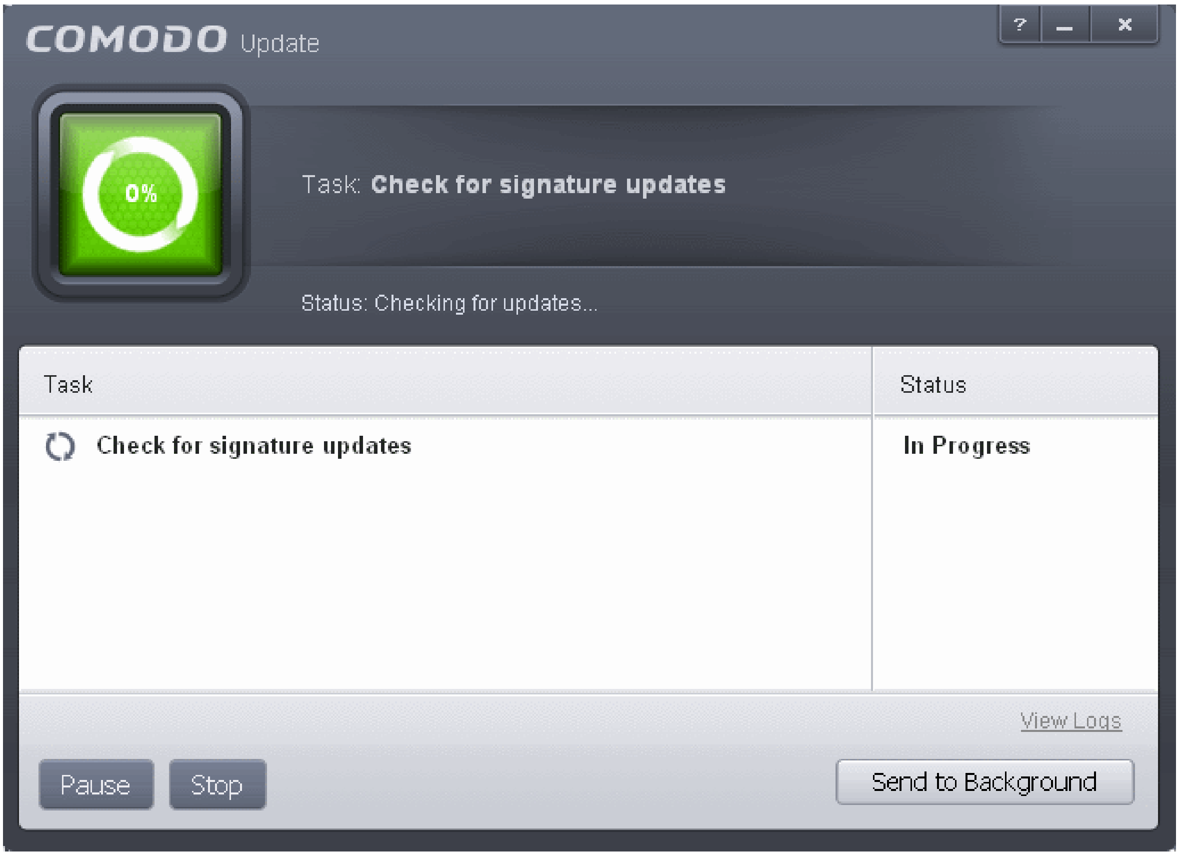
In order to guarantee continued and effective antivirus protection, it is imperative that your virus databases are updated as regularly as possible. Updates can be downloaded to your system **manually** or **automatically** from Comodo's update servers.

To manually check for the latest virus Database and program updates

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


COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Scan
Scan your computer for viruses and spyware.
View Logs
View a record of security events, activity and alerts.
Update
Run the updater to check for program and virus database updates.
View Quarantine
View and manage threats quarantined by virus scanner.
Sandbox Tasks
Advanced Tasks

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

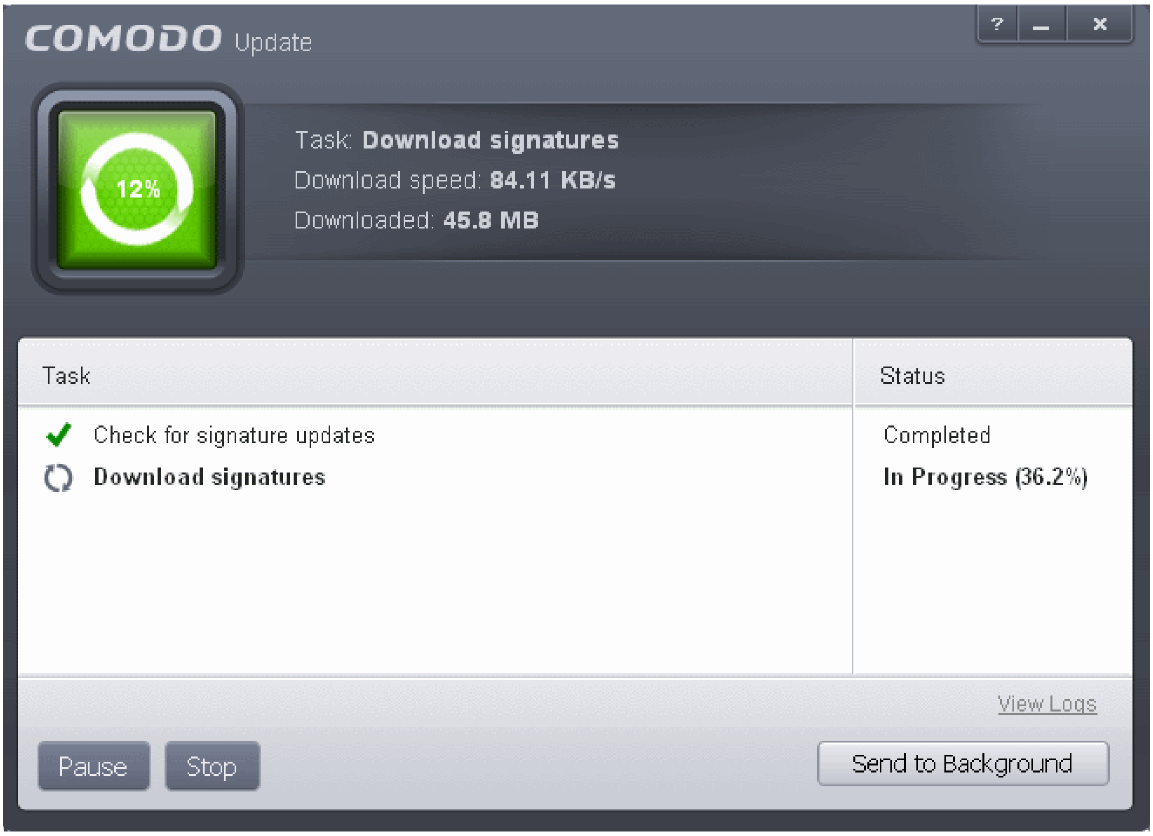


Task: **Check for signature updates**

Status: Checking for updates...

Task	Status
Check for signature updates	In Progress

If the updates are available, they will be downloaded.

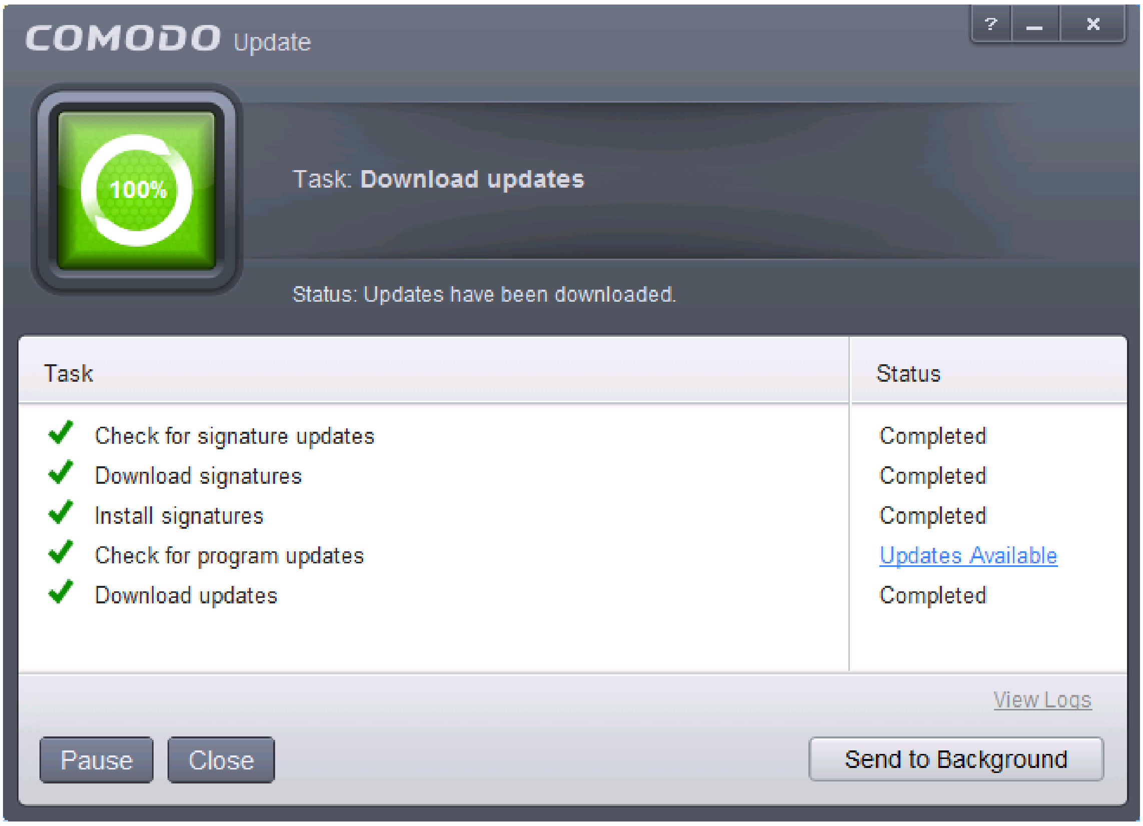


Task: **Download signatures**
Download speed: **84.11 KB/s**
Downloaded: **45.8 MB**

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

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

The virus signature database will be updated on completion.

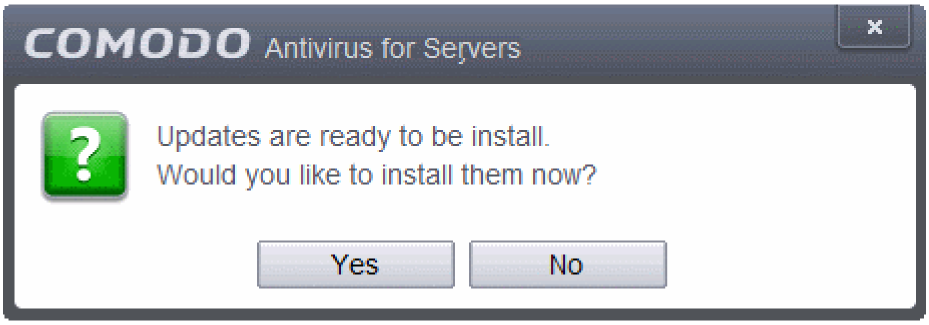


Task: **Download updates**

Status: Updates have been downloaded.

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

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



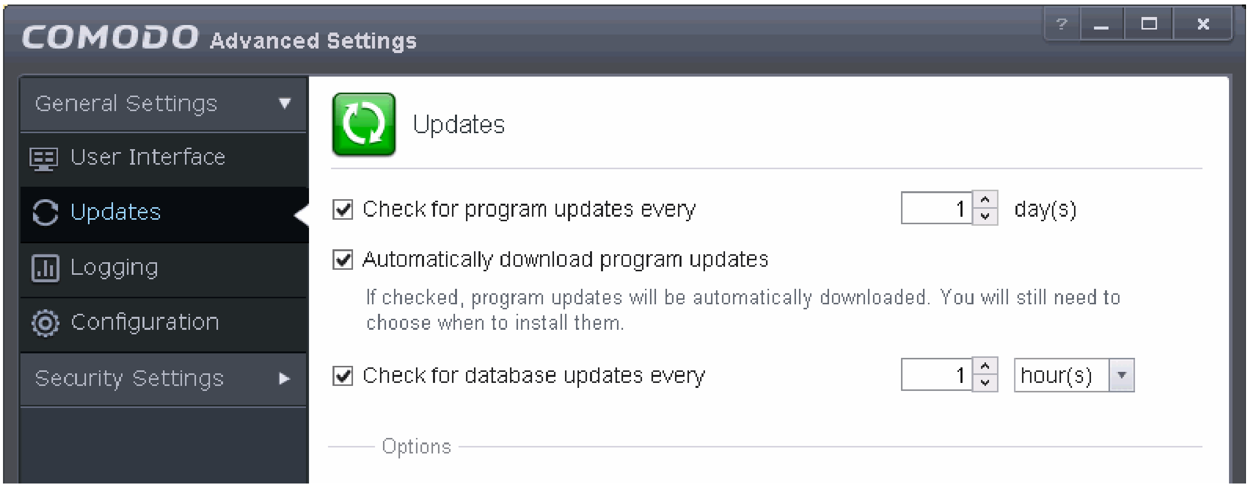
COMODO Antivirus for Servers

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

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

Automatic Updates

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



Updates

☑ Check for program updates every 1 day(s)

☑ Automatically download program updates

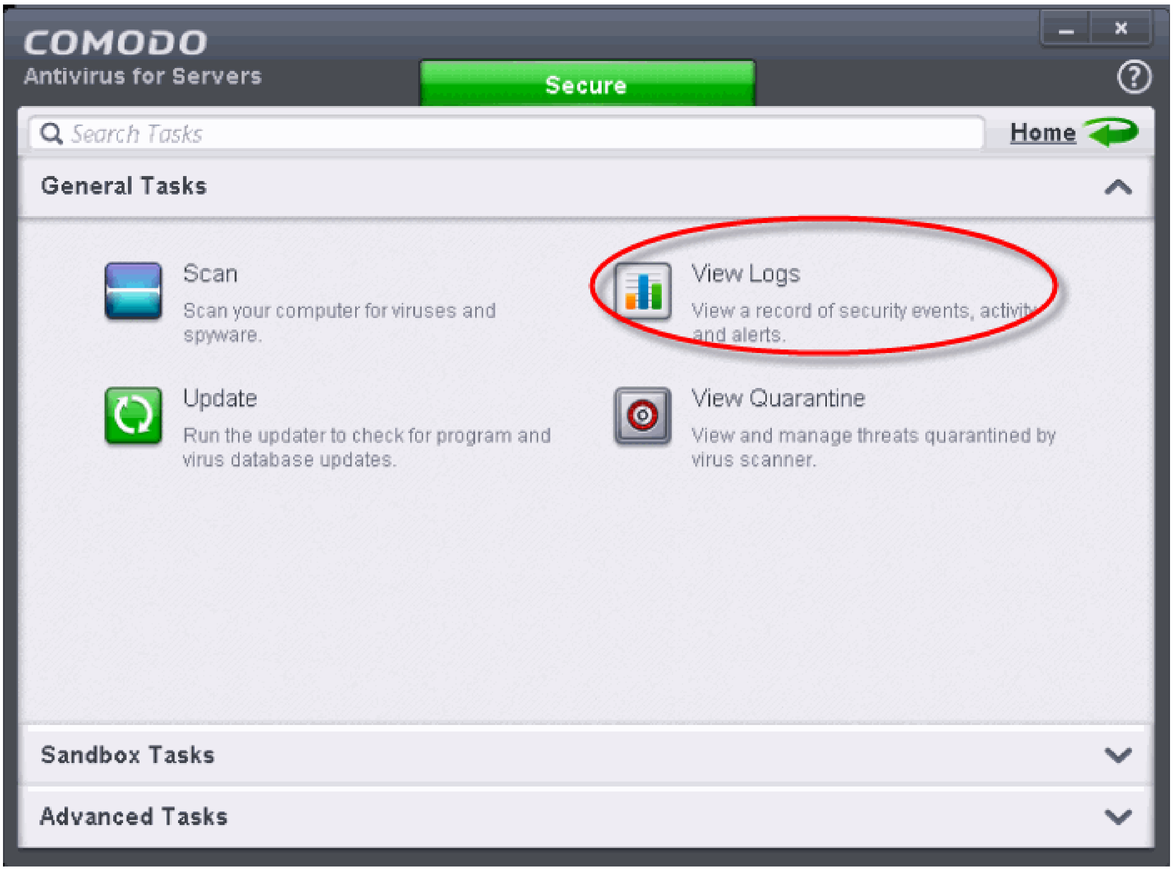
If checked, program updates will be automatically downloaded. You will still need to choose when to install them.

☑ Check for database updates every 1 hour(s)

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

2.5. View CAVS Logs

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



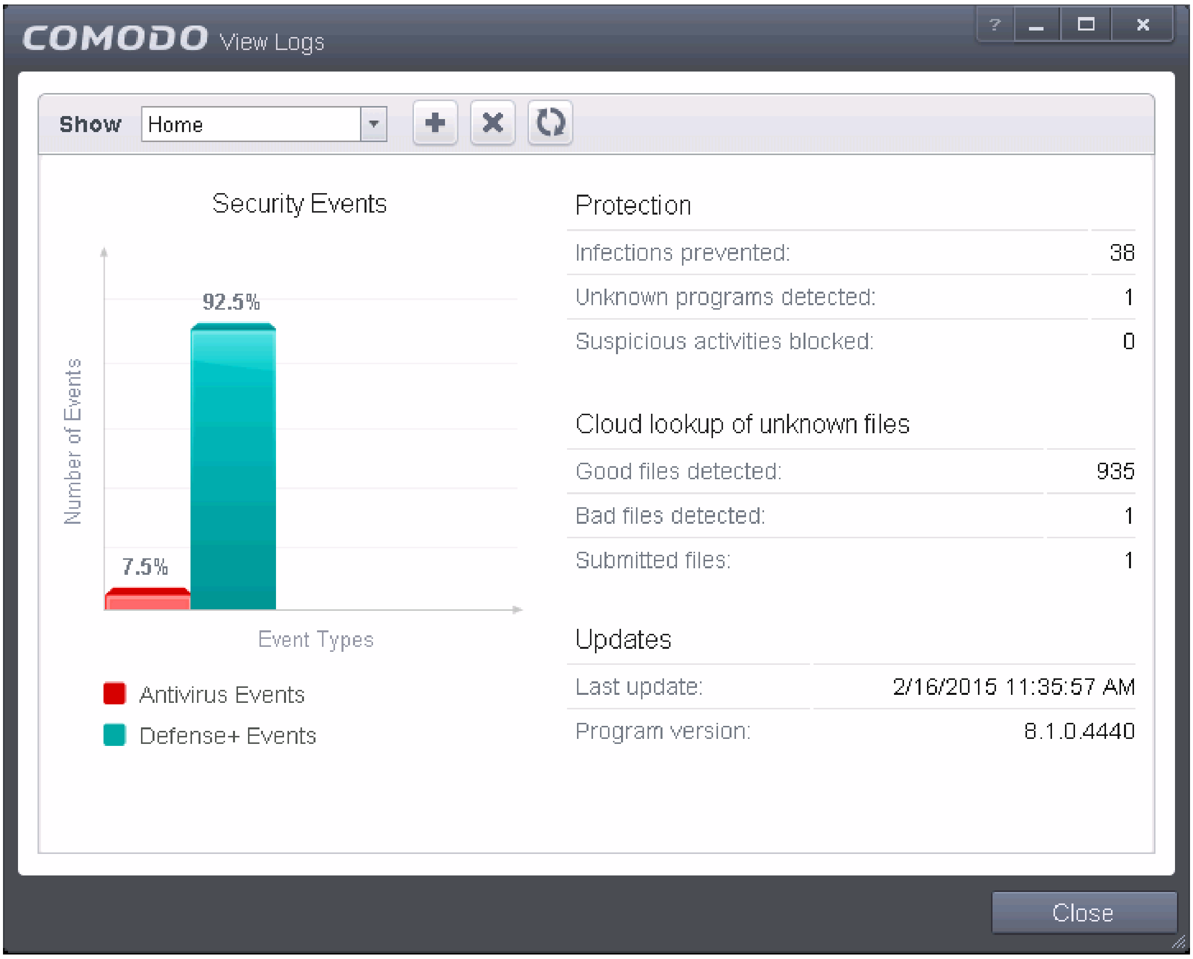
Scan
Scan your computer for viruses and spyware.

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

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

View Quarantine
View and manage threats quarantined by virus scanner.

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



Protection	
Infections prevented:	38
Unknown programs detected:	1
Suspicious activities blocked:	0

Cloud lookup of unknown files	
Good files detected:	935
Bad files detected:	1
Submitted files:	1

Updates	
Last update:	2/16/2015 11:35:57 AM
Program version:	8.1.0.4440

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

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

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

'Logs per Module':

- **Antivirus**
- **Defense+**

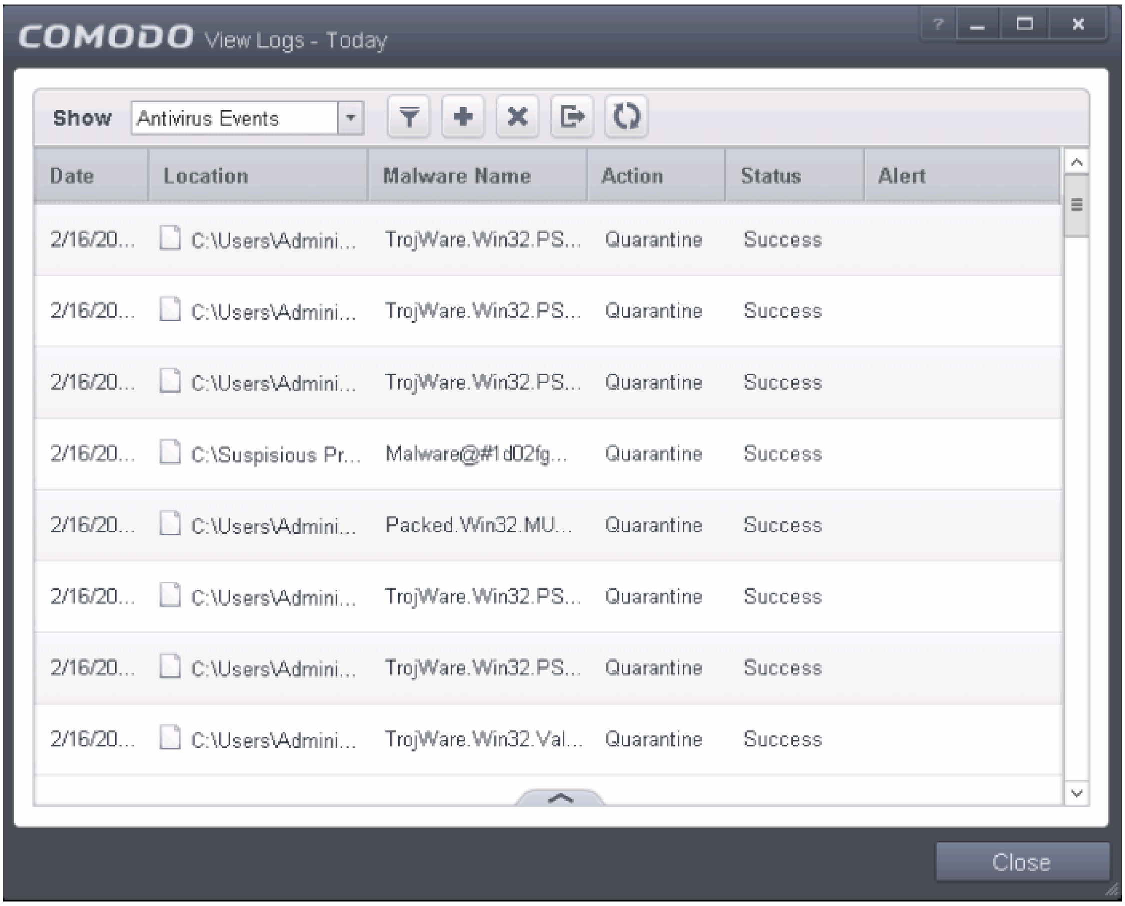
'Other Logs':

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

2.5.1. Antivirus Logs

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

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



Date	Location	Malware Name	Action	Status	Alert
2/16/20...	C:\Users\Admini...	TrojWare.Win32.PS...	Quarantine	Success	
2/16/20...	C:\Users\Admini...	TrojWare.Win32.PS...	Quarantine	Success	
2/16/20...	C:\Users\Admini...	TrojWare.Win32.PS...	Quarantine	Success	
2/16/20...	C:\Suspisious Pr...	Malware@#1d02fg...	Quarantine	Success	
2/16/20...	C:\Users\Admini...	Packed.Win32.MU...	Quarantine	Success	
2/16/20...	C:\Users\Admini...	TrojWare.Win32.PS...	Quarantine	Success	
2/16/20...	C:\Users\Admini...	TrojWare.Win32.PS...	Quarantine	Success	
2/16/20...	C:\Users\Admini...	TrojWare.Win32.Val...	Quarantine	Success	

Column Descriptions

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

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

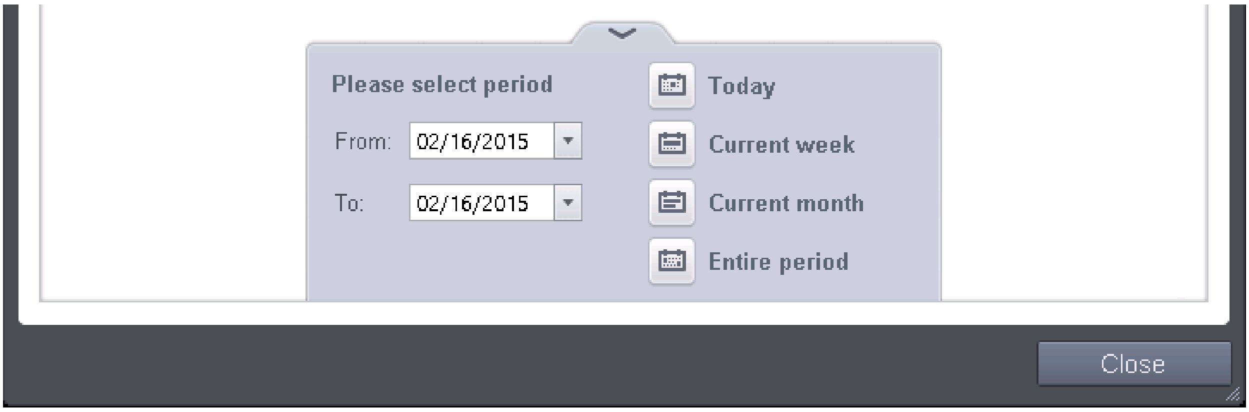
2.5.1.1. Filtering Antivirus Logs

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

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

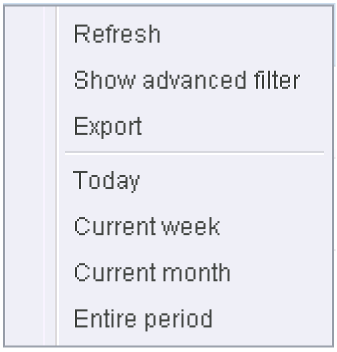
Preset Time Filters:

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



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

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



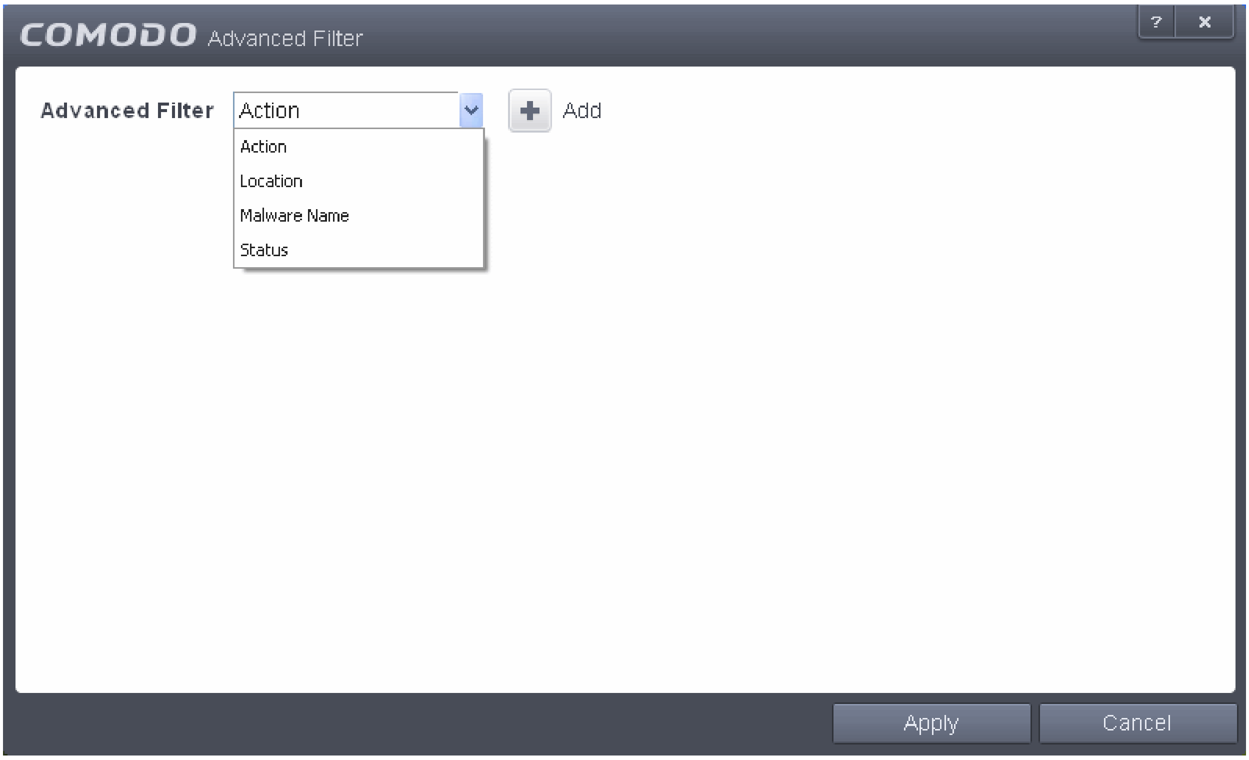
Advanced Filters:

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

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

To configure Advanced Filters for Antivirus events

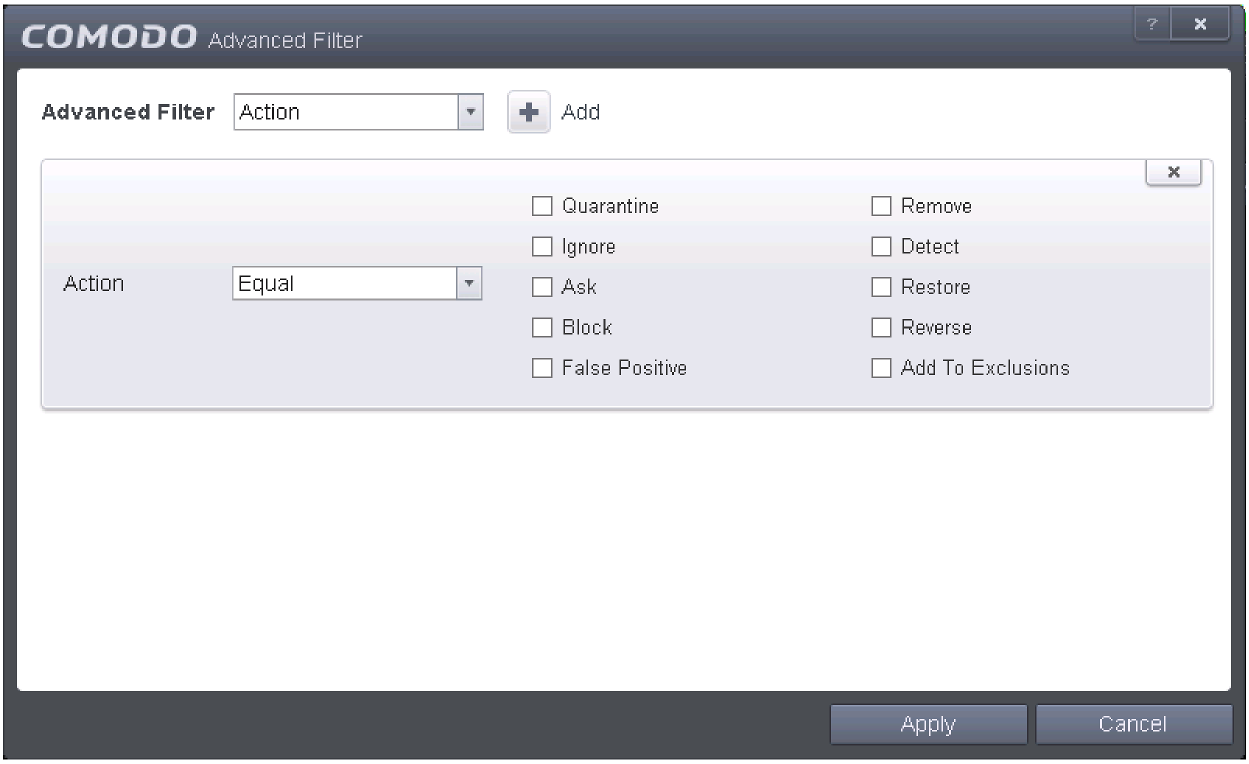
1. Click the funnel button from the title bar. The Advanced Filter interface for AV events will open
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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



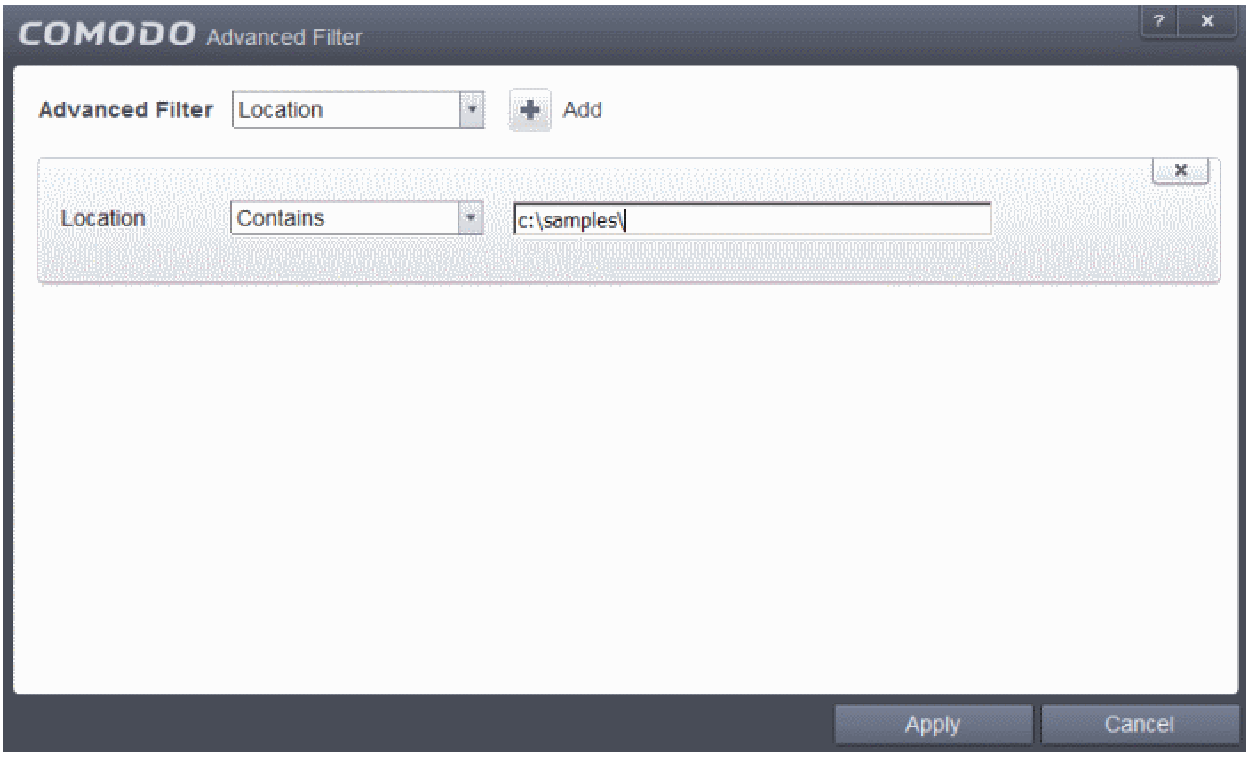
a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.

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

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

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

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



Advanced Filter: Location

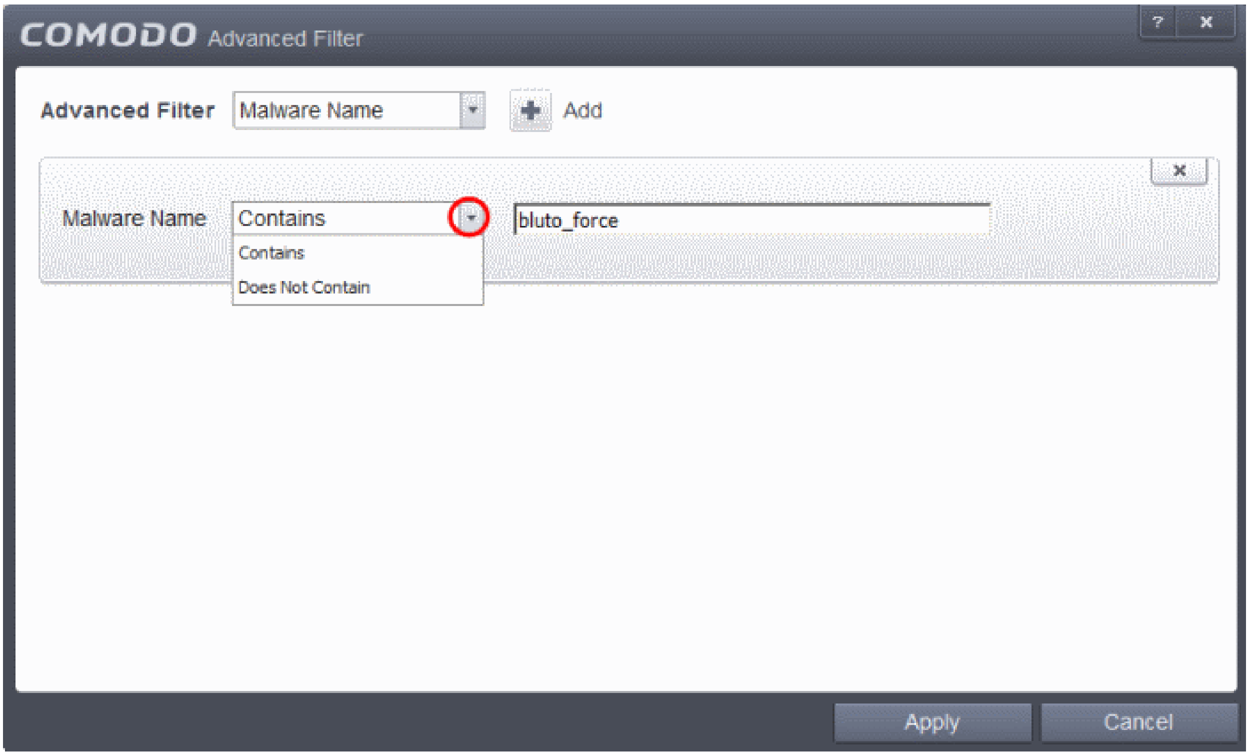
Location: Contains — c:\samples\

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

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

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

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



Advanced Filter: Malware Name

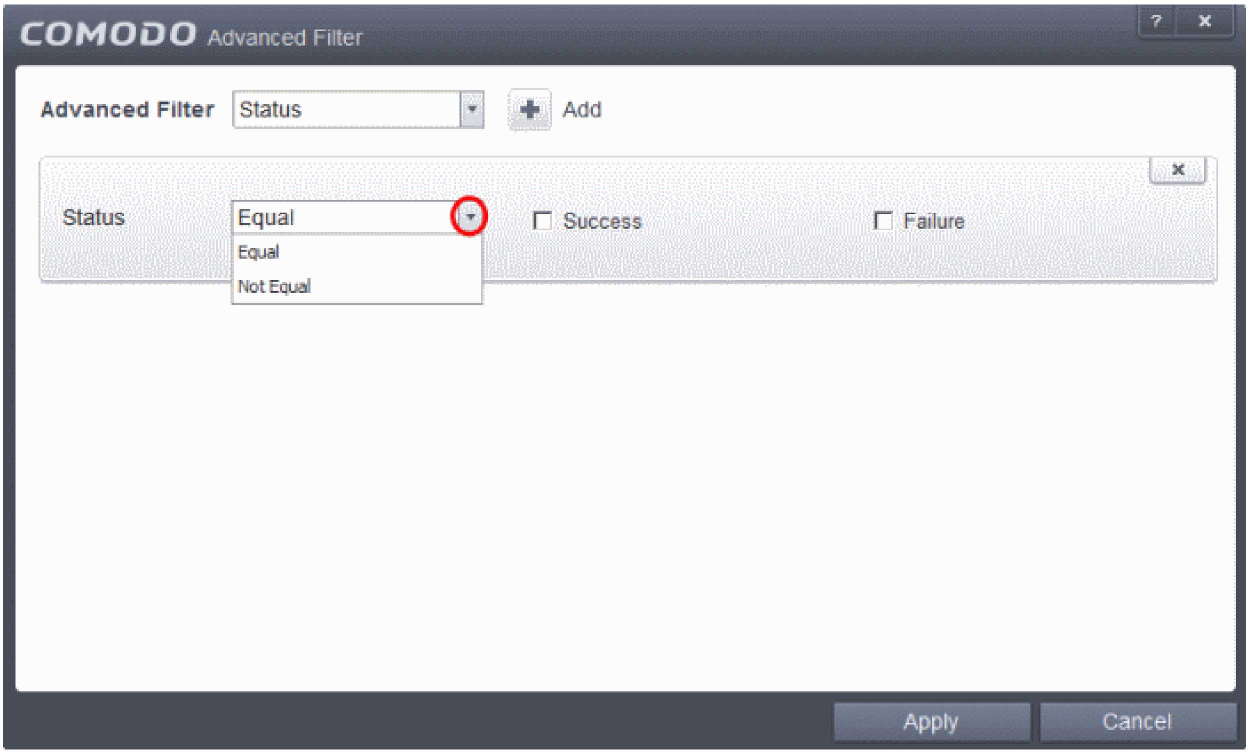
Malware Name: Contains — bluto_force

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

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

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

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



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

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

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

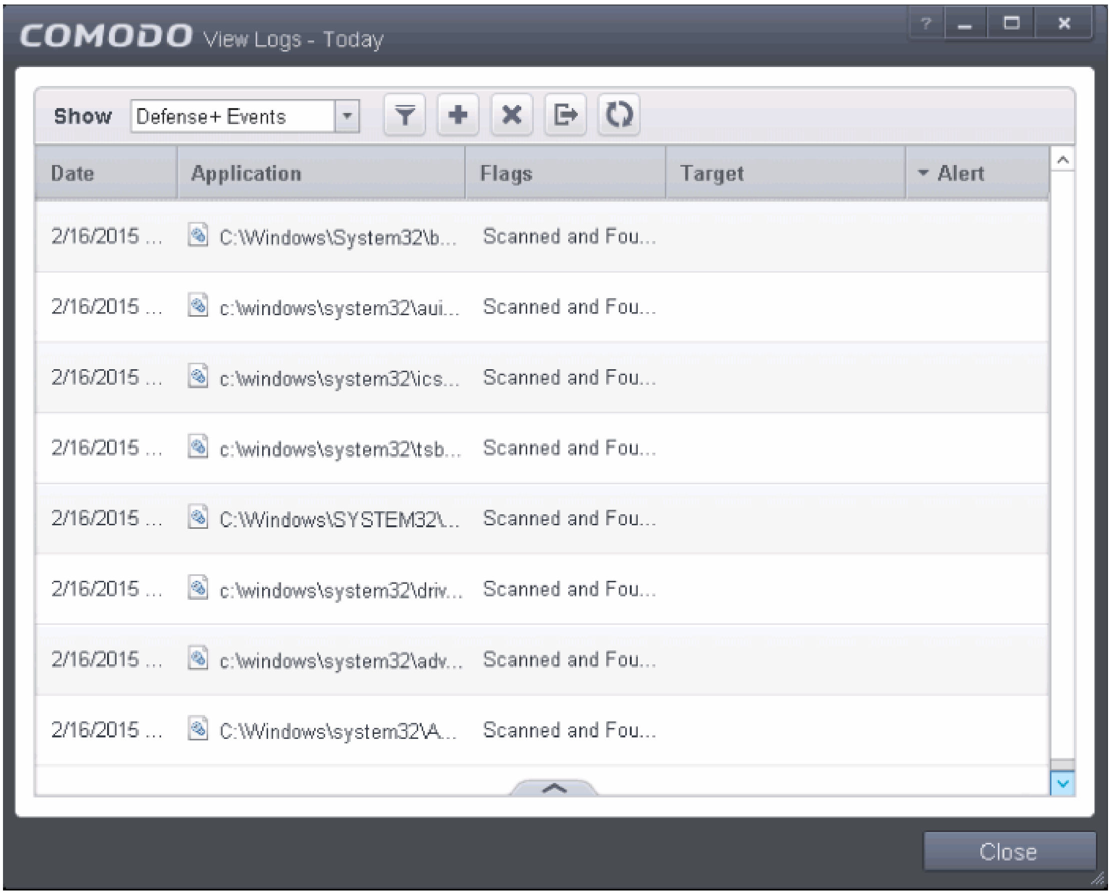
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.5.2. Defense+ Logs

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

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



Date	Application	Flags	Target	Alert
2/16/2015 ...	C:\Windows\System32\b...	Scanned and Fou...		
2/16/2015 ...	c:\windows\system32\aui...	Scanned and Fou...		
2/16/2015 ...	c:\windows\system32\ics...	Scanned and Fou...		
2/16/2015 ...	c:\windows\system32\tsb...	Scanned and Fou...		
2/16/2015 ...	C:\Windows\SYSTEM32\...	Scanned and Fou...		
2/16/2015 ...	c:\windows\system32\driv...	Scanned and Fou...		
2/16/2015 ...	c:\windows\system32\adv...	Scanned and Fou...		
2/16/2015 ...	C:\Windows\system32\A...	Scanned and Fou...		

Column Descriptions

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

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

2.5.2.1. Filtering Defense+ Logs

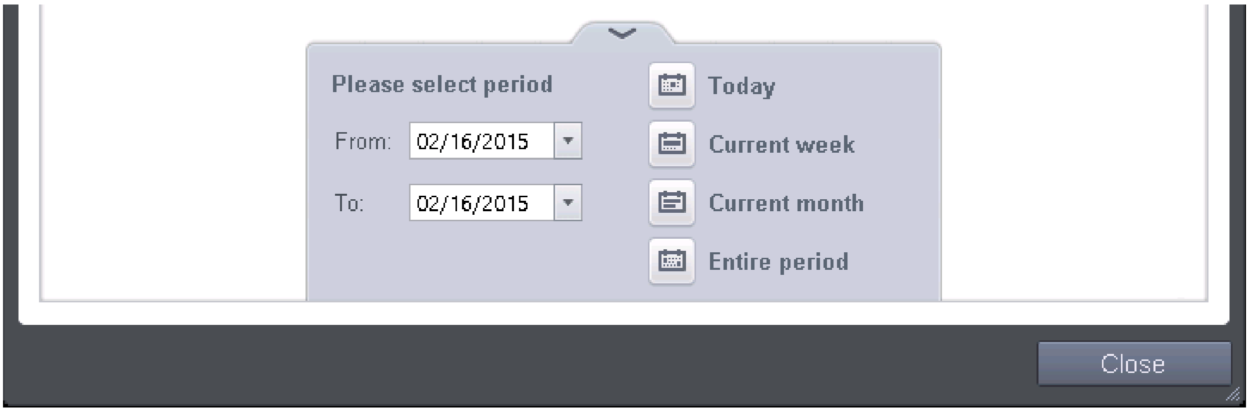
CAVS allows you to create custom views of all logged events according to user defined criteria. You can use the following types of filters:

- Preset Time Filters

- Advanced Filters

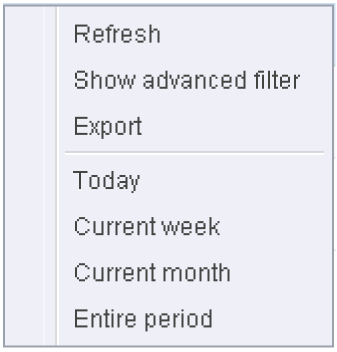
Preset Time Filters

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



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

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



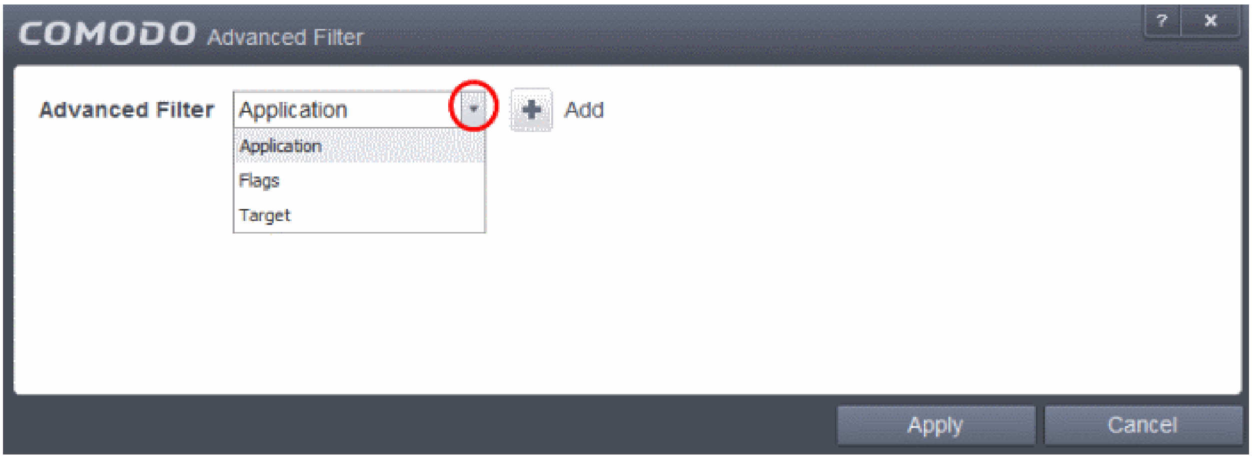
Advanced Filters

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

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

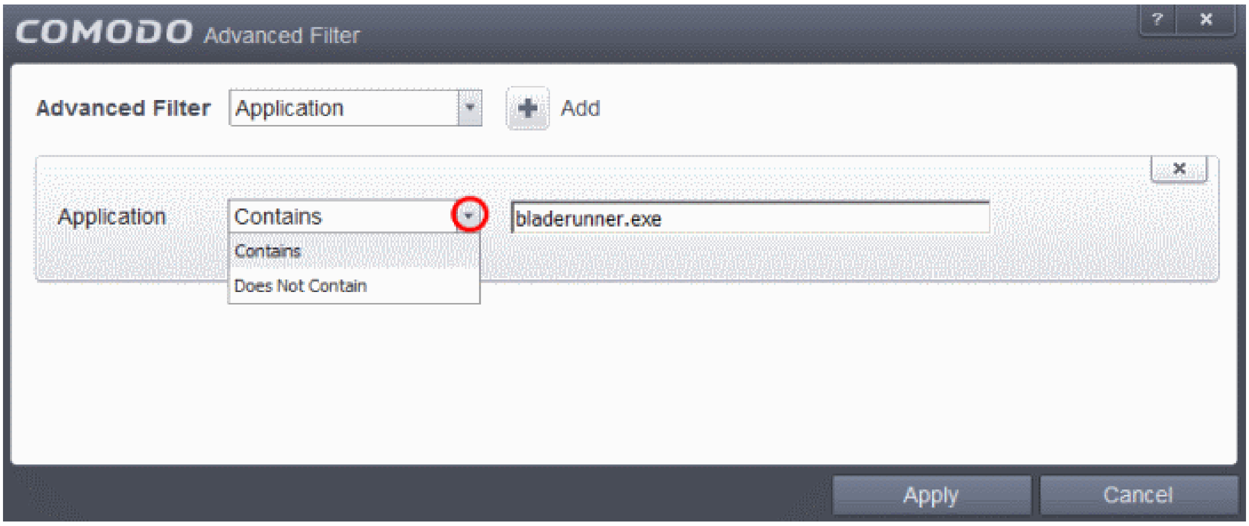
To configure Advanced Filters for Defense+ events

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



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

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

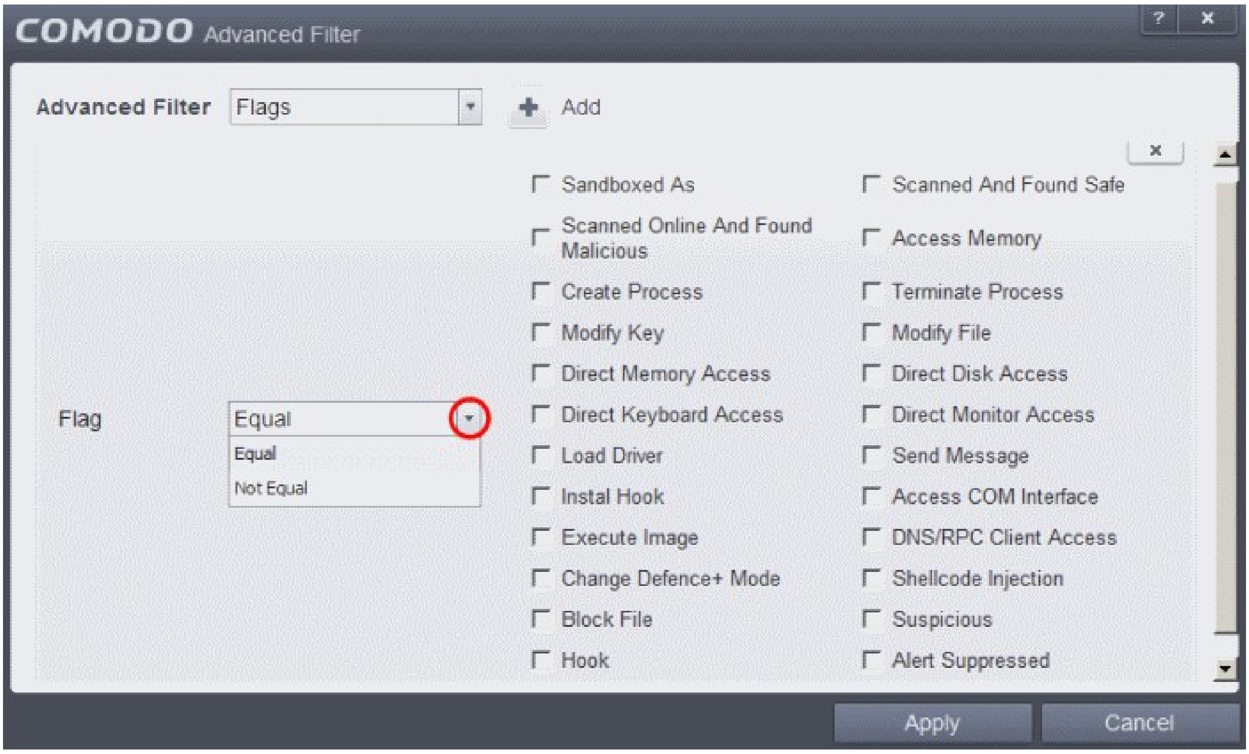


bladerunner.exe

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

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

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



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

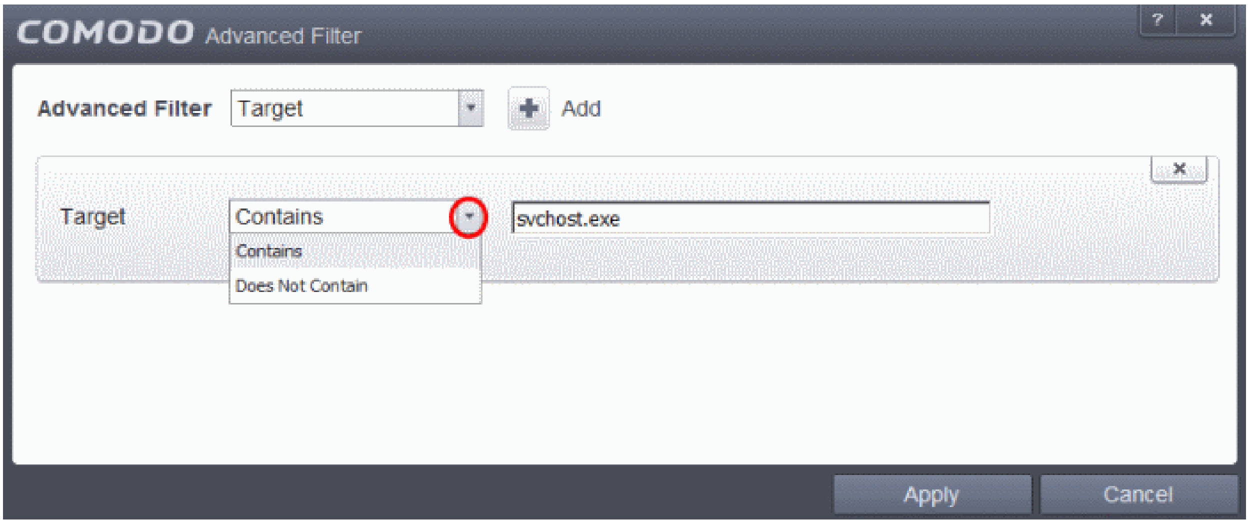
d) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

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

- Alert Suppressed

For example, if you select 'Equal' option from the drop-down field and select 'Direct Memory Access' from the checkboxes, , then only events of applications that tried to access the server memory will be displayed. If you select 'Not Equal' option from the drop-down field and select 'Modify Key' check box, then all events that do not have the entry 'Modify Key' in the 'Flags' column will be displayed. You can select more than one check box options from this interface, as required.

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



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

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

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

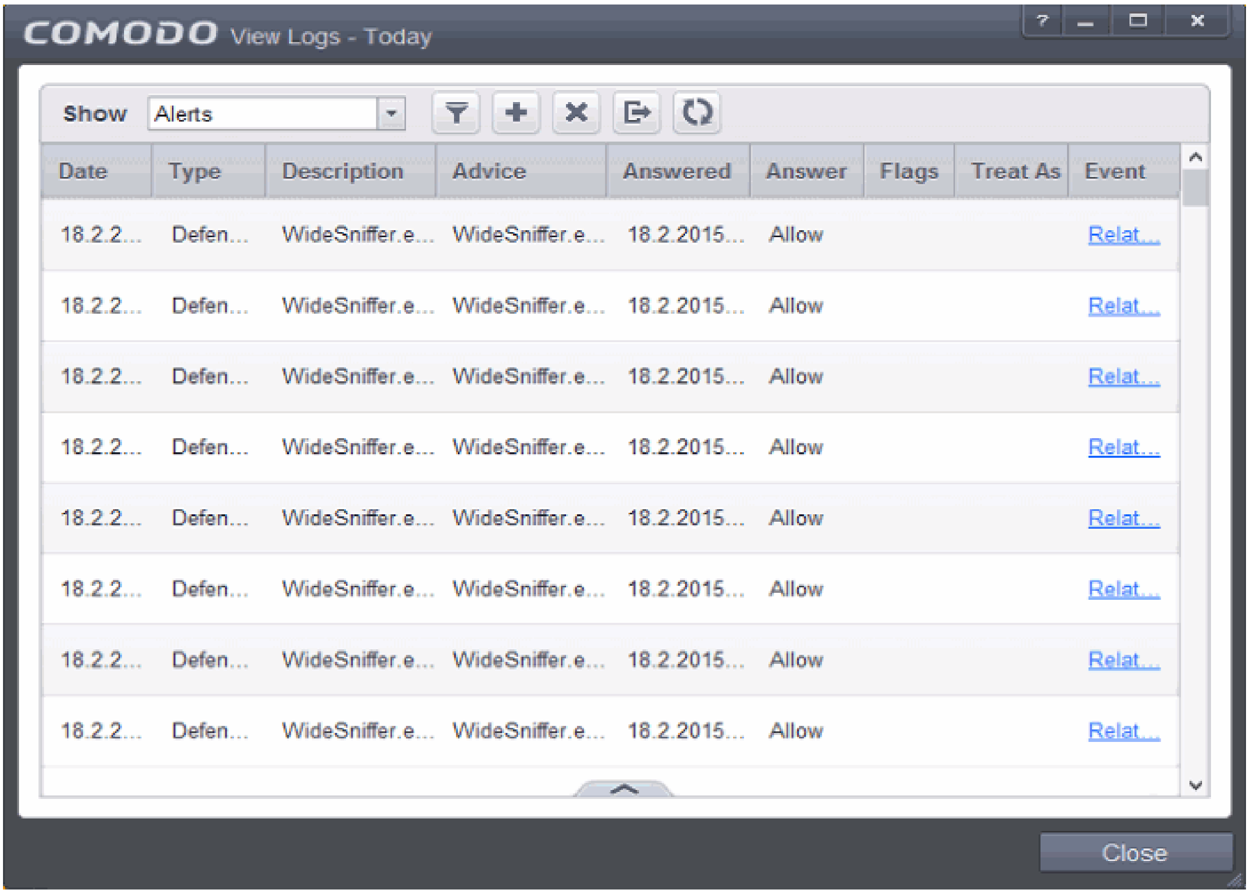
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.5.3.'Alerts' Logs

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

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



Date	Type	Description	Advice	Answered	Answer	Flags	Treat As	Event
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...
18.2.2...	Defen...	WideSniffer.e...	WideSniffer.e...	18.2.2015...	Allow			Relat...

Column Descriptions

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

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

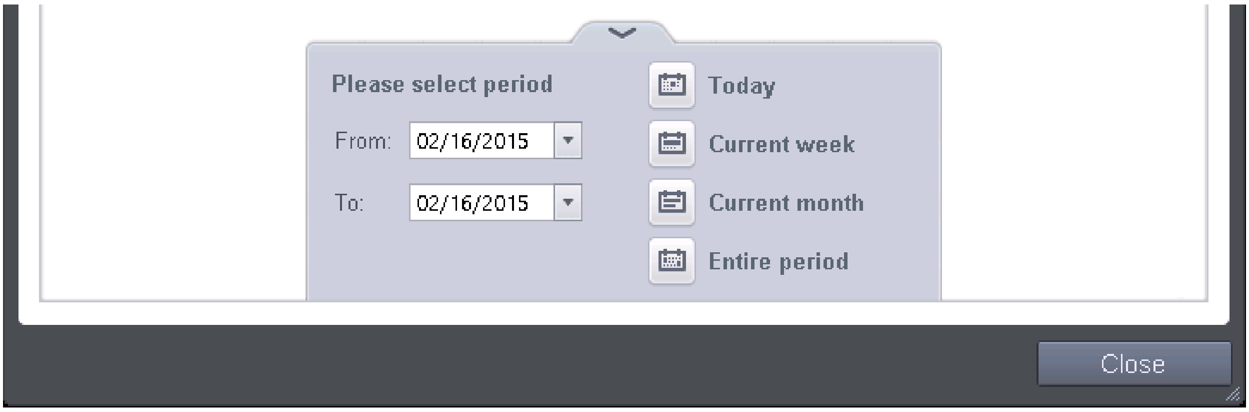
2.5.3.1. Filtering 'Alerts Displayed' Logs

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

- Preset Time Filters
- Advanced Filters

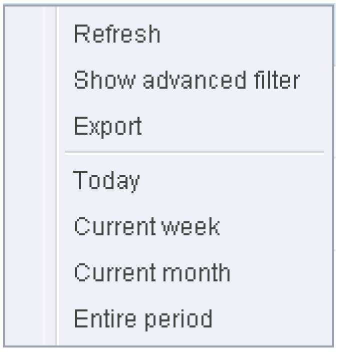
Preset Time Filters

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



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

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



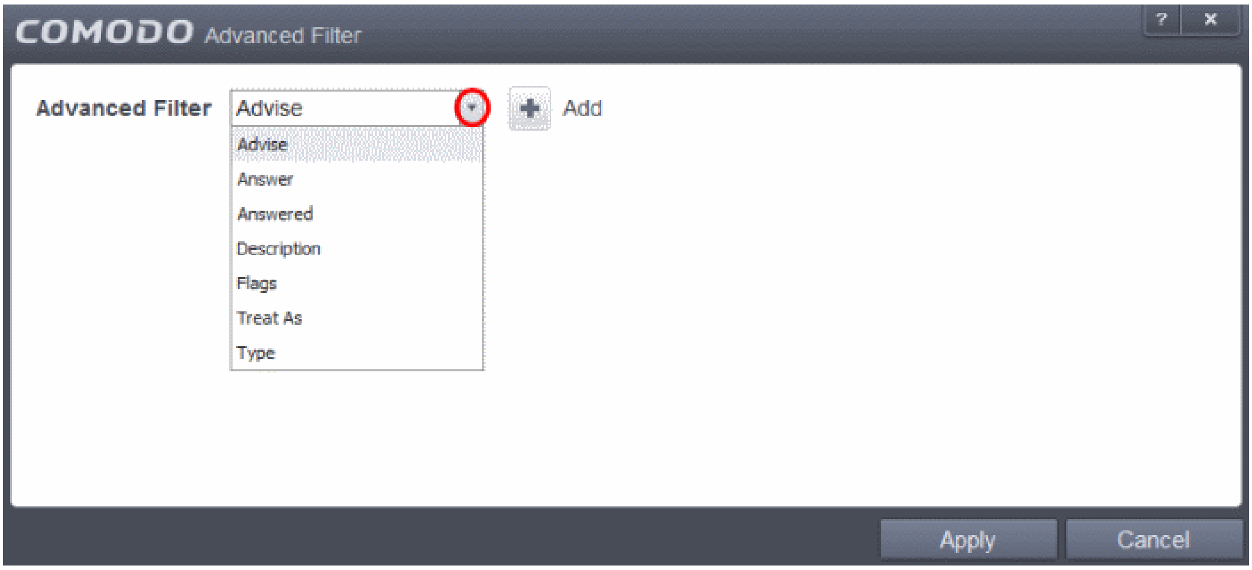
Advanced Filters

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

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

To configure Advanced Filters for Alerts Displayed

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

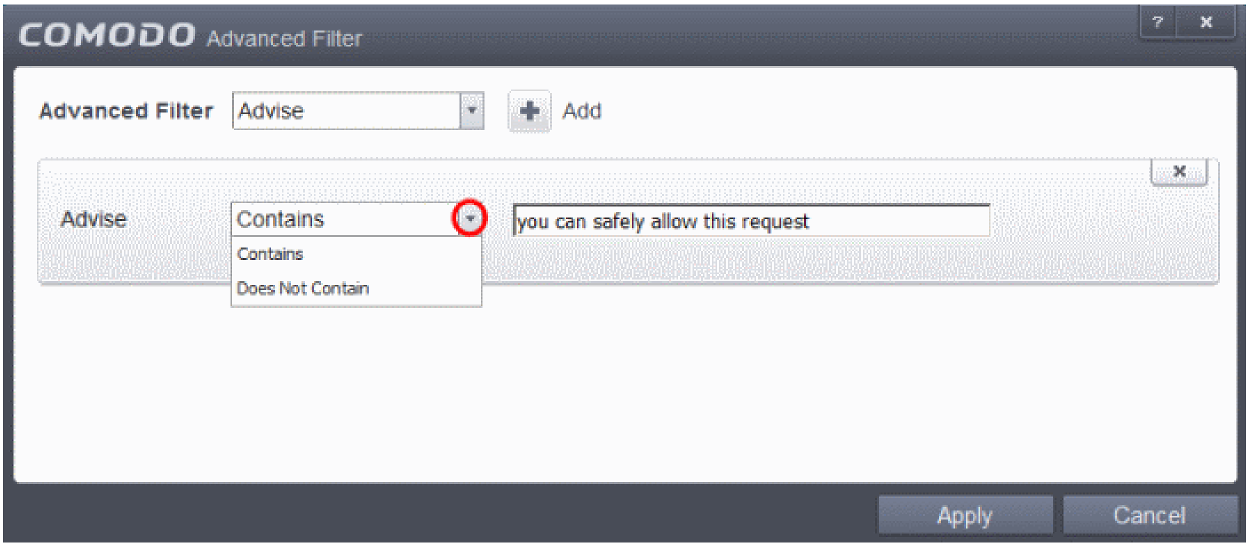


You have 7 categories of filters that you can add. Each of these categories can be further refined by either selecting or deselecting specific filter parameters or by the user typing a filter string in the field provided. You can add and configure any number of filters in the 'Advanced Filter' dialog.

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

i. **Advise**: The 'Advise' option enables you to filter the alerts based on advices given by CAVS in the alert.

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



Advanced Filter: Advise

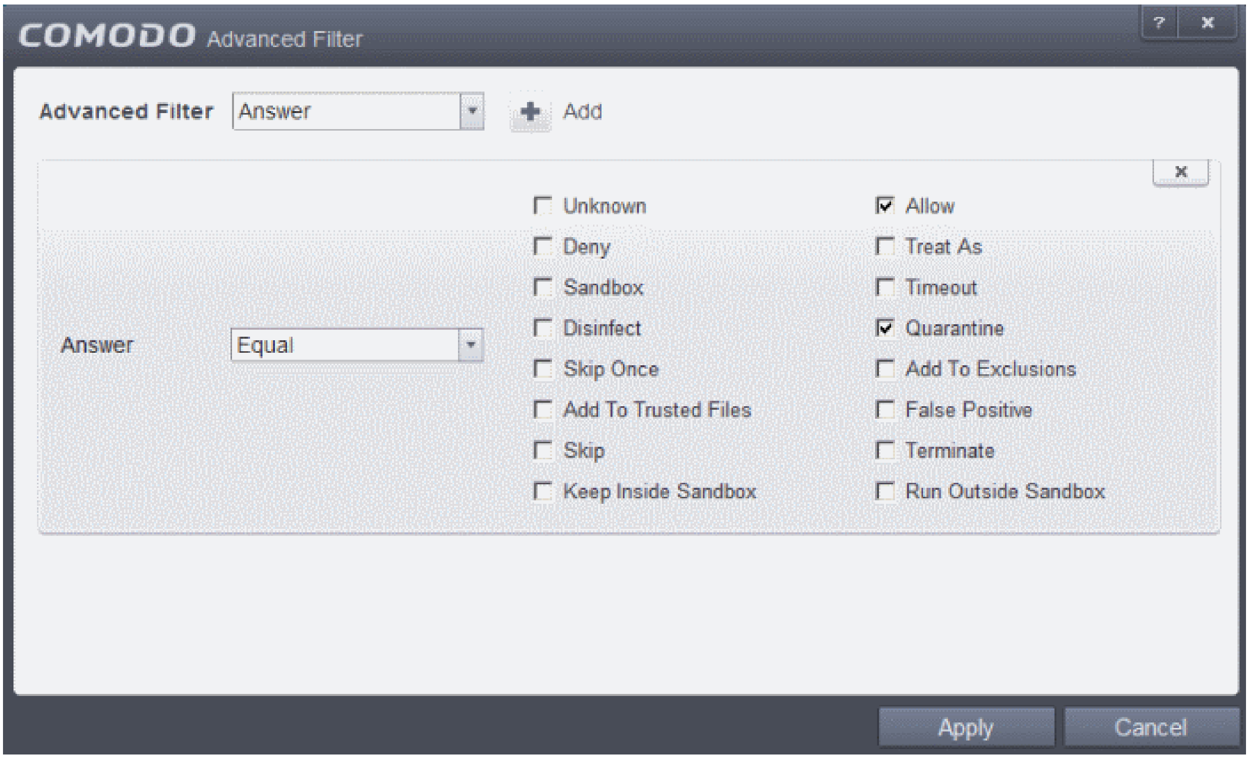
Advise: Contains — you can safely allow this request

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

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

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

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



Advanced Filter: Answer

Answer: Equal

□ Unknown
□ Deny
□ Sandbox
□ Disinfect
□ Skip Once
□ Add To Trusted Files
□ Skip
□ Keep Inside Sandbox
☑ Allow
□ Treat As
□ Timeout
☑ Quarantine
□ Add To Exclusions
□ False Positive
□ Terminate
□ Run Outside Sandbox

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

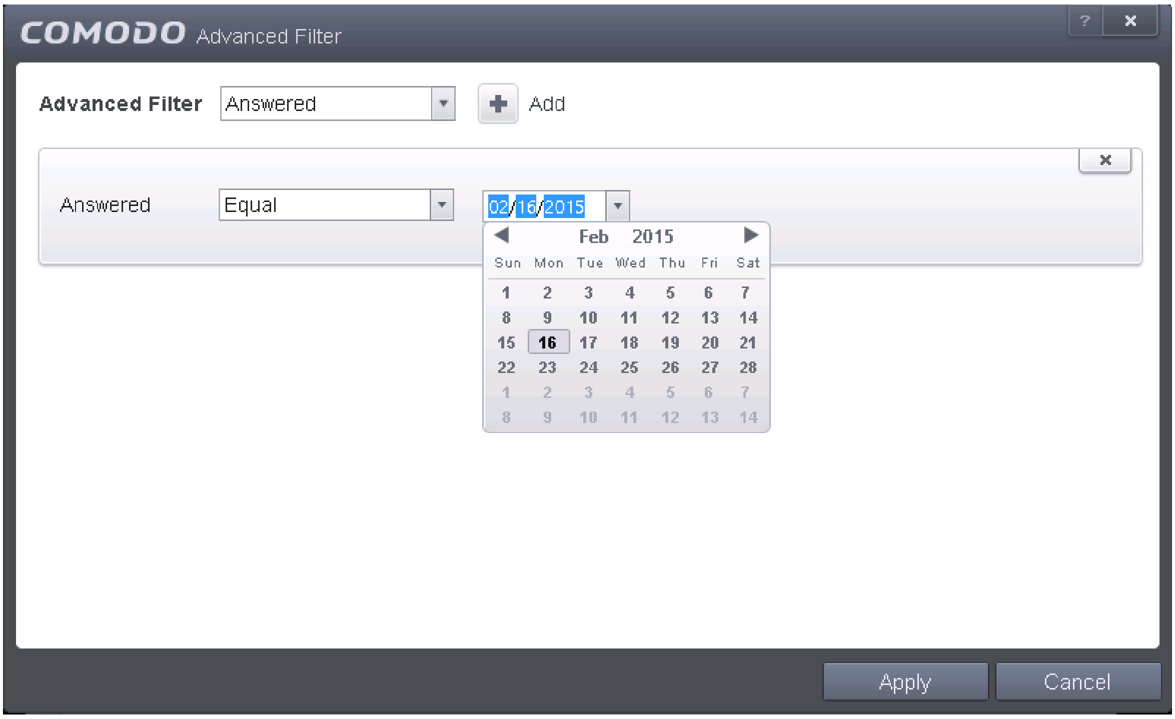
b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Unknown

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

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

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



COMODO Advanced Filter

Advanced Filter: Answered

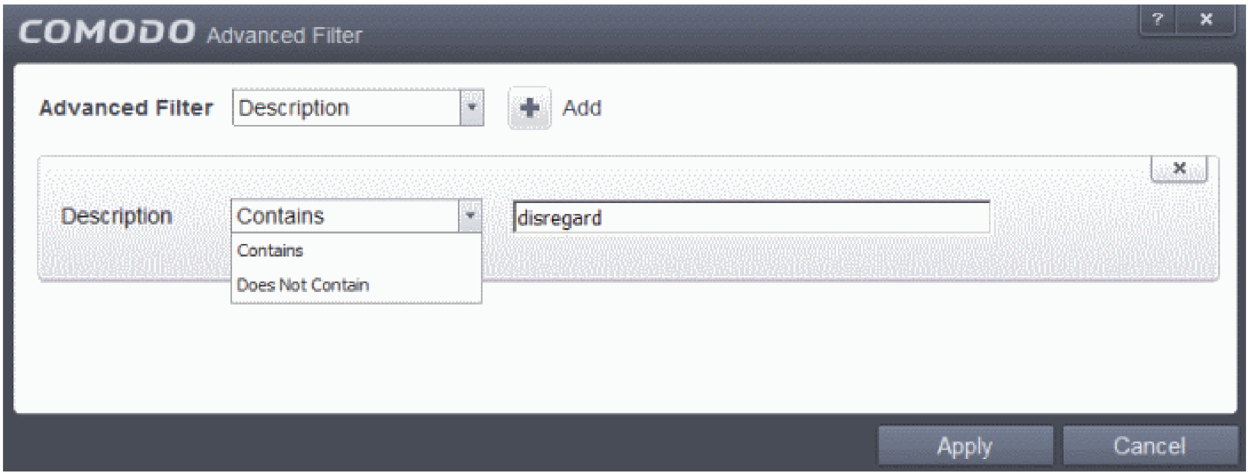
Answered: Equal, 02/16/2015

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

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

For example, if you select 'Equal' from the drop-down and select '09/05/2013', only the log of alerts answered on 09/05/2013 will be displayed.

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

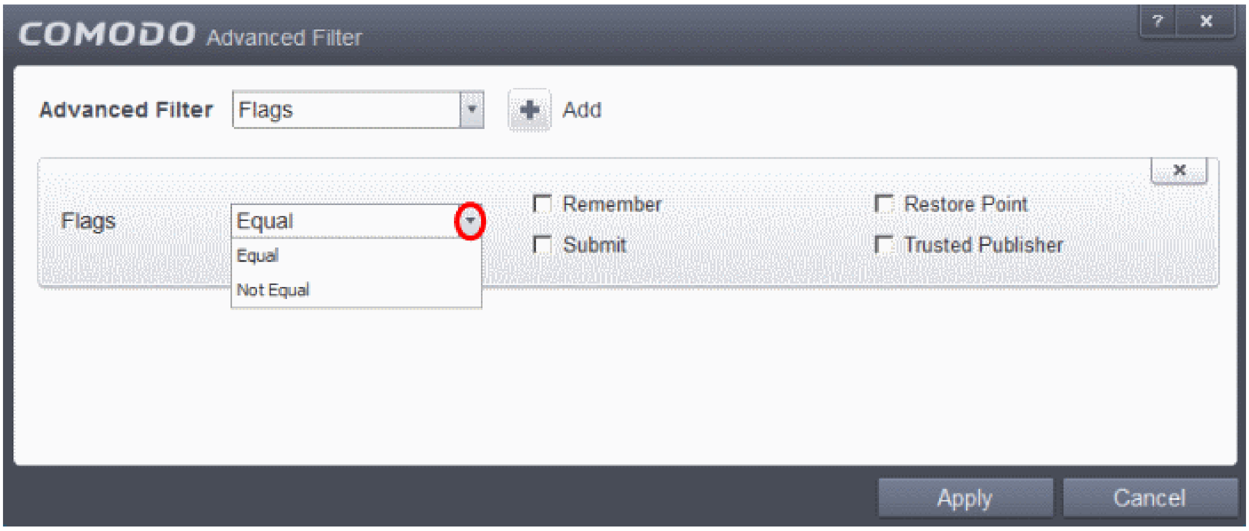


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

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

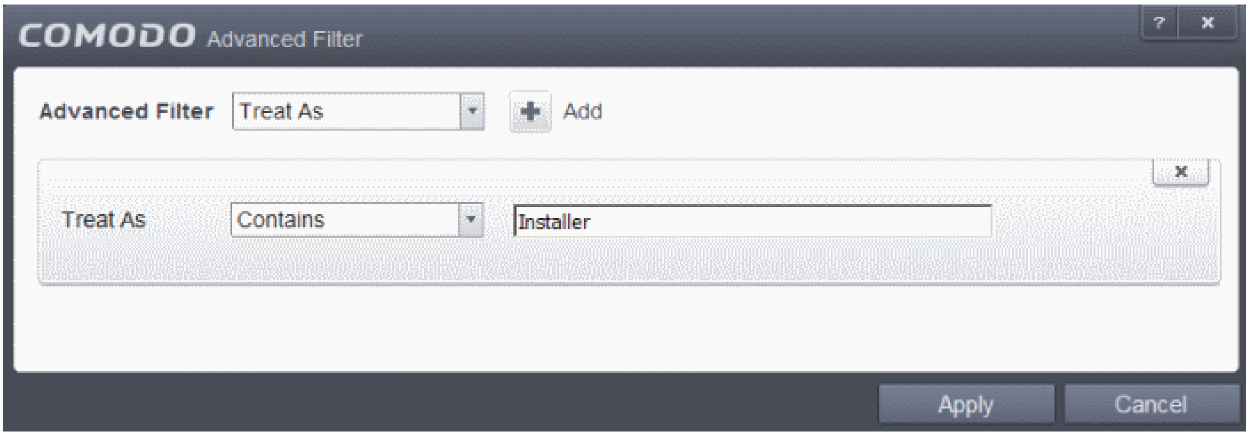


a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

- Remember
- Restore Point
- Submit
- Trusted Publisher

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



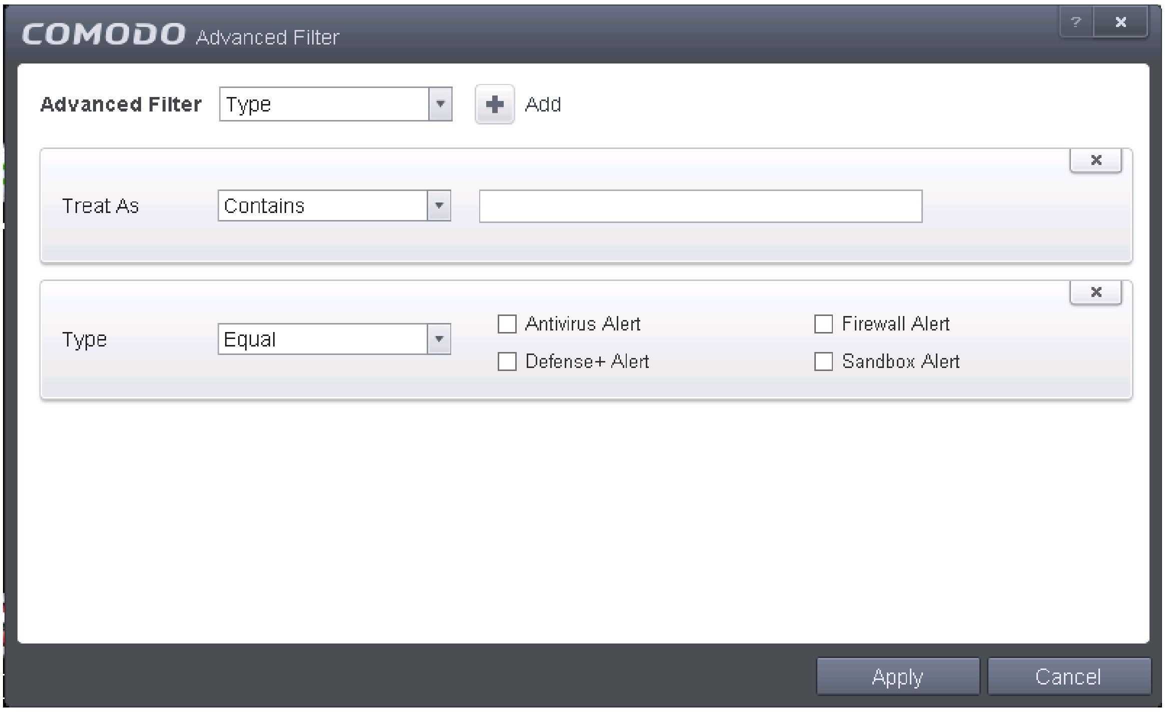
Treat As: Contains — Installer

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

b) Enter the text or word as your filter criteria

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

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



Treat As: Contains

Type: Equal

□ Antivirus Alert □ Firewall Alert

□ Defense+ Alert □ Sandbox Alert

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

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

- Antivirus Alert
- Defense+ Alert
- Firewall Alert
- Sandbox Alert

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

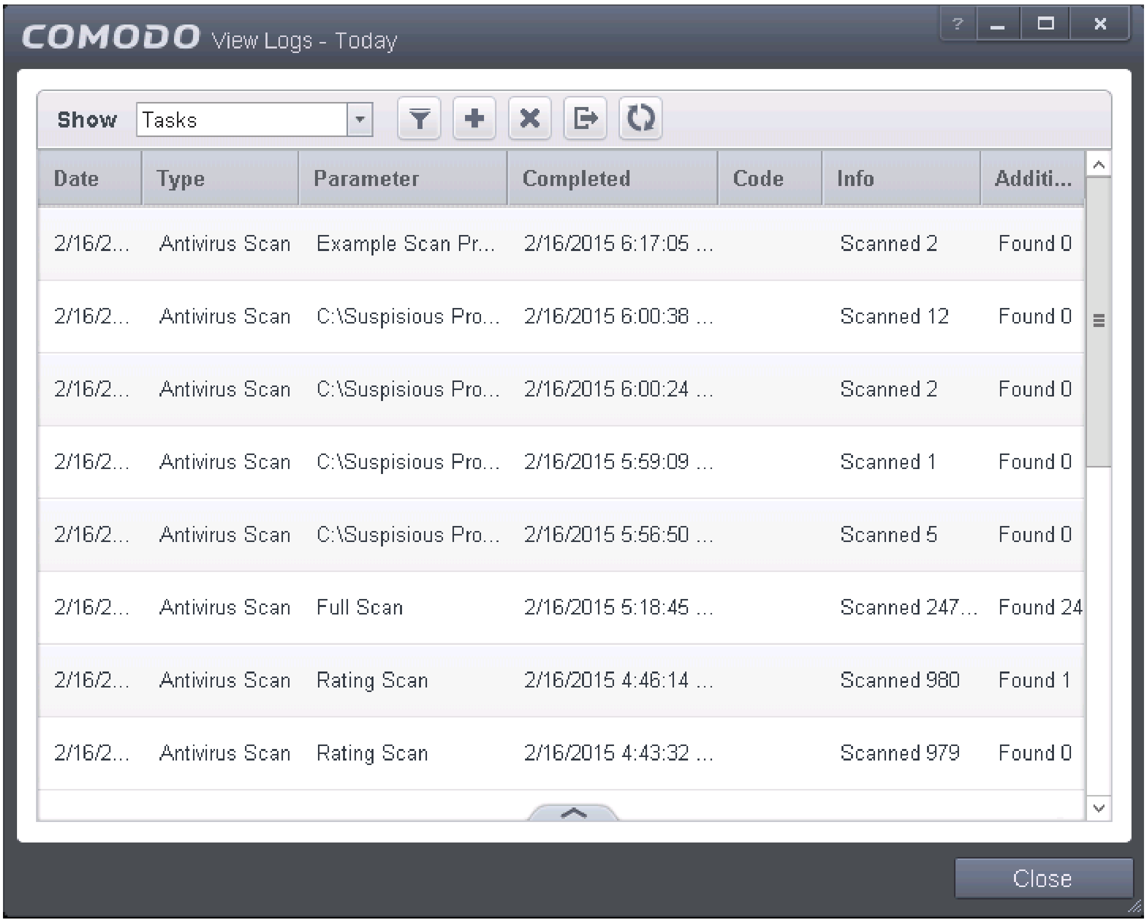
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.5.4. Tasks

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

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



Show: Tasks

Date	Type	Parameter	Completed	Code	Info	Additi...
2/16/2...	Antivirus Scan	Example Scan Pr...	2/16/2015 6:17:05 ...		Scanned 2	Found 0
2/16/2...	Antivirus Scan	C:\Suspisious Pro...	2/16/2015 6:00:38 ...		Scanned 12	Found 0
2/16/2...	Antivirus Scan	C:\Suspisious Pro...	2/16/2015 6:00:24 ...		Scanned 2	Found 0
2/16/2...	Antivirus Scan	C:\Suspisious Pro...	2/16/2015 5:59:09 ...		Scanned 1	Found 0
2/16/2...	Antivirus Scan	C:\Suspisious Pro...	2/16/2015 5:56:50 ...		Scanned 5	Found 0
2/16/2...	Antivirus Scan	Full Scan	2/16/2015 5:18:45 ...		Scanned 247...	Found 24
2/16/2...	Antivirus Scan	Rating Scan	2/16/2015 4:46:14 ...		Scanned 980	Found 1
2/16/2...	Antivirus Scan	Rating Scan	2/16/2015 4:43:32 ...		Scanned 979	Found 0

Column Descriptions

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

6. **Info & Additional Info -** Provides additional information of the task.

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

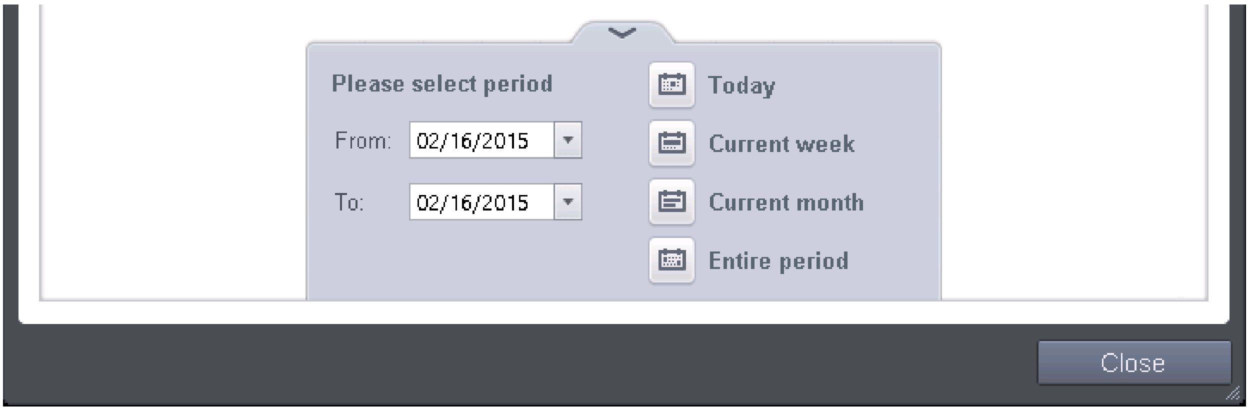
2.5.4.1. Filtering 'Tasks Launched' Logs

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

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

Preset Time Filters

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



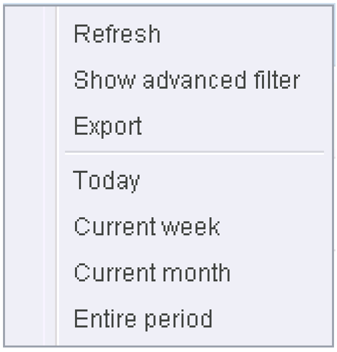
Please select period

From: 02/16/2015

To: 02/16/2015

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

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



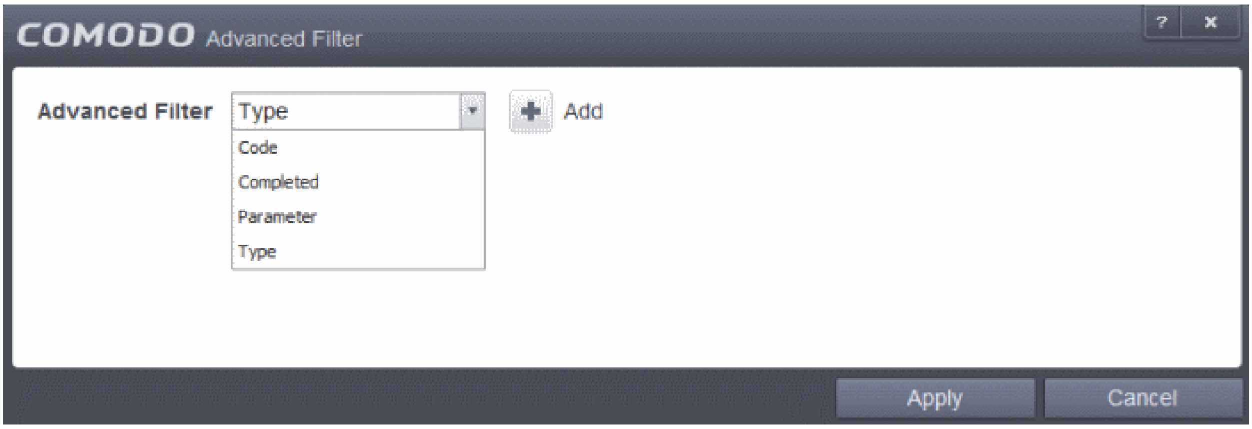
Advanced Filters

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

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

To configure Advanced Filters for 'Tasks' logs

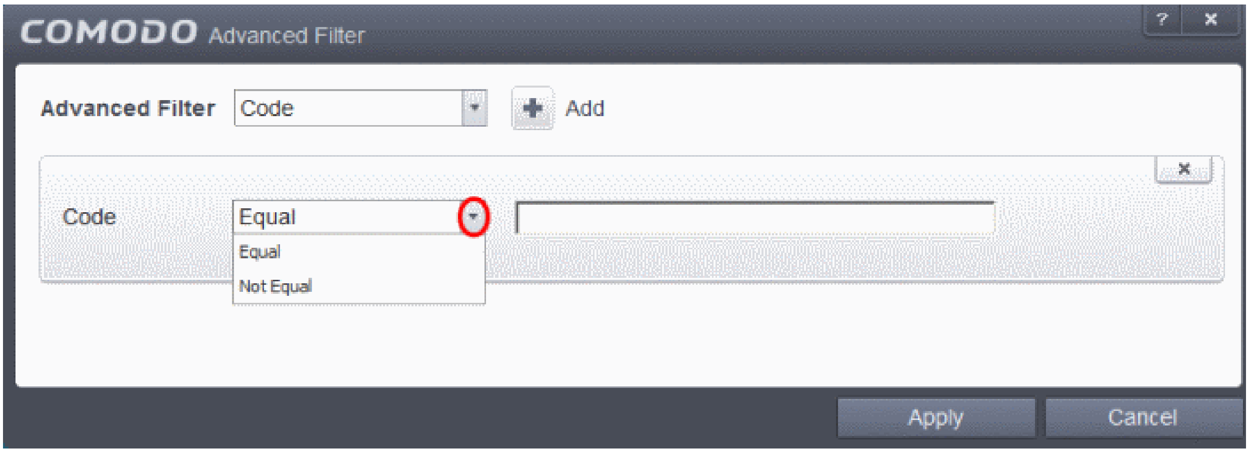
1. Click the funnel button from the title bar. The Advanced Filter interface for Tasks log viewer will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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

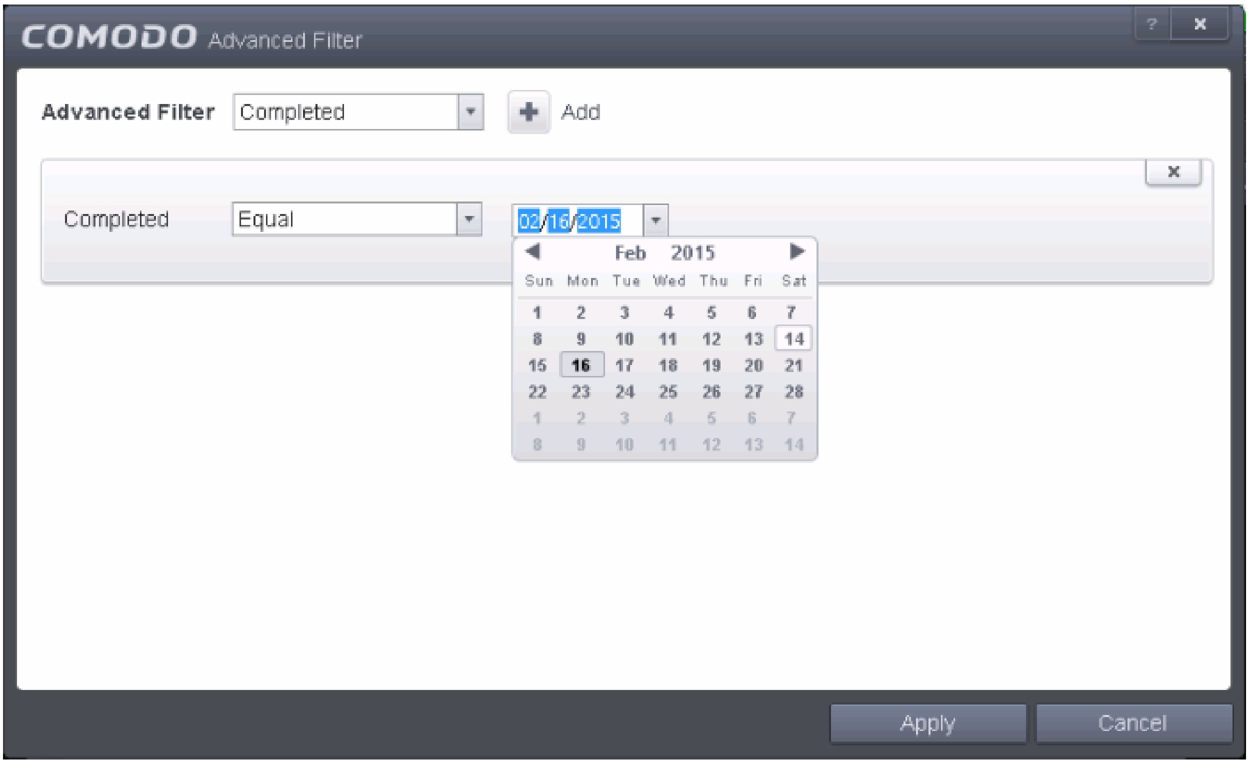


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

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

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



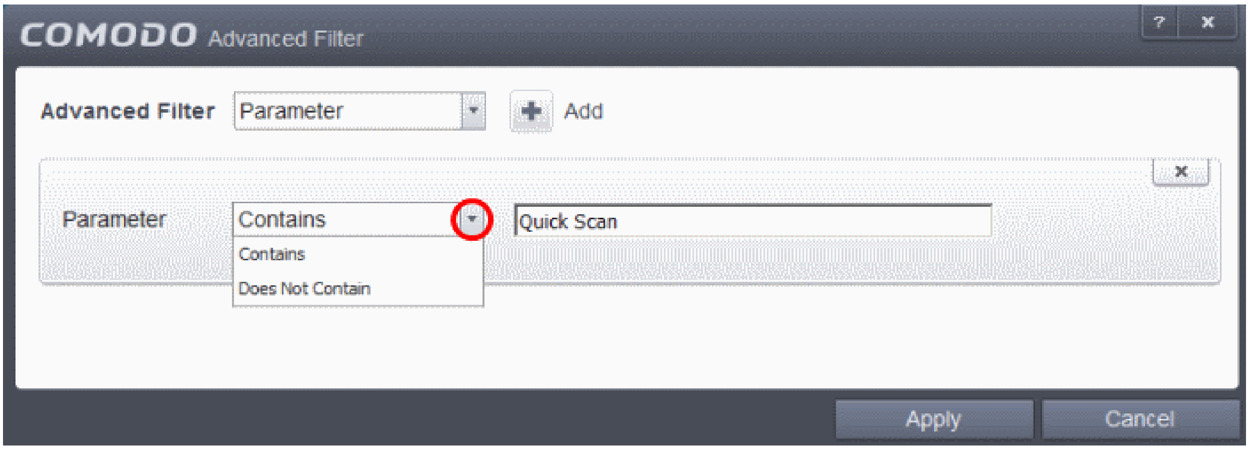
a) Select any one of the following option the drop-down box.

- Equal
- Not Equal

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

For example, if you select 'Equal' from the drop-down and select '09/05/2013' , only the log of Tasks completed on 09/05/2013 will be displayed.

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

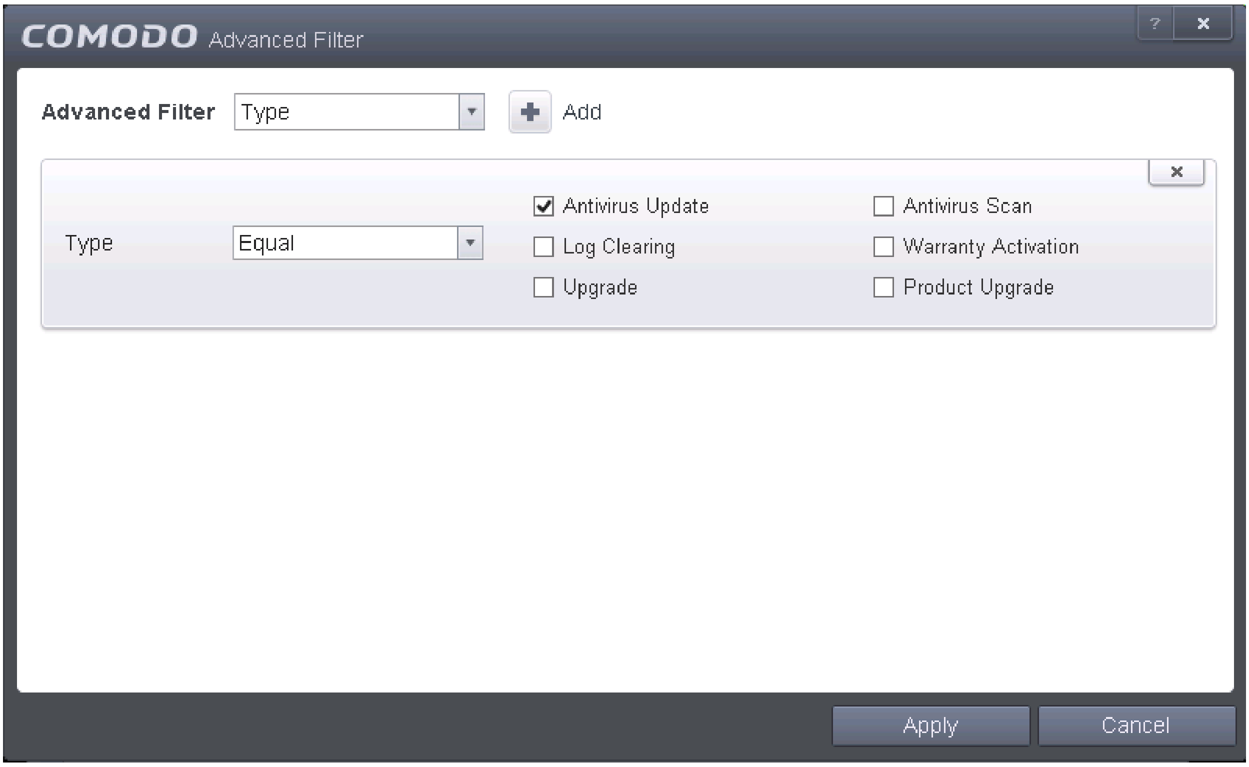


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

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



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

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

- Antivirus Update
- Antivirus Scan
- Logs Clearing
- Upgrade
- Warranty Activation
- Product Upgrade

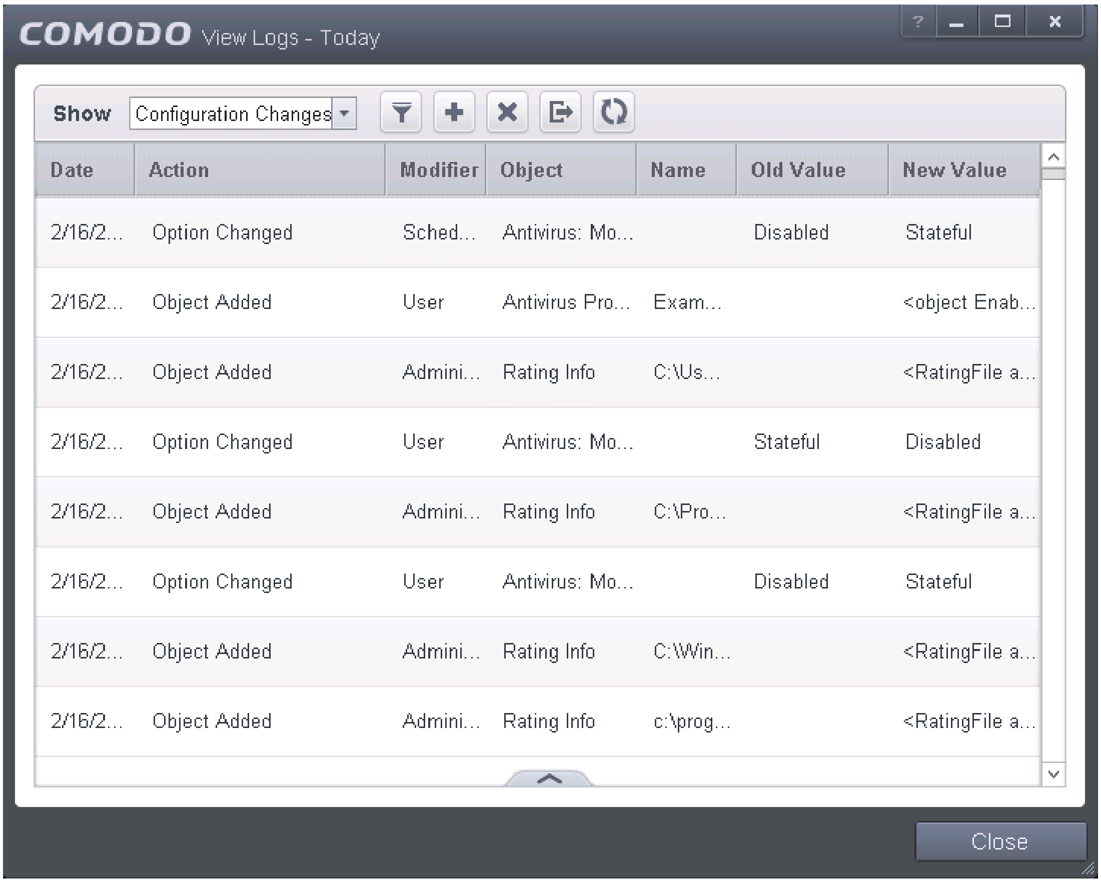
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.5.5. Configuration Changes

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

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



Date	Action	Modifier	Object	Name	Old Value	New Value
2/16/2...	Option Changed	Sched...	Antivirus: Mo...		Disabled	Stateful
2/16/2...	Object Added	User	Antivirus Pro...	Exam...		<object Enab...
2/16/2...	Object Added	Admini...	Rating Info	C:\Us...		<RatingFile a...
2/16/2...	Option Changed	User	Antivirus: Mo...		Stateful	Disabled
2/16/2...	Object Added	Admini...	Rating Info	C:\Pro...		<RatingFile a...
2/16/2...	Option Changed	User	Antivirus: Mo...		Disabled	Stateful
2/16/2...	Object Added	Admini...	Rating Info	C:\Win...		<RatingFile a...
2/16/2...	Object Added	Admini...	Rating Info	c:\prog...		<RatingFile a...

Column Descriptions

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

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

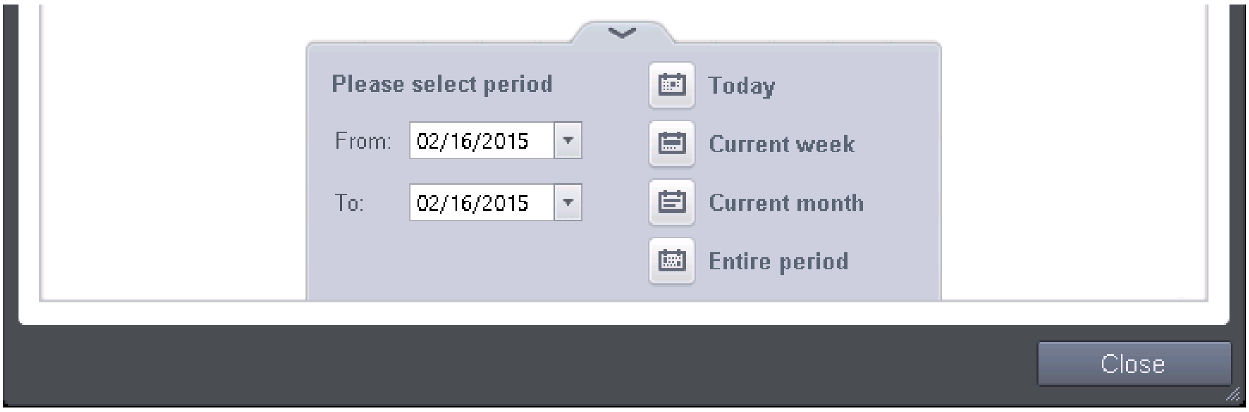
2.5.5.1. Filtering 'Configuration Changes' Logs

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

- Preset Time Filters
- Advanced Filters

Preset Time Filters

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



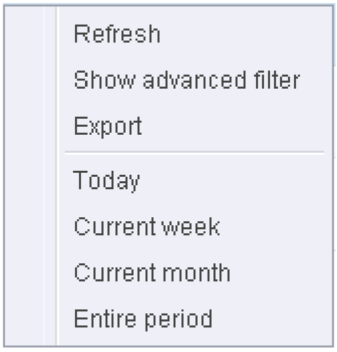
Please select period

From: 02/16/2015

To: 02/16/2015

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

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



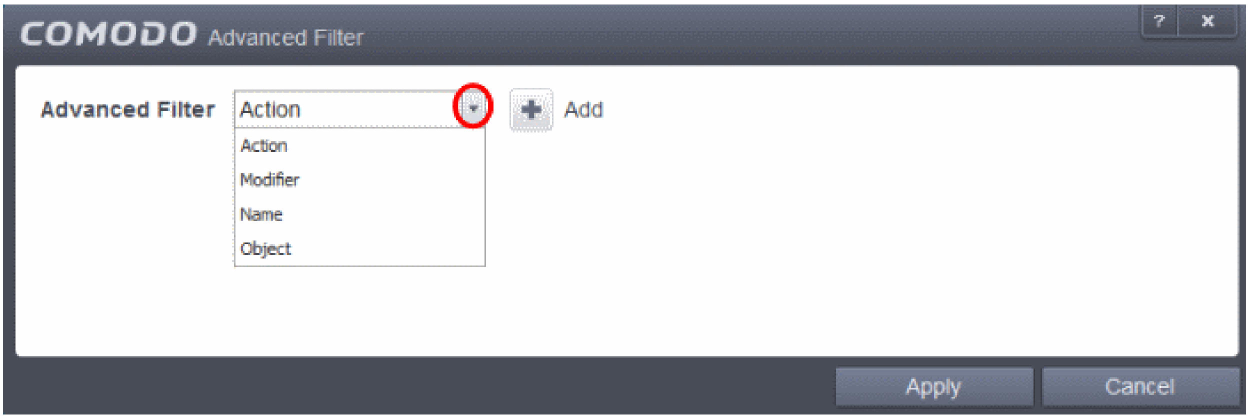
Advanced Filters

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

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

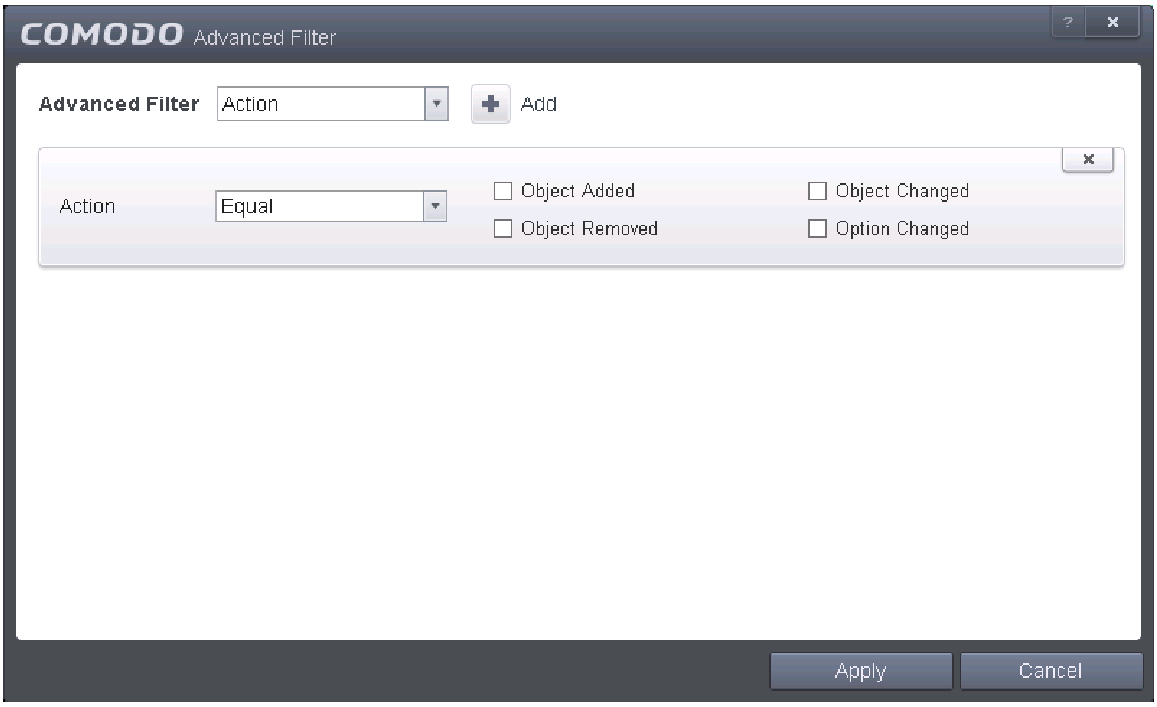
To configure Advanced Filters for Configuration Changes Logs

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



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

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

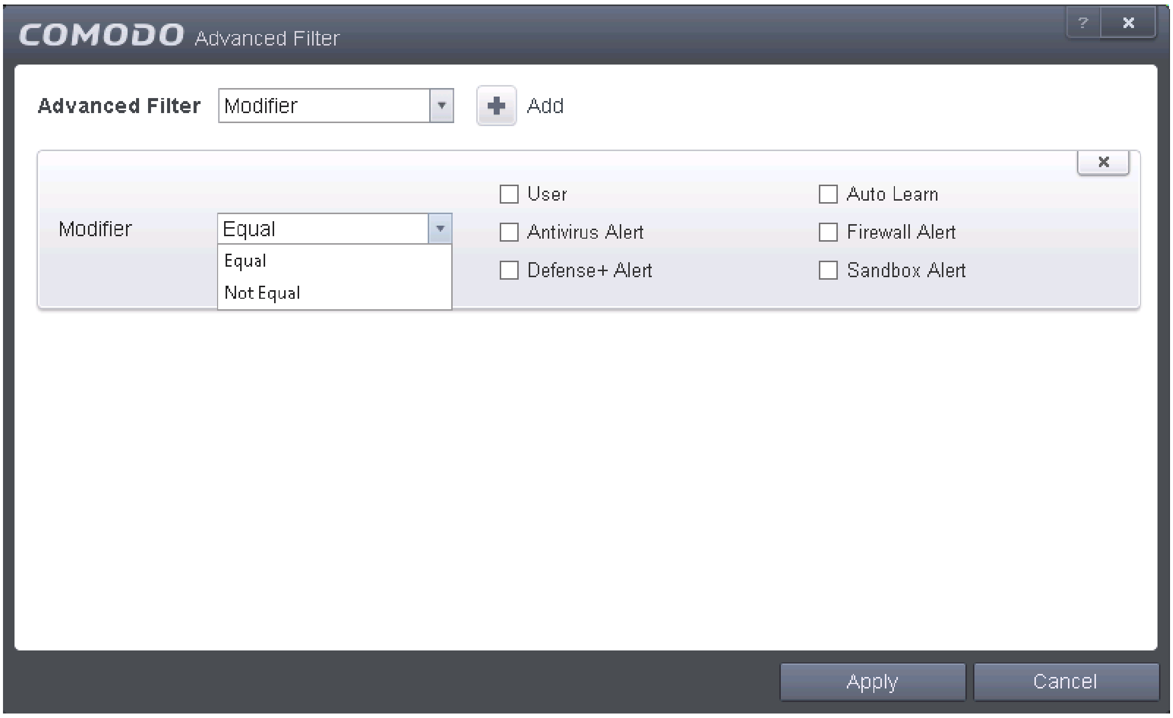


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

b) Now select the checkboxes of the specific filter parameters to refine your search. The parameters available are:
   - Object Added
   - Object Changed
   - Object Removed
   - Option Changed

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

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



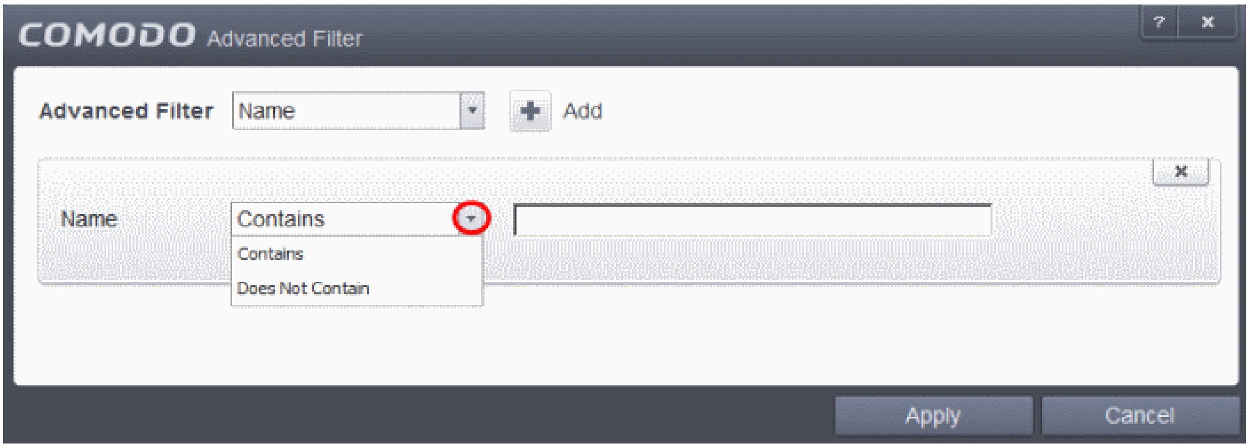
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

- User
- Auto Learn
- Antivirus Alert
- Defense+ Alert
- Firewall Alert
- Sandbox Alert

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

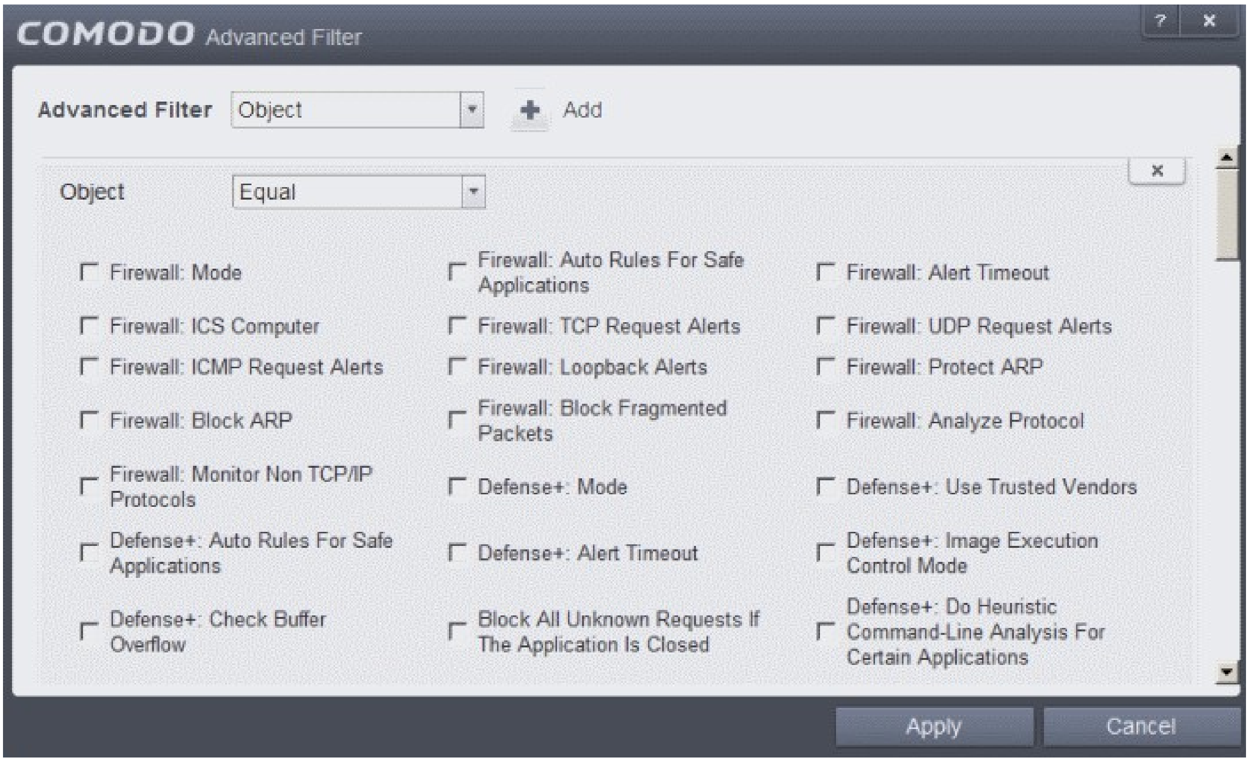
iii. **Name**: The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



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

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

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



□ Firewall: Mode
□ Firewall: Auto Rules For Safe Applications
□ Firewall: Alert Timeout
□ Firewall: ICS Computer
□ Firewall: TCP Request Alerts
□ Firewall: UDP Request Alerts
□ Firewall: ICMP Request Alerts
□ Firewall: Loopback Alerts
□ Firewall: Protect ARP
□ Firewall: Block ARP
□ Firewall: Block Fragmented Packets
□ Firewall: Analyze Protocol
□ Firewall: Monitor Non TCP/IP Protocols
□ Defense+: Mode
□ Defense+: Use Trusted Vendors
□ Defense+: Auto Rules For Safe Applications
□ Defense+: Alert Timeout
□ Defense+: Image Execution Control Mode
□ Defense+: Check Buffer Overflow
□ Block All Unknown Requests If The Application Is Closed
□ Defense+: Do Heuristic Command-Line Analysis For Certain Applications

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

b) Now select the check-boxes of the specific objects as filter parameters to refine your search. Scroll the window to the right to see all the parameters options.

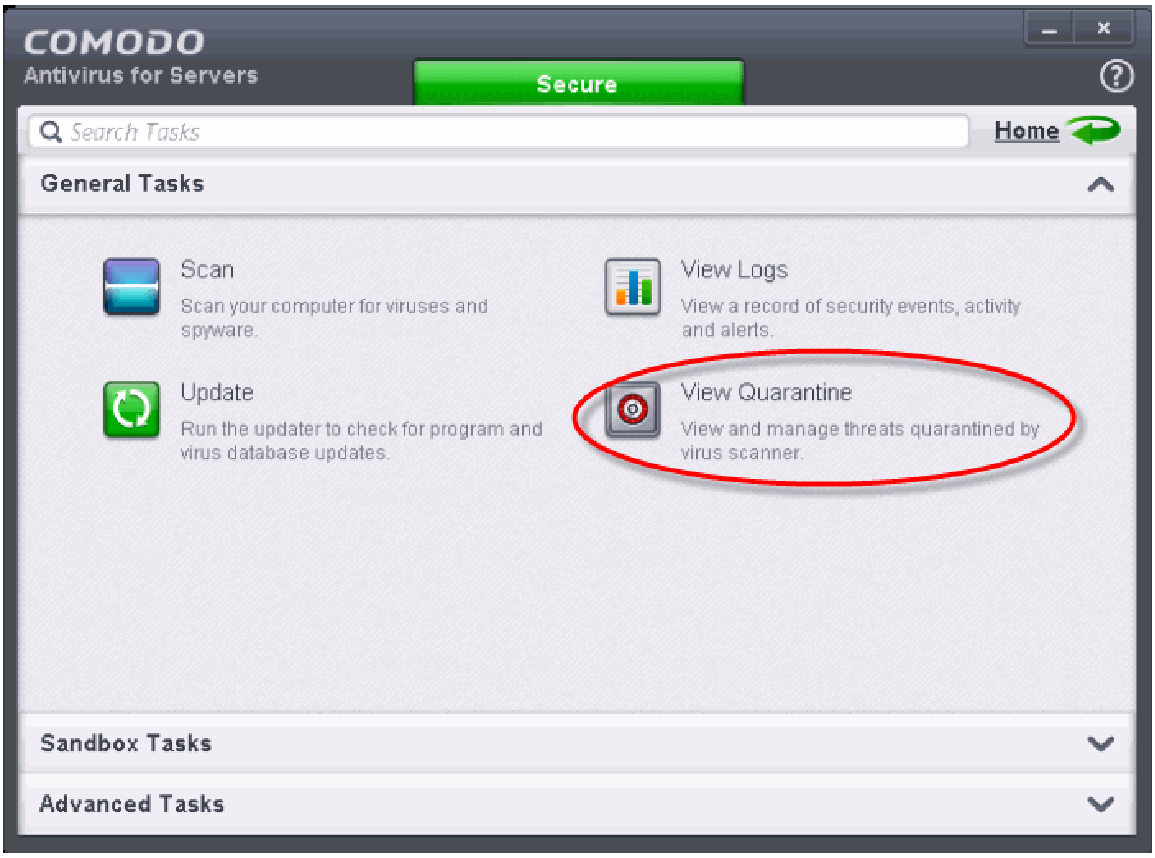
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

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

2.6. Manage Quarantined Items

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

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



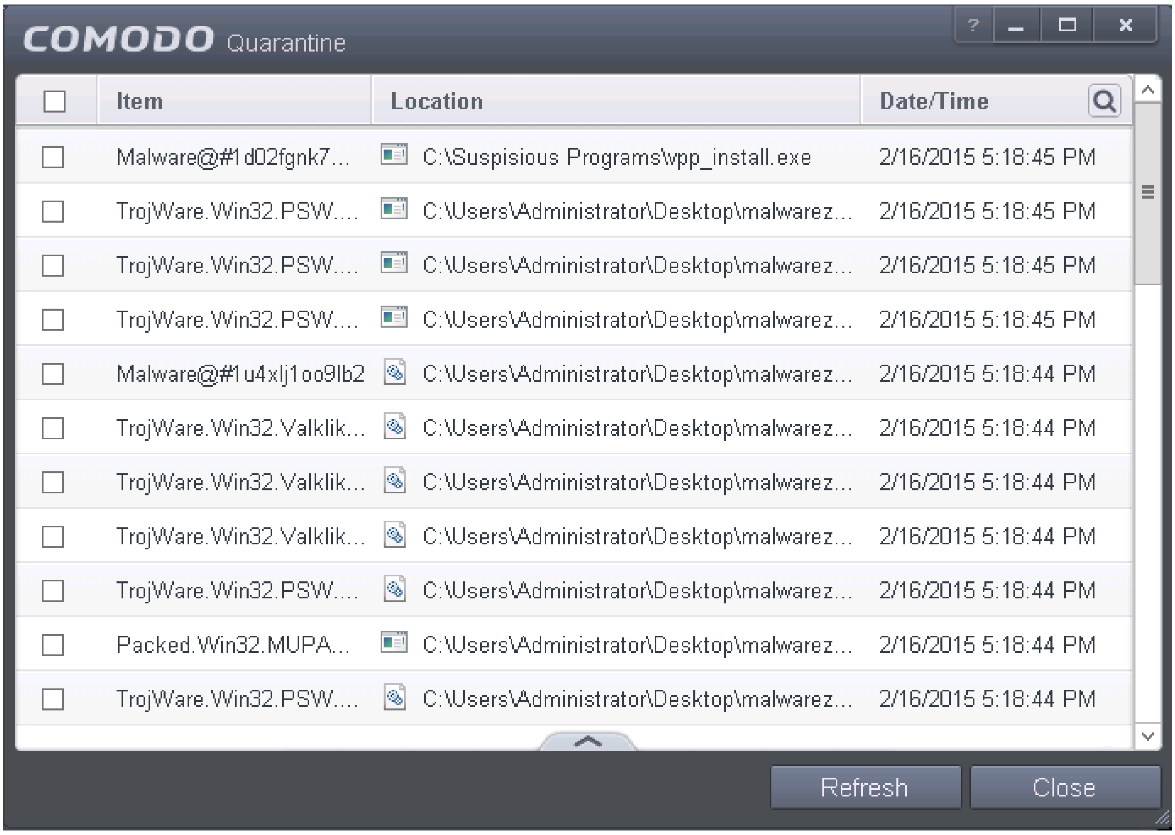
Scan
Scan your computer for viruses and spyware.

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

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

View Quarantine
View and manage threats quarantined by virus scanner.

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



☐	Item	Location	Date/Time
☐	Malware@#1d02fgnk7...	C:\Suspisious Programs\wpp_install.exe	2/16/2015 5:18:45 PM
☐	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:45 PM
☐	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:45 PM
☐	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:45 PM
☐	Malware@#1u4xlj1oo9lb2	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
☐	TrojWare.Win32.Valklik...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
☐	TrojWare.Win32.Valklik...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
☐	TrojWare.Win32.Valklik...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
☐	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
☐	Packed.Win32.MUPA...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
☐	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM

Column Descriptions

- **Item** - Indicates which application or process propagated the event;

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

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

The Quarantined Items interface also allows you to:

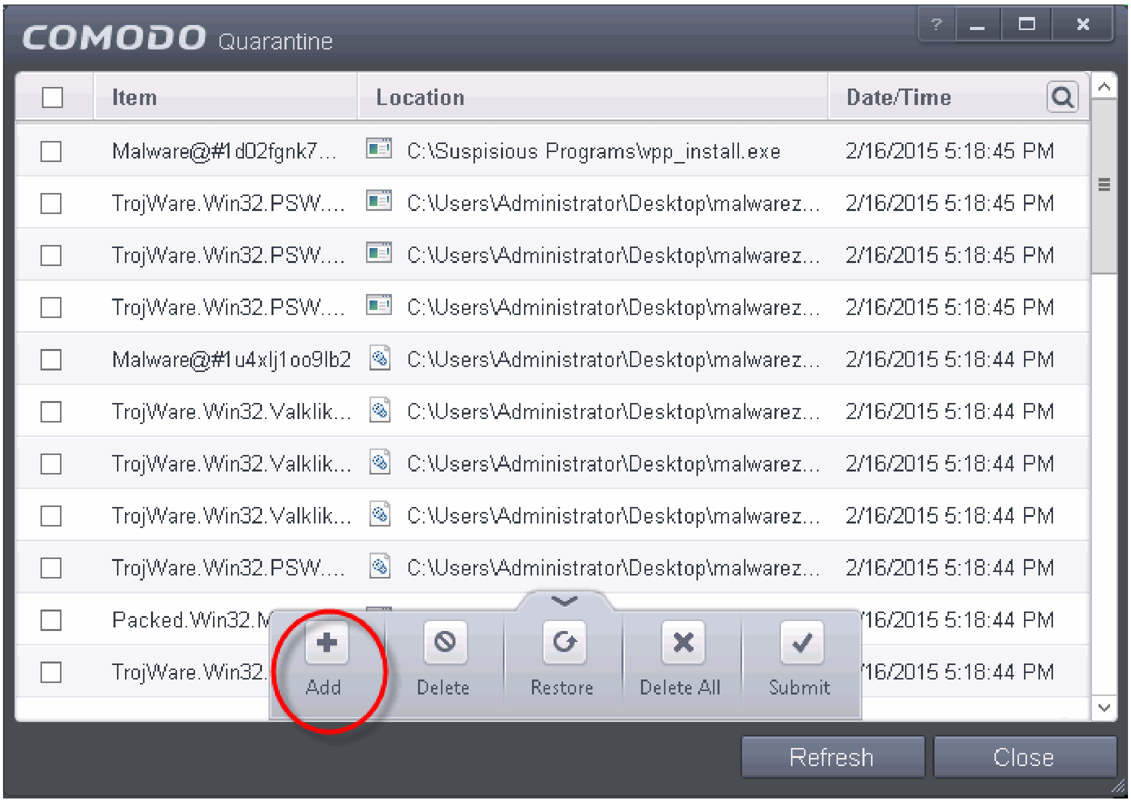
- **Manually add applications, executables or other files, that you do not trust, as a Quarantined item**
- **Delete a selected quarantined item from the system**
- **Restore a quarantined item to oits original location**
- **Delete all quarantined items**
- **Submit selected quarantined items to Comodo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

Manually adding files as Quarantined Items

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

To manually add a Quarantined Item

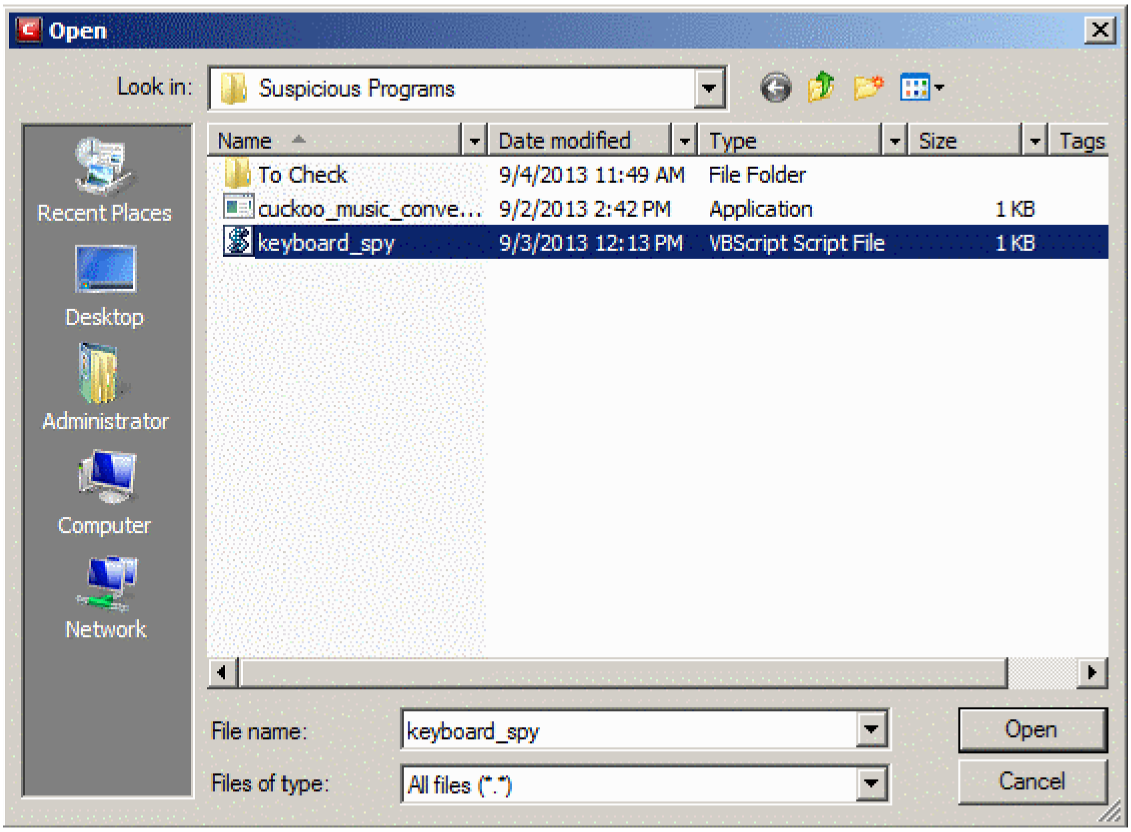
1. Click the handle from the bottom of the Quarantine interface and select 'Add' from the options.



COMODO Quarantine

□	Item	Location	Date/Time
□	Malware@#1d02fgnk7...	C:\Suspisious Programs\vpp_install.exe	2/16/2015 5:18:45 PM
□	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:45 PM
□	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:45 PM
□	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:45 PM
□	Malware@#1u4xlj1oo9lb2	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
□	TrojWare.Win32.Valklik...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
□	TrojWare.Win32.Valklik...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
□	TrojWare.Win32.Valklik...	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
□	TrojWare.Win32.PSW....	C:\Users\Administrator\Desktop\malwarez...	2/16/2015 5:18:44 PM
□	Packed.Win32.M		/16/2015 5:18:44 PM
□	TrojWare.Win32.		/16/2015 5:18:44 PM

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



Name	Date modified	Type	Size	Tags
To Check	9/4/2013 11:49 AM	File Folder		
cuckoo_music_conve...	9/2/2013 2:42 PM	Application	1 KB	
keyboard_spy	9/3/2013 12:13 PM	VBScript Script File	1 KB	

File name: keyboard_spy

Files of type: All files (*.*)

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

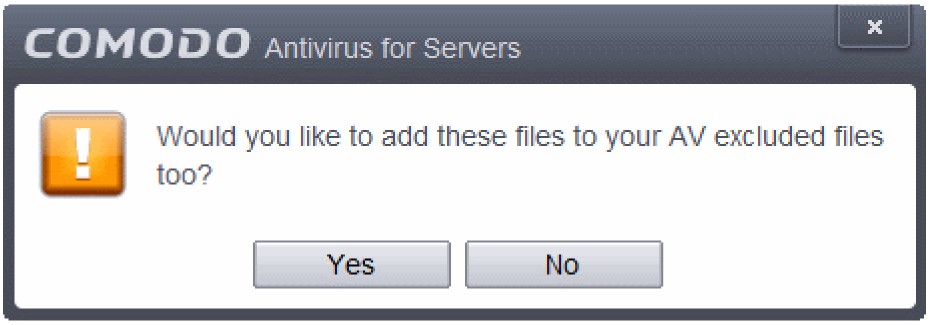
To delete a quarantined item from the system

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

This deletes the file from the system permanently.

