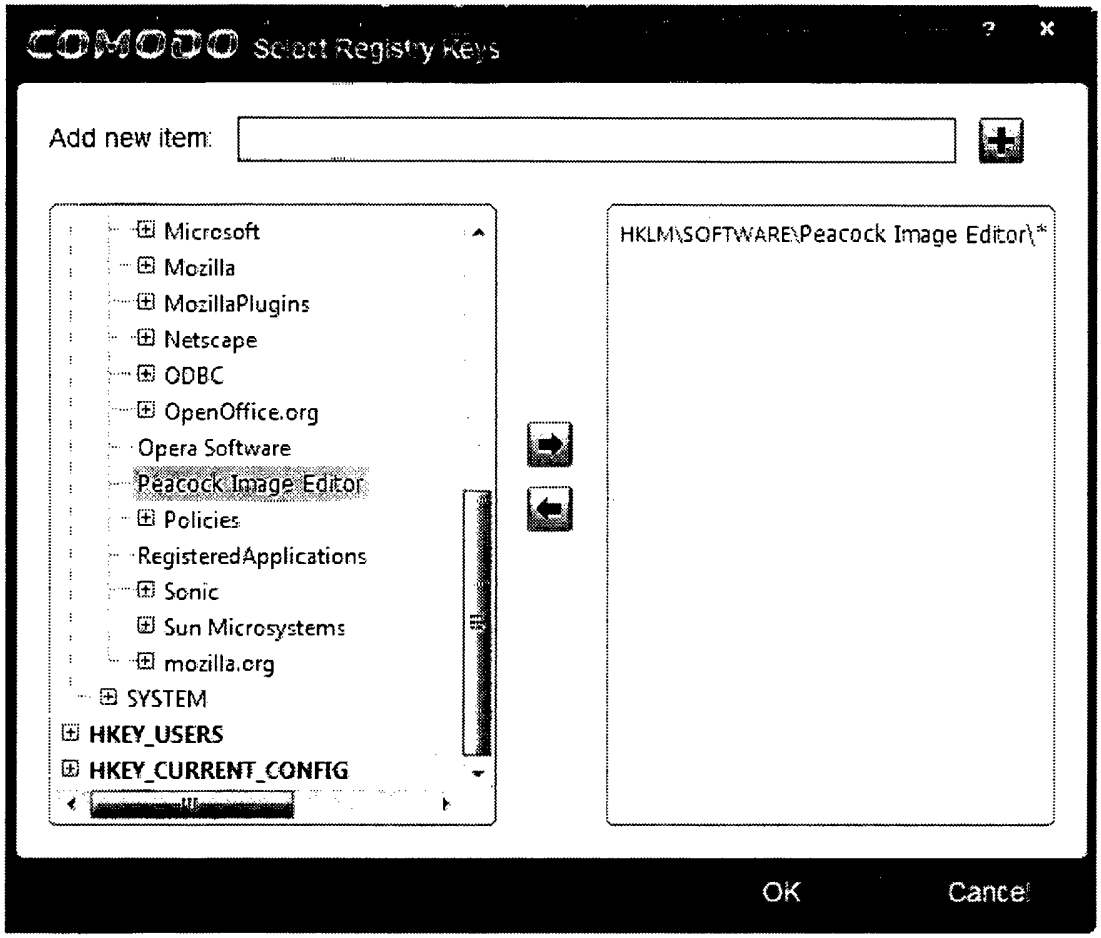
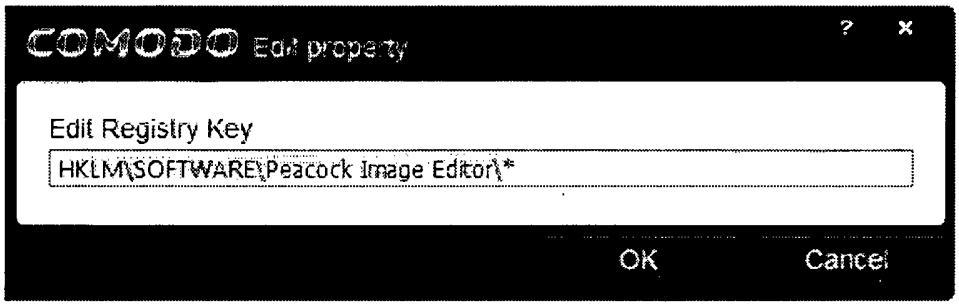


You can add items by browsing the registry tree in the right hand pane, selecting the key and moving it to right hand side pane by clicking the right arrow button. To add item manually enter its name in the 'Add new item' field and press the '+' button.

To edit an item in the Registry Protection list

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



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

Note: The Registry Groups cannot be edited from this interface. You can edit Registry Groups from the Manage Registry Groups interface. Refer to the section **Registry Groups** for more details.

To delete an item from Registry Protection list

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

The selected item will be deleted from the Registry Protection list. CIS will not generate alerts, if the key or the group is modified by other programs.

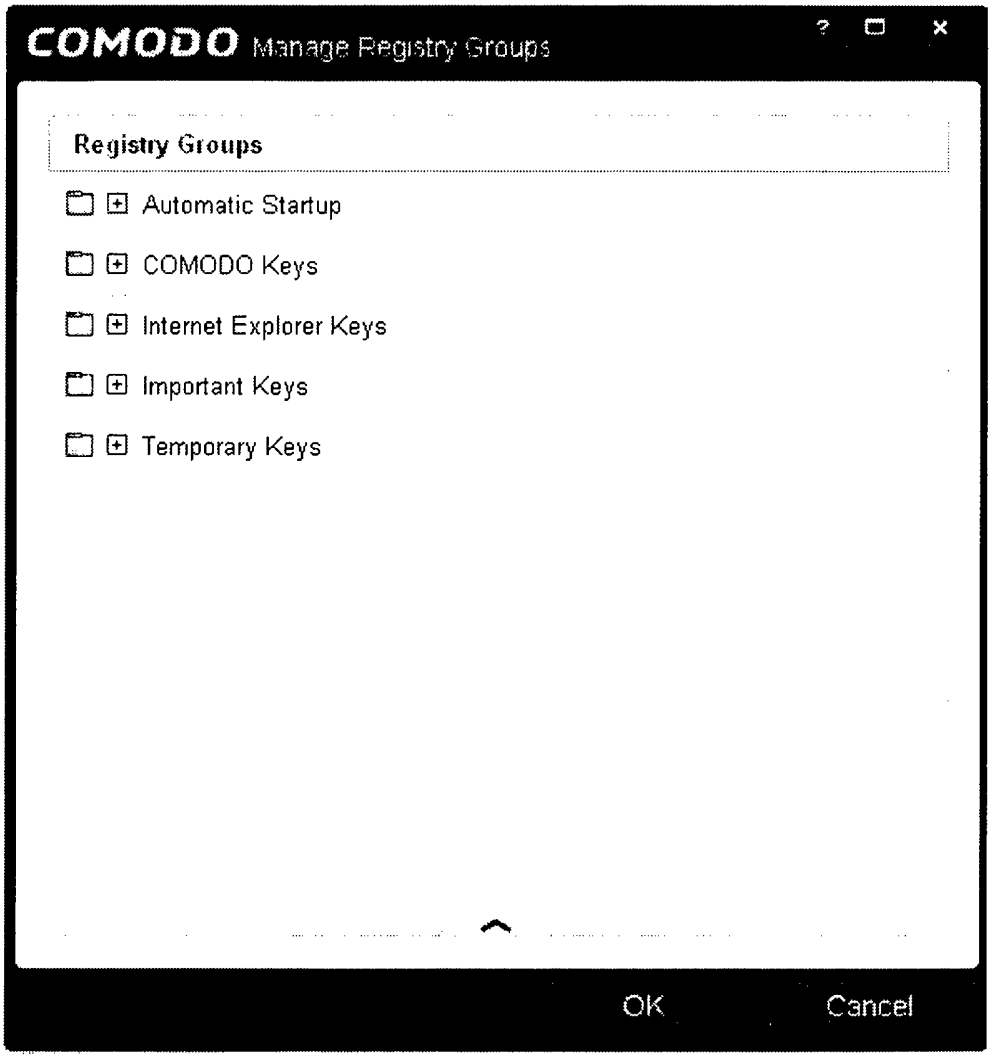
Registry Groups

Registry groups are predefined batches of one or more registry keys. Creating a registry group allows you to quickly add it to Registry Protection list.

To open the Manage Registry Groups interface

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

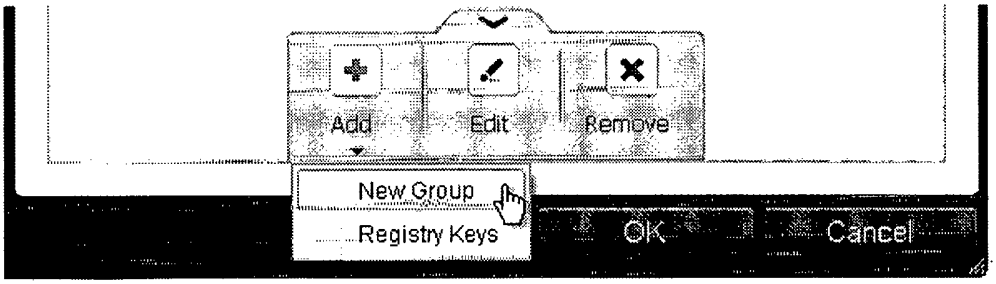
The 'Manage Registry Groups' interface will open.



This interface allows you to

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

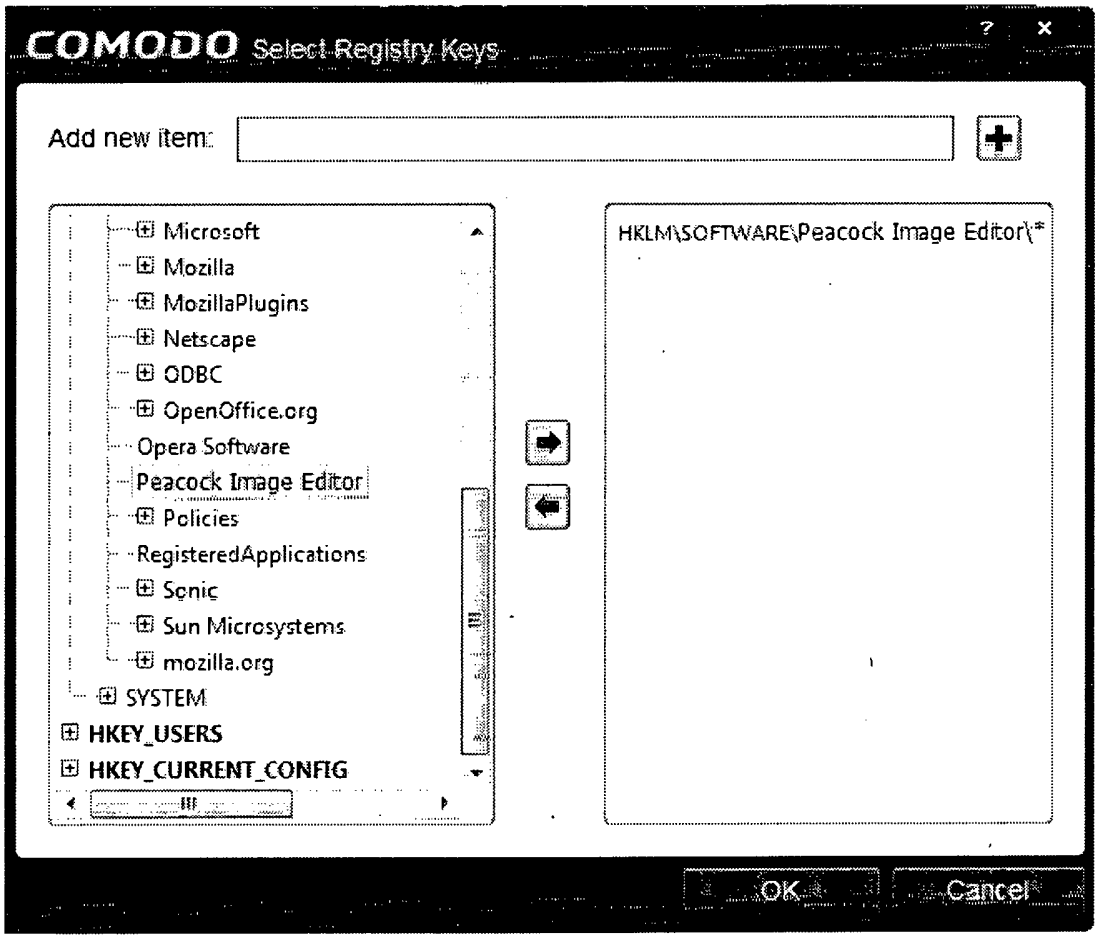
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK



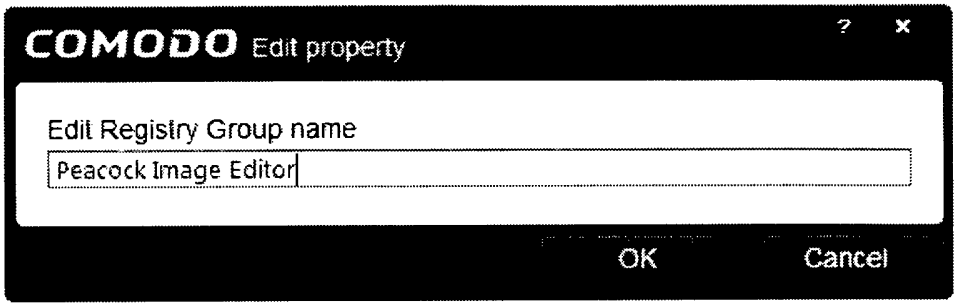
- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



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

item' field and press the '+' button.

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog



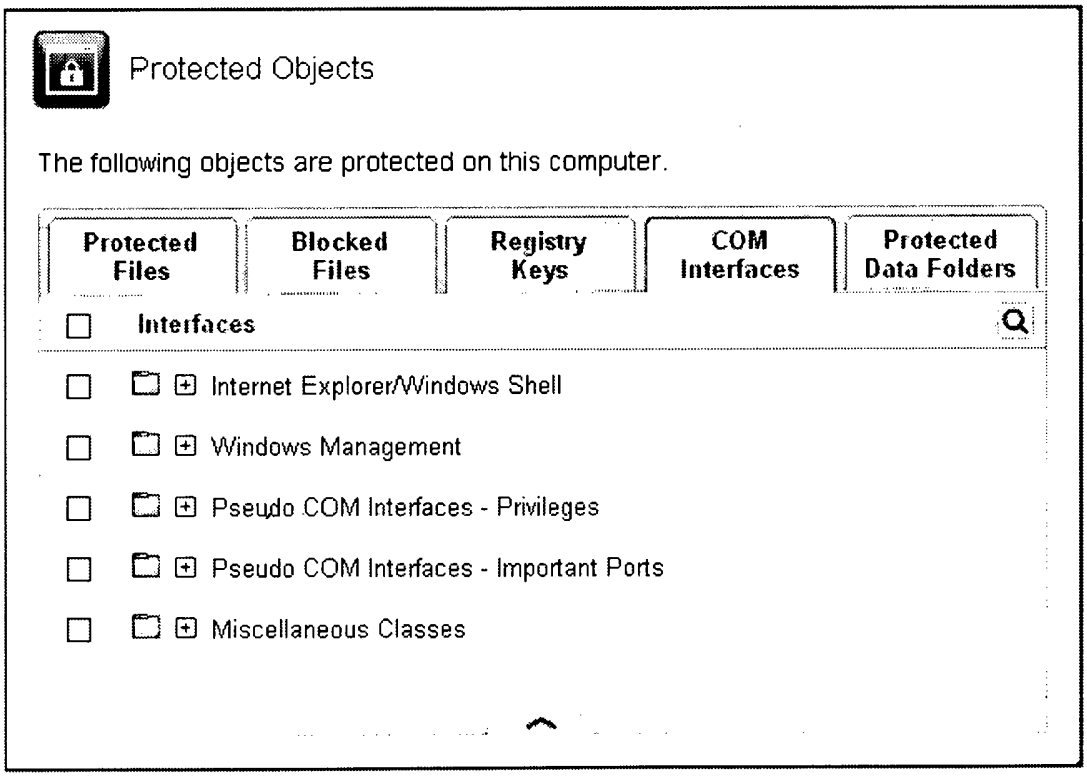
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.4.4. Protected COM interfaces

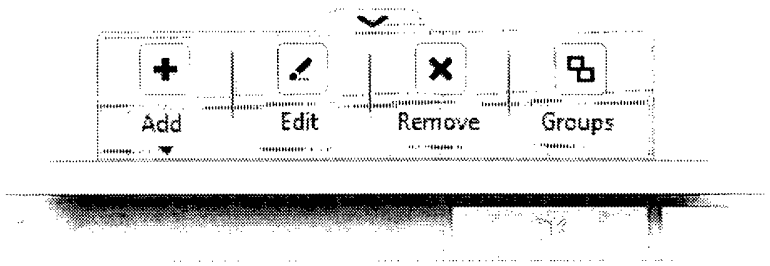
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on your computer. It is a critical part of any security system to restrict processes from accessing the Component Object Model - in other words, to protect the COM interfaces.

Comodo Internet Security automatically protects COM interfaces against against modification, corruption and manipulation by malicious processes. The predefined **COM Interface groups** can be accessed by clicking the 'Groups...' button.

The 'COM Interface' allows you to view the list of predefined **COM Interface groups** protected by CIS, edit them and to add new COM interface components to the list. This interface can be accessed by clicking the 'COM Interfaces' tab in the Protected Objects interface.

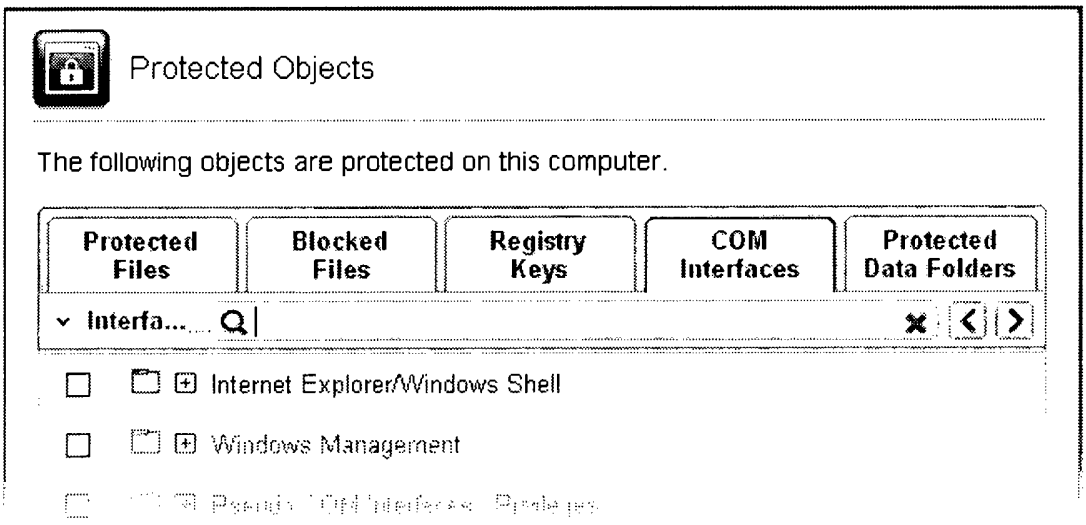


Clicking the handle at the bottom of the interface opens an options panel with the following options:



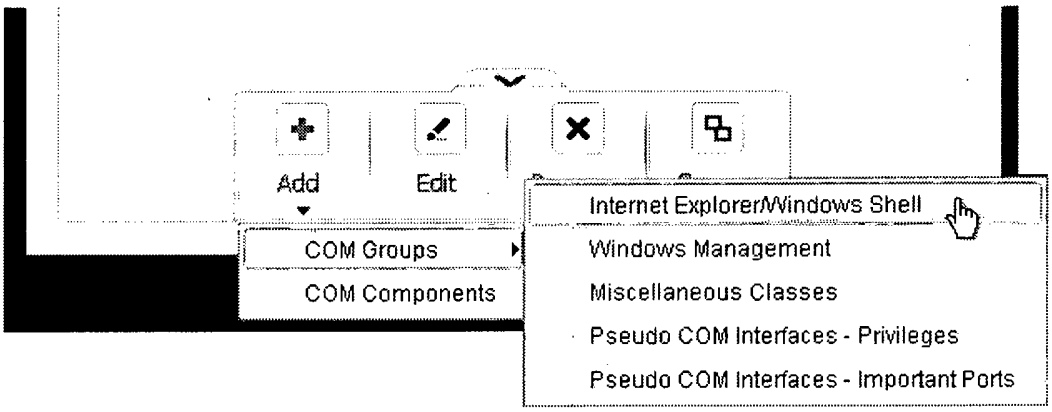
- **Add** - Allows you to add COM groups or individual COM components to COM Protection list.
- **Edit** - Allows you to edit the COM Class.
- **Remove** - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.
- **Groups** - Opens the Manage COM Groups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

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.



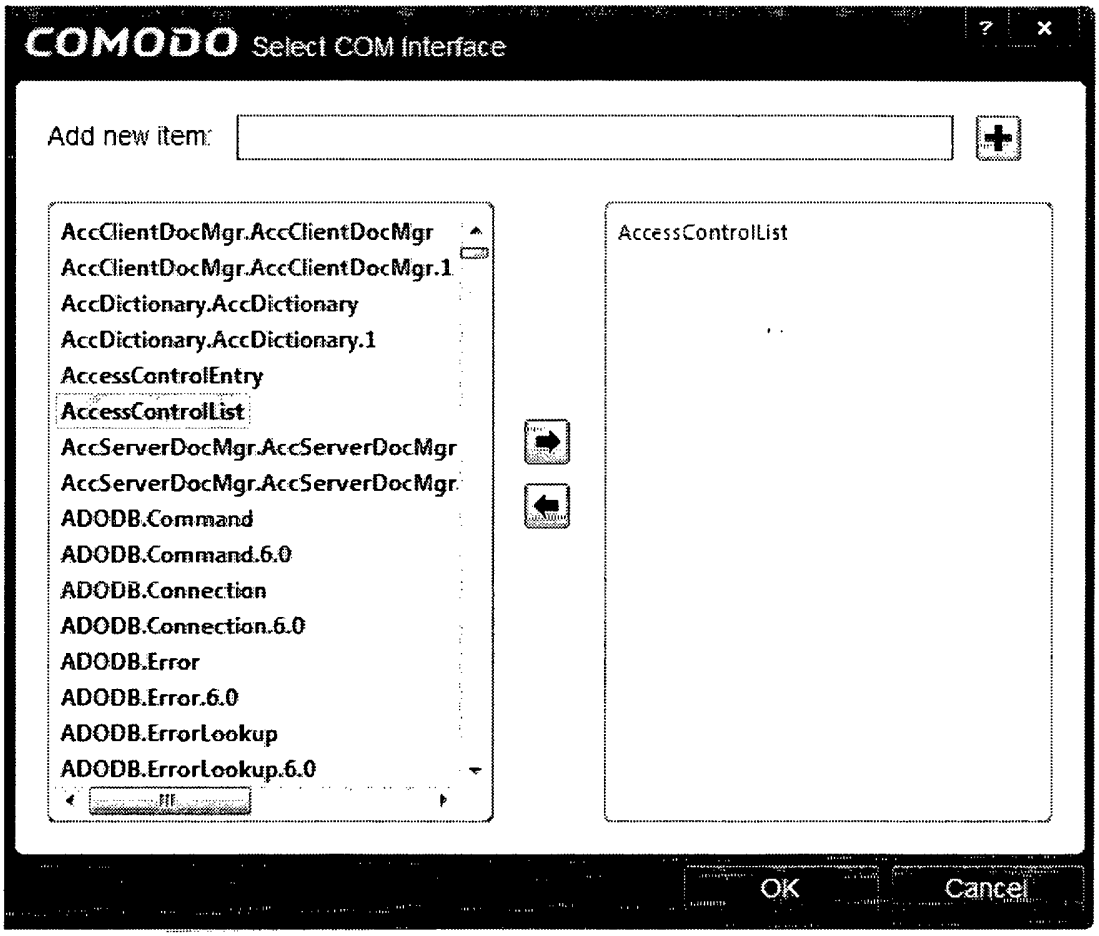
To manually add a COM Group or individual COM component

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



You can add the items by following methods:

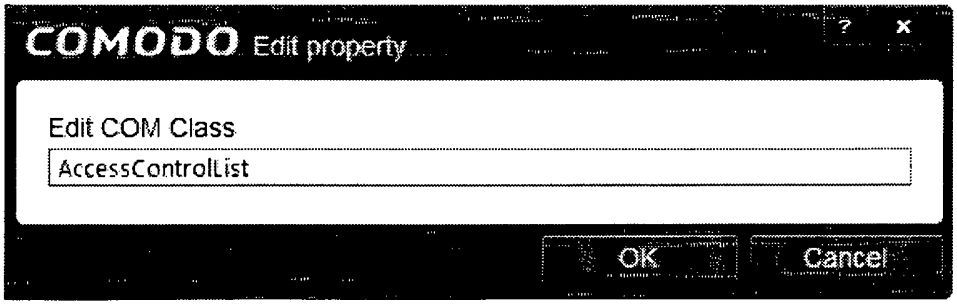
- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section **COM Groups**.
- **Adding COM Components** - Selecting 'COM components' opens the 'Select COM Interfaces' dialog.



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

To edit an item in the COM Protection

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



- Edit the COM Class and click OK

Note: The COM Groups cannot be edited from this interface. You can edit COM Groups from the Manage COM Groups interface. Refer to the section **COM Groups** for more details.

To delete an item from COM Protection list

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

The selected item will be deleted from the COM Protection list. CIS will not generate alerts, if the COM component or the group is modified by other programs or processes.

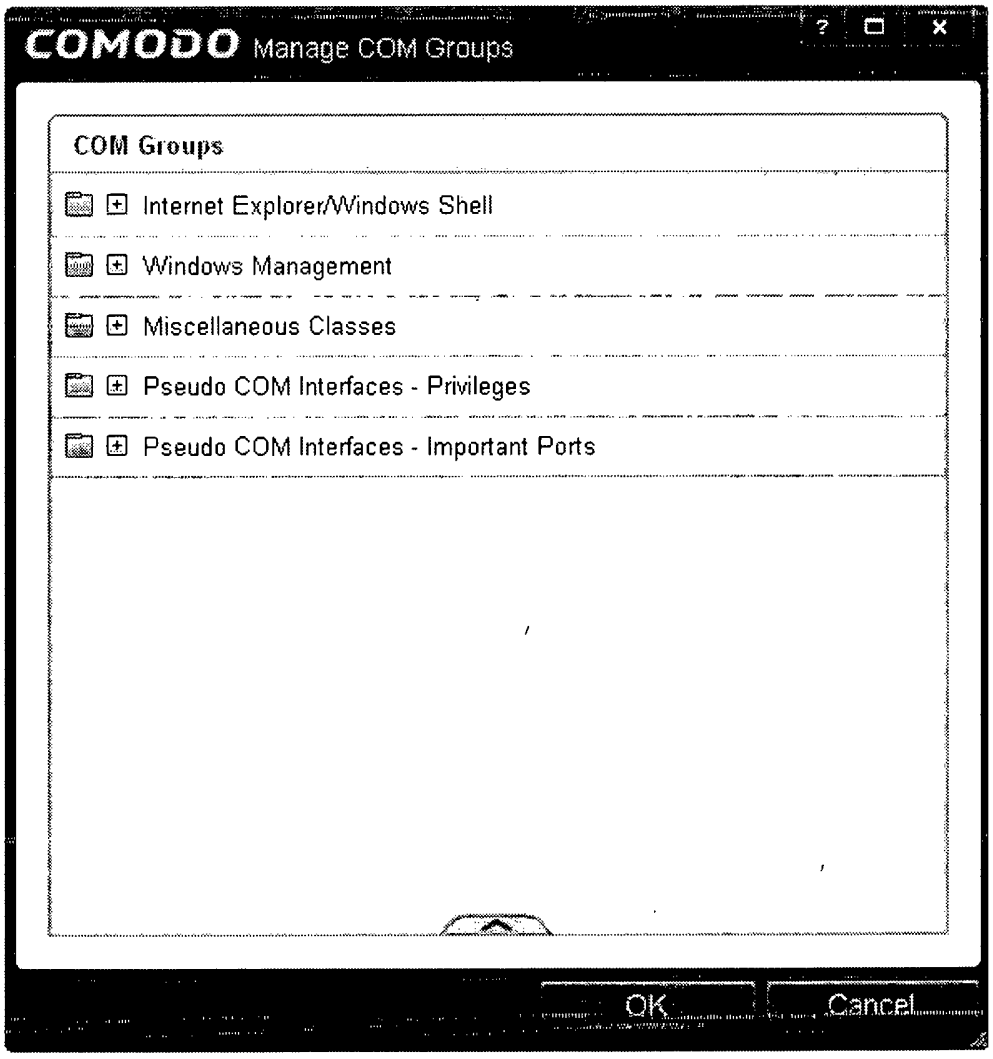
COM Groups

COM groups are handy, predefined groupings of COM interfaces. Creating a COM group allows you to quickly add it to COM Protection list.

To open the Manage COM Groups interface

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

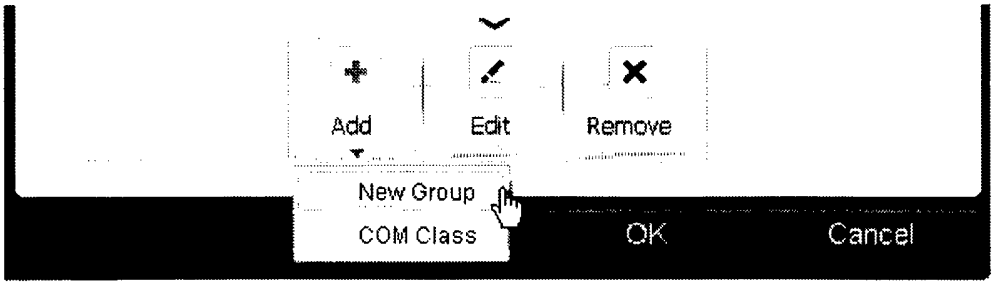
The 'Manage COM Groups' interface will open.



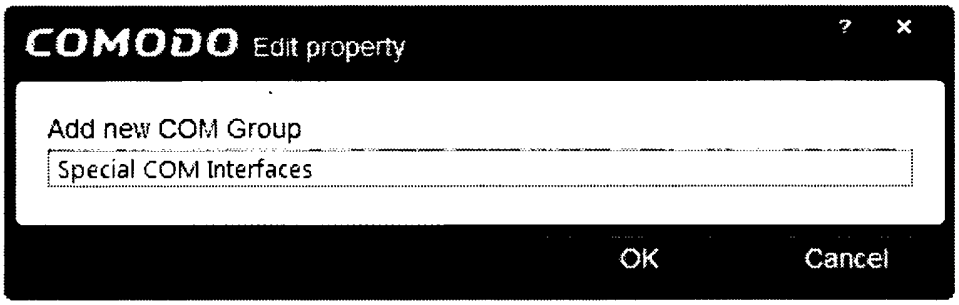
This interface allows you to:

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

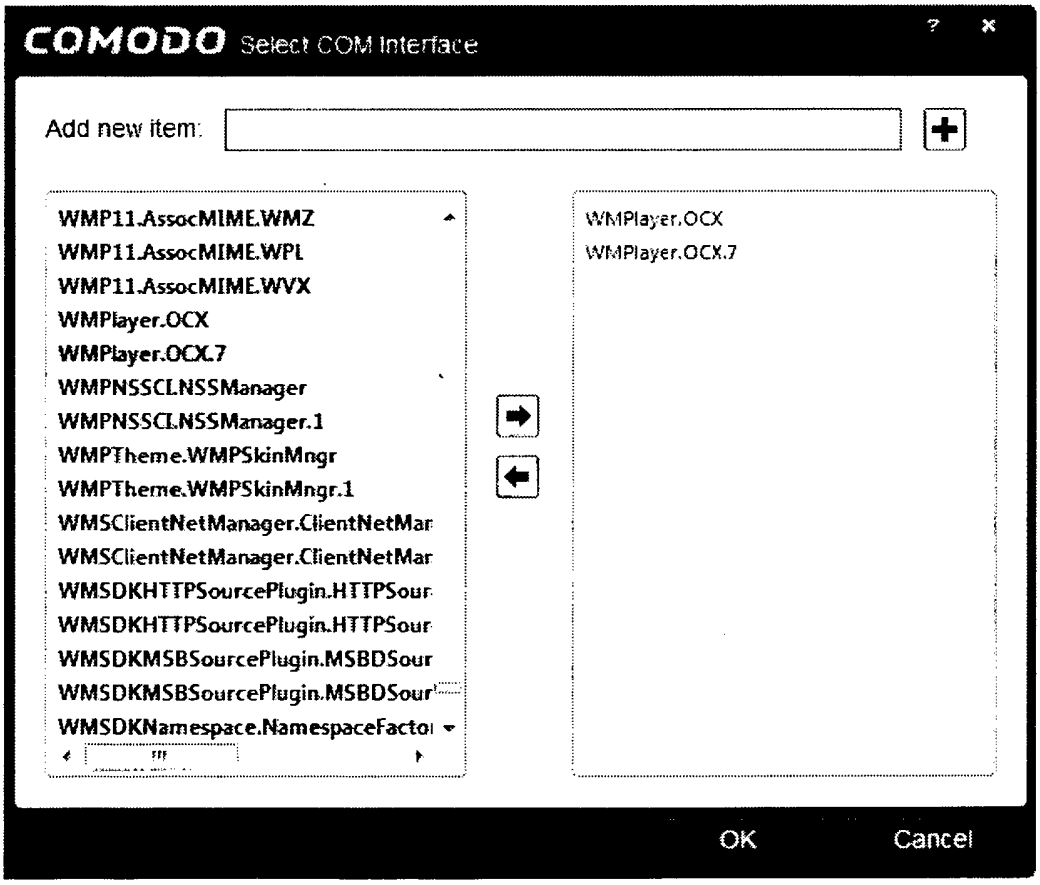
- To add a new group or add new COM Component(s) to an existing group, click the handle from the bottom and click 'Add'.



- **Add a new group** - Select 'New Group' from the 'Add' drop-down, enter a name for the group in the 'Edit property' dialog and click OK.



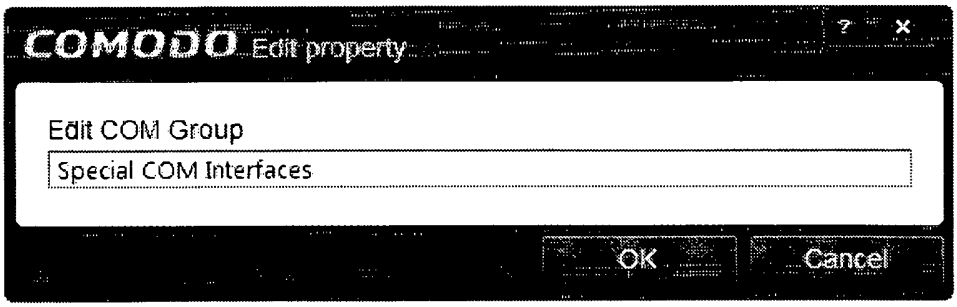
- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class. The 'Select COM Interface' dialog will be opened.



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

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit

Property dialog



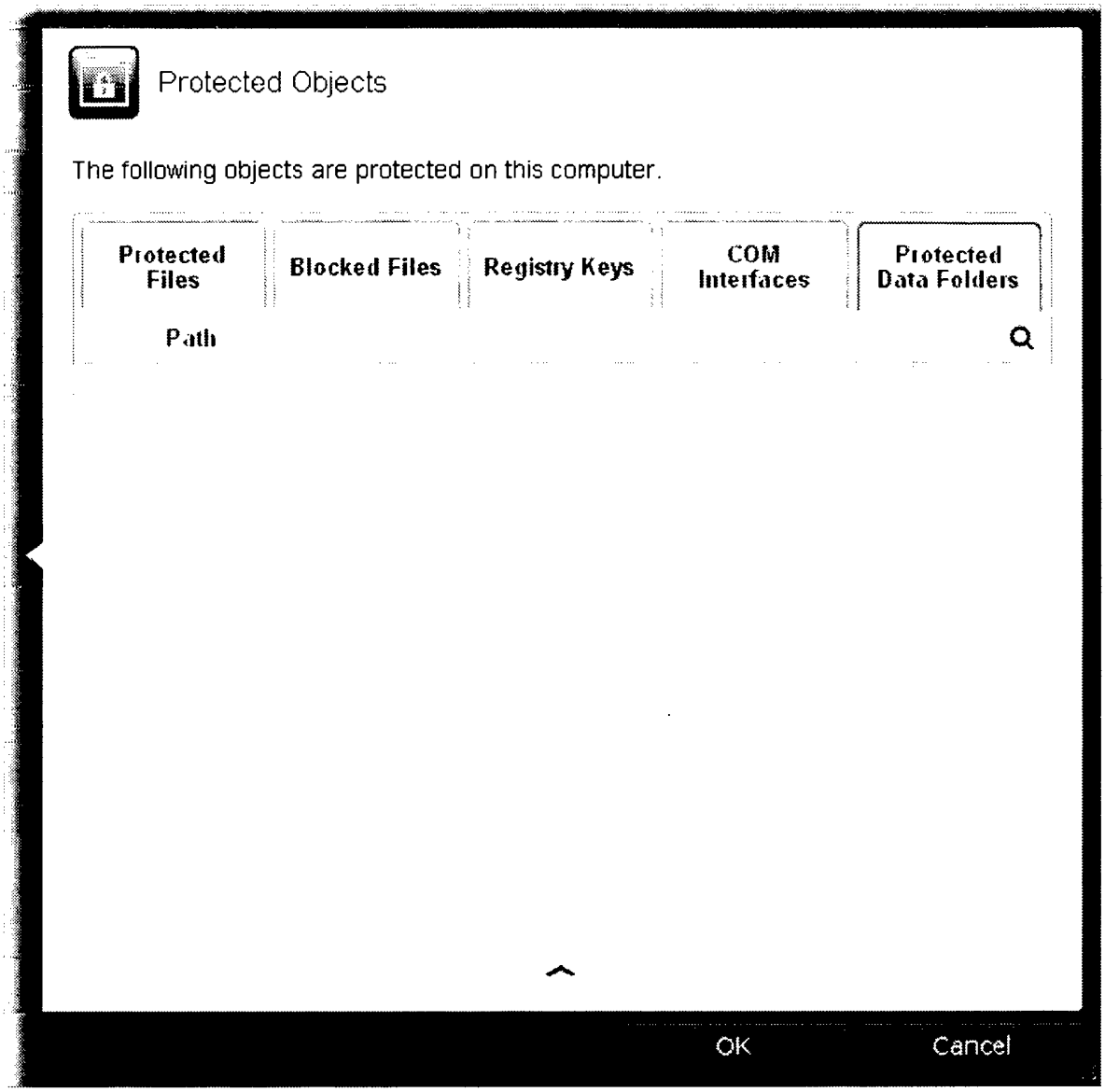
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual COM Component from a group, click + at the left of the group to expand the group, select the item to be removed, click the handle and choose 'Remove'.

6.2.2.4.5. Protected Data Folders

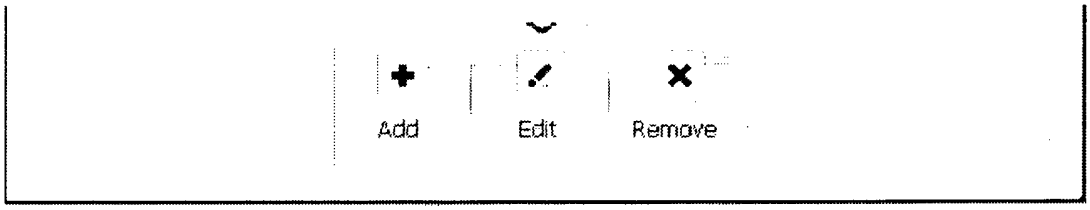
The data files in the folders listed under the Protected Data Folders area cannot be seen, accessed or modified by any known or unknown application that is running inside the sandbox.

Tip: Files and folders that are added to **'Protected Files'** interface are allowed read access by other programs but cannot be modified, whereas the files/folders in 'Protected Data folders' are totally hidden to sandboxed programs. If you want a file to be read by other programs but protected from modifications, then add it to 'Protected Files' list. If you want to totally conceal a data file from all the sandboxed programs but allow read/write access by other known/trusted programs, then add it to Protected Data Folders.

To open the Protected Data Folders interface, Click the 'Protected Data Folders' tab in the Protected Objects interface:



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



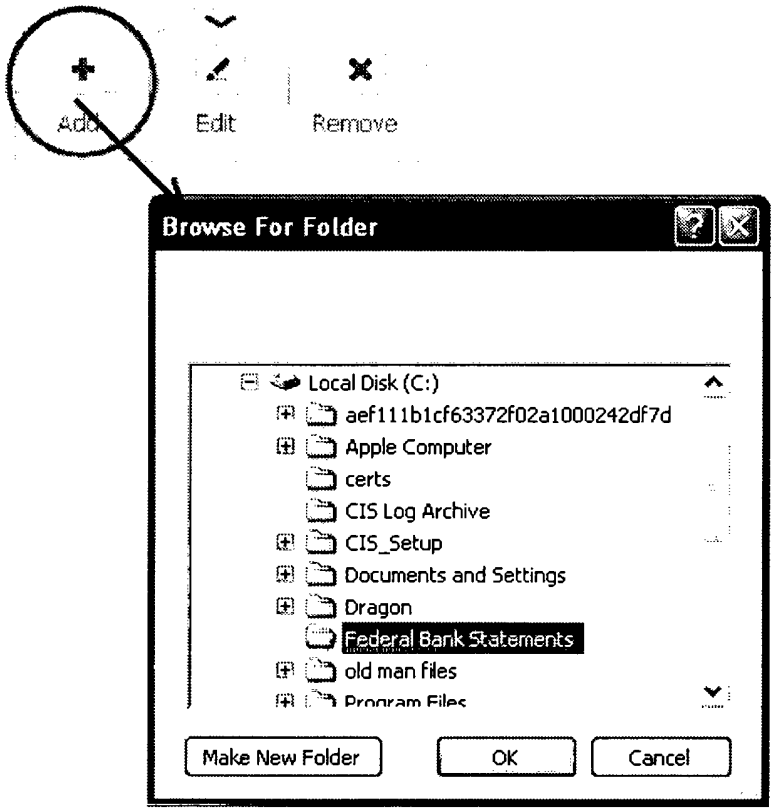
- **Add** - Allows you to add folders to Protected Data Folders list.
- **Edit** - Allows you to edit the path of the added folders.
- **Remove** - Deletes the currently selected folder.

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

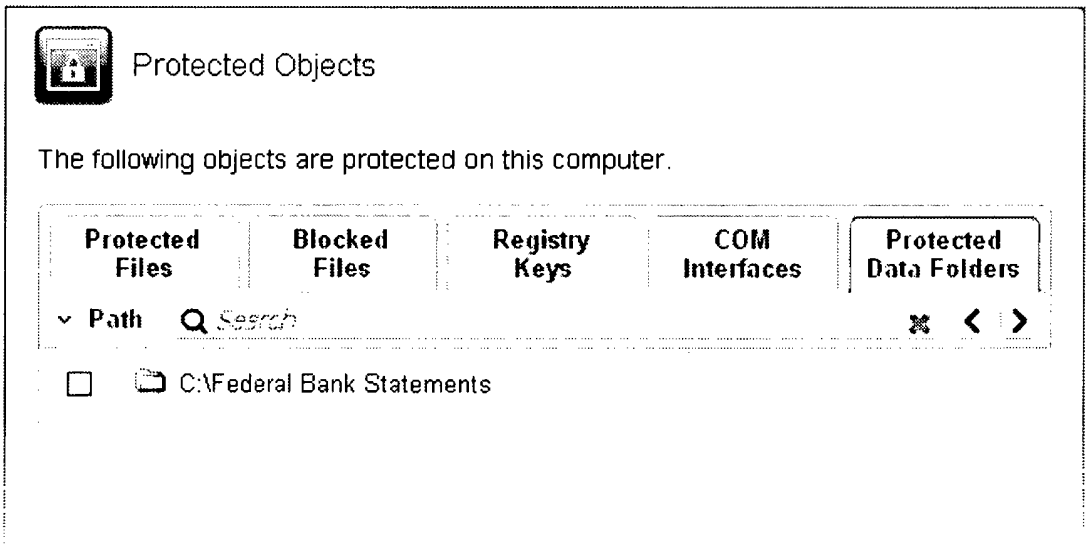


To add a folder to be protected

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



- Navigate to the folder to be added and click OK.



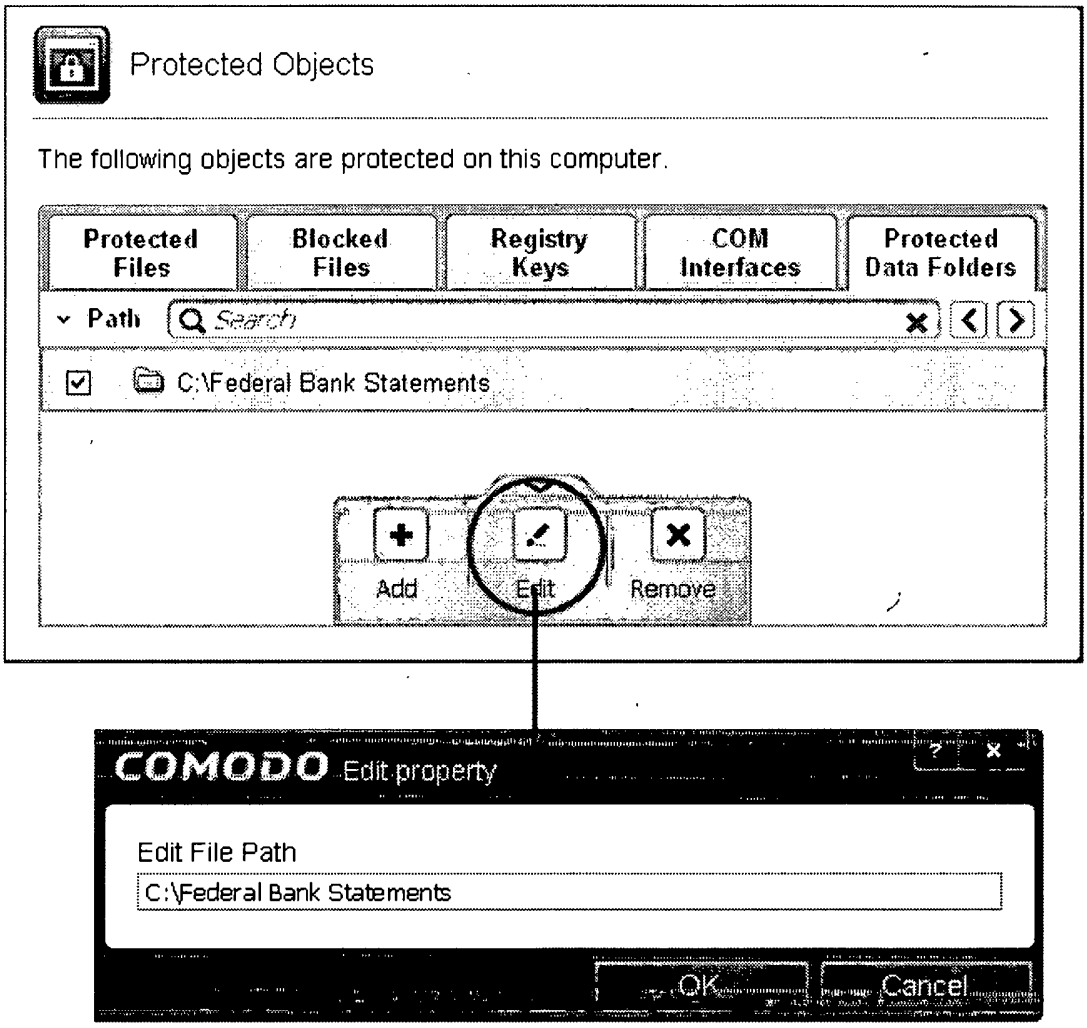
- Click OK to confirm your choice.

Best Available Copy

To edit the path of a protected folder

- Select the folder to be edited
- Click the handle from the bottom center and choose 'Edit'.

The Edit Property dialog will appear.



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

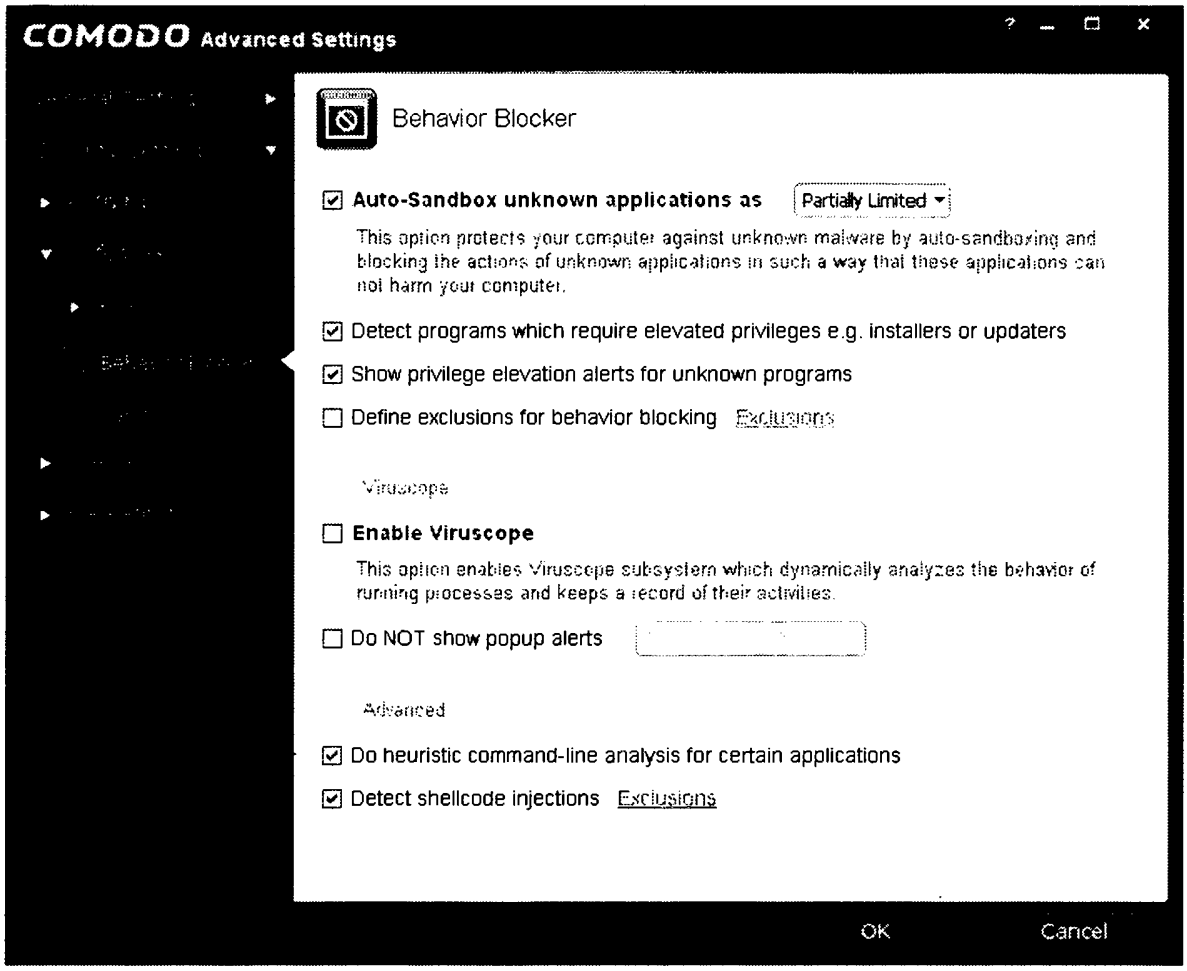
To remove an item from Protected Data Folders list

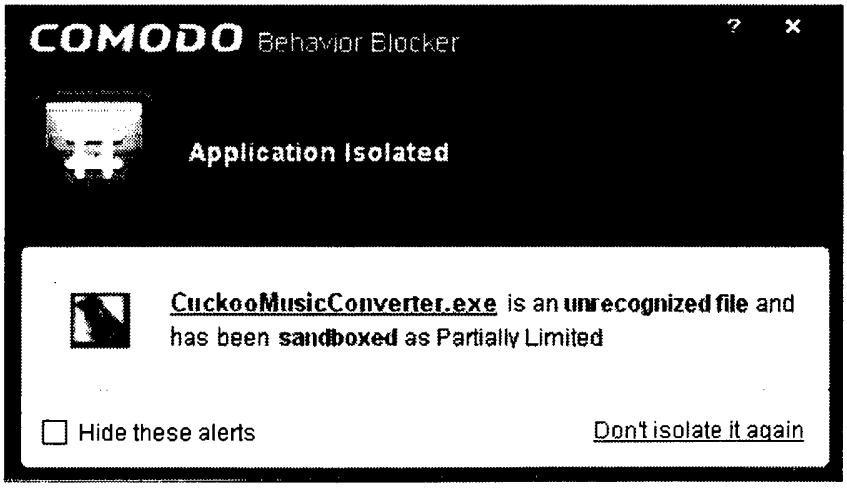
- Select the folder from the list, click the handle from the bottom and choose 'Remove'.
- The selected folder will be removed from the protected folders list. CIS will not generate alerts, if the folder is subjected to unauthorized access.

6.2.2.5. Behavior Blocker

The Behavior Blocker is an integral part of the Defense+ engine and is responsible for authenticating every executable image that is loaded into the memory. The Behavior Blocker intercepts all files before they are loaded and intercepts any prefetching/caching attempts. It calculates the hash of the executable at the point it attempts to load then compares this hash with the list of known / recognized applications that are on the Comodo safe list. If the hash matches the one on record for the executable, then the application is safe and the Behavior Blocker allows it to run. If no matching hash is found, then the executable is 'unrecognized' and is run inside the auto-sandbox. You will be notified via an alert when this happens.

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

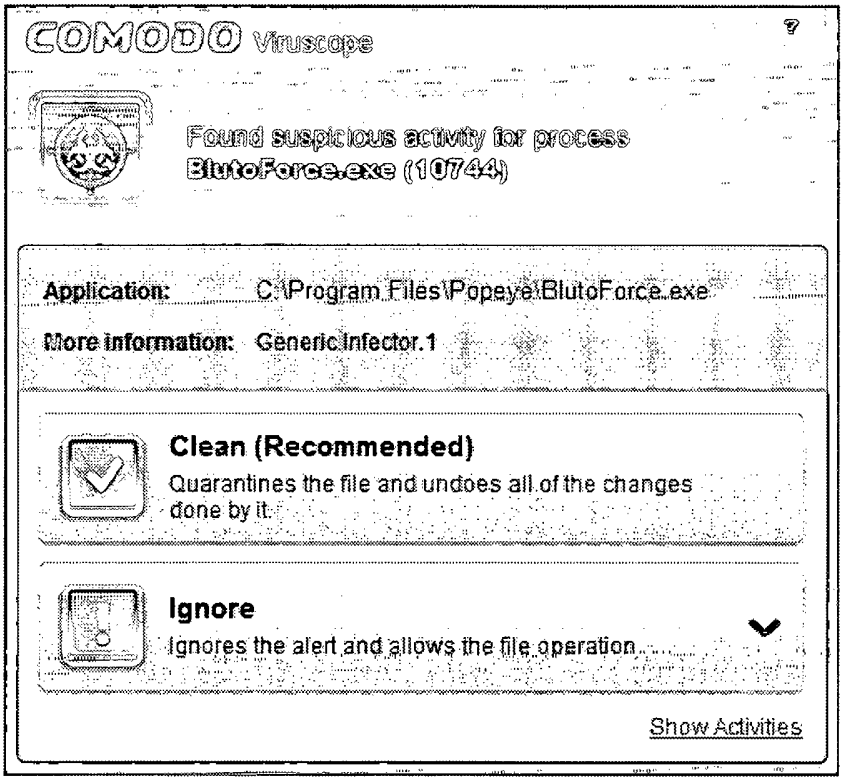




Viruscope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the Behavior Blocker by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide you with more granular control over otherwise legitimate software which requires certain actions to be implemented in order to

run correctly.

Viruscope alerts give you the opportunity to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer.



Note: The Behavior Blocker configuration setting can also be set in the 'Advanced View' of the 'Home' screen beside the Auto-Sandbox status link in the 'Defense+ and Sandbox' pane.

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

Note: The 'auto-sandbox' referred to here is distinct from the Virtual Desktop discussed in **Sandbox Tasks**. For the most part, the 'auto-sandbox' is a non-virtual environment under which unrecognized applications are allowed to run under a set of strict access restrictions (default='Partially Limited'). These restrictions prevent the application from taking actions that are damaging to your system. Users can, however, enable 'Full Virtualization' of auto-sandboxed files in the Behavior Blocker settings.

Configuring Access Restriction

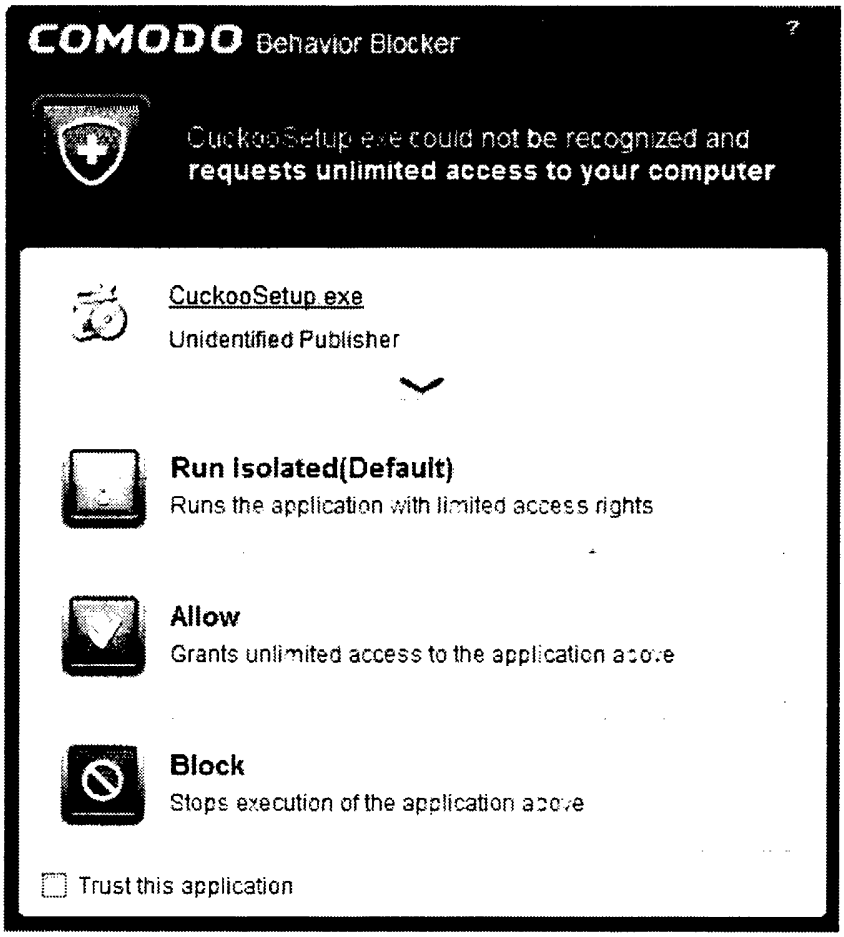
The Behavior Blocker will auto-sandbox an unknown executable and restrict its execution privileges according to an access restriction level set by you. Access restriction levels determine what level of rights a sandboxed application has to access other software and hardware resources on your computer:

- **Partially Limited** - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(***Default***)
- **Limited** - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
- **Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
- **Untrusted** - The application is not allowed to access any operating system resources. The application is not

allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.

- **Blocked** - The application is not allowed to run at all.
- **Fully Virtualized** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.

- **Detect programs which require elevated privileges**: Allows you to instruct the Behavior Blocker to display alerts when an installer or updater requires administrator or elevated privileges to run. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of your computer such as the registry. Refer to the section **Understanding Security Alerts** for more details.



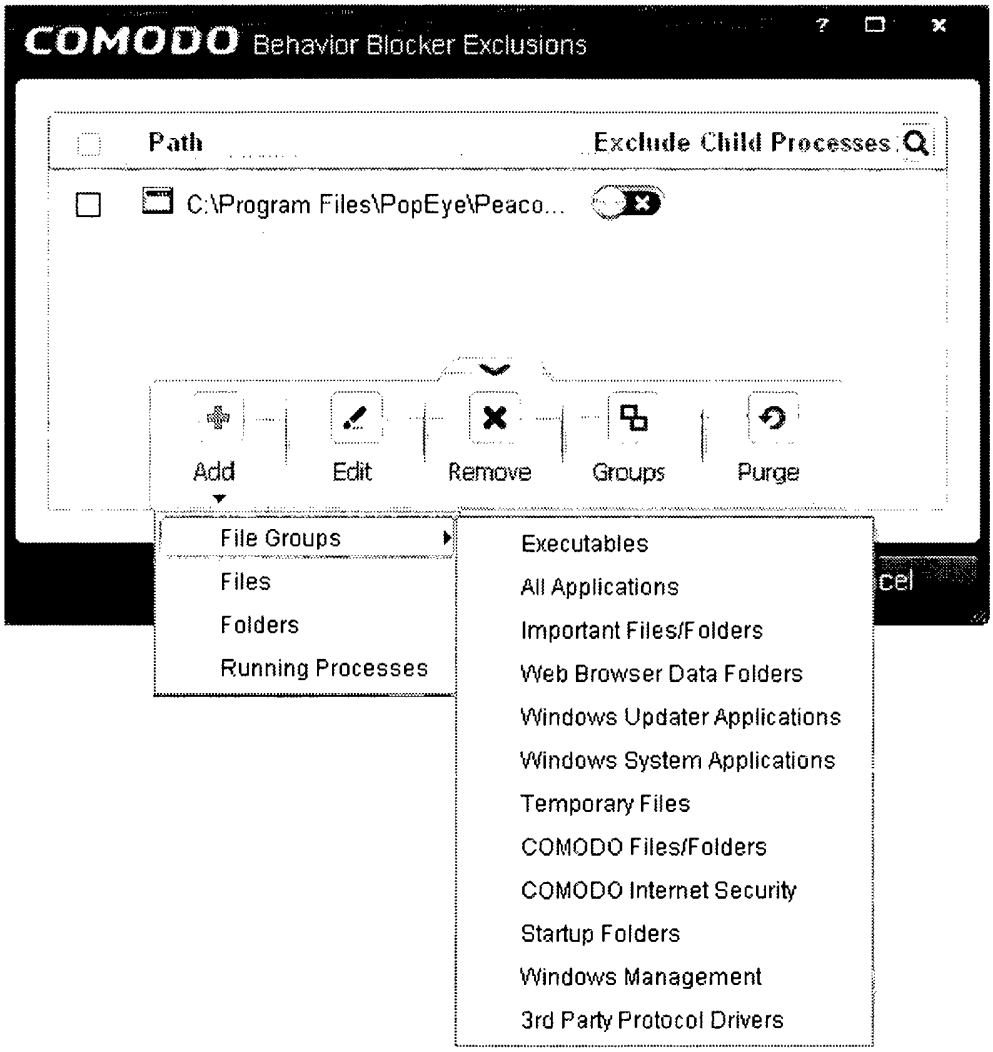
You can decide on whether or not to allow the installer or update based on your assessment, from the alert itself. (***Default=Enabled***)

- **Show privilege elevation alerts for unknown programs** : Allows you to instruct the Behavior Blocker 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***)
- **Define exclusions for behavior blocking** - Allows you to add file paths which are to be excluded from monitoring by the Behavior Blocker. The executables included in the exclusions area are allowed to run without authenticity checking. ***(Default = Disabled)***

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

To define exclusions:

- Select the 'Define exceptions for behavior blocking' checkbox and click the Exclusions link. The 'Manage Exceptions' dialog will appear.



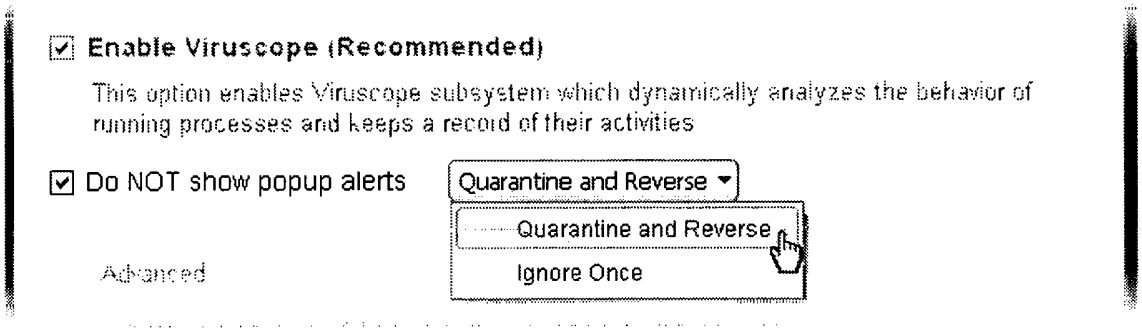
- Click the handle at the bottom of the interface and choose 'Add'
- You can add items by selecting the required option from the drop-down:
  - **File Groups** - Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. For more details on file groups, refer to the section **File Groups**.
  - **Running Processes** - As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.
  - **Browse Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
  - **Browse File** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.
- After adding an item, choose whether or not the child processes of the files/applications also need to be excluded from Behavior Blocking using the toggle switch under the 'Exclude Child Process' column.
- Click 'OK' to implement your settings.

Viruscope Settings

Viruscope monitors the activities of all processes, regardless of whether they are running normally or inside the sandbox. If suspicious activity is detected, Viruscope will generate a pop-up alert that allows you to block or allow the activity.

- **Enable Viruscope (Recommended)** - Allows you to enable or disable Viruscope. If enabled, the Viruscope monitors the activities of all the running processes and generates alerts on suspicious activities. (***Default = 'Disabled'***)

- **Do NOT show popup alerts** - Allows you to configure whether or not to show Viruscope alerts when a suspicious activity is recognized. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Quarantine and Reverse' or 'Ignore'. (***Default = Disabled***)



  - **Quarantine and Reverse** - Moves the process and its parent application to quarantine and reverses the action that was taken by the process. (***Default***)
  - **Ignore Once** - The action will be allowed for one time. If the same activity is recognized again, an alert will be generated.

Advanced Settings:

- **Do heuristic command-line analysis for certain applications** - Selecting this option instructs Comodo Internet Security to perform heuristic analysis of programs that are capable of executing code such as visual basic scripts and java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscipt.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CIS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the Internet, for example, the alert will state 'test.vbs' is attempting to connect to the Internet ***(Default = Enabled).***

  If this option is disabled, the alert would only state 'wscript.exe' is trying to connect to the Internet'.

Background note: 'Heuristics' describes the method of analyzing a file to ascertain whether it contains codes typical of a virus. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that matches a signature on the virus blacklist. This helps to identify previously unknown (new) viruses.

- **Detect shellcode injections (i.e. Buffer overflow protection)** - Enabling this setting turns-on the Buffer over flow protection.

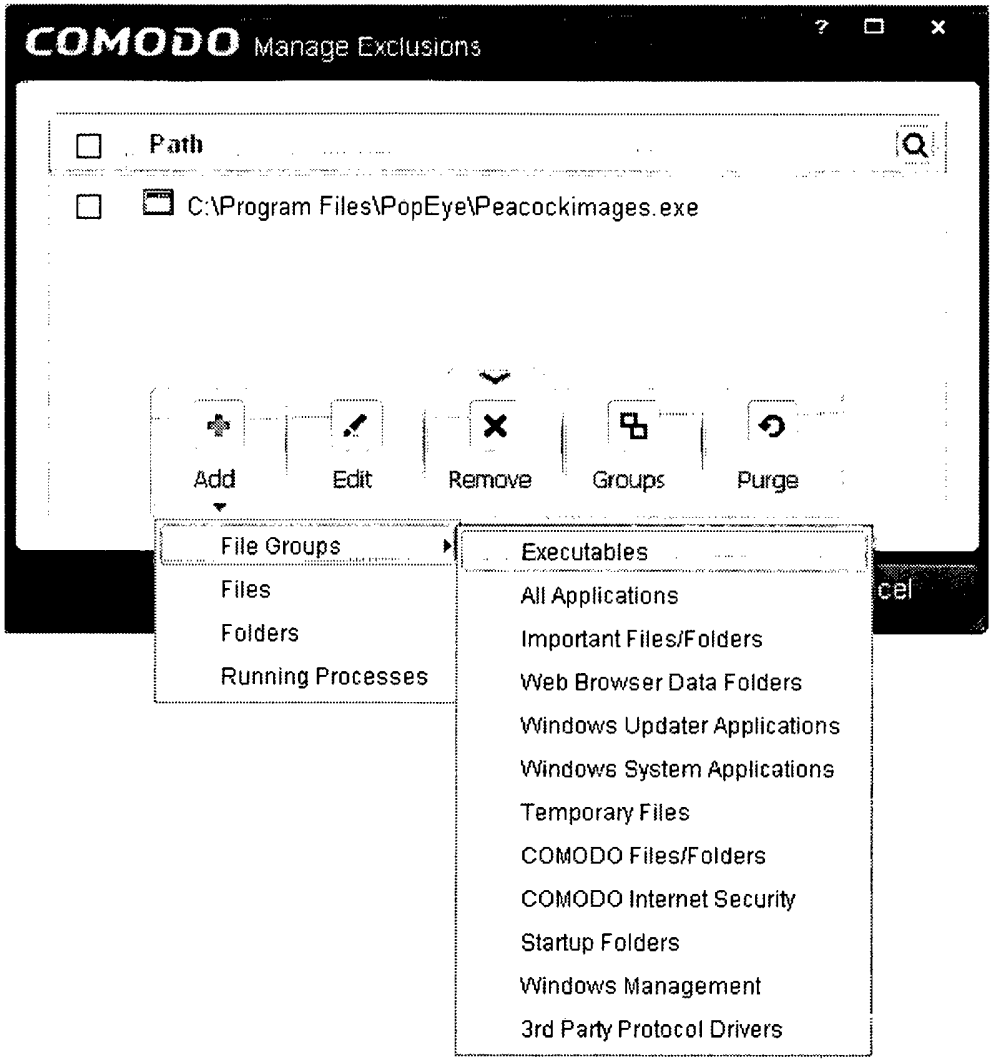
  Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

  Turning-on buffer overflow protection instructs the Comodo Internet Security to raise pop-up alerts in every event of a possible buffer overflow attack. You can allow or deny the requested activity raised by the process under execution depending on the reliability of the software and its vendor. **Click here** for more details on the alerts.

  Comodo recommends that this setting to be maintained selected always ***(Default = Enabled).***

  To exclude some of the file types from being monitored under Detect Shellcode injections.

  - Select the 'Detect shellcode injections' checkbox and click the Exclusions link. The 'Manage Exclusions' dialog will appear.



- Click the handle from the bottom of the interface and choose 'Add'
- You can add items by selecting the required option from the drop-down:
  - **File Groups** - Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. For more details on file groups, refer to the section **File Groups**.
  - **Running Processes** - As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.
  - **Browse Folders** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
  - **Browse File** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.

Note: These settings are recommended for advanced users only.

- Click 'OK' to implement your settings.

6.2.2.5.1. The Sandbox - An Overview

Comodo Internet Security's new sandbox is an isolated operating environment for unknown and untrusted applications. Running

an application in the sandbox means that it cannot make permanent changes to other processes, programs or data on your 'real' system. Comodo have integrated sand-boxing technology directly into the security architecture of Comodo Internet Security to complement and strengthen the Firewall, Defense+ and Antivirus modules.

Applications in the sandbox are executed under a carefully selected set of privileges and write to a virtual file system and registry instead of the real system. This delivers the smoothest user experience possible by allowing unknown applications to run and operate as they normally would while denying them the potential to cause lasting damage.

After an unknown application has been placed in the sandbox, CIS also automatically queues it for submission to Comodo Cloud Scanners for automatic behavior analysis. Firstly, the files undergo another antivirus scan on our servers. If the scan discovers the file to be malicious, then it is designated as malware, the result is sent back to the local installation of CIS and the local black-list is updated. If the scan does not detect that the file is malicious then its behavior will be monitored by running it in a virtual environment within Comodo's Instant Malware Analysis (CIMA) servers and all its activities are recorded. If these behaviors are found to be malicious then the signature of the executable is automatically added to the antivirus black list. If no malicious behavior is recorded then the file is placed into 'Unrecognized Files' (for execution within the sandbox) and will be submitted to our technicians for further checks. The cloud scanning processes take around 15 minutes to complete and report their results back to CIS.

By uniquely deploying 'sandboxing as security', CIS 2013 offers improved security, fewer pop-ups and greater ease of use than ever before.

6.2.2.5.2. Unknown Files: The Auto-Sandboxing and Scanning Processes

- When an executable is first run it passes through the following CIS security inspections:
  - Antivirus scan
  - HIPS Heuristic check
  - Buffer Overflow check
- If the processes above determine that the file is malware then the user is alerted and the file is quarantined or deleted
- An application can become recognized as 'safe' by CIS (and therefore not auto-sandboxed or scanned in the cloud) in the following ways:
  - Because it is on the local Comodo White List of known safe applications
  - Because the user has added the application to the local '**Trusted Files**'
  - By the user granting the installer elevated privileges (CIS detects if an executable requires administrative privileges. If it does, it **asks the user**. If they choose to trust, CIS regards the installer and all files generated by the installer as safe)
  - Additionally, a file is not auto-sandboxed or sent for analysis in the cloud if it is defined as an Installer or Updater in HIPS Ruleset (See **Active HIPS Rules** for more details)
  - **Cloud Scanning Part 1**

    Files and processes that pass the security inspections above but are not yet recognized as 'safe' (white-listed) are 'Unrecognized' files. In order to try to establish whether a file is safe or not, CIS will first consult Comodo's File Look-Up Server (FLS) to check the very latest signature databases:
    - A digital hash of the unrecognized process or file is created.
    - These hashes are uploaded to the FLS to check whether the signature of the file is present on the latest databases. This database contains the latest, global black list of the signatures of all known malware and a white list of the signatures of the 'safe' files.
      - First, our servers check these hashes against the latest available black-list
      - If the hash is discovered on this blacklist then it is malware
      - The result is sent back to the local installation of CIS
    - If the hash is not on the latest black-list, it's signature is checked against the latest white-list
      - If the hash is discovered on this white-list then it is trusted
      - The result is sent back to local installation of CIS
      - The local white-list is updated
    - The FLS checks detailed above are near instantaneous.

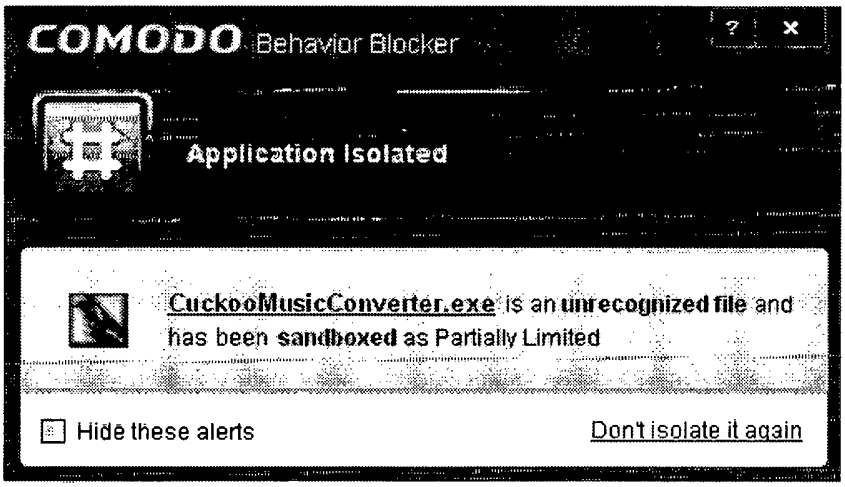
- **Sandbox and Cloud Scanning Part 2**

  If the hash is not on the latest black-list or white-list then it remains as 'unrecognized'. CIS simultaneously takes two distinct but complementary actions -

  (1) It will run the unrecognized file in the auto-sandbox so that it cannot access important operating system files or damage your computer

  (2) It will leverage Comodo's Cloud Scanning technology to determine whether the file behaves in a malicious fashion.

- Unrecognized files and applications will be isolated and run in the auto-sandbox. CIS will alert the user that it is going to run the application in the sandbox.



- By default, auto-sandboxed applications are run with 'Partially Limited' restrictions.

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

  - Partially Limited - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.(Default)
  - Limited - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
  - Restricted - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
  - Untrusted - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
  - Blocked - The application is not allowed to run at all.
  - Fully Virtualized - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.

- Unrecognized files are simultaneously uploaded to Comodo's Instant Malware Analysis servers for further checks:
  - Firstly, the files undergo another antivirus scan on our servers.
  - If the scan discovers the file to be malicious (for example, heuristics discover it is a brand new variant) then it is designated as malware. This result is sent back to the local installation of CIS and the local and global black-list is updated.

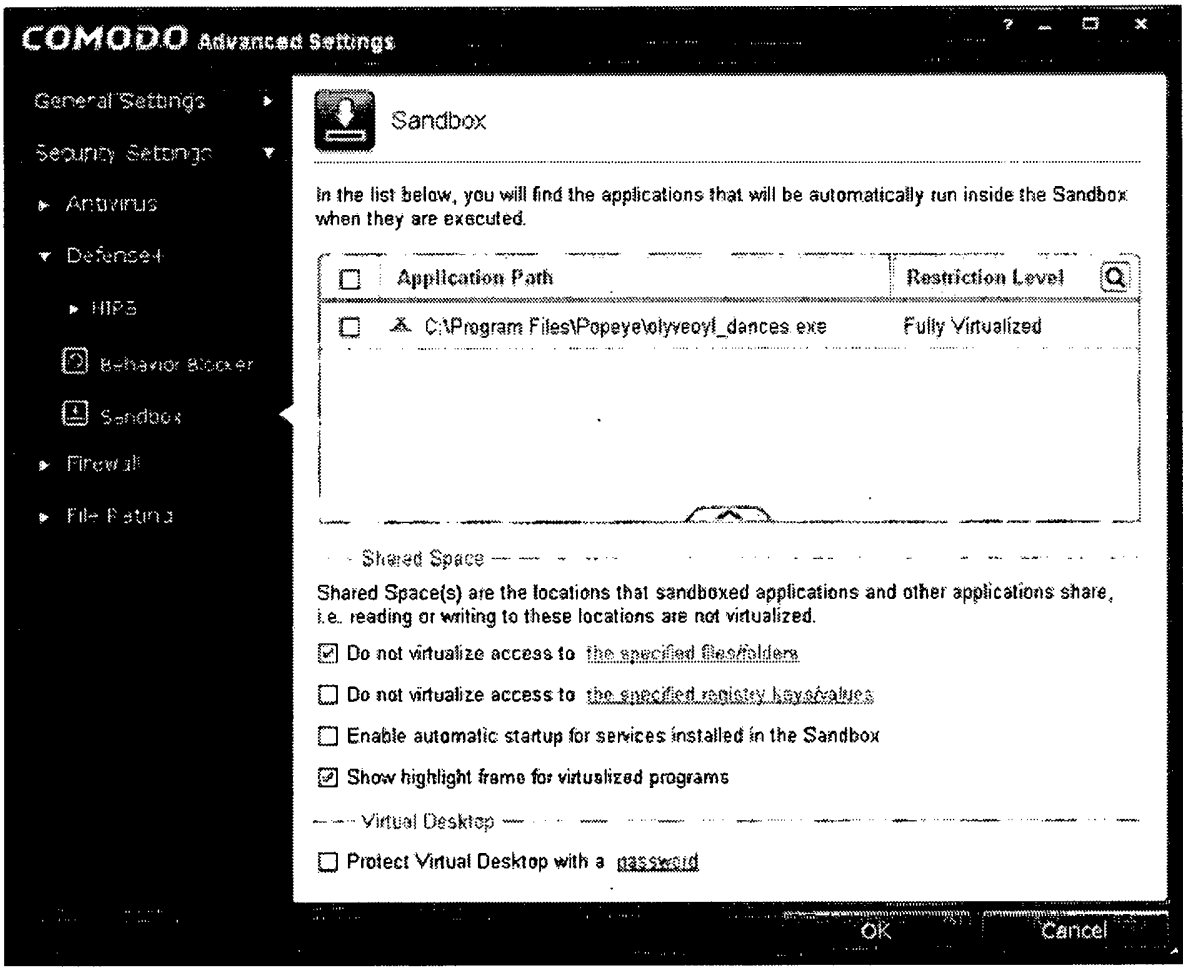
- If the scan does not detect that the file is malicious then it passes onto the the next stage of inspection - behavior monitoring.
- The behavior analysis system is a cloud based service that is used to help determine whether a file exhibits malicious behavior. Once submitted to the system, the unknown executable will be automatically run in a virtual environment and all actions that it takes will be monitored. For example, processes spawned, files and registry key modifications, host state changes and network activity will be recorded.
- If these behaviors are found to be malicious then the signature of the executable is automatically added to the antivirus black list.
- If no malicious behavior is recorded then the file is placed into 'Unrecognized Files' and will be submitted to our technicians for further checks. Note: Behavior Analysis can identify malicious files and add to the global black list, but it cannot declare that a file is 'safe'. The status of 'safe' can only be given to a file after more in-depth checks by our technicians.
- In either case, the result is reported back to your CIS installation in approximately 15 minutes. If the executable was not found to be malicious then it will be run in the auto-sandbox. It will simultaneously be added to the 'Unrecognized Files' list and uploaded to our technicians for analysis. If it is discovered to be a threat then CIS will show an AV alert to the user. From this alert the user can opt to quarantine, clean (delete) or disinfect the malicious file. This new threat will be automatically added to the global black list database and therefore benefit all CIS users.

6.2.2.6. Configure the Sandbox

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

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

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

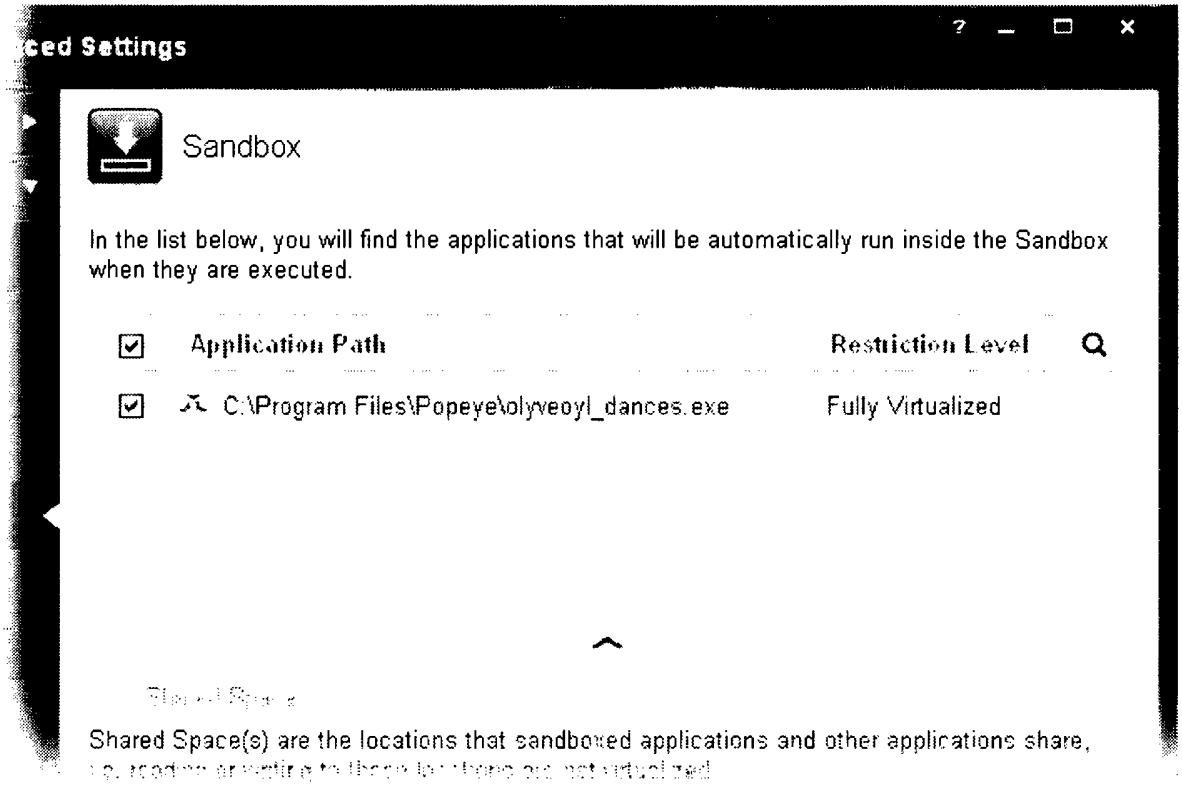


Click the following links to find out more about each section:

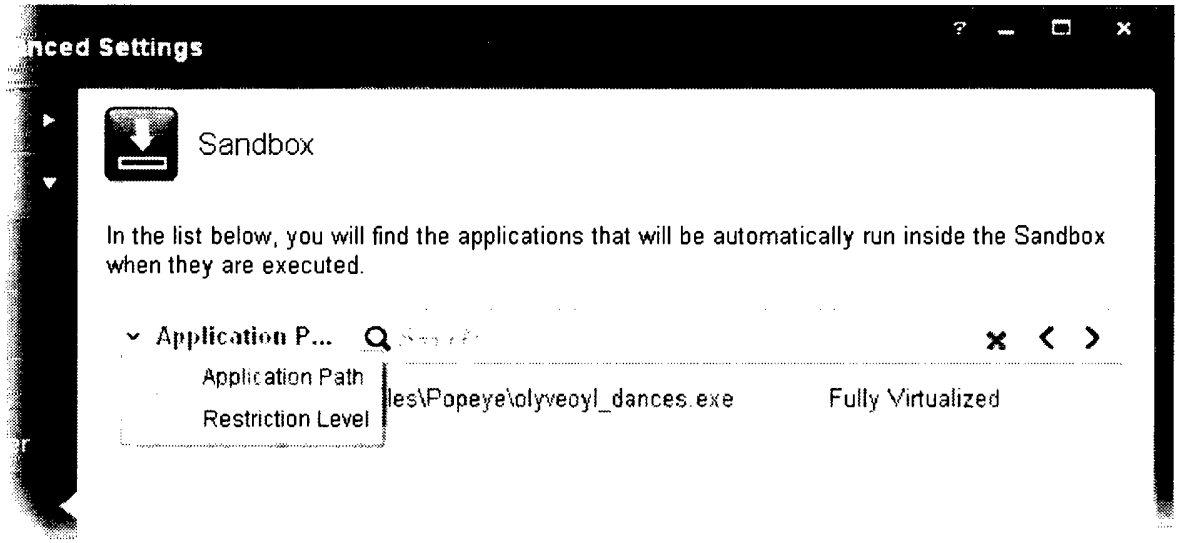
- **Sandboxed Programs** - Add and configure programs that should always run sandboxed
- **Shared Space Settings** - Files downloaded or generated by sandboxed applications that you wish to be able to access from your real system should be downloaded to the shared space
- **Virtual Desktop** - Create an 'exit' password for the Virtual Desktop. If set, the Virtual Desktop cannot be closed or minimized until the correct password is entered. This prevents guests or younger users from exiting this sandbox environment.

Sandboxed Programs

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

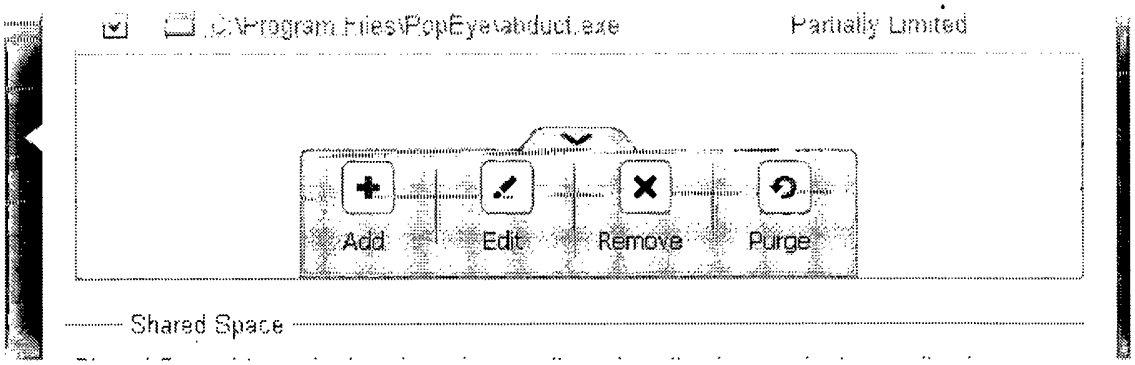


You can search for a application or program from the list by clicking the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter the name of the application in part or full 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 pane opens the sandbox tools panel:



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

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

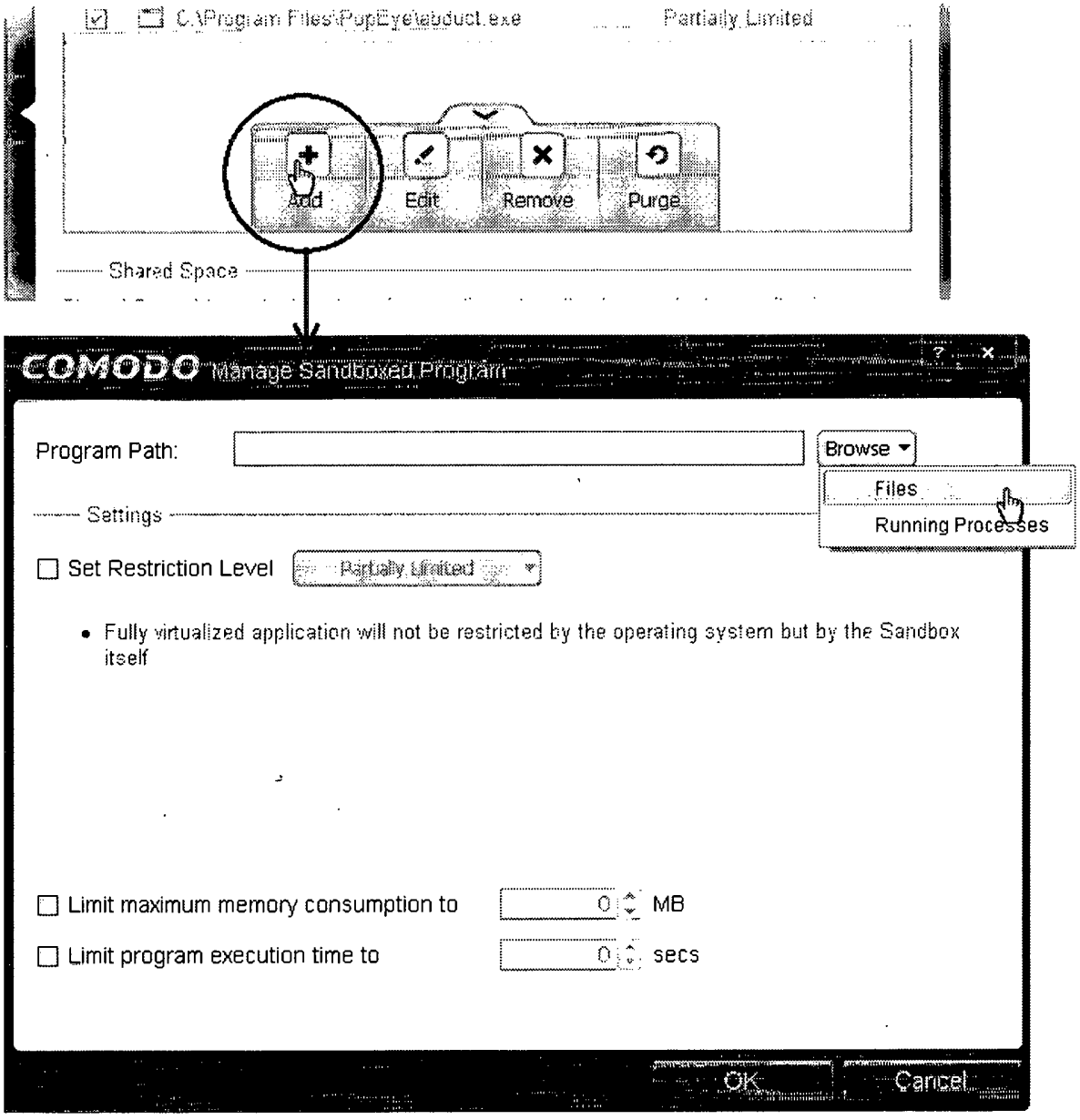
- Right click on the program or file to be opened from the Windows Explorer and select 'Run in Comodo Sandbox'

or

- Flip the 'Scan objects' pane in the CIS Home screen to show 'Sandbox Objects' and drag and drop the program or file from Windows Explorer to the pane

To manually add a program to Sandbox

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



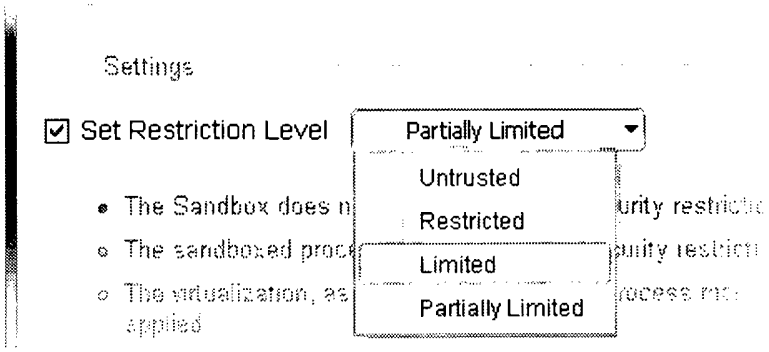
- The 'Manage Sandboxed Program' interface will open:

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

- **Files** - Allows you to navigate to the executable of the program you wish to add.
- **Running Processes** - Allows you to add a program to the sandbox by choosing a running process.

Settings:

- **Set Restriction Level** - The Access restriction level determines the amount of privileges a sandboxed application has to access other software and hardware resources on your computer. (***Default = Disabled***)
- Set an access restriction level by enabling the 'Set Restriction Level' check-box and choosing a level from the drop-down.
- If you do not set a restriction level, CIS will automatically apply a level of 'Fully Virtualized'.



- **Fully Virtualized** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Untrusted -** The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Please note, some applications that require user interaction may not work properly under this setting.
- **Restricted -** The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Please note, applications like computer games may not work properly under this setting.
- **Limited -** Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is not allowed to execute actions that require Administrator account privileges. Access to many system resources, like the clipboard, are also prohibited.
- **Partially Limited** (***Default***)- The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed.

- **Limit maximum memory consumption to**: You can define how much system memory can be allocated to the application by selecting this check-box then entering the desired memory (in MB) in the combo box beside it (***Default = Disabled***).
- **Limit the program execution time to**: You can define how long the program is allowed to run by selecting this check-box then entering the time (in seconds). The program will be terminated after this time has elapsed. (***Default = Disabled***).
- Click OK to add the program to the list of sandboxed programs. From this point onwards the application will be run in the sandbox.
- If you wish to remove it at a later date, simply select it in the list and click 'Remove'. Next time you execute this application it will run outside of the sandbox (presuming it is not then detected as malicious or automatically sandboxed as **per the sandboxing process**).
- To edit the restriction settings for an application included in the sandbox, select the application and click 'Edit'. The process is same as explained in **adding a program to sandbox**.

Shared Space Settings:



'Shared Space' is a dedicated area on your local drive that sandboxed applications are permitted to write to and which can also be accessed by non-sandboxed applications (hence the term 'Shared Space'). For example, any files or programs you download via a sandboxed browser that you wish to be able to access from your real system should be downloaded to the shared space. This folder is also used by the Virtual Desktop and is located by default at 'C:/Program Data/Shared Space'.

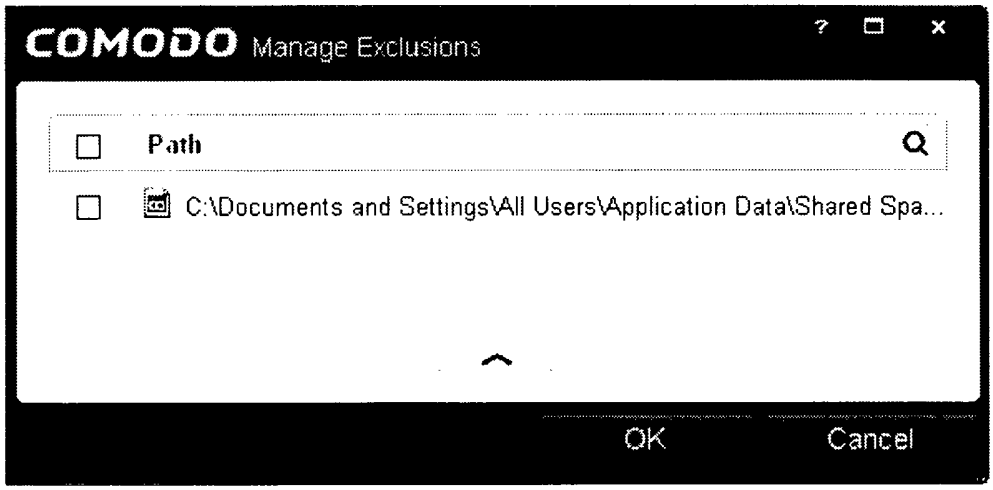
You can access the shared space folder in the following ways:

- Clicking the 'Shared Space' shortcut on your computer desktop

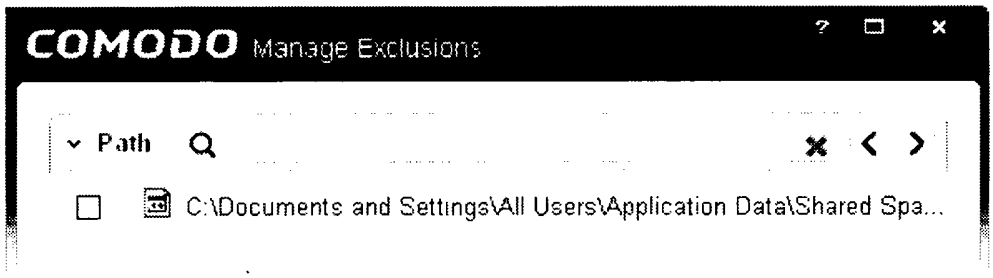
- Clicking 'Shared Space' button on the CIS interface
- Opening 'Sandbox Tasks' from the Tasks interface then clicking 'Open Shared Space'
- By default, sandboxed applications can access folders and files on your 'real' system but cannot save any changes to them. However, you can define exclusions to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

To define exclusions for files and folders

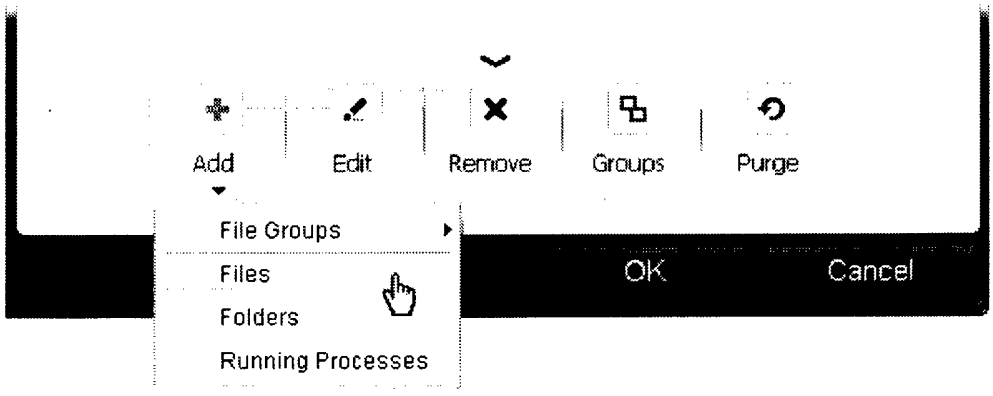
- Enable the 'Do not virtualize access to the specified files/folders' check-box then click on the words 'the specified files/folders'. The 'Manage Exclusions' dialog will appear.



You can search for specific excluded path, file or folder from the list by clicking the search icon at the far right in the column header and entering the name of the file/folder in full or part. You can navigate through the successive results by clicking the left and right arrows.



- Click the handle at the bottom to open the tools menu then click 'Add'.



Files - Allows you to specify files or applications that sandboxed applications are able to access

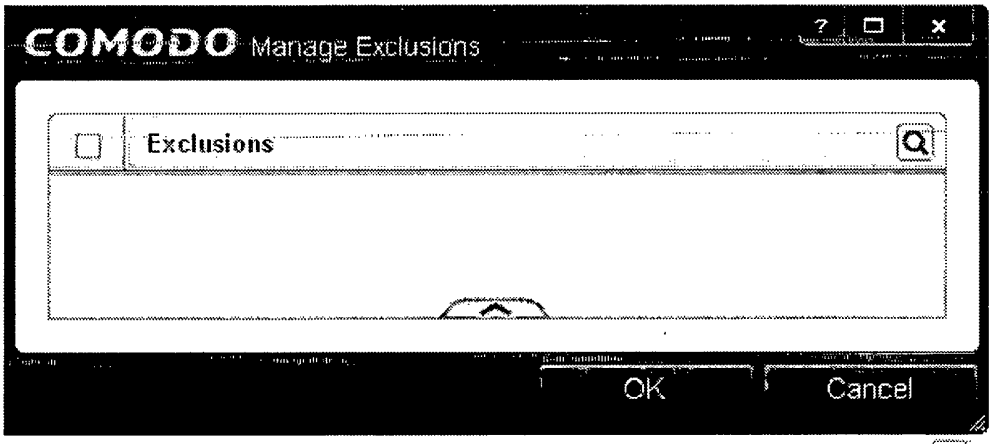
Folders - Specify a folder that can be accessed by sandboxed applications
File Groups - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exclusion for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl. For more details on file groups, refer to the section **File Groups**.

- **Running Processes** - Allows you to specify a parent program that sandboxed applications are able to access by choosing a running process.

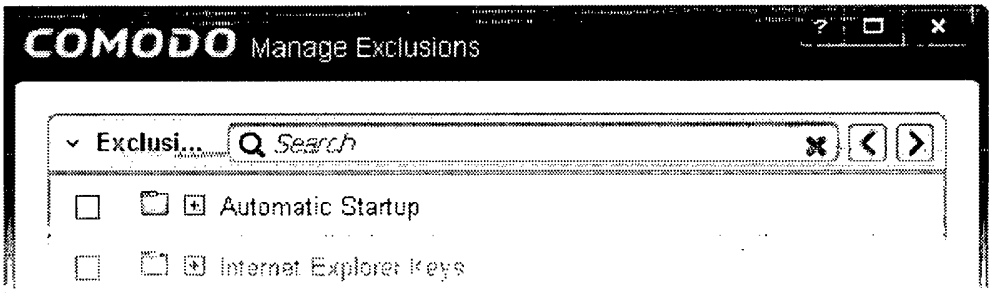
- To edit an exclusion, select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Change file or folder location path and click 'OK'
  - Click 'OK' to implement your settings
  - To manage available file groups, click the 'Groups' button from the tools menu. The 'Manage 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 exclusions for specific Registry keys and values

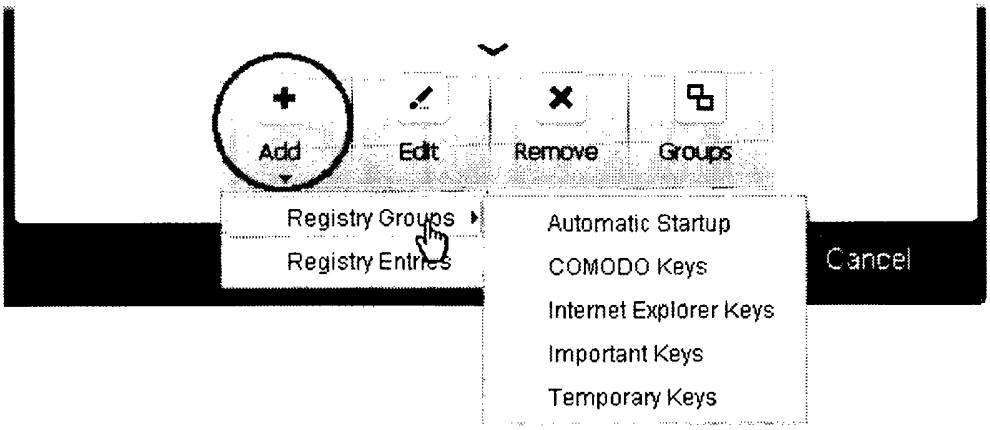
- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the words 'the specified registry keys/values'. The 'Manage Exclusions' dialog will appear.



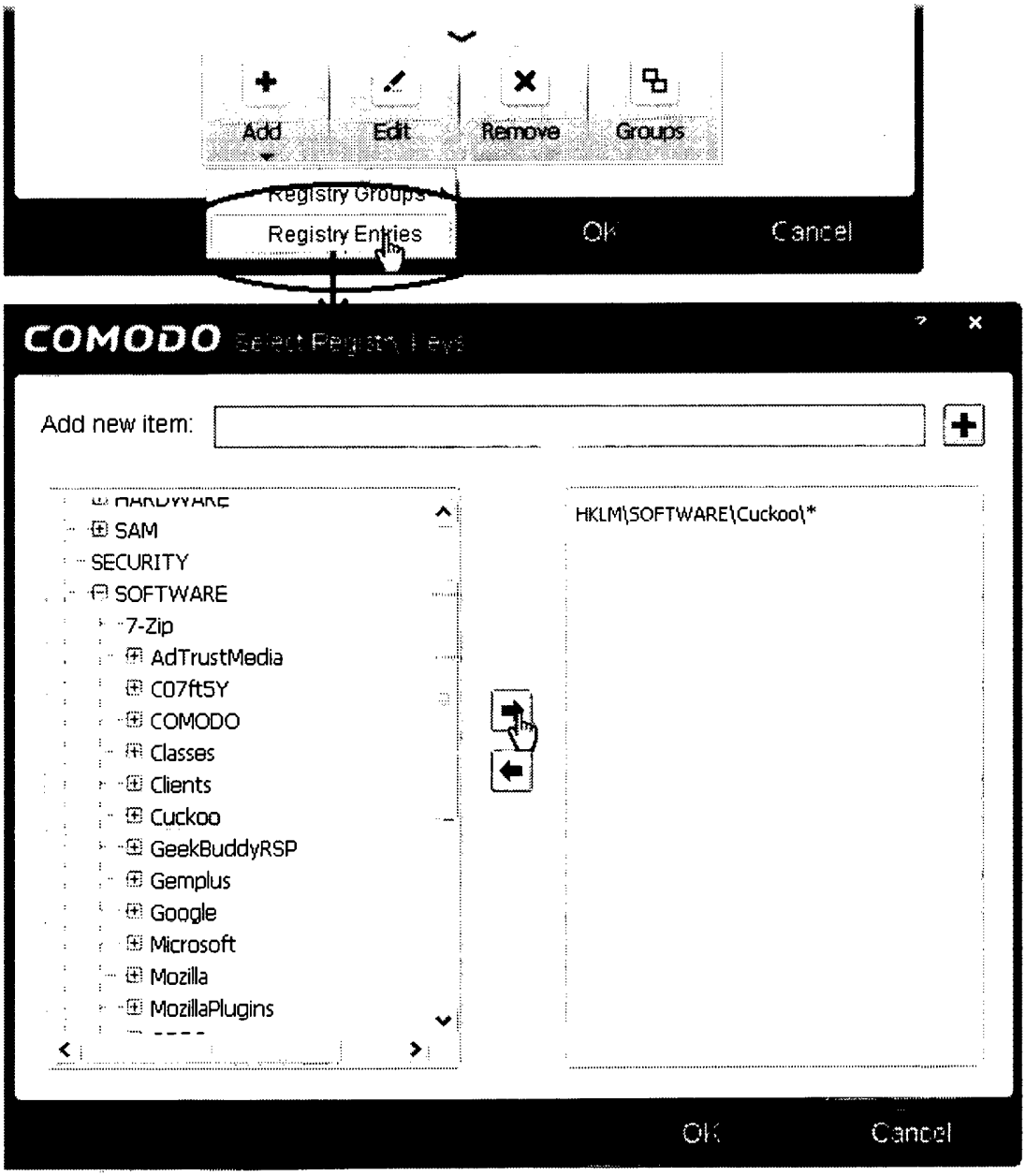
You can search for specific excluded Registry Keys or Values from the list by clicking the search icon at the far right in the column header and entering the name of the key/value in full or part. You can navigate through the successive results by clicking the left and right arrows.



- Click the handle at the bottom to open the tools menu then click 'Add'.

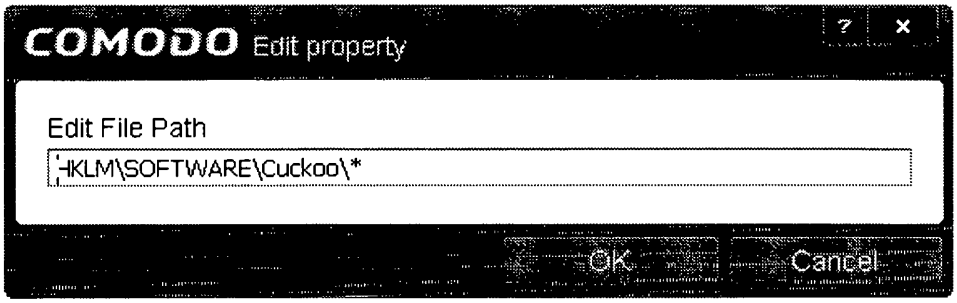


- **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exclusions. For an explanation of CIS registry groups, refer to the section **Registry Groups**.
- **Registry Entries** - Opens an interface that allows you to quickly browse Windows registry keys and add them as exclusions:



- Click 'OK' to implement your settings.

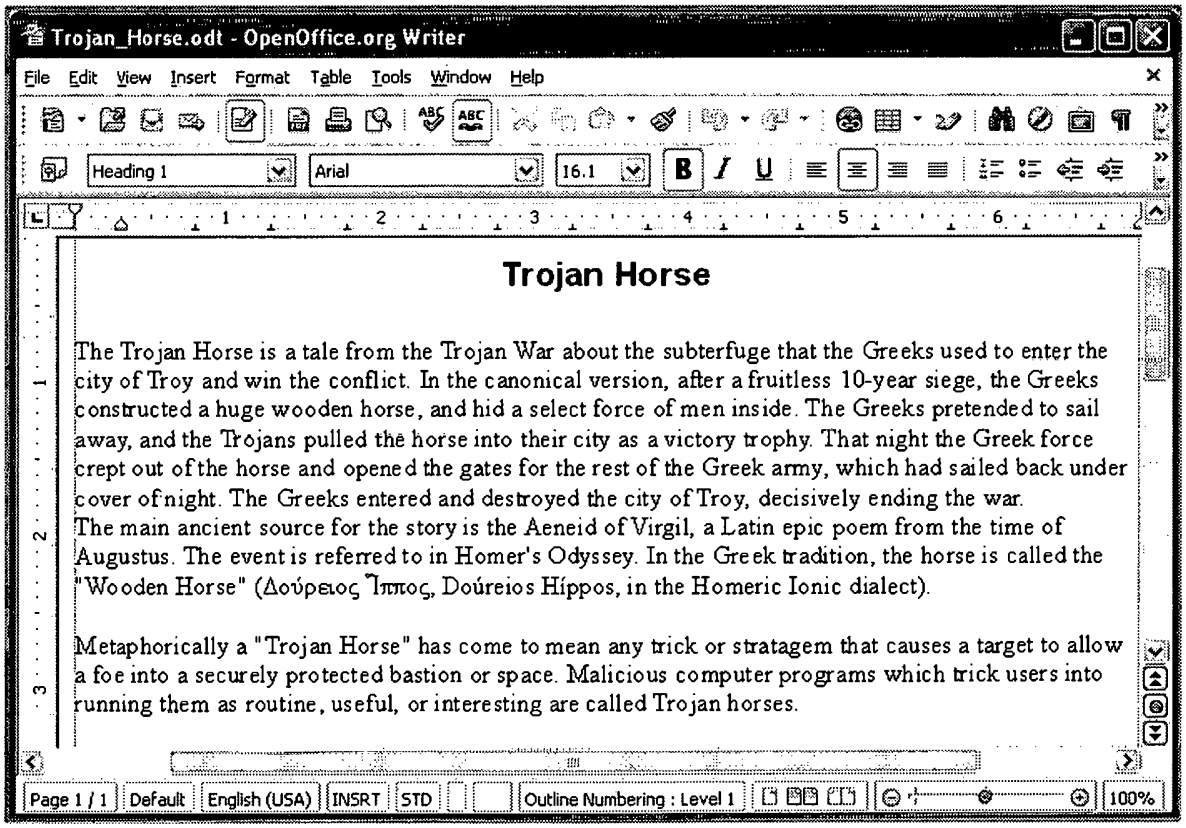
- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Edit the key path and click OK.



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

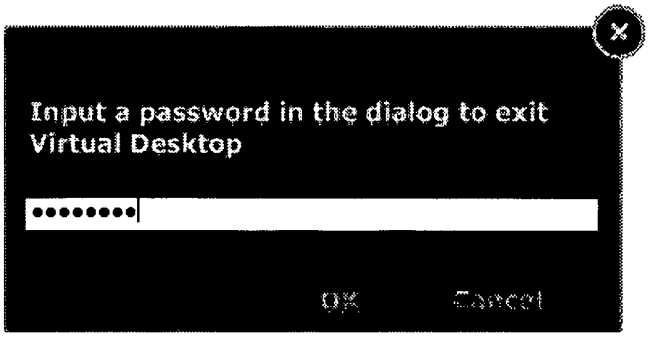
Other Settings:

- **Enable automatic startup for services installed in the sandbox** - By default, CIS does not permit sandboxed services to run at Windows startup. Select this check-box to allow them to do so. (***Default = Disabled***)
- **Show highlight frame for virtualized programs** - If enabled, CIS displays a green border around the windows of programs that are running inside the sandbox. The following example shows an .odt document opened with a sandboxed version OpenOffice Writer:



Virtual Desktop Settings

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



The exit password for the Virtual Desktop acts as a security measure to prevent guest users or younger users from exiting out of the isolated environment you have prepared for them and potentially exposing the real system to danger.

To set an exit password for Virtual Desktop:

- Select the 'Protect Virtual Desktop with a password' check-box then click the words password. The 'Change password' dialog will appear.

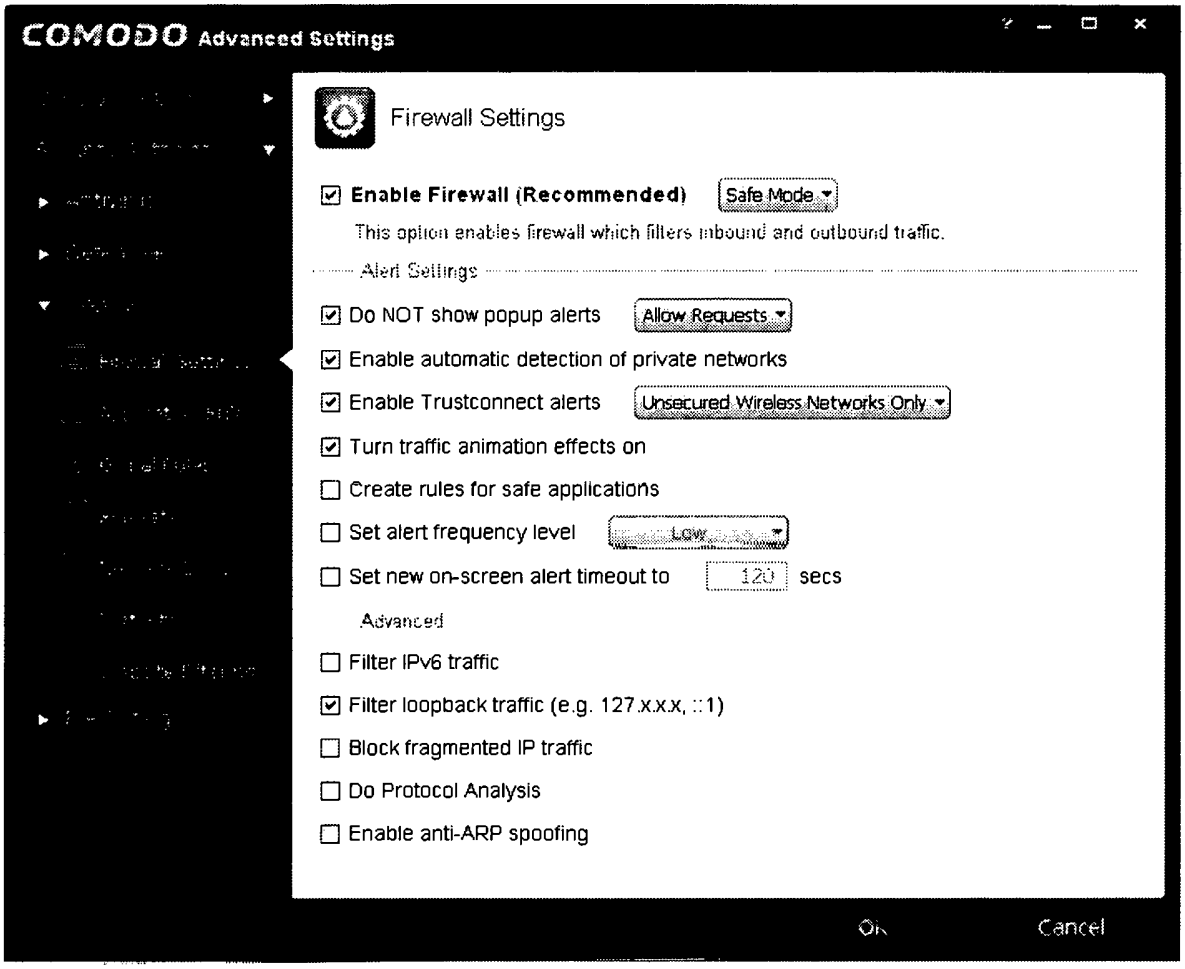


- Type a password which contains a combination of alphabetic and numeric characters and symbols which cannot be easily guessed by others. We recommend a password of at least 8 character in length.
- Re-enter the password in the 'Retype' field then click 'OK'.

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

6.2.3. Firewall Settings

The Firewall component of Comodo Internet Security offers the highest levels of security against inbound and outbound threats. It checks that all network traffic in and out of your computer is legitimate, it stealths your computer's ports against hackers and it blocks malicious software from transmitting your confidential data over the Internet. Comodo Firewall also makes it easy for you to specify exactly which applications are allowed to connect to the Internet and immediately warns you when there is suspicious activity. Also you can configure rules to allow or block access to specific websites for particular users of your computer.



The 'Firewall Settings' area has several sub-sections that allow you to configure overall behavior; configure network zones and portsets and (for advanced users) to configure and deploy traffic filtering rules on an application specific and global basis.

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

- **Firewall Behavior Settings** - Configure settings that govern the overall behavior of the firewall component.
- **Application Rules** - View, create and modify rules that determine the network access privileges of individual applications or specific types of application
- **Global Rules** - View, create and modify rules that apply to all traffic flowing in and out of your computer.
- **Rule Sets** - Predefined collections of firewall rules that can be applied, out-of-the-box, to Internet capable applications such as browsers, email clients and FTP clients.
- **Network Zones** - A network zone is a named grouping of one or more IP addresses. Once created, you can specify a zone as the target of firewall rule.
- **Portsets** - Predefined groups of regularly used ports that can used and reused when creating traffic filtering rules.
- **Website Filtering** - Create website filtering rules which let you determine which sites certain users can or cannot access.

Background note on rules: Both application rules and global rules are consulted when the firewall is determining whether or

not to allow or block a connection attempt.

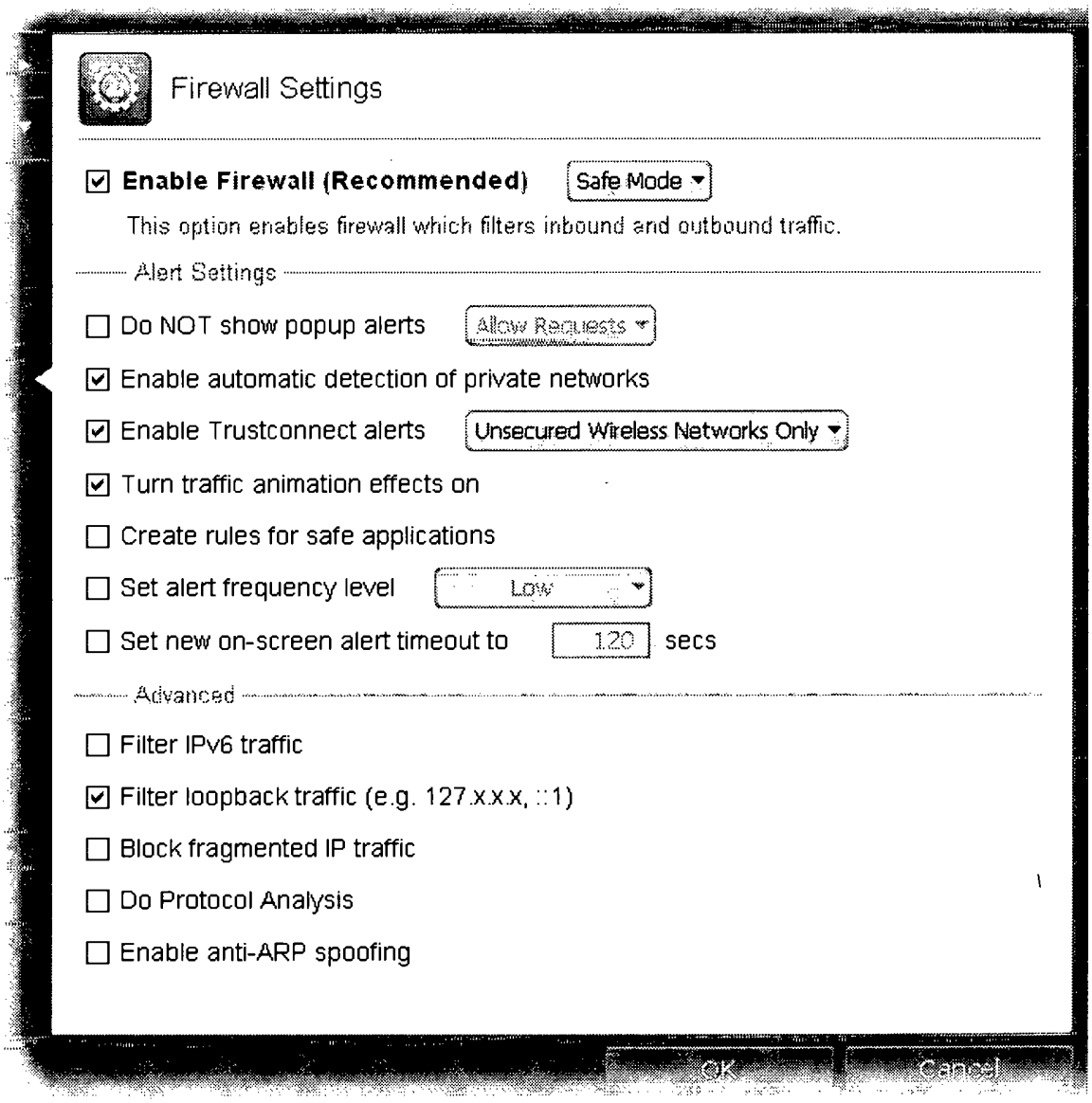
- For Outgoing connection attempts, the application rules are consulted first then the global rules.

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

6.2.3.1. Firewall Behavior Settings

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

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

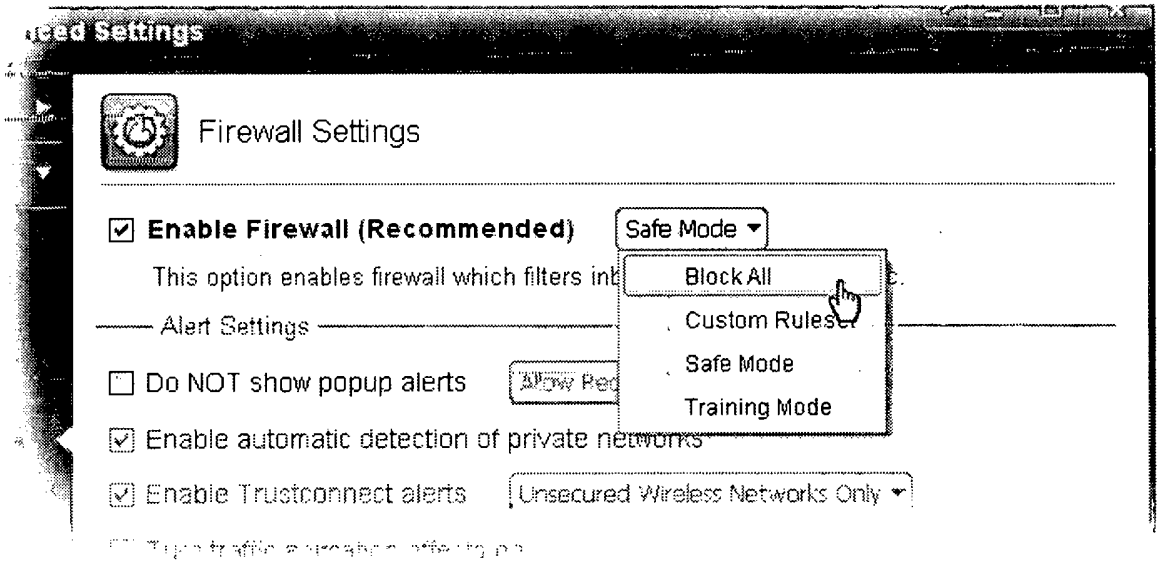


General Settings

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

Note: The Firewall configuration settings can also be modified in the 'Advanced View' of the Home screen by clicking the status link beside Firewall in the Firewall pane.

If enabled, you can also choose the security level from the accompanying drop-down menu:



The choices available are:

- **Block All:** The firewall blocks all traffic in and out of your computer regardless of any user-defined configuration and rules. The firewall does not attempt to learn the behavior of any application and does not automatically create traffic rules for any applications. Choosing this option effectively prevents your computer from accessing any networks, including the Internet.
- **Custom Ruleset Mode:** The firewall applies ONLY the custom security configurations and **network traffic rules** specified by the user. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. You will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, you have specified rules and policies that instruct the firewall to trust the application's connection attempt).

  If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.
- **Safe Mode *(Default)***: While filtering network traffic, the firewall automatically creates rules that allow all traffic for the components of applications certified as 'Safe' by Comodo, if the checkbox **Create rules for safe applications** is selected. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This deploys the **predefined firewall ruleset** 'Trusted Application' onto the application.

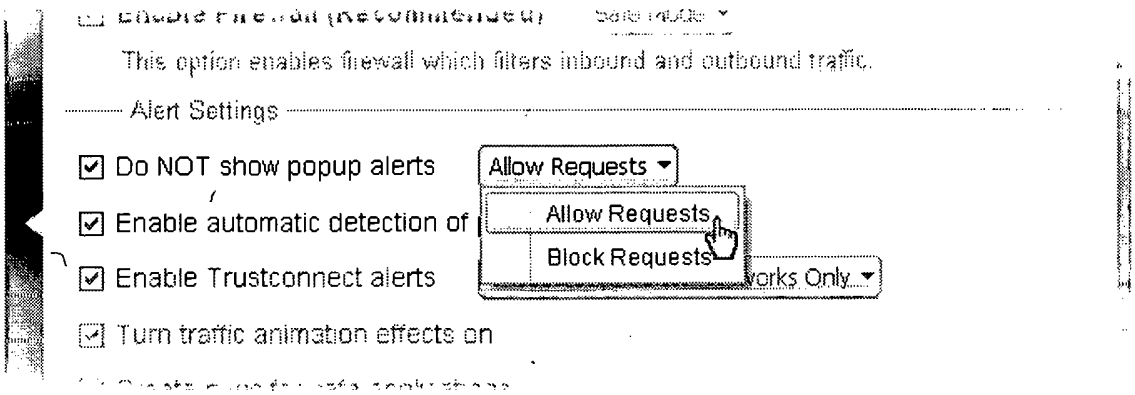
  'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.
- **Training Mode** : The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. You will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on your computer are assigned the **correct network access rights**.

Alert Settings

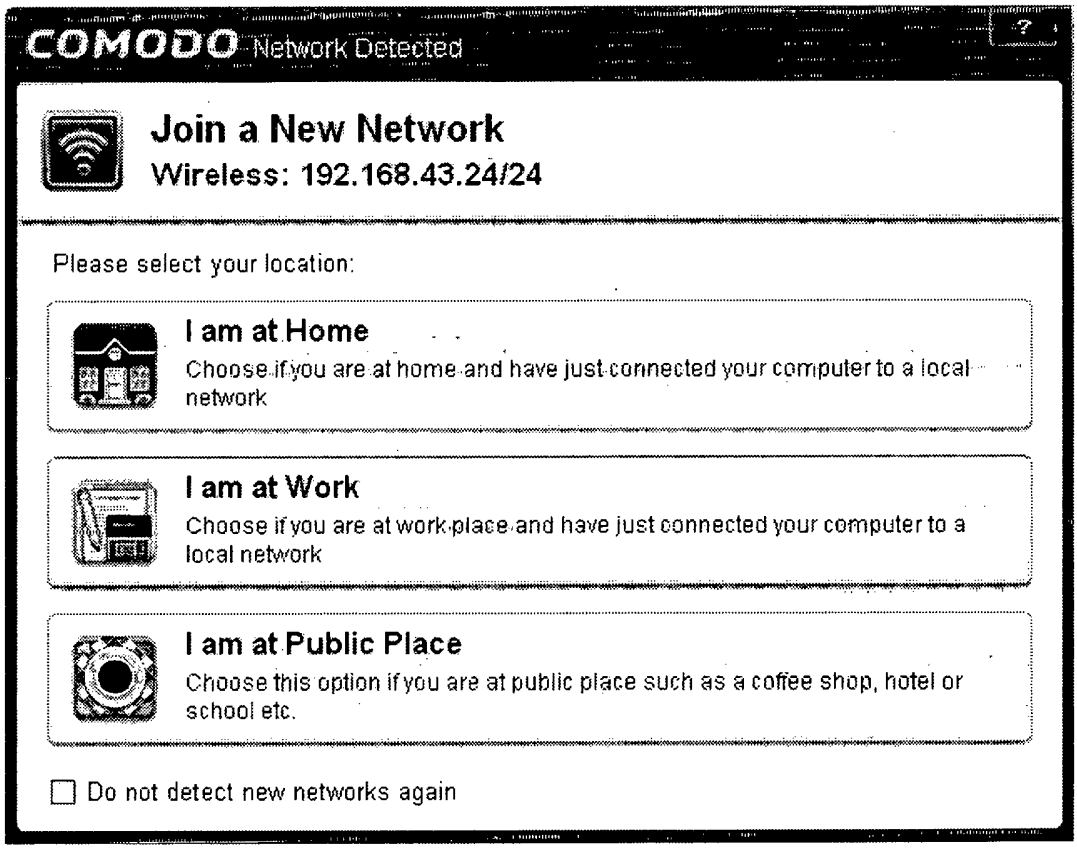
- **Do NOT show popup alerts** - Configure whether or not you want to be notified when the firewall encounters a request for network access. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness. (***Default = Enabled***)

Best Available Copy

If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Requests' or 'Allow Requests'.



- **Enable automatic detection of private networks** - Instructs Comodo Firewall to keep monitoring whether your computer is connected to any new wired or wireless network. The firewall will display an alert as shown below if it detects a new network (for example, when you connect to a wired home or office network or a Wi-Fi network).

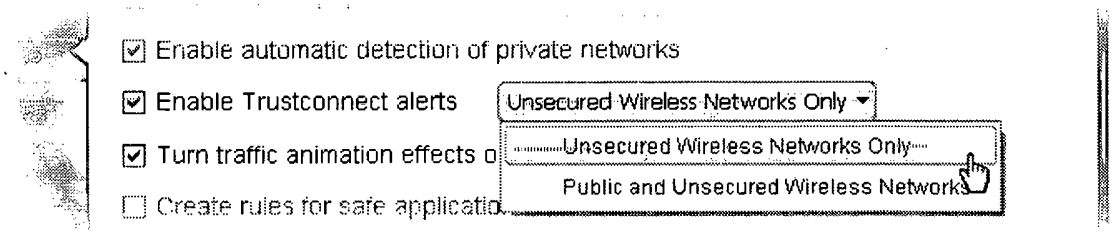


You can select the type of new network you are connected to, so that the firewall configuration is optimized for the type of connection. Comodo recommends users to leave this option at its default, enabled setting ***(Default = Enabled)***.

Enable Trustconnect alerts - If you are connecting to Internet at a public place like an airport or a coffee shop then you are potentially exposing yourself to danger. Unsecured public networks can allow other people to easily eavesdrop on your communications or even gain access to your computer to steal your confidential information. In order to safeguard against such attempts, Comodo recommends you encrypt your connection in public hotspots using TrustConnect - a secure Internet proxy service.

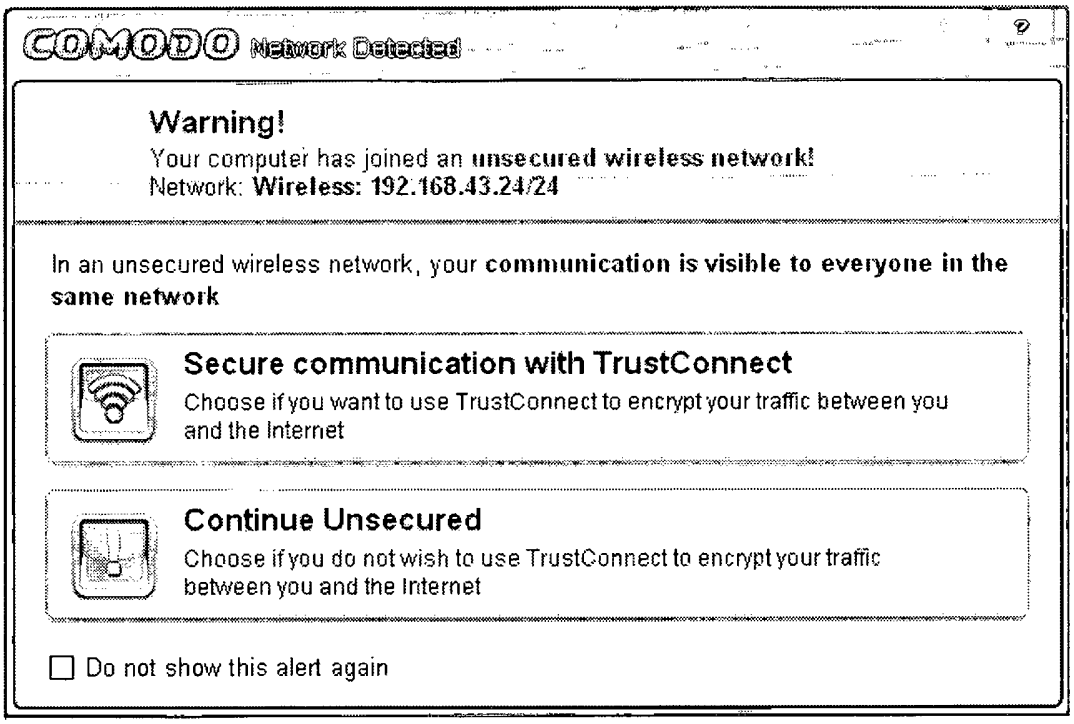
If selected, Comodo Firewall will display an alert if it detects you are connected to the Internet through an unsecured network

(***Default=Enabled***). The drop-down options allow you to select the conditions under which you want alerts to be displayed:



- **Unsecured Wireless Networks Only** (***Default***) - TrustConnect alerts are displayed only if you are connecting to an unencrypted wireless network.
- **Public and Unsecured Wireless Networks only** - TrustConnect alerts are displayed whenever you connect to a public wireless network irrespective of whether the connection is encrypted

You will be alerted and offered the opportunity to secure the connection via the following notification:



- **Turn traffic animation effects on** - By default, the Comodo Internet Security's 'Shield' tray icon displays a small animation whenever traffic moves to or from your computer.



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

- **Create rules for safe applications** - Comodo Firewall trusts the applications if:
  - The application/file is included in the Trusted Files list under File Rating Settings;
  - The application is from a vendor included in the **Trusted Software Vendors** list under File Rating Settings;
  - The application is included in the extensive and constantly updated Comodo safelist.

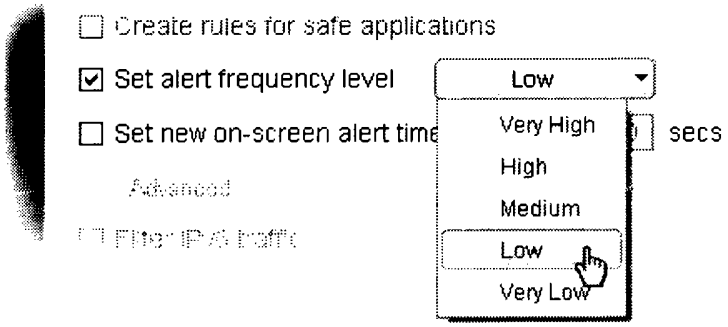
By default, CIS does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is

beneficial to beginners who find difficulties in setting up the rules.

Enabling this checkbox instructs CIS to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the **Application Rules** interface. The Advanced users can edit/modify the rules as they wish ***(Default = Disabled).***

Background Note: Prior to version 4.x , CIS would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CIS version 3.x).

- **Set alert Frequency level** - Enabling this option allows you to configure the amount of alerts that Comodo Firewall generates, from the drop-down. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in '**Application Rules**' and '**Global Rules**'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages. (***Default=Disabled***)



The options available are:

- **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.
- **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.
- **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.
- **Low:** The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.
- **Very Low**: The firewall shows only one alert for an application.

The Alert Frequency settings refer only to connection attempts by applications or from IP addresses that you have not (yet) decided to trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.

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

Advanced Settings

Comodo Firewall features advanced detection settings to help protect your computer against common types of denial of service (DoS) attack. When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server.

- **Filter IP v6 traffic** - If enabled, CIS will filter IPv6 network traffic in addition to IPv4 traffic.(***Default = Disabled***).

Background Note: IPv6 stands for Internet Protocol Version 6 and is intended to replace Internet Protocol Version 4 (IPv4). The move is primarily driven by the anticipated exhaustion of available IP addresses. IPv4 was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available. This hard limit has already led to the development of 'work-around' solutions such as Network Address Translation (NAT), which enable multiple hosts on private networks to access the Internet using a single IP address.

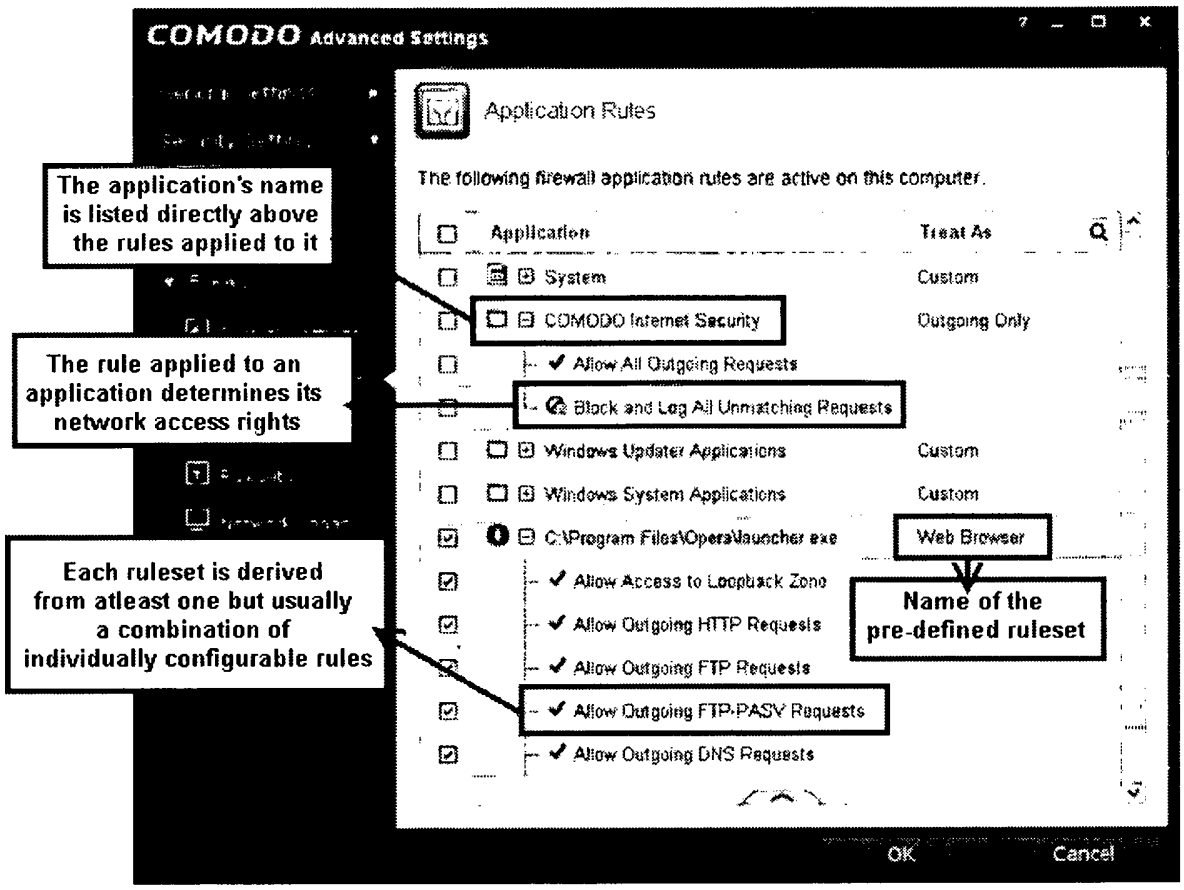
IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

- **Filter loopback traffic**: Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately also received by it. This involves no connection outside your computer to the Internet or a local network. The IP address of the loopback network is 127.0.0.1, which you may have heard referred to under its domain name of 'http://localhost' i.e. the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this box checked means the firewall filter traffic sent through this channel. communicate using the loopback channel. (***Default = Enabled***).
- **Block Fragmented IP traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time (***Default = Disabled***).
- **Do protocol Analysis** - Protocol Analysis is key to the detection of fake packets used in denial of service attacks. Checking this option means Comodo Firewall checks every packet conforms to that protocols standards. If not, then the packets are blocked (***Default = Disabled***).
- **Enable anti-ARP spoofing** - A gratuitous Address Resolution Protocol (ARP) frame is an ARP Reply that is broadcast to all machines in a network and is not in response to any ARP Request. When an ARP Reply is broadcast, all hosts are required to update their local ARP caches, whether or not the ARP Reply was in response to an ARP Request they had issued. Gratuitous ARP frames are important as they update your machine's ARP cache whenever there is a change to another machine on the network (for example, if a network card is replaced in a machine on the network, then a gratuitous ARP frame informs your machine of this change and requests to update your ARP cache so that data can be correctly routed). However, while ARP calls might be relevant to an ever shifting office network comprising many machines that need to keep each other updated , it is of far less relevance to, say, a single computer in your home network. Enabling this setting helps to block such requests - protecting the ARP cache from potentially malicious updates ***(Default = Disabled).***

6.2.3.2. Application Rules

Overview of Rules and Rulesets

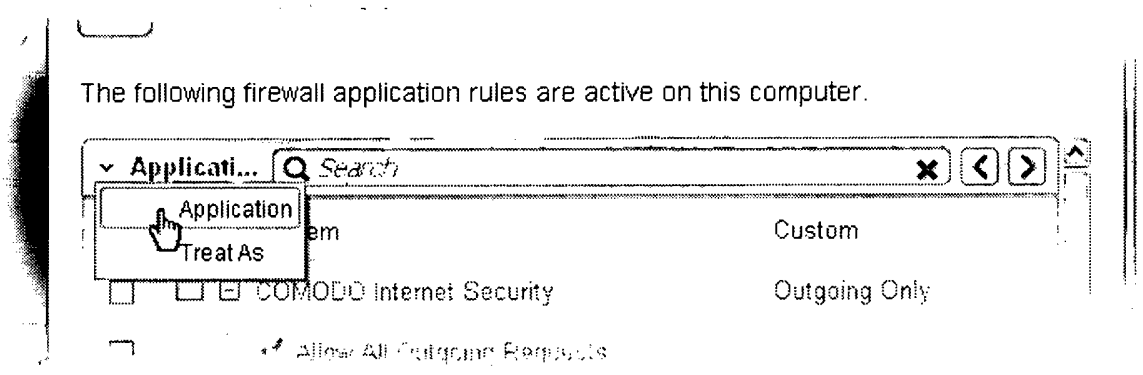
Whenever an application makes a request for Internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Ruleset that has been specified for that application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual network access rule contains instructions that determine whether the application should be allowed or blocked; which protocols it is allowed to use; which ports it is allowed to use and so forth.



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

You can use the search option to find a specific name in the list.

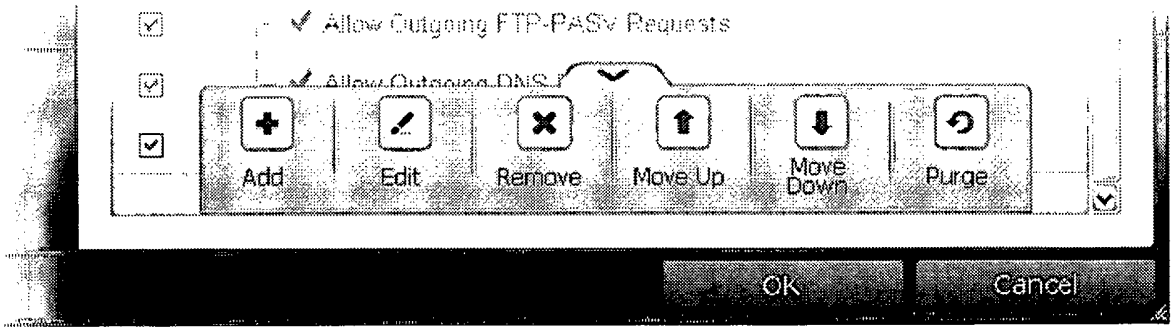
To use the search option, click the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

General Navigation:

Clicking the handle at the bottom center of the interface opens a rule control panel:



- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the sections **'Creating or Modifying Firewall Rules'** and **'Adding and Editing a Firewall Control Rule'.**
- **Edit** - Allows the user to modify the Firewall rule or ruleset of the selected application. See the sections **'Creating or Modifying Firewall Rules'** and **'Adding and Editing a Firewall Rule'**.
- **Remove** - Deletes the selected ruleset.
- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

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

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

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

- Double click on the specific rule to begin **'Adding and Editing a Firewall Rule'**
- Select the specific rule and click the handle at the bottom center and choose 'Edit' from the options to begin **'Adding and Editing a Firewall Rule'**

Users can also re-prioritize rulesets by clicking the handle at the bottom center and select 'Move Up' or 'Move Down' from the options.

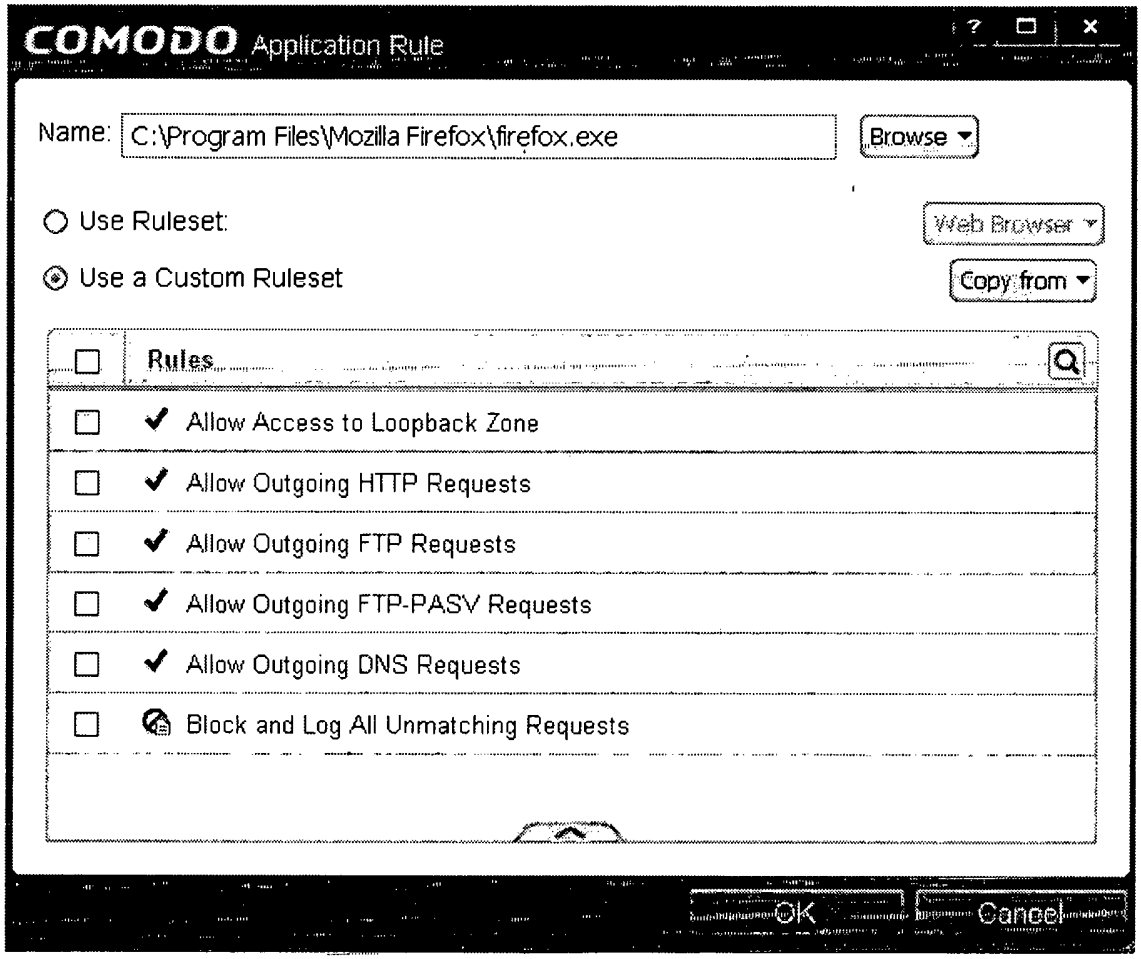
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications like 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo Firewall to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements. For more details, see **Predefined Rule Sets.**

- See **Application Rule interface** for an introduction to the rule setting interface
- See **Creating and Modifying Firewall Rulesets** to learn how to create and edit Firewall rulesets
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration

Application Rule interface

Firewall rules can be added/modified/removed and re-ordered through the Application Rule interface. Any rules created using **Adding and Editing a Firewall Rule** is displayed in this list.

The Application Rule interface is displayed when you click 'Add' or 'Edit' from the options in 'Application Rules' interface.

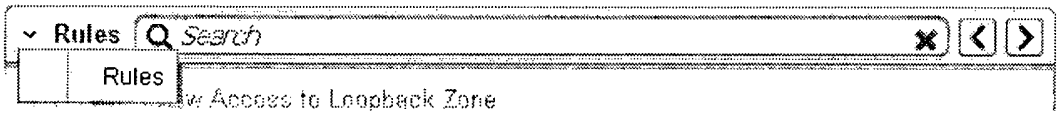


Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see **Understanding Firewall Rules** for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied.

Users can also re-prioritize rulesets by clicking the handle at the bottom center and select 'Move Up' or 'Move Down' from the options. To begin creating Firewall rulesets, first read **'Overview of Rules and Rulesets'** then **'Creating and Modifying Firewall Rulesets'**

You can use the search option to find a specific rule in the list.

To use the search option, click the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

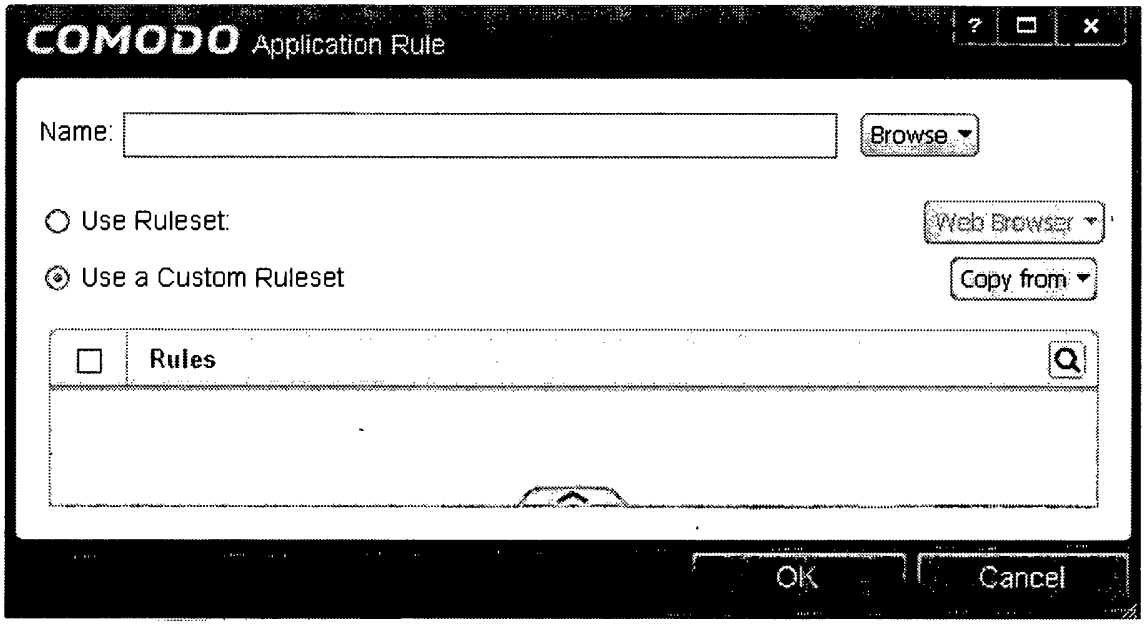
Creating and Modifying Firewall Rulesets

To begin defining an application's Firewall ruleset, you need take two basic steps.

- Step 1 - **Select the application that you wish the ruleset is to be applied.**
- Step2 - **Configure the rules for this application's ruleset.**

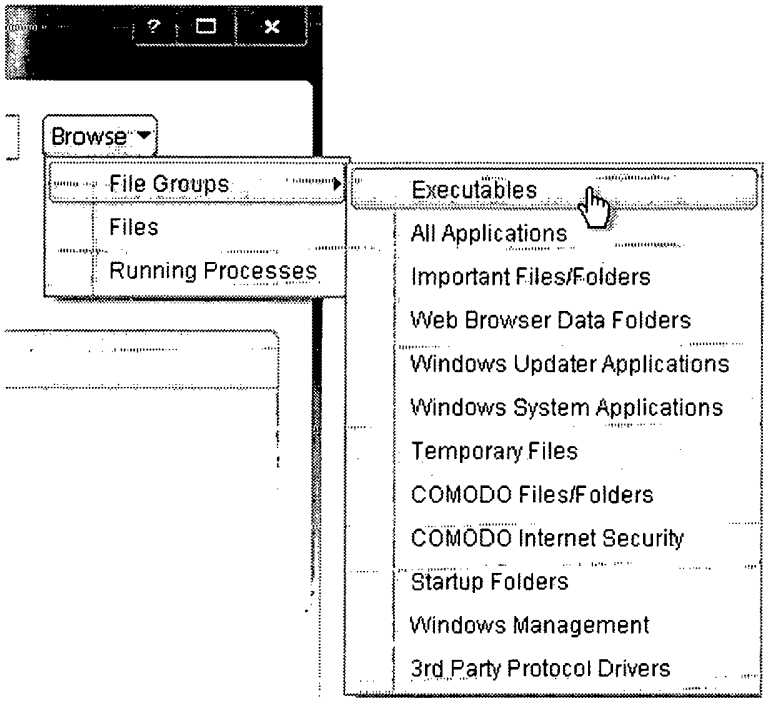
Step 1 - Select the application that you wish the ruleset is to be applied

If you wish to define a ruleset for a new application (i.e. one that is not already listed) then click the handle from the **Application Rules interface** and select 'Add' from the options. This brings up the '**Application Rule**' interface shown below:



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

- Click 'Browse' button.

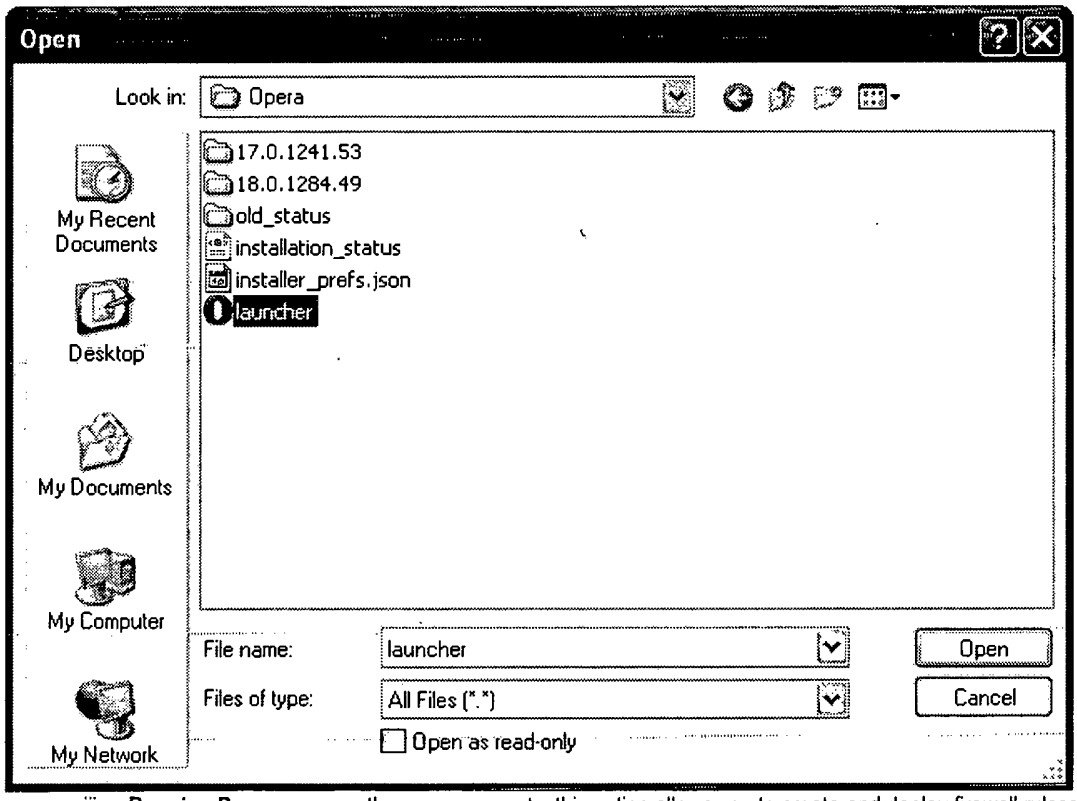


You now have 3 methods available to choose the application for which you wish to create a ruleset - **File Groups**; **Files** and

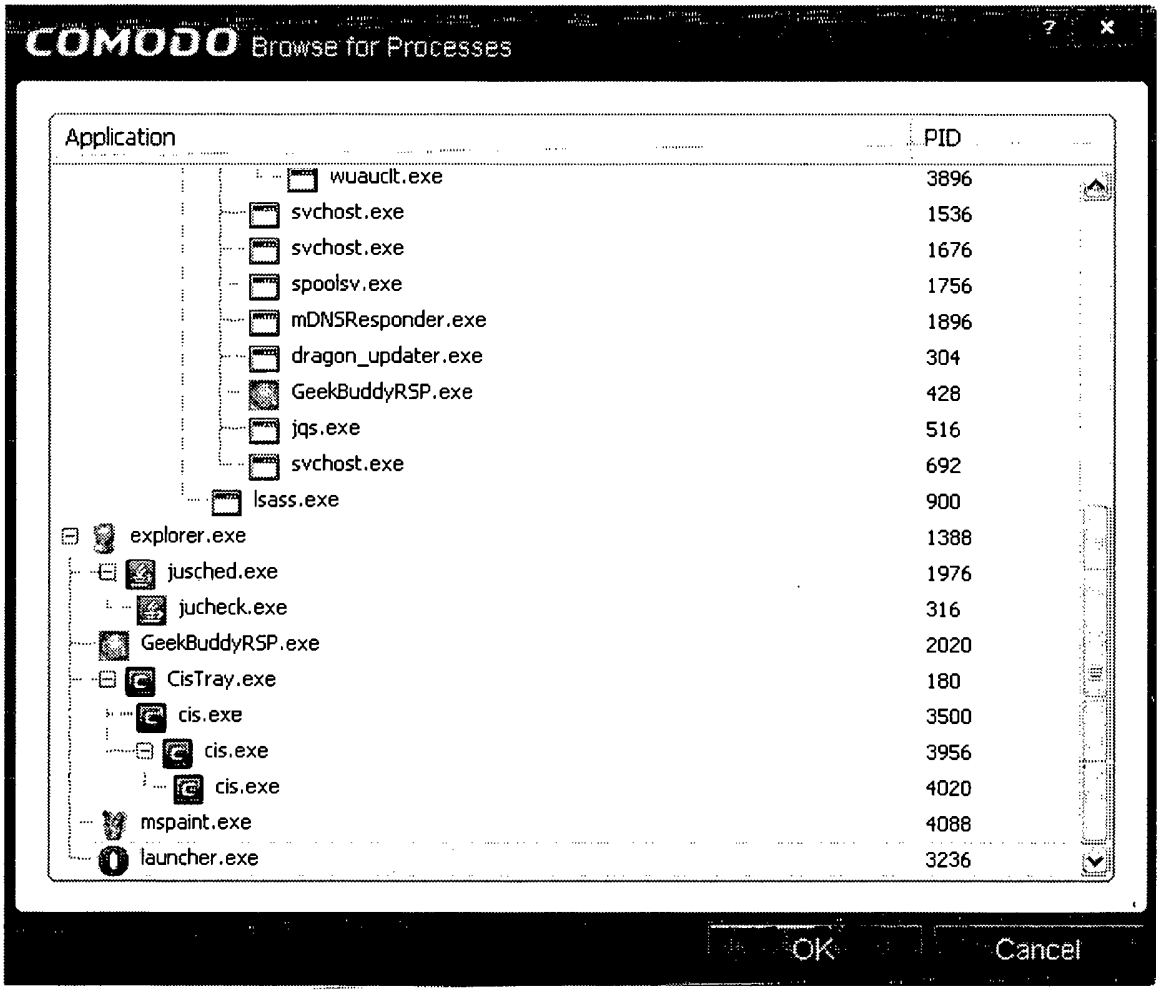
Running Processes and

i. **File Groups** - choosing this option allows you to create firewall ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a Firewall Ruleset for any file that attempts to connect to the Internet with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders. To view the file types and folders that are affected by choosing one of these options, you need to visit the 'Protected Files' of Comodo Internet Security by navigating to: Advanced Settings > Security Settings > Defense+ > HIPS > File Protection> Protected Files and clicking the handle from the bottom center > Groups. For more details on file groups, refer to the section **File Groups**.

ii. **Files** - this option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the firewall ruleset. In the example below, we have decided to create a firewall ruleset for the Opera web browser.



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



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

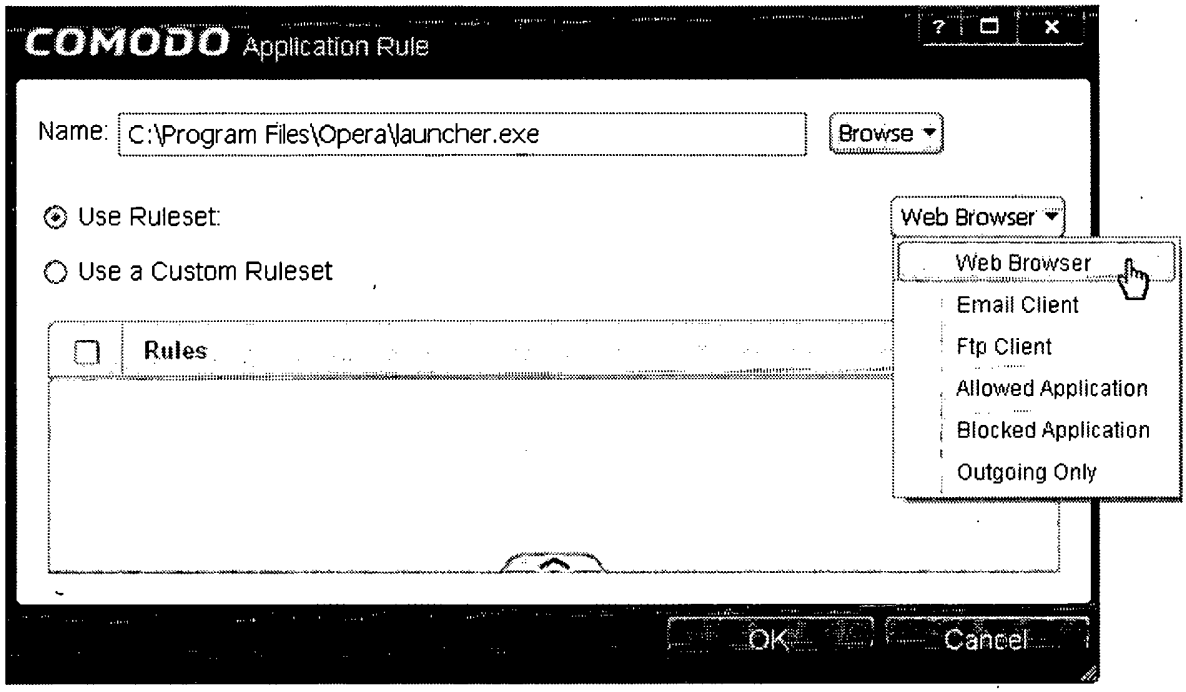
Having selected the individual application, running process or file group, the next stage is to Configure the rules for this application's Firewall Ruleset.

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

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

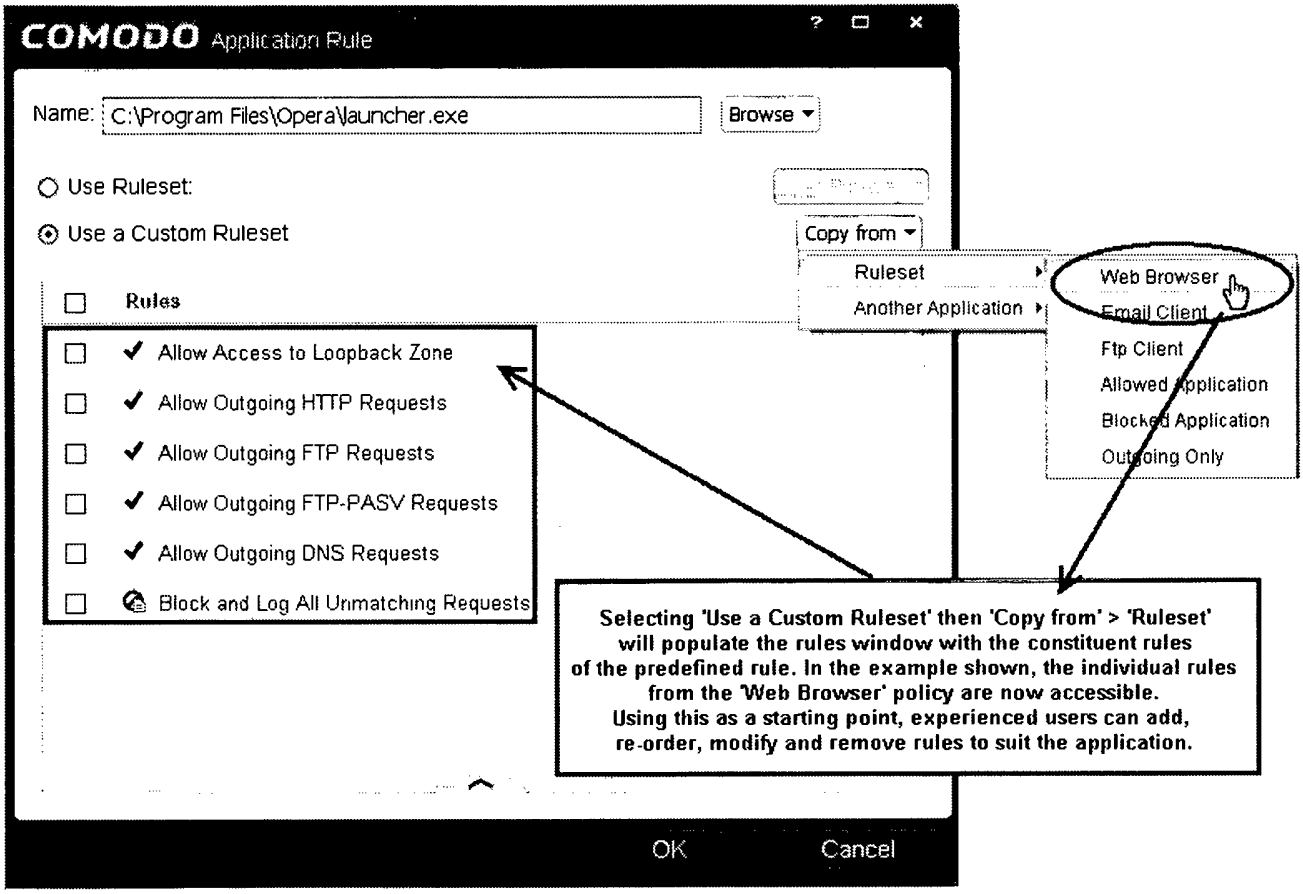
- **Use a Predefined Ruleset** - Selecting this option allows the user to quickly deploy a existing ruleset on to the target application. Choose the ruleset you wish to use from the drop-down menu. In the example below, we have chosen 'Web Browser' because we are creating a ruleset for the 'Opera' browser.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

Best Available Copy



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

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



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

- Clicking the handle from the bottom right and choosing 'Add' from the options to add individual Firewall rules. See '**Adding and Editing a Firewall Rule**' for an overview of the process.
- Use the 'Copy From' button to populate the list with the Firewall rules of a **Predefined Firewall Rule.**
- Use the 'Copy From' button to populate the list with the Firewall rules of another application's ruleset.

