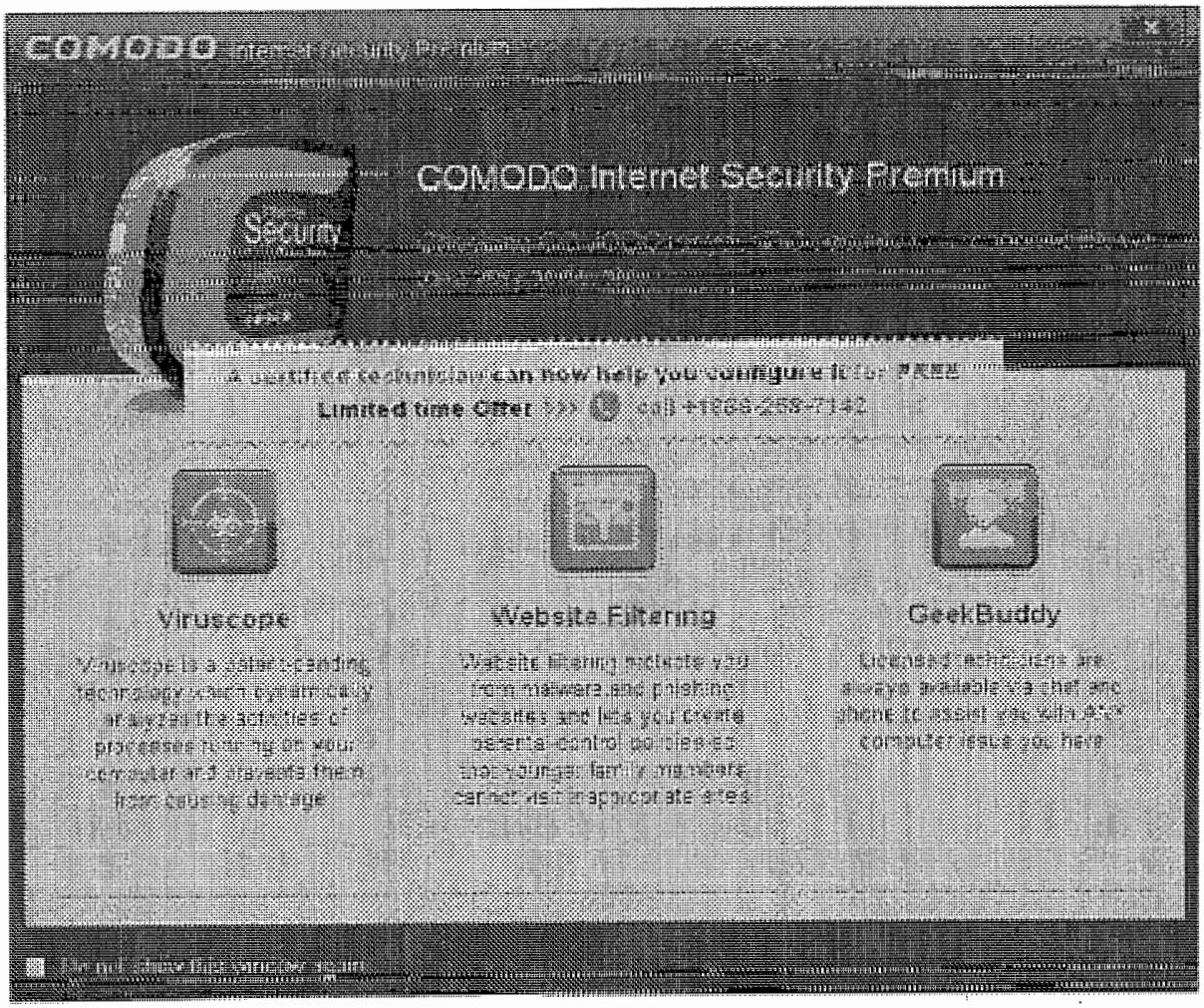
(*Default = Enabled*):



Tip: You can disable the Welcome Screen by selecting the checkbox 'Do not show this window again' in the window itself.

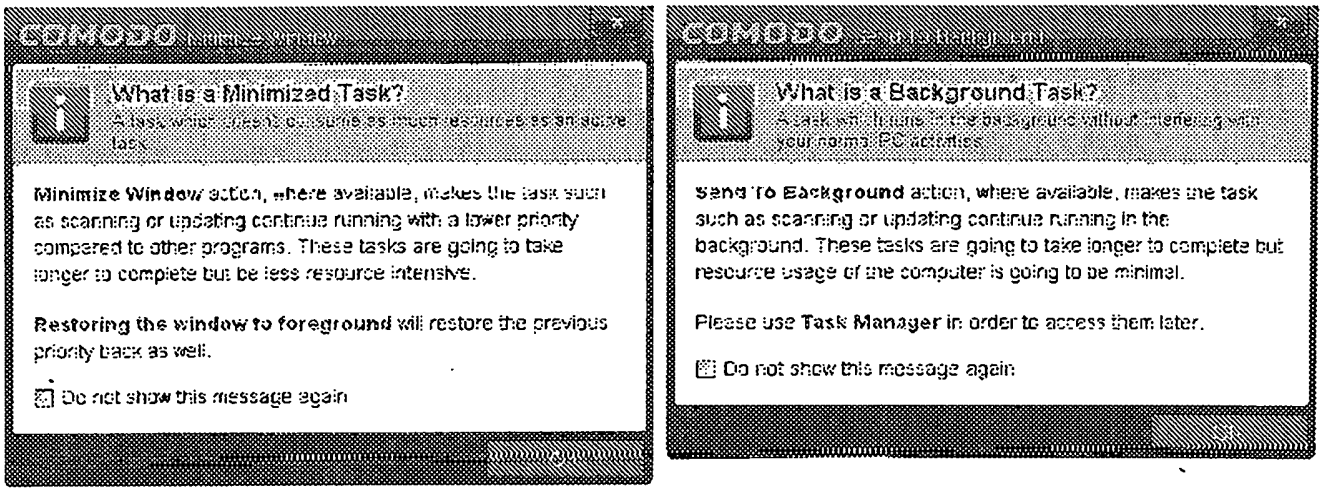
- **Show desktop widget** - The CIS desktop widget displays at-a-glance information about CIS security status, speed of outgoing and incoming traffic, number of background tasks and links to social networking sites.



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

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

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



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

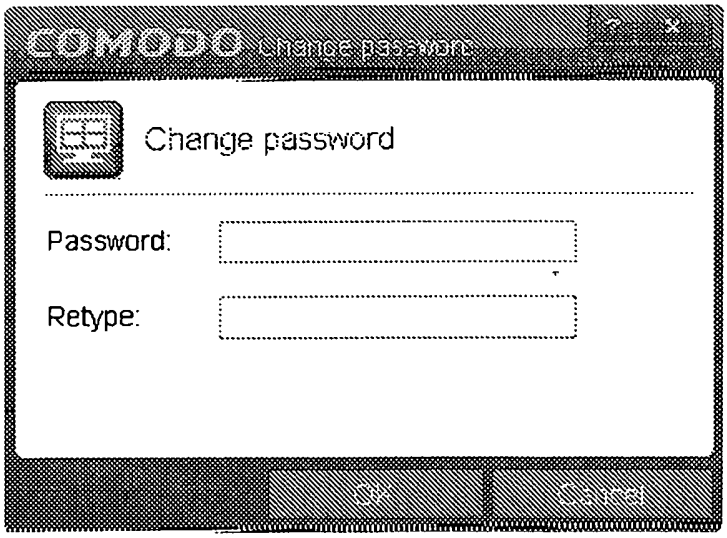
Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

- **Play sound when an alert is shown** - CIS generates a chime whenever it raises a security alert to grab your attention. If you do not want the sound to be generated, clear this check box (***Default = Enabled***).
- **Enable Password Protection** - Enforces password protection for all important configuration sections and wizards within the interface. If you enable this feature, you must first specify and confirm a password by clicking the 'Set Password' link. You will then be asked for this password whenever you try to access important configuration areas (for example, all sections in the General Tasks, Firewall Tasks, Sandbox Tasks and Advanced Tasks will request the password).

  This setting is of particular value to parents, network administrators and administrators of shared computers to prevent other users from modifying critical settings and exposing the machine to threats (***Default = Disabled***).

  To enable password protection

  - Select the 'Enable Password Protection' check-box then click 'Set Password'. The Change password dialog will appear.

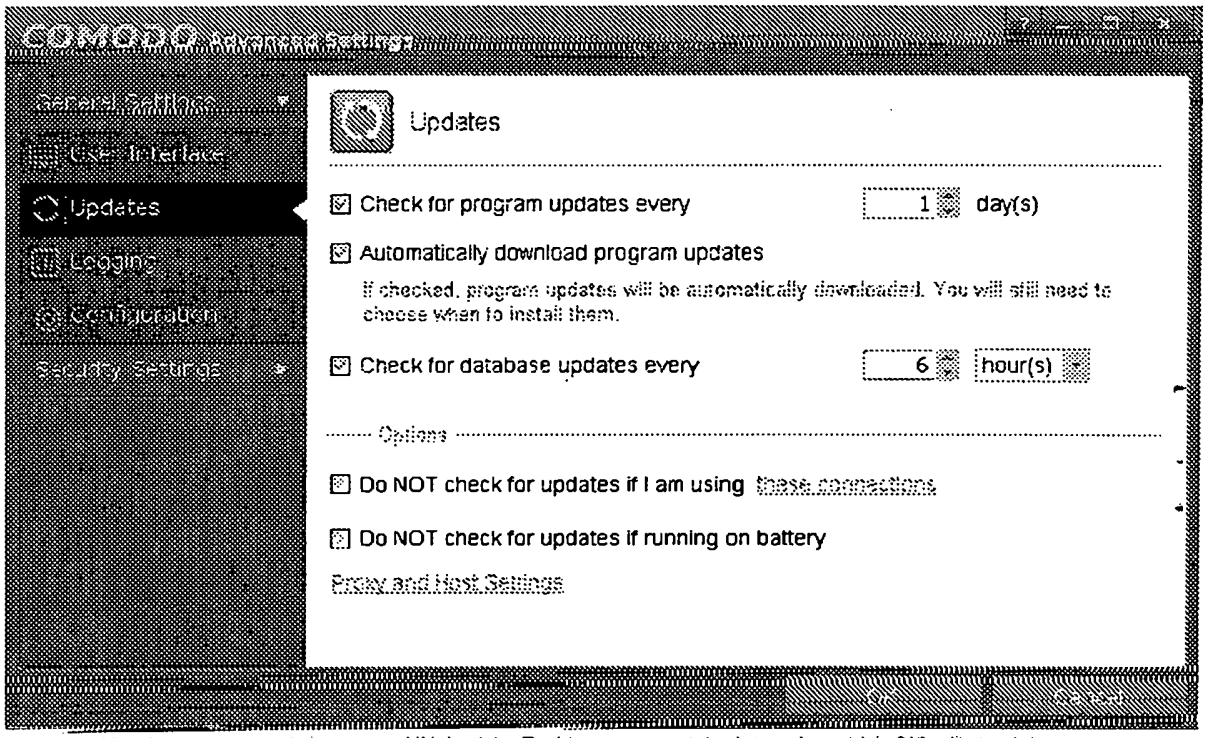


- Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

6.1.2. Configure Program and Virus Database Updates

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

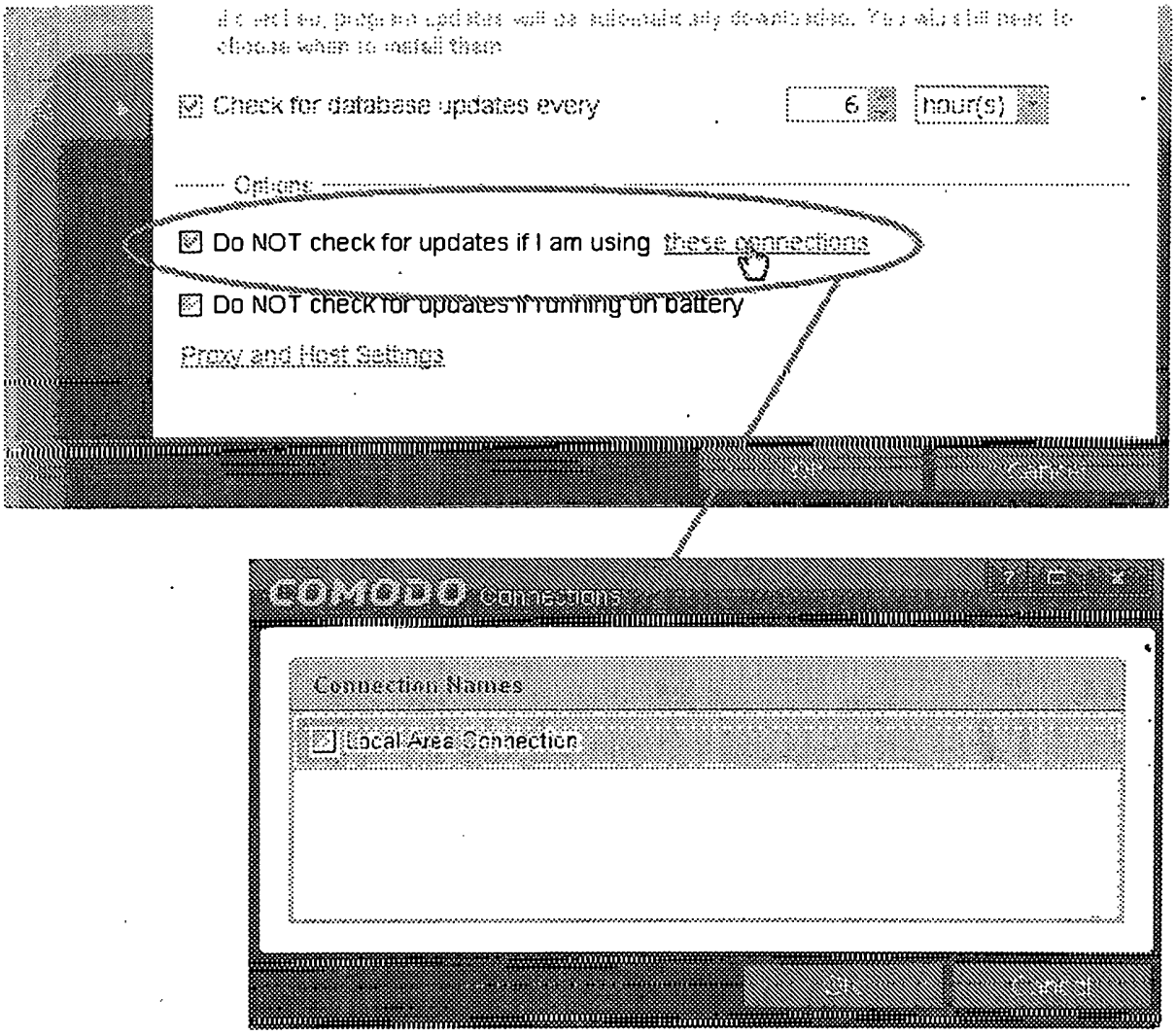
This screen can be accessed by clicking 'Updates' under the 'General Settings' section of 'Advanced Settings':



- **Check program updates every NN day(s)** - Enables you to set the interval at which CIS will check for program updates. Select the interval in days from the drop-down combo box. ***(Default = 1 day)***
- **Automatically download program updates** - Instructs CIS to automatically download program updates as soon as they are available. ***(Default=Enabled)***
- **Check for database updates every NN hour(s)/day(s)** - Enables you to set the interval at which CIS will check for virus signature database updates. Select the interval in hours or days from the first drop-down combo box and set hours or days in the second drop-down box. ***(Default and recommended = 6 hours)***
- **Do NOT check updates if am using these connections** - Enables you to restrict CIS from checking for updates if you use certain types of Internet connection. For example, you may not wish to check updates if using a wireless connection you know to be slow or not secure ***(Default = Disabled)***

  To do this:

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



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

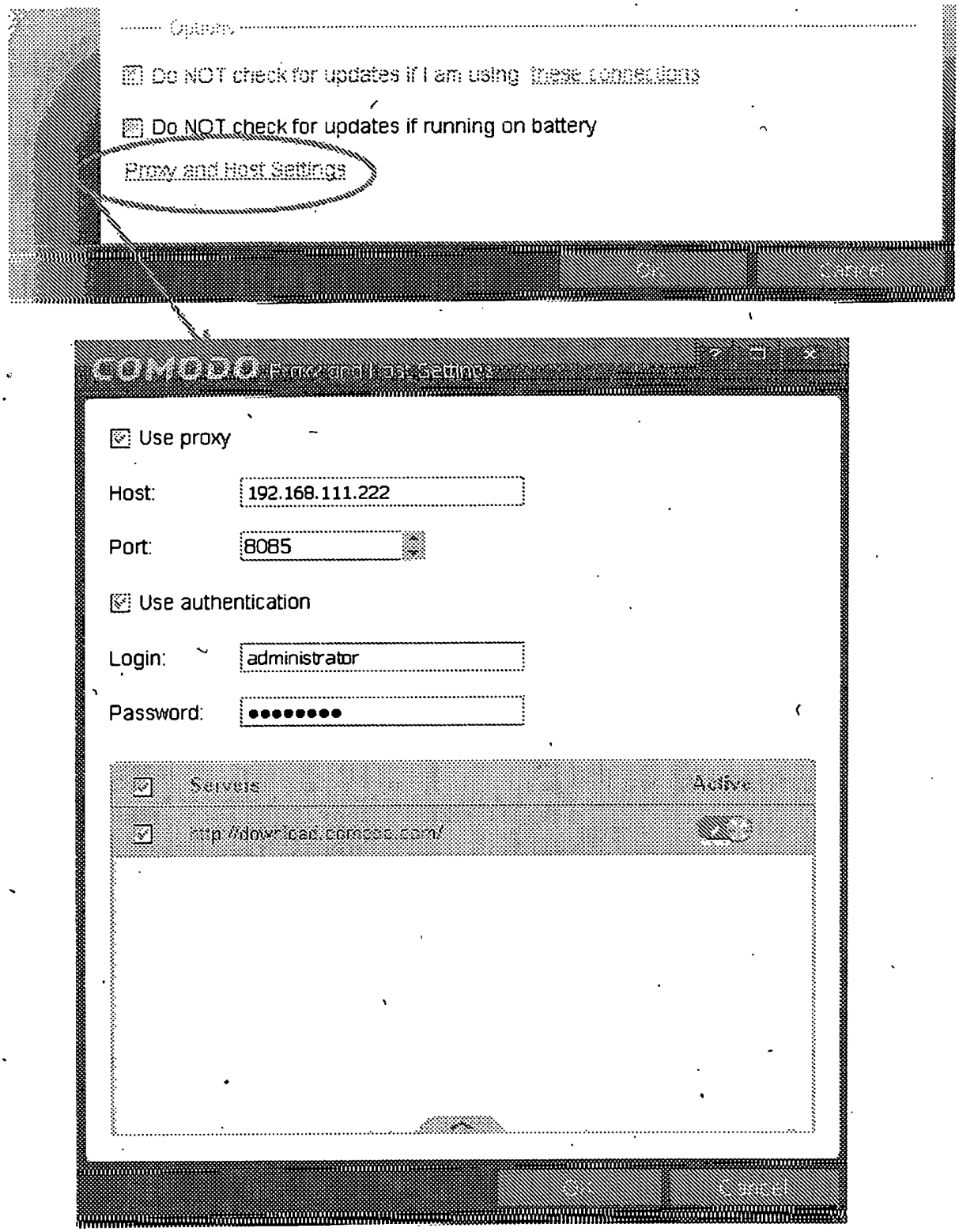
- **Do NOT check for updates if running on battery** - If enabled, CIS will not download updates if it detects your computer is running from battery power. This is intended to extend battery lifetime on laptops. ***(Default = Enabled)***

- **Proxy and Host Settings** - Allows you to select the host from which updates are downloaded. By default, CIS will directly download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CIS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CIS at this proxy/staging server. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

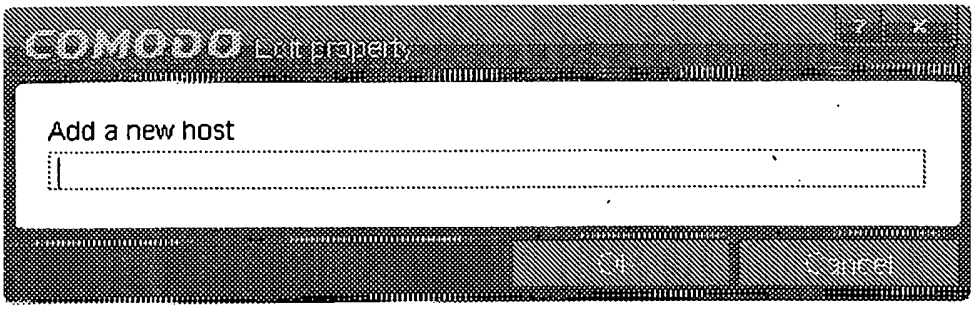
Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php

To configure updates via proxy server

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



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

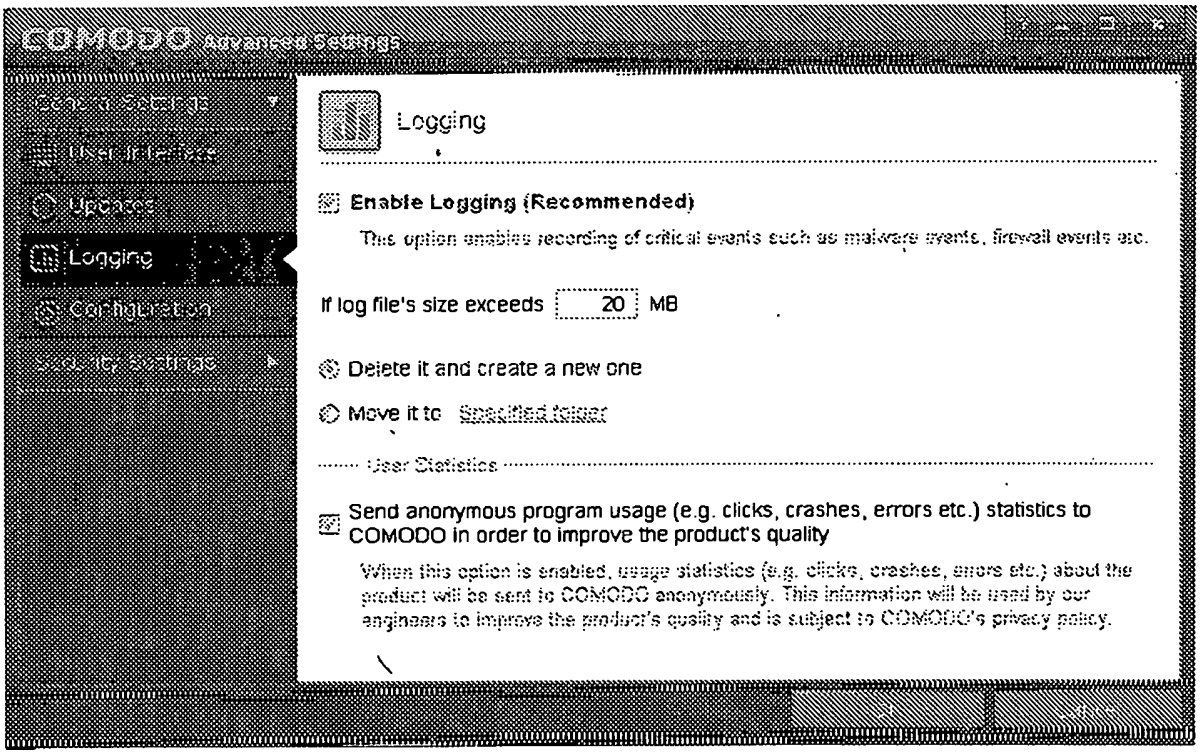


- If you specify multiple servers:
  - Activate or deactivate each update server using the 'Active' toggle switch alongside it
  - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CIS will commence downloading from the first server that contains new updates.
- Click 'OK' for your settings to take effect.

6.1.3. Log Settings

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

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

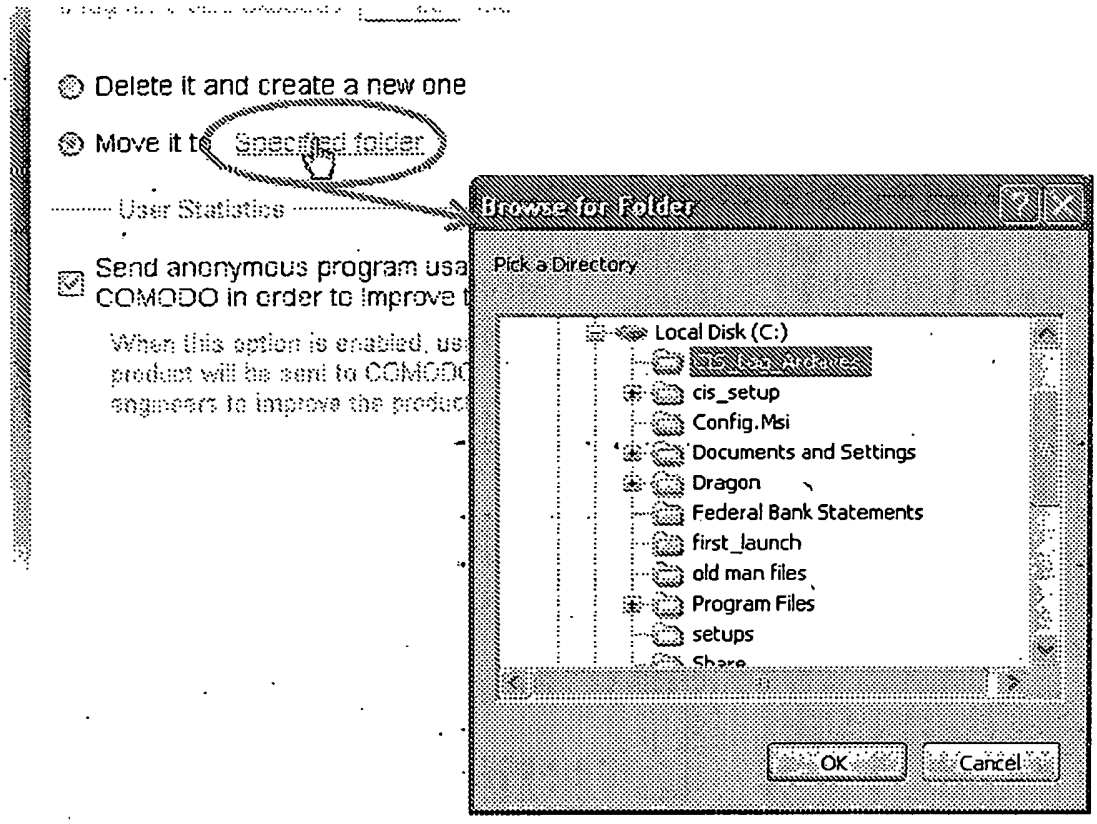


- **Enable Logging** - CIS logs events only if this setting is enabled. (*Default = Enabled*)
- **If the log file's size exceeds (Mb(s))** - Enables you to specify behavior when the log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.
  - Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds

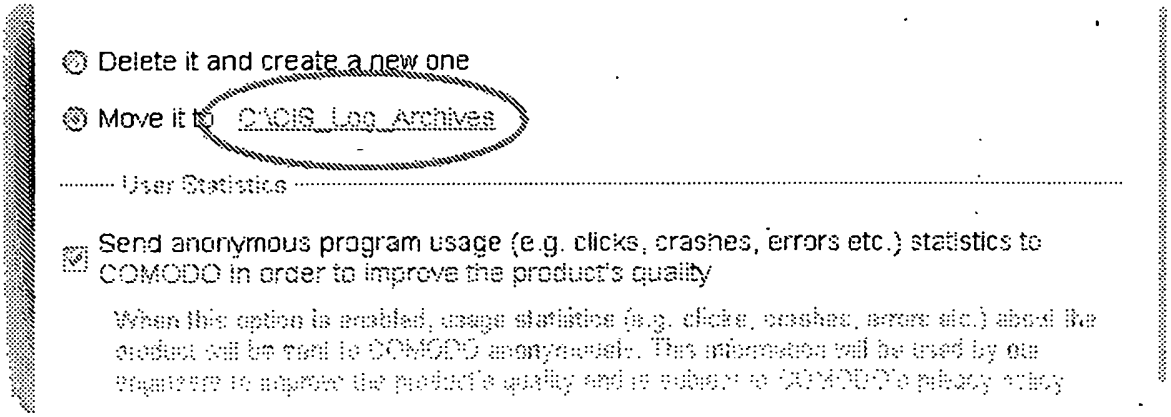
(MB)' ***(Default = 20MB).***

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

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



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



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

- **Send anonymous program usage (e.g. clicks, crashes, errors etc) statistics to COMODO in order to improve the product's quality** - Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS instillation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy

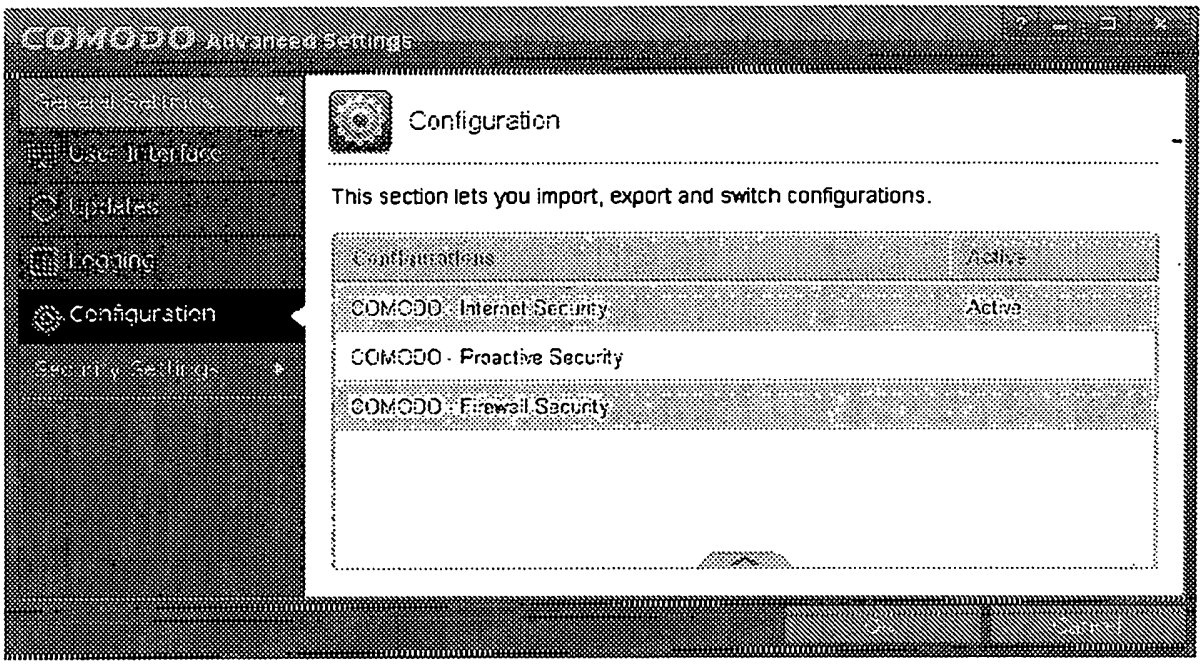
is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. ***(Default = Enabled).***

6.1.4. Manage CIS Configurations

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

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

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



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

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

6.1.4.1. Comodo Preset Configurations

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

Click the links below to find out more details on each configuration:

- COMODO - Internet Security
- COMODO - Proactive Security
- COMODO - Firewall Security

COMODO - Internet Security - This configuration is activated by default, when both Antivirus and Firewall components are installed (i.e. the complete installation). The firewall is always set to 'Safe mode' but, according to the results of the malware scan performed during the setup process, the HIPS setting may vary. If no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is 'Safe Mode'.

- Behavior Blocker is Enabled.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- Defense+ is tuned to prevent infection of the system.

If you wish to switch to Internet Security option, you can select the option from the 'Configuration' panel.

COMODO - Proactive Security - This configuration turns CIS into the ultimate protection machine. All possible protections are activated and all critical COM interfaces and files are protected. During the setup, if only Comodo Firewall installation option is selected, the next screen allows users to select this configuration as default CIS configuration. If selected, Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

If you wish to switch to Proactive Security option, you can select the option from the 'Configuration' panel.

COMODO - Firewall Security - This configuration is activated when the user chooses to install Firewall only and selects optimum protection settings for HIPS. Firewall is always set to Safe mode. But according to the malware scanning results performed during the setup process, if no malware is found, HIPS is set to Clean PC mode. Otherwise, the default is Safe mode.

- Behavior Blocker is disabled.
- Computer Monitor and Keyboard are NOT monitored.
- Only commonly infected files/folders are protected against infection.
- Only commonly exploited COM interfaces are protected.
- HIPS is tuned to prevent infection of the system and detect Internet access request leaks even if it is infected.

If you wish to switch to Firewall Security option, you can select the option from the 'Configuration' panel.

6.1.4.2. Importing/Exporting and Managing Personal Configurations

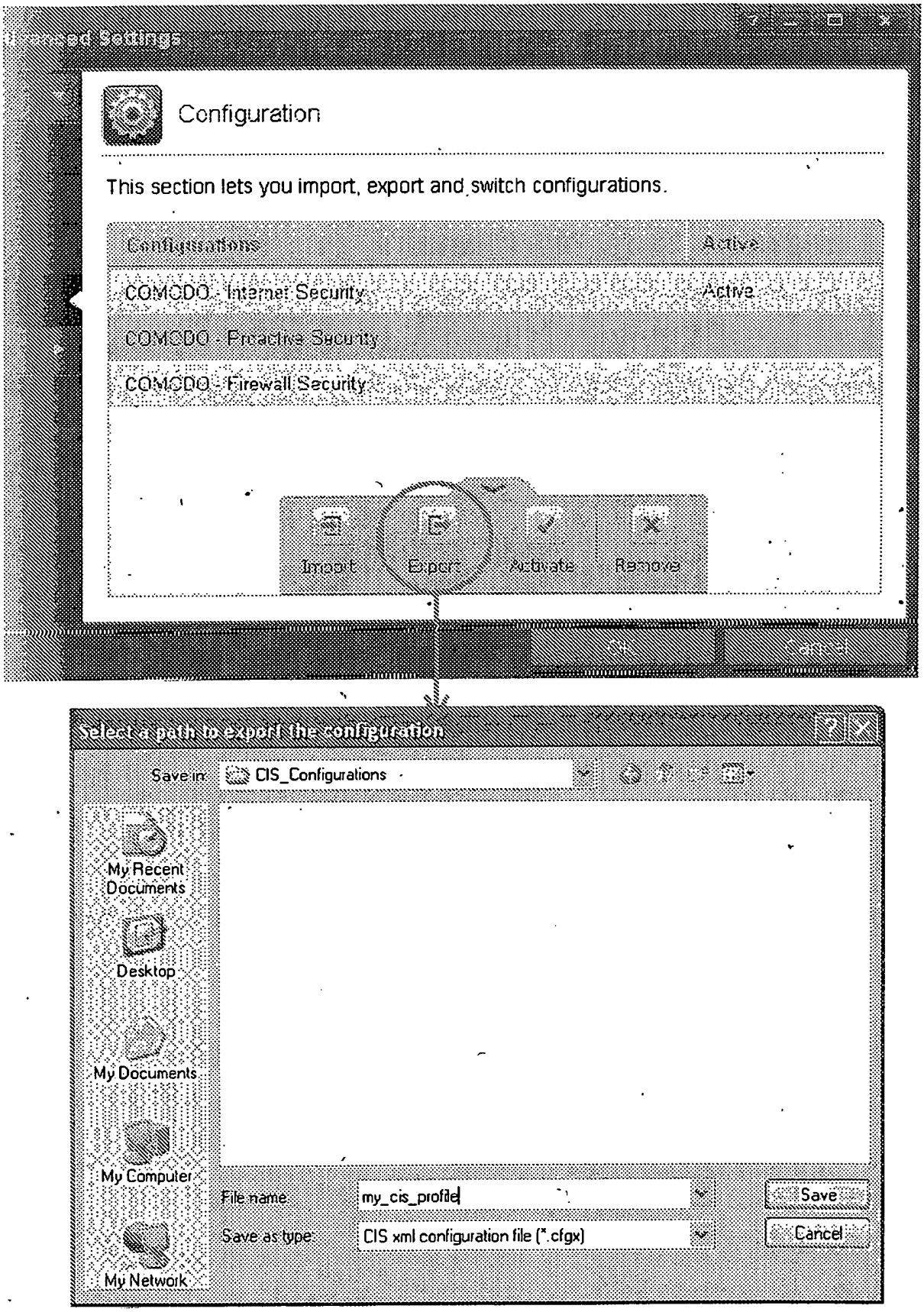
The CIS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Configuration' tab under 'General Settings' in 'Advanced Settings' interface.

Click the area on which you would like more information:

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

Exporting a stored configuration to a file

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface
2. Select the configuration, click the handle at the foot of the interface and choose 'Export'. The 'Select a path to export the configuration' dialog will open.



3. Navigate to the location where you want to save the configuration file, type a name (e.g., 'My CIS Profile') for the file to be saved in .cfgx format and click 'Save'.

A confirmation dialog will appear on successful export of the configuration.

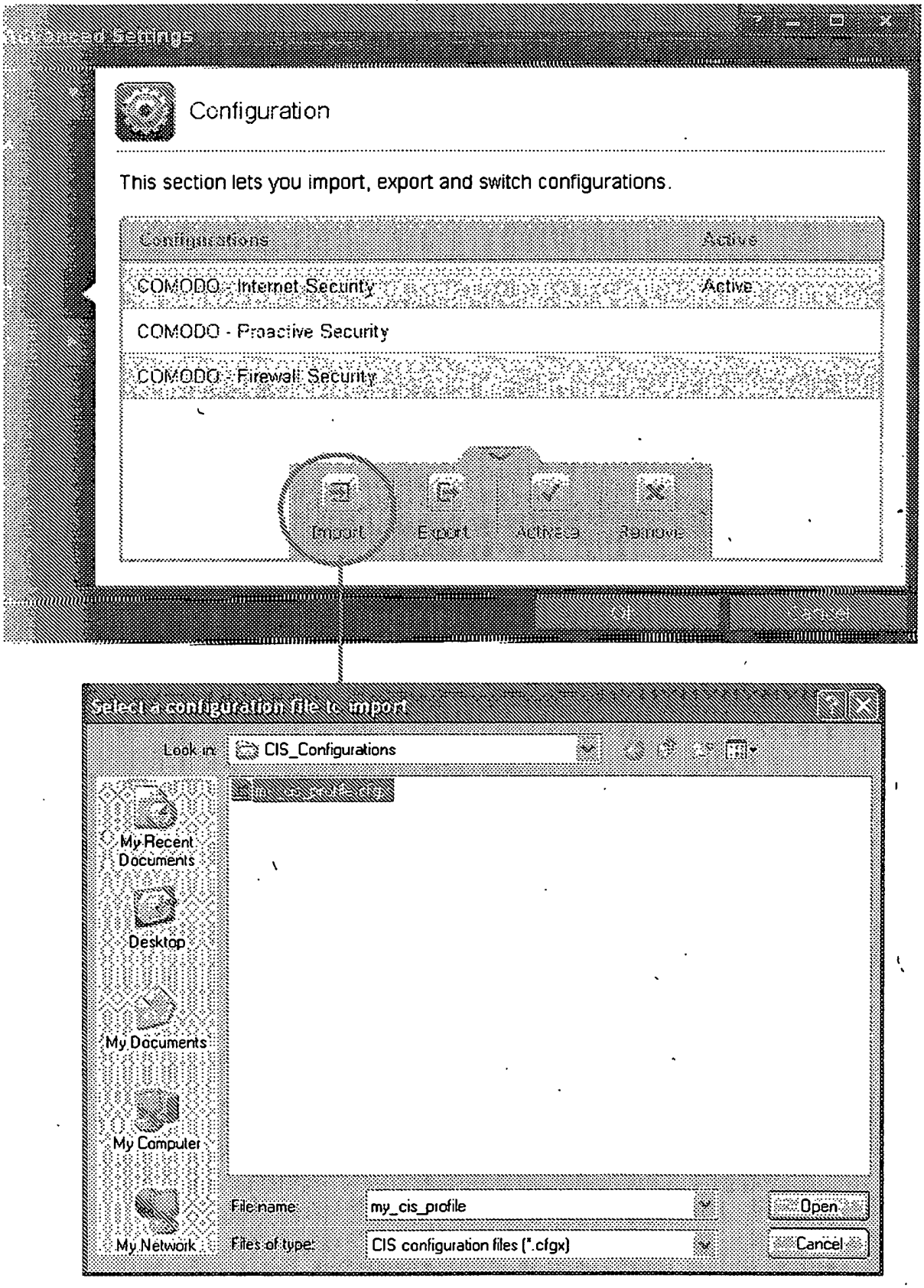


Importing a saved configuration from a file

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

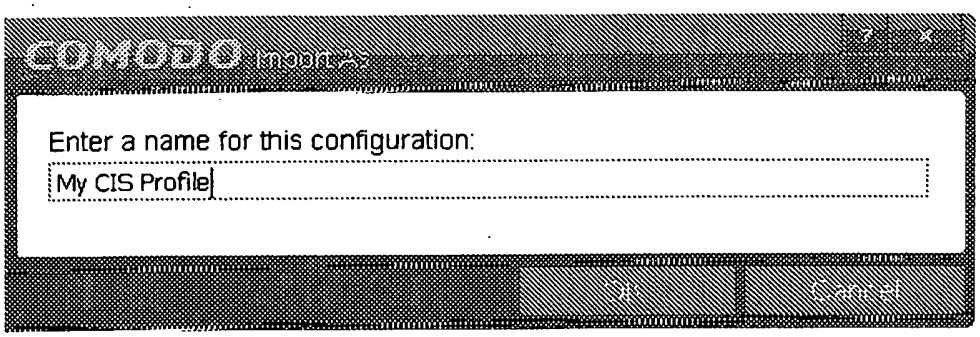
To import a profile

1. Open 'Configurations' panel by clicking 'Configuration' under General Settings in 'Advanced Tasks' interface, click the handle at the foot of the interface and choose Import from the options.



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

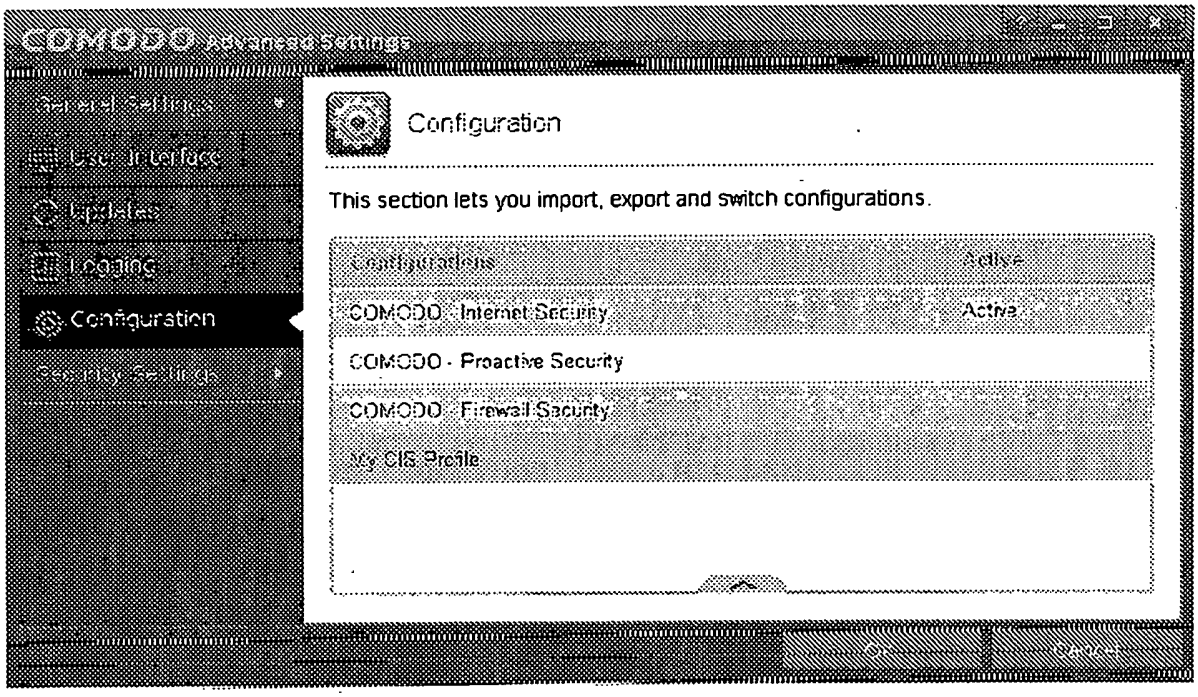
2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



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



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

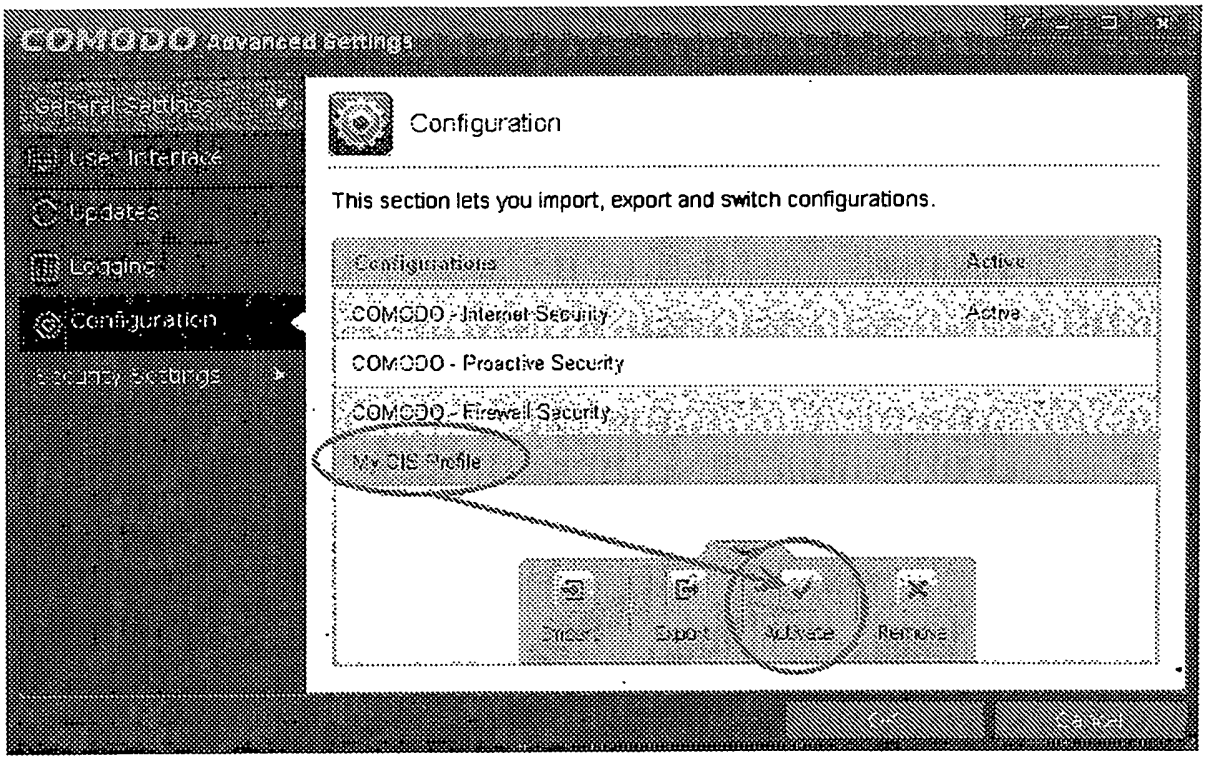


Selecting and implementing a different configuration profile

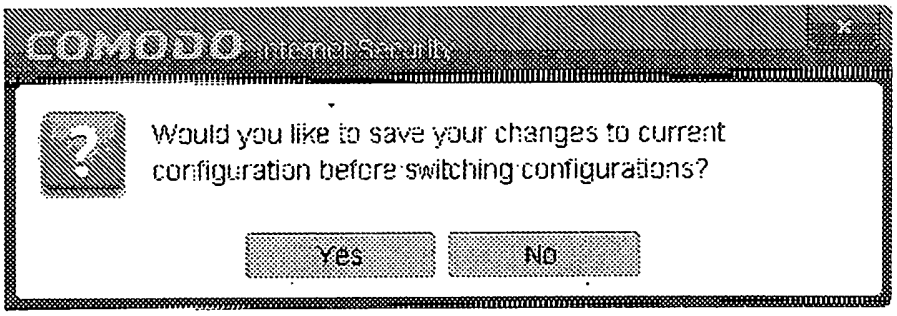
You can change the configuration profile active in CIS at any time from the 'Configurations' panel

To change the active configuration profile

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



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

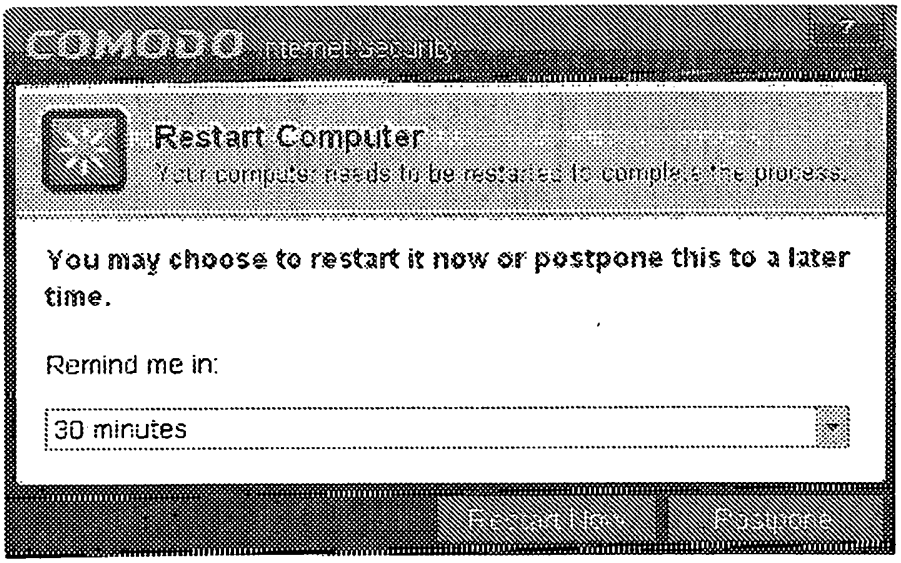


3. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

An activation confirmation dialog will be displayed. But the new profile will be implemented only on the next restart of the computer.



A 'Restart Computer' alert will appear at the bottom right of the screen.



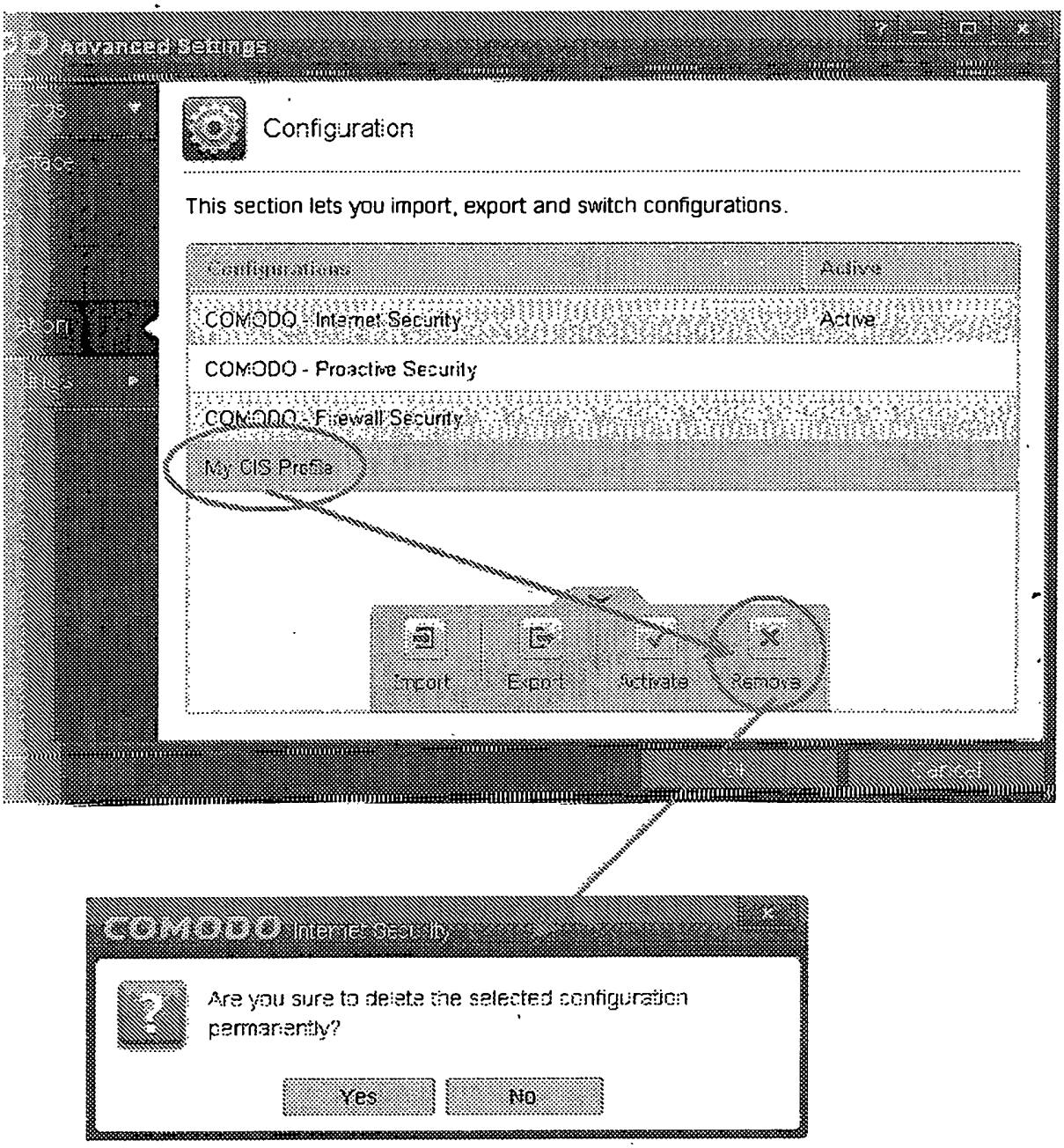
- If your want to restart the computer immediately, save all your work and click 'Restart Now'.
- If you want to restart the computer at a later time, select when you need to be reminded from the drop-down and click 'Postpone'.

Deleting an inactive configuration profile

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

To remove an unwanted profile

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

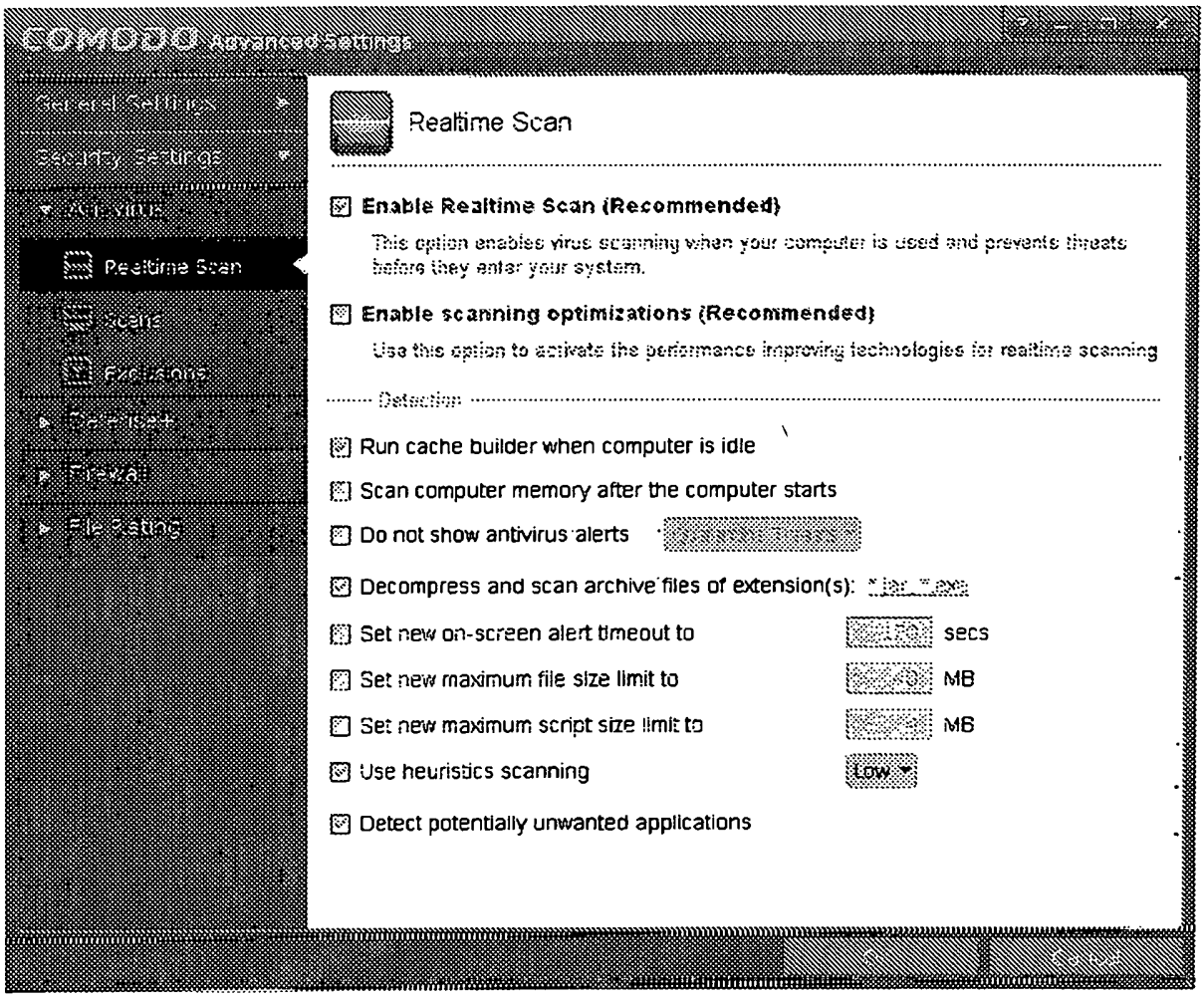


3. Click 'Yes'. The configuration profile will be deleted from your computer.



6.2. Security Settings

The Security Settings area enables you to perform granular configuration of the Antivirus, Firewall, Defense+ and File ratings components of Comodo Internet Security. Although these settings play a large part in governing the level of security offered by the application, Comodo Internet Security 6.2 does ship with secure defaults for all major settings so provides 'out-of-the-box' protection for all users.



Click the following links to go straight to the topic that explains the respective settings screen:

- Antivirus Settings
  - Real-time Scanner Settings
  - Custom Scan Settings
  - Exclusions
- Defense+ Settings
  - HIPS Behavior Settings
  - Active HIPS Rules
  - Predefined HIPS Rule Sets
  - Protected Objects
  - Behavior Blocker
  - Sandbox Settings
- Firewall Settings
  - Firewall Behavior Settings

- Application Rules
- Global Rules
- Predefined Rule Sets
- Network Zones
- Port Sets
- Website Filtering

- Manage File Rating
  - File Rating Settings
  - Trusted Files
  - Unrecognized Files
  - Submitted Files
  - Trusted Vendors List

6.2.1. Antivirus Settings

The Antivirus Settings category has sub-sections that allow you to configure Real Time Scans (a.k.a 'On-Access' scanning), Custom Scans, and Exclusions (a list of the files you consider safe).

Click the following links to jump to each section:

- Real Time Scan - To set the parameters for on-access scanning;
- Custom Scan - To create scan profiles and run custom scans, schedule custom scans and set the parameters for custom scans;
- Exclusions - To see the list of ignored threats and to set the parameters for Exclusions.

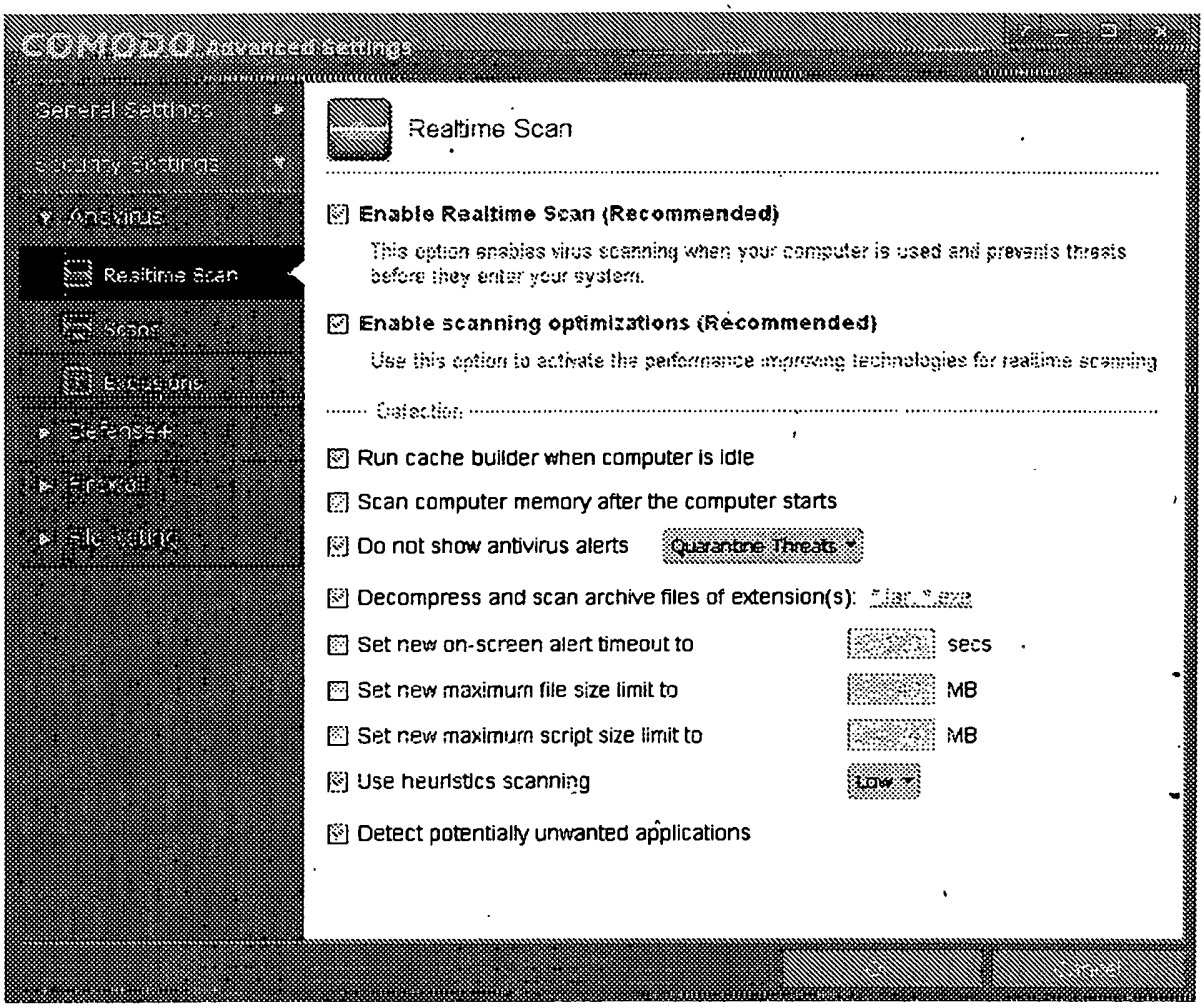
6.2.1.1. Real-time Scanner Settings

The real-time scanner (aka 'On-Access Scan') is always ON and checks files in real time when they are created, opened or copied (as soon as you interact with a file, Comodo Antivirus checks it). This instant detection of viruses assures you, the user, that your system is perpetually monitored for malware and enjoys the highest level of protection.

The real-time scanner also scans system memory on start. If you launch a program or file which creates destructive anomalies, then the scanner blocks it and alerts you immediately. Should you wish, however, you can specify that CIS does not show you alerts if viruses are found but automatically deals with them (choice of auto-quarantine or auto-block/delete). It is highly recommended that leave the Real Time Scanner enabled to ensure your system remains continually free of infection.

To open the Real Time Scan settings panel

- Click 'Tasks > Advanced Tasks > Open Advanced Settings > Security Settings > Antivirus > Realtime Scan':



- **Enable Realtime Scan** - Allows you to enable or disable real-time scanning. Comodo recommends to leave this option selected.(***Default=Enabled***)
- **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to reduce consumption of system resources and speed-up the scanning process ***(Default = Enabled)***

Note: The above two settings can be modified from the 'Advanced View' of the Home screen by clicking the status link beside Antivirus. If you choose Disabled option, both 'Enable Realtime Scan' and 'Enable scanning optimizations' will be disabled. If you choose 'Stateful', both the settings will be enabled and on choosing 'On Access', only 'Enable Realtime Scan' will be enabled.

Detection Settings

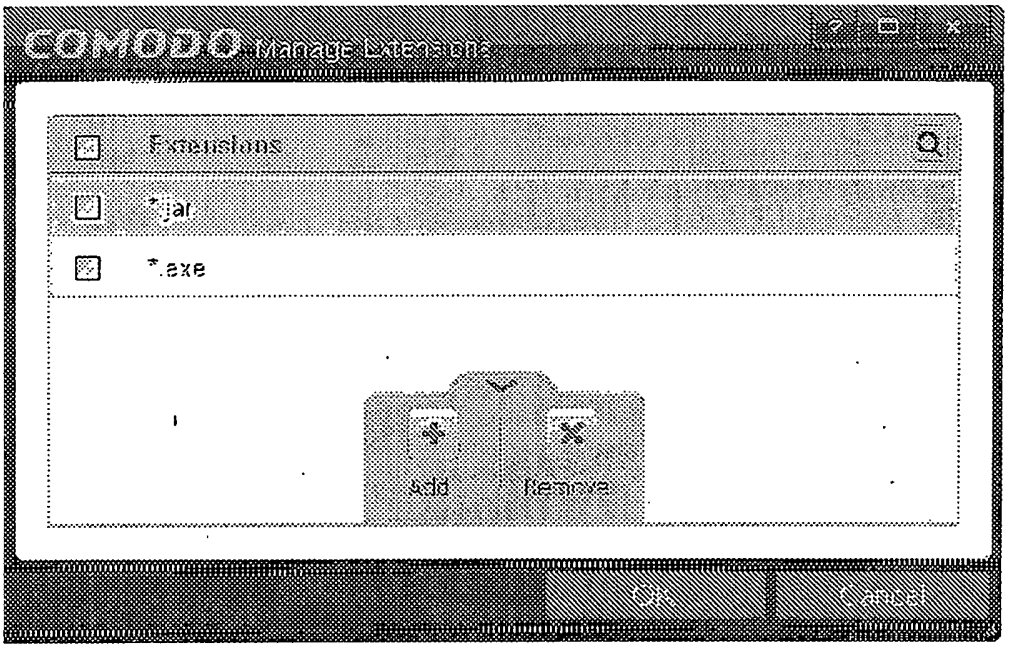
- **Run cache builder when computer is idle** - CIS runs the Antivirus Cache Builder whenever the computer is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (***Default = Enabled***).
- **Scan computer memory after the computer starts** - When this check box is selected, the Antivirus scans the system memory during system start-up ***(Default = Disabled)***
- **Do not show antivirus alerts** - Allows you to configure whether or not to show antivirus alerts when malware is encountered. Choosing 'Do not show antivirus alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then you have a choice of default responses that CIS should automatically take - either 'Block Threats' or 'Quarantine Threats'. (***Default = Enabled***)
  - **Quarantine Threats** - Moves the detected threat(s) to quarantine for your later assessment and action. (***Default***)
  - **Block Threats** - Stops the application or file from execution, if a threat is detected in it.

Note: If you deselect this option and thus enable alerts then your choice of quarantine/block is presented within the alert itself.

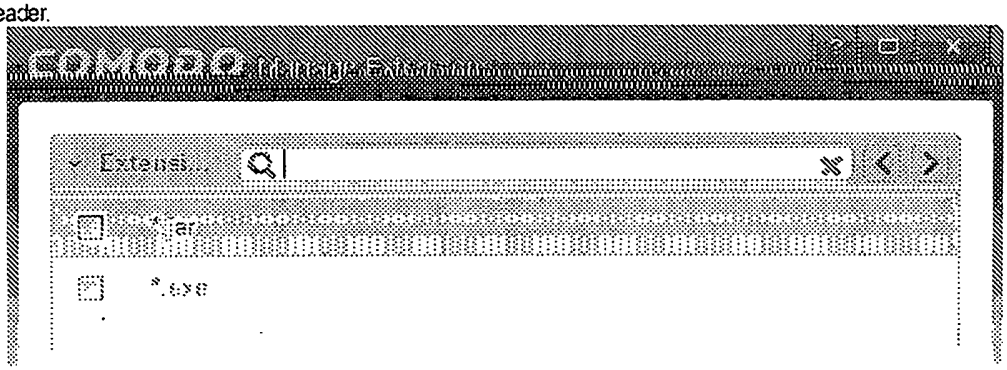
- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default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

  You can add the archive file types that should be decompressed and scanned by Comodo Antivirus.

  - Click link on the file type displayed at the right end. The 'Manage Extensions' dialog will open.



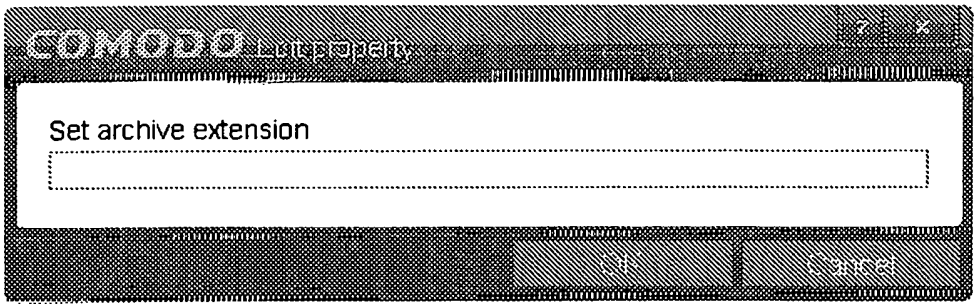
You can use the search option to find a specific file extension in the list by clicking the search icon at the far right in the column header.



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

Adding a New File Type

- To add a file type, click the up arrow at the bottom center and click 'Add'.



- Enter the extension (e.x.: rar, msi, zip, 7z, cab and so on) to be included in the Edit property dialog and click OK.
- Repeat the process to add more extensions
- Click OK in the 'Manage Extensions' dialog

- **Set new on-screen alert timeout to** - This box allows you to set the time period (in seconds) for which the alert message should stay on the screen. (***Default = 120 seconds***)
- **Set new maximum file size limit to** - This box allows you to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned. (***Default = 40 MB***)
- **Set new maximum script size limit to** - This box allows you to set a maximum size (in MB) for the script files to be scanned during on-access scanning. Files larger than the size specified here, are not scanned. (***Default = 4 MB***)
- **Use heuristics scanning** - Allows you to enable or disable Heuristics scanning and define scanning level. (***Default = Enabled***)

  Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  Leave this option selected to keep Heuristics scanning enabled. Else, deselect this checkbox. If enabled, you can select the level of Heuristic scanning from the drop-down:

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

6.2.1.2. Scan Profiles

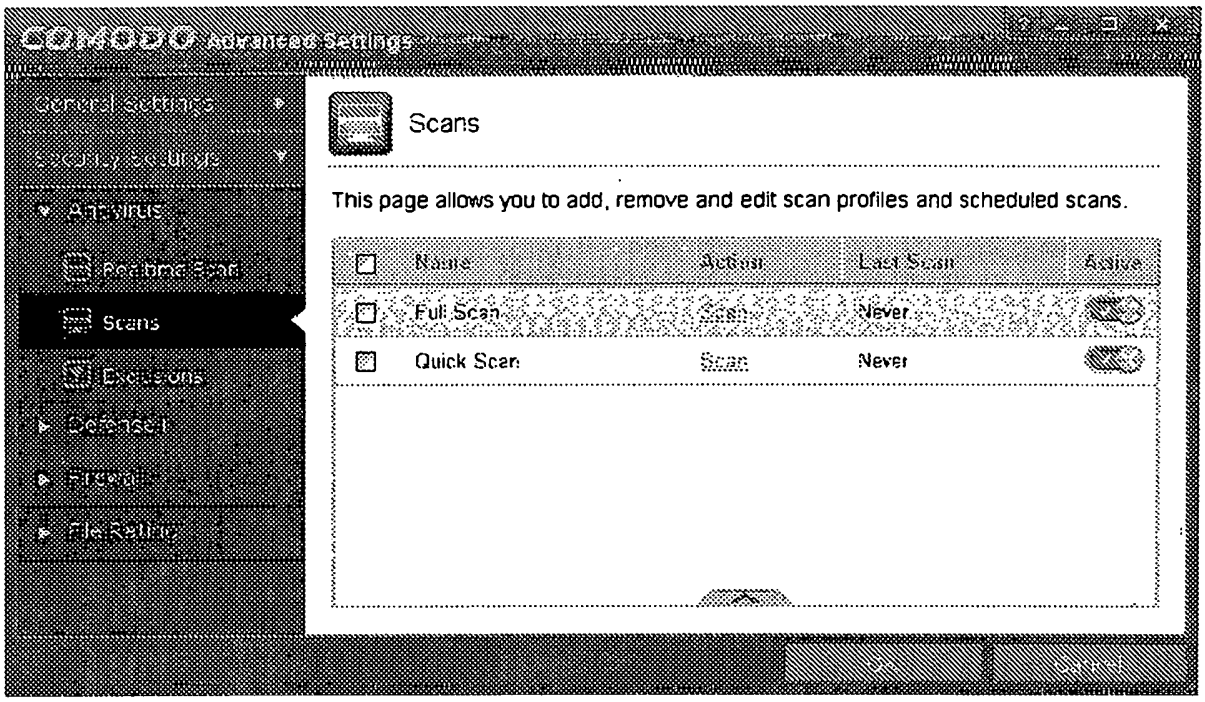
The Scan Profiles area allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CIS:

- Where to scan (which files, folders or drives should be covered by the scan)
- When to scan (you have the option to specify a schedule)

- How to scan (options that let you specify the behavior of the scan engine when running this profile)

To open the panel

- Click Security Settings > Antivirus > 'Scans' tab in the 'Advanced Settings' panel.



CIS ships with two predefined scan profiles:

- **Full Scan** - Covers every local drive, folder and file on your system.
- **Quick Scan** - Covers critical areas in your system which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of your computer and keeping them clean is essential.

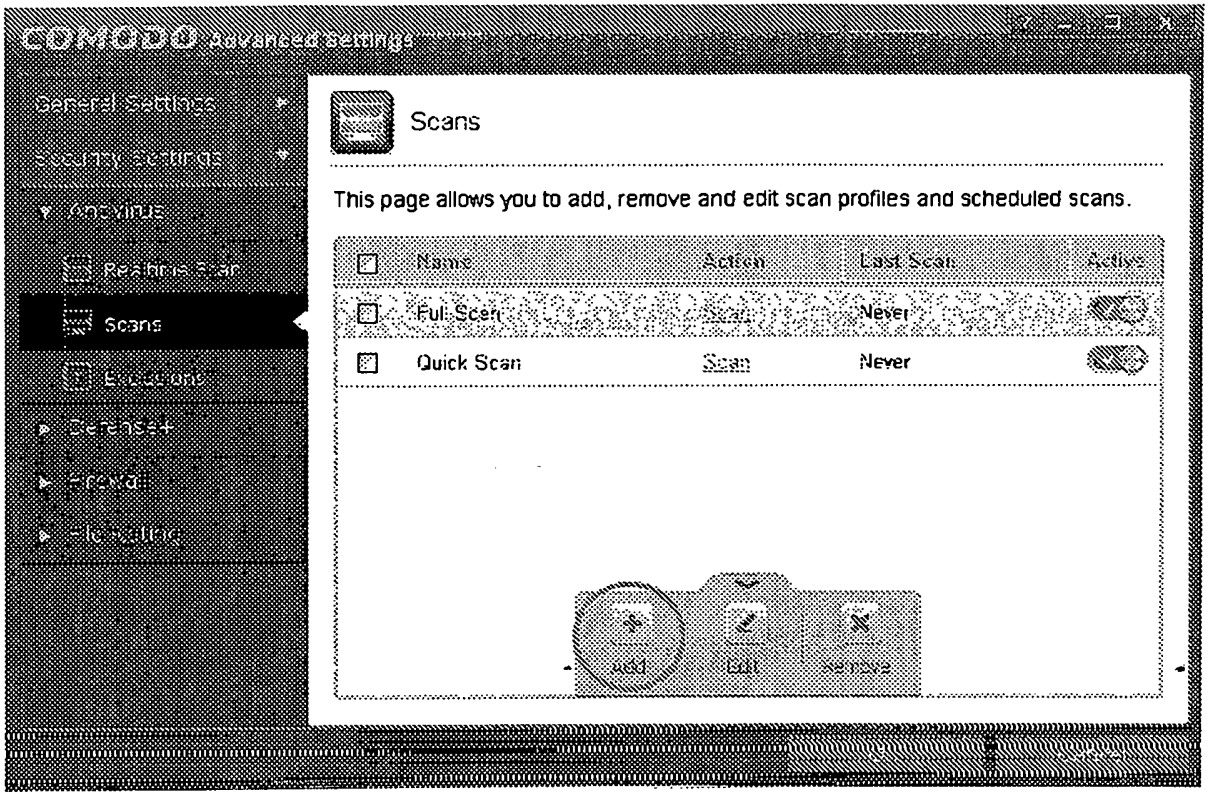
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

- Creating a Scan Profile
- Running a custom scan

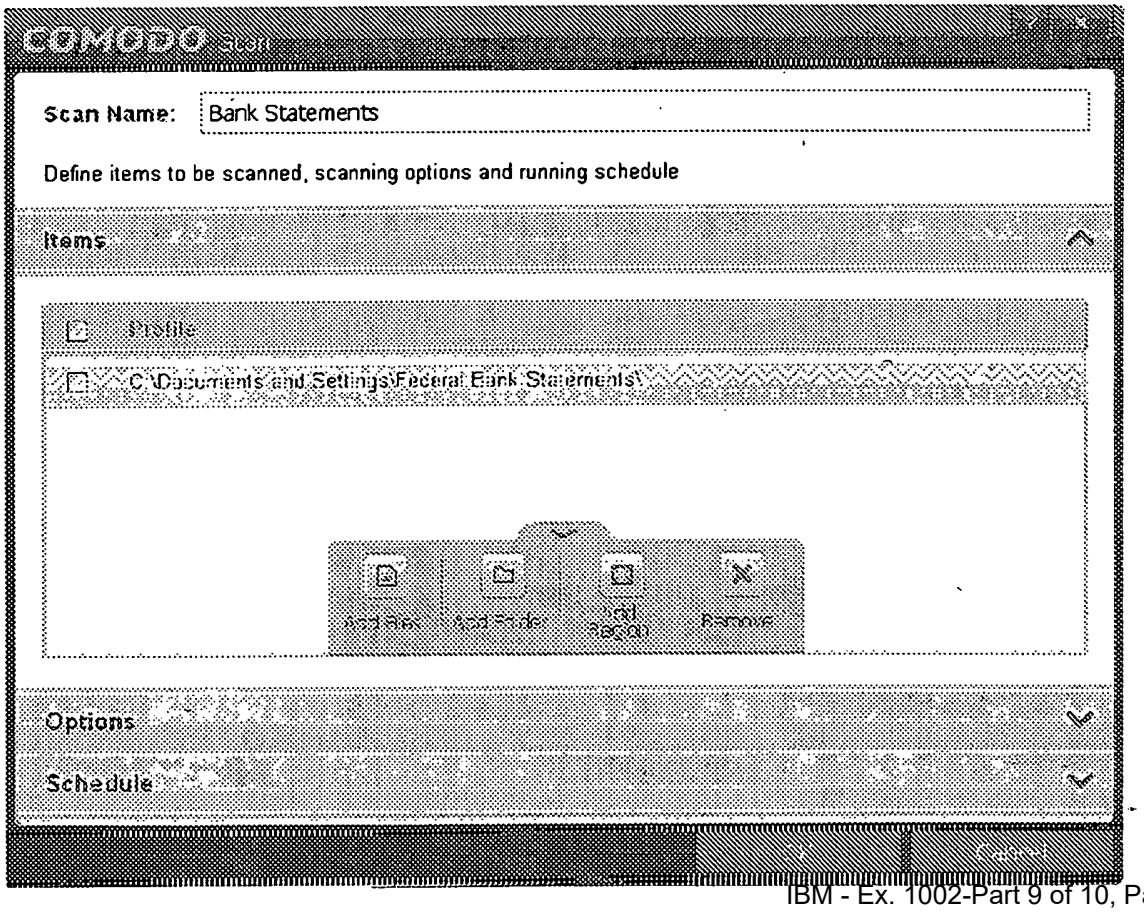
To create a custom profile

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

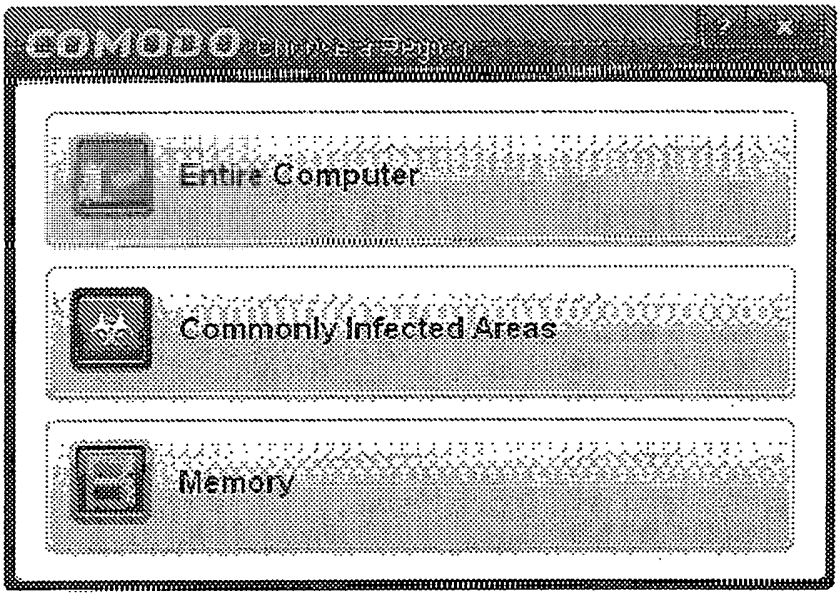


The scan profile interface will be displayed.

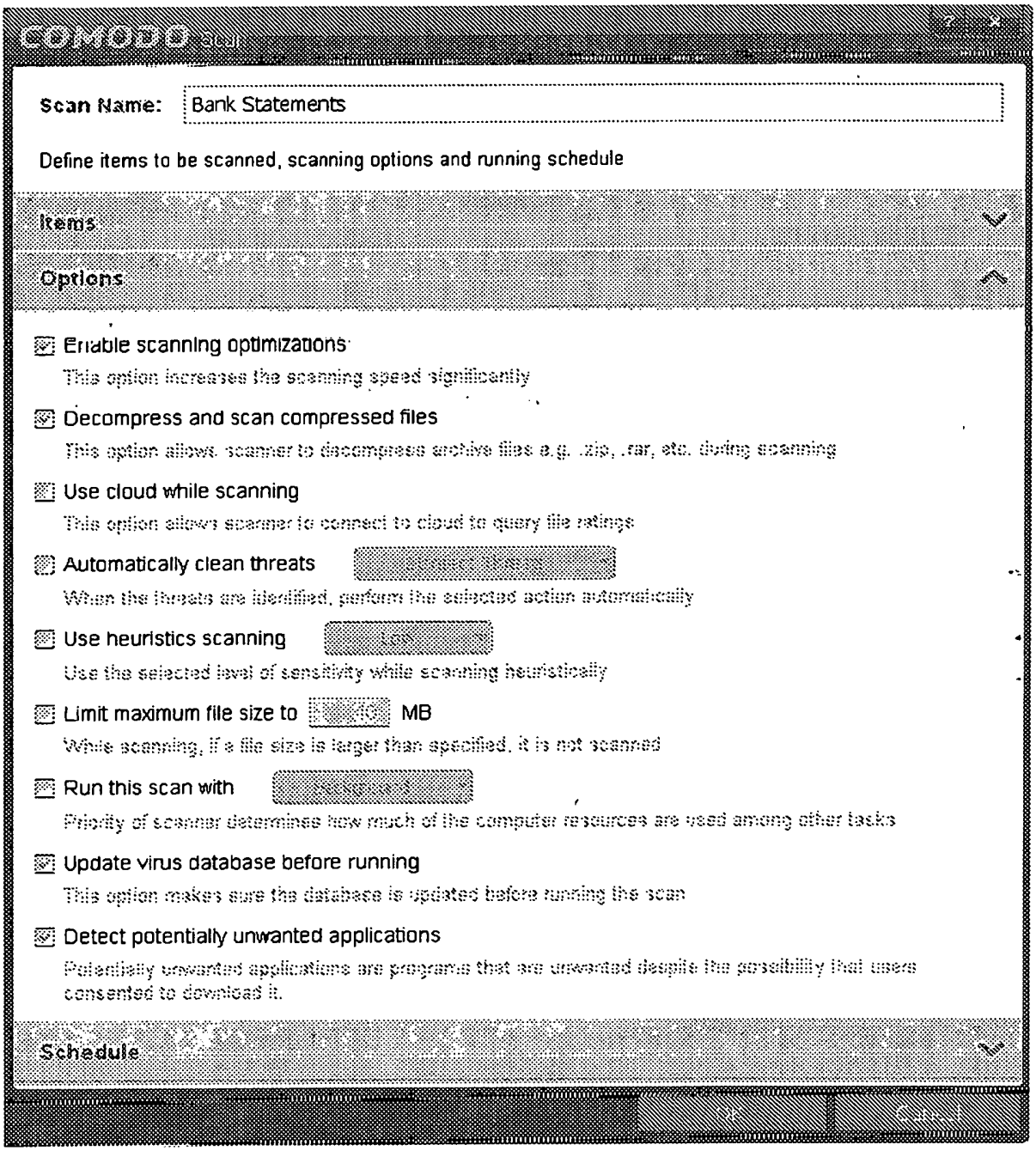
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items that should be included in the profile



- **Add Files** - Allows you to navigate to specific files that you wish to add to the profile
- **Add Folder** - Opens the 'Browse For Folder' window and allows you to select entire folders
- **Add Region** - Allows you to add predefined regions to the profile. For example, 'Full Computer', 'Commonly Infected Areas' and 'System Memory'.



- Repeat the process to add more items into the profile
- Click 'Options' to further customize the scan



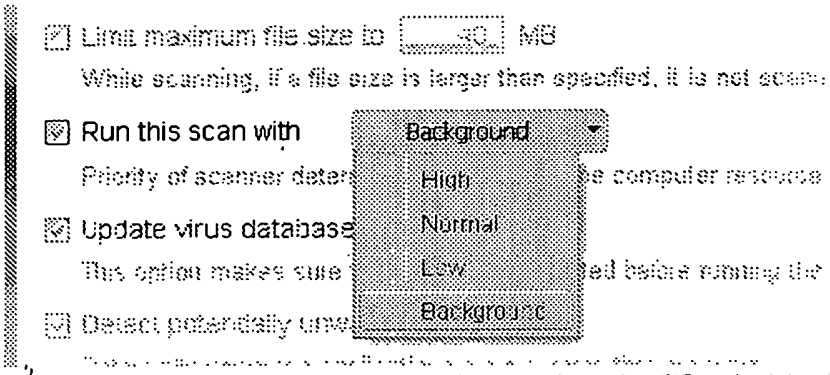
- **Options**:
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)***.
  - **Decompress and scan compressed files** - When this check box is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives ***(Default = Enabled)***.
  - **Use cloud while scanning** - Selecting this option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled your system is capable of detecting zero-day malware even if your local antivirus database is out-dated. ***(Default = Disabled)***.
  - **Automatically clean threats** - Enables you to select the action to be taken against the detected threats and infected files automatically from disinfecting Threats and moving the threats to quarantine. ***(Default = Disabled)***.

- **Use heuristics scanning** - Enables you to select whether or not Heuristic techniques should be applied on scans in this profile. You are also given the opportunity to define the heuristics scan level. ***(Default = Disabled).***

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

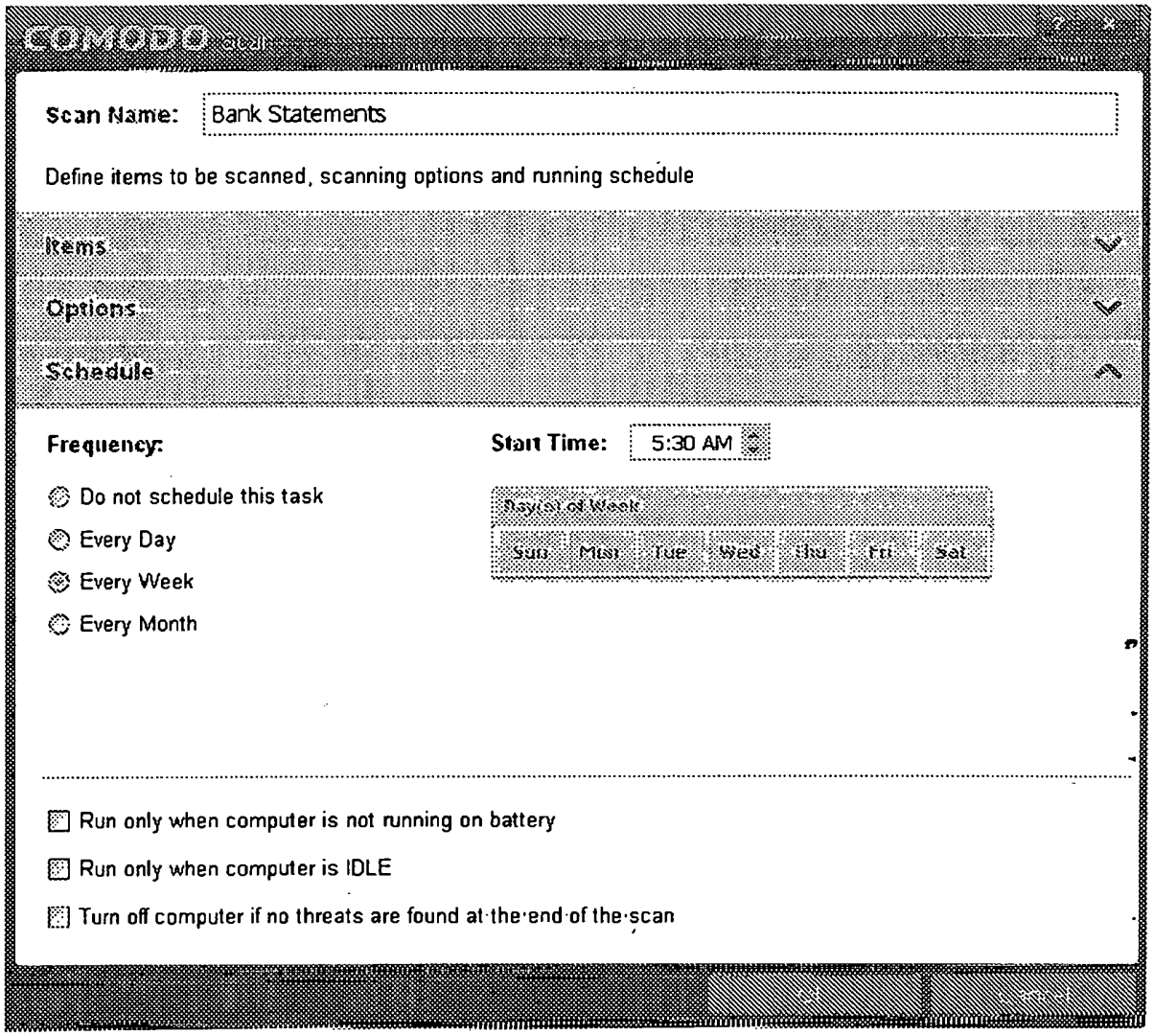
  This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  - **Low** - Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.
- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run Scan with** - Enables you to set the priority of the scanning from High to Low or to run at background. ***(Default = Disabled)***.



- **Update virus database before running** - Selecting this option makes CIS to check for virus database updates and if available, update the database before commencing the scan. ***(Default = Enabled)***.
- **Detect potentially unwanted applications** - When this check box is selected, 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 be performed periodically, set a Schedule for the custom scan by clicking 'Schedule'

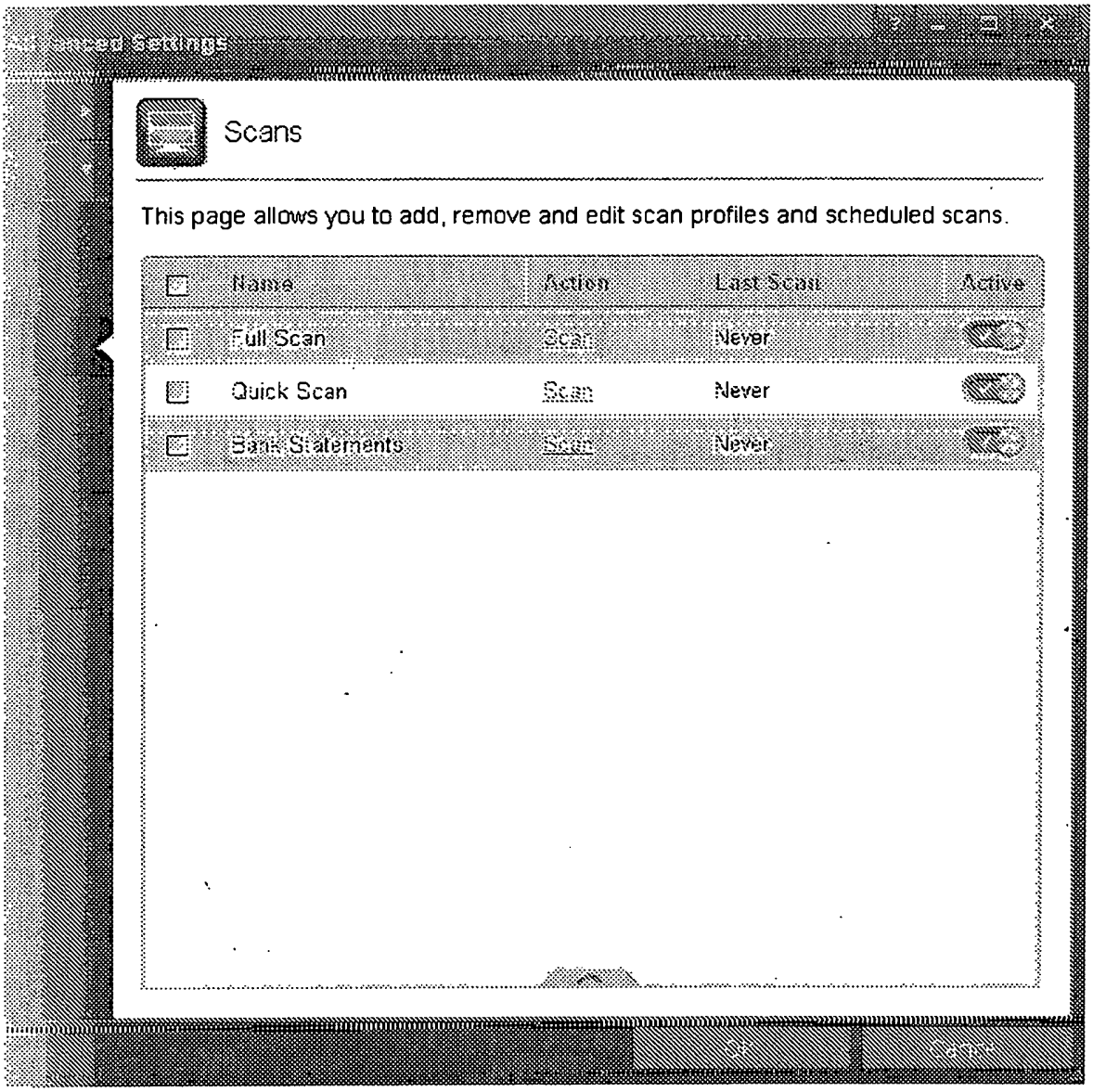


- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - Runs the scan every day at the time specified
- **Every Week** - Scans the areas defined in the scan profile on the day(s) of the week specified in 'Days of the Week' field and the time specified in the 'Start Time' field. You can select the days of the week by directly clicking on them.
- **Every Month** - Scans the areas defined in the scan profile on the day(s) of the month specified in 'Days of the month' field and the time specified in the 'Start Time' field. You can select the days of the month by directly clicking on them.
- **Run only when computer is not running on battery** - This option is useful when you are using a laptop or any other battery driven portable computer. Selecting this option runs the scan only if the computer runs with the adapter 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.

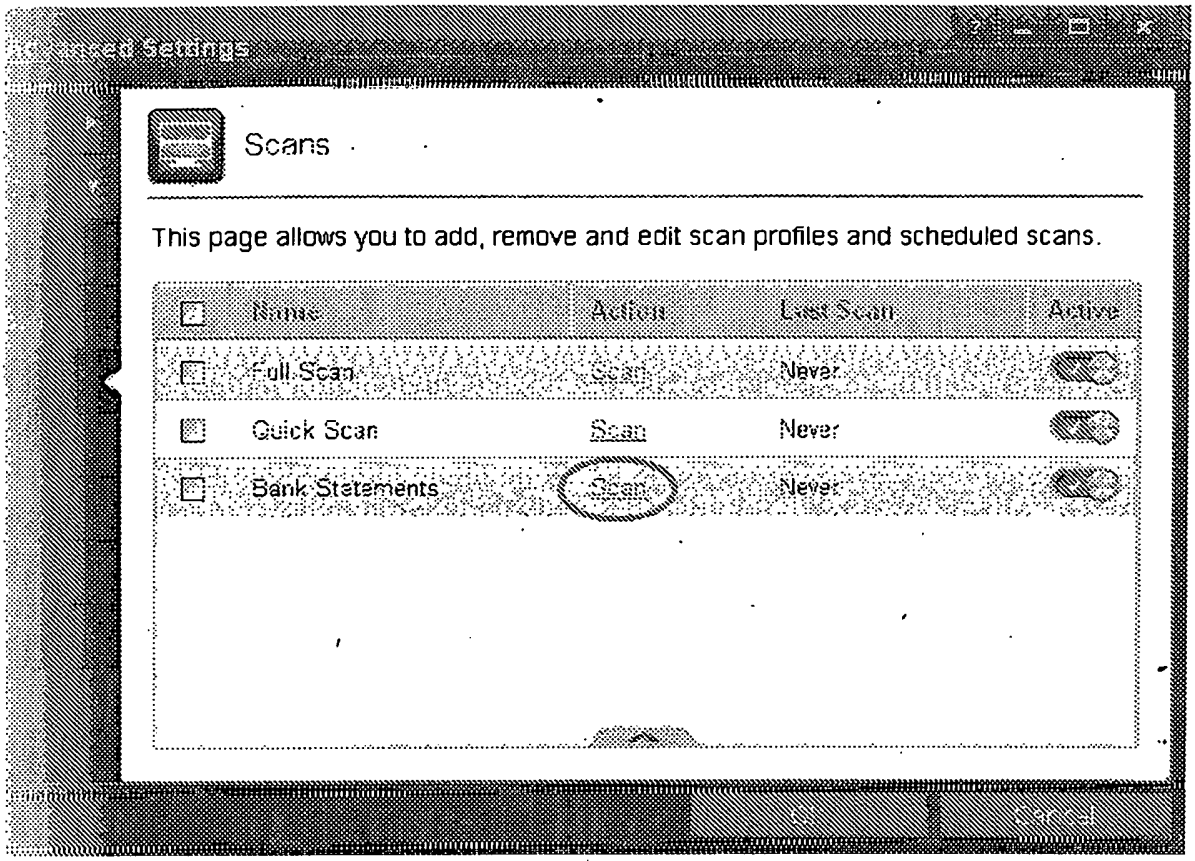
Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row

to toggle between on and off status.

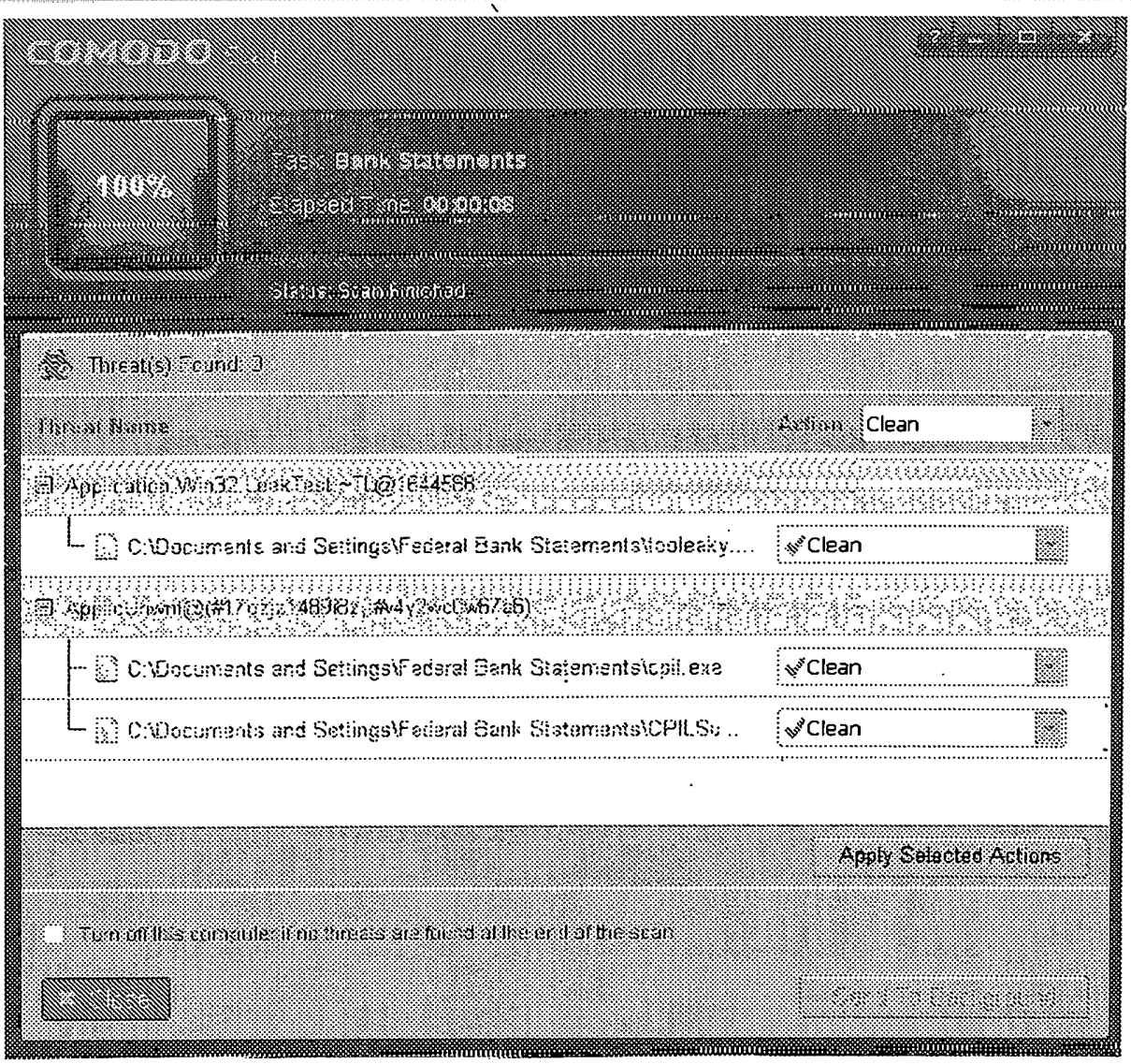


To run a custom scan as per scan profile

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



- The scan will be started and on completion the results will be displayed.



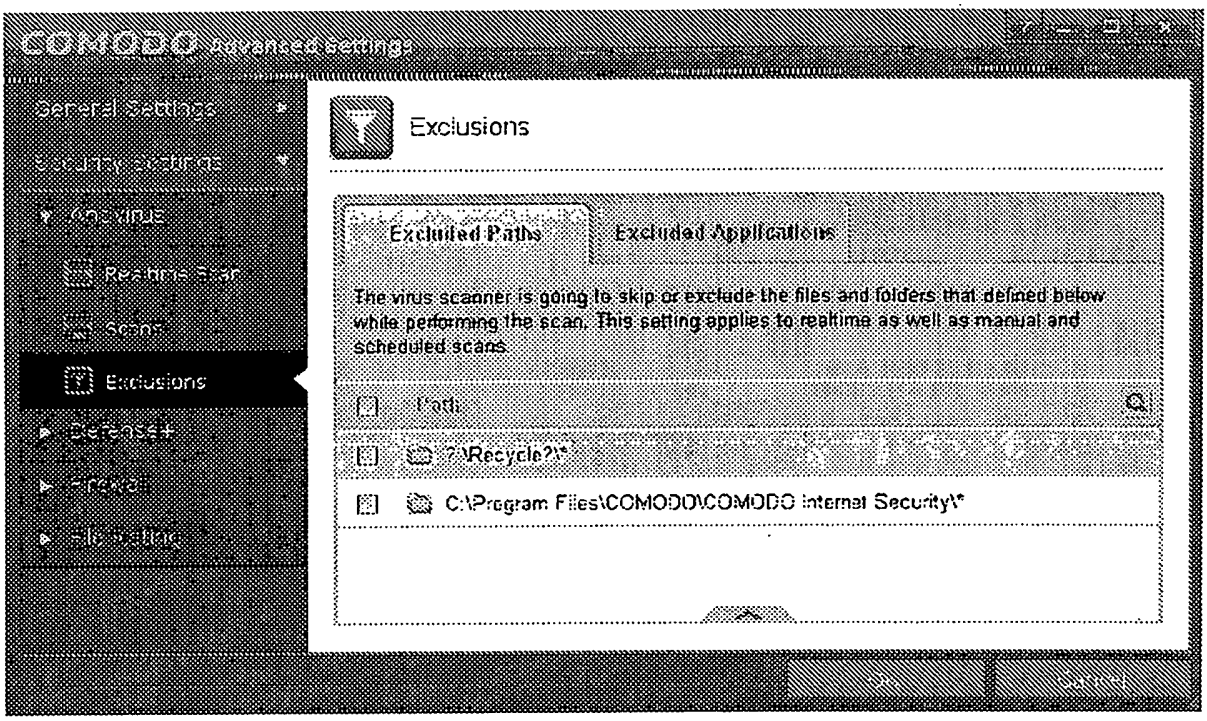
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

6.2.1.3. Exclusions

The 'Exclusions' panel under the Antivirus Settings Settings displays a list of paths and applications/files for which you have selected **Ignore** from the Scan Results window of various scans or added to the Exclusions from an antivirus alert.

To open the Exclusions panel

- Click Security Settings > Antivirus > 'Exclusions' tab in the 'Advanced Settings' panel.

