- Scan individual file/folder
- Processing Infected Files

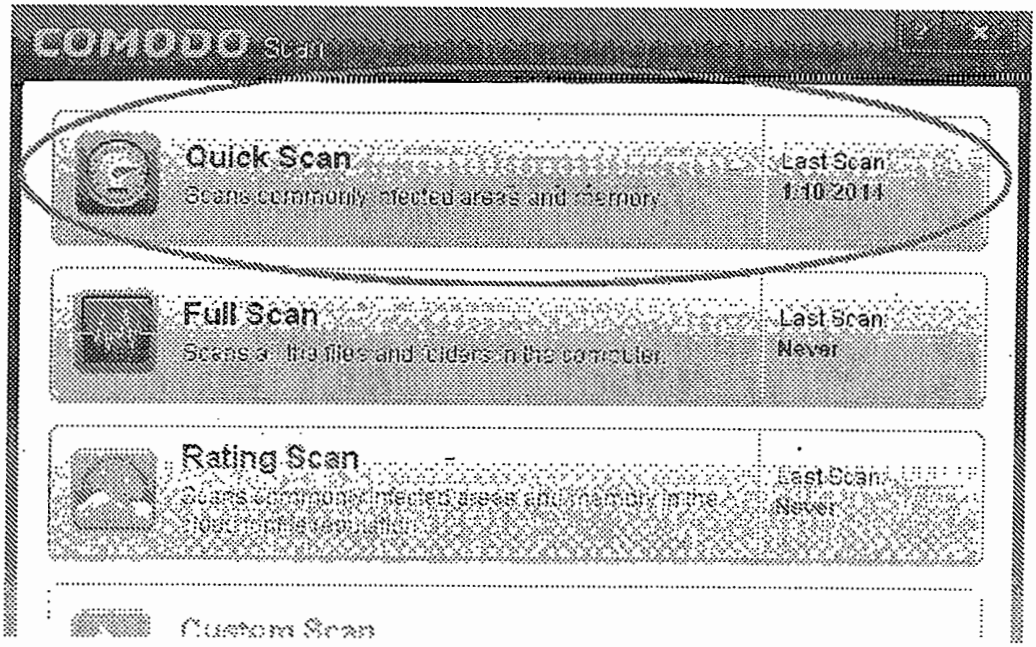
2.1.1. Run a Quick Scan

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

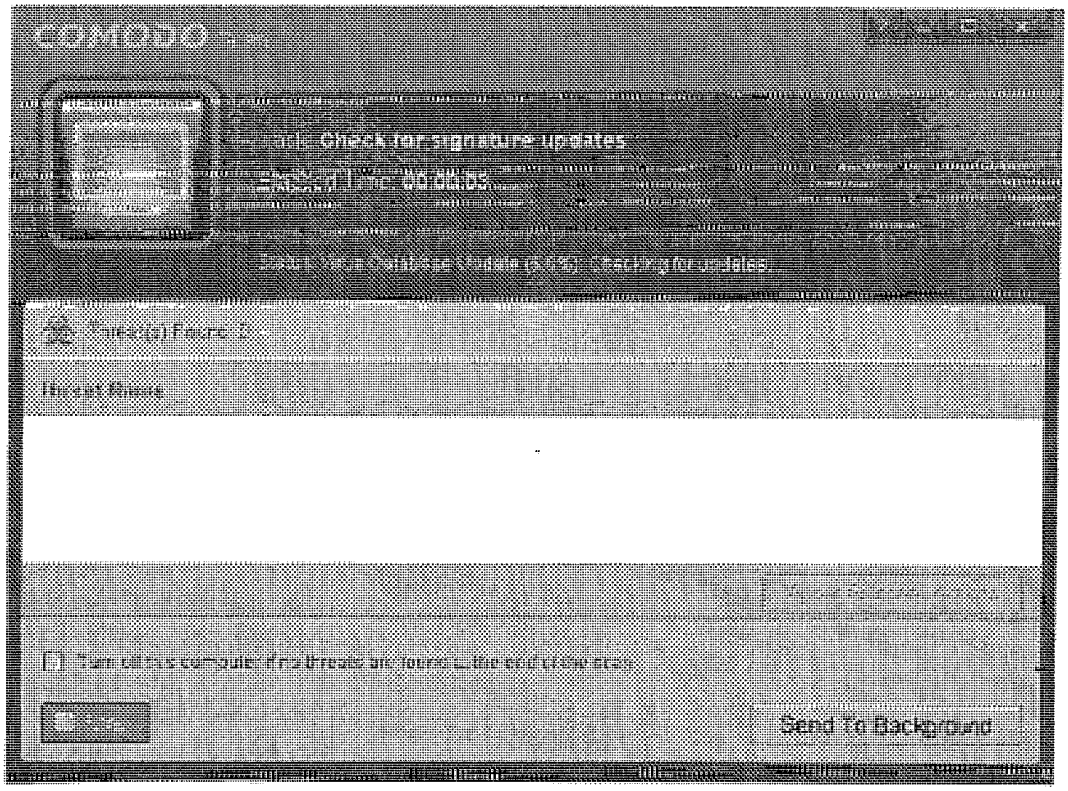
You can customize which items are scanned under a 'Quick Scan' and create a scan schedule from the 'Advanced Tasks' interface. Refer to Antivirus Settings > Scan Profiles for more details.

To run a Quick Scan

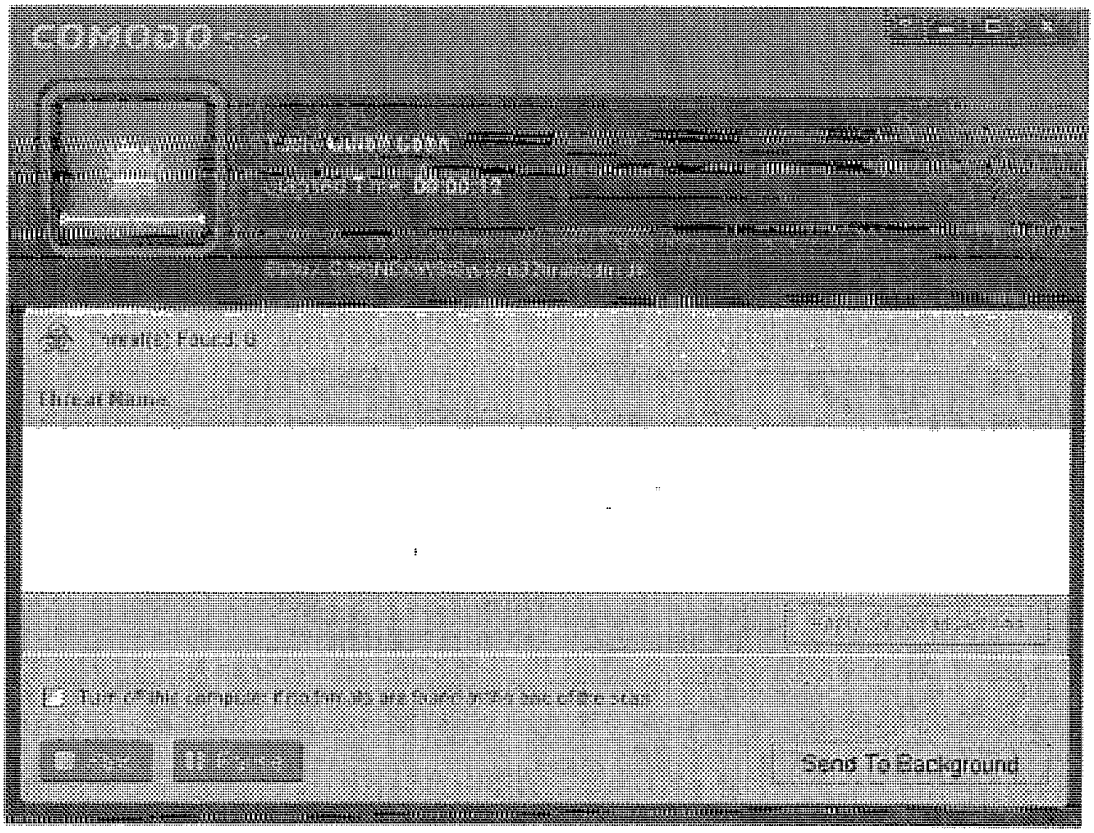
- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



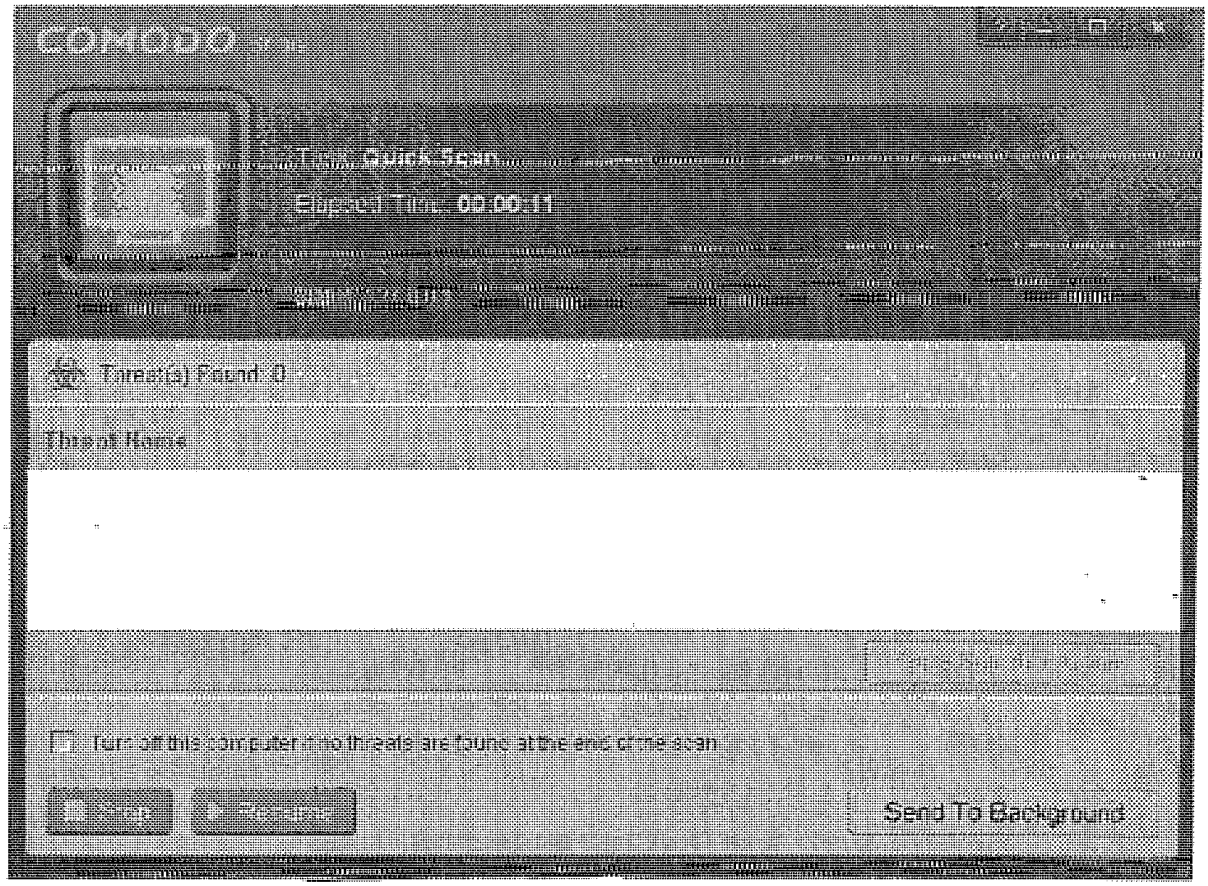
The scanner will start and first check whether your virus signature database is up-to-date:



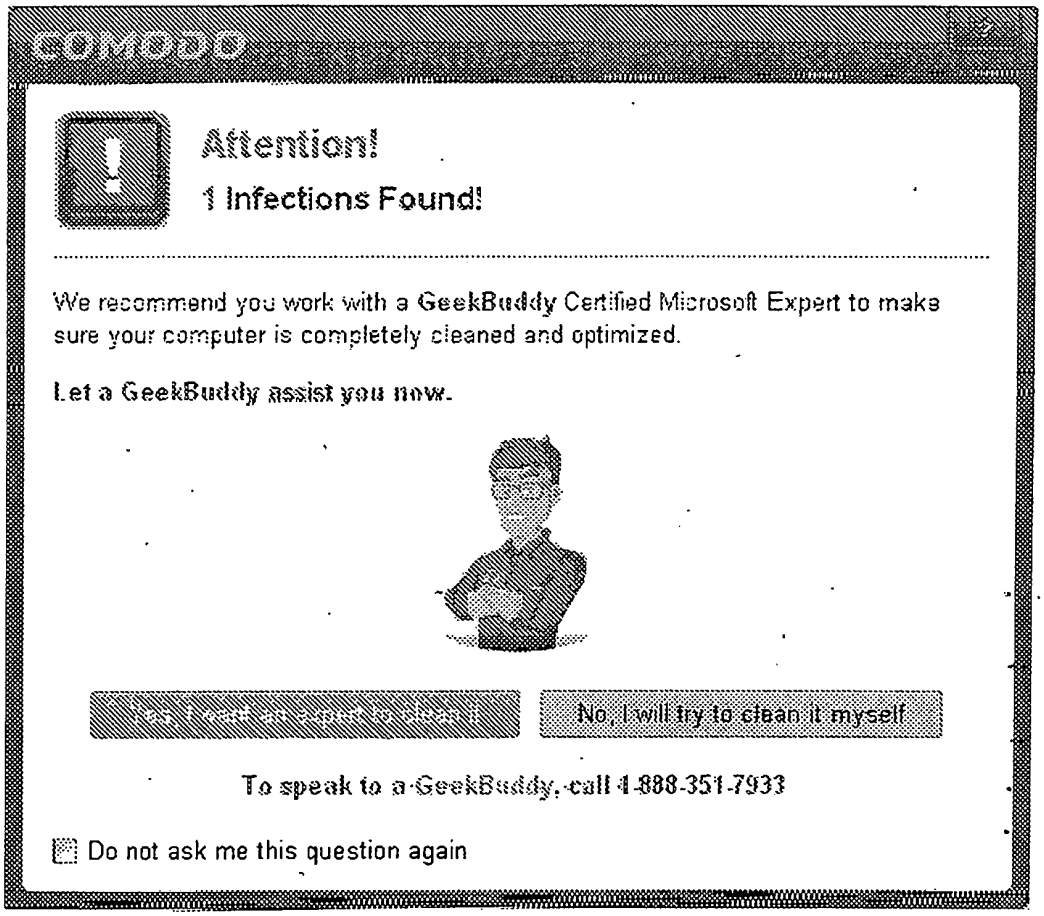
If the database is outdated, the scanner will first download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:



- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'. You can still keep track of the scan progress from the 'Task Manager' interface.



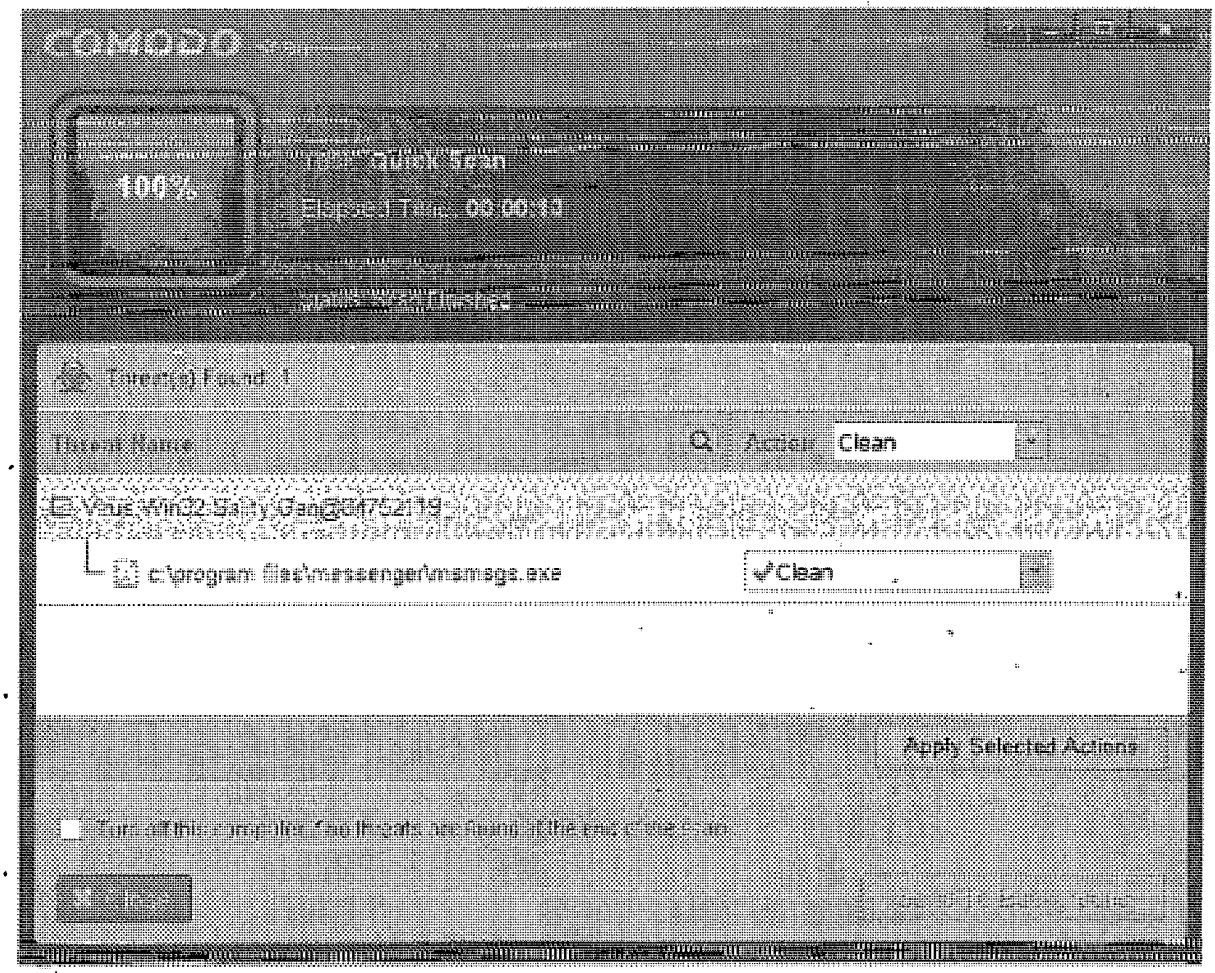
- An alert screen will be displayed at the end of the scan if issues were detected. The alert will display the number of threats/infections discovered and present you with cleaning options:



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

  For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.

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



The results window shows the number of objects scanned and the number of threats (Viruses, Rootkits, Malware). Use the drop-down menu to choose whether to clean, move to quarantine or ignore the threat. Refer to Processing the infected files for more details.