To restore a quarantined item to its original location

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



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

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

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

To remove all the quarantined items permanently

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

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

To submit selected quarantined items to Comodo for analysis

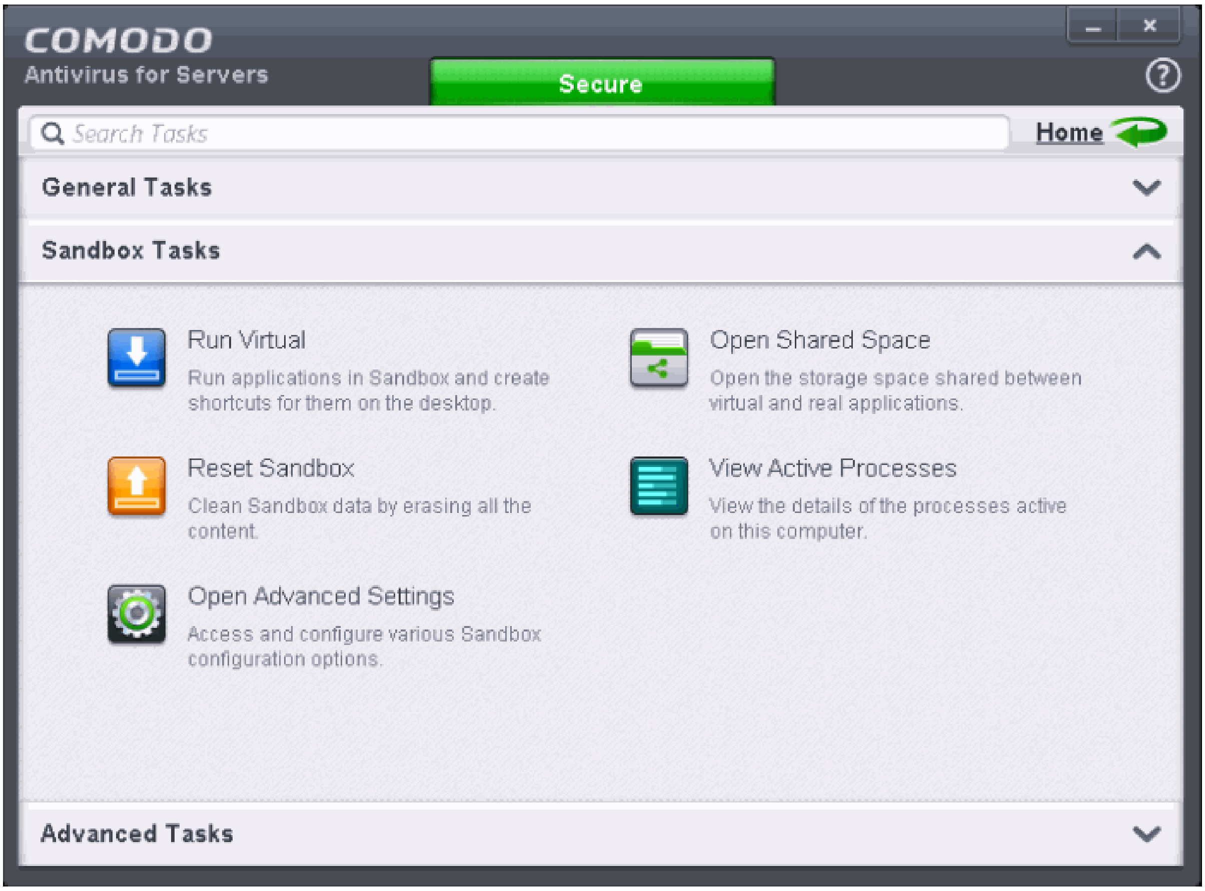
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

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

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

3. Sandbox Tasks – Introduction

Comodo Endpoint Security features a fully functional sandbox environment that allows you to run unknown, untrusted and suspicious applications. Applications executed inside the sandbox will not affect other processes, programs or data on your real computer. In addition to running suspicious applications inside the sandbox on an ad-hoc basis, you can create a desktop shortcut of programs that should always run in the sandbox.



Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.

Open Shared Space
Open the storage space shared between virtual and real applications.

Reset Sandbox
Clean Sandbox data by erasing all the content.

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

Open Advanced Settings
Access and configure various Sandbox configuration options.

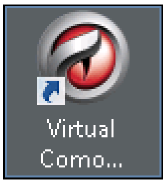
The Sandbox Tasks interface has shortcuts for the following tasks:

- **Run Virtual** - Allows you to run individual applications in the sandbox.
- **Reset Sandbox** - Allows you to clear all data written by programs run inside the sandbox.
- **Open Shared Space -** Opens the folder 'Shared Space' which is shared by your host operating system and the applications running inside the sandbox. The folder is created at the location 'C:\ProgramData\ Shared Space'.
- **Open Advanced Settings** –Access advanced auto-sandbox settings interface, add programs that should always run inside the sandbox and create new auto-sandboxing rules. This is covered in the **Configuring Rules for Auto-Sandbox** section of 'Advanced Settings'.
- **View Active Processes** – Opens the 'Active Process List' interface that displays all currently active processes initiated by applications that are currently running your system. Refer to the section View Active Process List for more details.

3.1. Run an Application in the Sandbox

Comodo Endpoint 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 **the sandboxing process** is not created for it).

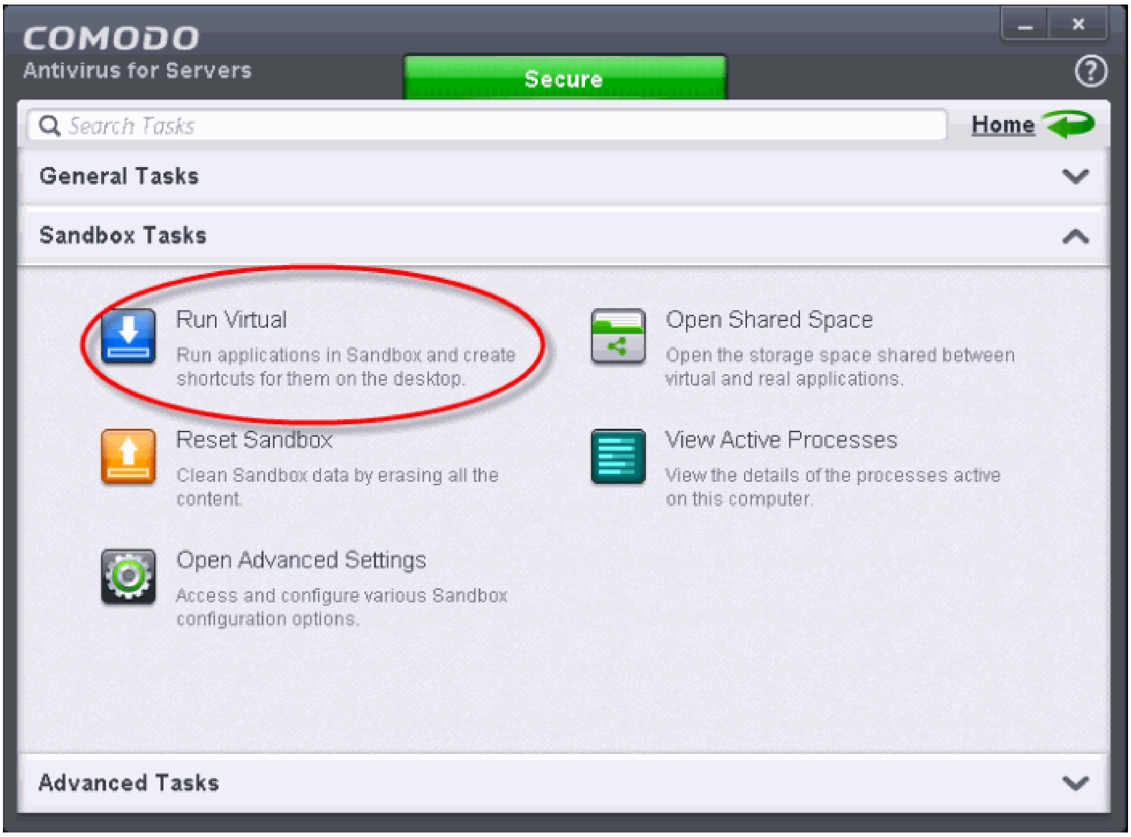
You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:



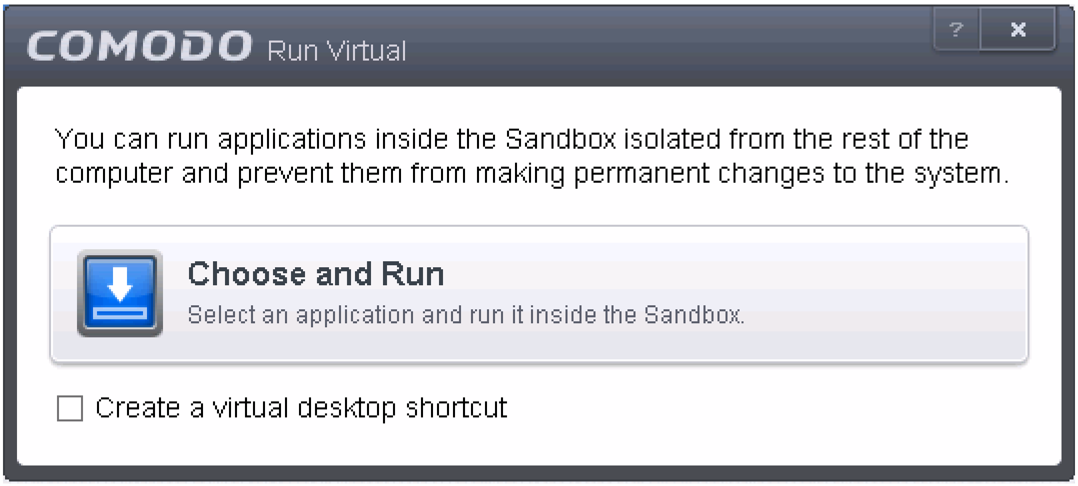
Note: If you wish to run an application in the sandbox on a long-term/permanent basis then **add the file to the sandbox.**

To run an application in the Sandbox

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


COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Sandbox Tasks
Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset Sandbox
Clean Sandbox data by erasing all the content.
View Active Processes
View the details of the processes active on this computer.
Open Advanced Settings
Access and configure various Sandbox configuration options.
Advanced Tasks

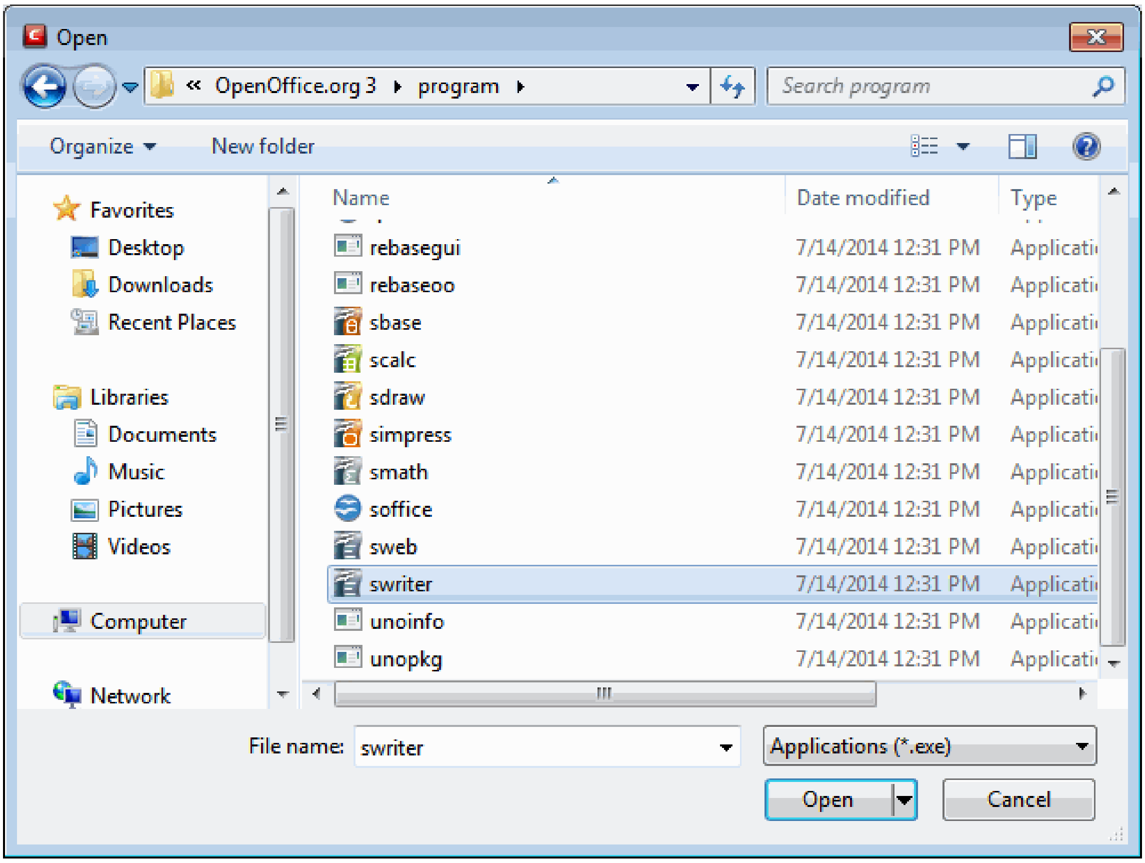
The 'Run Virtual' dialog will be displayed.



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

☐ Create a virtual desktop shortcut

2. To run an application inside the sandbox, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is sandboxed. If you wish to run the application in the sandbox in future, then select 'Create a virtual desktop shortcut'.



Name	Date modified	Type
rebasegui	7/14/2014 12:31 PM	Applicati
rebaseoo	7/14/2014 12:31 PM	Applicati
sbase	7/14/2014 12:31 PM	Applicati
scalc	7/14/2014 12:31 PM	Applicati
sdraw	7/14/2014 12:31 PM	Applicati
simpress	7/14/2014 12:31 PM	Applicati
smath	7/14/2014 12:31 PM	Applicati
soffice	7/14/2014 12:31 PM	Applicati
sweb	7/14/2014 12:31 PM	Applicati
swriter	7/14/2014 12:31 PM	Applicati
unoinfo	7/14/2014 12:31 PM	Applicati
unopkg	7/14/2014 12:31 PM	Applicati

File name: swriter

Applications (*.exe)

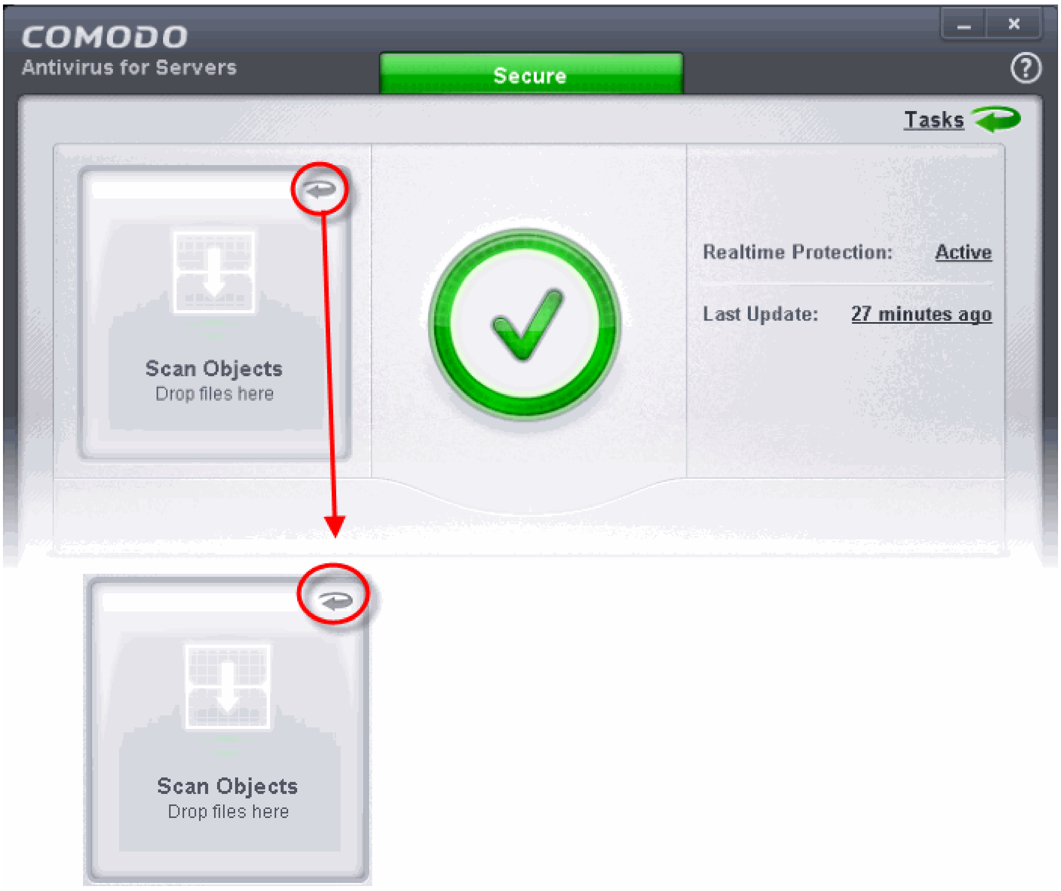
3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

Alternatively, you can run an application inside the sandbox by the following shortcut methods:

- **By dragging-and-dropping the application on to CAVS Home screen**
- **From the context sensitive menu**
- **Running browsers inside sandbox**

Drag-and-drop the application on to CAVS Home Screen

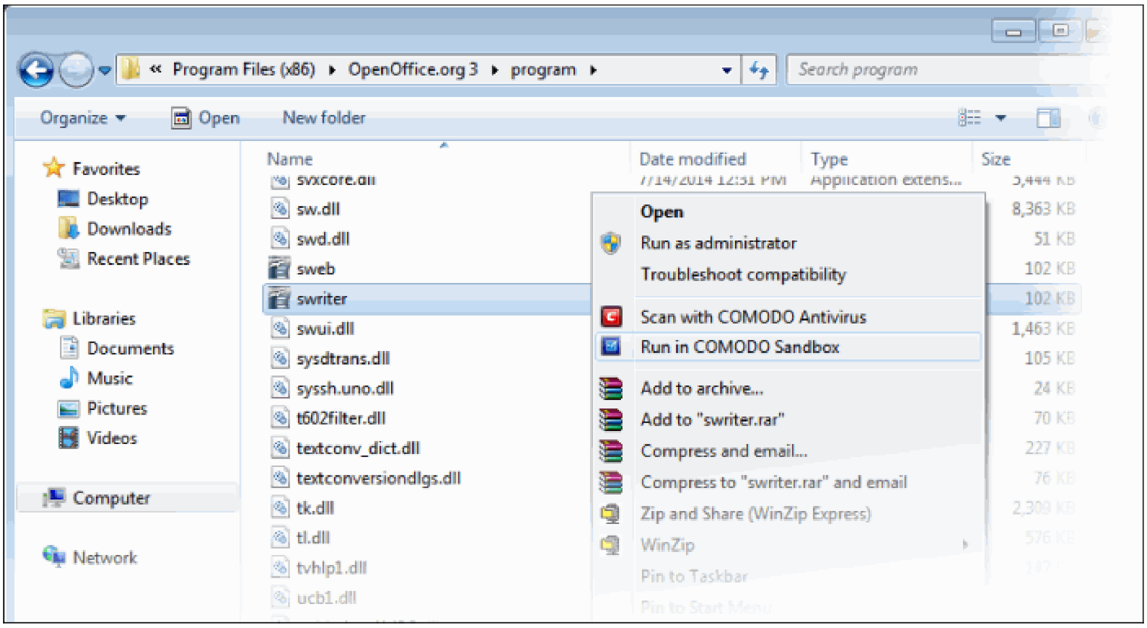
The Home screen of the CAVS interface has a flippable pane at the left side allowing you to run instant scans or run a program in sandbox. To flip the pane to carry out these tasks, just click the curved arrow at the top right side of the pane.



- To run a program in a sandbox, first flip the pane by clicking the curved arrow at the top right side to display 'Sandbox Objects'.
- Now, navigate to the program in your system that you want to run in sandboxed environment and just drag and drop into the box.

Running a program from the context sensitive menu

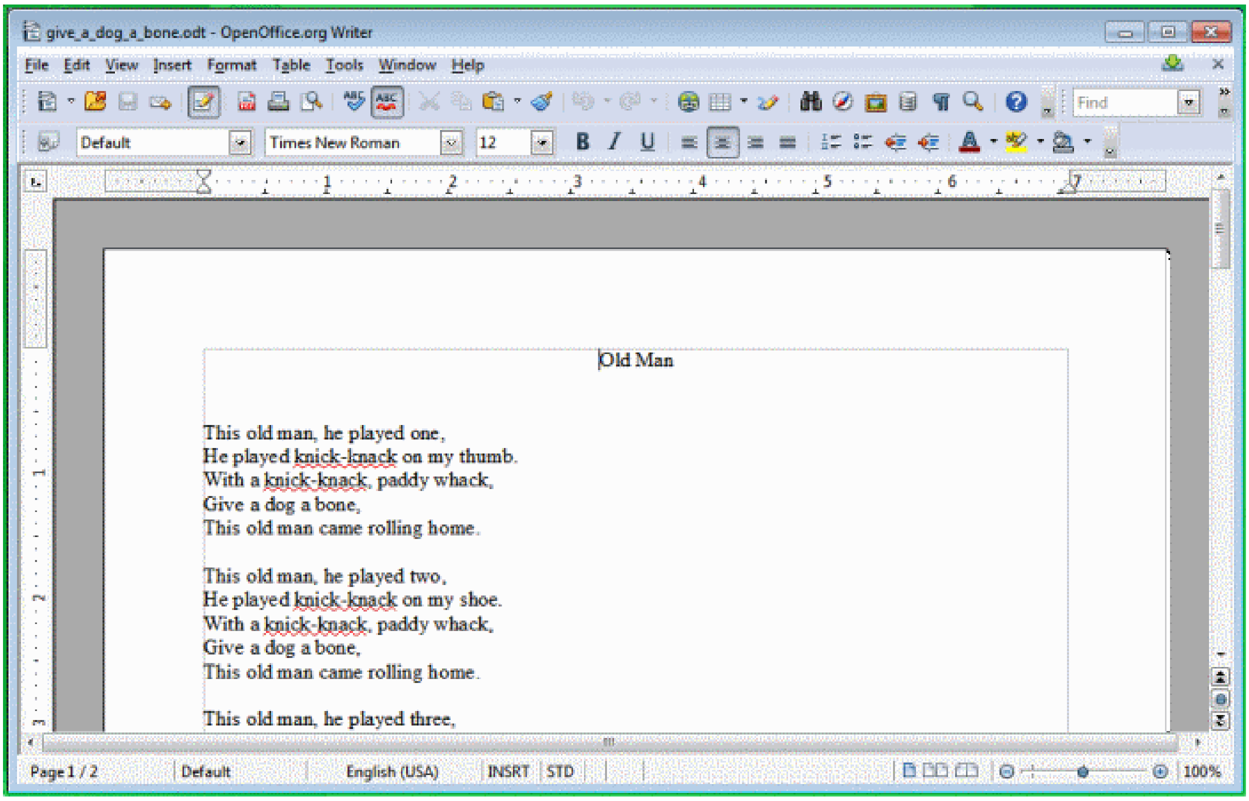
- Navigate to the program in your system that you want to run in sandboxed environment and right click on it



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

Running Browsers inside the Sandbox

The CAVS Desktop Widget displays shortcut icons of the browsers installed in your computer.


give_a_dog_a_bone.odt - OpenOffice.org Writer
File Edit View Insert Format Table Tools Window Help
Find
Default
Times New Roman
12
Page 1 / 2
Default
English (USA)
INSRT
STD
100%

Old Man

This old man, he played one,
He played knick-knack on my thumb.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played two,
He played knick-knack on my shoe.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played three,

- Clicking on a browser icon will start the browser inside the sandbox.

The browser will be started and executed inside the sandbox at 'Fully Virtualized' level. CAVS displays a green border around the windows of programs to indicate that they are running inside the sandbox, if the setting '**Show highlight frame for virtualized programs**' is enabled in **Sandbox Settings**.

The application will run in the Sandbox on this occasion only. If you often want the browser to run sandboxed then create a 'virtual shortcut' for the application by selecting the check-box 'Create a virtual desktop shortcut' in **step 2**. If you wish to run an application in the sandbox on a long-term/permanent basis then **add the file to the Sandbox.**

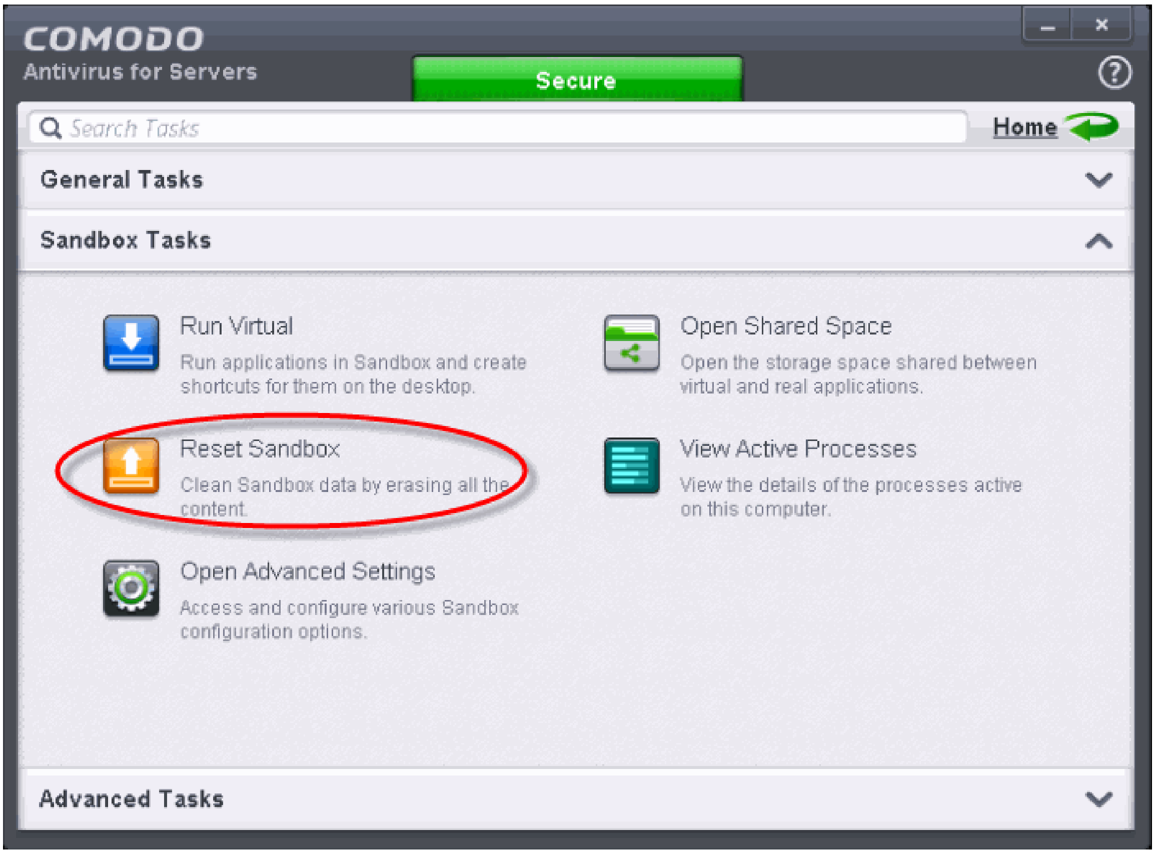
3.2. Reset the Sandbox

Programs running inside the sandbox store the changes to the files accessed by them inside the sandbox so that the changes do not affect the real computer system. Items stored in the sandbox could, depending on your usage patterns, contain malware downloaded from websites or private data in your browsing history. Periodically resetting the sandbox will clear all this data and help protect your privacy and security. If data has accumulated over a long period of time, then resetting the sandbox will also help the sandbox environment operate more smoothly.

The Reset Sandbox option under the Sandbox Tasks allows you to delete all the items stored in the sandbox.

To clear the sandbox

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



Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.

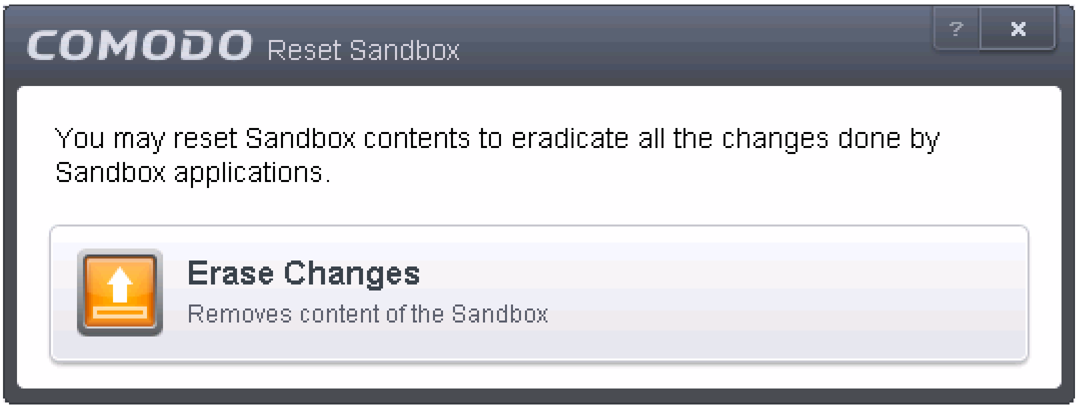
Open Shared Space
Open the storage space shared between virtual and real applications.

Reset Sandbox
Clean Sandbox data by erasing all the content.

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

Open Advanced Settings
Access and configure various Sandbox configuration options.

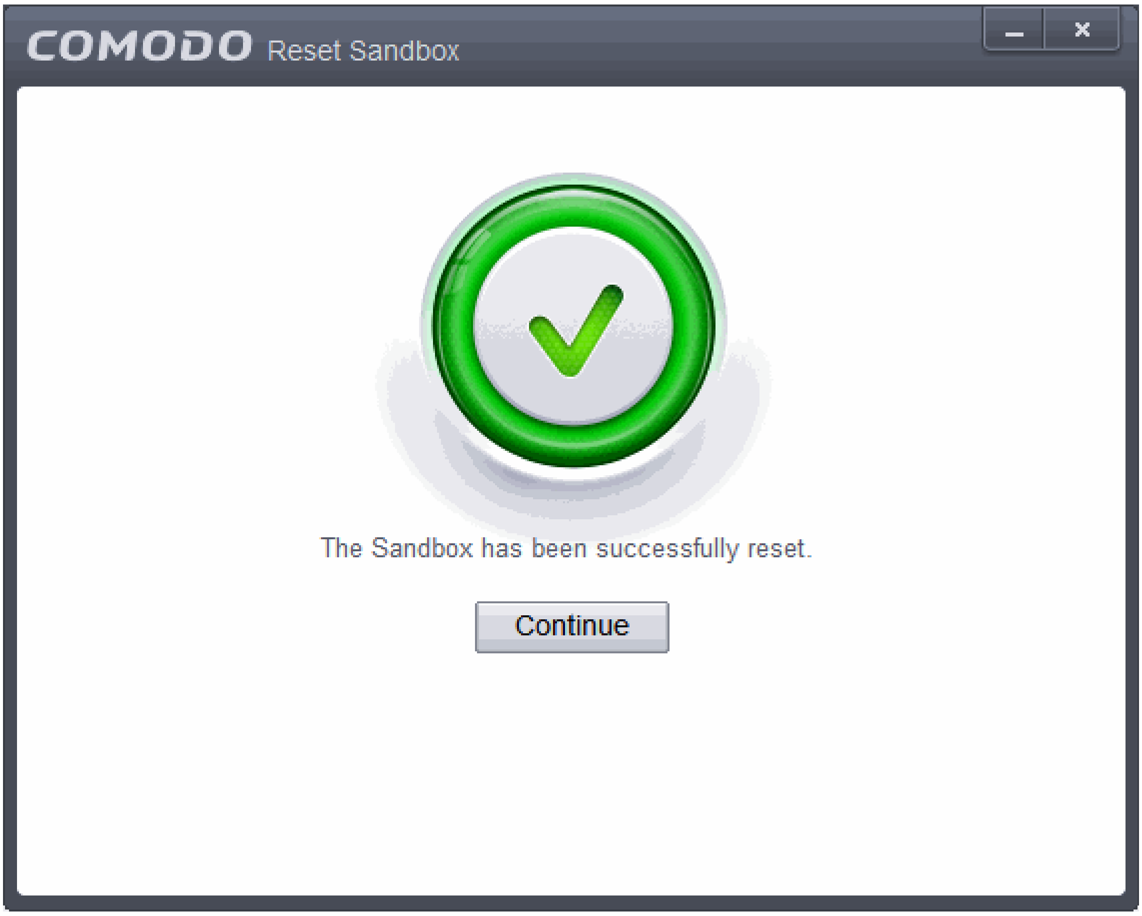
The 'Reset Sandbox' dialog will appear.



You may reset Sandbox contents to eradicate all the changes done by Sandbox applications.

Erase Changes
Removes content of the Sandbox

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



The Sandbox has been successfully reset.

Click 'Continue' to close the dialog.

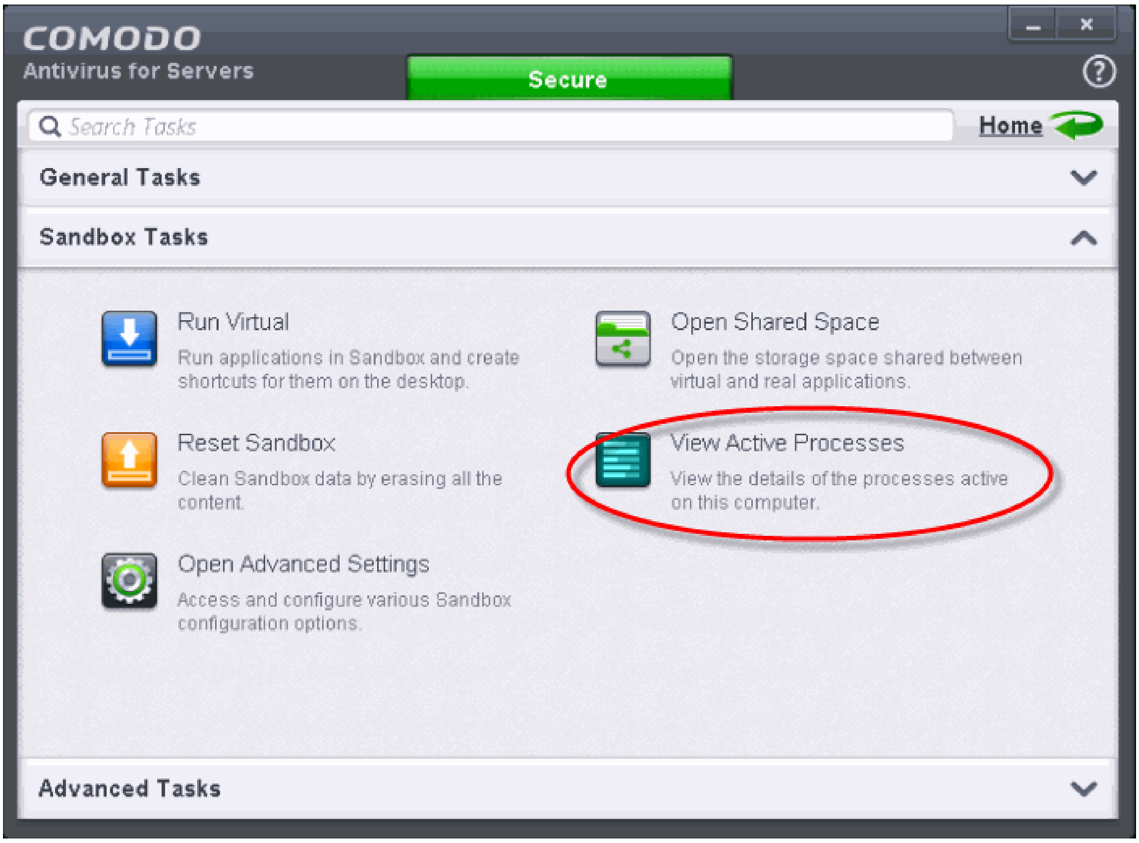
3.3. View Active Process List

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

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

To view Active Process list

- Open the Sandbox Tasks interface and Click 'View Active Processes'.



Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.

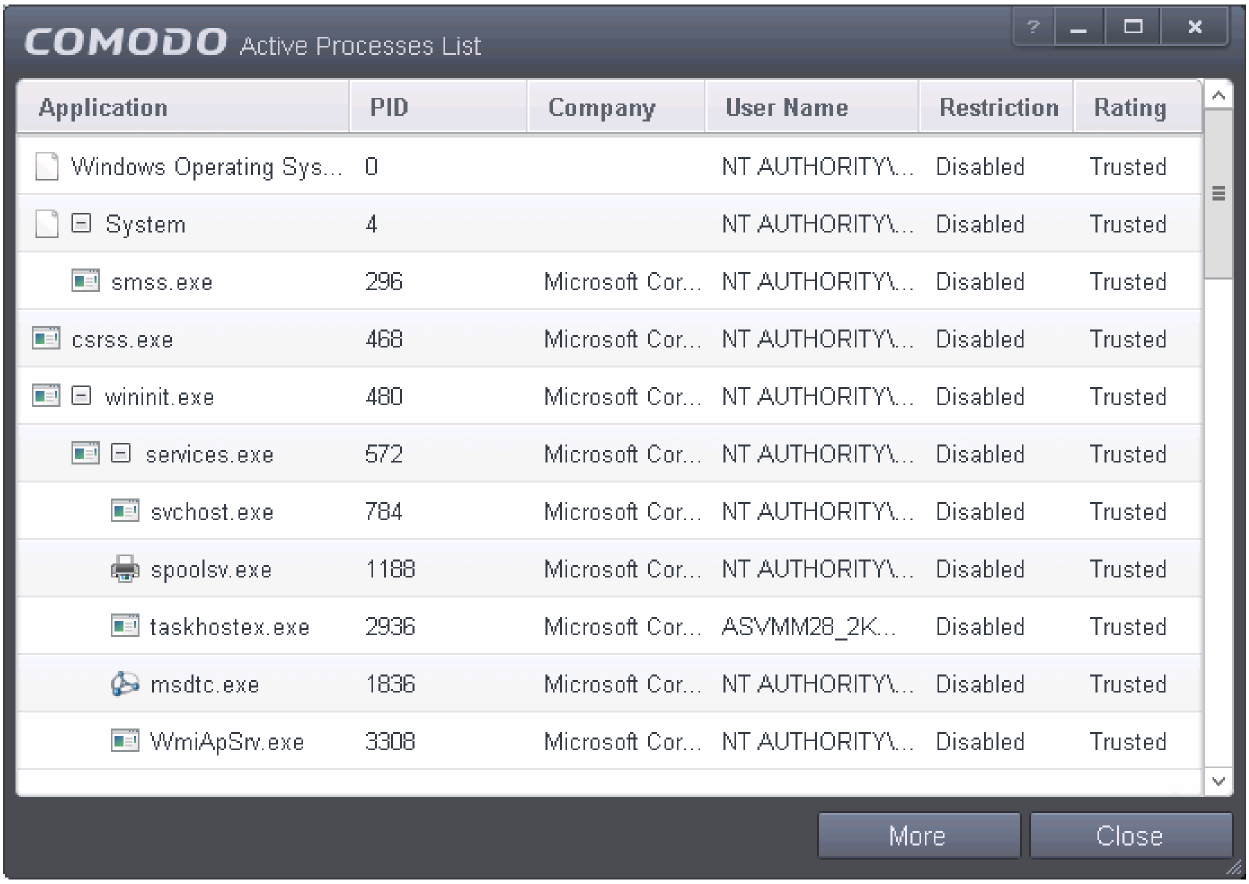
Open Shared Space
Open the storage space shared between virtual and real applications.

Reset Sandbox
Clean Sandbox data by erasing all the content.

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

Open Advanced Settings
Access and configure various Sandbox configuration options.

The Active Processes List screen will be displayed.



COMODO Active Processes List

Application	PID	Company	User Name	Restriction	Rating
Windows Operating Sys...	0		NT AUTHORITY\...	Disabled	Trusted
System	4		NT AUTHORITY\...	Disabled	Trusted
smss.exe	296	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
csrss.exe	468	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
wininit.exe	480	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
services.exe	572	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
svchost.exe	784	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
spoolsv.exe	1188	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
taskhostex.exe	2936	Microsoft Cor...	ASVMM28_2K...	Disabled	Trusted
msdtc.exe	1836	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted
WmiApSrv.exe	3308	Microsoft Cor...	NT AUTHORITY\...	Disabled	Trusted

Column Descriptions

- Application – Displays the names of applications that are currently running.
- PID – Process Identification Number.
- Company – Displays the name of the software developer.
- User Name – The name of the user that started the process.
- Restriction – Displays the level of sandbox setting selected for the program.
- Rating – Displays the rating of the application whether trusted or unknown.

Right-click on any process to:

- Show full path: Displays the location of the executable in addition to it's name.
- Show Sandboxed Only: Displays the details of the sandboxed programs only.

Tip: You can open the Active Process List screen that shows only the processes that are curently running inside the sandbox by clicking the process button from the CAVS widget. Refer to the section **Viewing Active Processes list of Sandboxed Applications** for more details.

- Add to Trusted Files: The selected unknown program is added to CAVS **File list** with Trusted Status. Refer to the section **File list** for more details.
- Online Lookup: The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: Opens the folder containing the file in Windows Explorer.

Clicking the 'More' button at the bottom of the screen will open the Comodo KillSwitch application – an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on your system.

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

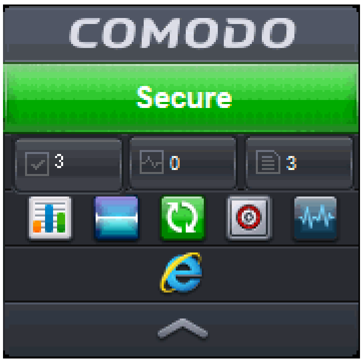
Viewing Active Processes list of Sandboxed Applications

CAVS allows you to view only the processes initiated by the applications that are running inside the sandbox, by clicking a shortcut from the CAVS widget. These applications include:

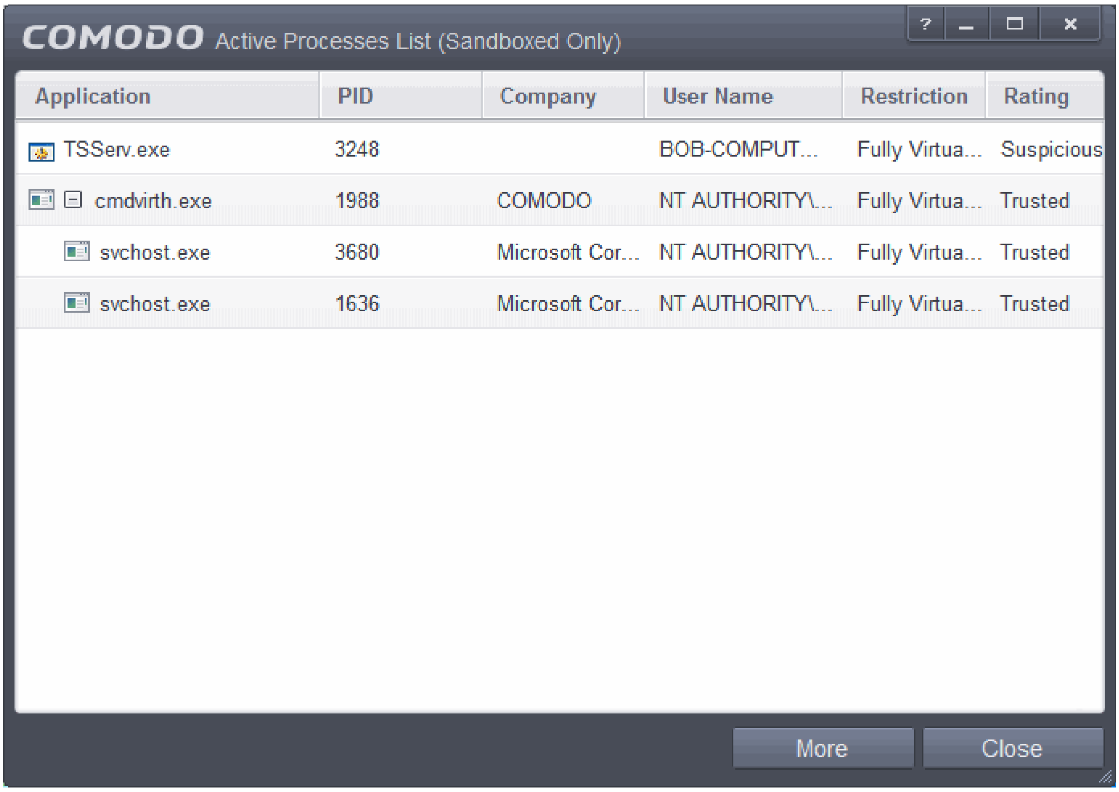
- Auto-Sandbox - Applications that are run inside the sandbox as per the rules defined for them or by default sandbox rules. Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details on defining auto-sandbox rules.
- Run Virtual - Applications that are selected and run in Sandbox. Refer to '**Run an Application in the Sandbox**' for more details.
- Applications that are run inside the sandbox using the context sensitive menu - **Click here** for more details.
- Running browsers inside the sandbox from the Widget - **Click here** for more details.
- Drag-and-drop applications on to CAVS Home Screen - **Click here** for more details.
- Programs that are added manually - Refer to the section '**Configuring Rules for Auto-Sandbox**' for more details.

To view Active Process list of sandboxed applications

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



The Active Processes List (Sandboxed Only) screen will be displayed.


COMODO Active Processes List (Sandboxed Only)

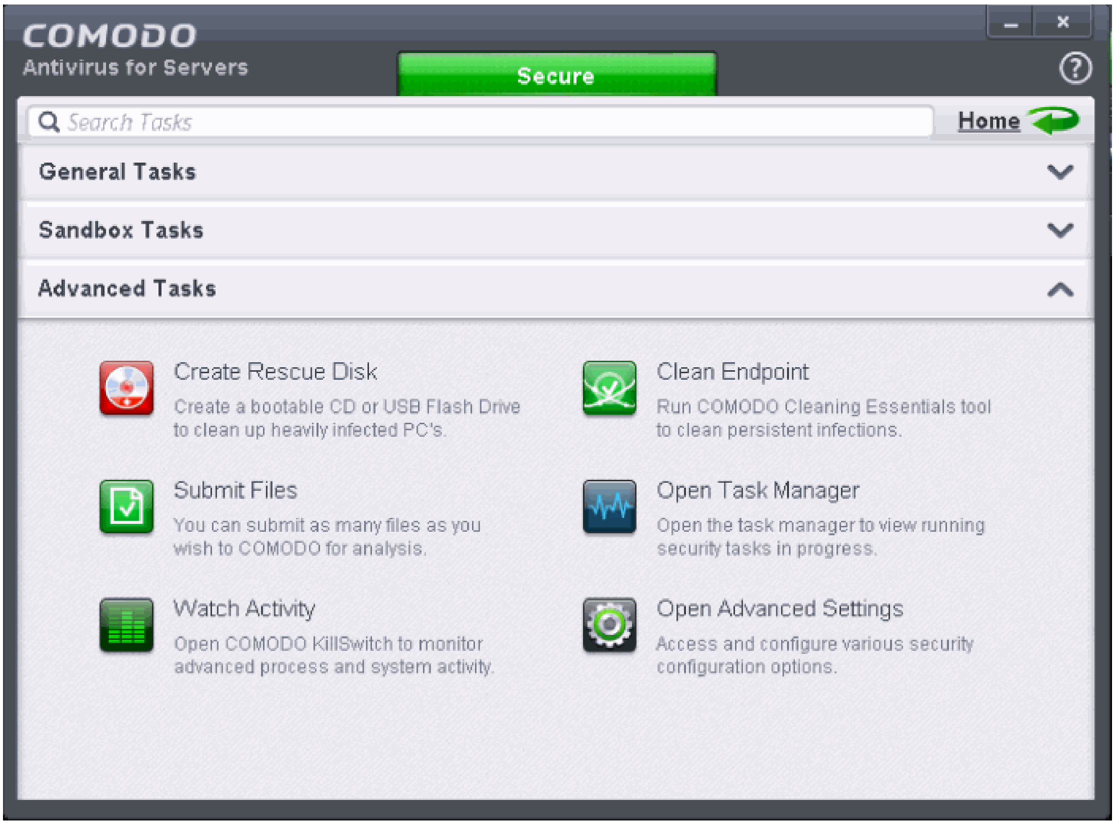
Application	PID	Company	User Name	Restriction	Rating
TSServ.exe	3248		BOB-COMPUT...	Fully Virtua...	Suspicious
cmdvirth.exe	1988	COMODO	NT AUTHORITY\...	Fully Virtua...	Trusted
svchost.exe	3680	Microsoft Cor...	NT AUTHORITY\...	Fully Virtua...	Trusted
svchost.exe	1636	Microsoft Cor...	NT AUTHORITY\...	Fully Virtua...	Trusted

4. Advanced Tasks - Introduction

The 'Advanced Tasks' area allows you modify the overall configuration of CAVS and to take advantage of several other Comodo utilities. Click the following links to find out more about each item:

- **Create Rescue Disk - Burn a bootable ISO that lets you run virus scans in pre-boot environments**
- **Submit Files - Directly Submit unknown/suspicious files to Comodo for analysis**
- **Watch Activity - Use Comodo Killswitch to identify unsafe processes and manage system activity**
- **Clean Endpoint - Deploy Comodo Cleaning Essentials to eradicate persistent infections from your server**
- **Open Advanced Settings - Configure overall behavior, define custom rulesets and much more**

Some of these utilities require the download and installation of additional setup files. After installation, the utility will start directly next time you click the button.



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Open Task Manager
Open the task manager to view running security tasks in progress.

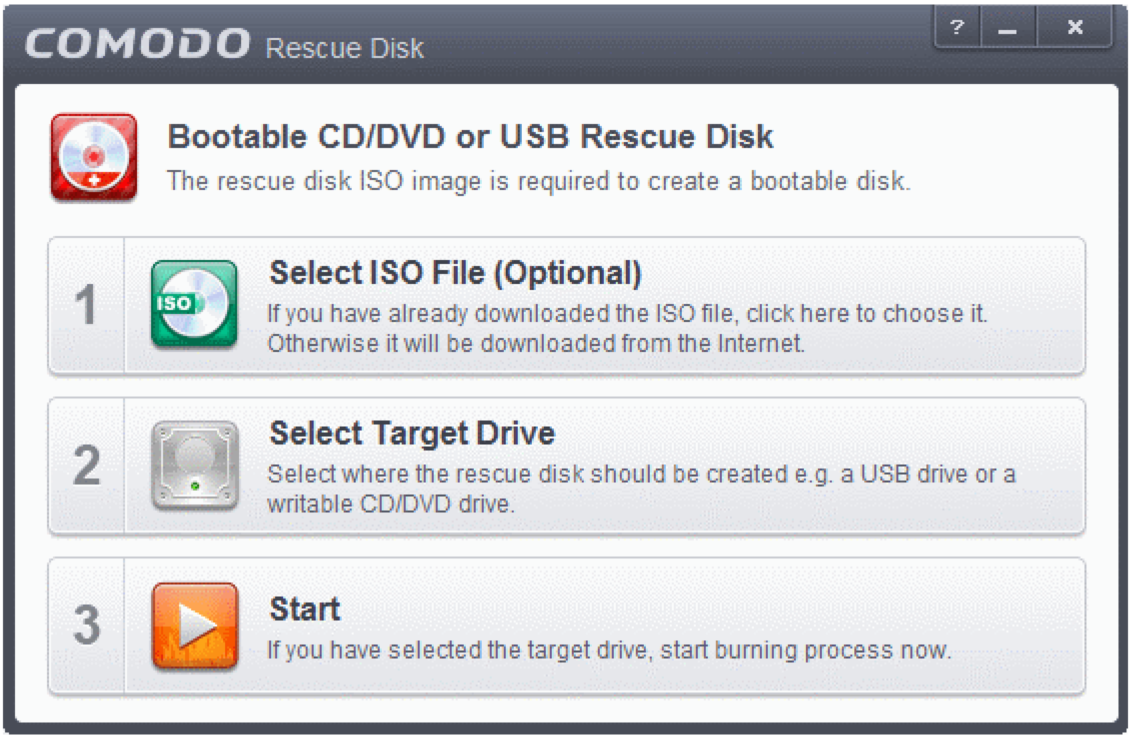
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

4.1. Create a Rescue Disk

Comodo Rescue Disk (CRD) is a bootable disk image that allows users to run virus scans in a pre-boot environment (before Windows loads). CRD runs Comodo Cleaning Essentials on a lightweight distribution of the Linux operating system. It is a powerful virus, spyware, rootkit scanner and cleaner which works in both GUI and text mode. The tool can provide a more comprehensive and thorough scan than regular malware cleaning applications because it cleans your server before server software is loaded. CRD is intended to be used when malware embeds itself so deeply into your server that regular AV software cannot remove it. The rescue disk is also very effective at removing infections that are preventing Windows Server from booting in the first place. Apart from the virus scanner, CRD also provides tools to explore files in your hard drive, take screen-shots and browse web pages.

- Clicking the 'Create Rescue Disk' button in CAVS 'Advanced Settings' opens a utility that allows you to download and burn the CRD iso to a CD/DVD, USB or other drive. **Click here** to jump to a walk-through of this process



Bootable CD/DVD or USB Rescue Disk

The rescue disk ISO image is required to create a bootable disk.

1 **Select ISO File (Optional)**
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.

2 **Select Target Drive**
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.

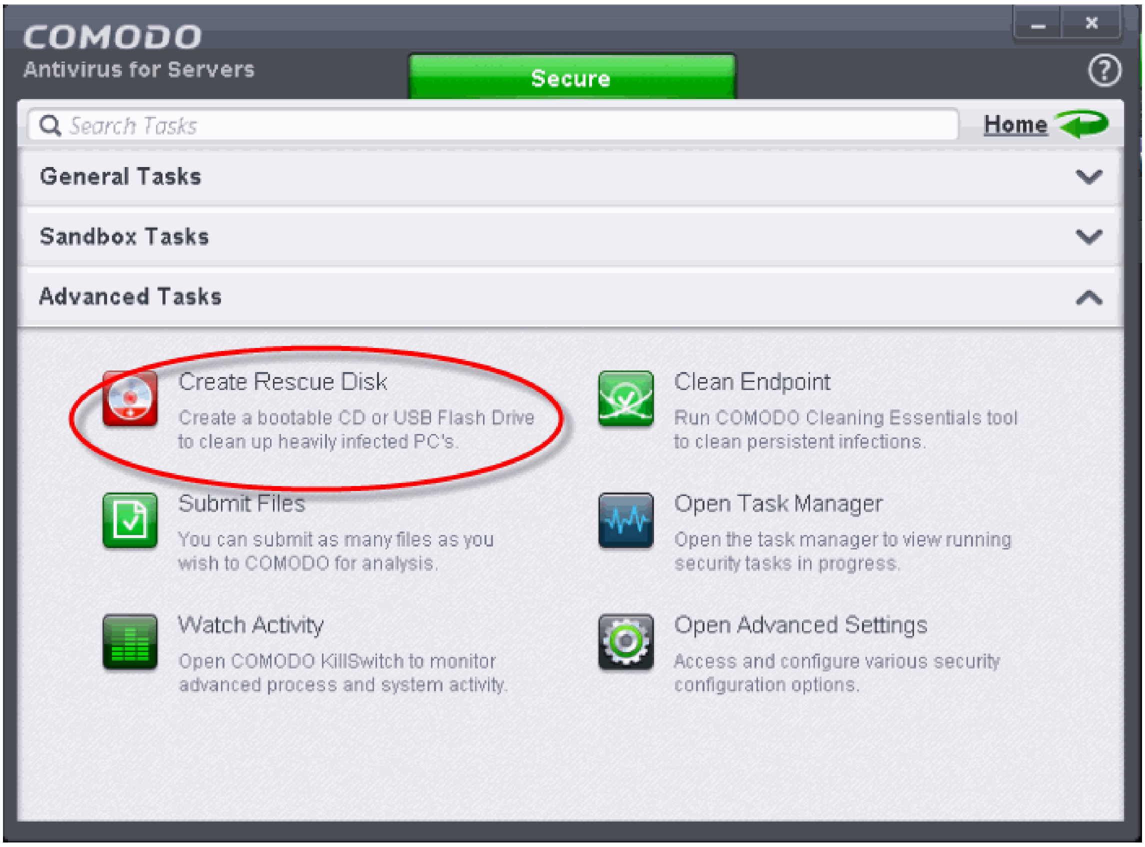
3 **Start**
If you have selected the target drive, start burning process now.

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

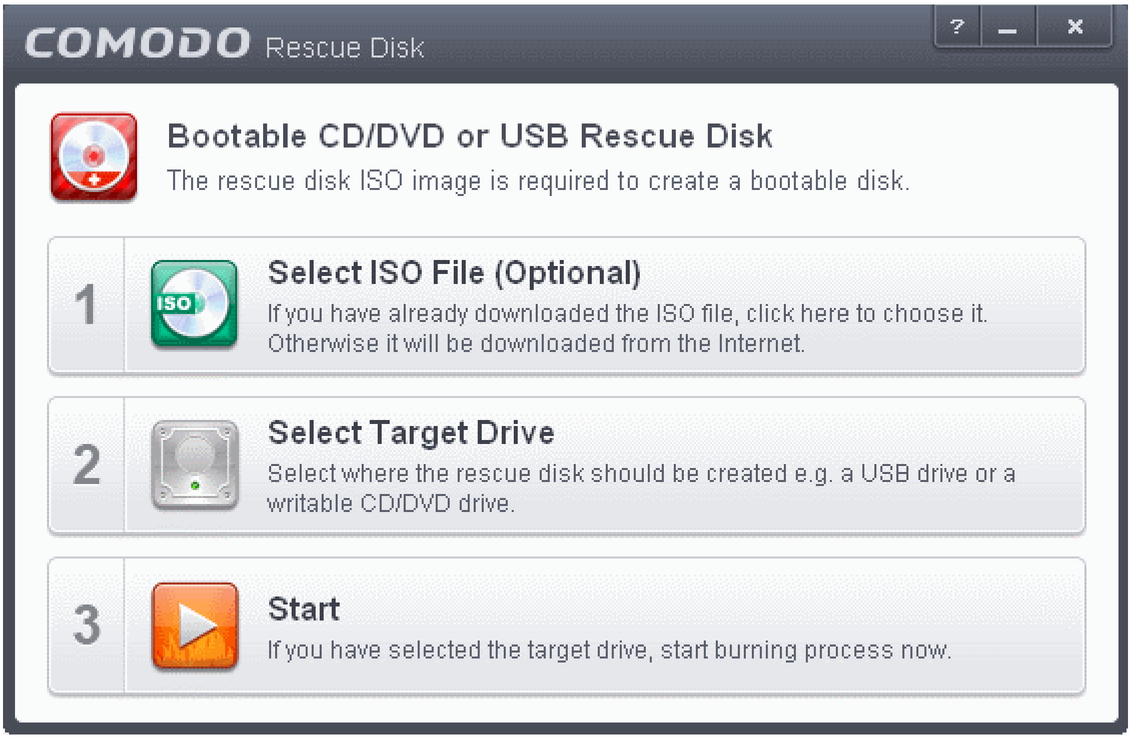
- Details of how to change boot order on your server can be found in the Rescue Disk user guide at **http://help.comodo.com/topic-170-1-493-5227-Changing-Boot-Order.html**
- Details of how to initiate CRD after booting can be found at **http://help.comodo.com/topic-170-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html**
- Details of how to start running scans on your pre-boot environment are available at **http://help.comodo.com/topic-170-1-493-5216-Starting-Comodo-Cleaning-Essentials.html** and **http://help.comodo.com/topic-170-1-493-5217-CCE-Interface.html**

4.1.1.Downloading and Burning Comodo Rescue Disk

To create a Comodo Rescue Disk, Click 'Create Rescue Disk' button from the Advanced Tasks interface.


COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Sandbox Tasks
Advanced Tasks
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
Open Task Manager
Open the task manager to view running security tasks in progress.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
Open Advanced Settings
Access and configure various security configuration options.

The Comodo Rescue Disk interface will open.


COMODO Rescue Disk
Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.
1
ISO
Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.
2
Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.
3
Start
If you have selected the target drive, start burning process now.

The Comodo Rescue Disk interface displays the steps involved in creation of a new Rescue Disk on a CD/DVD or in a USB drive.

Step 1- Select the ISO file

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

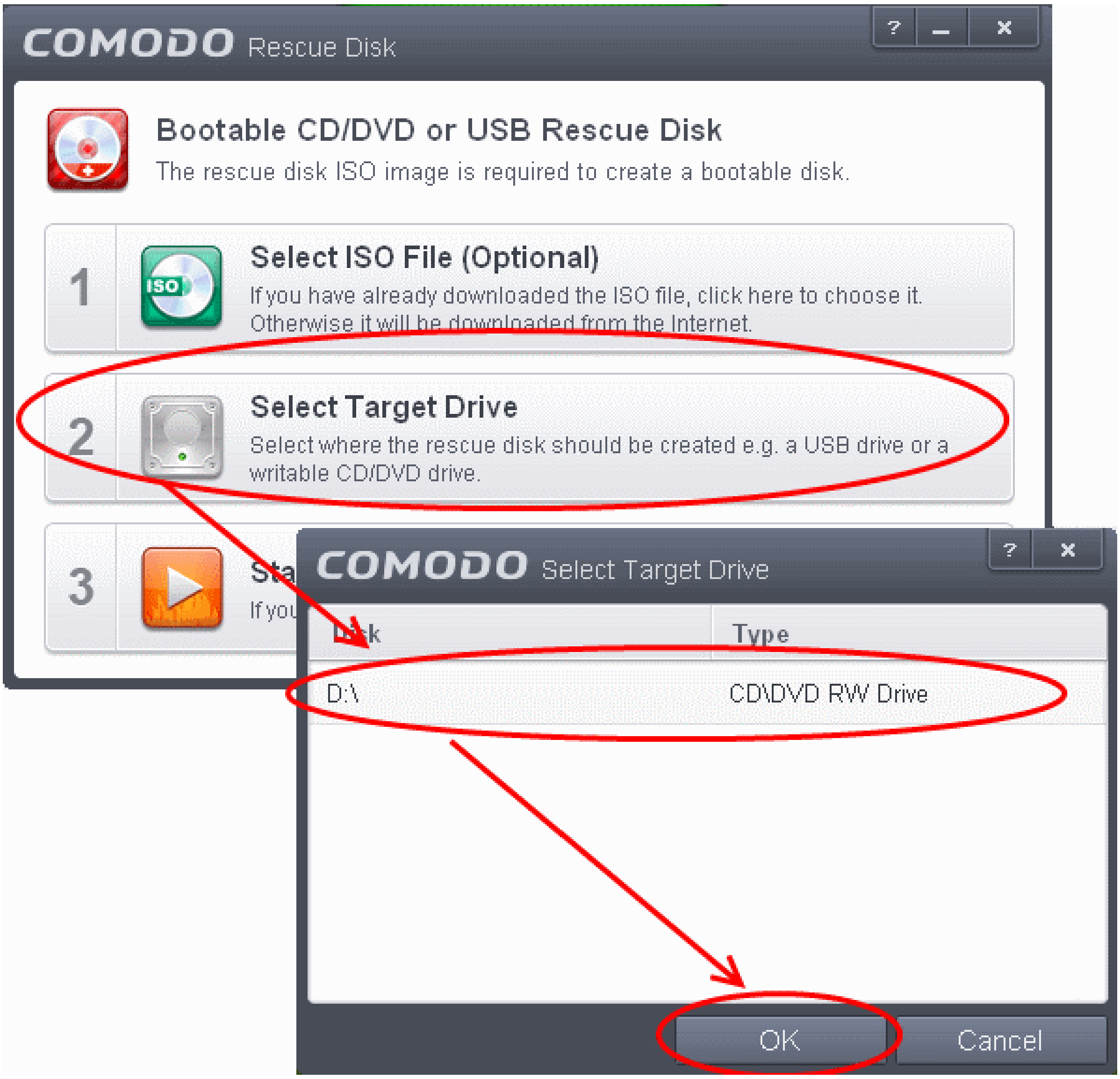
- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

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

To burn the Rescue disk on a CD or a DVD

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



COMODO Rescue Disk

Bootable CD/DVD or USB Rescue Disk

The rescue disk ISO image is required to create a bootable disk.

1 Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.

2 Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.

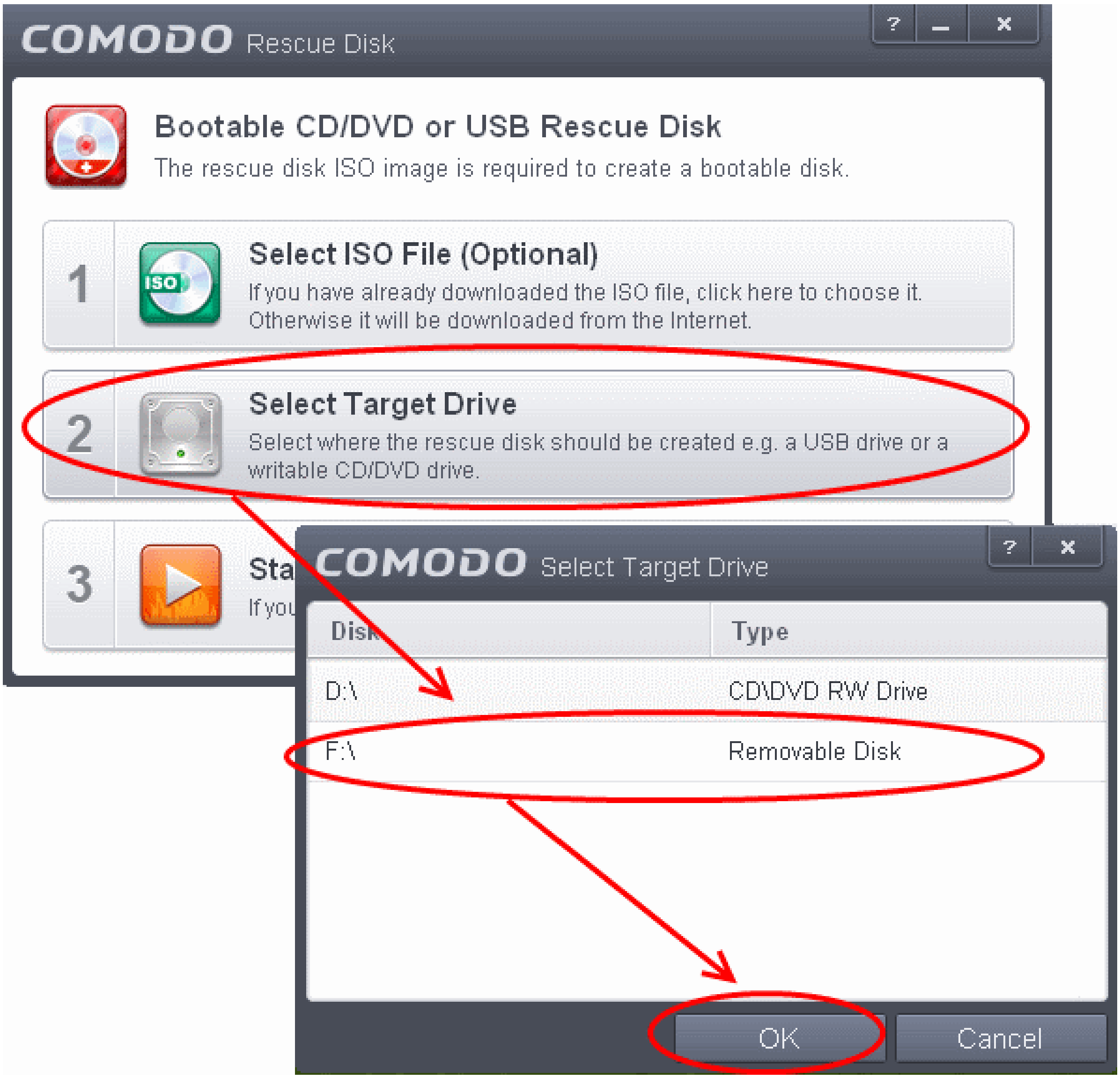
3 Sta... If you...

COMODO Select Target Drive

Disk	Type
D:\	CD\DVD RW Drive

To burn the Rescue disk on a USB Drive

- Insert a formatted USB memory to a free USB port on your computer
- Click 'Select Target Drive' from the 'Comodo Rescue Disk' interface and select the drive from the Select Disk dialog

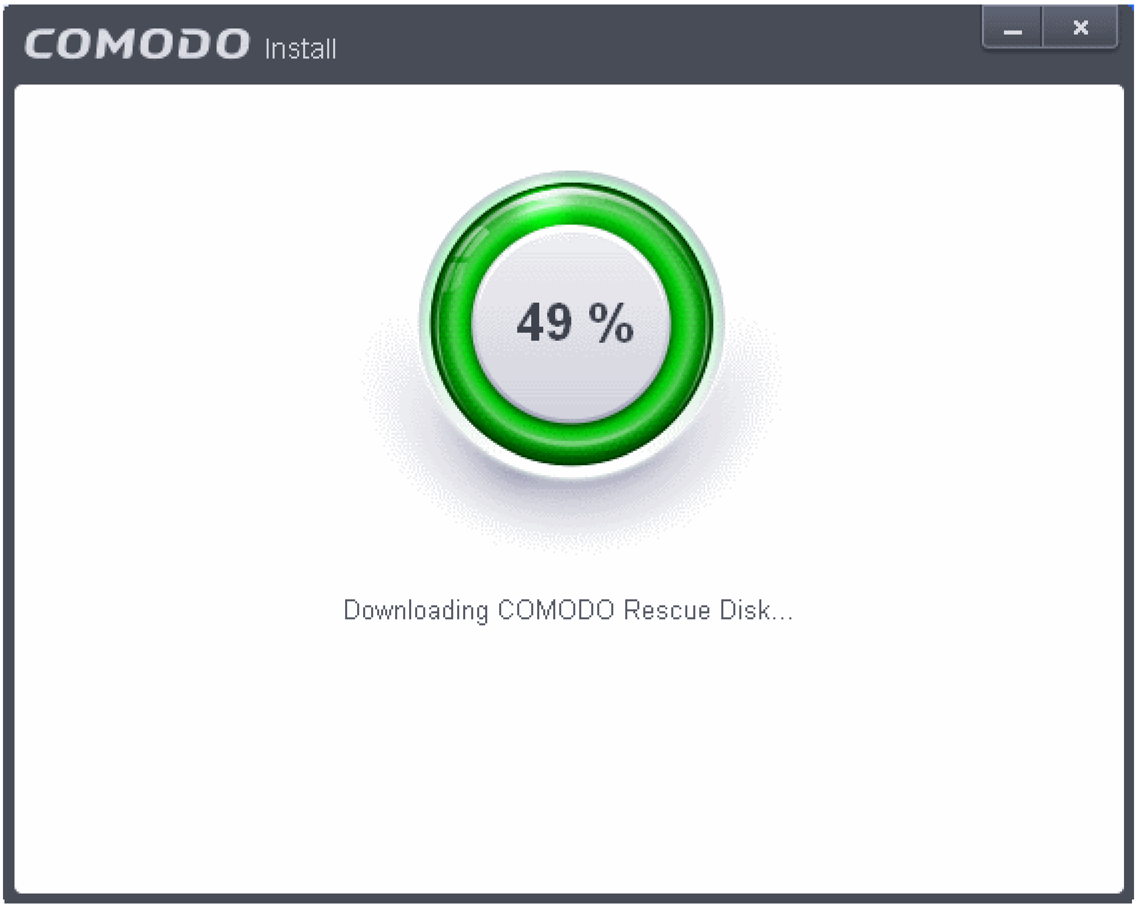


COMODO Rescue Disk
Bootable CD/DVD or USB Rescue Disk
The rescue disk ISO image is required to create a bootable disk.
1
Select ISO File (Optional)
If you have already downloaded the ISO file, click here to choose it. Otherwise it will be downloaded from the Internet.
2
Select Target Drive
Select where the rescue disk should be created e.g. a USB drive or a writable CD/DVD drive.
3
Sta
If you
COMODO Select Target Drive
OK
Cancel

Disk	Type
D:\	CD\DVD RW Drive
F:\	Removable Disk

Step 3 - Burn the Rescue Disk

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

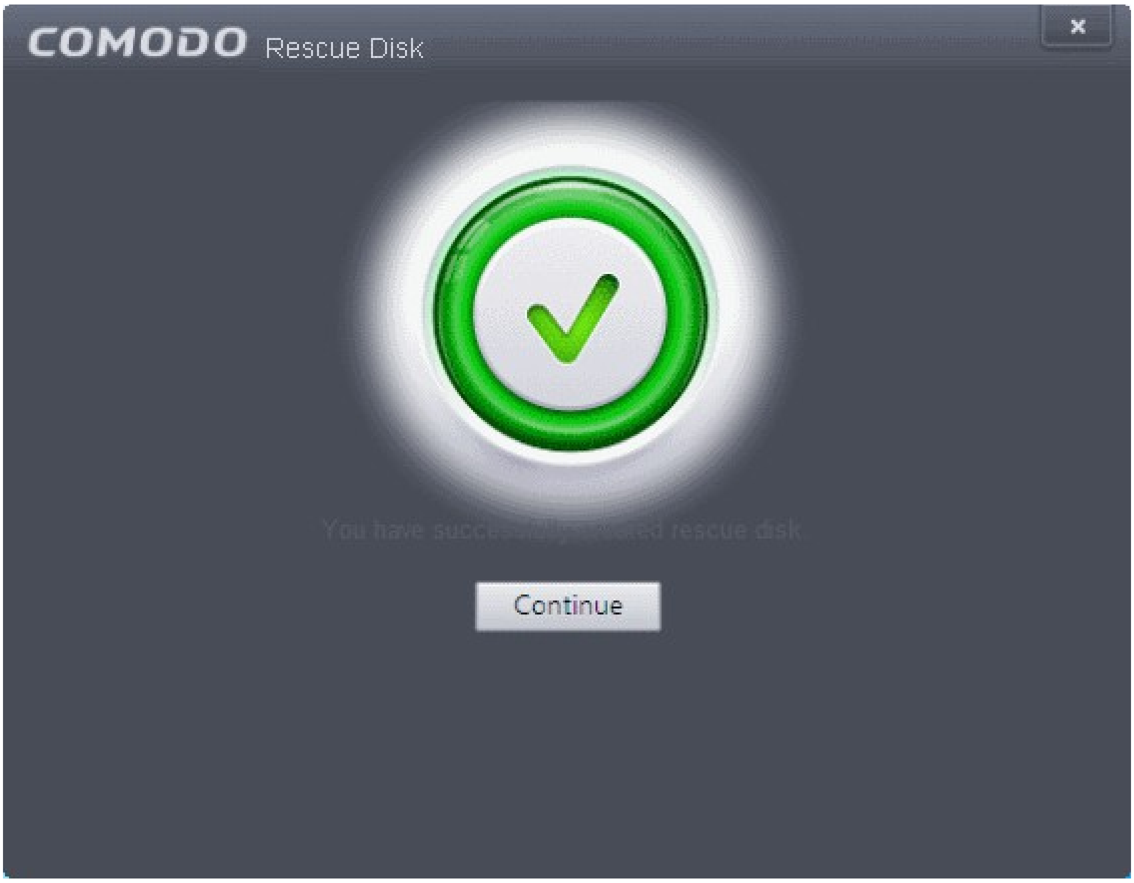


Downloading COMODO Rescue Disk...

On completion, the files will be written on to the CD/DVD or the USB Drive.

Creating rescue disk

- Wait till the completion of the process. Do not eject the CD/DVD or the USB drive. On completion of the process, the CD/DVD will be ejected automatically.



You have successfully created rescue disk

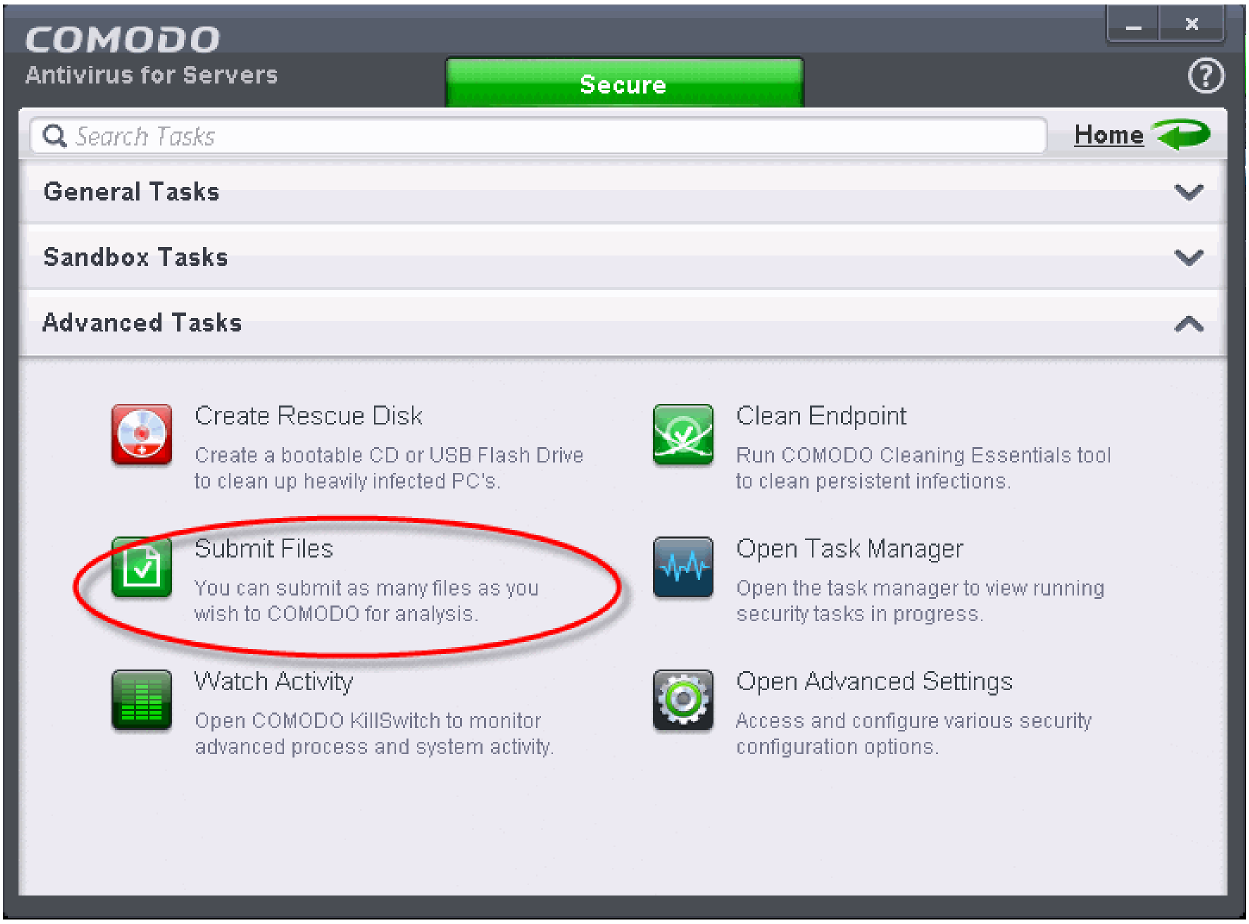
Your Bootable Comodo Rescue Disk is created. Click 'Continue' to go back to CAVS interface.

4.2. Submit Files

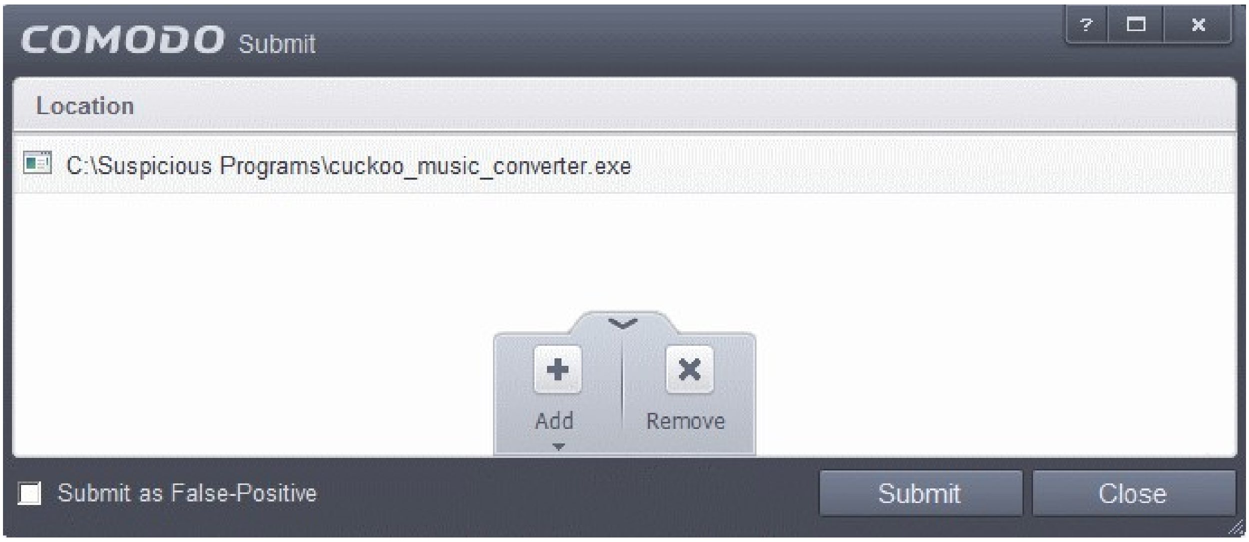
As the name suggests, the 'Submit Files' interface allows you to send as many files as you wish to Comodo for analysis. Files which CAVS classifies as 'Unknown' or 'Unrecognized' are not in the Comodo safe list but have also not been identified as known malware. By sending these files to Comodo, you allow our team to analyze them and classify them as either 'Safe' or 'Malicious'. You can also submit files you suspect of being 'false positives' (those files that you feel CAVS has incorrectly identified as malware). Subsequent to classification, they will be added to the white or black list accordingly.

Note: Unrecognized files can also be submitted from the '**File List**' interface should you prefer.

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


COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Sandbox Tasks
Advanced Tasks
Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.
Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.
Submit Files
You can submit as many files as you wish to COMODO for analysis.
Open Task Manager
Open the task manager to view running security tasks in progress.
Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.
Open Advanced Settings
Access and configure various security configuration options.

The 'Submit' interface will open.



C:\Suspicious Programs\cuckoo_music_converter.exe

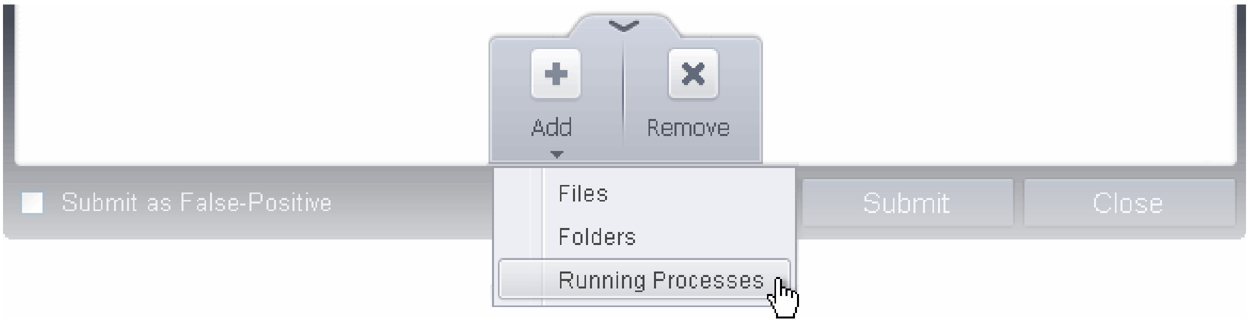
□ Submit as False-Positive

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

- **Add** - Allows you to add files to the 'Submit Files' list
- **Remove** - Allows you to remove files from the 'Submit Files' list

To add new file(s) to 'Submit Files' list

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



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

- **Files -** Allows you to navigate to the file or executable of the program you wish to add.
- **Folders -** Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'Trusted Files' list.
- **Running Processes -** Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'Trusted Files' list.

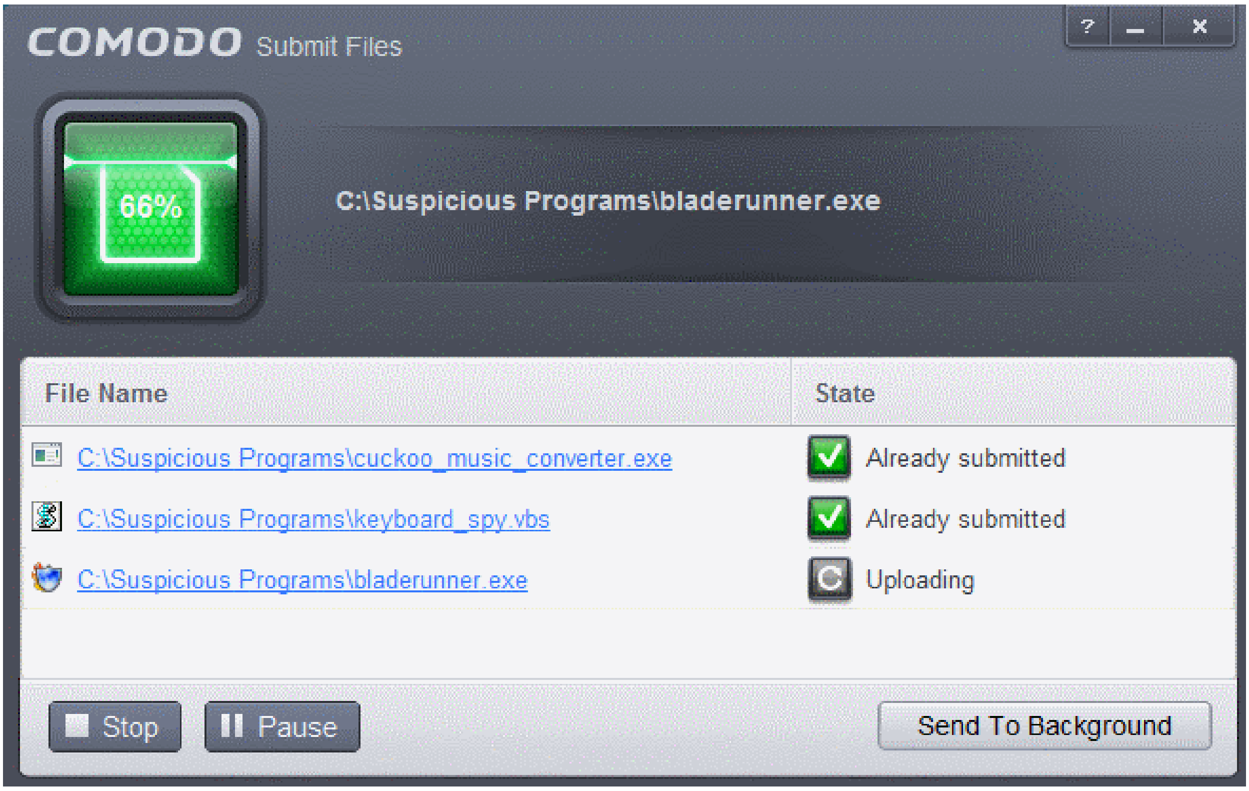
- Repeat the process to add more files and to submit them at-once.

To remove the files from 'Submit Files' list

- Select the file from the list
- Click the handle from the bottom center and select Remove

After adding the files you want to submit, click 'Submit' button. If you want to submit the files as False Positives to Comodo, select the 'Submit as False-Positive check' box.

The files will be submitted and the progress will be displayed

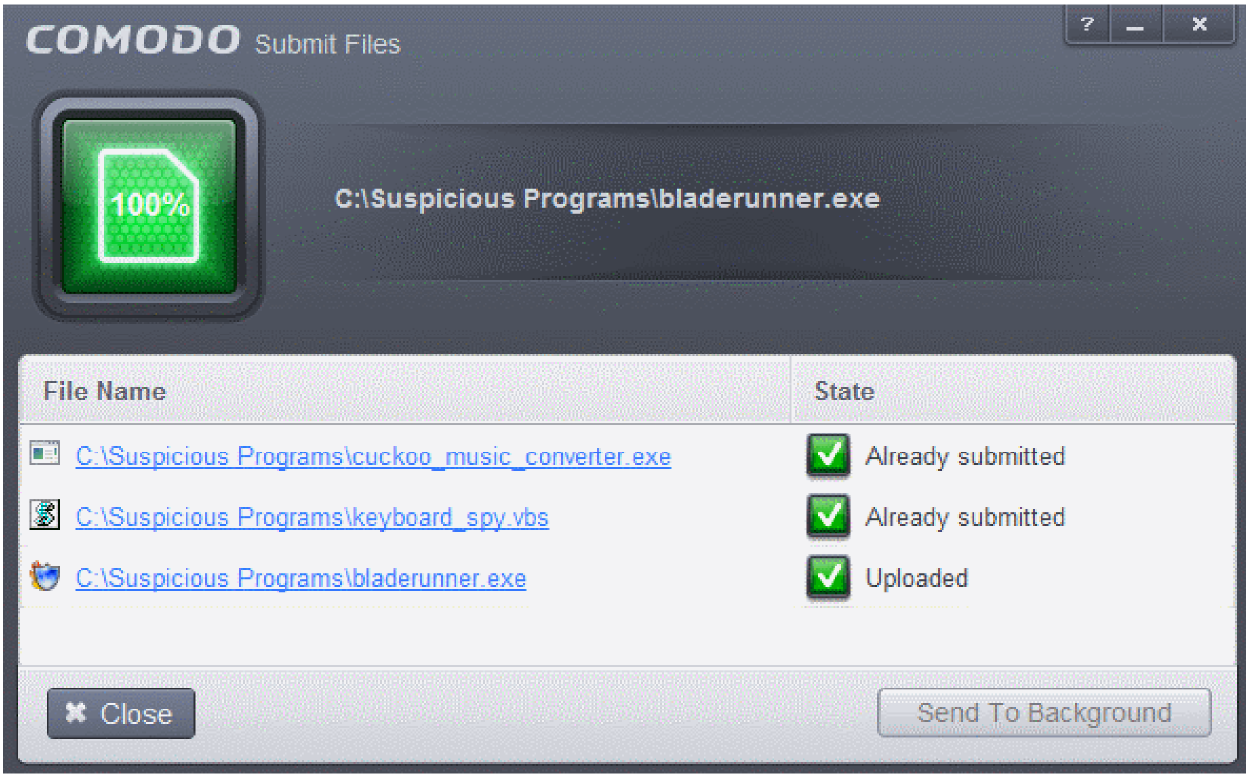


C:\Suspicious Programs\bladerunner.exe

File Name	State
C:\Suspicious Programs\cuckoo_music_converter.exe	✓ Already submitted
C:\Suspicious Programs\keyboard_spy.vbs	✓ Already submitted
C:\Suspicious Programs\bladerunner.exe	Uploading

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

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by our technicians. The results screen displays these results on completion:



File Name	State
C:\Suspicious Programs\cuckoo_music_converter.exe	✓ Already submitted
C:\Suspicious Programs\keyboard_spy.vbs	✓ Already submitted
C:\Suspicious Programs\bladerunner.exe	✓ Uploaded

- 'Uploaded' - The file's signature was not found in the list of files that are waiting to be tested and was therefore uploaded from your machine to our research labs.
- 'Already submitted' - The file has *already* been submitted to our labs by another CAVS user and was not uploaded from your machine at this time.

Comodo will analyze all submitted files. If they are found to be trustworthy, they will be added to the Comodo safe list (i.e. white-listed). Conversely, if they are found to be malicious then they will be added to the database of virus signatures (i.e. black-listed).

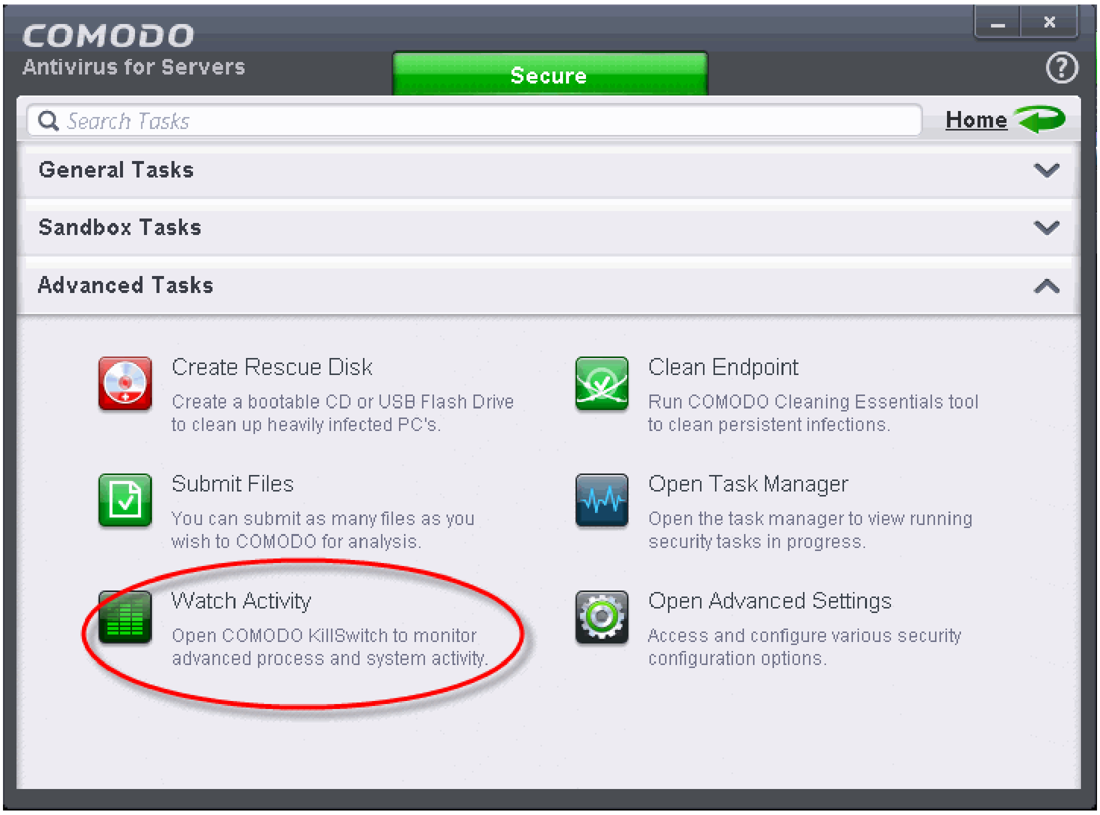
The list of files submitted from your computer can be viewed from the **Submitted Files** interface.

4.3. Identify and Kill Unsafe Running Processes

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

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

Comodo KillSwitch can be directly accessed from the CAVS interface by clicking the 'Watch Activity' button in the 'Advanced Tasks' interface.



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

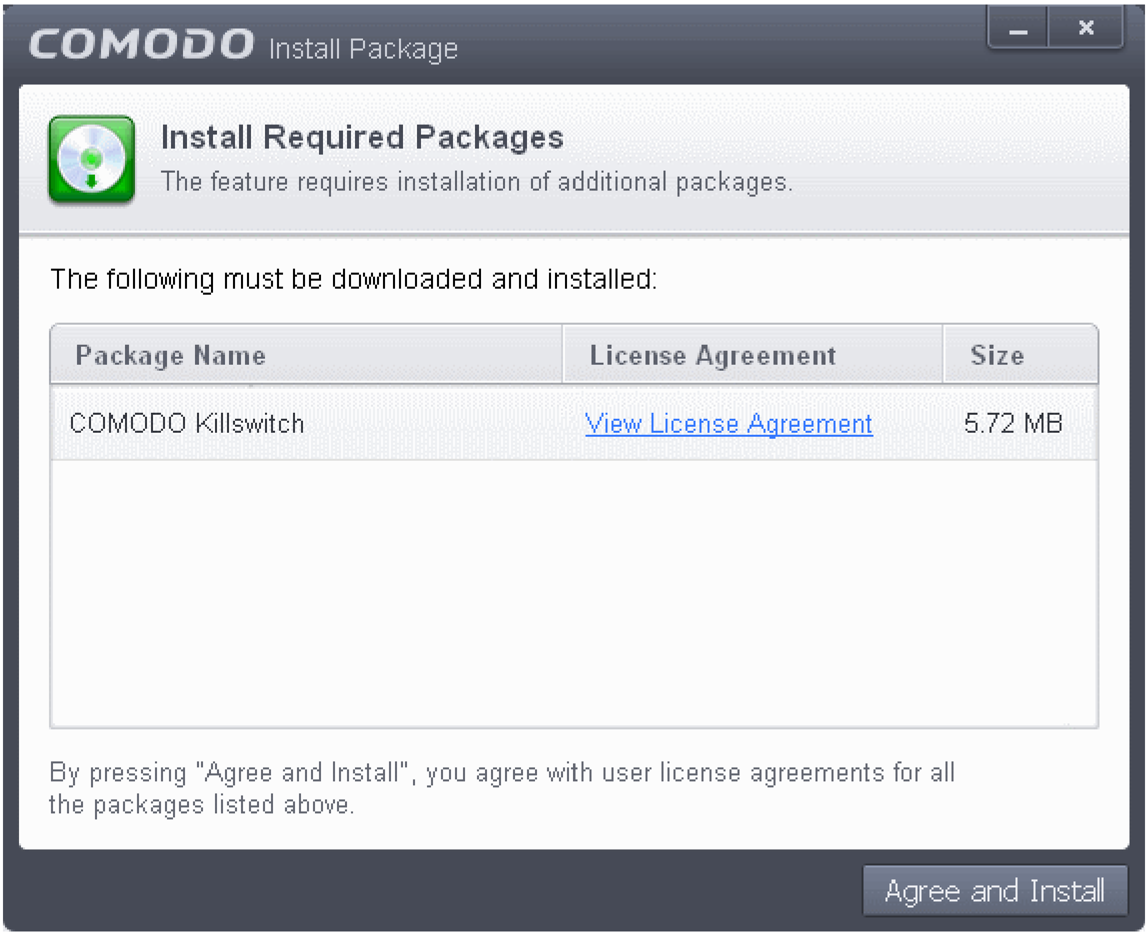
Open Task Manager
Open the task manager to view running security tasks in progress.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

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

Note: Comodo Cleaning Essentials (CCE) contains Killswitch component and if you have already installed CCE when using the '**Clean Endpoint** ' feature, then the Killswitch interface will open on clicking 'Watch Activity'.



Install Required Packages

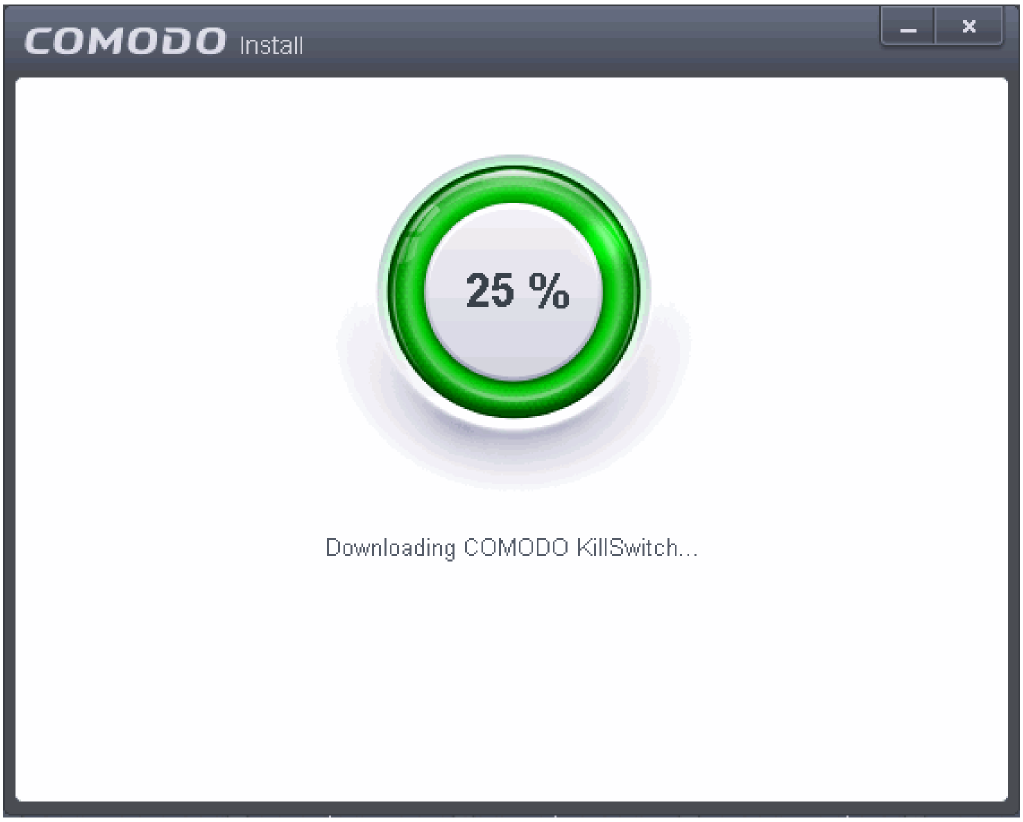
The feature requires installation of additional packages.

The following must be downloaded and installed:

Package Name	License Agreement	Size
COMODO Killswitch	View License Agreement	5.72 MB

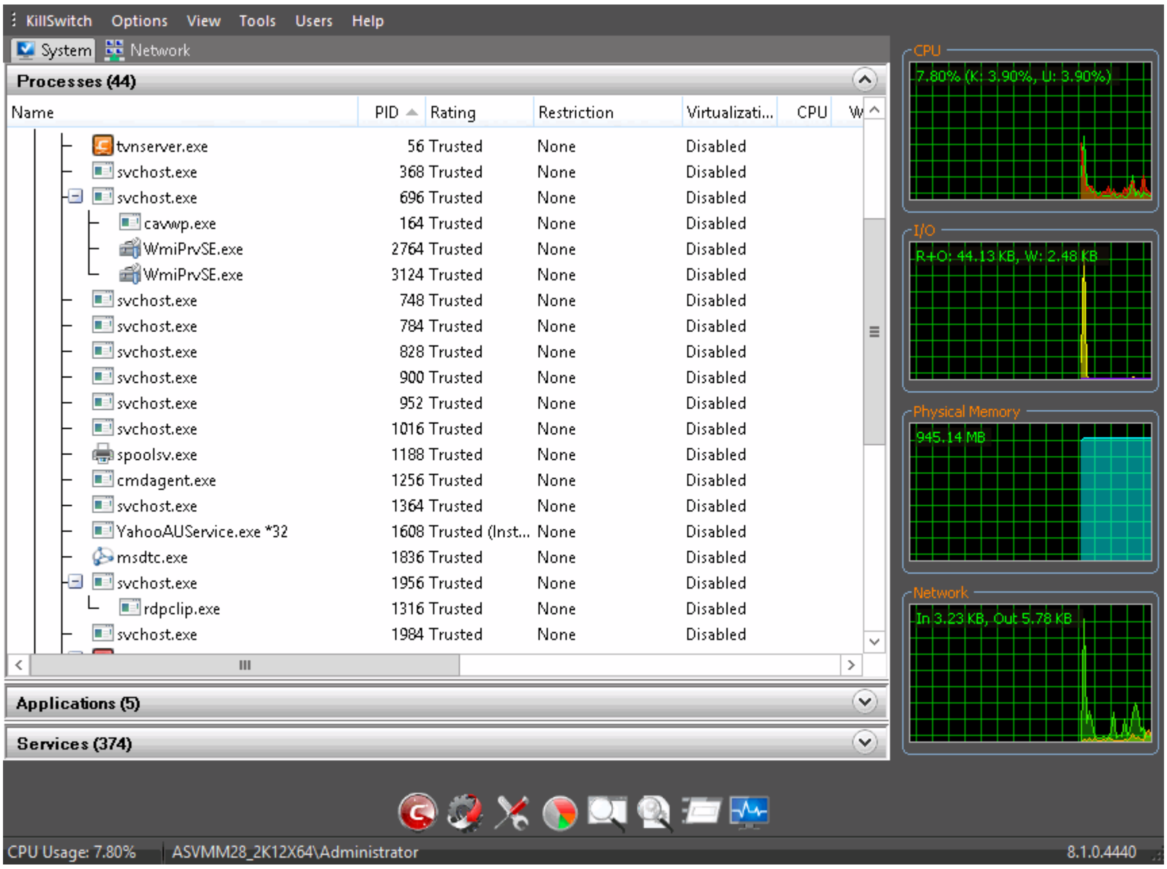
By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.

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



Downloading COMODO KillSwitch...

On completion of installation, the Comodo KillSwitch main interface will be opened.



Processes (44)

Name	PID	Rating	Restriction	Virtualizati...	CPU	W
tvnserver.exe	56	Trusted	None	Disabled		
svchost.exe	368	Trusted	None	Disabled		
svchost.exe	696	Trusted	None	Disabled		
cavwp.exe	164	Trusted	None	Disabled		
WmiPrvSE.exe	2764	Trusted	None	Disabled		
WmiPrvSE.exe	3124	Trusted	None	Disabled		
svchost.exe	748	Trusted	None	Disabled		
svchost.exe	784	Trusted	None	Disabled		
svchost.exe	828	Trusted	None	Disabled		
svchost.exe	900	Trusted	None	Disabled		
svchost.exe	952	Trusted	None	Disabled		
svchost.exe	1016	Trusted	None	Disabled		
spoolsv.exe	1188	Trusted	None	Disabled		
cmdagent.exe	1256	Trusted	None	Disabled		
svchost.exe	1364	Trusted	None	Disabled		
YahooAUService.exe *32	1608	Trusted (Inst...	None	Disabled		
msdtc.exe	1836	Trusted	None	Disabled		
svchost.exe	1956	Trusted	None	Disabled		
rdpclip.exe	1316	Trusted	None	Disabled		
svchost.exe	1984	Trusted	None	Disabled		

Applications (5)

Services (374)

CPU Usage: 7.80% ASVMM28_2K12X64\Administrator 8.1.0.4440

On clicking the 'Watch Activity' button from next time onwards, Comodo Killswitch will be opened.

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

4.4. Remove Deeply Hidden Malware

Comodo Cleaning Essentials (CCE) is a set of computer security tools designed to help users identify and remove malware and unsafe processes from infected servers.

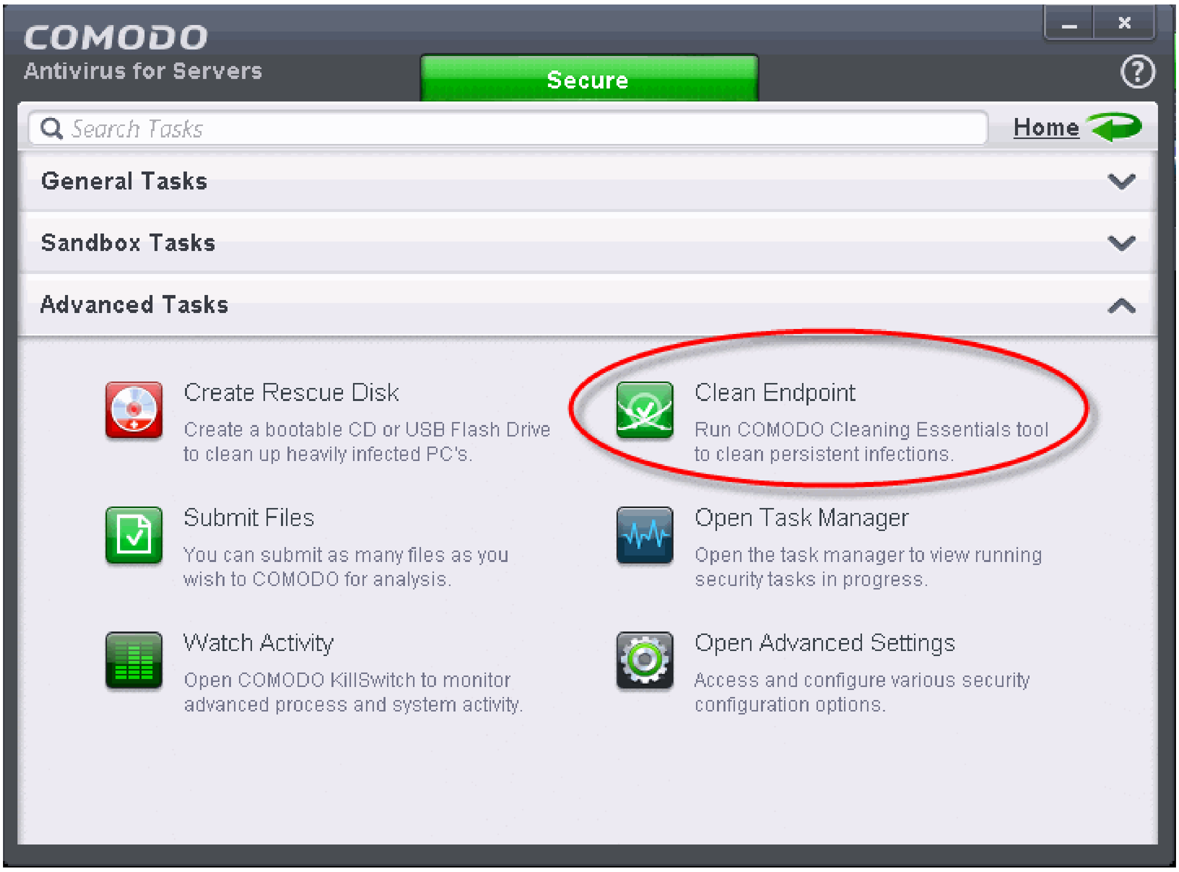
Major features include:

- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits, hidden files and malicious registry keys hidden deep in your system.
- **Autorun Analyzer** - An advanced utility to view and handle services and programs that were loaded when your system booted-up.

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

For more details on the features and usage of the application, please refer to the online guide at **http://help.comodo.com/topic-119-1-328-3516-Introduction-to-Comodo-Cleaning-Essentials.html**.

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



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

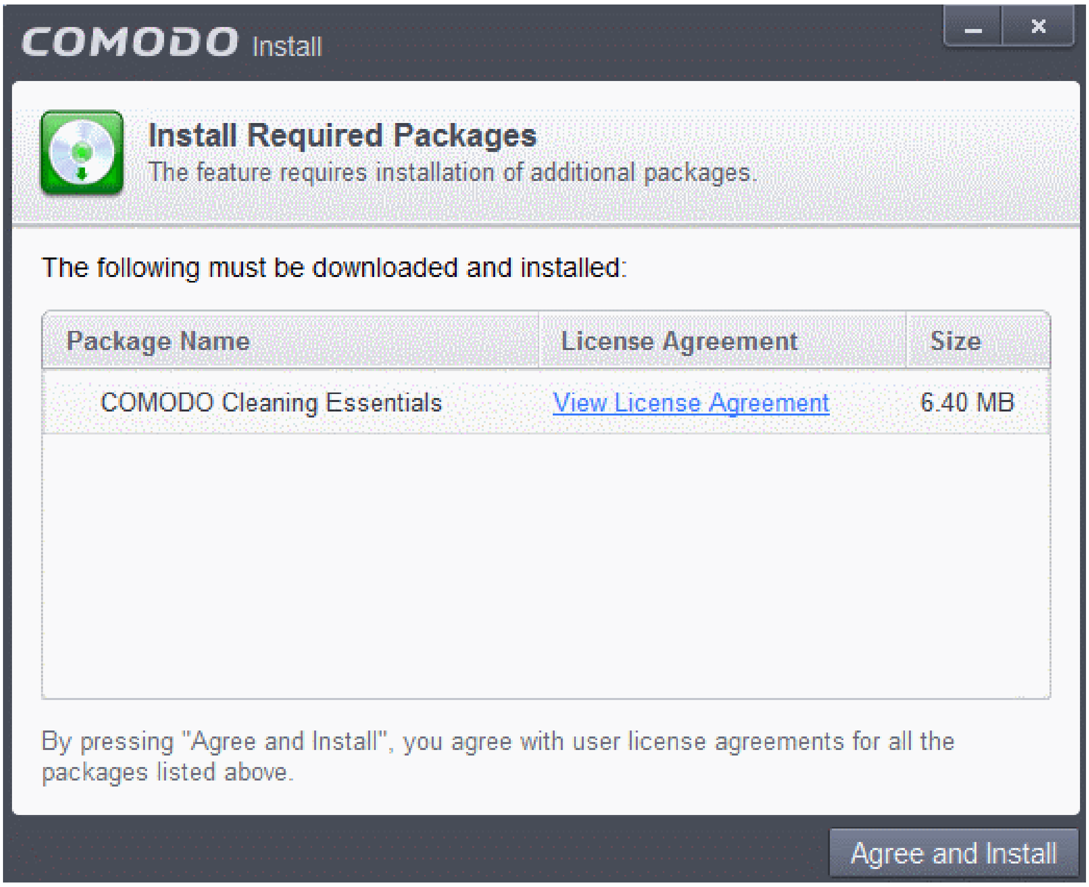
Submit Files
You can submit as many files as you wish to COMODO for analysis.

Open Task Manager
Open the task manager to view running security tasks in progress.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

- Clicking the 'Clean Endpoint' for the first time, CAVS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.



Install Required Packages

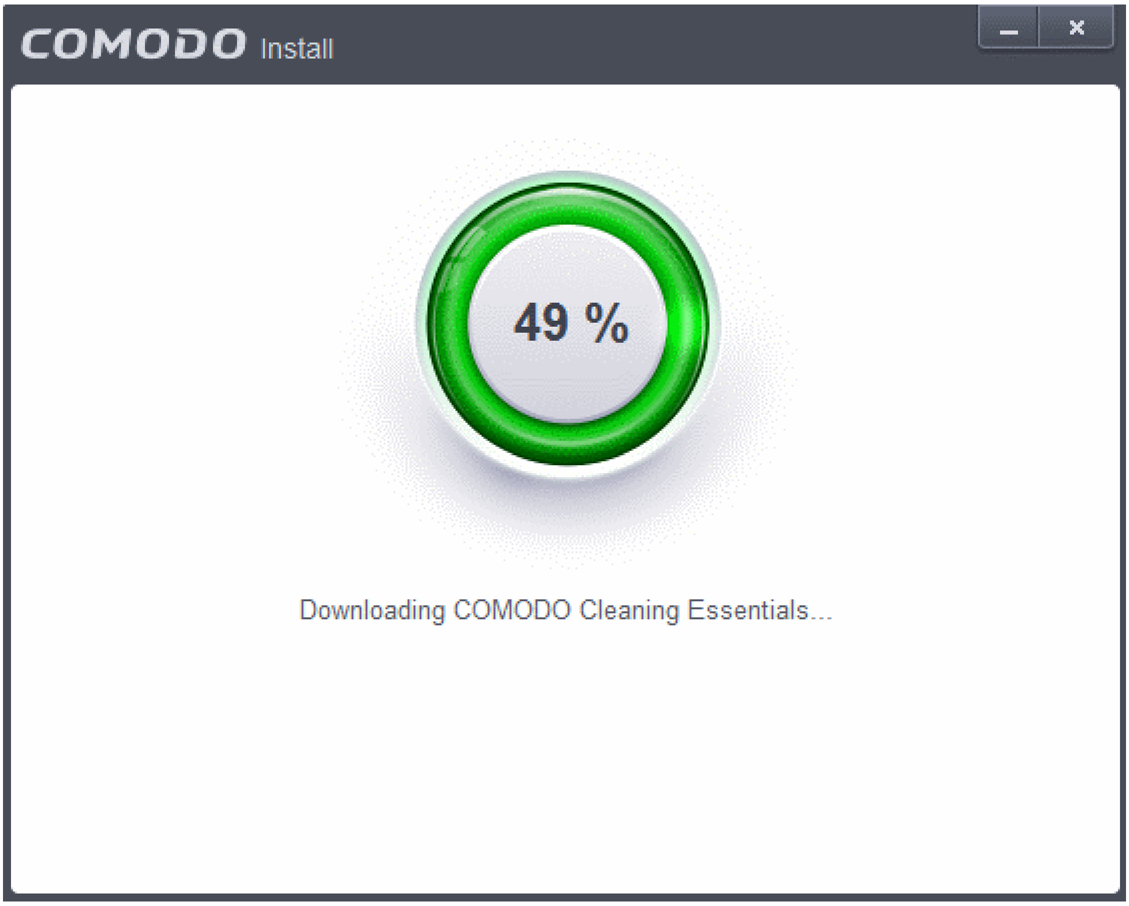
The feature requires installation of additional packages.

The following must be downloaded and installed:

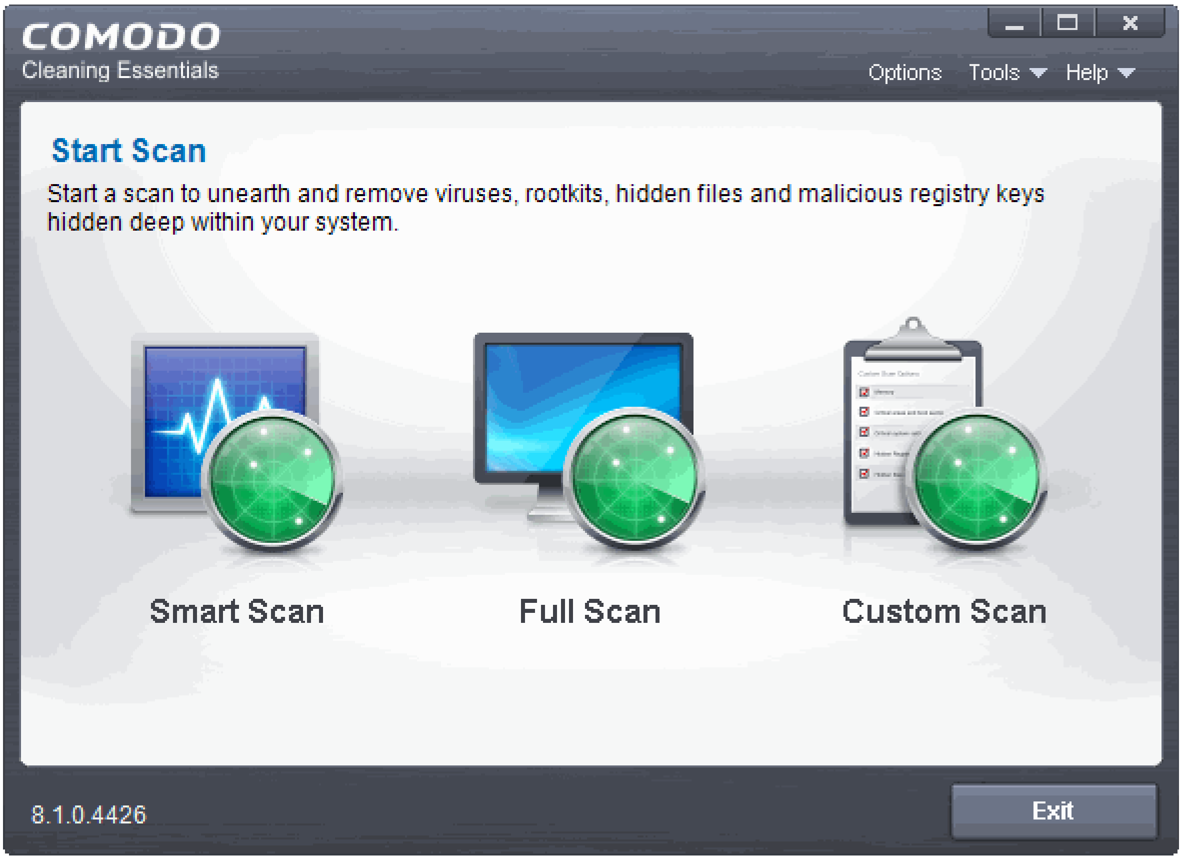
Package Name	License Agreement	Size
COMODO Cleaning Essentials	View License Agreement	6.40 MB

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

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



On completion of installation, the Comodo Cleaning Essentials main interface will be opened.

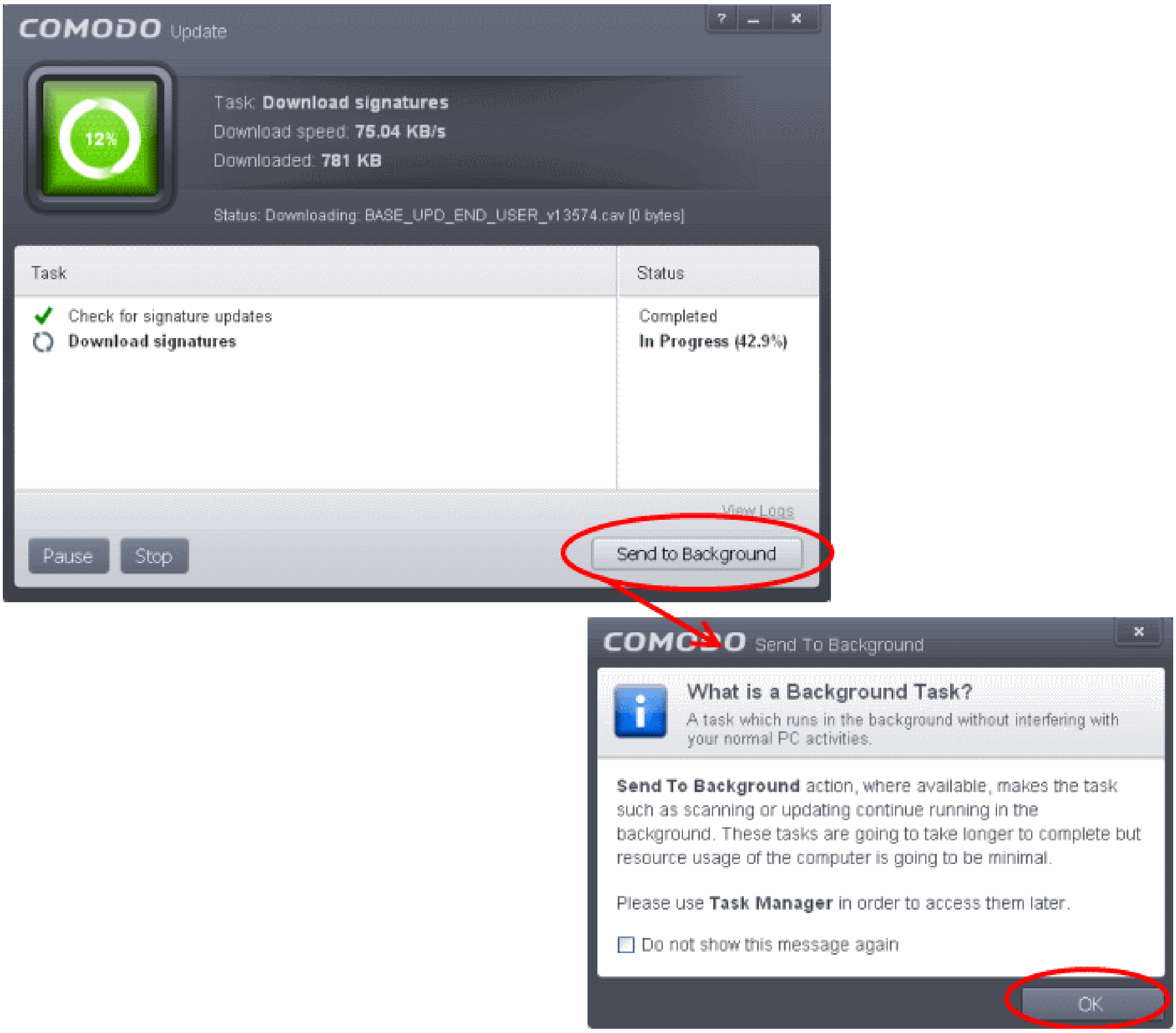

COMODO
Cleaning Essentials
Options
Tools
Help
Start Scan
Start a scan to unearth and remove viruses, rootkits, hidden files and malicious registry keys hidden deep within your system.
Smart Scan
Full Scan
Custom Scan
8.1.0.4426
Exit

- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at **http://help.comodo.com/topic-119-1-328-3525-The-Main-Interface.html**

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

4.5. Manage CAVS Tasks

CAVS has the ability to concurrently run several tasks like on-demand or scheduled scans, virus signature database updates and so on. The tasks that are currently run, can be sent to background from the progress interface, by clicking Send to Background as shown in the example below.



Task: **Download signatures**
Download speed: **75.04 KB/s**
Downloaded: **781 KB**

Status: Downloading: BASE_UPD_END_USER_v13574.cav [0 bytes]

Task	Status
✓ Check for signature updates	Completed
○ **Download signatures**	**In Progress (42.9%)**

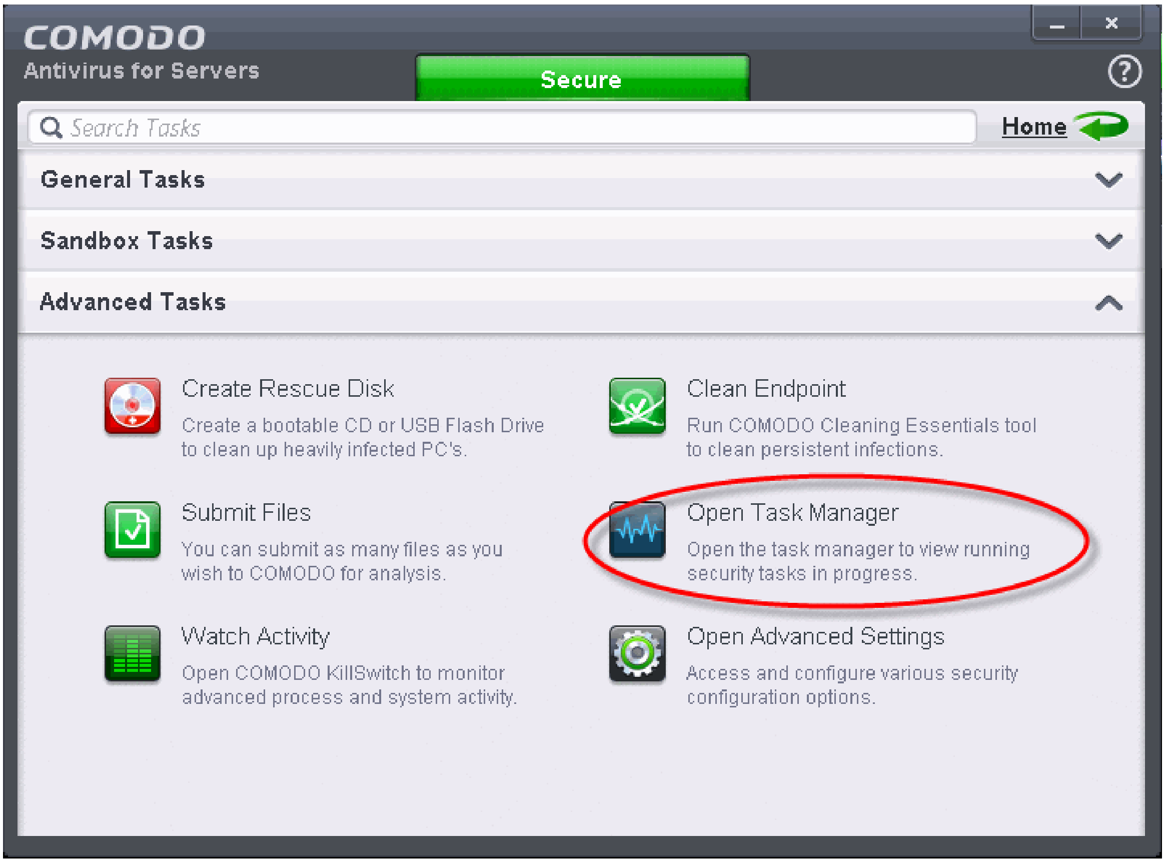
What is a Background Task?
A task which runs in the background without interfering with your normal PC activities.

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

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

□ Do not show this message again

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



General Tasks

Sandbox Tasks

Advanced Tasks

Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

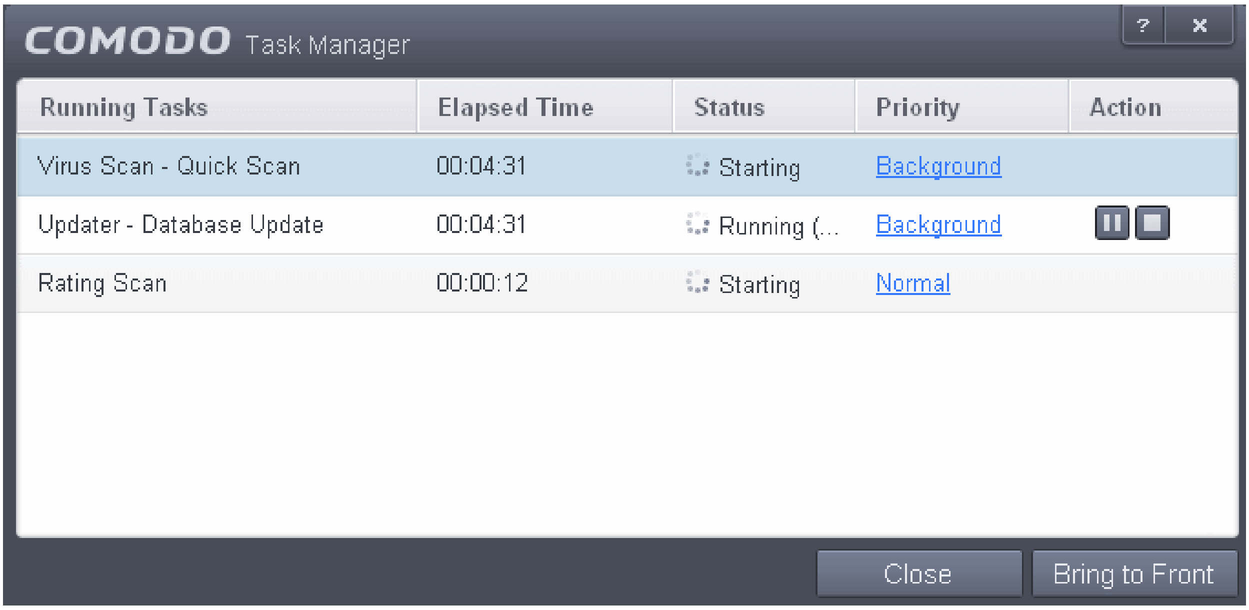
Open Task Manager
Open the task manager to view running security tasks in progress.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

Tip: The Task Manager can also be opened by clicking on the center tab in the Status row of the **widget** that displays the number of tasks that are currently running.

The Task Manager window displays a list of background tasks that are currently running with the details of time elapsed on each task, status and priority.



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Quick Scan	00:04:31	Starting	Background	
Updater - Database Update	00:04:31	Running (...	Background	⏸ ⏹
Rating Scan	00:00:12	Starting	Normal	

From the Task Manager interface, you can:

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

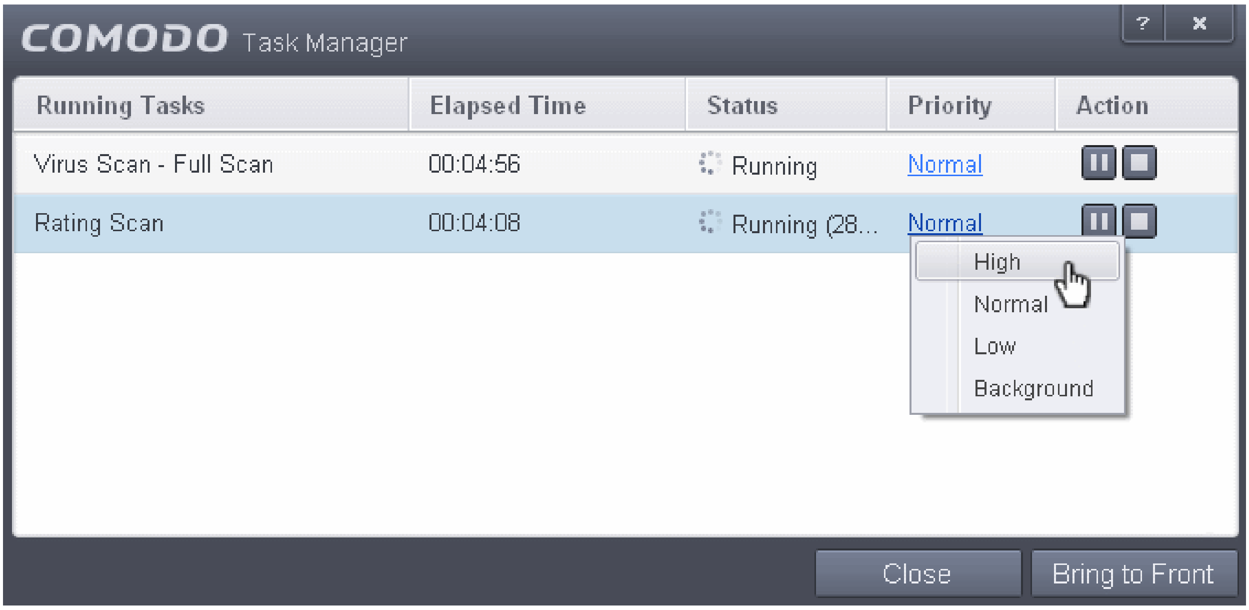
- **Bring a selected task to foreground**

Reassigning Priorities for a task:

The Priority column in the Task Manager interface displays the current priority assigned for each task.