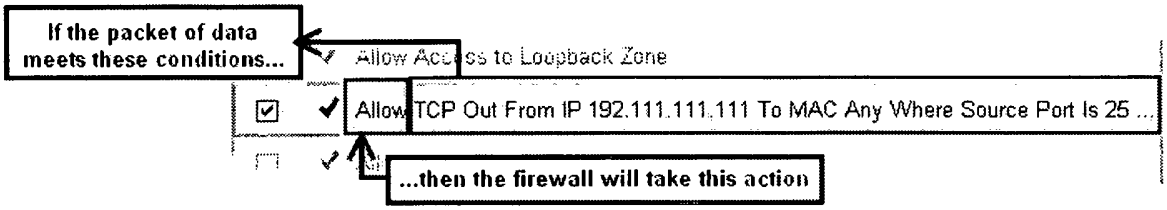
General Tips:

- If you wish to create a reusable ruleset for deployment on multiple applications, we advise you add a new **Predefined Firewall Rules** (or modify one of the existing ones to suit your needs) - then come back to this section and use the '**Ruleset**' option to roll it out.
- If you want to build a bespoke ruleset for maybe one or two specific applications, then we advise you choose the '**Use a Custom Ruleset**' option and create your ruleset either from scratch by adding individual rules or by using one of the built-in rulesets as a starting point.

Understanding Firewall Rules

At their core, each Firewall can be thought of as a simple **IF THEN** trigger - a set of **conditions** (or attributes) pertaining to a packet of data from a particular application and an **action** it that is enforced if those conditions are met.

As a packet filtering firewall, Comodo Firewall analyzes the attributes of *every single* packet of data that attempts to enter or leave your computer. Attributes of a packet include the application that is sending or receiving the packet, the protocol it is using, the direction in which it is traveling, the source and destination IP addresses and the ports it is attempting to traverse. The firewall then tries to find a Firewall rule that matches all the conditional attributes of this packet in order to determine whether or not it should be allowed to proceed. If there is no corresponding Firewall rule, then the connection is automatically blocked until a rule is created.



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

If you chose 'TCP' , 'UDP' or 'TCP and 'UDP', then the rule has the form: **Action |Protocol | Direction |Source Address | Destination Address | Source Port | Destination Port**

If you chose 'ICMP', then the rule has the form: **Action |Protocol | Direction | Source Address | Destination Address | ICMP Details**

If you chose 'IP', then the rule has the form: **Action | Protocol | Direction | Source Address | Destination Address | IP Details**

- **Action**: The action the firewall takes when the conditions of the rule are met. The rule shows '**Allow**', '**Block**' or '**Ask**'.**
- **Protocol**: States the protocol that the target application must be attempting to use when sending or receiving packets of data. The rule shows '**TCP**', '**UDP**', '**TCP** or **UDP**', '**ICMP**' or '**IP**'
- **Direction**: States the direction of traffic that the data packet must be attempting to negotiate. The rule shows '**In**', '**Out**' or '**In/Out**'
- **Source Address**: States the source address of the connection attempt. The rule shows '**From**' followed by one of the following: **IP** , **IP range**, **IP Mask** , **Network Zone**, **Host Name** or **Mac Address**
- **Destination Address**: States the address of the connection attempt. The rule shows '**To**' followed by one of the following: **IP**, **IP range**, **IP Mask**, **Network Zone**, **Host Name** or **Mac Address**
- **Source Port**: States the port(s) that the application must be attempting to send packets of data through. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **Destination Port**: States the port(s) on the remote entity that the application must be attempting to send to. Shows '**Where Source Port Is**' followed by one of the following: '**Any**', '**Port #**', '**Port Range**' or '**Port Set**'
- **ICMP Details**: States the ICMP message that must be detected to trigger the action. See **Adding and Editing a Firewall Rule** for details of available messages that can be displayed.
- **IP Details**: States the type of IP protocol that must be detected to trigger the action: See **Adding and Editing a Firewall Rule** to see the list of available IP protocols that can be displayed here.

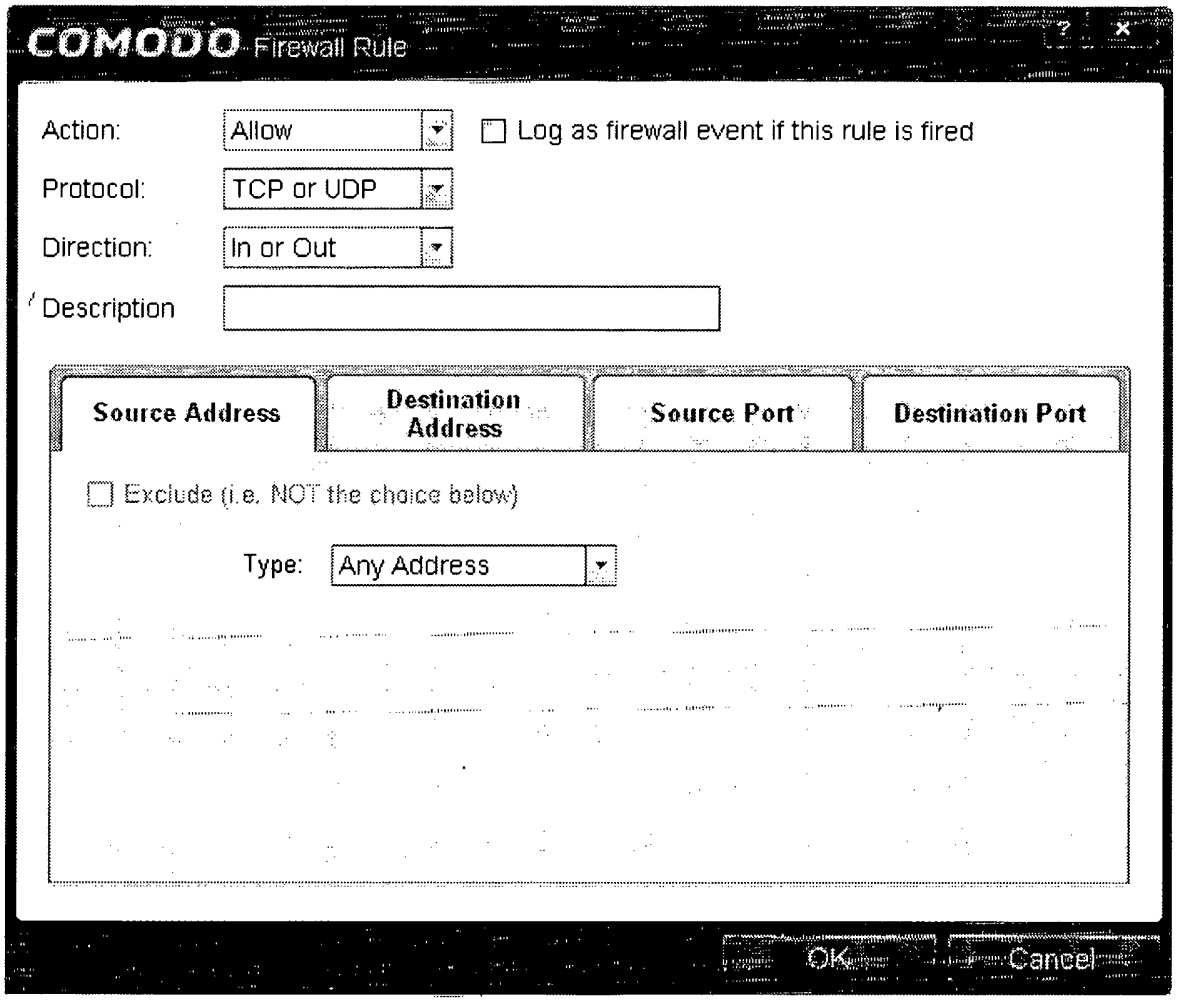
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section '**Global Rules**' to understand the interaction between Application Rules and Global Rules.

* *If you chose to add a descriptive name when creating the rule then this name is displayed here rather than it's full parameters. See the next section, '**Adding and Editing a Firewall Rule**', for more details.*

** *If you selected 'Log as a firewall event if this rule is fired' then the action is postfixed with 'Log'. (e.g. Block & Log)*

Adding and Editing a Firewall Rule

The Firewall Rule Interface is used to configure the actions and conditions of an individual Firewall rule. If you are not an experienced firewall user or are unsure about the settings in this area, we advise you first gain some background knowledge by reading the sections '**Understanding Firewall Rules**', '**Overview of Rules and Policies**' and '**Creating and Modifying Firewall Rulesets**'



General Settings

- **Action:** Define the action the firewall takes when the conditions of the rule are met. Options available via the drop down menu are '**Allow**' ***(Default)***, '**Block**' or '**Ask**'.
- **Protocol:** Allows the user to specify which protocol the data packet should be using. Options available via the drop down menu are '**TCP**', '**UDP**', '**TCP or UDP**' ***(Default)***, '**ICMP**' or '**IP**' .

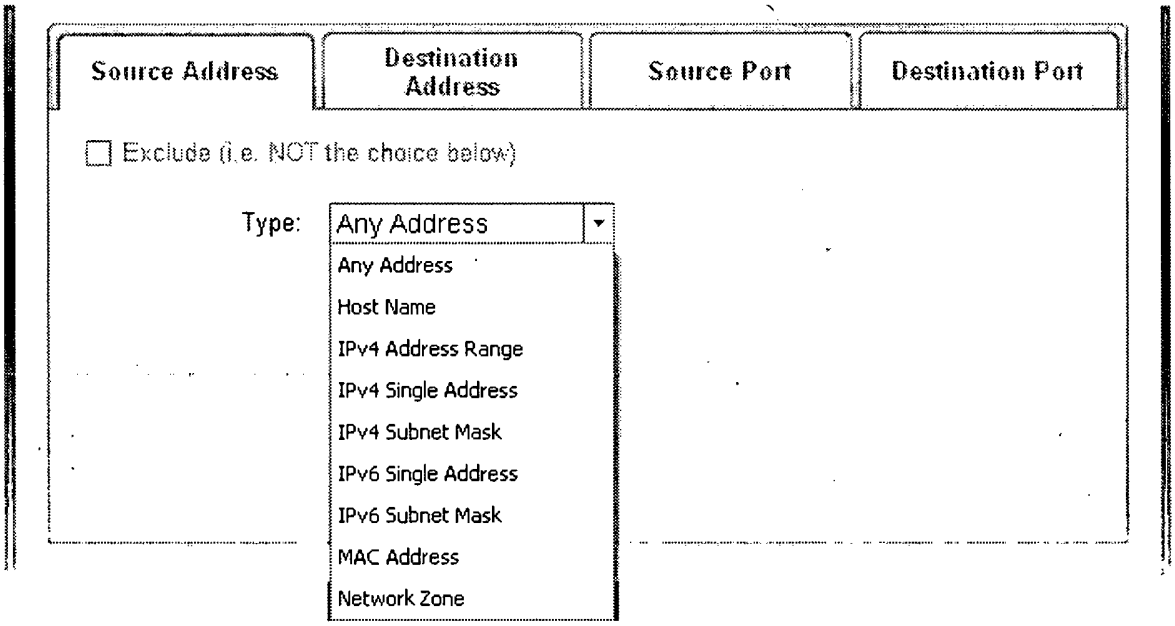
Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

- **Direction:** Allows the user to define which direction the packets should be traveling. Options available via the drop down menu are **'In', 'Out'** or **'In/Out' *(Default).***
- **Log as a firewall event if this rule is fired:** Checking this option creates an entry in the **firewall event log viewer** whenever this rule is called into operation. (i.e. when ALL conditions have been met) ***(Default = Disabled).***
- **Description**: Allows you to type a friendly name for the rule. Some users find it more intuitive to name a rule by it's intended purpose. ('Allow Outgoing HTTP requests'). If you create a friendly name, then this is displayed to represent instead of the full actions/conditions in the main **Application Rules interface** and the **Application Rule interface**.

Protocol

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

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



Source Address and Destination Address:

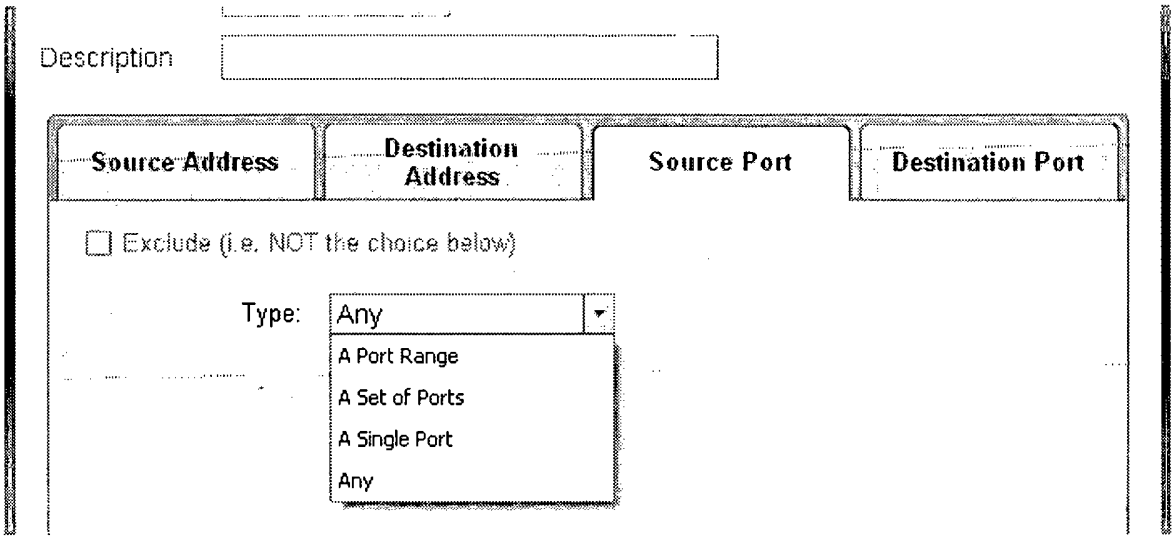
1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.
9. You can choose an entire network zone by selecting Zone .This menu defaults to Local Area Network. But you can also define your own zone by first creating a Zone through the '**Network Zones**' area.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable. For example, if you are creating an Allow rule and you check the Exclude box in the Source IP tab and enter values for the IP range, then that IP range is excluded. You have to create a separate Allow rule for the range of IP addresses that you DO want to use.

Source Port and Destination Port:

Enter the source and destination Port in the text box.

Best Available Copy



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

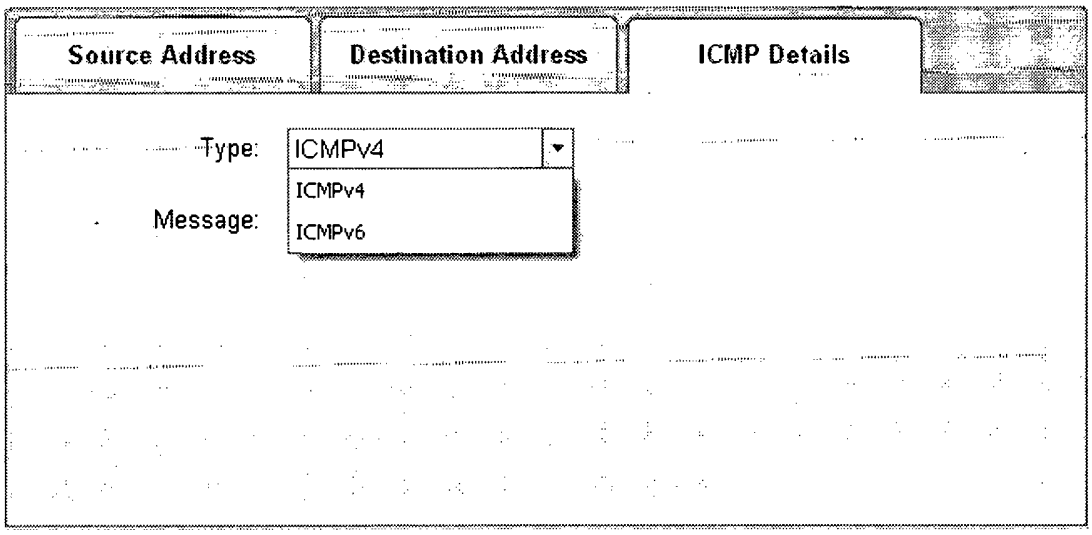
ii. **ICMP**

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

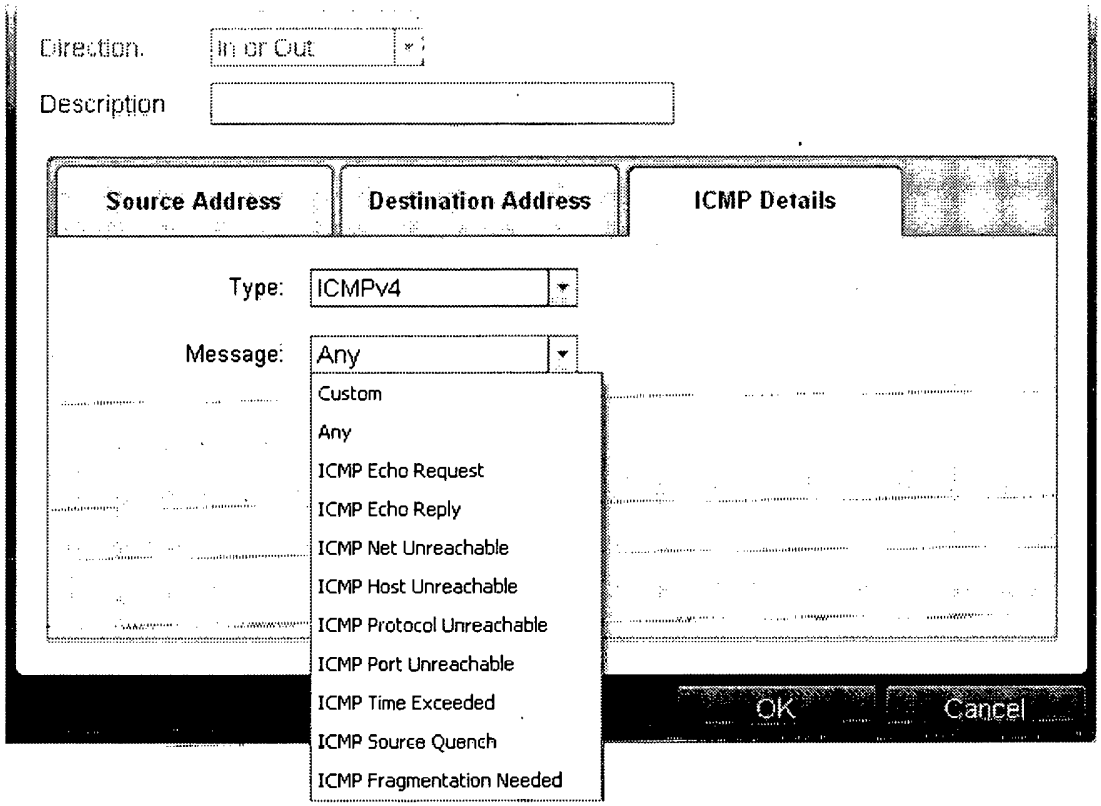
- **ICMP Details**

ICMP (Internet Control Message Protocol) packets contain error and control information which is used to announce network errors, network congestion, timeouts, and to assist in troubleshooting. It is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. So you can create rules to allow / block specific types of ping requests. With Comodo Firewall you can create rules to allow/ deny inbound ICMP packets that provide you with information and minimize security risk.

1. Type in the source/ destination IP address. Source IP is the IP address from which the traffic originated and destination IP is the IP address of the computer that is receiving packets of information.
2. Under the 'ICMP Details' tab, choose the ICMP version from the 'Type' drop-down.



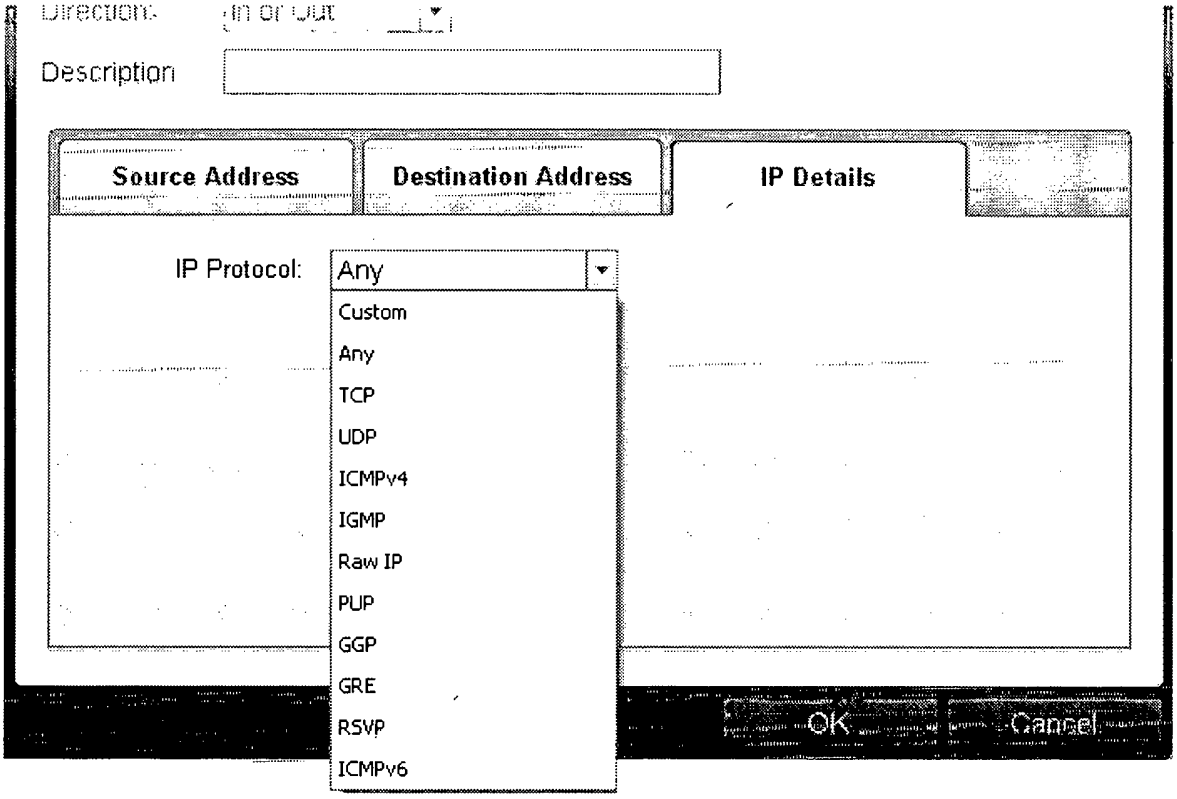
3. Specify ICMP Message , Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.



When you select a particular ICMP message , the menu defaults to set its code and type as well. If you select the ICMP message type 'Custom' then you are asked to specify the code and type.

iii. **IP**

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



- **IP Details**

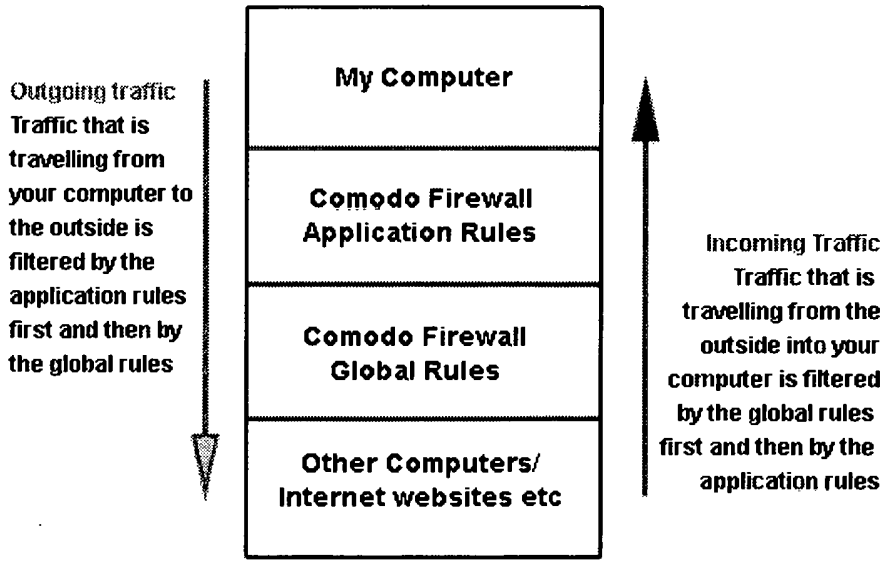
Select the types of IP protocol that you wish to allow, from the ones that are listed.

6.2.3.3. Global Rules

Unlike Application rules, which are applied to and triggered by traffic relating to a specific application, Global Rules are applied to all traffic traveling in and out of your computer.

Comodo Firewall analyzes every packet of data in and out of your PC using combination of Application and Global Rules.

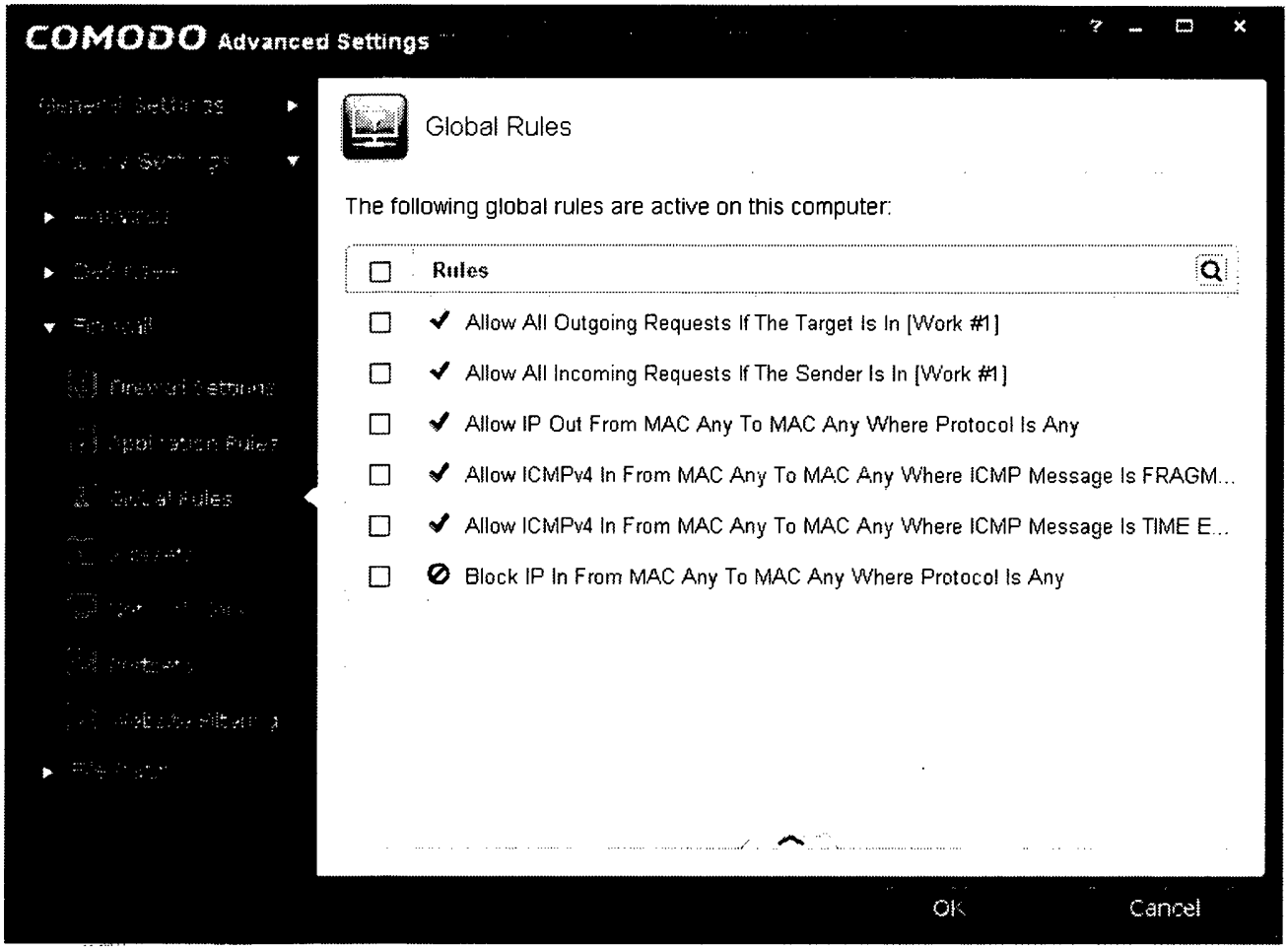
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.



Therefore, outgoing traffic has to 'pass' both the application rule then any global rules before it is allowed out of your system. Similarly, incoming traffic has to 'pass' any global rules first then application specific rules that may apply to the packet.

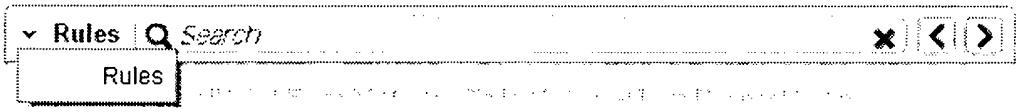
Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

- The Global Rules panel, accessible by clicking Security Settings > Firewall > Global rules tab from the Advanced tasks interface, allows you to view, add and manage the rules



You can use the search option to find a specific rule in the list.

To use the search option, click the search icon  at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

General Navigation:

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



- **Add** - Allows you to add a new global rule. See the section **'Adding and Editing a Firewall Rule'** for guidance on creating a new rule.
- **Edit** - Allows you to modify the selected global rule. See the section **'Adding and Editing a Firewall Rule'** for guidance on editing a new rule.
- **Remove** - Deletes the selected rule.
- **Purge** - Runs a system check to verify that all the applications for which rules are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

The configuration of Global Rules is identical to that for application rules. To add a global rule, click the 'Add...' button on the right. To edit an existing global rule, right click and select 'edit'.

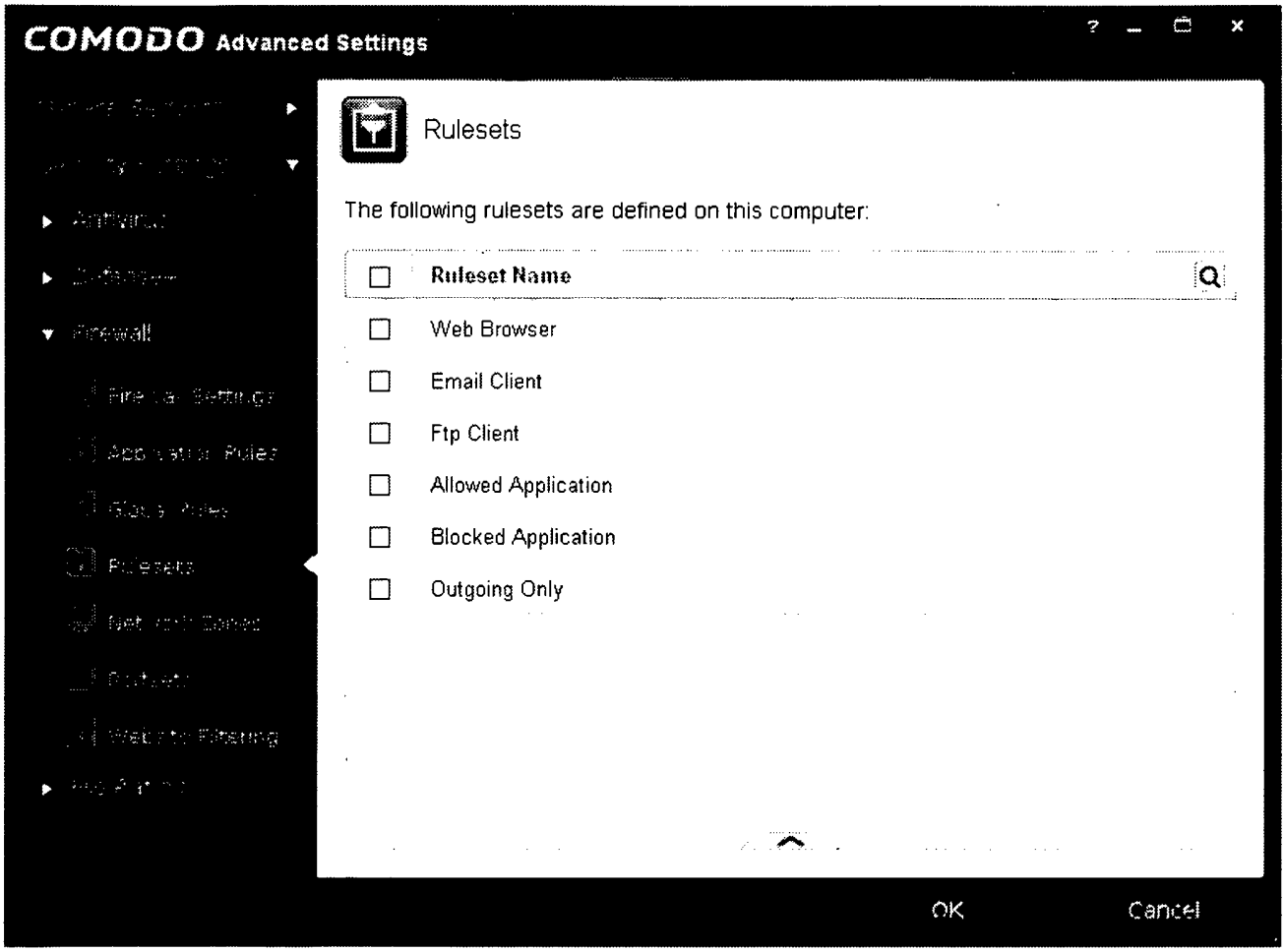
- See **Application Rules** for an introduction to the rule setting interface.
- See **Understanding Firewall Rules** for an overview of the meaning, construction and importance of individual rules.
- See **Adding and Editing a Firewall Rule** for an explanation of individual rule configuration.

6.2.3.4. Firewall Rule Sets

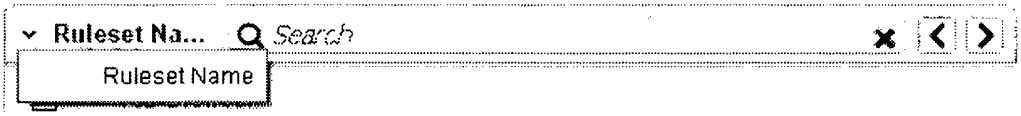
As the name suggests, a firewall Ruleset is a set of one or more individual Firewall rules that have been saved and which can be re-deployed on multiple applications. This section contains advice on the following:

- **Predefined Rulesets**
- **Creating a new ruleset**

The Predefined rulesets interface can be accessed by clicking Security Settings > Firewall > Rulesets from the 'Advanced Settings' interface.



You can use the search option to find a specific ruleset in the list by clicking the search icon at the far right in the column header.



- Enter the name of the item to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Predefined Rulesets

Although each application's firewall ruleset *could* be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to broad application category. For example, you may choose to apply the ruleset 'Web Browser' to the applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined policies to suit their environment and requirements. (for example, you may wish to keep the 'Web Browsers' name but wish to redefine the parameters of it rules).

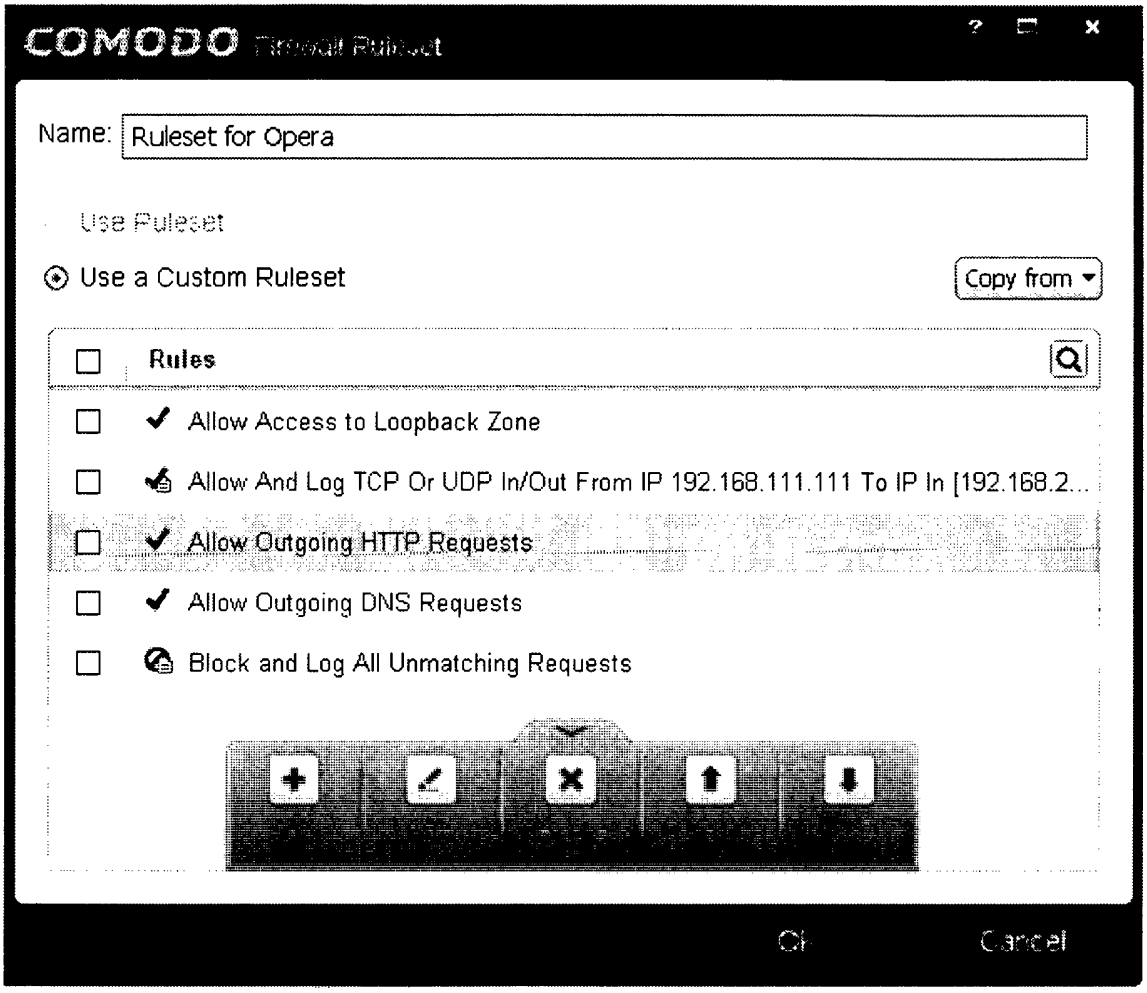
Creating a new ruleset

You can create new rulesets with network access control rules customized as per your requirements and can roll out them to

required applications while **creating Firewall ruleset** for the applications individually.

To add a new Ruleset

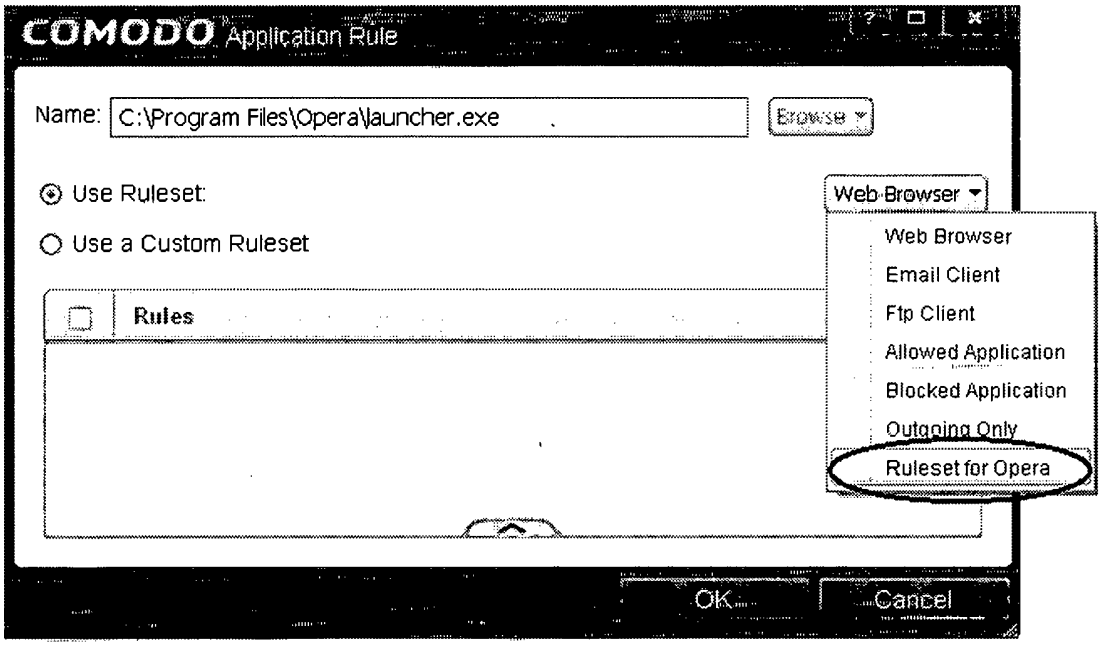
- Click the handle from the bottom center and select 'Add' from the options



- As this is a new ruleset, you need to name it in the text field at the top. It is advised that you choose a name that accurately describes the category/type of application you wish to define the ruleset for. Next you should add and configure the individual rules for this ruleset. See '**Adding and Editing a Firewall Rule**' for more advice on this.

Once created, this ruleset can be quickly called from 'Use Ruleset' when **creating or modifying a Firewall ruleset**.

Best Available Copy



To view or edit an existing predefined Ruleset

- Double click on the Ruleset Name in the list

  or

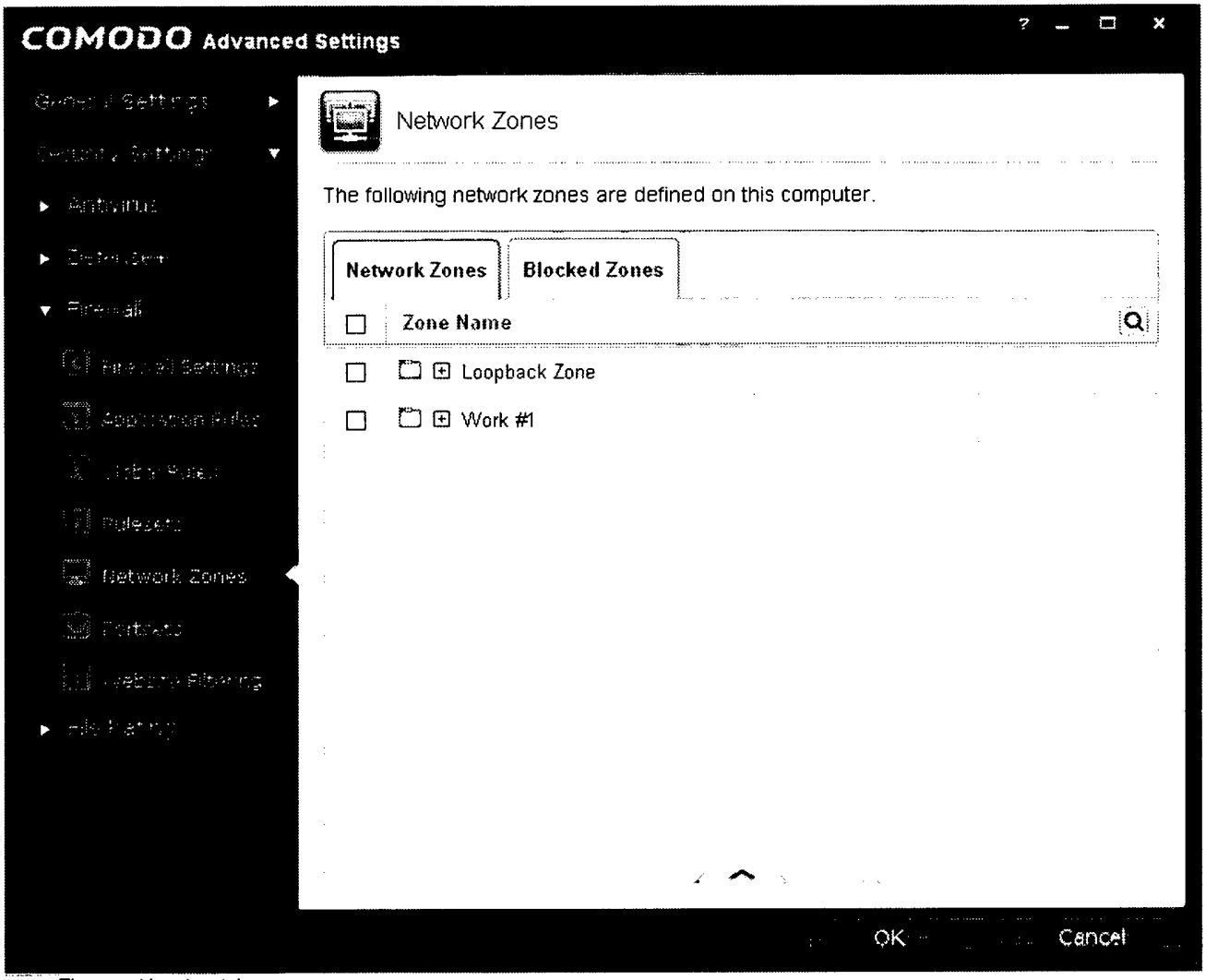
- Select the Ruleset Name, click the handle from the bottom center and select Edit from the options
- Details of the process from this point on can be found **here**.

6.2.3.5. Network Zones

The Network Zones panel allows you to:

- Define network zones that are trusted, and to specify access privileges to them
- Define network zones that are untrusted, and to block access to them

The Network Zones panel can be accessed by clicking Security Settings > Firewall > Network Zones from the 'Advanced Settings' interface.



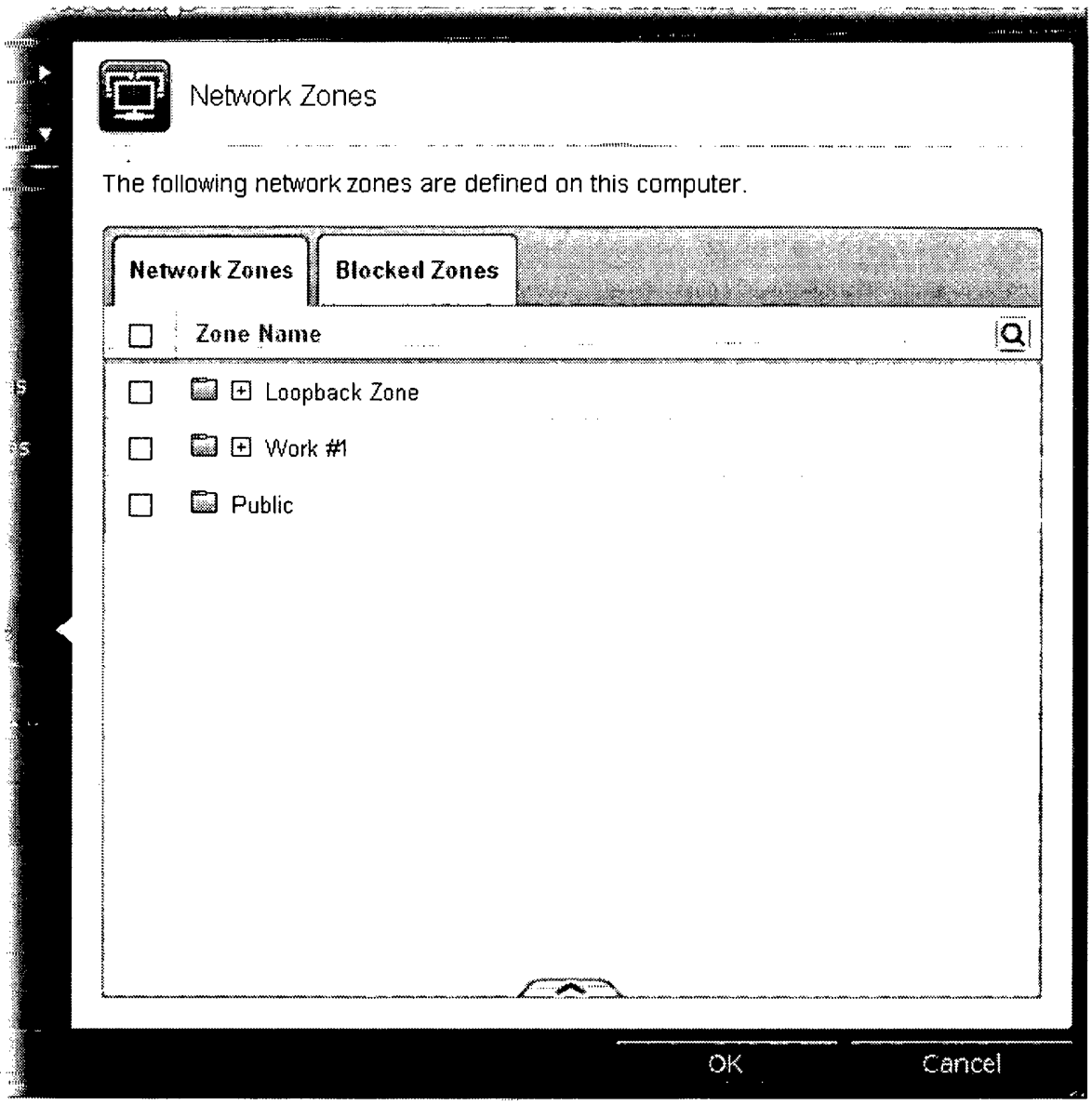
The panel has two tabs:

- **Network Zones** - Allows you to define network zones and to allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.
- **Blocked Zones** - Allows you to define trusted networks that are not trustworthy and to block access to them.

6.2.3.5.1. Network Zones

A 'Network Zone' can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied.

Background Note: A computer network is a connection between computers through a cable or some type of wireless connection. It enables users to share information and devices between computers and other users within the network. Obviously, there are certain computer networks where you need to grant access to, including your home or work network. Conversely, there may be other networks where you want to restrict communication with - or even block entirely.



Note 1: Adding a zone to this area does not, in itself, define any permission levels or access rights to the zone. This area allows to define the zones so you can quickly assign such permissions **in other areas of the firewall.**

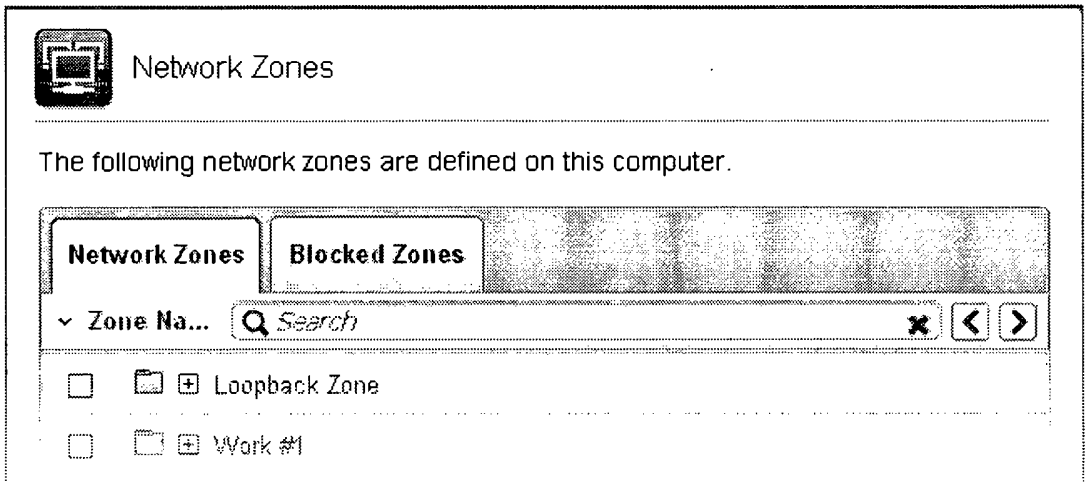
Note 2: A network zone can be designated as 'Trusted' and allowed access from the '**Manage Network Connections**' interface (An example would be your home computer or network).

Note 3: A network zone can be designated as 'Blocked' and denied access by using the '**Blocked Zones**' interface. (An example would be a known spyware site).

Note 4: An application can be assigned specific access rights to and from a network zone when defining an **Application Rule**. Similarly, a custom **Global Rule** can be assigned to a network zone to all activity from a zone.

Note 5: By default, Comodo Firewall automatically detects any new networks (LAN, Wireless etc) once you connect to them. This can be disabled by deselecting the option 'Enable automatic detection of private networks' in the **Firewall Settings** panel.

You can use the search option to find a network zone in the list by clicking the search icon at the far right in the column header.



- Enter the name of the item to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

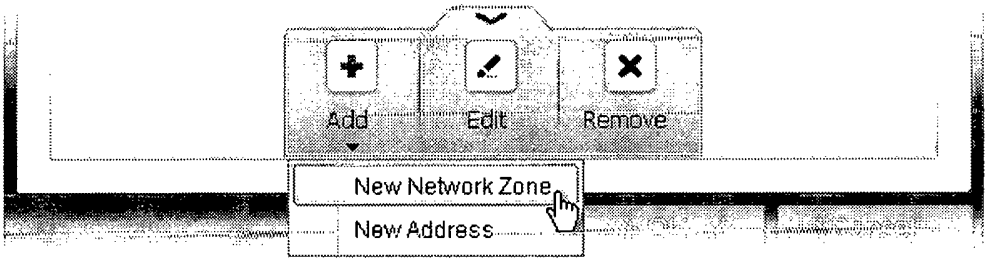
Defining a new Network Zone

To add a new network zone:

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

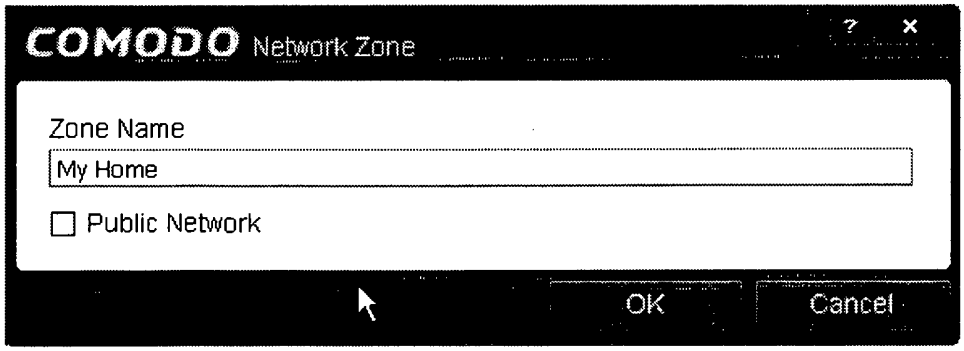
Step 1 - Define a name for the zone

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



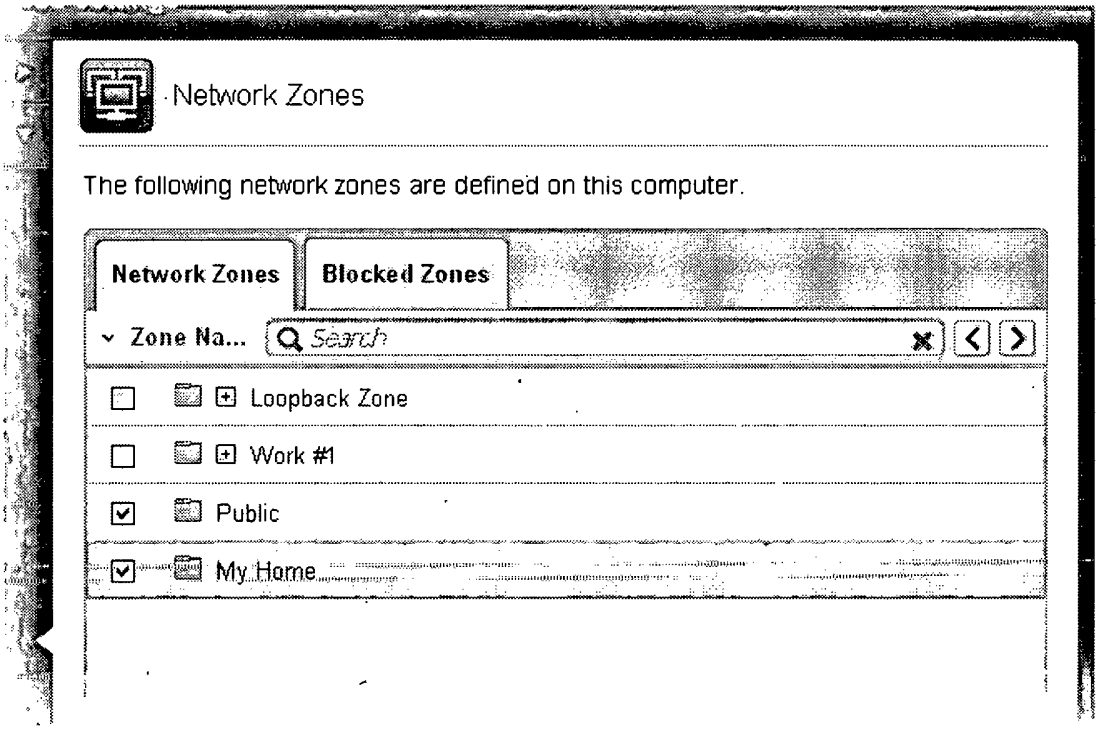
A dialog box will appear, prompting you to specify a name for the new zone.

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



3. Select the checkbox 'Public Network' if you are defining a network zone for a network in a public place, for example, when you are connecting to a Wi-Fi network at an airport, restaurant etc., so that Comodo Firewall will optimize the configuration accordingly.
4. Click 'Apply' to confirm your zone name.

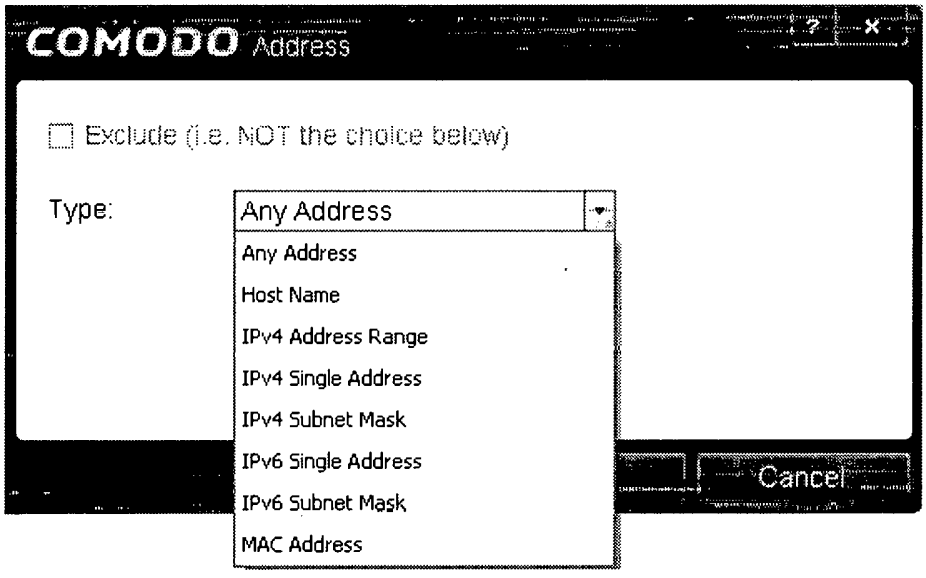
   This adds the name of your new zone to the Network Zones list.



Step 2 - Select the addresses to be included in this zone

1. Select the network name, click the handle at the bottom center and choose 'Add' > 'New Address' from the options or click the + button beside the new network zone name and double click on '(add addresses here)'

   The 'Address' dialog allows you to select an address from the Type drop-down box shown below ***(Default = Any Address)***. The Exclude check box will be enabled only if any other choice is selected from the drop-down box.



Select Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.
4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

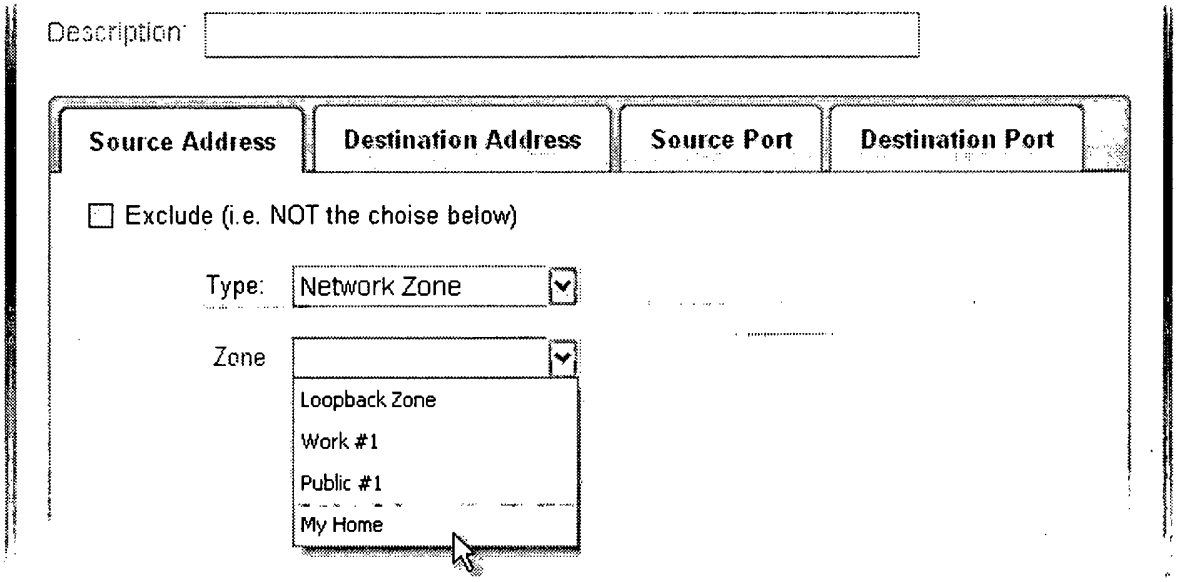
- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

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

The new zone now appears in the main list along with the addresses you assigned to it.

Once created, a network zone can be:

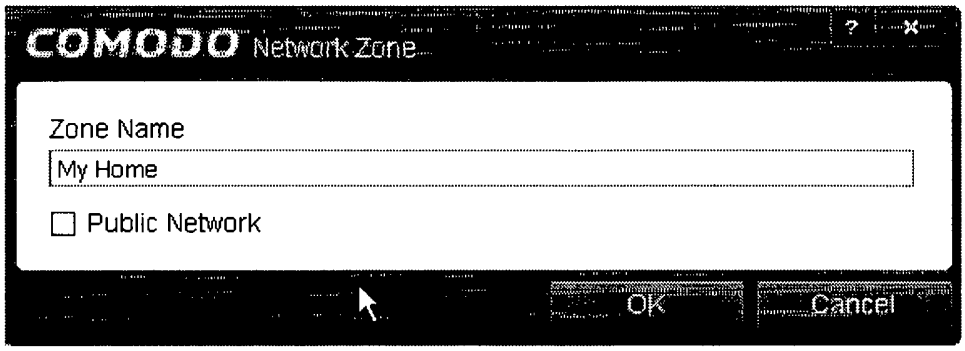
- Quickly called as 'Zone' when **creating or modifying a Firewall Ruleset**



- Quickly called and designated as a blocked zone from the '**Blocked Zones**' interface

To edit the name of an existing Network Zone

1. Select the name of the zone in the list (e.g. My Home), click the handle at the bottom center and choose 'Edit' from the options or double click on the network zone name.



2. Edit the name of the zone.

To add more addresses to an existing Network Zone

- Select the network name, click the handle at the bottom center and choose 'Add > A new Address' from the options
- Add new address from the **'Address' interface**.

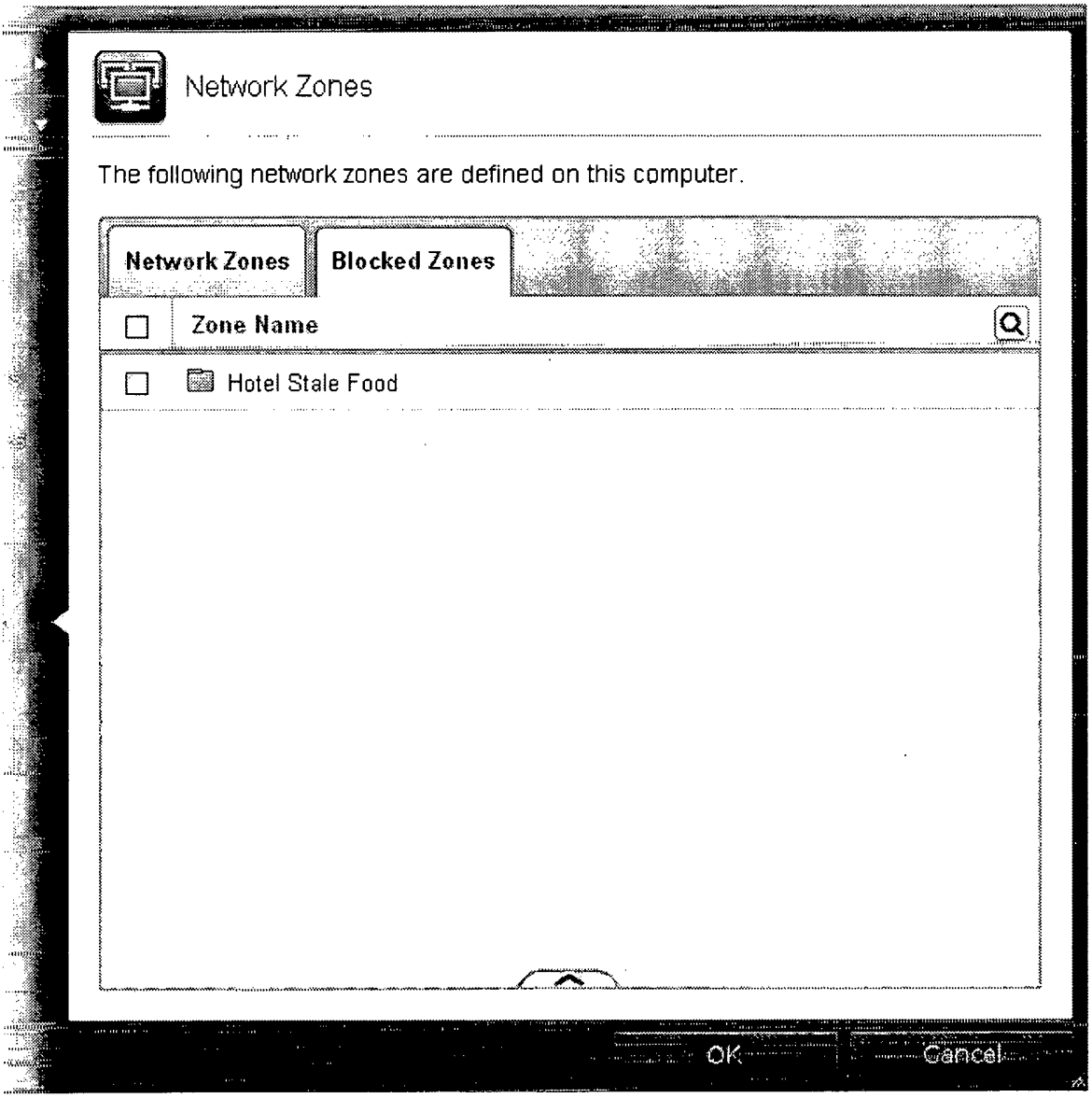
To modify or change the existing address in a zone

- Click the + button beside the network zone name to expand the addresses
- Double click on the address to be edited or select the address, click the handle from the bottom center and choose Edit from the options
- Edit the address from the **'Address' interface**.

6.2.3.5.2. Blocked Zones

A computer network enables users to share information and devices between computers and other users within the network. Obviously, there are certain computer networks that you need to 'trust' and grant access to - for example your home or work network. Unfortunately, there may be other, untrustworthy networks that you want to restrict communication with - or even block entirely.

Note: We advise new or inexperienced users to first read **'Network Zones'** , **'Stealth Ports Wizard'** and **'Application Rules'** before blocking zones using this interface.



The 'Blocked Network Zones' tab allows you to:

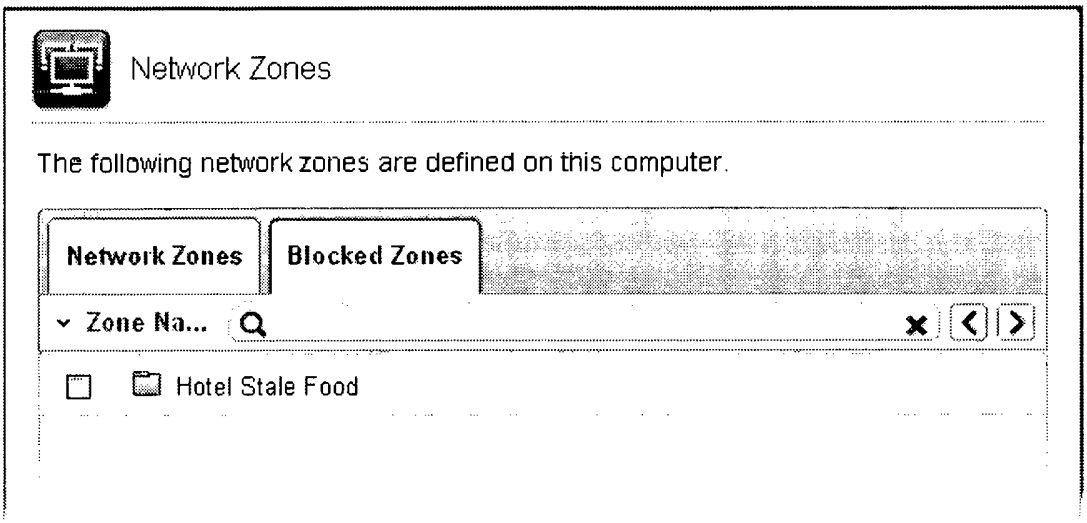
- **Deny access to a specific network by selecting a pre-existing network zone and designating it as blocked**
- **Deny access to a specific network by manually defining a new blocked zone**

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

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

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

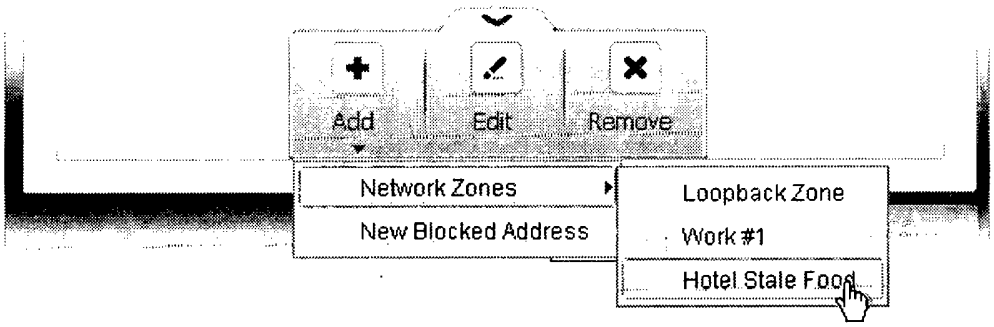
You can use the search option to find a blocked zone in the list by clicking the search icon at the far right in the column header.



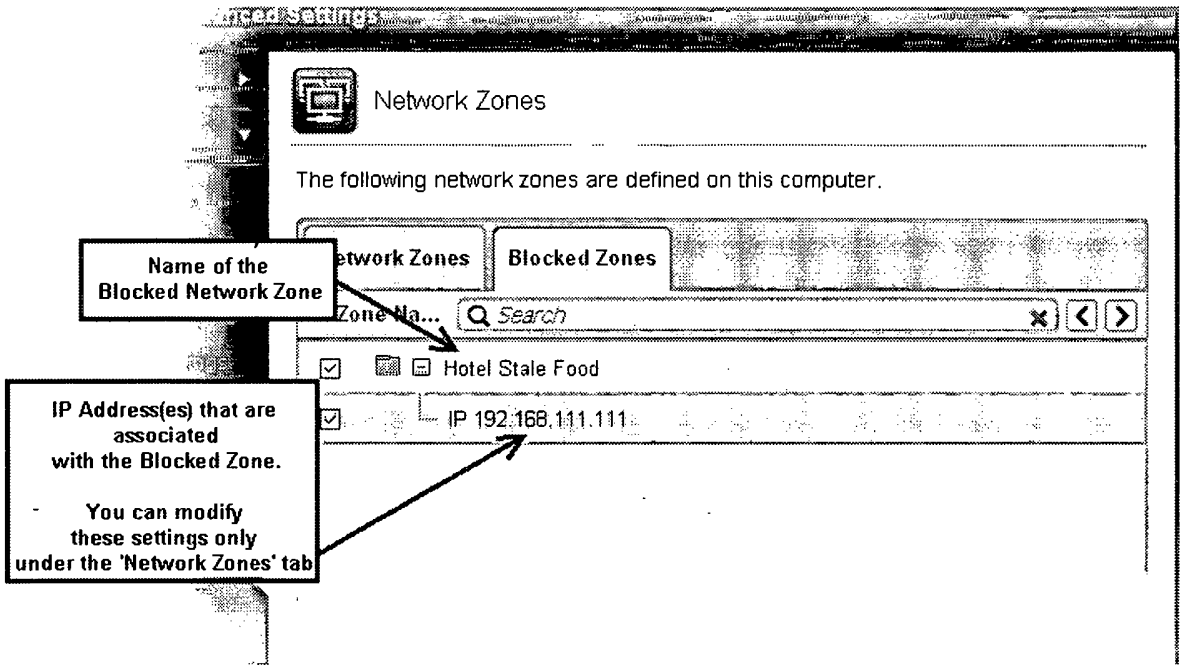
- Enter the name of the zone to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

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

1. Click the handle from the bottom center and choose 'Add' > 'Network Zones' from the options
2. Select the particular zone you wish to block.



The selected zone will appear in the 'Blocked Zones' interface.

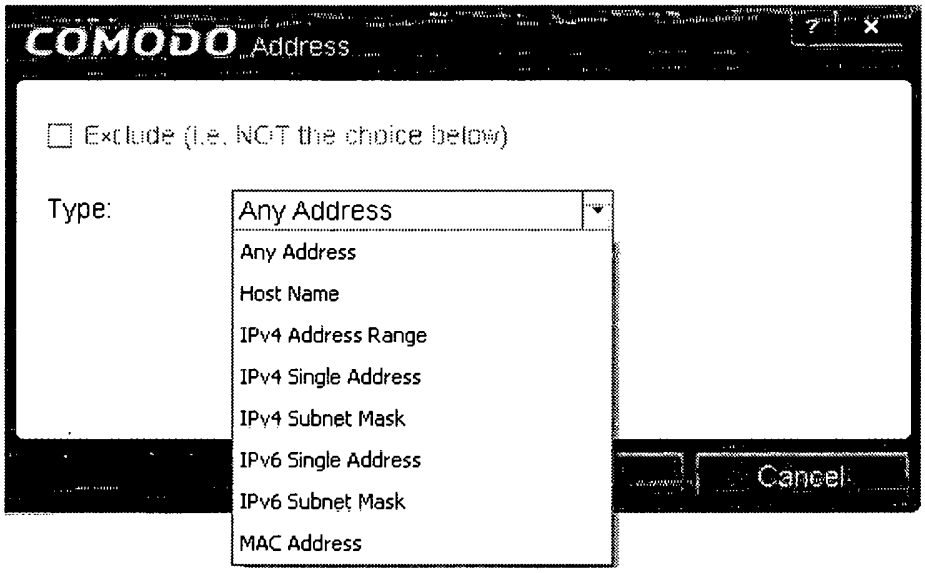


3. Click 'OK' to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

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

1. Click the handle from the bottom center and choose 'Add' > 'New Blocked Address' from the options.

The Address dialog will appear. The 'Address' dialog allows you to select an address from the Type drop-down box shown below ***(Default = Any Address)***.



Select Address:

1. You can choose any IP Address by selecting Any Address in the Type drop-down box. This menu defaults to an IP range of 0.0.0.0- 255.255.255.255 to allow connection from all IP addresses.
2. You can choose a named host by selecting a Host Name which denotes your IP address.
3. You can choose an IPv4 Range by selecting IPv4 Address Range - for example the range in your private network and entering the IP addresses in the Start Range and End Range text boxes.

4. You can choose a Single IPv4 address by selecting IPv4 Single Address and entering the IP address in the IP address text box, e.g., 192.168.200.113.
5. You can choose IPv4 Mask by selecting IPv4 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
6. You can choose a Single IPv6 address by selecting IPv6 Single Address and entering the IP address in the IP address text box, e.g., 3ffe:1900:4545:3:200:f8ff:fe21:67cf.
7. You can choose IPv6 Mask by selecting IPv6 Subnet Mask. IP networks can be divided into smaller networks called sub-networks (or subnets). An IP address/ Mask is a subnet defined by IP address and mask of the network. Enter the IP address and Mask of the network.
8. You can choose a MAC Address by selecting MAC Address and entering the address in the address text box.

- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

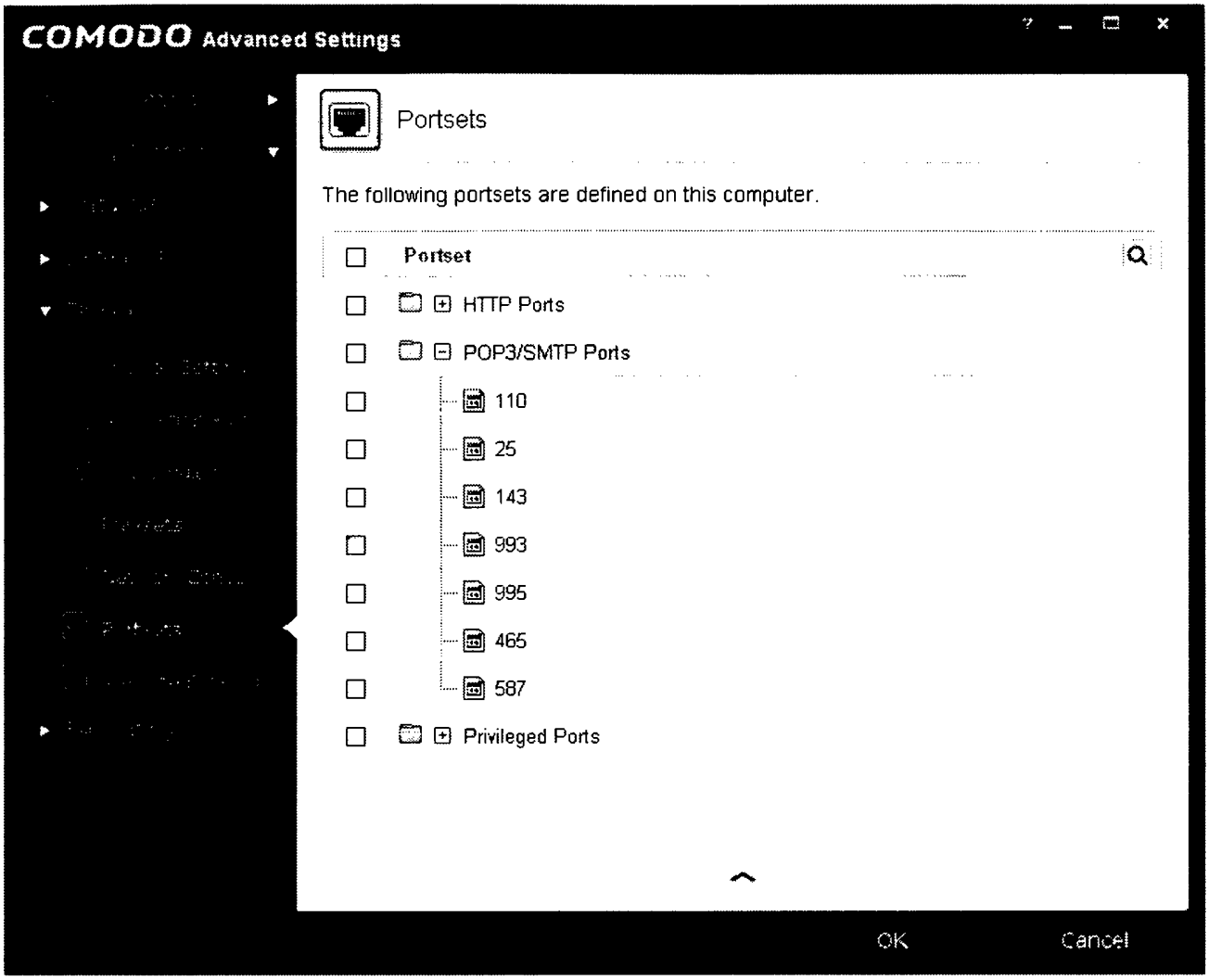
2. Select the address to be blocked and click OK

   The address(es) you blocked will appear under the 'Blocked Zones' tab. You can modify these addresses at any time by selecting the entry and clicking 'Edit'.
3. Click 'OK' in 'Network Zones' interface to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

6.2.3.6. Port Sets

Port Sets are handy, predefined groupings of one or more ports that can be re-used and deployed across multiple **Application Rules** and **Global Rules**.

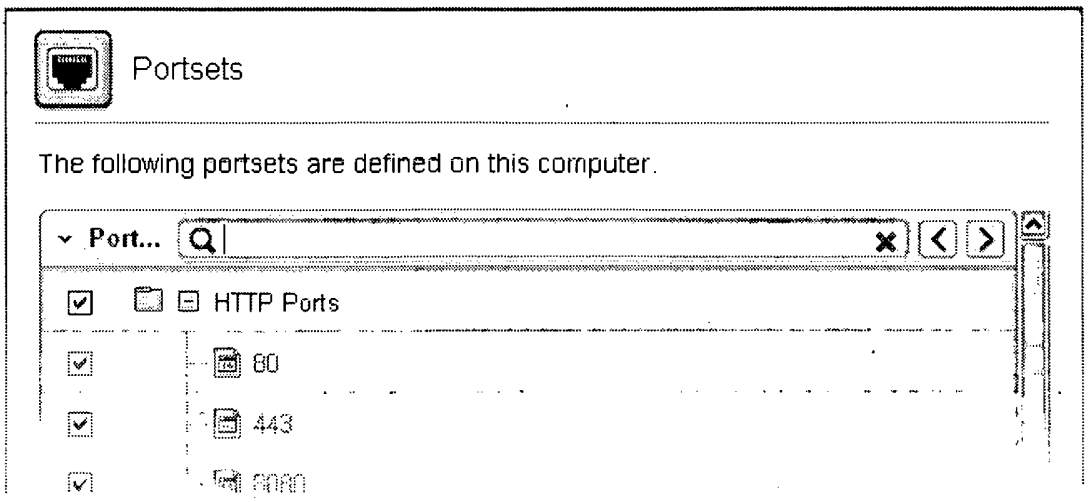
- The Port Sets panel enables you to view and manage pre-defined port sets and t add new port sets
- The Port Sets panel can be accessed by clicking Security Settings > Firewall > Portsets from the Advanced Tasks interface



The Port Sets are displayed as a tree structure. Clicking the + button beside the port set name expand the list of ports defined in it. The default port sets shipped with Comodo Internet Security are:

- **HTTP Ports**: 80, 443 and 8080. These are the default ports for http traffic. Your Internet browser uses this ports to connect to the Internet and other networks.
- **POP3/SMTP Ports**: 110, 25, 143, 995, 465 and 587. These are the ports that are typically used by mail clients like Outlook Express and WinMail for communication using the POP3, SMTP and IMAP protocols.
- **Privileged Ports:** 0-1023. This set can be deployed if you wish to create a rule that allows or blocks access to the privileged port range of 0-1023. Privileged ports are so called because it is usually desirable to prevent users from running services on these ports. Network admins usually reserve or prohibit the use of these ports.

You can use the search option to find a specific port set in the list by clicking the search icon at the far right in the column header.



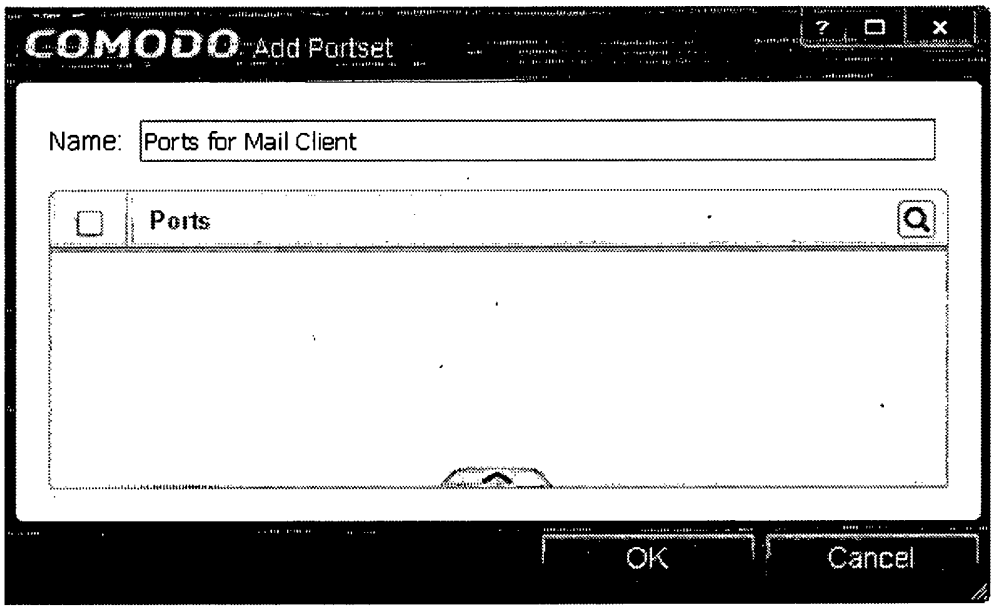
- Enter the name of the port set to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

Defining a new Port Set

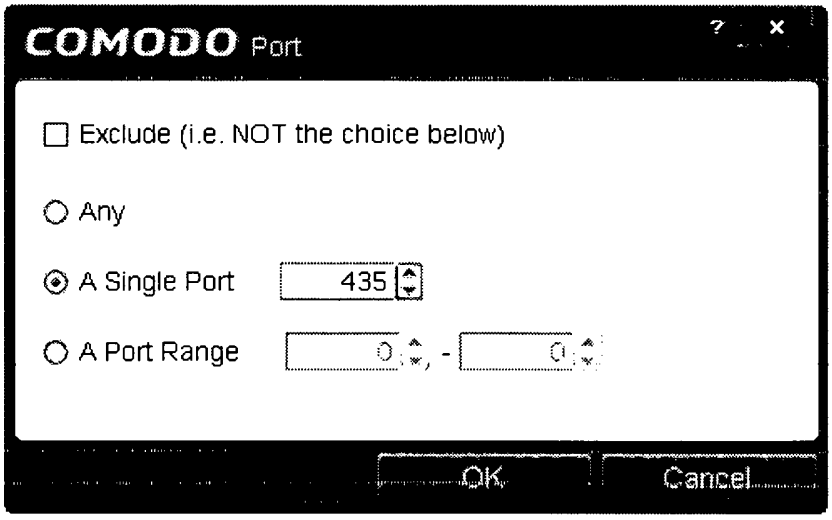
You can create new portsets and allow access to them for applications, with the access privileges specified through **Application Rule** interface. Refer to '**Creating or Modifying Firewall Rules**' for more details.

To add a new portset

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



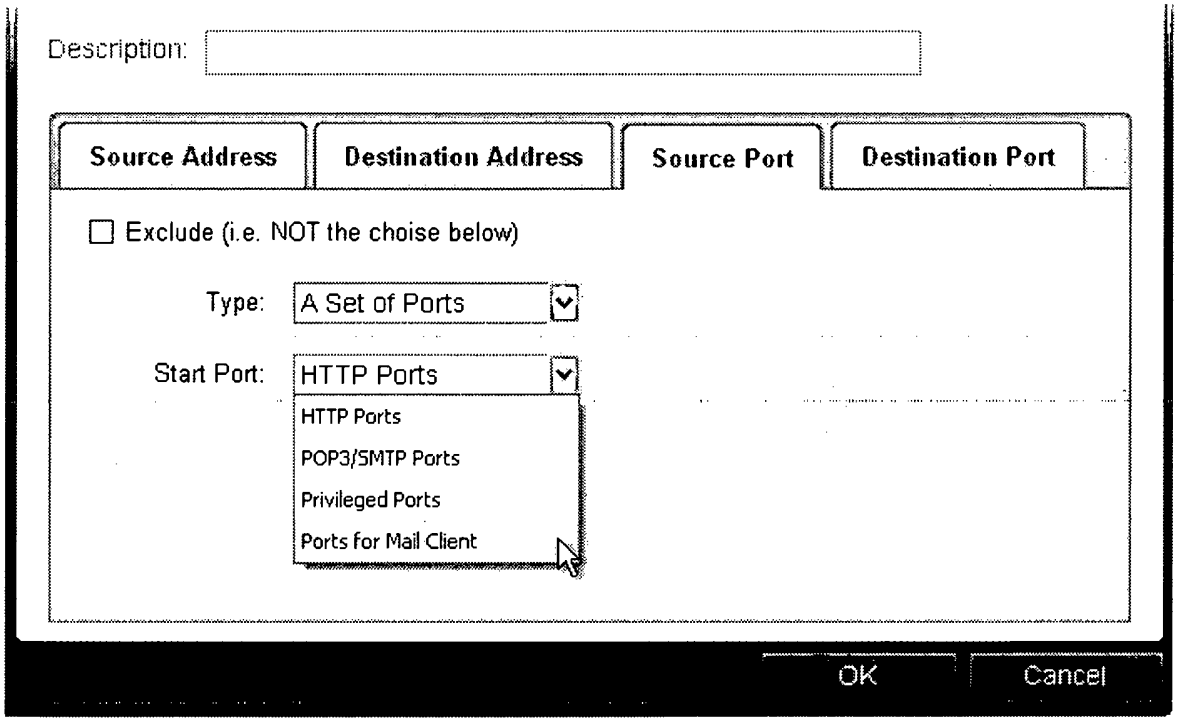
2. Enter a name for the new portset in the Name field.
3. To add ports to the new portset, click the handle from the bottom center and choose 'Add' from the options.



4. Specify the ports to be included in the new portset:
    - **Any -** to choose all ports;
    - **A single port -** Define the port number in the combo box beside;
    - **A port range** - Enter the start and end port numbers in the respective combo boxes.
    - Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.
5. Click 'OK' in the 'Port' dialog. The ports will be added to the new portset in the 'Edit Portset' interface.
6. Click 'OK' in the 'Edit Portsets' interface to create the new portset.

    Once created, a Portset can be:

    - Quickly called as 'A Set of Ports' when **creating or modifying a Firewall Ruleset**



To edit an existing port set

- Select the portset from the 'Portsets' interface, click the handle from the bottom center and select the 'Edit' from the options to bring up the 'Edit Portset' dialog.

- The editing procedure is similar to **adding the portset** explained above.

6.2.3.7. Website Filtering

The Website filtering section allows you to set up rules to allow or block access to specific websites. Rules can be created for particular users of your computer, which makes this feature very useful for both home and work environments. For example, parents can block juvenile users from visiting inappropriate websites while companies can prevent employees from visiting social networking sites during working hours. You also have the option to create a log event whenever a user tries to visit a website which is in conflict with a rule.

The Website Filtering panel can be accessed by clicking Security Settings > Firewall > Website Filtering tab from 'Advanced Settings' interface.



Brief overview:

- Rules are constructed from one or more 'categories'.
- A category is a collection of one or more 'Websites'
- A 'Website' can be specified with its full URL or part of URL with wildcard character (*)
- You must set a rule to be 'Allow', 'Block' or 'Ask' and must specify to which users it should apply.

CIS ships with four preset categories of Websites which can be added to rules that you create. Three of these are non-modifiable lists which are managed by Comodo. These are 'Comodo Safe category', 'Comodo Phishing category' and 'Comodo Malware category'. The fourth preset, 'Exclusions', is empty by default but allows you to specify websites that should be allowed. You should add URLs to the 'Exclusions' category over time if you find you require access to a website which is blocked by a category.

CIS also ships with two predefined rules, 'Allowed Sites' and 'Blocked sites', both of which are modifiable. If switched on, the 'Blocked sites' rule will proactively block access to websites in the 'Comodo defined Malware sites' and 'Comodo defined Phishing Sites' categories. If you wish, you can add other categories to this rule to expand its coverage. The 'Allowed Sites' rule will permit access to websites in the Comodo 'Safe Sites' category and 'Exclusions' categories.

To set up a new rule of your own, click the 'Rules' tab, click 'Add', name your rule, add categories to the rule, specify to which users it should apply and whether it should be 'Allow', 'Block' or 'Ask'.

The 'Website Filtering' panel has two tabs:

- **Rules** - Allows you to define Website Filtering Rules and assign to required users. Refer to the section '**Creating or Modifying Website Filtering Rules**' for more details.
- **Categories** - Allows you to define categories of Websites to be allowed or blocked in Website filtering rules. Refer to the section '**Defining or Modifying Website Categories**' for more details.

General Advice:

- It is the 'Categories' section where you specify the website(s) you wish to block or allow, not the 'Rules' section. A rule is mainly for specifying the user(s) for whom a category of URLs should be filtered and whether those categories should be allowed or blocked.
- When creating a new rule, you will be required to specify which categories should be included. You can elect to use just the pre-defined Comodo categories but, if you wish to filter specific websites, you will need to create your own category.
- For example, if you wanted to create a category to block youtube.com and certain other leisure websites, you would *click 'Categories' > 'Add Category' > Type name for category > Select your new category in list > 'Add Website' > Type www.youtube.com. Click 'Add Website' again to add more sites.* You will now be able to select this category when creating a rule for a user(s).
- Refer to the section '**Defining or Modifying Website Categories**' for more details on specifying Website categories.

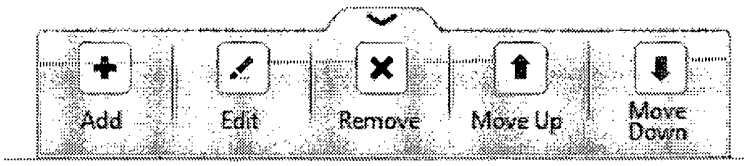
6.2.3.7.1. Creating and Modifying Website Filtering Rules

The 'Rules' tab allows you to create, view, edit and specify exclusions to your website filtering rules. The powerful rule-configuration interface lets you create rules which are as sweeping or as granular as you require. Rules can be created on a per-user basis, allowing you to control exactly which websites certain people can or cannot visit. You can also disable or enable a rule as required at any time.

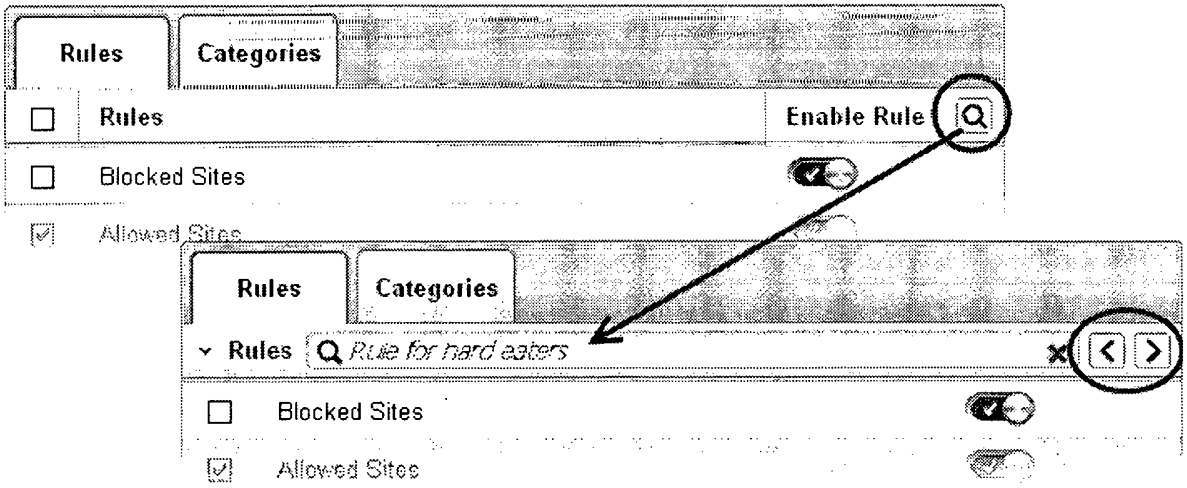
Comodo Firewall implements rules for the currently logged-in user based on the order they are in this list. Should a conflict exist between individual rules, then the rules at the top takes priority. Click the handle and use the 'Move Up' or 'Move Down' buttons to change a rule's priority.



- The switches in the 'Enable Rule' column enable you to quickly turn a rule on or off
- The check-boxes next to a rule name allow you to select it for editing, removing or re-prioritizing using the controls at the bottom of the interface:



You can search for a specific rule by clicking the search icon at the far right in the column header.



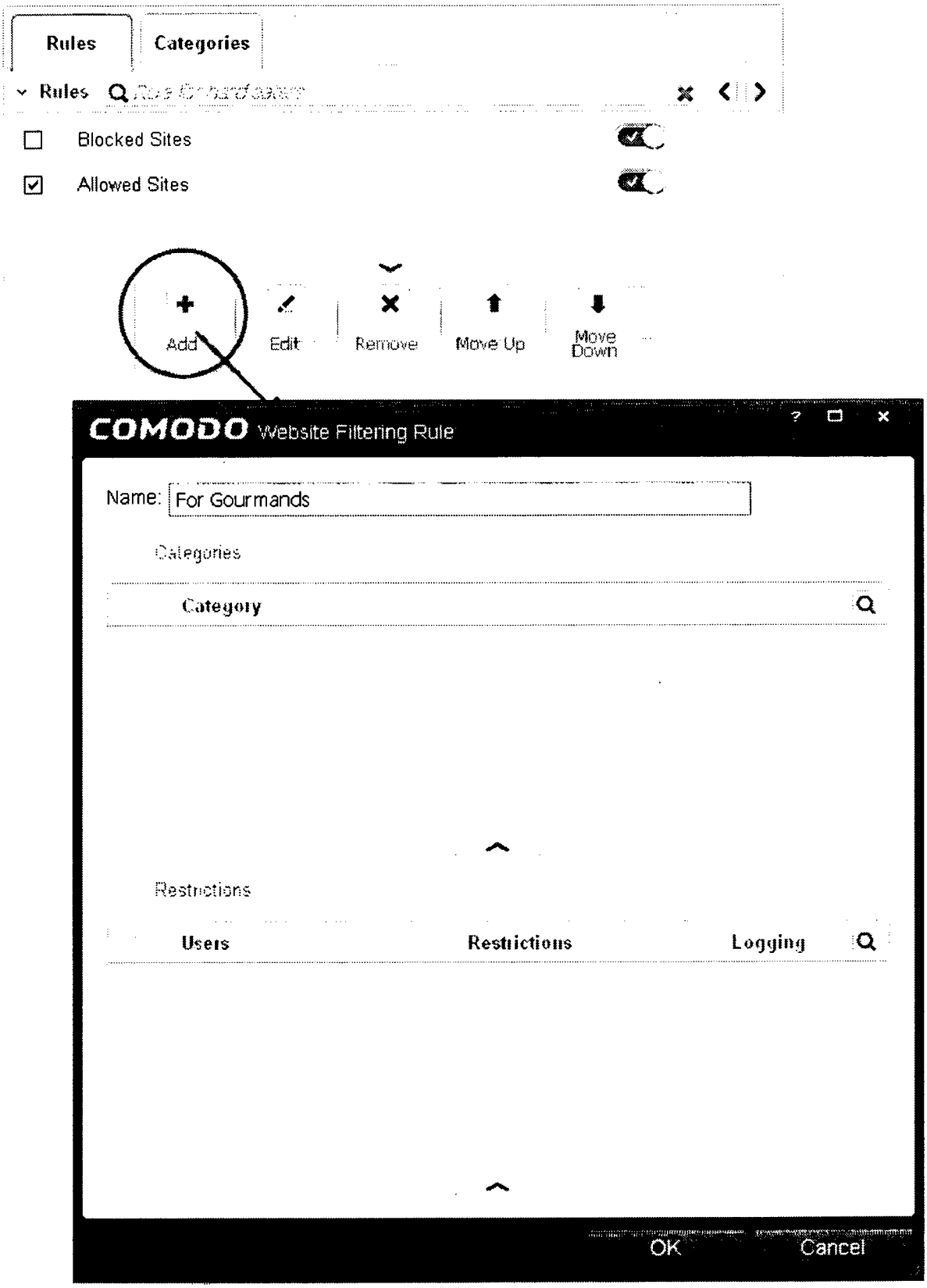
- Enter full or part of the name of the rule in the search field.
- Click the right or left arrow at the far right to begin the search.
- Click the ✖ icon in the search field to close the search option.

The Rules interface allows you to:

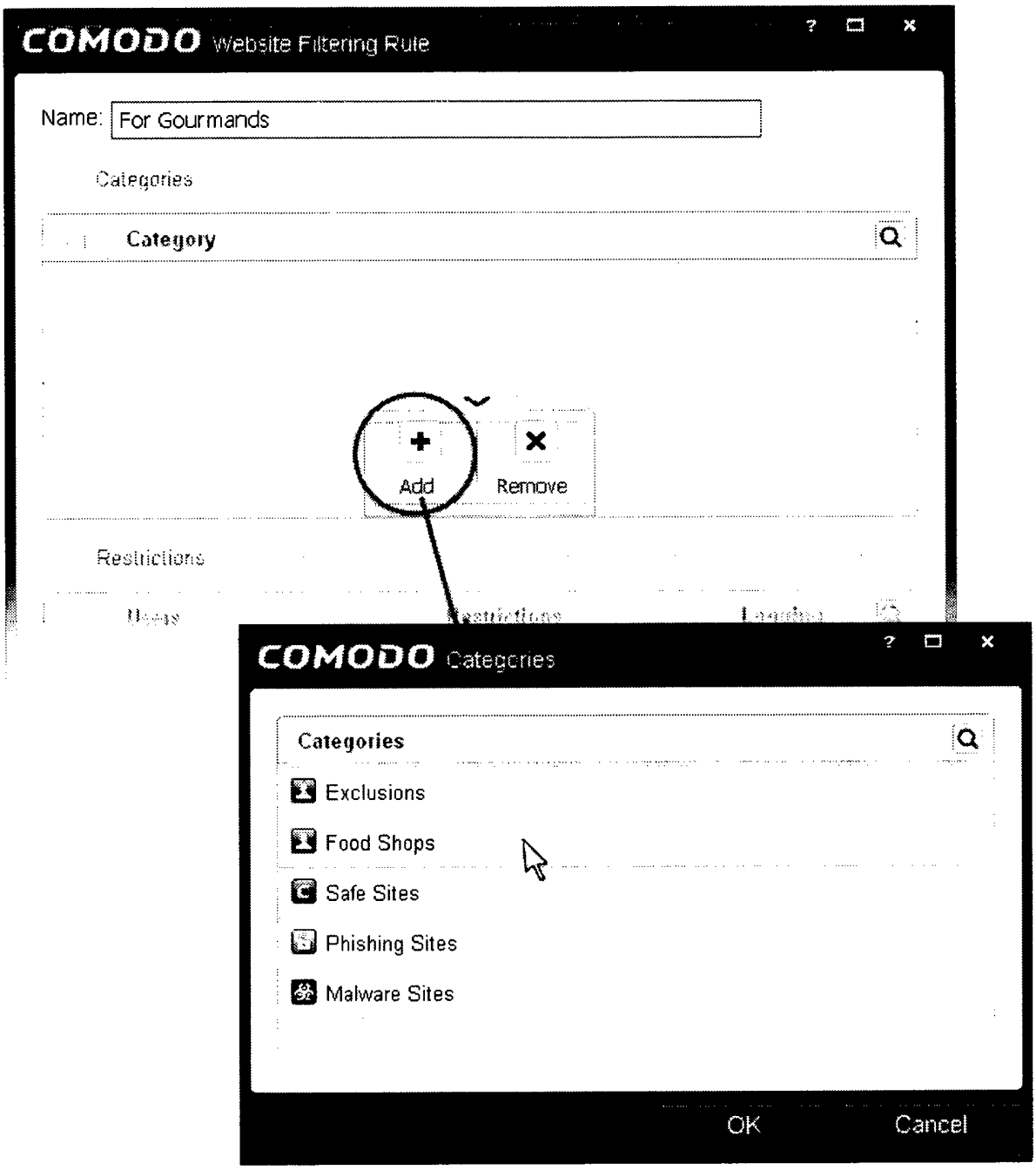
- **Create new Website filtering Rules**
- **Edit existing rules**
- **Change priority of the rules**
- **Remove unwanted rules**

To create a new Website Filtering rule

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' from the 'Advanced Settings' interface.
2. Click the handle at the bottom of the Rules interface and select 'Add':



3. Enter a name for your new filter.
4. Select the categories that should be added to the filter:
    - Click the handle at the bottom of the 'Category' pane and choose 'Add'.



Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

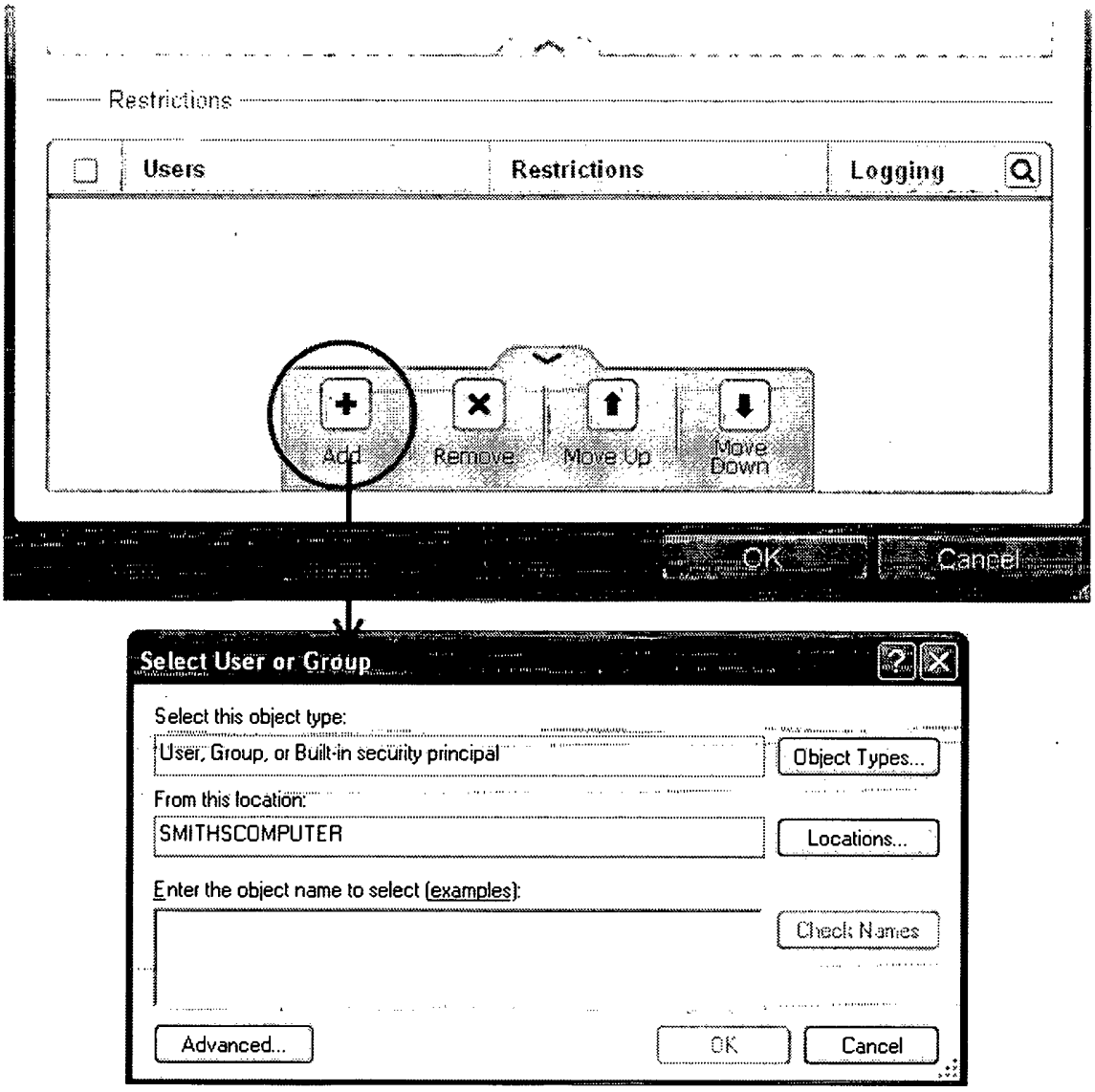
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Comodo Safe Sites** - Websites that are considered safe according to global whitelist
- **Comodo Phishing Sites** - Websites that lead to phishing websites, as per dynamically updated Comodo Blacklist
- **Comodo Malware Sites** - Websites that may inject malware into your system, as per dynamically updated Comodo Blacklist

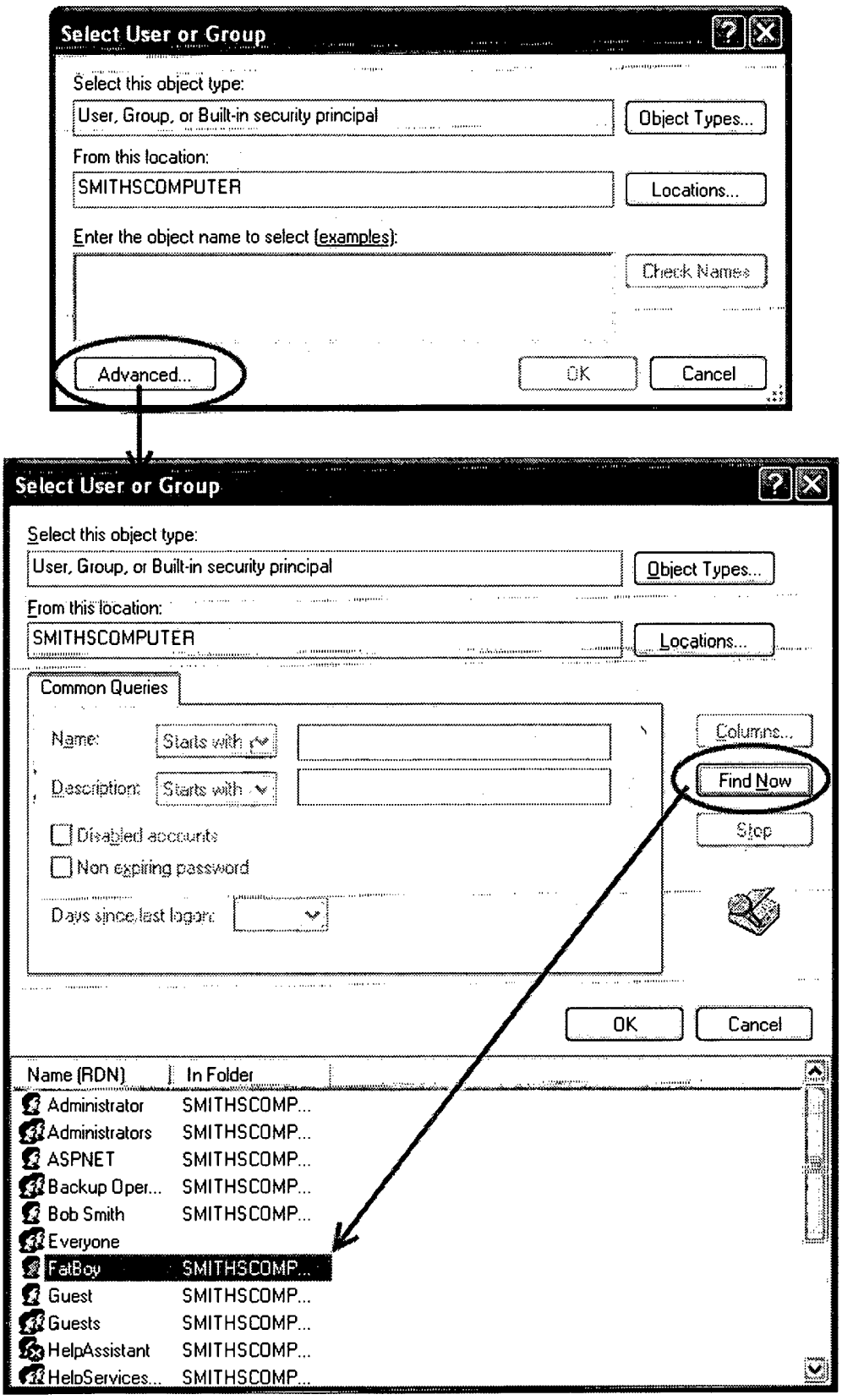
For more details on creating and modifying user specified categories, Refer to the section **Defining or Modifying Website Categories**

5. Add Users or User Groups to whom the rule should be applied:

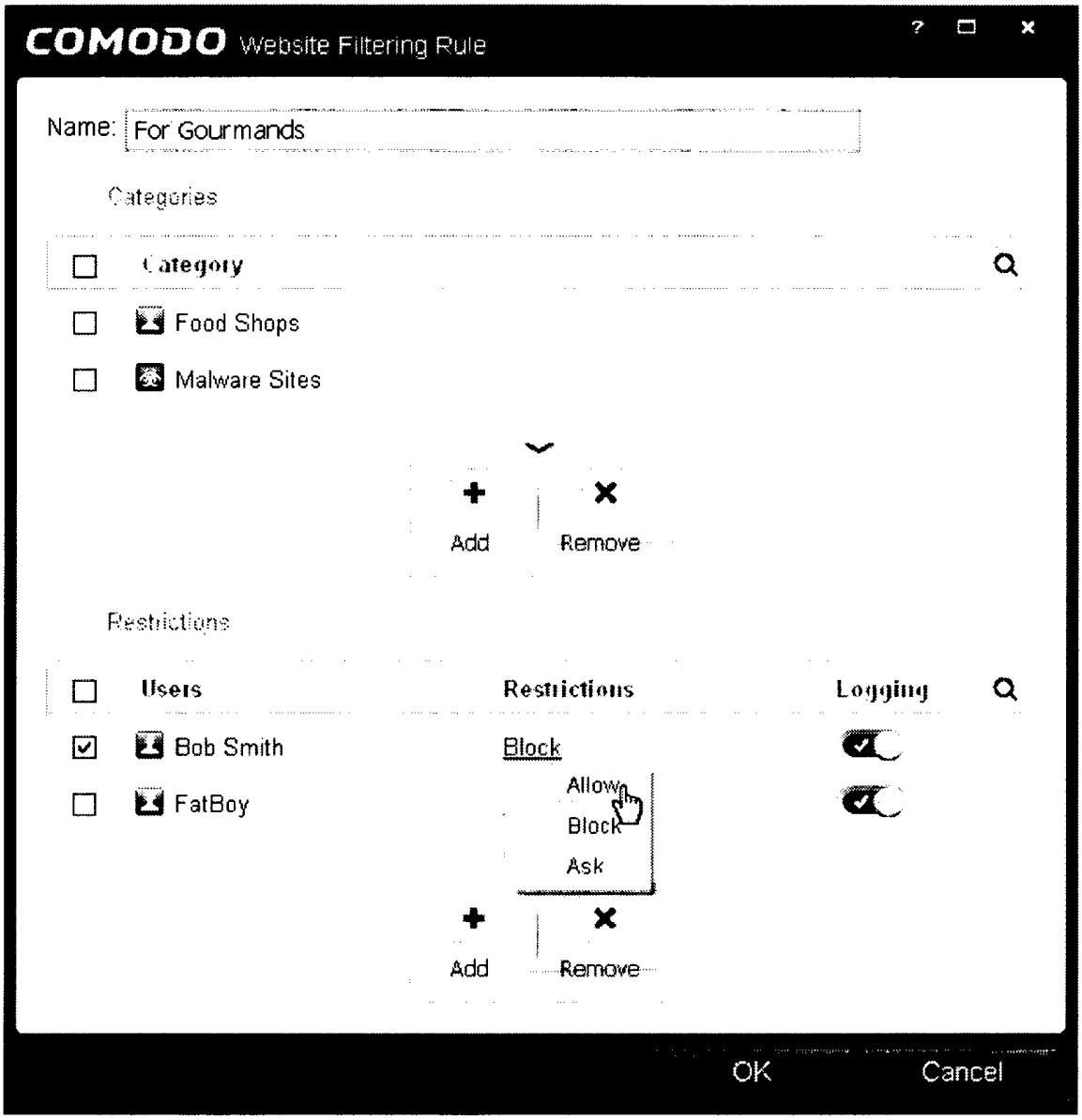
- Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:



- Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format <domain name>\<user/group name> or <user/group name>@<domain name>. Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.


Select User or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
SMITHSCOMPUTER
Locations...
Enter the object name to select (examples):
Check Names
Advanced...
OK
Cancel
Select User or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
SMITHSCOMPUTER
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Name (RDN)
In Folder
Administrator SMITHSCOMP...
Administrators SMITHSCOMP...
ASPNET SMITHSCOMP...
Backup Oper... SMITHSCOMP...
Bob Smith SMITHSCOMP...
Everyone
FatBoy SMITHSCOMP...
Guest SMITHSCOMP...
Guests SMITHSCOMP...
HelpAssistant SMITHSCOMP...
HelpServices... SMITHSCOMP...

After adding target users or groups, you next need to specify whether those users should be allowed or blocked from viewing the websites in the category or they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:



- **Allow** - The websites in the categories can be accessed by the user.
- **Block** - The websites in the categories cannot be accessed by the user.
- **Ask** - An alert will be displayed in the browser (shown below) if the user tries to access any of the websites in the category. The user can decide whether or not to continue.



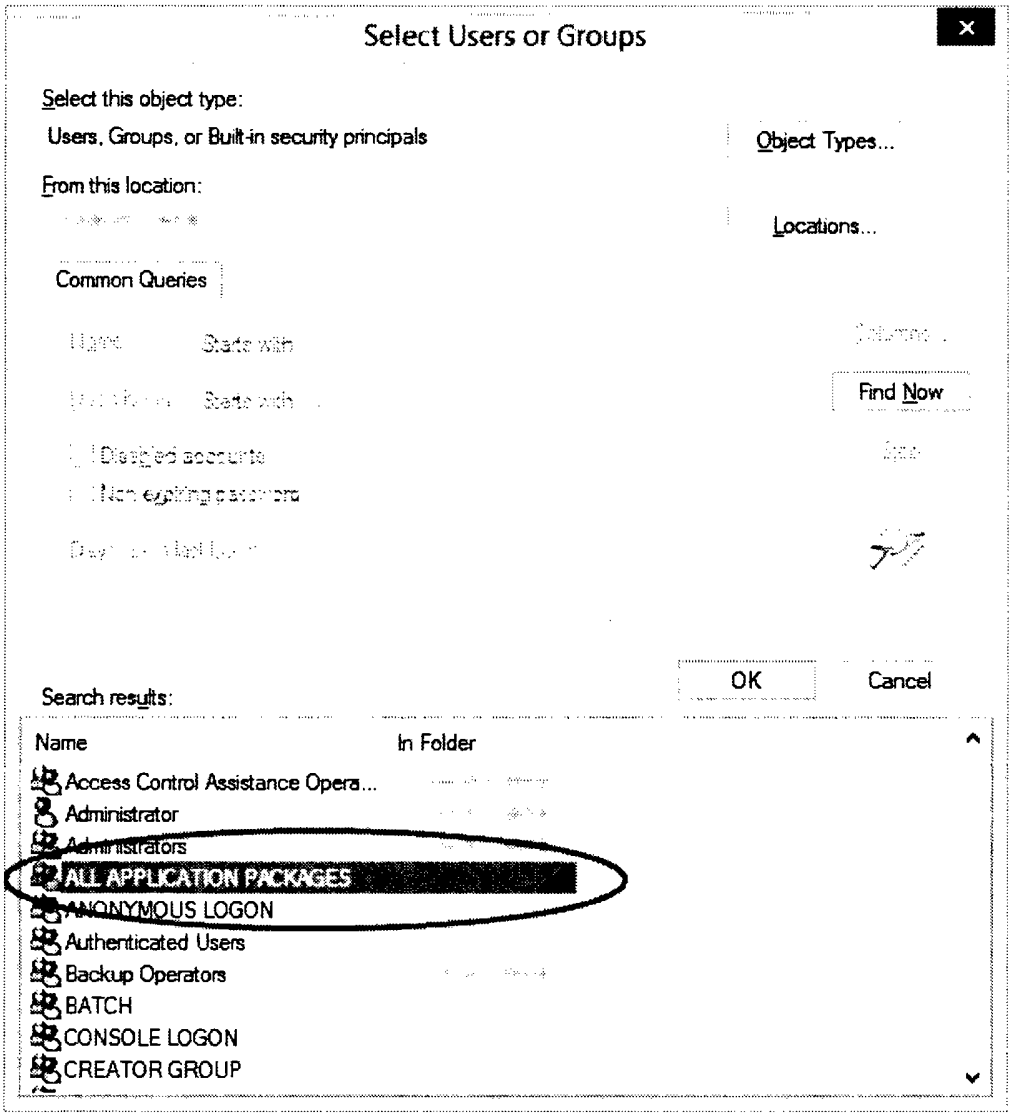
6. Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.
7. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
8. Make sure that the rule is enabled using the toggle switch under the Enable Rule column for the rule to take effect.
    - You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

Important Note to Windows 8 and Windows 8.1 users: If you are using Internet Explorer 11 version 11.0.9600.16384, it is mandatory to add the user group 'ALL APPLICATION PACKAGES' to the Restrictions list in addition to the intended users for each rule you create.

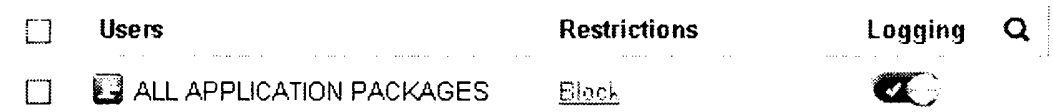
If you or other users access websites using Internet Explorer 11 on Windows 8/8.1, then you must add this user group or your rules will have no effect. For example, users will still be able to access blocked websites.

To add 'ALL APPLICATION PACKAGES' to the restrictions list

- Click 'Advanced' in the 'Select User or Group' dialog



- Click 'Find Now' and select 'ALL APPLICATION PACKAGES' from the list of users and groups displayed in the list at the bottom
- Click OK



To edit existing rules

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule to be edited under the 'Rules' tab by selecting the checkbox beside the rule.
3. Click the handle from the bottom center of the Rules interface and choose 'Edit' from the options.

The ' Website Filtering Rule' interface for the selected rule will open. You can add/remove categories, add/remove users or change the restriction for selected users from this interface. Refer to **To create a new Website Filtering Rule** for more details on this interface.

To remove a Website Filtering Rule

Best Available Copy

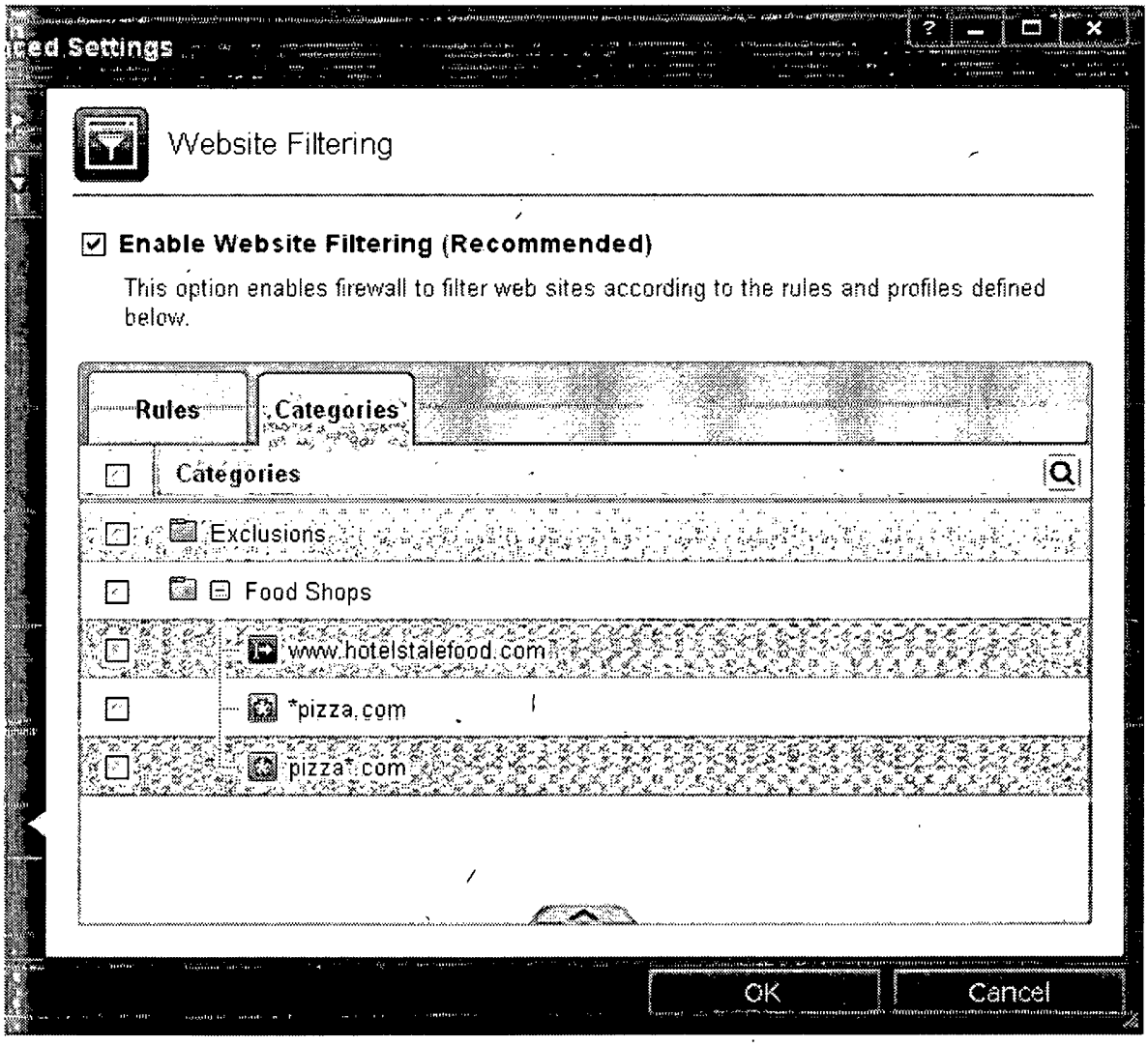
1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule(s) to be removed under the 'Rules' tab by selecting the checkbox(es) beside them.
3. Click the handle from the bottom center of the Rules interface and choose 'Remove' from the options.

To change the priority of Website Filtering Rules

1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule to be moved under the 'Rules' tab by selecting the checkbox beside the rule.
3. Click the handle from the bottom center of the Rules interface and choose 'Move Up' or 'Move Down' option to change the order of the rules in the interface.

6.2.3.7.2. Defining or Modifying Website Categories

The 'Categories' pane displays a list of user-defined categories that can be added to rules. A category can be a list of one or more URLs and/or part of URL with wildcard character. You can search for a specific category by clicking the search icon at the far right in the column header.



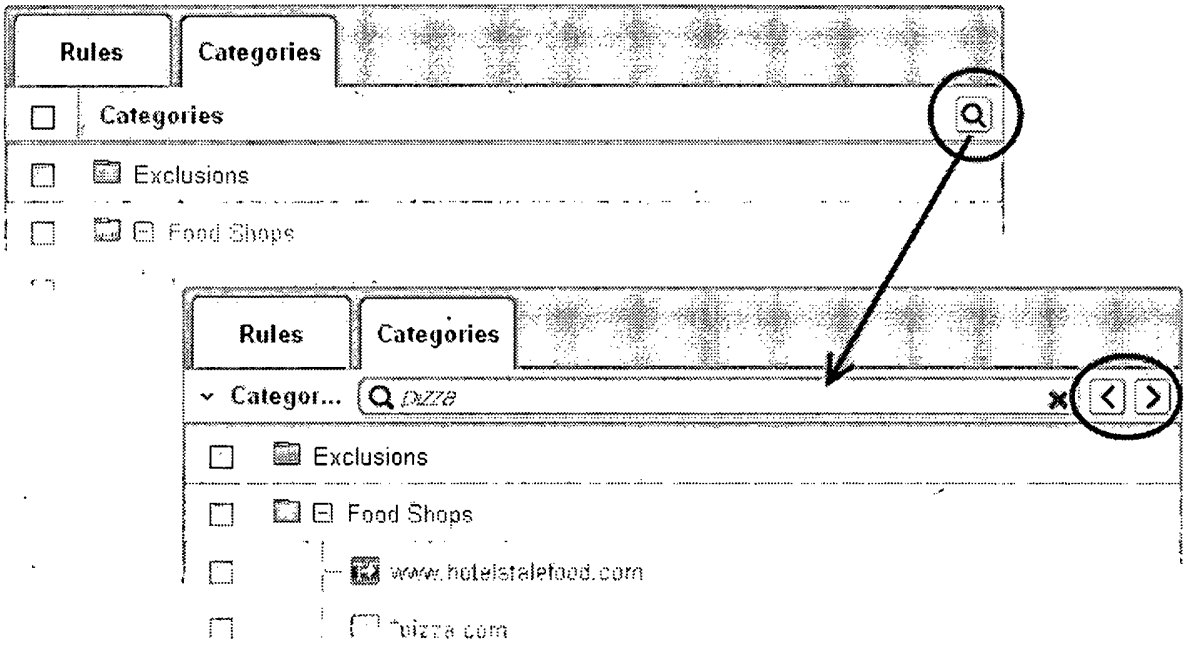
The 'Categories' pane allows you to:

- **Add a new category of Websites**

Best Available Copy

- Rename a Category
- Remove unwanted Websites from a category
- Remove a Category

To search for a specific category, click the search icon at the far right in the column header.



- Enter full or part of the name of the category in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

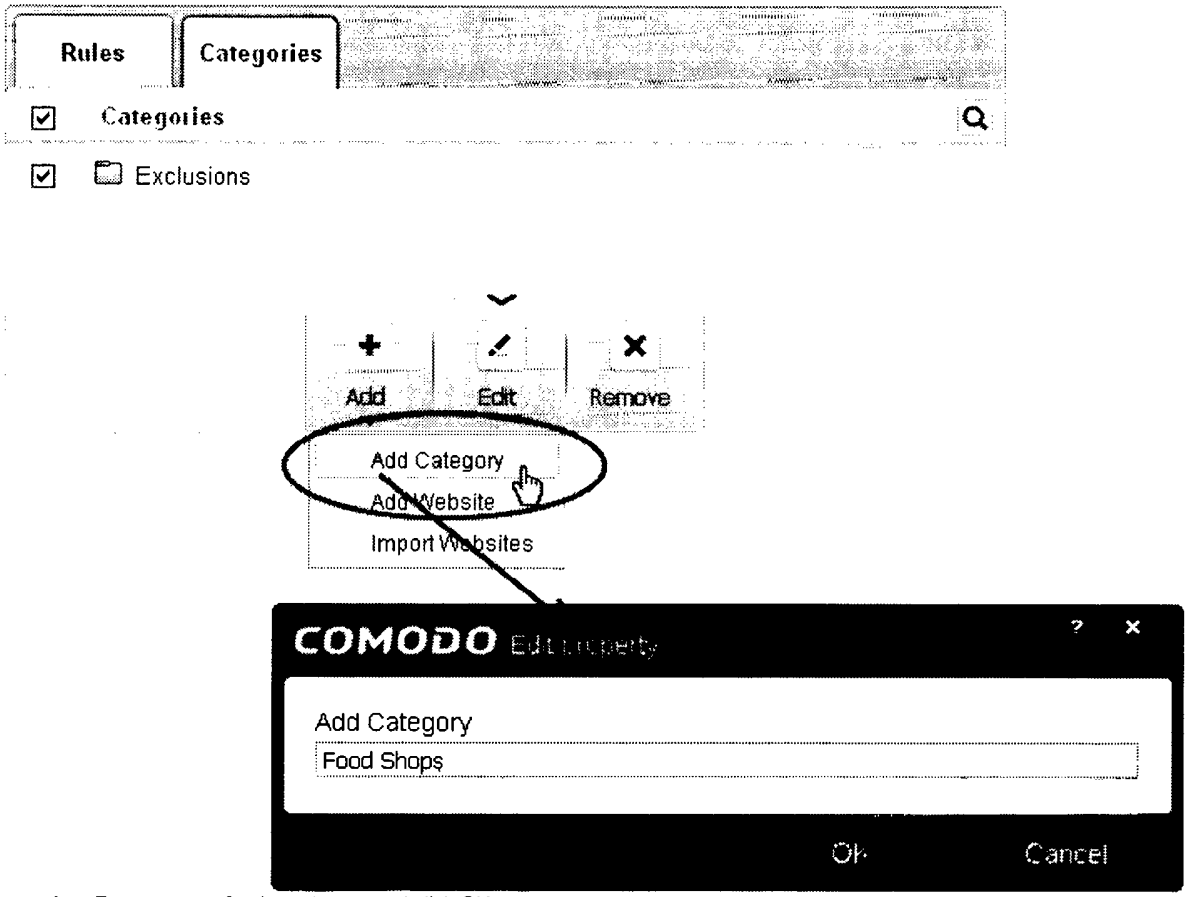
Adding a New Category of Websites

Adding a new category involves two steps:

- Step 1 - Define a name for the category
- Step 2 - Add Websites to be included to the category

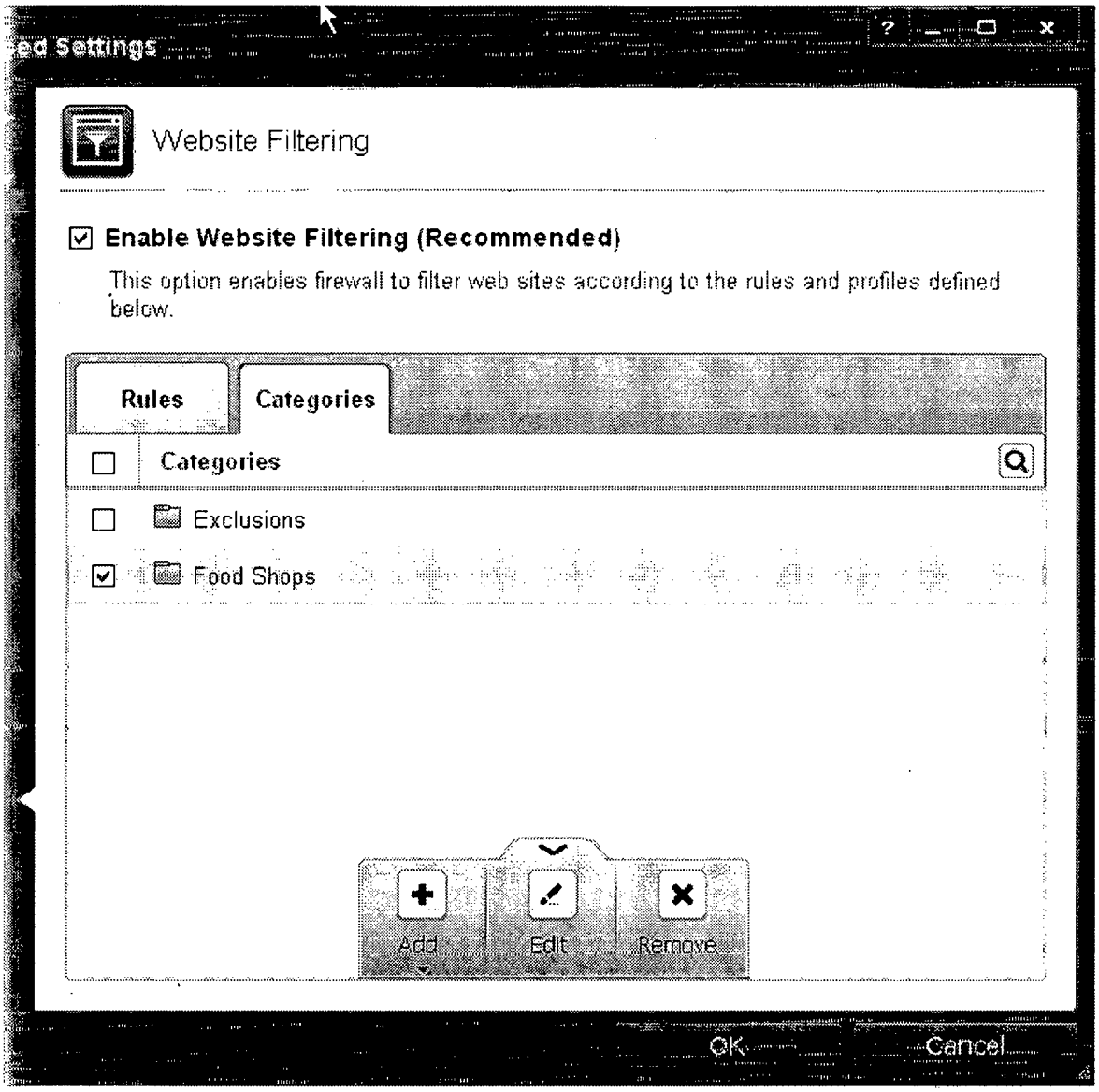
Step 1 - Define a name for the category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Click the handle from the bottom center of the 'Categories' pane, click 'Add' from the options and choose 'Add Category' from the drop-down. The 'Edit Property' dialog will open.



4. Enter a name for the category and click OK

The new category will be created and added under the 'Categories' tab.



You can add URLs of websites to be included in the category.

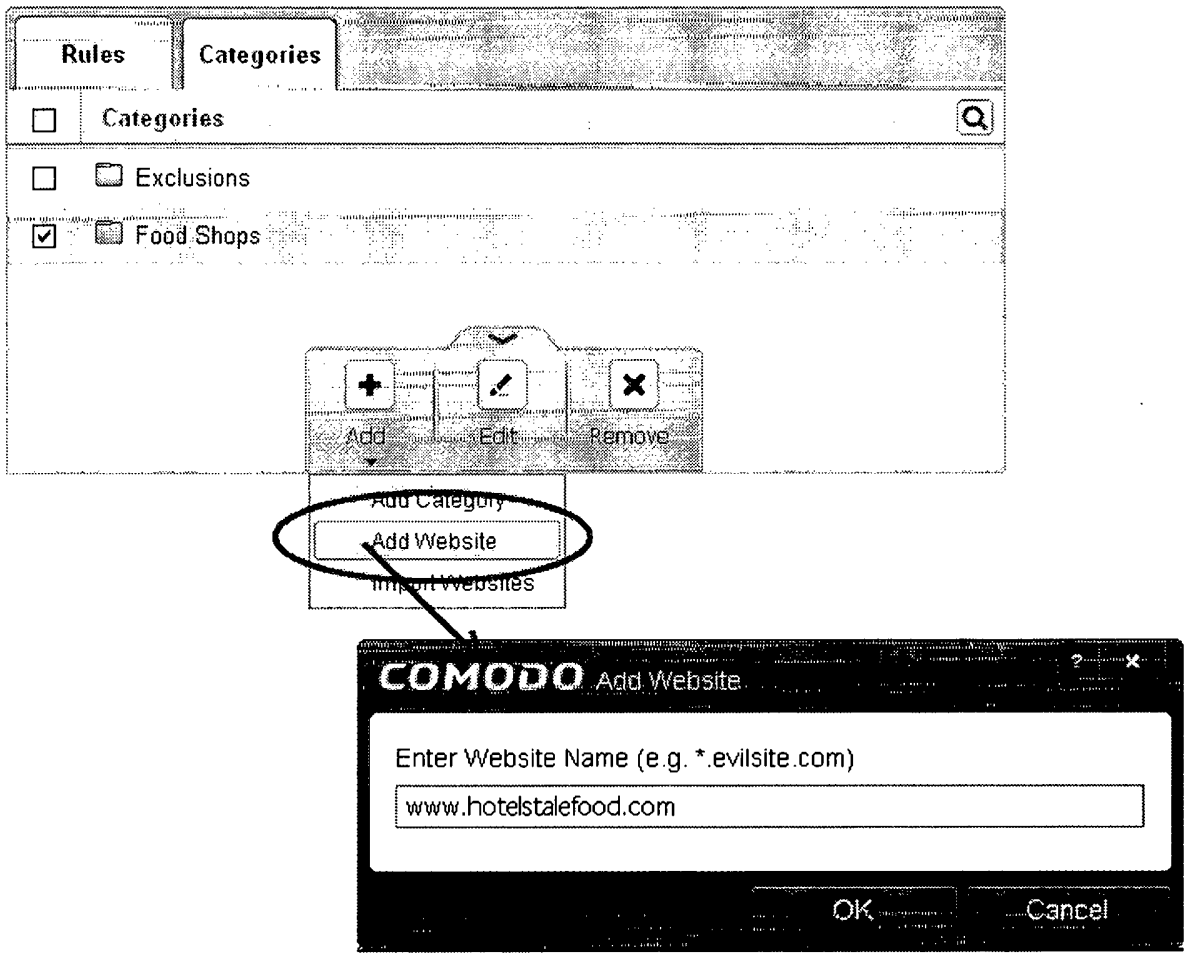
Step 2 - Add URLs to be included to the category

You can add websites to a category in two ways:

- **Manually Specify Websites**
- **Upload Website URLs from a text file**

To manually specify websites

1. Select the Category under the 'Categories' tab.
2. Click the handle at the bottom of the 'Categories' pane, click 'Add' then choose 'Add Website' from the drop-down menu. The 'Add Website' dialog will open:

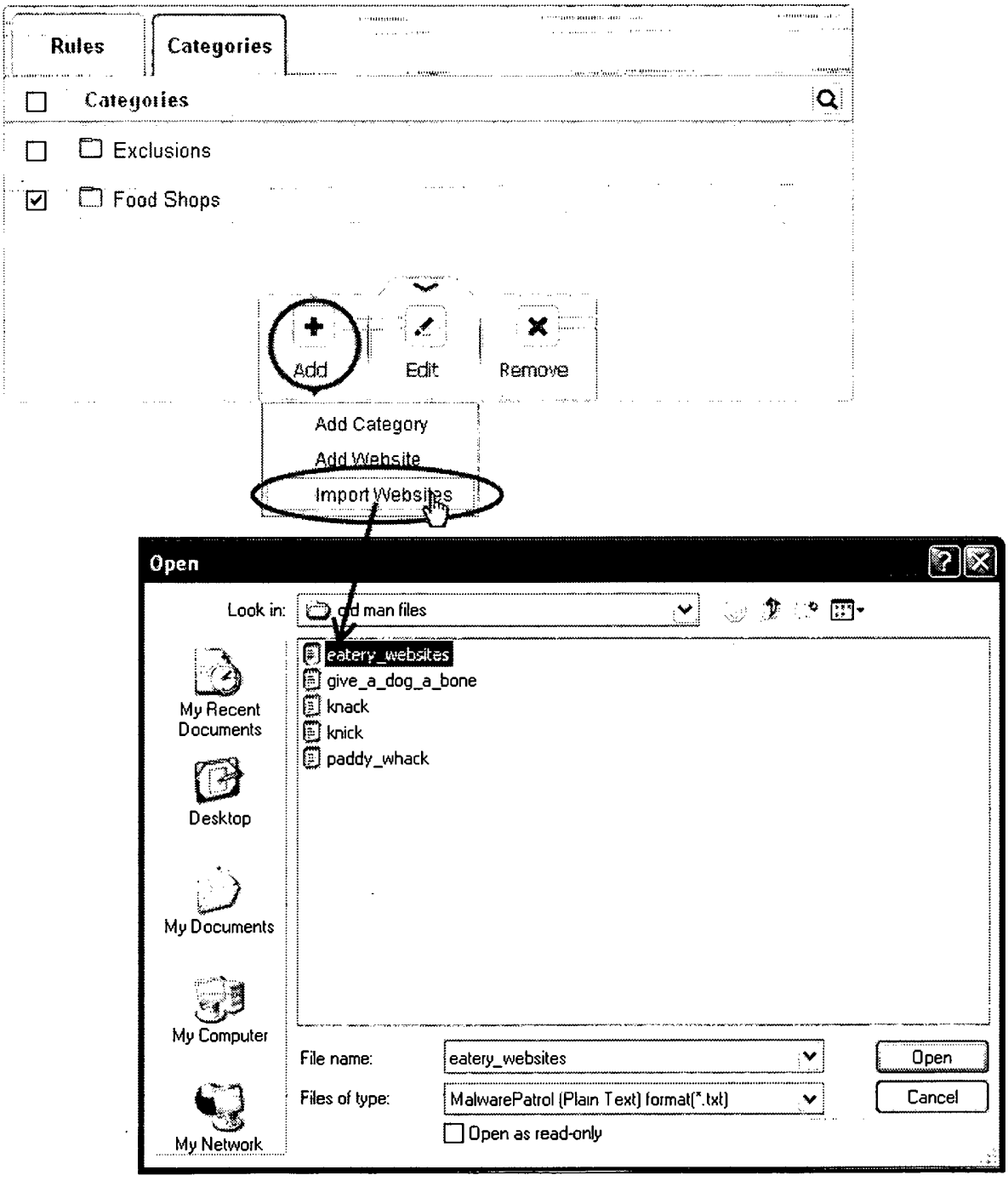


3. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
    - To add a specific website/webpage, enter the full URL of the website/webpage
    - To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
    - To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.
    - To include all the websites with URLs that contain a specific string, add the wildcard character befor and after the string. For example, "*pizza*" will cover hotpizza.com, spicypizza.com and so on.

    The website will be added to the category.
4. Repeat the process to add more websites.

To upload a list of websites from a text file

1. Select the target category from the 'Categories' tab.
2. Click the handle at the bottom of the 'Categories' pane then click 'Add' and choose 'Import'
3. Navigate to the file containing your list of URLs.



Note: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.

4. Click 'Open'.

CIS will automatically add the websites specified in the text file into the selected category.

To rename a category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.

3. Select the category to be renamed.
4. Click the handle from the bottom center of the 'Categories' pane and choose 'Edit' from the options. The 'Edit Property' dialog will open.
5. Enter the new name for the category and click OK

The category will be renamed immediately both under the Categories tab and in the Website Filtering Rules to which it is applied.

To remove a Website from a category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Click the + button beside the category to be edited to expand the website list
4. Select the Website(s) to be removed
5. Click the handle from the bottom center of the 'Categories' pane and choose 'Remove' from the options.

To remove a Category

1. Open the 'Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > ' Website Filtering' tab from the 'Advanced Settings' interface
2. Click the 'Categories' tab to open the 'Categories' pane.
3. Select the Category to be removed
4. Click the handle from the bottom center of the 'Categories' pane and choose 'Remove' from the options.

Note: You cannot remove a category which is currently applied in a Website Filtering Rule. Before removing a category, make sure you remove the category from the rules to which it is applied.

6.2.4. Manage File Rating

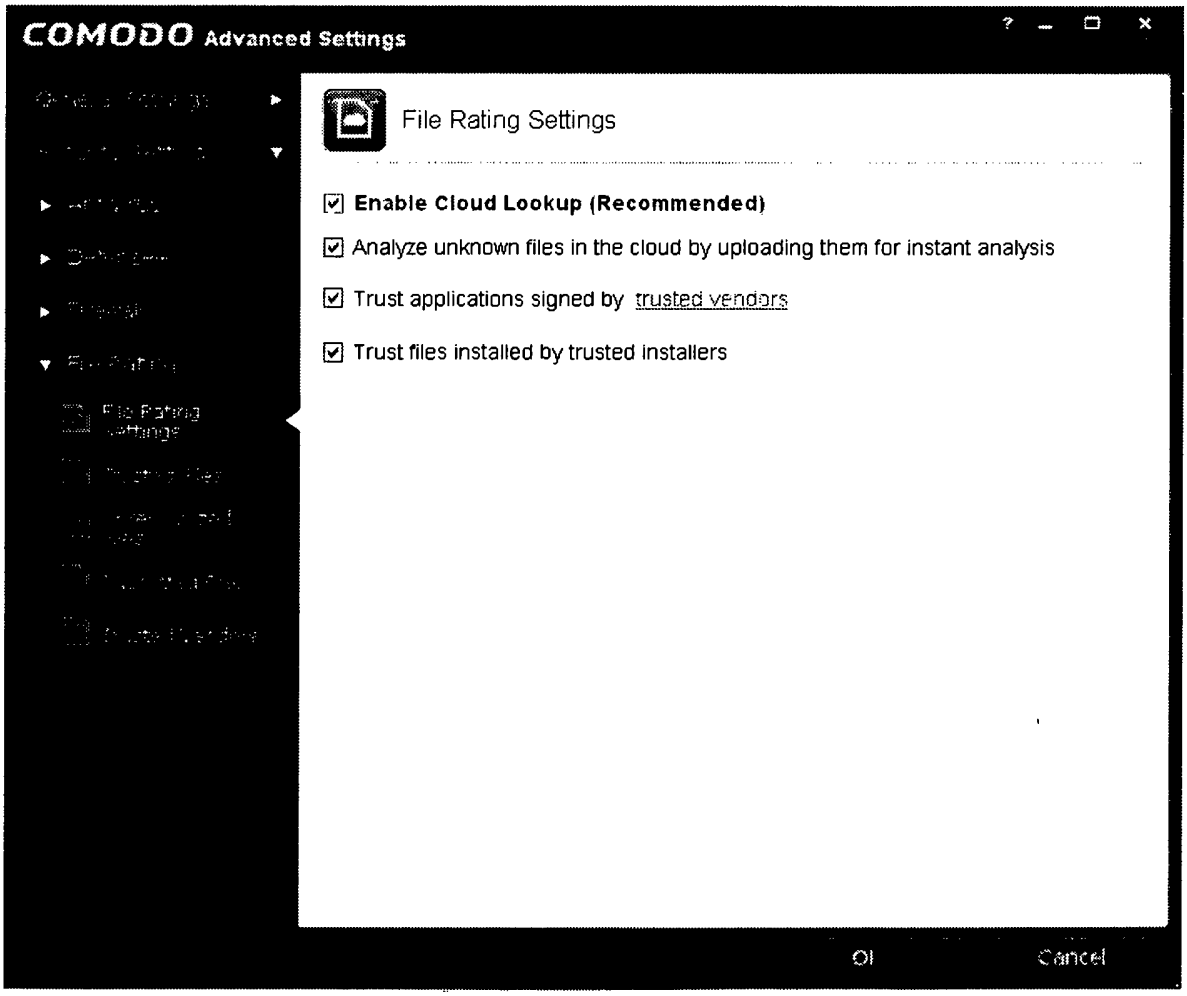
The CIS file rating system is a cloud-based file look-up service (FLS) that attempts to ascertain the reputation of files on your computer by consulting a global database. Whenever a file is first accessed, CIS will check the file against our master whitelist and blacklists and will award it trusted status if:

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

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

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

- Manually add files and executables to Trusted Files list.
- Submit unrecognized files for look-up and view the list of files you have submitted previously.
- View and manage the Trusted Software Vendor list.



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

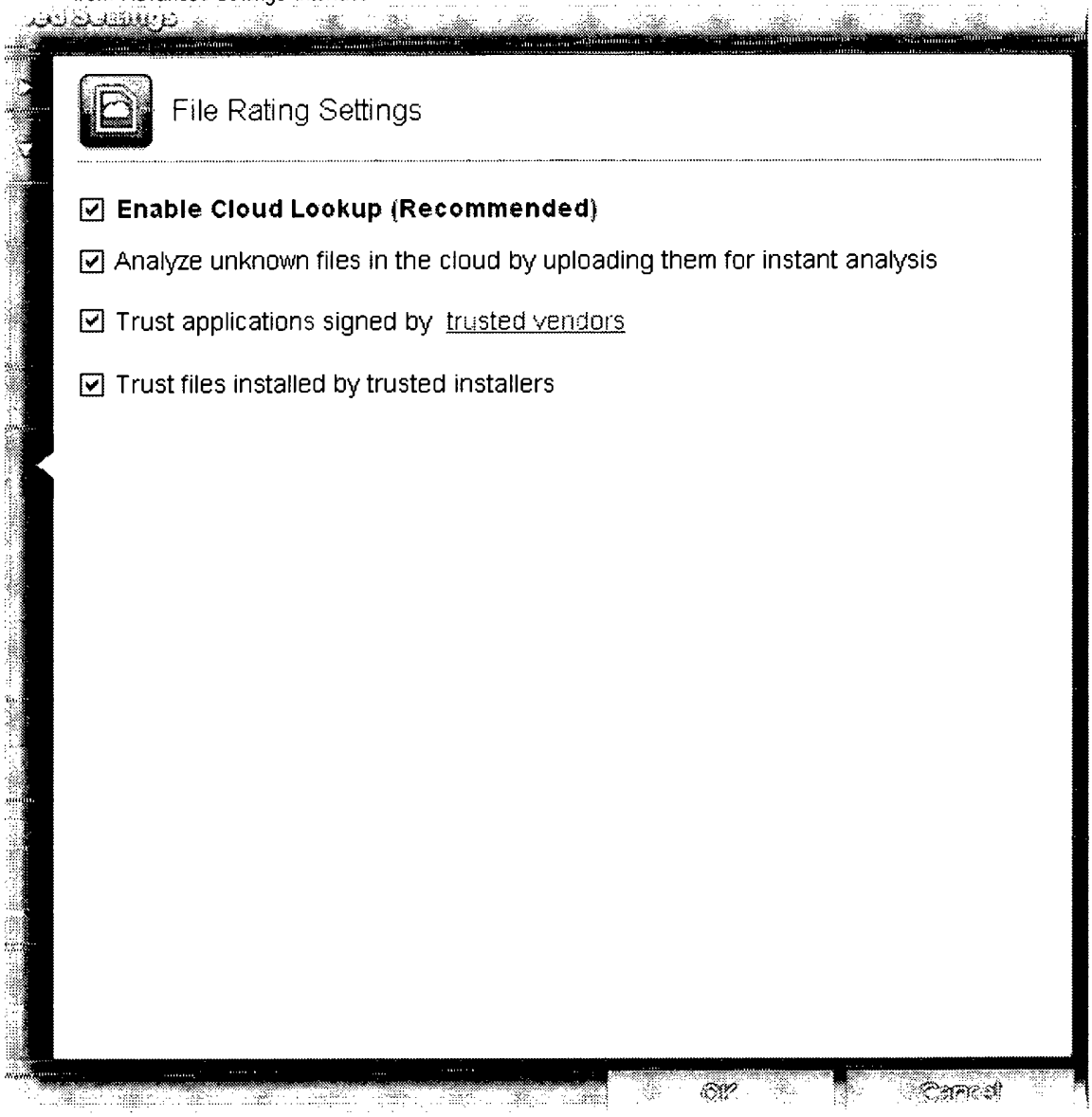
- **File Rating Settings** - Configure settings that govern the overall behavior of file rating.
- **Trusted Files** - View and add to the list of trusted files.

- **Unrecognized Files** - View and manage unrecognized items.
- **Submitted Files** - View any files already submitted to Comodo for analysis.
- **Trusted Vendors** - View the list of trusted software vendors and manually add vendors.

6.2.4.1. File Rating Settings

The file ratings 'Settings' panel allows you to configure the overall behavior of the feature.

- The File Rating Settings panel can be accessed by clicking Security Settings > File Rating > File Rating Settings tab from 'Advanced Settings' interface



- **Enable Cloud Lookup** - Allows you to enable or disable File Rating.(***Default and recommended =Enabled***)
- **Analyze unknown files in the cloud by uploading them for instant analysis** - Instructs CIS to automatically submit to Comodo those files whose trustworthiness could not be assessed by cloud look-up. Comodo Technicians will analyze the file and add it to future blacklists if found to be malicious. (***Default =Disabled***)
- **Trust applications signed by trusted vendors** - If enabled, CIS will award trusted status to executables and files that are code-signed by vendors in the Trusted Vendors list. Click the words 'trusted vendors' to open the **Trusted Vendors** panel. (***Default =Enabled***)
- **Trust files installed by trusted installers** - If enabled, CIS will trust executables and files whose parent applications

are listed under the 'Installer or Updater' rule in **HIPS Rules**. (***Default =Enabled***)

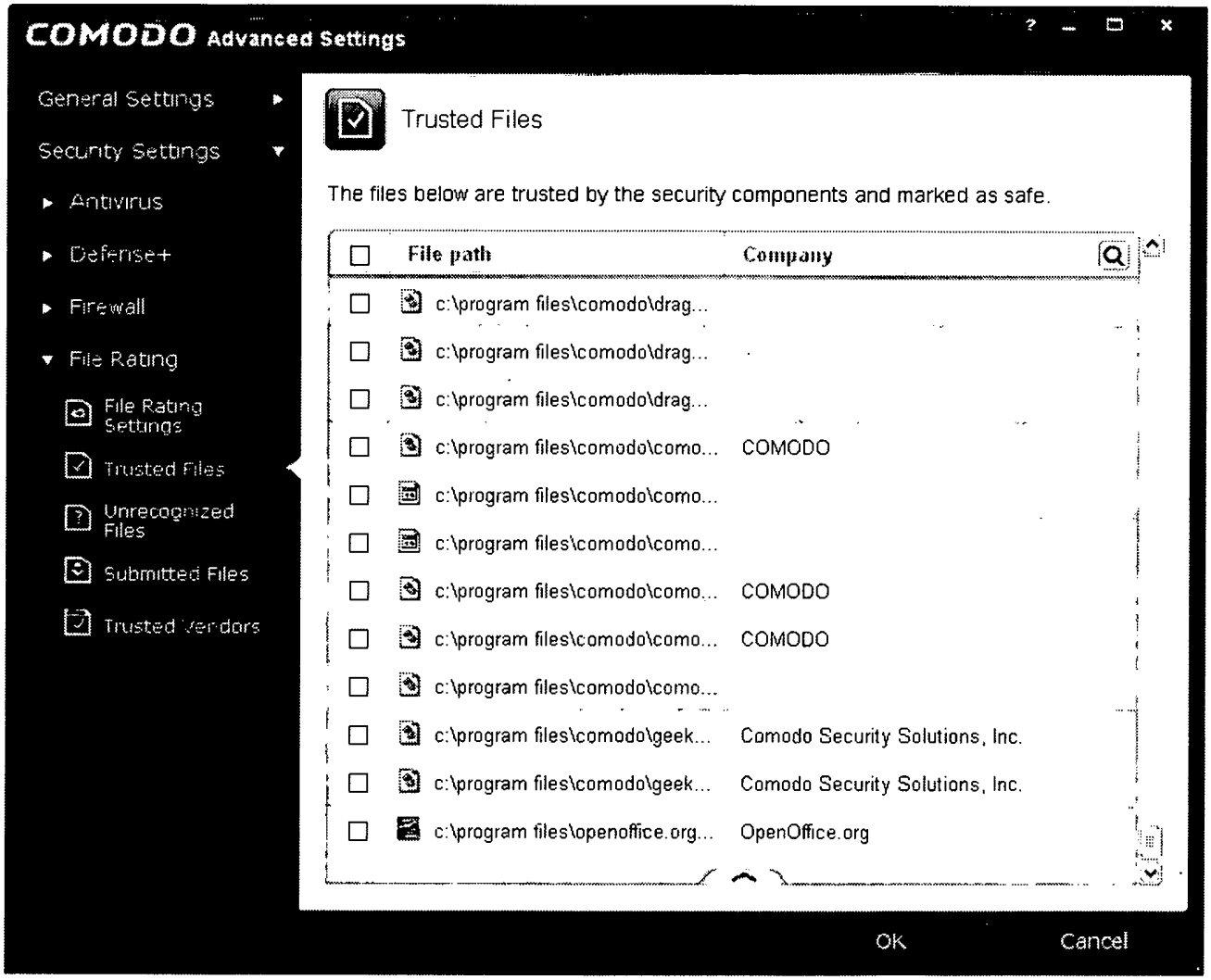
6.2.4.2. Trusted Files

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

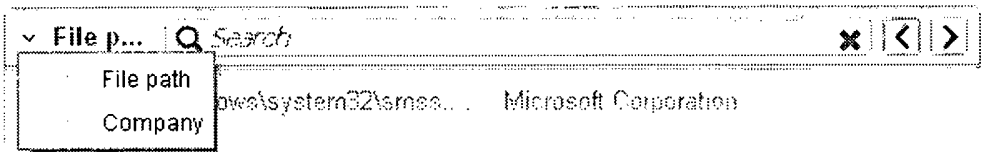
CIS allows you to define a personal safe list of files to complement the default Comodo safe list.

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

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

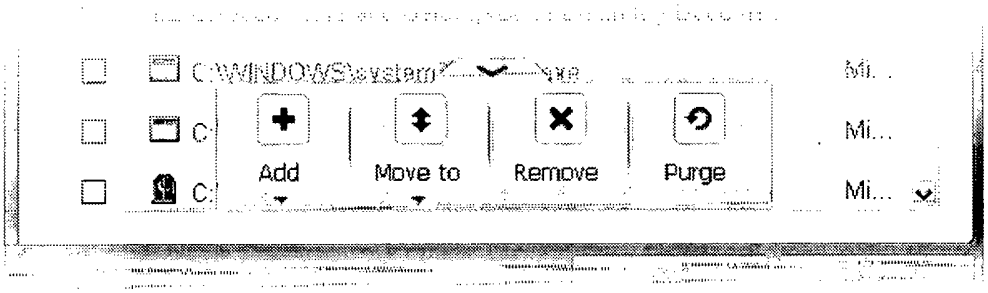


You can use the search option to find a specific item in the list by clicking the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter the name of the item to be searched 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:



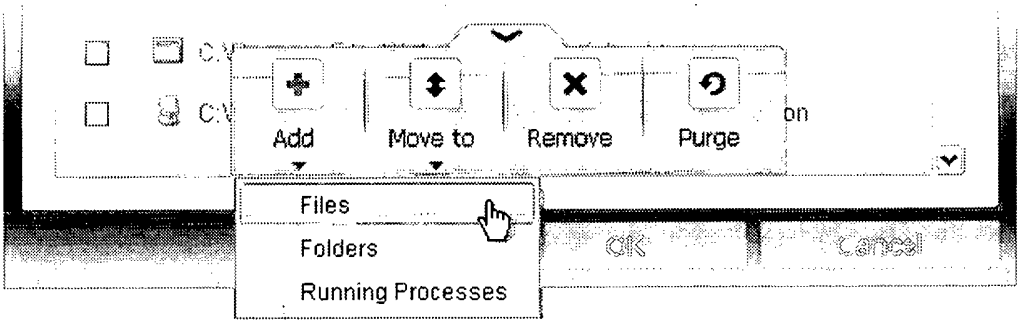
- **Add** - Allows you to add files to Trusted Files list manually
- **Move** - Allows you to move files from Trusted Files list to Blocked Files or Unrecognized Files list
- **Remove** - Allows you to remove files from Trusted Files list
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file is removed, or 'purged', from the list.

Adding files to Trusted Files list

CIS allows you to add files and executables to the list of Trusted Files so that those files will be given Trusted status. For the files added manually, it generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. By this way, even if the file name is changed later, it will retain its Trusted status as the hash remains same. However you can also add files by their file names, but if you happen to change the file name later, it looses its 'Trusted' status.

To add new file(s) to Trusted Files list

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



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

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

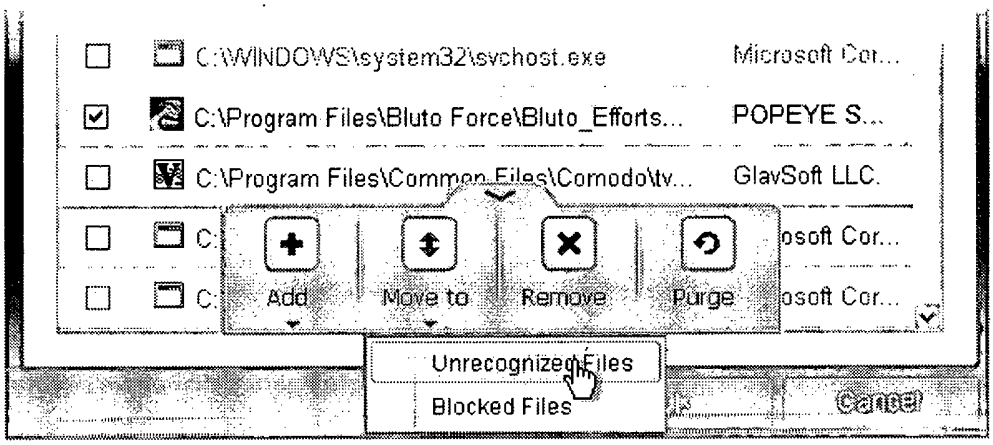
Best Available Copy

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

- Click OK for your changes to take effect.

To move an included entry to Unrecognized Files or Blocked Files

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



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

To remove an included entry from the Trusted Files list

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

6.2.4.3. Unrecognized Files

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

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

The files that are moved to Unrecognized Files list either automatically or manually, can be checked for their trustworthiness in two ways:

- Online Lookup - If you are uncertain with the reliability of a file or executable added to the unrecognized file, you can perform an online lookup for the same by contacting Comodo servers. Comodo's master safe list database will be checked for any information available about the executable/file in question and the results will be displayed. Based on the results, you can decide on
  - Trusting the file and allowing it to run by adding it to the **Trusted Files** list,

    or
  - Block the file by moving it to **Blocked Files** list.

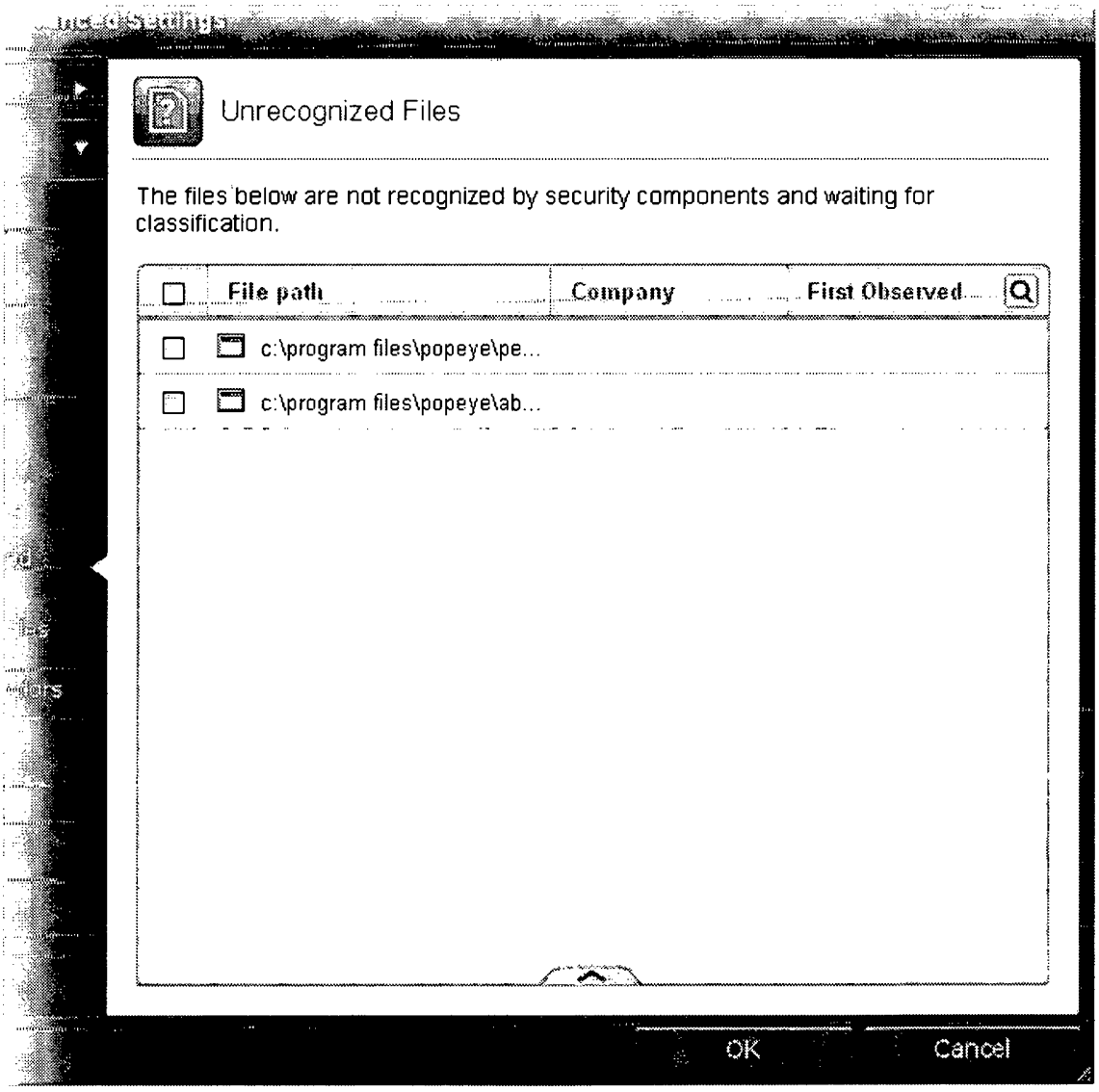
  Refer to the section **To perform an online lookup for unrecognized files** for more details.

- Submitting file(s) for analysis at Comodo - You can also submit the files moved to Unrecognized File list or the files for which the Online File Look Up did not yield any results for analysis by experts at Comodo. Files submitted will be analyzed thoroughly by experienced technicians at Comodo and will be added to global safe list, if the file is found trustworthy or to global blacklist, if the file appears to be malicious and will be added to the next virus database update. This will benefit all the CIS users worldwide. Refer to the section **To manually submit files to Comodo** for more details on submitting suspicious files to Comodo.