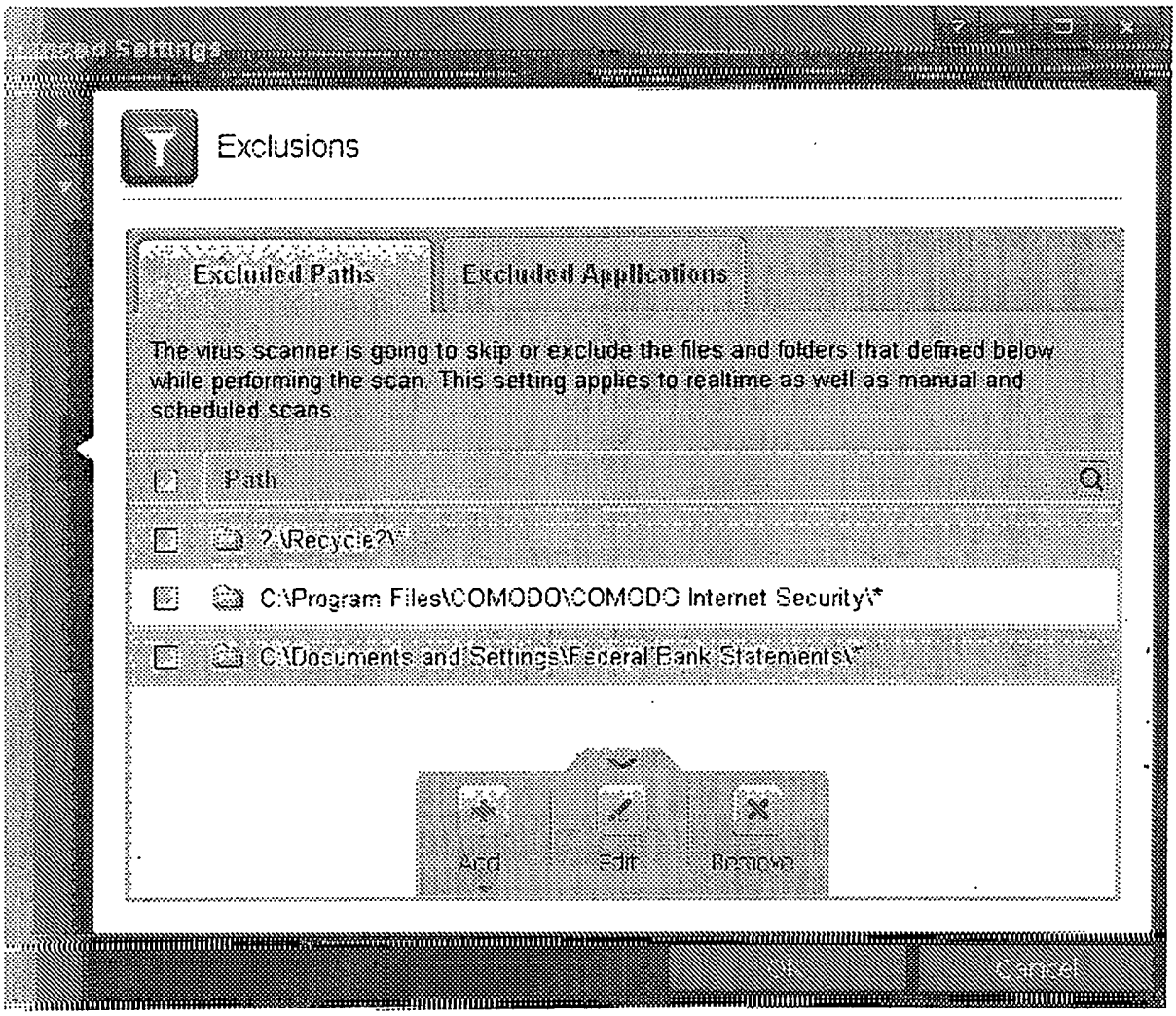


The 'Exclusions' panel has two tabs:

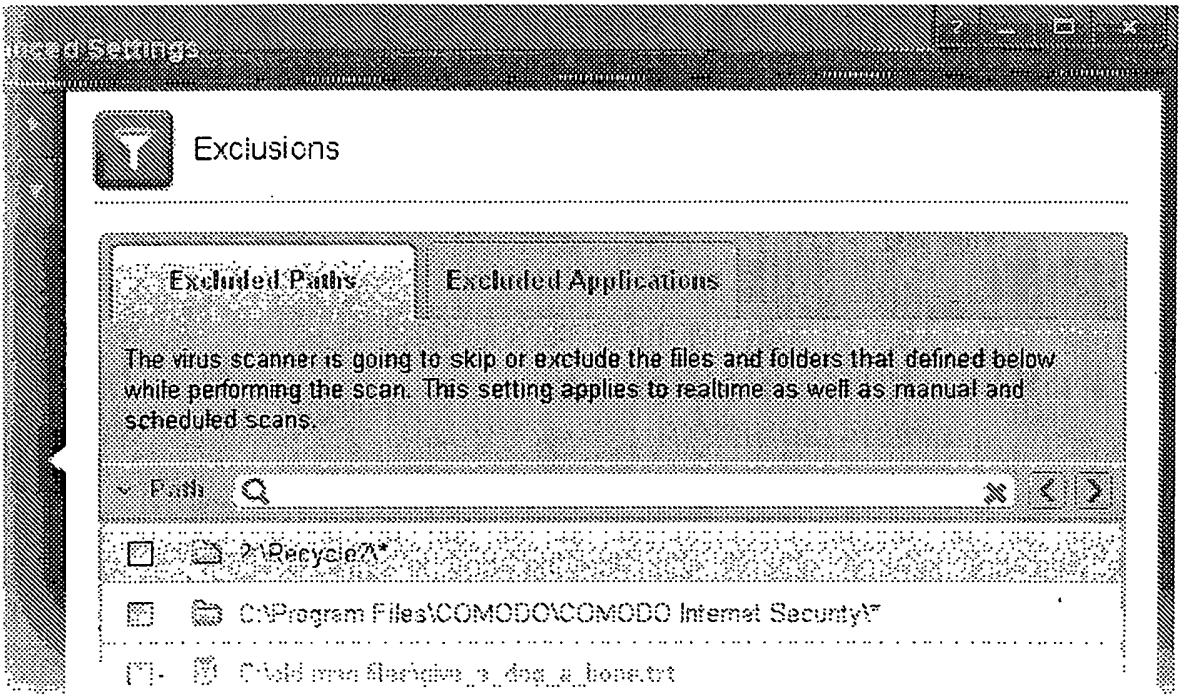
- **Excluded Paths** - Displays a list of paths/folders/files in your computer, which are excluded from both real-time and on-demand antivirus scans. Refer to the section Excluding Drives/Folders/Files from all types of scans for more details on adding and removing exclusion items in this interface.
- **Excluded Applications** - Displays a list of programs/applications in your computer, which are excluded from real-time antivirus scans. The items are included on clicking 'Ignore' from the Scan Results window of various scans and Antivirus Alerts or manually. Please note that these items are excluded only on real-time sans but will be scanned on running on-demand scans Refer to the section Excluding Programs/Applications from real-time scans more details on manually adding and removing exclusion items in this interface.

Excluding Drives/Folders/Files from all types of scans

You can exclude a drive partition, a folder, a sub-folder or a file from both the real-time and on-demand/custom scheduled antivirus scans at any time, by adding them to Excluded Paths.



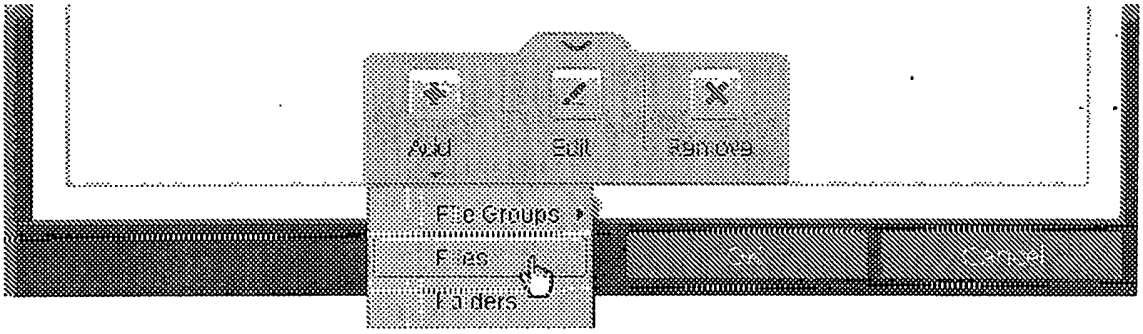
You can use the search option to find a specific excluded path, folder or file from the list by clicking the search icon at the far right in the column header.



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

To add item(s) to excluded paths

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



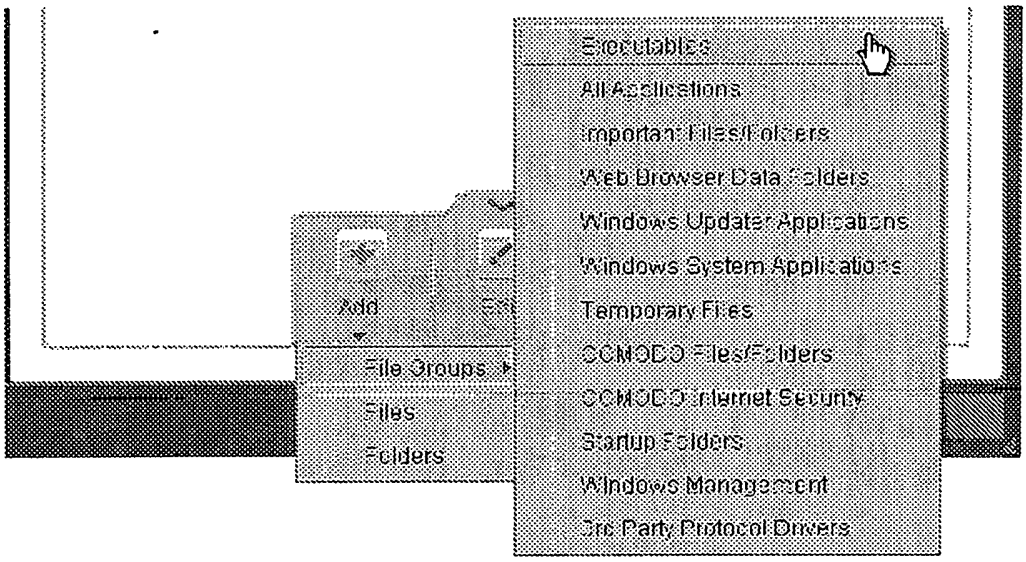
You can choose to add a:

- File Group
- Drive partition/Folder

  or,
- an individual file

Adding a File Group

- Choosing File Groups allows you to exclude a category of pre-set files or folders. For example, selecting 'Executables' would enable you to exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

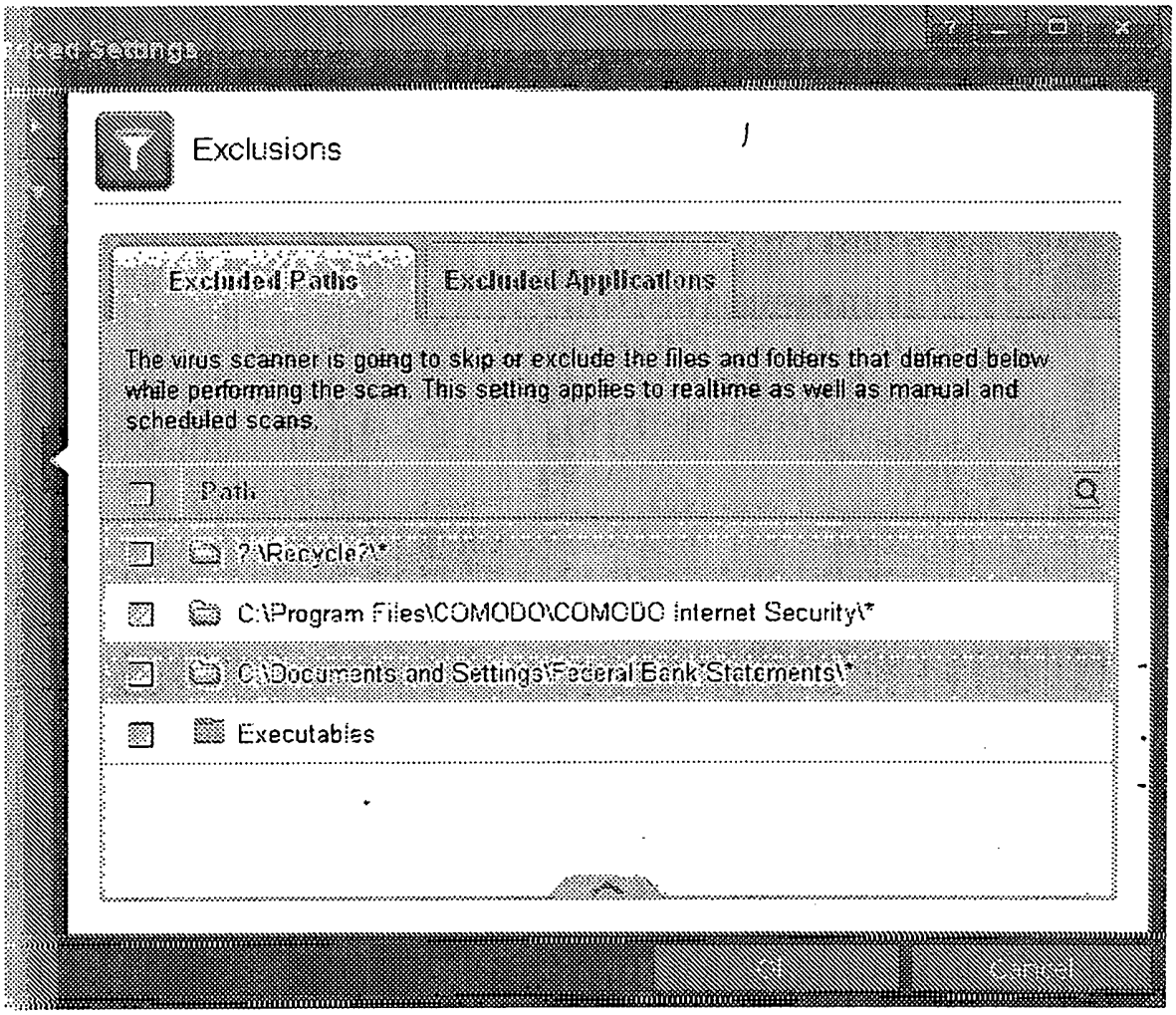


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

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

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

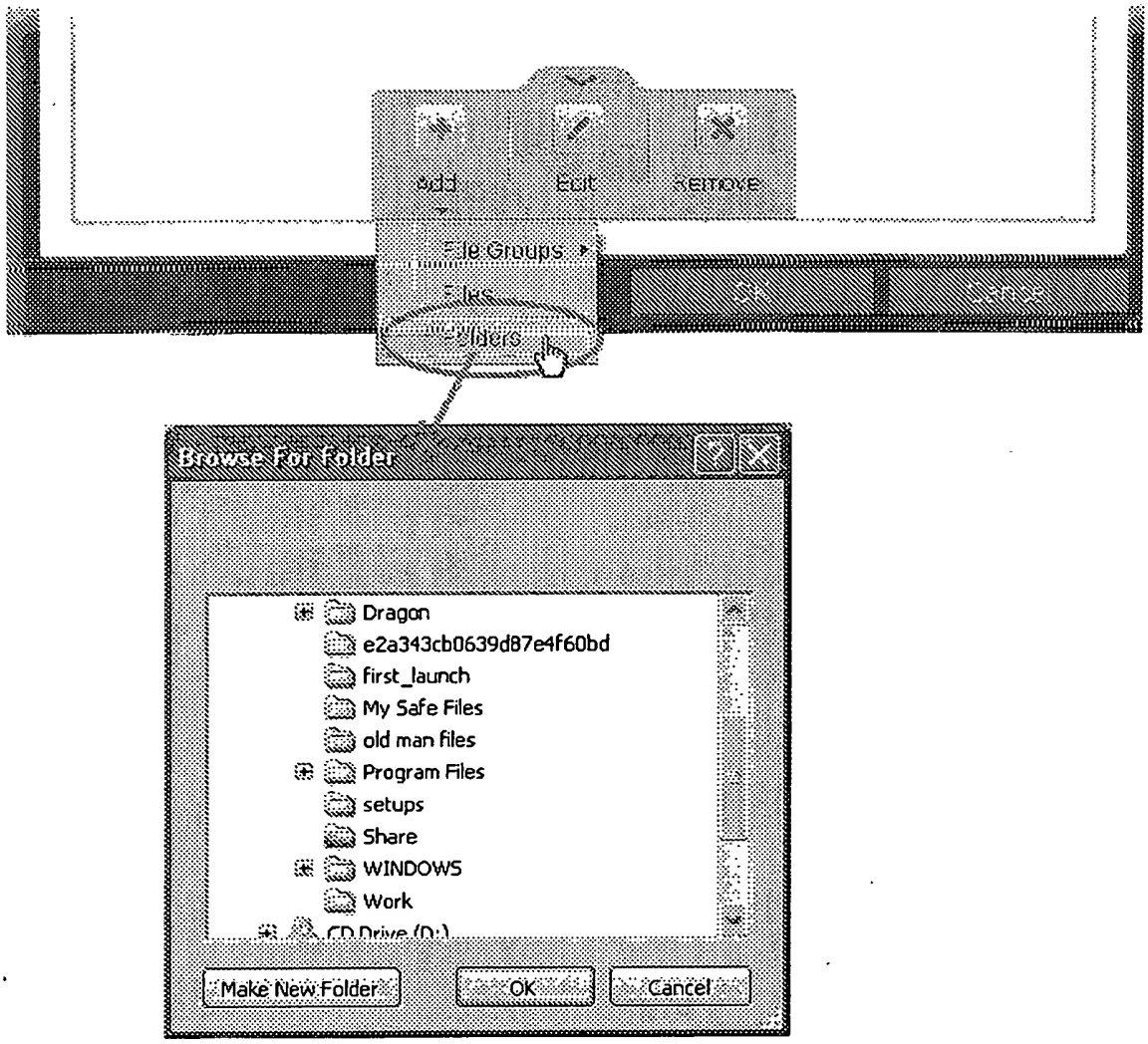
The file groups will be added to Excluded Paths.



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

Adding a Drive Partition/Folder

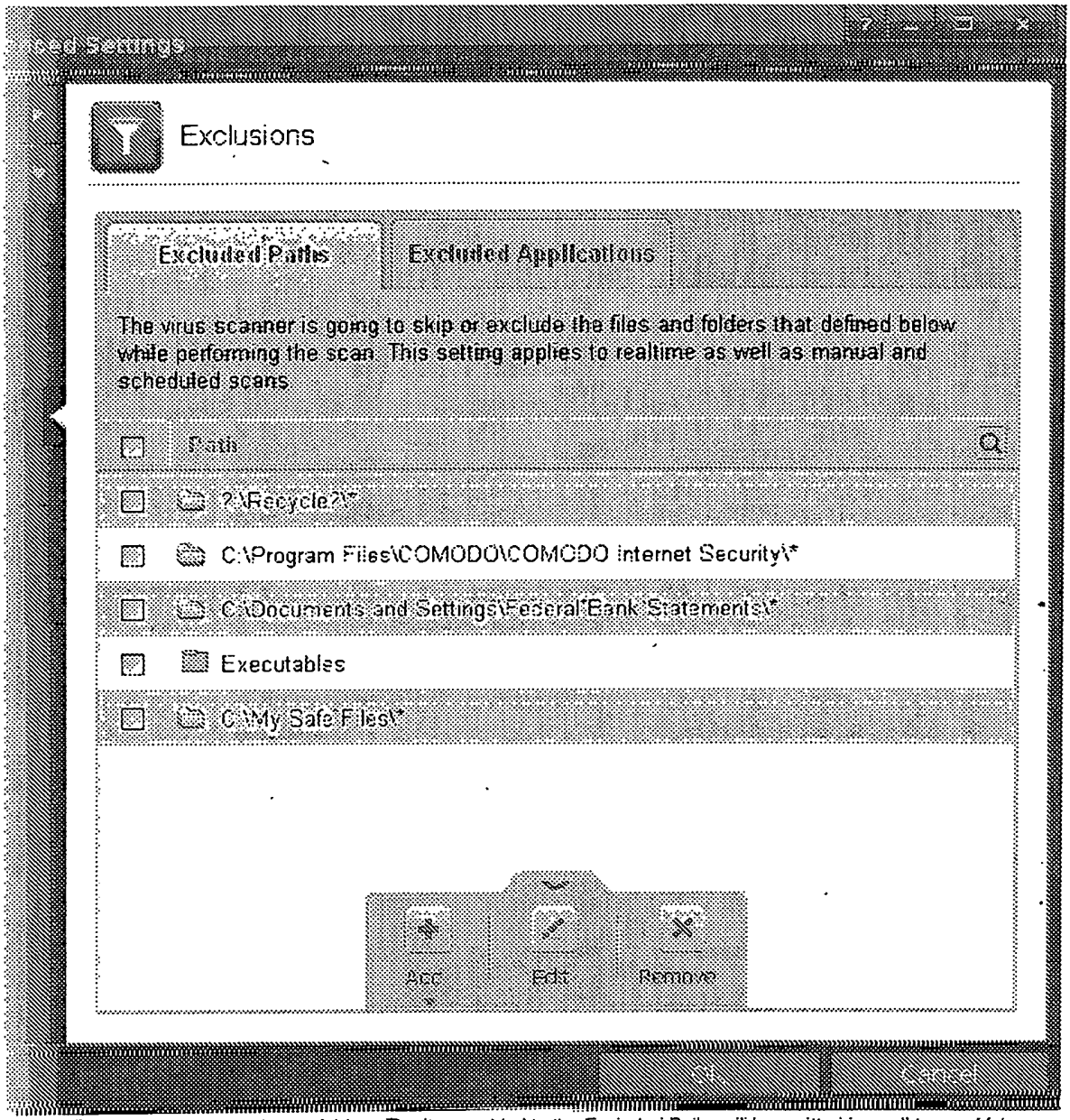
- To add a folder, choose 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will appear.

- Navigate to the drive partition or folder you want to add to excluded paths and click OK

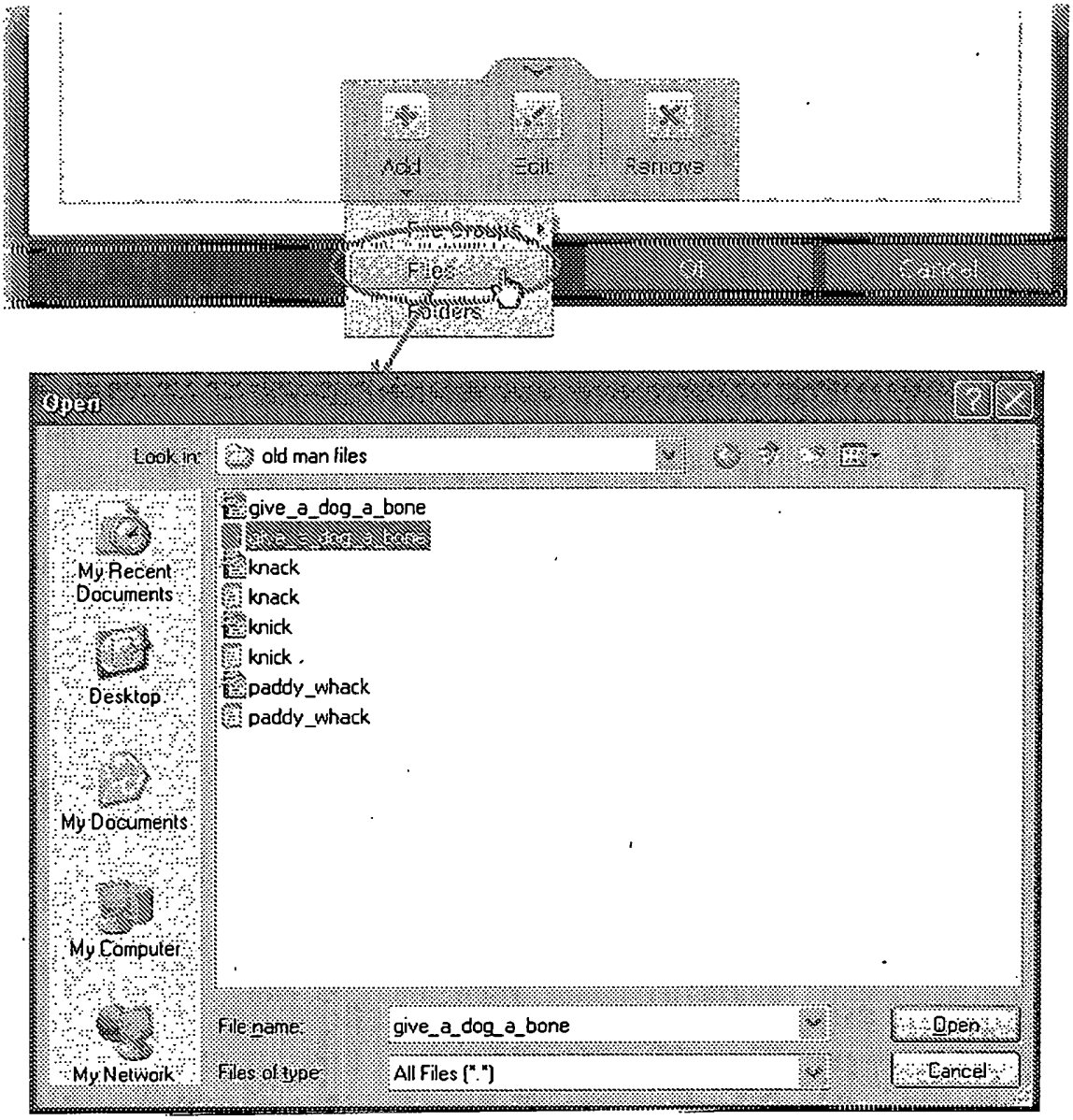
The drive partition/folder will be added to Excluded Paths.



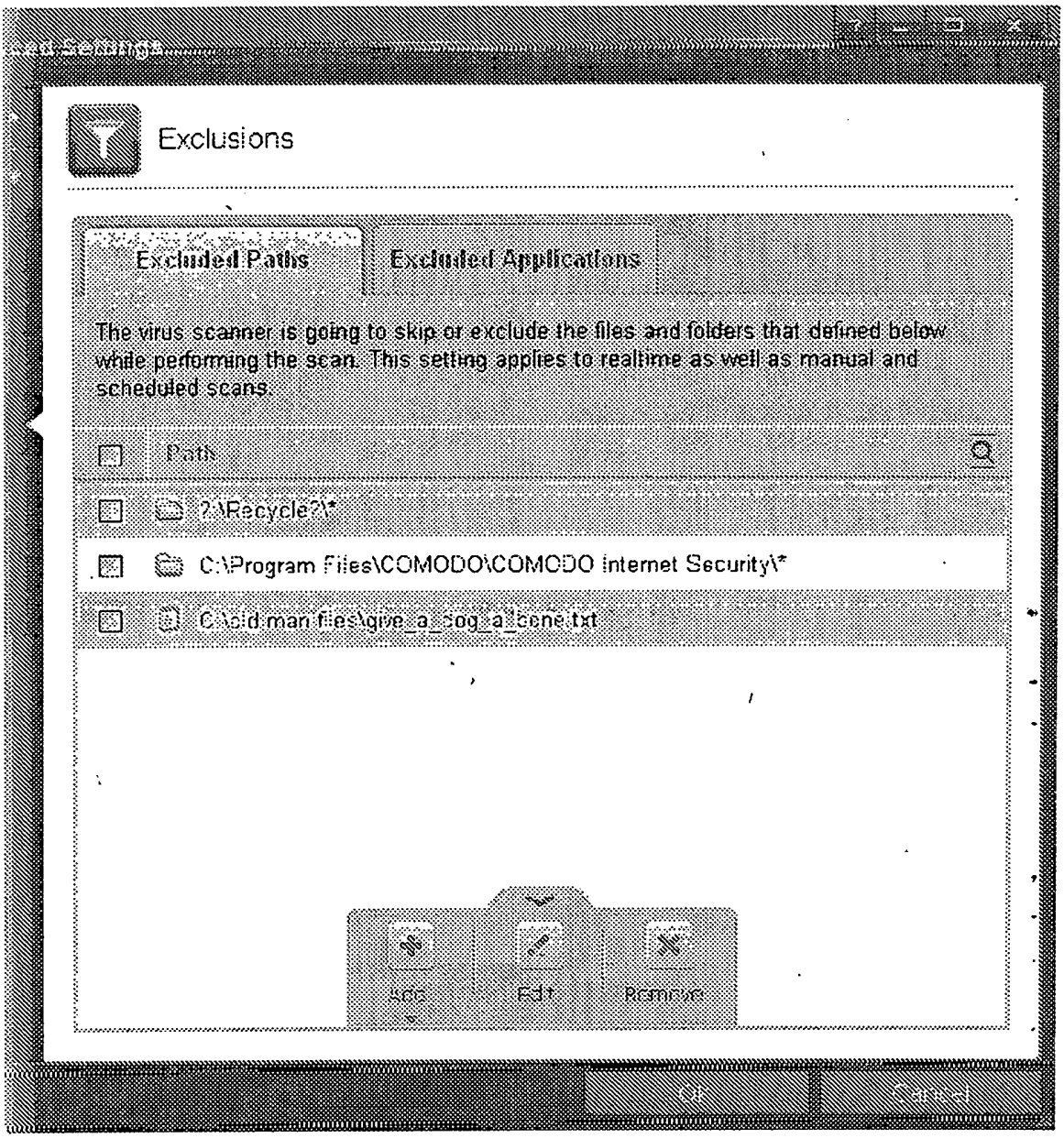
- Repeat process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

Adding an individual File

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



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

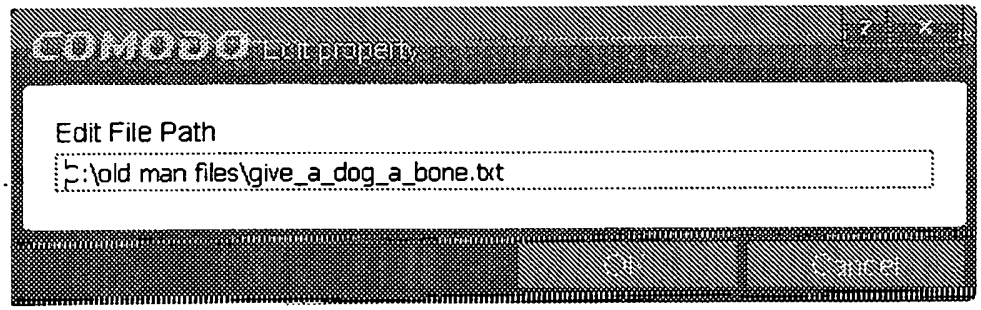


The file will be added to Excluded Paths.

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

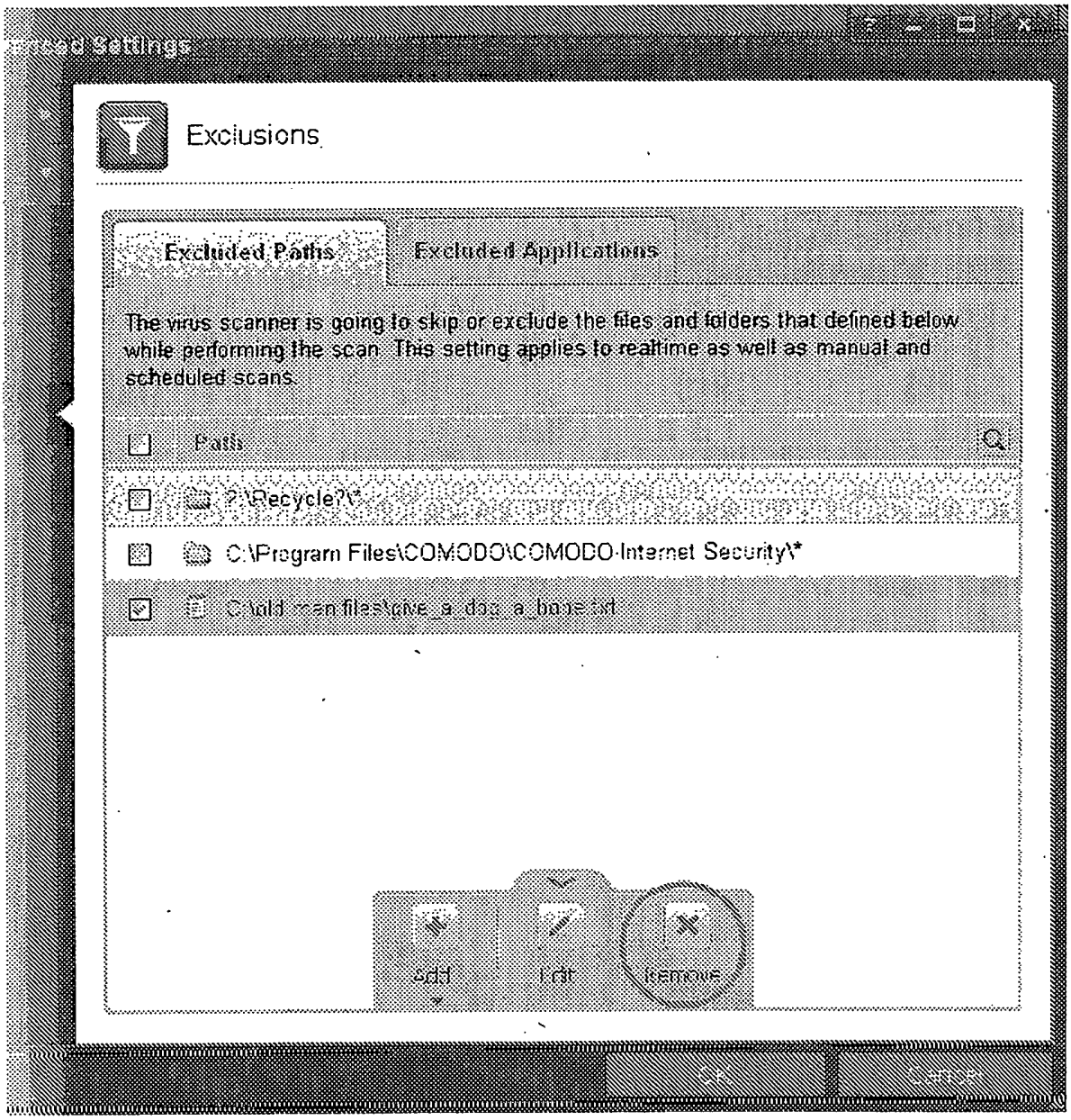
To edit the path of an added item

- Select the item, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



To remove an item from the Excluded Paths

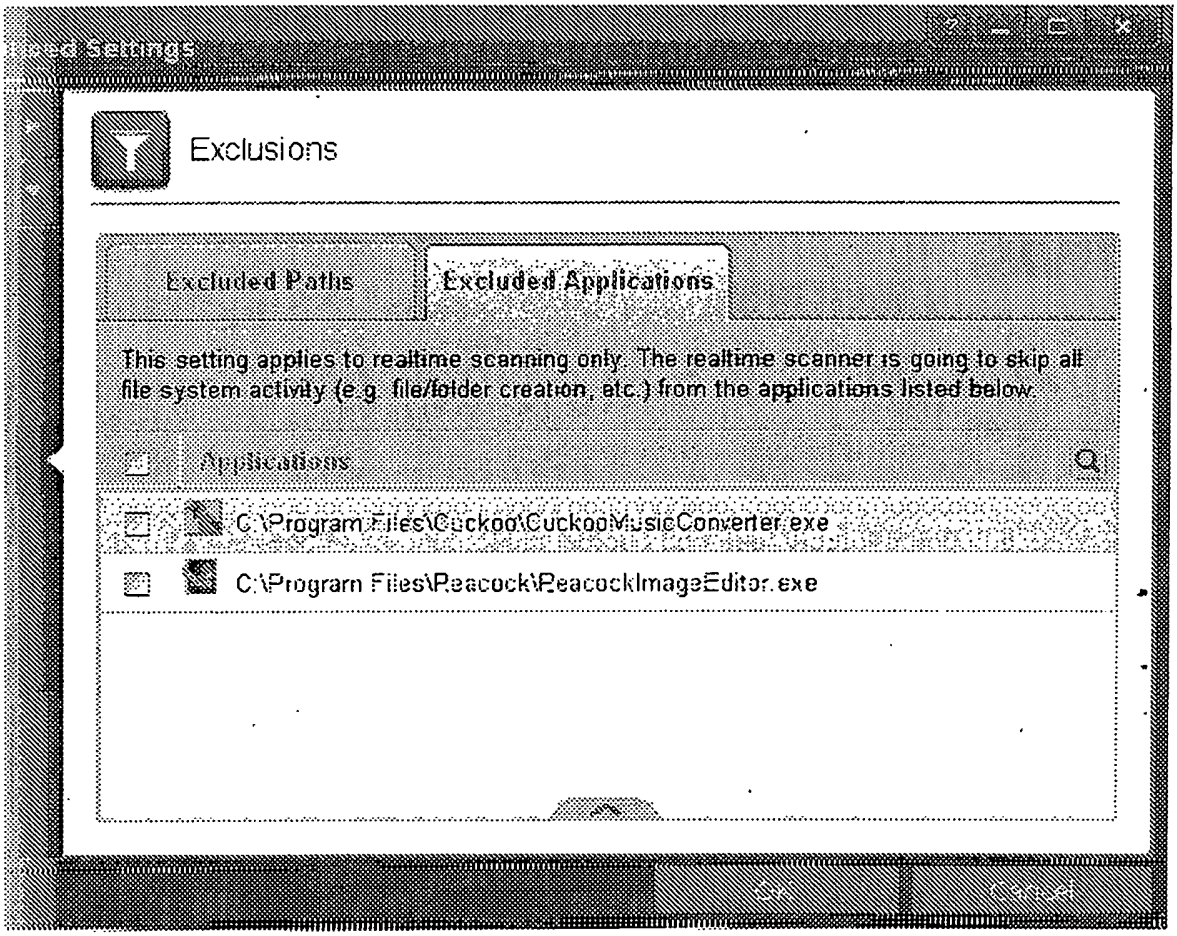
- Select the item, click the handle from the bottom center and select 'Remove'.



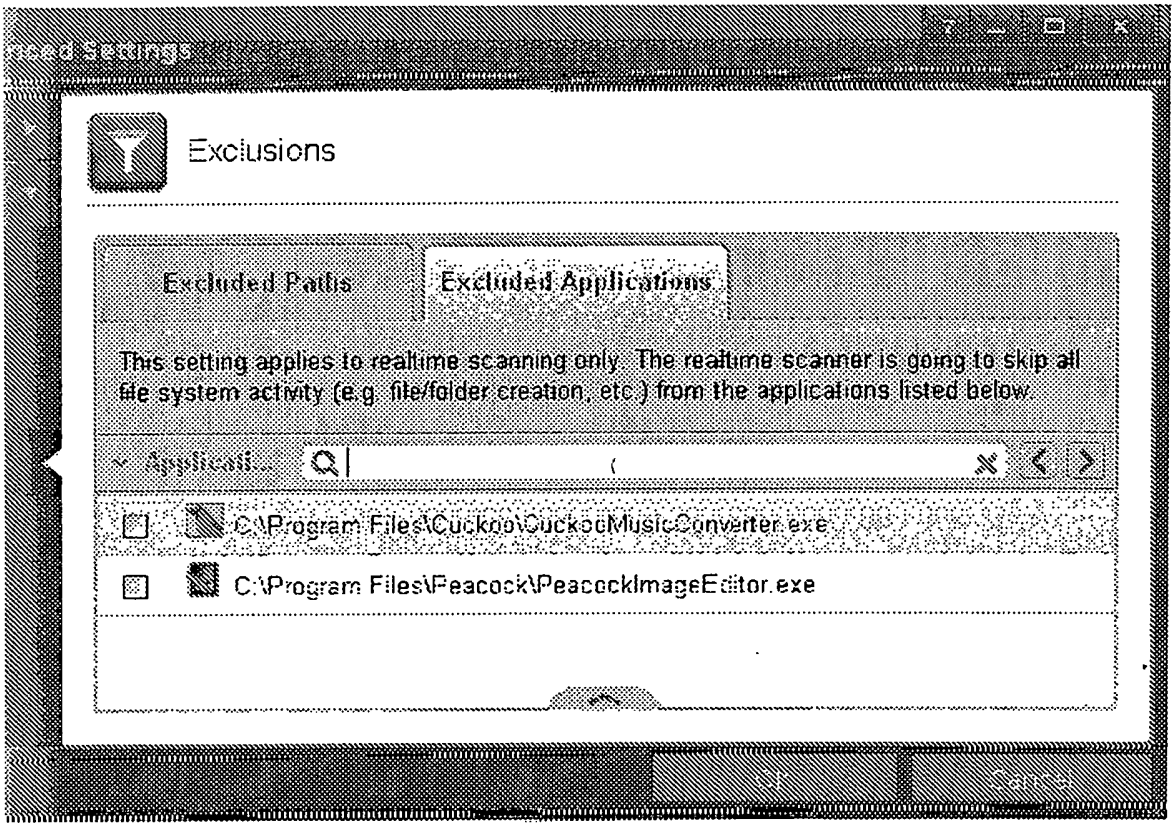
- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

Excluding Programs/Applications from Real-time Scans

The 'Excluded Applications' tab allows you to manually add programs, applications of files to Excluded Applications list for excluding them from real-time scans. Also you can remove the items from Excluded Applications that were added by mistake.



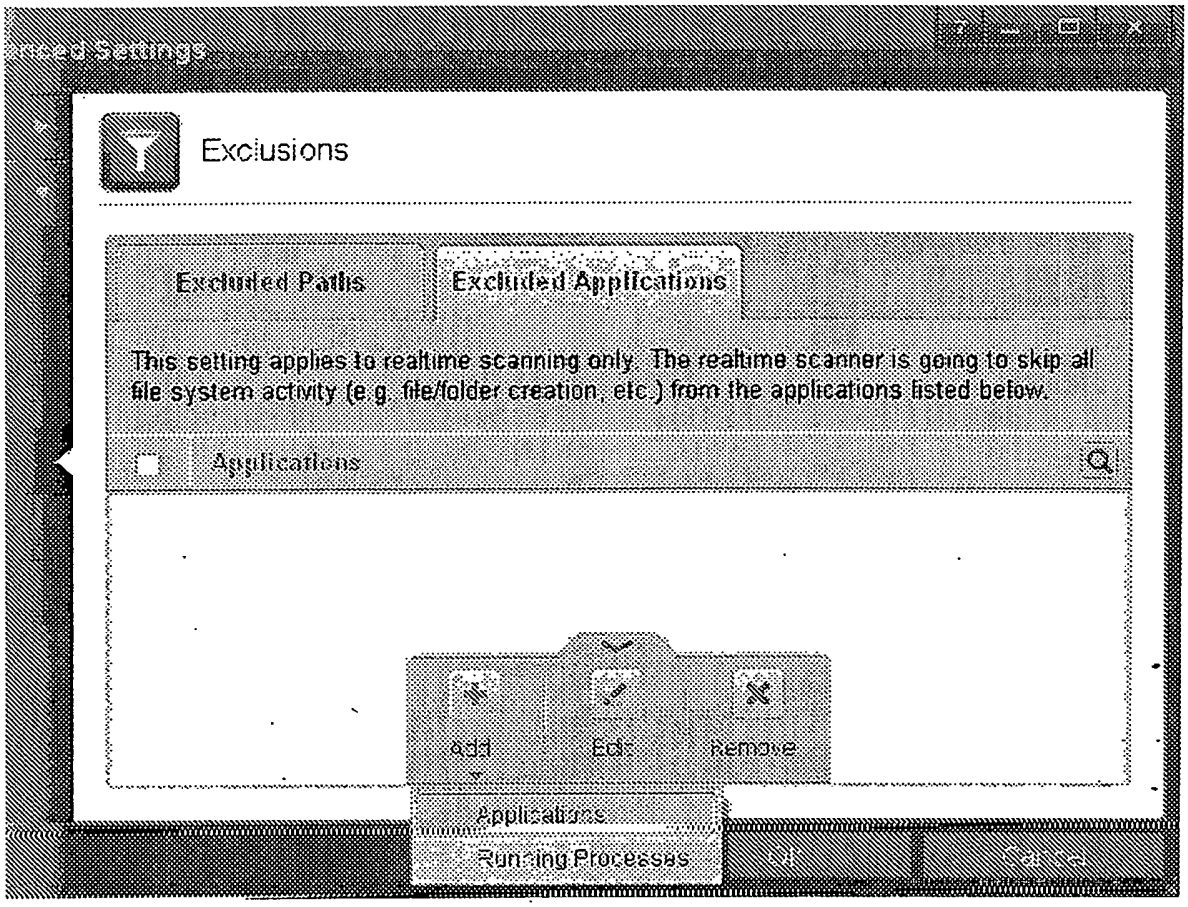
You can use the search option to find a specific excluded application from the list by clicking the search icon at the far right in the column header.



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

To add an item to Excluded Applications

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

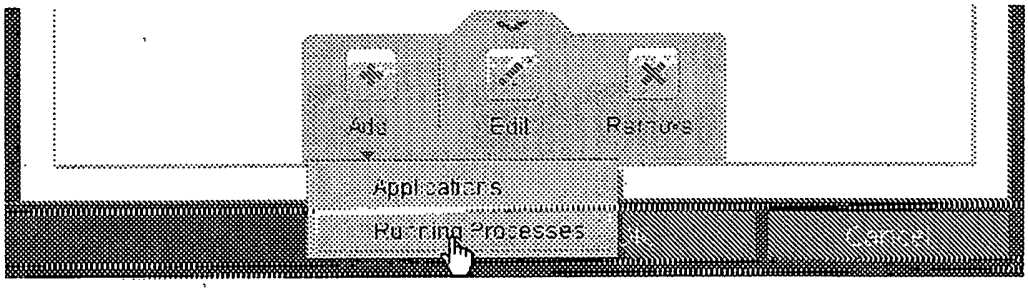


You can choose to add an application by:

- Selecting it from the running processes - This option allows you to choose the target application from the list of processes that are currently running on your PC.
- Browsing your computer for the application - This option is the easiest for most users and simply allows you to browse the files which you want to exclude from a virus scan.

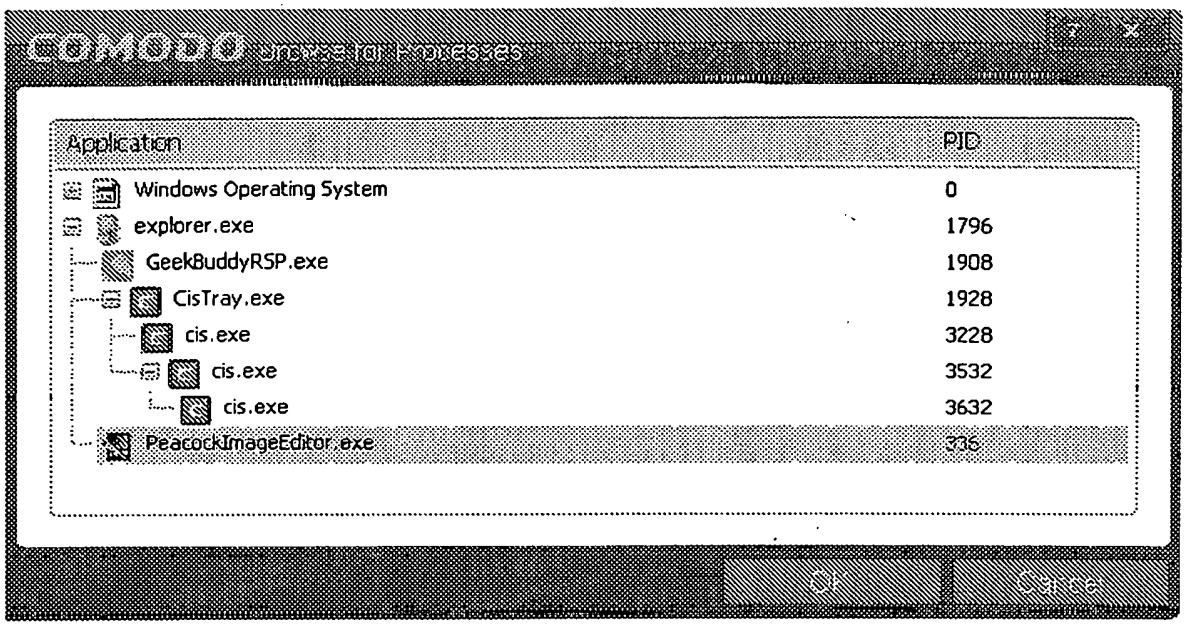
Adding an application from a running processes

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

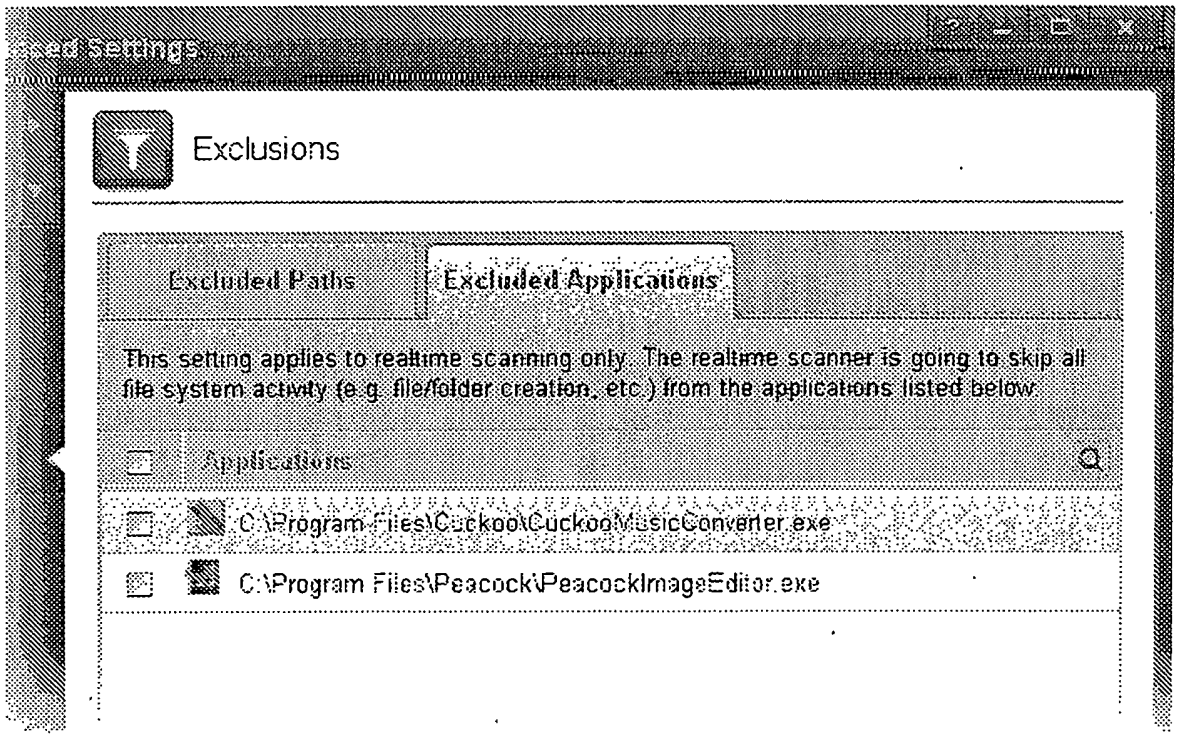


A list of currently running processes in your computer will be displayed

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

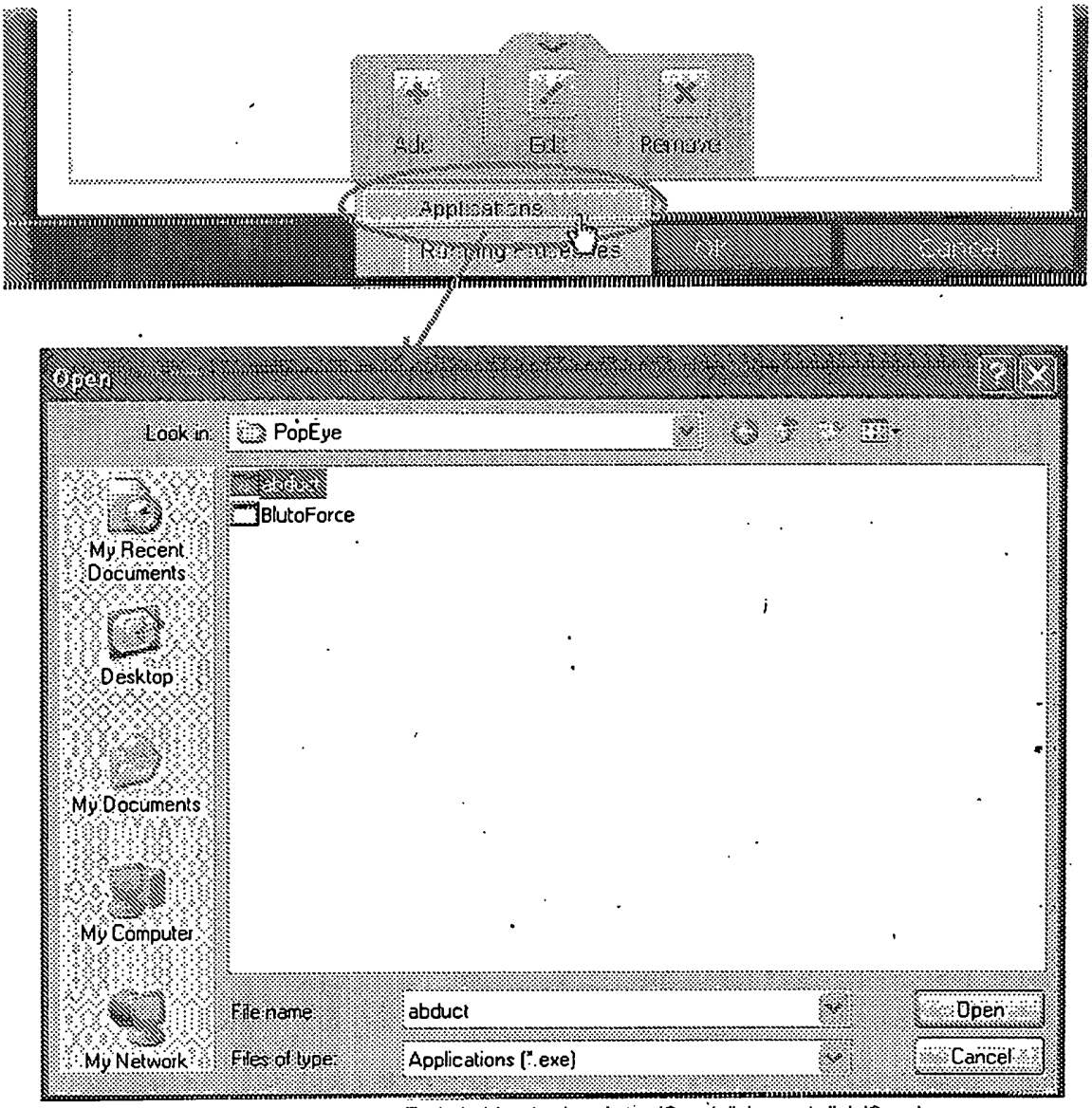


The application will be added to Excluded Applications.



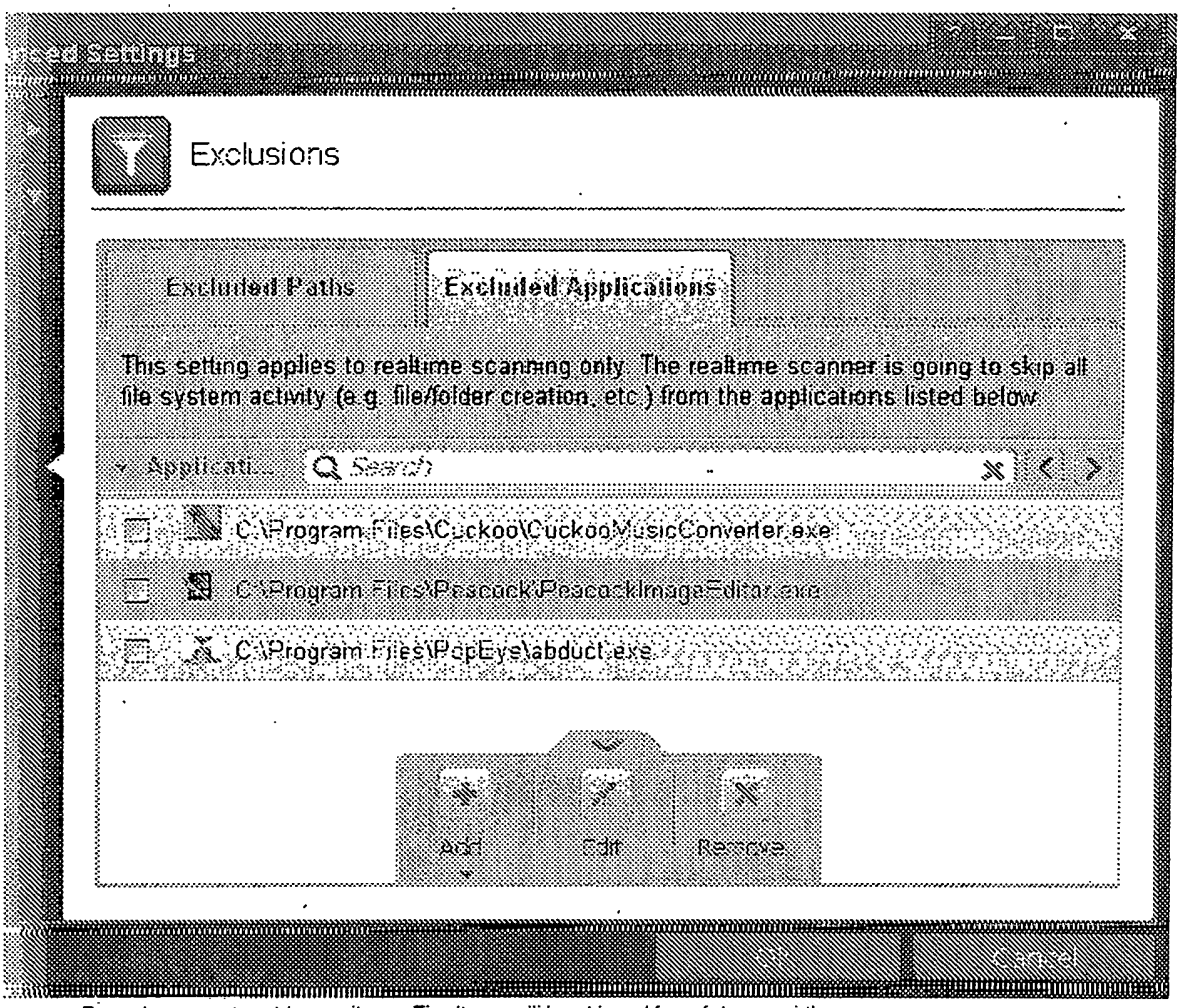
Browsing to the Application

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



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

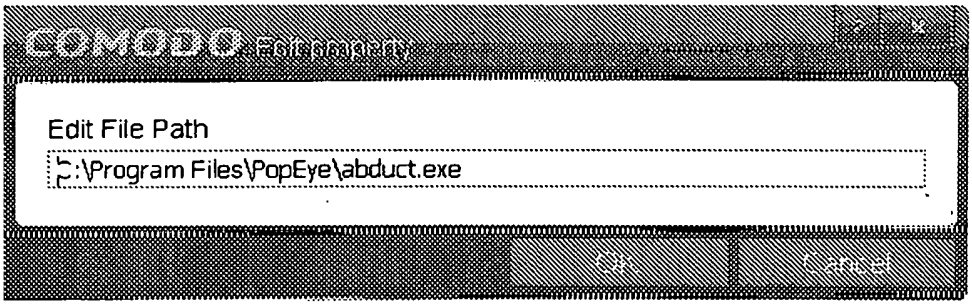
The file will be added to 'Excluded Applications'.



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

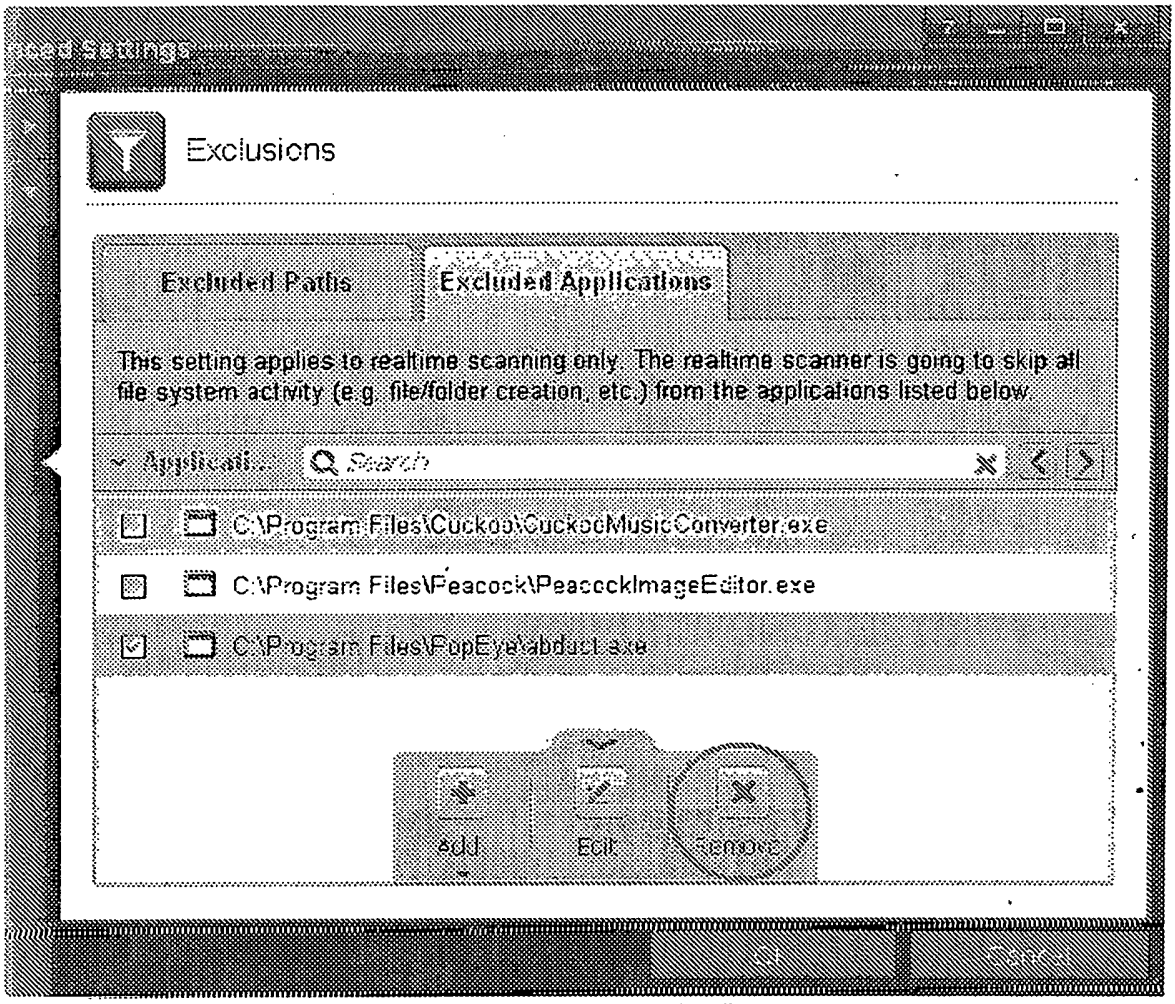
To edit the path of the application added to Excluded Application

- Select the application, click the handle from the bottom center and select 'Edit'.
- Make the required changes for the file path in the Edit Property dialog.



To remove an item from the Excluded Applications

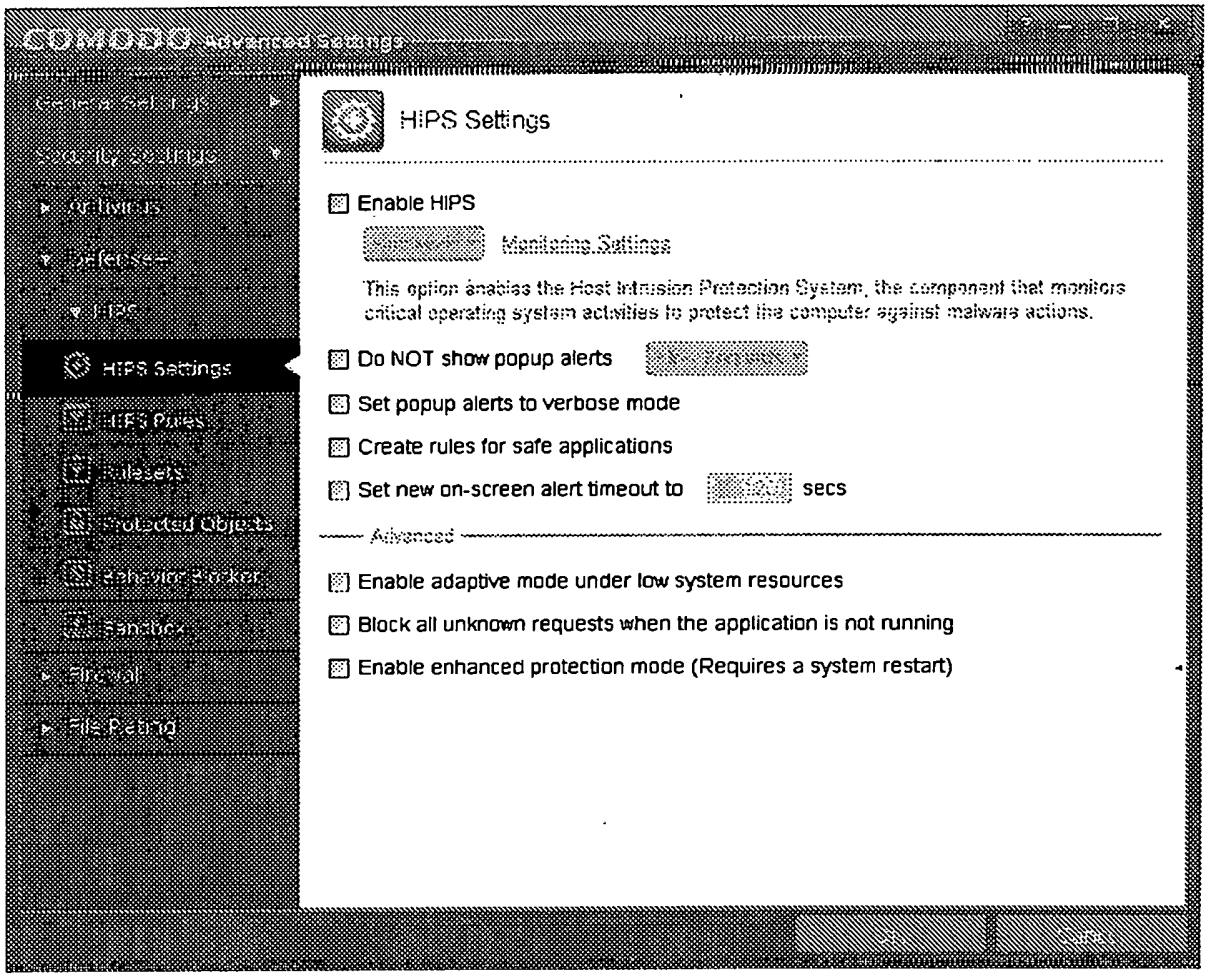
- Select the item, click the handle from the bottom center and select 'Remove'.



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

6.2.2. Defense+ Settings

Defense+ is a collective term that covers the Host Intrusion Prevention (HIPS), sandboxing and behavior blocker components of Comodo Internet Security. Together, these technologies ensure all applications, processes and services on your PC behave in a secure manner - and are prevented from taking actions that could damage your computer or your data.



The Defense+ settings area allows you to configure the following:

- HIPS
  - HIPS Behaviour Settings
  - Active HIPS Rules
  - Predefined HIPS Rule Sets
  - Protected Objects
- Behavior Blocker
- Sandbox Settings

6.2.2.1. HIPS Behavior Settings

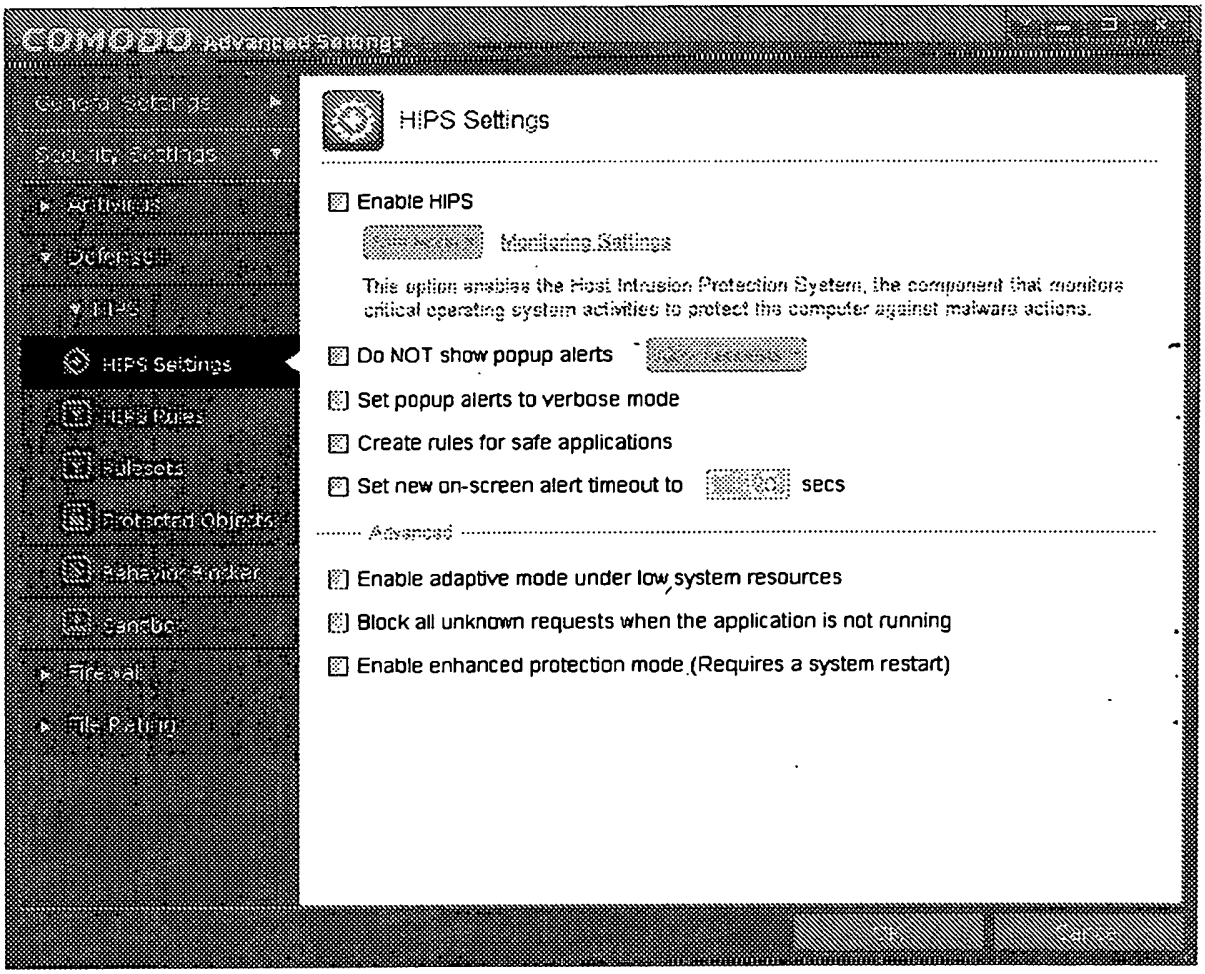
HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo Internet Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs. Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

Note for beginners: This page often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your computer to perform a task or function. Every program, application and device you run on your computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. (e.g., when you start Microsoft Word, the executable file 'winword.exe' instructs your computer to start and run the Word application). Other types of

executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.

Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data; steal your identity; corrupt system files; give control of your PC to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms.

- The HIPS Settings panel allows you to enable/disable HIPS, set its security level and configure its general behavior.
- The HIPS Settings panel can be accessed by clicking Security Settings > Defense+ > HIPS > 'HIPS Settings' tab from 'Advanced Settings' interface



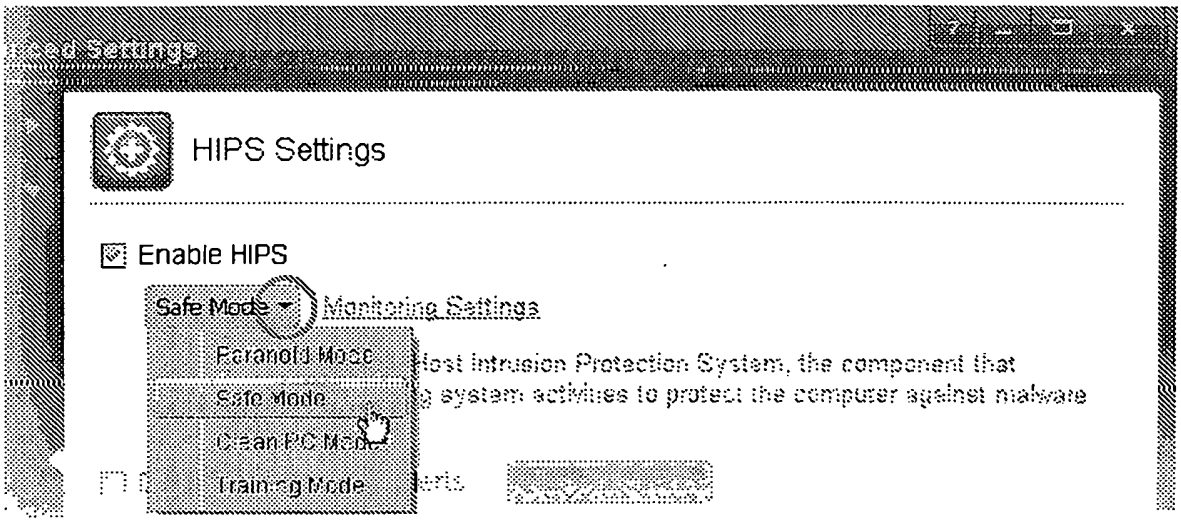
- **Enable HIPS** - Allows you to enable/disable the HIPS protection.*(Default=Disabled)*

Note: The HIPS settings can also be configured in the 'Advanced View' of the 'Home' screen by clicking the status link beside HIPS in the 'Defense+ and Sandbox' pane.

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

Configuring Security Level of HIPS

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



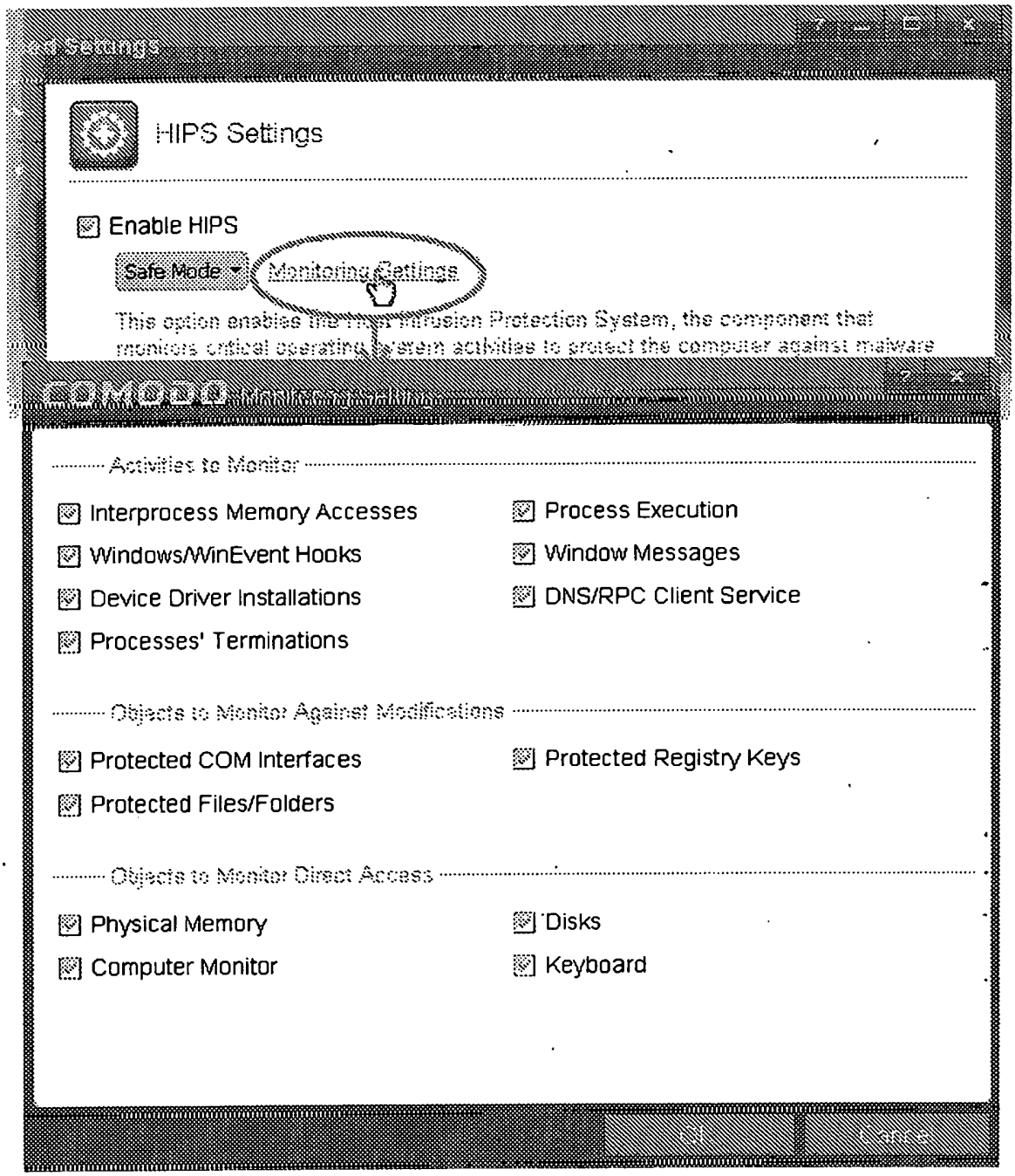
The choices available are:

- **Paranoid Mode**: This is the highest security level setting and means that Defense+ monitors and controls all executable files apart from those that you have deemed safe. Comodo Internet Security does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses *your* configuration settings to filter critical system activity. Similarly, the Comodo Internet Security does automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the HIPS alert. Choosing this option generates the most amount of HIPS alerts and is recommended for advanced users that require complete awareness of activity on their system.
- **Safe Mode**: While monitoring critical system activity, Defense+ automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules these activities, if the checkbox 'Create rules for safe applications' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs the Defense+ not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of HIPS alerts.
- **Clean PC Mode:** From the time you set the slider to 'Clean PC Mode', Defense+ learns the activities of the applications currently installed on the computer while all new executables introduced to the system are monitored and controlled. This patent-pending mode of operation is the recommended option on a new computer or one that the user knows to be clean of malware and other threats. From this point onwards HIPS alerts the user whenever a new, unrecognized application is being installed. In this mode, the files in 'Unrecognized Files' are excluded from being considered as clean and are monitored and controlled.
- **Training Mode**: Defense+ monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. You do not receive any HIPS alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

Configuring the Monitoring Settings

The activities, entities and objects that should monitored by HIPS can be configured by clicking the Monitoring Settings link.

Note: The settings you choose here are universally applied. If you disable monitoring of an activity, entity or object using this interface it completely switches off monitoring of that activity on a ***global*** basis - effectively creating a universal '**Allow**' rule for that activity . This 'Allow' setting ***over-rules*** any Ruleset specific 'Block' or 'Ask' setting for that activity that you may have selected using the 'Access Rights' and 'Protection Settings' interface.



Activities To Monitor:

- **Interprocess Memory Access** - Malware programs use memory space modification to inject malicious code for numerous types of attacks, including recording your keyboard strokes; modifying the behavior of the invaded application; stealing confidential data by sending confidential information from one process to another process etc. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of the invaded process, or 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and HIPS alerts you when an application attempts to modify the memory space allocated to another application ***(Default = Enabled)***.
- **Windows/WinEvent Hooks** - In the Microsoft Windows® operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) *before* they reach an application. The function can act on events and, in some cases, modify or discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer; take over control of your mouse and keyboard to remotely administer your computer. Leaving this box checked means that you are warned every time a hook is

executed by an untrusted application *(Default = Enabled)*.

- **Device Driver Installations** - Device drivers are small programs that allow applications and/or operating systems to interact with a hardware device on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable damage to your computer or even pass control of that device to a hacker. Leaving this box checked means HIPS alerts you every time a device driver is installed on your machine by an untrusted application *(Default = Enabled)*.
- **Processes' Terminations** - A process is a running instance of a program. (for example, the Comodo Internet Security process is called 'cis.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your system). Terminating a process, obviously, terminates the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, Defense+ monitors and alerts you to all attempts by an untrusted application to close down another application *(Default = Enabled)*.
- **Process Execution** - Typical malware like rootkits, keylogger etc. would often invoke by itself and runs its process mostly at the background. These processes, invisible at the foreground will act as agents for infecting your computer and to steal your confidential and sensitive information like your credit card details and passwords and pass to hackers. With this setting enabled, the HIPS monitors and alerts you to whenever a process is invoked by an untrusted application. *(Default = Enabled)*.
- **Windows Messages** - This setting means Comodo Internet Security monitors and detects if one application attempts to send special Windows Messages to modify the behavior of another application (e.g. by using the WM_PASTE command) *(Default = Enabled)*.
- **DNS/RPC Client Service** - This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack whereby an malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' pc's which are sending out these requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled prevents malware from using the DNS Client Service to launch such an attack *(Default = Enabled)*.

Background Note: DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever you type a domain name, your Internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to your computer, telling it to connect to the IP in question.

Objects To Monitor Against Modifications:

- **Protected COM Interfaces** enables monitoring of COM interfaces you specified from the COM Protection pane. *(Default = Enabled)*
- **Protected Registry Keys** enables monitoring of Registry keys you specified from the Registry Protection pane. *(Default = Enabled)*.
- **Protected Files/Folders** enables monitoring of files and folders you specified from the File Protection pane. *(Default = Enabled)*.

Objects To Monitor Against Direct Access:

Determines whether or not Comodo Internet Security should monitor access to system critical objects on your computer. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advises the average user to leave these settings enabled:

- **Physical Memory:** Monitors your computer's memory for direct access by an applications and processes. Malicious programs attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address. This overwrites its internal structures and can be used by malware to force the system to execute its code *(Default = Enabled)*.
- **Computer Monitor:** Comodo Internet Security raises an alert every time a process tries to directly access your computer monitor. Although legitimate applications sometimes require this access, there is also an emerging category

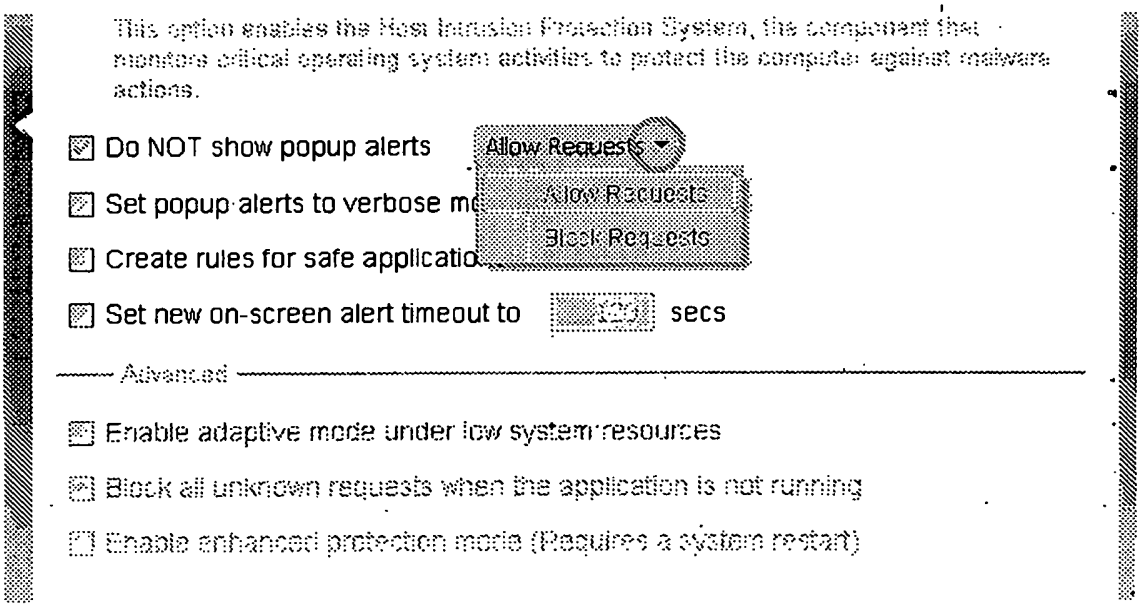
of spyware programs that use such access to monitor users' activities. (for example, to take screen shots of your current desktop; to record your browsing activities etc) ***(Default = Enabled)***.

- **Disks:** Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data ***(Default = Enabled)***.
- **Keyboard:** Monitors your keyboard for access attempts. Malicious software, known as 'key loggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Internet Security alerts you every time an application attempts to establish direct access to your keyboard ***(Default = Enabled)***.

Checkbox Options

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

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



- **Set popup alerts to verbose mode** - Enabling this option instructs CIS to display HIPS Alerts in verbose mode, providing more more informative alerts and more options for the user to allow or block the requests ***(Default = Disabled)***.
- **Create rules for safe applications** - Automatically creates rules for safe applications in HIPS Ruleset ***(Default = Disabled)***.

> Note: HIPS trusts the applications if:
>
> - The application/file is included in the Trusted Files list
> - The application is from a vendor included in the Trusted Software Vendors list
> - The application is included in the extensive and constantly updated Comodo safelist.

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

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

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

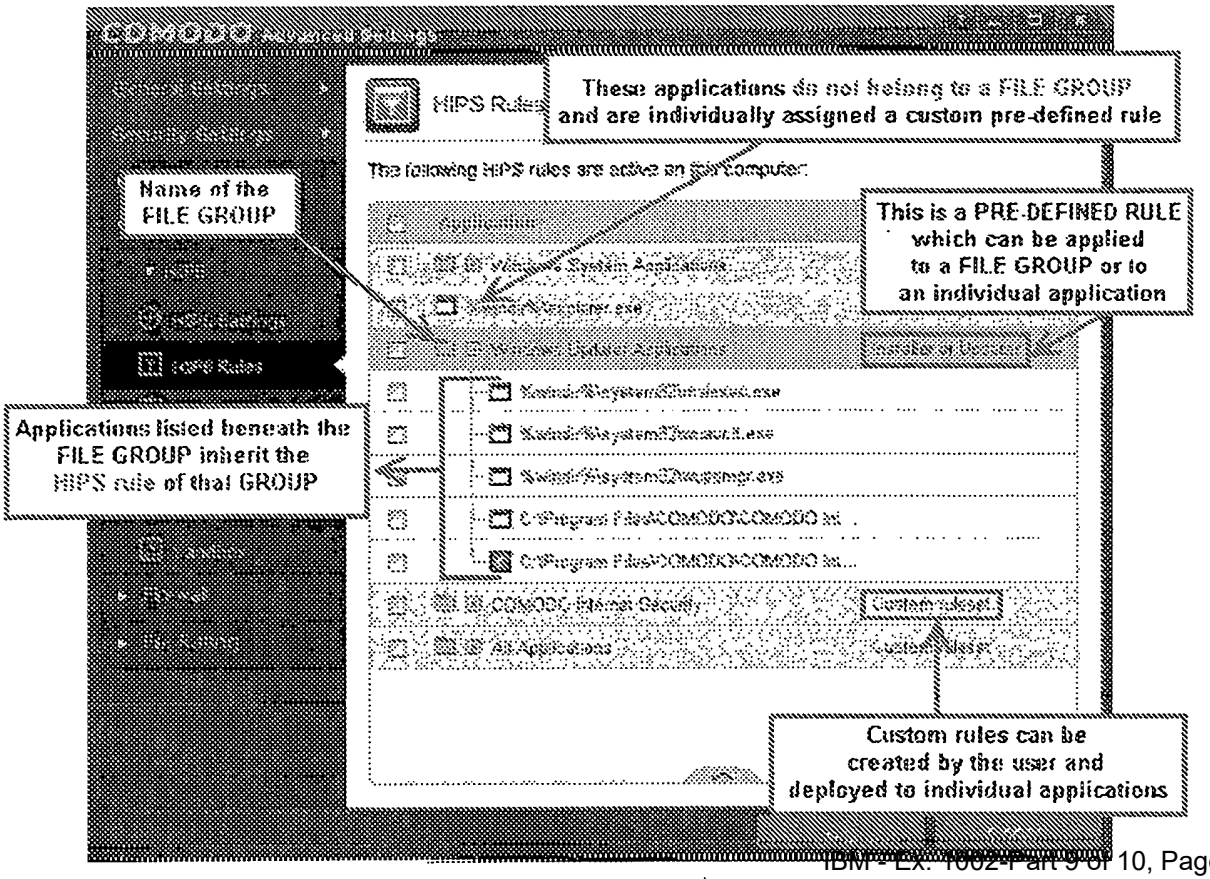
- **Set new on-screen alert time out to**: Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

Advanced HIPS Settings

- **Enable adaptive mode under low system resources** - Very rarely (and only in a heavily loaded system), low memory conditions might cause certain CIS functions to fail. With this option enabled, CIS will attempt to locate and utilize memory using adaptive techniques so that it can complete its pending tasks. However, the cost of enabling this option may be reduced performance in even lightly loaded systems ***(Default = Disabled)***.
- **Block all unknown requests if the application is closed** - Selecting this option blocks all unknown execution requests if Comodo Internet Security is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CIS security settings then it is OK to leave this box unchecked. ***(Default = Disabled)***
- **Enable enhanced protection mode** - On 64 bit systems, enabling this mode will activate additional host intrusion prevention techniques to countermeasure extremely sophisticated malware that tries to bypass regular countermeasures. Because of limitations in Windows 7/8 x64 systems, some HIPS functions in previous versions of CIS could theoretically be bypassed by malware. Enhanced Protection Mode implements several patent-pending ways to improve HIPS. CIS requires a system restart for enabling enhanced protection mode. (***Default = Disabled***)

6.2.2.2. Active HIPS Rules

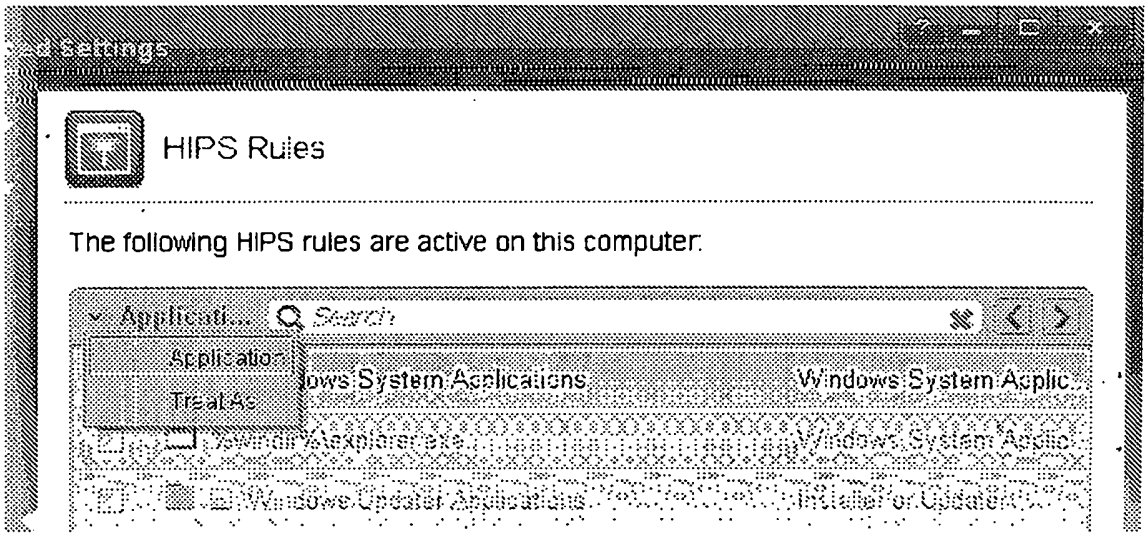
The HIPS rules tab lists the different groups of applications installed in your system and the Rulesets applied to them. You can change the ruleset applied to selected applications and also create custom rulesets to be applied to selected applications.



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

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

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



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

General Navigation:

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

- **Add** - Allows the user to Add a new Application to the list then create it's ruleset. See the section 'Creating or Modifying a HIPS Ruleset'.
- **Edit** - Allows the user to modify the HIPS rule of the selected application. See the section 'Creating or Modifying a HIPS Ruleset'.
- **Remove** - Deletes the selected ruleset.

Note: You cannot remove individual applications from a file group using this interface - you must use the 'File Groups' interface to do this.

- **Purge** - Runs a system check to verify that all the applications for which rulesets are listed are actually installed on the host machine at the path specified. If not, the rule is removed, or 'purged', from the list.

Users can re-order the priority of rules by simply selecting the application name or file group name in question, clicking the handle at the bottom center and selecting 'Move Up' or 'Move Down' from the options. To alter the priority of applications that belong to a file group, you must use the 'File Groups' interface.

Creating or Modifying a HIPS Ruleset

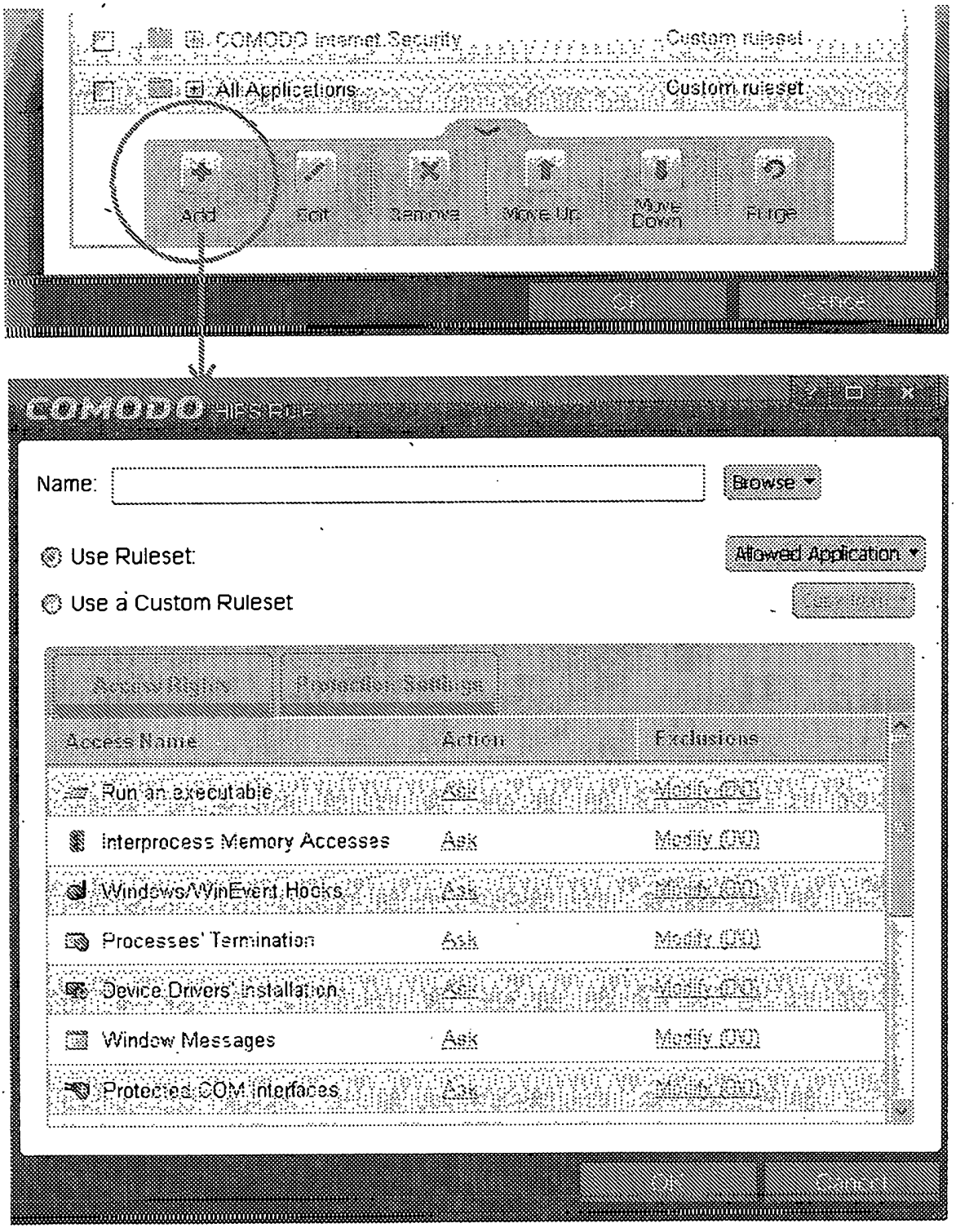
To begin defining an application's HIPS Ruleset

1. Select the application or file group that you wish the ruleset to apply to.

2. Configure the ruleset for this application.

Step 1 - Select the application or file group that you wish the ruleset to apply to

If you wish to define a rule for a new application (i.e. one that is not already listed), click the handle from the HIPS Rules pane and select 'ADD'. This brings up the 'HIPS Rule' interface as shown below.

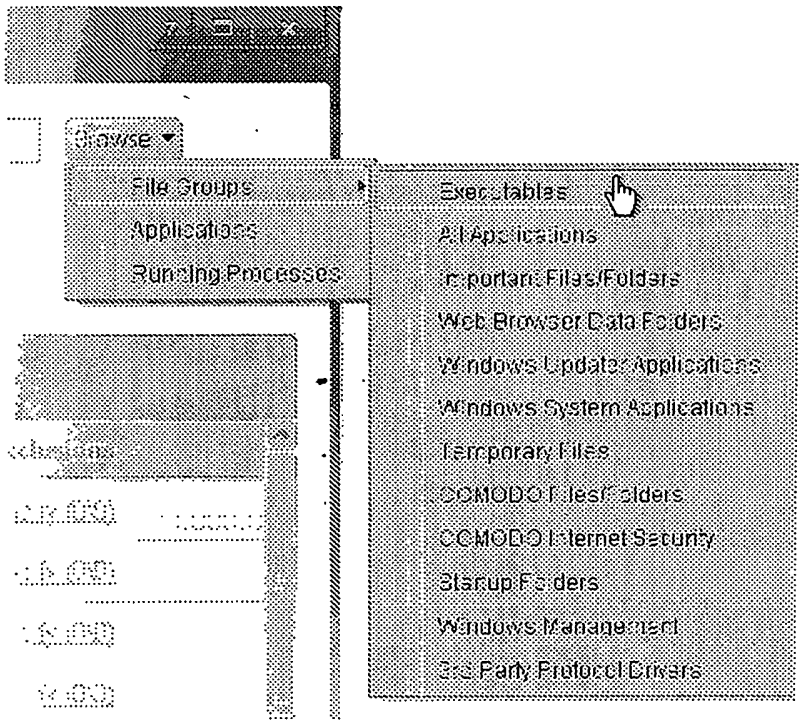


Because you are defining the HIPS rule settings for a new application, you can notice that the 'Name' box is blank. (If you were editing an existing rule instead, then this interface would show that application's name with installation path or application group's name.)

- Click 'Browse' to begin.

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

1. **File Groups** - Choosing this option allows you to create a HIPS ruleset for a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc - each of which provide a fast and convenient way to apply a generic ruleset to important files and folders.

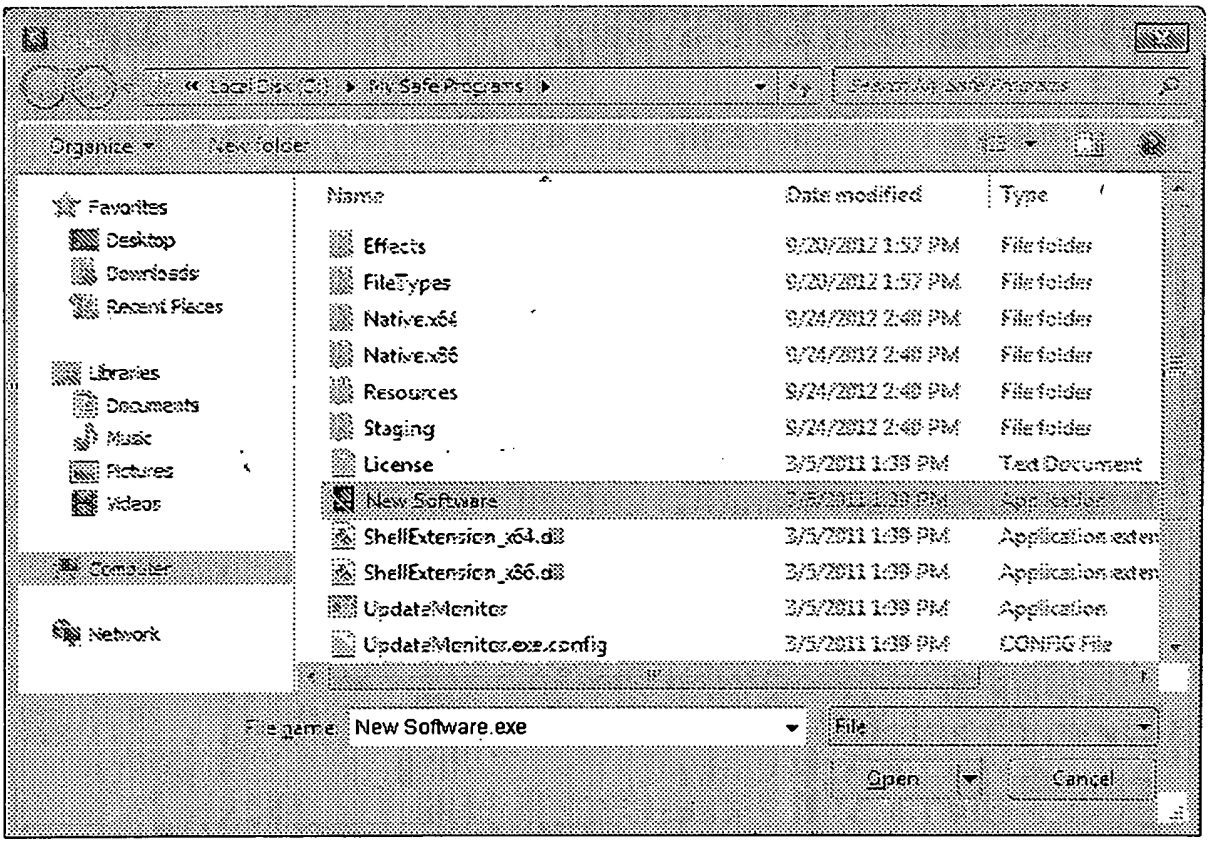


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

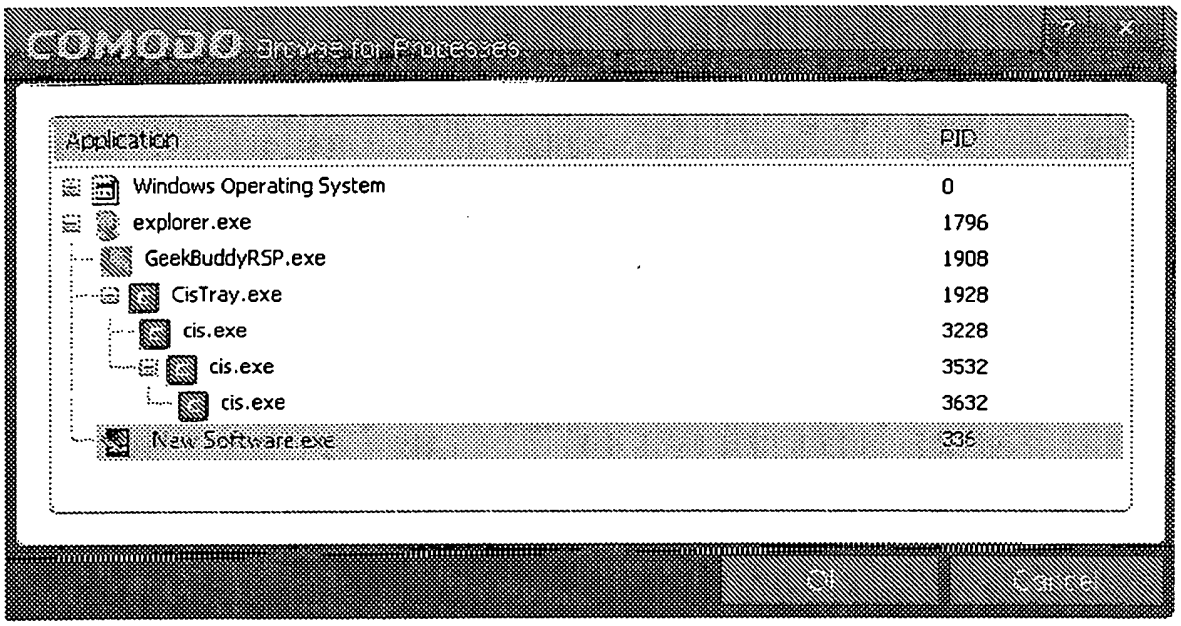
The ' File Groups interface can be accessed by the following method:

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

2. **Applications** - This option is the easiest for most users and simply allows you to browse to the location of the application for which you want to deploy the ruleset.



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



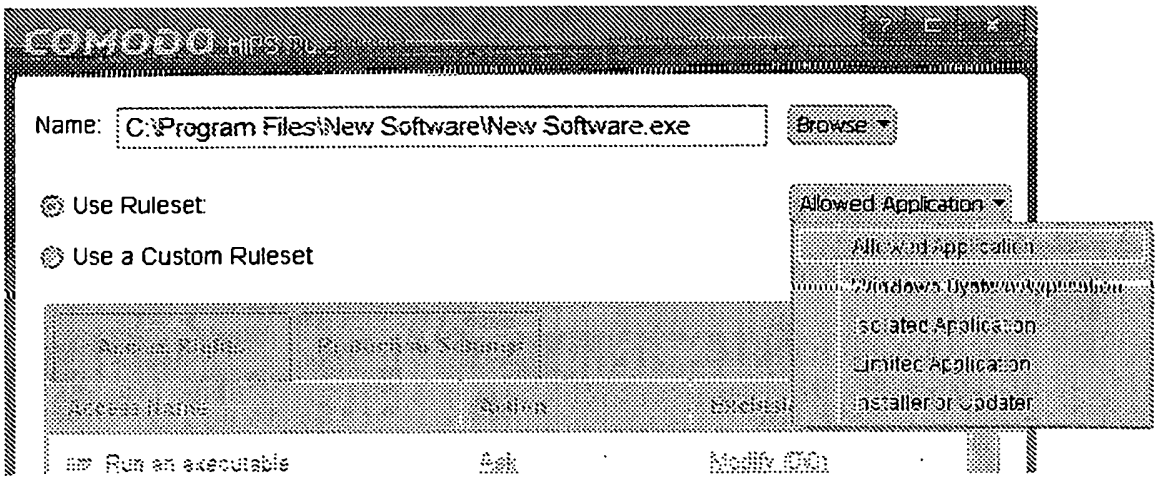
Having selected the individual application, running process or file group, the next stage is to Configure the rules for this ruleset.

Step 2 - Configure the HIPS Ruleset for this application

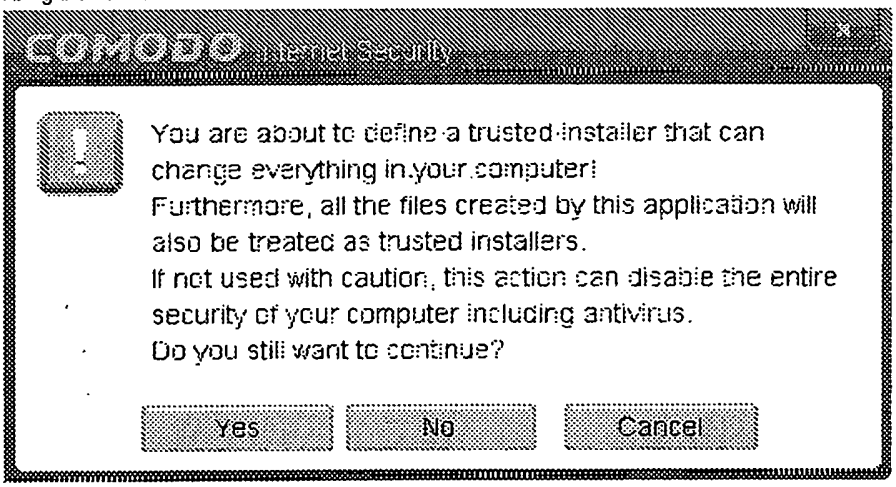
There are two broad options available for selecting a ruleset that applies to an application - Use Ruleset or Use a Custom Ruleset.

1. **Use Ruleset** - Selecting this option allows the user to quickly deploy an existing HIPS ruleset on to the target

application. Choose the ruleset you wish to use from the drop down menu. In the example below, we have chosen 'Allowed Application'. The name of the ruleset you choose is displayed in the 'Treat As' column for that application in the HIPS Rules interface ***(Default = enabled)***.



Note on 'Installer or Updater' Rule : Applying the Predefined Ruleset 'Installer or Updater' for an application defines it as a trusted installer and all files created by the application will also be considered as trusted files. Some applications may have hidden code that could impair the security of your computer if allowed to create files of their own. Comodo advises you to use this Predefined Ruleset - 'Installer or Updater' with caution. On applying this ruleset to any application, an alert dialog will be displayed, describing the risks involved.

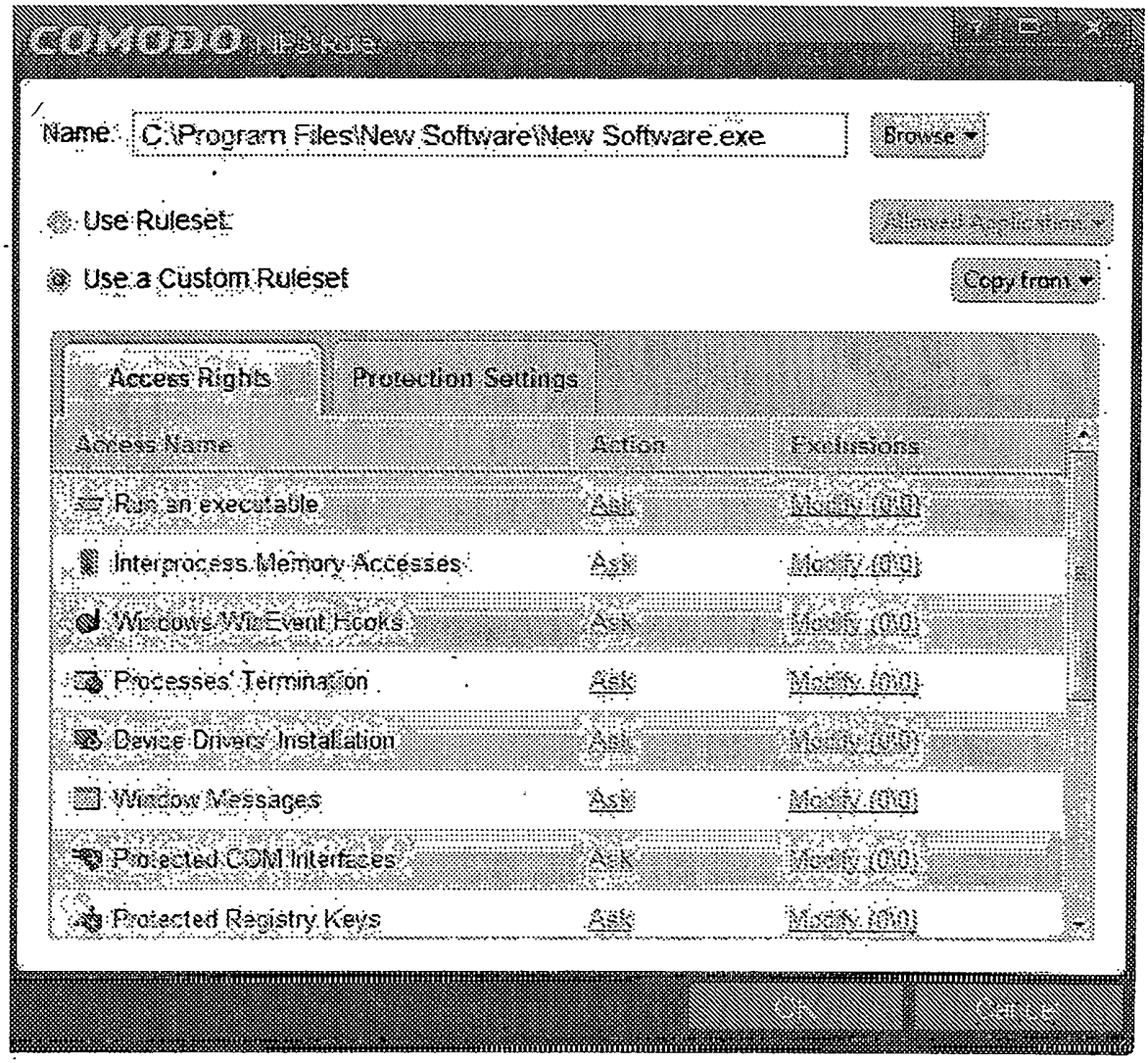


General Note: Predefined Rulesets, once chosen, cannot be modified directly from this interface - they can only be modified and defined using the 'Rulesets' interface. If you require the ability to add or modify settings for an specific application then you are effectively creating a new, custom ruleset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

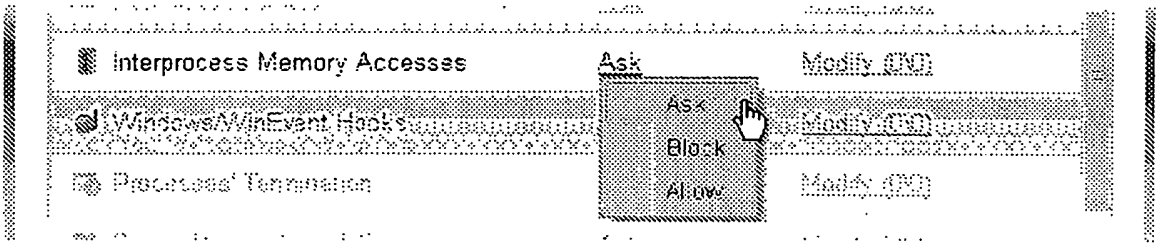
2. **Use a Custom Ruleset** - designed for more experienced users, the 'Custom Ruleset' option enables full control over the configuration specific security ruleset and the parameters of each rule within that ruleset. The Custom ruleset has two main configuration areas - Access Rights and Protection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

   In simplistic terms 'Access Rights' determine what the application *can do* to other processes and objects whereas 'Protection Settings' determine what the application *can have done to it* by other processes.