To change the priority for a task

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



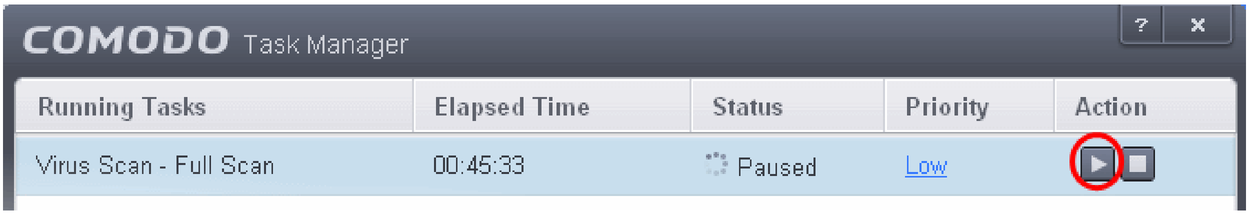
COMODO Task Manager

Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:04:56	Running	Normal	
Rating Scan	00:04:08	Running (28...	Normal	

Pausing/Resuming or Stopping running tasks

The Action column displays the Pause/Resume and Stop buttons

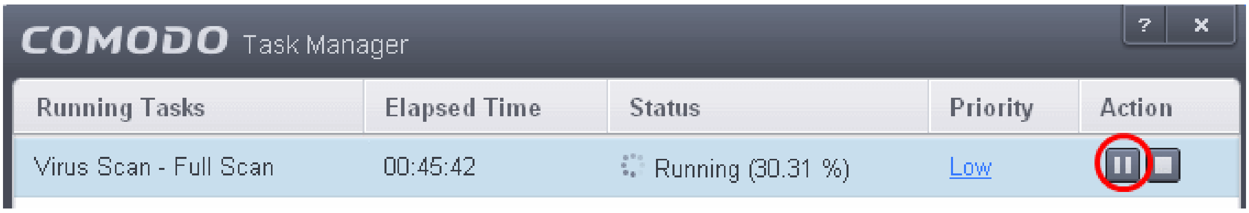
- To pause a running task, click the Pause button



COMODO Task Manager

Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:45:33	Paused	Low	

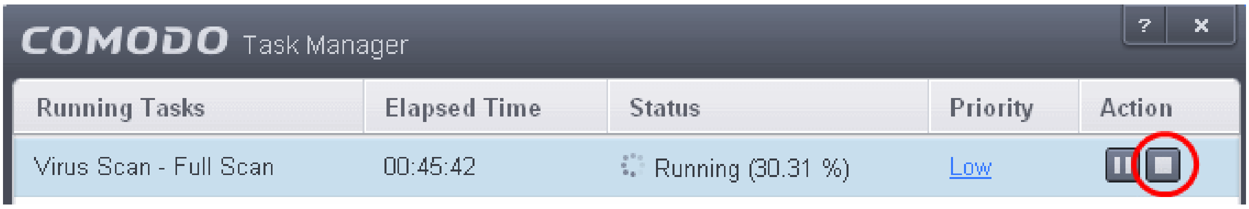
- To resume a paused task, click the Resume button



COMODO Task Manager

Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:45:42	Running (30.31 %)	Low	

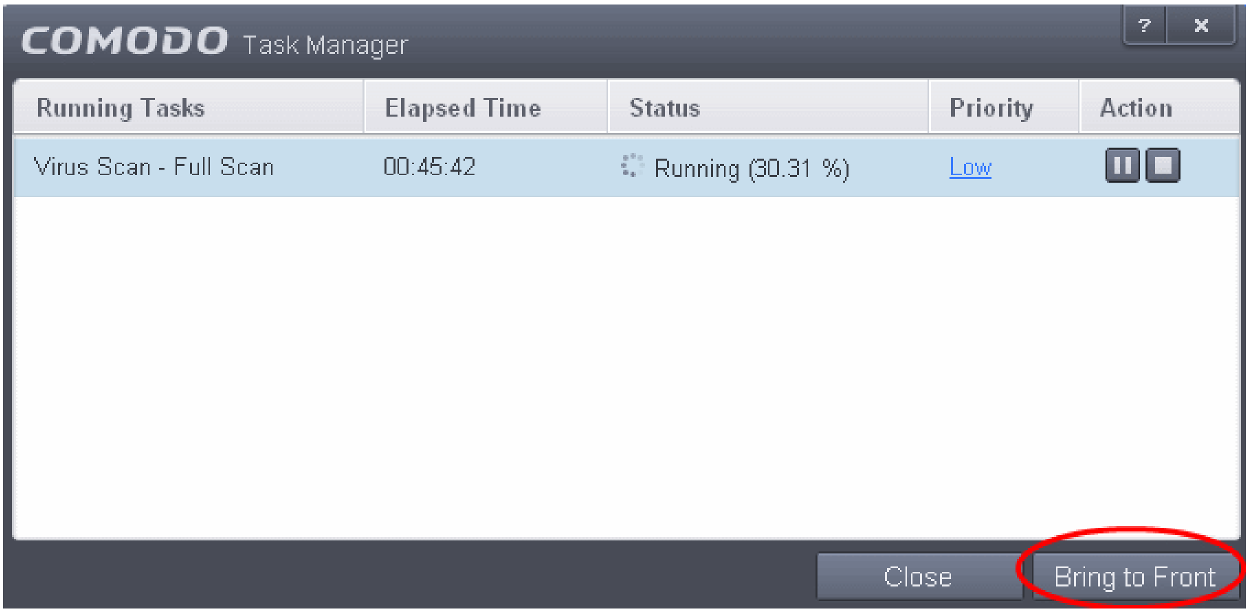
- To stop a running task, click the stop button



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:45:42	Running (30.31 %)	Low	

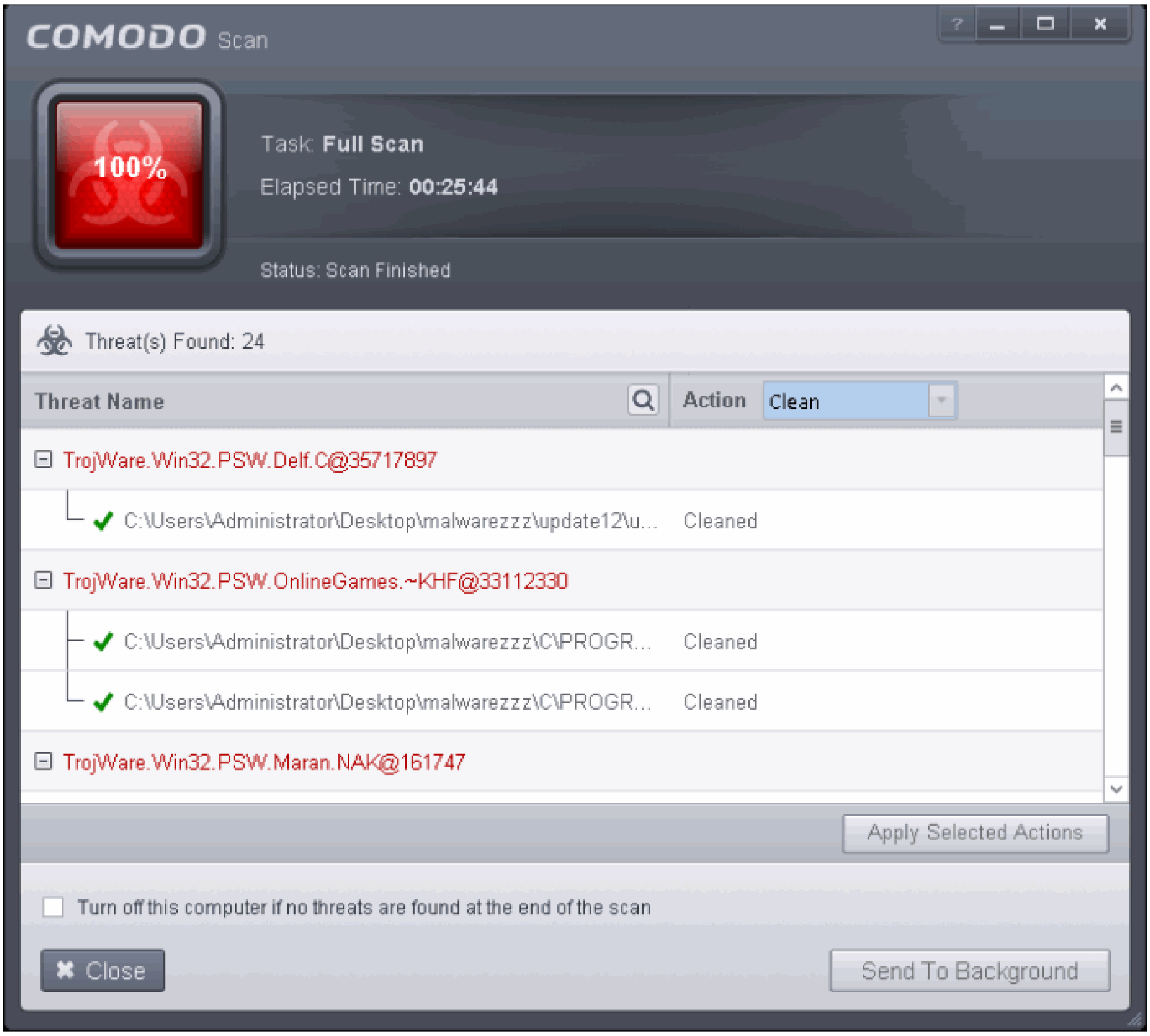
Bringing a running task to foreground

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



Running Tasks	Elapsed Time	Status	Priority	Action
Virus Scan - Full Scan	00:45:42	Running (30.31 %)	Low	

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



Task: **Full Scan**

Elapsed Time: **00:25:44**

Status: Scan Finished

Threat(s) Found: 24

```
Threat Name                                                      Action  Clean
⊟ TrojWare.Win32.PSW.Delf.C@35717897
   └ ✓ C:\Users\Administrator\Desktop\malwarezzz\update12\u...  Cleaned
⊟ TrojWare.Win32.PSW.OnlineGames.~KHF@33112330
   ├ ✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...     Cleaned
   └ ✓ C:\Users\Administrator\Desktop\malwarezzz\C\PROGR...     Cleaned
⊟ TrojWare.Win32.PSW.Maran.NAK@161747
```

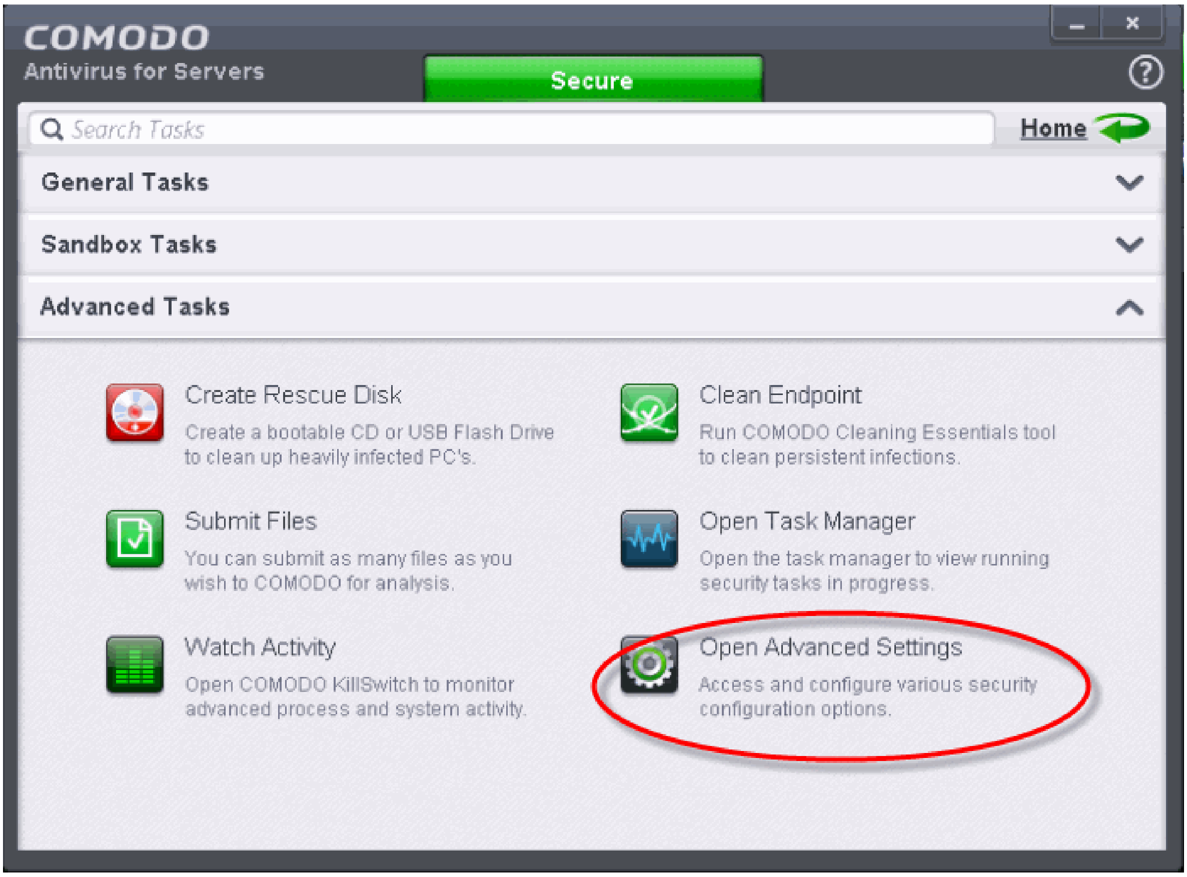
□ Turn off this computer if no threats are found at the end of the scan

5. Advanced Settings

The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Antivirus for Servers. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced users delve into granular configuration of the Antivirus, Defense+ and File Ratings modules. For example, the 'Security Settings' area allows you to create custom virus scan schedules, create virus exclusions, create HIPS rules and specify how the file rating system deals with trusted and untrusted files.

To open 'Advanced Settings':

- Click the 'Tasks' arrow if you are on the CAVS home screen
- Click 'Advanced Tasks' then 'Open Advanced settings'



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

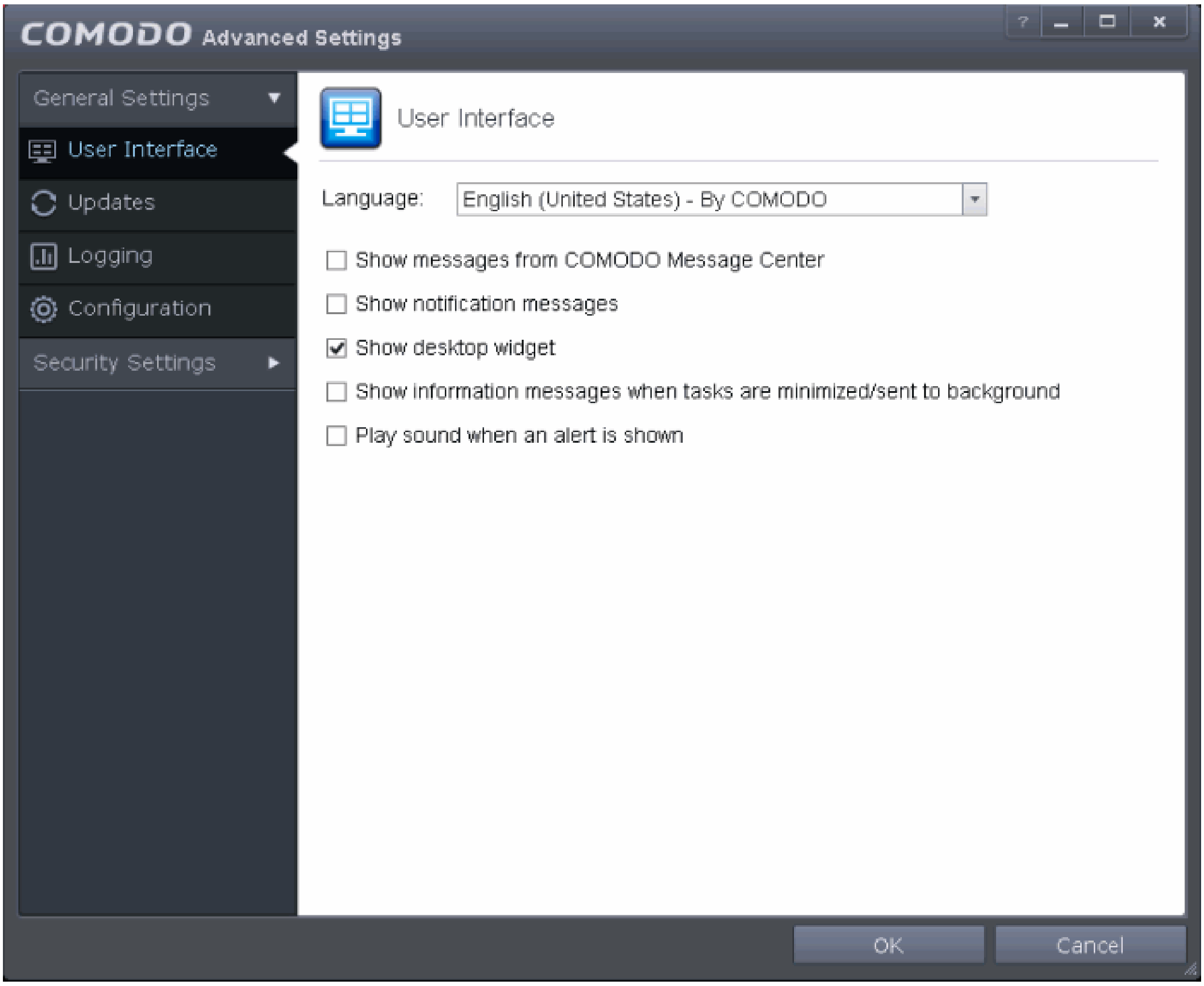
Submit Files
You can submit as many files as you wish to COMODO for analysis.

Open Task Manager
Open the task manager to view running security tasks in progress.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

The 'Advanced Settings' panel will open:



User Interface

Language: English (United States) - By COMODO

□ Show messages from COMODO Message Center

□ Show notification messages

☑ Show desktop widget

□ Show information messages when tasks are minimized/sent to background

□ Play sound when an alert is shown

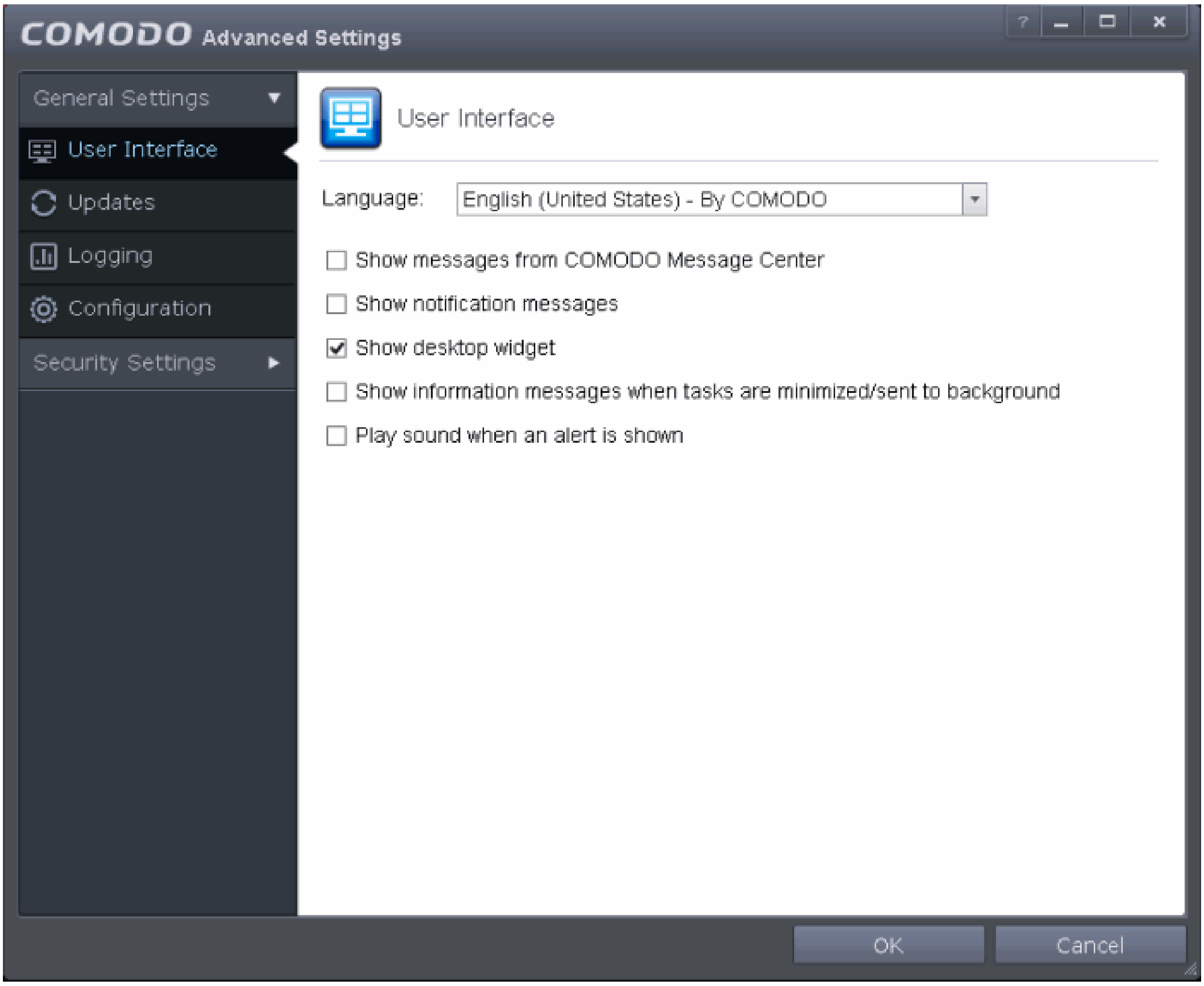
Please click the following links to find out more about each section:

- **General Settings** - Allows you to configure the appearance and behavior of the application
    - **Customize User Interface**
    - **Configure Program and database Updates**
    - **Log Settings**
    - **Manage CAVS Configurations**

- **Security Settings** - Advanced configuration of Antivirus, Defense+ and File Ratings modules
    - **Antivirus Settings**
    - **Defense+ Settings**
    - **File Ratings**

5.1. General Settings

The 'General Settings' area enables you to customize the appearance and overall behavior of CAVS. You can configure general properties like the interface language, notification messages, automatic updates, logging and more.



Language: English (United States) - By COMODO

☐ Show messages from COMODO Message Center

☐ Show notification messages

☑ Show desktop widget

☐ Show information messages when tasks are minimized/sent to background

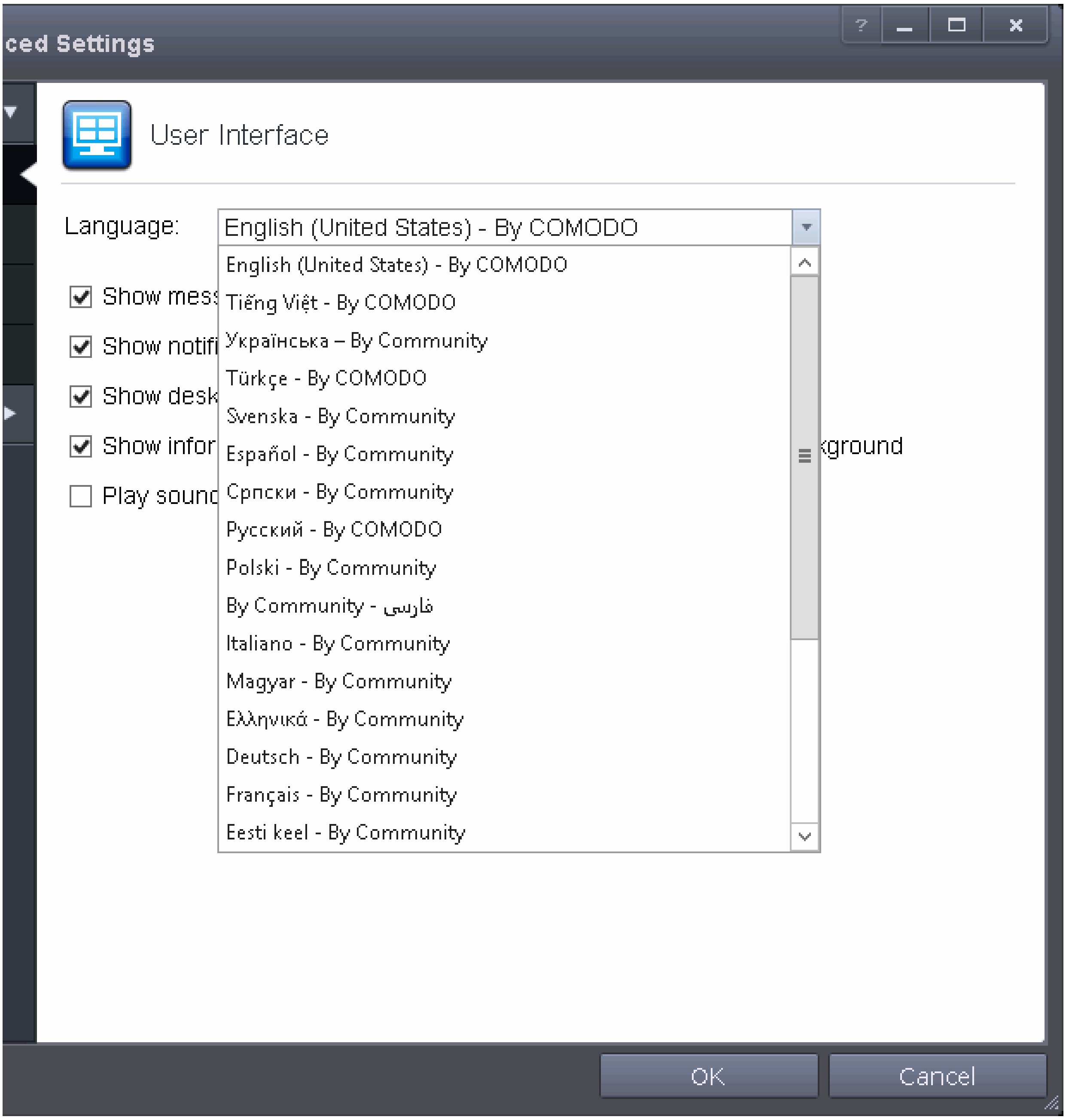
☐ Play sound when an alert is shown

The category has the following sections:

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

5.1.1. Customize User Interface

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



ced Settings

User Interface

Language: English (United States) - By COMODO

☑ Show mess

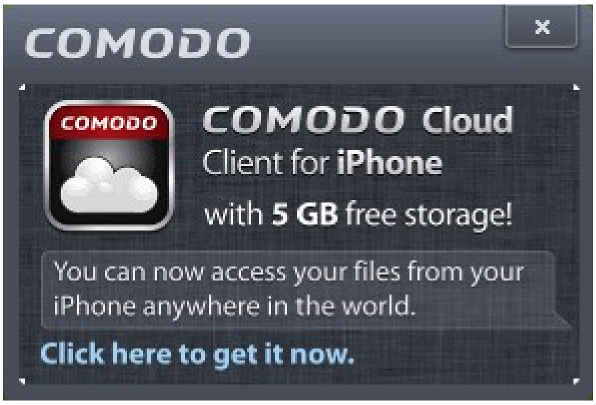
☑ Show notifi

☑ Show desk

☑ Show infor ... kground

□ Play sounc

- **Language Settings** - CAVS is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (***Default = English (United States)***).
- **Show messages from COMODO Message Center -** If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world.



COMODO

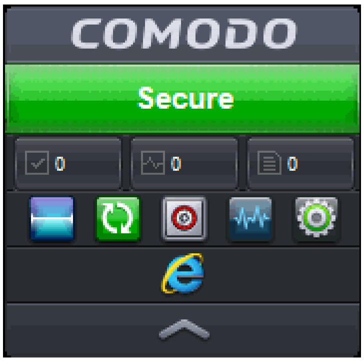
COMODO Cloud Client for iPhone with 5 GB free storage!

You can now access your files from your iPhone anywhere in the world.

Click here to get it now.

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

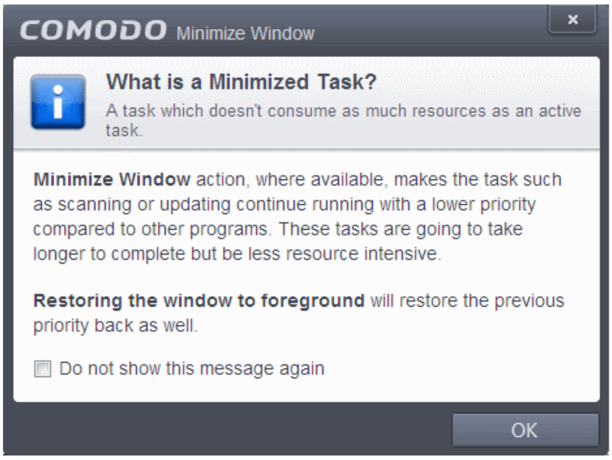
- **Show notification messages -** These are the CAVS system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CAVS is taking and any CAVS status updates. For example 'Defense+ is learning ' is generated when these module is learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have not selected 'Do not show antivirus alerts' check box in **Antivirus > Real-time Scan settings** screen. Clear this check box if you do not want to see these system messages (***Default = Enabled***).
- **Show desktop widget -** The CAVS Widget is a handy control that provides at-a-glance information about the security status, number of tasks running and shortcuts to common tasks.



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

Tip: You can disable the widget from the CAVS system tray icon. Right click on the CAVS system tray icon and deselect the 'Show' option that appears on hovering the mouse cursor on 'Widget' .

- **Show information messages when tasks are minimized/sent to background -** CAVS displays messages explaining the effects of minimizing or moving a running task like an AV scan to the background:



COMODO Minimize Window

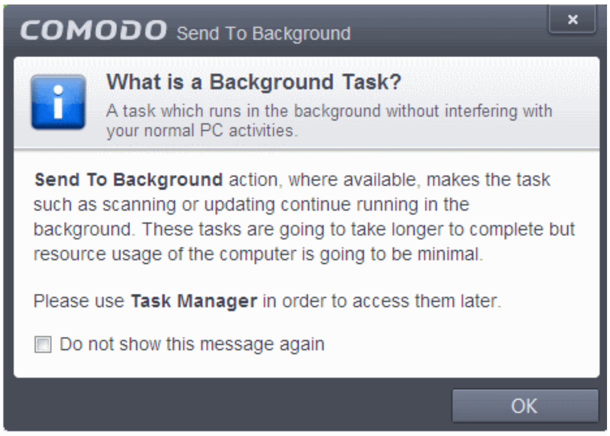
What is a Minimized Task?

A task which doesn't consume as much resources as an active task.

Minimize Window action, where available, makes the task such as scanning or updating continue running with a lower priority compared to other programs. These tasks are going to take longer to complete but be less resource intensive.

Restoring the window to foreground will restore the previous priority back as well.

□ Do not show this message again



COMODO Send To Background

What is a Background Task?

A task which runs in the background without interfering with your normal PC activities.

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

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

□ Do not show this message again

If you do not want these messages to be displayed, clear this check-box (***Default = Enabled***).

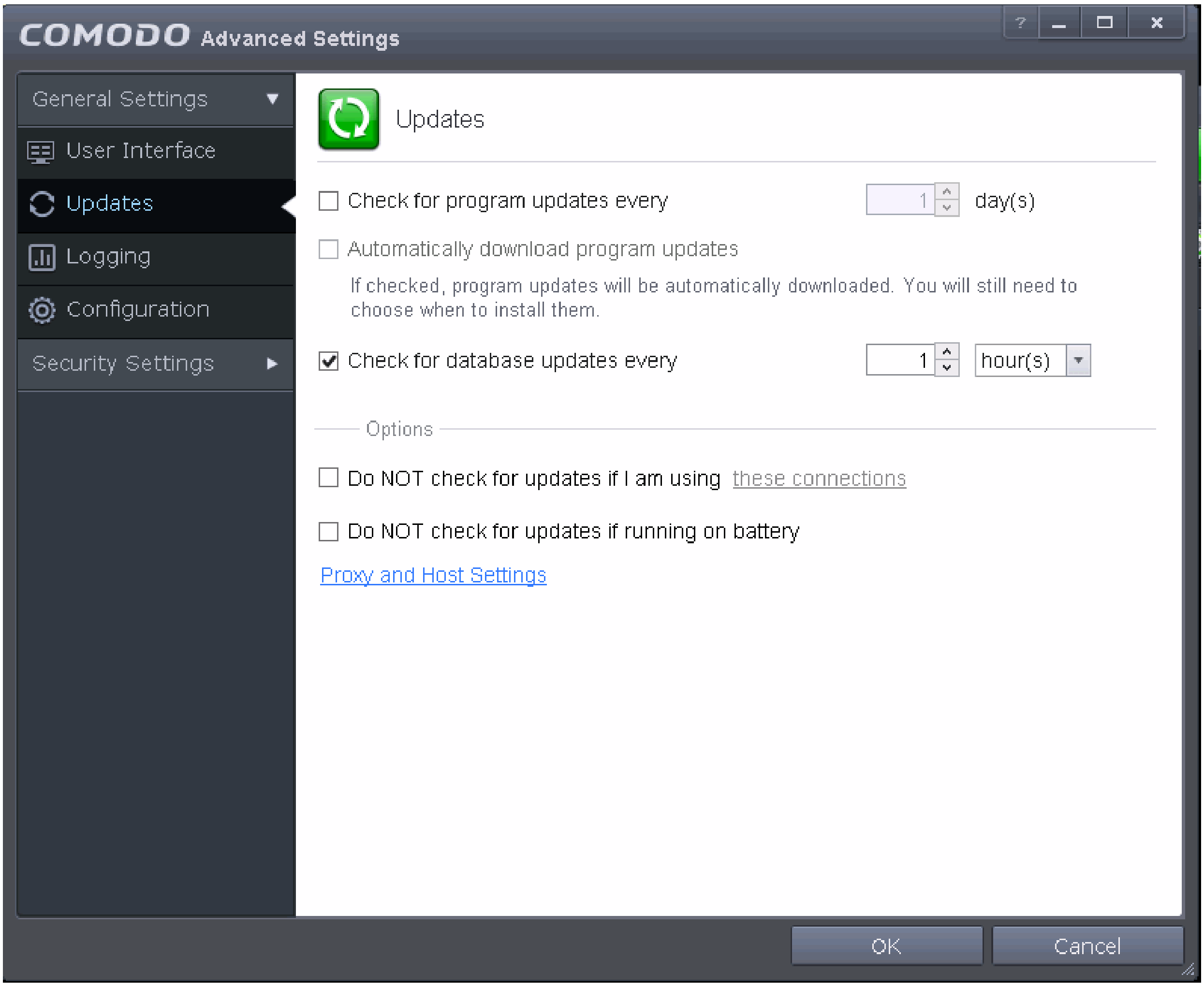
Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **Play sound when an alert is shown -** CAVS generates a chime whenever it raises a security alert to grab your attention. If you do not want the sound to be generated, clear this check box (***Default = Disabled***)

5.1.2. Configure Program and Virus Database Updates

The 'Updates' area allows you to configure settings that govern CAVS program and virus database updates.

This screen can be accessed by clicking 'Updates' under the 'General Settings' section of 'Advanced Settings':



Updates

□ Check for program updates every 1 day(s)

□ Automatically download program updates

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

☑ Check for database updates every 1 hour(s)

Options

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

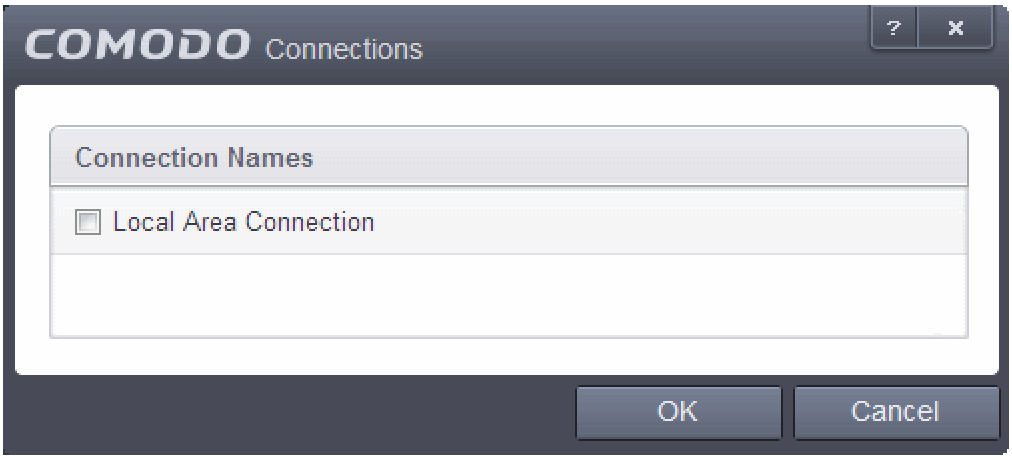
□ Do NOT check for updates if running on battery

Proxy and Host Settings

- **Check program updates every NN day(s)** - Enables you to set the interval at which CAVS will check for program updates. Select the interval in days from the drop-down combo box. ***(Default = 1 day)***
- **Automatically download program updates** - Instructs CAVS to automatically download program updates as soon as they are available. ***(Default=Disabled)***
- **Check** for database updates every NN hour(s)/day(s) - Enables you to set the interval at which CAVS will check for virus signature database updates. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 1 hours)***
- Do NOT check updates if am using these connections - Enables you to restrict CAVS from checking for updates if you use certain types of Internet connection. For example, you may not wish to check updates if using a wireless connection you know to be slow or not secure. ***(Default = Disabled)***

  To do this:

  - Select the 'Do NOT check updates if am using these connections' check-box
  - Then click the 'these connections'. The connections dialog will appear with the list of connections you use.



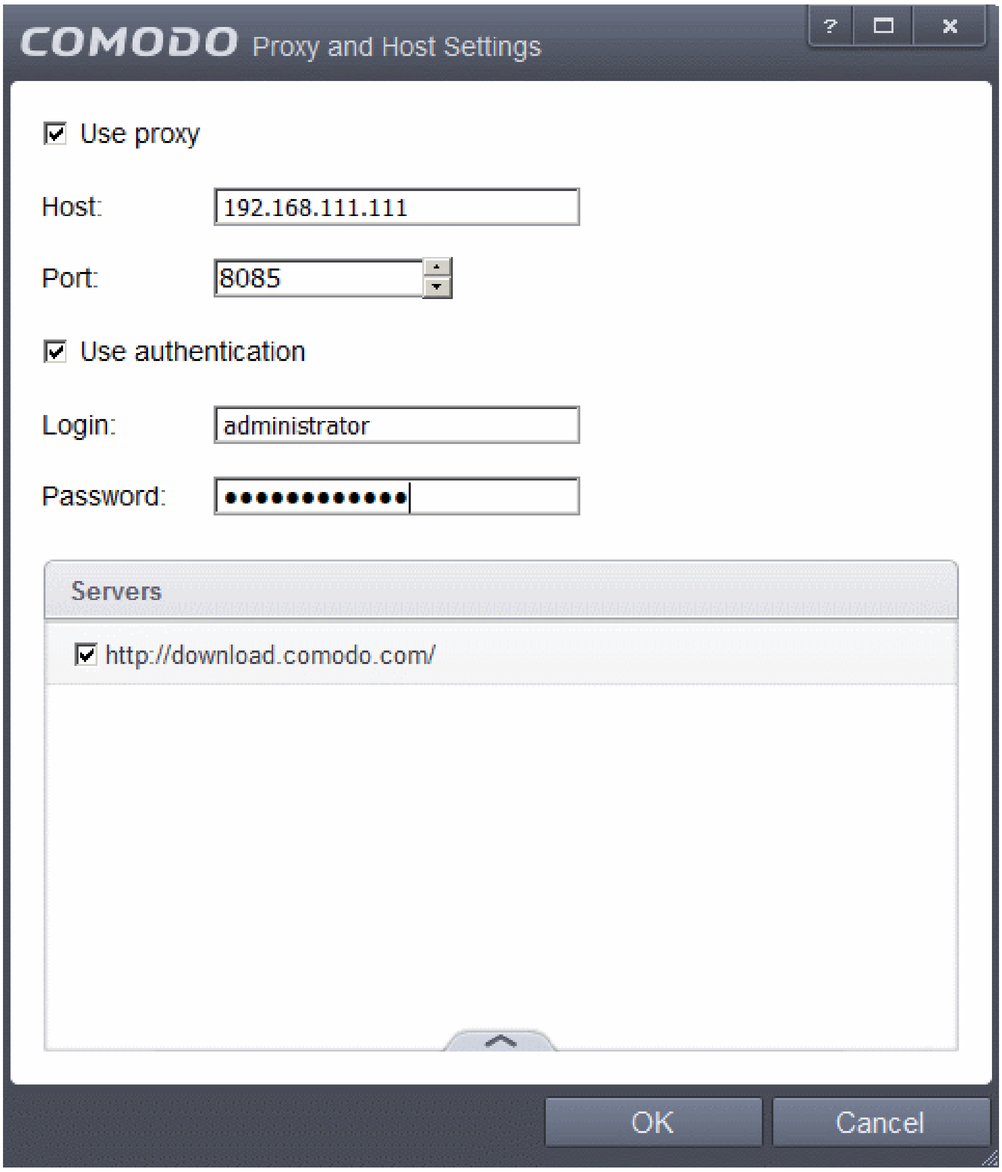
- Select the connection through which you do not want CAVS to check for updates and click OK.

- **Do NOT check for updates if running on battery -** If enabled, CAVS will not download updates if it detects your server is running from battery power. ***(Default = Disabled)***
- **Proxy and Host Settings -** Allows you to select the host from which updates are downloaded. By default, CAVS will directly download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CAVS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CAVS at this proxy/staging server. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

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

To configure updates via proxy server

- Click 'Proxy and Host Settings' at the bottom of the 'Updates' interface. The 'Proxy and Host Settings' interface will open.



☑ Use proxy

Host: 192.168.111.111

Port: 8085

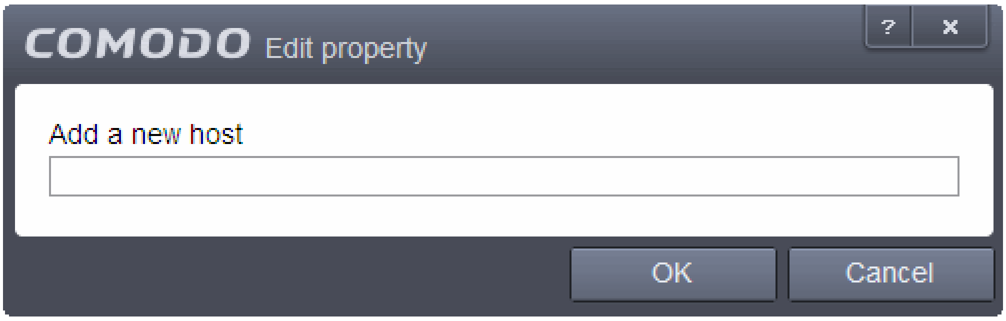
☑ Use authentication

Login: administrator

Password: ••••••••••••••

☑ http://download.comodo.com/

- Select the 'Use Proxy' check-box.
- Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.
- You can add multiple servers from which updates are available. To do this, click the handle at the bottom center of the 'Servers' panel, click the 'Add' button then enter the host name in the 'Edit Property' dialog.



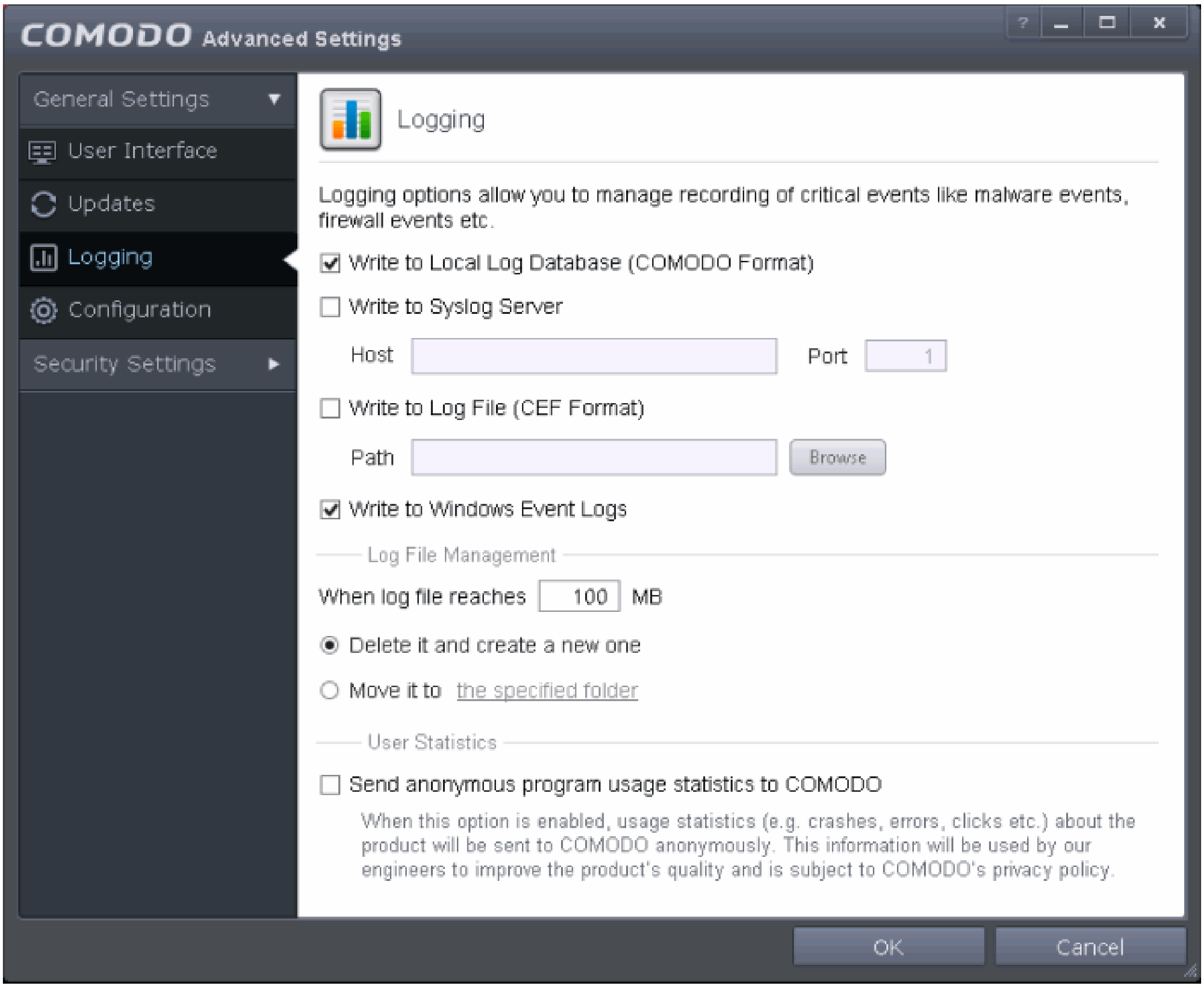
- If you specify multiple servers:
  - Activate or deactivate each update server by selecting or deselecting the check-box alongside it

- Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CAVS will commence downloading from the first server that contains new updates.
- Click 'OK' for your settings to take effect.

5.1.3. Log Settings

By default, Comodo Antivirus for Servers maintains detailed logs of all Antivirus and Defense+ events. Logs are also created for 'Alerts Displayed', 'Tasks Launched' and 'Configuration Changes'.

- This 'Logging' interface allows you to specify whether you want to enable logging; the maximum size of the log file and how CAVS should react if the maximum file size is exceeded.



Logging

Logging options allow you to manage recording of critical events like malware events, firewall events etc.

☑ Write to Local Log Database (COMODO Format)

□ Write to Syslog Server

Host | Port 1

□ Write to Log File (CEF Format)

Path | Browse

☑ Write to Windows Event Logs

Log File Management

When log file reaches 100 MB

● Delete it and create a new one

○ Move it to the specified folder

User Statistics

□ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, errors, clicks etc.) about the product will be sent to COMODO anonymously. This information will be used by our engineers to improve the product's quality and is subject to COMODO's privacy policy.

Note: If you wish to actually view, manage and export logs, then you need to open the '**View Logs**' interface under 'General Settings' (Tasks > General Settings > View Logs).

Logging Options

- **Write to Local Log Database** – Instructs CAVS to store the log files in the local storage of the endpoint in Comodo format so that they can be viewed from Tasks > General Settings > View Logs interface. Refer to the section '**View Logs**' for more details. The Log storage depends on the log file management settings configured in the '**Log File Management**' settings area in the same interface. (***Default = Enabled***).
- **Write to Syslog Server** – Instructs CAVS to forward the log files to an external Syslog Server integrated with the CESM server that remotely manages your CAVS installation. Enter the IP address/hostname of the Syslog server in the Host text field and enter the port through which Syslog server listens to CESM in the 'Port' field (default port = 514). (***Default = Disabled***).

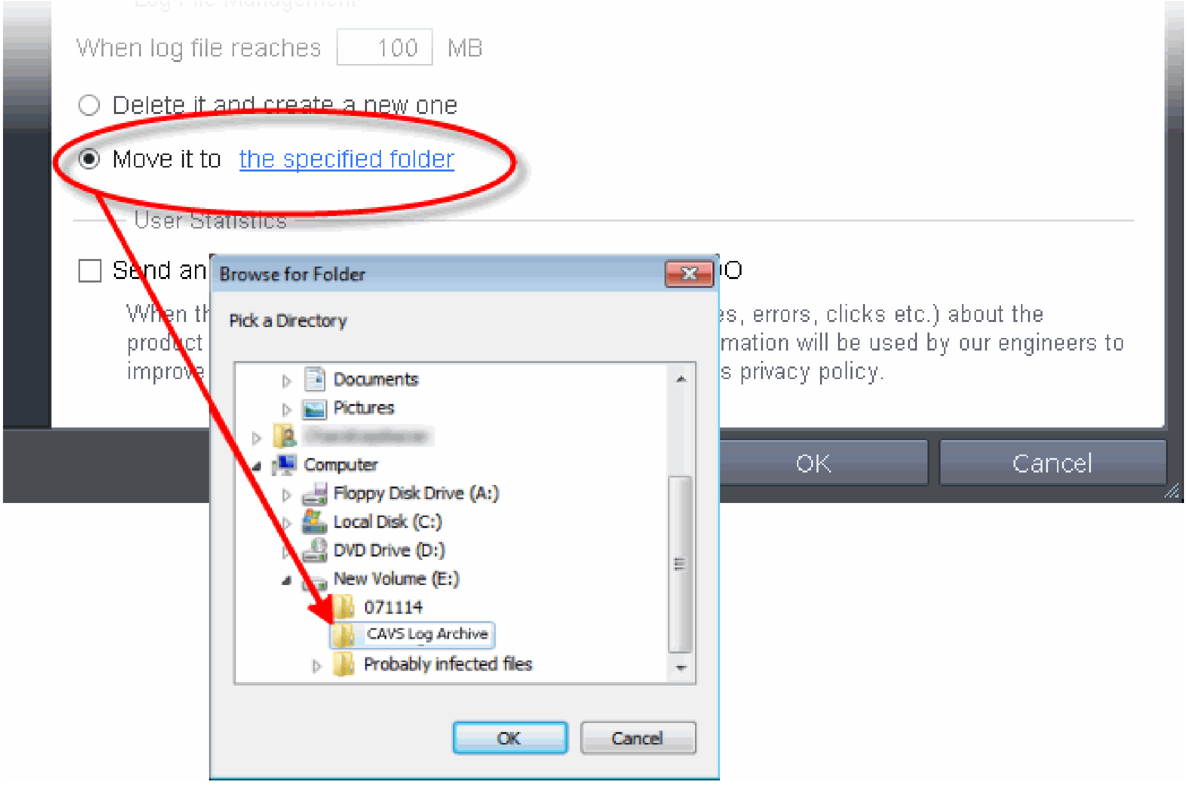
- **Write to Log file (CEF) Format** – Instructs CAVS to store the log files at a specified location in the local storage or a network storage, in Common Event Format (CEF) format, also known as NCSA Common Log Format, which is standardized text file format. When selecting this option, click 'Browse', select the storage location and navigate to the log file to which the logs are to be added. (***Default = Disabled***).
- **Write to Windows Event Logs** – Instructs CAVS to store the log events to the Windows Event Logs. (***Default = Enabled***)

Log File Management

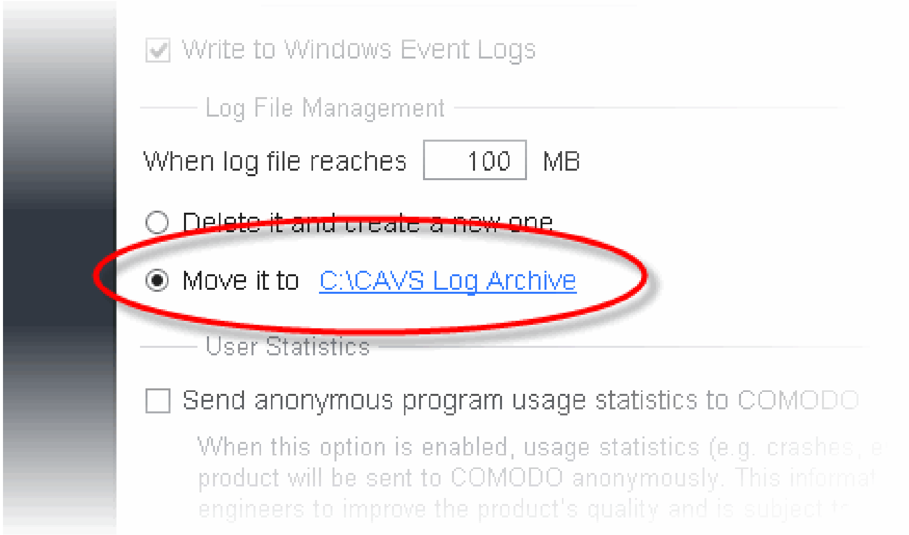
- **If the log file's size exceeds (Mb)** - Enables you to specify behavior when the Local Log Database (Comodo Format) log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.
- Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' ***(Default = 100MB).***

If you want to discard the log file if it reaches the maximum size, select **'Delete it and create a new one'.** Once the log file reaches the specified maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant***(Default = Enabled).***

If you want to save the log file even if it reaches the maximum size, select **'Move it to'** and select a destination folder for the log file ***(Default = Disabled).***



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



☑ Write to Windows Event Logs

Log File Management

When log file reaches 100 MB

○ Delete it and create a new one

● Move it to C:\CAVS Log Archive

User Statistics

□ Send anonymous program usage statistics to COMODO

When this option is enabled, usage statistics (e.g. crashes, e
product will be sent to COMODO anonymously. This informat
engineers to improve the product's quality and is subject to

Once the log file reaches the maximum size, it will be automatically moved to the selected folder and a new log file will be created with the log of events occurring from that instant.

User Statistics

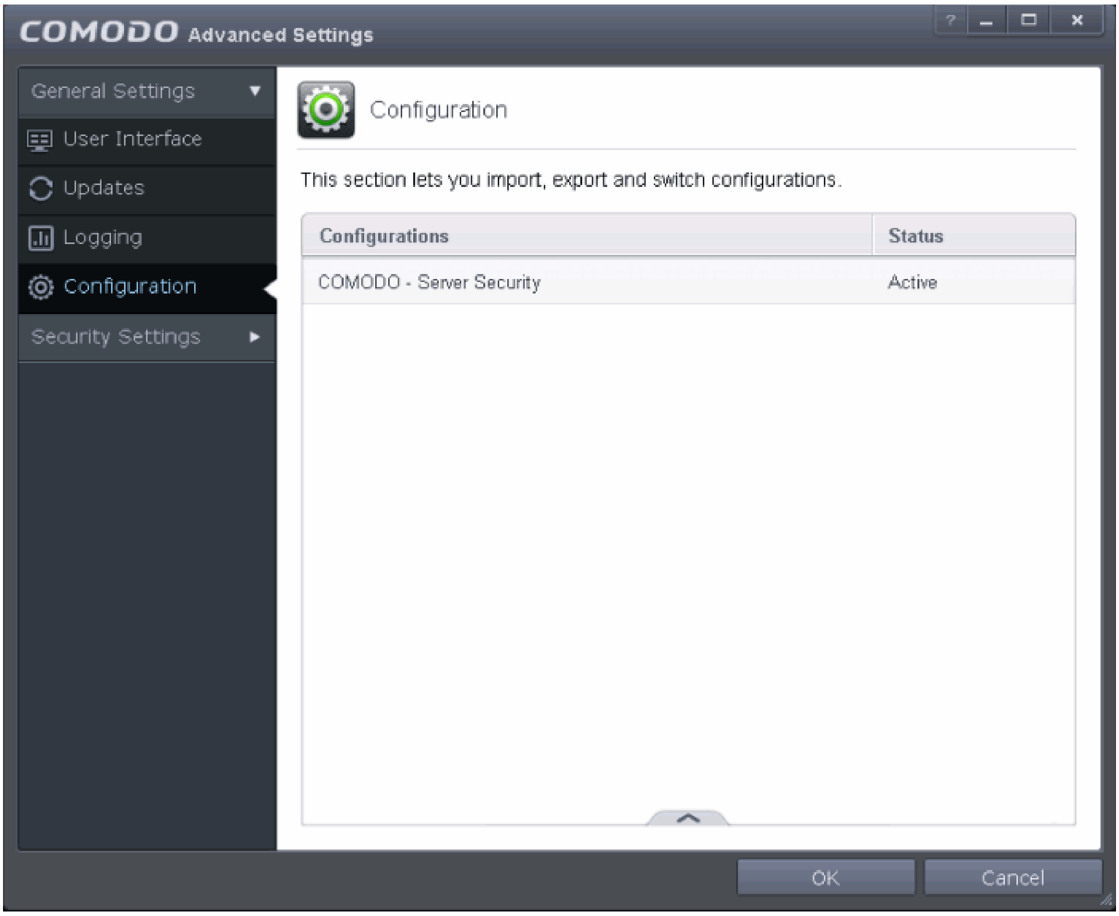
- **Send anonymous program usage (e.g. clicks, crashes, errors etc) statistics to COMODO in order to improve the product's quality** - Comodo collects collects the usage details from millions of CAVS users to analyze their usage patterns for the continual enhancement of the product. Your CAVS instillation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. ***(Default = Disabled).***

5.1.4. Manage CAVS Configurations

Comodo Antivirus for Servers allows you to maintain, save and export multiple configurations of your security settings as configuration profiles. This is especially useful if you are a network administrator looking to roll out a standard security configuration across multiple servers. If you are upgrading your system and there is a need to uninstall and re-install CAVS then it can be great time-saver to export your configuration settings beforehand. After re-installation, you can import your previous settings and avoid having to configure everything over again.

Note: Any changes you make over time will be automatically stored in the currently active profile. If you want to export your current settings then export the 'Active' profile.

This panel can be accessed by clicking 'Configuration' under the 'General Settings' section of 'Advanced Settings':



This section lets you import, export and switch configurations.

Configurations	Status
COMODO - Server Security	Active

The currently active configuration is indicated under the 'Active' column. Click the following links for more details:

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

5.1.4.1. Comodo Preset Configurations

By default, CAVS is installed with 'COMODO - Server Security' as the active configuration. Reminder - the active profile is, in effect, your current CAVS settings. Any changes you make to settings are recorded in the active profile. You can change the active profile at any time from the 'Configuration' panel.

COMODO - Server Security: This configuration is activated by default.

- Realtime scan is enabled.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Defense+ is disabled

If you want to switch to another configuration, first you have to create and save a configuration profile in the panel. Then you can select it and make it active.

5.1.4.2. Importing/Exporting and Managing Personal Configurations

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

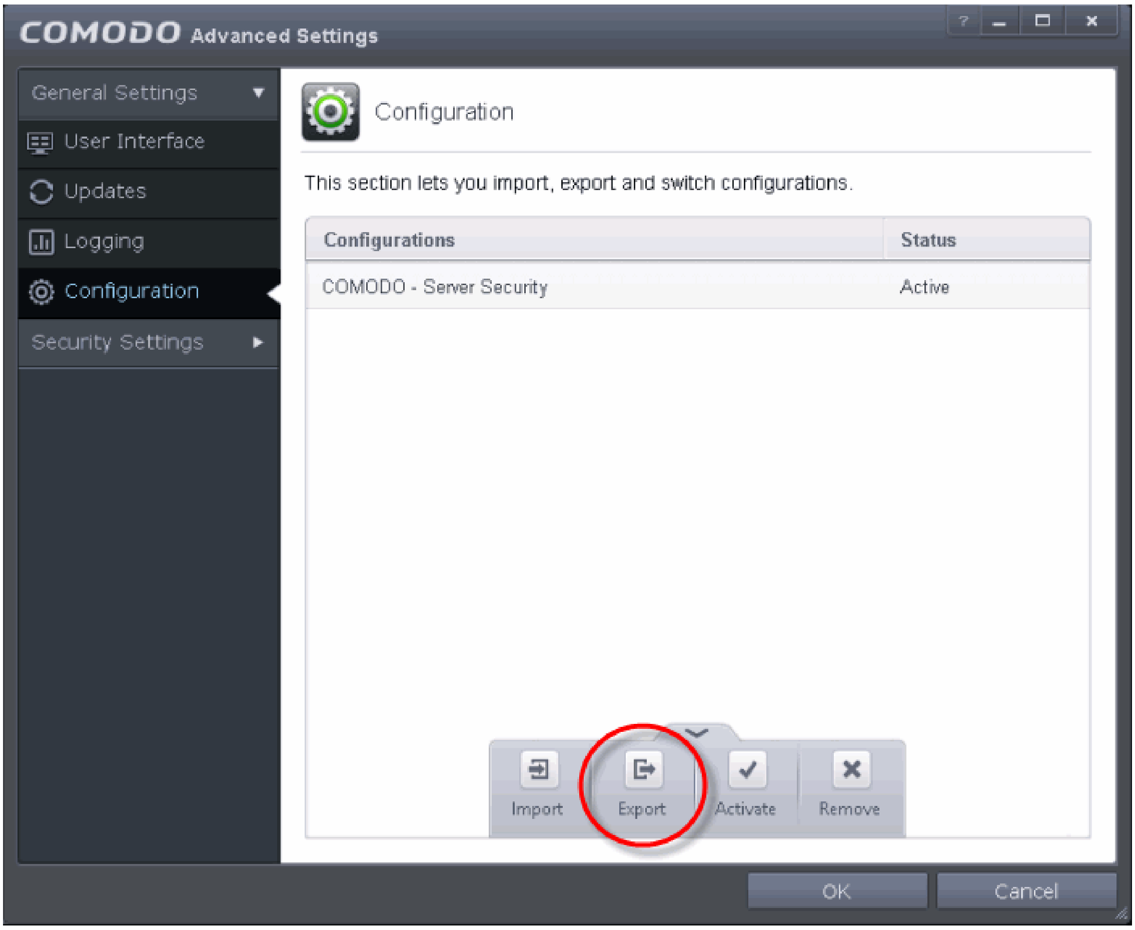
Click the area on which you would like more information:

- **Export a stored configuration to a file**
- **Import a saved configuration from a file**

- **Select a different active configuration setting**
- **Delete a inactive configuration profile**

Exporting a stored configuration to a file

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

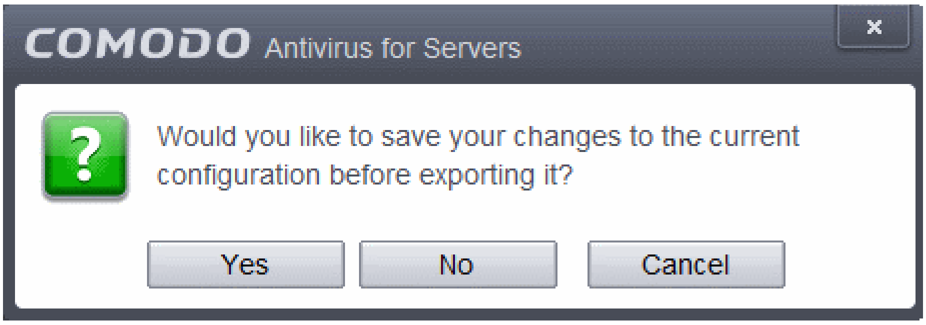


This section lets you import, export and switch configurations.

Configurations	Status
COMODO - Server Security	Active

2. Select the configuration, click the handle at the foot of the interface and choose 'Export'.

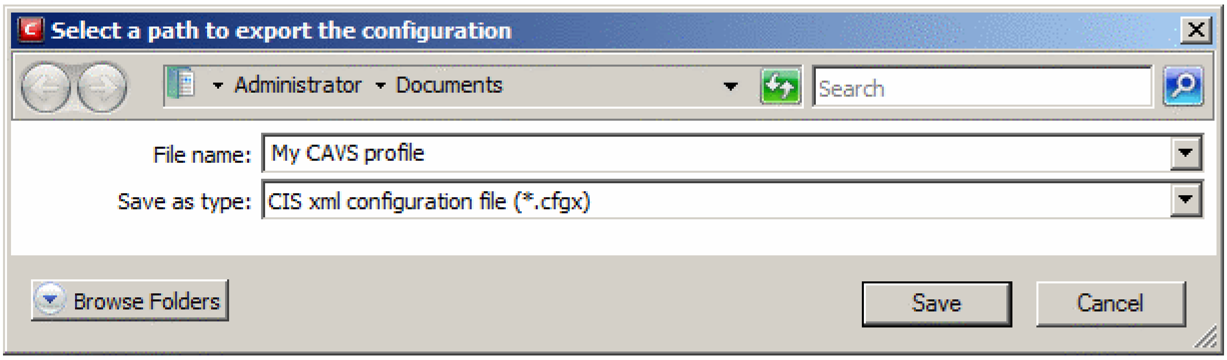
You will have the option to save any changes done in the selected configuration before exporting.



Would you like to save your changes to the current configuration before exporting it?

3. Click 'Yes' to save the changes to the current configuration before exporting, else click 'No'.

The 'Select a path to export the configuration' dialog will open.



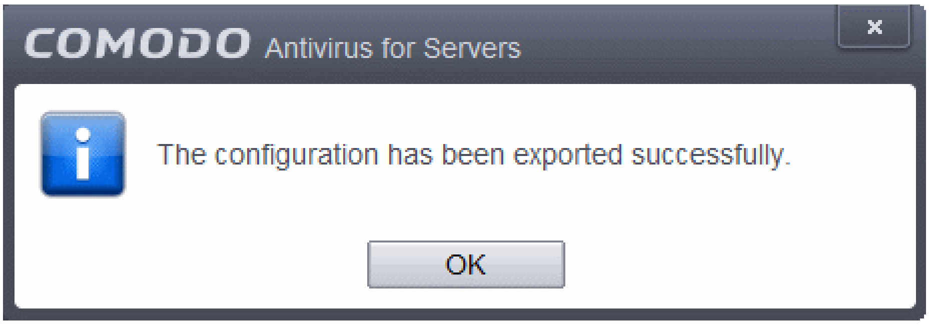
Select a path to export the configuration
Administrator ▸ Documents
Search
Browse Folders
Save
Cancel

File name: My CAVS profile

Save as type: CIS xml configuration file (*.cfgx)

4. Navigate to the location where you want to save the configuration file, type a name (e.g., 'My CAVS Profile') for the file to be saved in .cfgx format and click 'Save'.

A confirmation dialog will appear on successful export of the configuration.



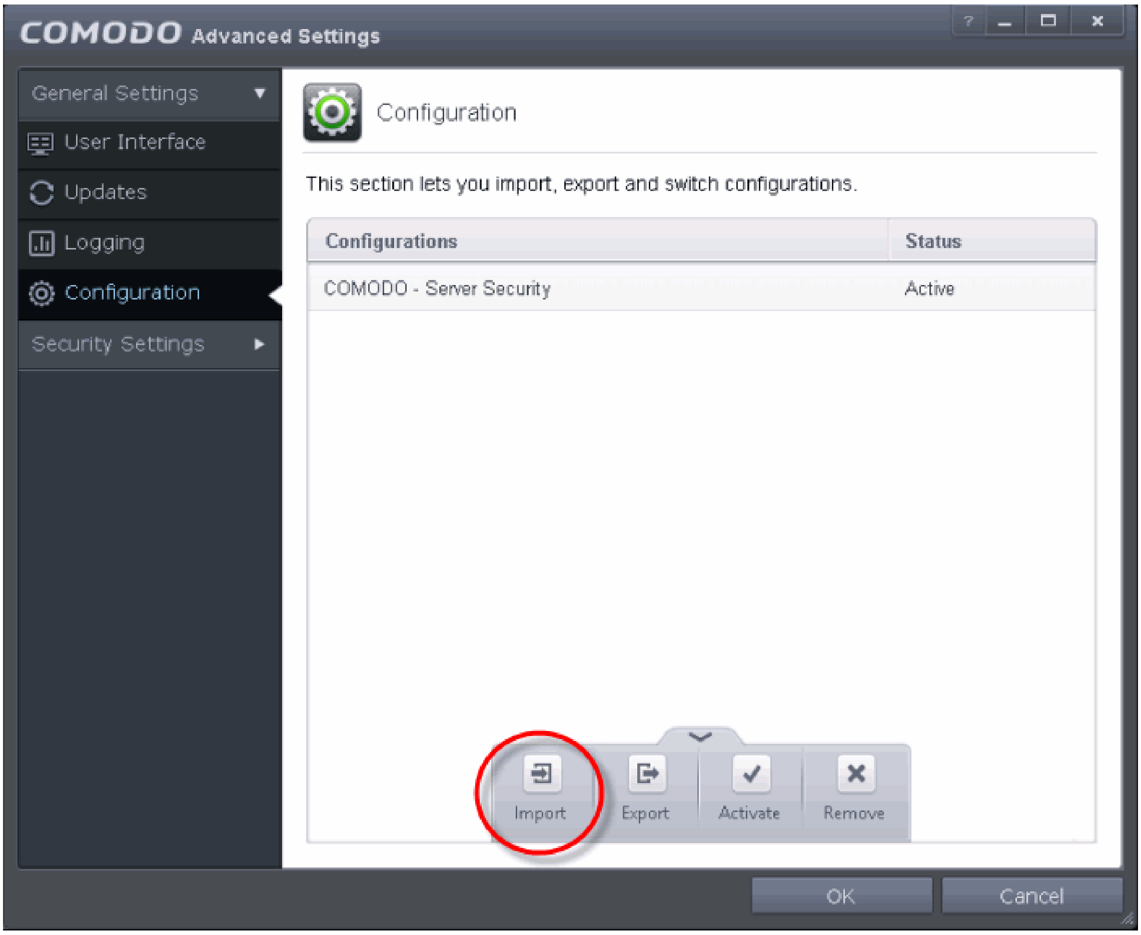
The configuration has been exported successfully.

Importing a saved configuration from a file

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

To import a profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface, click the handle at the foot of the interface and choose Import from the options.

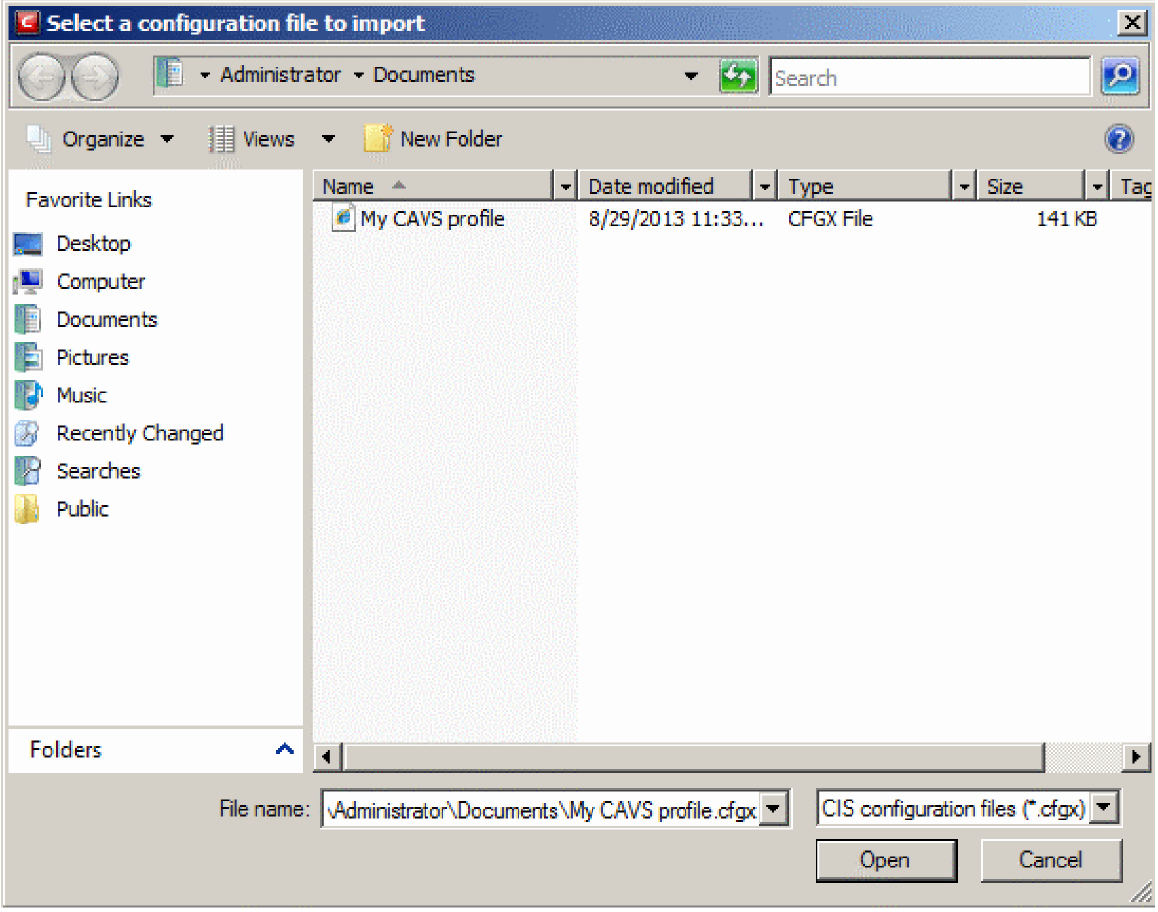


Configuration

This section lets you import, export and switch configurations.

Configurations	Status
COMODO - Server Security	Active

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

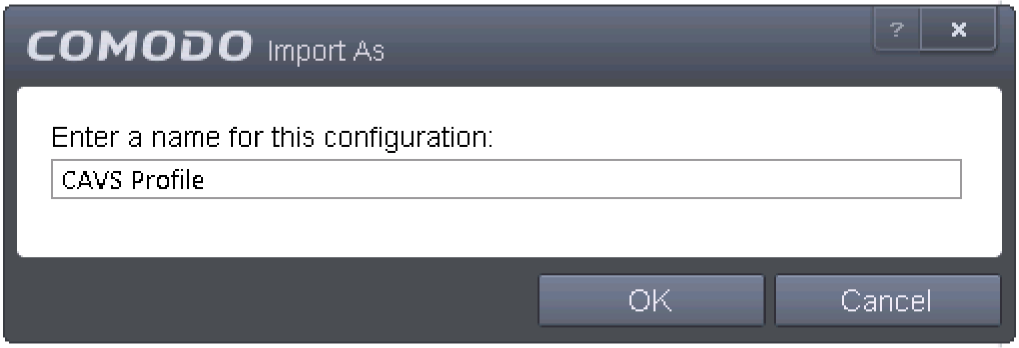


Name	Date modified	Type	Size	Tag
My CAVS profile	8/29/2013 11:33...	CFGX File	141 KB	

File name: \Administrator\Documents\My CAVS profile.cfgx

CIS configuration files (*.cfgx)

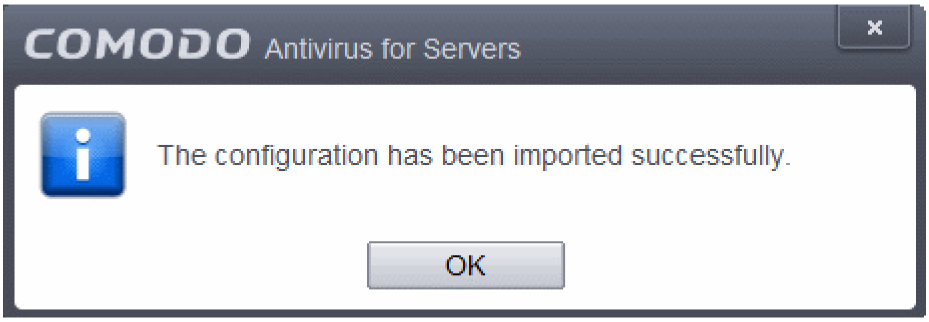
2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



Enter a name for this configuration:

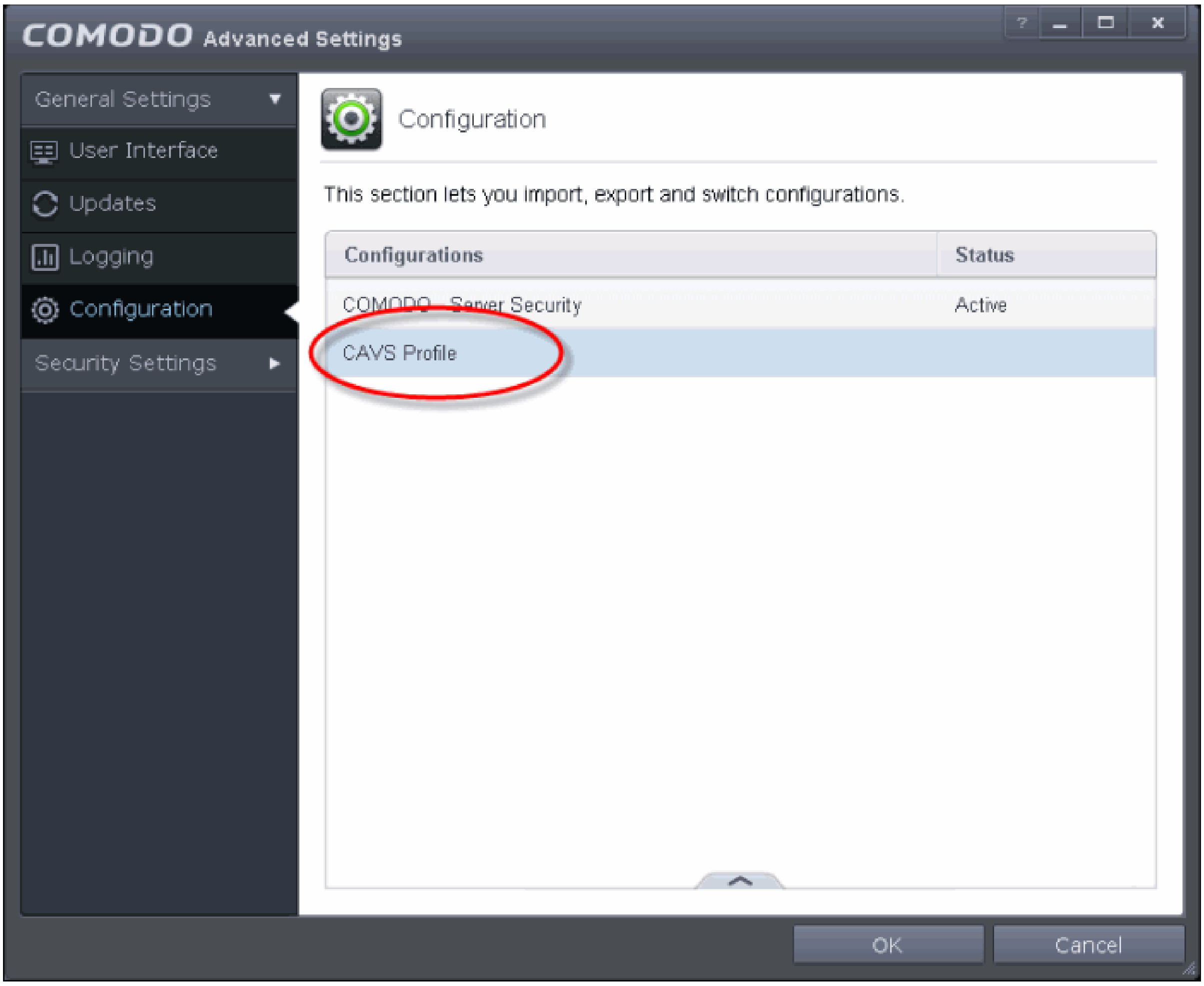
CAVS Profile

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



The configuration has been imported successfully.

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



This section lets you import, export and switch configurations.

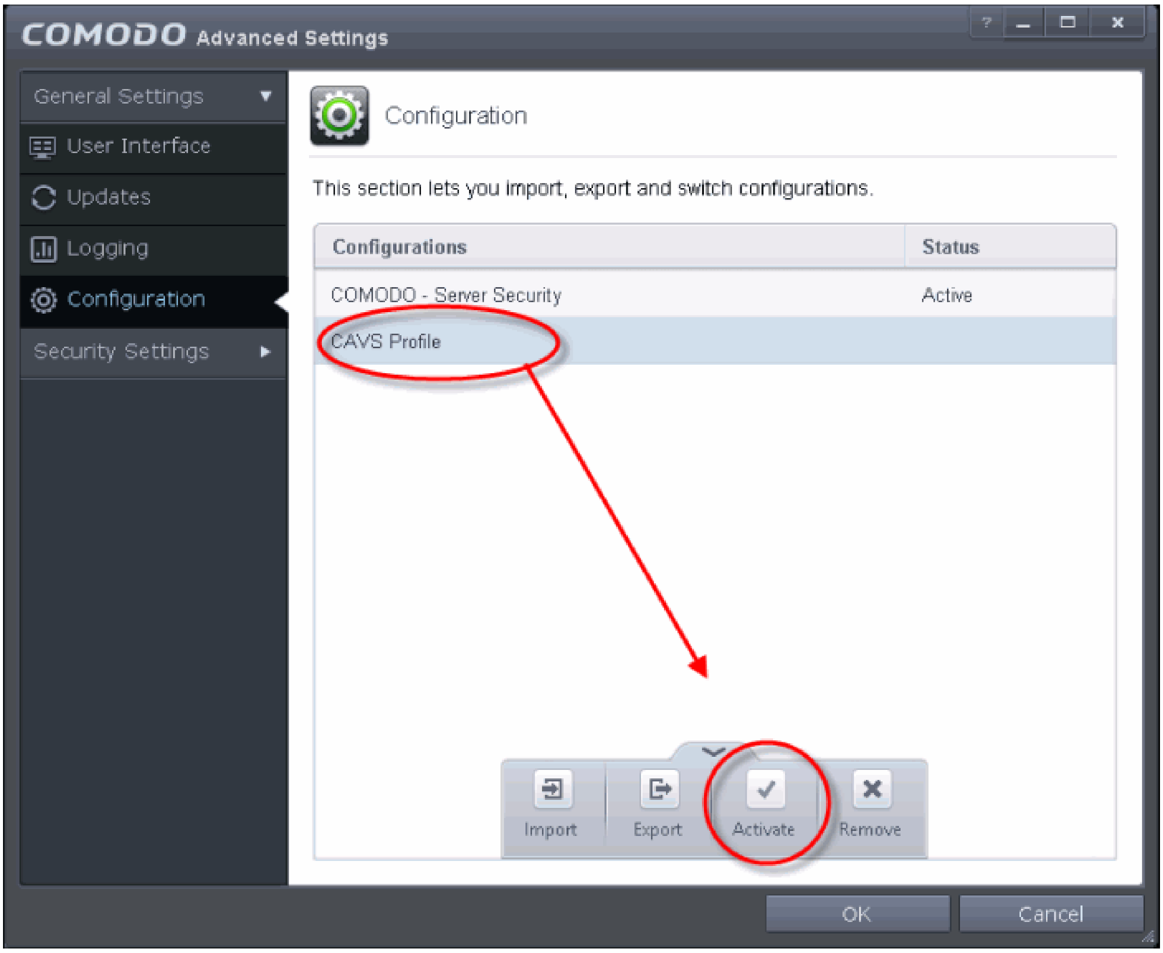
Configurations	Status
COMODO - Server Security	Active
CAVS Profile	

Selecting and Implementing a different configuration profile

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

To change the active configuration profile

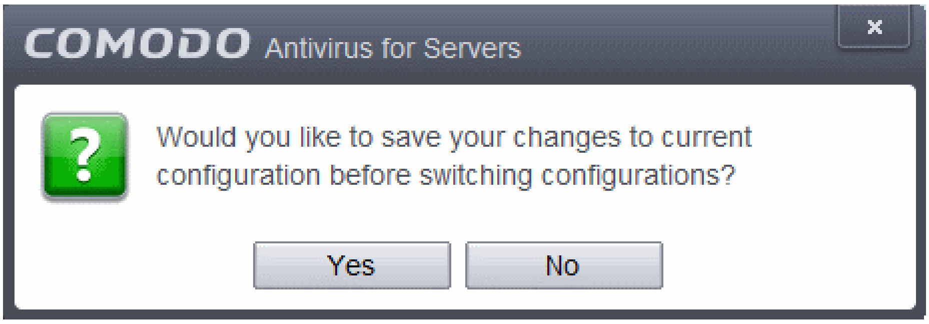
1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration profile you want to activate, click the handle at the foot of the interface and choose Activate from the options.



This section lets you import, export and switch configurations.

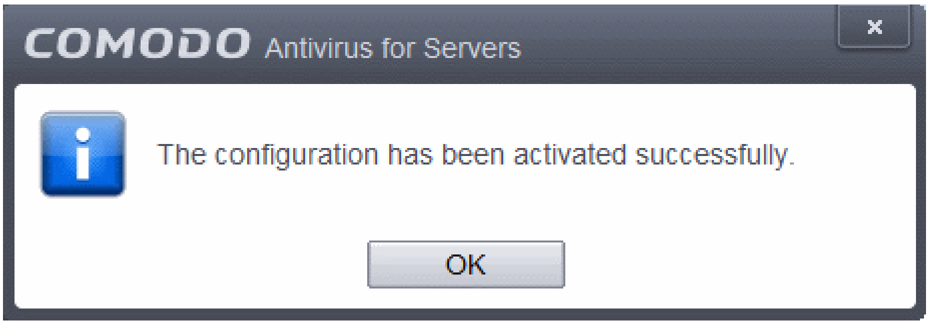
Configurations	Status
COMODO - Server Security	Active
CAVS Profile	

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



Would you like to save your changes to current configuration before switching configurations?

3. Click 'Yes' to save the changes to current configuration, else click 'No'. The new profile will be implemented immediately and the confirmation dialog will be displayed.



COMODO Antivirus for Servers

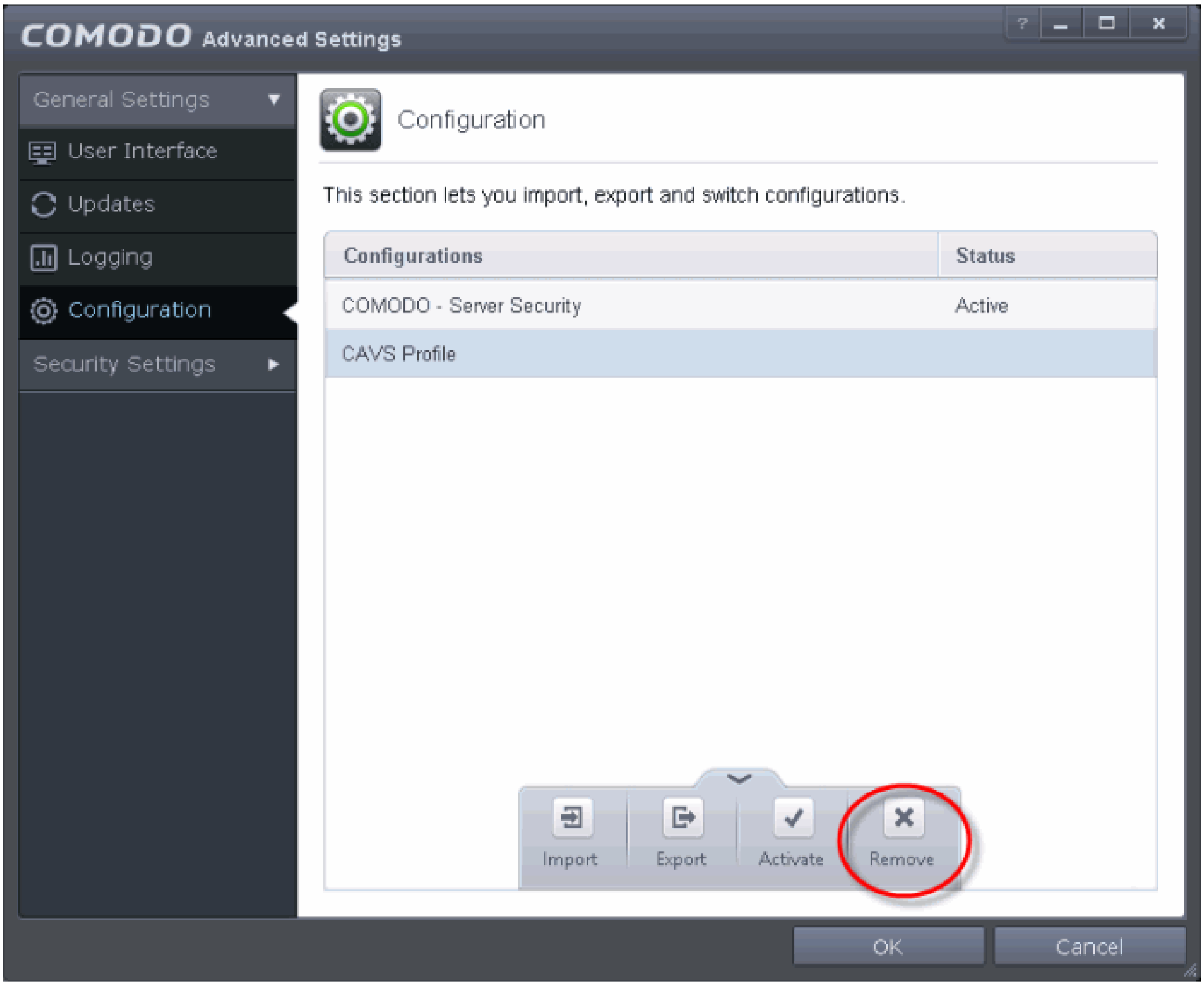
The configuration has been activated successfully.

Deleting an inactive configuration profile

You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that CAVAS is currently using - only the inactive ones. For example if the COMODO – Server Security is the active profile, you can only delete the inactive profiles.

To remove an unwanted profile

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



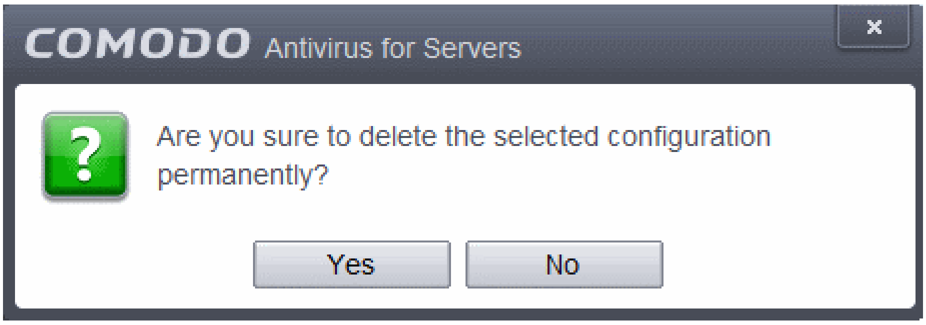
COMODO Advanced Settings

Configuration

This section lets you import, export and switch configurations.

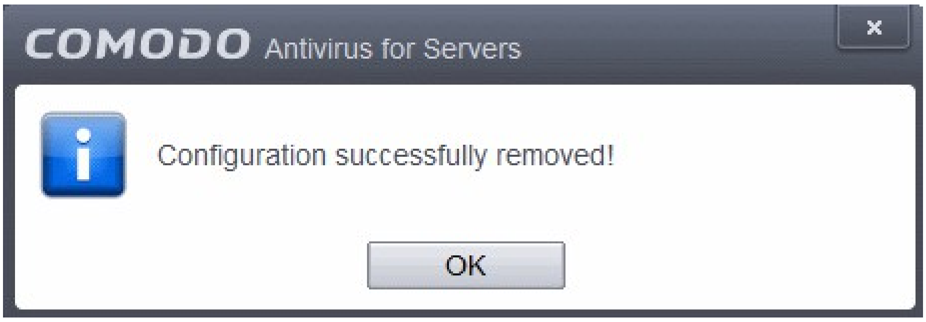
Configurations	Status
COMODO - Server Security	Active
CAVS Profile	

A confirmation dialog will be displayed.



Are you sure to delete the selected configuration permanently?

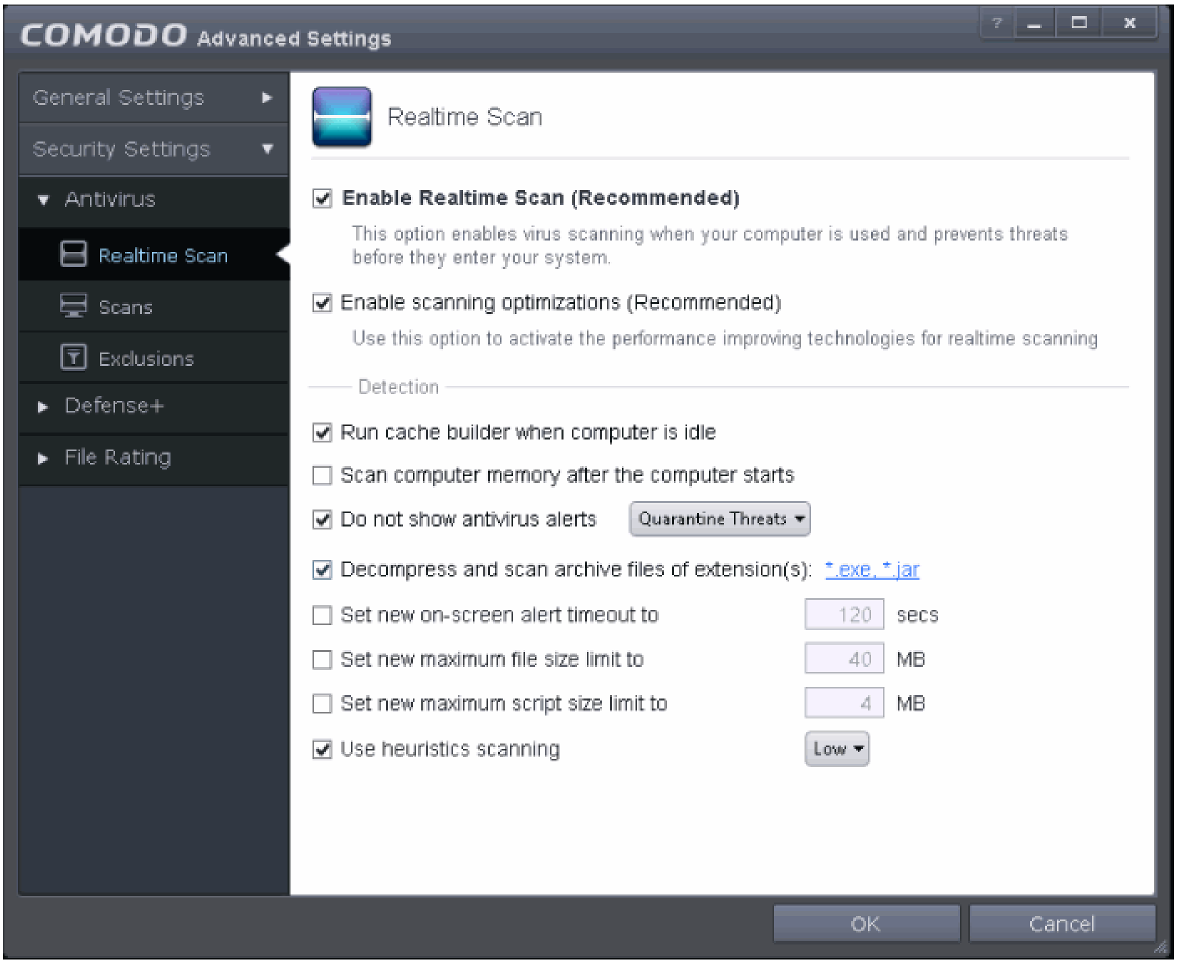
3. Click 'Yes'. The configuration profile will be deleted from your server.



Configuration successfully removed!

5.2. Security Settings

The Security Settings area enables you to perform granular configuration of the Antivirus, Defense+ and File ratings components of CAVS. Although these settings play a large part in governing the level of security offered by the application, CAVS does ship with secure defaults for all major settings so provides 'out-of-the-box' protection for all users.



Realtime Scan

☑ **Enable Realtime Scan (Recommended)**

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning

Detection

☑ Run cache builder when computer is idle

□ Scan computer memory after the computer starts

☑ Do not show antivirus alerts — Quarantine Threats

☑ Decompress and scan archive files of extension(s): *.exe, *.jar

□ Set new on-screen alert timeout to 120 secs

□ Set new maximum file size limit to 40 MB

□ Set new maximum script size limit to 4 MB

☑ Use heuristics scanning — Low

Click the following links to go straight to the topic that explains the respective settings screen:

- **Antivirus Settings**
  - **Real-time Scanner Settings**
  - **Custom Scan Settings**
  - **Exclusions**
- **Defense+ Settings**
  - **HIPS Behavior Settings**
  - **Active HIPS Rules**
  - **Predefined HIPS Rule Sets**
  - **Protected Objects**
  - **Hips Groups**
  - **Sandbox**
- **Manage File Rating**
  - **File Rating Settings**
  - **File Groups**
  - **File List**
  - **Submitted Files**
  - **Trusted Vendors List**

5.2.1. Antivirus Settings

The Antivirus Settings category has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe).

Click the following links to jump to each section:

- **Real Time Scan** - To set the parameters for on-access scanning;
- **Custom Scan** - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans;
- **Exclusions** - To see the list of ignored threats and to set the parameters for Exclusions.

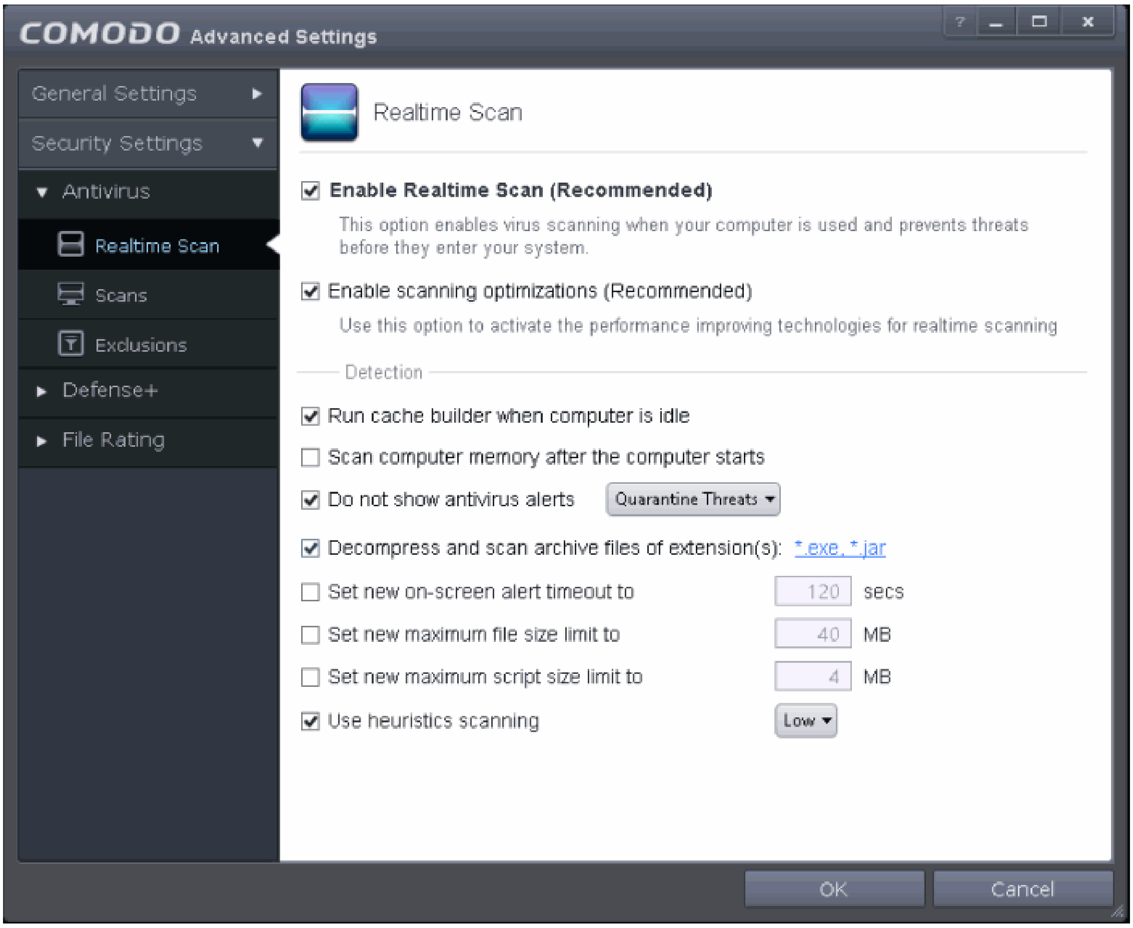
5.2.1.1. Real-time Scanner Settings

The real-time scanner (aka 'On-Access Scan') is always ON and checks files in real time when they are created, opened or copied (as soon as you interact with a file, Comodo Antivirus checks it). This instant detection of viruses assures you, the user, that your server is perpetually monitored for malware and enjoys the highest level of protection.

The real-time scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, however, you can specify that CAVS does not show you alerts if viruses are found but automatically deals with them (choice of auto-quarantine or auto-block/delete). It is highly recommended that you leave the Real Time Scanner enabled to ensure your system remains continually free of infection.

To open the Real Time Scan settings panel

- Click 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Antivirus > Realtime Scan':



Realtime Scan

☑ **Enable Realtime Scan (Recommended)**

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Enable scanning optimizations (Recommended)

Use this option to activate the performance improving technologies for realtime scanning

Detection

☑ Run cache builder when computer is idle

☐ Scan computer memory after the computer starts

☑ Do not show antivirus alerts: Quarantine Threats

☑ Decompress and scan archive files of extension(s): *.exe, *.jar

☐ Set new on-screen alert timeout to 120 secs

☐ Set new maximum file size limit to 40 MB

☐ Set new maximum script size limit to 4 MB

☑ Use heuristics scanning: Low

- **Enable Realtime Scan** - Allows you to enable or disable real-time scanning. Comodo recommends to leave this option selected.(***Default=Enabled***)
- **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization

techniques like running the scan in the background in order to reduce consumption of system resources and speed-up the scanning process ***(Default = Enabled)***

Note: The above two settings can be modified from the 'Advanced View' of the Home screen by clicking the status link beside Antivirus. If you choose Disabled option, both 'Enable Realtime Scan' and 'Enable scanning optimizations' will be disabled. If you choose 'Stateful', both the settings will be enabled and on choosing 'On Access', only 'Enable Realtime Scan' will be enabled.

Detection Settings

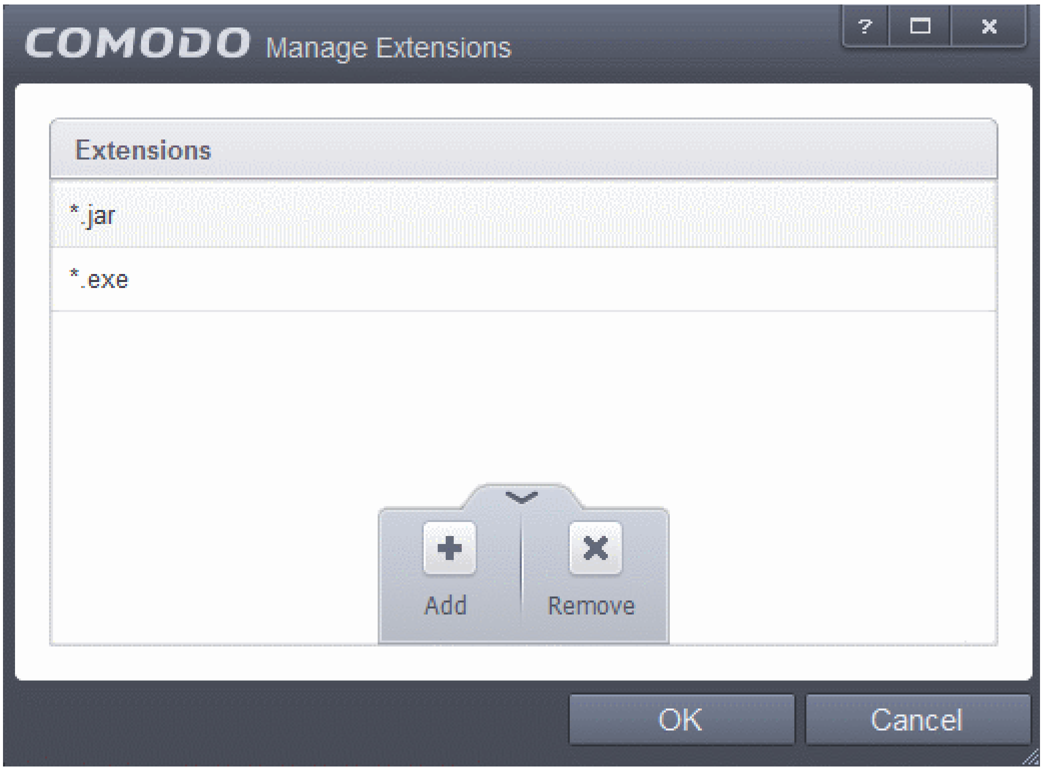
- **Run cache builder when computer is idle -** CAVS runs the Antivirus Cache Builder whenever the server is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (***Default = Enabled***).
- **Scan computer memory after the computer starts** - When this check box is selected, the Antivirus scans the system memory during system start-up ***(Default = Disabled)***
- **Do not show antivirus alerts -** Allows you to configure whether or not to show antivirus alerts when malware is encountered. Choosing 'Do not show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CAVS should automatically take - either 'Block Threats' or 'Quarantine Threats'. (***Default = Enabled***)
  - **Quarantine Threats** - Moves the detected threat(s) to quarantine for your later assessment and action. (***Default***)
  - **Block Threats** - Stops the application or file from execution, if a threat is detected in it.

Note: If you deselect this option and thus enable alerts then your choice of quarantine/block is presented within the alert itself.

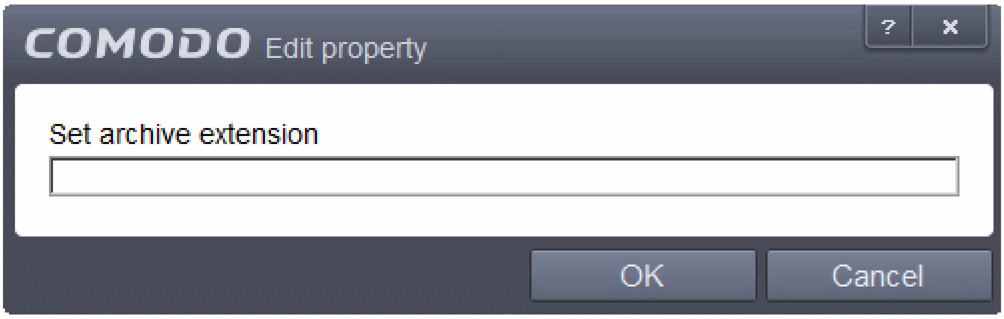
- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default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

  You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

  - Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.



  - To add a file type, click the up arrow at the bottom center and click 'Add'.



  - Enter the extension (e.x.: rar, msi, zip, 7z, cab and so on) to be included in the Edit property dialog and click OK.
  - Repeat the process to add more extensions
  - Click OK in the 'Manage Extensions' dialog

- **Set new on-screen alert timeout to** - This box allows you to set the time period (in seconds) for which the alert message should stay on the screen. (***Default = 120 seconds***)
- **Set new maximum file size limit to** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned. (***Default = 40 MB***)
- **Set new maximum script size limit to** - This box allows you to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (***Default = 4 MB***)
- **Use heuristics scanning** - Allows you to enable or disable Heuristics scanning and define scanning level. (***Default = Enabled***)

  Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  Leave this option selected to keep Heuristics scanning enabled. Else, deselect this checkbox. If enabled, you can select the level of Heuristic scanning from the drop-down:

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

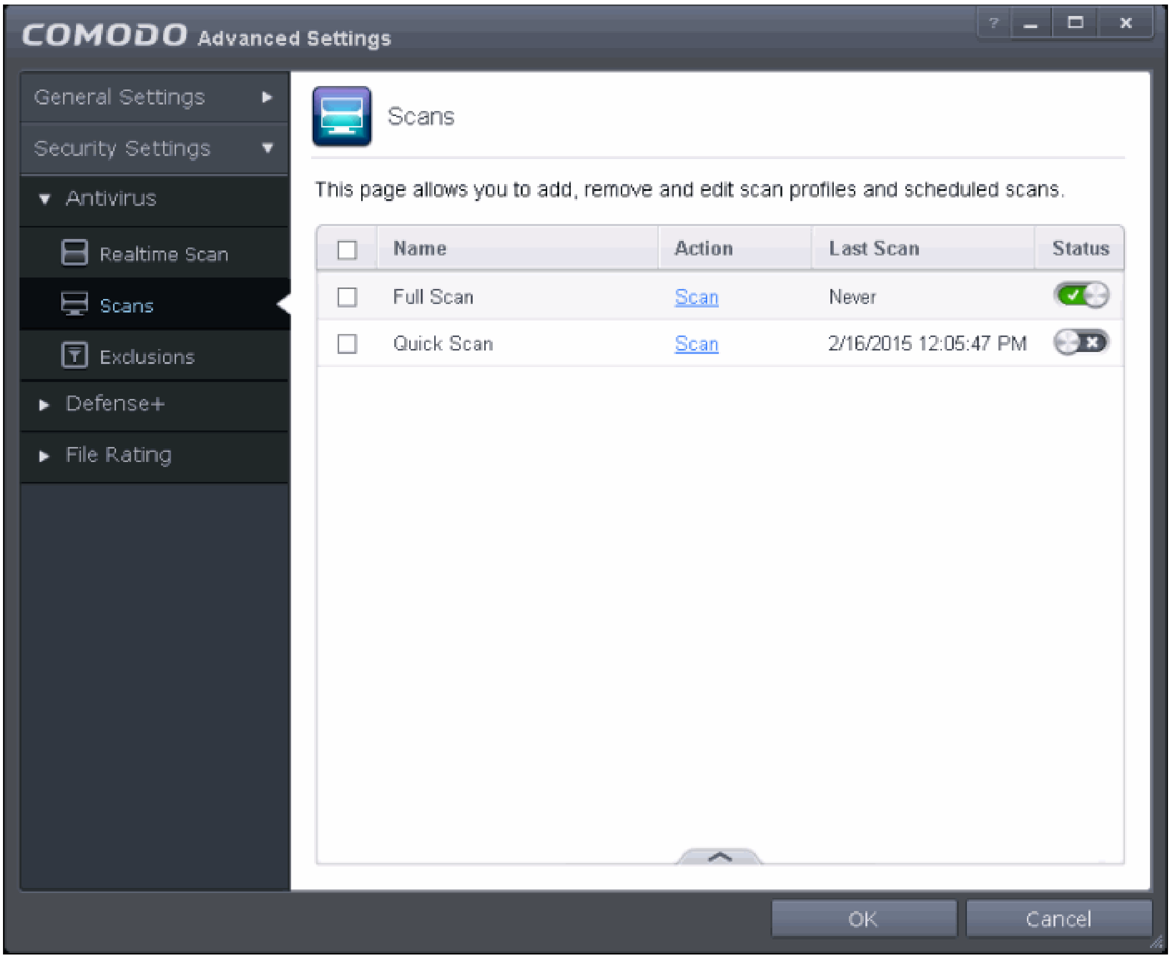
5.2.1.2. Scan Profiles

The Scan Profiles area allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CAVS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)
- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To open the panel

- Click Security Settings > Antivirus > 'Scans' tab in the 'Advanced Settings' panel.



Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗

CAVS ships with two predefined scan profiles:

- **Full Scan** - Covers every local drive, folder and file on your system.
- **Quick Scan** - Covers critical areas in your server which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of your server and keeping them clean is essential.

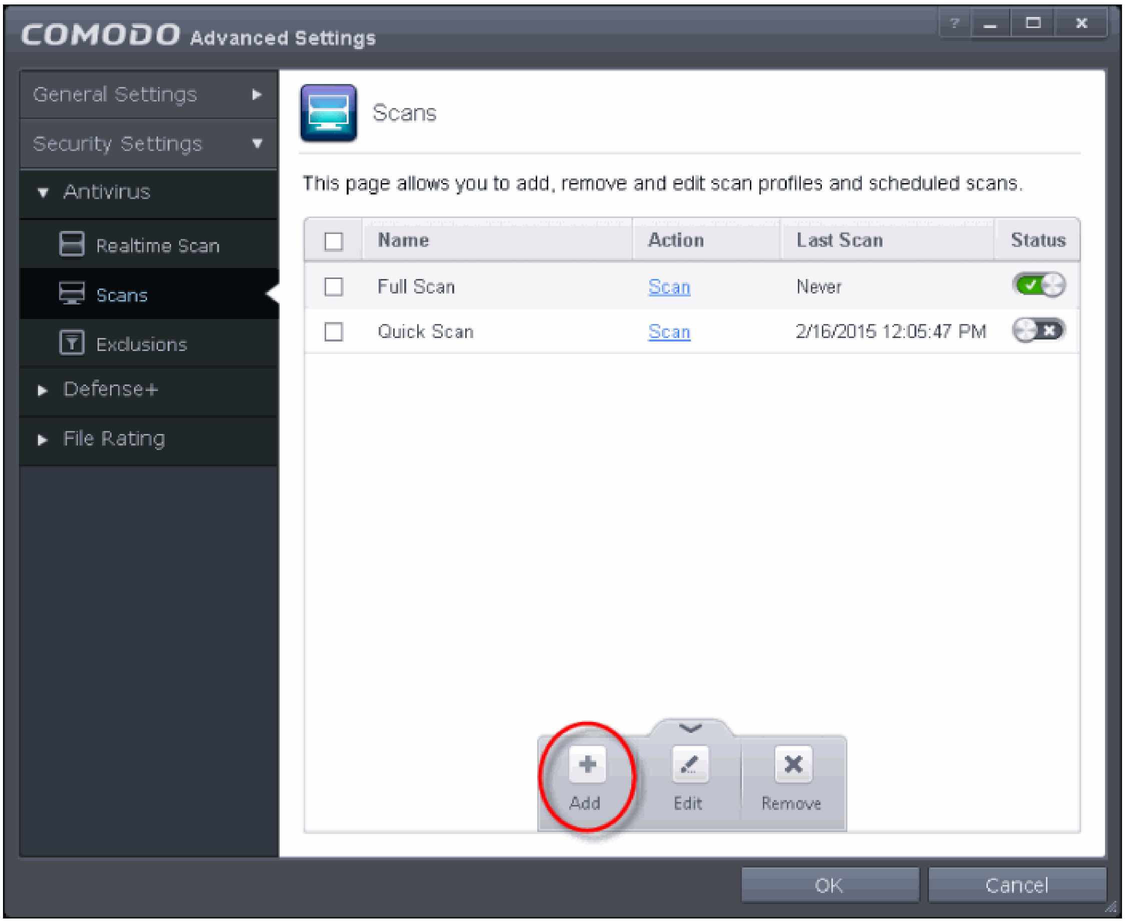
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

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

To create a custom profile

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

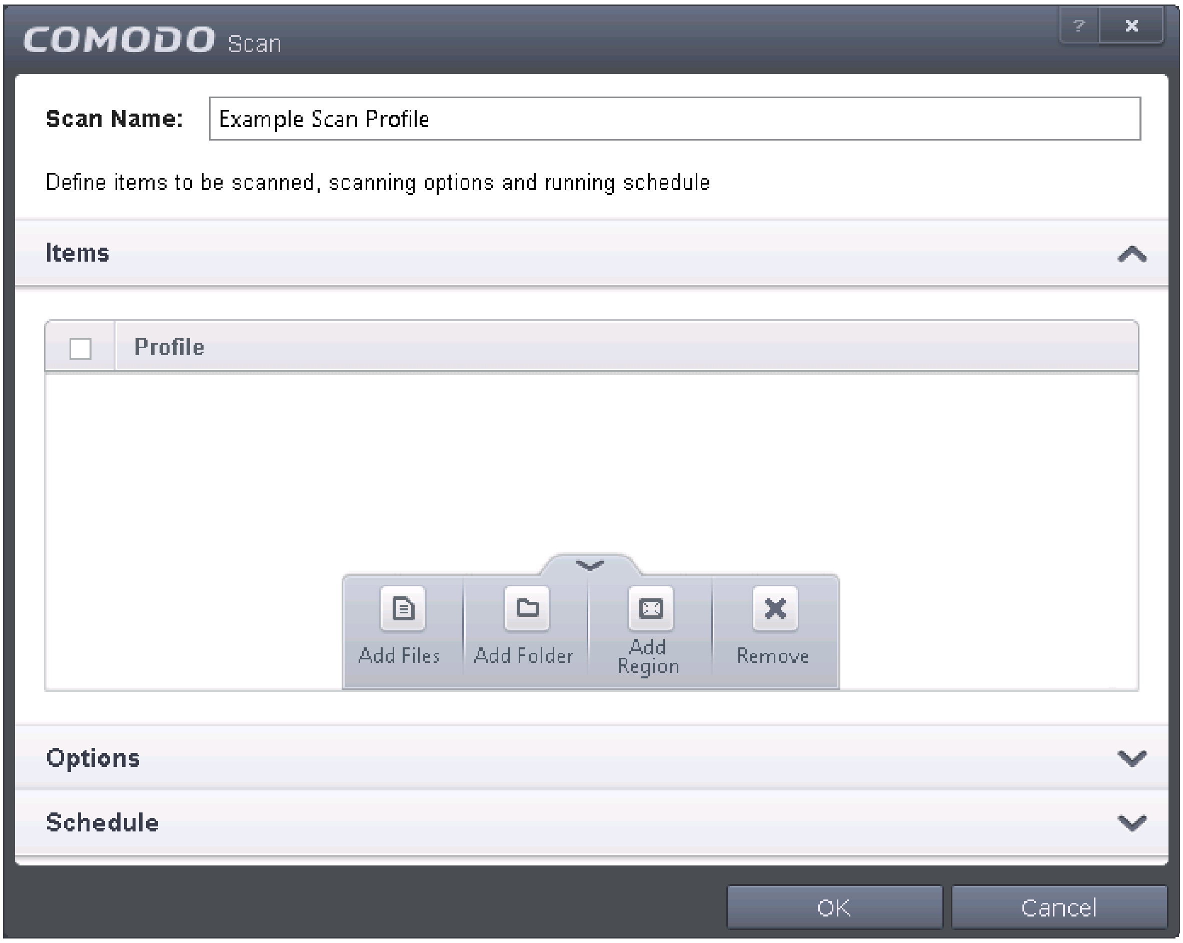


This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗

The scan profile interface will be displayed.

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

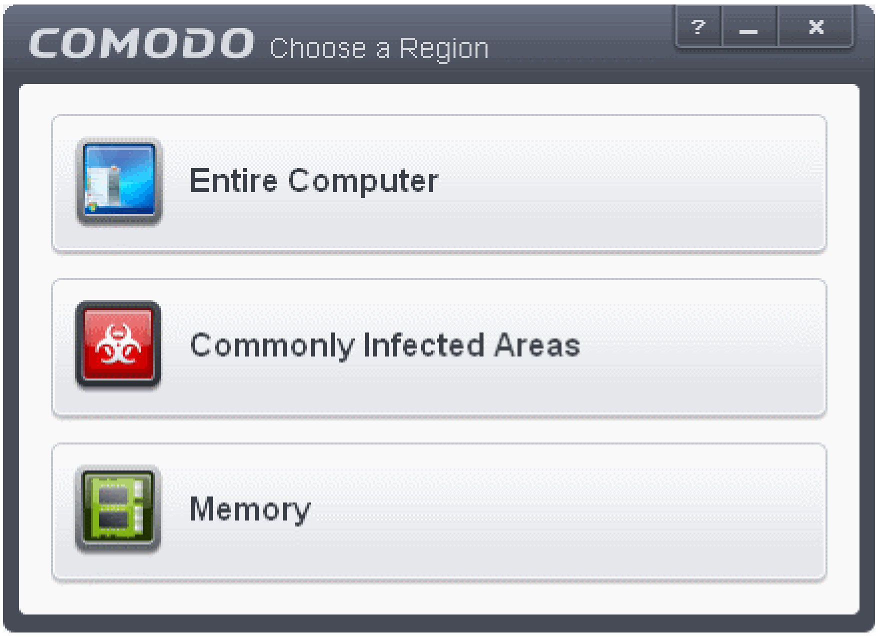


Scan Name: Example Scan Profile

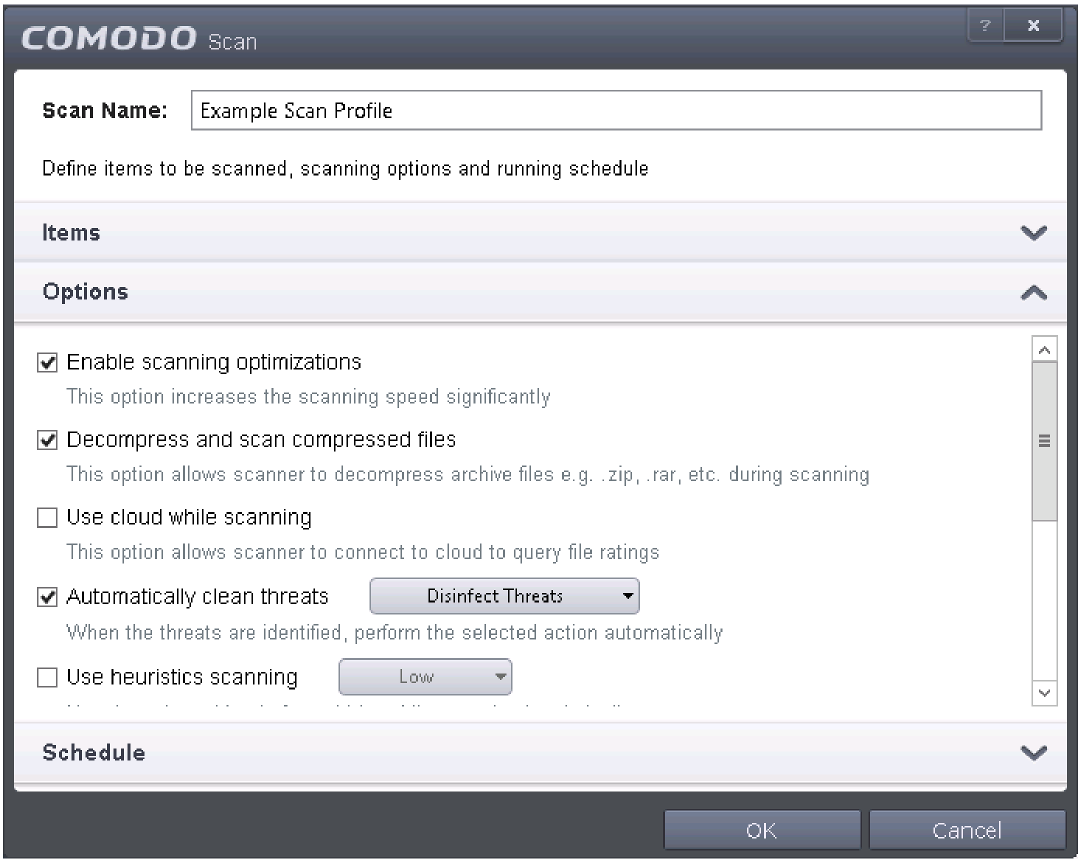
Define items to be scanned, scanning options and running schedule

□	Profile

- **Add Files -** Allows you to navigate to specific files that you wish to add to the profile
- **Add Folder -** Opens the 'Browse For Folder' window and allows you to select entire folders
- **Add Region -** Allows you to add predefined regions to the profile. For example, 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.



- Repeat the process to add more items into the profile
- Click 'Options' to further customize the scan



COMODO Scan

Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

☑ Enable scanning optimizations
This option increases the scanning speed significantly

☑ Decompress and scan compressed files
This option allows scanner to decompress archive files e.g. .zip, .rar, etc. during scanning

□ Use cloud while scanning
This option allows scanner to connect to cloud to query file ratings

☑ Automatically clean threats: Disinfect Threats
When the threats are identified, perform the selected action automatically

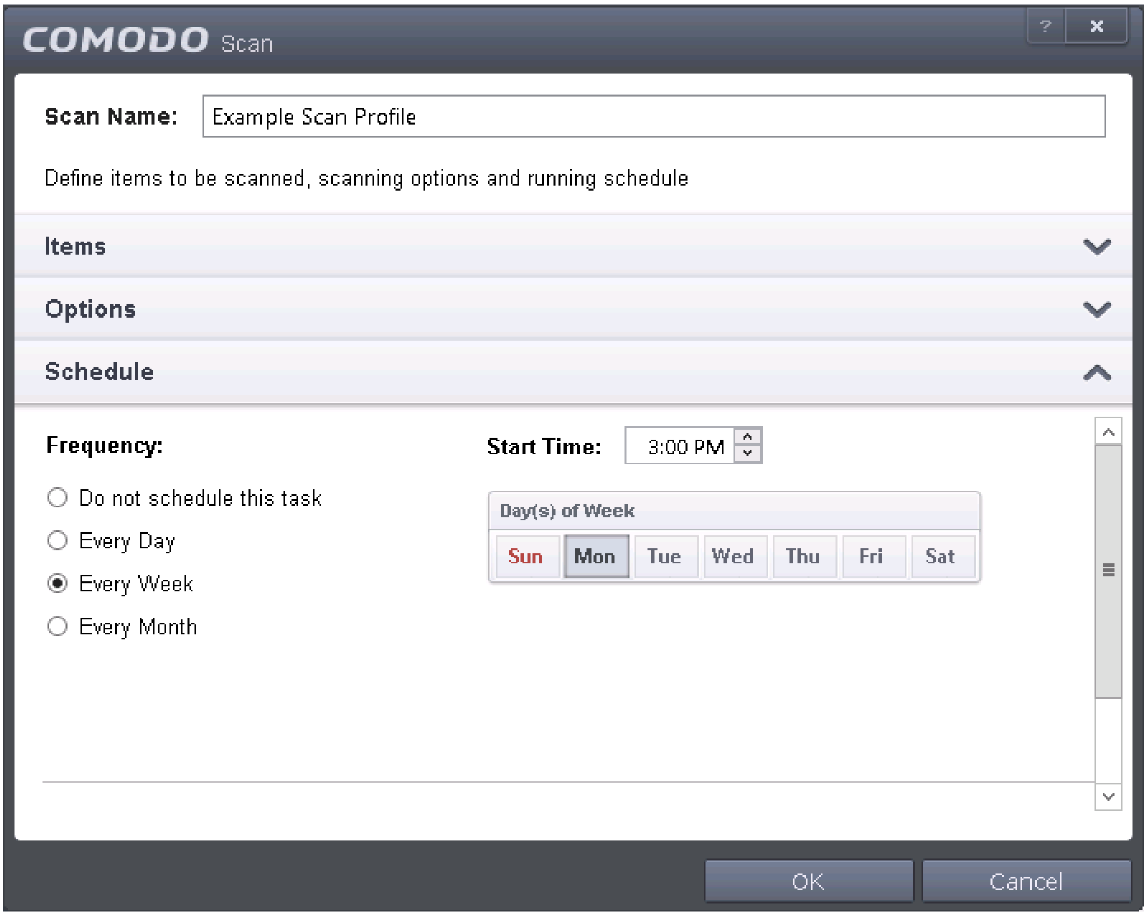
□ Use heuristics scanning: Low

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

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

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

        - **Low -** Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
        - **Medium -** Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
        - **High -** Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
    - **Limit maximum file size to -** Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
    - **Run Scan with -** Enables you to set the priority of the scanning from High to Low and to run at background. ***(Default = Disabled)***.
    - **Update virus database before running -** Selecting this option makes CAVS to check for virus database updates and if available, update the database before commencing the scan. ***(Default = Disabled)***.
    - **Detect potentially unwanted applications -** When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their server and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. ***Default = Disabled)***.
- If you want the scan to be performed periodically, set a Schedule for the custom scan by clicking 'Schedule'



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Frequency:

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

Start Time: 3:00 PM

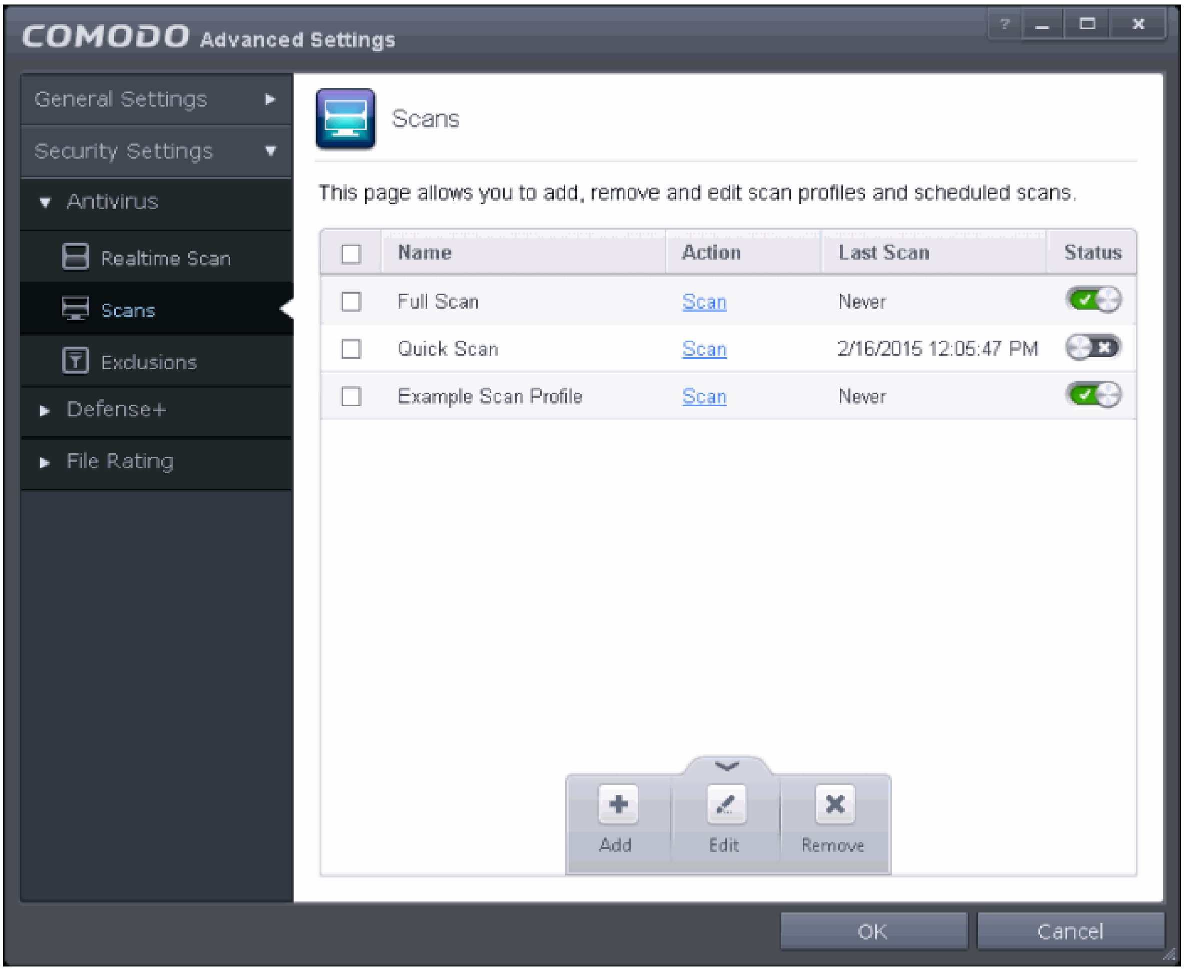
Day(s) of Week: Sun [✓ Mon] Tue Wed Thu Fri Sat

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

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

- Click OK to save the profile.

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



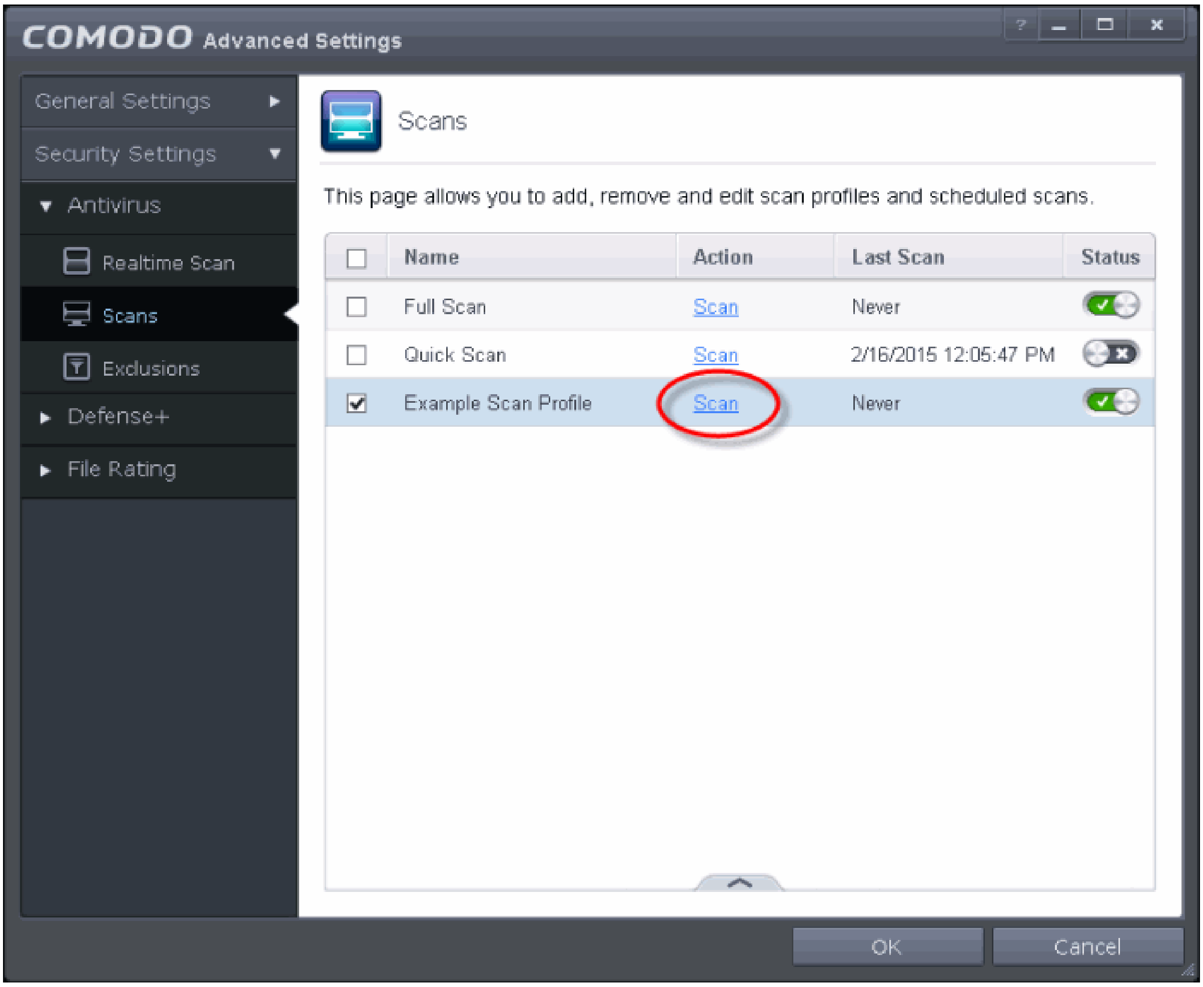
This page allows you to add, remove and edit scan profiles and scheduled scans.

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	2/16/2015 12:05:47 PM	✕
□	Example Scan Profile	Scan	Never	✓

To run a custom scan as per scan profile

- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface

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

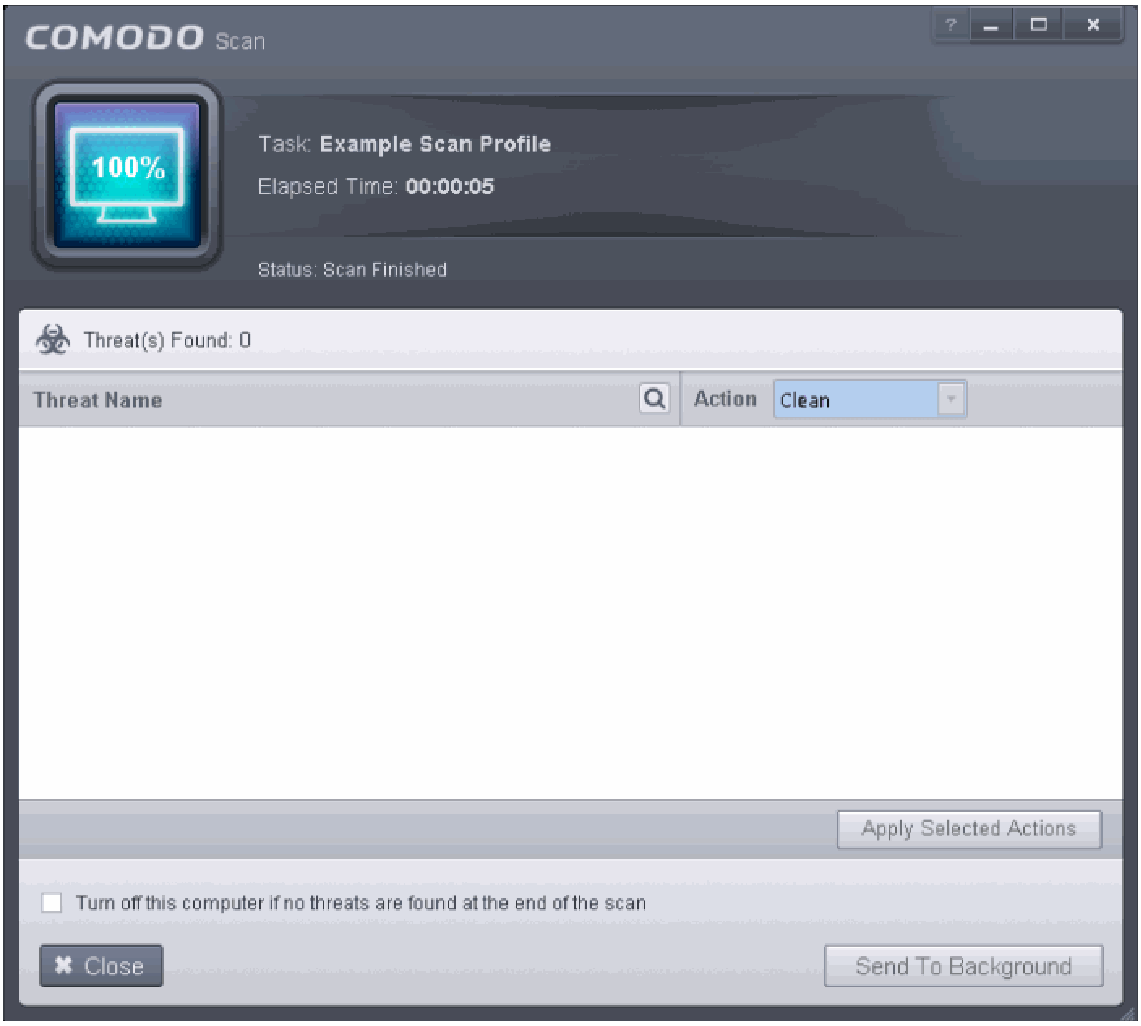


Scans

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

□	Name	Action	Last Scan	Status
□	Full Scan	Scan	Never	✓
□	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗
☑	Example Scan Profile	Scan	Never	✓

- The scan will be started and on completion the results will be displayed.



Task: **Example Scan Profile**

Elapsed Time: **00:00:05**

Status: Scan Finished

Threat(s) Found: 0

Threat Name	Action: Clean

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

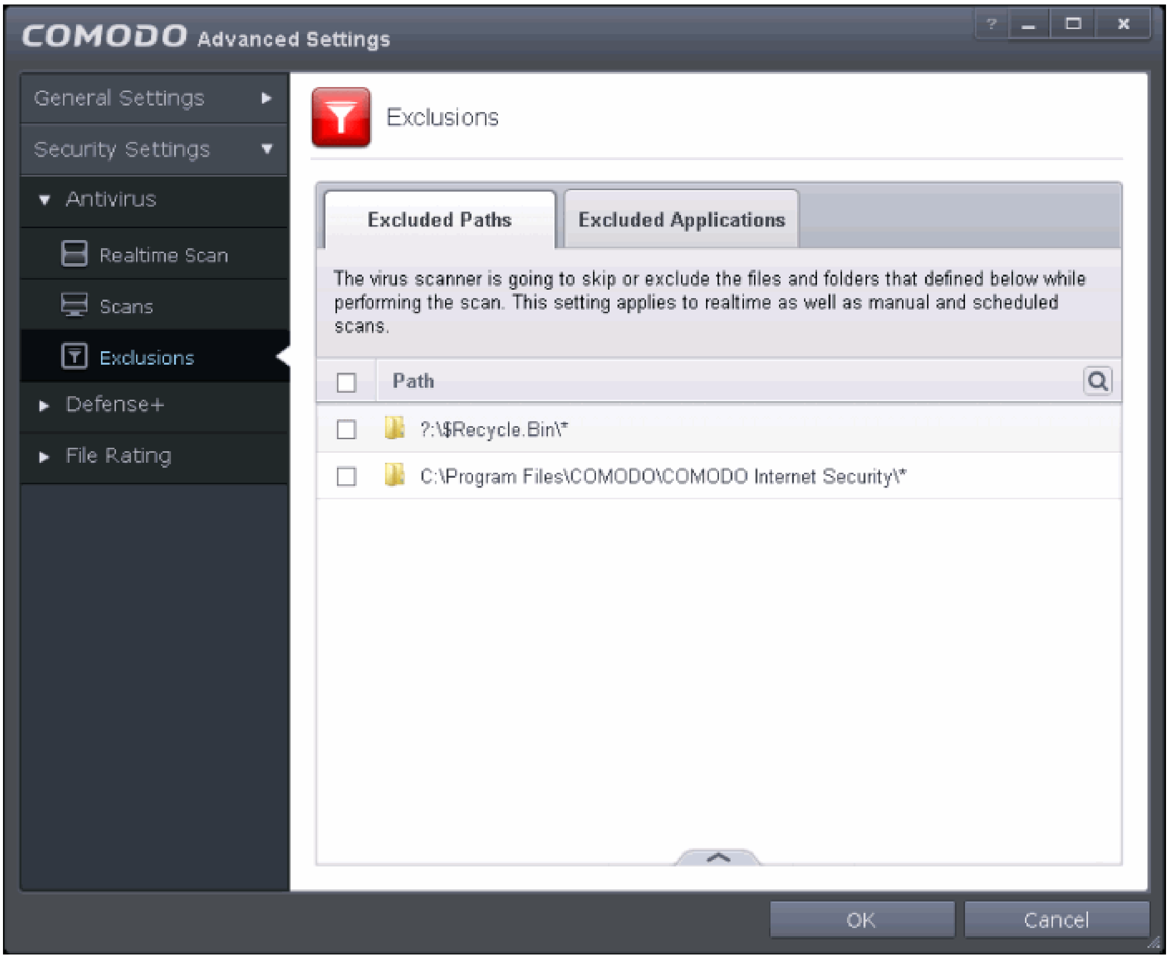
The scan results window will display any threats discovered during the scan (Viruses, Rootkits, Malware and so on). Refer to **Processing the infected files** for more details.