2.1.2. Run a Full Computer Scan

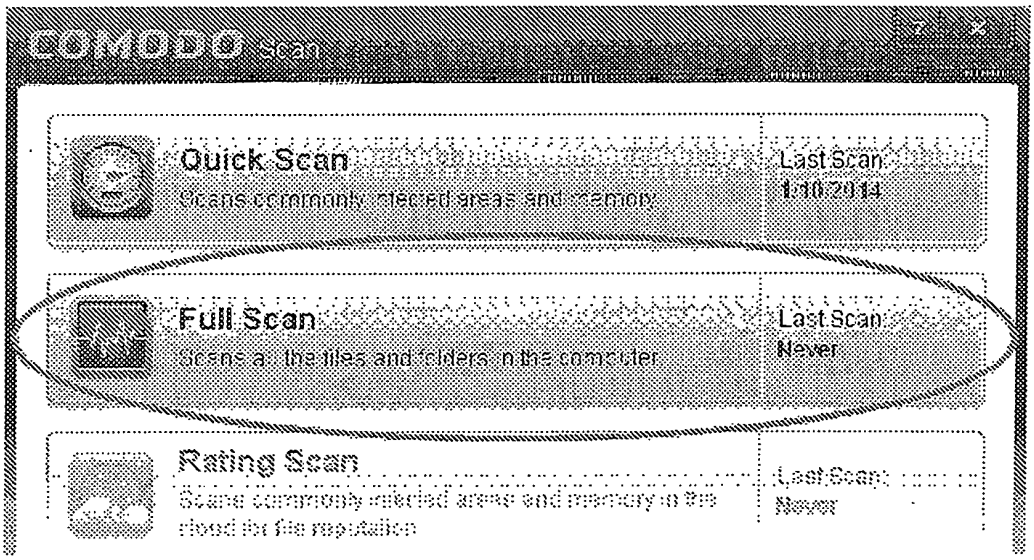
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

You can customize which items are included in a full scan and set-up a scan schedule from the 'Advanced Tasks' interface.

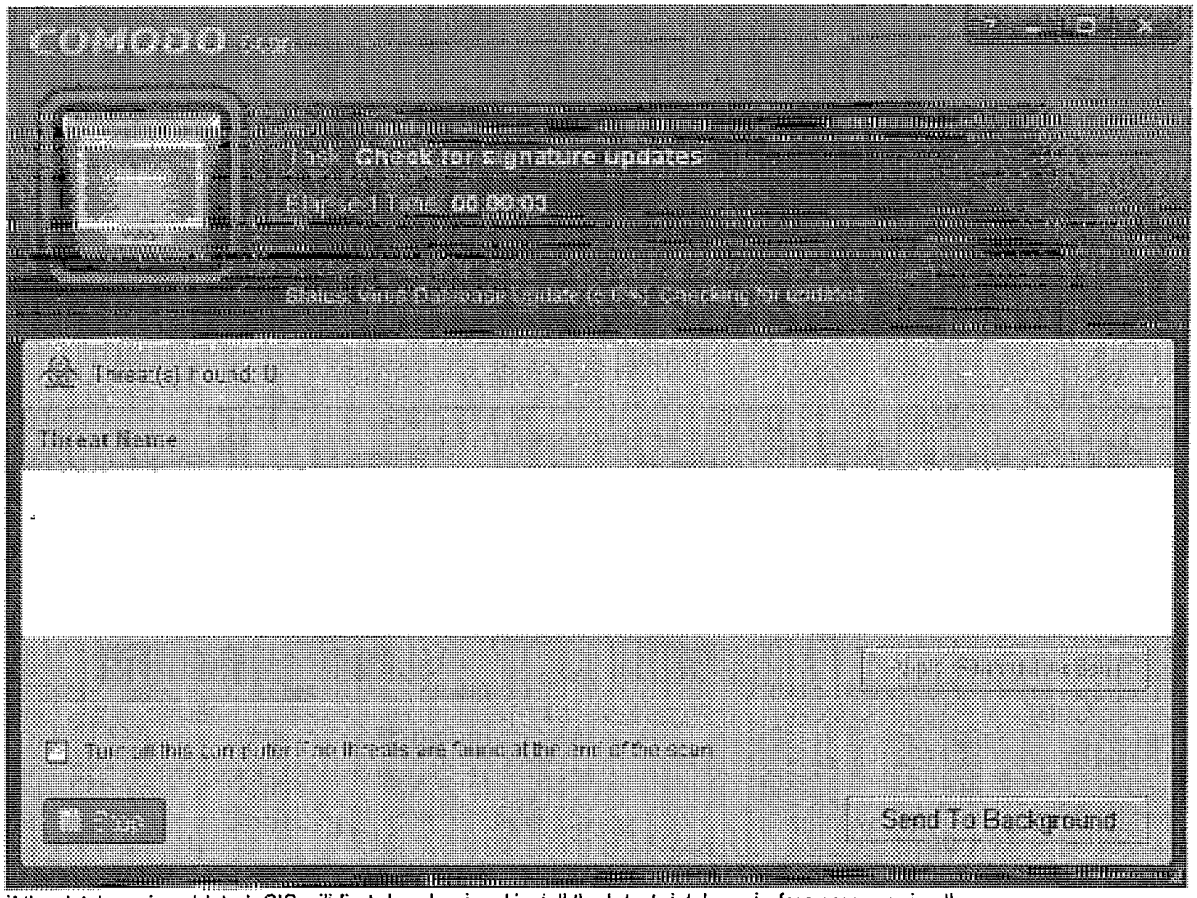
Refer to Antivirus Settings > Scan Profiles for more details.

To run a Full Computer Scan

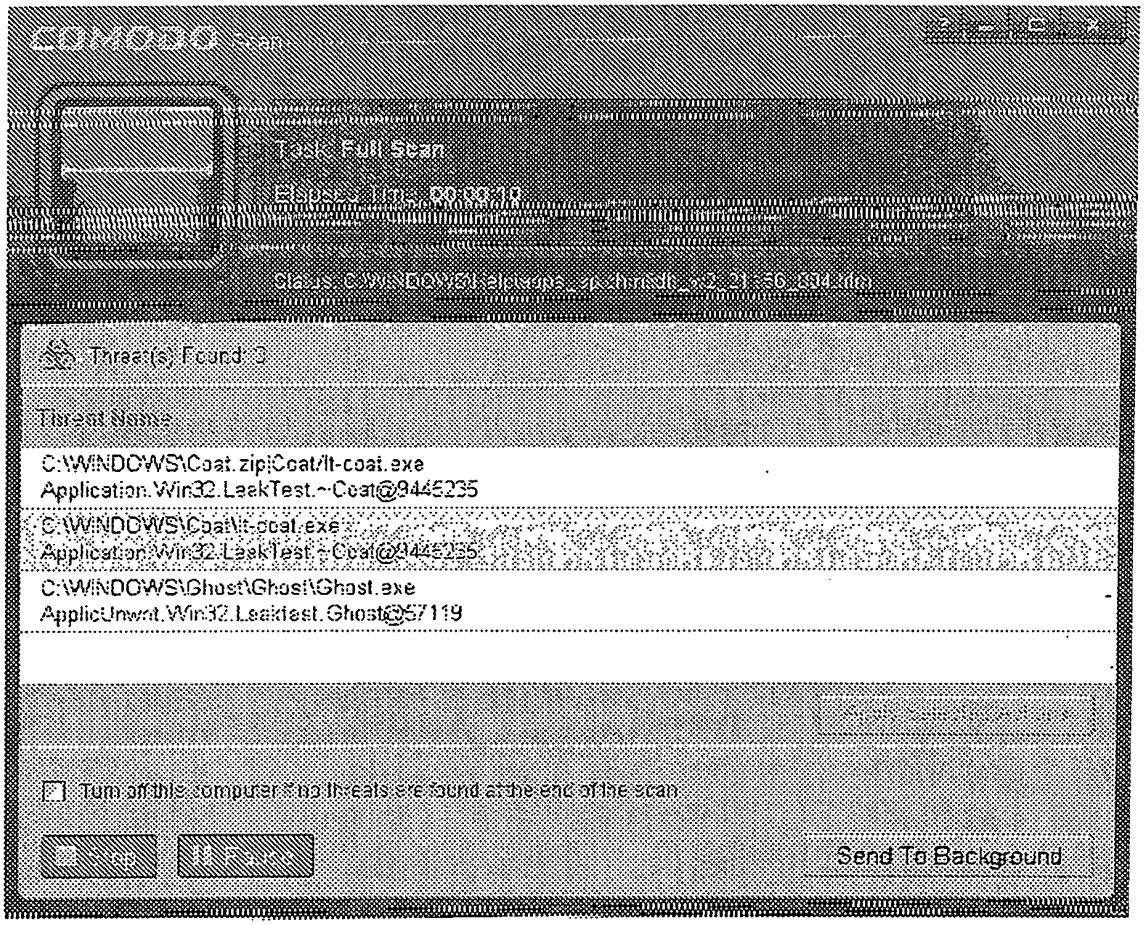
- Click 'Scan' from the General Tasks interface the click 'Full System Scan' from the 'Scan' interface.



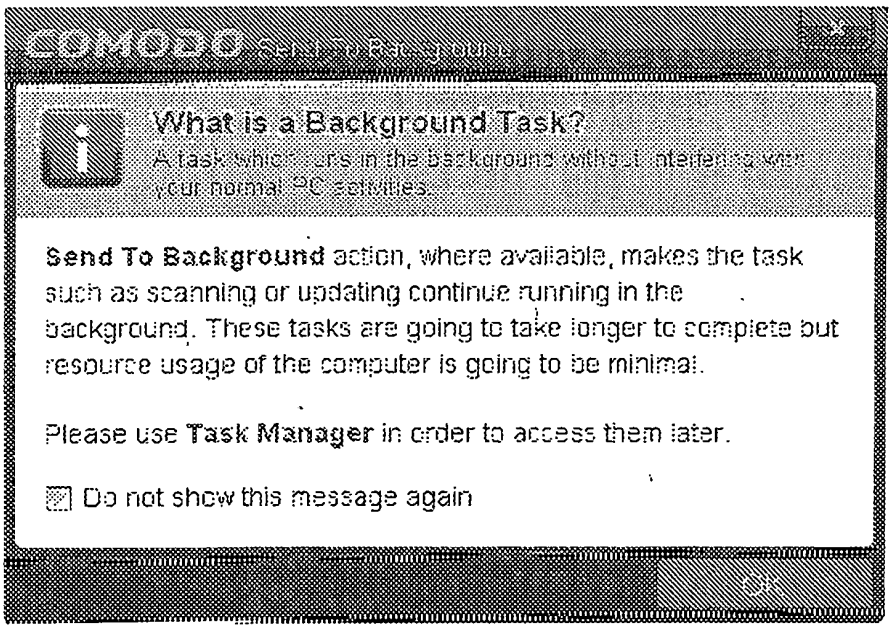
The scanner will start and first check whether your virus signature database is up-to-date.



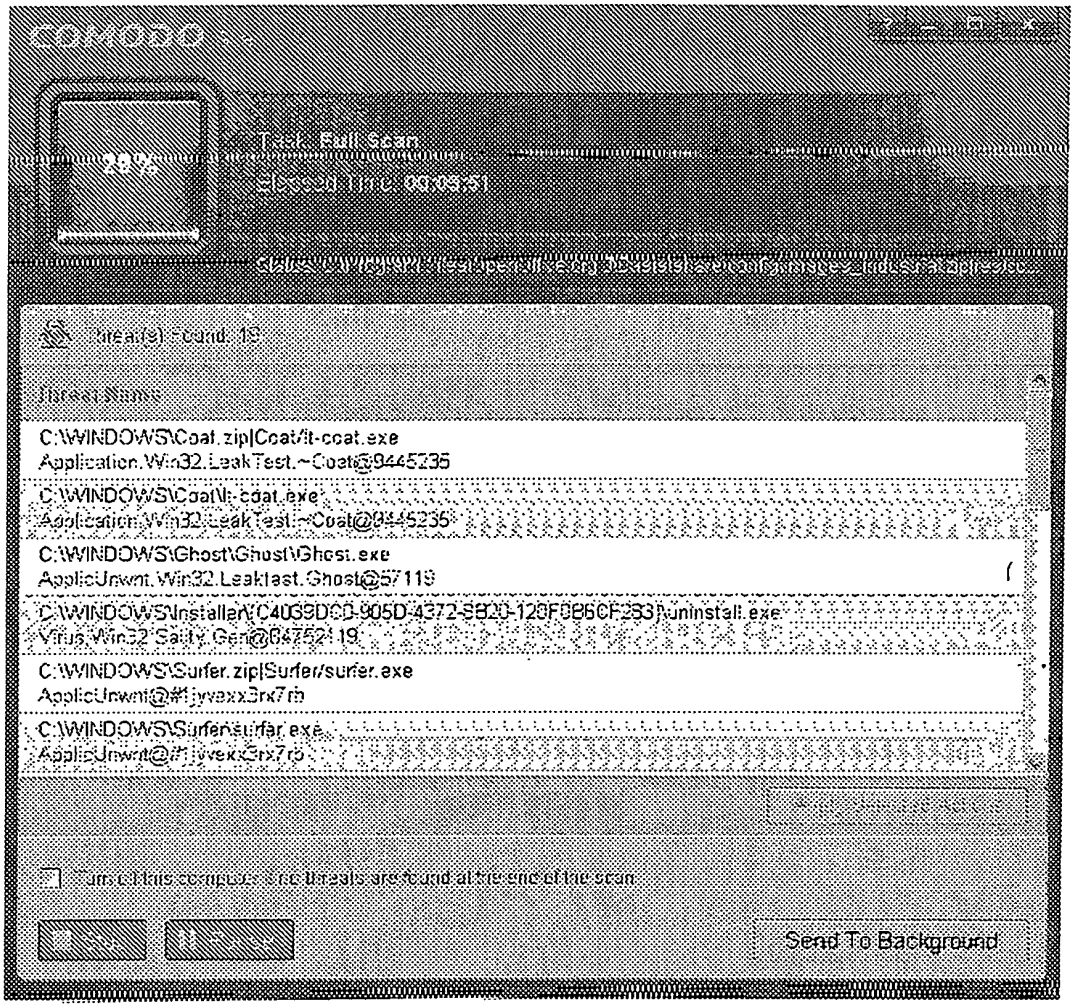
If the database is outdated, CIS will first download and install the latest database before commencing the scan.



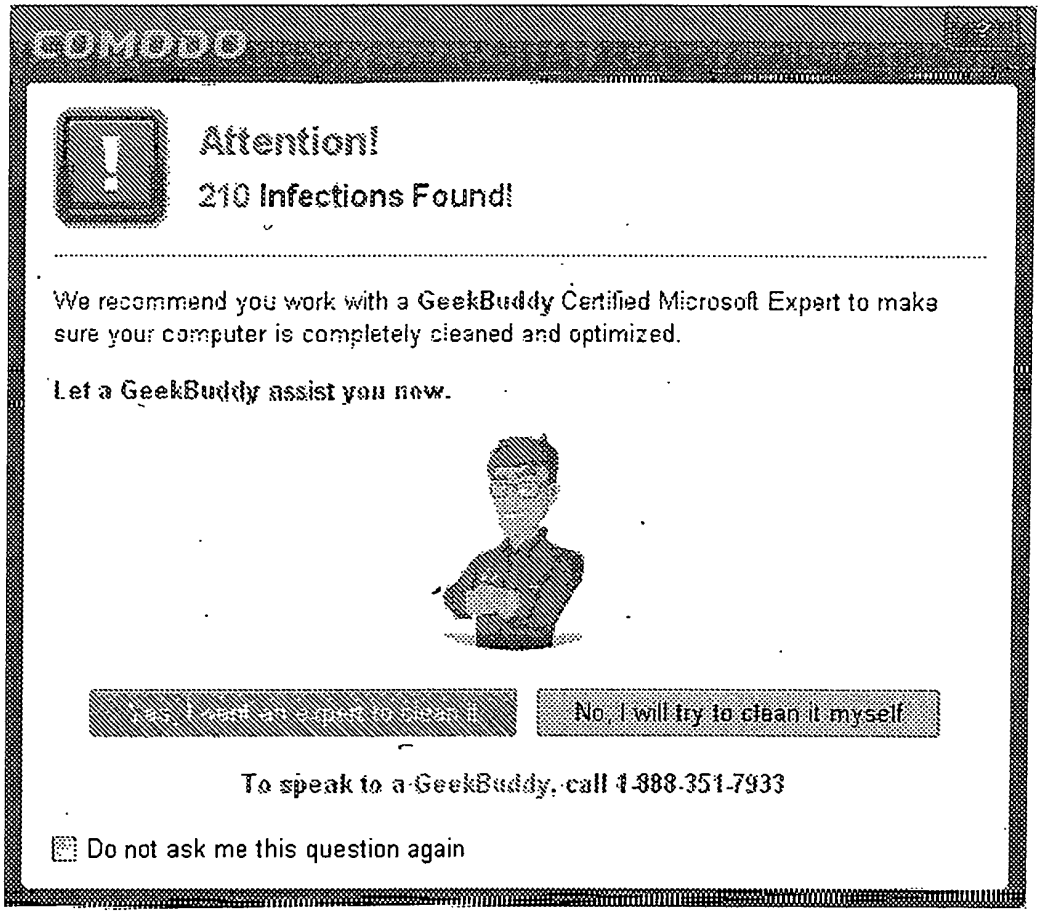
- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



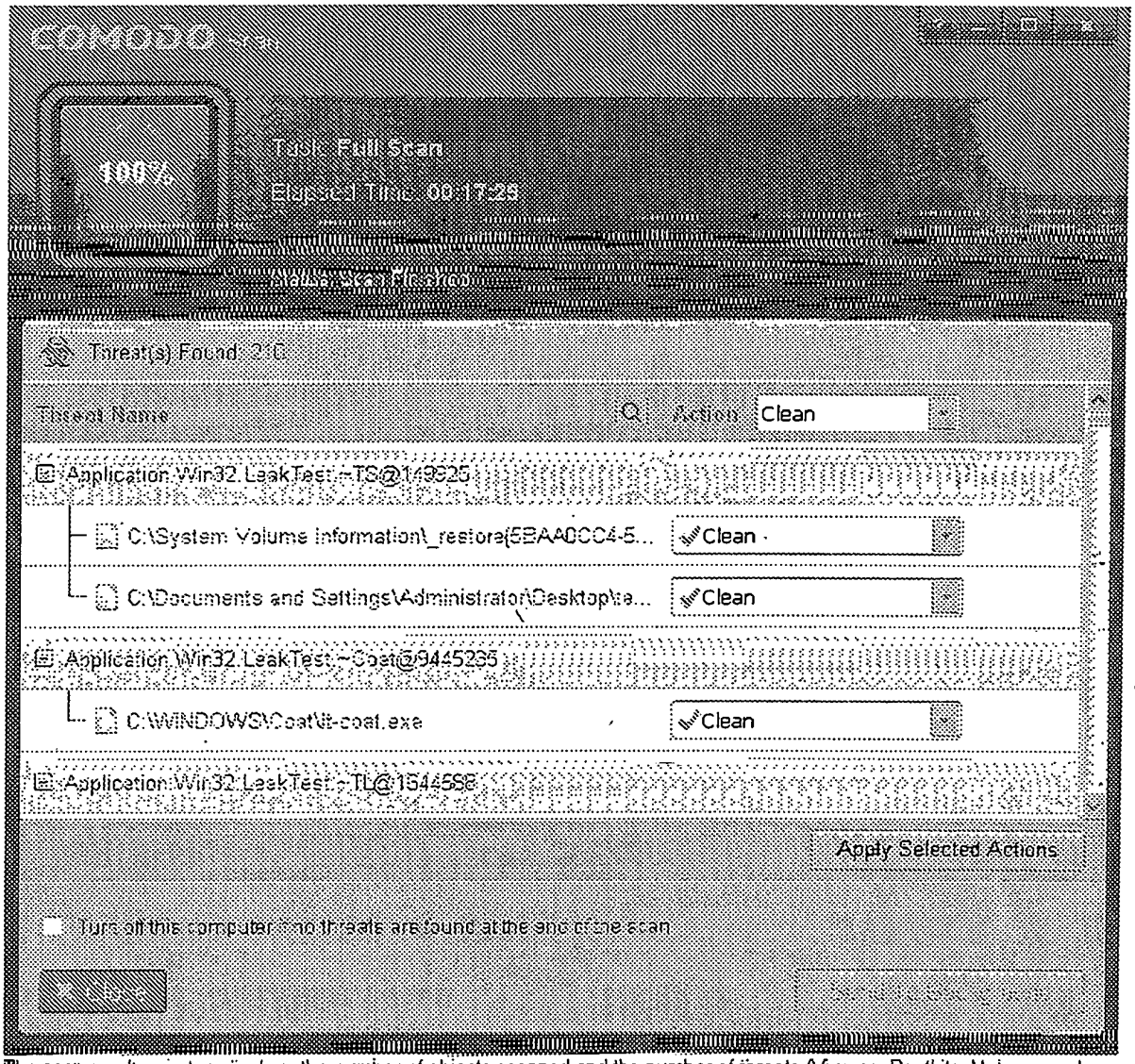
If you send to the background, you can continue to check scan progress by clicking 'Task Manager' on the home screen or by clicking 'Open Task Manager' icon from the 'Advanced Tasks' interface.