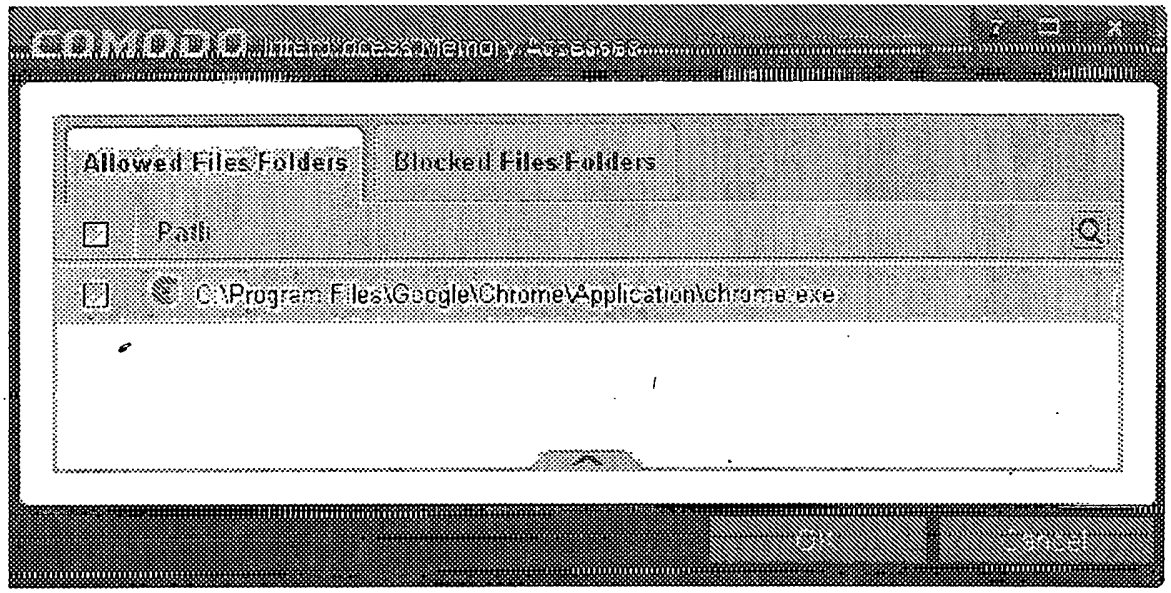
   i. **Access Rights** - The Process Access Rights tab allows you to determine what activities the applications in your custom ruleset are allowed to execute. These activities are called 'Access Names'.



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



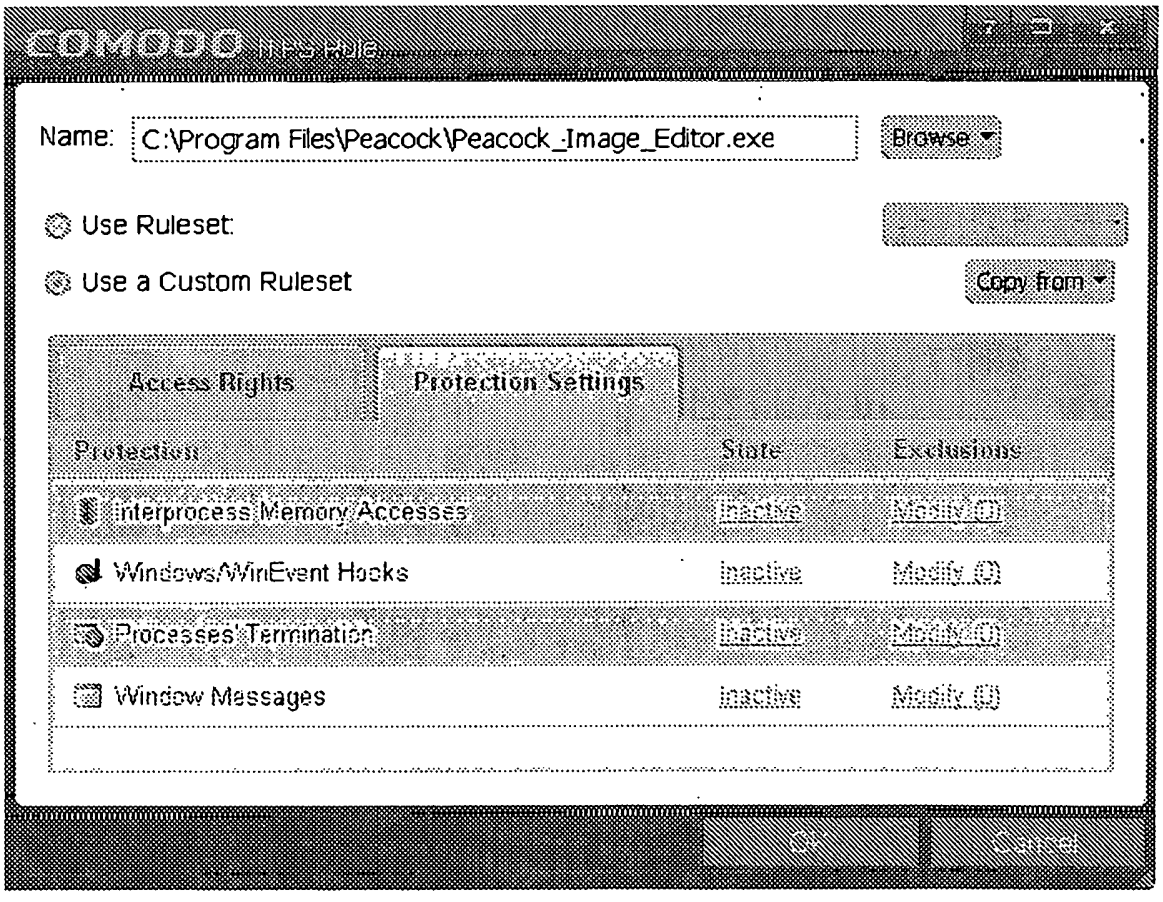
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.



Clicking the handle and selecting 'Add' allows you to choose which applications or file groups you wish this exception to apply to. (click here for an explanation of available options).

In the example above, the default action for '*Interprocess Memory Access*' is '*Ask*'. This means HIPS will generate an alert asking your permission if 'New Software.exe' tries to modify the memory space of any other program. Clicking 'Modify' then adding 'opera.exe' to the 'Allowed Applications' tab creates an exception to this rule. New Software.exe can now modify the memory space of opera.exe.

ii. **Protection Settings** - Protection Settings determine how protected the application or file group in your ruleset is *against* activities by other processes. These protections are called 'Protection Types'.



- Select 'Active' to enable monitoring and protect the application or file group against the process listed in the 'Protection Type' column. Select 'Inactive' to disable such protection.

Click here to view a list of definitions of the 'Protection Types' listed above and the implications of activating each setting.

Exceptions to your choice of 'Active' or 'Inactive' can be specified in the application's Ruleset by clicking the 'Modify' link on the right.

3. Click 'OK' to confirm your settings.

6.2.2.3. HIPS Rule Sets

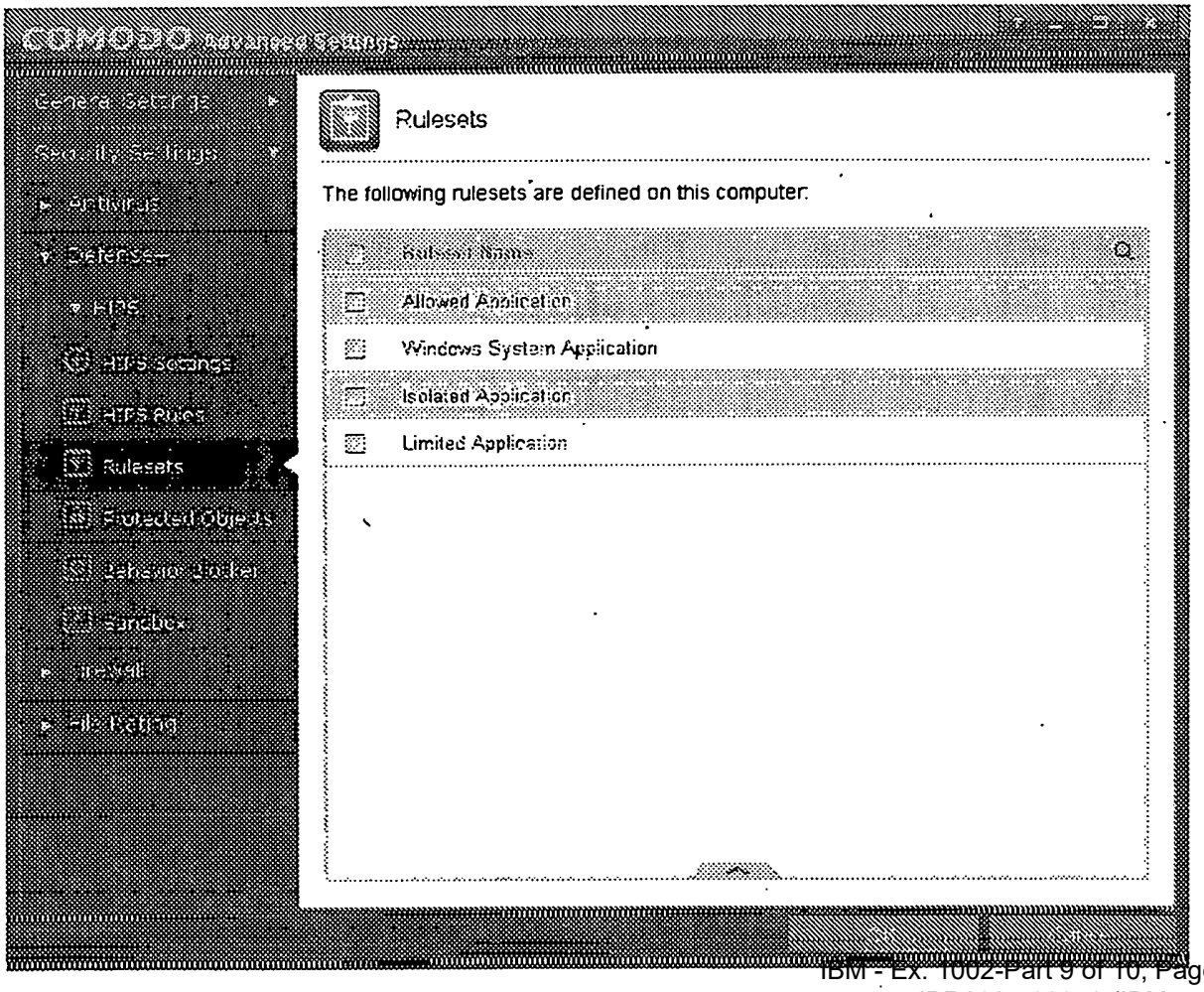
A Pre-defined ruleset is a set of access rights and protection settings that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined rulesets' is a set of rulesets that concern an application's access rights to memory, other programs, the registry etc.

Note: This section is for advanced and experienced users. If you are a novice user to Comodo Internet Security, we advise you first read the Active HIPS Rules section in this help guide if you have not already done so.

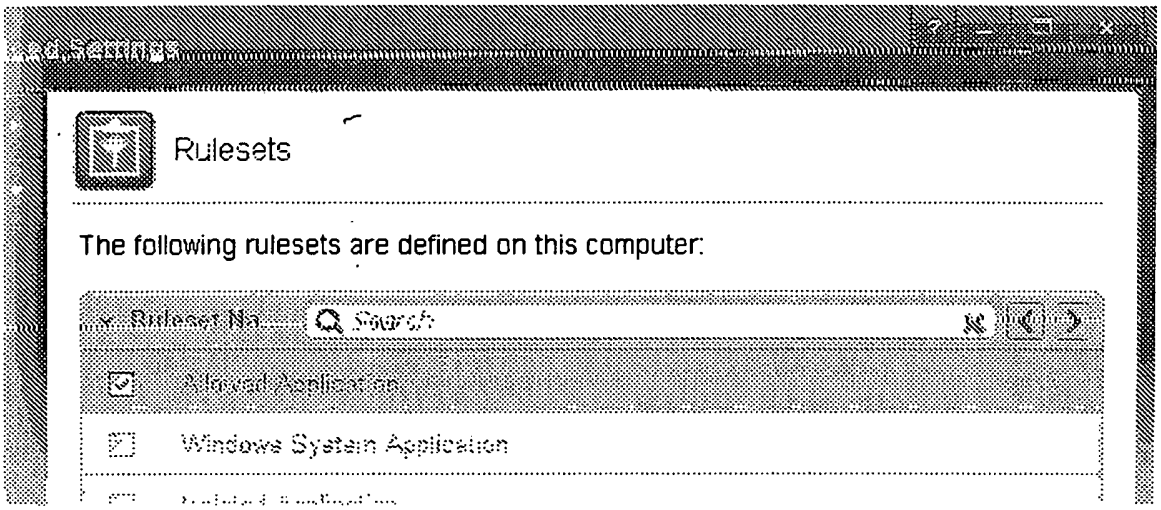
Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Internet Security contains a selection of rulesets according to broad application categories. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application. Users can, of course, modify these predefined rulesets to suit their environment and requirements.

To configure this category

- Navigate to: Advanced Tasks > Security Settings >Defense+ > HIPS > Rulesets. There are four default Rulesets listed under the 'Rules' column.



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



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

To view or edit an existing predefined ruleset

- Double click on the Ruleset in the list .

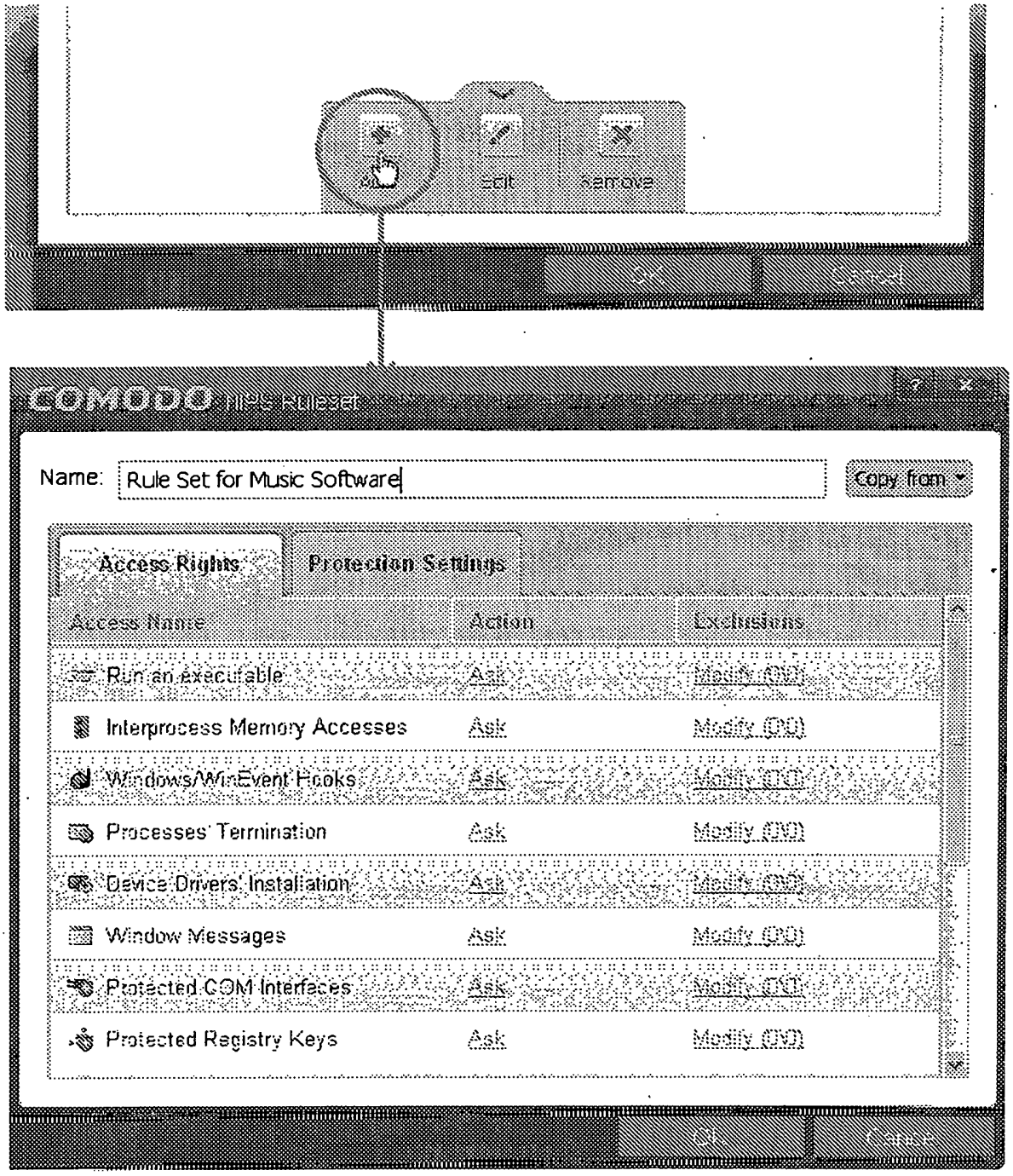
  or

- Select the Ruleset, click the handle at the bottom of the interface and choose 'Edit' from the options.

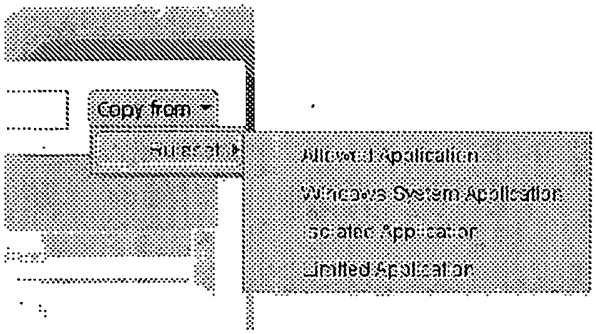
From here, you can modify a ruleset and, if desired, make changes to its 'Access Rights' and 'Protection Settings'. Any changes you make here are automatically rolled out to all applications that are currently applied with the ruleset.

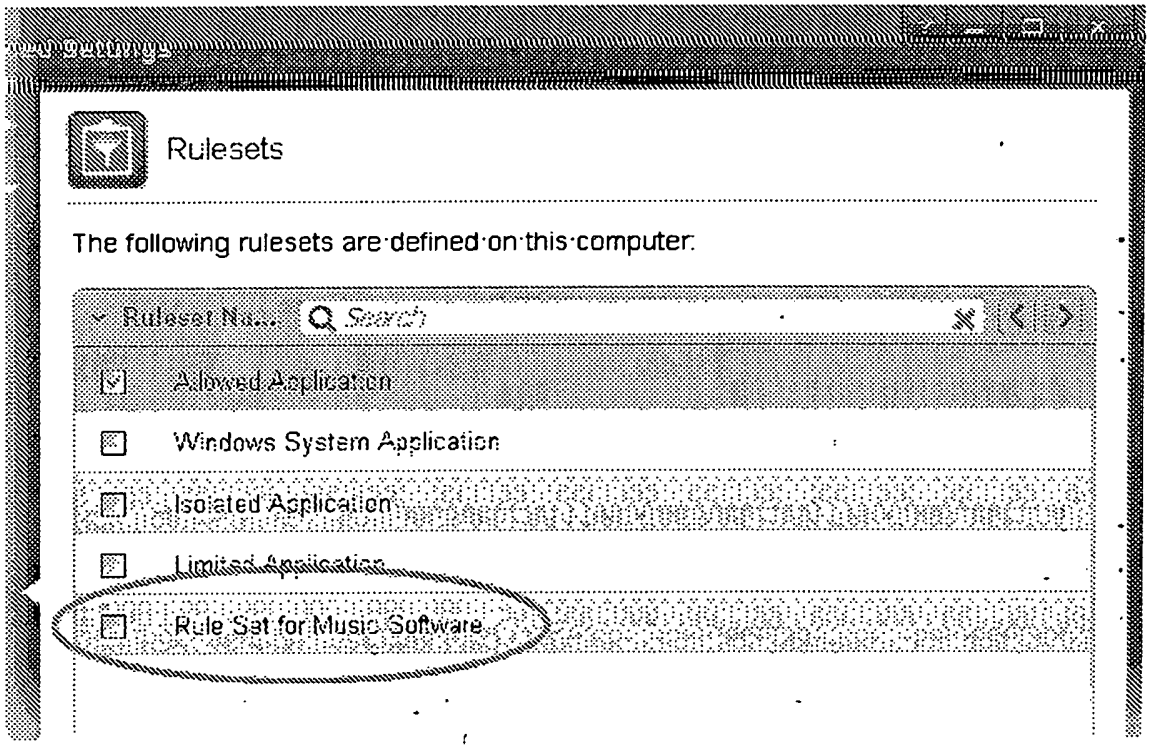
To create a new predefined ruleset

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


Edit
Remove
COMODO HIPS Helper
Name:
Rule Set for Music Software
Copy from
Access Rights
Protection Settings
Access Name
Action
Exclusions
Run an executable
Ask
Modify (0/0)
Interprocess Memory Accesses
Ask
Modify (0/0)
Windows/WinEvent Hooks
Ask
Modify (0/0)
Processes' Termination
Ask
Modify (0/0)
Device Drivers' Installation
Ask
Modify (0/0)
Window Messages
Ask
Modify (0/0)
Protected COM Interfaces
Ask
Modify (0/0)
Protected Registry Keys
Ask
Modify (0/0)

- Enter a name for the new ruleset.
- To copy the Access Rights and Protection Settings from another pre-existing ruleset, click 'Copy From' and select the ruleset from the drop-down
- To customize the Access Rights and Protection Settings as per the requirements of this new rule set, follow the procedure explained in the section Use a Custom Ruleset.
- Click OK to save the new ruleset.



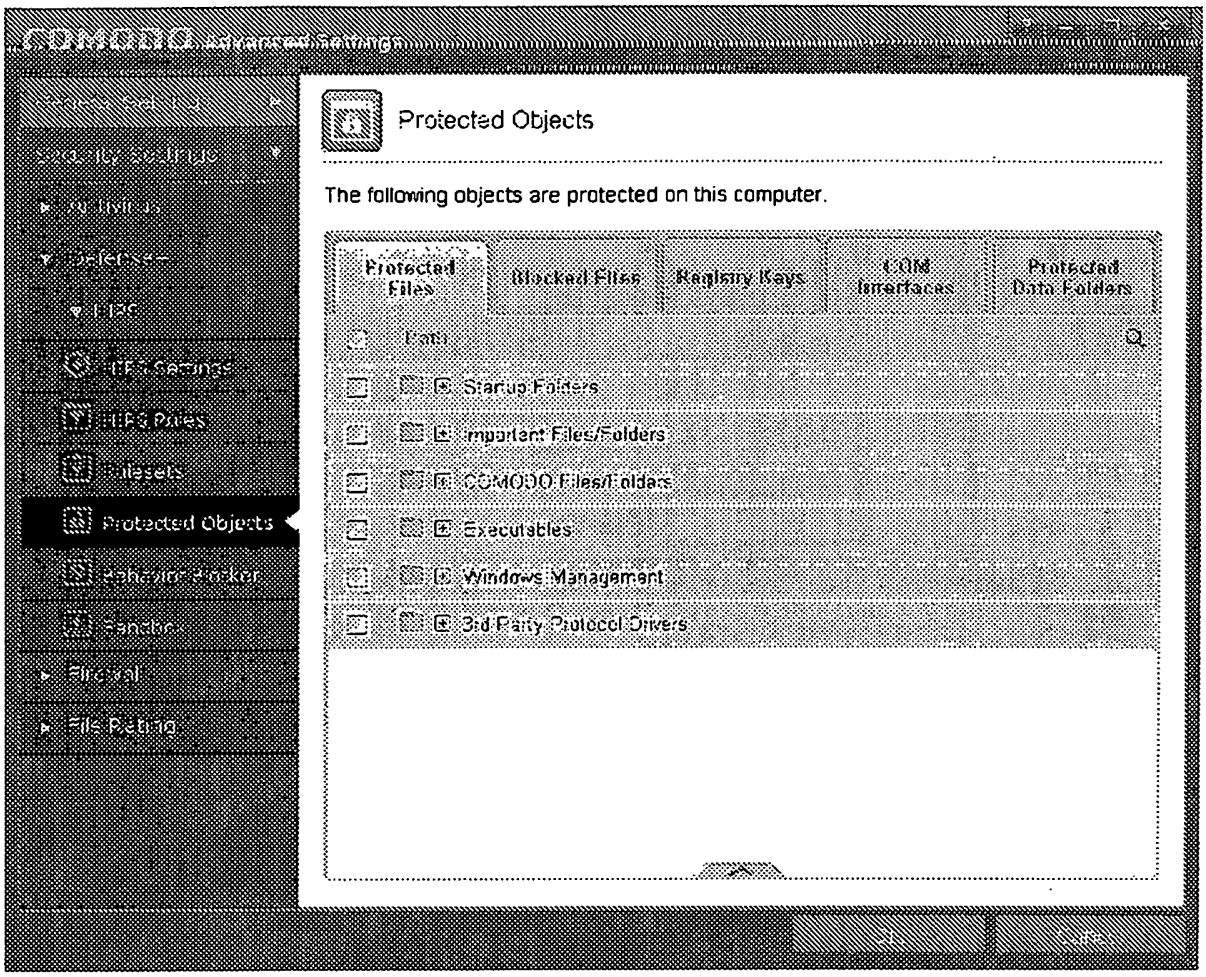


Once created, your ruleset is available for deployment onto specific application or file groups via the Active HIPS Rules interface.

6.2.2.4. Protected Objects

The Protected Objects panel allows you to protect specific files and folders, system critical registry keys and COM interfaces against access or modification by unauthorized processes and services.

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

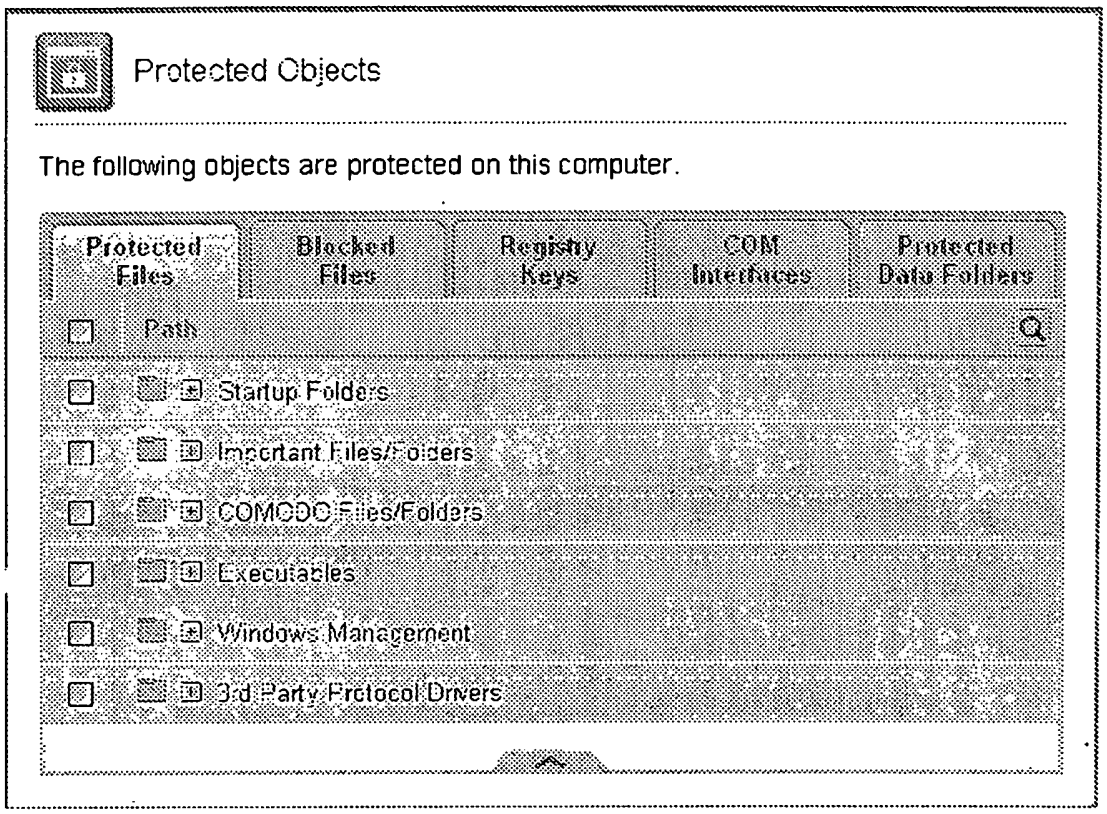


The panel has five tabs:

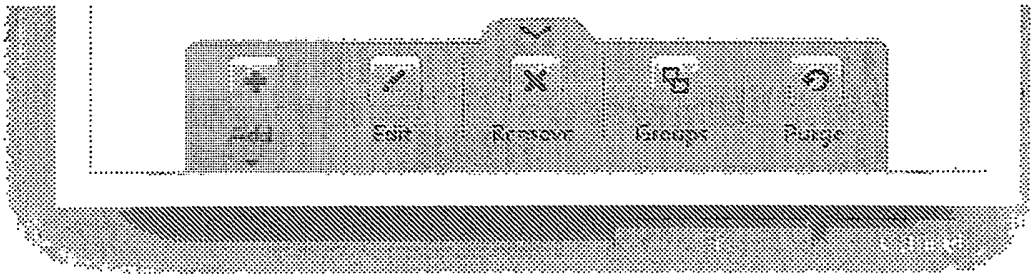
- Protected Files - Allows you to specify programs, applications and files that are to be protected from changes
- Blocked Files - Allows you to specify programs, applications and files that are to be blocked from execution and opening
- Registry Keys - Allows you to specify registry keys that are to be protected from changes
- COM Interfaces - Allows you to specify COM interfaces that are to be protected from changes
- Protected Data Folders - Allows you to specify folders containing data files that are to be protected from changes

6.2.2.4.1. Protected Files

The Protected Files tab displays a list of files and file groups that are protected from access by other programs, especially malicious programs such as virus, Trojans and spyware. It is also useful for safeguarding very valuable files (spreadsheets, databases, documents) by denying anyone and any program the ability to modify the file - avoiding the possibility of accidental or deliberate sabotage. If a file is 'Protected' it can still be accessed and read by users, but not altered. A good example of a file that ought to be protected is your 'hosts' file (c:\windows\system32\drivers\etc\hosts). Placing this in the 'Protected Files and Folders' area would allow web browsers to access and read from the file as per normal. However, should any process attempt to modify it then Comodo Internet Security blocks this attempt and produce a 'Protected File Access' pop-up alert.

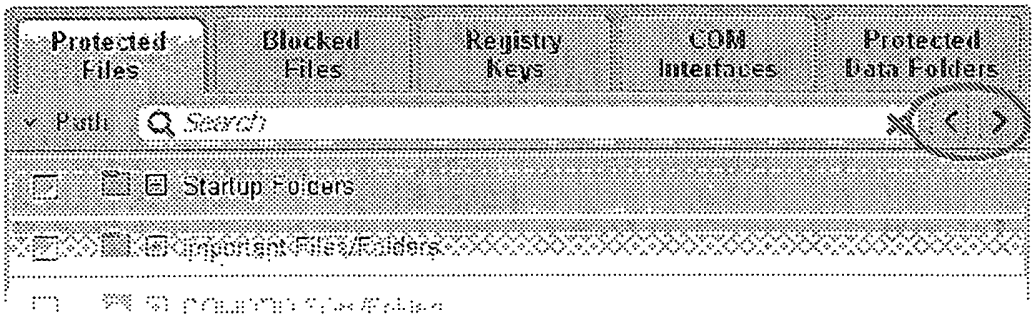


Clicking the handle at the bottom of the interface opens an options panel with the following options:

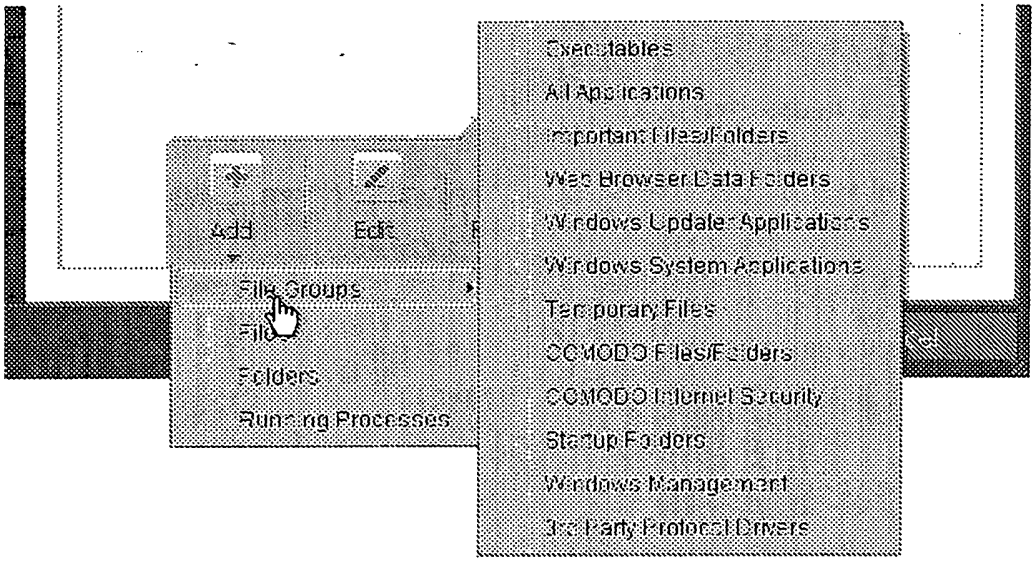


- Add - Allows you to add individual files, programs, applications to Protected Files.
- Edit - Allows you to edit the path of the file or group of a selected item in the Protected Files interface.
- Remove - Deletes the currently highlighted file or file group.
- Groups - Opens the Manage Groups interface that allows you to edit pre-defined file groups and define new file groups for inclusion in Protected Files list
- **Purge** - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

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



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



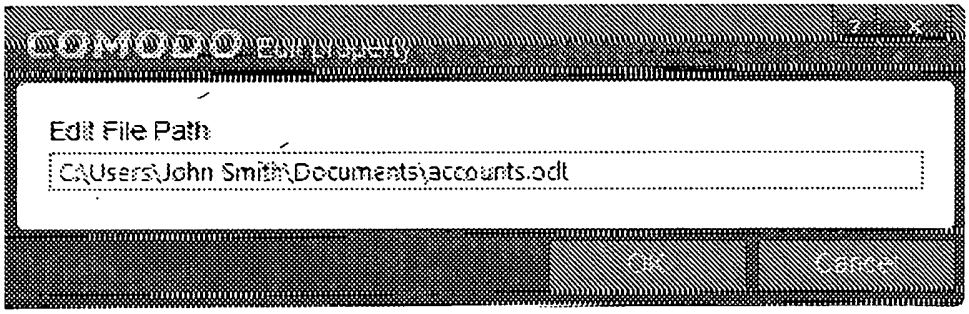
- Click the handle from the bottom center and select 'Add'.

You can add the files by following methods:

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

To edit an item in the Protected Files list

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



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

To delete an item from Protected Files list

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

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

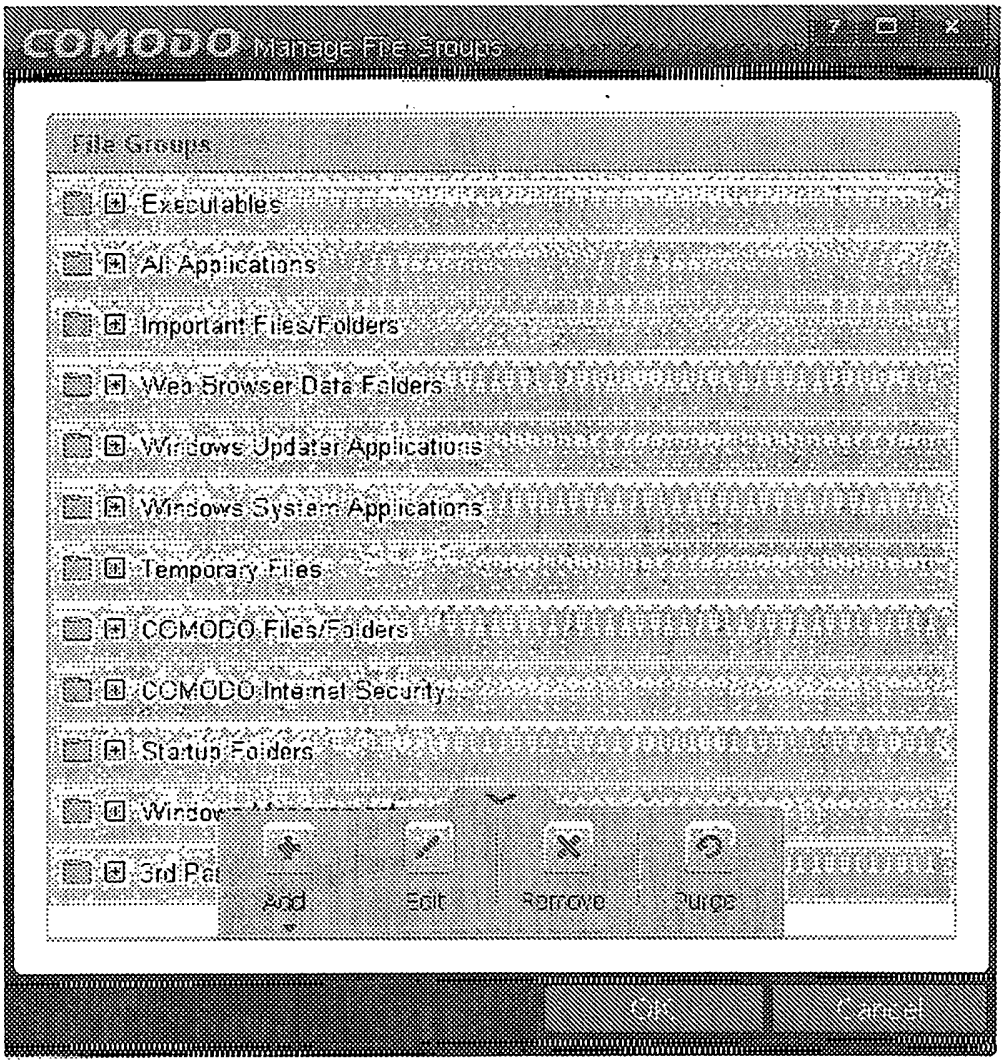
File Groups

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

To open the Manage File Groups interface

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

The Manage File Groups interface will open.

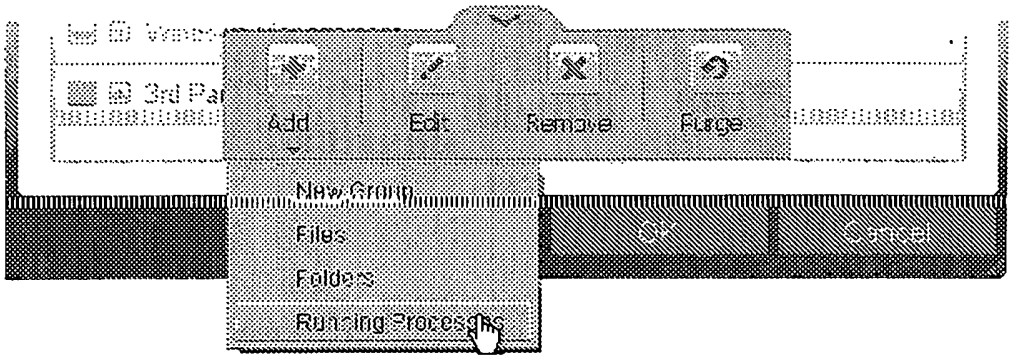


This interface allows you to

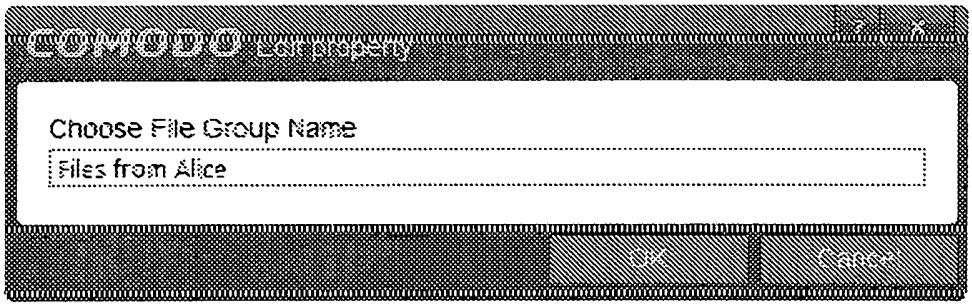
- Create a new File Group
- Edit the names of an Existing File Group
- Add a file to an existing file group
- Remove existing file group(s) or individual file(s) from existing group

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

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



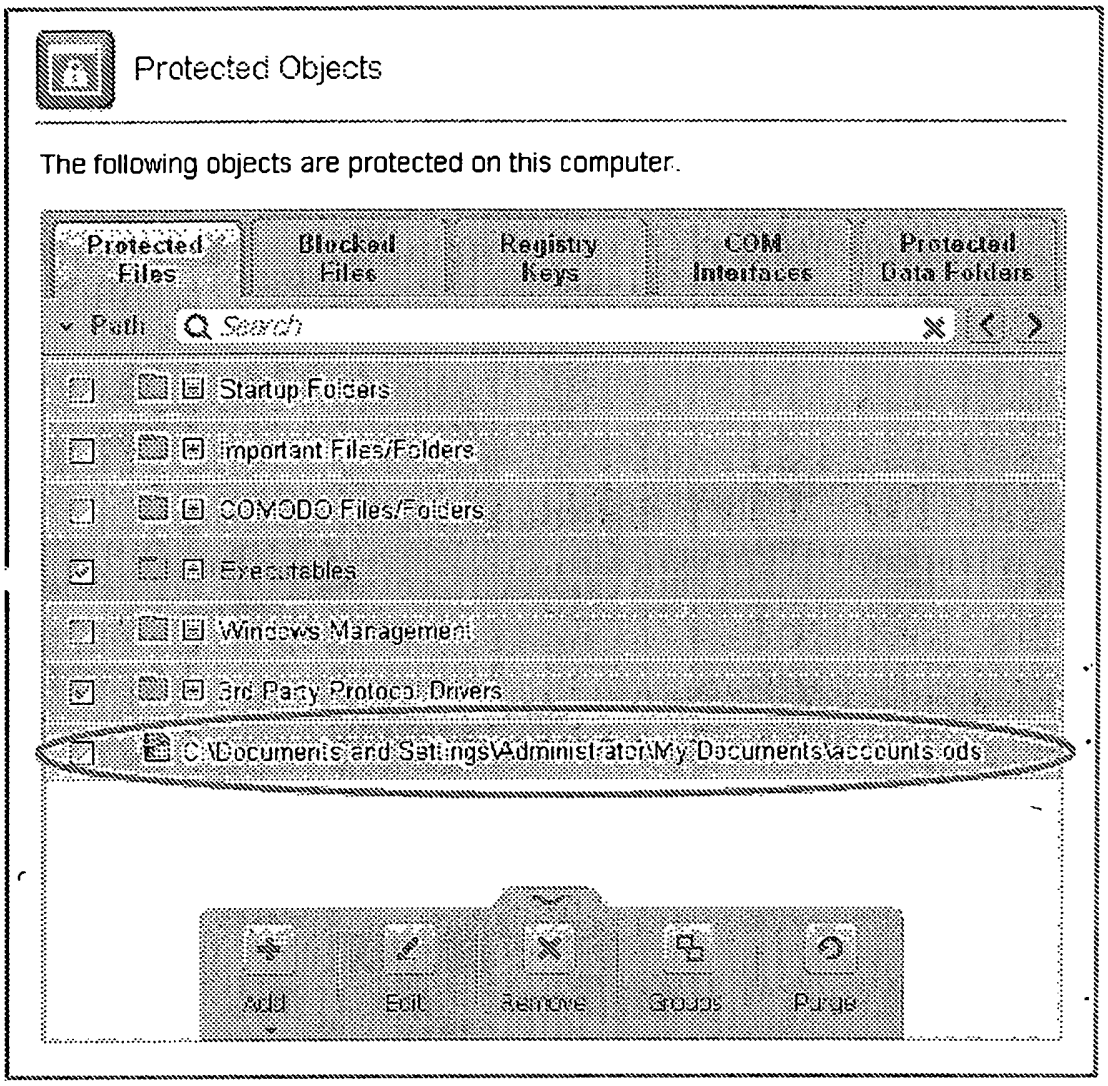
- **Add files to a group** - Select the Group, click the handle and select Add. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes

- To edit an existing group, select the group, click the handle and choose Edit. Edit the name of the group in the Edit Property dialog
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the file to be removed, click the handle and choose 'Remove'.

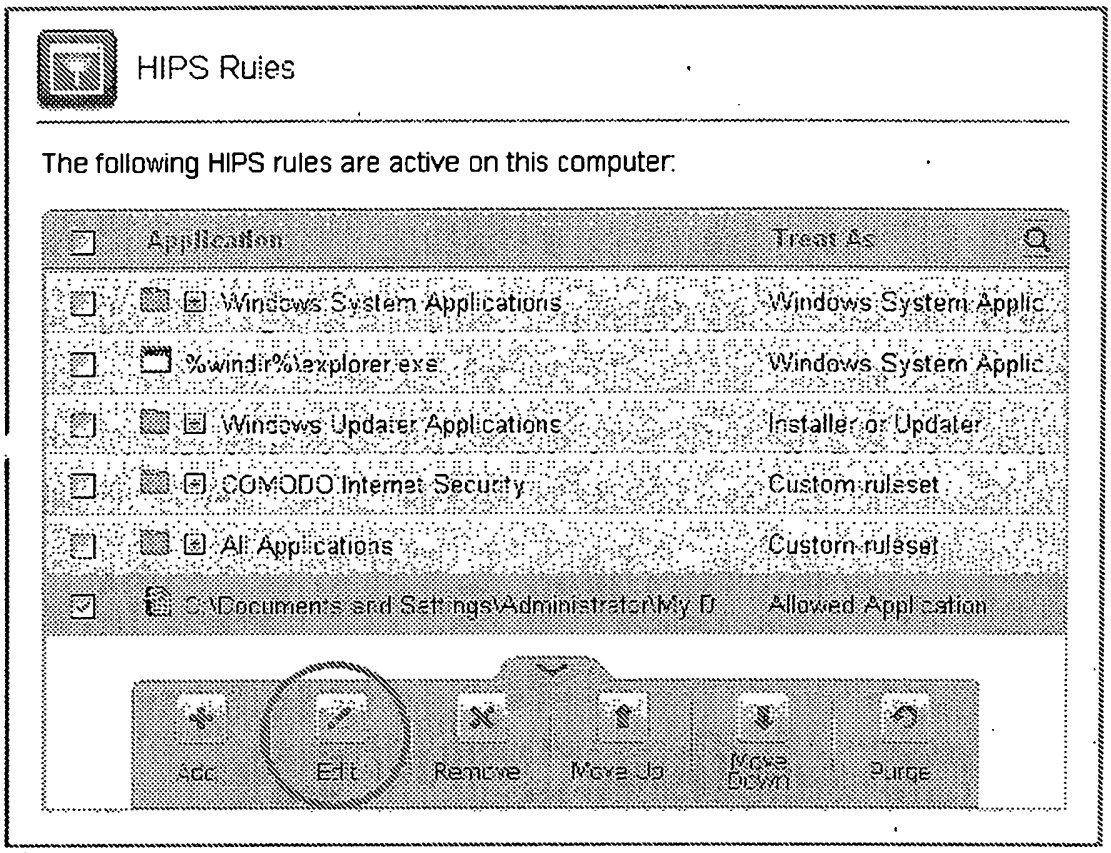
Exceptions

Users can choose to selectively allow another application (or file group) to modify a protected file by affording the appropriate Access Right in 'Active HIPS Rules' interface. A simplistic example would be the imaginary file 'Accounts.ods'. You would want the Open Office Calc program to be able to modify this file as you are working on it, but you would not want it to be accessed by a potential malicious program. You would first add the spreadsheet to the 'Protected Files' area. Once added to 'Protected Files', you would go into 'Active HIPS Rules' and create an exception for 'scalc' so that it alone could modify 'Accounts.ods'.

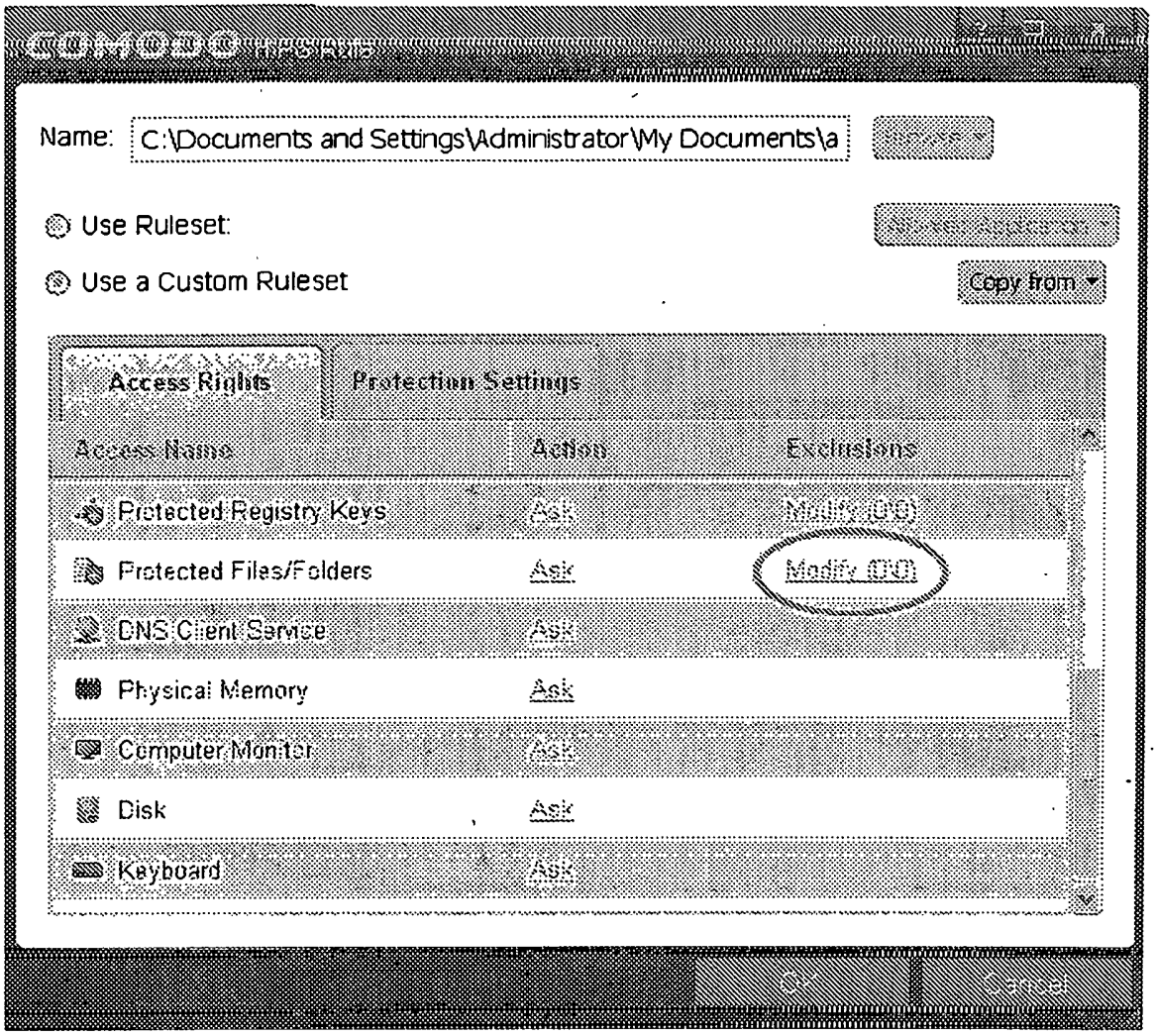
- First add Accounts.odt to Protected Files area.



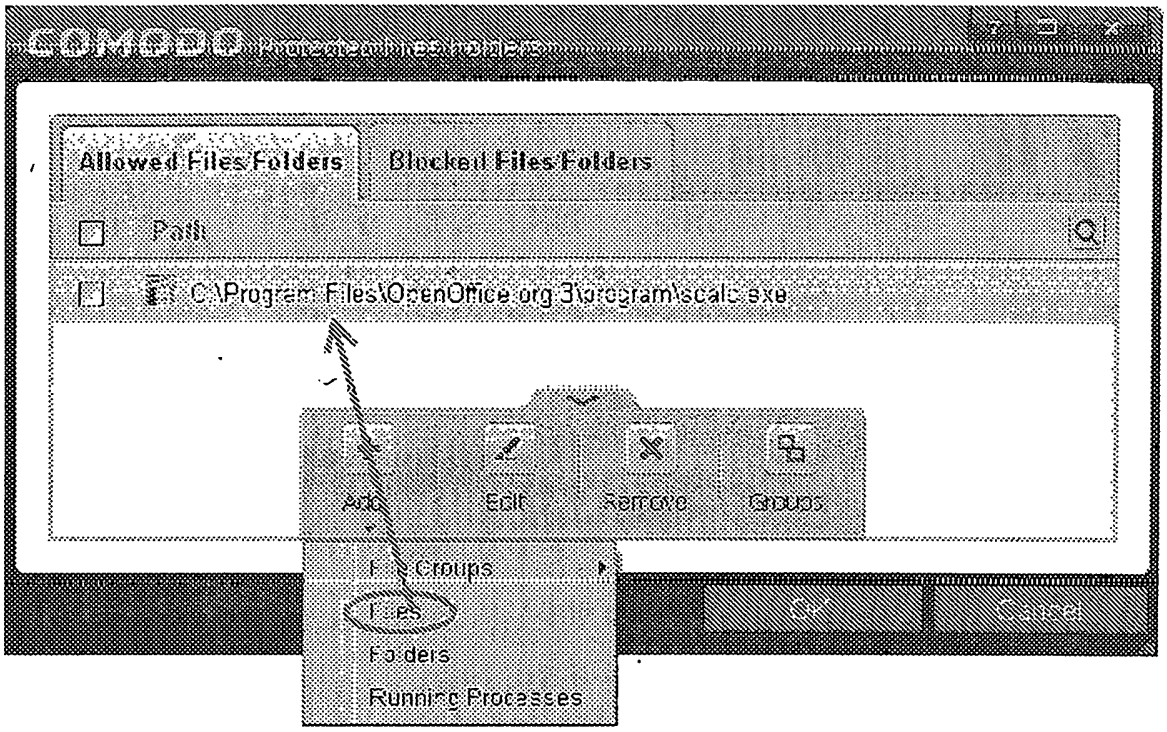
- Then go to HIPS Rules interface and add it to the list of applications. Click the handle at the bottom and choose 'Edit' after selecting the checkbox beside it.



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



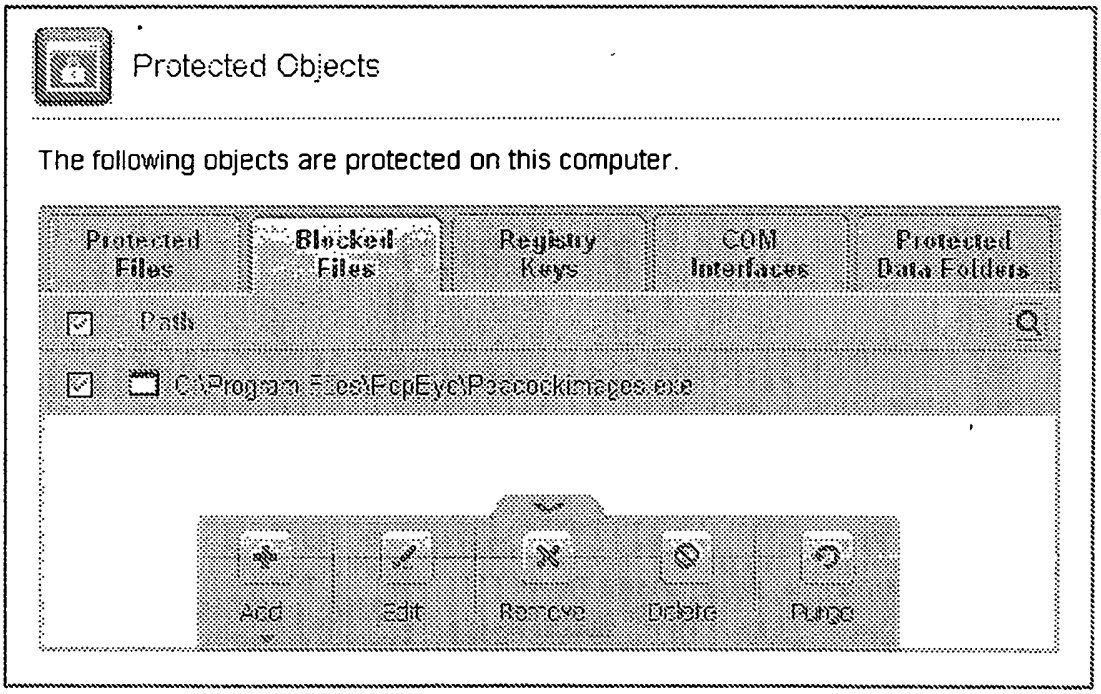
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scaic.exe as exceptions to the 'Ask' or 'Block' rule in the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



Another example of where protected files should be given selective access is the Windows system directory at 'c:\windows\system32'. Files in this folder should be off-limits to modification by anything except certain, Trusted, applications like Windows Updater Applications. In this case, you would add the directory c:\windows\system32* to the 'Protected Files area (* = all files in this directory). Next go to 'HIPS Rules', locate the file group 'Windows Updater Applications' in the list and follow the same process outlined above to create an exception for that group of executables.

6.2.2.4.2. Blocked Files

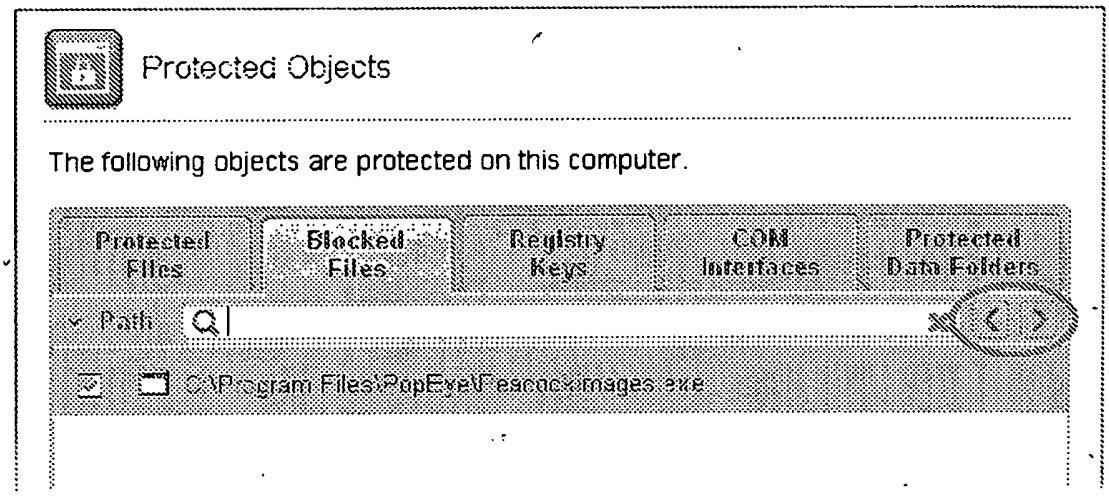
Defense+ allows you to lock-down files and folders by completely denying all access rights to them from other processes or users - effectively cutting it off from the rest of your system. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files that are placed in 'Protected Files', users cannot selectively allow any process access to a blocked file.



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

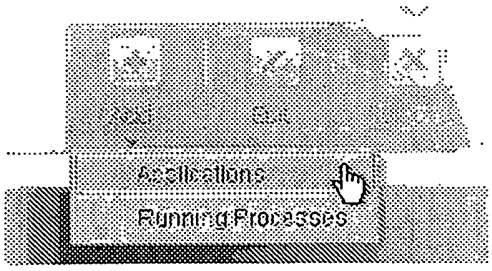
- Add - Allows you to add individual files, programs, applications to Blocked Files.
- Edit - Allows you to edit the path of the file.
- Remove - Releases the currently highlighted file from the blocked files list.
- Delete - Deletes the highlighted file from your computer
- Purge - Runs a system check to verify that all the files listed are actually installed on the host machine at the path specified. If not, the file or the file group is removed, or 'purged', from the list.

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



To manually add an individual file or application

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

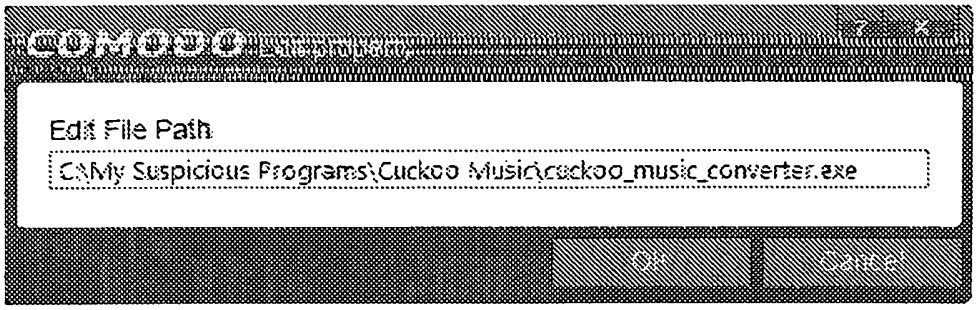


You can add the files by following methods:

- Selecting from currently running Processes
- Browsing to File

To edit an item in the Blocked Files list

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



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

To release an item from Blocked Files list

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

The selected item will be removed from the Blocked Files list. CIS will not block the application or file from execution or opening then onwards.

To permanently delete a blocked file from your system

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

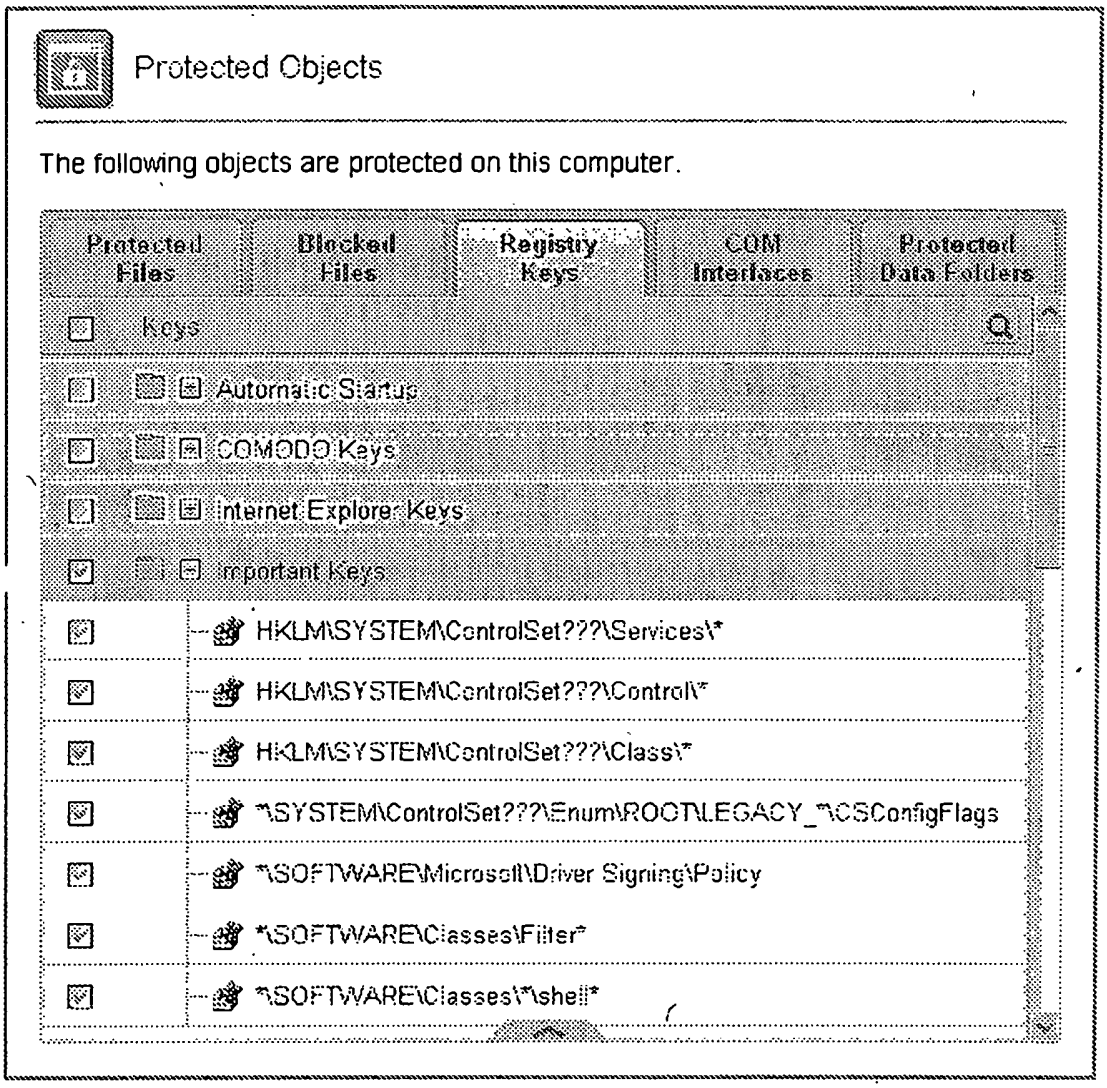
The selected item will be deleted from your computer immediately.

Warning: Deleting a file from from the Blocked Files interface permanently deletes the file from your system, rendering it inaccessible in future and it cannot be undone. Ensure that you have selected the correct file to be deleted before clicking 'Delete'.

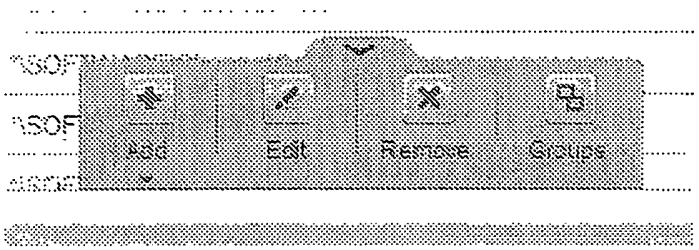
6.2.2.4.3. Protected Registry Keys

The 'Registry Keys' panel allows you to protect system critical registry keys against modification. Irreversible damage can be caused to your system if important registry keys are corrupted or modified in any way. It is essential that your registry keys are protected against any type of attack.

Click the 'Registry Keys' tab in the Protected Objects interface.



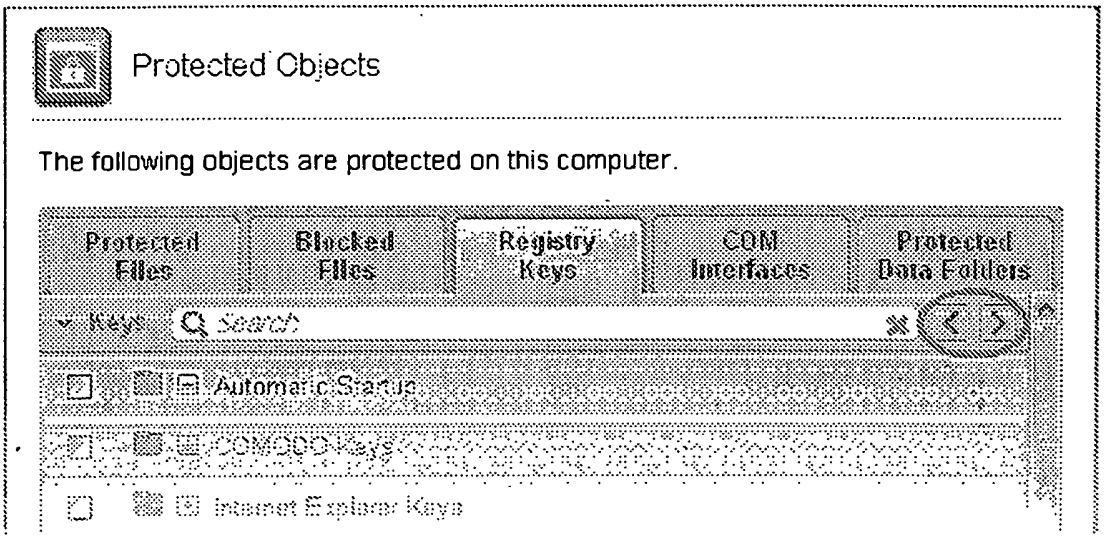
Clicking the handle at the bottom of the interface opens an options panel with the following options:



- Add - Allows you to add Registry groups or individual registry keys/entries to Registry Protection list.
- Edit - Allows you to edit the path of the Registry group or individual registry keys/entries of the selected item in the Registry Protection interface.
- Remove - Deletes the currently highlighted Registry group or individual registry key from the Registry Protection list.
- Groups - Opens the Manage Registry Groups interface that allows you to edit pre-defined Registry groups and define new Registry groups for inclusion in Registry Protection list.

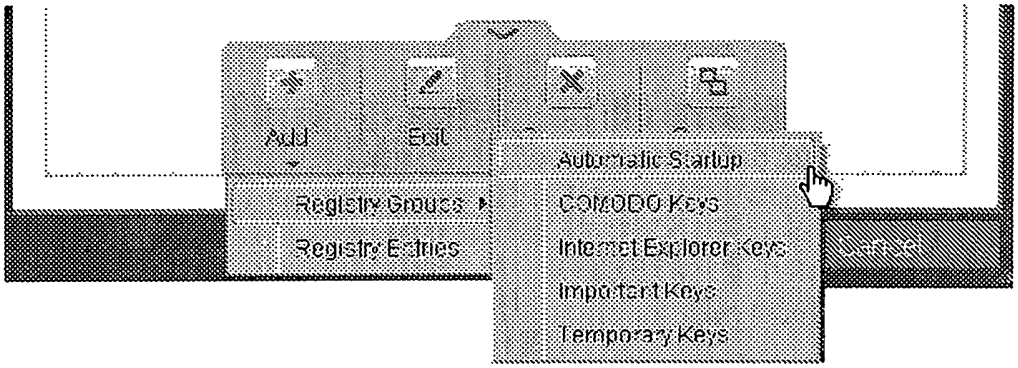
You can use the search option to find a specific registry key or group in the list by clicking the search icon at the far right in

the column header and entering the key/group name in full or part. You can navigate through the successive results by clicking the left and right arrows.



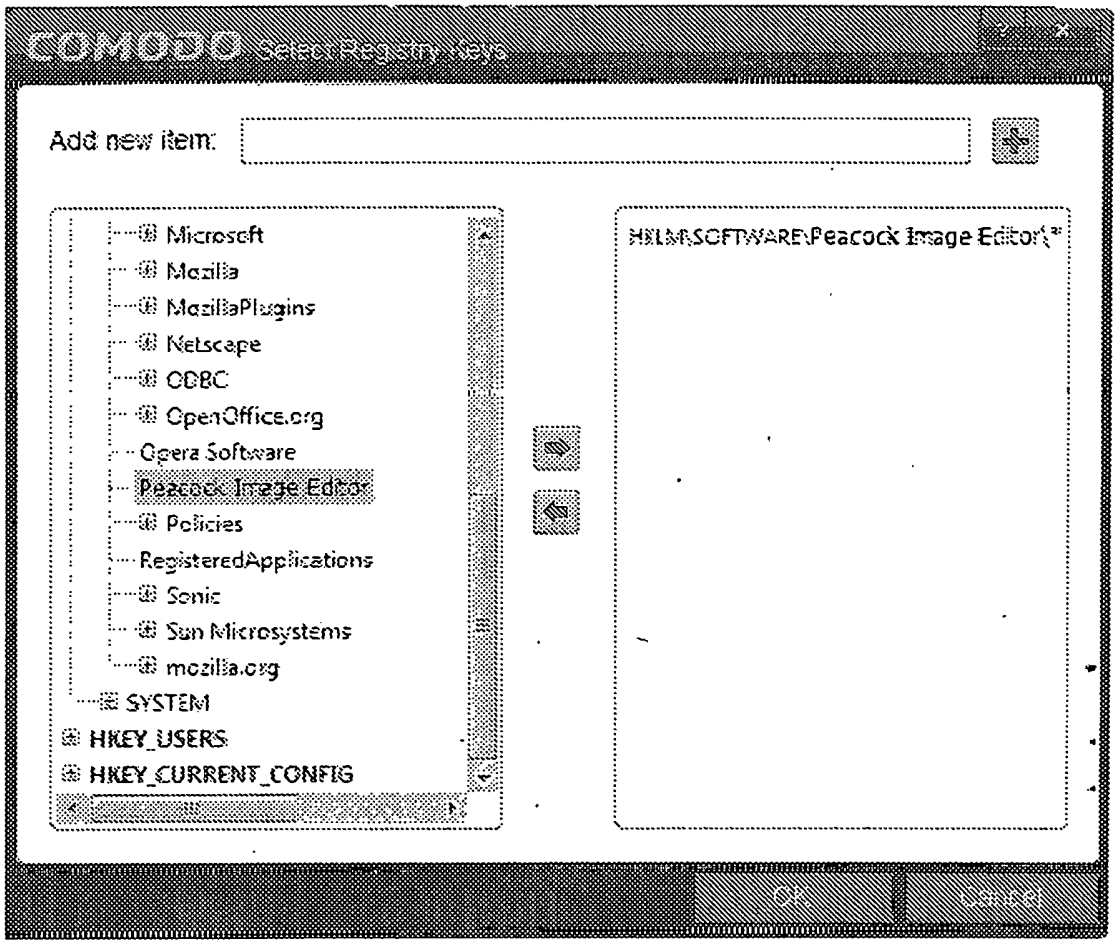
To manually add an individual Registry key or Registry Group

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



You can add the items by following methods:

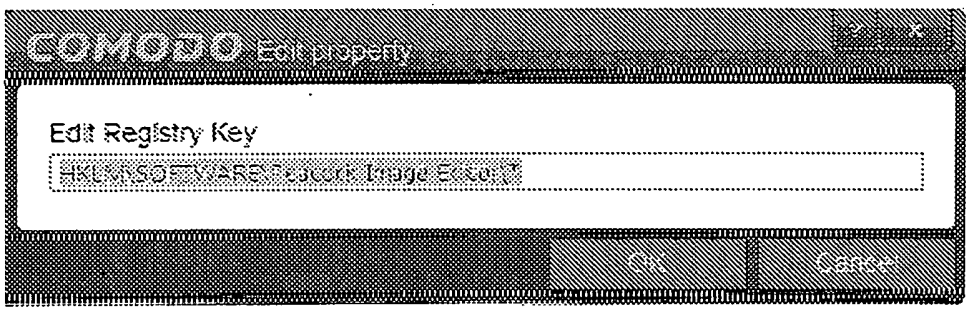
- **Adding Registry Groups** - Selecting Registry Groups allows you to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'. For explanations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



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

To edit an item in the Registry Protection list

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



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

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

To delete an item from Registry Protection list

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

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

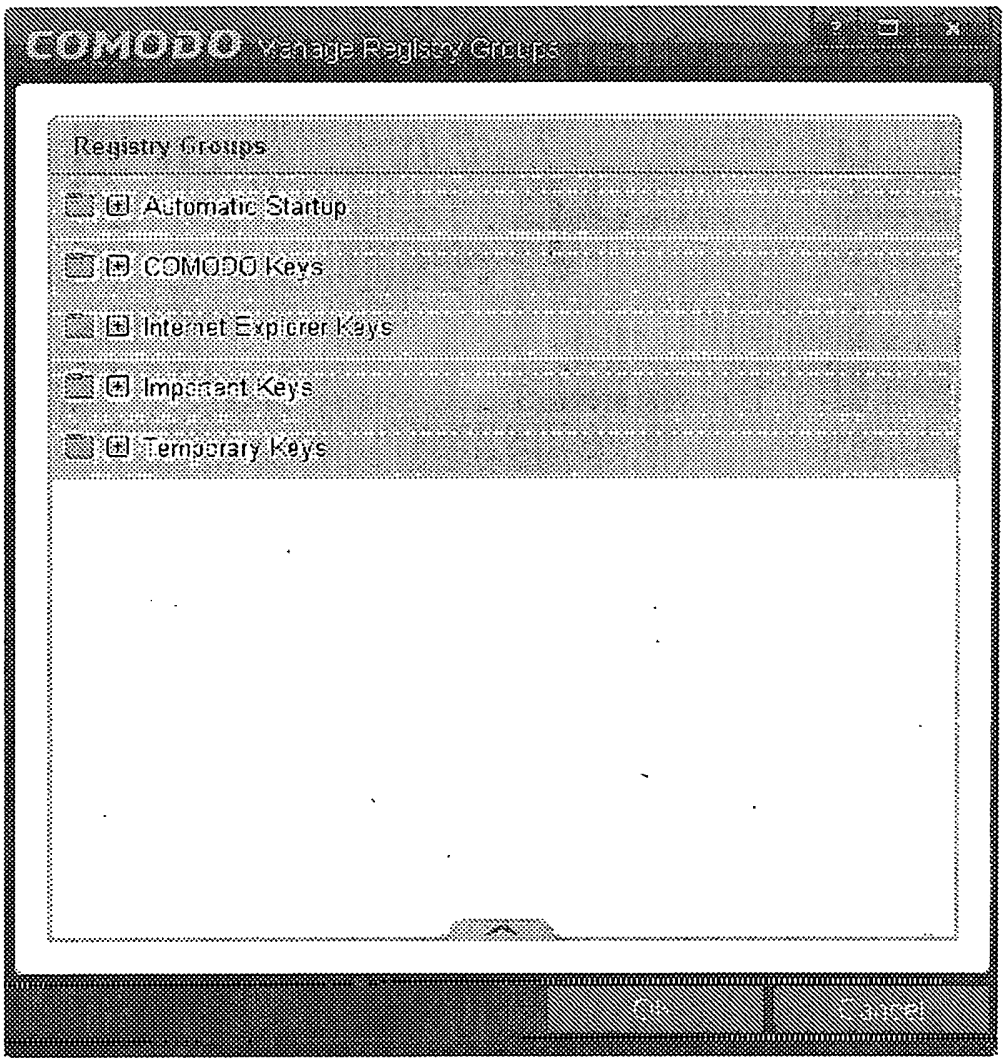
Registry Groups

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

To open the Manage Registry Groups interface

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

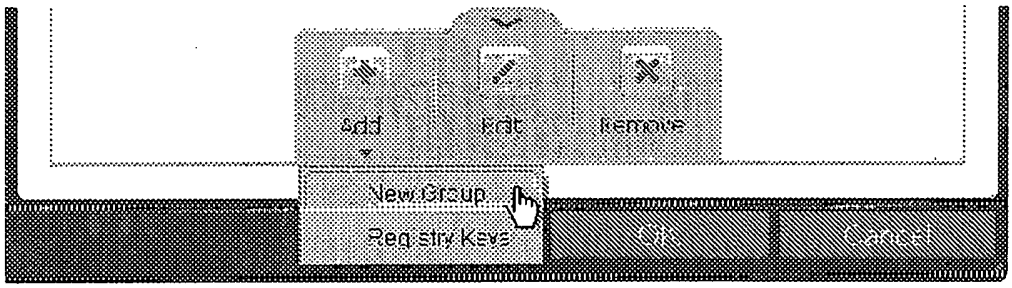
The 'Manage Registry Groups' interface will open.



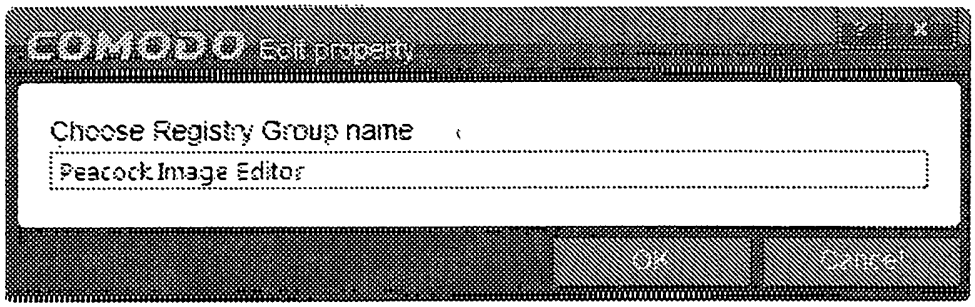
This interface allows you to

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

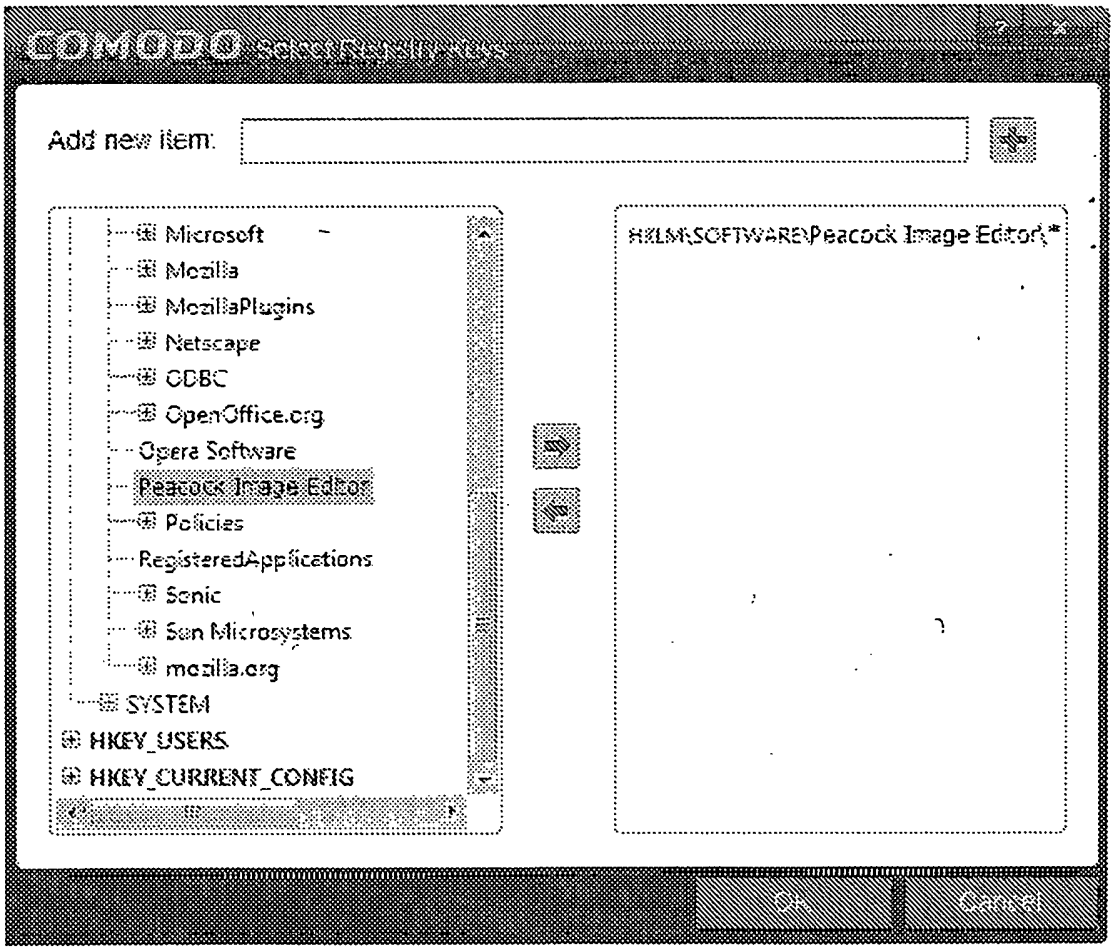
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



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



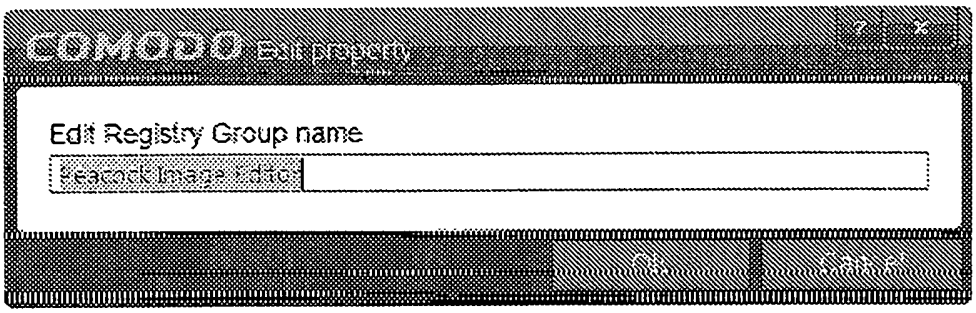
- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



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

item' field and press the '+' button.

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



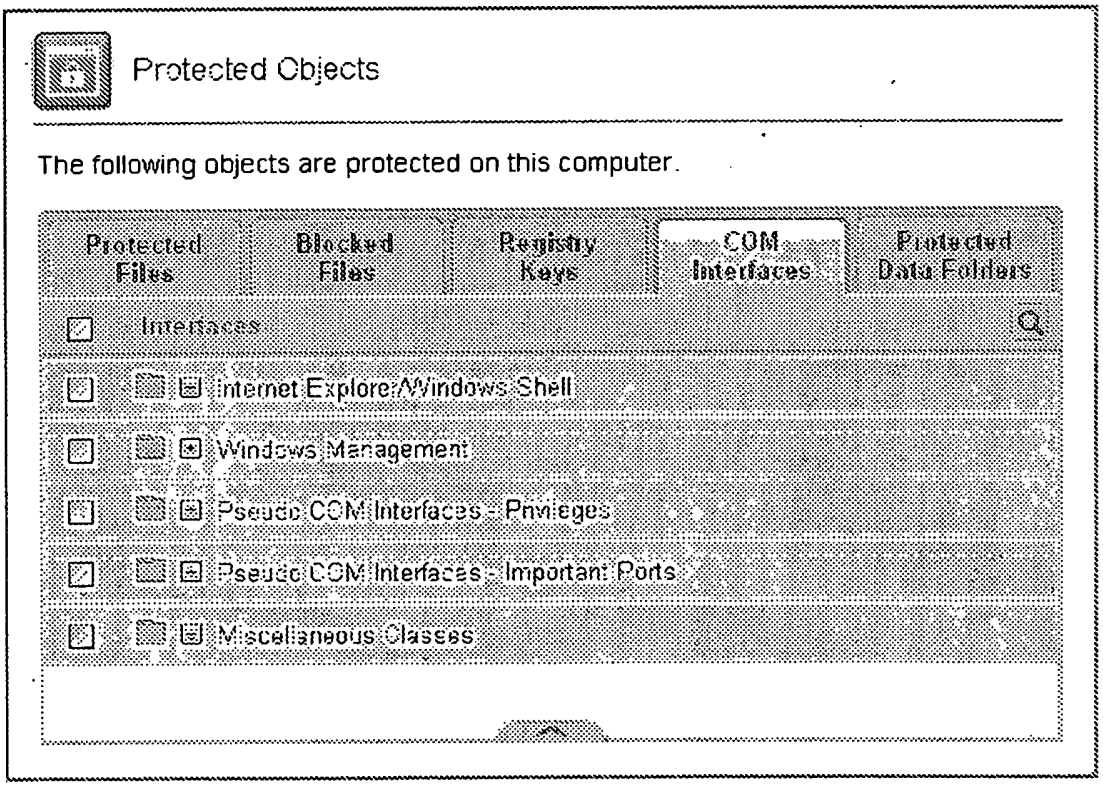
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.4.4. Protected COM interfaces

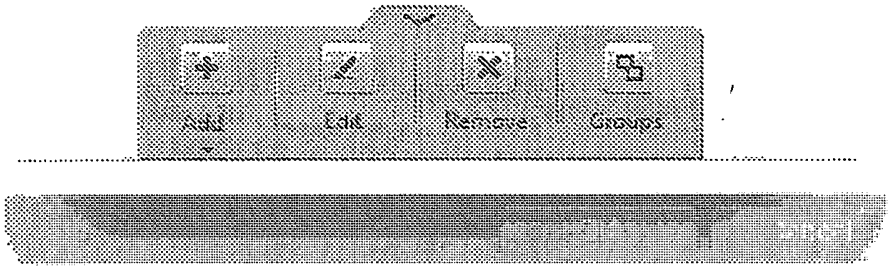
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers 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.

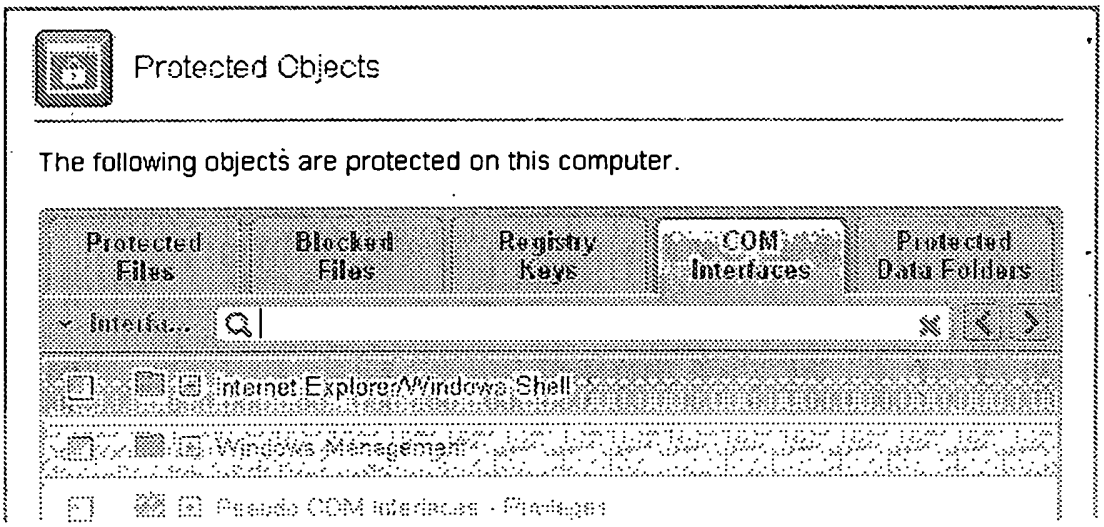


Clicking the handle at the bottom of the interface opens an options panel with the following options:



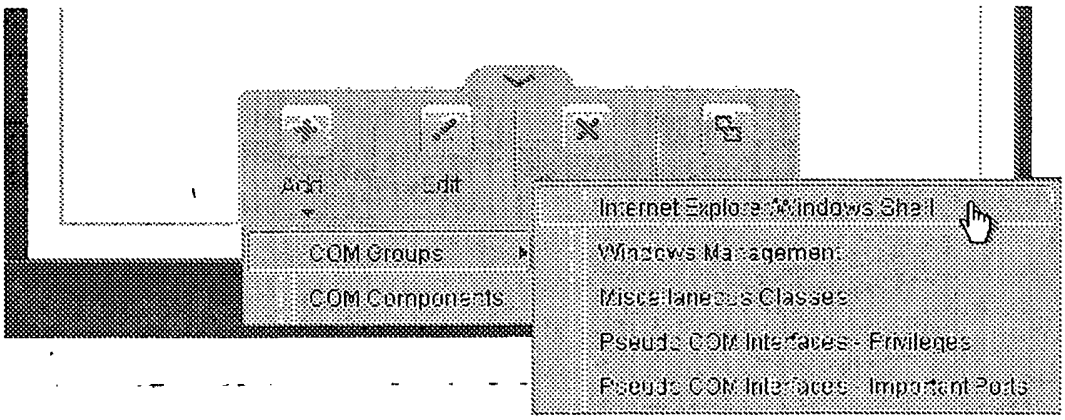
- Add - Allows you to add COM groups or individual COM components to COM Protection list.
- Edit - Allows you to edit the COM Class.
- Remove - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.
- Groups - Opens the Manage COM Groups interface that allows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



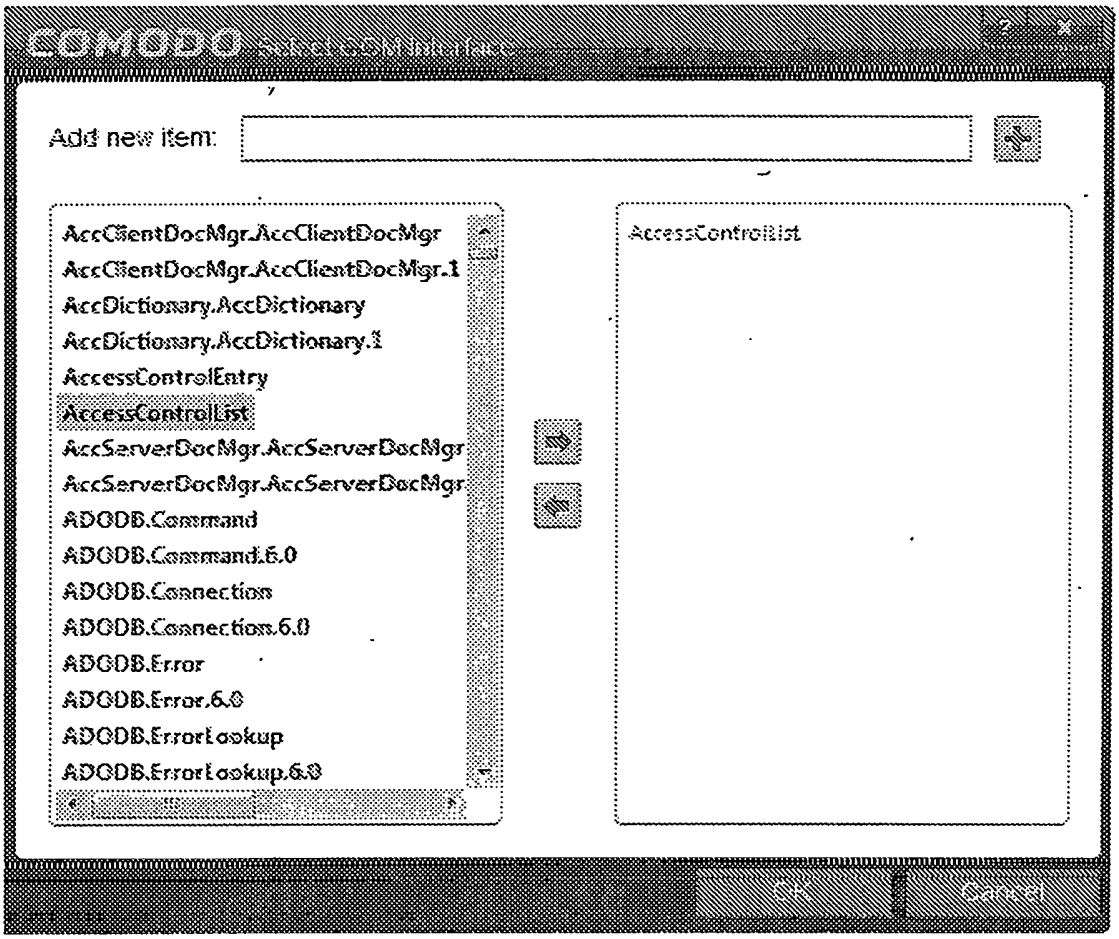
To manually add a COM Group or individual COM component

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



You can add the items by following methods:

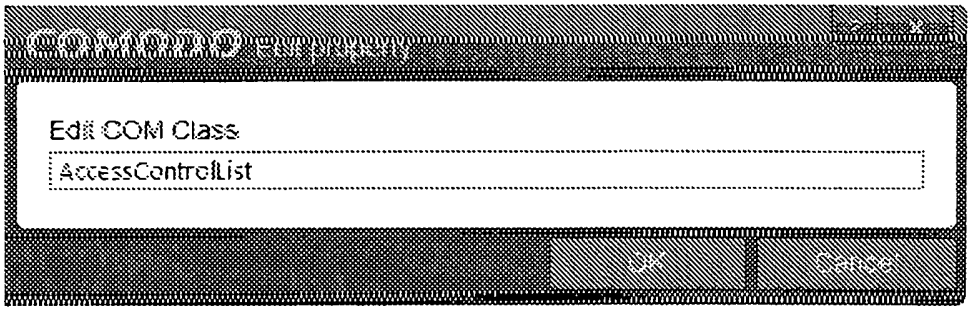
- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section COM Groups.
- **Adding COM Components** - Selecting 'COM components'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

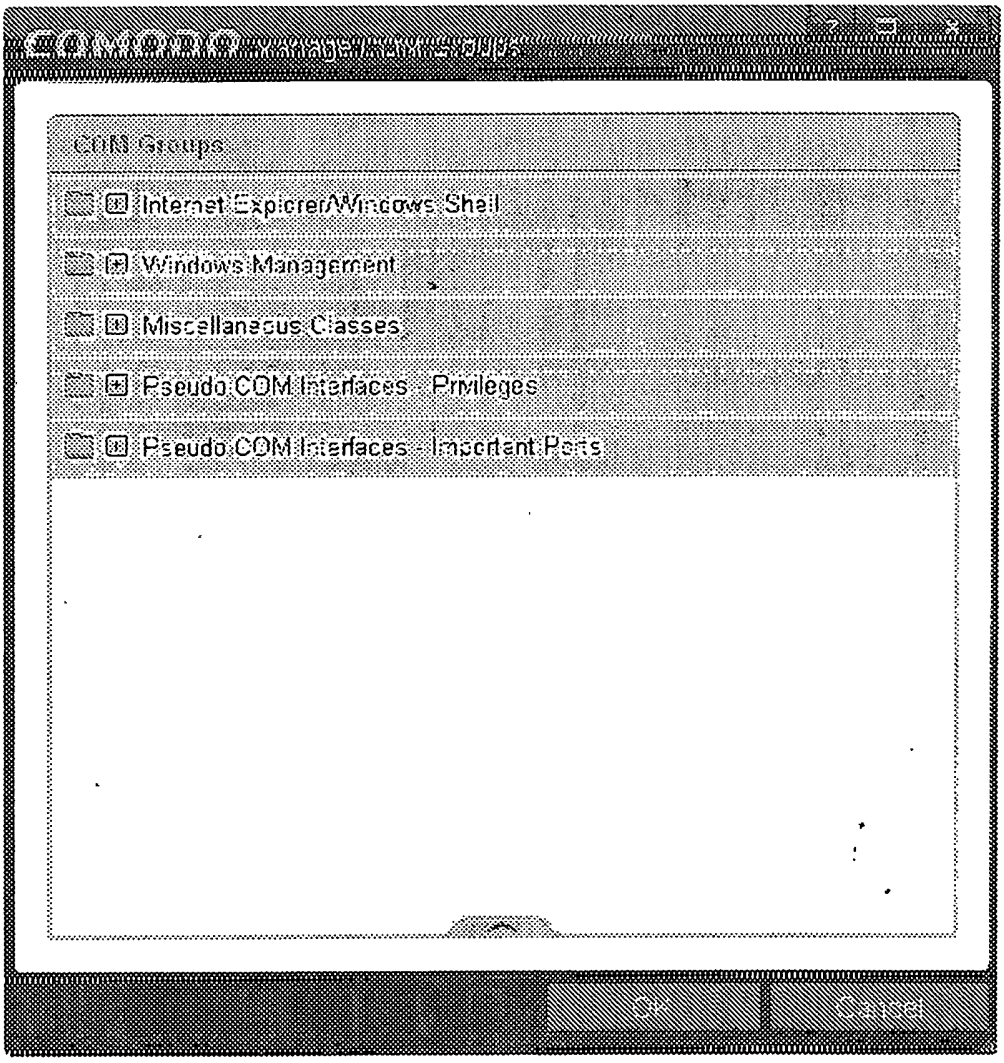
COM Groups

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'.

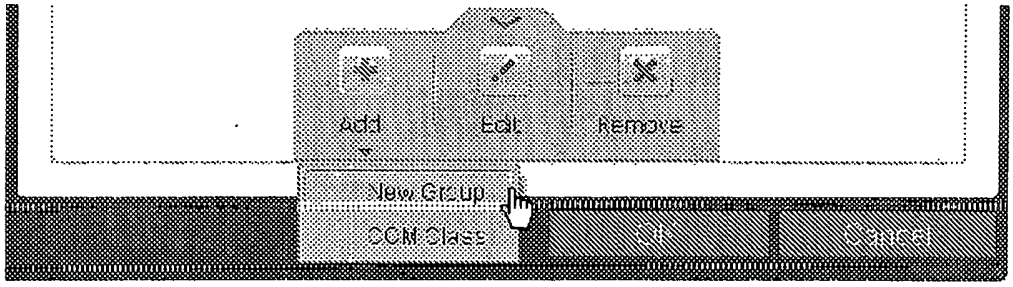
The 'Manage COM Groups' interface will open.



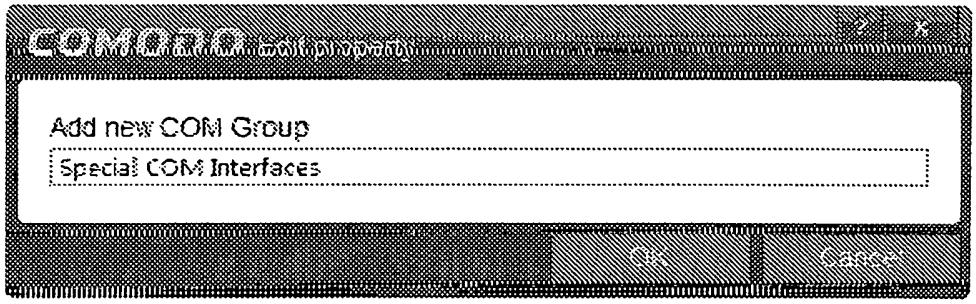
This interface allows you to:

- 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

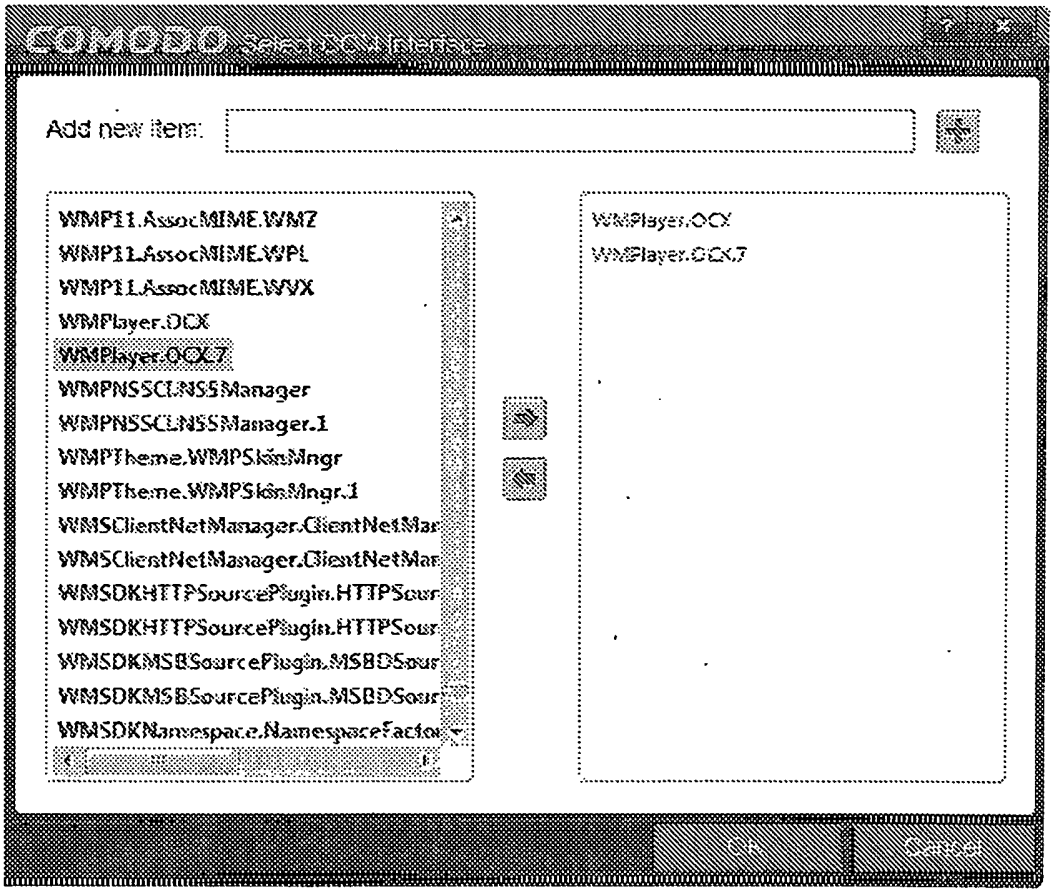
- To add a new group or add new COM Component(s) to an existing group, click the handle from the bottom and click 'Add'.



- **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.



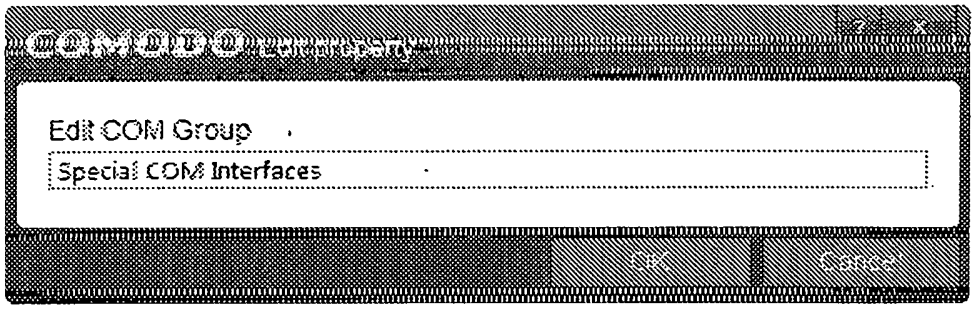
- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class. The 'Select COM Interface' dialog will be opened.



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



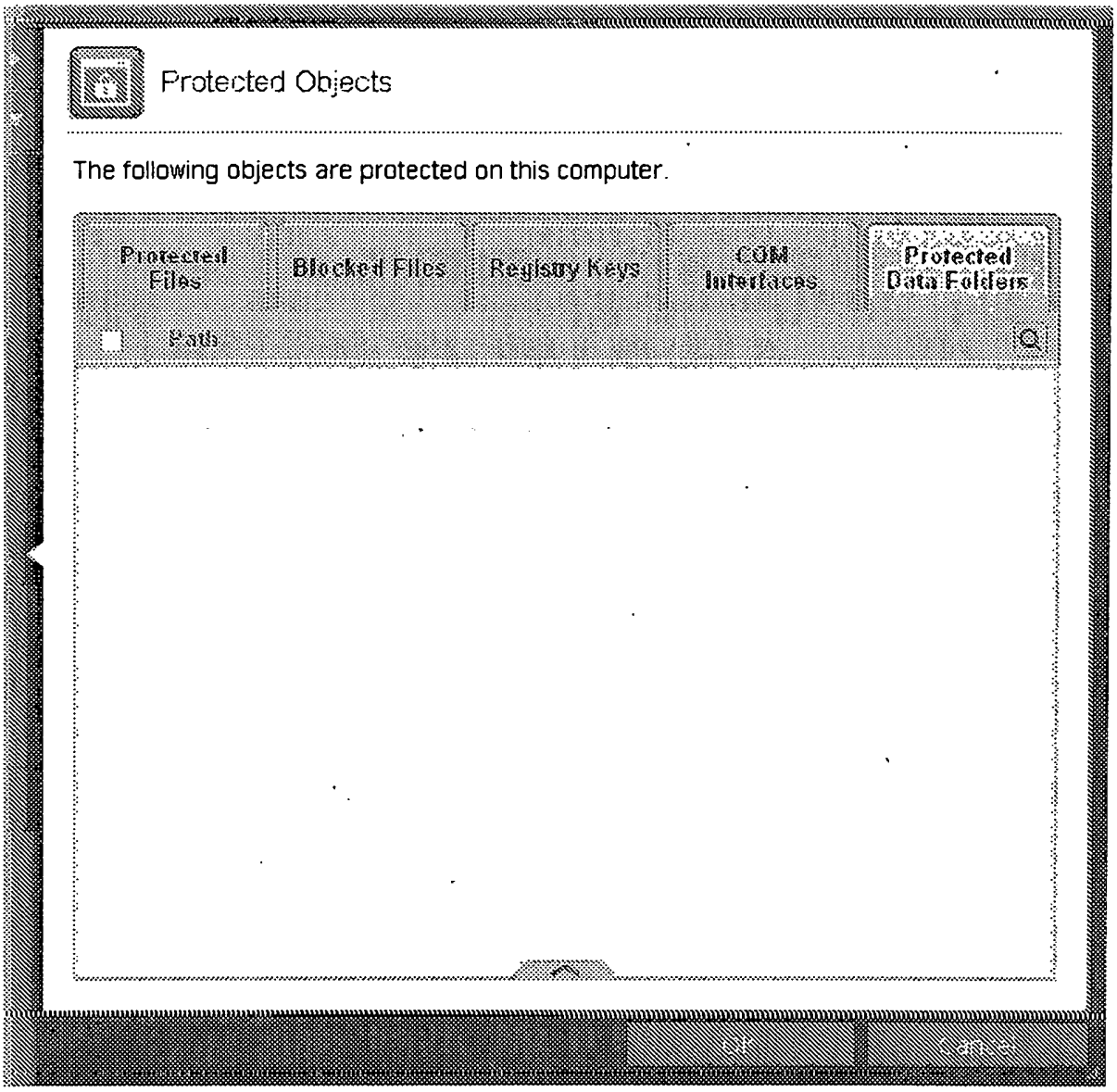
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual COM Component from a group, click + at the left of the group to expand the group, select the item to be removed, click the handle and choose 'Remove'.