5.2.1.3. Exclusions

The 'Exclusions' panel under the Antivirus Settings displays a list of paths and applications/files for which you have selected **Ignore** from the **Scan Results** window of various scans or added to the Exclusions from an antivirus alert.

To open the Exclusions panel

- Click Security Settings > Antivirus > 'Exclusions' tab in the 'Advanced Settings' panel.



The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

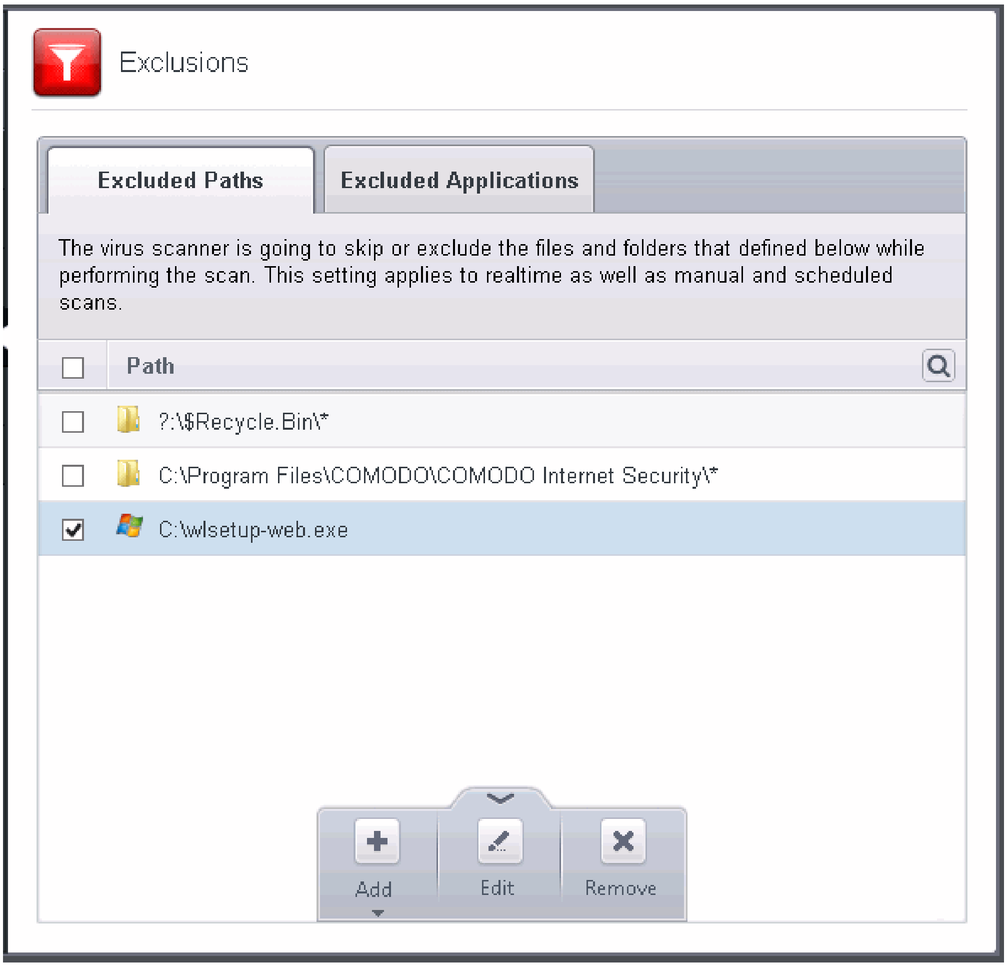
□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*

The Exclusions panel has two tabs:

- **Excluded Paths -** Displays a list of paths/folders/files in your server, which are excluded from both real-time and on-demand antivirus scans. Refer to the section **Excluding Drives/Folders/Files from all types of scans** for more details on adding and removing exclusion items in this interface.
- **Excluded Applications** - Displays a list of programs/applications in your server, which are excluded from real-time antivirus scans. The items are included on clicking 'Ignore' from the **Scan Results** window of various scans and **Antivirus Alerts** or manually. Please note that these items are excluded only on real-time sans but will be scanned on running on-demand scans Refer to the section **Excluding Programs/Applications from real-time scans** more details on manually adding and removing exclusion items in this interface.

Excluding Drives/Folders/Files from all types of scans

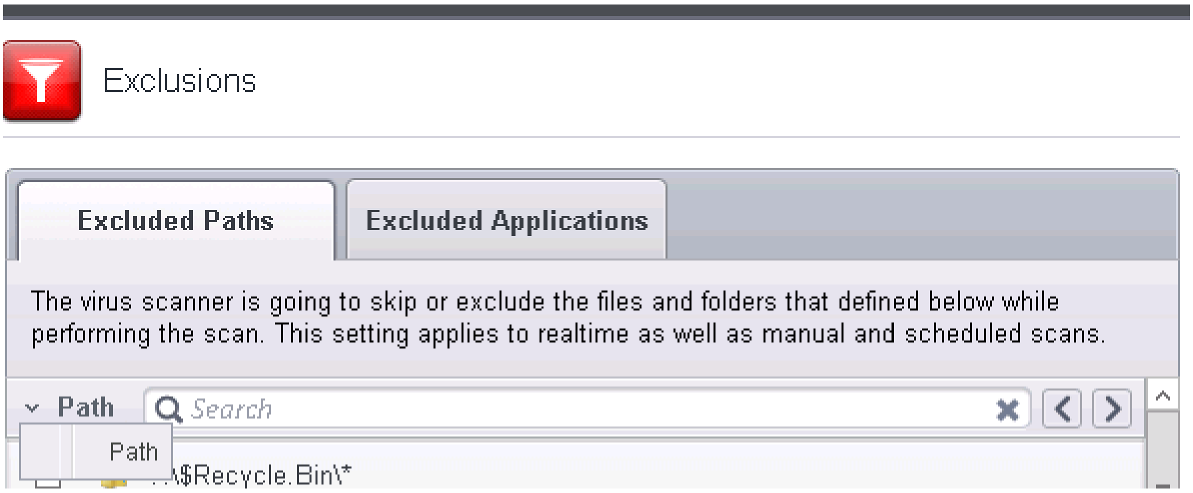
You can exclude a drive partition, a folder, a sub-folder or a file from both the real-time and on-demand/custom scheduled antivirus scans at any time, by adding them to Excluded Paths.



The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
☑	C:\wlsetup-web.exe

You can use the search option to find a specific excluded path, folder or file from the list by clicking the 🔍 search icon at the far right in the column header.

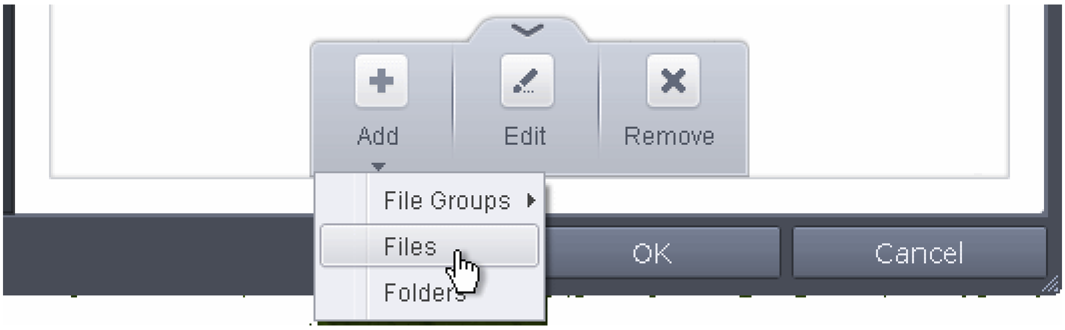


The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

- Enter the path, folder name or file name to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

To add item(s) to excluded paths

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



You can choose to add a:

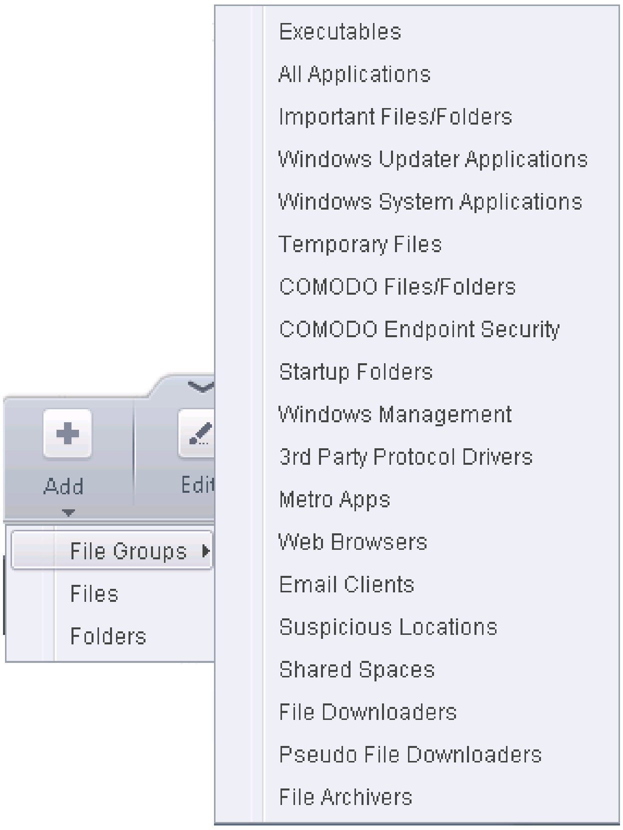
- **File Group**
- **Drive partition/Folder**

  or

- **an individual file**

Adding a File Group

- Choosing File Groups allows you to exclude a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

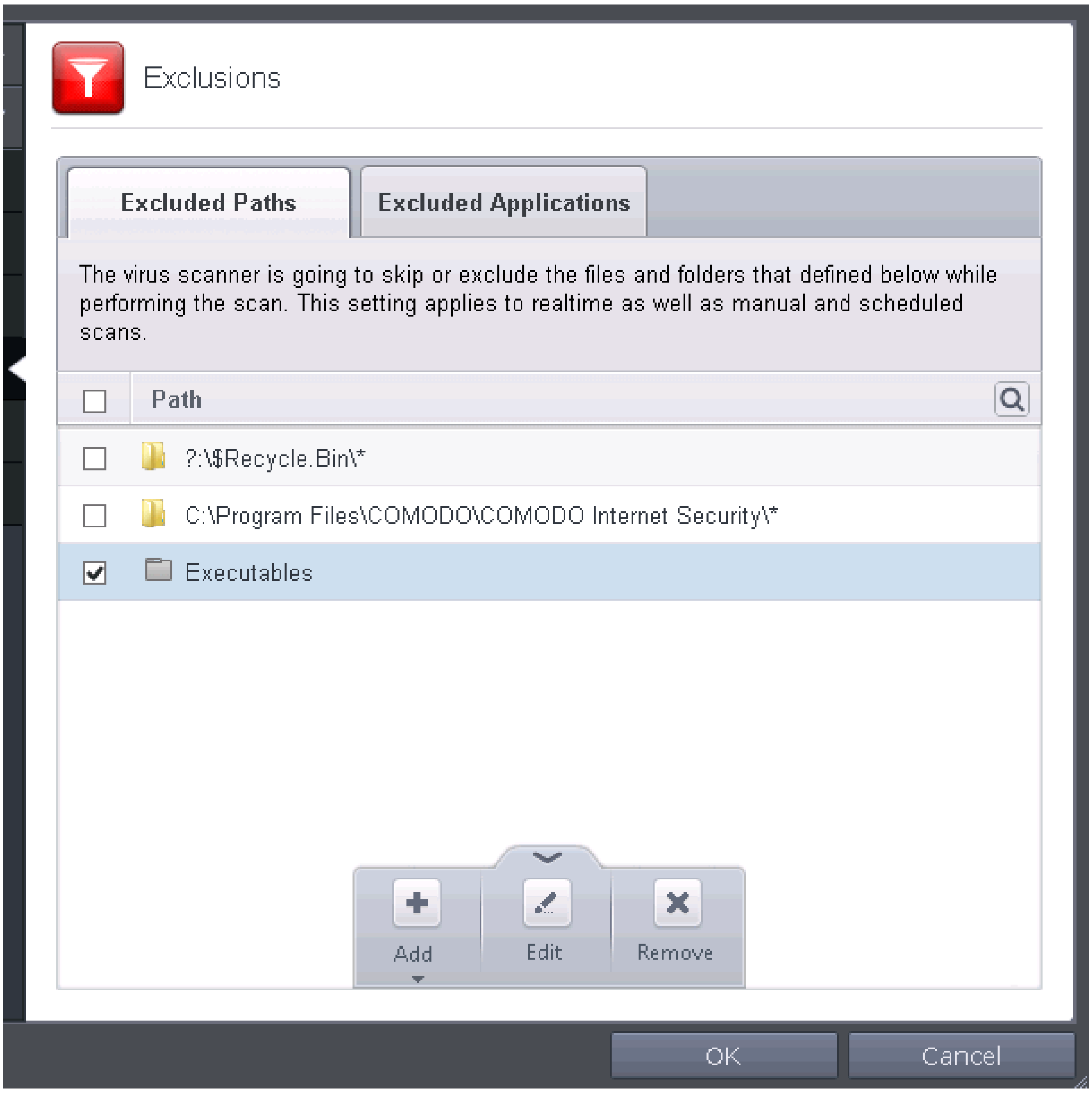


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

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

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

The file groups will be added to Excluded Paths.



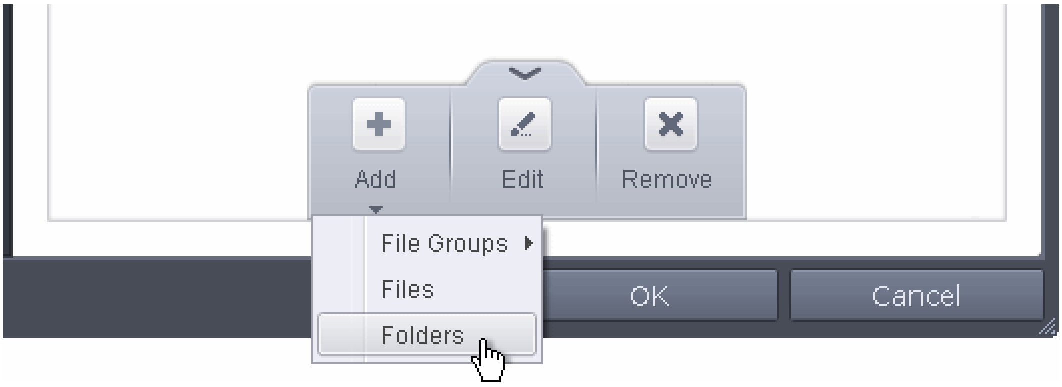
The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
☑	Executables

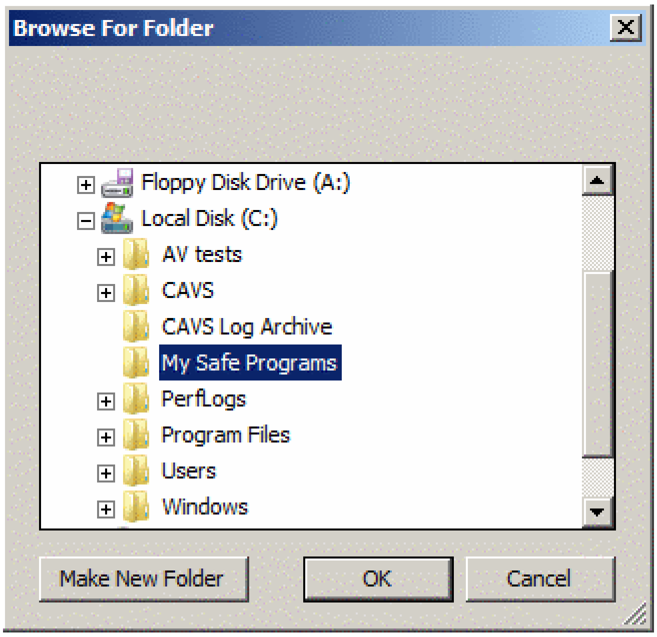
- Repeat process to add more file groups. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding a Drive Partition/Folder

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

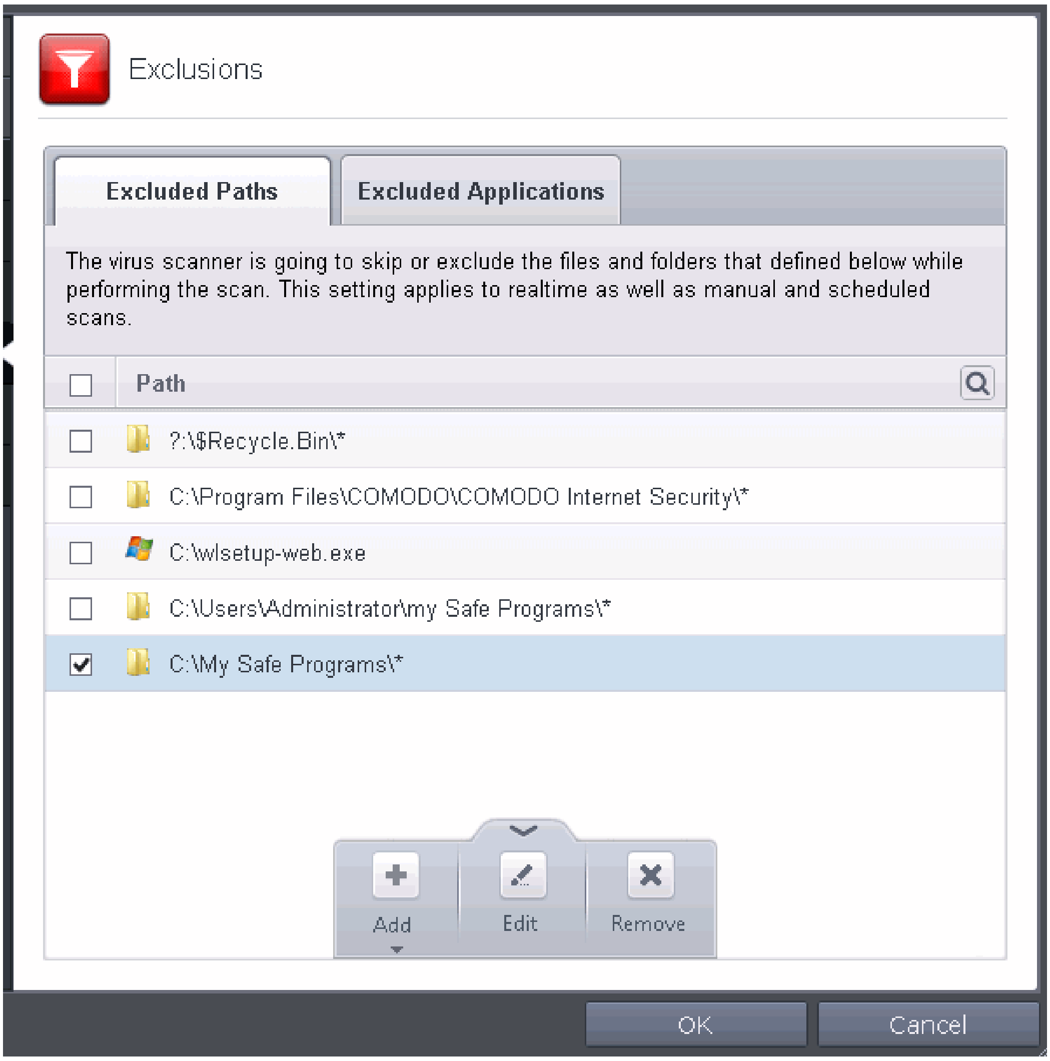


The 'Browse for Folder' dialog will appear.



- Navigate to the drive partition or folder you want to add to excluded paths and click OK

The drive partition/folder will be added to Excluded Paths.



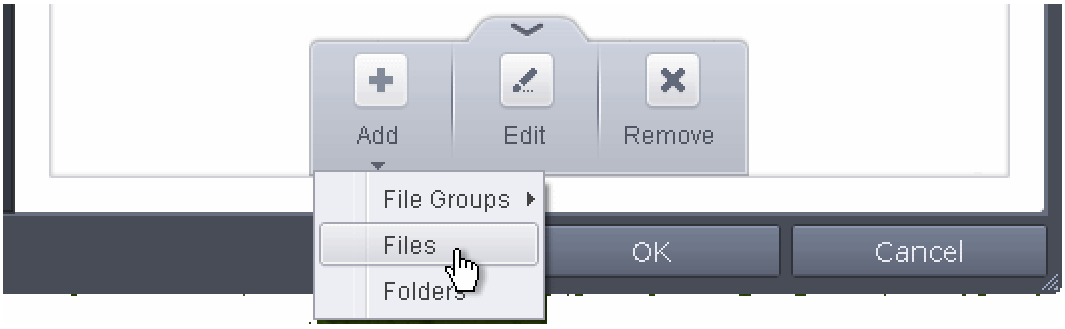
The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	C:\wlsetup-web.exe
□	C:\Users\Administrator\my Safe Programs*
☑	C:\My Safe Programs*

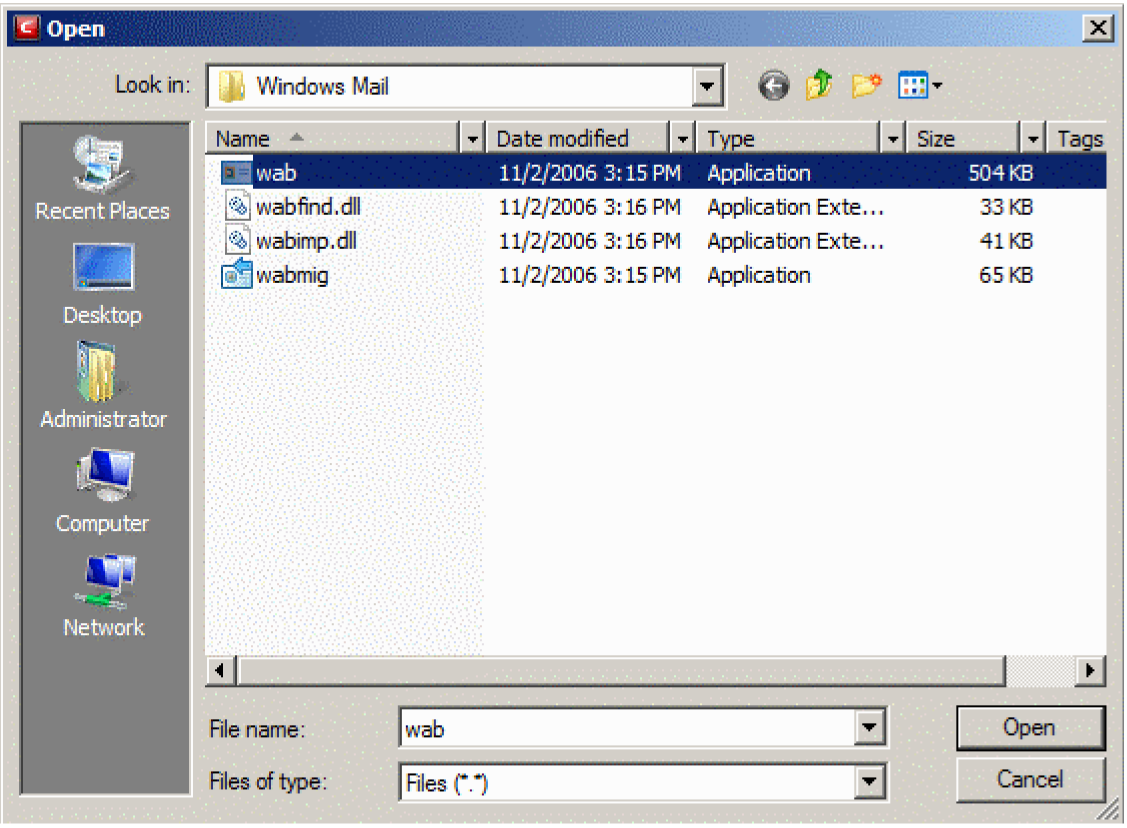
- Repeat process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding an individual File

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



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

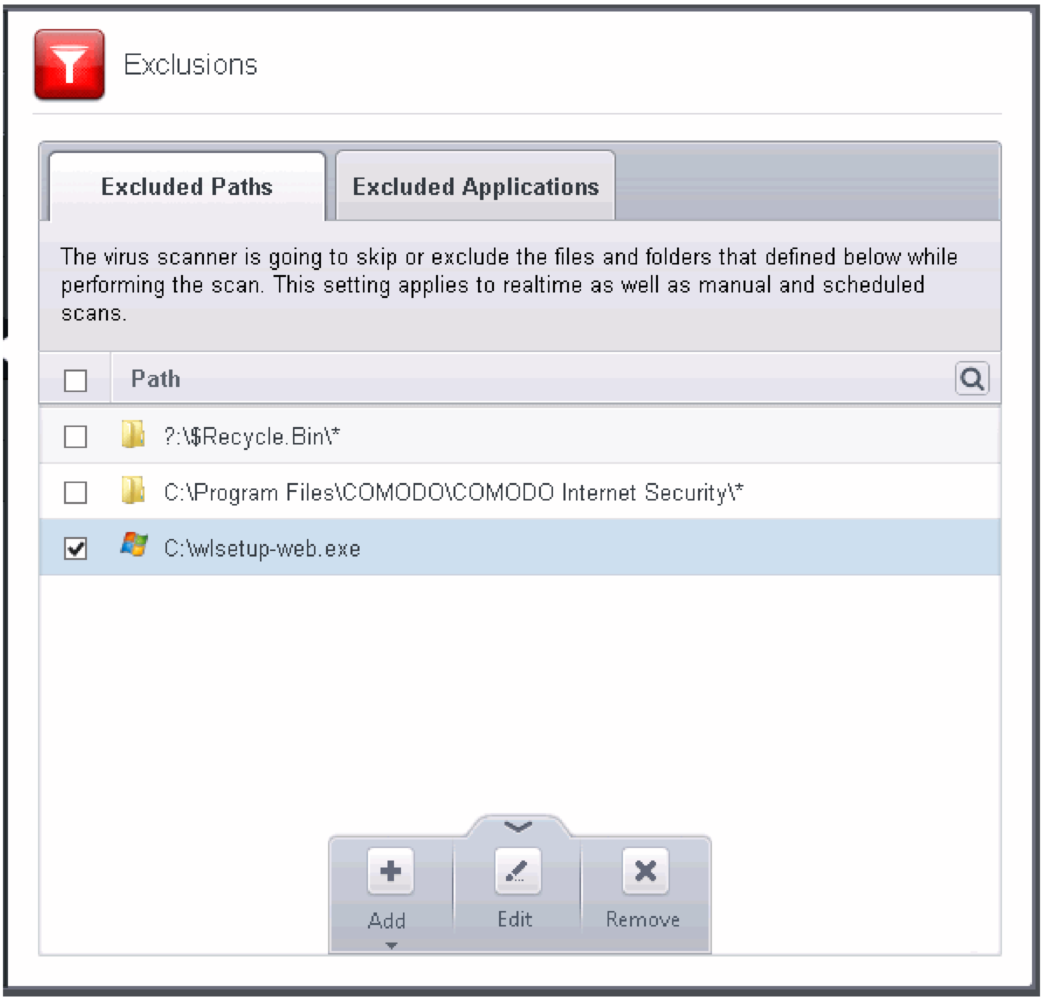


Name	Date modified	Type	Size	Tags
wab	11/2/2006 3:15 PM	Application	504 KB	
wabfind.dll	11/2/2006 3:16 PM	Application Exte...	33 KB	
wabimp.dll	11/2/2006 3:16 PM	Application Exte...	41 KB	
wabmig	11/2/2006 3:15 PM	Application	65 KB	

File name: wab

Files of type: Files (*.*)

The file will be added to Excluded Paths.



Exclusions

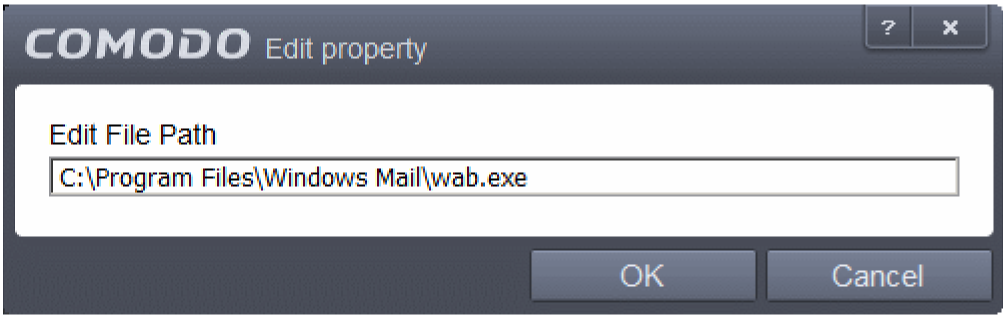
The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
☑	C:\wlsetup-web.exe

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

To edit the path of an added item

- Select the item, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.

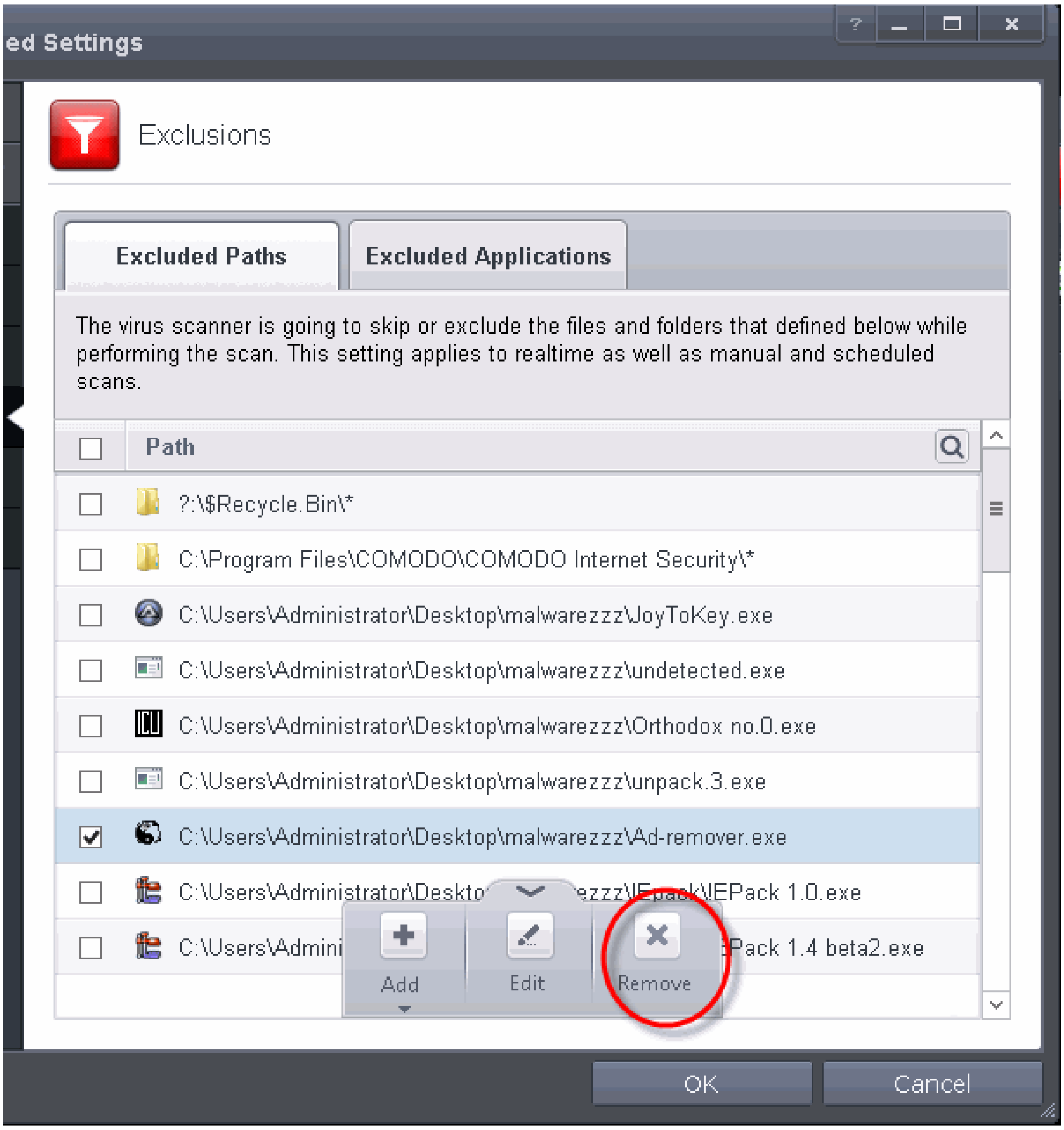


Edit File Path

C:\Program Files\Windows Mail\wab.exe

To remove an item from the Excluded Paths

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



ed Settings

Exclusions

The virus scanner is going to skip or exclude the files and folders that defined below while performing the scan. This setting applies to realtime as well as manual and scheduled scans.

□	Path
□	?:\$Recycle.Bin*
□	C:\Program Files\COMODO\COMODO Internet Security*
□	C:\Users\Administrator\Desktop\malwarezzz\JoyToKey.exe
□	C:\Users\Administrator\Desktop\malwarezzz\undetected.exe
□	C:\Users\Administrator\Desktop\malwarezzz\Orthodox no.0.exe
□	C:\Users\Administrator\Desktop\malwarezzz\unpack.3.exe
☑	C:\Users\Administrator\Desktop\malwarezzz\Ad-remover.exe
□	C:\Users\Administrator\Deskto ezzz\IEpack\IEPack 1.0.exe
□	C:\Users\Admini Pack 1.4 beta2.exe

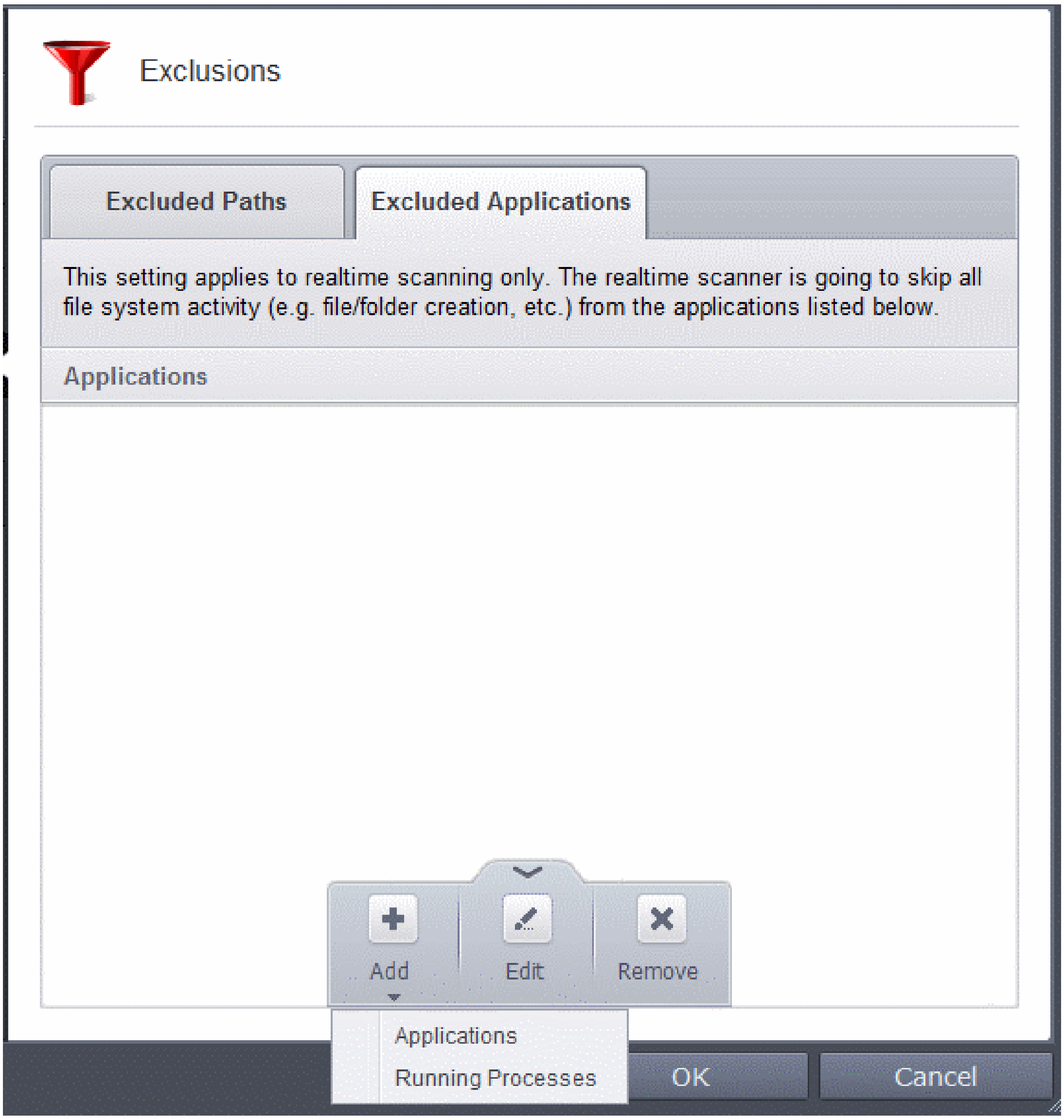
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

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

To add an item to Excluded Applications

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



Exclusions

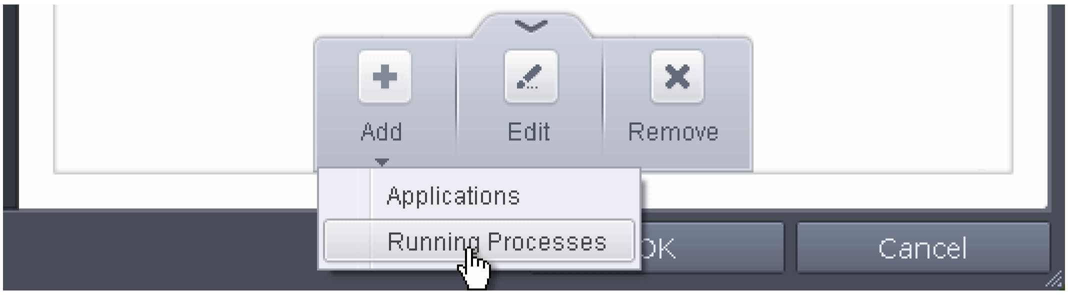
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

You can choose to add an application by:

- **Selecting it from the running processes** - This option allows you to choose the target application from the list of processes that are currently running on your server.
- **Browsing your server for the application** - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.

Adding an application from a running processes

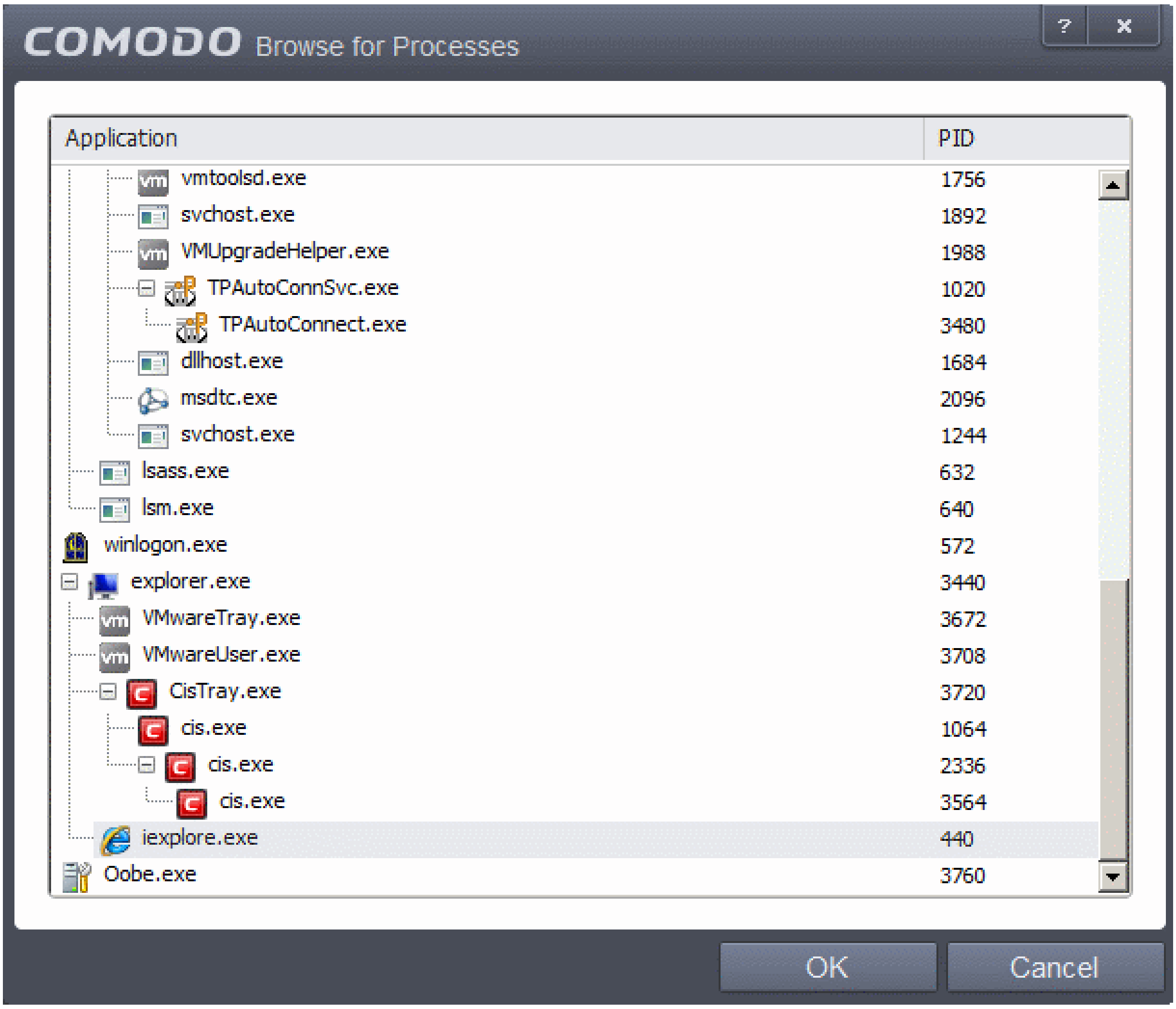
- Choose 'Running Processes' from the 'Add' drop-down



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

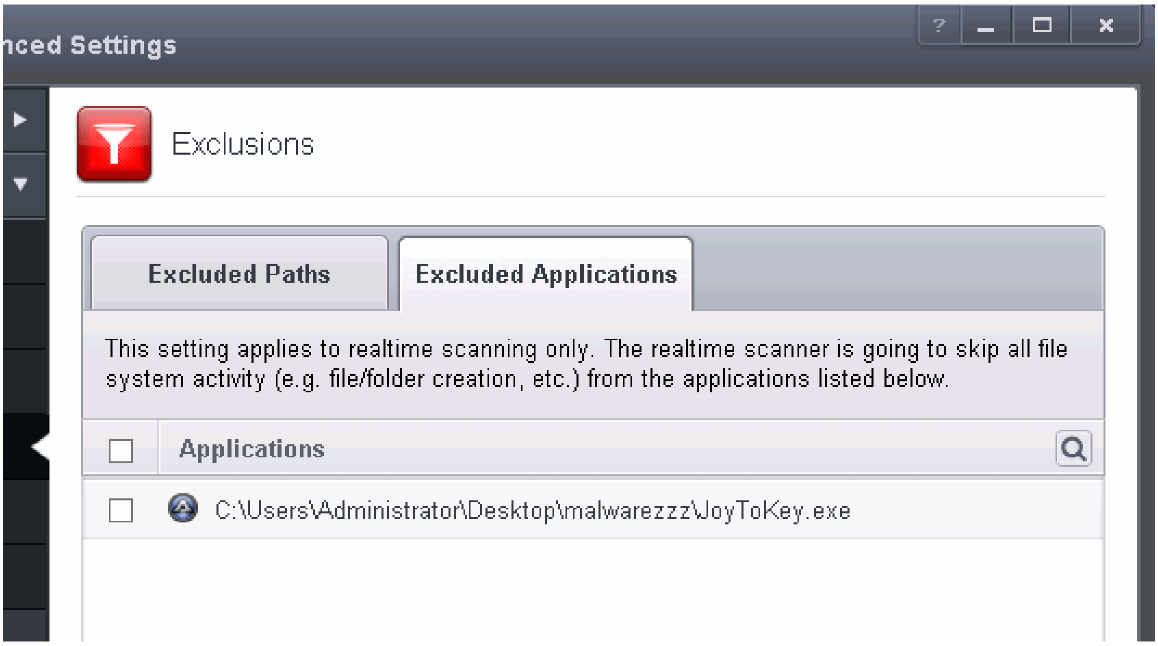
- Select the process, whose target application is to be added to excluded applications and click OK from the

Browse for Process dialog.



Application	PID
vmtoolsd.exe	1756
svchost.exe	1892
VMUpgradeHelper.exe	1988
TPAutoConnSvc.exe	1020
TPAutoConnect.exe	3480
dllhost.exe	1684
msdtc.exe	2096
svchost.exe	1244
lsass.exe	632
lsm.exe	640
winlogon.exe	572
explorer.exe	3440
VMwareTray.exe	3672
VMwareUser.exe	3708
CisTray.exe	3720
cis.exe	1064
cis.exe	2336
cis.exe	3564
iexplore.exe	440
Oobe.exe	3760

The application will be added to Excluded Applications.



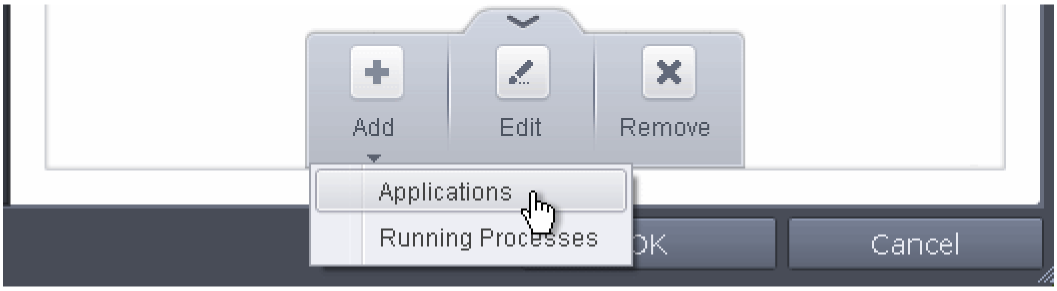
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

□ Applications

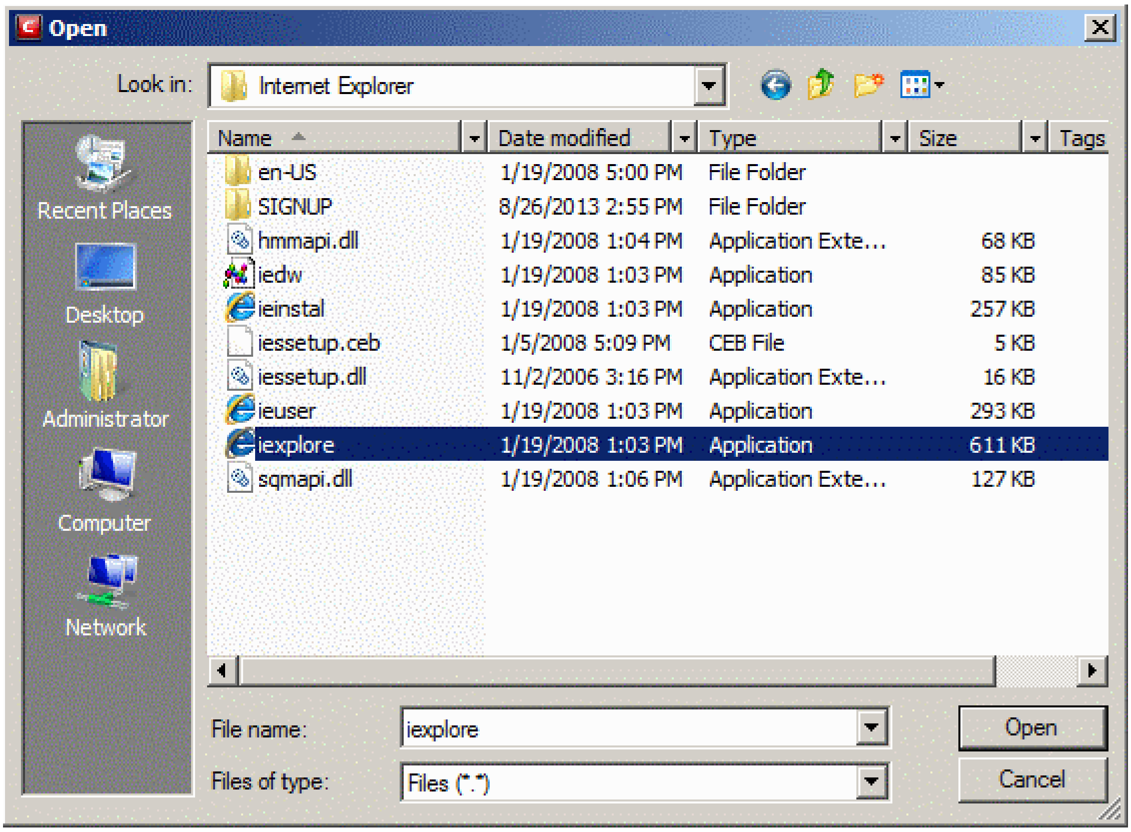
□ C:\Users\Administrator\Desktop\malwarezzz\JoyToKey.exe

Browsing to the Application

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



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



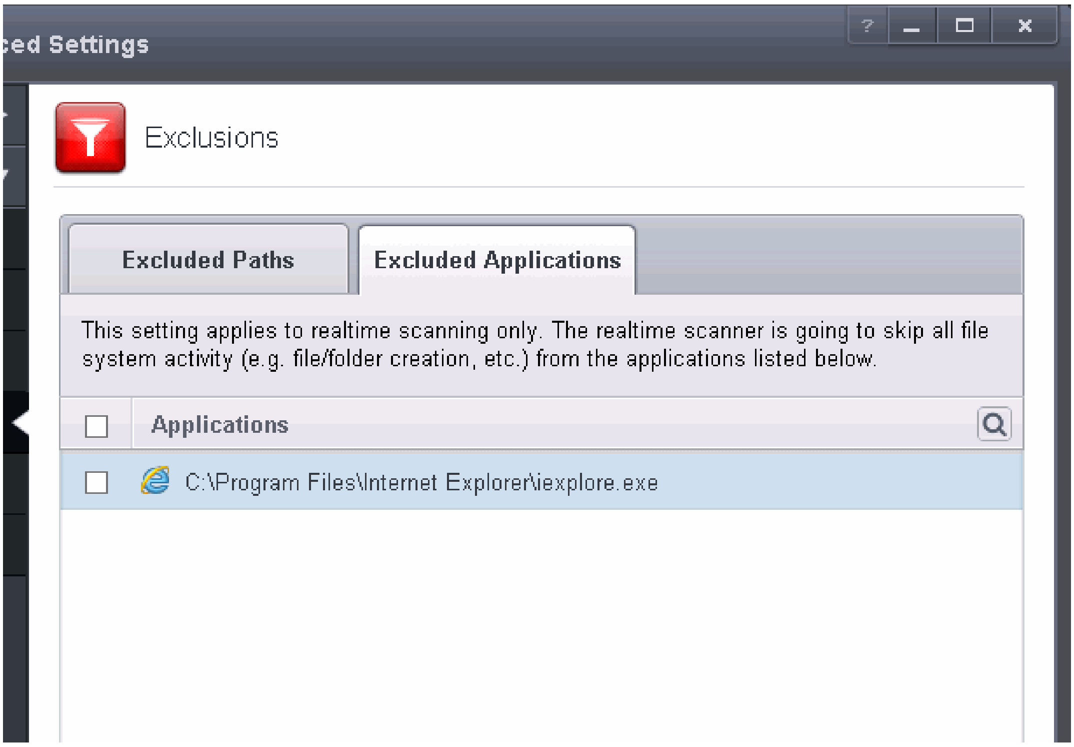
Look in: Internet Explorer

Name	Date modified	Type	Size	Tags
en-US	1/19/2008 5:00 PM	File Folder		
SIGNUP	8/26/2013 2:55 PM	File Folder		
hmmapi.dll	1/19/2008 1:04 PM	Application Exte...	68 KB	
iedw	1/19/2008 1:03 PM	Application	85 KB	
ieinstal	1/19/2008 1:03 PM	Application	257 KB	
iessetup.ceb	1/5/2008 5:09 PM	CEB File	5 KB	
iessetup.dll	11/2/2006 3:16 PM	Application Exte...	16 KB	
ieuser	1/19/2008 1:03 PM	Application	293 KB	
iexplore	1/19/2008 1:03 PM	Application	611 KB	
sqmapi.dll	1/19/2008 1:06 PM	Application Exte...	127 KB	

File name: iexplore

Files of type: Files (*.*)

The file will be added to 'Excluded Applications'.



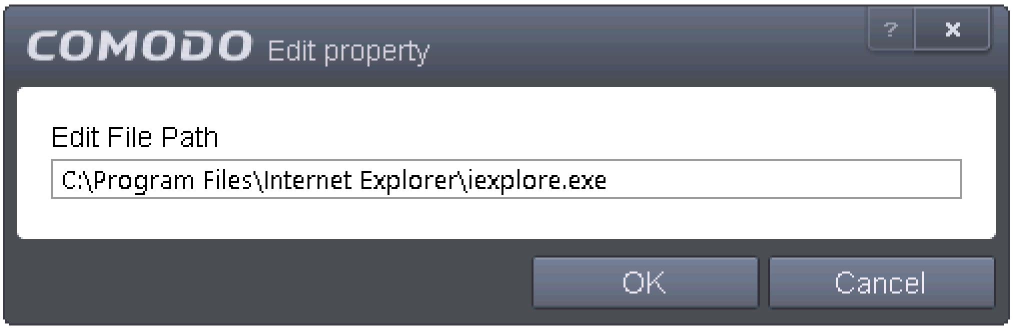
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

□	Applications
□	C:\Program Files\Internet Explorer\iexplore.exe

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

To edit the path of the application added to Excluded Application

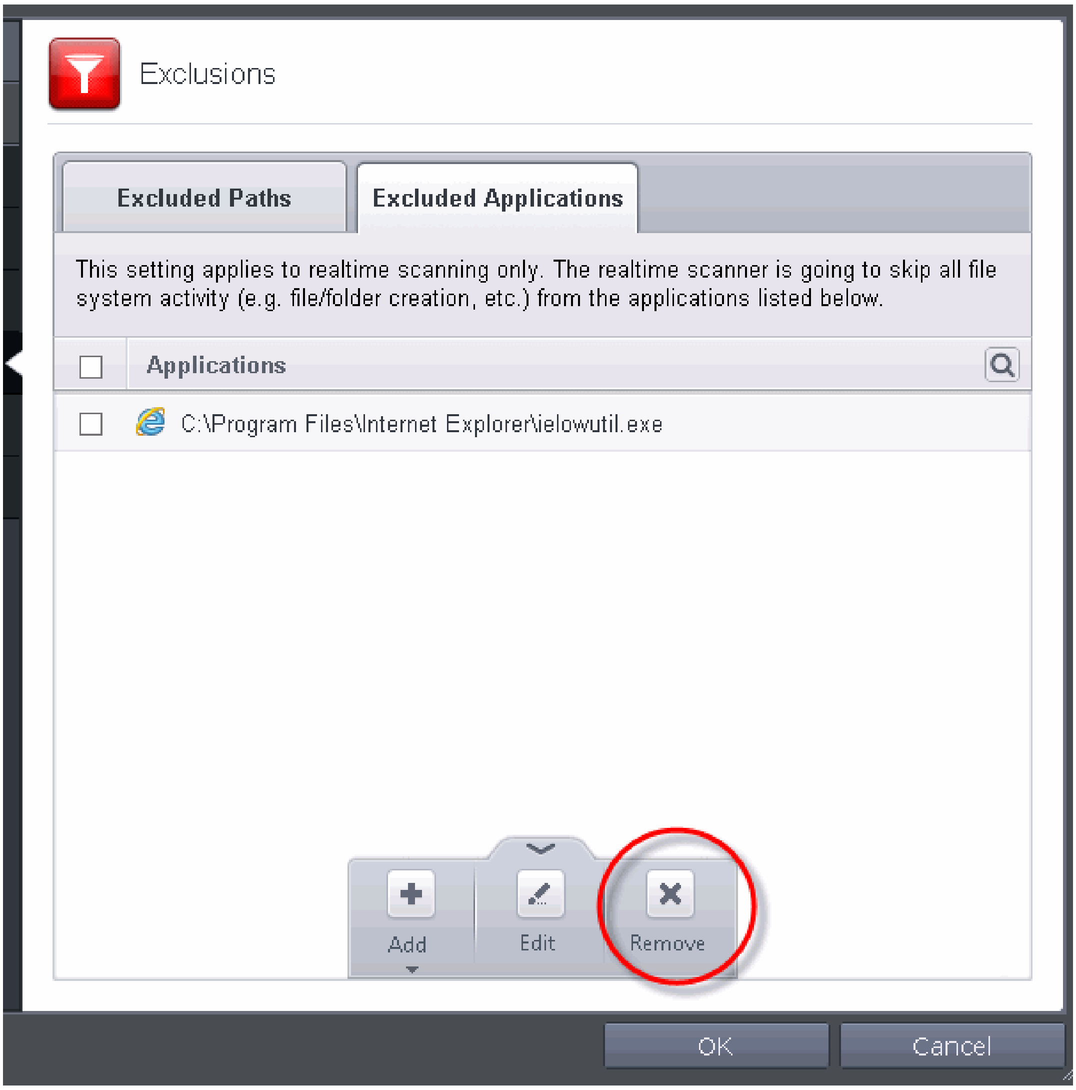
- Select the application, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



Edit File Path: C:\Program Files\Internet Explorer\iexplore.exe

To remove an item from the Excluded Applications

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



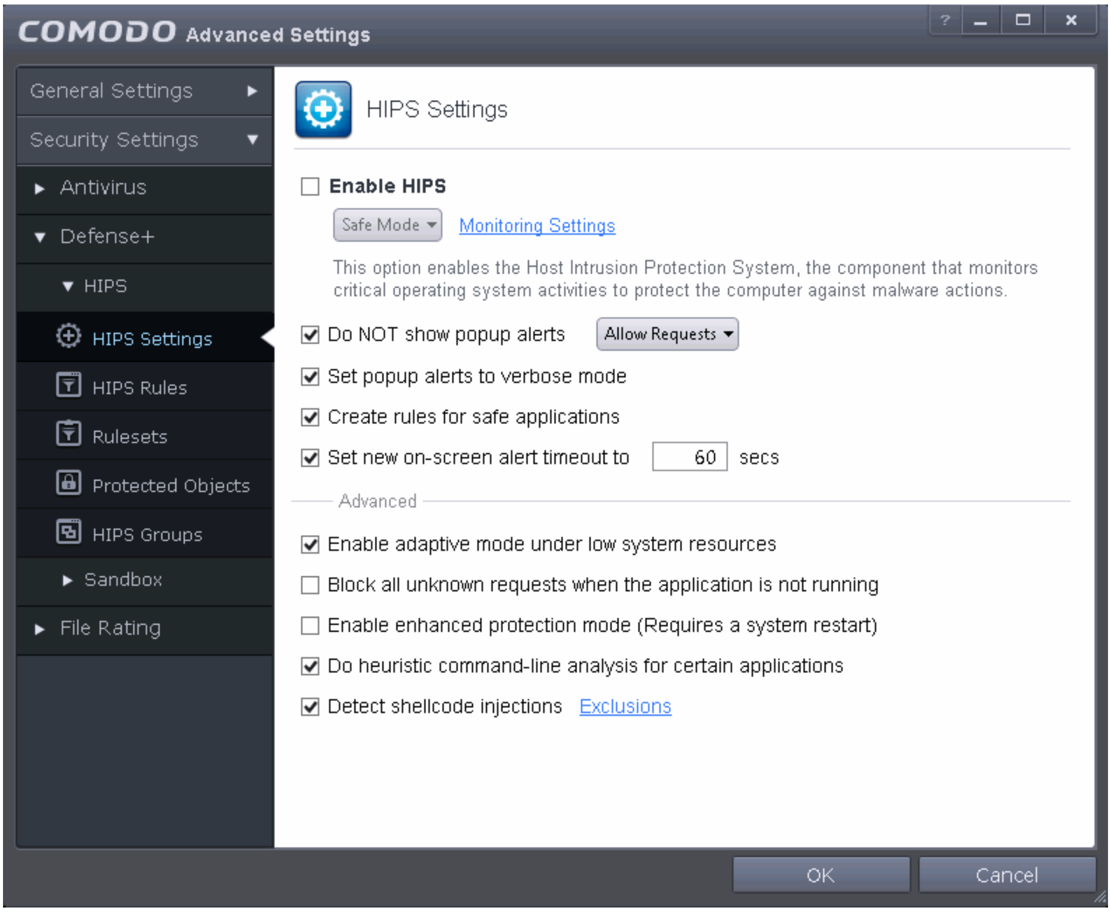
This setting applies to realtime scanning only. The realtime scanner is going to skip all file system activity (e.g. file/folder creation, etc.) from the applications listed below.

□	Applications
□	C:\Program Files\Internet Explorer\ielowutil.exe

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

5.2.2. Defense+ Settings

Defense+ is a Host Intrusion Prevention (HIPS) technology that ensure all applications, processes and services on your server behave in a secure manner - and are prevented from taking actions that could damage your server or your data.



□ **Enable HIPS**

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do NOT show popup alerts Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

☑ Enable adaptive mode under low system resources

□ Block all unknown requests when the application is not running

□ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Detect shellcode injections Exclusions

The Defense+ settings area allows you to configure the following:

- HIPS
  - **HIPS Behaviour Settings**
  - **Active HIPS Rules**
  - **Predefined HIPS Rule Sets**
  - **Protected Objects**
  - **HIPS Groups**
  - **Sandbox**

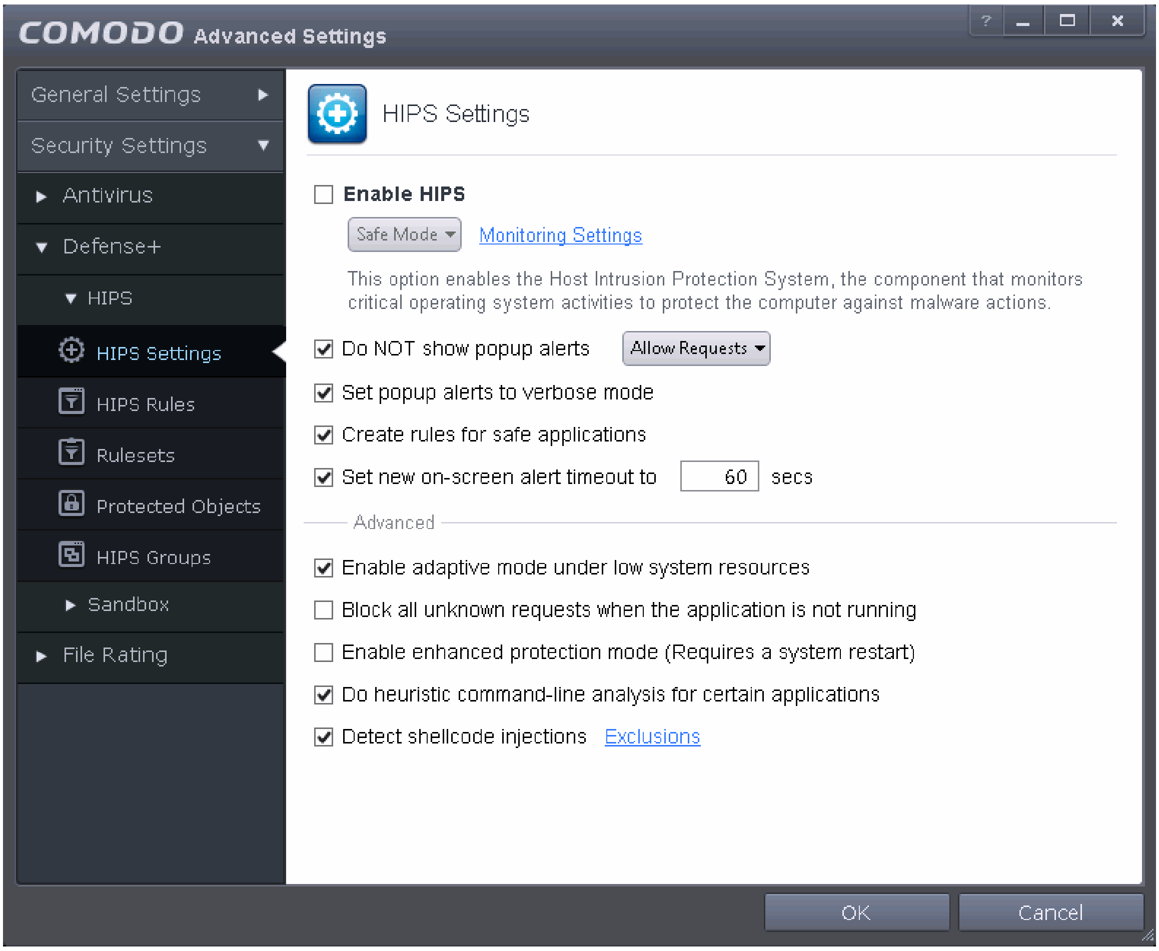
5.2.2.1. HIPS Behavior Settings

HIPS constantly monitors server activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. CAVS ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs. Administrators looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

Note: This page often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your server to perform a task or function. Every program, application and device you run on your server 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 server 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 server to delete valuable data; steal your identity; corrupt server files; give control of your server to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms.

- The HIPS Settings panel allows you to enable/disable HIPS, set its security level and configure its general behavior.
- The HIPS Settings panel can be accessed by clicking Security Settings > Defense+ > HIPS > 'HIPS Settings' tab from 'Advanced Settings' interface



HIPS Settings

□ **Enable HIPS**

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do NOT show popup alerts Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

Advanced

☑ Enable adaptive mode under low system resources

□ Block all unknown requests when the application is not running

□ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Detect shellcode injections Exclusions

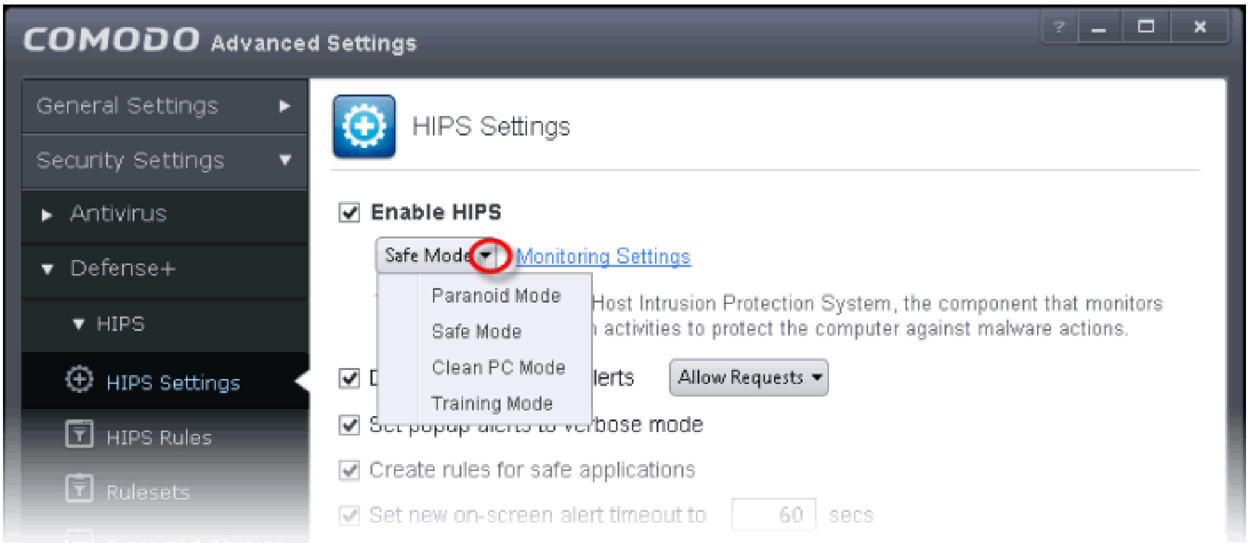
- **Enable HIPS -** Allows you to enable/disable the HIPS protection.***(Default=Disabled)***

Note: The HIPS settings can also be configured in the 'Advanced View' of the 'Home' screen by clicking the status link beside HIPS in the 'Defense+ ' pane.

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

Configuring Security Level of HIPS

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



☑ Enable HIPS

Host Intrusion Protection System, the component that monitors … activities to protect the computer against malware actions.

☑ D… …lerts Allow Requests

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

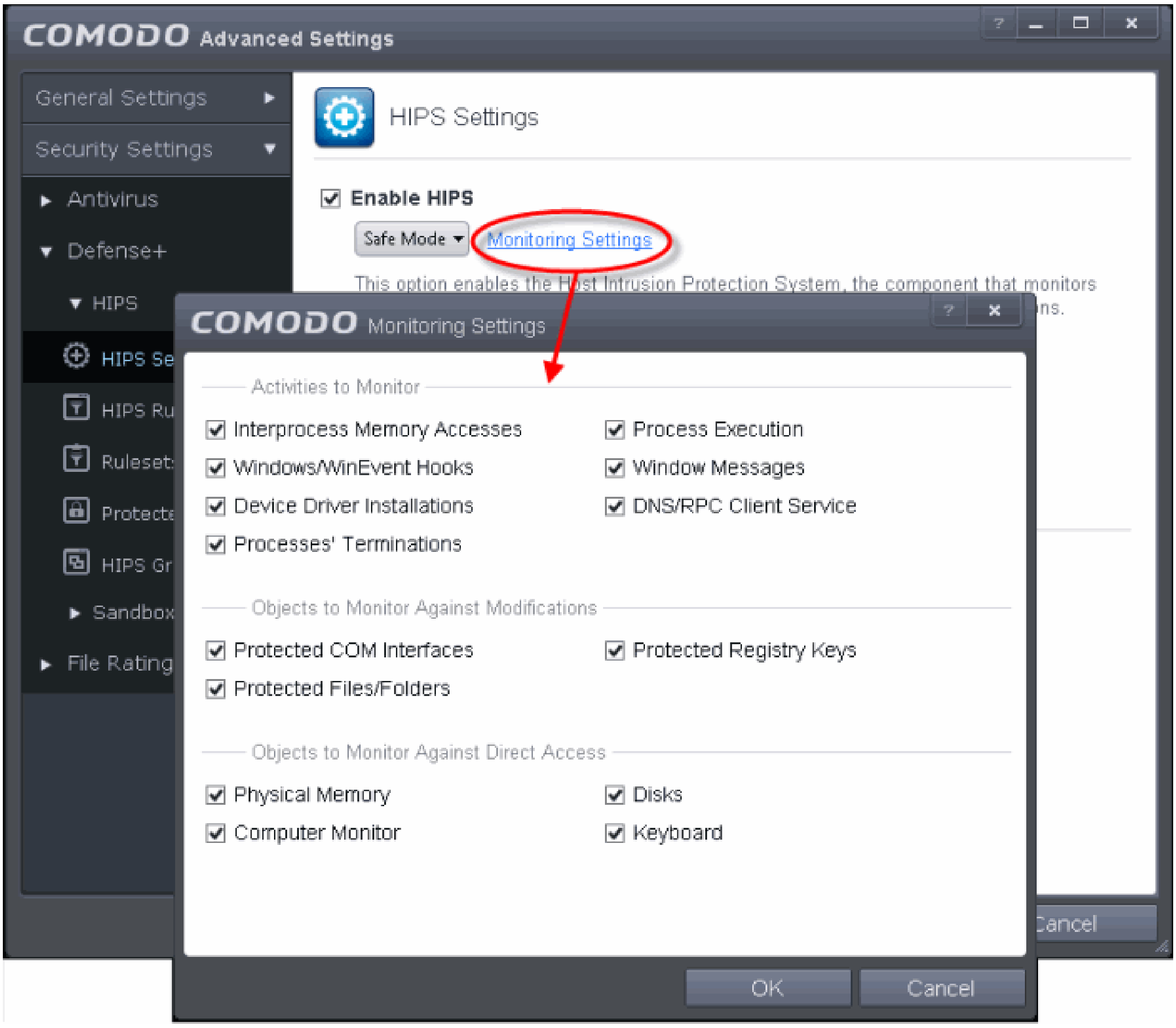
The choices available are:

- **Paranoid Mode**: This is the highest security level setting and means that Defense+ monitors and controls all executable files apart from those that you have deemed safe. CAVS 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, CAVS does automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their server.
- **Safe Mode**: While monitoring critical server activity, Defense+ automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules these activities, if the checkbox '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs the Defense+ not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Clean PC Mode:** From the time you set the slider to 'Clean PC Mode', Defense+ learns the activities of the applications currently installed on the server while all new executables introduced to the server are monitored and controlled. This patent-pending mode of operation is the recommended option on a new server or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files with 'Unrecognized' rating in the '**File List**' are excluded from being considered as clean and are monitored and controlled.
- **Training Mode**: Defense+ monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your server are safe to run.

Configuring the Monitoring Settings

The activities, entities and objects that should monitored by HIPS can be configured by clicking the Monitoring Settings link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a ***global*** basis - effectively creating a universal '**Allow**' rule for that activity . This 'Allow' setting ***over-rules*** any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the '**Access Rights**' and '**Protection Settings**' interface.



☑ Enable HIPS

Activities to Monitor

☑ Interprocess Memory Accesses
☑ Windows/WinEvent Hooks
☑ Device Driver Installations
☑ Processes' Terminations
☑ Process Execution
☑ Window Messages
☑ DNS/RPC Client Service

Objects to Monitor Against Modifications

☑ Protected COM Interfaces
☑ Protected Files/Folders
☑ Protected Registry Keys

Objects to Monitor Against Direct Access

☑ Physical Memory
☑ Computer Monitor
☑ Disks
☑ Keyboard

Activities To Monitor:

- **Interprocess Memory Access -** Malware programs use memory space modification to inject malicious code for numerous types of attacks, including recording your keyboard strokes; modifying the behavior of the invaded application; stealing confidential data by sending confidential information from one process to another process etc. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of the invaded process, or 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application ***(Default = Enabled)***.
- **Windows/WinEvent Hooks -** In the Windows Server, 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 server; take over control of your mouse and keyboard to remotely administer your server. 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 server. 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 server instability if it conflicts with other drivers on your server. The installation of a malicious driver could, obviously, cause irreparable damage to your server or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application ***(Default = Enabled)***.
- **Processes' Terminations -** A process is a running instance of a program. (for example, the CAVS process is called 'cis.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your server). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, Defense+ monitors and alerts you to all attempts by an untrusted application to close down another application ***(Default = Enabled)***.
- **Process Execution** - Typical malware like rootkits, keylogger etc. would often invoke by itself and runs its process mostly at the background. These processes, invisible at the foreground will act as agents for infecting your server and to steal your confidential and sensitive information like your credit card details and passwords and pass to hackers. With this setting enabled, the HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. ***(Default = Enabled)***.
- **Windows Messages -** This setting means CAVS monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) ***(Default = Enabled)***.
- **DNS/RPC Client Service -** This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby a malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' pc's which are sending out these requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack ***(Default = Enabled)***.

Background Note: DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever you type a domain name, your Internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to your server, telling it to connect to the IP in question.

Objects To Monitor Against Modifications:

- **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the **COM Protection** pane. ***(Default = Enabled)***
- **Protected Registry Keys** enables monitoring of Registry keys you specified from the **Registry Protection** pane. ***(Default = Enabled)***.
- **Protected Files/Folders** enables monitoring of files and folders you specified from the **File Protection** pane. ***(Default = Enabled)***.

Objects To Monitor Against Direct Access:

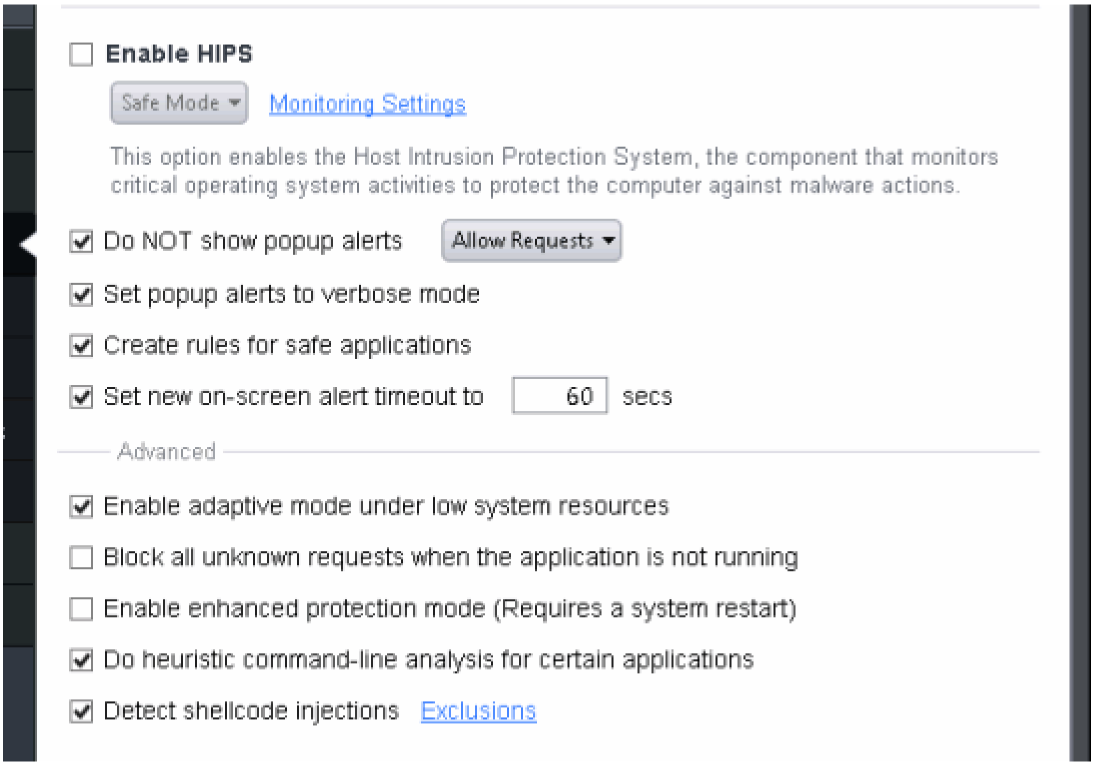
Determines whether or not CAVS should monitor access to system critical objects on your server. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:

- **Physical Memory:** Monitors your server'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 server to execute its code ***(Default = Enabled)***.
- **Computer Monitor:** CAVS raises an alert every time a process tries to directly access your server 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, CAVS alerts you every time an application attempts to establish direct access to your keyboard ***(Default = Enabled)***.

Checkbox Options

- **Do NOT show popup alerts** - Configure whether or not you want to be notified when the HIPS encounters a malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness. (***Default = Enabled***)

  If you choose not to show alerts then you have a choice of default responses that CAVS should automatically take - either 'Block Requests' or 'Allow Requests'.



□ **Enable HIPS**

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☑ Do NOT show popup alerts Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

Advanced

☑ Enable adaptive mode under low system resources

□ Block all unknown requests when the application is not running

□ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

☑ Detect shellcode injections Exclusions

- **Set popup alerts to verbose mode -** Enabling this option instructs CAVS to display HIPS Alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests
- **Create rules for safe applications -** Automatically creates rules for safe applications in HIPS Ruleset ***(Default = Disabled).***

Note: HIPS trusts the applications if:

- The application/file is rated as 'Trusted' in the **File List**
- The application is from a vendor included in the **Trusted Software Vendors** list
- The application is included in the extensive and constantly updated Comodo safelist.

By default, CAVS 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 CAVS to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the **HIPS Rules** interface. The Advanced users can edit / modify the rules as they wish.

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

Advanced HIPS Settings

- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CAVS functions to fail. With this option enabled, CAVS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, the cost of enabling this option may be reduced performance in even lightly loaded systems ***(Default = Disabled)***.
- **Block all unknown requests if the application is closed -** Selecting this option blocks all unknown execution requests if CAVS is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CAVS security settings then it is OK to leave this box unchecked. ***(Default = Disabled).***
- **Enable enhanced protection mode** - On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. CAVS requires a system restart for enabling enhanced protection mode. (***Default = Disabled***)
- **Do heuristic command-line analysis for certain applications** - Selecting this option instructs Comodo Endpoint Security to perform heuristic analysis of programs that are capable of executing code such as visual basic scripts and java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscipt.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CAVS detects c:teststest.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'.
- **Detect shellcode injections (i.e. Buffer overflow protection) -** Enabling this setting turns-on the Buffer over flow protection.

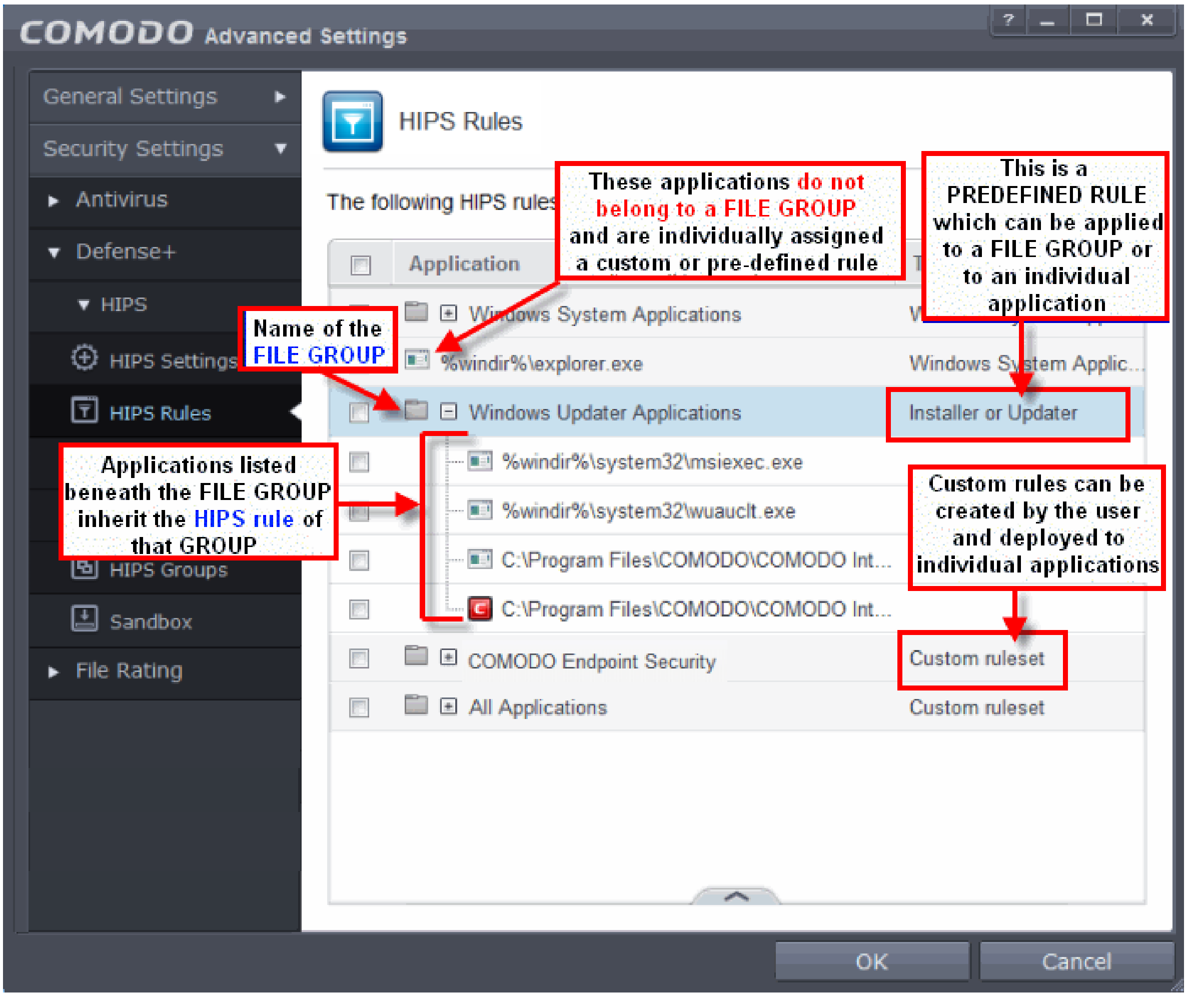
  Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

  Turning-on buffer overflow protection instructs the Comodo Antivirus for Servers to raise pop-up alerts in every event of a possible buffer overflow attack. You can allow or deny the requested activity raised by the process under execution depending on the reliability of the software and its vendor.

  Comodo recommends that this setting to be maintained selected always ***(Default = Enabled).***

5.2.2.2. Active HIPS Rules

The HIPS rules tab lists the different groups of applications installed in your server and the Rulesets applied to them. You can change the ruleset applied to selected applications and also create custom rulesets to be applied to selected applications.



The following HIPS rules

Application	T
Windows System Applications	W
%windir%\explorer.exe	Windows System Applic...
Windows Updater Applications	Installer or Updater
%windir%\system32\msiexec.exe	
%windir%\system32\wuauclt.exe	
C:\Program Files\COMODO\COMODO Int...	
C:\Program Files\COMODO\COMODO Int...	
COMODO Endpoint Security	Custom ruleset
All Applications	Custom ruleset

These applications do not belong to a FILE GROUP and are individually assigned a custom or pre-defined rule

This is a PREDEFINED RULE which can be applied to a FILE GROUP or to an individual application

Name of the FILE GROUP

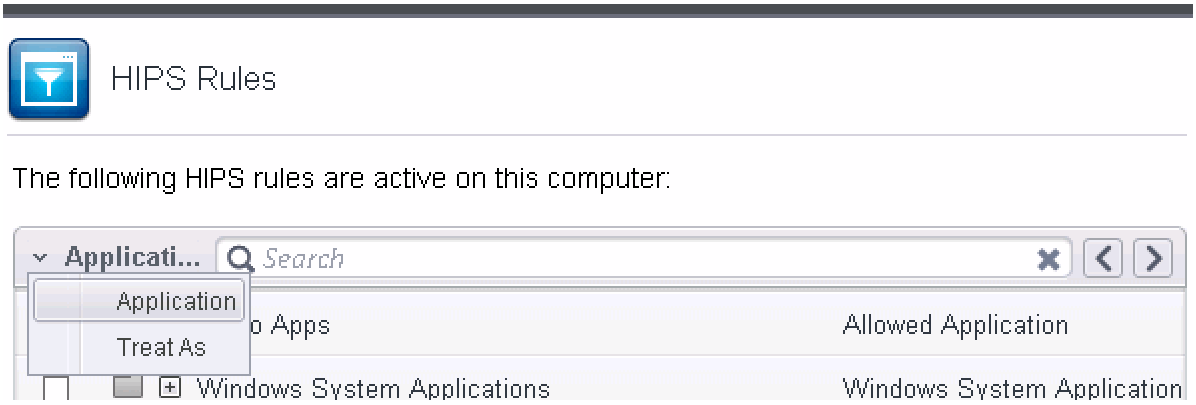
Applications listed beneath the FILE GROUP inherit the HIPS rule of that GROUP

Custom rules can be created by the user and deployed to individual applications

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

You can use the search option to find a specific file or a company in the list.

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



The following HIPS rules are active on this computer:

...o Apps	Allowed Application
☐ ⊞ Windows System Applications	Windows System Application

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

General Navigation:

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

- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See the section '**Creating or Modifying a HIPS Ruleset**'.
- **Remove** - Deletes the selected ruleset.

Note: You cannot remove individual applications from a file group using this interface - you must use the '**File Groups**' interface to do this.

- **Purge** - Runs a server check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

Users can re-order the priority of rules by simply selecting the application name or file group name in question, clicking the handle at the bottom center and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the **'File Groups'** interface.

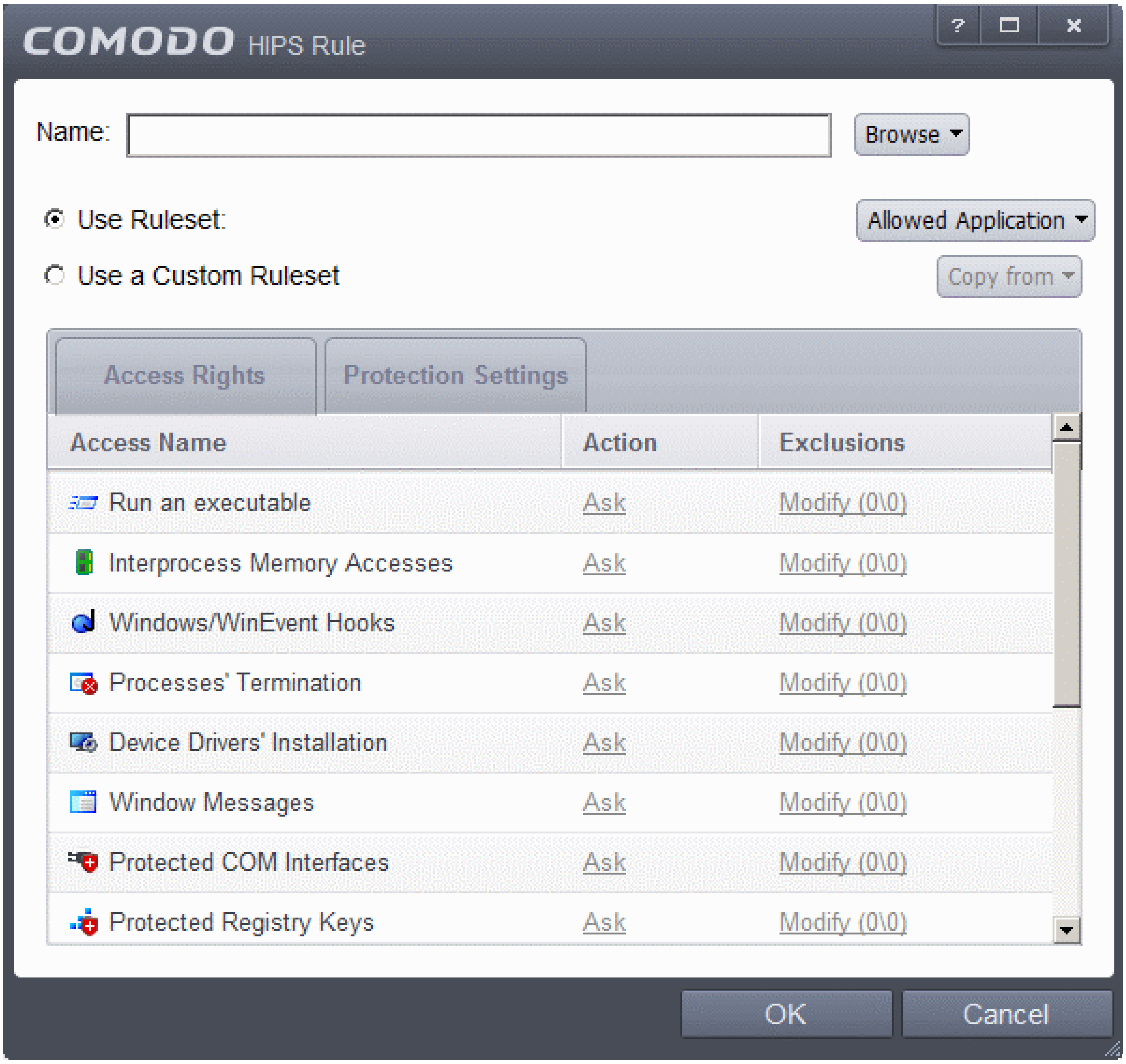
Creating or Modifying a HIPS Ruleset

To begin defining an application's HIPS Ruleset

1. **Select the application or file group that you wish the ruleset to apply to.**
2. **Configure the ruleset for this application.**

Step 1 - Select the application or file group that you wish the ruleset to apply to

If you wish to define a rule for a new application (i.e. one that is not already listed), click the handle from the **HIPS Rules pane** and select 'Add'. This brings up the 'HIPS Rule' interface as shown below.



Name:

● Use Ruleset: Allowed Application

○ Use a Custom Ruleset

Copy from

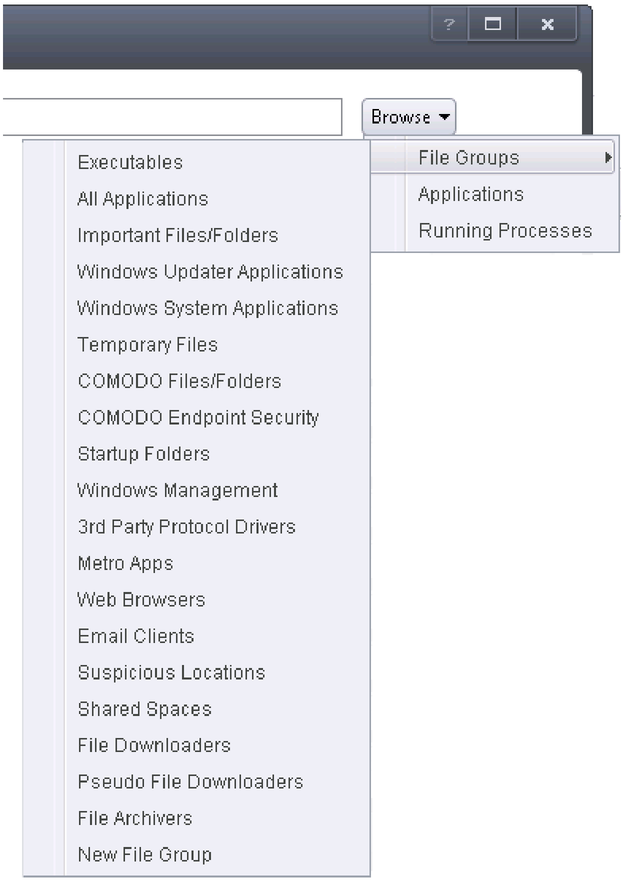
Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (0\0)

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

- Click 'Browse' to begin.

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

1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

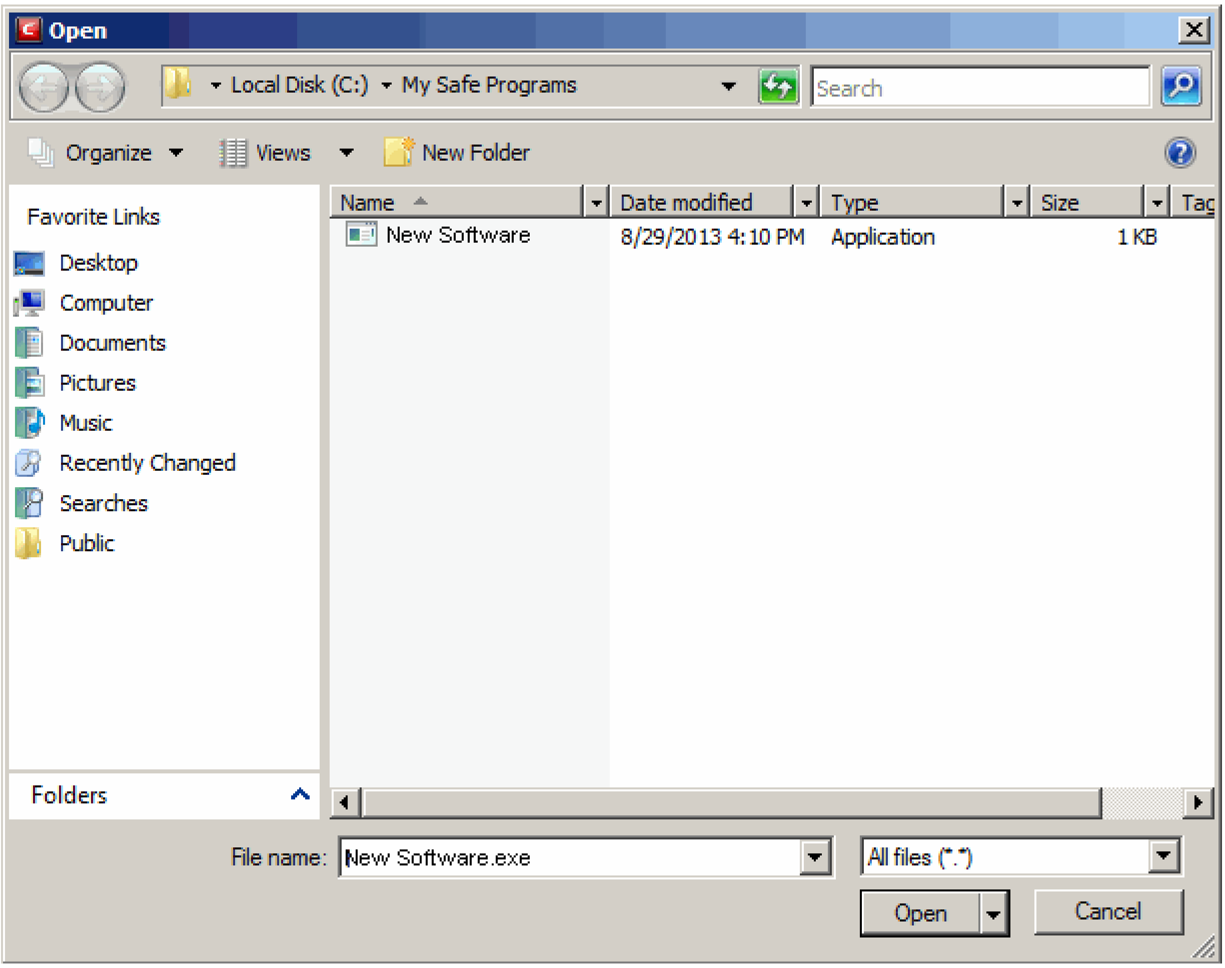


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

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

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

2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.

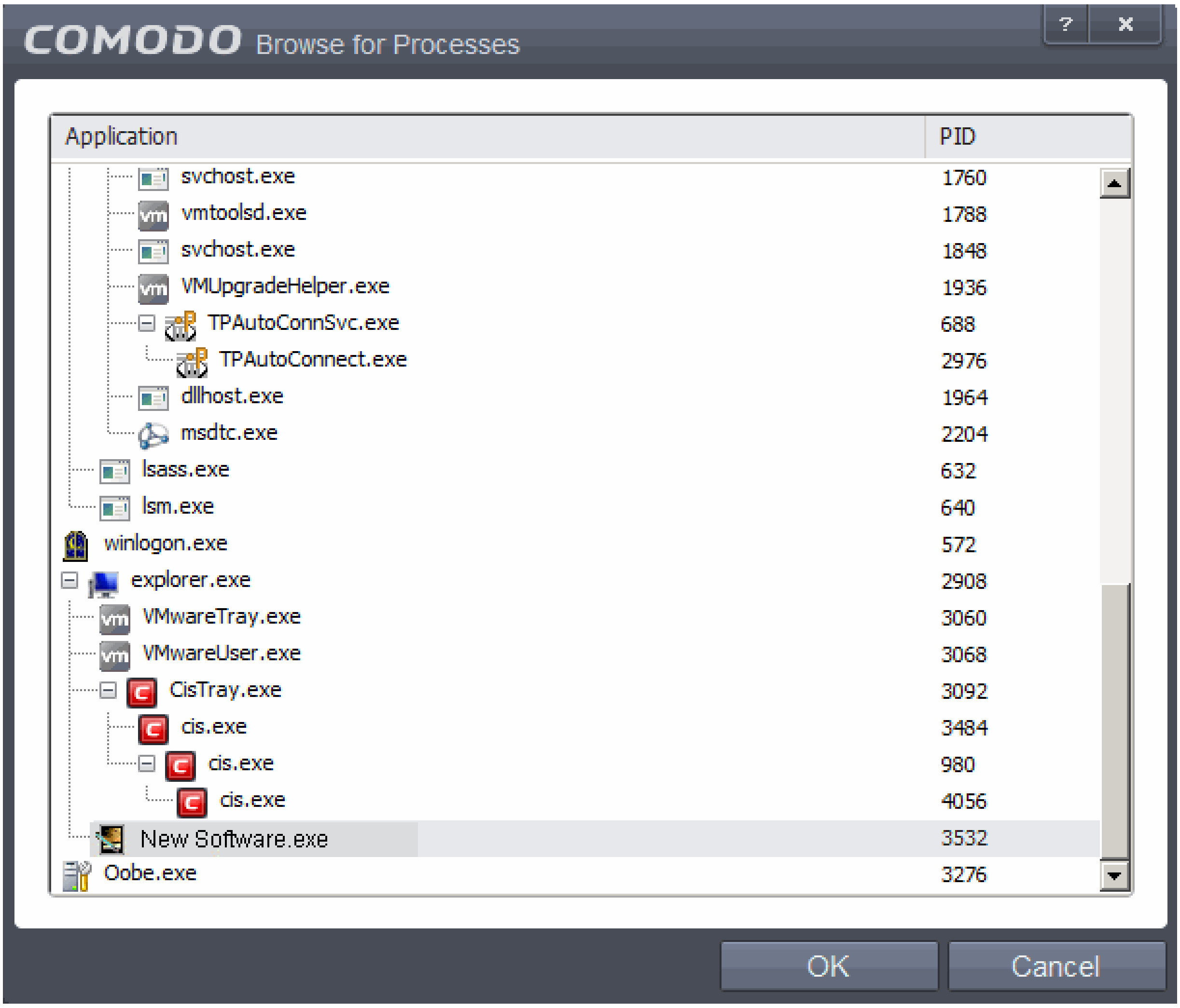


Name	Date modified	Type	Size
New Software	8/29/2013 4:10 PM	Application	1 KB

File name: New Software.exe

All files (*.*)

3. **Running Processes -** as the name suggests, this option allows you to create and deploy a ruleset for any process that is currently running on your server.



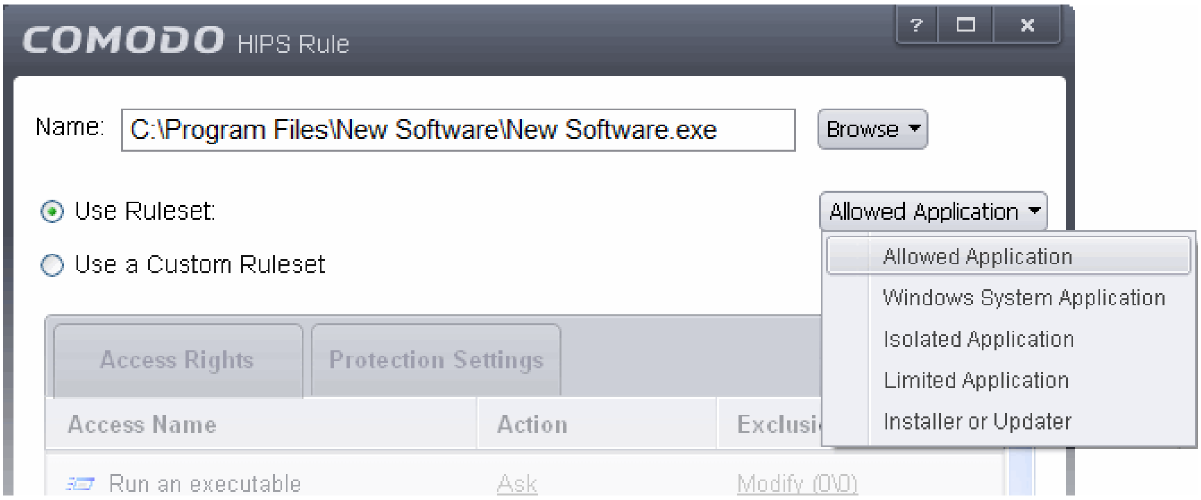
Application	PID
svchost.exe	1760
vmtoolsd.exe	1788
svchost.exe	1848
VMUpgradeHelper.exe	1936
TPAutoConnSvc.exe	688
TPAutoConnect.exe	2976
dllhost.exe	1964
msdtc.exe	2204
lsass.exe	632
lsm.exe	640
winlogon.exe	572
explorer.exe	2908
VMwareTray.exe	3060
VMwareUser.exe	3068
CisTray.exe	3092
cis.exe	3484
cis.exe	980
cis.exe	4056
New Software.exe	3532
Oobe.exe	3276

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

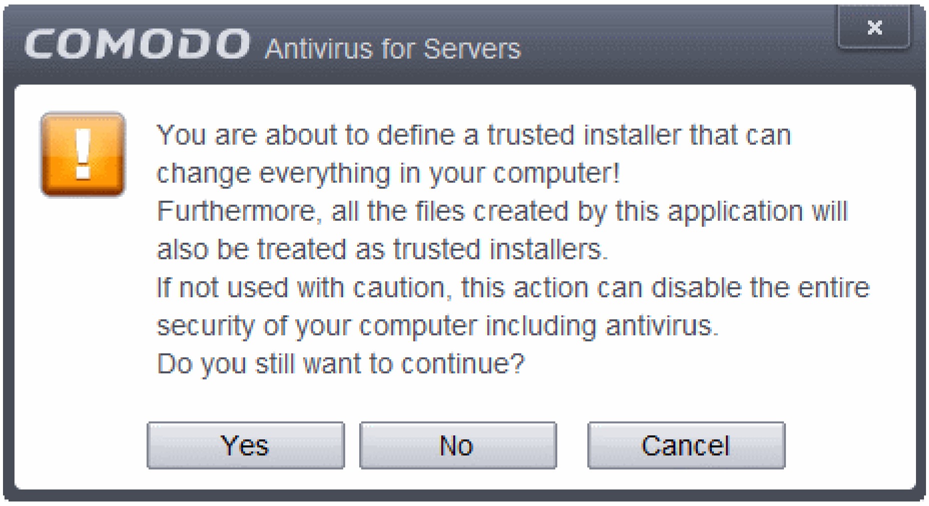
Step 2 - Configure the HIPS Ruleset for this application

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

1. **Use Ruleset -** Selecting this option allows the user to quickly deploy an existing HIPS ruleset on to the target application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the **HIPS Rules** interface ***(Default = Enabled).***



Note on 'Installer or Updater' Rule : Applying the Predefined Ruleset 'Installer or Updater' for an application defines it as a trusted installer and all files created by the application will also be considered as trusted files. Some applications may have hidden code that could impair the security of your server if allowed to create files of their own. Comodo advises you to use this Predefined Ruleset - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.



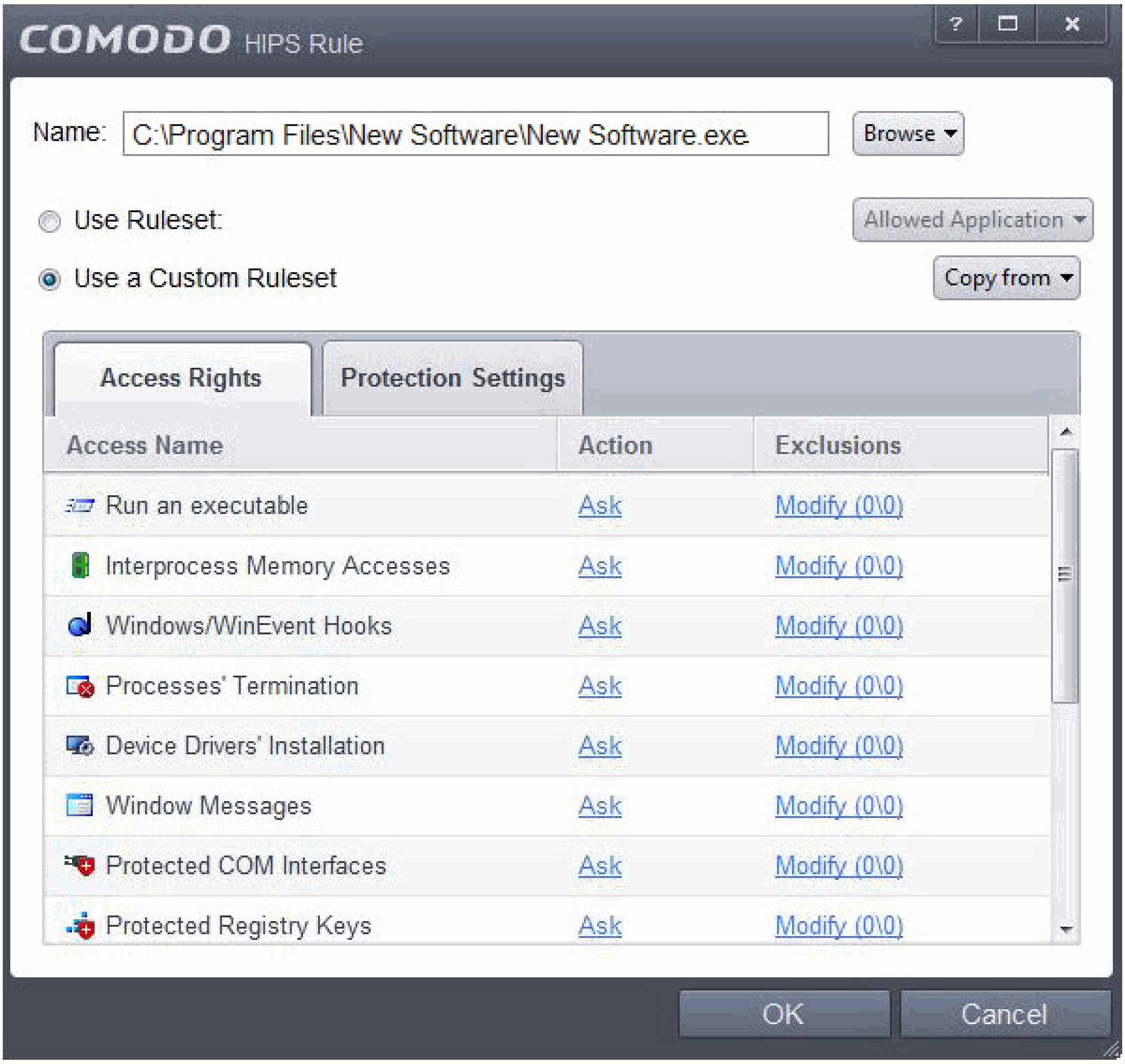
You are about to define a trusted installer that can change everything in your computer!
Furthermore, all the files created by this application will also be treated as trusted installers.
If not used with caution, this action can disable the entire security of your computer including antivirus.
Do you still want to continue?

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

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

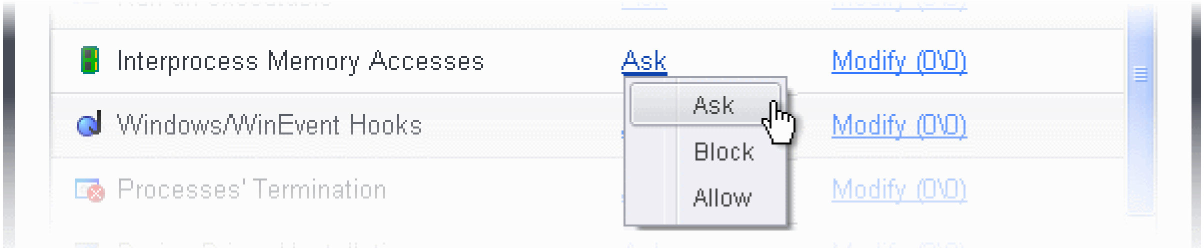
   In simplistic terms 'Access Rights' determine what the application *can do* to other processes and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

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

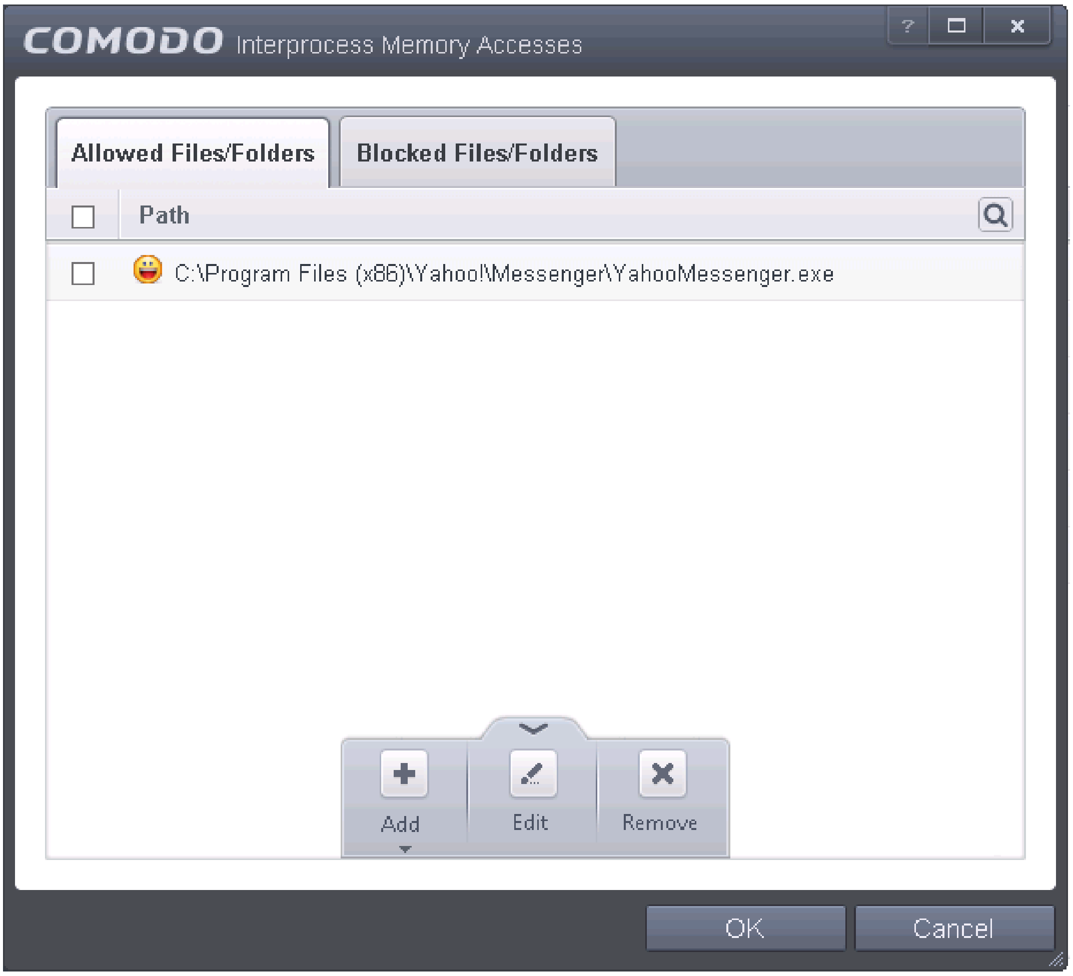


Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (0\0)

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



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

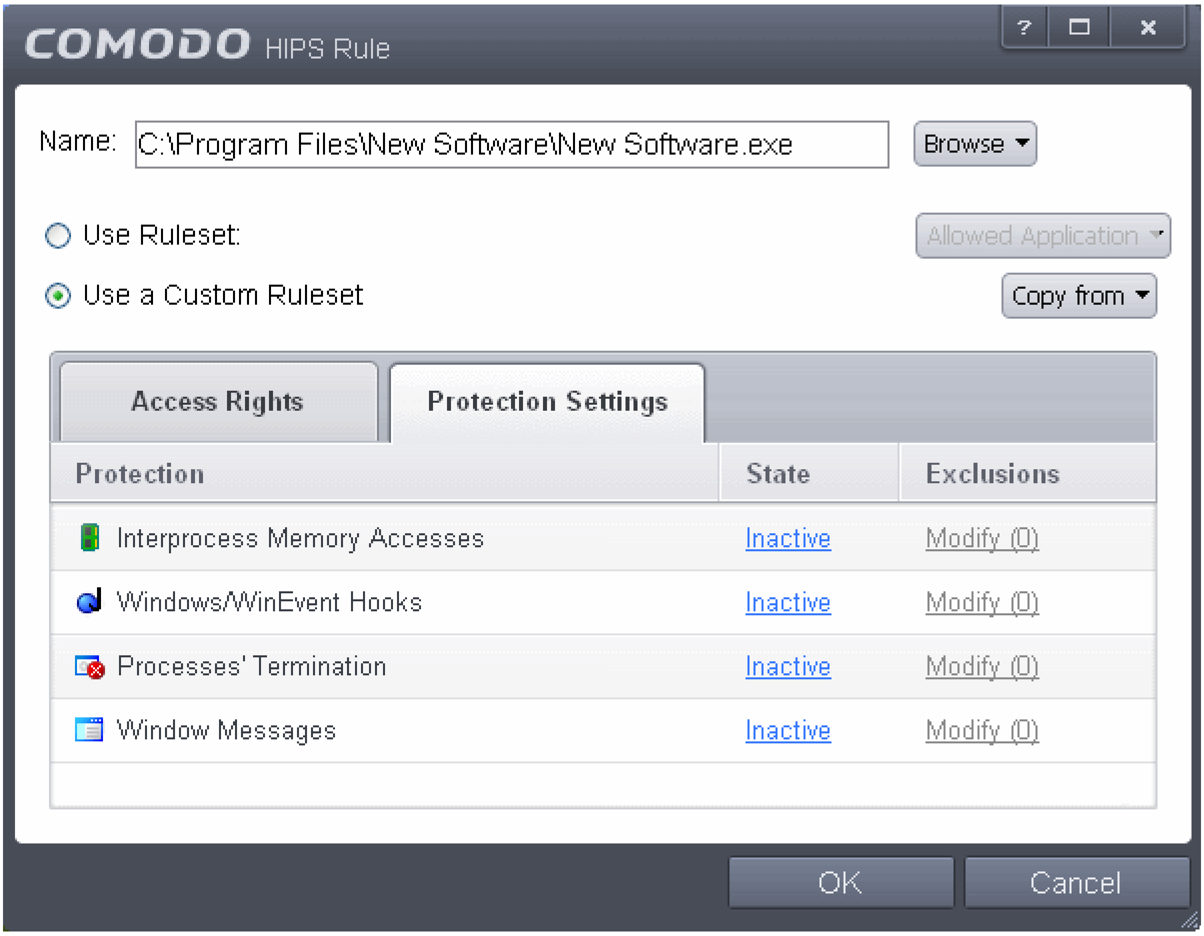


□ C:\Program Files (x86)\Yahoo!\Messenger\YahooMessenger.exe

Clicking the handle and selecting 'Add' allows you to choose which applications or file groups you wish this exception to apply to. (**click here** for an explanation of available options).

In **the example above**, the default action for '*Interprocess Memory Access*' is '*Ask*'. This means HIPS will generate an alert asking your permission if 'New Software.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'opera.exe' to the 'Allowed Applications' tab creates an exception to this rule. New Software.exe can now modify the memory space of opera.exe.

ii. **Protection Settings -** Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



Name: C:\Program Files\New Software\New Software.exe

○ Use Ruleset:

● Use a Custom Ruleset

Protection	State	Exclusions
Interprocess Memory Accesses	Inactive	Modify (0)
Windows/WinEvent Hooks	Inactive	Modify (0)
Processes' Termination	Inactive	Modify (0)
Window Messages	Inactive	Modify (0)

- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection Type' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

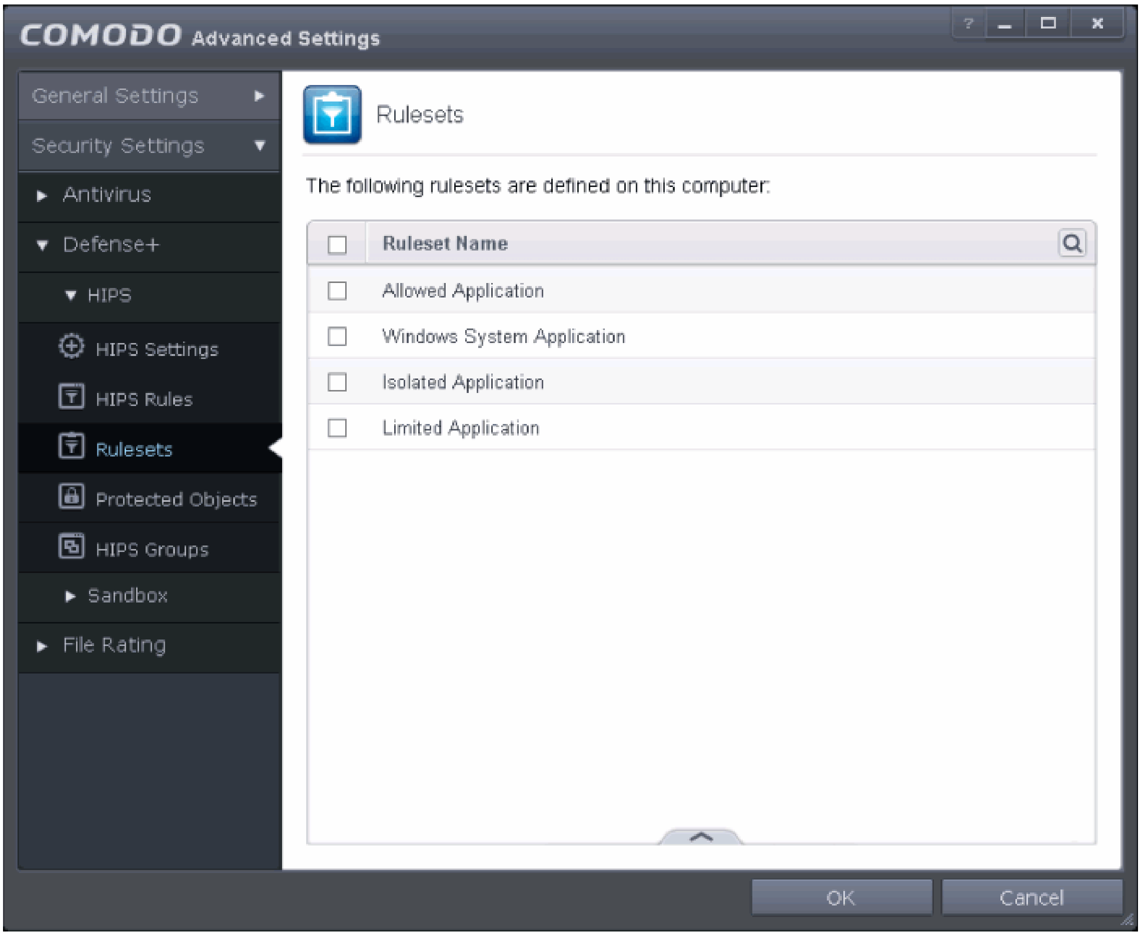
5.2.2.3. HIPS Rule Sets

A Pre-defined ruleset is a set of **access rights and protection settings** that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined rulesets' is a set of rulesets that concern an application's access rights to memory, other programs, the registry etc.

Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your server. For this reason, CAVS contains a selection of rulesets according to broad application categories. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements.

To configure this category

- Navigate to: Advanced Tasks > Security Settings >Defense+ > HIPS > Rulesets. There are four default Rulesets listed under the 'Rules' column.

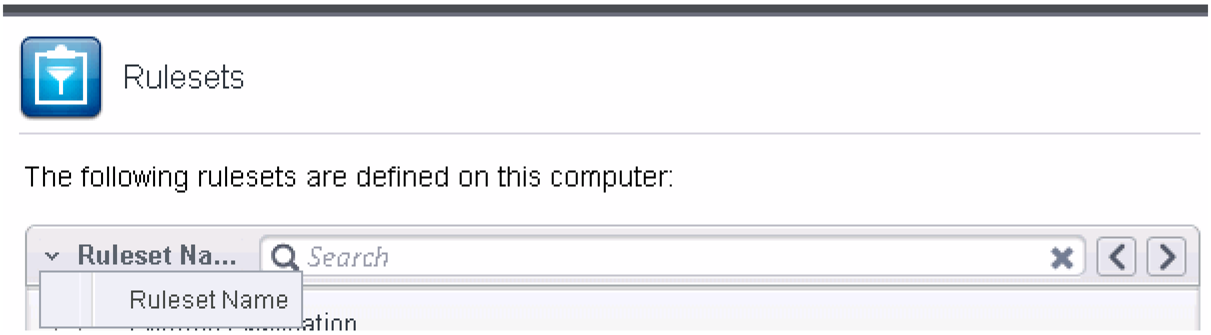


The following rulesets are defined on this computer:

□	Ruleset Name
□	Allowed Application
□	Windows System Application
□	Isolated Application
□	Limited Application

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

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



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

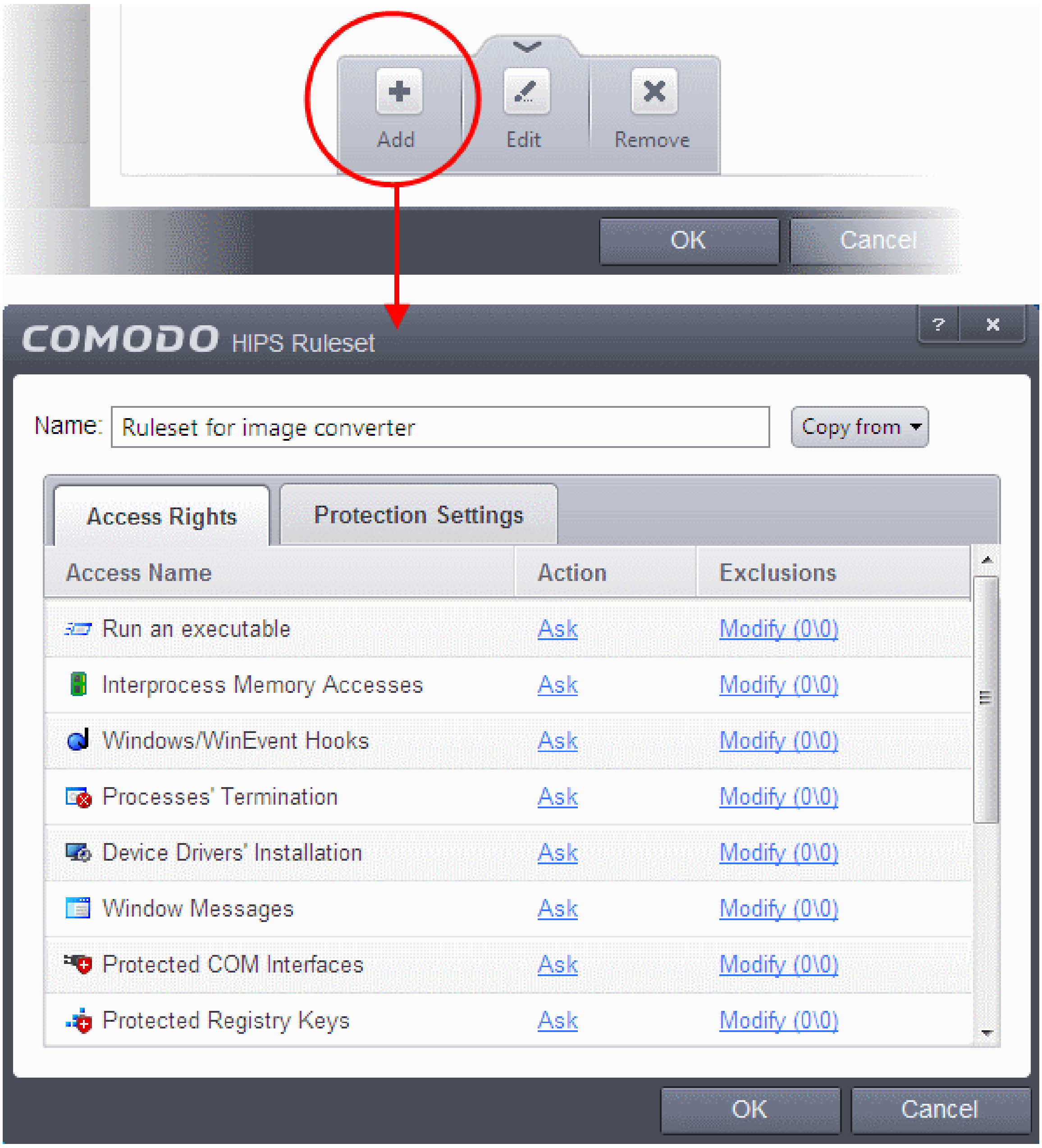
To view or edit an existing predefined ruleset

- Select the Ruleset, click the handle at the bottom of the interface and choose 'Edit' from the options.

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

To create a new predefined ruleset

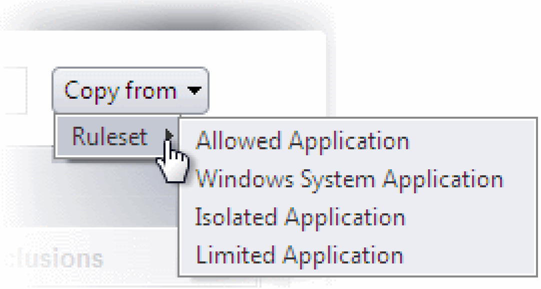
- Click up arrow at the bottom of the interface and choose 'Add' from the options.



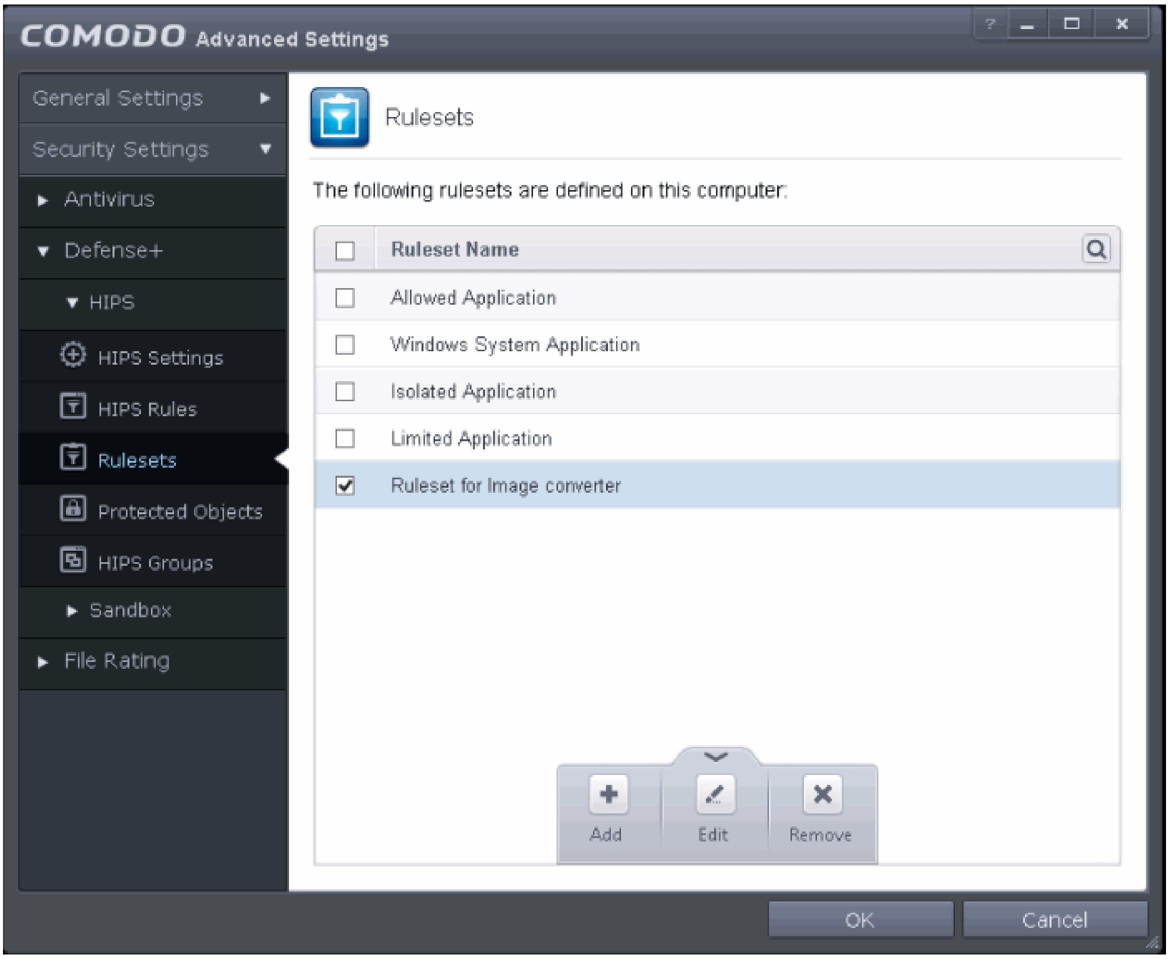
Name: Ruleset for image converter

Access Name	Action	Exclusions
Run an executable	Ask	Modify (0\0)
Interprocess Memory Accesses	Ask	Modify (0\0)
Windows/WinEvent Hooks	Ask	Modify (0\0)
Processes' Termination	Ask	Modify (0\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (0\0)

- Enter a name for the new ruleset.
- To copy the **Access Rights** and **Protection Settings** from another pre-existing ruleset, click 'Copy From' and select the ruleset from the drop-down
- To customize the **Access Rights** and **Protection Settings** as per the requirements of this new rule set, follow the procedure explained in the section **Use a Custom Ruleset**.



- Click OK to save the new ruleset.



The following rulesets are defined on this computer:

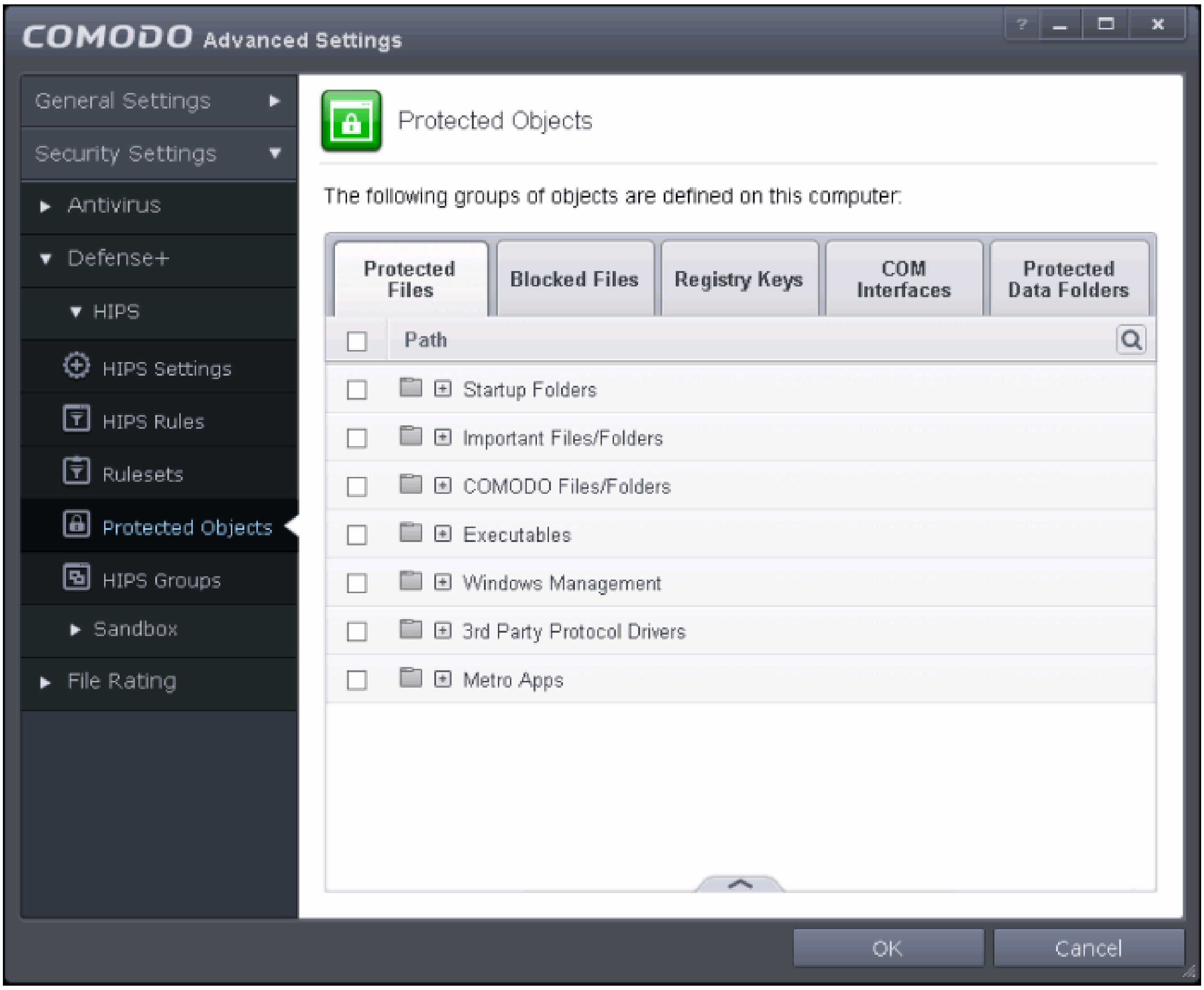
□	Ruleset Name
□	Allowed Application
□	Windows System Application
□	Isolated Application
□	Limited Application
☑	Ruleset for Image converter

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

5.2.2.4. Protected Objects

The Protected Objects panel allows you to protect specific files and folders, system critical registry keys and COM interfaces against access or modification by unauthorized processes and services.