- Any detected threats will be displayed in full at the end of the scan. The alert will tell you how many threats were found; the name and location of the threats and will provide you with virus removal options:



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



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

2.1.3. Run a Rating Scan

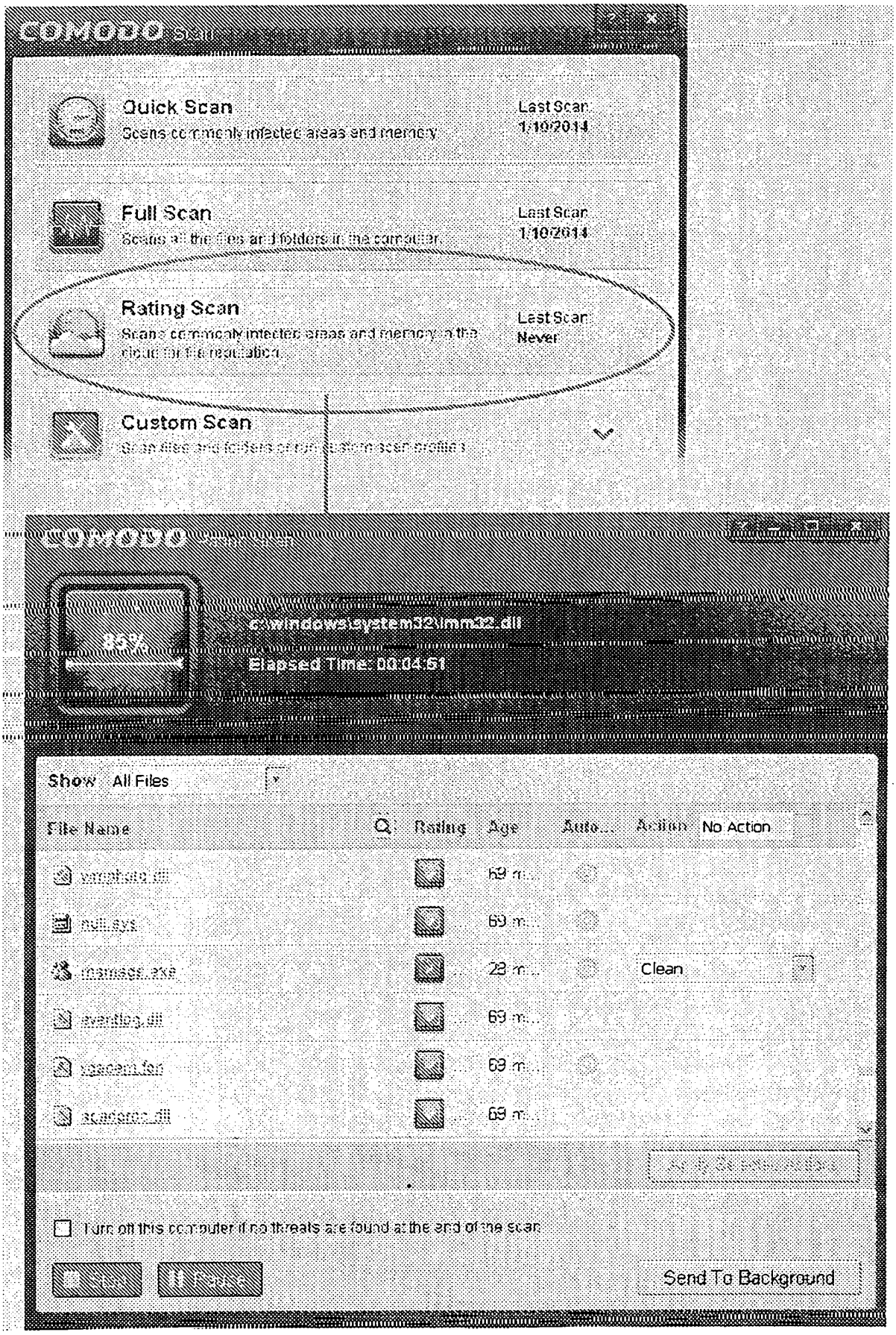
The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

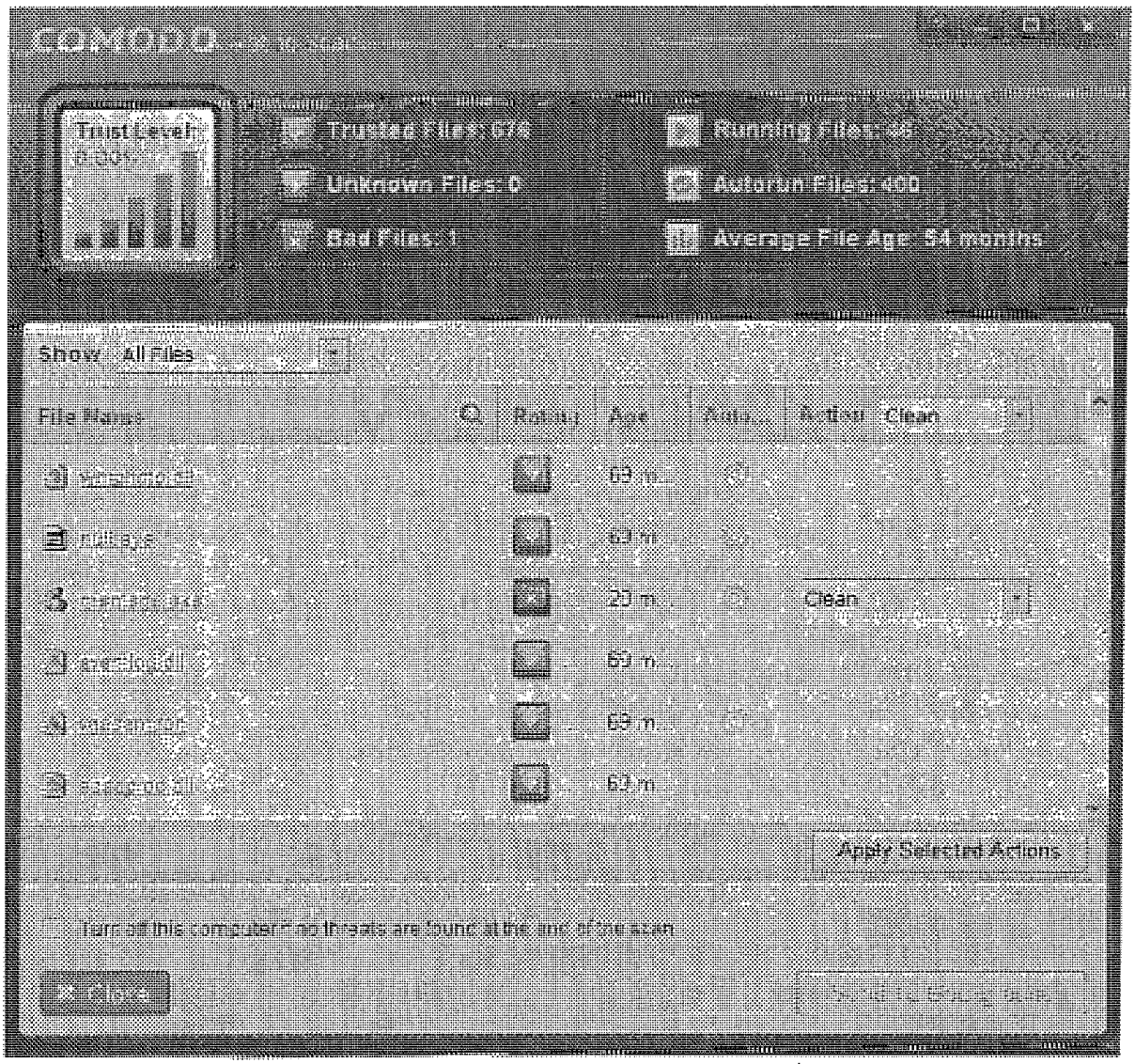
- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Bad - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

To run a Rating scan

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

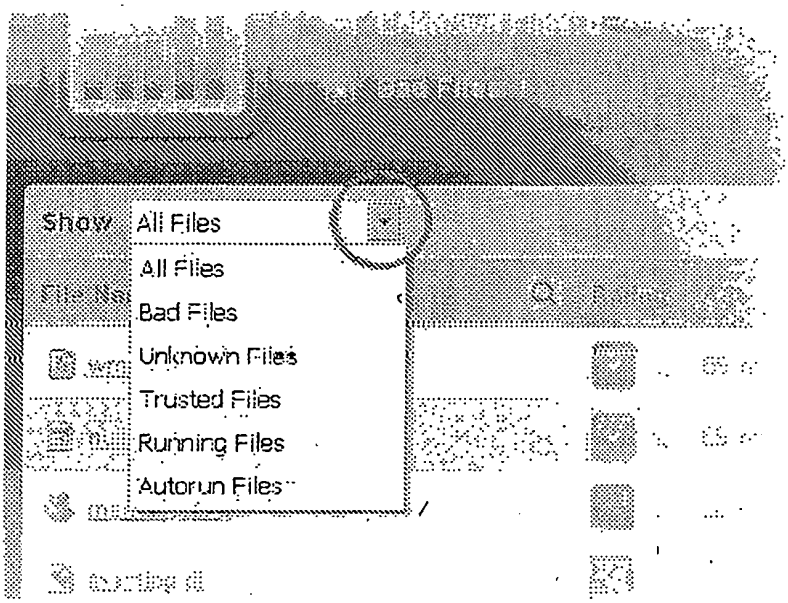


After the cloud scanners have finished their analysis, file ratings will be displayed as follows:

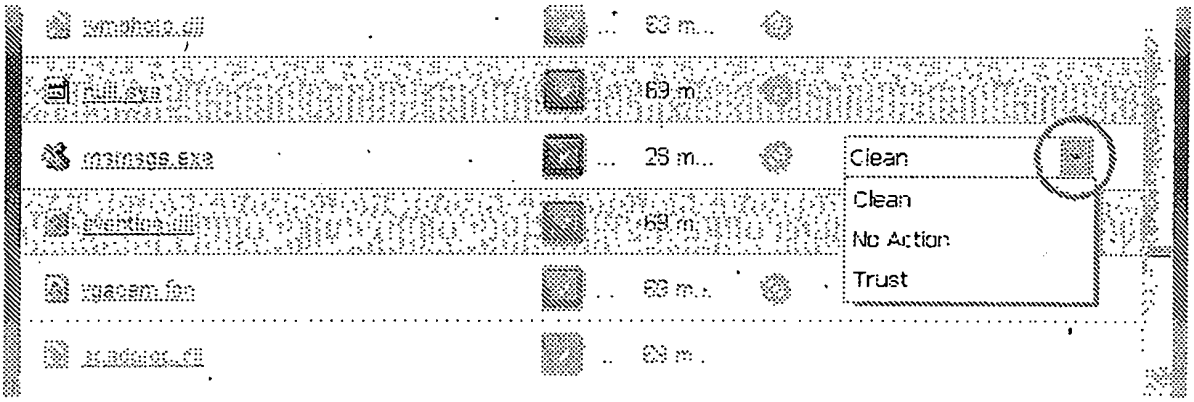


- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your computer
- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous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

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

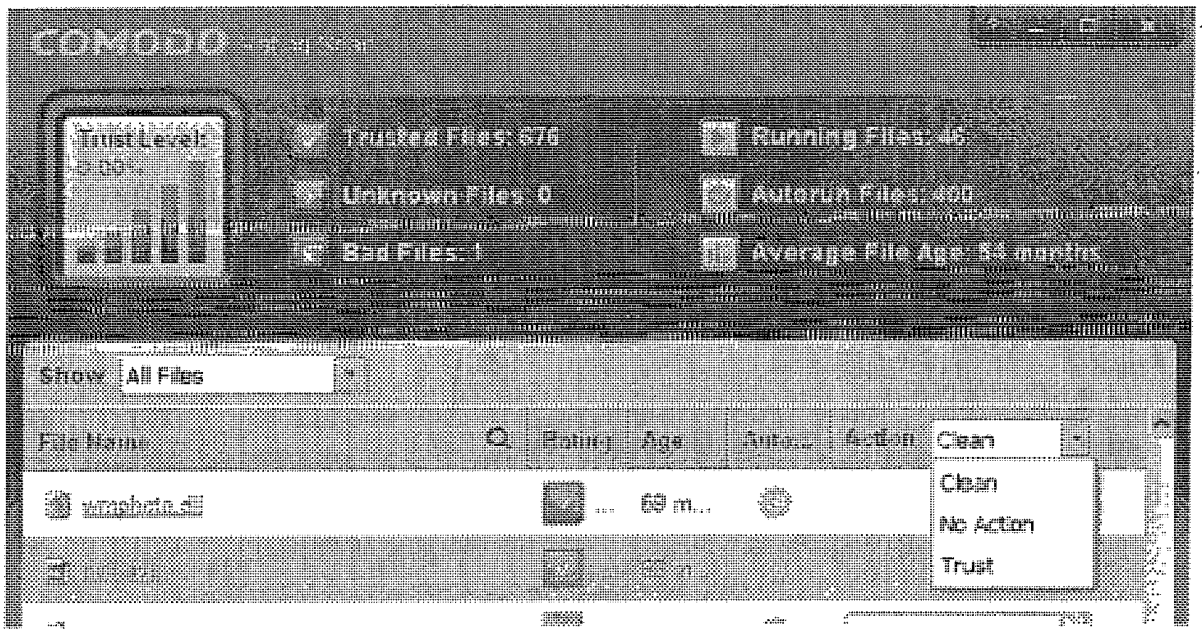


Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

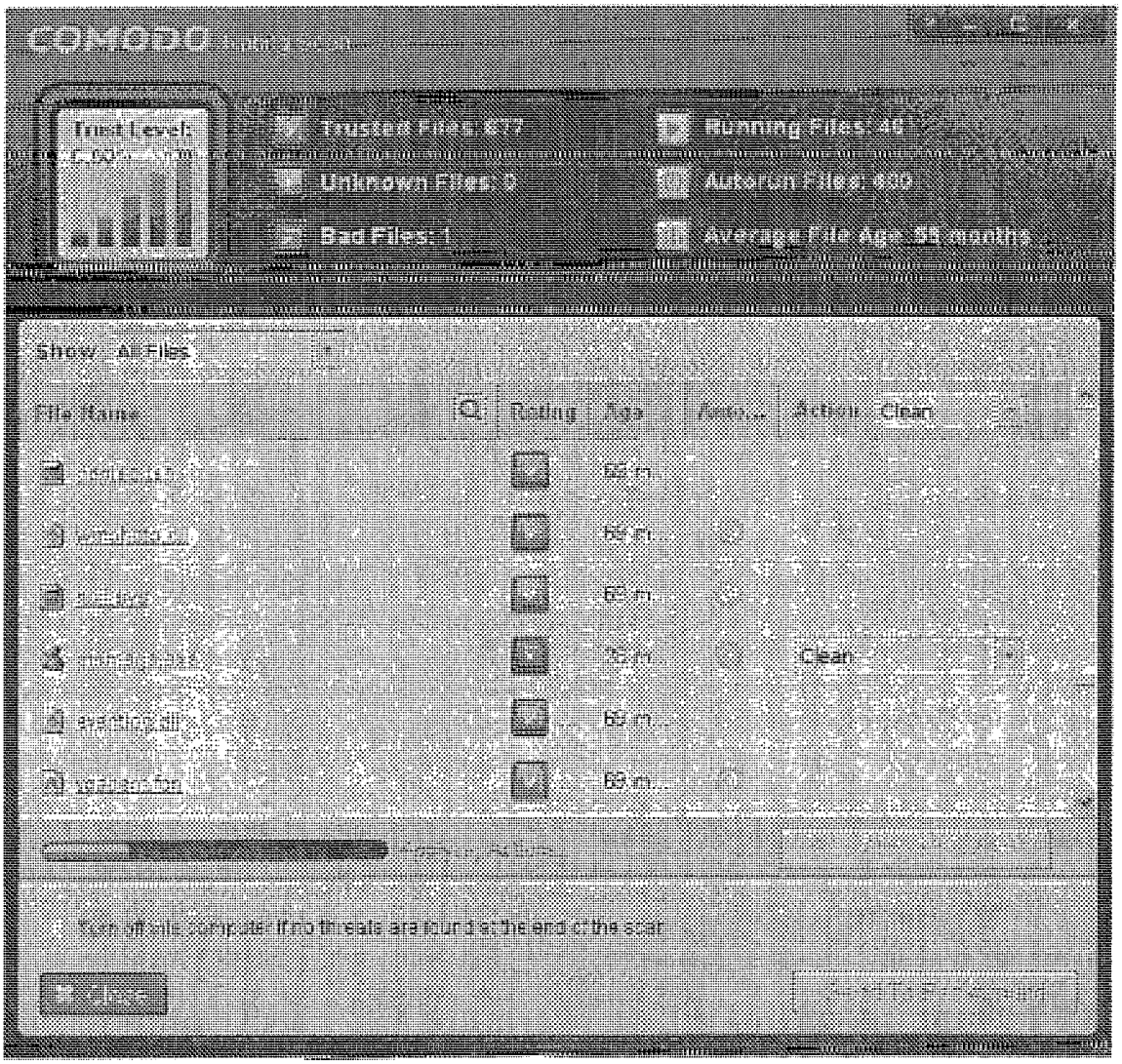


- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See Manage Quarantined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

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



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

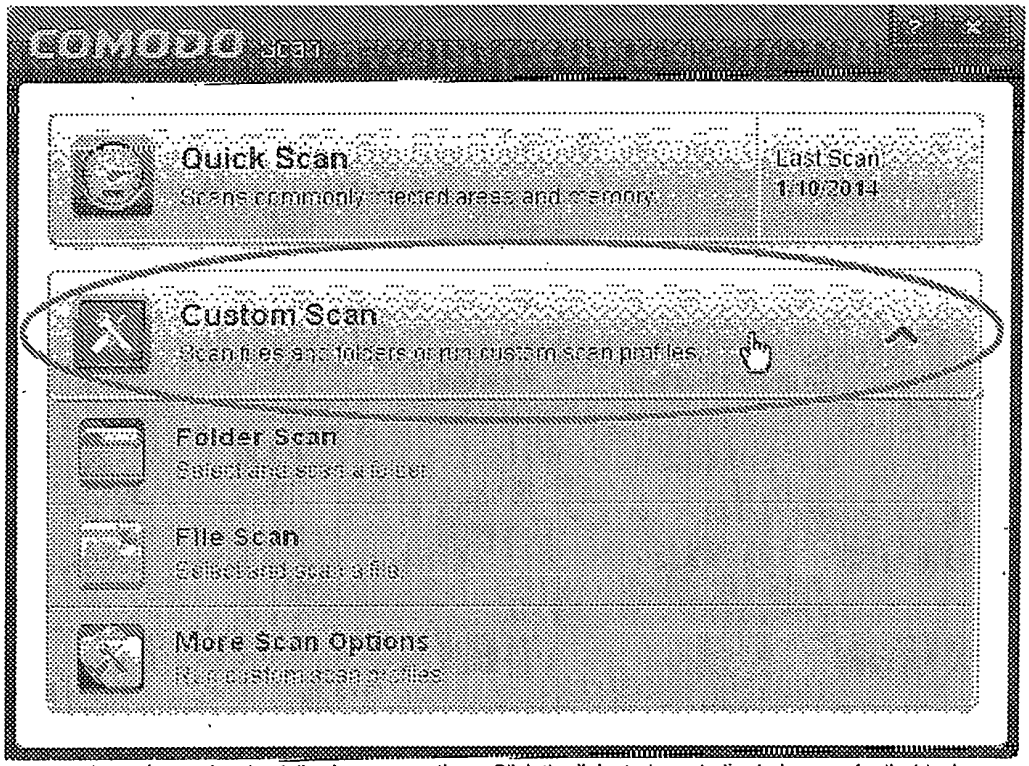


- Click 'Close' to exit.