6.2.2.4.5. Protected Data Folders

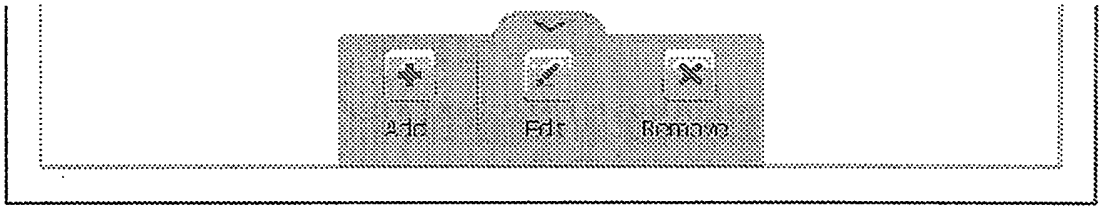
The data files in the folders listed under the Protected Data Folders area cannot be seen, accessed or modified by any known or unknown application that is running inside the sandbox.

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:

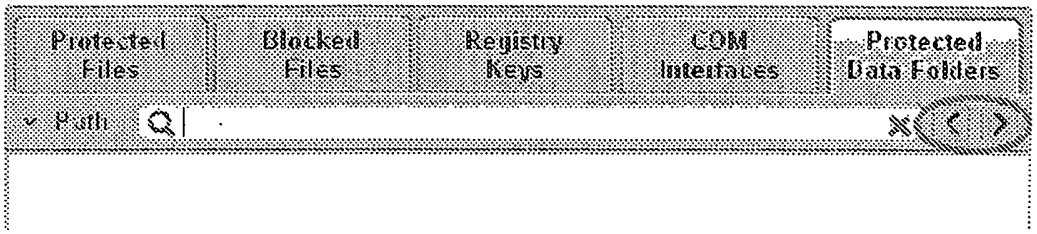


Clicking the handle at the bottom of the interface opens an options panel with the following options:



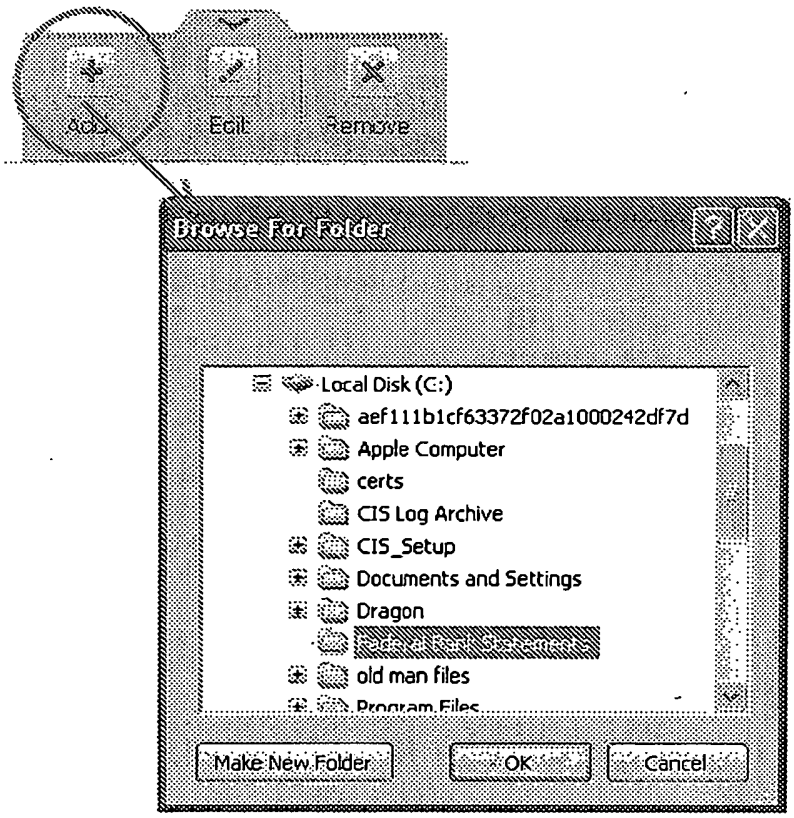
- Add - Allows you to add folders to Protected Data Folders list.
- Edit - Allows you to edit the path of the added folders.
- Remove - Deletes the currently selected folder.

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.

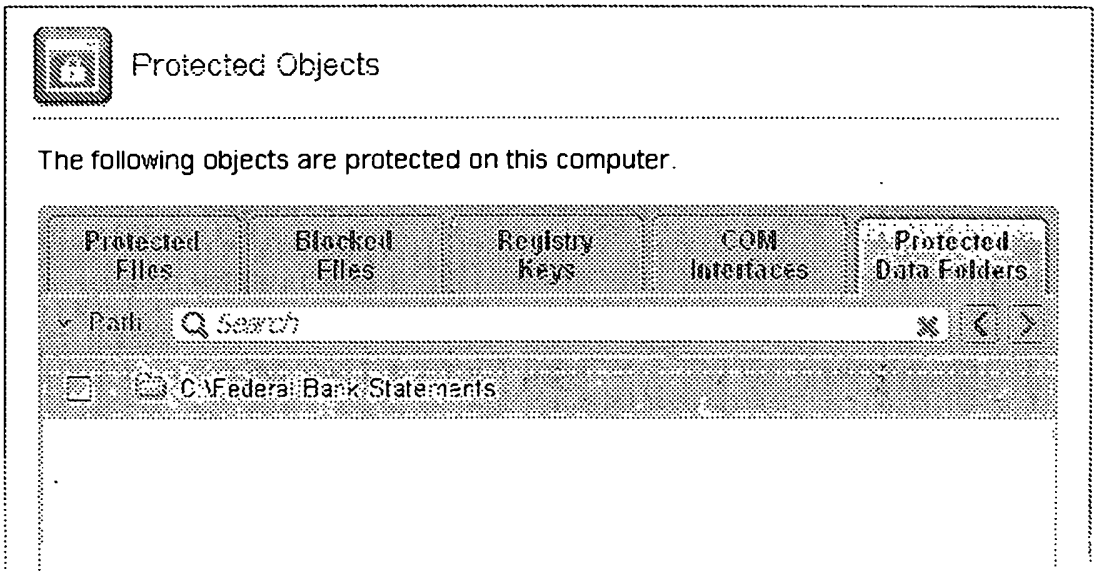


To add a folder to be protected

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



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

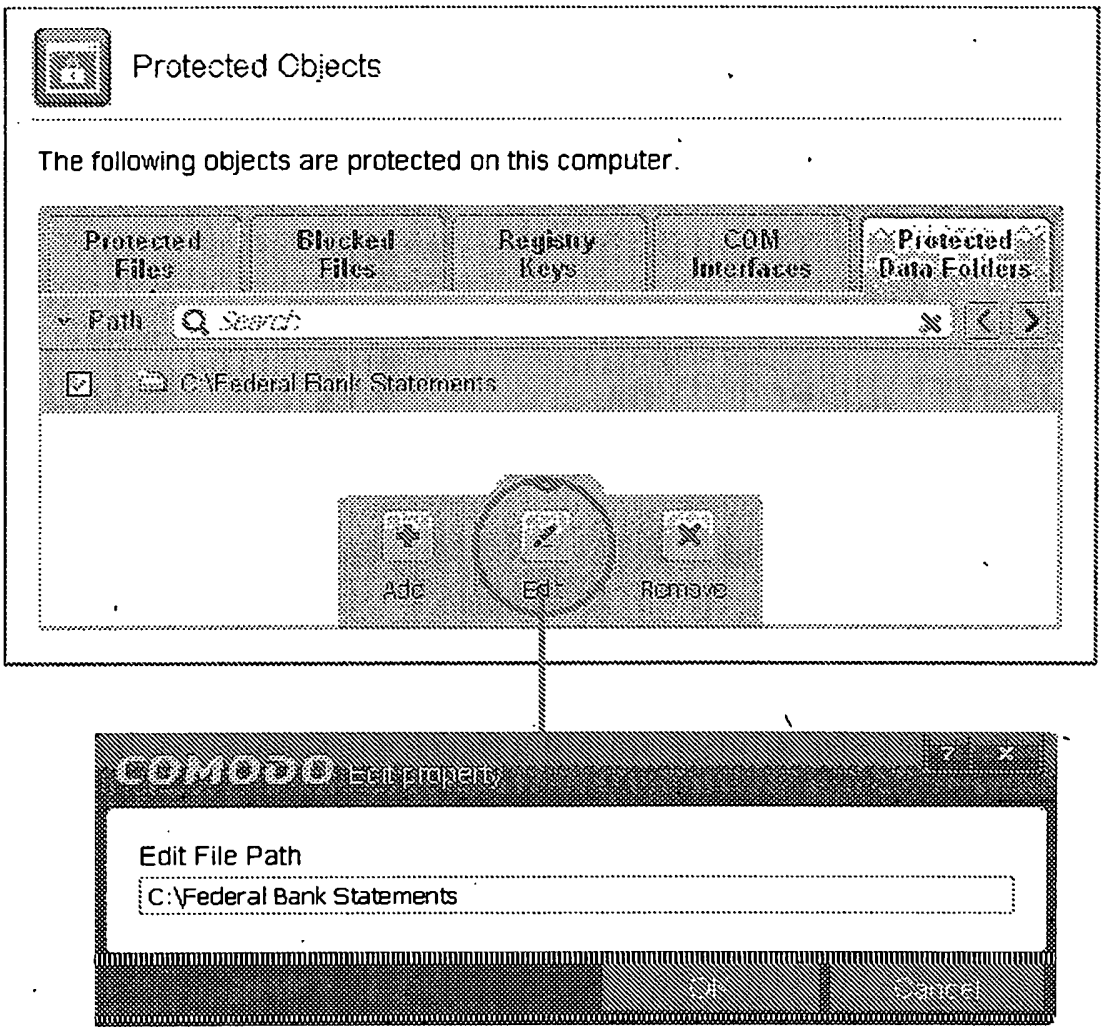


- Click OK to confirm your choice.

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

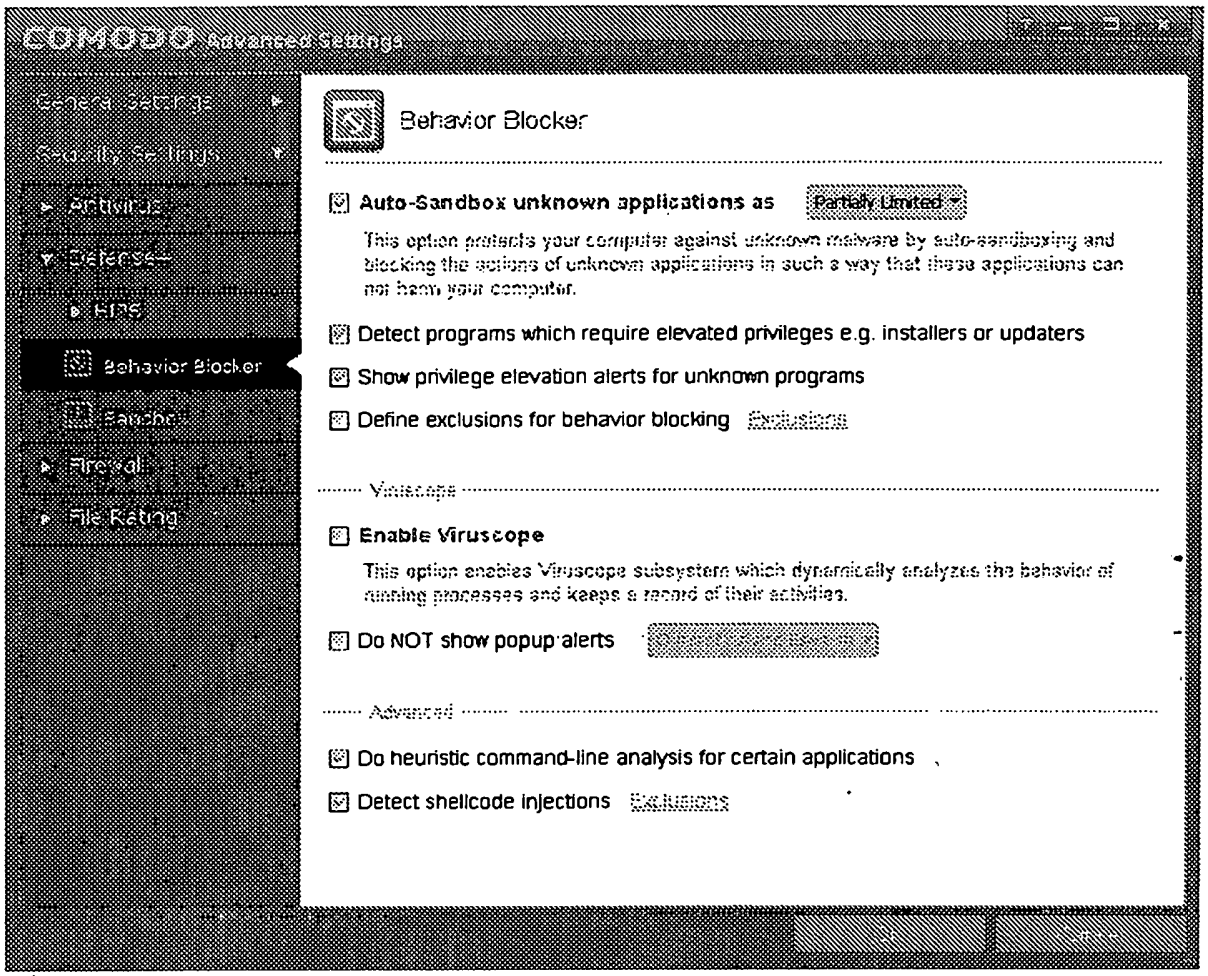
To remove an item from Protected Data Folders list

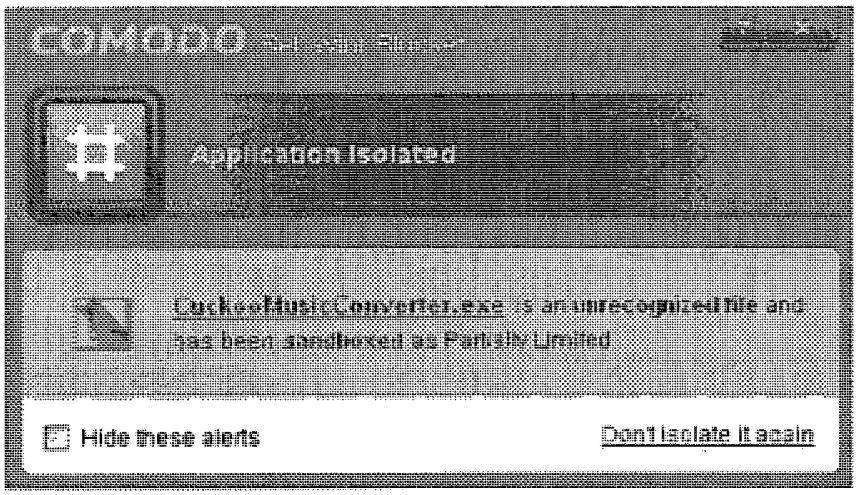
- Select the folder from the list, click the handle from the bottom and choose 'Remove'.
- The selected folder will be removed from the protected folders list. CIS will not generate alerts, if the folder is subjected to unauthorized access.

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.

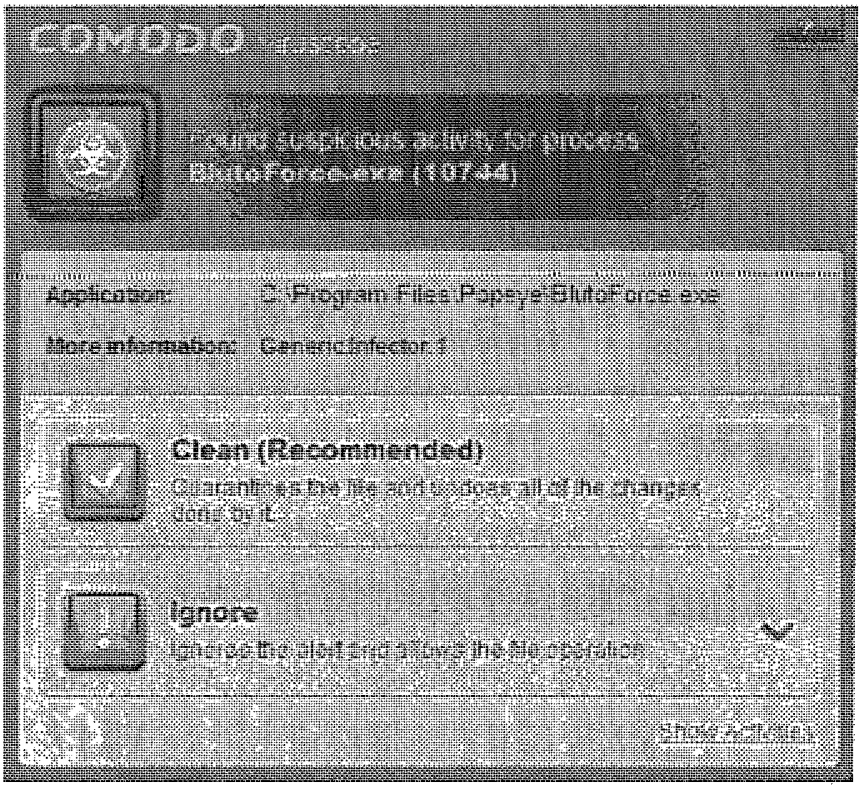




Viruscope monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core 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.



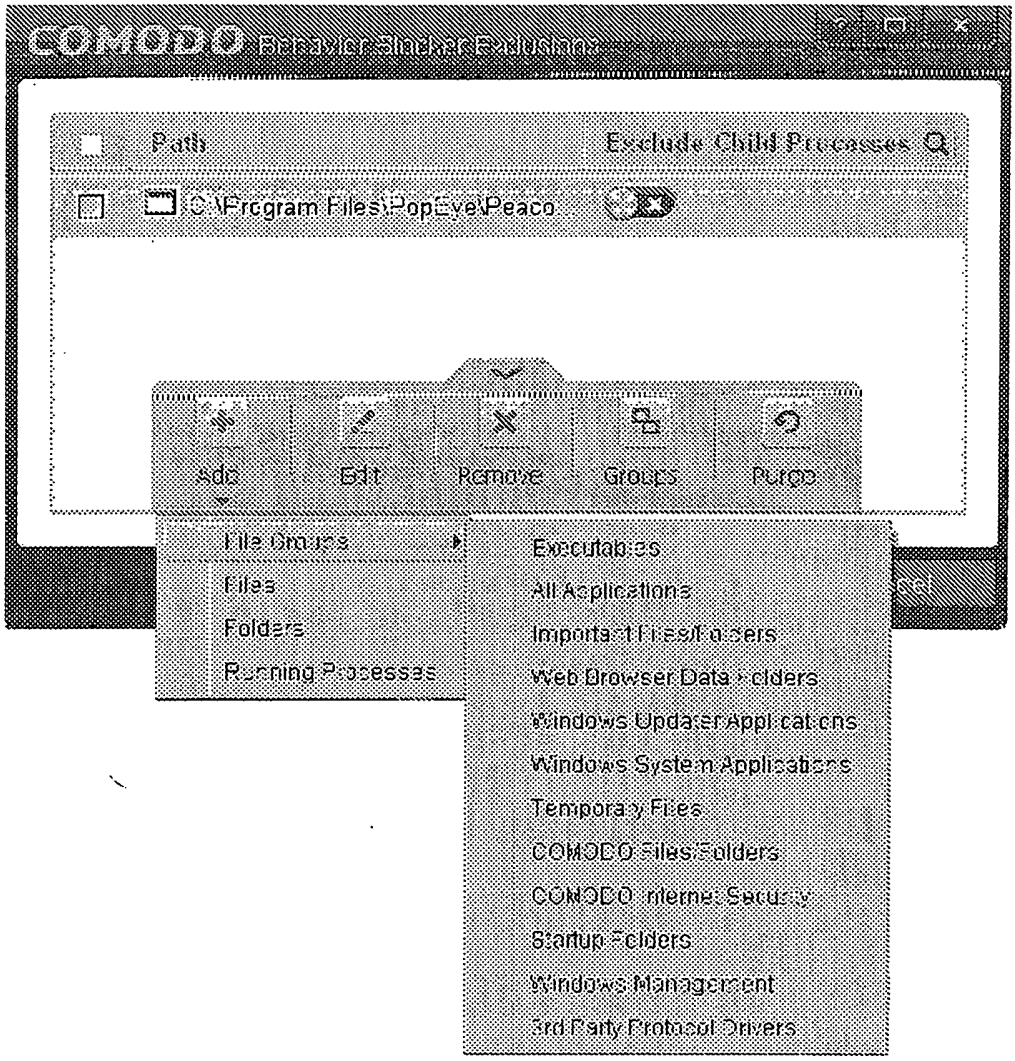
You can decide on whether or not to allow the installer or update based on your assessment, from the alert itself. (***Default=Enabled***)

- **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.



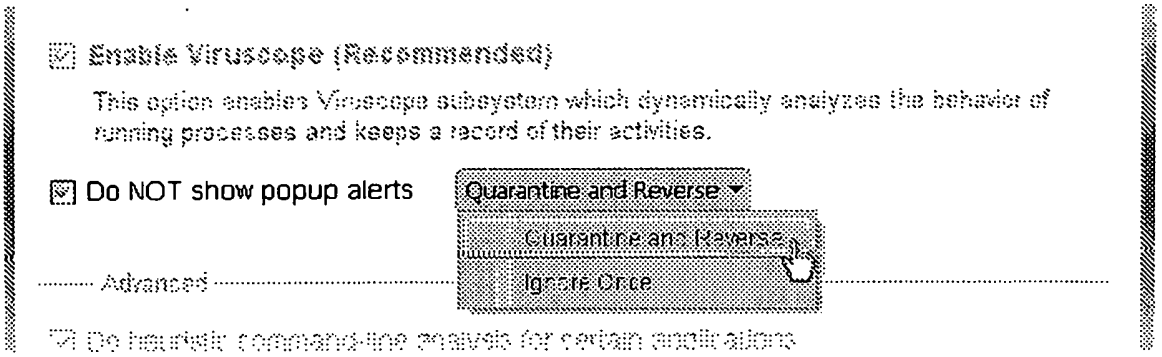
- Click the handle at the bottom of the interface and choose 'Add'
- You can add items by selecting the required option from the drop-down:
  - **File Groups** - Enables you to select a category of pre-set files or folders. For example, selecting 'Executables' would enable you to create a ruleset for 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 wscript.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CIS detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the internet, for example, the alert will state 'test.vbs' is attempting to connect to the internet ***(Default = Enabled)***.

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

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

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

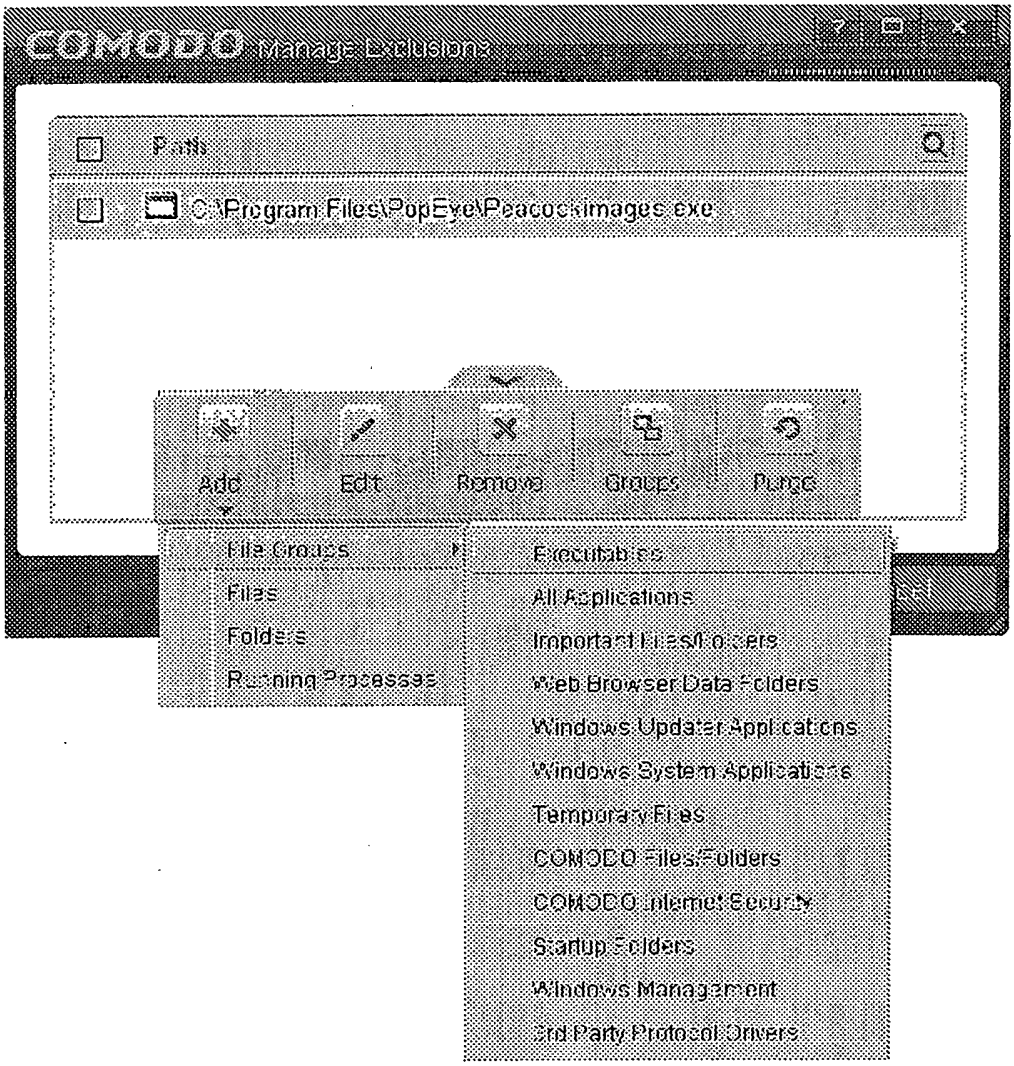
  Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow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

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

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

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

  - Select the 'Detect shellcode injections' checkbox and click the 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.

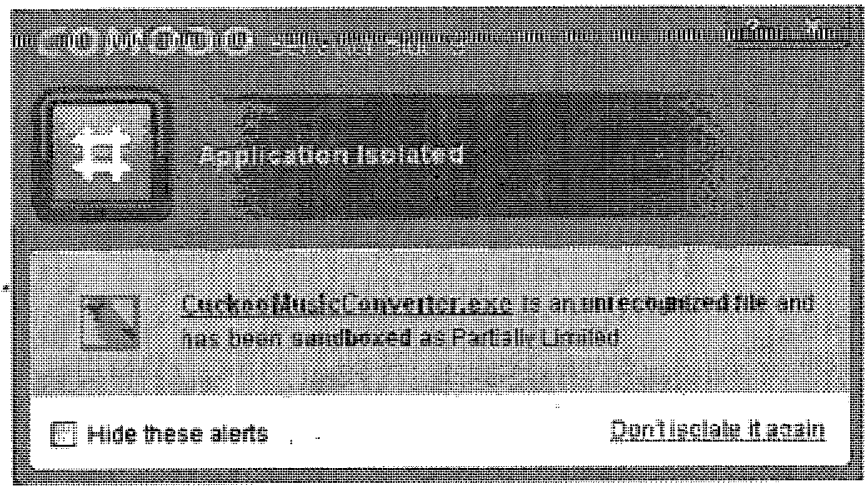
- **Sandbox and Cloud Scanning Part 2**

  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.

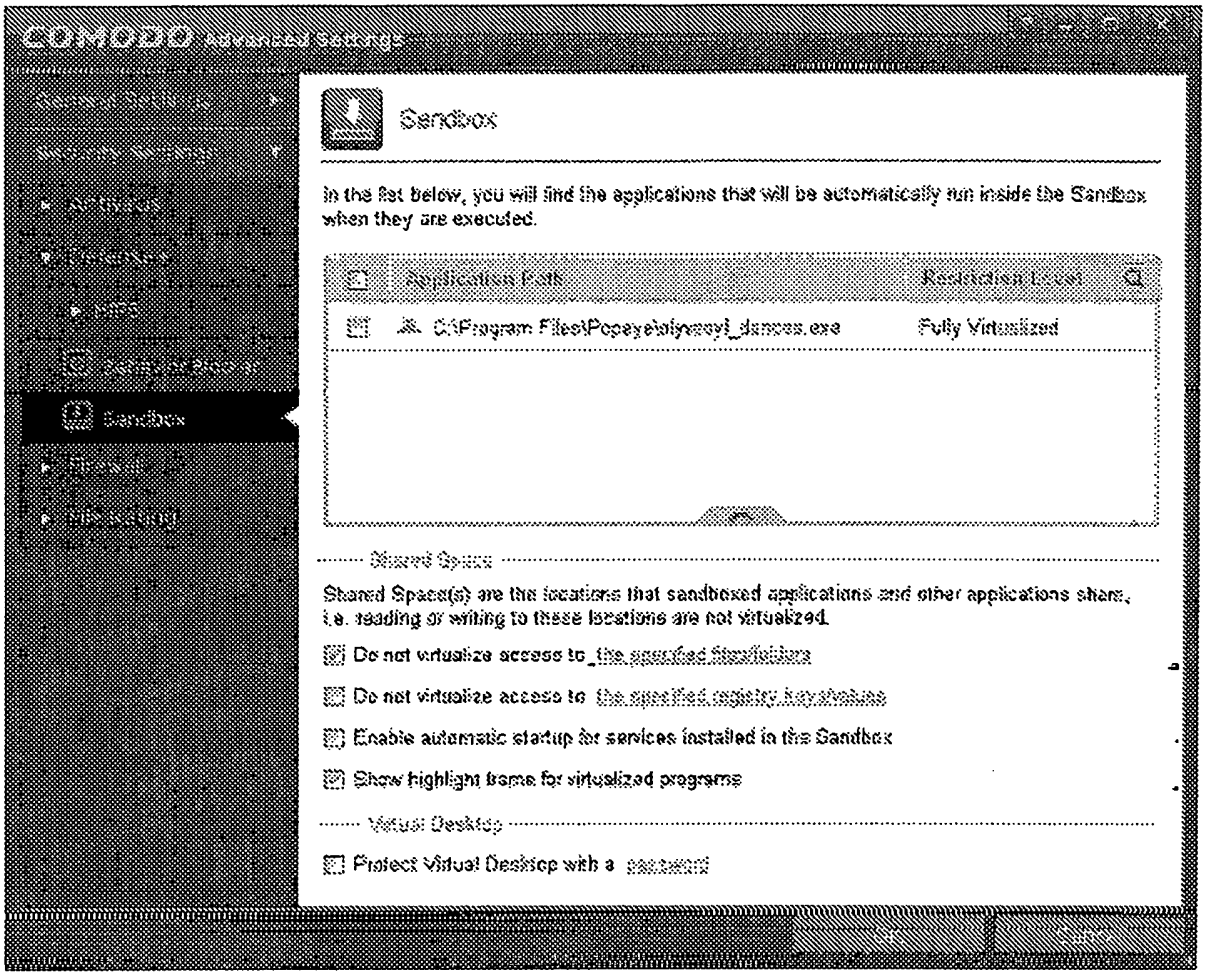
- If the scan does not detect that the file is malicious then it passes onto the the next stage of inspection - behavior monitoring.
- The behavior analysis system is a cloud based service that is used to help determine whether a file exhibits malicious behavior. Once submitted to the system, the unknown 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

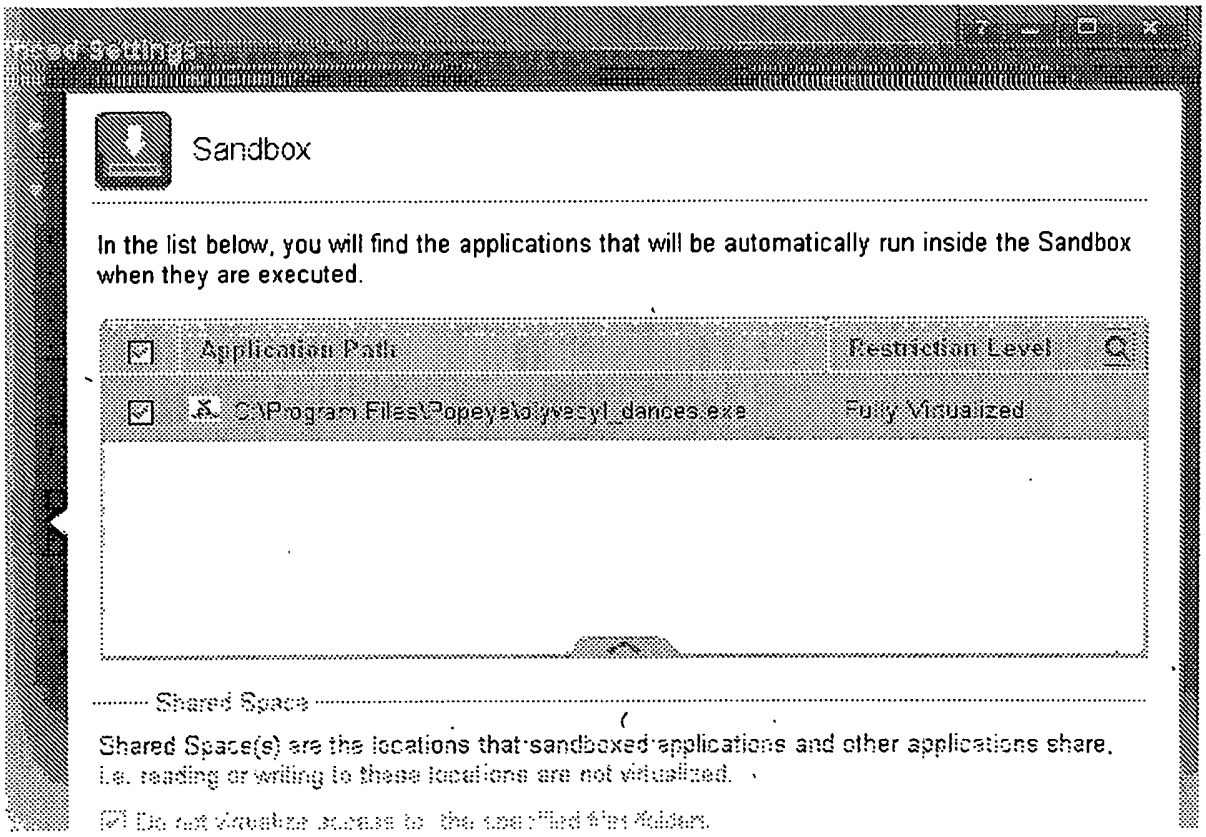


Click the following links to find out more about each section:

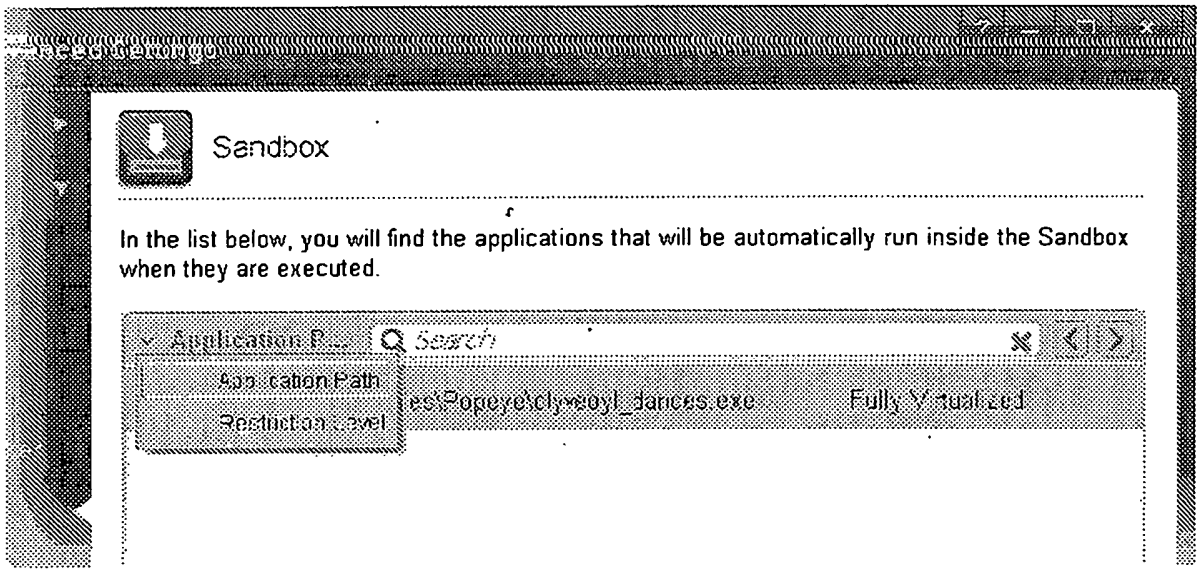
- Sandboxed Programs - Add and configure programs that should always run sandboxed
- Shared Space Settings - Files downloaded or generated by sandboxed applications that you wish to be able to access from your real system should be downloaded to the shared space
- Virtual Desktop - Create an 'exit' password 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.

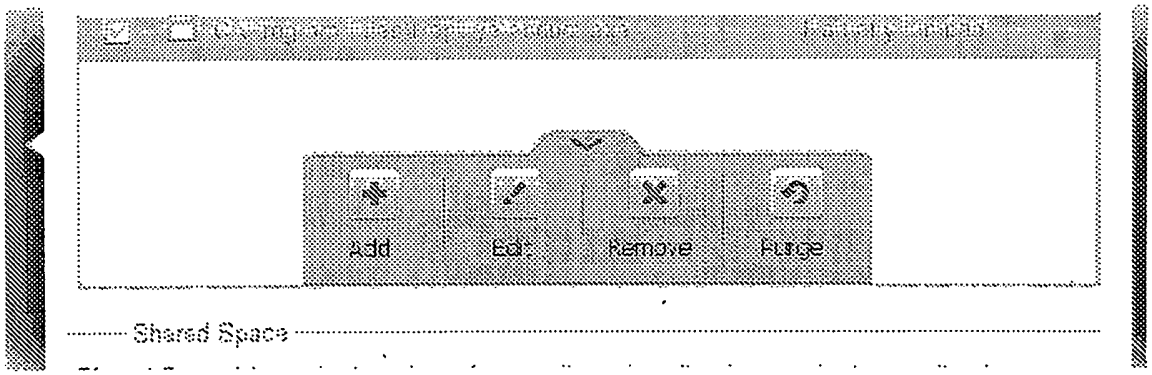


You can search for a application or program from the list by clicking the search icon at the far right in the column header.



- 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:

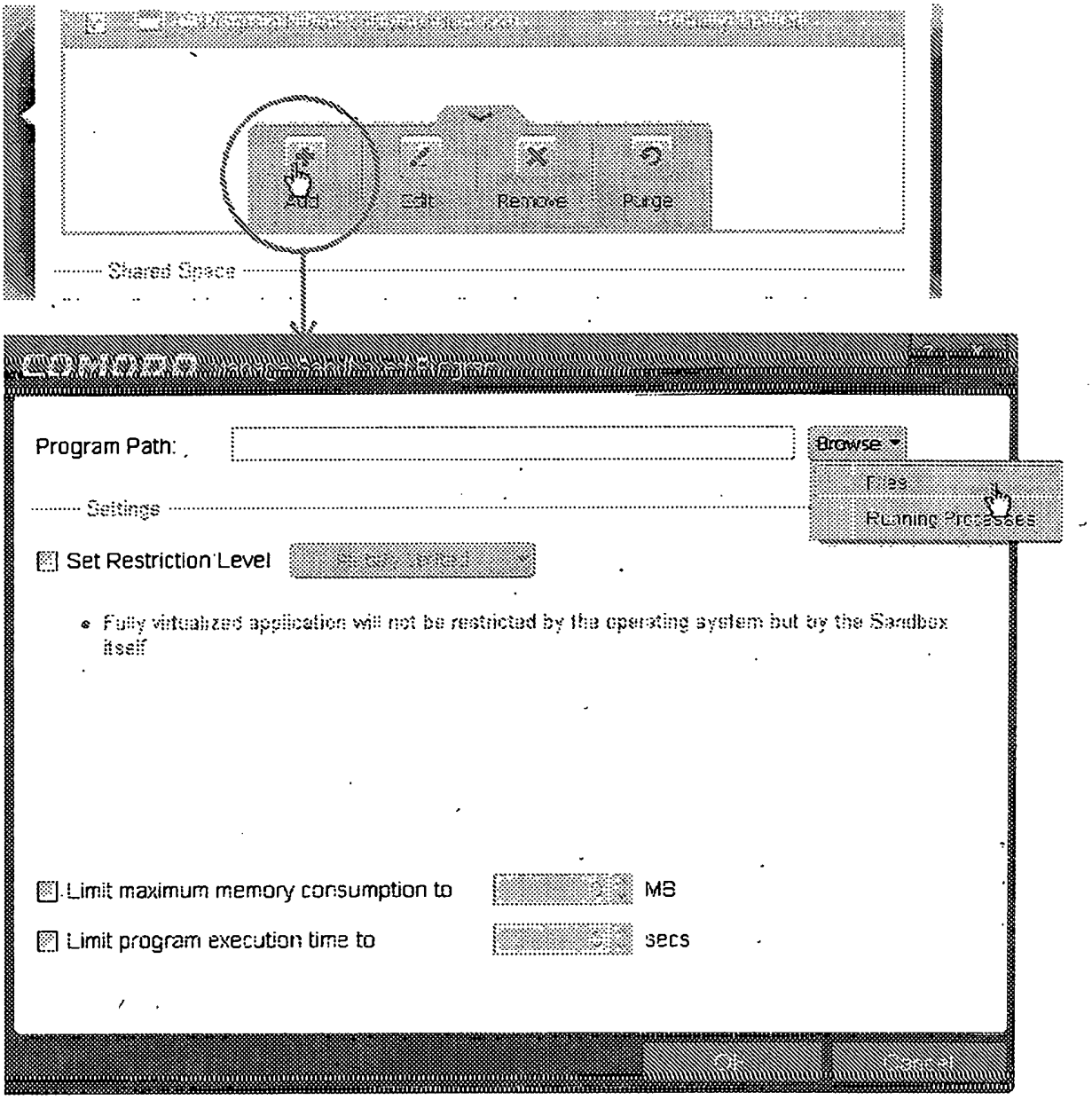
- Right click on the program or file to be opened from the Windows Explorer and select 'Run in Comodo Sandbox'

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':



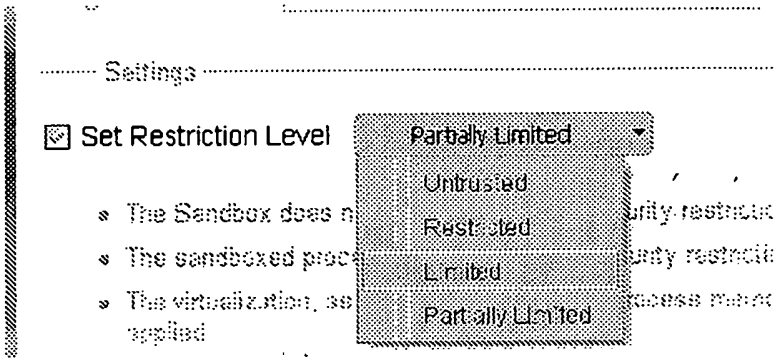
- The 'Manage Sandboxed Program' interface will open:

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:

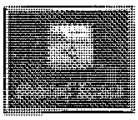
- **Set Restriction Level** - The Access restriction level determines the amount of privileges a sandboxed application has to access other software and hardware resources on your computer. (***Default = Disabled***)
- Set an access restriction level by enabling the 'Set Restriction Level' check-box and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

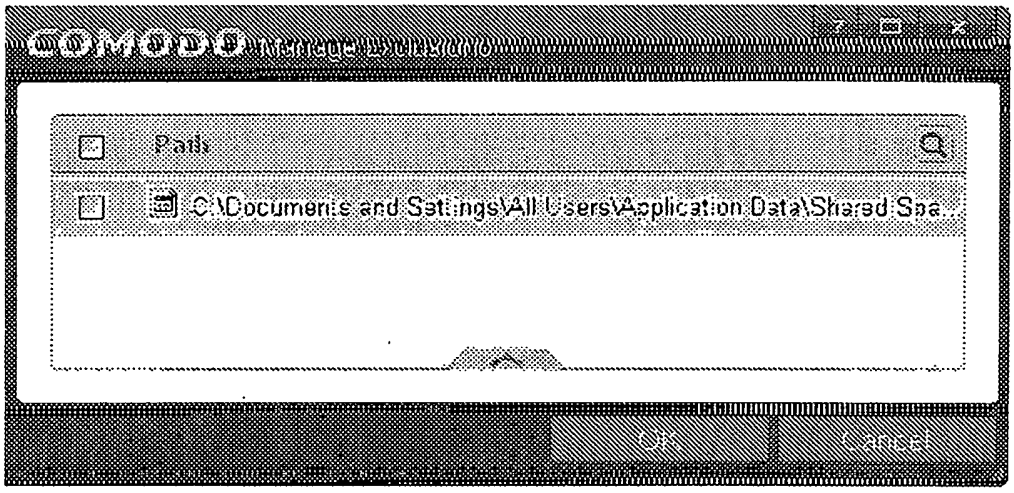
You can access the shared space folder in the following ways:

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

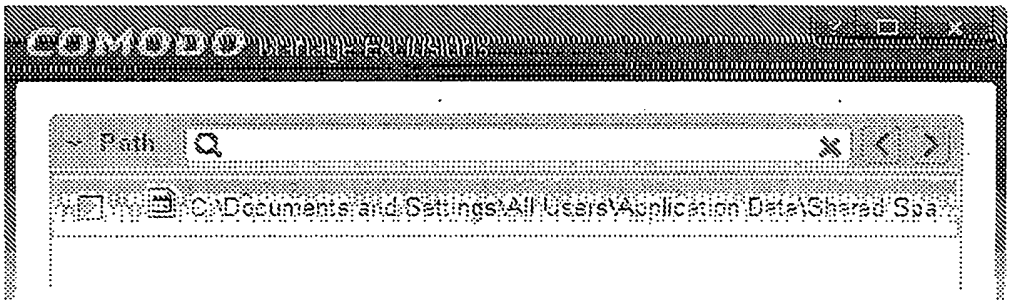
- Clicking 'Shared Space' button on the CIS interface
- Opening 'Sandbox Tasks' from the Tasks interface then clicking 'Open Shared Space'
- By default, sandboxed applications can access folders and files on your 'real' system but cannot save any changes to them. However, you can define exclusions to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

To define exclusions for files and folders

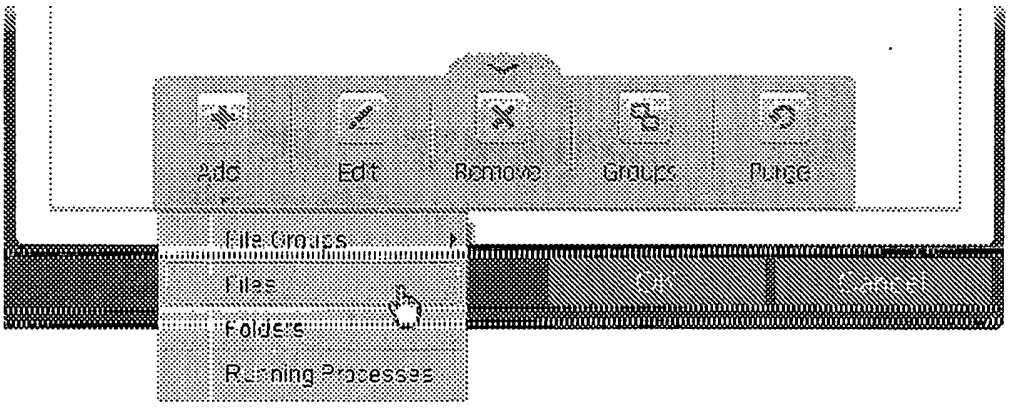
- Enable the 'Do not virtualize access to the specified files/folders' check-box then click on the words 'the specified files/folders'. The 'Manage Exclusions' dialog will appear.



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

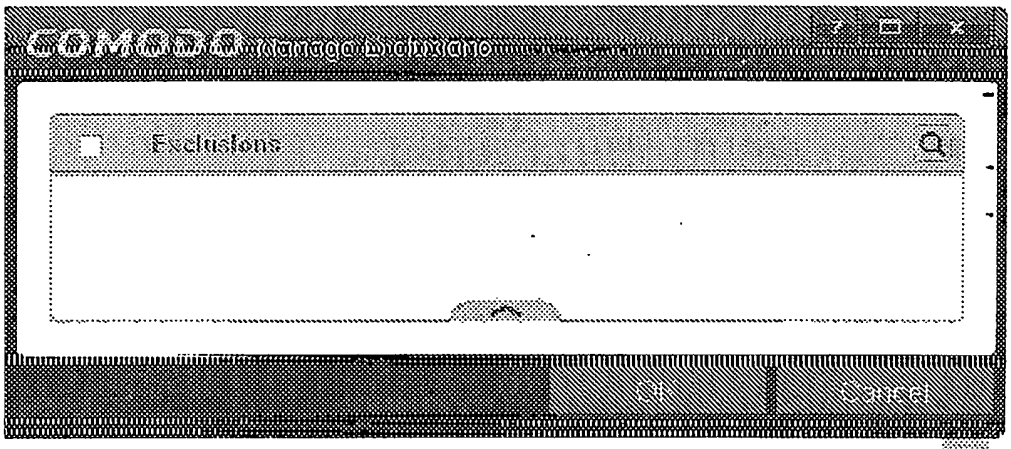
Folders - Specify a folder that can be accessed by sandboxed applications
File Groups - Enables you to choose a category of files or folders to which access should be granted. For example, selecting 'Executables' would enable you to create an exclusion for all files with the extensions .exe .dll .sys .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.

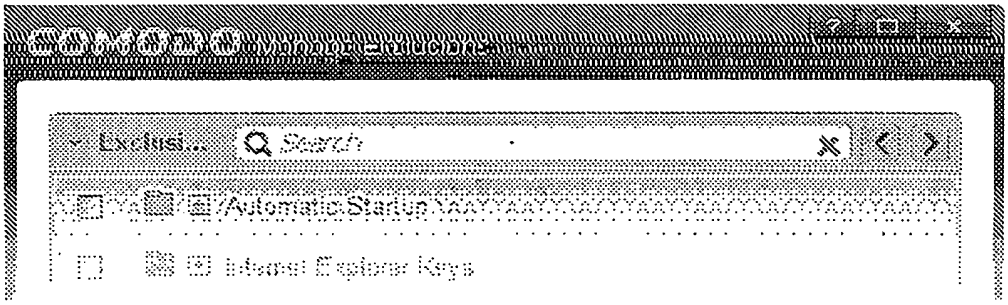
- To edit an exclusion, select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Change file or folder location path and click 'OK'
  - Click 'OK' to implement your settings
  - To manage available file groups, click the 'Groups' button from the tools menu. The 'Manage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

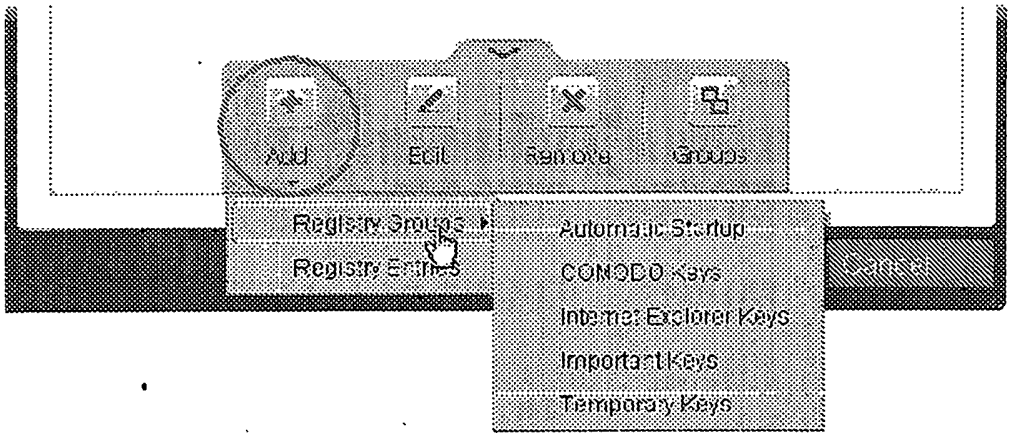
- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click on the words 'the specified registry keys/values'. The 'Manage Exclusions' dialog will appear.



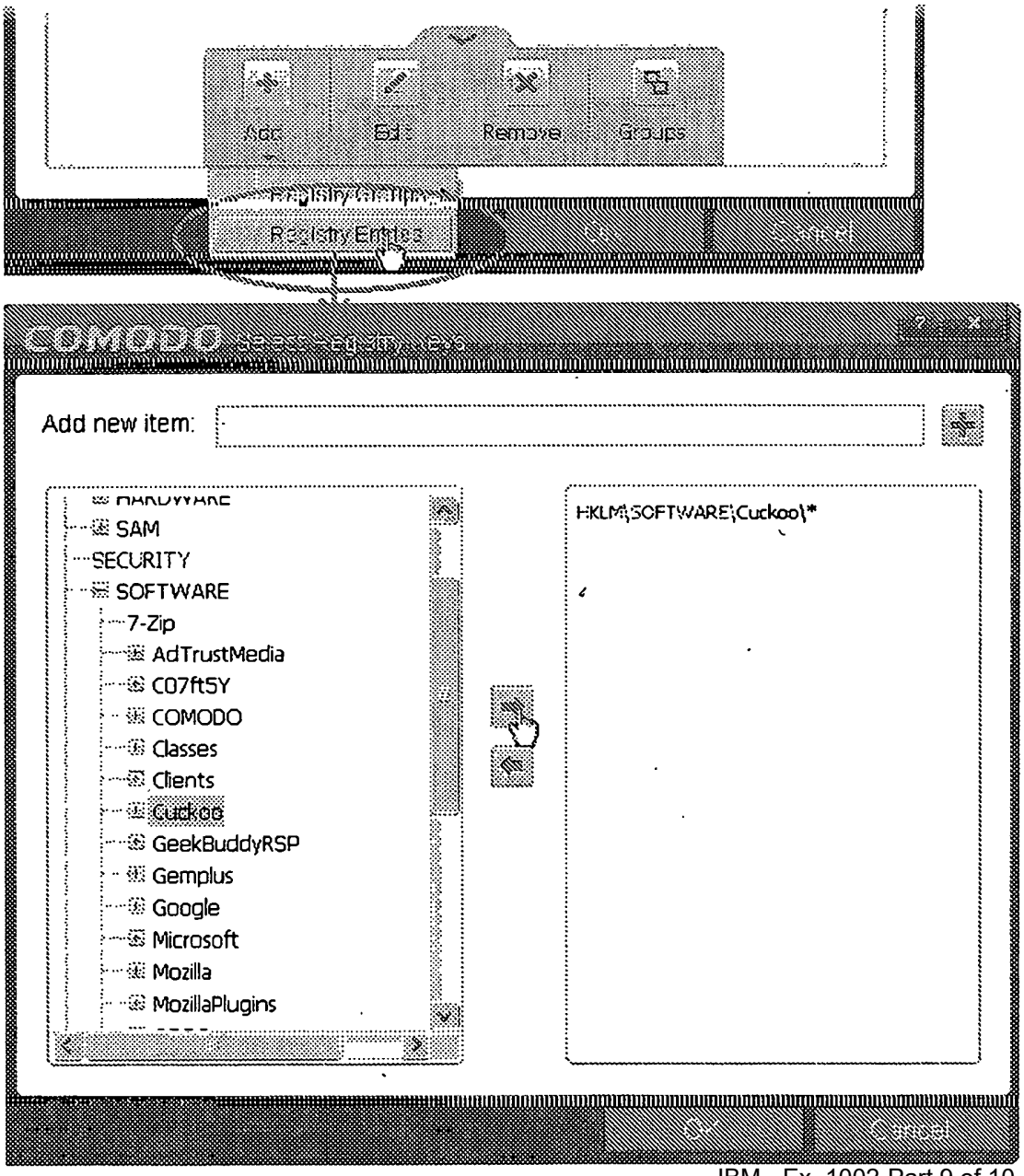
You can search for specific excluded Registry Keys or Values from the list by clicking the search icon at the far right in the column header and entering the name of the key/value in full or part. You can navigate through the successive results by clicking the left and right arrows.



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

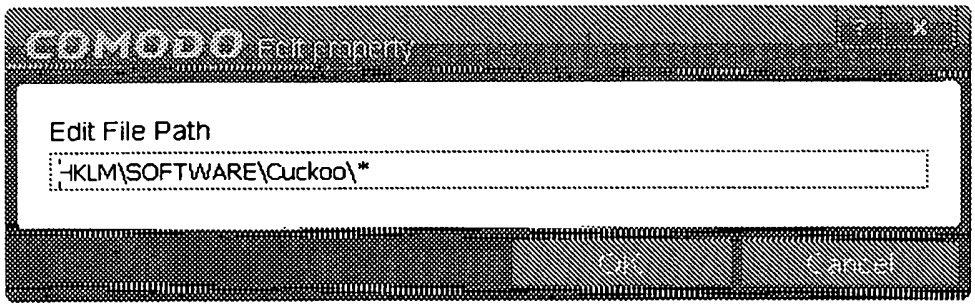


- **Registry Groups** - Allows you to batch select a predefined group of important registry keys as exclusions. For an explanation of CIS registry groups, refer to the section Registry Groups.
- **Registry Entries** - Opens an interface that allows you to quickly browse Windows registry keys and add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



- Click 'OK' to implement your settings.

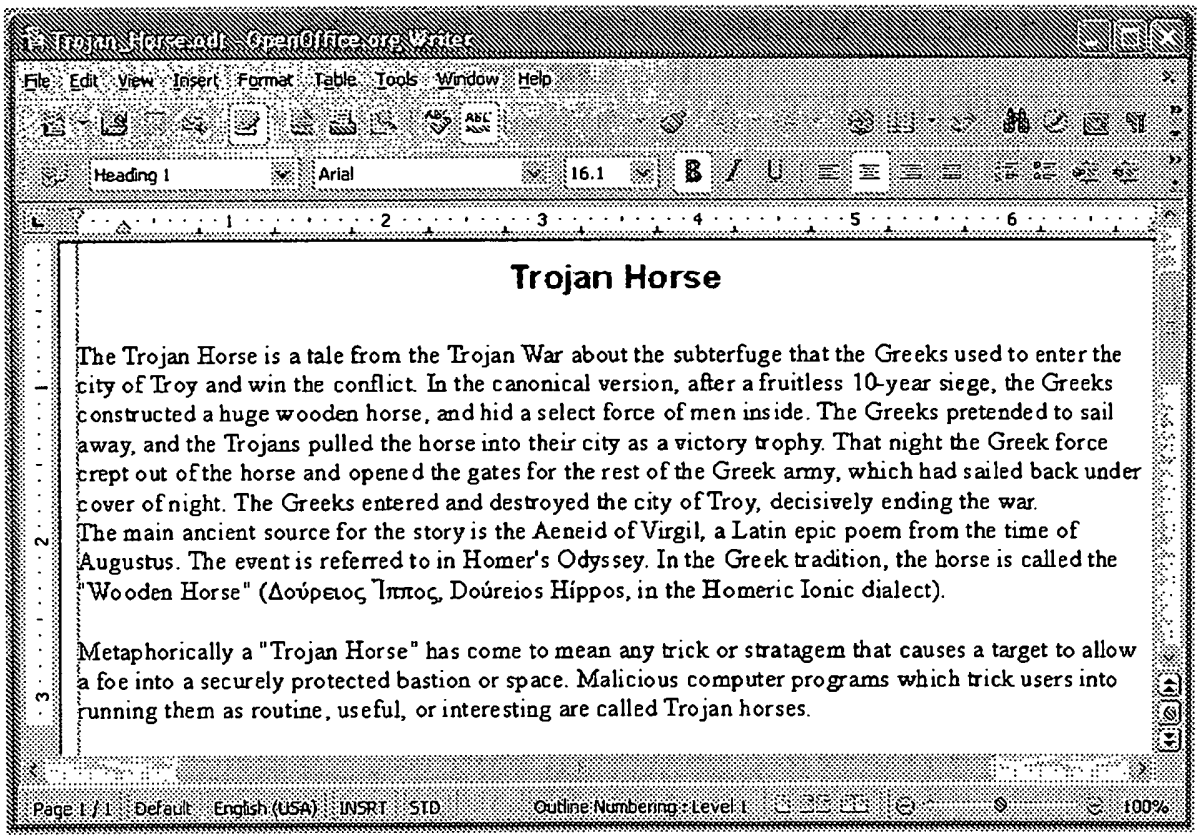
- To edit an exception, first select it from the list, click the handle to open the tools menu then select 'Edit'.
  - Edit the key path and click OK.



- 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

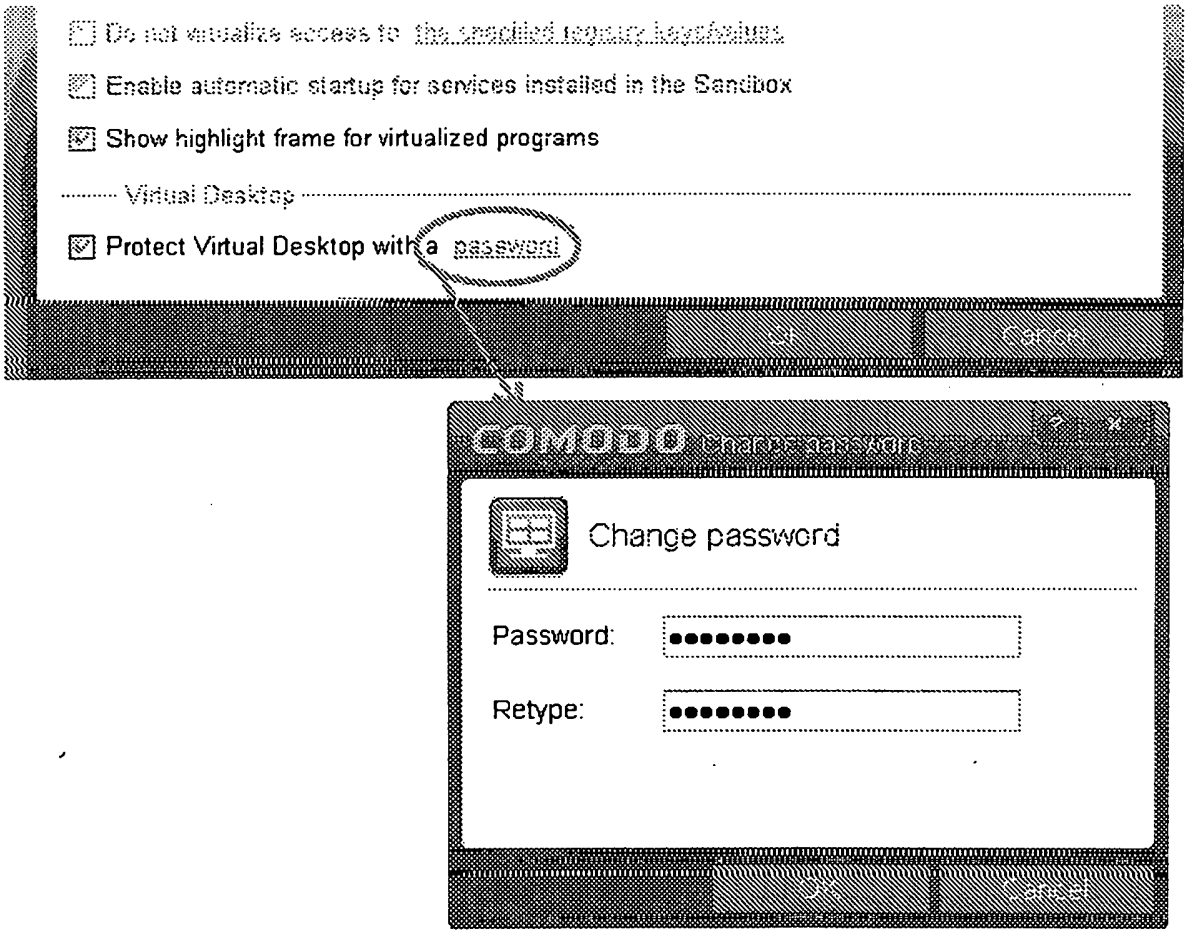
The Virtual Desktop Settings area allows you to password protect your Virtual Desktop. Once set, the password has to be entered every time when the Virtual Desktop is closed.



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.

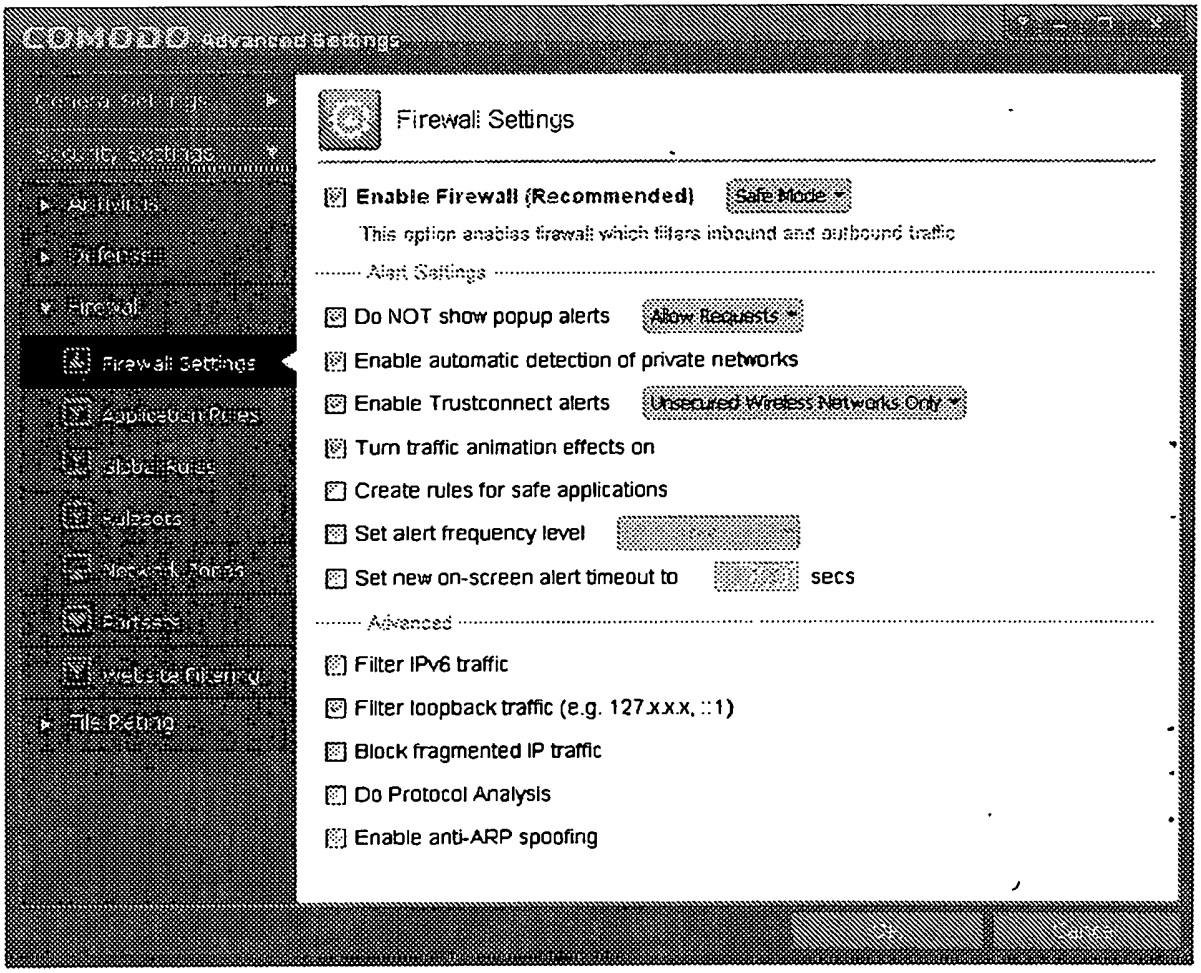


- Type a password which contains a combination of alphabetic and numeric characters and symbols which cannot be easily guessed by others. We recommend a password of at least 8 character in length.
- Re-enter the password in the 'Retype' field then click 'OK'.

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

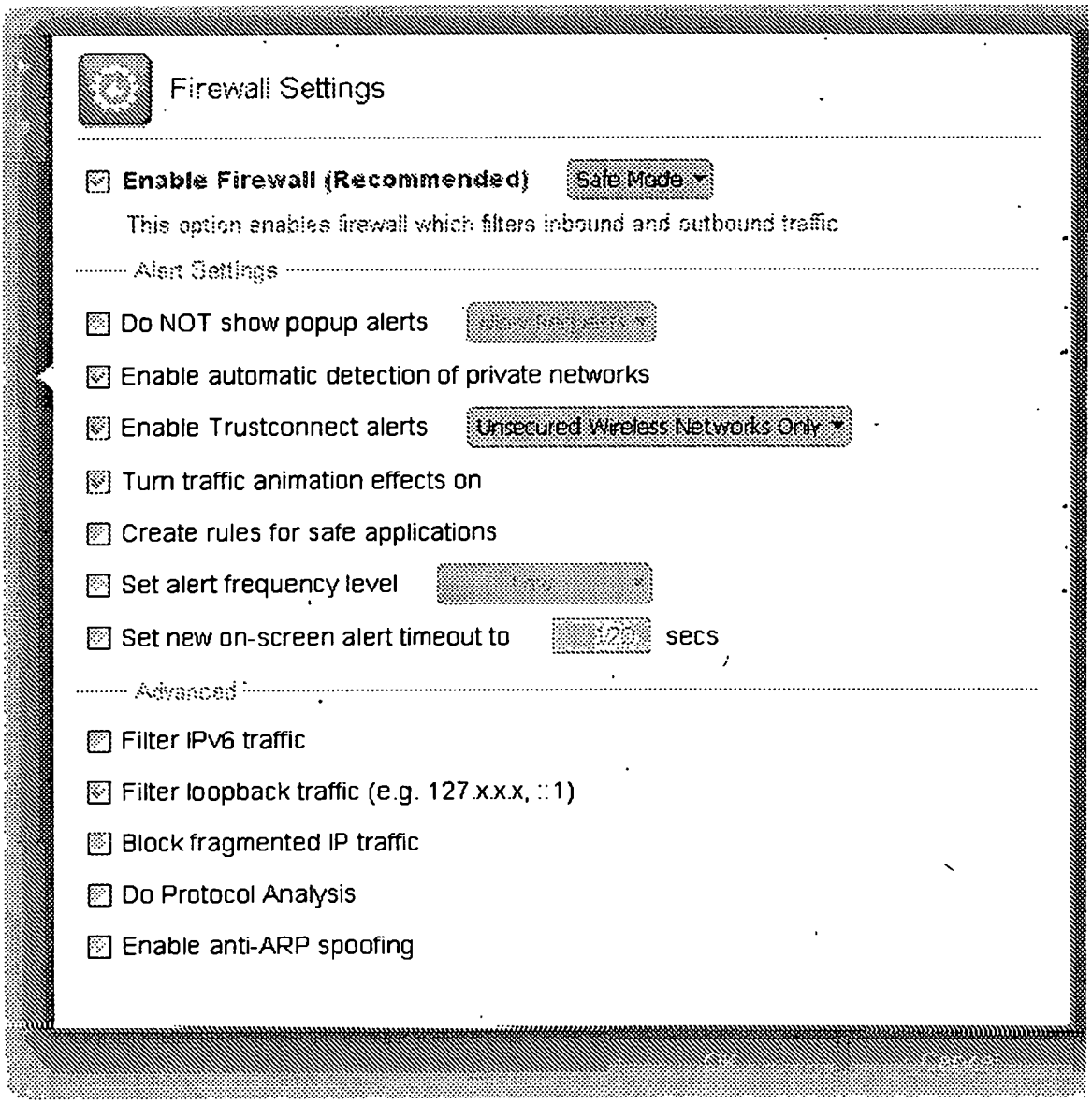
not to allow or block a connection attempt.

- 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

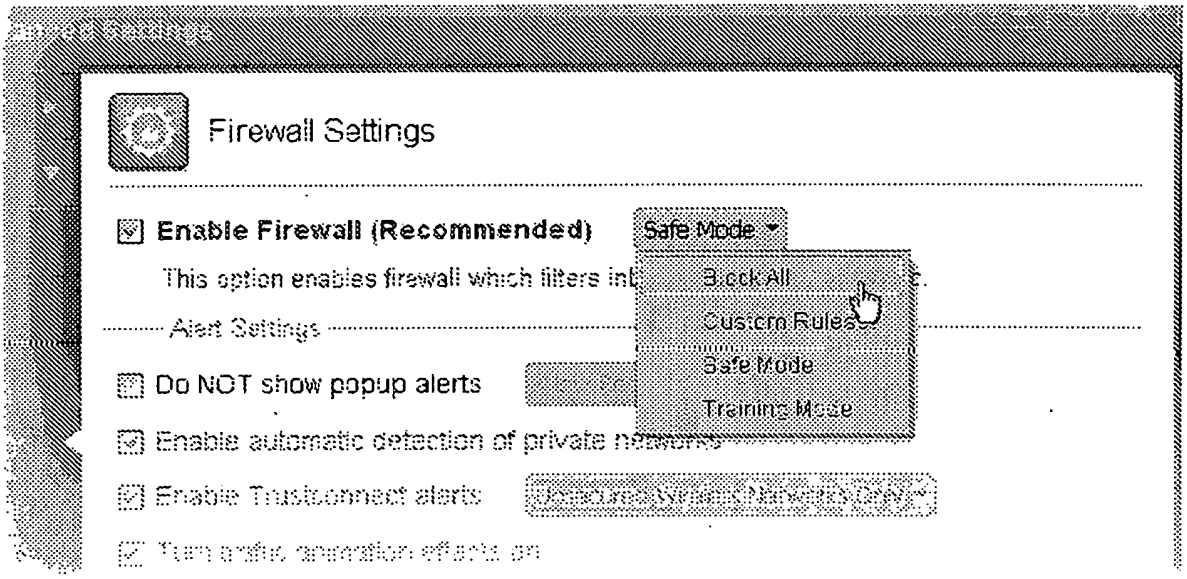


General Settings

- **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).

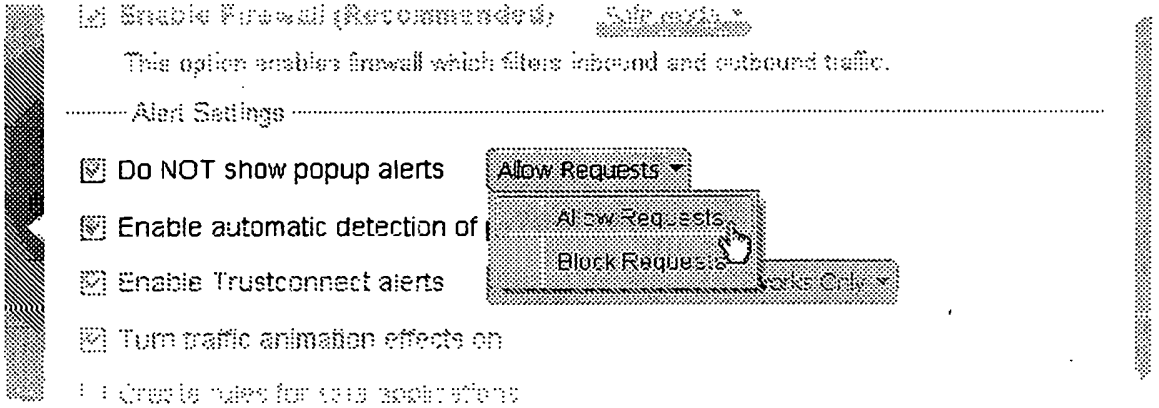
  If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This 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***)

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).

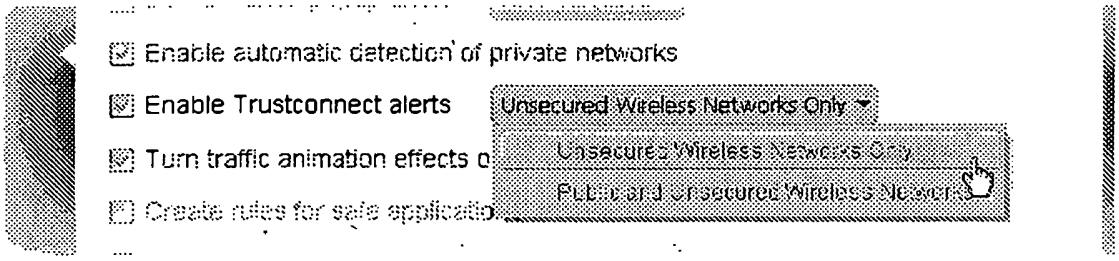


You can select the type of new network you are connected to, so that the firewall configuration is optimized for the type of connection. Comodo recommends users to leave this option at its default, enabled setting ***(Default = Enabled)***.

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.

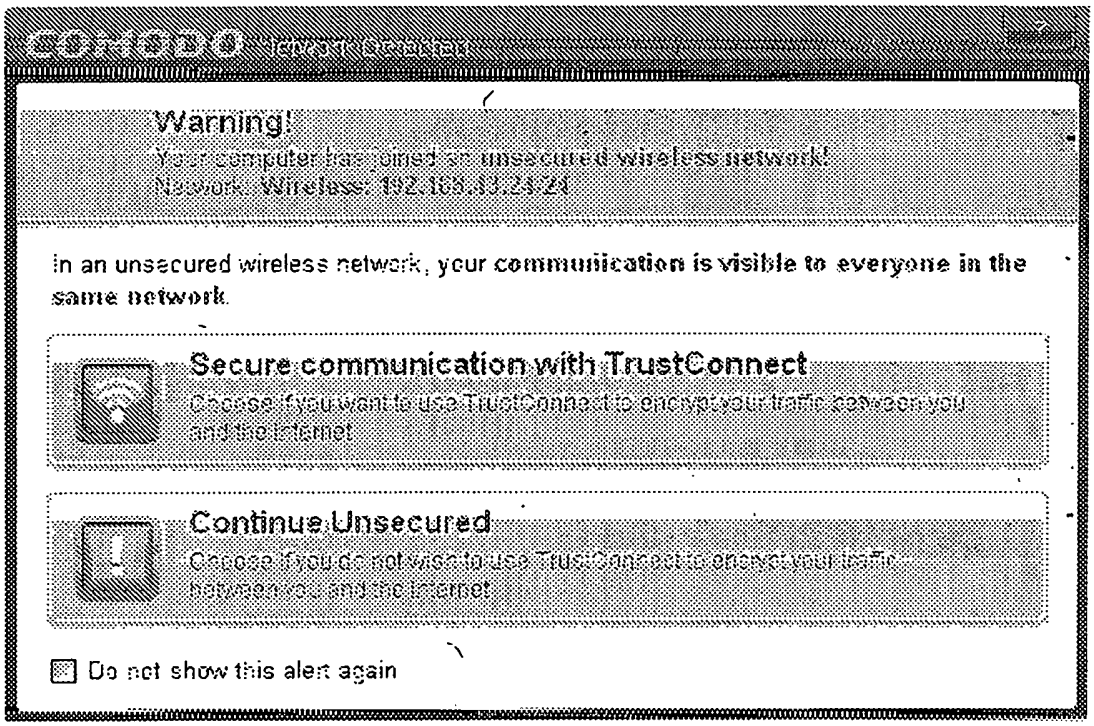
If selected, Comodo Firewall will display an alert if it detects you are connected to the Internet through an unsecured network.

(***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.

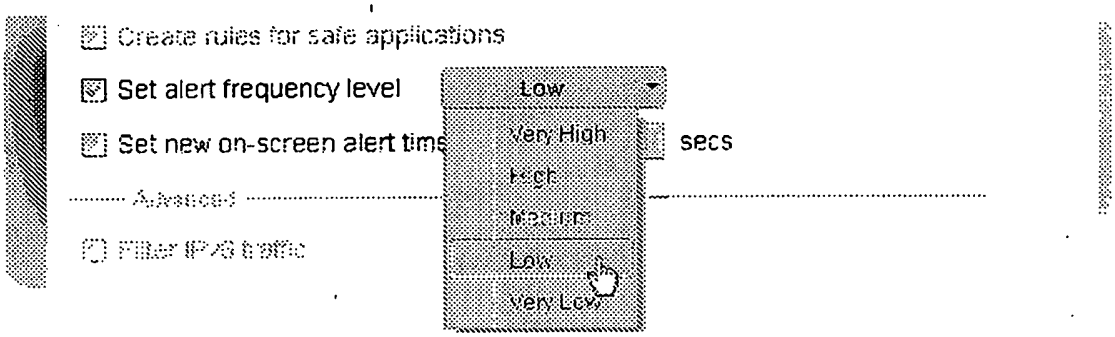
By default, CIS does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is

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.

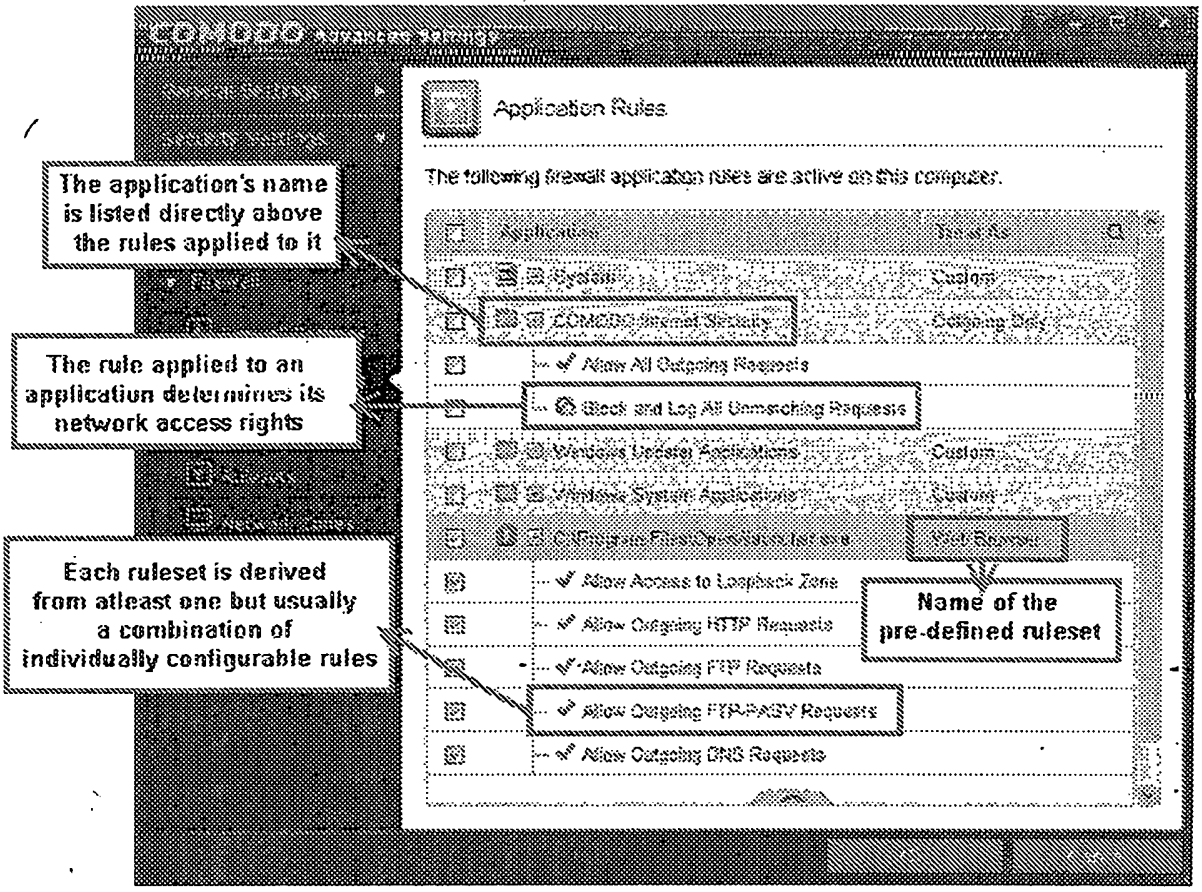
IPv6 on the other hand, uses 128 bits per address (delivering 3.4×1038 unique addresses) and is viewed as the only realistic, long term solution to IP address exhaustion. IPv6 also implements numerous enhancements that are not present in IPv4 - including greater security, improved support for mobile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

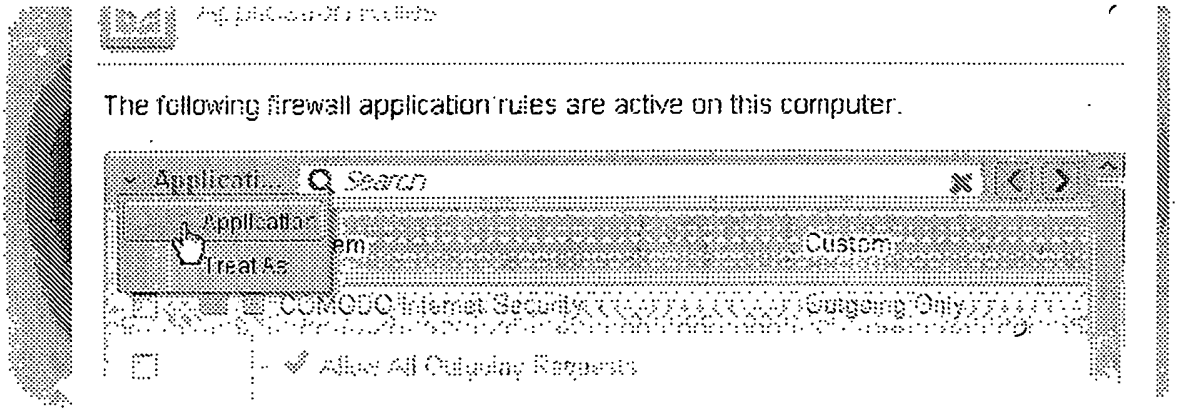
Whenever an application makes a request for internet or network access, Comodo Firewall allows or denies this request based upon the Firewall Ruleset that has been specified for that application. Firewall Rulesets are, in turn, made up from one or more individual network access rules. Each individual 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.

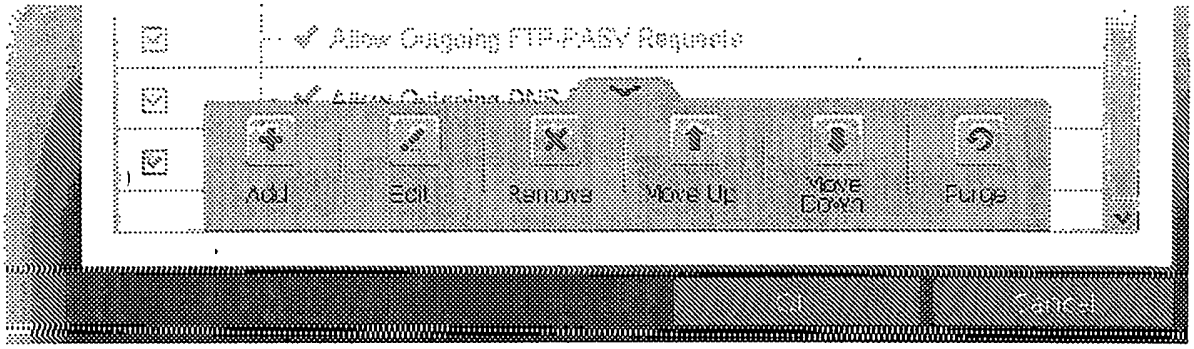
To use the search option, click the search icon at the far right in the column header.



- 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.

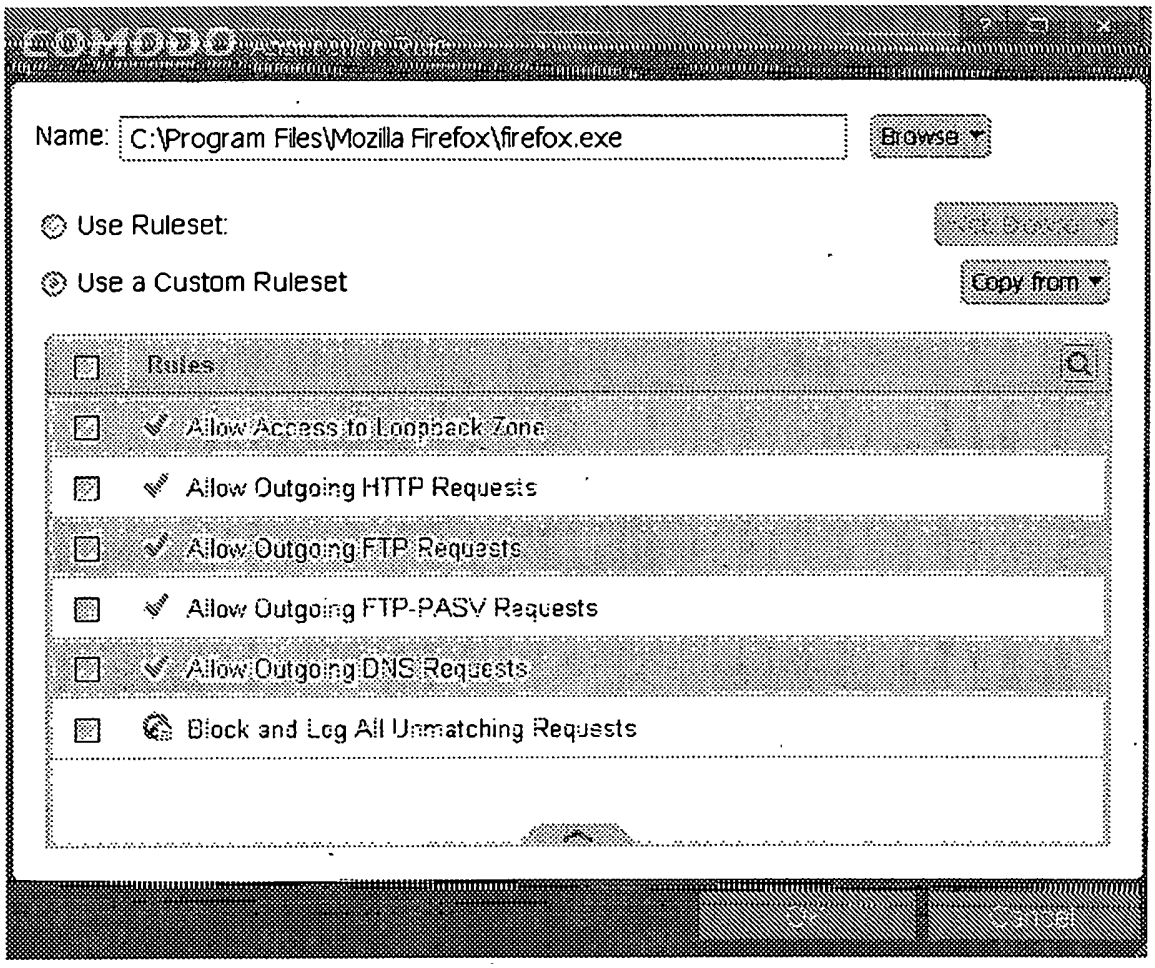
Although each ruleset can be defined from the ground up by individually configuring its constituent rules, this practice would be time consuming if it had to be performed for every single program on your system. For this reason, Comodo Firewall contains a selection of predefined rulesets according to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

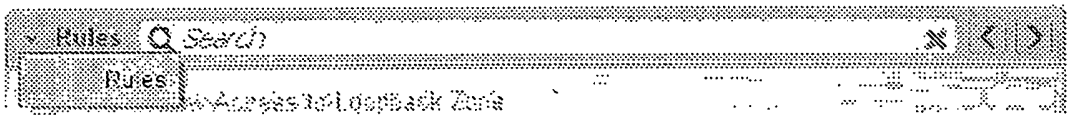


Comodo Firewall applies rules on a *per packet* basis and applies the **first** rule that matches that packet type to be filtered (see Understanding Firewall Rules for more information). If there are a number of rules in the list relating to a packet type then one nearer the top of the list is applied.

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.

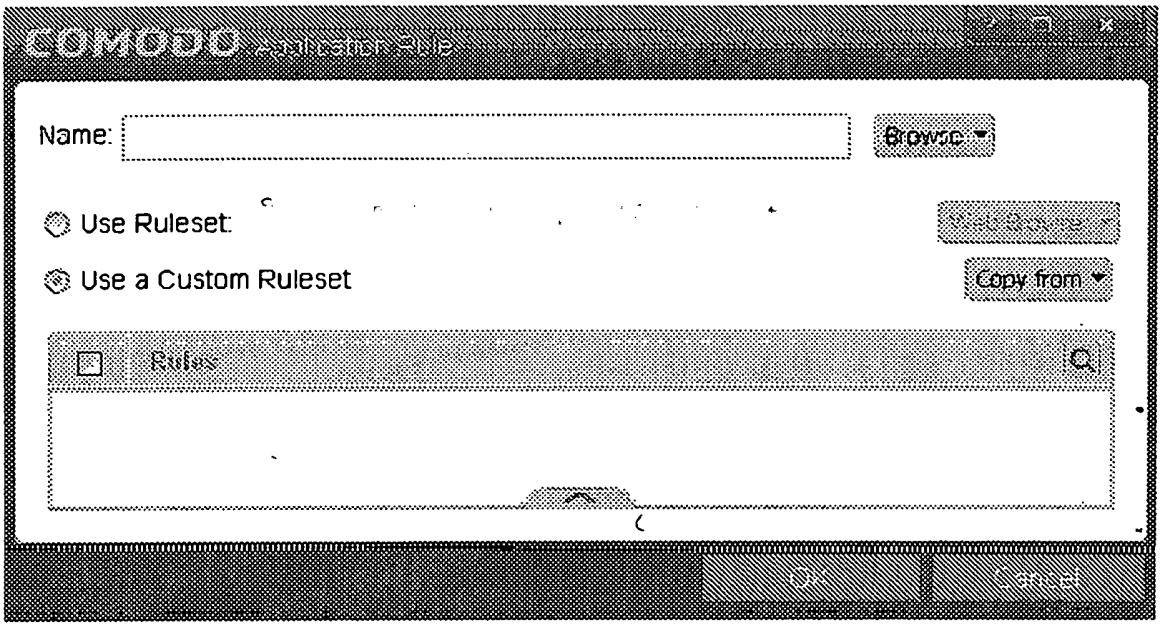
Creating and Modifying Firewall Rulesets

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.

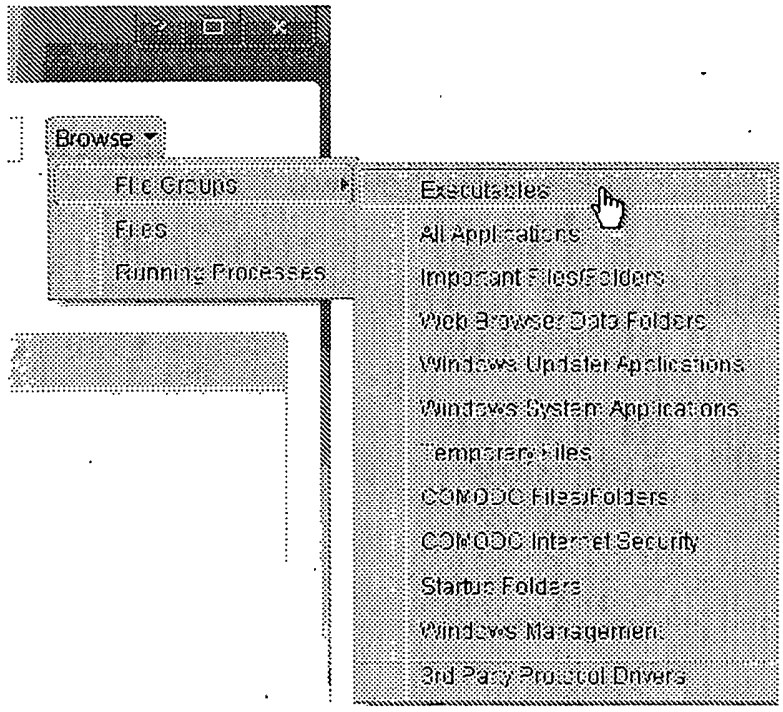
Step 1 - Select the application that you wish the ruleset is to be applied

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.

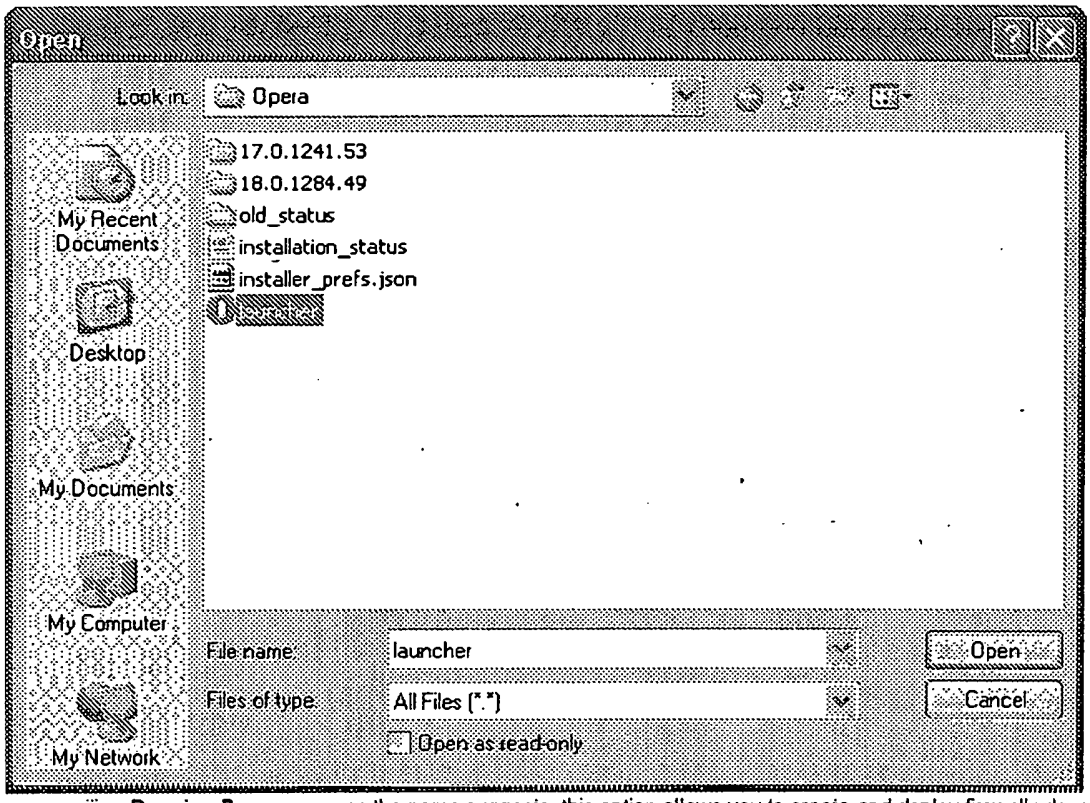


You now have 3 methods available to choose the application for which you wish to create a ruleset - File Groups, Files and

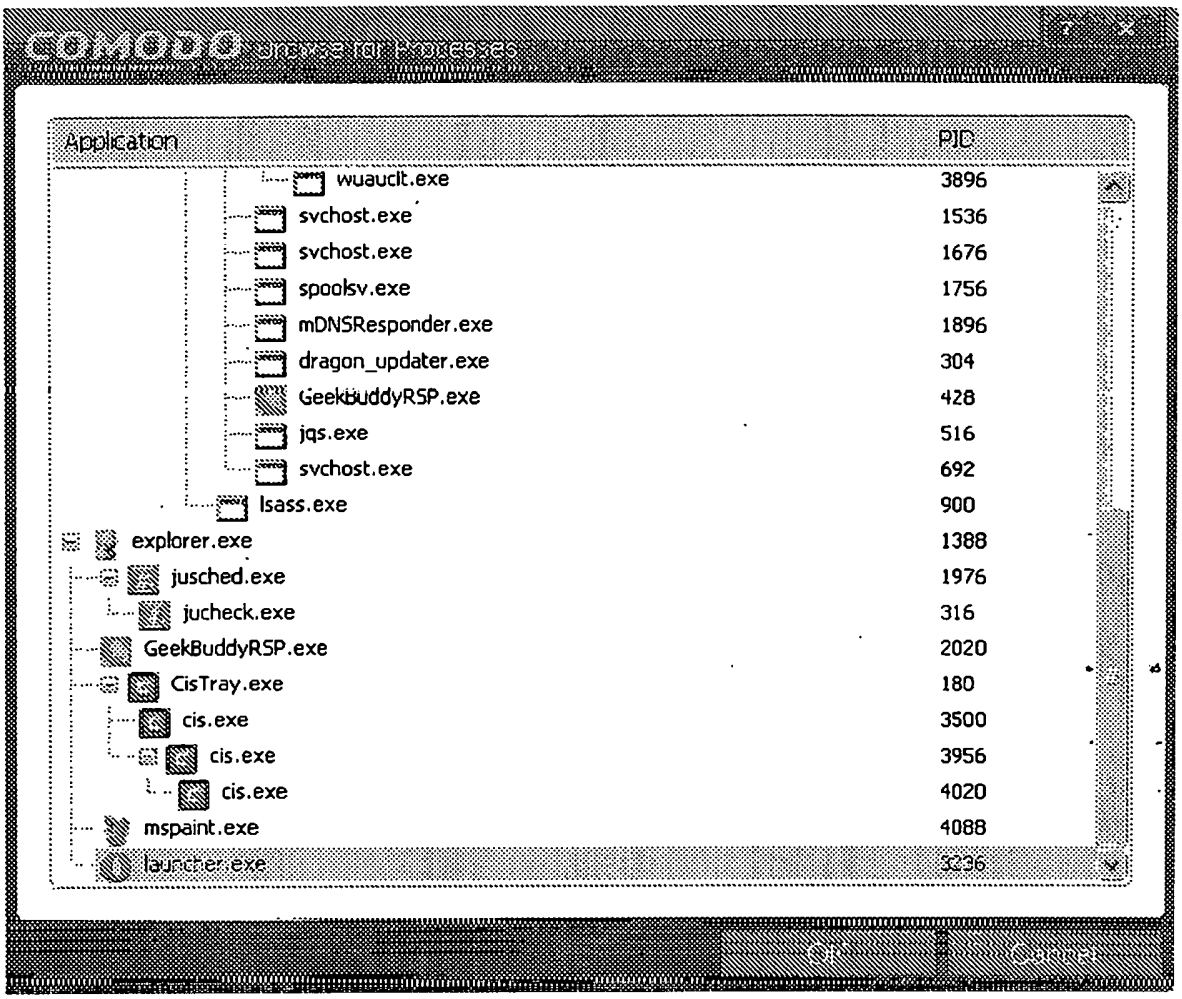
Running Processes and

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.



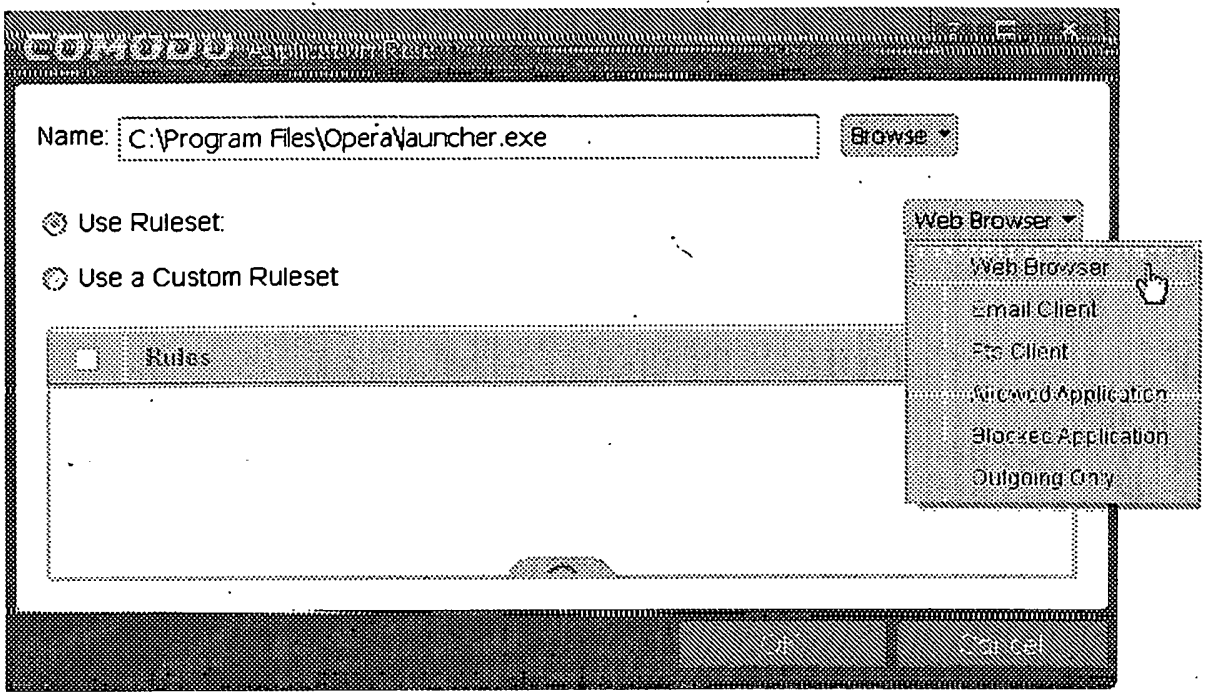
You can choose an individual process (shown above) or the parent process of a set of running processes. Click 'OK' to confirm your choice.

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

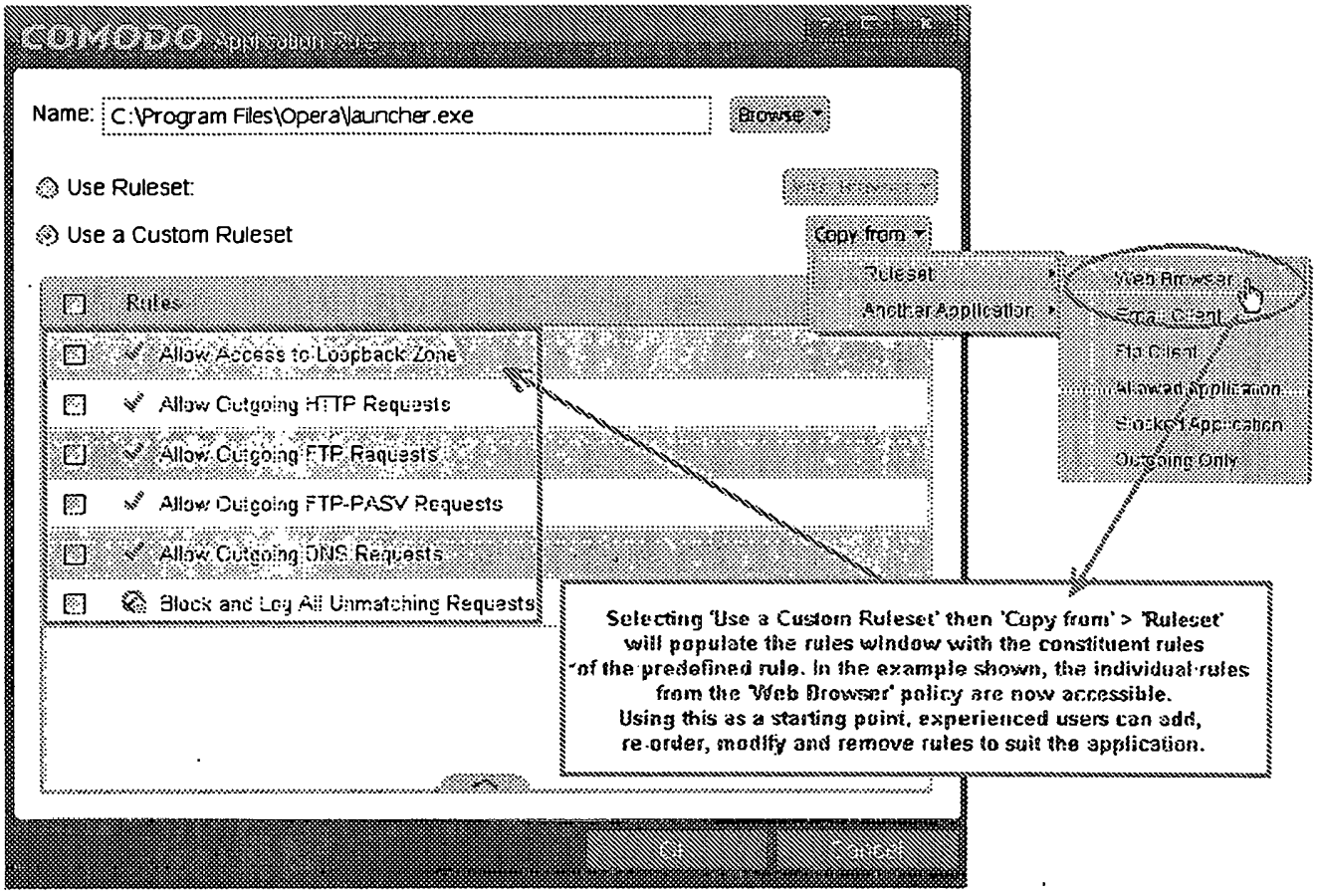
There are two broad options available for creating a ruleset that applies to an application - Use a Predefined Ruleset or Use a Custom Ruleset.

- **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)***.