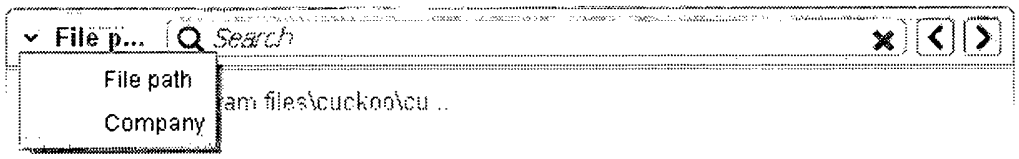
The 'Unrecognized Files' panel displays the list of files added as Unrecognized Files and allows you to assess the pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be moved to 'Trusted Files' using the **'Move to'** button. Similarly, files that are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

You can also add files upon which you are suspicious into 'Unrecognized Files' list to check whether the master Comodo safe list contains more information on them or to submit the files to Comodo for analysis. Experts at Comodo will analyze the files and add them to global white-list or black-list accordingly.

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

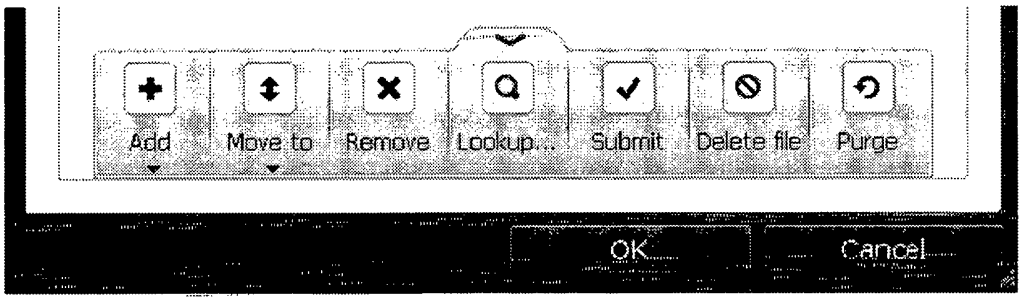


You can use the search option to find a specific item in the list by clicking the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the name of the item to be searched 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.

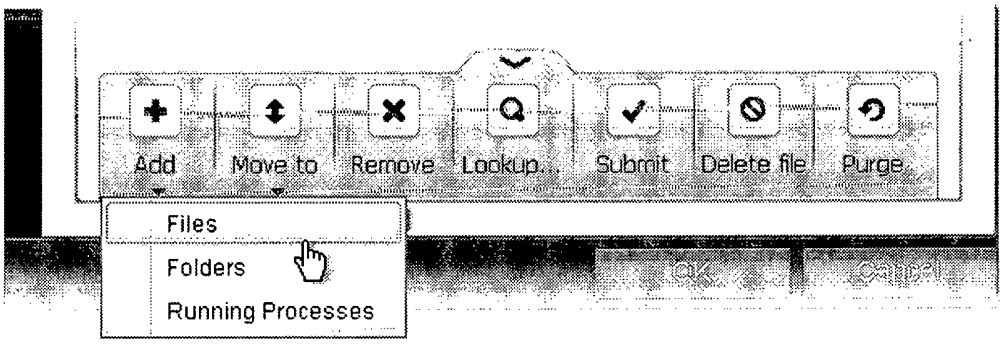
Clicking the handle at the bottom center of the panel opens the following options:



- **Add** - Allows you to add files to 'Unrecognized Files' list manually
- **Move** - Allows you to move files from 'Unrecognized Files' list to Trusted Files or Blocked Files list
- **Remove** - Allows you to remove files from 'Unrecognized Files' list
- **Lookup** - Starts the online lookup of selected file with the master Comodo safelist if any details are available
- **Submit** - Begins the **file submission process**.
- Delete file - Deletes the highlighted file from your computer
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file is removed, or 'purged', from the list.

To manually add files to 'Unrecognized Files' list

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



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

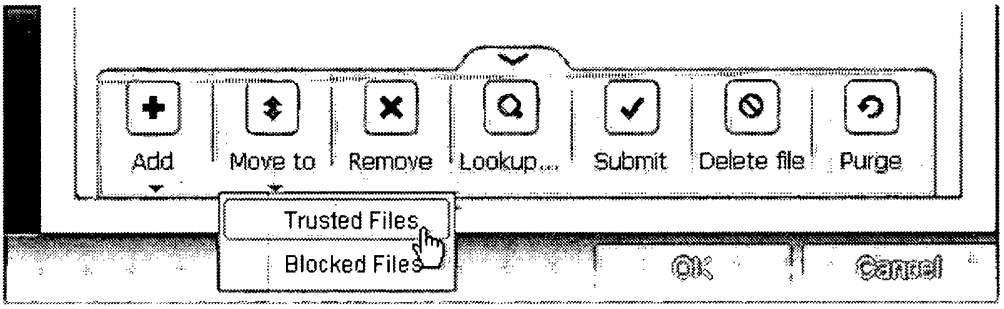
- **Files** - Allows you to navigate to the file or executable of the program you wish to add.
- **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'Unrecognized Files' list.
- **Running Processes** - Allows you to select a currently running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

application, which invoked the process will be added to 'Unrecognized Files' list.

- Click OK for your changes to take effect.

To move an included entry to Trusted Files or Blocked Files

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



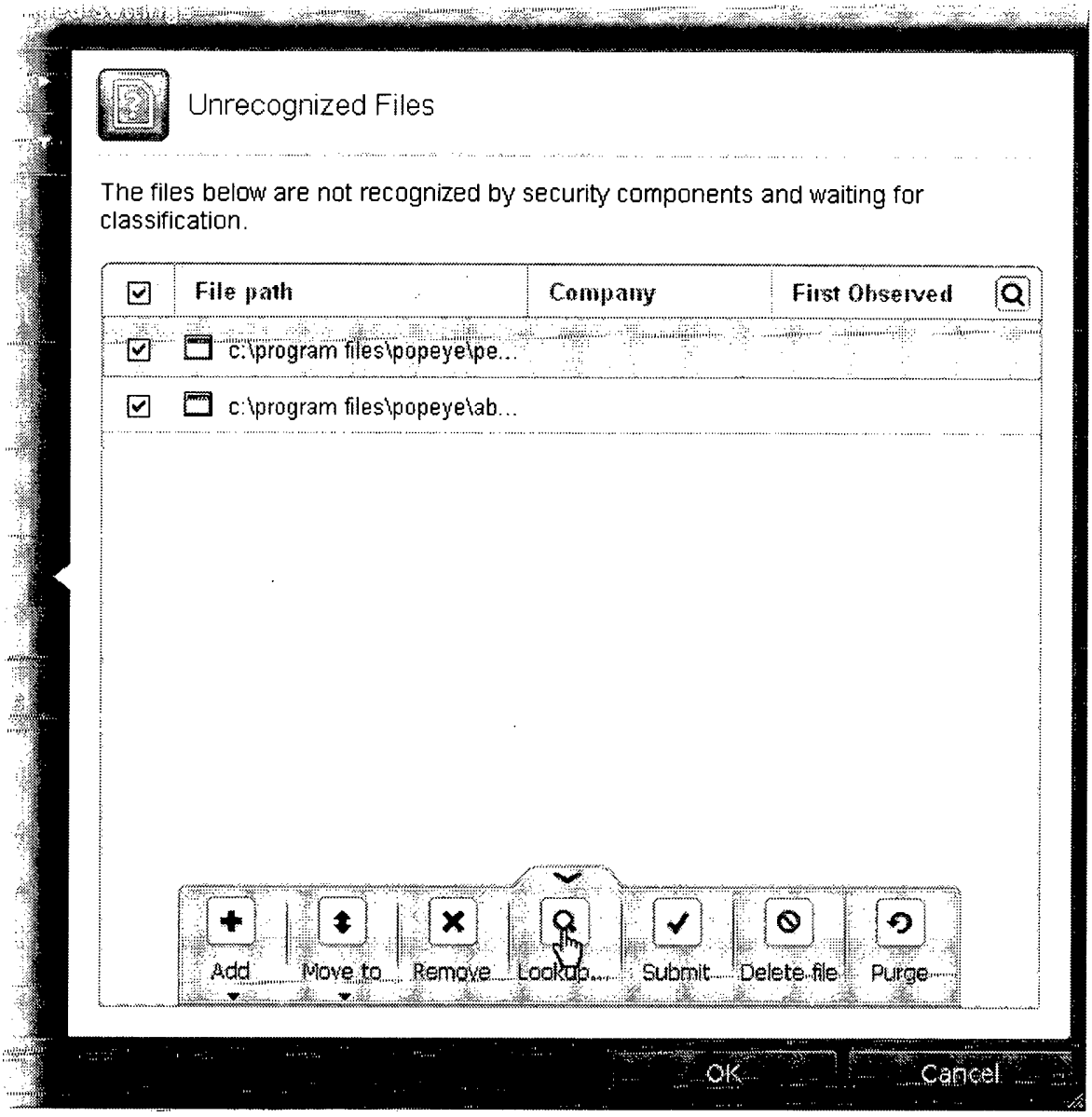
- Choose 'Trusted Files' or 'Blocked Files' from the drop-down.
- Click OK for your changes to take effect.

To remove an included entry from the Unrecognized Files list

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

To perform an online lookup for unrecognized files

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



Comodo servers will be contacted immediately to conduct a search of Comodo's master safe list database to check if any information is available about the files in question and the results will be displayed.



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

To manually submit files to Comodo

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

You can view the list of files you submitted so far, from the **Submitted Files** panel.

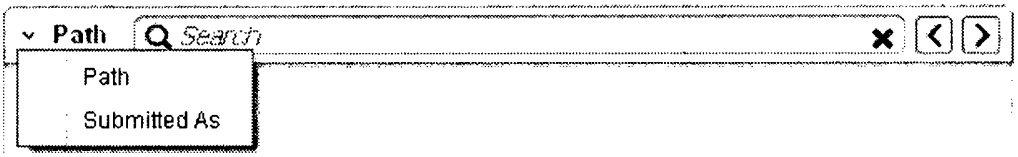
6.2.4.4. Submitted Files

The Submitted Files panel displays a list of files you have submitted so far for analysis to Comodo.



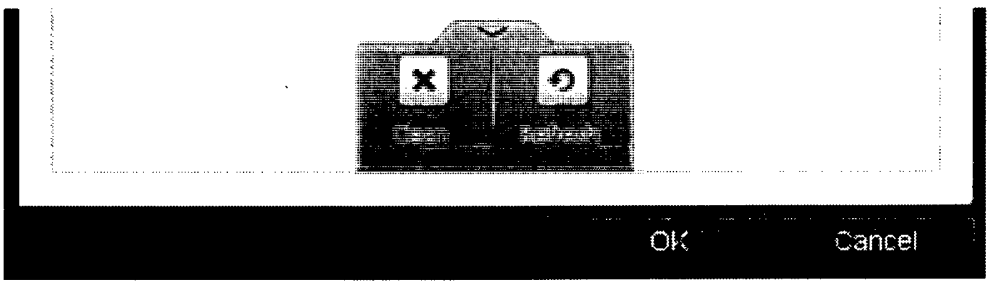
You can use the search option to find a specific file in the list.

To use the search option, click the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.
- Enter partly or fully the file path or the submitted status as per the selected criteria in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the ✖ icon in the search field to close the search option.

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



- **Clean** - Clears the list
- **Refresh** - Reloads the list to add items that are submitted recently

6.2.4.5. Trusted Vendors List

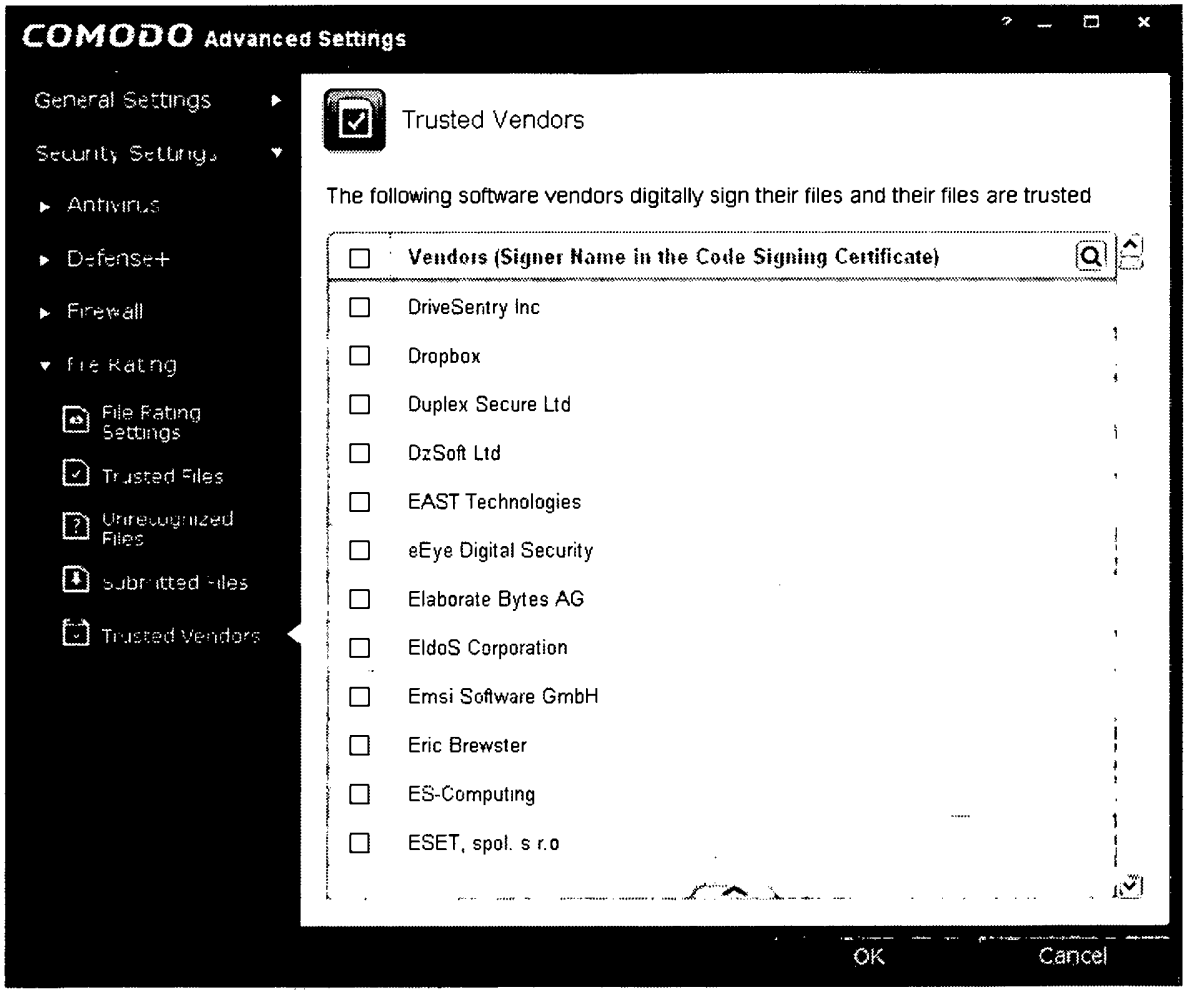
In Comodo Internet Security, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

From this point:

- IF the vendor is on the Trusted Software Vendor List AND the user has enabled '**Trust Applications signed by Trusted Vendors**' in the File Rating Settings panel, THEN the application will be trusted and allowed to run.
- IF the vendor is not on the Trusted Software Vendor List OR the user has not enabled 'Trust Applications signed by Trusted Vendors' THEN the application will be sandboxed. If the application in question is an installer then CIS will generate an elevated privilege alert.

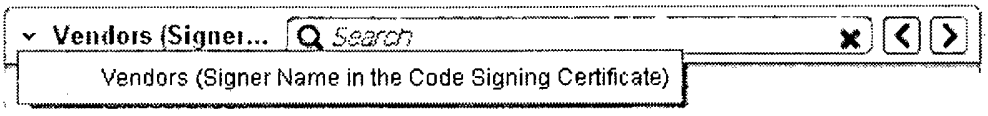
Software publishers may be interested to know that they can have their signatures added, free of charge, to the 'master' Trusted Software Vendor List that ships to all users with CIS. Details about this can be found at the foot of this page.

The 'Trusted Software Vendors' panel can be opened by clicking Security Settings > File Rating > Trusted Vendors.



You can use the search option to find a specific vendor in the list.

To use the search option, click the search icon at the far right in the column header.



- Click the chevron on the left side of the column header and select the search criteria from the drop-down.

- Enter partly or fully the vendor's name in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the icon in the search field to close the search option.

Click here to read background information on digitally signing software

Click here to learn how to Add / Define a user-trusted vendor

Software Vendors - click here to find out about getting your software added to the list

Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

i. **Content Source**: The software they are downloading and are about to install ***really comes from the publisher that signed it.***

ii. **Content Integrity**: That the software they are downloading and are about to install ***has not be modified or corrupted since it was signed.***

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

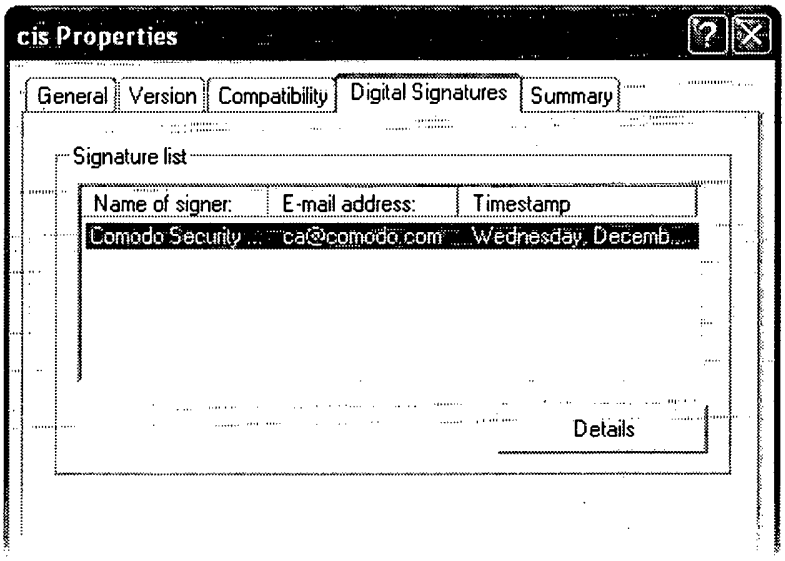
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by Comodo Internet Security (if you would like to read more about code signing certificates, see **http://www.instantssl.com/code-signing/**).

One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question. For example, the main program executable for Comodo Internet Security is called 'cis.exe' and has been digitally signed.

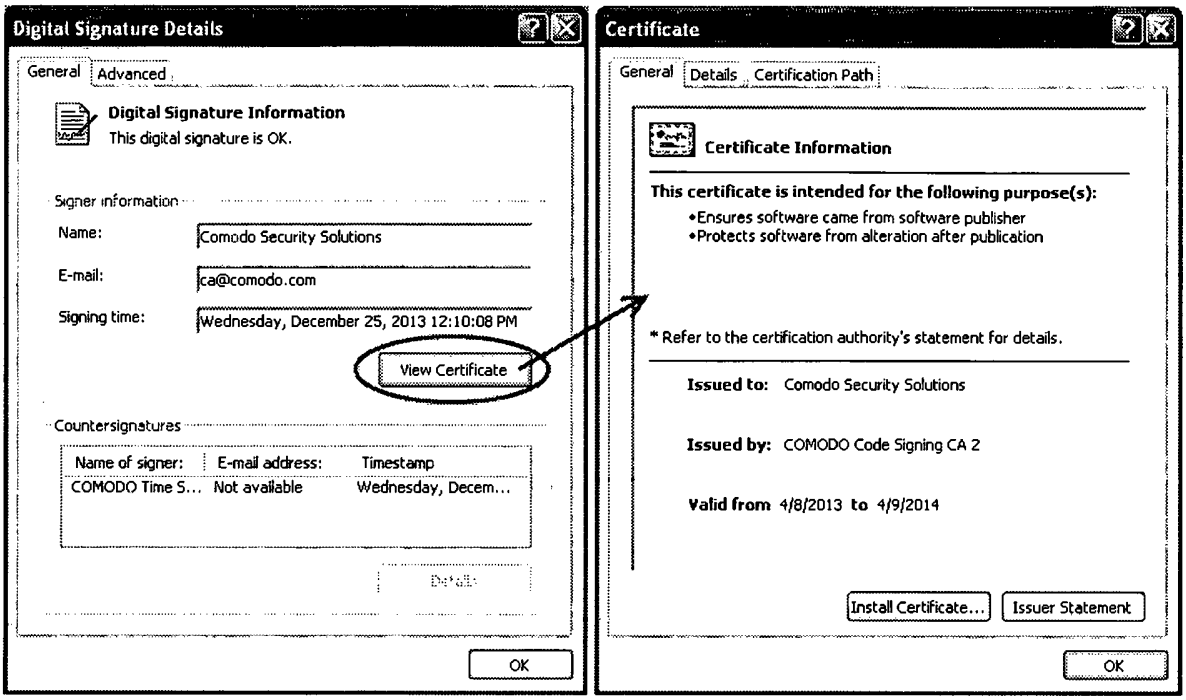
- Browse to the (default) installation directory of Comodo Internet Security.
- Right click on the file cis.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

This displays the name of the CA that signed the software as shown below:



Click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate.

(see below).



It should be noted that the example above is a special case in that Comodo, as creator of 'cis.exe', is both the signer of the software and, as a trusted CA, it is also the counter-signer (see the 'Countersignatures' box). In the vast majority of cases, the signer or the certificate (the vendor) and the counter-signer (the Trusted CA) are different. **See this example** for more details.

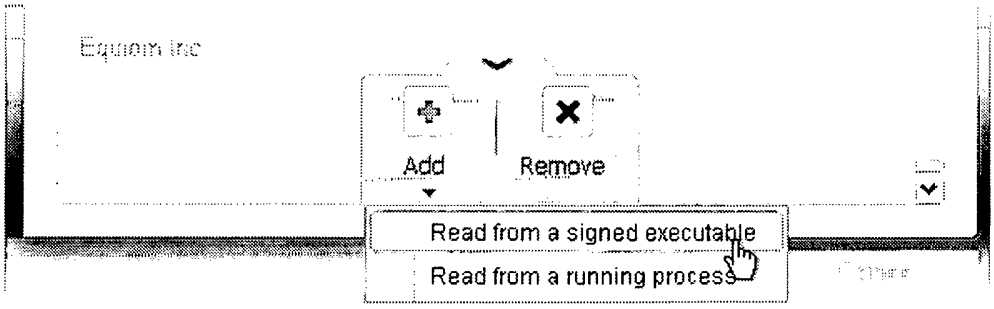
Adding and Defining a User-Trusted Vendor

A software vendor can be added to the local 'Trusted Software Vendors' list in two ways:

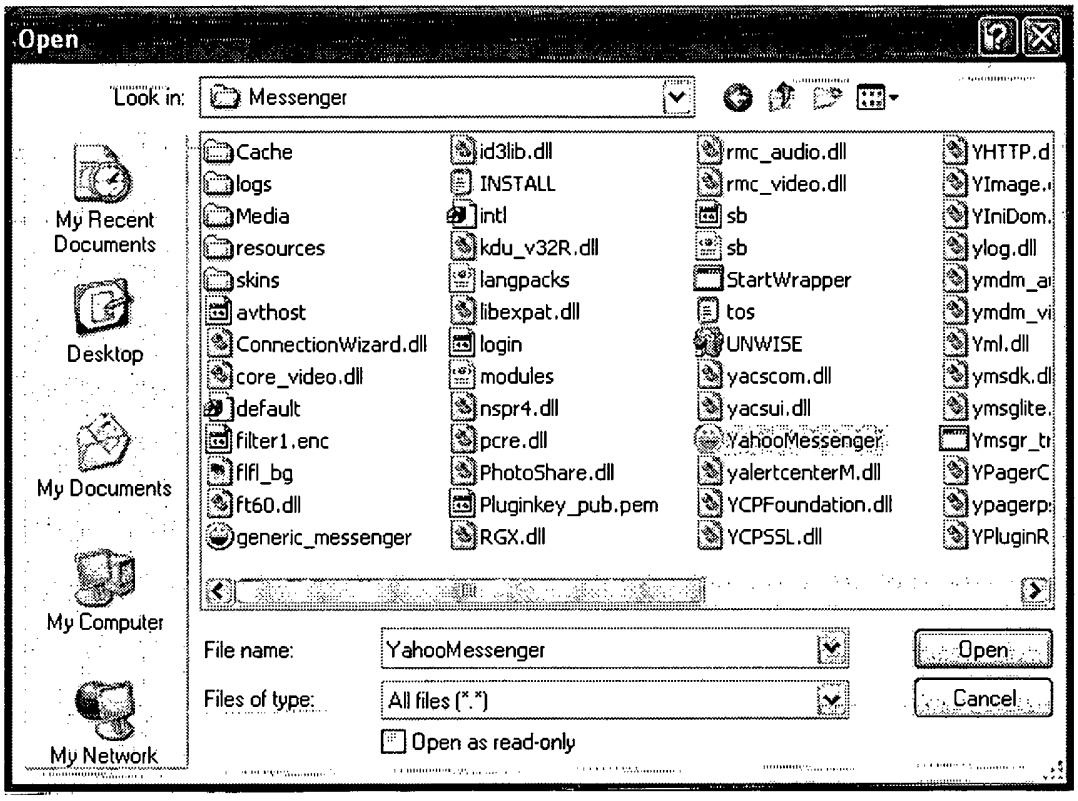
- **By reading the vendor's signature from an executable file on your local drive**
- **By reading the vendor's signature from an running process**

To add a trusted vendor by reading the vendor's signature from an executable

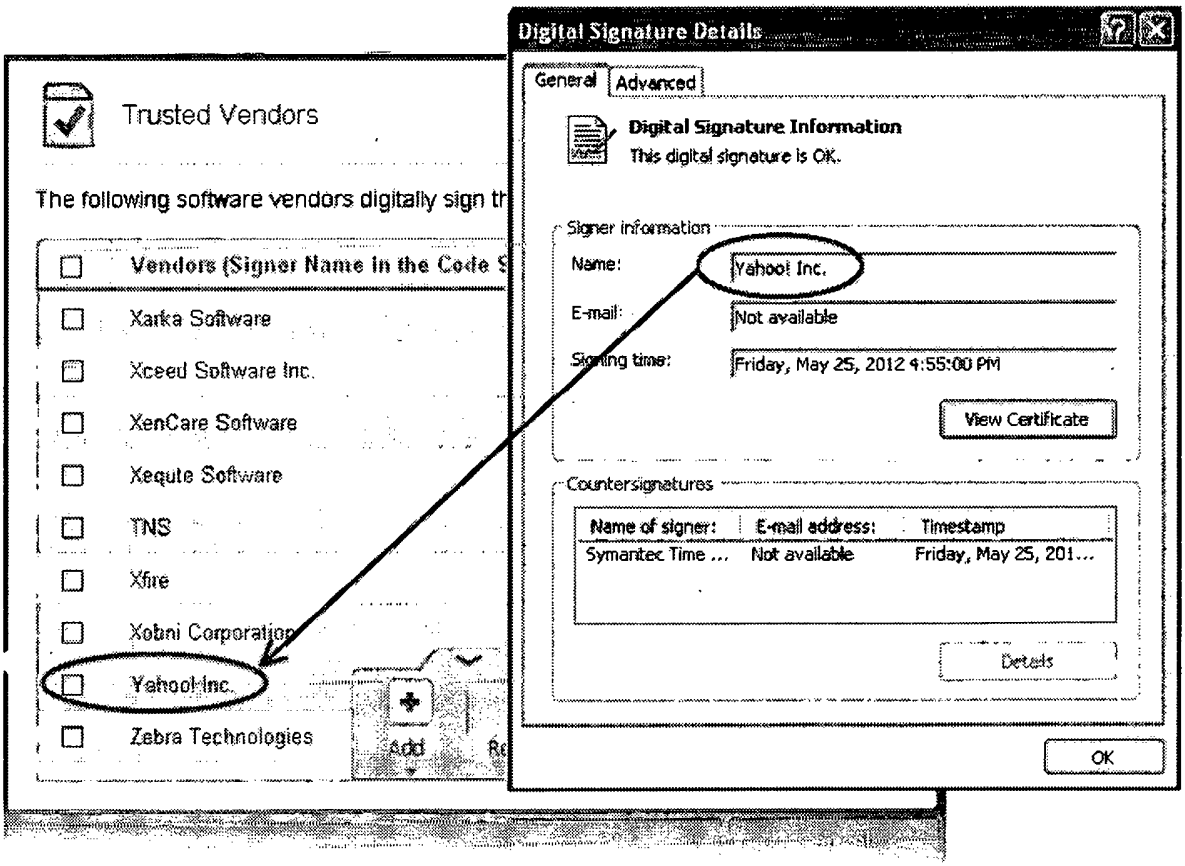
- Click the handle from the bottom center and choose 'Add' > 'Read from a signed executable'



- Browse to the location of the executable your local drive. In the example below, we are adding the executable 'YahooMessenger.exe'.



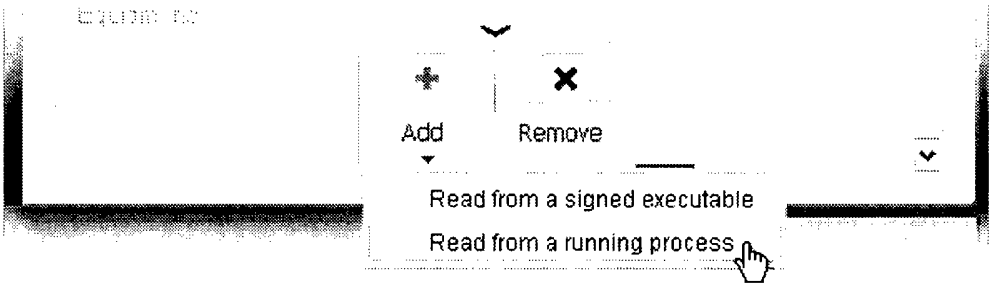
On clicking 'Open', Comodo Internet Security checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the Trusted Vendor list (TVL):



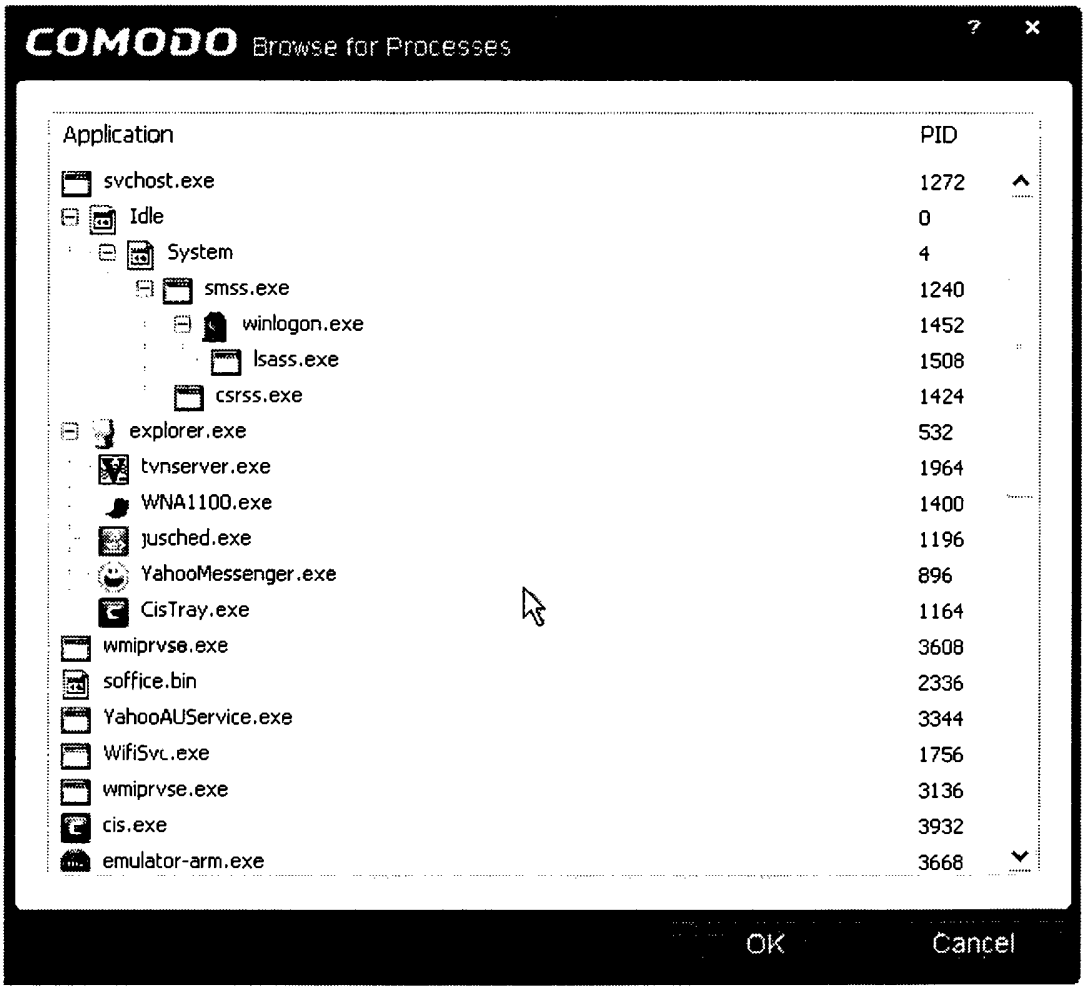
In the example above, Comodo Internet Security was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to the list. All future software that is signed by the vendor 'Yahoo! Inc.' is automatically added to the Comodo Trusted Vendor list UNLESS you change **this setting in File Rating Settings**.

To add a trusted vendor from a currently running process

- Click the handle from the bottom center and choose 'Add' > 'Read from a running process'

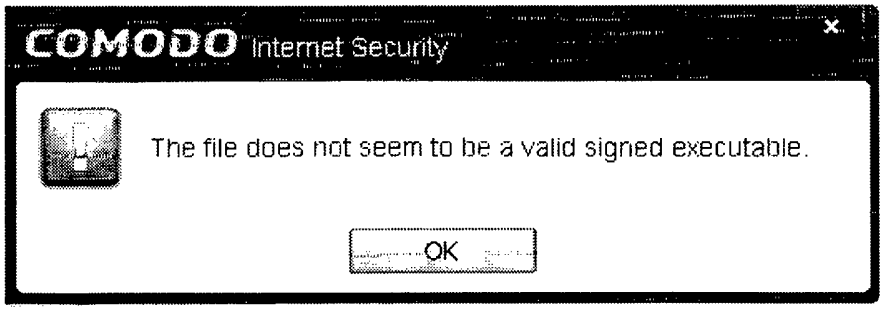


- Select the signed executable that you want to trust and click the 'OK' button.



Comodo Internet Security performs the same certificate check as described above. If the parent application of the selected process is signed, CIS adds the vendor to the Trusted Software Vendors list.

If Comodo Internet Security cannot verify that the software certificate is signed by a Trusted CA then it does not add the software vendor to the list of 'Trusted Vendors'. In this case, you can see the following error message.



Note: The 'Trusted Software Vendors' list displays two types of software vendors:

- User defined trusted software vendors - As the name suggests, these are added by the user via one of the two methods outlined earlier. These vendors can be removed by the user by selecting and clicking the 'Remove' button.
- Comodo defined trusted software vendors - These are the vendors that Comodo, in it's capacity as a Trusted CA, has independently validated as legitimate companies. If the user needs to remove any of these vendors from the list, it can be done by selecting the vendor, clicking 'Remove' and restarting the system. Please note that the removal will take effect only on restarting the system.

The Trusted Vendor Program for Software Developers

Software vendors can have their software added to the default Trusted Vendor List that is shipped with Comodo Internet Security. This service is free of cost and is also open to vendors that have used code signing certificates from any Certificate Authority. Upon adding the software to the Trusted Vendor list, CIS automatically trusts the software and does not generate any warnings or alerts on installation or use of the software.

The vendors have to apply for inclusion in the Trusted Vendors list through the sign-up form at **http://internetsecurity.comodo.com/trustedvendor/signup.php** and make sure that the software can be downloaded by our technicians. Our technicians check whether:

- The software is signed with a valid code signing certificate from a trusted CA;
- The software does not contain any threats that harm a user's PC;

before adding it to the default Trusted Vendor list of the next release of CIS.

More details are available at **http://internetsecurity.comodo.com/trustedvendor/overview.php**.

7.Comodo GeekBuddy

Comodo GeekBuddy is a personalized computer support service provided by friendly computer experts at Comodo. If you experience any issues at all with your computer, simply click the GeekBuddy icon to establish a chat session with one of our technicians.

After requesting your permission, they'll establish a remote connection to your PC and fix the problems right in front of your eyes. No longer do you need to make time consuming calls to impatient help desk support staff. Instead, just sit back and relax while our friendly technicians do the work for you.

Visit **http://www.geekbuddy.com/** for more details.

One of the great features of the CIS interface is that you can immediately launch a chat with a qualified computer support technician by clicking 'Help icon  > Support > Get Live Support. If you have opted not to include GeekBuddy during CIS installation, choosing Get Live Support will start the installation automatically.

GeekBuddy is included with CIS Pro and Complete versions and is available with CIS Premium. The GeekBuddy section of this guide is broken down into the following sections:

- **Overview of the Services**
- **Activation of Service**
- **Launching the Client and Using the Service**
- **Accepting Remote Desktop Requests**
- **Chat History**
- **Using Issue Tracker**
- **Uninstalling Comodo GeekBuddy**

7.1. Overview of Services

Comodo GeekBuddy includes the following services:

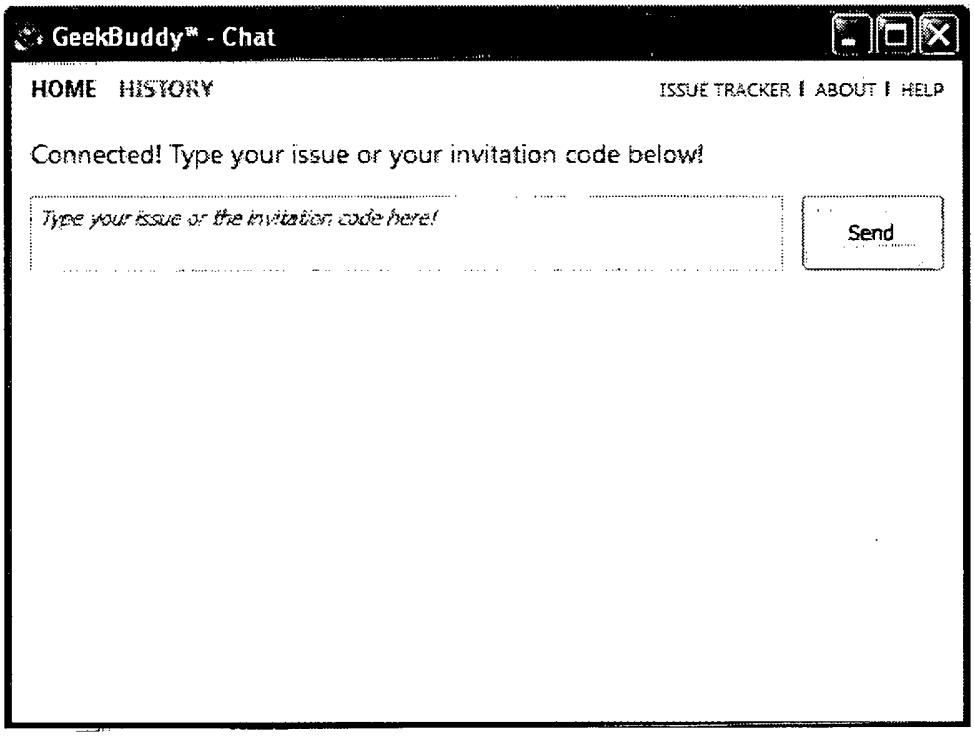
- **Virus & Malware Removal** - Our technicians remotely clear any detected viruses or malware that is found on your PC.
- **Internet and Online Identity Security** - Optimization of your computer's security settings to prevent loss of sensitive data and identity theft.
- **Printer or Email Account Setup** - Installation or updating of printer software and/or drivers, checking ink levels and configuring your printer to work on a wireless or wired network. We set up your Internet-based email account - any provider, any account. Great for new computers and novice email users.
- **Software Activation** - Installation, configuration, and activation of third party software in your system.
- **General PC Troubleshooting** - Detailed system check to identify and eliminate basic hardware and software conflicts in your Windows PC.
- **Computer Power Setting Optimization** - Optimization of your power management settings based on how you use your computer. Your Geek will help you go green and save money on your electric bill.
- **Comodo Software Installation and Set up** - Installation and support of software supplied by Comodo.
- **Comodo Account Questions** - Clarification of any doubts regarding your account in Comodo.

7.2. Activation of Service

GeekBuddy is included in CIS Pro and Complete versions and users who purchased either of these CIS versions can skip this section and move on to the next section **'Launching the Client and Using the Service'**. GeekBuddy client is downloaded along with CIS Premium (a free version) with a trial license, but to use the full service, you have to purchase and activate it.

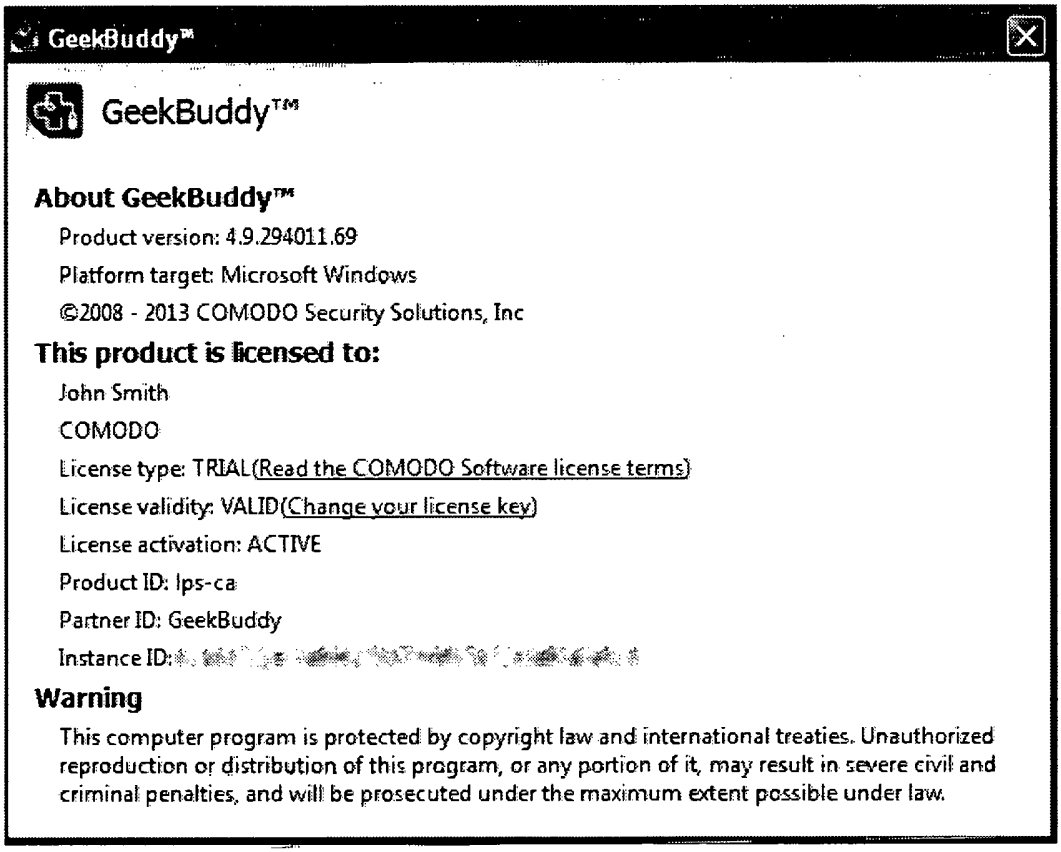
Start the GeekBuddy client by clicking the desktop shortcut icon  or from the 'Start Menu'.

The GeekBuddy Chat screen will be displayed.



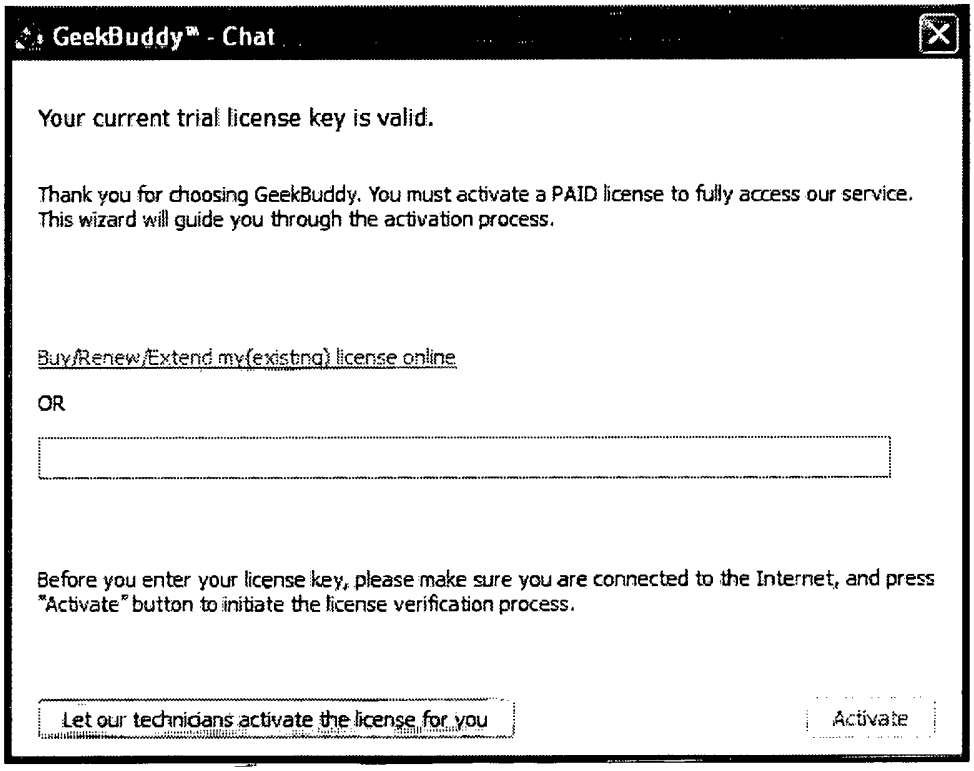
- Click the 'About' link at the top far right of the screen.

The About GeekBuddy screen will be displayed.

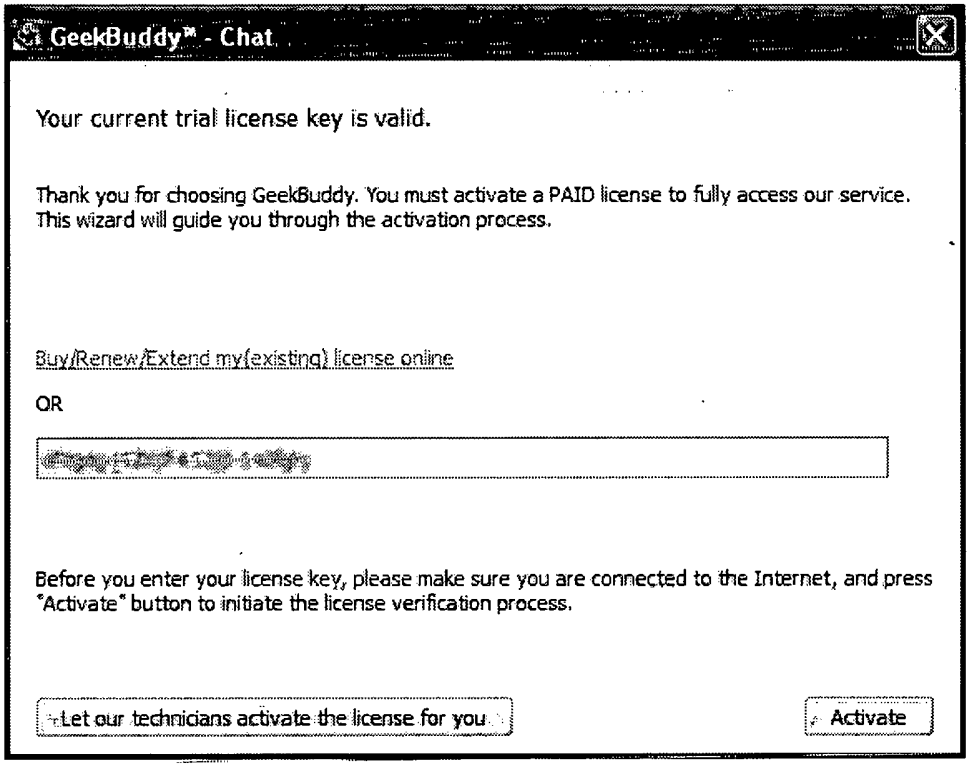


- Click the 'Change your license key' link in the screen.

The 'Activate your License' screen will be displayed.

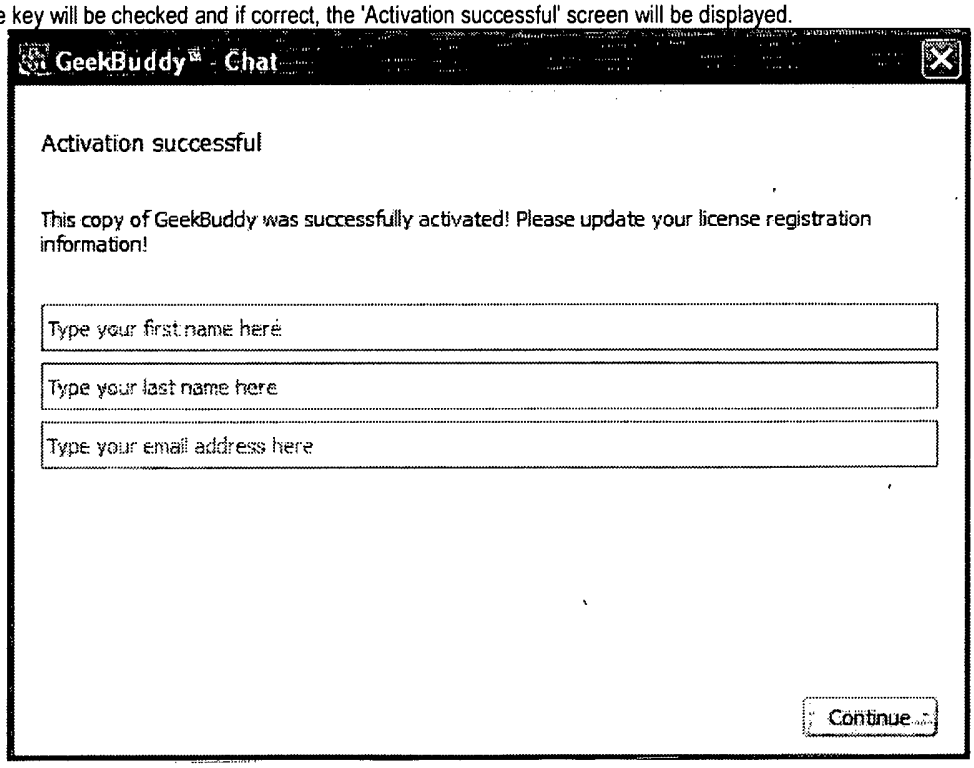


- Enter the License Key from your GeekBuddy retail package or the key you received through your email (for online purchases).

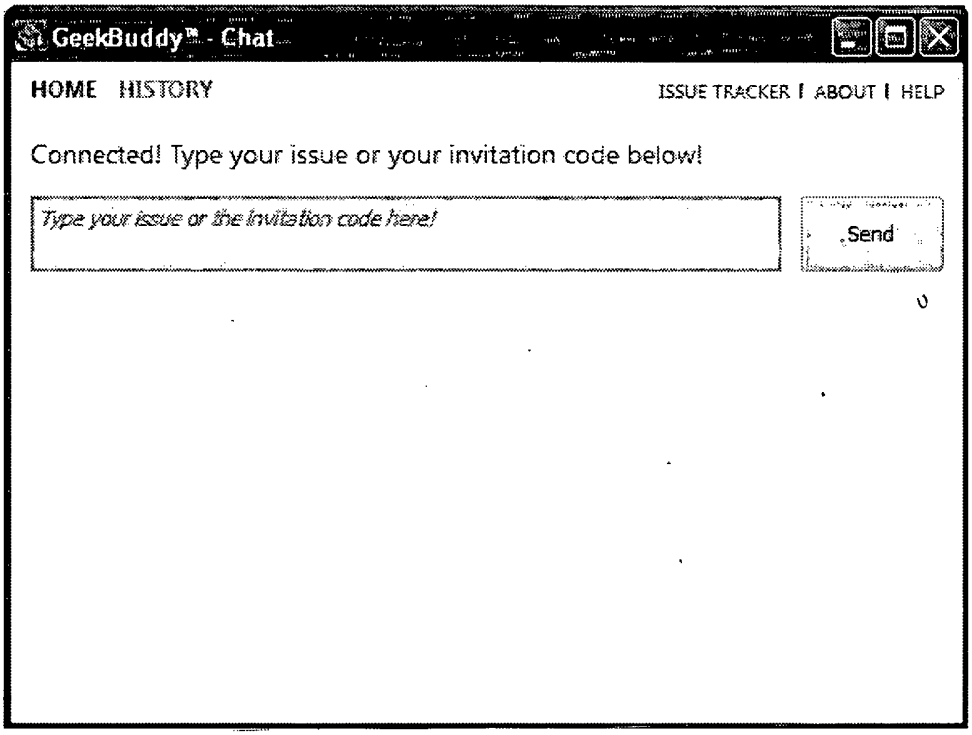


- Click the 'Activate' button or if you need more help on this click the 'Let our technicians activate the license for you' button.

The license key will be checked and if correct, the 'Activation successful' screen will be displayed.



- Enter the name and email details in the respective fields.
- Click 'Continue'.



The home page of GeekBuddy will be displayed. Now you can start using it and seek the help of an expert to resolve your computer problems.

Click the following links for more details on how to start and using them:

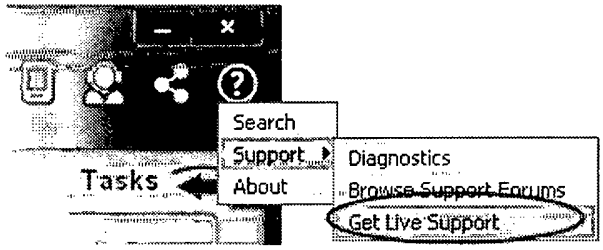
- **Launching the Client and Using the Service**
- **Using Issue Tracker**

7.3. Launching the Client and Using the Service

The GeekBuddy client required for the services is installed in your system automatically along with CIS Pro and Complete. For CIS Premium, it is installed automatically if you have selected the option Install Comodo GeekBuddy during installation .

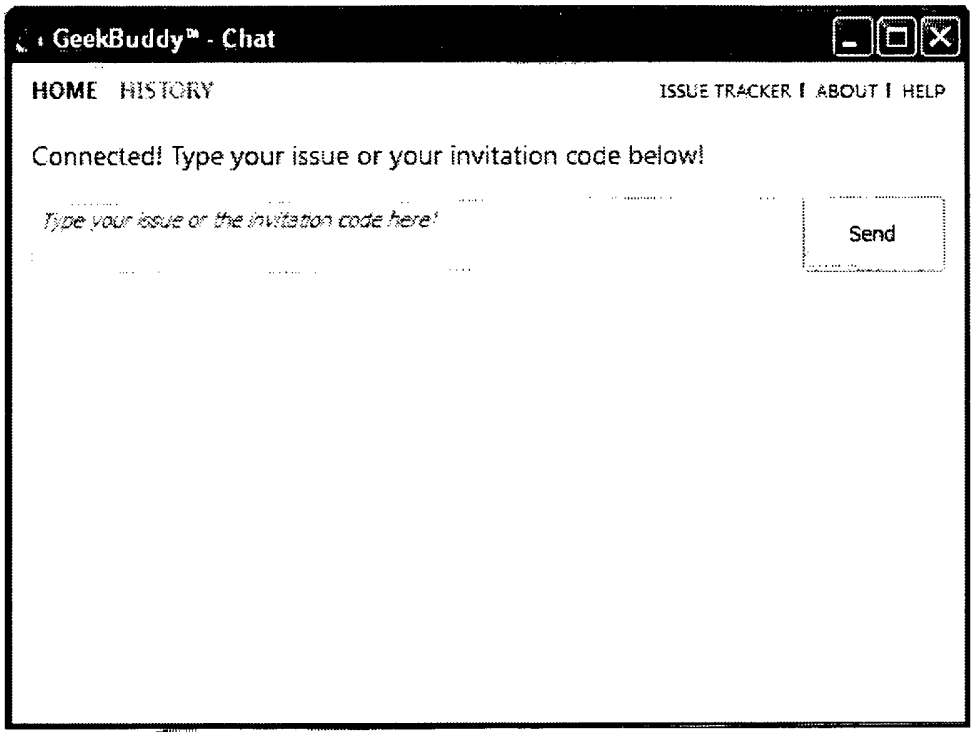
You can start the client and start a live chat session with a GeekBuddy expert using any one of the following methods:

- Double click the GeekBuddy desktop icon 
- Launch a chat with a qualified computer support technician by clicking this  icon in the title bar controls at the top right side of the main interface.
- Launch a chat with a qualified computer support technician by clicking Help > Support > Get Live Support at the top right side of the main interface.



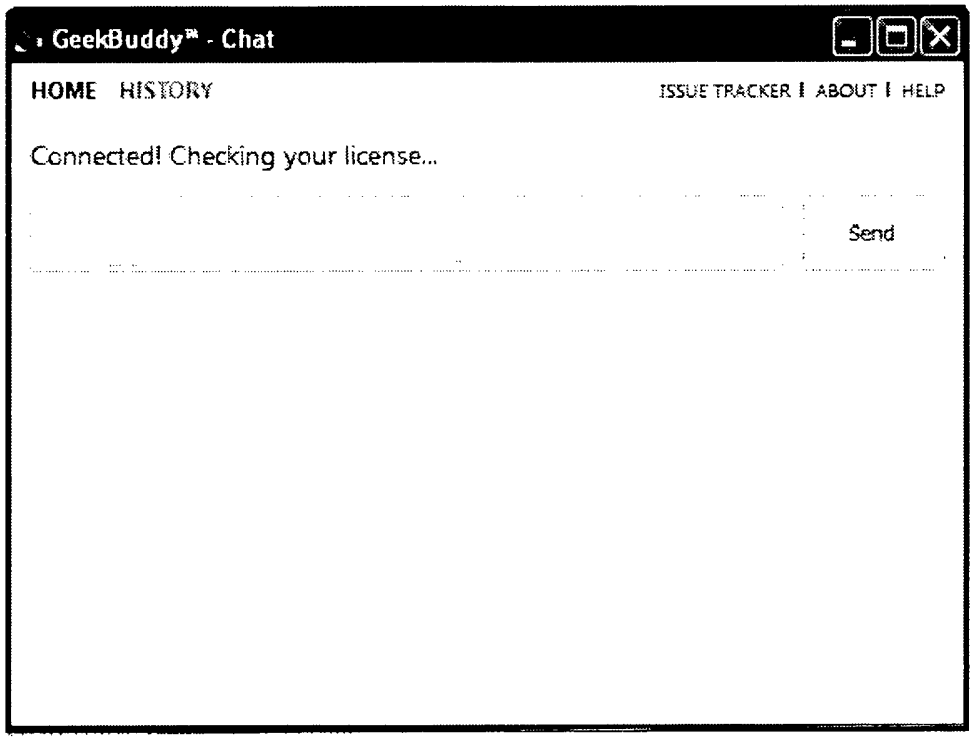
- Launch the GeekBuddy client directly from the Windows Start Menu - Click Start > All Programs > Comodo > GeekBuddy > GeekBuddy.

The GeekBuddy Home screen will open.

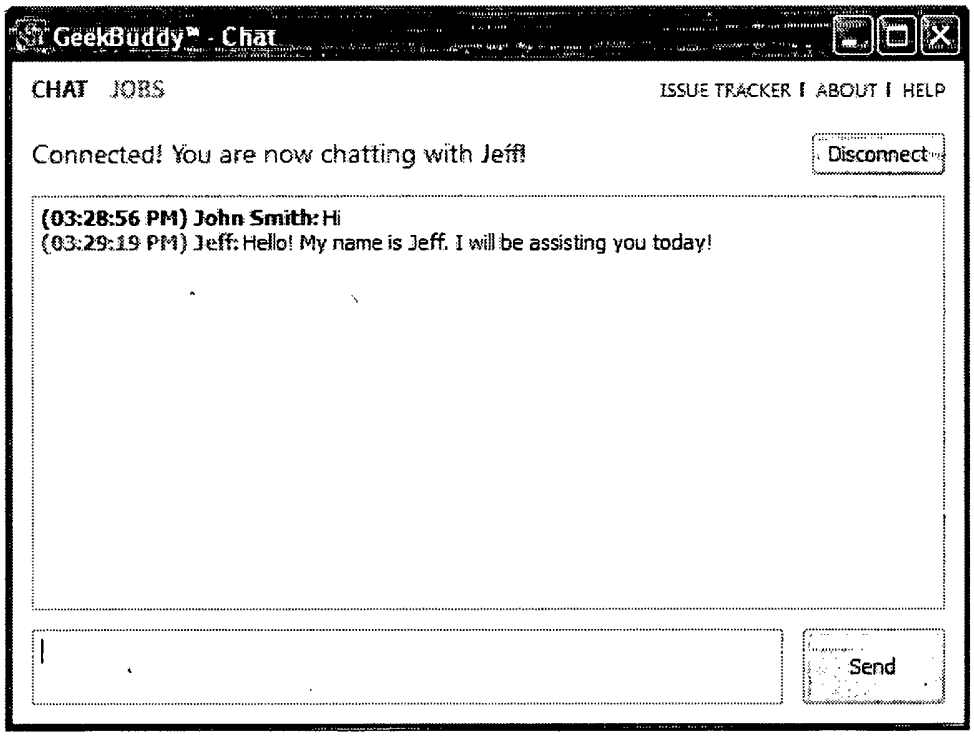


- To contact a support technician, type your issue in the field or enter the invitation code if you have it and click the 'Send' button.

You will be connected to a GeekBuddy...



...and once the connection is established, our support technician will initiate a chat with you.

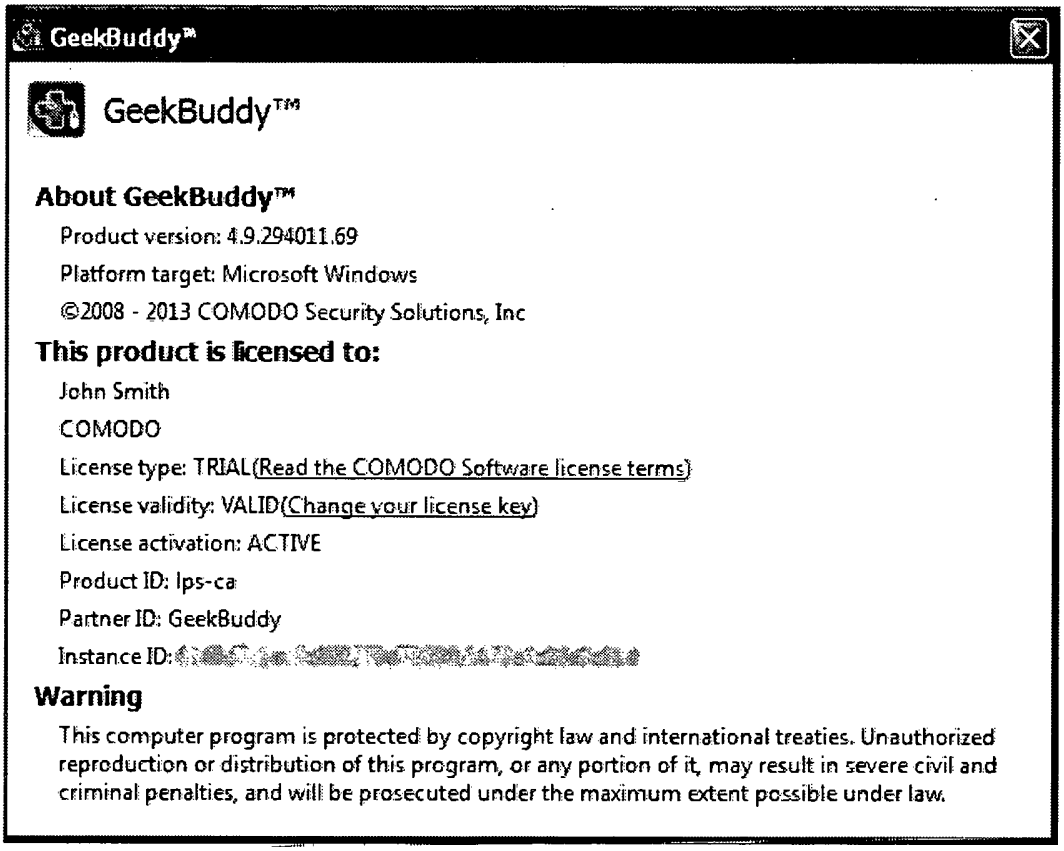


- Proceed to chat now.
- Explain your problem. The technician will assess your problem with you and work with you to fix any issues.

About GeekBuddy

- Click the 'About' link at the top far right of the screen.

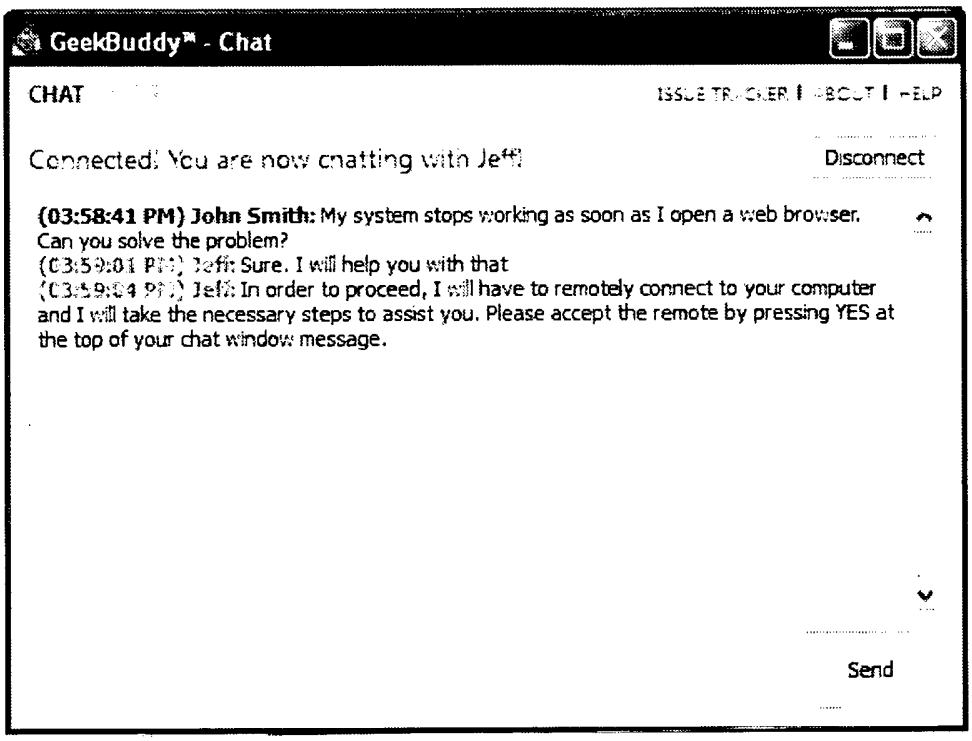
The About GeekBuddy information screen will be displayed.



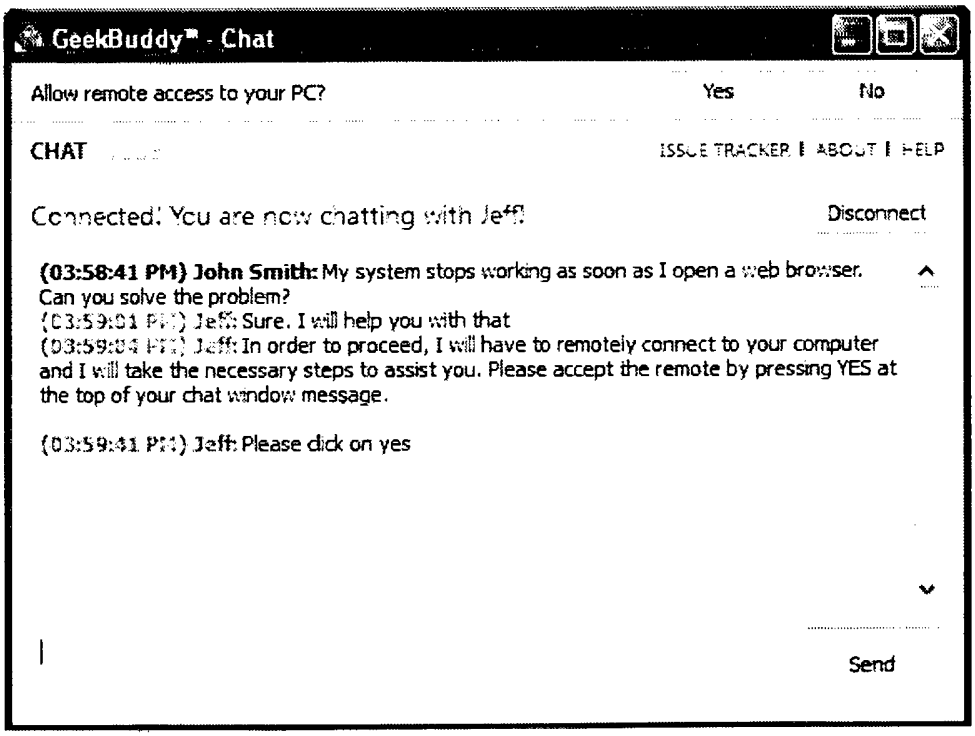
The 'About' dialog displays the copyright and product version information. The screen also displays information about the licensee, its validity and to change the license key or activate the account.

7.4. Accepting Remote Desktop Requests

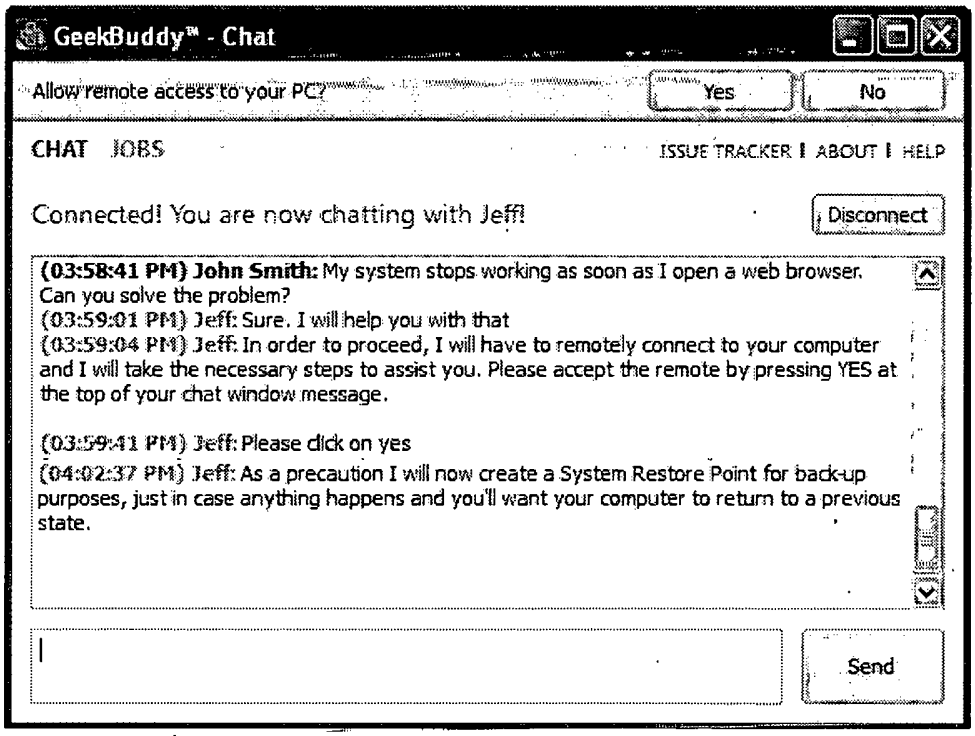
In order to solve certain issues, the support technician may need to directly connect to your computer via aremote connection. Remote control can only go ahead if you grant permission for this to happen. Our technicians will always request your permission via the chat window.



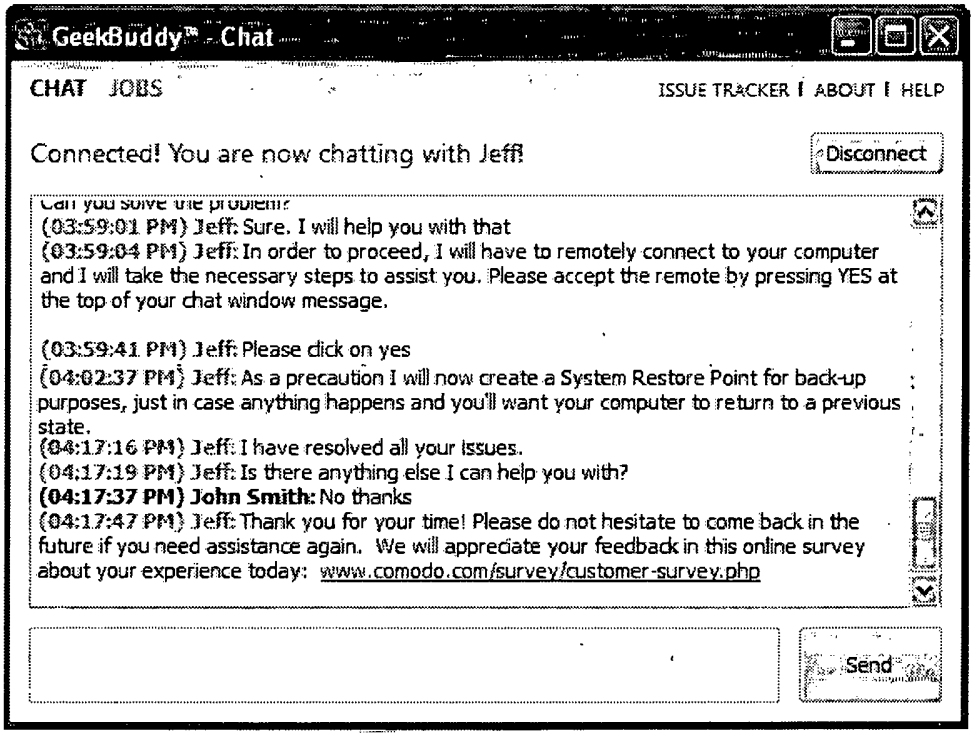
The technician will ask your permission before he or she makes any changes to your machine. Such changes might include installing programs, creating system restore points or deleting unnecessary or infected files.



- Click the 'Yes' button at the top of the interface in order to allow the technician to connect to your computer.



Upon completion of their work, the technician will disconnect from your computer, inform you that the requested tasks have been completed and ask whether you would like help with anything else.



- Click the 'Disconnect' button and confirm it in the next screen to end the session with our GeekBuddy.

Congratulations, you just finished your first GeekBuddy support session. We hope you enjoy using your trouble-free computer.

7.5. Chat History

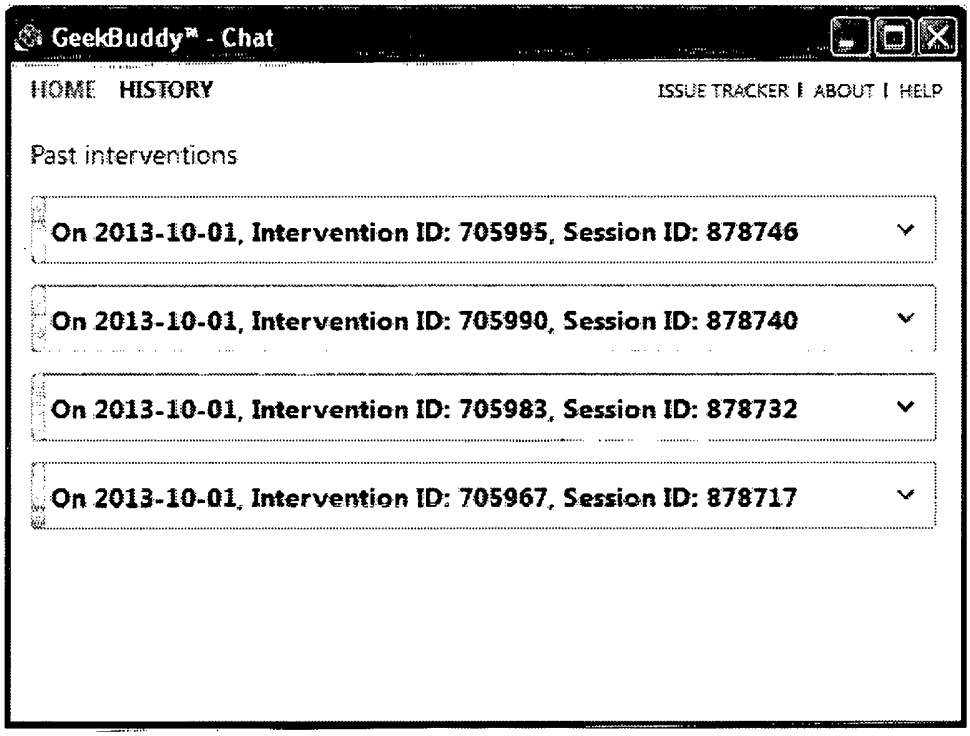
GeekBuddy keeps a local record of every chat session you have with a Comodo technician. Clicking the 'History' link at the top

of the interface will display all chat sessions that you had with our technician. This helps you keep track of previous computer issues and chats and can be useful as a reference when trying to fix future issues.

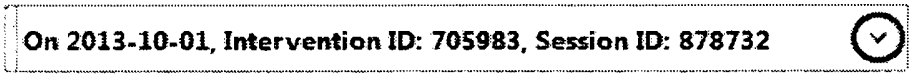
To view history of chat sessions

- Click the 'History' link at the top of the interface.

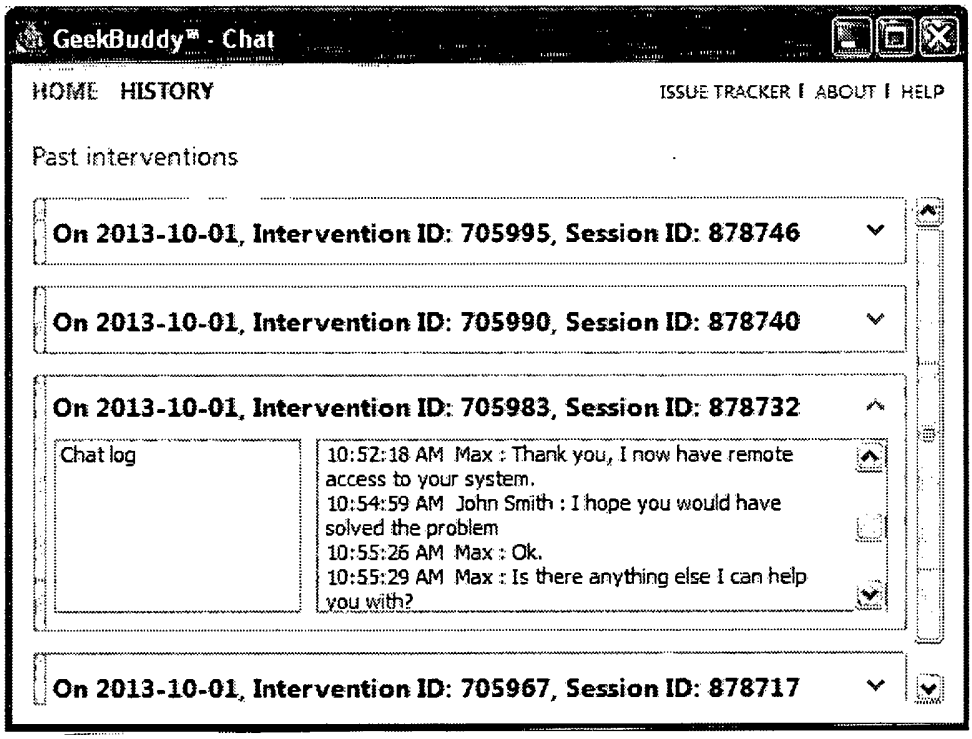
All the sessions will be displayed.



- Click on the arrow button at the far end of the session history box that you want to view or double-click anywhere on the box.



- The chat session that you had with our technician will be displayed on the right side.

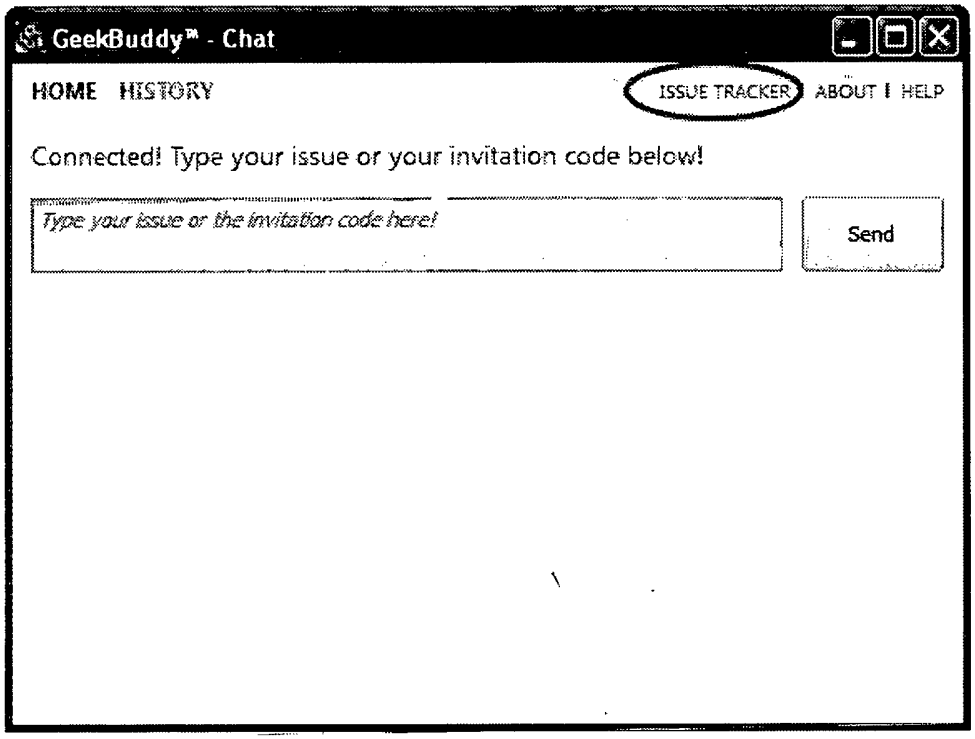


Similarly you can view the chat history of other sessions also.

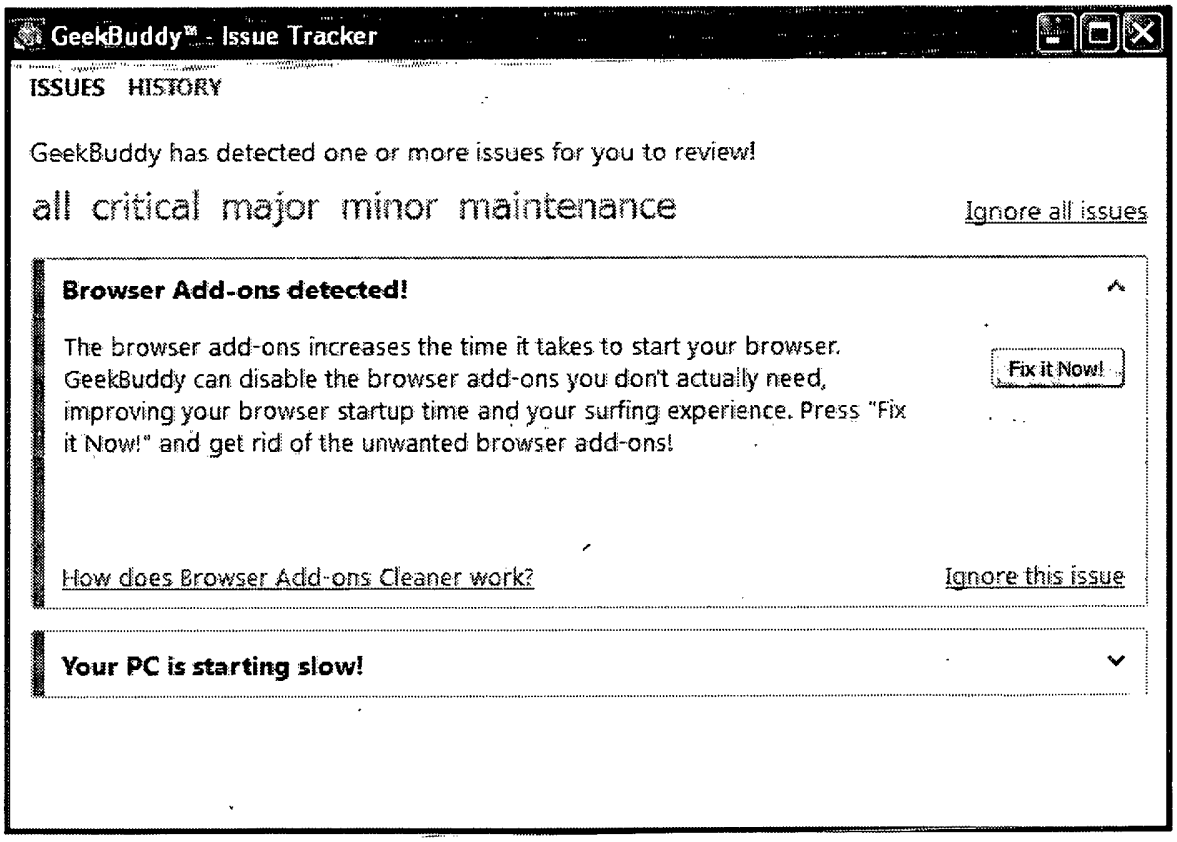
7.6. Using Issue Tracker

Issue Tracker helps you maintain the security and efficiency of your computer by automatically identifying problems on your computer and helping you to fix them. For example, Issue Tracker will alert you if you have too many startup programs/services (can cause computer slow down); an inefficient registry (can also cause slow down and crashes) or your hard drive contains files that might compromise your privacy. In many cases you will be presented with a simple wizard that will allow you to deal with the issue quickly and easily. If the problem is beyond the scope of Issuer Tracker, you will be offered the opportunity to contact a GeekBuddy representative who will help resolve the issues.

To start the Issue Tracker, click the 'Issue Tracker' link on the right top in the user interface.



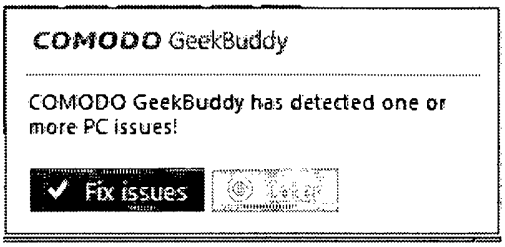
The Issue Tracker interface will list the problems that it has detected.



Popup Alert

At the time of starting your computer, Issue Tracker will detect problems in your system and provide an alert at the bottom right

side of the screen.



- Click the Fix issues to open the Issue Tracker interface.

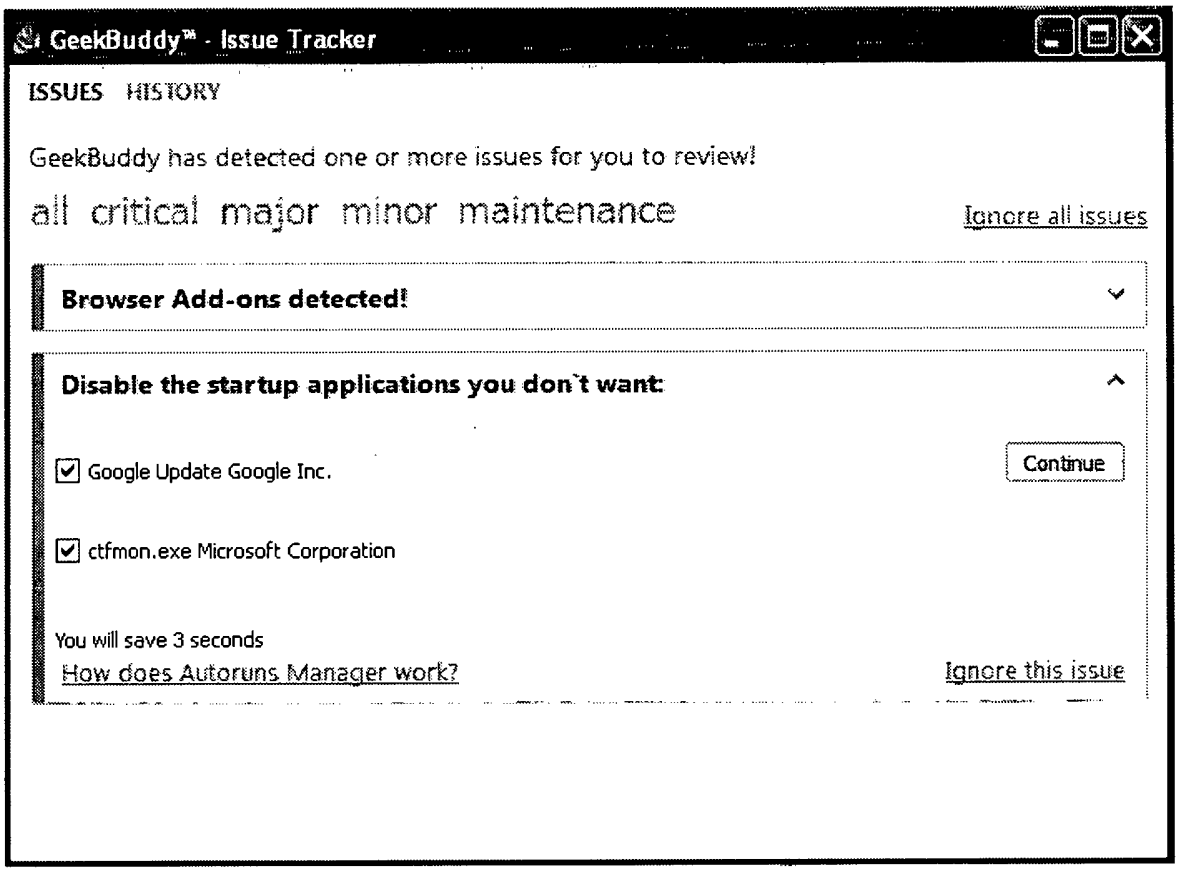
The Issue Tracker interface will list the problems that it has detected.

The problems detected will be categorized as critical, major, minor and maintenance issues. Click on the relevant link to view the problem. Clicking the 'Show all issues' link will display all the problems in your computer and the color code at the left of each issue indicates the category of the issue.

S. No.	Issue	Color Code
1	Critical	Red
2	Major	Orange
3	Minor	Yellow
4	Maintenance	Blue

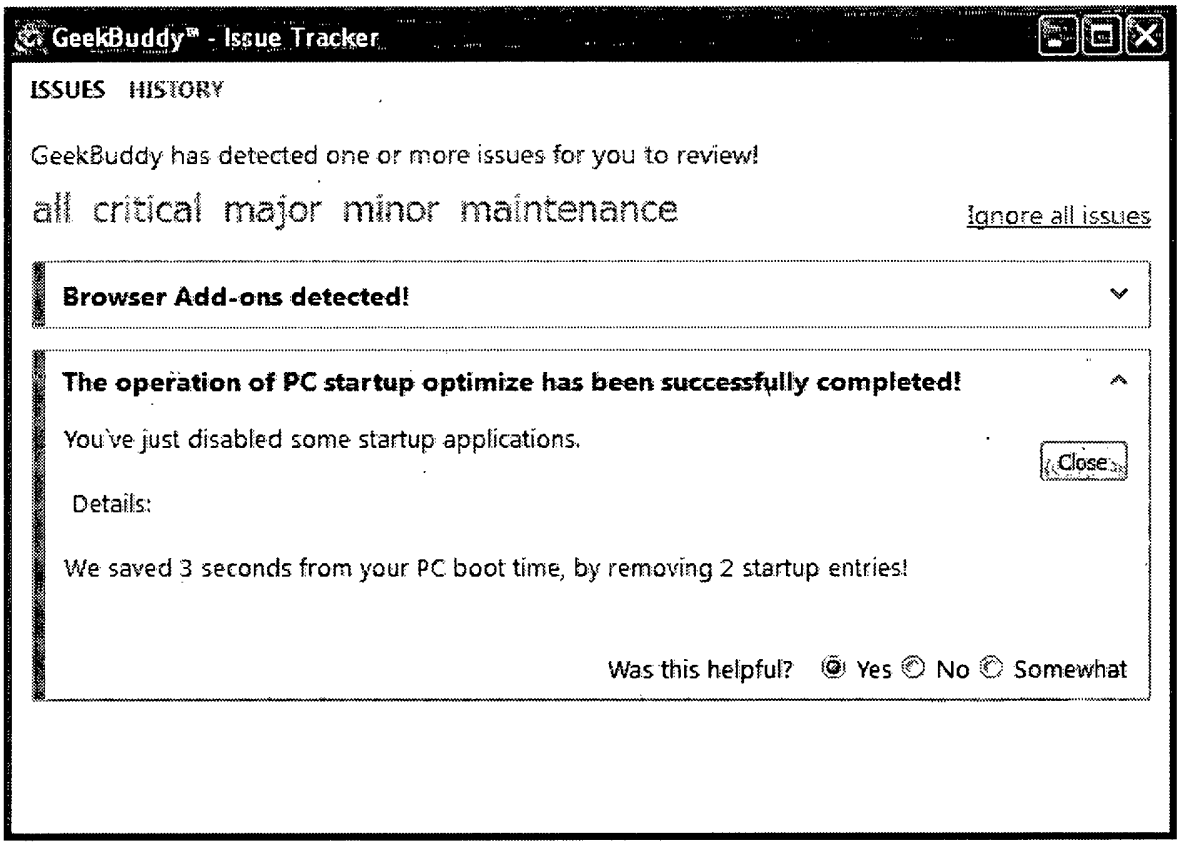
Some of the common problems that occur in any computer are junk registry entries, slow bootup time and the presence of files that might compromise your privacy.

Each issue discovered will be accompanied with a 'Fix it Now' button. For example, for the issue of slow bootup time, clicking this button will display a list of startup programs in your system (programs which are automatically loaded during Windows start-up and will running in the background). You can identify the programs you do not want to run at start-up and disable them. Doing so will save system resources and improve the performance of your computer.



- Select the programs that you want to disable during startup and click the 'Continue' button.

The selected programs will be disabled and the successfully completed screen will be displayed.



- Provide your feedback at the bottom of the interface and click the 'Close' button.

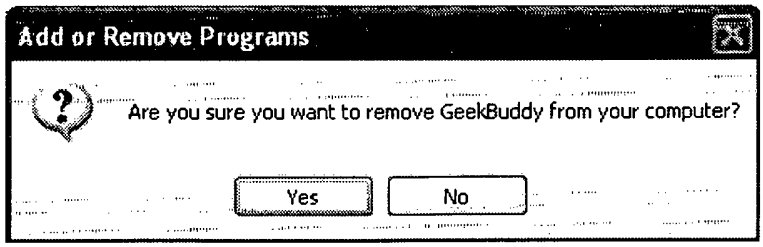
For some of the issues listed, you have to seek the help of an expert technician.

- Click 'Ignore all issues' link to disregard all the issues in your system displayed by Issue Tracker.
- Click 'Ignore this issue' beside a particular entry to disregard that problem.
- Click 'History' link at the top of the interface to view the actions taken for the problems.
- Click the 'Fix it Now!' button beside an issue to resolve it.

7.7. Uninstalling Comodo GeekBuddy

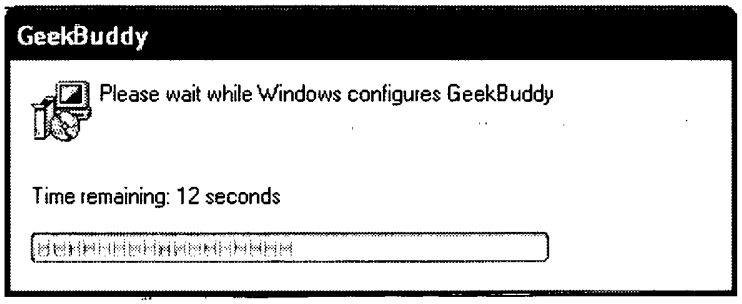
To uninstall Comodo GeekBuddy

- Click Start > Control Panel
- In the Control Panel, double-click Add/Remove Programs
- In the list of currently installed programs, click GeekBuddy
- Click the 'Change/Remove' button.



- Click 'Yes' to confirm uninstallation.

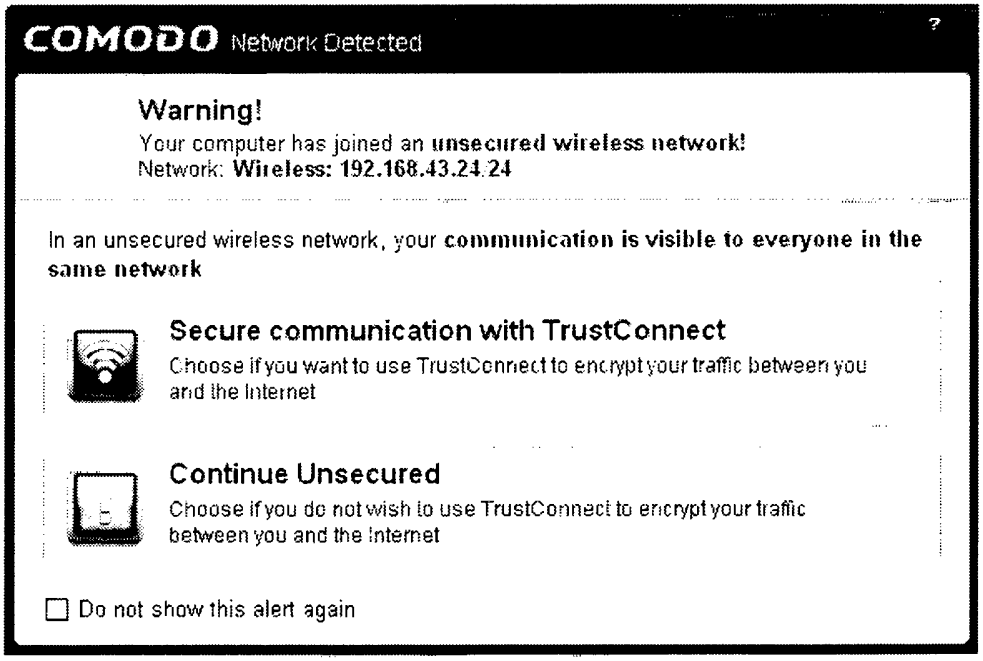
The progress of GeekBuddy removal will be displayed...



---and after a few minutes the uninstallation will be complete.

8. TrustConnect Overview

Comodo TrustConnect is a secure Internet proxy service that creates an encrypted session when users are accessing the Internet over public wireless connections. Since these wireless sessions can be relatively easily intercepted, they present a significant data vulnerability gap for businesses and consumers alike. Whenever Comodo Internet Security detects unsecured wireless connections it will present you with the opportunity to use your TrustConnect account for the connection.



TrustConnect is designed to eliminate these types of data hijacks by preventing criminals from attacking or scanning your system from the local network that you are using to connect to the Internet. It also encrypts all of your traffic destined for the Internet (including Web site addresses, instant messaging conversations, personal information, plain text usernames and passwords and other important information). After connecting to the service, the TrustConnect software indicates that traffic is being encrypted as it leaves your system. Data thieves and hackers cannot 'sniff' or intercept your data - they can't even determine where your information is coming from because, as you are connecting to the Internet through a SSL secured VPN connection to the TrustConnect servers, your requests appear to come from our IP address. Ordinarily, cyber criminals could easily intercept these broadcasts.

Setting up Comodo TrustConnect is easy, as it works on most operating systems (Windows, Mac OS X) as well as with most firewall applications. Typical setup takes less than three minutes. TrustConnect clients are available for Windows, Mac OS, Linux

and iPhone mobile devices and can be downloaded by logging into your account at **https://accounts.comodo.com/account/login**. Your Comodo Internet Security Complete confirmation email contains confirmation of your the username that you set up during initial sign up and a subscription ID for the service. Once logged in, click the TrustConnect tab to add subscriptions, change billing and contact information, and review the ongoing status of your service. Your Comodo Internet Security Complete TrustConnect account has a 10 GB/month data transfer limit.

Comodo Internet Security - Complete customers also receive the $99 value 'Live, Expert Computer Support' Comodo GeekBuddy. Please visit **http://www.geekbuddy.com** for full product details.

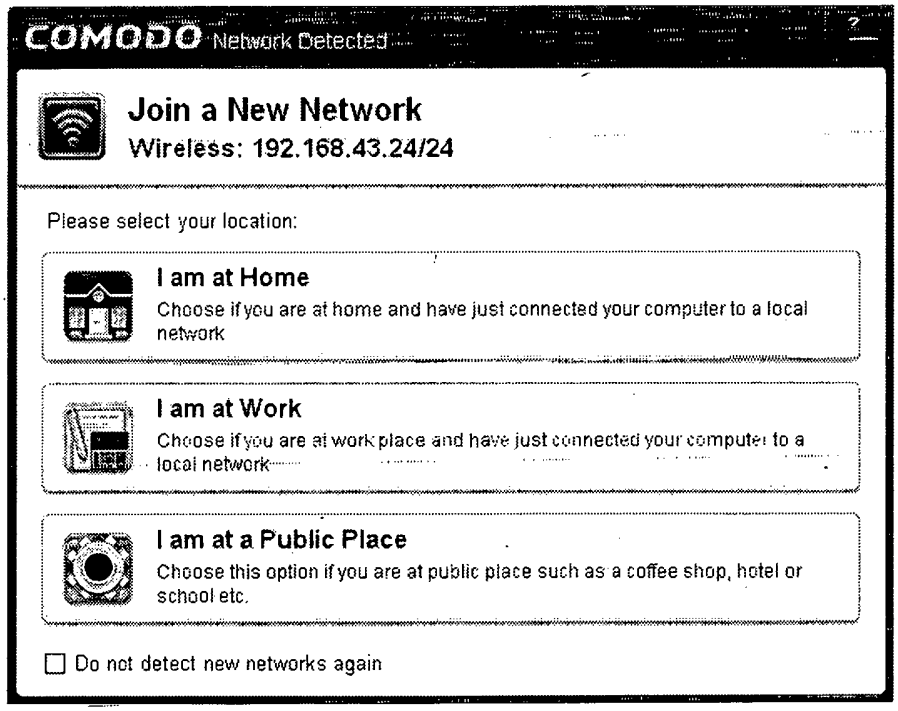
TrustConnect System Requirements

- Windows 8
- Windows 7
- Windows Vista
- Windows XP
- Mac OS X
- Linux (containing kernel 2.4 or later)
- FreeBSD, OpenBSD

For users of Comodo Internet Security - Complete, TrustConnect is integrated with the application and need not install the TC client in their systems.

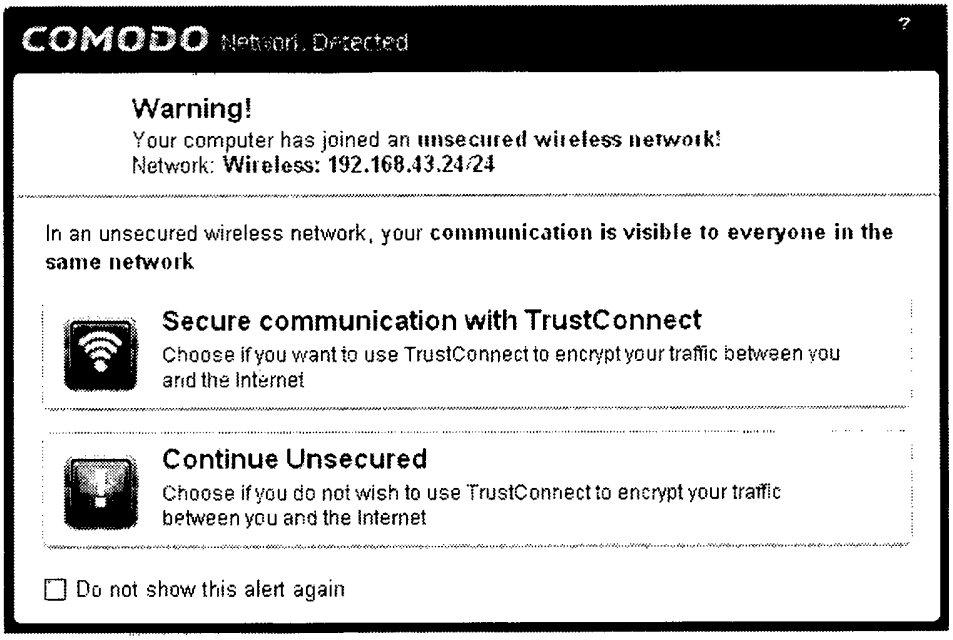
Comodo Internet Security Complete Users

CIS Complete product includes TrustConnect service and the application is installed automatically along with CIS. When a new wireless connection is established by your system, a Network Detected dialog will be displayed.



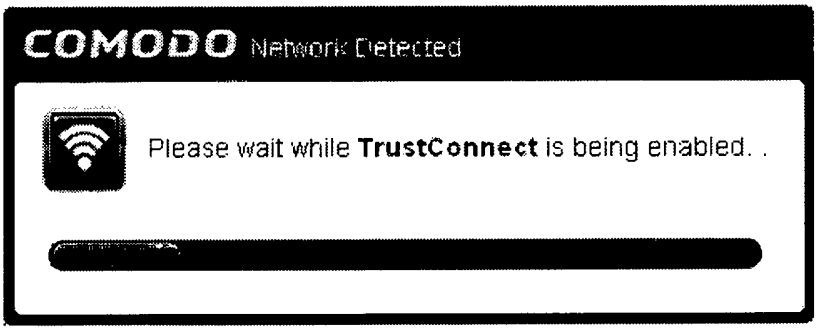
- Select your location from the dialog

A TrustConnect alert will be displayed depending on the settings configured in **Firewall Behavior Settings** interface.



Select whether you want to connect to the Internet via TrustConnect thus encrypting the traffic between your system and the Internet or use the unsecured network.

If you choose 'Secure communication with TrustConnect', CIS will establish the connection via TC...



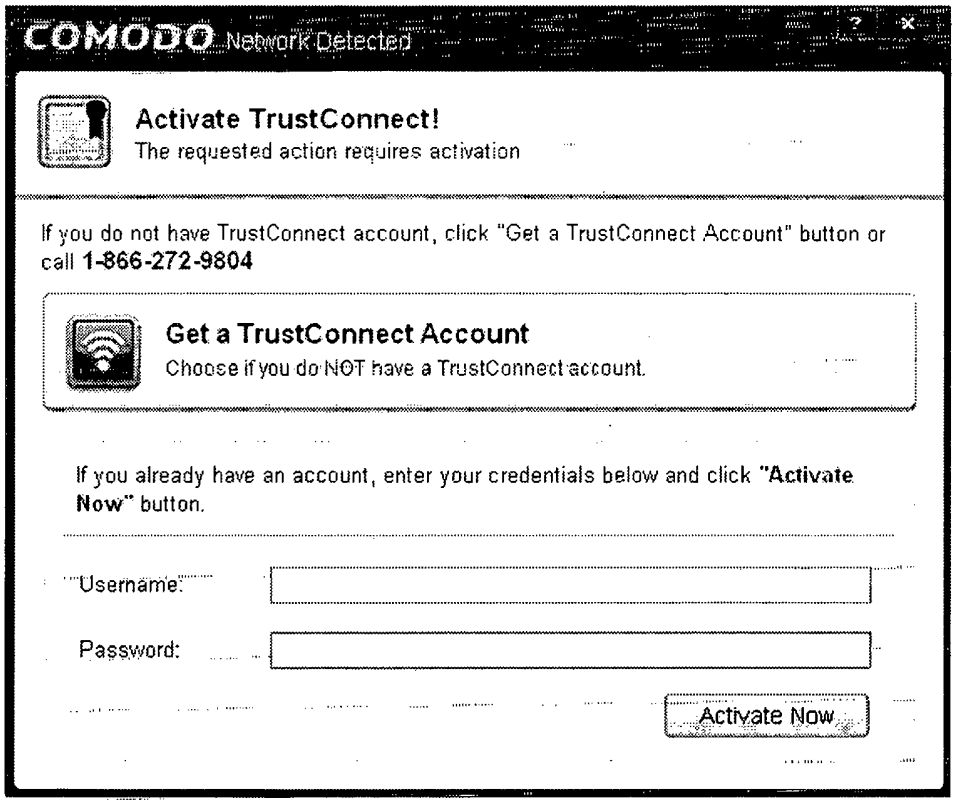
...and on successful connection, you can view the details in the system tray.



Choose 'Continue Unsecured' option if you do not want to establish an encrypted connection.

Comodo Internet Security Pro / Premium Users

TrustConnect service is not included with CIS Pro / Premium and these users should subscribe for using the service. When the option 'Secure communication with TrustConnect is selected, a 'Activate TrustConnect' dialog will be displayed.

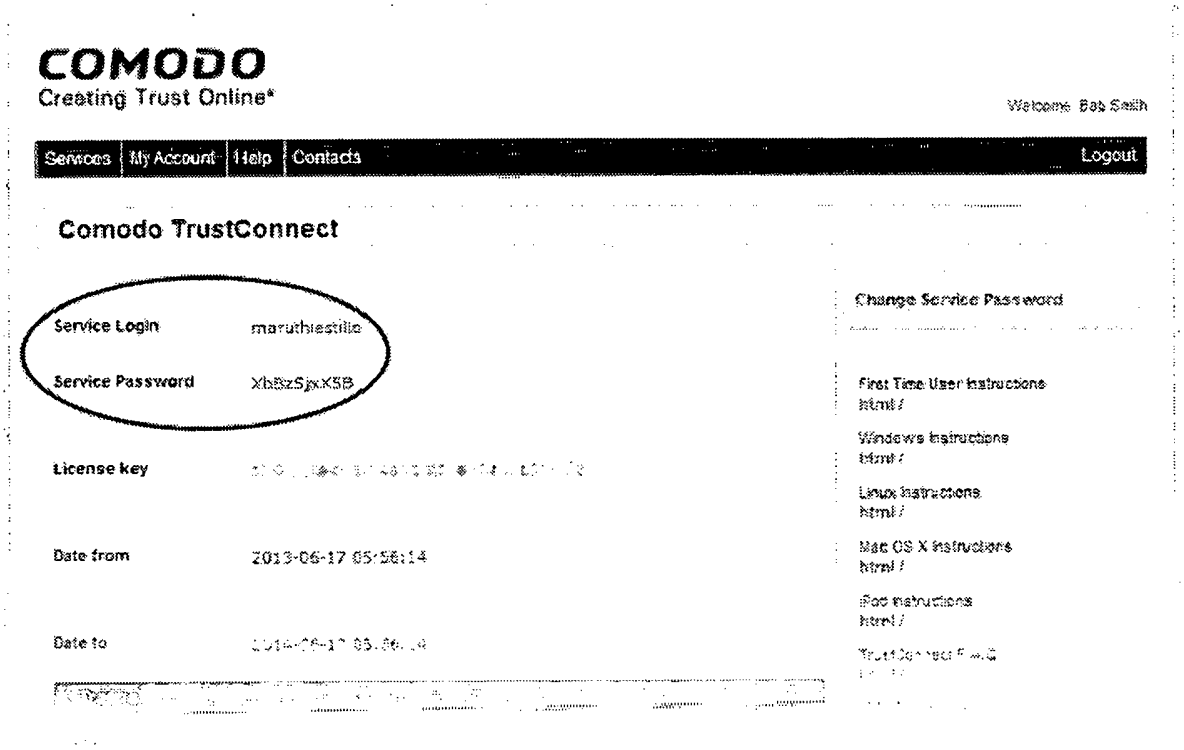


- You can purchase the TC service by clicking the 'Get a TrustConnect Account', enter the TC service credentials and activate the service.
- If you already have a TC account, enter the TC service credentials in the Username and Password fields and click the 'Activate Now' button.

To find your TC service credentials

- In the **https://accounts.comodo.com/** page login to your CAM account using the CAM username and password sent via email at the time of account creation.
- Click 'TrustConnect' in the menu bar or in the drop down from 'Services' tab.

The account details of your TC service will be displayed.



The TC Service Login and Service Password for your account should be entered in the Username and Password fields respectively in the 'Activate TrustConnect' dialog.

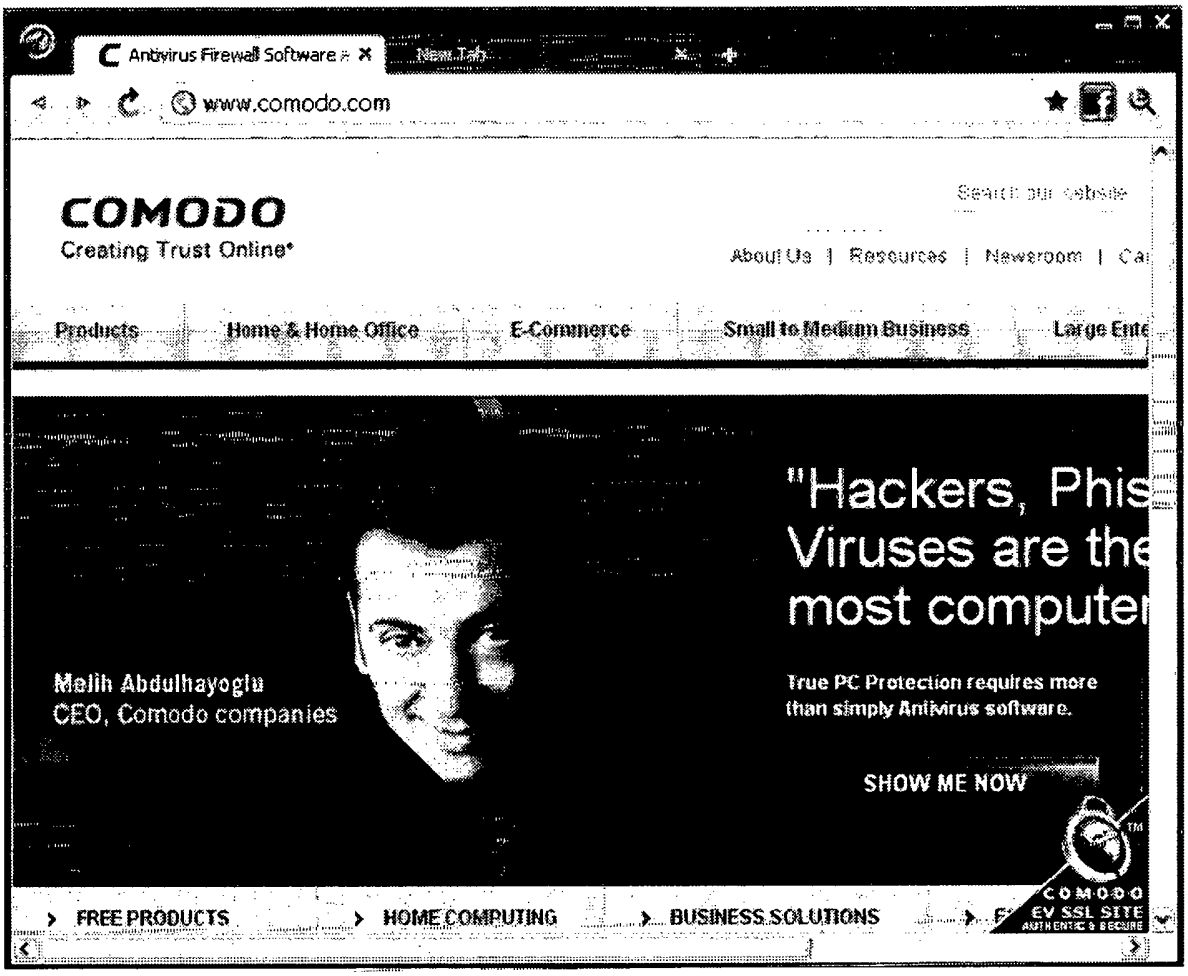
Please note that this activation dialog will appear only for the first time you are trying to connect via TC. After the activation process is successfully completed, subsequent attempts to connect via TC to the Internet will be automatically established.

9. Comodo Dragon

Comodo Dragon is a fast and versatile Internet Browser based on Chromium and infused with Comodo's unparalleled level of security.

To help make your Internet browsing experience even safer, Comodo Dragon is installed on your computer as a part of Comodo Internet Security. Comodo Dragon gives you the complete complement of features offered by Chromium with superior security and privacy.

- **Comodo Dragon Features**
- **Starting Comodo Dragon**
- **Comodo Dragon Help**



Features:

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

Comodo Dragon Security:

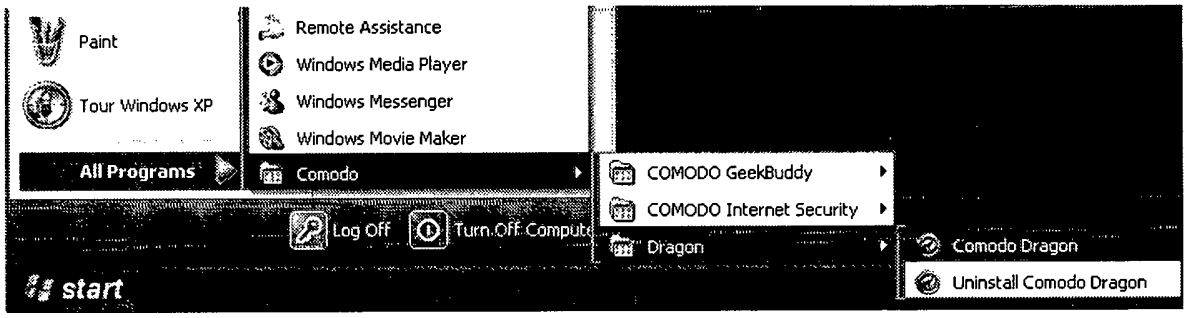
- Has privacy enhancements that surpass those in Chromium's technology
- Has Domain Validation technology that identifies and segregates superior SSL certificates from inferior ones
- Stops cookies and other Web spies
- PrivDog can disable cookies, spyware, malware and other trackers.
- Prevents all Browser download tracking to ensure your privacy

Starting Comodo Dragon

Comodo Dragon is installed in your computer along with Comodo Internet Security 2013. You can start the browser in two ways:

From the Start menu:

- Click Start > All Programs > Comodo > Dragon > Comodo Dragon:



From the Destop Icon:

- Double Click on the Comodo Dragon Desktop icon created during the installation:



9.1. Introduction to PrivDog

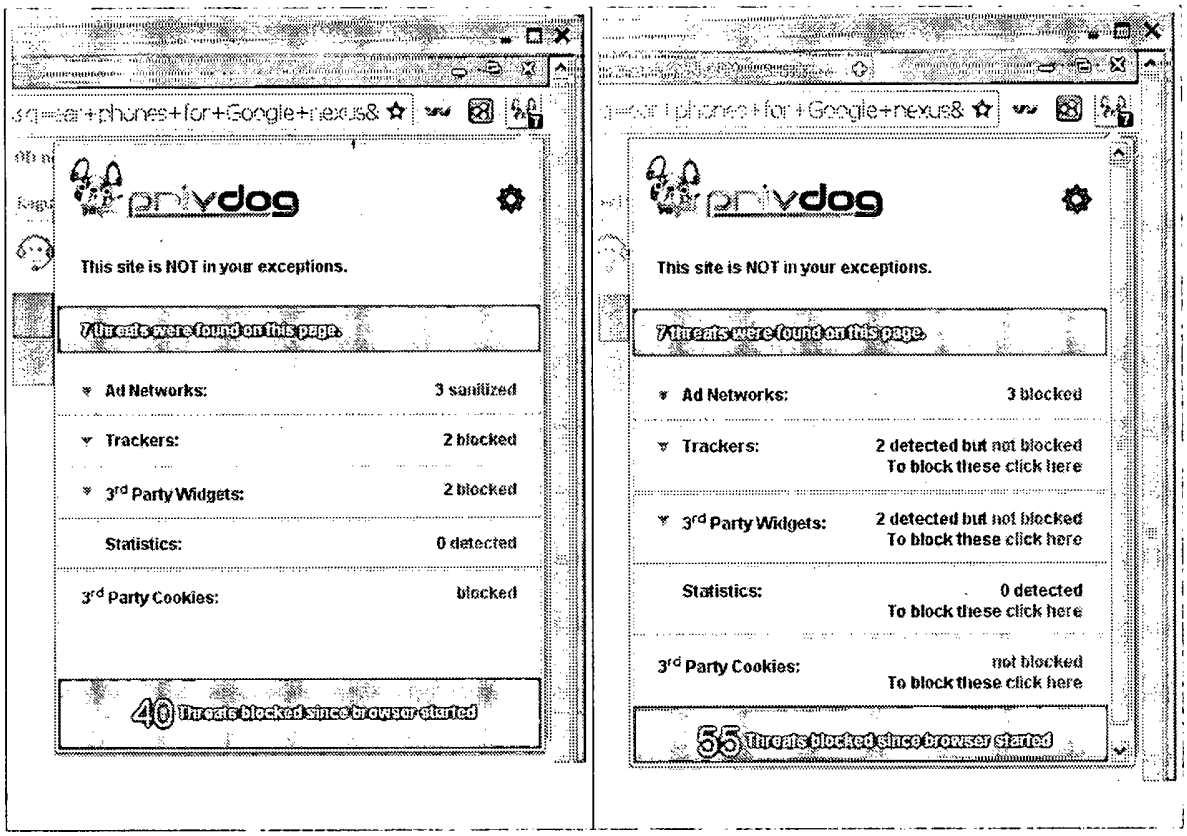
What would be your reaction if you knew that almost all your online activity was tracked by multiple agencies without your knowledge? The data they collect might be used for legitimate but unwelcome reasons such as adverts that follow you around the internet or for creating a profile of your online browsing activity. In the worst cases, it could be used by online fraudsters with the sole objective of stealing your personal and confidential information by deploying intelligence gathering cookies, spyware and other malware.

PrivDog provides you the power to control these activities and make surfing the web safe and private again. PrivDog is a browser extension that improves the transparency, privacy and speed of your online experience by automatically detecting and blocking processes that are attempting to track your online activity. Whenever you visit a website, PrivDog will display the number of privacy threats it has blocked in the top-right corner of your browser. Clicking the PrivDog icon will reveal a more detailed breakdown of the types of threats it has stopped, which can include advertising networks, 3rd party trackers, cookies, widgets and other data collection processes. The extension can also block all current banner ads in a webpage and replace them with safe and trusted ads.

You can install PrivDog while installing Comodo Internet Security or by downloading the app from **www.privdog.com/downloads.html**. The supported browsers for PrivDog include Comodo Dragon, Comodo IceDragon, Google Chrome and Mozilla Firefox.

9.1.1. Using PrivDog

- The total number of potential threats on the page you are visiting will be overlaid over the PrivDog icon at the top-right corner of the browser. Click the icon to reveal a breakdown of current activity by threat-type.



The bottom of the summary page states the total number of threats blocked for all pages in your current session.

Ad Networks - Displays the number of advertisements published by 3rd party ad networks that were replaced with ads from AdTrustMedia (sanitized) or completely blocked (blocked) depending on the settings configured. Clicking anywhere on the row will expand or collapse the list.

Trackers - Displays the number of trackers that were blocked or allowed for that page depending on the settings configured. Clicking anywhere on the row will expand or collapse the list.

3rd Party Widgets - Displays the number of widgets that were blocked or allowed for that page depending on the settings configured. Clicking anywhere on the row will expand or collapse the list.

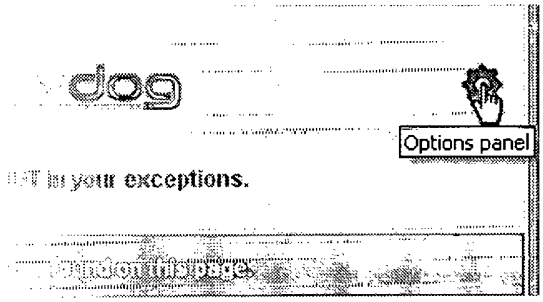
Statistics - Displays the number of analytical trackers that were blocked or allowed for that page depending on the settings configured. Clicking anywhere on the row will expand or collapse the list.

3rd Party Cookies - Displays whether 3rd party cookies are blocked or not depending on the settings configured.

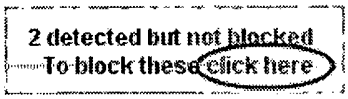
9.1.2. PrivDog Settings Configuration

The Options page allows you to configure the settings for the Trackers, 3rd Party Widgets, Ads, Statistics, Preferences and add websites to Exceptions list.

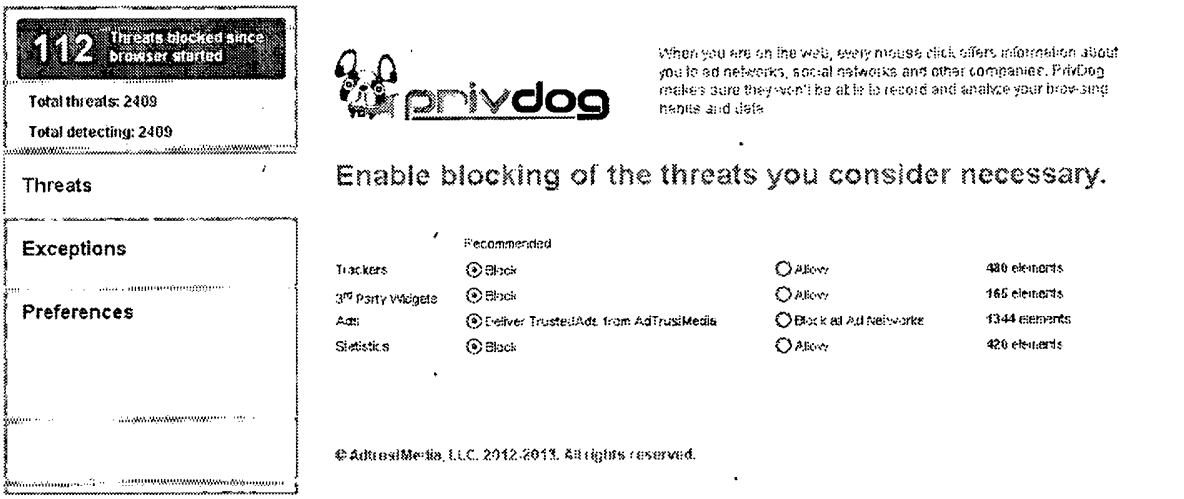
To open the Options Panel, click the PrivDog icon at the top right side of the browser and click the gear icon in the drop-down.



Alternatively, click on the words 'click here' in the row of a blocked item to go to the respective settings page directly.



The Options Panel displays the total number of threats that it has blocked since the browser was opened for the session and by default opens with the Threats settings page.

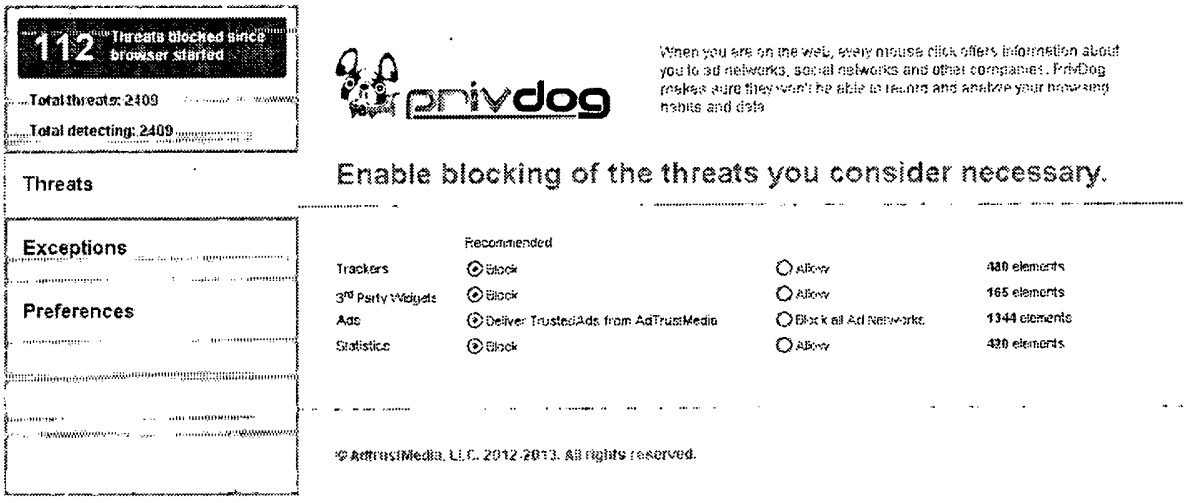


The panel allows you to configure the settings for:

- **Threats**
- **Exceptions**
- **Preferences**

9.1.3. Threats

The page displays the number of elements at the far end of each item that PrivDog has detected so far in the browser.

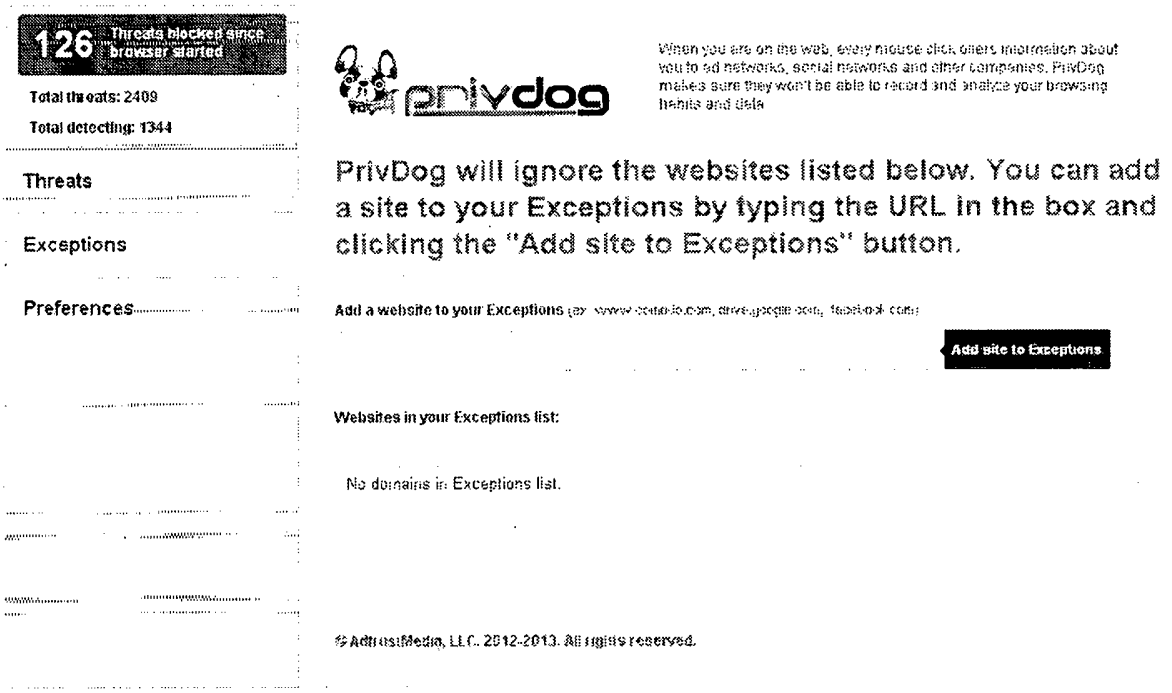


- Select the option whether to block or allow the items in the list.

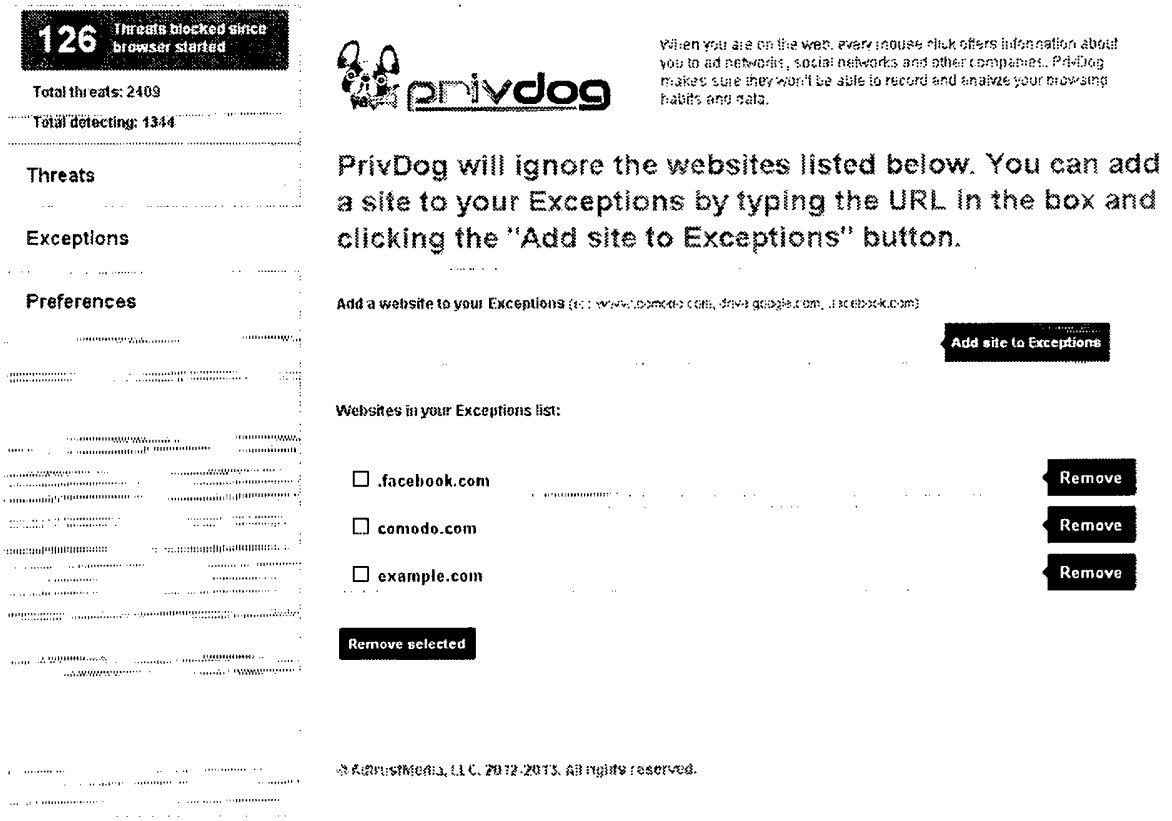
9.1.4. Exceptions

The Exceptions screen allows you add a domain name or a subdomain name for which PrivDog will not perform a scan to detect threats. You should make sure the websites that you add to the Exceptions list are trustworthy and dependable.

- Enter the url of the website(s) in the field and click the 'Add site to Exceptions' button.



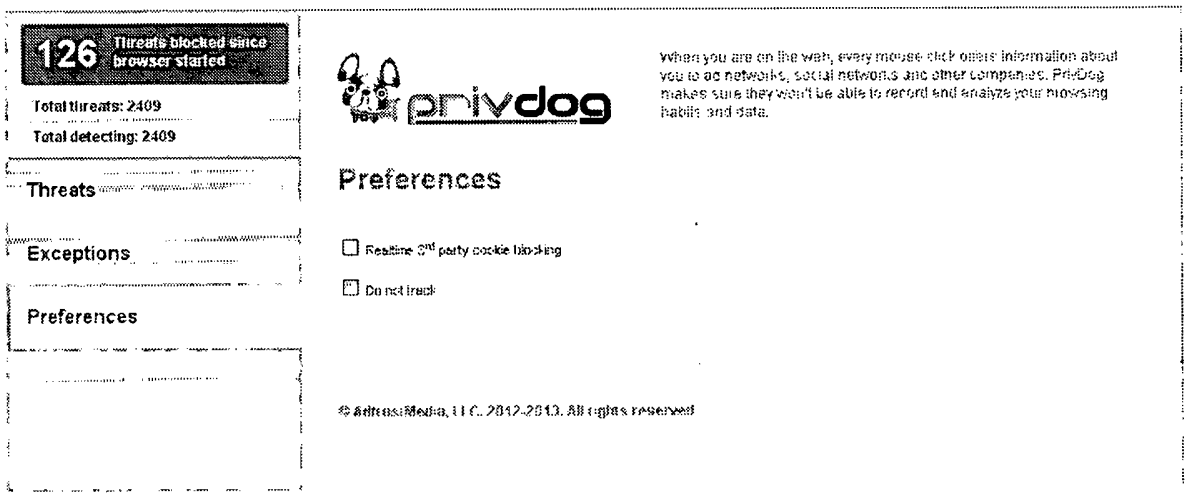
The added website(s) will displayed in the Exceptions list.



To remove a website from the Exceptions list, select the checkbox beside it and click the 'Remove' button beside it or click the 'Remove selected' button if you select more than one website.

9.1.5. Preferences

In the Preferences screen you can choose to either allow or block 3rd party cookies in the browser.



- **Realtime 3rd party cookie blocking** - When this option is enabled, PrivDog will check in realtime for 3rd party cookies that are being installed and block them.
- **Do not track** - When this option is enabled, PrivDog will block the tracking activities of 3rd party cookies that are already installed.

Comodo Dragon Help

Comodo Dragon's intuitive multi-tabbed interface enables easy and fast access to sophisticated features of the browser. Please refer to the Comodo Dragon online help guide at **http://help.comodo.com/topic-120-1-279-2524-Comodo-Dragon---Introduction.html** for more details on using the browser.

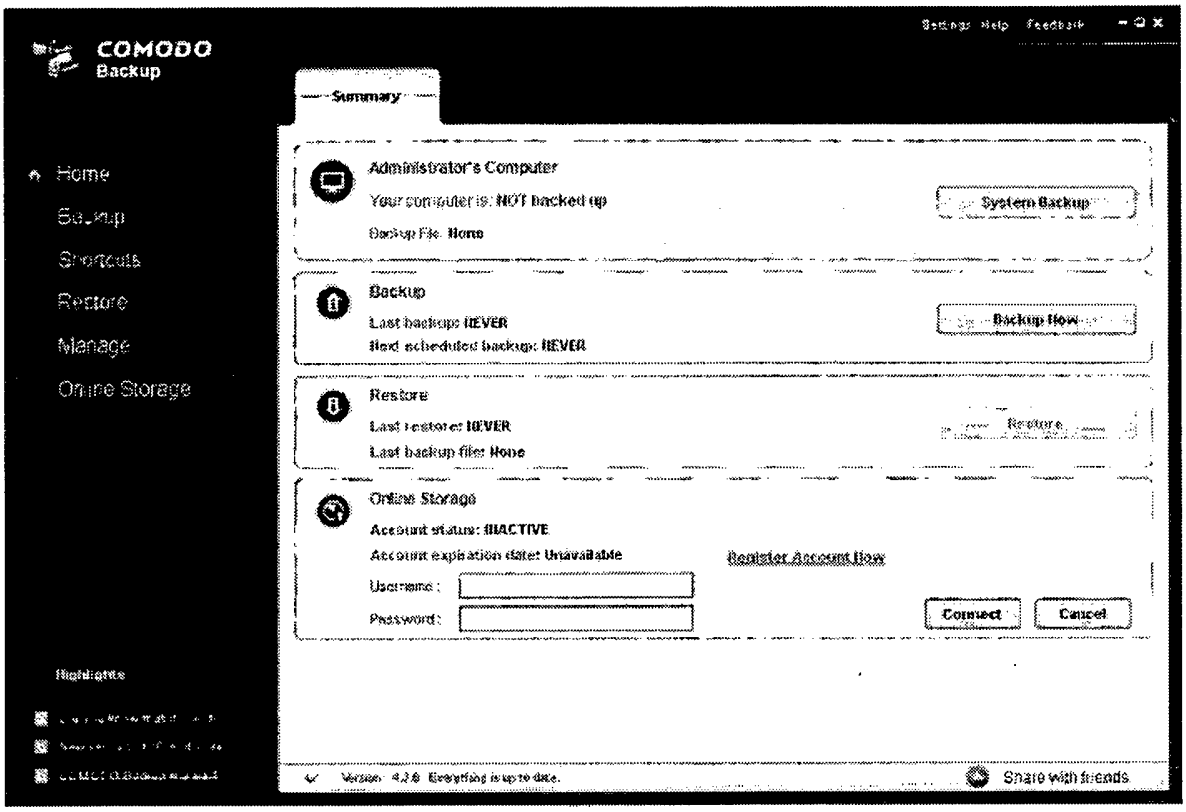
10. Comodo BackUp

Comodo BackUp is a powerful and easy to use desktop application that helps home and business users protect their valuable data against damage or loss. CIS Complete package includes Comodo BackUp with 50 GB of online storage space.

The application's streamlined design and task orientated architecture means even novice users can learn how to create, run and restore their first backup job in a matter of minutes. Other features include full scheduling, password protection, a backup integrity checker and a range of preset backup jobs that allow you to quickly create copies of important data sets such as the Windows Registry, mail accounts and user settings.

Comodo BackUp is also seamlessly integrated to Windows Explorer so that you can just select the folders or files you want to back up, right click on them and quick start the Back Up wizard.

- **Comodo Backup Features**
- **Starting Comodo Backup**
- **Comodo Backup Help**



Comodo Backup Features and Benefits

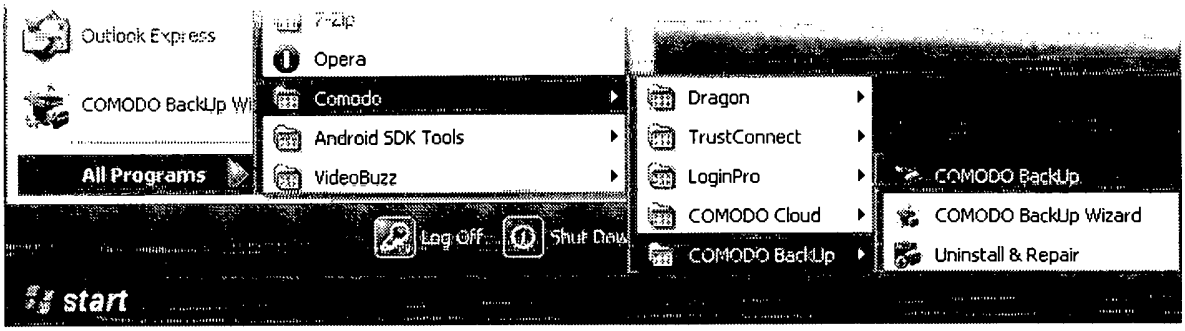
- **Quick backup** of entire drives or individual files or folders to your local computer, network drive, FTP server or Comodo's online server.
- **Step by step wizards** to guide even novice users through the entire backup, restore and scheduling procedures.
- **Flexible storage options** allow you to specify full, incremental or differential backups.
- **Protection** of invaluable personal and business data from loss or corruption.
- **Quick recovery** of files with a few clicks of the mouse.
- **Granular scheduling options** to take automatic backups at a time that suits you.
- **Real-time backups** synchronization feature to get your files copied over as soon as you save them.
- **Built in checker** to confirm the integrity of your backup files before committing to a restore.
- **Backup presets** including mail folders, windows registry, messenger archives and master boot records.
- **Powerful encryption options** to protect your files so that it cannot be accessed by anyone but you.
- **Comodo Cloud** - online file storage service. Backup your files to a highly secure online storage which can also be mounted as a virtual drive in your system.

  CIS Complete package includes 50 GB of online storage space at Comodo's online server. You can log-in to your online storage account with the user name and password that you entered during CIS Complete Registration process. Refer to **Activating Your License** for more details.
- **Command line and scripting support** to automate the online backup and restore operations.

Starting Comodo Backup

From the Start Menu

- Click Start > All Programs > COMODO > COMODO Backup > COMODO Backup:



From the Destop Icon:

- Double Click on the Comodo Backup Desktop icon created during the installation:



Comodo Backup Help

Comodo BackUp's streamlined interface provides fingertip access and control over all functional areas of the software. Please refer to the Comodo Backup online help guide at **http://help.comodo.com/topic-9-1-455-4910-Comodo-BackUp-Introduction.html** for more details on using the product.

Appendix 1 - CIS How to... Tutorials

The 'How To...' section of the guide contains guidance on key tasks of Comodo Internet Security. Use the links below to go to each tutorial's page.

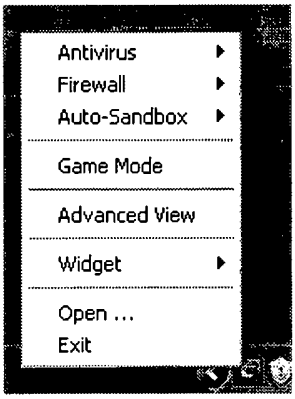
How to...:

- **Enable / Disable AV, Firewall and Auto-Sandbox Easily** - Guidance on changing the current enabled/disabled states of Antivirus, Firewall and Defense+.
- **Setup the Firewall for maximum security and usability** - A brief outline of the setting up a secure connection to Internet
- **Block Internet Access while allowing local network (LAN) Access** - guidance on configuring the Firewall to allow only Intranet or LAN connection and to block Internet connection
- **Block/allow websites selectively to users of your computer** - guidance on configuring website filtering rules for different users to selectively allow or block specific websites to them
- **Setup HIPS for maximum security and usability** - A brief outline of how to set Host intrusion Protection for the optimum balance between security and usability
- **Setup Behavior Blocker for maximum security and usability** - A brief outline of how to set Behavior Blocker for the maximum security against untrusted applications
- **Password protect your CIS settings** - Explains how to protect your CIS settings
- **Reset a Forgotten Password (Advanced)** - Explains how to create a new password for CIS
- **Run an instant Antivirus scan on selected items** - Guidance on initiating a manual scan on selected folders/files to check for viruses and other malware.
- **Create an Antivirus scanning schedule** - Guidance on time-table scheduling of antivirus scans to be run on selected items at selected intervals
- **Run an untrusted program inside sandbox** - Guidance on executing a program that you do not trust to be safe, inside sandbox to protect any harmful effects of the program upon your system.
- **Run Browsers inside Sandbox** - Guidance on running your browser, inside sandbox when you plan to visit untrusted websites.
- **Run Untrusted Programs inside Virtual Desktop** - Guidance on executing a program that you do not trust to be safe, inside the virtual Desktop.
- **Run Browsers Inside the Virtual Desktop** - Guidance on running your browser, inside virtual Desktop when you plan to do online banking, online shopping and so on.
- **Restore incorrectly quarantined item(s)** - Help to restore files and executables that were moved to quarantine by mistake
- **Submit quarantined items to Comodo for analysis** - Advice on how to send suspicious files/executables to Comodo for analysis
- **Enable file sharing applications like BitTorrent and Emule** - Explains how to configure Comodo Firewall for file sharing through popular software
- **Block any downloads of a specific file type** - Explains how to configure Defense+ to block downloads of files of a specific type
- **Selectively disable Behavior Blocker and Auto-Sandboxing for specific files** - Explains how to exclude specific files or file types from the auto-sandboxing process
- **Switch between complete CIS suite and individual components (just AV or FW)** - Explains how to uninstall or install Firewall or Antivirus components after installation.
- **Switch Off Automatic Antivirus and Software Updates** - Explains how to stop automatic software and virus updates
- **Temporarily suppress alerts when playing games** - Helps you to switch off CIS pop-up alerts to avoid interruptions while playing games

- **Renew or upgrade your license** - Explains how to renew or upgrade your license
- **How to use CIS Protocol Handlers** - Explains how to use CIS protocol handlers

Enable / Disable AV, Firewall and Auto-Sandbox Easily

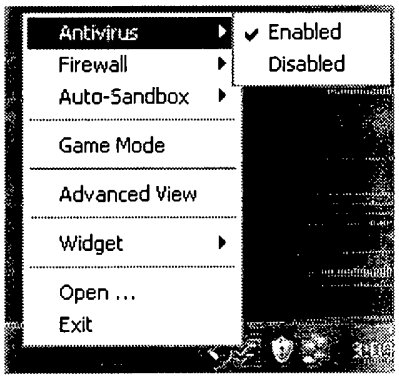
Comodo Internet Security allows users to quickly switch the Enabled/Disabled states of **Antivirus**, **Firewall** and **Auto-Sandbox** by right clicking on the system tray icon (the CIS interface should be in **Compact View**).



Antivirus

To enable/disable the Antivirus

1. Right click on the system tray icon keeping the CIS interface in Compact View.
2. Move the mouse cursor over 'Antivirus'



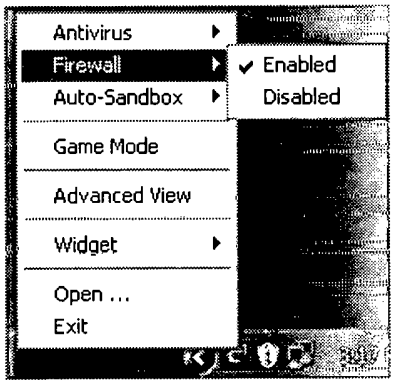
3. Choose 'Enabled or Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Firewall

To enable/disable the Firewall

1. Right click on the system tray icon keeping the CIS interface in Compact View
2. Move the mouse cursor over 'Firewall'



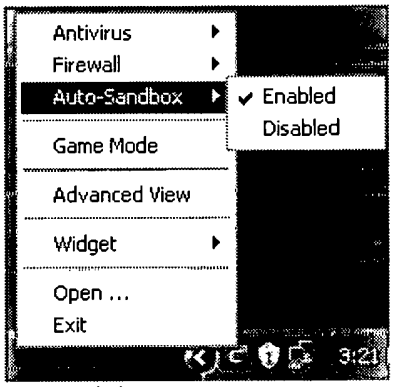
3. Choose 'Enabled or Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

Auto-Sandbox

To enable/disable the Auto-Sandbox

1. Right click on the system tray icon keeping the CIS interface in Compact View.
2. Move the mouse cursor over 'Behavior Blocker'



3. Choose 'Enabled or Disabled' as per your choice

You can find the set security level also from **the Home Screen**.

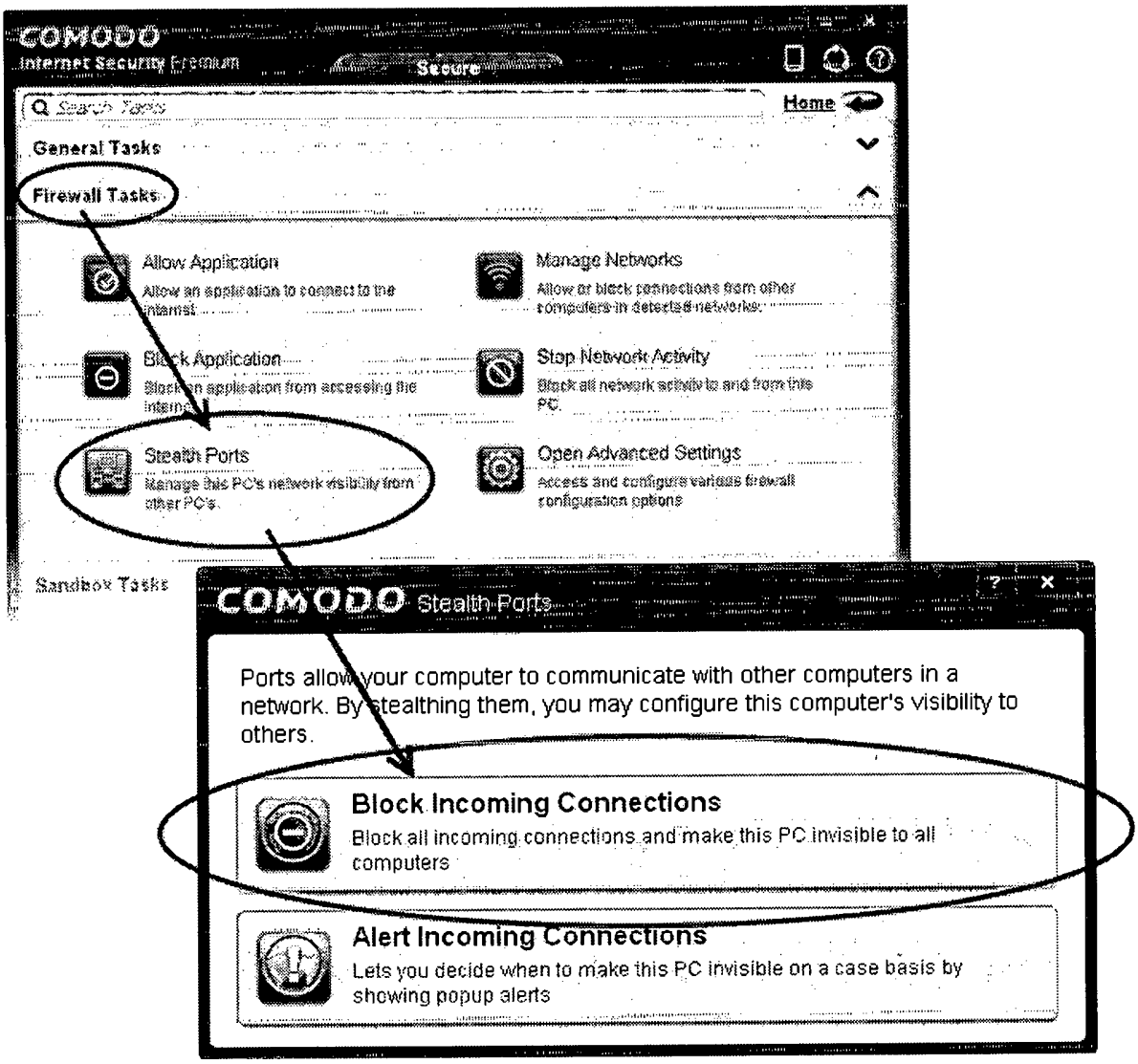
Set up the Firewall For Maximum Security and Usability

This page outlines the functions of Comodo's Firewall and helps you to set up a secure connection to the Internet.

Stealth Ports Settings

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

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface
3. Open Stealth Ports interface by clicking the 'Stealth Ports' icon  from the Firewall Tasks panel



4. Select 'Block Incoming Connections' to make computer's ports are invisible to all networks

Click here for more details on Stealthing your Computer Ports

Network Zones Settings

The 'Network Zones' settings allow you to configure the protection level for network connection to a Router/home network. (This is usually done **automatically** for you).

To view the configurations

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Network Zones' under Firewall from the left hand side pane
4. Click 'Network Zones' tab from the 'Network Zones' interface



Check the Loopback zone and Local Area Network #1. **In most cases**, the loopback zone IP address should be *127.0.01/255.0.0.0*

In most cases, the IP address of the auto detected Network zone should be *192.168.1.100/255.255.255.0* .

5. Check these addressees and click 'OK'.

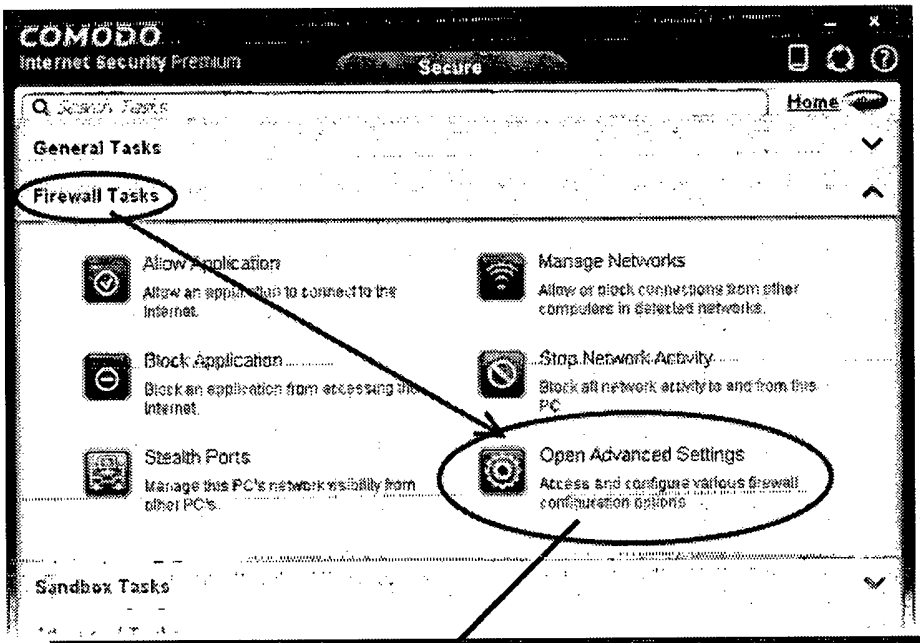
Click here for more details on Network Zones settings

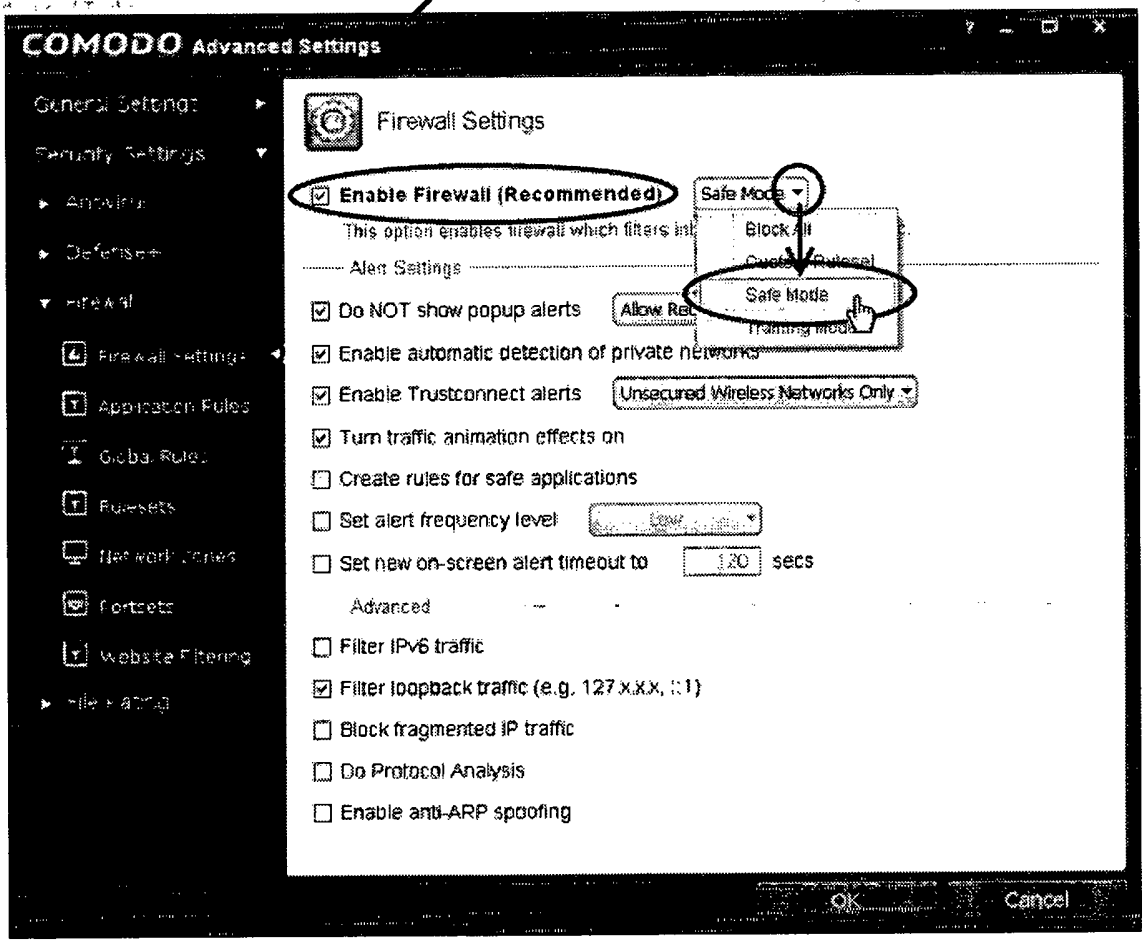
Firewall Behavior Settings

The Firewall Behavior Settings option allows you to configure the protection level for your Internet connection and the frequency of alerts generated.

To open Firewall Behavior Settings panel

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Firewall Settings' under Firewall from the left hand side pane
4. Ensure that 'Enable Firewall' is selected and choose **Safe mode** from the drop-down beside it.



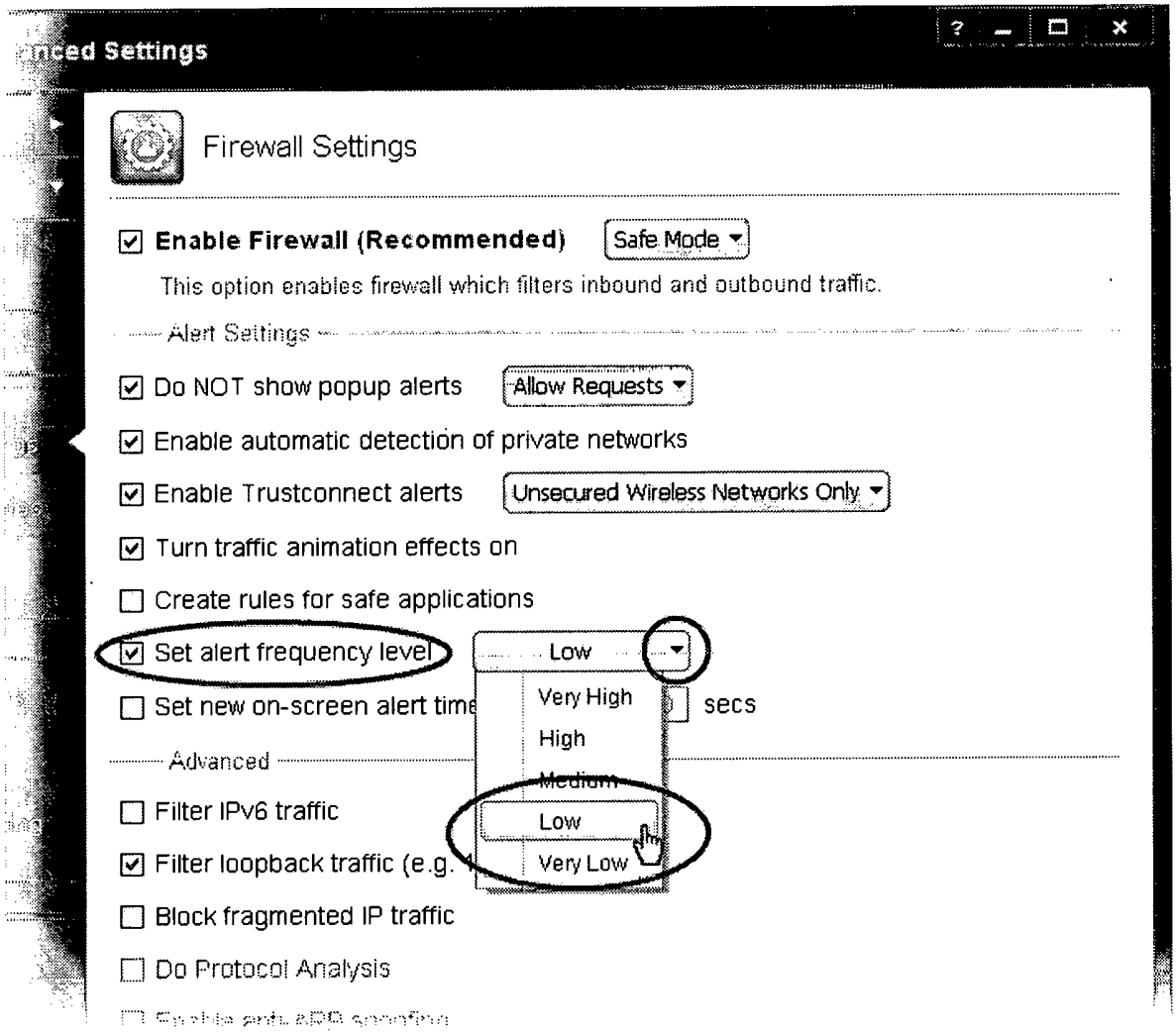


Safe Mode: While filtering network traffic, the firewall will automatically create rules that allow all traffic for the components of applications certified as 'Safe' by Comodo. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should you choose, you can grant that application Internet access by choosing 'Treat this application as a Trusted Application' at the alert. This will deploy the predefined firewall policy 'Trusted Application' onto the application.

Alert Settings

Under 'Alert Settings' in the same interface:

- Deselect Do NOT show popup alerts
- Select 'Set alert frequency level' option and choose 'Low' from the drop-down. At the 'Low' setting, the firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users.



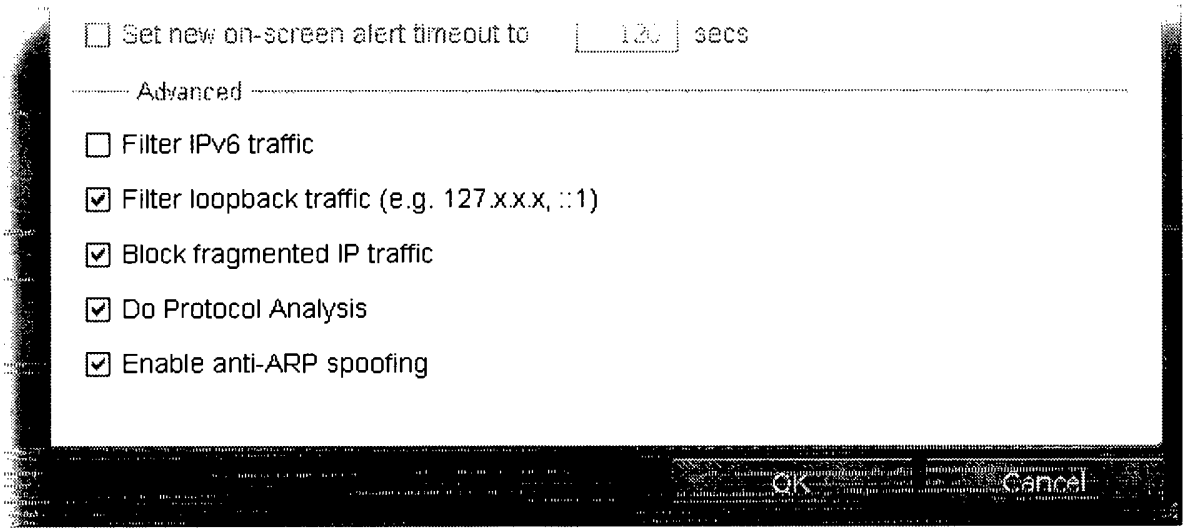
Advanced Settings

When launching a denial of service or 'flood' attack, an attacker bombards a target machine with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. To protect from such attacks, make the following settings under 'Advanced' in the 'Firewall Settings' interface:

- Select **Filter loopback traffic**
- Ensure that the **Block fragmented IP traffic** is selected
    - **Block fragmented IP traffic** - When a connection is opened between two computers, they must agree on a Maximum Transmission Unit (MTU). IP Datagram fragmentation occurs when data passes through a router with an MTU less than the MTU you are using i.e when a datagram is larger than the MTU of the network

over which it must be sent, it is divided into smaller 'fragments' which are each sent separately. Fragmented IP packets can create threats similar to a DOS attack. Moreover, these fragmentations can double the amount of time it takes to send a single packet and slow down your download time.

- Select the **Do Protocol Analysis** checkbox to detect fake packets used in denial of service attacks
- Select **Enable anti-ARP spoofing**



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

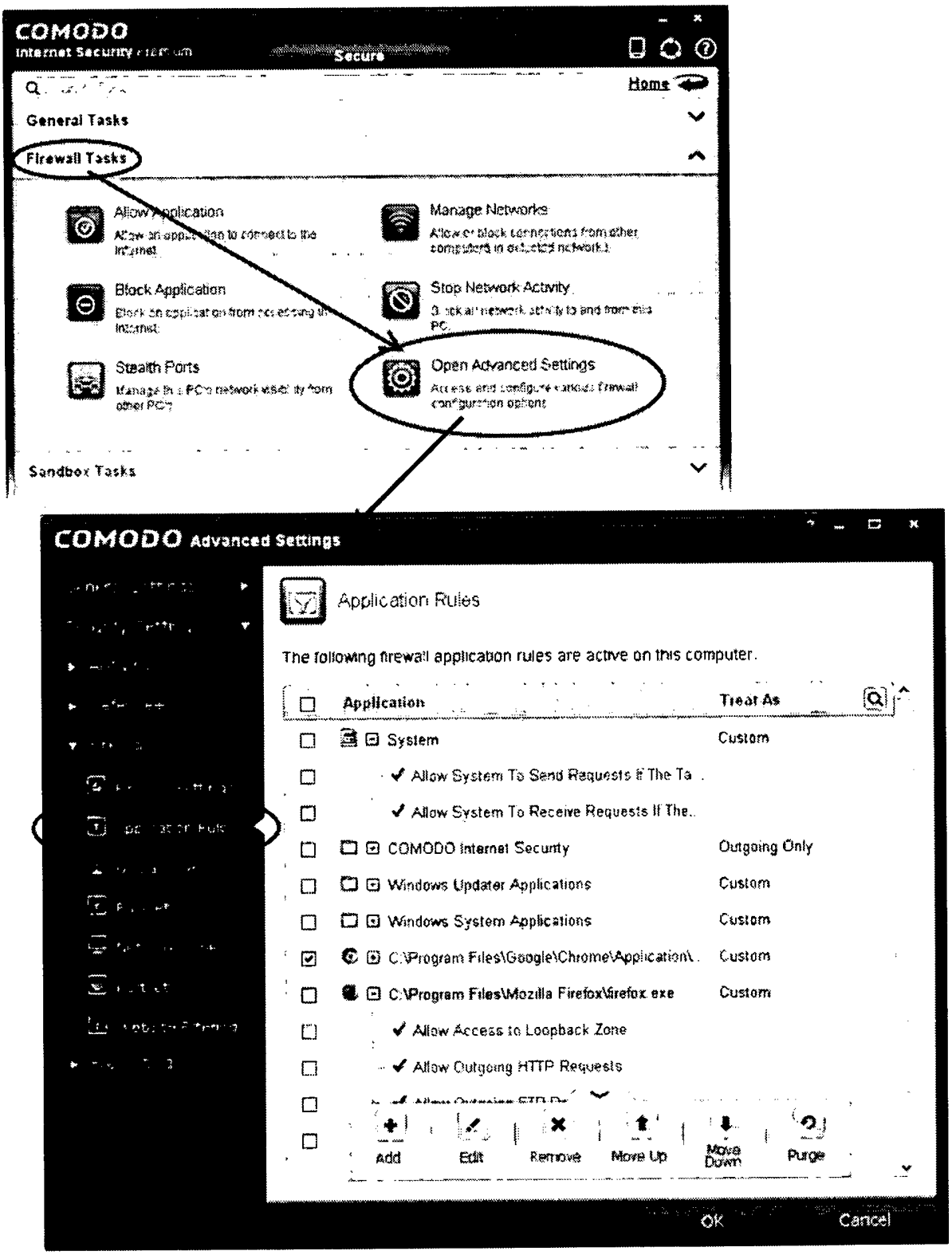
Click here for more details on Firewall Behavior Settings

Setting-up Application Rules, Global Rules and Predefined Firewall Rulesets

You can configure and deploy traffic filtering rules and policies on an application specific and global basis and predefined firewall rulesets.