2.1.4. Run a Custom Scan

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

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



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

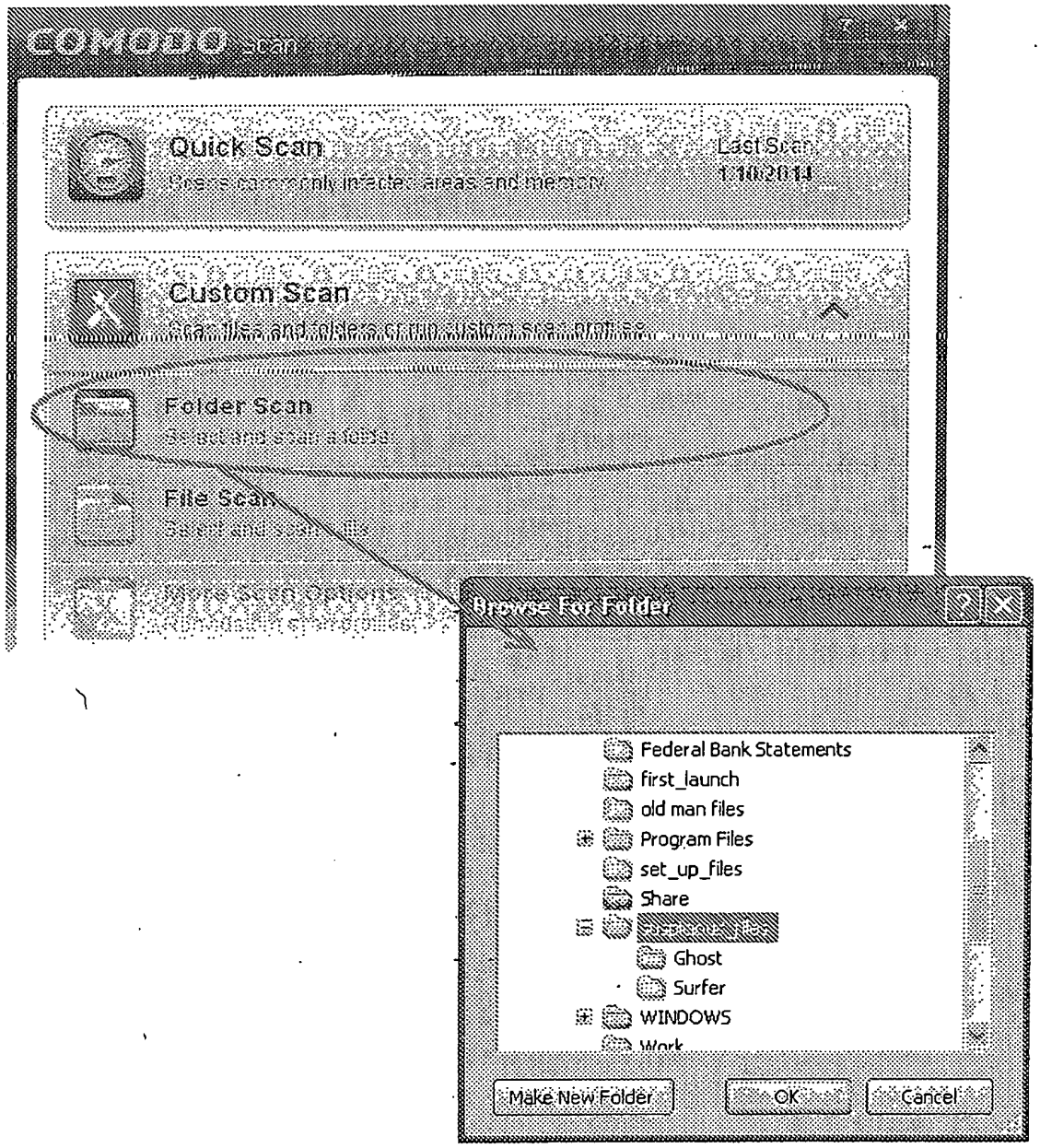
- Folder Scan - scan individual folders
- File Scan - scan an individual file
- More Scan Options - create a custom scan profile here

2.1.4.1. Scan a Folder

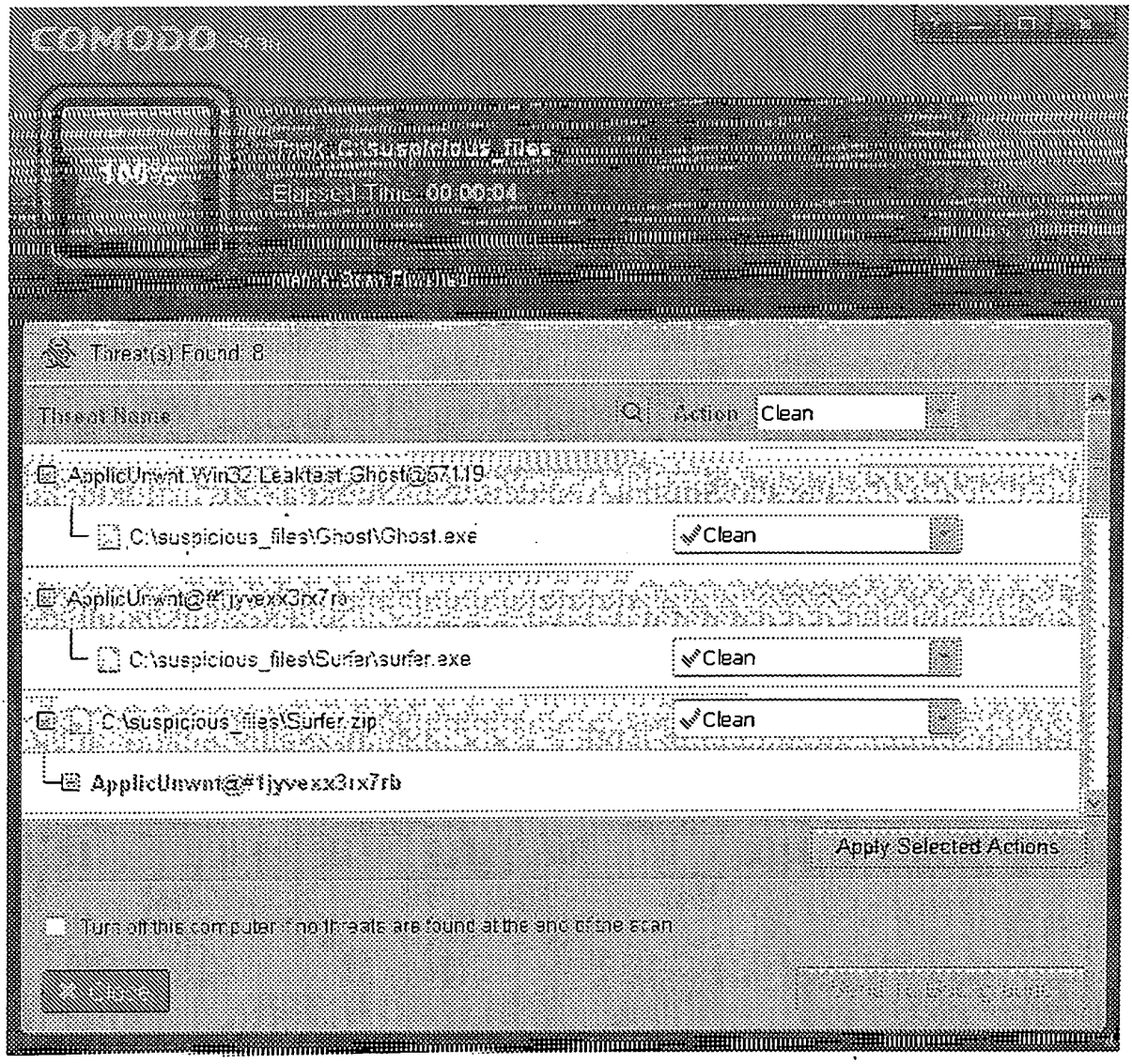
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan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

To scan a specific folder

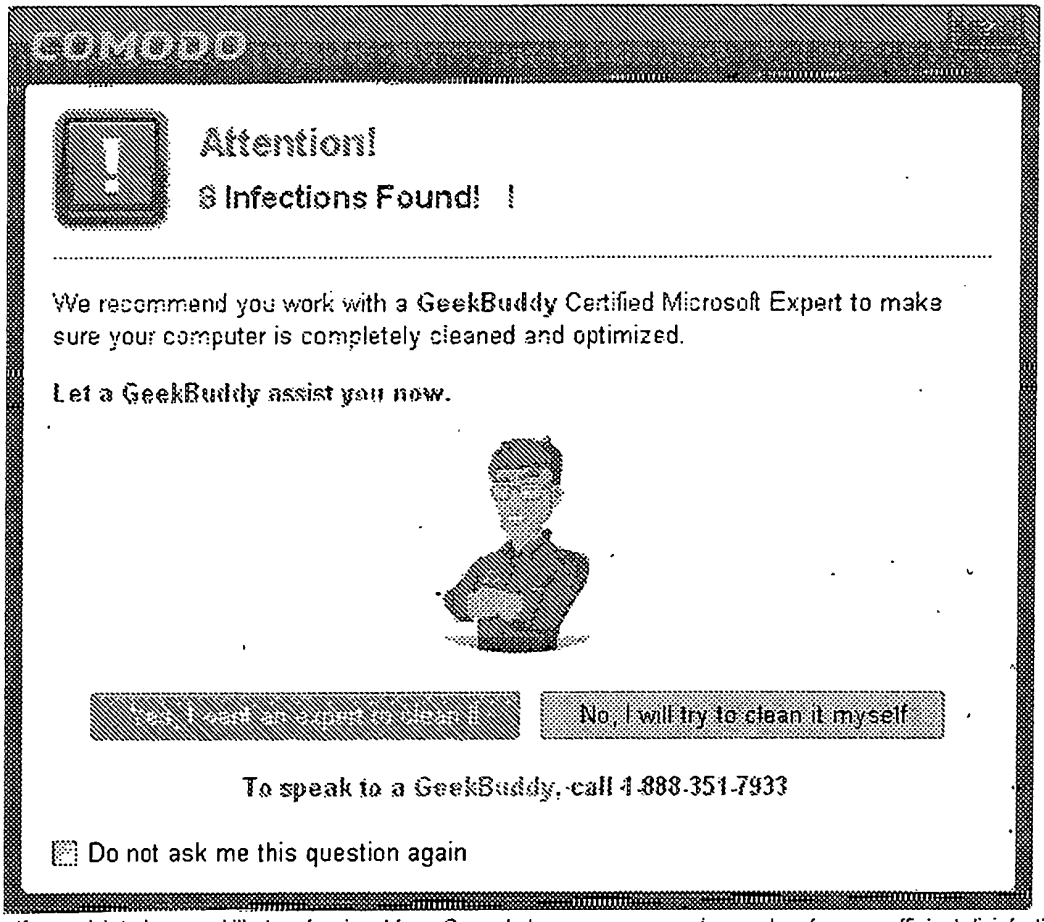
- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'Folder Scan' from the 'Custom Scan' pane
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click OK.



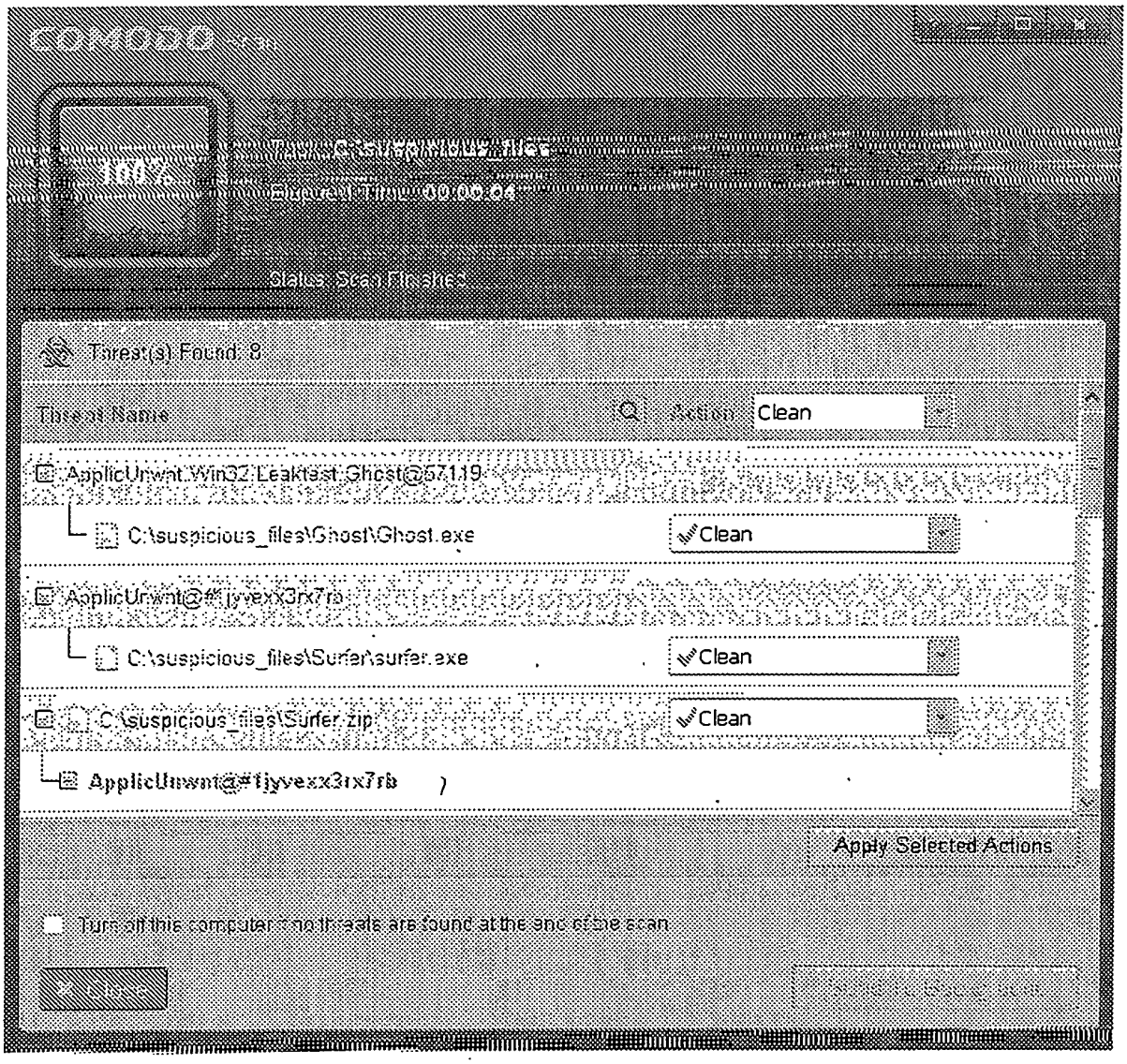
The folder will be scanned instantly and the results will be displayed with a list of any identified infections



- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
  - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



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

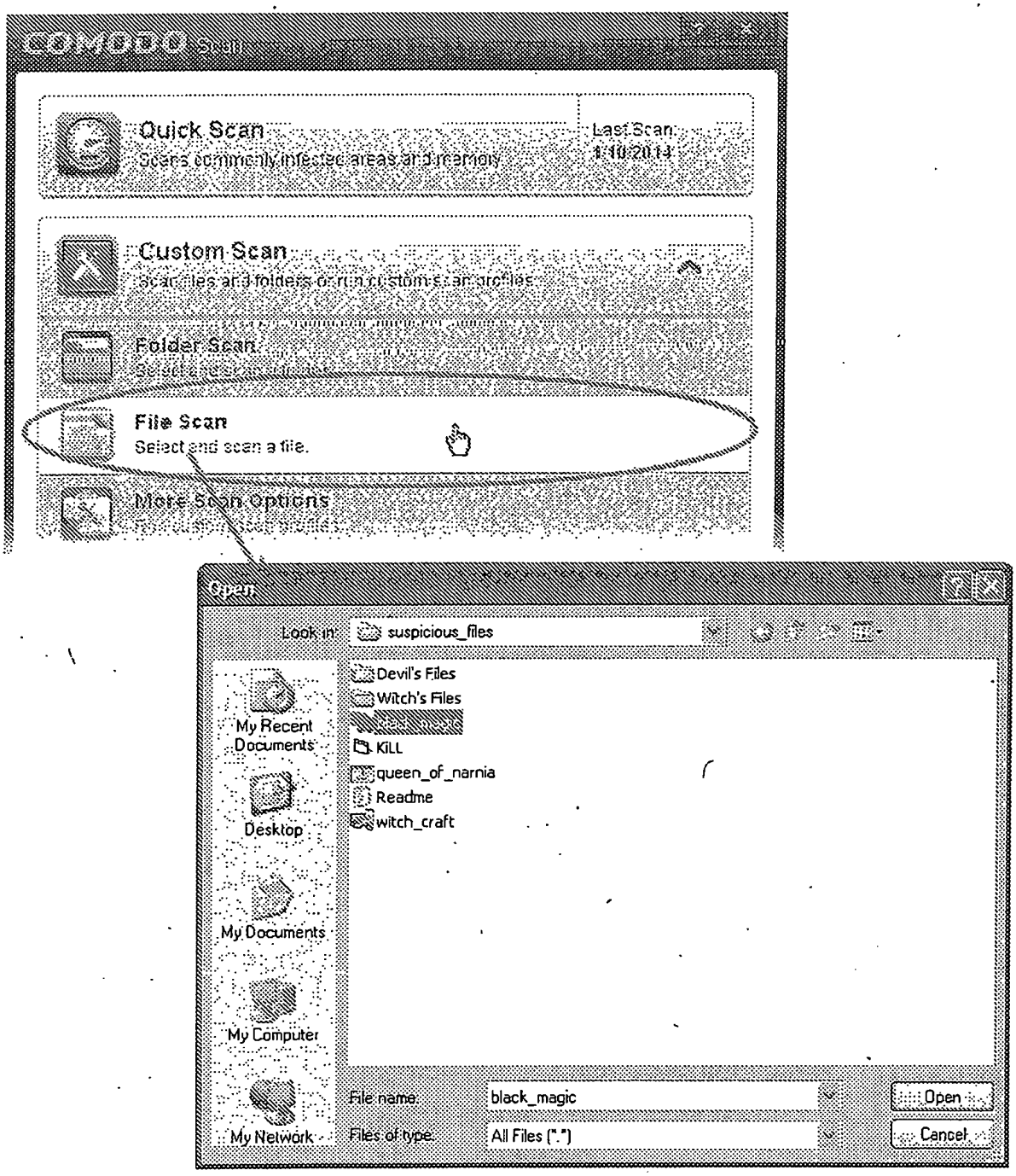
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CIS interface or by right clicking it. Refer to Scan Individual File/Folder for more details.