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

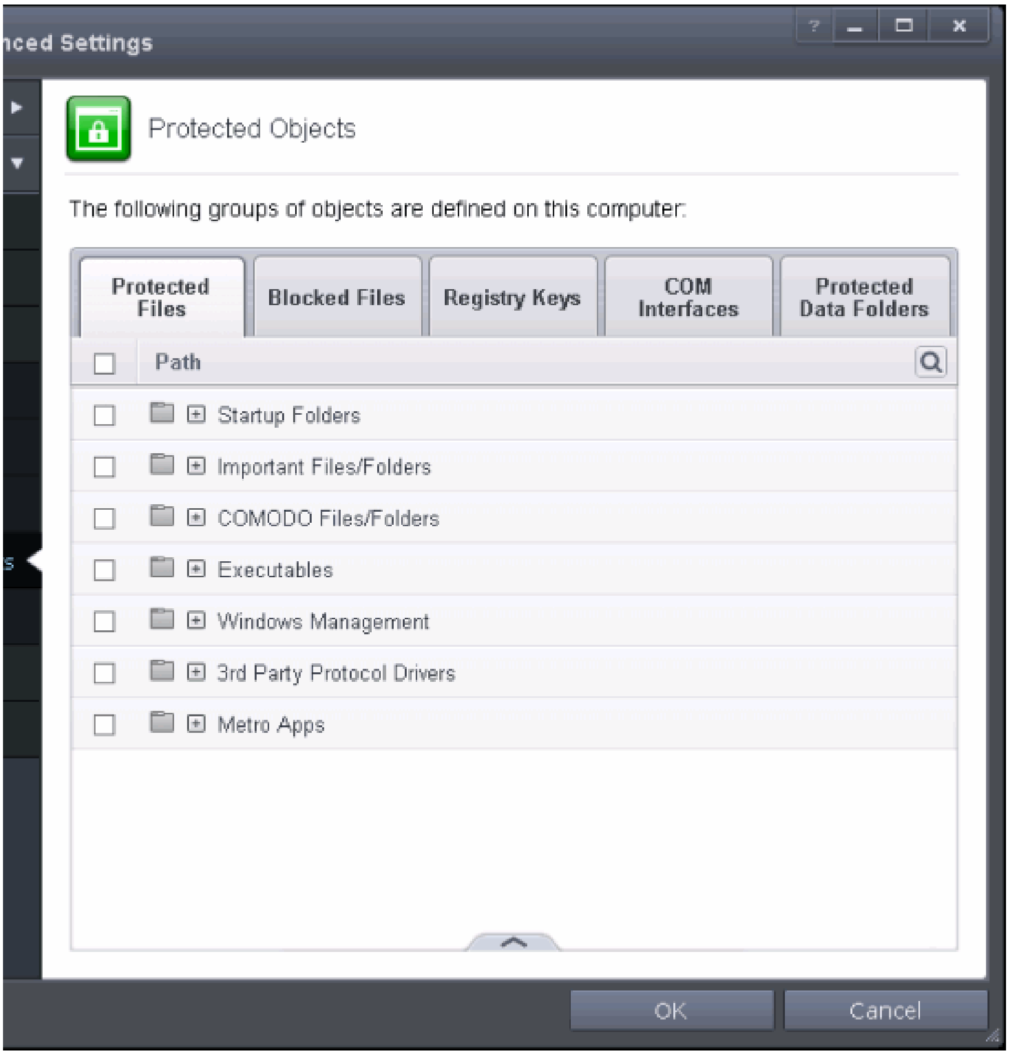


The panel has five tabs:

- **Protected Files** - Allows you to specify programs, applications and files that are to be protected from changes
- **Blocked Files** - Allows you to specify programs, applications and files that are to be blocked from execution and opening
- **Registry Keys -** Allows you to specify registry keys that are to be protected from changes
- **COM Interfaces** - Allows you to specify COM interfaces that are to be protected from changes
- **Protected Data Folders** - Allows you to specify folders containing data files that are to be protected from changes by Sandboxed programs

5.2.2.4.1. Protected Files

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



Protected Objects

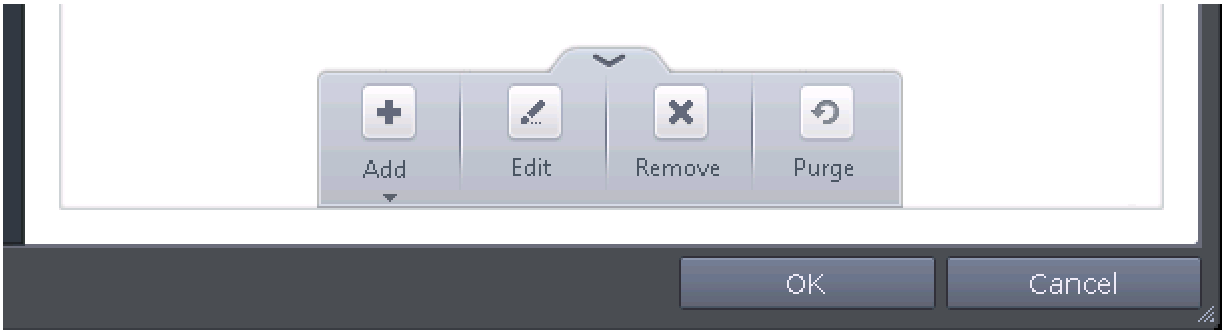
The following groups of objects are defined on this computer:

Protected Files | Blocked Files | Registry Keys | COM Interfaces | Protected Data Folders

□ Path

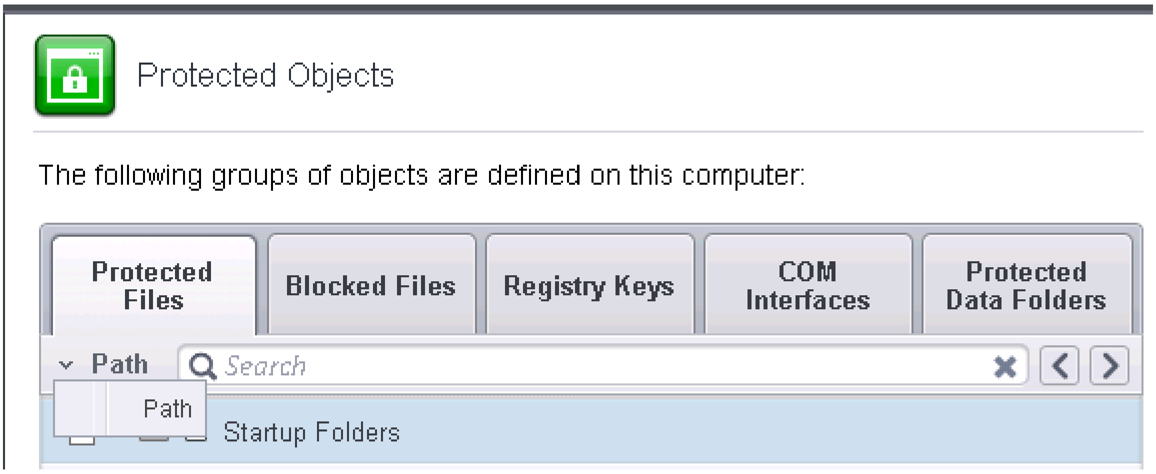
- □ Startup Folders
- □ Important Files/Folders
- □ COMODO Files/Folders
- □ Executables
- □ Windows Management
- □ 3rd Party Protocol Drivers
- □ Metro Apps

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



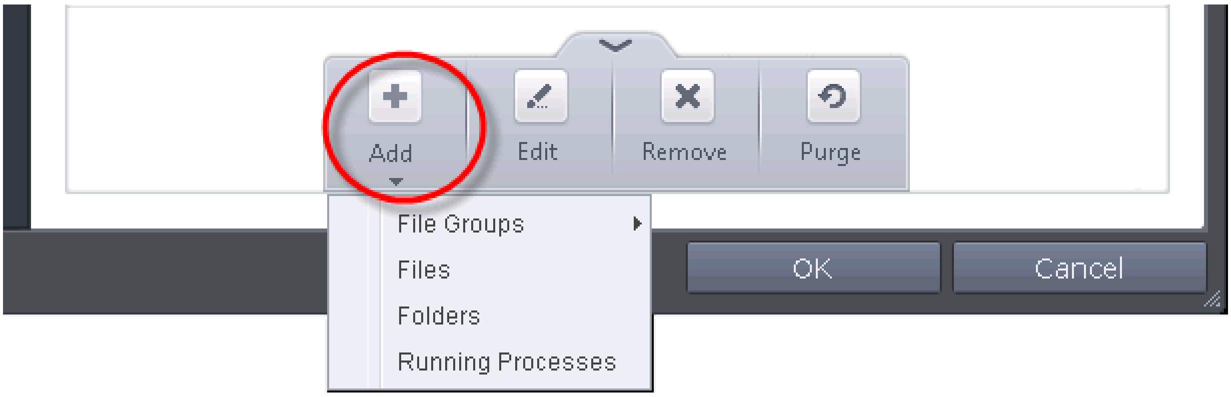
- **Add** - Allows you to add individual files, programs, applications to Protected Files.
- **Edit** - Allows you to edit the path of the file or group of a selected item in the Protected Files interface.
- **Remove** - Deletes the currently highlighted file or file group.
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

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



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

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

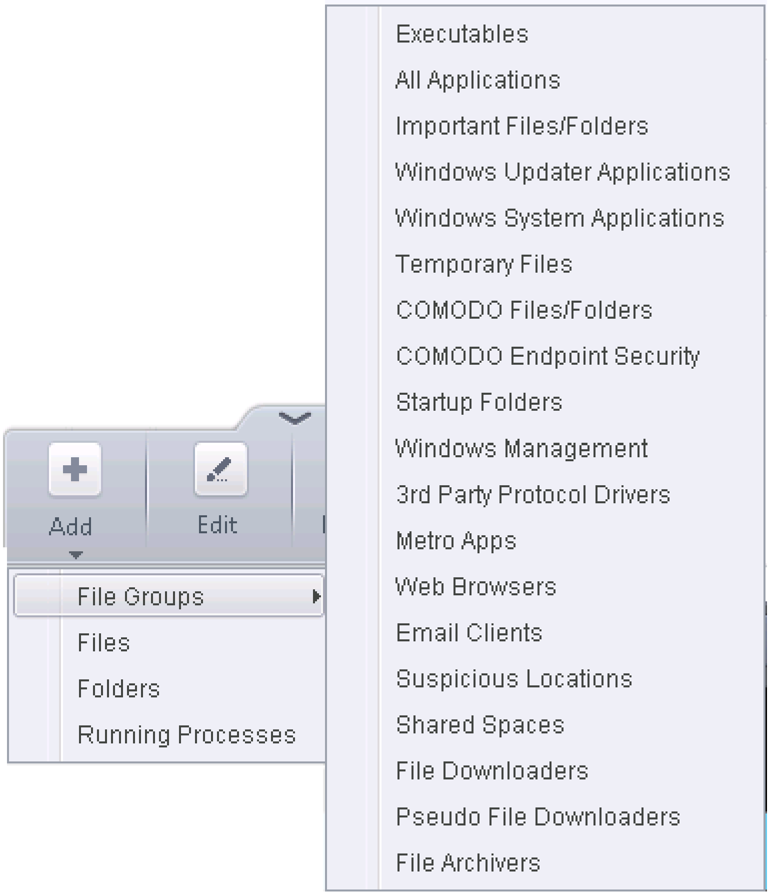


You can add the files by following methods:

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

Adding a File Groups

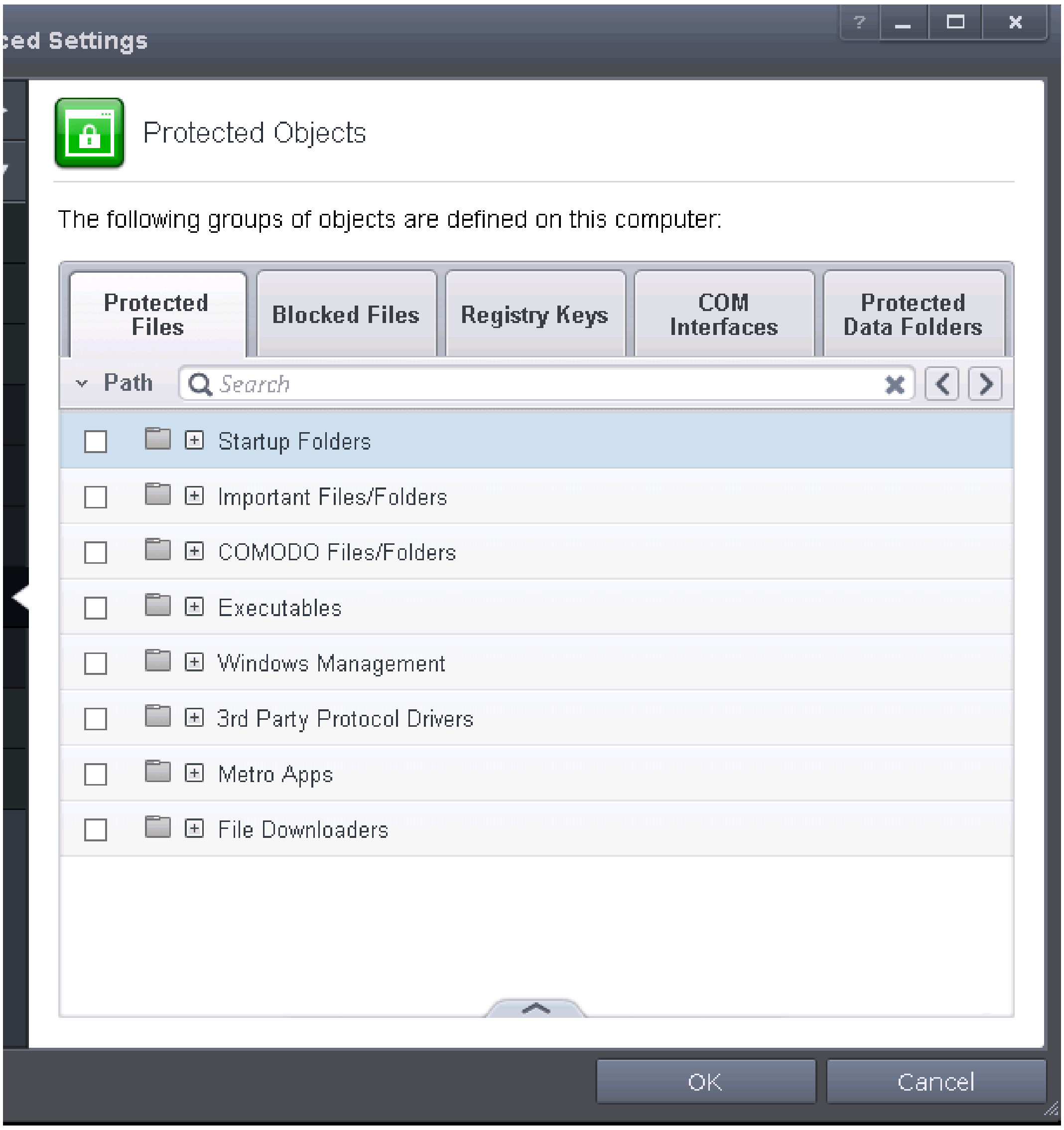
Choosing File Groups allows you to add a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' and so on - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.



CAVS ships with a set of predefined File Groups and can be viewed in Advanced Settings > File Rating >**File Groups**. You can also add new file groups here which will be displayed in the predefined list.

To add a file group to Protected Files, click 'Add' > 'File Groups' and select the type of File Group from the list.

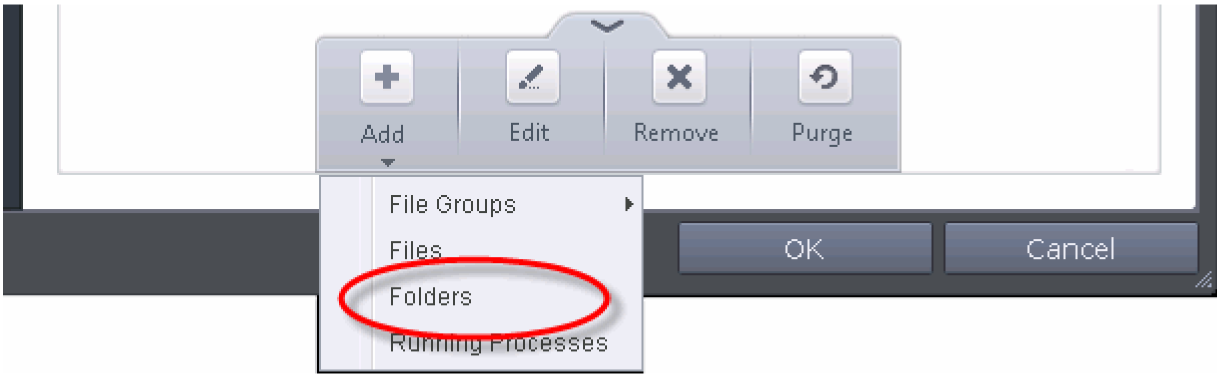
The file group will be added to Protected Files.



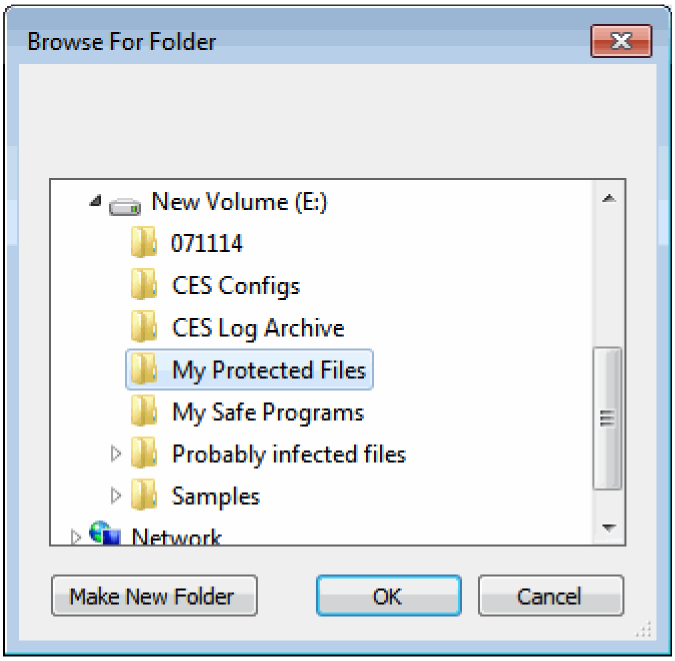
- Repeat the process to add more file groups. The items added to the Protected Files will be protected from access by other programs.

Adding a Drive Partition/Folder

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

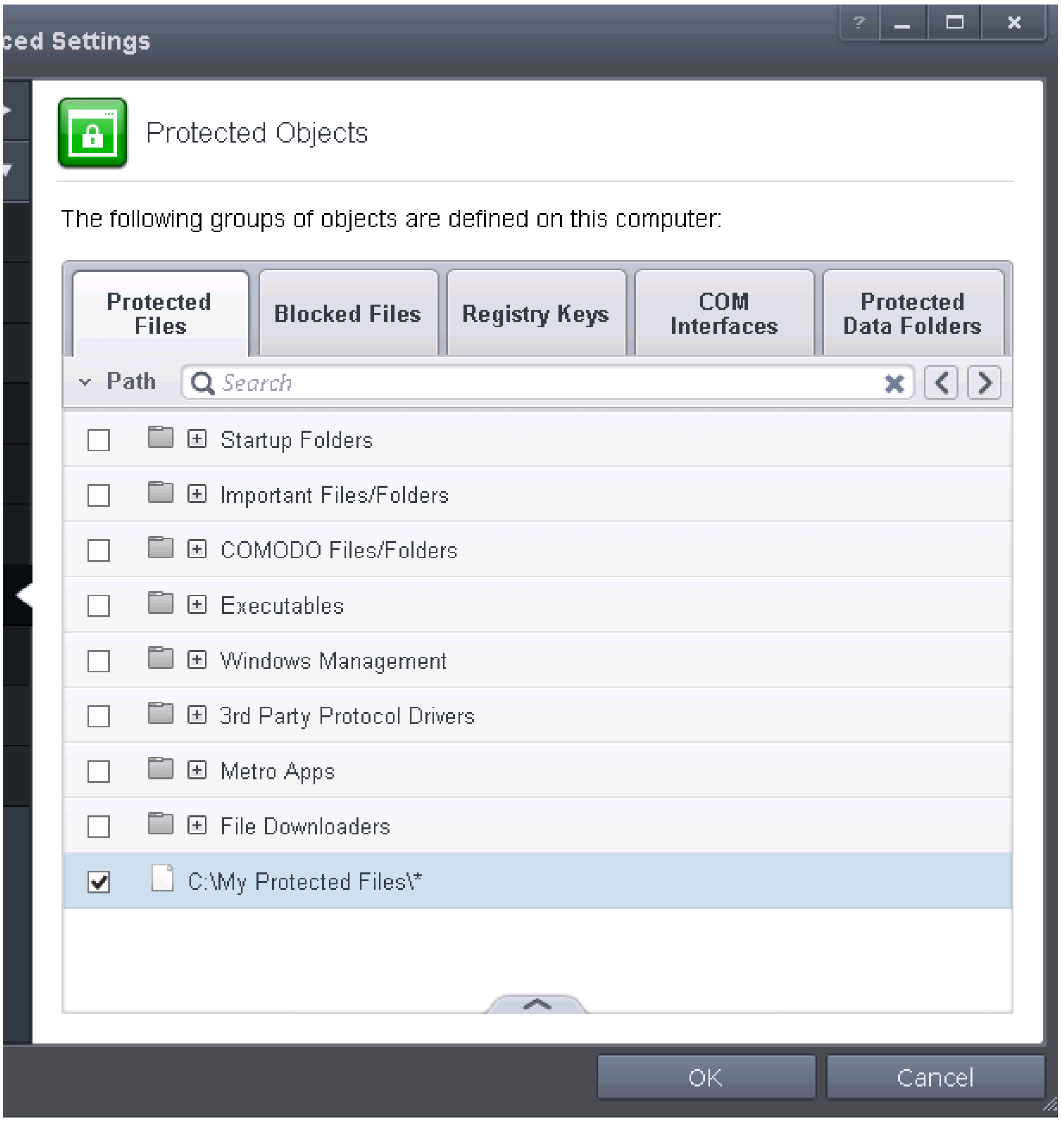


The 'Browse for Folder' dialog will appear.



- Navigate to the drive partition or folder you want to add to Protected Files and click OK

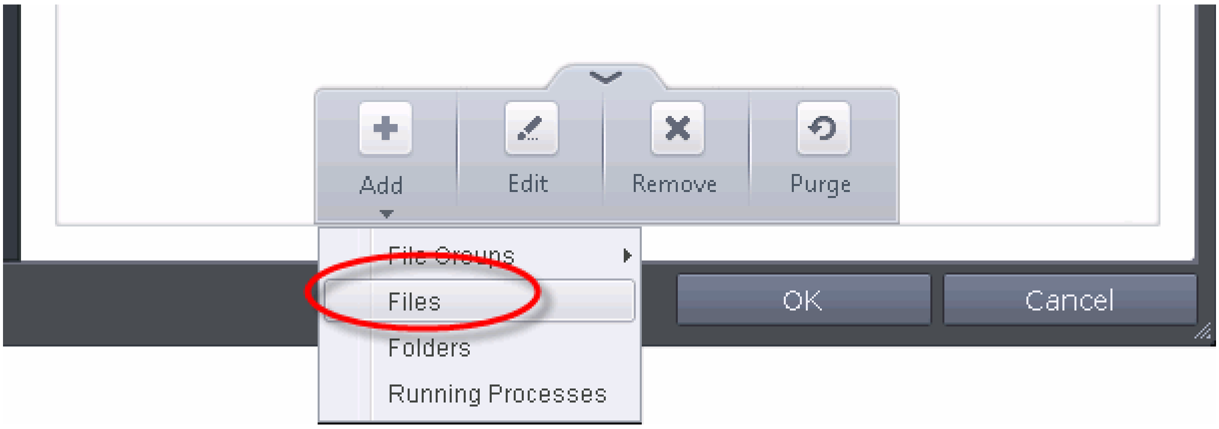
The drive partition/folder will be added to Excluded Paths.



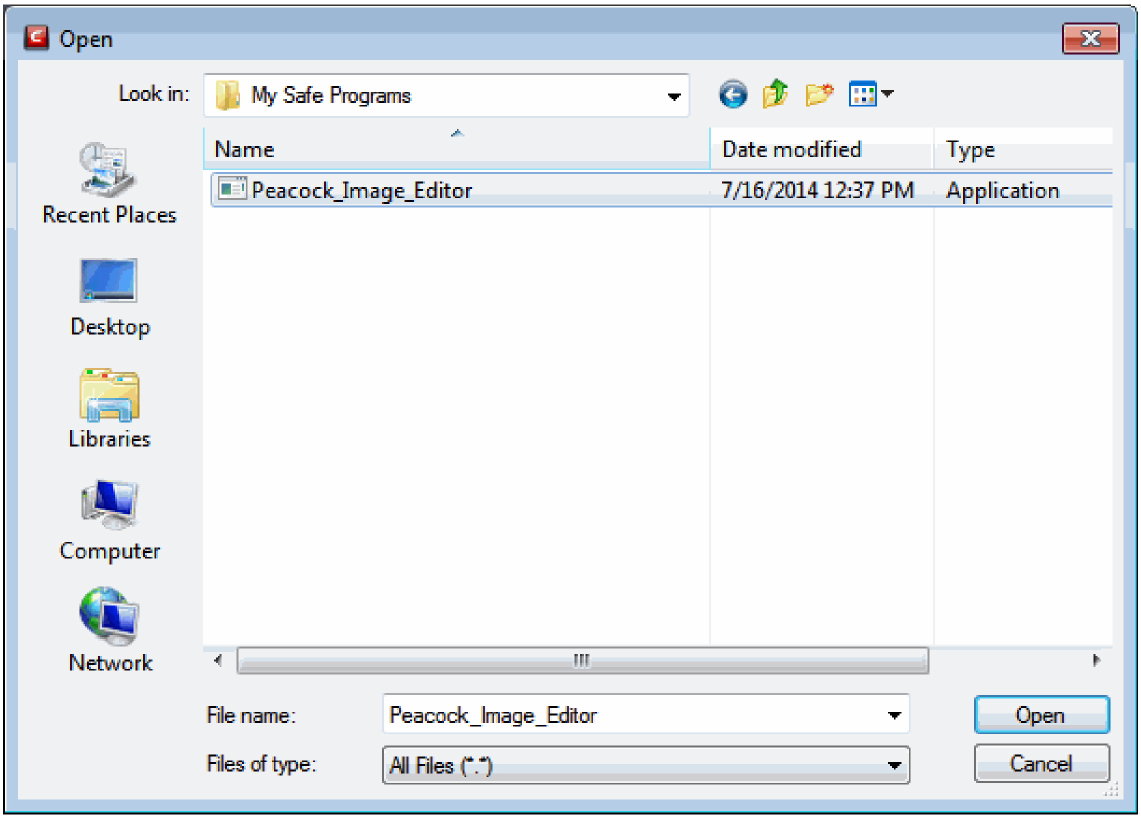
- Repeat the process to add more folders. The items added to the Protected Files will be protected from access by other programs.

Adding an individual File

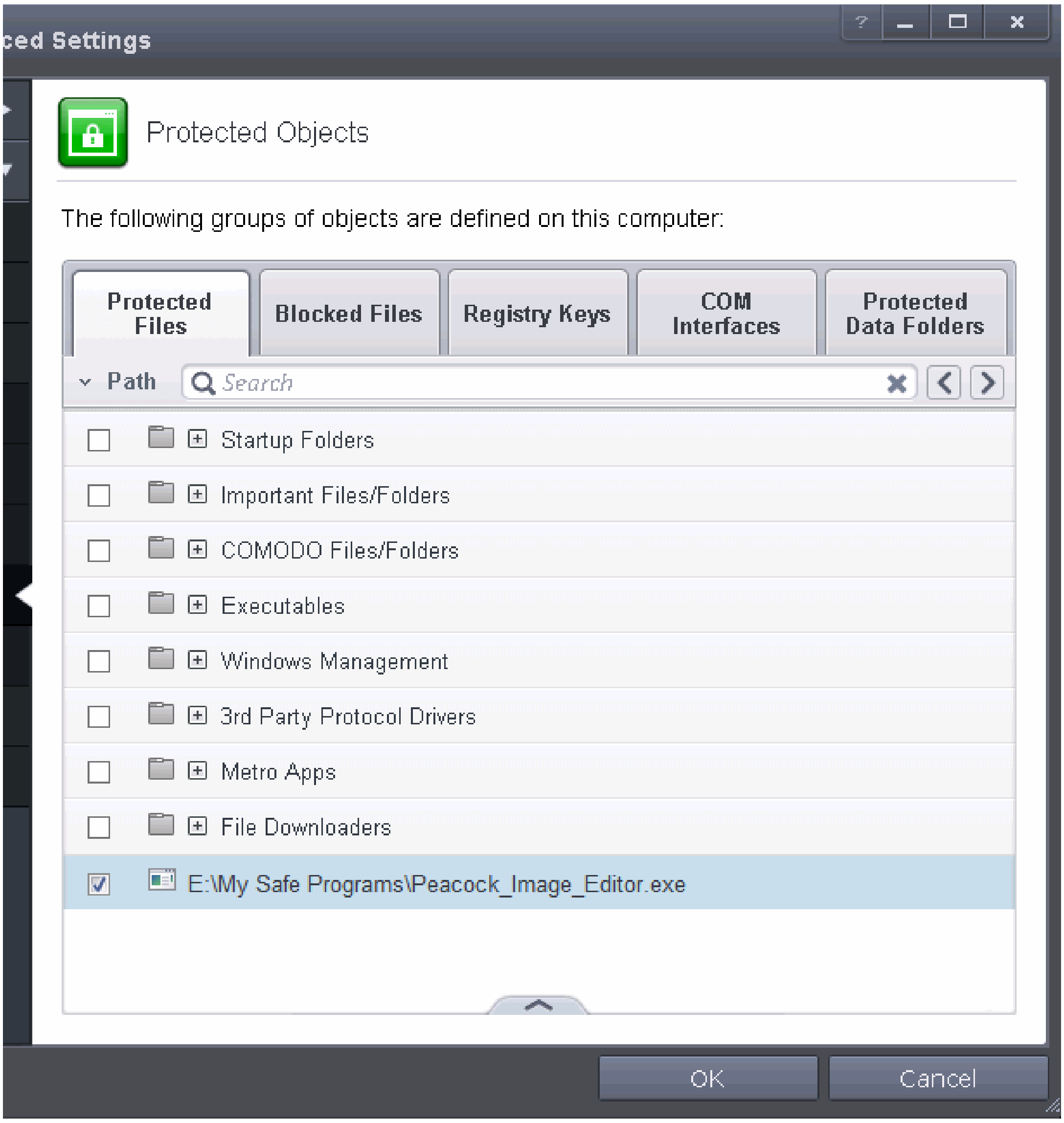
- Choose 'Files' from the 'Add' drop-down.



- Navigate to the file you want to add to Protected Files in the 'Open' dialog and click 'Open'



The file will be added to Protected Files.



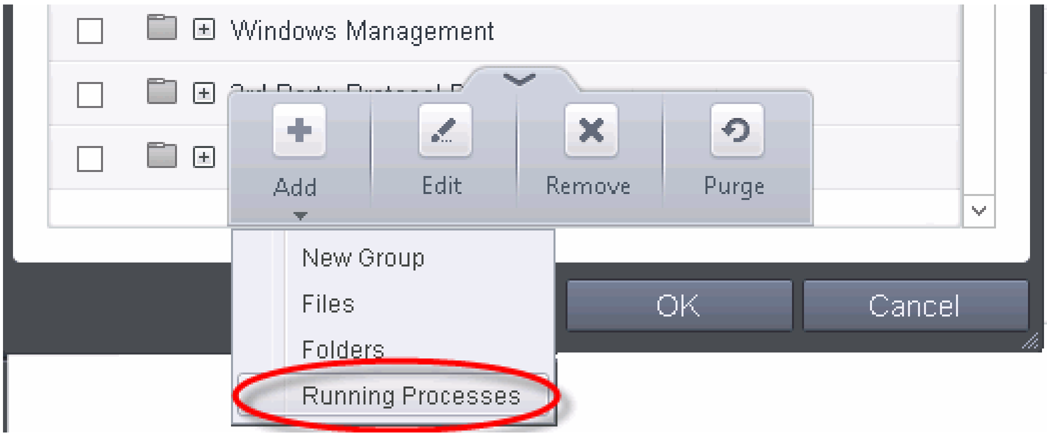
The following groups of objects are defined on this computer:

- □ Startup Folders
- □ Important Files/Folders
- □ COMODO Files/Folders
- □ Executables
- □ Windows Management
- □ 3rd Party Protocol Drivers
- □ Metro Apps
- □ File Downloaders
- ☑ E:\My Safe Programs\Peacock_Image_Editor.exe

- Repeat the process to add more files. The items added to the Protected Files will be protected from access by other programs.

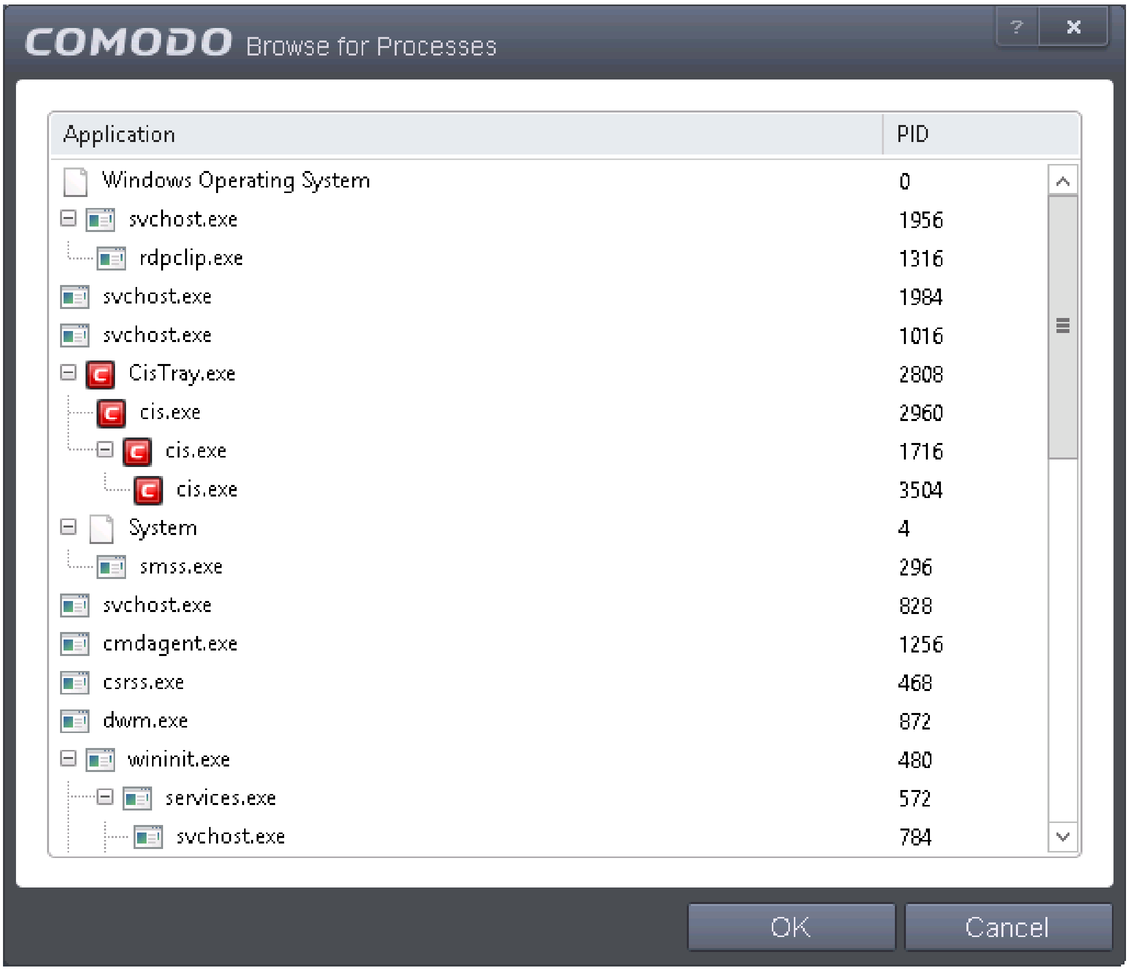
Adding an application from a running processes

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



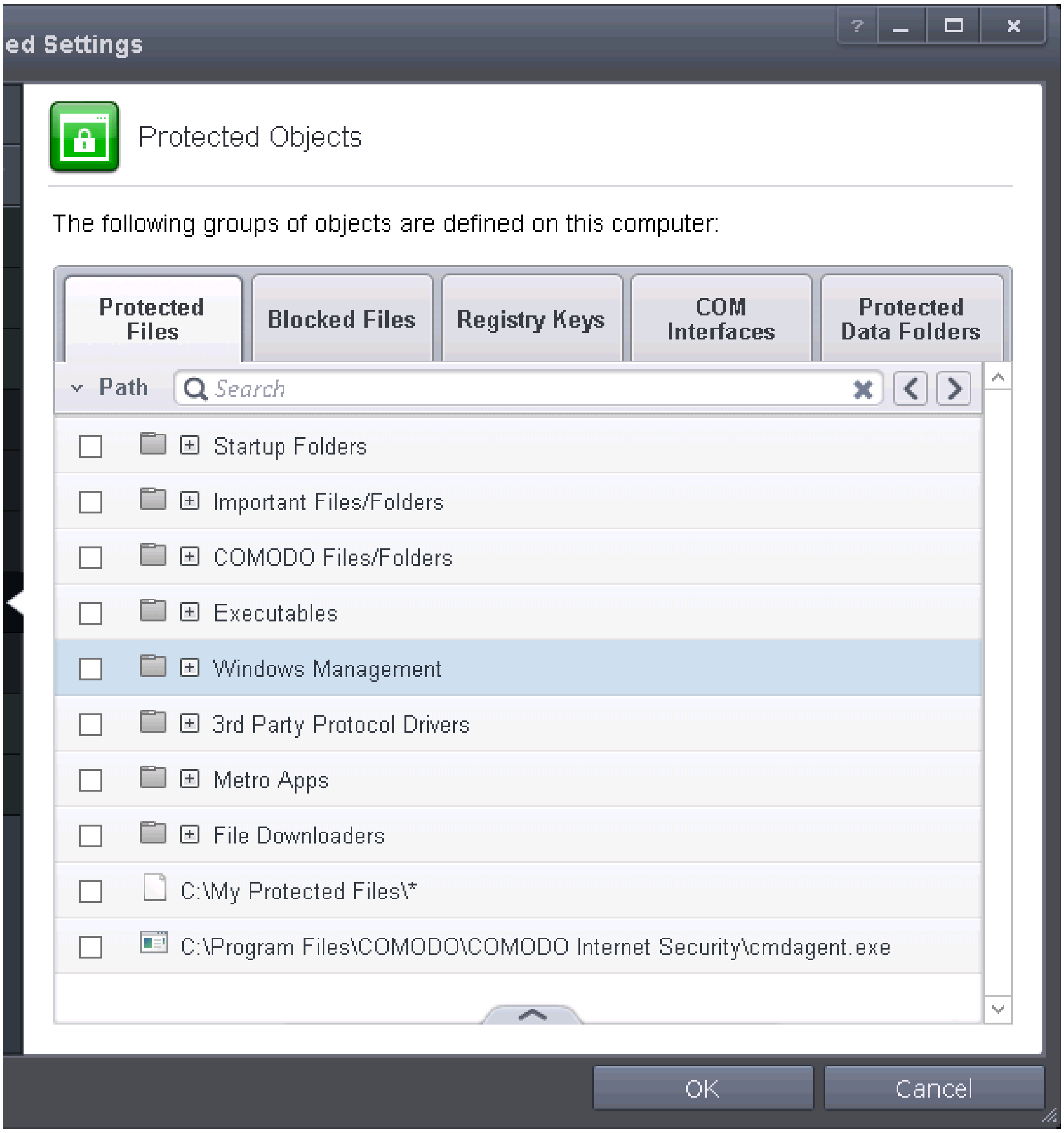
A list of currently running processes in your computer will be displayed

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



Application	PID
Windows Operating System	0
svchost.exe	1956
rdpclip.exe	1316
svchost.exe	1984
svchost.exe	1016
CisTray.exe	2808
cis.exe	2960
cis.exe	1716
cis.exe	3504
System	4
smss.exe	296
svchost.exe	828
cmdagent.exe	1256
csrss.exe	468
dwm.exe	872
wininit.exe	480
services.exe	572
svchost.exe	784

The application will be added to Protected Files.



Protected Objects

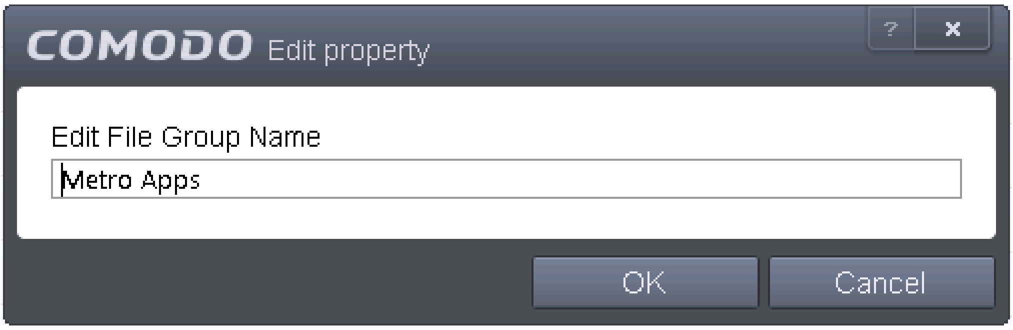
The following groups of objects are defined on this computer:

- □ Startup Folders
- □ Important Files/Folders
- □ COMODO Files/Folders
- □ Executables
- □ Windows Management
- □ 3rd Party Protocol Drivers
- □ Metro Apps
- □ File Downloaders
- □ C:\My Protected Files*
- □ C:\Program Files\COMODO\COMODO Internet Security\cmdagent.exe

- Repeat the process to add more files. The items added to the Protected Files will be protected from access by other programs.

To edit an item in the Protected Files list

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



Edit File Group Name

Metro Apps

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

To delete an item from Protected Files list

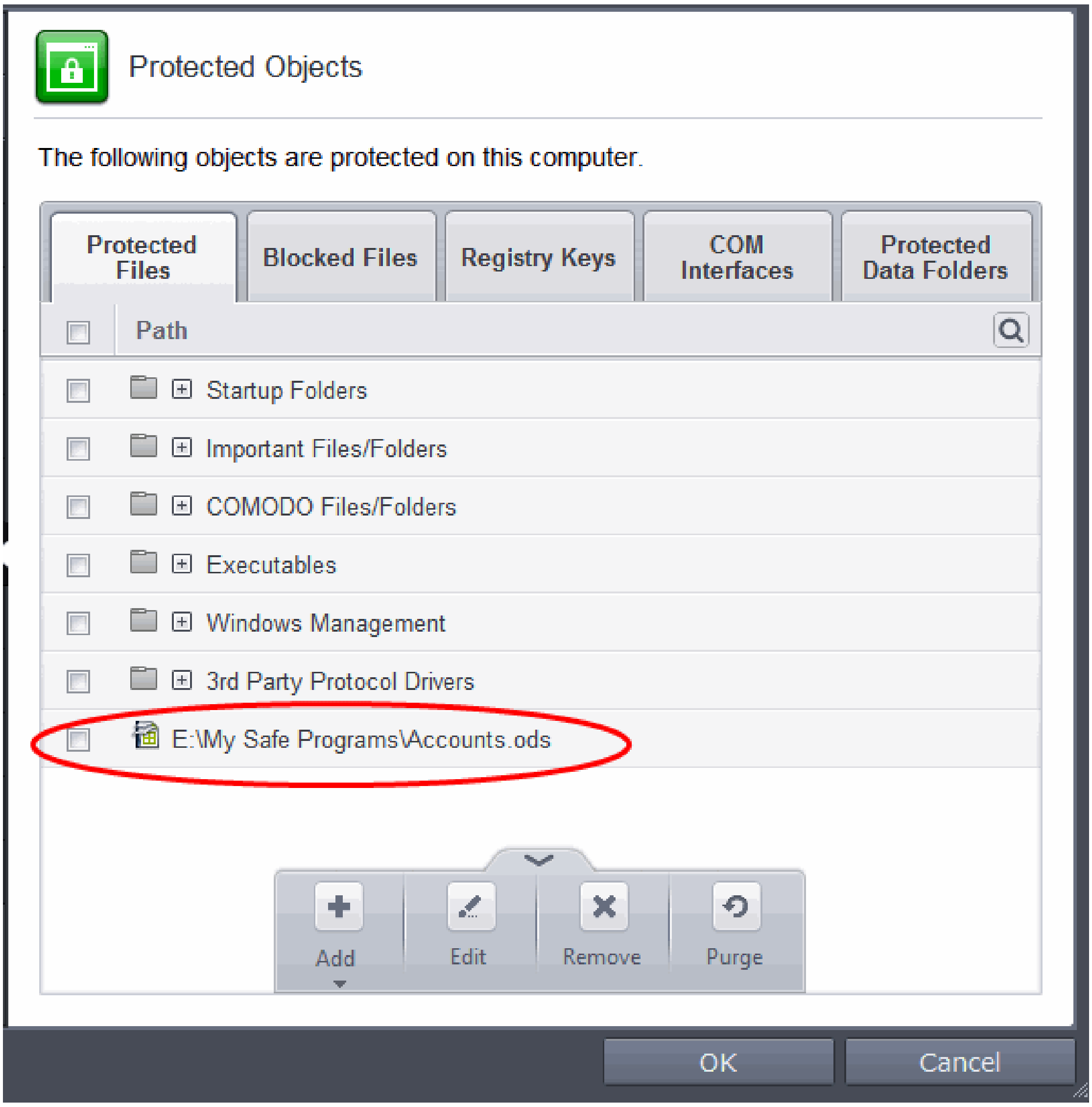
- Select the item from the list, click the handle from the bottom and select 'Remove'.

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

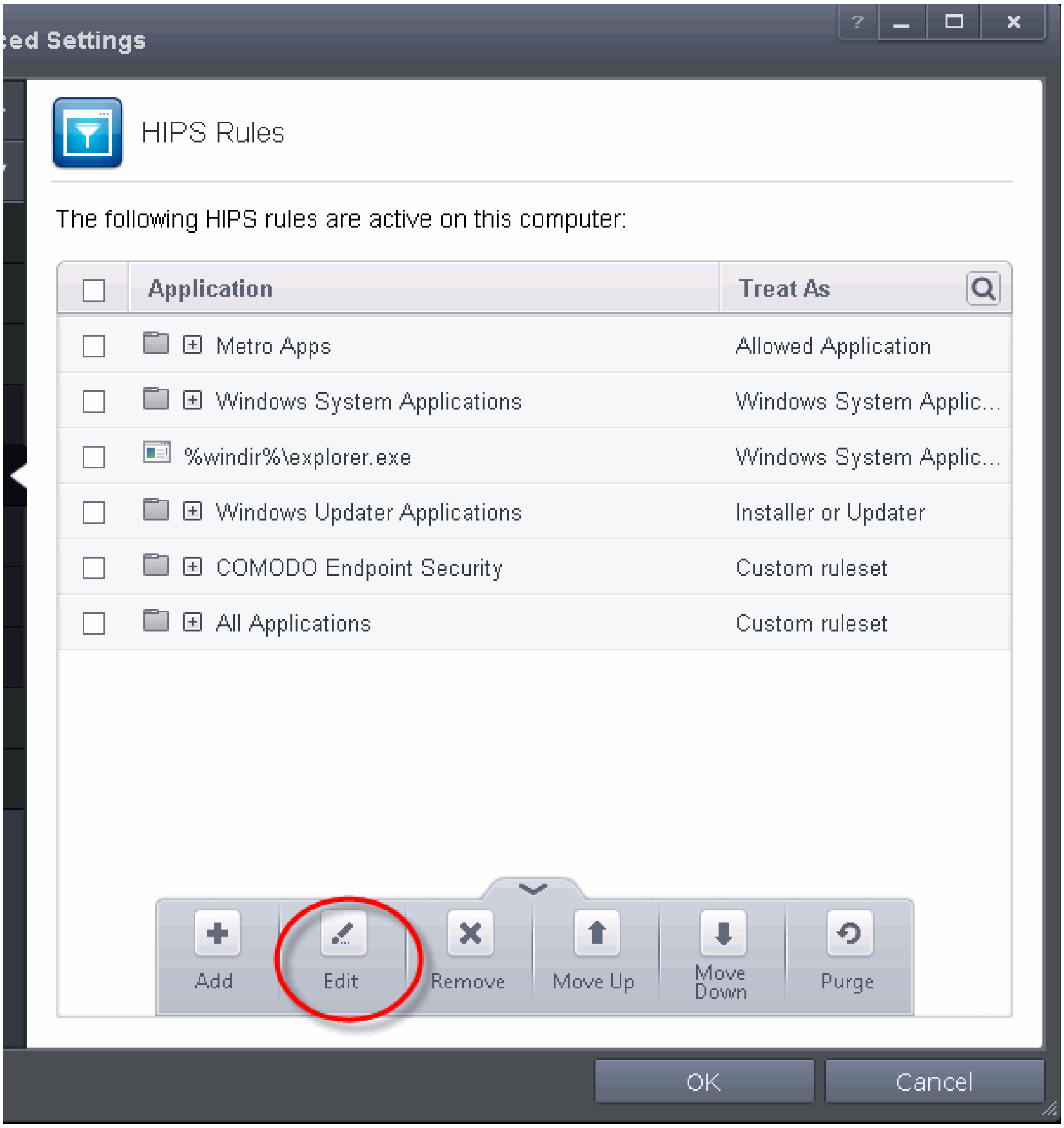
Exceptions

Users can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate Access Right in '**Active HIPS Rules**' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the Open Office Calc program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potential malicious program. You would first **add** the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into '**Active HIPS Rules**' and create an exception for 'scalc' so that it alone could modify 'Accounts.ods'.

- First add Accounts.ods to Protected Files area.



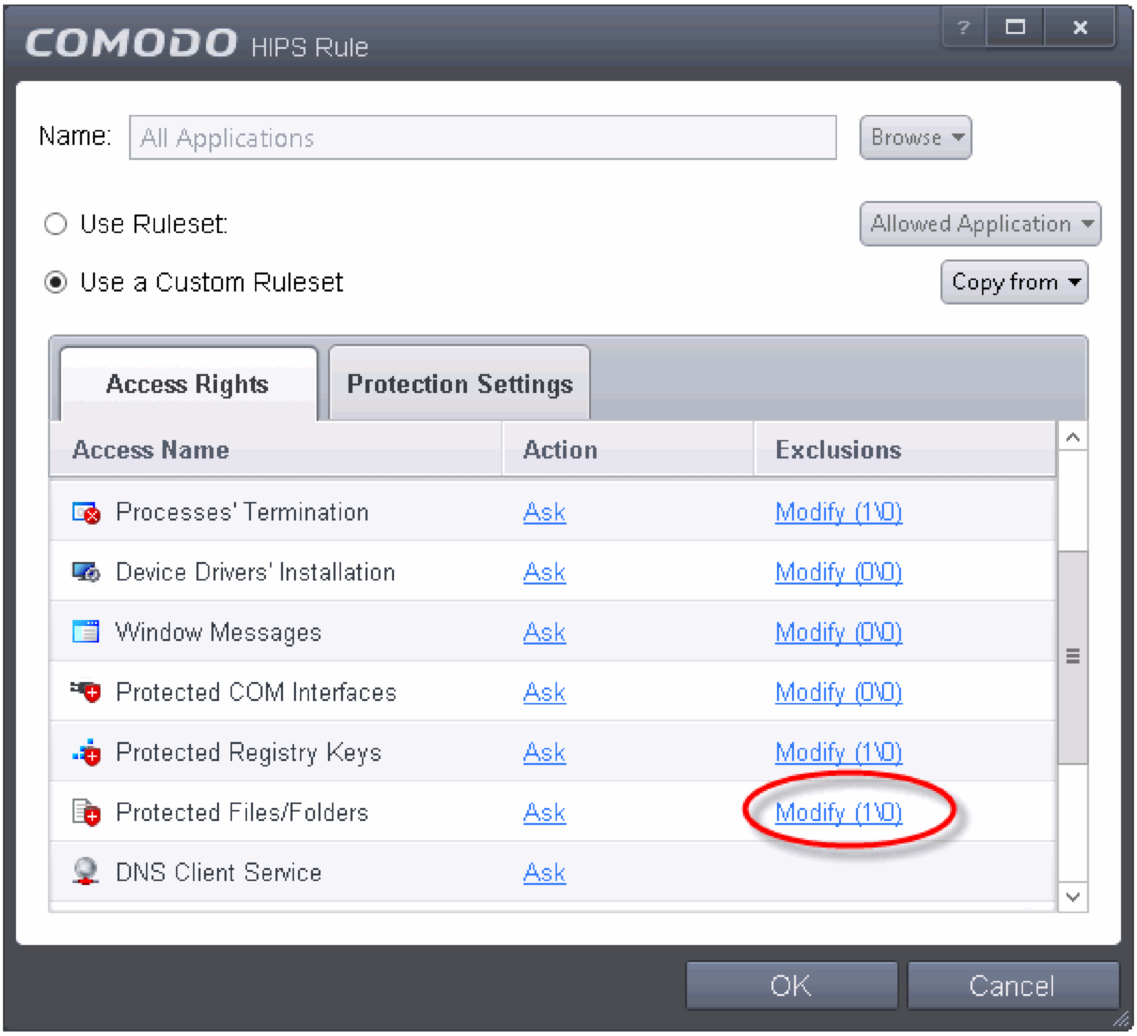
- Then go to HIPS Rules interface and add it to the list of applications (Click Add > select User Ruleset > Allowed Application > Browse and select the file).



The following HIPS rules are active on this computer:

□	Application	Treat As
□	Metro Apps	Allowed Application
□	Windows System Applications	Windows System Applic...
□	%windir%\explorer.exe	Windows System Applic...
□	Windows Updater Applications	Installer or Updater
□	COMODO Endpoint Security	Custom ruleset
□	All Applications	Custom ruleset

- Select the file, click the up arrow and choose 'Edit'.
- In the HIPS Rule interface, select 'Use a custom ruleset'.



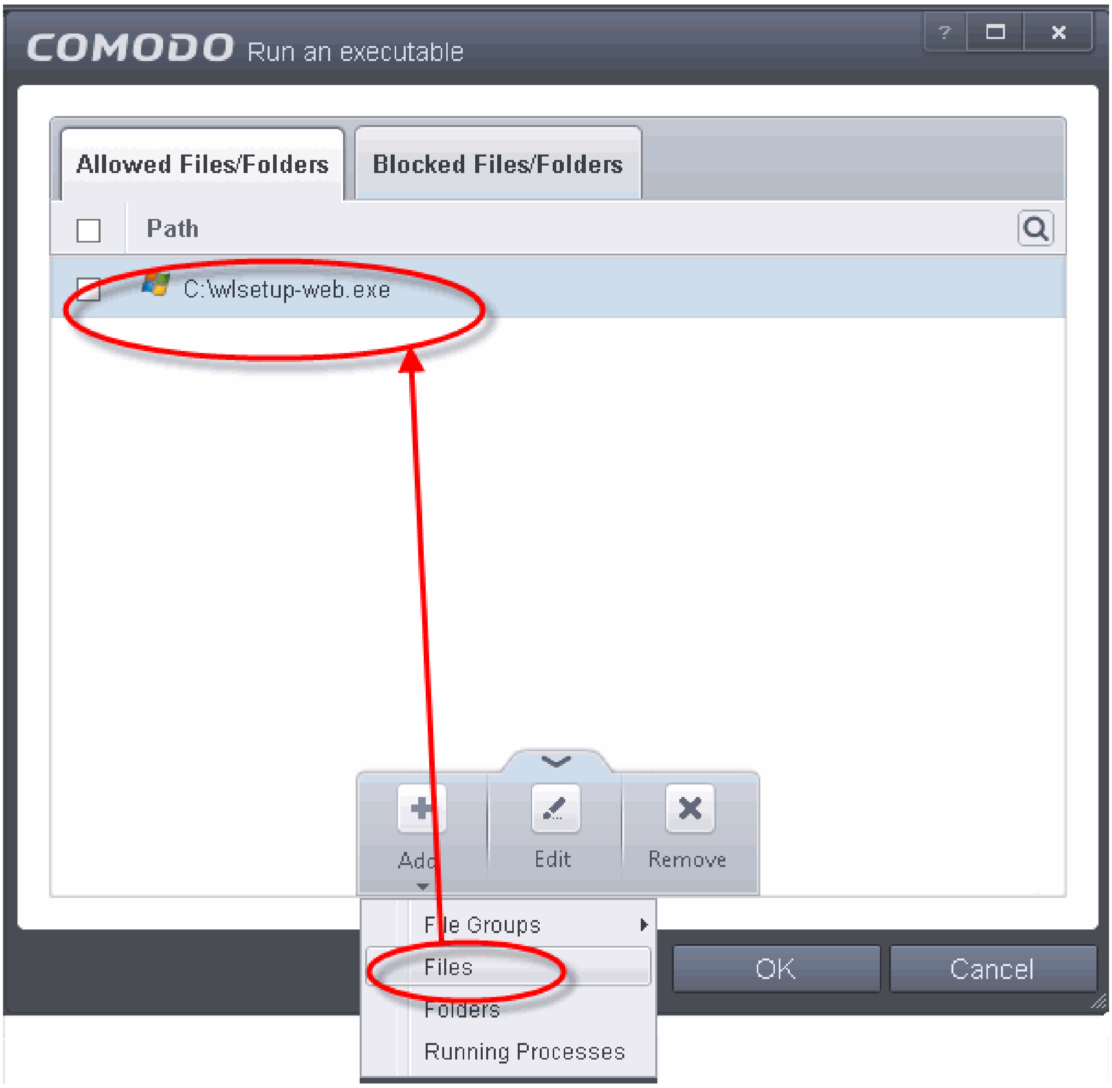
Name: All Applications

○ Use Ruleset:

● Use a Custom Ruleset

Access Name	Action	Exclusions
Processes' Termination	Ask	Modify (1\0)
Device Drivers' Installation	Ask	Modify (0\0)
Window Messages	Ask	Modify (0\0)
Protected COM Interfaces	Ask	Modify (0\0)
Protected Registry Keys	Ask	Modify (1\0)
Protected Files/Folders	Ask	Modify (1\0)
DNS Client Service	Ask	

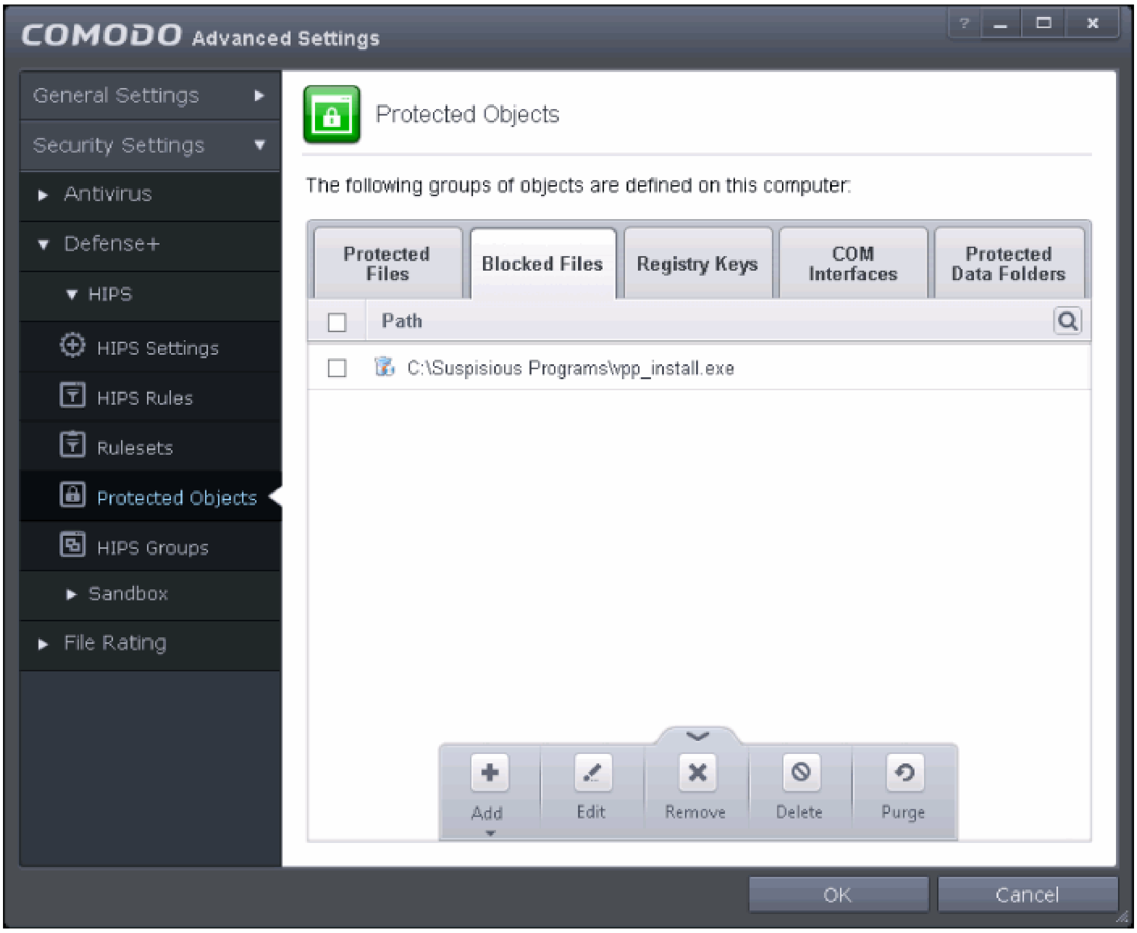
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the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



Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area (* = all files in this directory). Next go to '**HIPS Rules**', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

5.2.2.4.2. Blocked Files

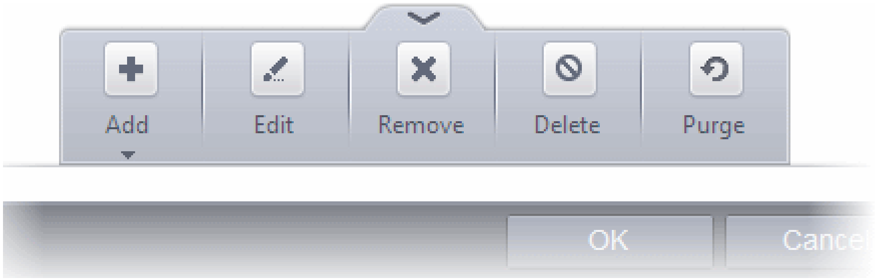
Defense+ allows you to lock-down files and folders by completely denying all access rights to them from other processes or users - effectively cutting it off from the rest of your server. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files that are placed in 'Protected Files', users cannot selectively allow any process access to a blocked file.



The following groups of objects are defined on this computer:

□ C:\Suspisious Programs\wpp_install.exe

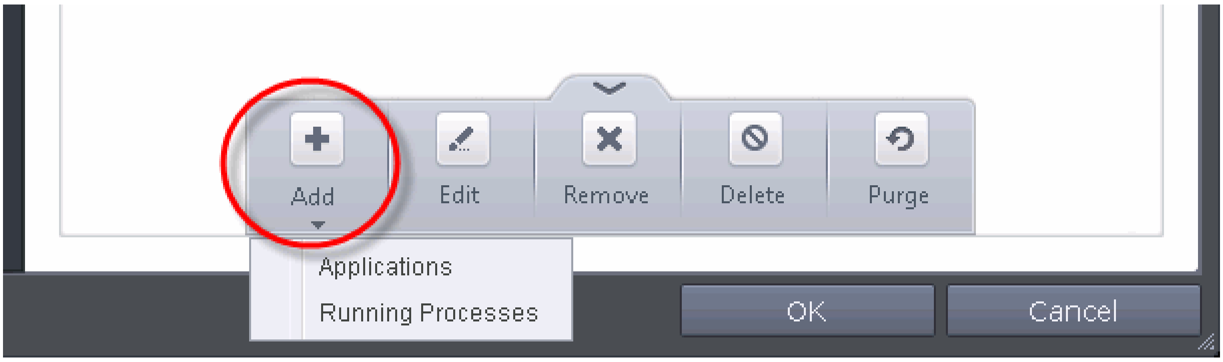
Clicking the handle at the bottom of the interface opens an options panel with the following options:



- **Add** - Allows you to add individual files, programs, applications to Blocked Files.
- **Edit** - Allows you to edit the path of the file.
- **Remove** - Releases the currently highlighted file from the blocked files list.
- **Delete** - Deletes the highlighted file from your server
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

To manually add an individual file or application

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

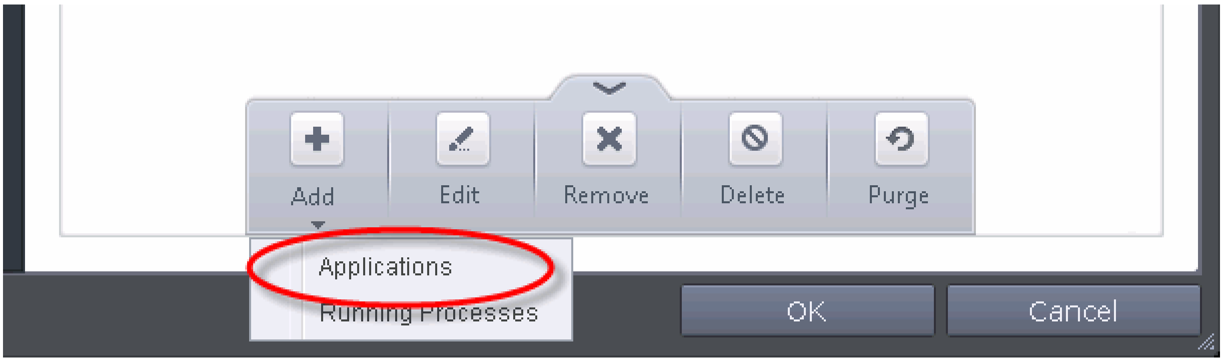


You can add the files by following methods:

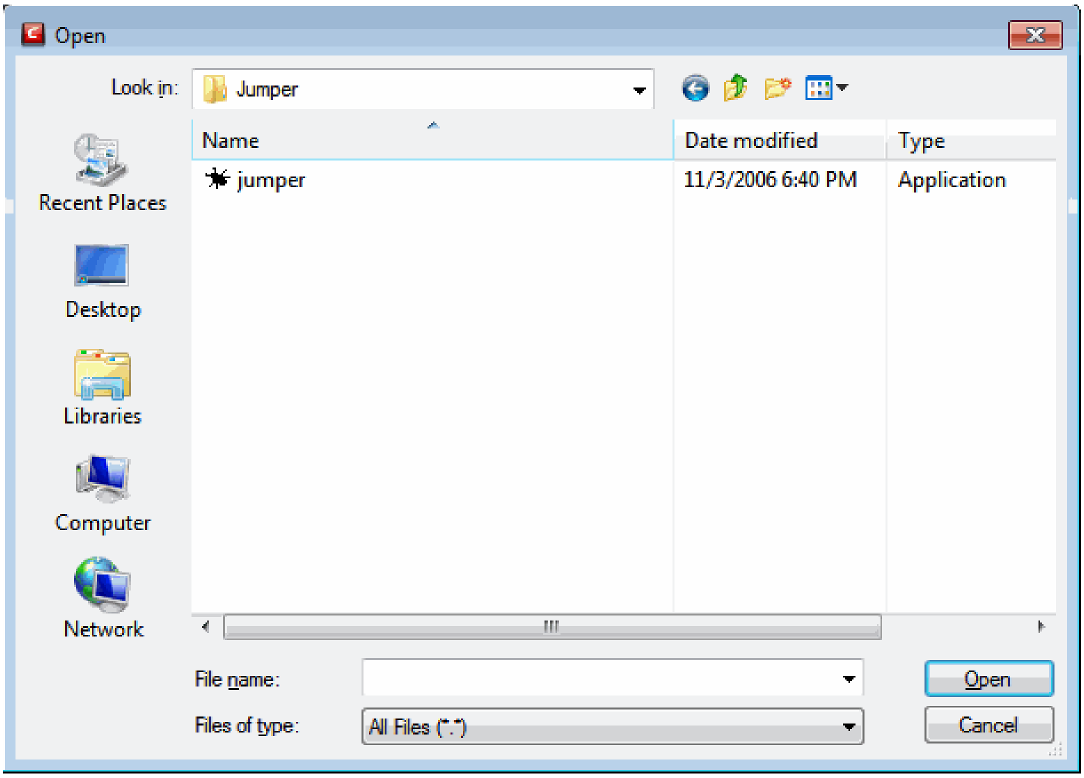
- **Selecting a File**
- **Selecting from currently running Processes**

Adding a File

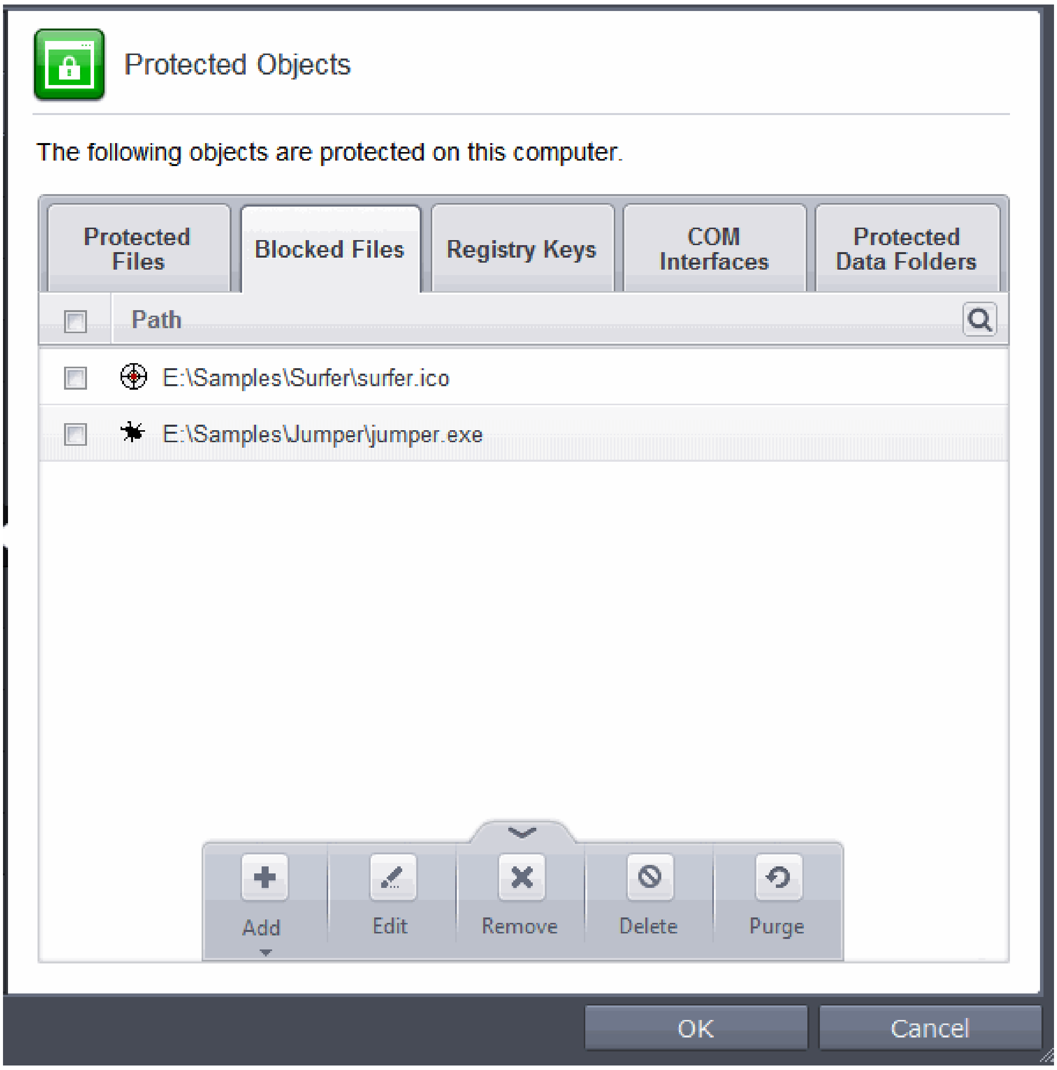
- Choose 'Applications' from the 'Add' drop-down.



- Navigate to the file you want to add to Blocked Files in the 'Open' dialog and click 'Open'



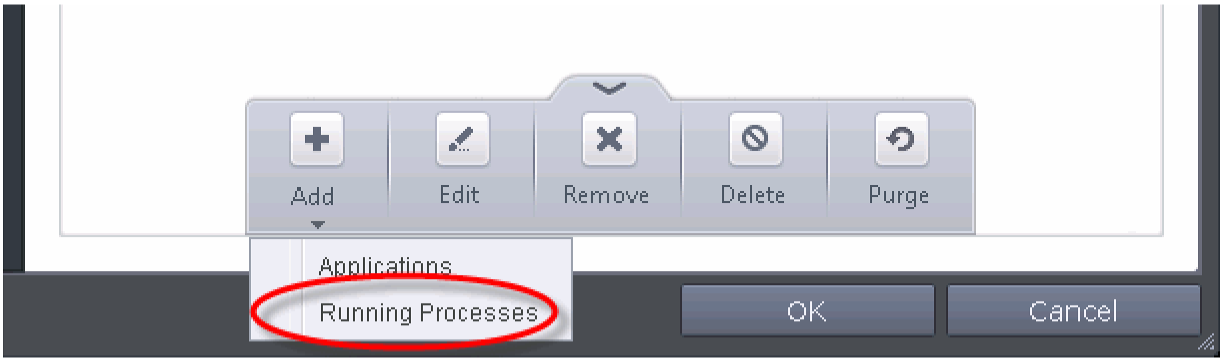
The file will be added to Blocked Files.



- Repeat the process to add more files.

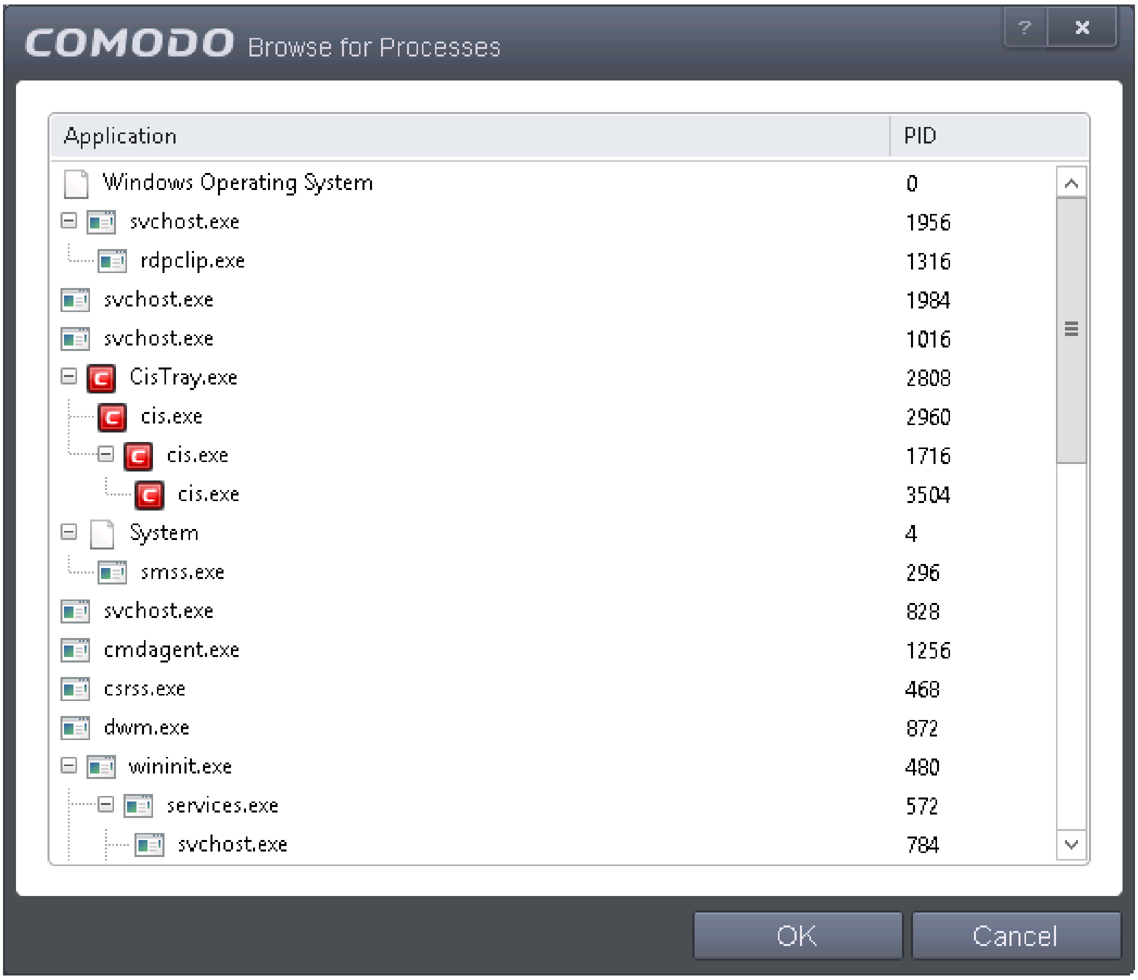
Adding an application from a running processes

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



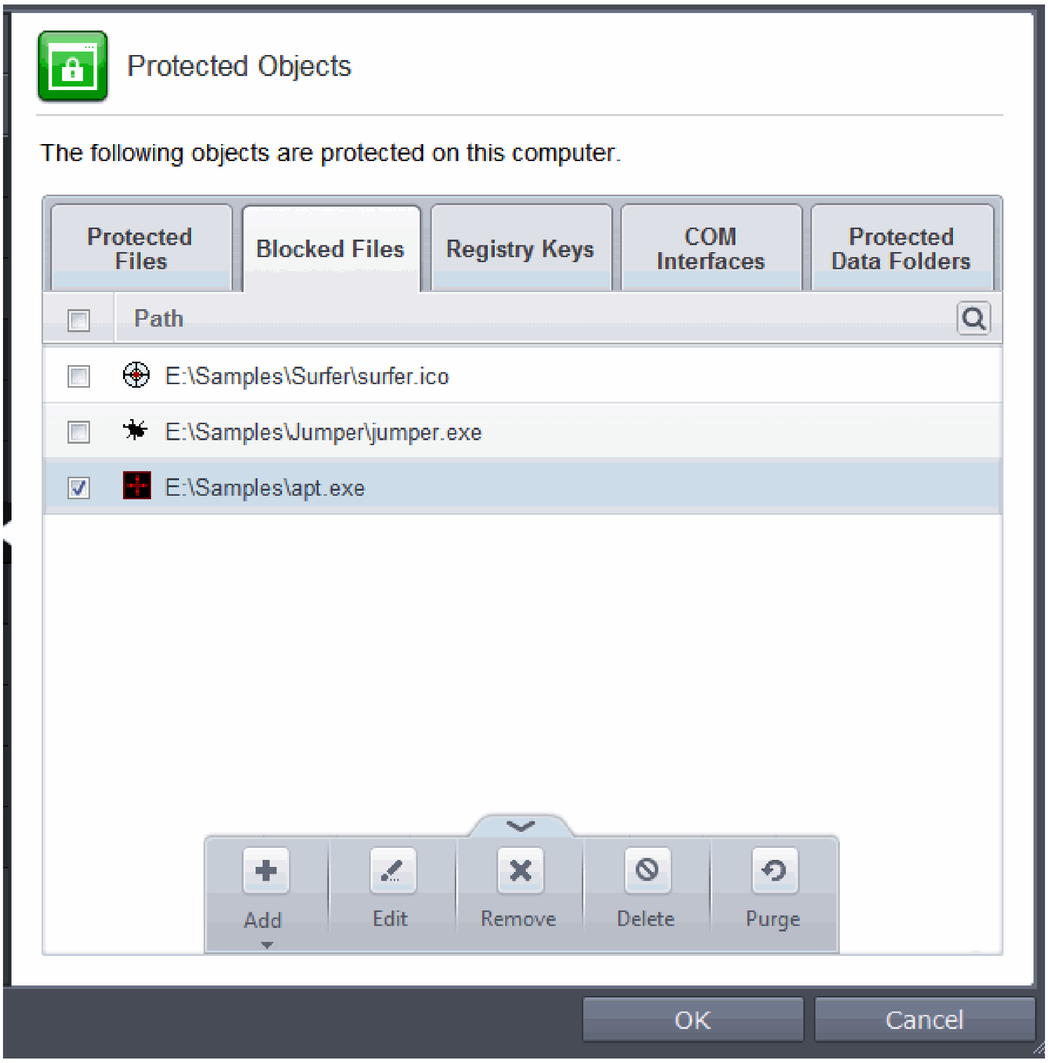
A list of currently running processes in your computer will be displayed

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



Application	PID
Windows Operating System	0
svchost.exe	1956
rdpclip.exe	1316
svchost.exe	1984
svchost.exe	1016
CisTray.exe	2808
cis.exe	2960
cis.exe	1716
cis.exe	3504
System	4
smss.exe	296
svchost.exe	828
cmdagent.exe	1256
csrss.exe	468
dwm.exe	872
wininit.exe	480
services.exe	572
svchost.exe	784

The application will be added to Blocked Files.



Protected Objects

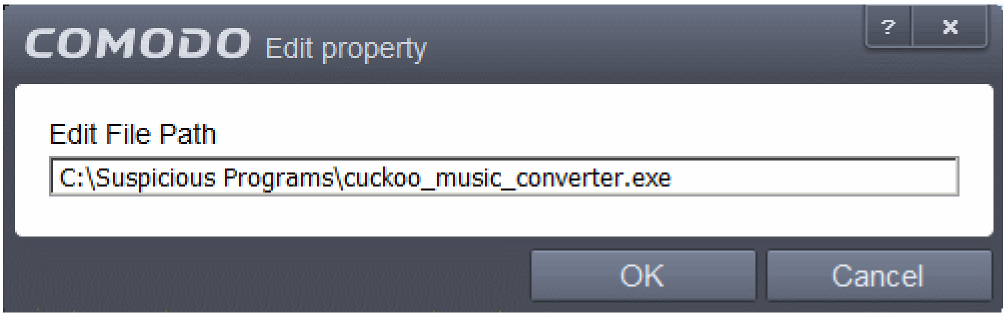
The following objects are protected on this computer.

□	Path
□	E:\Samples\Surfer\surfer.ico
□	E:\Samples\Jumper\jumper.exe
☑	E:\Samples\apt.exe

- Repeat the process to add more files.

To edit an item in the Blocked Files list

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



COMODO Edit property

Edit File Path

C:\Suspicious Programs\cuckoo_music_converter.exe

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

To release an item from Blocked Files list

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

The selected item will be removed from the Blocked Files list. CAVS will not block the application or file from execution or opening then onwards.

To permanently delete a blocked file from your system

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

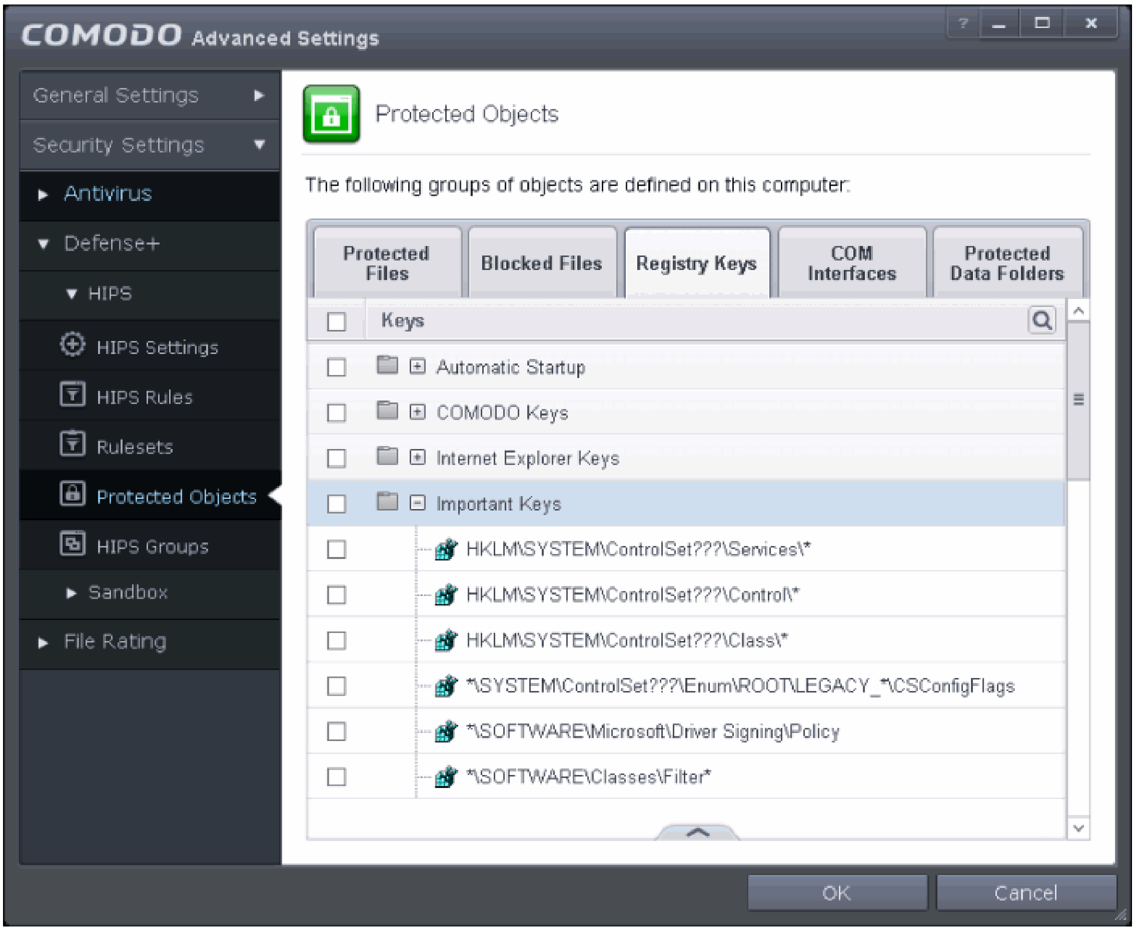
The selected item will be deleted from your server immediately.

Warning: Deleting a file from from the Blocked Files interface permanently deletes the file from your server, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

5.2.2.4.3. Protected Registry Keys

The 'Registry Protection' panel allows you to protect system critical registry keys against modification. Irreversible damage can be caused to your server if important registry keys are corrupted or modified in any way. It is essential that your registry keys are protected against any type of attack.

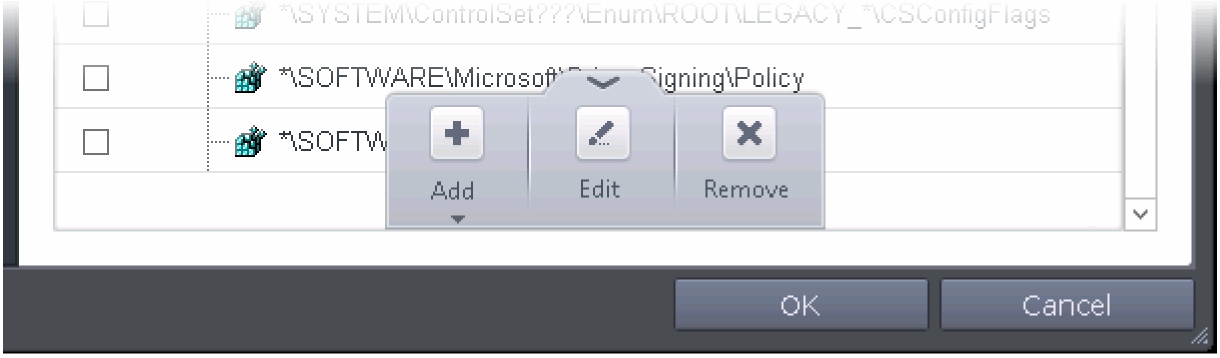
Click the 'Registry Keys' tab in the Protected Objects interface.



The following groups of objects are defined on this computer:

- □ Automatic Startup
- □ COMODO Keys
- □ Internet Explorer Keys
- □ Important Keys
  - □ HKLM\SYSTEM\ControlSet???\Services*
  - □ HKLM\SYSTEM\ControlSet???\Control*
  - □ HKLM\SYSTEM\ControlSet???\Class*
  - □ *\SYSTEM\ControlSet???\Enum\ROOT\LEGACY_*\CSConfigFlags
  - □ *\SOFTWARE\Microsoft\Driver Signing\Policy
  - □ *\SOFTWARE\Classes\Filter*

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

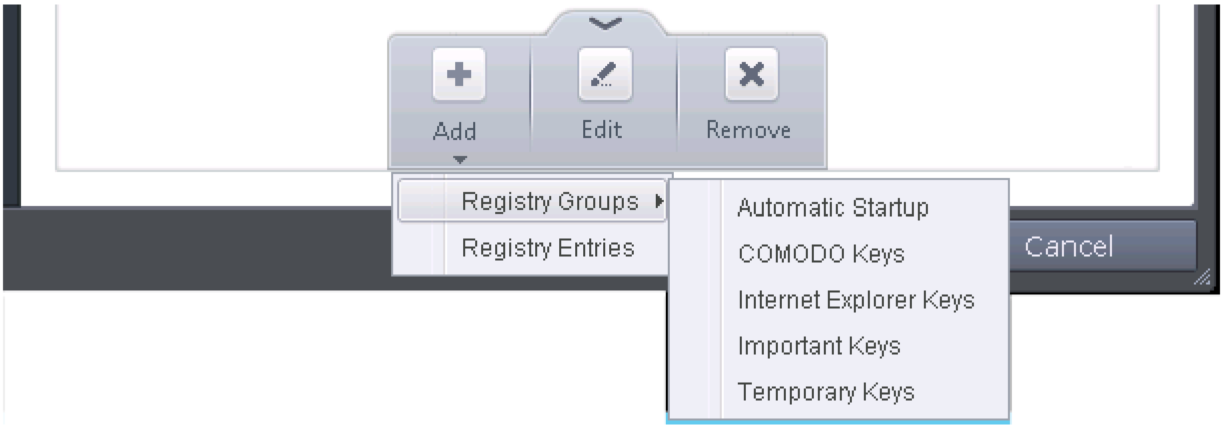

*\SYSTEM\ControlSet???\Enum\ROOT\LEGACY_*\CSConfigFlags
*\SOFTWARE\Microsoft\Driver Signing\Policy
*\SOFTW
Add
Edit
Remove
OK
Cancel

- **Add** - Allows you to add Registry groups or individual registry keys/entries to Registry Protection list.

- **Edit** - Allows you to edit the path of the Registry group or individual registry keys/entries of the selected item in the Registry Protection interface.
- **Remove** - Deletes the currently highlighted Registry group or individual registry key from the Registry Protection list.

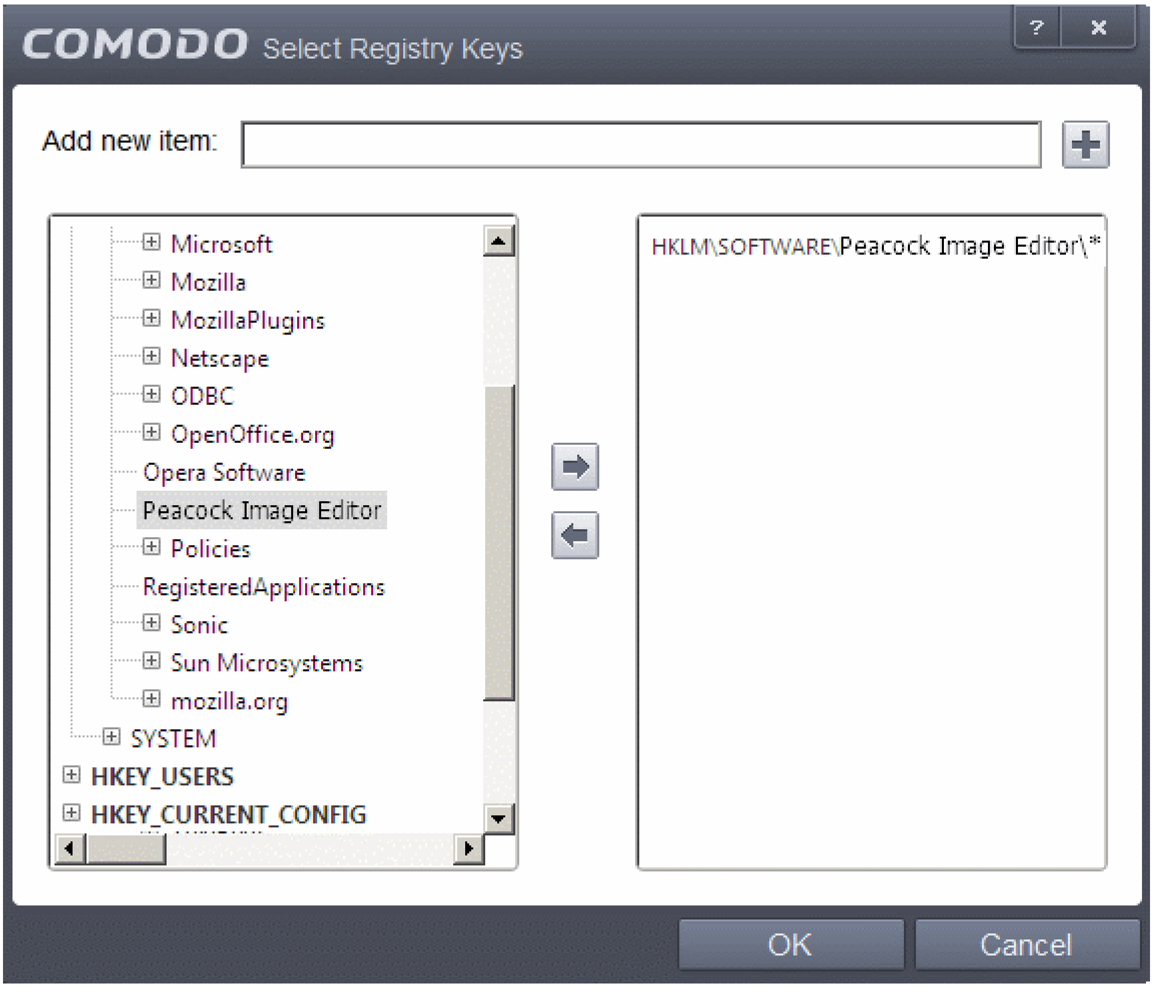
To manually add an individual Registry key or Registry Group

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



You can add the items by following methods:

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

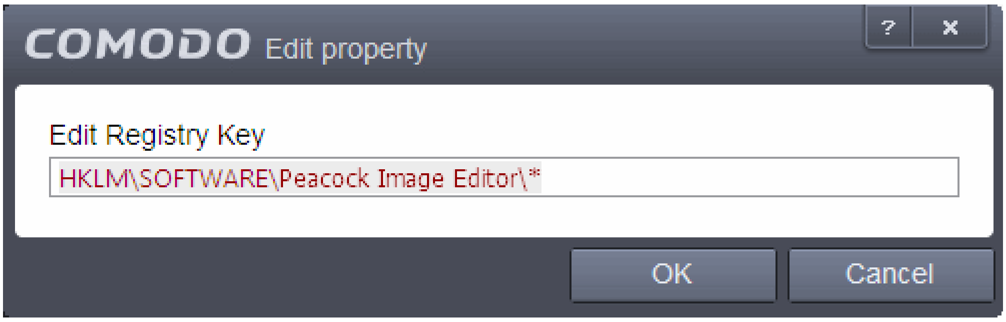


HKLM\SOFTWARE\Peacock Image Editor*

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

To edit an item in the Registry Protection list

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



Edit Registry Key

HKLM\SOFTWARE\Peacock Image Editor*

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

Note: The Registry Groups cannot be edited from this interface. You can edit Registry Groups from the Manage Registry Groups interface. Refer to the section **Registry Groups** for more details.

To delete an item from Registry Protection list

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

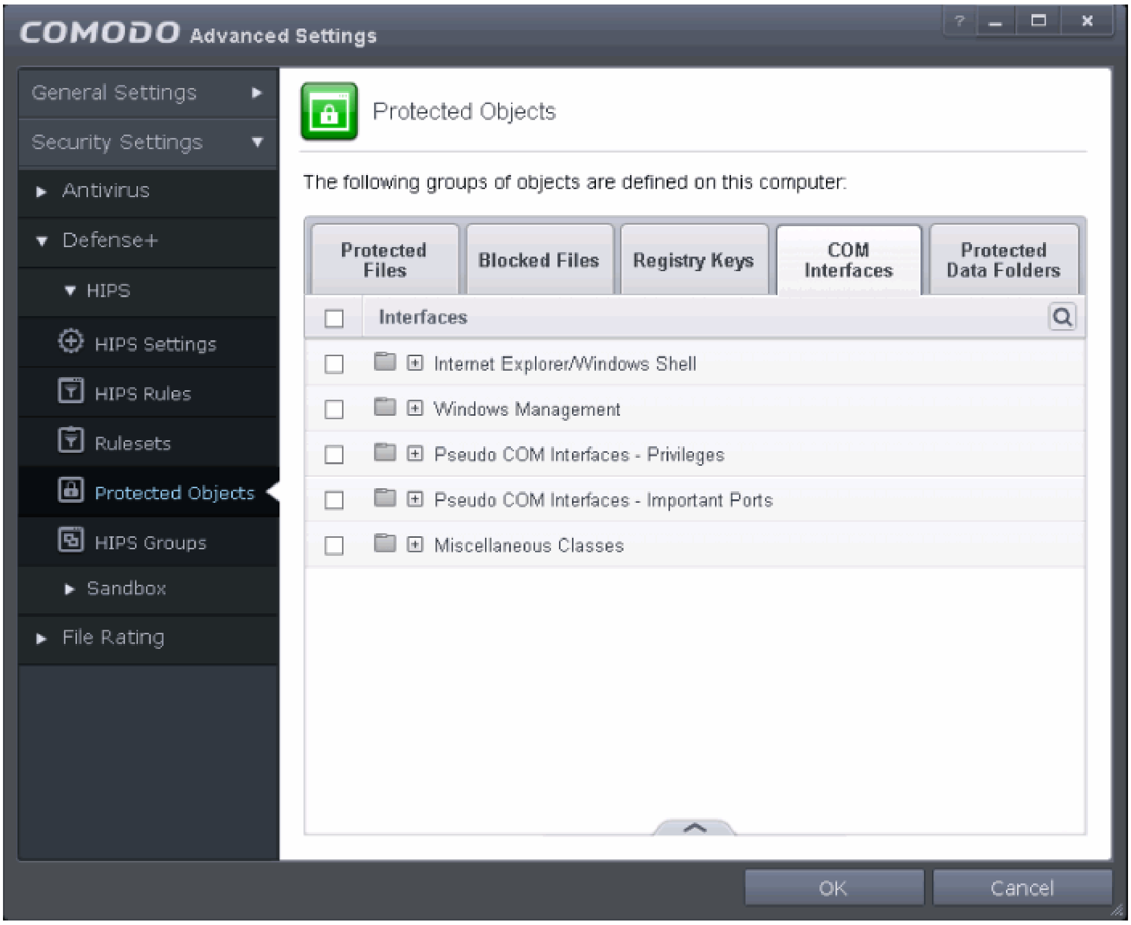
The selected item will be deleted from the Registry Protection list. CAVS will not generate alerts, if the key or the group is modified by other programs.

5.2.2.4.4. Protected COM interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on your server. 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.

CAVS automatically protects COM interfaces against against modification, corruption and manipulation by malicious processes. The predefined **COM Interface groups** can be accessed by clicking the 'Groups...' button.

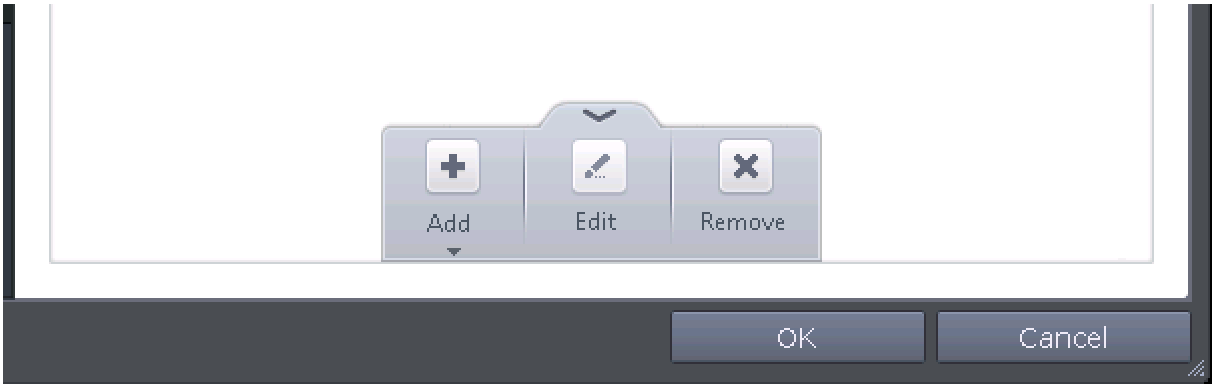
The 'COM Interface' allows you to view the list of predefined **COM Interface groups** protected by CAVS, edit them and to add new COM interface components to the list. This interface can be accessed by clicking the 'COM Interfaces' tab in the Protected Objects interface.



The following groups of objects are defined on this computer:

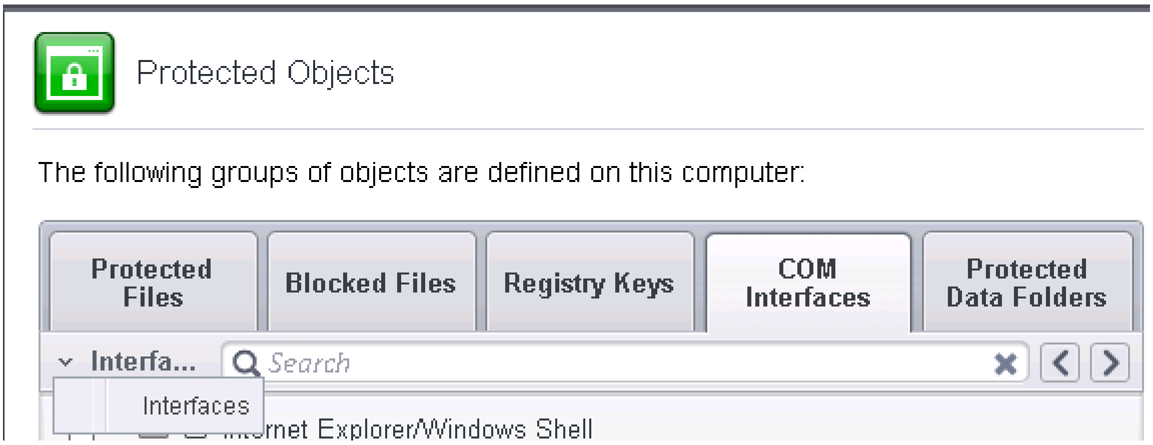
□	Interfaces
□	Internet Explorer/Windows Shell
□	Windows Management
□	Pseudo COM Interfaces - Privileges
□	Pseudo COM Interfaces - Important Ports
□	Miscellaneous Classes

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



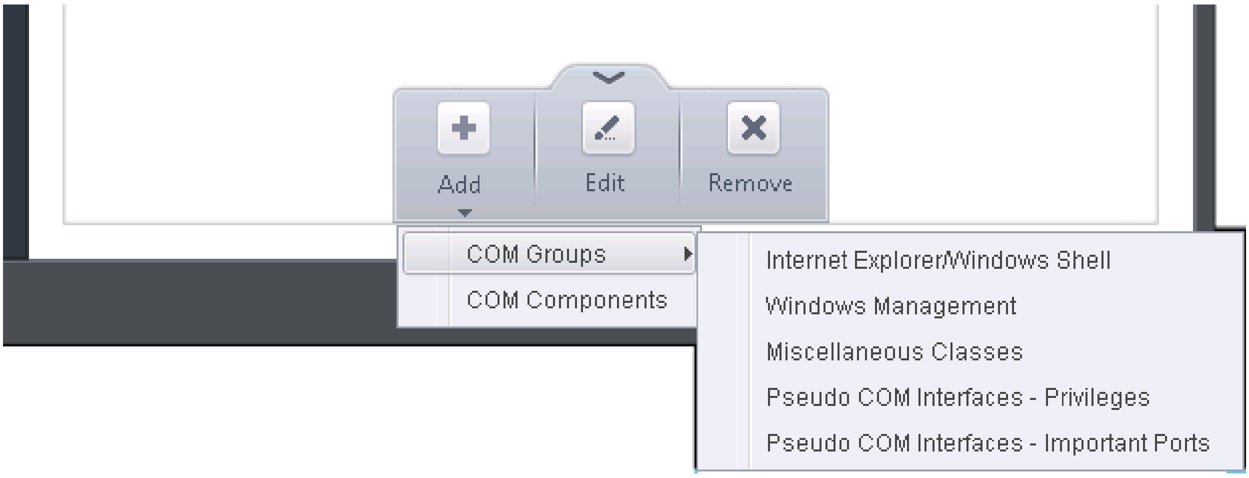
- **Add** - Allows you to add COM groups or individual COM components to COM Protection list.
- **Edit** - Allows you to edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.

You can search for a specific COM interface from the list by clicking the search icon at the far right in the column header and entering the name of the COM interface in full or part. You can navigate through the successive results by clicking the left and right arrows.



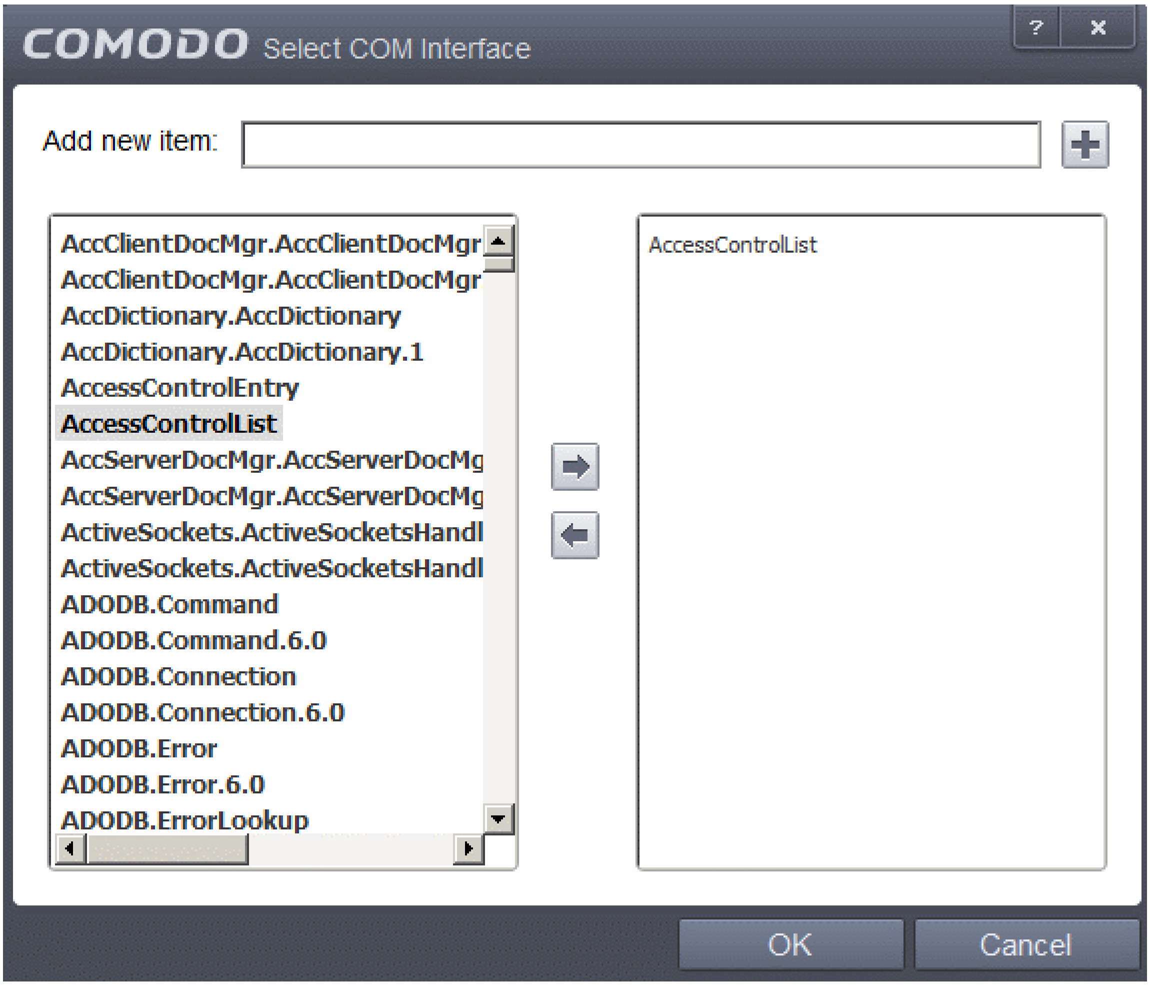
To manually add a COM Group or individual COM component

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


Add
Edit
Remove
COM Groups
COM Components
Internet Explorer/Windows Shell
Windows Management
Miscellaneous Classes
Pseudo COM Interfaces - Privileges
Pseudo COM Interfaces - Important Ports

You can add the items by following methods:

- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section **COM Groups**.
- **Adding COM Components** - Selecting 'COM components' opens the 'Select COM Interfaces' dialog.

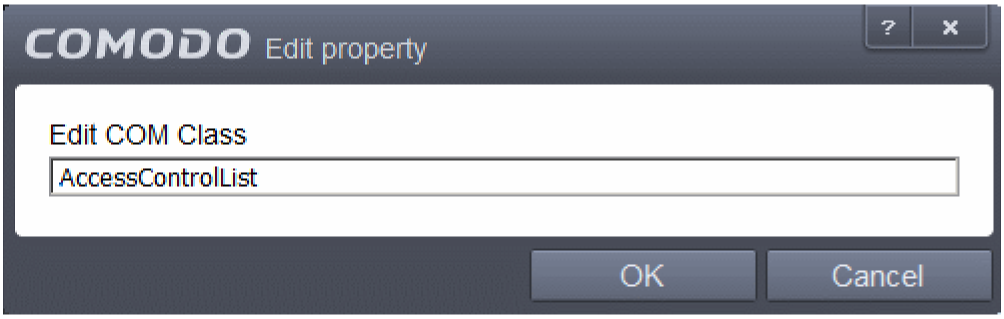


COMODO Select COM Interface
?
×
Add new item:
+
AccClientDocMgr.AccClientDocMgr
AccClientDocMgr.AccClientDocMgr
AccDictionary.AccDictionary
AccDictionary.AccDictionary.1
AccessControlEntry
AccessControlList
AccServerDocMgr.AccServerDocMg
AccServerDocMgr.AccServerDocMg
ActiveSockets.ActiveSocketsHandl
ActiveSockets.ActiveSocketsHandl
ADODB.Command
ADODB.Command.6.0
ADODB.Connection
ADODB.Connection.6.0
ADODB.Error
ADODB.Error.6.0
ADODB.ErrorLookup
AccessControlList
OK
Cancel

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

To edit an item in the COM Protection

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



Edit COM Class: AccessControlList

- Edit the COM Class and click OK

Note: The COM Groups cannot be edited from this interface. You can edit COM Groups from the Manage COM Groups interface. Refer to the section **COM Groups** for more details.

To delete an item from COM Protection list

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

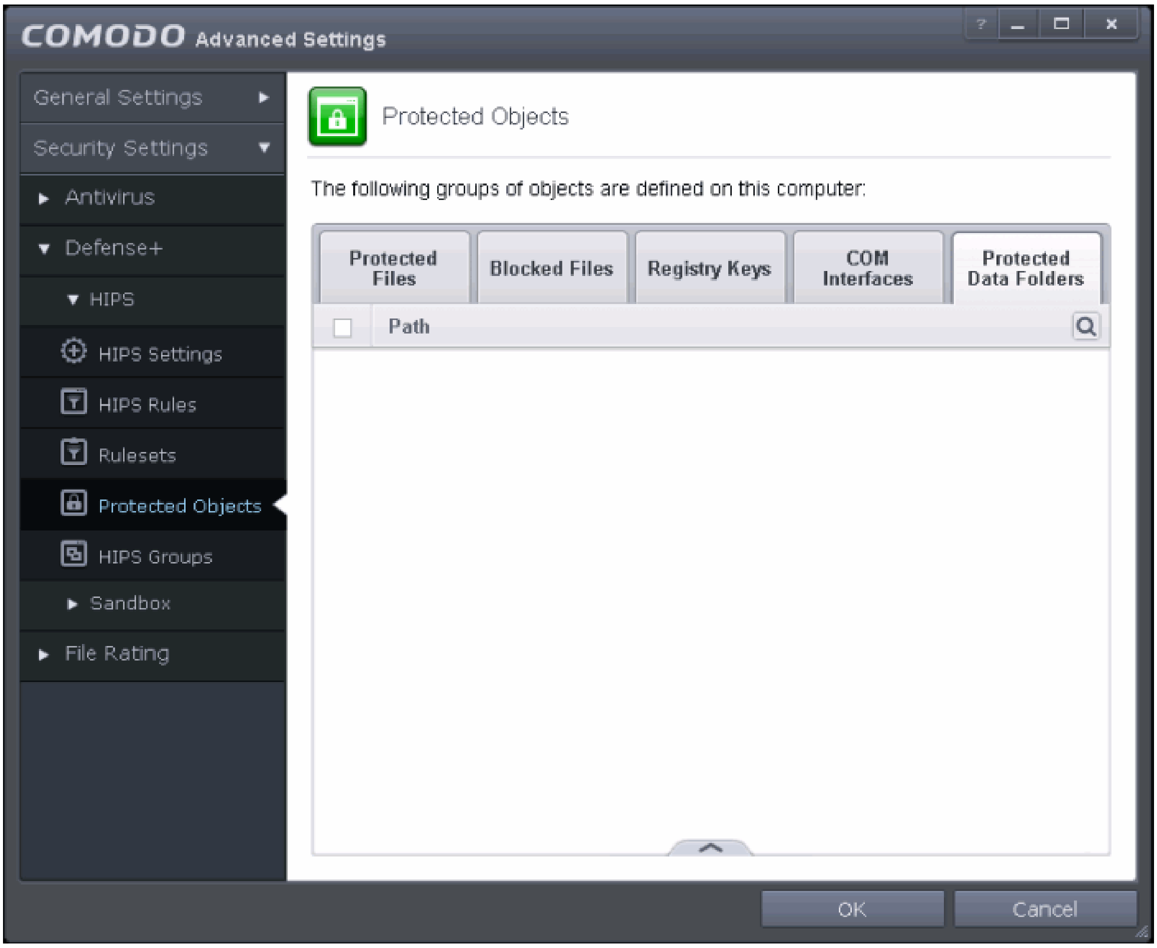
The selected item will be deleted from the COM Protection list. CAVS will not generate alerts, if the COM component or the group is modified by other programs or processes.

5.2.2.5. Protected Data Folders

The data files in the folders listed under the Protected Data Folders area cannot be seen, accessed or modified by any known or unknown application that is running inside the sandbox.

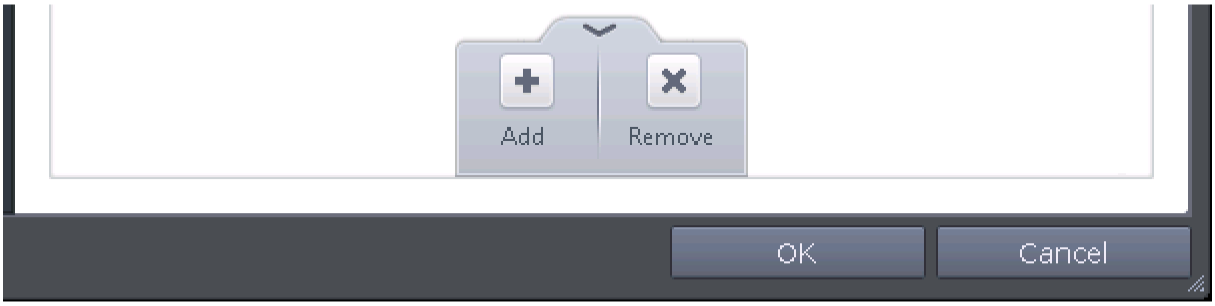
Tip: Files and folders that are added to '**Protected Files**' interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to sandboxed programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all the sandboxed programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

To open the Protected Data Folders interface, Click the 'Protected Data Folders' tab in the Protected Objects interface:



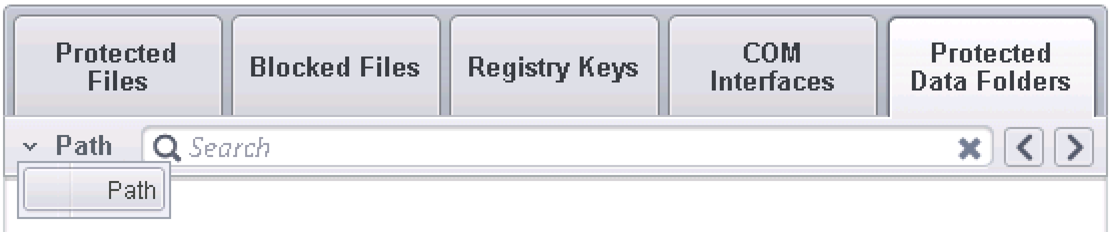
The following groups of objects are defined on this computer:

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



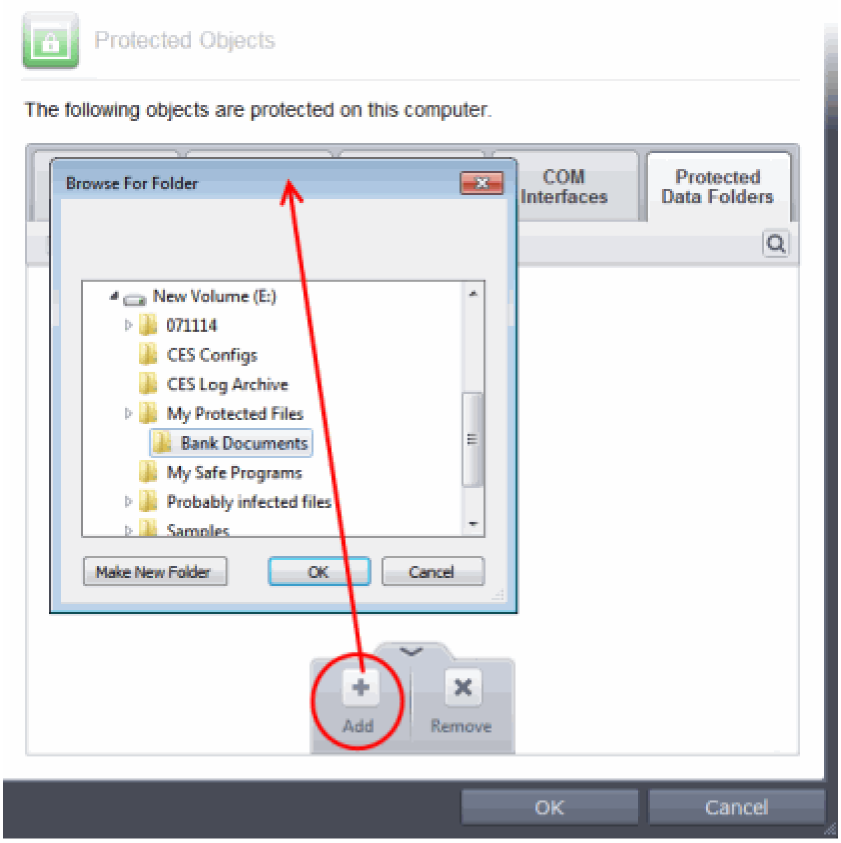
- **Add** - Allows you to add folders to Protected Data Folders list.
- **Remove** - Deletes the currently selected folder.

You can use the search option to find a specific folder by clicking the search icon 🔍 at the far right of the column header. You can search by entering the folder name in full or part.

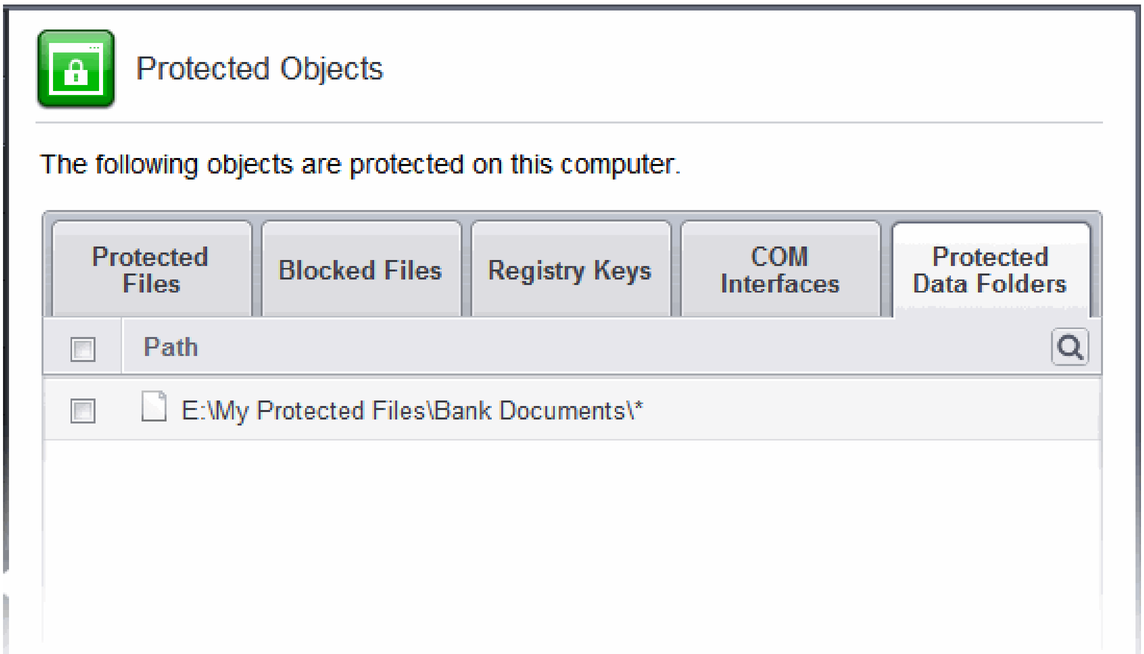


To add a folder to be protected

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



- Navigate to the folder to be added and click OK.



Protected Objects

The following objects are protected on this computer.

□ E:\My Protected Files\Bank Documents*

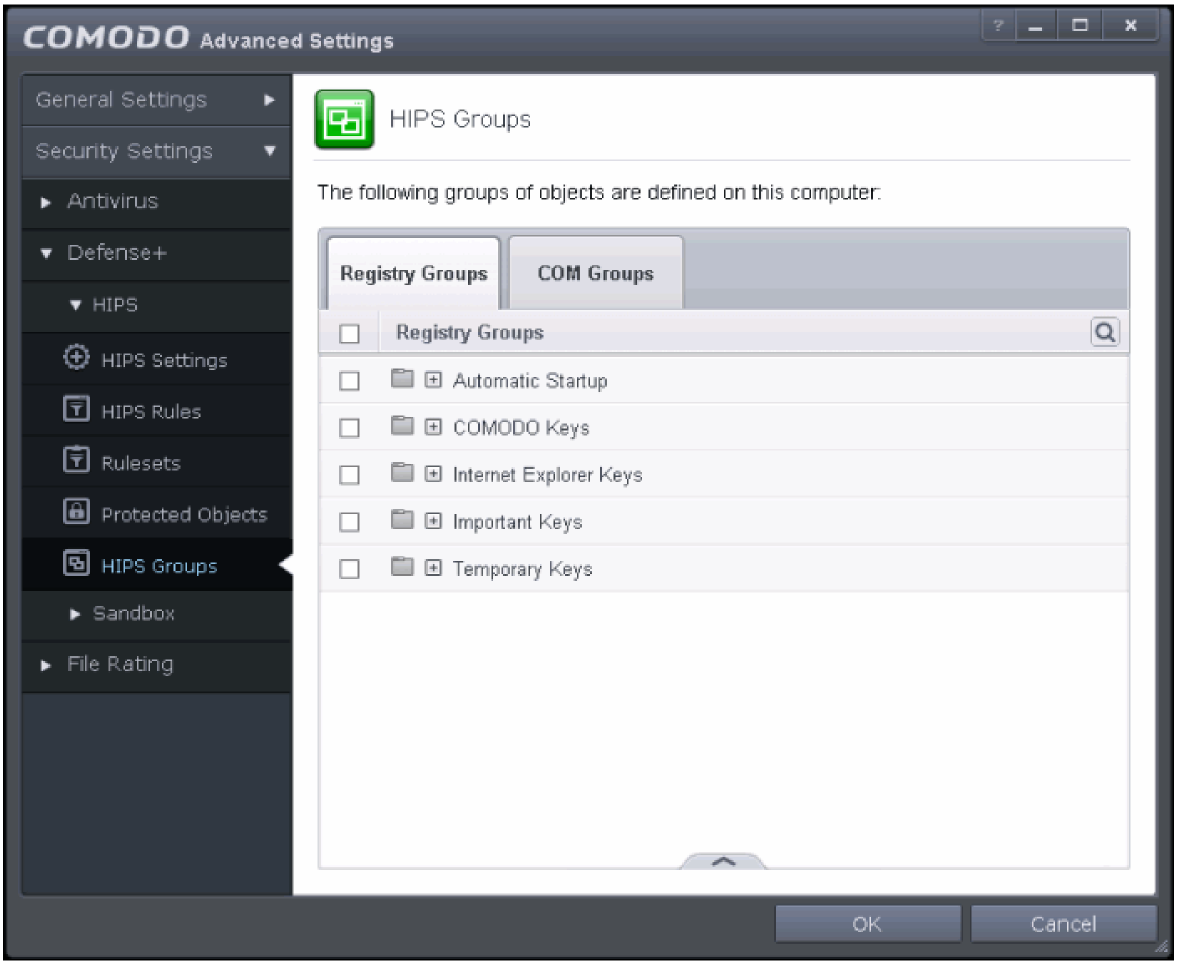
To remove an item from Protected Data Folders list

- Select the folder from the list, click the handle from the bottom and choose 'Remove'.
- The selected folder will be removed from the protected folders list. CAVS will not generate alerts, if the folder is subjected to unauthorized access.

5.2.2.6. HIPS Groups

The HIPS Groups panel allows you to add, edit or remove predefined Registry and COM Groups. CAVS ships with some important predefined Registry and COM Groups and this interface allows you to add new groups. Once added, these newly added groups are also available for including in the **Registry Keys** and **COM Interfaces** for protection.

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



The panel has two tabs:

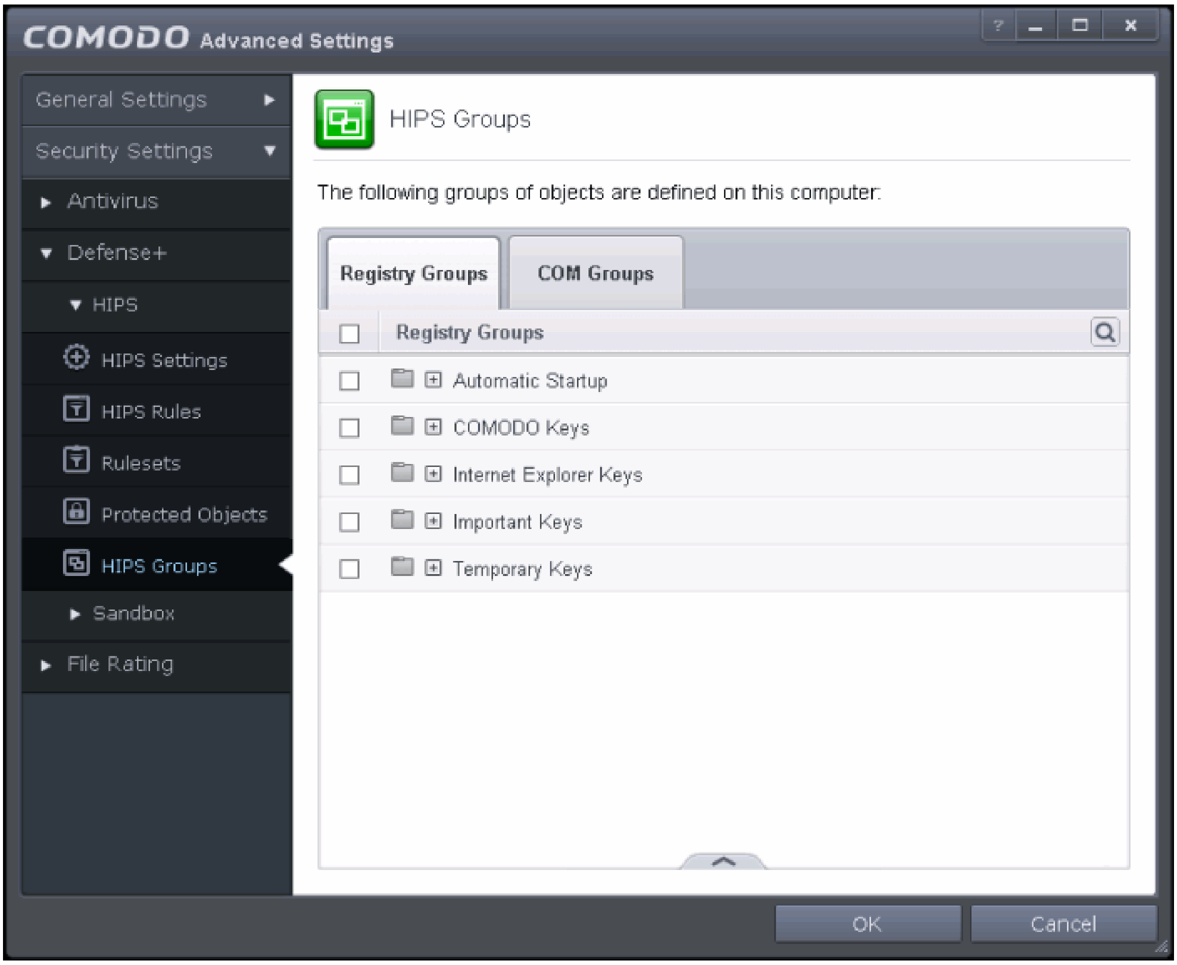
- **Registry Groups** - Allows you to create new groups and add registry keys to groups that are to be protected from changes
- **COM Groups** - Allows you to create new COM groups and add COM classes to groups that are to be protected from changes

5.2.2.6.1. Registry Groups

Registry groups are predefined batches of one or more registry keys. Creating a registry group allows you to quickly add it to Registry Protection list.

To open the Registry Groups interface

- In the Advanced Settings screen, click Security Settings > Defense+ > HIPS > HIPS Groups and select the Registry Groups tab.



The following groups of objects are defined on this computer:

	Registry Groups
□	Automatic Startup
□	COMODO Keys
□	Internet Explorer Keys
□	Important Keys
□	Temporary Keys

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

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

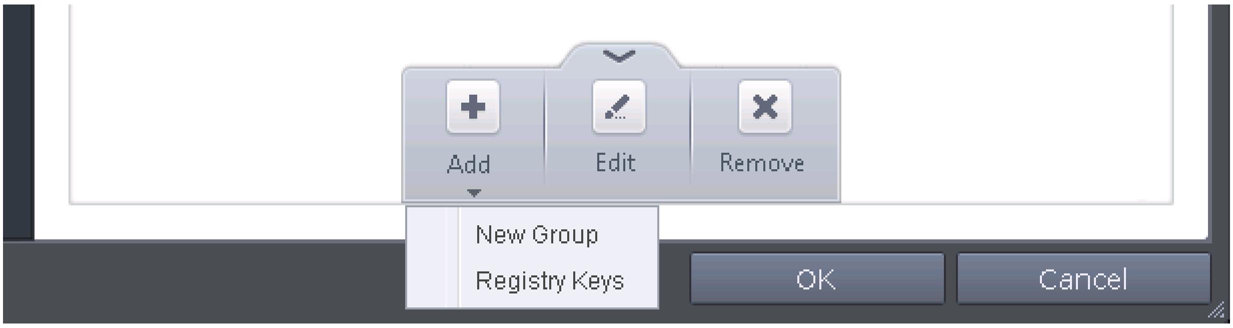
Click the chevron on the left side of the column header and select the search criteria from the drop-down.

- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

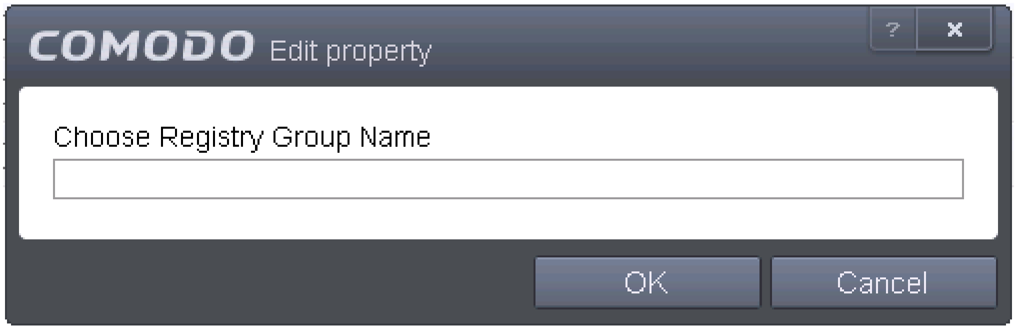
This interface allows you to

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

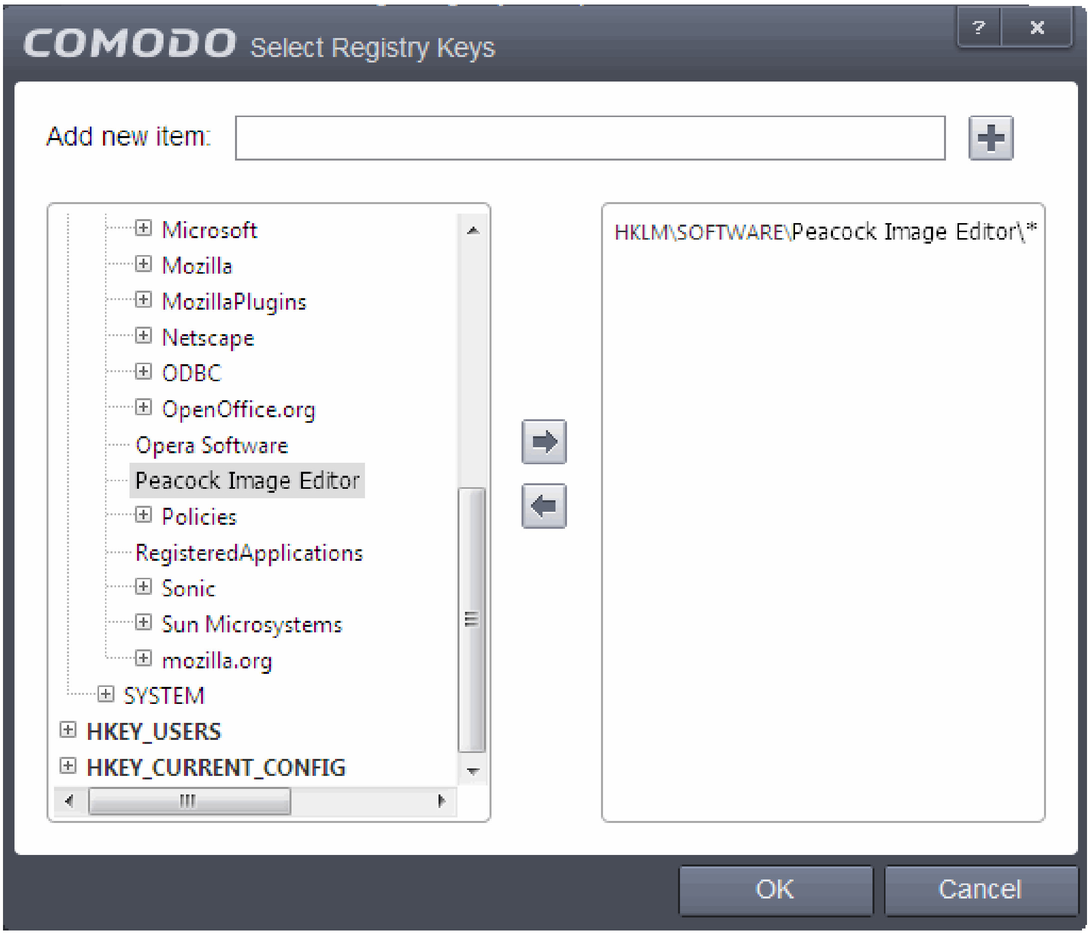
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click 'OK'



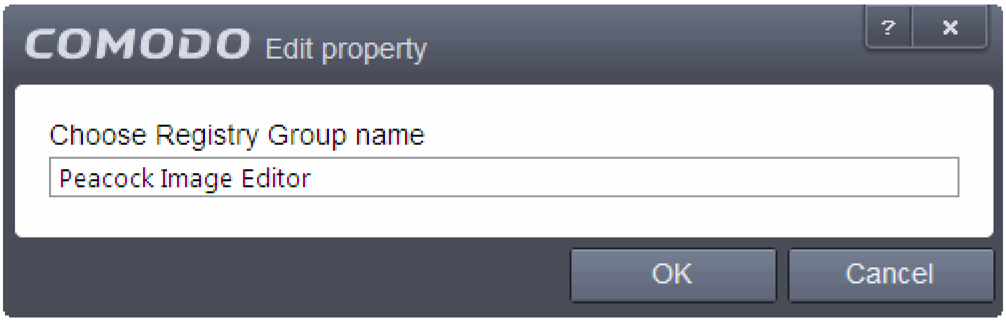
- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



HKLM\SOFTWARE\Peacock Image Editor*

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

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



Choose Registry Group name

Peacock Image Editor

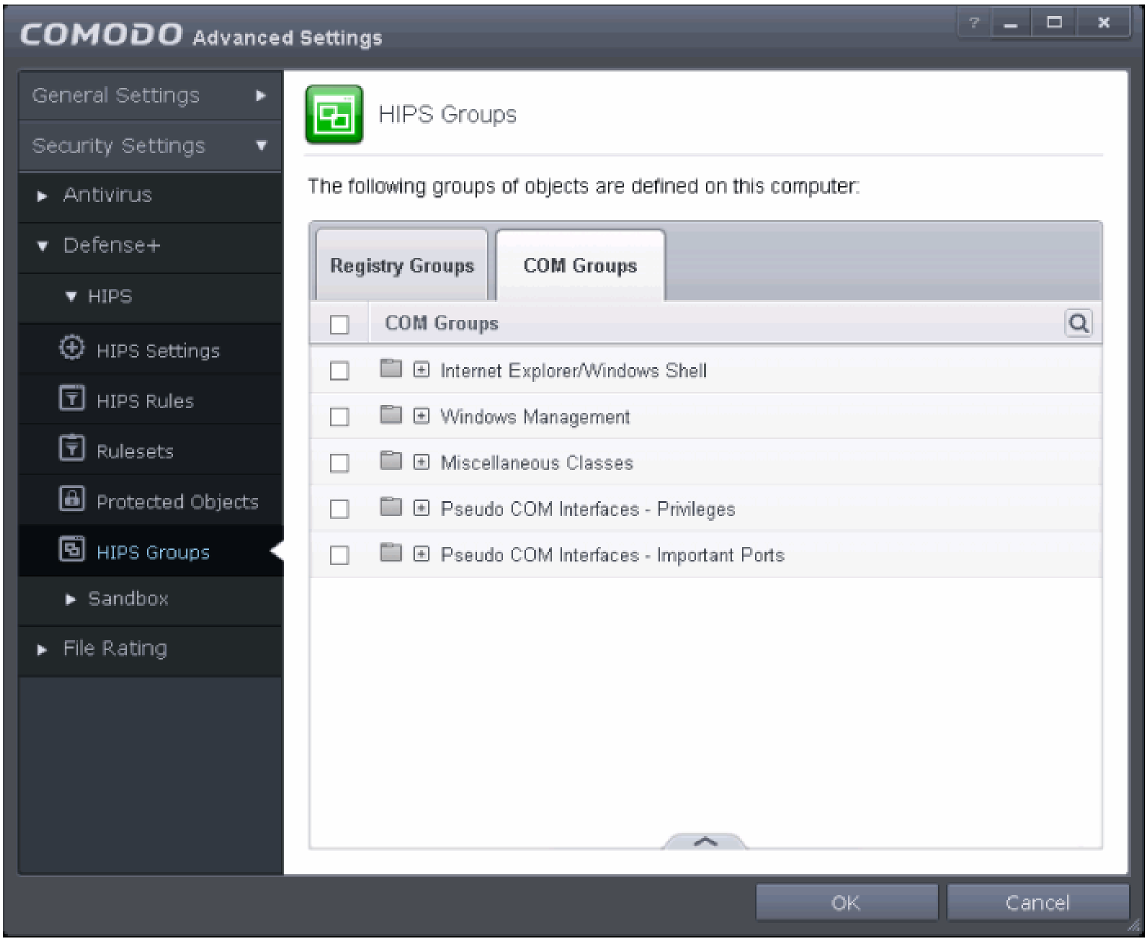
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

5.2.2.6.2. COM Groups

COM groups are handy, predefined groupings of COM interfaces. Creating a COM group allows you to quickly add it to COM Protection list.