To view the Application Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Application Rules' under Firewall from the left hand side pane



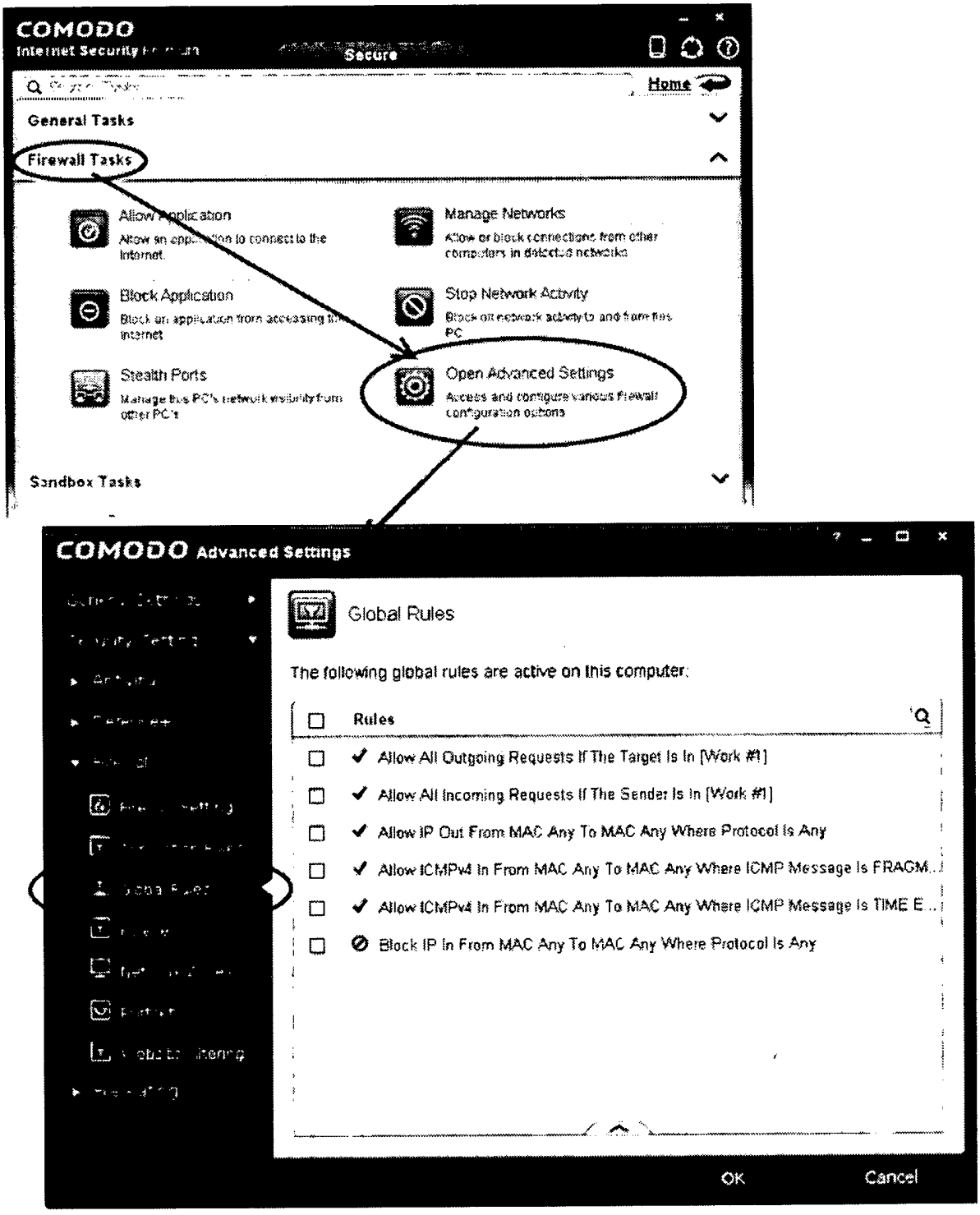
4. Click the handle from the bottom and Add or Edit rules for specific applications manually or remove them.

Click here for more details on Application Rules

To view the Global Rules

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen

2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Global Rules' under Firewall from the left hand side pane



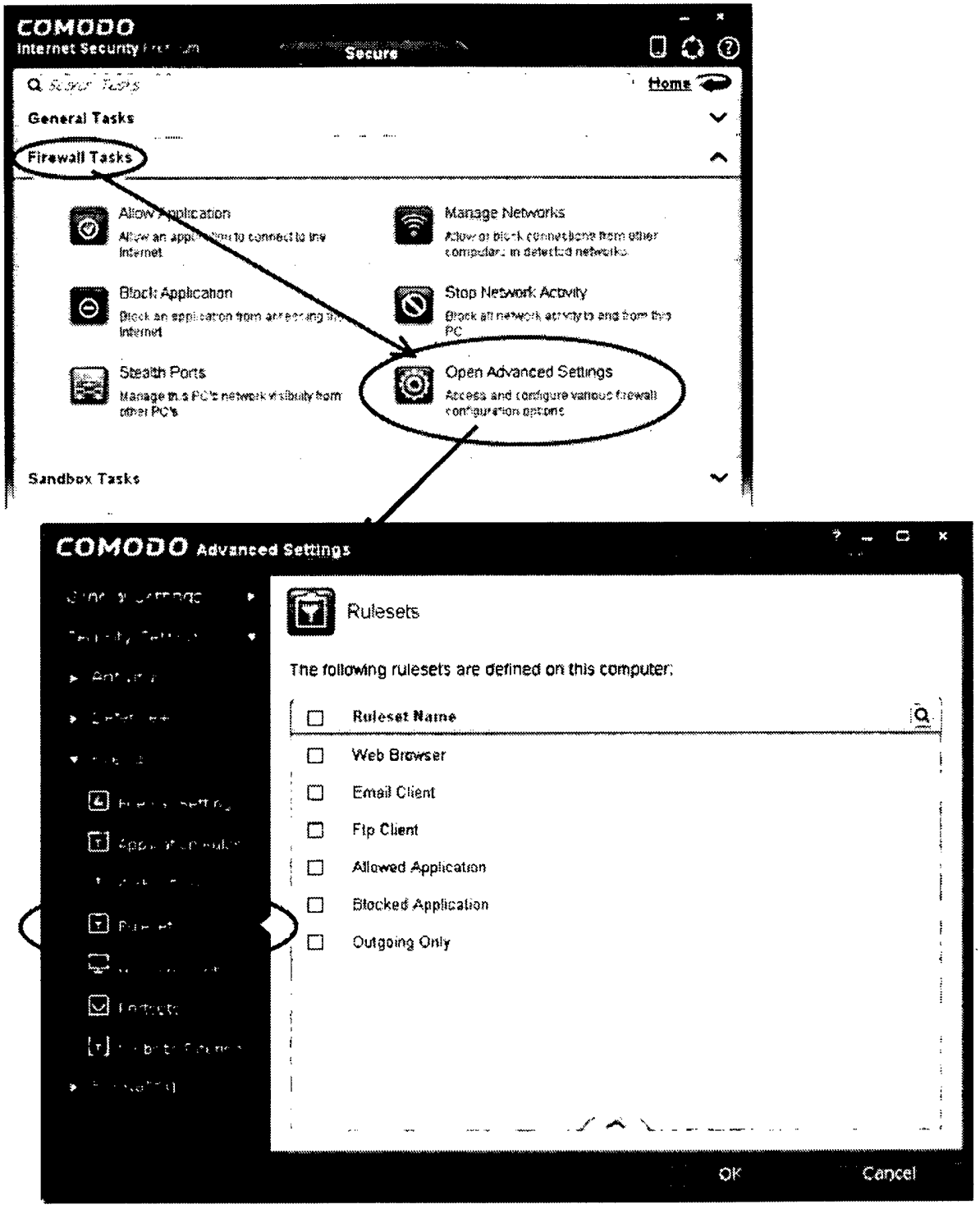
4. Click the handle from the bottom and Add or Edit global rules manually or remove them.

Click here for more details on Global Rules

To view Predefined Firewall rulesets

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.

3. Click 'Rulesets' under Firewall from the left hand side pane



4. Click the handle from the bottom to and Add, Edit or remove rulesets.

You need not make your own rulesets, the defaults are usually enough.

Click here for more details on pre-defined firewall rulesets

Block Internet Access while Allowing Local Area Network (LAN) Access

You can configure Comodo Firewall to block Internet access while allowing free connections to an internal network (Intranet or LAN).

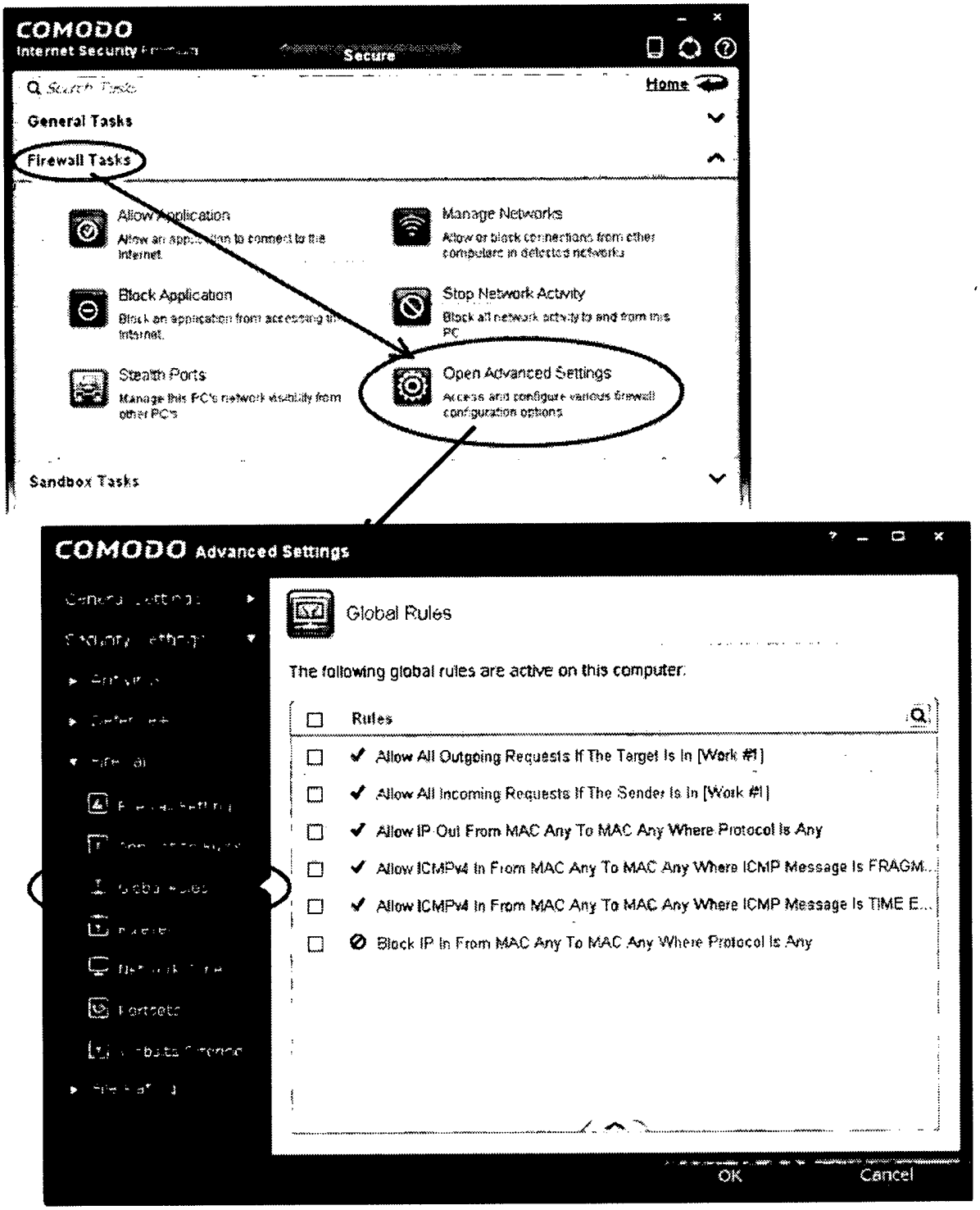
Example scenarios:

- In your network at home, you want your child's computer to connect to other computers at home but disable Internet access to them for safety reasons
- In your corporate network, you want your employee's computers to connect to your local network machines but disable Internet access for them for bandwidth restrictions

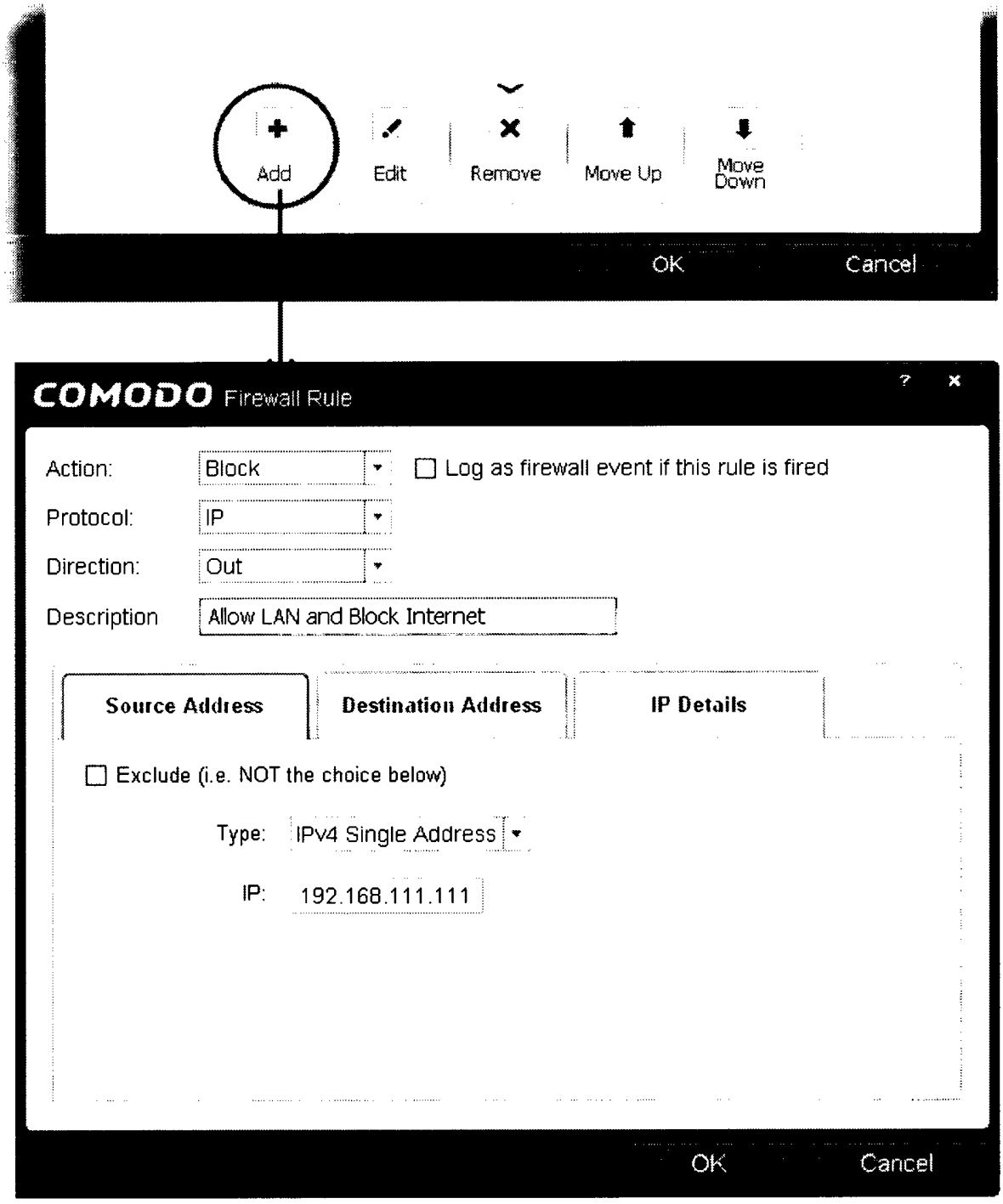
To selectively block connection to Internet whilst allow connection to internal network you need to create a Global Rule under Advanced Firewall Settings and password protect your configuration to prevent others from altering it.

To create a Global Rule

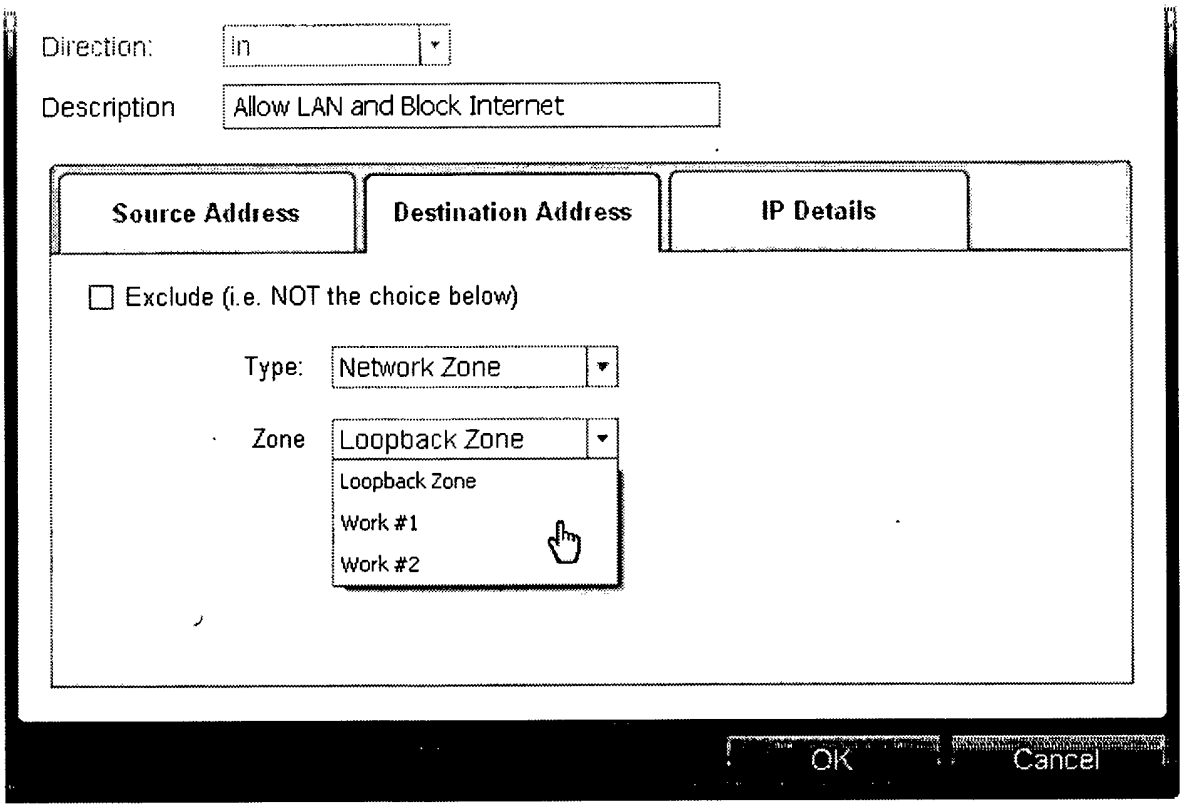
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Global Rules' under Firewall from the left hand side pane



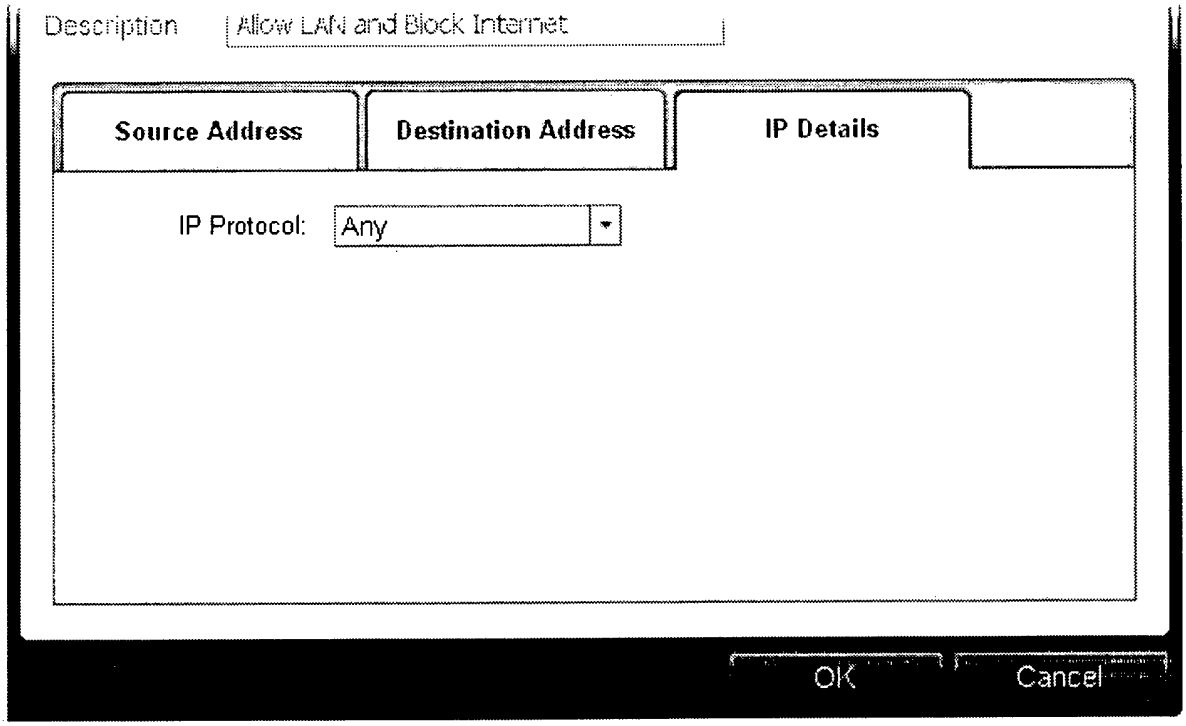
4. Click the handle from the bottom and choose 'Add' from the options. The Firewall Rule interface will open.



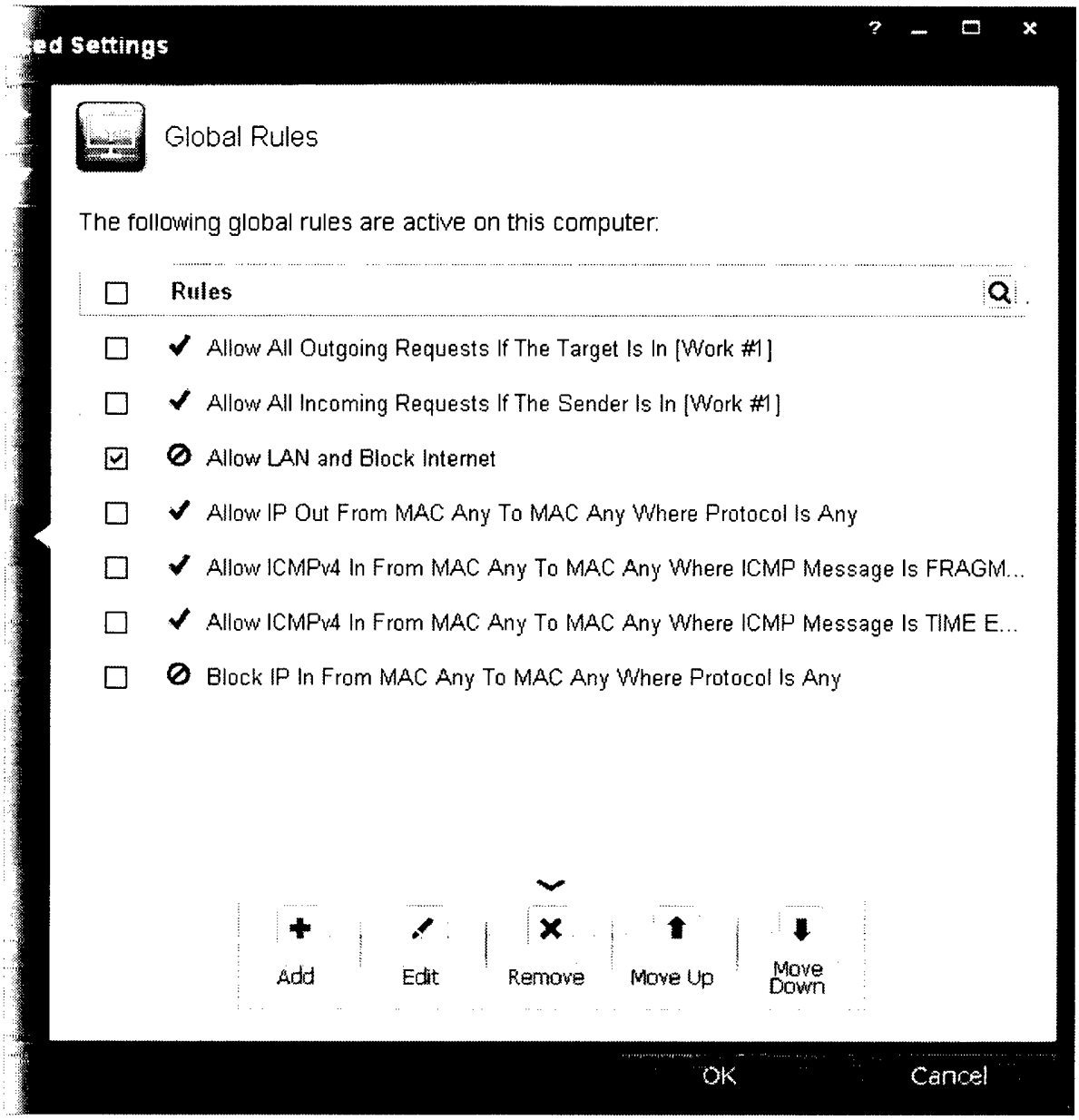
5. Choose the following options from the drop-down menus:
   - Action = Block;
   - Protocol = IP;
   - Direction = Out.
6. Enter a description for the new rule in the Description text box.
7. Click the 'Source Address' tab, choose 'IPv4 Single Address' or 'IPv6 Single address' as per your network and enter the IP address of the computer in the IP text box.
8. Click the 'Destination Address' tab, choose 'Network Zone' from the Type drop-down and choose your local area network from the 'Zone' drop-down.



9. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.



10. Click 'OK'. The created policy will be added to the list of Global Rules.
11. Select the rule, click the handle from the bottom and click 'Move Up' repeatedly until the rule moves to the first position.

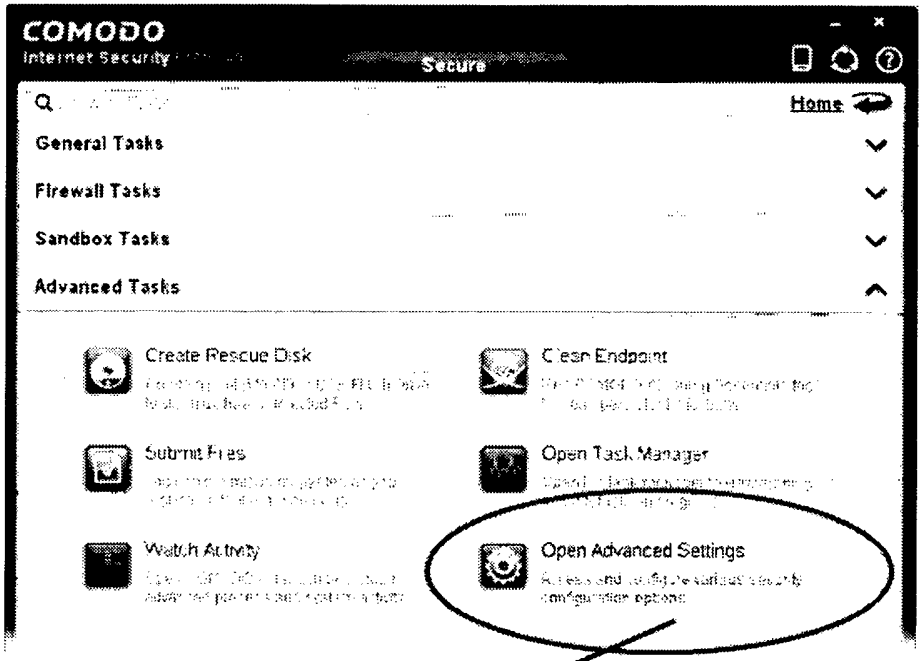


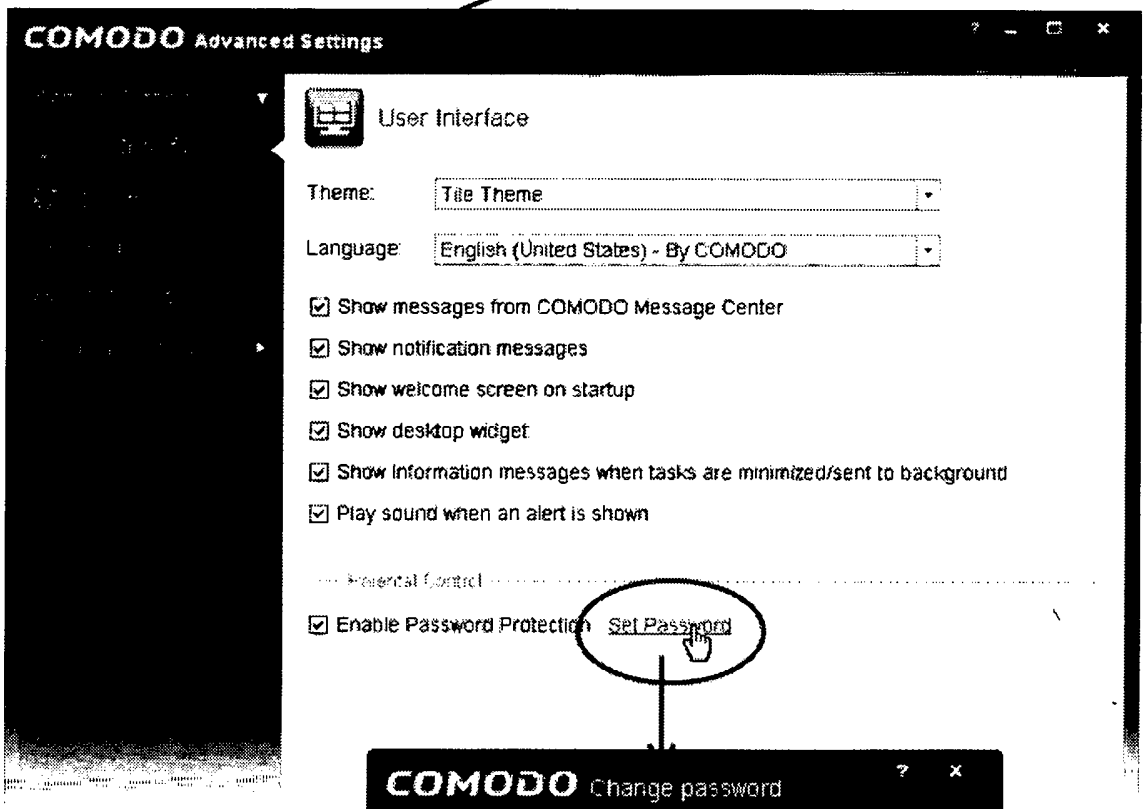
12. Click 'OK' for your configuration to take effect.

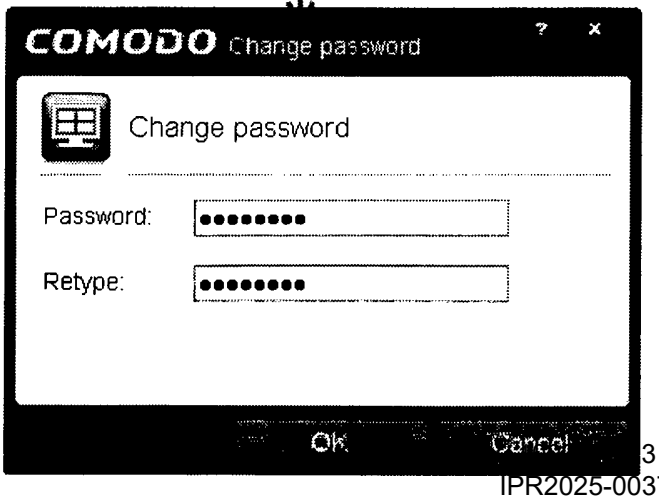
Your Firewall is now configured to allow access to internal network but to block Internet access. Now you need to password protect this configuration to prevent others from changing it.

To password protect your configuration

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'User Interface' under General Settings from the left hand side pane

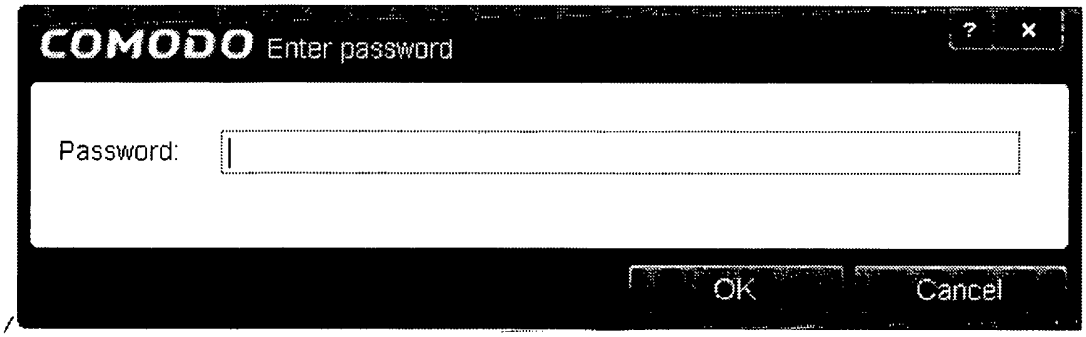

COMODO
Internet Security
Secure
Home
General Tasks
Firewall Tasks
Sandbox Tasks
Advanced Tasks
Create Rescue Disk
Clean Endpoint
Submit Files
Open Task Manager
Watch Activity
Open Advanced Settings


COMODO Advanced Settings
User Interface
Theme:
Tile Theme
Language:
English (United States) - By COMODO
Show messages from COMODO Message Center
Show notification messages
Show welcome screen on startup
Show desktop widget
Show information messages when tasks are minimized/sent to background
Play sound when an alert is shown
Enable Password Protection
Set Password


COMODO Change password
Change password
Password:
Retype:
Ok
Cancel

4. Select 'Enable Password Protection' under 'Parental Control' and click 'Set Password' link. The Change password dialog will appear.
5. Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

The configuration is now password protected. From the next attempt to change any configuration changes to CIS, you will be prompted to enter the password to proceed.



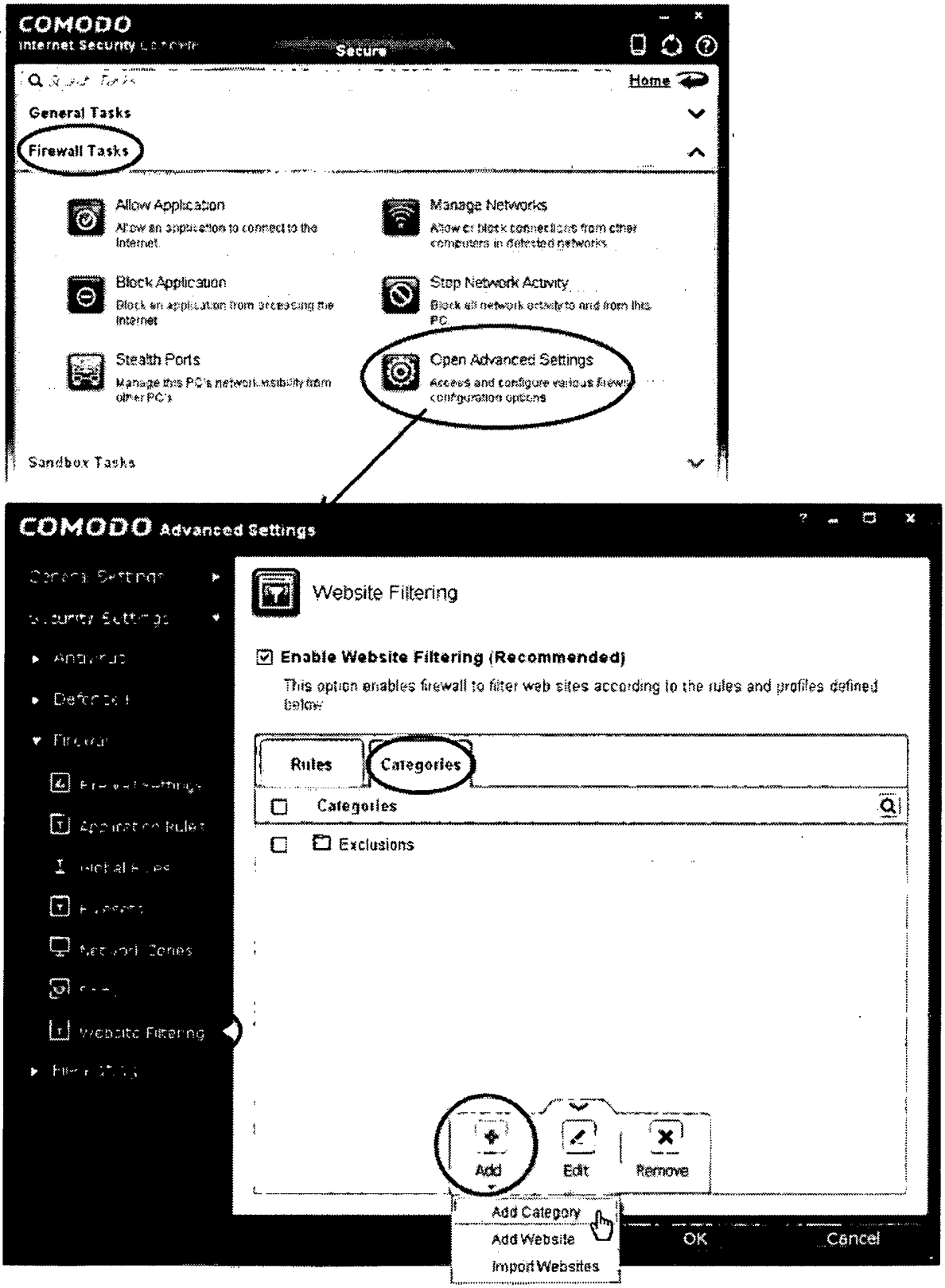
Block/allow Websites Selectively to Users of Your Computer

Comodo Internet Security allows you to specify a single or a group of website(s) that can be selectively allowed or blocked to different users of your computer. Configuring the website filtering involves two steps:

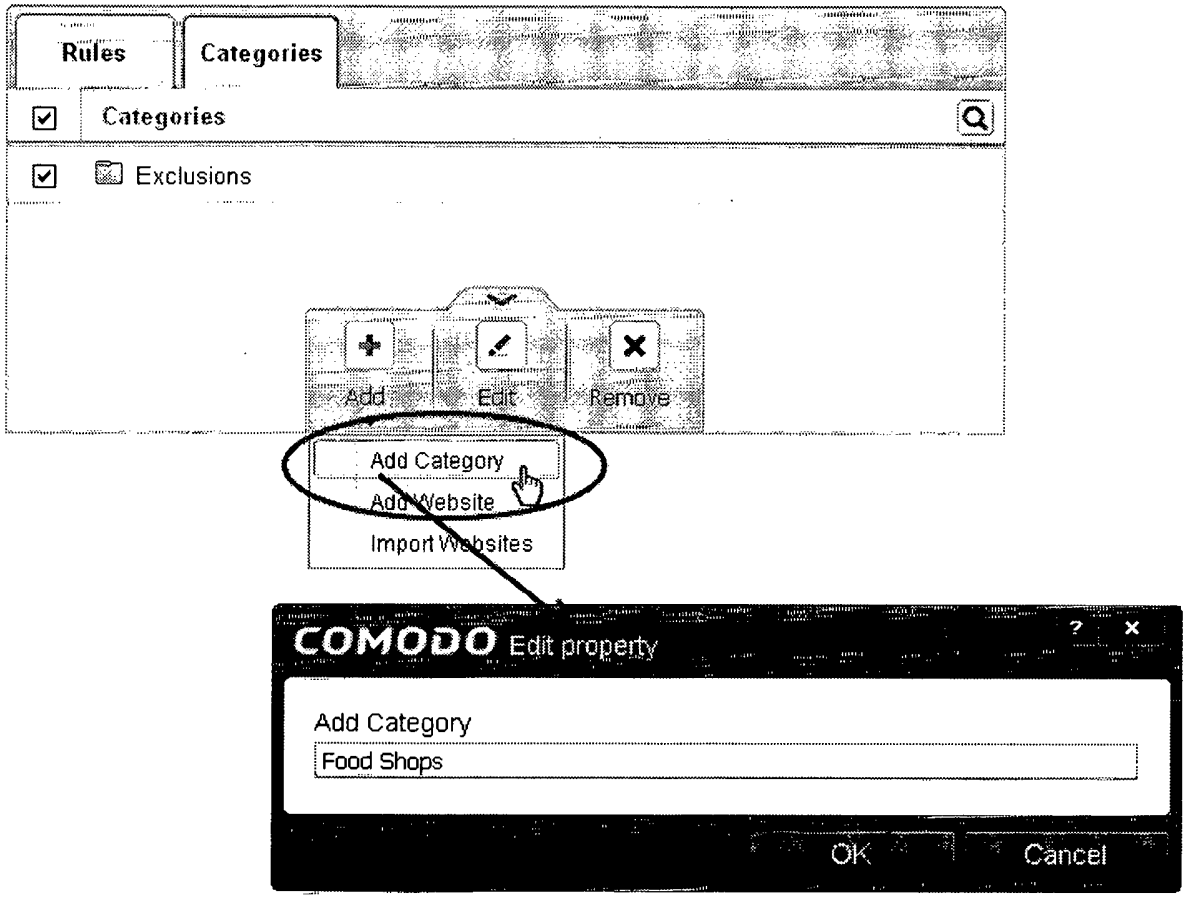
- **Define Website Categories and add websites**
- **Create Firewall rules for allowing or blocking website categories to selected users**

To define website categories

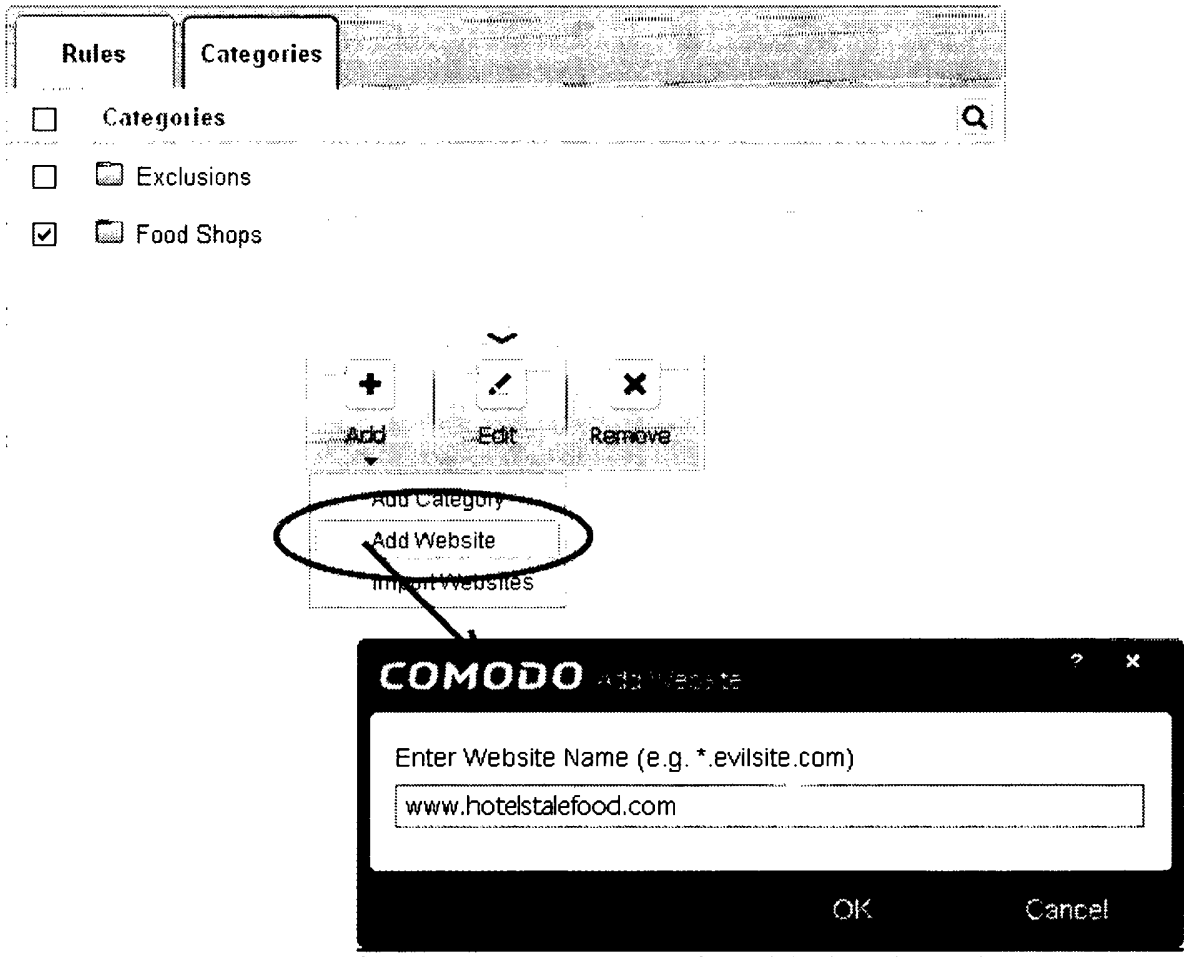
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen.
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Website Filtering' under Firewall from the left hand side pane.
4. Ensure that the 'Enable Website Filtering Filtering' checkbox is selected.
5. Click 'Categories' tab from the 'Website Filtering' interface.



6. Click the handle from the bottom center of the 'Categories' pane, click 'Add' from the options and choose 'Add Category' from the drop-down. The 'Edit Property' dialog will open.



7. Enter a name for the category and click OK. The new category will be created and added under the 'Categories' tab.
8. Select the category, click the handle at the bottom of the 'Categories' pane, click 'Add' then choose 'Add Website' from the drop-down menu. The 'Add Website' dialog will open:



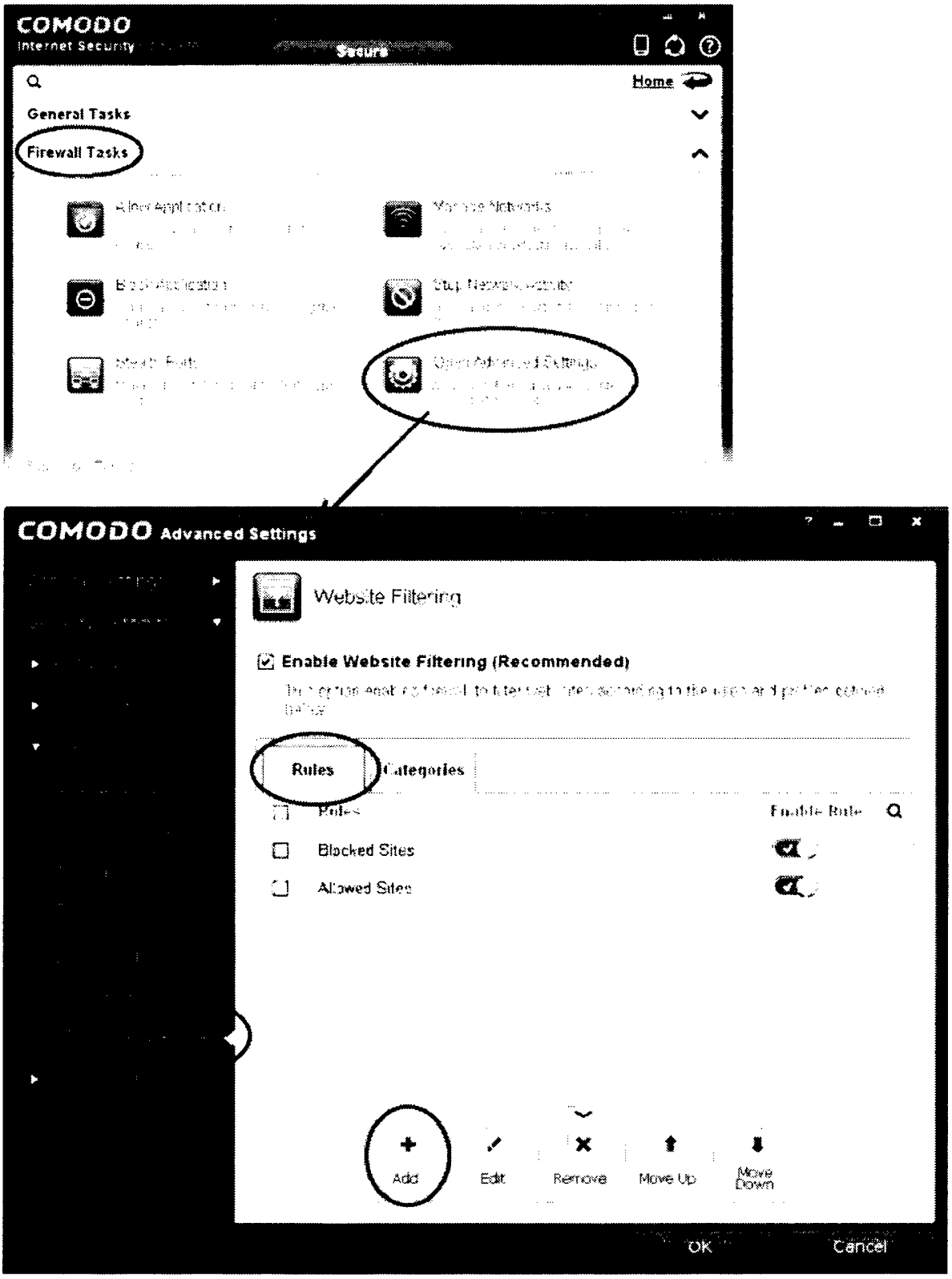
9. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
    - To add a specific website/webpage, enter the full URL of the website/webpage
    - To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
    - To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.
    - To include all the websites with URLs that contain a specific string, add the wildcard character befor and after the string. For example, "*pizza*" will cover hotpizza.com, spicypizza.com and so on.

The website(s) will be added to the category.

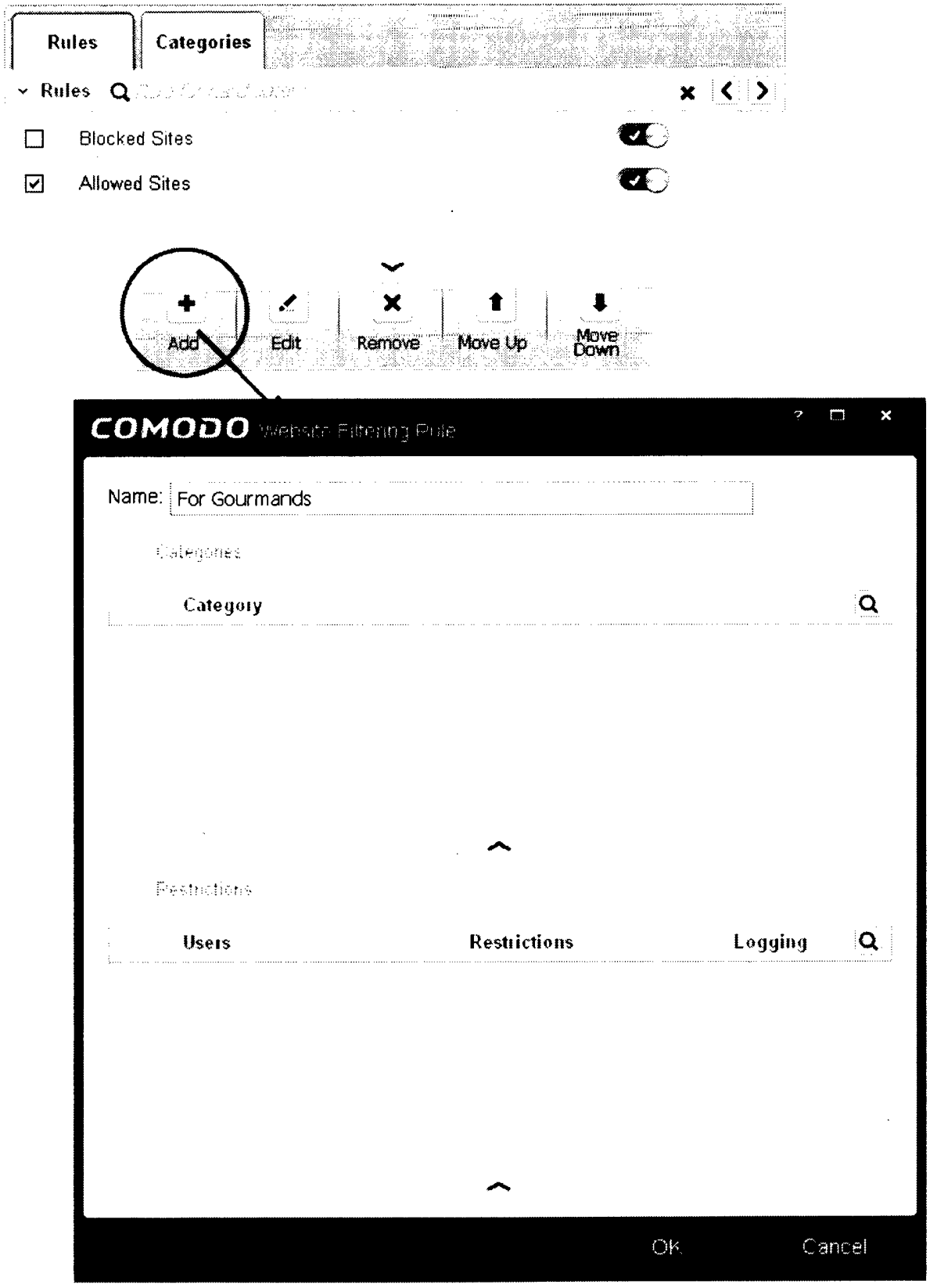
10. Repeat the process to add more websites.
11. Click OK in the 'Advanced Settings' interface to save your settings

To create rules for selectively blocking or allowing websites to users

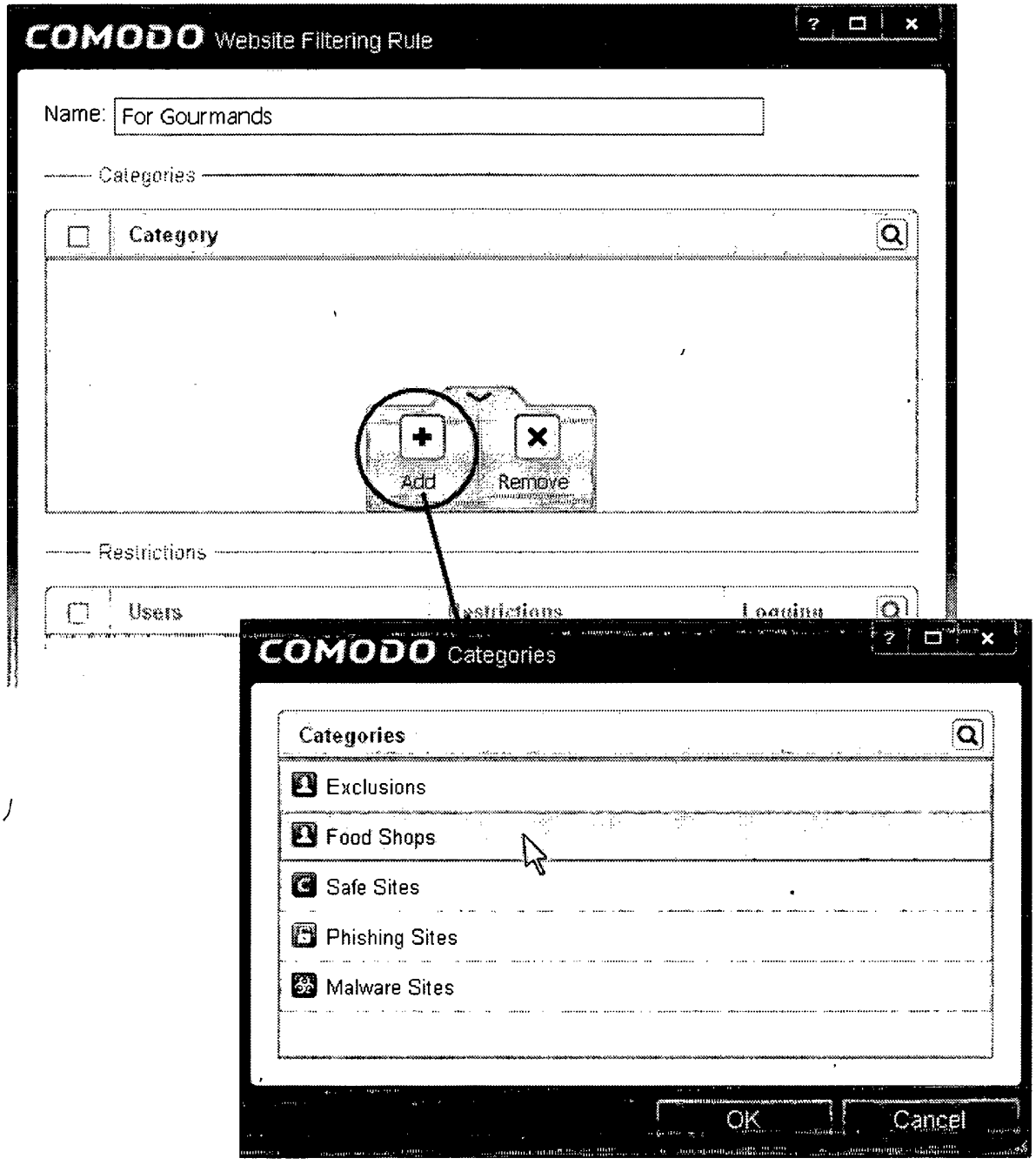
1. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
2. Click 'Website Filtering' under Firewall from the left hand side pane.
3. Click 'Rules' tab from the 'Website Filtering' interface.
4. Click the handle at the bottom of the Rules interface and select 'Add':



5. Enter a name for your new filter in the 'Website Filtering Rule' dialog.



6. Select the categories that should be added to the filter:
    - Click the handle at the bottom of the 'Category' pane and choose 'Add'.



- Select a category and click 'OK' to add it to your rule. Repeat the process to add more categories.

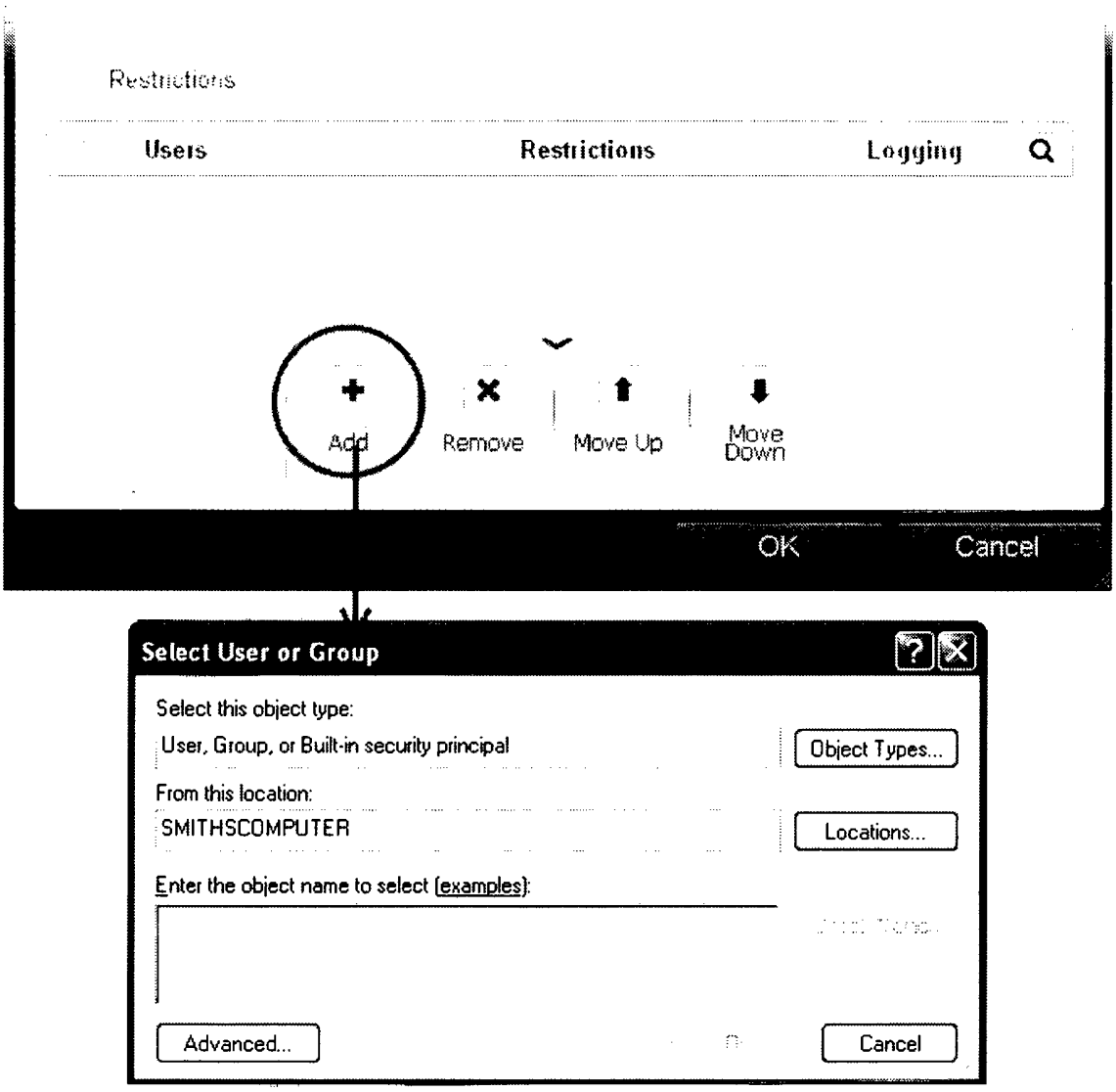
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **Comodo Safe Sites** - Websites that are considered safe according to global whitelist
- **Comodo Phishing Sites** - Websites that lead to phishing websites, as per dynamically updated Comodo Blacklist
- **Comodo Malware Sites** - Websites that may inject malware into your system, as per dynamically updated Comodo Blacklist

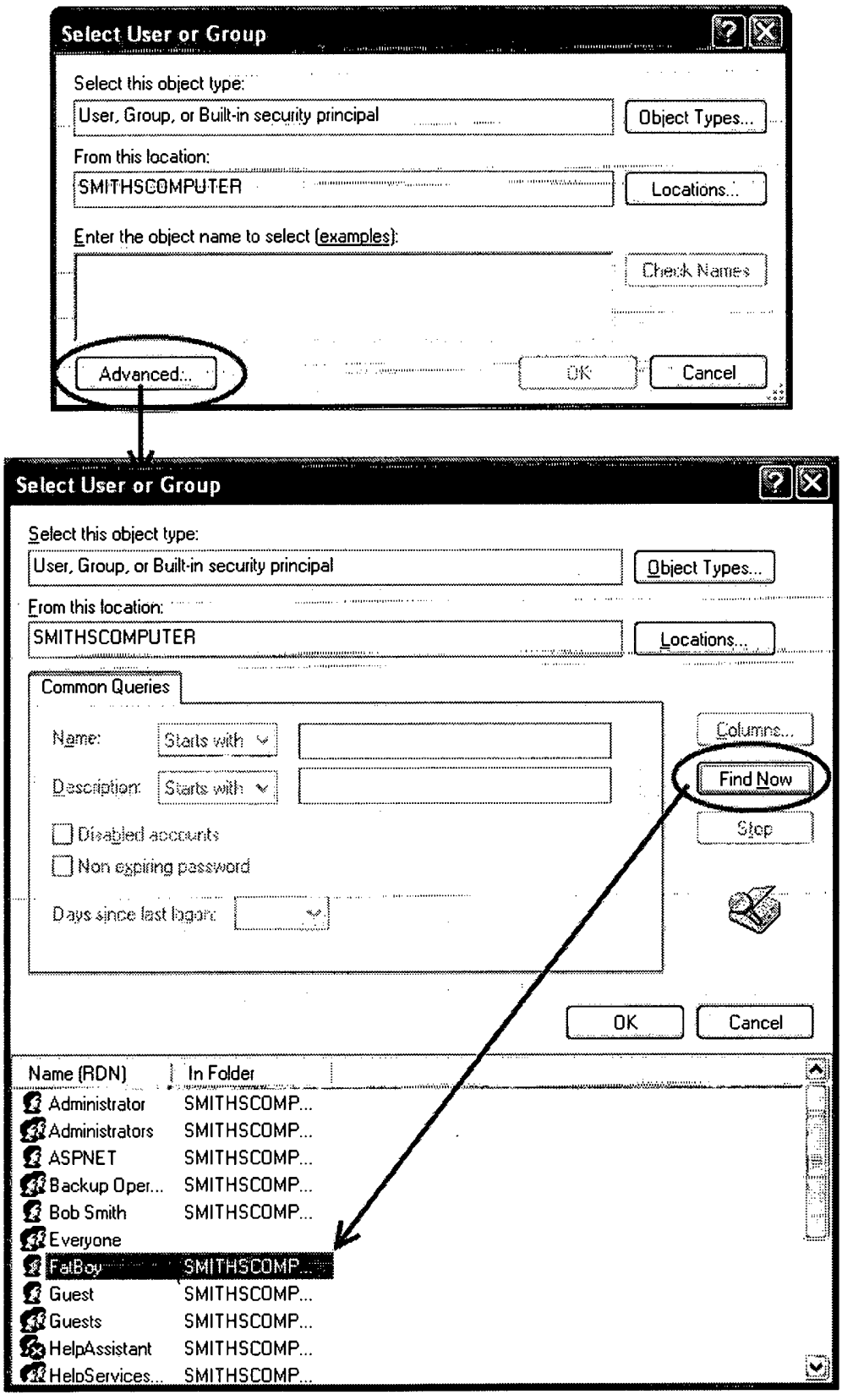
For more details on creating and modifying user specified categories, Refer to the section **Defining or Modifying Website Categories**

7. Add Users or User Groups to whom the rule should be applied:

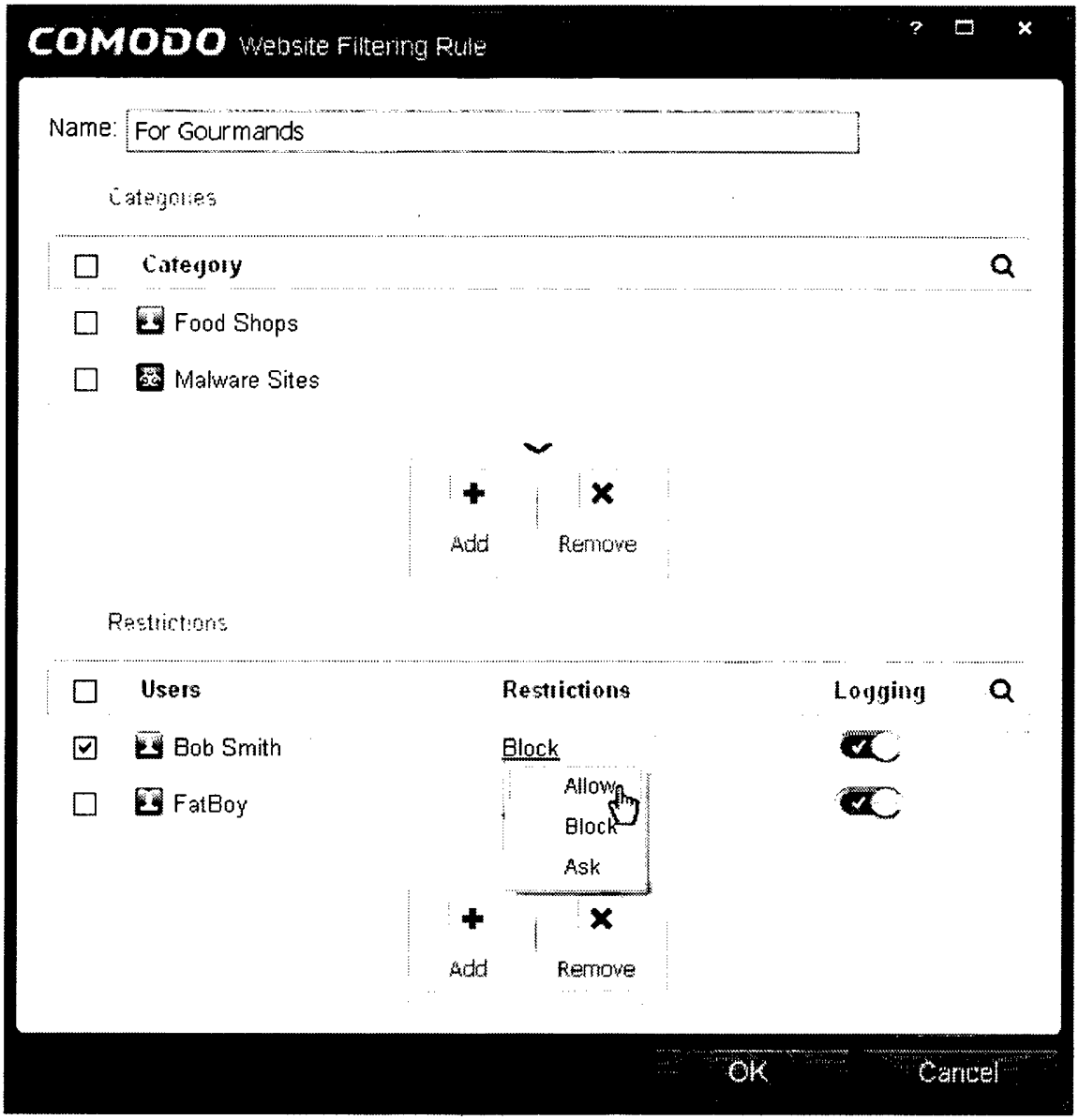
   - Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:



   - Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format <domain name>\<user/group name> or <user/group name>@<domain name>. Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the addition of the users.



- After adding target users or groups, you next need to specify whether those users should be allowed or blocked from viewing the websites in the category or they should be asked if they want to continue. This is done by modifying the link in the 'Restrictions' column:



Allow - The websites in the categories can be accessed by the user.

Block - The websites in the categories cannot be accessed by the user.

Ask - An alert will be displayed in the browser if the user tries to access any of the websites in the category. The user can decide whether or not to continue.

- Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.

8. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
9. Ensure that the rule is enabled using the toggle switch under the Enable Rule column for the rule to take effect.
    - You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

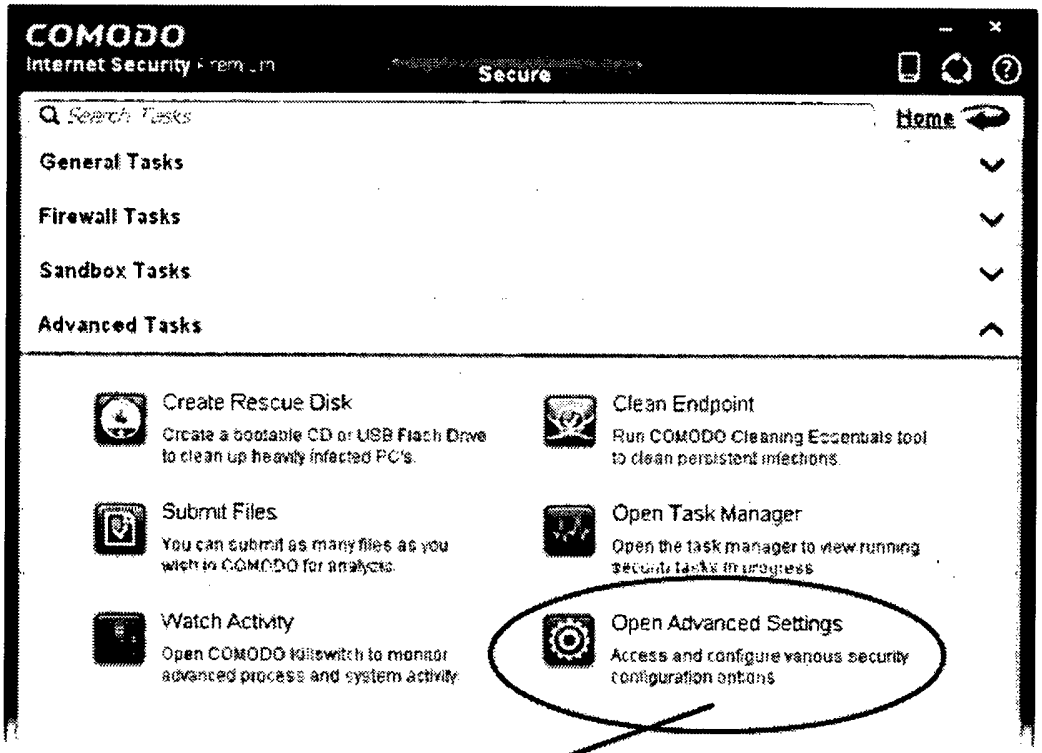
You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

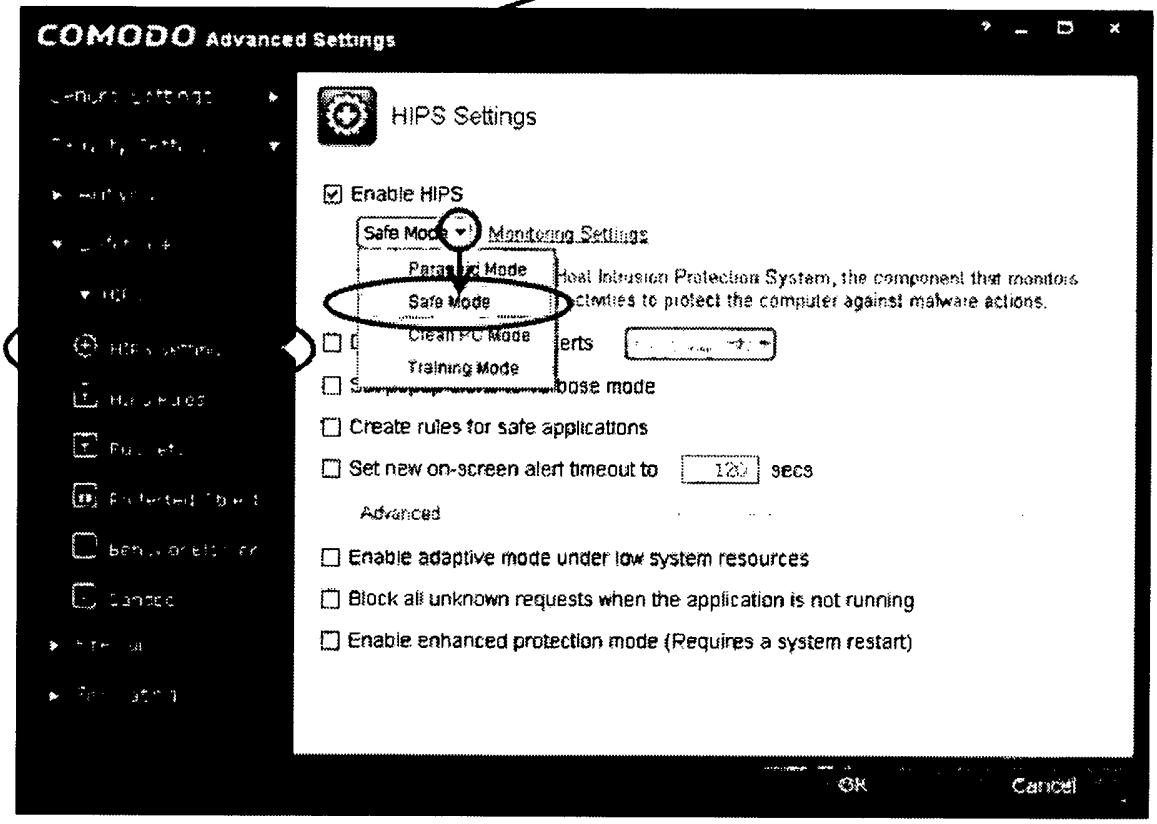
Set up the HIPS for Maximum Security and Usability

This page explains on configuring the Host Intrusion Prevention System (HIPS) component of CIS to provide maximum security from the malicious programs that try to execute from within your system and to protect your system from data theft, computer crashes and system damage by preventing most types of buffer overflow attacks, prevent possible attacks from root-kits, inter-process memory injections, key-loggers and more.

To configure HIPS

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'HIPS' > 'HIPS Settings' from the left hand side pane

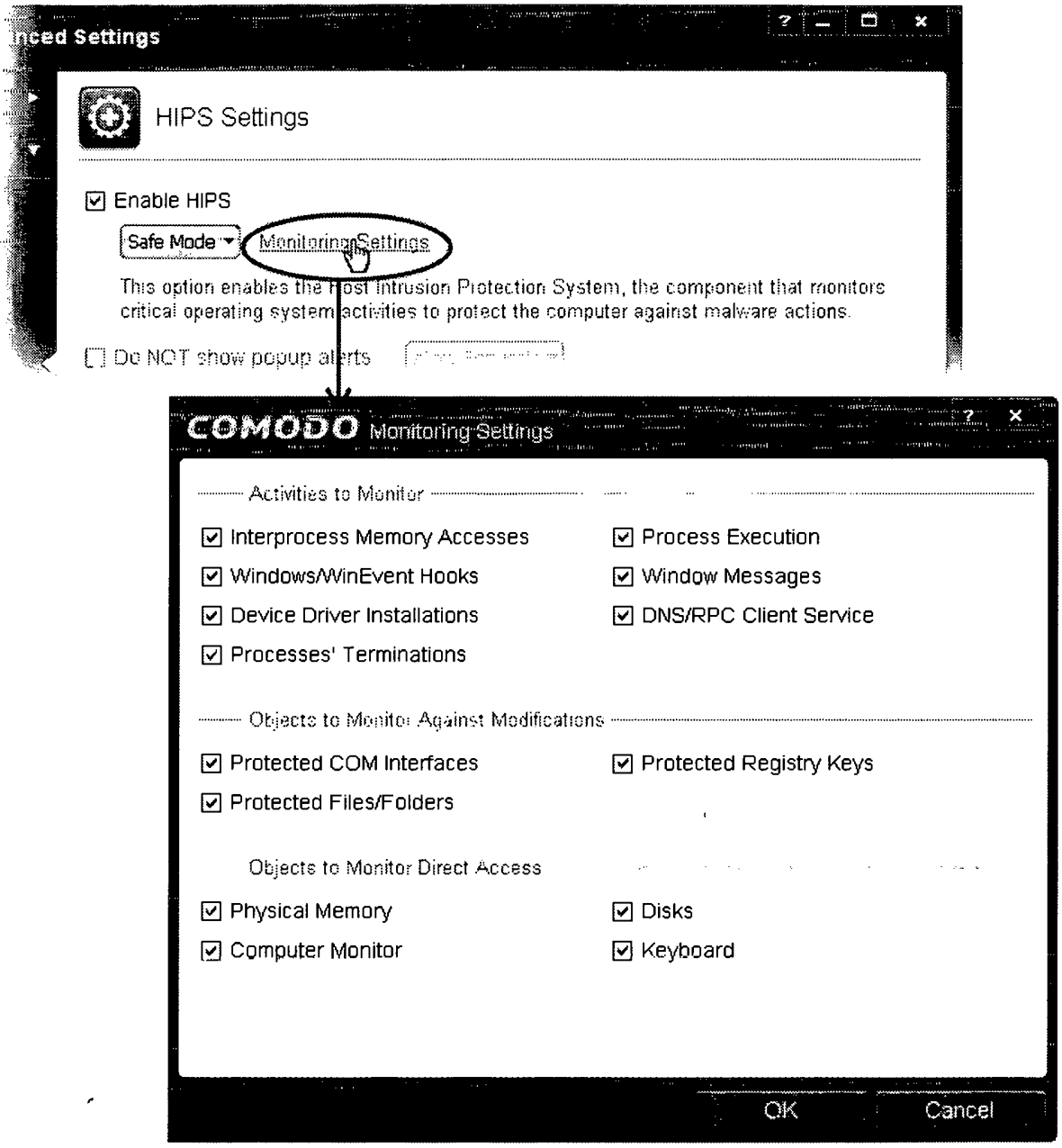




4. Select Enable HIPS
5. Choose 'Safe Mode' from the drop-down below it. Refer to **HIPS Behavior Settings** for more details on the Security Levels.

Monitoring Settings

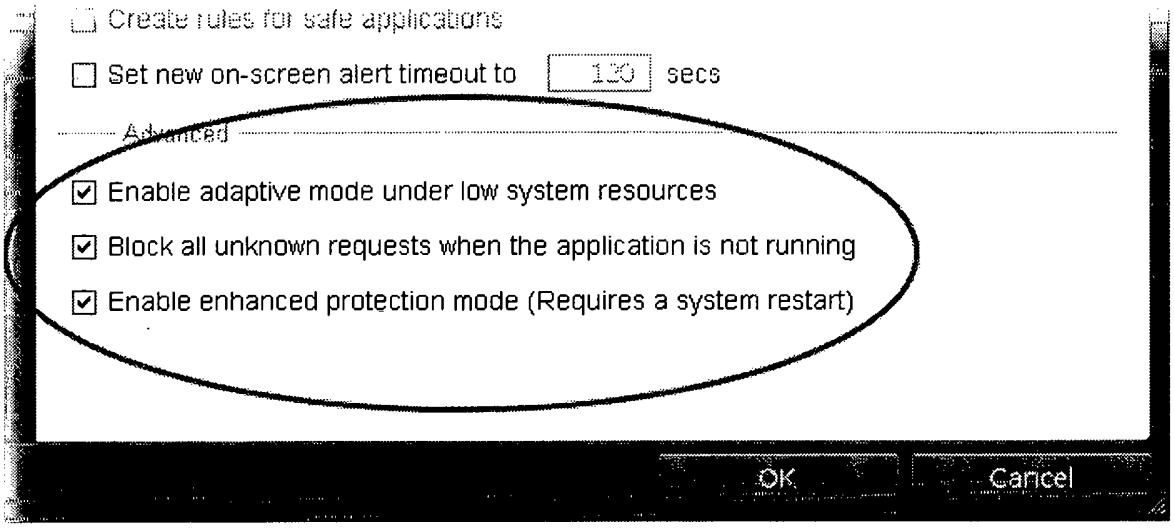
6. Click Monitoring Settings from the HIPS Settings interface



7. Make sure that all the check boxes are selected and click OK

Advanced Settings

8. Make the following settings under Advanced in the HIPS Settings interface



- Optional - Enable 'Block all unknown requests if the application is not running'. Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked.
- If you are using a 64-bit system, in order to maximize the security, it is important to select 'Enable enhanced protection mode (Requires a system restart)' - Enabling this mode will activate additional host intrusion prevention techniques in Defense+ to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures.

  Because of limitations in Windows 7 x64, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS in Defense+.

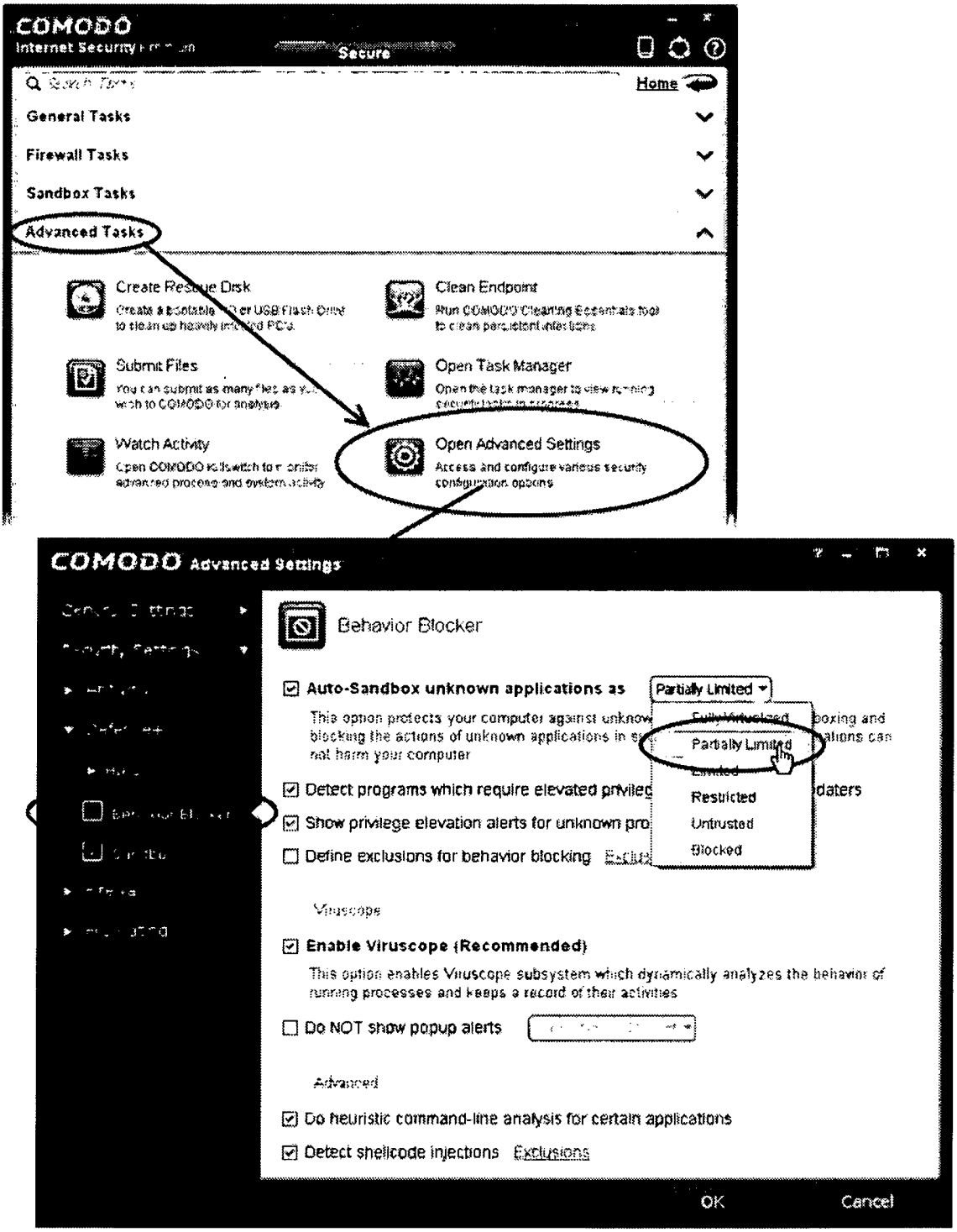
Click here for more details on HIPS Behavior Settings

Set up the Behavior Blocker for Maximum Security and Usability

This page explains on configuring the Behavior Blocker to auto-sandbox applications that are unrecognized by CIS to prevent potential damages to your system from untrusted programs.

To configure Behavior Blocker

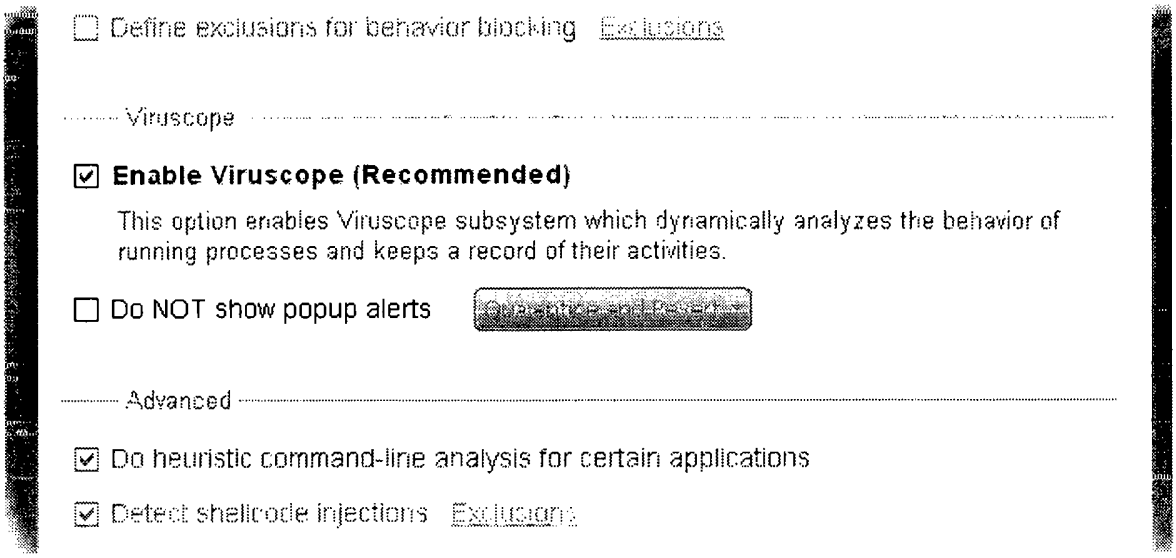
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'Behavior Blocker' from the left hand side pane



4. Make sure that the check box 'Auto-sandbox unknown applications as' is selected and choose 'Partially Limited' from the drop-down menu.

Viruscope Settings

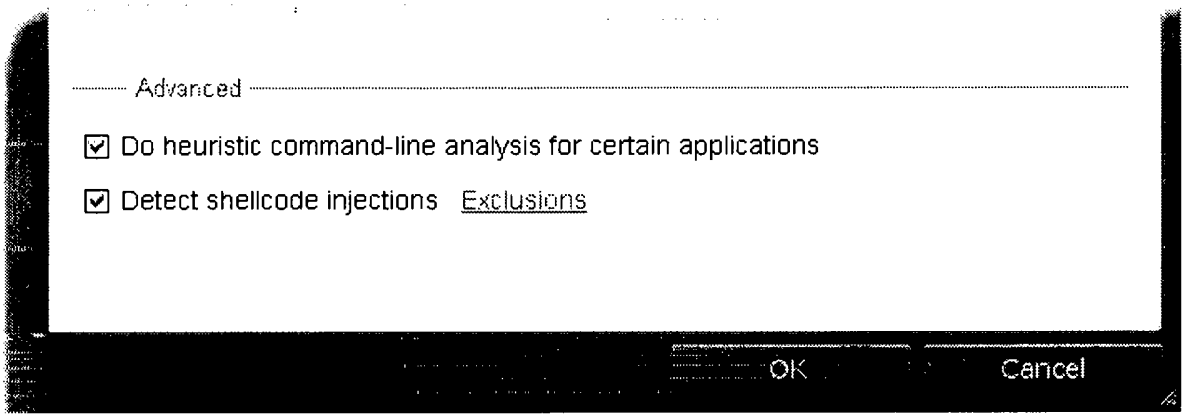
5. Make sure 'Enable Viruscope' checkbox is selected under 'Viruscope'



Advanced Settings

6. Make sure that both the check boxes:
    - Do heuristic command-line analysis for certain applications;
    - Detect shellcode injections

    ... are selected.



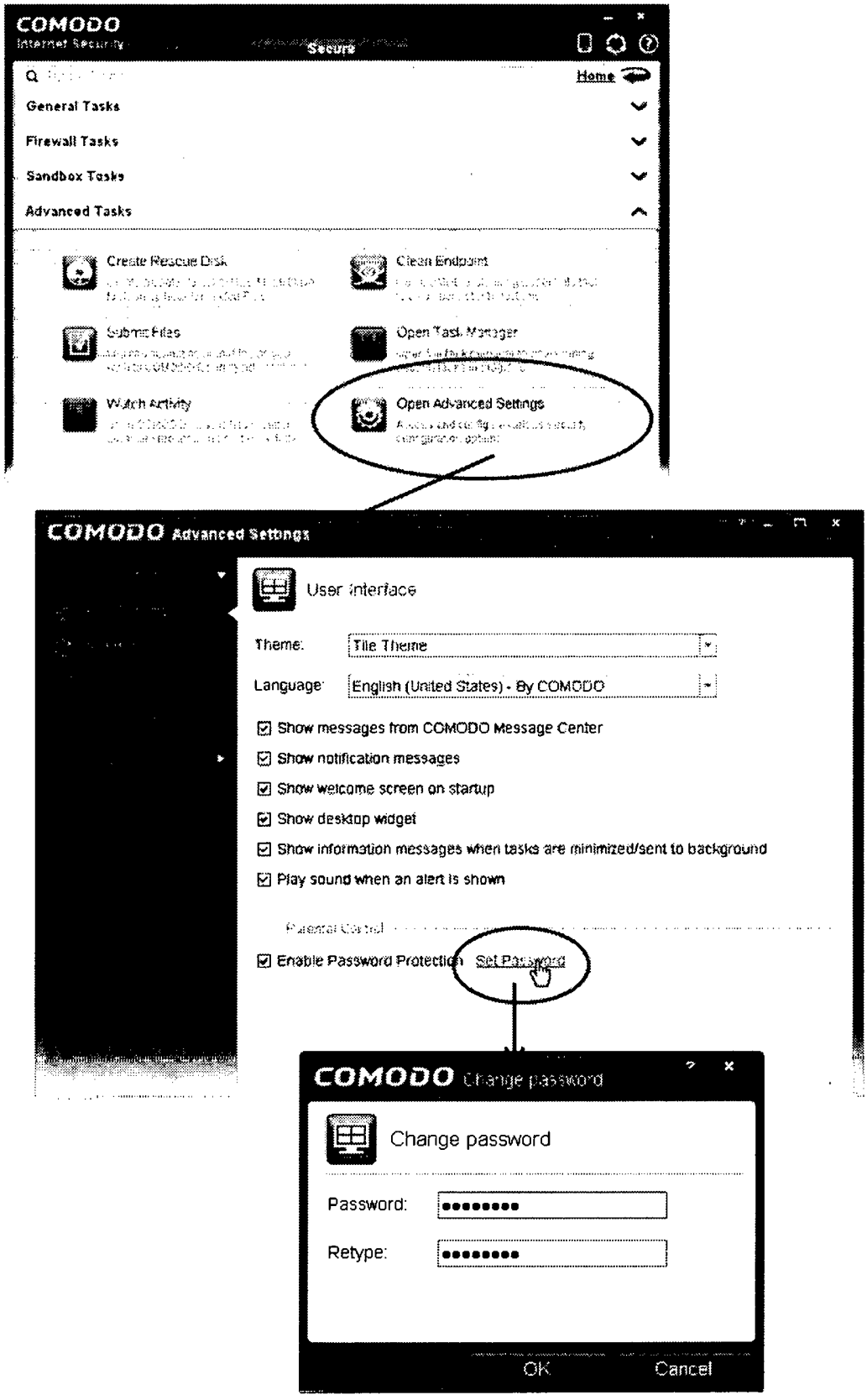
Click here for more details on Behavior Blocker Settings

Password Protect Your CIS Settings

This page explains how to password protect access to the CIS interface. Implementing the steps explained on this page means another user will not be able to access the CIS interface to modify or over-ride the security settings you have implemented.

To enable password protection

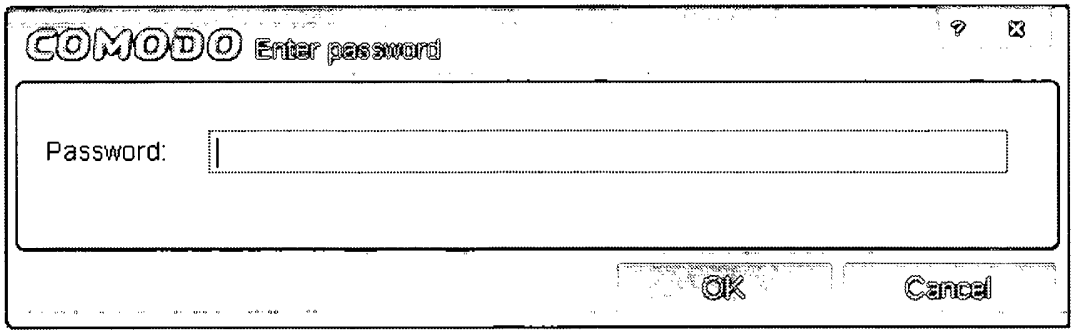
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'User Interface' under General Settings from the left hand side pane



4. Select 'Enable Password Protection' under 'Parental Control' and click 'Set Password' link. The Change password dialog will appear.

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

The configuration is now password protected. From the next attempt to change any configuration changes to CIS, you will be prompted to enter the password to proceed.



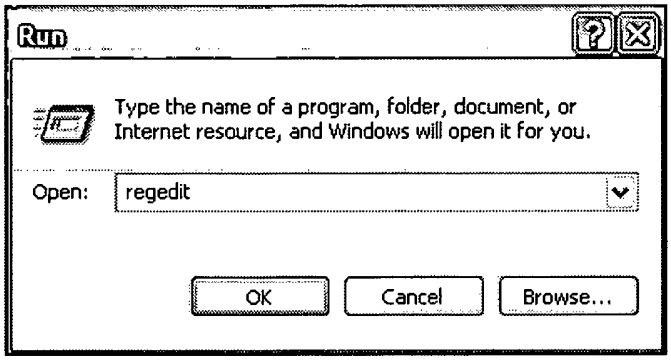
Reset Forgotten Password (Advanced)

This page explains how to remove password protection/reset password just in case you forgot the password you had set for COMODO Internet Security.

Note: It is not possible to 'retrieve' a forgotten password - you can only reset it. To do this involves modification of the Windows registry and is only recommended for experienced users.

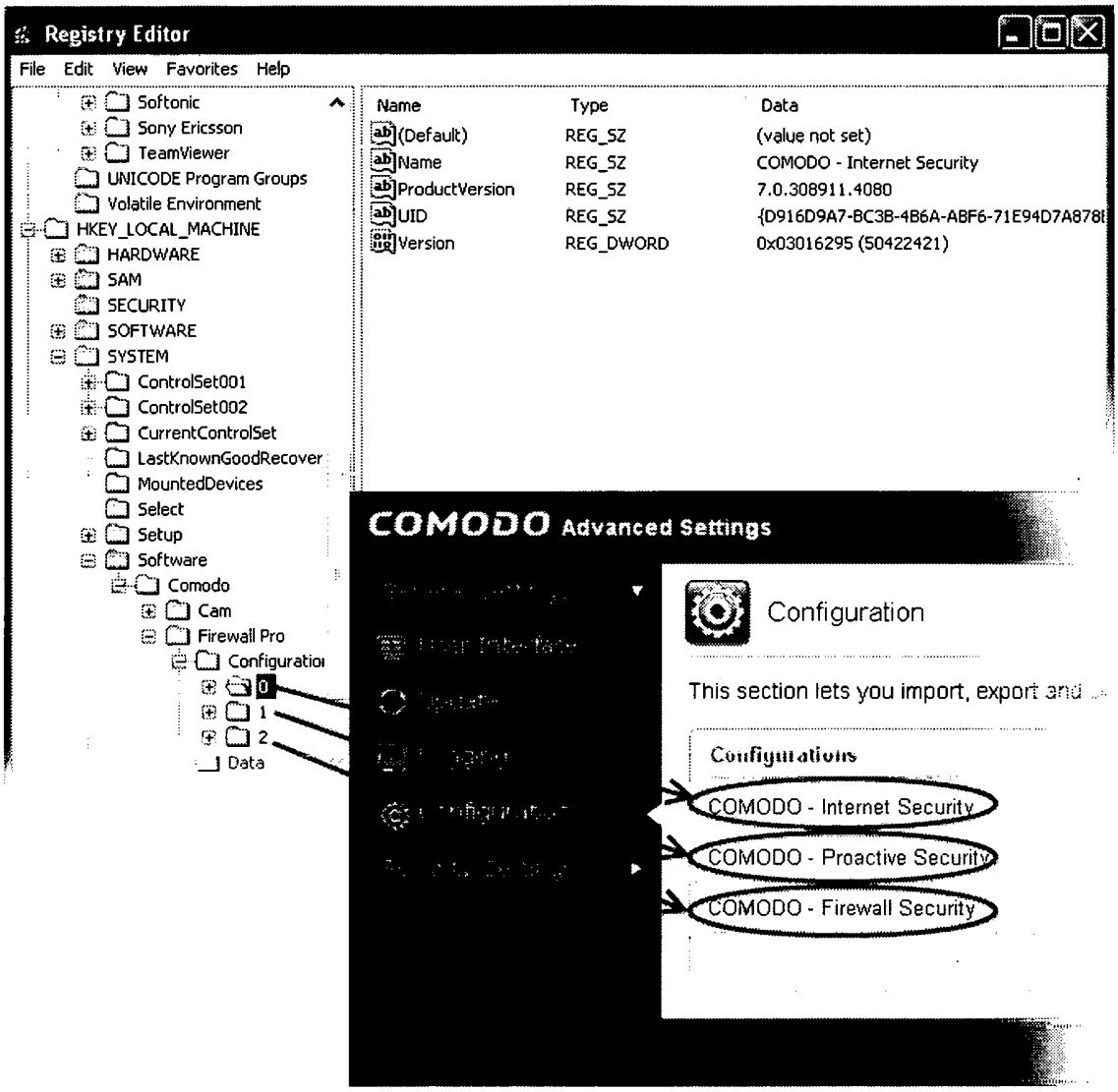
To disable password protection in CIS

1. Click Start > Run, from the Windows Start menu
2. Type 'regedit' in the text box and click 'OK'

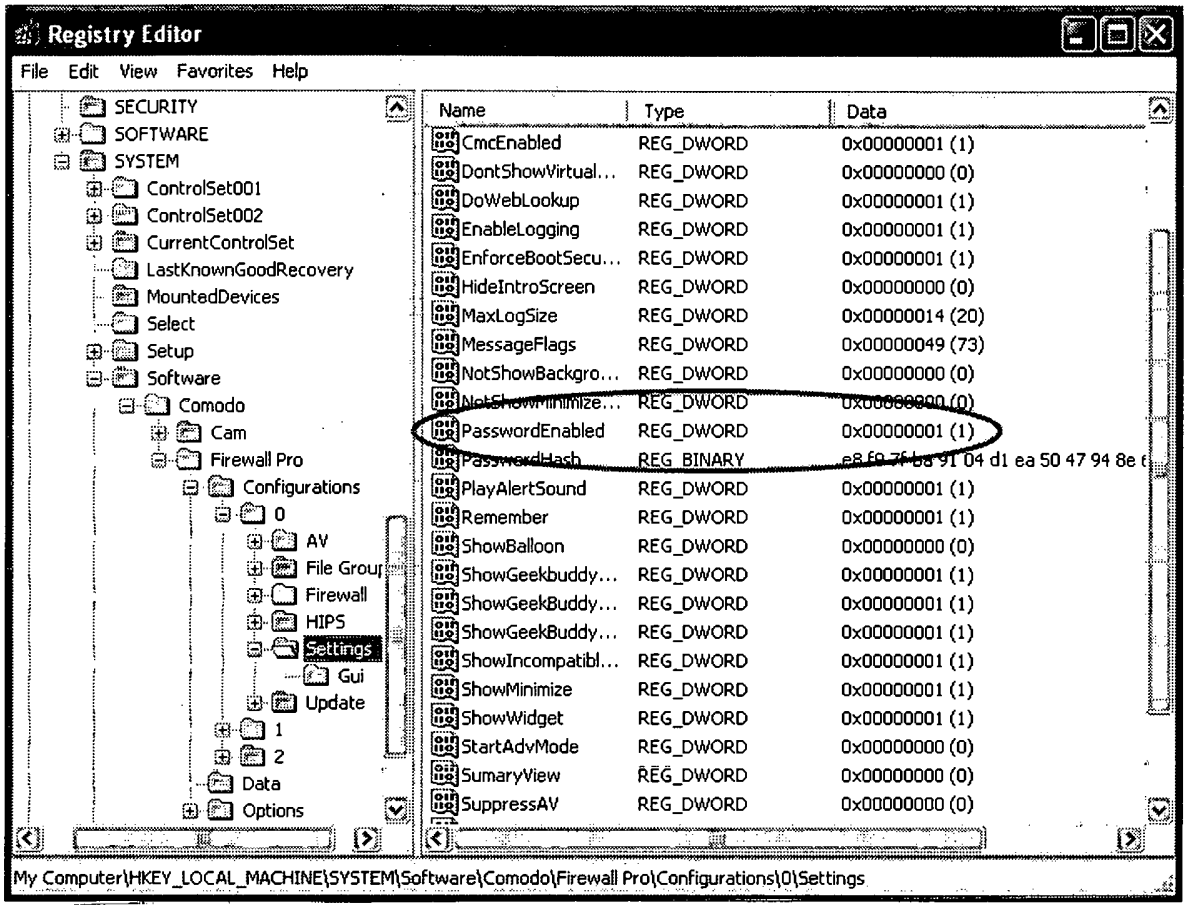


3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\

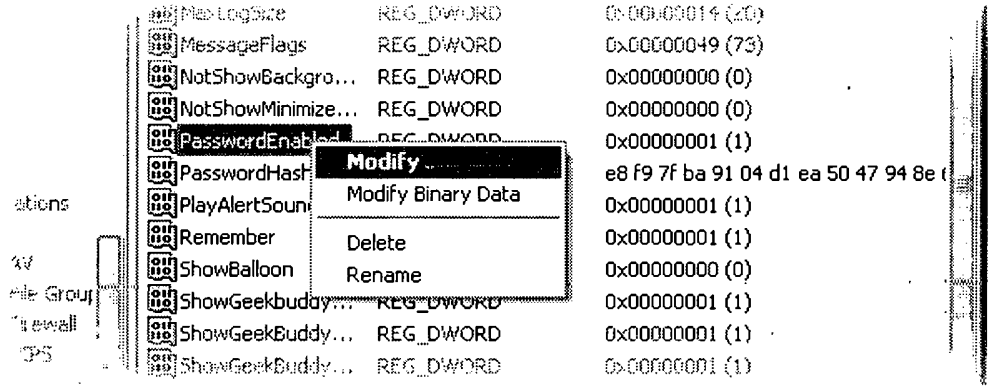
Under the Configurations folder you will see sub-folders named 0,1,2,... depending on the number of preset configurations in CIS. These folders contain registry keys for the settings of the preset configurations in the order of the configurations displayed in **Advanced Settings > General Settings > Configuration** interface. For example, the folder 0 contains the keys for COMODO - Internet Security, the folder 1 contains the keys for COMODO - Proactive Security and so on.



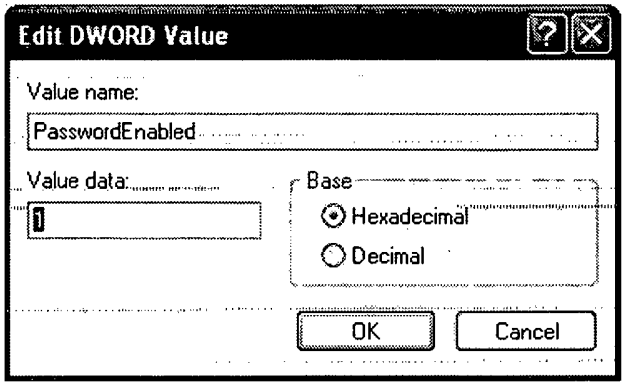
4. Select the folder corresponding to the configuration for which you wish to reset the password and navigate to Settings, for example, navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\0\Settings to reset password in COMODO - Internet Security configuration.



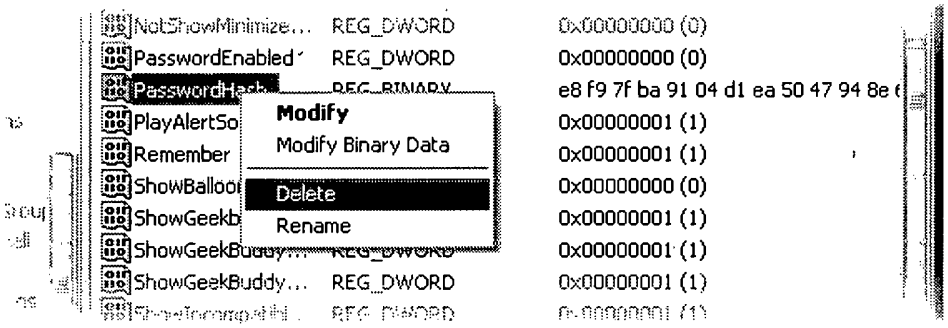
5. Right-click 'PasswordEnabled' key and select 'Modify'



6. In the 'Edit DWORD Value dialog box, change the 'Value data' from 1 to 0



7. Click 'OK'
8. Right-click 'PasswordHash' and select 'Delete'.



9. Restart the system for the changes to take effect

Now you should be able to access all settings, uninstall CIS and set a new password.

Note: If CIS doesn't allow regedit to change those registry items, try to boot in safe mode and repeat the above steps.

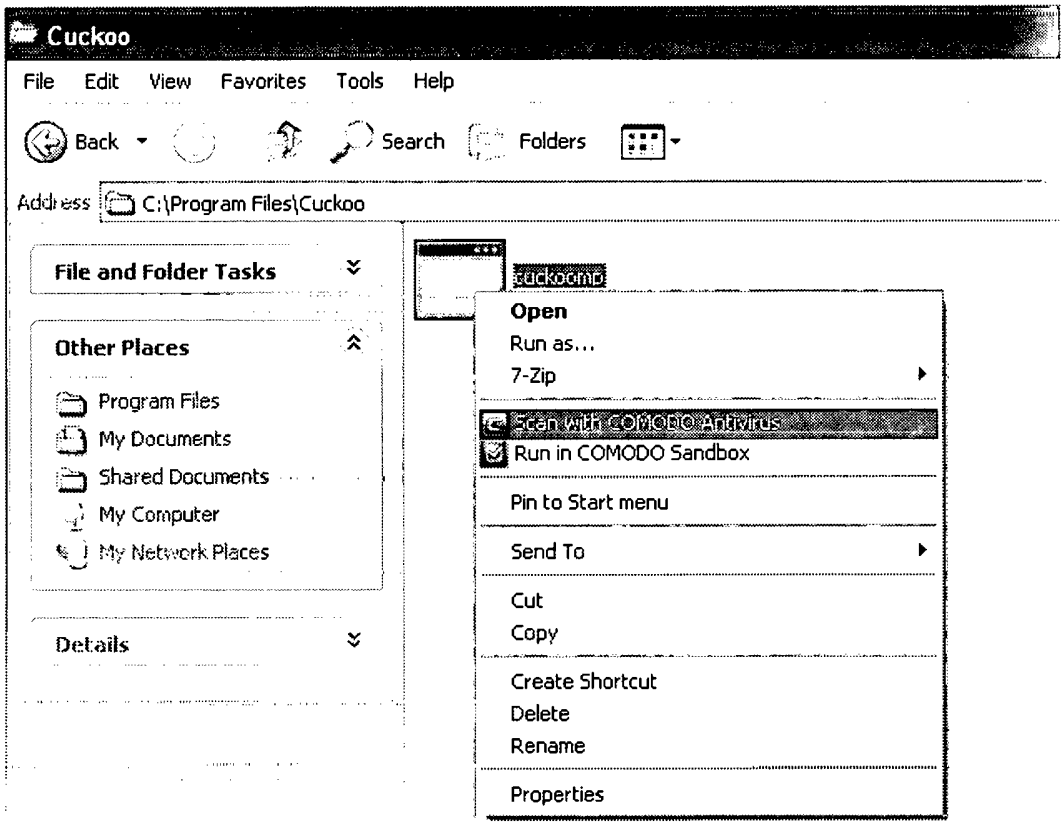
Run an Instant Antivirus Scan on Selected Items

You can run an instant antivirus scan on any selected area like disks, folders files etc. You can also check a wide range of removable storage devices such as CDs, DVDs, external hard-drives, USB connected drives, digital cameras - even your iPod and mobile phones too!!! This is useful if you have just copied a file/folder or a program from an external device like a USB drive, another system in your network, or downloaded from the Internet.

Click here for more details on running on-demand scans.

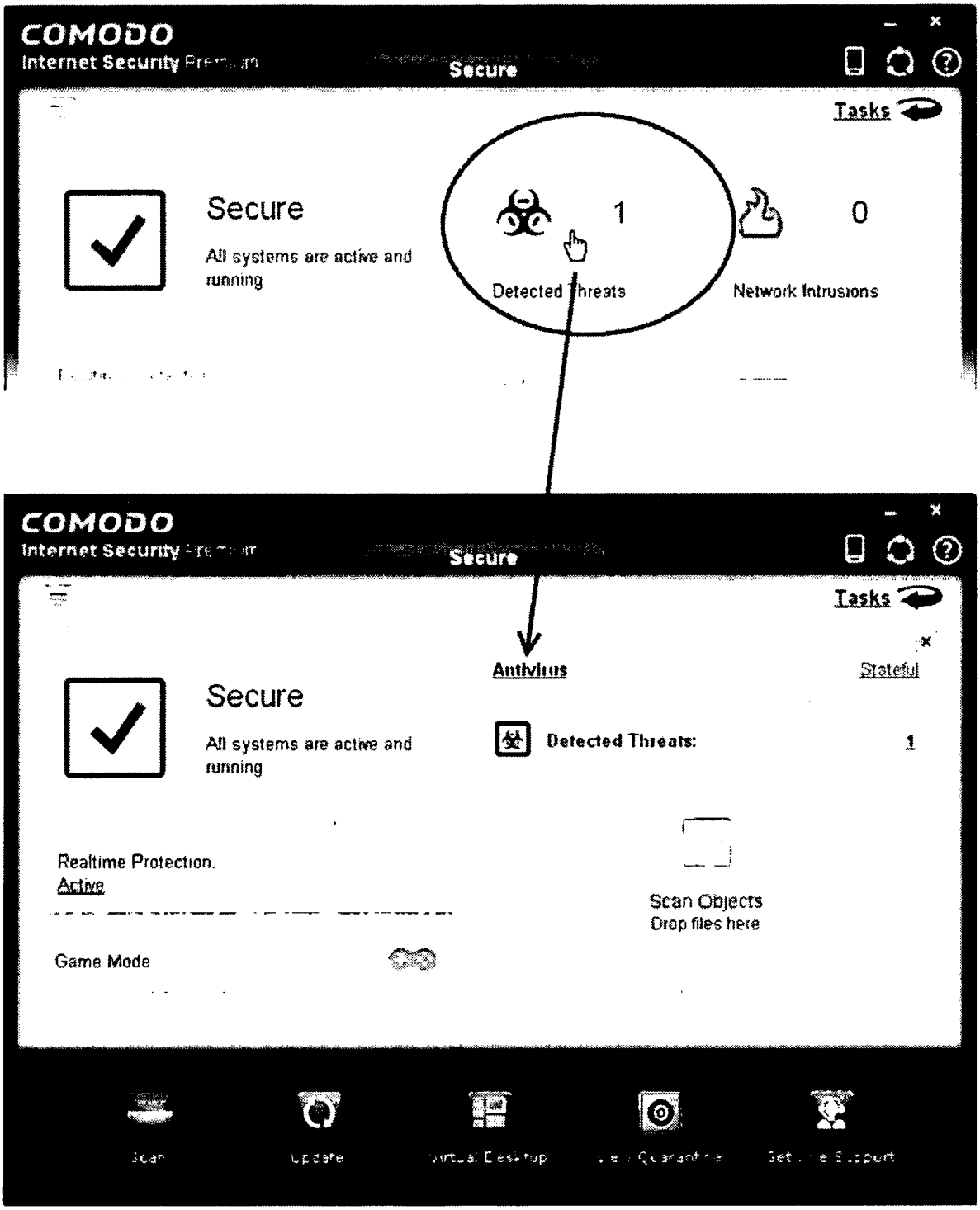
To instantly scan an item

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

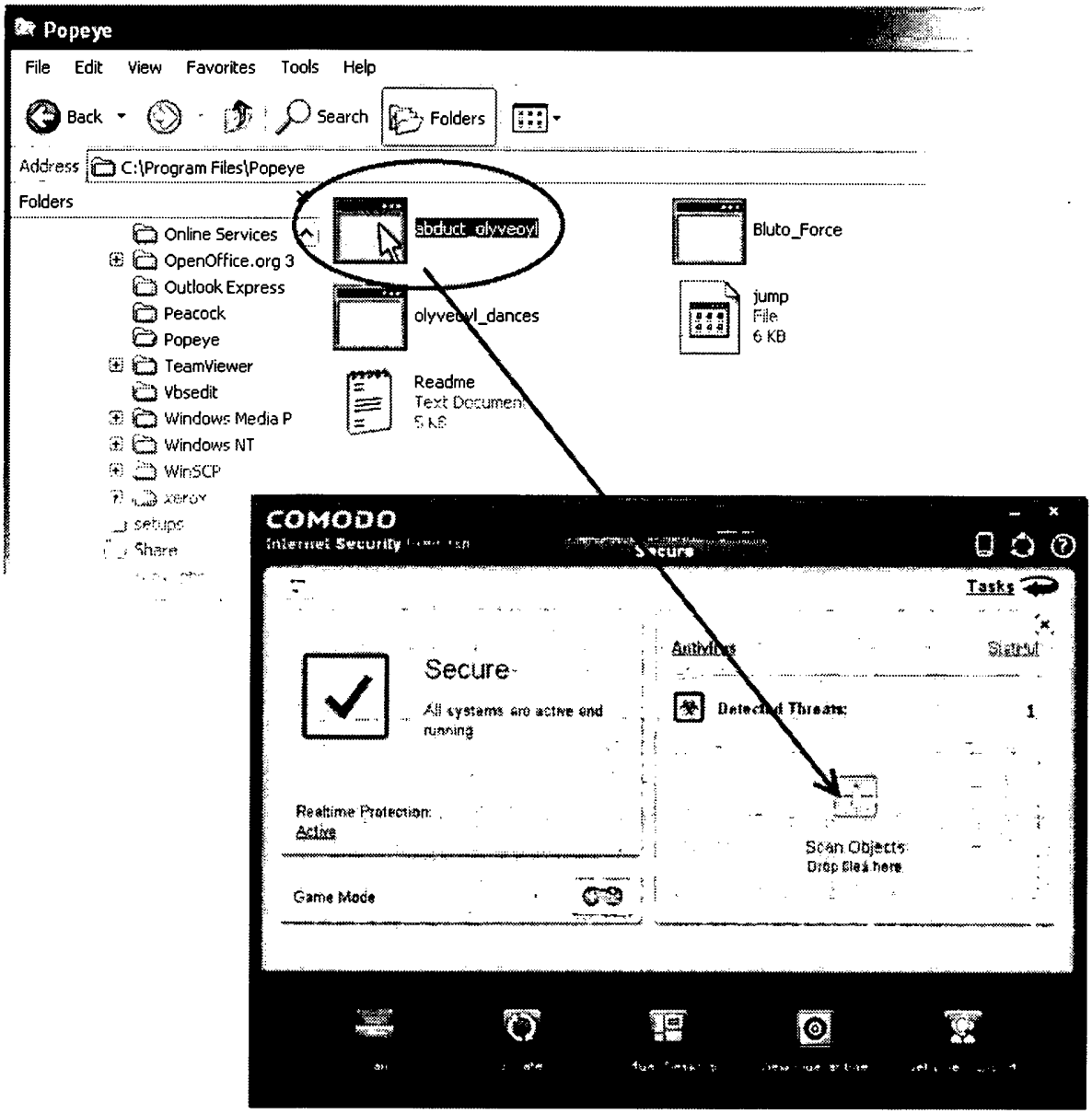


OR

- Click the Antivrus tile at the 'Home' screen in compact view to flip-open the Antivirus pane

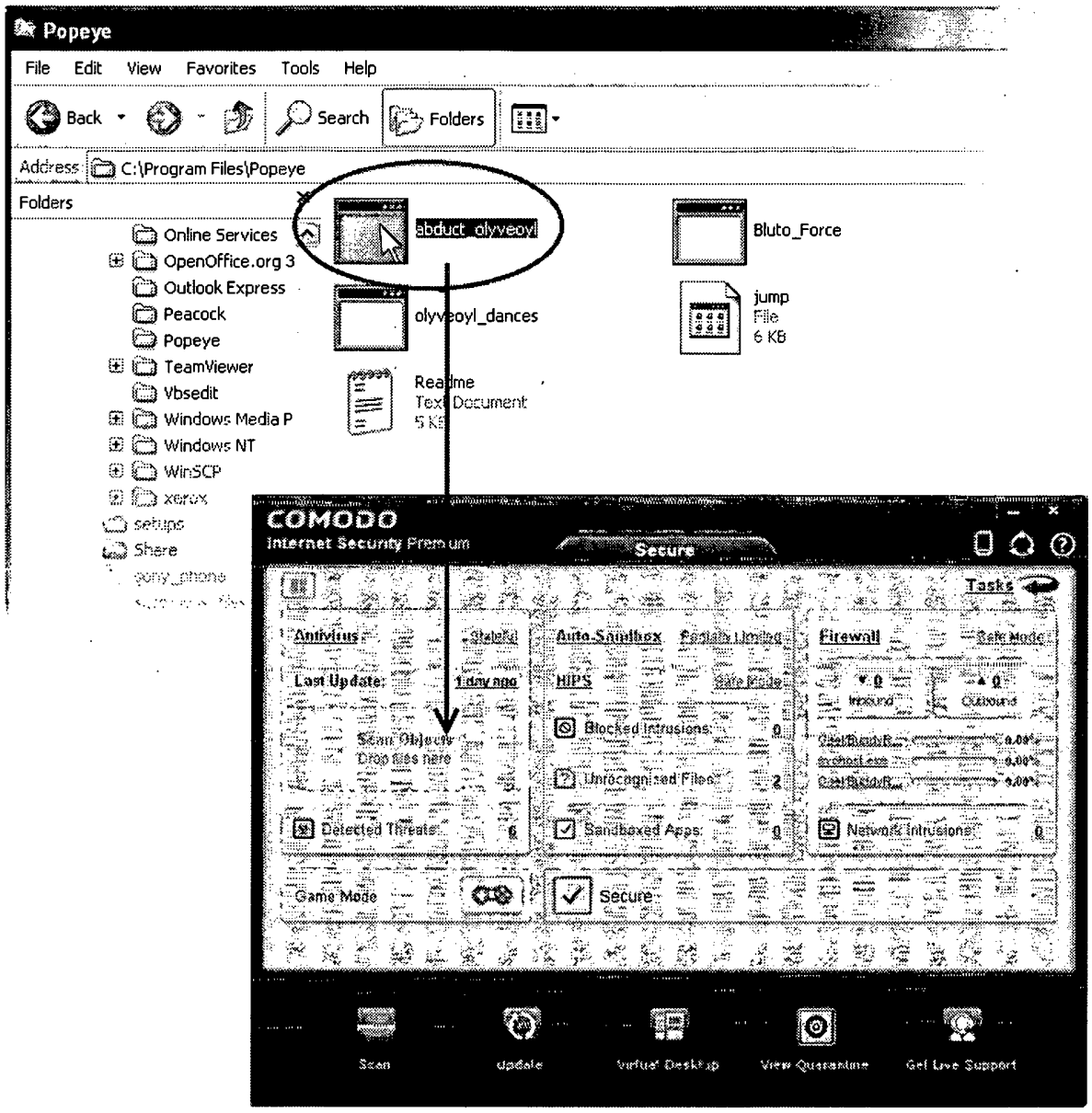


- Drag and drop the item over the area marked 'Scan Objects'.



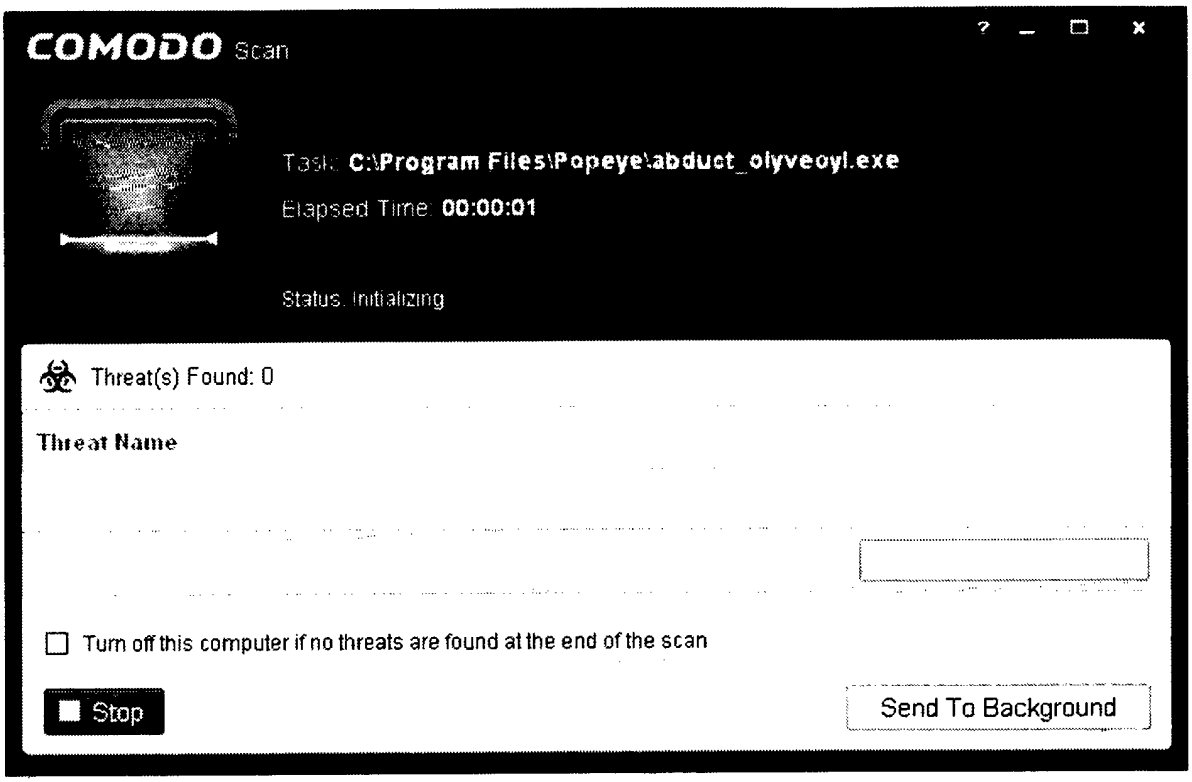
OR

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



The item will be scanned immediately.

Best Available Copy



...and on completion of scanning, the scan finished dialog be displayed with the number of threats found.

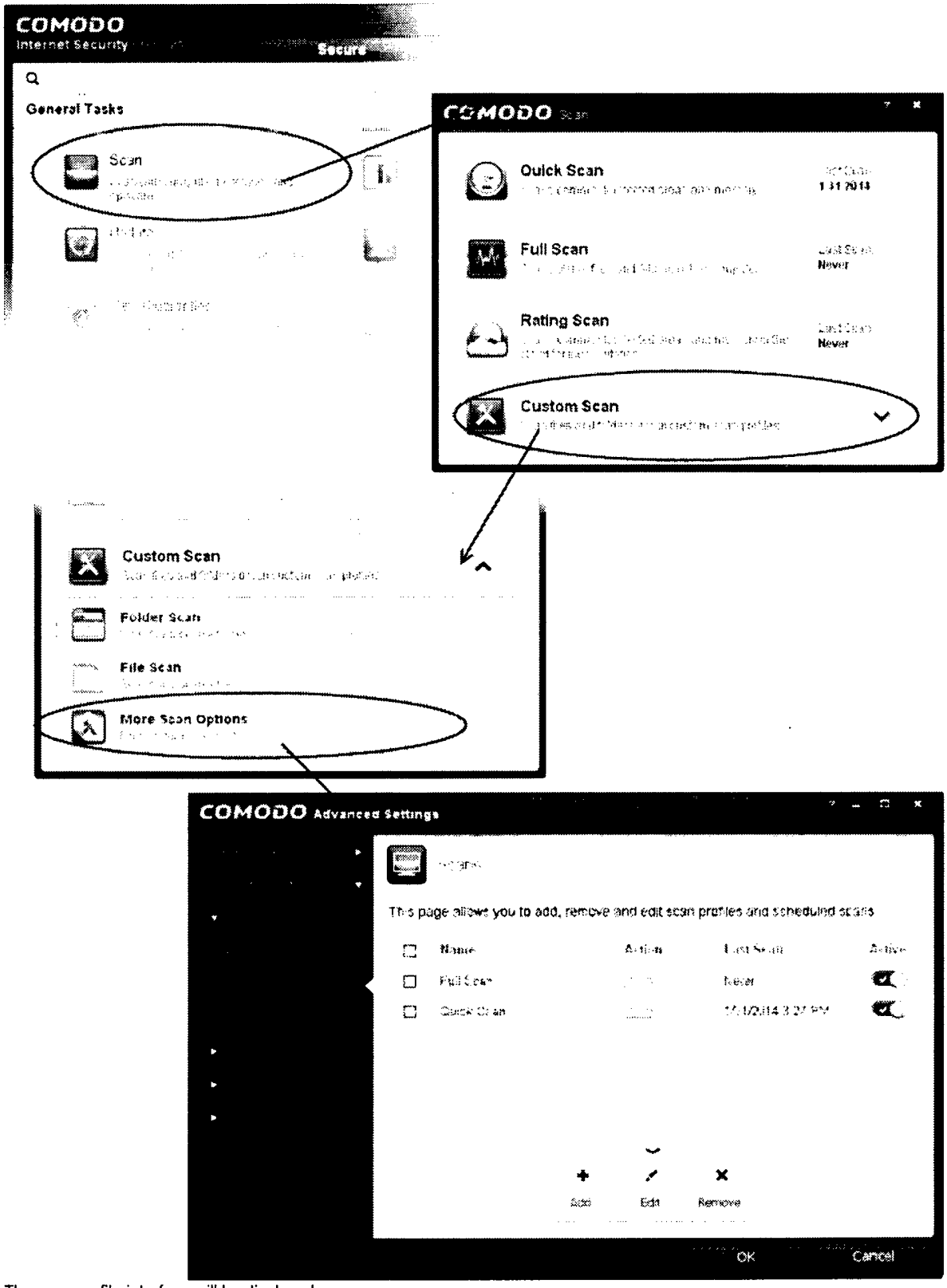
Click here for more details to take action on the infected item(s).

Create an Antivirus Scanning Schedule

Comodo Internet Security allows you to schedule Antivirus scans on your entire system or on specific areas according to your preferences. You can create a custom scan profile defining exactly which files and folders are to be scanned, when they are to be scanned and how they are to be scanned.

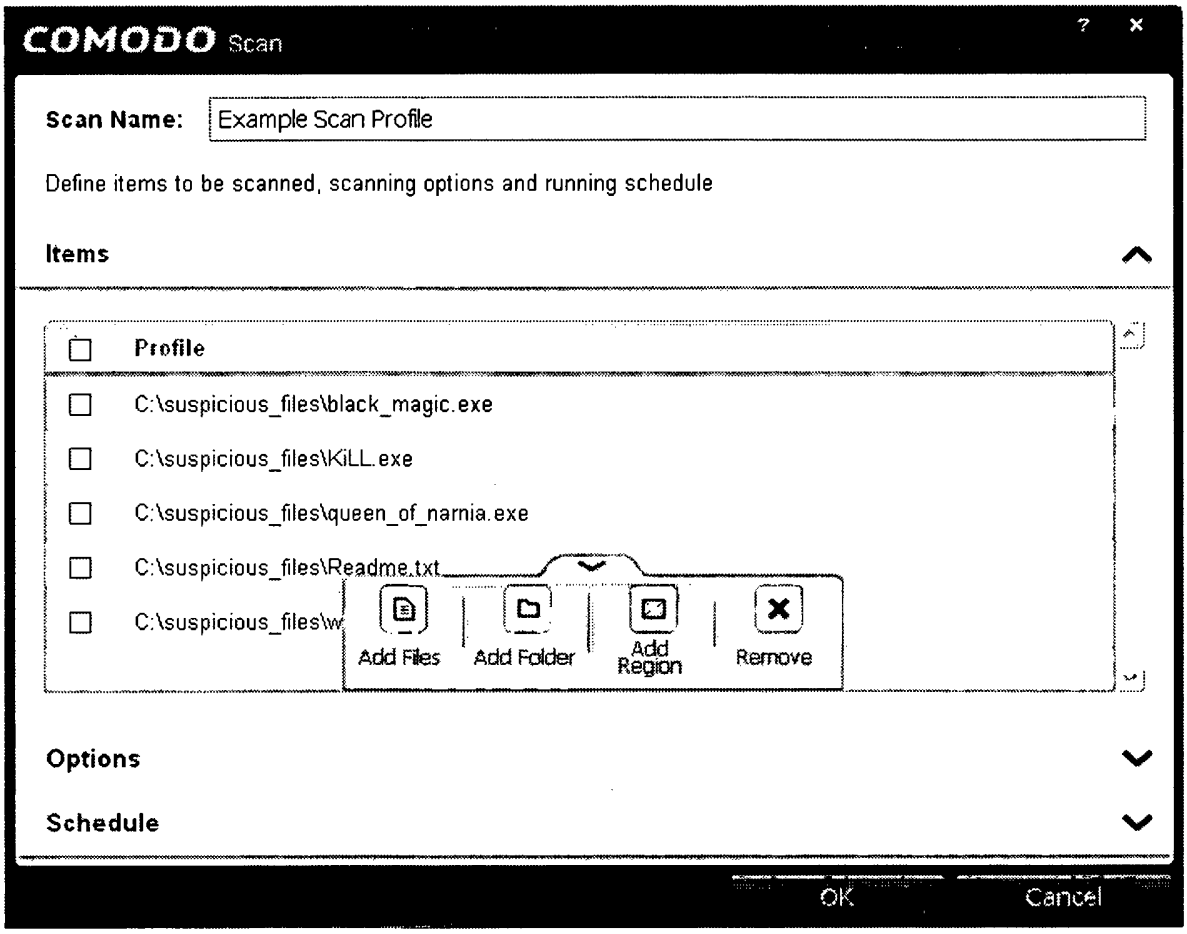
To create an antivirus scanning schedule

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

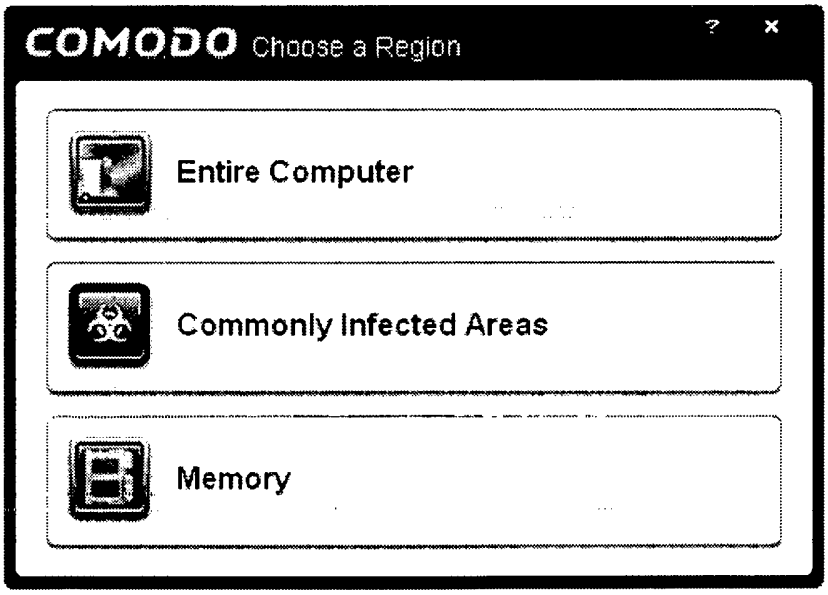


The scan profile interface will be displayed.

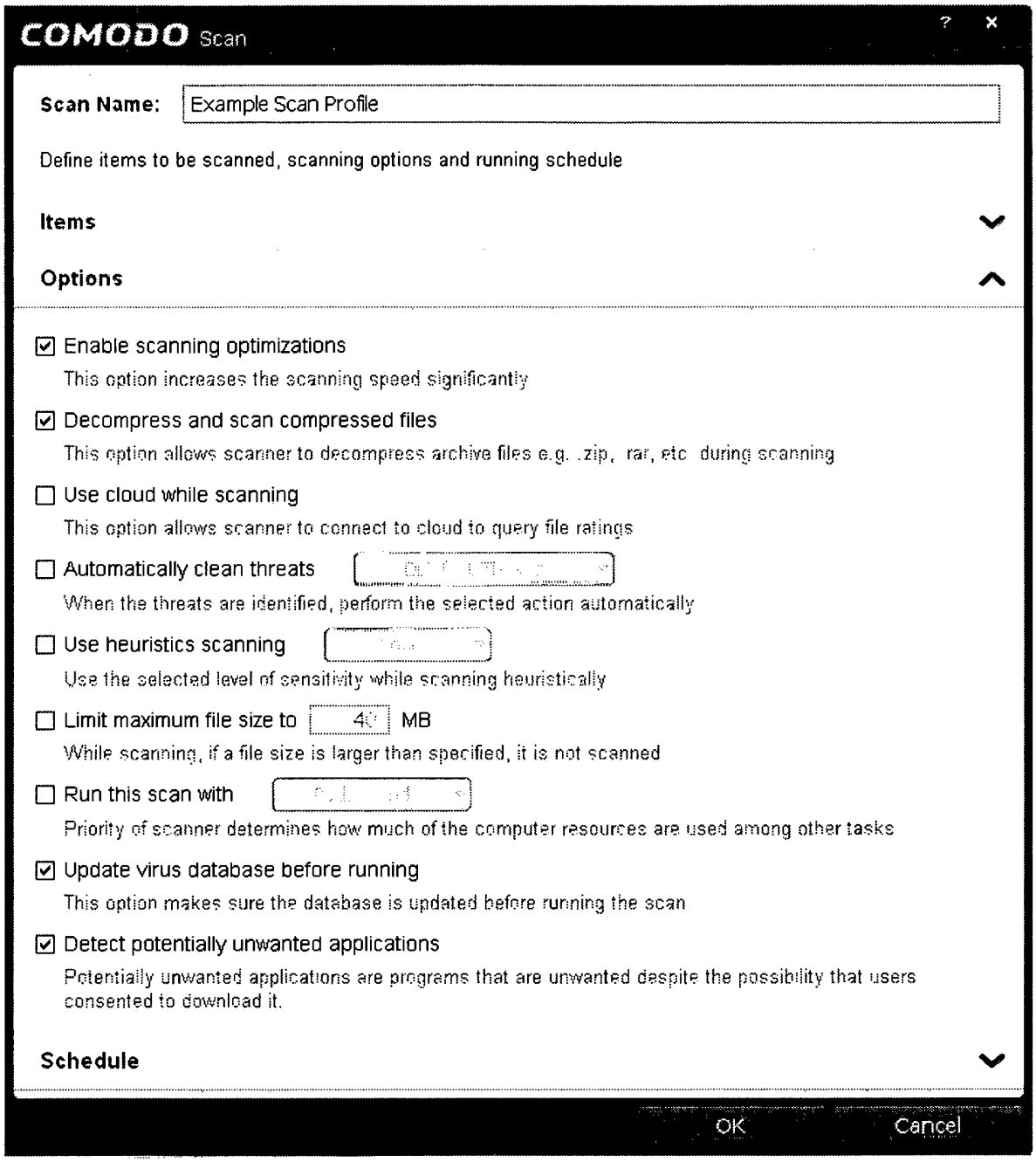
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



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



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



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

scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Disabled).***

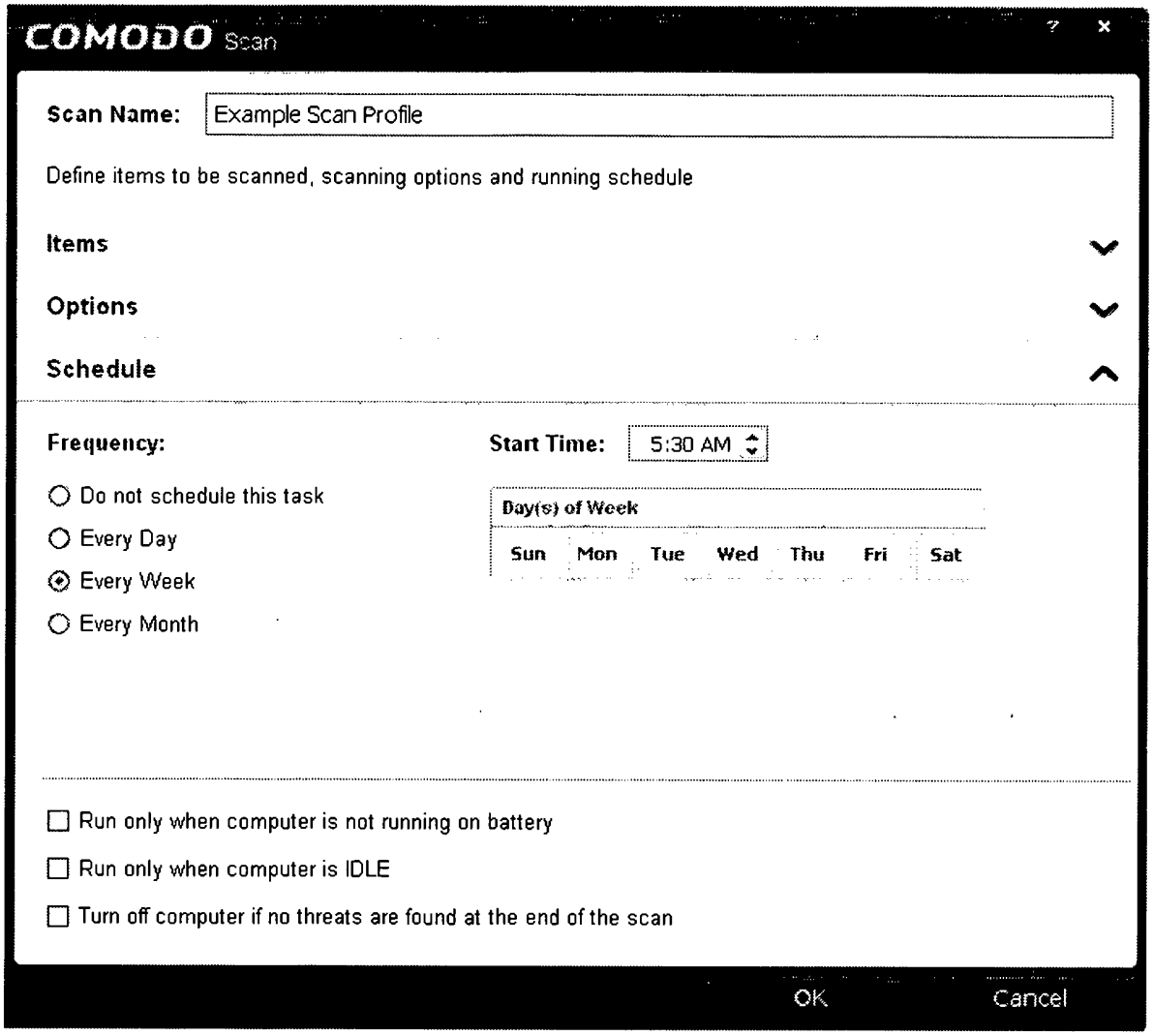
Background Info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so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

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

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

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

- To schedule the scan to run at set intervals, click 'Schedule':



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

- Click OK to save the profile.

The profile will be saved and the selected areas will be scanned repeatedly as per the set schedule.

Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row

to toggle between on and off status.

Run Untrusted Programs In the Sandbox

Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows hows a 'virtual' shortcut will appear on your desktop:



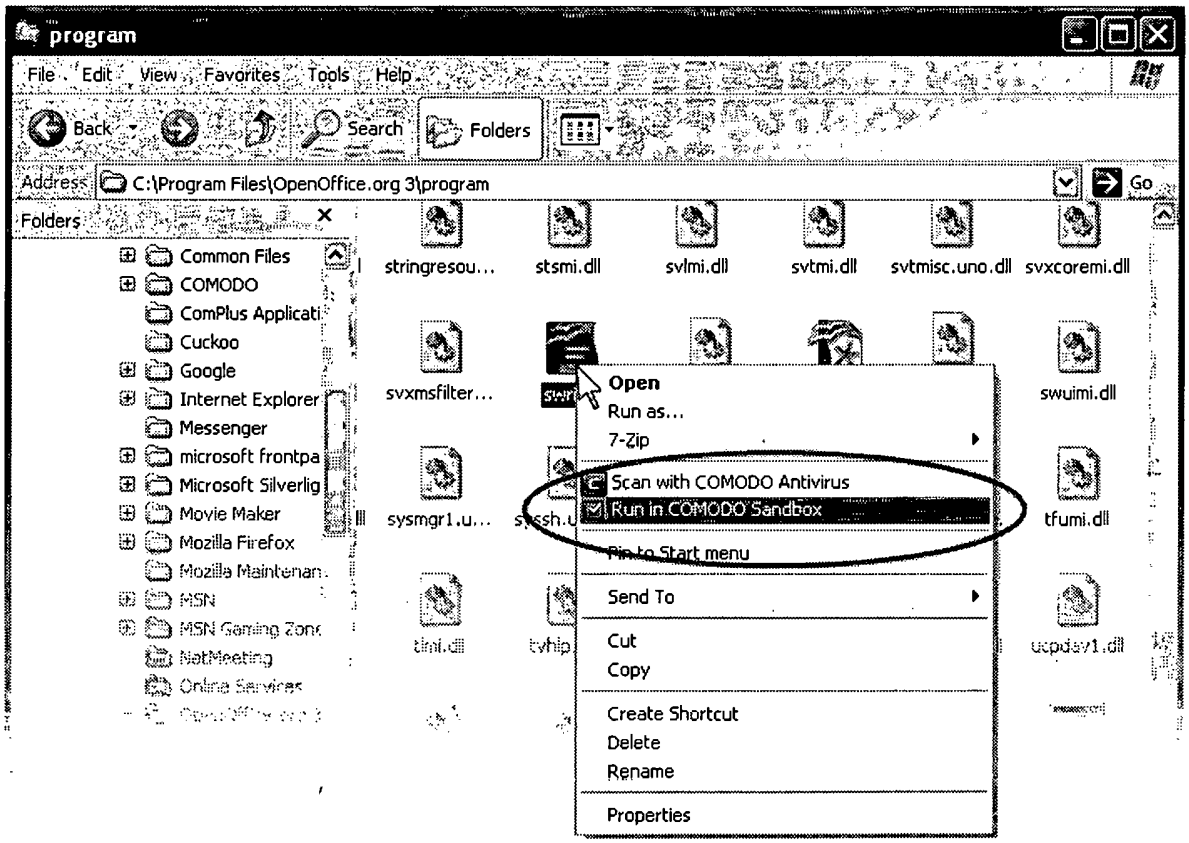
Comodo Internet Security allows you to run a program in the sandbox:

- **From the right click options**
- **From the Sandbox Tasks interface**

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

Run a program inside the sandbox through right click options

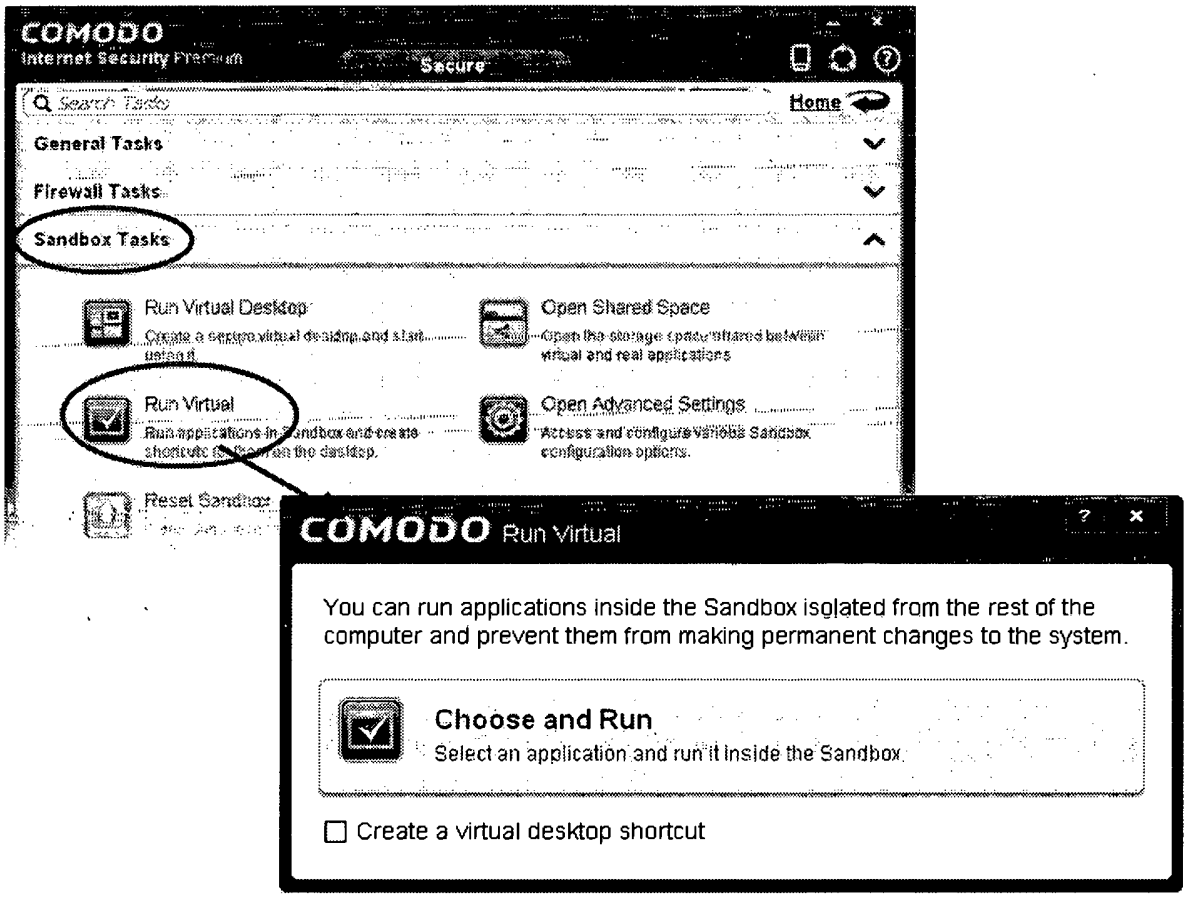
1. Browse to the installation folder of the .exe file through Windows Explorer
2. Right click on the program that you want to run inside the sandbox



3. Choose 'Run in Comodo Sandbox' from the context sensitive menu

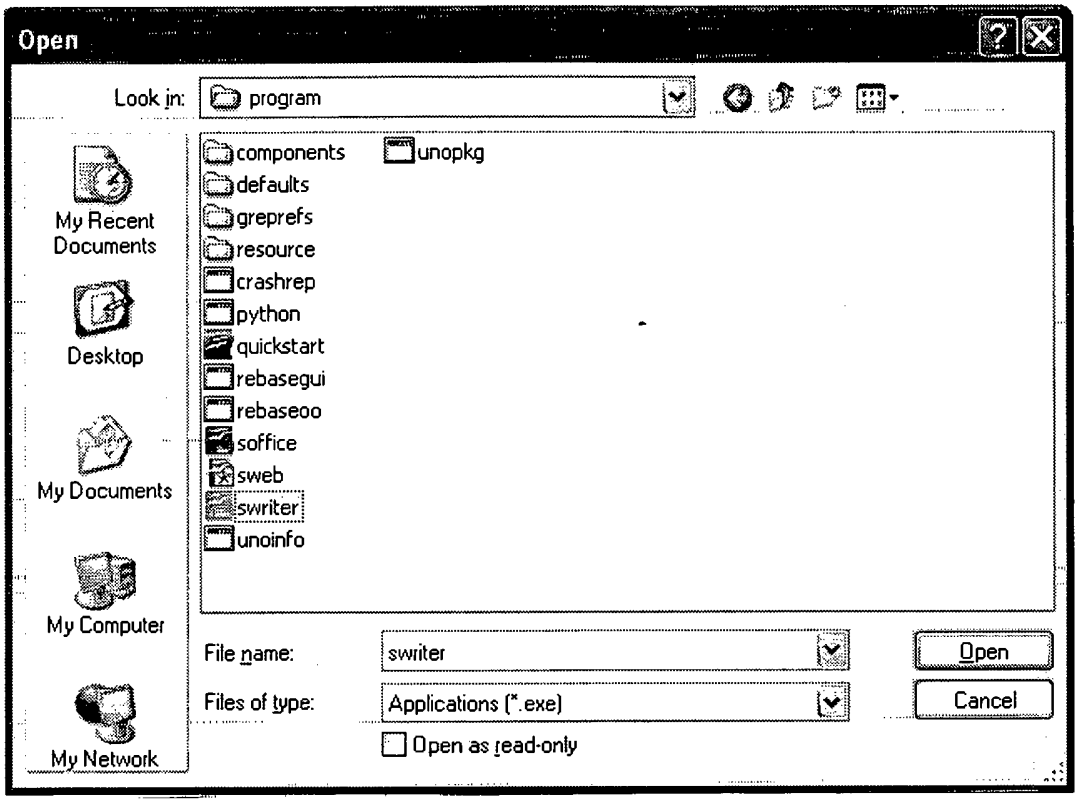
Run a program in sandbox from Sandbox Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Sandbox Tasks' and click 'Run Virtual' from the 'Sandbox Tasks' interface



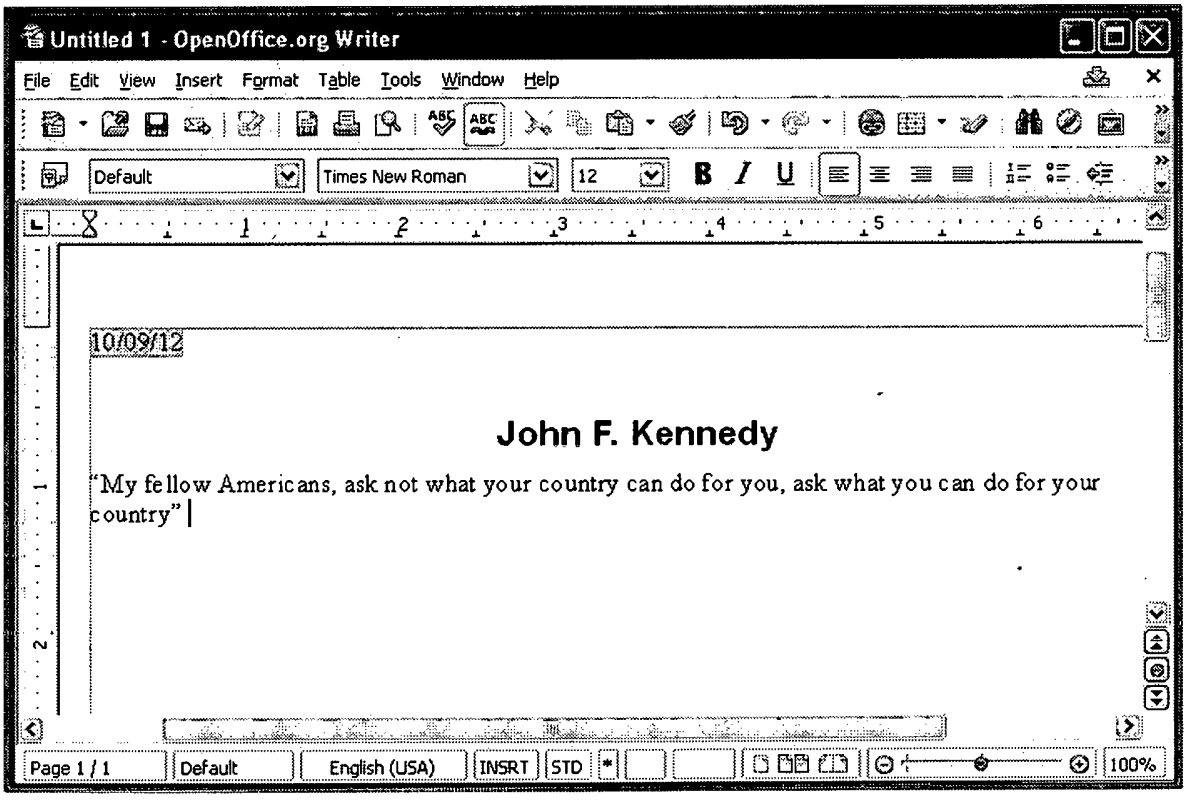
The 'Run Virtual' dialog will be displayed.

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



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

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



Run Browsers Inside Sandbox

This page explains how to run your Internet browser inside the sandbox. Surfing the Internet with a sandboxed browser is the same as normal, with the benefit that any malicious files you inadvertently download cannot do damage your real computer. You can also create a desktop shortcut to run the browser inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



Comodo Internet Security allows you to run a browser in the sandbox:

- **From the desktop widget**
- **From the Sandbox Tasks interface**

Starting a browser from the desktop widget

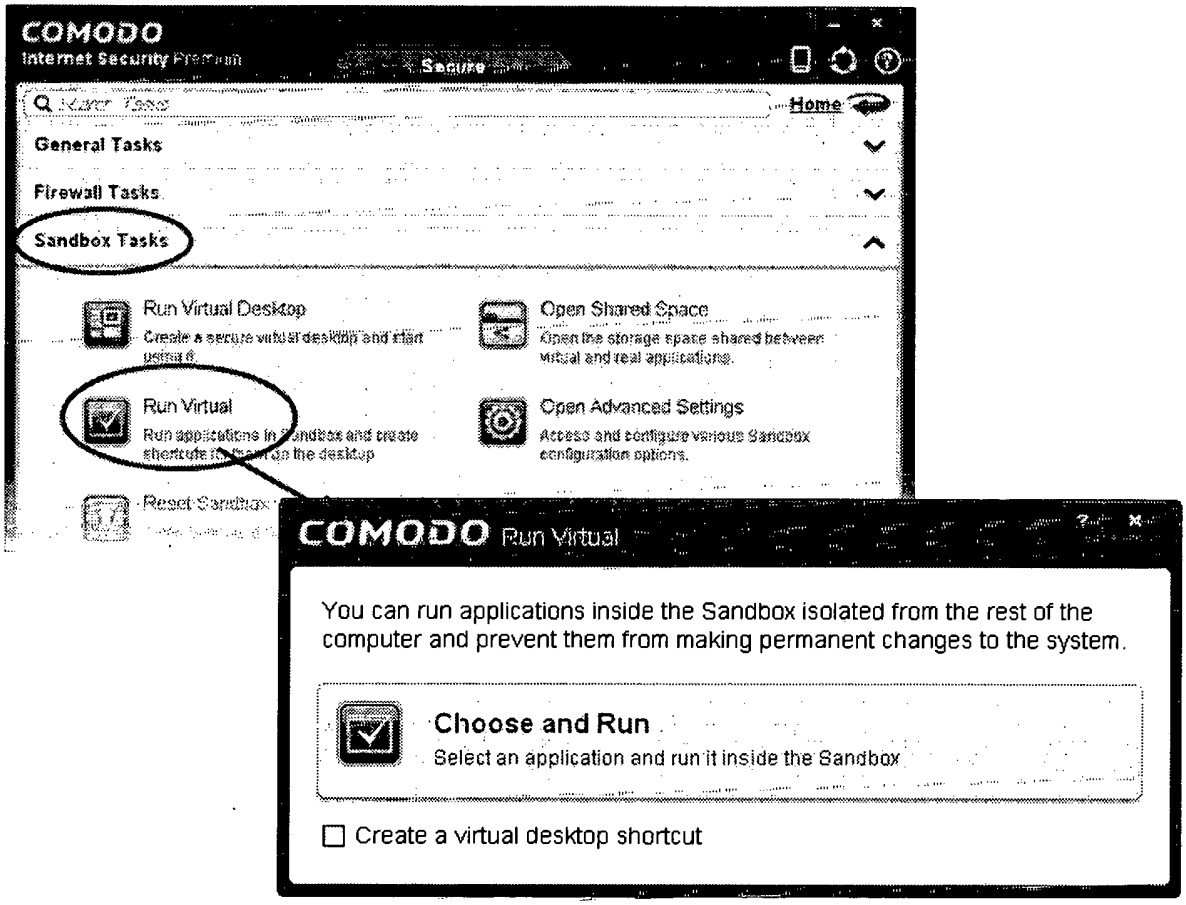
The CIS Desktop Widget displays shortcut icons of the browsers installed in your computer.



- To start a browser inside the sandbox, click on the browser icon.

Starting a browser from the Sandbox Tasks interface

1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. Click 'Sandbox Tasks' and click 'Run Virtual' from the 'Sandbox Tasks' interface



The 'Run Virtual' dialog will be displayed.

3. To run a browser inside the sandbox, click 'Choose and Run', navigate to the installation location of the browser and select the exe file of the browser. If you wish to create a desktop shortcut to run the browser in the sandbox in future, then select 'Create a virtual desktop shortcut'.

The browser will run with a green border indicating that it is sandboxed.

Run Untrusted Programs Inside Virtual Desktop

This page explains how to run untrusted programs inside the Virtual Desktop. Applications running in the virtual desktop also leave no cookies or history behind on your real system, making it ideal for testing out beta/unstable software.

Applications installed or the files stored in your system can be opened inside the Virtual Desktop by the following methods:

- **Opening the applications/files from the desktop shortcuts**
- **Sharing the application/files through the Shared Space folder**

Desktop Shortcuts

You can copy the files or create shortcuts for the applications/files to be opened in Virtual Desktop, in the desktop of your real system. The shortcuts of your real desktop will be available in the Virtual Desktop. You can double click on the icon to open the respective application of file inside the Virtual Desktop.

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

Shared Space

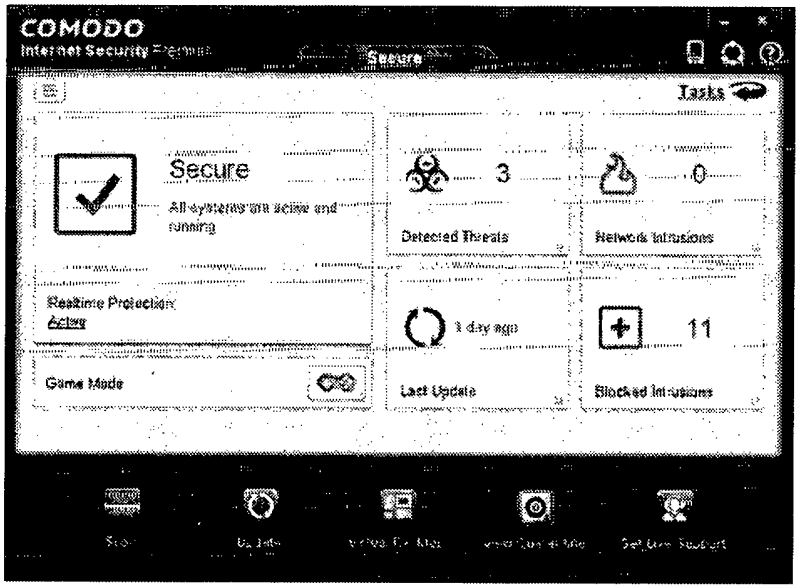
The Virtual Desktop creates a folder Shared Space in the location "C:\Documents and Settings\All Users\Application Data\Shared Space", which can be shared by your host operating system and the Virtual Desktop.

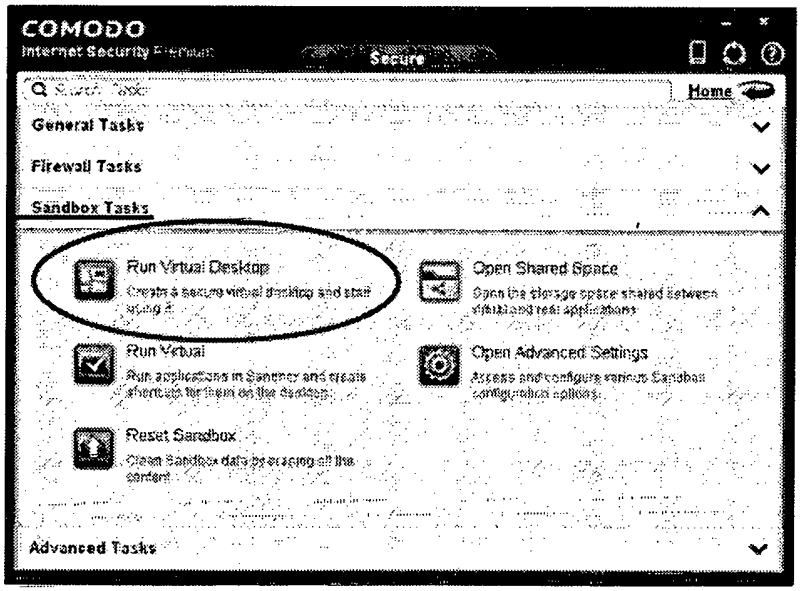
The Shared Space can be accessed in the following ways:

- Click 'Open Shared Space' under 'Sandbox' Tasks in the Tasks Interface
- Click the 'Shared Space' shortcut icon from the home screen of CIS
- Click the 'Shared Space' shortcut icon from the CIS widget
- Click the 'Shared Space' desktop shortcut icon

To open an application or file from your host system in the Virtual Desktop

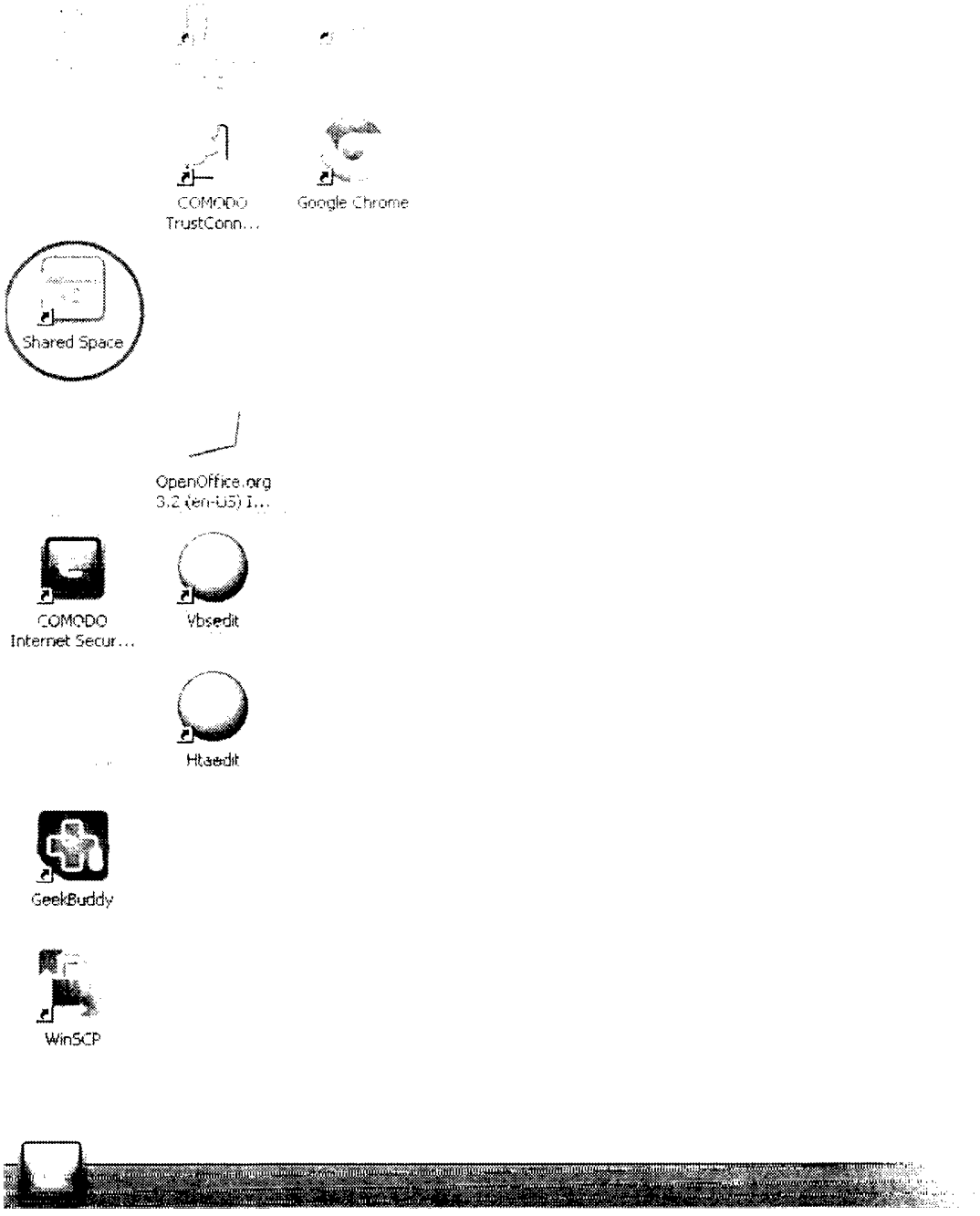
1. Open the 'Shared Space' as mentioned above
2. Copy/Move the application or the file to be opened into the Shared Space
3. Start 'Virtual Desktop' by clicking the Virtual Desktop shortcut in the CIS home screen or by clicking Sandbox Tasks > Run Virtual Desktop from the Tasks interface of CIS.