2.1.4.2. Scan a File

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

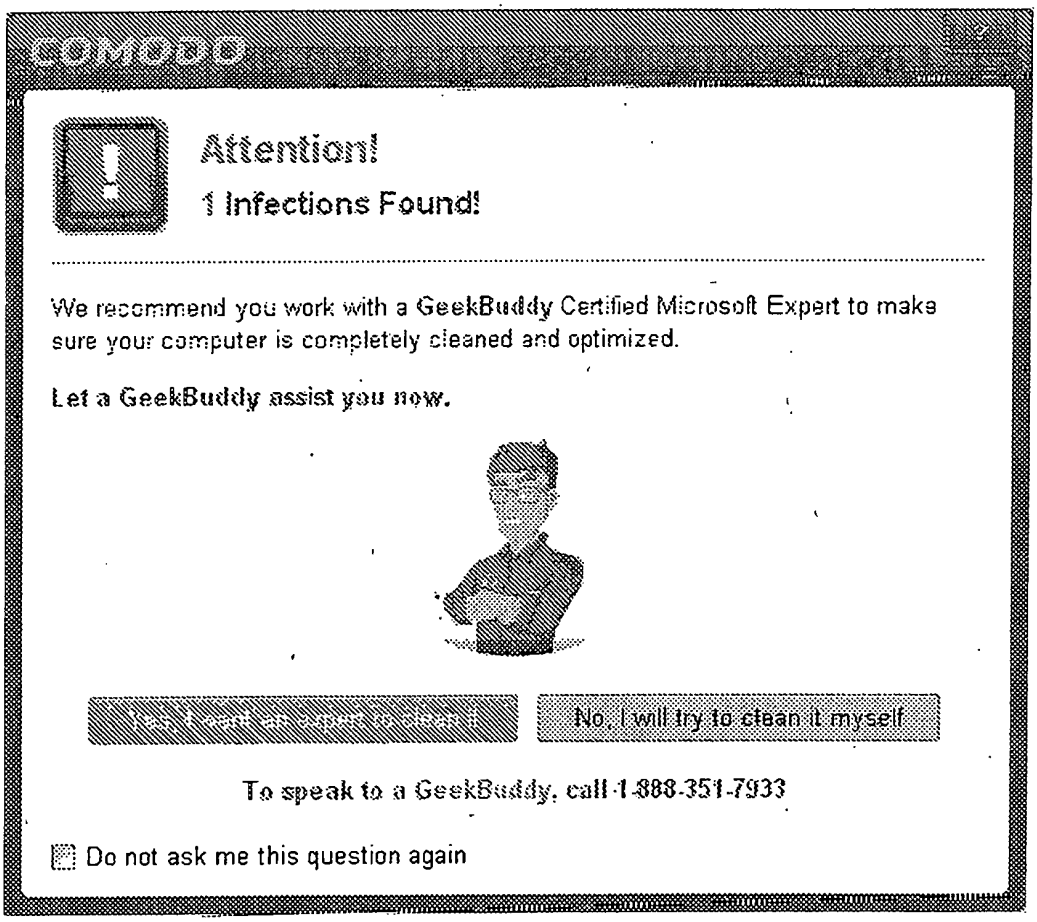
To scan a specific file

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

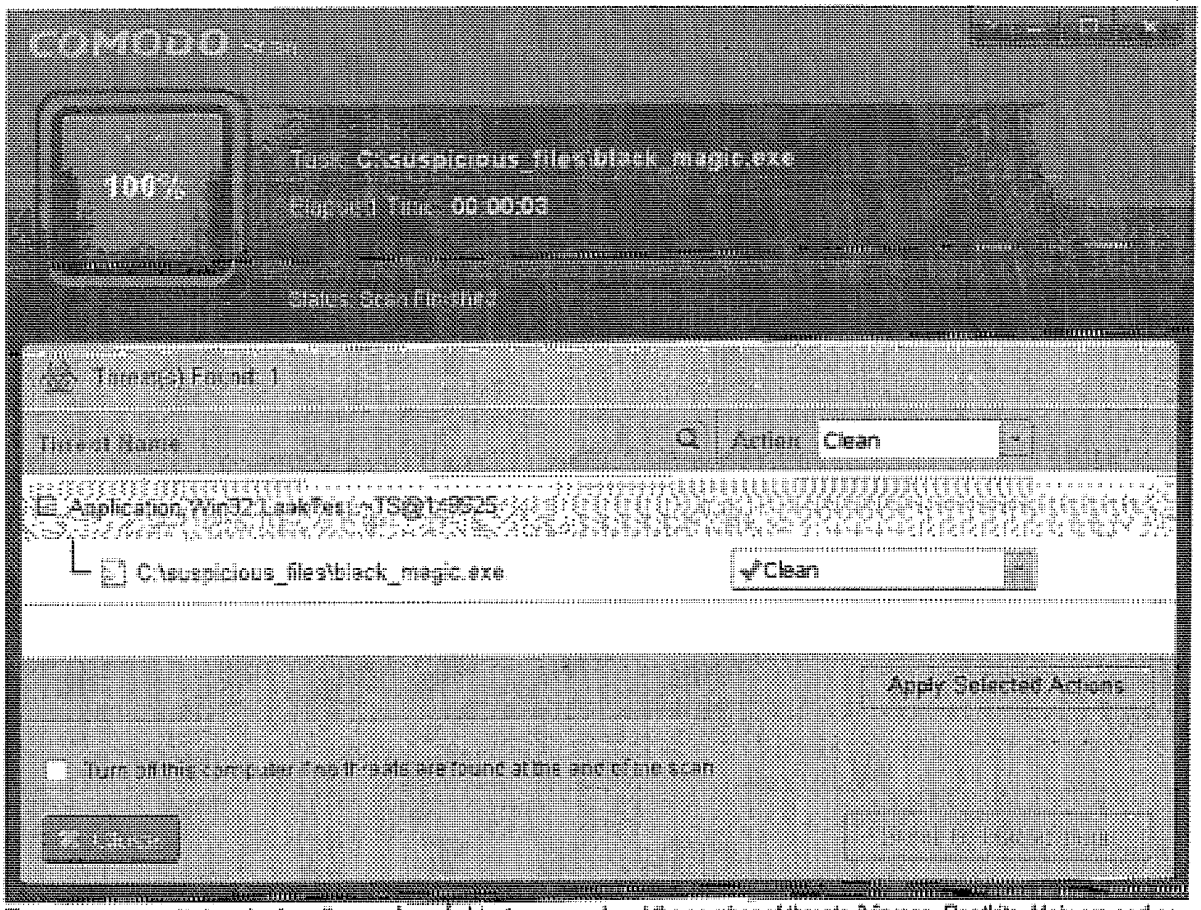


The file will be scanned instantly.

- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



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

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

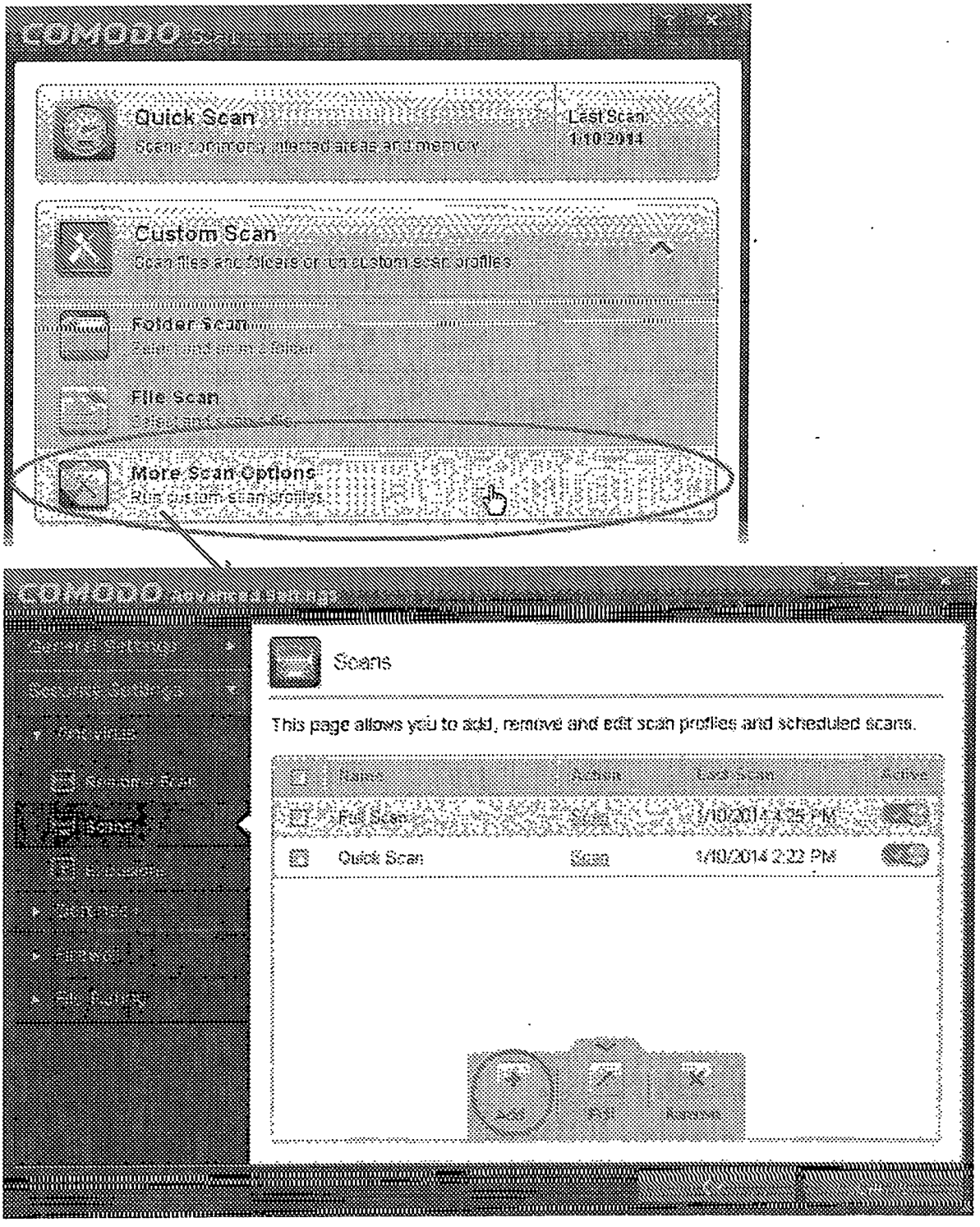
2.1.4.3. Create, Schedule and Run a Custom Scan

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

- Creating a Scan Profile
- Running a custom scan

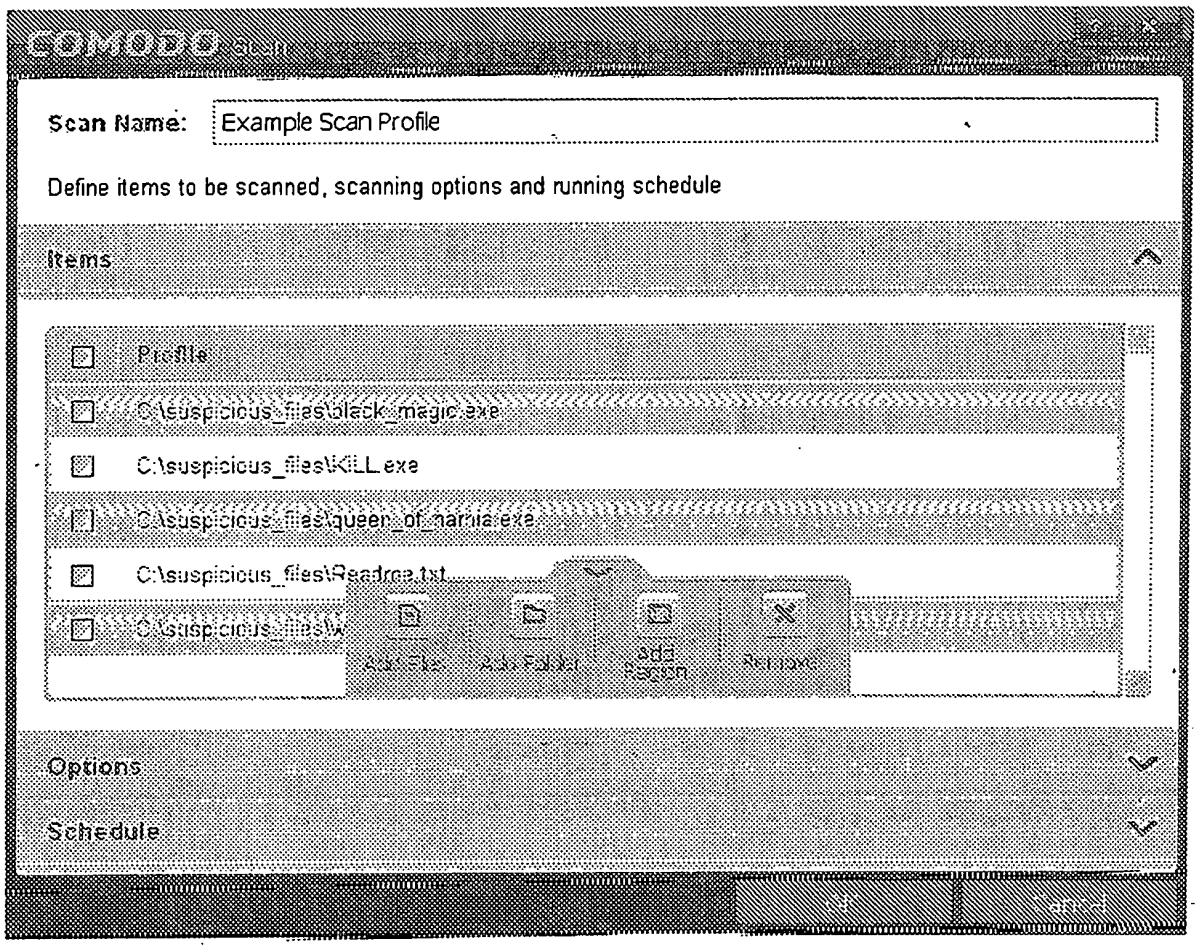
To create a custom profile

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

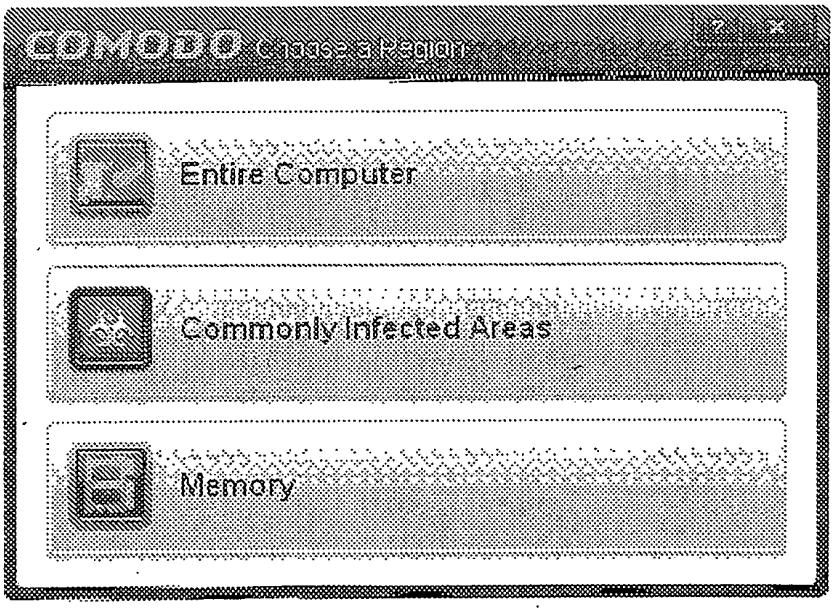


The scan profile interface will be displayed.