To open the COM Groups interface

- In the Advanced Settings screen, click Security Settings > Defense+ > HIPS > HIPS Groups and select the COM Groups tab.



The following groups of objects are defined on this computer:

□ COM Groups
□ Internet Explorer/Windows Shell
□ Windows Management
□ Miscellaneous Classes
□ Pseudo COM Interfaces - Privileges
□ Pseudo COM Interfaces - Important Ports

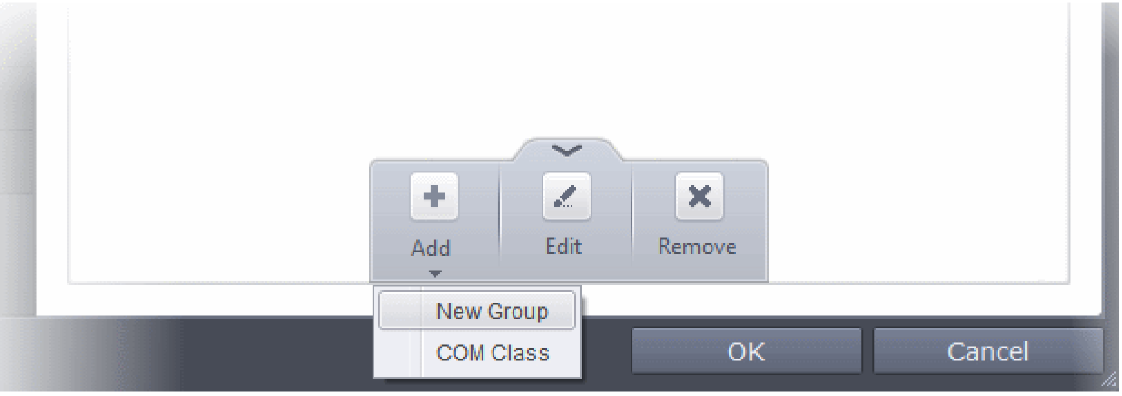
To use the search option, click the search icon at the far right in the column header.

- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.

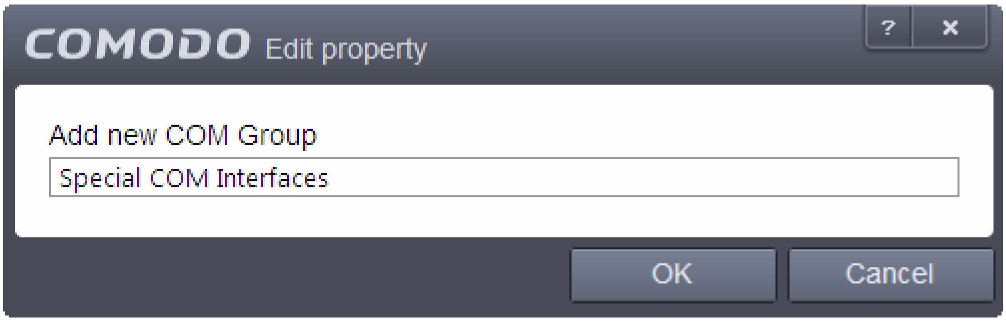
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

This interface allows you to:

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



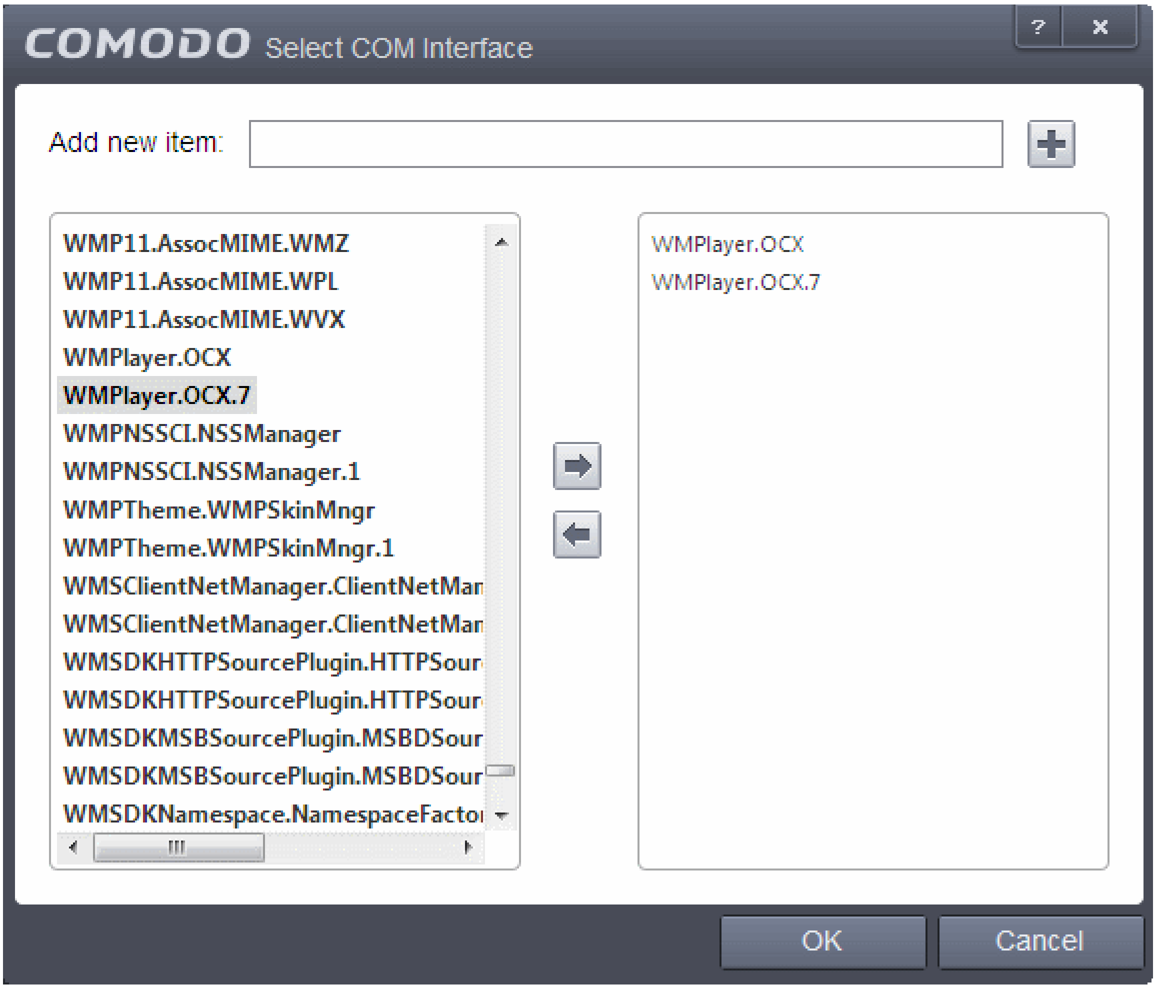
- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK.



Add new COM Group

Special COM Interfaces

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

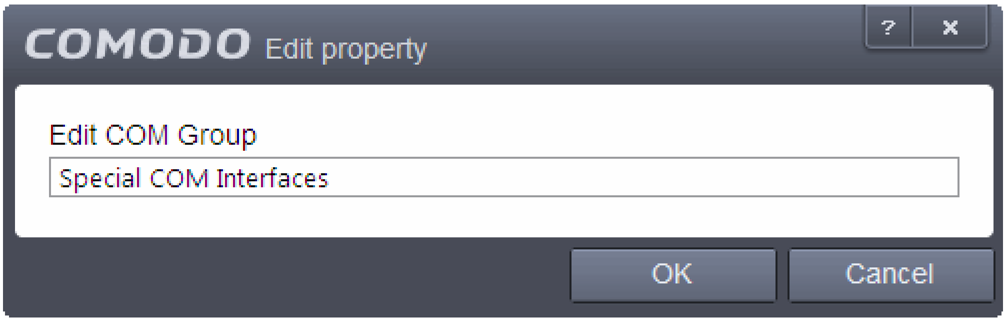


WMP11.AssocMIME.WMZ
WMP11.AssocMIME.WPL
WMP11.AssocMIME.WVX
WMPlayer.OCX
WMPlayer.OCX.7
WMPNSSCI.NSSManager
WMPNSSCI.NSSManager.1
WMPTheme.WMPSkinMngr
WMPTheme.WMPSkinMngr.1
WMSClientNetManager.ClientNetMan
WMSClientNetManager.ClientNetMan
WMSDKHTTPSourcePlugin.HTTPSour
WMSDKHTTPSourcePlugin.HTTPSour
WMSDKMSBSourcePlugin.MSBDSour
WMSDKMSBSourcePlugin.MSBDSour
WMSDKNamespace.NamespaceFacto

WMPlayer.OCX
WMPlayer.OCX.7

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

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



Edit COM Group
Special COM Interfaces

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

5.2.2.7. Sandbox

The Sandbox is an integral part of the Defense+ engine and is used to run potentially unsafe applications in an isolated environment to prevent damage to your system. The Defense+ engine through various analysis determines whether an application is trusted, unrecognized or malware. You can define rules how these identified applications can be run in the Sandbox, that is,

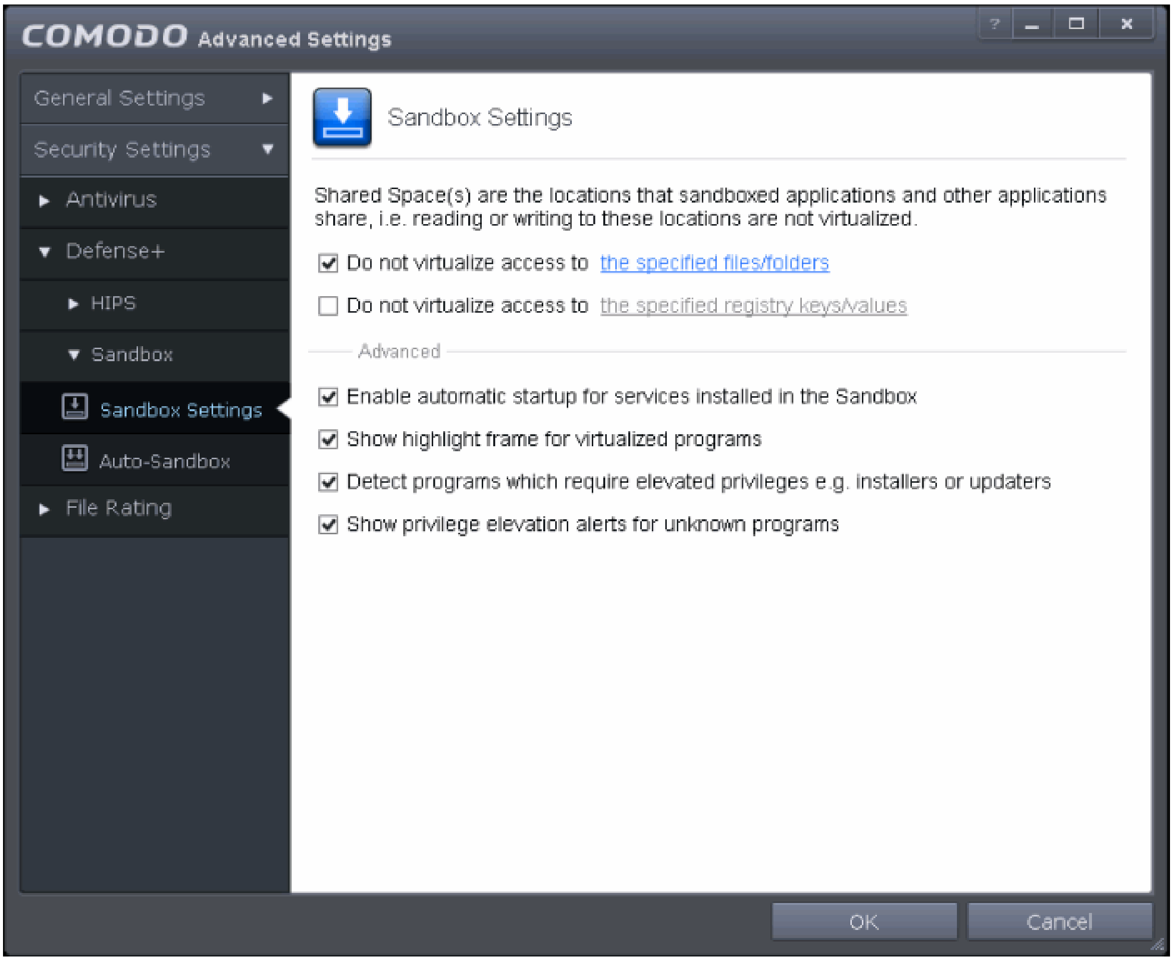
- run with restricted access to operating system resources
- run completely isolated from your operating system and files on the rest of your computer
- completely block from running
- or allow it to run outside the sandbox environment without any restriction.

For more information about defining rules, refer to the section **Configuring Rules for Auto-Sandbox**.

The Sandbox creates a new folder called Shared Space in your system by default at 'C:/Program Data/Shared Space' for sharing files between it and the real computer system. The applications running inside the sandbox will be allowed to store their data in the shared space for future sessions. This data will can also be accessed by non-sandboxed applications. The settings for accessing Shared Space, generating sandbox alerts, enabling startup services for applications installed in sandbox can be configured in Sandbox Settings screen. Refer to the section **Configuring the Sandbox** for more details.

For more information about the Sandbox environment refer to the section **The Sandbox – An Overview**.

For more information about how the Defense+ engine determines the reputation of a file, refer to the section **Unknown Files: The Scanning Processes**.



Sandbox Settings

Shared Space(s) are the locations that sandboxed applications and other applications share, i.e. reading or writing to these locations are not virtualized.

☑ Do not virtualize access to the specified files/folders

☐ Do not virtualize access to the specified registry keys/values

Advanced

☑ Enable automatic startup for services installed in the Sandbox

☑ Show highlight frame for virtualized programs

☑ Detect programs which require elevated privileges e.g. installers or updaters

☑ Show privilege elevation alerts for unknown programs

The 'Sandbox' configuration panel can be accessed by clicking 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Defense + > Sandbox'. The options 'Sandbox Settings' and 'Auto-Sandbox' under Sandbox allow you to quickly configure Sandbox settings and create rules and conditions for auto-sandboxing selected programs.

Refer to the following sections for more details:

- **The Sandbox – An Overview**
- **Unknown Files: The Scanning Processes**

- **Configuring the Sandbox Settings**
- **Configuring Rules for Auto-Sandbox**

5.2.2.7.1. The Sandbox - An Overview

Comodo Antivirus for Servers's new sandbox is an isolated operating environment for unknown and untrusted applications. Running an application in the sandbox means that it cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have integrated sand-boxing technology directly into the security architecture of Comodo Antivirus for Servers to complement and strengthen the Defense+ and Antivirus modules.

Applications in the sandbox are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of the real system. This delivers the smoothest user experience possible by allowing unknown applications to run and operate as they normally would while denying them the potential to cause lasting damage.

After an unknown application has been placed in the sandbox, CAVS also automatically queues it for submission to Comodo Cloud Scanners for automatic behavior analysis. Firstly, the files undergo another antivirus scan on our servers. If the scan discovers the file to be malicious, then it is designated as malware, the result is sent back to the local installation of CES 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 '**File List**' with 'Unrecognized' rating (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 CAVS.

By uniquely deploying 'sandboxing as security', CAVS offers improved security, fewer pop-ups and greater ease of use than ever before.

5.2.2.7.2. Unknown Files: The Scanning Processes

- When an executable is first run it passes through the following CAVS security inspections:
  - Antivirus scan
  - HIPS Heuristic check
  - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CAVS (and therefore not scanned in the cloud) in the following ways:
  - Because it is on the local Comodo White List of known safe applications
  - Because the user has rated the file as 'Trusted' in the **File List**
  - By the user granting the installer elevated privileges (CAVS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CAVS regards the installer and all files generated by the installer as safe)
  - Additionally, a file is not sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS Ruleset (See **Active HIPS Rules** for more details)

Cloud Scanning

Files and processes that pass the security inspections above but are not yet recognized as 'safe' (white-listed) are 'Unrecognized' files. In order to try to establish whether a file is safe or not, CAVS will first consult Comodo's File Look-Up Server (FLS) to check the very latest signature databases:

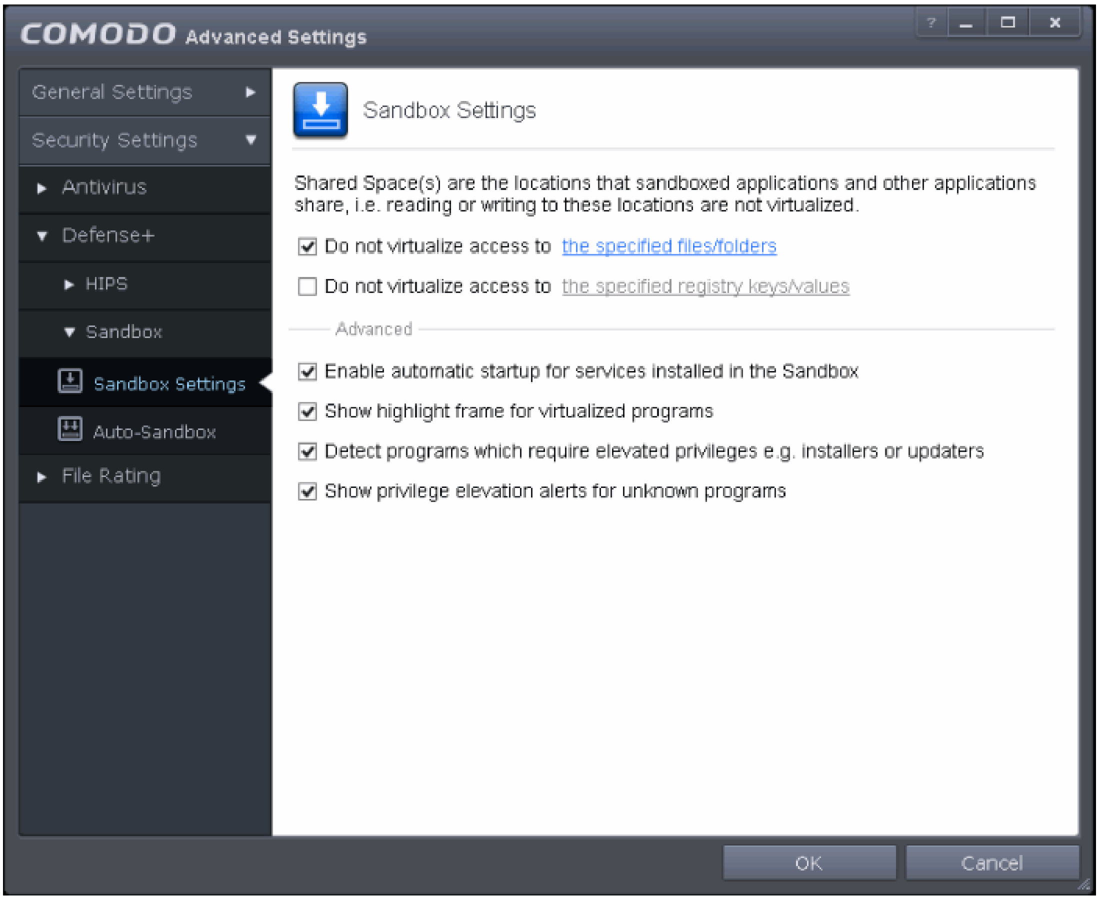
- A digital hash of the unrecognized process or file is created.
- These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all known malware and a white list of the signatures 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 CAVS
- 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 CAVS
  - The local white-list is updated
- The FLS checks detailed above are near instantaneous.
- If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'.
- Unrecognized files are simultaneously uploaded to Comodo's Instant Malware Analysis servers for further checks:
- Firstly, the files undergo another antivirus scan on our servers.
  - If the scan discovers the file to be malicious (for example, heuristics discover it is a brand new variant) then it is designated as malware. This result is sent back to the local installation of CAVS and the local and global black-list is updated.
  - If the scan does not detect that the file is malicious then it passes onto the next stage of inspection - behavior monitoring.
  - The behavior analysis system is a cloud based service that is used to help determine whether a file exhibits malicious behavior. Once submitted to the system, the unknown executable will be automatically run in a virtual environment and all actions that it takes will be monitored. For example, processes spawned, files and registry key modifications, host state changes and network activity will be recorded.
  - If these behaviors are found to be malicious then the signature of the executable is automatically added to the antivirus black list.
  - If no malicious behavior is recorded then the file is rated as 'Unrecognized' 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 CAVS installation in approximately 15 minutes. It will simultaneously be added to the '**File List**' as 'Unrecognized' and uploaded to our technicians for analysis. If is discovered to be a threat then CAVS 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 CAVS users.

5.2.2.8. Configuring the Sandbox

The 'Sandbox Settings' section of 'Advanced Settings' allows you to configure the Sandbox settings that determine how proactive the Sandbox should be and which types of files it should check.

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



Sandbox Settings

Shared Space(s) are the locations that sandboxed applications and other applications share, i.e. reading or writing to these locations are not virtualized.

☑ Do not virtualize access to the specified files/folders

☐ Do not virtualize access to the specified registry keys/values

Advanced

☑ Enable automatic startup for services installed in the Sandbox

☑ Show highlight frame for virtualized programs

☑ Detect programs which require elevated privileges e.g. installers or updaters

☑ Show privilege elevation alerts for unknown programs

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

- Shared Space Settings - Files downloaded or generated by sandboxed applications that you wish to be able to access from your real system should be downloaded to the shared space
- Advanced Settings – Allows you to configure Sandbox alert settings as well as to enable automatic startup services for programs installed in the Sandbox.

Shared Space Settings:

'Shared Space' is a dedicated area on your local drive that sandboxed applications are permitted to write to and which can also be accessed by non-sandboxed applications (hence the term 'Shared Space'). For example, any files or programs you download via a sandboxed browser that you wish to be able to access from your real system should be downloaded to the shared space. This is located by default at 'C:/Program Data/Shared Space'.

You can access the shared space folder in the following ways:

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

- **Do not virtualize access to the specified files/folders**
- **Do not virtualize access to the specified registry keys/values**

To define exceptions for files and folders

- Enable the 'Do not virtualize access to the specified files/folders' check-box then click on the words the specified files/folders. The 'Manage Exclusions' dialog will appear.
  - Click the handle at the bottom to open the tools menu then click 'Add.

  i. **Files** - Allows you to specify files or applications that sandboxed applications are able to access

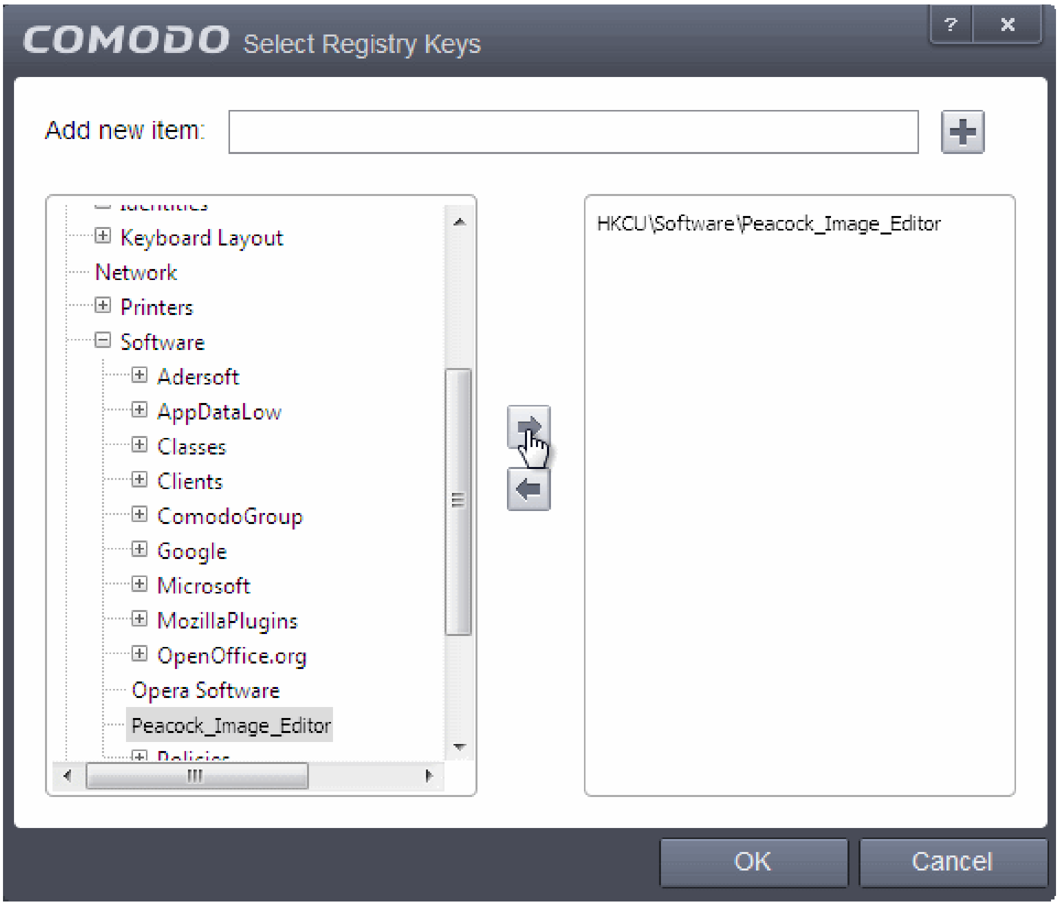
  ii. **Folders** - Specify a folder that can be accessed by sandboxed applications

  iii. **File Groups** - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exception for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl. For more details on file groups, refer to the section **File Groups**.

  iv. **Running Processes** - Allows you to add a program that sandboxed applications are able to access
- To edit an exception, select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Change file or folder location path and click 'OK'
- Click 'OK' to implement your settings
- To manage available file groups, click the 'Groups' button from the tools menu. The 'Manage File Groups' dialog allows you to view, add and edit file groups. Please refer to **File Groups** if you need more information with this area.

To define exceptions for specific Registry keys and values

- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the words the specified registry keys/values. The 'Manage Exclusions' dialog will appear.
  - Click the handle at the bottom to open the tools menu then click 'Add'.
  - **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exceptions. For an explanation of CAVS registry groups, refer to the section **Registry Groups**.
  - **Registry Entries** - Opens an interface that allows you to quickly browse Windows registry keys and add them as exceptions:

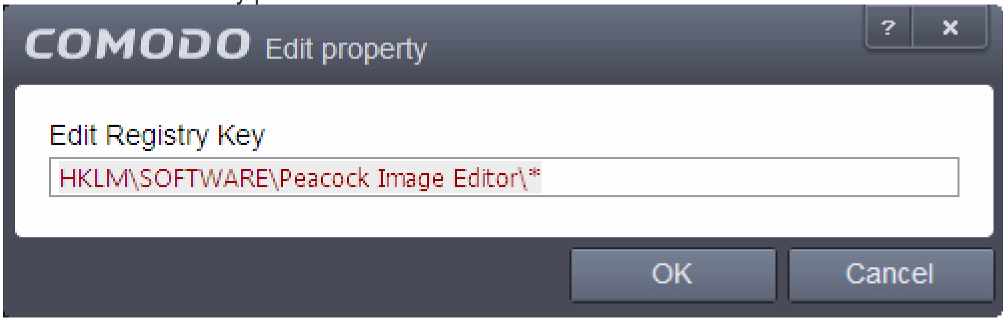


HKCU\Software\Peacock_Image_Editor

- Click 'OK' to implement your settings.

- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.

- Edit the key path and click OK.



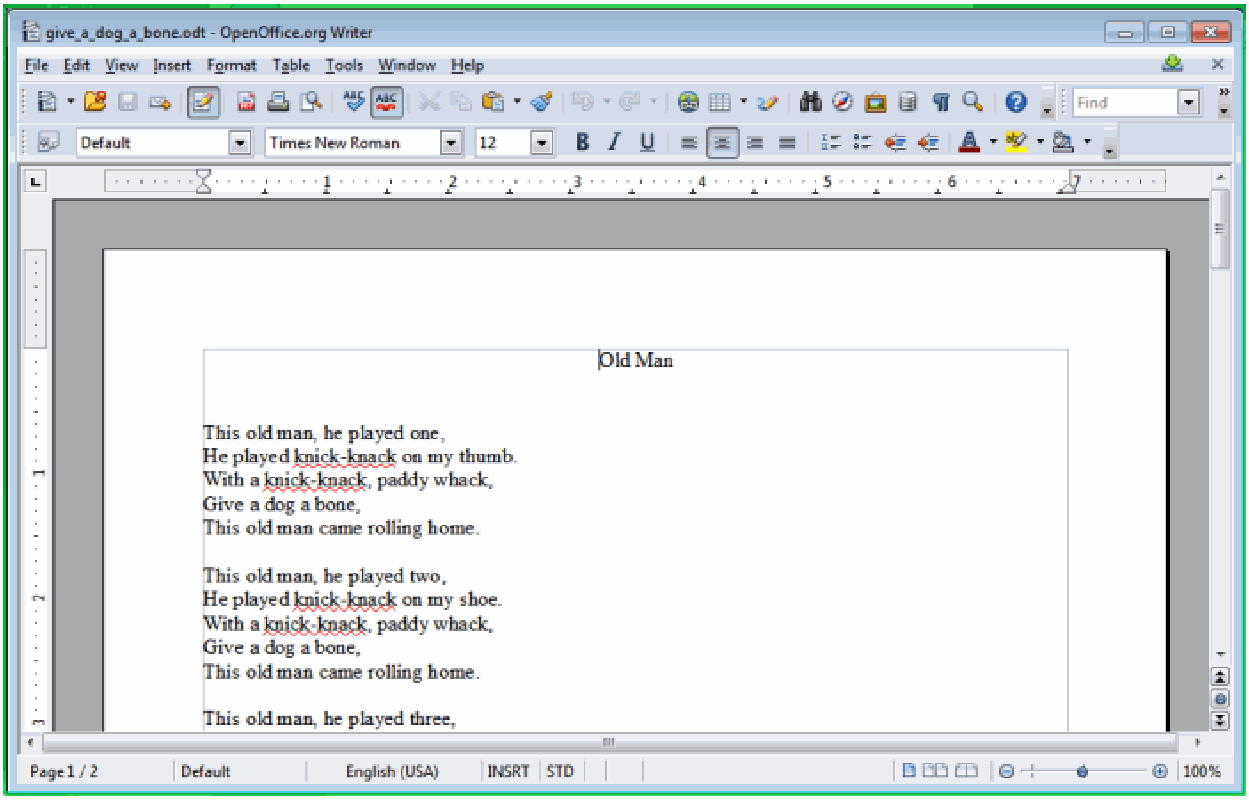
Edit Registry Key

HKLM\SOFTWARE\Peacock Image Editor*

Advanced Settings:

- **Enable automatic startup for services installed in the sandbox** - By default, CAVS does not permit sandboxed services to run at Windows startup. Select this check-box to allow them to do so. (***Default = Enabled***)
- **Show highlight frame for virtualized programs** - If enabled, CAVS displays a green border around the windows of programs that are running inside the sandbox. (***Default = Enabled***)

The following example shows an .odt document opened with a sandboxed version OpenOffice Writer:


give_a_dog_a_bone.odt - OpenOffice.org Writer
File Edit View Insert Format Table Tools Window Help
Default
Times New Roman
12
Find
Page 1 / 2
Default
English (USA)
INSRT
STD
100%

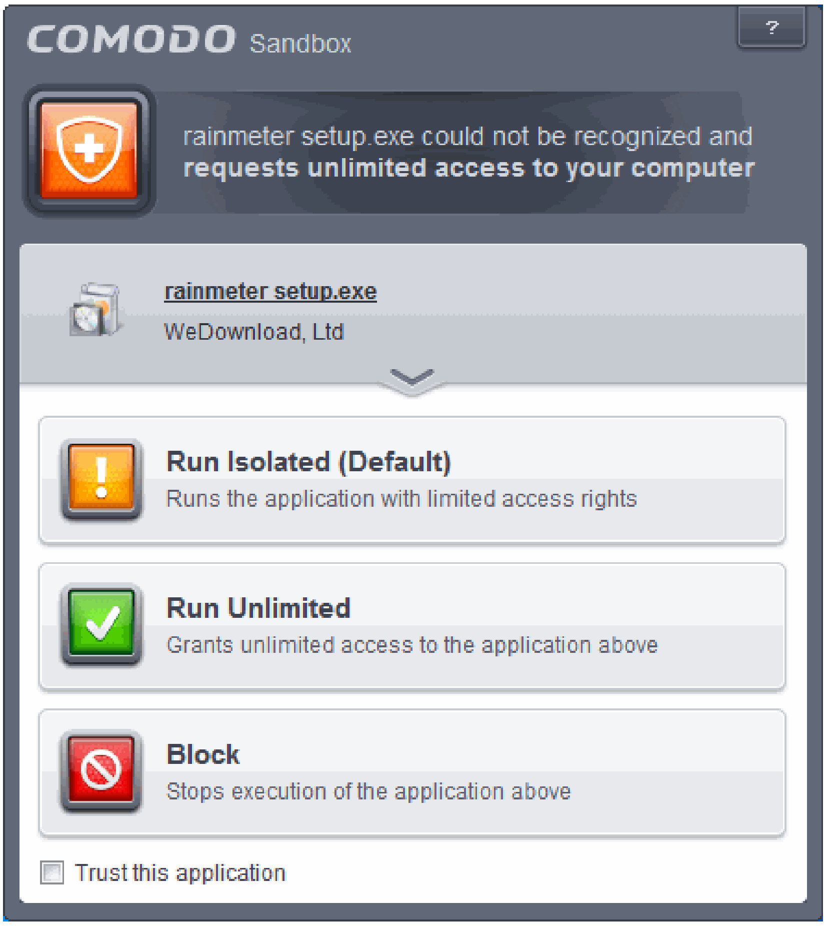
Old Man

This old man, he played one,
He played knick-knack on my thumb.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played two,
He played knick-knack on my shoe.
With a knick-knack, paddy whack,
Give a dog a bone,
This old man came rolling home.

This old man, he played three,

- **Detect programs which require elevated privileges:** Allows you to instruct the Sandbox to display alerts when an installer or updater requires administrator or elevated privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry. Refer to the section **Understanding Security Alerts** for more details.



COMODO Sandbox

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

rainmeter setup.exe
WeDownload, Ltd

Run Isolated (Default)
Runs the application with limited access rights

Run Unlimited
Grants unlimited access to the application above

Block
Stops execution of the application above

□ Trust this application

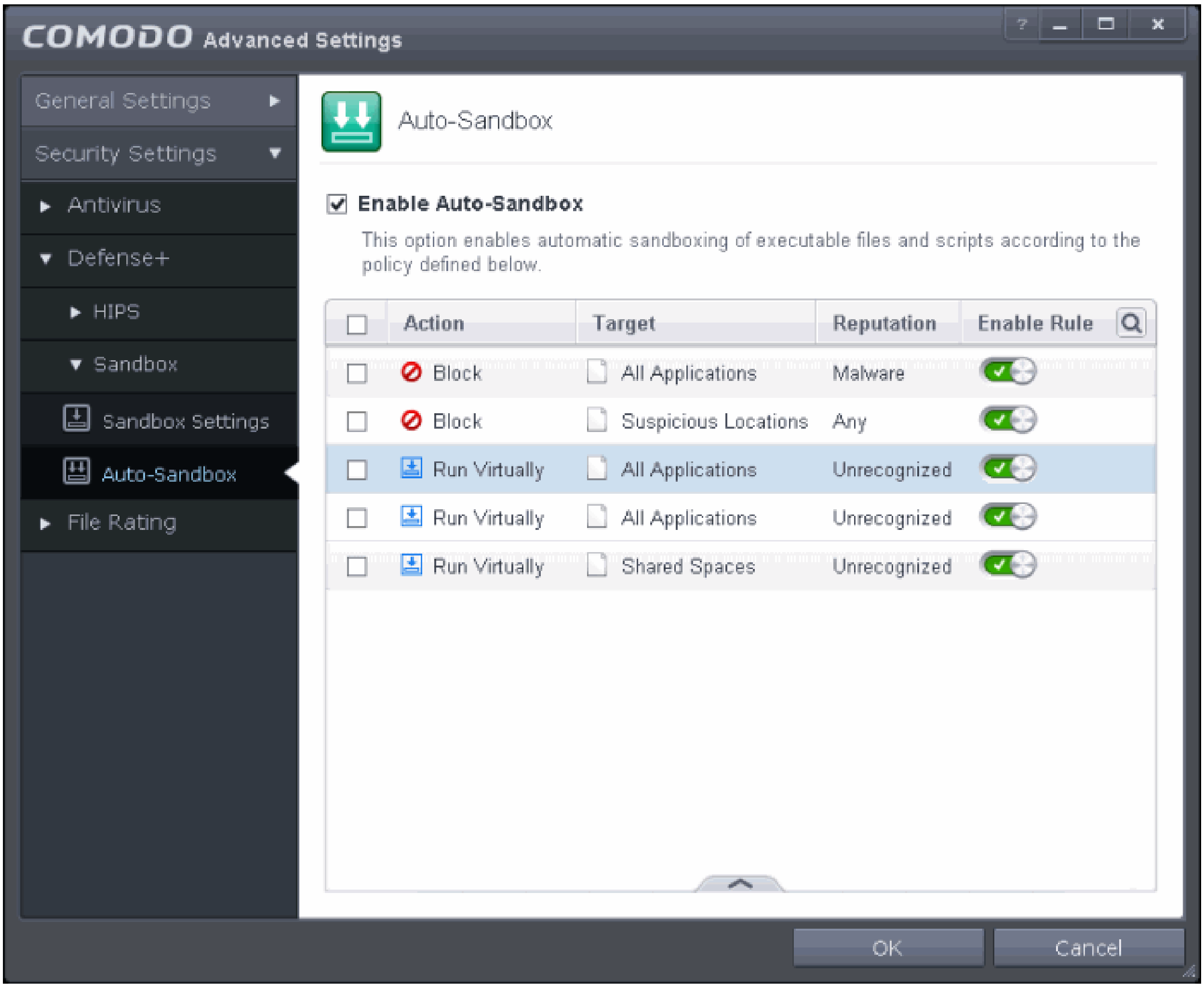
You can decide on whether or not to allow the installer or update based on your assessment, from the alert itself. (***Default=Enabled***)

- **Show privilege elevation alerts for unknown programs** : Allows you to instruct the Sandbox to display alerts when a new or unrecognized program, application or executable requires administrator or elevated privileges to run. You can decide on whether or not to allow the unknown application based on your assessment, from the alert itself. (***Default=Enabled***)

5.2.2.9. Configuring Rules for Auto-Sandbox

The 'Auto-Sandbox' interface allows you to add and define rules for programs that should be run in the sandboxed environment. A sandboxed application has much less opportunity to damage your computer because it is run isolated from your operating system and your files. This allows you to safely run applications that you are not 100% sure about. Auto-sandbox rules allow you to determine whether programs should be allowed to run with full privileges, ignored, run restricted or run in fully virtualized environment. For easy identification, Comodo Antivirus for Servers will show a green border around programs that are running in the sandbox.

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



Auto-Sandbox

☑ **Enable Auto-Sandbox**

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malware	✓
□	Block	Suspicious Locations	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	Shared Spaces	Unrecognized	✓

- **Enable Auto-Sandbox** - Allows you to enable or disable the Sandbox. If enabled, the applications are run inside the sandbox as per the rules defined. (***Default = Enabled***)

The interface displays the configured rules:

- **Action –** Displays the operation that the sandbox should perform on the target files if the rule is triggered.
- **Target** – The files, file groups or specified locations on which the rule will be executed.
- **Reputation –** The trust status of the files to which the rule should apply. Can be 'Malware', 'Trusted' or 'Unrecognized'.
- **Enable Rule –** Allows you to enable/disable the rule.

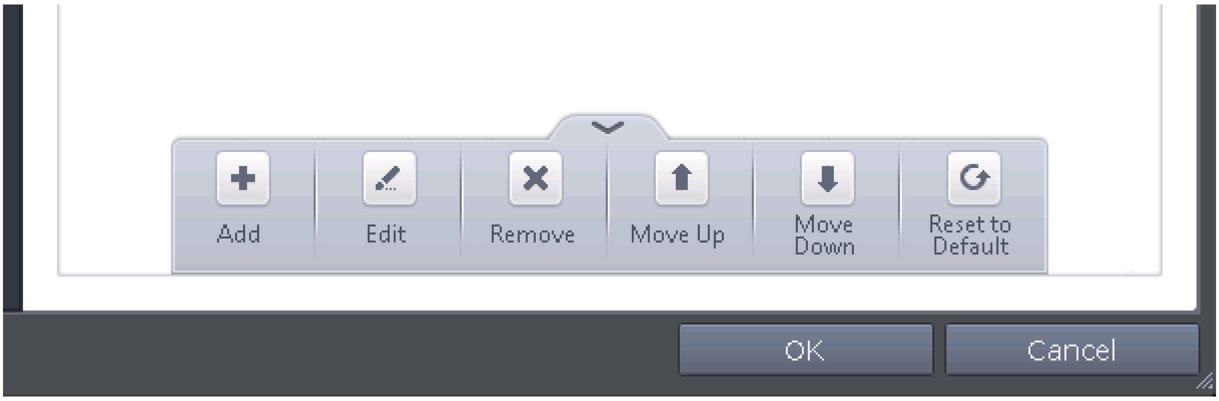
CAVS ships with a set of pre-defined auto-sandbox rules that are configured to provide maximum protection for your system. The table provides the configuration settings for these pre-defined rules:

Rule	Action	Target	Restriction Level	Rating	Source			Log Action	Limit Maximum memory	Limit Program Execution Time	Quarantine
					Created by	Located on	Downloaded from				
1	Block	File Group - All Applications	N/A	Malware	Any	Any	Any	On	N/A	N/A	On

2	Block	File Group - Suspicious Locations	N/A	Any	Any	Any	Any	On	N/A	N/A	Off
3 Applicable only for Windows 8.0 and 8.1	Ignore	All Metro Apps	Off	Any	Any	Any	Any	On	N/A	N/A	N/A
4	Run Virtual	File Group - All Applications	Off	Unrecognized	Any	Any	Internet	On	Off	Off	N/A
					Any	Network Drive	Any				
					Any	Removable Drive	Any				
5	Run Virtual	File Group - All Applications	Off	Unrecognized	File Group – Web Browsers	Any	Any	On	Off	Off	N/A
					File Group – Email Clients	Any	Any				
					File Group – File Downloaders	Any	Any				
					File Group – Pseudo-File Downloaders						
6	Run	File Group	Off	Unrecog	Any	Any	Any	On	Off	Off	N/A

	Virtual	– Shared Spaces		nized							

Clicking the handle at the bottom of the interface opens a rule configuration panel:



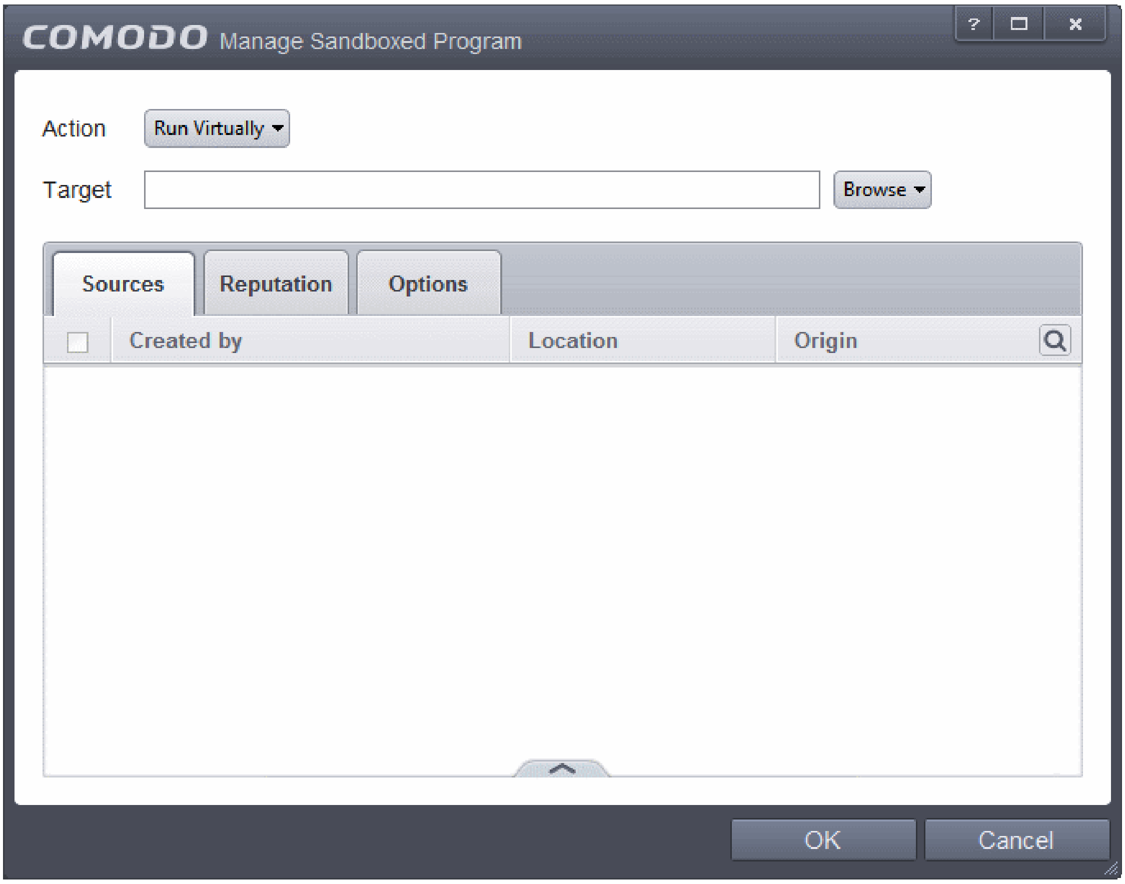
- **Add** - Allows you to add a new sandbox rule. See the section '**Adding an Auto-Sandbox Rule**' for guidance on creating a new rule.
- **Edit** - Allows you to modify the selected sandbox rule. See the section '**Editing an Auto-Sandbox Rule**' for more details.
- **Remove** - Deletes the selected rule.
- **Reset to Default** – Resets to default the rule.

Users can also re-prioritize the sandbox rules by using the 'Move Up' and 'Move Down' buttons.

Adding an Auto-Sandbox Rule

Auto-sandbox rules can be created for a single application, for all applications in a folder or file group, from running processes or for applications based on their file or process hash. ‘Source’, ‘Reputation’ and ‘Options’ allow you to add detailed filters to your rule. They are, however, optional, so you can create a very simple rule to run an application in the sandbox just by specifying the action and the target application.

- Click the 'Add' button from the options.

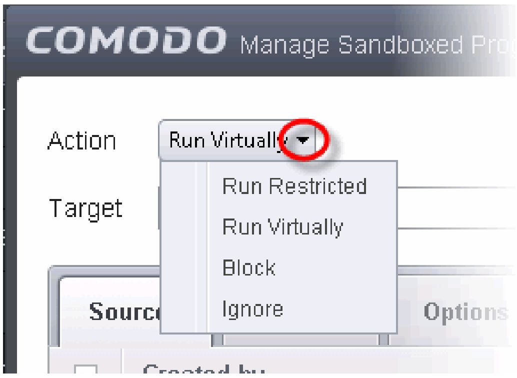


The Manage Sandboxed Program screen will be displayed.

- **Step 1** – Select the Action
- **Step 2** – Select the Target
- **Step 3** – Select the Sources
- **Step 4** – Select the File Reputation
- **Step 5** – Select the Options

Step 1 – Select the Action

The options under the Action drop-down button combined with the Set Restriction Level setting in the Options tab determine the amount of privileges an auto-sandboxed application has access to other software and hardware resources on your computer.



The options available under the Action button are:

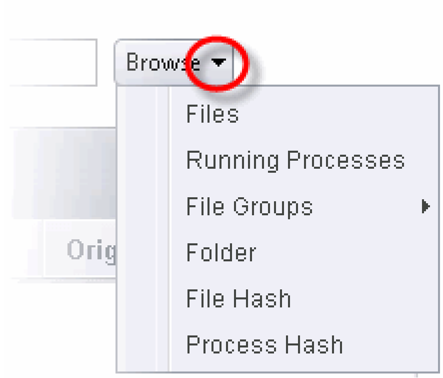
- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.

- **Run Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be sandboxed and allowed to run with all privileges.

Select the action from the options.

Step 2 – Select the Target

The next step is to select the target to which the auto-sandbox rule is to be applied. Click the Browse button beside the Target field.

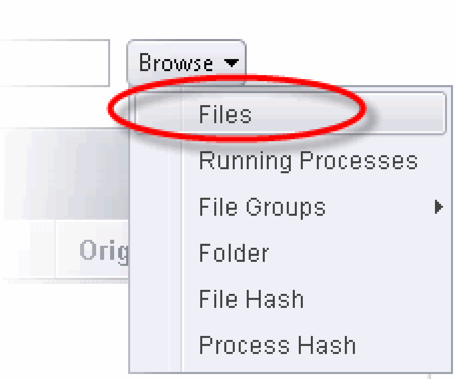


You have five options available to add the target path.

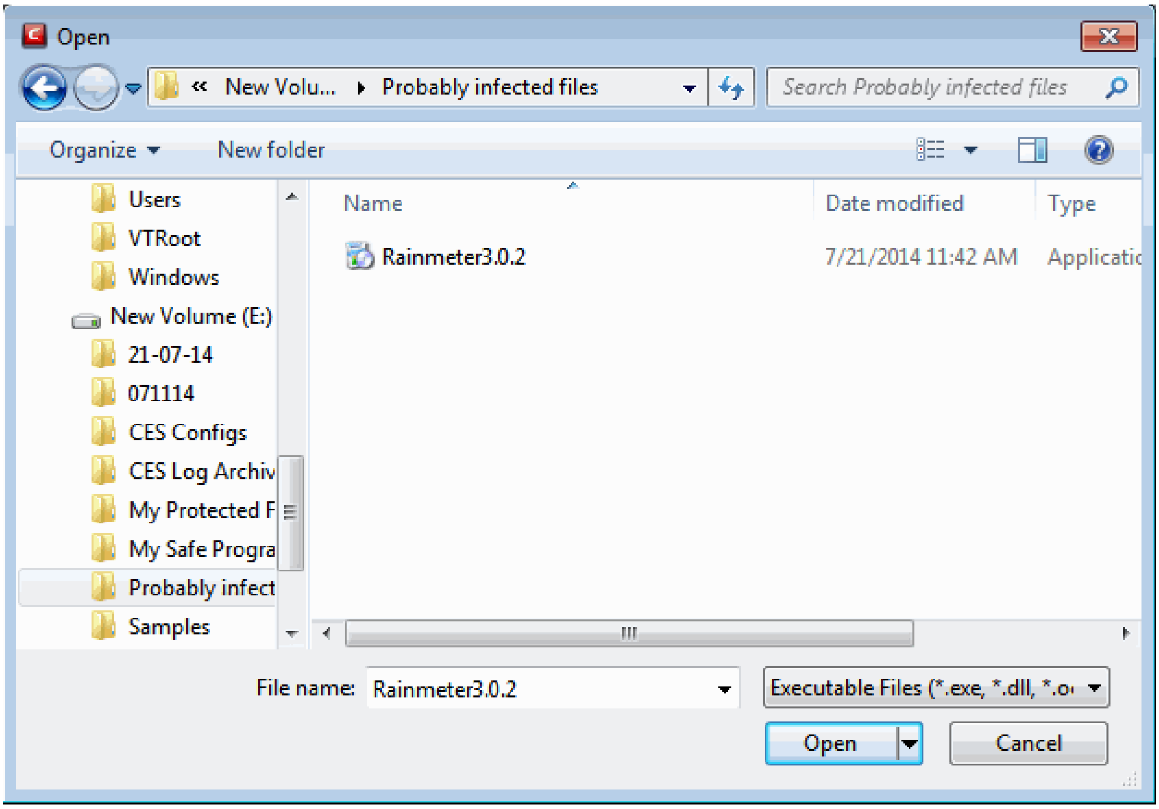
- **Files** – Allows to add individual files as target.
- **Running Processes** – As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** – Allows to add predefined File Groups as target. To add or modify a predefined file group refer to the section **File Groups** for more details.
- **Folder** – Allows you to add a folder or drive as the target
- **File Hash** – Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

Adding an individual File

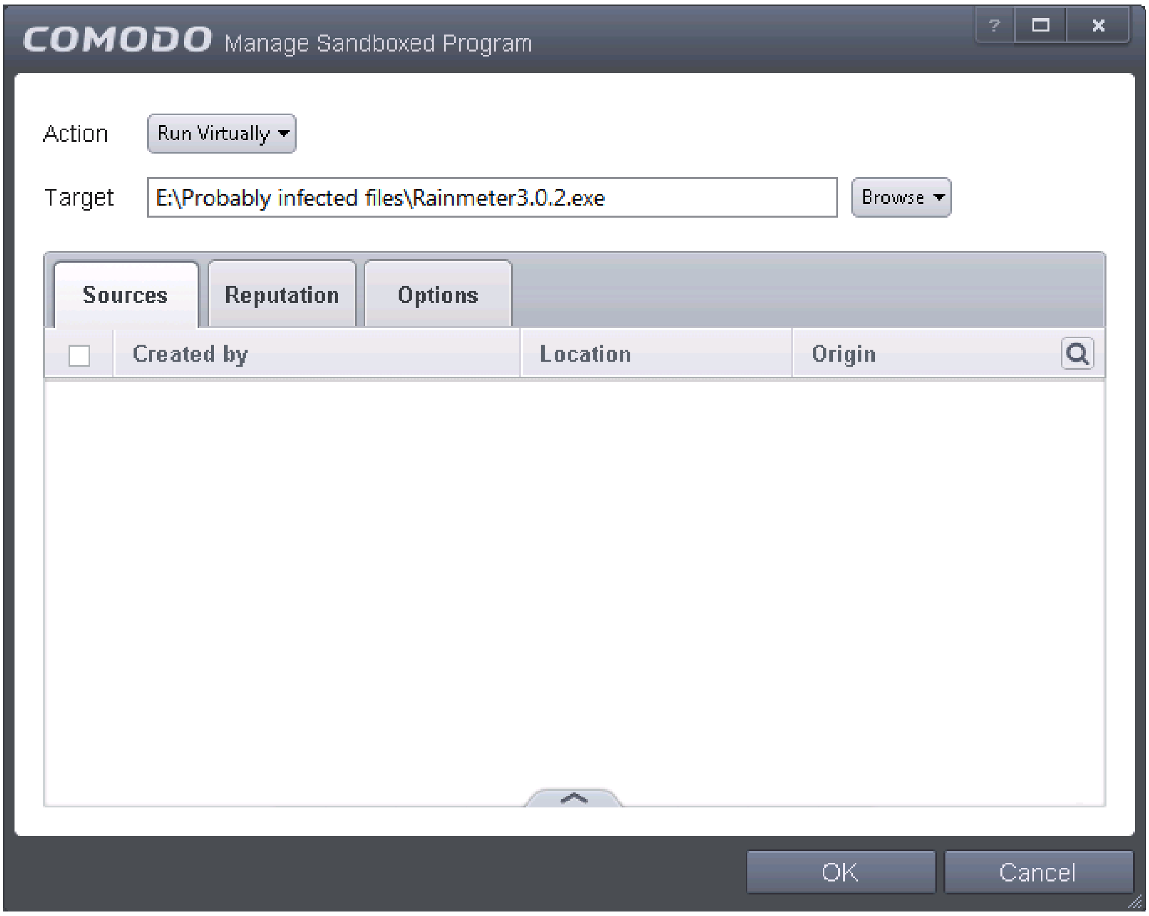
- Choose 'Files' from the 'Browse' drop-down.



- Navigate to the file you want to add as target in the 'Open' dialog and click 'Open'



The file will be added as target and will be run as per the action chosen in **Step 1**.



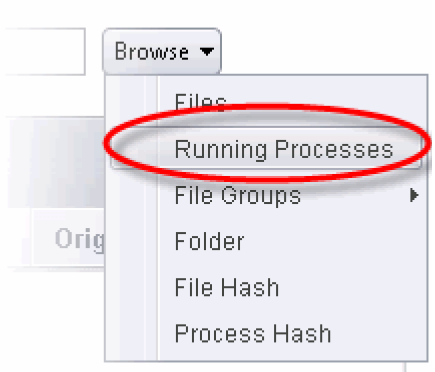
Action: Run Virtually

Target: E:\Probably infected files\Rainmeter3.0.2.exe

If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

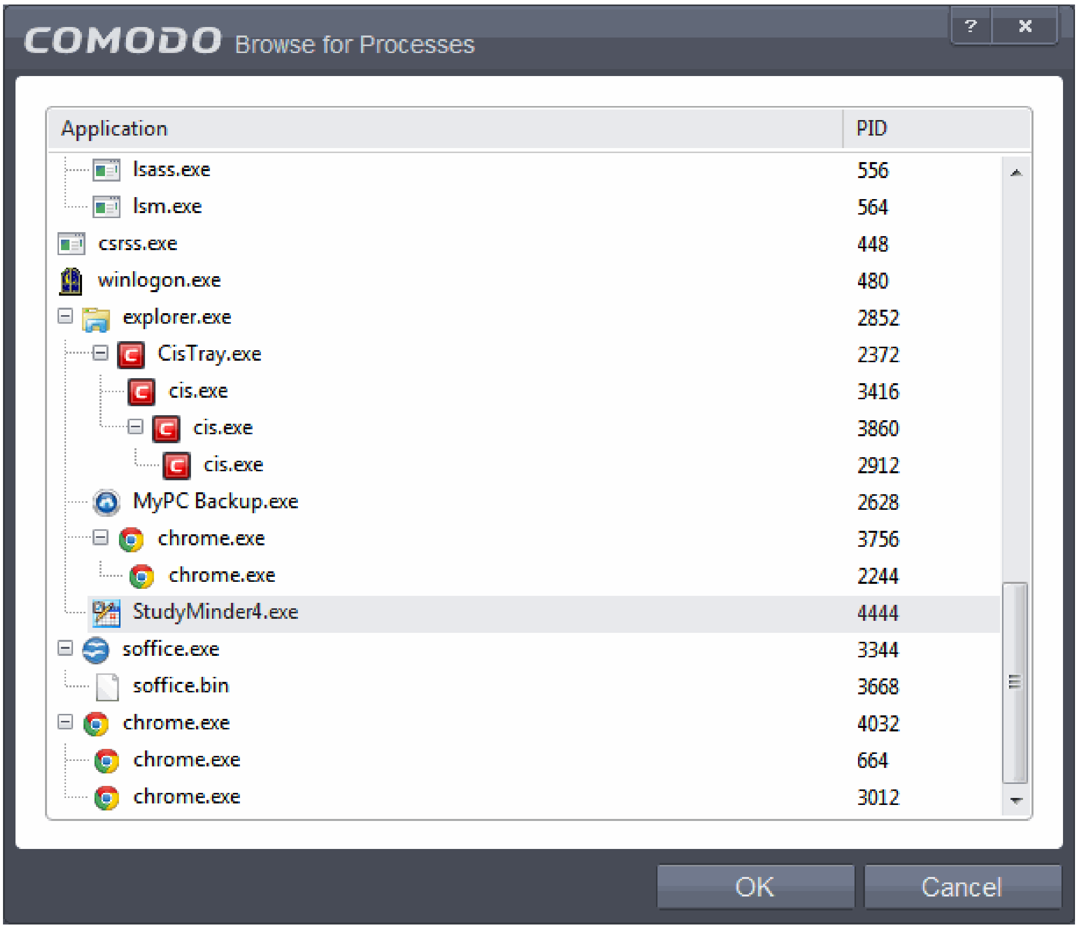
Adding an application from a running processes

- Choose 'Running Processes' from the 'Browse' drop-down.



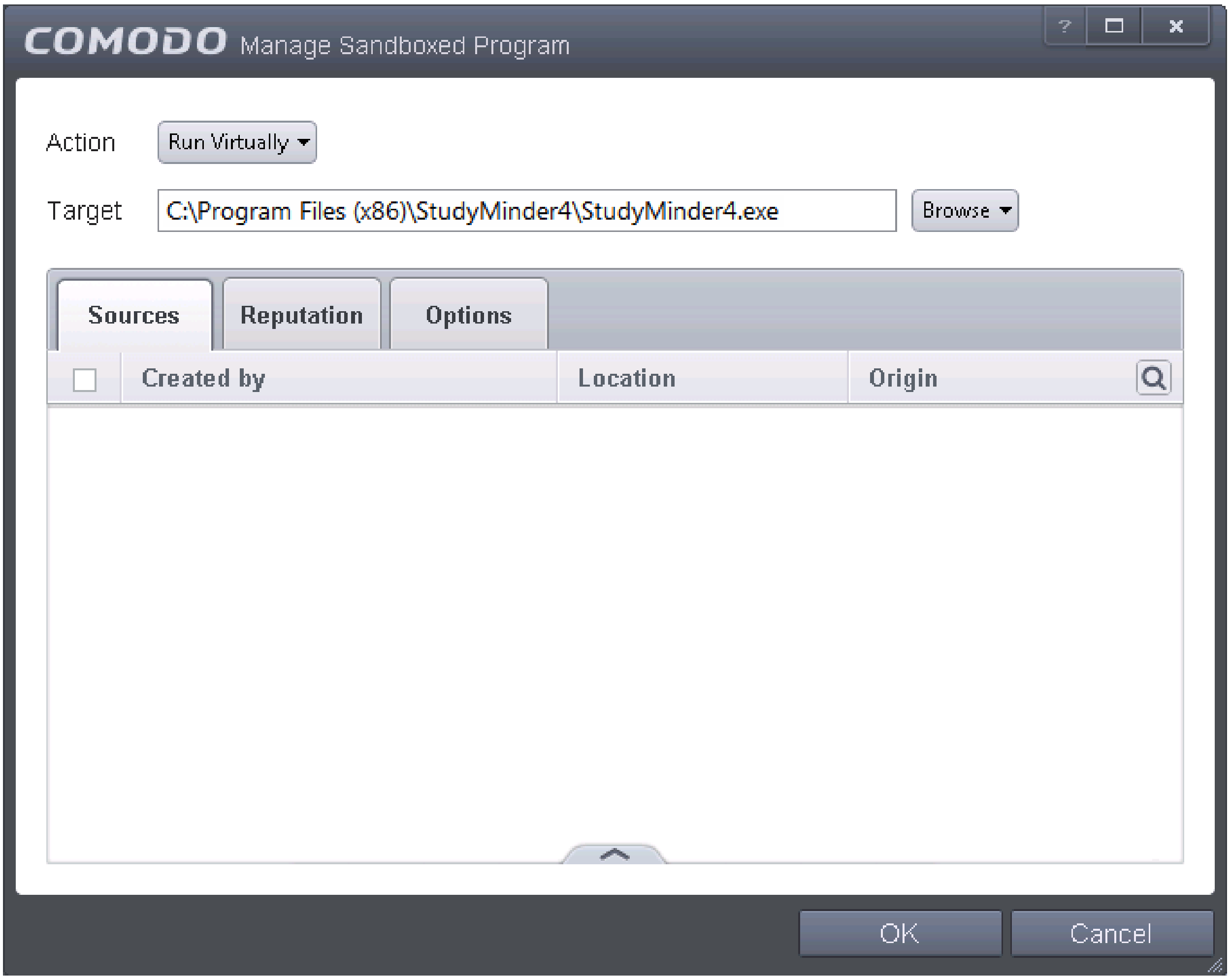
A list of currently running processes in your computer will be displayed.

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



Application	PID
lsass.exe	556
lsm.exe	564
csrss.exe	448
winlogon.exe	480
explorer.exe	2852
CisTray.exe	2372
cis.exe	3416
cis.exe	3860
cis.exe	2912
MyPC Backup.exe	2628
chrome.exe	3756
chrome.exe	2244
StudyMinder4.exe	4444
soffice.exe	3344
soffice.bin	3668
chrome.exe	4032
chrome.exe	664
chrome.exe	3012

The file will be added as target and will be run as per the action chosen in **Step 1**.



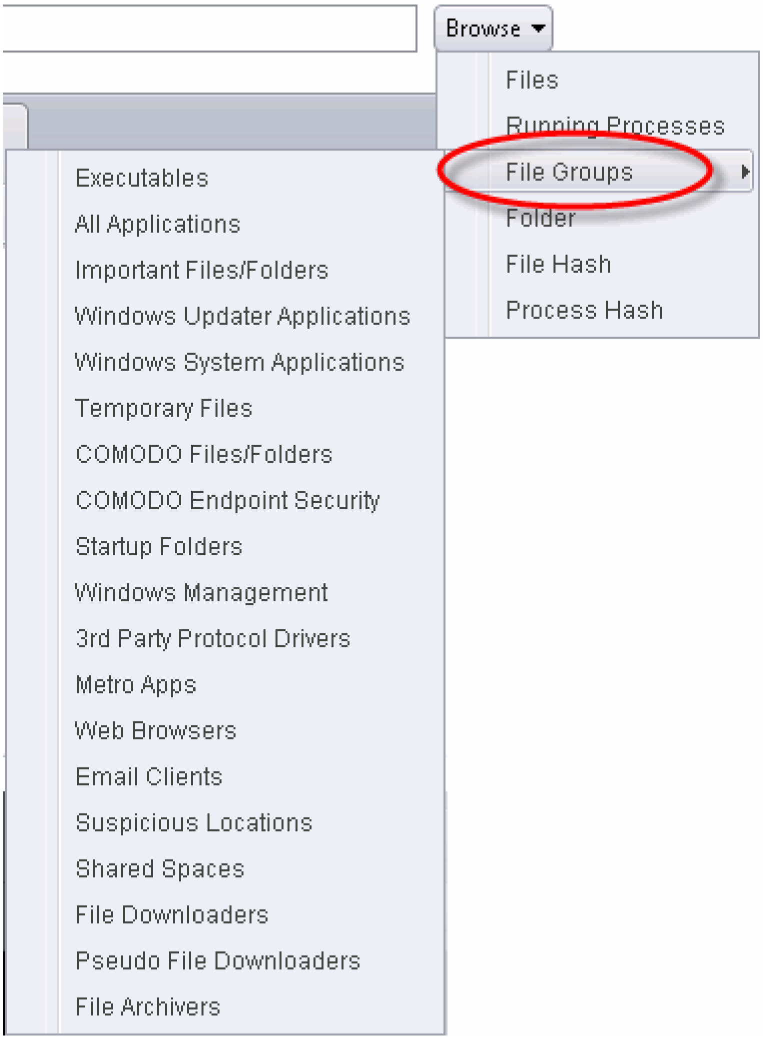
Action: Run Virtually

Target: C:\Program Files (x86)\StudyMinder4\StudyMinder4.exe

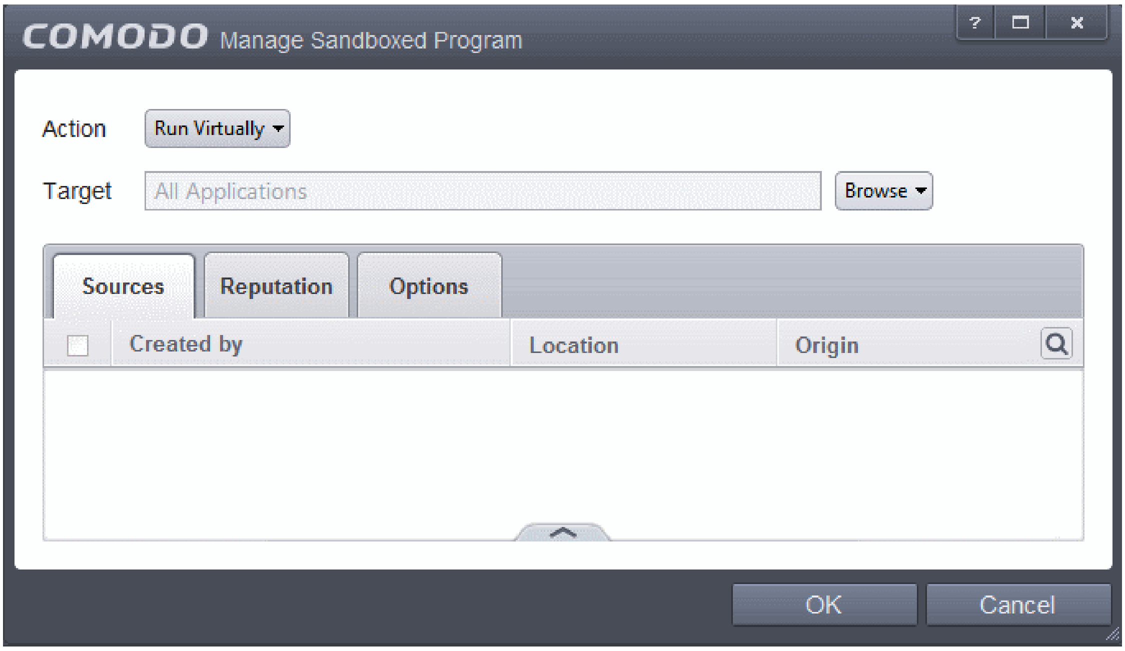
If you want to just add an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Adding a File Group

- Choose 'File Groups' from the 'Browse' drop-down. Choosing File Groups allows you to include a category of pre-set files or folders. For more details on how to manage file groups refer to the section **File Groups**.



- Select the preset file group from the options.
- The file group will be added as target and the applications inside it will be run as per the action chosen in **Step 1**.


COMODO Manage Sandboxed Program

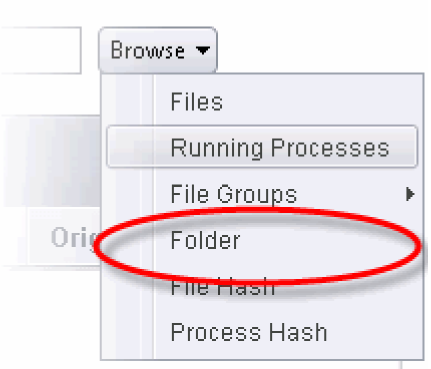
Action: Run Virtually

Target: All Applications

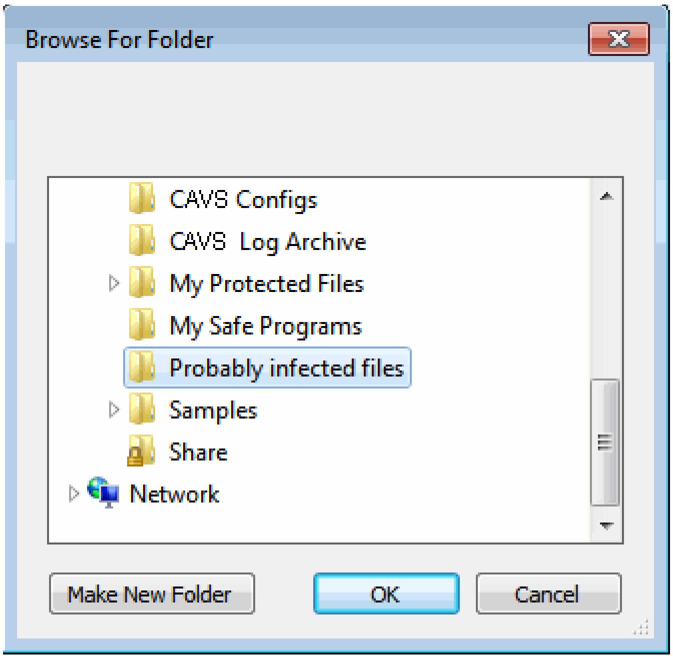
If you want to just add the applications in the file group for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Adding a Folder/Drive Partition

- Choose 'Folder' from the 'Browse' drop-down.

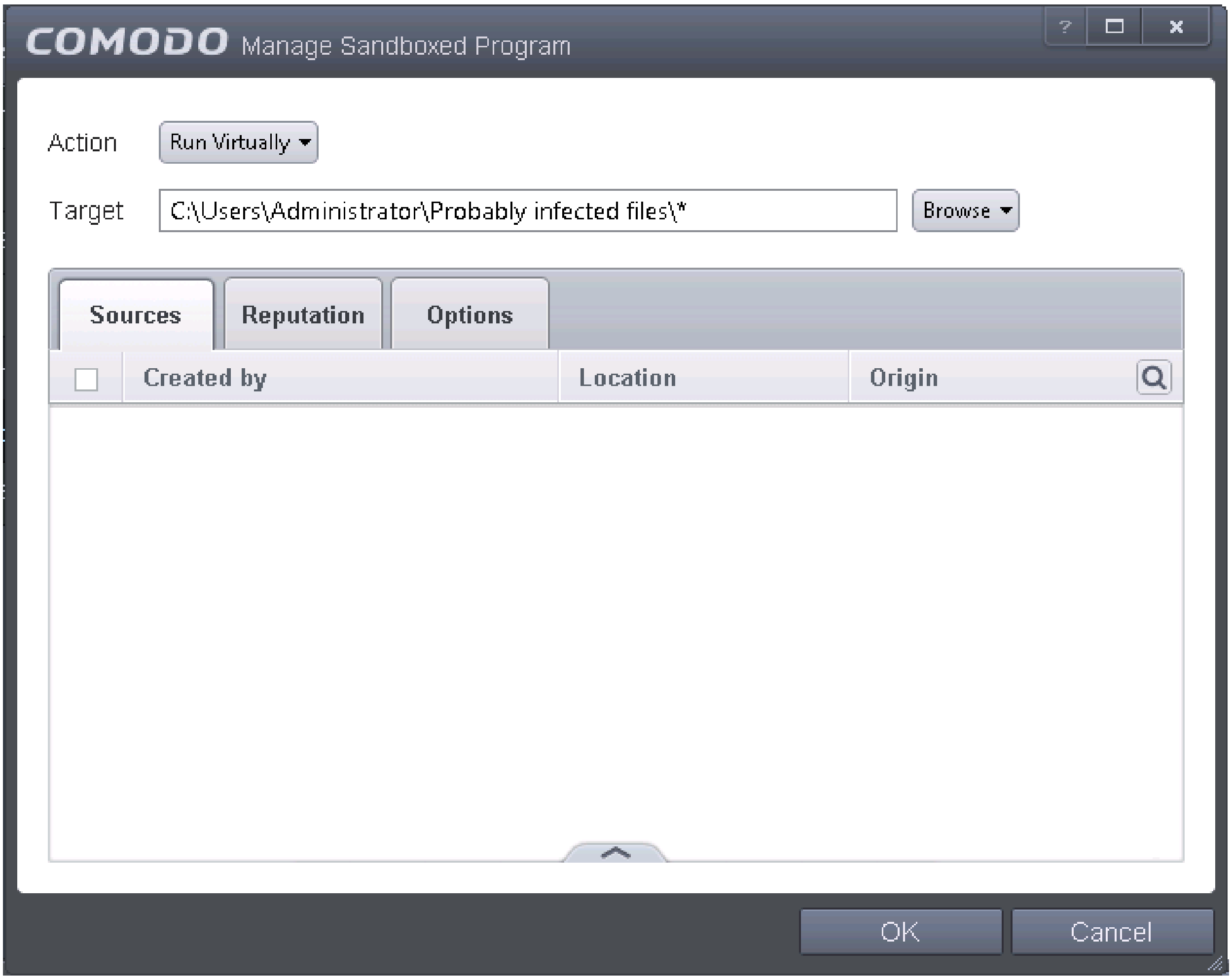


The 'Browse for Folder' dialog will appear.



- Navigate to the drive partition or folder you want to add as target and click OK

The drive partition/folder will be added as target and will be run as per the action chosen in **Step 1**.



Action: Run Virtually

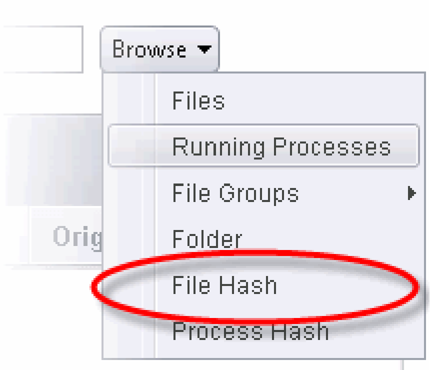
Target: C:\Users\Administrator\Probably infected files*

Browse

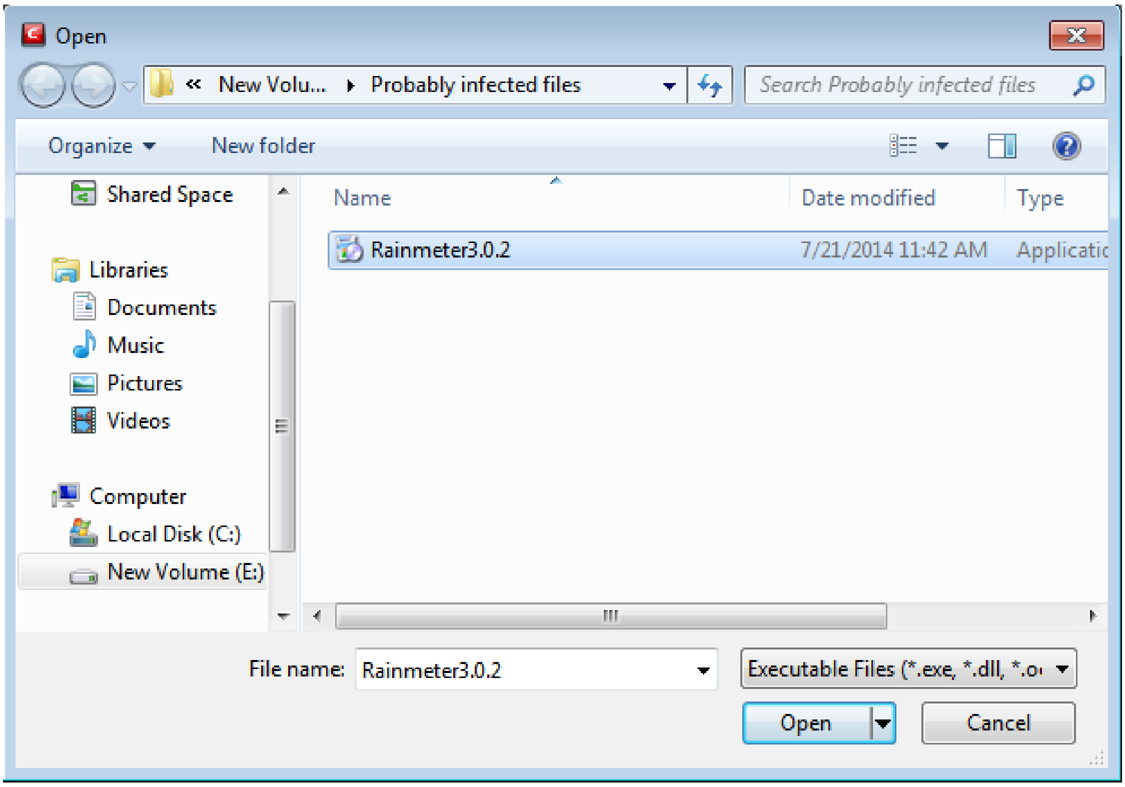
If you want to just add the applications in the drive partition/folder for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Adding a file based on its hash value

- Choose 'File Hash' from the 'Browse' drop-down.



- Navigate to the file whose hash value you want to add as target in the 'Open' dialog and click 'Open'

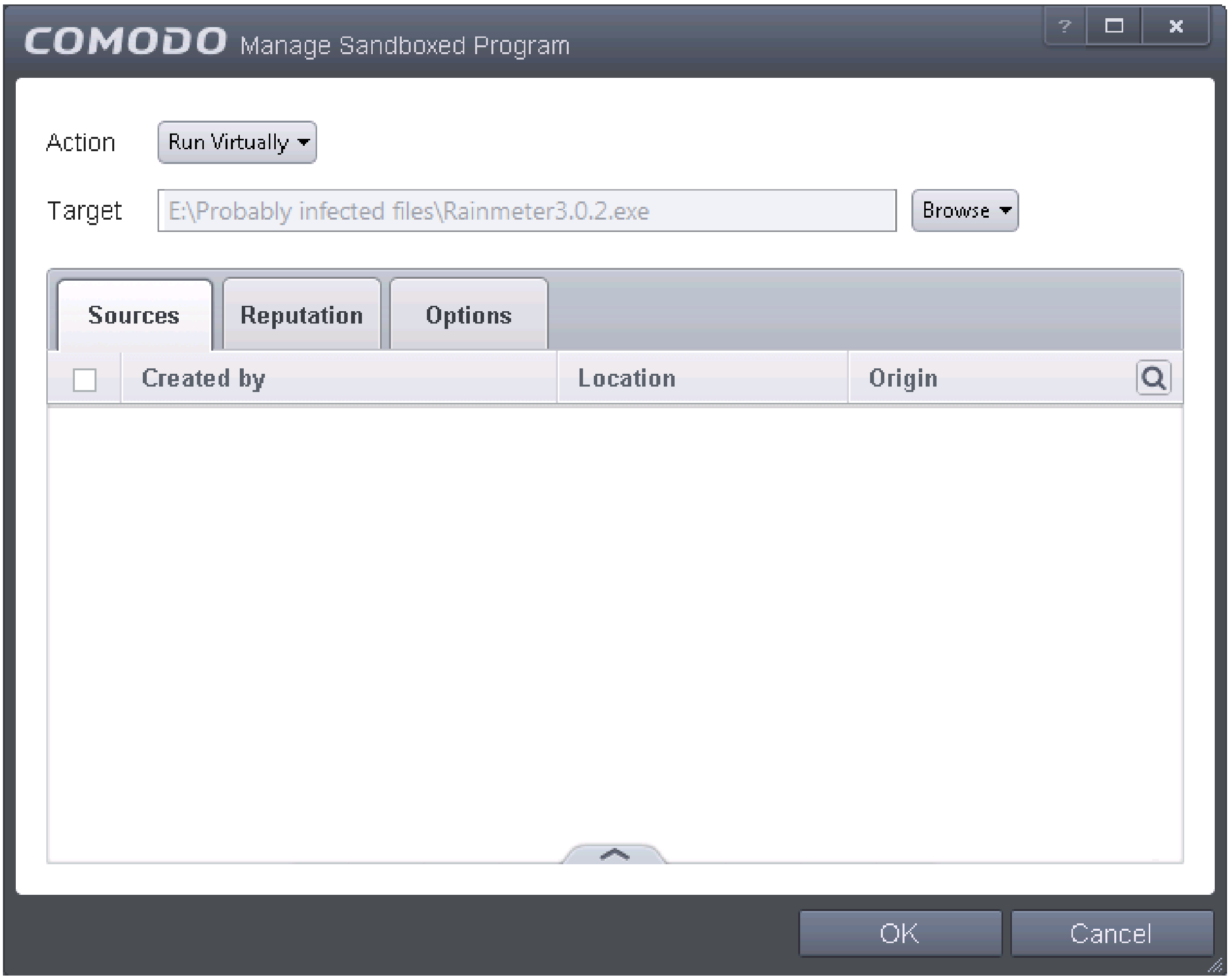


Name	Date modified	Type
Rainmeter3.0.2	7/21/2014 11:42 AM	Applicatic

File name: Rainmeter3.0.2

Executable Files (*.exe, *.dll, *.o

The file will be added as target and will be run as per the action chosen in **Step 1**.



Action: Run Virtually

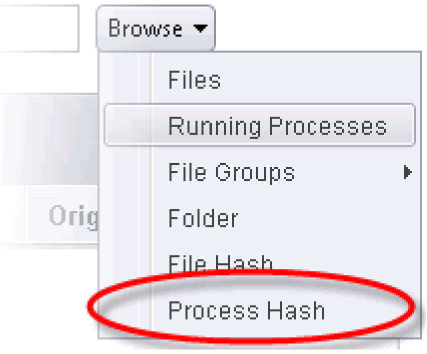
Target: E:\Probably infected files\Rainmeter3.0.2.exe

□	Created by	Location	Origin

If you want to just add the hash value of an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

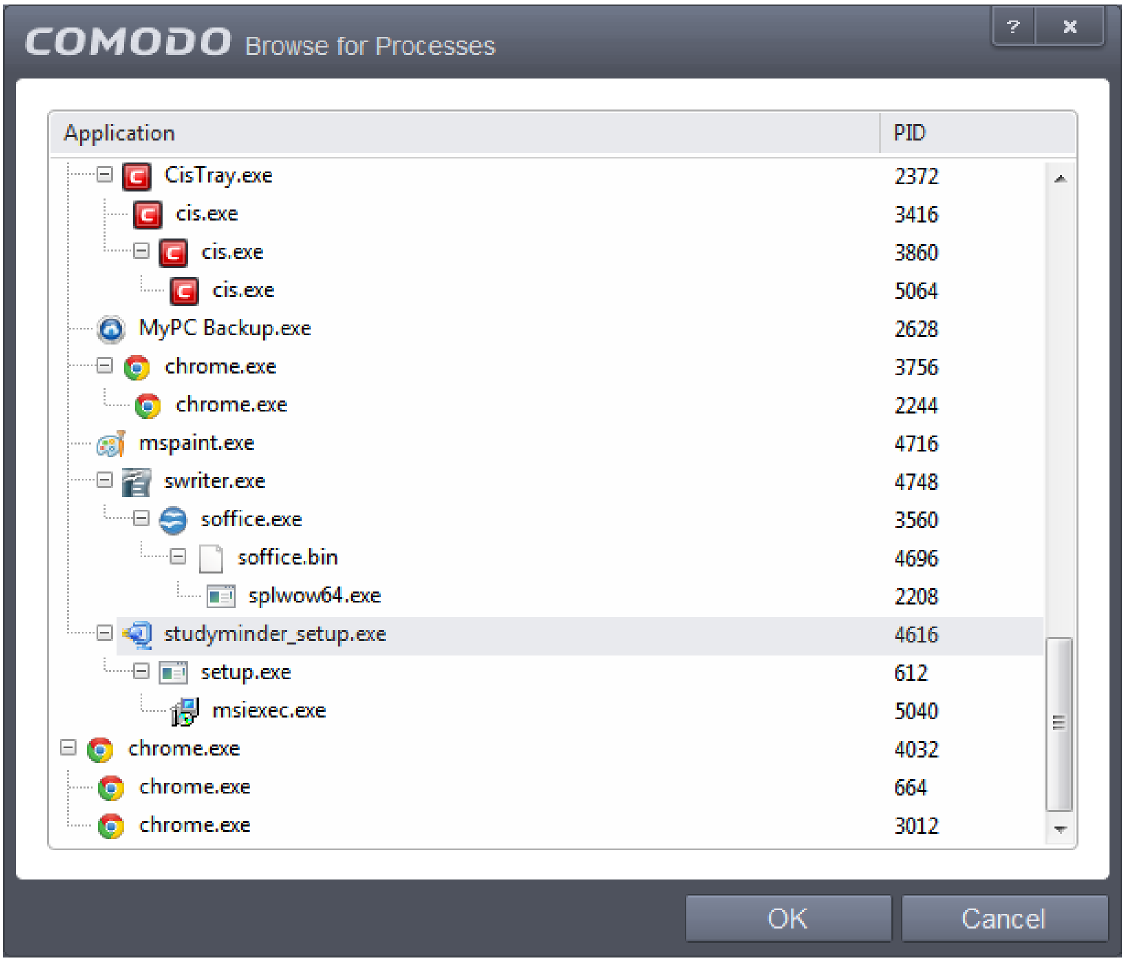
Adding an application from a running process based on its hash value

- Choose 'Process Hash' from the 'Browse' drop-down.



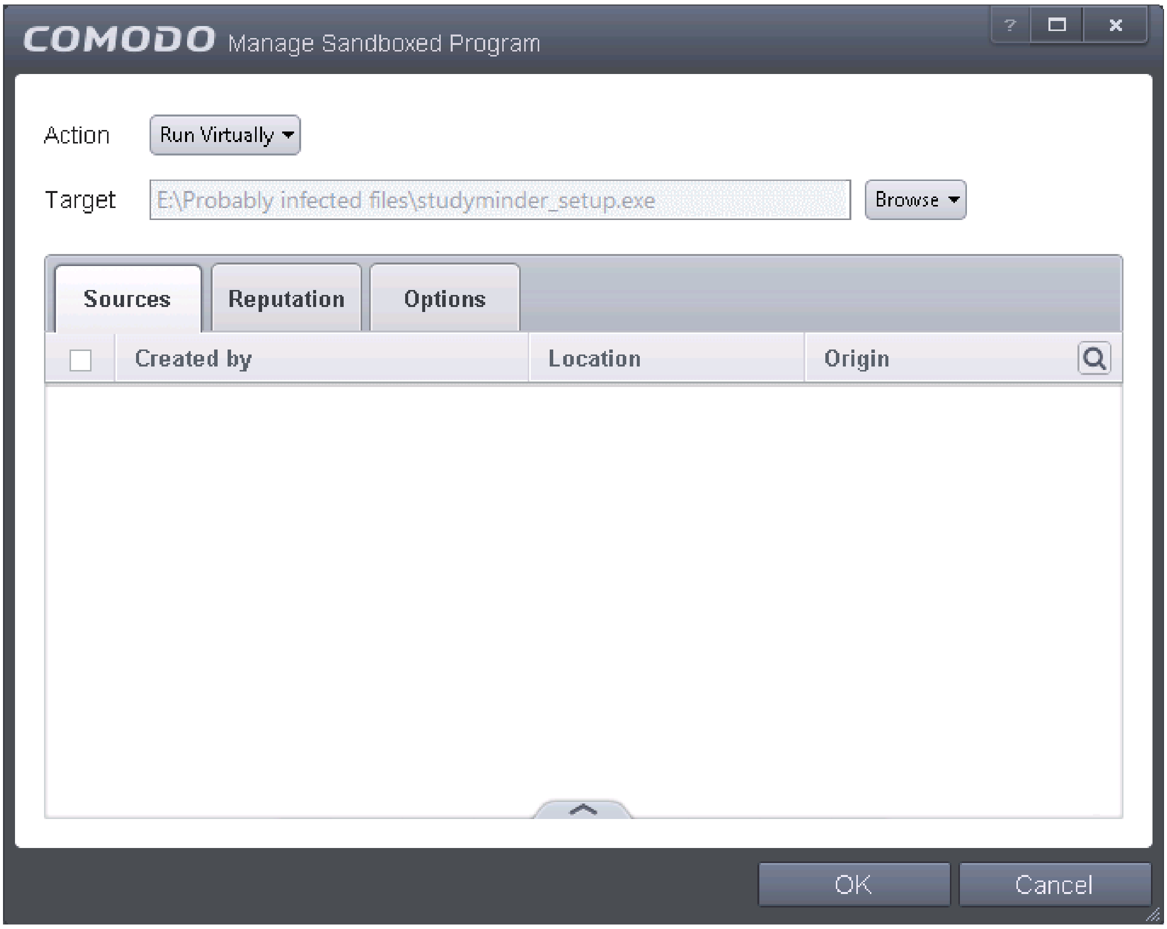
A list of currently running processes in your computer will be displayed.

- Select the process, whose hash value of the target application is to be added to target and click 'OK' from the Browse for Process dialog.


COMODO Browse for Processes

Application	PID
CisTray.exe	2372
cis.exe	3416
cis.exe	3860
cis.exe	5064
MyPC Backup.exe	2628
chrome.exe	3756
chrome.exe	2244
mspaint.exe	4716
swriter.exe	4748
soffice.exe	3560
soffice.bin	4696
splwow64.exe	2208
studyminder_setup.exe	4616
setup.exe	612
msiexec.exe	5040
chrome.exe	4032
chrome.exe	664
chrome.exe	3012

The file will be added as target and will be run as per the action chosen in **Step 1**.



COMODO Manage Sandboxed Program

Action: Run Virtually

Target: E:\Probably infected files\studyminder_setup.exe

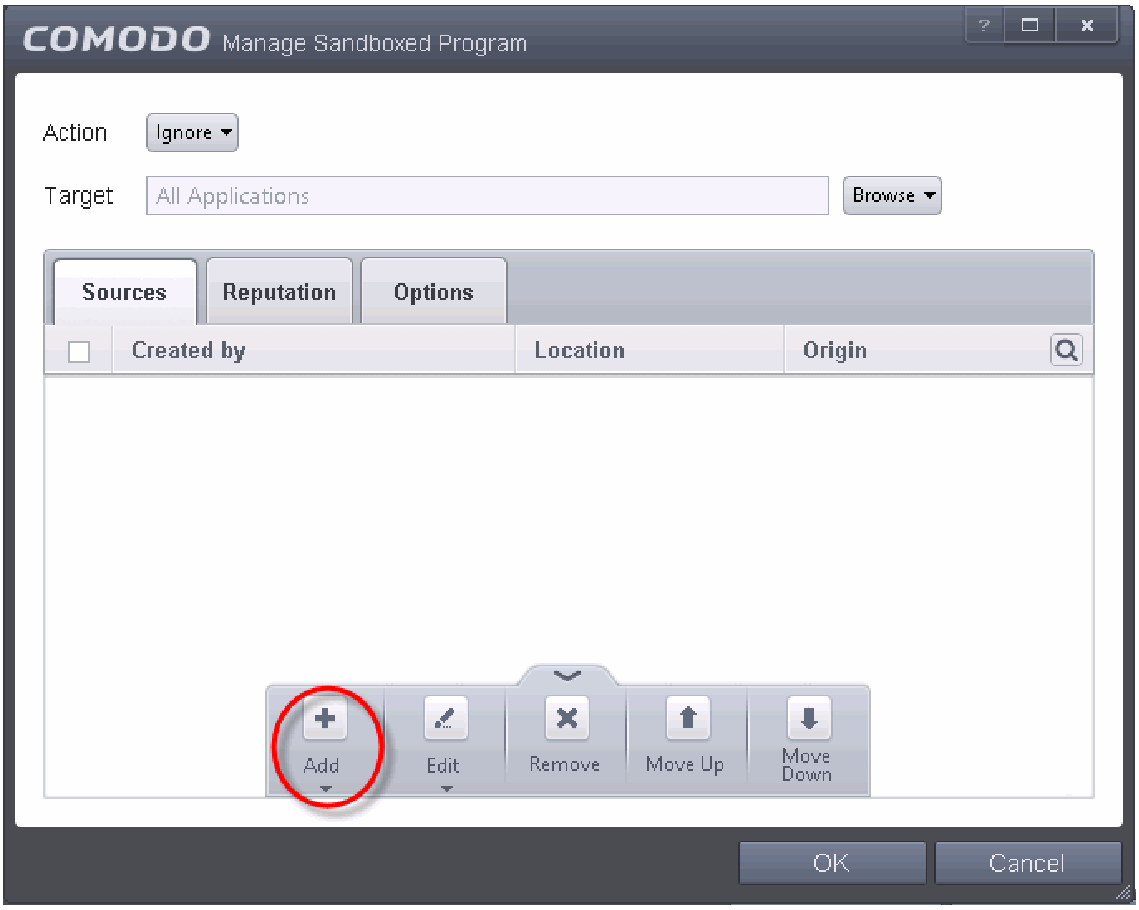
If you want to just add the process hash value of an application for a particular action as selected in **Step 1** without specifying any filters or options, then click 'OK'. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Source** and **Reputation** filters and **Options** for the rule.

Step 3 – Select the Sources

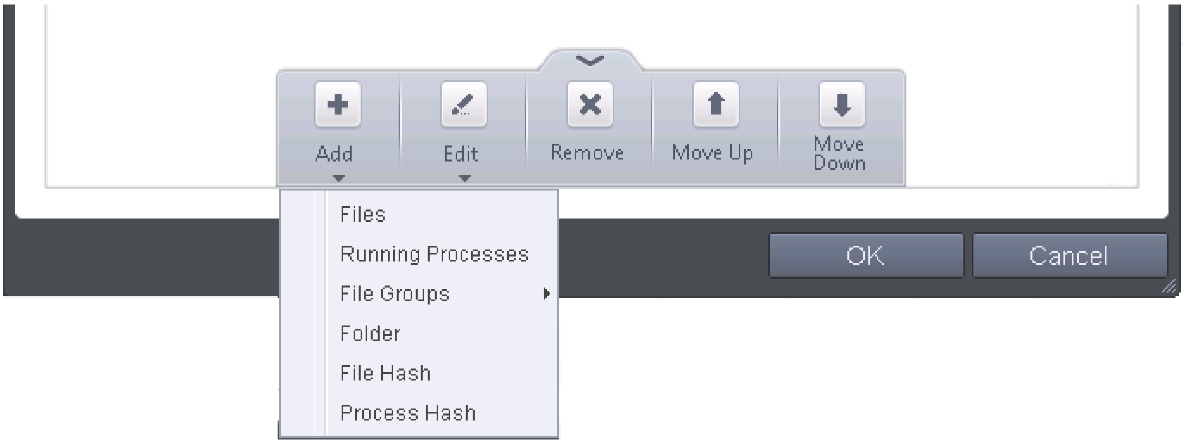
If you want to include a number of items for a rule but want the rule to be applied for certain conditions only, then you can do this in this step. For example, if you include all executables in the Target but want the rule to be applied for executables that were downloaded from the internet only, then the filter can be applied in the Sources. Another example is if you want to run unrecognized files from network share, you have to create an ignore rule with All Applications as target and source located on network drives.

To add a source

- Click the handle at the bottom and then click Add from the options.



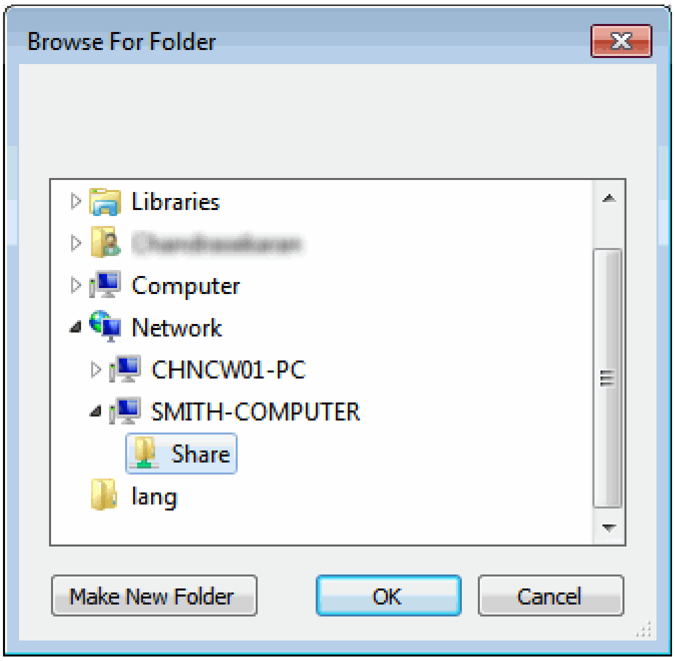
The options available are available are same as available under the Browse button beside Target as explained in **Step 2**. Refer to previous section for each of options for more details.



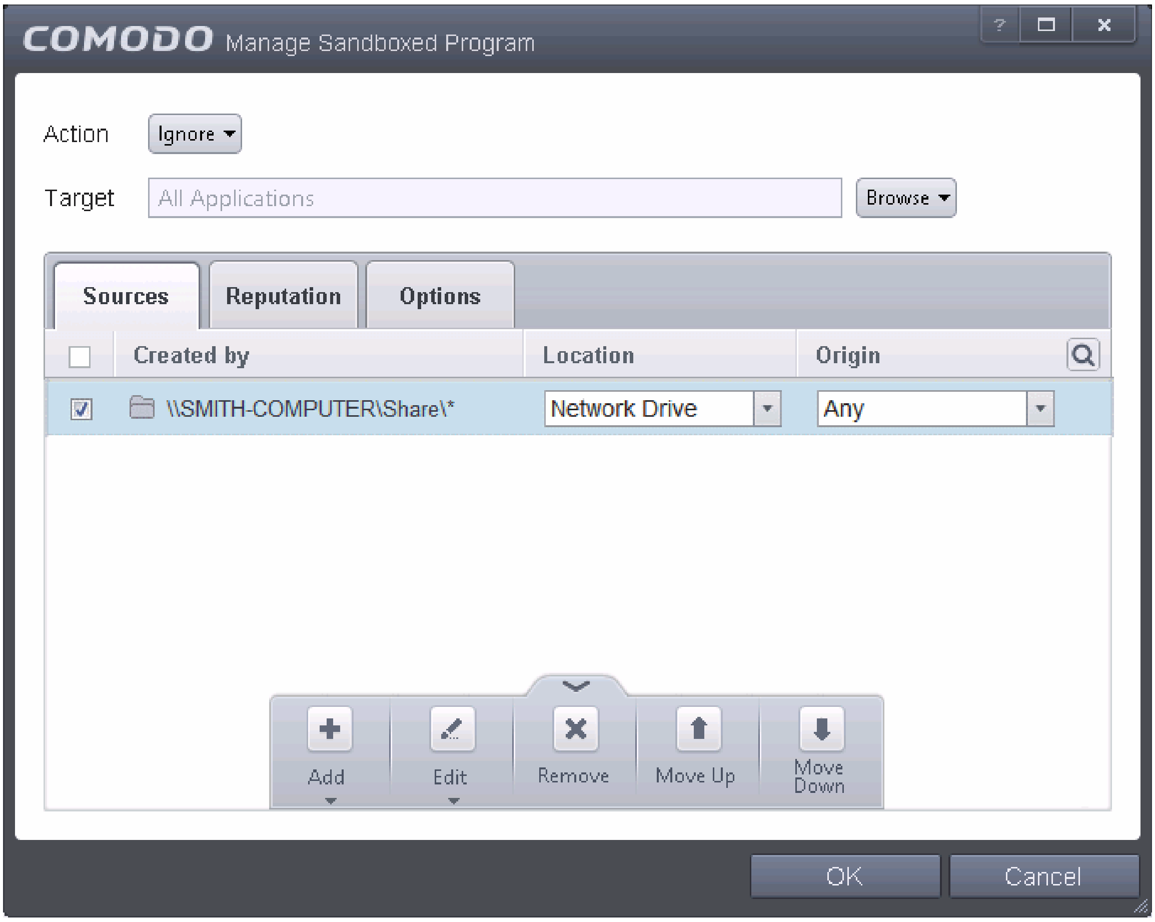
The following example describes how to add an Ignore rule for Unrecognized files from a network source:

- In **Step 1**, select the action as Ignore
- In **Step 2**, select the Target as All Applications in File Groups
- In **Step 3**, click Folder from the Add options.

The Browse For Folder dialog will be displayed.



- Navigate to the source folder in the network, select it and click 'OK'.



Action: Ignore

Target: All Applications

□	Created by	Location	Origin
☑	\\SMITH-COMPUTER\Share\*	Network Drive	Any

The selected network source folder will be added under the 'Created by' column and the screen displays the options to specify the location and from where the files were downloaded.

- **Location** – The options available are:
  - Any
  - Local Drive

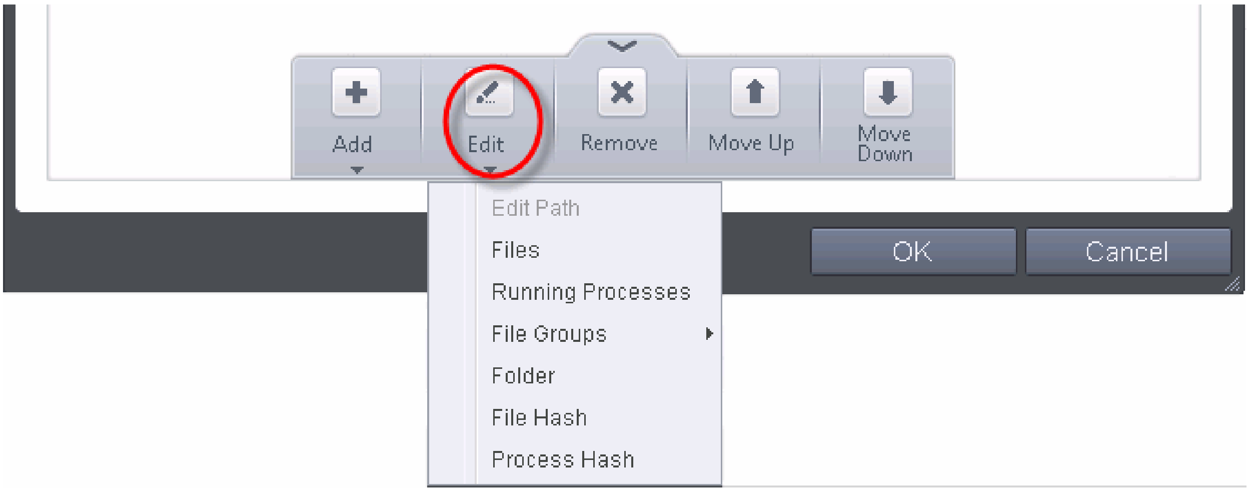
- Removable Drive
- Network Drive

Since the source is located in a network, select Network Drive from the options.

- **Origin** – The options available are:
  - Any – The rule will apply to files that were downloaded to the source folder from both Internet and Intranet.
  - Internet – The rule will apply to files that were downloaded to the source folder from Internet only.
  - Intranet – The rule will apply to files that were downloaded to the source folder from Intranet only.

Repeat the process to add more source folders.

- Click the Edit button to change the source path from the options:



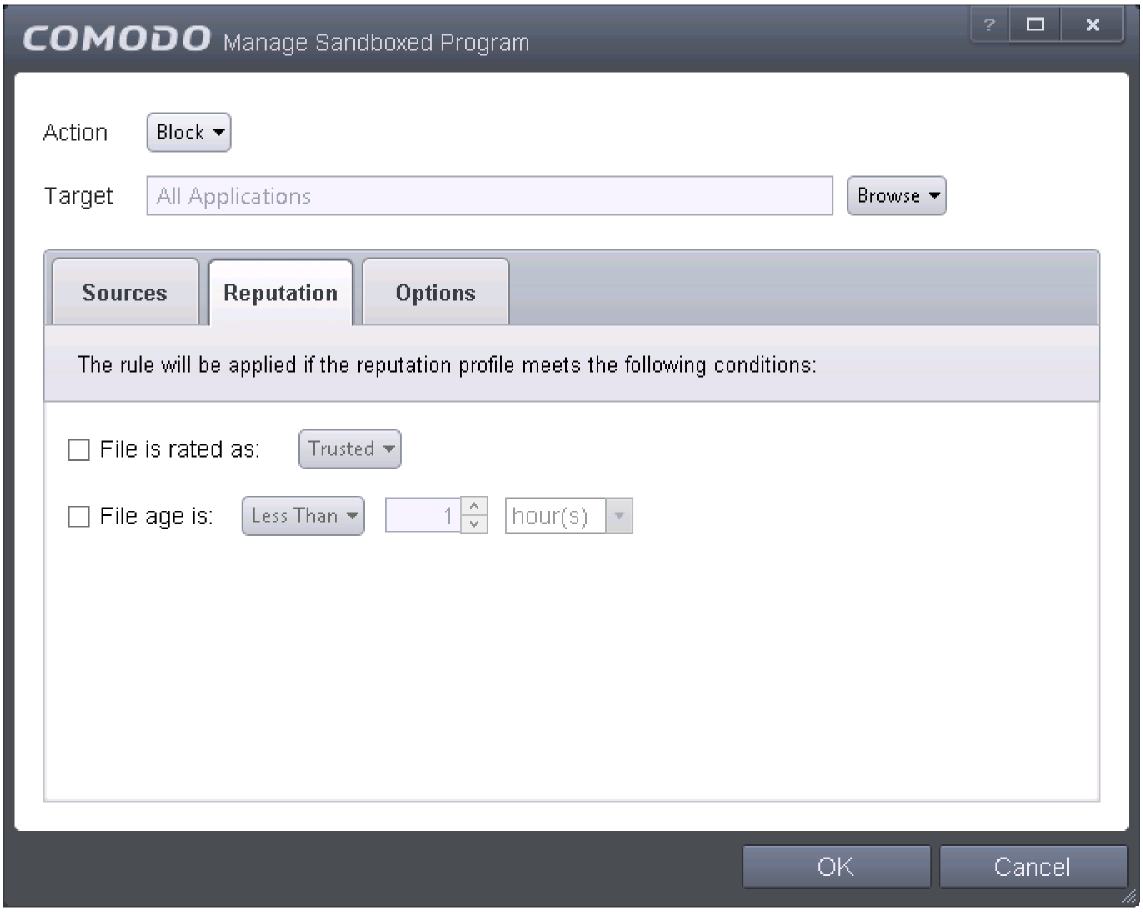
- To remove a source from the list, select it and click the Remove button.
- Use the 'Move Up' and 'Move Down' buttons to specify the order of source path.

If you want to just add the Sources for a particular action as selected in **Step 1** without specifying rating of the file or options, then click 'OK'. The default values for Reputation will be 'Any' and for Options it will be 'Log when this action is performed'. If required you can configure **Reputation** filters and **Options** for the rule.

Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options in **Step 4**.

Step 4 – Select the File Reputation

- Click the Reputation tab in the Manage Sandboxed Program interface.



By default, the file rating is not selected meaning the rating could be Any. The options available are:

- **Trusted** – Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by Defense+. Refer to the sections **File Rating Settings** and **File List** for more information.
- **Unrecognized** – Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section **File List** for more information.
- **Malware** – Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. Refer the section **Unknown Files – The Scanning Process** for more information.

By default, file age is not selected, so the age could be Any. The options available are:

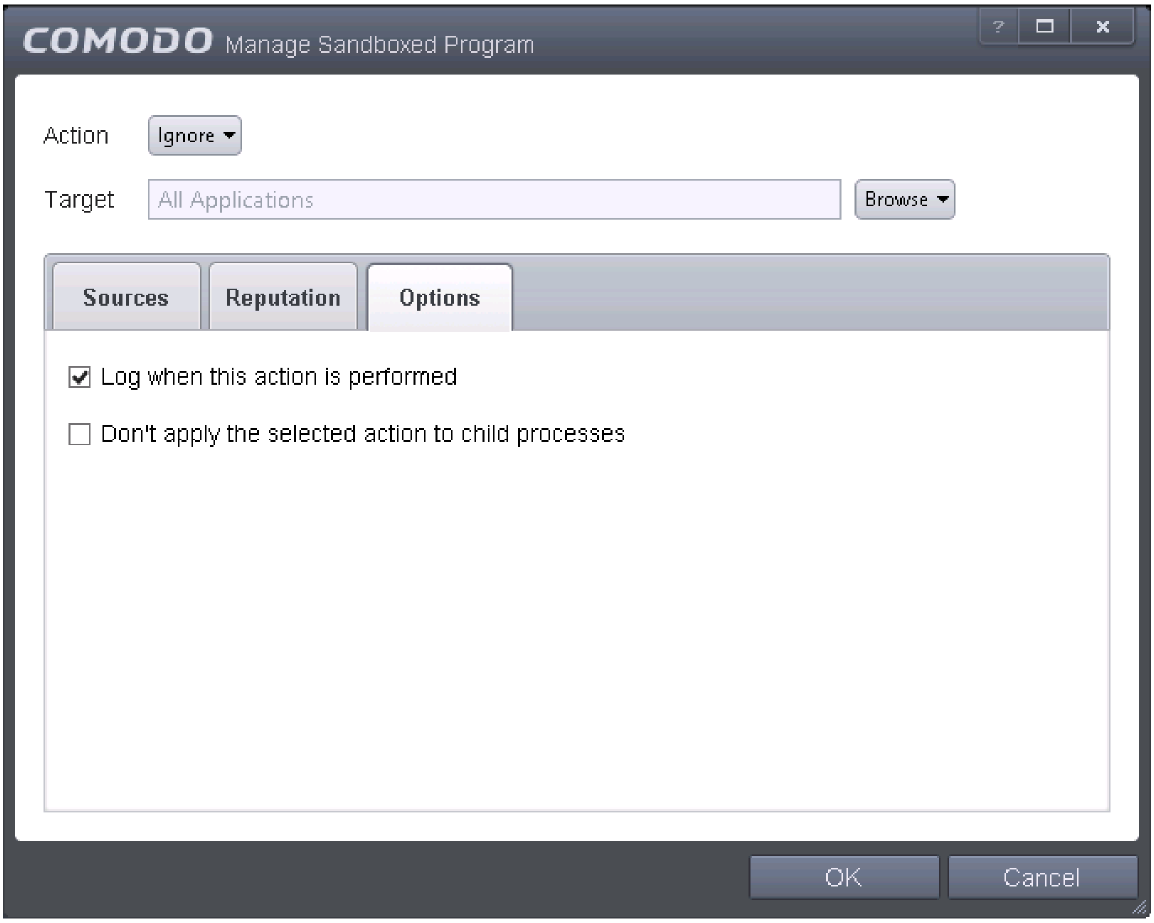
- Less Than – CAVS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (***Default and recommended = 1 hours)***
- More Than - CAVS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 1 hours)***

Select the category from the options. Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options.

If you want to just add the Sources and Reputation for a particular action as selected in **Step 1** without specifying the options, then click 'OK'. The default values for Options will be 'Log when this action is performed'. If required you can configure **Options** for the rule.

Step 5 – Select the Options

- Click the Options tab in the Manage Sandboxed Program interface.



☑ Log when this action is performed

□ Don't apply the selected action to child processes

By default, the 'Log when this action is performed' The options available for Ignore action are:

- **Log when this action is performed –** Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** – Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CAVS treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
    - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
    - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox rules individually applied as per their file rating.

The 'Skip child processes' option is available for the Ignore action only. For actions – Run Restricted and Run Virtually – the following options are available:

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Set Restriction Level** – When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
    - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(***Default***)
    - **Limited -** Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
    - **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited

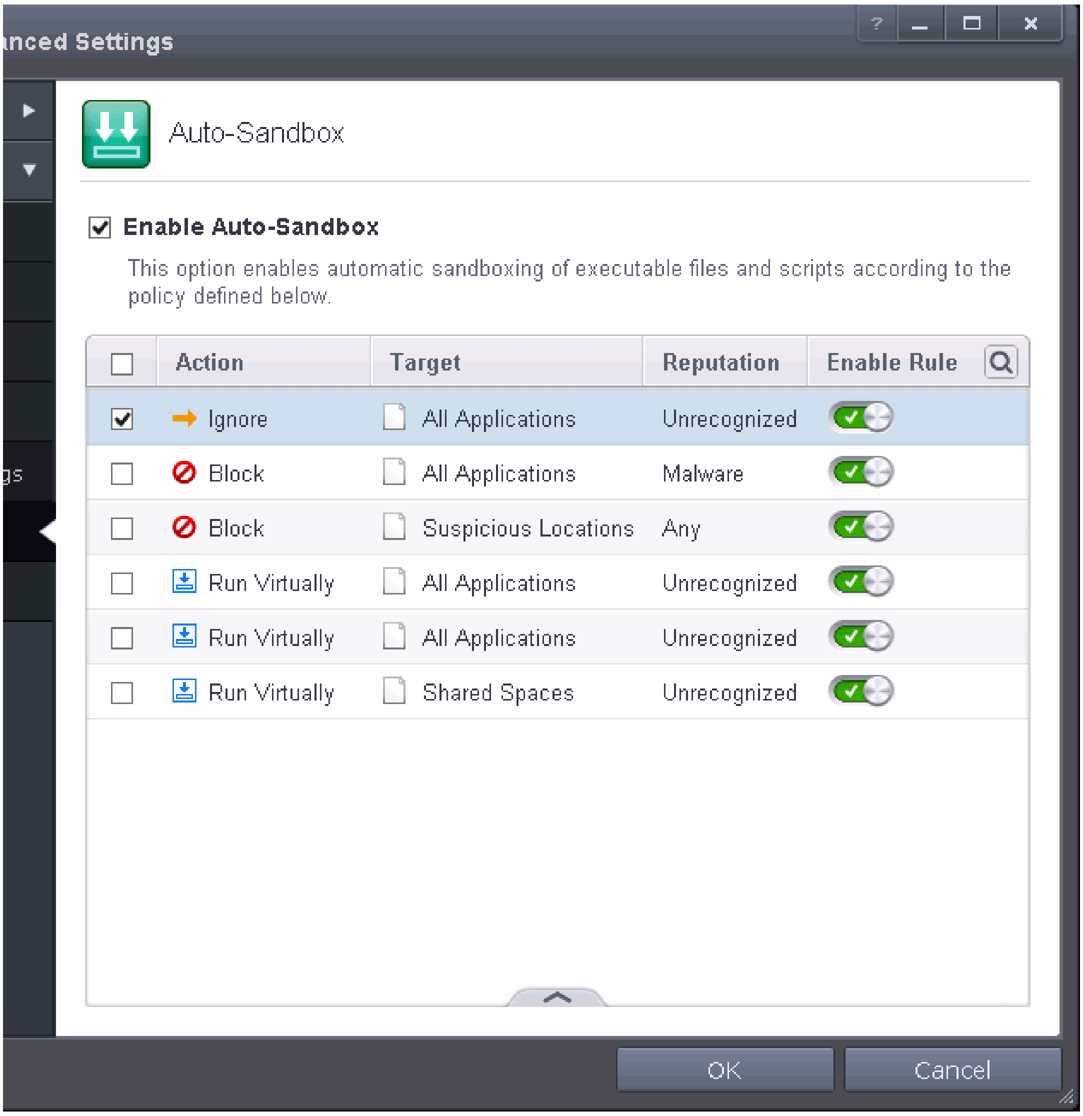
access rights. Some applications, like computer games, may not work properly under this setting.

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

- **Limit maximum memory consumption to** – Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** – Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For Block action, the following options are available:

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Quarantine program** – If checked, the programs will be automatically quarantined. Refer to the section **Manage Quarantined Items** for more information.



Auto-Sandbox

☑ **Enable Auto-Sandbox**

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
☑	Ignore	All Applications	Unrecognized	✓
□	Block	All Applications	Malware	✓
□	Block	Suspicious Locations	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	Shared Spaces	Unrecognized	✓

Choose the options and click 'OK'. The rule will be added and displayed in the list.

Editing an Auto-Sandbox Rule

- To edit an auto-sandbox rule, select it from the list and click 'Edit' from the options.

The Manage Sandboxed Program interface will be displayed. The procedure is similar to adding Adding an **Auto-**

Sandbox Rule.

- Click 'OK' to save the changes to the rule.

Important Note: Please make sure the auto-sandbox rules do not conflict. If it does conflict, the settings in the rule that is higher in the list will prevail.

5.2.3. Manage File Rating

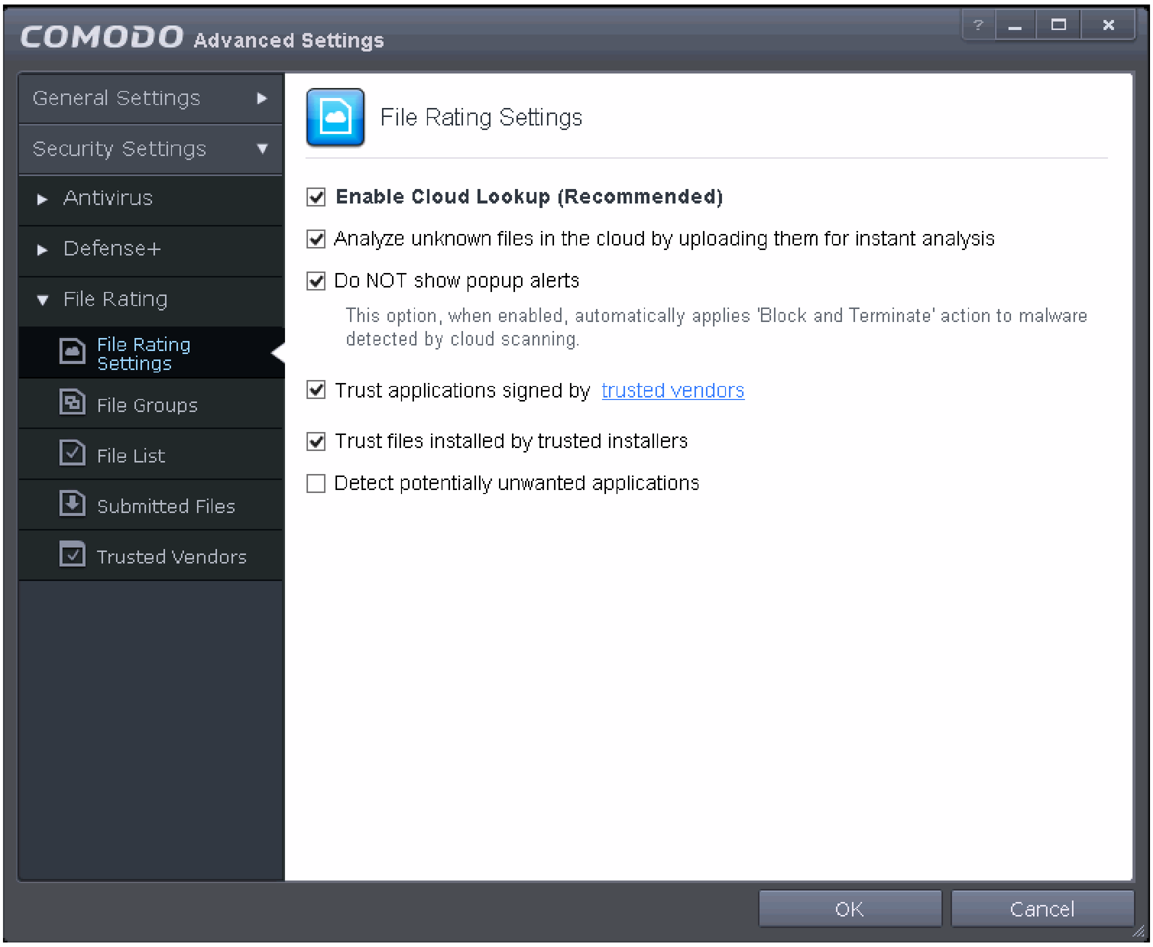
The CAVS rating system is a cloud-based file lookup service (FLS) that ascertains the reputation of files on your server. Whenever a file is first accessed, CAVS will check the file against our master whitelist and blacklists and will award it trusted status if:

- The application/file is awarded 'Trusted' status in the **local File List**;
- The application is from a vendor included in the **Trusted Software Vendors** list;
- The application is included in the extensive and constantly updated Comodo safelist.

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

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

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



File Rating Settings

☑ **Enable Cloud Lookup (Recommended)**

☑ Analyze unknown files in the cloud by uploading them for instant analysis

☑ Do NOT show popup alerts

This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

☐ Detect potentially unwanted applications

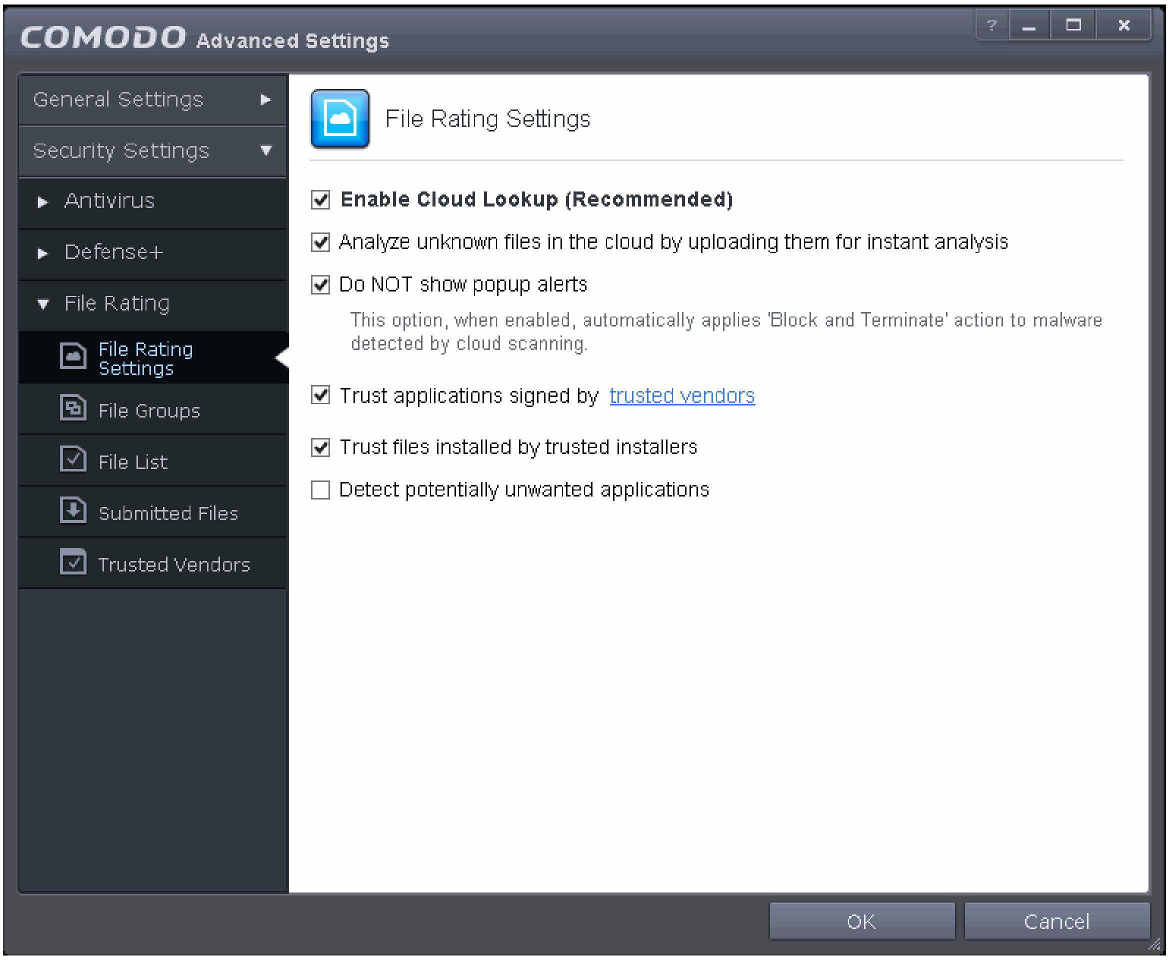
Click the following links to jump to the section you need help with:

- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **File Groups** - Create predefined groups of one or more file types.
- **File Lists** - View the list of programs. Applications and executable files in your computer with their file rating and manually add files to it
- **Submitted Files** - View the list of files submitted for analysis to Comodo.
- **Trusted Vendors** - View the list of trusted software vendors and manually add vendors

5.2.3.1. File Rating Settings

The File Rating Settings panel allows you to configure the overall behavior of File Rating feature of CAVS.

- The File Rating Settings panel can be accessed by clicking Security Settings > File Rating > File Rating Settings tab from 'Advanced Settings' interface



File Rating Settings

☑ **Enable Cloud Lookup (Recommended)**

☑ Analyze unknown files in the cloud by uploading them for instant analysis

☑ Do NOT show popup alerts

This option, when enabled, automatically applies 'Block and Terminate' action to malware detected by cloud scanning.

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

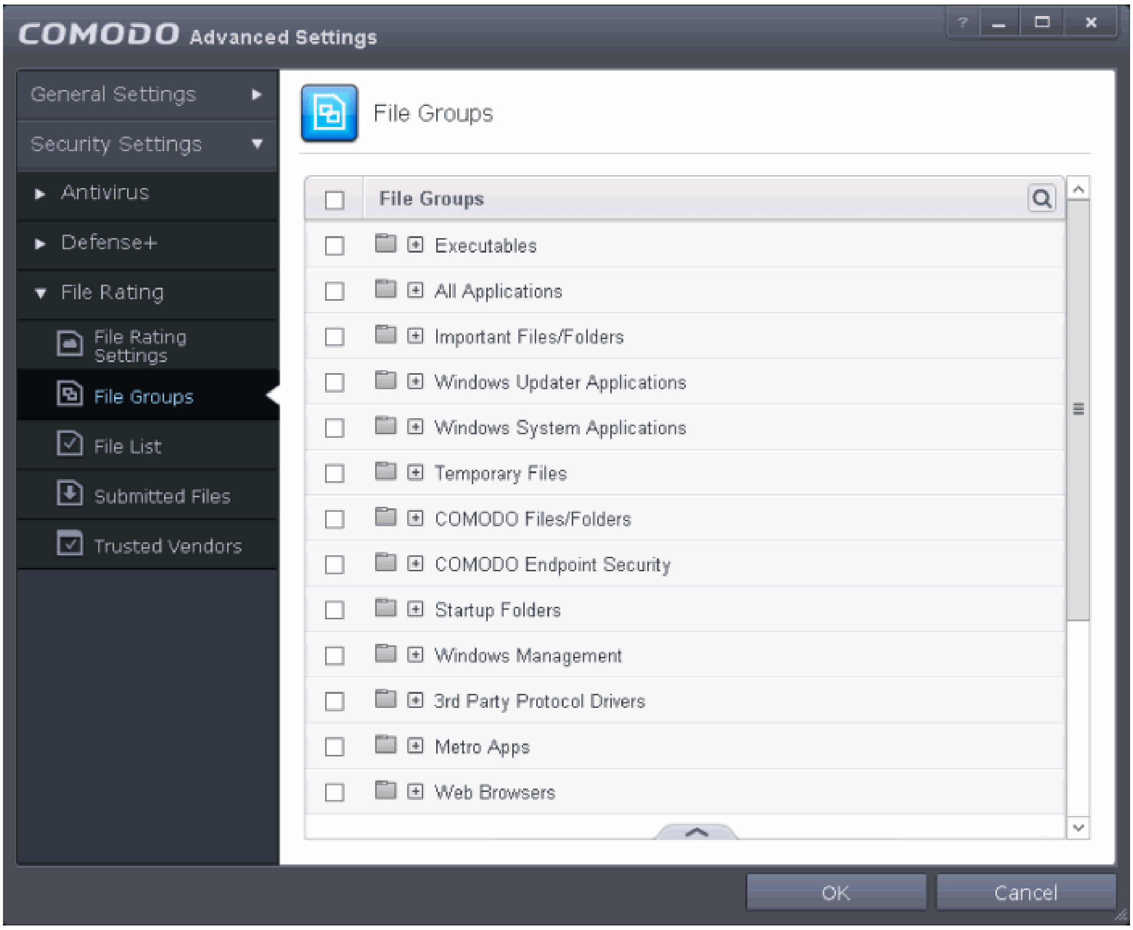
☐ Detect potentially unwanted applications

- **Enable Cloud Lookup -** Allows you to enable or disable File Rating.(***Default and recommended =Enabled***)
- **Analyze unknown files in the cloud by uploading them for instant analysis -** Instructs CAVS to upload files whose trustworthiness could not be assessed by cloud lookup to Comodo for analysis immediately. The experts at Comodo will analyze the file and add to the the whitelist or blacklist according to the analysis. (***Default =Enabled***)
- **Trust applications signed by trusted vendors -** When this option is enabled, CAVS will award trusted status to the executables and files that are digitally signed by vendors in the Trusted Vendors list using their code signing certificates. Clicking the words 'trusted vendors' will open the **Trusted Vendors** panel. (***Default =Enabled***)
- **Trust files installed by trusted installers -** When this option is enabled, CAVS will consider the executable and files stored by applications that are assigned with Installer or Updater rule under **HIPS Rules** or the applications. (***Default =Enabled***)
- **Detect potentially unwanted applications -** When this check box is selected, Antivirus scans also scans for applications that (i) a user may or may not be aware is installed on their computer and (ii) may functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet ***(Default =Disabled).***

5.2.3.2. File Groups

File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various CAVS functions such as adding them to Exclusions, HIPS Rules, Auto-Sandbox and so on. CAVS ships with a set of predefined File Groups and if required users can add new File Groups, edit and manage all the groups.

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

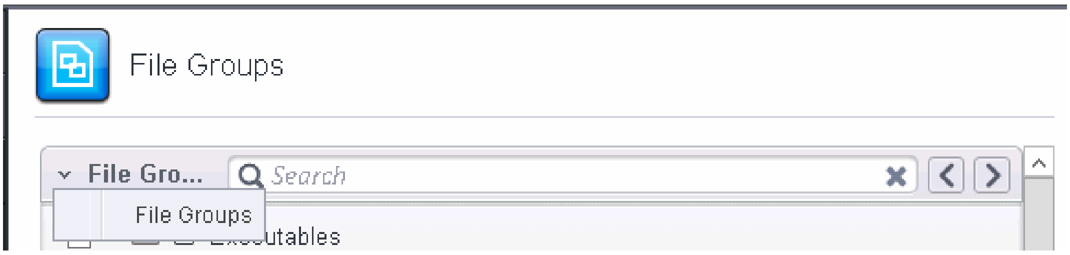


File Groups

- □ Executables
- □ All Applications
- □ Important Files/Folders
- □ Windows Updater Applications
- □ Windows System Applications
- □ Temporary Files
- □ COMODO Files/Folders
- □ COMODO Endpoint Security
- □ Startup Folders
- □ Windows Management
- □ 3rd Party Protocol Drivers
- □ Metro Apps
- □ Web Browsers

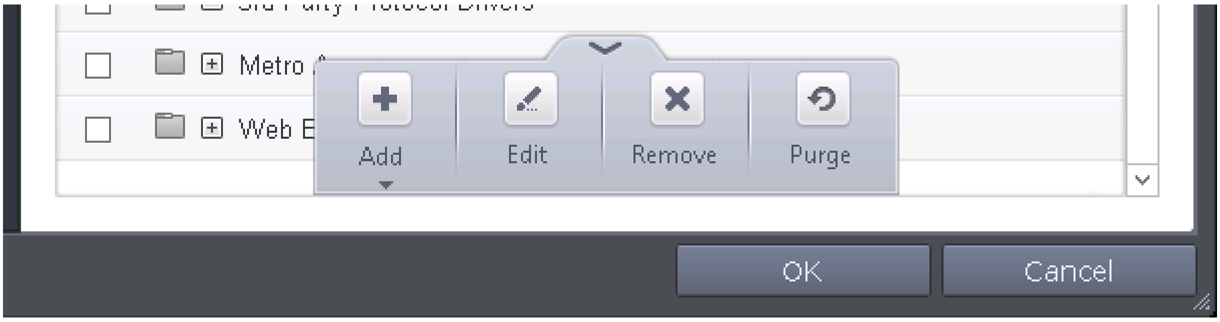
You can use the search option to find a specific name in the list.