4. Open Shared Space inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.

Note: The Shared space home screen icon will be available only in the **Classic Windows Mode** and **Tablet + Classic Mode**



5. Double click on the application/file in the shared space to open it inside the virtual Desktop.

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

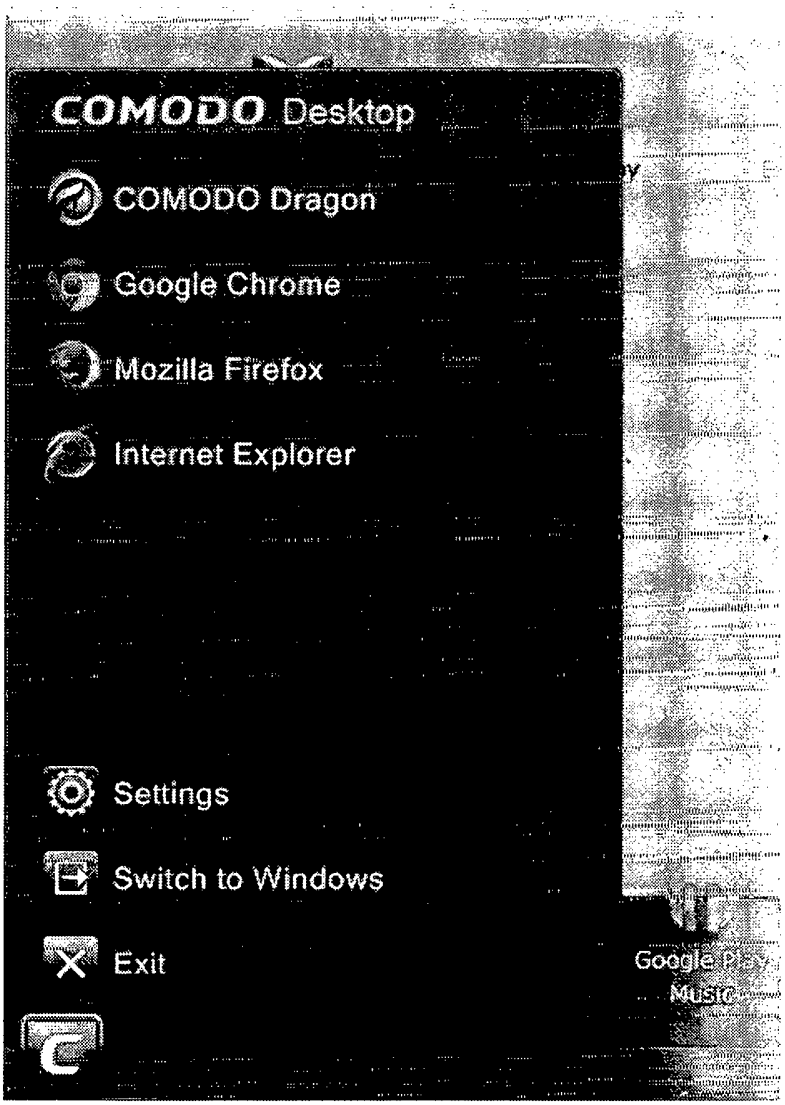
Run Browsers Inside the Virtual Desktop

The Virtual Desktop provides an extremely secure environment for Internet related activities because it isolates your browser

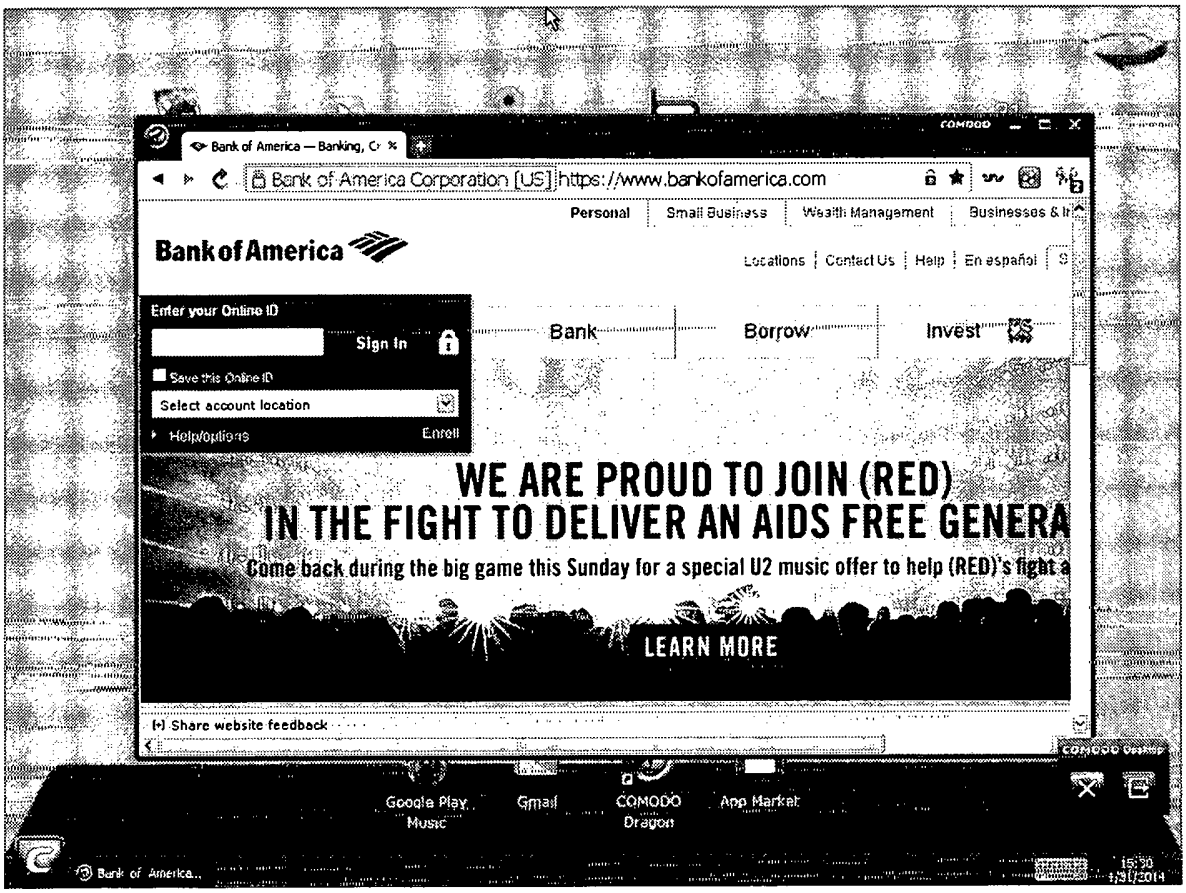
from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net inside the virtual desktop removes this threat to your machine by preventing any website from installing anything on your real computer. Furthermore, the Virtual Keyboard allows you to securely enter user-names, credit card numbers and passwords without fear of key-logging software recording your physical keystrokes.

To run a browser inside the Virtual Desktop

1. Click the 'C' button
2. Select the browser you want to run from the browsers displayed.



The browser will open inside the Virtual Desktop.



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

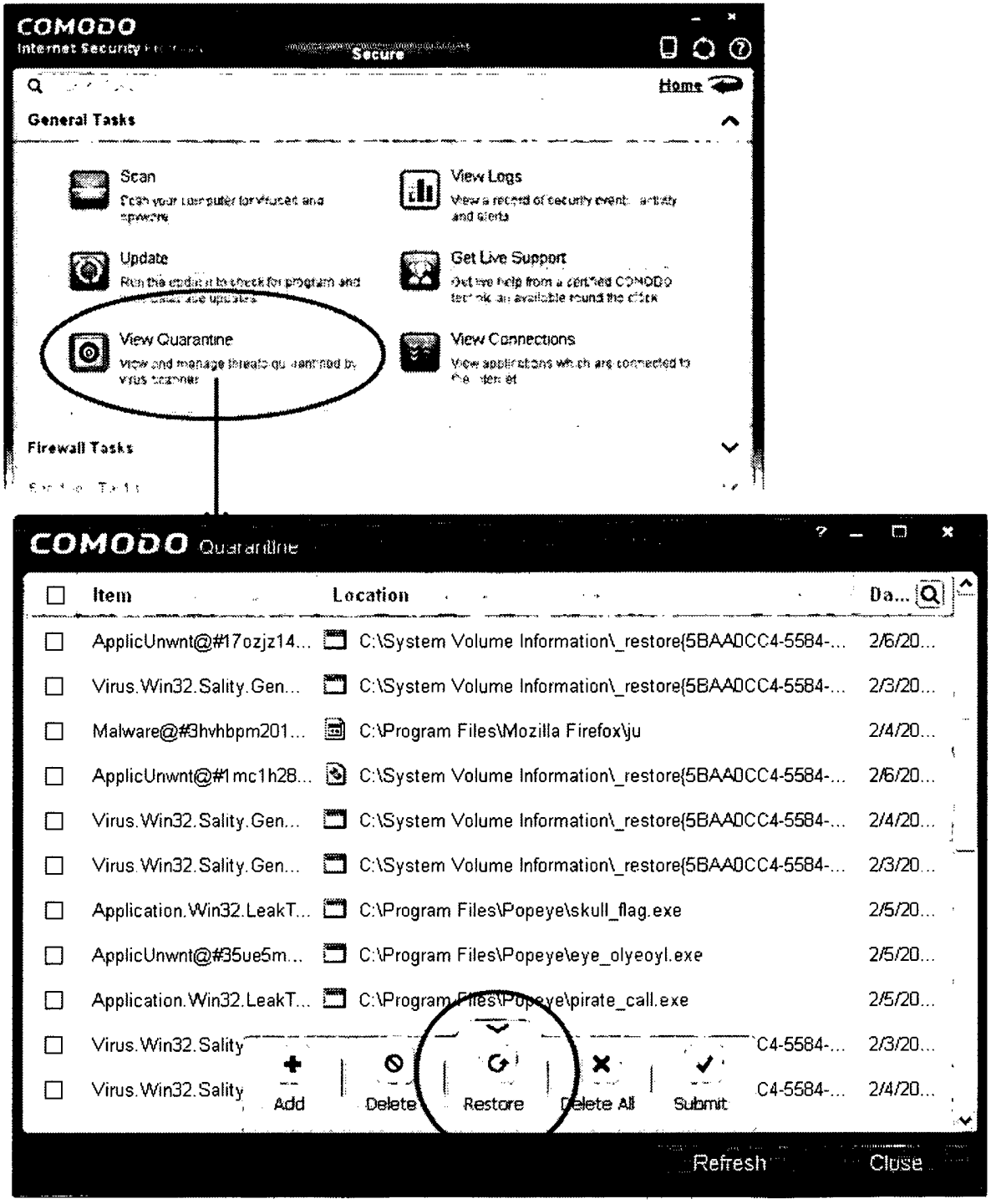
Restore Incorrectly Quarantined Item(s)

If you have incorrectly quarantined item(s) or you feel an item has been incorrectly quarantined by the application (a false positive) then you can restore it/them using the following procedure:

To submit Quarantined items

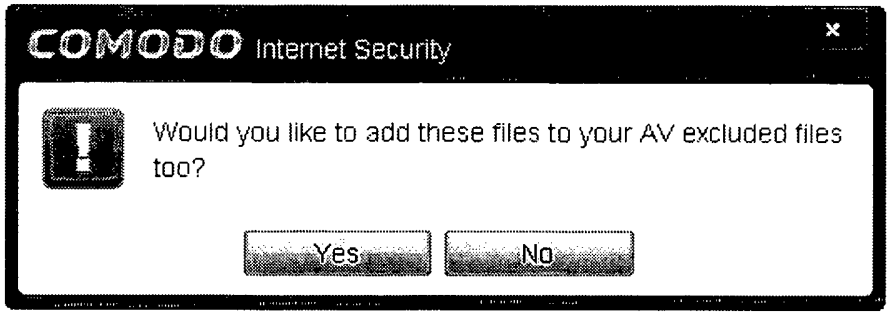
1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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



3. Choose the items to be restored by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Restore'.

An option to add the selected items to AV excluded files will open.



If you select 'Yes', these items will not be included for AV scans. If you select' No', these items will be included for AV scans and quarantined during the next scanning.

All the selected files will be restored to their original locations immediately.

5. Click 'Close' button to exit.

Click here for more details on the Quarantined Items.

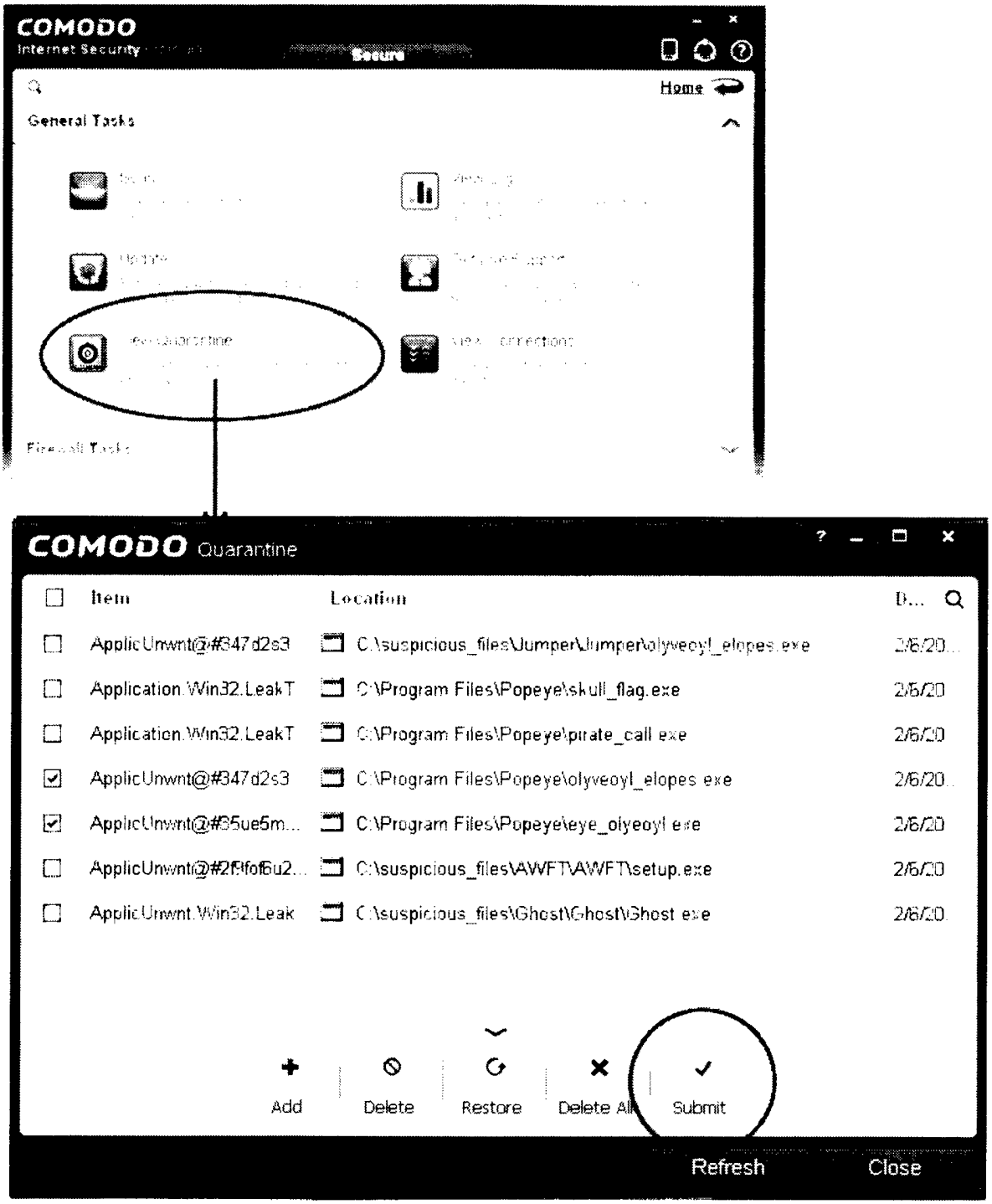
Submit Quarantined Items to Comodo for Analysis

Items which have been quarantined as a result of an On Access, On Demand or Scheduled Scans, can be sent to Comodo for Analysis. After the analysis, if the submitted item is found to be a False Positive, it will be added to Comodo Safe List. Conversely, if it is found to be a malware, it will be added to the anti-malware Black list. This helps Comodo to enhance its virus signature database and helps millions of other CIS users to benefit out of it. **Click here** for more details on Quarantined Items.

To submit Quarantined items

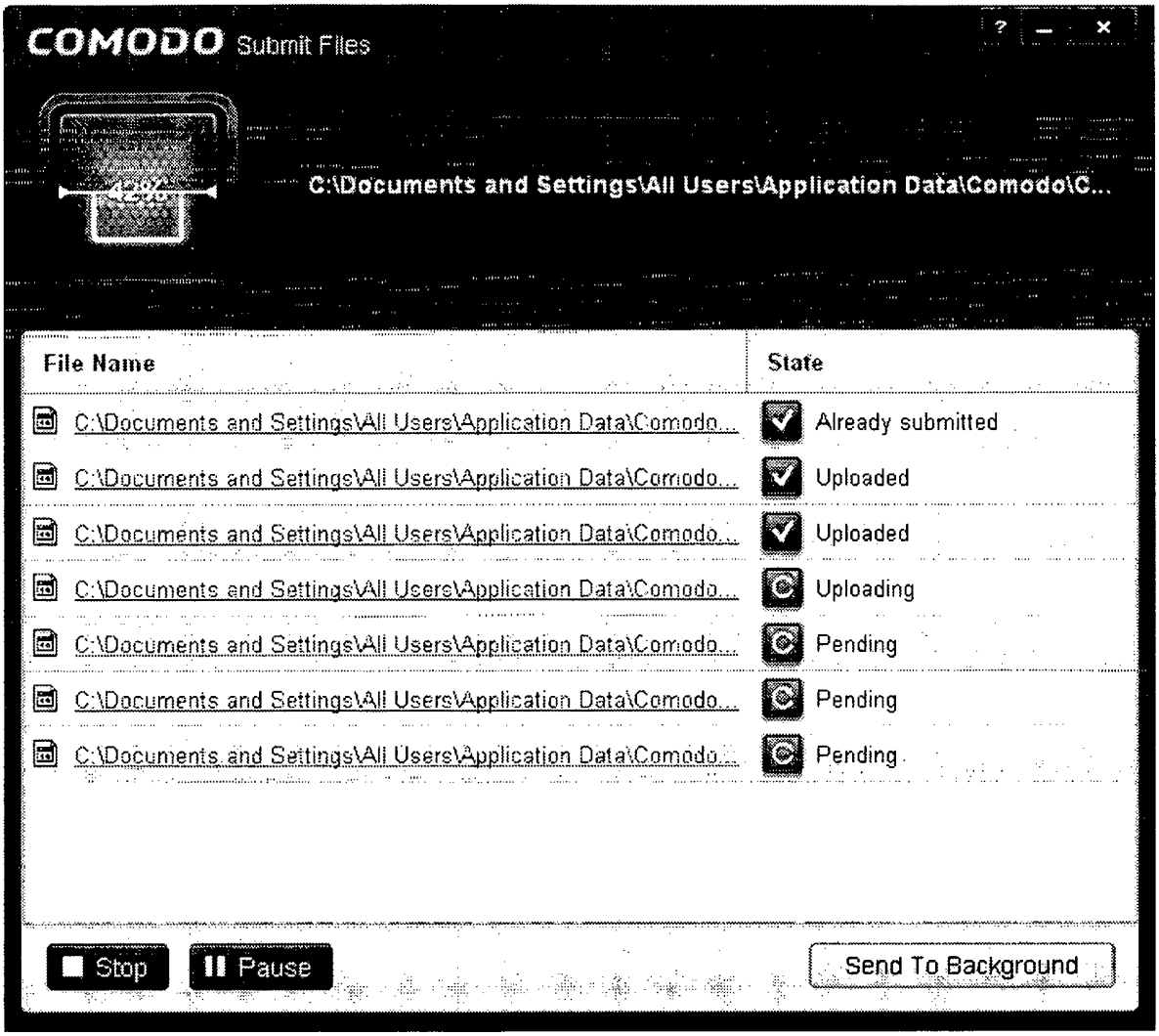
1. Click the 'Tasks' arrow on the home screen to open the main Tasks menu
2. In 'General Tasks', click 'View Quarantine'

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

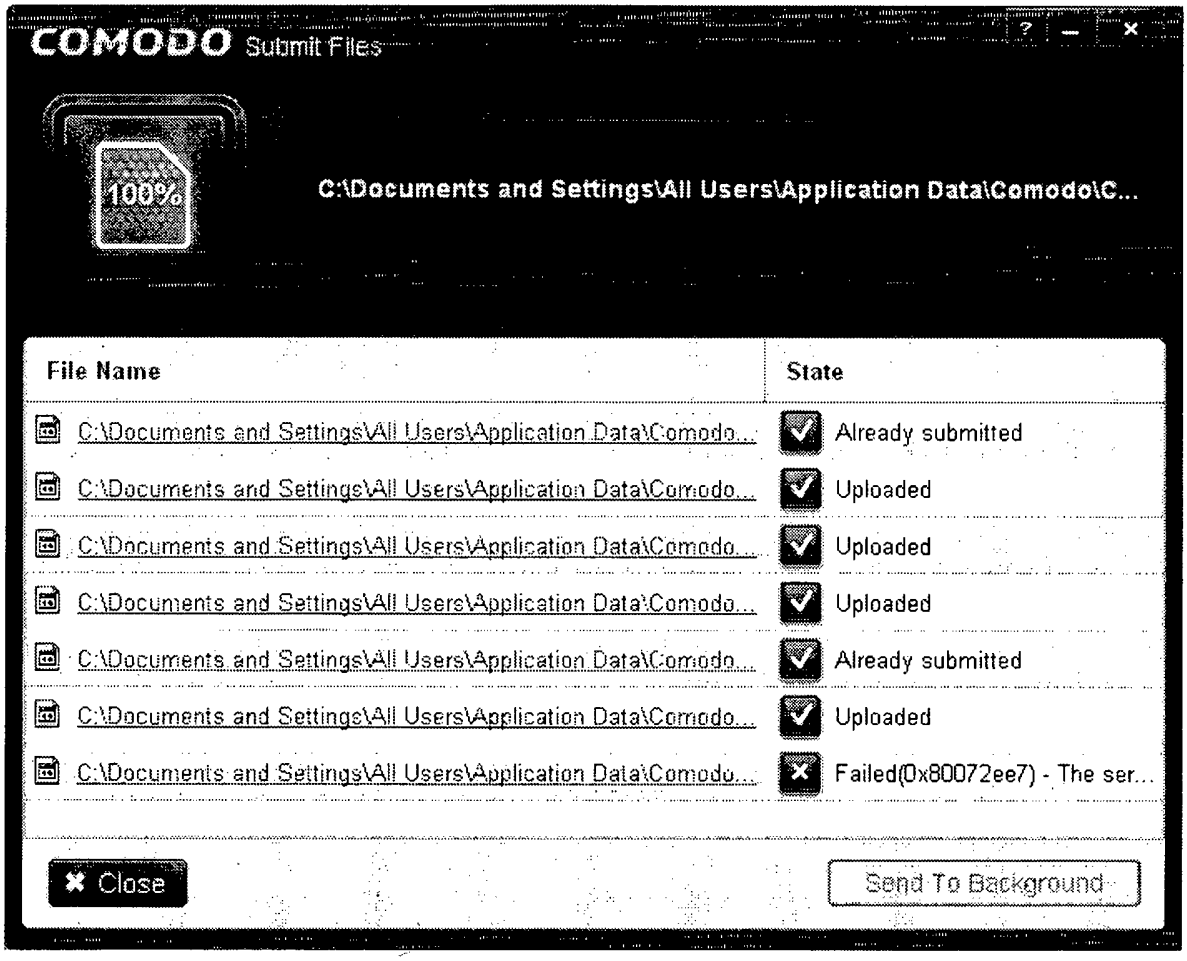


3. Choose the items to be submitted to Comodo for analysis by selecting the checkboxes beside them.
4. Click the handle from the bottom and choose 'Submit'.

The submission progress will be indicated.



On completion, the submission results will be displayed, indicating whether the file is successfully submitted or already submitted by other users and is pending for analysis.



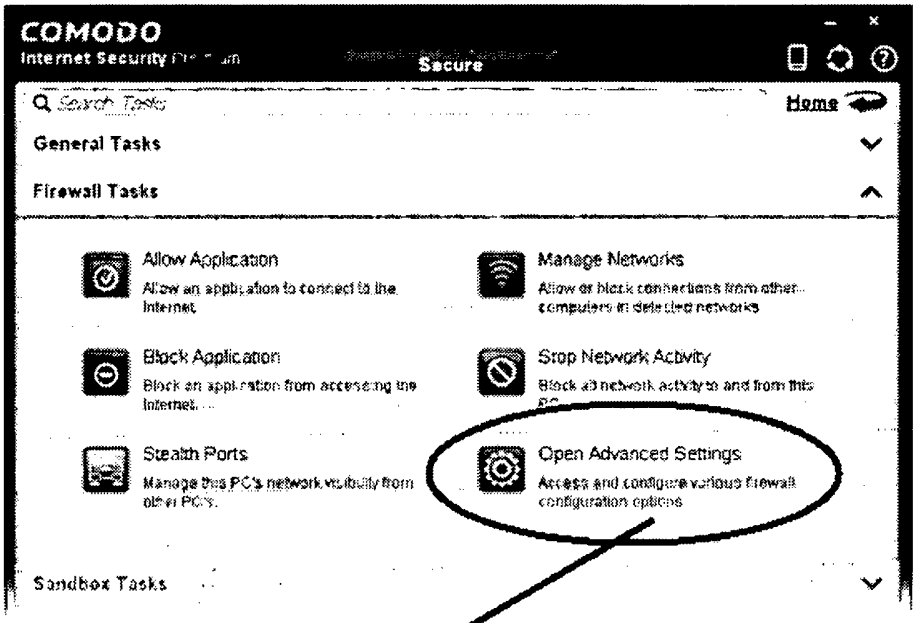
Enable File Sharing Applications like BitTorrent and Emule

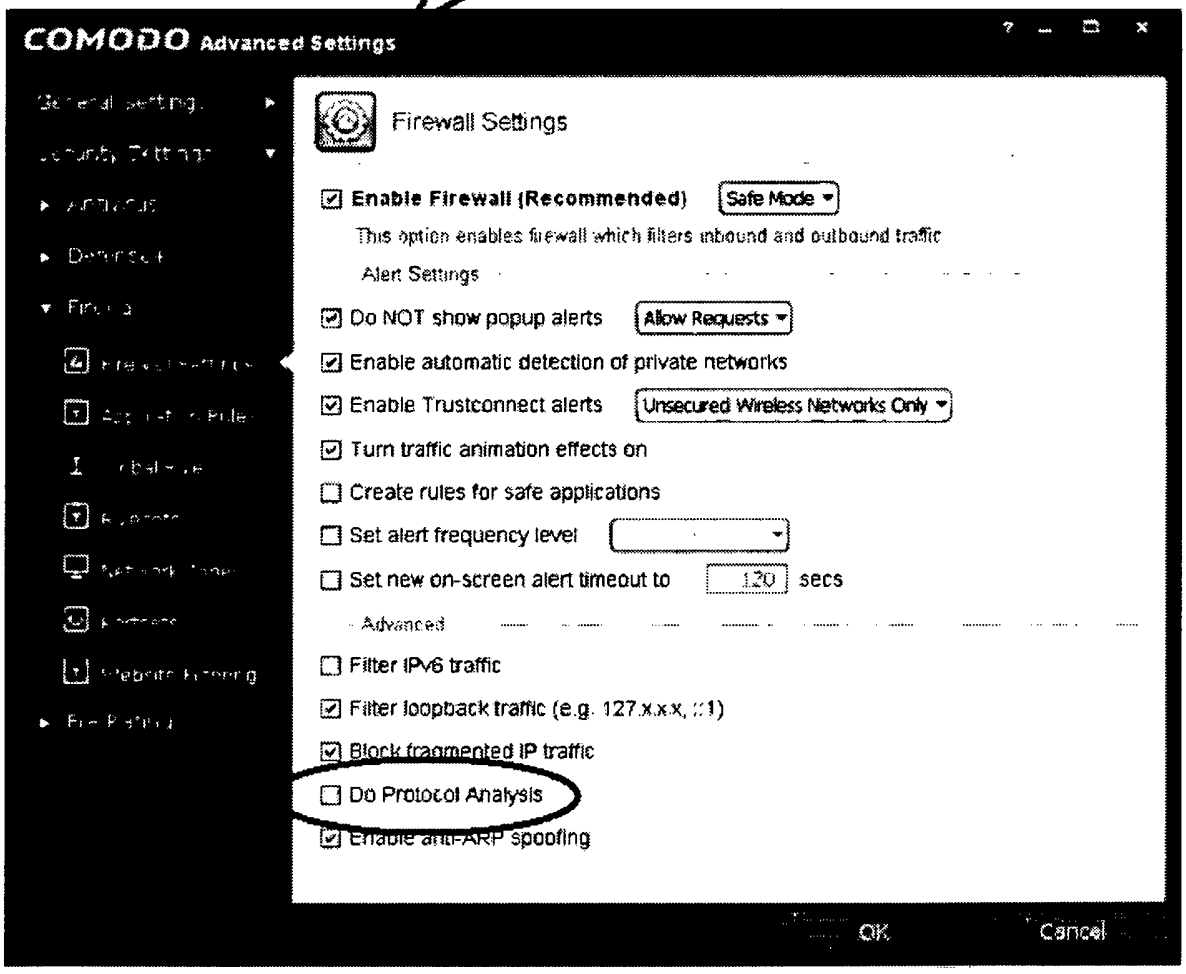
This page explains how to configure Comodo Firewall for file sharing applications like Shareaza/Emule and BitTorrent/UTorrent. To allow these file sharing applications, you must:

- **Disable 'Do Protocol analysis'** ***(disabled, by default)***
- **Create a 'Predefined Firewall Ruleset' for Shareaza/Emule**
- **Create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent**

To Disable 'Do Protocol analysis'

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.

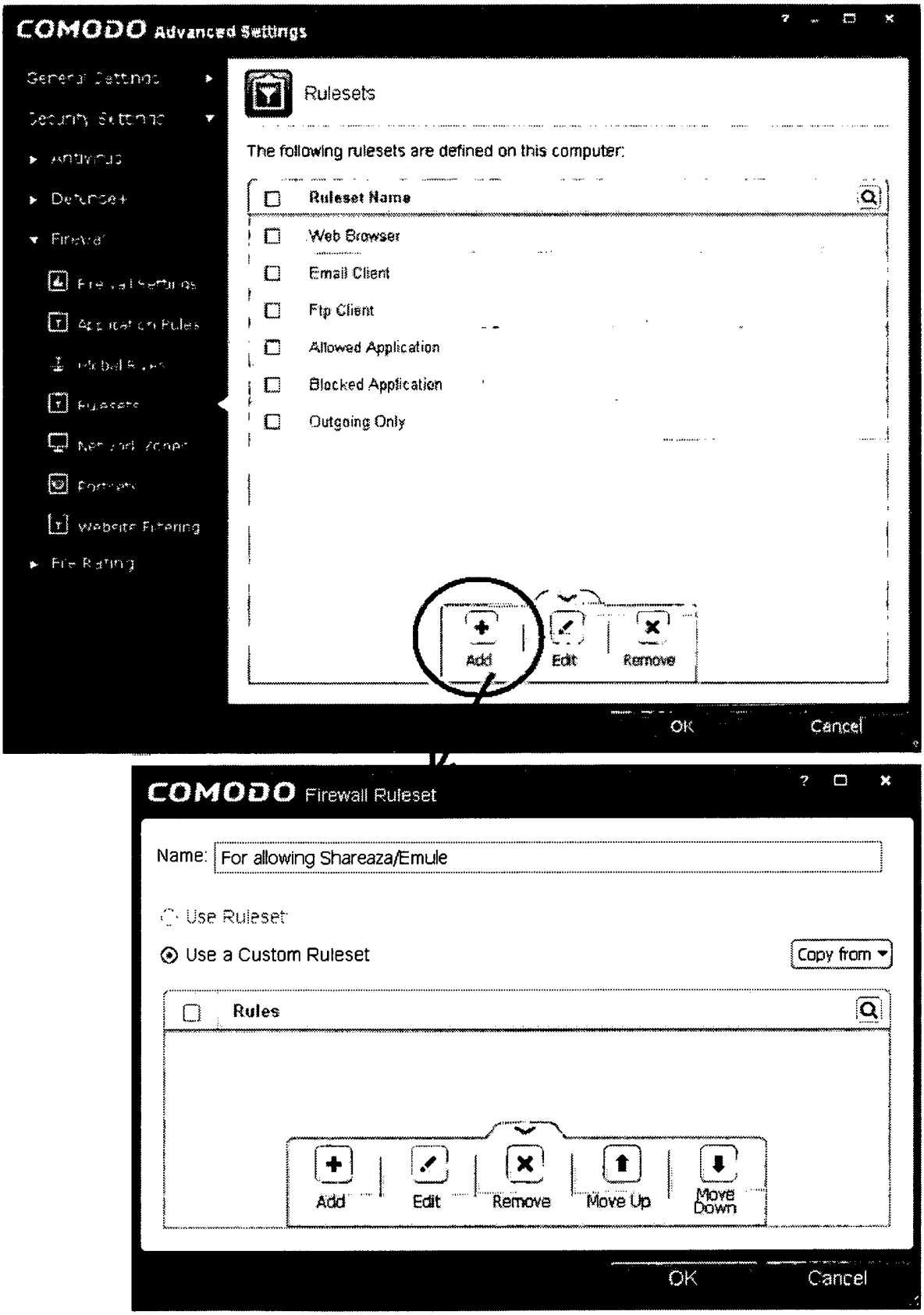




3. Ensure that 'Do Protocol Analysis' checkbox is not selected.

To Create a 'Predefined Firewall Ruleset' for Shareaza/Emule

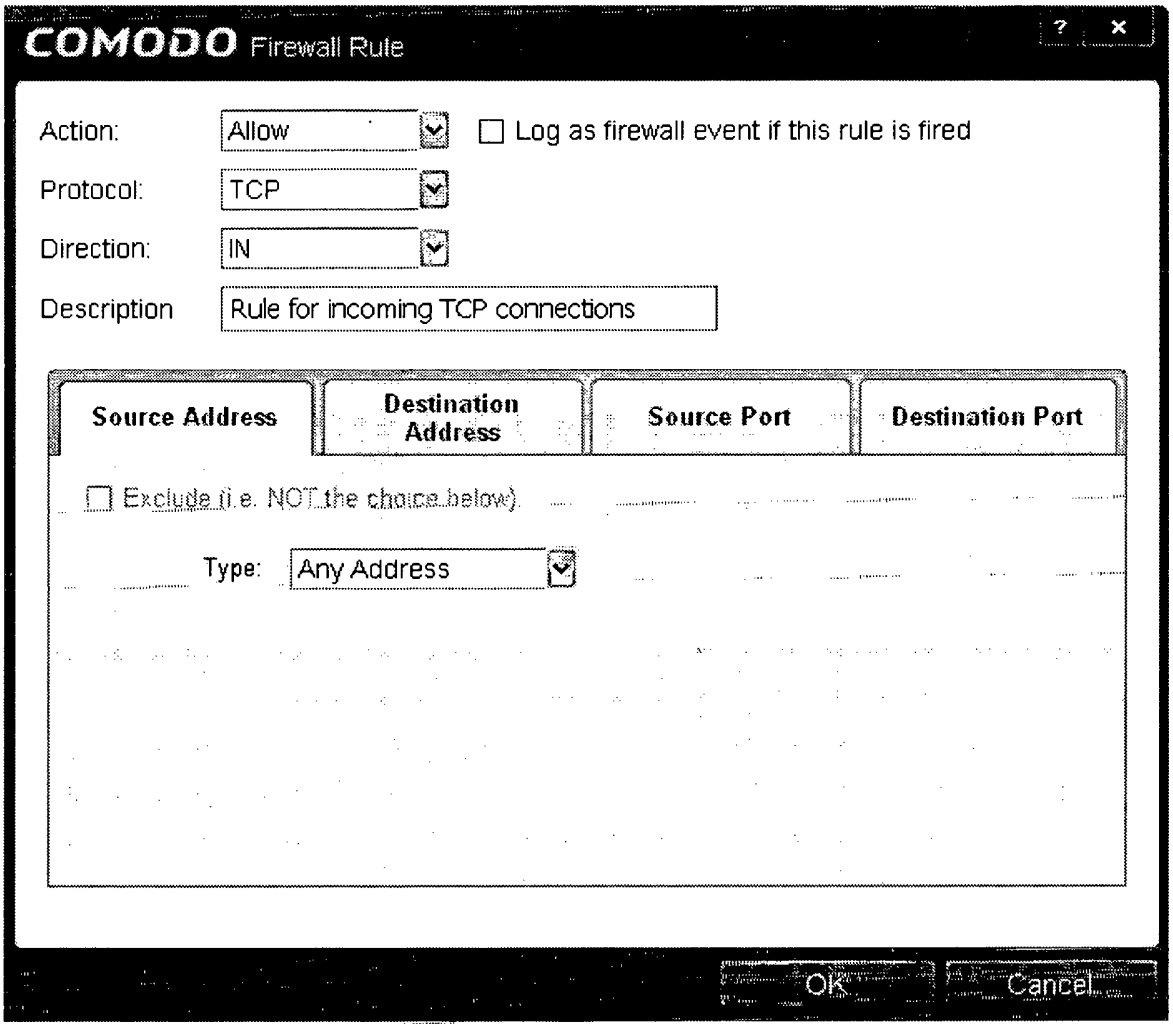
1. Click 'Rulesets' under 'Firewall' from the LHS navigation pane of 'Advanced Settings' interface to open 'Rulesets' panel
2. Click the handle from the bottom of the panel and choose 'Add'



The 'Firewall Ruleset' interface will open for creating a new set of rules.

3. Click the handle from the bottom and choose 'Add'

4. Enter a descriptive name for the new ruleset to be created in the 'Description' text box (for example: For allowing Shareaza/Emule).
5. Now you need to create six rules for the newly created ruleset. To do so, click 'Add'. The 'Firewall Rule' interface will appear. For creating each rule, select the check box and choose the drop-down options under each tab as given below. After creating each rule, click 'OK' for the rule to be added. Click handle in the 'Firewall Ruleset' interface and choose 'Add' to create the next rule.



Rule 1

- Action : Allow
- Protocol : TCP
- Direction : In
- Description : Rule for incoming TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1025 / End Port = 65535)
- Destination port : A Single Port : (Port : Your TCP port of Shareaza/Emule)

Rule 2

- Action : Allow
- Protocol : UDP
- Direction : In
- Description : Rule for incoming UDP connections

- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start Port = 1025 / End Port = 65535)
- Destination port : A Single Port : (Port : Your UDP port of Shareaza/Emule)

Rule 3

- Action : Allow
- Protocol : TCP or UDP
- Direction : Out
- Description : Rule for outgoing TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1025 / end port = 65535)
- Destination port : A port range : (start port = 1025 / end port = 65535)

Rule 4

- Action : Allow
- Protocol : ICMP
- Direction : Out
- Description : Ping the server (edk network)
- Source Address : Any Address
- Destination Address : Any Address
- ICMP Details : Message : ICMP Echo Request

Rule 5

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A port range : (start port = 1025 / end port = 65535)
- Destination port : Type : Single Port; (Port : 80)

Rule 6

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.

The new ruleset will be created and added as a Predefined ruleset. Start Shareaza or Emule. When Comodo raises a pop-up alert, choose 'Treat this application as', select the descriptive name you gave for this rule (e.g. For allowing Shareaza/Emule) from the options and select 'Remember my answer'.

To create a 'Predefined Firewall Ruleset' for BitTorrent/Utorrent'

1. Click 'Rulesets' under 'Firewall' from the LHS navigation pane of 'Advanced Settings' interface to open 'Rulesets' panel
2. Click the handle from the bottom of the panel and choose 'Add'

The 'Firewall Ruleset' interface will open for creating a new set of rules.

3. Click the handle from the bottom and choose 'Add'
4. Enter a descriptive name for the new ruleset to be created in the 'Description' text box (for example: For allowing BitTorrent/Utorrent).
5. Now you need to create six rules for the newly created ruleset. To do so, click 'Add'. The 'Firewall Rule' interface will appear. For creating each rule, select the check box and choose the drop-down options under each tab as given below. After creating each rule, click 'OK' for the rule to be added. Click handle in the 'Firewall Ruleset' interface and choose 'Add' to create the next rule.

Rule 1

- Action : Allow
- Protocol : TCP or UDP
- Direction : In
- Description : Rule for incoming TCP and UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1025 / End port = 65535)
- Destination port : A Single Port (Port: The port of BitTorrent/Utorrent)

Rule 2

- Action : Allow
- Protocol : TCP
- Direction : Out
- Description : Rule for outgoing TCP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1025 / End port = 65535)
- Destination port : A Port Range : (Start port = 1025 / End port = 65535)

Rule 3

- Action : Allow
- Protocol : UDP
- Direction : Out
- Description : Rule for outgoing UDP connections
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Single Port: Port: the port of utorrent
- Destination port : A Port Range : (Start port = 1025 / End port = 65535)

Rule 4

- Action : Ask (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : TCP
- Direction : Out
- Description : Rule for HTTP requests
- Source Address : Any Address
- Destination Address : Any Address
- Source port : A Port Range : (Start port = 1025 / End port = 65535)

- Destination port ; A Single Port (Port = 80)

Rule 5

- Action : Block (Also select the check box 'Log as a firewall event if this rule is fired')
- Protocol : IP
- Direction : In/Out
- Description : Block and Log All Unmatching Requests
- Source Address : Any Address
- Destination Address : Any Address
- IP Details : IP Protocol : Any

6. Click 'OK' in the 'Firewall Ruleset' interface.

The new ruleset will be created and added as a Predefined Firewall ruleset. Start BitTorrent or Utorrent. When Comodo raises a pop-up alert, choose 'Treat this application as', select the descriptive name you gave for this rule (e.g. For allowing BitTorrent/Utorrent) from the options and select 'Remember my answer'.

Block any Downloads of a Specific File Type

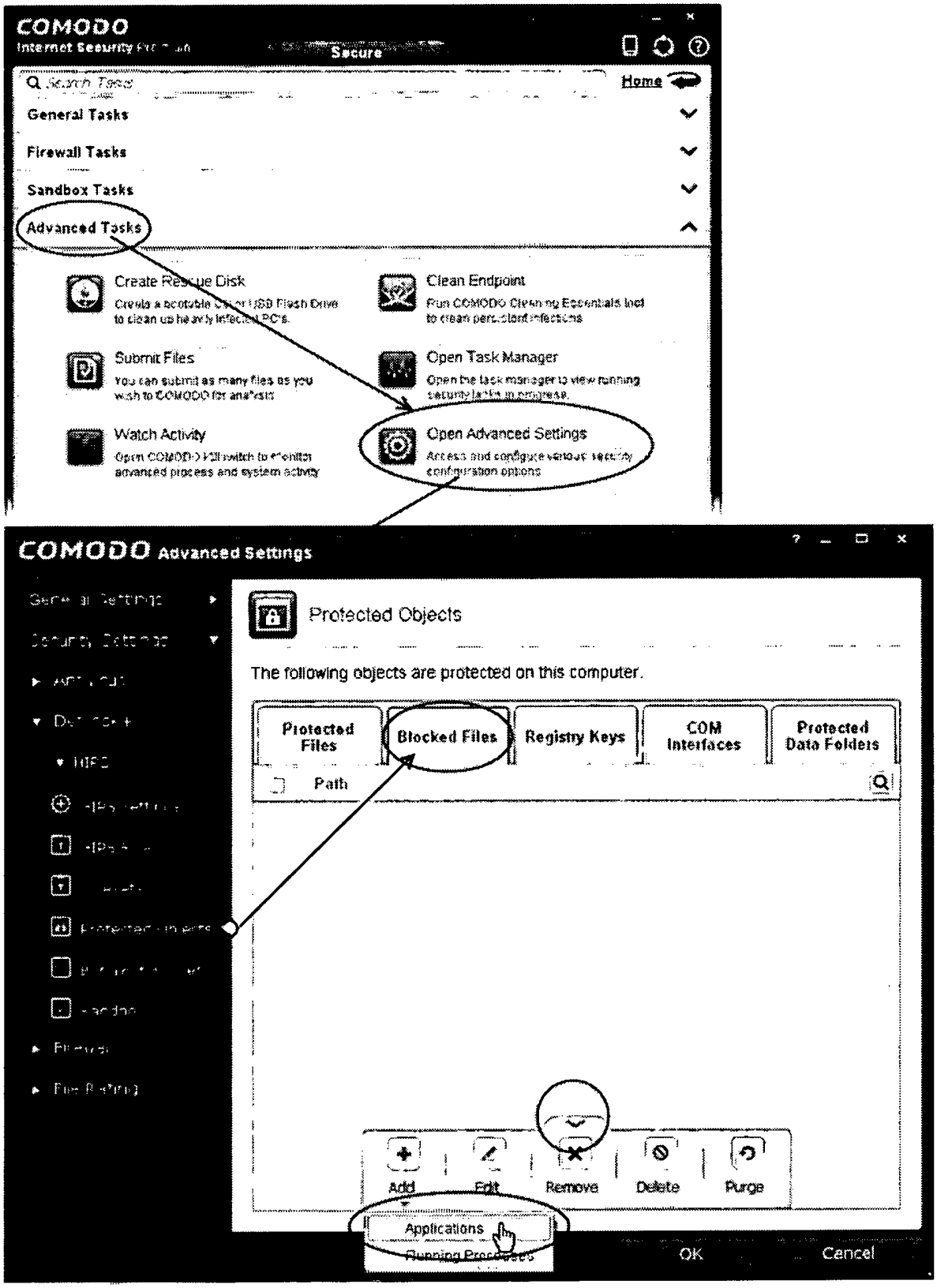
Comodo Internet Security can be configured to block downloads of specific types of file.

Example scenarios:

- Some malicious websites try to push downloads of malware in .exe file format. .exe files are programs which can execute commands on your computer. If the .exe is malicious in intent then these commands could include the installation of key logging programs, initiation of buffer overflow attacks or code to turn your PC into a zombie. For this reason, you may wish to block all downloads of files with a .exe file extension.
- You want to avoid downloading media files like audio files (e.g. files with extensions .wma, .mp3, .wav, .midi), video files (e.g. files with extensions .wmv, .avi, .mpeg, .swf) or image files (e.g. files with extensions .bmp. .jpg, .png) for your disk space restrictions.

To selectively block downloading of specific file type, you need to configure Defense+ component of CIS to block the specific file type from the default download folder of your browser.

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'HIPS' > 'Protected Objects' from the left hand side pane
4. Click 'Blocked Files' tab



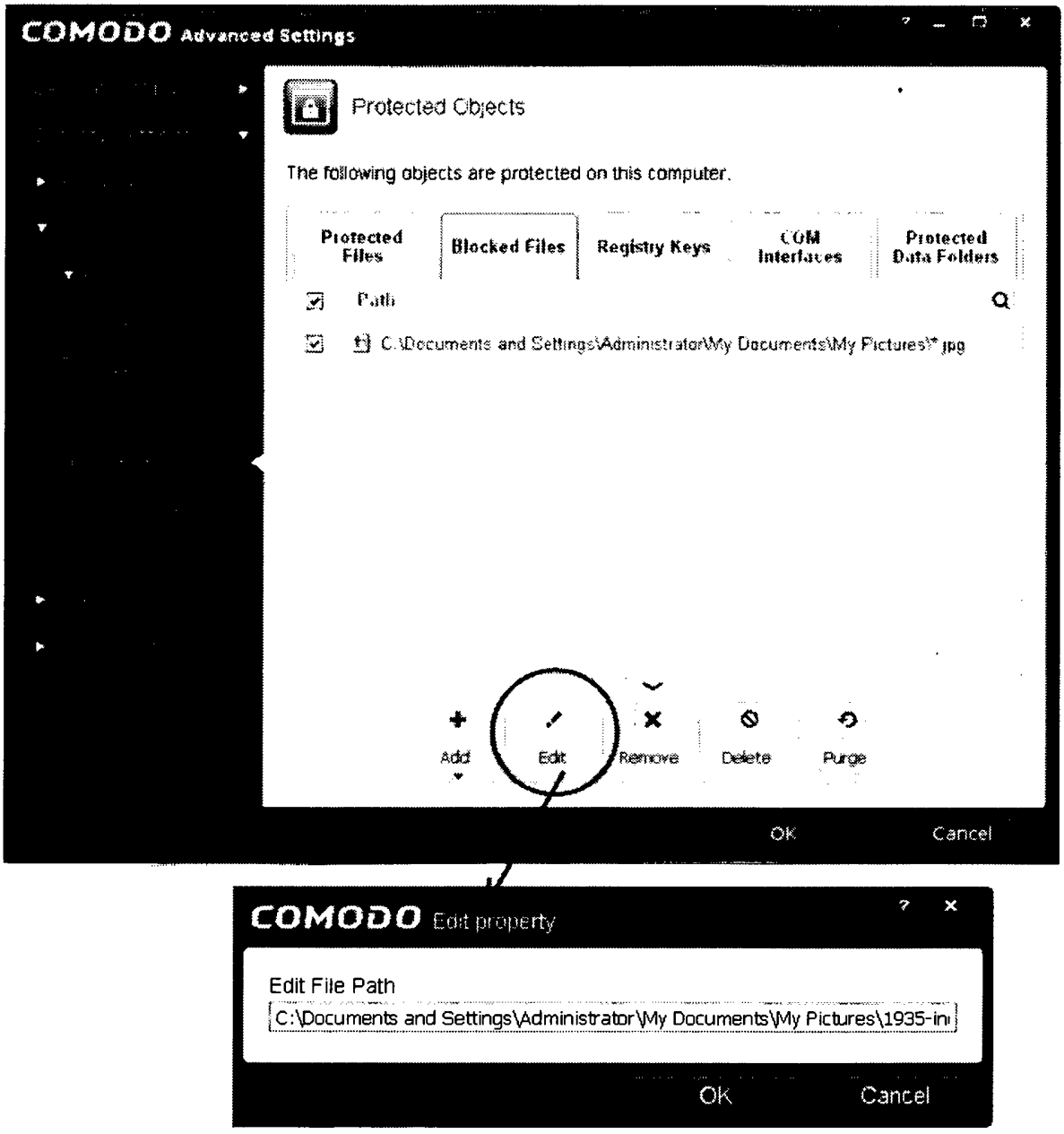
5. Click the handle from the bottom and choose 'Add' > 'Applications'.
6. Browse to the default download folder for that particular file type of your Internet Browser from the Open dialog

- For example, the default download locations for some file types in Internet Explorer are given below:
    - Executable files - C:\Documents and Settings\user name\Local Settings\Temporary Internet Files\

- Document files - C:\Documents and Settings\user name\My Documents\
- Image files - C:\Documents and Settings\user name\My Documents\My Pictures\
- Music files - C:\Documents and Settings\user name\My Documents\My Music\
- Video files - C:\Documents and Settings\user name\My Documents\My Videos\

7. Select file from the folder and click 'Open'

The file will be added to blocked files list.



8. Select the entry from the Blocked Files interface, click the handle from the bottom and choose Edit

The Edit Property dialog will appear.

9. Change the file name at the end of the file path to *.file_extension" (e.g. *.exe, *.jpg)



10. Click OK in the 'Edit Property' dialog
11. Click OK in the Advanced Settings interface to save your settings

The download of the specific file type to the specified folder through the browser will be blocked. If you have more than one browser, repeat the same for the other browsers too.

Note: Blocking files in this way will only block the downloads of the specific file types in the specified folders. If you change the download destination while downloading a file through your web browser, the download will be allowed.

Tip: To unblock the download, Advanced Settings > Defense+ > HIPS > File Protection > Blocked Files, select the file path, click the handle from the bottom and choose 'Remove'.

Disable Behavior Blocker and Auto-Sandboxing on a Per-application Basis

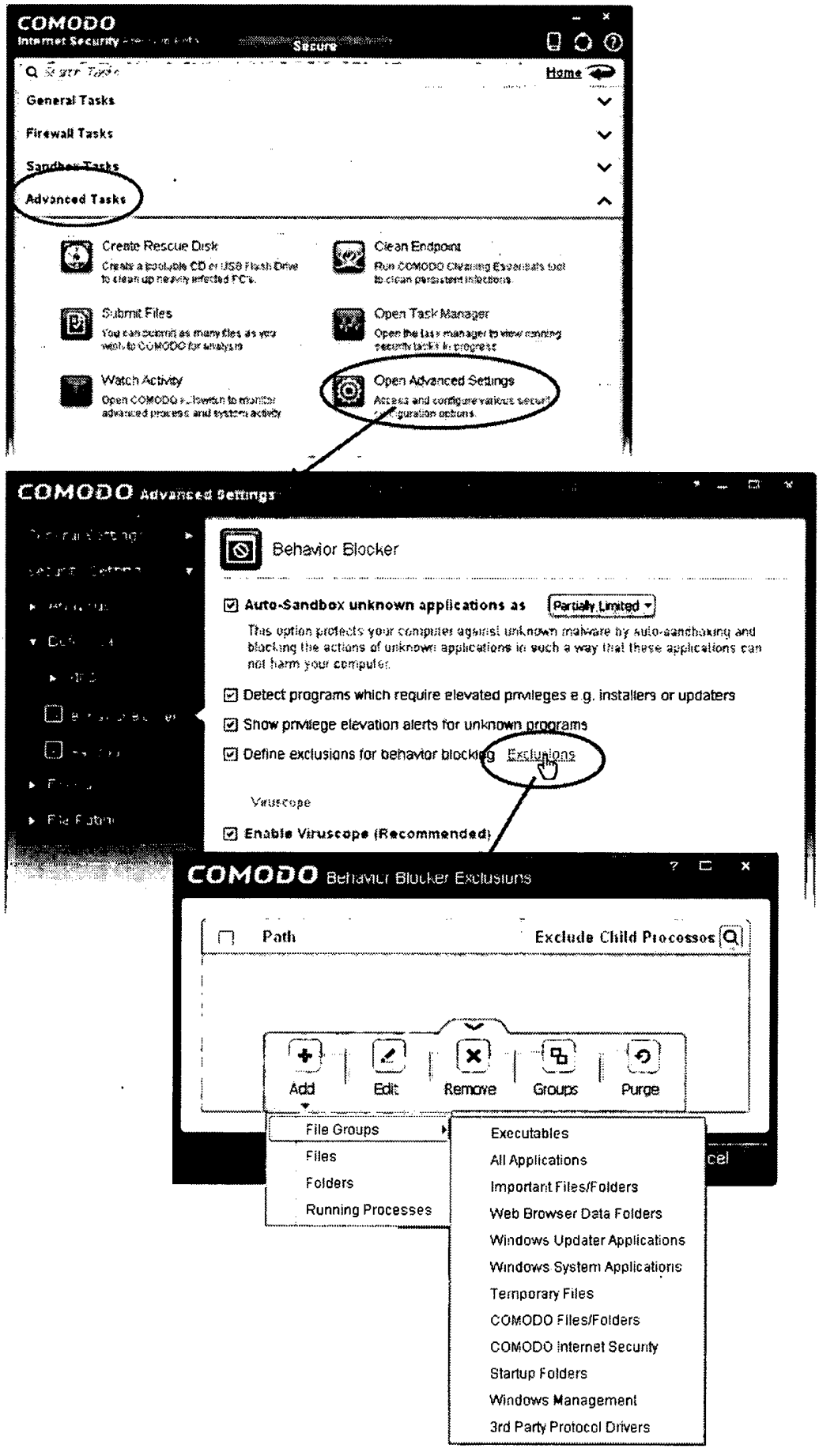
Behavior Blocker will auto-sandbox run unknown executables and queue them for submission to Comodo Cloud scanners for behavior analysis. Users do, however, have the option to exclude specific files or file types from this auto-sandboxing process. This is particularly useful for developers that are creating new applications which, by their nature, are as yet unknown to the Comodo safe list.

To disable the auto-sandboxing selectively

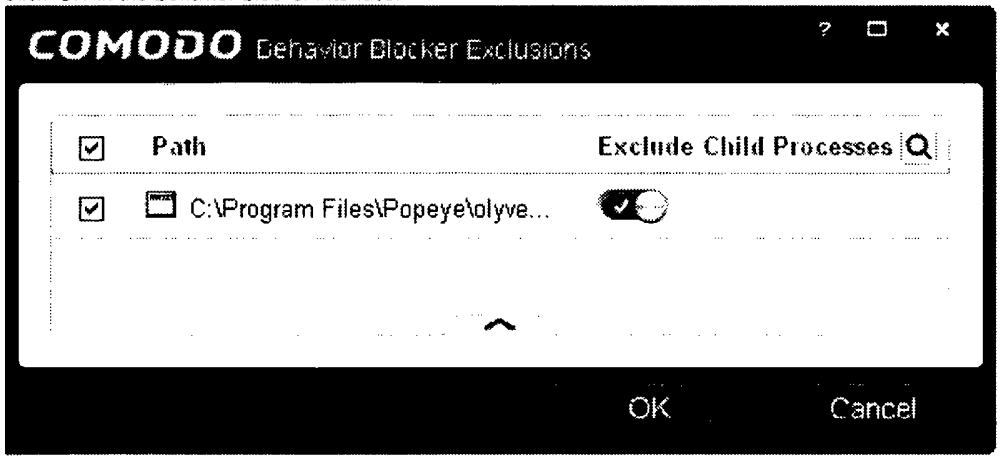
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Security Settings' > 'Defense+' > 'Behavior Blocker' in the left hand side navigation pane of Advanced Settings pane
4. Select the check box 'Define exceptions for behavior blocking and then click on the words 'Exceptions'

The Behavior Blocker Exceptions interface will open.

5. Click the handle from the bottom and choose 'Add' from the options to add the files/executables to be excluded from monitoring by Behavior Blocker and Auto-Sandboxing.
    - You can add items by selecting the required option from the drop-down:
        - **File Groups** - Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. For more details on file groups, refer to the section **File Groups**.
        - **Files** - Opens the 'Open' window and enables you to navigate to the application or file you wish to add.
        - **Folder** - Opens the 'Browse for Folders' window and enables you to navigate to the folder you wish to add.
        - **Running Processes** - As the name suggests, this option allows you to select an application or executable from the processes that are currently running on your PC.


COMODO
Internet Security
Secure
Home
General Tasks
Firewall Tasks
Sandbox Tasks
Advanced Tasks
Create Rescue Disk
Clean Endpoint
Submit Files
Open Task Manager
Watch Activity
Open Advanced Settings
COMODO Advanced Settings
Behavior Blocker
Auto-Sandbox unknown applications as
Partially Limited
This option protects your computer against unknown malware by auto-sandboxing and blocking the actions of unknown applications in such a way that these applications can not harm your computer.
Detect programs which require elevated privileges e.g. installers or updaters
Show privilege elevation alerts for unknown programs
Define exclusions for behavior blocking
Exclusions
Viruscope
Enable Viruscope (Recommended)
COMODO Behavior Blocker Exclusions
Path
Exclude Child Processes
Add
Edit
Remove
Groups
Purge
File Groups
Files
Folders
Running Processes
Executables
All Applications
Important Files/Folders
Web Browser Data Folders
Windows Updater Applications
Windows System Applications
Temporary Files
COMODO Files/Folders
COMODO Internet Security
Startup Folders
Windows Management
3rd Party Protocol Drivers

6. Click 'OK' in the Behavior Blocker interface.



7. Select whether the child processes of the application also needs to be excluded using the 'Exclude Child Processes' toggle switch.
8. Click OK in the Advanced Settings panel for your settings to take effect.

The selected application will not be auto-sandboxed on its execution.

Alternatively...

1. Add the files to the list of **Trusted Files**
2. Digitally sign your files with a code signing certificate from a trusted CA then manually add your organization to the **Trusted Software Vendors** list
3. Disable Behavior Blocker by de-selecting the 'Enable Auto-Sandbox unknown applications as' check box in the Behavior Blocker settings panel. *Not recommended.*

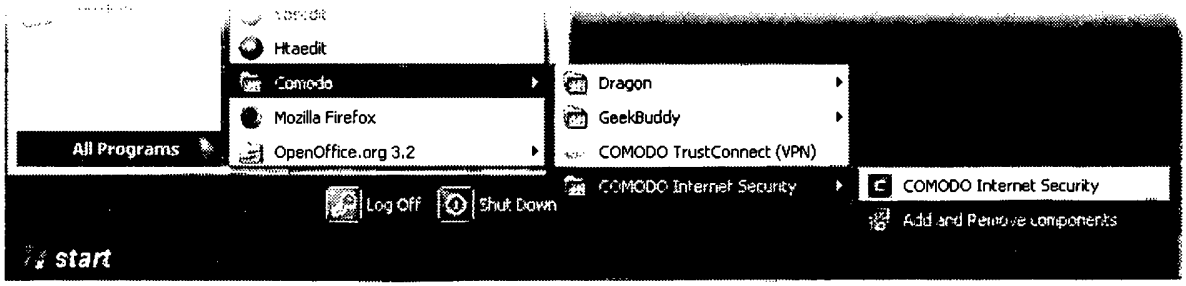
For more details on Auto-Sandboxing process, refer to the section **Unknown Files: The Auto-Sandboxing and Scanning Processes**.

Switch Between Complete CIS Suite and Individual Components (just AV or FW)

Comodo Internet Security provides the flexibility of installation as a complete security suite or as individual components. You can choose the installation type **during the installation** itself. Even after the installation, you can switch the installation type without the requirement of uninstallation of the software, retaining your configuration settings. You might have installed the CIS as complete suite initially but may want to retain the AV part or FW part and uninstall the other or vice versa. The inbuilt uninstaller of CIS enables to switch your installation type at any point of time.

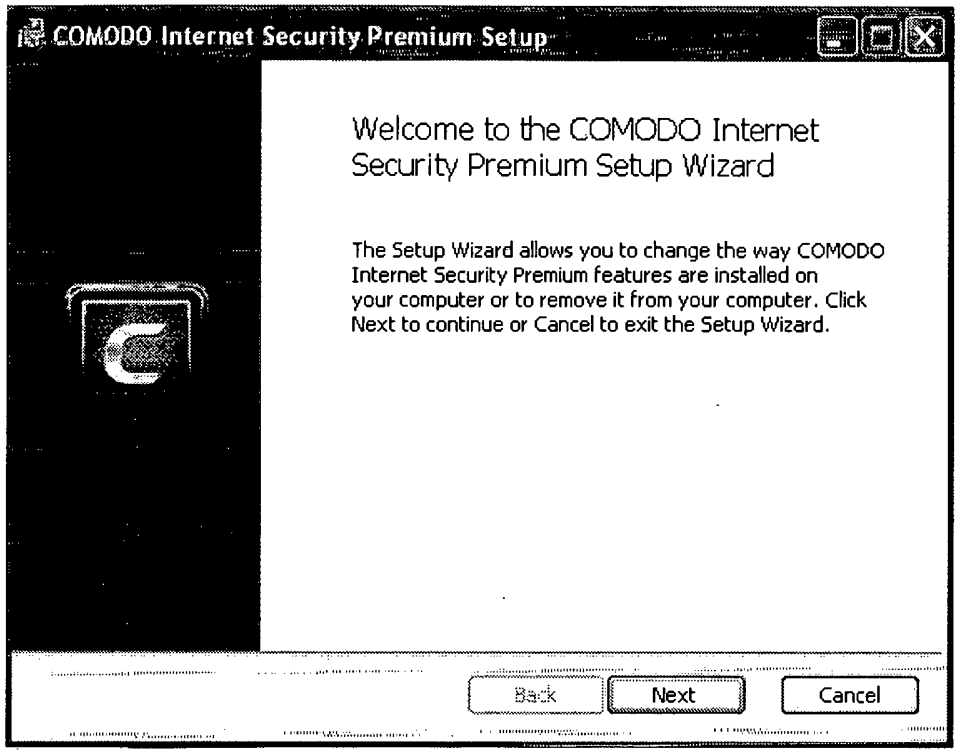
To switch the installation type

1. Click Start > All Programs > COMODO > COMODO Internet Security > Add and Remove Components

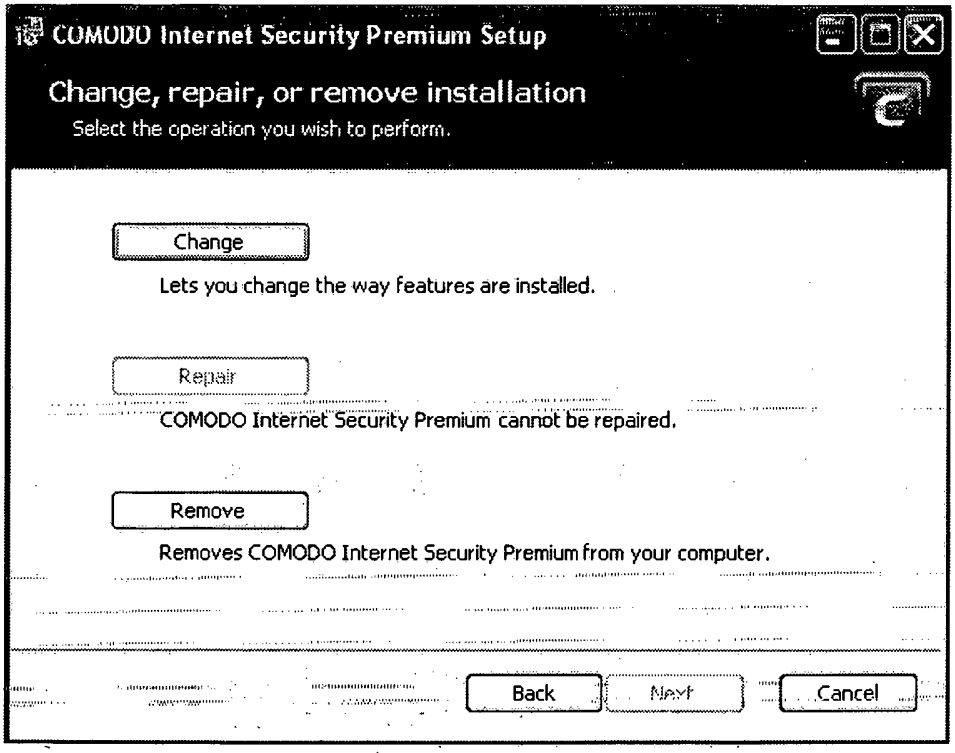


or click Start > Control Panel > Add/Remove Programs > Comodo Internet Security > Change.

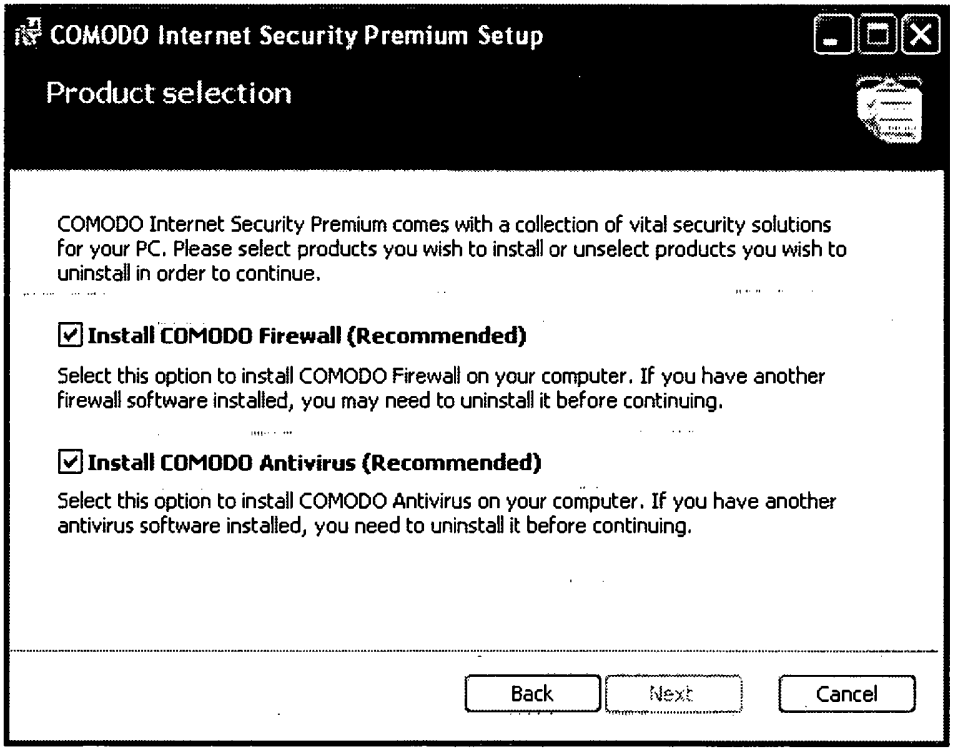
The Configuration Wizard will start.



2. Click 'Next'. The configuration selection screen will appear.



3. Select 'Change' button to change the installed features and click 'Next.' The Product Selection screen will appear.

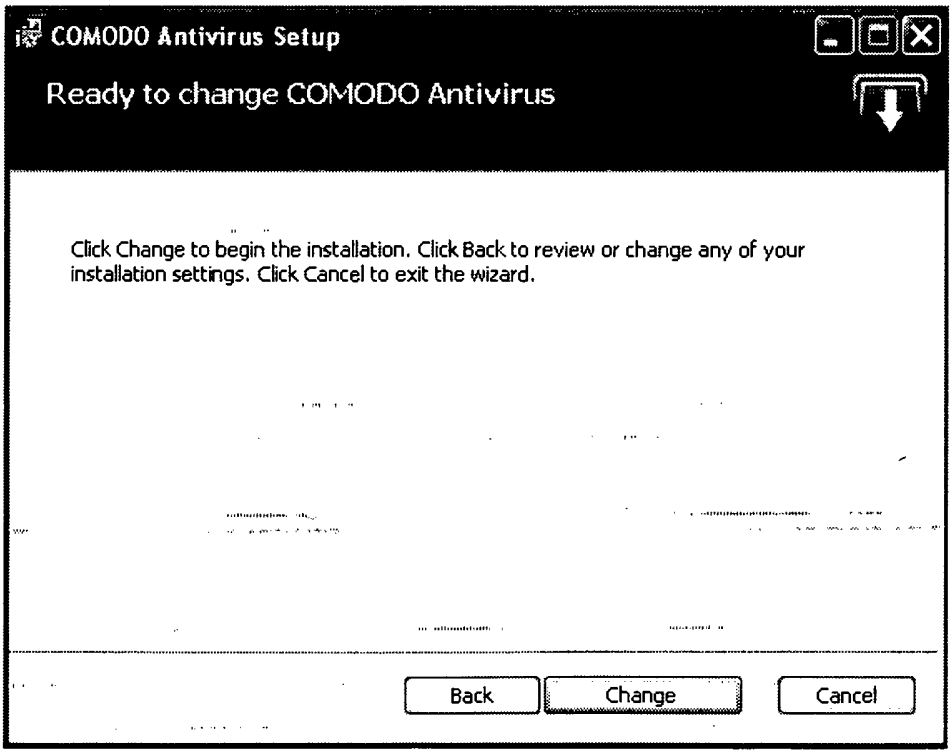


Select the installation type.

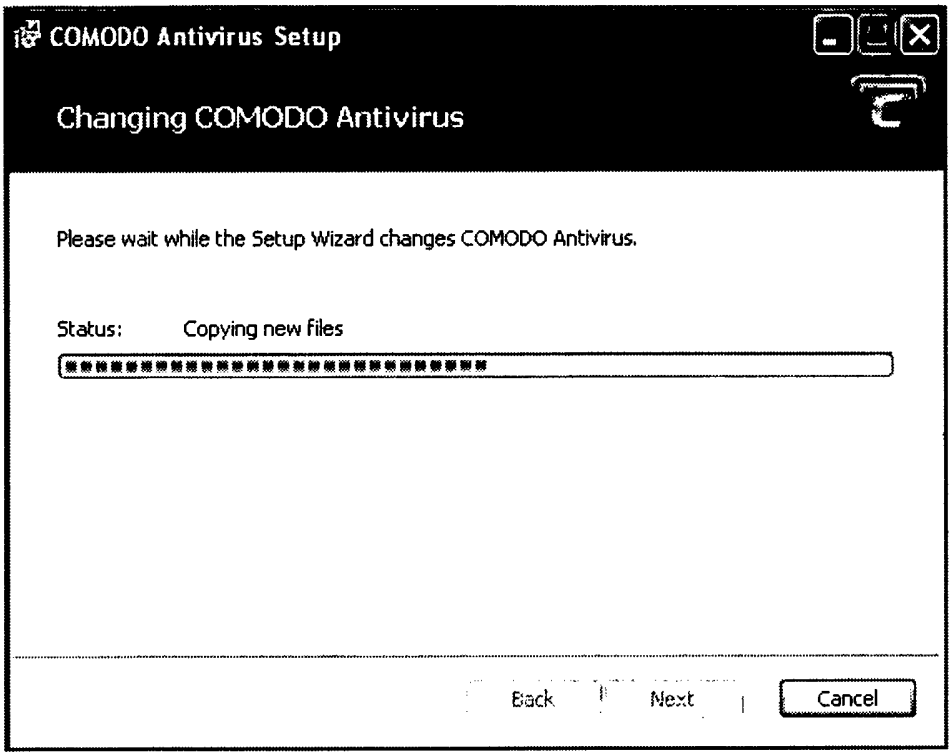
- If you want the complete installation, select both Install COMODO Antivirus and Install COMODO Firewall.
- If you want only the Antivirus part and not the Firewall part, select only the Install COMODO Antivirus and uncheck Install COMODO Firewall.
- If you want only the Firewall part and not the Antivirus part, select only the Install COMODO Firewall and uncheck Install COMODO Antivirus.

Click here for more details on the installation of individual components.

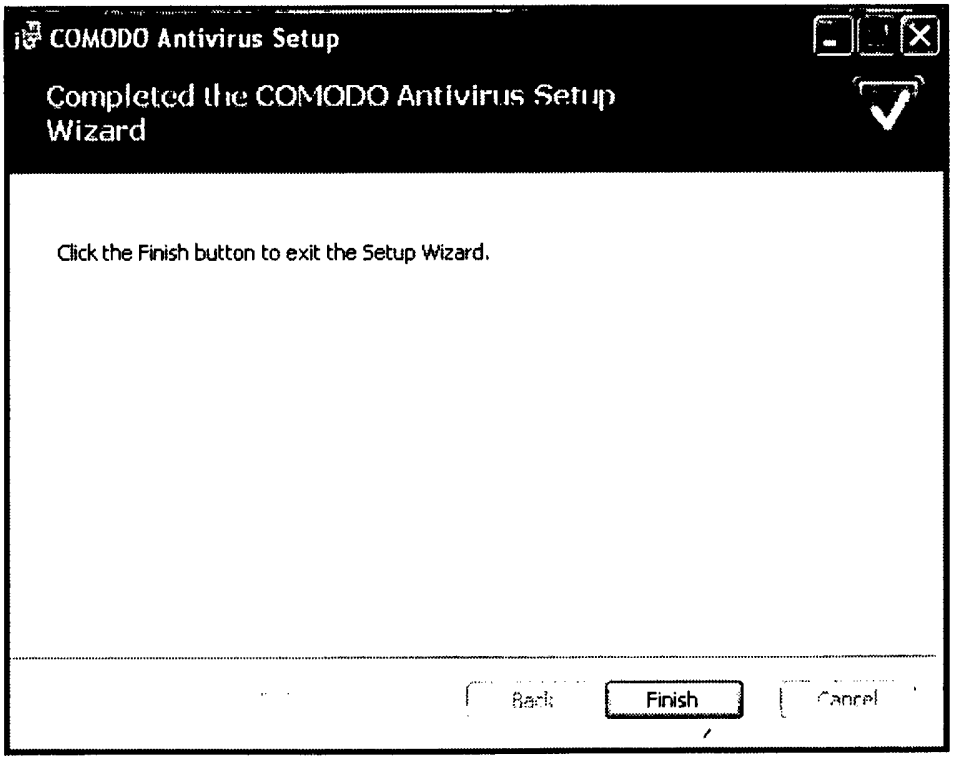
- Click 'Next'. Wait till the CIS is configured and is ready for the change.



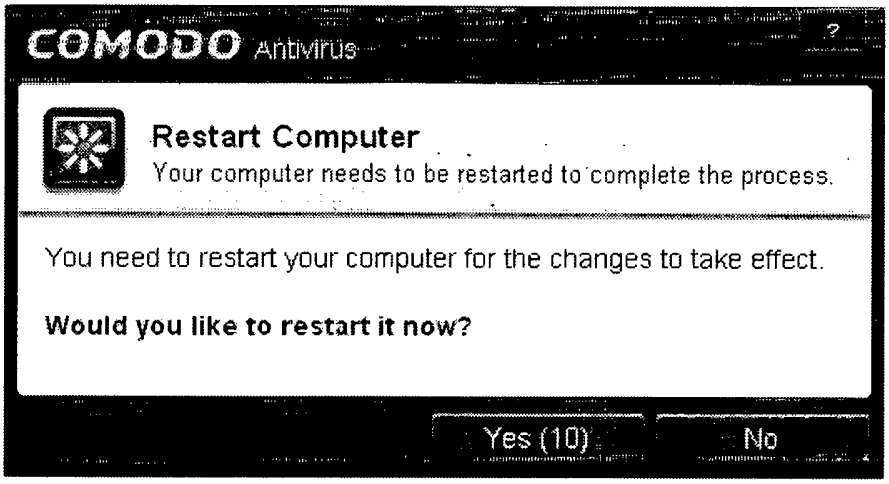
4. Click 'Change' in the next screen. The change progress will be indicated...



... and on completion, Click the Finish button to exit the wizard.



In order for the configuration change to take effect, your computer needs to be restarted. A 'Restart Computer' dialog with a countdown timer will be displayed.



- If you want to restart the system at a later time, click 'No'.
- If you want to restart the system immediately, please save any unsaved data and click 'Yes' or leave the dialog for the system to restart at the end of countdown timer.

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

Switch Off Automatic Antivirus and Software Updates

By default, Comodo Internet Security will automatically check for software and Antivirus database updates. However, some users like to have control over what gets downloaded and when it gets downloaded. For example, network administrators may not wish to automatically download because it will take up to much bandwidth during the day. Similarly, users that have particularly heavy traffic loads may not want automatic updates because they conflict with their other download/upload activity.

CIS provides full control over virus and software updates. Click the appropriate link below to find out more:

- **Switch off automatic software and virus signature database updates entirely**
- **Switch off automatic software and virus signature database selectively**
- **Switch off automatic virus signature database updates prior to Antivirus Scans**

To switch off automatic updates entirely:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane
4. Deselect the check boxes 'Check for program updates every xxx day(s)' and 'Check for database updates every xxx hour(s)'

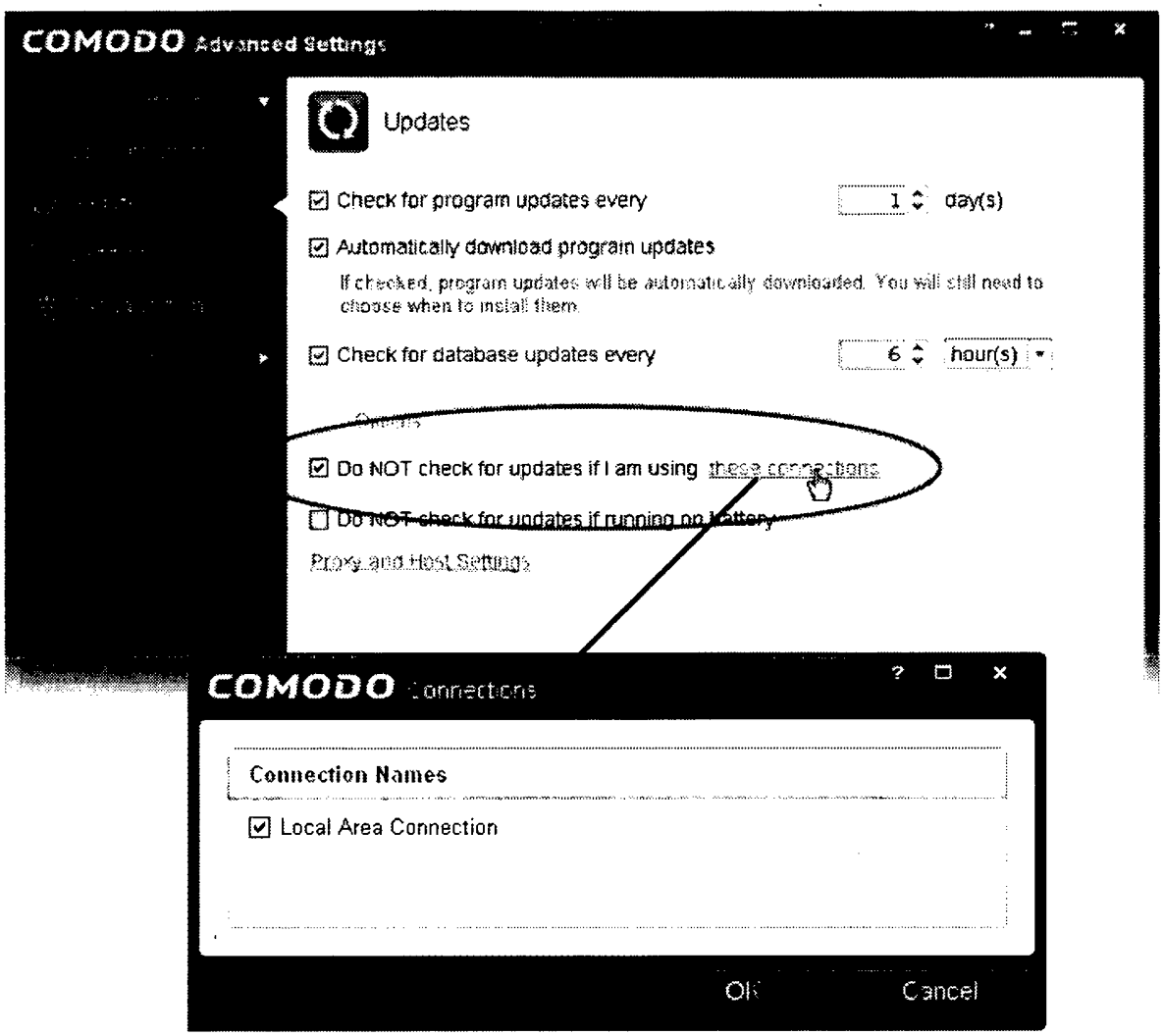


5. Click 'OK' in the Advanced Settings panel.

To switch off automatic updates selectively:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface

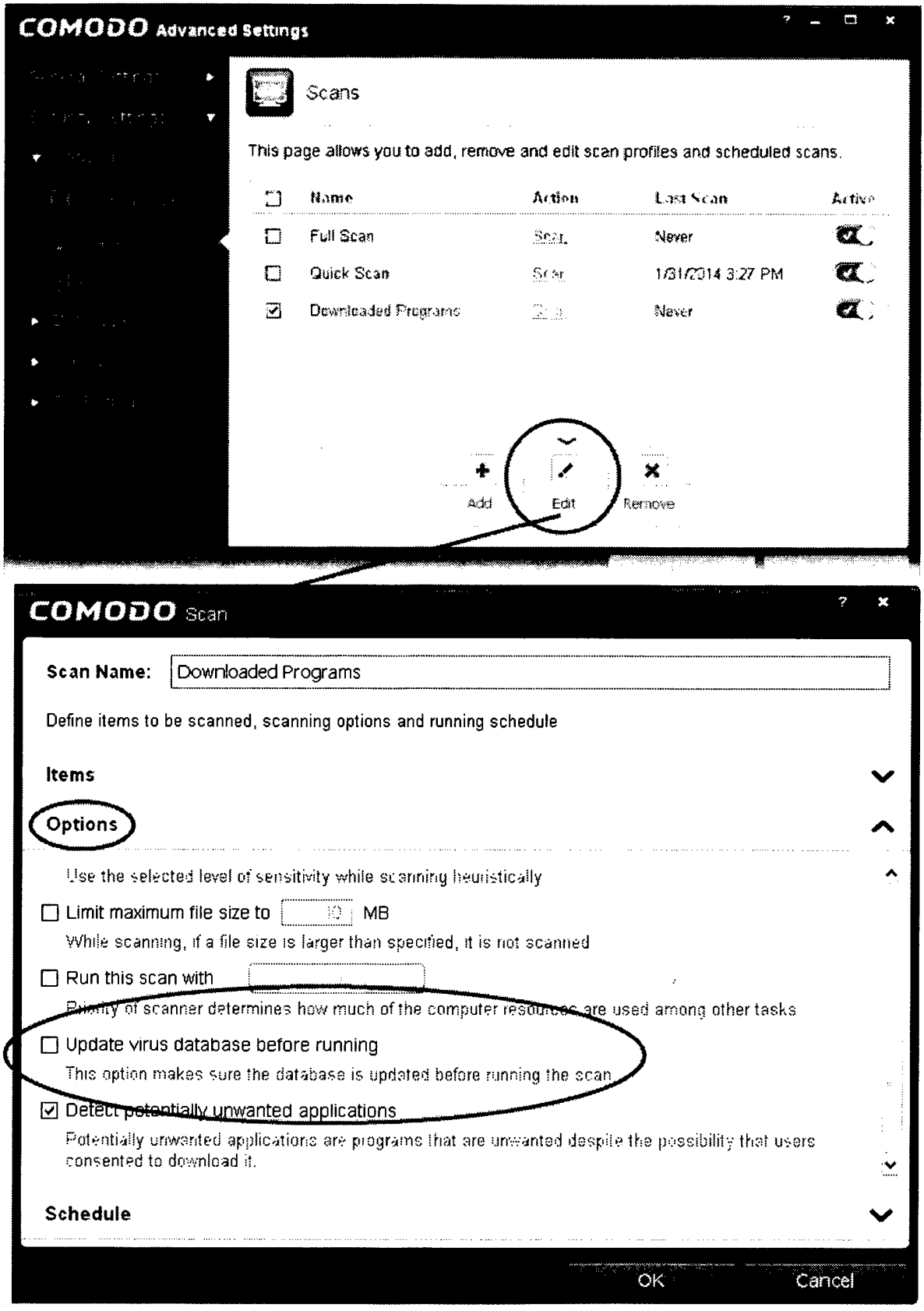
3. Click 'Updates' under 'General Settings' from the left hand side navigation pane



- If you want to suppress automatic updates when you are connected to Internet through certain networks
  - Select the 'Do NOT check updates if am using these connections' check-box
  - Then click the 'these connections'. The 'Connections' dialog will appear with the list of connections you use.
  - Select the connection through which you do not want CIS to check for updates and click OK.
- If you want to suppress automatic updates when your computer is running on battery
  - Select the 'Do NOT check for updates if running on battery' checkbox

To switch off automatic virus signature database updates prior to AV Scans:

1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open Advanced Settings panel by clicking Advanced Tasks > Advanced Settings from the Tasks interface
3. Click 'Security Settings' > Antivirus' > 'Scans'. A list defined scan profiles will be displayed.
4. Select the scan profile for which you do want the automatic virus database updates prior to the scan



5. Click the handle from the bottom and select 'Edit'
6. Click 'Options' to open the Options pane and deselect 'Update virus database before running' checkbox.

7. Click 'OK' on the 'Scan' interface.
8. Click 'OK' in the 'Advanced Settings' interface for your changes to take effect.

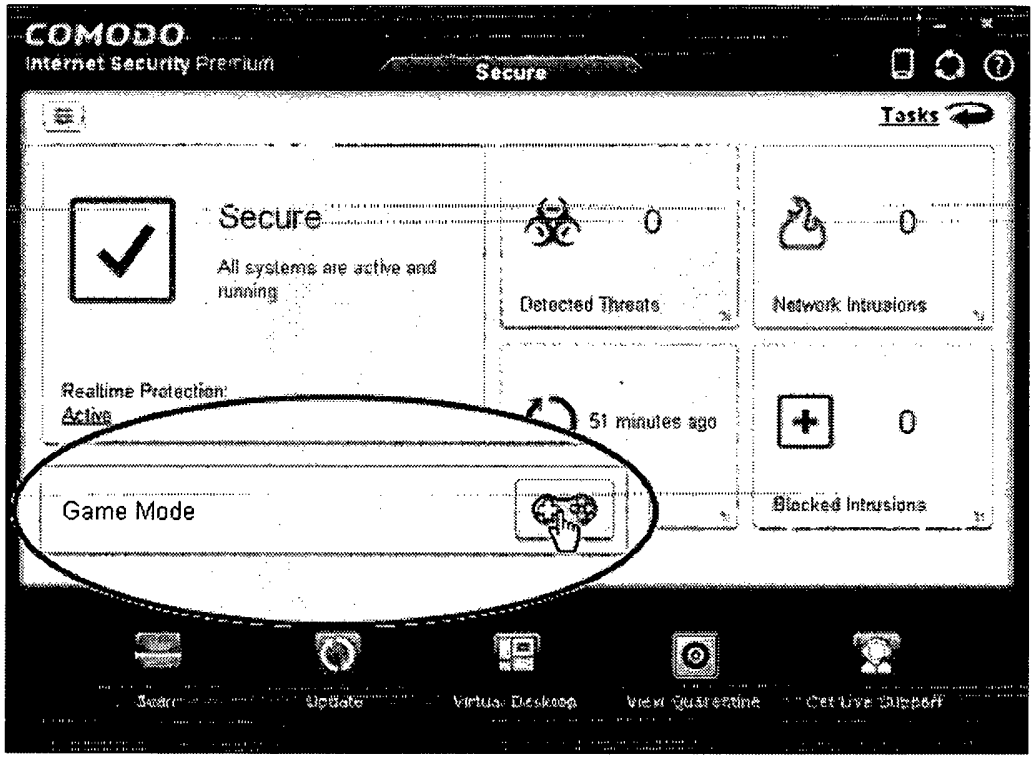
Suppress CIS Alerts Temporarily while Playing Games

Because of continuous monitoring of all your system activities in granular level for implementing Default-Deny Protection, Comodo Internet Security generates pop-up alerts whenever it identifies any event appearing to be a malicious activity or execution of programs that require privileges like Internet access and file access rights. Each alert provides information and options that enable you to make an informed decision on whether you want to allow or block a request or activity. Alerts also to allow you to instruct Comodo Internet Security on how it should behave in future when it encounters activities of the same type.

But at times when you are involved in activities like playing computer games, where you do not want to be interfered with such alerts, you can temporarily stop them from being displayed. require undisturbed environment. During this time, the operations that can interfere with users' gaming experience are either suppressed or postponed.

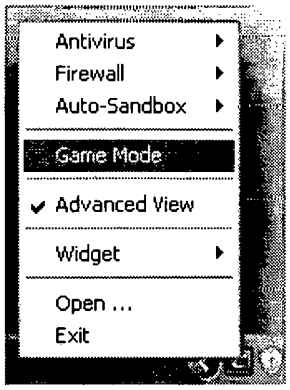
To temporarily stop pop-up alerts

- Click 'Game Mode' button from CIS Home screen



or

- Right click on the CIS System Tray icon and select 'Game Mode' from the options.

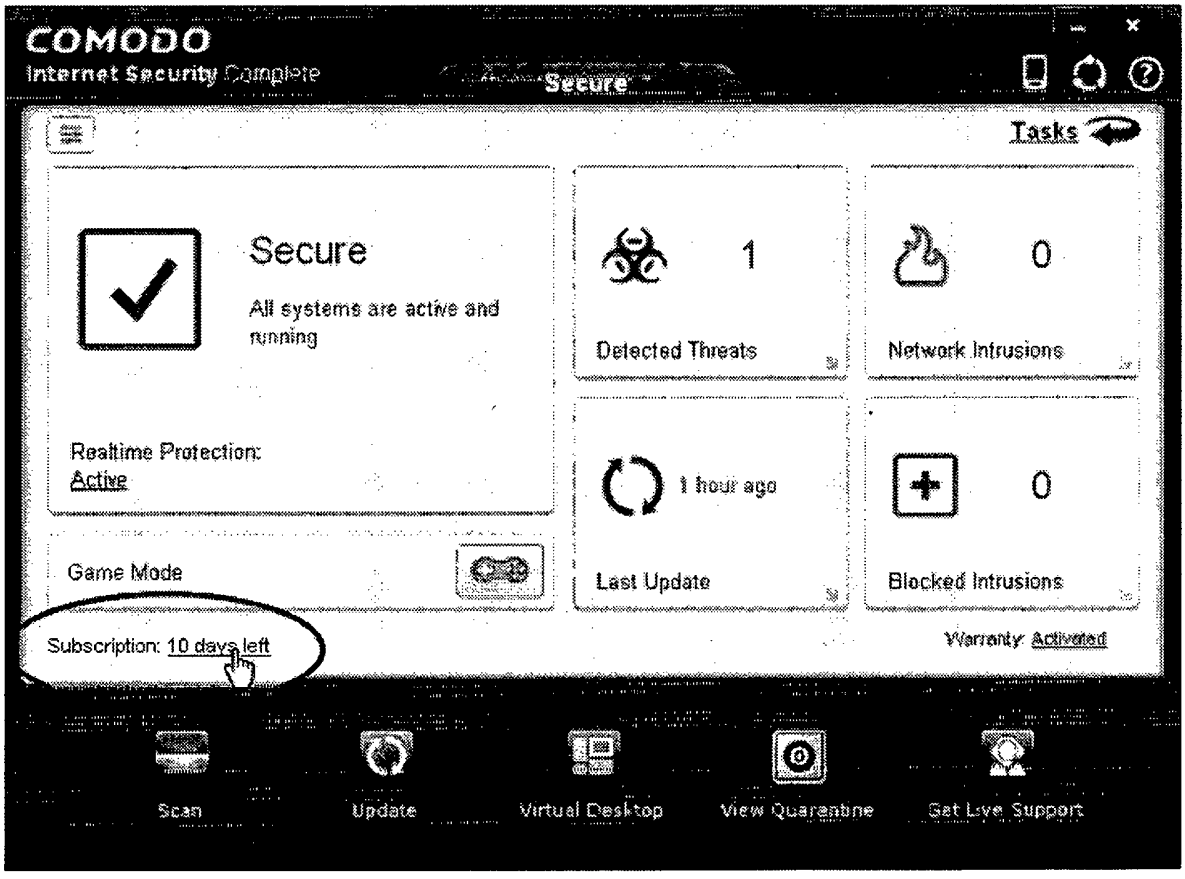


The alerts are now suppressed. To resume alerts and scheduled scans, just de-activate Game Mode from the home screen or the system tray icon right click options.

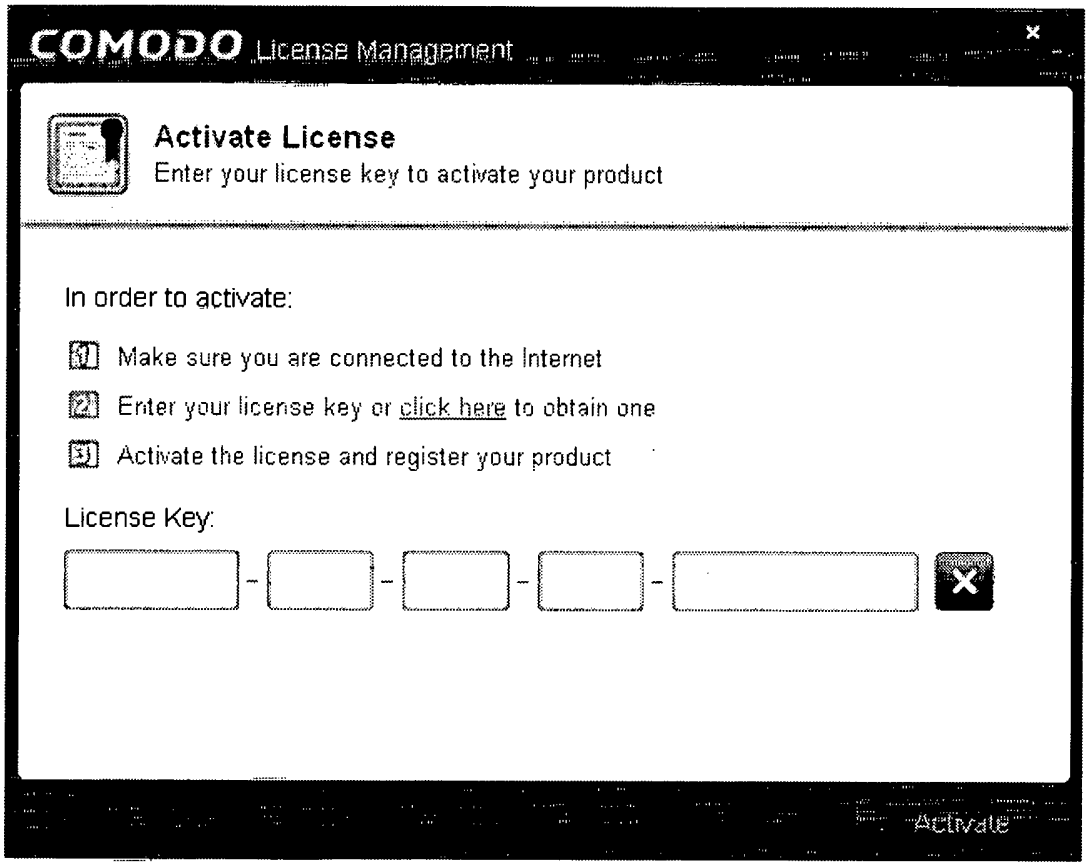
Renew or Upgrade your License

In order to enjoy continued protection from Comodo Internet Security, you will need to renew your license when it is due to expire.

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



The Product Activation Wizard will start.



- Click the 'click here' link. You will be taken to the purchase page at **https://secure.comodo.com/home/purchase.php?afl=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUIzRkY&lid=&**
- Select your CIS Package.
- Select 'Existing Comodo User' checkbox in 'Enter Customer Details' area, enter your login and password and complete the payment procedure.
- The License key will be sent to you by email. Enter the license key and click the 'Activate' button.
- After successful validation, your subscription will be activated and a confirmation screen will be displayed.

If you are renewing a license for the same CIS product then entering the license key will upgrade the license without requiring re-installation. If you are upgrading license types, then installation of the new product type will begin automatically. You may need to restart your computer to finalize the upgrade.

If you are using any of the trial versions of CIS, you have to purchase the license at the end of trial period in order to continue using the product. An alert will be displayed after the expiry of trial period.

- Click the the 'Renew Now' button in the alert screen and follow the same purchase and activation procedure explained above.

How to use CIS Protocol Handlers

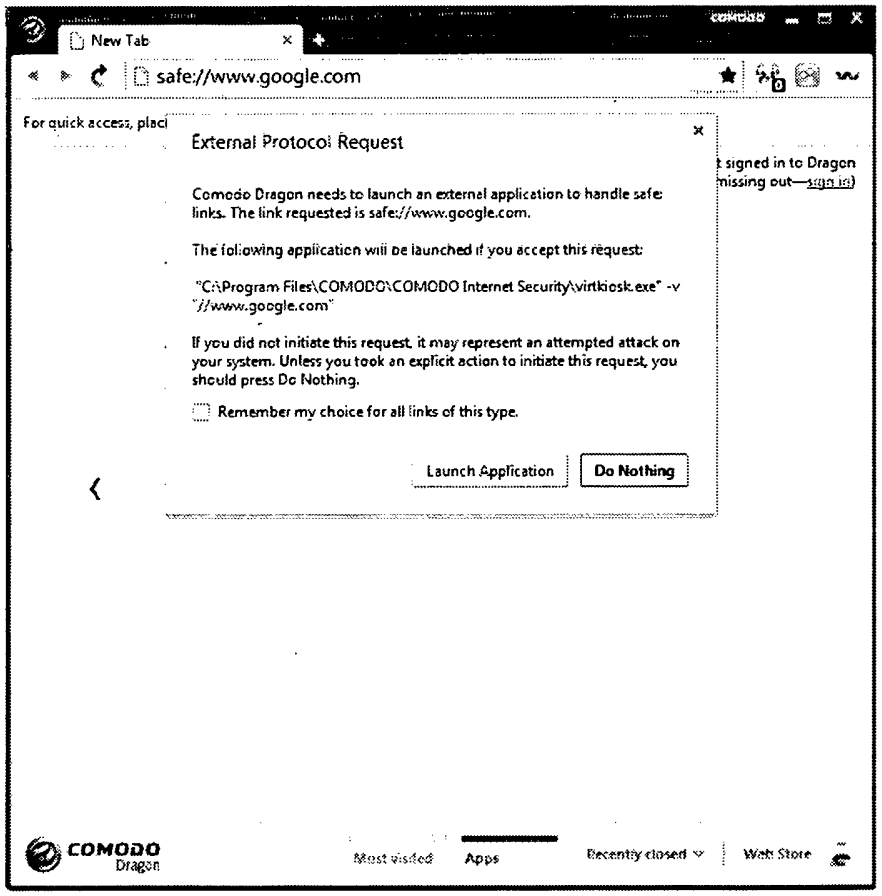
COMODO Internet Security has its own protocol handlers that allow you to perform certain tasks from a web page. This includes tasks like opening a web page from a sandboxed browser, or starting a virus database update etc. CIS 2013 supports several protocol handlers listed below.

1 – safe://

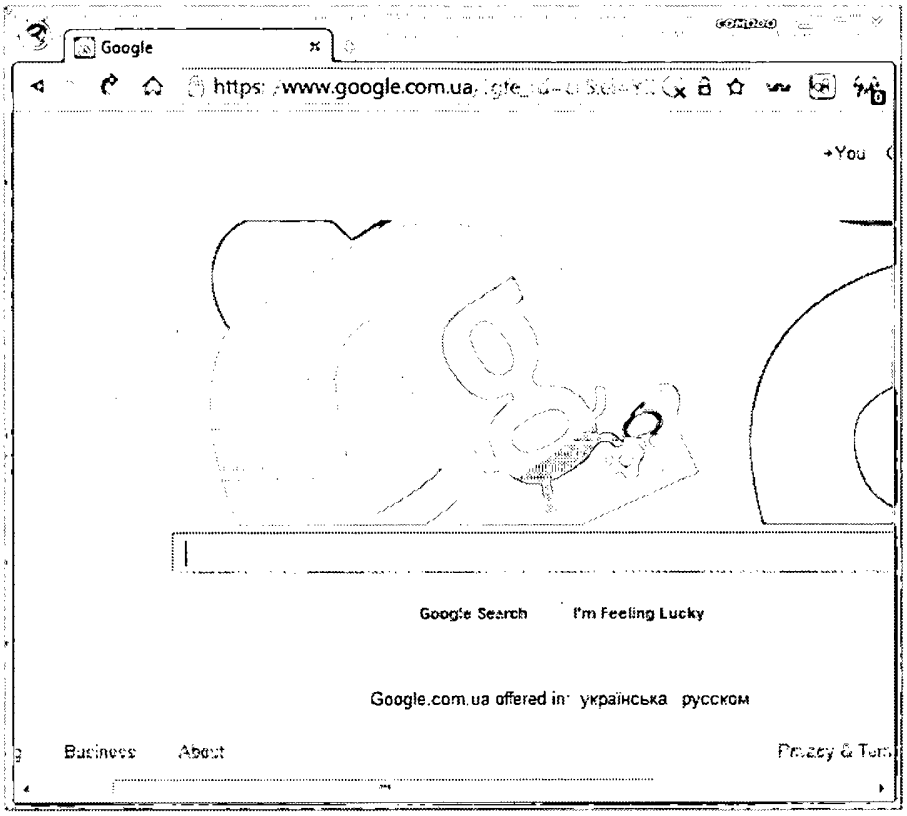
This protocol is used to open any URL with a sandboxed browser.

For example: Try *safe://www.google.com*

The URL will be open in a sandboxed browser. Note the green border:



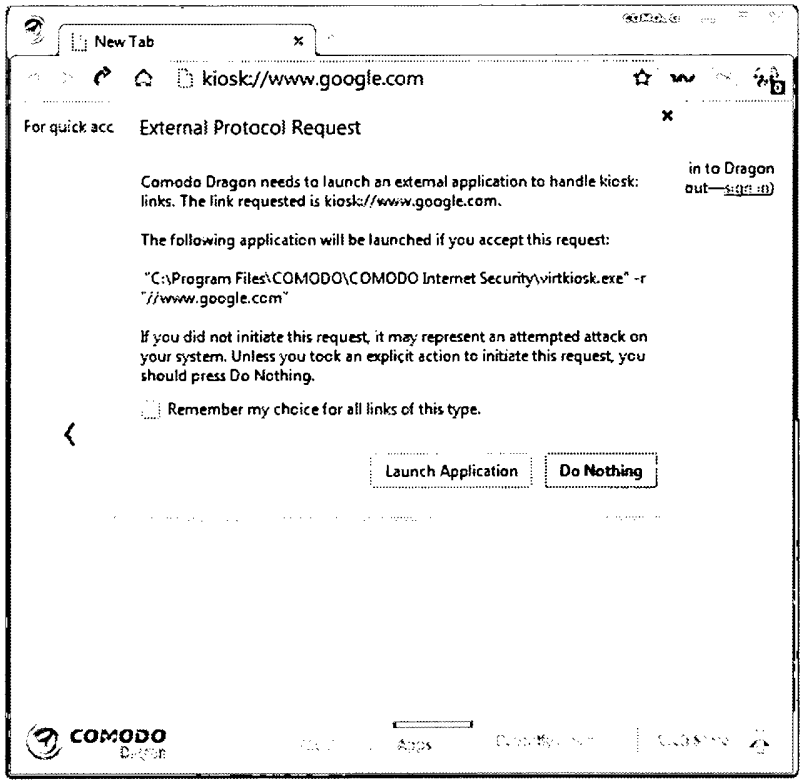
Best Available Copy



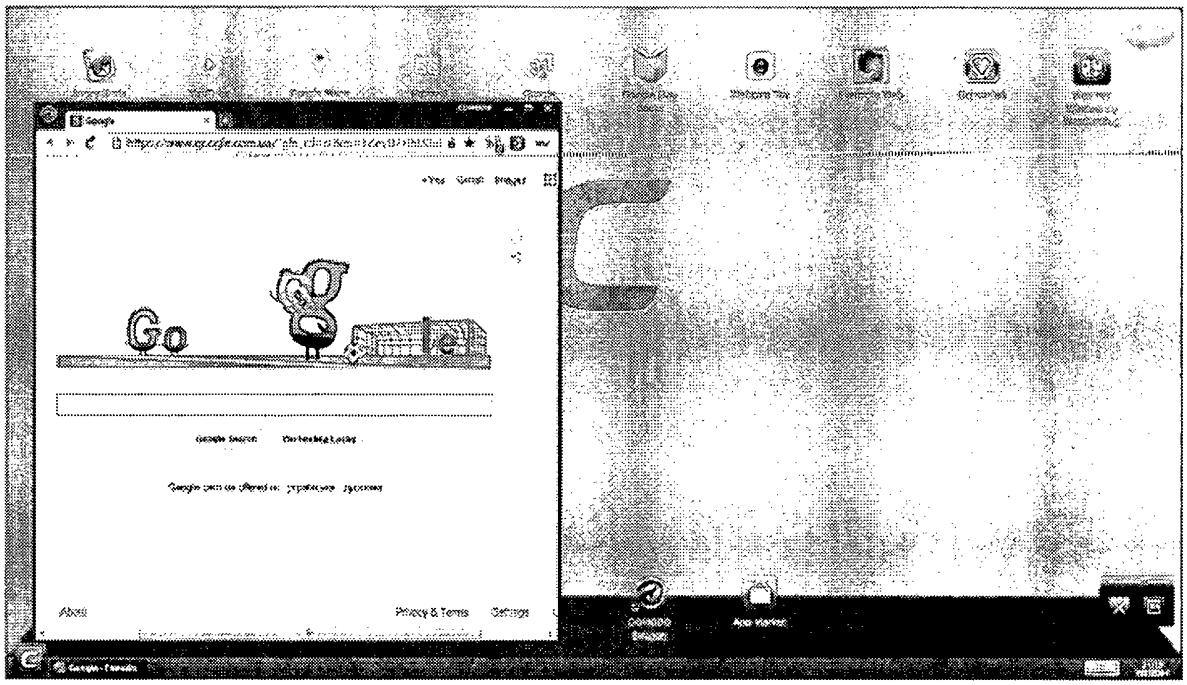
2 – kiosk://

Like the previous one, opens the URL from COMODO Virtual Kiosk.

E.g. Try *kiosk://www.google.com*



URL will display in a browser from the kiosk:



Appendix 2 - Comodo Secure DNS Service

Introduction

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Most of the networks use recursive DNS services that are provided by their ISP or that reside on their own set of small DNS servers but it becomes essential to have a secure and broadly distributed DNS service to have a faster and safe DNS resolution.

Background Note: Every device on the Internet is uniquely identified by a 32-bit number (IPv4) or a 128-bit number (Ipv6). While this is perfectly satisfactory for computers, humans are far more comfortable remembering names rather than a string of numbers. The Domain Name System (DNS) provides the translation between those names and numbers. Virtually every piece of software, device, and service on the Internet utilizes DNS to communicate with one another. DNS also makes this information available across the entire span of the Internet, allowing users to find information remotely.

Comodo Secure DNS is a broadly distributed Recursive DNS service that gives you full control to determine how your clients interact with the Internet. It requires no hardware or software and provides reliable, faster, smarter and safer Internet experience.

- Reliable - Comodo Secure DNS Directory Services Platform currently spans across five continents around the world. This allows us to offer you the most reliable fully redundant DNS service anywhere. Each node has multiple servers, and is connected by several Tier 1 carriers to the Internet.
- Faster - Our strategically placed nodes are located at the most optimal intersections of the Internet. Unlike most DNS providers, Comodo Secure DNS Directory Services Platform uses Anycast routing technology - which means that no matter where you are located in the world, your DNS requests are answered by the closest available Comodo Secure DNS set of servers. Combine this with our huge cache and we can get the answers you seek faster and more reliably than anyone else. Furthermore, our "name cache invalidation" solution signals the Comodo Secure DNS recursive servers anytime one of our authoritative customers or partners updates a DNS record, fundamentally eliminating the concept of a TTL.
- Smarter - Comodo's highly structured search and guide pages get you where you want to be, when you inadvertently attempt to go to a site that doesn't exist.
- Safer - As a leading provider of computer security solutions, Comodo is keenly aware of the dangers that plague the Internet today. Secure DNS helps users keep safe online with its malware domain filtering feature. Secure DNS references a real-time block list (RBL) of harmful websites (i.e. phishing sites, malware sites, spyware sites, excessive advertising sites, etc.) and will warn you whenever you attempt to access a site containing potentially threatening content. Additionally, our 'name cache invalidation' solution signals the Comodo Secure DNS recursive servers whenever a DNS record is updated - fundamentally eliminating the concept of a TTL. Directing your requests through highly secure servers can also reduce your exposure to the DNS Cache Poisoning attacks that may affect everybody else using your ISP.

To start Comodo Secure DNS service the DNS settings of your computer has to be modified to point to our server's IP addresses. Comodo Internet Security automatically modifies the DNS settings of your system during its installation to get the services. You can also modify the DNS settings of your system manually, if you haven't selected the option during installation. You can also revert to the previous settings if you want, at anytime.

Click the following links to get the instructions for manually modifying the DNS settings on your router or on your computer.

- **Router**
- **Windows XP**
- **Windows 7/ Windows Vista**

Router - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Router by modifying the DNS settings accessible

through DNS Server settings of your router. Comodo recommends making the change on your router so that with one change, all the computers on your network can benefit from Comodo Secure DNS.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Primary DNS : 8.26.56.26

Secondary DNS : 8.20.247.20

To stop Comodo Secure DNS service

- **Modify the DNS server IP address to your previous settings**.

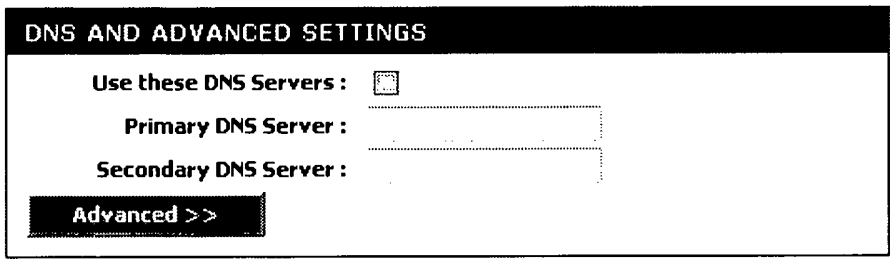
To modify the DNS settings

1. Login to your router. To log in and configure your router, you can open it up in your web browser. If you don't know the IP address for your router, don't worry, it is typically one of the following:

   http://192.168.0.1
   http://192.168.1.1
   http://192.168.10.1

   If you have forgotten your router's username and/or password, the most common username is "admin" and the password is either blank, "admin", or "password". If none of those work, you can often reset the password to the manufacturer default by pressing a button on the router itself, or in some cases access without a password if you try to access your router quickly after you've cycled the power to it.

2. Find the DNS Server Settings. Look for "DNS" next to a field which allows two or three sets of numbers (these fields may be empty).

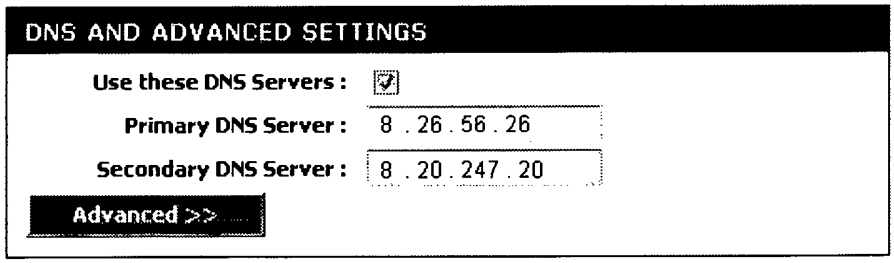


3. Select the check box Use these DNS Servers, type the Comodo Secure DNS Server settings as your DNS server settings and click 'Save'/'Apply'.

   Primary DNS server address for Comodo Secure DNS is: 8.26.56.26

   Secondary DNS server address for Comodo Secure DNS is: 8.20.247.20

   When you are done, the above example would look like this.



You can disable Comodo Secure DNS by:

- Deselecting the check box 'Use these DNS servers' address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.

Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable Comodo Secure DNS service in your Windows XP computer by modifying the DNS settings accessible through Control Panel > Network Connections.

To enable the Comodo Secure DNS service, modify the DNS server IP address settings to Comodo Secure DNS server IP addresses. The IP address are:

Preferred DNS : 8.26.56.26

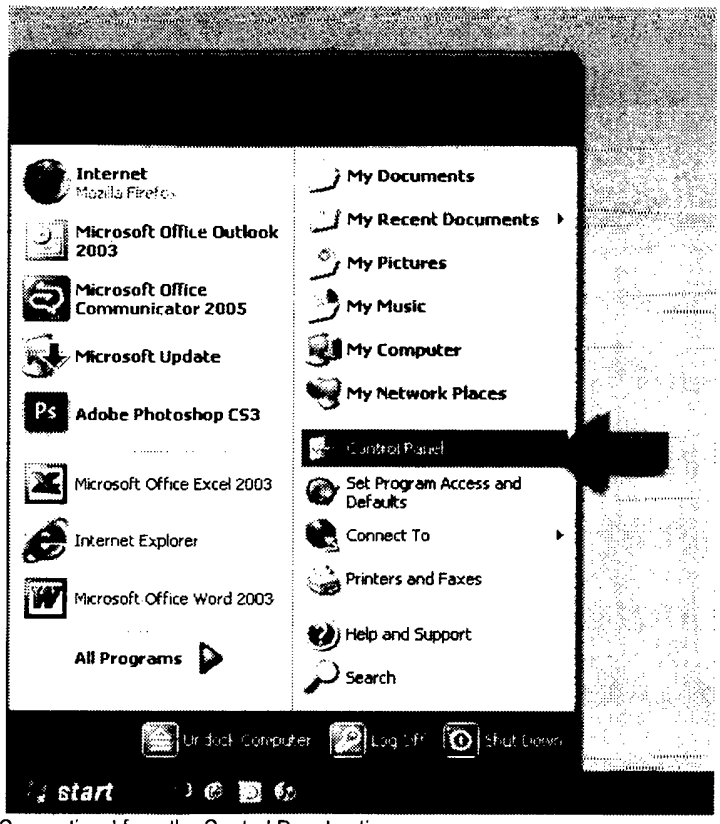
Alternate DNS : 8.20.247.20

To stop Comodo Secure DNS service

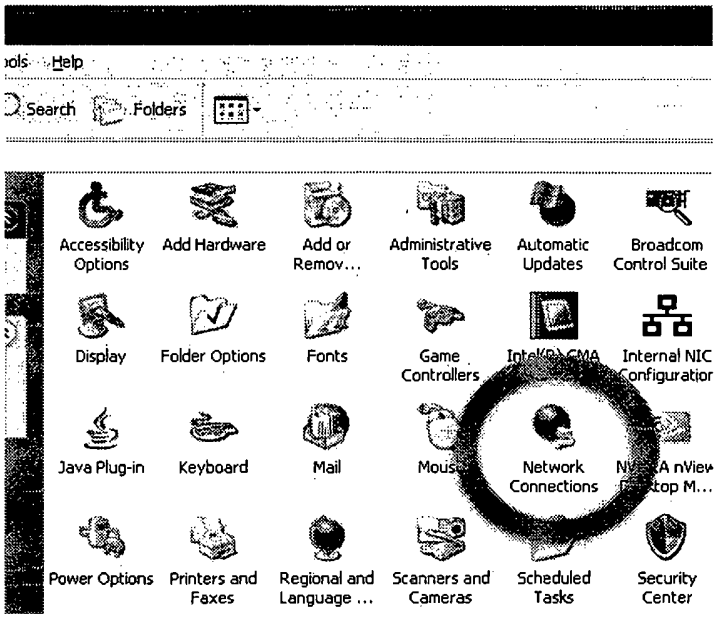
- **Modify the DNS server IP address to your previous settings.**

To modify the DNS settings

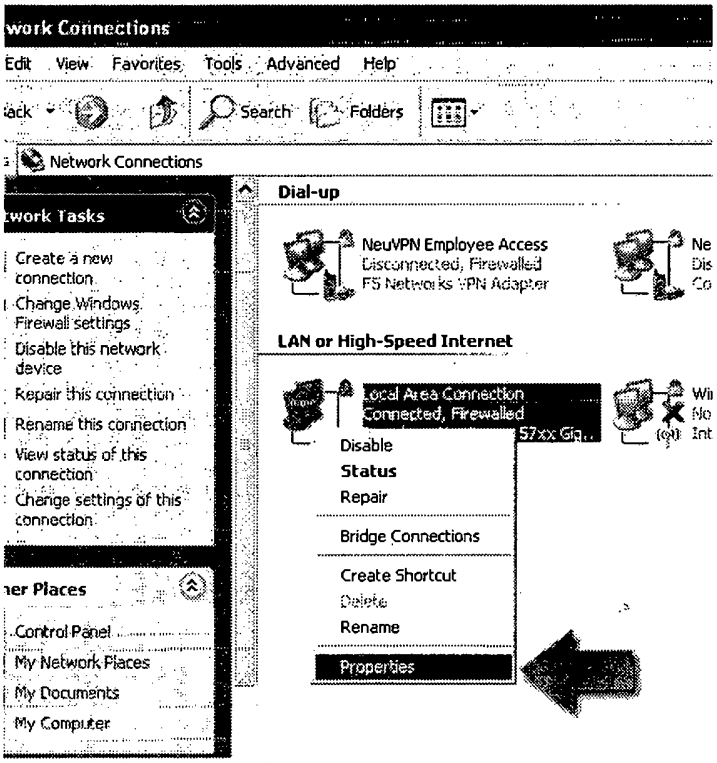
1. Select the 'Control Panel' from the Start Menu.



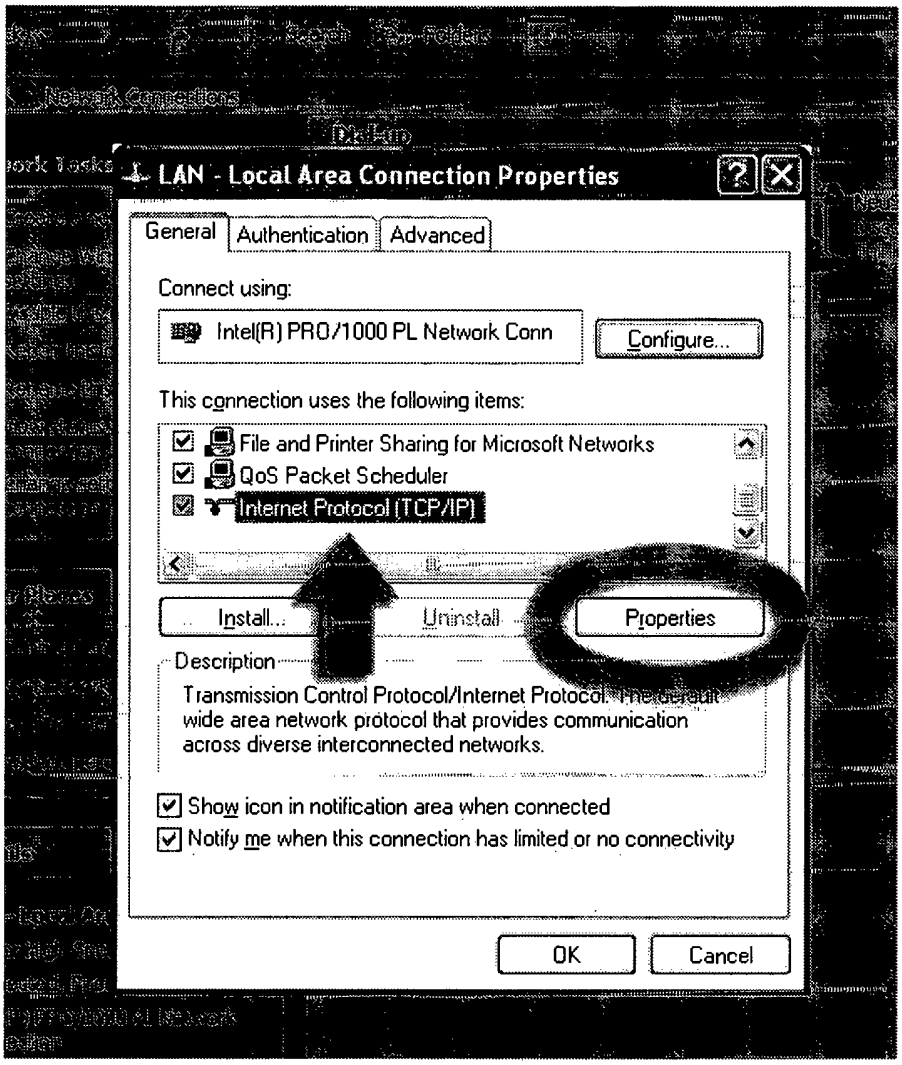
2. Click 'Network Connections' from the Control Panel options.



3. Right click on your connection from the Network Connections window and click 'Properties'.



4. Select 'Internet Protocol (TCP/IP)' and click 'Properties'.

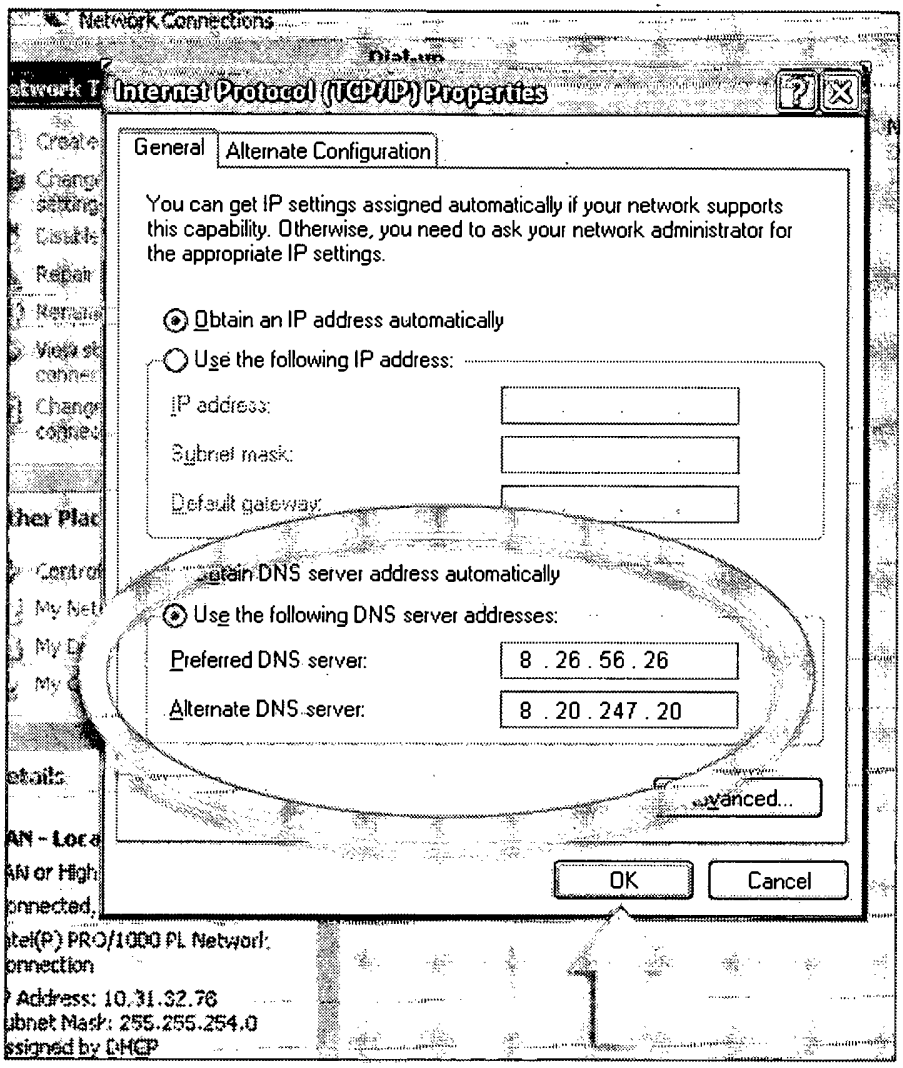


5. Click the radio button Use the following DNS server addresses and type in Comodo Secure DNS addresses in the Preferred DNS server and Alternate DNS server fields.

   Please note down your current DNS settings before switching to Comodo Secure DNS, in case you want to return to your old settings for any reason.

   Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26

   Alternate DNS server address for Comodo Secure DNS is: 8.20.247.20

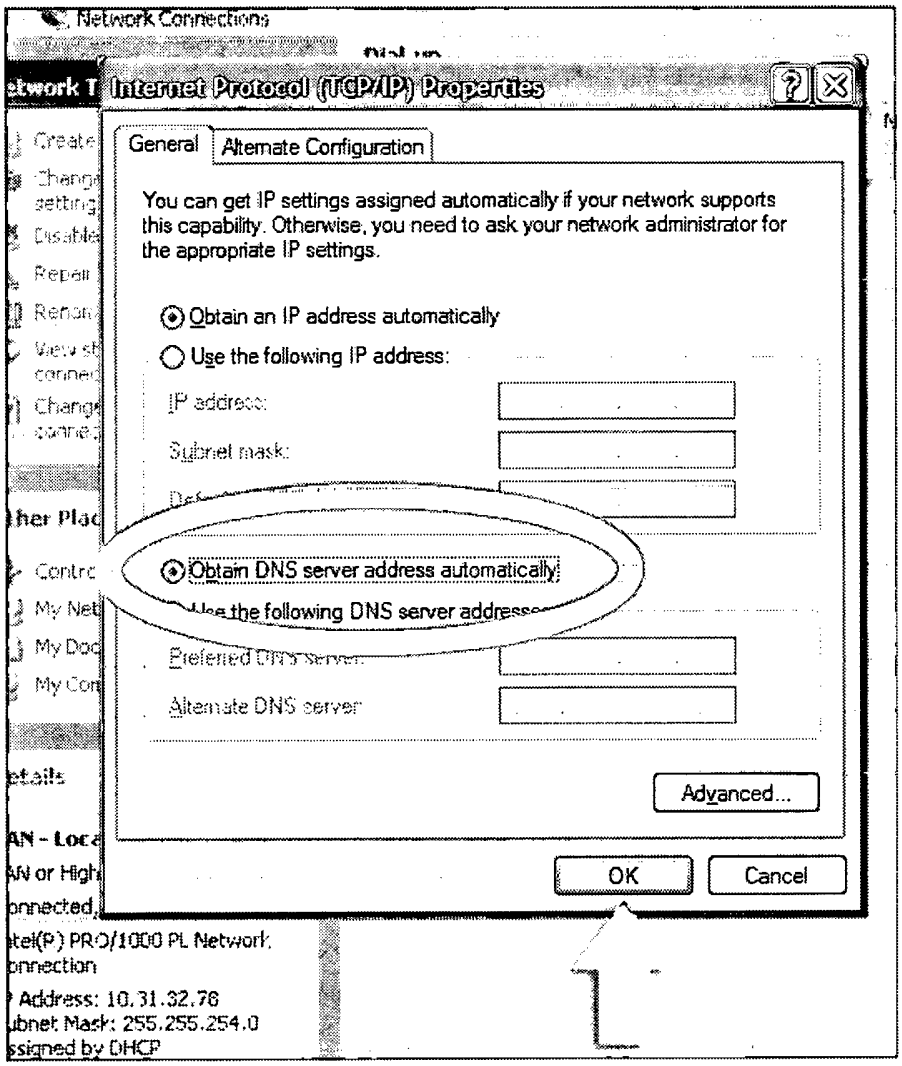


You can disable Comodo Secure DNS by:

- Selecting 'Obtain DNS server address automatically'. This means that you use the DNS server provided by your ISP. This is the option that most home users should choose if they wish to disable the service.

or

- Entering different preferred and alternate DNS server IP addresses.



Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service

You can manually enable or disable the Comodo Secure DNS service by changing your DNS server addresses to:

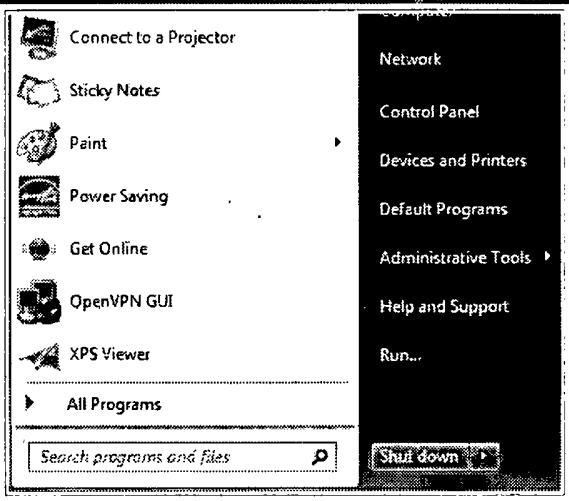
- Preferred DNS : 8.26.56.26
- Alternate DNS : 8.20.247.20

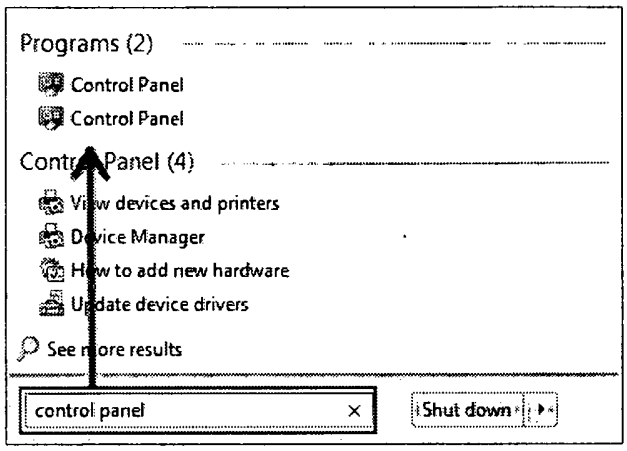
Enabling Comodo DNS in Windows 7 / Vista

Disabling Comodo DNS in Windows 7 / Vista

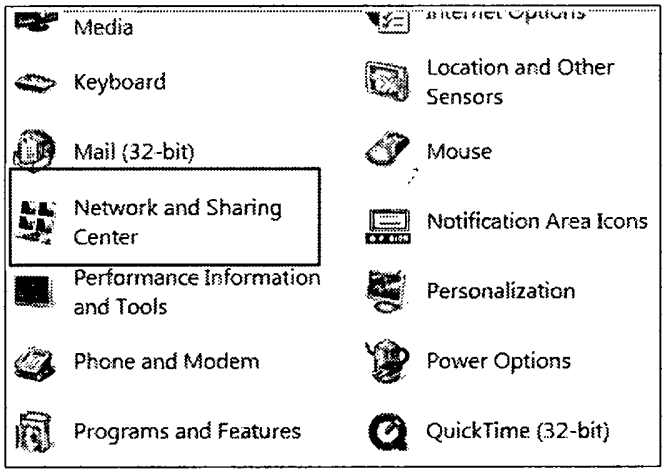
Enabling Comodo DNS in Windows 7 / Vista

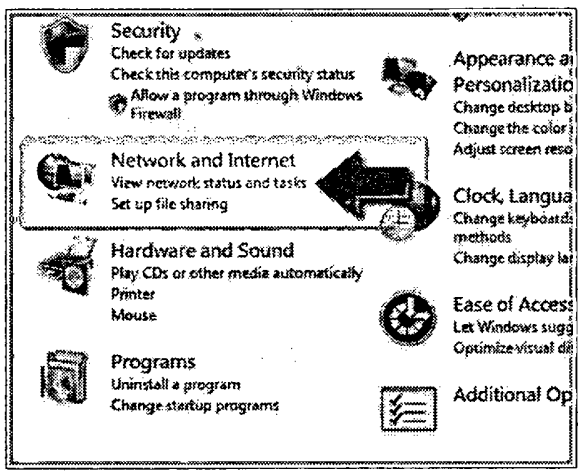
1. Open the control panel by either selecting it from the Windows 'Start' menu or by typing 'control panel' into the search box then clicking the program name.



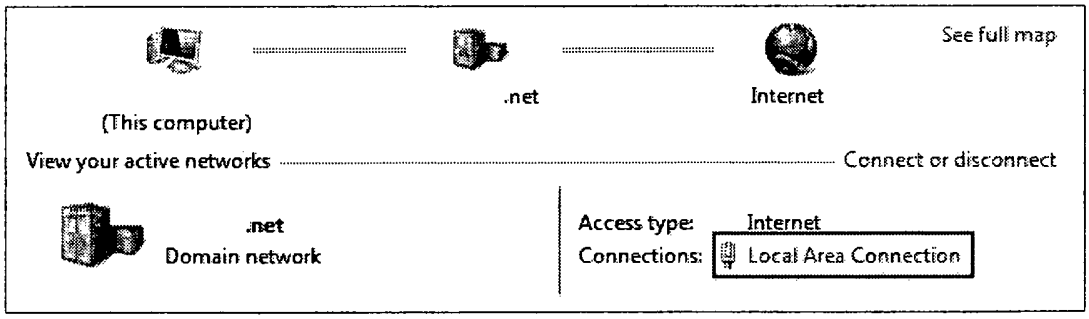


2. From the control panel menu, select 'Network and Sharing Center' (Windows 7) or 'Network and Internet (Vista):

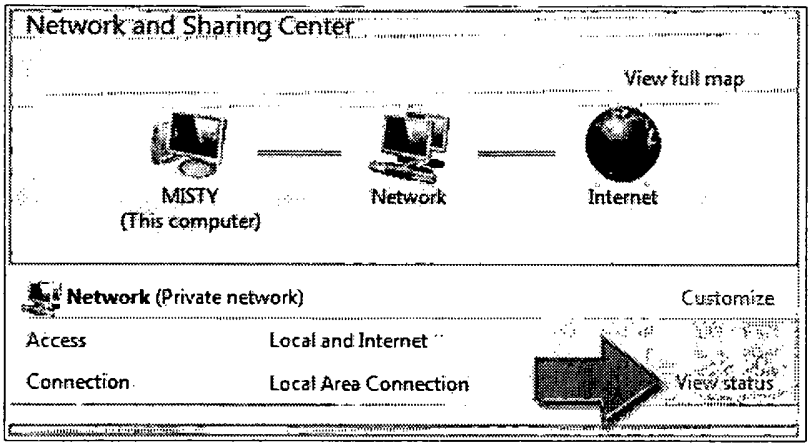




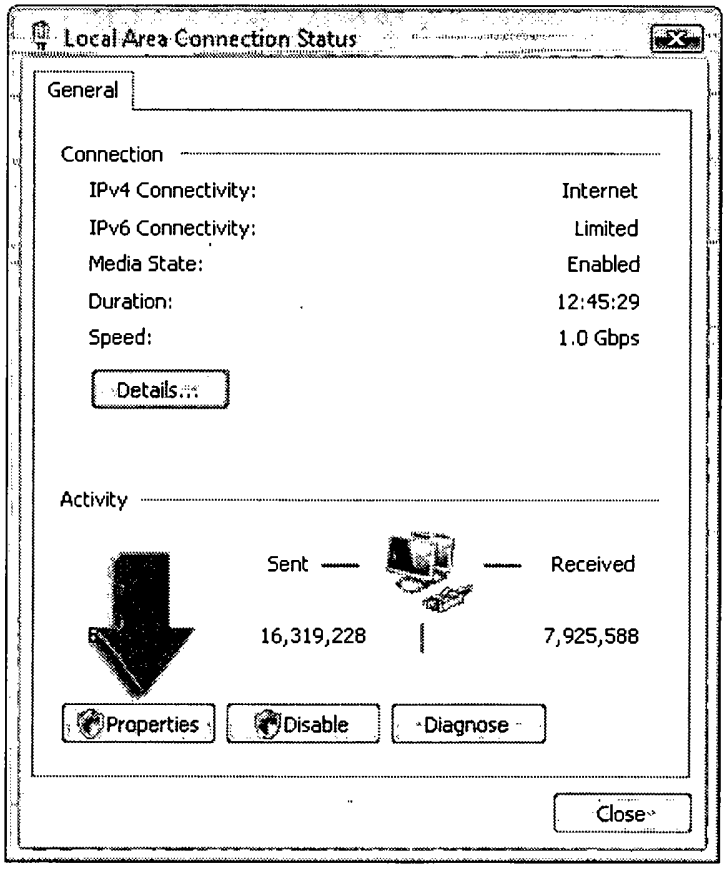
3. In the Network and Sharing center, click the connection type next to 'Connections' (Windows 7):



or 'View Status' (Vista):

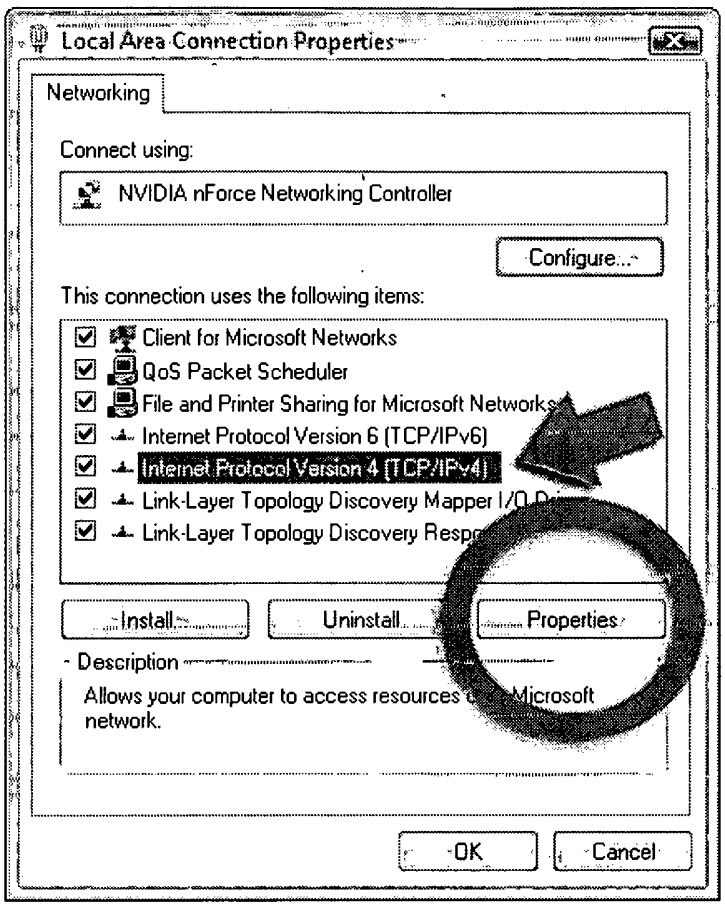


4. This will open the 'Local Area Connection Status' dialog. Click the 'Properties' button:

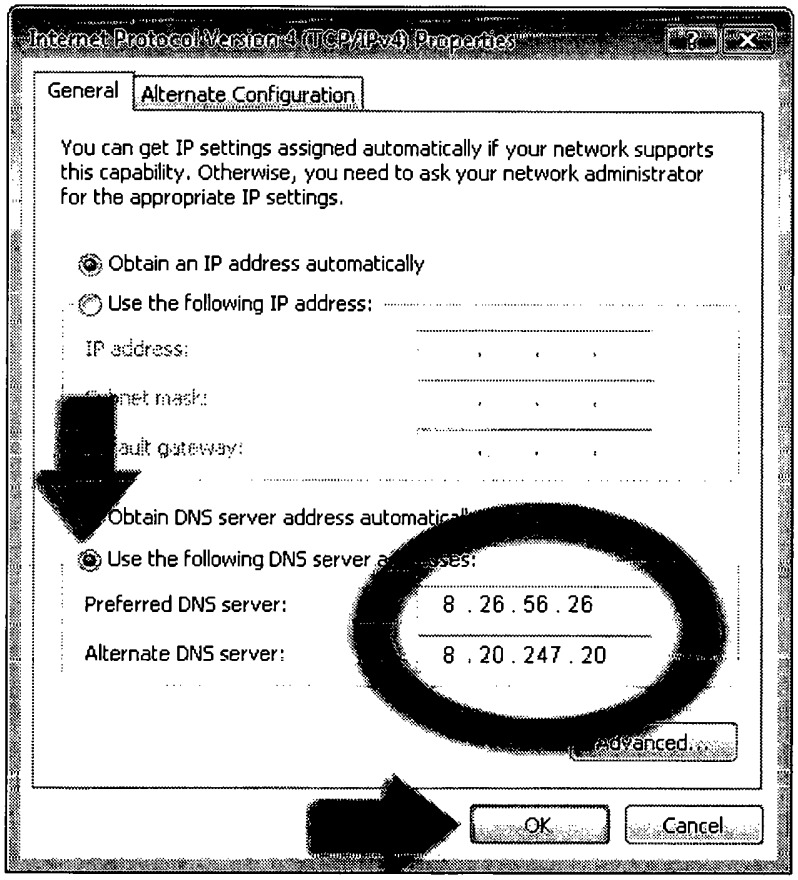


At this point, Windows might ask for your permission to continue or request that you enter an Administrator password.

5. Once you have granted permission/entered an admin password, you will be presented with the 'Local Area Connection Properties' dialog. Scroll down the list and select 'Internet Protocol Version 4 (TCP/IP)' then click the 'Properties' button:



6. Enable 'Use the following DNS server addresses'. Doing so will allow you to enter the addresses of Comodo DNS servers in the fields provided. Enter the addresses listed below then click 'OK' to activate your settings:
    - Preferred DNS : 8.26.56.26
    - Alternate DNS : 8.20.247.20

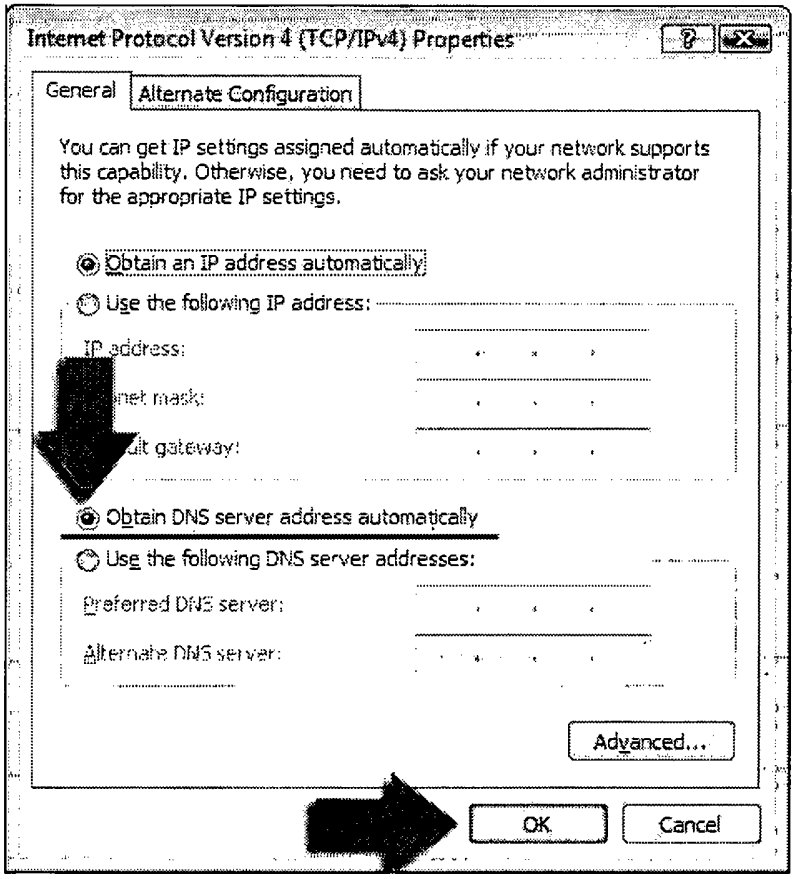


Your computer will now use Comodo DNS as it's default domain name resolution service for all applications that connect to the Internet.

Disabling Comodo DNS in Windows 7 / Vista

To disable Comodo DNS, you need to instruct Windows to automatically obtain the address of a DNS server. Doing so means you will use the DNS server provided by your ISP. To do this:

- Follow steps 1 to 7 of the '**Enabling Comodo DNS in Windows 7 / Vista**' tutorial to open the IP4 properties dialog
- Enable 'Obtain DNS server address automatically' then click 'OK'.



Note: Alternatively, you can enter the server addresses of a different DNS service before clicking 'OK'

Appendix 3 - Glossary Of Terms

A B C D E F G H I J K L M N O P Q R S U V W X Y Z

A

ACK

The acknowledgment bit in a TCP packet. (ACKnowledgment code) - Code that communicates that a system is ready to receive data from a remote transmitting station, or code that acknowledges the error-free transmission of data.

Back to the top

Adware

Adware 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

Auto-sandbox

Auto-sandboxing describes the process whereby applications and processes which are unknown to Comodo Internet Security will be automatically run in a isolated operating environment. Sandboxed applications are run under a set of access restrictions so they cannot cause damage the underlying file structure or operating system. The access restriction level applied to

sandboxed applications can be set by the user and includes 'Limited', 'Partially Limited', 'Restricted', 'Untrusted', 'Blocked' and 'Fully Virtualized'.

Conceptually, the auto-sandbox is designed to securely handle 'unknown' executables - those which are not present on Comodo's black-list (definitely malicious) or white-list (definitely safe). If the unknown file turns out to be malicious then it cannot cause any harm because the sand-boxing process denied it access to critical system resources. On the other hand, programs that are unknown but perfectly harmless will run just as well in the sandbox. This allows safe applications the freedom to run as intended while denying malicious applications the ability to cause damage.

The auto-sandbox process is further enhanced if it is married to a system that can subsequently classify these unknown files as either 'safe' or 'malicious'. In Comodo Internet Security, sandboxed files can be submitted to Comodo servers* for automated behavior analysis. If this analysis discovers the file is malicious then it is added to the black-list which is distributed to all CIS users. If the file does not exhibit malicious behavior it is passed to Comodo labs for more in-depth tests and possible inclusion on the white-list.

** if enabled by the user*

Back to the top

B

Behavior Analysis

An activity performed by CIS to determine whether an unknown application in the sandbox is malicious or not. Unknown files are analyzed by Comodo Cloud Scanners and Comodo's Instant Malware Analysis (CIMA) servers. If found to be safe, they will be submitted to Comodo labs for further checks.

Back to the top

Behavior Blocker

A Host Intrusion Protection (HIPS) mechanism that monitors the behavior of software and files in your system and prevents them from taking actions that would cause damage.

Back to the top

Brute-force

Brute-force search is a trivial but very general problem-solving technique, that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

Back to the top

Buffer Overflow

A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations, often causing the process to crash or produce incorrect results. Hackers use buffer overflows as a trigger to execute to execute malicious code.

Back to the top

Bug

Error in a program that cause problems.

Back to the top

C

CA - Certification Authority

A Certificate Authority (CA) is trusted third party that validates ownership information about a web-server then issues an SSL/TLS certificate to the organization that owns the server. The certificate is then placed on the web-server and is used to secure connections between the server and any clients (browsers) that connect to it. For example, an online store would use a certificate to secure its order forms and payment pages.

A Certificate Authority (CA) such as Comodo CA will sign the certificates it issues with their private key. However, for the website's certificate to operate correctly, there is a reciprocal client side requirement - the internet browser that the visitor is using MUST physically contain the certificate authority's 'root certificate'. This root is required to successfully authenticate any website certificates that have been signed by the CA. If the root certificate is not embedded in a browser, then the website's certificate will not be trusted and visitors will see an error message. Certificate Authorities proactively supply browser vendors with their root certificates for inclusion in the browser's 'certificate store' - an internal repository of root certificates that ships with

each browser.

Back to the top

CIS Widget

The CIS Widget is a handy control panel that shows information about the security status of your computer, the speed of outgoing and incoming traffic and other useful information. The widget also has shortcuts to common CIS tasks and allows users to launch sandboxed instances of any internet browser they have installed on their system. By default, the widget is displayed on the desktops of Windows computers running CIS version 6.0 and above.

Back to the top

COM Interfaces

Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers and malicious programs to launch attacks on a computer. Comodo Internet Security automatically protects COM interfaces against modification.

Back to the top

Computer Network

A computer network is a connection between computers through a cable or some type of wireless connection. It enables users to share information and devices between computers and other users within the network.

Back to the top

D

Debugging

The process of identifying a program error and the circumstances in which the error occurs, locating the source(s) of the error in the program and fixing the error.

Back to the top

DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices to connect to a network and be automatically assigned an IP address.

Back to the top

Digital Certificate

A digital certificate is a file used to cryptographically bind a company's Public Key to its identity. Like a driving license or passport binds a photograph to personal information about its holder, a digital certificate binds a Public Key to information about that company. They are issued for between 1 and 5 year validity periods.

Digital certificates are issued by a Certificate Authority like Comodo. Each CA acts as a trusted third party and conducts background checks on a company to ensure they are legitimate before issuing a certificate to them. Apart from providing an encrypted connection between a internet browser and a website, digital certificates are intended to reassure website visitors that the company they are about to make a purchase from can be trusted.

To get a digital certificate, a company must first generate a Certificate Signing Request (CSR) on their web-server. This CSR contains their public key and their identity information. They then enroll and pay for the certificate and send their CSR to the CA.

The CA's validation department will check that the identity information in the CSR is correct by conducting background checks and will sometimes request that the company supplies documentation such as articles of incorporation. Once validation is satisfactorily completed, the CA will issue the certificate to the customer. The customer will then install it on their website to secure sensitive areas like payment pages.

Back to the top

Digital Signature

Digital signatures are used for authentication and integrity, meaning it guarantees that the person sending a message is indeed the same person who he/she claims to be and the message has not been altered. To authenticate oneself using a digital signature, a person needs to download and install Digital Certificates in their systems from Certificate Authorities such as Comodo. The client certificate then can be imported into their browsers and email clients. The same certificate can also be used

to digitally sign a document before sending it. The recipient can easily find out if the document has been tampered with en-route.

Back to the top

DNS

DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. When a user searches for a website name like 'www.domain.com', their browser will first contact a DNS server to discover the IP address associated with that domain name. Once it has this information, it can successfully connect to the website in question.

Back to the top

Dynamic IP

The procedure of allocating temporary IP addresses as they are needed. Dynamic IP's are often, though not exclusively, used for dial-up modems.

Back to the top

E

Encryption

Encryption is a technique that is used to make data unreadable and make it secure. Usually this is done by using secret keys and the encrypted data can be read only by using another set of secret keys. There are two types of encryption - symmetric encryption and asymmetric encryption.

Symmetric encryption is applying a secret key to a text to encrypt it and use the same key to decrypt it. The problem with this type of encryption lies during the exchange of secret keys between the sender and the recipient over a large network or the Internet. The secret keys might fall into wrong hands during the exchange process.

Asymmetric encryption overcomes this problem by using two cryptographically related keys, a key pair - a public key and a private key. The private key is kept secret in your system and the public key is made available freely to anyone who might want to exchange messages with you. Any message, be it text, documents or binary files that are encrypted using the public key can be decrypted using the corresponding private key only. Similarly anything that is encrypted using the private key can be decrypted using the corresponding public key. Typically public keys are made available to everyone by using Digital Certificates. The certificates are issued by a Certificate Authority (CA), which identifies a server or user and usually contains information such as the CA who issued it, the organization's name, email address of the user and country and the public key of the user. When a secure encrypted communication is required between a client and a server, a query is sent over to the other party for the certificate and the public key can be extracted from it.

Back to the top

End User

The person who uses a program after it's been compiled and distributed.

Back to the top

EPKI Manager

Enterprise Public Key Infrastructure Manager. The EPKI Manager allows you to issue bulk numbers of:

- SSL Certificates for use on domain names owned by your Company;
- SecureEmail Certificates (S/MIME) for use by employees of your Company.

Your nominated EPKI Manager Administrator(s) will be able to manage all the company's Certificates from a central web based console. Additional certificates may be purchased through the console in minutes; ensuring new servers and employee email may be secured in minutes rather than days. For more information about EPKI Manager click **here**.

Back to the top

Ethernet

Ethernet is a frame-based computer networking technology for local area networks (LANs). The name comes from the physical concept of ether. It defines wiring and signaling for the physical layer, and frame formats and protocols for the media access control (MAC)/data link layer of the OSI model. Ethernet is mostly standardized as IEEEs 802.3. It has become the most widespread LAN technology in use during the 1990s to the present, and has largely replaced all other LAN standards such as token ring, **FDDI**, and **ARCNET**.

Back to the top

Executable Files

An 'executable' is a file that instructs a computer to perform a task or function. Every program, application and device run on computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. For example, when Microsoft Word is started, the executable file 'winword.exe' instructs the computer to start and run the Word application. Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Back to the top

F

False Positive

When an antivirus scan is run and the scanner reports that some programs are infected with malware which may not be the actual case and the files are safe. This kind of false alert is called 'False Positive'. Too much of False Postive results can be annoying and the user might just ignore legitimate warning or delete legitimate files causing the relevant program or operating system to malfunction.

Back to the top

Firewall

A firewall is an application that helps an user or administrator to have a control over how the system should be connected with other network/systems or over the Internet.

Back to the top

FS type

Type of file system.

Back to the top

FTP

File Transfer Protocol (FTP) is a protocol used for file transfer from computer to computer across a TCP network like the Internet. An anonymous FTP is a file transfer between locations that does not require users to identify themselves with a password or log-in. FTP uses the TCP/IP protocols to enable data transfer. FTP is most commonly used to download files from a server or to upload a file to a server.

Back to the top

G

Graphical User Interface (GUI)

The visual symbols and graphics with which a user controls a piece of software or device. Most software has a GUI that comprises of windows, menus, and toolbars. The user interacts with the GUI by clicking their mouse on a GUI element. Operating systems like Windows use GUI's because most users find them easier to use than less friendly interfaces like a command line.

Back to the top

H

Heuristics

Heuristics is a technique that continuously evolves based on experience for solving problems, discovery and learning. When the term is used in computer security parlance, Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist. Comodo Internet Security applies this technology in the application, which is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

Back to the top

HIPS

A Host Intrusion Protection System (HIPS) is designed to identify and block zero malware by monitoring the behavior of all applications and processes. It is designed to prevent actions that could cause damage to your operating system, system-memory, registry keys or personal data.

Security software using a HIPS system will generally enforce rules prescribing the permitted activities of processes and executables at the point of execution. Examples of such activities can include changes to files or directories, accessing protected COM interfaces, modifications to the registry, starting up another application or writing to the memory space of another

application. The precise nature of these rules can be set by the user or pre-configured by the vendor.

If an executable or process attempts to perform an action that transgresses these rules then the HIPS system will block the attempt and generate an alert notifying the user of that action. Most HIPS alerts will also include security advice.

Back to the top

HTTP

HTTP (Hypertext Transfer Protocol) is the foundation protocol of the World Wide Web. It sets the rules for exchanges between browser and server. It provides for the transfer of hypertext and hypermedia, for recognition of file types, and other functions.

Back to the top

I

ICMP

The Internet Control Message Protocol (ICMP) is part of Internet Protocol (IP) suite and used to report network applications communications errors, network congestion, timeouts and availability of remote hosts.

Back to the top

IDS

An Intrusion Detection System (IDS) is software/hardware that detects and logs inappropriate, incorrect, or anomalous activity. IDS are typically characterized based on the source of the data they monitor: host or network. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Back to the top

IMAP

Internet Message Access Protocol'. IMAP is a method of distributing email. It is different from the standard POP3 method in that with IMAP, email messages are stored on the server, while in POP3, the messages are transferred to the client's computer when they are read. Thus, using IMAP allows you to access your email from more than one machine, while POP3 does not. This is important because some email servers only work with some protocols.

Back to the top

Information Security Exposure

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

Back to the top

Internet Service Provider (ISP)

A company or organization that provides the connection between a local computer or network, and the larger Internet.

Back to the top

IP - Internet Protocol

The Internet Protocol (IP) is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched network. An IP address is a numeric address that is used to identify a network interface on a specific network or subnetwork. Every computer or server on the Internet has an IP address. When a user types a domain name such as www.domain.com into the address bar of their browser, the browser still needs to find the IP address associated with that domain in order to reach the website. It finds the IP address by consulting with a DNS server.

There are currently two versions of IP in use today - IPv4 and Ipv6.

IPv4 (Internet Protocol version 4) was developed in 1981 and is still the most widely deployed version - accounting for almost all of today's Internet traffic. However, because IPv4 uses 32 bits for IP addresses, there is a physical upper limit of around 4.3 billion possible IP addresses - a figure widely viewed as inadequate to cope with the further expansion of the Internet. In simple terms, the number of devices requiring IP addresses is in danger of exceeding the number of IP addresses that are available.

IPv6 is intended to replace IPv4, which uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile devices and more efficient routing of data packets.

Back to the top

K

Key Logger

Key logger is a software application or a hardware device that keeps tracks of computer activity in real time including the keys that are pressed. Key loggers are used to troubleshoot technical problems in computer systems. The application can also be used for malicious purposes such as to steal passwords and other sensitive information.

Back to the top

L

LAN

A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology running at 10, 100 or 1,000 Mbit/s (1,000 Mbit/s is also known as 1 Gbit/s).

Back to the top

Leak Test

Leak Test is a way to find out how well your system is protected by your security software from external and internal threats. Typically these tests are down-loadable and should not cause any harm to your system while being run. The Firewall Leak Tests are used to test how effective the firewall component of your security software is at detecting and blocking outgoing connection attempts. If an application is able to connect to the Internet without your knowledge, it poses a real danger meaning it can easily retrieve private and confidential information from your system and transmit it.

Host Intrusion Prevention System (HIPS) tests are designed to test how well your security software is capable of protecting your internal system from malicious attacks such as viruses. A good HIPS system will deny the malware from accessing your critical operating system files, registry keys, COM interfaces and running processes.

Back to the top

License

The official terms of use for a specific program. A software license is a legal document since it formally restricts the rights of the user.

Back to the top

M

MAC Address

A Media Access Control (MAC) address is a number that is hardwired in network adapters and is used to identify the device or system in which it is installed.

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

Back to the top

Malicious File

Often called 'Malware', a malicious file is software designed to damage computer systems, steal sensitive information or gain unauthorized access to private computer systems. For example it may be coded to gather sensitive information from a system such as passwords, credit card details and send them back to the creator of the malware.

Back to the top

Malware

Malware is short for 'malicious software'. It is an umbrella term that describes a wide range of malicious software including viruses, trojans, worms, scripts and root kits. When installed on a computer system or network, malware can disrupt operations, steal sensitive and personal information, delete important data, create zombie networks and perform other destructive operations.

Back to the top

N

Network (computer)

Networking is the scientific and engineering discipline concerned with communication between computer systems. Such networks involves at least two computers, which can be separated by a few inches (e.g. via Bluetooth) or thousands of miles (e.g. via the Internet). Computer networking is sometimes considered a sub-discipline of telecommunications.

Back to the top

Network Zone

A Network Zone can consist of an individual machine (including a single home computer connected to Internet) or a network of thousands of machines to which access can be granted or denied. The creation of network zones helps an administrator to apply changes for all the computer(s) in selected zone(s).

Back to the top

NIDS

NIDS - Network-Based Intrusion Detection System. Detects intrusions based upon suspicious network traffic. A network intrusion detection system (NIDS) is a system that tries to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic.

Back to the top

NNTP

Network News Transfer Protocol - Refers to the standard protocol used for transferring Usenet news from machine to machine. A protocol is simply a format used to transfer data to two different machines. A protocol will set out terms to indicate what error checking method will be used, how the sending machine will indicate when it is has finished sending the data, and how the receiving machine will indicate that it has received the data.

Back to the top

O

Operating System (OS)

The essential software to control both the hardware and other software of a computer. An operating system's most obvious features are managing files and applications. An OS also manages a computer's connection to a network, if one exists. Microsoft Windows, Macintosh OS, and Linux are operating systems.

Back to the top

P

Ping

Ping is a computer network tool used to test whether a particular host is reachable across an IP network.

Back to the top

PKCS

PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Security.

Back to the top

PKCS#7

See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS).

Back to the top

PKCS#10

See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.

Back to the top

PKCS#12

Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

Back to the top

Plugin

A program that allows a Web browser to display a wider range of content than originally intended. For example: the Flash plugin allows Web browsers to display Flash content.

Back to the top

POP2

There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Back to the top

POP3

POP3 is the abbreviation for Post Office Protocol - a data format for delivery of emails across the Internet.

Back to the top

Ports

A computer port is an interface that allows communication between applications or processes running on a host computer and other computers, devices or networks.

Your computer sends and receives data to other computers and to the Internet through a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, your machine almost definitely connects to Internet using port 80 and port 443. Your e-mail application connects to your mail server through port 25.

Back to the top

Potentially Unwanted Applications

A potentially unwanted application (PUA) is a piece of software that (i) a user may or may not be aware is installed on their computer, and/or (ii) may have functionality and objectives that are not clear to the user. Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. Because of this ambiguity, many antivirus companies use the term 'Potentially Unwanted Application' to identify such software.

Back to the top

Q

Quarantined Files

After an antivirus scan, files that are detected as malware may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any files moved into quarantine are encrypted so they cannot be run or executed. This prevents infected files from corrupting the rest of a computer.

Back to the top

R

Registry Keys

The Windows Registry serves as an archive for collecting and storing the configuration settings of all computer hardware, software and Windows components. Every time an application or hardware is started, it will access the registry keys relating to it. Applications will also access and modify their registry keys constantly during the course of their execution. As the registry is one of the most regularly accessed parts of Windows, it plays a critical role in the stability, reliability and performance of a computer. Indeed, many computer problems are caused by registry errors. Corrupt keys and invalid keys left by uninstalled applications can often cause severe degradation in system performance, crashes and, in extreme cases, can render a system un-bootable. Inexperienced users are, however, discouraged from making manual adjustments to the registry because a single change can have potentially devastating consequences. There are several dedicated registry cleaners available today, including **Comodo PC TuneUp**.

Back to the top

S

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of email

encapsulated in MIME.

Back to the top

Single User Certificate

A single use certificate refers to the x.509 and associated private key generated by SecureEmail on Alice; stored on SES and downloaded by Bob after a successful SSL client authentication.

Back to the top

SMB

A message format used by DOS and Windows to share files, directories and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include Lan Manager, Windows for Workgroups, Windows NT, and Lan Server. There are also a number of products that use SMB to enable file sharing among different operating system platforms.

Back to the top

SMTP

Simple Mail Transfer Protocol is the most widely used standard for email transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred.

Back to the top

SNMP

Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Back to the top

Spyware

Spyware is a program that performs certain actions without the consent of the user such as displaying advertisements, collecting personal and sensitive information and changing the configuration of the computer. Not all tracking software are malicious since you may have agreed to the conditions as a trade-off for obtaining certain services for free. The tracking software will monitor your online activities to decide what kind of ads should be shown for you.

Back to the top

SSL

Secure Sockets Layer (SSL) is a commonly used protocol for ensuring secure message transmission on the internet. It facilitates an encrypted connection between a web server and an internet browser. It was developed by Netscape in 1994 as a direct response to growing concerns over internet security.

The encryption provided by SSL means that all data passed between a web server and a browser is private and cannot be eavesdropped on. You can tell if you are in an SSL session if the URL begins with https.

SSL is used on the payment pages of millions of websites to protect their online transactions with their customers.

Back to the top

STATIC IP

An IP address which is the same every time you log on to the Internet. See IP for more information.

Back to the top

Stealth Port

Port Stealthing is a security technique whereby ports on an Internet connected PC are hidden so that they provide no response to a remote port scan.

A computer sends and receives data to other computers and to the Internet through an interface called a port. There are over 65,000 numbered ports on every computer - with certain ports being traditionally reserved for certain services. For example, most computers connect to the internet using ports 80 and port 443. Most e-mail applications connect to their mail server through port 25. A 'port scanning' attack consists of sending a message to each port to find out which are open and which are

being used by services. With this knowledge, a hacker can determine which attacks are likely to work against a particular computer. Port stealthing effectively makes it invisible to a port scan. This differs from simply 'closing' a port as NO response is given to any connection attempt ('closed' ports respond with a 'closed' reply- revealing to the hacker that there is actually a PC in existence).

Back to the top

Stateful Packet Inspection

Stateful Packet Inspection, also known as SPI, is an enhanced firewall technique that uses dynamic packet filtering method over the older method of static packet filtering. SPI scrutinizes the packet contents, monitors traffic and keeps track of the sources of packets. A network administrator can configure the firewall that uses SPI according to the needs of the organization, for example, close ports until requested by legitimate users to open them.

Back to the top

SYN

SYN (synchronize) is a type of packet used by the Transmission Control Protocol (TCP) when initiating a new connection to synchronize the sequence numbers on two connecting computers. The SYN is acknowledged by a SYN/ACK by the responding computer.

Back to the top

T

TCP

TCP stands for Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Back to the top

Token-Ring

LAN technology was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5 by the Institute of Electrical and Electronics Engineers. Initially very successful, it went into steep decline after the introduction of 10BASE-T for **Ethernet** and the EIA/TIA 568 cabling standard in the early 1990s. A fierce marketing effort led by IBM sought to claim better performance and reliability over Ethernet for critical applications due to its deterministic access method, but was no more successful than similar battles in the same era over their Micro Channel architecture. IBM no longer uses or promotes Token-Ring. Madge Networks, a one time competitor to IBM, is now considered to be the market leader in Token Ring.

Back to the top

Trojan

A Trojan is a type of malware that looks like a legitimate piece of software and users are tricked to install and execute in their computers. The malware takes the name from the Greek mythology, Trojan Horse, a wooden horse that was used by the Greeks to infiltrate the city of Troy. Once the malware is activated, it can damage the system, spread other computer viruses and also create a back door so as to allow online fraudsters to take access or control the system.

Back to the top

Trusted Files

In Comodo Internet Security, a trusted file is one that is considered safe and is allowed to run on a user's computer. This type of file can also be referred to as a 'safe' file or a 'white-listed' file.

A file will be treated as safe if it is in the 'Trusted Files' list OR if it is digitally signed by a 'Trusted Software Vendor'. Comodo Internet Security ships with a list of trusted files and a list of Trusted Vendors. Users can add their own trusted files and vendors to their local installation. They can also submit files and vendors to Comodo so they can be considered for inclusion in future safe lists.

Back to the top

Trusted Software Vendor

A Trusted Software Vendor (TSV) is a publisher of software that is automatically trusted by Comodo Internet Security software. Executable files that have been digitally signed by a TSV will be allowed to run normally and will not be placed in the sandbox.

Many software vendors digitally sign their software with a code signing certificate. Digitally signed software helps a user to identify the publisher and to be sure that the software he/she is downloading is genuine and has not been tampered with. Each code signing certificate is counter-signed by a trusted certificate authority (CA) after the CA has conducted detailed checks that the vendor is a legitimate company.

Back to the top

U

User

A person who uses a computer, including a programmer or **end user**.

Back to the top

V

Virtual Desktop

The Virtual Desktop is a standalone sandbox featured in Comodo Internet Security which allows users to run any applications in a completely virtual environment. Software in the virtual desktop will not affect other processes, programs or data on the user's computer. Similarly, internet browsers running in the virtual desktop leave behind no personally identifying cookies or history on an employee's real system. The virtual desktop also features a virtual keyboard which provides additional security when entering usernames and passwords on website login pages. Although the virtual desktop is primarily intended for users to test unknown or beta software and for launching highly secure browsing sessions, it can be used to run most software. The virtual desktop interface is available in both desktop and tablet optimized versions.

Back to the top

Virtual Machine (VM)

Virtual machine is a software application that emulates a computing environment in which a program or an operating system can be installed and run. There are many advantages in using a VM such as for testing out new applications or procedures without affecting the host system.