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

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



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

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

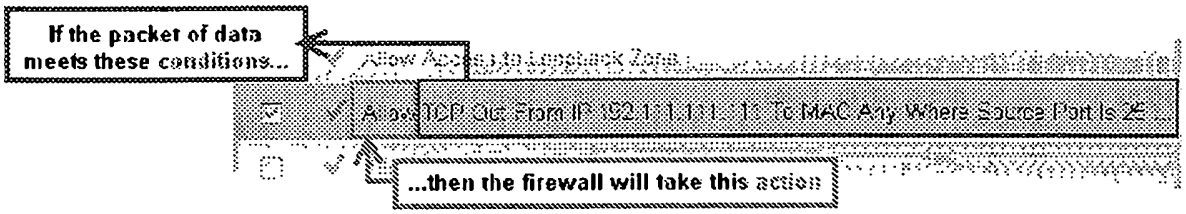
General Tips:

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

Understanding Firewall Rules

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

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



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

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

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

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

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

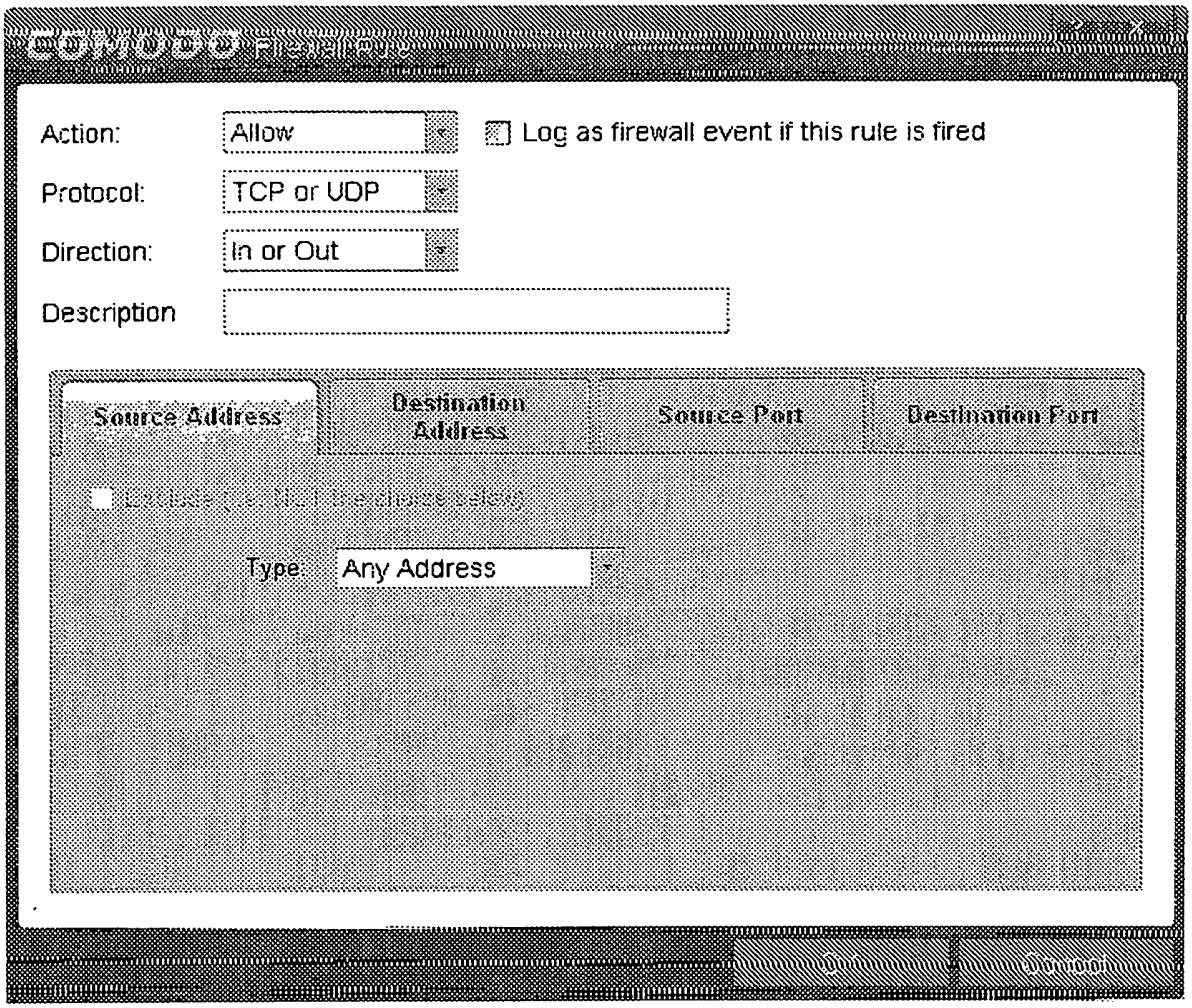
Once a rule is applied, Comodo Firewall monitors all network traffic relating to the chosen application and take the specified action if the conditions are met. Users should also see the section 'Global Rules' to understand the interaction between Application Rules and Global Rules.

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

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

Adding and Editing a Firewall Rule

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



General Settings

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

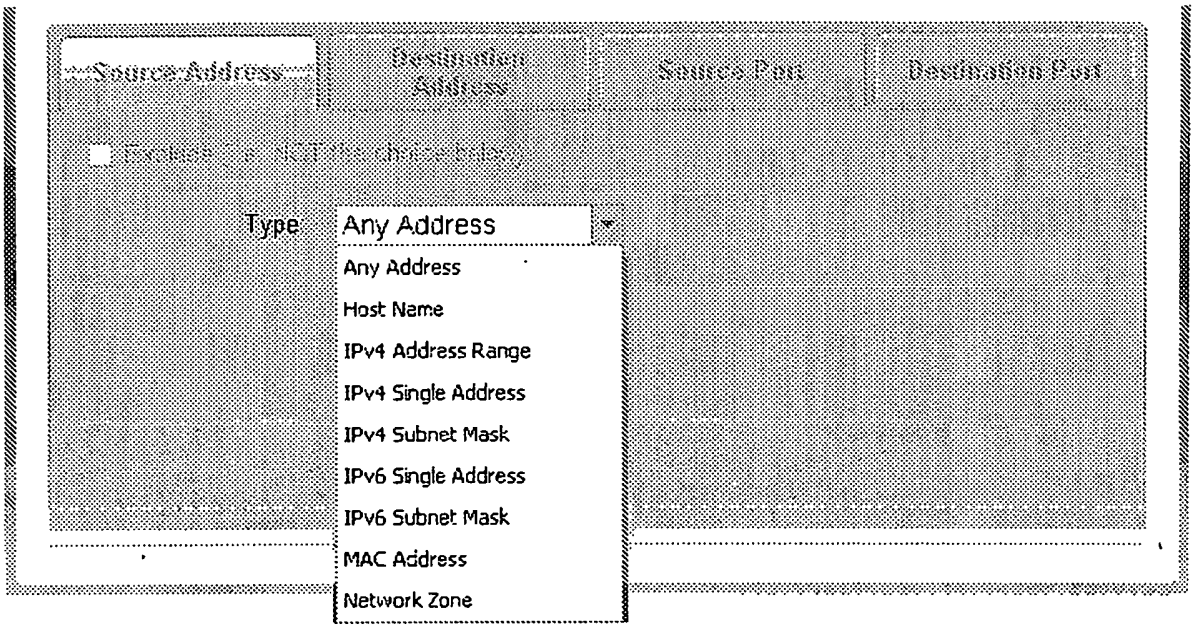
Note: Your choice here alters the choices available to you in the tab structure on the lower half of the interface.

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

Protocol

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

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



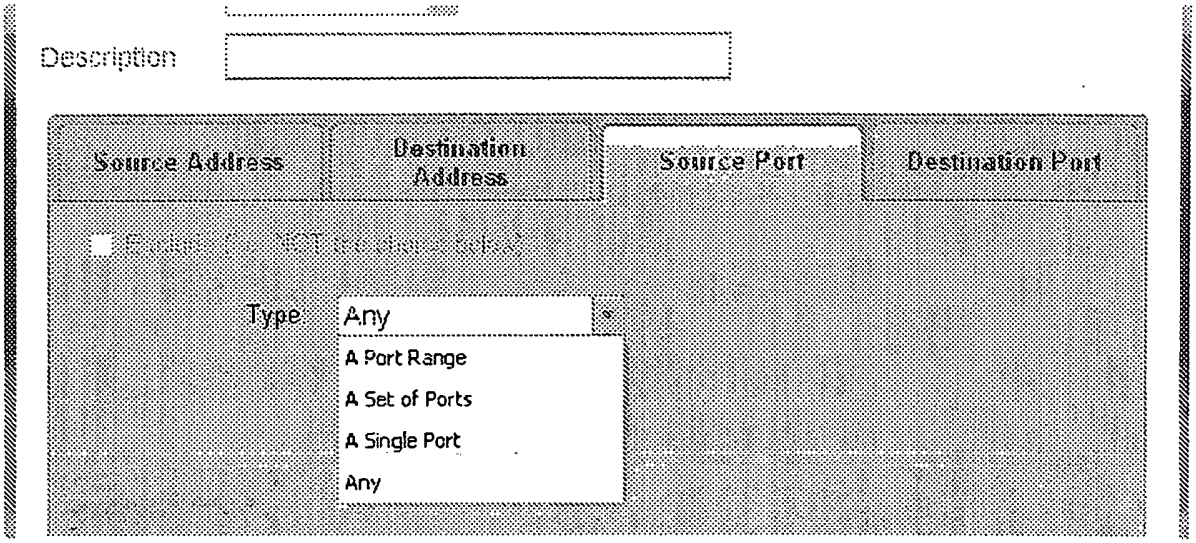
Source Address and Destination Address:

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

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

Source Port and Destination Port:

Enter the source and destination Port in the text box.



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

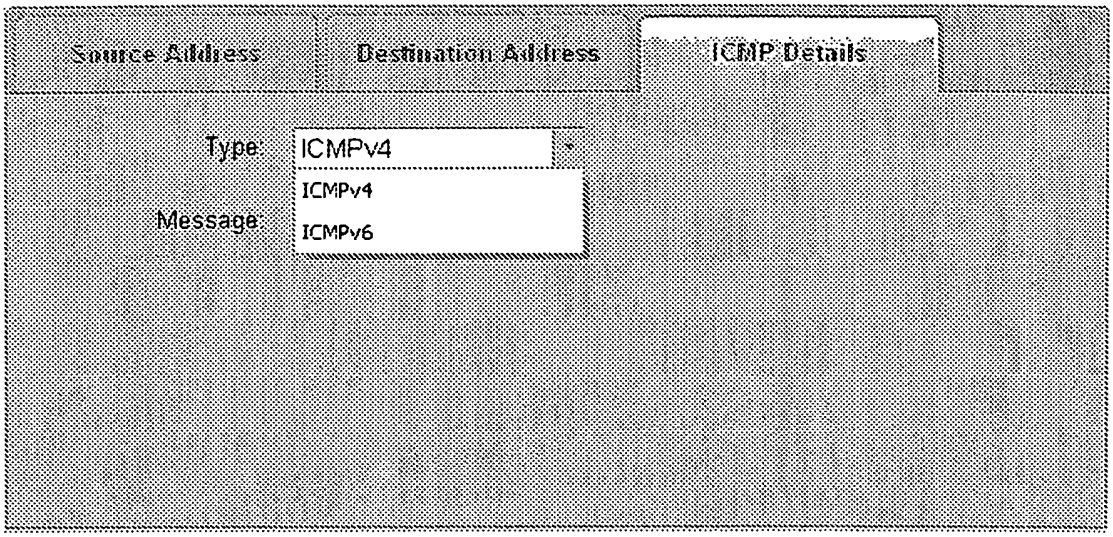
ii. **ICMP**

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.

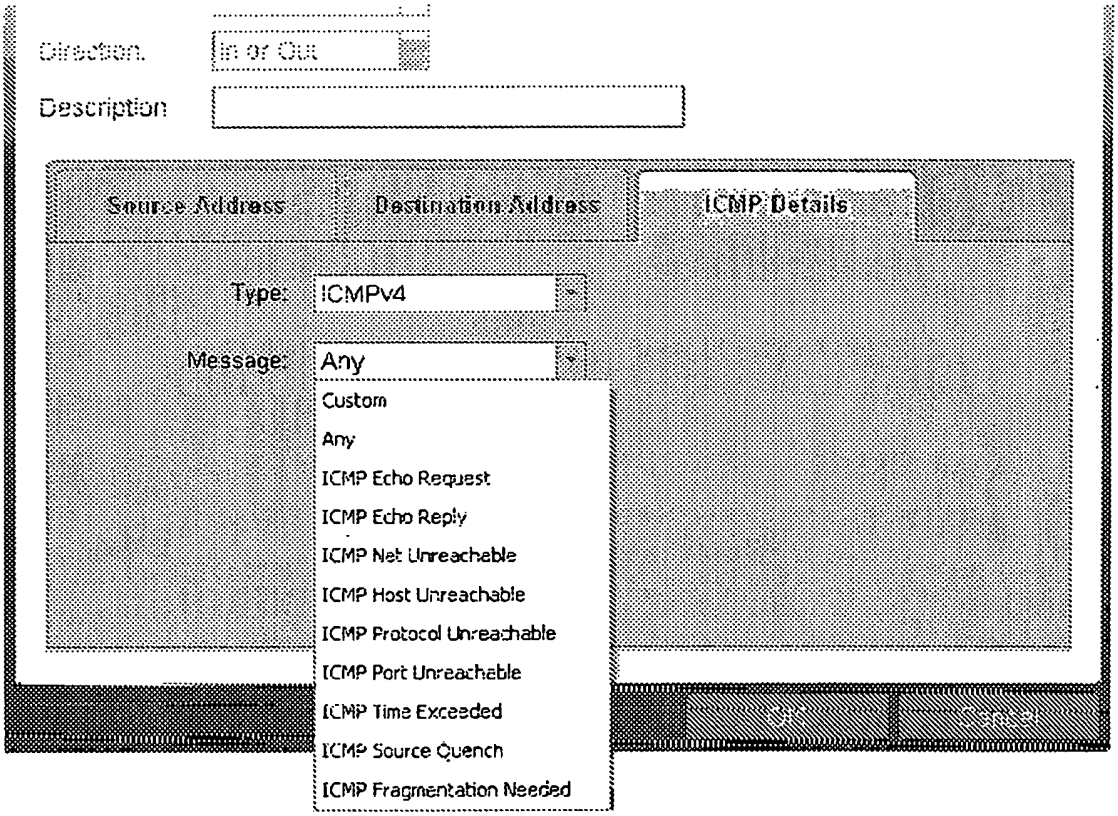
- **ICMP Details**

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.



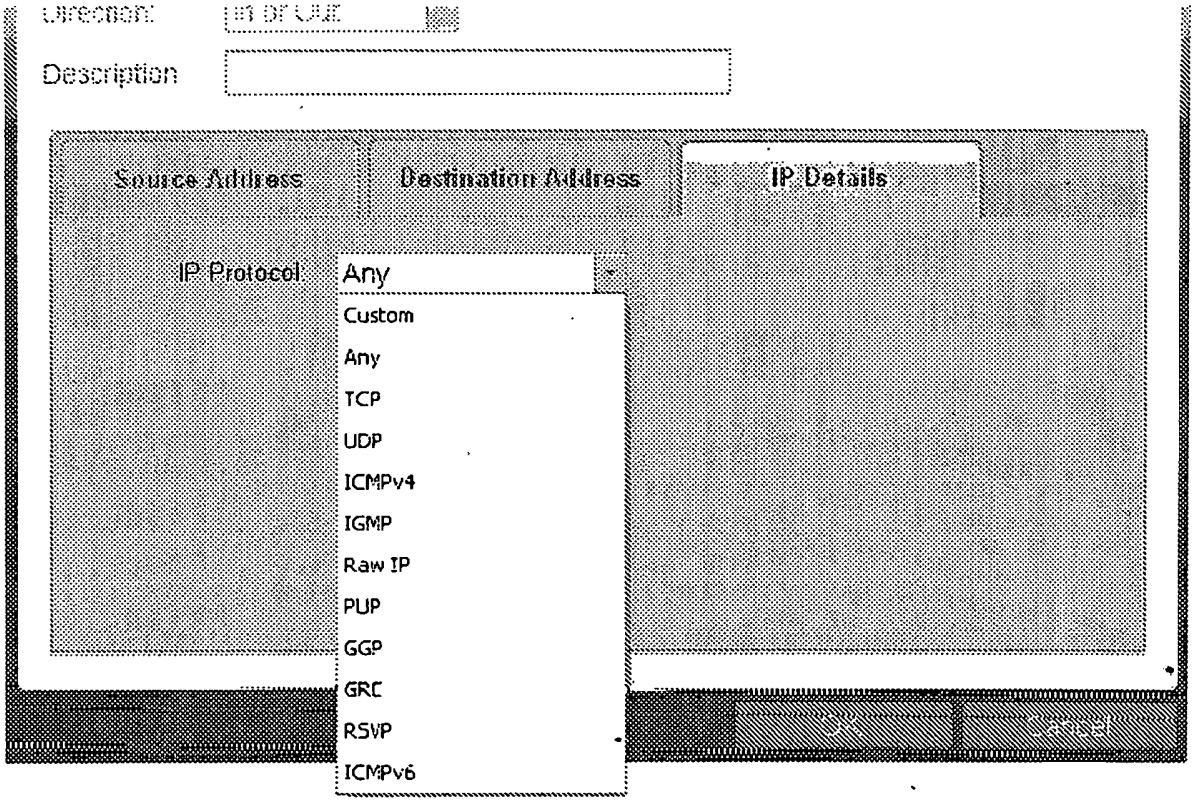
3. Specify ICMP Message , Types and Codes. An ICMP message includes a Message that specifies the type, that is, the format of the ICMP message.



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**

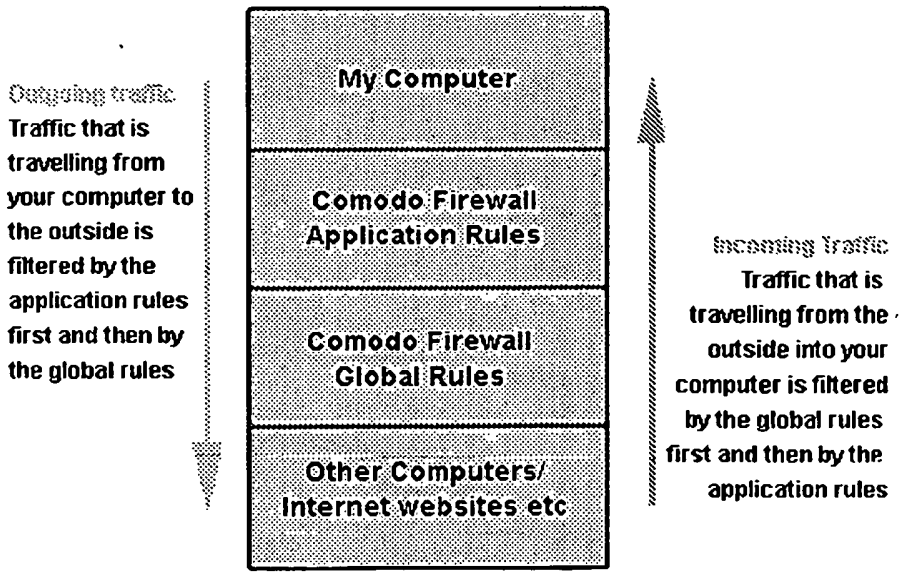
Select the types of IP protocol that you wish to allow, from the ones that are listed.

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.

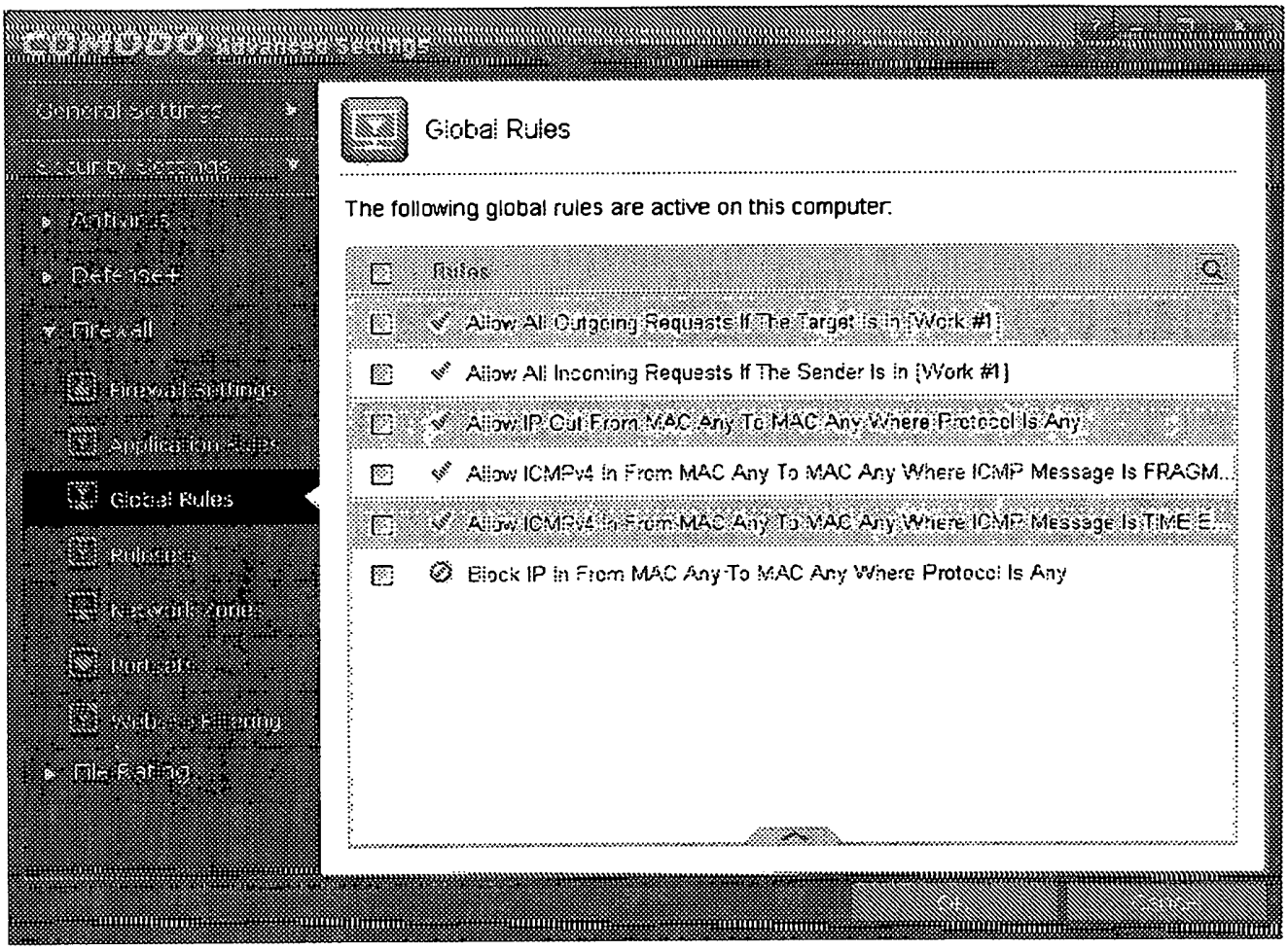
- For Outgoing connection attempts, the application rules are consulted first and then the global rules second.
- For Incoming connection attempts, the global rules are consulted first and then the application rules second.



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.

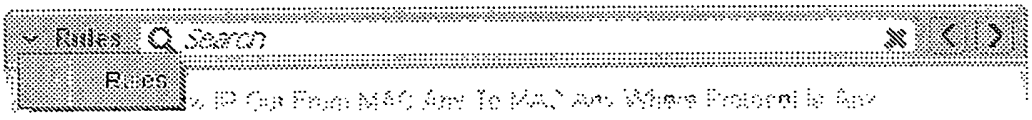
Global Rules are mainly, but not exclusively, used to filter incoming traffic for protocols other than TCP or UDP.

- 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.

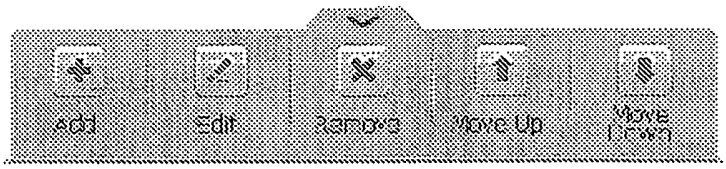
To use the search option, click the search icon at the far right in the column header.



- 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'.

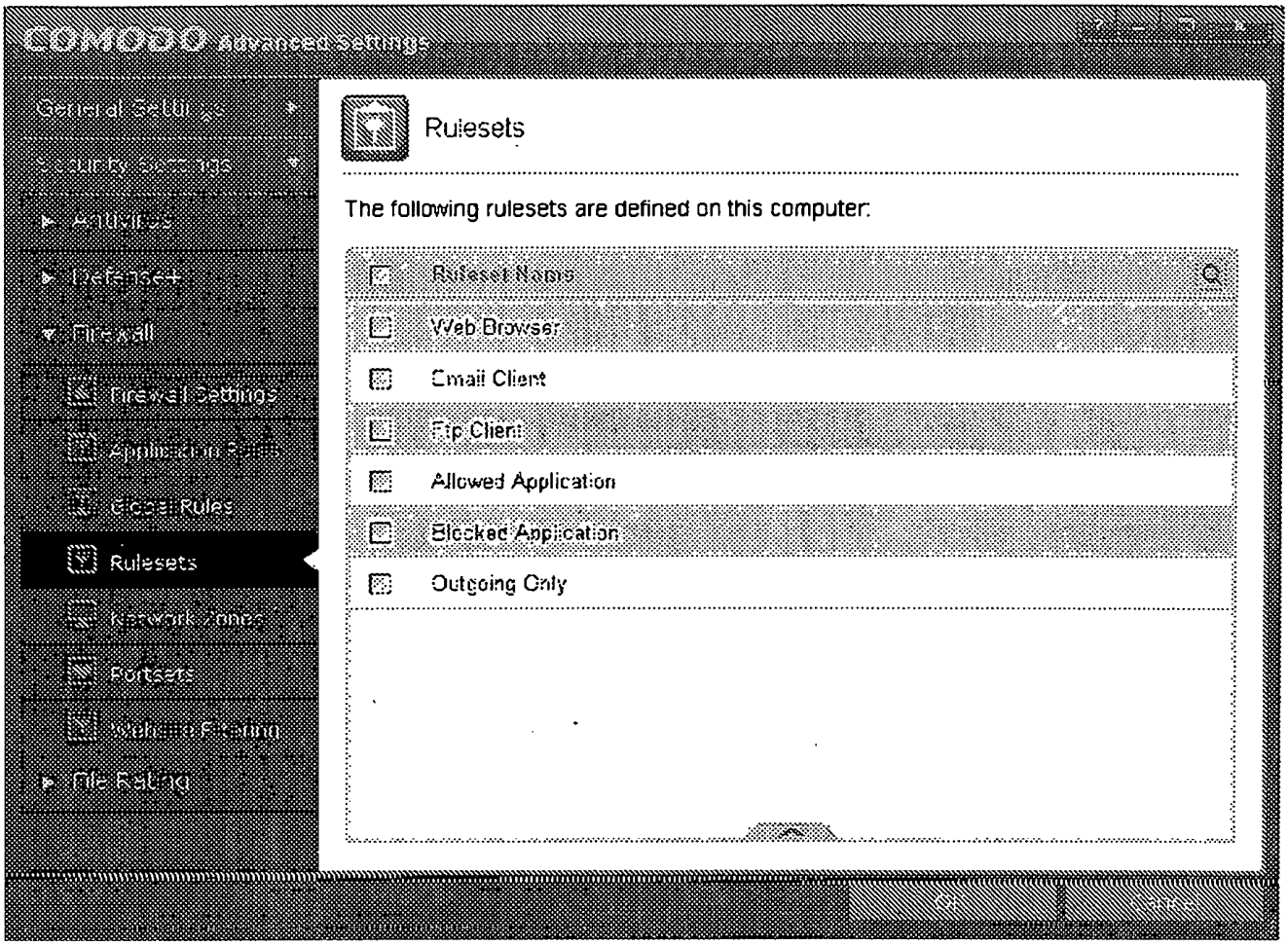
- See Application Rules for an introduction to the rule setting interface.
- See Understanding Firewall Rules for an overview of the meaning, construction and importance of individual rules.
- See Adding and Editing a Firewall Rule for an explanation of individual rule configuration.

6.2.3.4. Firewall Rule Sets

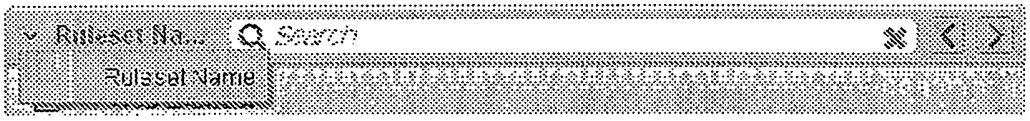
As the name suggests, a firewall Ruleset is a set of one or more individual Firewall rules that have been saved and which can be re-deployed on multiple applications. This section contains advice on the following:

- 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).

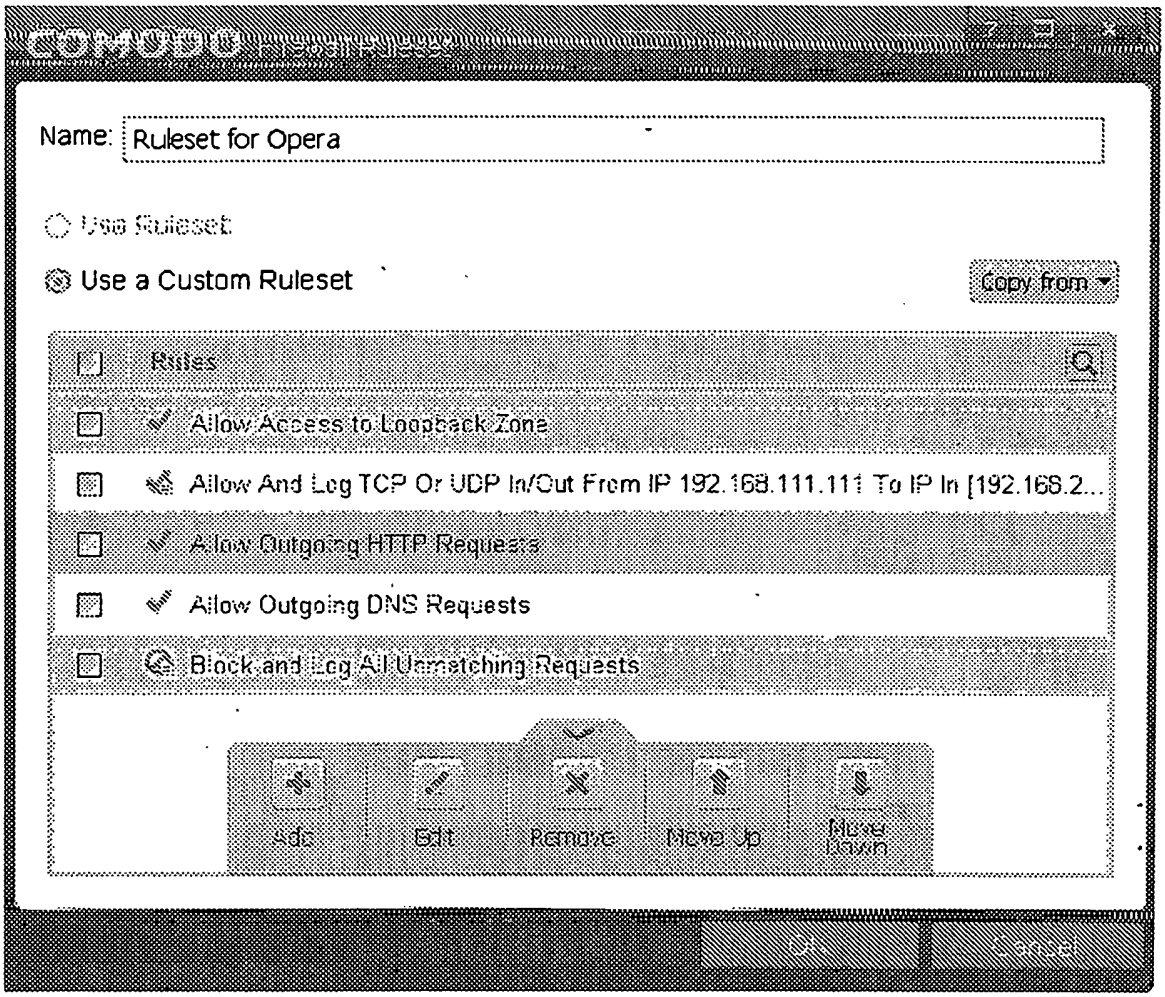
Creating a new ruleset

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.

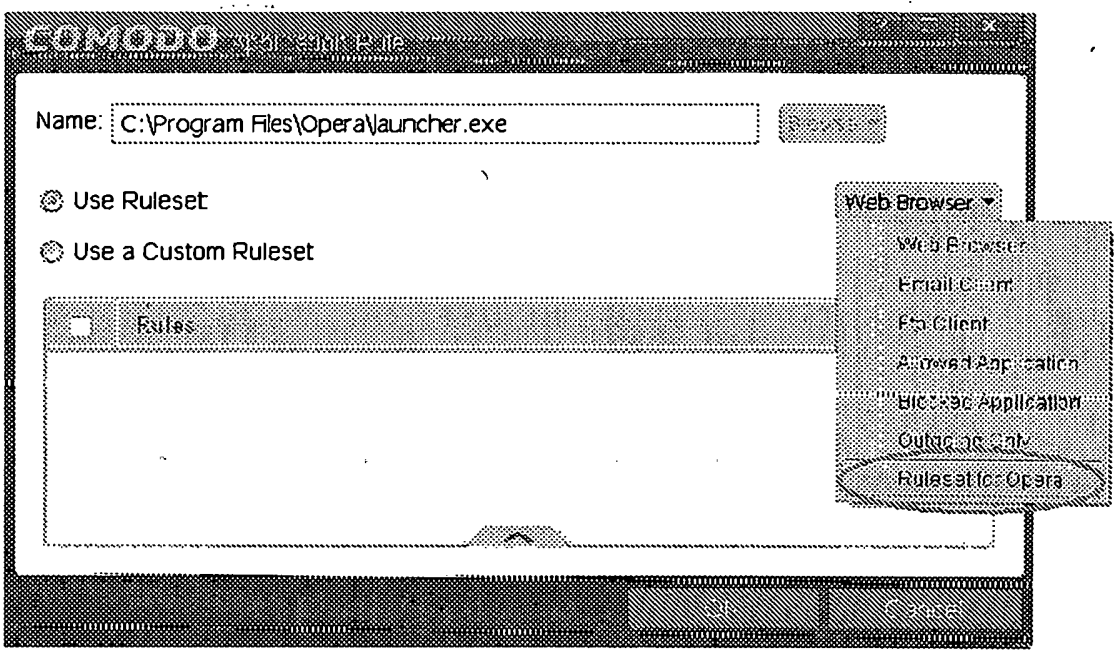
To add a new Ruleset

- 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.



To view or edit an existing predefined Ruleset

- Double click on the Ruleset Name in the list

  or

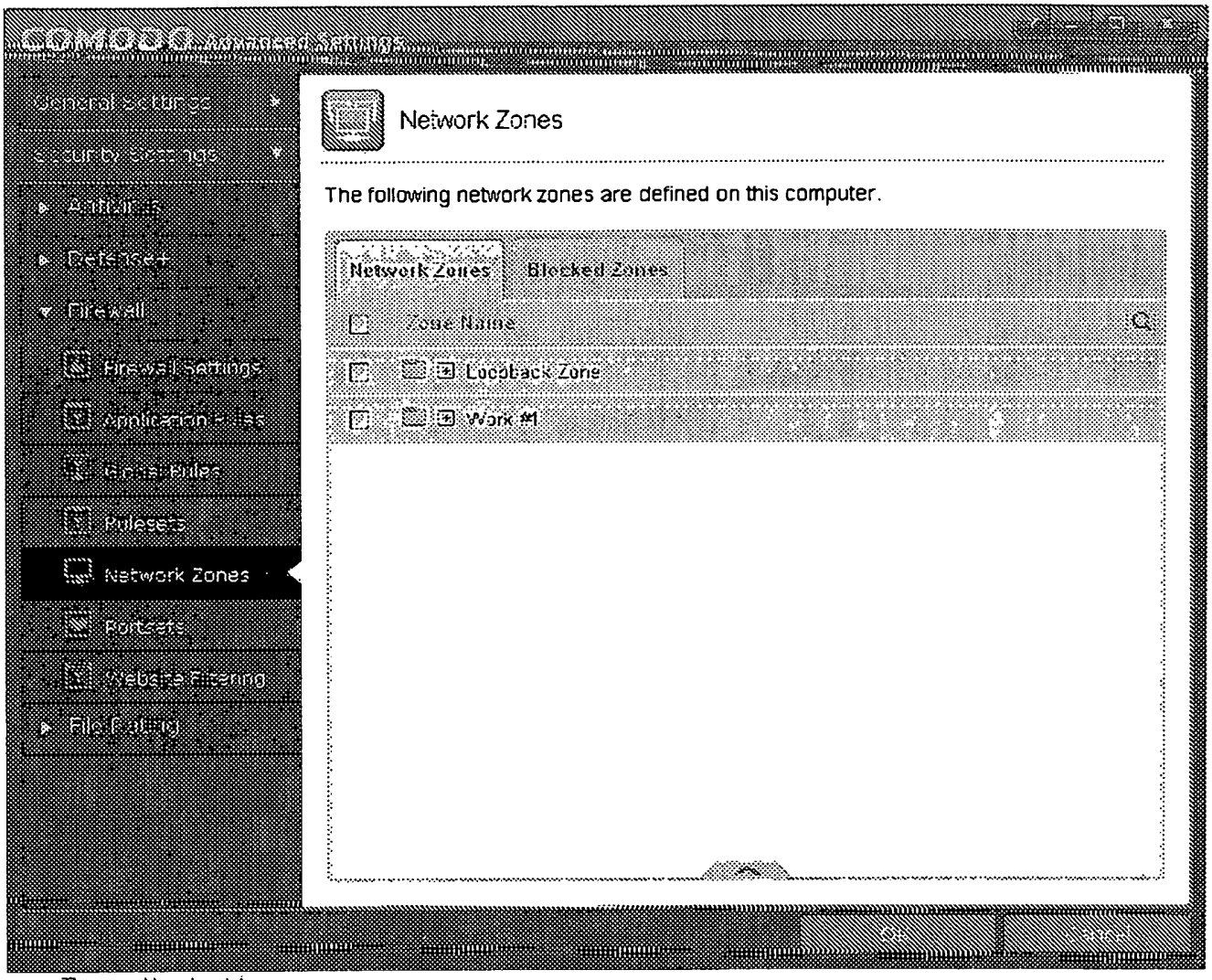
- Select the Ruleset Name, click the handle from the bottom center and select Edit from the options
- Details of the process from this point on can be found here.

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.



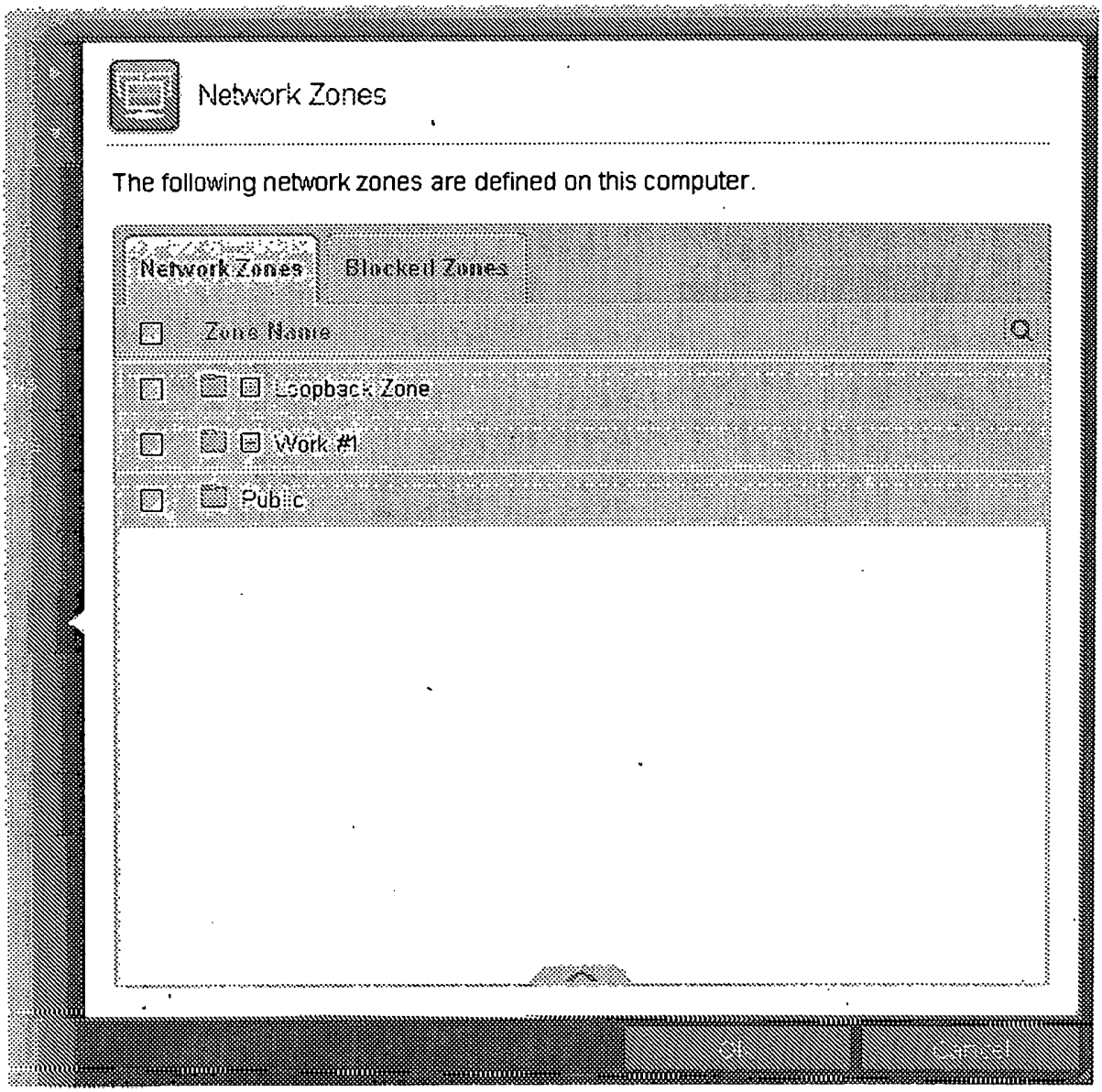
The panel has two tabs:

- 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.

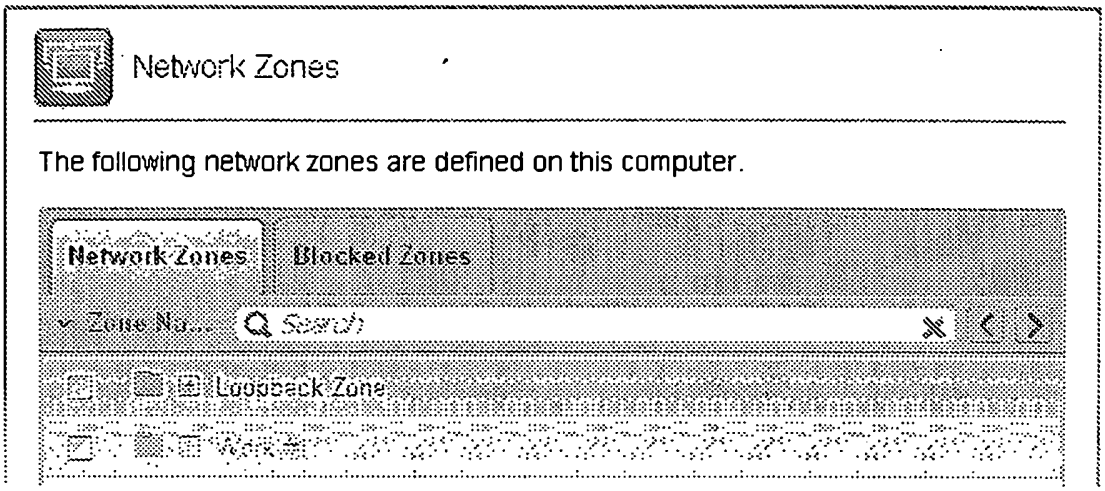
Note 2: A network zone can be designated as 'Trusted' and allowed access from the 'Manage Network Connections' interface (An example would be your home computer or network).

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.

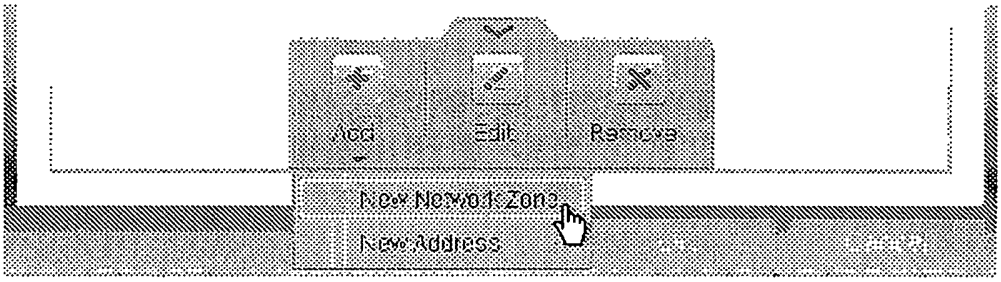
Defining a new Network Zone

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.

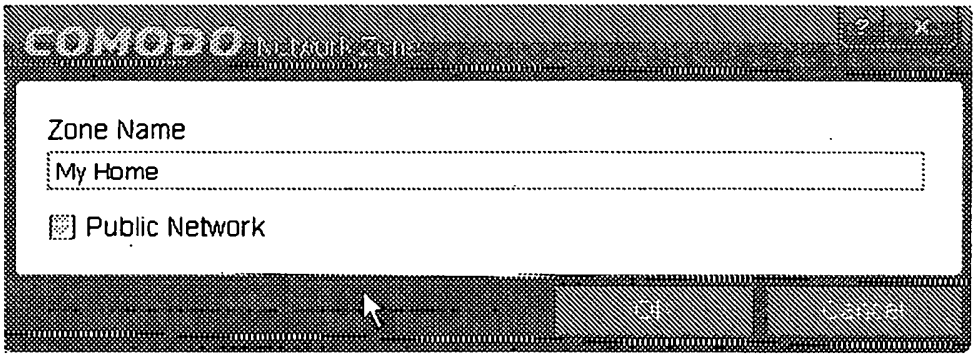
Step 1 - Define a name for the zone

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



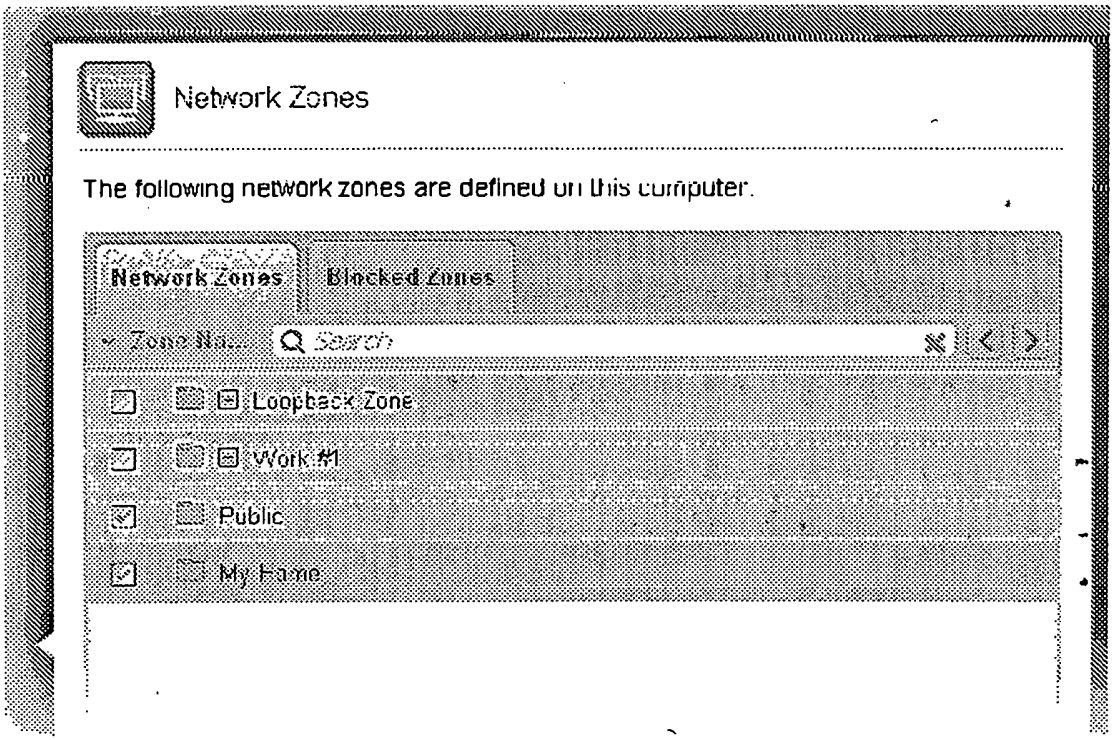
A dialog box will appear, prompting you to specify a name for the new zone.

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.

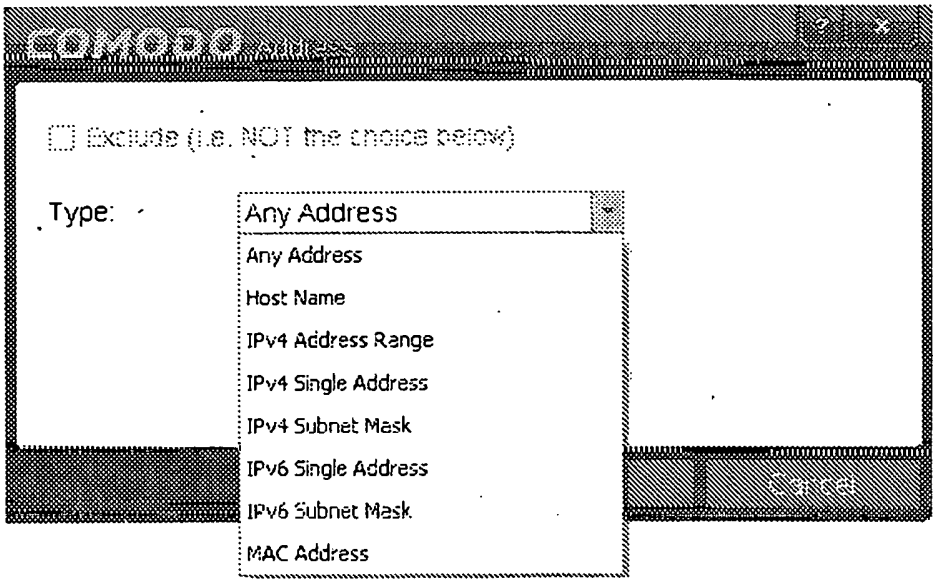
   This adds the name of your new zone to the Network Zones list.



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.

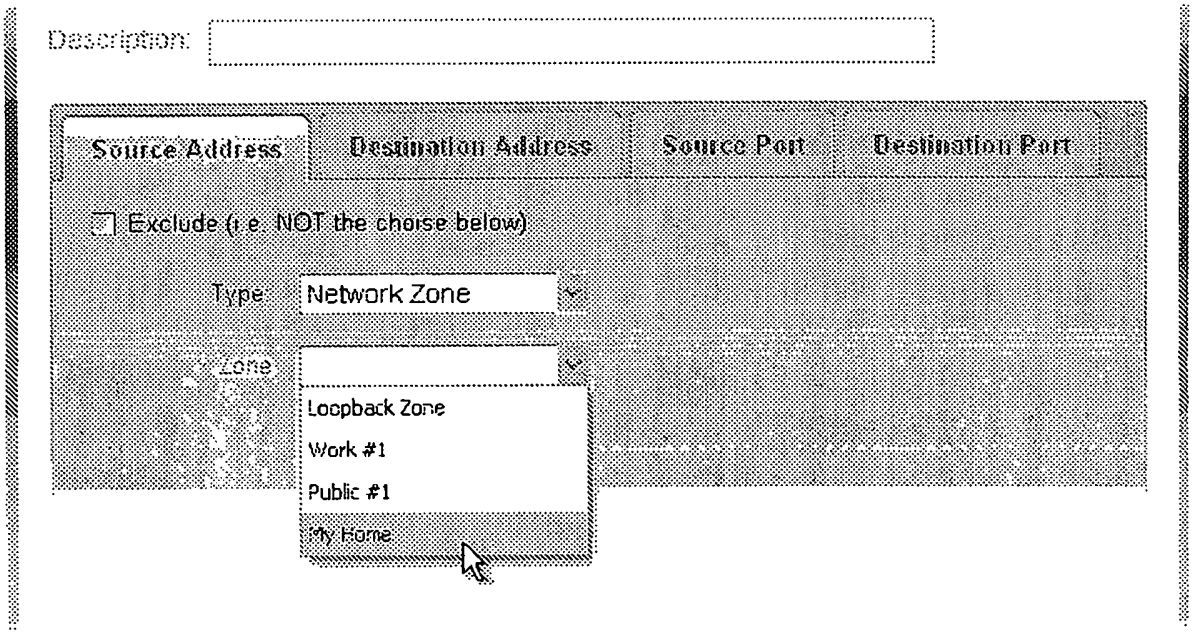
- Exclude (i.e. NOT the choice below): The opposite of what you specify is applicable.

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:

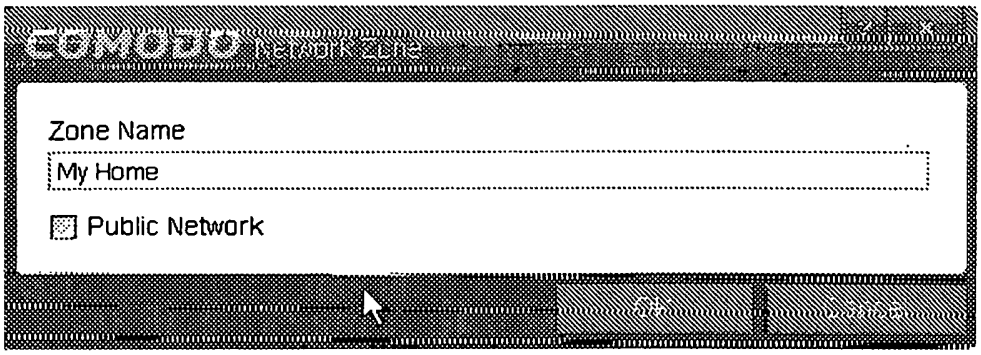
- Quickly called as 'Zone' when creating or modifying a Firewall Ruleset



- 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.

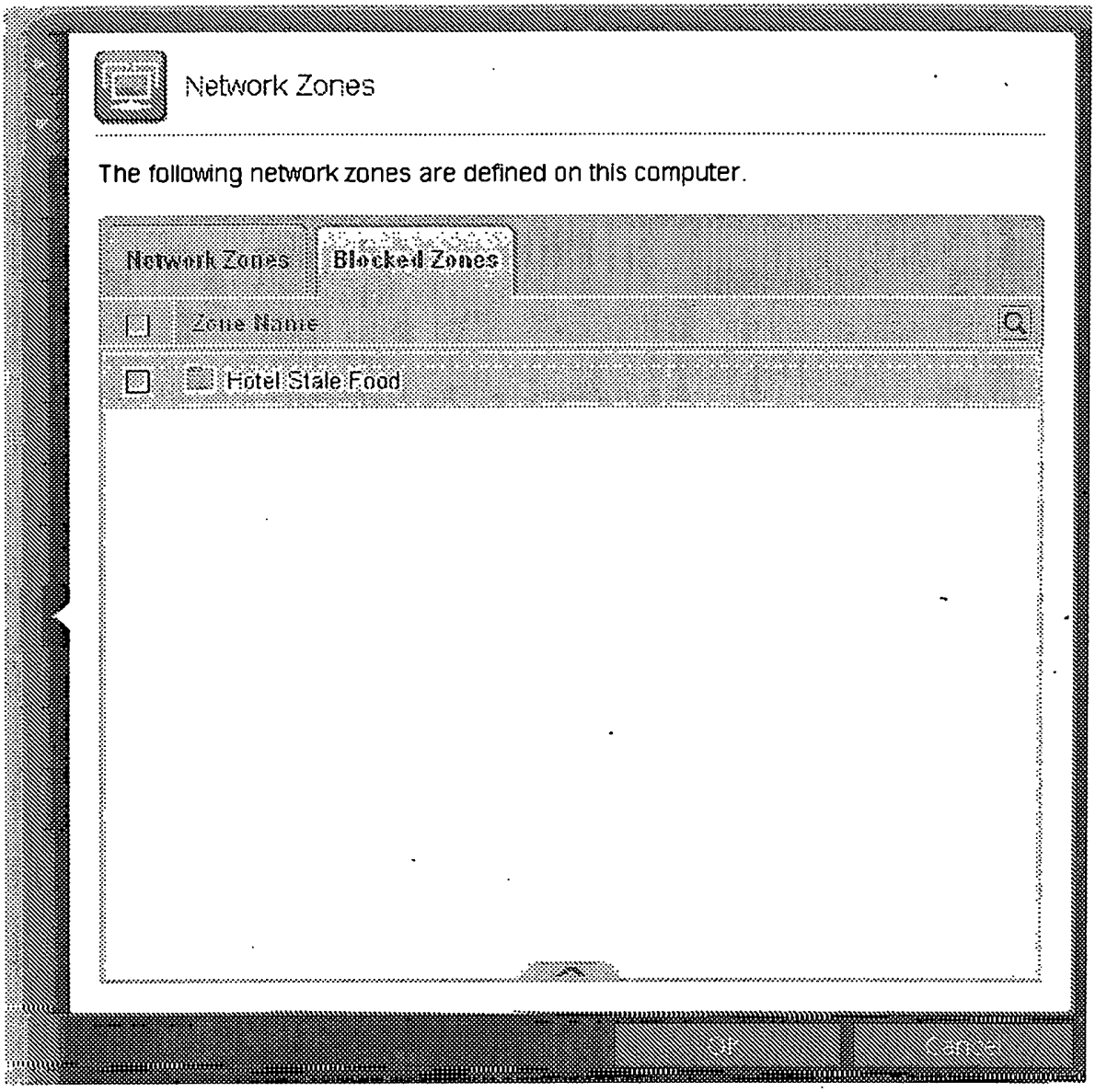
To modify or change the existing address in a zone

- 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:

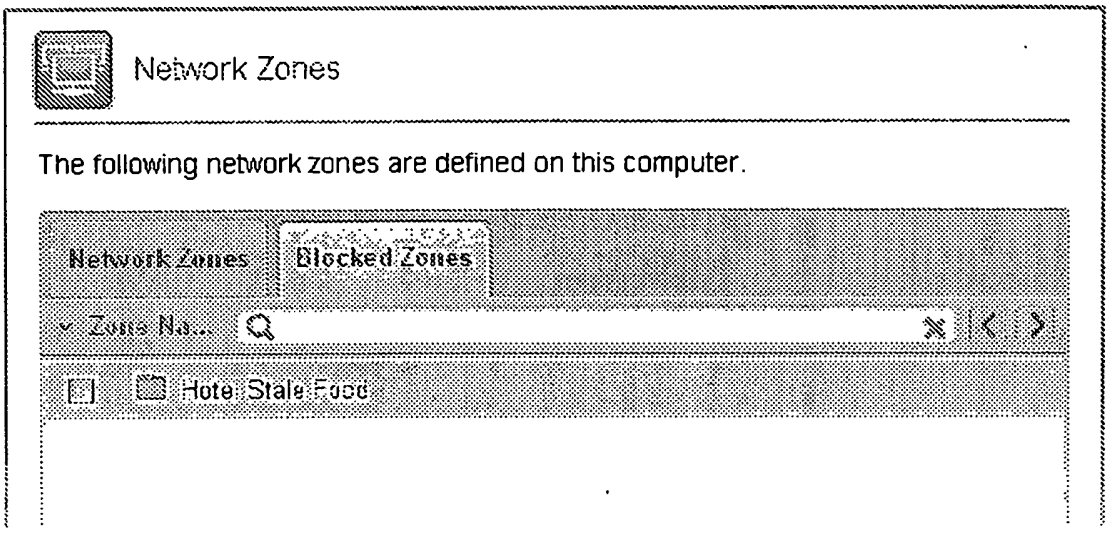
- Deny access to a specific network by selecting a pre-existing network zone and designating it as blocked
- Deny access to a specific network by manually defining a new blocked zone

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.

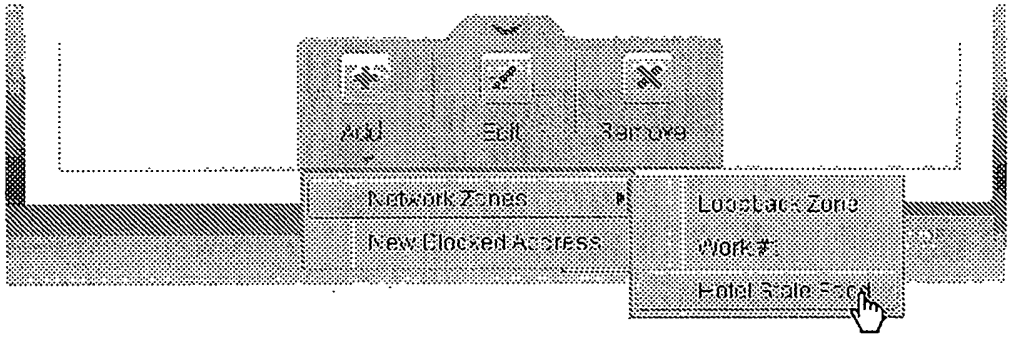
You can use the search option to find a blocked zone in the list by clicking the search icon at the far right in the column header.



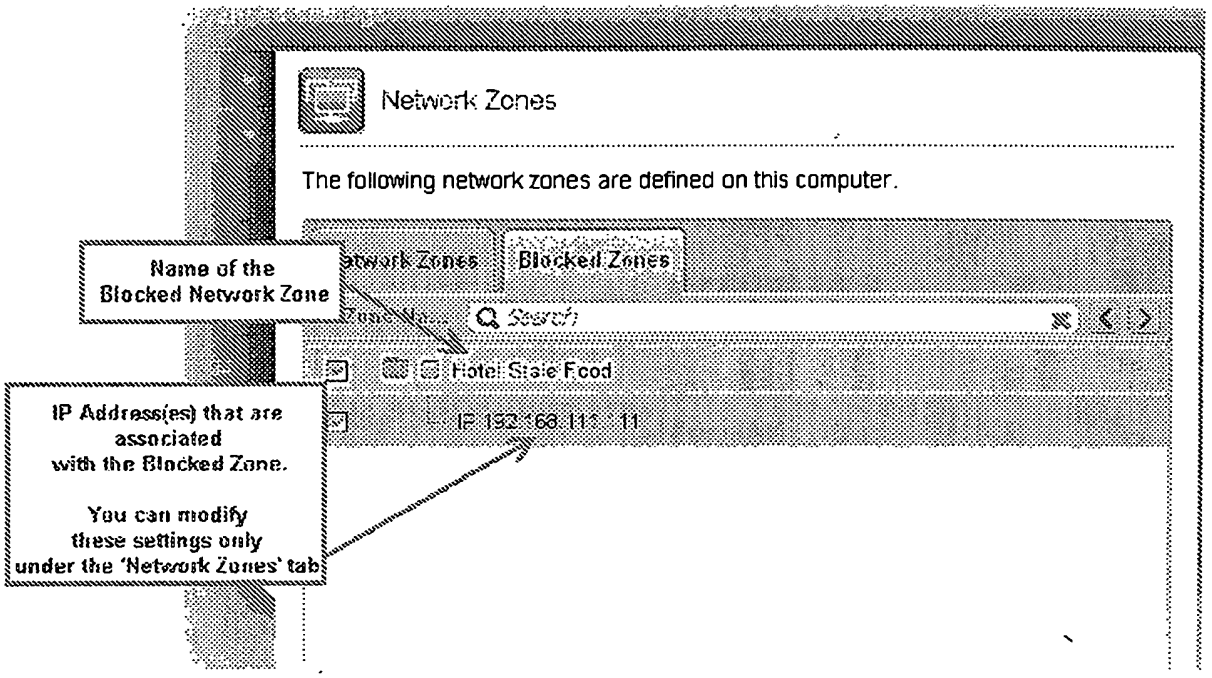
- Enter the name of the zone to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the icon in the search field to close the search option.

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.

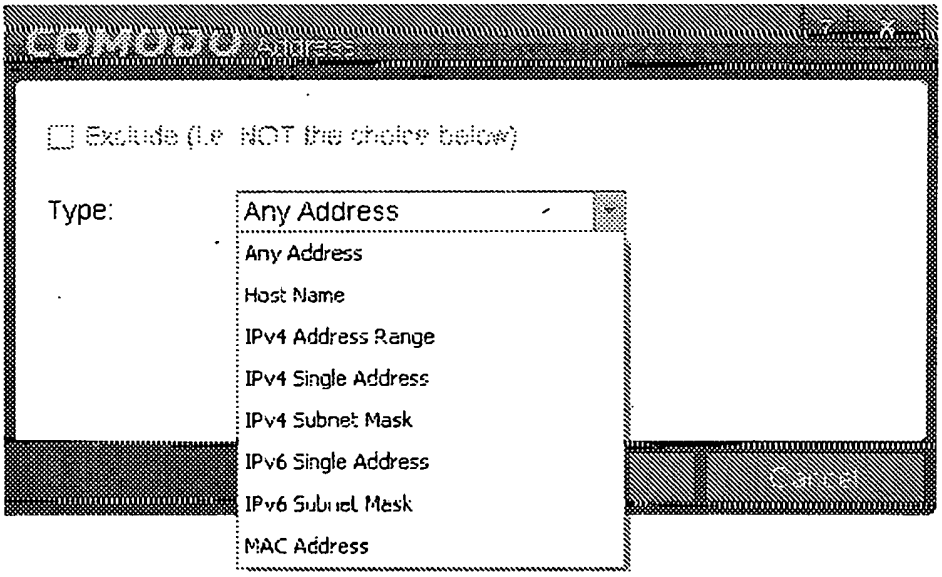


3. Click 'OK' to confirm your choice. All traffic intended for and originating from computer or devices in this zone are now blocked.

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.

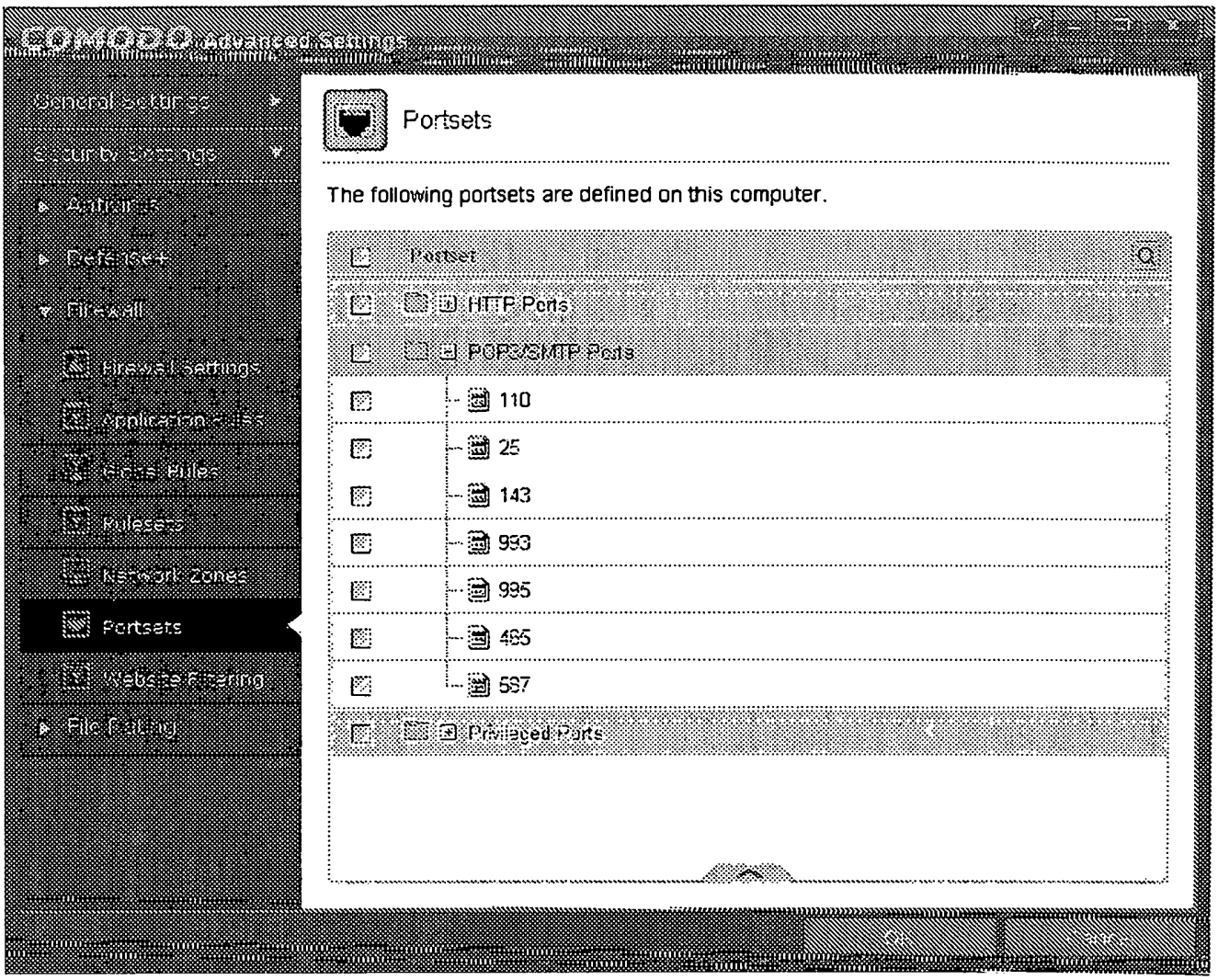
2. Select the address to be blocked and click OK

   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.

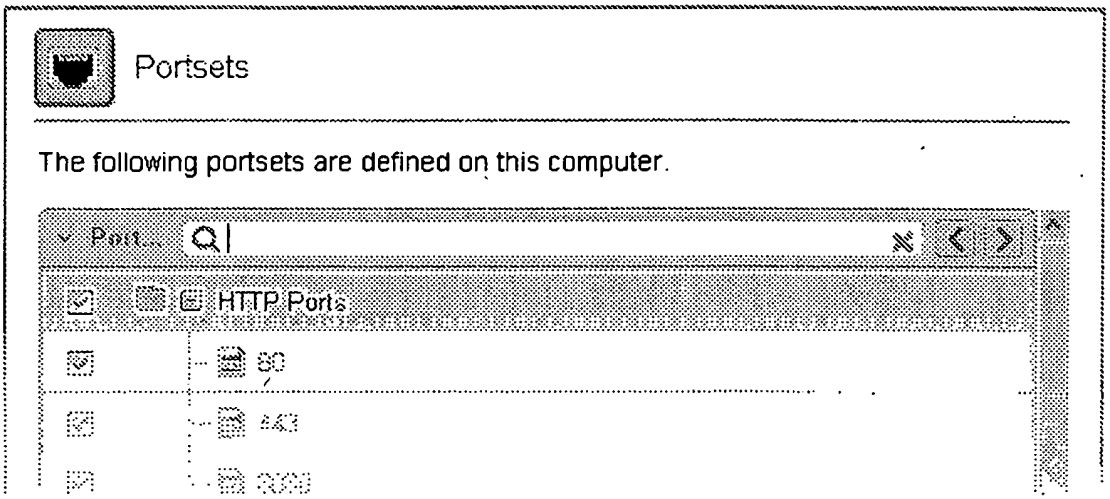
- The Port Sets panel enables you to view and manage pre-defined port sets and t add new port sets
- The Port Sets panel can be accessed by clicking Security Settings > Firewall > Portsets from the Advanced Tasks interface



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.



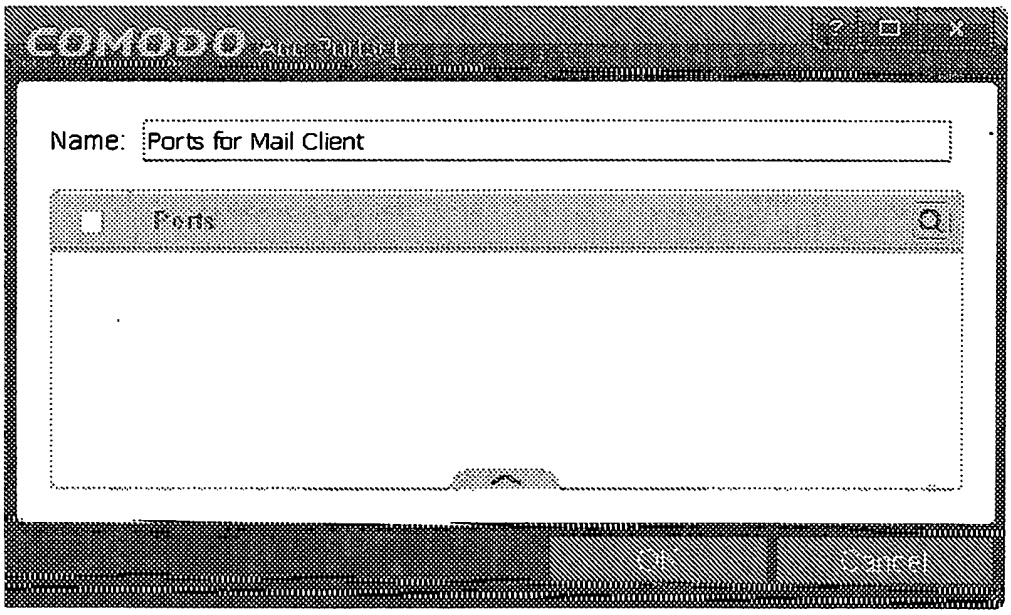
- Enter the name of the port set to be searched in full or part in the search field.
- Click the right or left arrow at the far right of the column header to begin the search.
- Click the icon in the search field to close the search option.

Defining a new Port Set

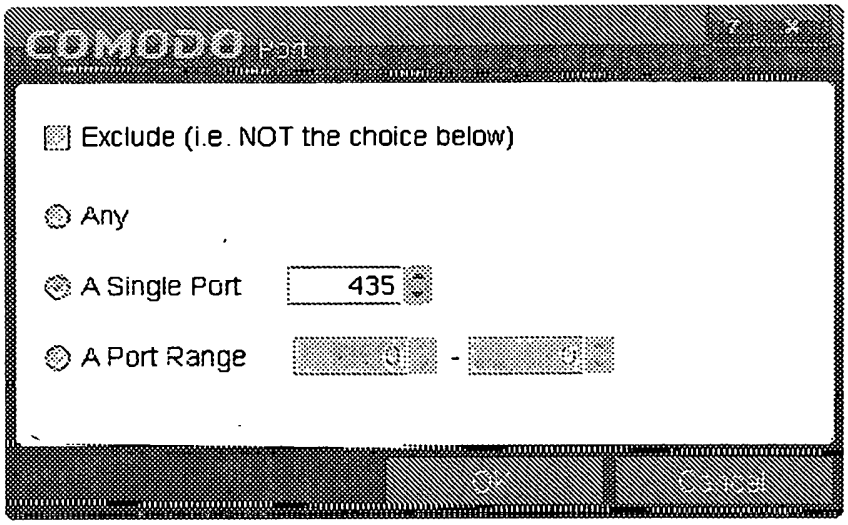
You can create new portsets and allow access to them for applications, with the access privileges specified through Application Rule interface. Refer to 'Creating or Modifying Firewall Rules' for more details.

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.

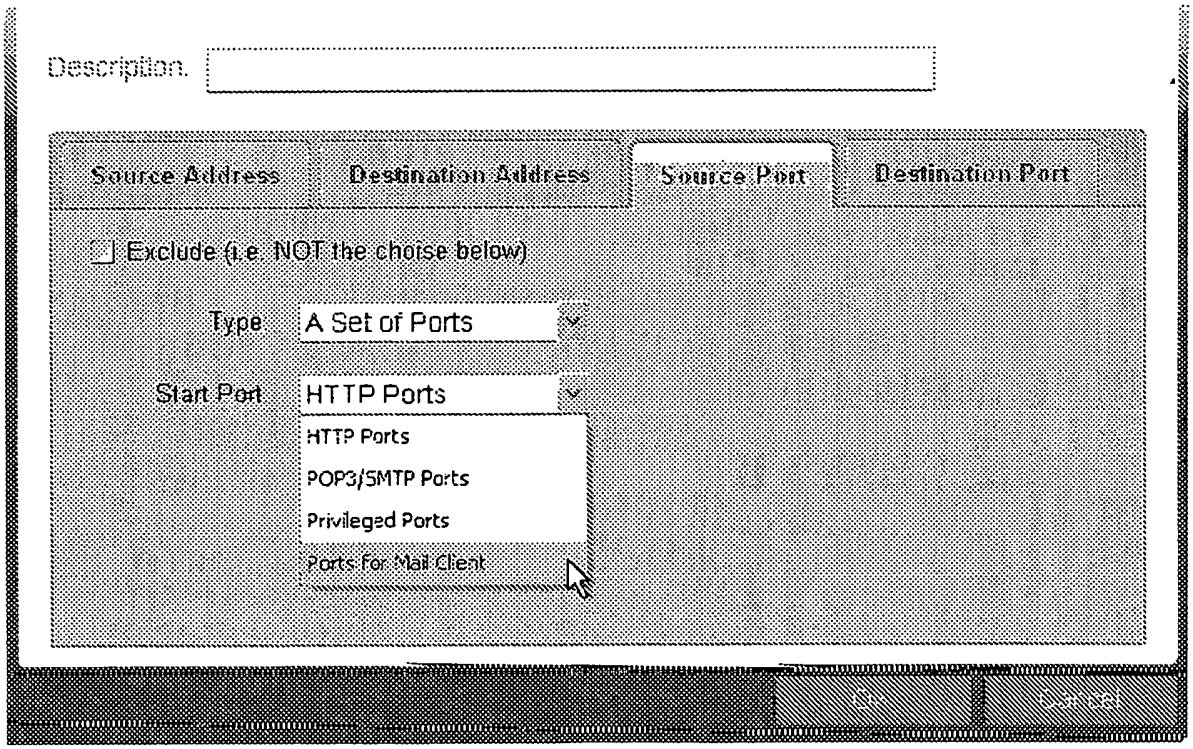


2. Enter a name for the new portset in the Name field.
3. To add ports to the new portset, click the handle from the bottom center and choose 'Add' from the options.



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

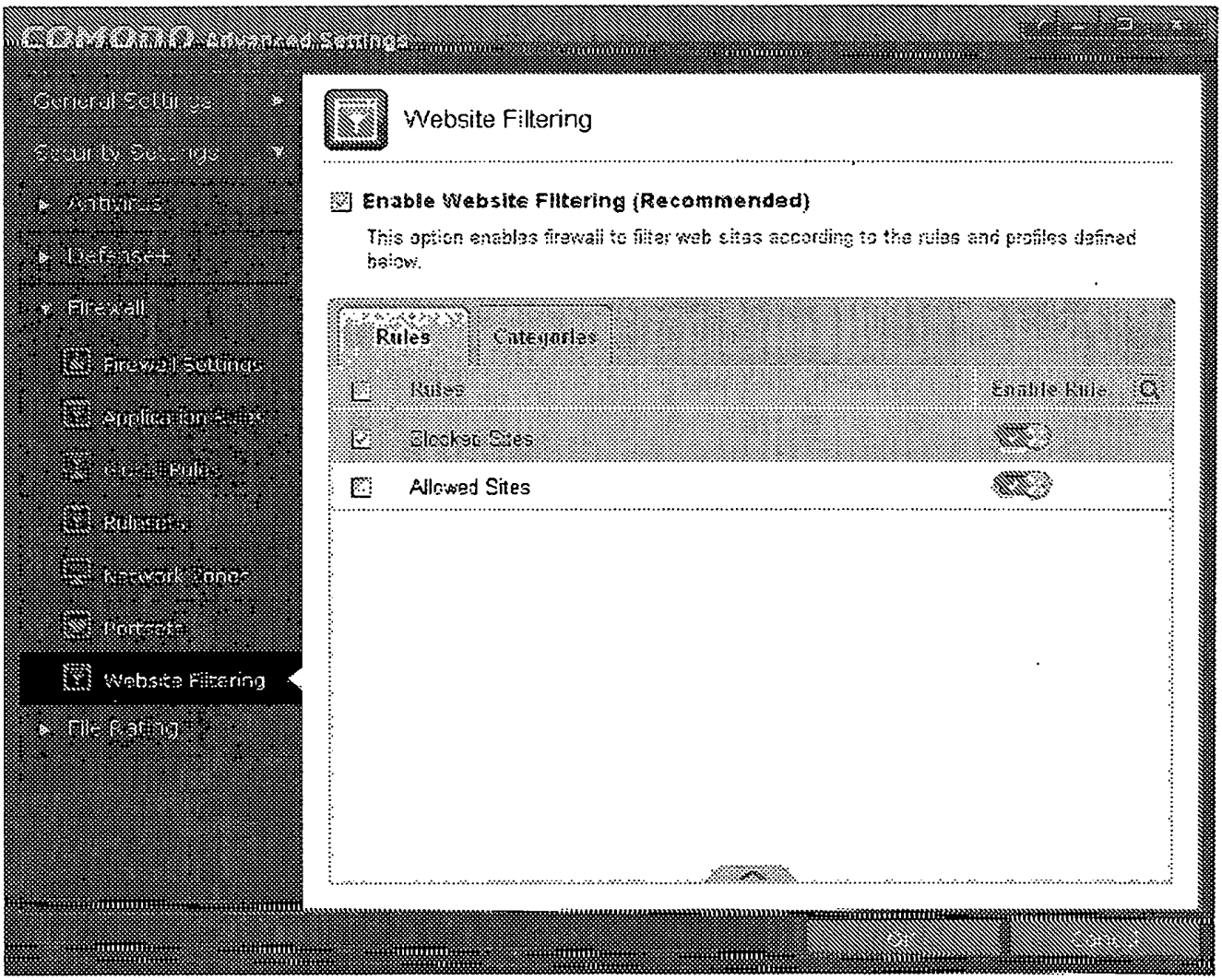
- Select the portset from the 'Portsets' interface, click the handle from the bottom center and select the 'Edit' from the options to bring up the 'Edit Portset' dialog.

- 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.

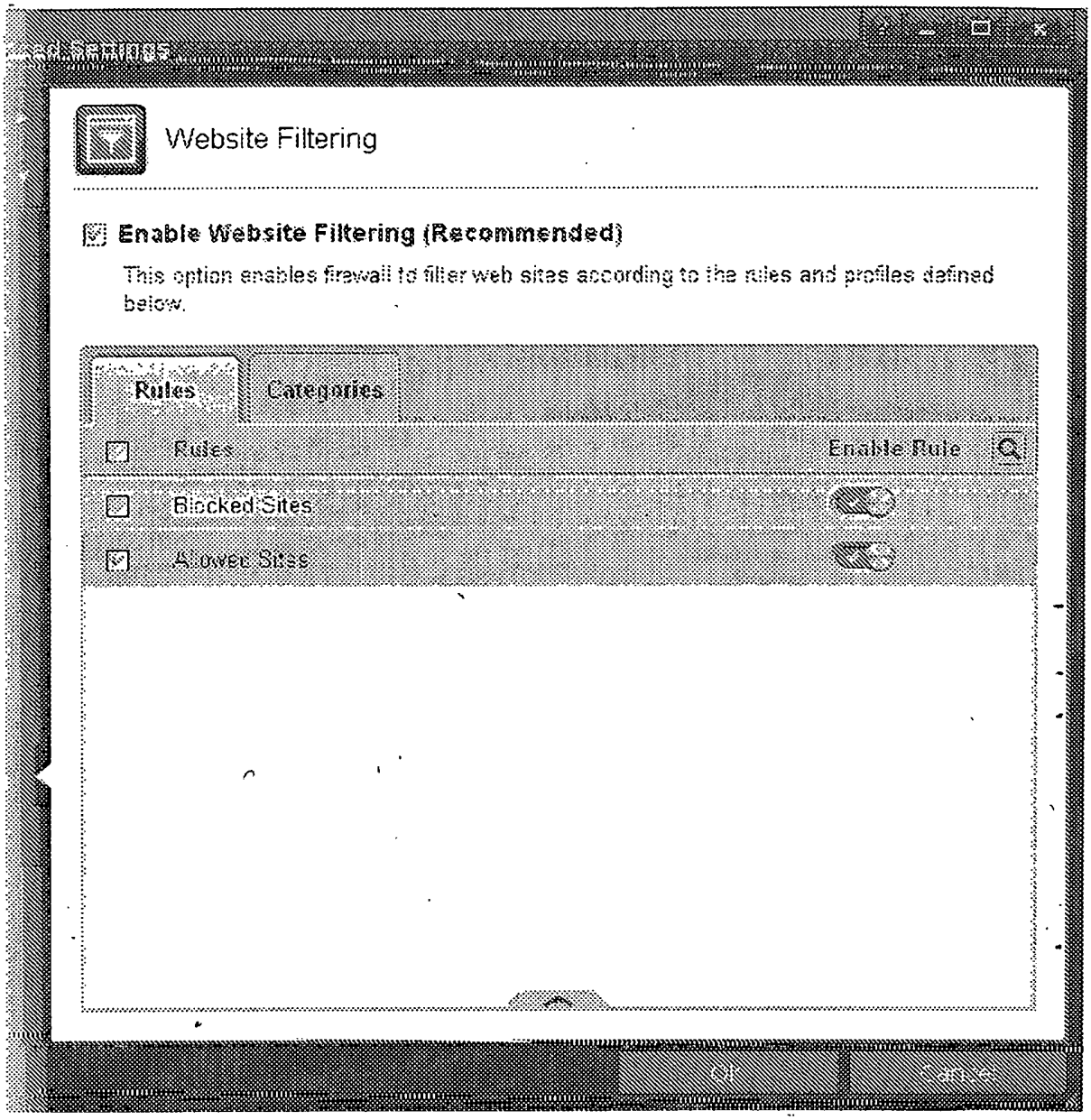
General Advice:

- 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.

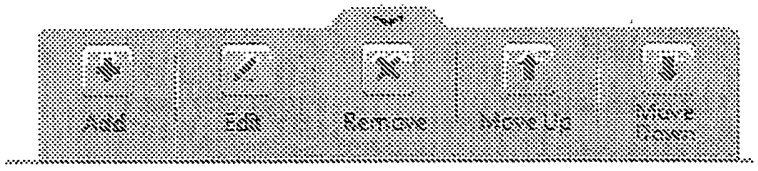
6.2.3.7.1. Creating and Modifying Website Filtering Rules

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.

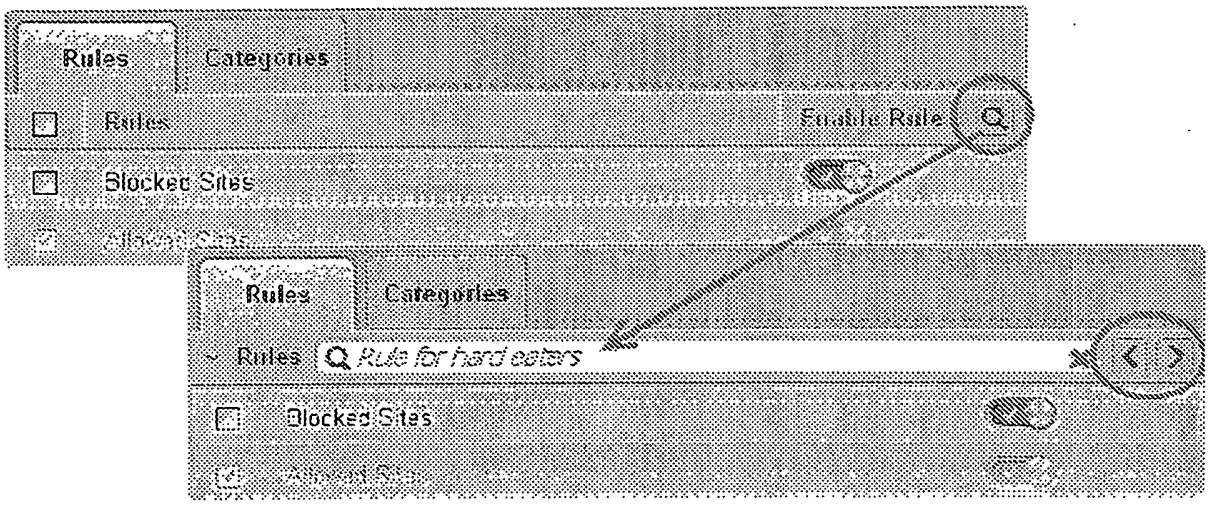
Comodo Firewall implements rules for the currently logged-in user based on the order they are in this list. Should a conflict exist between individual rules, then the rules at the top takes priority. Click the handle and use the 'Move Up' or 'Move Down' buttons to change a rule's priority.



- 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.



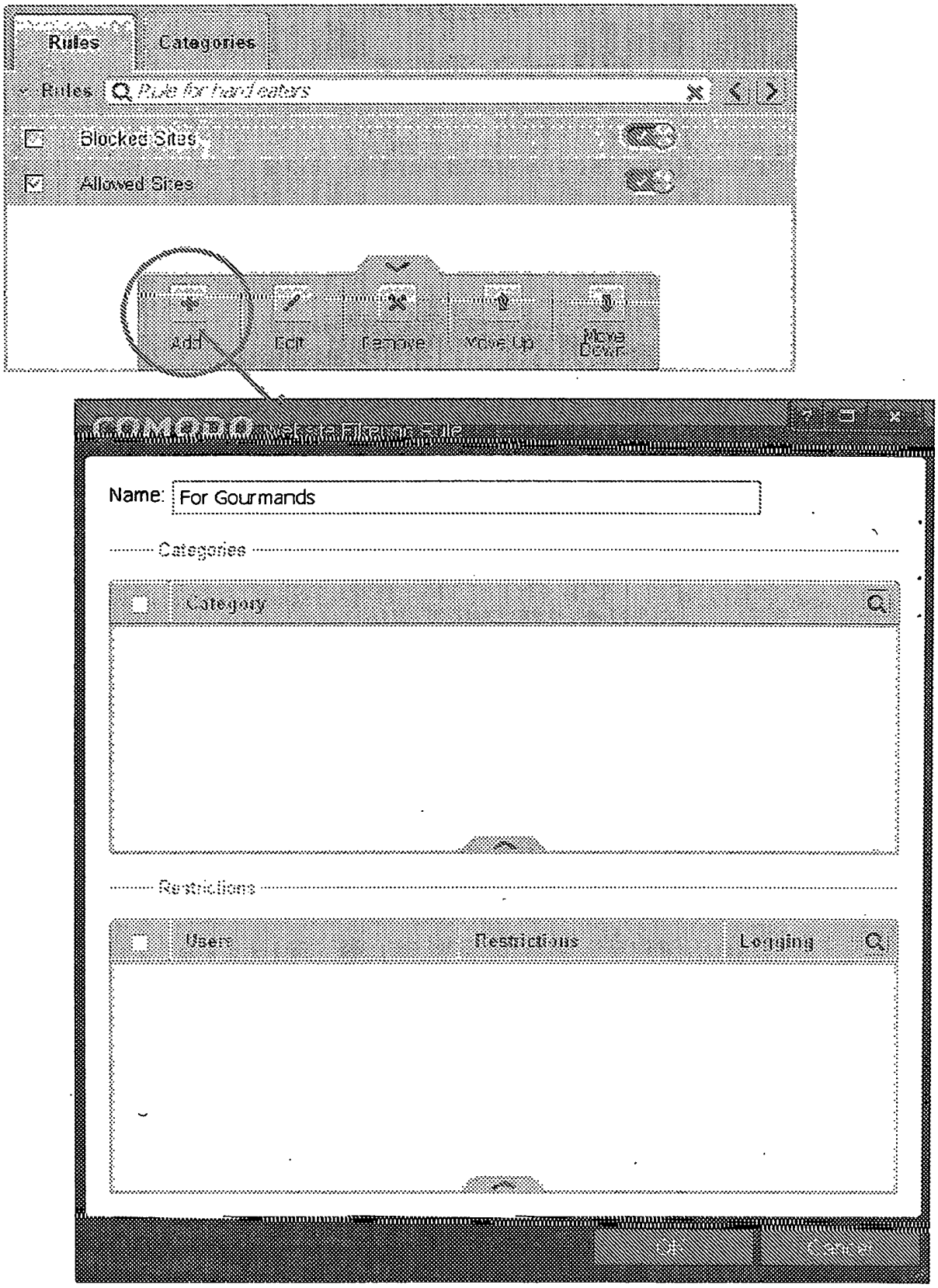
- Enter full or part of the name of the rule in the search field.
- Click the right or left arrow at the far right to begin the search.
- Click the icon in the search field to close the search option.

The Rules interface allows you to:

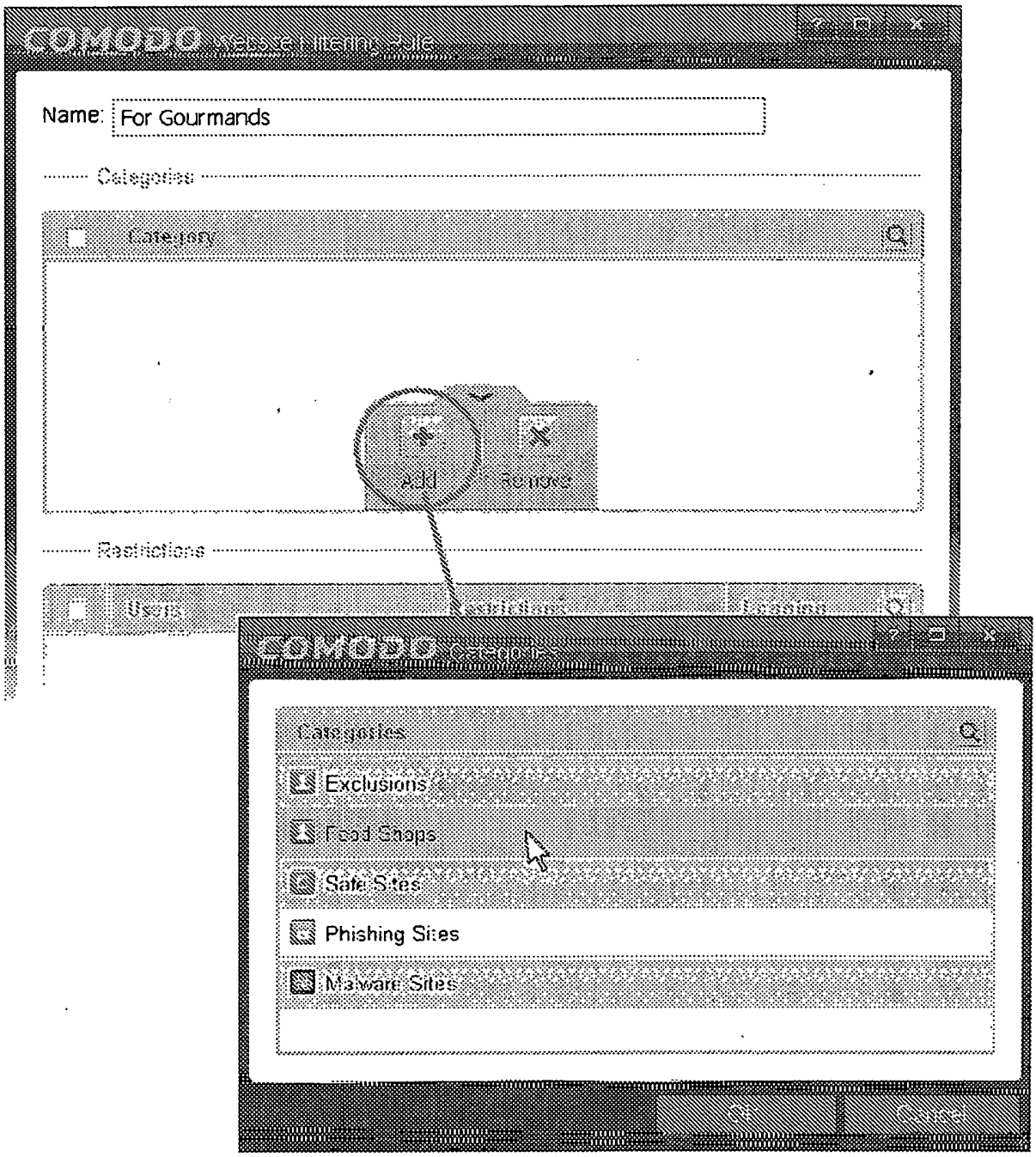
- Create new Website filtering Rules
- Edit existing rules
- Change priority of the rules
- Remove unwanted rules

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.

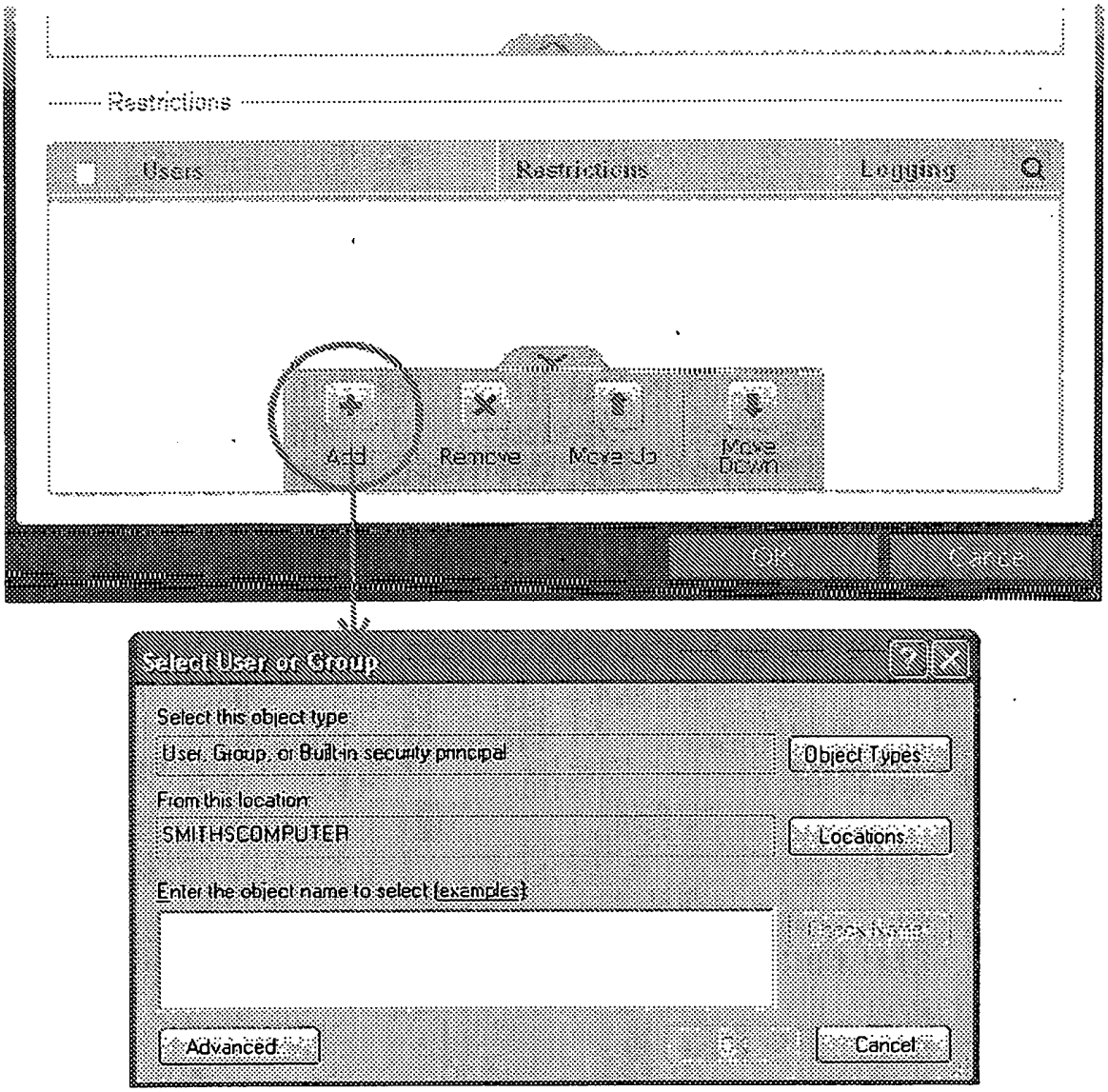
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **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

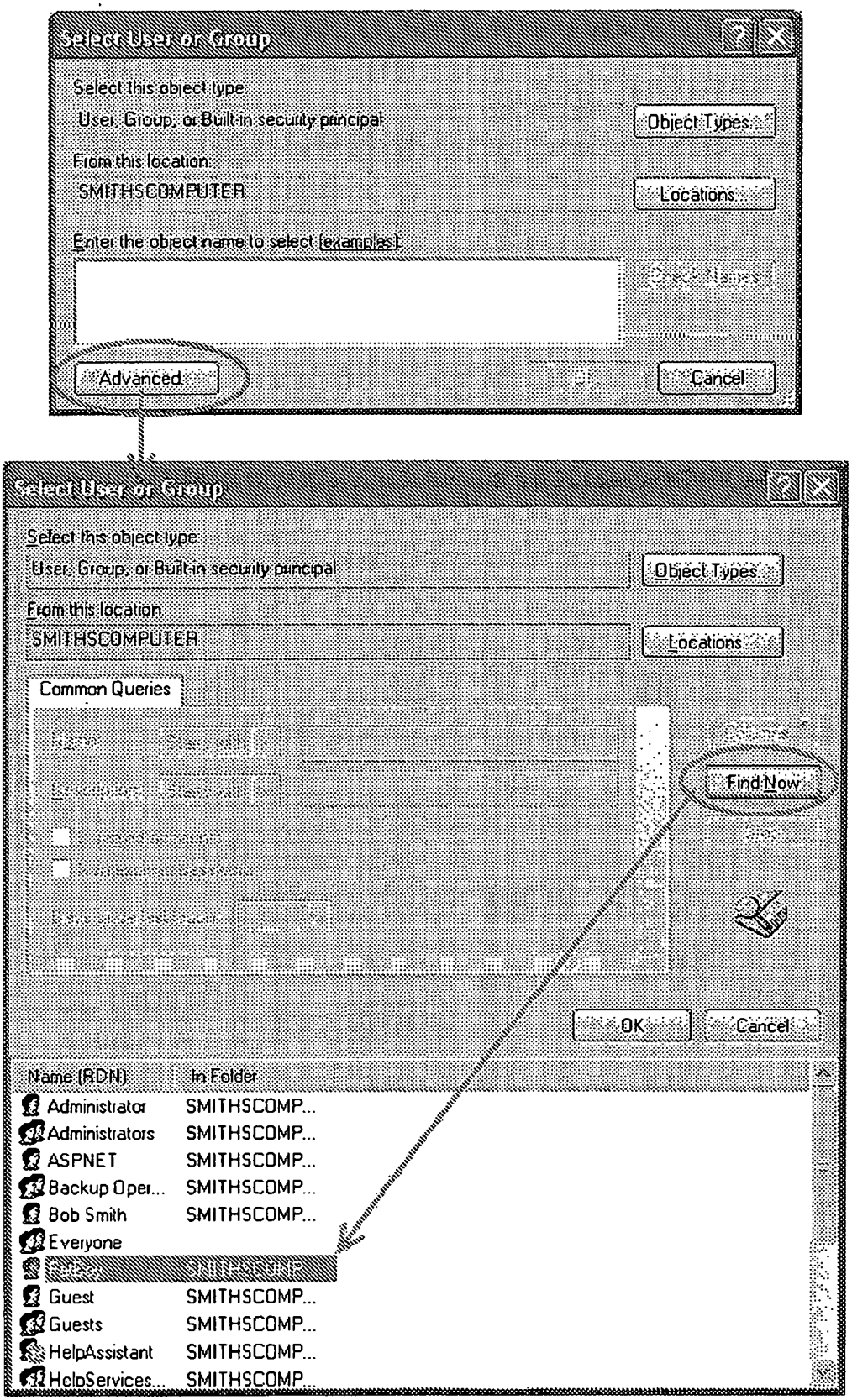
For more details on creating and modifying user specified categories, Refer to the section Defining or Modifying Website Categories

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

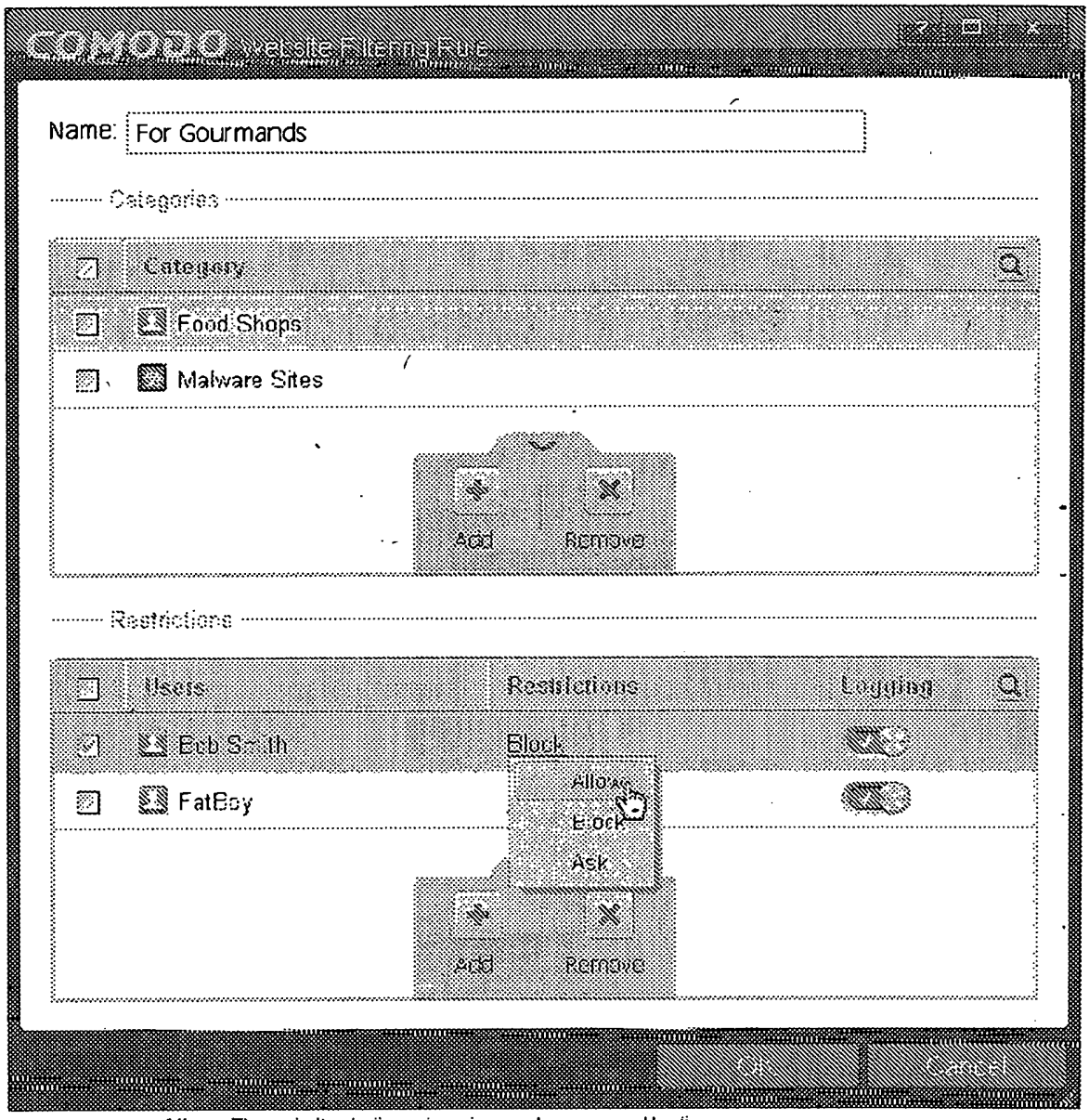
- Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:



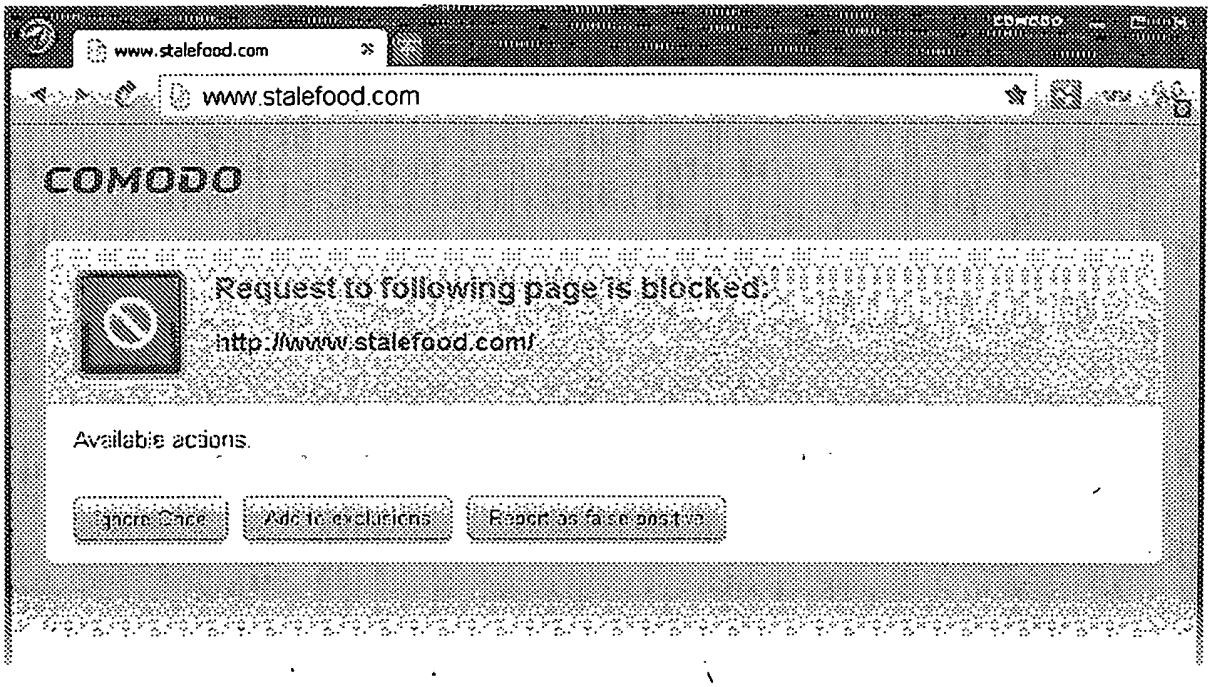
- Enter the names of the users to whom the filter is to be applied in the 'Enter the object name to select' text box with the format <domain name>\<user/group name> or <user/group name>@<domain name>. Alternatively, click 'Advanced' then 'Find Now' to locate specific users. Click 'OK' to confirm the 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
Find Now
OK
Cancel
Name (RDN)
In Folder
Administrator SMITHSCOMP...
Administrators SMITHSCOMP...
ASPNET SMITHSCOMP...
Backup Oper... SMITHSCOMP...
Bob Smith SMITHSCOMP...
Everyone
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.