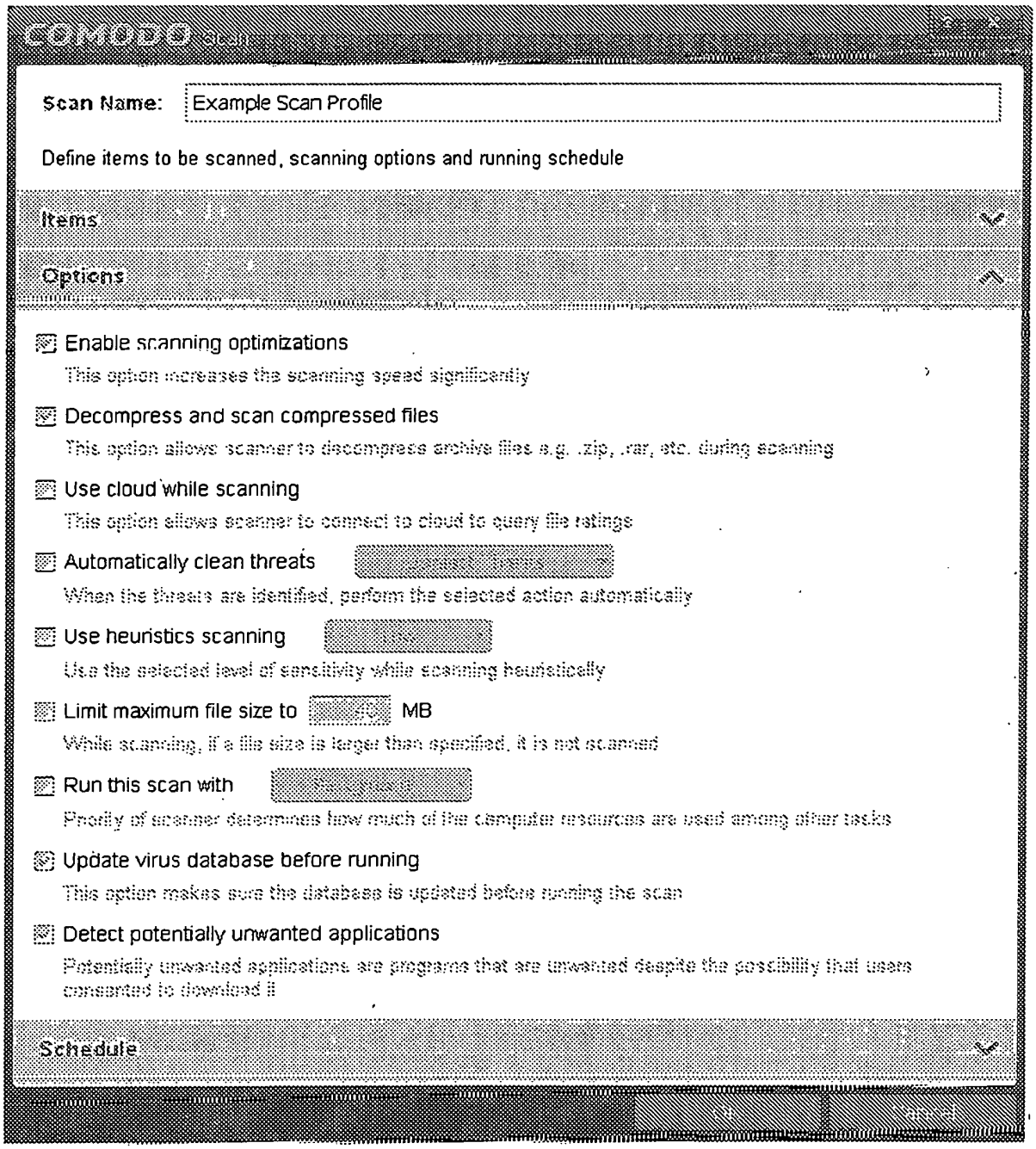
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:



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



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



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

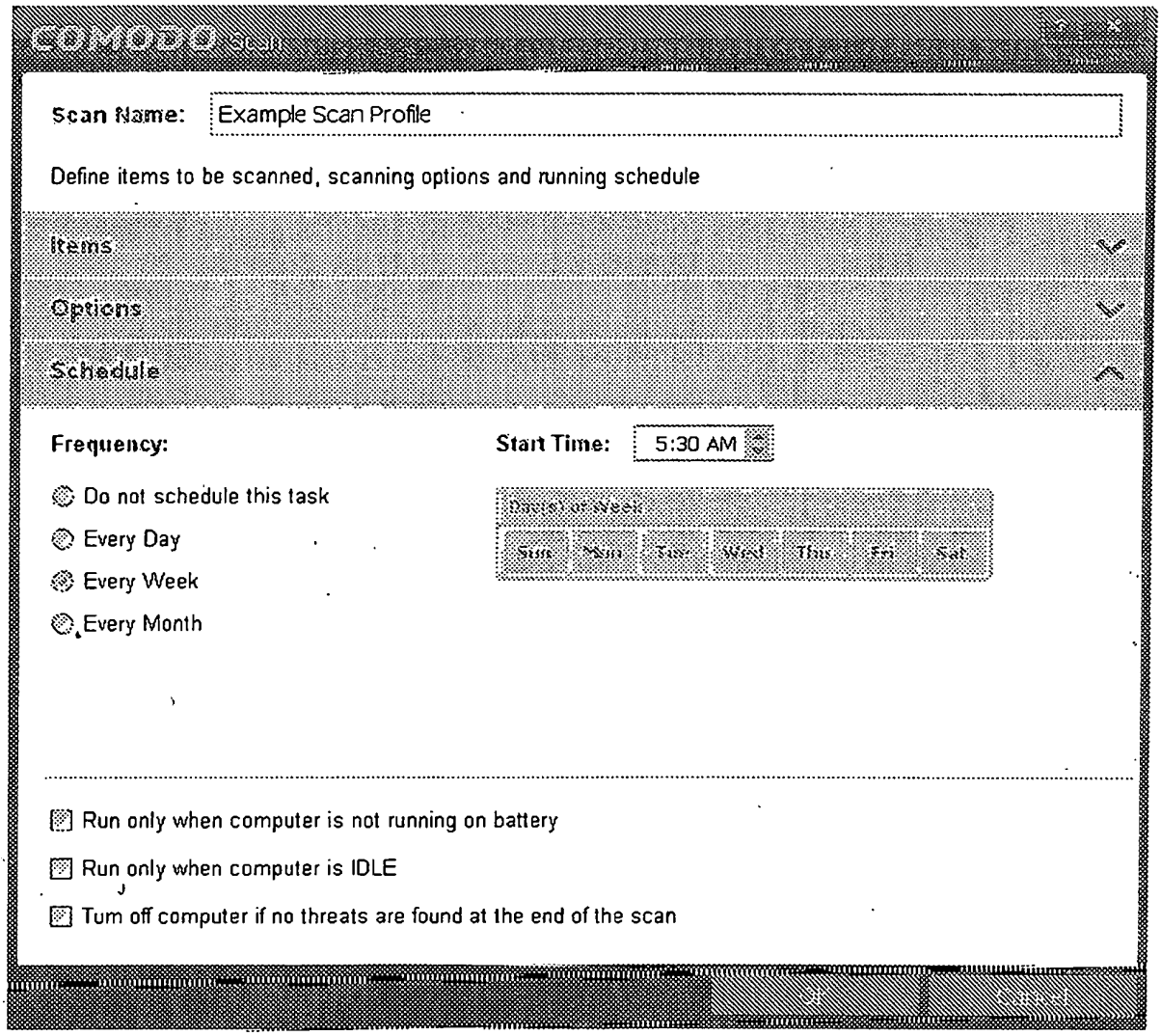
Background Info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so 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 *(Default = Enabled)*.

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

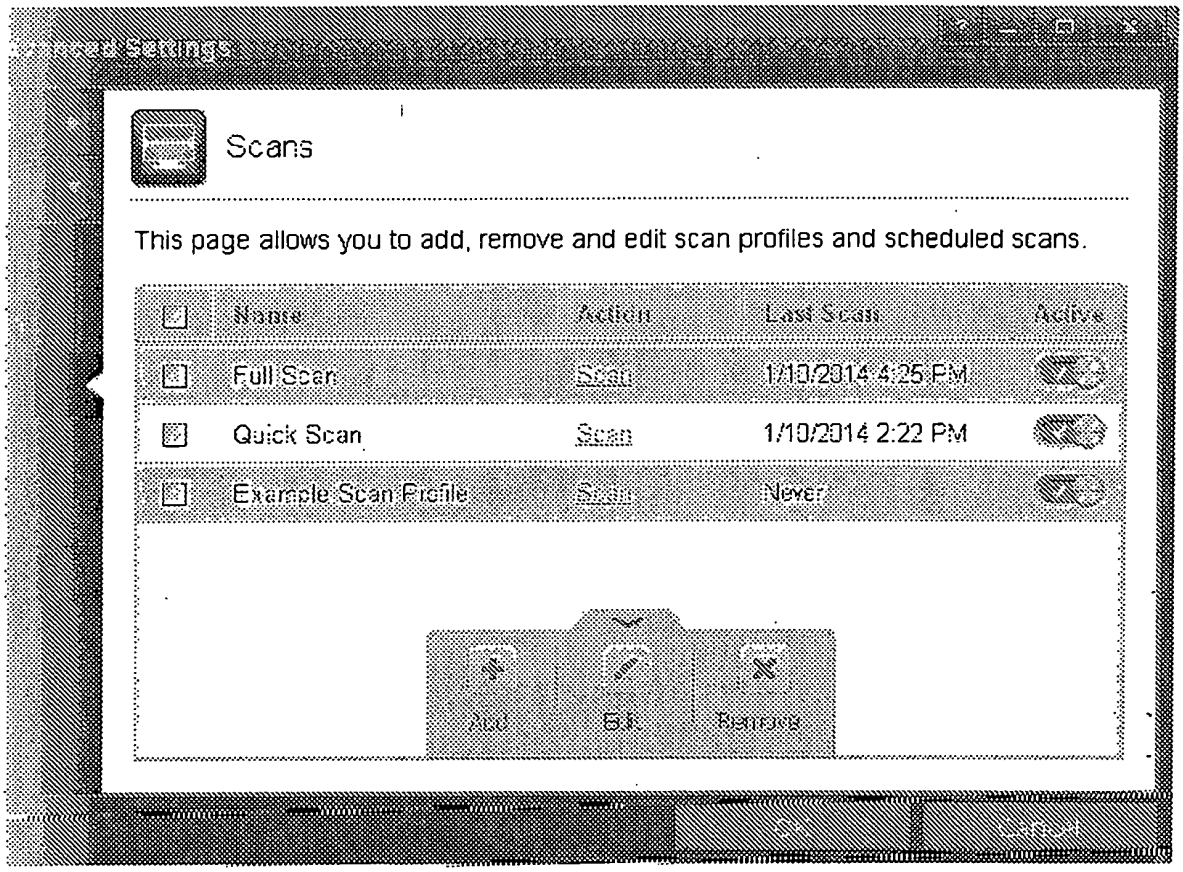


- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - The Antivurus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field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

- Click OK to save the profile.

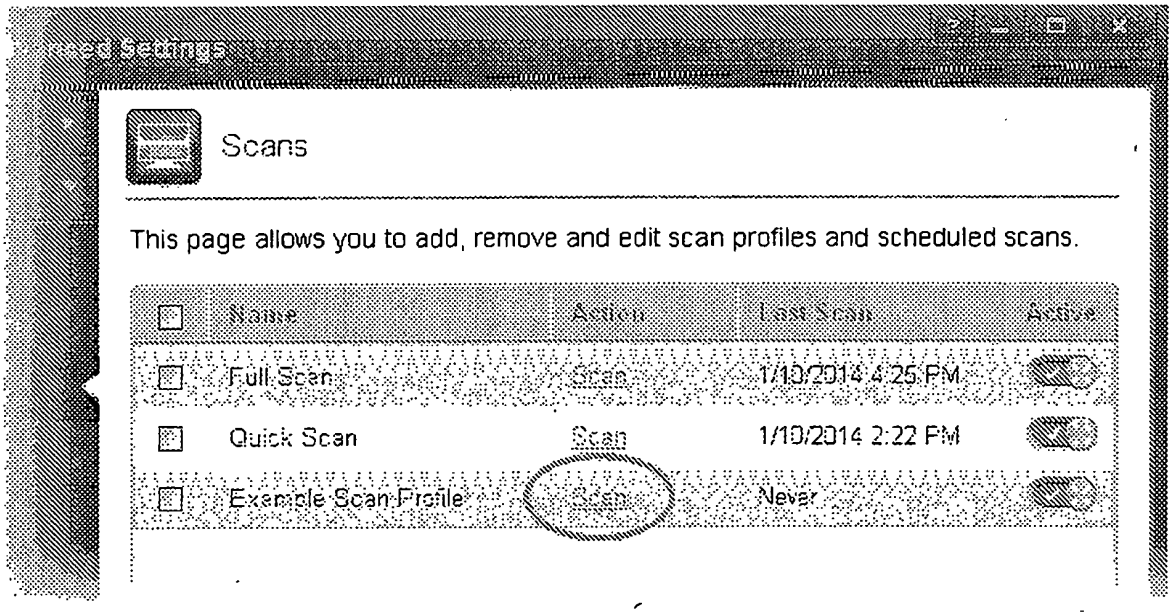
Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.

The profile will be available for deployment in future.



To run a custom scan

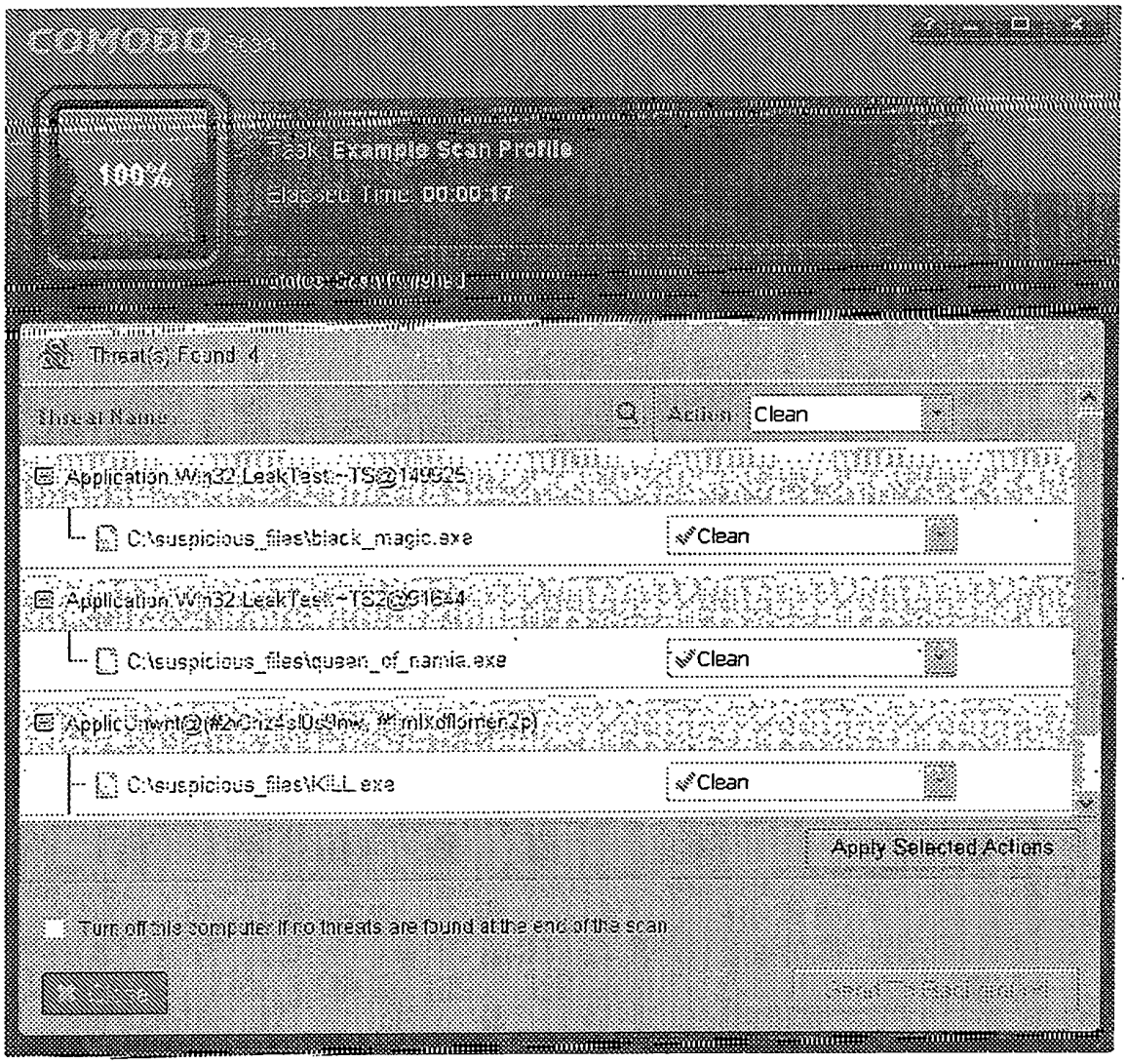
- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click 'Scan' beside the required scan profile.



- The scan will be started.
- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes; I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
  - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



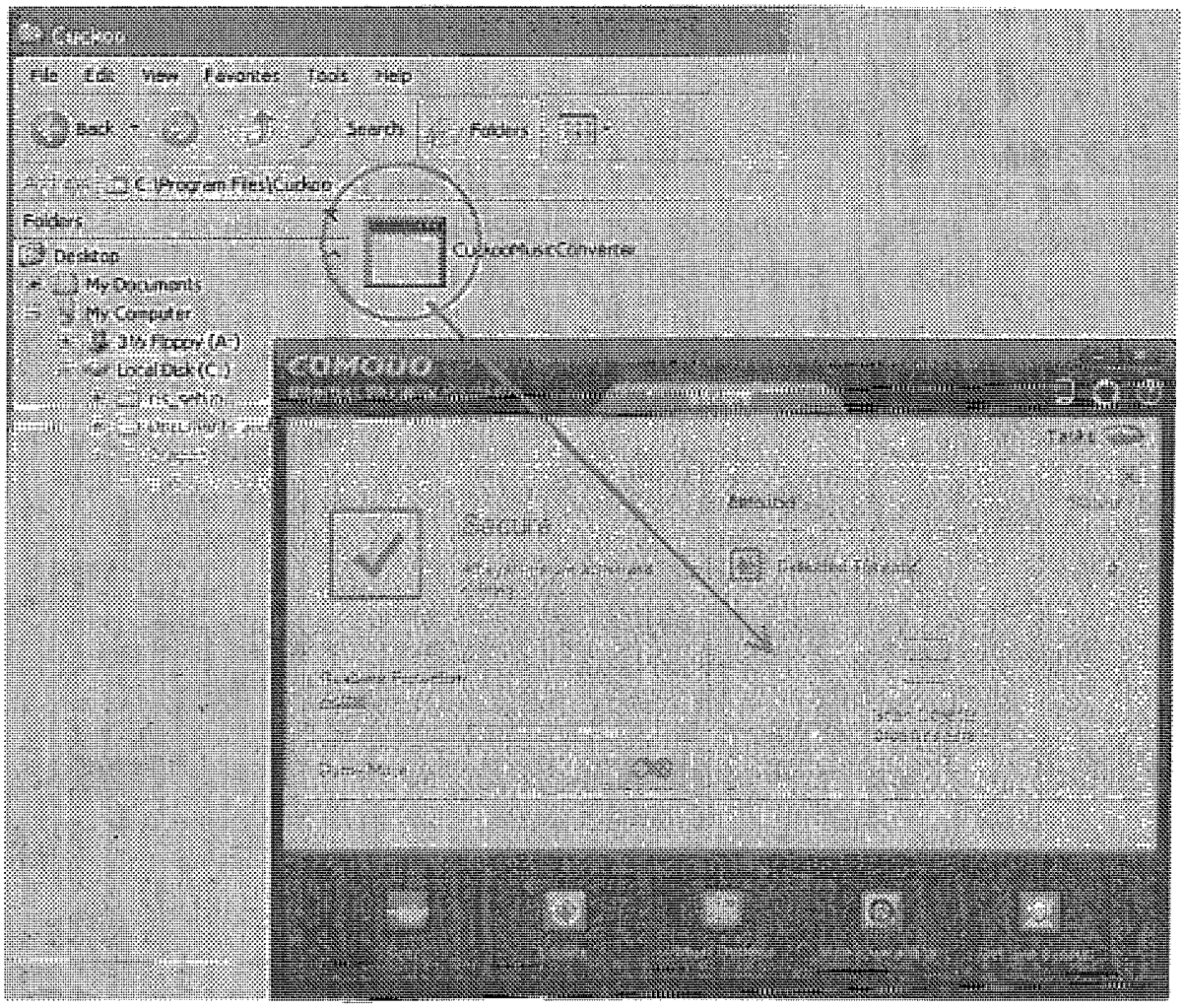
- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