Back to the top

Virus

A computer virus is an executable application capable of causing damage to computer files, folders and components. Viruses are also capable of self-replication so can infect multiple items on a system if left unchecked. The malicious activities performed by a virus are wide ranging and include stealing confidential information, modifying user data, overwriting or damaging files and erasing hard disk content.

Back to the top

Viruscope

Viruscope is an innovative subsystem that monitors all the processes running on a computer in real time to find any suspicious actions taken by any of the processes. If a suspicious activity is identified, Viruscope generates an alert. The alert allows the user to quickly block the process, reverse the effects of the action and move the parent application of the process to quarantine, if the activity is found to be malicious, or to allow the process, if the action is found to be legitimate.

Back to the top

Virus Database

A database of the digital signatures of all known computer viruses and malware. This database, sometimes referred to as a 'black list', enables antivirus software to detect any malware running on a customer's computer.

Every time a file or executable is identified as being malware, antivirus companies will create a digital signature of the file and add it to their database of blacklisted files. This database is then distributed to their customers as an update to their antivirus software. If the blacklisted signature of the malware is found anywhere on a customers computer, then the file is flagged as infected and may be quarantined or deleted.

Comodo has a dedicated team of technicians and crawlers that are continually searching for new virus strains to add to our database. Comodo's virus database is available for public download at
http://internetsecurity.comodo.com/updates/vdp/database.php

Back to the top

Vulnerability

In network security, a vulnerability refers to any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network.

Back to the top

W

Website Filtering

Website Filtering is a security technique whereby access to specific websites can be selectively blocked or allowed to particular users of the computer. The website filtering is very useful for parental control as it allows to block inappropriate websites to juvenile users. Also, in work environments, administrators can prevent employees from visiting social networking sites during working hours.

Back to the top

Web server

The term Web server can mean one of two things:

1. A computer that is responsible for accepting **HTTP** requests from clients, which are known as Web browsers, and serving them Web pages, which are usually HTML documents and linked objects (images, etc.).

2. A computer program that provides the functionality described in the first sense of the term.

Back to the top

Worm

A Worm, another type of malware, unlike virus is capable of spreading from computer to computer without any human help. The worm with its capability to replicate itself several times over consumes most of the system memory causing the computer to slow down or crash altogether. It can also cause bandwidth jam while spreading to other computers in the network.

Back to the top

Wildcard

Wildcards are symbols that add flexibility to a keyword search by extending the parameters of a search word. A wildcard item is usually denoted with the asterisk symbol, '*'. This stands for one-or-more characters (useful for all suffixes or prefixes). In digital certification terms, a 'wildcard certificate' means that the certificate will secure the domain plus unlimited sub-domains of that domain. A wildcard certificate is applied for using the format '*.domain.com'.

Back to the top

X

X.509

An internationally recognized standard for certificates that defines their required parts

Back to the top

Z

Zero-Day Malware

Zero-day malware describes new computer viruses or worms that have been discovered in the public realm but which antivirus vendors have not yet created a digital signature for. The term means that the antivirus companies have had 'zero-days' to react. New malware can reasonably be called 'zero-day' for the the length of time between its discovery and the creation of a signature to combat it. For most antivirus vendors, this is usually measured in a matter of hours. Of course, the malware itself may have been at large for a much longer period of time before it was discovered. Because of this window of vulnerability, most security software has grown beyond a reliance on traditional, signature based detection. Most antivirus software now contains layers of prevention-based technologies intended to detect and neutralize 'unknown' malware until such time as a signature can be created. Example technologies include heuristic detection, host intrusion prevention (HIPS), automatic sandboxing and real-time behavior analysis.

Back to the top

Appendix 4 – CIS Versions

Comodo Internet Security is available in three versions – Premium (free), Pro and Complete. The Pro version includes **Comodo GeekBuddy** (Comodo support experts available 24/7 to fix any problem with your computer) and the Virus Free Guarantee (if your computer becomes damaged as a result of malware and Comodo support services cannot return it to a working condition then we'll pay the costs of getting it repaired. Please see the **End User License Agreement** for full details). CIS Complete includes GeekBuddy, the Virus Free Guarantee, **TrustConnect** (a secure Internet proxy service that ensures 128 bit encrypted connectivity from any public wireless hotspot) and a Comodo Online Backup account (50GB of online storage space).

Product	Includes					Protection Plan		Price*
	Antivirus	Firewall	GeekBuddy	TrustConnect	Online Storage	Virus Free Guarantee (VFG) / Identity Protection (IDP)	Virus Removal Service	
CIS Premium 7.x	✓	✓	✓	✘	✘	✘	✘	Free
CIS Pro 7.x	✓	✓	✓	✘	✘	✓	✓	$39.99/year or $3.99/month
CIS Complete 7.x	✓	✓	✓	✓ (10 GB / Month)	✓ (50 GB Free. Upgrades available)	✓	✓	$89.99/year or $8.99/month
CAV Free	✓	✘	✘	✘	✘	✘	✘	Free
CAV Advanced	✓	✘	✘	✘	✘	✘	✓	$19.99/year or $3.49/month
Comodo Firewall	✘	✓	✘	✘	✘	✘	✘	Free

* Most CIS products also have discounts for multi-year purchases.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **http://www.comodo.com.**

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:**

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Date Mailed : February 4, 2021

Glenn Coleman
600 Third Avenue
New York, NY 10016

Serial Number : 16/141378

Applicant is advised that under rule MPEP 707.13 the office action previously mailed on September 9, 2020 to applicant's attorney was returned to the office as undeliverable. Currently the office has no official change of address from applicant's attorney of record.

The time period as specified on the attached PTO-326 form for reply to the Office action will be restarted to run from the mailing date of this letter.

707.13 Returned Office Action [R-6]

Office actions are sometimes returned to the Office because the United States Postal Service has not been able to deliver them. Upon receipt of the returned Office action, the Technology Center (TC) technical support staff will check the application file record to ensure that the Office action was mailed to the correct correspondence address. If the Office action was not mailed to the correct correspondence address, it should be stamped "remailed" with the remailing date and mailed to the correct correspondence address. The period running against the application begins with the date of remailing. If the Office action was mailed to the correct correspondence address and it was addressed to an attorney or agent, a letter **>along with a copy of the Office action may be sent to the first named inventor or assignee (if available)< informing him or her of the returned action. **>The time period for reply to the Office action will be restarted to run from the mailing date of the letter informing applicant of the returned action.

/Merilyn S. Watts/
Technical Operation Review Program Manager
Office of Patent Examination Support Services
(571) 272-4398

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/141,378	09/25/2018	Glenn Coleman	LCOM_ENT_CLOUD_US01	2440

158266 7590 09/09/2020

Condo Roccia Koptiw LLP
1800 JFK Boulevard
Suite 1700
Philadelphia, PA 19103

EXAMINER	
KORSAK, OLEG	

ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
09/09/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 16/141,378	Applicant(s) Coleman et al.	
	Examiner OLEG KORSAK	Art Unit 2492	AIA (FITF) Status Yes

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 08/14/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-17 and 19-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-17 and 19-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This action is in response to amendment filed August 14, 2020 for the application # 16/141,378 filed on September 25, 2018. Claims 1-17, 19 and 20 are pending and are directed toward NETWORK ISOLATION WITH CLOUD NETWORKS.

Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Response to Arguments

Applicant's arguments with regards to claims 1-17, 19 and 20 have been fully considered, but they are moot because of new grounds of rejection. Further to keep the record clear, Examiner is responding to "not associated" argument:

"is not associated" **argument** – Applicant argues that the cited portion states that the virtual machine environment uses a virtual guest OS that is not associated with a host OS architecture. In fact, Hoy states that the virtual guest OS is separate. (Hoy at para. [0026]) Thus, Hoy fails to teach or suggest implementing an "isolated computing environment using an

operating system associated with the hosting computing system and comprising a sandboxed computing environment...," as recited in claim 1 (REMARKS, pages 8-9).

Response: According to cited by Applicant [0026] of Hoy "The browser is activated by a desk-top shortcut or application on the host system that allows the user to link to the isolated Internet access of the virtual guest system by launching the virtual guest web browser, which operates transparently to the user in the virtual guest system." Therefore at least "isolated computing environment using an operating system associated with the hosting computing system" was explicitly and clearly disclosed by Hoy.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-17, 19 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Hoy et al. (US 2013/0318594 Pub. Date: Nov. 28, 2013) in view of Comodo (Comodo Internet Security Software Version 7.0 User Guide Version 7.0.111114, 579 pages, 2014), hereinafter referred to as Hoy and Comodo respectively.

As per **claim 1**, Hoy teaches a host computer system comprising: a memory; and a processor (*a computerized work station comprises a computer operatively connected with one or*

more user-accessible data entry devices, a display device viewable by the user, and computer-accessible data storage, Hoy, [0022]) configured to:

implement a workspace, wherein the workspace is configured to enable operation of a first set of one or more applications or processes via a first memory space (*providing for the computer an operating system and one or more applications programs that run on said operating system, Hoy, [0022]*);

implement an isolated computing environment (*and supporting a virtual computer system operating on the computer. Hoy, [0022]*), the isolated computing environment using an operating system associated with the host computing system and comprising a sandboxed computing environment being configured to enable operation of a second set of one or more applications or processes via a second memory space (*Also operating on the host computer is a hypervisor system that creates a virtual machine environment that is separate from the host computer's operating system. This virtual machine has a virtual guest operating system on which a modified browser is run. Hoy, [0026]*),

wherein the isolated computing environment is configured to access an Internet-based cloud service via at least one application of the second set of one or more applications or processes (*The browser is activated by a desk-top shortcut or application on the host system that allows the user to link to the isolated Internet access of the virtual guest system by launching the virtual guest web browser, which operates transparently to the user in the virtual guest system. Hoy, [0026]*);

isolate the isolated computing environment from the workspace using an internal isolation firewall (*this is accomplished by providing a host computer that is surrounded by a host based firewall. Hoy, [0025]*); and

communicate with a proxy server in order to access the Internet-based cloud service (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, as above. Hoy, [0073]*), wherein the isolated computing environment is configured to authenticate with an authentication device in order to allow communication between the at least one application and the Internet-based cloud service (*To allow for this, the firewall 11 around the host OS 17 selectively enables the host OS 17 to access the Internet directly through ports 80 or 443, which are otherwise disabled, provided that the websites being accessed are on a white list of predetermined trusted sites with which the host OS 17 is permitted to communicate with. Hoy, [0057]*).

Hoy does **not** use term "sandbox", although teaches that "Because it is exposed to potentially malicious software as it browses the Internet, the virtual guest system browser and its virtual operating system may be a hardened version that is exceptionally resistant to corruption, or it may have enhanced anomaly detection to aid in noting when dangerous data has been encountered by the browser. The virtual guest system also has no connection whatsoever to the LAN, and cannot access any address on the LAN." Which is essentially a definition of sandboxed environment as known in the art. To exclude any doubt a secondary reference by Comodo is provided, which explicitly teaches a sandboxed computing environment (*An innovative sandboxed environment to run programs and browse the Internet isolated from your real computer. Comodo, page 10*). Comodo also explicitly teaches an Internet-based cloud service (*Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo, page 553.* See also *Comodo Cloud - online file storage service. Backup your files to a*

highly secure online storage which can also be mounted as a virtual drive in your system.

Comodo, page 466)

> Hoy in view of Comodo are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Comodo. This would have been desirable Applications and browsers running inside the virtual desktop leave no cookies or history behind on your real system, making it an extremely secure environment for Internet banking and online shopping (Comodo, pages 10-11).

As per **claim 2**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to access the Internet-based cloud service via one or more of a local area network (LAN), a wide area network (WAN), a cellular network, a Wi-Fi network, a digital subscribers line (DSL) network, a cloud computing network, a data center, or a satellite network (*The home system, when the host is "home" on the trusted LAN network, is allowed by the HBFW to communicate to other LAN resources as well as any whitelisted sites outside the LAN on the Internet. Hoy, [0062]*).

As per **claim 3**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the Internet-based cloud service comprises one or more of an Infrastructure as a Service (IaaS), a Software as a Service (SaaS), or a Platform as a Service (PaaS) (*through Comodo's proprietary Directory Services Platform, Comodo, page 17*).

As per **claim 4**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to select the proxy server from a plurality of proxy servers, the plurality of proxy servers comprising one or more of an Internet-based proxy server or a local network-based proxy server (*A proxy/web-content filter 4 is connected with and cooperates with the firewall hardware 3 to control the type of data permitted to pass from the Internet 5 into the local system 1, filtering e.g., pornographic material or data not intended for the system 1, and*

also blocks communications from users on the LAN trying to reach disallowed sites, e.g., requests to access www.onlinecasino.com. Hoy, [0038]).

As per **claim 5**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to determine whether to send web traffic to a local network-based proxy server or an Internet-based proxy server based on a location of the host computer system (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, Hoy, [0073]*).

As per **claim 6**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to determine whether to send web traffic to a local network-based proxy server or an Internet-based proxy server based on an identity of a network to which the host computer system is connected (*Proxy content filter 4 may optionally be used to screen undesirable or inappropriate incoming or outgoing data, Hoy, [0073]*).

As per **claim 7**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the processor is configured to determine whether to send web traffic to a local network-based proxy server or an Internet-based proxy server based on an identity of the at least one application running in the isolated computing environment (*The virtual guest system 13 shows no software installed except for a browser and possibly some related supportive software, such as Adobe or Windows Media Player that cooperate with the browser when certain types of files are accessed on the Internet, and potentially an email program such as Microsoft Outlook for certain configurations. Hoy, [0048]*).

As per **claim 8**, Hoy in view of Comodo teaches the host computer system of claim 1, wherein the internal isolation firewall is configured to segregate the first memory space from the second memory space and is configured to enforce policies for communication between the first

memory space and the second memory space using the internal isolation firewall (*The guest computer and the host computer communicate with each other by a limited permissible internal host-based firewall in the host system that is provided by the hypervisor or some other local program. Communications across this internal firewall between the guest system and the host system are limited to cut and paste of displayed documents or files, commands to print documents, and file transfer requested manually by the host, Hoy, [0030]*).

As per **claim 9**, Hoy in view of Comodo teaches the host computer system of claim 8, wherein the internal isolation firewall is further configured to generate a message to prompt a user of the host computer system, the message indicating whether to allow communication between the first memory space and the second memory space (*i.e., directed intentionally by the human user of the given system. Hoy, [0030]*).

Claims 10, 11 and 14-20 have limitations similar to those treated in the above rejection, and are met by the references as discussed above, and are rejected for the same reasons of obviousness as used above. In regards to **claim 10**, "a server" is taught by Hoy (*A host computer supports a virtual guest system running thereon. ABSTRACT*), and by Comodo (*The Virtual Desktop creates a folder Shared Space in the location "C:\Documents and Settings\All Users\Application Data\Shared Space". The 'Shared Space' folder can be shared by your host operating system and the Virtual Desktop. Page 223*).

As per **claim 12**, Hoy in view of Comodo teaches the cloud computing system of claim 11, wherein the proxy comprises is a first proxy, and the server is configured to determine whether to send traffic to the first proxy or a second proxy, (*Proxy and Host Settings - Allows you to select the host from which updates are downloaded. By default, CIS will directly download updates from Comodo servers. However, advanced users and network admins may*

wish to first download updates to a proxy/staging server and have individual CIS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CIS at this proxy/staging server. Comodo, page 259).

> Hoy in view of Comodo are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Comodo. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved (Comodo, page 259).

As per **claim 13**, Hoy in view of Comodo teaches the cloud computing system of claim 12, wherein the server is configured to determine whether to send traffic to the first proxy or the second proxy based on user-provided credentials (*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. Comodo, page 260*).

> Hoy in view of Comodo are analogous art to the claimed invention, because they are from a similar field of endeavor of systems, components and methodologies for providing secure communication between computer systems. It would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention to modify Hoy in view of Comodo. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved (Comodo, page 259).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or

improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely

online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-17, 19 and 20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10554475, and over claims 1-20 of U.S. Patent No. 10558798. Although the claims at issue are not identical, they are not patentably distinct from each other because all elements of claims 1-17, 19 and 20 of the instant application correspond to elements of claims 1-20 of the cited patents. The above claims of the present application would have been obvious over claims of the U.S. Patent No. 10554475, and over claims of U.S. Patent No. 10558798 because each element of the claims of the present application is anticipated by the claims of the U.S. Patent No. 10554475, and the claims of U.S. Patent No. 10558798 and as such are unpatentable for obviousness-type double patenting (*In re Goodman* (CAFC) 29 USPQ2D 2010 (12/3/1993)).

Claims 1-17, 19 and 20 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of copending Applications No. 16/059381, 16/109275, 16/141,535, 16/138,696, 16/144,609, 16/144,761, 16/146,149, 16/142,810, 16/146,490, 16/163,796, 16/163,884, and 16/164,342. Although the claims at issue are not identical, they are not patentably distinct from each other because each element of the claims of the present application is anticipated by the claims of cited applications and as such are unpatentable for obviousness-type double patenting (*In re Goodman* (CAFC) 29 USPQ2D 2010 (12/3/1993)).

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OLEG KORSAK whose telephone number is (571)270-1938. The examiner can normally be reached on 5:00 AM- 4:00 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, SALEH NAJJAR can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OLEG KORSAK/
Primary Examiner, Art Unit 2492

Notice of References Cited	Application/Control No. 16/141,378	Applicant(s)/Patent Under Reexamination Coleman et al.	
	Examiner OLEG KORSAK	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
	A					
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

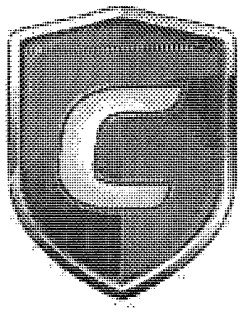
*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Comodo (Comodo Internet Security Software Version 7.0 User Guide Version 7.0.111114, 579 pages, 2014) (Year: 2014)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

COMODO
Creating Trust Online®



Comodo
Internet Security
Software Version 7.0

User Guide
Guide Version 7.0.111114

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

Table of Contents

1.Introduction to Comodo Internet Security....6
1.1.Special Features....10
1.2.System Requirements....14
1.3.Installation....14
1.3.1.CIS Premium - Installation....14
1.3.2.CIS Pro - Installation and Activation....31
1.3.3.CIS Complete - Installation and Activation....45
1.3.4.Activating CIS Pro/Complete Services after Installation....60
1.3.4.1.Activating Your License....60
1.3.4.2.Activating Your Guarantee Coverage....67
1.3.4.3.Renewal of Your License....70
1.4.Starting Comodo Internet Security....71
1.5.The Main Interface....73
1.5.1.The Home Screen....75
1.5.2.The Tasks Interface....85
1.5.3.The Widget....86
1.5.4.The System Tray Icon....87
1.6.Understanding Security Alerts....89
2.General Tasks - Introduction....108
2.1.Scan and Clean Your Computer....108
2.1.1.Run a Quick Scan....110
2.1.2.Run a Full Computer Scan....114
2.1.3.Run a Rating Scan....119
2.1.4.Run a Custom Scan....124
2.1.4.1.Scan a Folder....124
2.1.4.2.Scan a File....128
2.1.4.3.Create, Schedule and Run a Custom Scan....131
2.2.Instantly Scan Files and Folders....139
2.3.Processing Infected Files....144
2.4.Manage Virus Database and Program Updates....149
2.5.Manage Quarantined Items....152
2.6.View CIS Logs....156
2.6.1.Antivirus Logs....158
2.6.1.1.Filtering Antivirus Logs....159
2.6.2.Firewall Logs....163
2.6.2.1.Filtering Firewall Logs....165
2.6.3.Defense+ Logs....171
2.6.3.1.Filtering Defense+ Logs....172
2.6.4.'Website Filtering' Logs....176
2.6.4.1.Filtering 'Website Filtering' Logs....177
2.6.5.'Alerts' Logs....180
2.6.5.1.Filtering 'Alerts Displayed' Logs....181
2.6.6.Tasks....187
2.6.6.1.Filtering 'Tasks Launched' Logs....187

2.6.7.Configuration Changes....191
2.6.7.1.Filtering 'Configuration Changes' Logs....193
2.7.Get Live Support....197
2.8.View Active Internet Connections....197
2.9.View Active Process List....201
3.Firewall Tasks - Introduction....204
3.1.Allow or Block Internet Access to Applications Selectively....205
3.2.Stealth your Computer Ports....206
3.3.Manage Network Connections....208
3.4.Stop all Network Activities....209
3.5.Advanced Firewall Settings....209
4.Sandbox Tasks - Introduction....211
4.1.The Virtual Desktop....212
4.1.1.Starting the Virtual Desktop....213
4.1.2.The Main Interface....215
4.1.3.Running Browsers inside the Virtual Desktop....220
4.1.4.Opening Files and Running Applications inside the Virtual Desktop....221
4.1.5.Configuring the Virtual Desktop....222
4.1.6.Closing the Virtual Desktop....223
4.2.Run an Application in the Sandbox....224
4.3.Reset the Sandbox....228
5.Advanced Tasks - Introduction....230
5.1.Create a Rescue Disk....231
5.1.1.Downloading and Burning Comodo Rescue Disk....233
5.2.Remove Deeply Hidden Malware....237
5.3.Submit Files....240
5.4.Identify and Kill Unsafe Running Processes....242
5.5.Manage CIS Tasks....245
6.Advanced Settings....249
6.1.General Settings....251
6.1.1.Customize User Interface....251
6.1.2.Configure Program and Virus Database Updates....256
6.1.3.Log Settings....259
6.1.4.Manage CIS Configurations....261
6.1.4.1.Comodo Preset Configurations....261
6.1.4.2.Importing/Exporting and Managing Personal Configurations....262
6.2.Security Settings....270
6.2.1.Antivirus Settings....271
6.2.1.1.Real-time Scanner Settings....271
6.2.1.2.Scan Profiles....274
6.2.1.3.Exclusions....283
6.2.2.Defense+ Settings....300
6.2.2.1.HIPS Behavior Settings....301
6.2.2.2.Active HIPS Rules....307
6.2.2.3.HIPS Rule Sets....315
6.2.2.4.Protected Objects....318

6.2.2.4.1.Protected Files....319
6.2.2.4.2.Blocked Files....327
6.2.2.4.3.Protected Registry Keys....329
6.2.2.4.4.Protected COM Interfaces....335
6.2.2.4.5.Protected Data Folders....340
6.2.2.5.Behavior Blocker....343
6.2.2.5.1.The Sandbox - An Overview....349
6.2.2.5.2.Unknown Files: The Auto-Sandboxing and Scanning Processes....350
6.2.2.6.Configure the Sandbox....352
6.2.3.Firewall Settings....363
6.2.3.1.Firewall Behavior Settings....364
6.2.3.2.Application Rules....369
6.2.3.3.Global Rules....383
6.2.3.4.Firewall Rule Sets....385
6.2.3.5.Network Zones....388
6.2.3.5.1.Network Zones....389
6.2.3.5.2.Blocked Zones....394
6.2.3.6.Port Sets....398
6.2.3.7.Website Filtering....402
6.2.3.7.1.Creating and Modifying Website Filtering Rules....403
6.2.3.7.2.Defining or Modifying Website Categories....413
6.2.4.Manage File Rating....420
6.2.4.1.File Rating Settings....421
6.2.4.2.Trusted Files....422
6.2.4.3.Unrecognized Files....424
6.2.4.4.Submitted Files....429
6.2.4.5.Trusted Vendors List....431
7.Comodo GeekBuddy....436
7.1.Overview of Services....437
7.2.Activation of Service....437
7.3.Launching the Client and Using the Service....441
7.4.Accepting Remote Desktop Requests....444
7.5.Chat History....446
7.6.Using Issue Tracker....448
7.7.Uninstalling Comodo GeekBuddy....452
8.TrustConnect Overview....453
9.Comodo Dragon....457
9.1.Introduction to PrivDog....459
9.1.1.Using PrivDog....459
9.1.2.PrivDog Settings Configuration....460
9.1.3.Threats....461
9.1.4.Exceptions....462
9.1.5.Preferences....463
10.Comodo BackUp....463
Appendix 1 - CIS How to... Tutorials....466
Enable / Disable AV, Firewall and Auto-Sandbox Easily....467

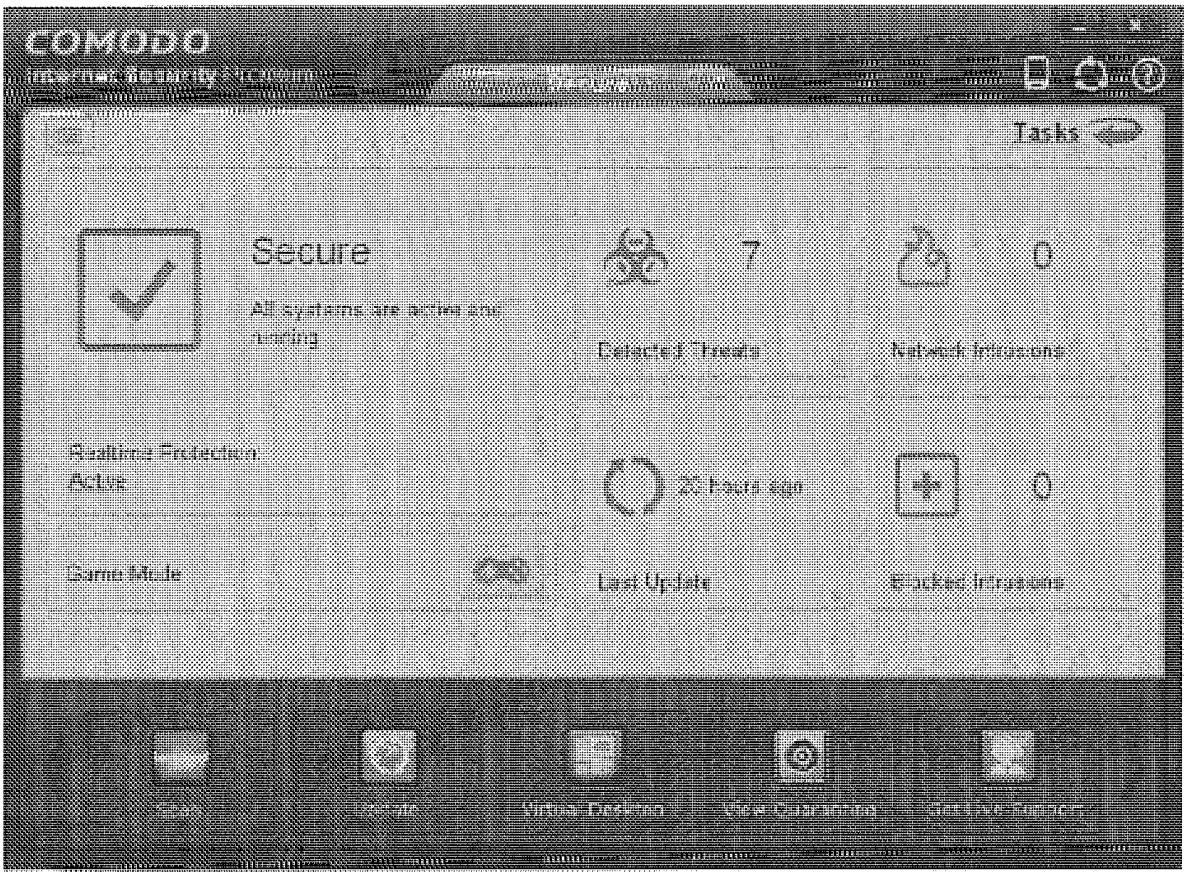
Set up the Firewall For Maximum Security and Usability 468
Block Internet Access while Allowing Local Area Network (LAN) Access 477
Block/allow Websites Selectively to Users of Your Computer 483
Set up the HIPS for Maximum Security and Usability 492
Set up the Behavior Blocker for Maximum Security and Usability 495
Password Protect Your CIS Settings 497
Reset Forgotten Password (Advanced) 499
Run an Instant Antivirus Scan on Selected Items 502
Create an Antivirus Scanning Schedule 507
Run Untrusted Programs in the Sandbox 513
Run Browsers Inside Sandbox 516
Run Untrusted Programs Inside Virtual Desktop 517
Run Browsers Inside the Virtual Desktop 519
Restore Incorrectly Quarantined Item(s) 521
Submit Quarantined Items to Comodo for Analysis 523
Enable File Sharing Applications like BitTorrent and Emule 526
Block any Downloads of a Specific File Type 532
Disable Behavior Blocker and Auto-Sandboxing on a Per-application Basis 535
Switch Between Complete CIS Suite and Individual Components (just AV or FW) 537
Switch Off Automatic Antivirus and Software Updates 541
Suppress CIS Alerts Temporarily while Playing Games 545
Renew or Upgrade your License 546
How to use CIS Protocol Handlers 548
Appendix 2 - Comodo Secure DNS Service 551
Router - Manually Enabling or Disabling Comodo Secure DNS Service 551
Windows XP - Manually Enabling or Disabling Comodo Secure DNS Service 553
Windows 7 / Vista - Manually Enabling or Disabling Comodo Secure DNS Service 557
Appendix 3 - Glossary Of Terms 563
Appendix 4 – CIS Versions 576
About Comodo 577

1. Introduction to Comodo Internet Security

Overview

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

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



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

Comodo Internet Security - Key Features:

- **Antivirus** - Proactive antivirus engine that automatically detects and eliminates viruses, worms and other malware. Apart from the powerful on-demand, on-access and scheduled scan capabilities, CIS users can now simply drag-and-drop items onto the home screen to run an instant virus scan.
- **Firewall** - Highly configurable packet filtering firewall that constantly defends your system from inbound and outbound Internet attacks.
- **Defense+** - A collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.
    - **Behavior Blocker** - Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be

auto-sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data.

- **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.
- **Viruscope** - Monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Using a system of behavior 'recognizers', Viruscope not only detects unauthorized actions but also allows you to completely undo them. Apart from representing another hi-tech layer of protection against malware, this also provides you with the granular power to reverse unwanted actions taken by legitimate software without blocking the software entirely.

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

Guide Structure

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

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

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

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

- Exclusions
- Defense+ Settings
  - HIPS Behavior Settings
  - Active HIPS Rules
  - HIPS Rule Sets
  - Protected Objects
  - Behavior Blocker
    - The Sandbox - An Overview
    - Unknown Files: The Sand-boxing and Scanning Processes
  - Configure the Sandbox
- Firewall Settings
  - Firewall Behavior Settings
  - Application Rules
  - Global Rules
  - Firewall Rule Sets
  - Network Zones
  - Port Sets
  - Website Filtering
- Manage File Rating
  - File Rating Settings
  - Trusted Files
  - Unrecognized Files
  - Submitted Files
  - Trusted Vendors List

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

- Comodo GeekBuddy
  - Overview of Services
  - Activation of Service
  - Launching the Client and Using the Service
  - Accepting Remote Desktop Requests
  - Chat History
  - Using Issue Tracker
  - Uninstalling Comodo GeekBuddy
- TrustConnect Overview
- Comodo Dragon
  - Introduction to PrivDog
- Comodo Backup
- Appendix 1 - CIS How to... Tutorials
  - Enable / Disable AV, Firewall and Auto-Sandbox Easily
  - Set up the Firewall For Maximum Security and Usability
  - Block Internet Access while Allowing Local Area Network (LAN) Access
  - Block/allow Websites Selectively to Users of Your Computer
  - Set up the HIPS for Maximum Security and Usability
  - Set up the Behavior Blocker for Maximum Security and Usability
  - Password Protect Your CIS Settings

- Reset Forgotten Password (Advanced)
- Run an Instant Antivirus Scan on Selected Items
- Create an Antivirus Scanning Schedule
- Run Untrusted Programs in the Sandbox
- Run Browsers inside Sandbox
- Run Untrusted Programs inside Virtual Desktop
- Run Browsers inside the Virtual Desktop
- Restore Incorrectly Quarantined Item(s)
- Submit Quarantined Items to Comodo for Analysis
- Enable File Sharing Applications like BitTorrent and Emule
- Block any Downloads of a Specific File Type
- Disable Behavior Blocker and Auto-Sandboxing on a per-application basis
- Switch Between Complete CIS Suite and Individual Components (just AV or FW)
- Switch Off Automatic Antivirus and Software Updates
- Suppres CIS Alerts Temporarily while Playing Games
- Renew or upgrade your License
- How To Use CIS Protocol Handlers

- Appendix 2 - Comodo Secure DNS Service
- Appendix 3 - Glossary of Terms
- Appendix 4 - CIS Versions

1.1. Special Features

Behavior Blocker

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

Host Intrusion Prevention System

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

Virtual Desktop

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

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

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

Advanced Network Firewall Engine

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

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

Comprehensive Antivirus Protection

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

Intuitive Graphical User Interface

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

Comodo GeekBuddy (Pro, Complete versions only)

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

The services include:

- Virus & Malware Removal
- Internet and Online Identity Security

- Printer or Email Account Setup
- Software Activation
- General PC Troubleshooting
- Computer Power Setting Optimization
- Comodo Software Installation and Set up
- Comodo Account Questions.

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

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

Comodo TrustConnect

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

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

Comodo Backup

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

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

Comodo Dragon

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

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

Comodo Internet Security - Extended Features

Highly Configurable Security Rules Interface

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

Application Behavior Analysis

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

Cloud Based Behavior Analysis

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

Viruscope

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

Website Filtering

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

Event logging

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

Memory Firewall Integration

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

'Training Mode' and 'Clean PC' Mode

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

Application Recognition Database (Extensive and proprietary application safe list)

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

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

Self Protection against Critical Process Termination

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

Sandboxing as a security feature

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

Submit Suspicious Files to Comodo

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

for all users.

Enhanced Browser Privacy

PrivDog, a new browser extension that can be installed with CIS, improves your online privacy by detecting and blocking any 3rd party trackers or ad networks that are monitoring your activity while on a website. Supported browsers include Comodo Dragon, Comodo Ice Dragon, Google Chrome and Mozilla Firefox.

1.2. System Requirements

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

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

1.3. Installation

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

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

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

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

Click the links below for detailed explanations:

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

1.3.1. CIS Premium - Installation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on

your computer. Click here to read the full note.

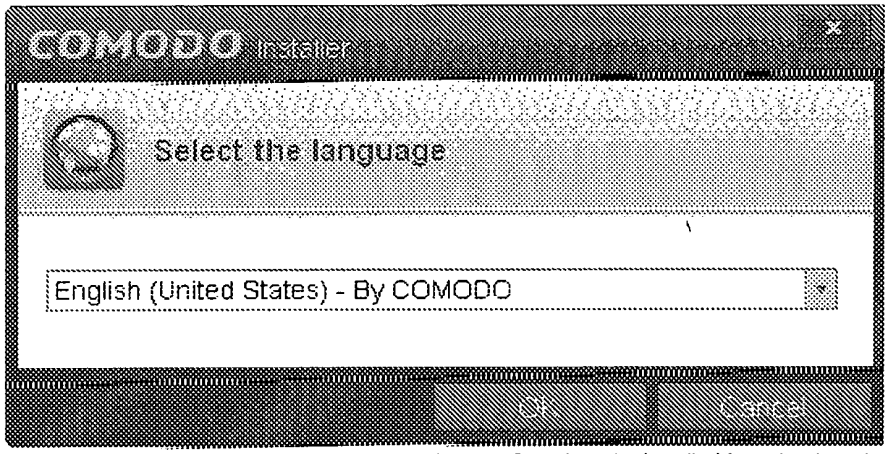
In order to install Comodo Internet Security - Premium, you need to download the setup file from http://www.comodo.com/home/download/download.php?prod=cis.

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

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

Step 1 - Choosing the Interface Language

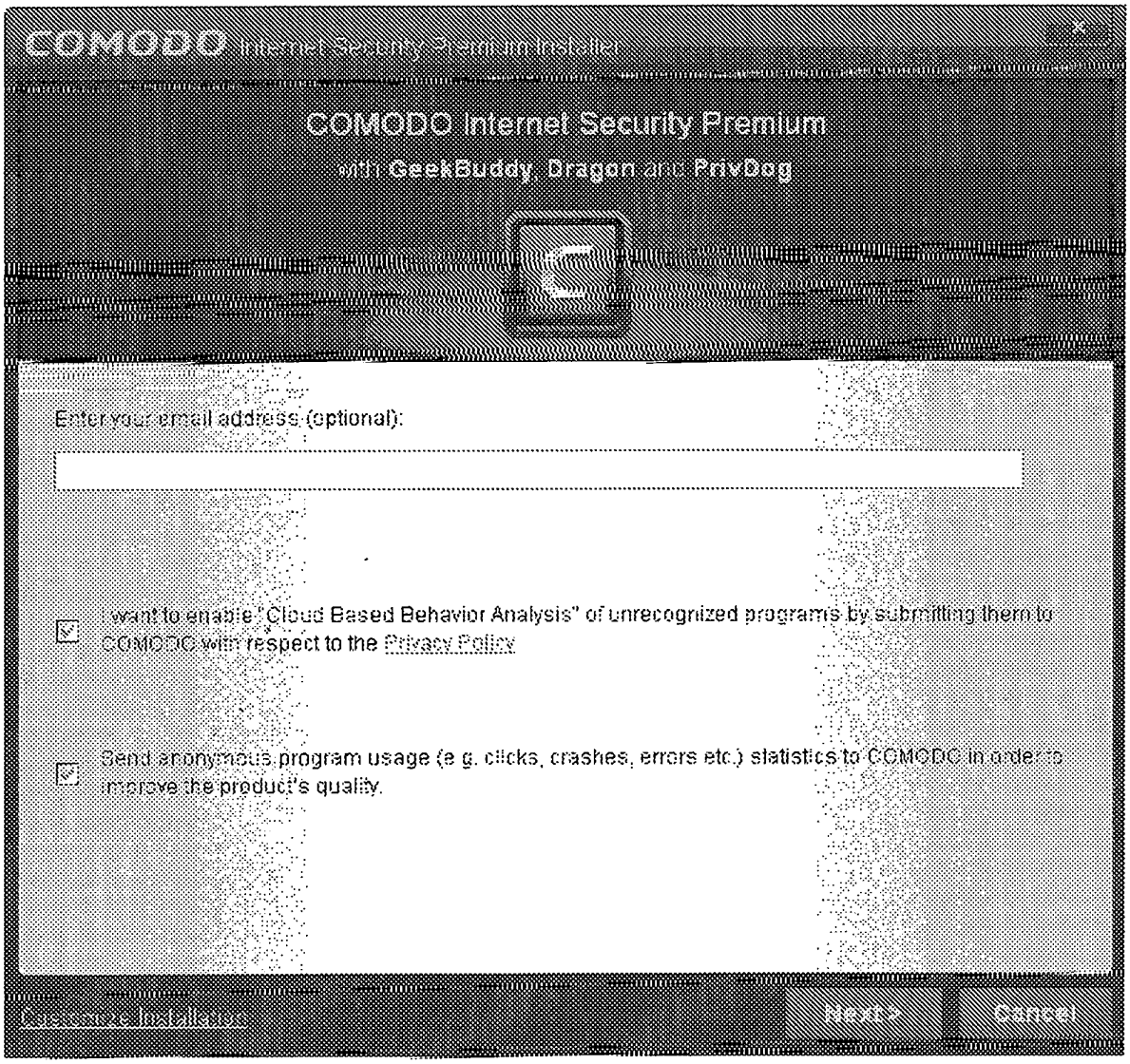
The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



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

Step 2 - Installation Configuration

The installation configuration screen will be displayed.



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

Receive Comodo News and Notifications

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

Cloud Based Behavior Analysis

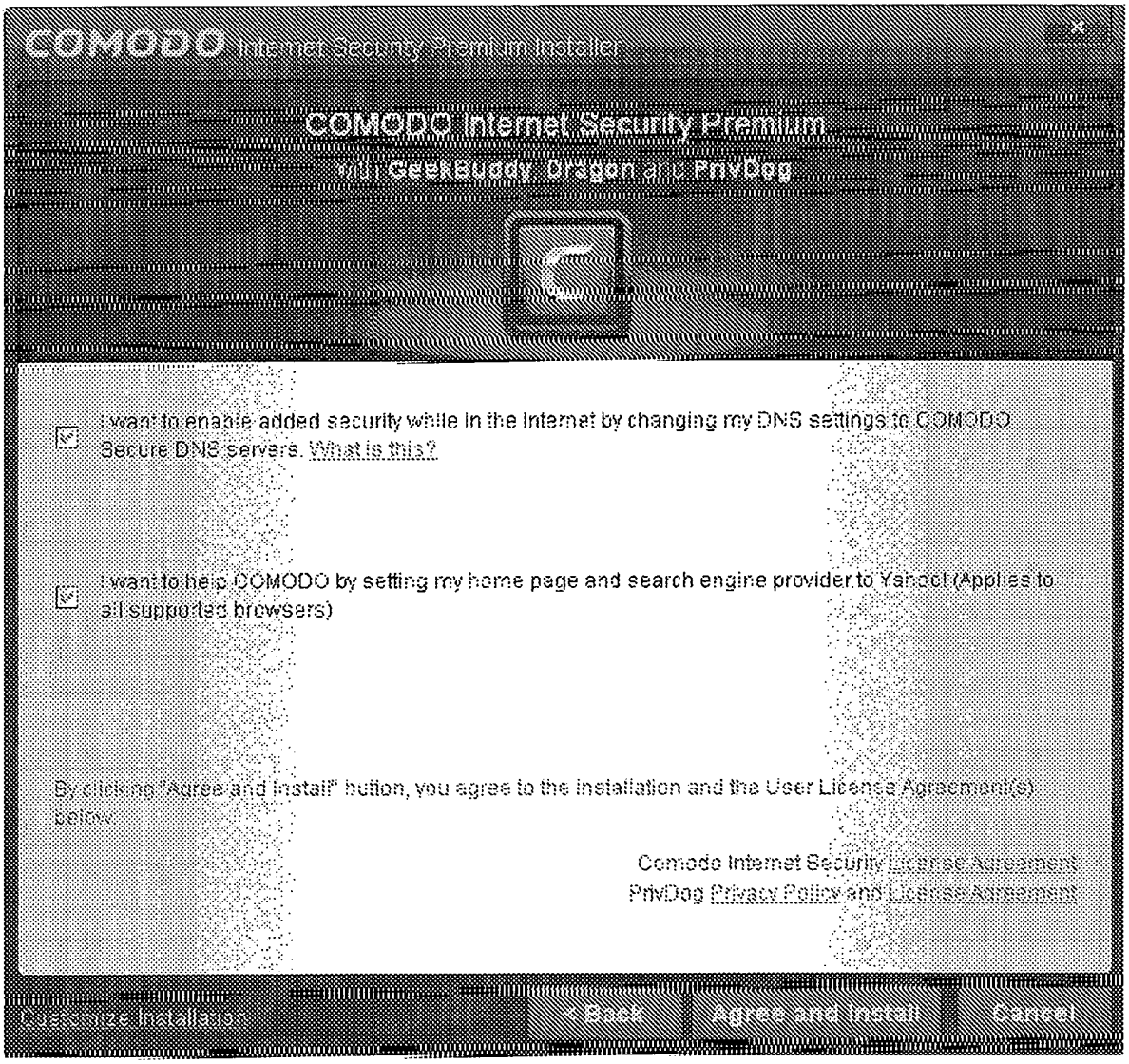
Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer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

Send Program Usage Data

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

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

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



DNS Settings

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

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

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

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

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

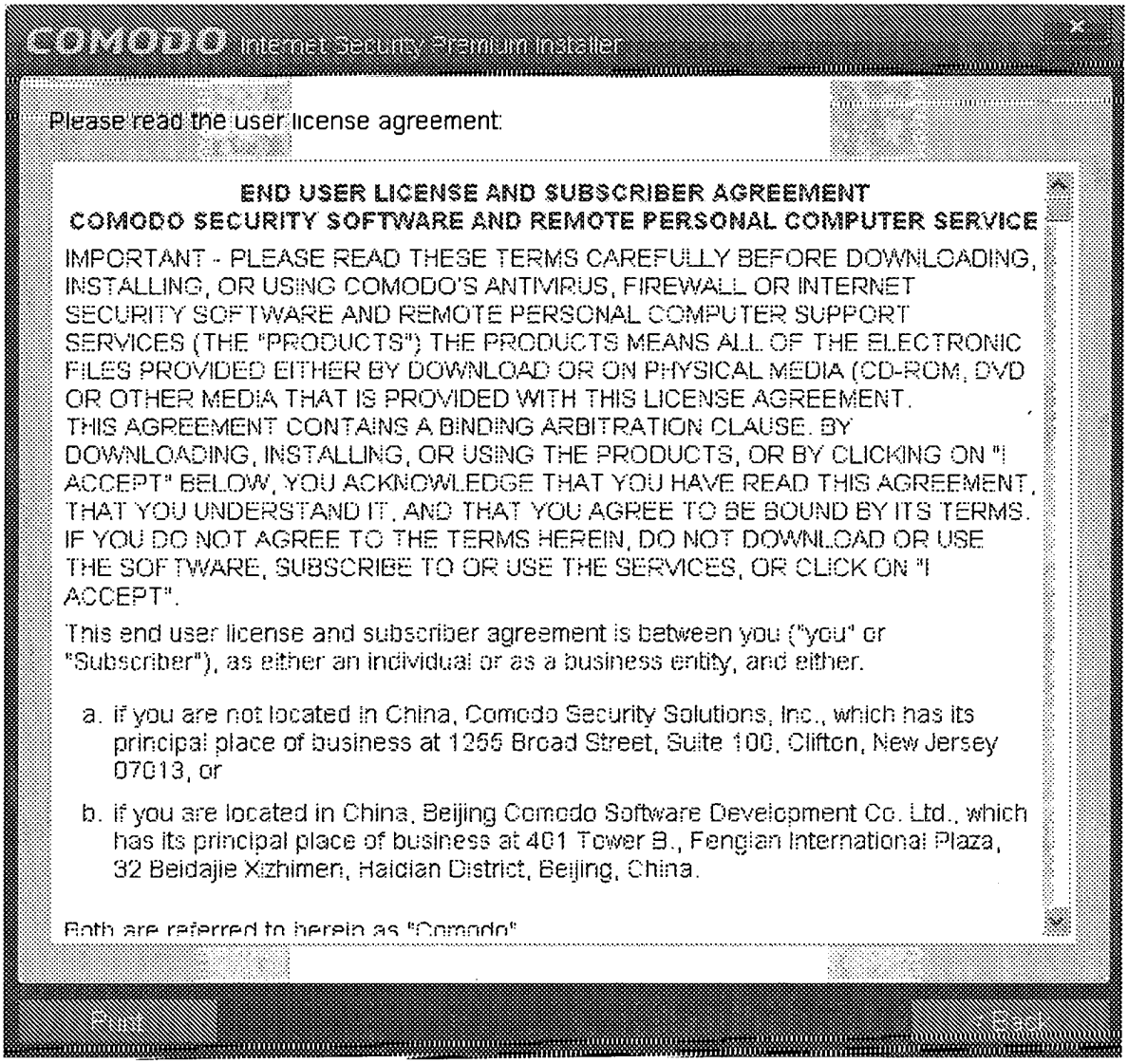
Browser Homepage

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

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

End User License Agreements

- Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.



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

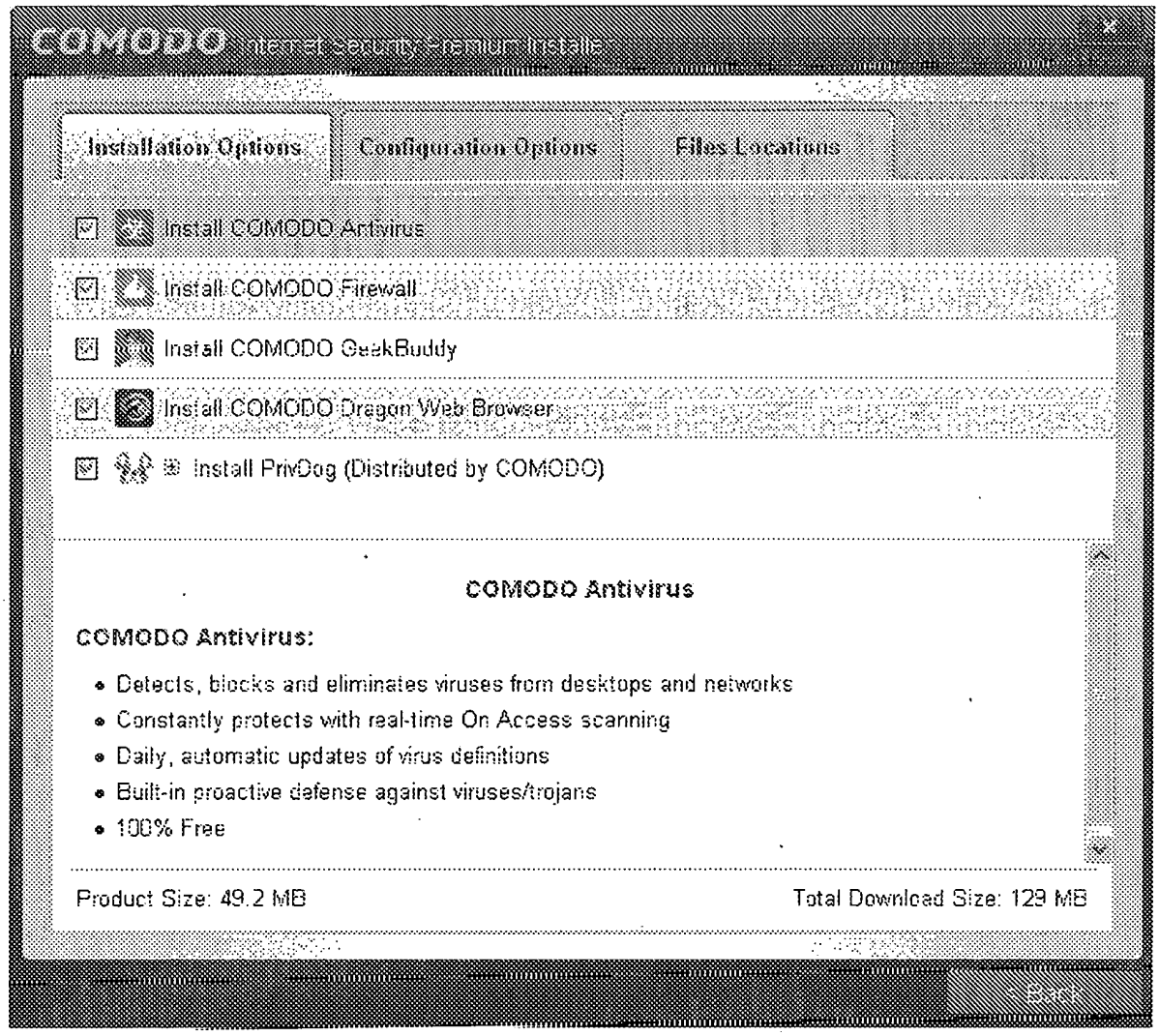
Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installation'. Otherwise, click 'Agree and Install' to begin installation.

Customizing Installation

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

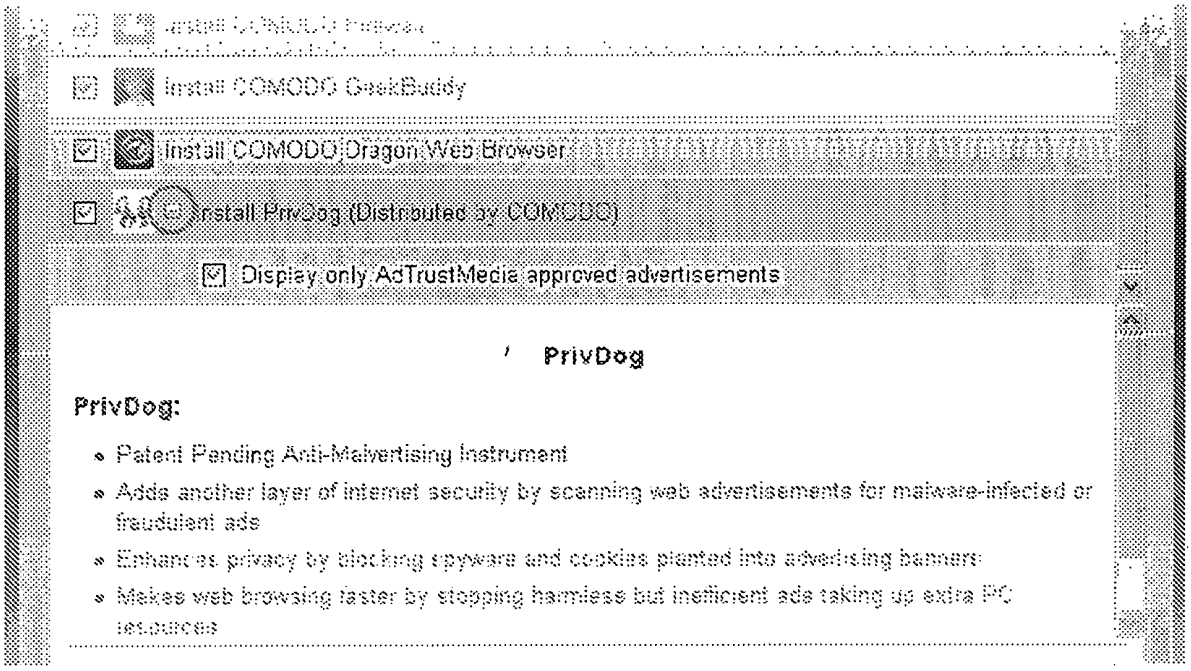
Select Components to Install (Click to go back to Step 2)

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



- **Install COMODO Firewall** - Selecting this option installs Comodo Firewall and Defense+ components. Deselect this option, if you already have third party Firewall protection activated in your computer system. Comodo Firewall installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO Antivirus** - Selecting this option installs Comodo Antivirus and Defense+ components. Deselect this option, if you already have a third party virus protection activated in your computer system. Comodo Antivirus installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- **Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.
- **Install PrivDog** - PrivDog is a browser extension that improves the transparency, privacy and speed of your online experience by automatically detecting and blocking processes that are attempting to track your online activity. Whenever you visit a website, PrivDog will display the number of privacy threats it has blocked in the top-right corner of your browser. Clicking the PrivDog icon will reveal a more detailed breakdown of the types of threats it has stopped, which can include advertising networks, 3rd party trackers, cookies, widgets and other data collection processes. The extension can also block all current banner ads in a webpage and replace them with safe and trusted ads. If you elect to install PrivDog, the extension will be automatically installed in any supported browsers detected on your system (Comodo Dragon, Comodo IceDragon, Google Chrome and Mozilla Firefox). You can remove the extension at any time from within the browser itself. Refer to the section Introduction to PrivDog for more details.

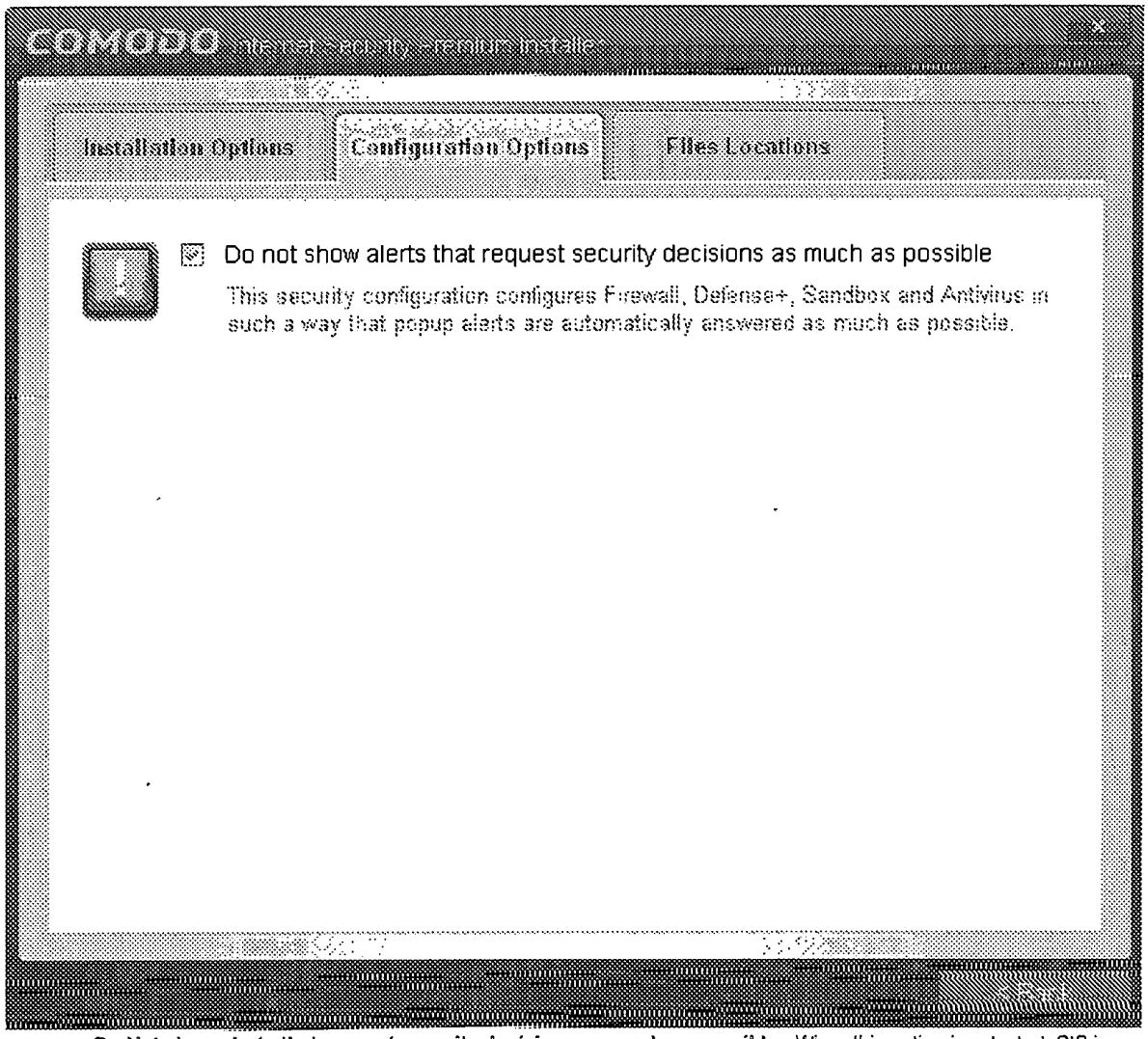
- Select the checkbox 'Install PrivDog' if you want to install PrivDog.



- Click the '+' button beside 'Install PrivDog' and select the 'Display only AdTrustMedia approved advertisements' checkbox, If you choose to view only ads from AdTrustMedia in your browser.

Configuration Options

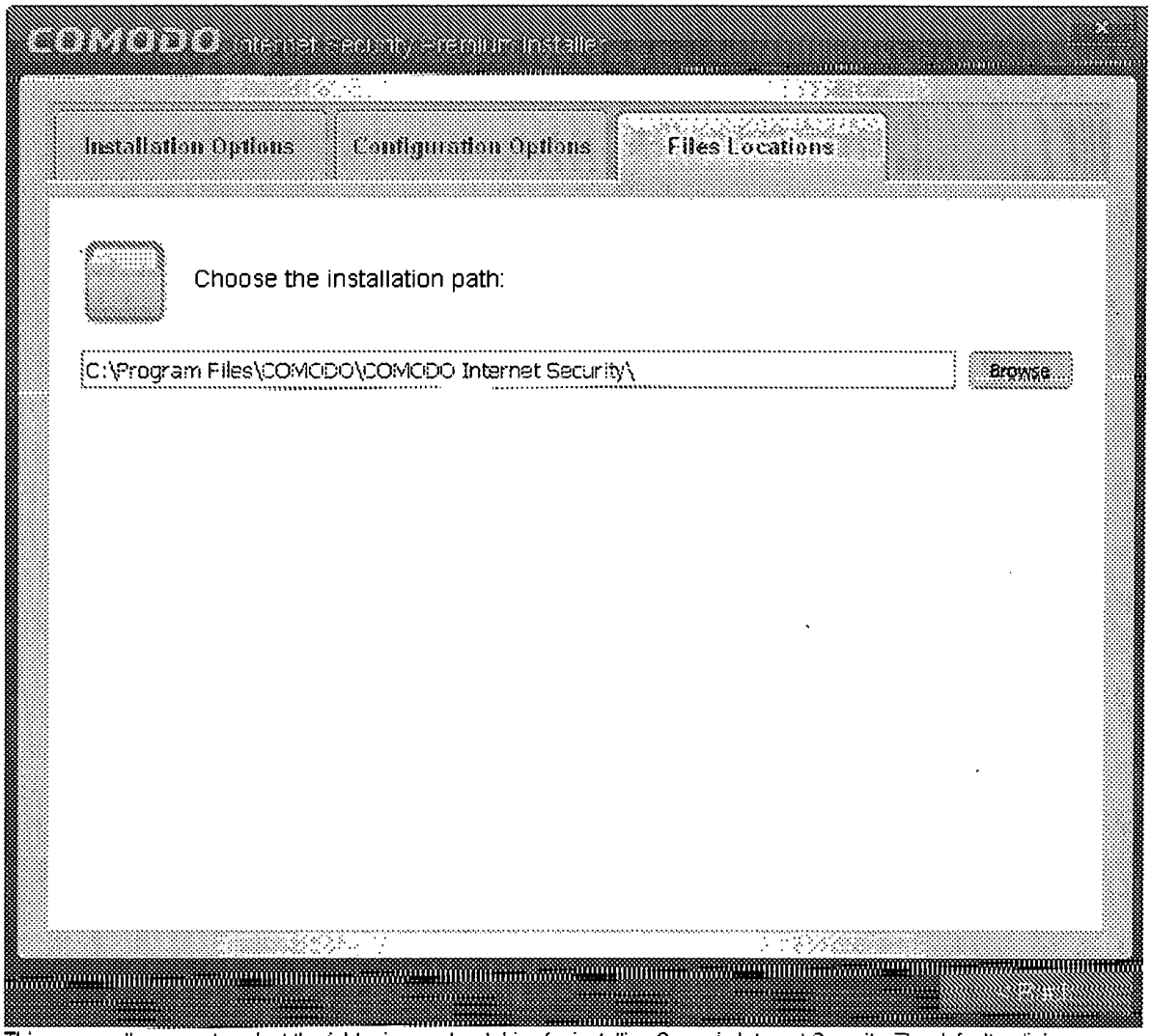
- Click the 'Configuration Options' tab to configure pop-up alert options.



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

Choosing Installation Location

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



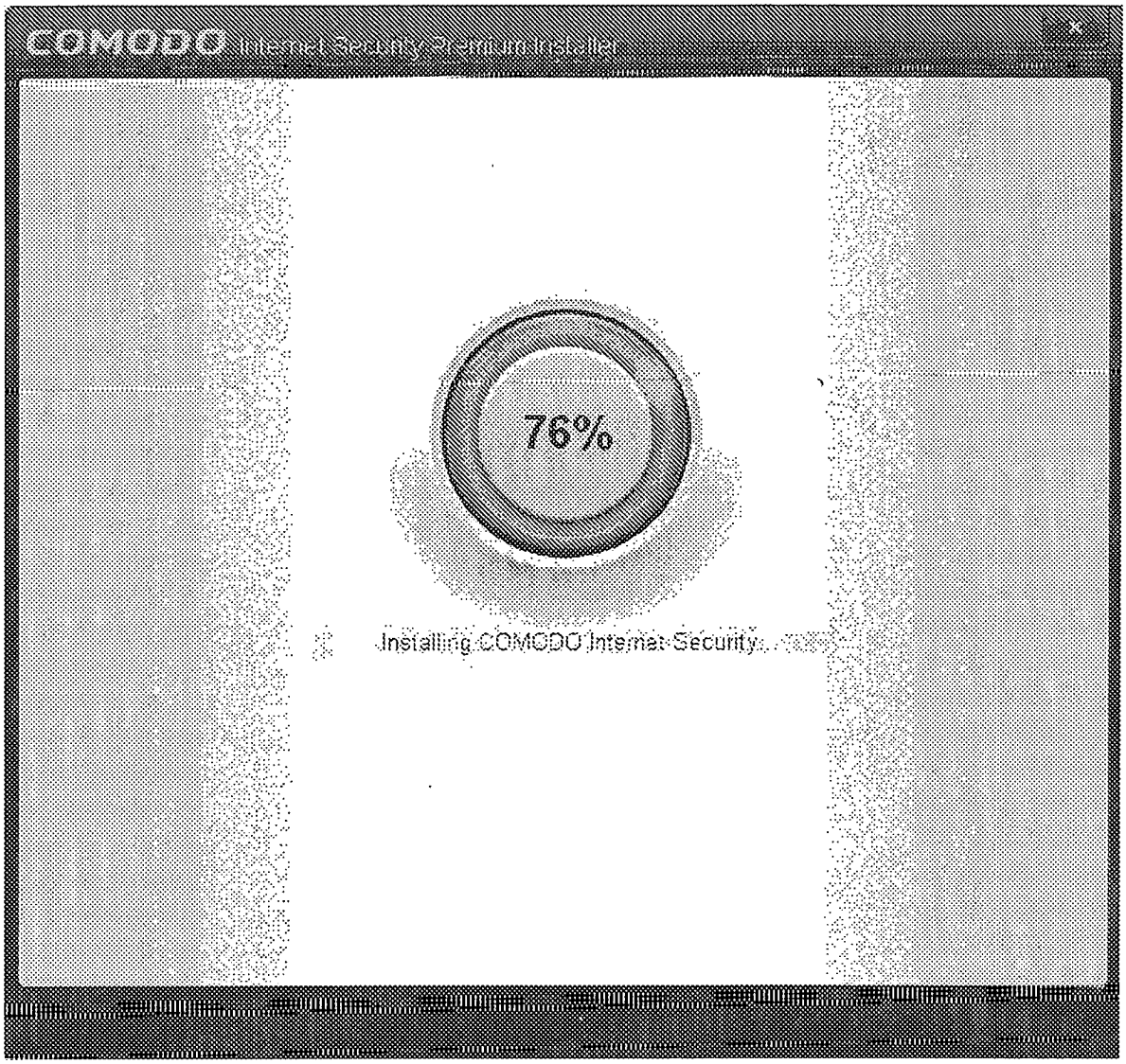
This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

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

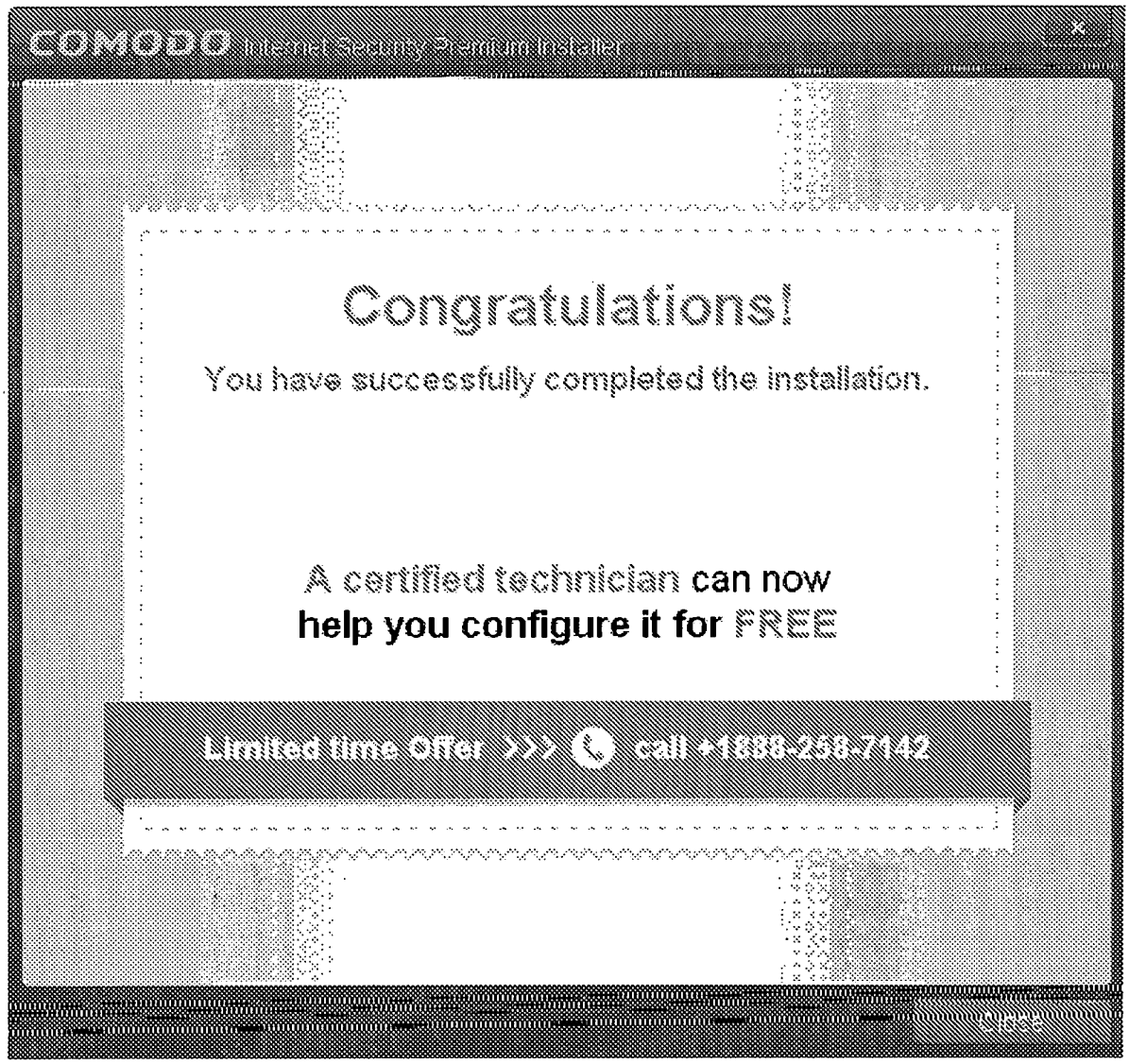
- Once you are satisfied with your settings, click 'Agree and Install' to begin installation (Click to go back to Step 2).

Step 3 - Installation Progress

The installation progress will be displayed...



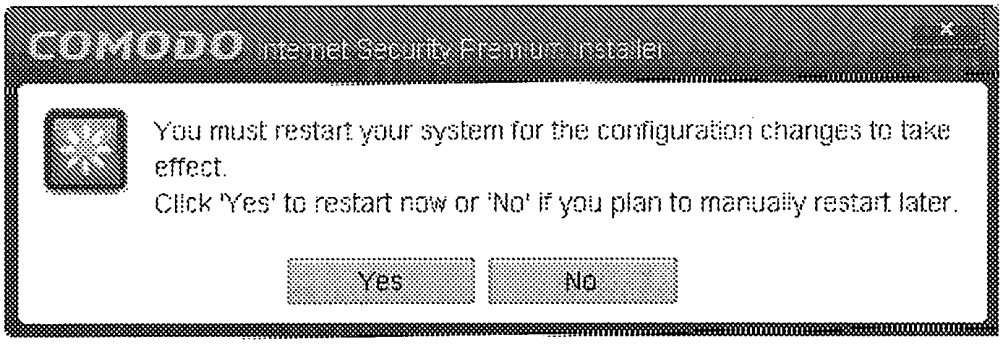
...and on completion, the successfully completed dialog will be displayed.



- Click the 'Close' button.

Step 4 - Restarting Your System

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

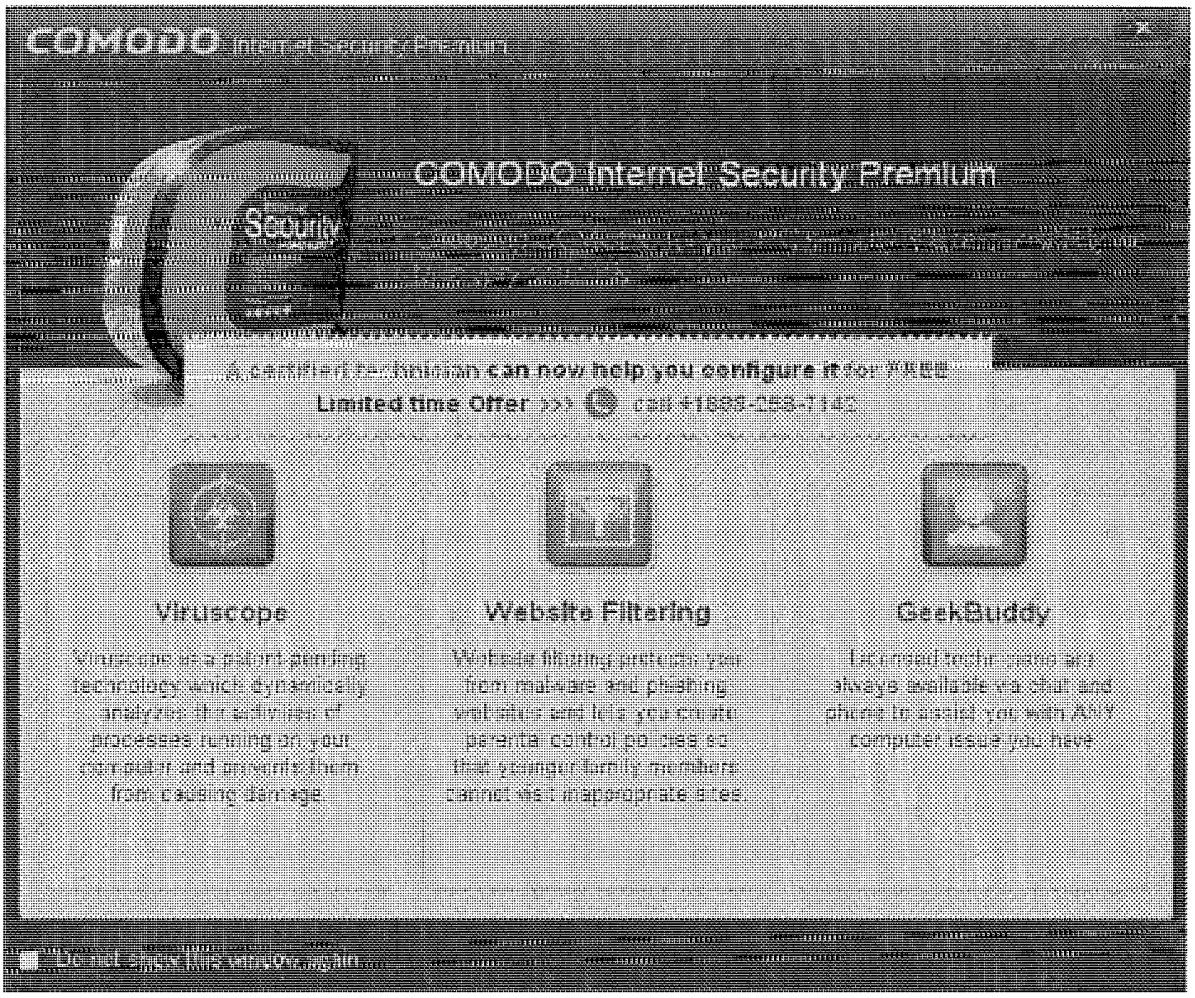


Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

Step 5 - After Restarting Your System

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



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

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

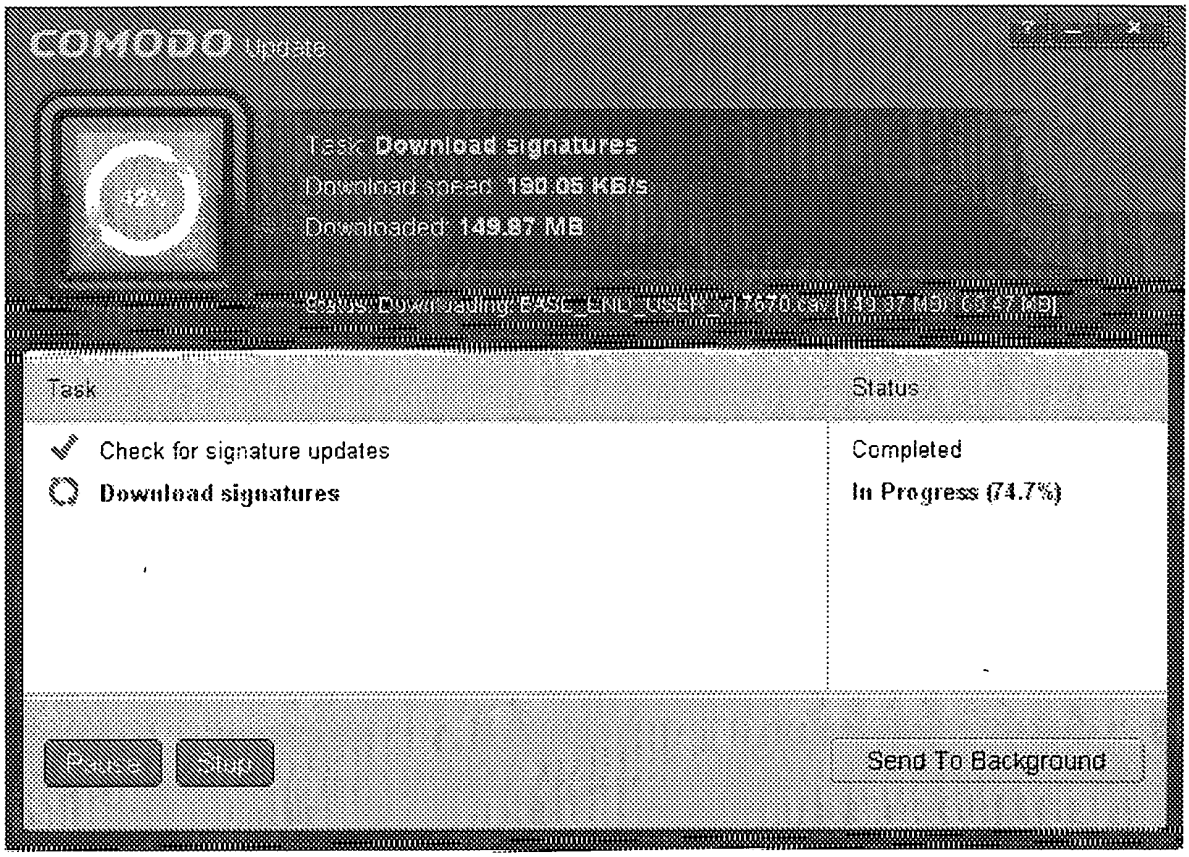


- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

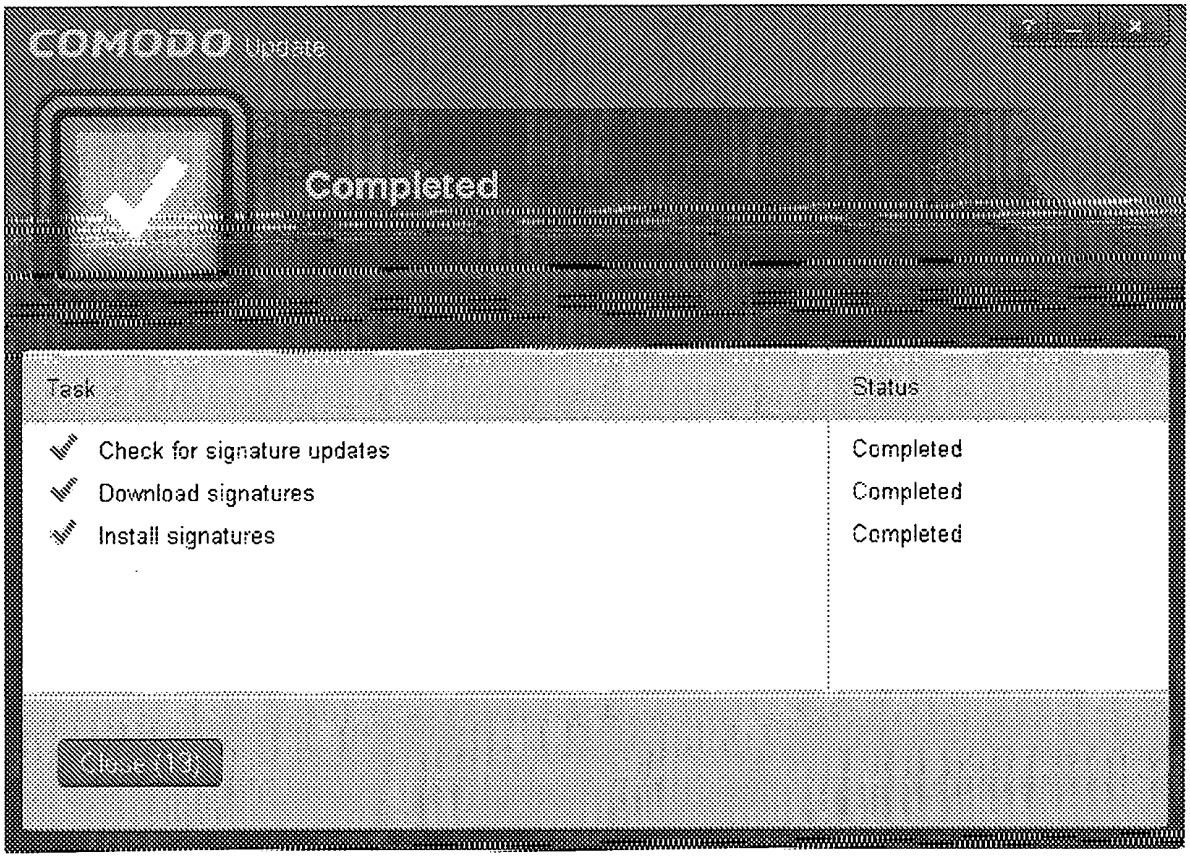
The CIS interface will open.



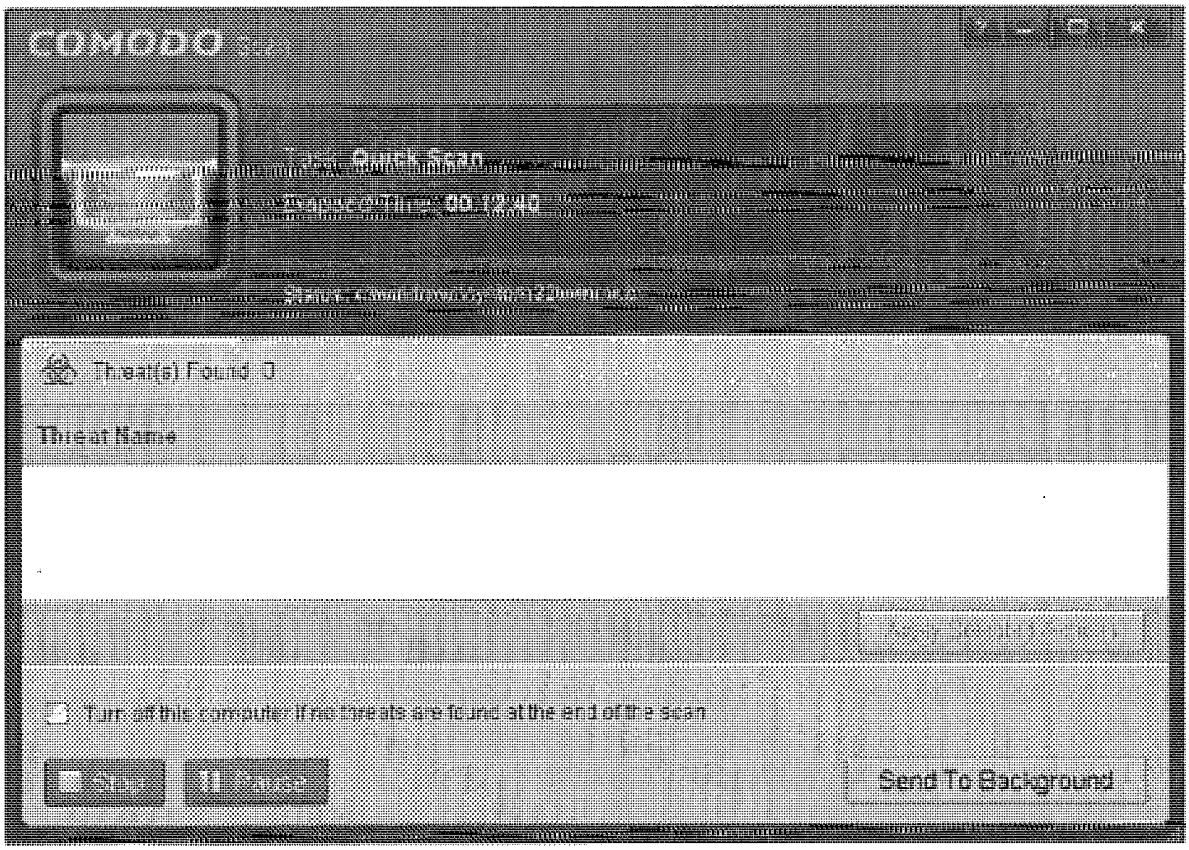
The virus database will be updated automatically for the first time after installation.



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

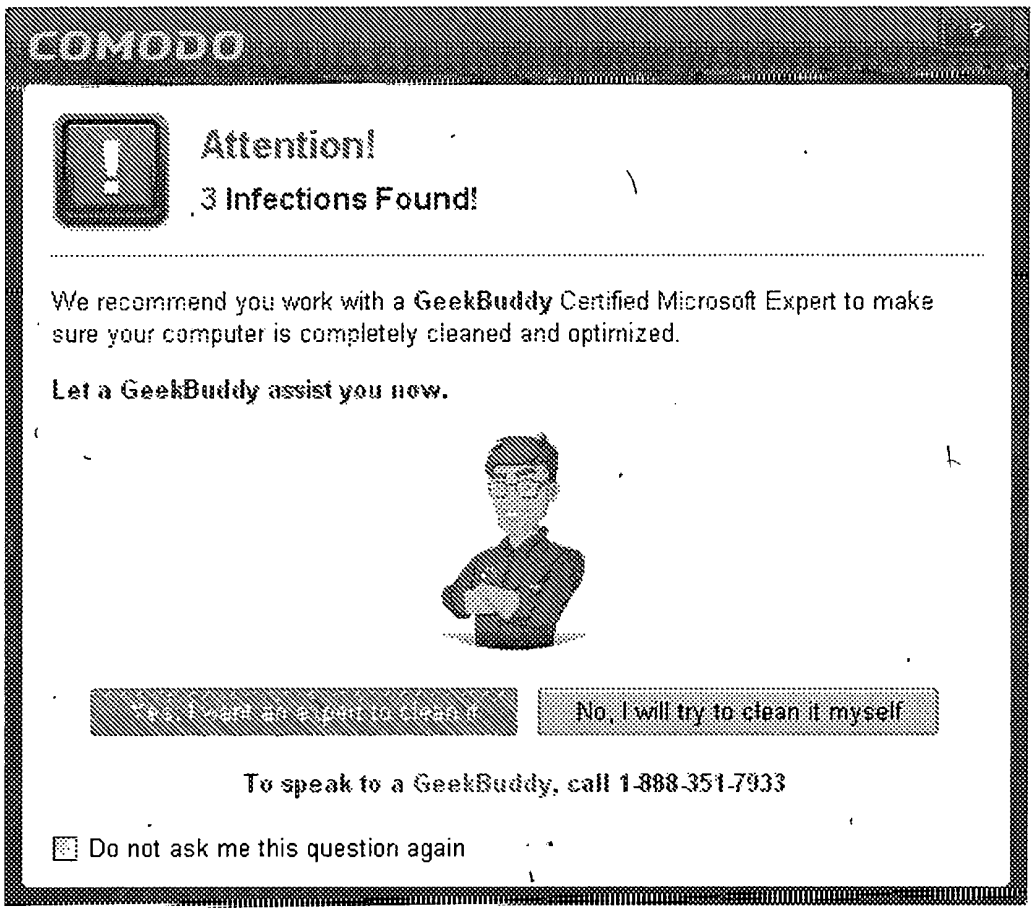


CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



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

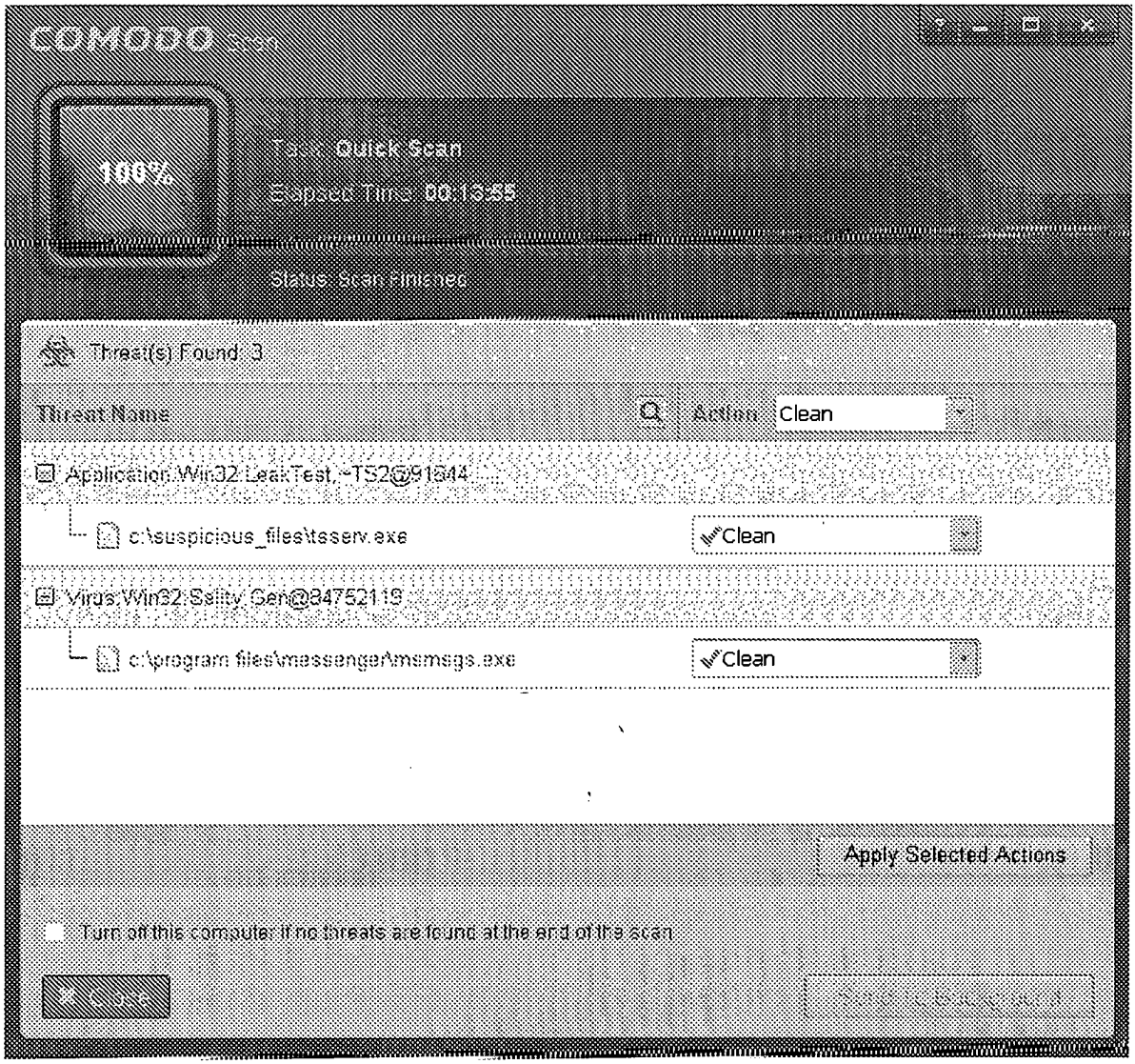
After the scanning is complete, and any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



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

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

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



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

1.3.2. CIS Pro - Installation and Activation

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

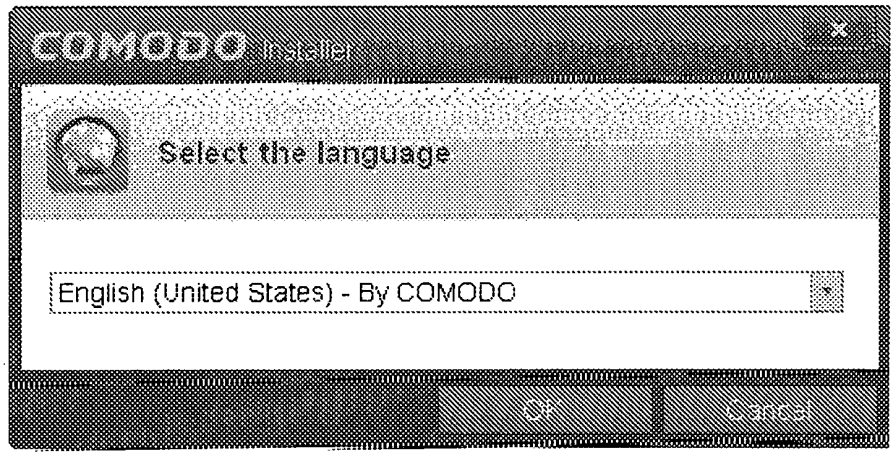
Comodo Internet Security Pro can be downloaded from http://www.comodo.com/home/download/download.php?prod=cis-pro after signing up for subscription and includes, Comodo Dragon, GeekBuddy and the Comodo Guarantee.

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

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

Step 1 - Choosing the Interface Language

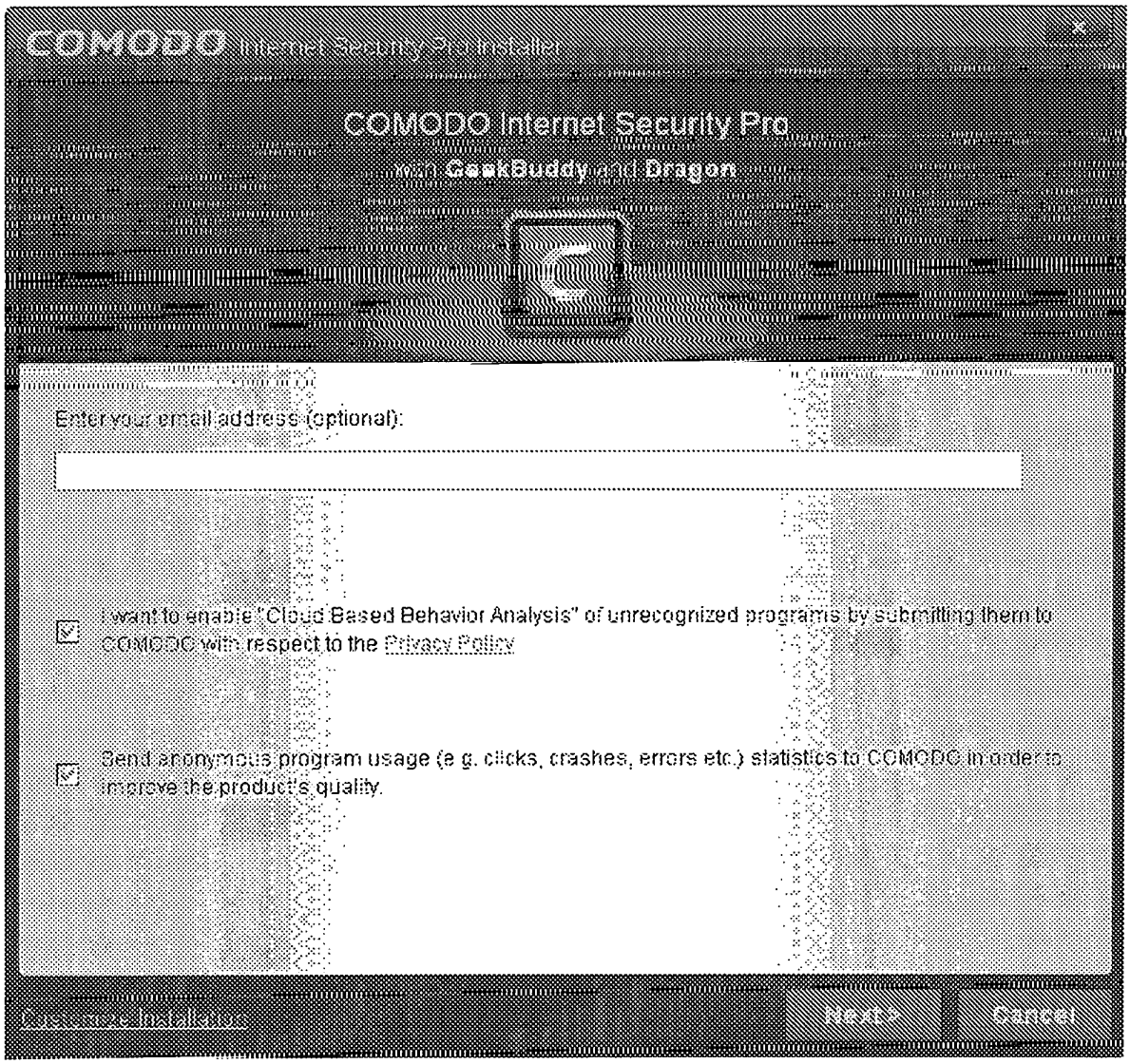
The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.



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

Step 2 - Installation Configuration

The installation configuration screen will be displayed.



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

Receive Comodo News and Notifications

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

Cloud Based Behavior Analysis

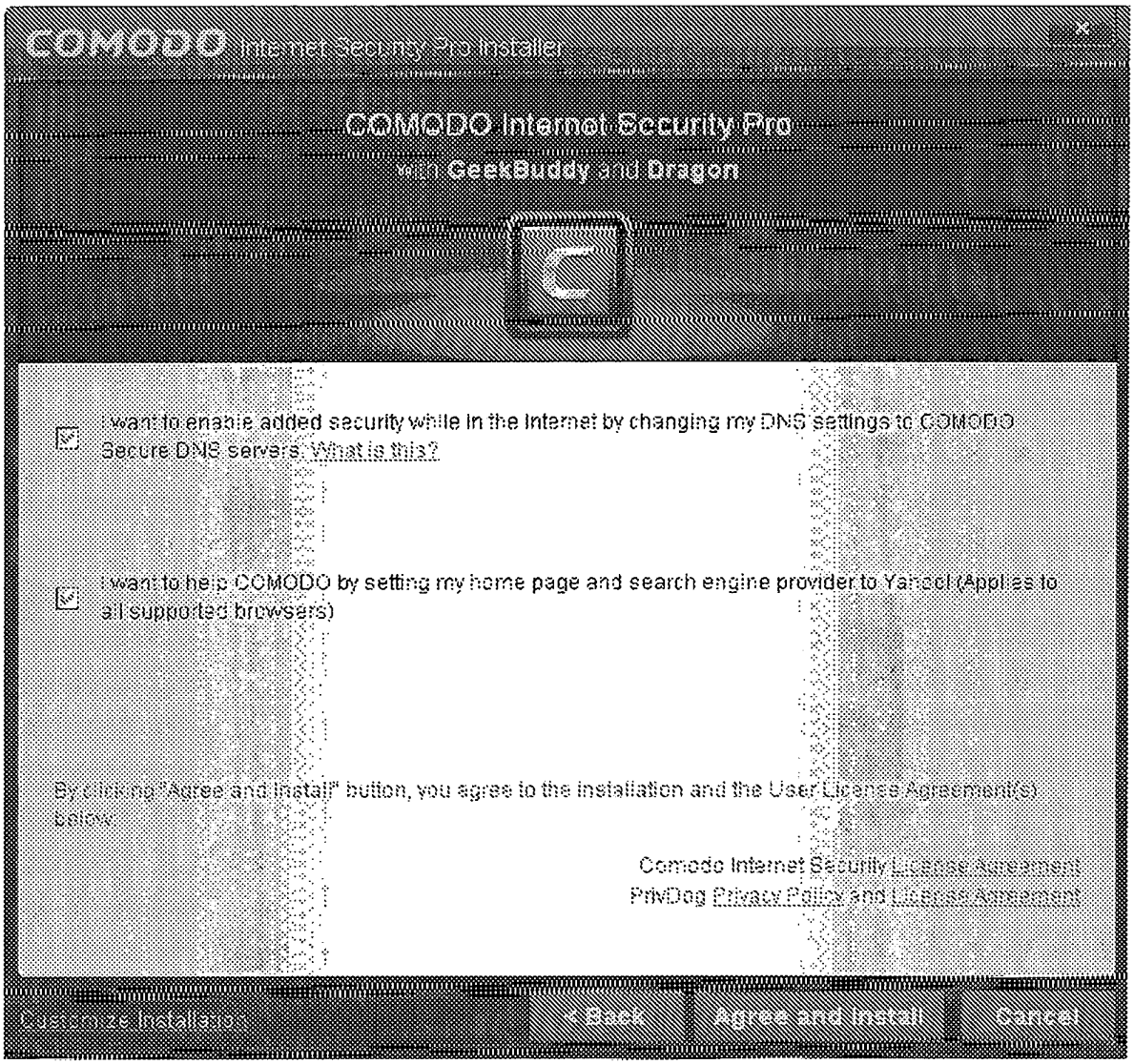
Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer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

Send Program Usage Data

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

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

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



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

DNS Settings

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

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

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

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

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

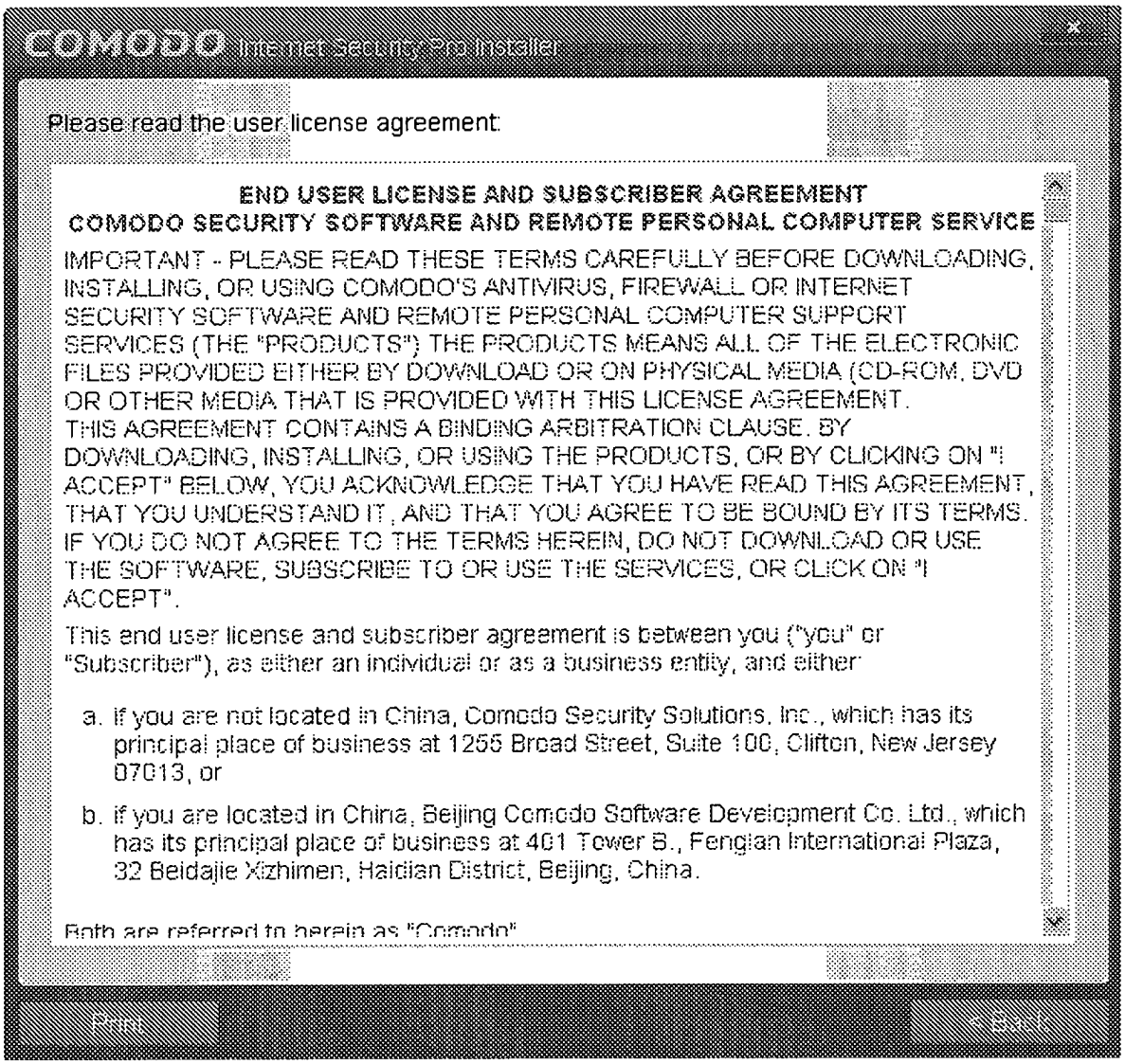
Browser Homepage

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

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

End User License Agreement

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.



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

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

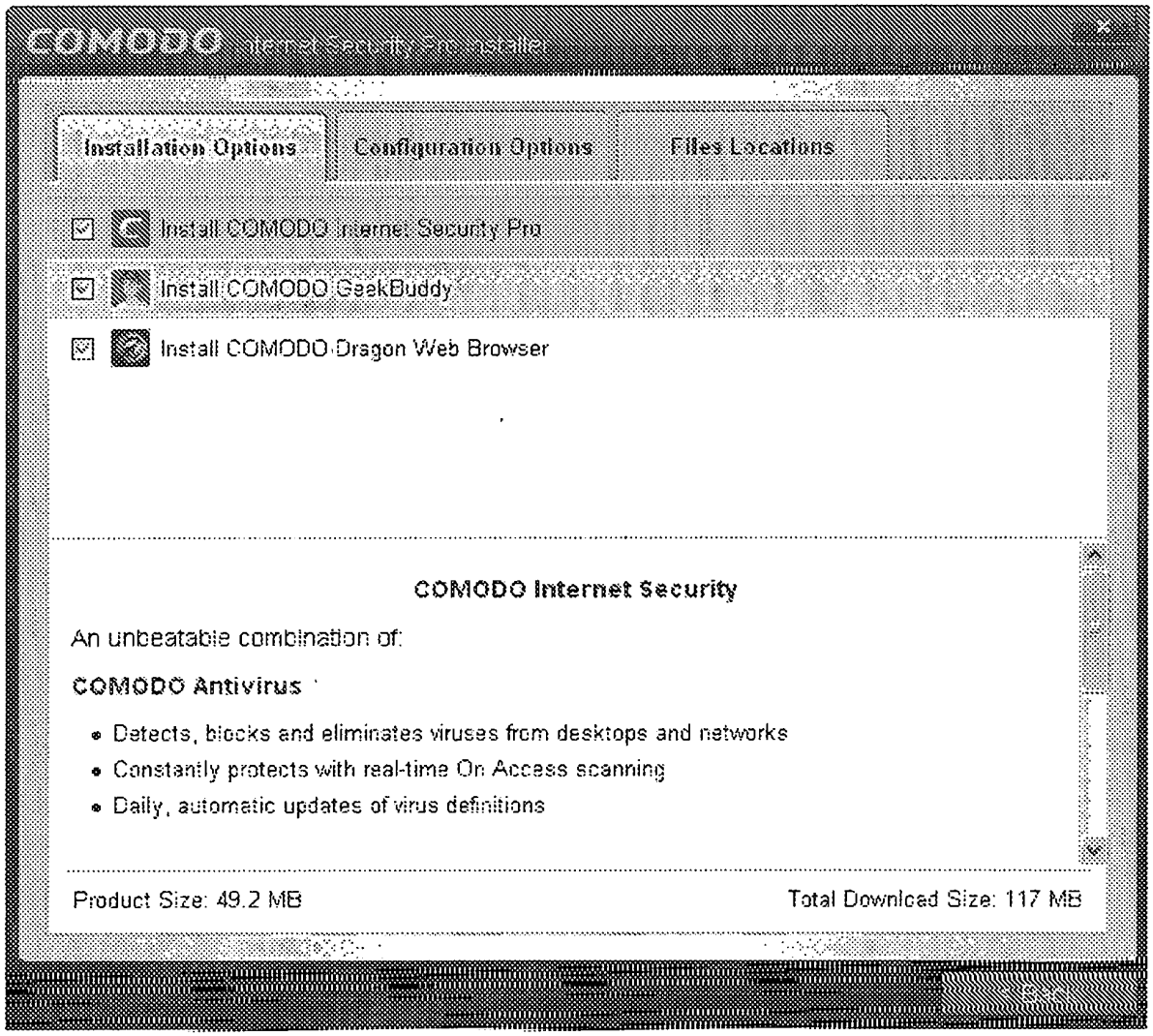
Customizing Installation

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

components to get the maximum benefit from Comodo Internet Security Pro 2013.

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

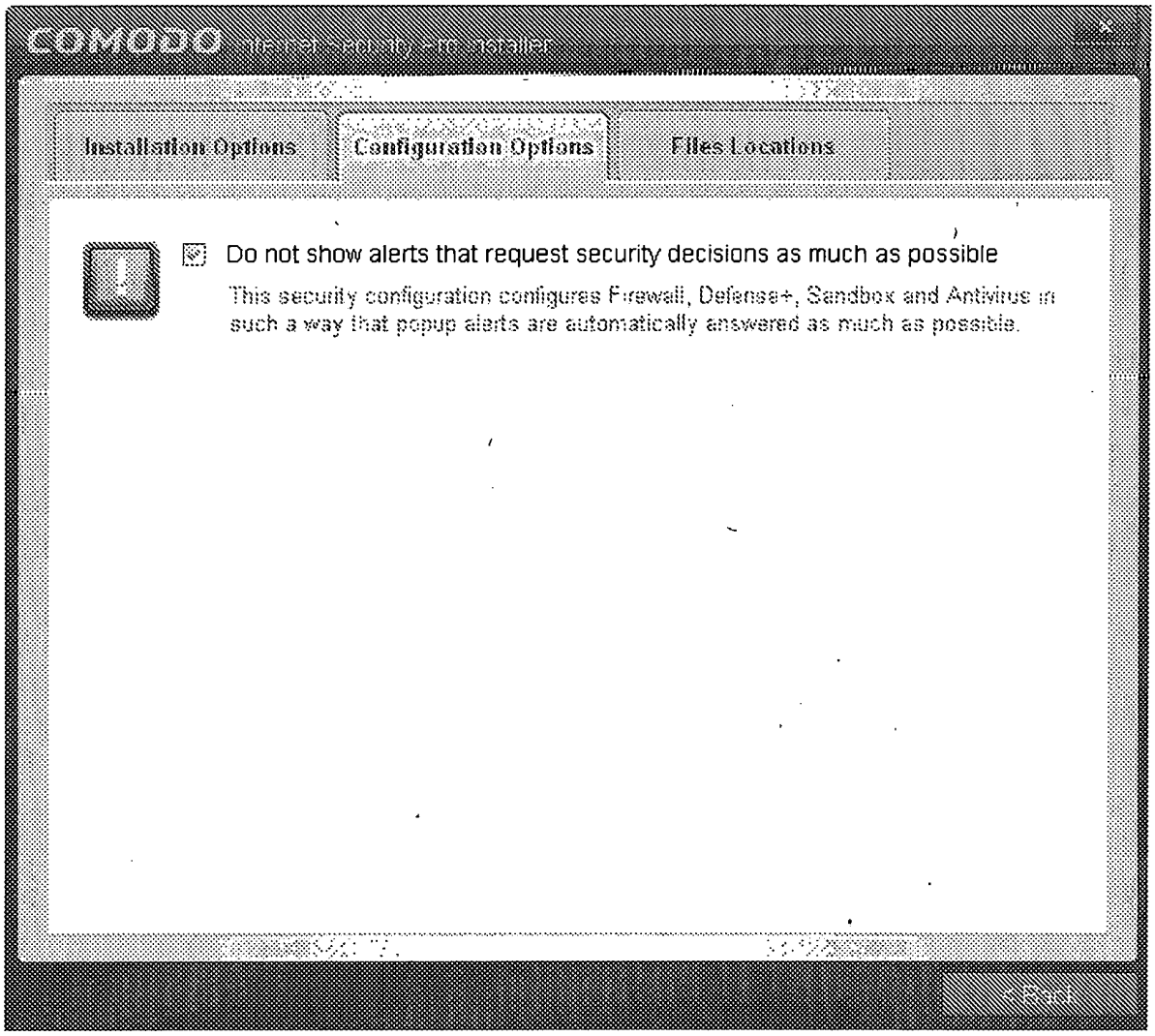
- Click the 'Installation Options' tab to select the components to be installed.



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

Configuration Options

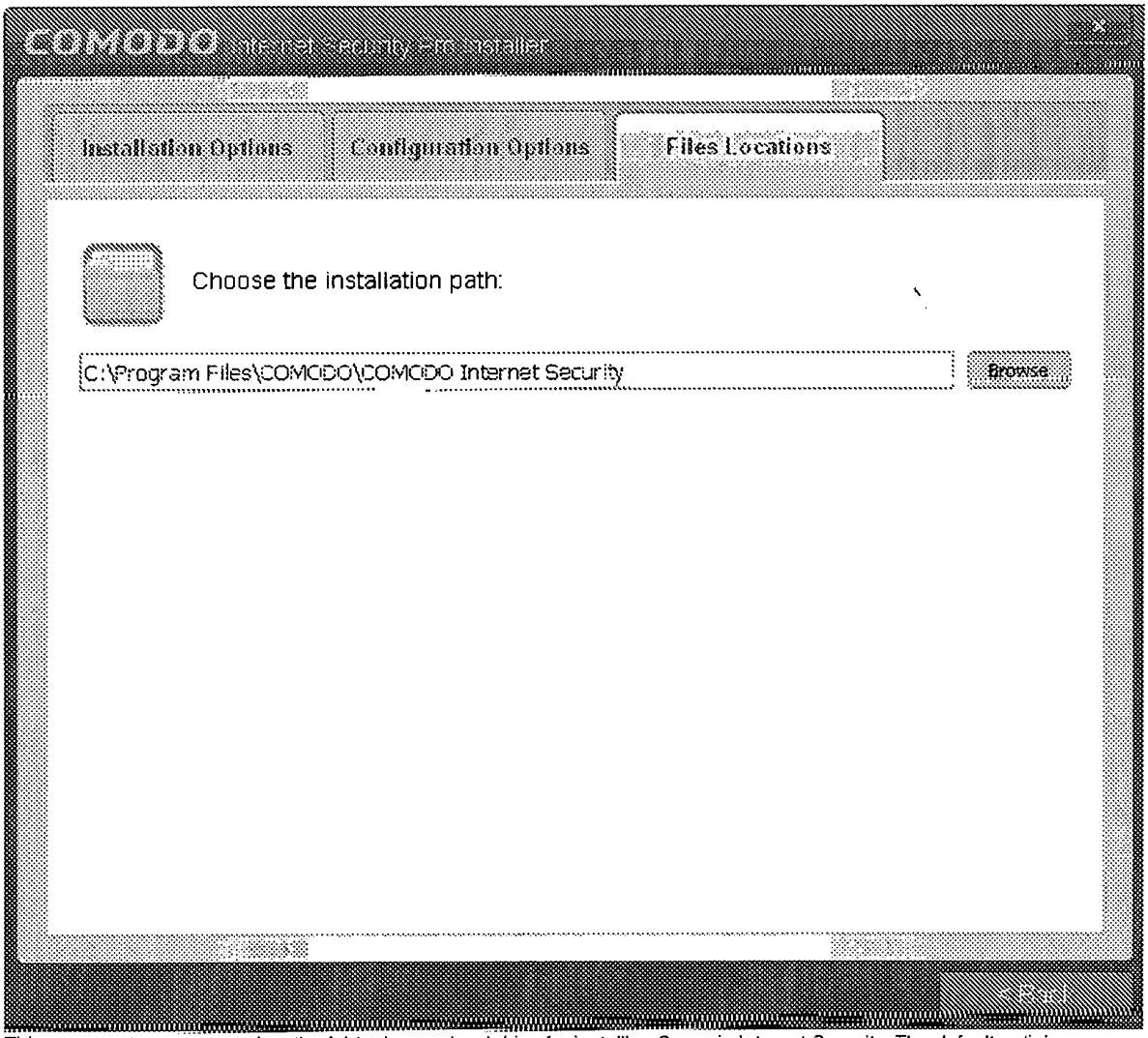
- Click the 'Configuration Options' tab to configure pop-up alert options.



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

Choose the Installation Location

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



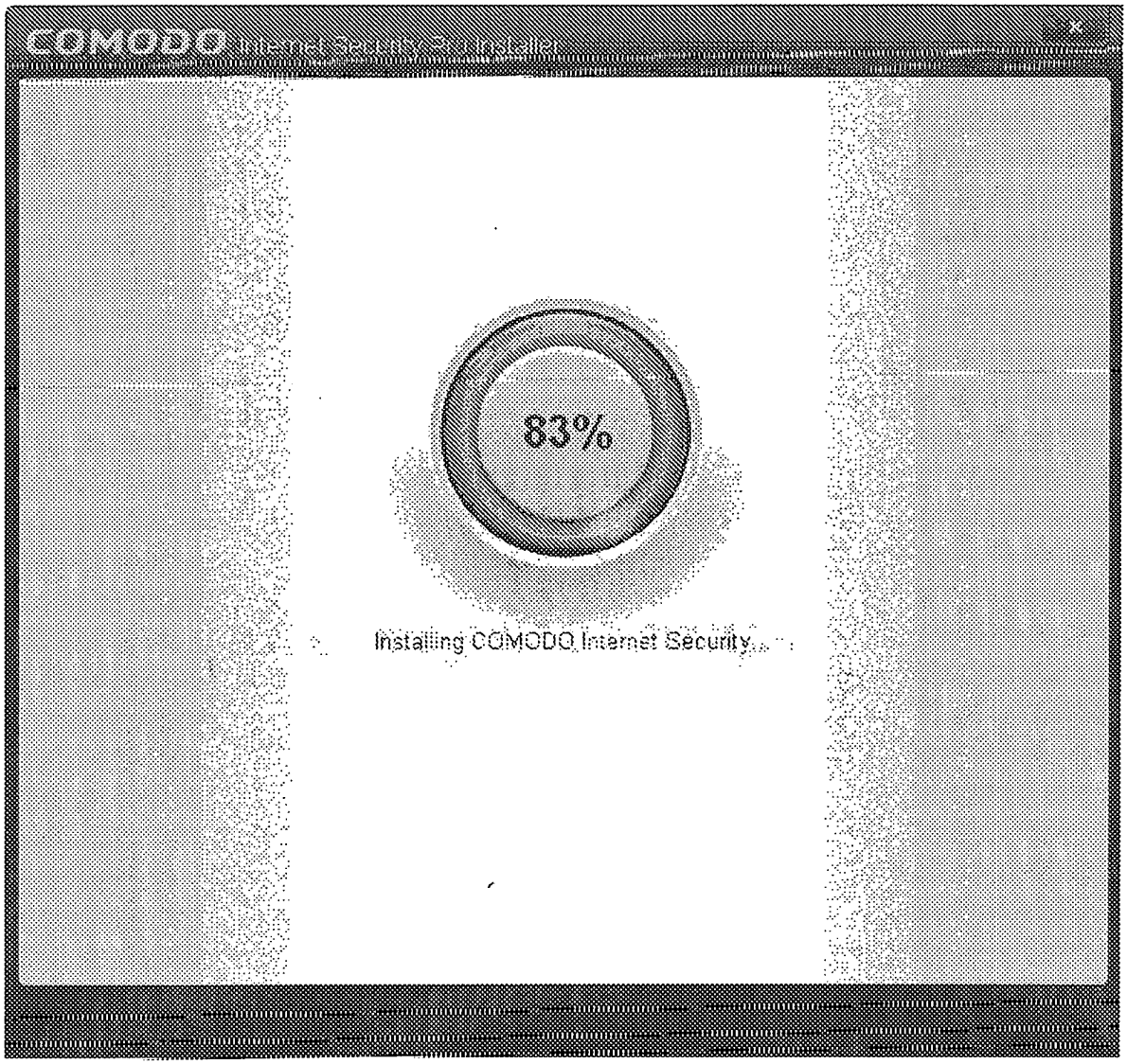
This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

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

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

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

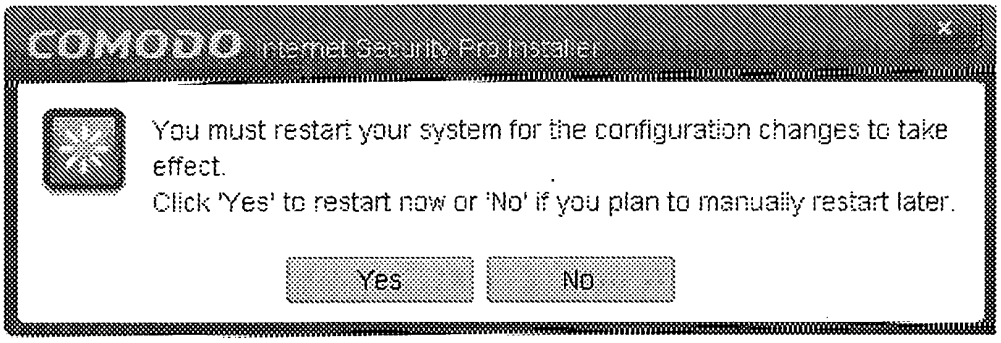
The installation progress will be displayed...



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

Step 4 - Restarting Your System

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

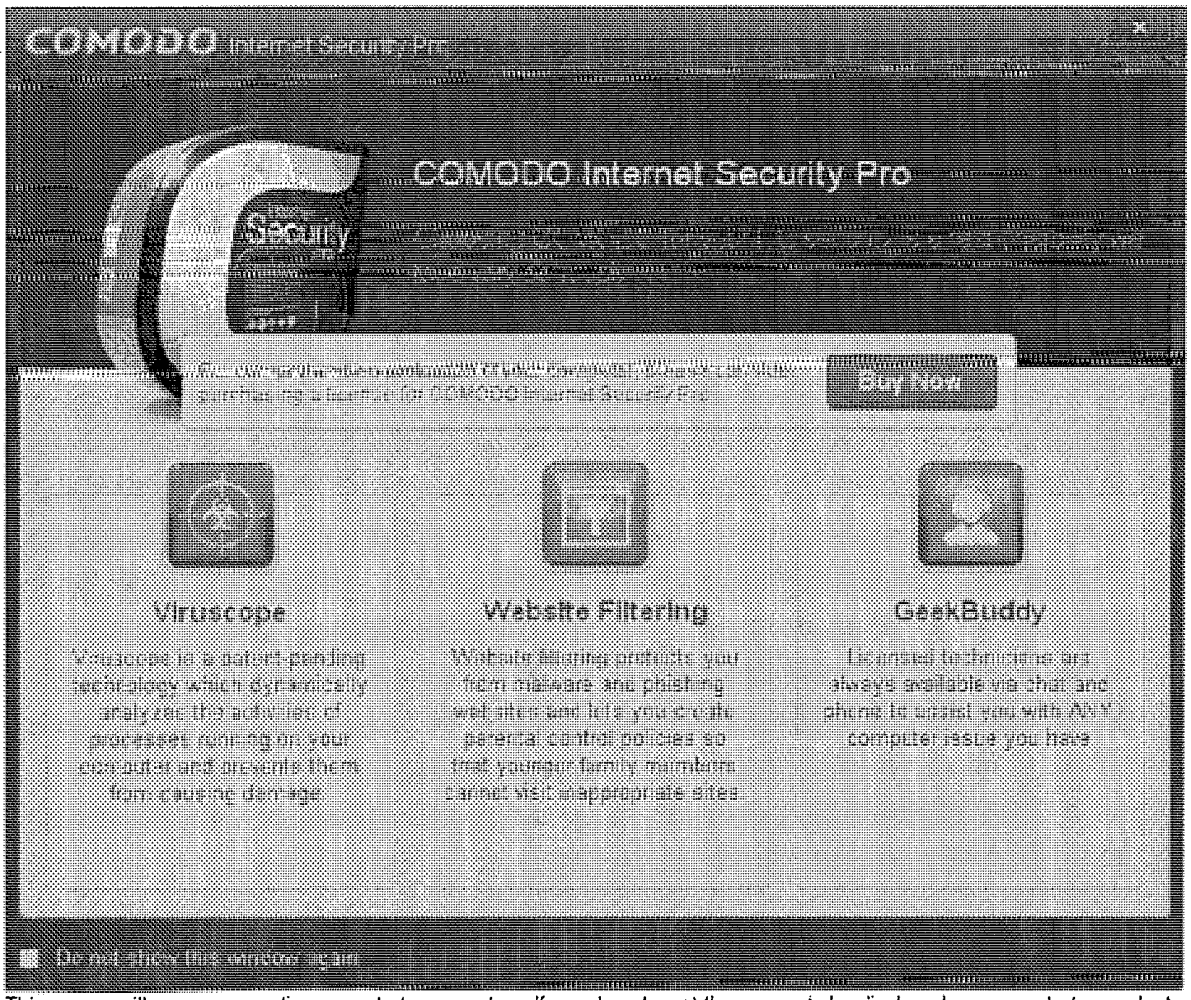


Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

Step 5 - After Restarting Your System

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



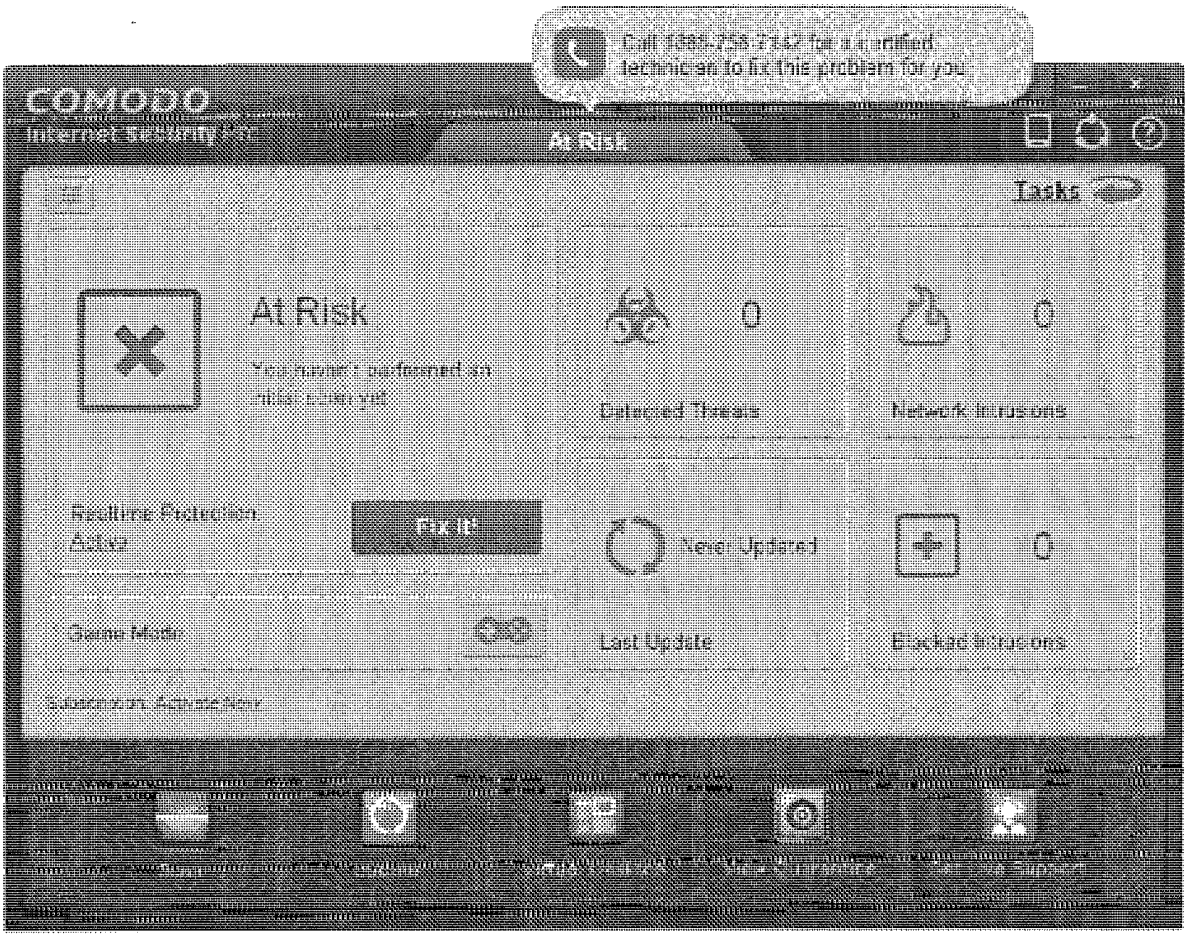
This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

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

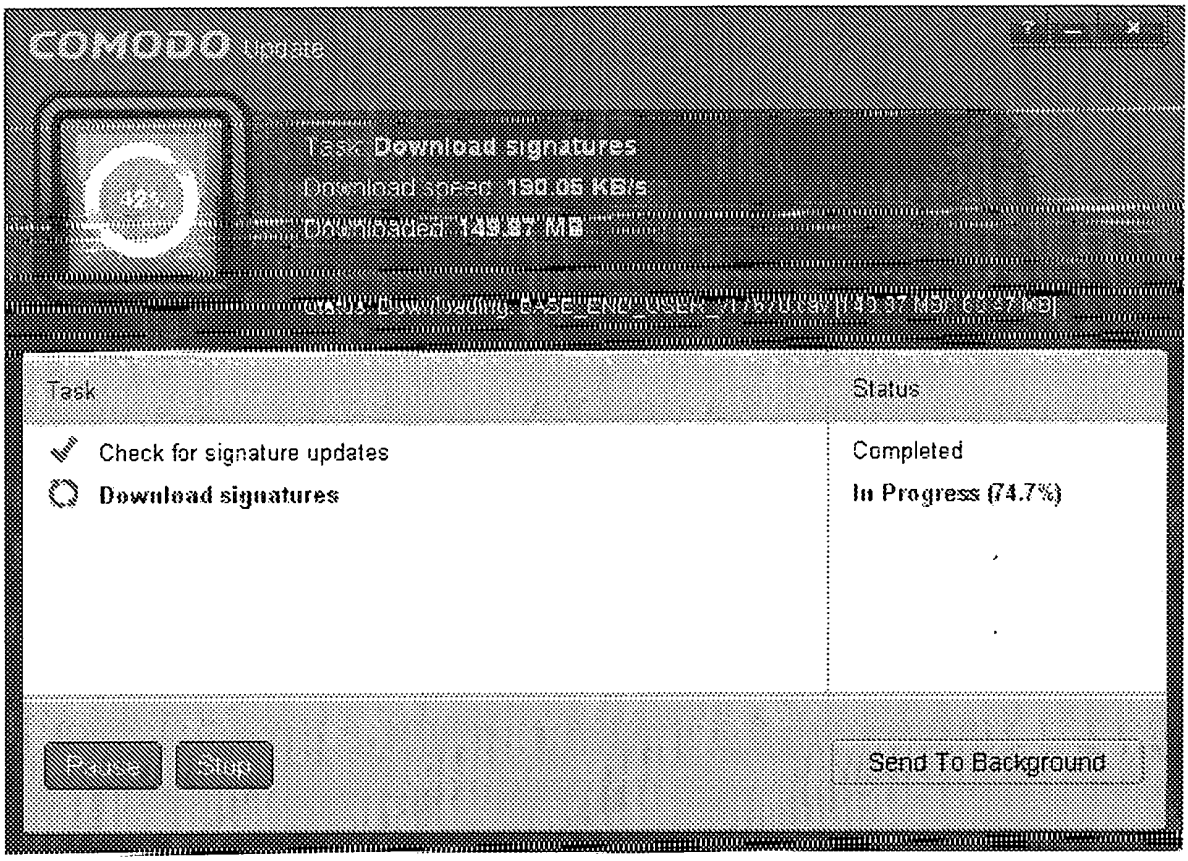


- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

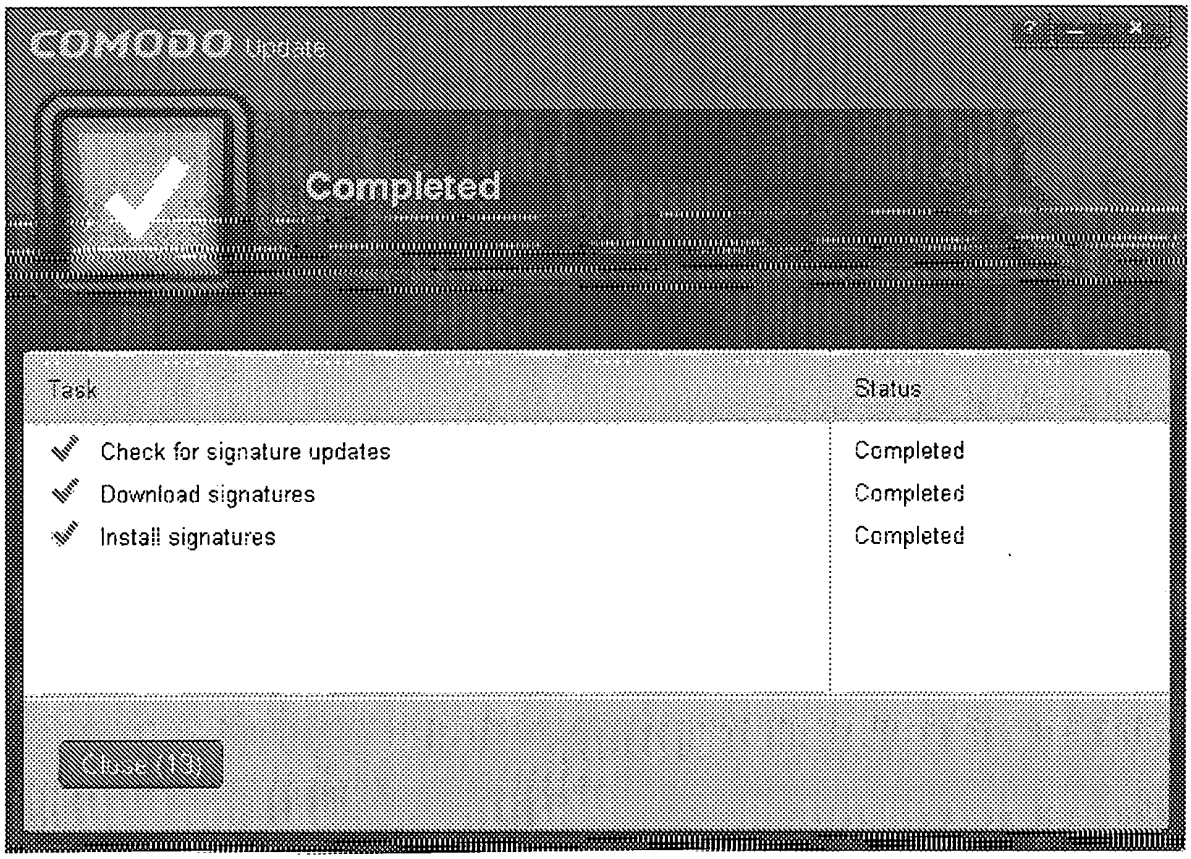
The main interface will be displayed:



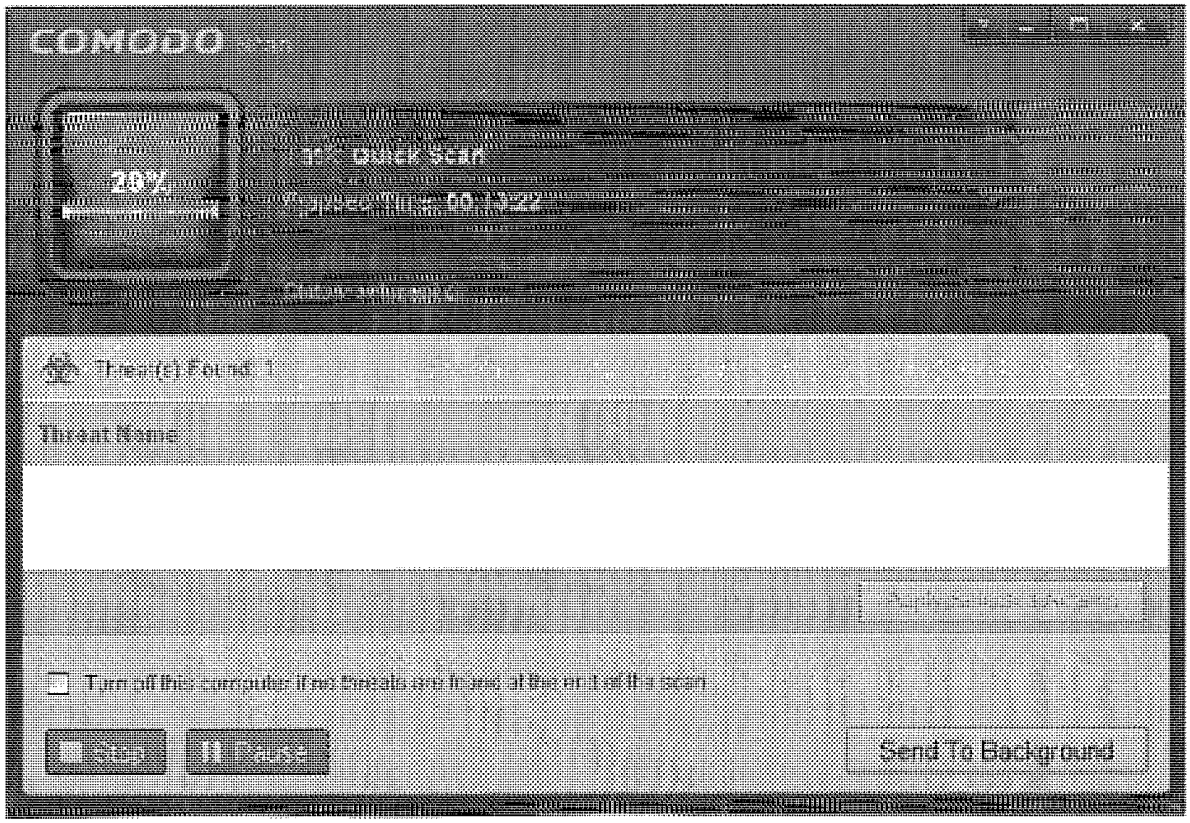
CIS will start its first virus database update at the background. You can view the progress by bringing the update task to foreground from the Task Manager interface. Refer to the section 'Manage CIS Tasks' for more details.



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

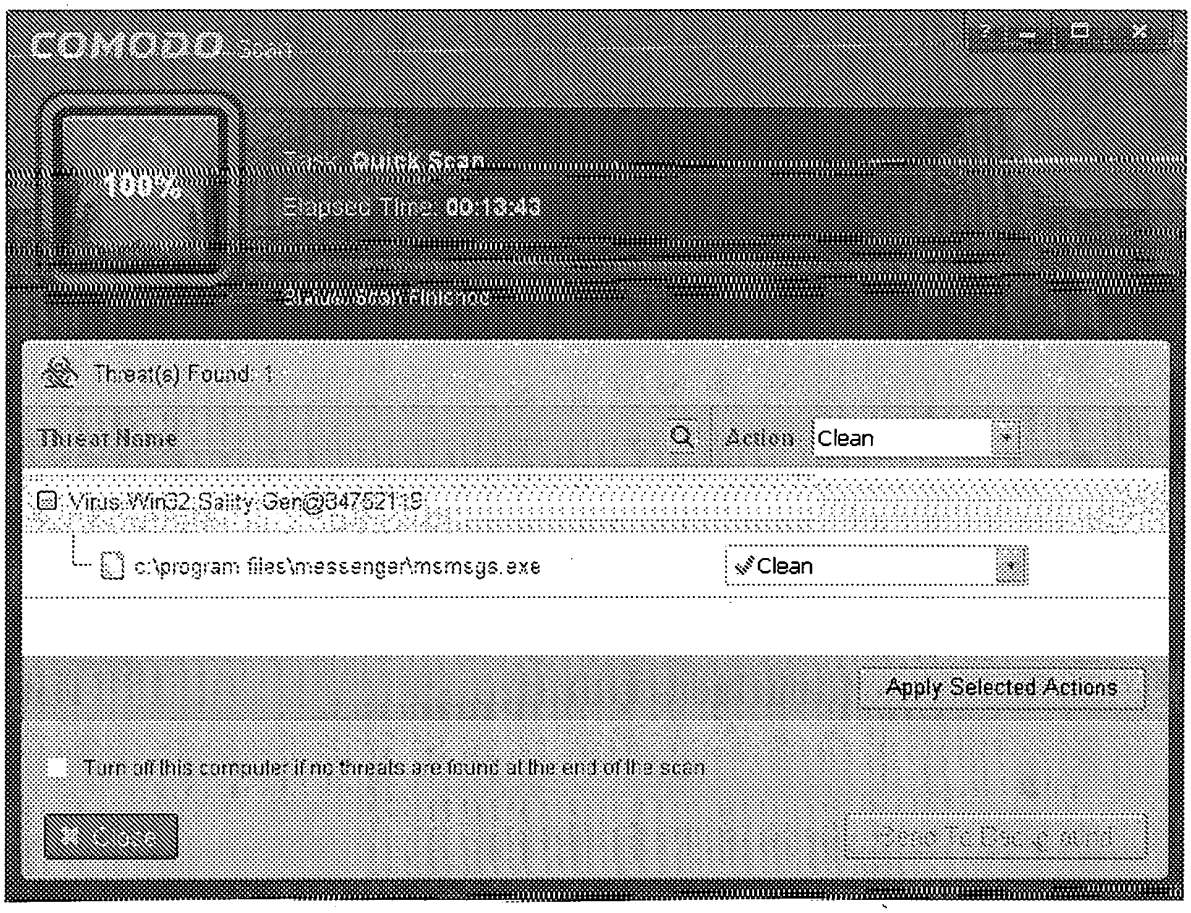


CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



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

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



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

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

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

1.3.3. CIS Complete - Installation and Activation

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

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

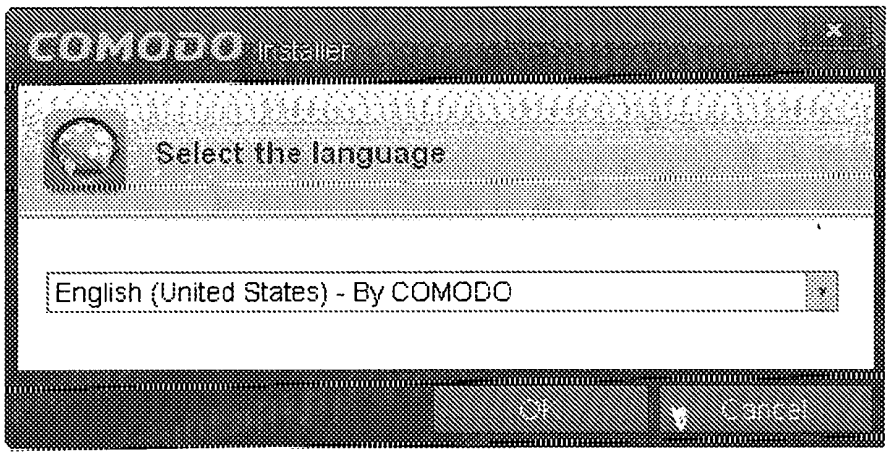
- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and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

64 bit setup files.

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

Step 1 - Choosing the Interface Language

The language selection dialog will be displayed.

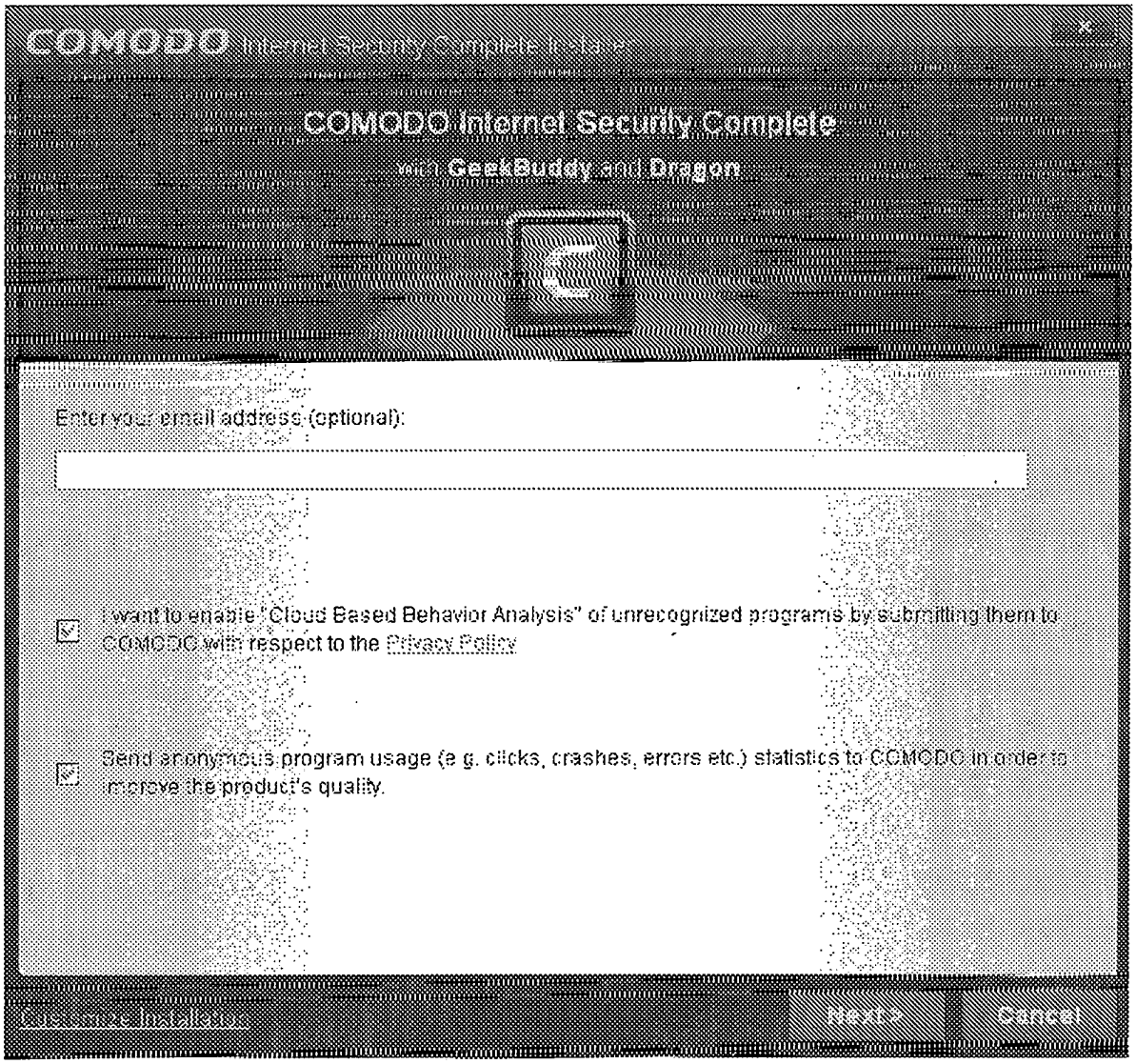


Comodo Internet Security is available in several languages.

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

Step 2 - Installation Configuration

The installation configuration screen will be displayed.



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

Receive Comodo News and Notifications

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

Cloud Based Behavior Analysis

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

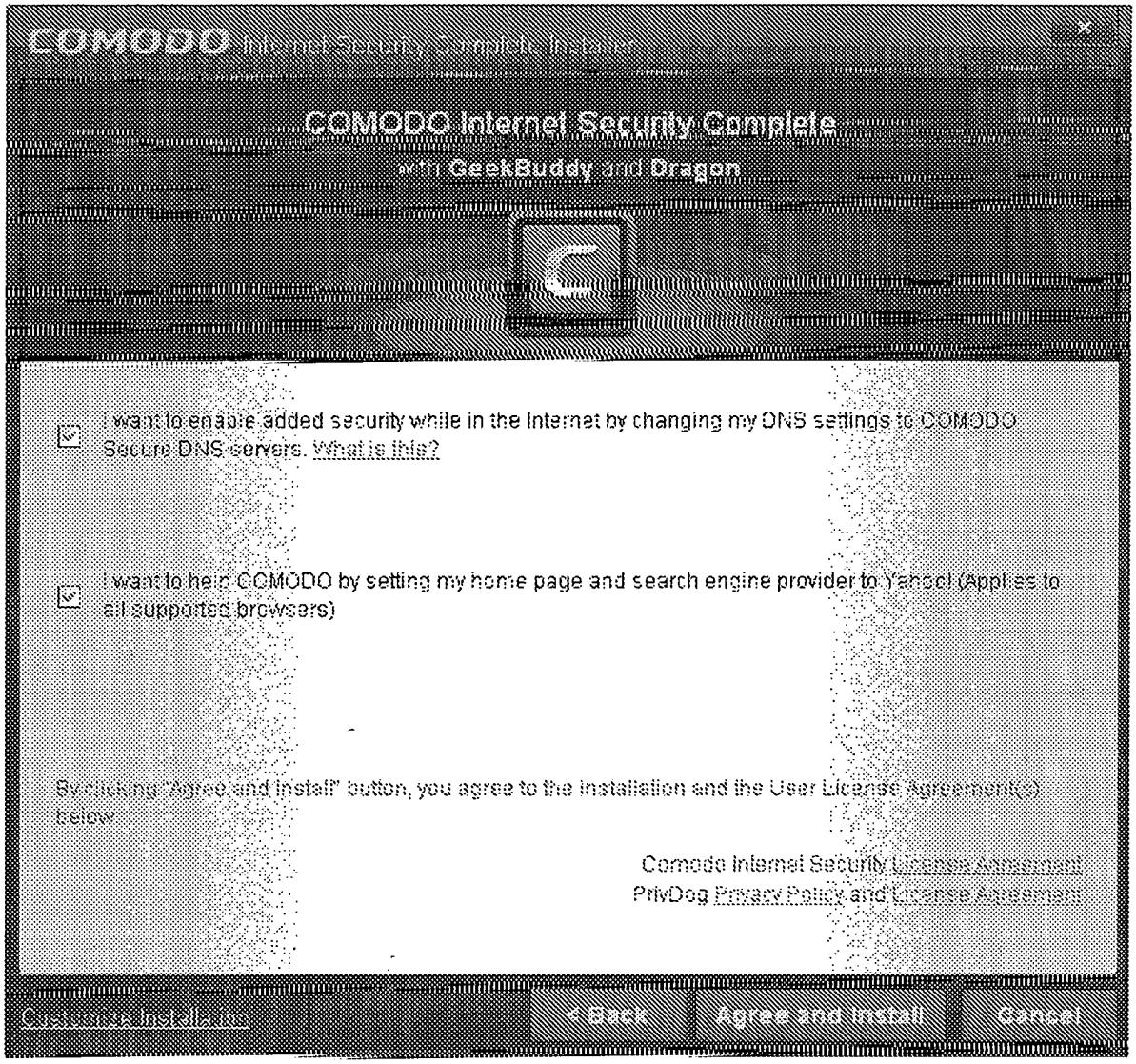
Send Program Usage Data

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

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

- Click the 'Next' button.

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



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

DNS Settings

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

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

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

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

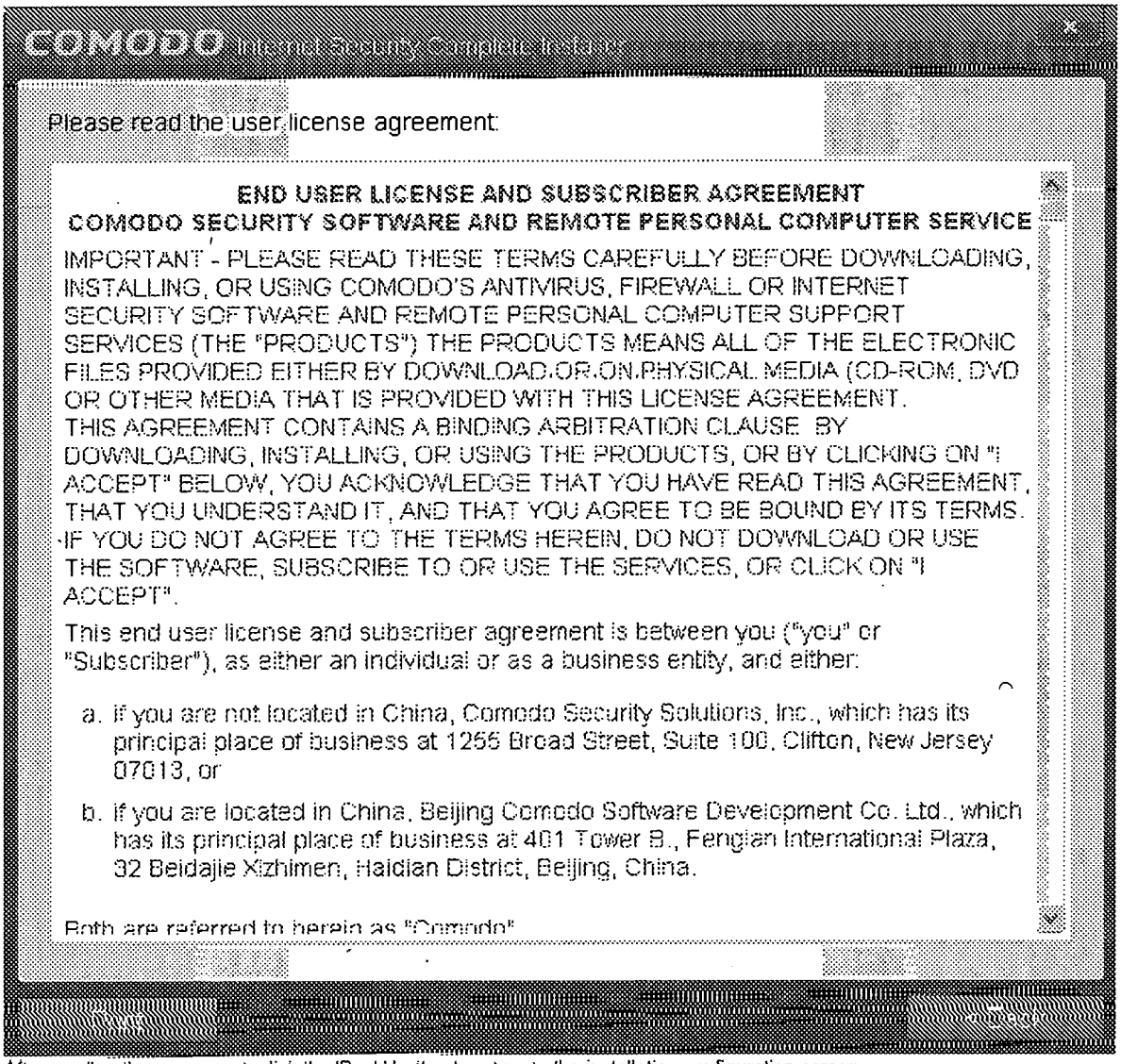
To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

Browser Homepage

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

End User License Agreements

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.



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

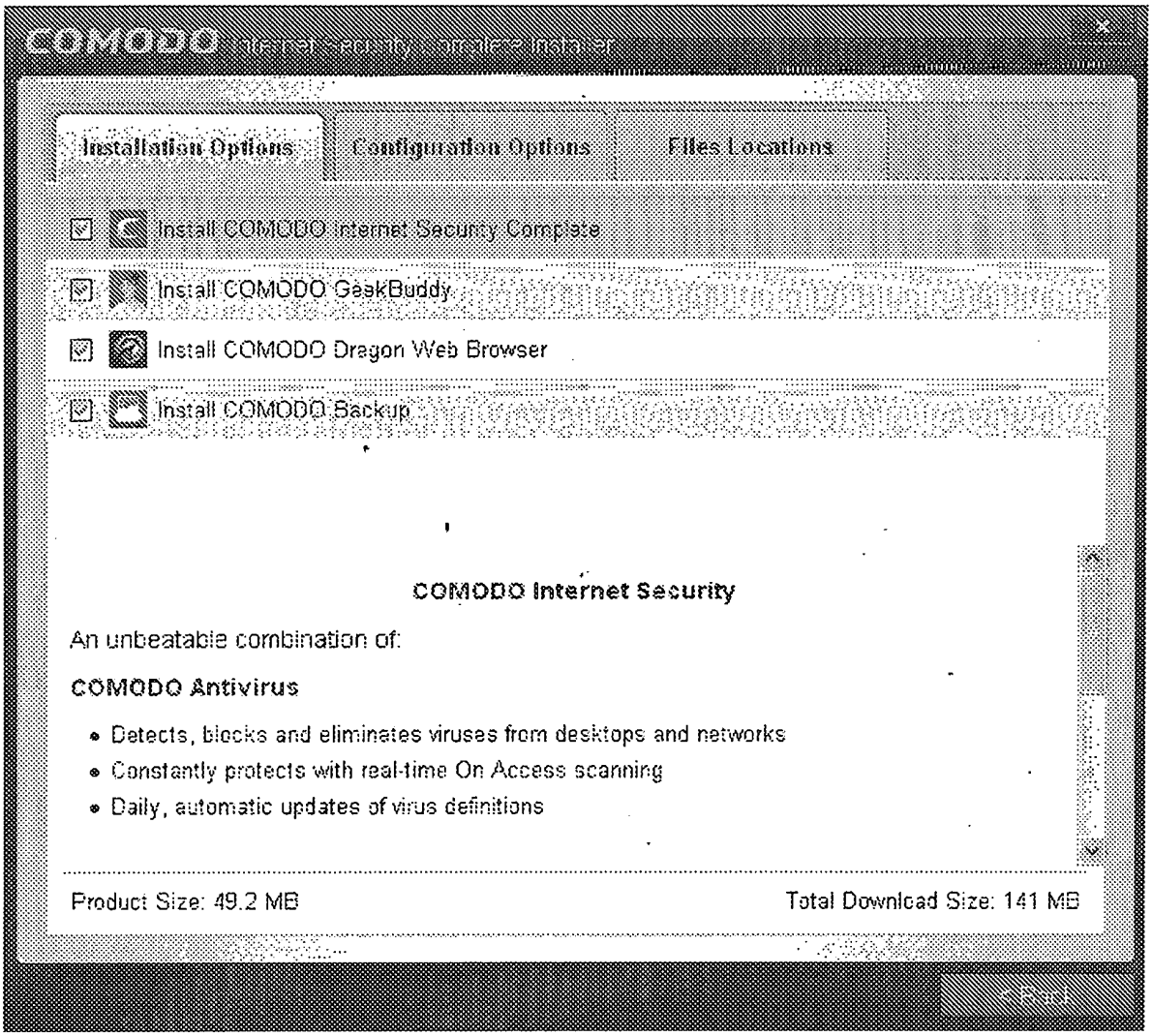
Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installation'. Otherwise, click 'Agree and Install' to begin installation.

Customizing Installation

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

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

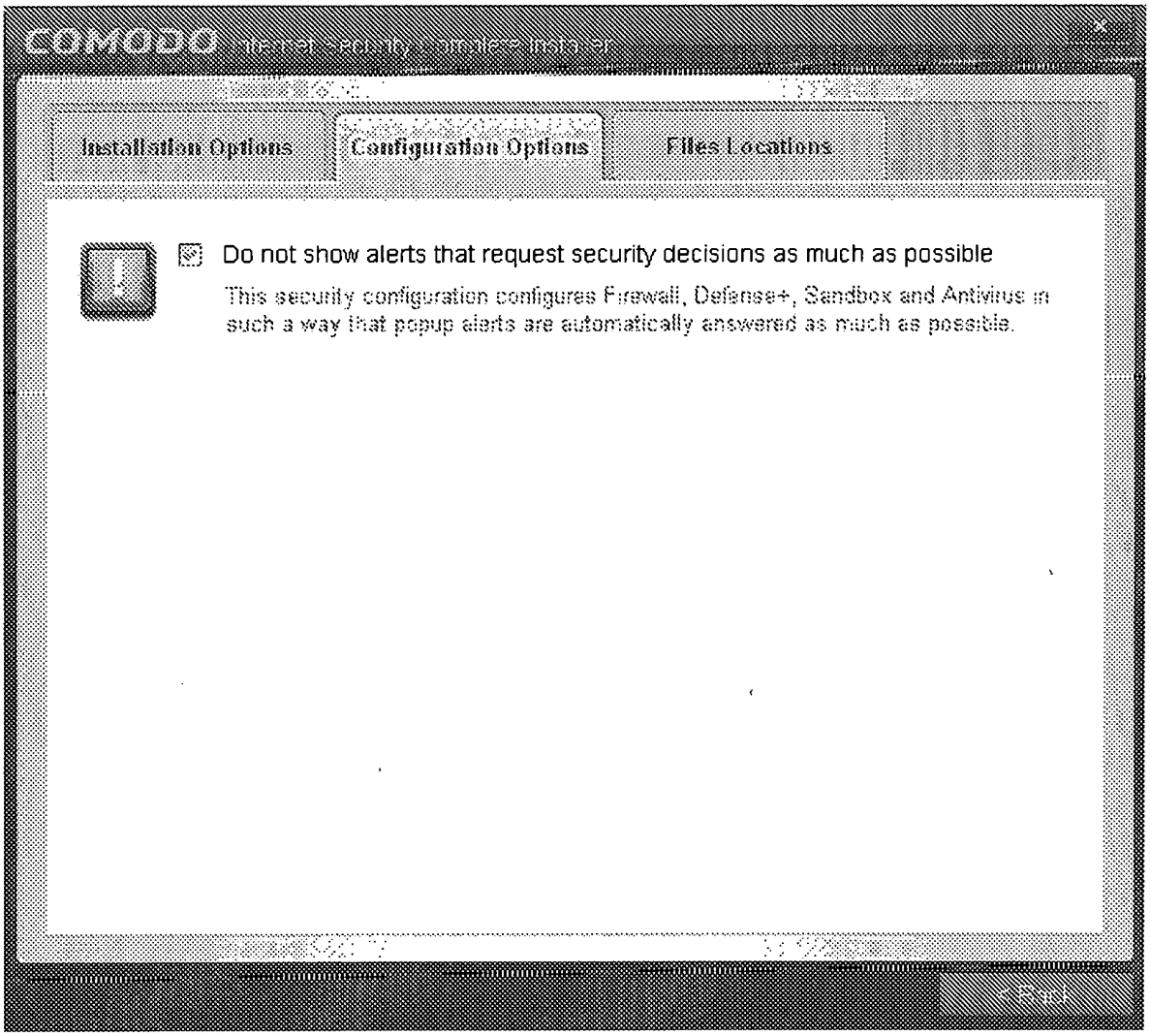
- Click the 'Installation Options' tab to select the components to be installed.



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

Configuration Options

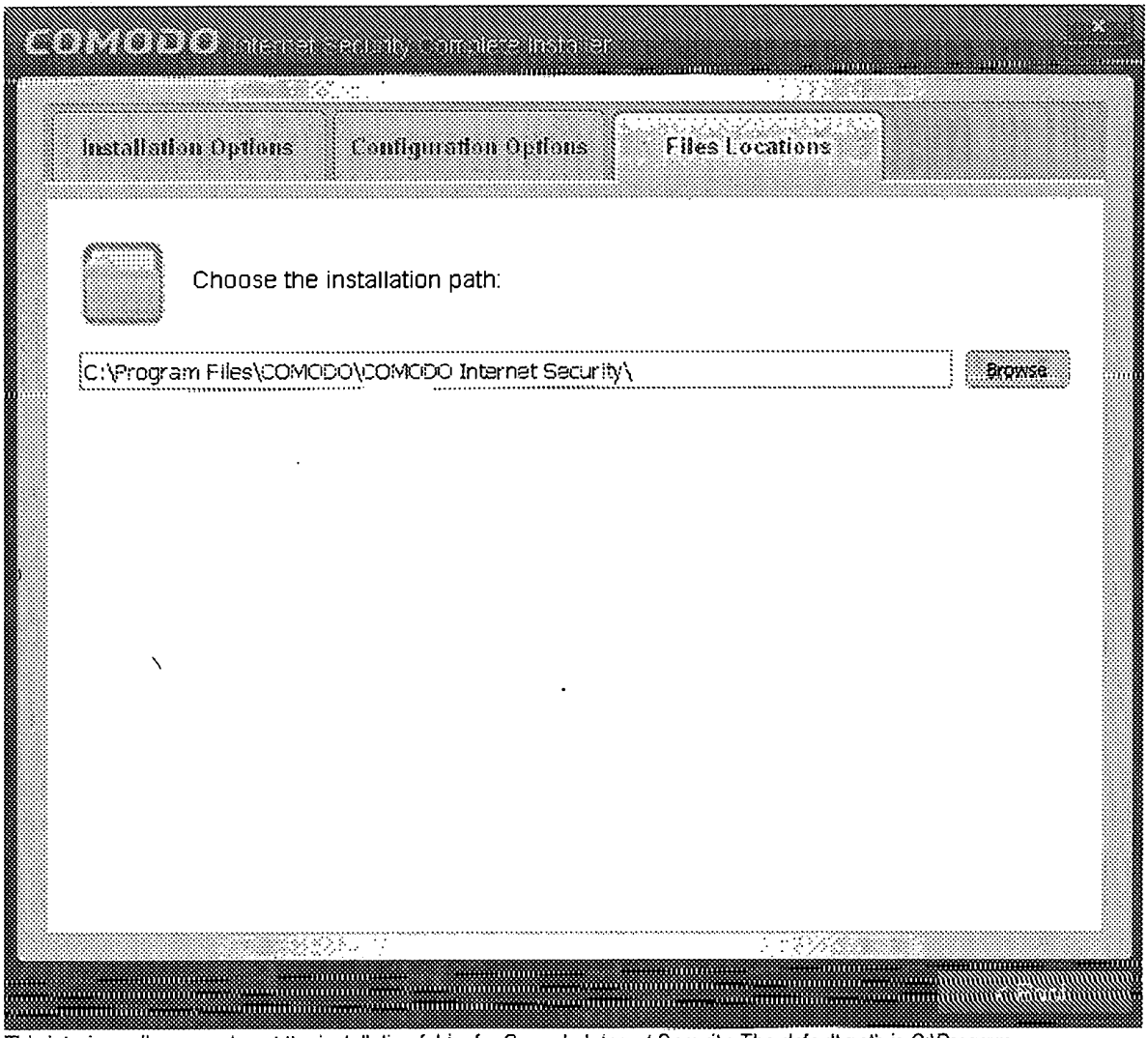
- Click the 'Configuration Options' tab to configure pop-up alert options.



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

Choosing Installation Location

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



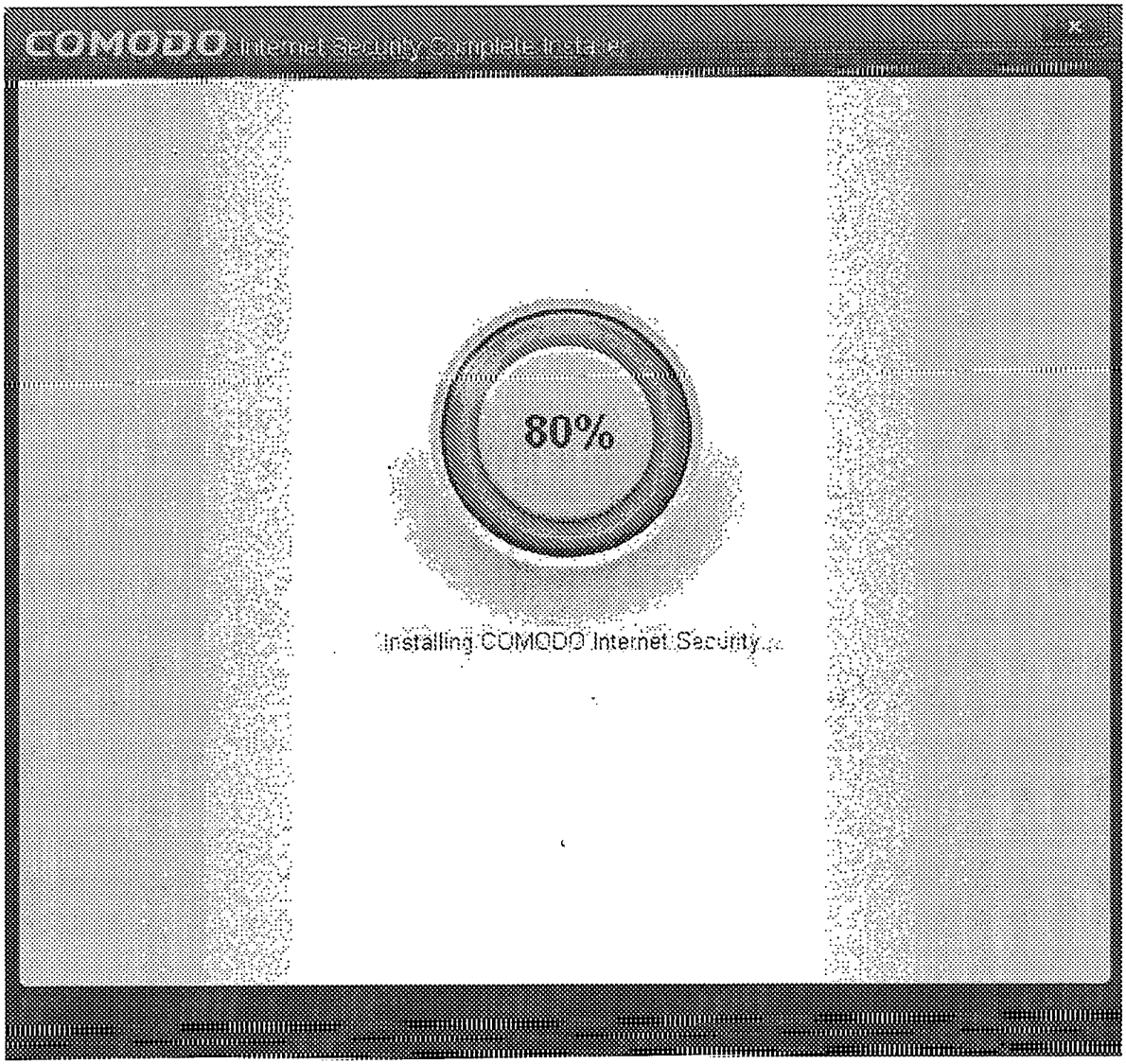
This interface allows you to set the installation folder for Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

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

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

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

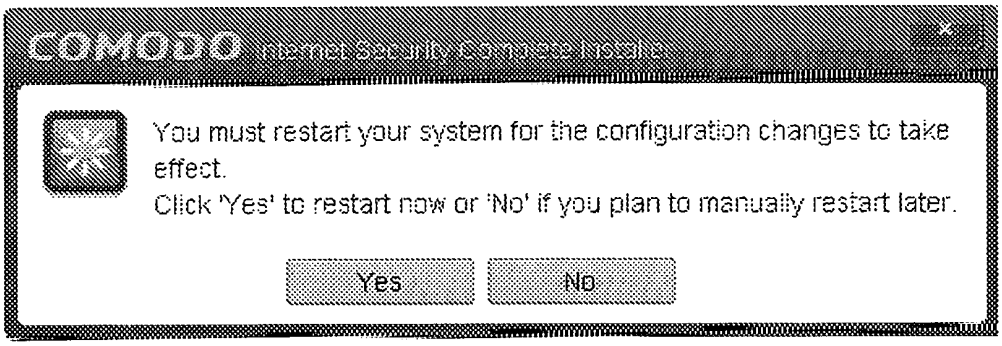
The installation progress will be displayed...