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



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

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



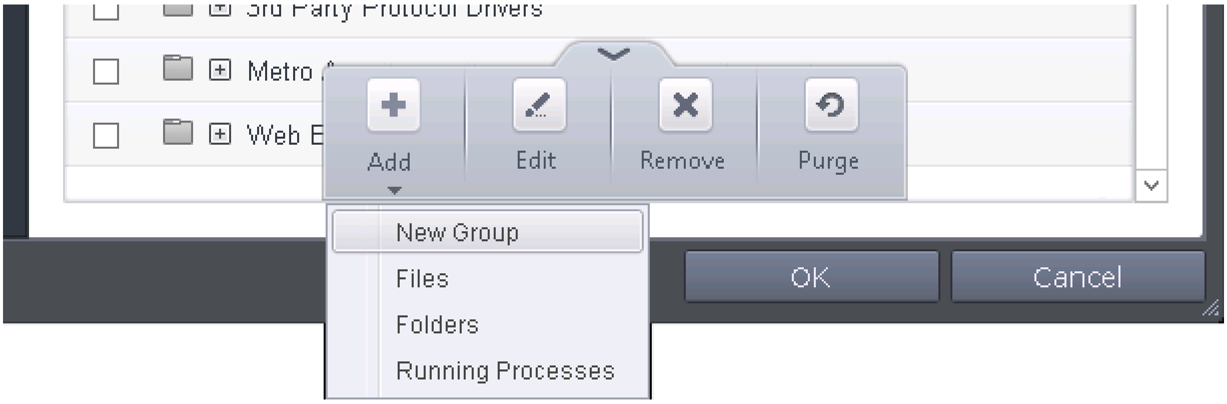
- **Add** – Allows you to add new groups, add individual files ,folders or running process to File Groups.
- **Edit** – Allows you to edit the name of file groups and edit file path of items under a file group.
- **Remove** – Allows you to delete a File Group or item(s) under a file group.
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

This interface allows you to

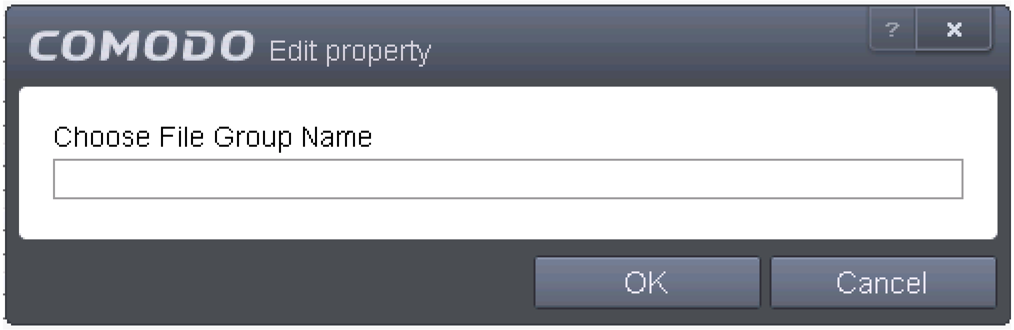
- **Create a new File Group**
- **Browsing to files or folders**
- **Selecting from currently running processes**

Adding a File Group

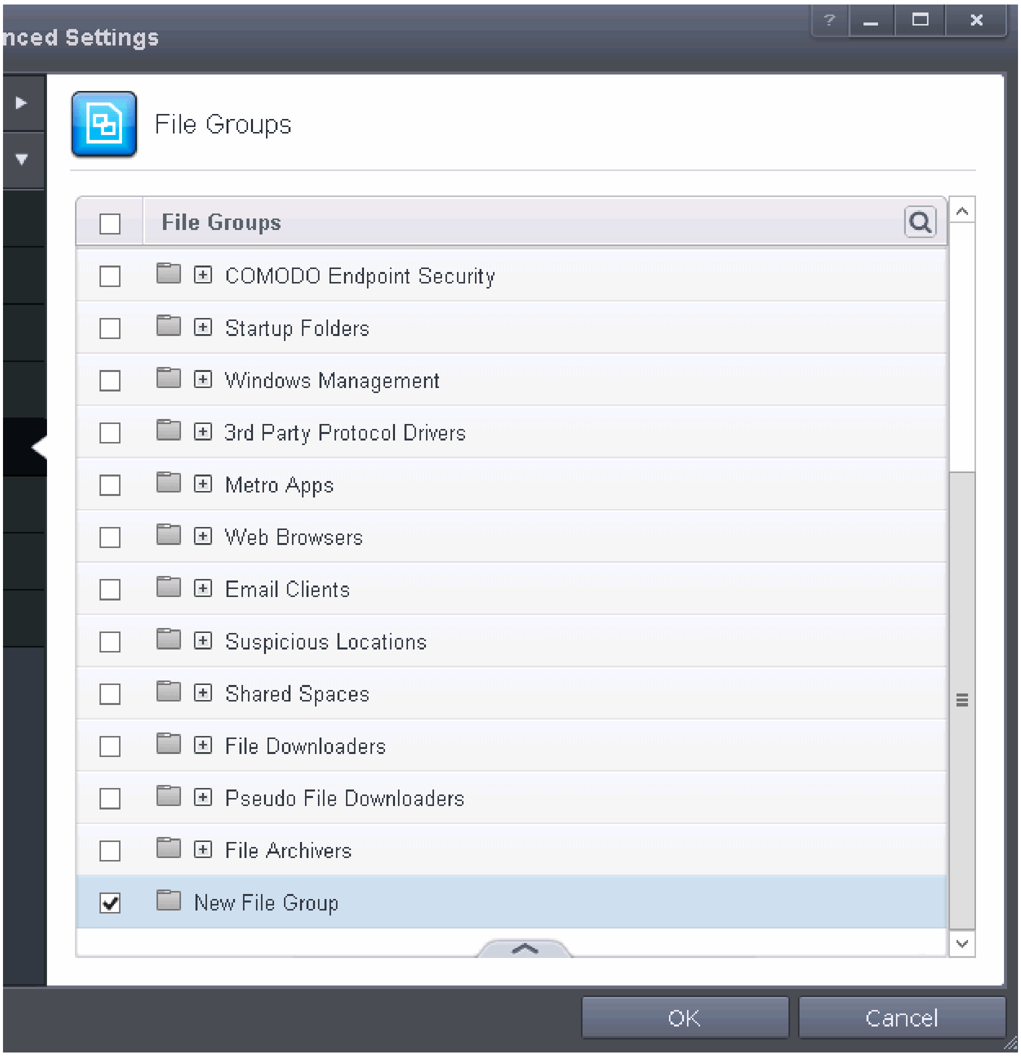
- To add a new File group or add files to an existing group, click the handle from the bottom and click 'Add'.



- Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK



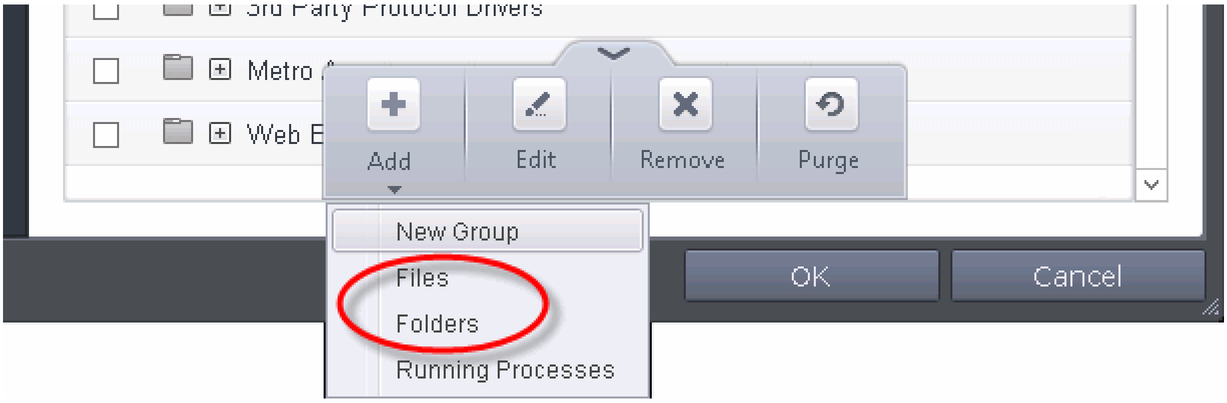
The File Group will be added and displayed in the list.



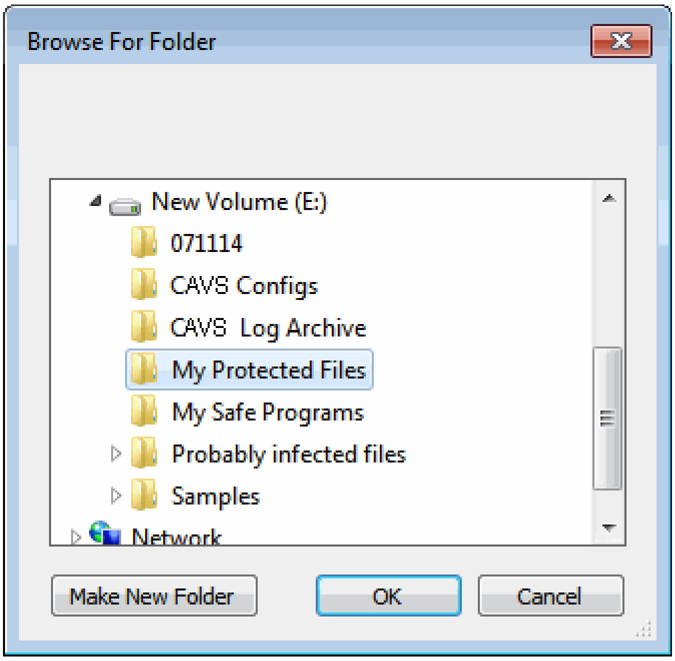
- To edit the name of an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog.

Add individual files or folder to a group

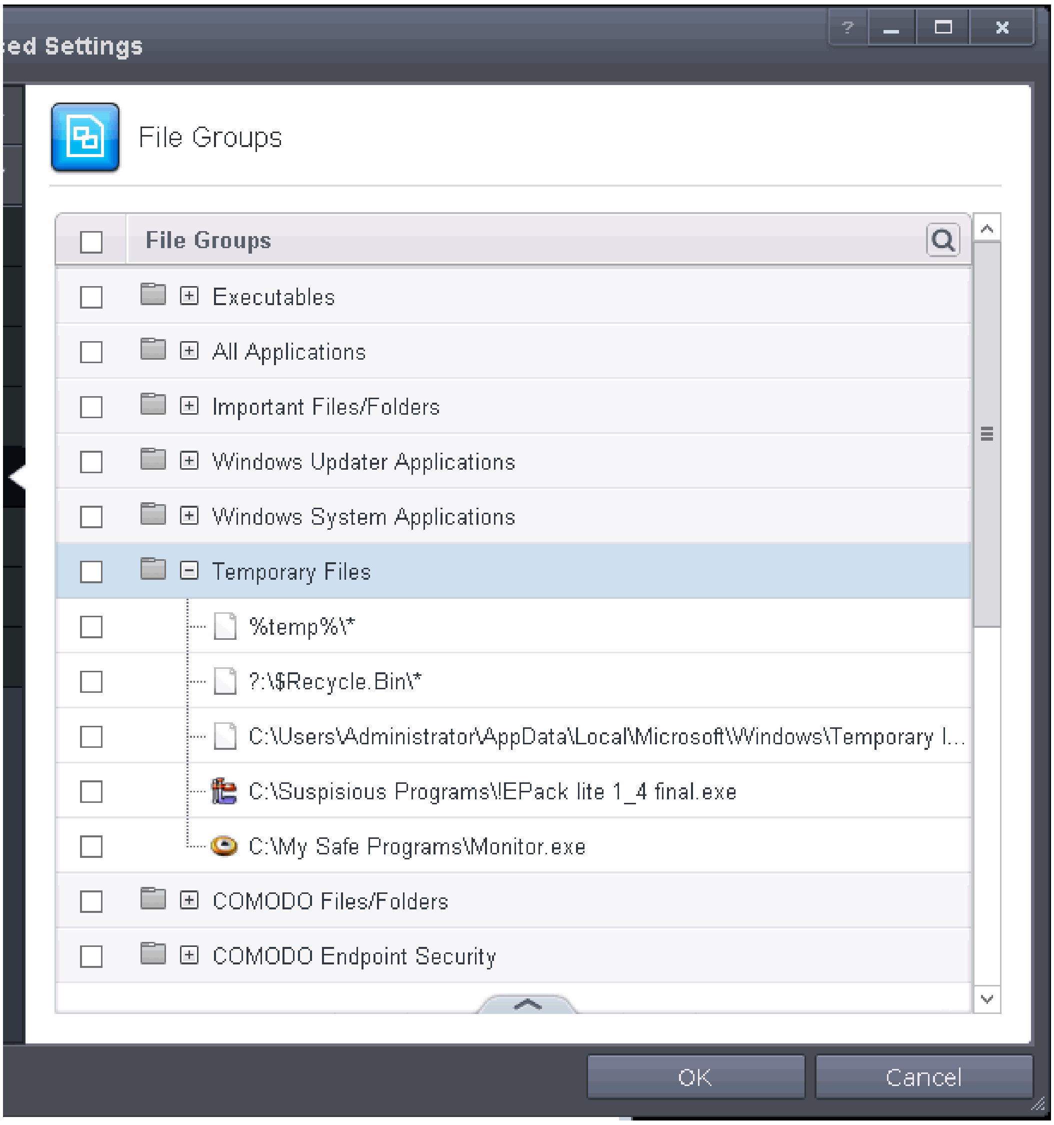
- Select the Group, click the handle and click Add. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes.
  - To add a file or folder, choose 'Files' or 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will open.



- Navigate to the individual file or folder you want to add to Files Groups and click OK



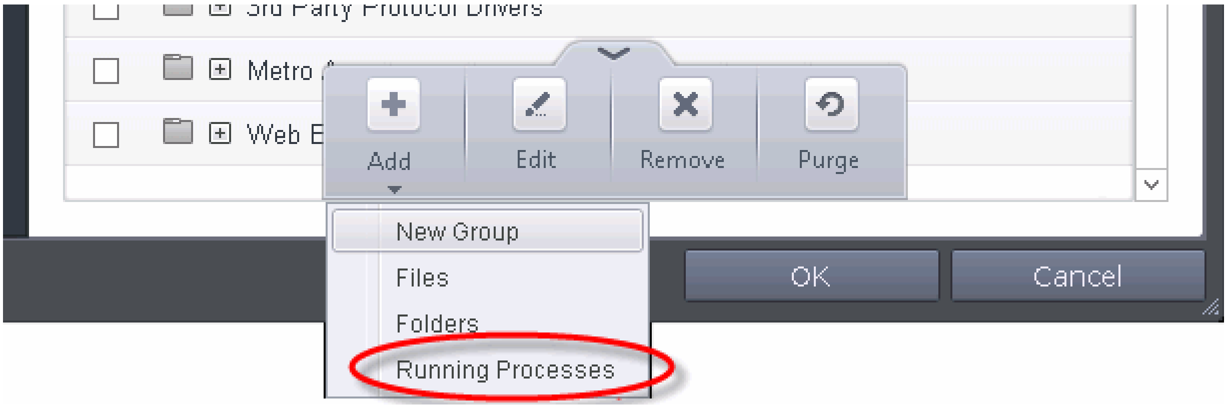
File Groups

- □ Executables
- □ All Applications
- □ Important Files/Folders
- □ Windows Updater Applications
- □ Windows System Applications
- □ Temporary Files
  - □ %temp%*
  - □ ?:\$Recycle.Bin*
  - □ C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary I...
  - □ C:\Suspisious Programs\!EPack lite 1_4 final.exe
  - □ C:\My Safe Programs\Monitor.exe
- □ COMODO Files/Folders
- □ COMODO Endpoint Security

The drive file/folder will be added to File Groups. Repeat the process to add more individual files or folders.

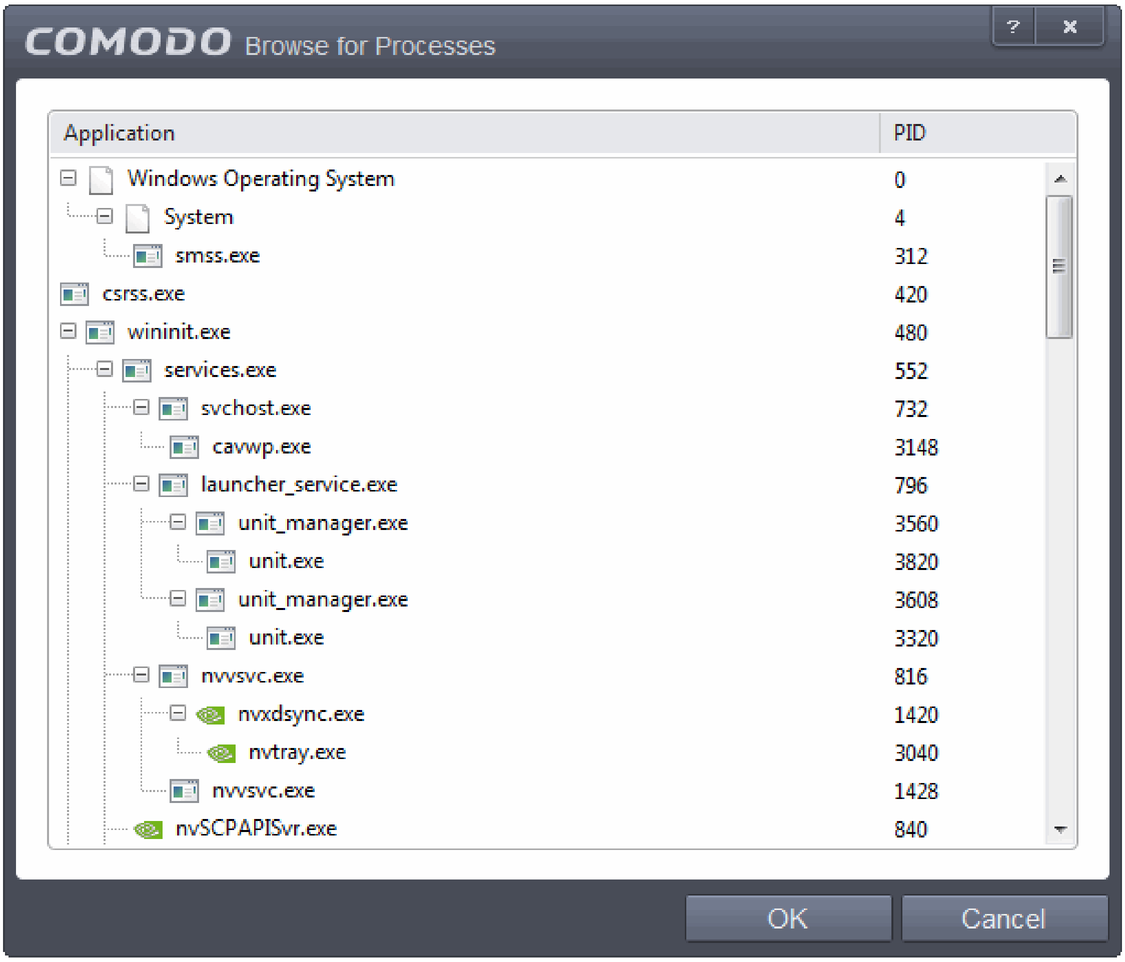
Add an application from a running processes

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



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

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

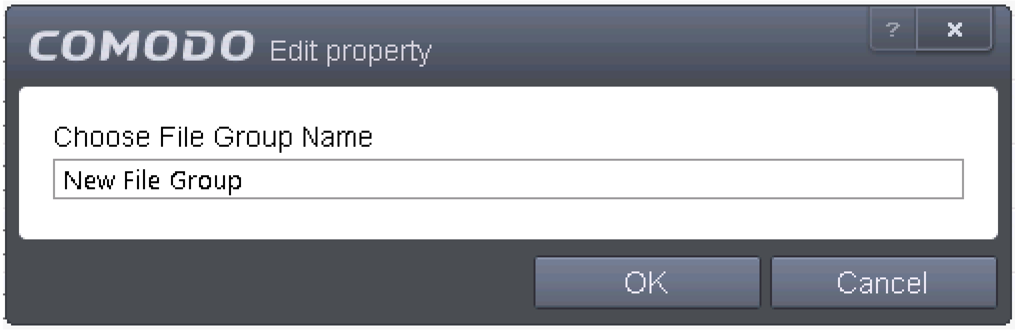


Application	PID
Windows Operating System	0
System	4
smss.exe	312
csrss.exe	420
wininit.exe	480
services.exe	552
svchost.exe	732
cavwp.exe	3148
launcher_service.exe	796
unit_manager.exe	3560
unit.exe	3820
unit_manager.exe	3608
unit.exe	3320
nvvsvc.exe	816
nvxdsync.exe	1420
nvtray.exe	3040
nvvsvc.exe	1428
nvSCPAPISvr.exe	840

The application will be added to File Groups.

To edit an item in the Files Groups list

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



Choose File Group Name

New File Group

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

To delete existing file group(s) individual file(s) from existing group

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

5.2.3.3. File List

The 'File List' pane displays a list of executable files, programs and applications and executable files discovered in your system with their file rating. CAVS rates the files as:

- **Trusted**
- **Unrecognized**
- **Malicious**

Trusted Files

Files with 'Trusted' rating are automatically given Defense+ trusted status. Files are identified as trusted in the following ways:

- Cloud-based file lookup service (FLS) - Whenever a file is first accessed, CAVS will check the file against our master whitelist and blacklists and will award it trusted status if:
    - The application is from a vendor included in the **Trusted Software Vendors** list;
    - The application is included in the extensive and constantly updated Comodo safelist.
- Administrator rating (Applicable only if your CAVS installation is remotely managed by your CESM administrator).
- User Rating – You can provide Trusted status to your files in two ways:
    - If an executable is unknown to the Defense+ safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, you could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted'.
    - You can assign 'Trusted' rating to any desired file from the Files List interface. Refer to the description of **changing the file rating** under the section **File Details** for more details.

  For the files assigned with 'Trusted' status by the user, CAVS generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. By this way, even if the file name is changed later, it will retain its Trusted status as the hash remains same.

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

  Creating your own list of Trusted Files allows you to define a personal safe list of files to complement the default Comodo safe list.

Unrecognized Files

Once installed, the HIPS watches all file system activity on your computer. Every new executable file introduced to the computer, is first scanned against the Comodo certified safe files database. If they are not safe, they are given 'Unrecognized' file rating for users to review and set their own rating. Apart from new executables, any executables that are modified are also given the 'Unrecognized' status.

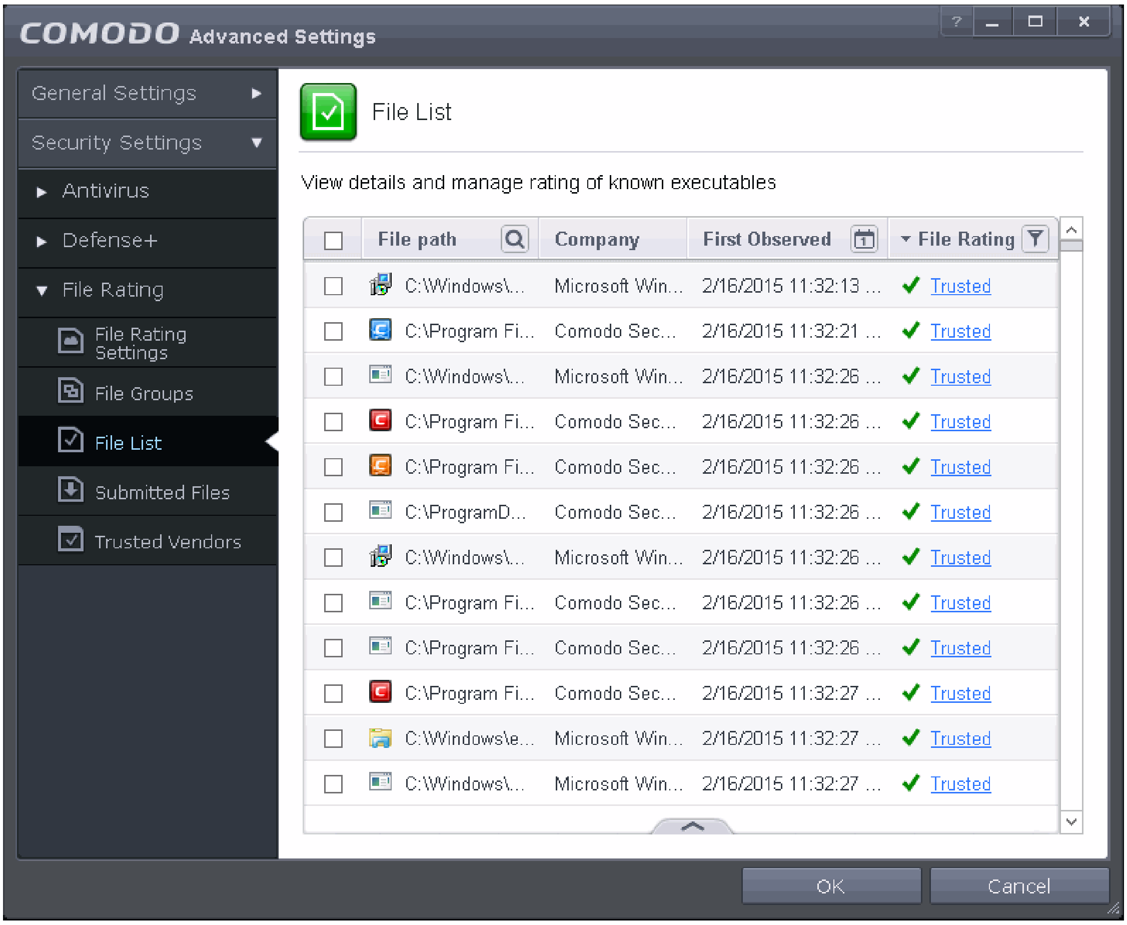
You can assess the pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be given the 'Trusted' rating. Refer to the description of **changing the file rating** for more details. You can also submit the files to Comodo for analysis. Experts at Comodo will analyze the files and add them to global white-list or black-list accordingly.

'Unrecognized Files' is specifically important while HIPS is in 'Clean PC Mode'. In Clean PC Mode, the files in 'Unrecognized Files' are NOT considered safe. For more information, please check '**Clean PC Mode' on the HIPS settings page**.

Malicious Files

Files that are identified as malicious from the FLS will be given 'Malicious' rating and will not be allowed to run by default.

The Trusted Files panel can be accessed by clicking 'Security Settings' > 'File Rating' > 'File List' from the Advanced Settings interface.



File List

View details and manage rating of known executables

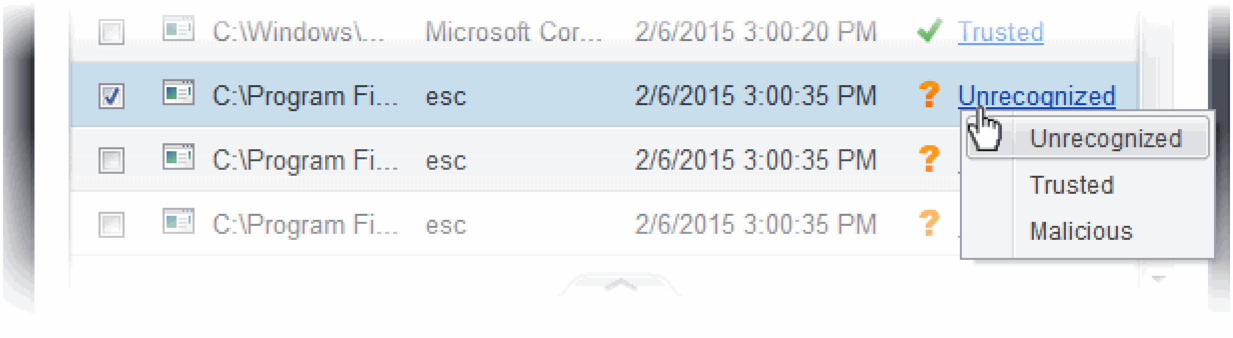
☐	File path	Company	First Observed	File Rating
☐	C:\Windows\...	Microsoft Win...	2/16/2015 11:32:13 ...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	2/16/2015 11:32:21 ...	✓ Trusted
☐	C:\Windows\...	Microsoft Win...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\ProgramD...	Comodo Sec...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\Windows\...	Microsoft Win...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	2/16/2015 11:32:26 ...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	2/16/2015 11:32:27 ...	✓ Trusted
☐	C:\Windows\e...	Microsoft Win...	2/16/2015 11:32:27 ...	✓ Trusted
☐	C:\Windows\...	Microsoft Win...	2/16/2015 11:32:27 ...	✓ Trusted

The pane displays the list of applications, programs and executable files discovered on your computer.

Column Descriptions:

- **File Path-** Indicates installation or storage path of the file;
- **Company –** Shows the publisher of the file;
- **First Observed -** Indicates date and time at which the file was first discovered by CAVS. For the files installed or stored before the installation of CAVS, it shows the first execution time of CAVS, when the file was discovered. For the files installed or stored after installation of CAVS, it shows when the file was stored.
- **File Rating -** Indicates the current CAVS rating of the file. The possible values are:
    - **Trusted**
    - **Unrecognized**
    - **Malicious**
    - The files are rated based on the following, in order of priority:

1. Administrator rating (Applicable only if your CAVS installation is remotely managed by your CESM administrator).
2. User rating (Rating as set by the user, if modified from the default rating)
3. FLS rating
    - The File rating can be modified by the user in two ways:
    - By clicking on the displayed rating in the row of the desired file and choosing the rating from the context sensitive menu.

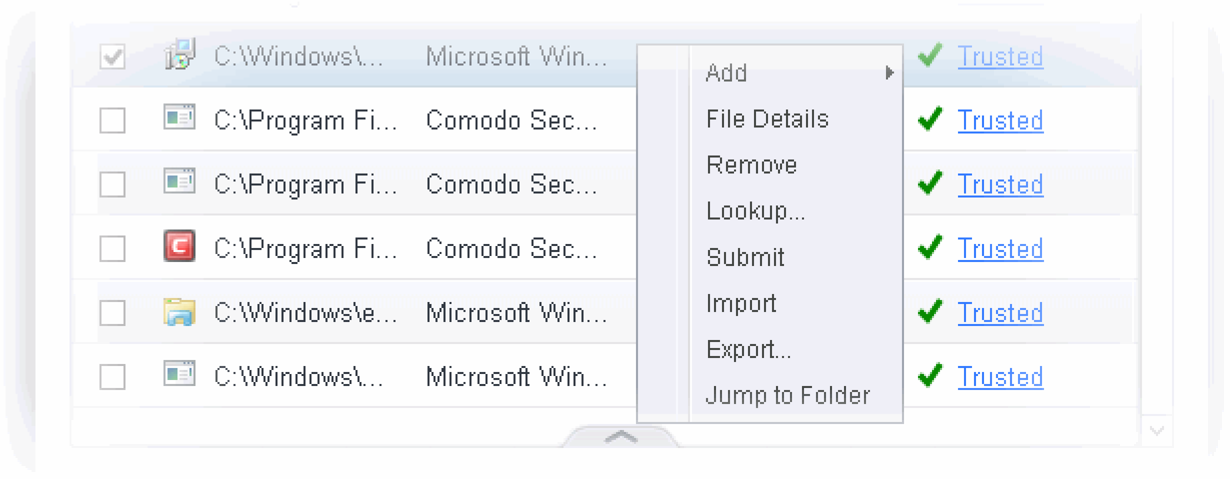


☐	C:\Windows\...	Microsoft Cor...	2/6/2015 3:00:20 PM	✓ Trusted
☑	C:\Program Fi...	esc	2/6/2015 3:00:35 PM	? Unrecognized
☐	C:\Program Fi...	esc	2/6/2015 3:00:35 PM	?
☐	C:\Program Fi...	esc	2/6/2015 3:00:35 PM	?

- From the 'File Details' dialog of the desired file by selecting it, clicking the handle from the bottom and choosing 'File Details' from the options. Refer to the description of **changing the file rating** under the section **File Details** for more details.

Context Sensitive Menu

Right clicking on a file opens a context sensitive menu that allows you to view the 'File Details' dialog, remove the file from the list, submit the file to Comodo for analysis and more.



☑	C:\Windows\...	Microsoft Win...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	✓ Trusted
☐	C:\Program Fi...	Comodo Sec...	✓ Trusted
☐	C:\Windows\e...	Microsoft Win...	✓ Trusted
☐	C:\Windows\...	Microsoft Win...	✓ Trusted

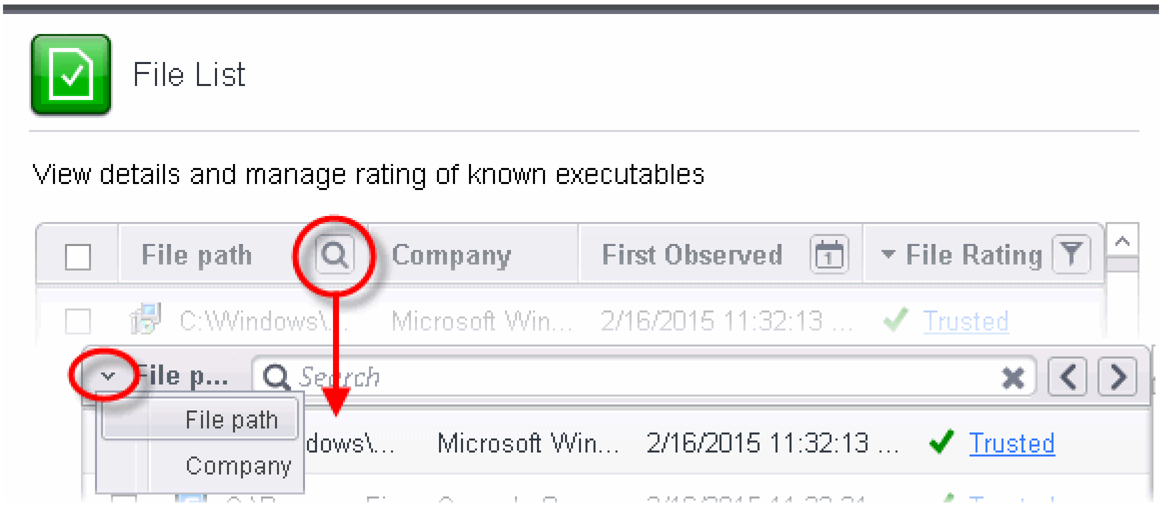
- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the file submission process.
- **Import** - Enables you import a file list from an XML file
- **Export** - Enables you export the current file list with existing ratings to an XML file
- **Jump to Folder** – Opens the folder containing the file in Windows Explorer.

Searching and Filtering options

You can use the search option to find a specific file based on the file path, file name or the publisher, from the list. Also, you can filter the list of files based on the installation/storage date and File rating.

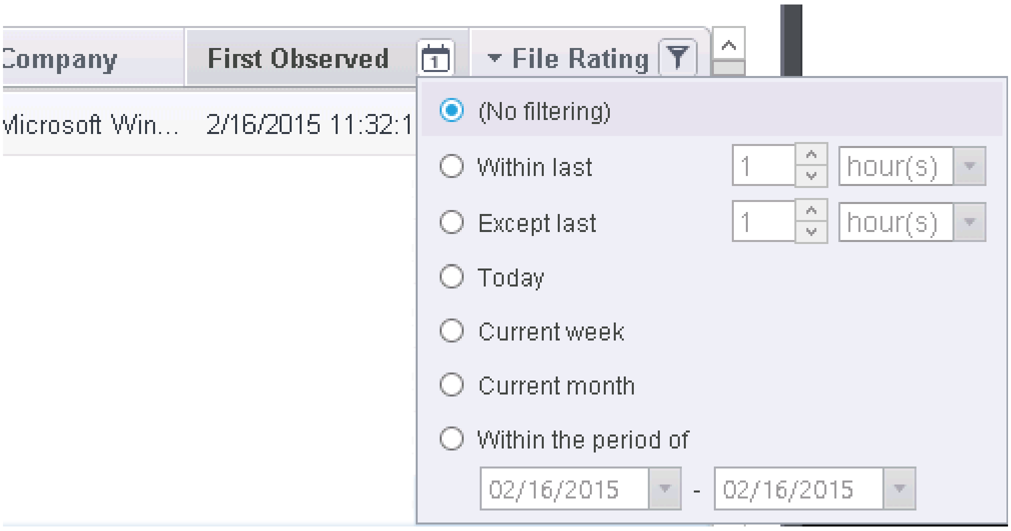
To use the search option, click the search 🔍 icon at the far right in the 'File path' column header.

- Click the chevron on the left side of the column header and select the search criteria from the drop-down.

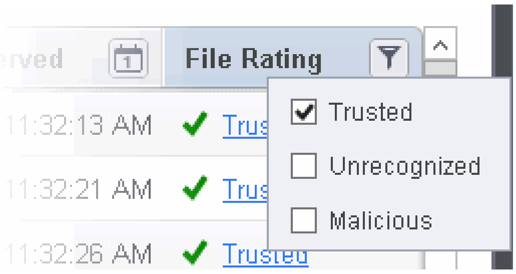


- Enter the file path or the name of company in part or full as per the selected criteria in the search field and press 'Enter' to begin the search.

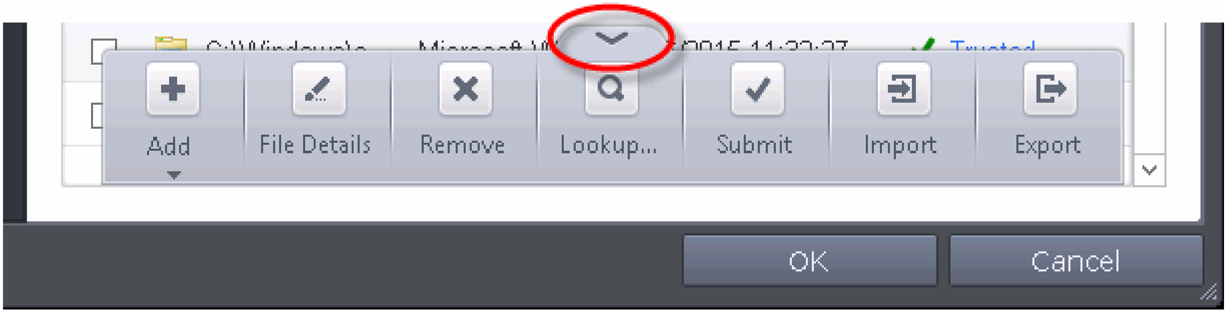
- To filter the list based on the date of installation or storage of the files, click the calendar icon at the right of the 'First Observed' column header and choose the time/date/period.



- To filter the list based on the file rating, click the funnel icon at the right of the 'File Rating' column header and select the ratings to display only the files with the selected rating(s).



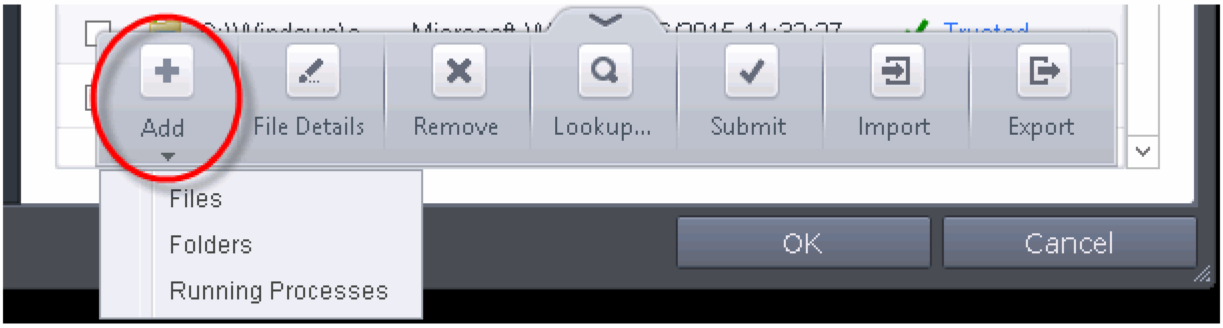
Clicking the handle at the bottom of the panel opens the following options:



- **Add** - Allows you to manually add files to the 'File List' with user defined rating
- **File Details** - Opens the 'File Details' dialog enabling you to view the details of the file and set user defined rating
- **Remove** - Allows you to remove files from 'File List'.
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the file submission process.
- **Import** - Enables you import a file list from an XML file
- **Export** - Enables you export the current file list with existing ratings to an XML file

To manually add files to 'File list'

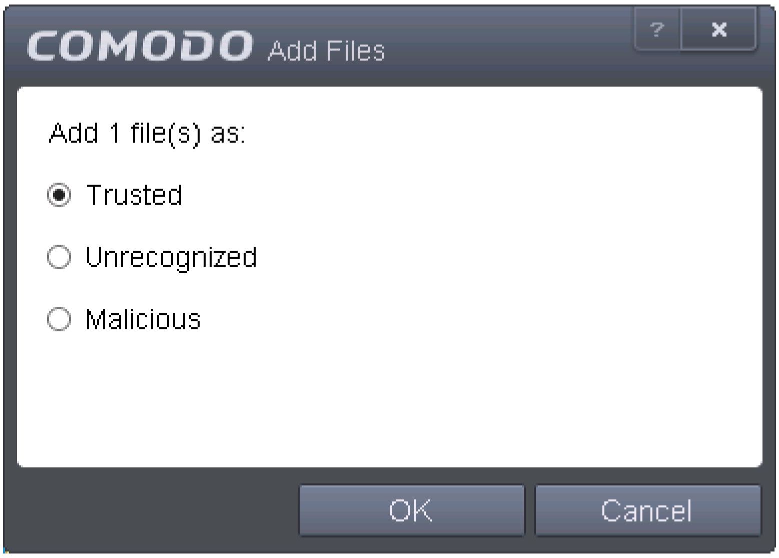
- Click the handle from the bottom and choose 'Add'



Tip: Alternatively, right click inside the File List page and choose 'Add' from the context sensitive menu.

- You can add files to the File list by three ways:
  - **Files** - Allows you to navigate to the file or executable of the program you wish to add and assign a rating.
  - **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'File List' with the rating you assign.
  - **Running Processes** - Allows you to select a currently running process. On selecting a process, the parent application, which invoked the process will be added to 'File List' with the rating you assign.

Once you have chosen the file(s) or the folder, you can assign the rating for the file(s) to be added.



Add 1 file(s) as:

● Trusted

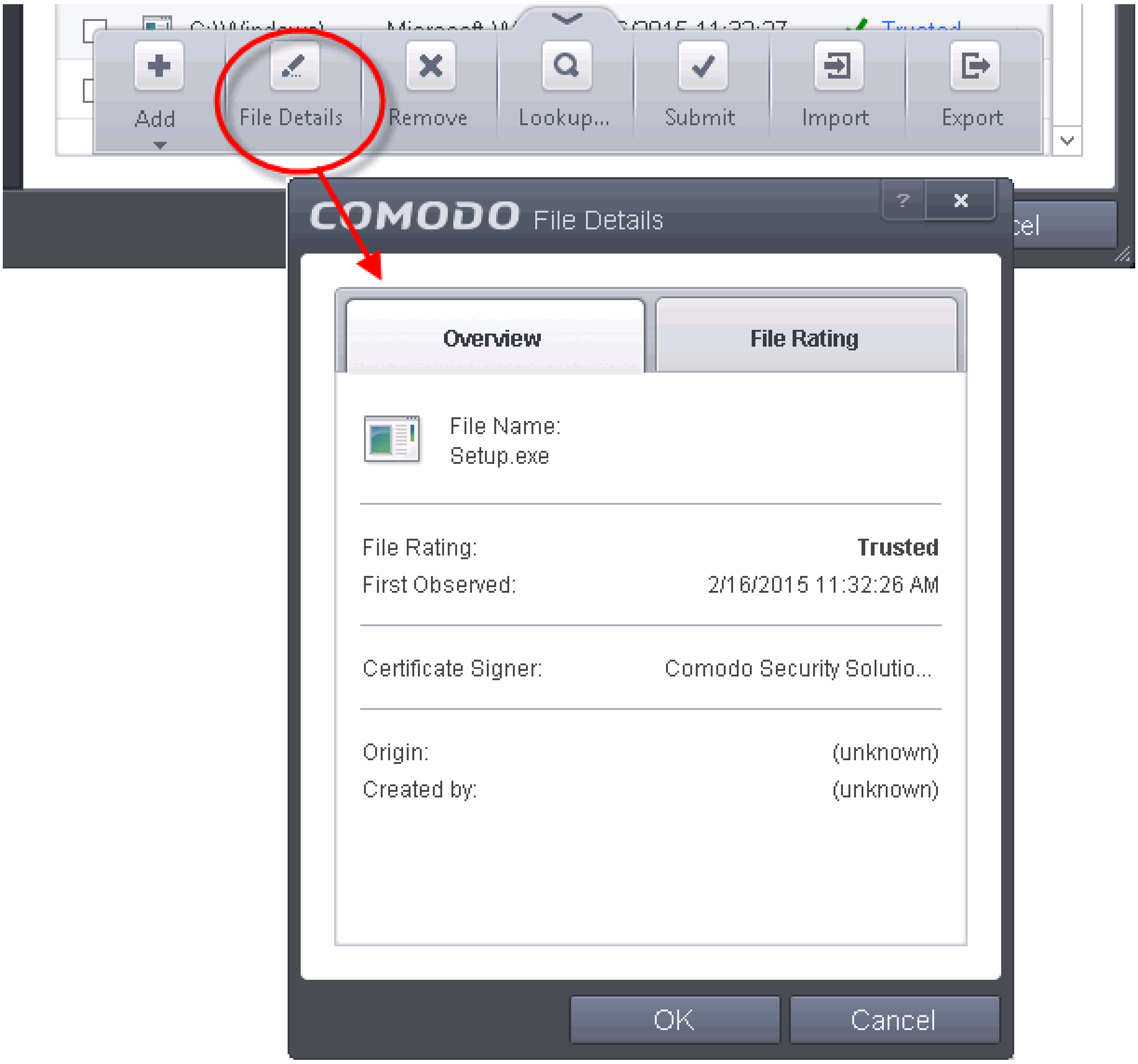
○ Unrecognized

○ Malicious

- Choose the rating to be assigned to the file(s). The available options are:
  - Trusted – The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
  - Unrecognized – The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
  - Malicious – The file will not be allowed to run.
  - Click OK in the 'Add Files' dialog
- Click 'OK' in the 'Advanced Settings' for your changes to take effect.

To view the 'File Details' and change the rating

- Choose the file to view its details
- Click the handle from the bottom and choose 'File Details'



File Name:
Setup.exe

File Rating: **Trusted**

First Observed: 2/16/2015 11:32:26 AM

Certificate Signer: Comodo Security Solutio...

Origin: (unknown)

Created by: (unknown)

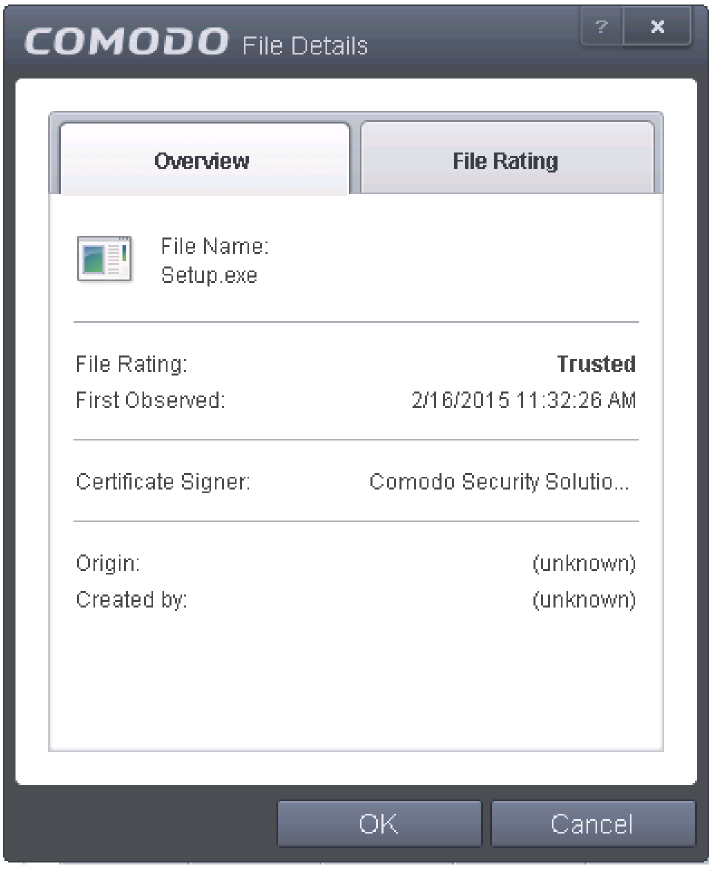
Tip: Alternatively, right click on the selected file inside the File List page and choose 'File Details' from the context sensitive menu.

The 'File Details' dialog will open. The dialog contains two tabs:

- **Overview**
- **File Rating**

Overview

The Overview tab displays the general details of the file and the publisher details.



File Name: Setup.exe

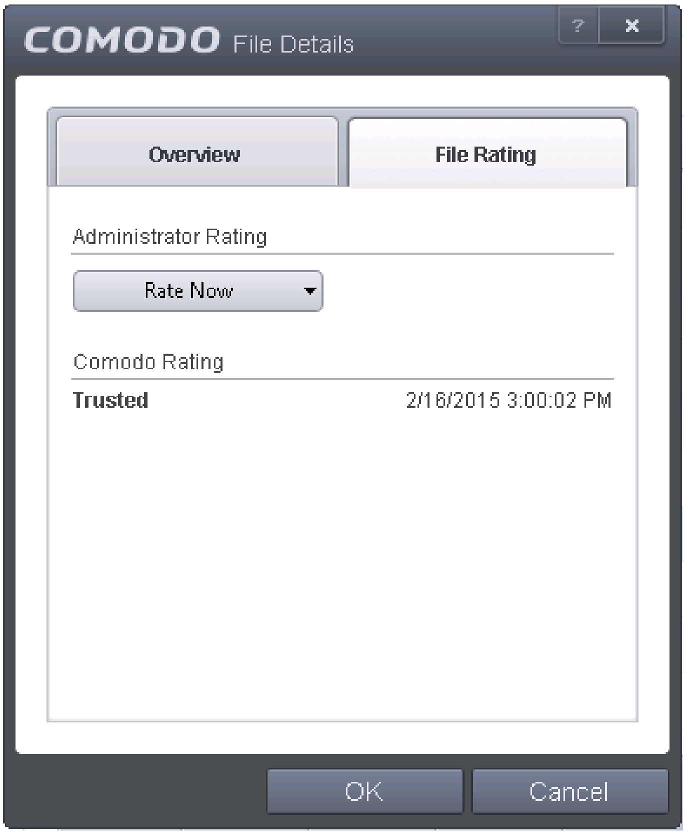
File Rating: **Trusted**
First Observed: 2/16/2015 11:32:26 AM

Certificate Signer: Comodo Security Solutio...

Origin: (unknown)
Created by: (unknown)

- Clicking the file name opens the Windows 'File Properties' dialog.
- Clicking 'Jump to folder' opens the folder containing the file in Windows Explorer, with the respective file selected.

File Rating



Administrator Rating

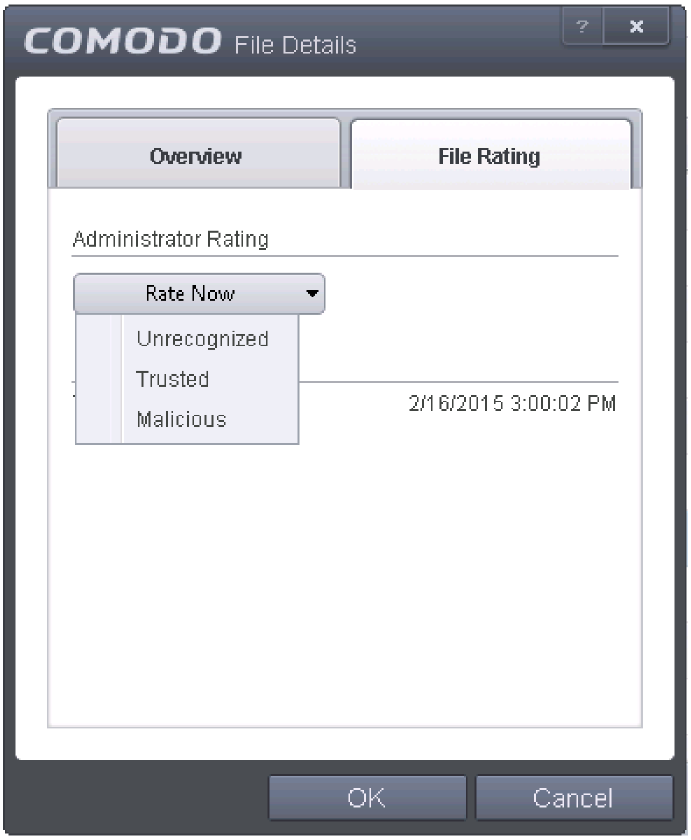
Comodo Rating
Trusted 2/16/2015 3:00:02 PM

The 'File Rating' tab enables you to change the current rating of the file and displays the current rating as per the analysis result from Comodo.

Note: If the CAVS installation is remotely managed by the CESM server on your network your Administrator's file rating for individual file will override your user file rating.

To change the user rating of the file

- Select the file from the 'File List' pane, click the handle from the bottom and choose File Rating from the options
- Click the File Rating tab from the File Details tab
- Click 'Rate Now' and choose the rating from the drop-down



The options available are:

- Trusted – The file(s) will be assigned the 'Trusted' status and allowed to run without any alerts
- Unrecognized – The file(s) will be assigned the 'Unrecognized' status. Depending on your HIPS settings, the file(s) will be allowed to run with an alert generation.
- Malicious – The file will not be allowed to run.
- Click 'OK' in the 'Files Details' dialog
- Click 'OK' in the 'Advanced Settings' interface to save your settings.

To remove files(s) from the File list

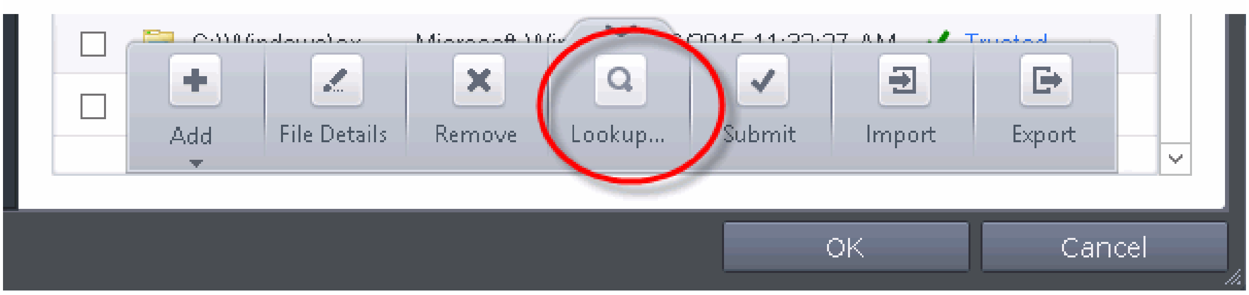
- Select the file(s) to be removed from the 'File List' pane. You can select several entries to be removed at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Remove'. The file is only removed from the list and not deleted from your system.

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Remove' from the context sensitive menu.

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

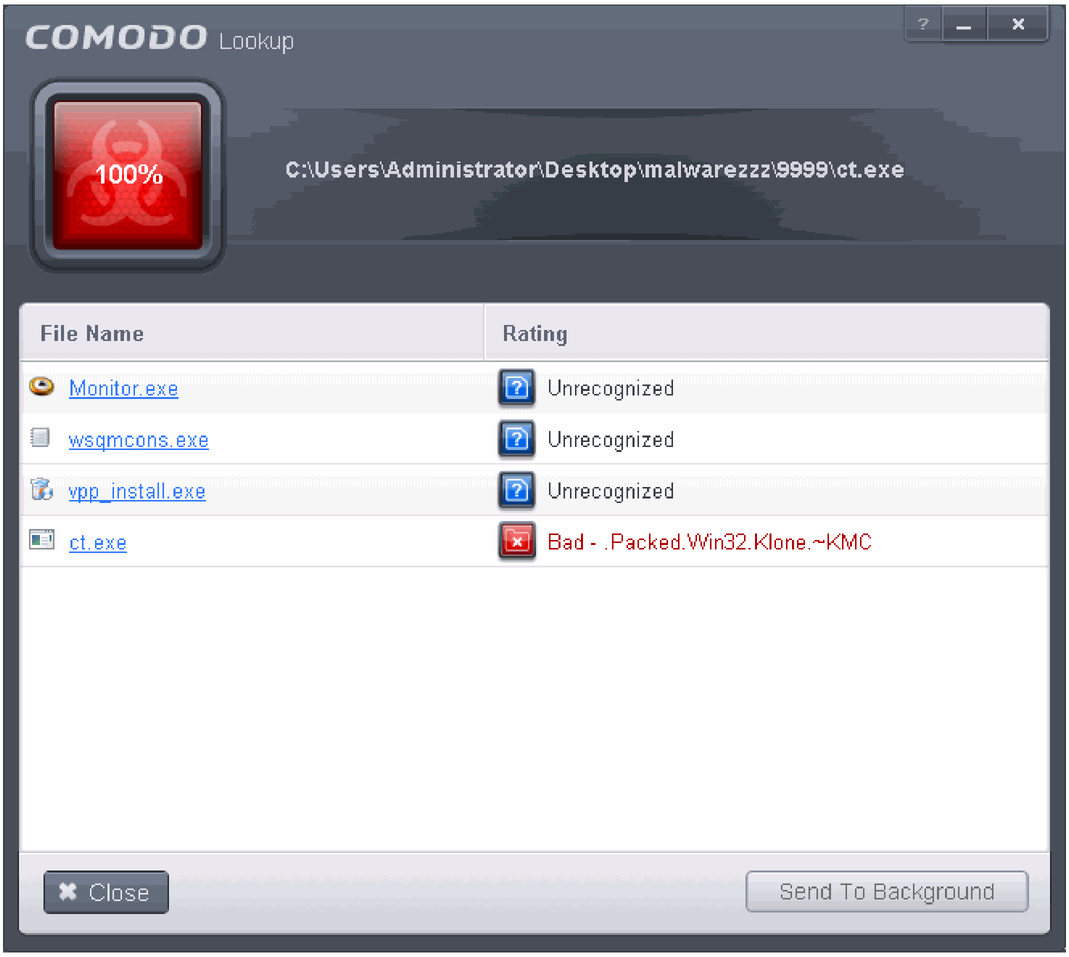
To perform an online lookup for files

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



Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Lookup' from the context sensitive menu.

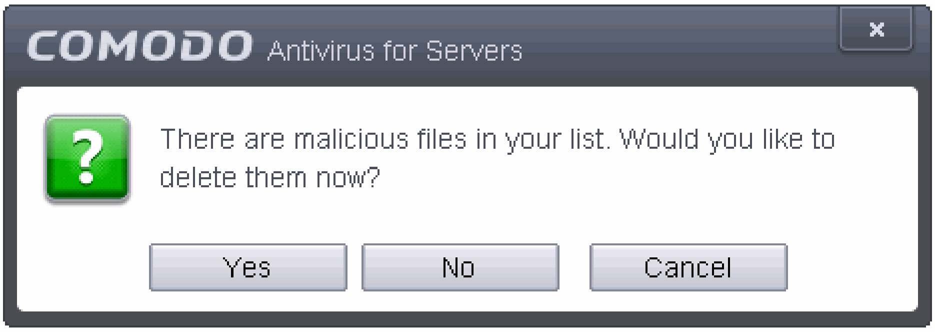
Comodo servers will be contacted immediately to conduct a search of Comodo's master safe list database to check if any information is available about the files in question and the results will be displayed.



C:\Users\Administrator\Desktop\malwarezzz\9999\ct.exe

File Name	Rating
Monitor.exe	Unrecognized
wsqmcons.exe	Unrecognized
vpp_install.exe	Unrecognized
ct.exe	Bad - .Packed.Win32.Klone.~KMC

If any malicious or unwanted file(s) is/are found, you will be given an option to delete the file from your computer on closing the dialog.



There are malicious files in your list. Would you like to delete them now?

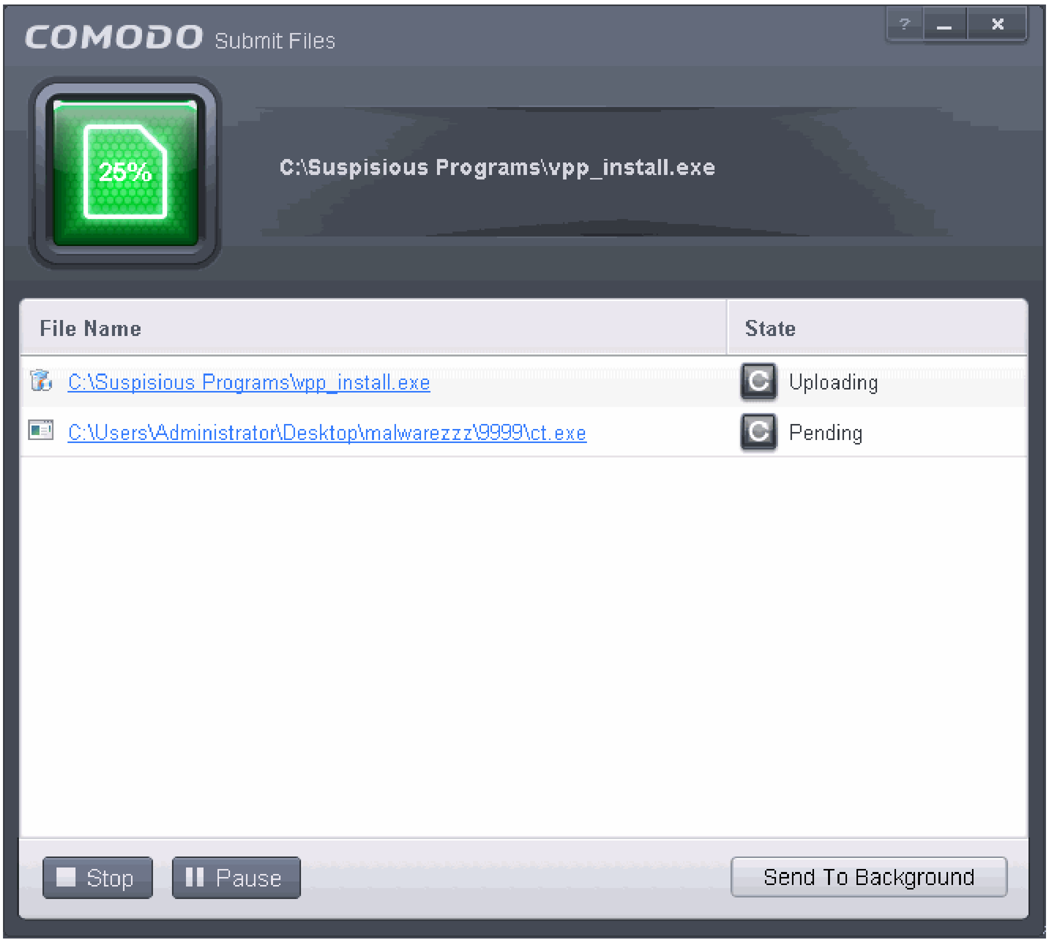
- Click 'Yes' to permanently delete the malicious file(s) from your computer.

- If a file is found to be safe, it will be indicated as 'Trusted' with a green icon. You can change its rating from the File Details dialog. Refer to the description of **changing the file rating** under the section **File Details** for more details.
- If no information is available, it will be indicated as 'Unknown' with a yellow icon. You can submit the file to Comodo for analysis. Refer to the **explanation below** for more details.

To manually submit files to Comodo

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

Tip: Alternatively, right click on a selected file inside the 'File List' page and choose 'Submit' from the context sensitive menu.



File Name	State
C:\Suspisious Programs\vpp_install.exe	Uploading
C:\Users\Administrator\Desktop\malwarezzz\9999\ct.exe	Pending

You can view the list of files you submitted so far, from the **Submitted Files** panel.

Exporting and Importing the File List

You can export the list of files with their currently assigned file ratings to an XML file and store the list on a safe place. This is useful to restore your File List, in case you are reinstalling the CAVS application for some reasons.

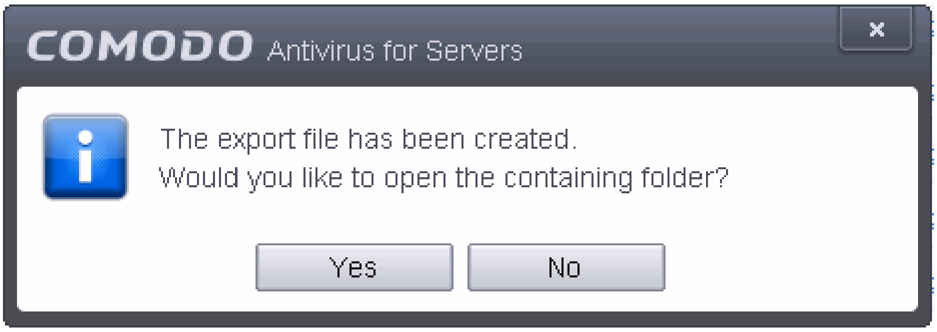
To export the File List

- Click the handle from the 'File List' pane and choose 'Export' from the options

Tip: Alternatively, right click inside the 'File List' page and choose 'Export' from the context sensitive menu.

- Navigate to the location to store the XML file containing the file list and click 'Save'.

The file will be created and saved. You will be given an option to view the folder containing the XML file for confirmation.



COMODO Antivirus for Servers

The export file has been created.
Would you like to open the containing folder?

To import a saved file list

- Click the handle from the 'File List' pane and choose 'Import' from the options

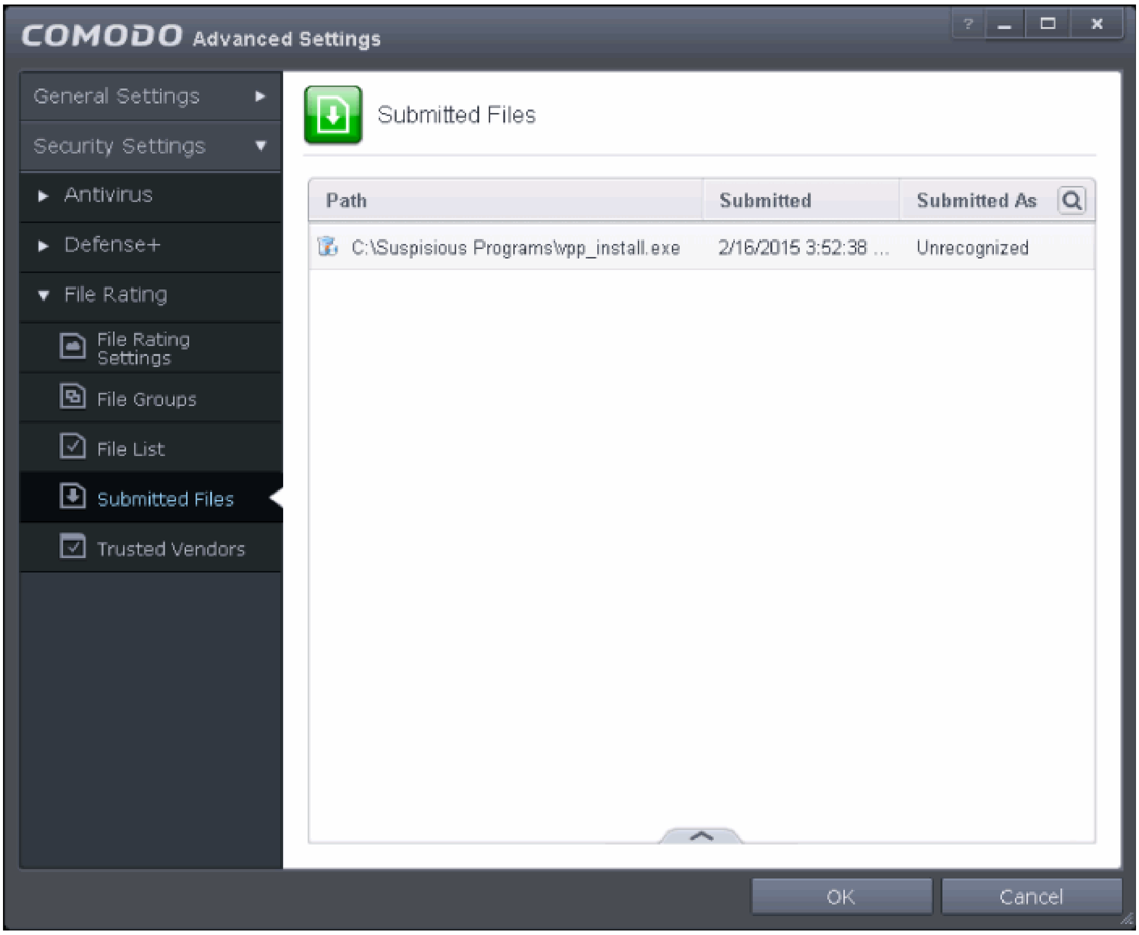
Tip: Alternatively, right click inside the 'File List' page and choose 'Import' from the context sensitive menu.

- Navigate to the location of the XML file containing the file list and click 'Open'.

The 'File List' will be populated as per the imported 'File List'.

5.2.3.4. Submitted Files

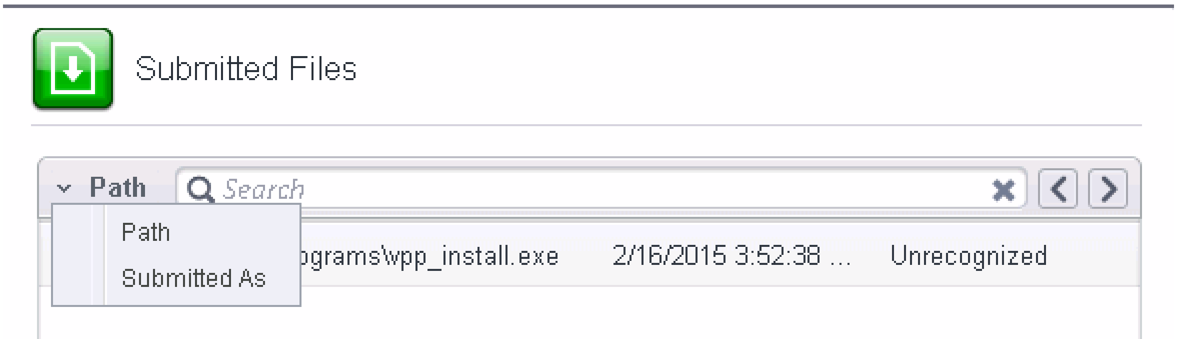
The Submitted Files panel displays a list of files you have submitted so far for analysis to Comodo.



Path	Submitted	Submitted As
C:\Suspisious Programs\wpp_install.exe	2/16/2015 3:52:38 ...	Unrecognized

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

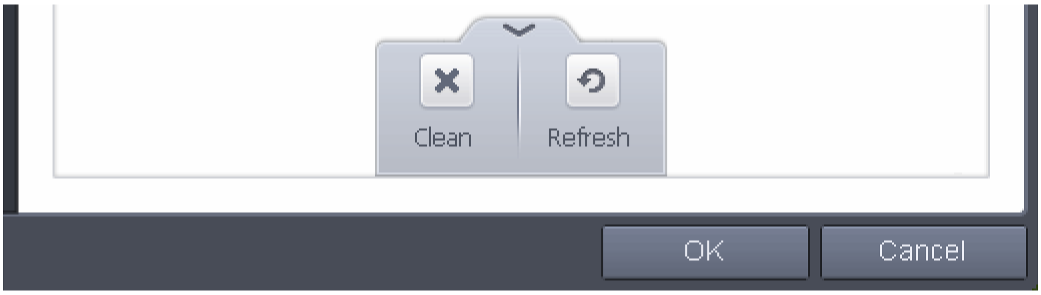
To use the search option, click the search 🔍 icon at the far right in the column header.



...ograms\wpp_install.exe | 2/16/2015 3:52:38 ... | Unrecognized

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

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



- **Clean** - Clears the list
- **Refresh** - Reloads the list to add items that are submitted recently

5.2.3.5. Trusted Vendors List

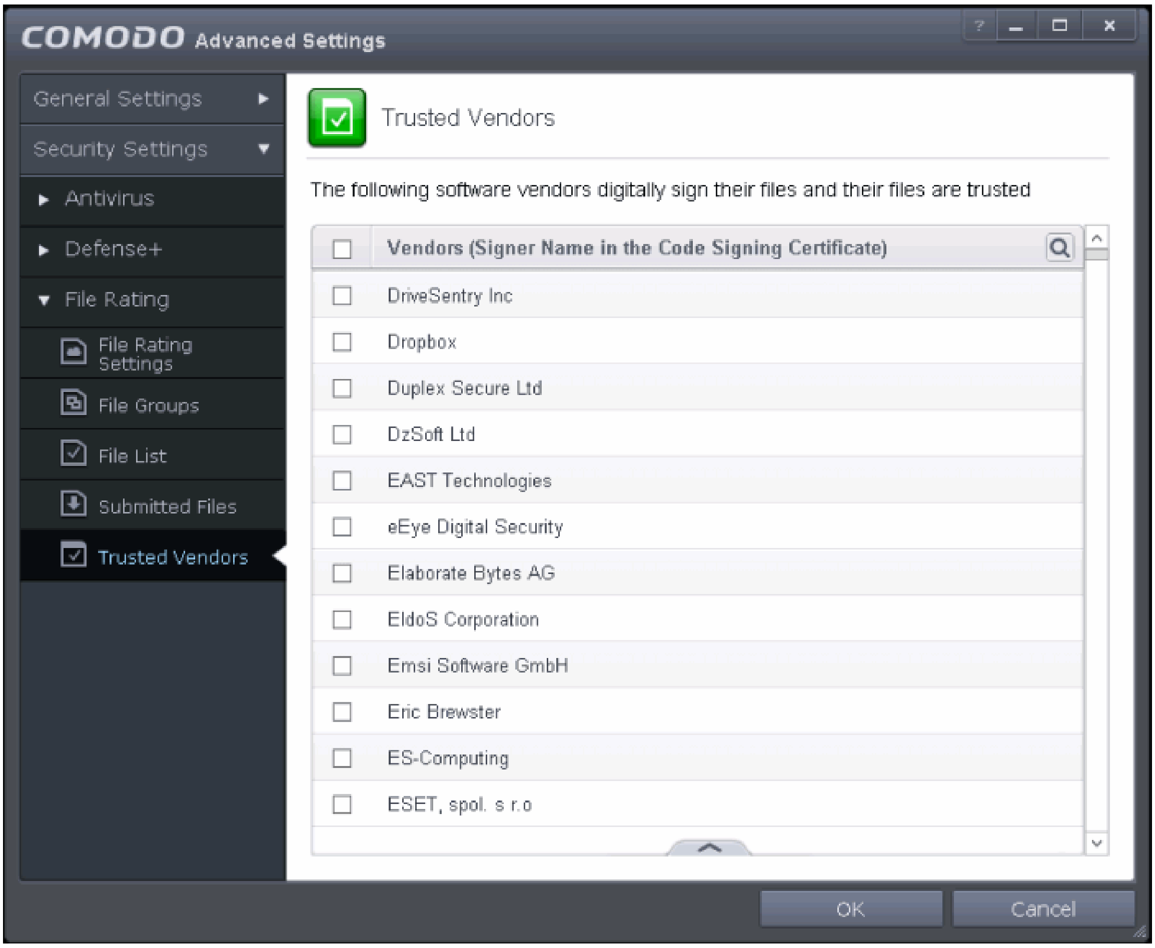
In CAVS, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

From this point:

- IF the vendor is on the Trusted Software Vendor List AND the user has enabled '**Trust Applications signed by Trusted Vendors**' in the File rating Settings panel, THEN the application will be trusted and allowed to run.
- IF the vendor is not on the Trusted Software Vendor List OR the user has not enabled 'Trust Applications signed by Trusted Vendors' THEN the application will be sandboxed. If the application in question is an installer then CAVS 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 CAVS. Details about this can be found at the foot of this page.

The 'Trusted Software Vendors' panel can be opened by clicking Security Settings > File Rating > Trusted Vendors.



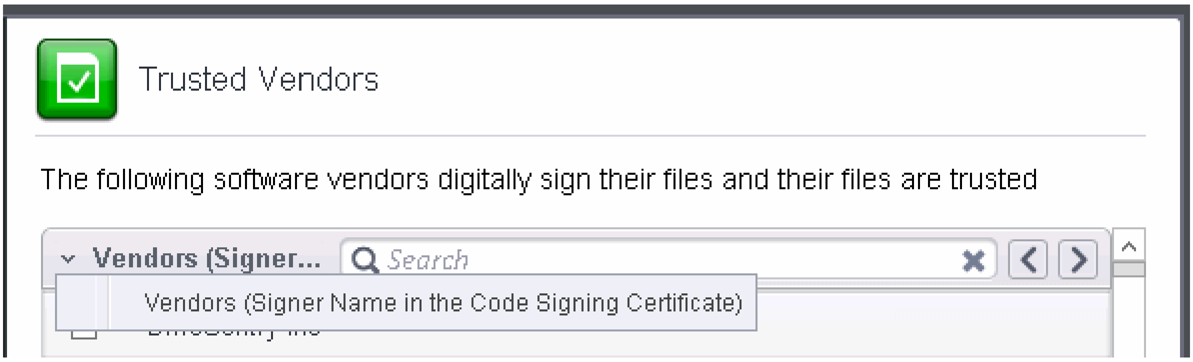
Trusted Vendors

The following software vendors digitally sign their files and their files are trusted

□	Vendors (Signer Name in the Code Signing Certificate)
□	DriveSentry Inc
□	Dropbox
□	Duplex Secure Ltd
□	DzSoft Ltd
□	EAST Technologies
□	eEye Digital Security
□	Elaborate Bytes AG
□	EldoS Corporation
□	Emsi Software GmbH
□	Eric Brewster
□	ES-Computing
□	ESET, spol. s r.o

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

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



Trusted Vendors

The following software vendors digitally sign their files and their files are trusted

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

Click here to read background information on digitally signing software

Click here to learn how to Add / Define a user-trusted vendor

Software Vendors - click here to find out about getting your software added to the list

Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

i. **Content Source**: The software they are downloading and are about to install ***really comes from the publisher that signed it.***

ii. **Content Integrity**: That the software they are downloading and are about to install ***has not be modified or corrupted since it was signed.***

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

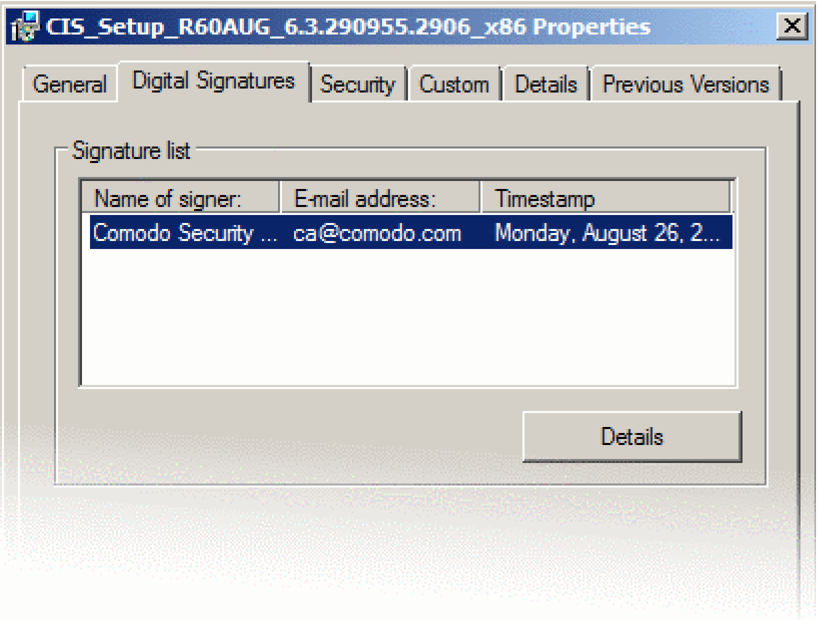
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by CAVS (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 CAVS is called 'CIS_Setup_R60AUG_6.3.290955.2906_x86.msi' and has been digitally signed.

- Browse to the (default) installation directory of CAVS.
- Right click on the setup file.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

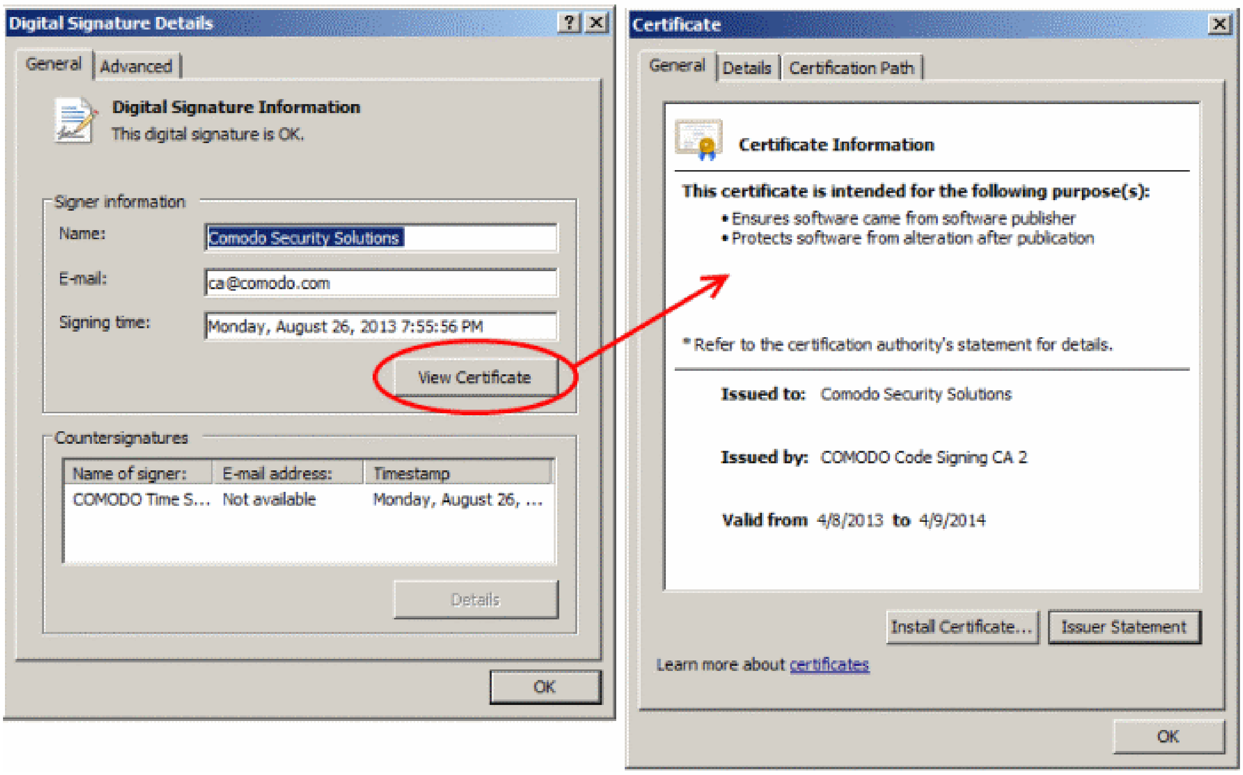
This displays the name of the CA that signed the software as shown below:



CIS_Setup_R60AUG_6.3.290955.2906_x86 Properties

Name of signer:	E-mail address:	Timestamp
Comodo Security ...	ca@comodo.com	Monday, August 26, 2...

Click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate. (see below).



Digital Signature Information
This digital signature is OK.

Signer information

Name:	Comodo Security Solutions
E-mail:	ca@comodo.com
Signing time:	Monday, August 26, 2013 7:55:56 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
COMODO Time S...	Not available	Monday, August 26, ...

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Comodo Security Solutions

Issued by: COMODO Code Signing CA 2

Valid from 4/8/2013 **to** 4/9/2014

It should be noted that the example above is a special case in that Comodo, as creator of 'CIS_Setup_R60AUG_6.3.290955.2906_x86.msi', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different. **See this example** for more details.

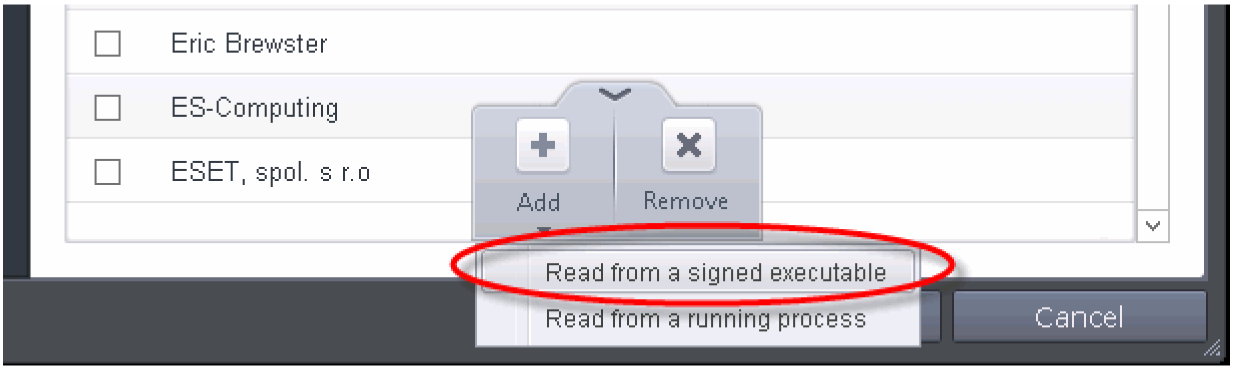
Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

- **By reading the vendor's signature from an executable file on your local drive**
- **By reading the vendor's signature from a running process**

To add a trusted vendor by reading the vendor's signature from an executable

- Click the handle from the bottom center and choose 'Add' > 'Read from a signed executable'

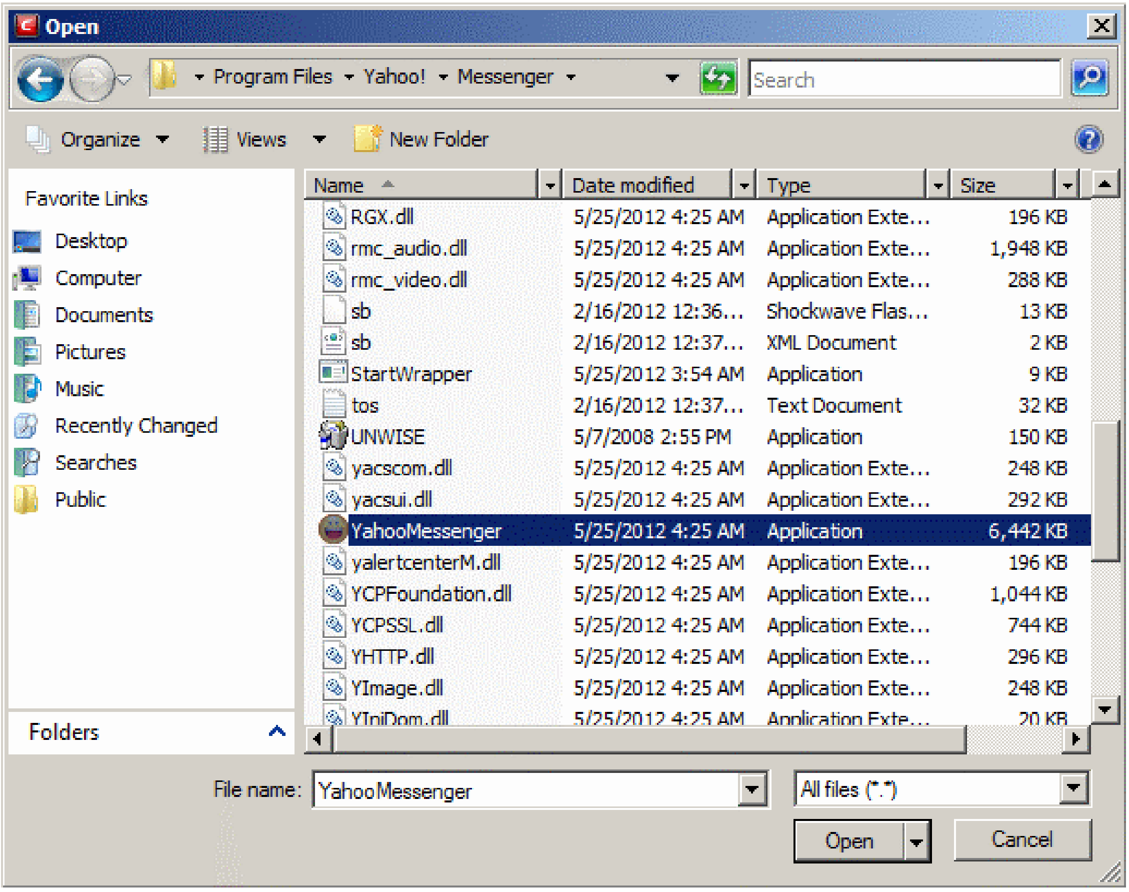


☐ Eric Brewster

☐ ES-Computing

☐ ESET, spol. s r.o

- Browse to the location of the executable your local drive. In the example below, we are adding the executable 'YahooMessenger.exe'.

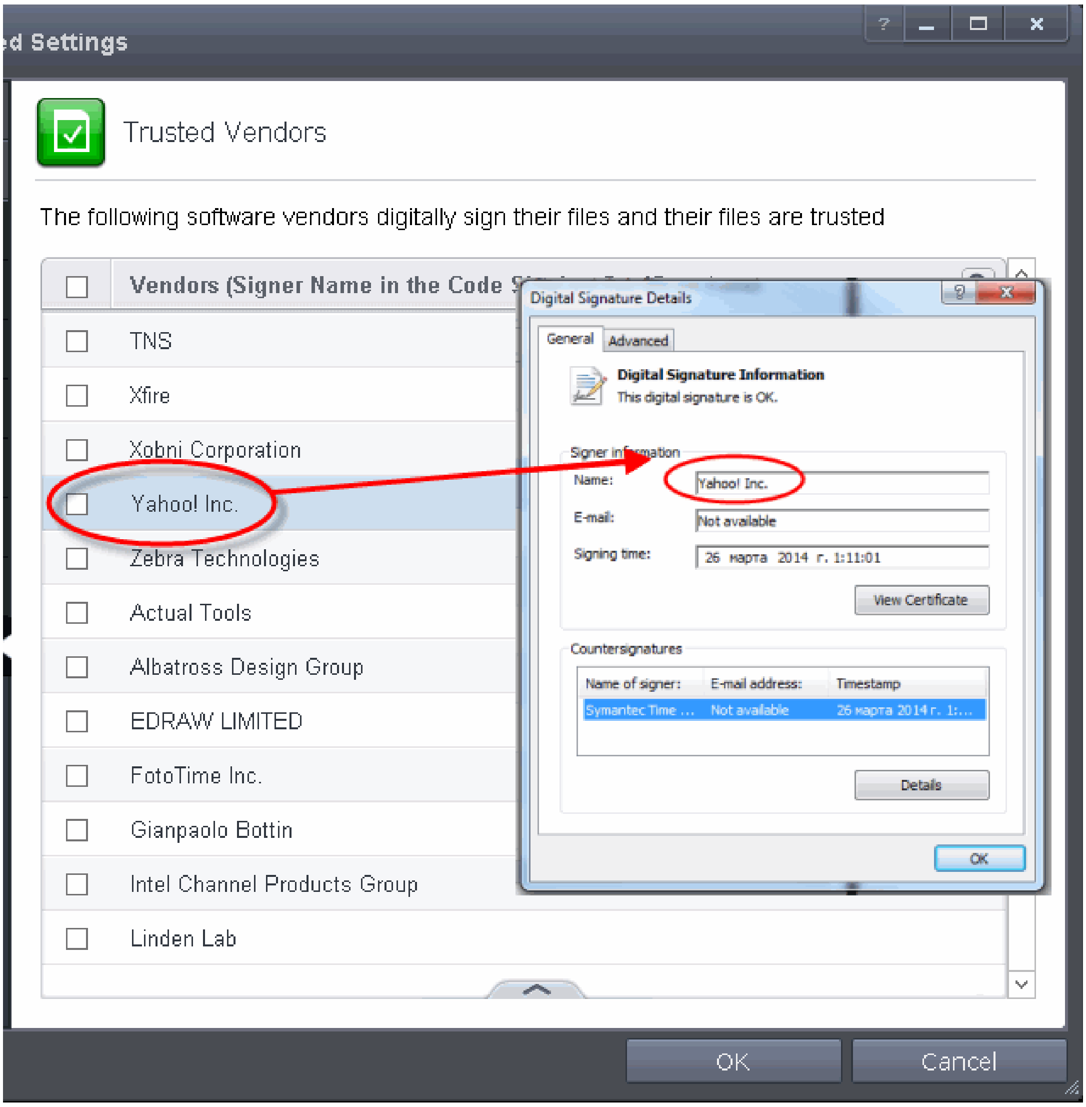


Name	Date modified	Type	Size
RGX.dll	5/25/2012 4:25 AM	Application Exte...	196 KB
rmc_audio.dll	5/25/2012 4:25 AM	Application Exte...	1,948 KB
rmc_video.dll	5/25/2012 4:25 AM	Application Exte...	288 KB
sb	2/16/2012 12:36...	Shockwave Flas...	13 KB
sb	2/16/2012 12:37...	XML Document	2 KB
StartWrapper	5/25/2012 3:54 AM	Application	9 KB
tos	2/16/2012 12:37...	Text Document	32 KB
UNWISE	5/7/2008 2:55 PM	Application	150 KB
yacscom.dll	5/25/2012 4:25 AM	Application Exte...	248 KB
yacsui.dll	5/25/2012 4:25 AM	Application Exte...	292 KB
YahooMessenger	5/25/2012 4:25 AM	Application	6,442 KB
yalertcenterM.dll	5/25/2012 4:25 AM	Application Exte...	196 KB
YCPFoundation.dll	5/25/2012 4:25 AM	Application Exte...	1,044 KB
YCPSSL.dll	5/25/2012 4:25 AM	Application Exte...	744 KB
YHTTP.dll	5/25/2012 4:25 AM	Application Exte...	296 KB
YImage.dll	5/25/2012 4:25 AM	Application Exte...	248 KB
YIniDom.dll	5/25/2012 4:25 AM	Application Exte...	20 KB

File name: YahooMessenger

All files (*.*)

On clicking 'Open', CAVS 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):



d Settings

Trusted Vendors

The following software vendors digitally sign their files and their files are trusted

□	Vendors (Signer Name in the Code S
□	TNS
□	Xfire
□	Xobni Corporation
□	Yahoo! Inc.
□	Zebra Technologies
□	Actual Tools
□	Albatross Design Group
□	EDRAW LIMITED
□	FotoTime Inc.
□	Gianpaolo Bottin
□	Intel Channel Products Group
□	Linden Lab

Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information
Name: Yahoo! Inc.
E-mail: Not available
Signing time: 26 марта 2014 г. 1:11:01

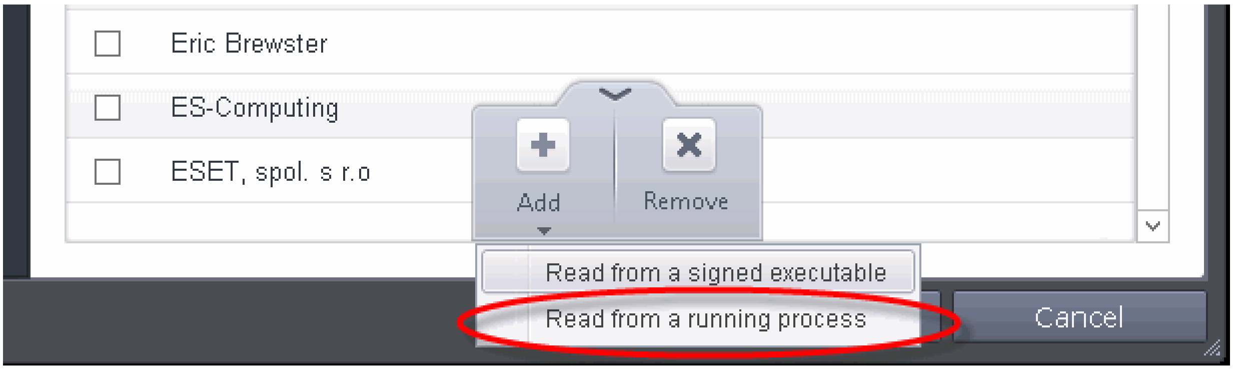
Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	26 марта 2014 г. 1:...

In the example above, CAVS was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to the list. All future software that is signed by the vendor 'Yahoo! Inc.' is automatically added to the Comodo Trusted Vendor list UNLESS you change **this setting in File Rating Settings**.

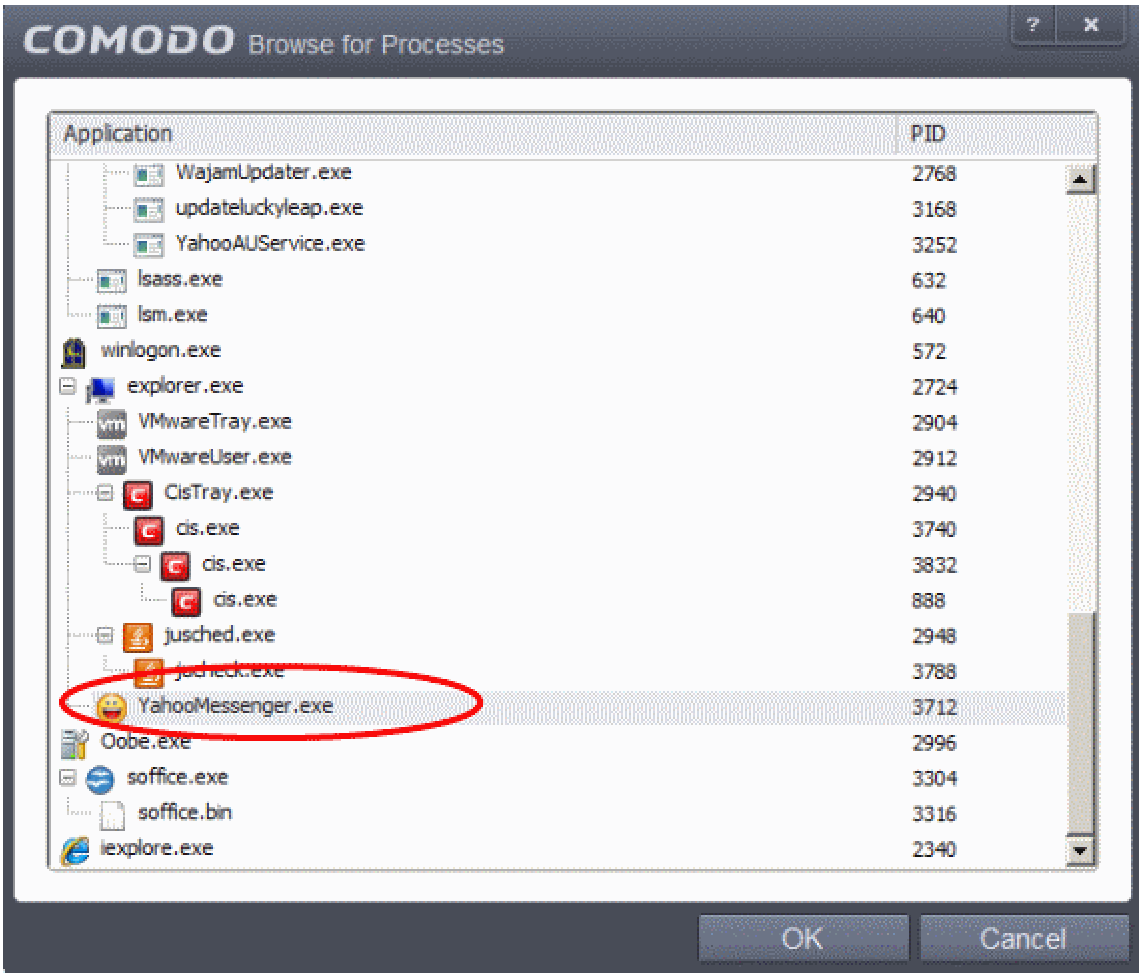
To add a trusted vendor from a currently running process

- Click the handle from the bottom center and choose 'Add' > 'Read from a running process'



□	Eric Brewster
□	ES-Computing
□	ESET, spol. s r.o

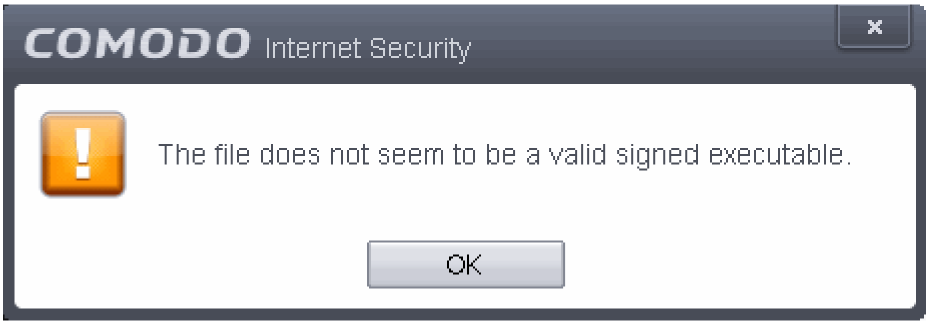
- Select the signed executable that you want to trust and click the 'OK' button.



Application	PID
WajamUpdater.exe	2768
updateluckyleap.exe	3168
YahooAUService.exe	3252
lsass.exe	632
lsm.exe	640
winlogon.exe	572
explorer.exe	2724
VMwareTray.exe	2904
VMwareUser.exe	2912
CisTray.exe	2940
cis.exe	3740
cis.exe	3832
cis.exe	888
jusched.exe	2948
jucheck.exe	3788
YahooMessenger.exe	3712
Oobe.exe	2996
soffice.exe	3304
soffice.bin	3316
iexplore.exe	2340

CAVS performs the same certificate check as described above. If the parent application of the selected process is signed, CAVS adds the vendor to the Trusted Software Vendors list.

If CAVS cannot verify that the software certificate is signed by a Trusted CA then it does not add the software vendor to the list of 'Trusted Vendors'. In this case, you can see the following error message.



The file does not seem to be a valid signed executable.

Note: The 'Trusted Software Vendors' list displays two types of software vendors:

- User defined trusted software vendors - As the name suggests, these are added by the user via one of the two methods outlined earlier. These vendors can be removed by the user by selecting and clicking the 'Remove' button.
- Comodo defined trusted software vendors - These are the vendors that Comodo, in it's capacity as a Trusted CA, has independently validated as legitimate companies. If the user needs to remove any of these vendors from the list, it can be done by selecting the vendor, clicking 'Remove' and restarting the system. Please note that the removal will take effect only on restarting the system.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default Trusted Vendor List that is shipped with CAVS. 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, CAVS 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 CAVS.

More details are available at **http://internetsecurity.comodo.com/trustedvendor/overview.php**.

Appendix 1 - CAVS How to... Tutorials

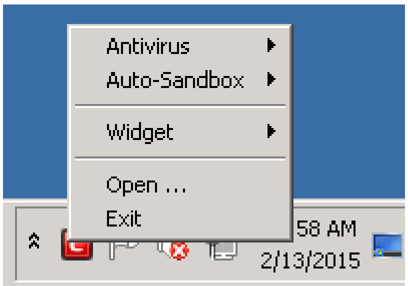
The 'How To...' section of the guide contains guidance on key tasks of Comodo Antivirus for Servers. Use the links below to go to each tutorial's page.

How to...

- **Enable / Disable AV and Auto-Sandbox Easily** - Guidance on changing the current enabled/disabled states of Antivirus and Defense+.
- **Setup HIPS for maximum security and usability** - A brief outline of how to set Host intrusion Protection for the optimum balance between security and usability.
- **Create Rules for Auto-Sandboxing Applications** - A brief outline of how to set create auto-sandbox rules for the maximum security against untrusted applications
- **Run an Instant Antivirus Scan on Selected Items** - Guidance on initiating a manual scan on selected folders/files to check for viruses and other malware.
- **Create an Antivirus Scanning Schedule** - Guidance on time-table scheduling of antivirus scans to be run on selected items at selected intervals
- **Run Untrusted Programs In The Sandbox** - Guidance on executing a program that you do not trust to be safe, inside sandbox to protect any harmful effects of the program upon your system.
- **Run Browsers Inside Sandbox** - Guidance on running your browser, inside sandbox when you plan to visit untrusted websites.
- **Restore Incorrectly Quarantined Item(s)** - Help to restore files and executables that were moved to quarantine by mistake.
- **Submit Quarantined Items to Comodo for Analysis** - Advice on how to send suspicious files/executables to Comodo for analysis.
- **Block any Downloads of a Specific File Type** - Explains how to configure Defense+ to block downloads of files of a specific type
- **Disable Auto-Sandboxing on a Per-application Basis** - Explains how to exclude specific files or file types from the auto-sandboxing process.
- **Switch Off Automatic Antivirus and Software Updates** - Explains how to stop automatic software and virus updates.

Enable / Disable AV and Auto-Sandbox Easily

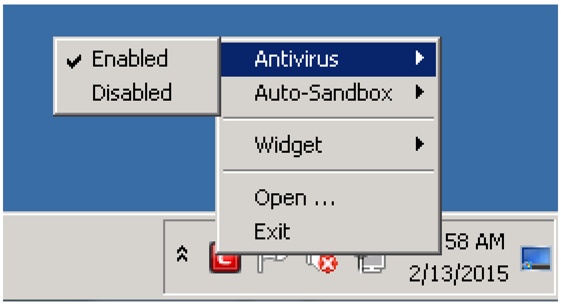
Comodo Antivirus for Servers allows users to quickly switch the Enabled/Disabled states of **Antivirus** and **Auto-Sandbox** by right clicking on the system tray icon.



Antivirus

To enable/disable the Antivirus

1. Right click on the system tray icon keeping the CAVS interface
2. Move the mouse cursor over 'Antivirus'



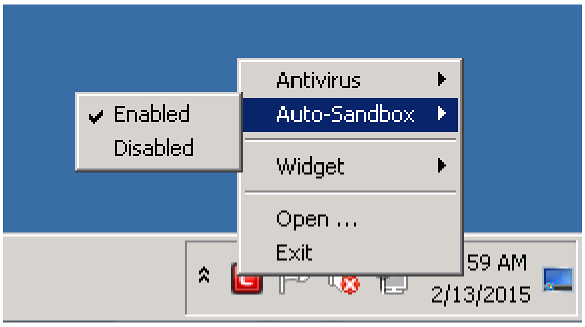
3. Choose 'Enabled' or 'Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Auto-Sandbox

To enable/disable the Auto-Sandbox

1. Right click on the system tray icon keeping the CAVS interface
2. Move the mouse cursor over 'Auto-Sandbox'



3. Choose 'Enabled' or 'Disabled' as per your choice

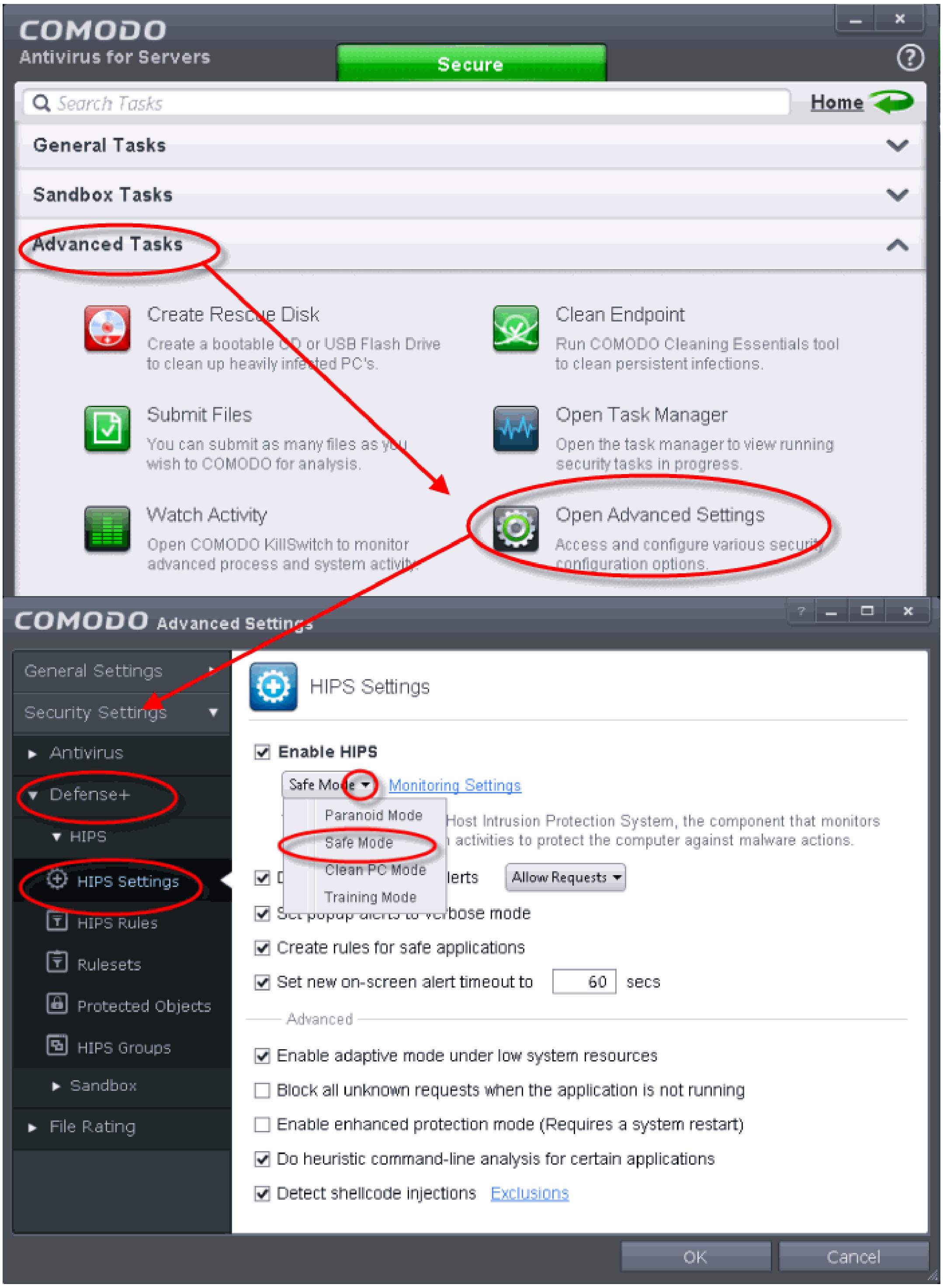
You can find the set security level also from **the Home Screen**.

Set up the HIPS for Maximum Security and Usability

This page explains on configuring the Host Intrusion Prevention System (HIPS) component of CAVS to provide maximum security from the malicious programs that try to execute from within your server and to protect your system from data theft, server crashes and system damage by preventing most types of buffer overflow attacks, prevent possible attacks from root-kits, inter-process memory injections, key-loggers and more.

To configure HIPS

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen.
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'HIPS' > 'HIPS Settings' from the left hand side pane.



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Open Task Manager
Open the task manager to view running security tasks in progress.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

☑ Enable HIPS

Safe Mode ▾ Monitoring Settings

Host Intrusion Protection System, the component that monitors
activities to protect the computer against malware actions.

☑ D lerts Allow Requests ▾

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs

Advanced

☑ Enable adaptive mode under low system resources

☐ Block all unknown requests when the application is not running

☐ Enable enhanced protection mode (Requires a system restart)

☑ Do heuristic command-line analysis for certain applications

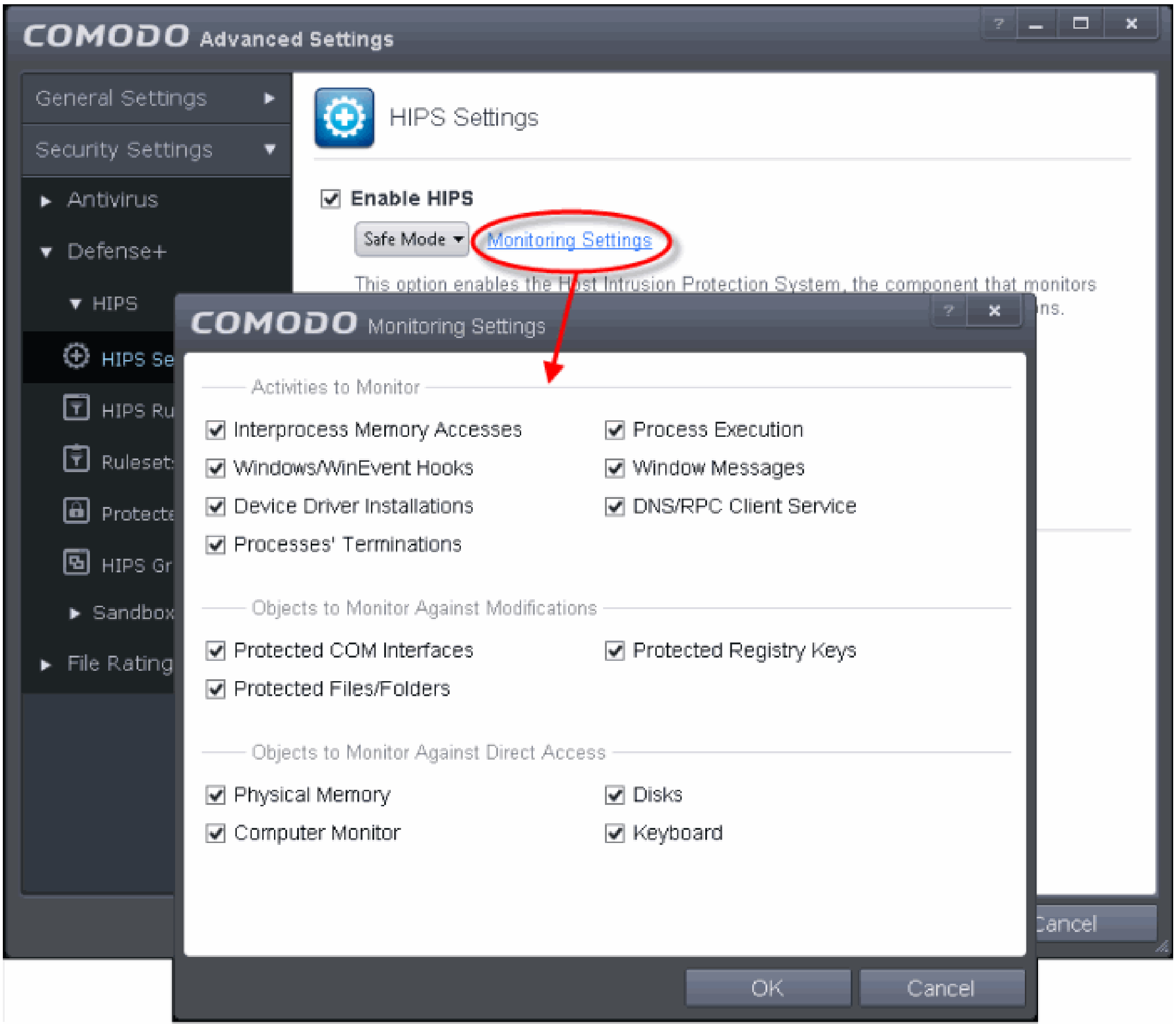
☑ Detect shellcode injections Exclusions

4. Select Enable HIPS

5. Choose 'Safe Mode' from the drop-down below it. Refer to **HIPS Behavior Settings** for more details on the Security Levels.

Monitoring Settings

6. Click Monitoring Settings from the HIPS Settings interface.



☑ Enable HIPS

Activities to Monitor

☑ Interprocess Memory Accesses
☑ Windows/WinEvent Hooks
☑ Device Driver Installations
☑ Processes' Terminations
☑ Process Execution
☑ Window Messages
☑ DNS/RPC Client Service

Objects to Monitor Against Modifications

☑ Protected COM Interfaces
☑ Protected Files/Folders
☑ Protected Registry Keys

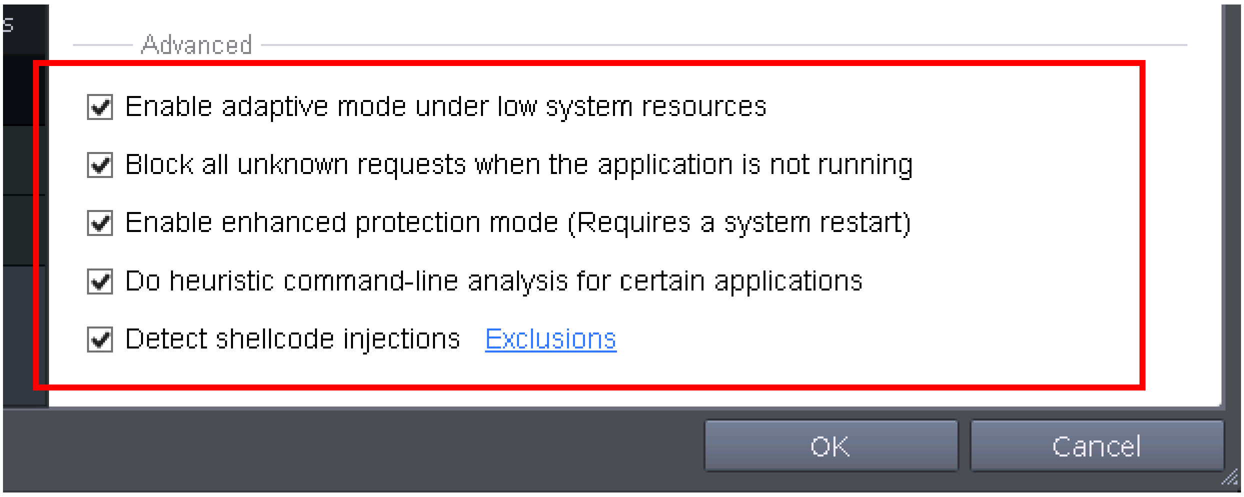
Objects to Monitor Against Direct Access

☑ Physical Memory
☑ Computer Monitor
☑ Disks
☑ Keyboard

7. Make sure that all the check boxes are selected and click OK.

Advanced Settings

8. Make the following settings under Advanced in the HIPS Settings interface.



Advanced

☑ Enable adaptive mode under low system resources
☑ Block all unknown requests when the application is not running
☑ Enable enhanced protection mode (Requires a system restart)
☑ Do heuristic command-line analysis for certain applications
☑ Detect shellcode injections

Optional – Enable '**Block all unknown requests if the application is not running**'. Selecting this option blocks all unknown execution requests if CAVS is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already ‘clean’ and are looking just to enable the highest CAVS security settings then it is OK to leave this box unchecked.

If you are using a 64-bit system, in order to maximize the security, it is important to select '**Enable enhanced protection mode** (Requires a system restart)' – Enabling this mode will activate additional host intrusion prevention techniques in Defense+ to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures.

Click here for more details on HIPS Behavior Settings

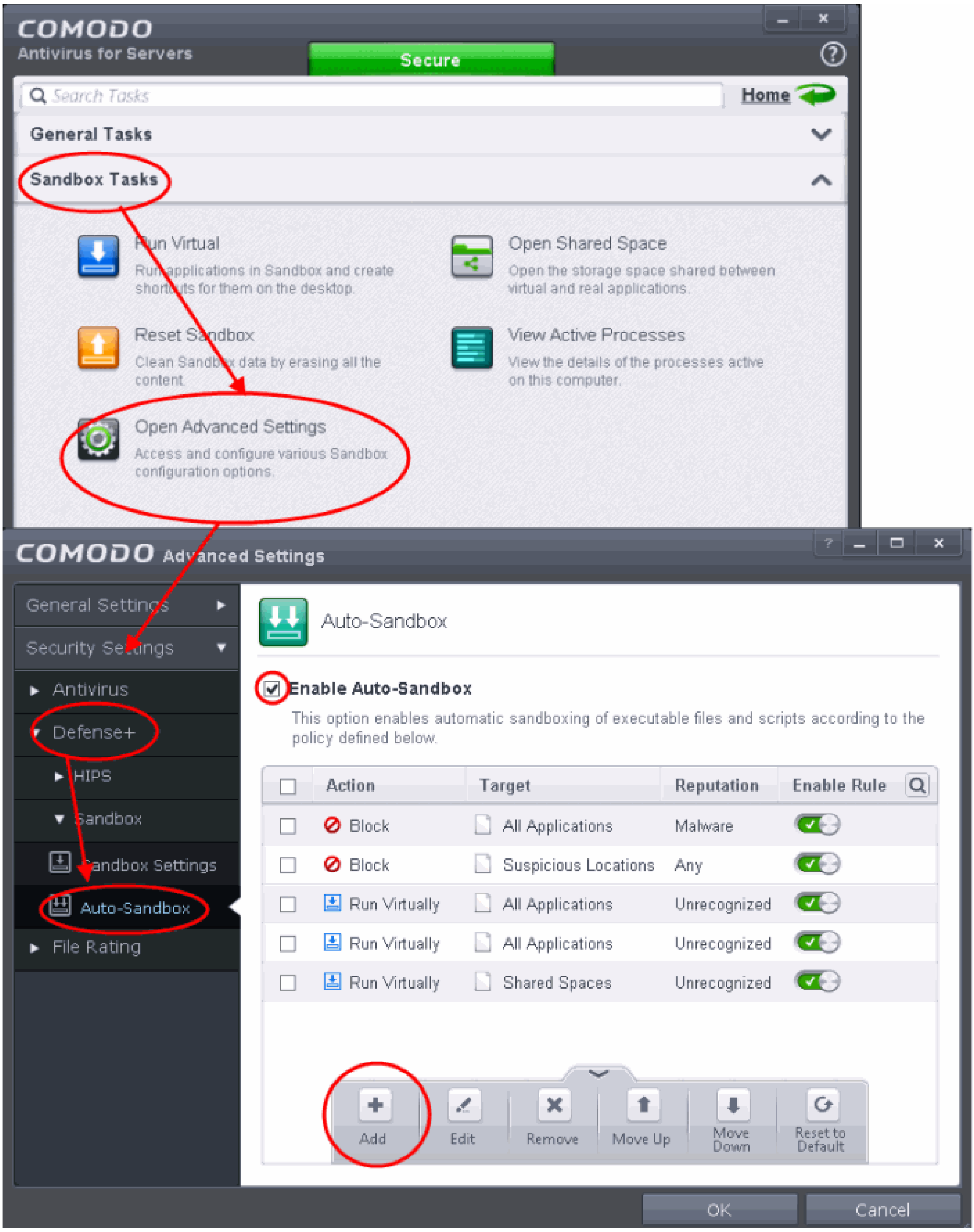
Create Rules for Auto-Sandboxing Applications

You can define rules for programs that should be run in the sandboxed environment. A sandboxed application has much less opportunity to damage your computer because it is run isolated from your operating system and your files.

CAVS ships with a set of pre-defined auto-sandbox rules that are configured to provide maximum protection for your system. Before creating a rule, check if your requirement is met by the default rules. Refer to the section **Configuring Rules for Auto-Sandbox** for more details.

To create auto-sandbox rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Sandbox Tasks' and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'Sandbox' > 'Auto-Sandbox' from the left hand side pane
4. Click the handle at the bottom of the interface and open the option panel



COMODO Antivirus for Servers

Secure

Search Tasks

Home

General Tasks

Sandbox Tasks

Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.

Open Shared Space
Open the storage space shared between virtual and real applications.

Reset Sandbox
Clean Sandbox data by erasing all the content.

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

Open Advanced Settings
Access and configure various Sandbox configuration options.

COMODO Advanced Settings

- General Settings
- Security Settings
  - Antivirus
  - Defense+
    - HIPS
    - Sandbox
      - Sandbox Settings
      - Auto-Sandbox
  - File Rating

Auto-Sandbox

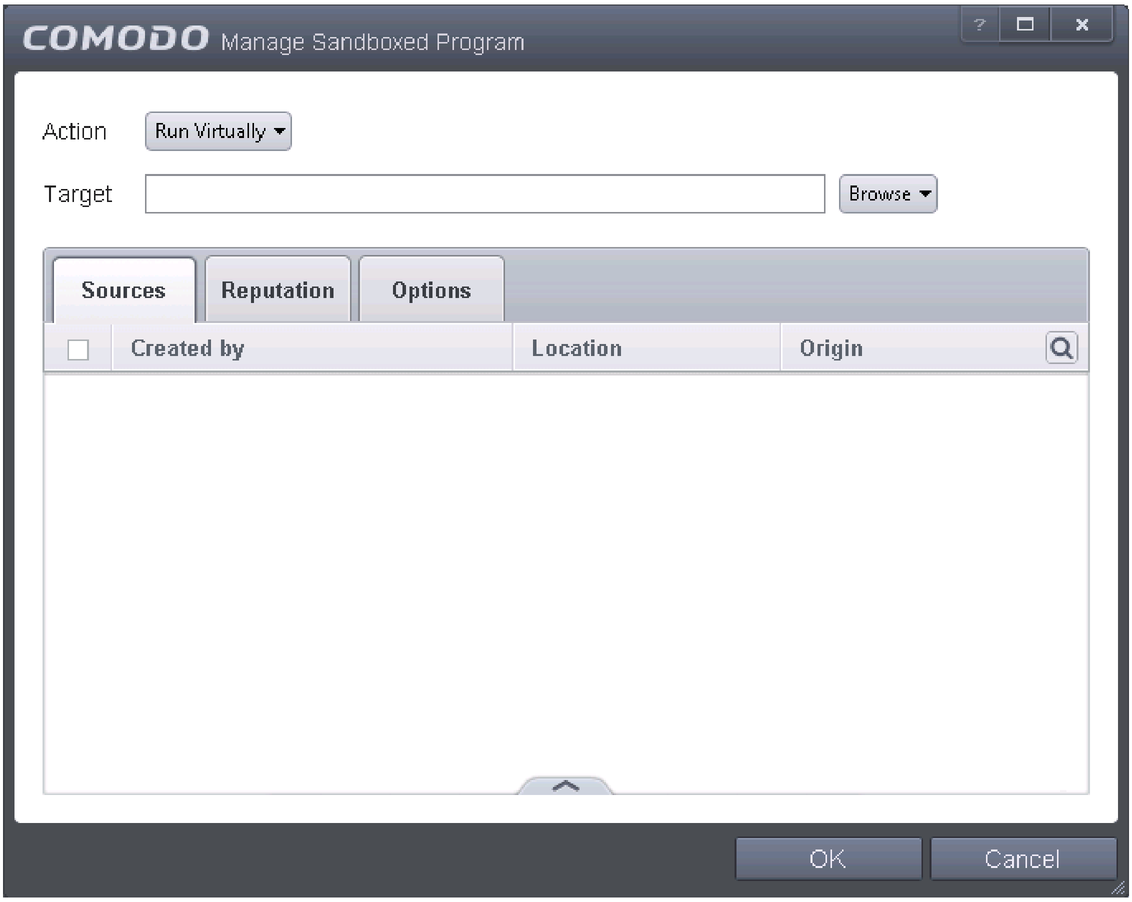
☑ Enable Auto-Sandbox

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malware	✓
□	Block	Suspicious Locations	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	Shared Spaces	Unrecognized	✓

5. Click the 'Add' button

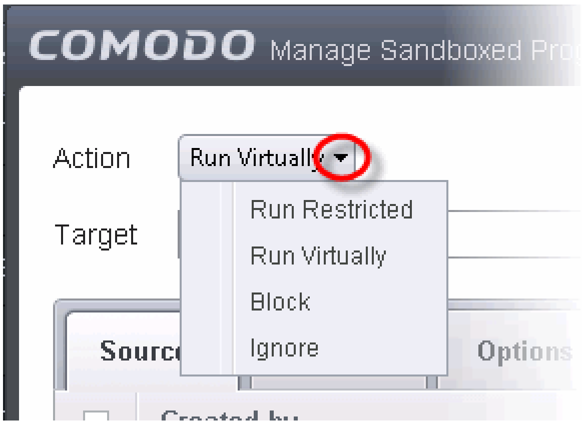
The Manage Sandboxed Program screen will be displayed.



- **Step 1** – Select the Action
- **Step 2** – Select the Target
- **Step 3** – Select the Sources
- **Step 4** – Select the File Reputation
- **Step 5** – Select the Options

Step 1 – Select the Action

The options under the Action drop-down button combined with the Set Restriction Level setting in the Options tab determine the amount of privileges an auto-sandboxed application has access to other software and hardware resources on your computer.



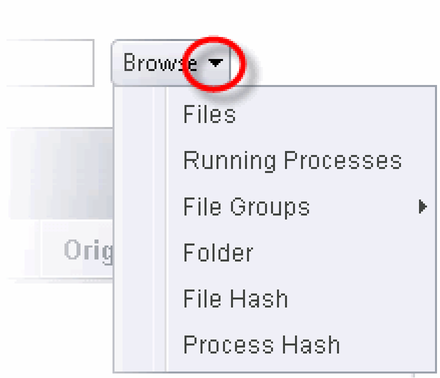
The options available under the Action button are:

- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.

- **Run Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be sandboxed and allowed to run with all privileges.

Step 2 – Select the Target

The next step is to select the target to which the auto-sandbox rule is to be applied. Click the Browse button beside the Target field.



You have six options available to add the target path.

- **Files** – Allows to add individual files as target.
- **Running Processes** – As the name suggests, this option allows you to add any process that is currently running on your computer
- **File Groups** – Allows to add predefined File Groups as target. To add or modify a predefined file group refer to the section **File Groups** for more details.
- **Folder** – Allows you to add a folder or drive as the target
- **File Hash** – Allows you to add a file as target based on its hash value
- **Process Hash** - Allows you to add any process that is currently running on your computer as target based on its hash value

Click here to know more about adding each of the options.

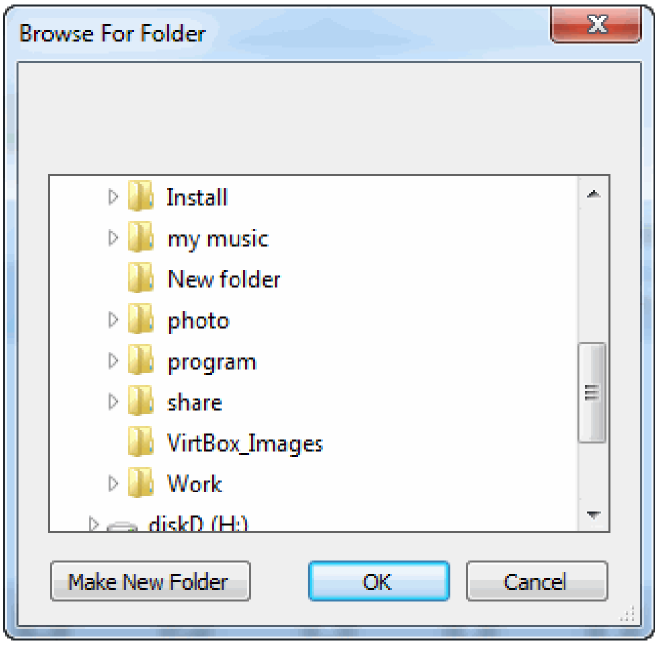
Step 3 – Select the Sources

If you want to include a number of items for a rule but want the rule to be applied for certain conditions only, then you can do this in this step. For example, if you include all executables in the Target but want the rule to be applied for executables that were downloaded from the internet only, then the filter can be applied in the Sources. Another example is if you want to run unrecognized files from network share, you have to create an ignore rule with All Applications as target and source located on network drives.

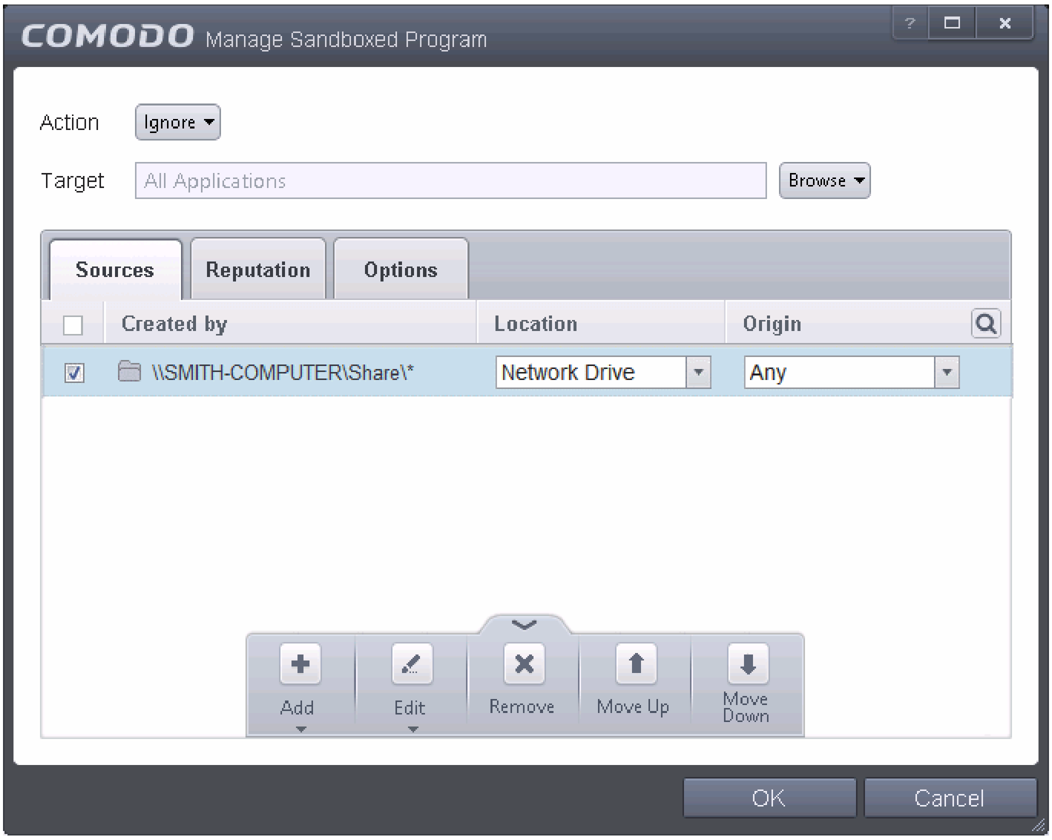
The following example describes how to add an Ignore rule for Unrecognized files from a network source:

- In **Step 1**, select the action as Ignore
- In **Step 2**, select the Target as All Applications in File Groups
- In **Step 3**, click Folder from the Add options.

The 'Browse For Folder' dialog will be displayed.



- Navigate to the source folder in the network, select it and click 'OK'.



Action: Ignore

Target: All Applications | Browse

□	Created by	Location	Origin
☑	\\SMITH-COMPUTER\Share\*	Network Drive	Any

The selected network source folder will be added under the 'Created by' column and the screen displays the options to specify the location and from where the files were downloaded.

- **Location** – The options available are:
  - Any
  - Local Drive
  - Removable Drive
  - Network Drive

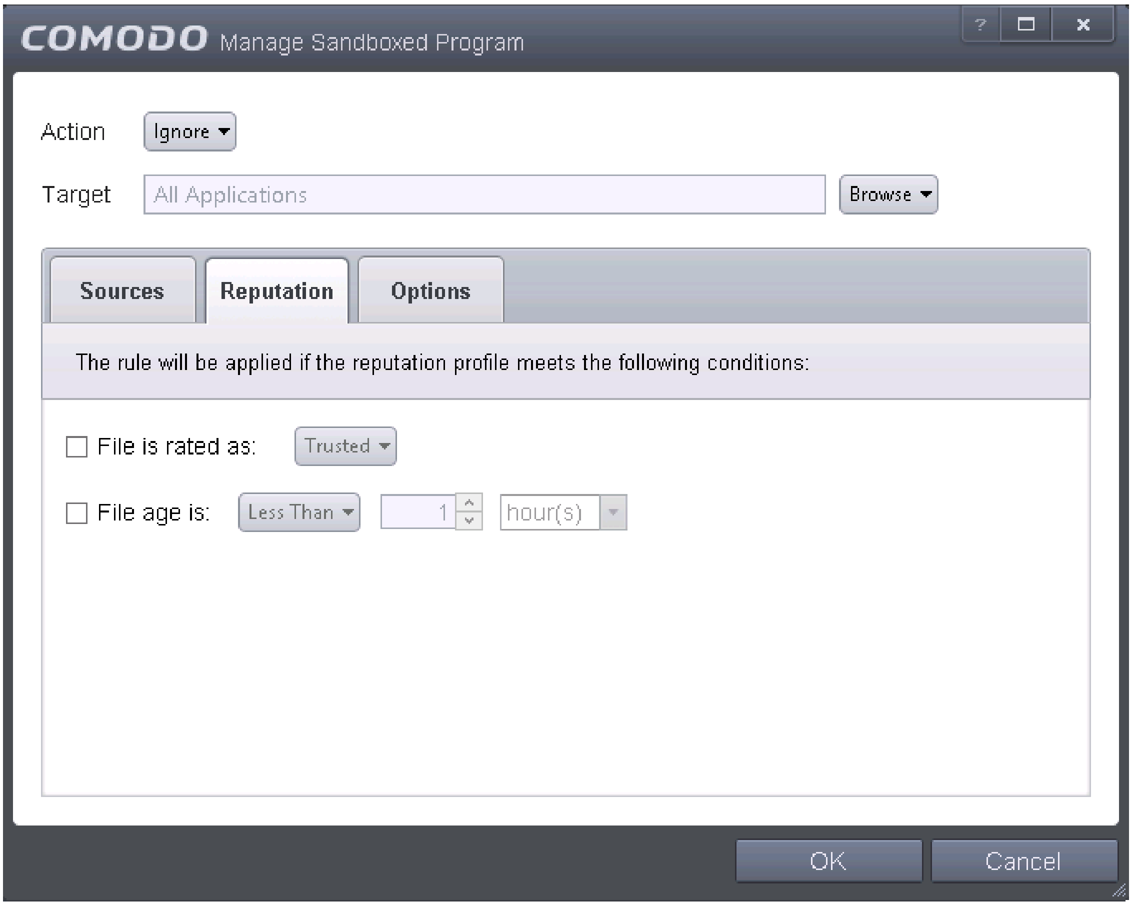
Since the source is located in a network, select Network Drive from the options.

- **Origin** – The options available are:
  - Any – The rule will apply to files that were downloaded to the source folder from both Internet and Intranet.
  - Internet – The rule will apply to files that were downloaded to the source folder from Internet only.
  - Intranet – The rule will apply to files that were downloaded to the source folder from Intranet only.

Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options in **Step 4**.

Step 4 – Select the File Reputation

- Click the Reputation tab in the Manage Sandboxed Program interface.



The rule will be applied if the reputation profile meets the following conditions:

☐ File is rated as: Trusted

☐ File age is: Less Than 1 hour(s)

By default, the file rating is not selected meaning the rating could be Any. The options available are:

- **Trusted** – Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files by Defense+. Refer to the sections **File Rating Settings** and **File List** for more information.
- **Unrecognized** – Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section '**File List**' for more information.
- **Malware** – Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions. Refer the section **Unknown Files – The Scanning Process** for more information.