2.2. Instantly Scan Files and Folders

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

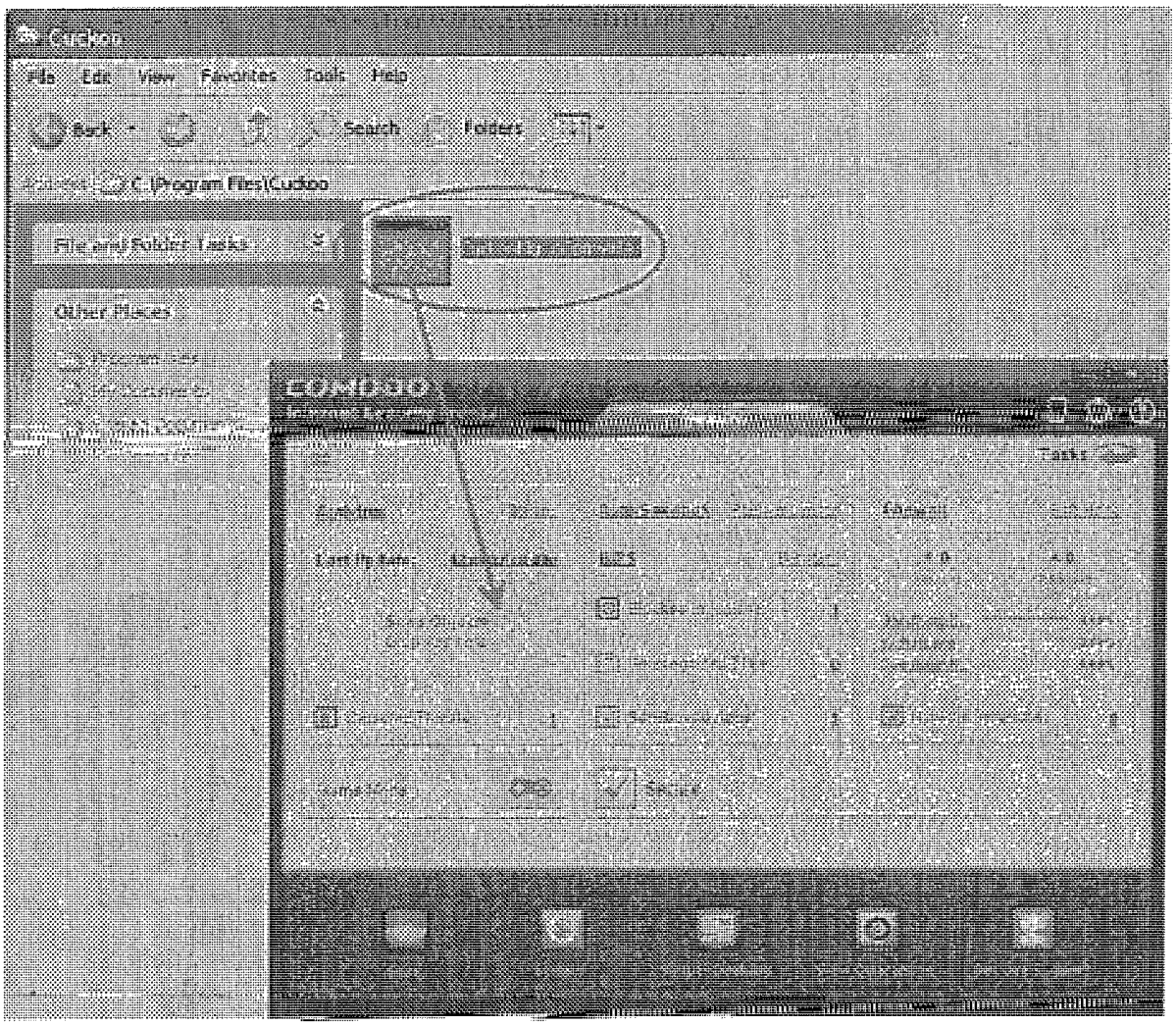
To instantly scan an item

- Click the Antivirus tile at the 'Home' screen in compact view to flip-open the Antivirus pane
- Drag and drop the item over the area marked 'Scan Objects'.



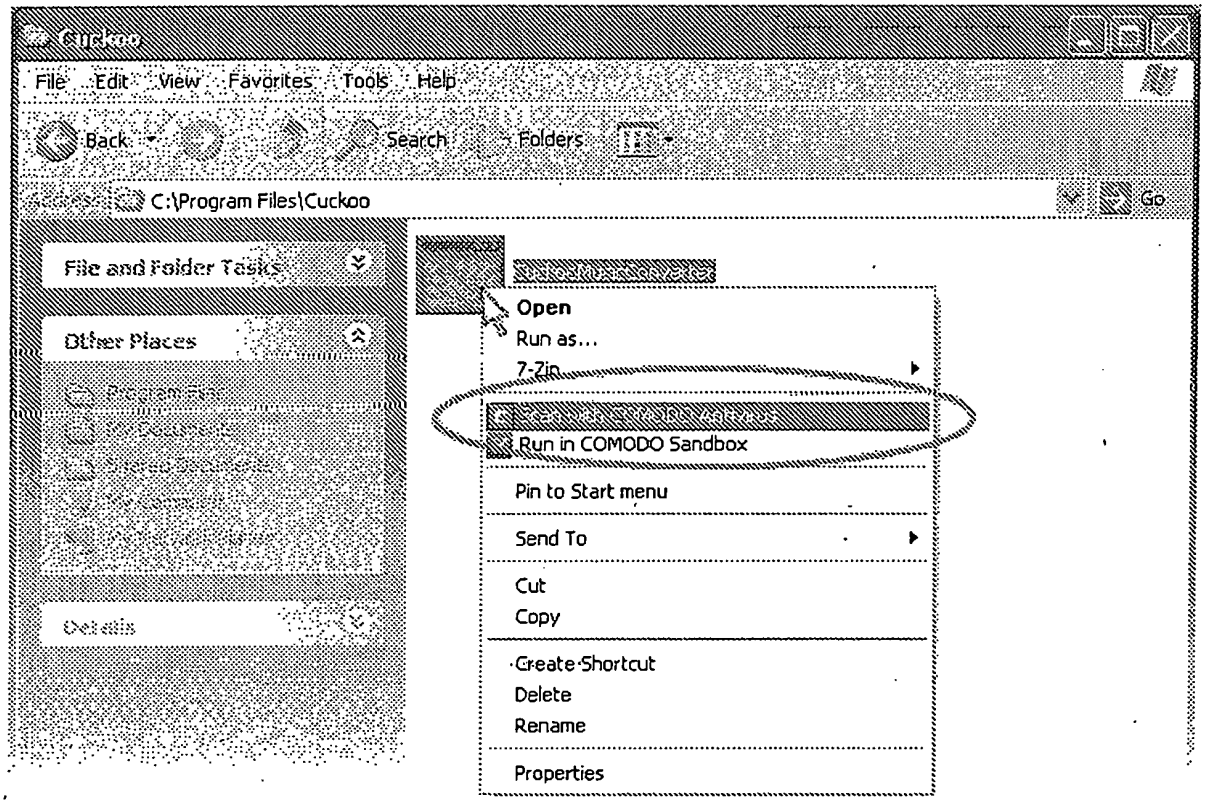
OR

- Switch to 'Advanced' View of the 'Home' screen by clicking the button at the top left of the home screen.
- Drag and drop the item over the area marked 'Scan Objects'.

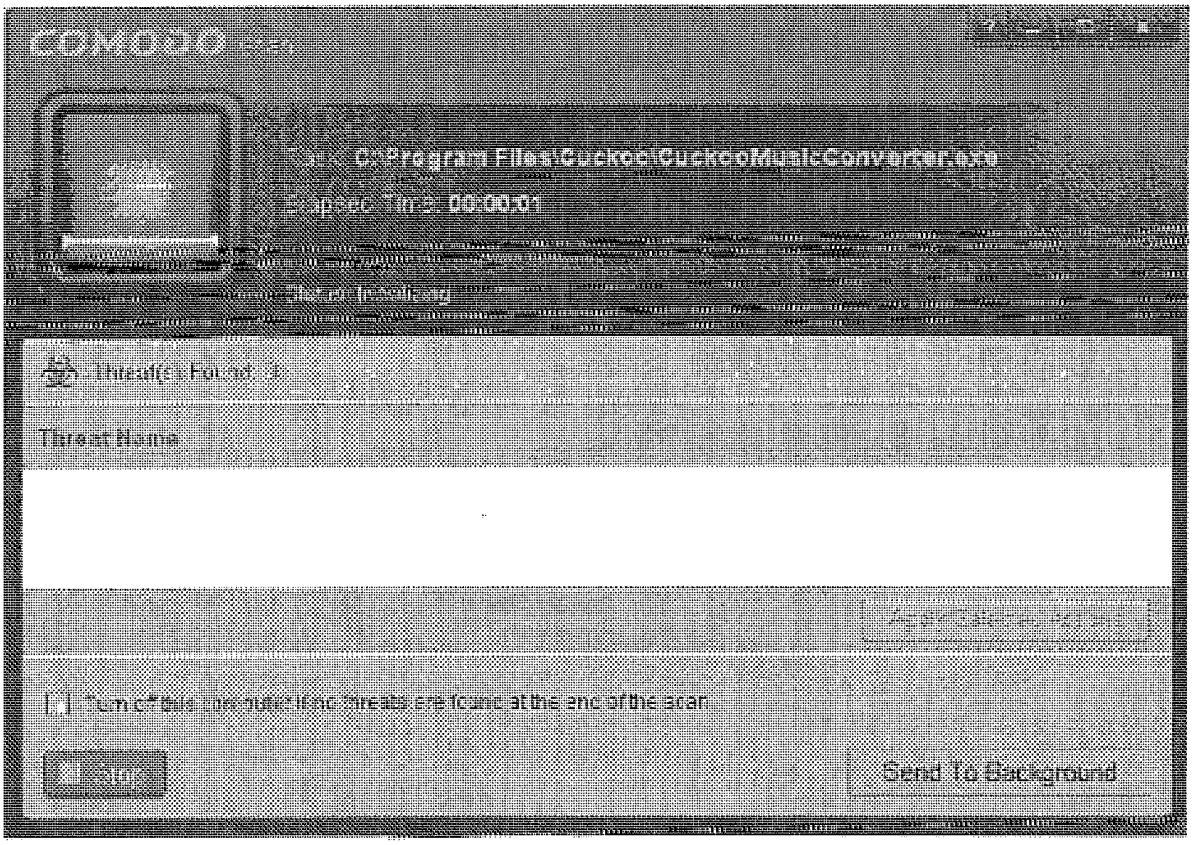


OR

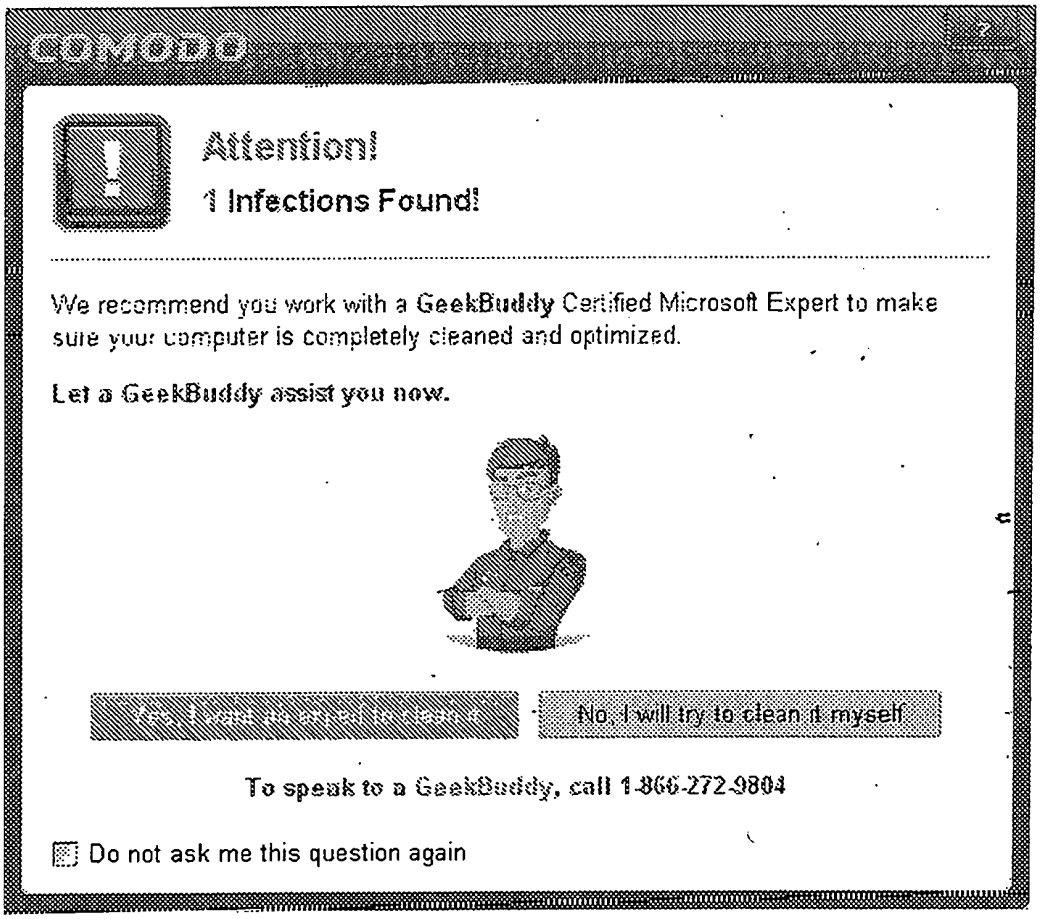
- Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



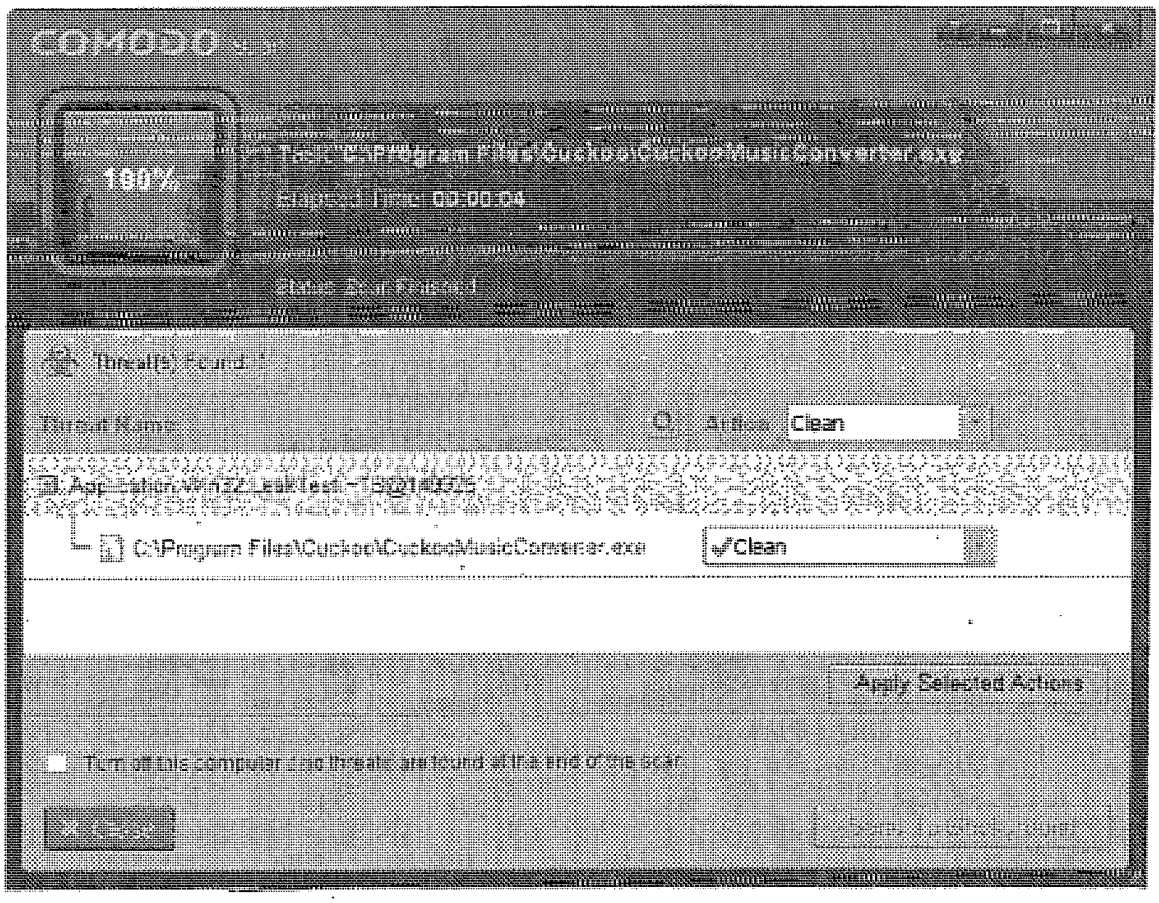
The item will be scanned immediately.



- On completion of scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



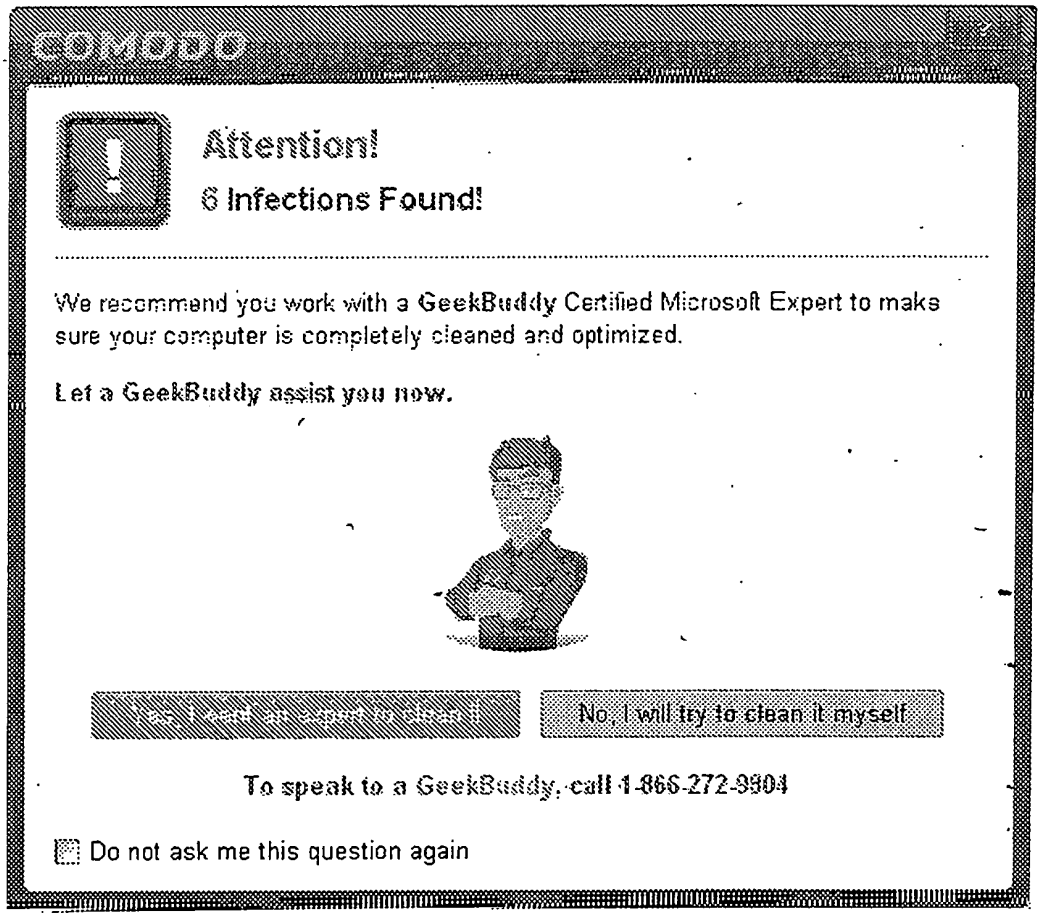
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed.