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

Step 4 - Restarting Your System

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

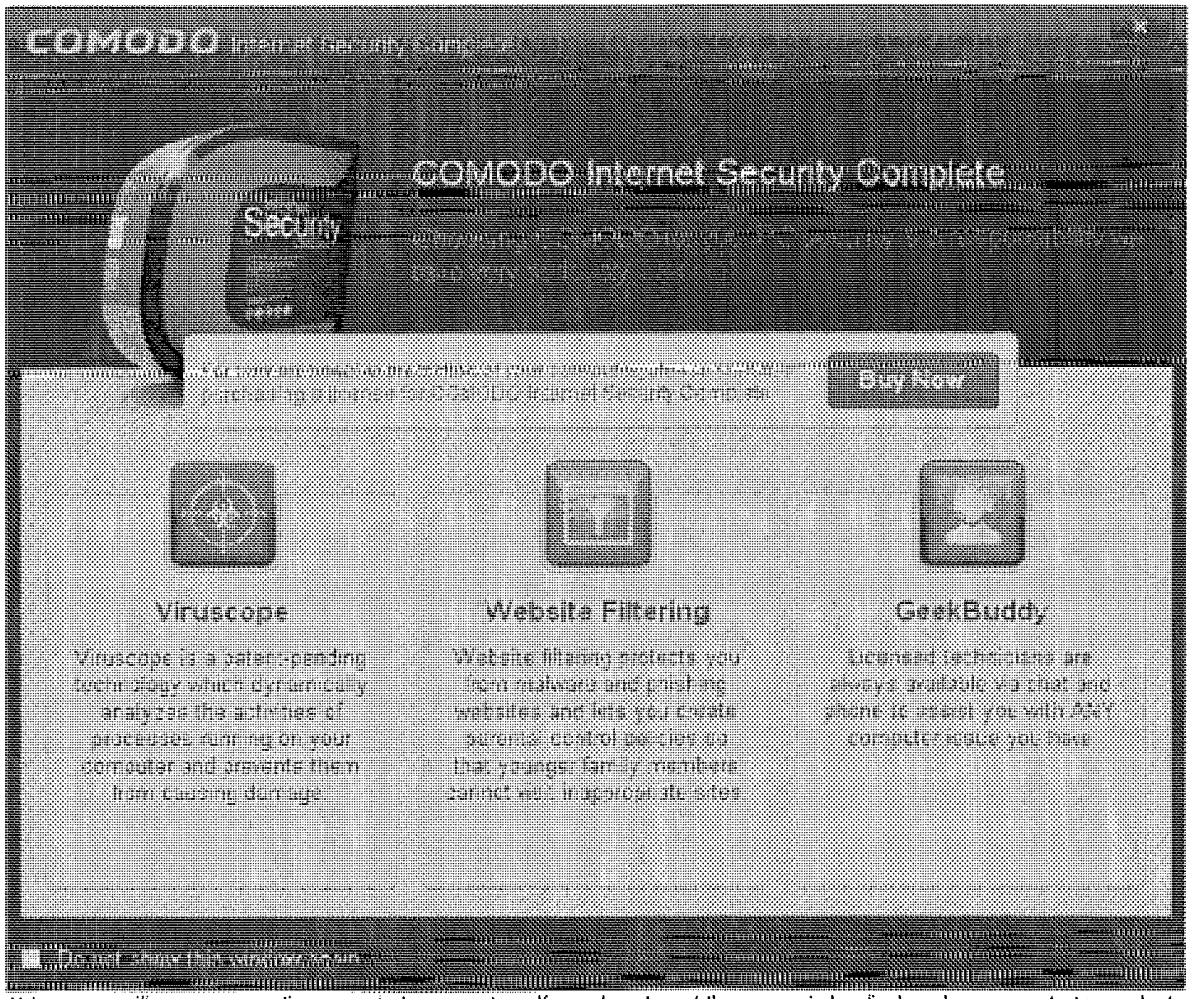


Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

Step 5 - After Restarting Your System

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



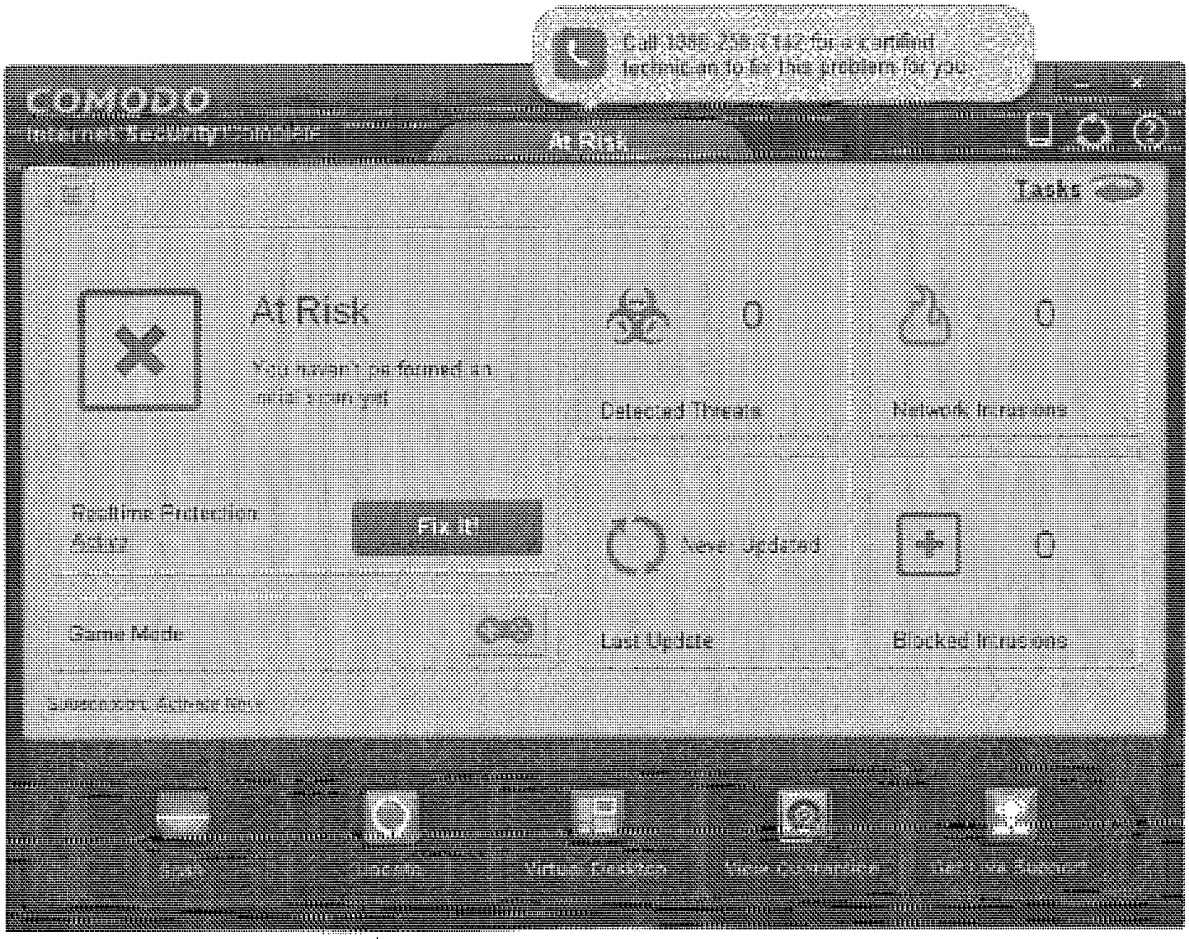
This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

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

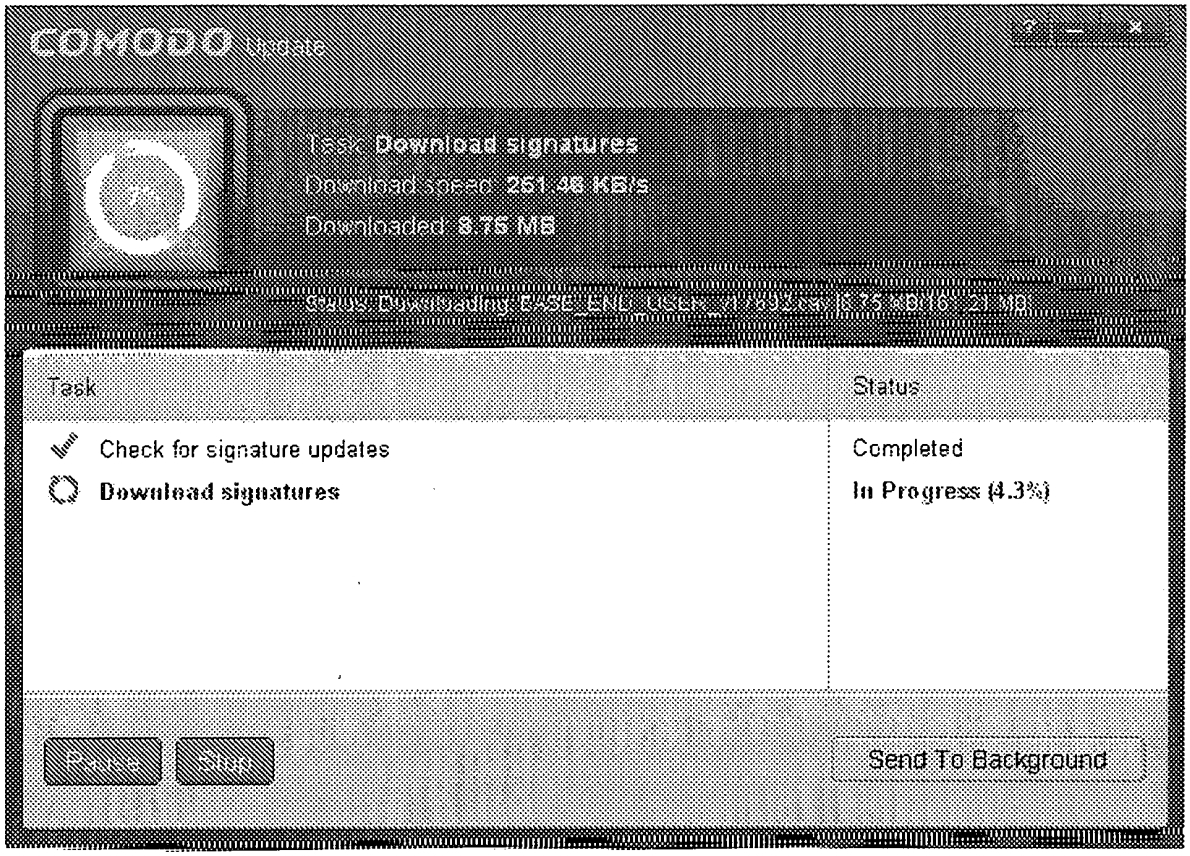


- Select your location from the three options
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard').

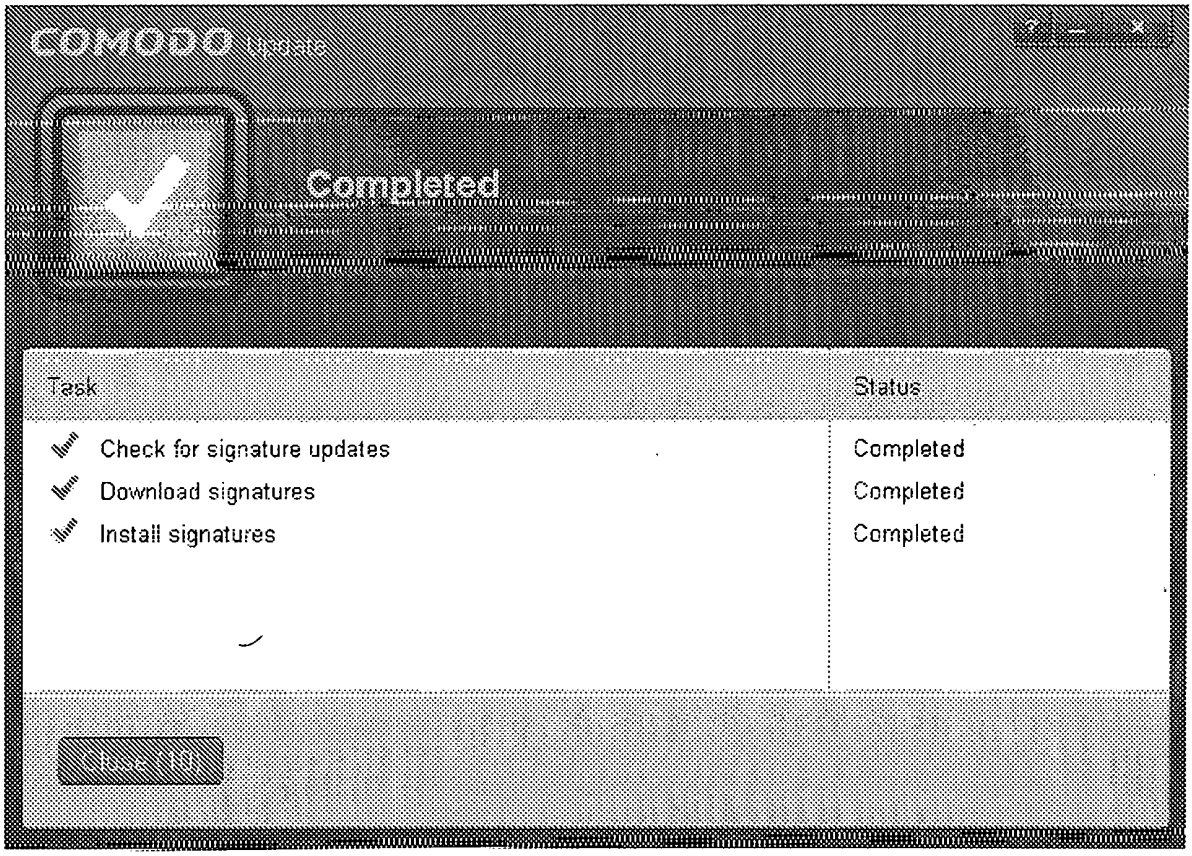
The main interface will be displayed:



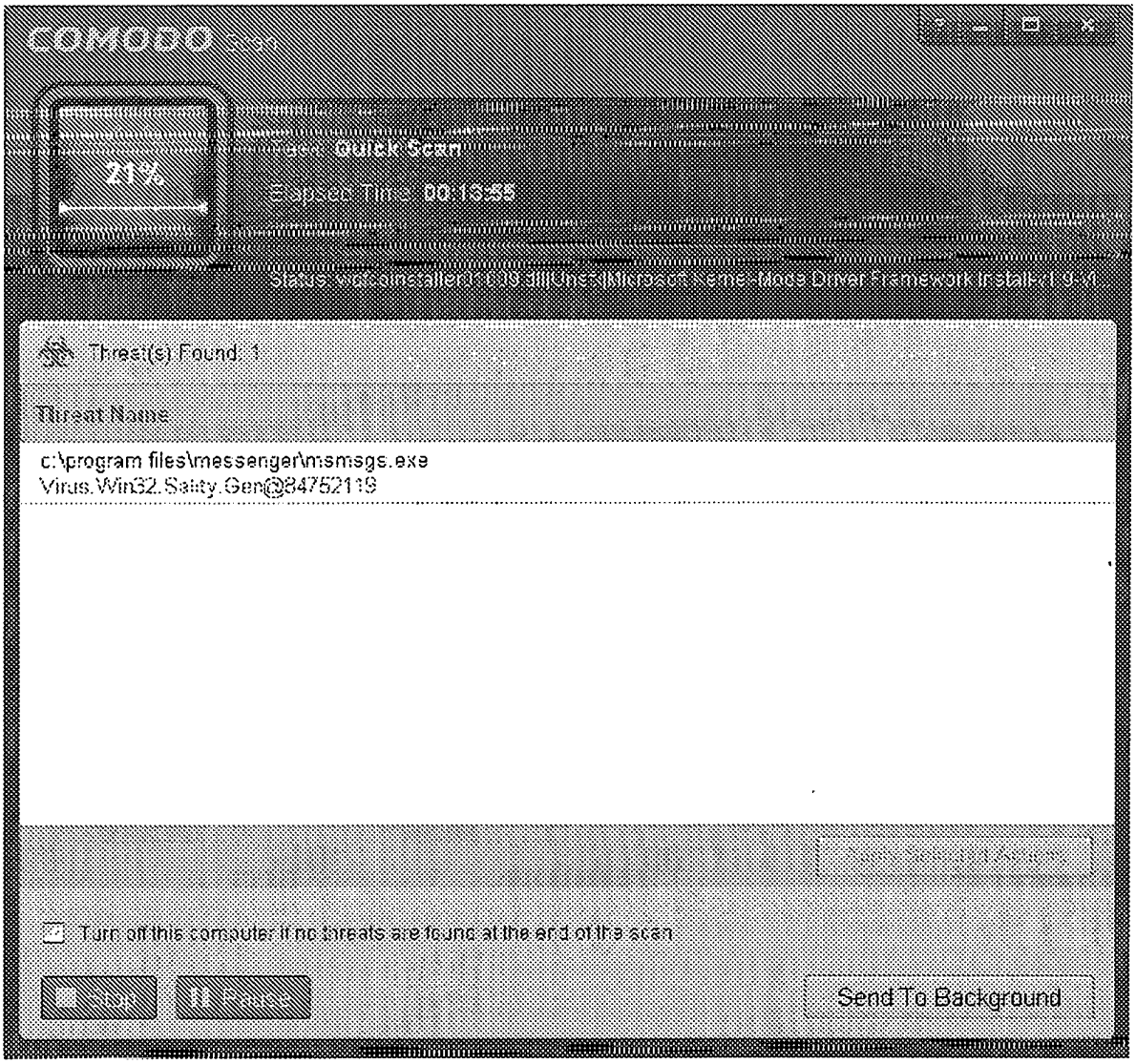
CIS will start its first virus database update at the background. You can view the progress by bringing the update task to foreground from the Task Manager interface. Refer to the section 'Manage CIS Tasks' for more details.



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

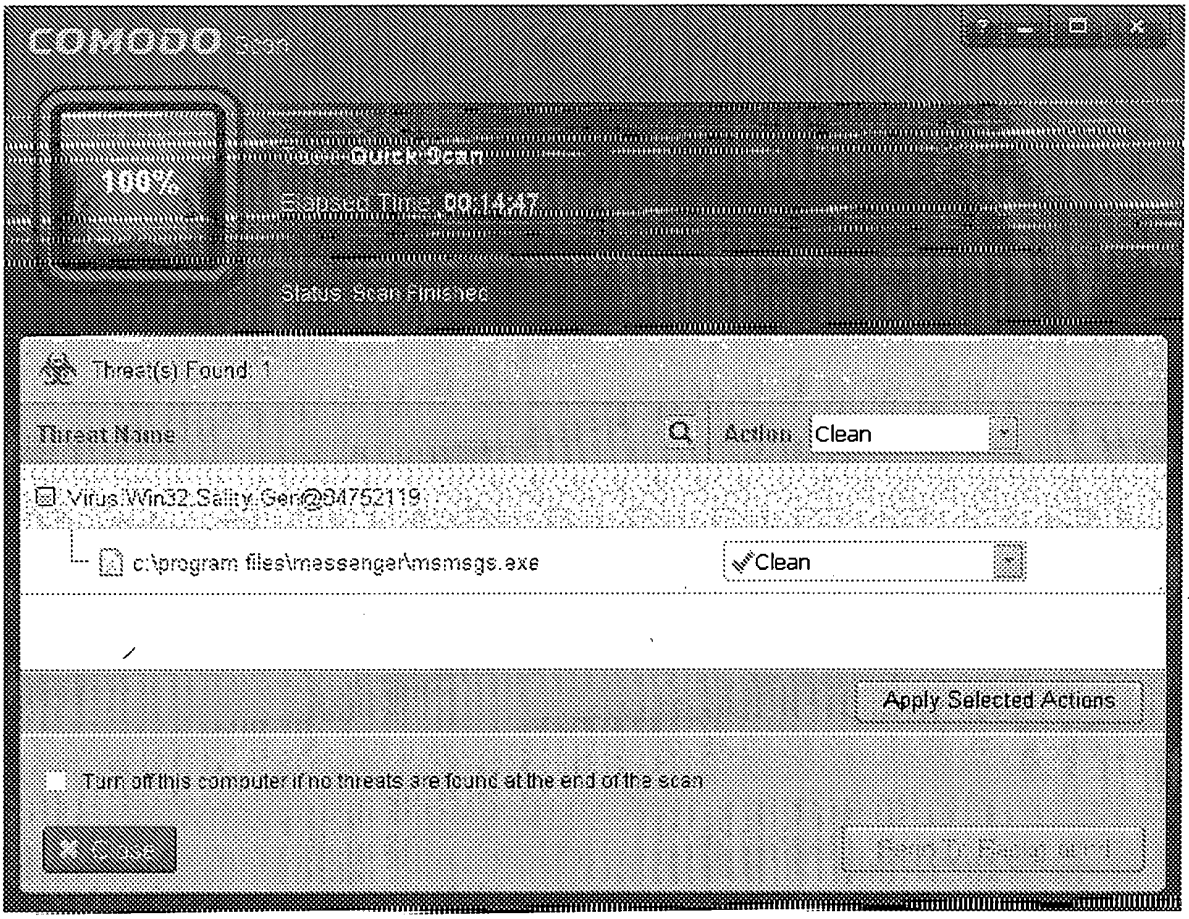


CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



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

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



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

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

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

1.3.4. Activating CIS Pro/Complete Services after Installation

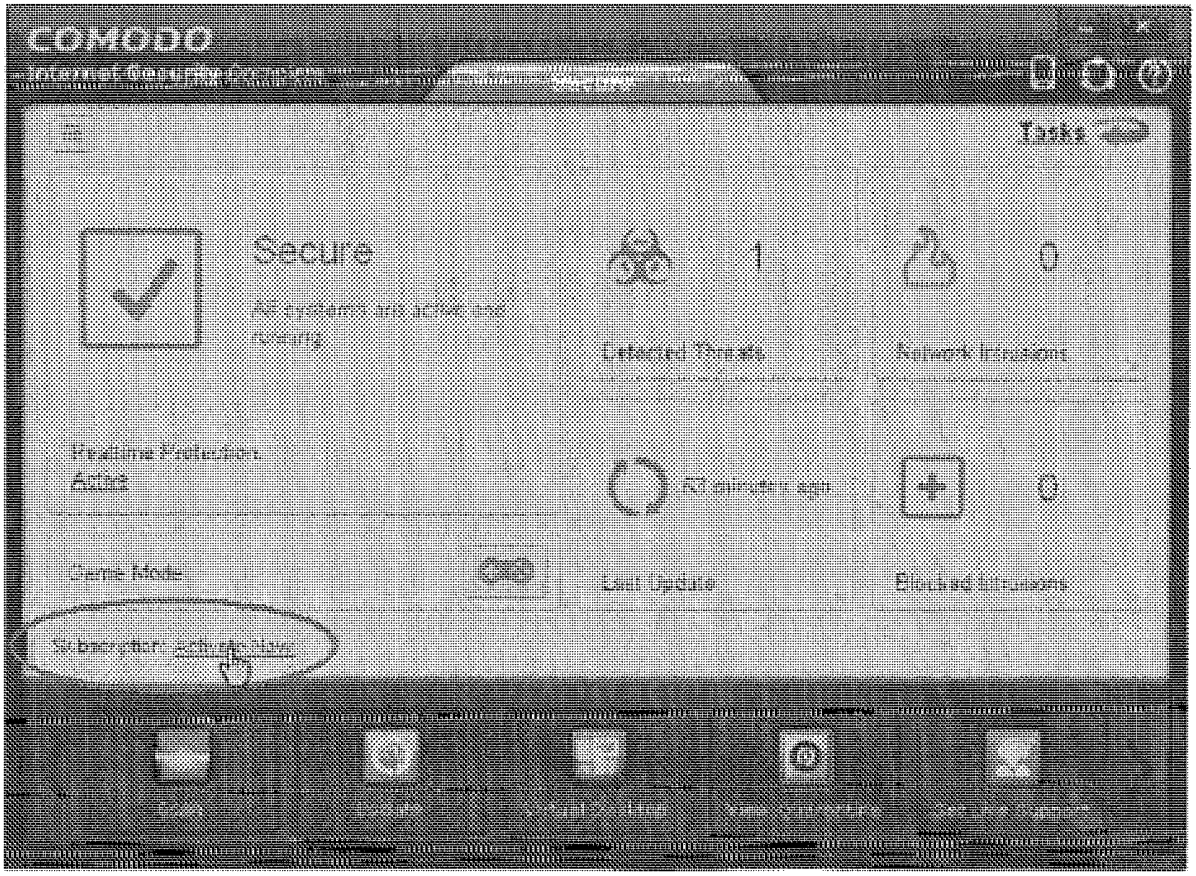
CIS Pro and CIS Complete should be activated after installation for continued use of the product. You will get alerts to activate the license if it has not been done so.

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

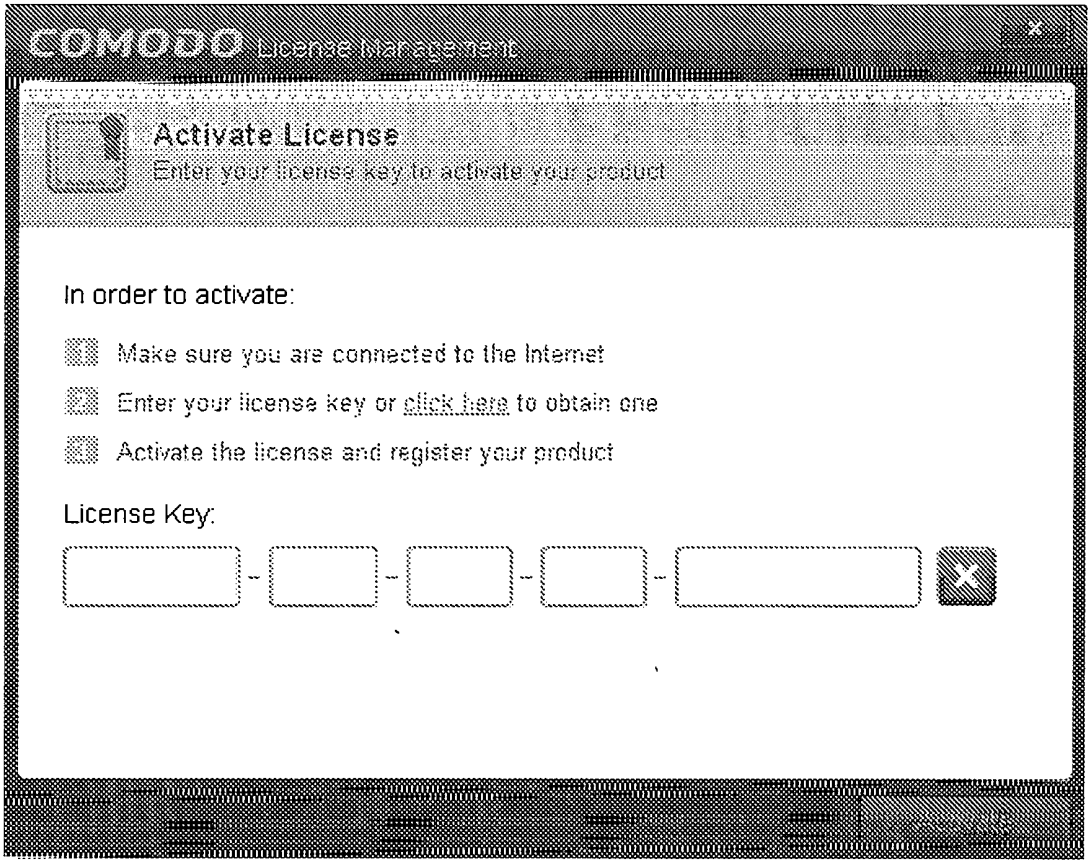
1.3.4.1. Activating Your License

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

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

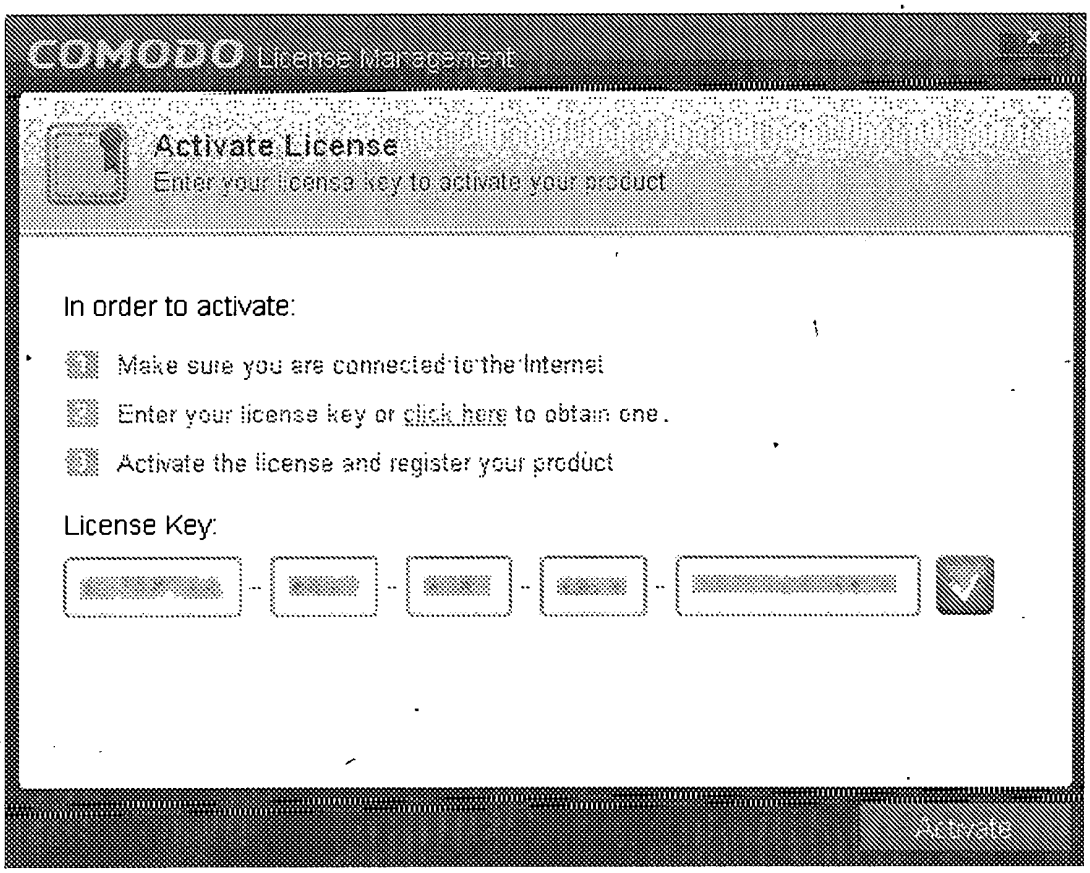


The License Activation Wizard will start.

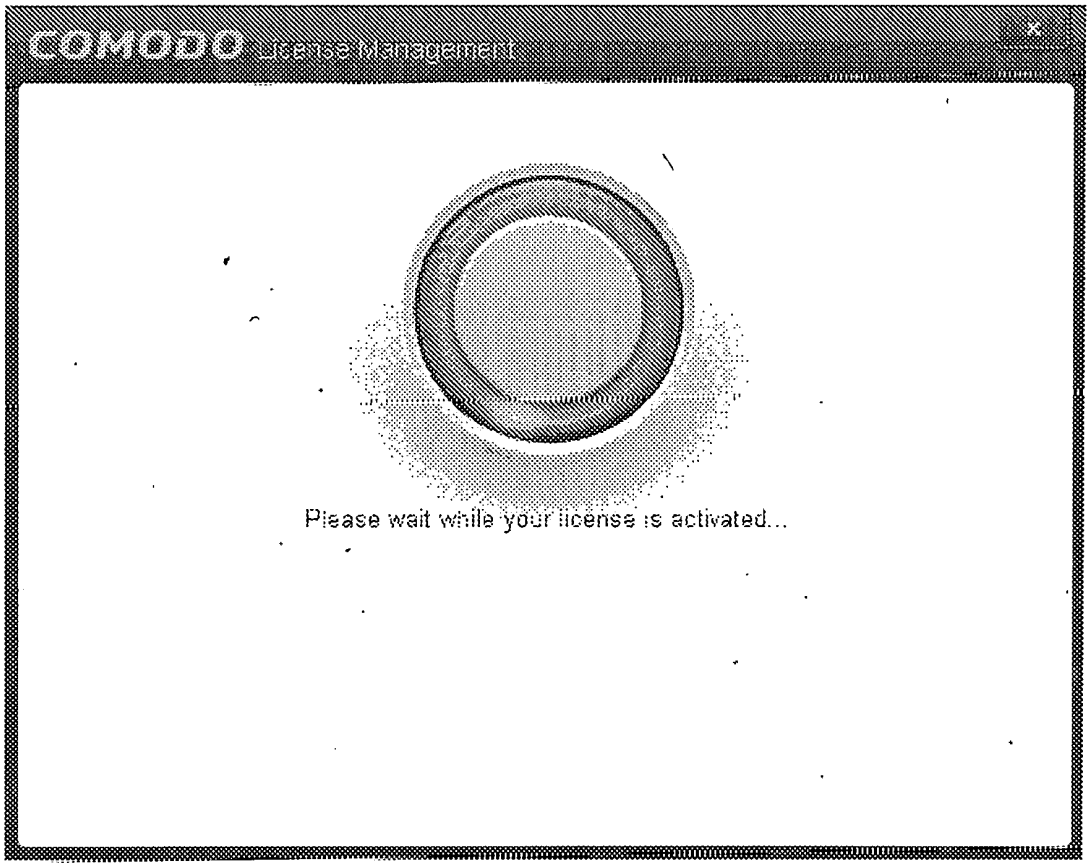


- You should have received your License key through email if you have purchased CIS Pro. For CIS Complete, the license key is available on the DVD itself or printed on an insert included in the box packaging. Enter the license key and click 'Activate'.

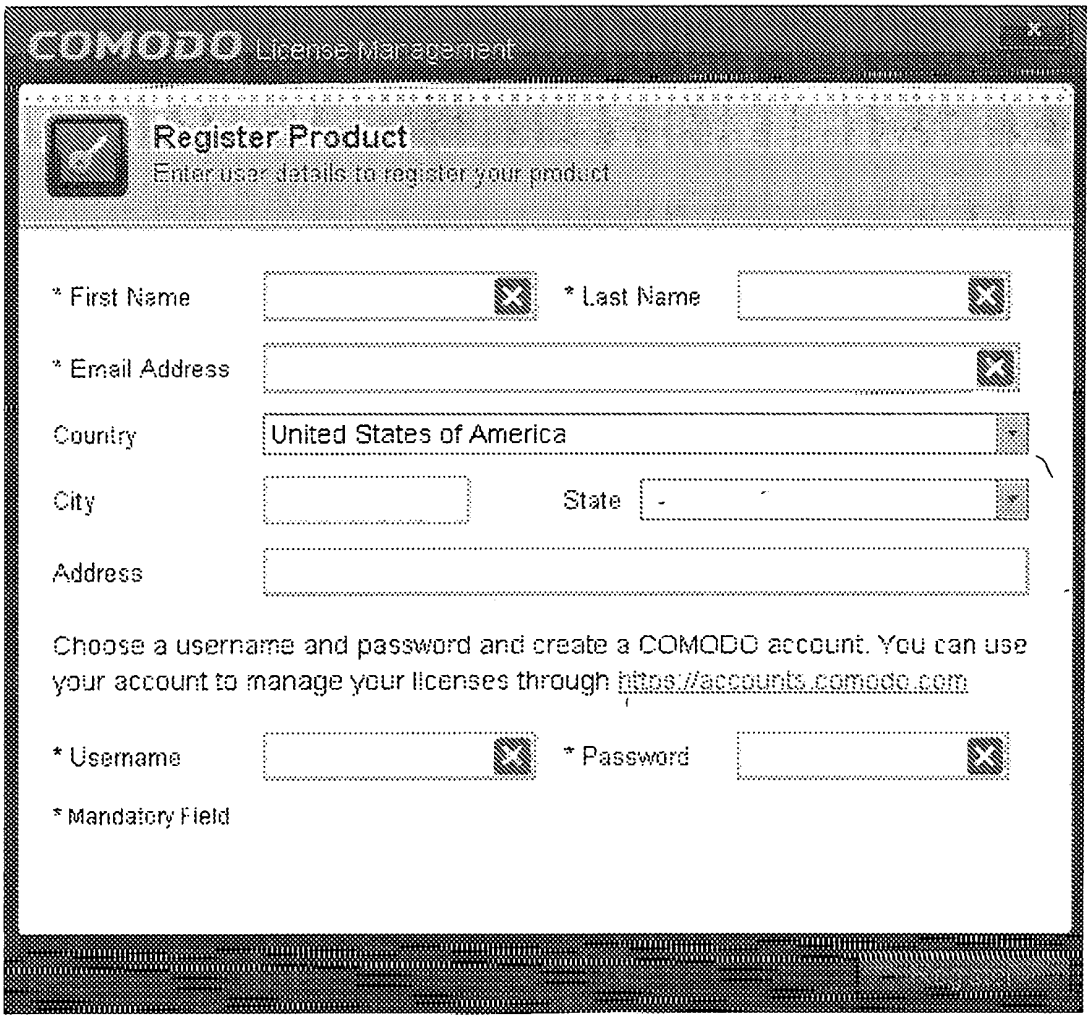
Tip: If you haven't subscribed for Comodo Internet Security - Pro or Complete so far, click the 'click here' link. You will be taken to the Comodo website enabling you to purchase the license.



- The wizard starts validating your key.



If you have not registered as an user in Comodo Accounts Manager (CAM), the following screen will be displayed.



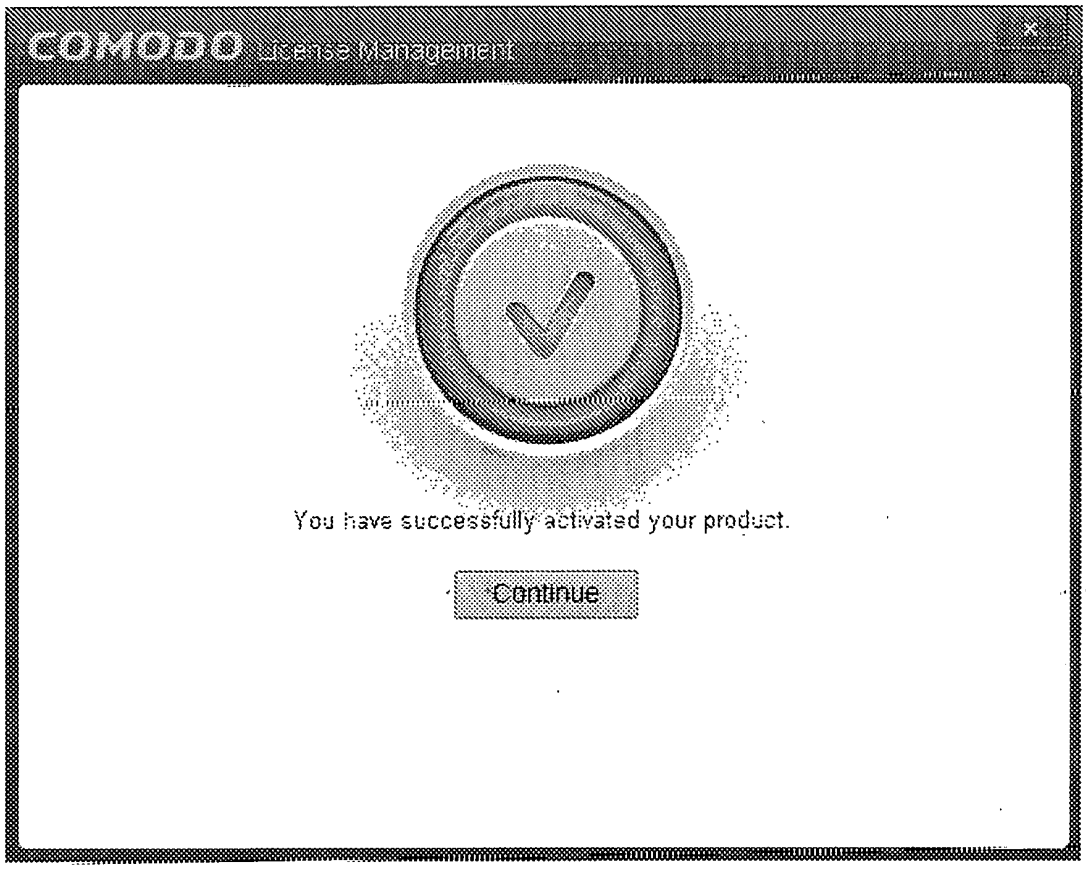
- Fill up the registration form with the login details and password for your Comodo Accounts Manager (CAM) account.



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

- Click 'Register'

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



- Click 'Continue' to exit the wizard.

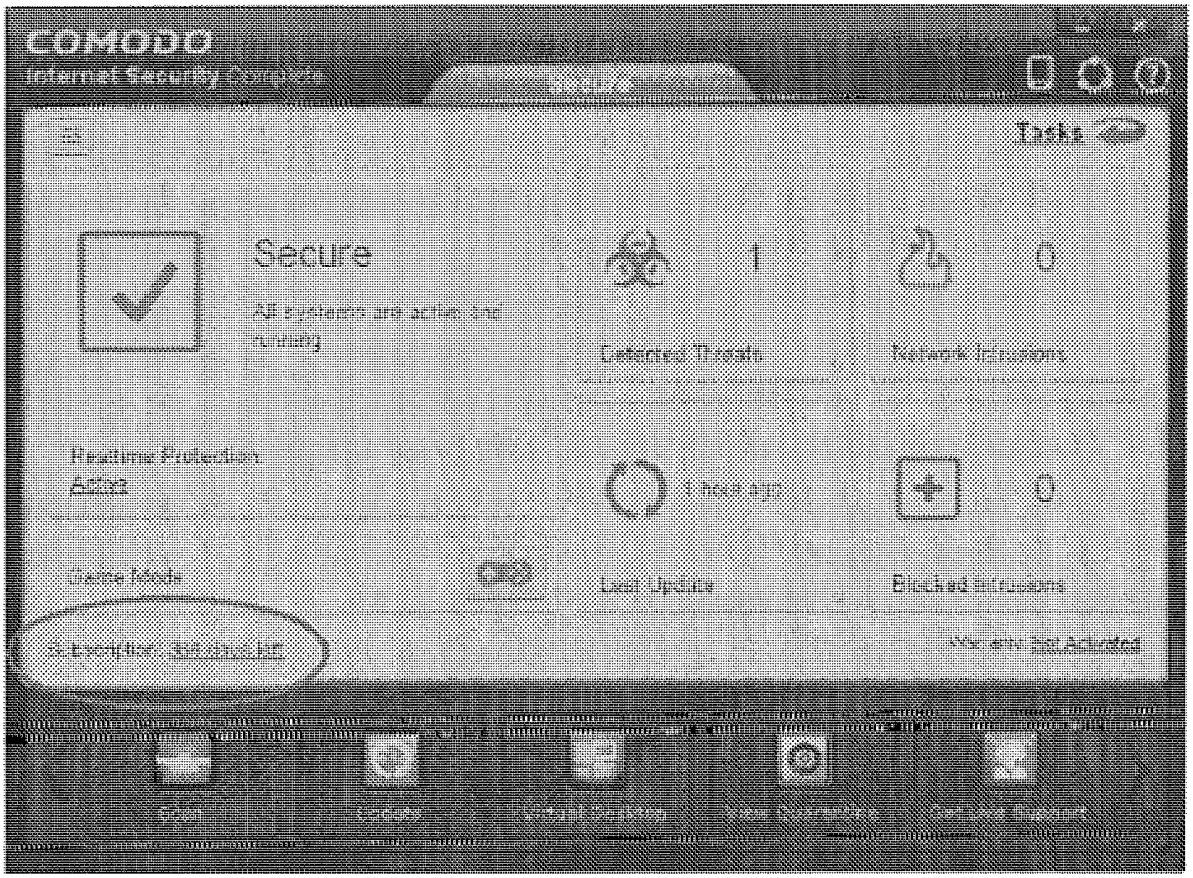
For CIS Pro users - Your CIS Pro product will be activated.

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

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

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

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



1.3.4.2. Activating Your Guarantee Coverage

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

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

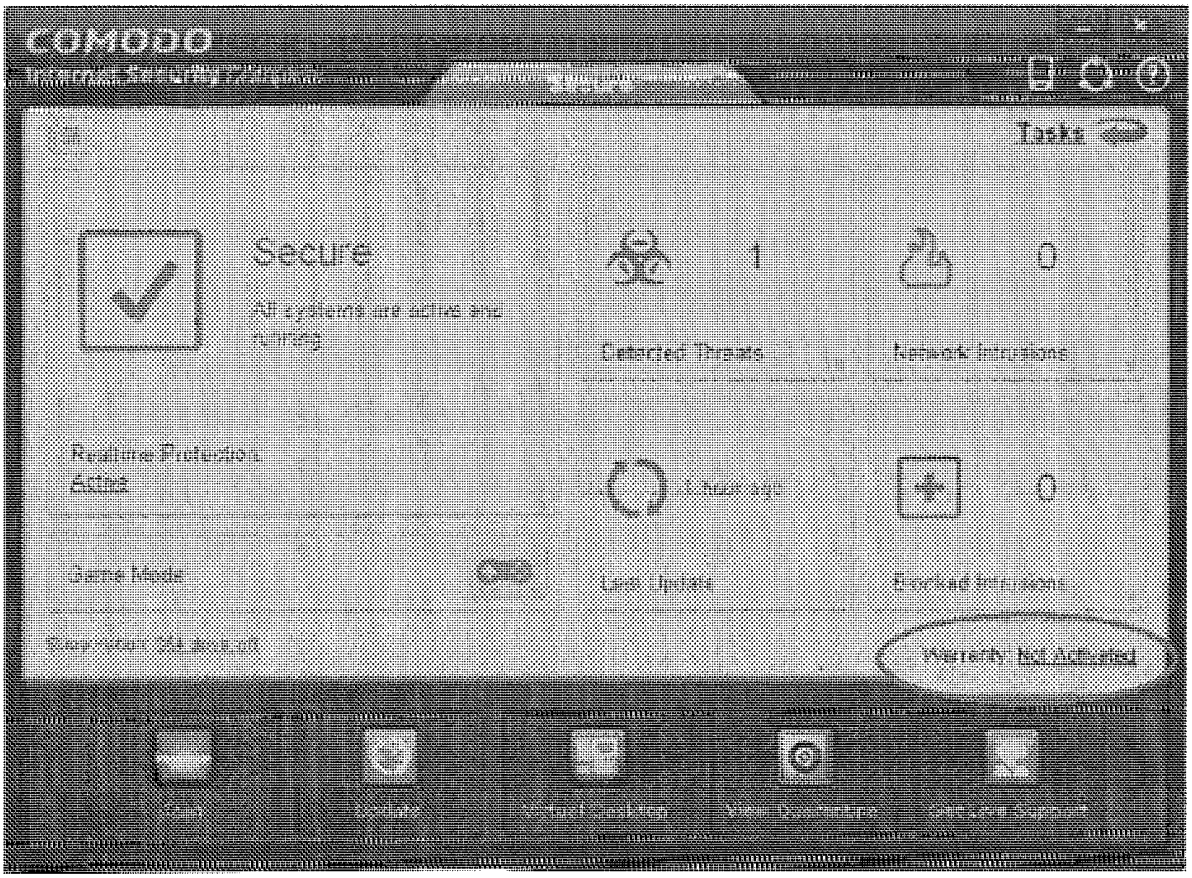
Limits: The guarantee is limited to the lesser of:

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

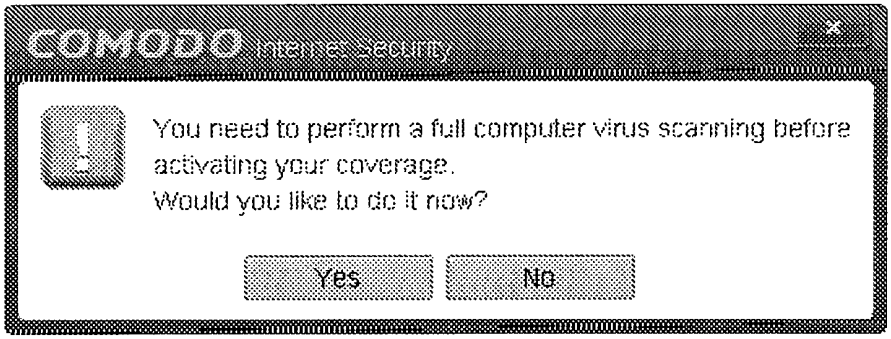
- The guarantee is limited to repairing the computer over the Internet to an operational state and excludes all claims for lost or expected profits, lost or corrupted data, lost or deleted work, or lost or damaged personal files. Comodo does not guarantee against the loss of any file or information.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

more details on running an Antivirus Scan Click here.

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



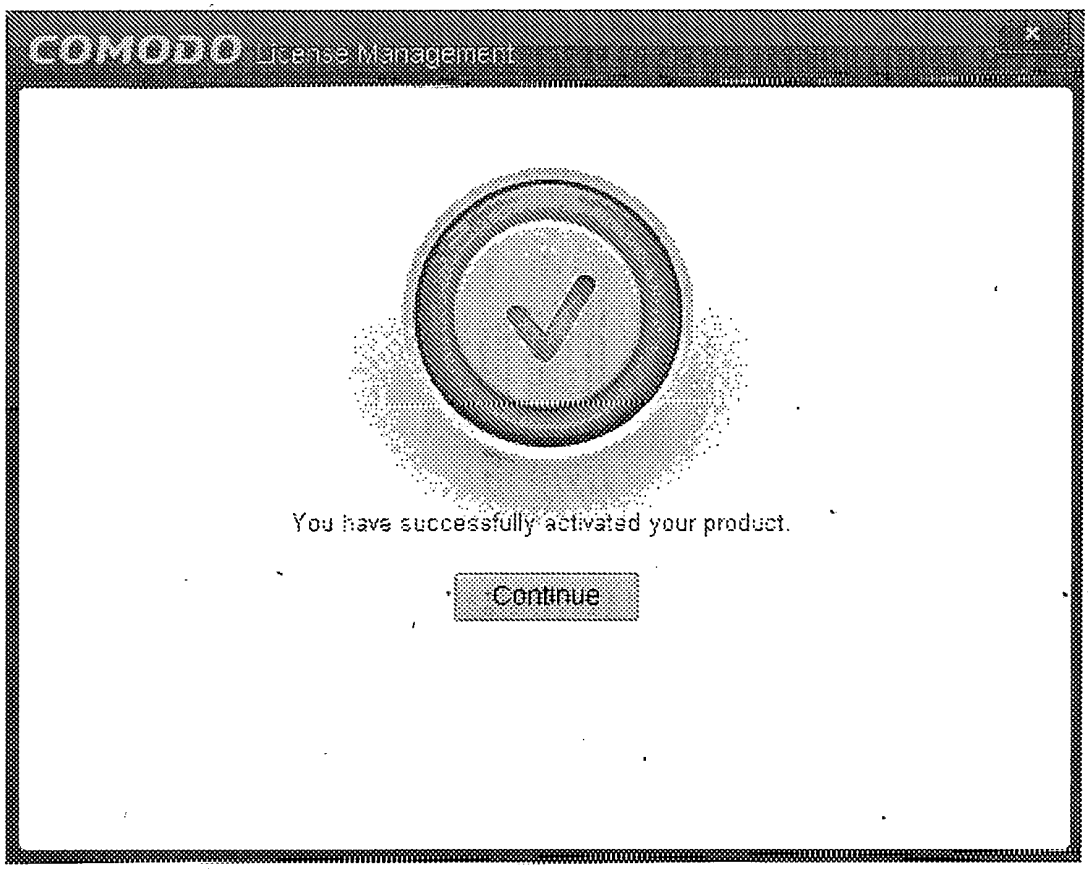
A full system scan to remove all known viruses is a mandatory requirement if your computer is to be eligible for guarantee coverage. If this step has already been performed (and your system is clean), then the process moves to step 2.



Click 'Yes' to run a full computer scan. Refer to the section Run a Full Computer Scan for more details on scanning your full computer and cleaning the infected files. All the infections and threats identified during the scan should be cleaned for your computer to be qualify for the warranty.

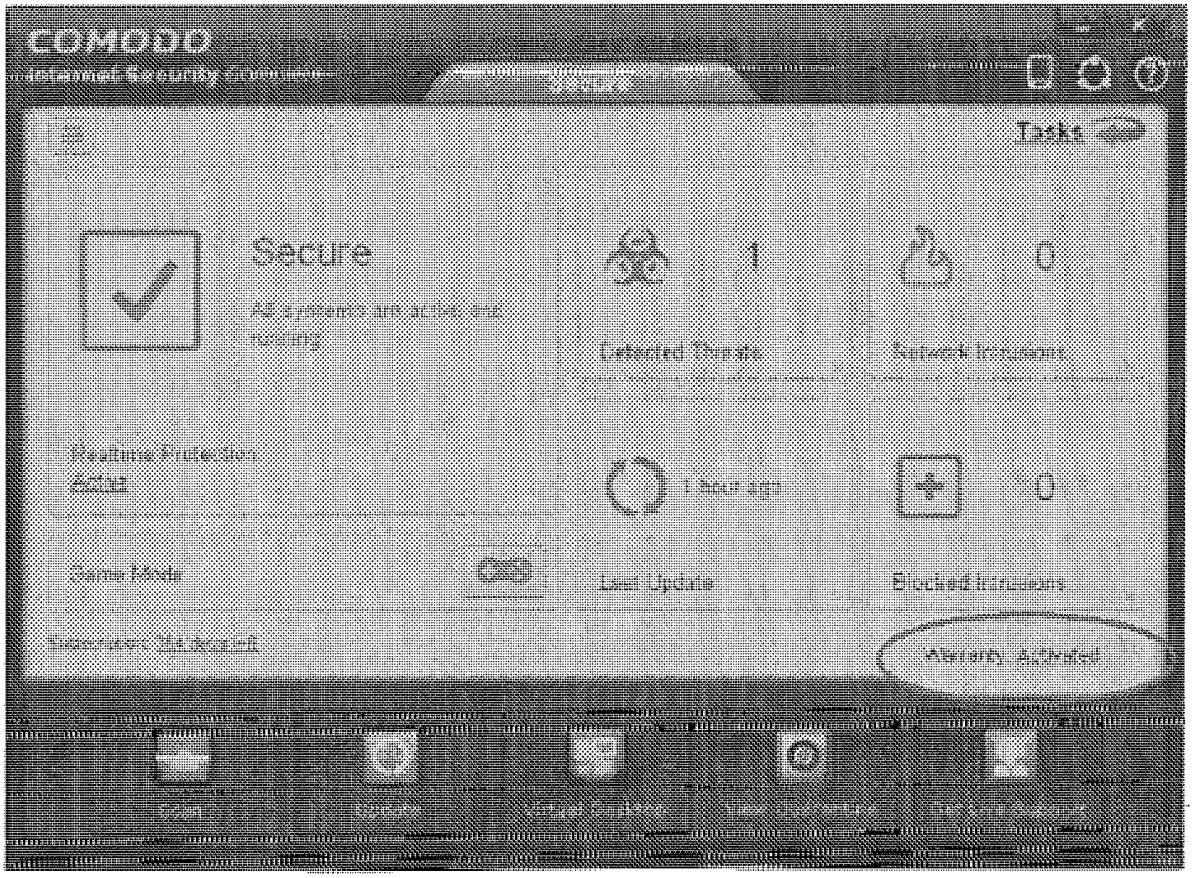
Step 2: The next stage is to run the Guarantee Activation Wizard again.

- Click 'Not Activated' beside 'Warranty:' again. The Guarantee Activation Wizard will start and on completion the 'successfully activated' screen will be displayed.



- Click 'Continue' to complete the activation wizard

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

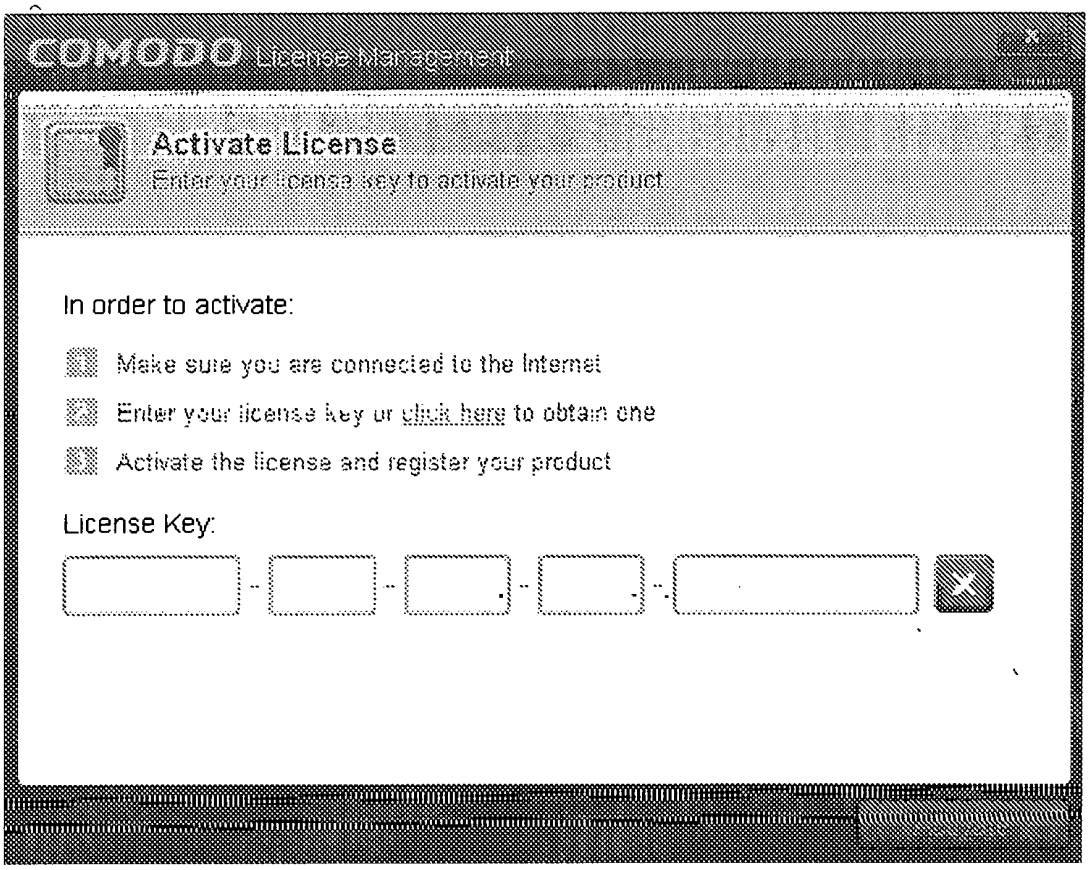


1.3.4.3. Renewal of Your License

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

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

The Product Activation Wizard will start.



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

1.4. Starting Comodo Internet Security

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

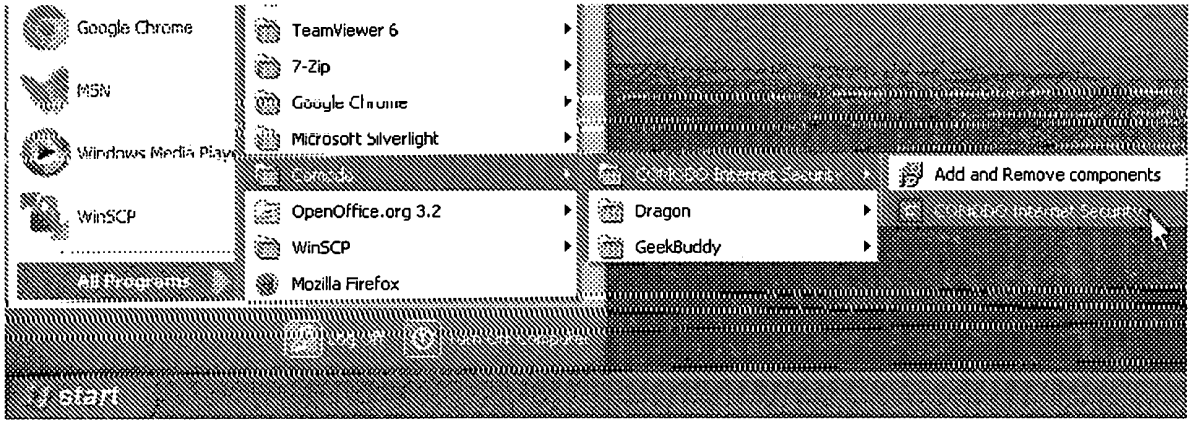
There are 4 different ways to access the main interface of Comodo Internet Security:

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

Start Menu

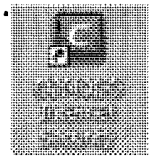
You can access Comodo Internet Security via the Windows Start Menu.

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



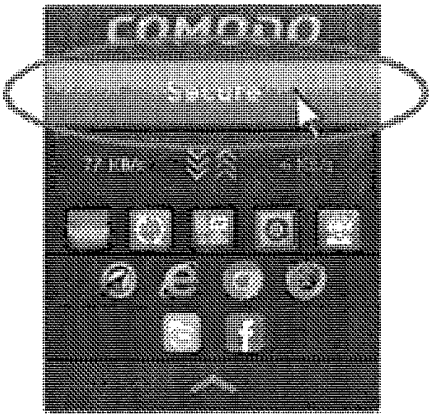
Windows Desktop

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



Widget

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



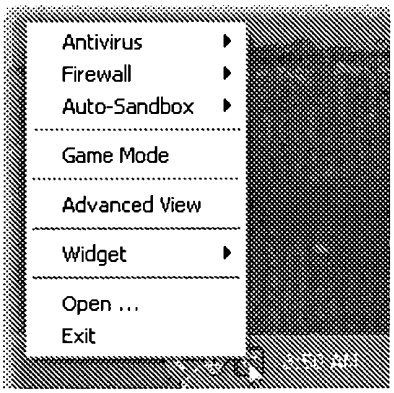
You can also view other details in the widget such as inbound and outbound traffic, number of tasks running, shortcuts to common CIS tasks and browsers and links to social media sites Twitter and Facebook. Refer to the section 'The Widget' for more details.

CIS Tray Icon

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



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



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

In game mode:

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

Deactivate Game Mode to resume alerts and scheduled scans.

Widget - Click here for more details on CIS Widget.

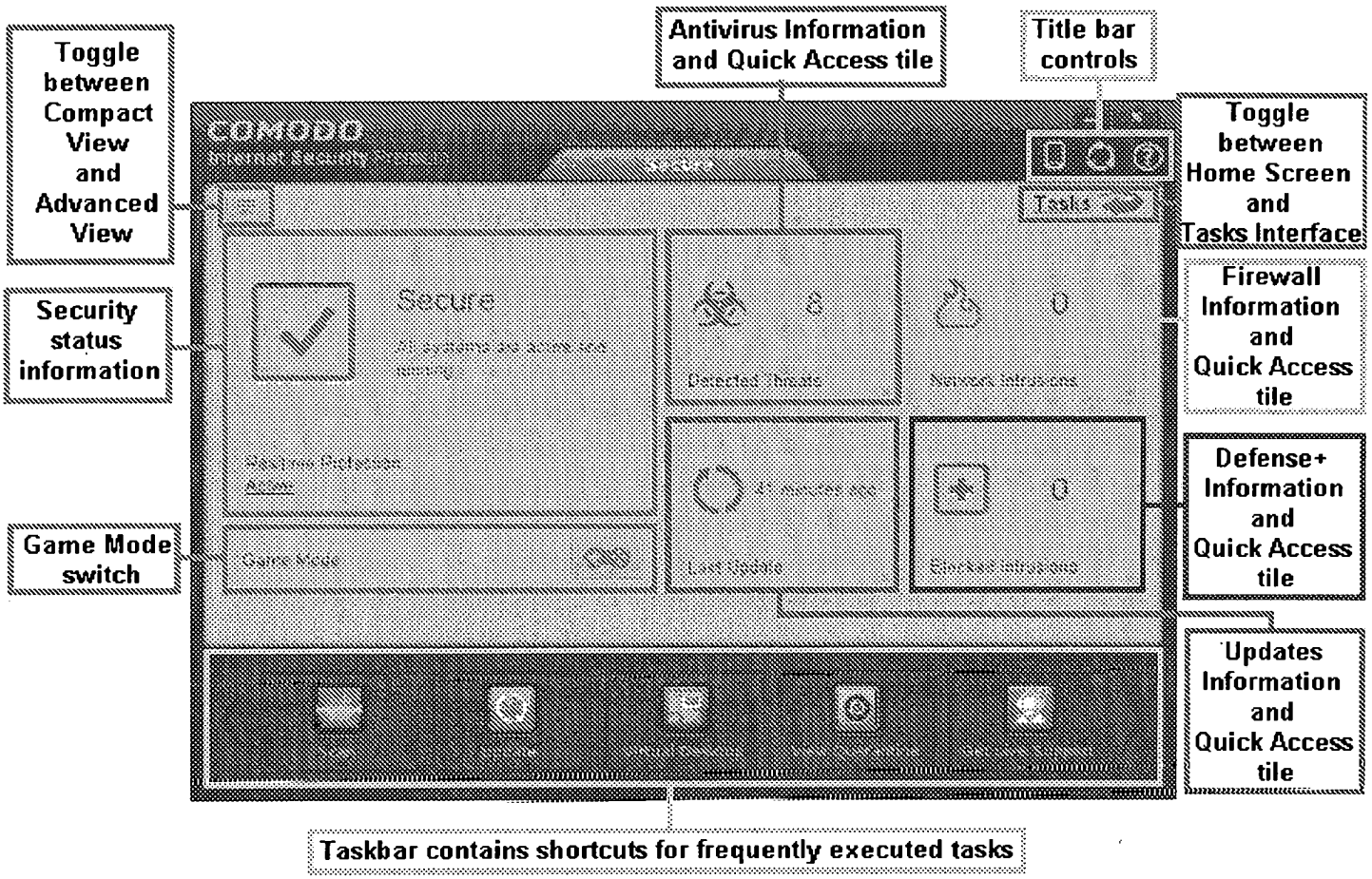
Refer to the section "The System Tray Icon for more details.

1.5. The Main Interface

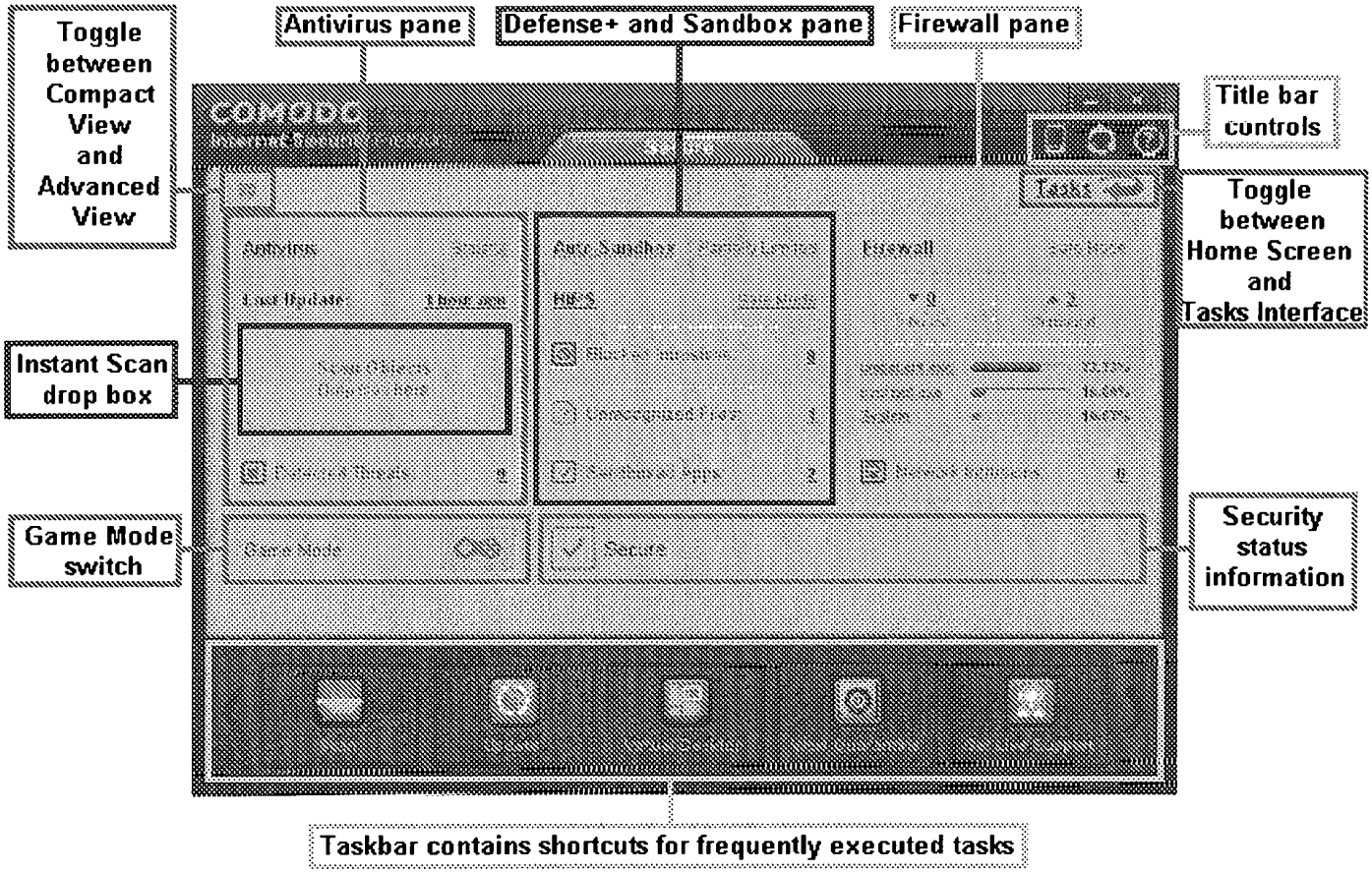
The CIS interface is designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.

- Click the curved arrow at the upper right to switch between the home screen and the tasks interface.
- Instantly run a virus scan on a file or folder by dragging it into the scan box.
- Switch on 'Game Mode' to make sure nothing interrupts you while you play a full screen game.
- Change the entire look and feel of the home screen from Advanced Settings.
- The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the Virtual Desktop, the update checker and the CIS Task Manager.
- Flip between 'Compact View' and 'Advanced View' by using the toggle button at the upper left  or from the system tray icon

Compact View



Advanced View



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

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

Click the following links for more information:

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

1.5.1. The Home Screen

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

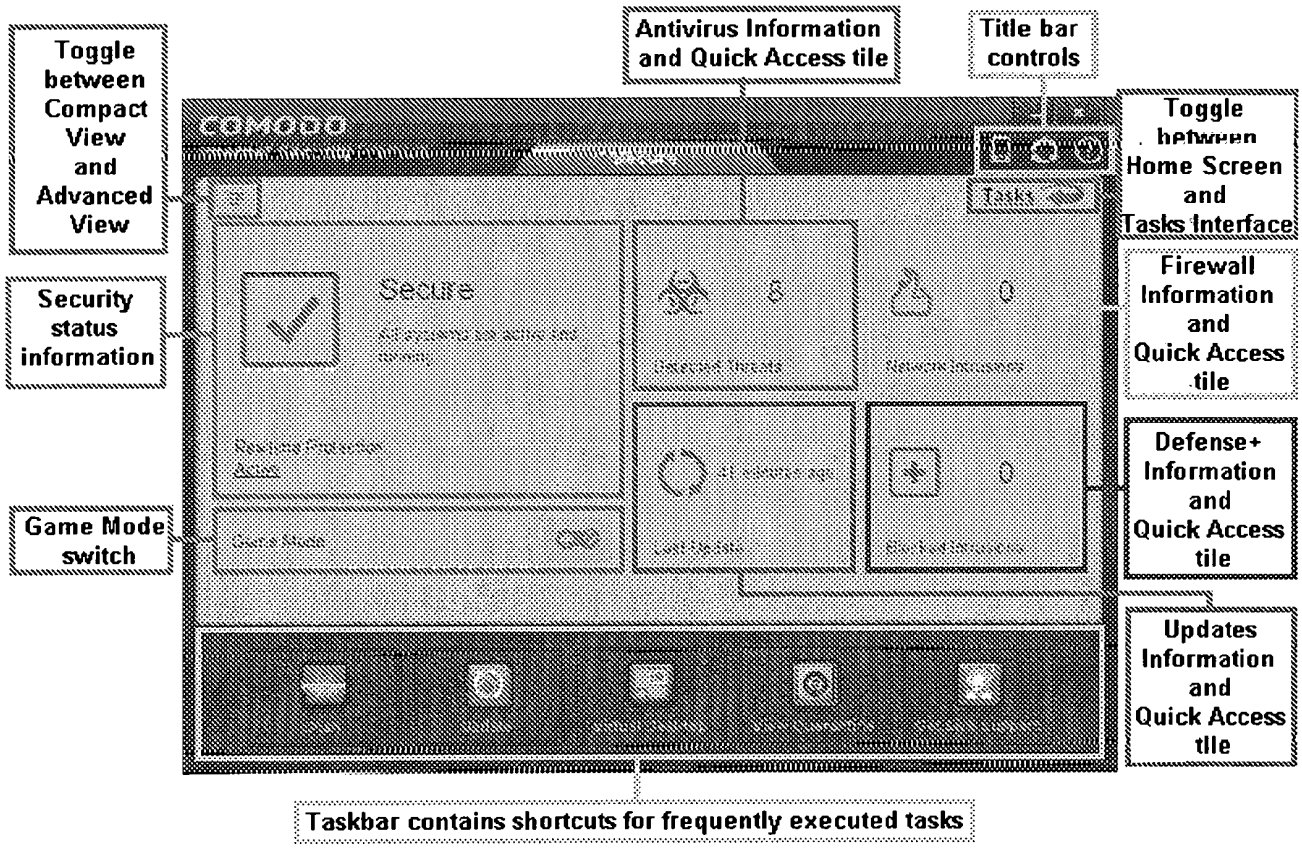
The home screen itself is available in two formats, 'Compact' view and 'Advanced' view. Use the button at the top-left to switch between them. 

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

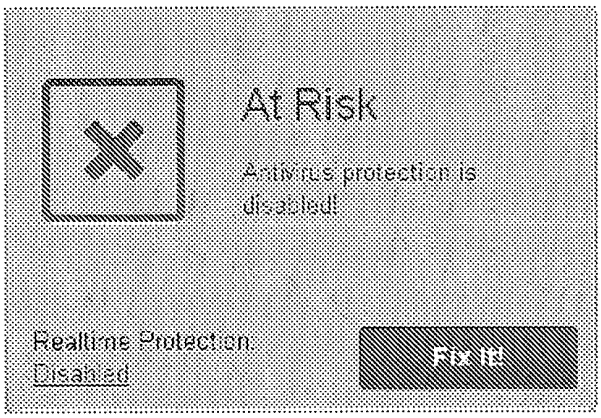
- Adding tasks to the Task Bar
- Title bar controls
- Game mode

Compact View

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



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



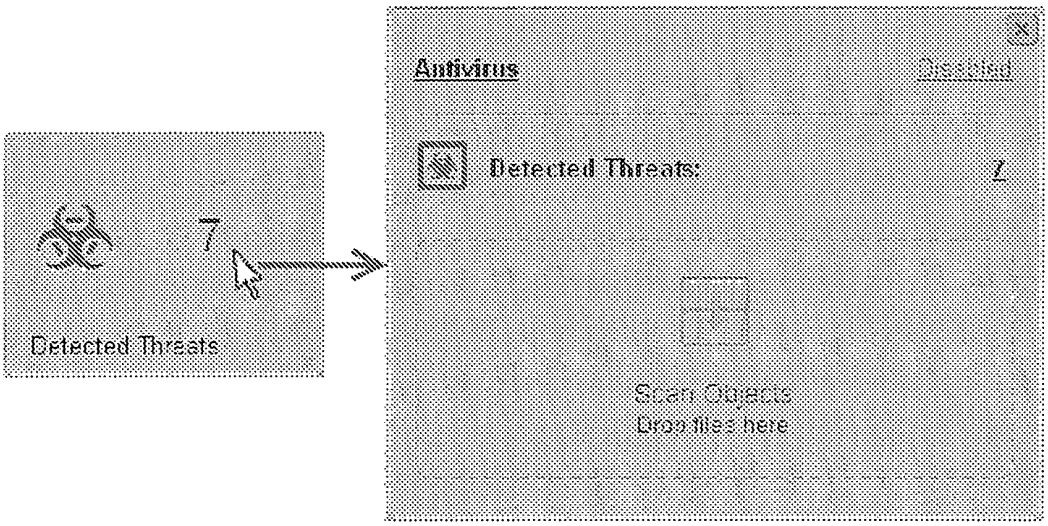
You can easily rectify the issue by clicking the 'Fix it!' button. CIS will automatically take necessary actions to resolve the problem.

From the Compact View of the home screen you can:

- Instantly scan objects
- Enable or disable security components

Instantly scan objects

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

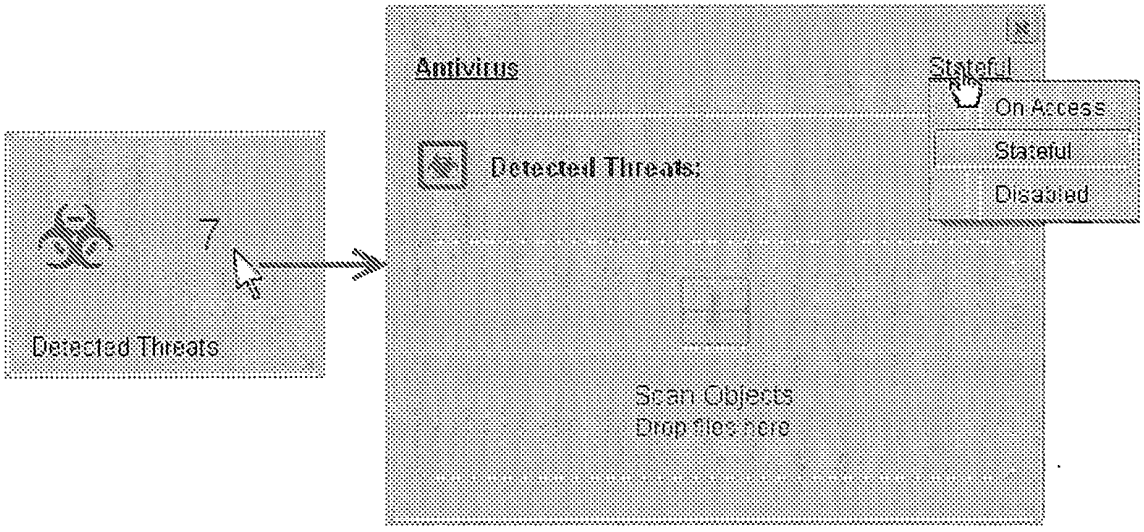


To run an instant scan, navigate to the file/folder that you want to scan and just drag-and-drop the file into the 'Scan Objects' box. The virus scan will commence immediately. Refer to 'Instantly Scan Individual Files and Folders' for more details.

Enable or disable security components

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

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

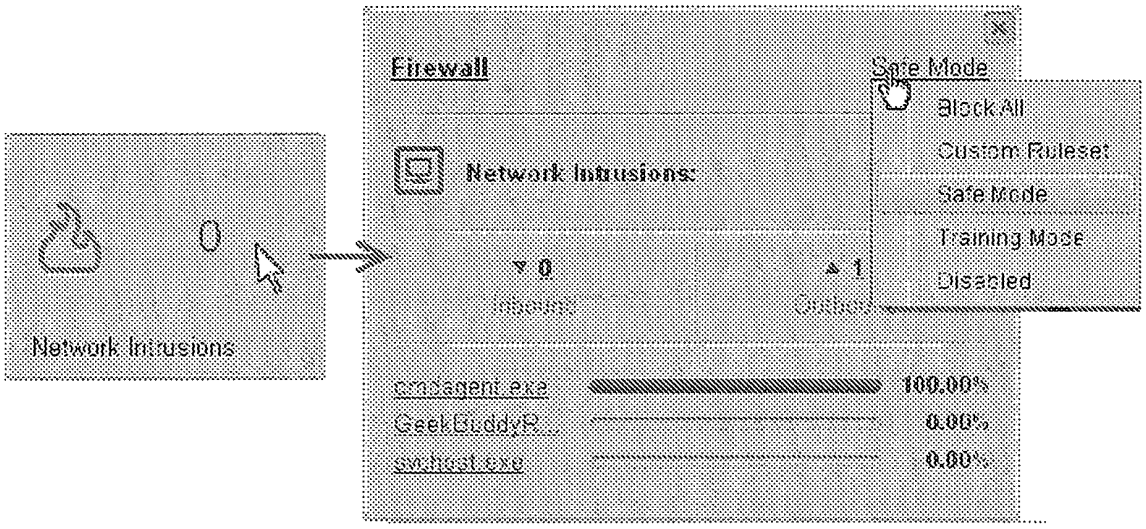


- Click 'Antivirus' at upper-left to open the 'Realtime Scanner Settings' interface. Refer to the section 'Real-

time Scanner Settings' for more details.

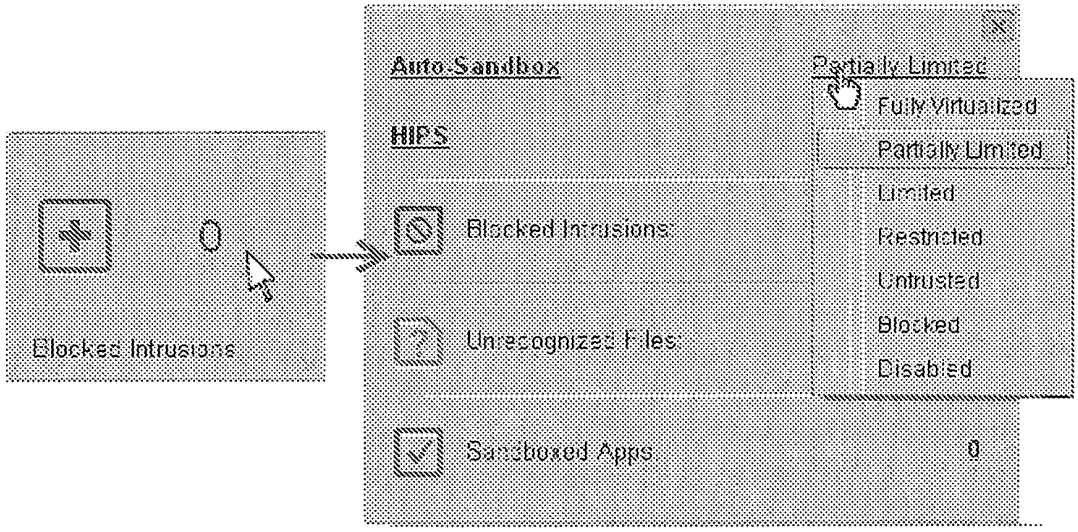
- Click the number of threats detected to open the Antivirus Log Viewer Module.
- Click the 'X' in the top right corner to return to the 4-tile view.

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

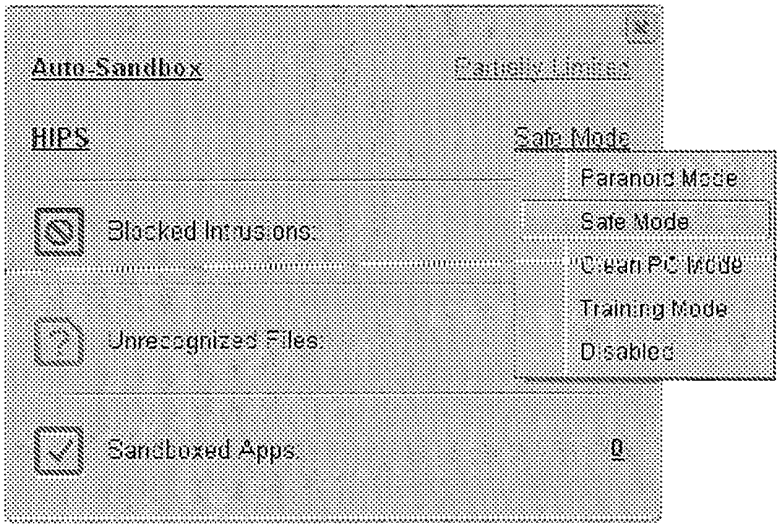


  - Click 'Firewall' to open the detailed 'Firewall Settings' interface. Refer to the section 'Firewall Behavior Settings' for more details.
  - Click the number of detected network intrusions to open the Firewall Log Viewer Module.
  - Click the numbers over 'inbound' and 'outbound' to open the View Connections dialog. You can also do this by clicking the application names at the bottom of the pane.
  - Click the 'X' in the top right corner to return to the 4-tile view.

- **Defense+** - Click the Defense+ tile to flip open a more detailed pane which displays the current Auto-Sandbox and HIPS modes and a statistical summary of events handled by the Behavior Blocker component.
  - Click **Auto-Sandbox** to open the Behavior Blocker Settings interface. Refer to the section 'Behavior Blocker' for more details.
  - Click the link to the right of this to view and modify auto-sandbox security levels. Refer to the section 'Behavior Blocker' for more details.

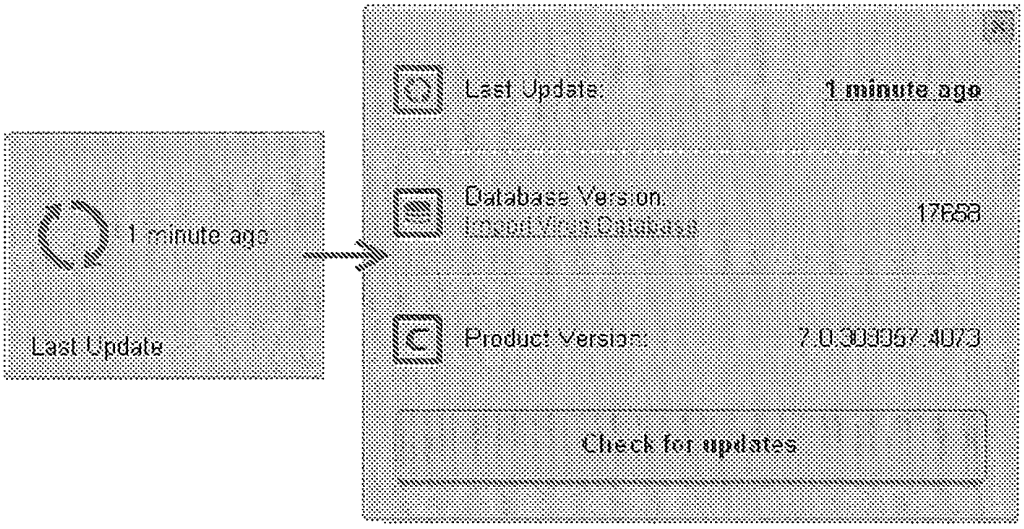


- Click **HIPS** to open the 'HIPS Settings' interface. Refer to the section 'HIPS Behavior Settings' for more details.
- Click the link to the right of this to view and modify HIPS security modes. Refer to the section 'HIPS Behavior Settings' for more details.



- Click the number of Blocked Intrusions to open the Defense+ Log Viewer module.
- Click the number of Unrecognized Files to open the Unrecognized Files interface.
- Click the number of Sandboxed Apps to open the Active Process List dialog.

- **Updates** - Click the 'Updates' tile to open a more detailed pane which displays when the virus database was last updated, the database version number and the software version number.

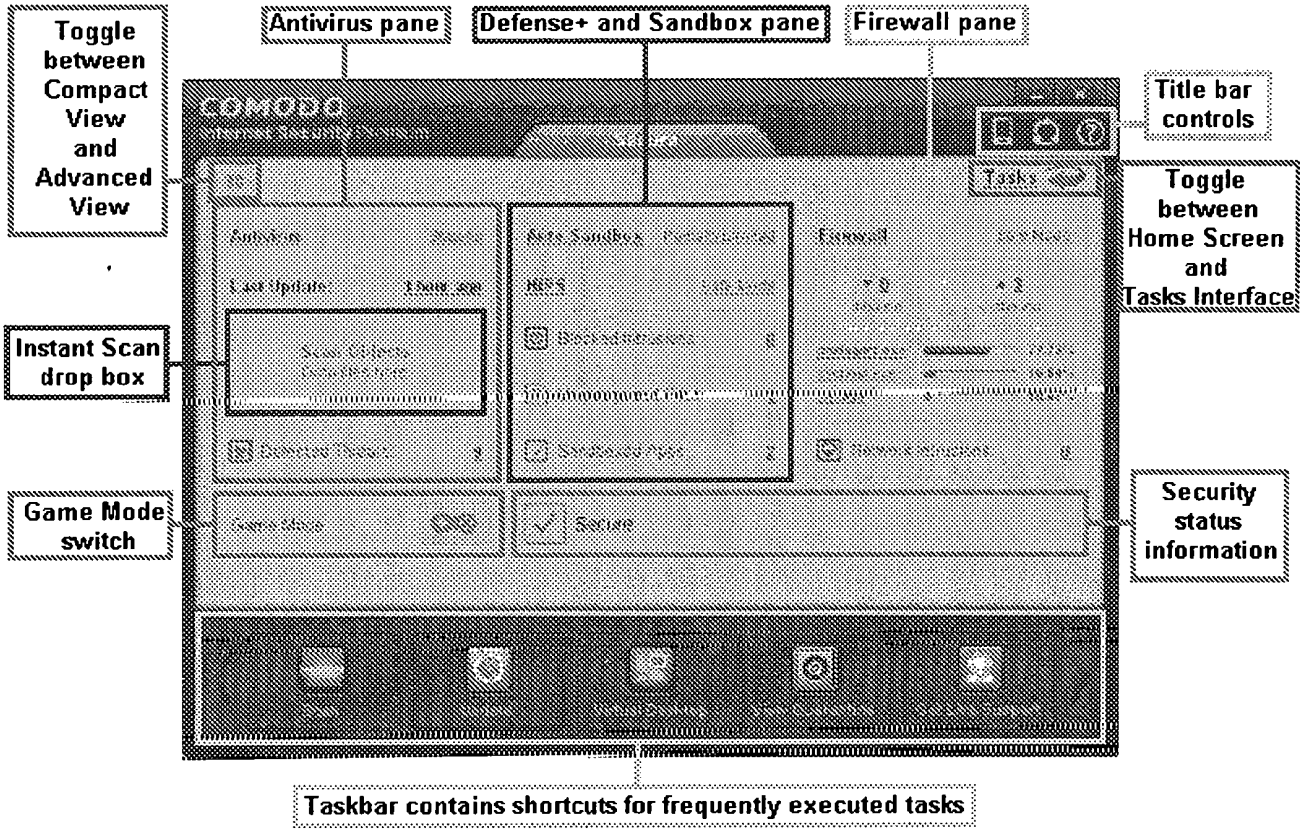


- Click on either the time of the last update or the 'Check for Updates' button to manually check for available updates. Refer to the section Manage Virus Database and Product Updates section for more details.
- Click the 'X' in the top right corner to return to the 4-tile view.

Advanced View

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

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



Click the following links to find out more:

- Antivirus Pane
- Defense+ and Sandbox Pane
- Firewall Pane

Antivirus Pane

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

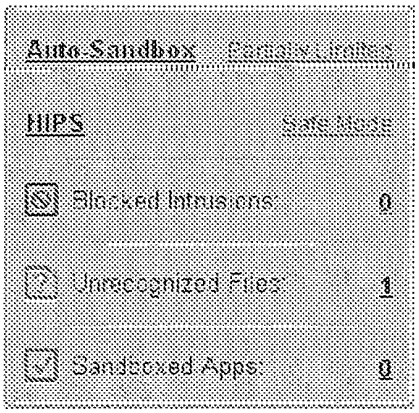


- **Antivirus** - Displays the current security level of the real-time antivirus scanner. Click on the security mode text to quickly switch between modes. Click 'Antivirus' to open the Realtime Scanner Settings interface. Refer to the section 'Real-time Scanner Settings' for more details.
- **Last Update** - Displays when the virus database was updated. Click the text link to start the updates again.

- **Detected Threats** - Displays the number of malware threats discovered so far from the start of current session as a link. Clicking this number will open the Antivirus Logs panel.
- **Scan Objects** - Drag-and-drop files, folders or even entire drives into this box to instantly scan them. Refer to the section Instantly Scan Files and Folders for more details.

Defense+ and Sandbox Pane

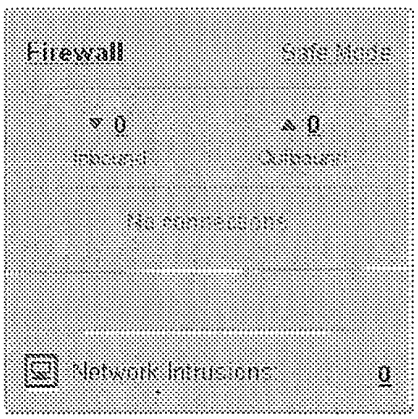
The Defense+ and Sandbox Pane allows you to quickly configure Auto-Sandbox and HIPS settings, view Defense+ logs and easily view the number of blocked intrusions, unrecognized files and sandboxed applications.



- Auto-Sandbox - Displays the current security level of the Behavior Blocker. Click on the security level itself to view or change it. Click **Auto-Sandbox** to open the 'Behavior Blocker Settings interface.' Refer to the section 'Behavior Blocker' for more details.
- **HIPS** - Click the text of the current HIPS mode to view or modify the mode. Click the word HIPS to open the 'HIPS Settings' interface. Refer to the section 'HIPS Behavior Settings' for more details.
- **Blocked Intrusions** - Displays the number of intrusions blocked by HIPS. Clicking on the numbered link will open the Defense+ logs. Refer to the section Defense+ Logs for more details.
- **Unrecognized Files** - Displays the number of files that are not recognized by CIS. These files may be considered as awaiting categorization. Clicking on the numbered link will open the Unrecognized Files screen which will allow you to run a file-lookup and to submit unknown files to Comodo for analysis. Refer to the section Unrecognized Files for more details.
- Sandboxed Apps - Displays the number of applications that are currently running inside the sandbox. Clicking the numbered link beside it will open the 'Active Processes List (Sandboxed Only)', which provides details of currently sandboxed applications. Refer to the section 'View Active Process List' for more details.

Firewall Pane

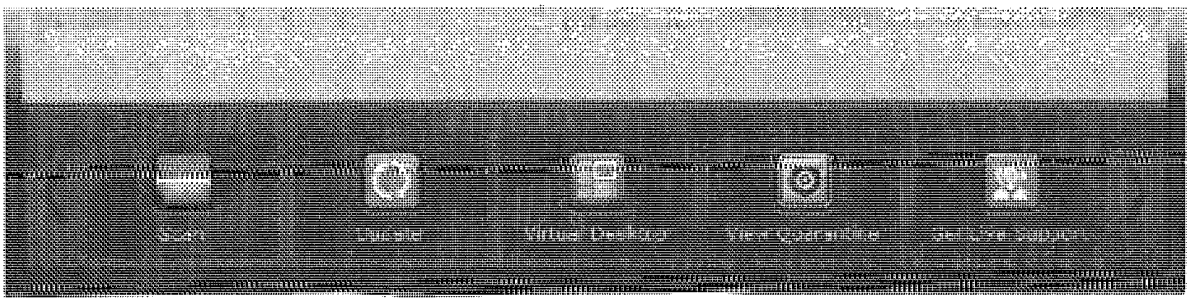
The Firewall Pane allows you to configure Firewall settings, view the number of inbound and outbound connections and the number of network intrusion attempts blocked by Firewall since the start of current session of CIS.



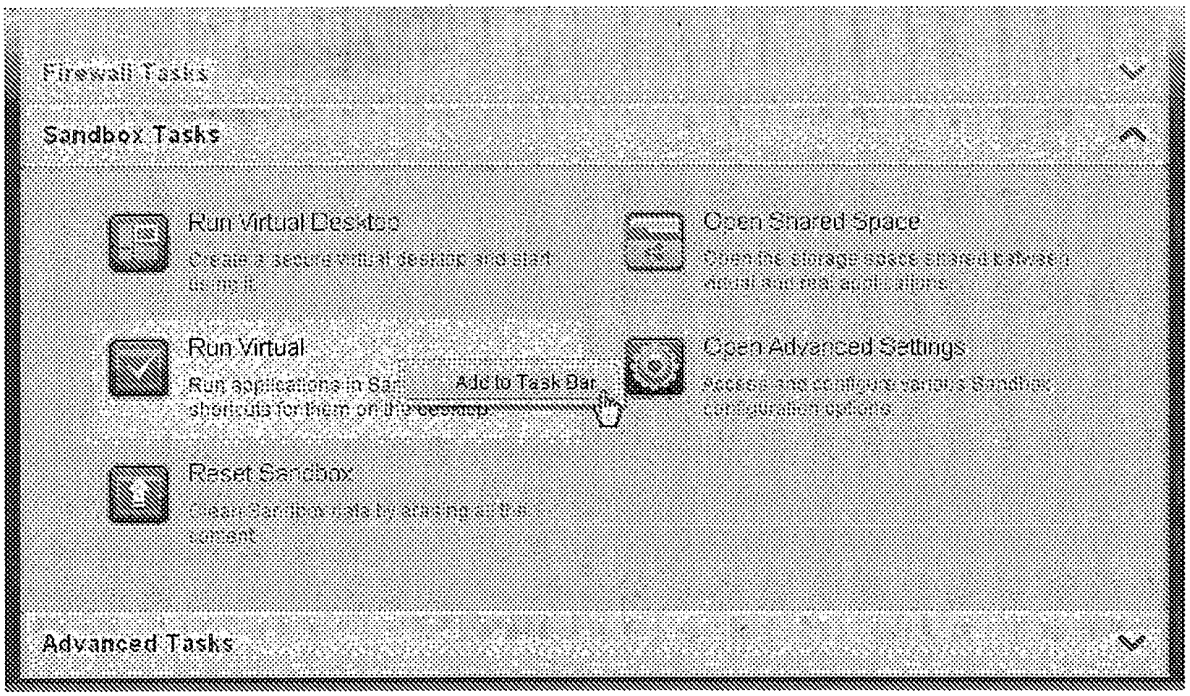
- Firewall - Displays the firewall's current security mode. Click on the level itself to quickly view and modify it. Click on '**Firewall**' to open the Firewall Settings interface. Refer to the section 'Firewall Behavior Settings' for more details.
- **Inbound / Outbound Connections** - A numerical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

Adding tasks to the Task Bar

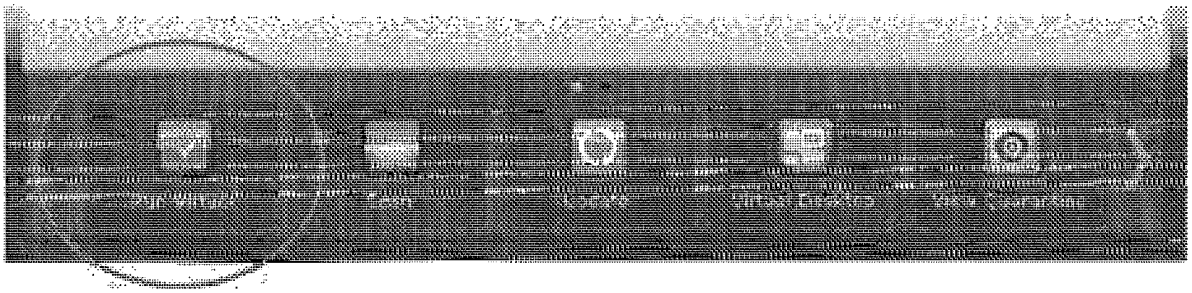
The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles < > on the left and right sides of the task bar to scroll through all tasks.



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



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



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

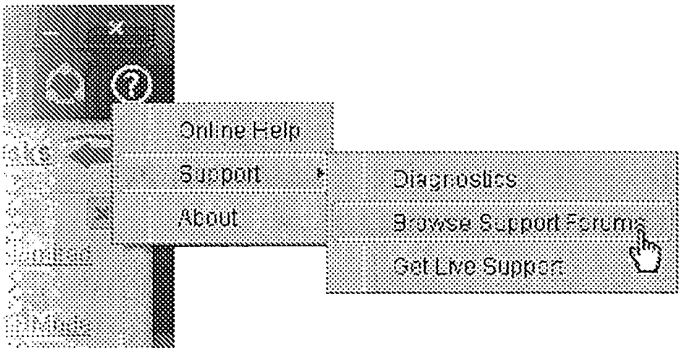
- To remove a task shortcut from the Task Bar, right click on it and choose 'Remove from task bar'.



Title bar controls

The title bar (top right) contains shortcuts for:

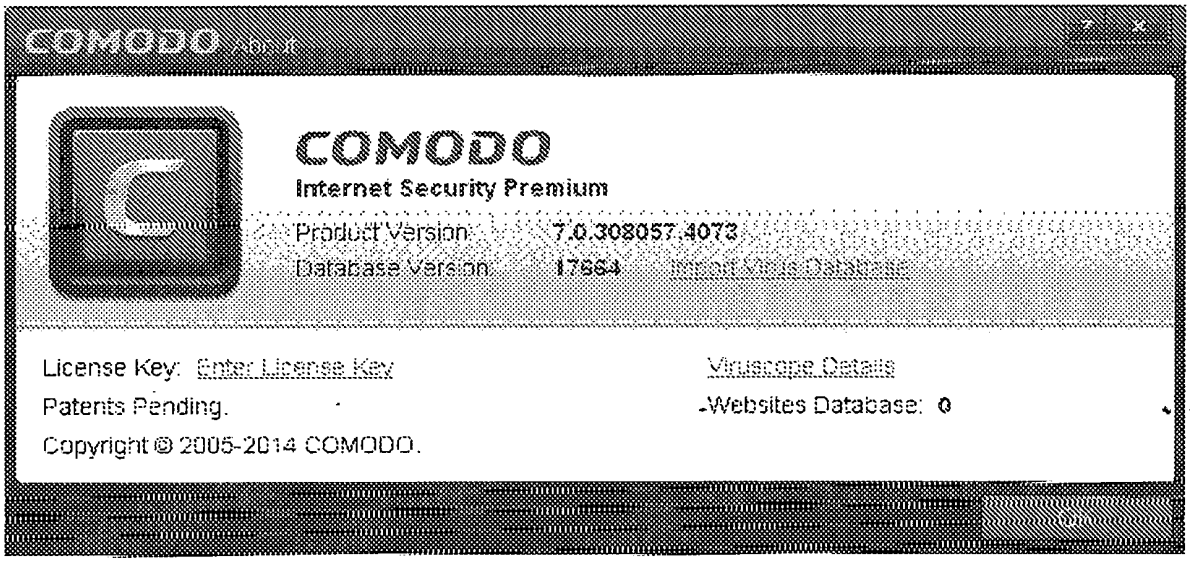
- Comodo Mobile Security app for Android phones and tablets. - Click the mobile icon and scan the QR code with your device to download the latest version of the app. You can also get the app from our website, https://m.comodo.com/ or from the Google Play app store at https://play.google.com/store/apps/details?id=com.comodo.pimsecure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



- Online Help - Opens Comodo Internet Security's online help guide at http://help.comodo.com/topic-72-1-522-6207-Introduction-to-Comodo-Internet-Security.html.
- Support - Click this link for the following options:
- Diagnostics - Helps to identify any problems with your installation.

- Browse Support Forum - Links to Comodo User Forums.
- Get Live Support - Launches the GeekBuddy support client.

- **About** - Displays the product version, virus signature database version, website database version (website filtering URLs), details of active Viruscope Recognizers and copyright information. The 'About' dialog also allows you to import a locally stored virus database and to enter a license key for CIS Pro.



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

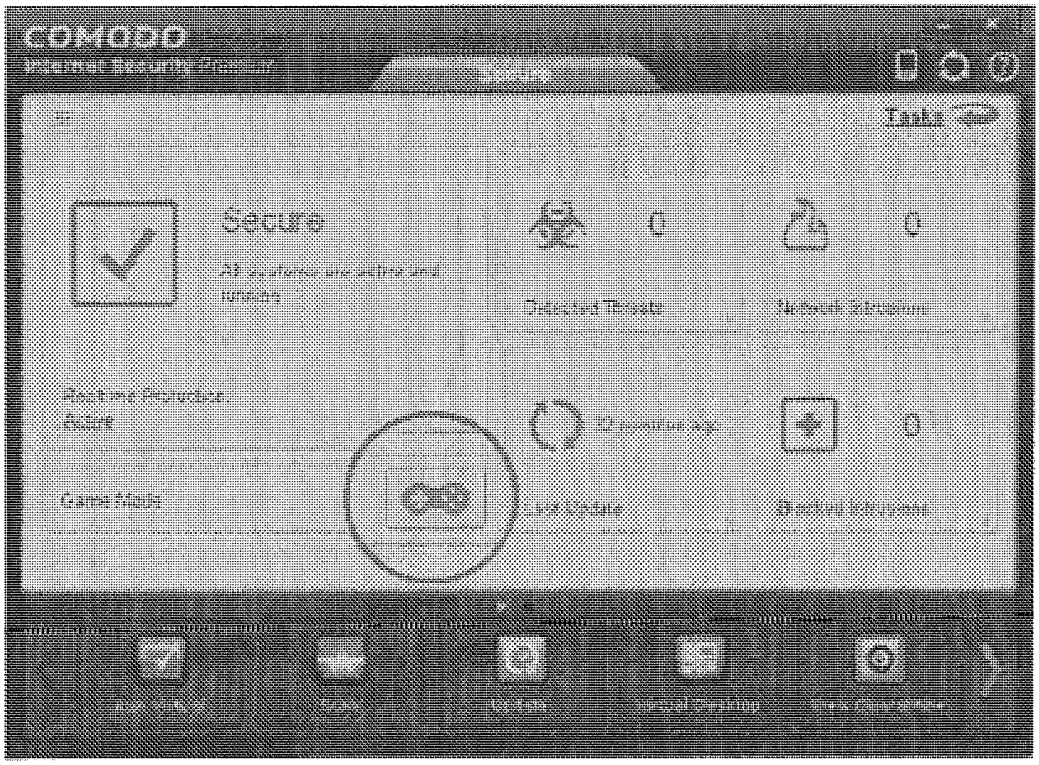
Game mode

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

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

To switch to Game mode

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



- Deactivate Game Mode to resume alerts and scheduled scans.

1.5.2. The Tasks Interface

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



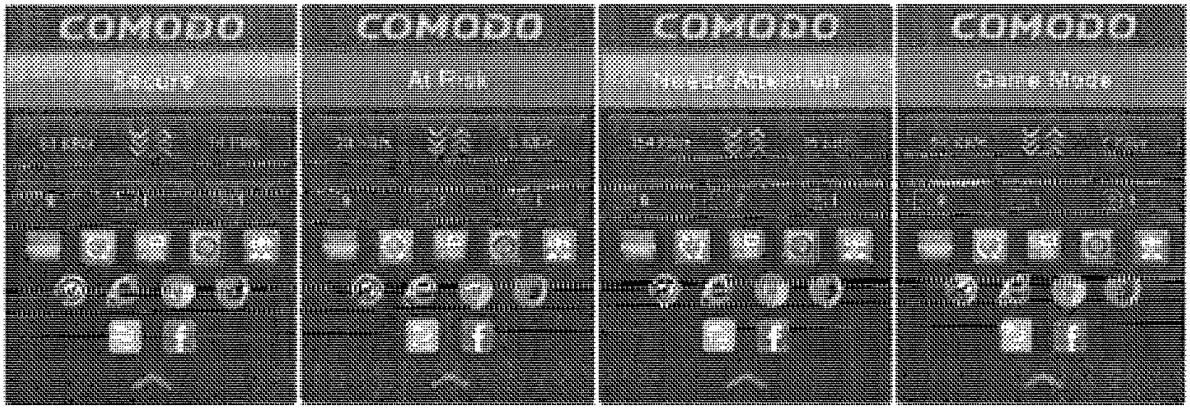
Tasks are broken down into four main sections. Click the following links for more details on each:

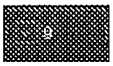
- General Tasks - Run antivirus scans, update virus database, view and manage quarantined threats, view logs of security events, activity and alerts and get live support. Refer to the section General Tasks for more details.
- Firewall Tasks - Allow or block applications, manage ports, manage networks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

1.5.3. The Widget

The CIS Widget is a handy control that lives on your desktop and provides at-a-glance information about overall security status, inbound and outbound traffic, sandboxed applications, unrecognized files and more. The Widget starts automatically with CIS unless it is disabled from the System Tray Icon or in the 'User Interface' of General Settings.

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

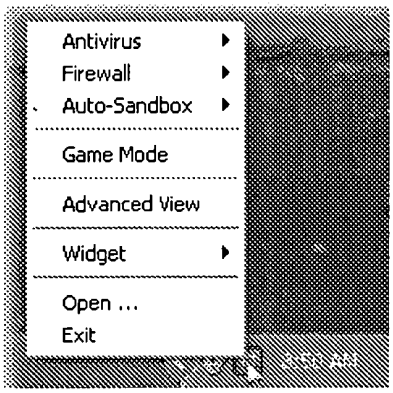


- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' opens the appropriate interface for you to take action immediately.
- The second row displays information about incoming and outgoing network traffic. The network traffic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

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

1.5.4. The System Tray Icon

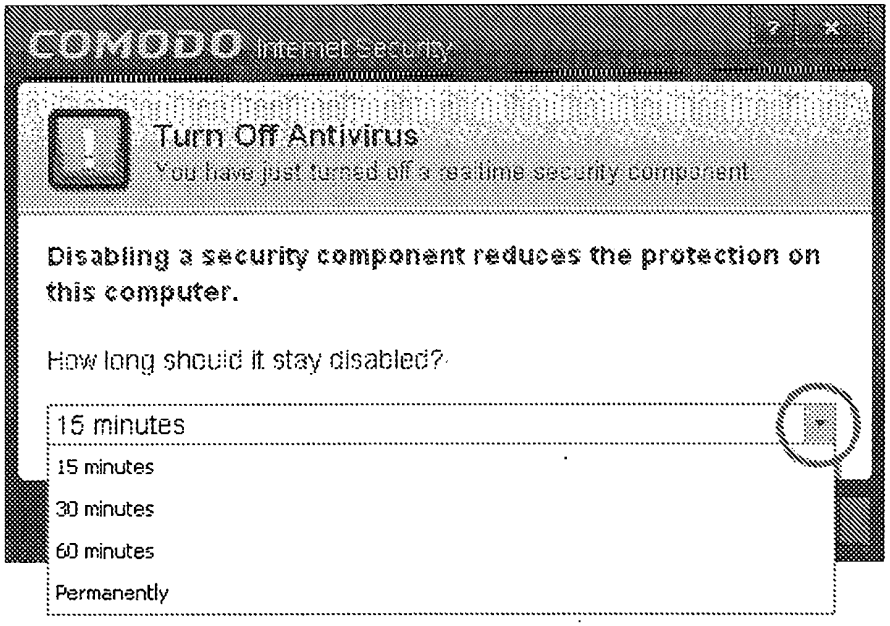
Double-clicking the system tray icon  will quickly open the CIS interface. Right-clicking the icon opens a context sensitive menu that allows you to configure various application settings:



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

Compact View	Advanced View
Antivirus - You can enable or disable Real-time antivirus scan. **Firewall** - You can enable or disable Firewall. **Auto-Sandbox** - You can enable or disable Auto-Sandbox. Refer to the section 'Behavior Blocker' for more details.	**Antivirus** - Options available are On Access, Stateful and Disabled. Refer to Antivirus Pane for more details. **Firewall** - Options available are Block All, Custom Ruleset, Safe Mode, Training Mode and Disabled. Refer to the section 'Firewall Behavior Settings' for more details. **Auto-Sandbox** - Options available are Fully Virtualized, Partially Limited, Limited, Restricted, Untrusted, Blocked and Disabled. Refer to the section 'Behavior Blocker' for more details. **HIPS** - Options available are Paranoid Mode, Safe Mode, Clean PC Mode, Training Mode and Disabled. Refer to the section HIPS Behavior Settings for more details.

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



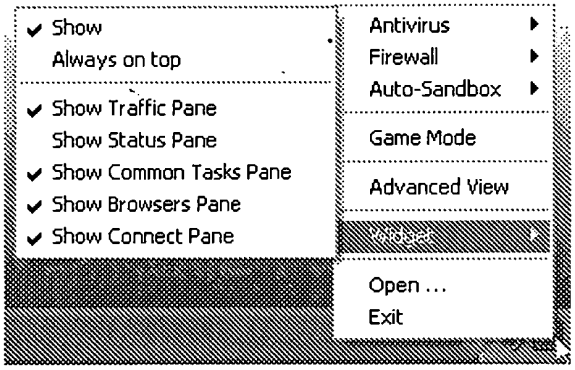
Select the period and click 'OK'. Unless you have selected 'Permanently', the security component will be automatically re-enabled after the stated time period has elapsed. You can, of course, manually re-enable at any time by right-clicking the tray icon and selecting 'Enable' for the component in question.

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

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

Deactivate Game Mode to resume alerts and scheduled scans.

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



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

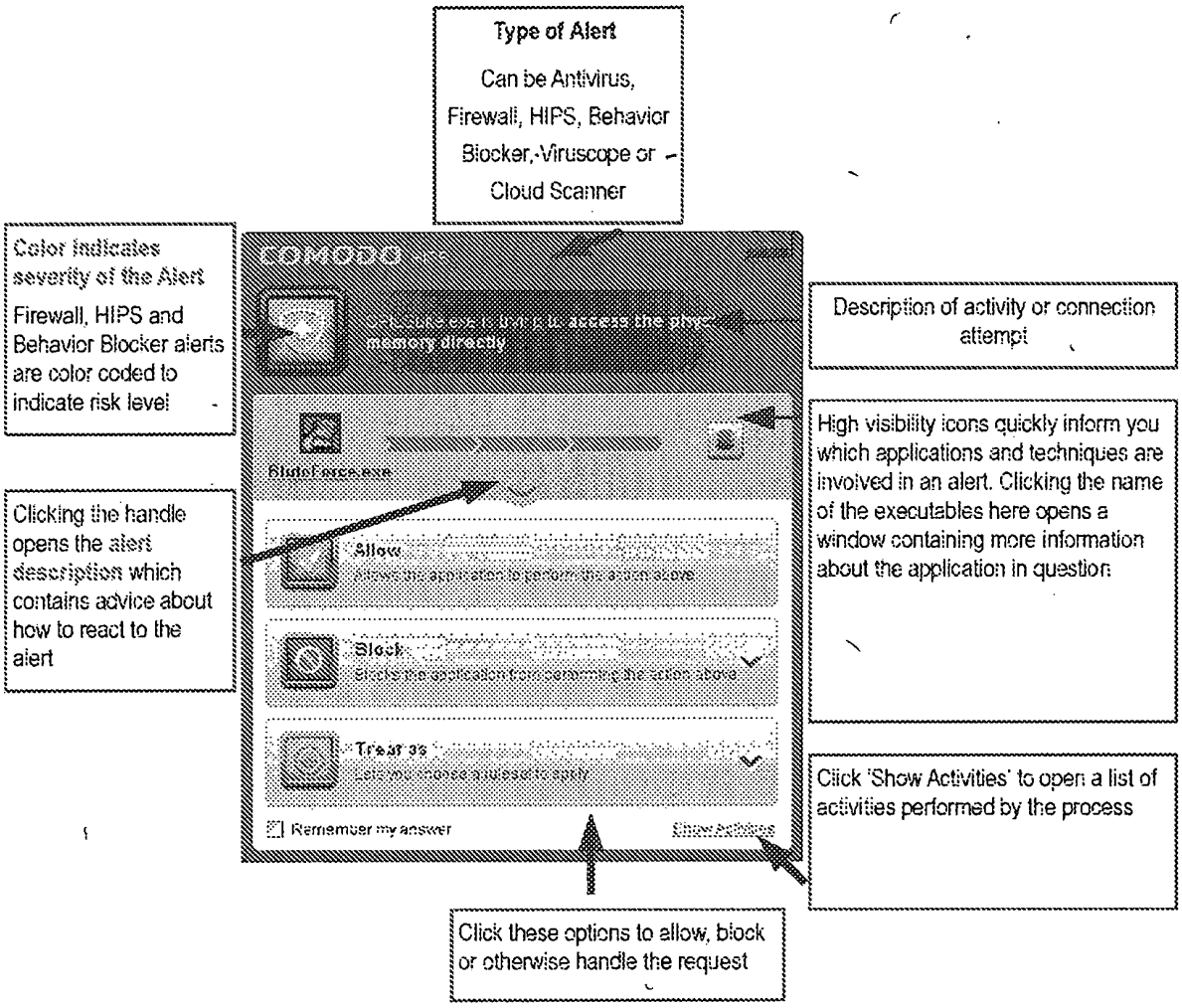
1.6. Understanding Security Alerts

- Alerts Overview
  - Alert Types
  - Severity Levels
  - Descriptions
- Antivirus Alerts
- Firewall Alerts
- HIPS Alerts

- Behavior BlockerAlerts
- Elevated Privilege Alerts
- Auto-Sandbox Alerts
- Viruscope Alerts

Alerts Overview

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



Alert Types

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

- Antivirus Alerts - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when Antivirus is enabled and the option 'Do not show antivirus alerts' is disabled in Real-time Scanner Settings.
- Firewall Alerts - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the Firewall is enabled and the option 'Do not show popup alerts' is disabled in Firewall Settings.
- HIPS Alerts - Shown whenever an application attempts an unauthorized action or tries to access protected

areas. HIPS alerts will only be generated if HIPS is enabled and Do NOT show popup alerts is disabled.

- Behavior Blocker Alerts (including Elevated Privilege Alerts) - Shown whenever an application tries to modify operating system or related files and when the Behavior Blocker automatically sandboxes an unrecognizable file. Behavior Blocker / Auto-Sandbox Alerts will be displayed only when auto-sandboxing is enabled under Behavior Blocker settings. Privilege Alerts will only be shown if enabled.
- Viruscope Alerts - Shown whenever a currently running process attempts to take suspicious actions. Viruscope alerts allow you to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. Viruscope Alerts will be displayed only when Viruscope is enabled under Behavior Blocker 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 Behavior Blocker components of CIS. For other types of alert, see Comodo Message Center notifications, Notification Messages and Information Messages.

Severity Level

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

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

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

Alert Description

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



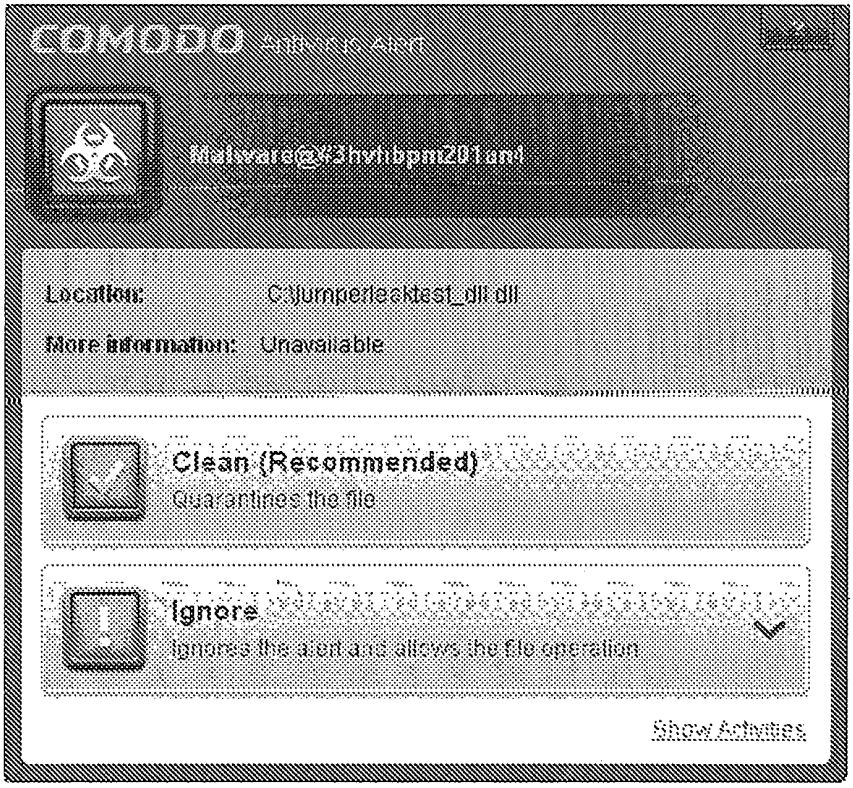
The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

Answering an Antivirus Alert

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

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



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

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

The following response-options are available:

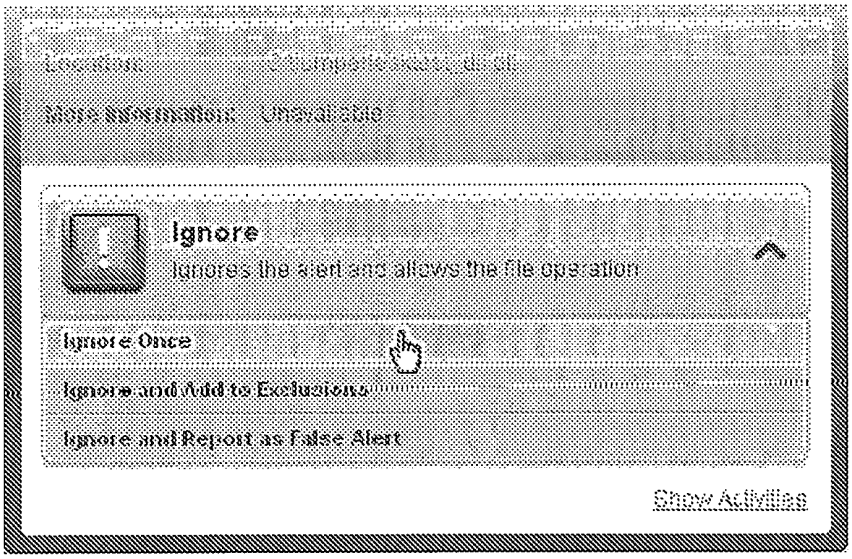
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the Quarantine interface. Refer to Manage Quarantined Items for more details on quarantined files.

  The Viruscope subsytem integrated with the Antivirus, also monitors the changes made to your computer by the virus or virus-like activities automatically reverts them, if you choose to clean the infected file or application, when Viruscope is enabled under Behavior Blocker settings.

Note: Though Viruscope has power to reverse majority of types of changes effected by the process(es) evoked by blocked applications, it has some limitations. Very few of the file activities that make permanent changes could be reverted. Examples include:

- Deletion of a file
- Moving a file to a different folder/location
- Loading a file image into a process, i.e. DLL file loading

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



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

Antivirus Notification

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



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

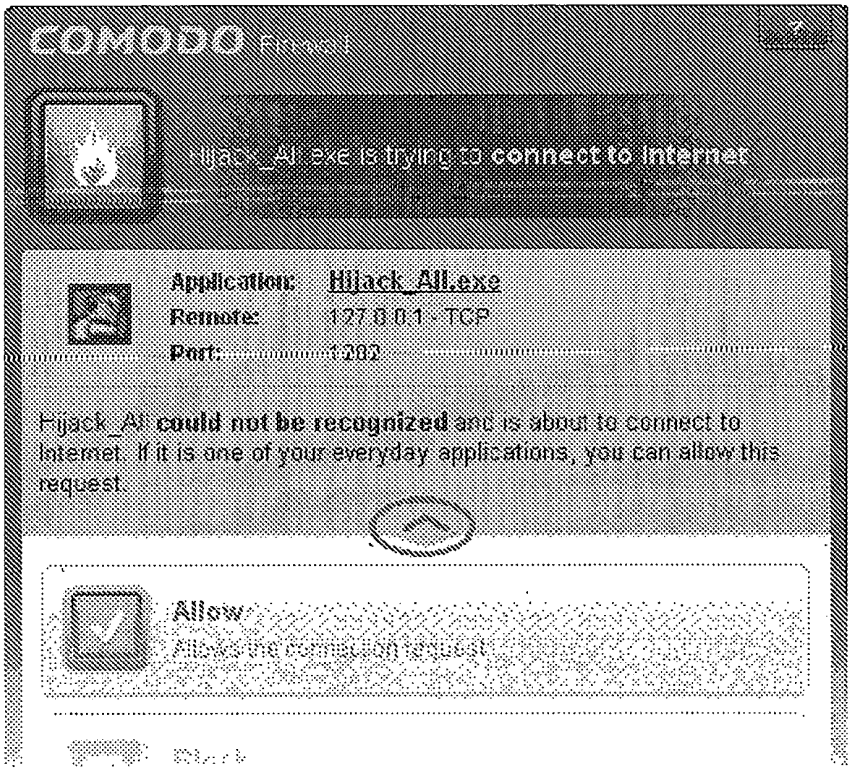
Answering Firewall Alerts

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



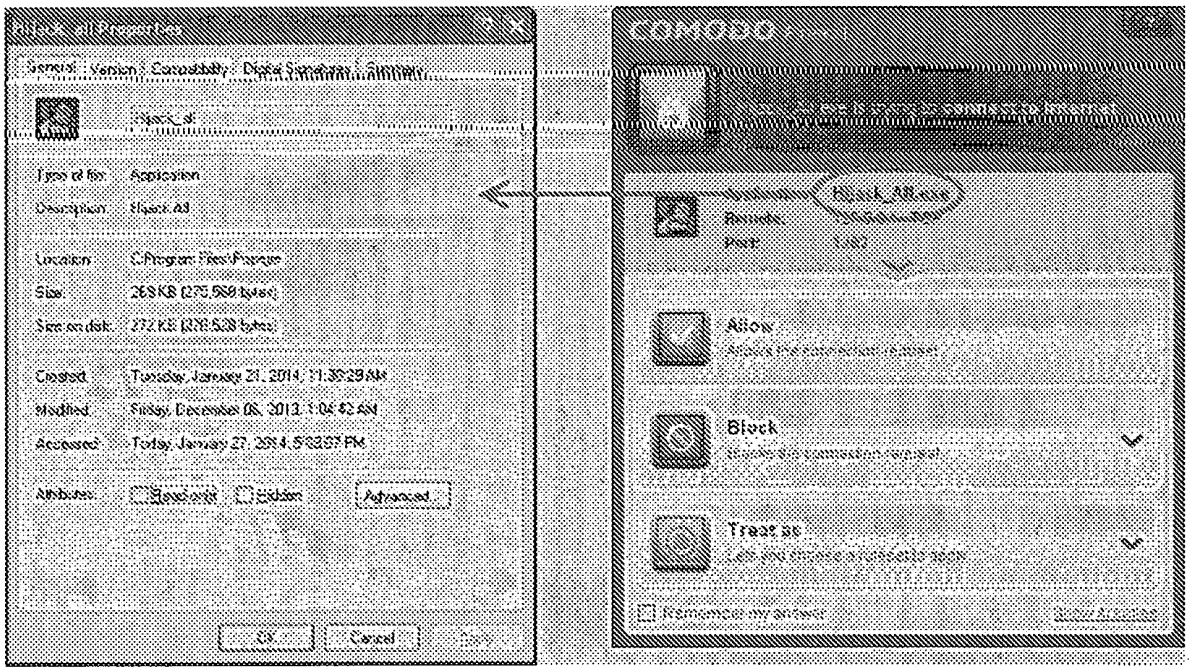
Tip: Clicking the Show Activities link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

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



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

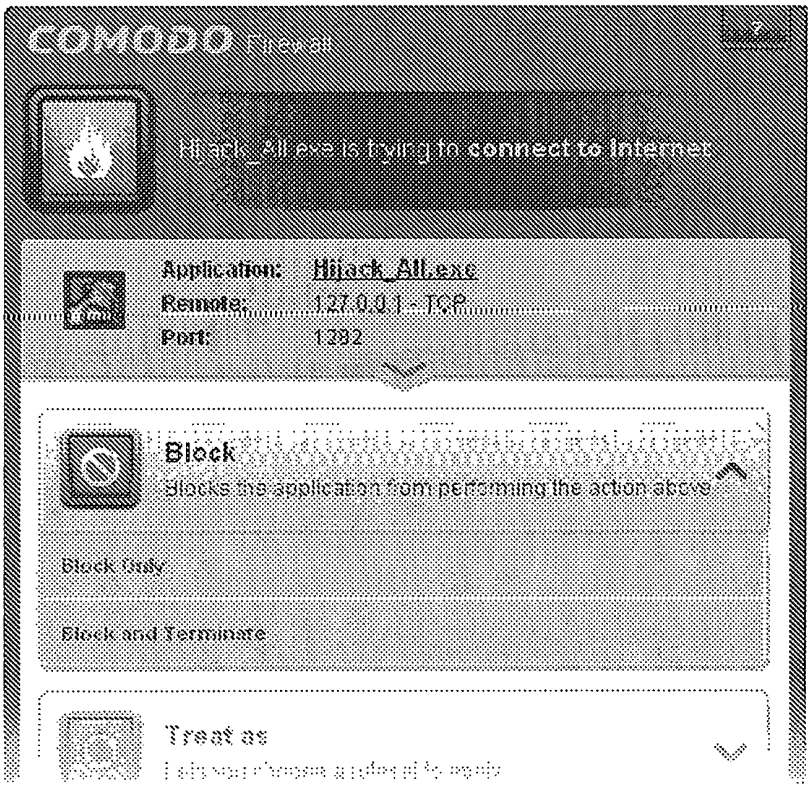
   If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.



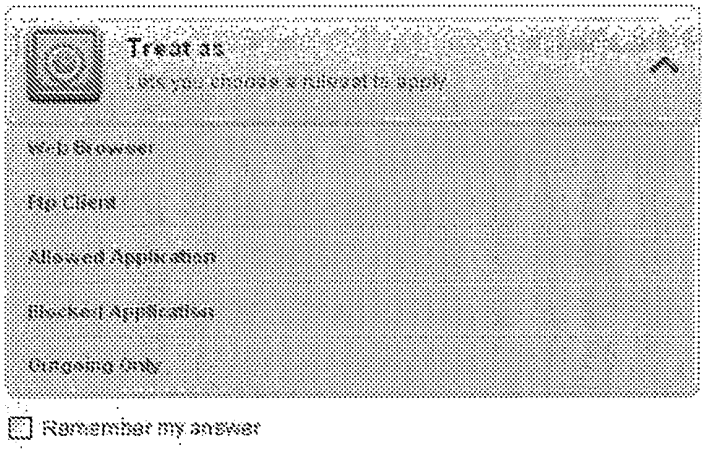
In all cases, clicking on the name of the application opens a properties window that can help you determine whether or not to proceed:

If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand

the alert, you can choose to block the connection (connection is not allowed to proceed) or block & terminate (connection is not allowed to proceed and the process/application that made the request is shut down).



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



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

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

Answering HIPS Alerts

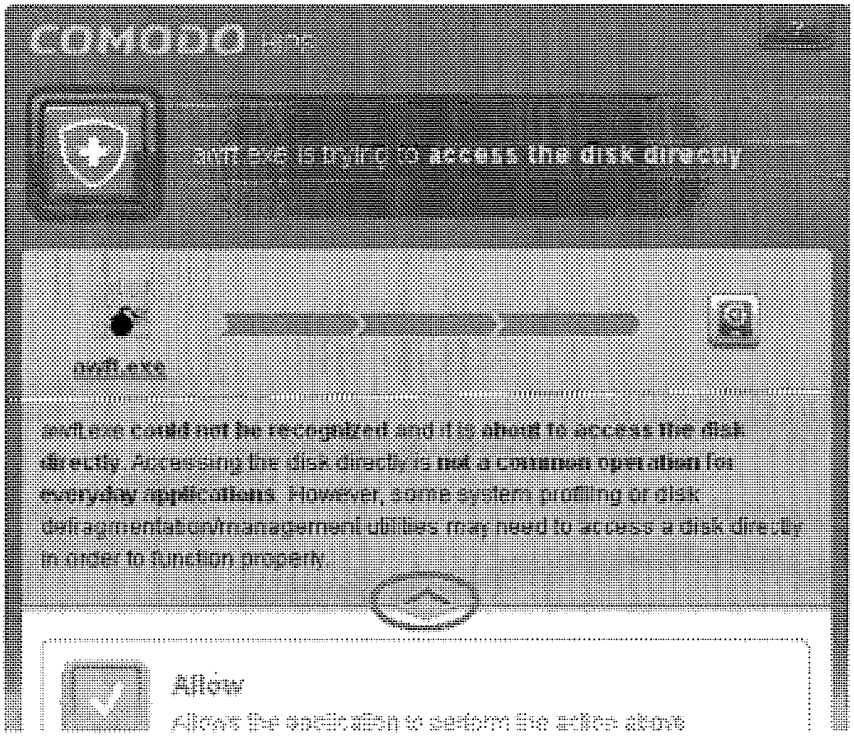
Comodo Internet Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:



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

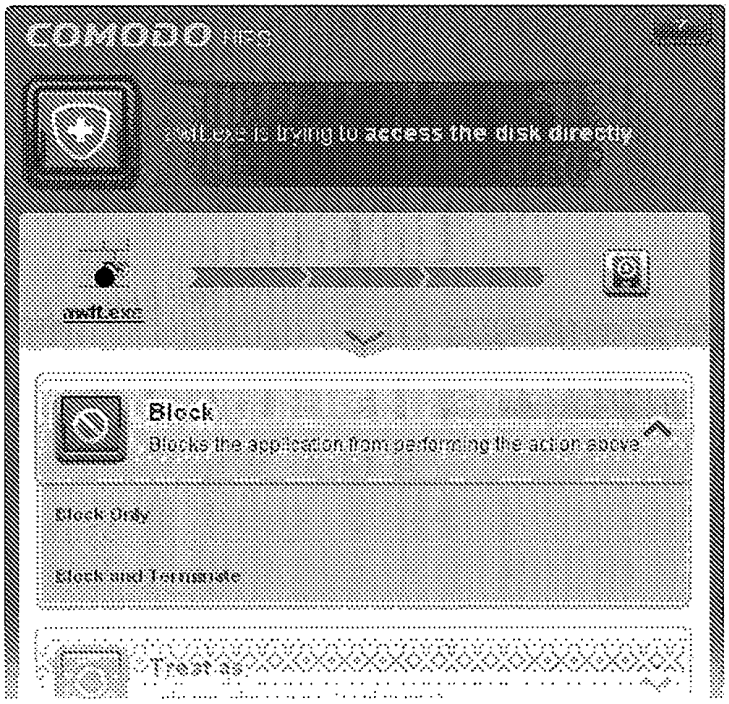
The Show Activities link is available only if Viruscope is enabled under Advanced Settings > Defense+ > Behavior Blocker Settings. If none of the processes associated with the application has started before the alert is generated, the Show Activities link is disabled and will not open the Process Activities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

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

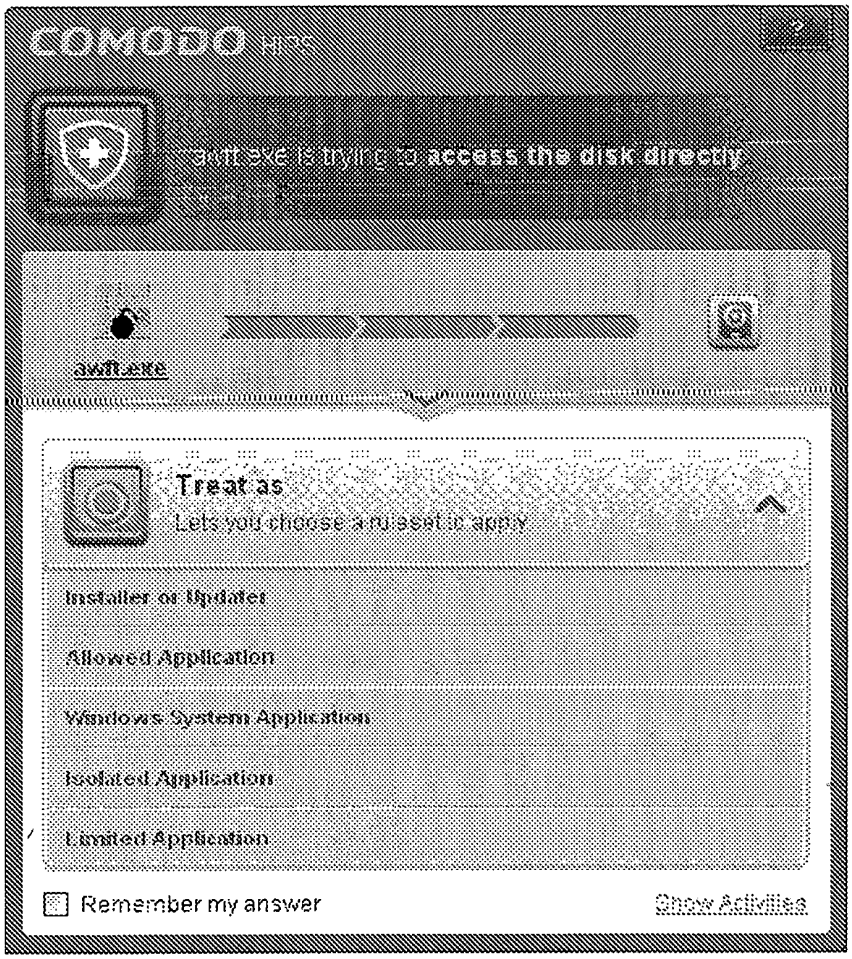


If it is one of your everyday applications and you simply want it to be allowed to continue then you should select **Allow**.

If you don't recognize the application then we recommend you select **Block** the application. You can choose to just block the connection or to block & terminate.



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



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

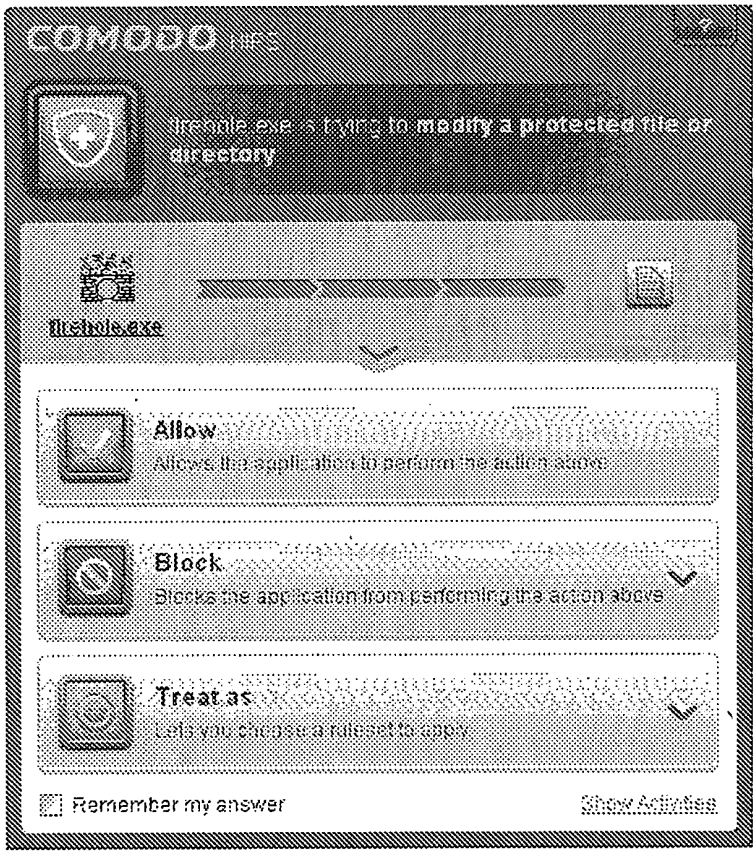
3. Pay special attention to **Device Driver Installation** and **Physical Memory Access** alerts. Again, not many legitimate applications would cause such an alert and this is usually a good indicator of malware / rootkit like behavior. Unless you know for a fact that the application performing the activity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



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



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



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

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

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

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

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

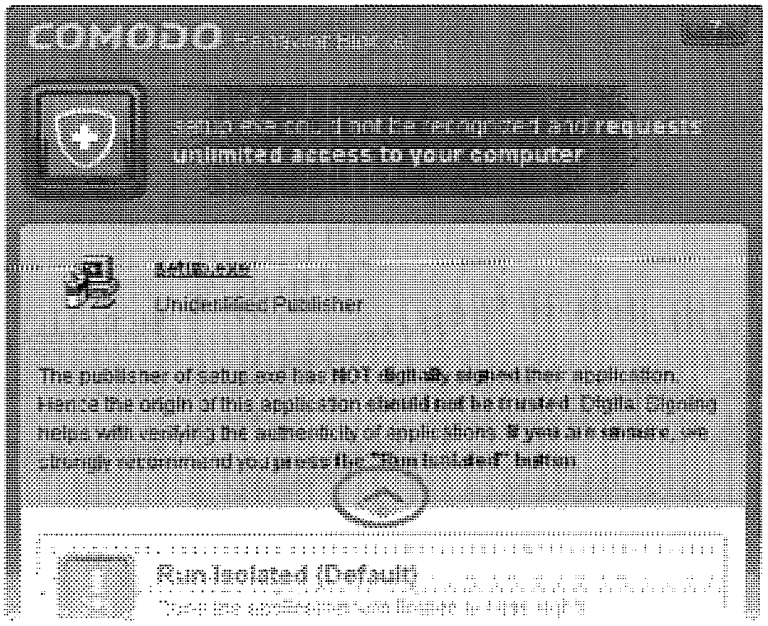
Answering a Behavior Blocker Alert

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

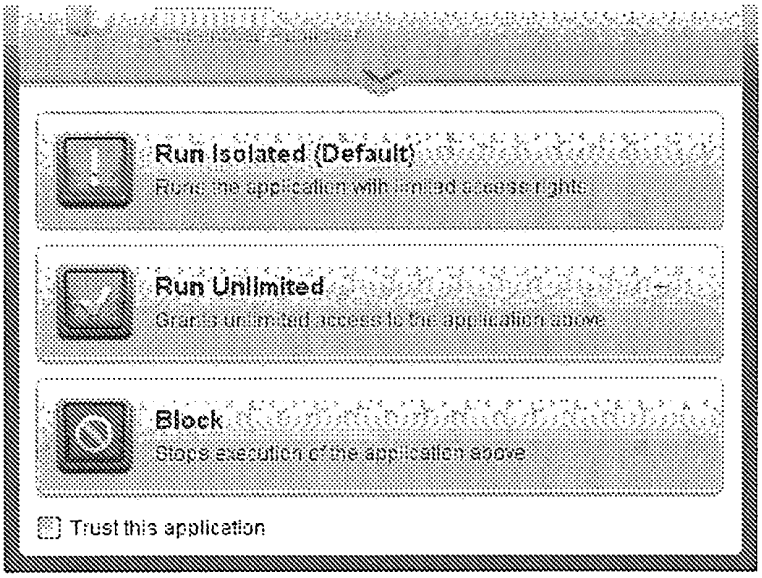
Please read the following advice before answering a Behavior Blocker alert:



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



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



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

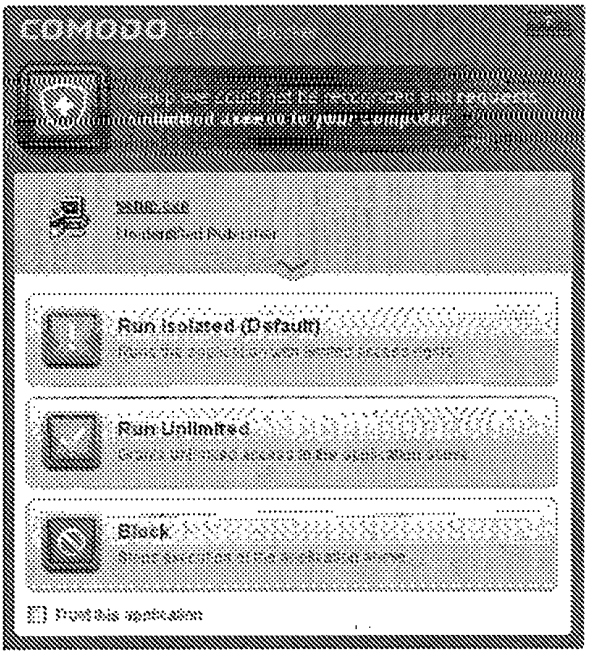
Run with Elevated Privileges Alert

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

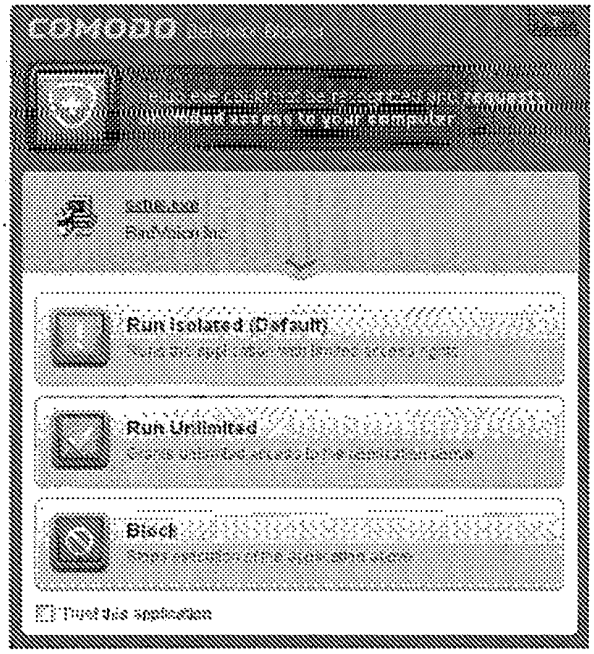
- If you have good reason to trust the publisher of the software then you can click the '**Run Unlimited**' button. This will grant the elevated privilege request and allow the installer to run.
- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted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

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

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



Unknown and not Digitally Signed



Unknown and Digitally Signed but not yet whitelisted (Not yet a 'Trusted Vendor')

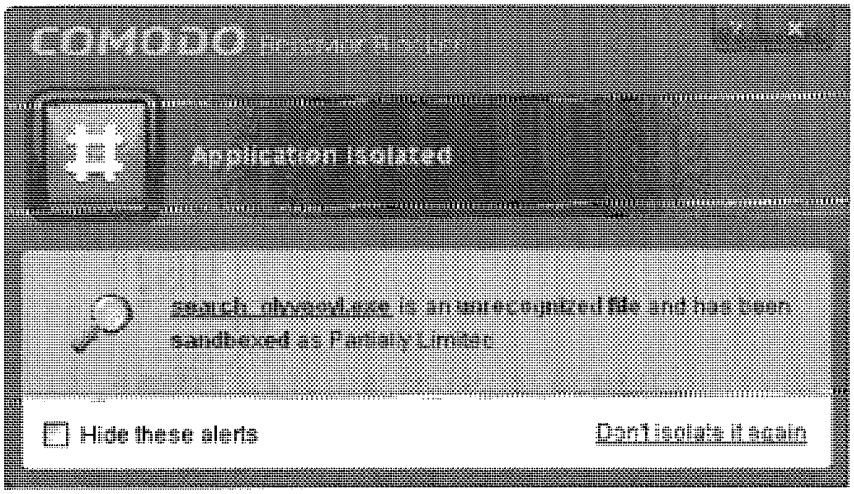
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

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

Auto-Sandbox Alerts

The Behavior Blocker will display an alert whenever it auto-sandboxes an unknown application:



The alert will show the name of the executable that has been auto-sandboxed. The application will be automatically added to Unrecognized Files list.

- Clicking the name of the application will open the Unrecognized Files interface, that displays a list of the unrecognized files including the currently auto-sandboxed application.
- Clicking Don't isolate it again removes the application from the Unrecognized Files list and adds it to the Trusted Files list, so that the application will not be auto-sandboxed in future. Choose this option if you are absolutely sure that the executable is safe.

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

Also see:

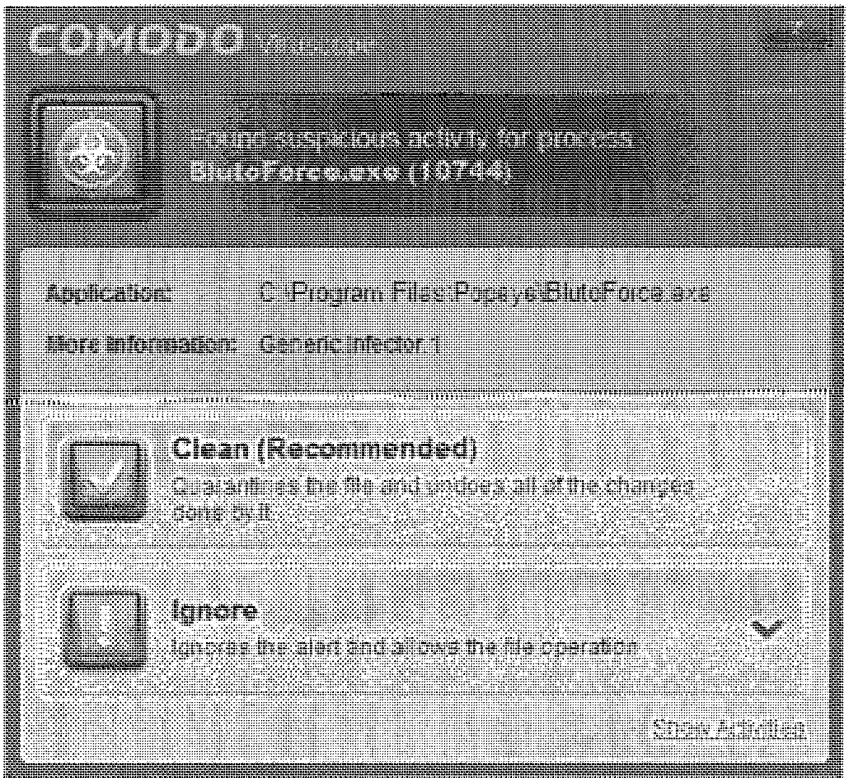
- 'Unknown Files: The Auto-Sandboxing and Scanning Processes' - to understand the decision making process behind why CIS chooses to auto-sandbox certain applications.

Answering a Viruscope Alert

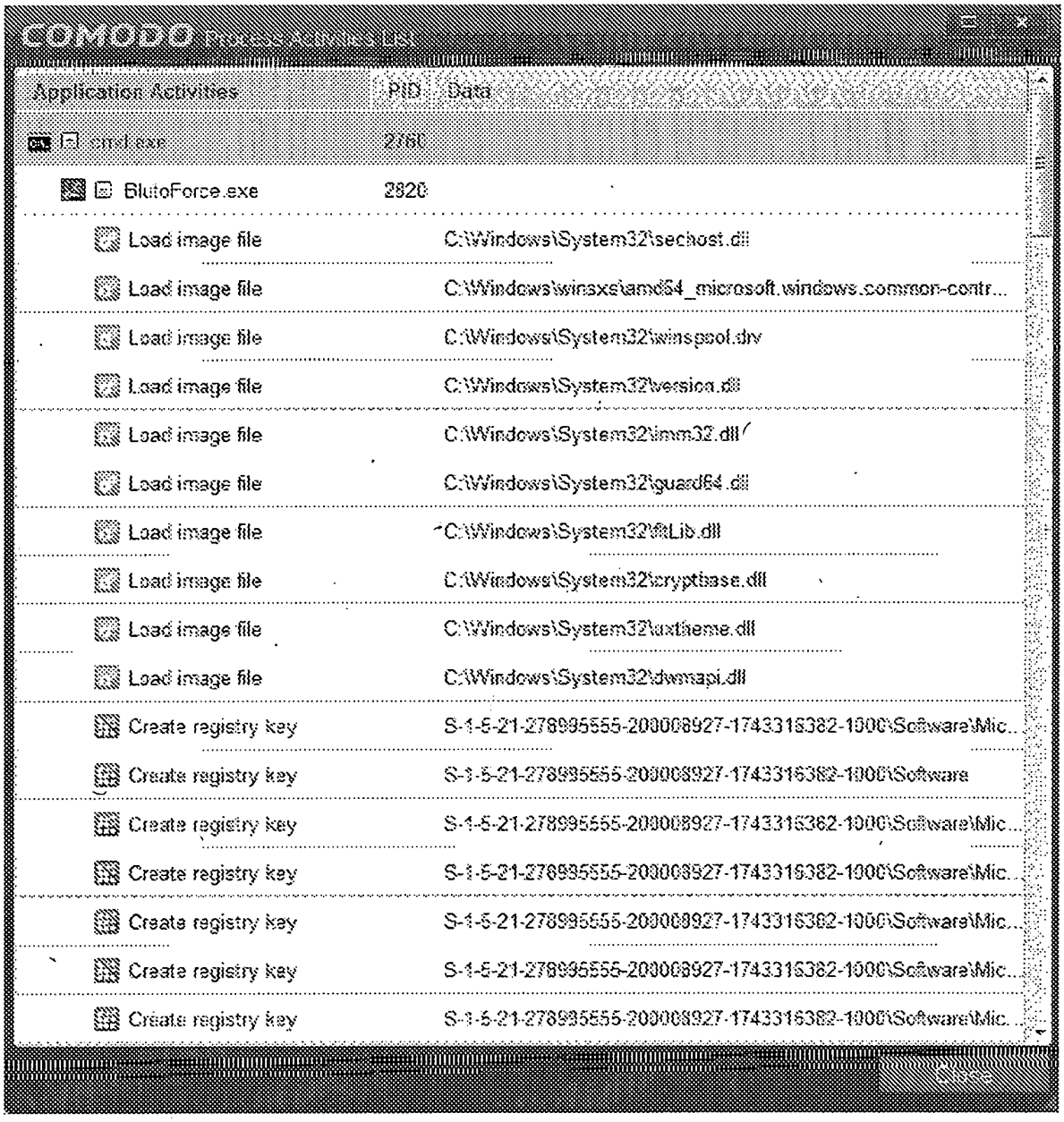
Comodo Internet Security generates a Viruscope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that Viruscope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a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

Please read the following advice before answering a Viruscope alert:

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



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



Column Descriptions

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

- Data - Displays the file affected by the action.

2. General Tasks - Introduction

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



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

- Scan and Clean your Computer
- Manage Virus Database and Program Updates
- Manage Quarantined Items
- View CIS Logs
- Get Live Support
- Manage CIS Tasks
- View Active Internet Connections

2.1. Scan and Clean Your Computer

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



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

- Run a Quick Scan
- Run a Full Computer Scan
- Run a Rating Scan
- Run a Custom Scan
    - Scan a Folder
    - Scan a File
    - Create and Schedule a Custom Scan

- Scan individual file/folder
- Processing Infected Files

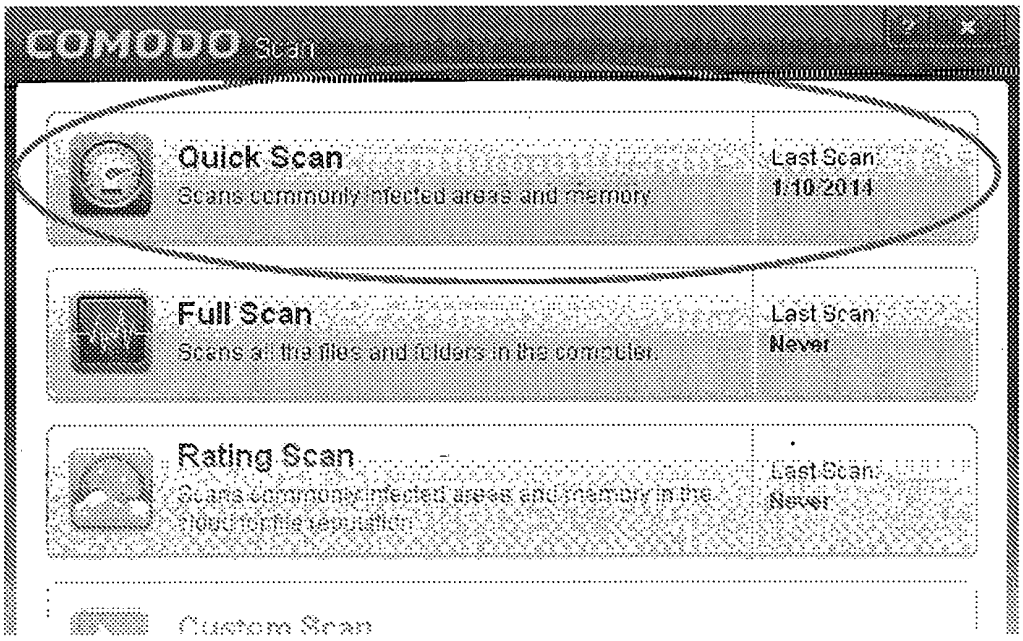
2.1.1. Run a Quick Scan

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

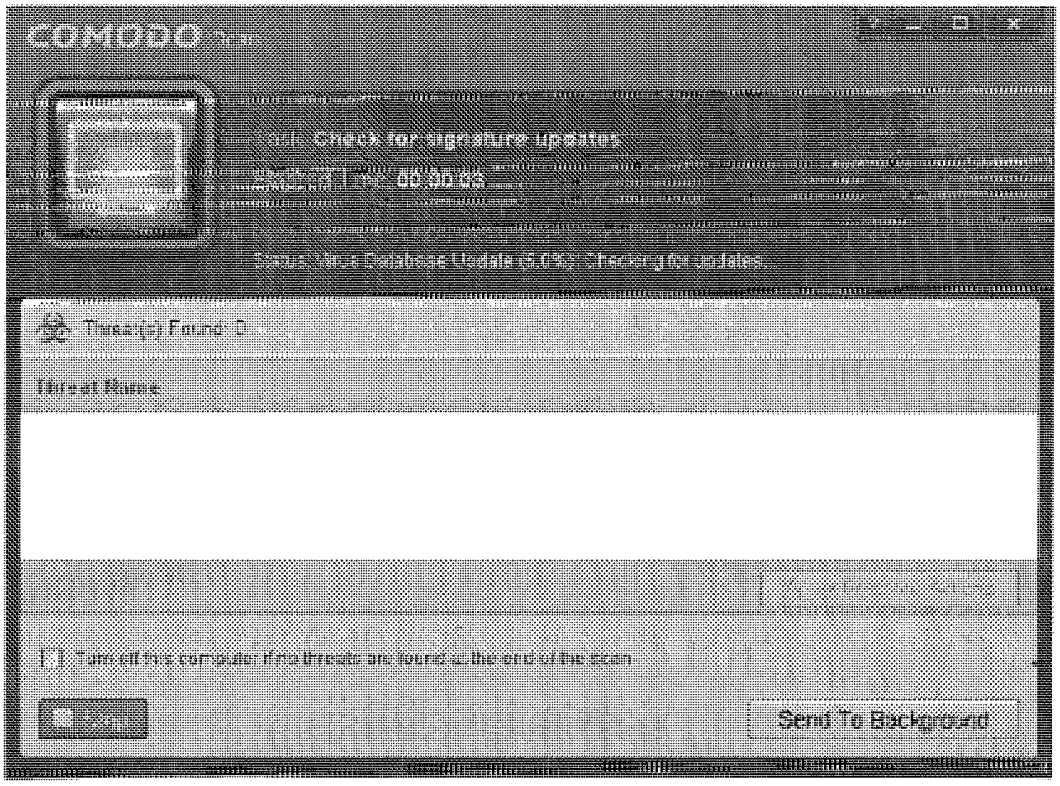
You can customize which items are scanned under a 'Quick Scan' and create a scan schedule from the 'Advanced Tasks' interface. Refer to Antivirus Settings > Scan Profiles for more details.

To run a Quick Scan

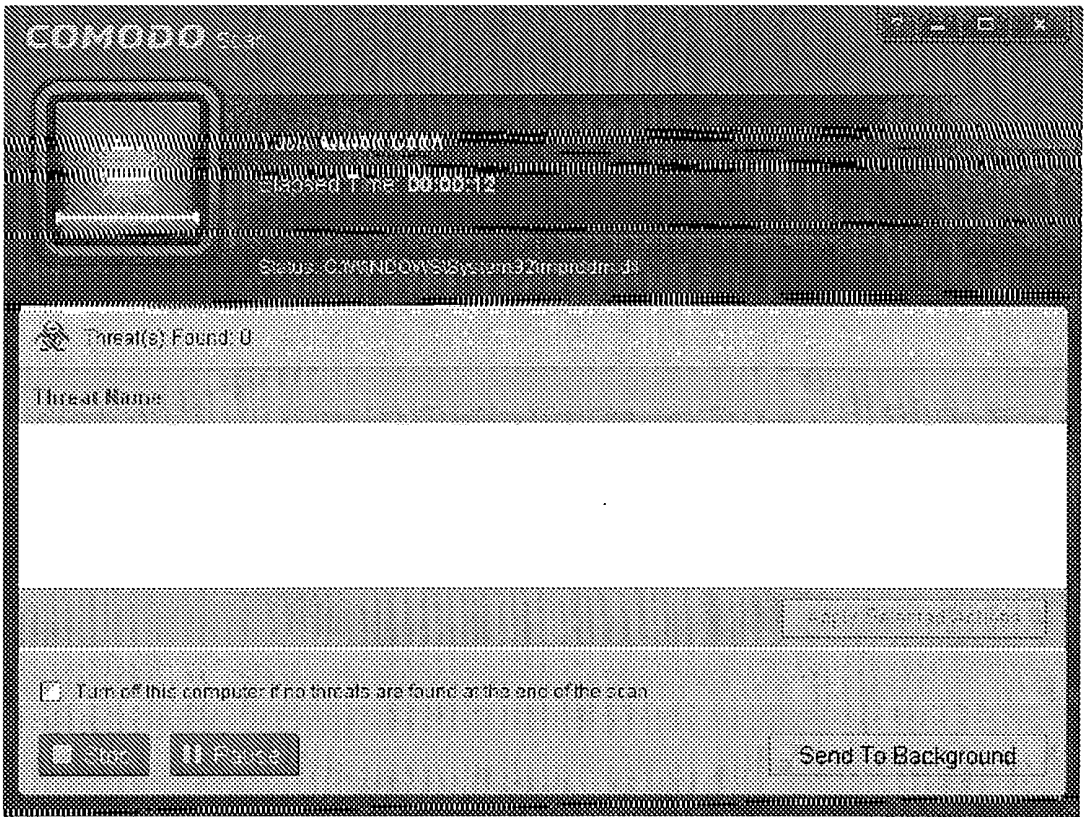
- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



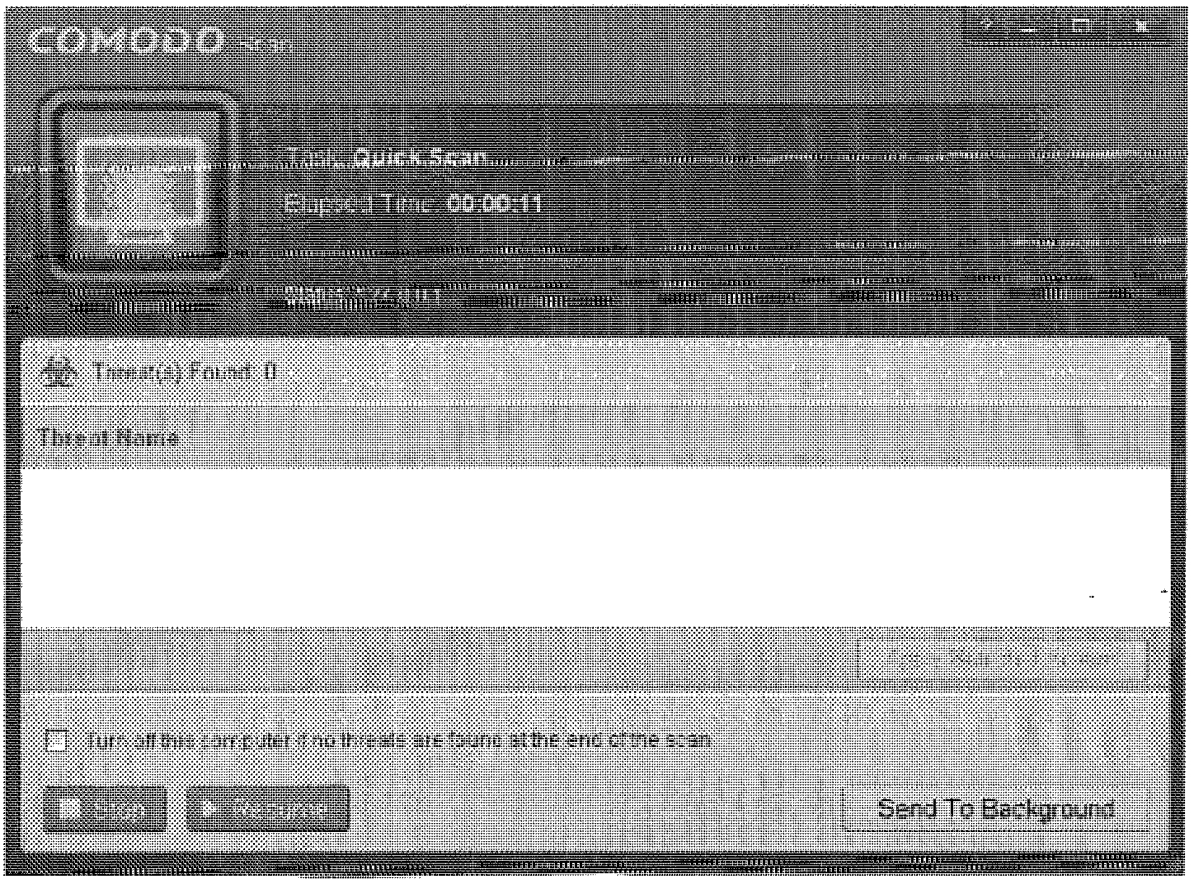
The scanner will start and first check whether your virus signature database is up-to-date:



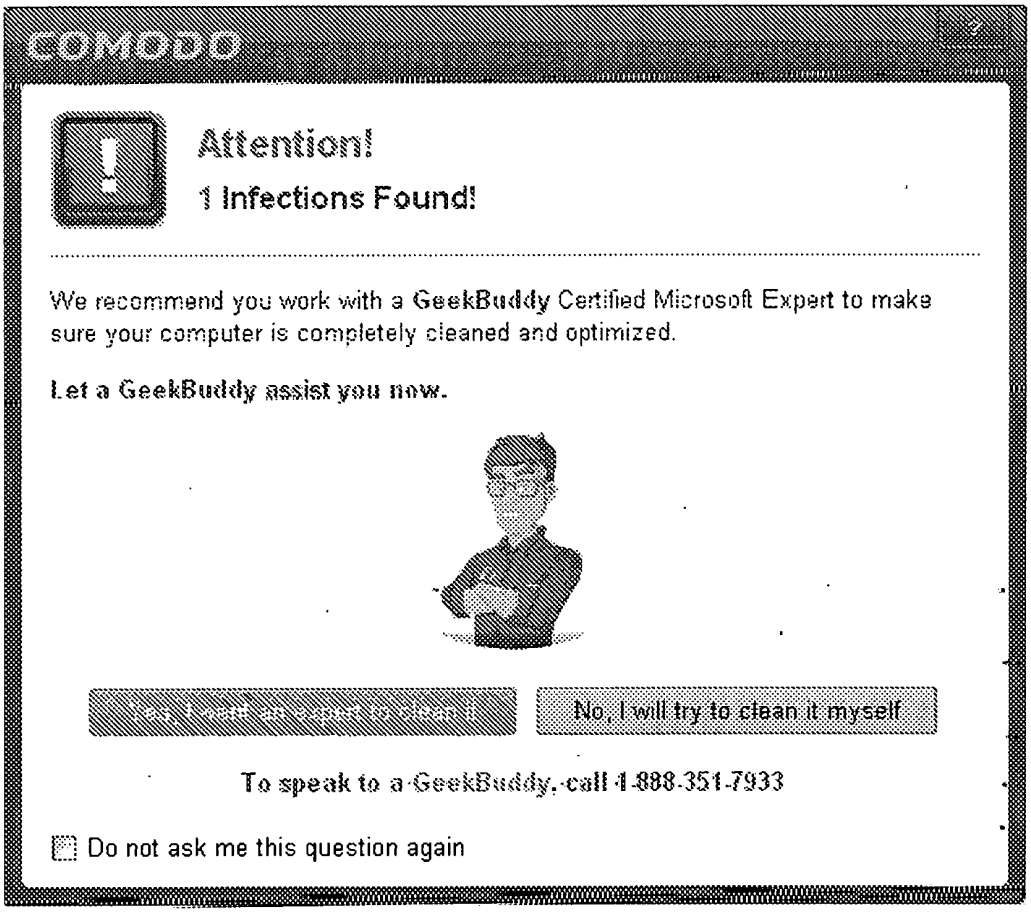
If the database is outdated, the scanner will first download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:



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



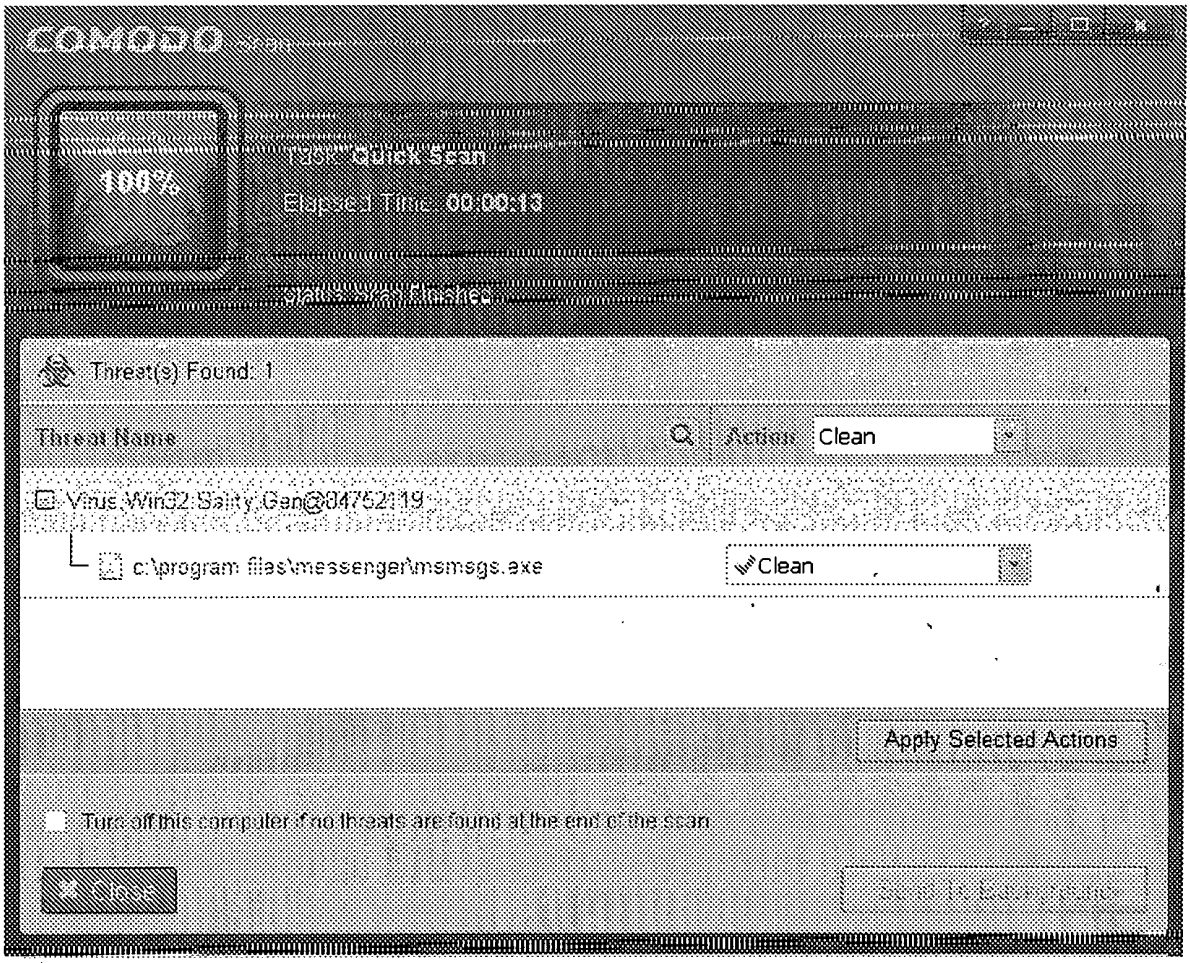
- An alert screen will be displayed at the end of the scan if issues were detected. The alert will display the number of threats/infections discovered and present you with cleaning options:



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

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

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



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

2.1.2. Run a Full Computer Scan

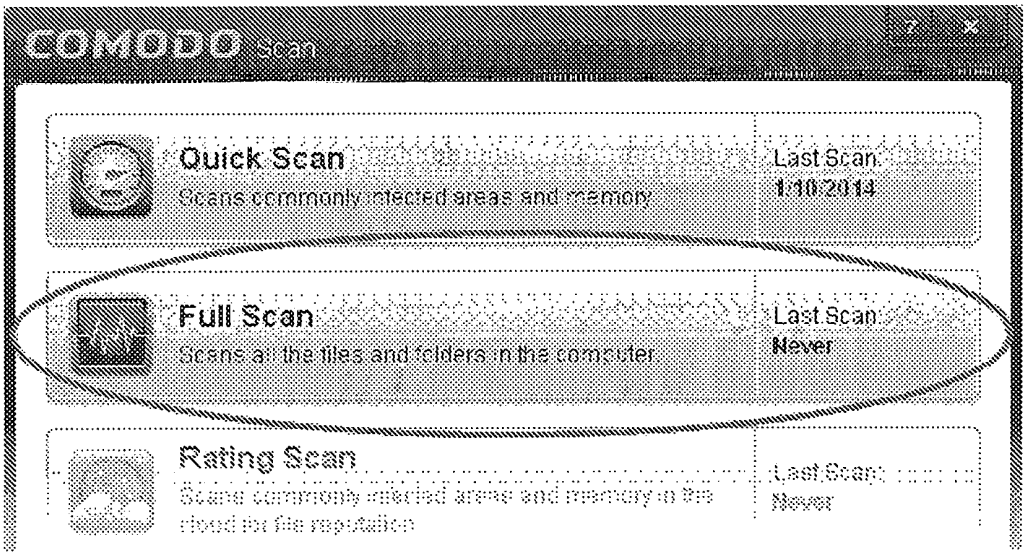
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

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

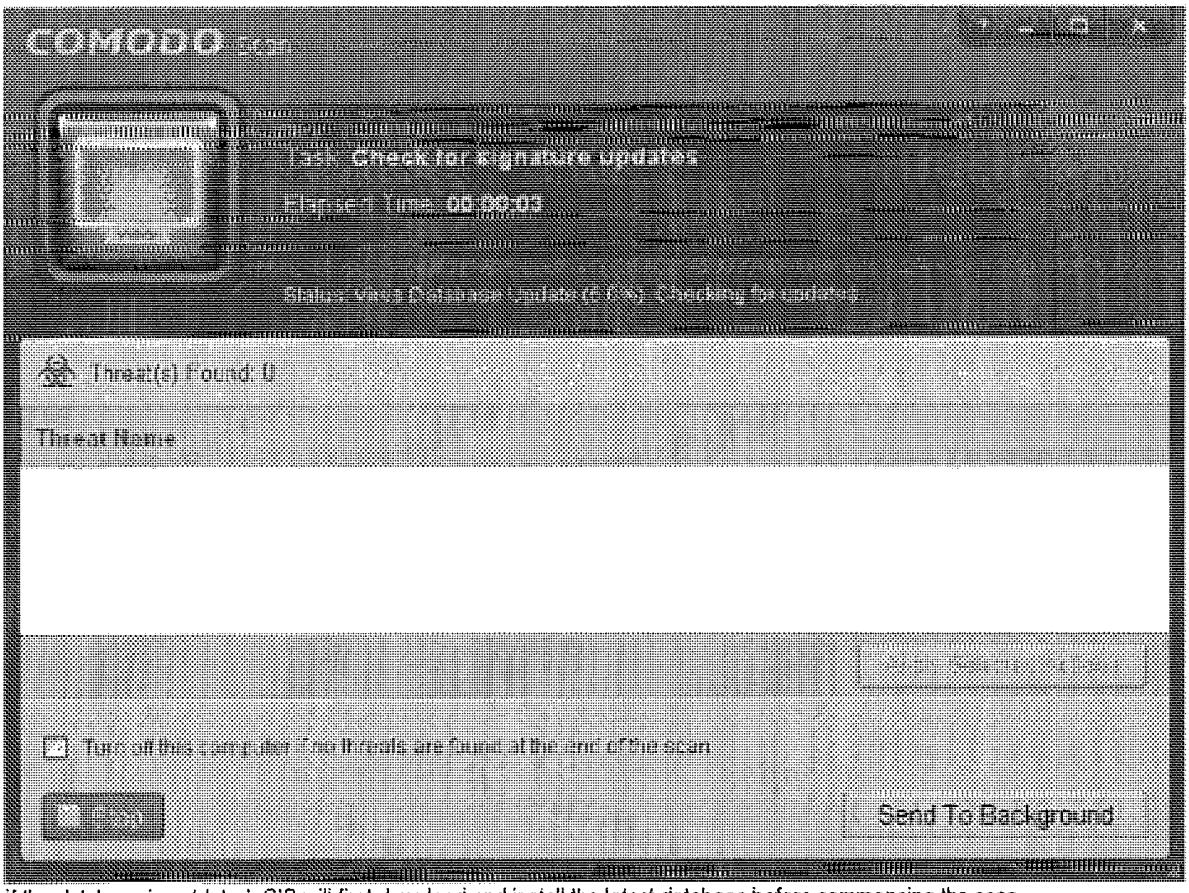
Refer to Antivirus Settings > Scan Profiles for more details.