By default, file age is not selected, so the age could be Any. The options available are:

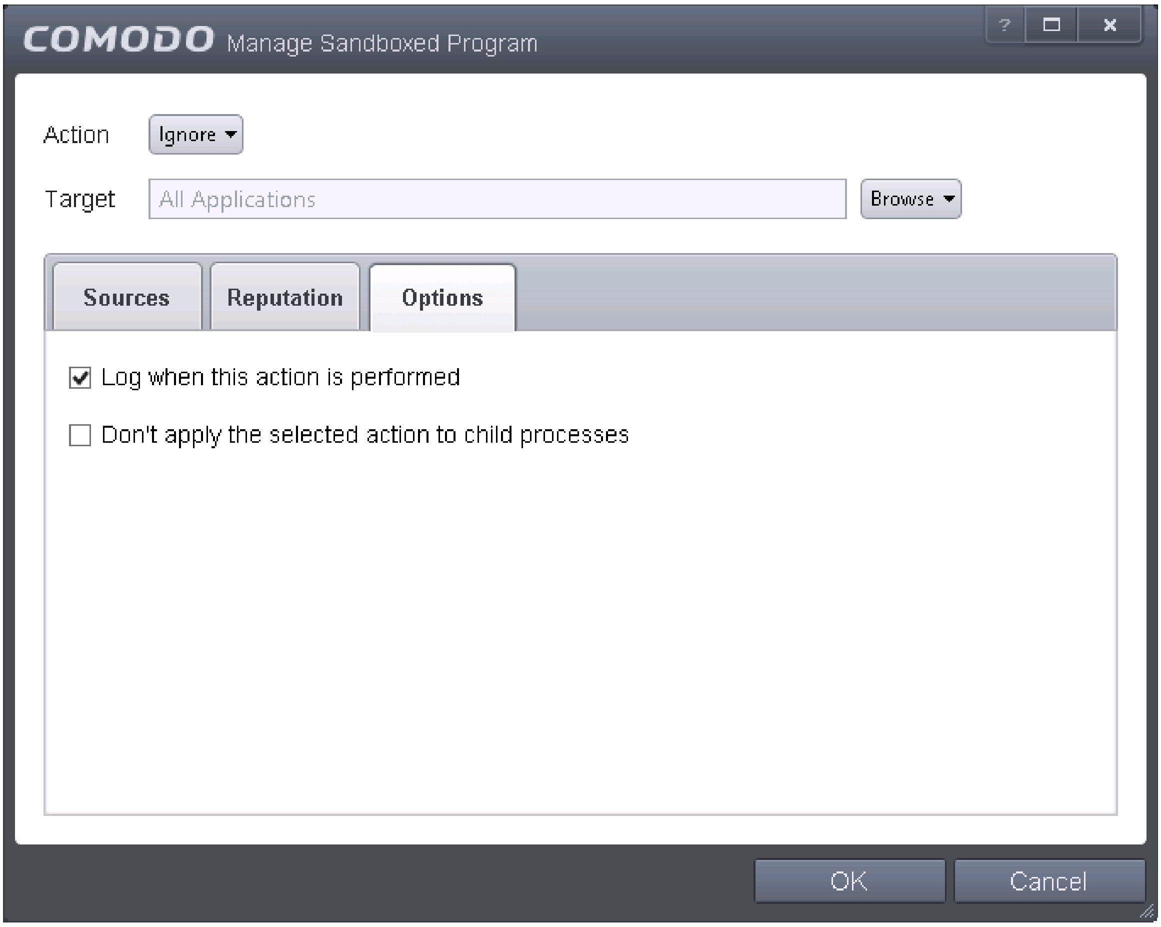
- Less Than – CAVS will check for reputation if a file is younger than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. (***Default and recommended = 1 hours)***

- More Than - CAVS will check for reputation if a file is older than the age you set here. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 1 hours)***

Select the category from the options. Since the example rule is created for files that are categorized as Unrecognized, the same has to be selected from the rating options.

Step 5 – Select the Options

- Click the Options tab in the Manage Sandboxed Program interface.



☑ Log when this action is performed

□ Don't apply the selected action to child processes

By default, the 'Log when this action is performed' The options available for Ignore action are:

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** – Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CAVS treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
  - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
  - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox rules individually applied as per their file rating.

The 'Don't apply the selected action to child processes' option is available for the Ignore action only. For actions – Run Restricted and Run Virtually – the following options are available:

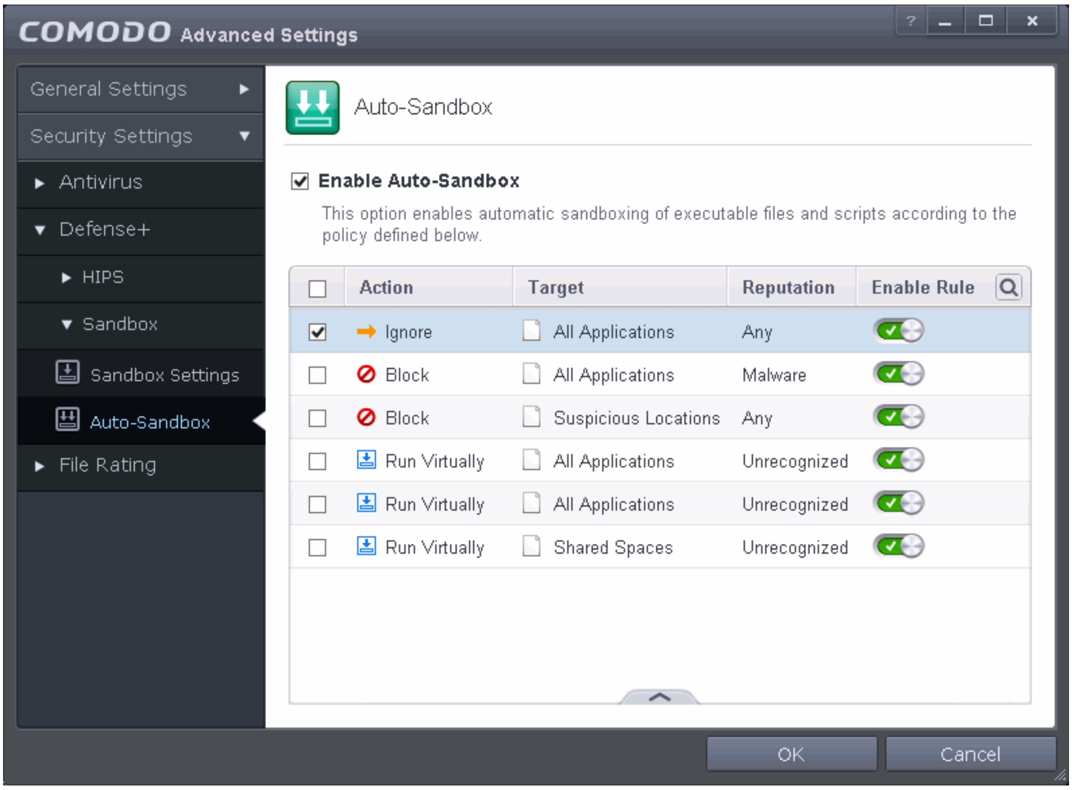
- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.

- **Set Restriction Level** – When Run Restricted is selected in Action, then this option is automatically selected and cannot be unchecked while for Run Virtually action the option can be checked or unchecked. The options for Restriction levels are:
  - **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(***Default***)
  - **Limited -** Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
  - **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
  - **Untrusted -** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
- **Limit maximum memory consumption to** – Enter the memory consumption value in MB that the process should be allowed.
- **Limit program execution time to** – Enter the maximum time in seconds the program should run. After the specified time, the program will be terminated.

For Block action, the following options are available:

- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Quarantine program** – If checked, the programs will be automatically quarantined. Refer to the section **Manage Quarantined Items** for more information.

Choose the options and click 'OK'. The rule will be added and displayed in the list.



☑ **Enable Auto-Sandbox**

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
☑	Ignore	All Applications	Any	✓
□	Block	All Applications	Malware	✓
□	Block	Suspicious Locations	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	Shared Spaces	Unrecognized	✓

That's it. You have created an Ignore auto-sandbox rule for unrecognized files with a Network drive as source.

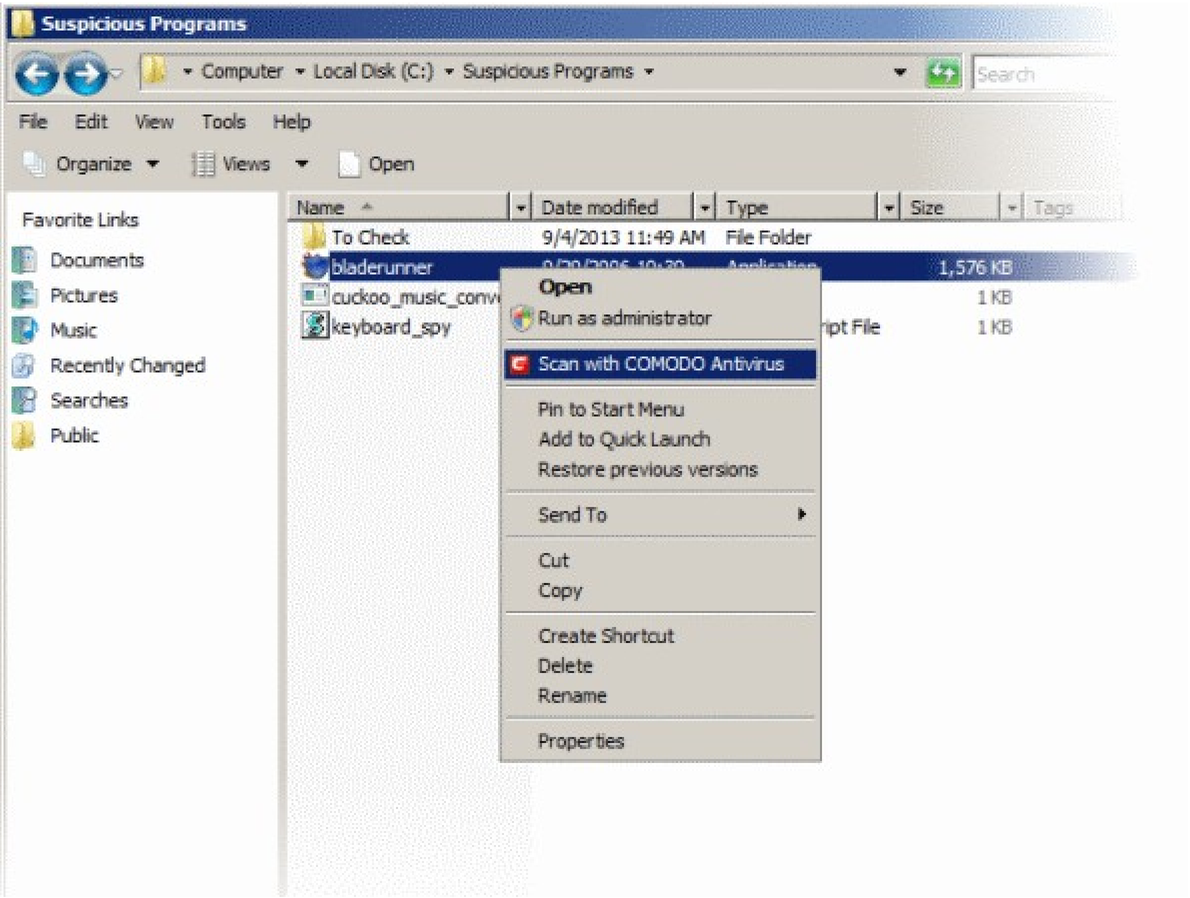
Run an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders files etc. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives, digital cameras - even your iPod and mobile phones too!!! This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from the Internet.

Click here for more details on running on-demand scans.

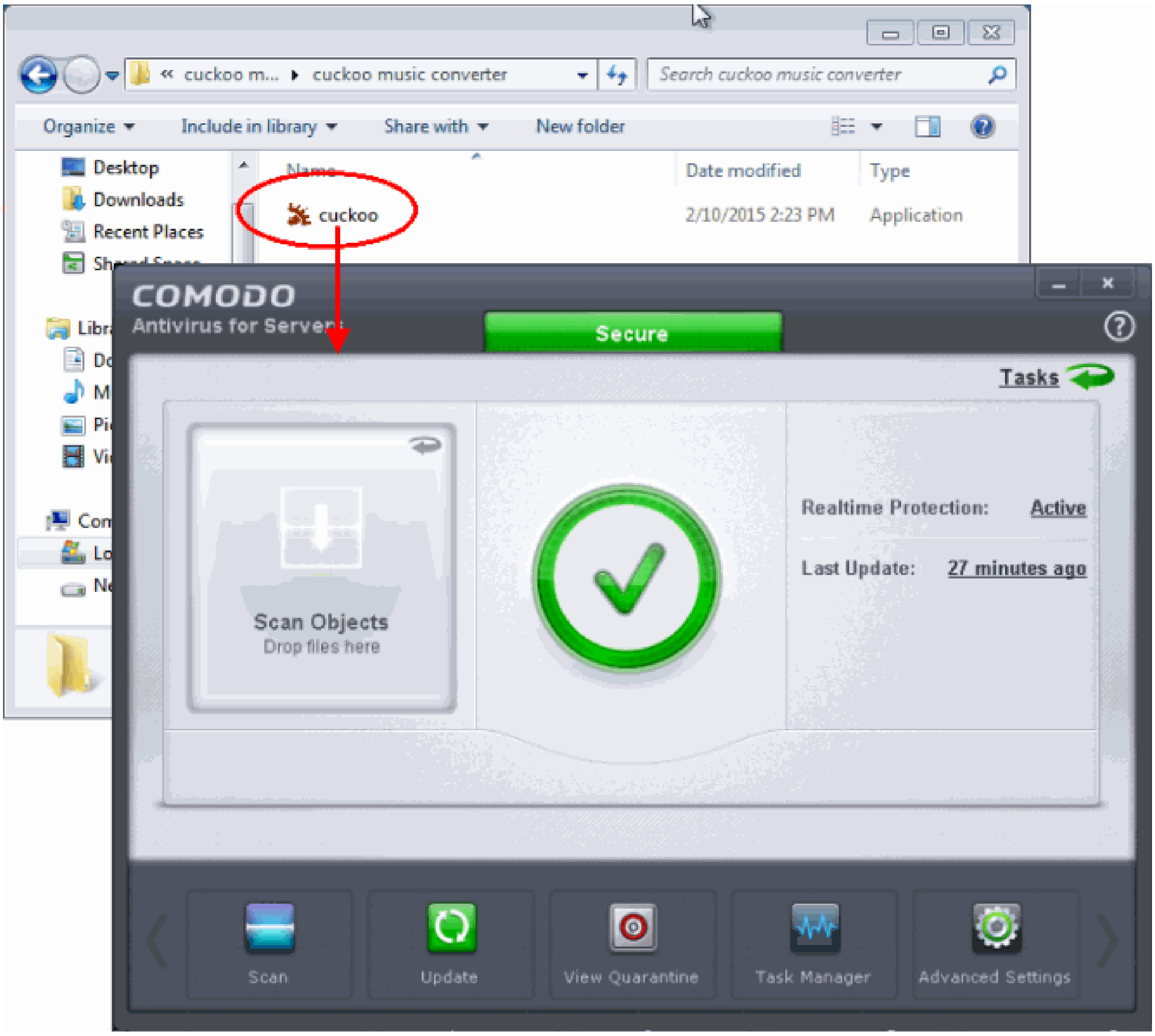
To instantly scan an item

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

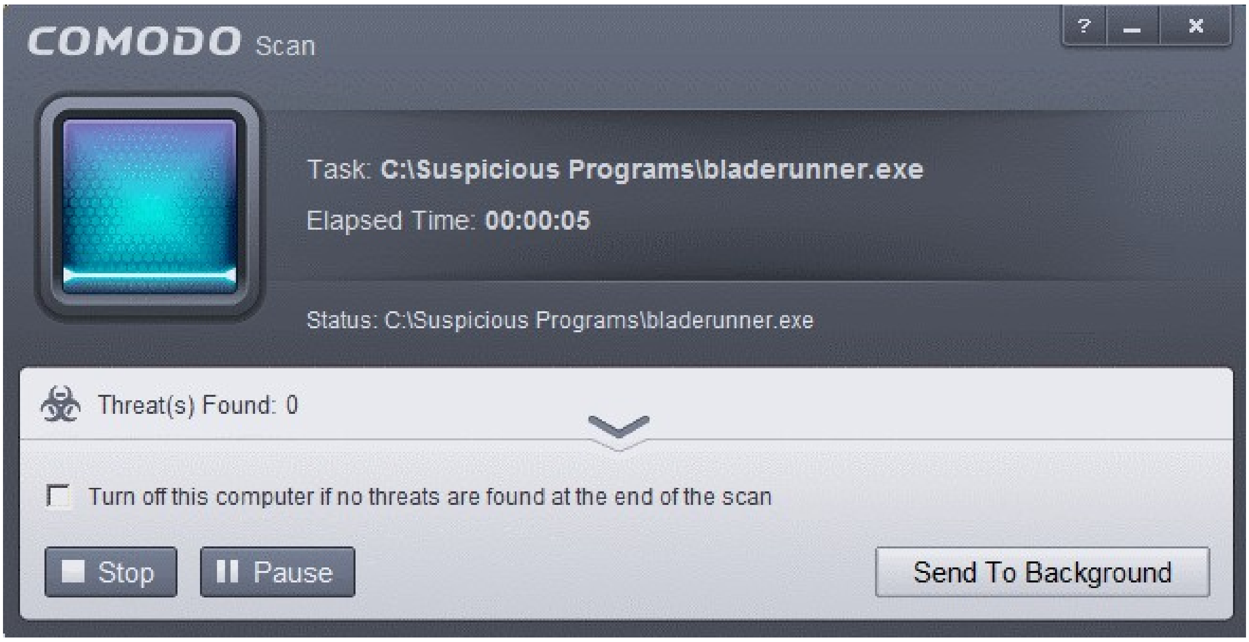


OR

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



The item will be scanned immediately.



Task: **C:\Suspicious Programs\bladerunner.exe**

Elapsed Time: **00:00:05**

Status: C:\Suspicious Programs\bladerunner.exe

Threat(s) Found: 0

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

...and on completion of scanning, the scan finished dialog be displayed with the number of threats found.

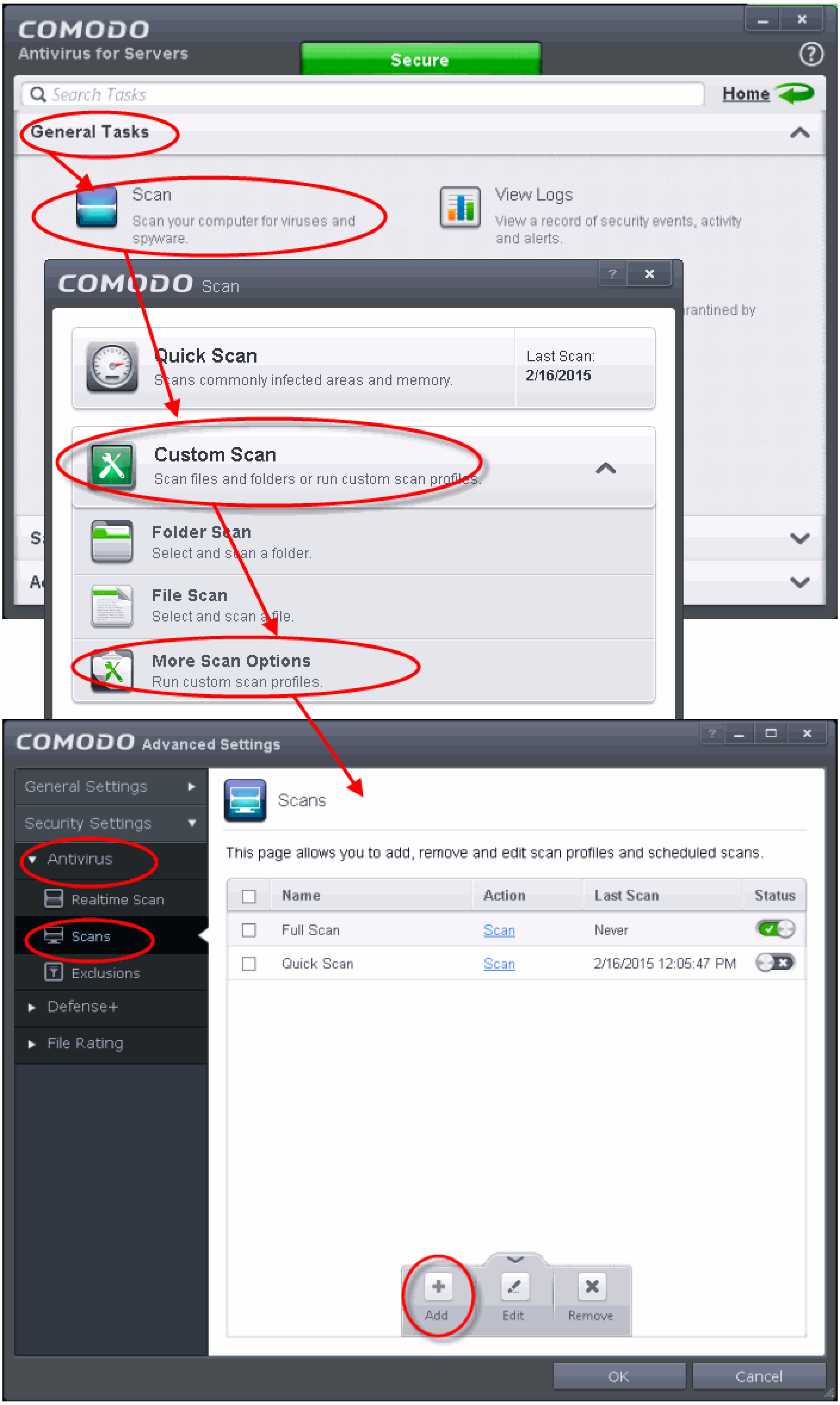
Click here for more details to take action on the infected item(s).

Create an Antivirus Scanning Schedule

CAVS allows you to schedule Antivirus scans on your entire server or on specific areas according to your preferences. You can create a custom scan profile defining exactly which files and folders are to be scanned, when they are to be scanned and how they are to be scanned.

To create an antivirus scanning schedule

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

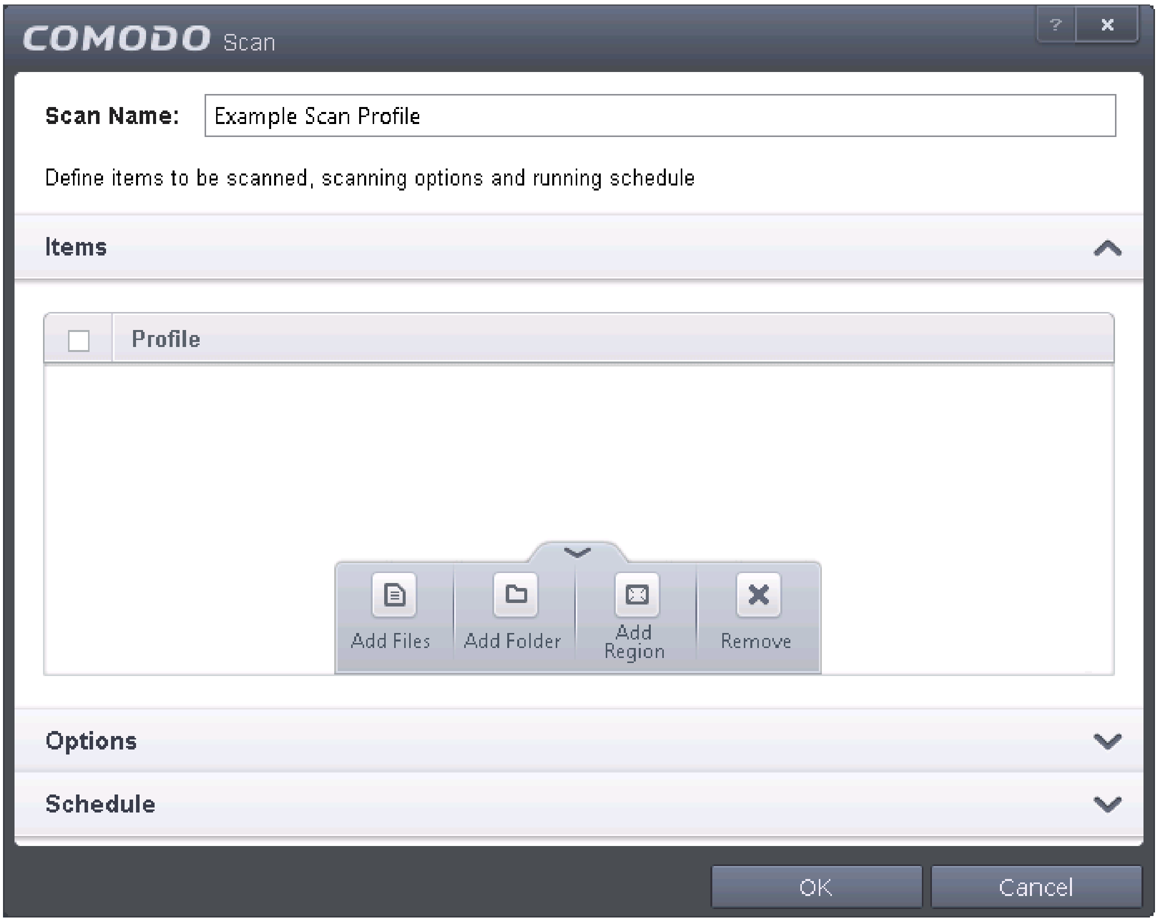


This page allows you to add, remove and edit scan profiles and scheduled scans.

☐	Name	Action	Last Scan	Status
☐	Full Scan	Scan	Never	✓
☐	Quick Scan	Scan	2/16/2015 12:05:47 PM	✗

The scan profile interface will be displayed.

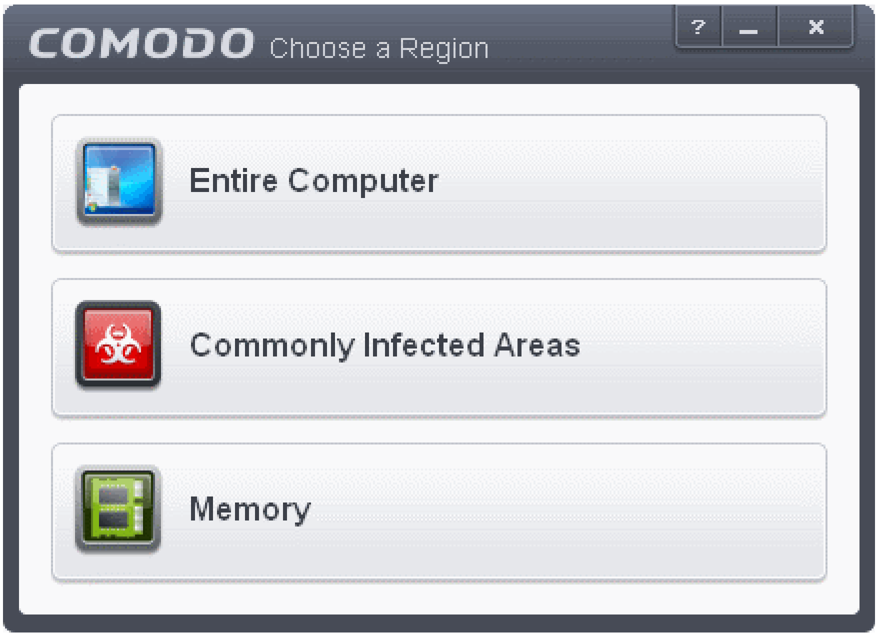
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



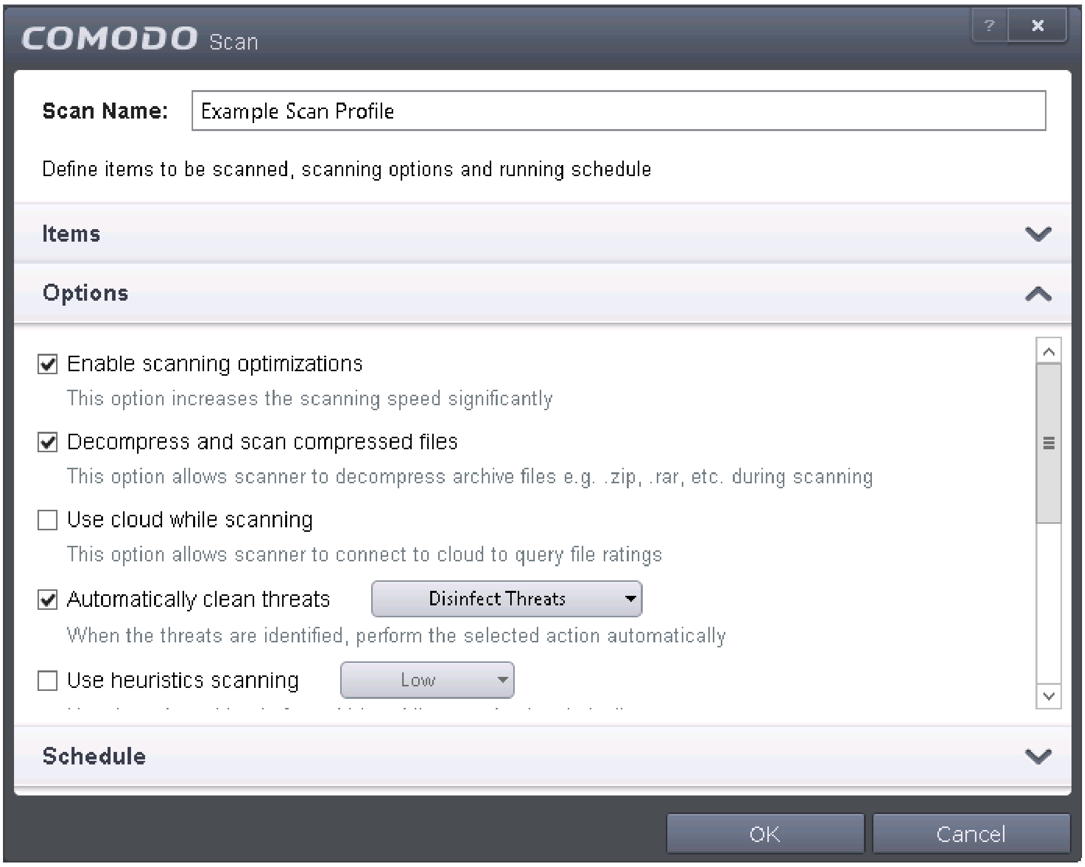
Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

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



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



COMODO Scan

Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Items

Options

☑ Enable scanning optimizations

This option increases the scanning speed significantly

☑ Decompress and scan compressed files

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

□ Use cloud while scanning

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

☑ Automatically clean threats: Disinfect Threats

When the threats are identified, perform the selected action automatically

□ Use heuristics scanning: Low

Schedule

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

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

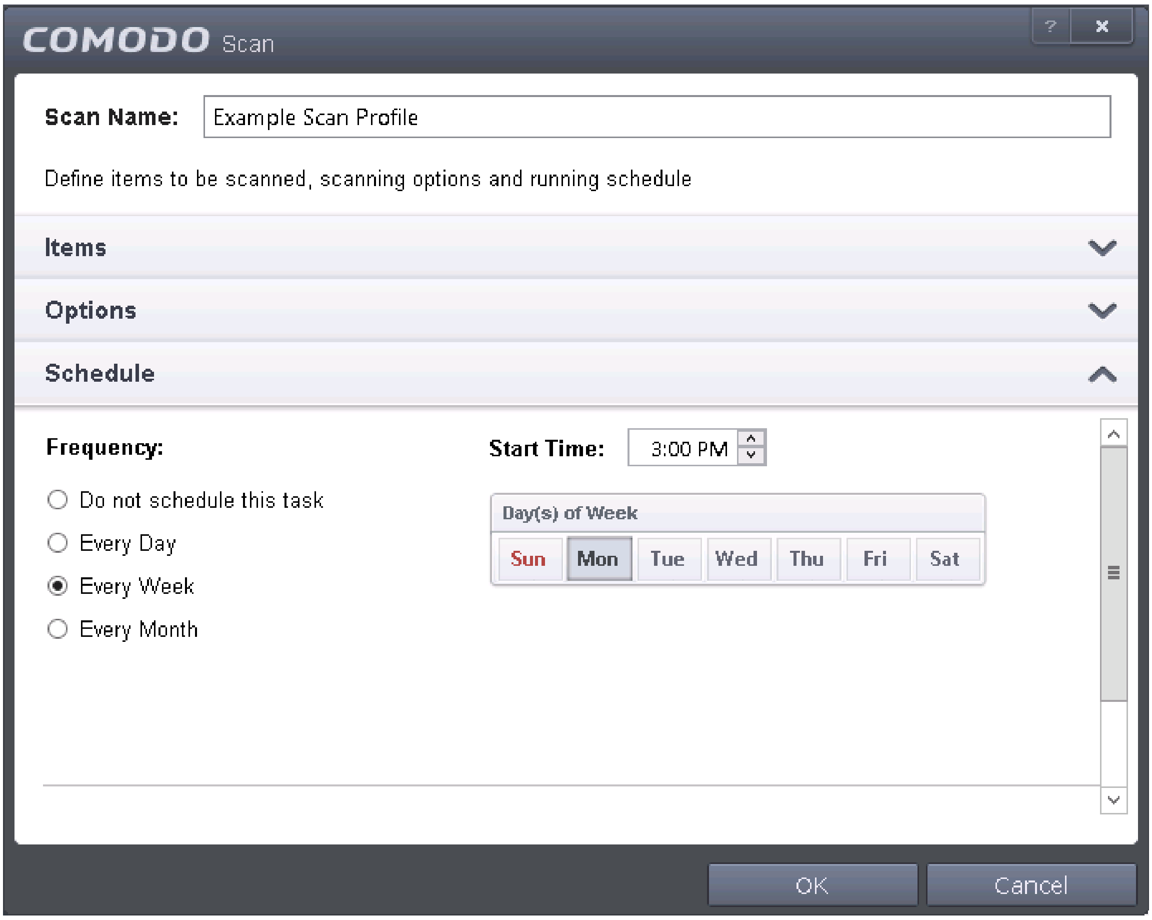
    This allows CAVS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

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

- **Medium -** Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
- **High -** Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

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

- To schedule the scan to run at set intervals, click 'Schedule':



Scan Name: Example Scan Profile

Define items to be scanned, scanning options and running schedule

Frequency:

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

Start Time: 3:00 PM

Day(s) of Week

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

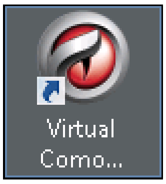
  - **Every Week -** The Antivurus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
  - **Every Month -** The Antivurus starts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

The profile will be saved and the selected areas will be scanned repeatedly as per the set schedule.

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

Run Untrusted Programs in the Sandbox

Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:



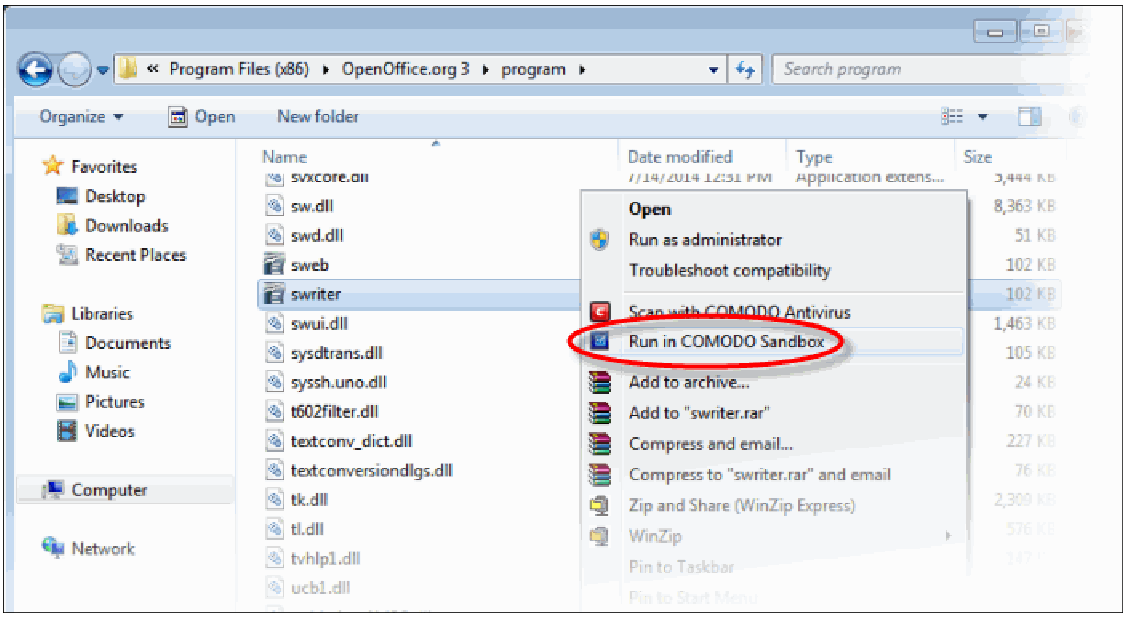
Comodo Antivirus for Servers allows you to run a program in the sandbox:

- **From the right click options**
- **From the Sandbox Tasks interface**

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

Run a program inside the sandbox through right click options

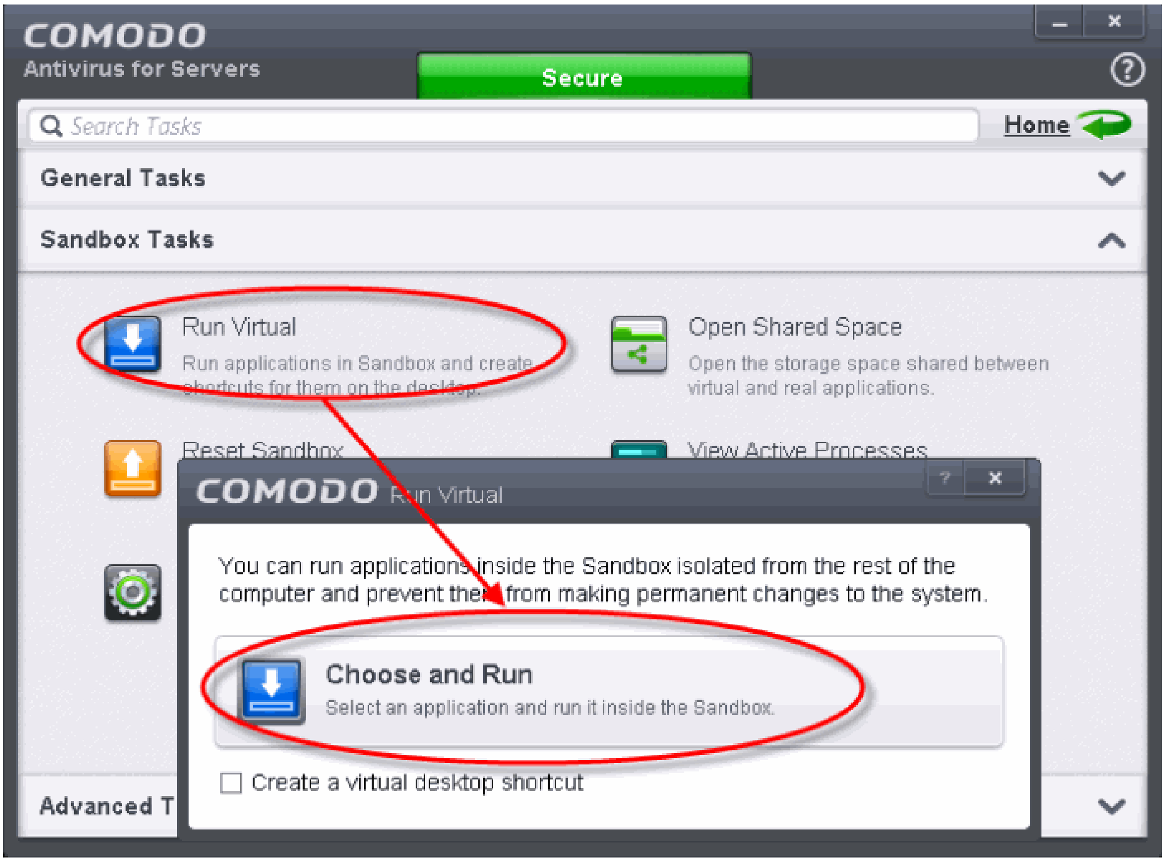
1. Browse to the installation folder of the .exe file through Windows Explorer.
2. Right click on the program that you want to run inside the sandbox.



Choose 'Run in COMODO Sandbox' from the context sensitive menu.

Run a program in sandbox from Sandbox Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Sandbox Tasks' and click 'Run Virtual' from the 'Sandbox Tasks' interface

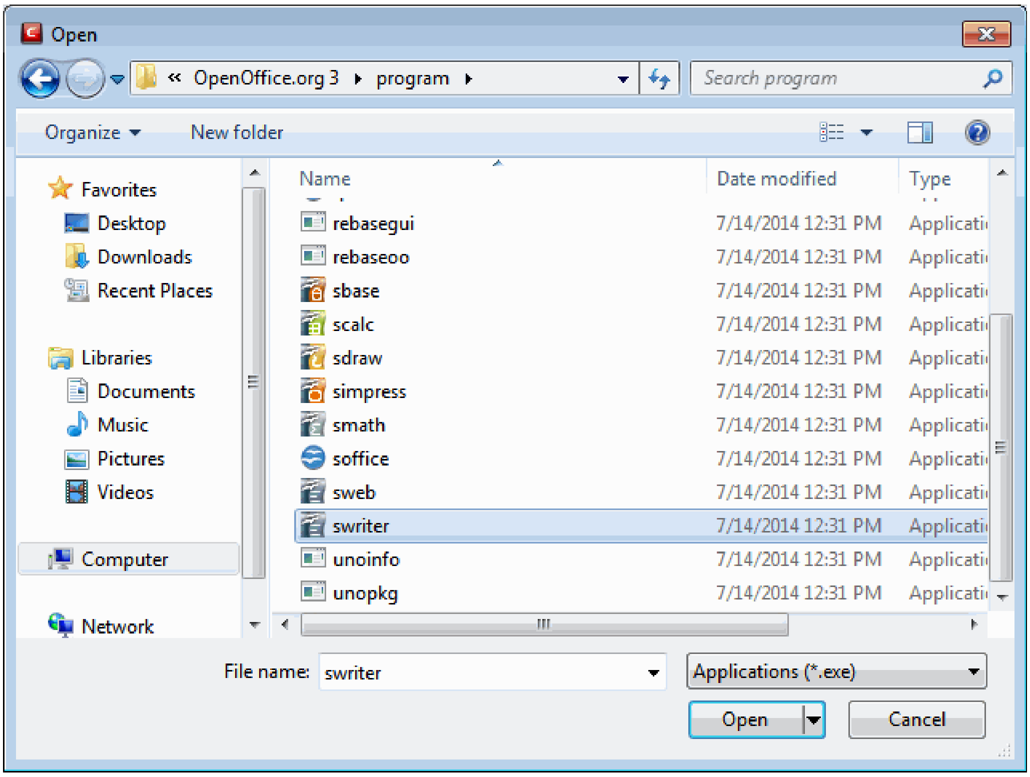

COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Sandbox Tasks
Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset Sandbox
View Active Processes
Advanced T
COMODO Run Virtual
Choose and Run
Select an application and run it inside the Sandbox.

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

□ Create a virtual desktop shortcut

The 'Run Virtual' dialog will be displayed.

3. To run an application inside the sandbox, click 'Choose and Run' then browse to the application. The application will run with a green border indicating that it is sandboxed. If you wish to run the application in the sandbox in future, then select 'Create a virtual desktop shortcut'.



Name	Date modified	Type
rebasegui	7/14/2014 12:31 PM	Applicati
rebaseoo	7/14/2014 12:31 PM	Applicati
sbase	7/14/2014 12:31 PM	Applicati
scalc	7/14/2014 12:31 PM	Applicati
sdraw	7/14/2014 12:31 PM	Applicati
simpress	7/14/2014 12:31 PM	Applicati
smath	7/14/2014 12:31 PM	Applicati
soffice	7/14/2014 12:31 PM	Applicati
sweb	7/14/2014 12:31 PM	Applicati
swriter	7/14/2014 12:31 PM	Applicati
unoinfo	7/14/2014 12:31 PM	Applicati
unopkg	7/14/2014 12:31 PM	Applicati

File name: swriter

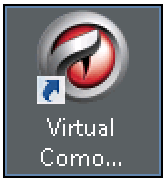
Applications (*.exe)

Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

The application will run in the Sandbox on this occasion only. If you often want the program to run sandboxed then create a 'virtual shortcut' for the application by selecting the check-box 'Create a virtual desktop shortcut'. If you wish to run an application in the sandbox on a long-term/permanent basis then **add the file to the Sandbox.**

Run Browsers Inside Sandbox

This page explains how to run your Internet browser inside the sandbox. Surfing the Internet with a sandboxed browser is the same as normal, with the benefit that any malicious files you inadvertently download cannot do damage your real computer. You can also create a desktop shortcut to run the browser inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:

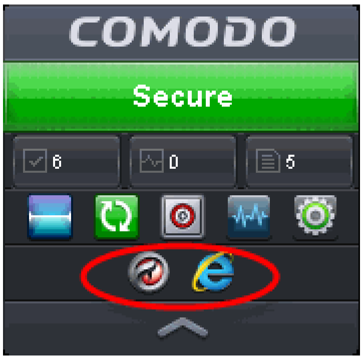


Comodo Antivirus for Servers allows you to run a browser in the sandbox:

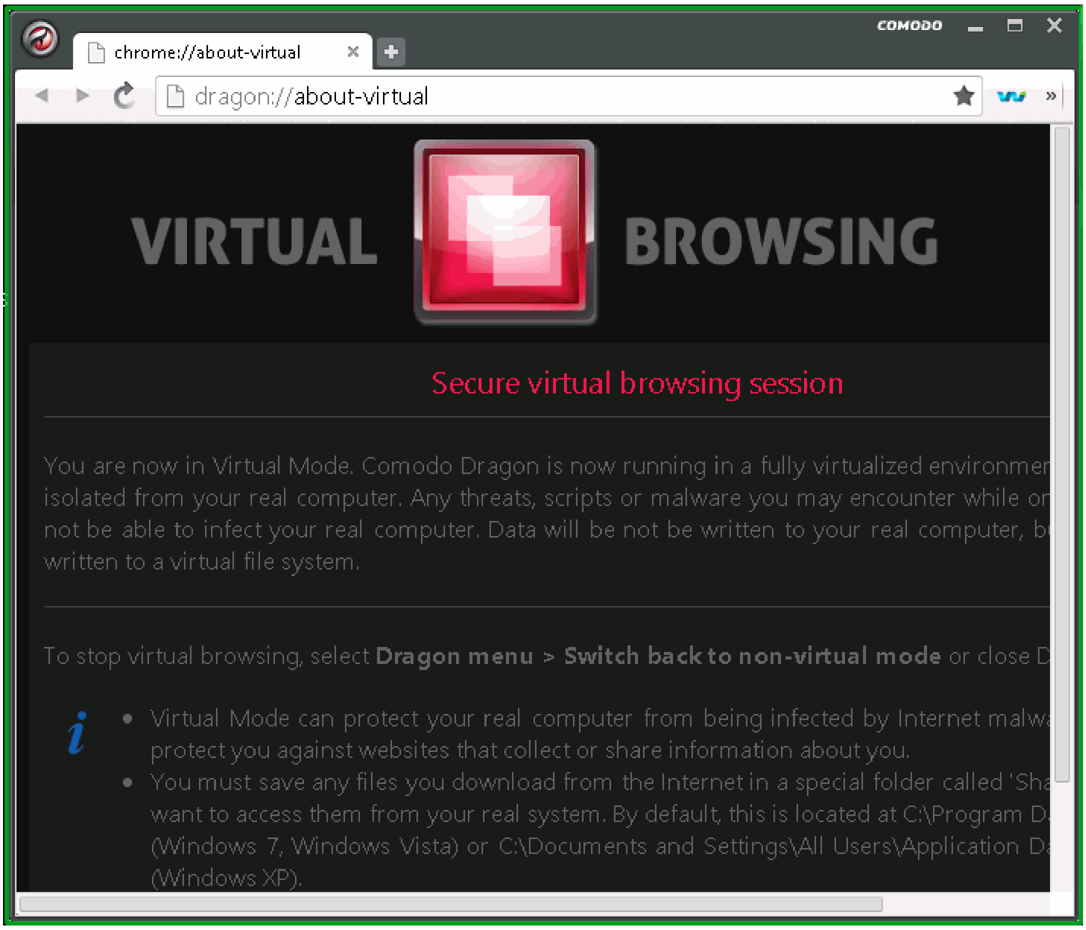
- **From the desktop widget**
- **From the Sandbox Tasks interface**

Starting a browser from the desktop widget

The CAVS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- To start a browser inside the sandbox, click on the browser shortcut icon.



Secure virtual browsing session

You are now in Virtual Mode. Comodo Dragon is now running in a fully virtualized environmen isolated from your real computer. Any threats, scripts or malware you may encounter while or not be able to infect your real computer. Data will be not be written to your real computer, b written to a virtual file system.

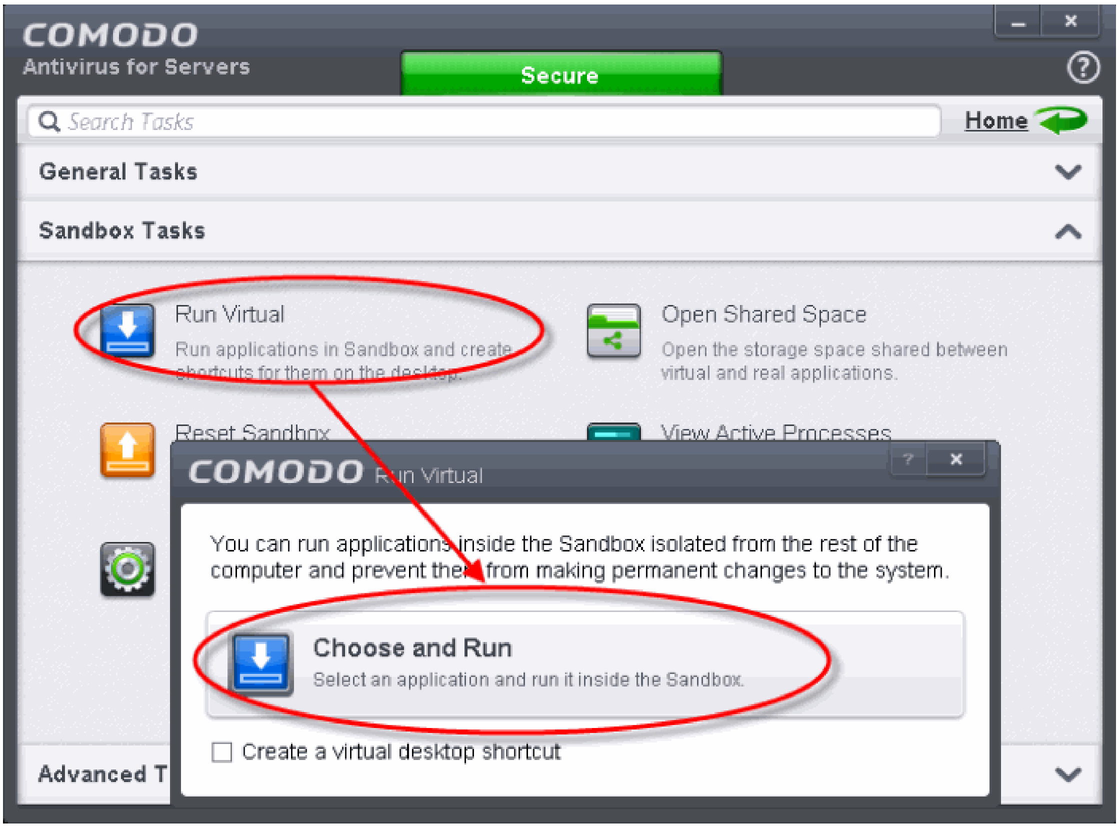
To stop virtual browsing, select **Dragon menu > Switch back to non-virtual mode** or close D

- Virtual Mode can protect your real computer from being infected by Internet malwa protect you against websites that collect or share information about you.
- You must save any files you download from the Internet in a special folder called 'Sha want to access them from your real system. By default, this is located at C:\Program D (Windows 7, Windows Vista) or C:\Documents and Settings\All Users\Application D (Windows XP).

Starting a browser from the Sandbox Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Sandbox Tasks' and click 'Run Virtual' from the 'Sandbox Tasks' interface

   The 'Run Virtual' dialog will be displayed.


COMODO
Antivirus for Servers
Secure
Search Tasks
Home
General Tasks
Sandbox Tasks
Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.
Open Shared Space
Open the storage space shared between virtual and real applications.
Reset Sandbox
View Active Processes
Advanced T
COMODO Run Virtual
You can run applications inside the Sandbox isolated from the rest of the computer and prevent them from making permanent changes to the system.
Choose and Run
Select an application and run it inside the Sandbox.
□ Create a virtual desktop shortcut

3. To run a browser inside the sandbox, click 'Choose and Run', navigate to the installation location of the browser and select the .exe file of the browser. If you wish to create a desktop shortcut to run the browser in the sandbox in future, then select 'Create a virtual desktop shortcut'.

The browser will run with a green border indicating that it is sandboxed.

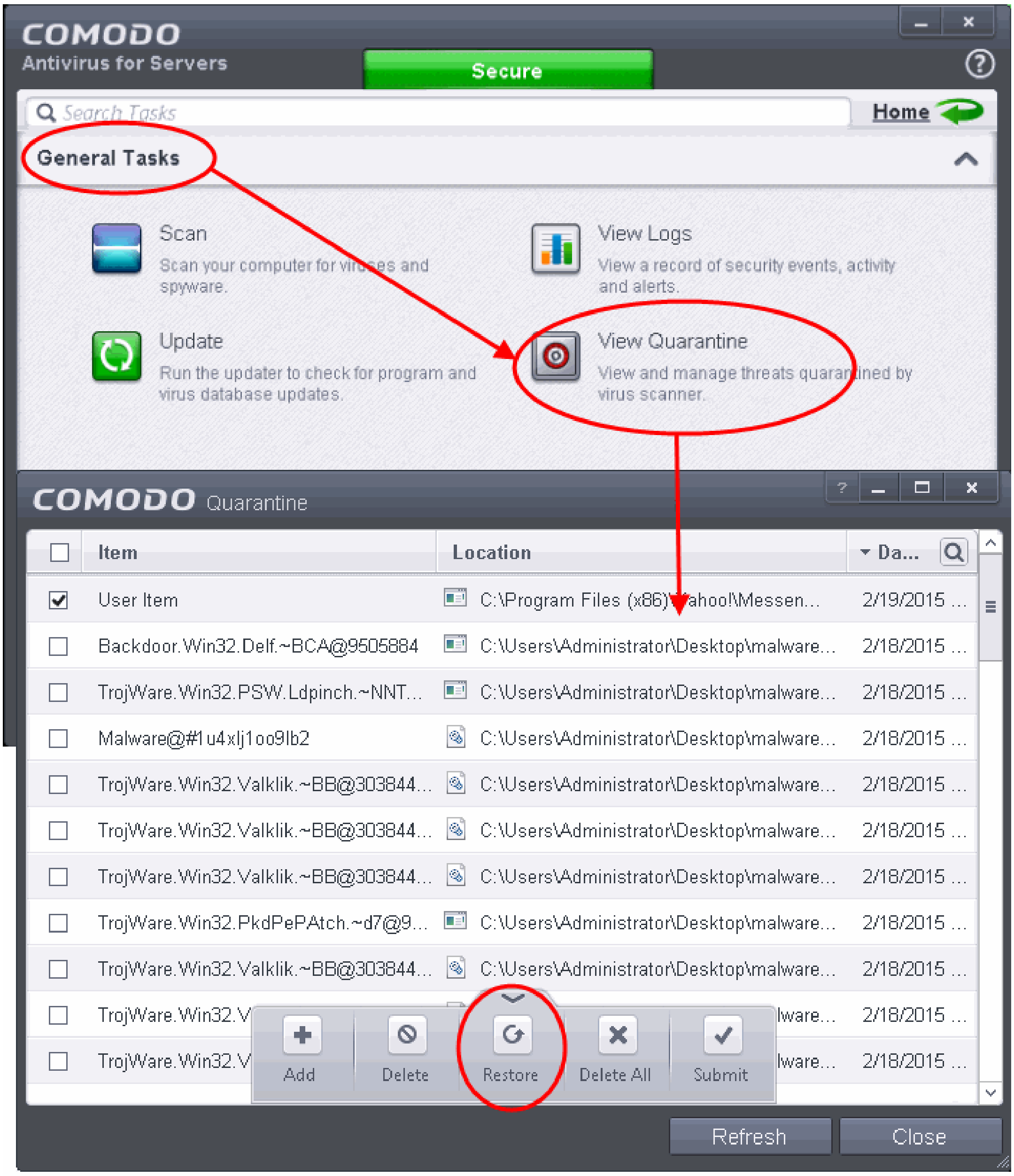
Restoring Incorrectly Quarantined Item(s)

If you have incorrectly quarantined item(s) or you feel an item has been incorrectly quarantined by the application (a false positive) then you can restore it/them using the following procedure:

To submit Quarantined items

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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



Scan
Scan your computer for viruses and spyware.

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

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

View Quarantine
View and manage threats quarantined by virus scanner.

□	Item	Location	Da...
☑	User Item	C:\Program Files (x86)\Yahoo!\Messen...	2/19/2015 ...
□	Backdoor.Win32.Delf.~BCA@9505884	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.PSW.Ldpinch.~NNT...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	Malware@#1u4xlj1oo9lb2	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.PkdPePAtch.~d7@9...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
□	TrojWare.Win32.V	lware...	2/18/2015 ...
□	TrojWare.Win32.V	lware...	2/18/2015 ...

3. Choose the items to be restored by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Restore'.

All the selected files will be restored to their original locations immediately.

5. Click 'Close' button to exit.

Click here for more details on the Quarantined Items.

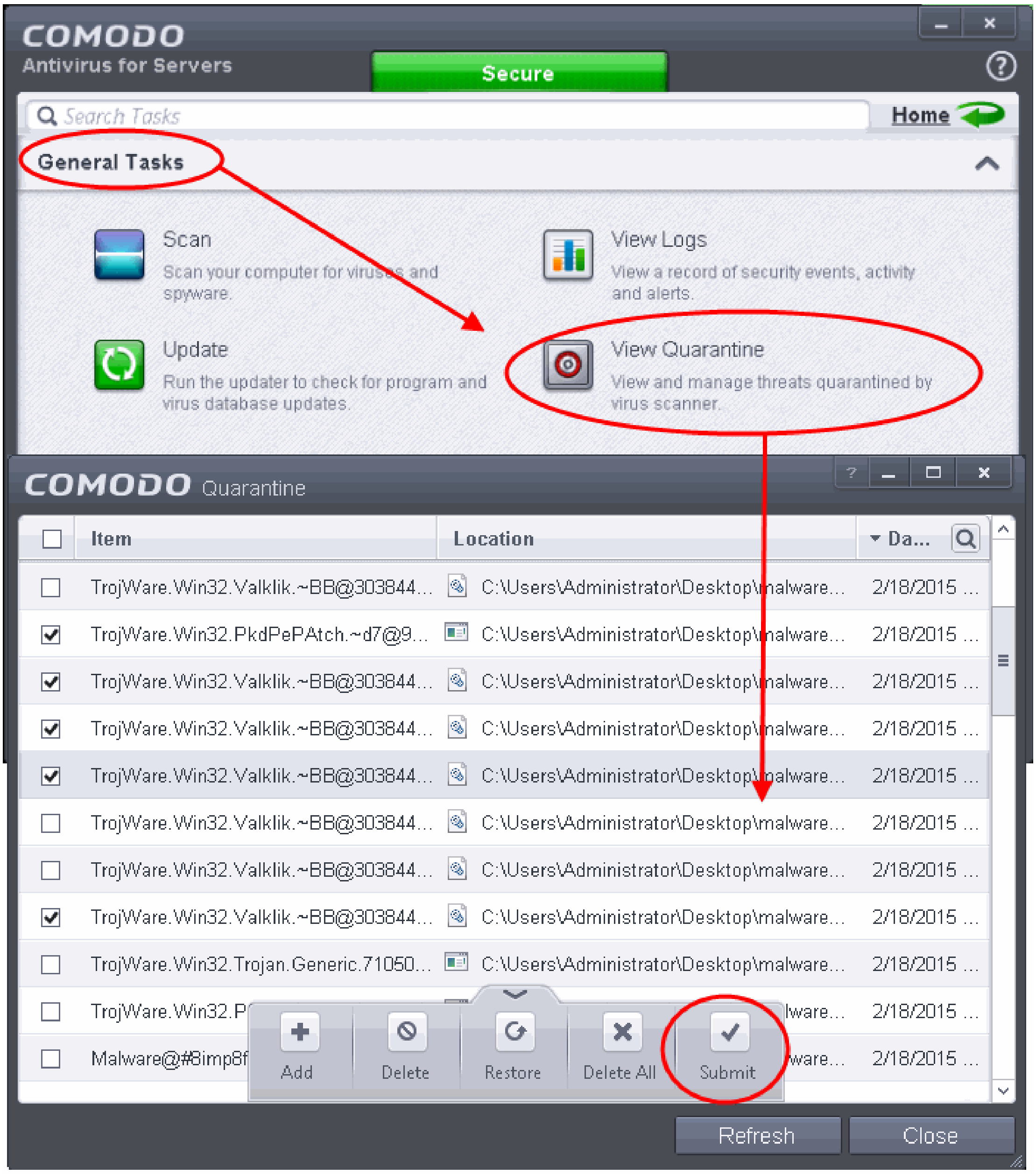
Submit Quarantined Items to Comodo for Analysis

Items which have been quarantined as a result of an On Access, On Demand or Scheduled Scans, can be sent to Comodo for Analysis. After the analysis, if the submitted item is found to be a False Positive, it will be added to Comodo Safe List. Conversely, if it is found to be a malware, it will be added to the anti-malware Black list. This helps Comodo to enhance its virus signature database and helps millions of other CAVS users to benefit out of it. **Click here** for more details on Quarantined Items.

To submit Quarantined items

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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



Scan
Scan your computer for viruses and spyware.

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

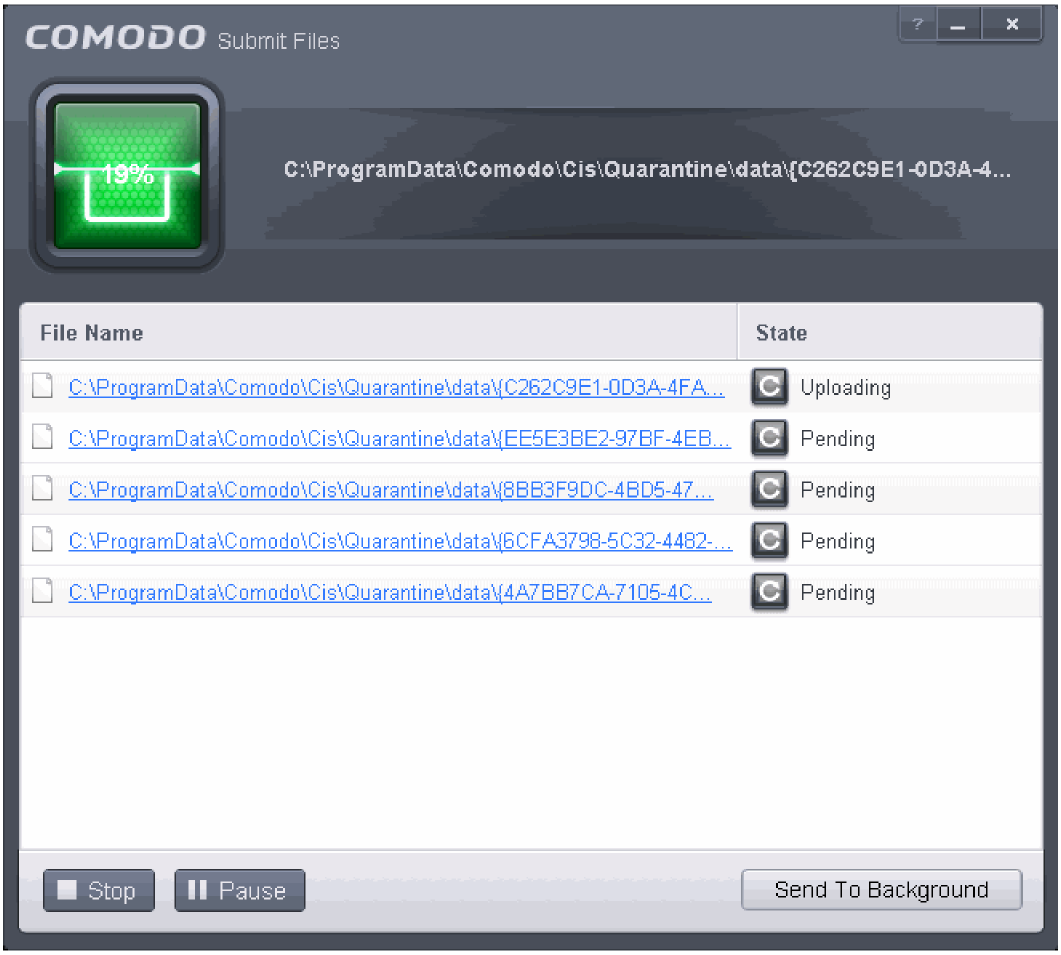
Update
Run the updater to check for program and virus database updates.

View Quarantine
View and manage threats quarantined by virus scanner.

☐	Item	Location	Da...
☐	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☑	TrojWare.Win32.PkdPePAtch.~d7@9...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☑	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☑	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☑	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☐	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☐	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☑	TrojWare.Win32.Valklik.~BB@303844...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☐	TrojWare.Win32.Trojan.Generic.71050...	C:\Users\Administrator\Desktop\malware...	2/18/2015 ...
☐	TrojWare.Win32.P	lware...	2/18/2015 ...
☐	Malware@#8imp8f	ware...	2/18/2015 ...

3. Choose the items to be submitted to Comodo for analysis by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Submit'.

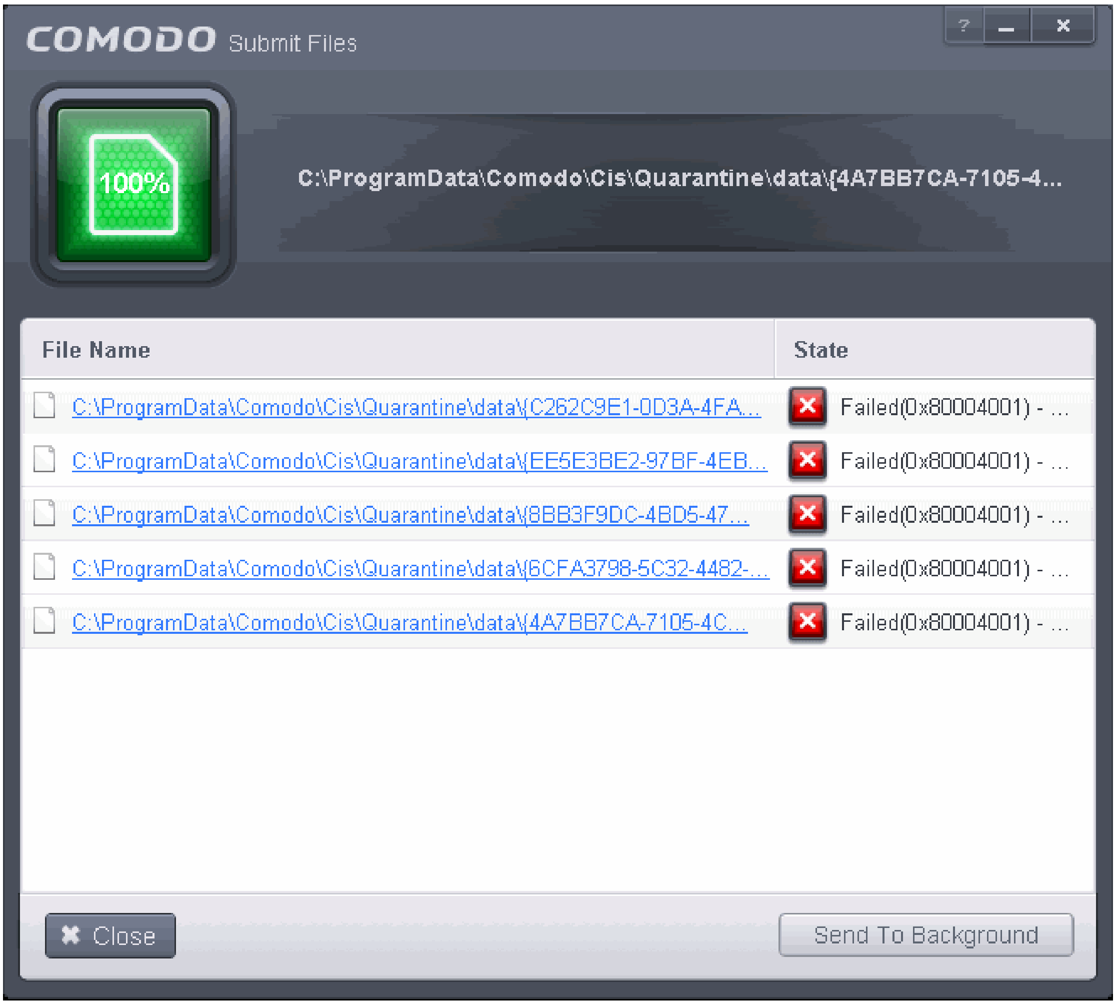
The submission progress will be indicated.



C:\ProgramData\Comodo\Cis\Quarantine\data\{C262C9E1-0D3A-4...

File Name	State
C:\ProgramData\Comodo\Cis\Quarantine\data\{C262C9E1-0D3A-4FA...	Uploading
C:\ProgramData\Comodo\Cis\Quarantine\data\{EE5E3BE2-97BF-4EB...	Pending
C:\ProgramData\Comodo\Cis\Quarantine\data\{8BB3F9DC-4BD5-47...	Pending
C:\ProgramData\Comodo\Cis\Quarantine\data\{6CFA3798-5C32-4482-...	Pending
C:\ProgramData\Comodo\Cis\Quarantine\data\{4A7BB7CA-7105-4C...	Pending

On completion, the submission results will be displayed, indicating whether the file is successfully submitted or already submitted by other users and is pending for analysis.



C:\ProgramData\Comodo\Cis\Quarantine\data\{4A7BB7CA-7105-4...

File Name	State
C:\ProgramData\Comodo\Cis\Quarantine\data\{C262C9E1-0D3A-4FA...	☒ Failed(0x80004001) - ...
C:\ProgramData\Comodo\Cis\Quarantine\data\{EE5E3BE2-97BF-4EB...	☒ Failed(0x80004001) - ...
C:\ProgramData\Comodo\Cis\Quarantine\data\{8BB3F9DC-4BD5-47...	☒ Failed(0x80004001) - ...
C:\ProgramData\Comodo\Cis\Quarantine\data\{6CFA3798-5C32-4482-...	☒ Failed(0x80004001) - ...
C:\ProgramData\Comodo\Cis\Quarantine\data\{4A7BB7CA-7105-4C...	☒ Failed(0x80004001) - ...

Block any Downloads of a Specific File Type

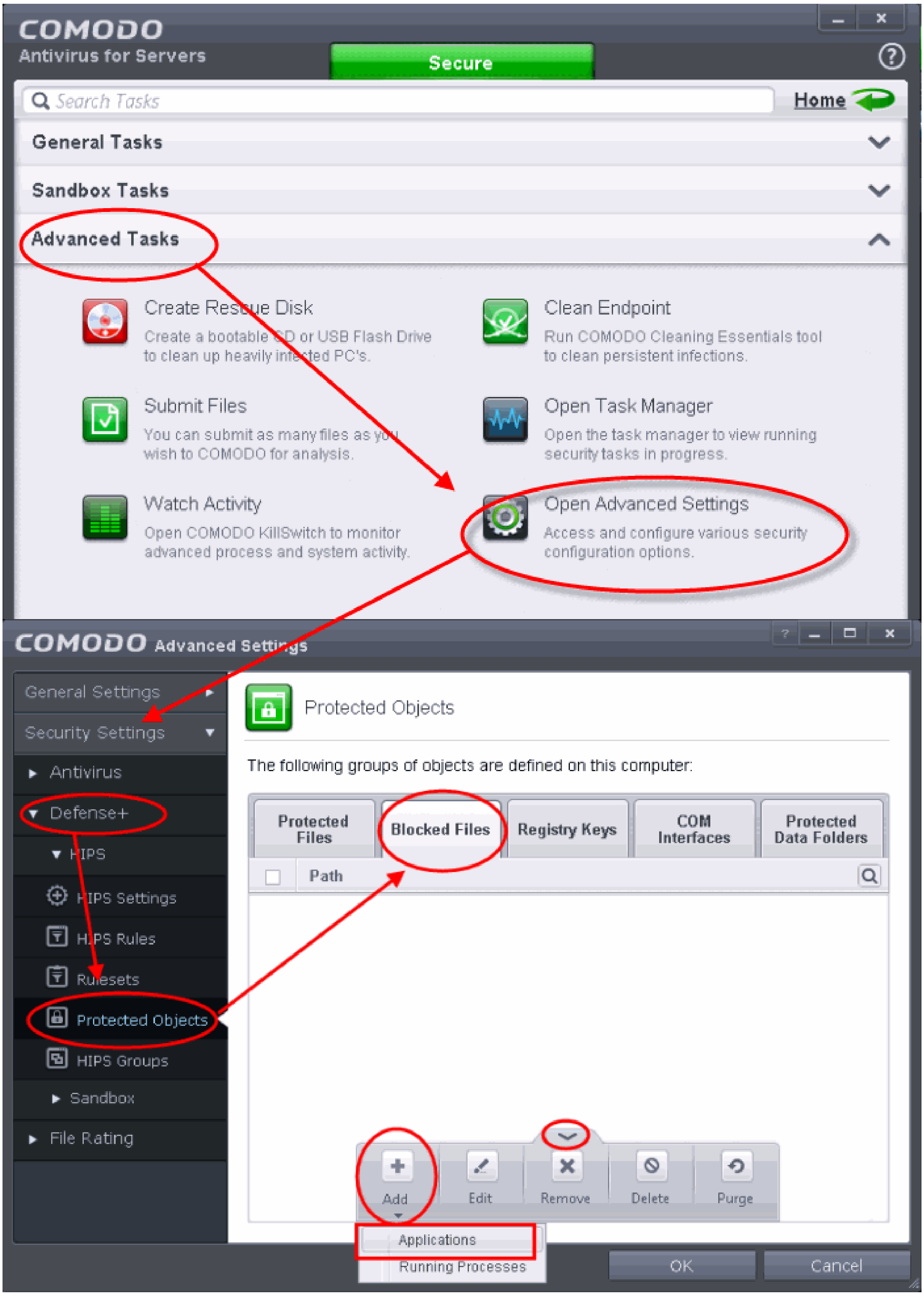
CAVS can be configured to block downloads of specific types of file.

Example scenarios:

- Some malicious websites try to push downloads of malware in .exe file format. .exe files are programs which can execute commands on your server. If the .exe is malicious in intent then these commands could include the installation of key logging programs, initiation of buffer overflow attacks or code to turn your server into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You want to avoid downloading media files like audio files (e.g. files with extensions .wma, .mp3, .wav, .midi), video files (e.g. files with extensions .wmv, .avi, .mpeg, .swf) or image files (e.g. files with extensions .bmp. .jpg, .png) for your disk space restrictions.

To selectively block downloading of specific file type, you need to configure Defense+ component of CAVS to block the specific file type from the default download folder of your browser.

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'HIPS' > 'Protected Objects' from the left hand side pane
4. Click 'Blocked Files' tab



5. Click the handle from the bottom and choose 'Add' > 'Applications'.

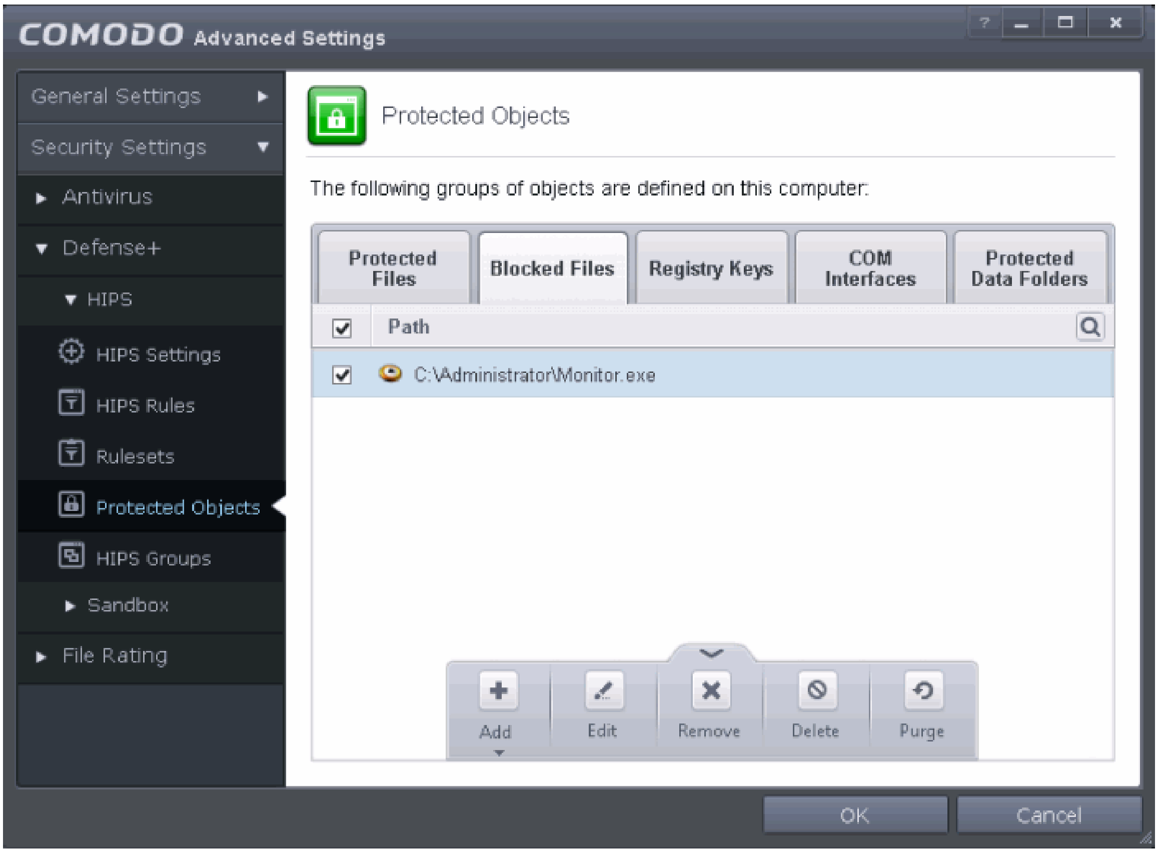
6. Browse to the default download folder for that particular file type of your Internet Browser from the Open dialog

- For example, the default download locations for some file types in Internet Explorer are given below:
  - Executable files - C:\Users\user name\AppData\Local\Temporary Internet Files\
  - Document files - C:\Users\user name\Documents\
  - Image files - C:\Users\user name\Pictures\
  - Music files - C:\Users\user name\Music\

- Video files - C:\Users\user name\Videos\

7. Select file from the folder and click 'Open'

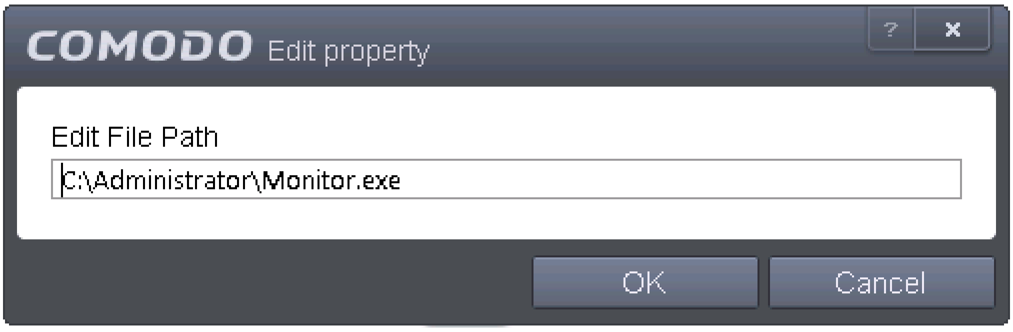
The file will be added to blocked files list.



The following groups of objects are defined on this computer:

☑ C:\Administrator\Monitor.exe

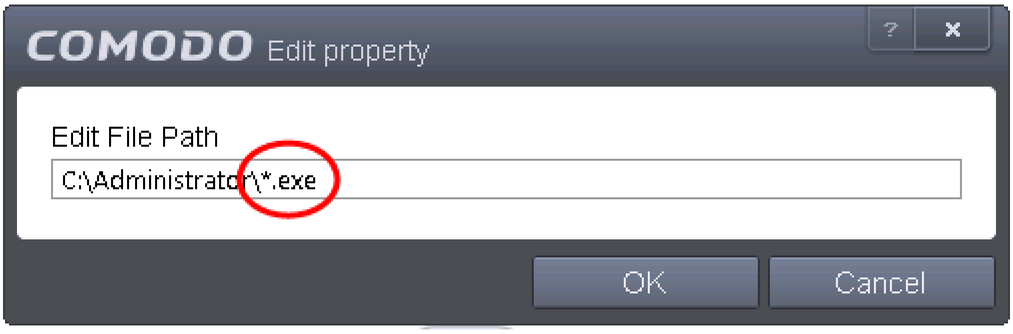
8. Select the entry from the Blocked Files interface, click the handle from the bottom and choose 'Edit'



Edit File Path: C:\Administrator\Monitor.exe

The Edit Property dialog will appear.

9. Change the file name at the end of the file path to *.file_extension” (e.g. *.exe, *.jpg)



Edit File Path: C:\Administrator\*.exe

10. Click 'OK 'in the 'Edit Property' dialog.
11. Click 'OK' in the 'Advanced Settings' interface to save your settings.

The download of the specific file type to the specified folder through the browser will be blocked. If you have more than one browser, repeat the same for the other browsers too.

Note: Blocking files in this way will only block the downloads of the specific file types in the specified folders. If you change the download destination while downloading a file through your web browser, the download will be allowed.

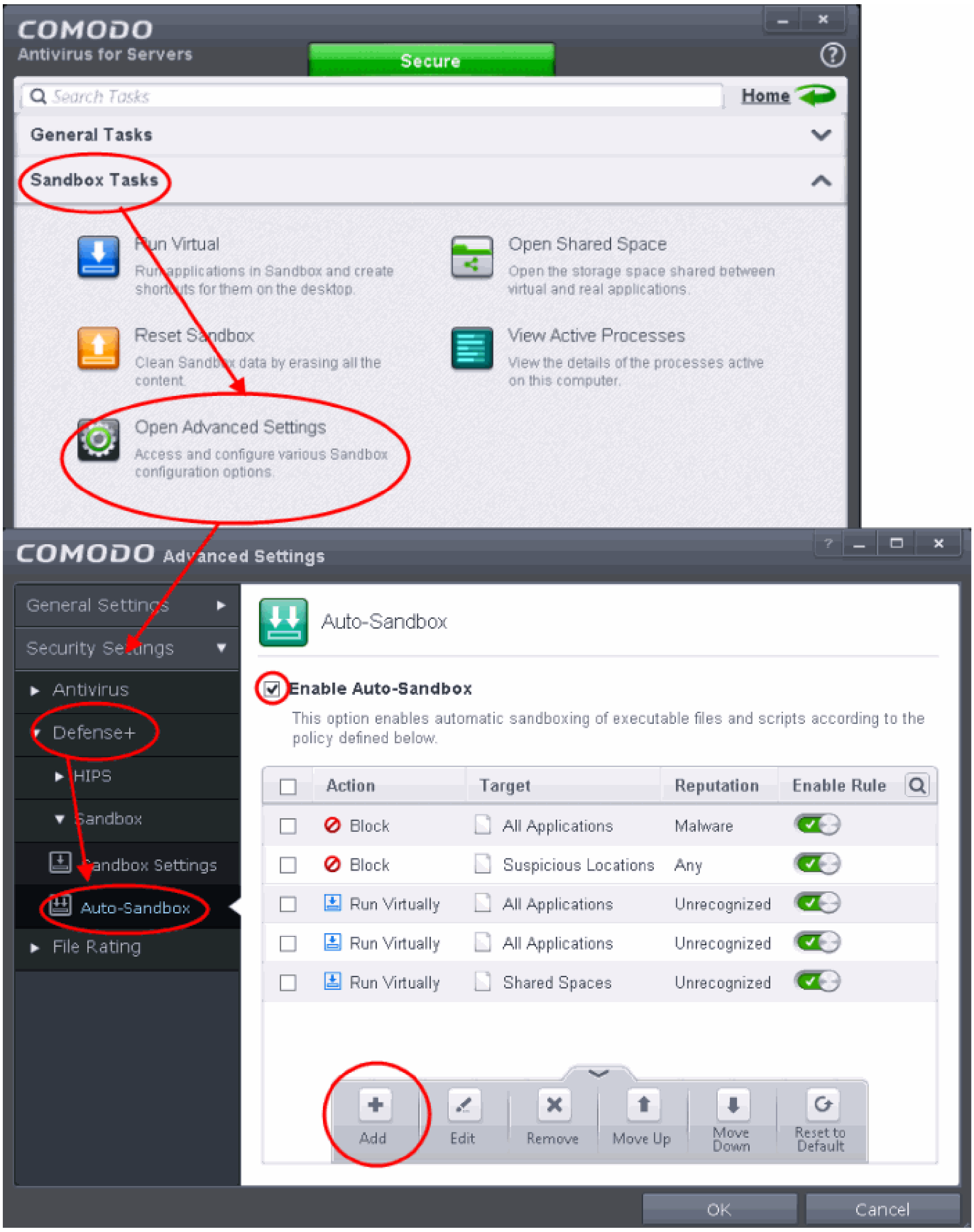
Tip: To unblock the download, Advanced Settings > Defense+ > HIPS > Protected Objects > Blocked Files, select the file path, click the handle from the bottom and choose 'Remove'.

Disable Auto-Sandboxing on a Per-application Basis

The default auto-sandbox rules will run unknown executables in sandboxed environment and queue them for submission to Comodo Cloud scanners for behavior analysis. Users do, however, have the option to exclude specific files or file types from this auto-sandboxing process by creating a rule. This is particularly useful for developers that are creating new applications which, by their nature, are as yet unknown to the Comodo safe list.

To disable the auto-sandboxing selectively

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Sandbox Tasks' and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'Sandbox' > 'Auto-Sandbox' from the left hand side pane
4. Click the handle at the bottom of the interface and open the option panel



Run Virtual
Run applications in Sandbox and create shortcuts for them on the desktop.

Open Shared Space
Open the storage space shared between virtual and real applications.

Reset Sandbox
Clean Sandbox data by erasing all the content.

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

Open Advanced Settings
Access and configure various Sandbox configuration options.

Auto-Sandbox

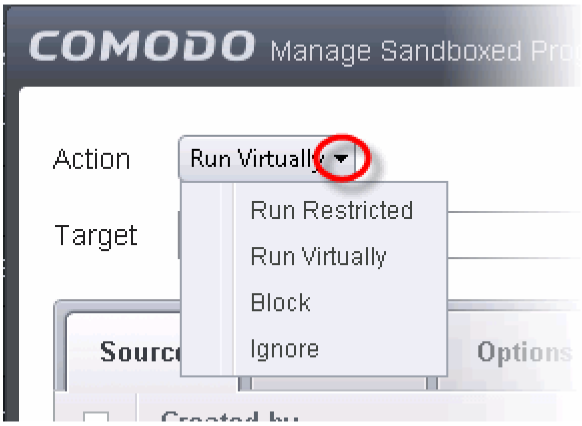
☑ Enable Auto-Sandbox

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

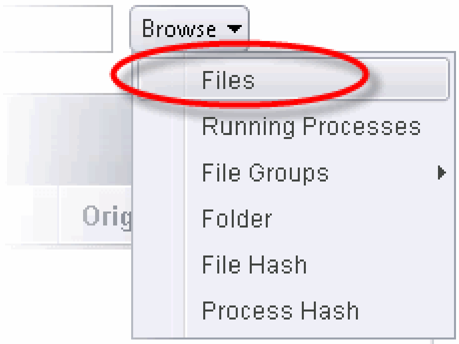
□	Action	Target	Reputation	Enable Rule
□	Block	All Applications	Malware	✓
□	Block	Suspicious Locations	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	Shared Spaces	Unrecognized	✓

5. Click the 'Add' button

6. In the Manage Sandboxed Program interface, select 'Ignore' from the 'Action' drop-down options:

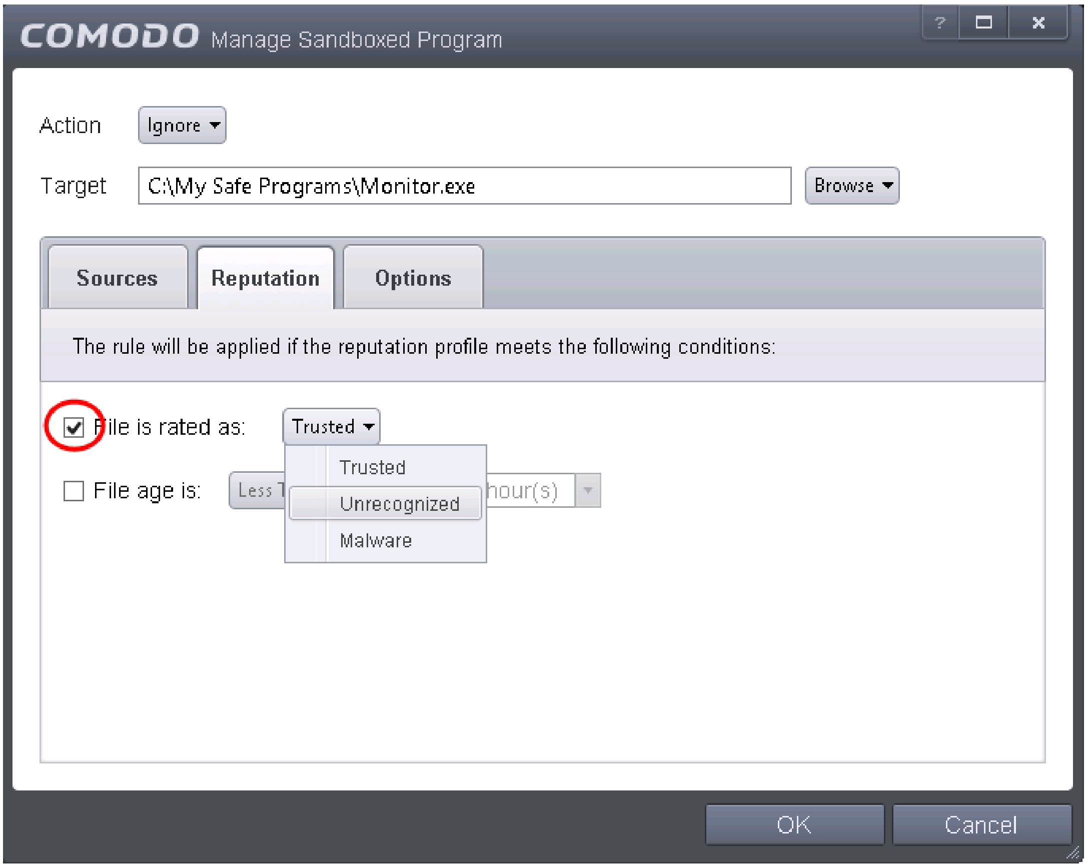


7. By default the Source tab will be selected. Click the Browse button beside the Target field then click Files from the options.



8. Navigate to the location where is the application is installed or stored, select it and click 'Open'. **Click here** for details about adding to target from other options.

9. Click the Reputation tab, select the checkbox beside 'Select file rating' and click 'Unrecognized' from the drop-down options.



Action: Ignore

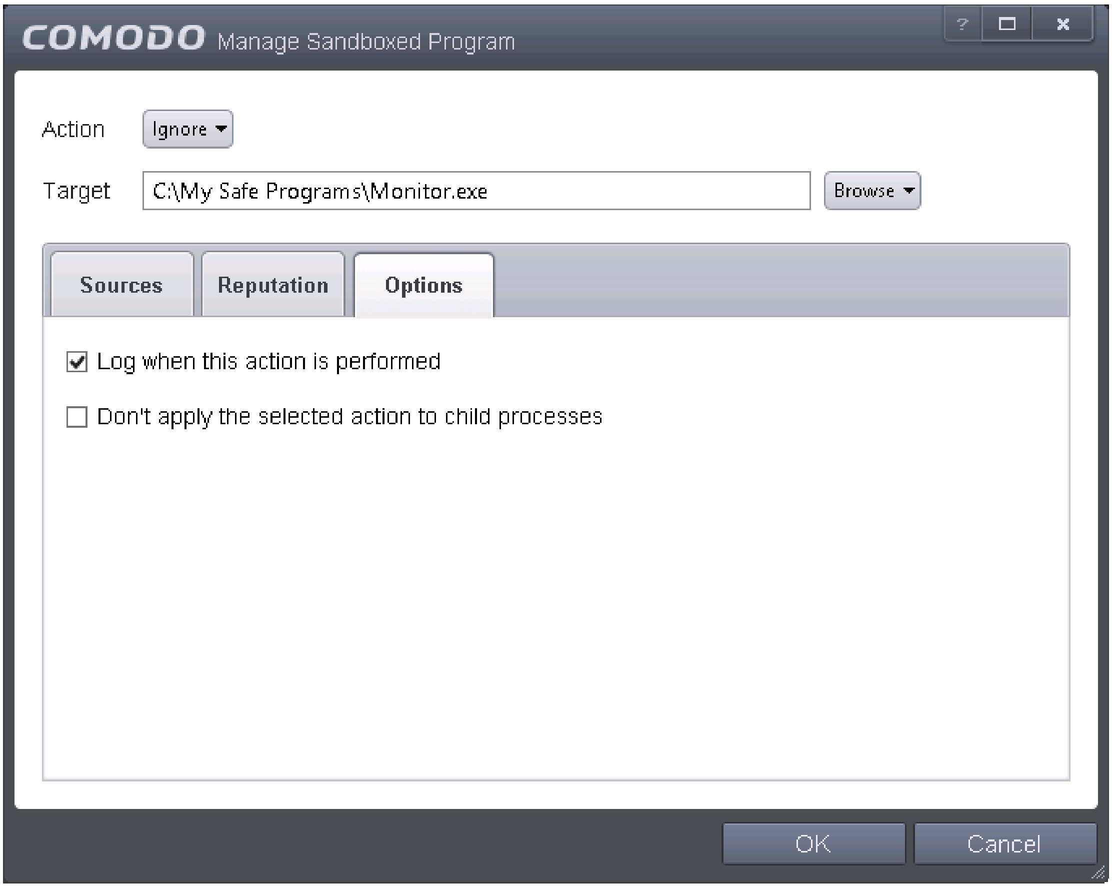
Target: C:\My Safe Programs\Monitor.exe

The rule will be applied if the reputation profile meets the following conditions:

☑ File is rated as: Trusted

☐ File age is:

10. Click the 'Options' tab.



Action: Ignore

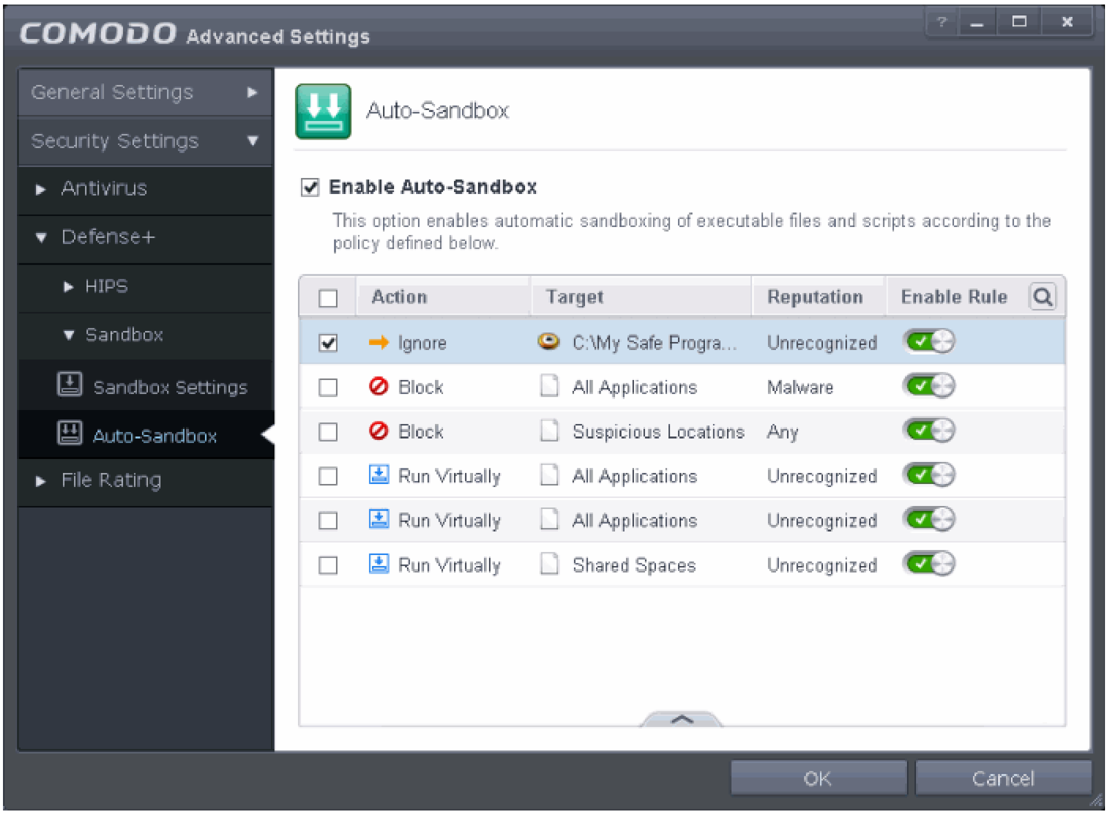
Target: C:\My Safe Programs\Monitor.exe

☑ Log when this action is performed

□ Don't apply the selected action to child processes

- By default, 'Log when this action is performed' will be selected.
- **Log when this action is performed** – Whenever this rule is applied for the action, it will be logged.
- **Don't apply the selected action to child processes** – Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CAVS treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
    - By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
    - If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox rules individually applied as per their file rating.

Select the options as required and click 'OK'.



Auto-Sandbox

☑ **Enable Auto-Sandbox**

This option enables automatic sandboxing of executable files and scripts according to the policy defined below.

□	Action	Target	Reputation	Enable Rule
☑	Ignore	C:\My Safe Progra...	Unrecognized	✓
□	Block	All Applications	Malware	✓
□	Block	Suspicious Locations	Any	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	All Applications	Unrecognized	✓
□	Run Virtually	Shared Spaces	Unrecognized	✓

The Ignore rule will be saved for the specified application and displayed in the Auto-Sandbox screen. Make sure to keep this rule above all other rules for unrecognized files.

Alternatively…

1. Assign Trusted rating to the file from the **File List** interface
2. Digitally sign your files with a code signing certificate from a trusted CA then manually add your organization to the **Trusted Software Vendors** list
3. Disable Auto-Sandbox by de-selecting the 'Enable Auto-Sandbox' check box in the Auto-sandbox settings panel. *Not recommended*.

For more details on creating rules for auto-sandboxing, refer to the section **Configuring Rules for Auto-Sandbox**.

Switch Off Automatic Antivirus and Software Updates

By default, CAVS will automatically check for software and Antivirus database updates. However, some users like to have control over what gets downloaded and when it gets downloaded. For example, network administrators may not wish to automatically download because it will take up to much bandwidth during the day. Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.

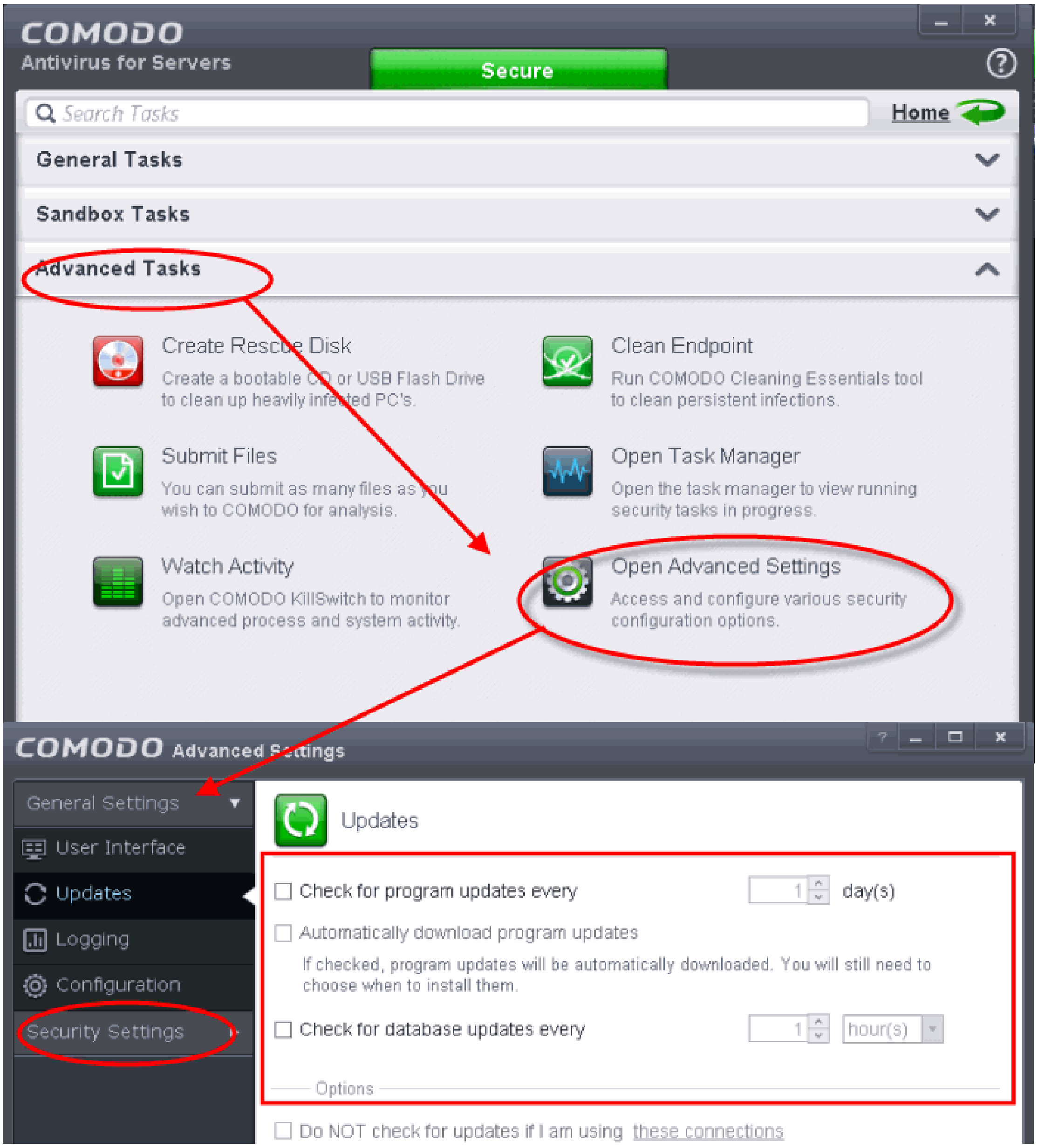
CAVS provides full control over virus and software updates. Click the appropriate link below to find out more:

- **Switch off automatic software and virus signature database updates entirely**
- **Switch off automatic software and virus signature database selectively**
- **Switch off automatic virus signature database updates prior to Antivirus Scans**

To switch off automatic updates entirely:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen

2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane
4. Deselect the check boxes 'Check for database updates every xxx hour(s)'



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Open Task Manager
Open the task manager to view running security tasks in progress.

Watch Activity
Open COMODO KillSwitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

Updates

□ Check for program updates every 1 day(s)

□ Automatically download program updates

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

□ Check for database updates every 1 hour(s)

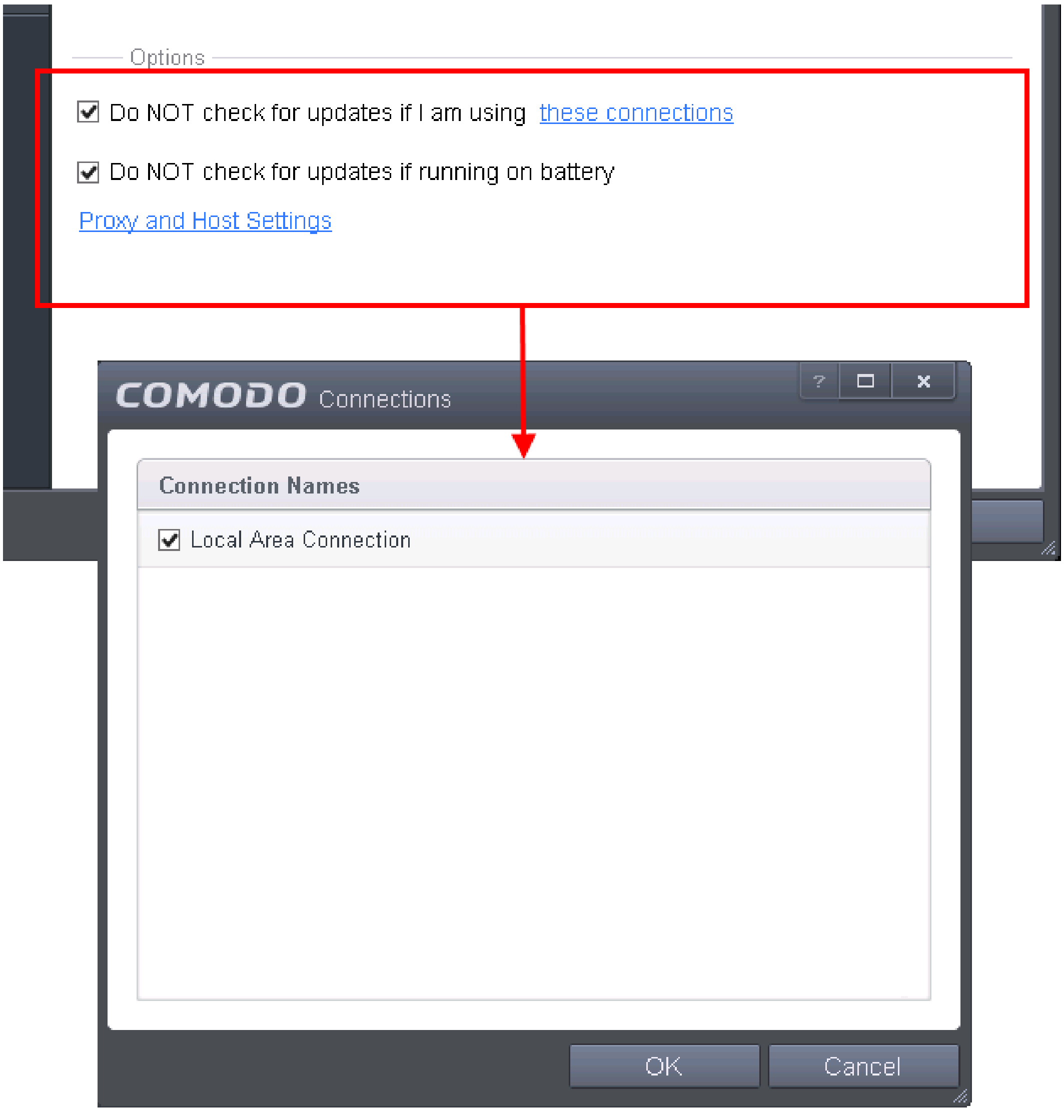
Options

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

5. Click 'OK' in the 'Advanced Settings' panel.

To switch off automatic updates selectively:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking 'Advanced Tasks' > 'Advanced Settings' from the Tasks interface
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane



Options

☑ Do NOT check for updates if I am using these connections

☑ Do NOT check for updates if running on battery

Proxy and Host Settings

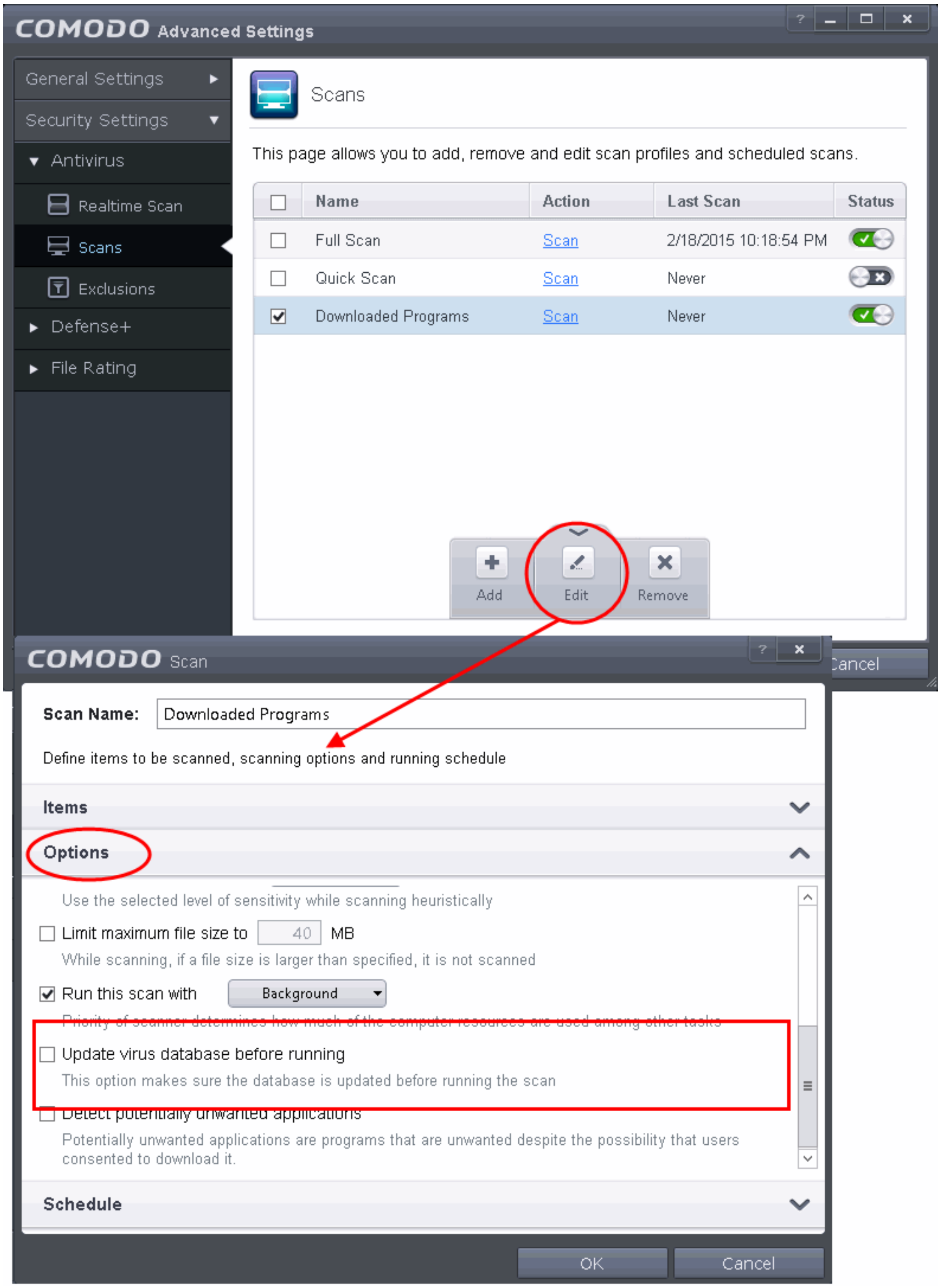
Connection Names
☑ Local Area Connection

- If you want to suppress automatic updates when you are connected to Internet through certain networks
  - Select the 'Do NOT check updates if am using these connections' check-box
  - Then click the 'these connections'. The 'Connections' dialog will appear with the list of connections you use.
  - Select the connection through which you do not want CAVS to check for updates and click OK.
- If you want to suppress automatic updates when your computer is running on battery
  - Select the 'Do NOT check for updates if running on battery' checkbox

To switch off automatic virus signature database updates prior to AV Scans:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking 'Advanced Tasks '> 'Advanced Settings' from the Tasks interface
3. Select the scan profile for which you do want the automatic virus database updates prior to the scan
4. Click the handle from the bottom and select 'Edit'.

5. Click 'Security Settings' > Antivirus' > 'Scans'. A list defined scan profiles will be displayed.



Scans

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

☐	Name	Action	Last Scan	Status
☐	Full Scan	Scan	2/18/2015 10:18:54 PM	✓
☐	Quick Scan	Scan	Never	✕
☑	Downloaded Programs	Scan	Never	✓

Scan Name: Downloaded Programs

Define items to be scanned, scanning options and running schedule

Items

Options

Use the selected level of sensitivity while scanning heuristically

☐ Limit maximum file size to 40 MB

While scanning, if a file size is larger than specified, it is not scanned

☑ Run this scan with Background

Priority of scanner determines how much of the computer resources are used among other tasks

☐ Update virus database before running

This option makes sure the database is updated before running the scan

☐ Detect potentially unwanted applications

Potentially unwanted applications are programs that are unwanted despite the possibility that users consented to download it.

Schedule

6. Click 'Options' to open the Options pane and deselect 'Update virus database before running' checkbox.
7. Click 'OK' on the 'Scan' interface.
8. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

Appendix 2 - Glossary of Common Terms

A B C D E F G H I J **K L M N O P Q R S U V W X** Y **Z**

A

ACK

The acknowledgment bit in a TCP packet. (ACKnowledgment code) - Code that communicates that a system is ready to receive data from a remote transmitting station, or code that acknowledges the error-free transmission of data.

Back to the top

Adware

Adware also known as advertising-supported application is designed as a tool to deliver advertisements that provides a source of revenue to its developer. The ads may appear on the screen during the installation process or on the user interface of the application. Since adware is mostly installed along with another software without the user's knowledge and may be used for malicious activities, the term 'adware' is often associated with malware.

Back to the top

Antivirus

An antivirus software is an application which is capable of detecting and removing malicious software such as viruses, trojans, worms and scripts from a computer system. A traditional (or 'classic') antivirus relies on a system of 'black-listed' signatures to detect malicious software. Under this system, antivirus vendors create digital signatures of any executable identified as malware. They then send this list of signatures to their customer's local antivirus software via regular (often daily) updates. The customer’s antivirus software will then flag as a virus any program with a signature matching a signature on the blacklist.

One drawback with the signature system is its reactive nature – it can only detect 'known' threats. The vendor has to first identify the file as a virus before they can create a signature of it. In many cases, this means the virus has to have already infected someones computer before a signature can be created to combat it.

Because of this limitation, most modern anti-viruses now deploy a wide range of layered technologies to determine the threat level of a particular file. Such technologies include heuristics, behavior analysis, cloud-based scanning, sand-boxing, host intrusion prevention and file-look up services.

Back to the top

Antivirus Scan

An audit performed by an antivirus application in order to detect malware and viruses in the file system and/or memory of a computer.

Back to the top

ARP

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address, also known as MAC address, in an Ethernet local area network.

Back to the top

Attached Resource Computer NETwork (ARCNET)

ARCNET is a local area network (LAN) protocol, similar in purpose to Ethernet or Token Ring. ARCNET was the first widely available networking system for microcomputers and became popular in the 1980s for office automation tasks. It has since gained a following in the embedded systems market, where certain features of the protocol are especially useful.

Back to the top

B

Behavior Analysis

An activity performed by CAVS to determine whether an unknown application in the sandbox is malicious or not. Unknown files are analyzed by Comodo Cloud Scanners and Comodo's Instant Malware Analysis (CIMA) servers. If found to be safe, they will be submitted to Comodo labs for further checks.

Back to the top

Brute-force

Brute-force search is a trivial but very general problem-solving technique, that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

Back to the top

Buffer Overflow

A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations, often causing the process to crash or produce incorrect results. Hackers use buffer overflows as a trigger to execute to execute malicious code.

Back to the top

Bug

Error in a program that cause problems.

Back to the top

C

CA - Certification Authority

A Certificate Authority (CA) is trusted third party that validates ownership information about a web-server then issues an SSL/TLS certificate to the organization that owns the server. The certificate is then placed on the web-server and is used to secure connections between the server and any clients (browsers) that connect to it. For example, an online store would use a certificate to secure its order forms and payment pages.

A Certificate Authority (CA) such as Comodo CA will sign the certificates it issues with their private key. However, for the website’s certificate to operate correctly, there is a reciprocal client side requirement - the internet browser that the visitor is using MUST physically contain the certificate authority’s ‘root certificate'. This root is required to successfully authenticate any website certificates that have been signed by the CA. If the root certificate is not embedded in a browser, then the website's certificate will not be trusted and visitors will see an error message. Certificate Authorities proactively supply browser vendors with their root certificates for inclusion in the browser’s ‘certificate store’ - an internal repository of root certificates that ships with each browser.

Back to the top

CAVS Widget

The CAVS Widget is a handy control panel that shows information about the security status of your server and other useful information. The widget also has shortcuts to common CAVS tasks and taskbar tasks. By default, the widget is displayed on the desktops of Windows Servers running CAVS version 6.0 and above.

Back to the top

COM Interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on a computer. CAVS automatically protects COM interfaces against modification.

Back to the top

Computer Network

A computer network is a connection between computers through a cable or some type of wireless connection. It enables users to share information and devices between computers and other users within the network.

Back to the top

D

Debugging

The process of identifying a program error and the circumstances in which the error occurs, locating the source(s) of the error in the program and fixing the error.

Back to the top

DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices to connect to a network and be automatically assigned an IP address.

Back to the top

Digital Certificate

A digital certificate is a file used to cryptographically bind a company’s Public Key to its identity. Like a driving license or passport binds a photograph to personal information about its holder, a digital certificate binds a Public Key to information about that company. They are issued for between 1 and 5 year validity periods.

Digital certificates are issued by a Certificate Authority like Comodo. Each CA acts as a trusted third party and conducts background checks on a company to ensure they are legitimate before issuing a certificate to them. Apart from providing an encrypted connection between a internet browser and a website, digital certificates are intended to reassure website visitors that the company they are about to make a purchase from can be trusted.

To get a digital certificate, a company must first generate a Certificate Signing Request (CSR) on their web-server. This CSR contains their public key and their identity information. They then enroll and pay for the certificate and send their CSR to the CA.

The CA's validation department will check that the identity information in the CSR is correct by conducting background checks and will sometimes request that the company supplies documentation such as articles of incorporation. Once validation is satisfactorily completed, the CA will issue the certificate to the customer. The customer will then install it on their website to secure sensitive areas like payment pages.

Back to the top

Digital Signature

Digital signatures are used for authentication and integrity, meaning it guarantees that the person sending a message is indeed the same person who he/she claims to be and the message has not been altered. To authenticate oneself using a digital signature, a person needs to download and install Digital Certificates in their systems from Certificate Authorities such as Comodo. The client certificate then can be imported into their browsers and email clients. The same certificate can also be used to digitally sign a document before sending it. The recipient can easily find out if the document has been tampered with en-route.

Back to the top

DNS

DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. When a user searches for a website name like 'www.domain.com', their browser will first contact a DNS server to discover the IP address associated with that domain name. Once it has this information, it can successfully connect to the website in question.

Back to the top

Dynamic IP

The procedure of allocating temporary IP addresses as they are needed. Dynamic IP's are often, though not exclusively, used for dial-up modems.

Back to the top

E

Encryption

Encryption is a technique that is used to make data unreadable and make it secure. Usually this is done by using secret keys and the encrypted data can be read only by using another set of secret keys. There are two types of encryption – symmetric encryption and asymmetric encryption.

Symmetric encryption is applying a secret key to a text to encrypt it and use the same key to decrypt it. The problem with this type of encryption lies during the exchange of secret keys between the sender and the recipient over a large network or the Internet. The secret keys might fall into wrong hands during the exchange process.

Asymmetric encryption overcomes this problem by using two cryptographically related keys, a key pair - a public key and a private key. The private key is kept secret in your system and the public key is made available freely to anyone who might want to exchange messages with you. Any message, be it text, documents or binary files that are encrypted using the public key can be decrypted using the corresponding private key only. Similarly anything that is encrypted using the private key can be decrypted using the corresponding public key. Typically public keys are made available to everyone by using Digital Certificates. The certificates are issued by a Certificate Authority (CA), which identifies a server or user and usually contains information such as the CA who issued it, the organization's name, email address of the user and country and the public key of the user. When a secure encrypted communication is required between a client and a server, a query is sent over to the other party for the certificate and the public key can be extracted from it.

Back to the top

End User

The person who uses a program after it's been compiled and distributed.

Back to the top

EPKI Manager

Enterprise Public Key Infrastructure Manager. The EPKI Manager allows you to issue bulk numbers of:

- SSL Certificates for use on domain names owned by your Company;
- SecureEmail Certificates (S/MIME) for use by employees of your Company.

Your nominated EPKI Manager Administrator(s) will be able to manage all the company's Certificates from a central web based console. Additional certificates may be purchased through the console in minutes; ensuring new servers and employee email may be secured in minutes rather than days. For more information about EPKI Manager click **here**.

Back to the top

Ethernet

Ethernet is a frame-based computer networking technology for local area networks (LANs). The name comes from the physical concept of ether. It defines wiring and signaling for the physical layer, and frame formats and protocols for the media access control (MAC)/data link layer of the OSI model. Ethernet is mostly standardized as IEEEs 802.3. It has become the most widespread LAN technology in use during the 1990s to the present, and has largely replaced all other LAN standards such as token ring, **FDDI**, and **ARCNET**.

Back to the top

Executable Files

An 'executable' is a file that instructs a computer to perform a task or function. Every program, application and device run on computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. For example, when Microsoft Word is started, the executable file 'winword.exe' instructs the computer to start and run the Word application. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Back to the top

F

False Positive

When an antivirus scan is run and the scanner reports that some programs are infected with malware which may not be the actual case and the files are safe. This kind of false alert is called 'False Positive'. Too much of False Postive results can be annoying and the user might just ignore legitimate warning or delete legitimate files causing the relevant program or operating system to malfunction.

Back to the top

Firewall

A firewall is an application that helps an user or administrator to have a control over how the system should be connected with other network/systems or over the Internet.

Back to the top

FS type

Type of file system.

Back to the top

FTP

File Transfer Protocol (FTP) is a protocol used for file transfer from computer to computer across a TCP network like the Internet. An anonymous FTP is a file transfer between locations that does not require users to identify themselves with a password or log-in. FTP uses the TCP/IP protocols to enable data transfer. FTP is most commonly used to download files from a server or to upload a file to a server.

Back to the top

G

Graphical User Interface (GUI)

The visual symbols and graphics with which a user controls a piece of software or device. Most software has a GUI that comprises of windows, menus, and toolbars. The user interacts with the GUI by clicking their mouse on a GUI element. Operating systems like Windows use GUI's because most users find them easier to use than less friendly interfaces like a command line.

Back to the top

H

Heuristics

Heuristics is a technique that continuously evolves based on experience for solving problems, discovery and learning. When the term is used in computer security parlance, Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist. Comodo Antivirus for Servers applies this technology in the application, which is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

Back to the top

HIPS

A Host Intrusion Protection System (HIPS) is designed to identify and block zero malware by monitoring the behavior of all applications and processes. It is designed to prevent actions that could cause damage to your operating system, system-memory, registry keys or personal data.

Security software using a HIPS system will generally enforce rules prescribing the permitted activities of processes and executables at the point of execution. Examples of such activities can include changes to files or directories, accessing protected COM interfaces, modifications to the registry, starting up another application or writing to the memory space of another application. The precise nature of these rules can be set by the user or pre-configured by the vendor.

If an executable or process attempts to perform an action that transgresses these rules then the HIPS system will block the attempt and generate an alert notifying the user of that action. Most HIPS alerts will also include security advice.

Back to the top

HTTP

HTTP (Hypertext Transfer Protocol) is the foundation protocol of the World Wide Web. It sets the rules for exchanges between browser and server. It provides for the transfer of hypertext and hypermedia, for recognition of file types, and other functions.

Back to the top

I

ICMP

The Internet Control Message Protocol (ICMP) is part of Internet Protocol (IP) suite and used to report network applications communications errors, network congestion, timeouts and availability of remote hosts.

Back to the top

IDS

An Intrusion Detection System (IDS) is software/hardware that detects and logs inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Back to the top

IMAP

Internet Message Access Protocol'. IMAP is a method of distributing email. It is different from the standard POP3 method in that with IMAP, email messages are stored on the server, while in POP3, the messages are transferred to the client's computer when they are read. Thus, using IMAP allows you to access your email from more than one machine, while POP3 does not. This is important because some email servers only work with some protocols.

Back to the top

Information Security Exposure

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

Back to the top

Internet Service Provider (ISP)

A company or organization that provides the connection between a local computer or network, and the larger Internet.

Back to the top

IP - Internet Protocol

The Internet Protocol (IP) is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched network. An IP address is a numeric address that is used to identify a network interface on a specific network or subnetwork. Every computer or server on the Internet has an IP address. When a user types a domain name such as www.domain.com into the address bar of their browser, the browser still needs to find the IP address associated with that domain in order to reach the website. It finds the IP address by consulting with a DNS server.

There are currently two versions of IP in use today – IPv4 and Ipv6.

IPv4 (Internet Protocol version 4) was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available.

IPv6 is intended to replace IPv4, which uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

Back to the top

K

Key Logger

Key logger is a software application or a hardware device that keeps tracks of computer activity in real time including the keys that are pressed. Key loggers are used to troubleshoot technical problems in computer systems. The application can also be used for malicious purposes such as to steal passwords and other sensitive information.

Back to the top

L

LAN

A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology running at 10, 100 or 1,000 Mbit/s (1,000 Mbit/s is also known as 1 Gbit/s).

Back to the top

Leak Test

Leak Test is a way to find out how well your system is protected by your security software from external and internal threats. Typically these tests are down-loadable and should not cause any harm to your system while being run. The Firewall Leak Tests are used to test how effective the firewall component of your security software is at detecting and blocking outgoing connection attempts. If an application is able to connect to the Internet without your knowledge, it poses a real danger meaning it can easily retrieve private and confidential information from your system and transmit it.

Host Intrusion Prevention System (HIPS) tests are designed to test how well your security software is capable of protecting your internal system from malicious attacks such as viruses. A good HIPS system will deny the malware from accessing your critical operating system files, registry keys, COM interfaces and running processes.

Back to the top

License

The official terms of use for a specific program. A software license is a legal document since it formally restricts the rights of the user.

Back to the top

M

MAC Address

A Media Access Control (MAC) address is a number that is hardwired in network adapters and is used to identify the device or system in which it is installed.

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

Back to the top

Malicious File

Often called 'Malware', a malicious file is software designed to damage computer systems, steal sensitive information or gain unauthorized access to private computer systems. For example it may be coded to gather sensitive information from a system such as passwords, credit card details and send them back to the creator of the malware.

Back to the top

Malware

Malware is short for 'malicious software'. It is an umbrella term that describes a wide range of malicious software including viruses, trojans, worms, scripts and root kits. When installed on a computer system or network, malware can disrupt operations, steal sensitive and personal information, delete important data, create zombie networks and perform other destructive operations.

Back to the top

N

Network (computer)

Networking is the scientific and engineering discipline concerned with communication between computer systems. Such networks involves at least two computers, which can be separated by a few inches (e.g. via Bluetooth) or thousands of miles (e.g. via the Internet). Computer networking is sometimes considered a sub-discipline of telecommunications.

Back to the top

Network Zone

A Network Zone can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied. The creation of network zones helps an administrator to apply changes for all the computer(s) in selected zone(s).

Back to the top

NIDS

NIDS - Network-Based Intrusion Detection System. Detects intrusions based upon suspicious network traffic. A network intrusion detection system (NIDS) is a system that tries to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic.

Back to the top

NNTP

Network News Transfer Protocol - Refers to the standard protocol used for transferring Usenet news from machine to machine. A protocol is simply a format used to transfer data to two different machines. A protocol will set out terms to indicate what error checking method will be used, how the sending machine will indicate when it is has finished sending the data, and how the receiving machine will indicate that it has received the data.

Back to the top

O

Operating System (OS)

The essential software to control both the hardware and other software of a computer. An operating system's most obvious features are managing files and applications. An OS also manages a computer's connection to a network, if one exists. Microsoft Windows, Macintosh OS, and Linux are operating systems.

Back to the top

P

Ping

Ping is a computer network tool used to test whether a particular host is reachable across an IP network.

Back to the top

PKCS

PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security.

Back to the top

PKCS#7

See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS).

Back to the top

PKCS#10

See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.

Back to the top

PKCS#12

Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

Back to the top

Plugin

A program that allows a Web browser to display a wider range of content than originally intended. For example: the Flash plugin allows Web browsers to display Flash content.

Back to the top

POP2

There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Back to the top

POP3

POP3 is the abbreviation for Post Office Protocol - a data format for delivery of emails across the Internet.

Back to the top

Ports

A computer port is an interface that allows communication between applications or processes running on a host computer and other computers, devices or networks.

Your computer sends and receives data to other computers and to the Internet through a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to Internet using port 80 and port 443. Your e-mail application connects to your mail server through port 25.

Back to the top

Potentially Unwanted Applications

A potentially unwanted application (PUA) is a piece of software that (i) a user may or may not be aware is installed on their computer or server, and/or (ii) may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. Because of this ambiguity, many antivirus companies use the term 'Potentially Unwanted Application' to identify such software.

Back to the top

Q

Quarantined Files

After an antivirus scan, files that are detected as malware may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any files moved into quarantine are encrypted so they cannot be run or executed. This prevents infected files from corrupting the rest of a computer or server.

Back to the top

R

Registry Keys

The Windows Registry serves as an archive for collecting and storing the configuration settings of all computer hardware, software and Windows components. Every time an application or hardware is started, it will access the registry keys relating to it. Applications will also access and modify their registry keys constantly during the course of their execution. As the registry is one of the most regularly accessed parts of Windows, it plays a critical role in the stability, reliability and performance of a computer. Indeed, many computer problems are caused by registry errors. Corrupt keys and invalid keys left by uninstalled applications can often cause severe degradation in system performance, crashes and, in extreme cases, can render a system un-bootable. Inexperienced users are, however, discouraged from making manual adjustments to the registry because a single change can have potentially devastating consequences. There are several dedicated registry cleaners available today, including **Comodo PC TuneUp**.

Back to the top

S

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email encapsulated in MIME.

Back to the top

Single User Certificate

A single use certificate refers to the x.509 and associated private key generated by SecureEmail on Alice; stored on SES and downloaded by Bob after a successful SSL client authentication.

Back to the top

SMB

A message format used by DOS and Windows to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include Lan Manager, Windows for Workgroups, Windows NT, and Lan Server. There are also a number of products that use SMB to enable file sharing among different operating system platforms.

Back to the top

SMTP

Simple Mail Transfer Protocol is the most widely used standard for email transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred.

Back to the top

SNMP

Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Back to the top

Spyware

Spyware is a program that performs certain actions without the consent of the user such as displaying advertisements, collecting personal and sensitive information and changing the configuration of the computer. Not all tracking software are malicious since you may have agreed to the conditions as a trade-off for obtaining certain services for free. The tracking software will monitor your online activities to decide what kind of ads should be shown for you.

Back to the top

SSL

Secure Sockets Layer (SSL) is a commonly used protocol for ensuring secure message transmission on the internet. It facilitates an encrypted connection between a web server and an internet browser. It was developed by Netscape in 1994 as a direct response to growing concerns over internet security.

The encryption provided by SSL means that all data passed between a web server and a browser is private and cannot be eavesdropped on. You can tell if you are in an SSL session if the URL begins with https.

SSL is used on the payment pages of millions of websites to protect their online transactions with their customers.

Back to the top

STATIC IP

An IP address which is the same every time you log on to the Internet. See IP for more information.

Back to the top

Stealth Port

Port Stealthing is a security technique whereby ports on an Internet connected PC are hidden so that they provide no response to a remote port scan.

A computer sends and receives data to other computers and to the Internet through an interface called a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, most computers connect to the internet using ports 80 and port 443. Most e-mail applications connect to their mail server through port 25. A 'port scanning' attack consists of sending a message to each port to find out which are open and which are being used by services. With this knowledge, a hacker can determine which attacks are likely to work against a particular computer. Port stealthing effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt ('closed' ports respond with a 'closed' reply- revealing to the hacker that there is actually a PC in existence).

Back to the top

Stateful Packet Inspection

Stateful Packet Inspection, also known as SPI, is an enhanced firewall technique that uses dynamic packet filtering method over the older method of static packet filtering. SPI scrutinizes the packet contents, monitors traffic and keeps track of the sources of packets. A network administrator can configure the firewall that uses SPI according to the needs of the organization, for example, close ports until requested by legitimate users to open them.

Back to the top

SYN

SYN (synchronize) is a type of packet used by the Transmission Control Protocol (TCP) when initiating a new connection to synchronize the sequence numbers on two connecting computers. The SYN is acknowledged by a SYN/ACK by the responding computer.

Back to the top

T

TCP

TCP stands for Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Back to the top

Token-Ring

LAN technology was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5 by the Institute of Electrical and Electronics Engineers. Initially very successful, it went into steep decline after the introduction of 10BASE-T for **Ethernet** and the EIA/TIA 568 cabling standard in the early 1990s. A fierce marketing effort led by IBM sought to claim better performance and reliability over Ethernet for critical applications due to its deterministic access method, but was no more successful than similar battles in the same era over their Micro Channel architecture. IBM no longer uses or promotes Token-Ring. Madge Networks, a one time competitor to IBM, is now considered to be the market leader in Token Ring.

Back to the top

Trojan

A Trojan is a type of malware that looks like a legitimate piece of software and users are tricked to install and execute in their computers. The malware takes the name from the Greek mythology, Trojan Horse, a wooden horse that was used by the Greeks to infiltrate the city of Troy. Once the malware is activated, it can damage the system, spread other computer viruses and also create a back door so as to allow online fraudsters to take access or control the system.

Back to the top

Trusted Files

In Comodo Antivirus for Serverrs, a trusted file is one that is considered safe and is allowed to run on a user's server. This type of file can also be referred to as a 'safe' file or a 'white-listed' file.

A file will be treated as safe if it is in the 'Trusted Files' list OR if it is digitally signed by a 'Trusted Software Vendor'. CAVS ships with a list of trusted files and a list of Trusted Vendors. Users can add their own trusted files and vendors to their local installation. They can also submit files and vendors to Comodo so they can be considered for inclusion in future safe lists.

Back to the top

Trusted Software Vendor

A Trusted Software Vendor (TSV) is a publisher of software that is automatically trusted by CAVS software. Executable files that have been digitally signed by a TSV will be allowed to run normally and will not be placed in the sandbox.

Many software vendors digitally sign their software with a code signing certificate. Digitally signed software helps a user to identify the publisher and to be sure that the software he/she is downloading is genuine and has not been tampered with. Each code signing certificate is counter-signed by a trusted certificate authority (CA) after the CA has conducted detailed checks that the vendor is a legitimate company.

Back to the top

U

User

A person who uses a computer, including a programmer or **end user**.

Back to the top

V

Virtual Machine (VM)

Virtual machine is a software application that emulates a computing environment in which a program or an operating system can be installed and run. There are many advantages in using a VM such as for testing out new applications or procedures without affecting the host system.

Back to the top

Virus

A computer virus is an executable application capable of causing damage to computer files, folders and components. Viruses are also capable of self-replication so can infect multiple items on a system if left unchecked. The malicious activities performed by a virus are wide ranging and include stealing confidential information, modifying user data, overwriting or damaging files and erasing hard disk content.

Back to the top

Virus Database

A database of the digital signatures of all known computer viruses and malware. This database, sometimes referred to as a 'black list', enables **antivirus software** to detect any malware running on a customer's computer.

Every time a file or executable is identified as being malware, antivirus companies will create a digital signature of the file and add it to their database of blacklisted files. This database is then distributed to their customers as an update to their antivirus software. If the blacklisted signature of the malware is found anywhere on a customers computer, then the file is flagged as infected and may be quarantined or deleted.

Comodo has a dedicated team of technicians and crawlers that are continually searching for new virus strains to add to our database. Comodo's virus database is available for public download at **http://internetsecurity.comodo.com/updates/vdp/database.php**

Back to the top

Vulnerability

In network security, a vulnerability refers to any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network.

Back to the top

W

Web server

The term Web server can mean one of two things:

1. A computer that is responsible for accepting **HTTP** requests from clients, which are known as Web browsers, and serving them Web pages, which are usually HTML documents and linked objects (images, etc.).

2. A computer program that provides the functionality described in the first sense of the term.

Back to the top

Worm

A Worm, another type of malware, unlike virus is capable of spreading from computer to computer without any human help. The worm with its capability to replicate itself several times over consumes most of the system memory causing the computer to slow down or crash altogether. It can also cause bandwidth jam while spreading to other computers in the network.

Back to the top

Wildcard

Wildcards are symbols that add flexibility to a keyword search by extending the parameters of a search word. A wildcard item is usually denoted with the asterisk symbol, '*'. This stands for one-or-more characters (useful for all suffixes or prefixes). In digital certification terms, a 'wildcard certificate' means that the certificate will secure the domain plus unlimited sub-domains of that domain. A wildcard certificate is applied for using the format '*.domain.com'.

Back to the top

X

X.509

An internationally recognized standard for certificates that defines their required parts

Back to the top

Z

Zero-Day Malware

Zero-day malware describes new computer viruses or worms that have been discovered in the public realm but which antivirus vendors have not yet created a digital signature for. The term means that the antivirus companies have had 'zero-days' to react. New malware can reasonably be called 'zero-day' for the the length of time between its discovery and the creation of a signature to combat it. For most antivirus vendors, this is usually measured in a matter of hours. Of course, the malware itself may have been at large for a much longer period of time before it was discovered. Because of this window of vulnerability, most security software has grown beyond a reliance on traditional, signature based detection. Most antivirus software now contains layers of prevention-based technologies intended to detect and neutralize 'unknown' malware until such time as a signature can be created. Example technologies include heuristic detection, host intrusion prevention (HIPS), automatic sandboxing and real-time behavior analysis.

Back to the top

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**