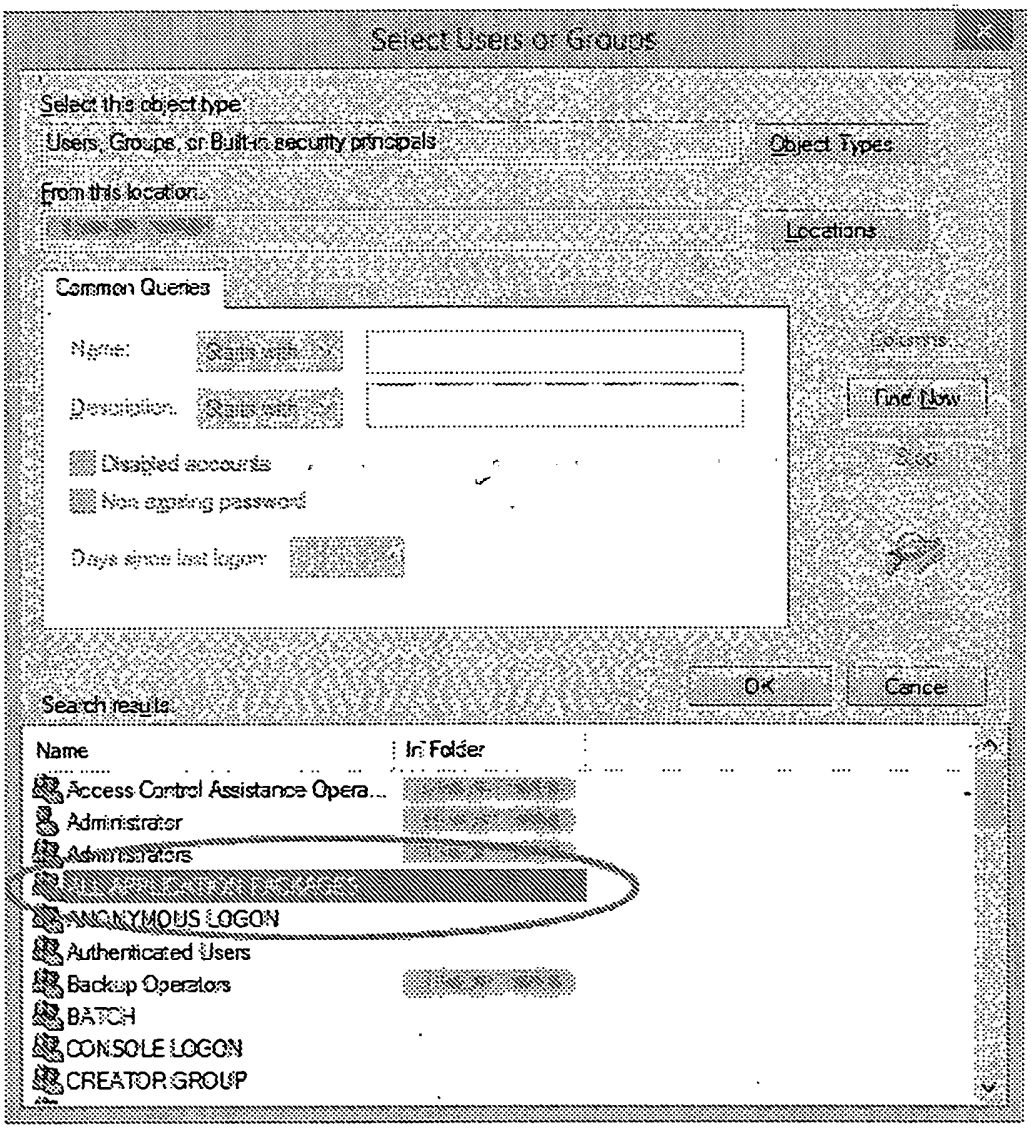
6. Use the 'Logging' switch to choose whether or not attempts to access a categorized website are logged.
7. Click 'OK' to save your new rule. The new rule will be added to the list of rules under the 'Rules' tab
8. Make sure that the rule is enabled using the toggle switch under the Enable Rule column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

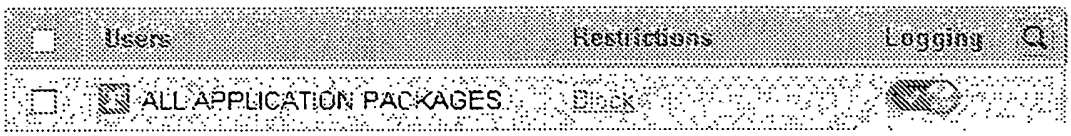
To add 'ALL APPLICATION PACKAGES' to the restrictions list

- 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

Restrictions



To edit existing rules

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

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

To remove a Website Filtering Rule

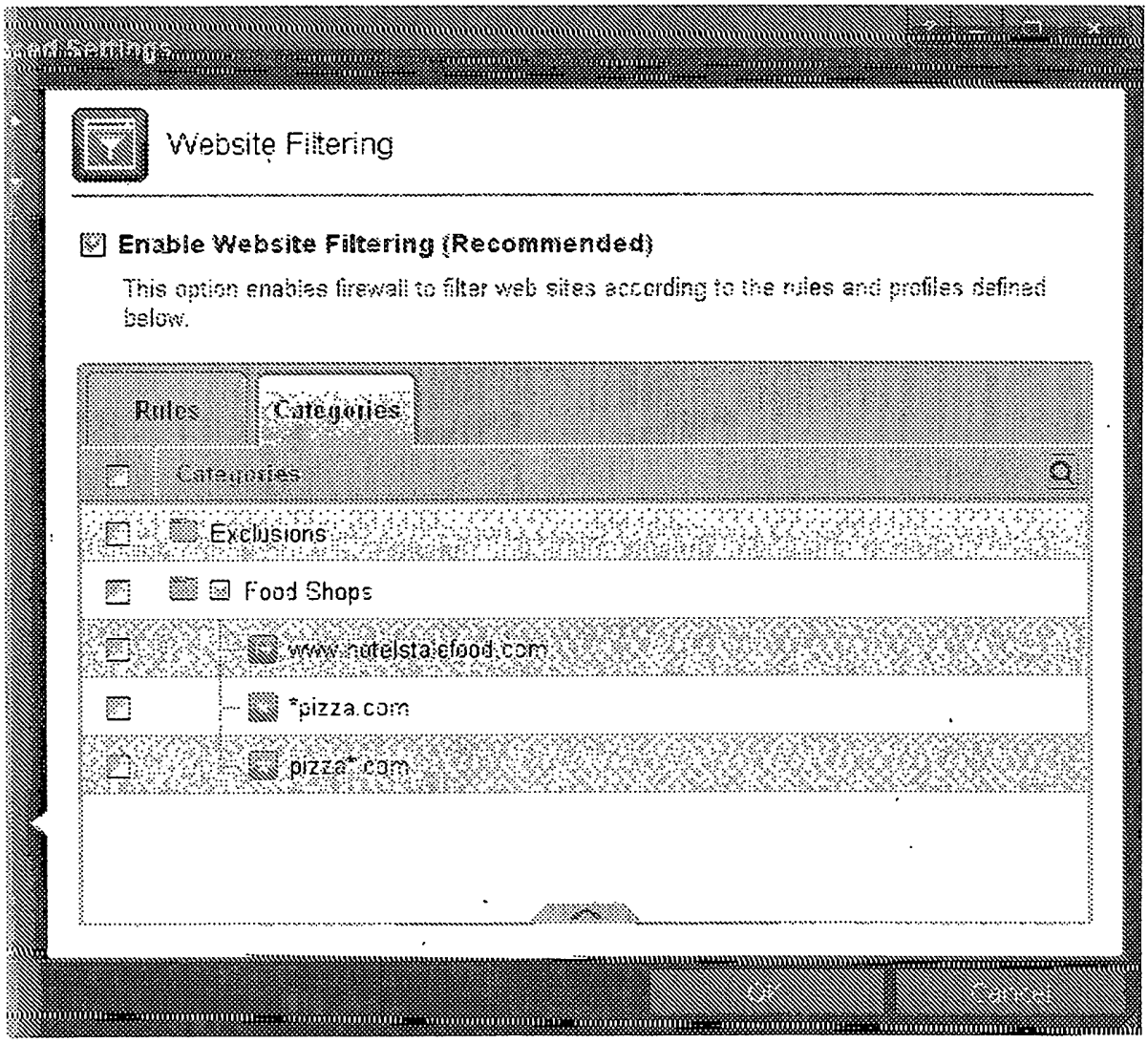
1. Open the ' Website Filtering' Panel by clicking 'Security Settings' > 'Firewall' > 'Website Filtering' tab from the 'Advanced Settings' interface
2. Choose the Website Filtering Rule(s) to be removed under the 'Rules' tab by selecting the checkbox(es) beside them.
3. Click the handle from the bottom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

To change the priority of Website Filtering Rules

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

6.2.3.7.2. Defining or Modifying Website Categories

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

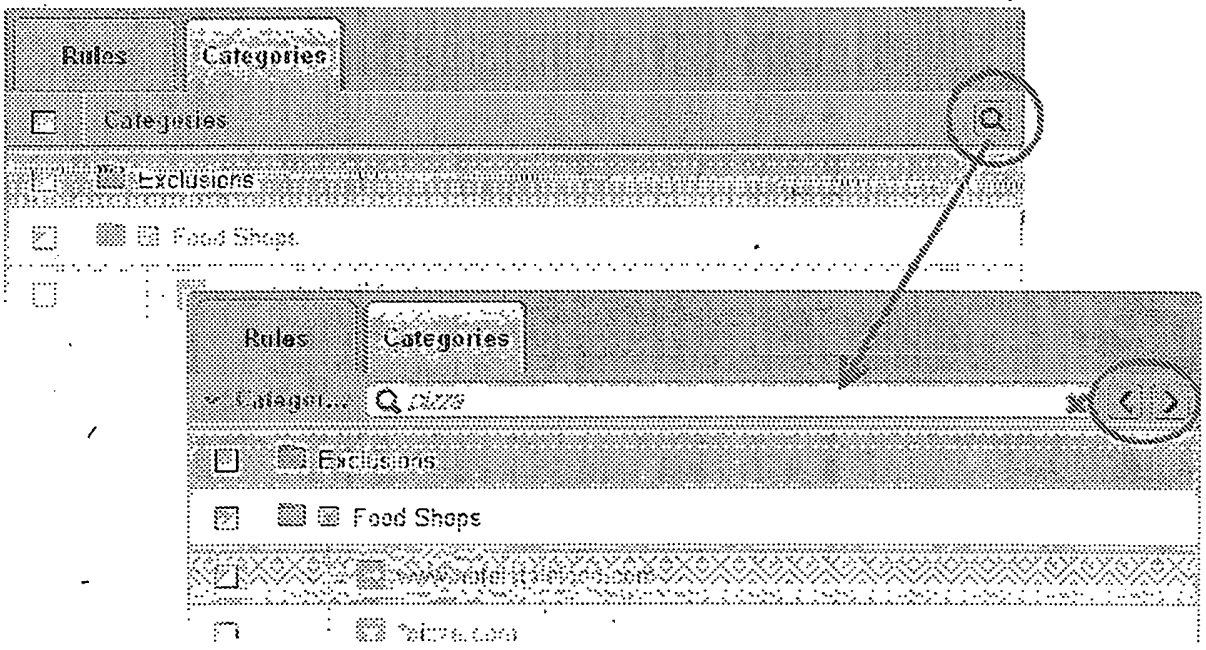


The 'Categories' pane allows you to:

- Add a new category of Websites

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

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



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

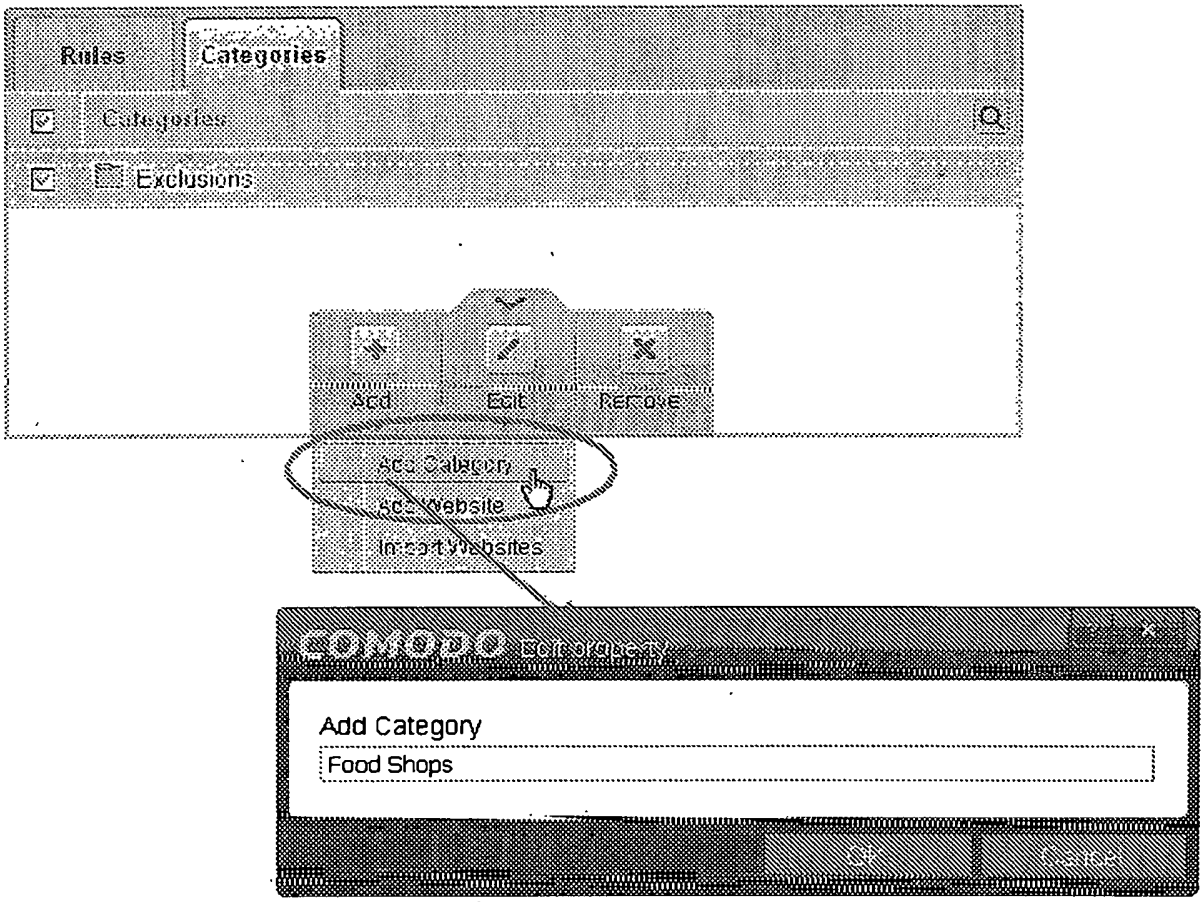
Adding a New Category of Websites

Adding a new category involves two steps:

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

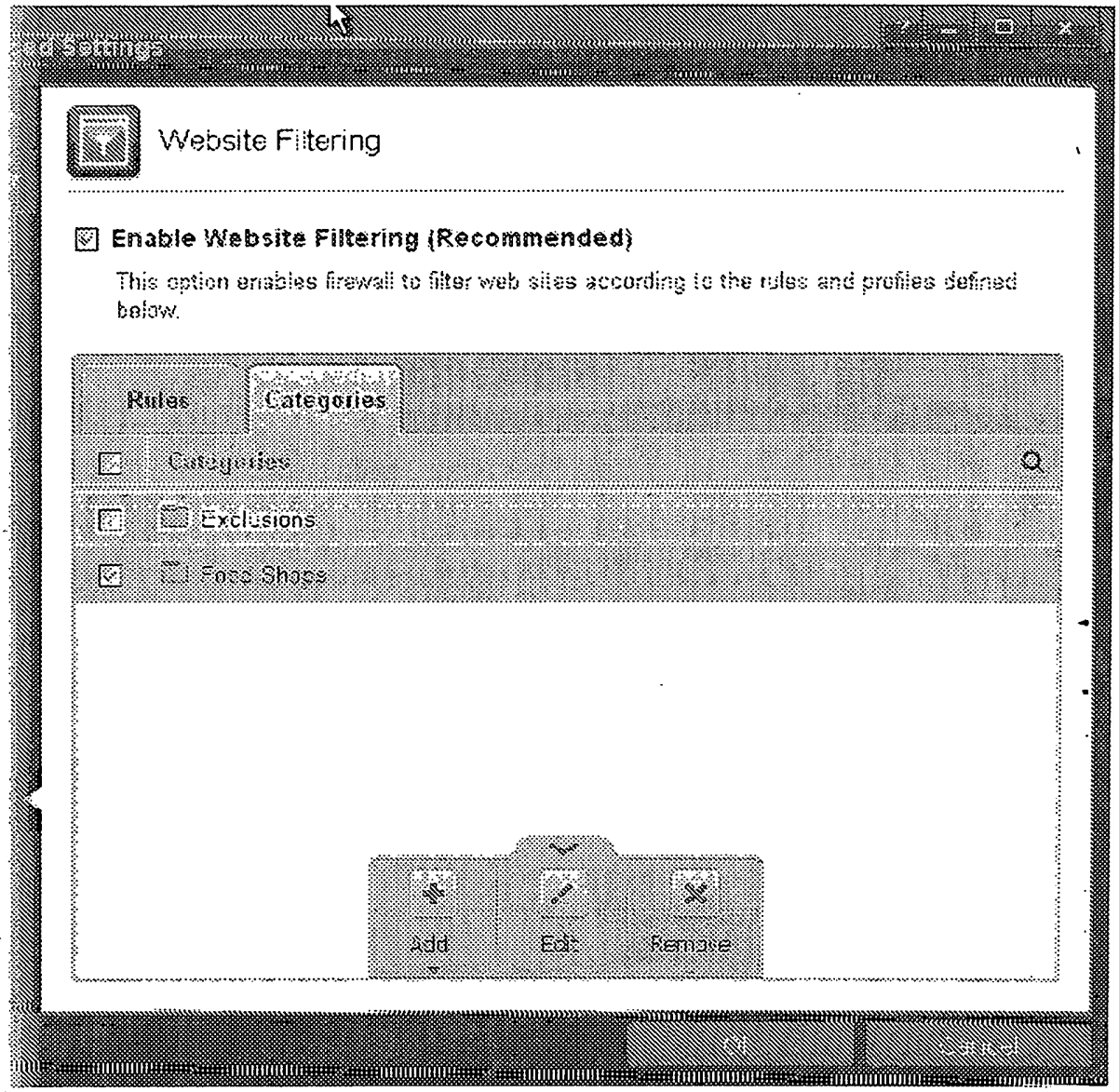
Step 1 - Define a name for the category

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



4. Enter a name for the category and click OK

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



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

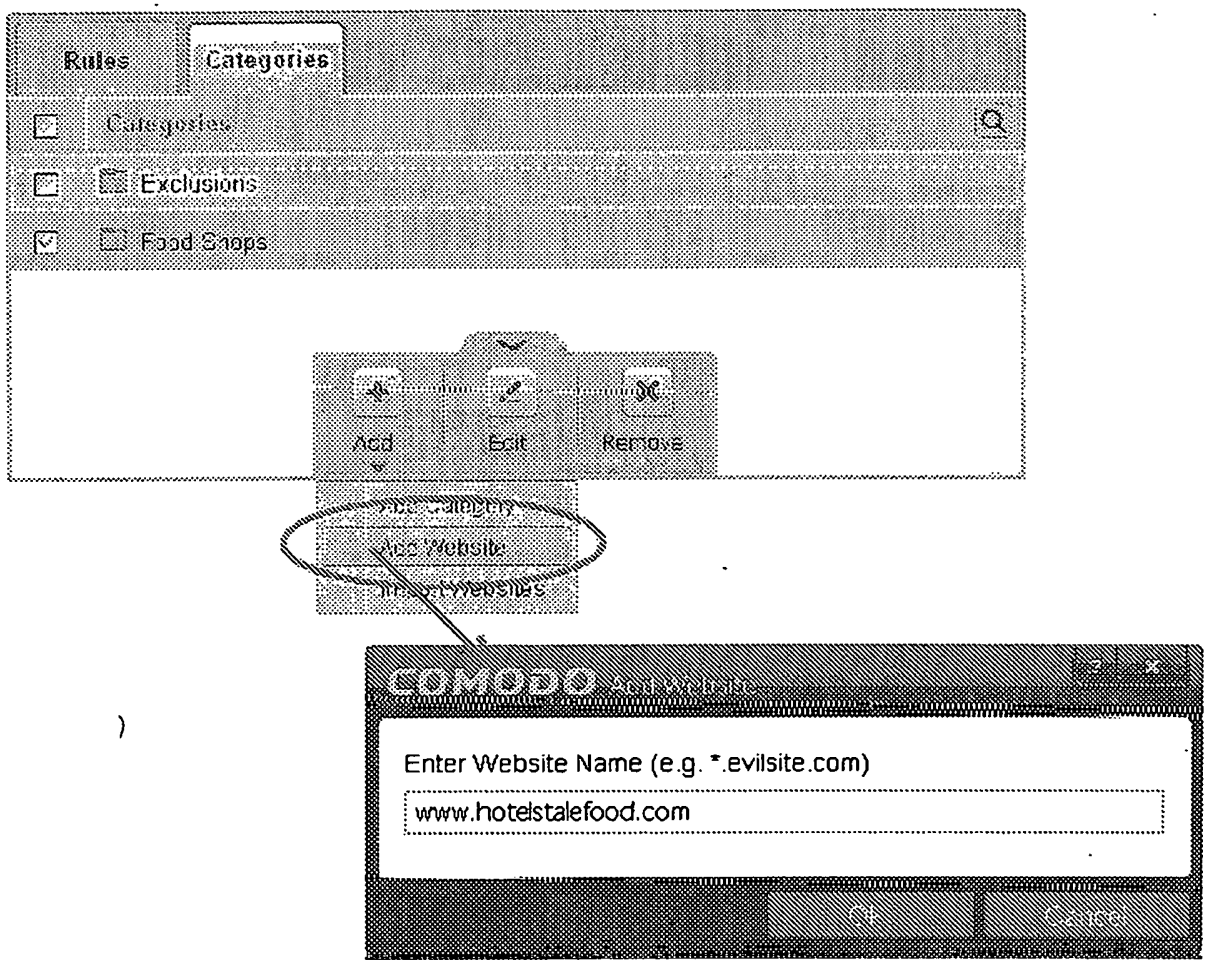
Step 2 - Add URLs to be included to the category

You can add websites to a category in two ways:

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

To manually specify websites

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

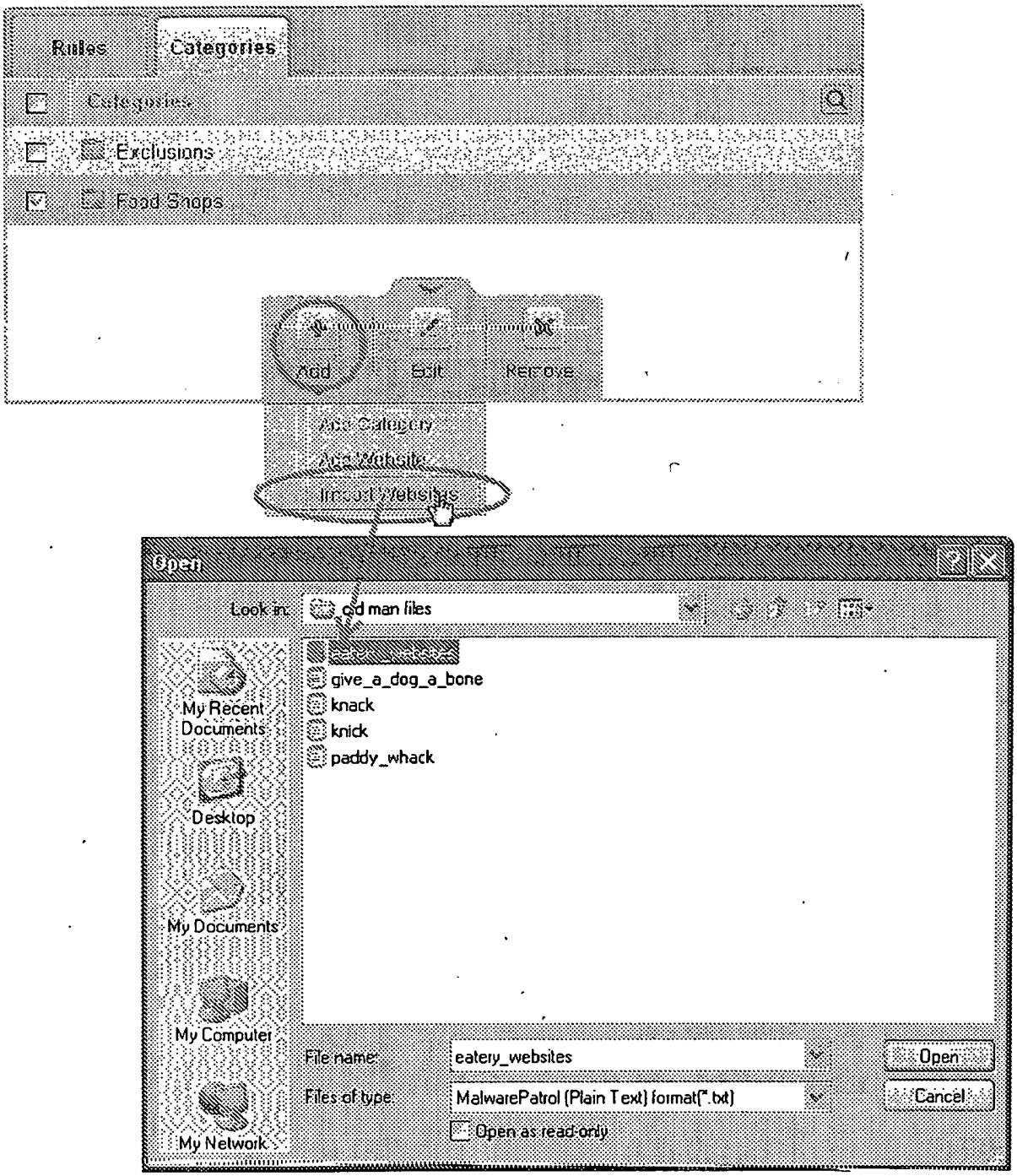


3. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
    - To add a specific website/webpage, enter the full URL of the website/webpage
    - To include all sub-domains of website, add a wildcard character and a period in front of the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

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

To upload a list of websites from a text file

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



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

4. Click 'Open'.

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

To rename a category

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

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

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

To remove a Website from a category

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

To remove a Category

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

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

6.2.4. Manage File Rating

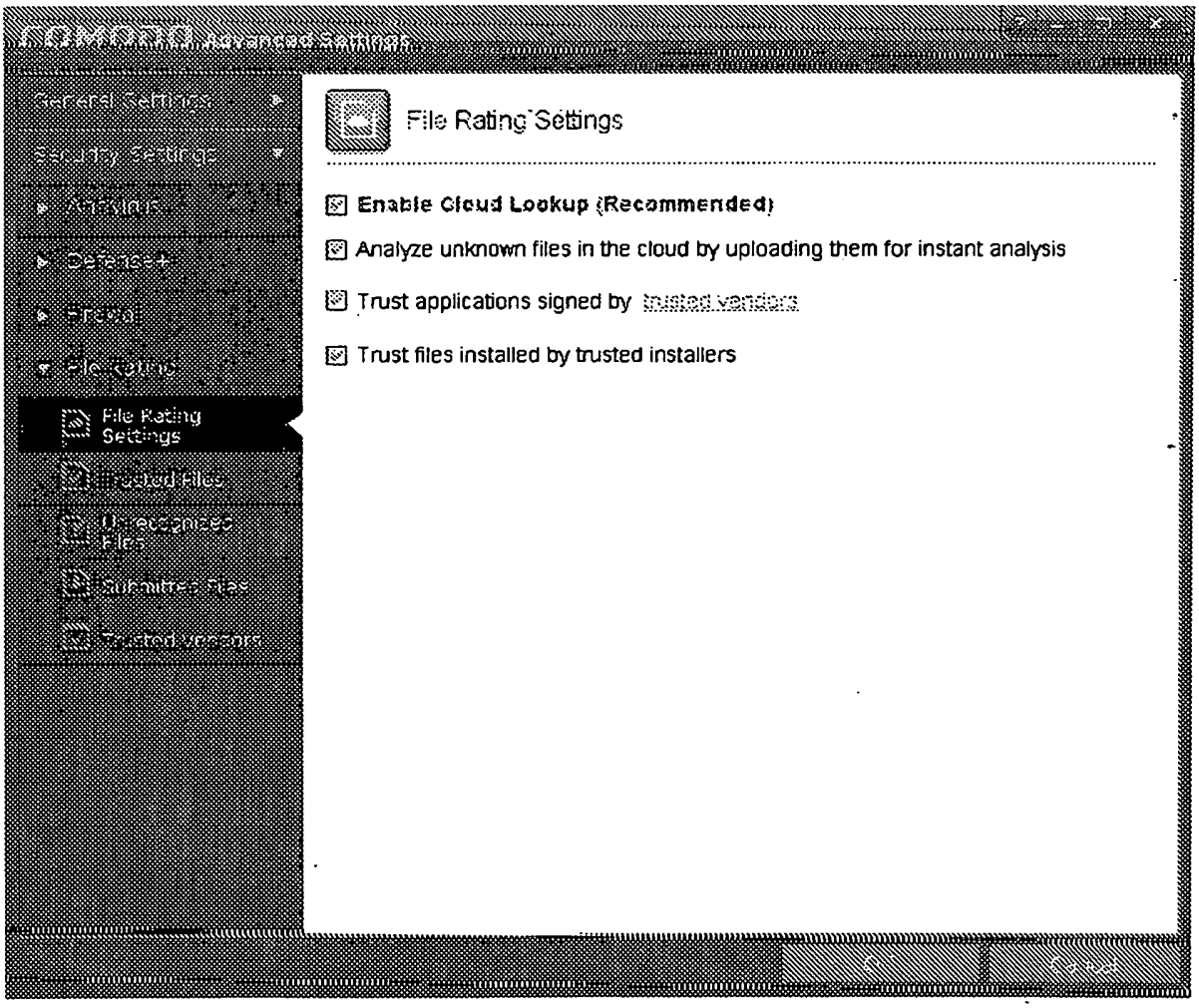
The CIS file rating system is a cloud-based file look-up service (FLS) that attempts to ascertain the reputation of files on your computer by consulting a global database. Whenever a file is first accessed, CIS will check the file against our master whitelist and blacklists and will award it trusted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

- The application/file is 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:

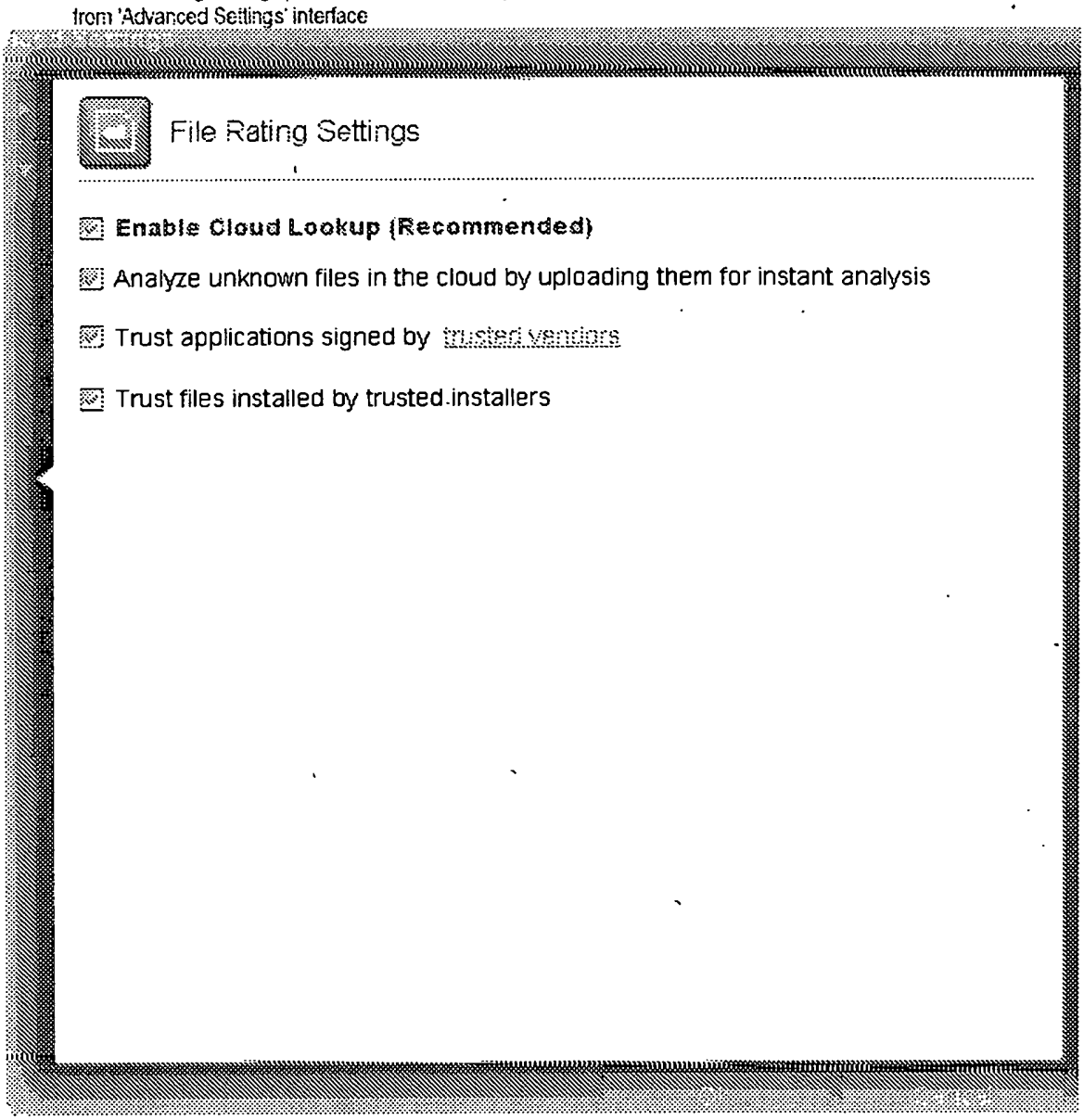
- File Rating Settings - Configure settings that govern the overall behavior of file rating.
- Trusted Files - View and add to the list of trusted files.

- 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***)

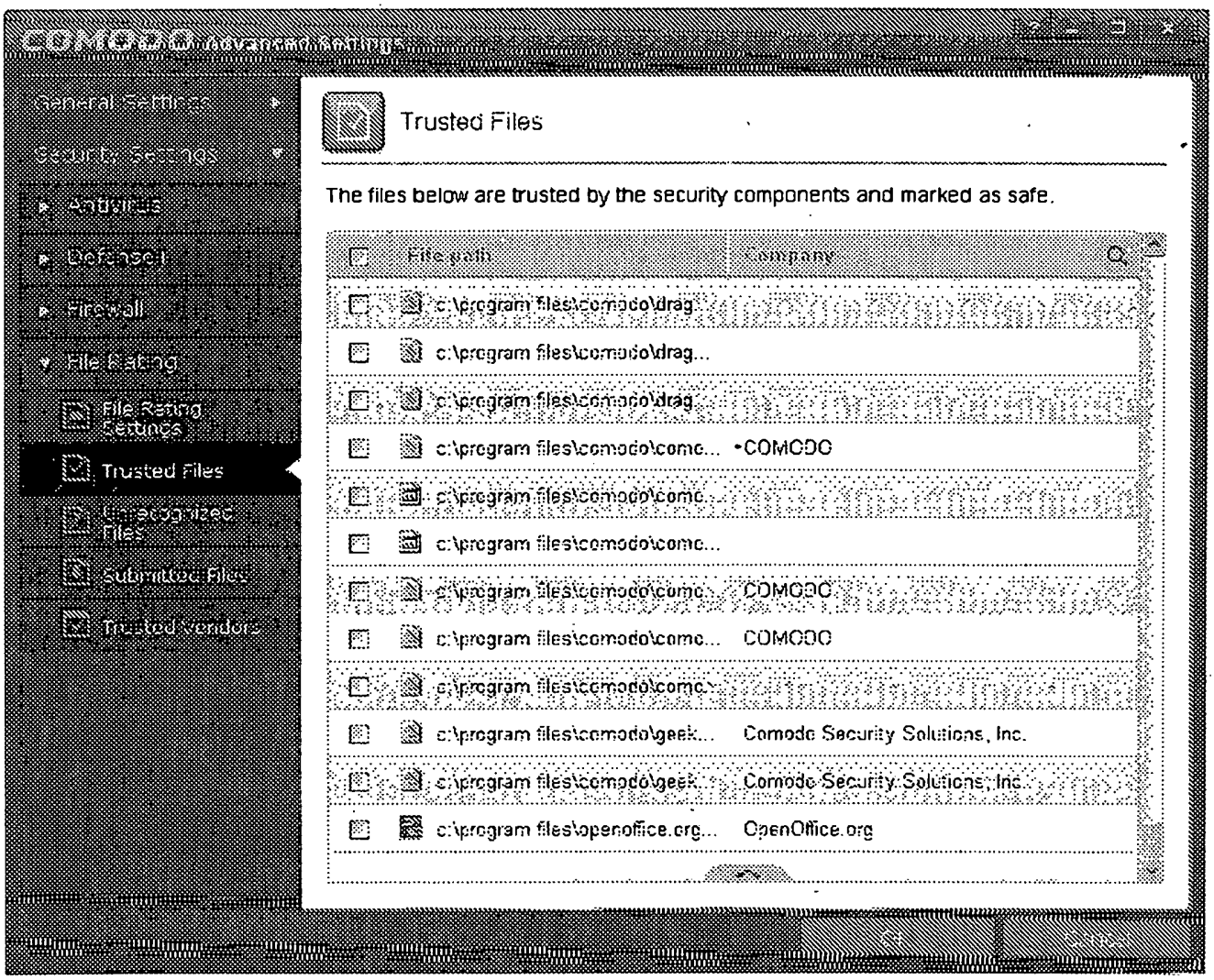
6.2.4.2. Trusted Files

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'.

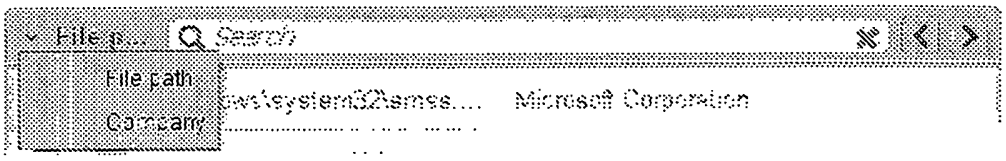
CIS allows you to define a personal safe list of files to complement the default Comodo safe list.

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

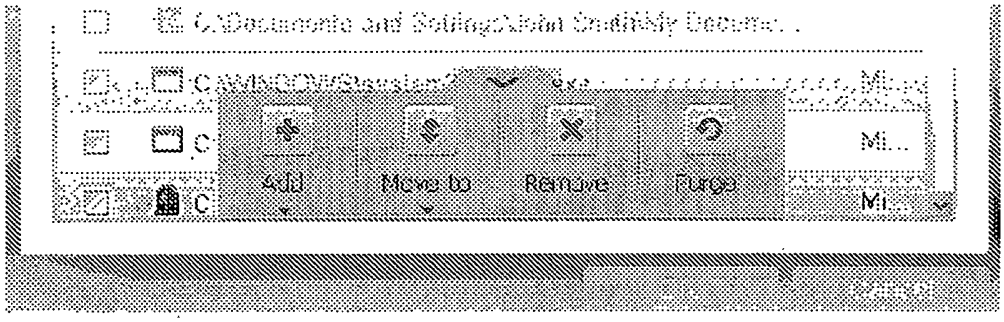


You can use the search option to find a specific item in the list by clicking the search icon  at the far right in the column header.



- 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:



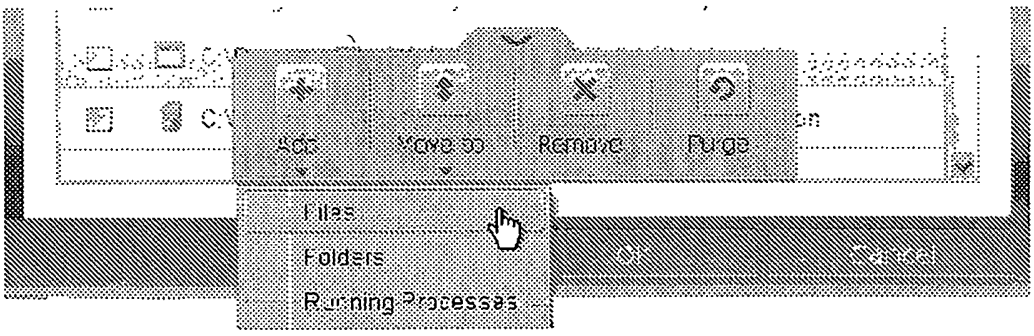
- Add - Allows you to add files to Trusted Files list manually
- Move - Allows you to move files from Trusted Files list to Blocked Files or Unrecognized Files list
- Remove - Allows you to remove files from Trusted Files list
- **Purge** - Runs a system check to verify that all the files listed are 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:

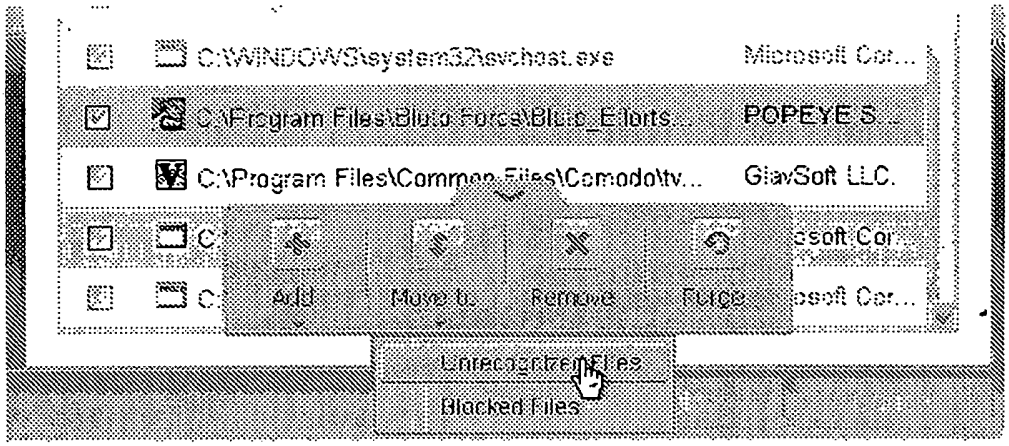
- **Files** - Allows you to navigate to the file or executable of the program you wish to add.

- **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.

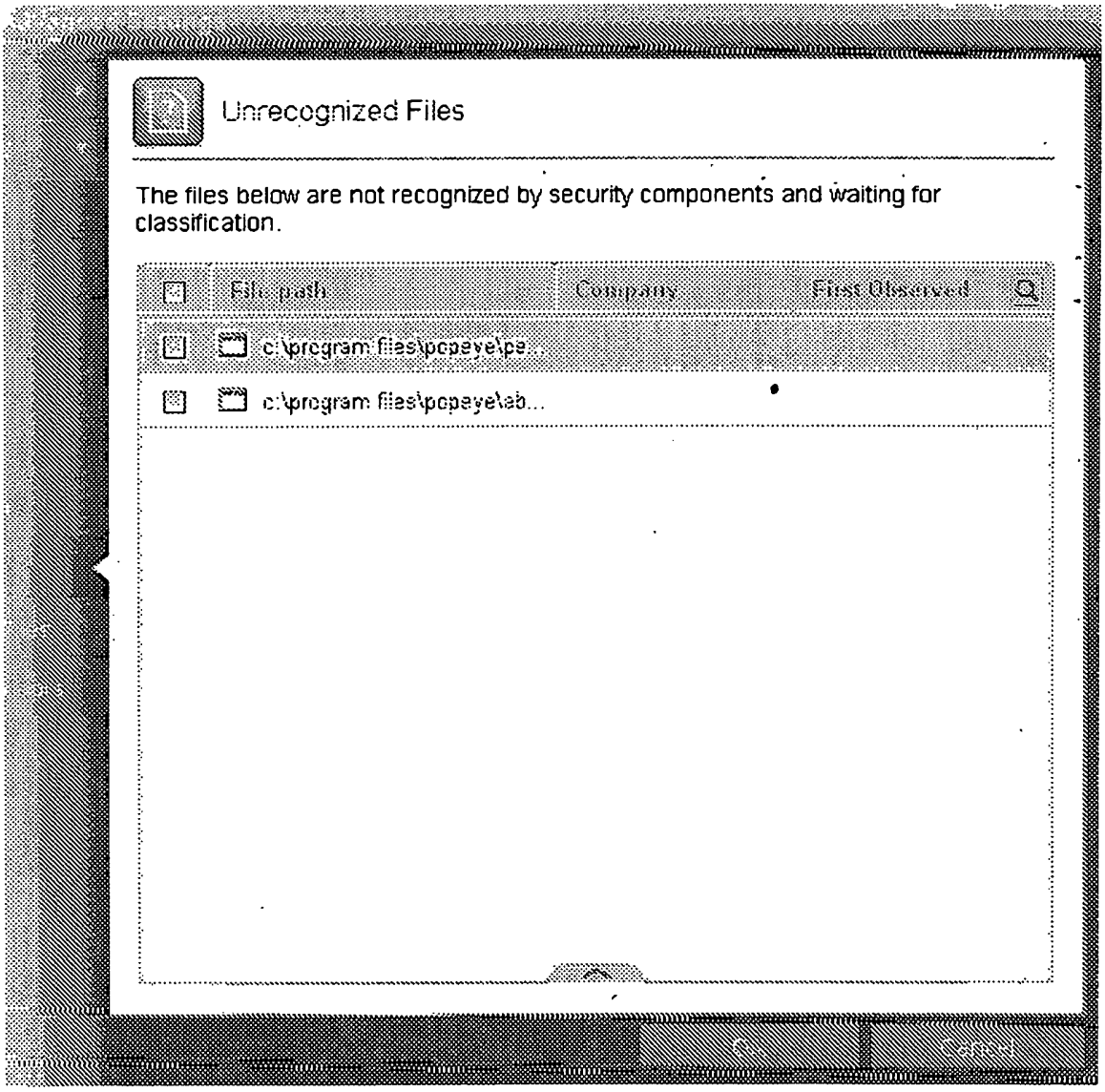
  Refer to the section To perform an online lookup for unrecognized files for more details.

- 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.

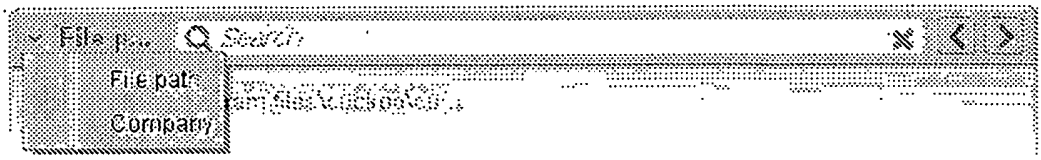
The 'Unrecognized Files' panel displays the list of files added as Unrecognized Files and allows you to assess the pending files to determine whether or not they are to be trusted. If they are trustworthy, they can be moved to 'Trusted Files' using the 'Move to' button. Similarly, files that are suspicious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

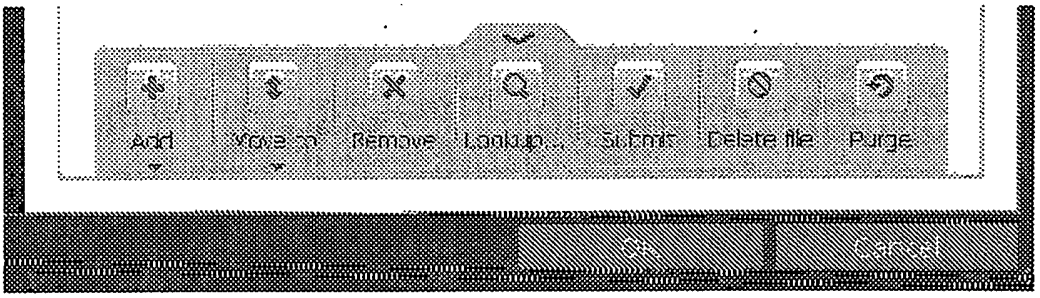


You can use the search option to find a specific item in the list by clicking the search icon at the far right in the column header.



- 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.

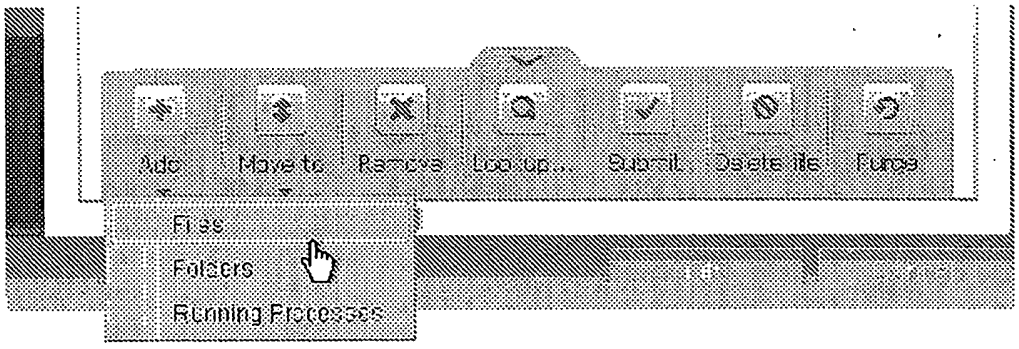
Clicking the handle at the bottom center of the panel opens the following options:



- 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:

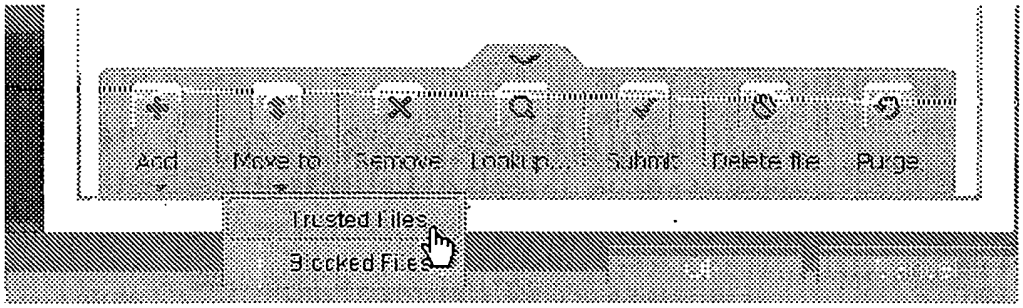
- **Files** - Allows you to navigate to the file or executable of the program you wish to add.
- **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'Unrecognized Files' list.
- **Running Processes** - Allows you to select a currently running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



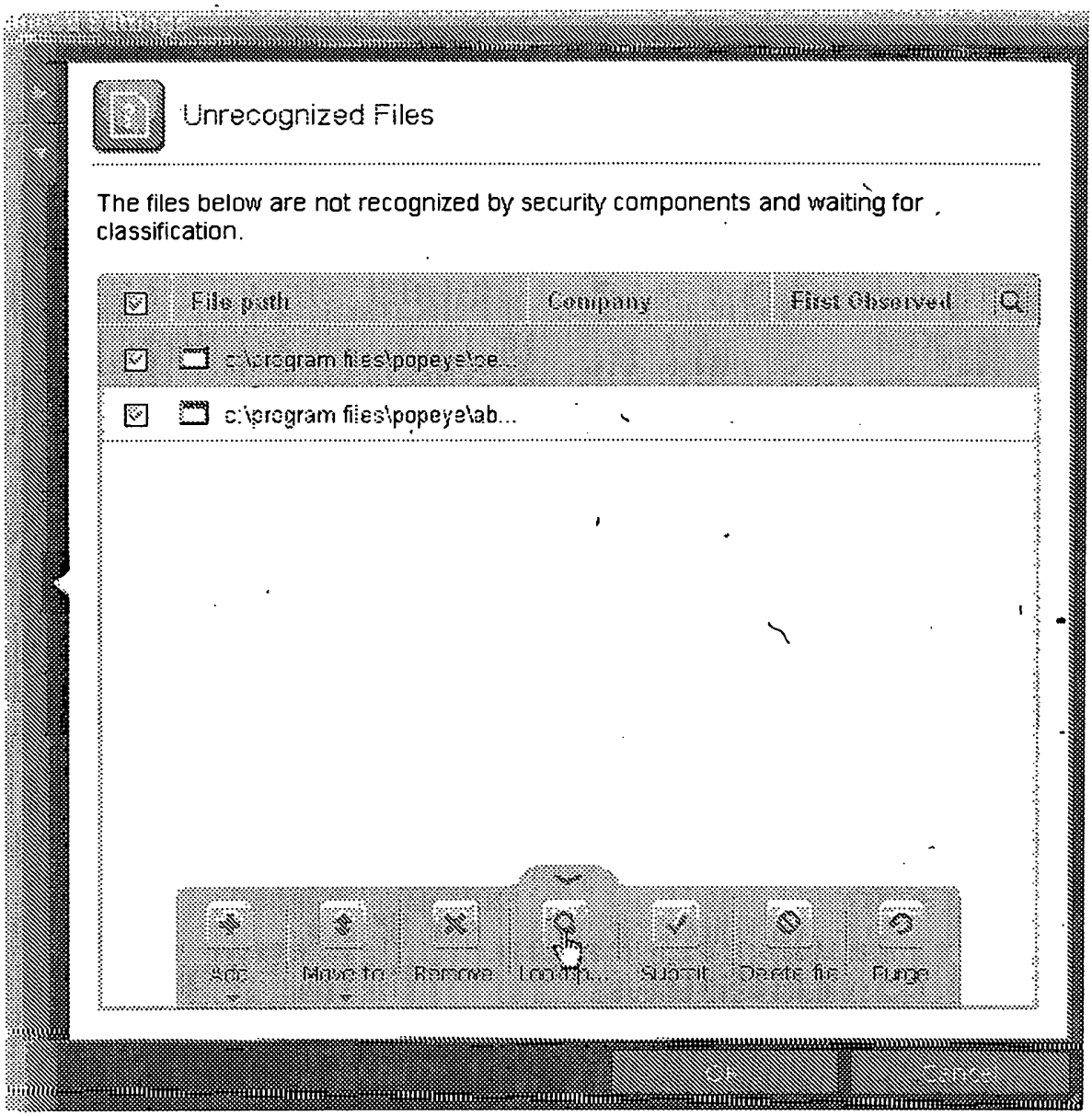
- Choose 'Trusted Files' or 'Blocked Files' from the drop-down.
- Click OK for your changes to take effect.

To remove an included entry from the Unrecognized Files list

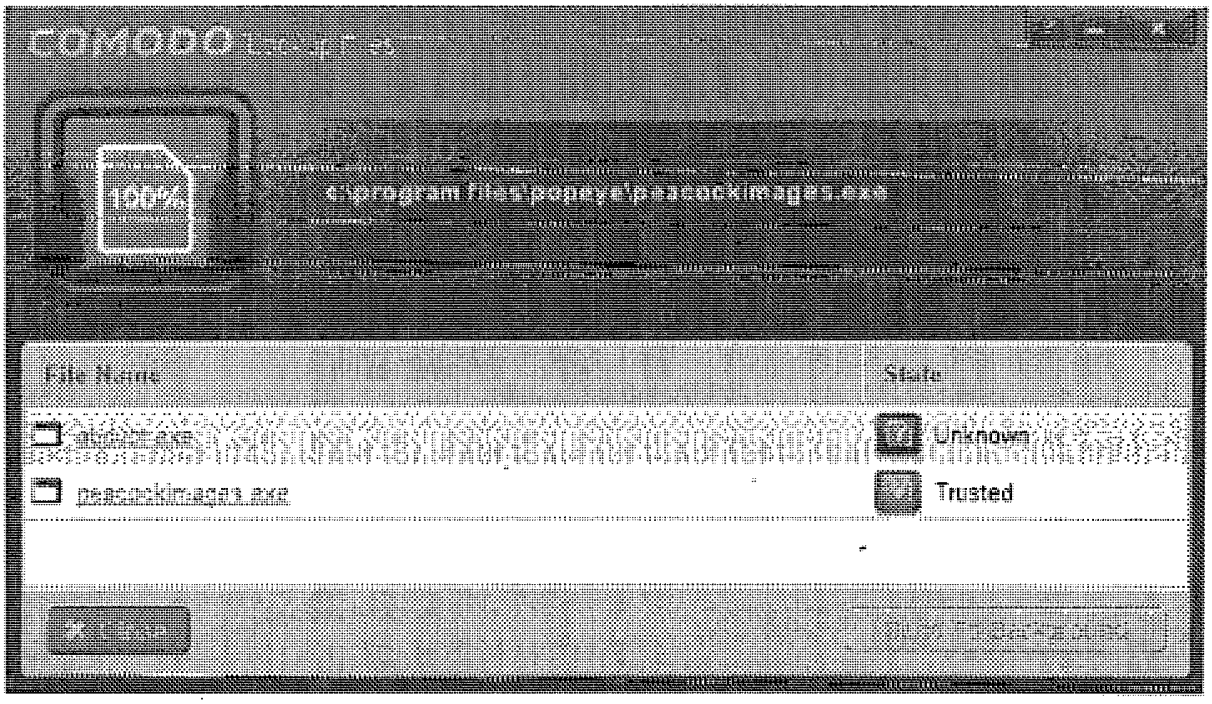
- Select the entry to be removed from the 'Unrecognized Files' list. You can select several entries to be removed at once by marking the check-boxes beside the entries.
- Click the handle from the bottom center and choose 'Remove'. The file is only removed from the list and not deleted from your system.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

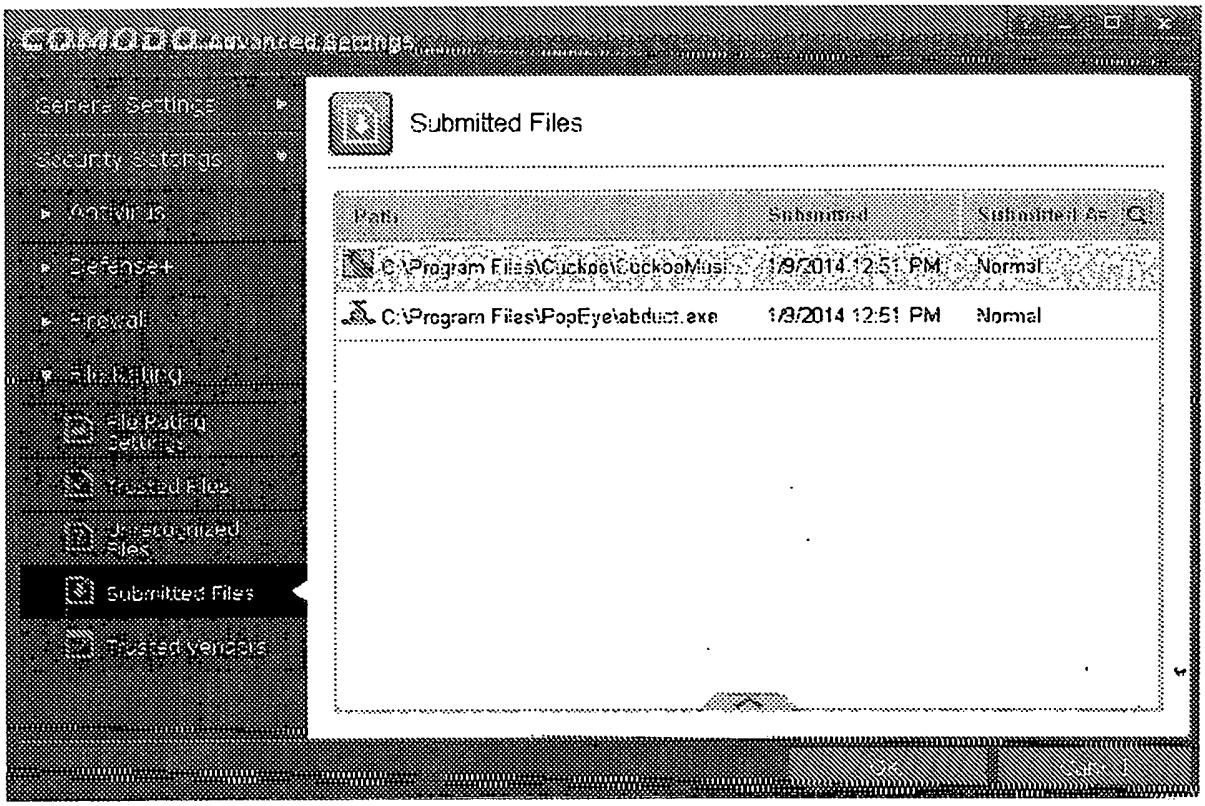
To manually submit files to Comodo

- 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.

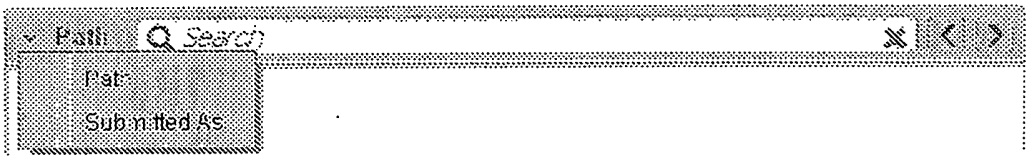
6.2.4.4. Submitted Files

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



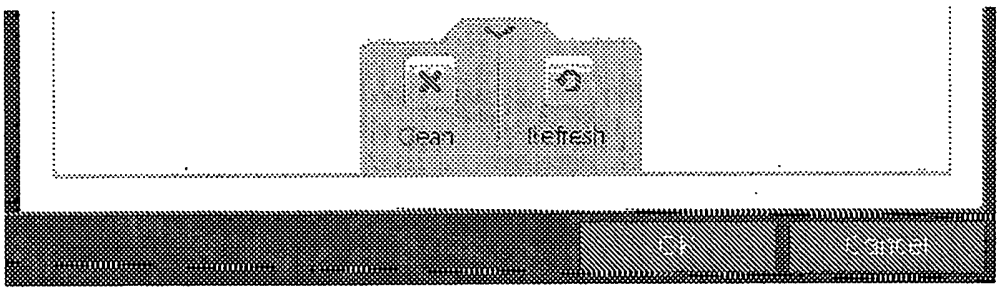
You can use the search option to find a specific file in the list.

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

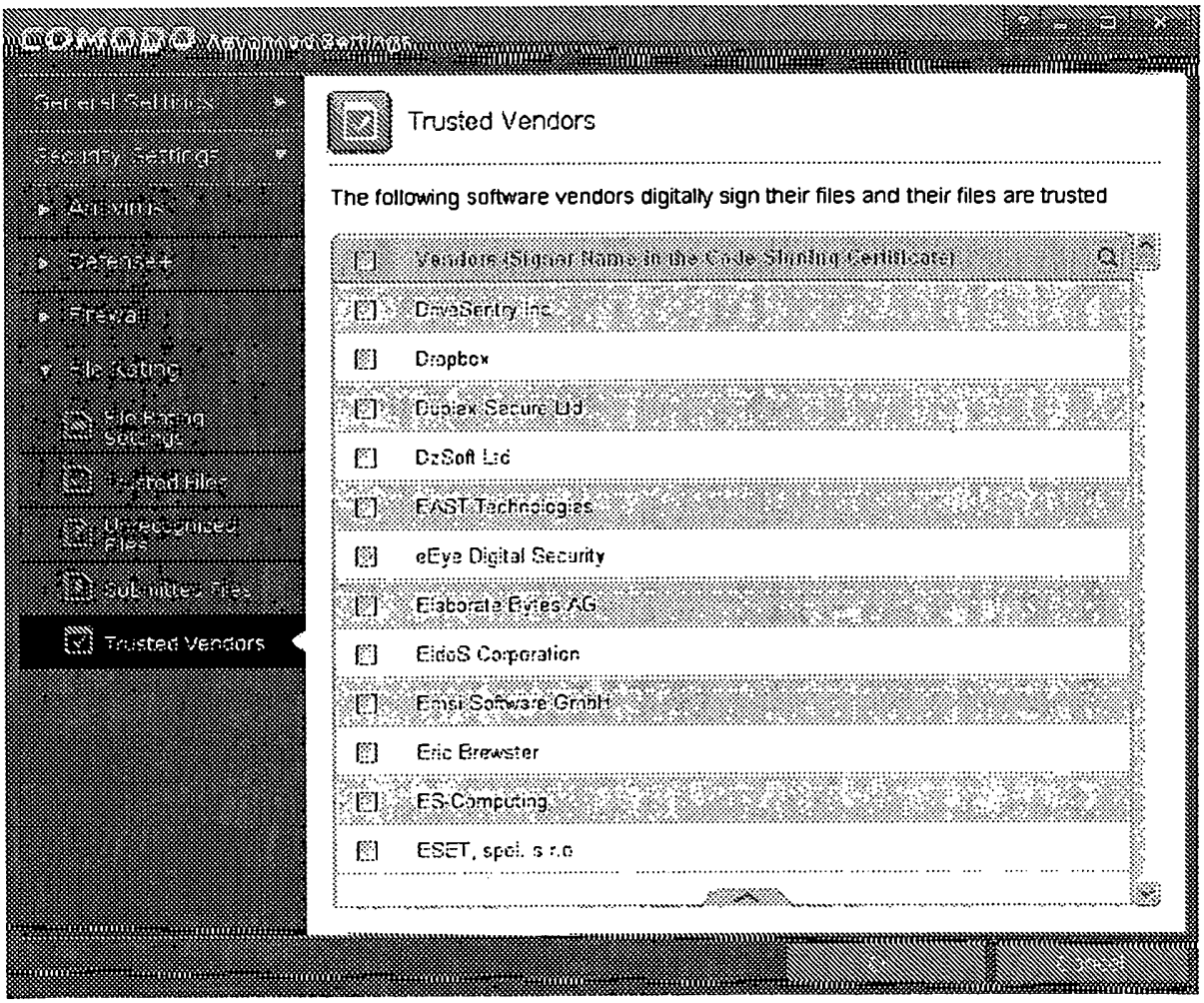
In Comodo Internet Security, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) OR that application has to be signed by one of the vendors in the 'Trusted Software Vendor List'.

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.

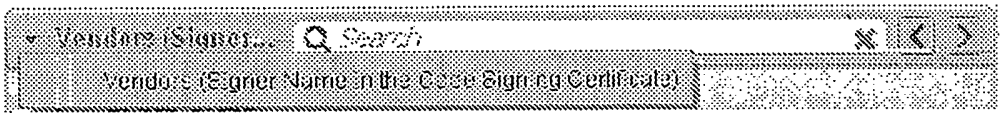
Software publishers may be interested to know that they can have their signatures added, free of charge, to the 'master' Trusted Software Vendor List that ships to all users with CIS. Details about this can be found at the foot of this page.

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.

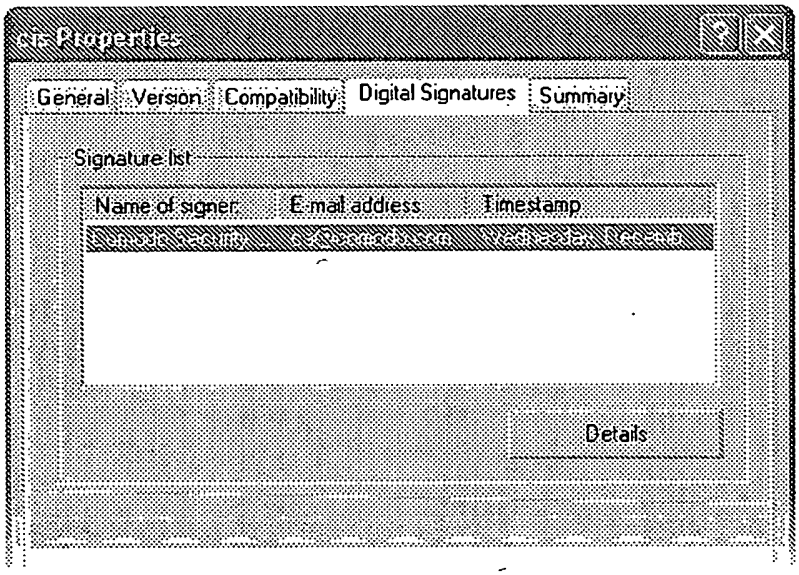
However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 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.

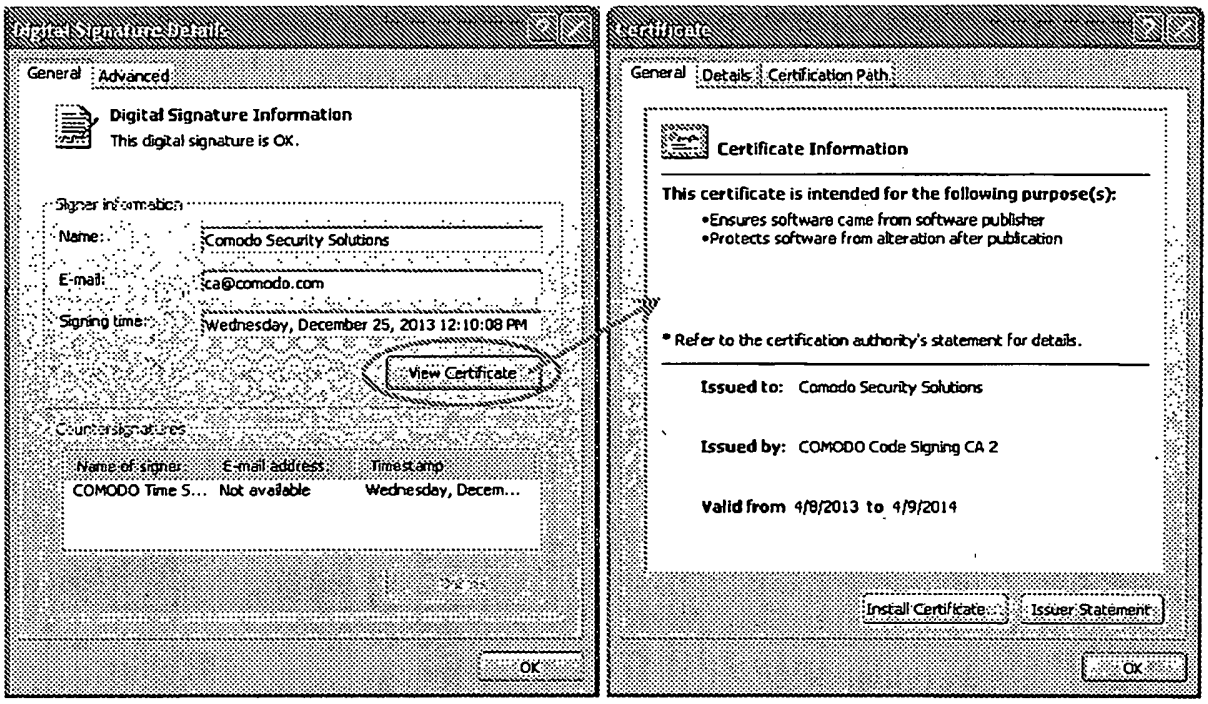
- Browse to the (default) installation directory of Comodo Internet Security.
- Right click on the file cis.exe.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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 of the certificate (the vendor) and the counter-signer (the Trusted CA) are different. See this example for more details.

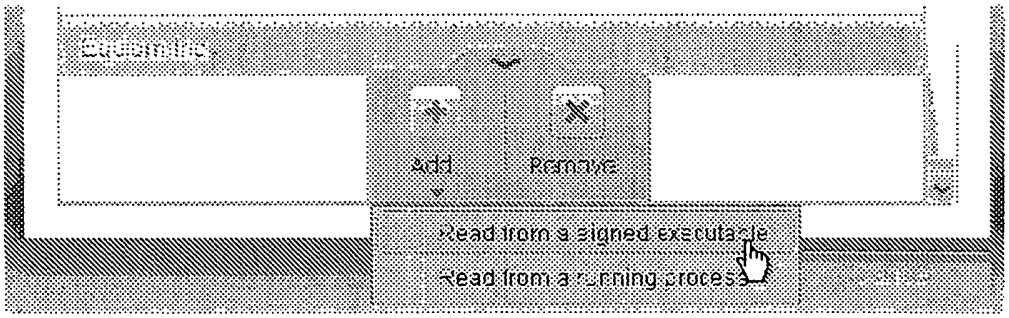
Adding and Defining a User-Trusted Vendor

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

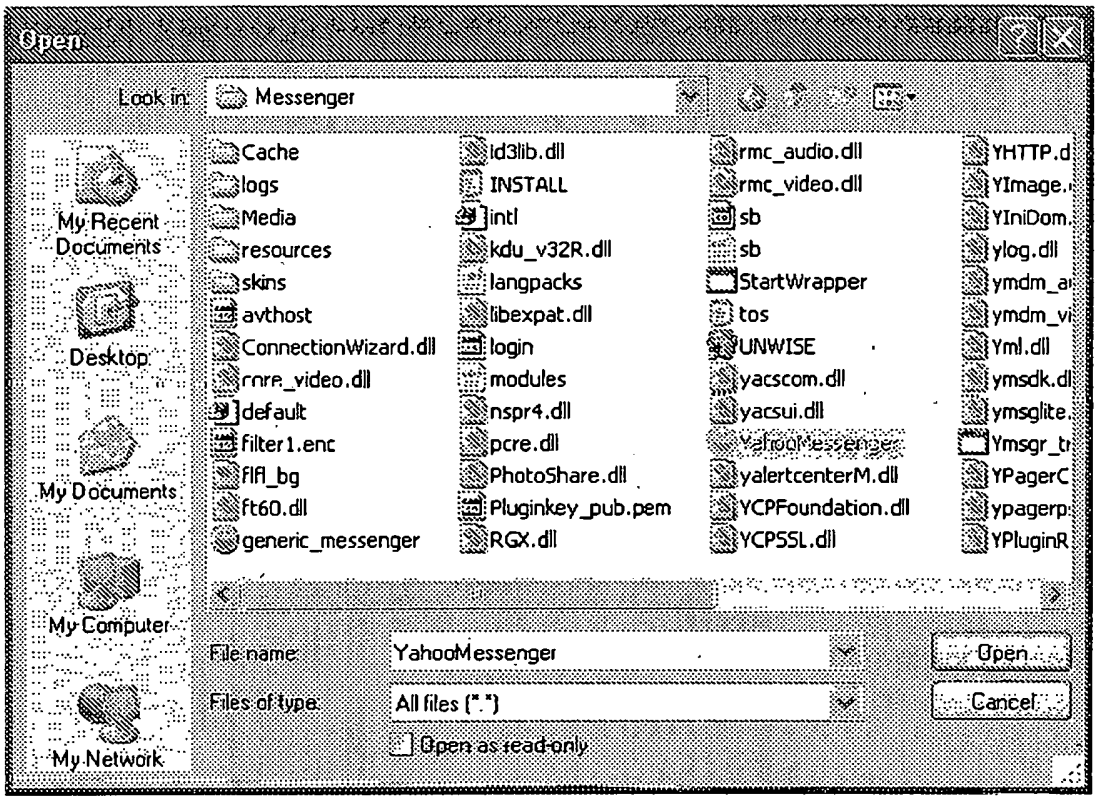
- By reading the vendor's signature from an executable file on your local drive
- By reading the vendor's signature from an running process

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

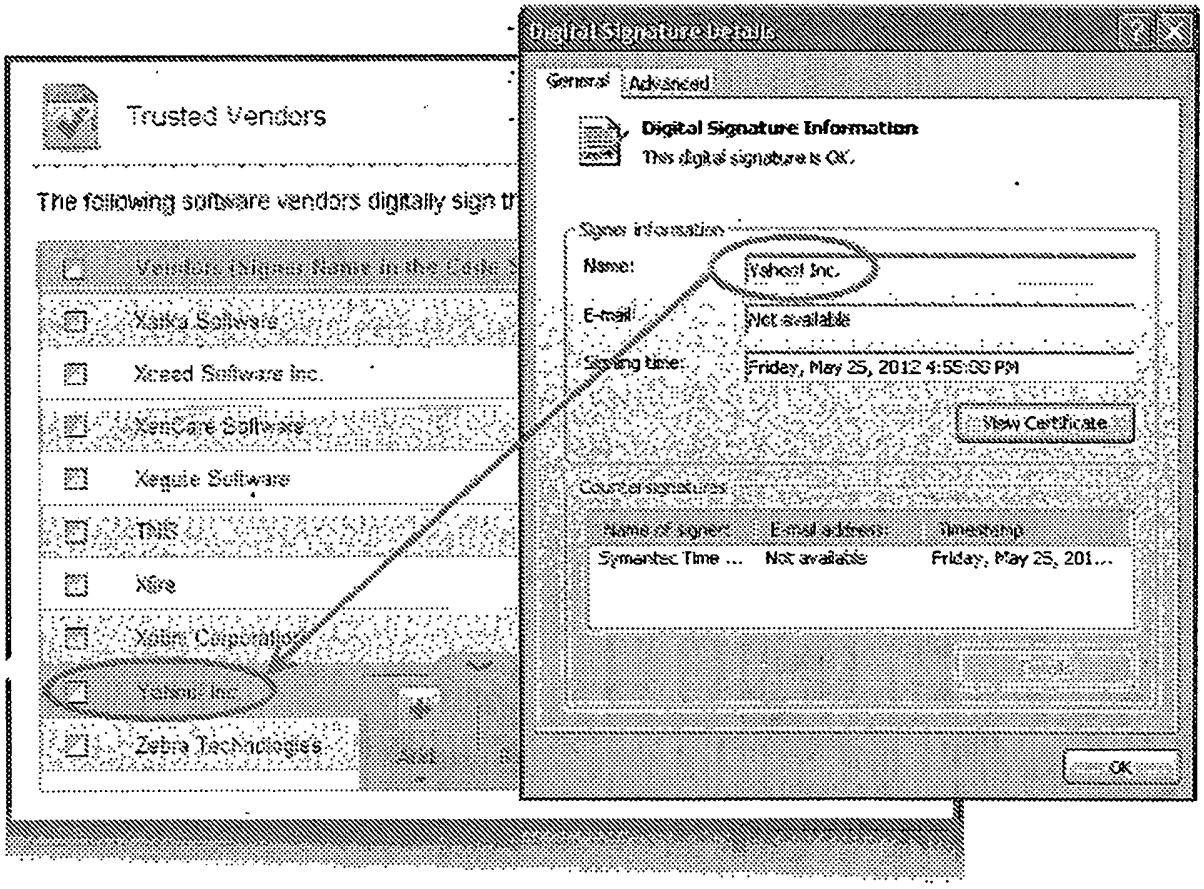
- Click the handle from the bottom center and choose 'Add' > 'Read from a signed executable'



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



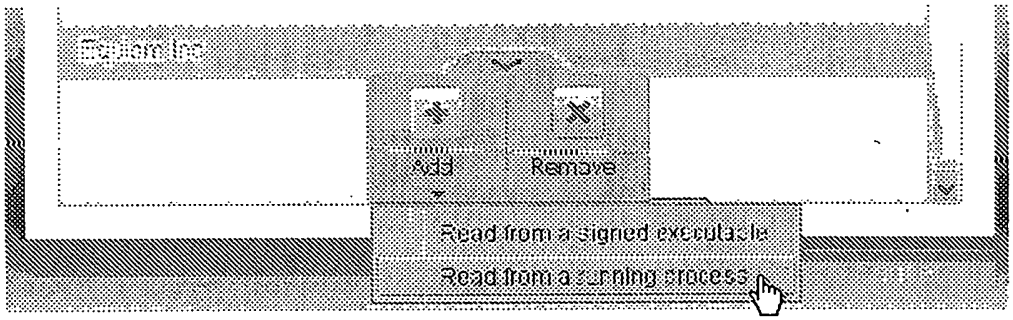
On clicking 'Open', Comodo Internet Security checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor (software signer) is added to the Trusted Vendor list (TVL):



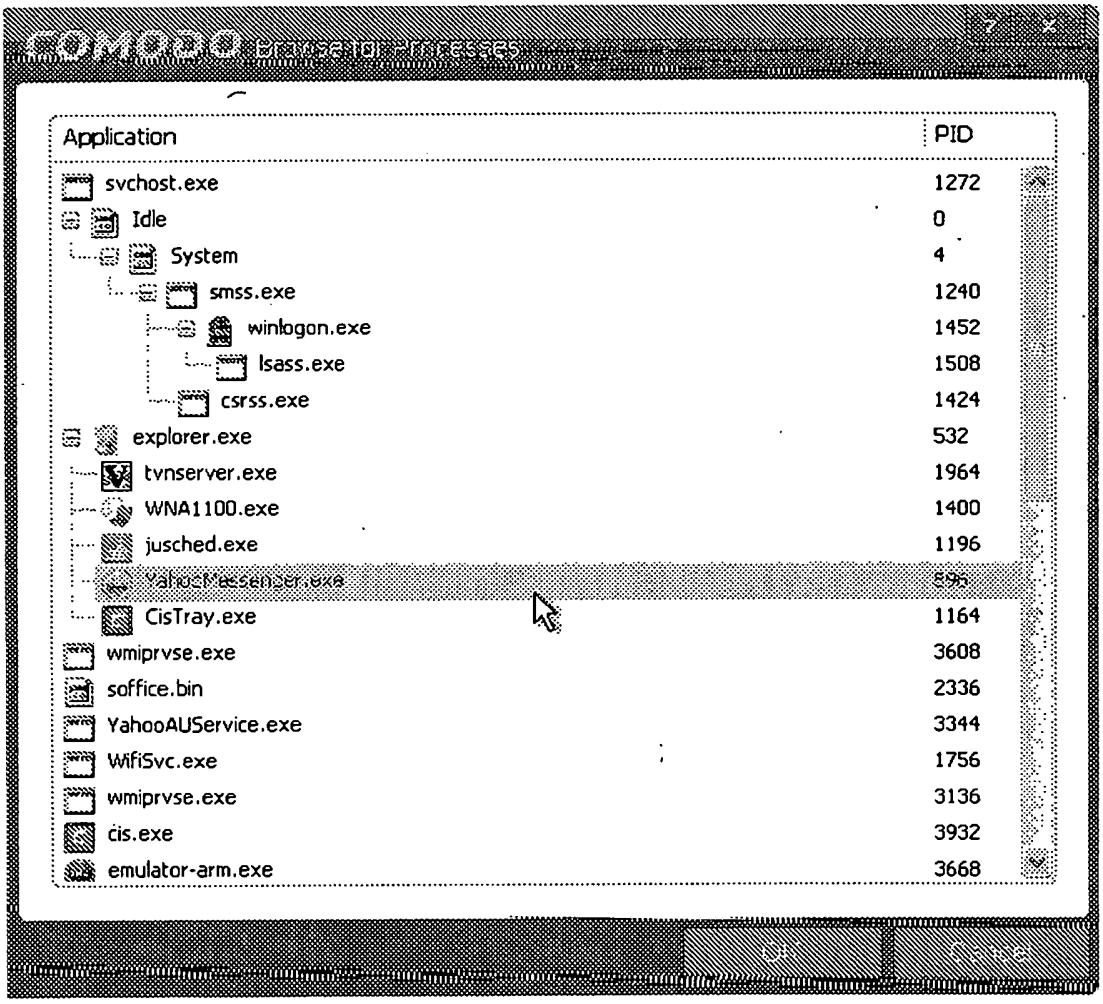
In the example above, Comodo Internet Security was able to verify and trust the vendor signature on YahooMessenger.exe because it had been counter-signed by the trusted CA 'Symantec'. The software signer 'Yahoo! Inc.' is now a Trusted Software Vendor and is added to the list. All future software that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

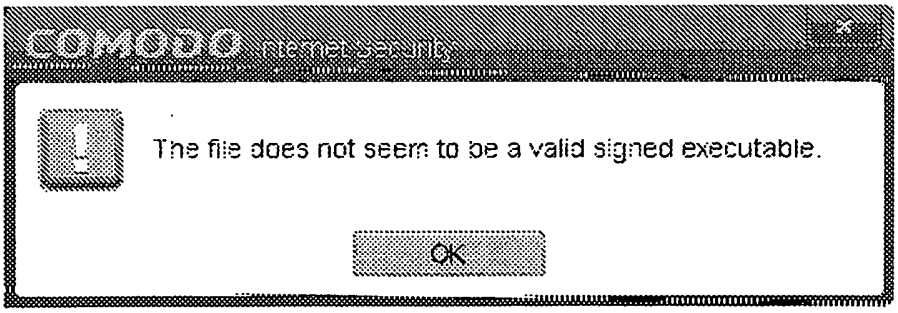


- Select the signed executable that you want to trust and click the 'OK' button.



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:

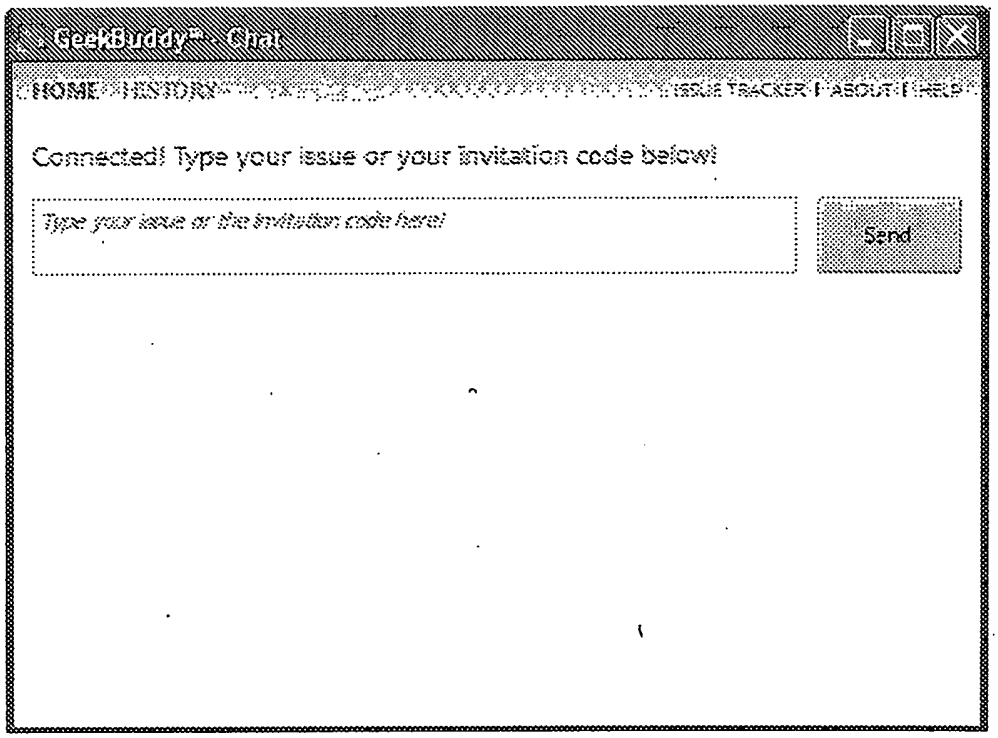
- **Virus & Malware Removal** - Our technicians remotely clear any detected viruses or malware that is found on your PC.
- **Internet and Online Identity Security** - Optimization of your computer's security settings to prevent loss of sensitive data and identity theft.
- **Printer or Email Account Setup** - 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.

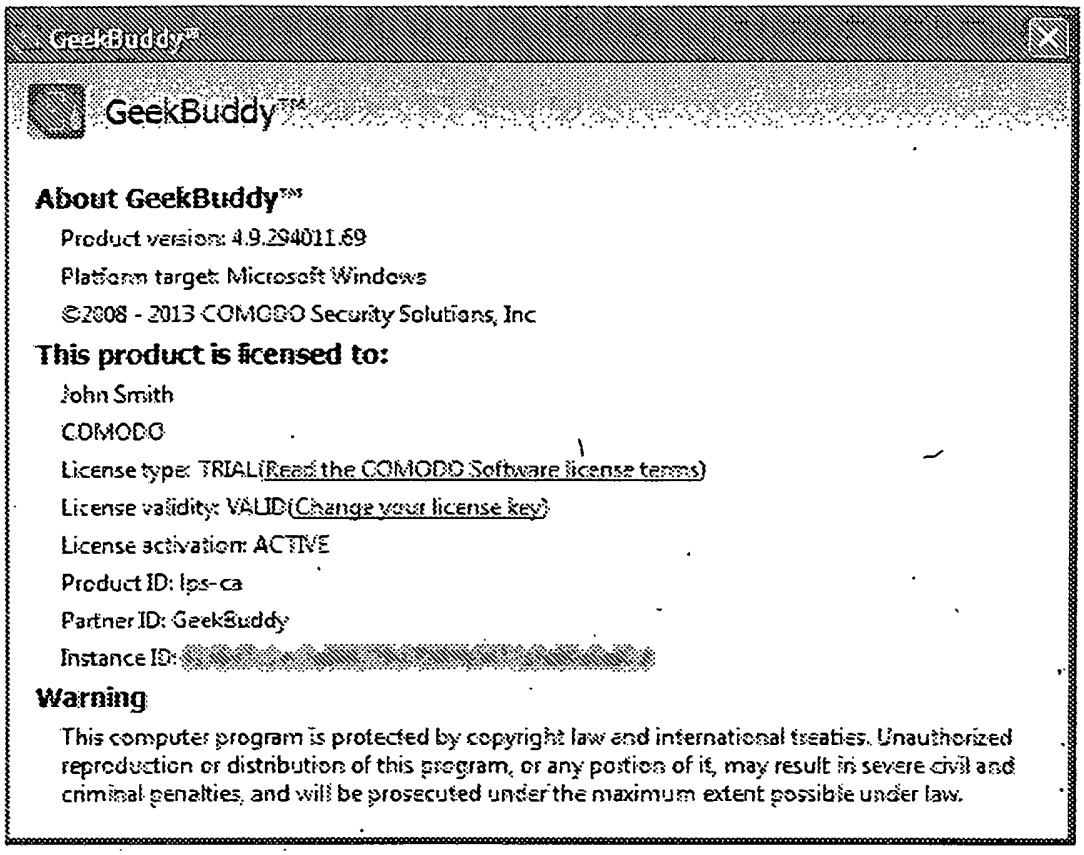
Start the GeekBuddy client by clicking the desktop shortcut icon  or from the 'Start Menu'.

The GeekBuddy Chat screen will be displayed.



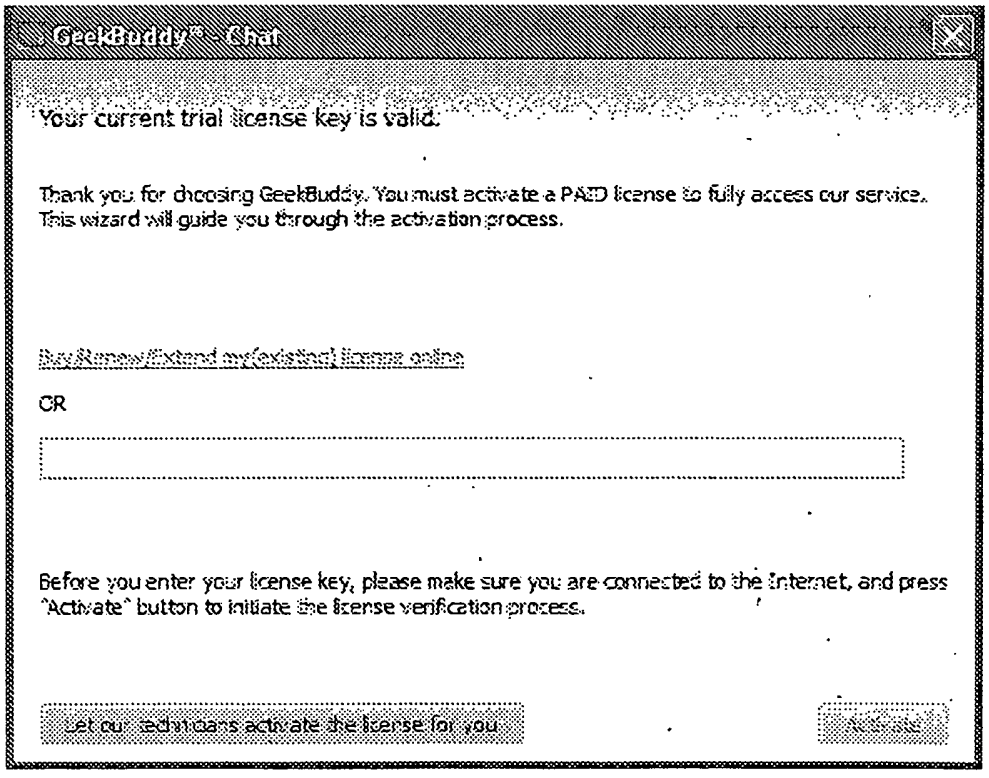
- Click the 'About' link at the top far right of the screen.

The About GeekBuddy screen will be displayed.

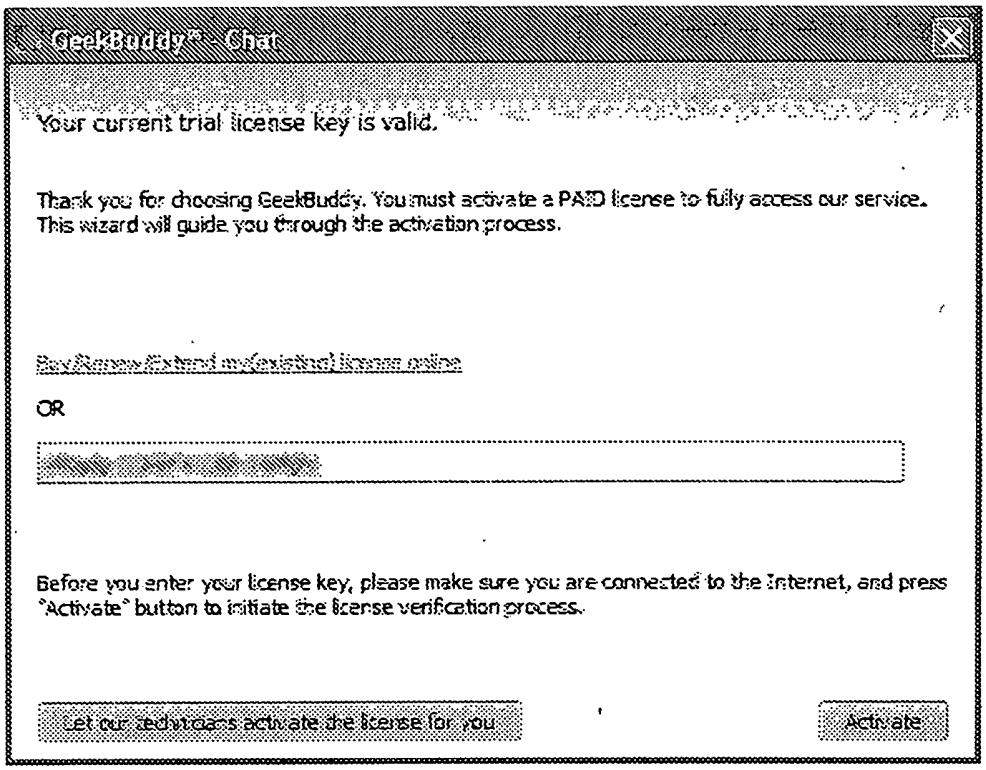


- Click the 'Change your license key' link in the screen.

The 'Activate your License' screen will be displayed.

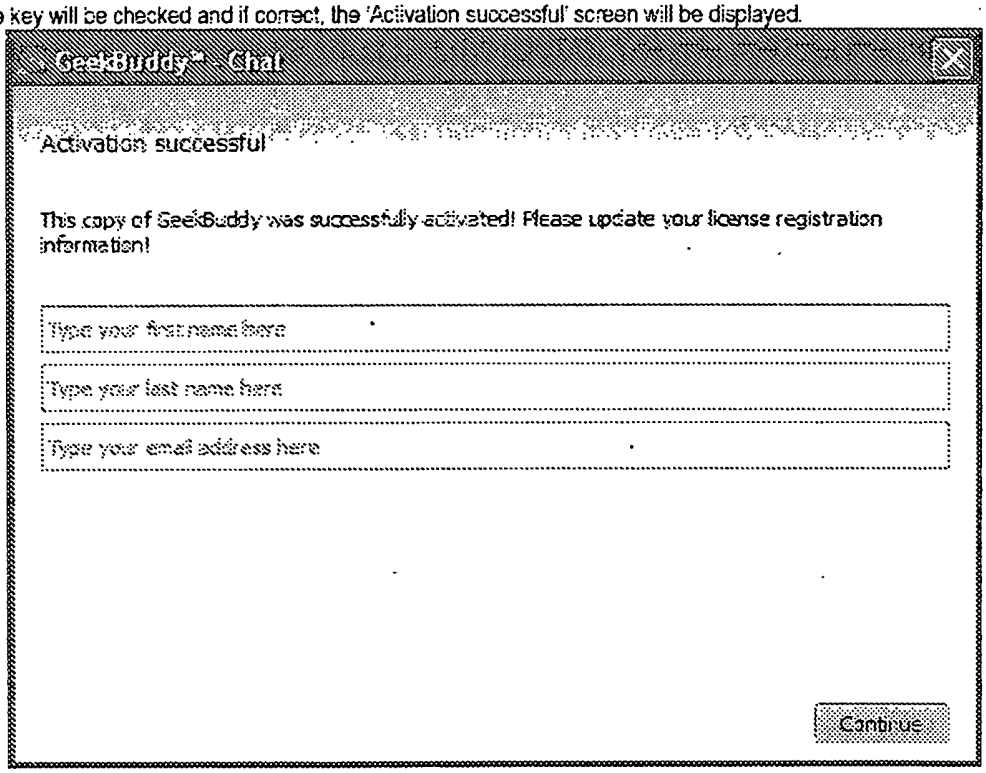


- Enter the License Key from your GeekBuddy retail package or the key you received through your email (for online purchases).

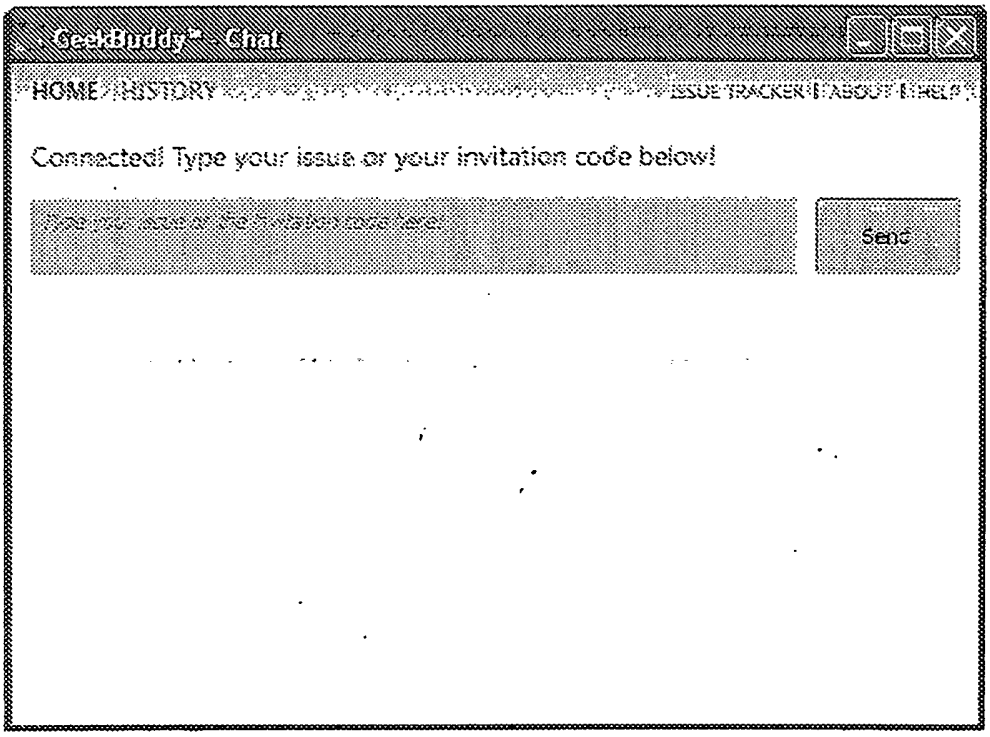


- Click the 'Activate' button or if you need more help on this click the 'Let our technicians activate the license for you' button.

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:

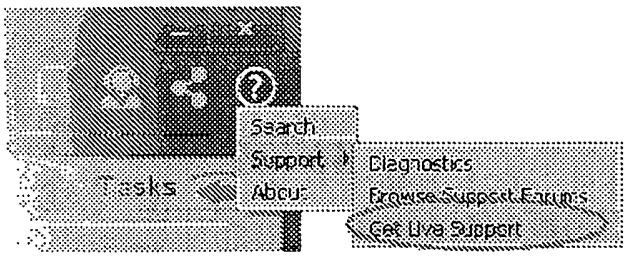
- Launching the Client and Using the Service
- Using Issue Tracker

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 .

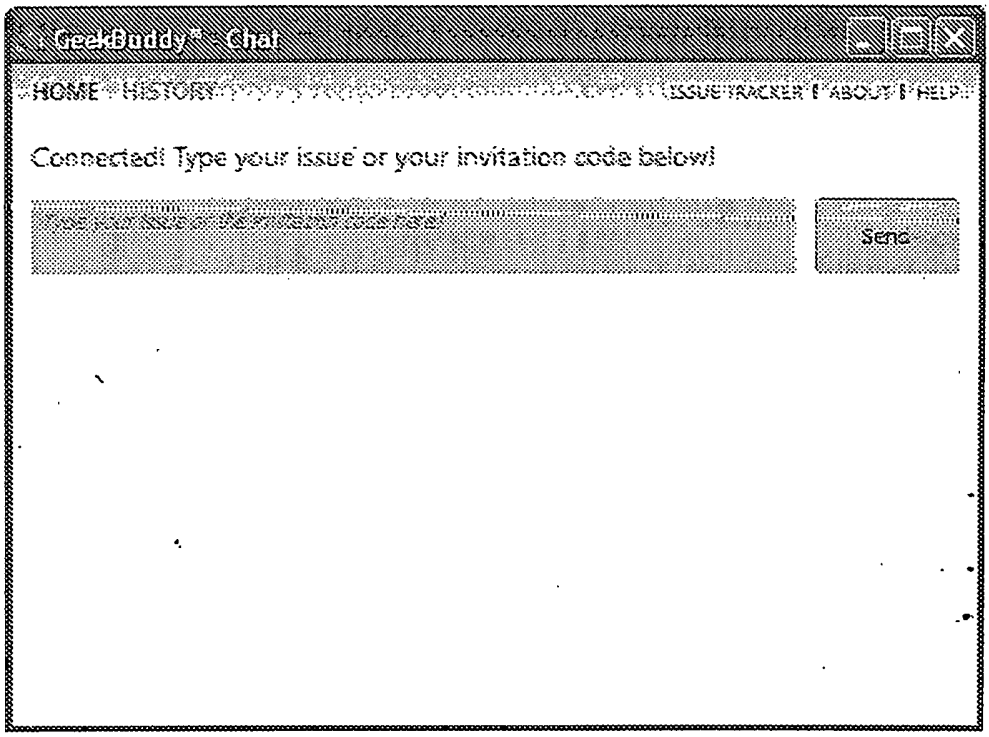
You can start the client and start a live chat session with a GeekBuddy expert using any one of the following methods:

- 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.



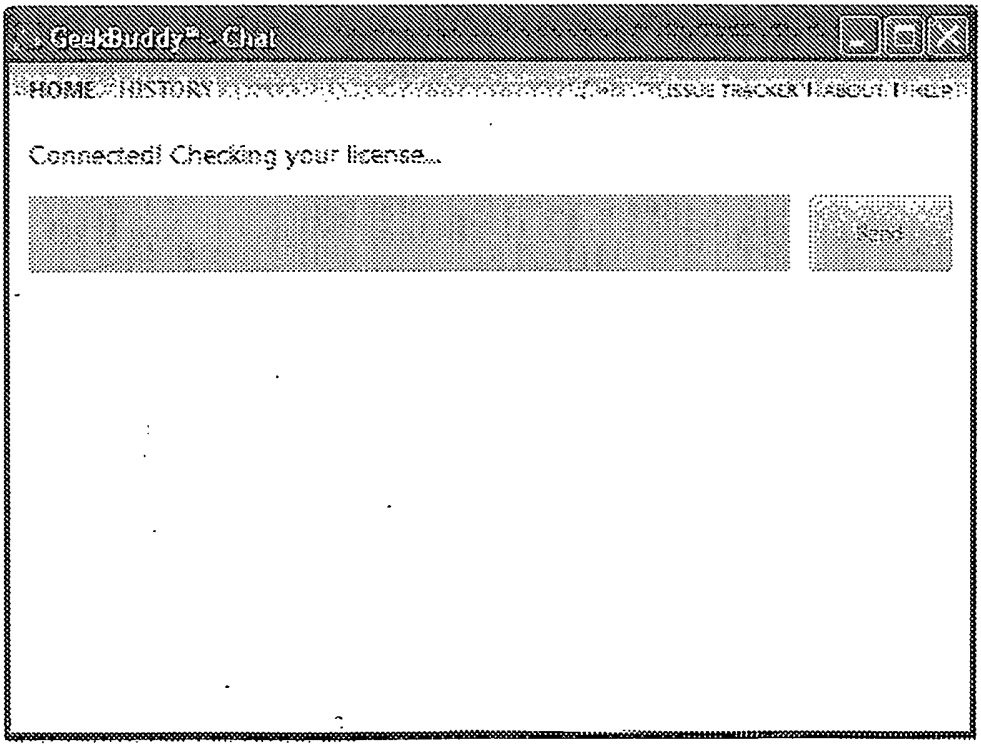
- Launch the GeekBuddy client directly from the Windows Start Menu - Click Start > All Programs > Comodo > GeekBuddy > GeekBuddy.

The GeekBuddy Home screen will open.

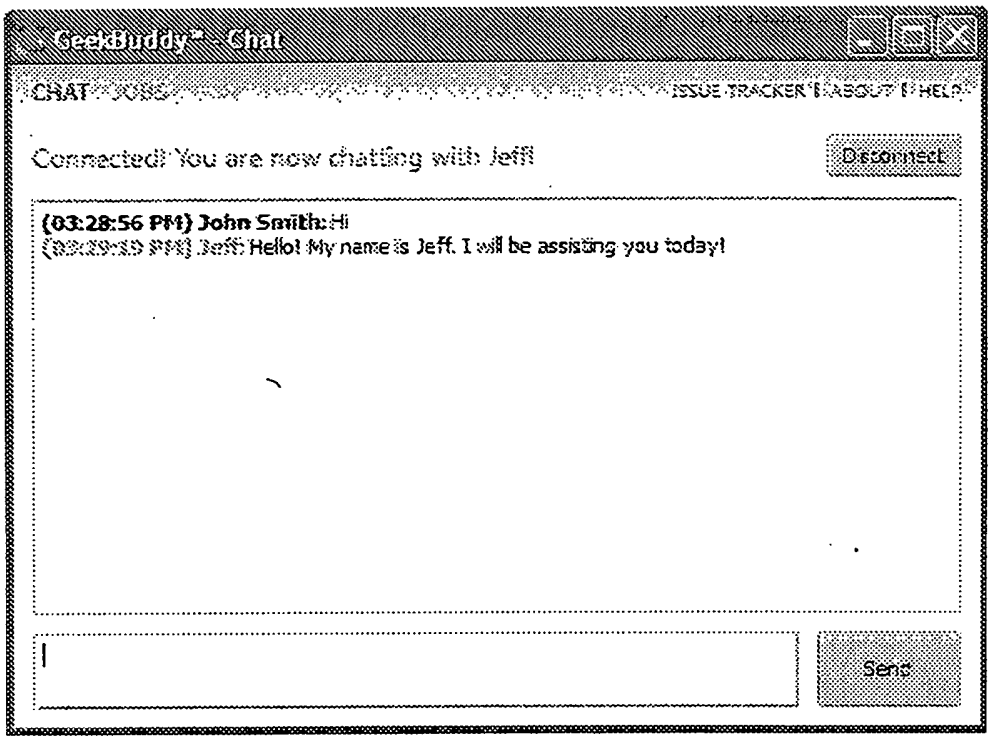


- To contact a support technician, type your issue in the field or enter the invitation code if you have it and click the 'Send' button.

You will be connected to a GeekBuddy...



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

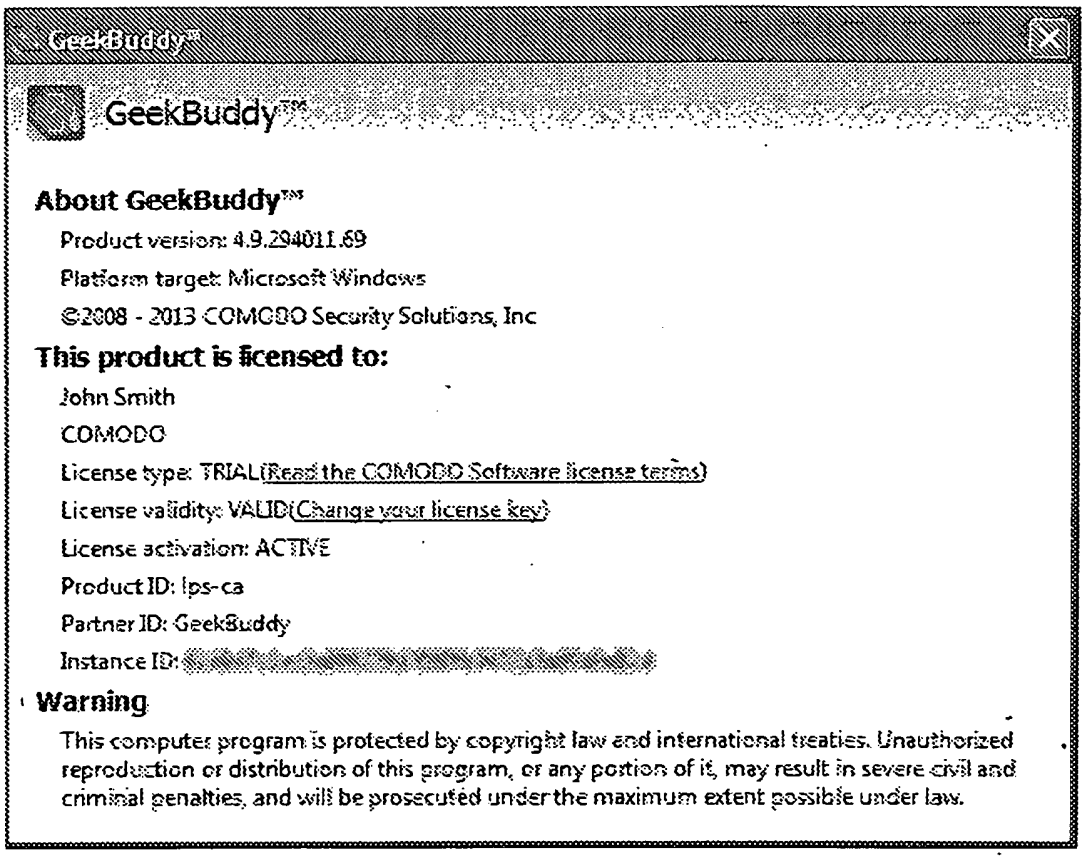


- Proceed to chat now.
- Explain your problem. The technician will assess your problem with you and work with you to fix any issues.