To run a Full Computer Scan

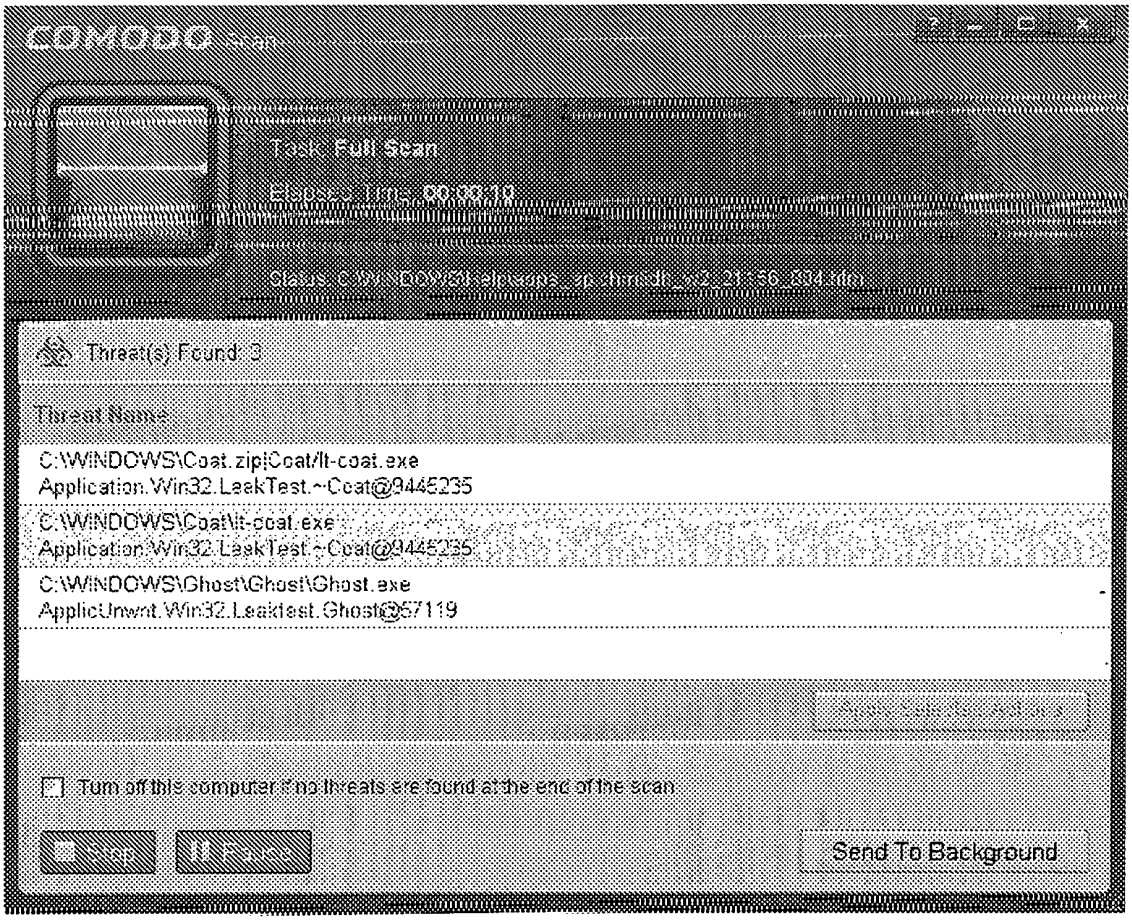
- Click 'Scan' from the General Tasks interface the click 'Full System Scan' from the 'Scan' interface.



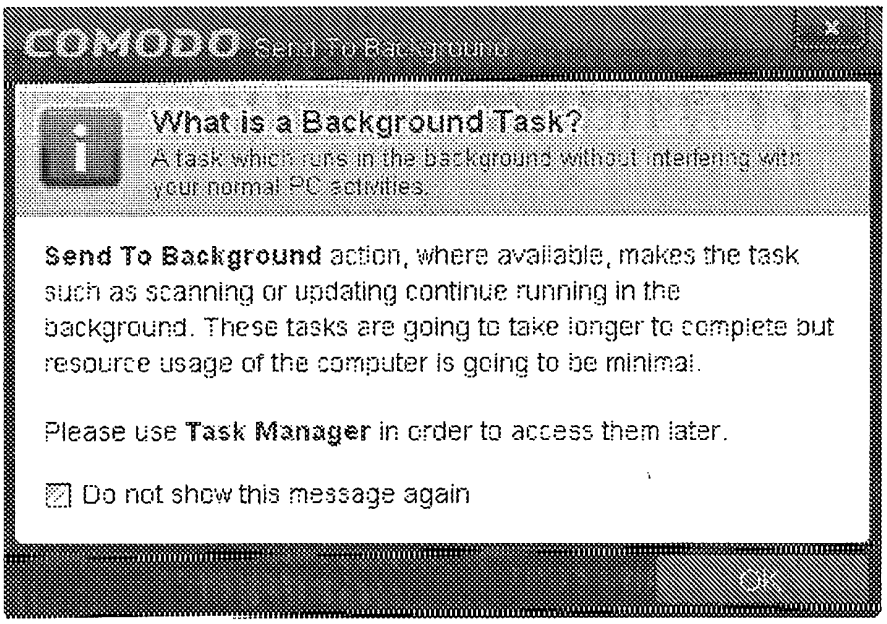
The scanner will start and first check whether your virus signature database is up-to-date.



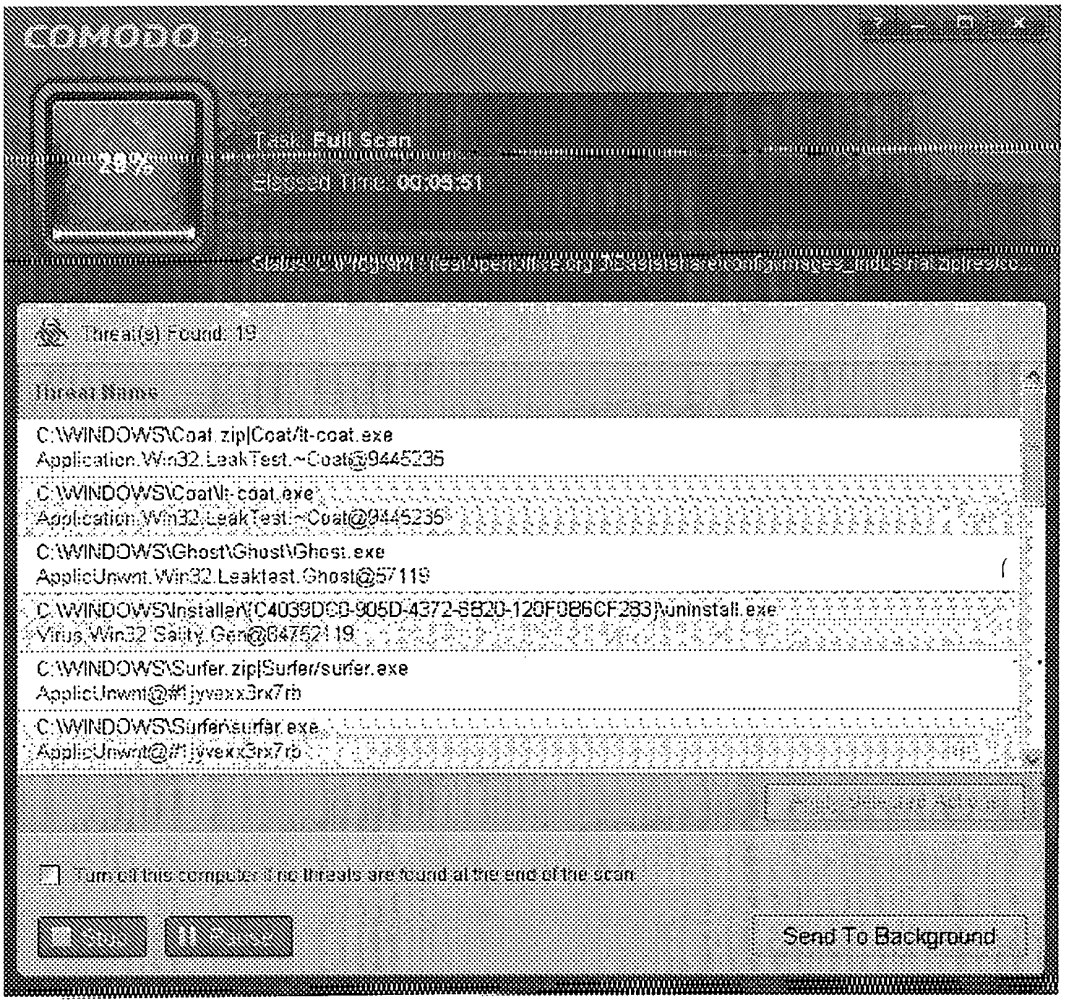
If the database is outdated, CIS will first download and install the latest database before commencing the scan.



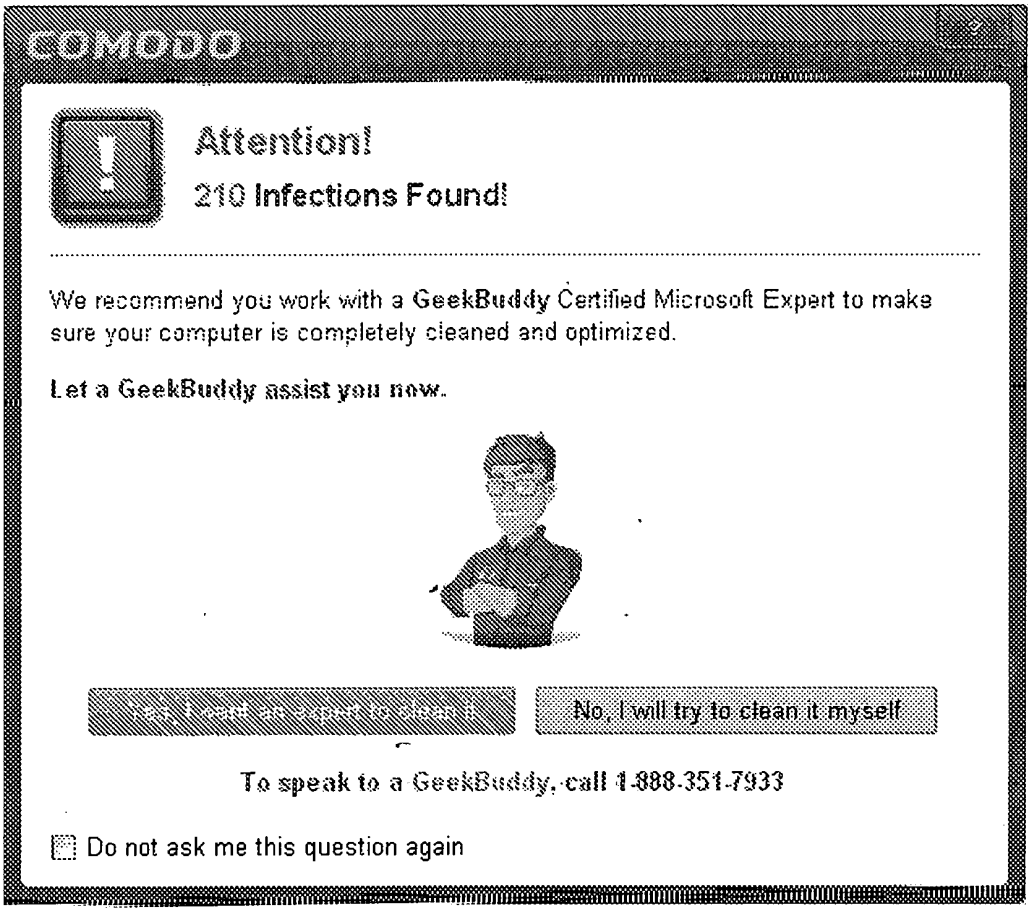
- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



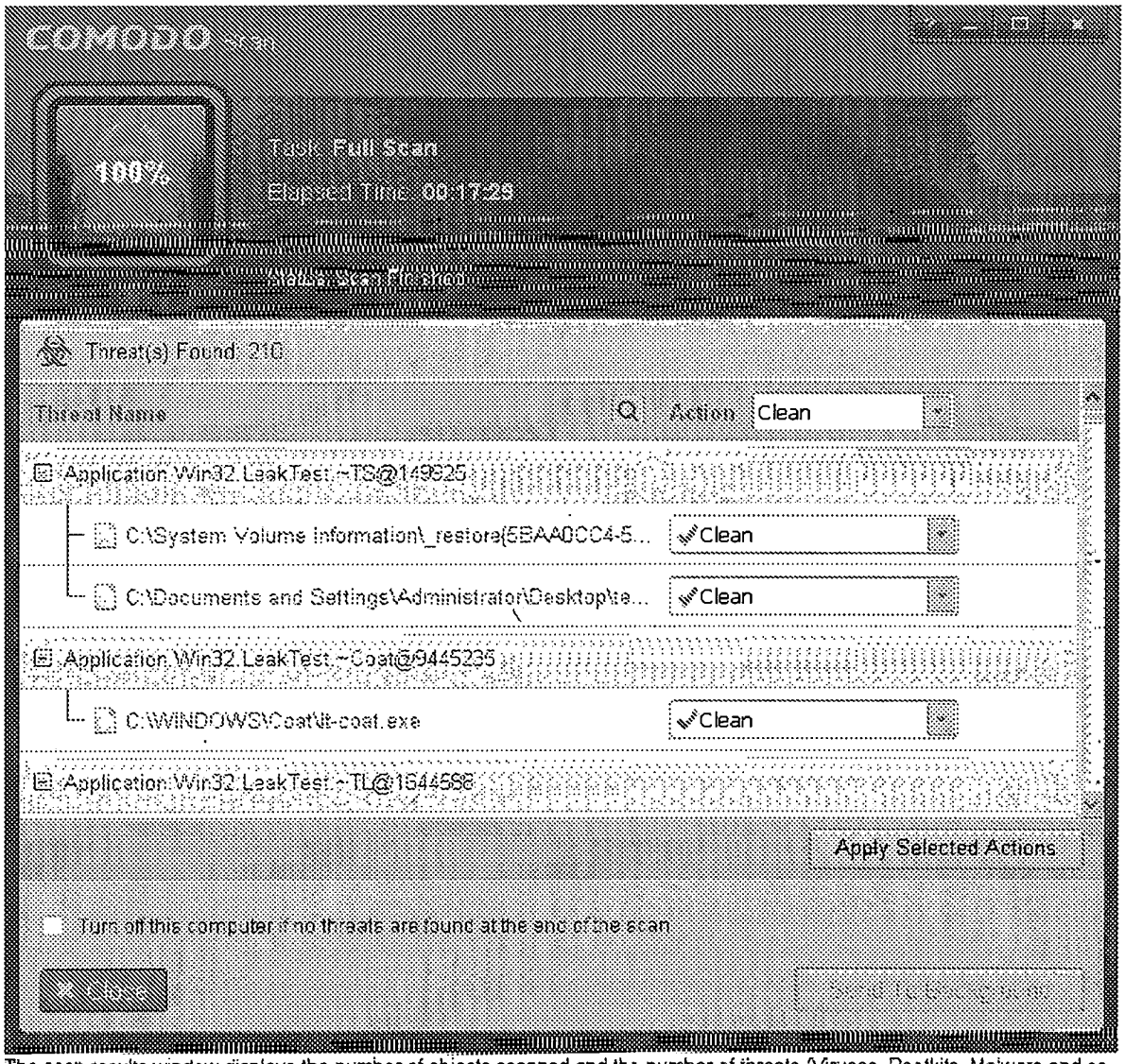
If you send to the background, you can continue to check scan progress by clicking 'Task Manager' on the home screen or by clicking 'Open Task Manager' icon from the 'Advanced Tasks' interface.



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



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



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

2.1.3. Run a Rating Scan

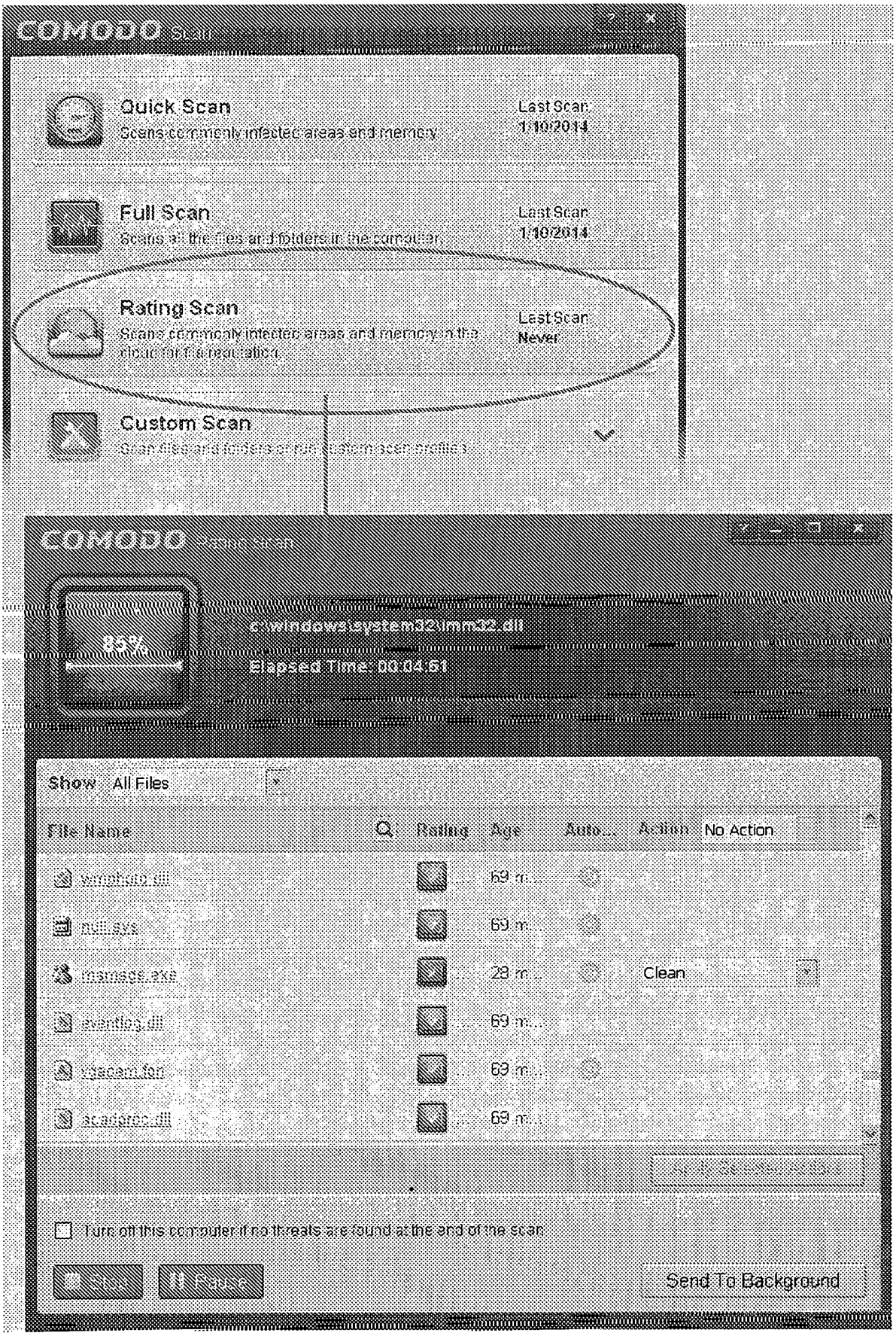
The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

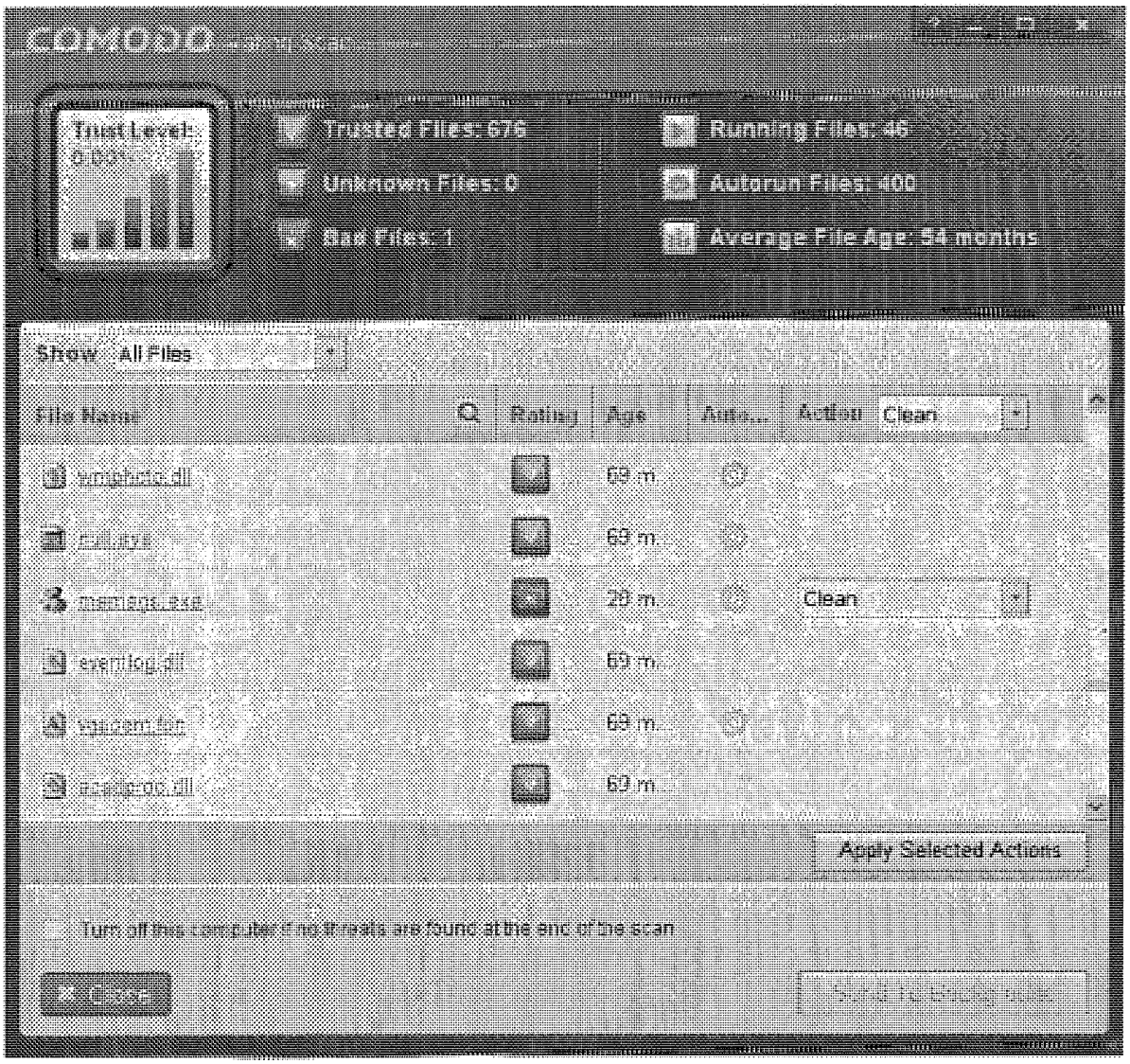
- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Bad - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

To run a Rating scan

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

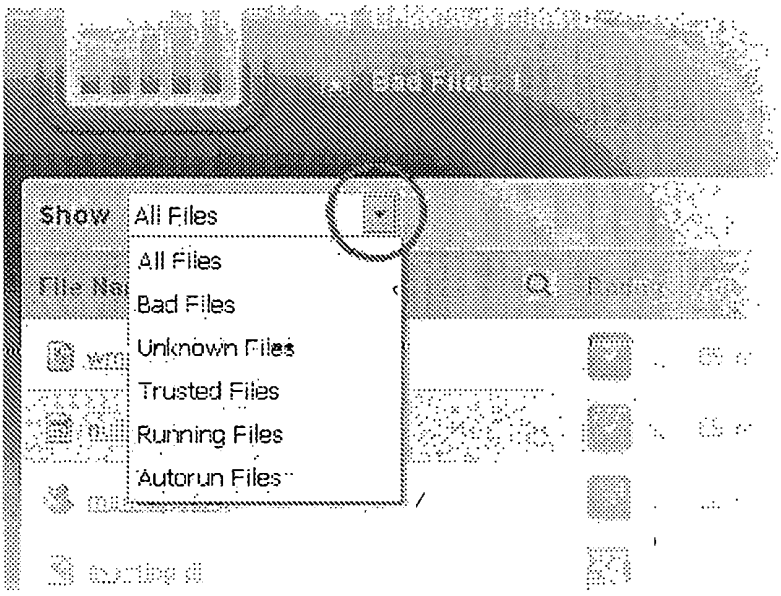


After the cloud scanners have finished their analysis, file ratings will be displayed as follows:

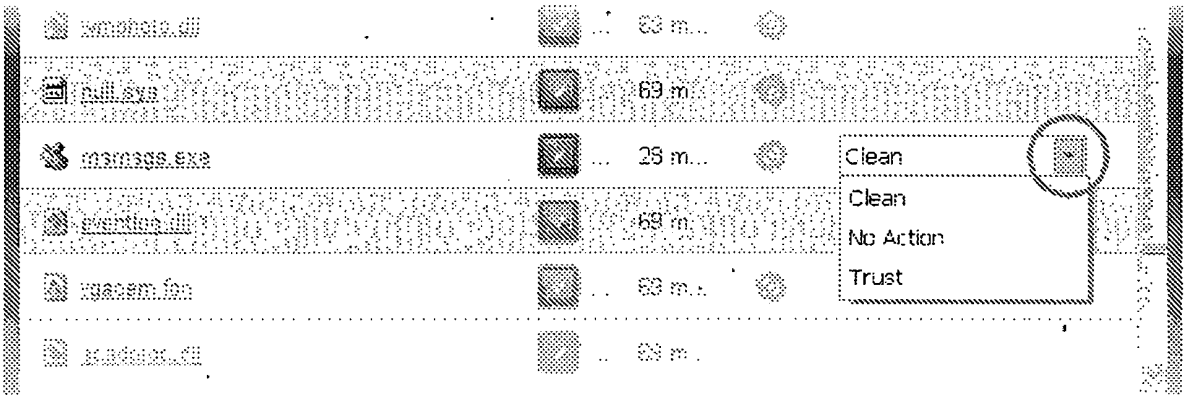


- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your computer
- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous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

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

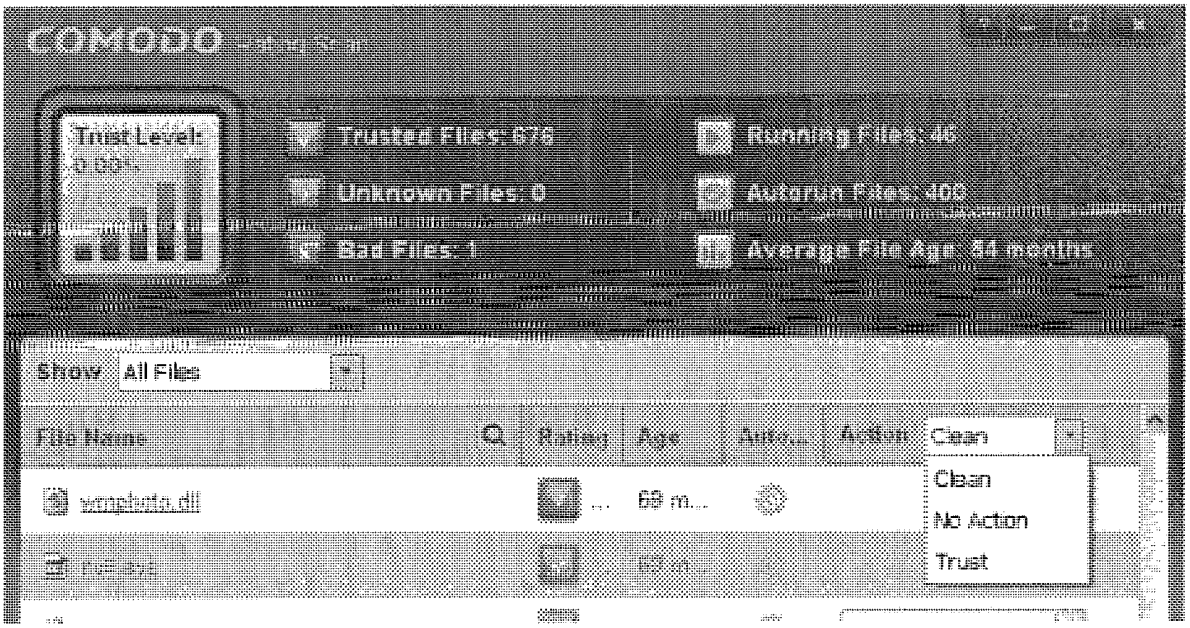


Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

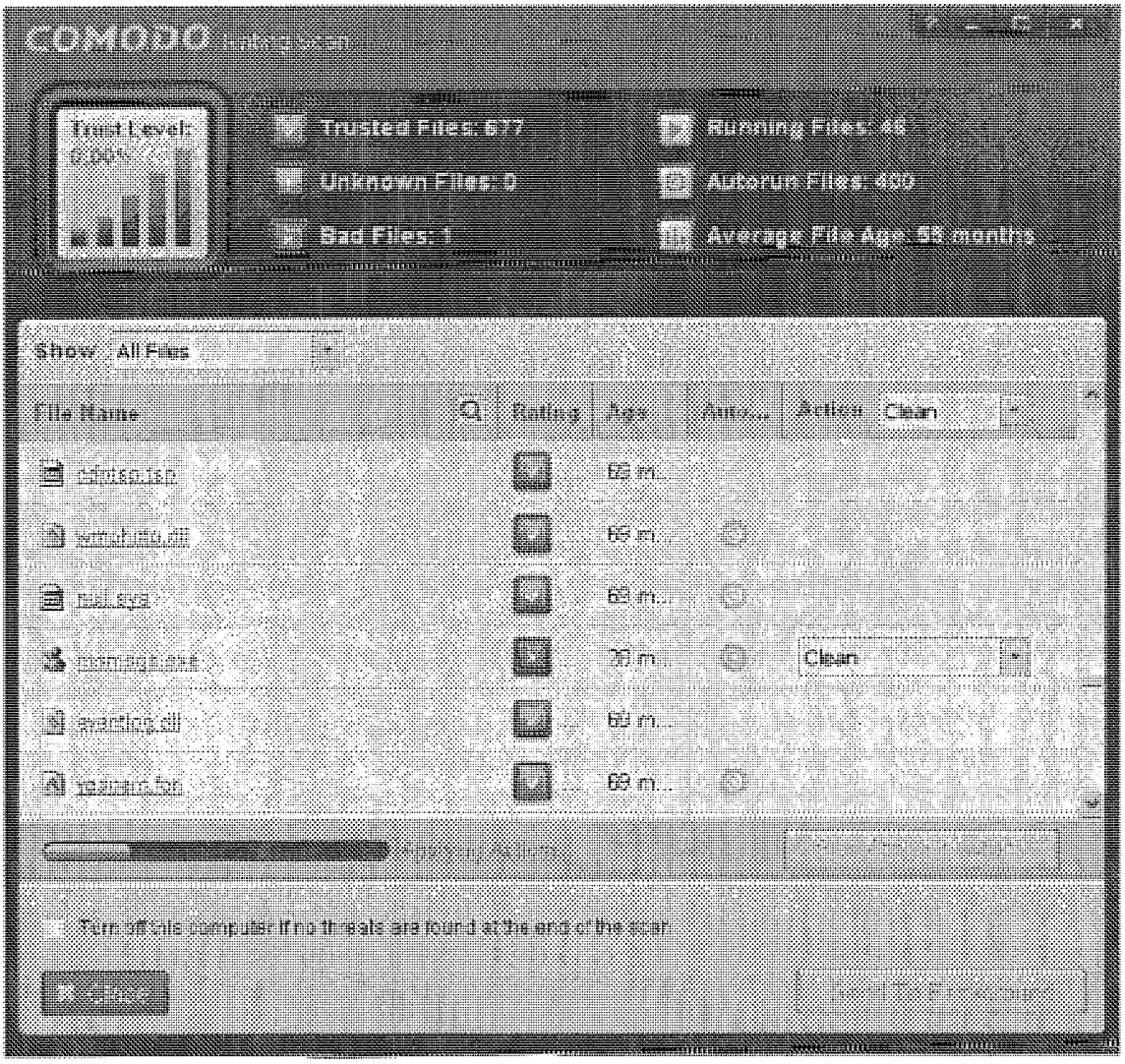


- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See Manage Quarantined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

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



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

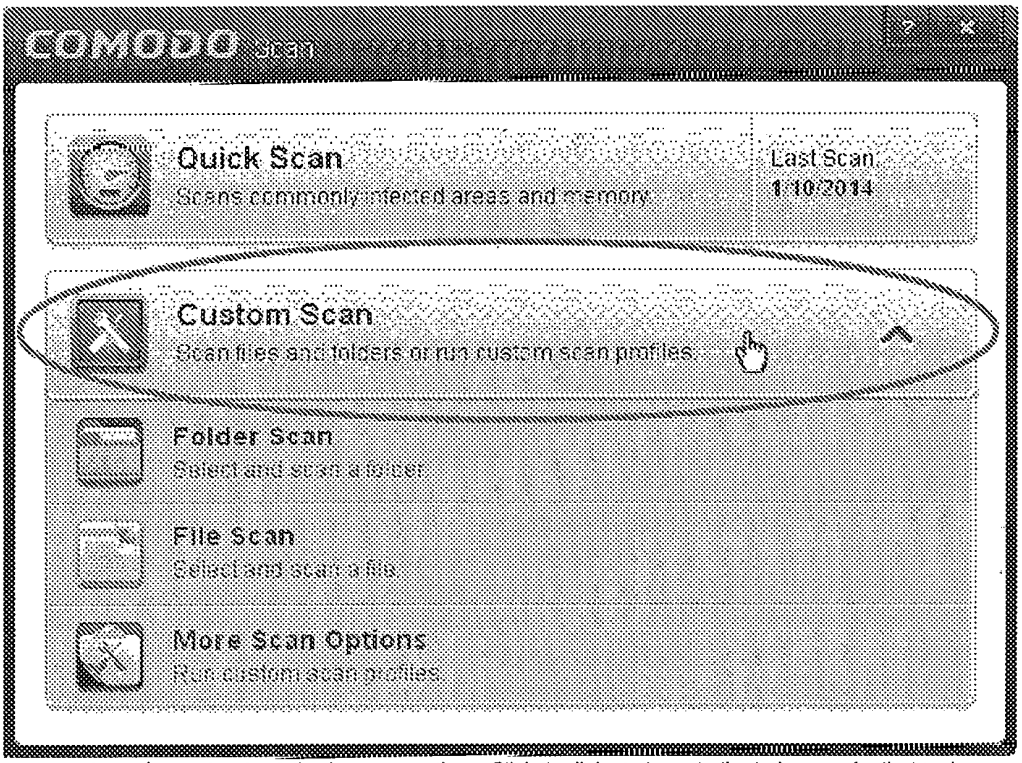


- Click 'Close' to exit.

2.1.4. Run a Custom Scan

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

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



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

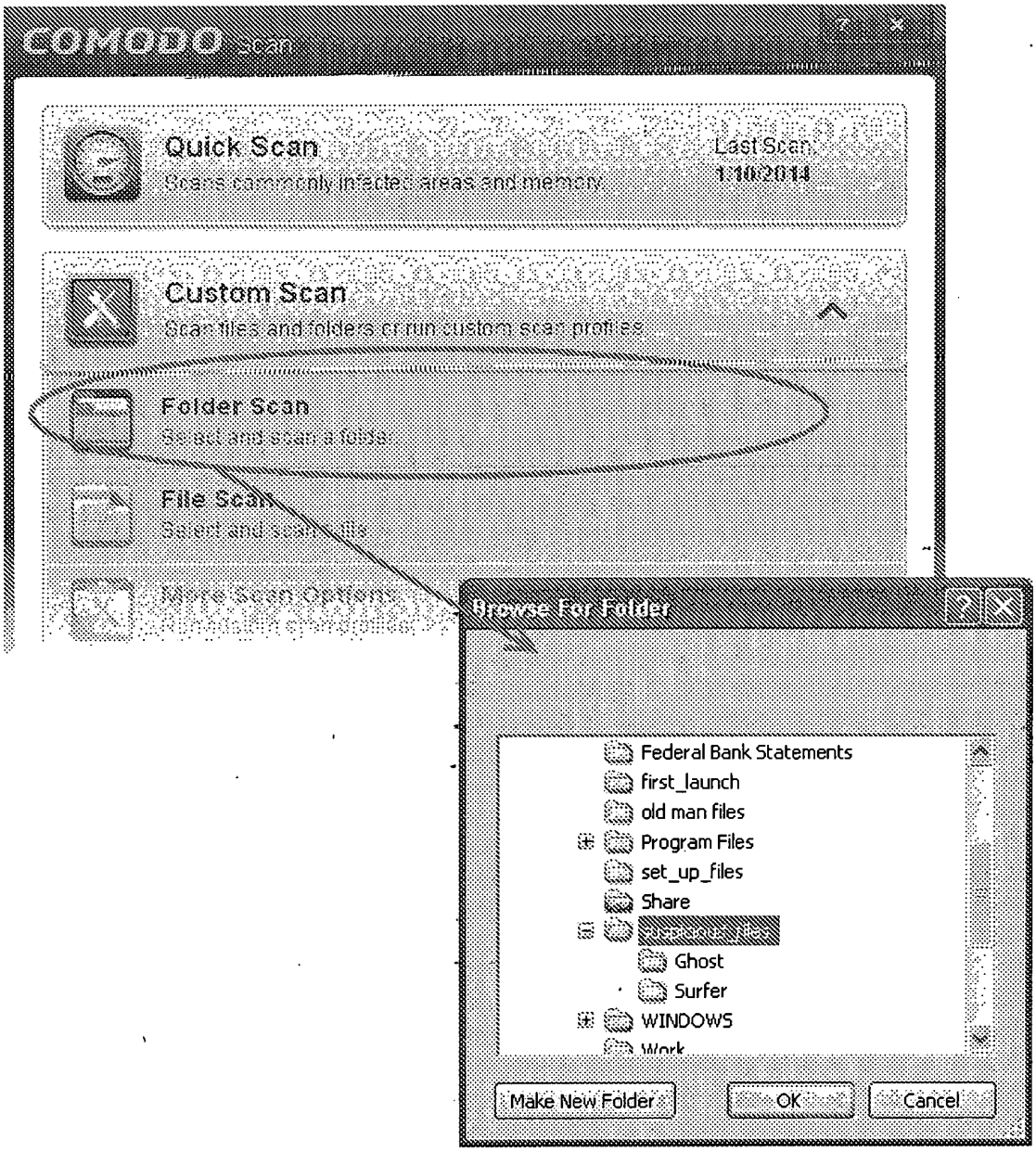
- Folder Scan - scan individual folders
- File Scan - scan an individual file
- More Scan Options - create a custom scan profile here

2.1.4.1. Scan a Folder

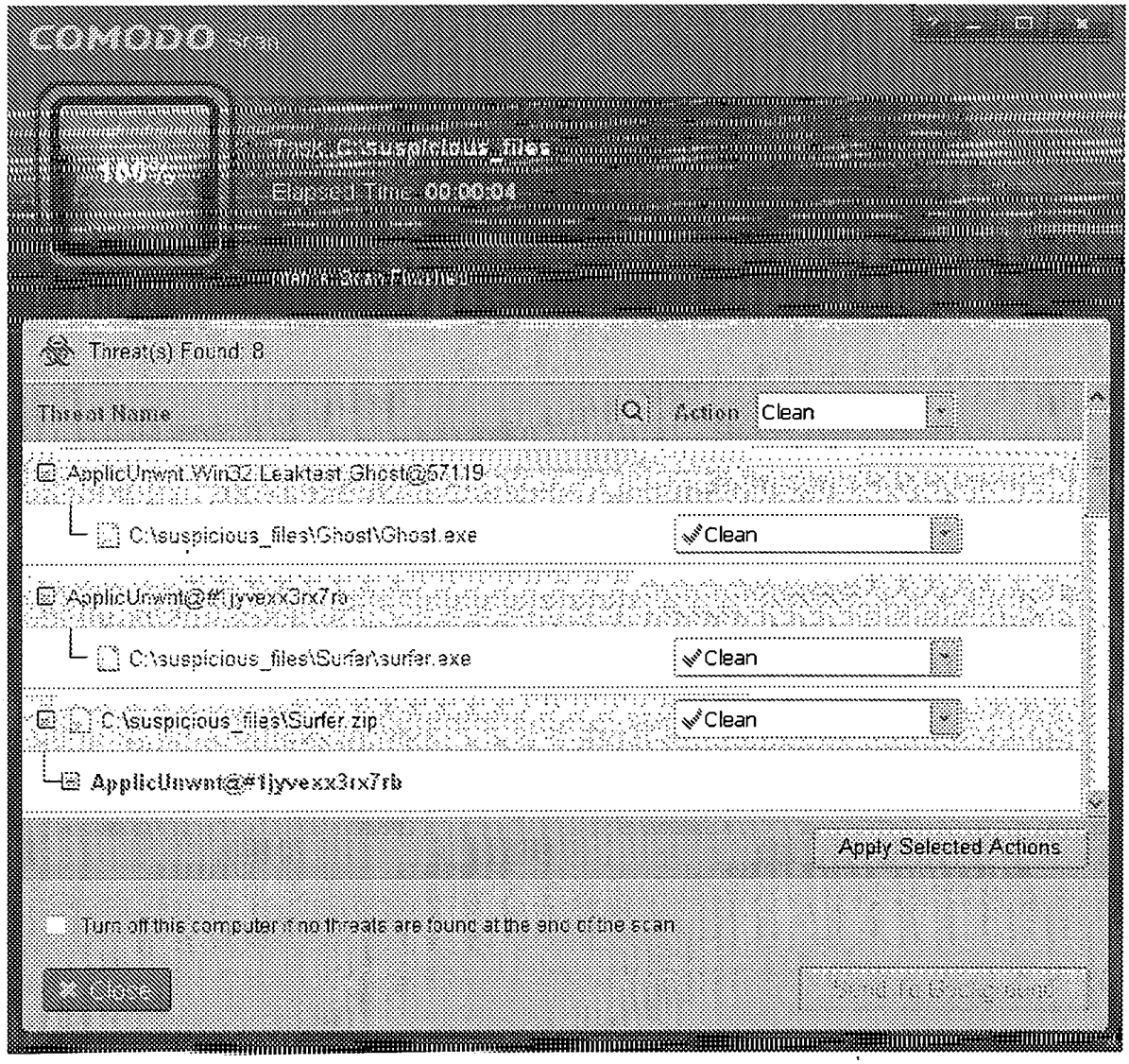
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan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

To scan a specific folder

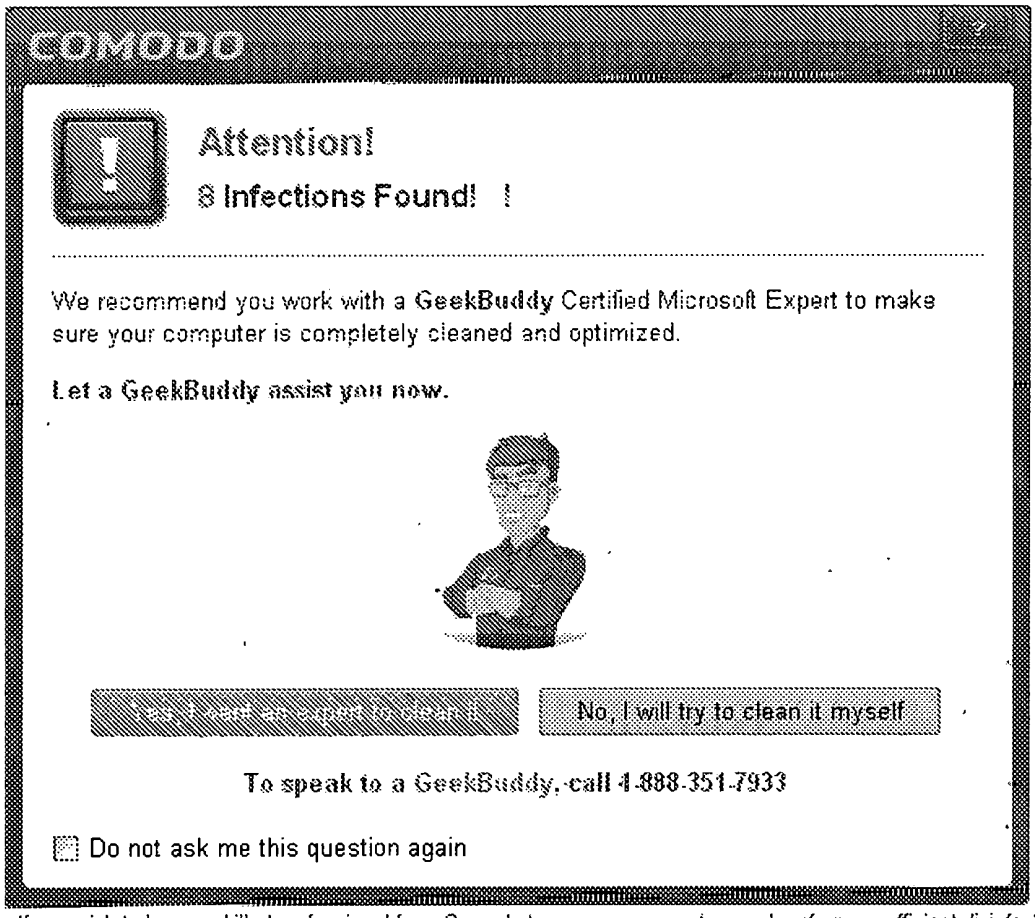
- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'Folder Scan' from the 'Custom Scan' pane
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click OK.



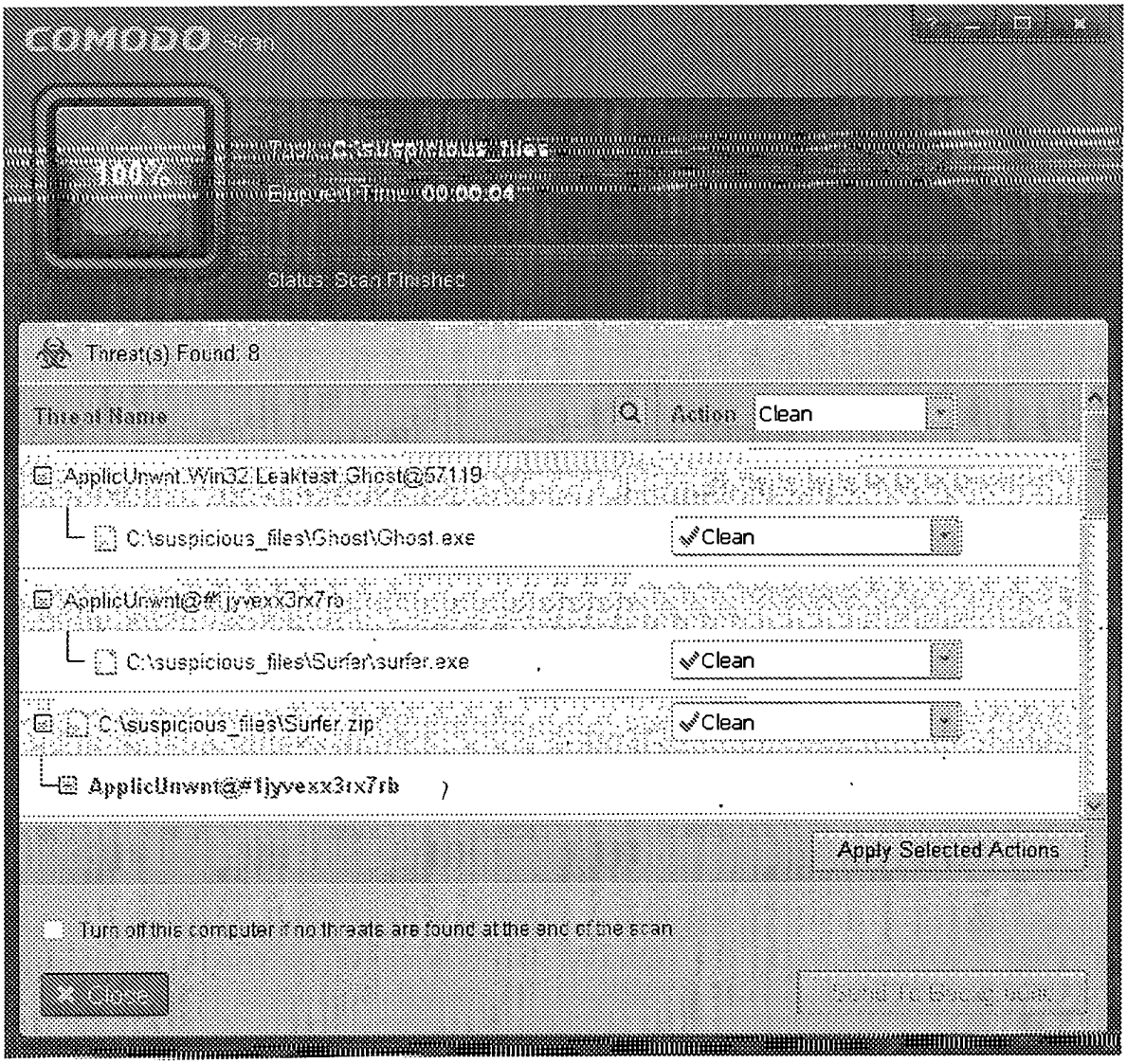
The folder will be scanned instantly and the results will be displayed with a list of any identified infections



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



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



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

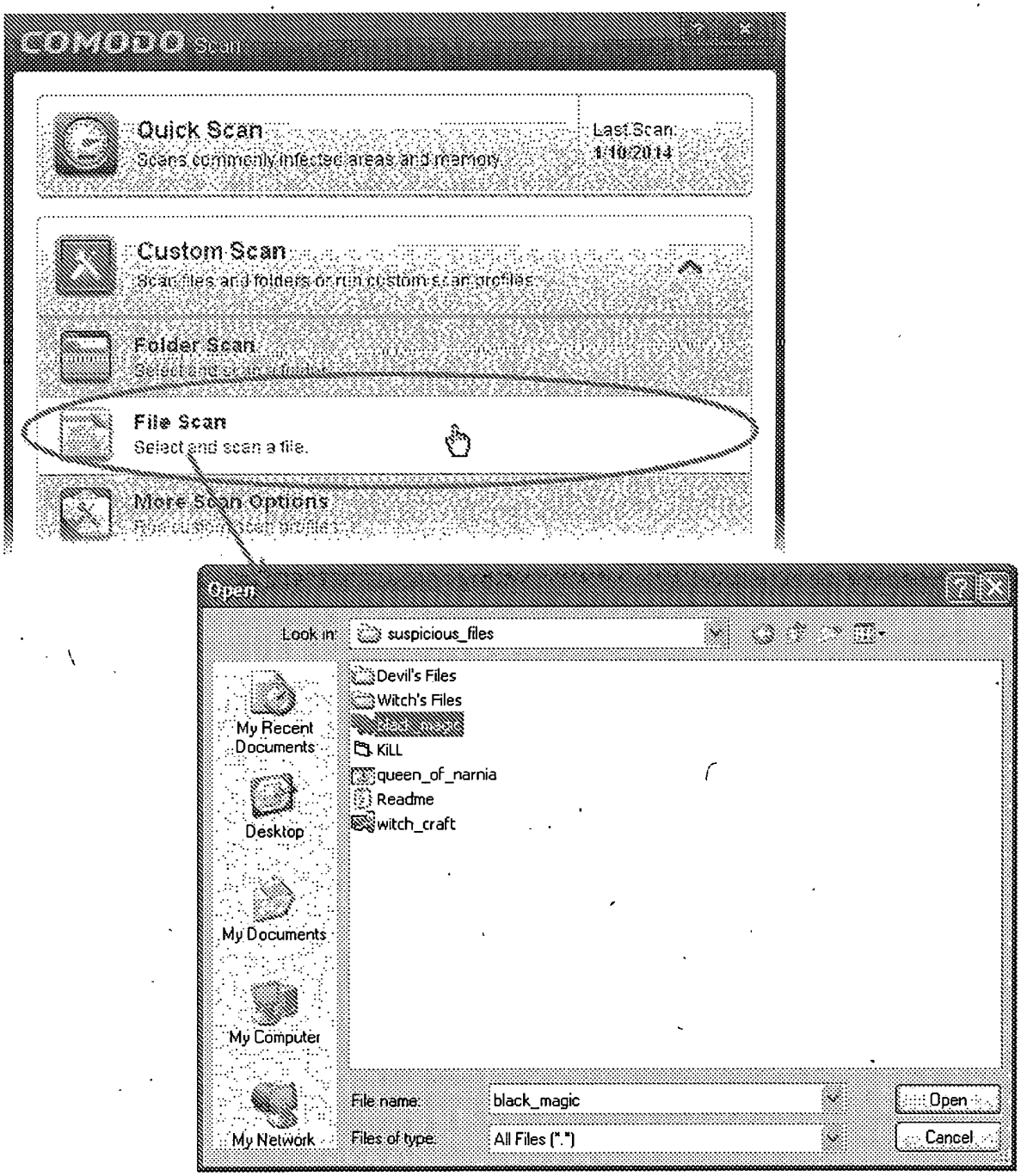
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CIS interface or by right clicking it. Refer to Scan Individual File/Folder for more details.

2.1.4.2. Scan a File

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

To scan a specific file

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

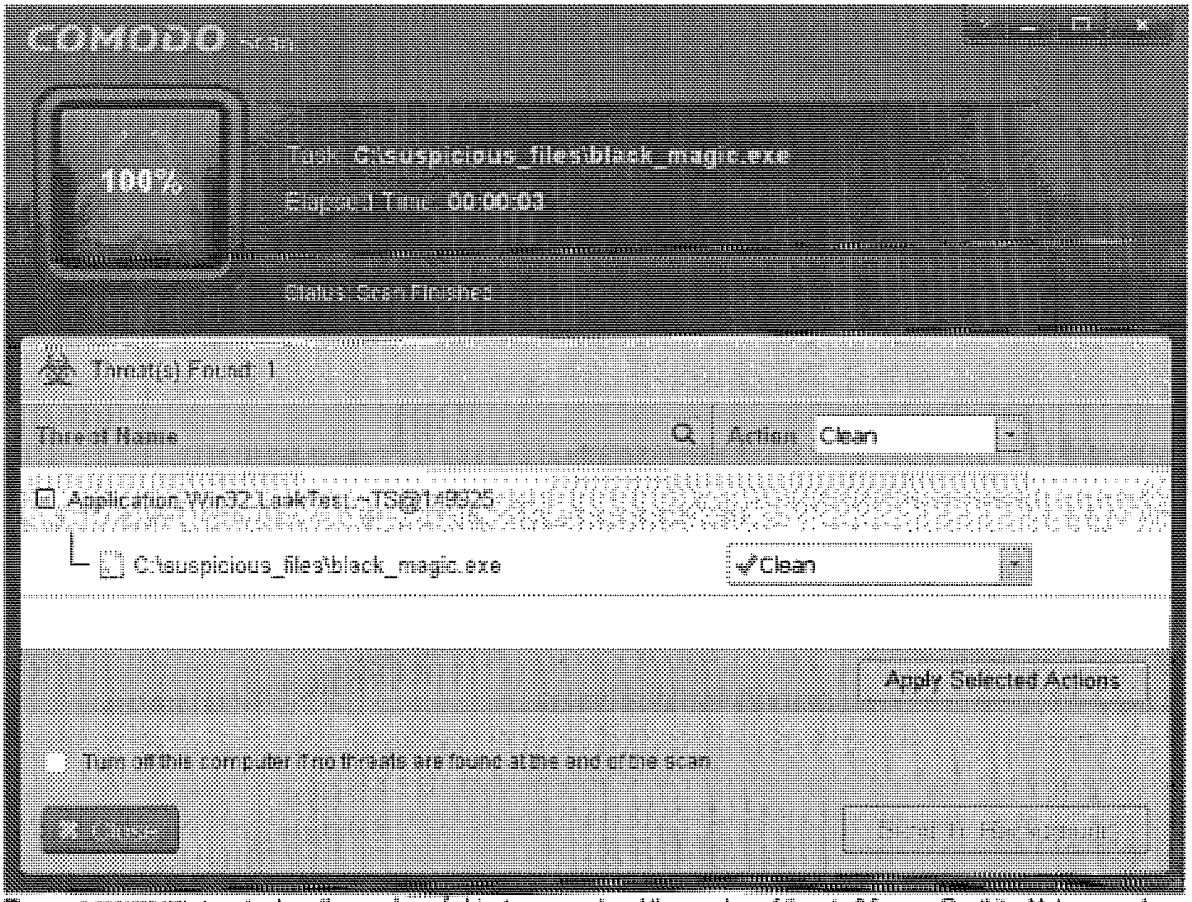


The file will be scanned instantly.

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



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



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

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

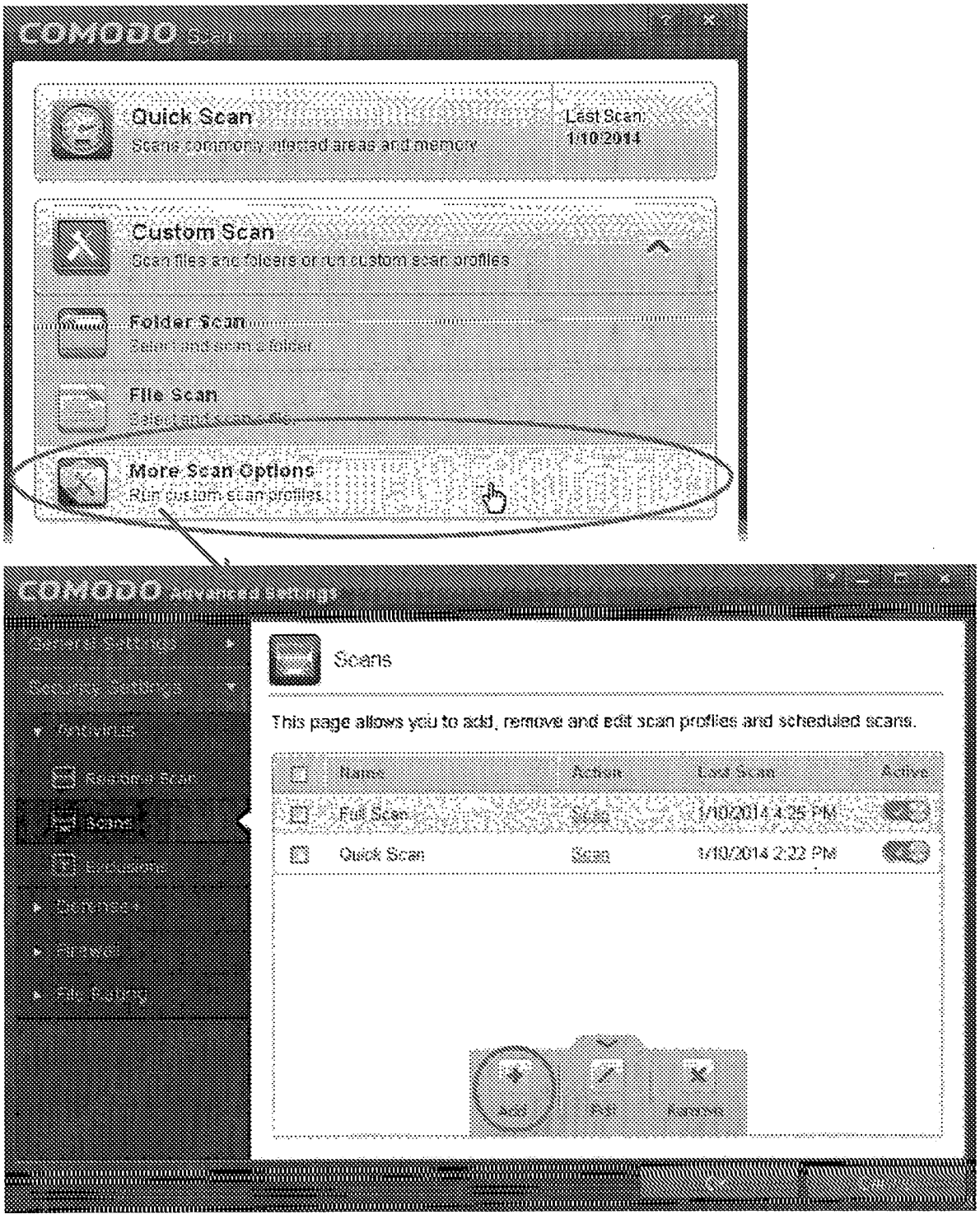
2.1.4.3. Create, Schedule and Run a Custom Scan

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

- Creating a Scan Profile
- Running a custom scan

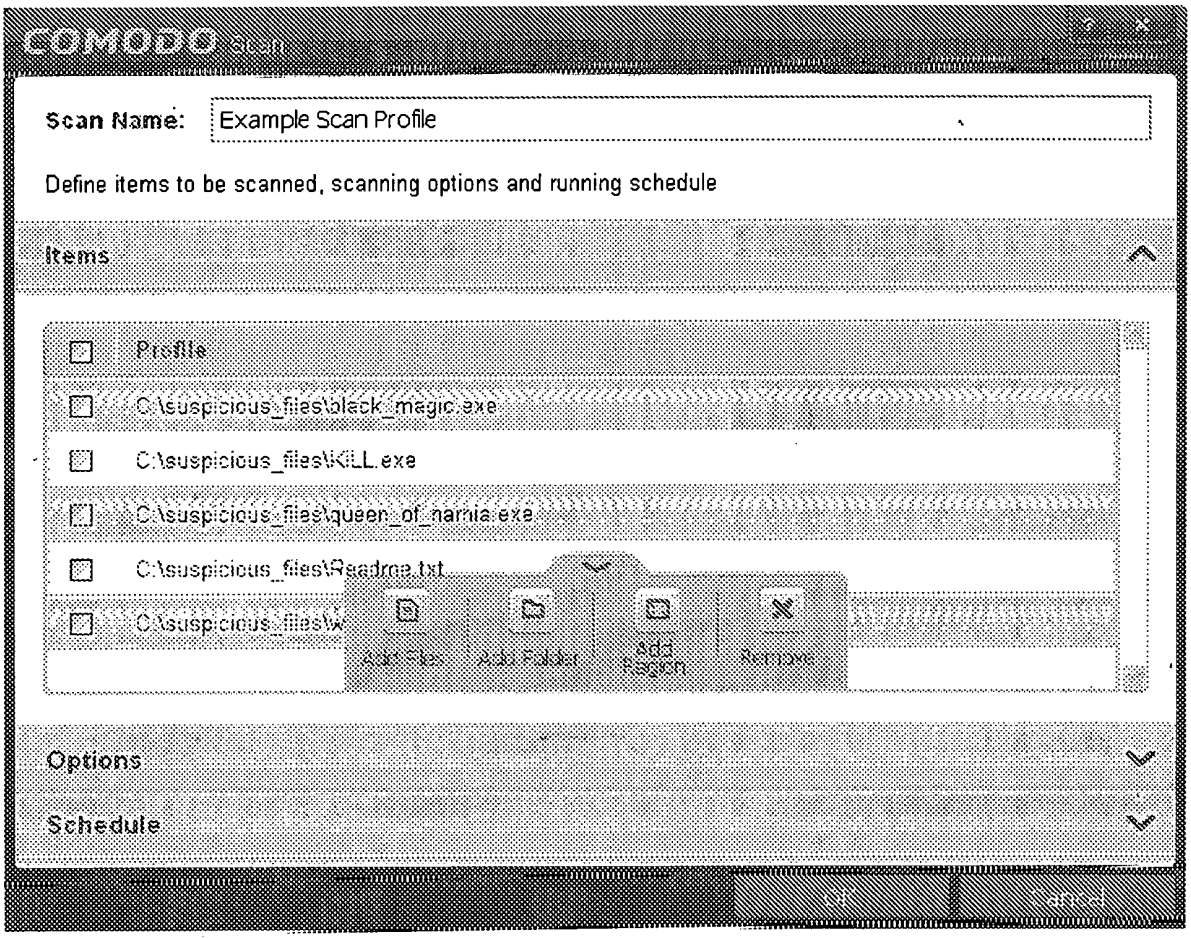
To create a custom profile

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

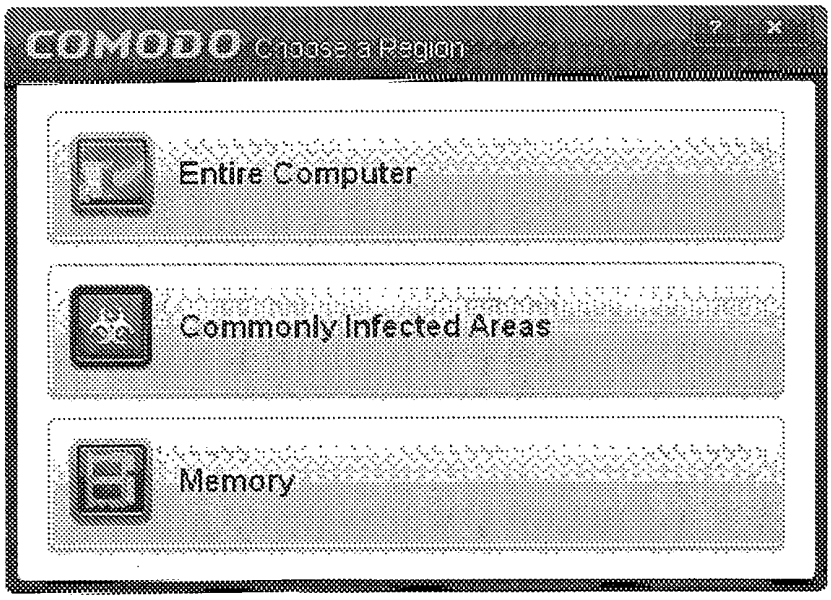


The scan profile interface will be displayed.

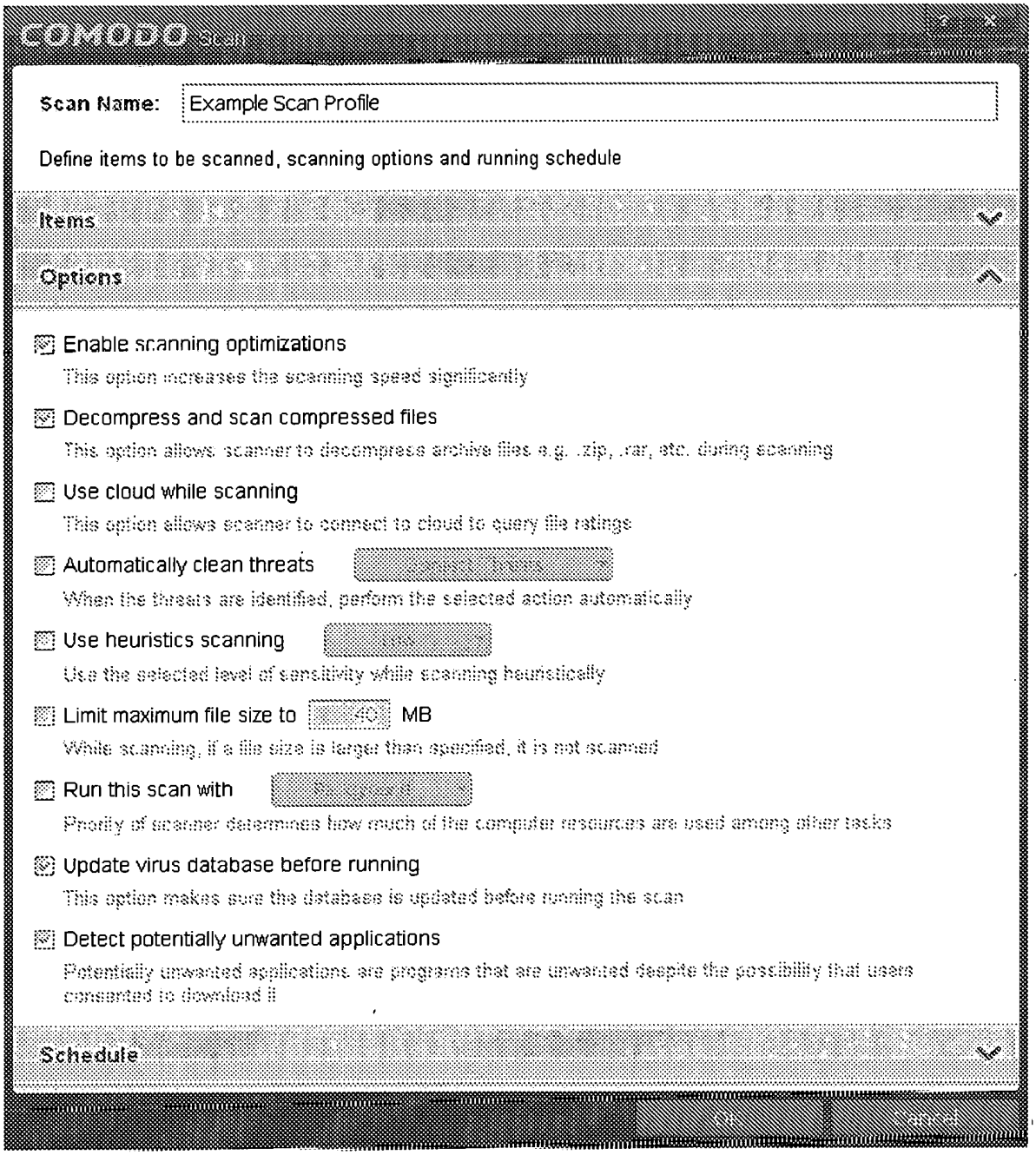
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



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



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



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

scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Disabled).***

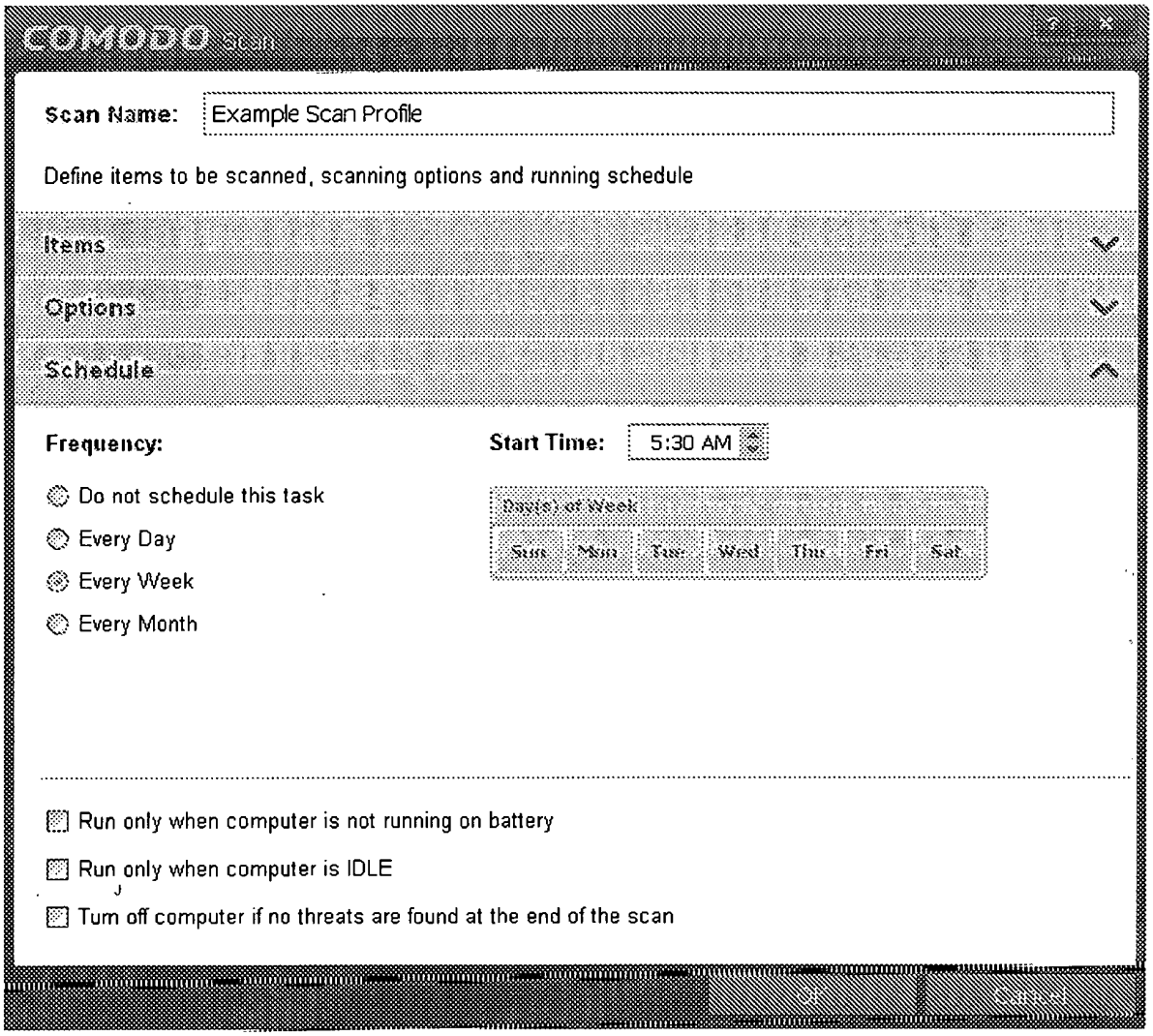
Background Info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so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

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

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

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

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

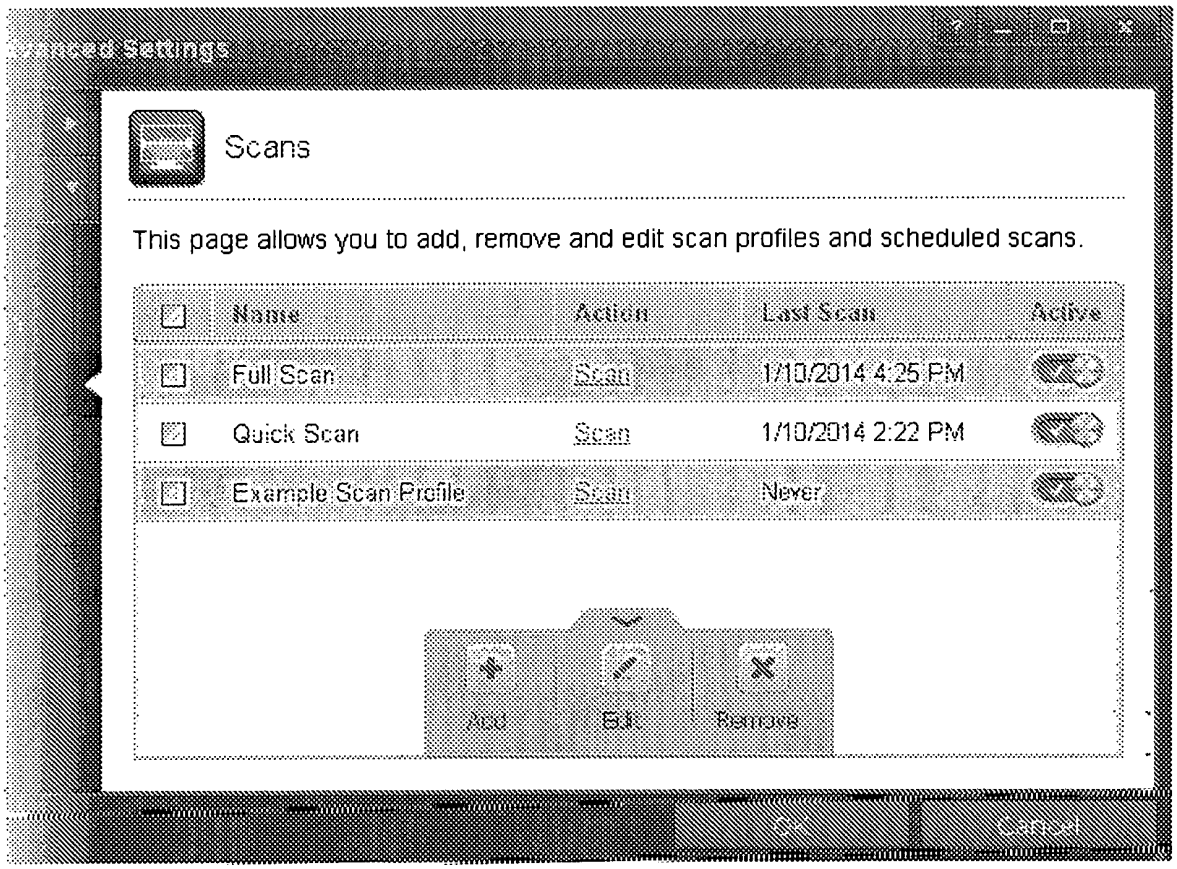


- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - The Antivurus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field
- **Every Week** - The Antivurus starts scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - The Antivurus starts scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery.
- **Run only when computer 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.

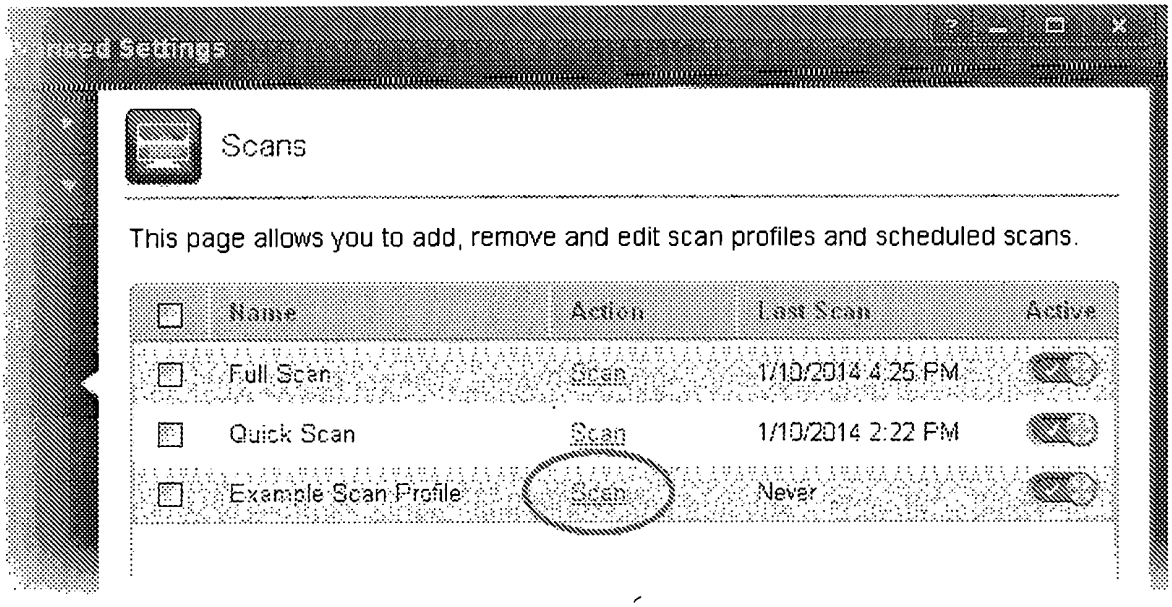
Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.

The profile will be available for deployment in future.

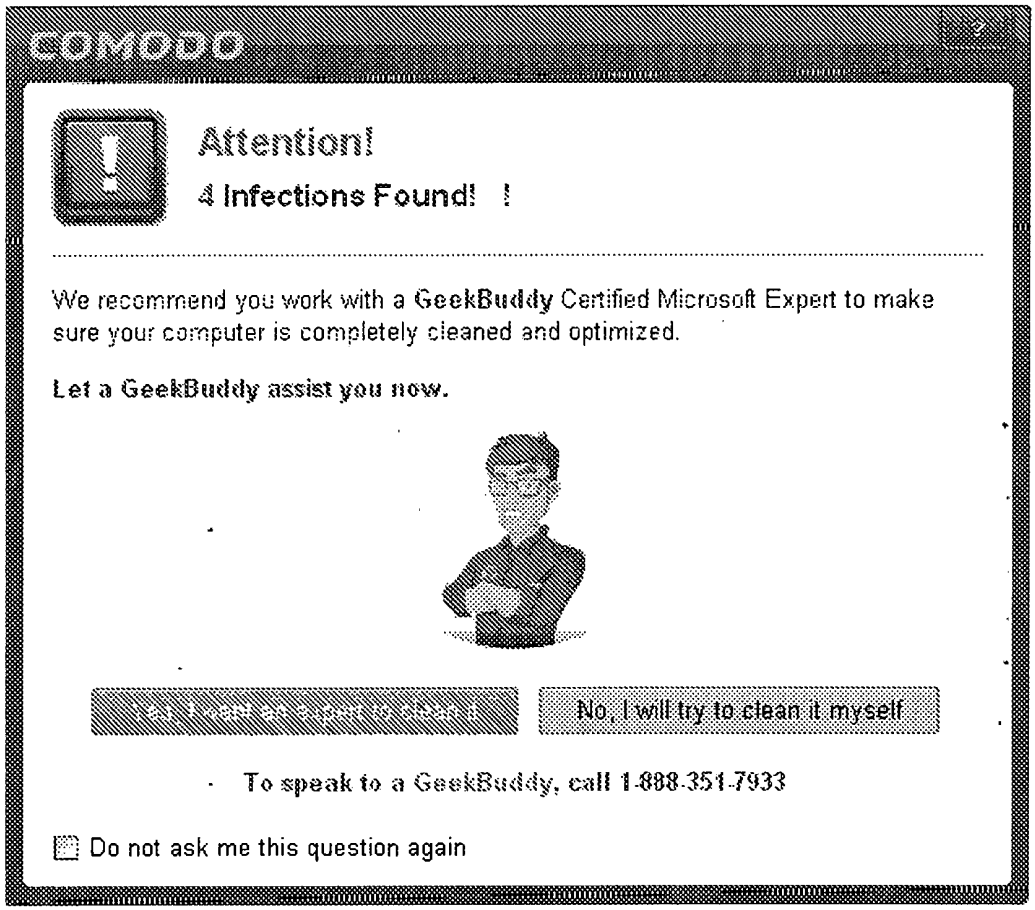


To run a custom scan

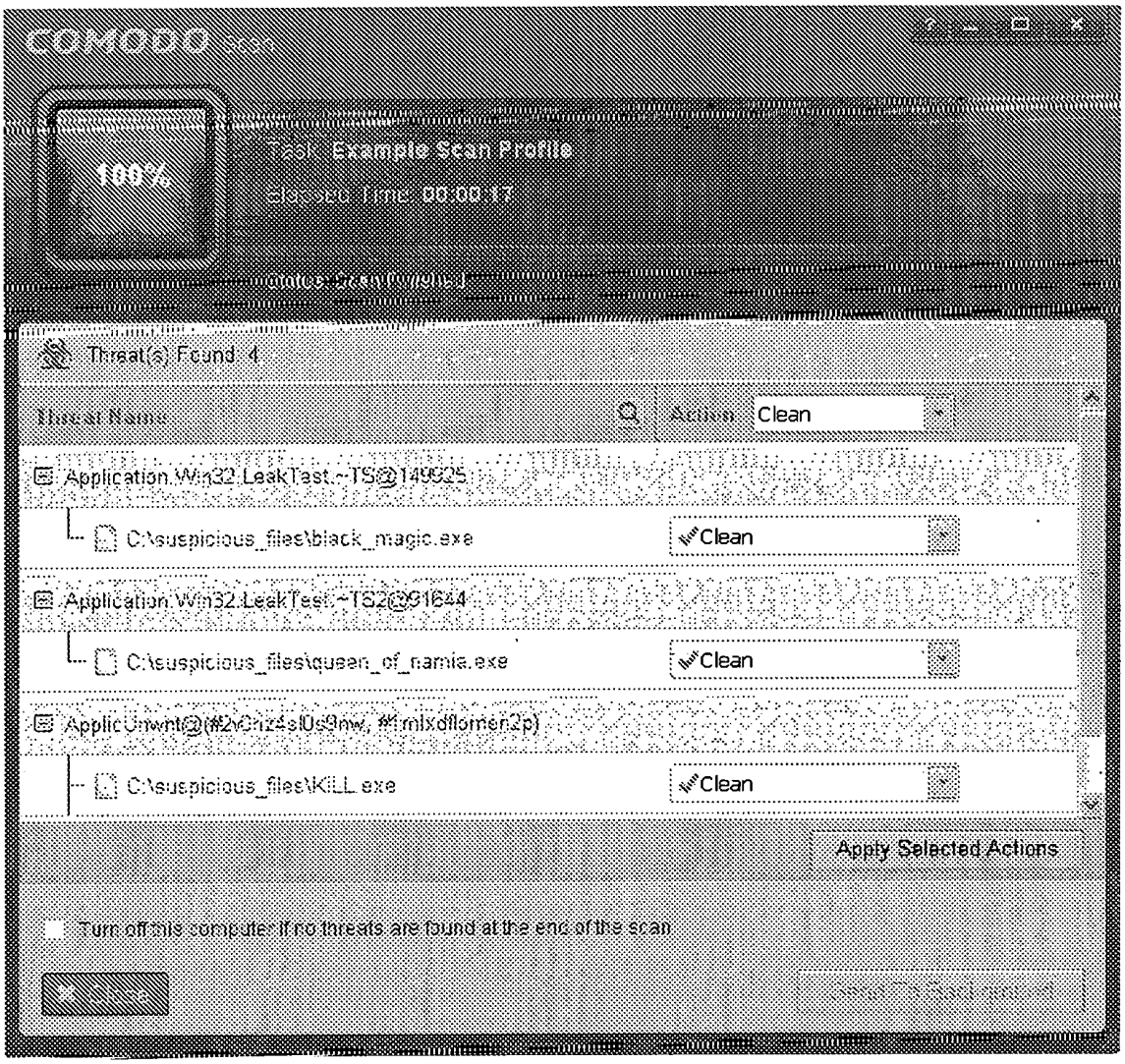
- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click 'Scan' beside the required scan profile.



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



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



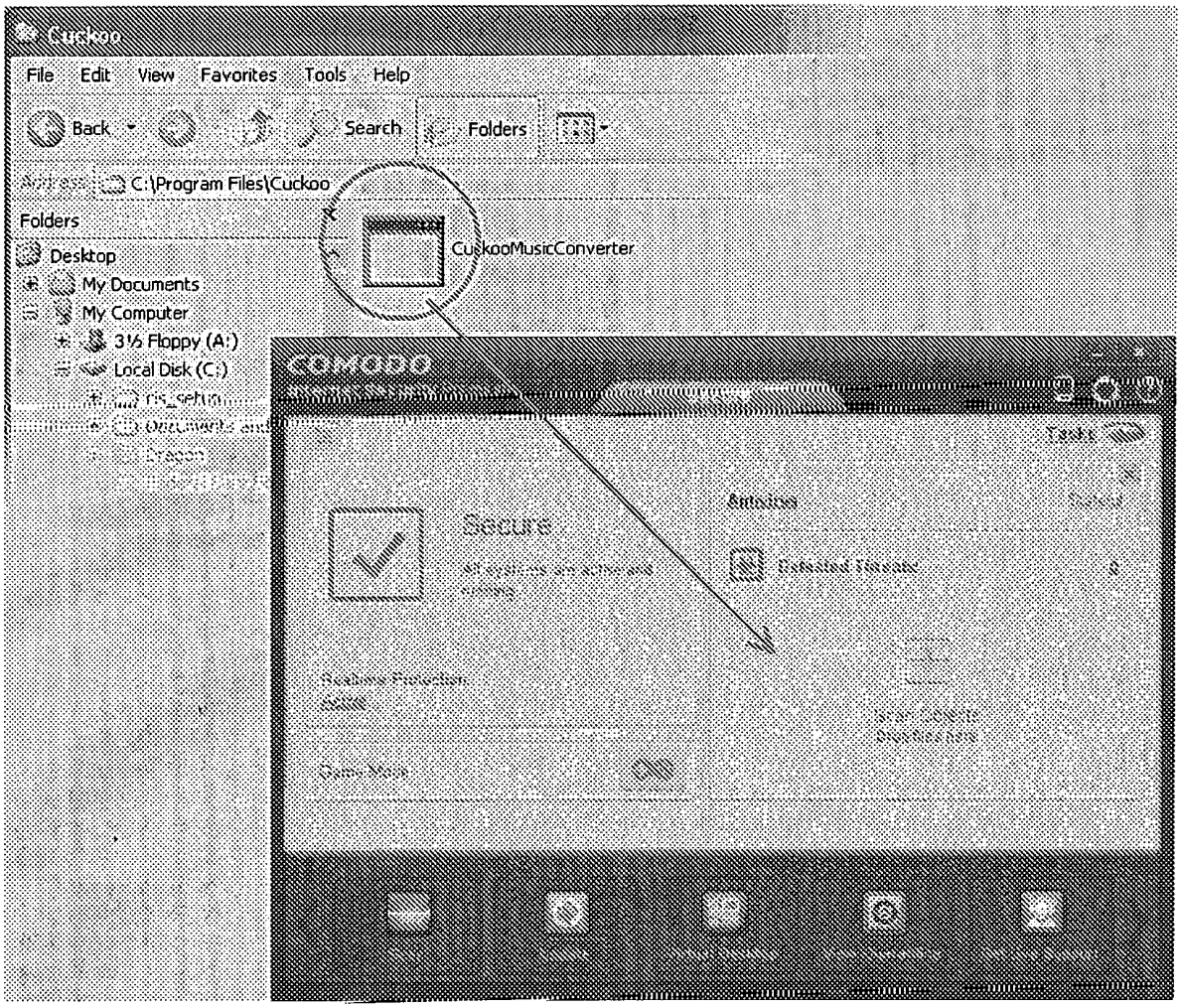
- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

2.2. Instantly Scan Files and Folders

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

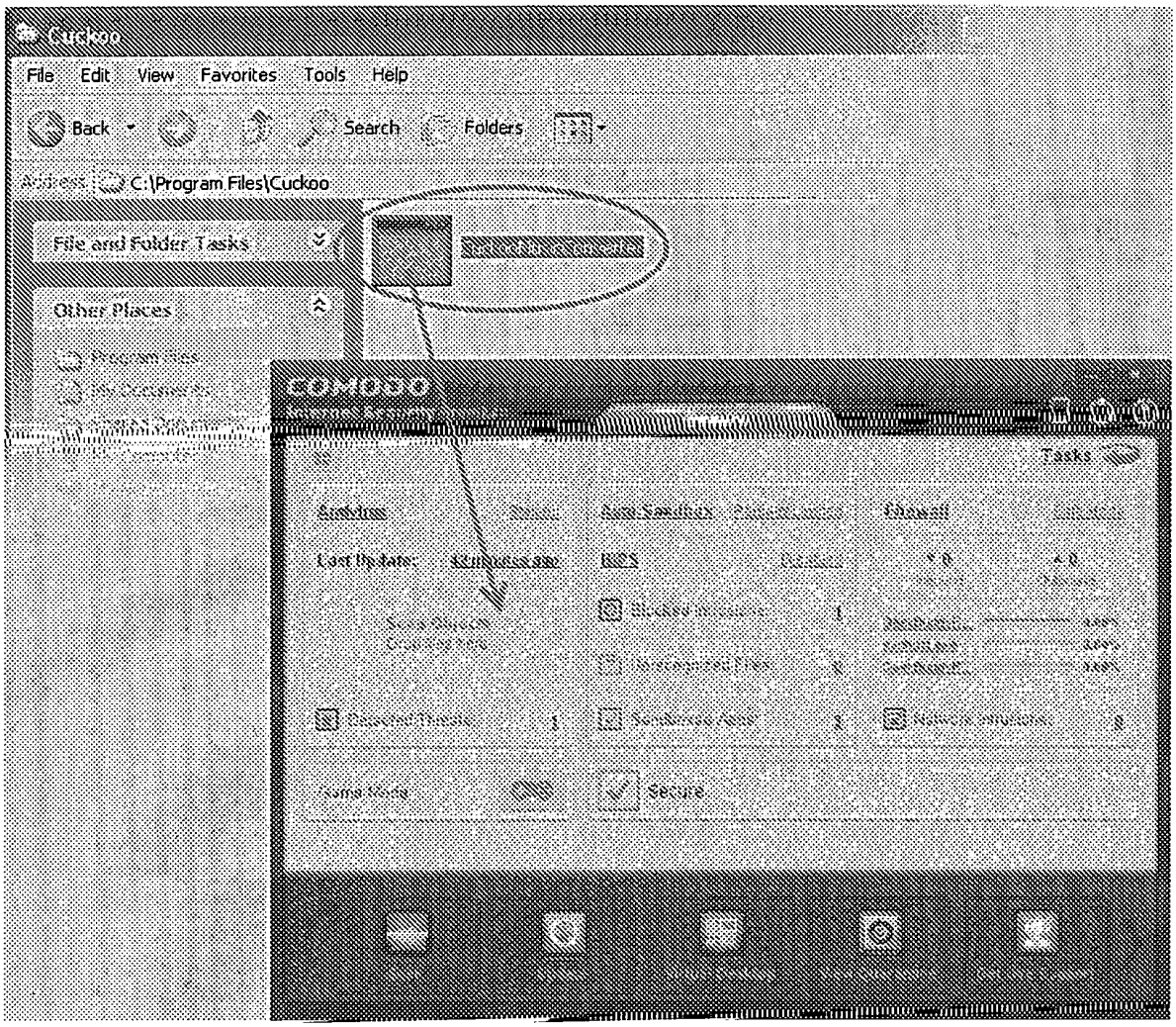
To instantly scan an item

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



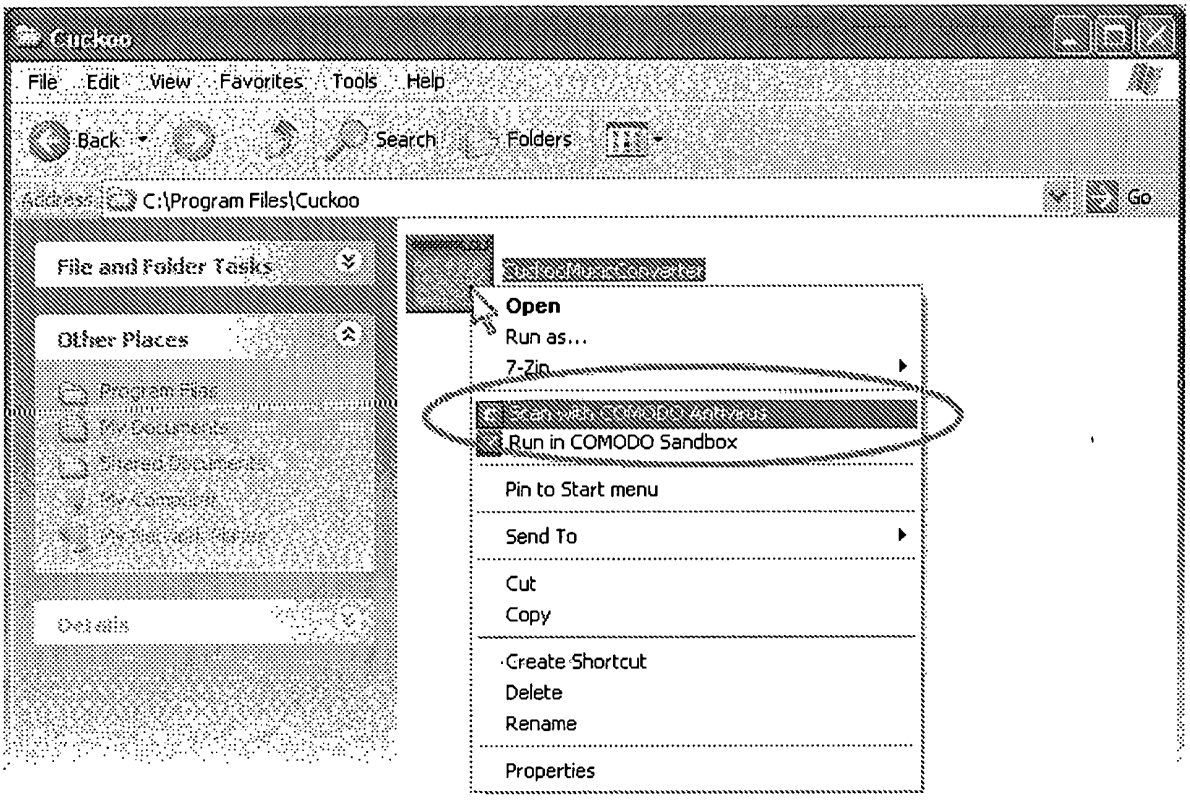
OR

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

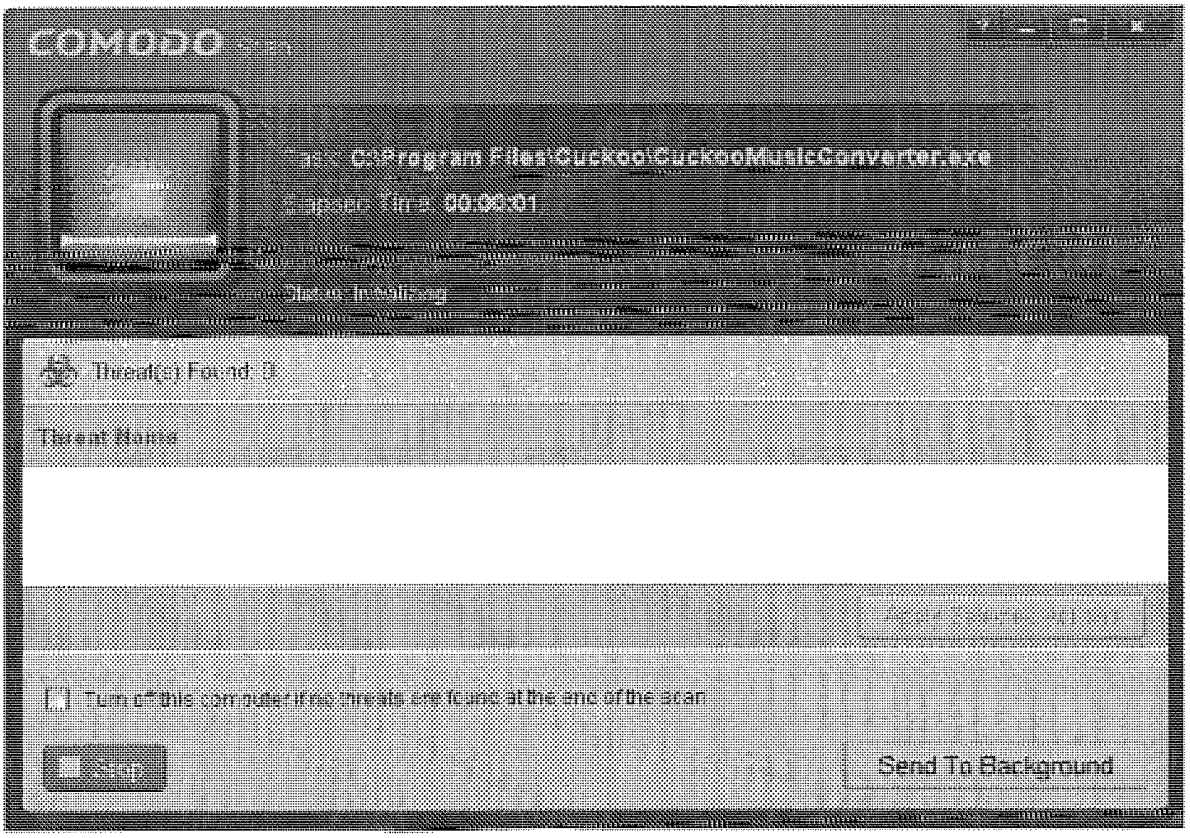


OR

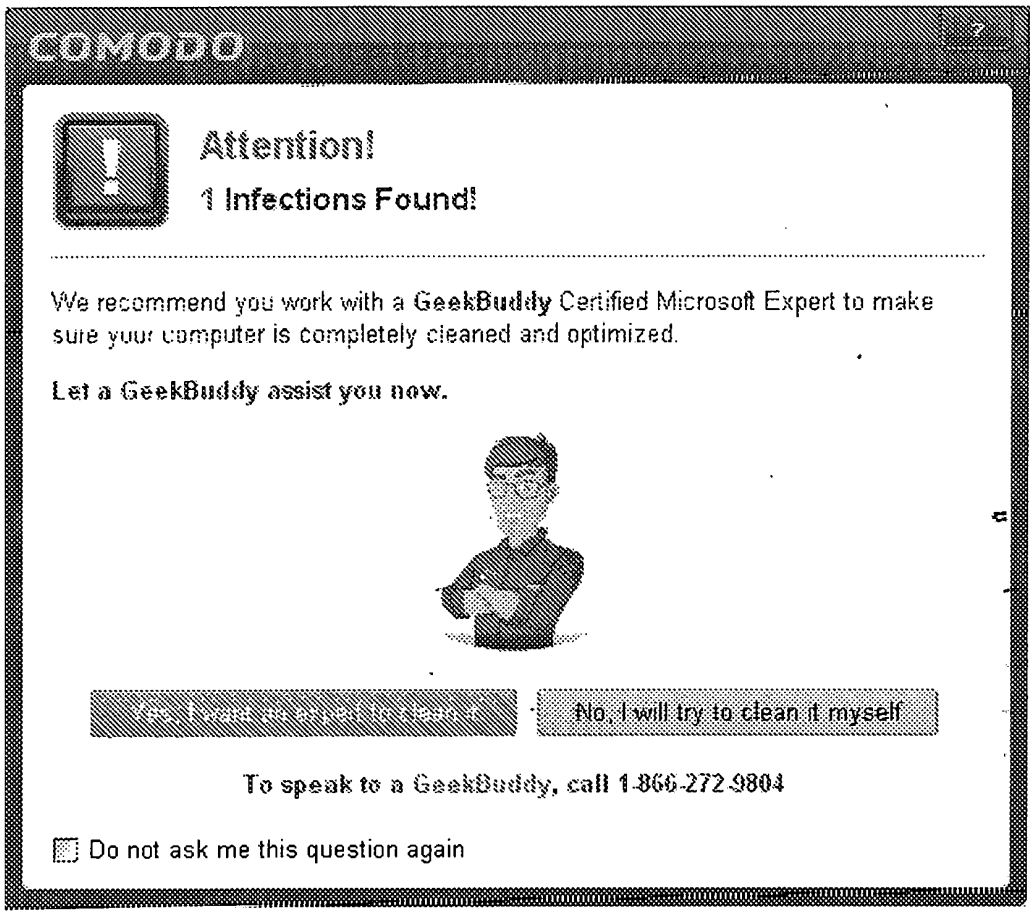
- Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



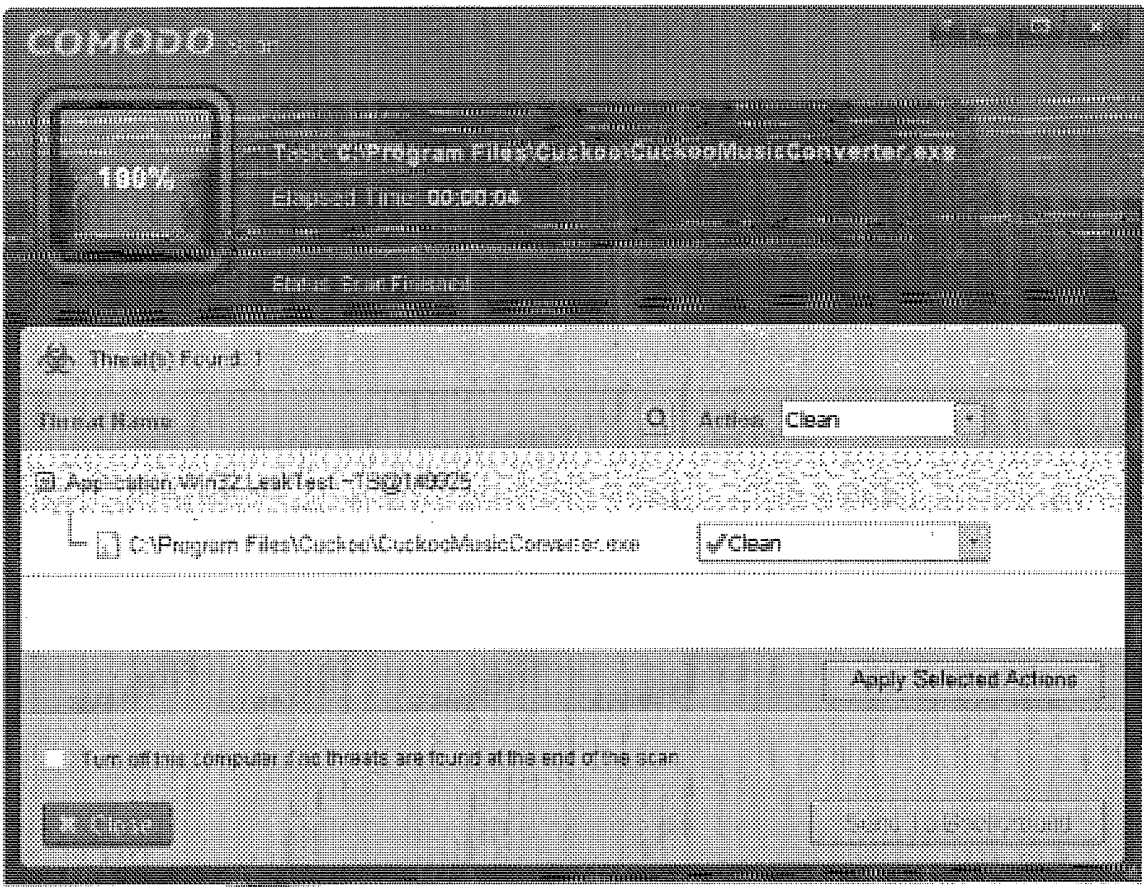
The item will be scanned immediately.



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



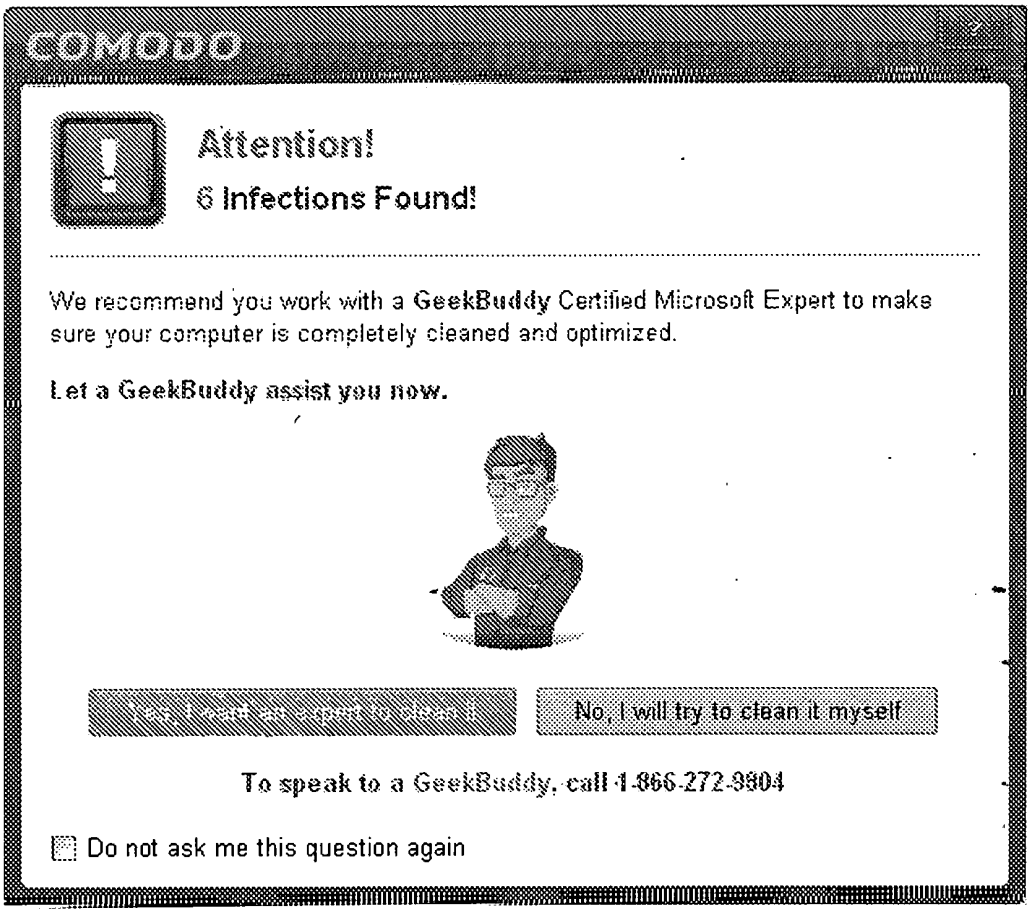
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up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



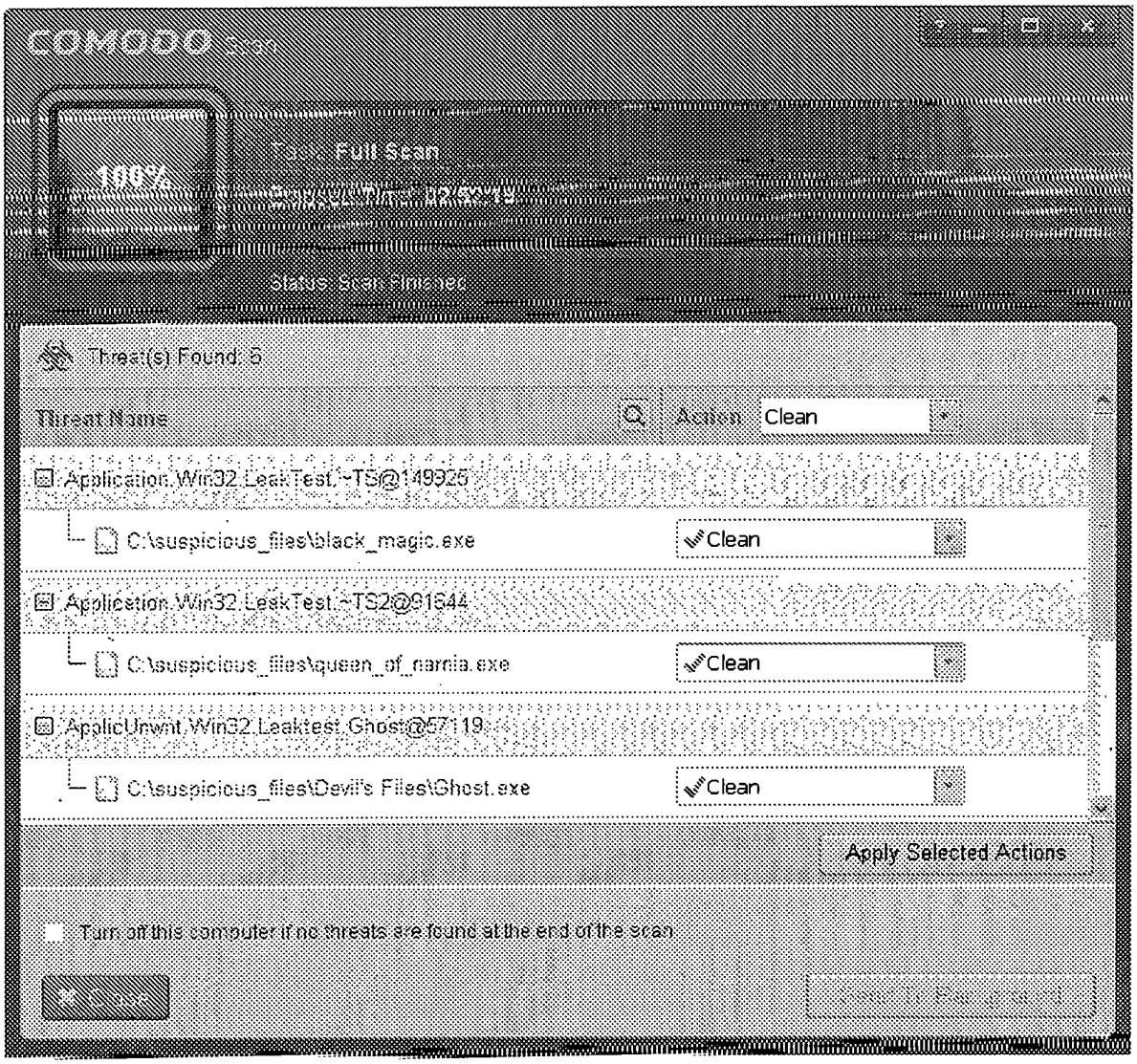
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

2.3. Processing Infected Files

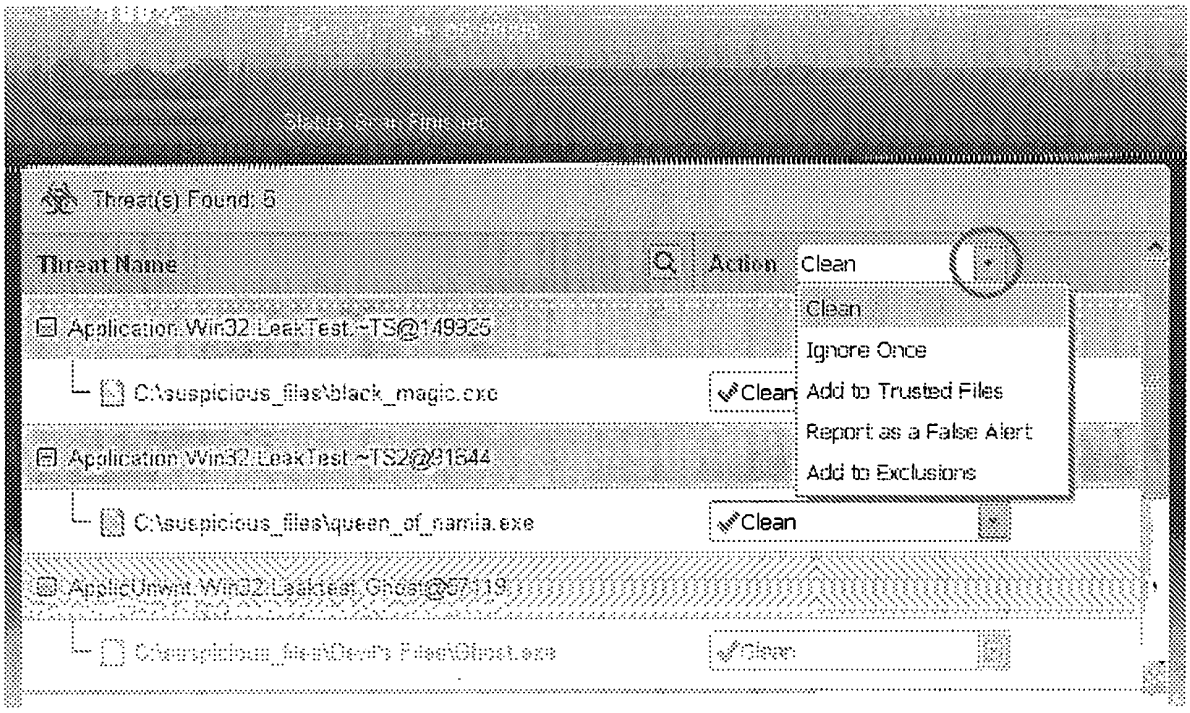
On completion of any on-demand or scheduled scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



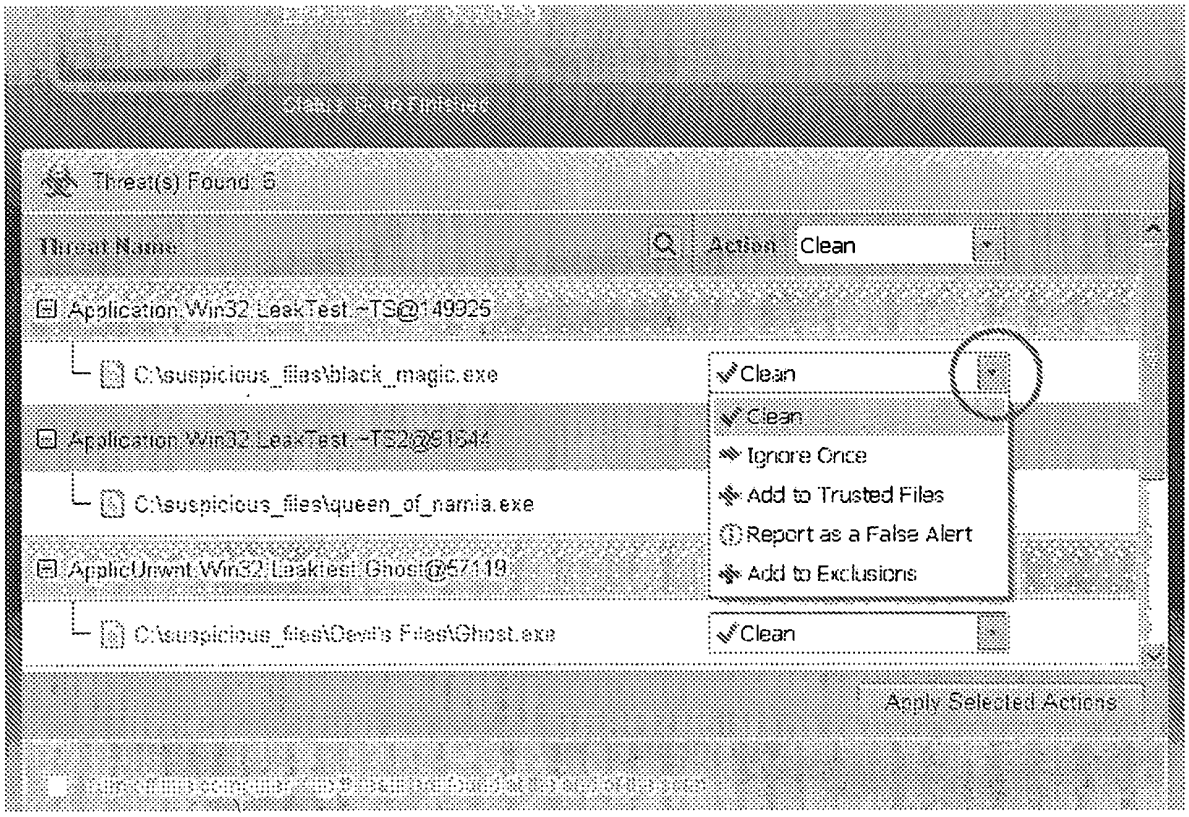
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



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



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



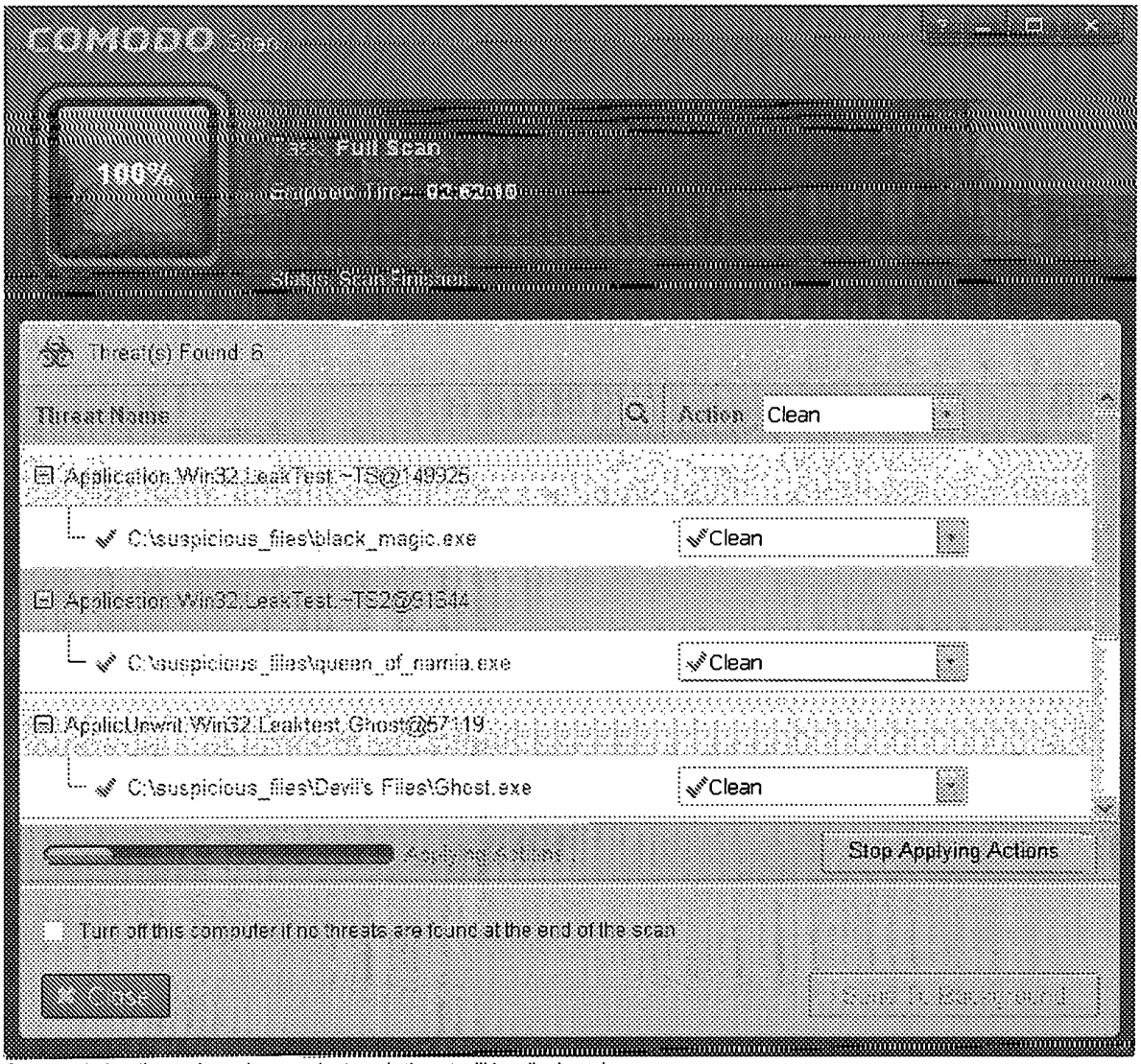
The choices for the actions available are:

- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application safe. If the disinfection routine is not available, Comodo Antivirus will

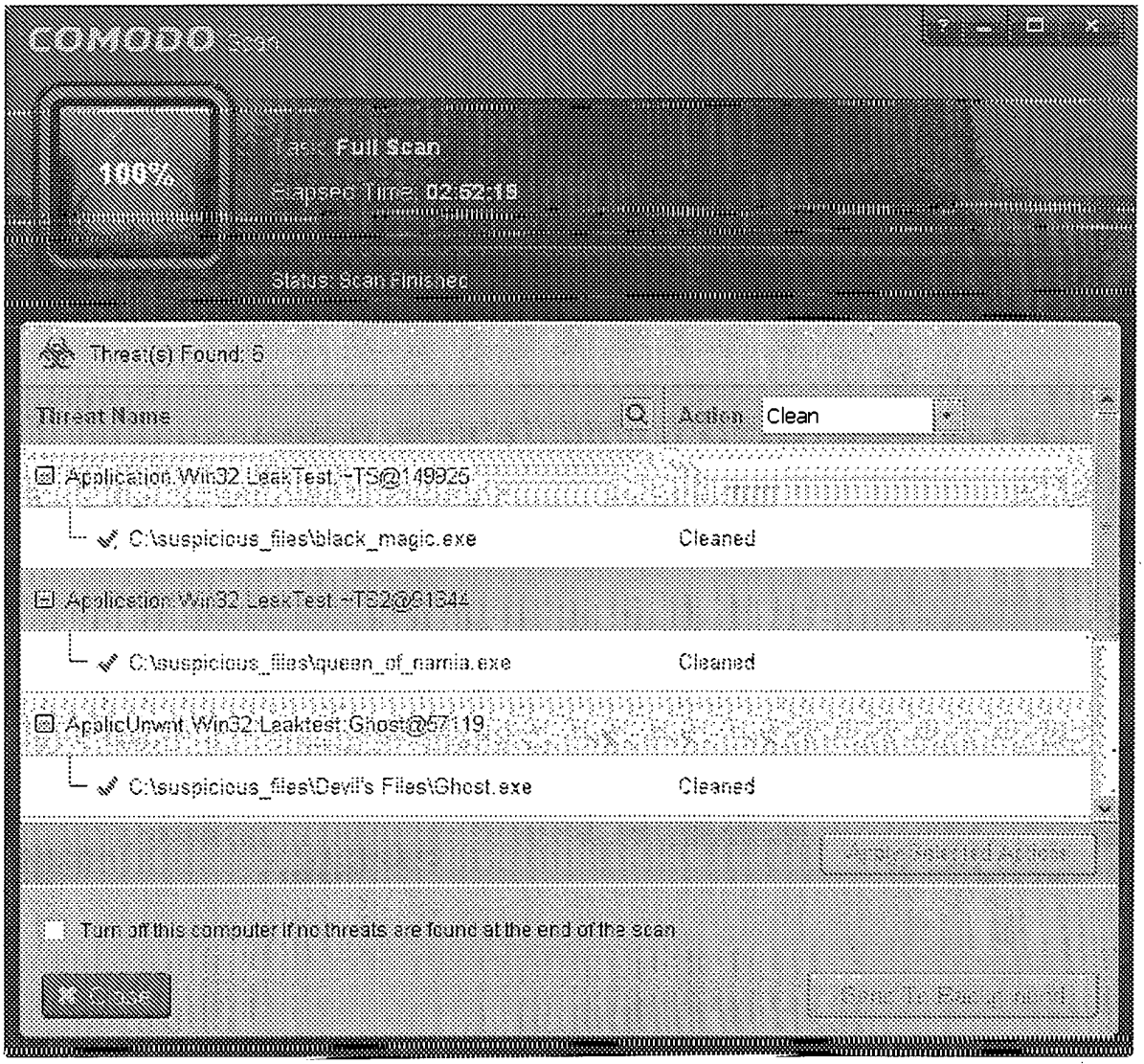
move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to Manage Quarantined Items.

- **Ignore Once** - If you want to ignore the threat this time only, select 'Ignore Once'. The file will be ignored only at that time. If the same application invokes again, the Antivirus will report it as a threat.
- **Add to Trusted Files** - If you trust the file, select 'Add to Trusted Files'. The file will be moved to Trusted Files list. The alert will not generated if the same application invokes again.
- **Report as a False Alert** - If you are sure that the file is safe, select 'Report as a False Alert'. The Antivirus will send the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.
- **Add to Exclusions** - The file will be moved to Exclusions list and will not be scanned in future. The alert will not generated if the same application invokes again.

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



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



- Click 'Close' to close the results window.

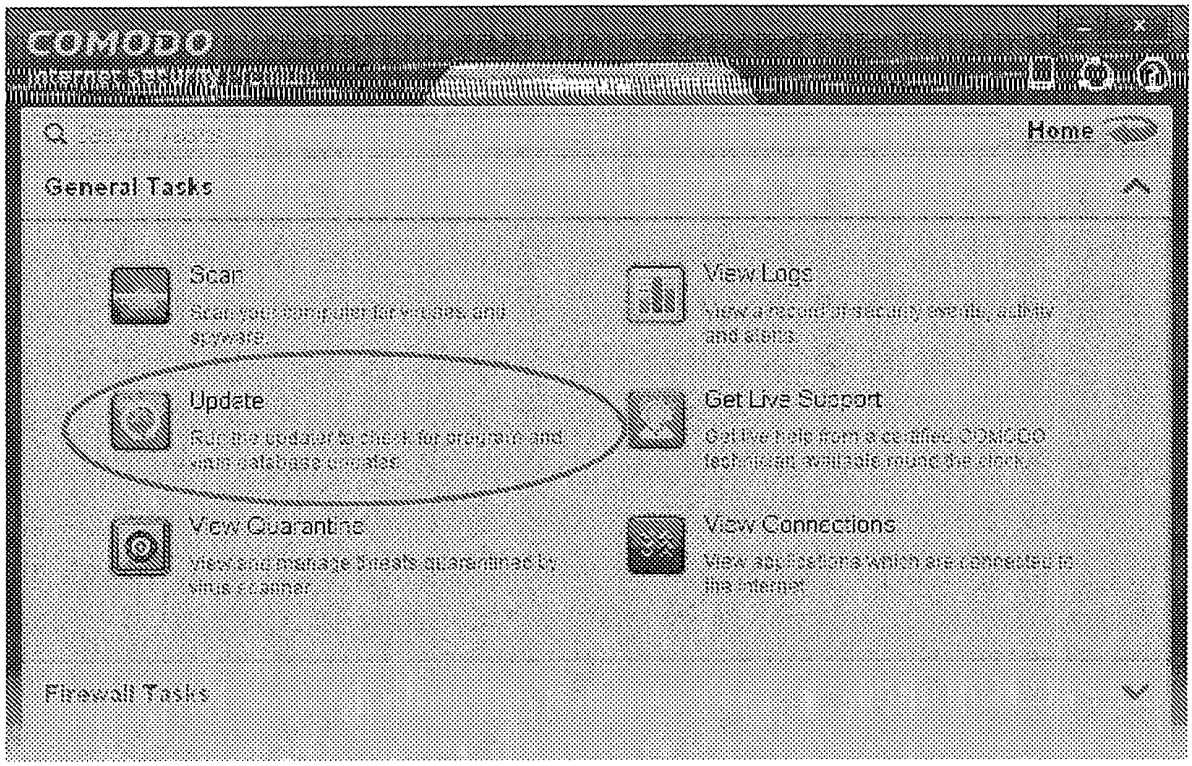
2.4. Manage Virus Database and Program Updates

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

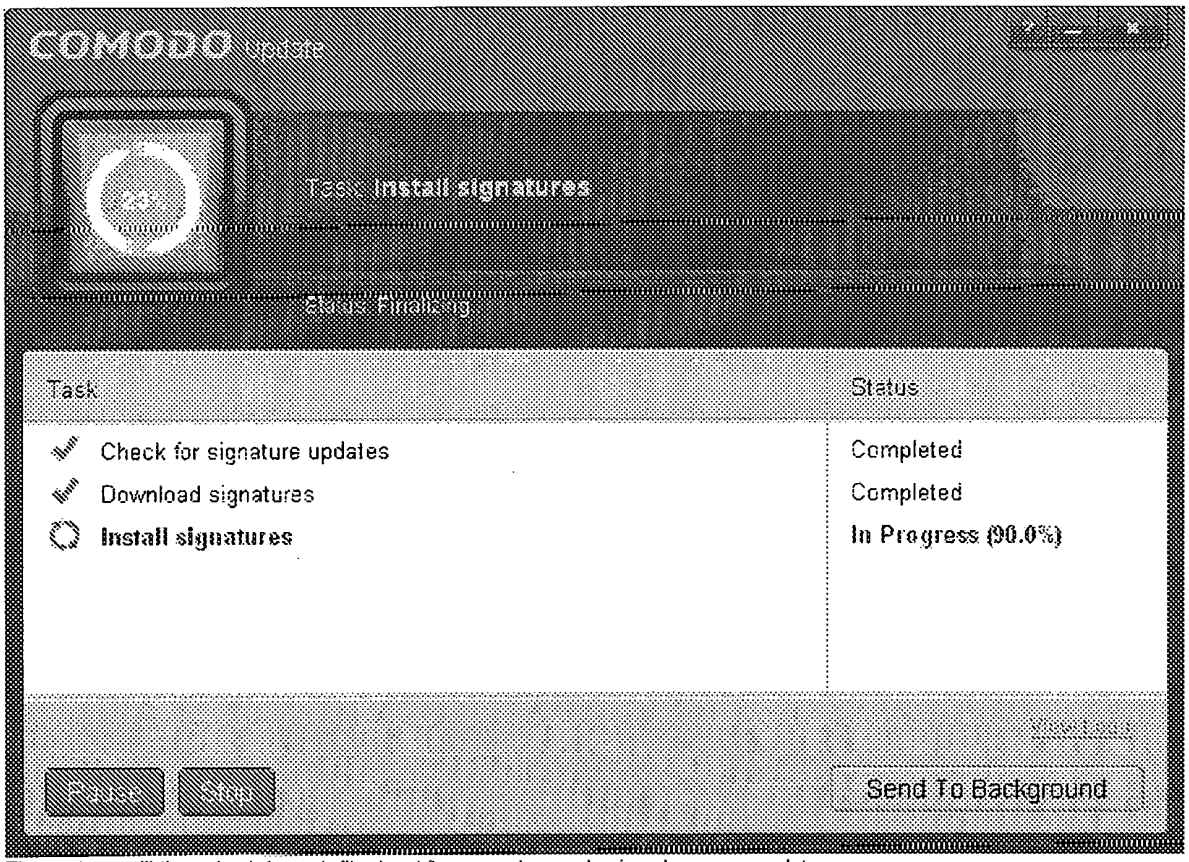
Note: You must be connected to Internet to download updates.

To manually check for the latest virus and program updates

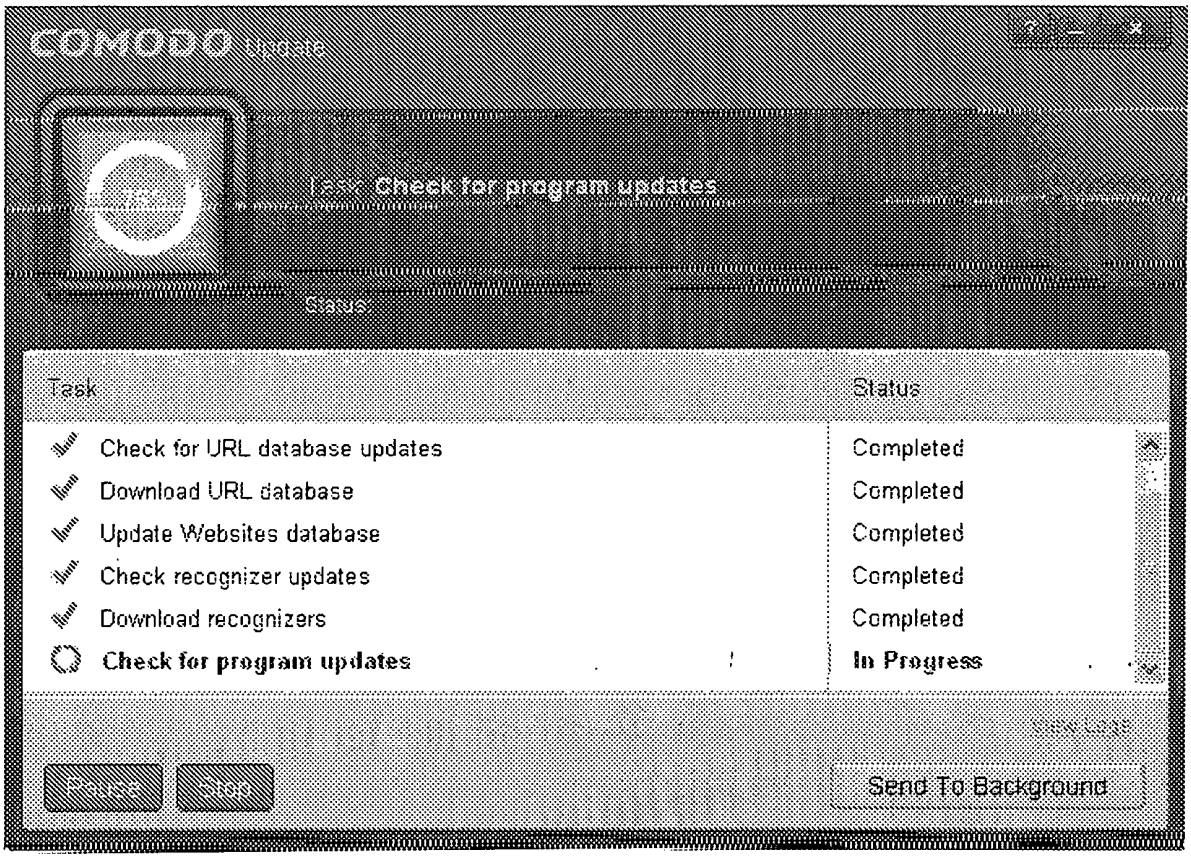
1. Switch to the 'Tasks' screen and click 'General Tasks' to open the 'General Tasks' interface.
2. Click 'Update'. The application will start checking for program and database updates



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



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



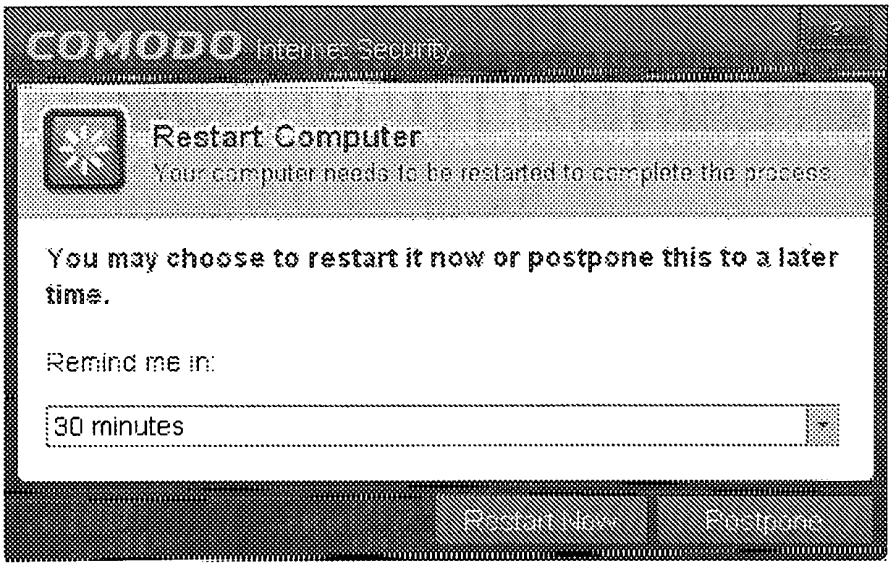
When all updates have been download you will be asked to confirm installation at the following dialog:



- Click 'Yes' to begin installation:

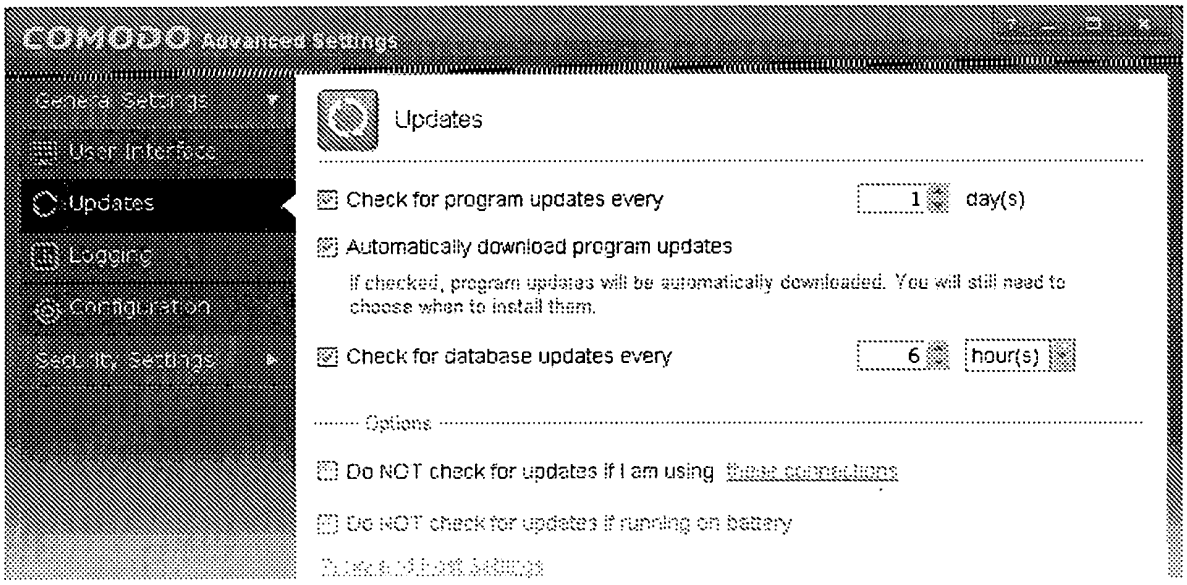
During the update process, new software components or features sometimes become available for installation. As these may alter the behavior of CIS in some manner, please carefully review these types of update before agreeing to their installation.

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



Automatic Updates

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

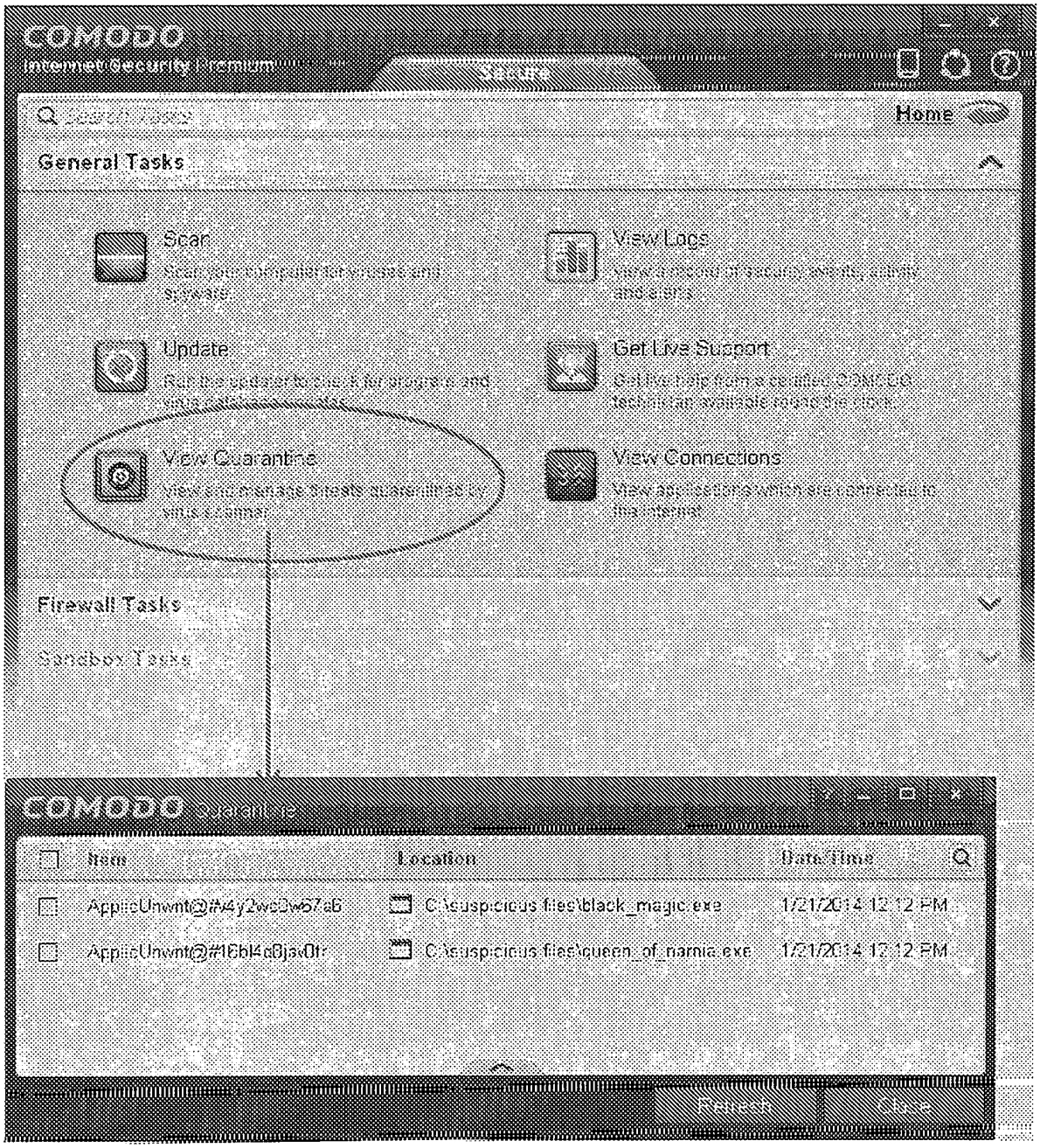


You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. Refer to Scan Profiles for more details.

2.5. Manage Quarantined Items

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

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



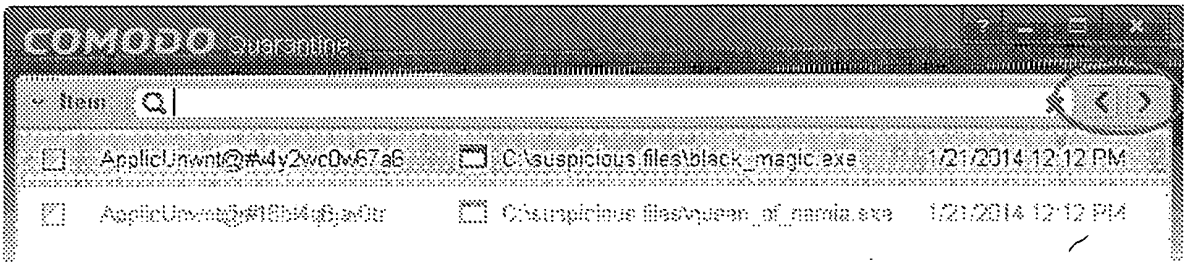
The 'Quarantine' interface displays a list of items moved to Quarantine from the results of real-time scanning, on-demand scanning and manually.

Column Descriptions

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

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

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



The Quarantined Items interface also allows you to:

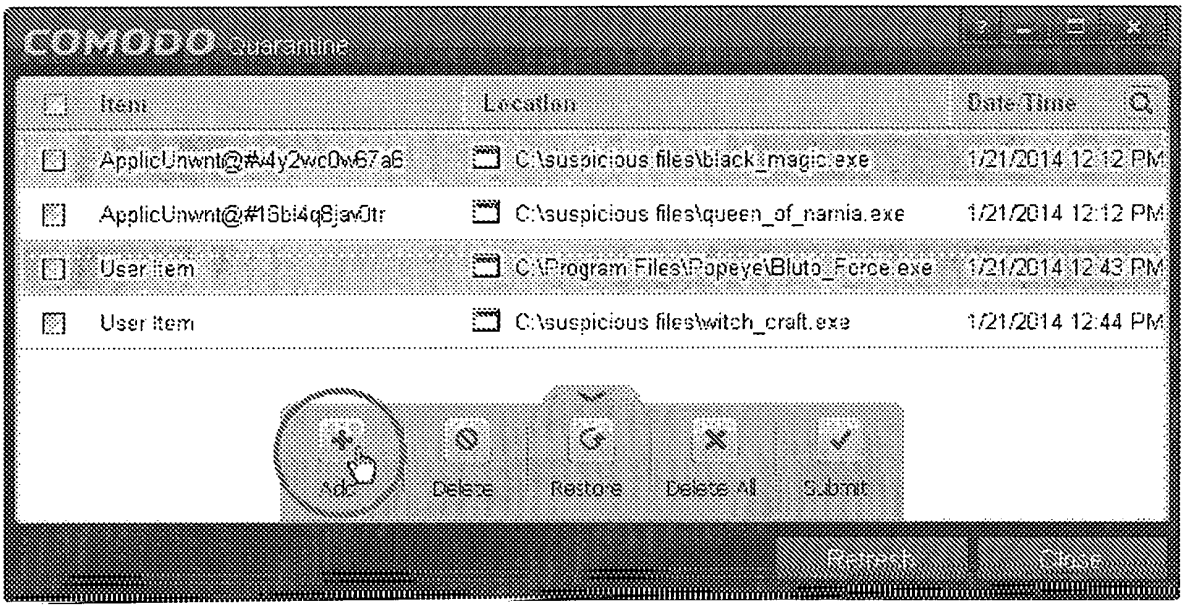
- Manually add applications, executables or other files, that you do not trust, as a Quarantined Item
- Delete a selected quarantined item from the system
- Restore a quarantined item to oits original location
- Delete all quarantined items
- Submit selected quarantined items to Comodo for analysis

Manually adding files as Quarantined Items

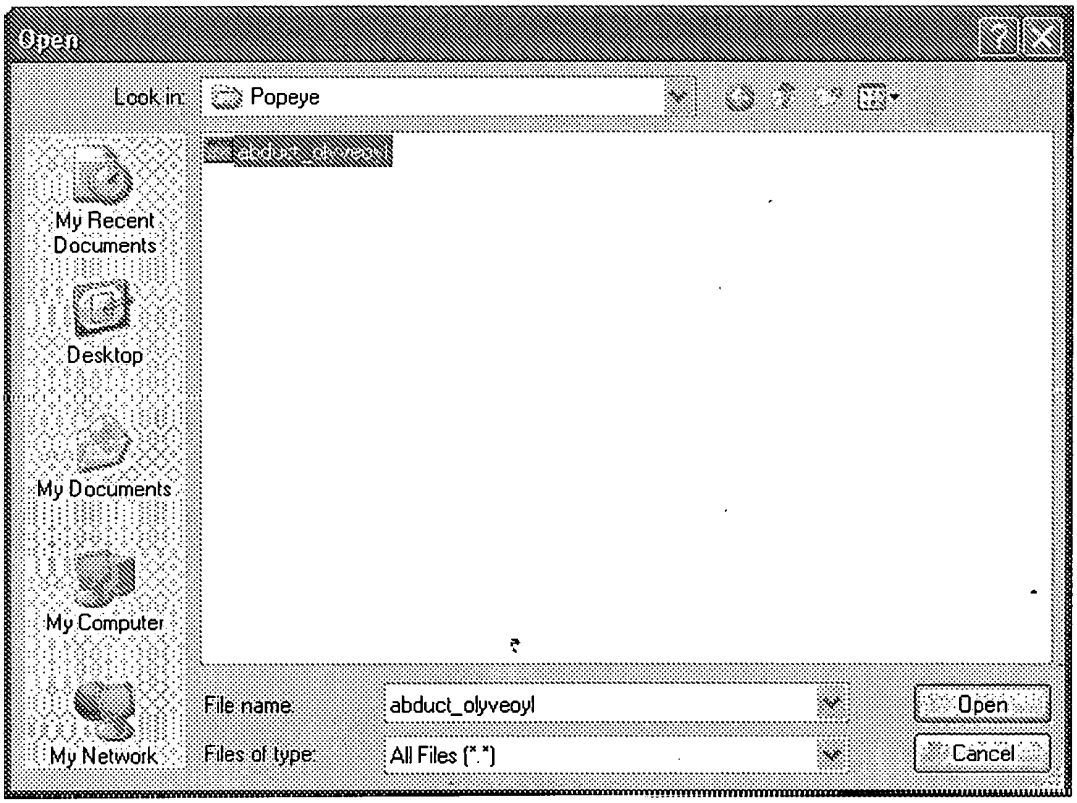
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined Item

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



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



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

To delete a quarantined item from the system

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

This deletes the file from the system permanently.

To restore a quarantined item to its original location

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



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

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

To remove all the quarantined items permanently

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

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

To submit selected quarantined items to Comodo for analysis

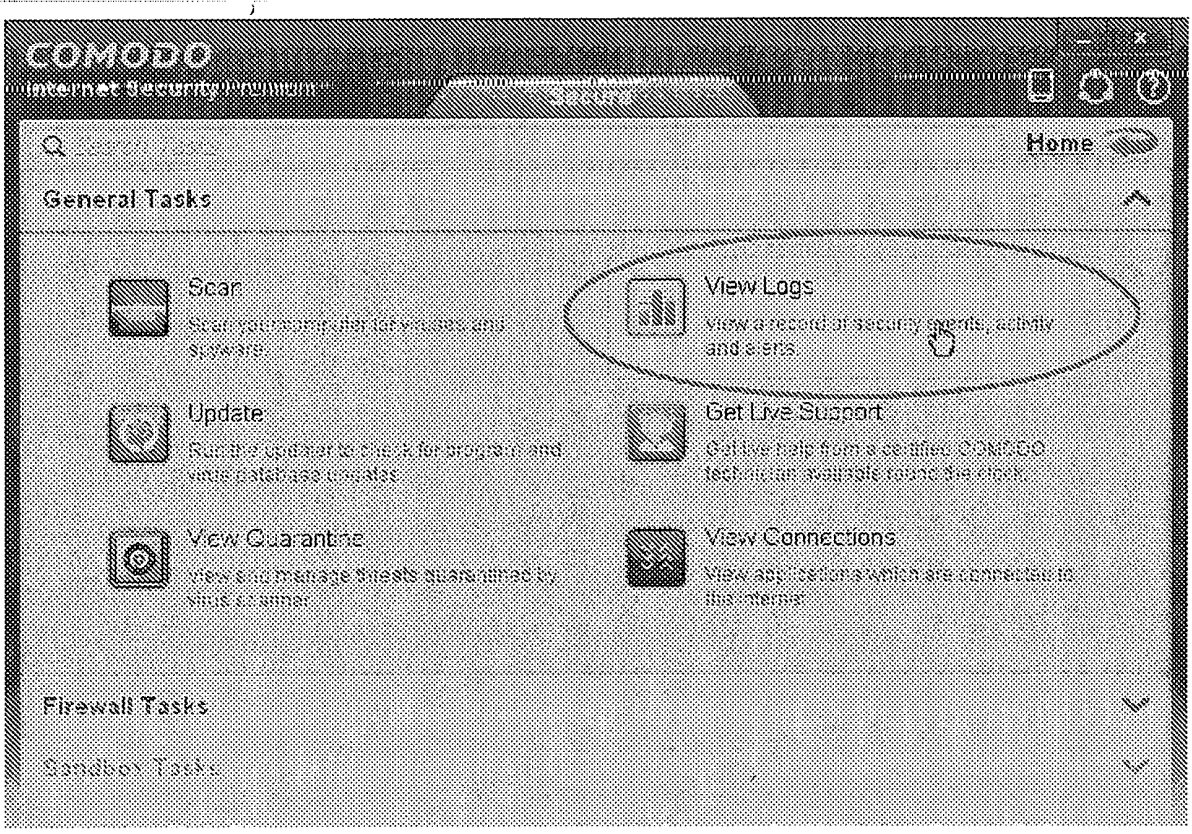
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

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

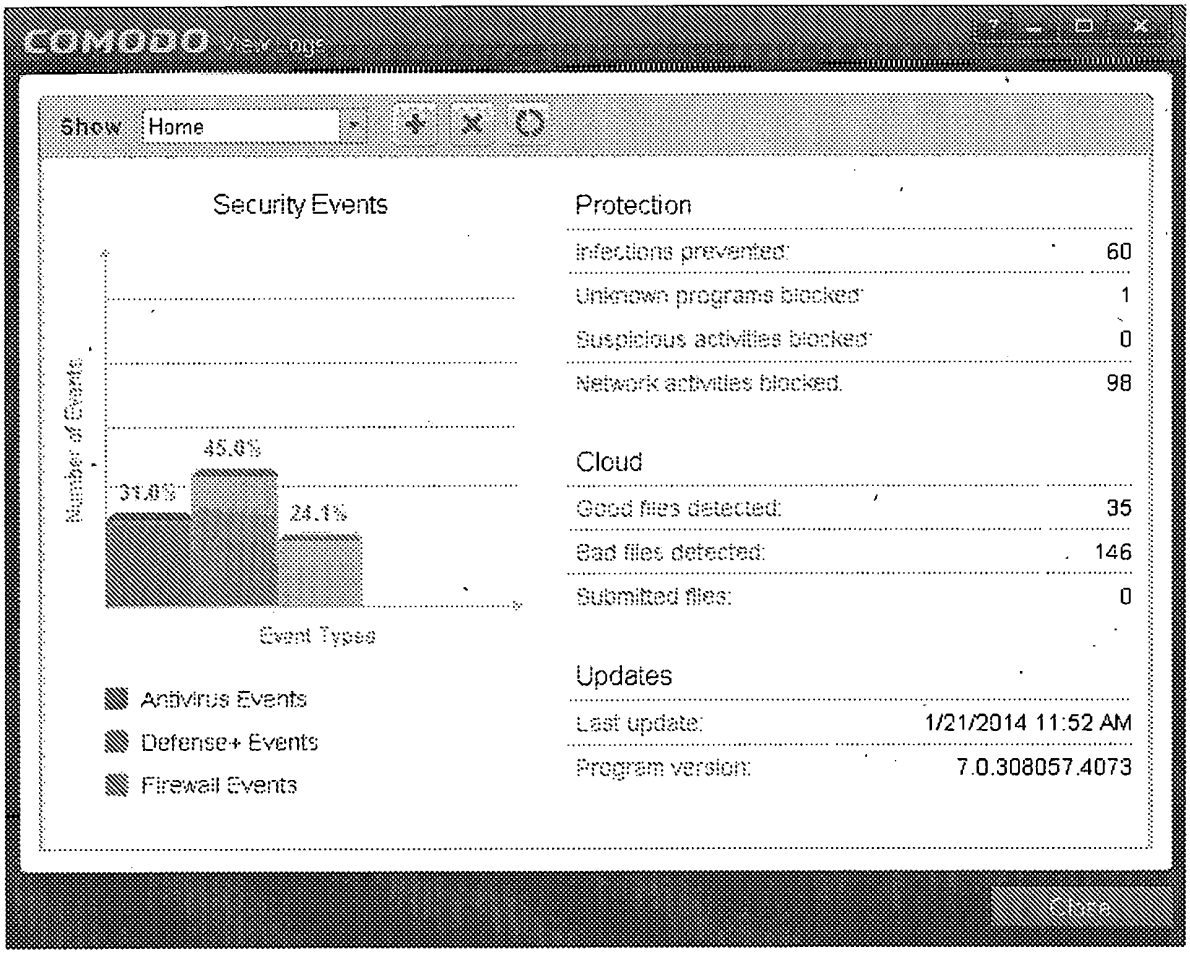
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

2.6. View CIS Logs

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



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



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

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

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

'Logs per Module':

- Antivirus
- Firewall
- Defense+
- Website Filtering

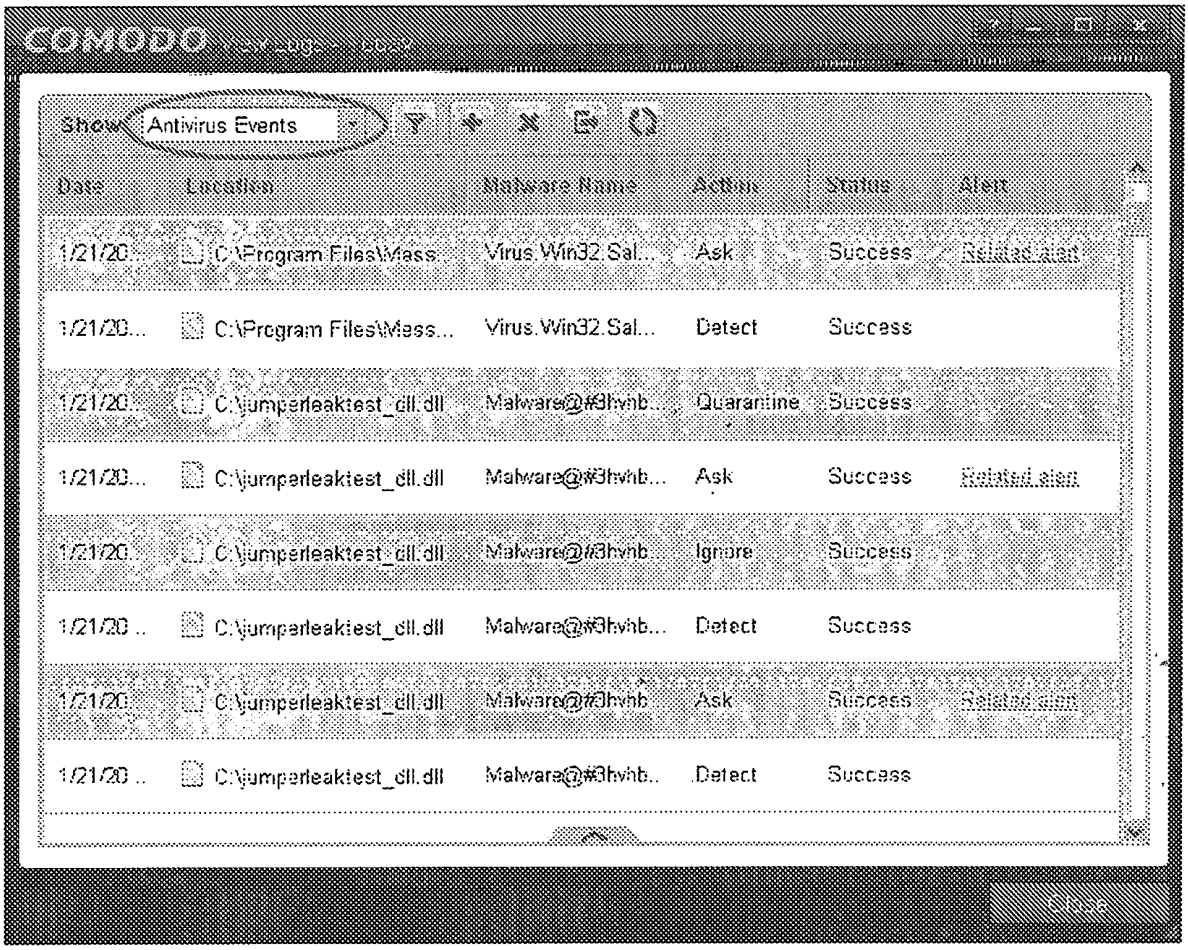
'Other Logs':

- Alerts Displayed
- Tasks Launched
- Configuration Changes

2.6.1. Antivirus Logs

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

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



Column Descriptions

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

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

2.6.1.1. Filtering Antivirus Logs

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