About GeekBuddy

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

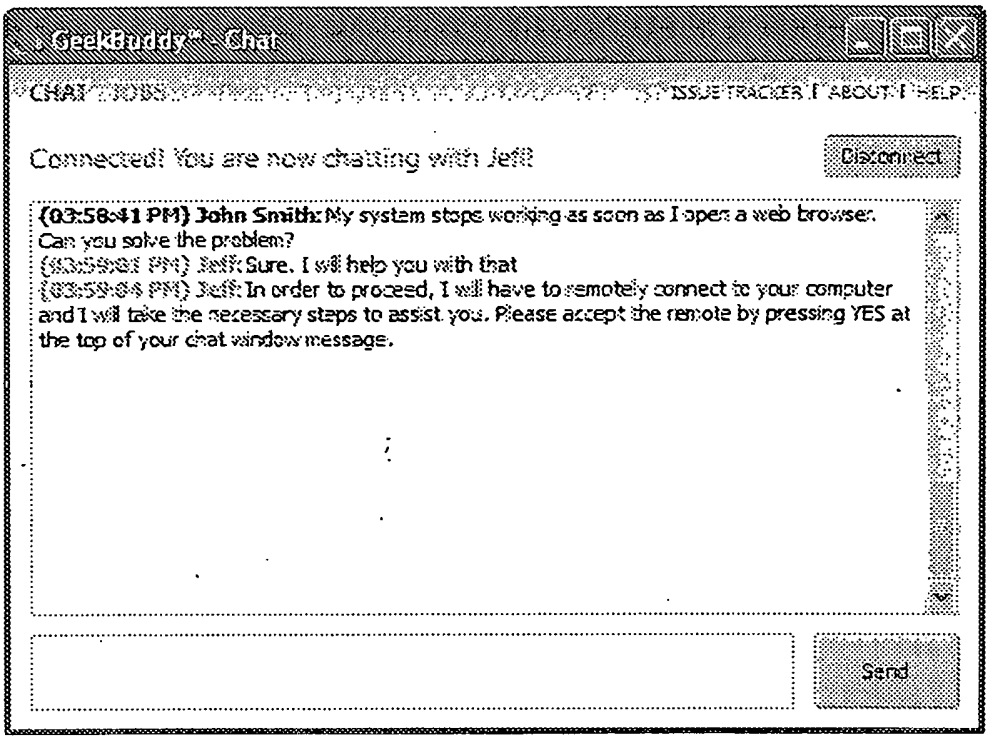
The About GeekBuddy information screen will be displayed.



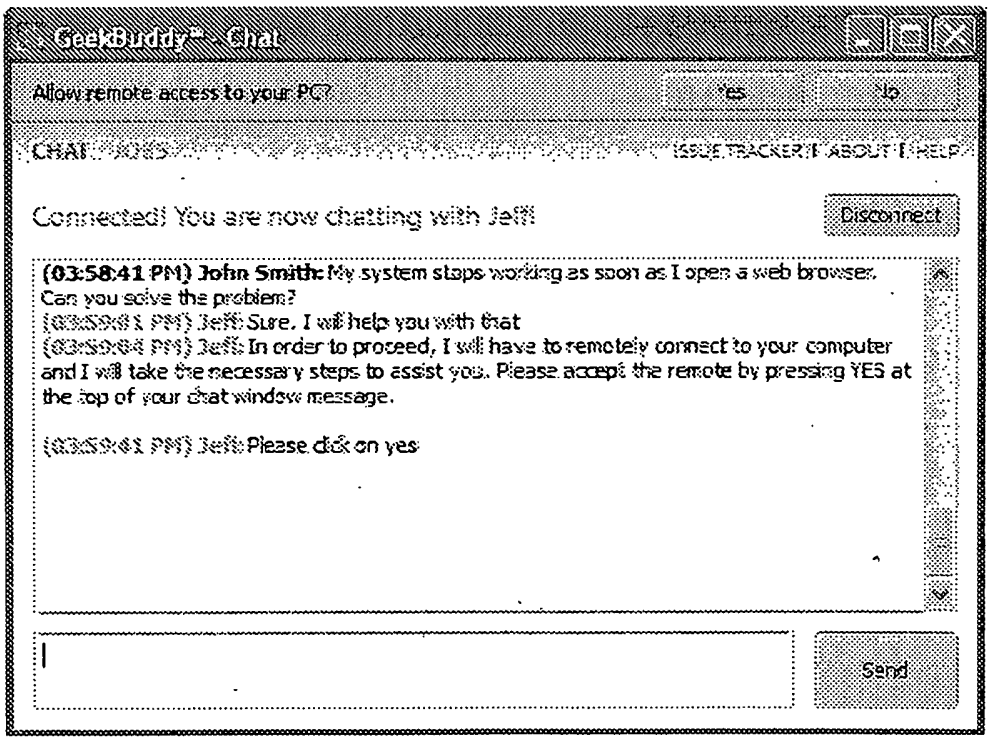
The 'About' dialog displays the copyright and product version information. The screen also displays information about the licensee, its validity and to change the license key or activate the account.

7.4. Accepting Remote Desktop Requests

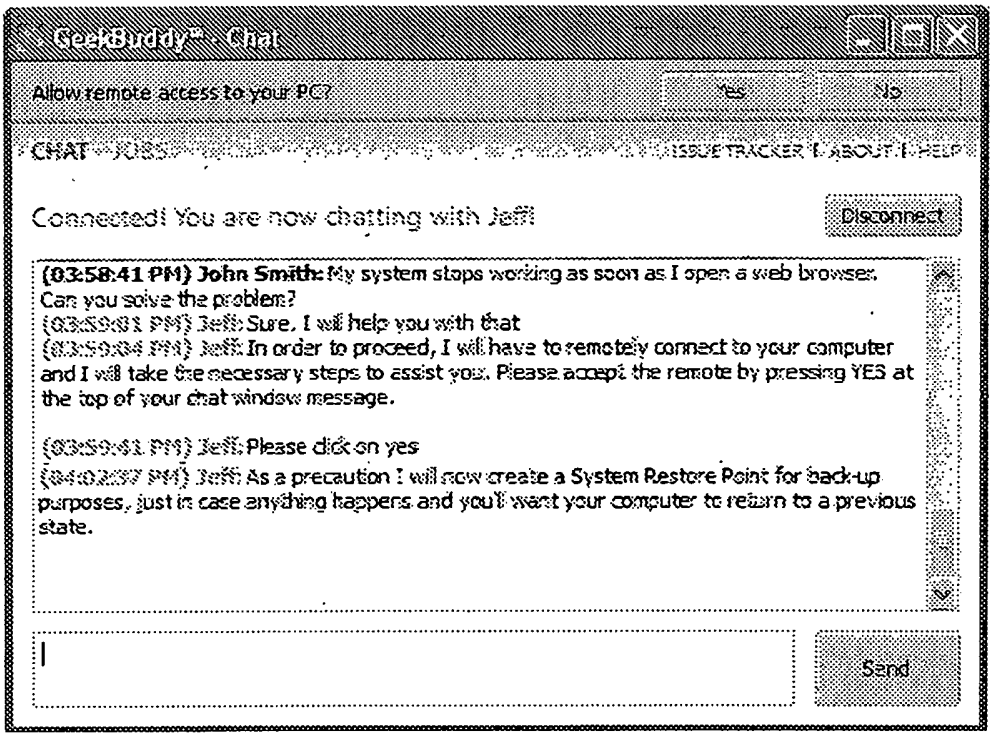
In order to solve certain issues, the support technician may need to directly connect to your computer via aremote connection. Remote control can only go ahead if you grant permission for this to happen. Our technicians will always request your permission via the chat window.



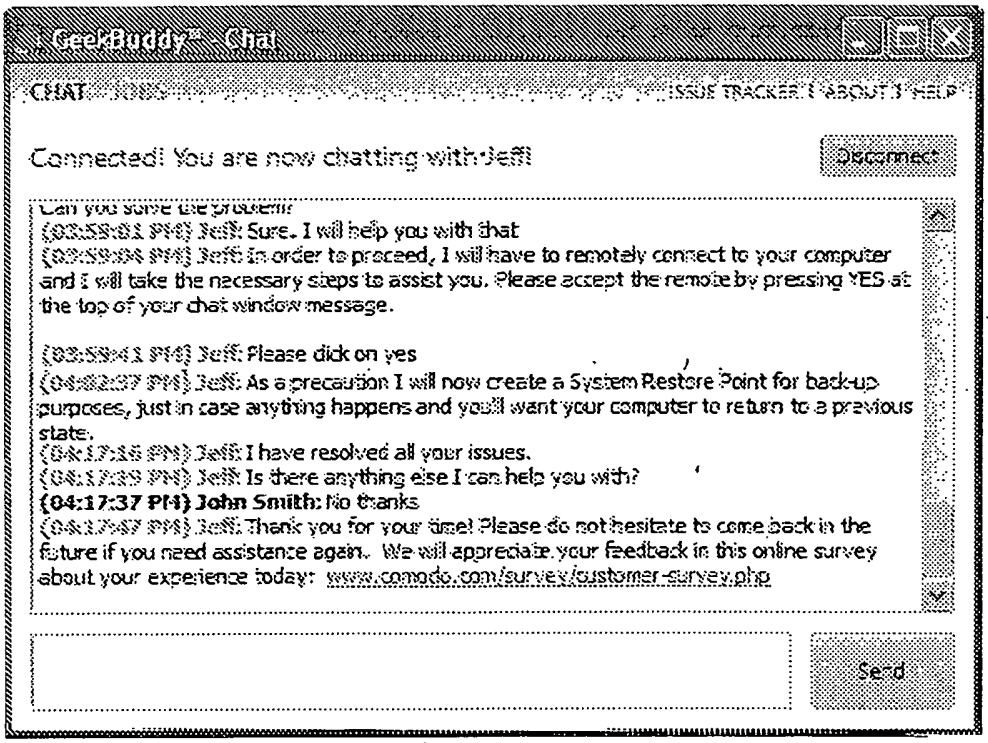
The technician will ask your permission before he or she makes any changes to your machine. Such changes might include installing programs, creating system restore points or deleting unnecessary or infected files.



- 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

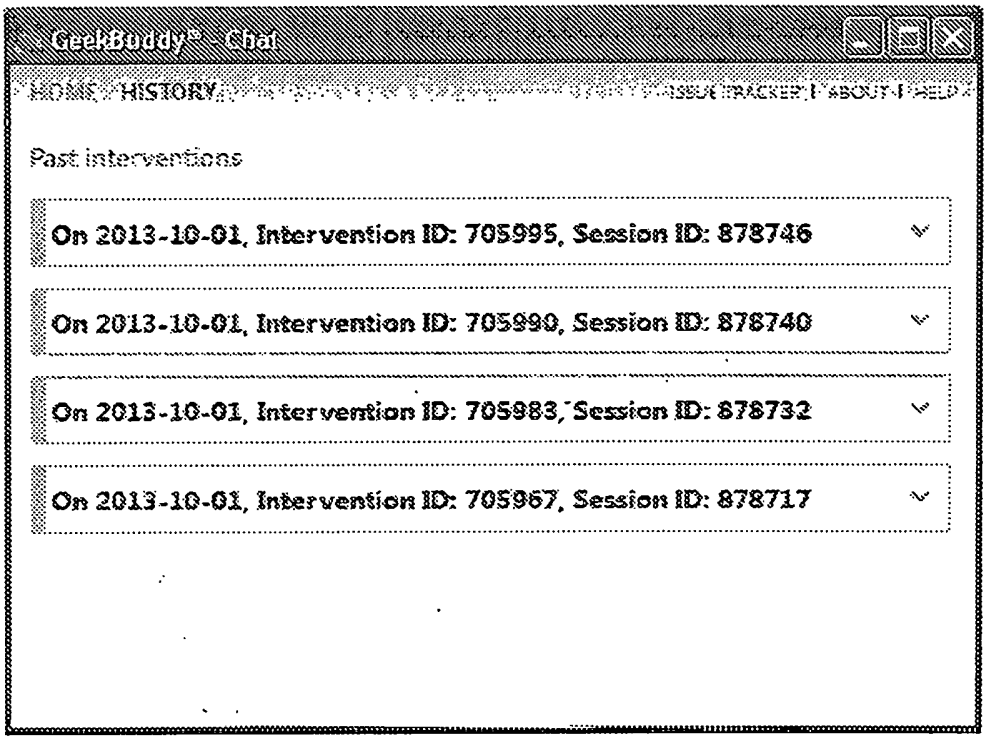
GeekBuddy keeps a local record of every chat session you have with a Comodo technician. Clicking the 'History' link at the top

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.

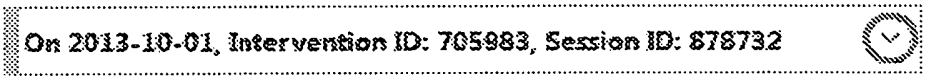
To view history of chat sessions

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

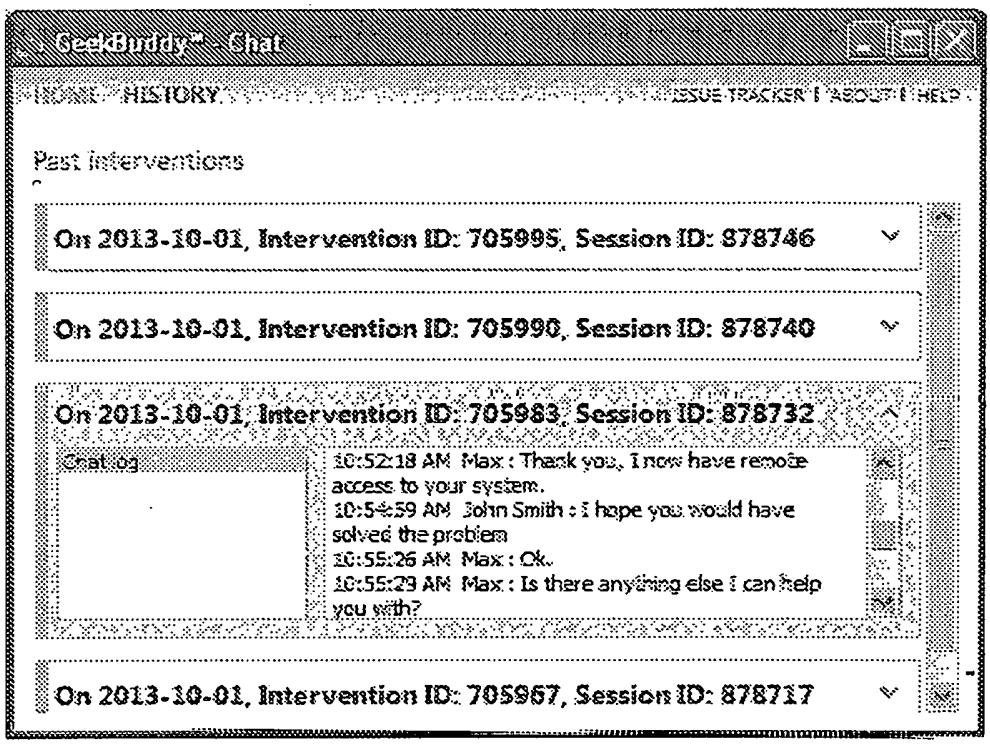
All the sessions will be displayed.



- 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.

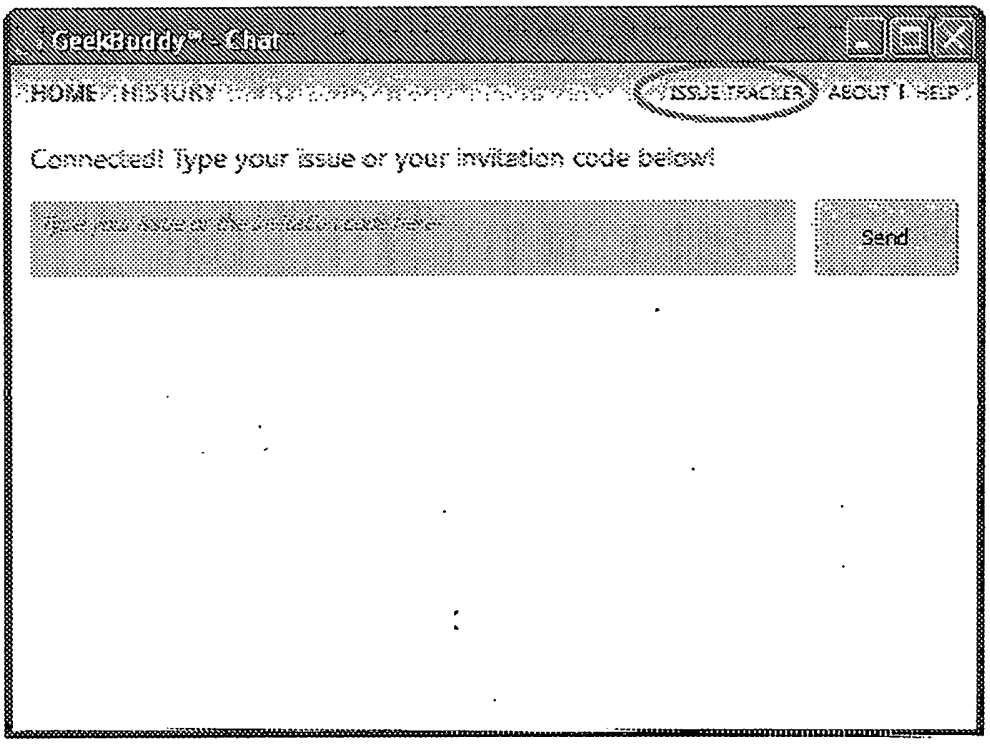


Similarly you can view the chat history of other sessions also.

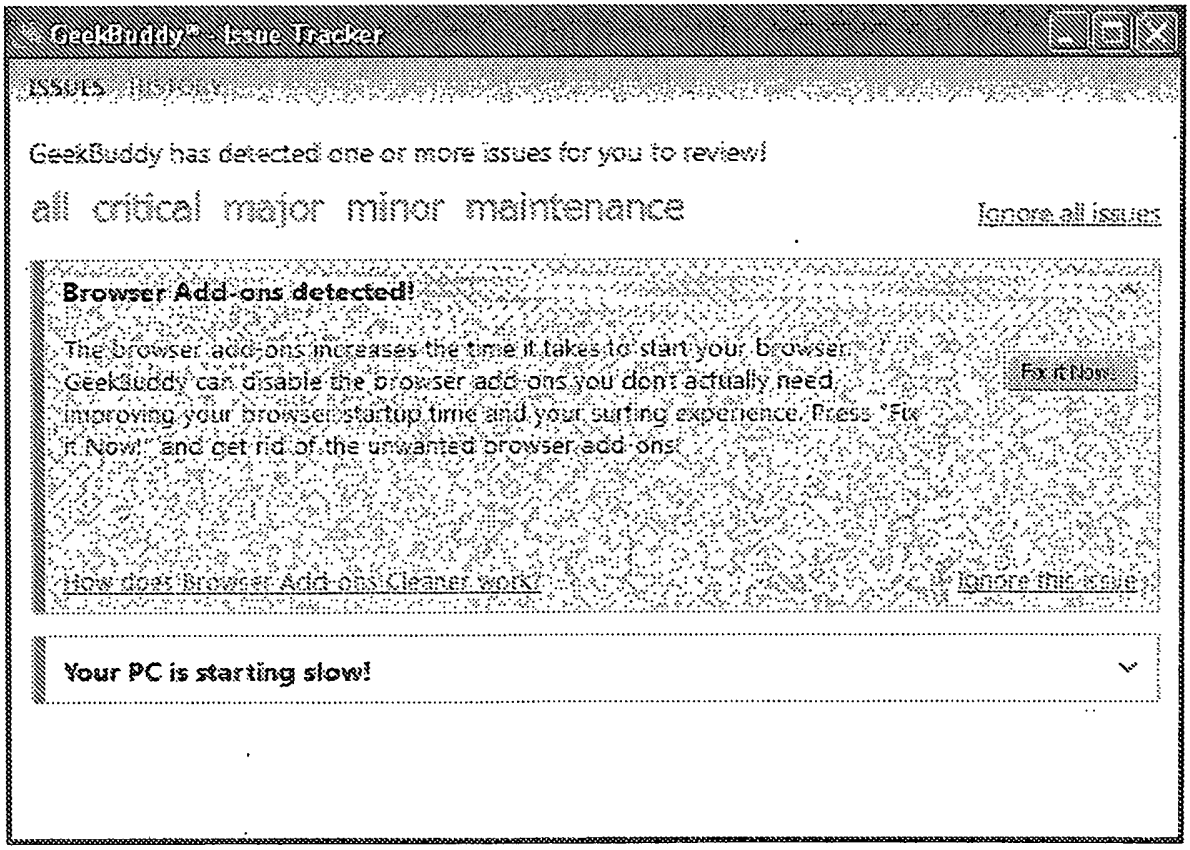
7.6. Using Issue Tracker

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.



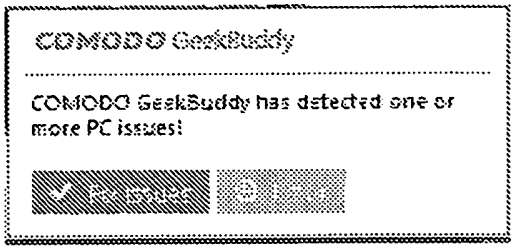
The Issue Tracker interface will list the problems that it has detected.



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.

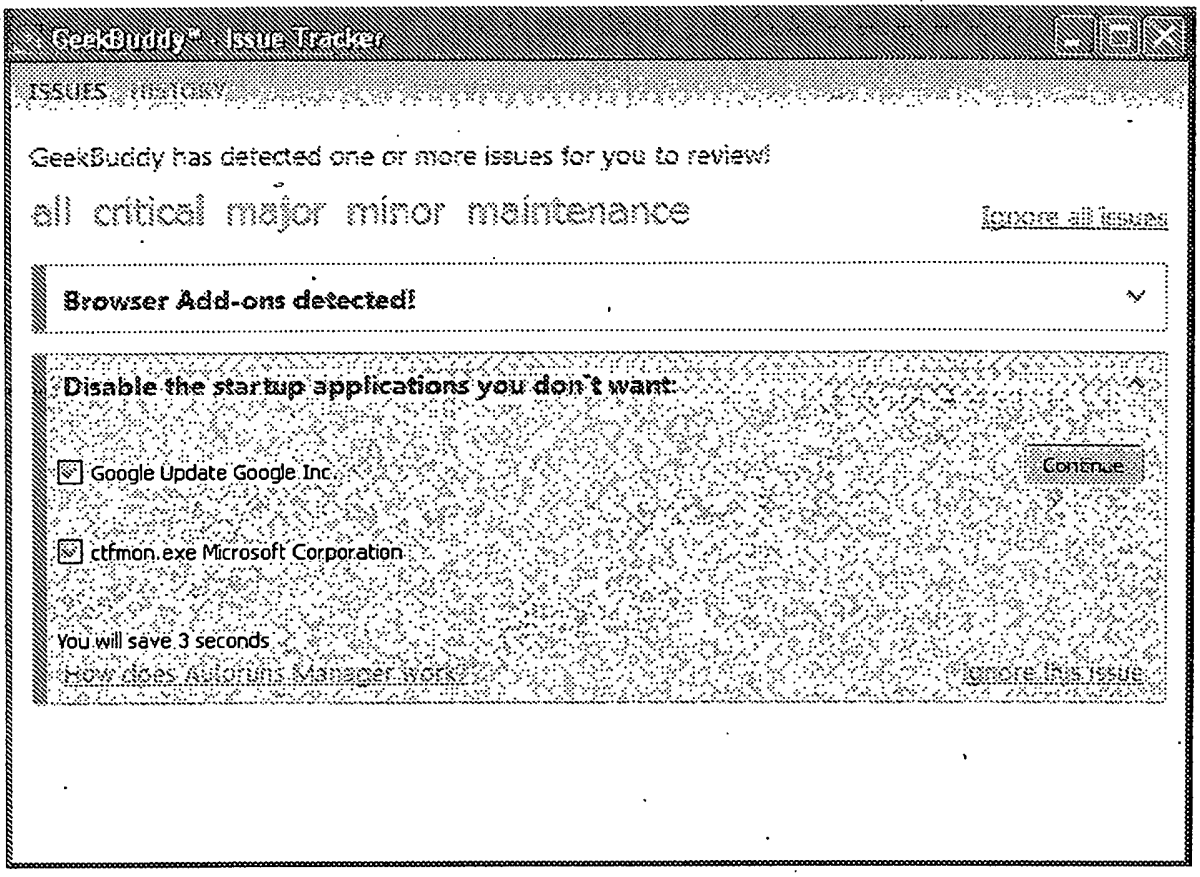
The Issue Tracker interface will list the problems that it has detected.

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

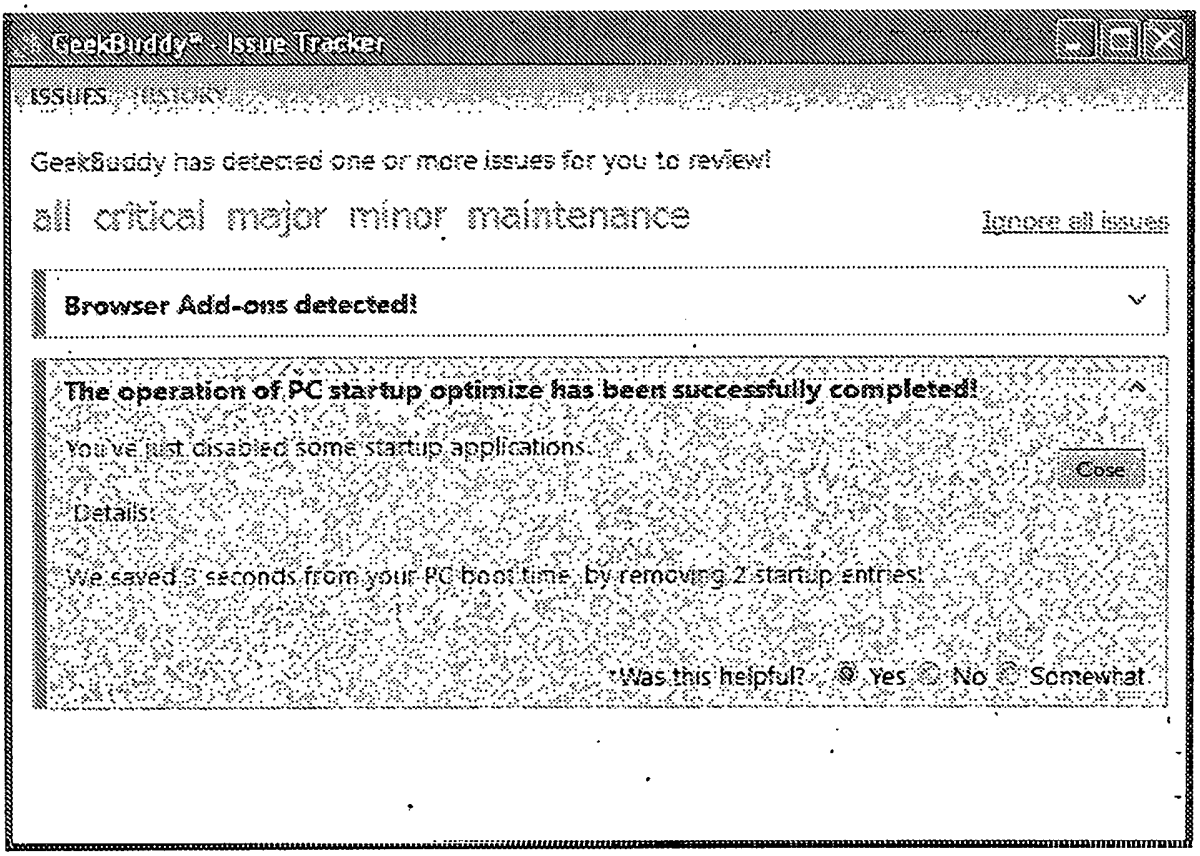
Some of the common problems that occur in any computer are junk registry entries, slow bootup time and the presence of files that might compromise your privacy.

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

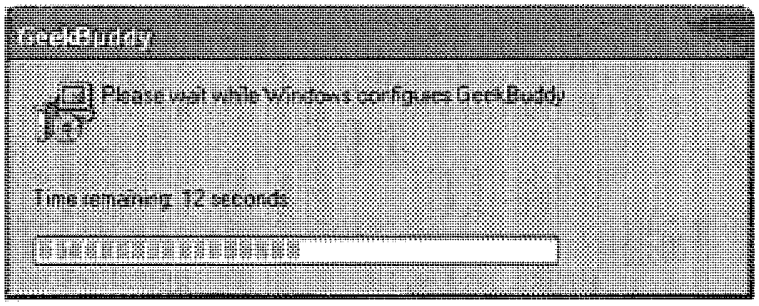
To uninstall Comodo GeekBuddy

- 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.

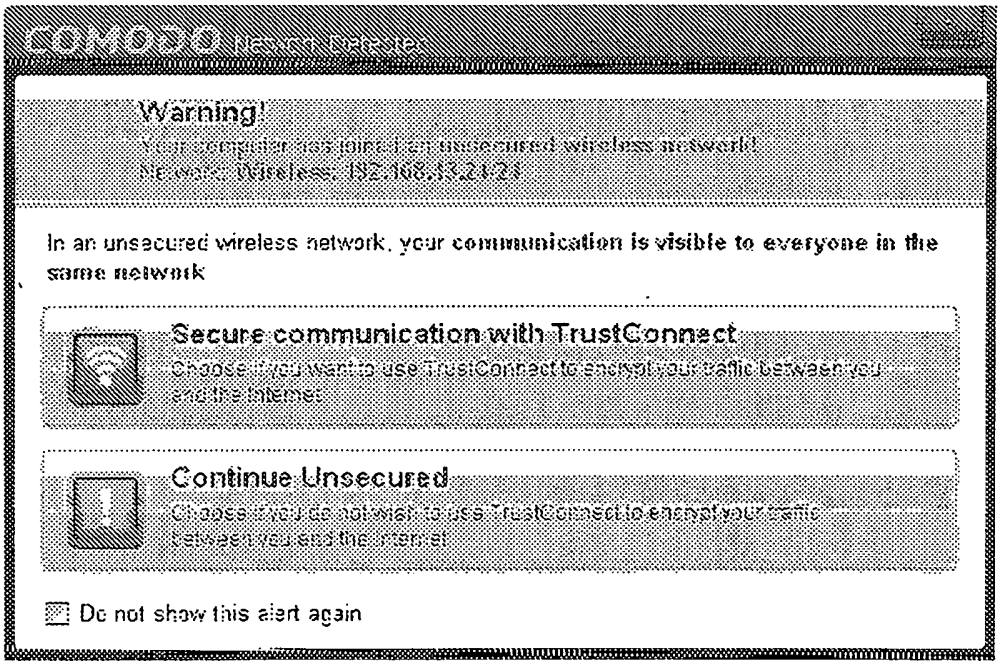
The progress of GeekBuddy removal will be displayed...



--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.

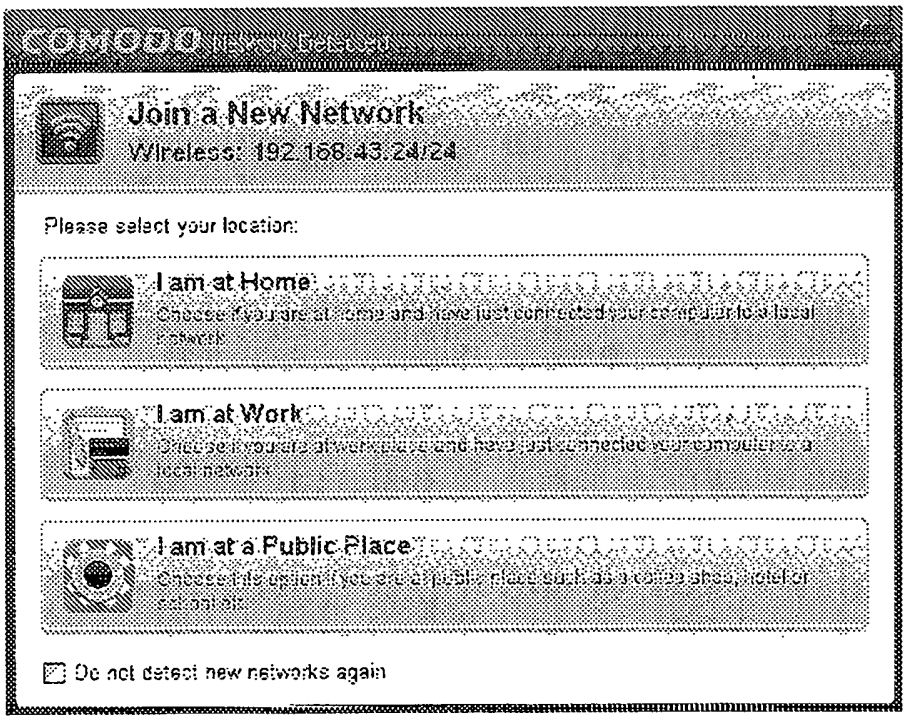
TrustConnect System Requirements

- 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.

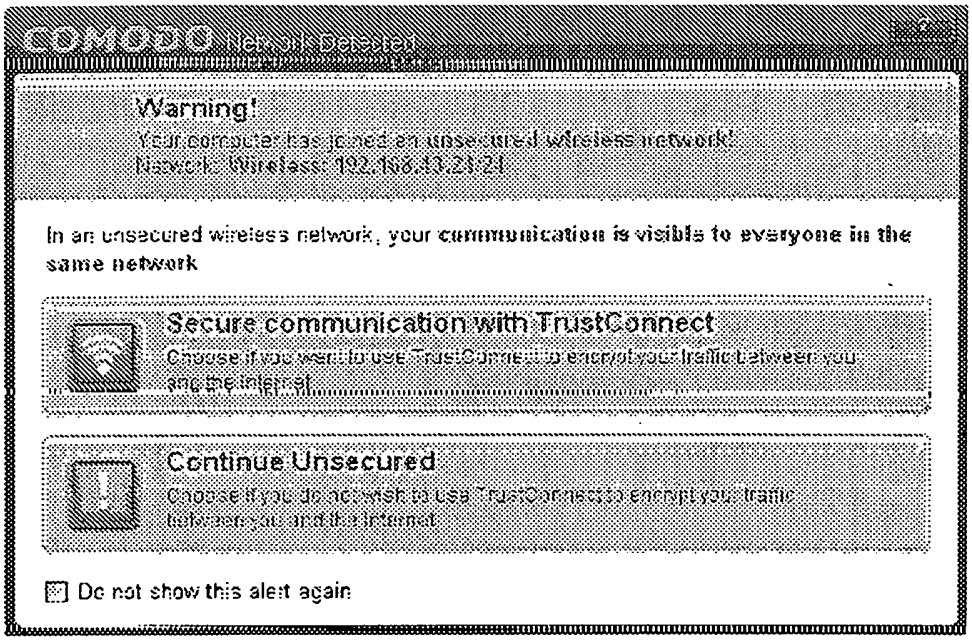
Comodo Internet Security Complete Users

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.



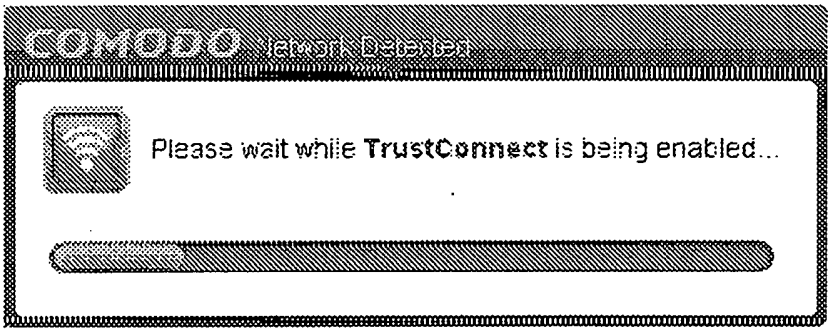
- Select your location from the dialog

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...



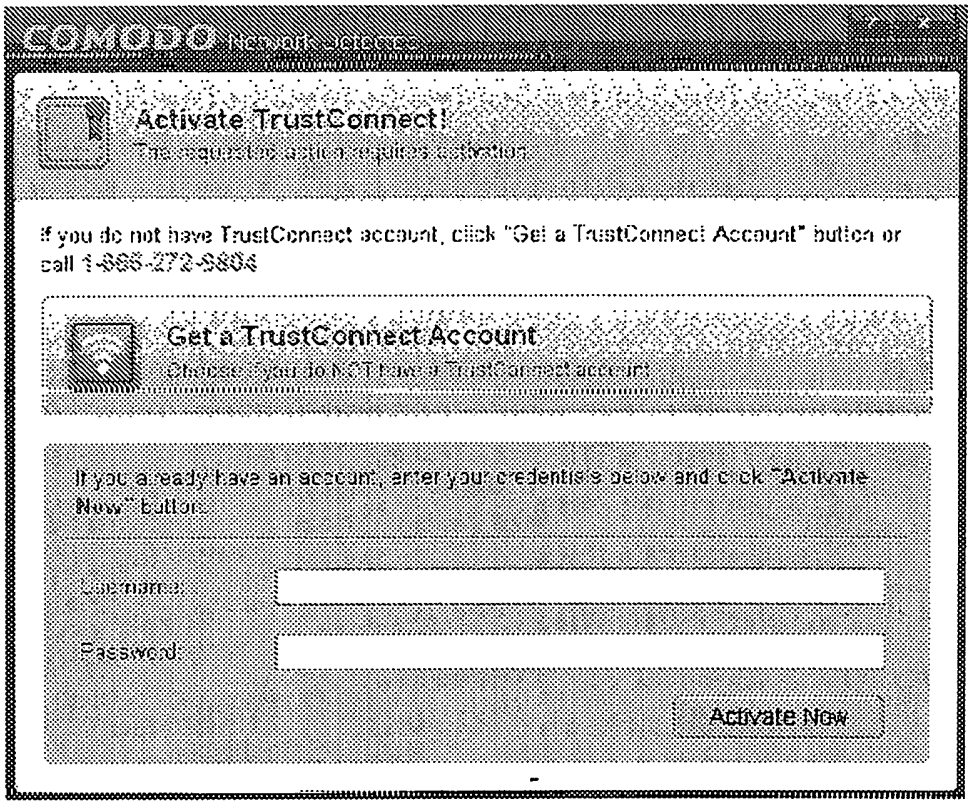
...and on successful connection, you can view the details in the system tray.



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.

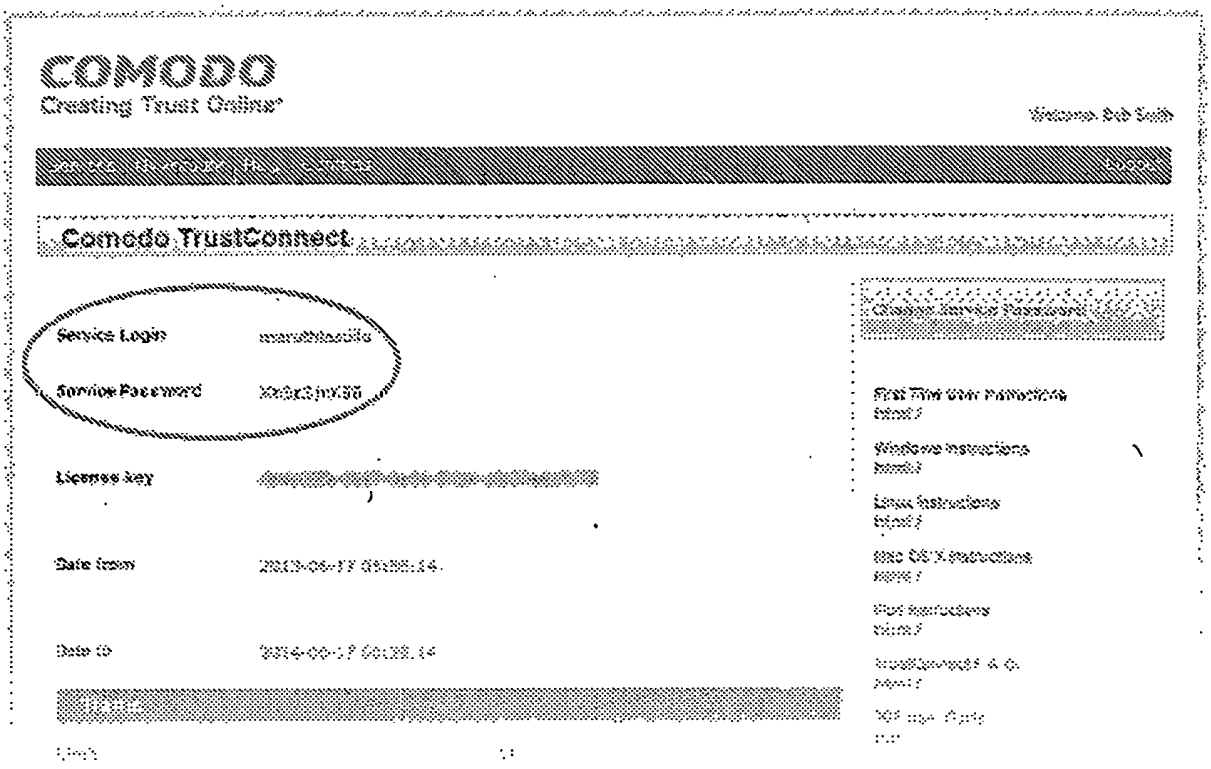


- You can purchase the TC service by clicking the 'Get a TrustConnect Account', enter the TC service credentials and activate the service.
- If you already have a TC account, enter the TC service credentials in the Username and Password fields and click the 'Activate Now' button.

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:

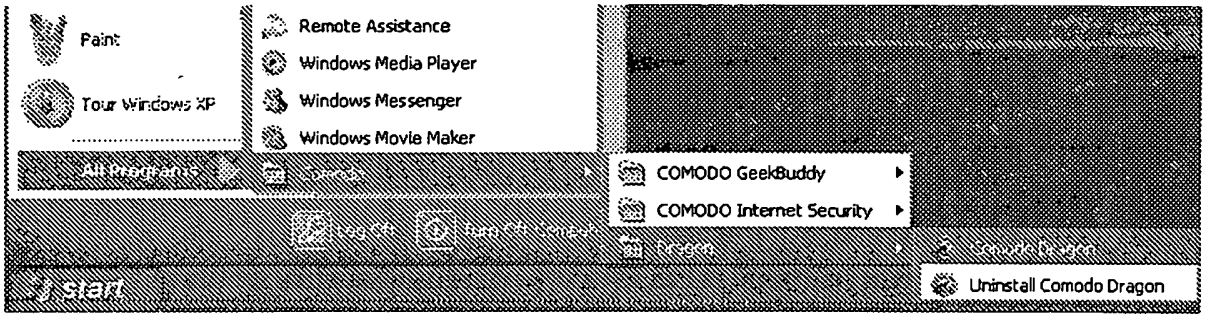
- Has privacy enhancements that surpass those in Chromium's technology
- Has Domain Validation technology that identifies and segregates superior SSL certificates from inferior ones
- Stops cookies and other Web spies
- PrivDog can disable cookies, spyware, malware and other trackers.
- Prevents all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

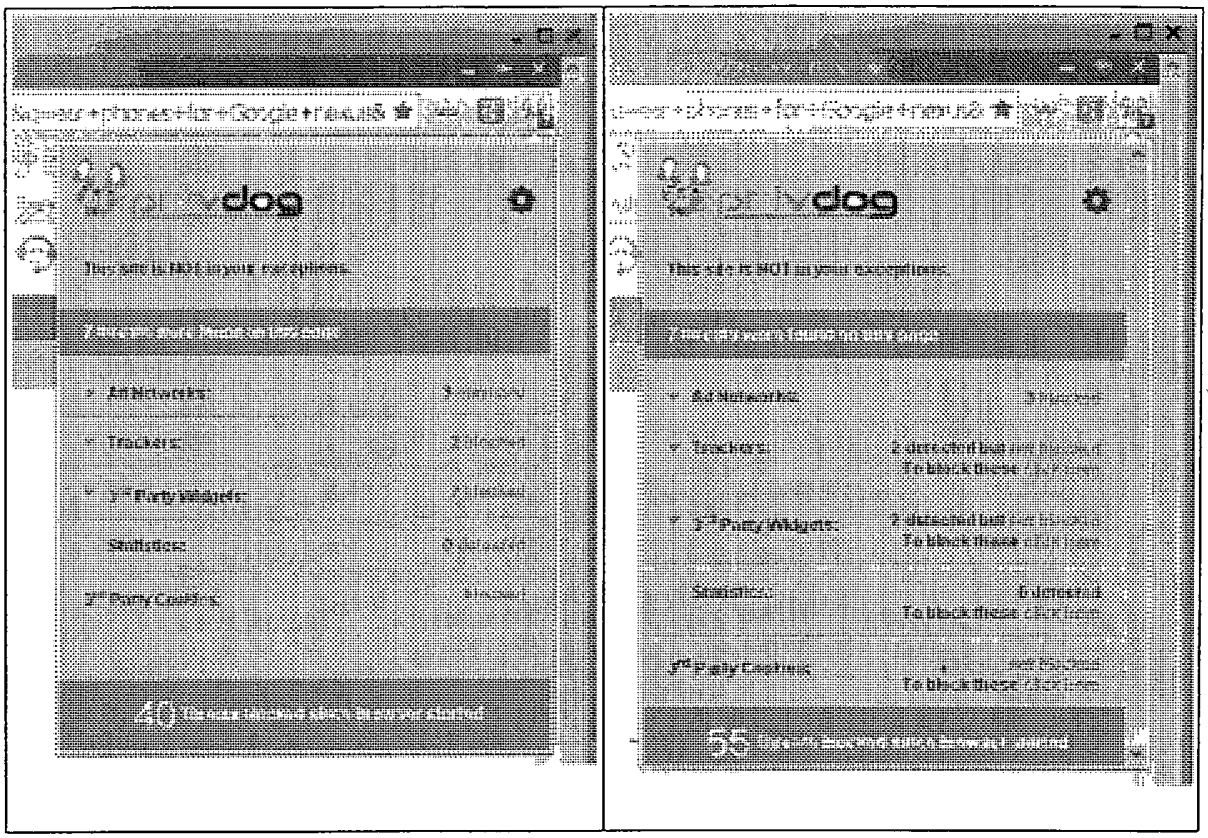
What would be your reaction if you knew that almost all your online activity was tracked by multiple agencies without your knowledge? The data they collect might be used for legitimate but unwelcome reasons such as adverts that follow you around the internet or for creating a profile of your online browsing 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.

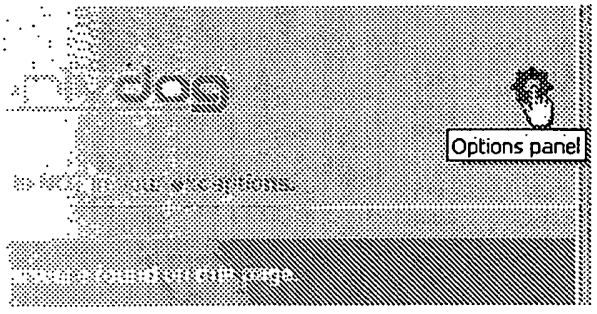
Statistics - Displays the number of analytical trackers that were blocked or allowed for that page depending on the settings configured. Clicking anywhere on the row will expand or collapse the list.

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

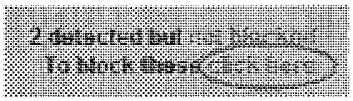
9.1.2. PrivDog Settings Configuration

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.

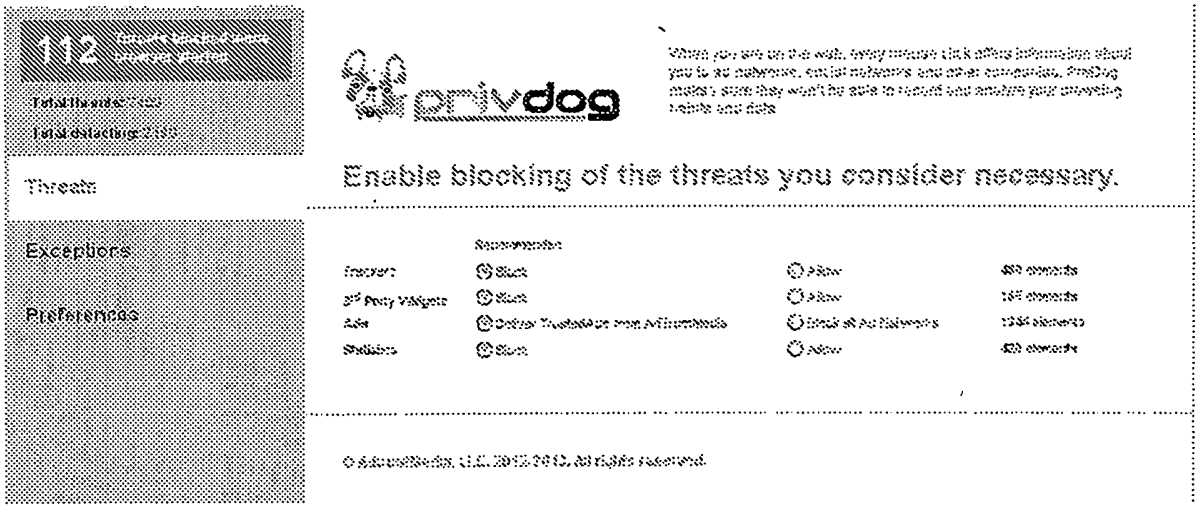


The panel allows you to configure the settings for:

- 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.

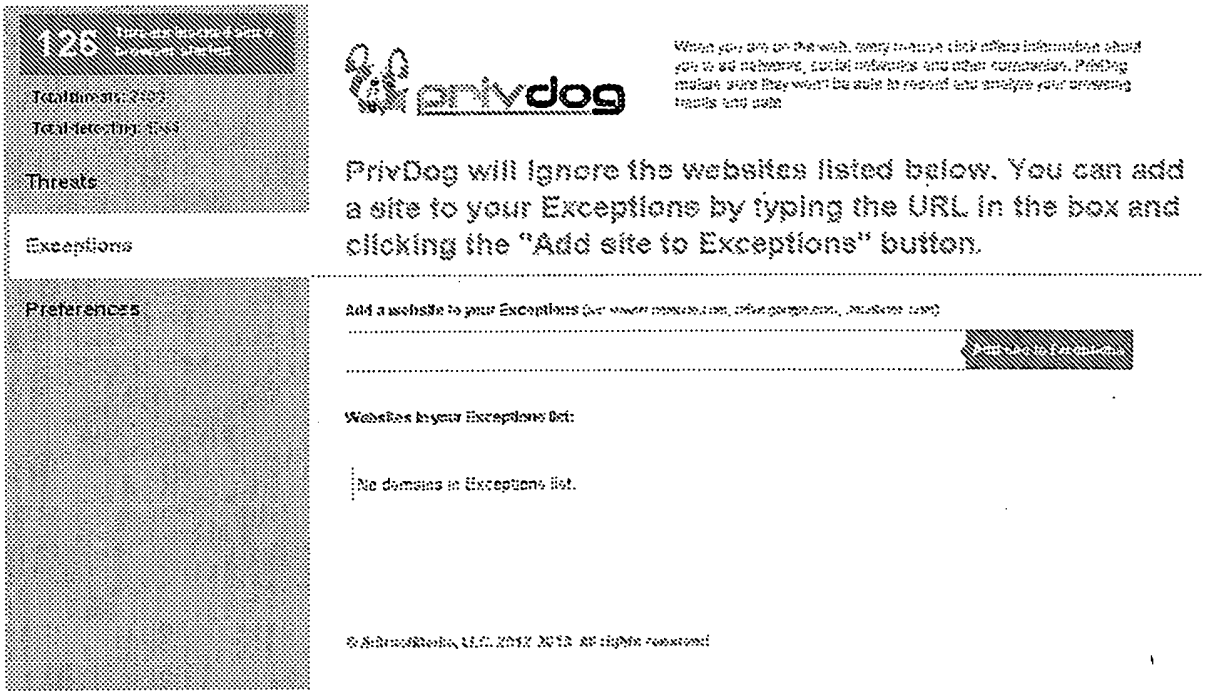


- Select the option whether to block or allow the items in the list.

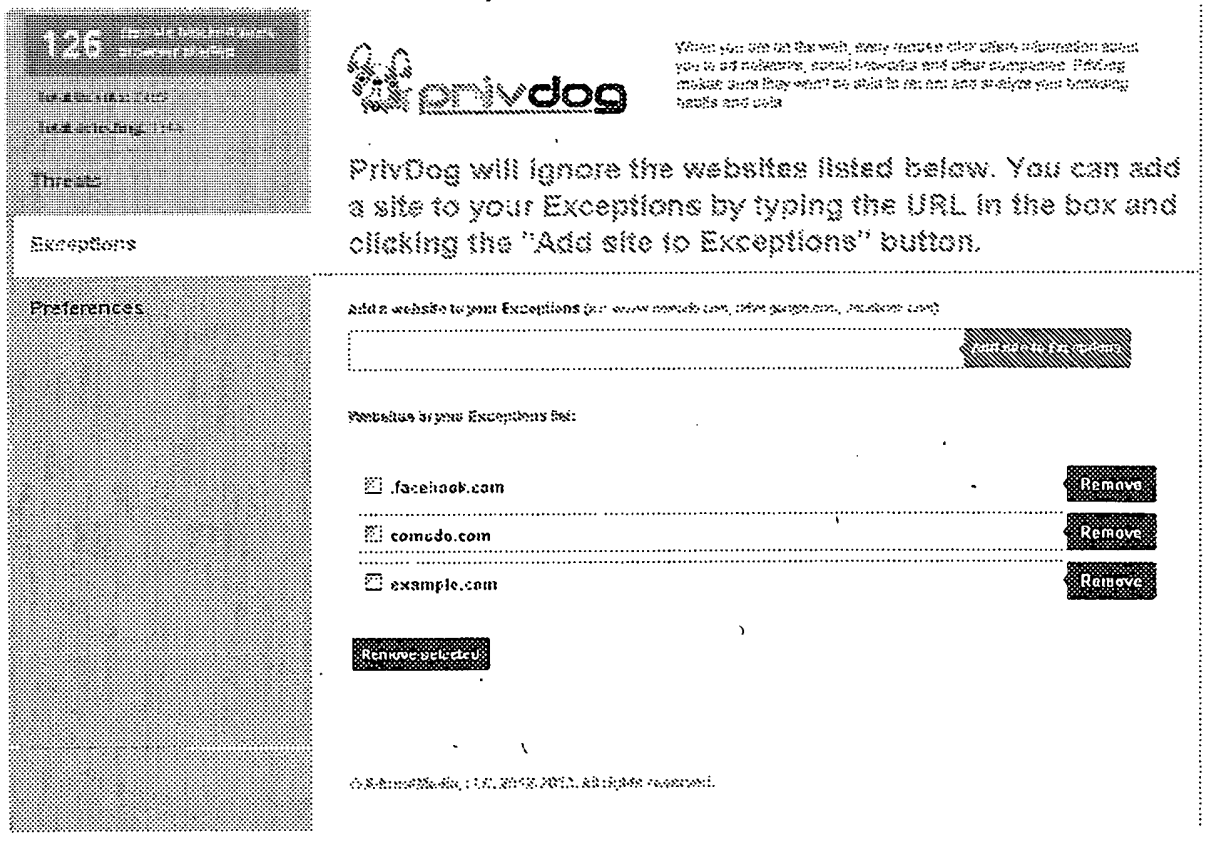
9.1.4. Exceptions

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.



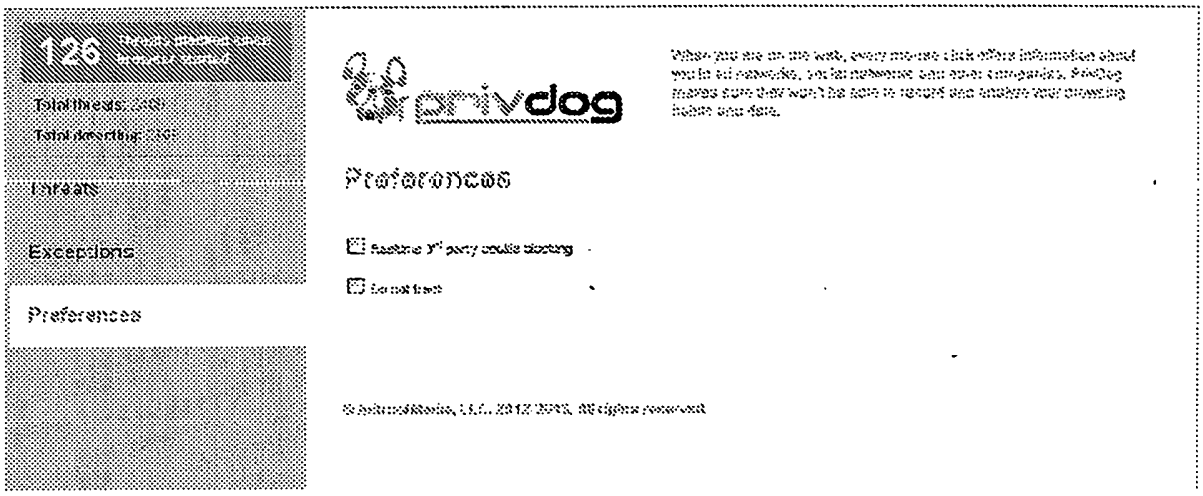
The added website(s) will displayed in the Exceptions list.



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-120-1-278-2524-Comodo-Dragon---Introduction.html for more details on using the browser.

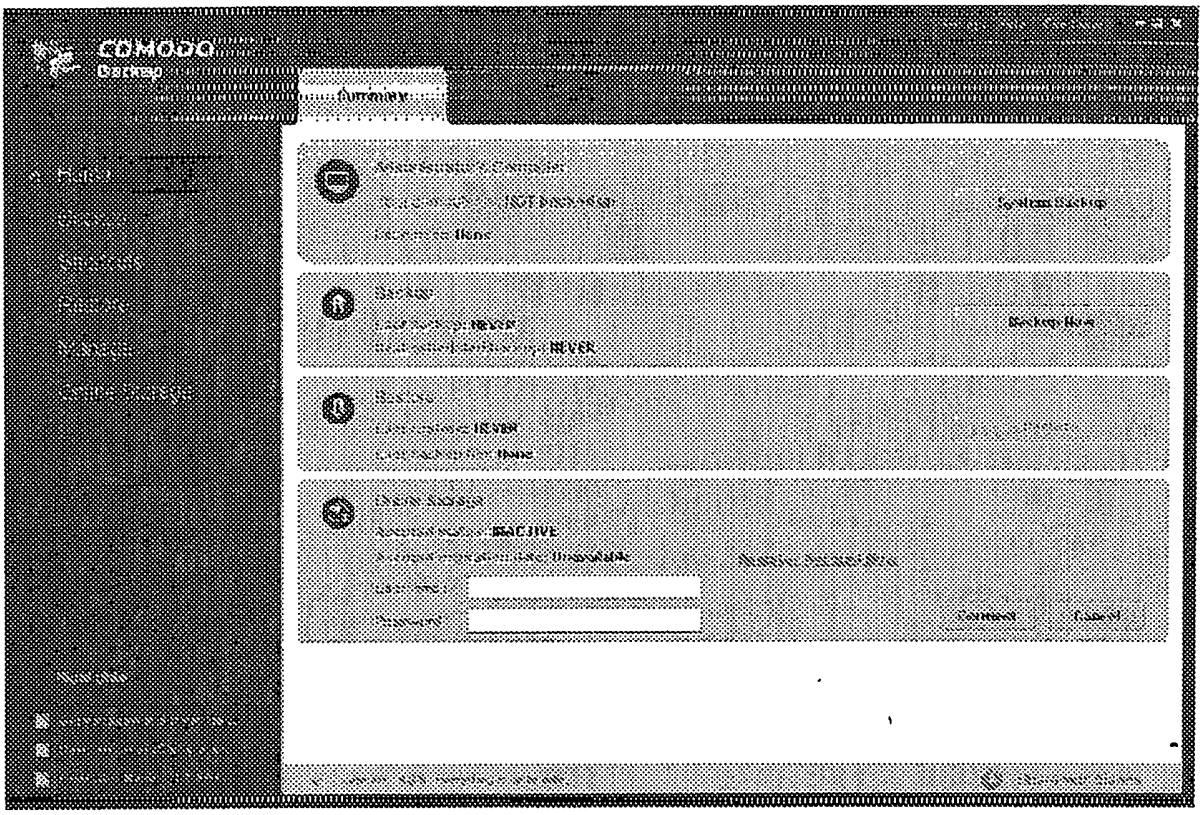
10. Comodo BackUp

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

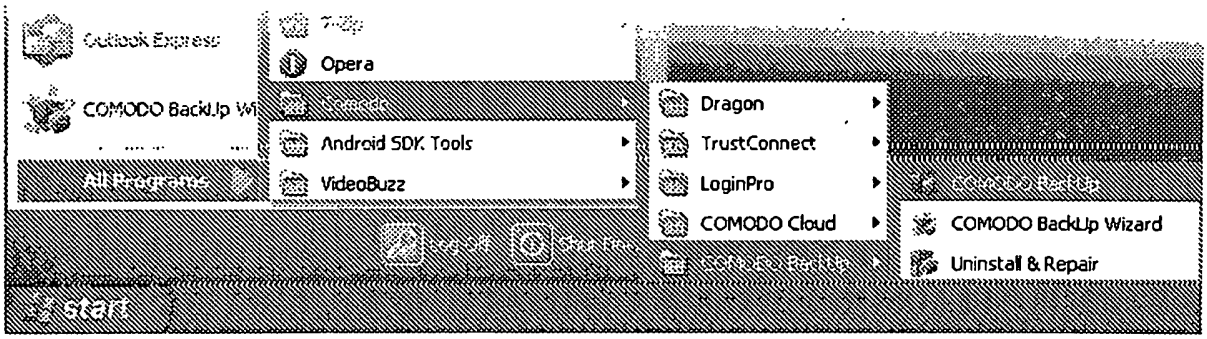
- **Quick backup** of entire drives or individual files or folders to your local computer, network drive, FTP server or Comodo's online server.
- **Step by step wizards** to guide even novice users through the entire backup, restore and scheduling procedures.
- **Flexible storage options** allow you 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-9-1-455-4810-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.

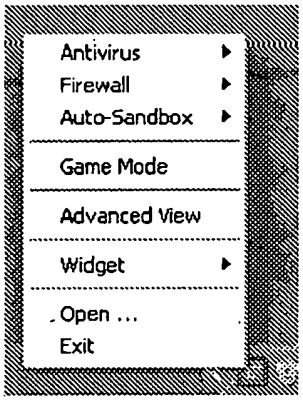
How to...:

- 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

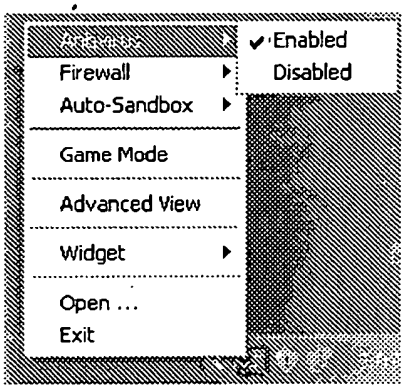
Comodo Internet Security allows users to quickly switch the Enabled/Disabled states of Antivirus, Firewall and Auto-Sandbox by right clicking on the system tray icon (the CIS interface should be in Compact View).



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'



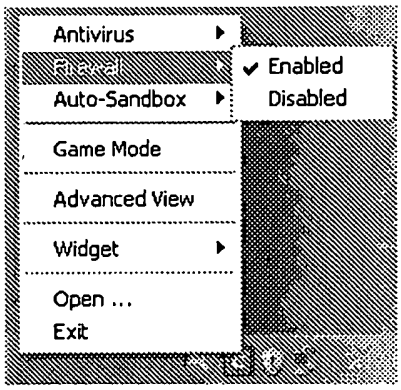
3. Choose 'Enabled or Disabled' as per your choice

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'



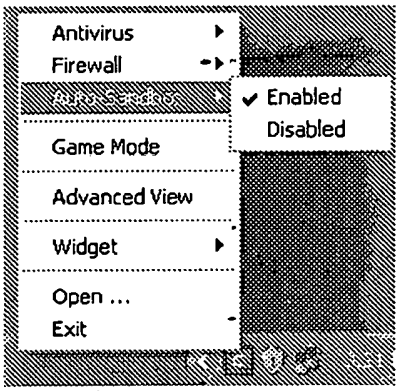
3. Choose 'Enabled or Disabled' as per your choice

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.

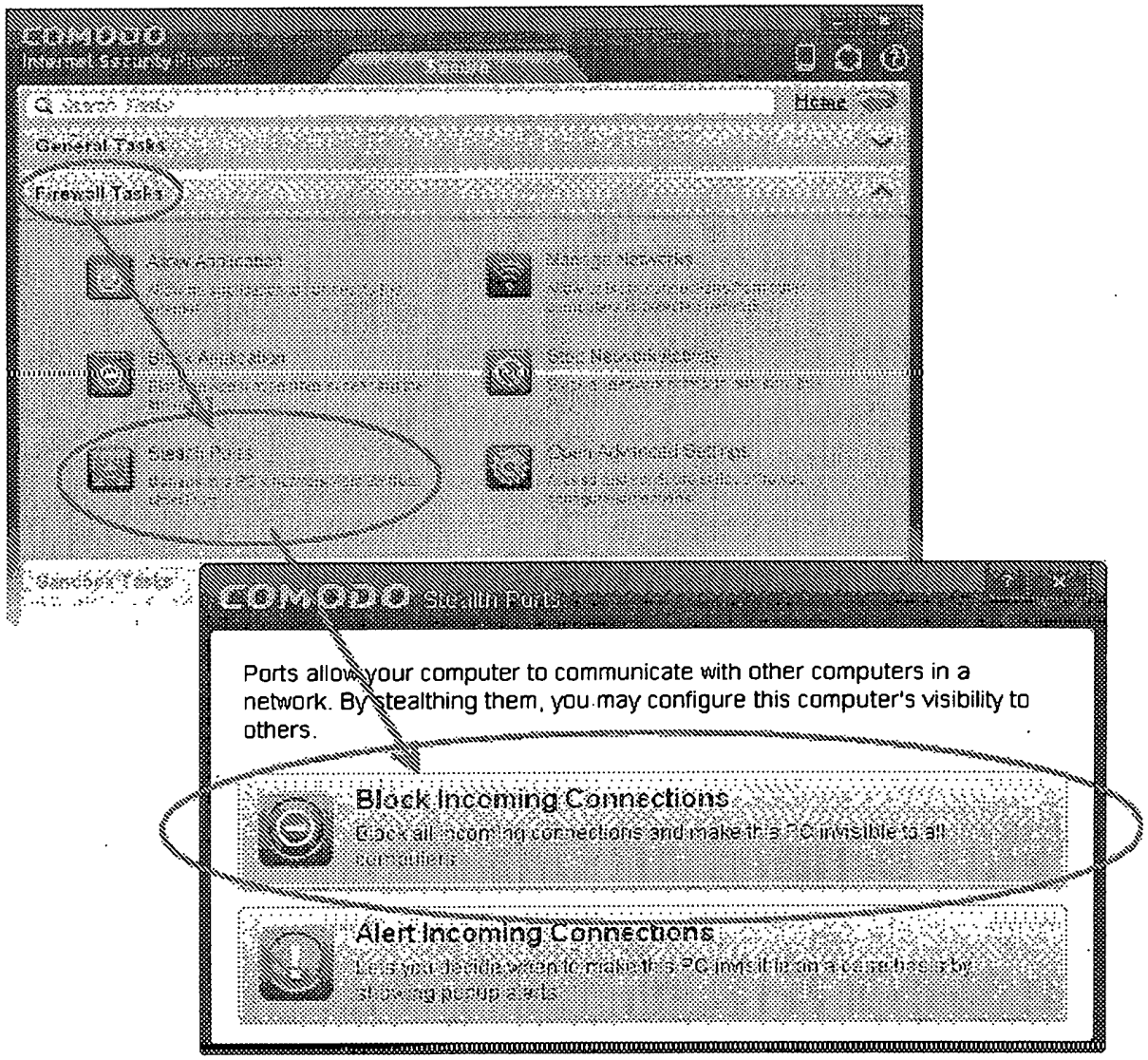
Set up the Firewall For Maximum Security and Usability

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

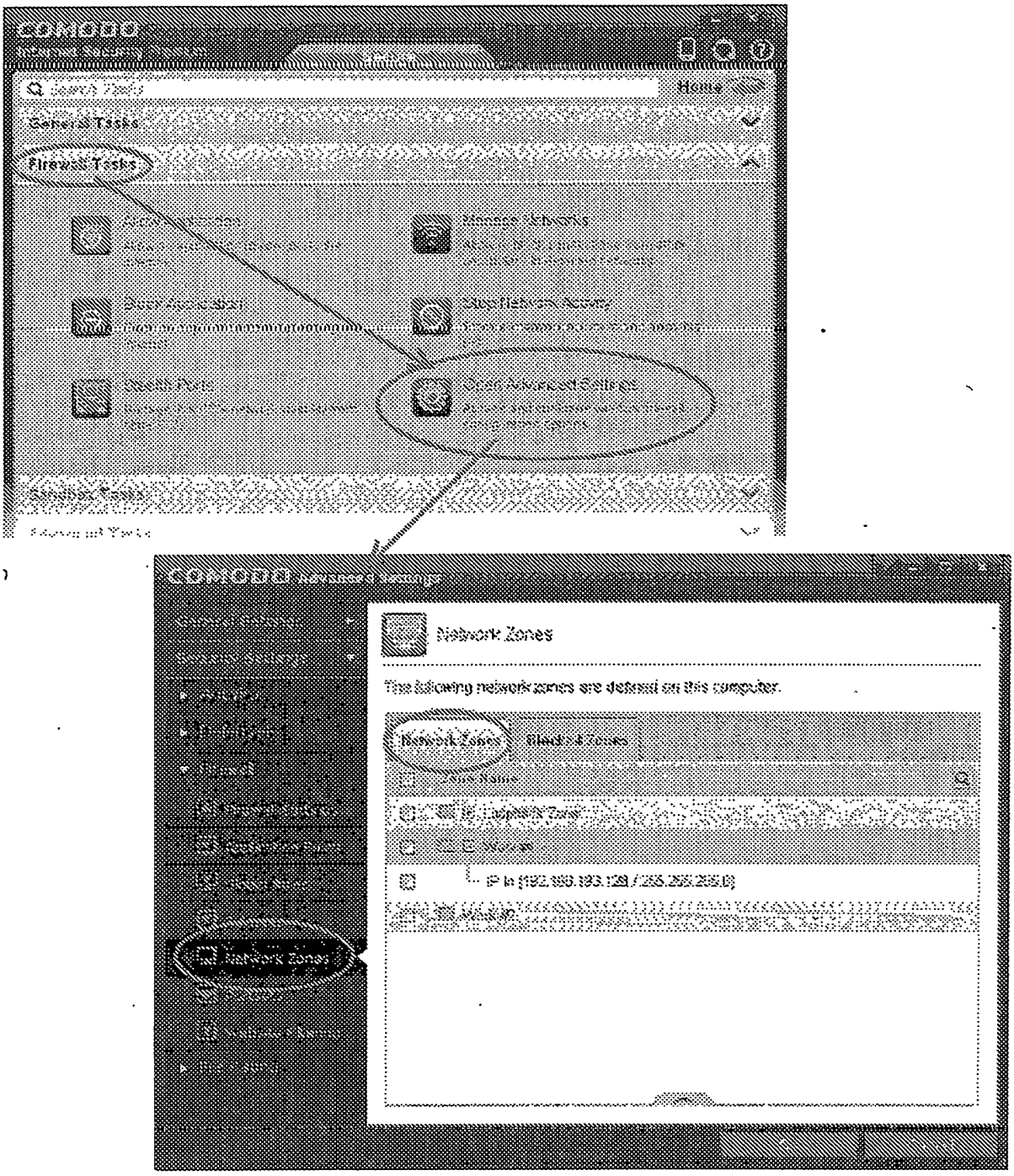
Click here for more details on Stealthing your Computer Ports

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 *127.0.0.1/255.0.0.0*

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

5. Check these addressees and click 'OK'.

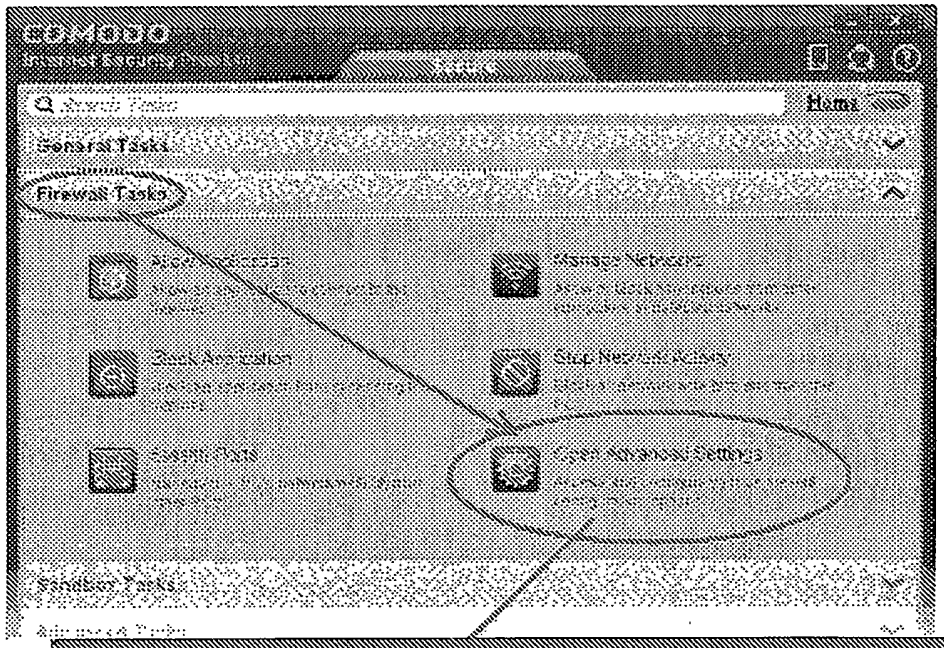
Click here for more details on Network Zones settings

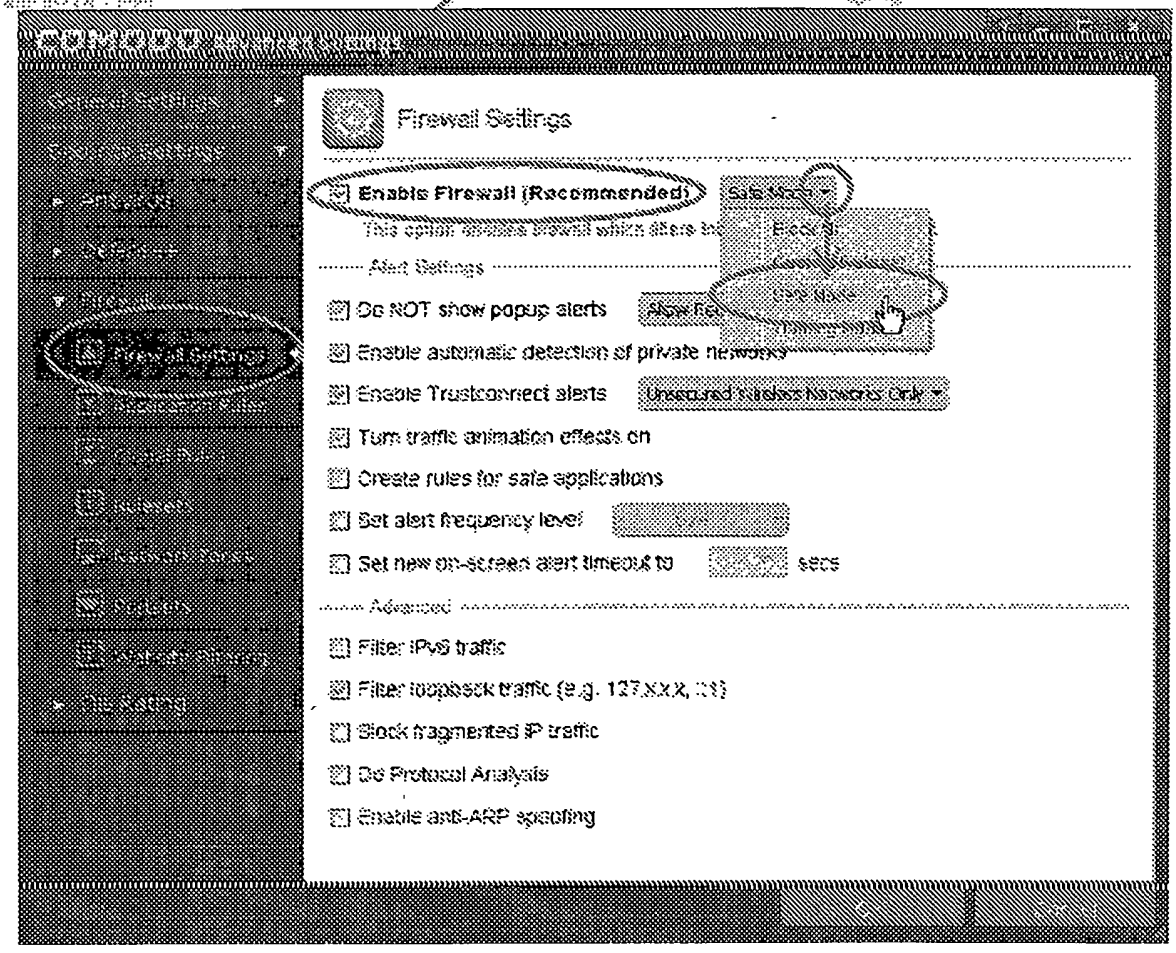
Firewall Behavior Settings

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

To open Firewall Behavior Settings panel

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



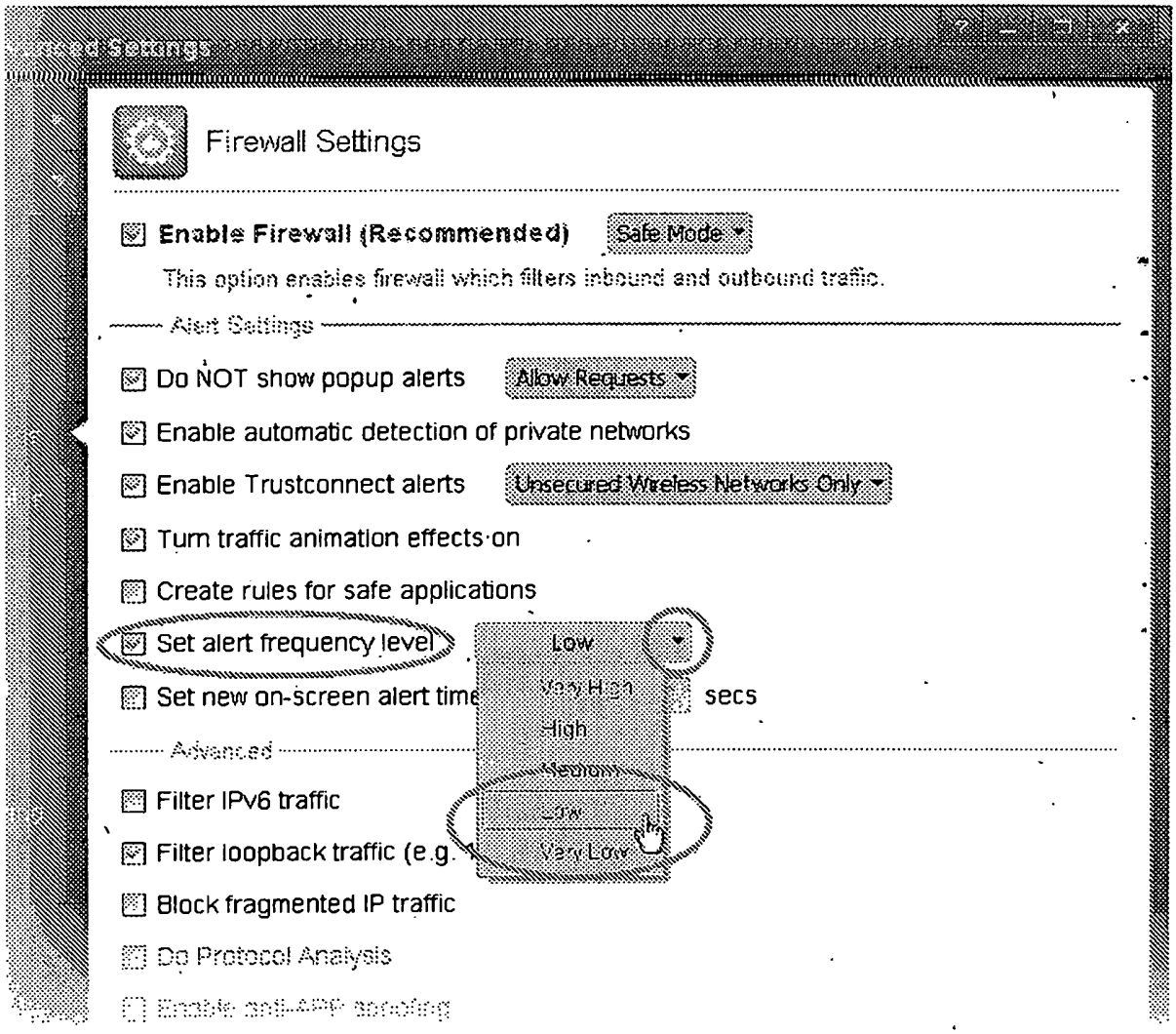


Safe Mode: While filtering network traffic, the firewall will automatically create rules that allow all traffic for the components of applications certified as 'Safe' by Comodo. For non-certified new applications, you will receive an alert whenever that application attempts to access the network. Should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

Alert Settings

Under 'Alert Settings' in the same interface:

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



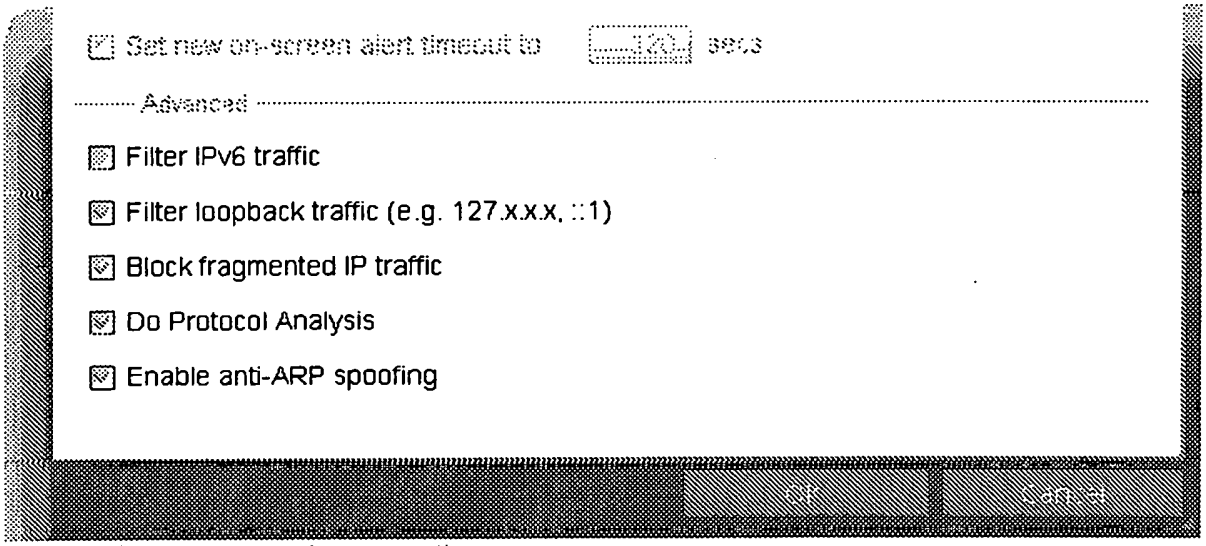
Advanced Settings

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

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

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

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



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

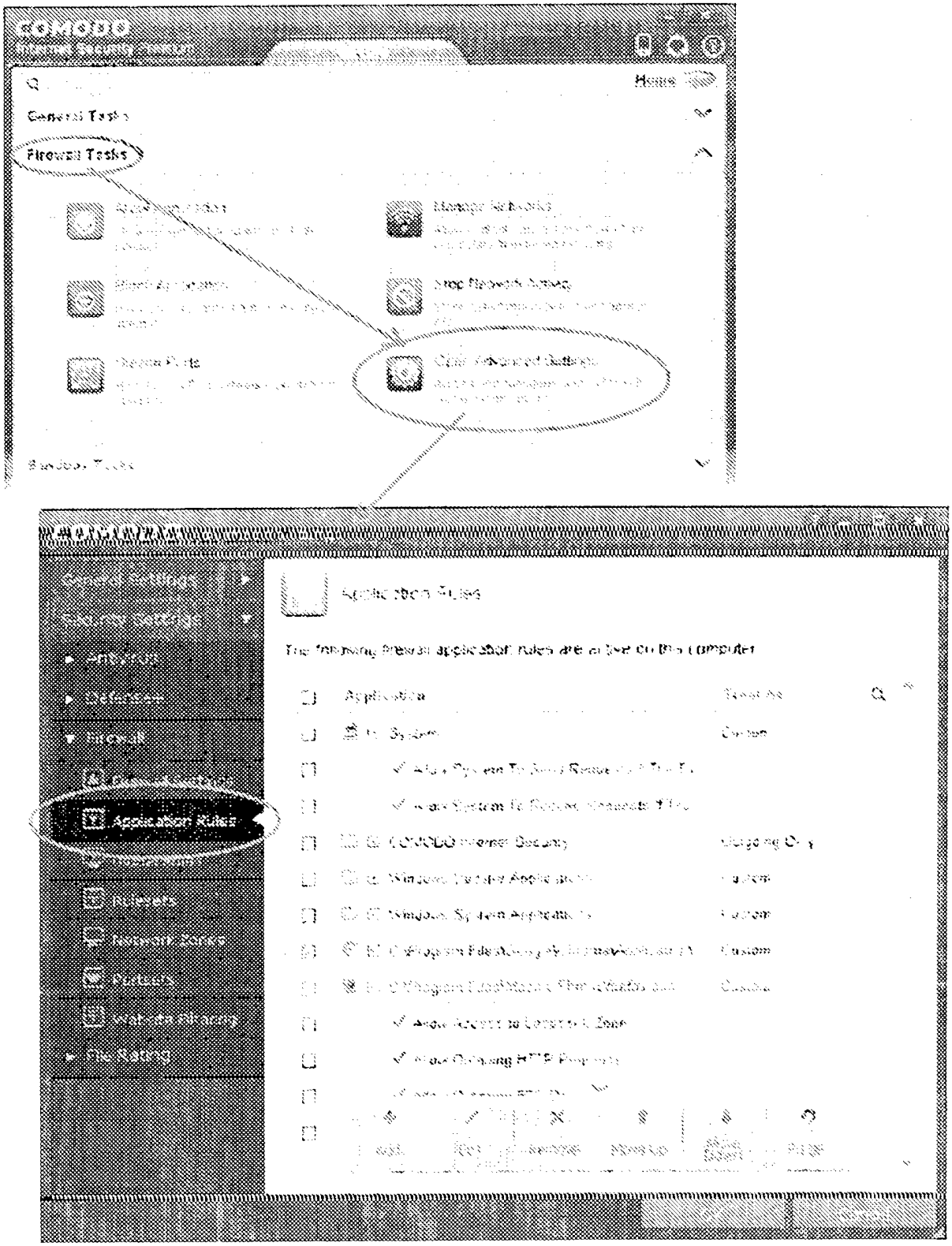
Click here for more details on Firewall Behavior Settings

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

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

To view the Application Rules

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



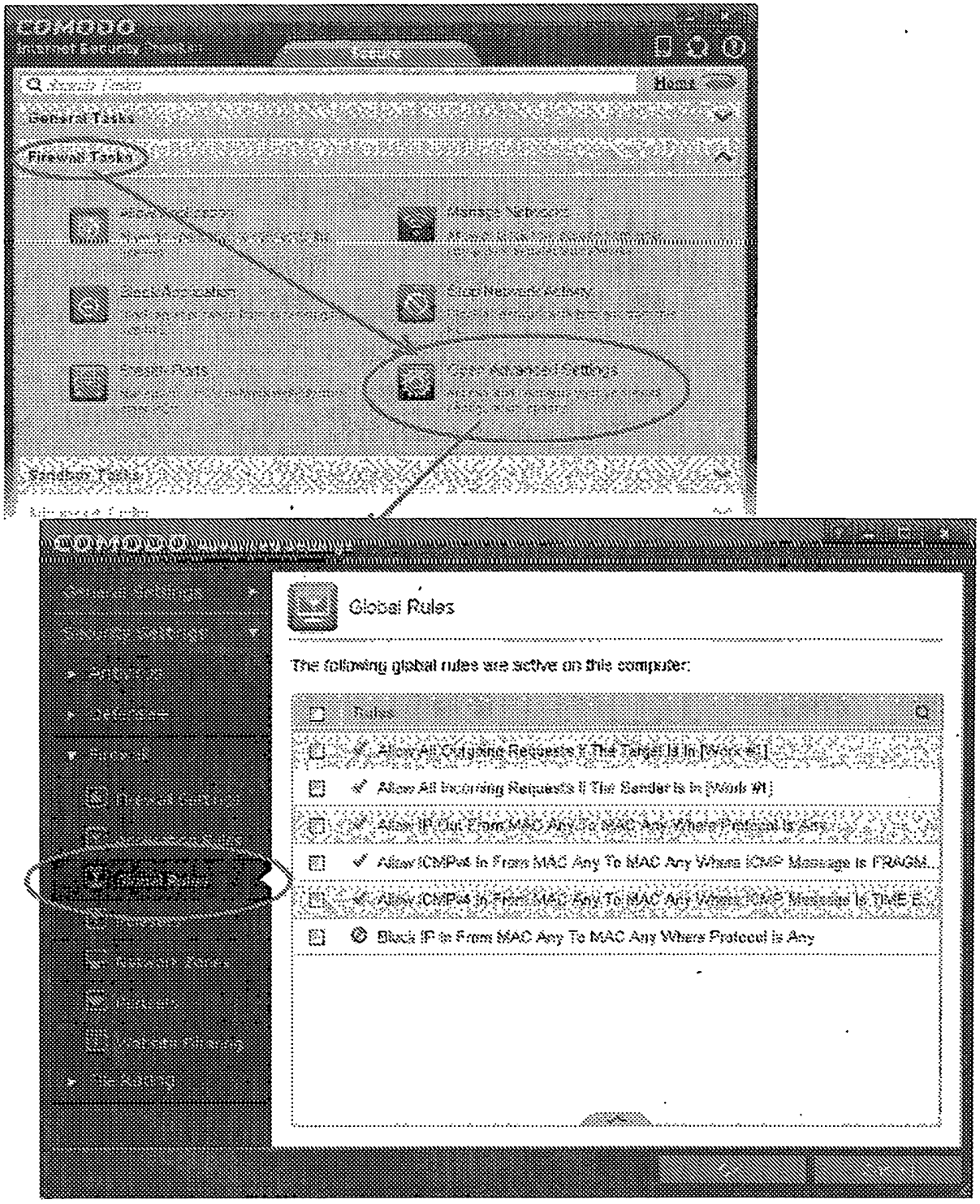
4 Click the handle from the bottom and Add or Edit rules for specific applications manually or remove them.

Click here for more details on Application Rules

To view the Global Rules

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

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



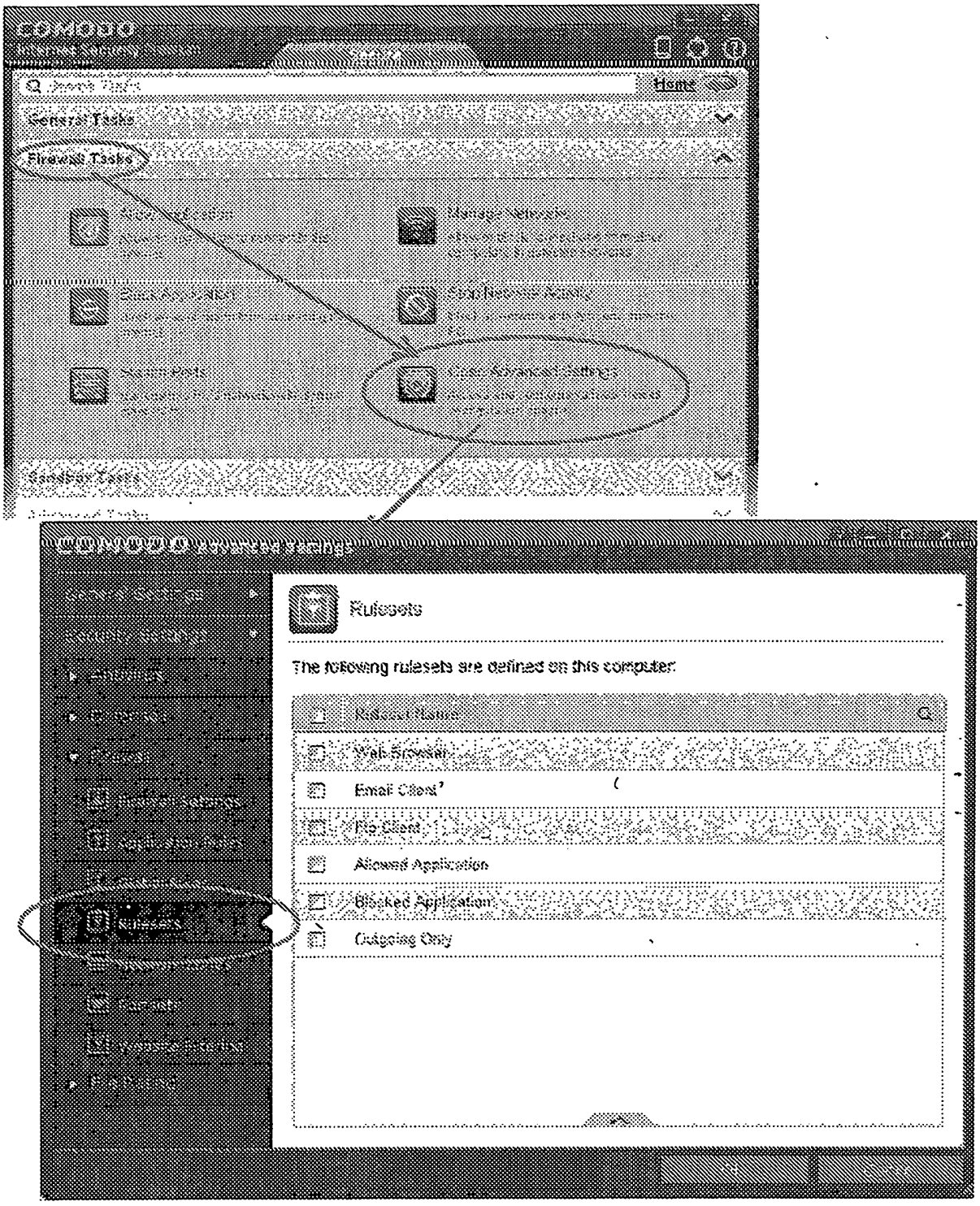
4. Click the handle from the bottom and Add or Edit global rules manually or remove them.

Click here for more details on Global Rules

To view Predefined Firewall rulesets

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

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



4. Click the handle from the bottom to 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).

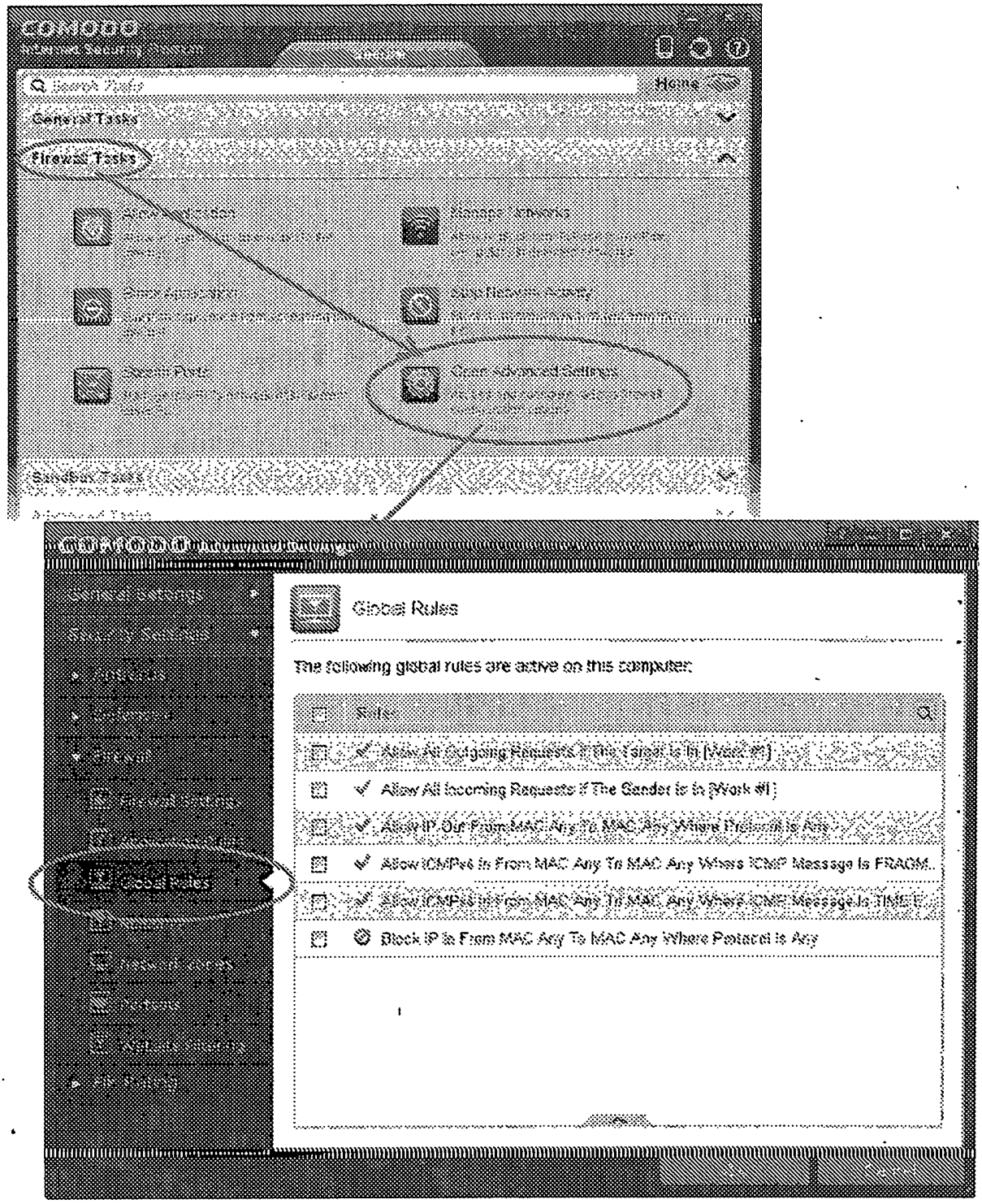
Example scenarios:

- 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

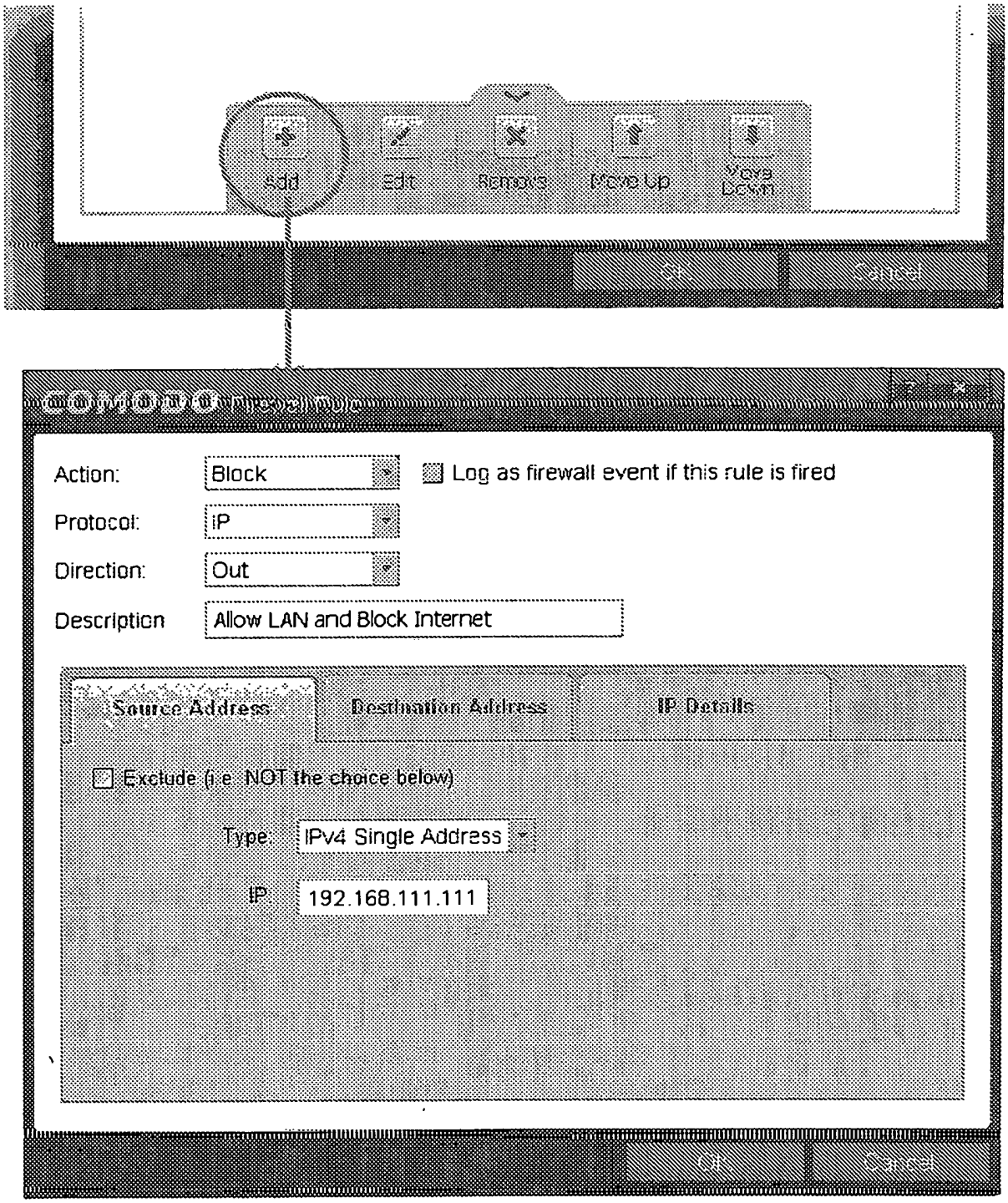
To selectively block connection to internet whilst allow connection to internal network you need to create a Global Rule under Advanced Firewall Settings and password protect your configuration to prevent others from altering it.

To create a Global Rule

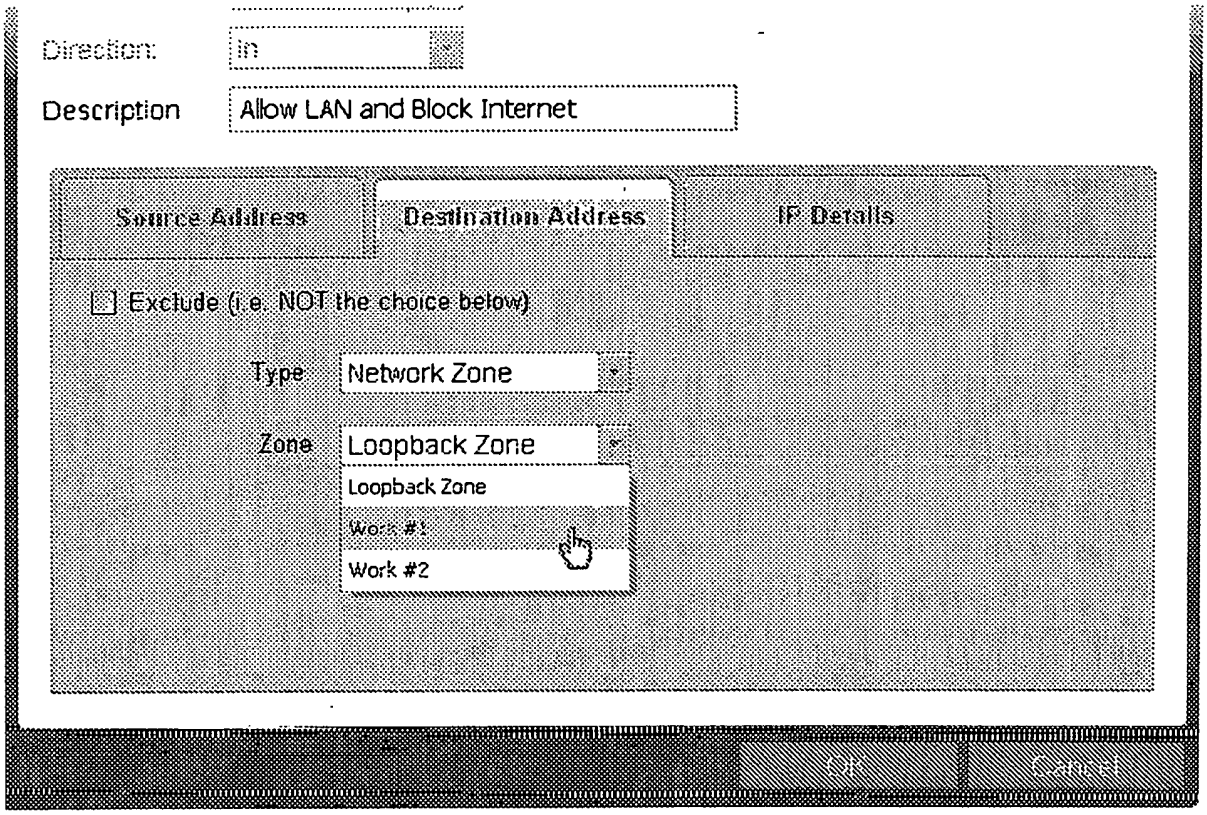
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Global Rules' under Firewall from the left hand side pane



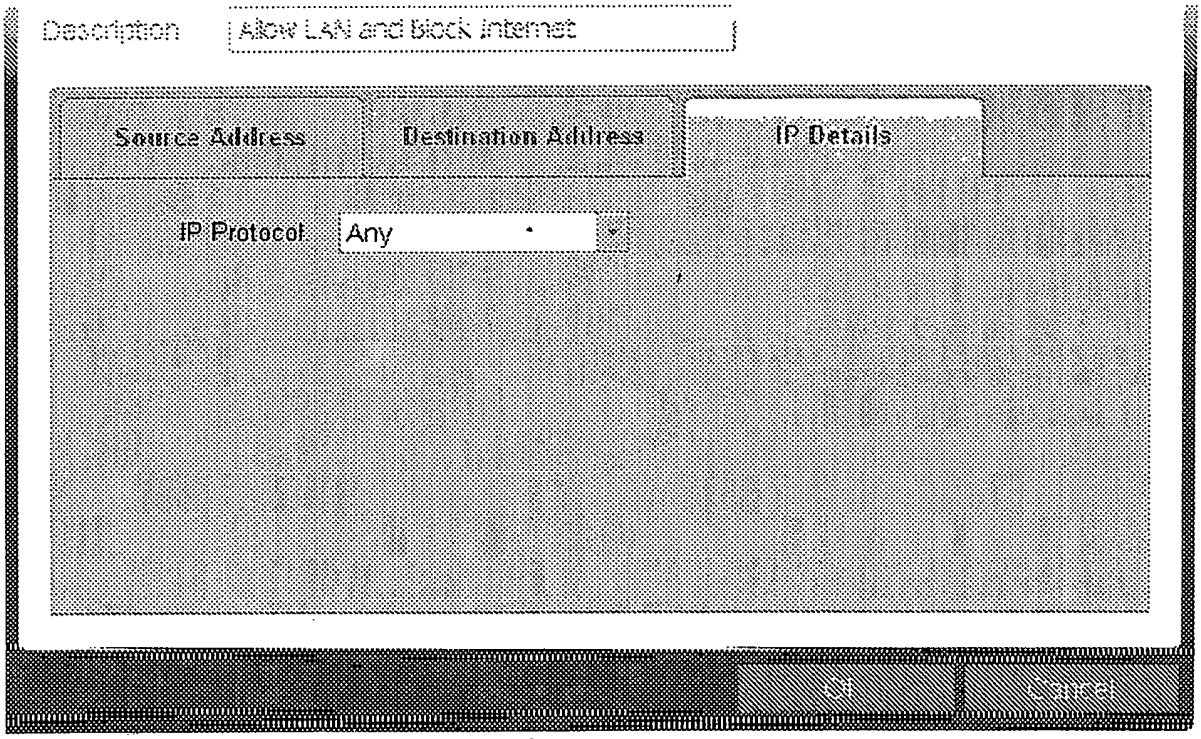
4. Click the handle from the bottom and choose 'Add' from the options. The Firewall Rule interface will open.



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.

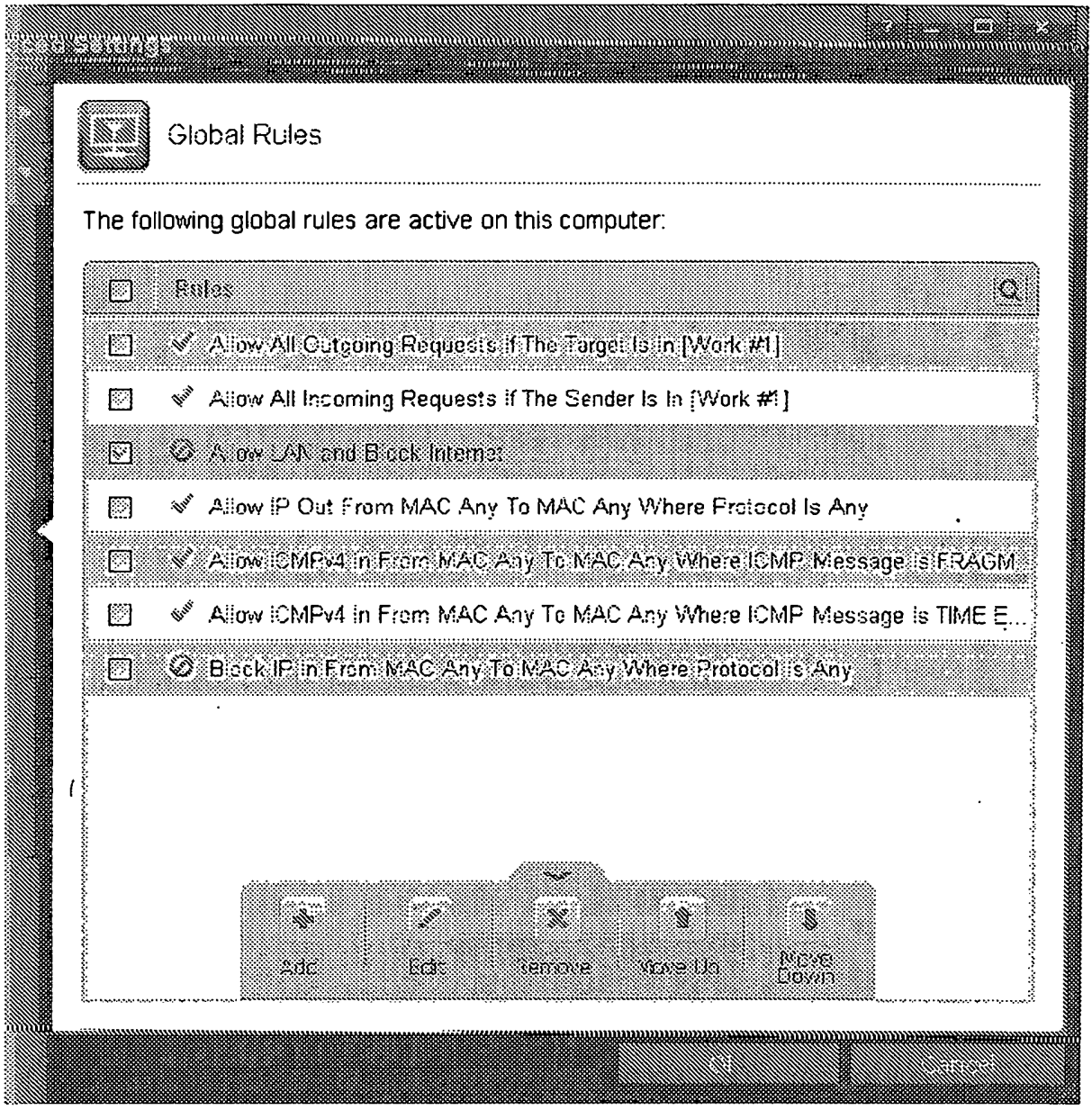


9. Click the 'IP Details' tab and choose 'Any' from the 'IP Protocol' drop-down.



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.

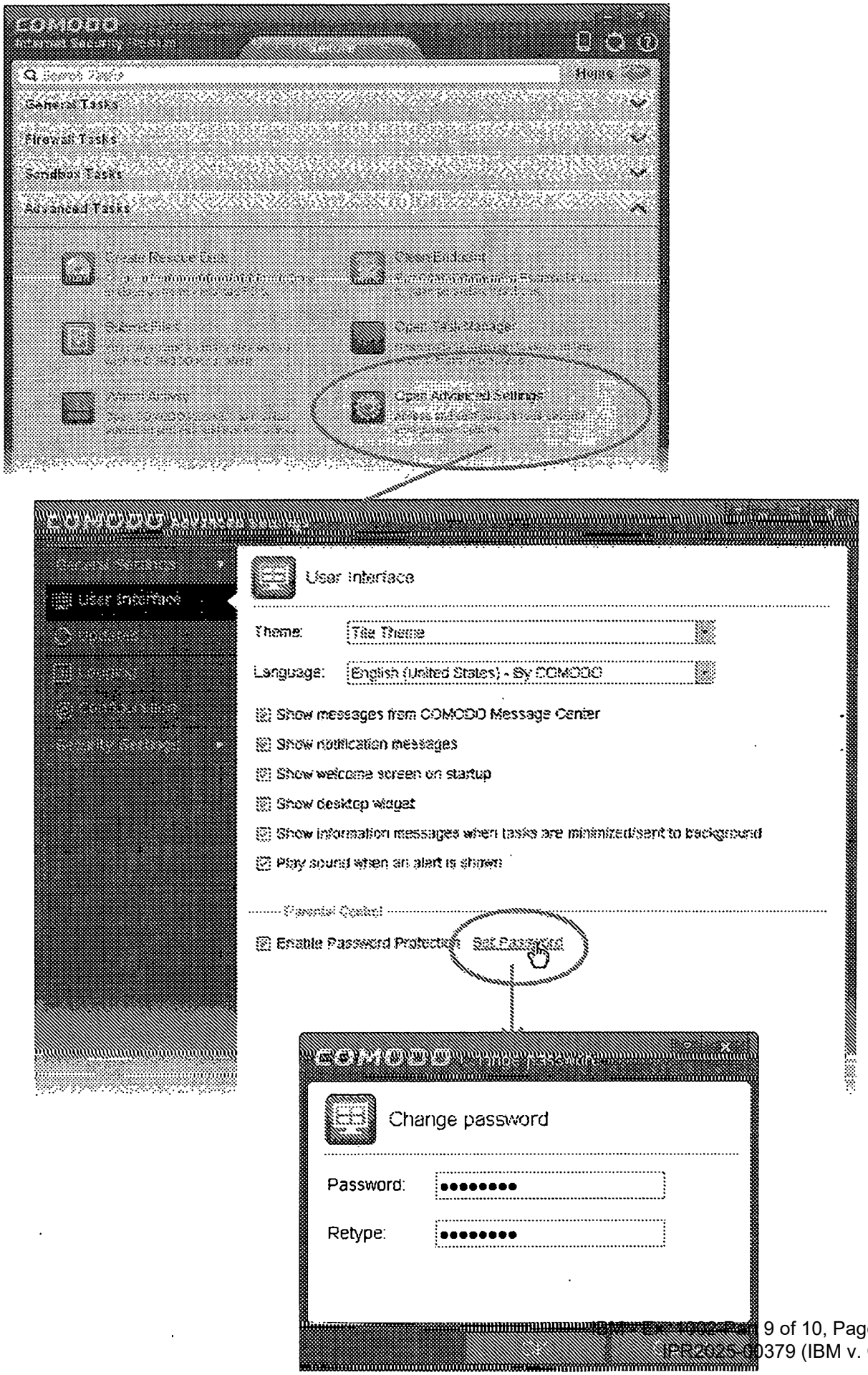


12. Click 'OK' for your configuration to take effect.

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.

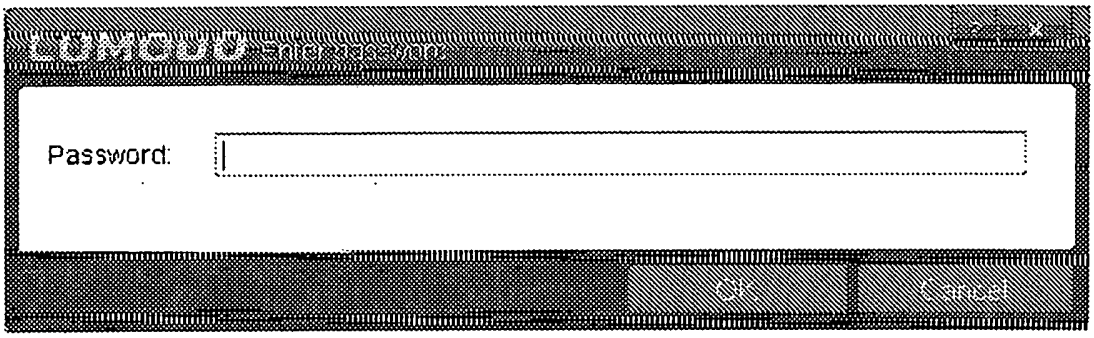
To password protect your configuration

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


Home
General Tasks
Firewall Tasks
Sandbox Tasks
Advanced Tasks
Open Advanced Settings
User Interface
Theme:
Language:
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
Change password
Password:
Retype:

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.



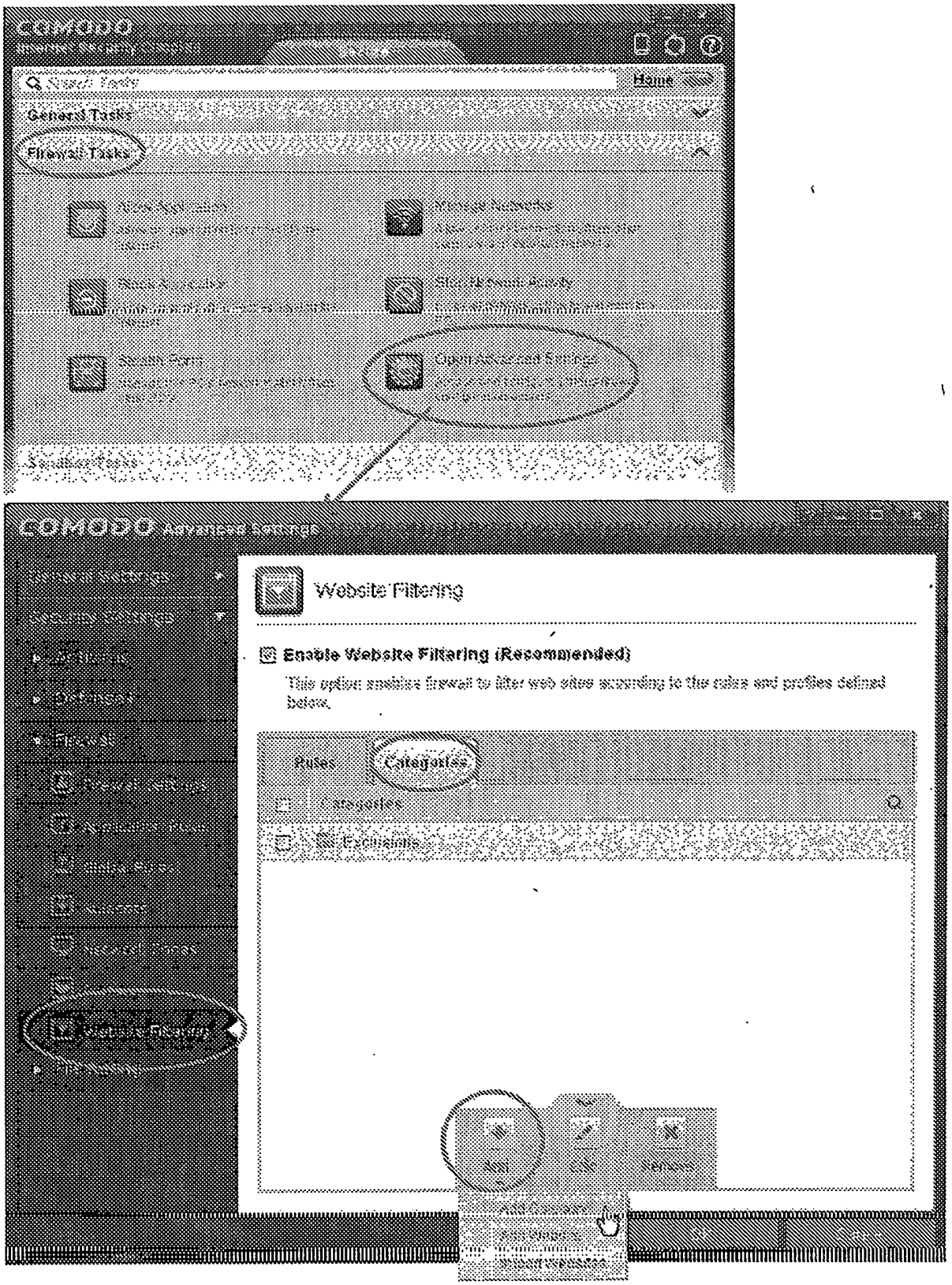
Block/allow Websites Selectively to Users of Your Computer

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:

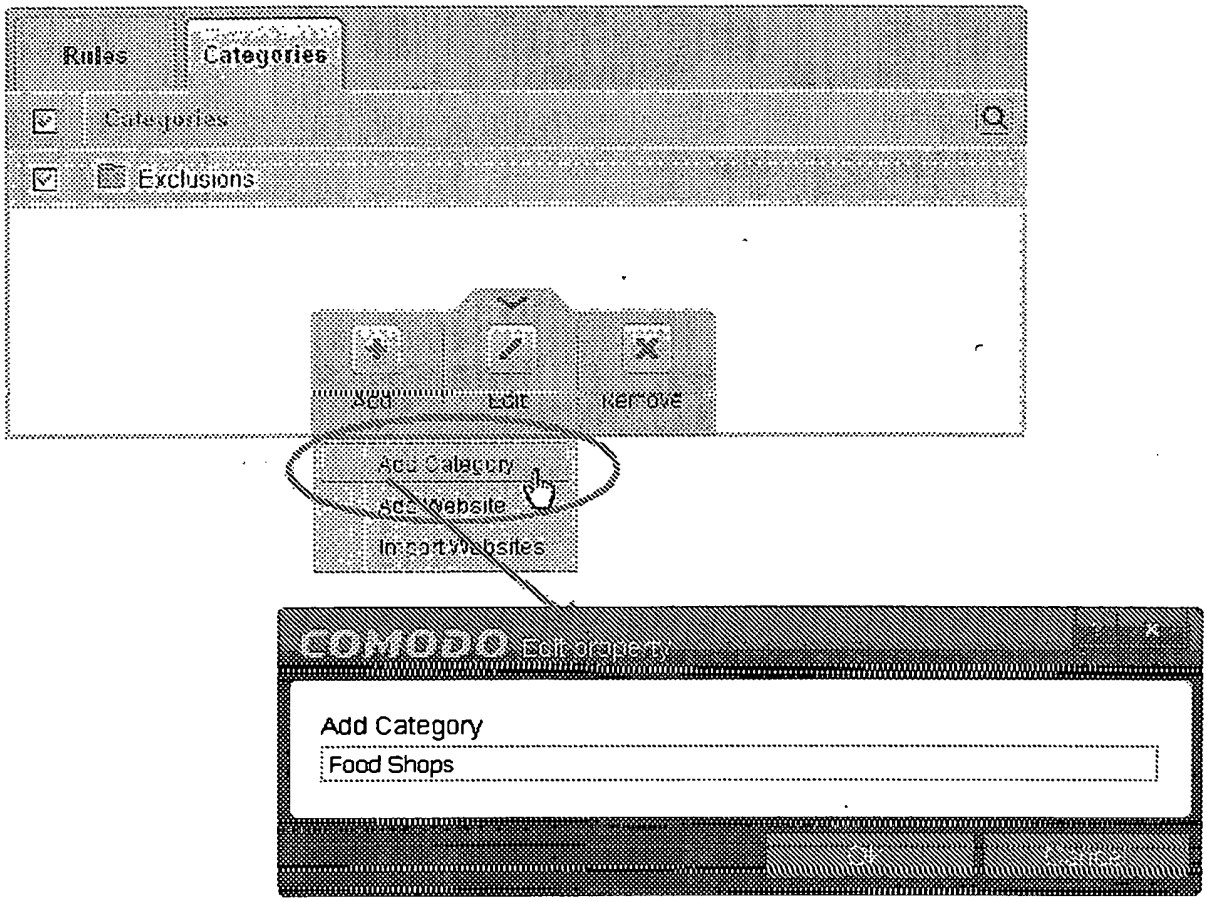
- Define Website Categories and add websites
- Create Firewall rules for allowing or blocking website categories to selected users

To define website categories

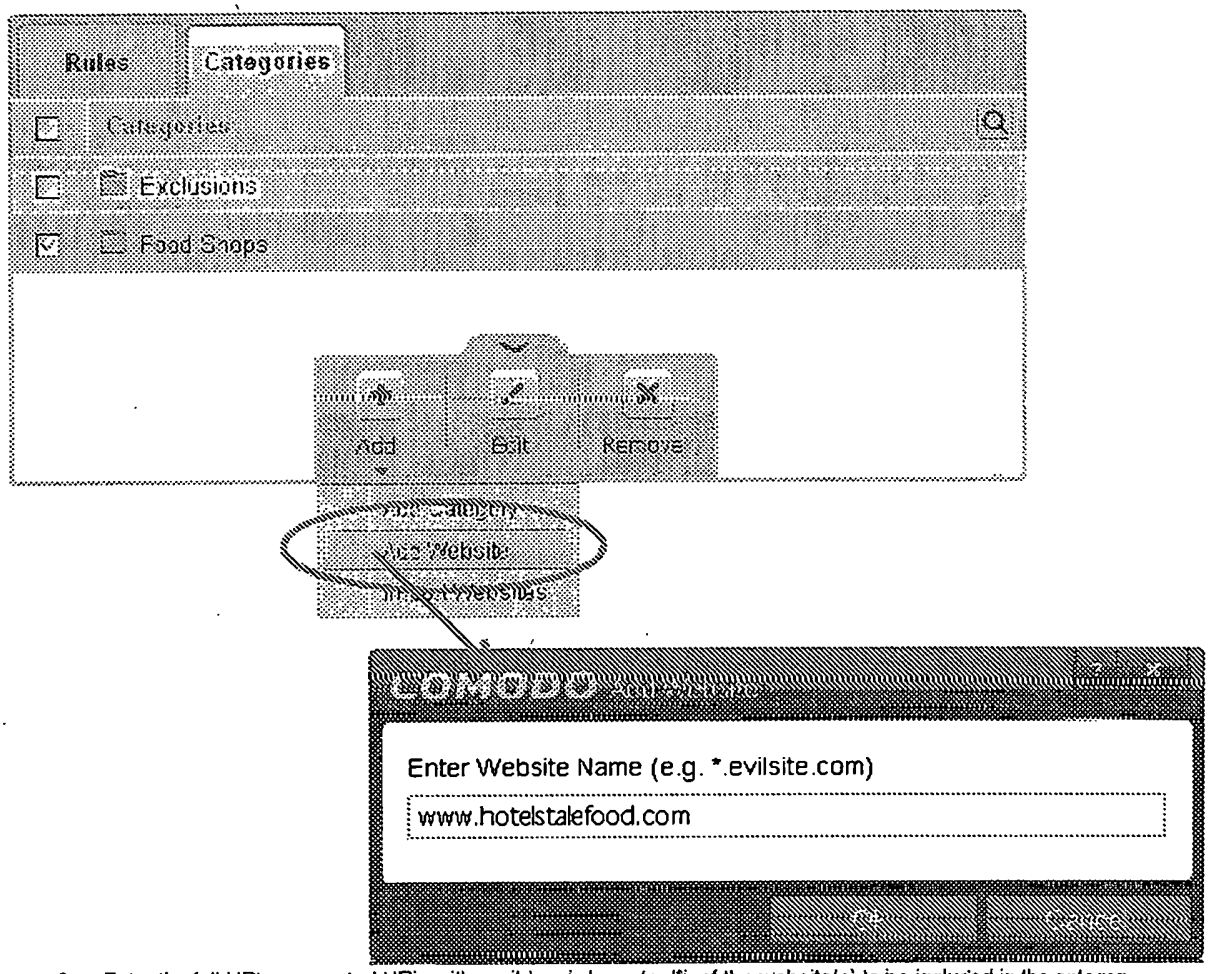
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen.
2. Open 'Firewall Tasks' by clicking 'Firewall Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Website Filtering' under Firewall from the left hand side pane.
4. Ensure that the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



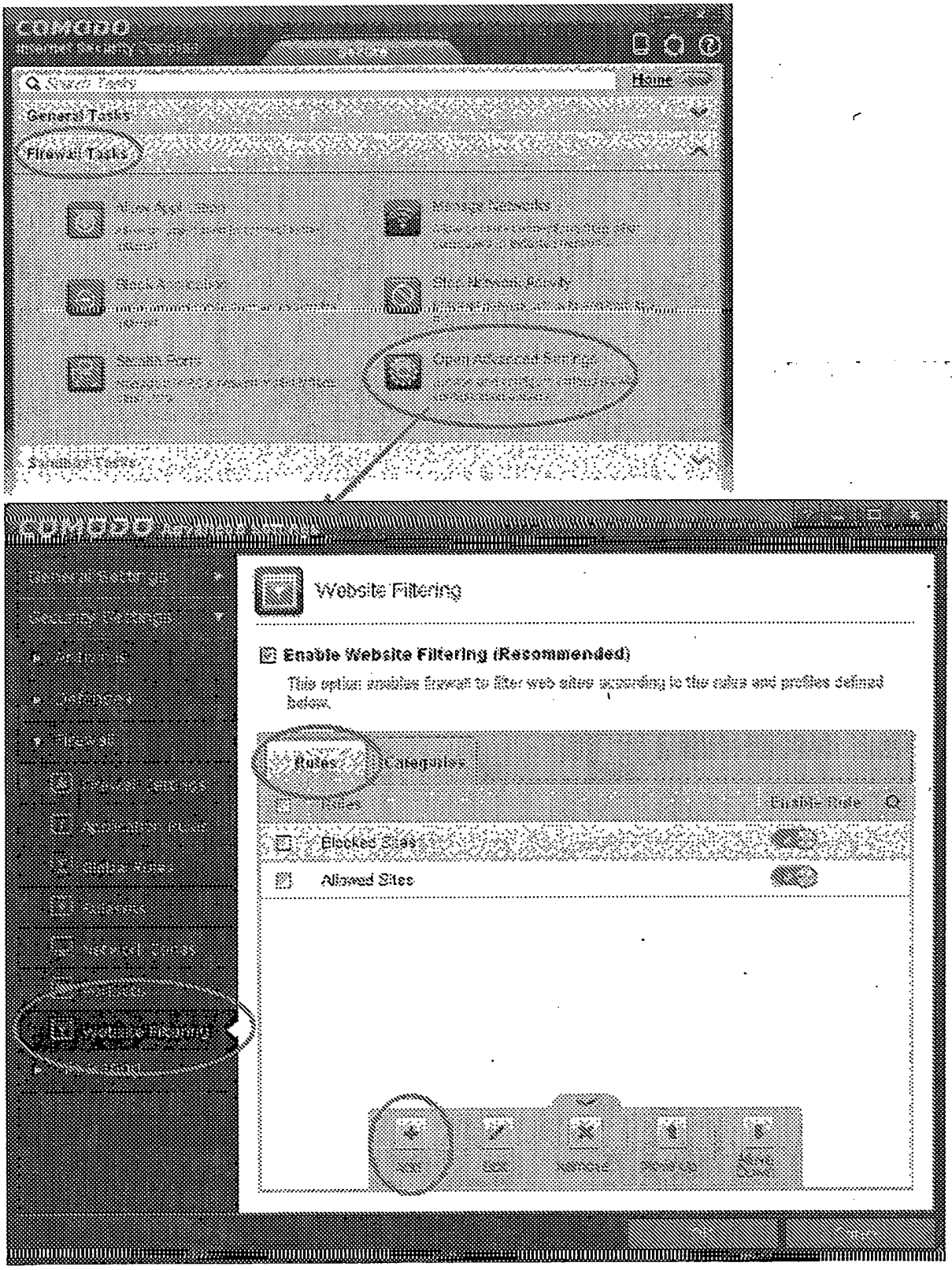
9. Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.
    - To add a specific website/webpage, enter the full URL of the website/webpage
    - To include all sub-domains of website, add a wildcard character and a period in front of the 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.

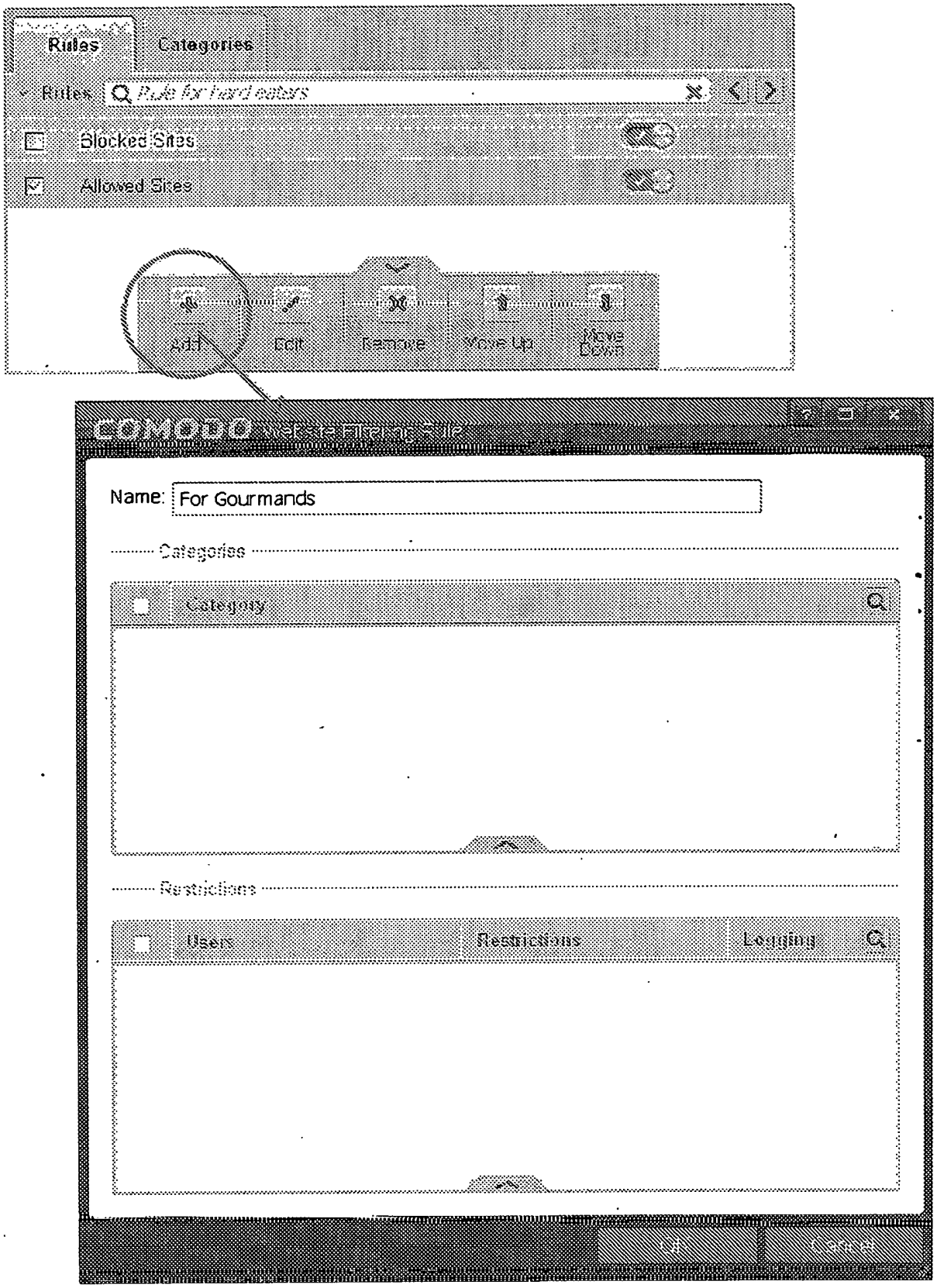
10. Repeat the process to add more websites.
11. Click OK in the 'Advanced Settings' interface to save your settings

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':

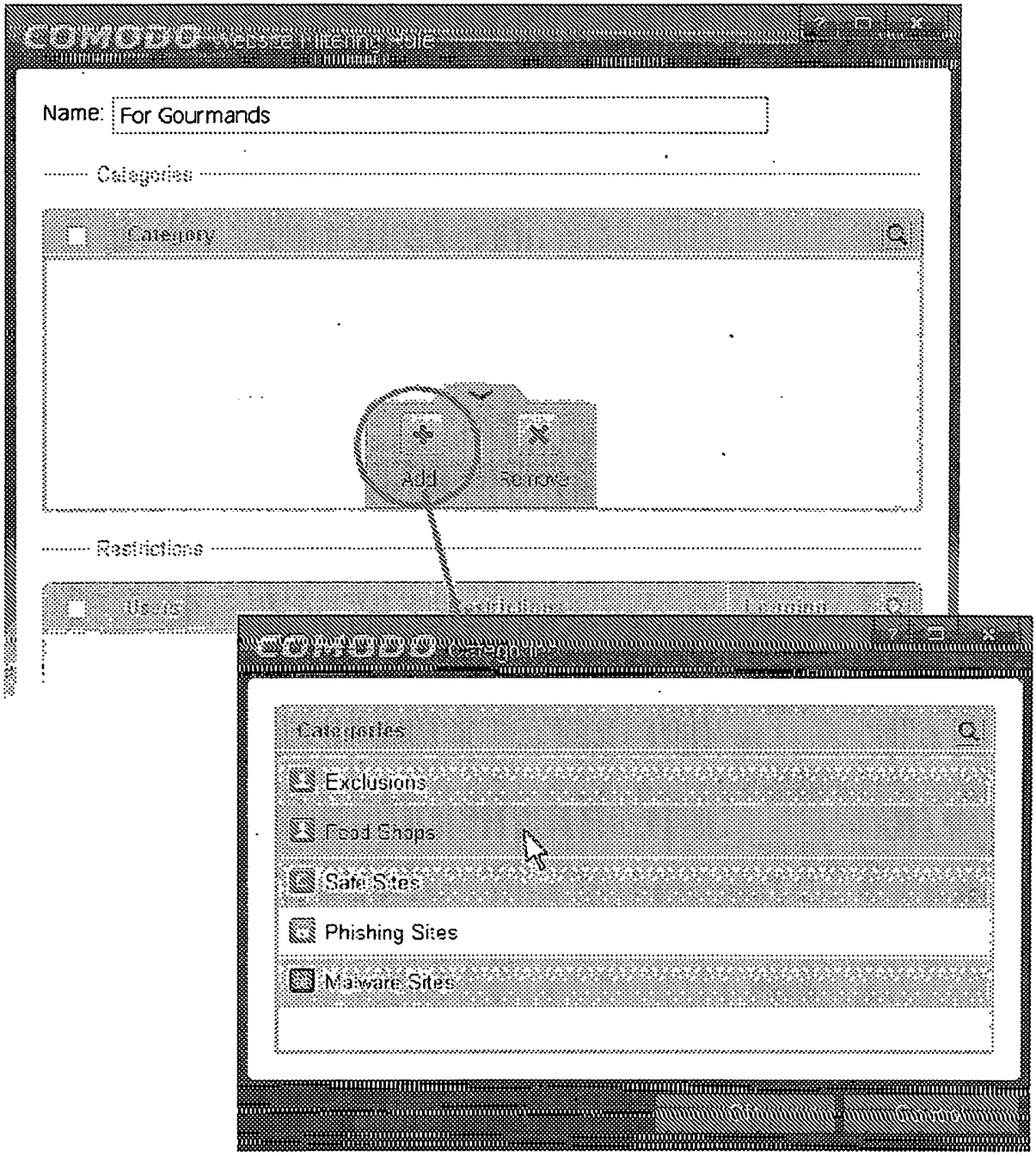


5. Enter a name for your new filter in the 'Website Filtering Rule' dialog.



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.

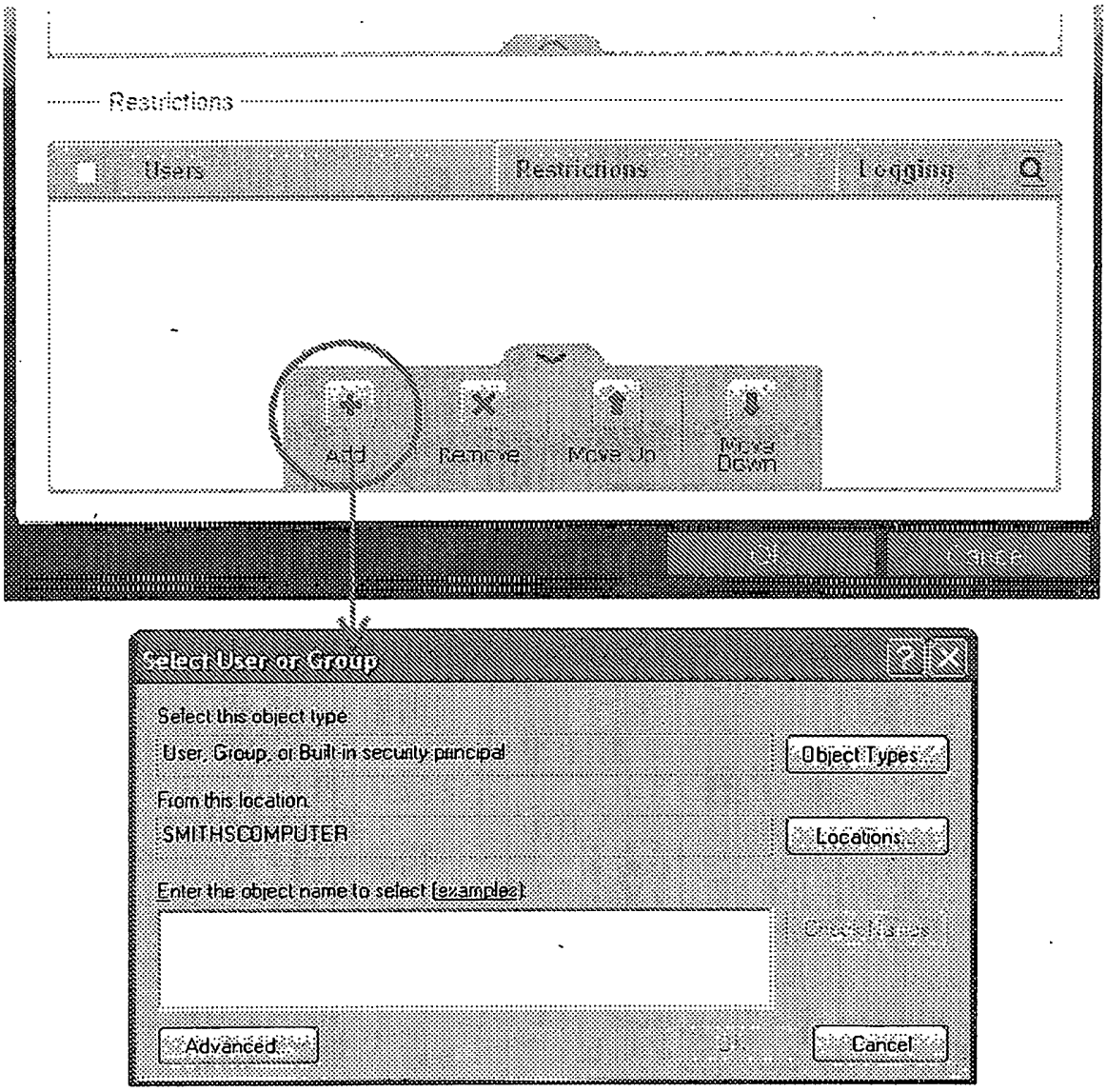
The 'categories' window contains a list pre-defined Comodo categories and any user created categories. Comodo categories cannot be modified.

- **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

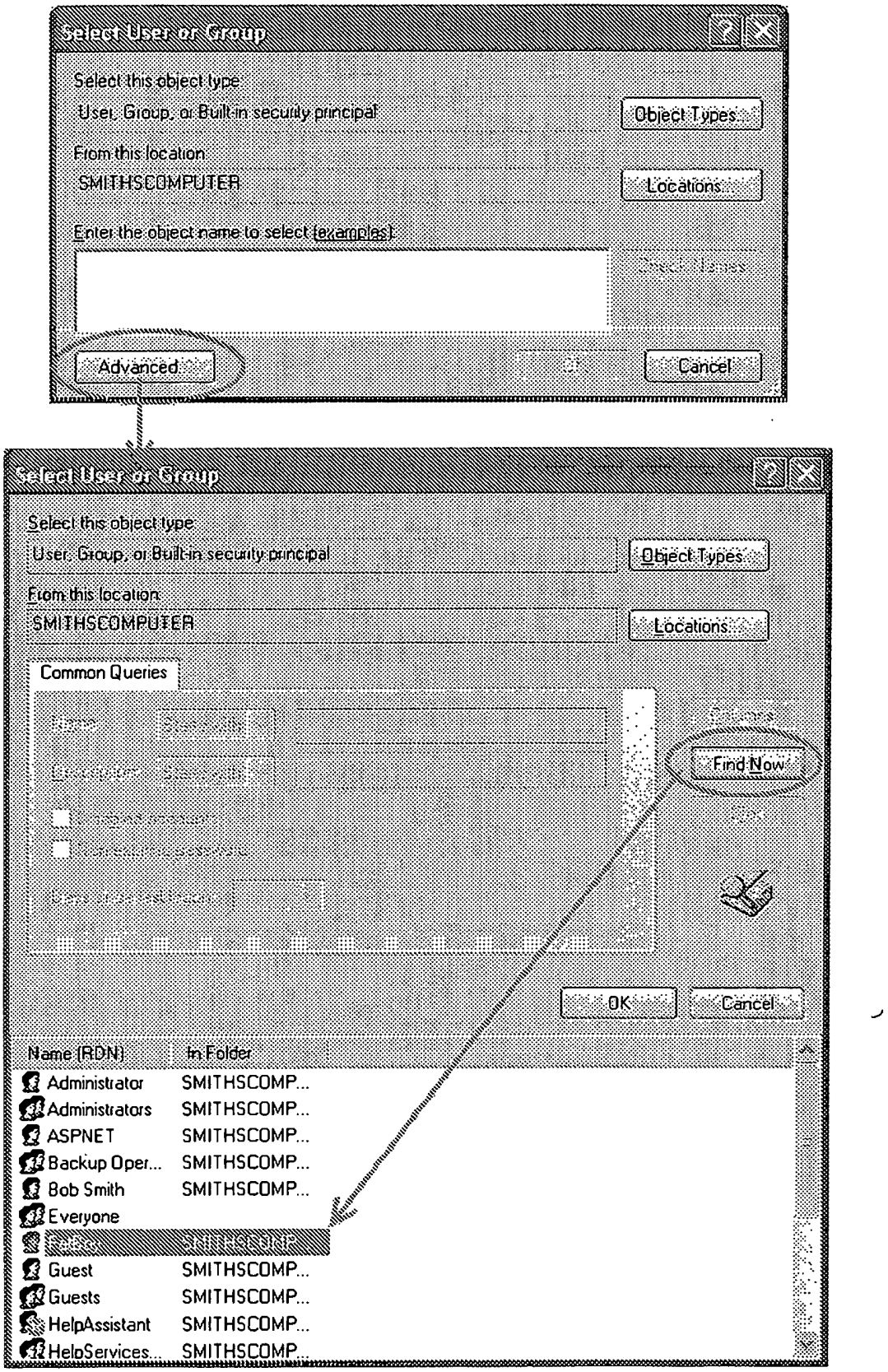
For more details on creating and modifying user specified categories, Refer to the section Defining or Modifying Website Categories

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

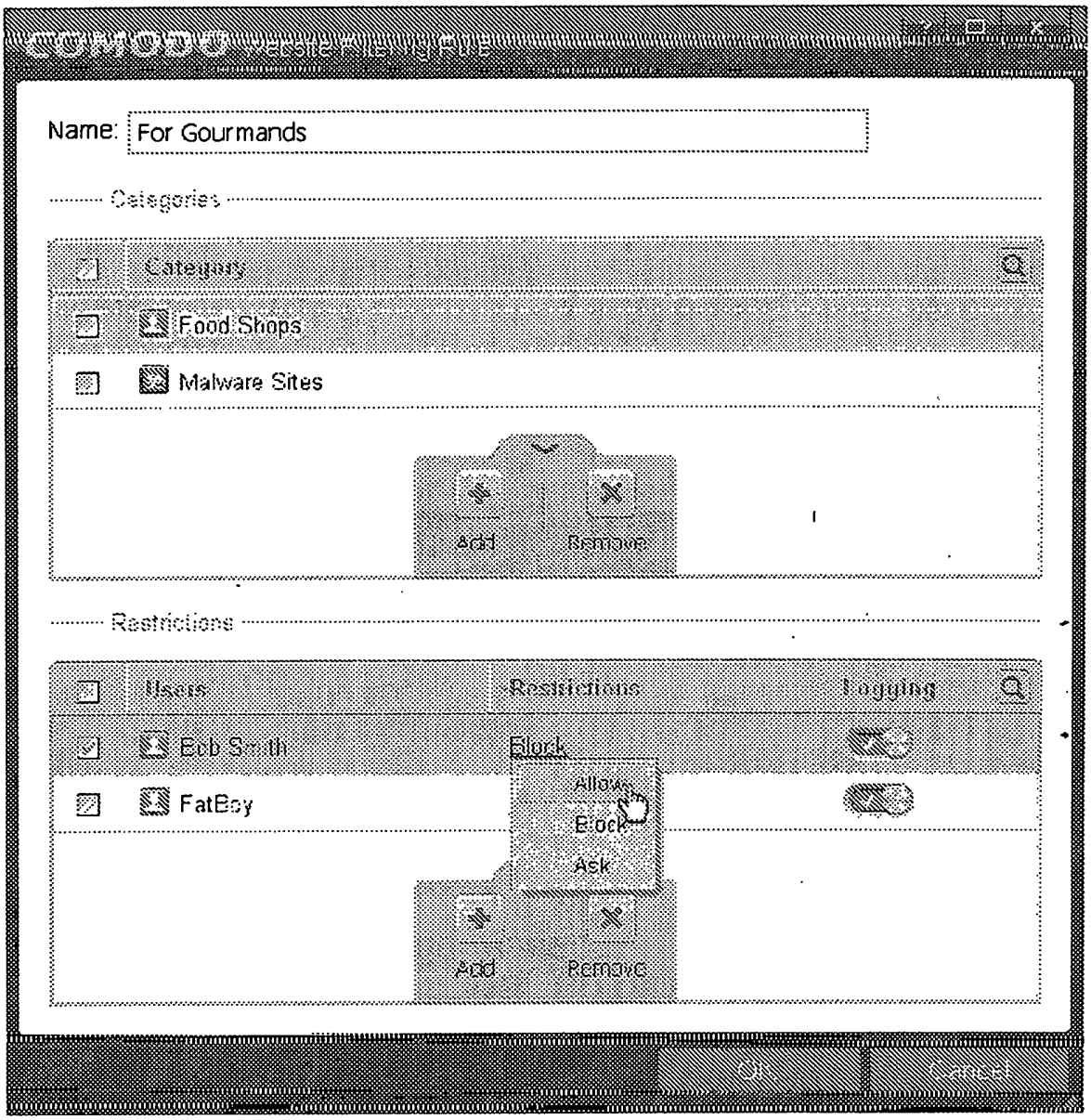
   - Click the handle at the bottom of the 'Restrictions' pane and click 'Add'. The 'Select User or Group' dialog will appear:



   - 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.

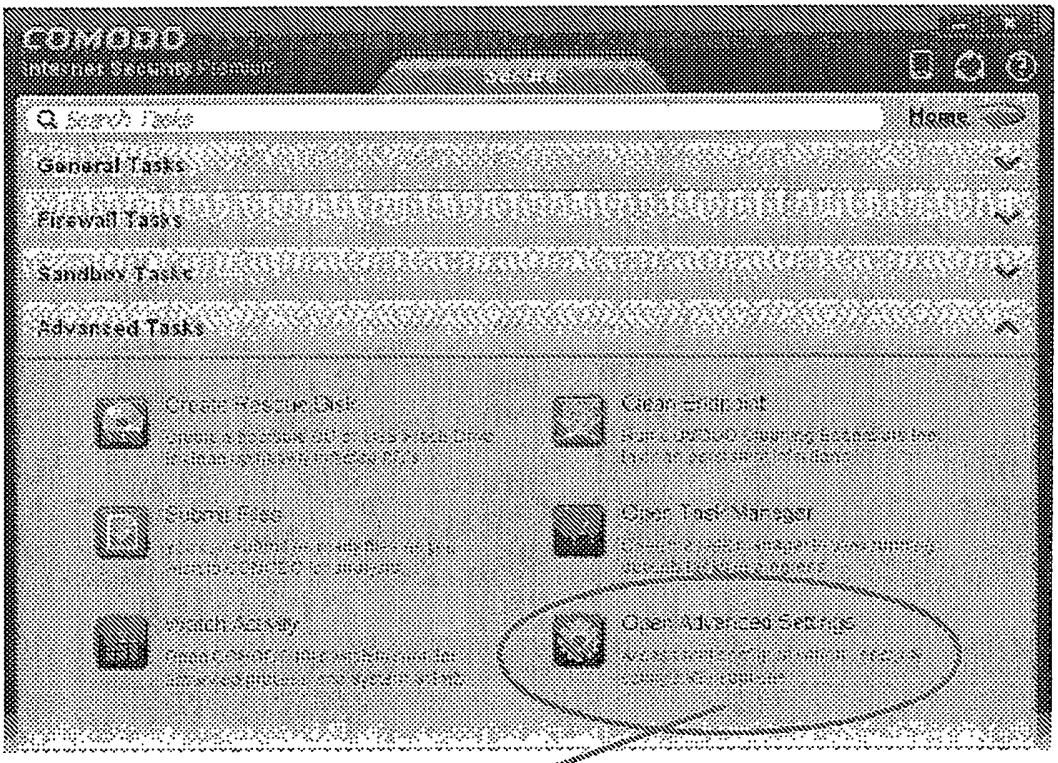
You can disable or enable rules at any time using the switch under the 'Enable Rule' column.

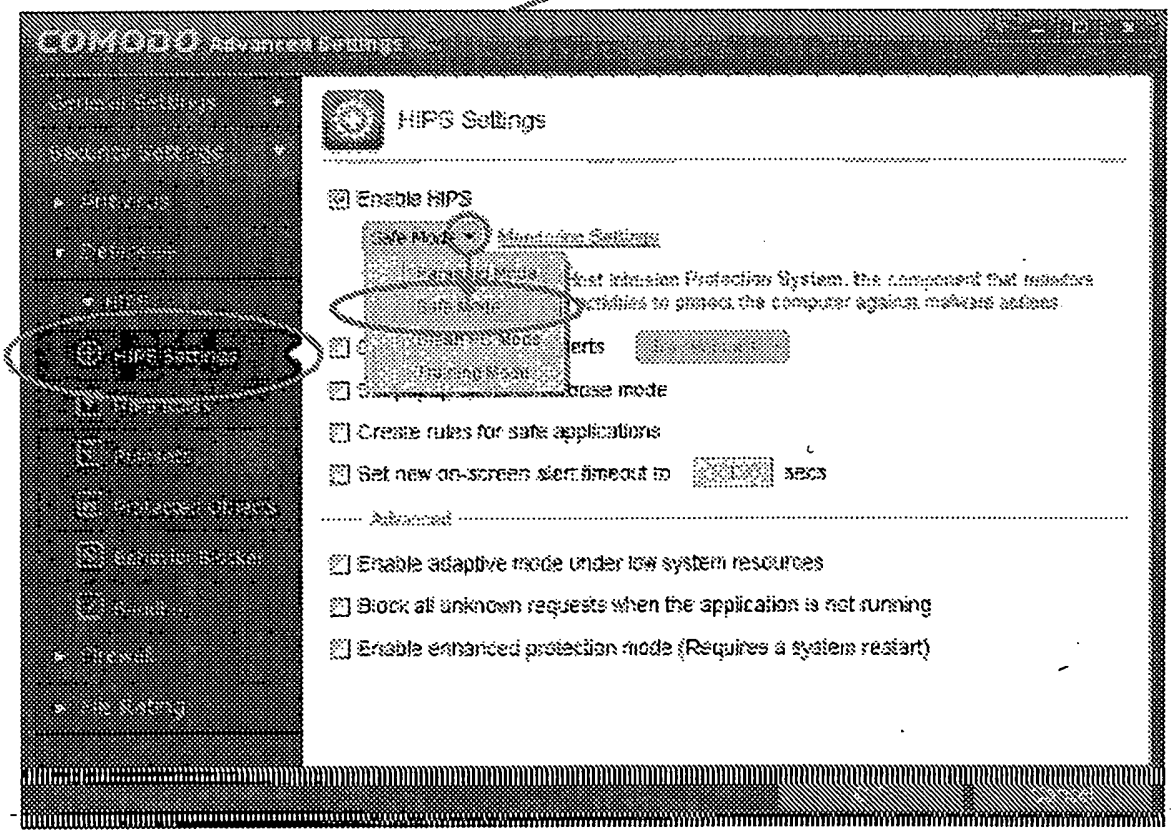
Set up the HIPS for Maximum Security and Usability

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

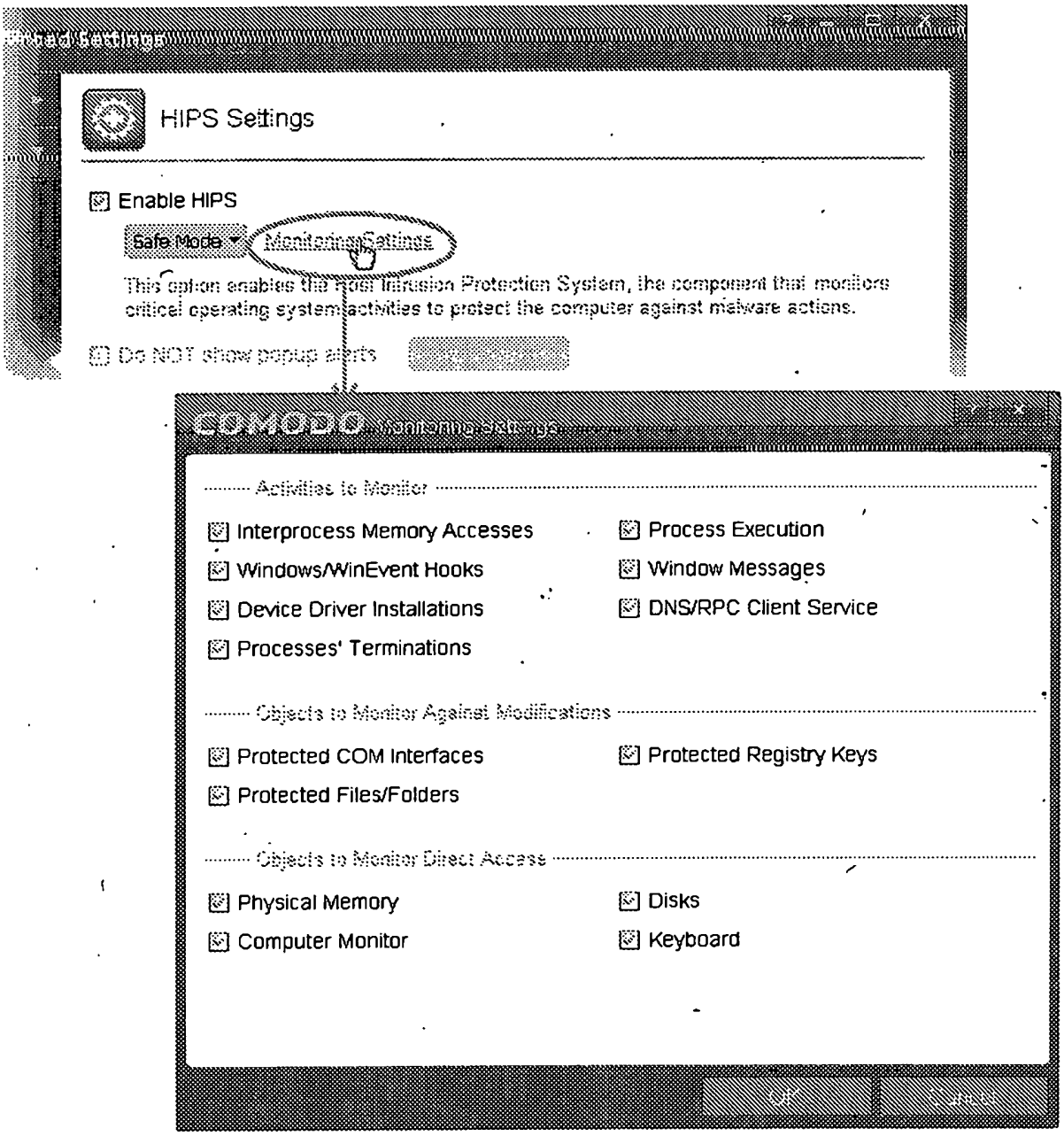




4. Select Enable HIPS
5. Choose 'Safe Mode' from the drop-down below it. Refer to HIPS Behavior Settings for more details on the Security Levels.

Monitoring Settings

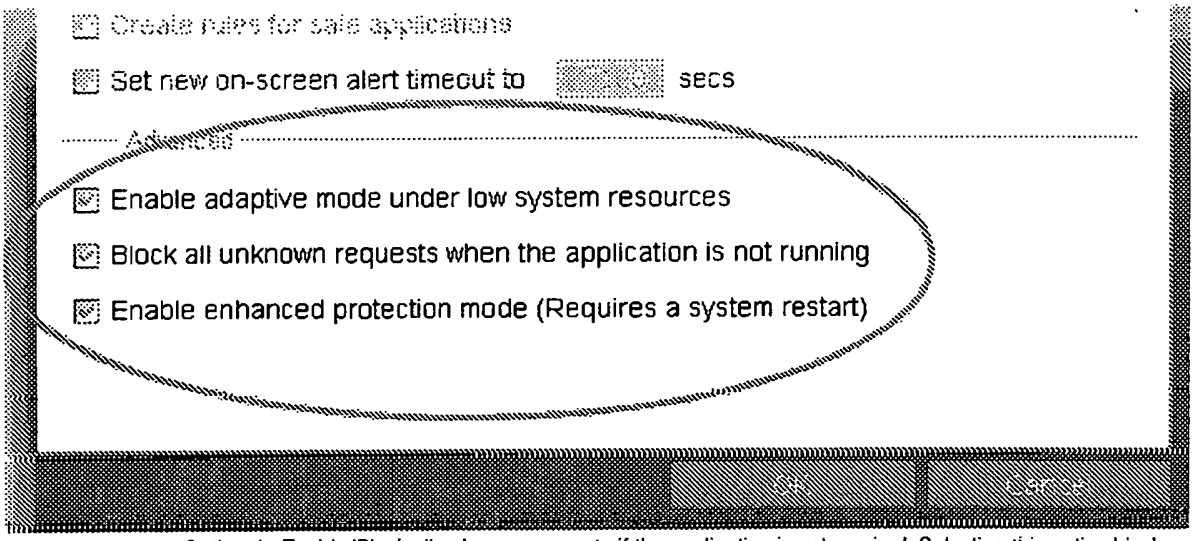
6. Click Monitoring Settings from the HIPS Settings interface



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+.

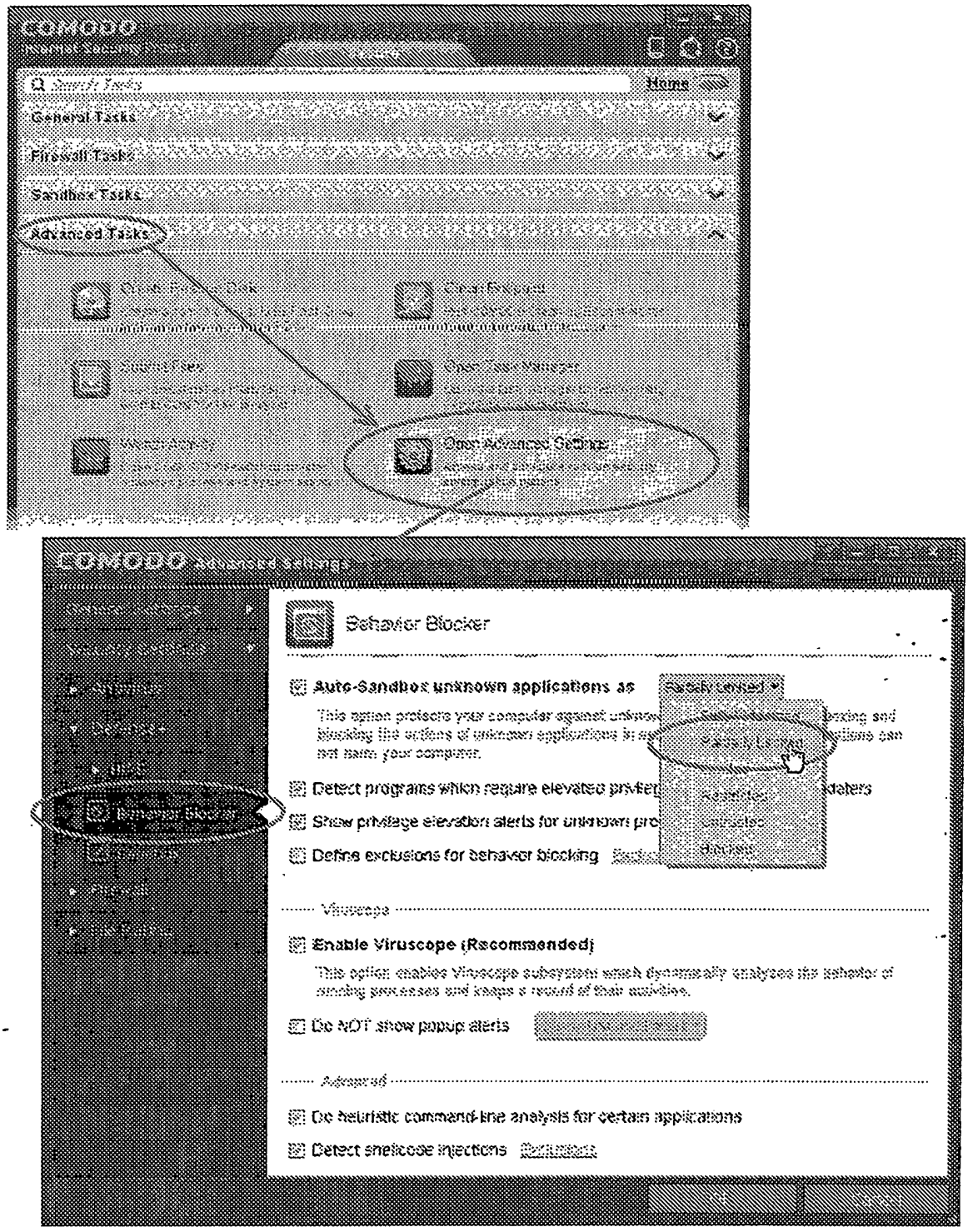
Click here for more details on HIPS Behavior Settings

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

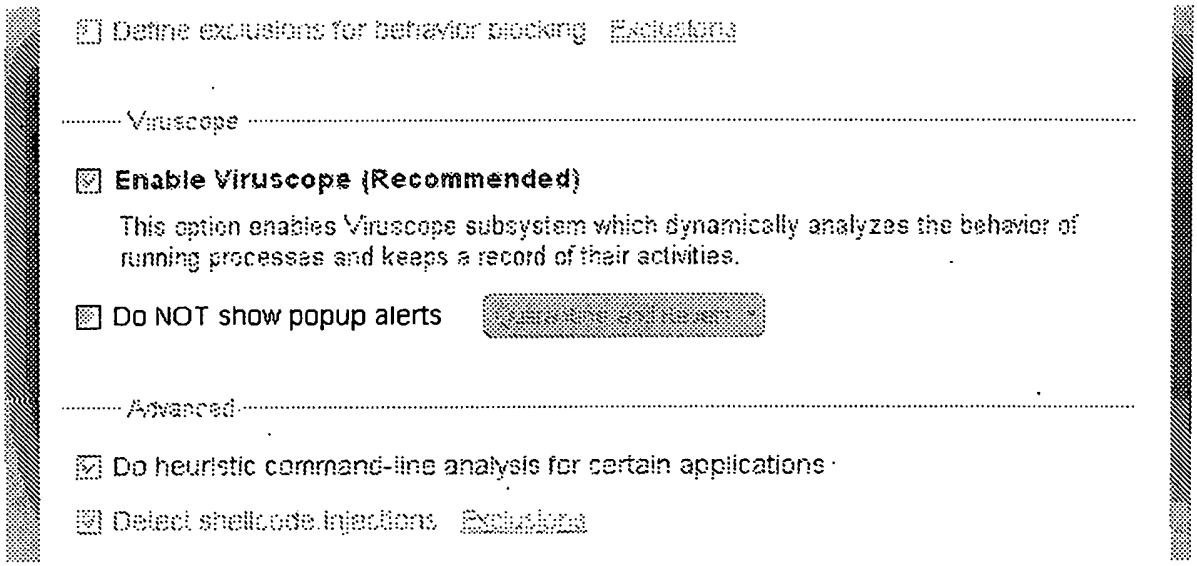
1. Open 'Tasks' interface by clicking the green curved arrow at top right of the 'Home' screen
2. Open 'Advanced Tasks' by clicking ' Advanced Tasks' from the Tasks interface and click 'Open Advanced Settings'.
3. Click 'Security Settings' > 'Defense+ ' > 'Behavior Blocker' from the left hand side pane



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

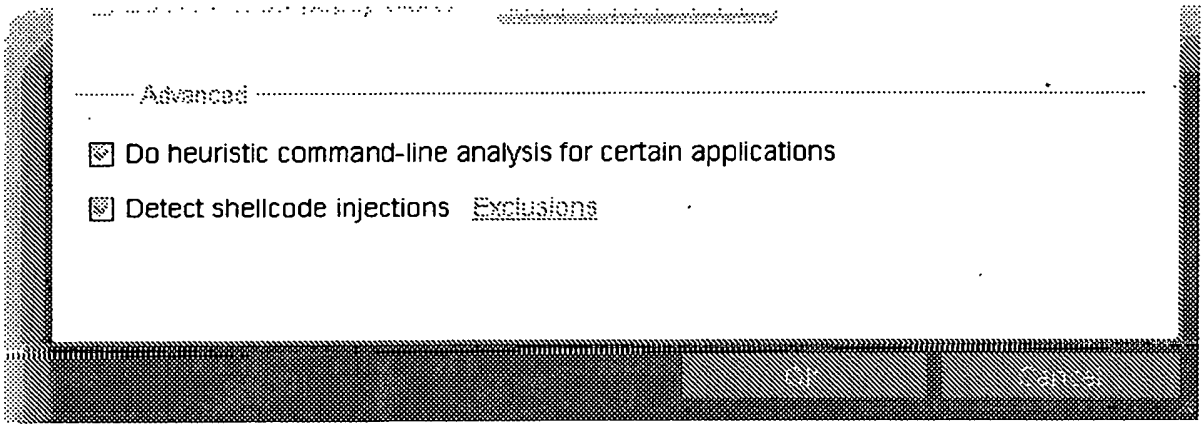
5. Make sure 'Enable Viruscope' checkbox is selected under 'Viruscope'



Advanced Settings

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

    ... are selected.



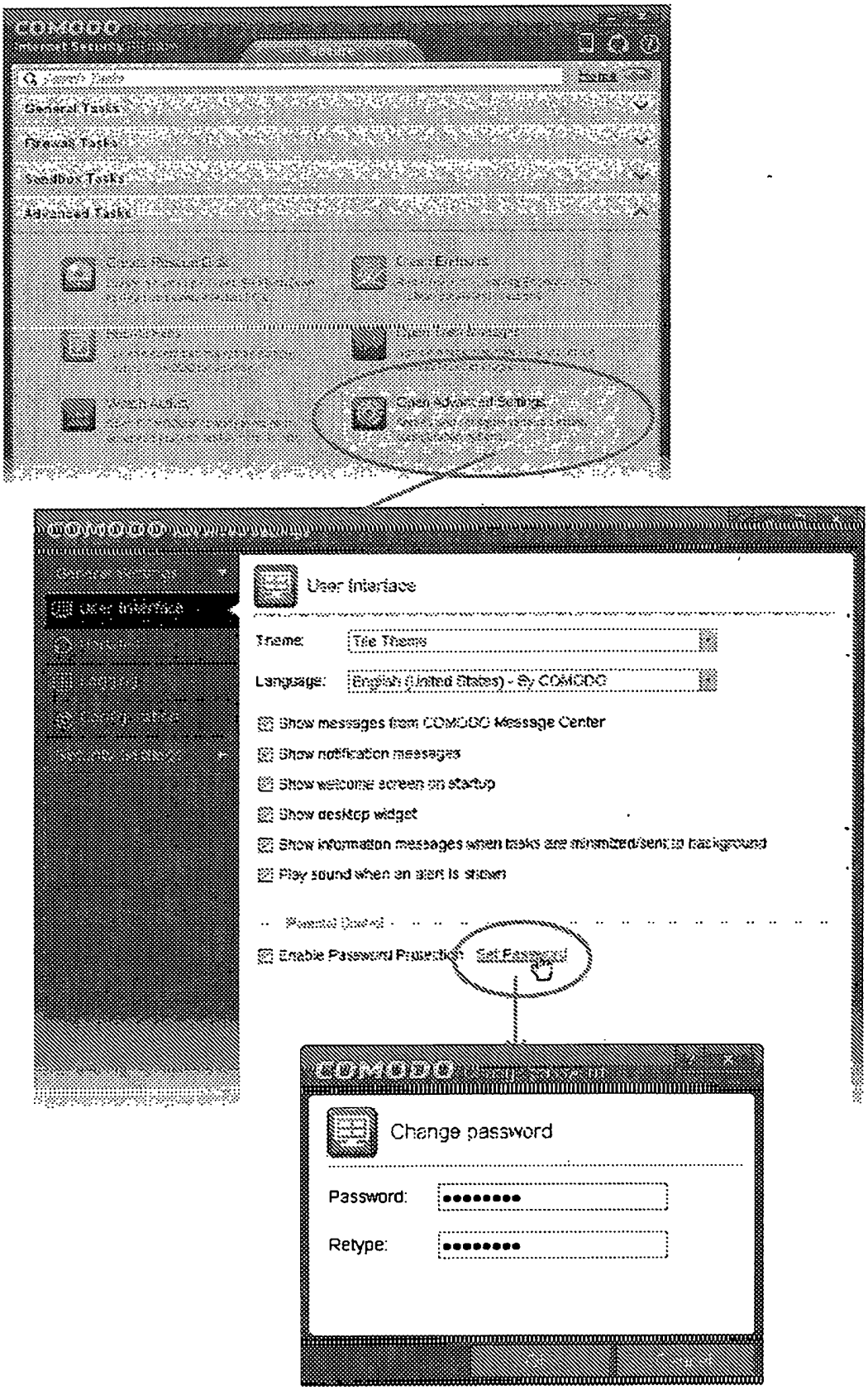
Click here for more details on Behavior Blocker Settings

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.

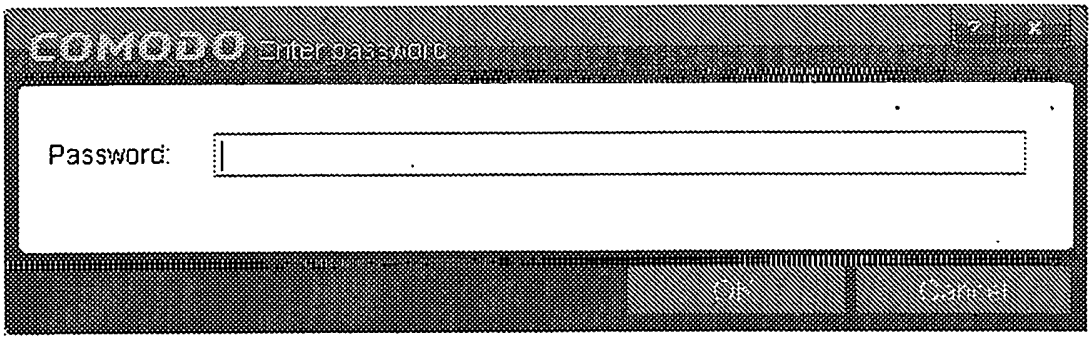
To enable password protection

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.



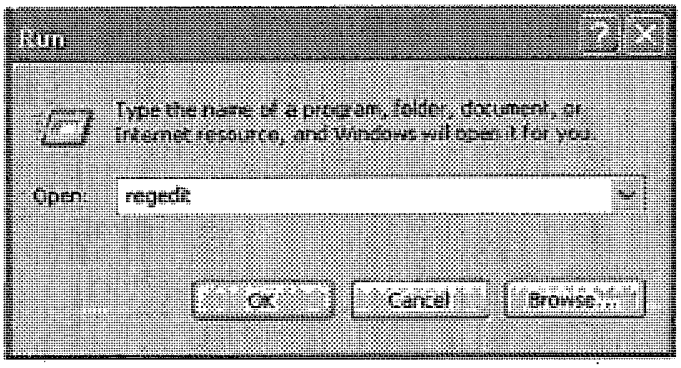
Reset Forgotten Password (Advanced)

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.

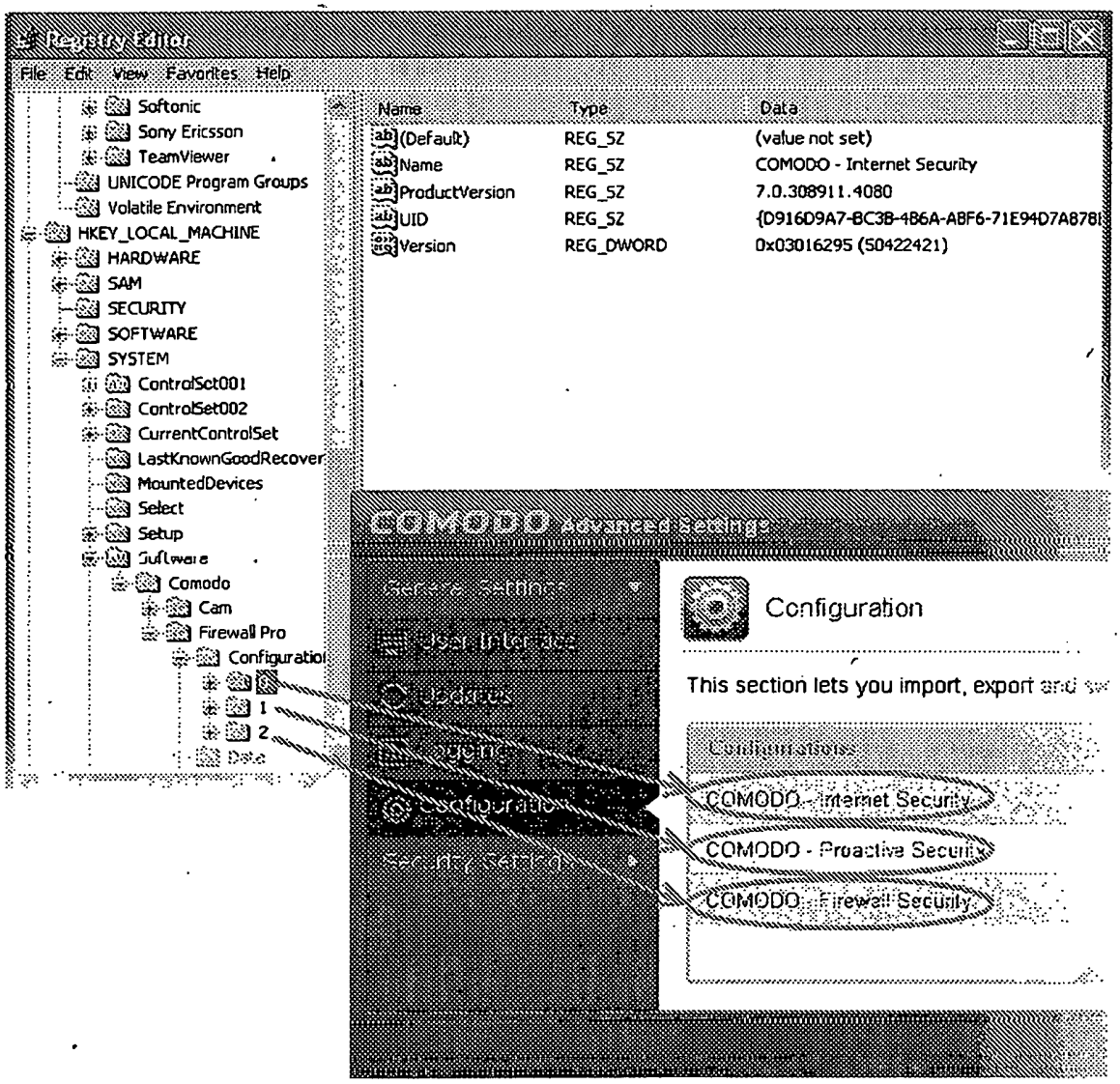
To disable password protection in CIS

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

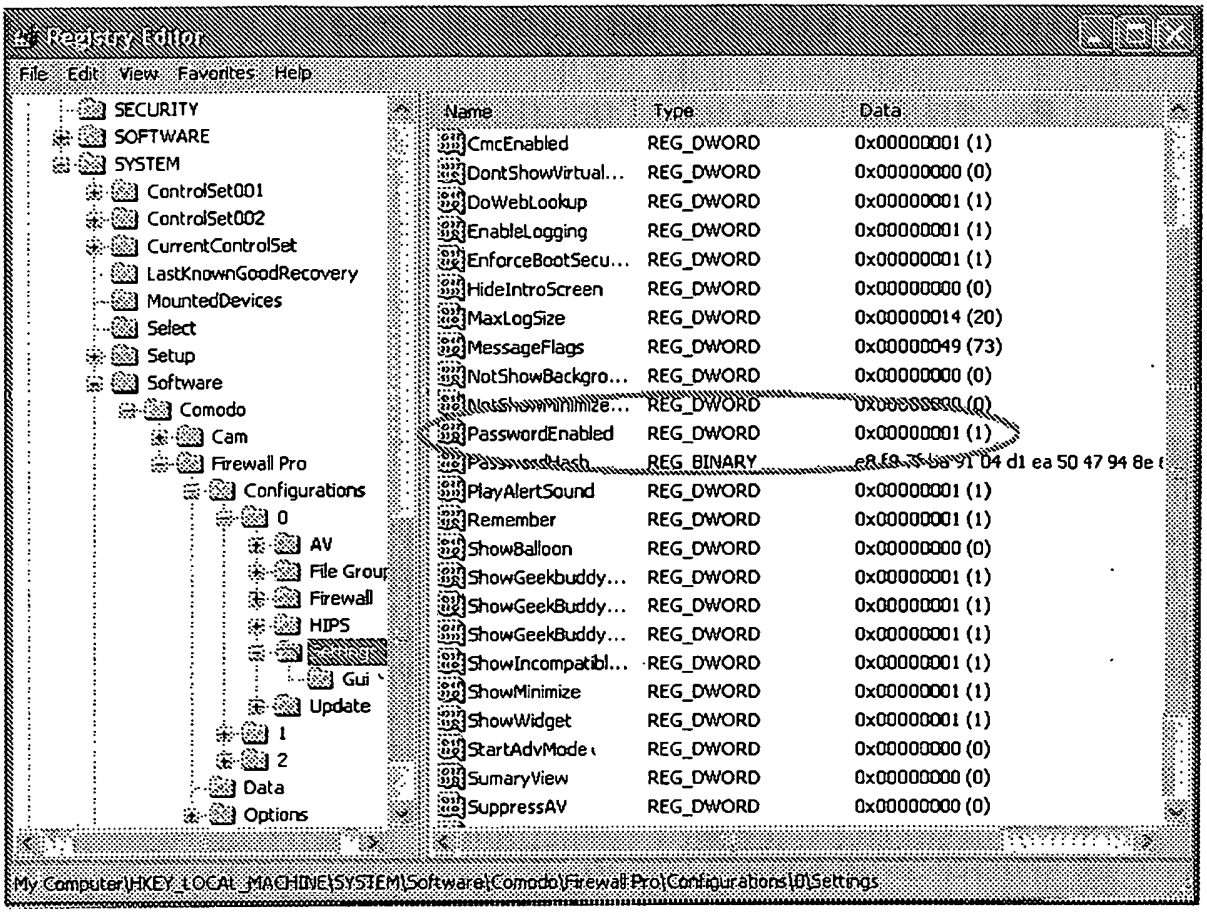


3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\

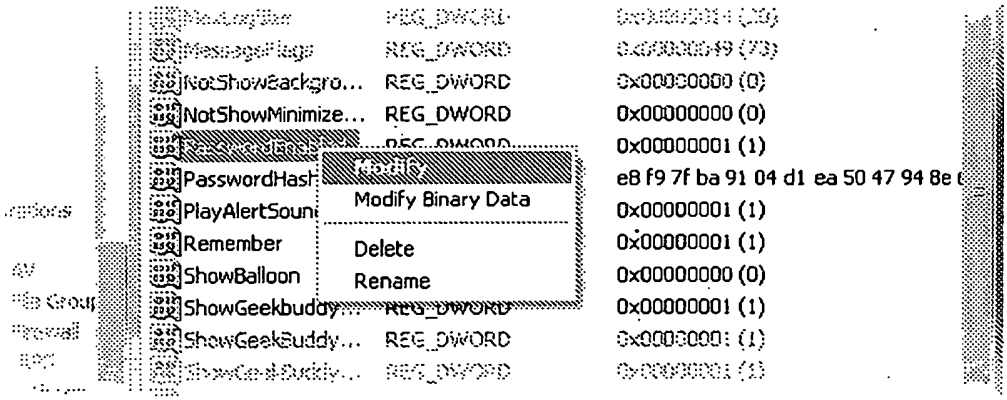
Under the Configurations folder you will see sub-folders named 0,1,2,... depending on the number of preset configurations in CIS. These folders contain registry keys for the settings of the preset configurations in the order of the configurations displayed in Advanced Settings > General Settings > Configuration 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.



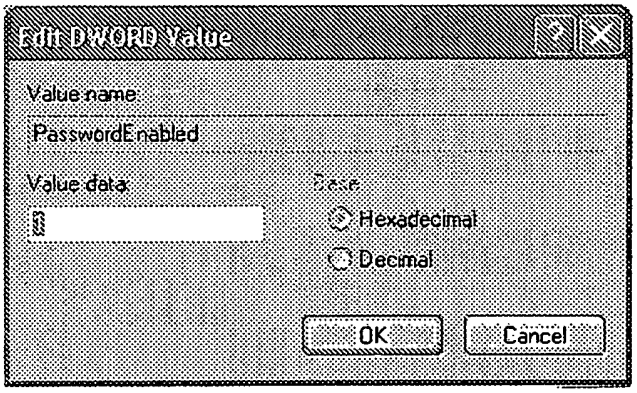
4. Select the folder corresponding to the configuration for which you wish to reset the password and navigate to Settings, for example, navigate to HKEY_LOCAL_MACHINE\SYSTEM\Software\Comodo\FirewallPro\Configurations\0\Settings to reset password in COMODO - Internet Security configuration.



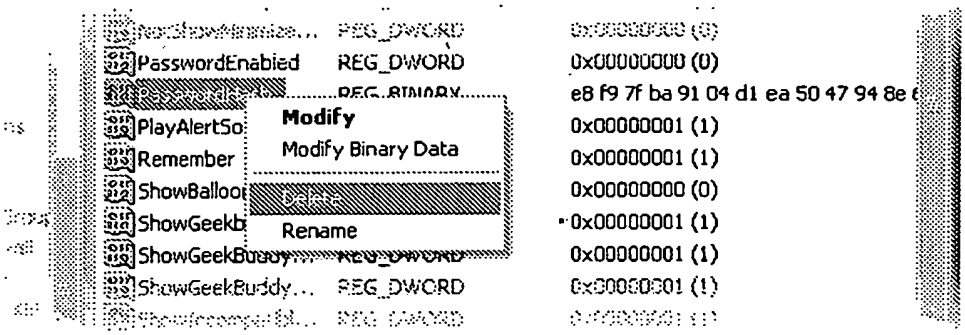
5. Right-click 'PasswordEnabled' key and select 'Modify'



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.

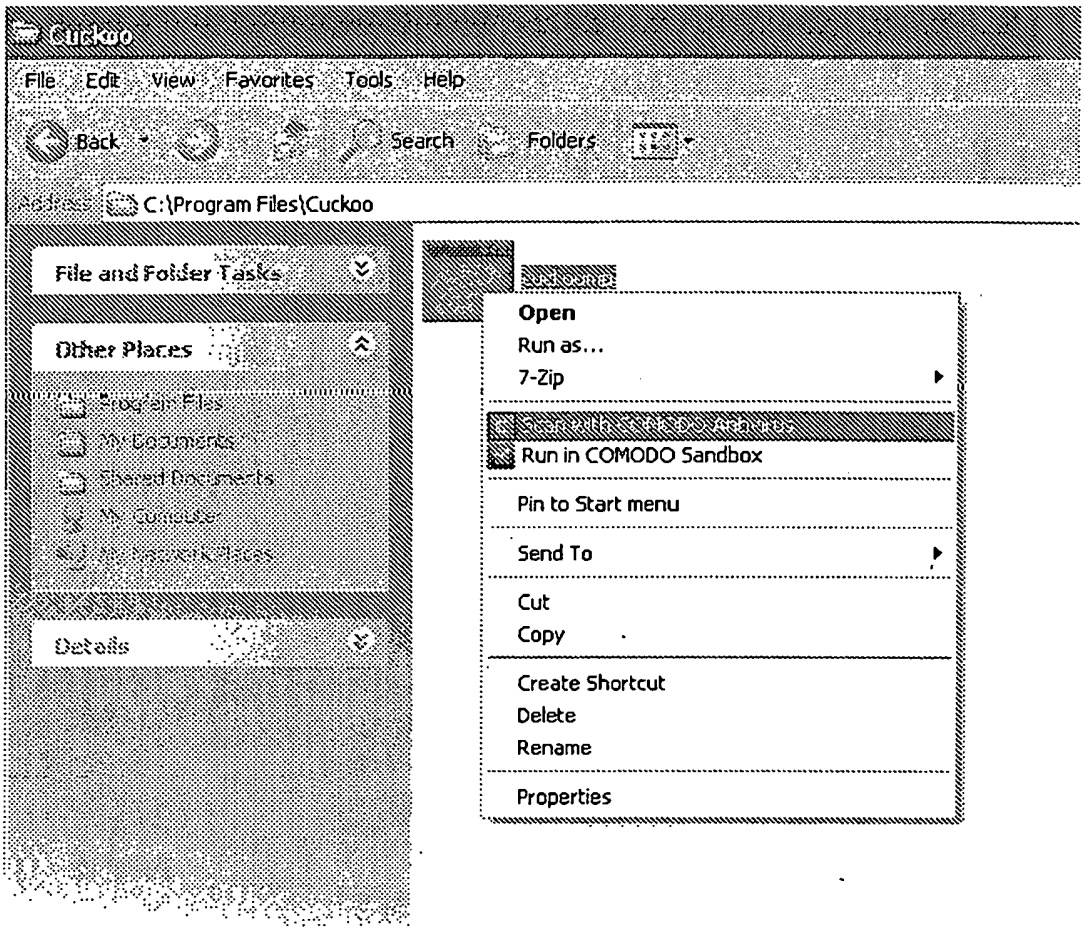
Run an Instant Antivirus Scan on Selected Items

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.

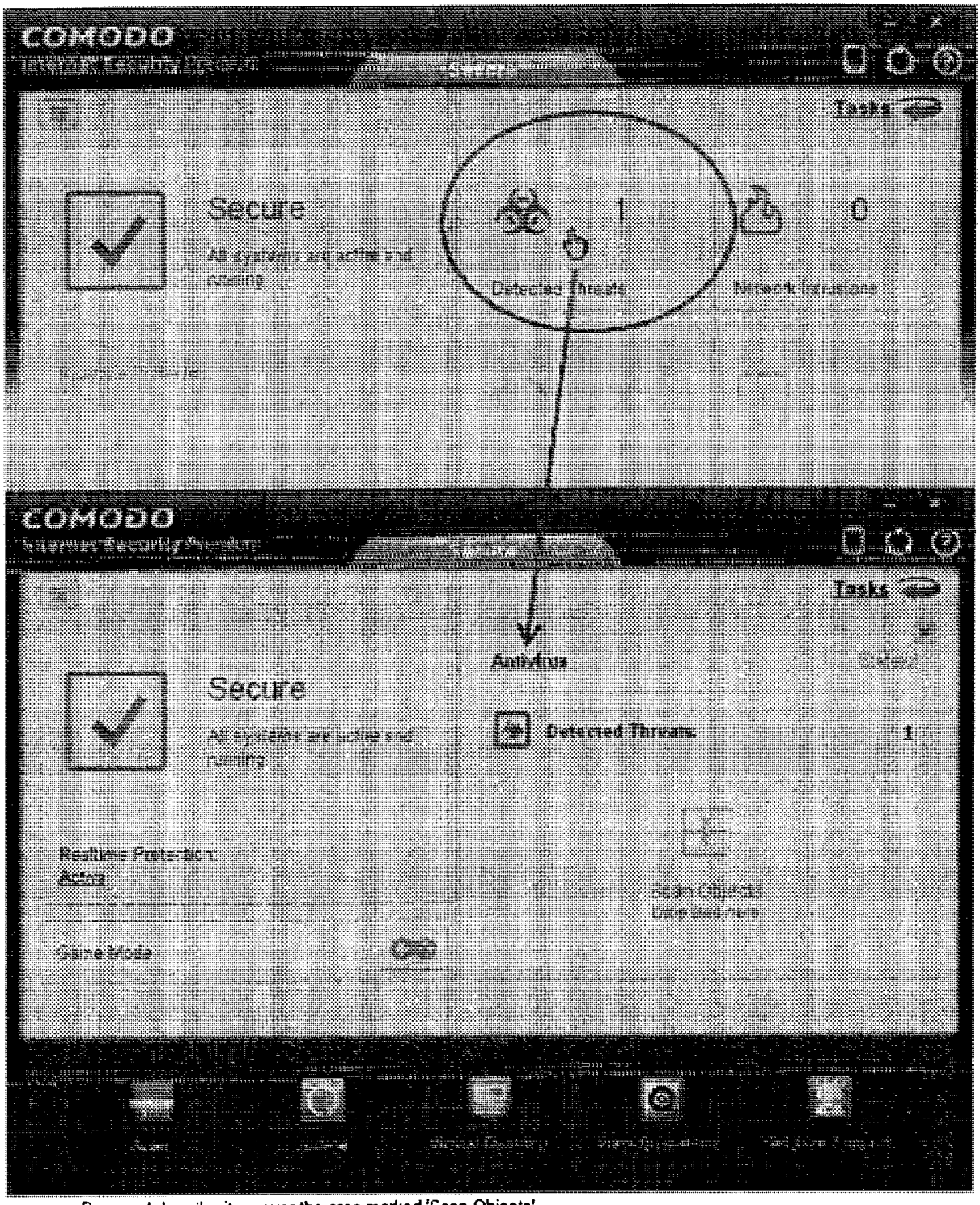
To instantly scan an item

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

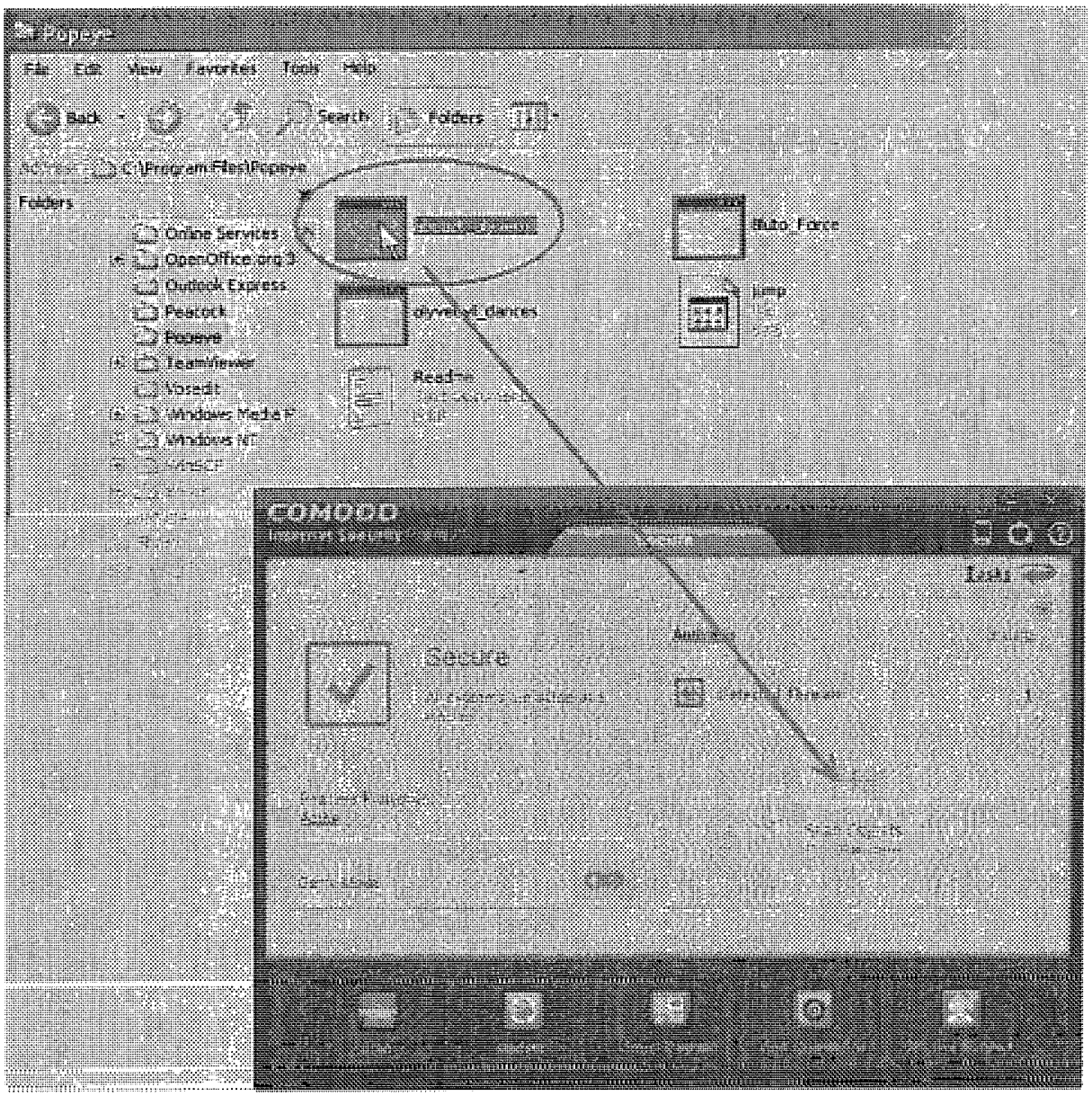


OR

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

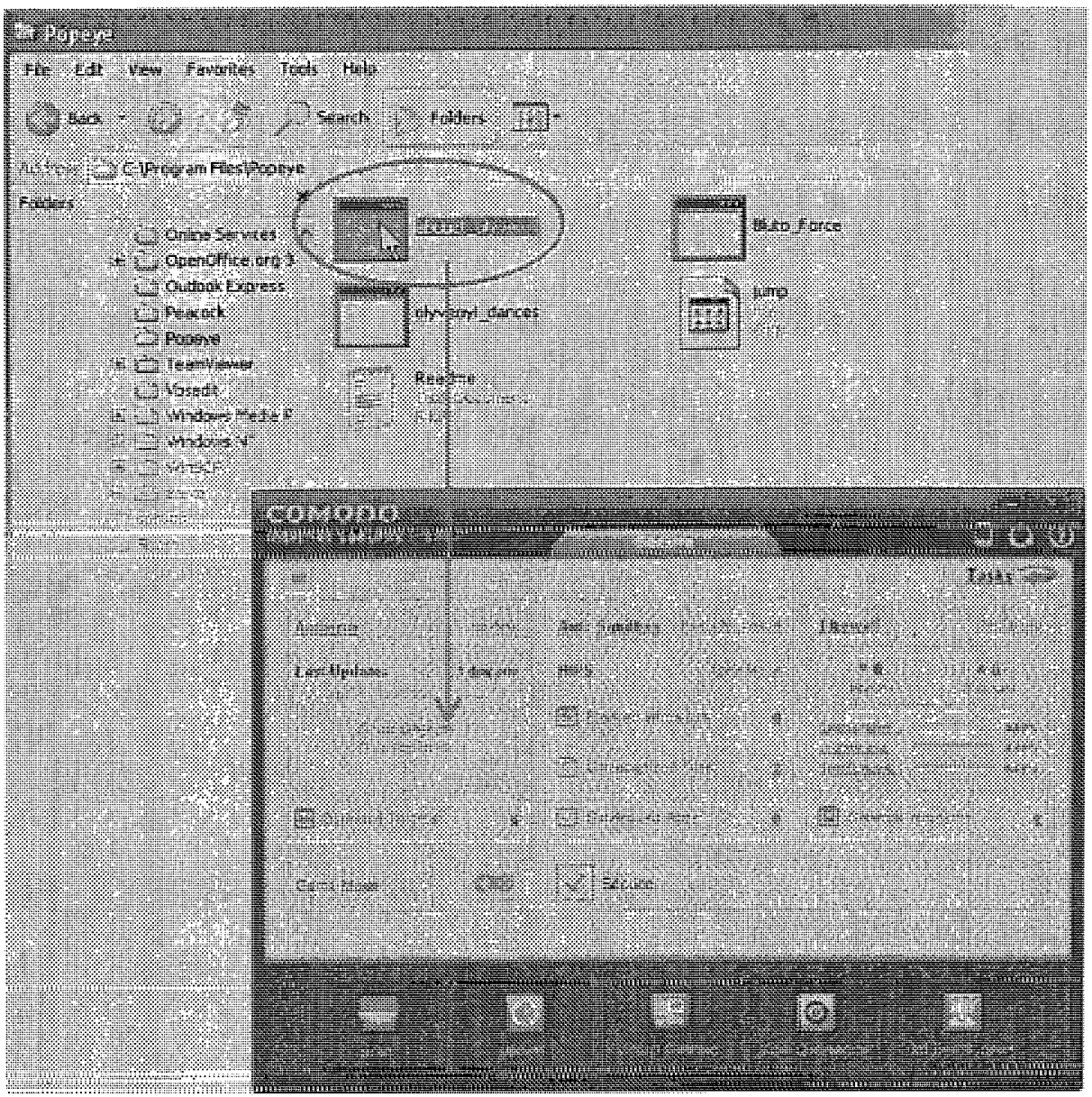


- Drag and drop the item over the area marked 'Scan Objects'.

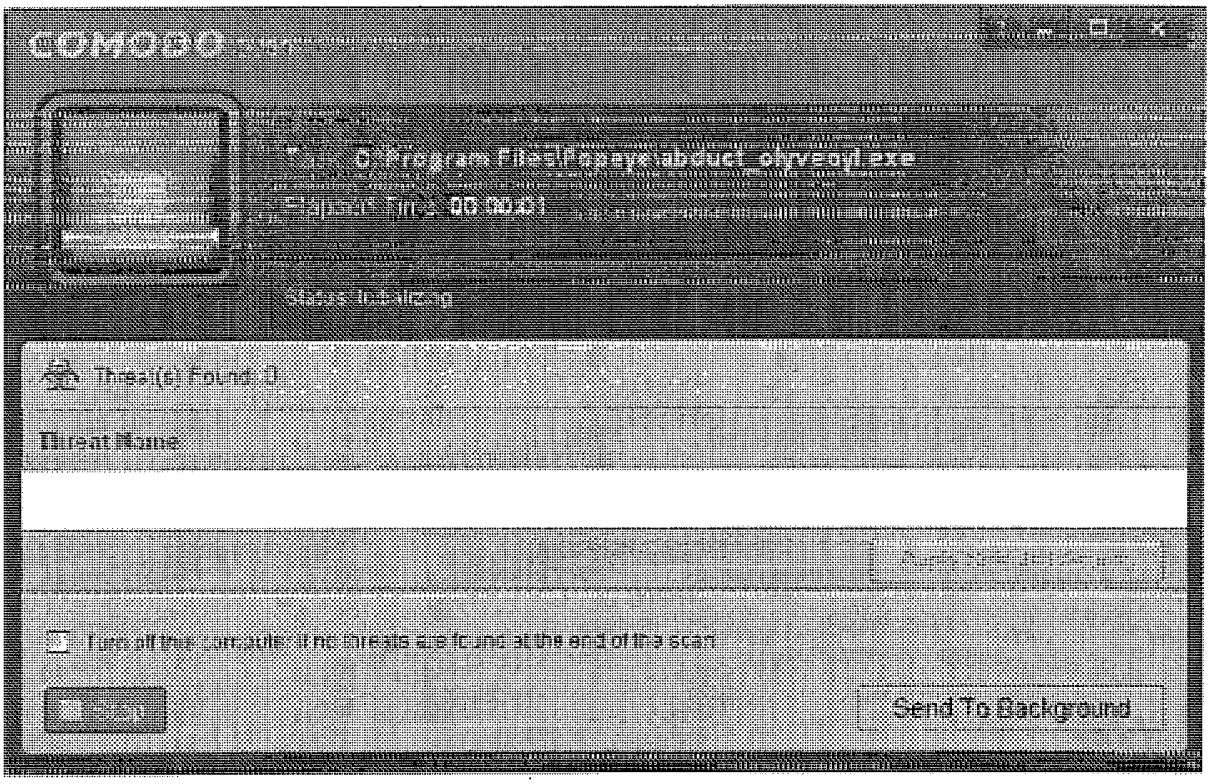


OR

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



The item will be scanned immediately.



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

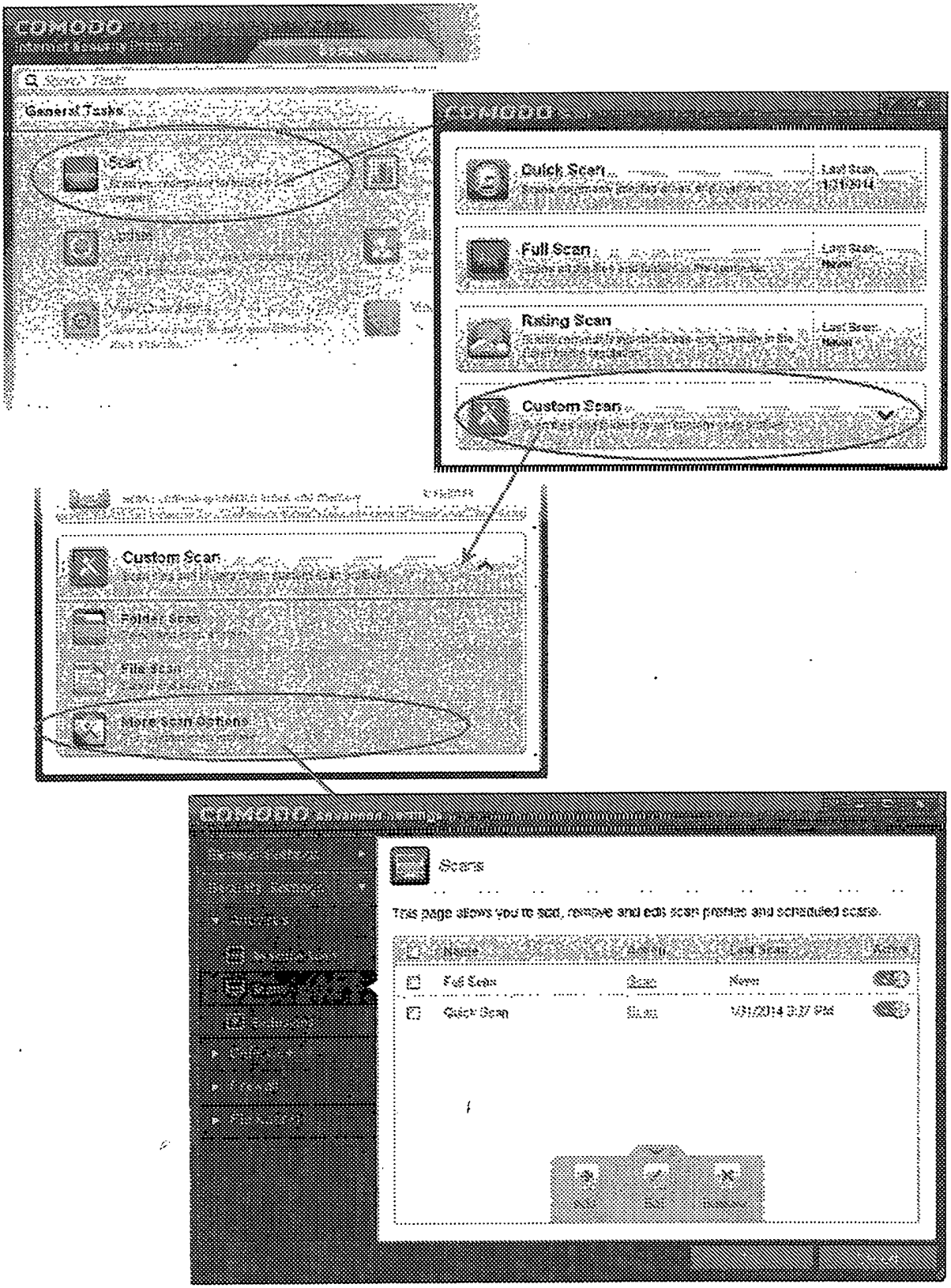
Click here for more details to take action on the infected item(s).

Create an Antivirus Scanning Schedule

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

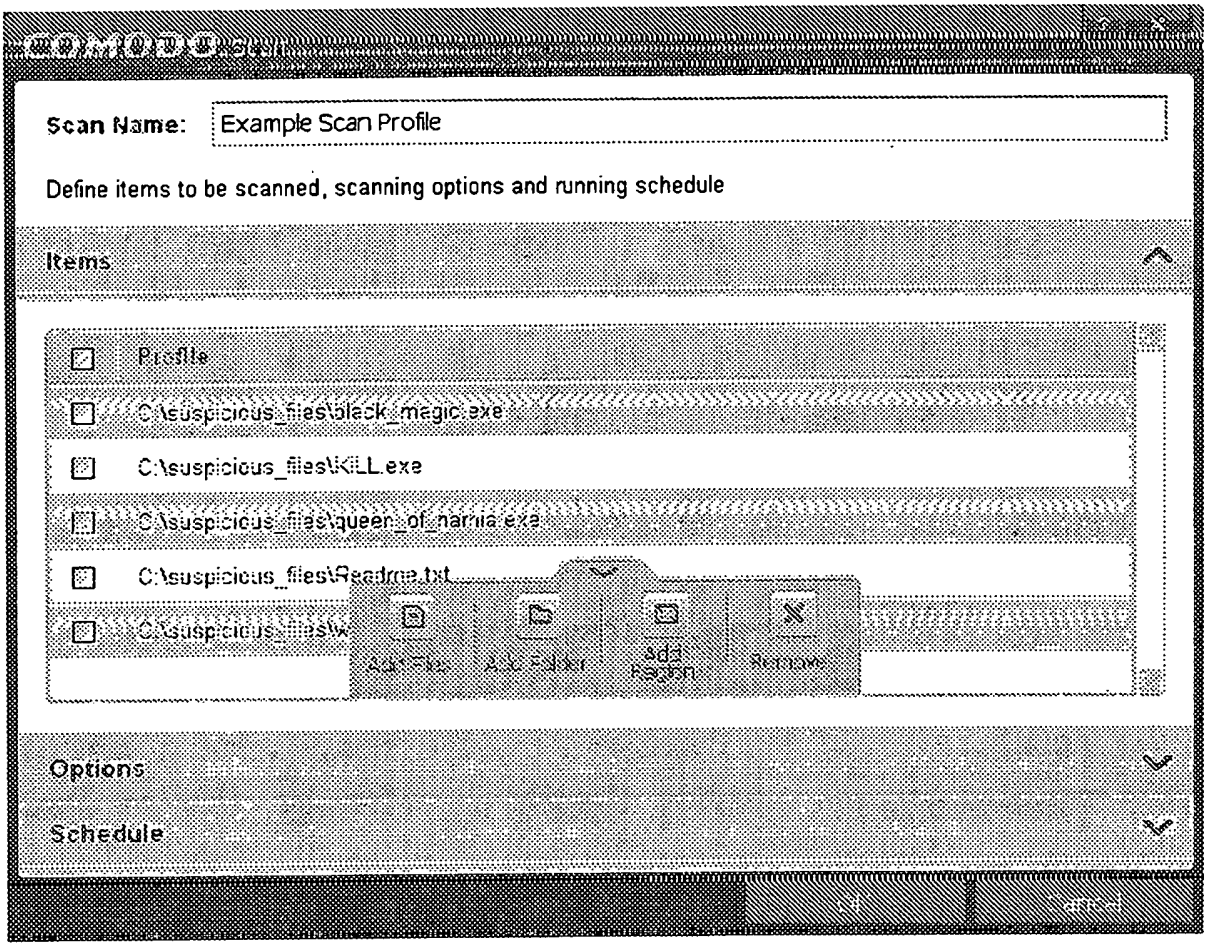
To create an antivirus scanning schedule

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

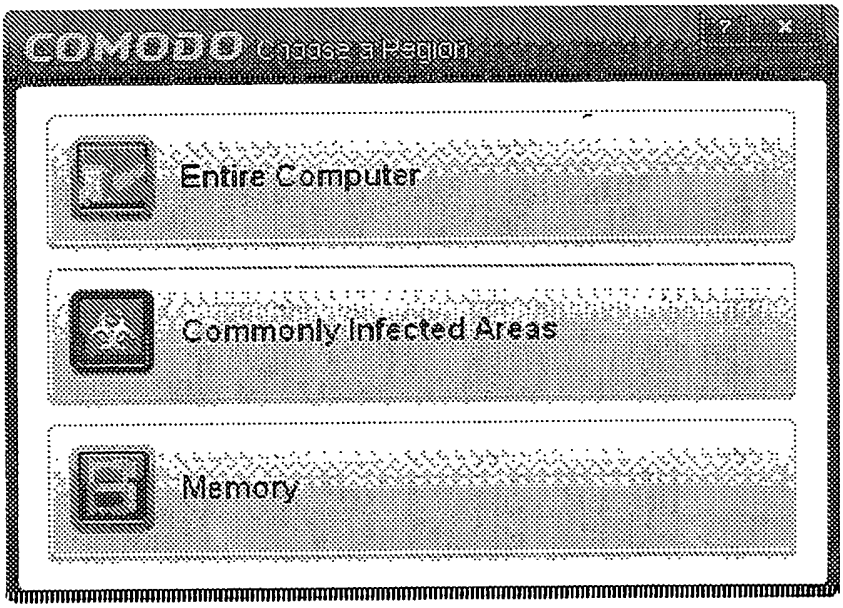


The scan profile interface will be displayed.

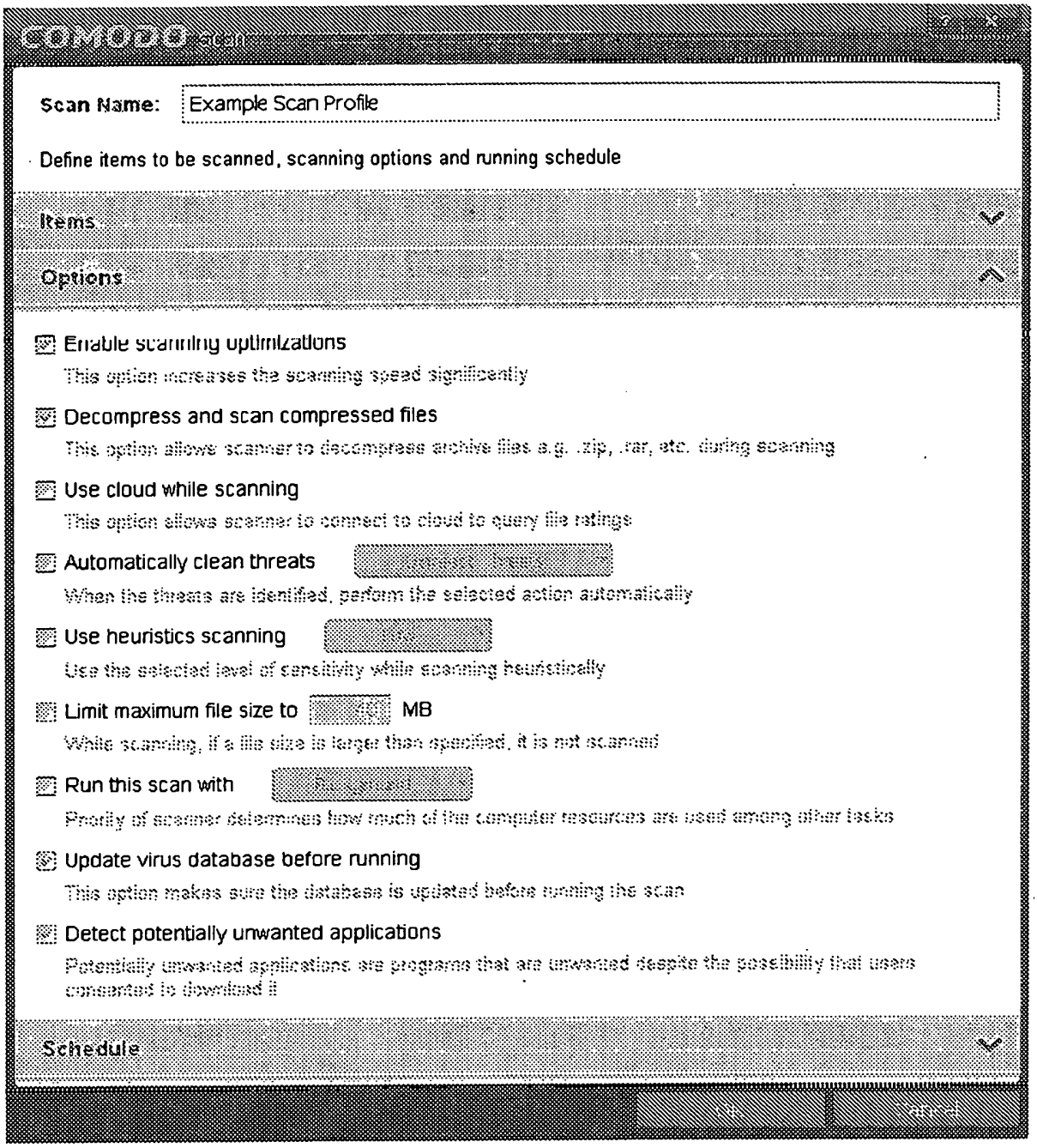
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



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



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



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

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

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

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

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

- **Limit maximum file size to** - Select this option if you want to impose size restrictions on files being scanned. Files of size larger than that specified here, are not scanned, if this option is selected ***(Default = 40 MB)***.
- **Run this scan with** - Enables you to set the priority of the scan profile. You can select the priority from the drop-down.(***Default = Disabled***).
- **Update virus database before running** - Instructs Comodo Internet Security to check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning (***Default = Enabled***) .
- **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':