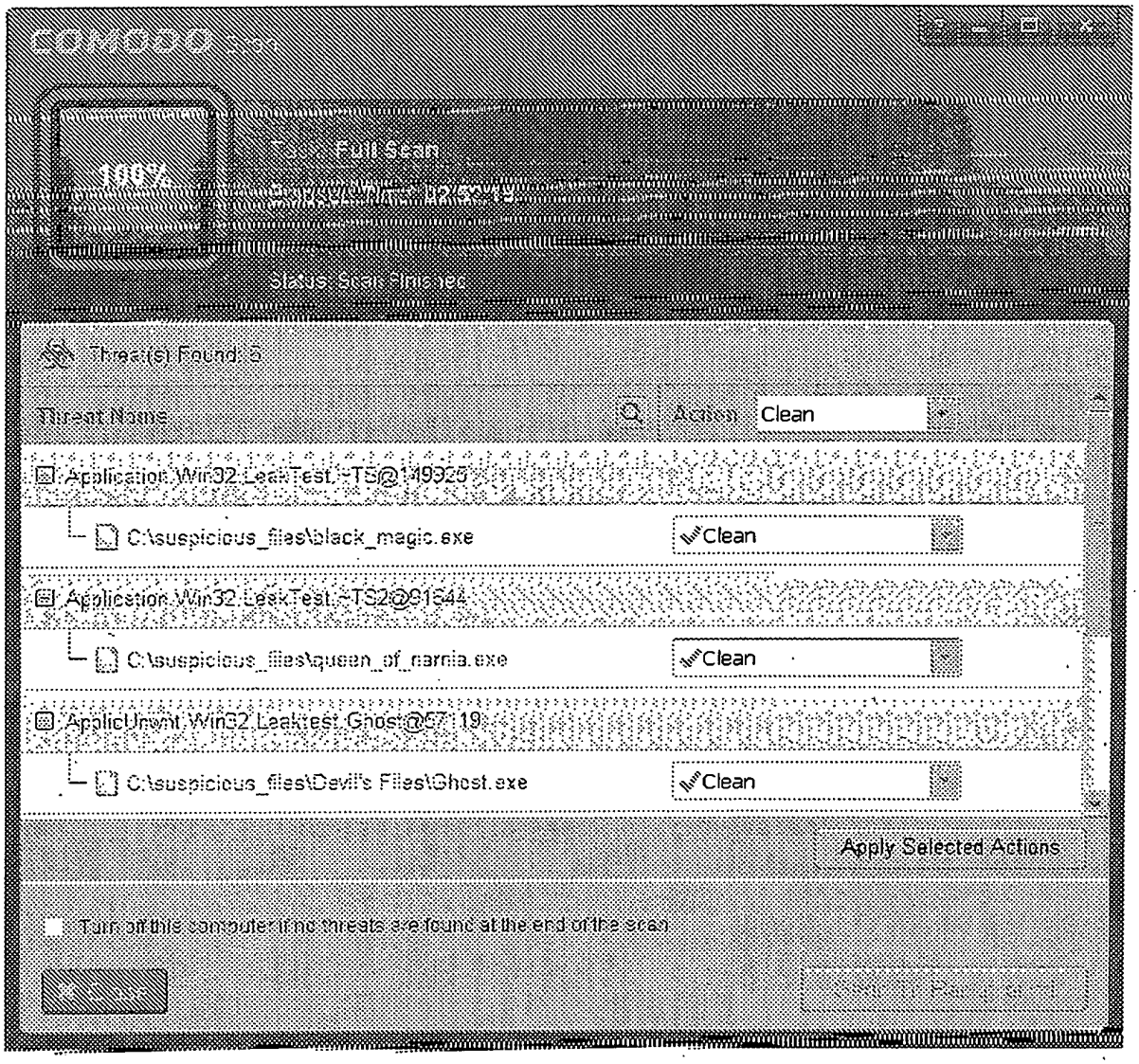
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

2.3. Processing Infected Files

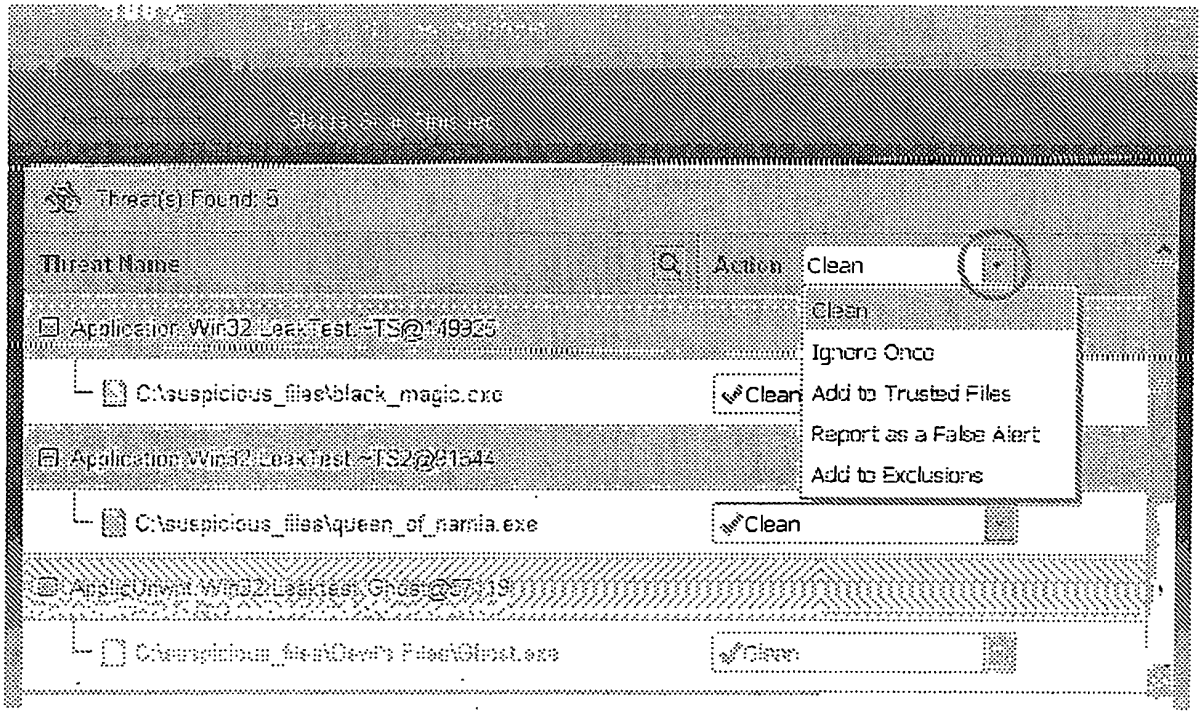
On completion of any on-demand or scheduled scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



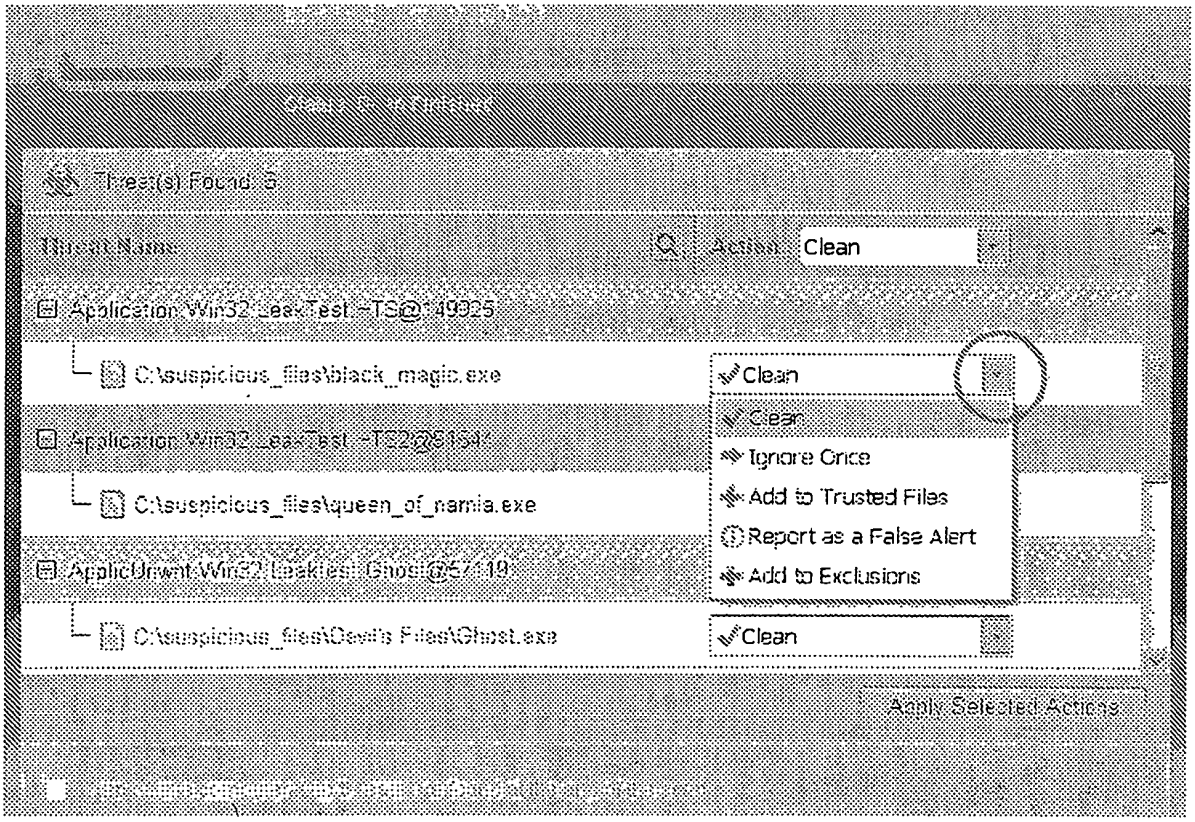
- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up for GeekBuddy services, the support chat session will start and a skilled technician will offer to clean your system.
    - For more details on GeekBuddy Expert help, refer to the section Comodo GeekBuddy.
- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:



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



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



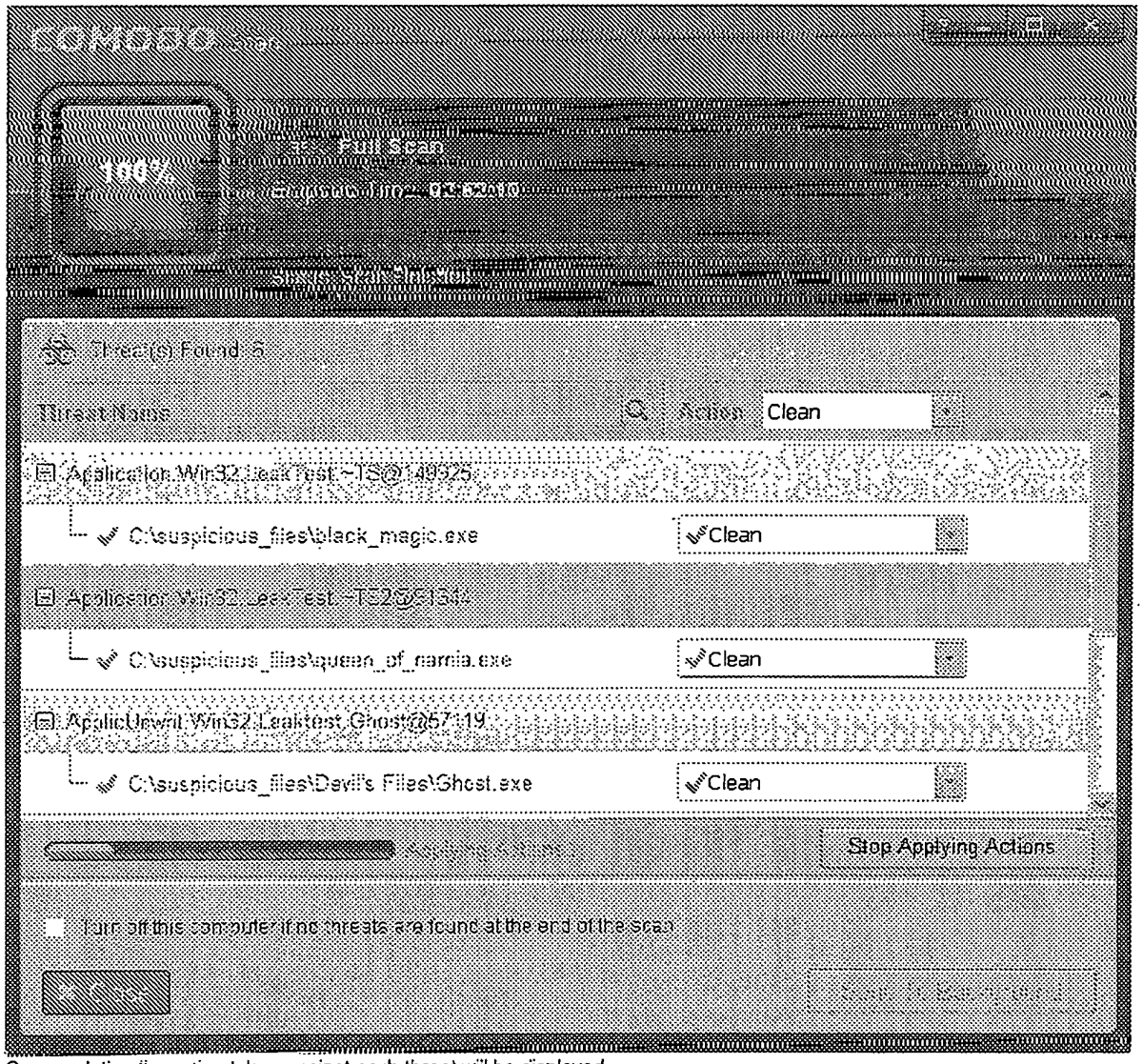
The choices for the actions available are:

- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application safe. If the disinfection routine is not available, Comodo Antivirus will

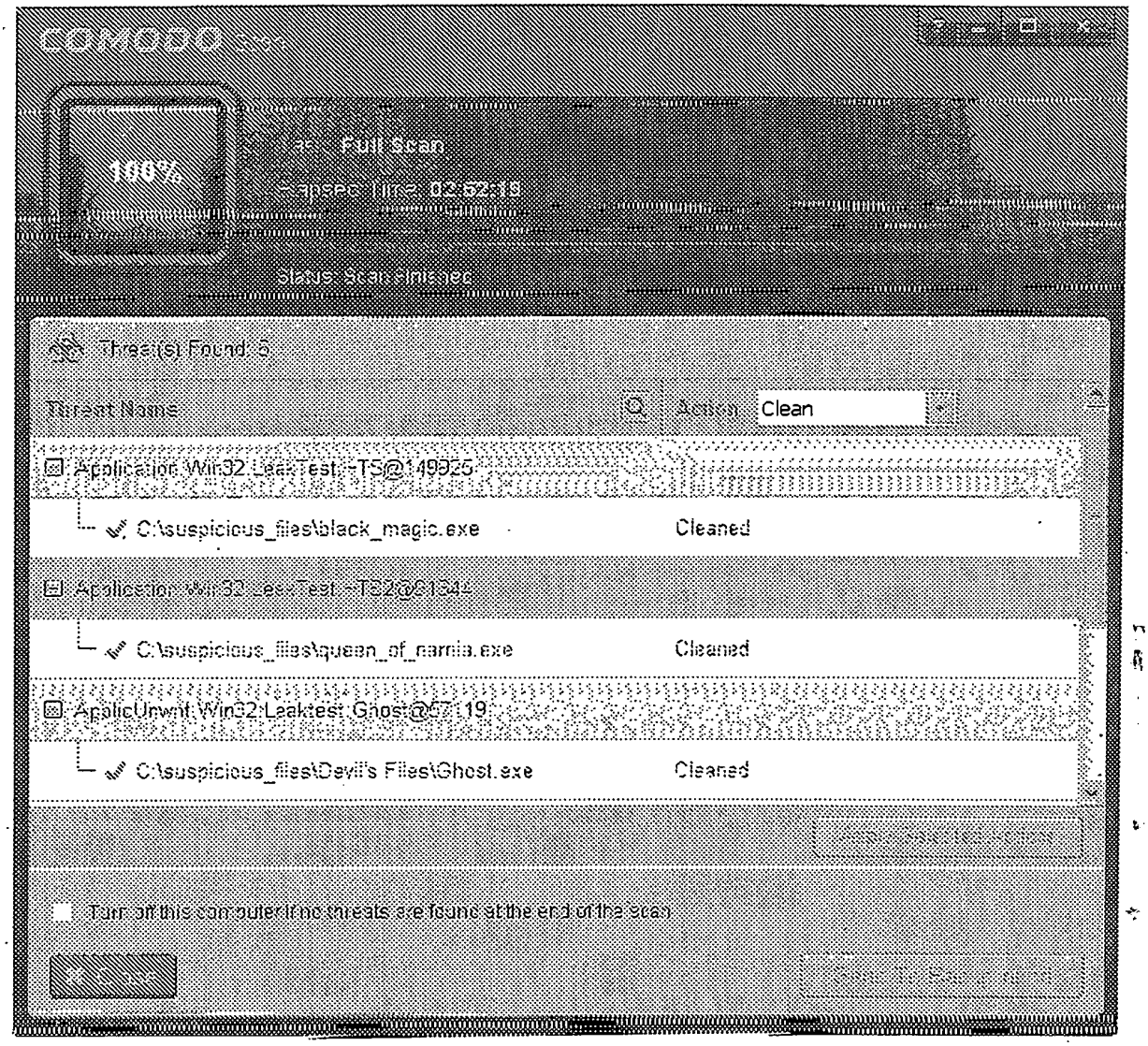
move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to Manage Quarantined Items.

- **Ignore Once** - If you want to ignore the threat this time only, select 'Ignore Once'. The file will be ignored only at that time. If the same application invokes again, the Antivirus will report it as a threat.
- **Add to Trusted Files** - If you trust the file, select 'Add to Trusted Files'. The file will be moved to Trusted Files list. The alert will not generated if the same application invokes again.
- **Report as a False Alert** - If you are sure that the file is safe, select 'Report as a False Alert'. The Antivirus will send the file to Comodo for analysis. If the file is trustworthy, it is added to the Comodo safe list.
- **Add to Exclusions** - The file will be moved to Exclusions list and will not be scanned in future. The alert will not generated if the same application invokes again.

- After selecting the action(s) to be applied, click 'Apply Selected Actions'. The files will be treated as per the action selected and the progress will be displayed.



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



- Click 'Close' to close the results window.

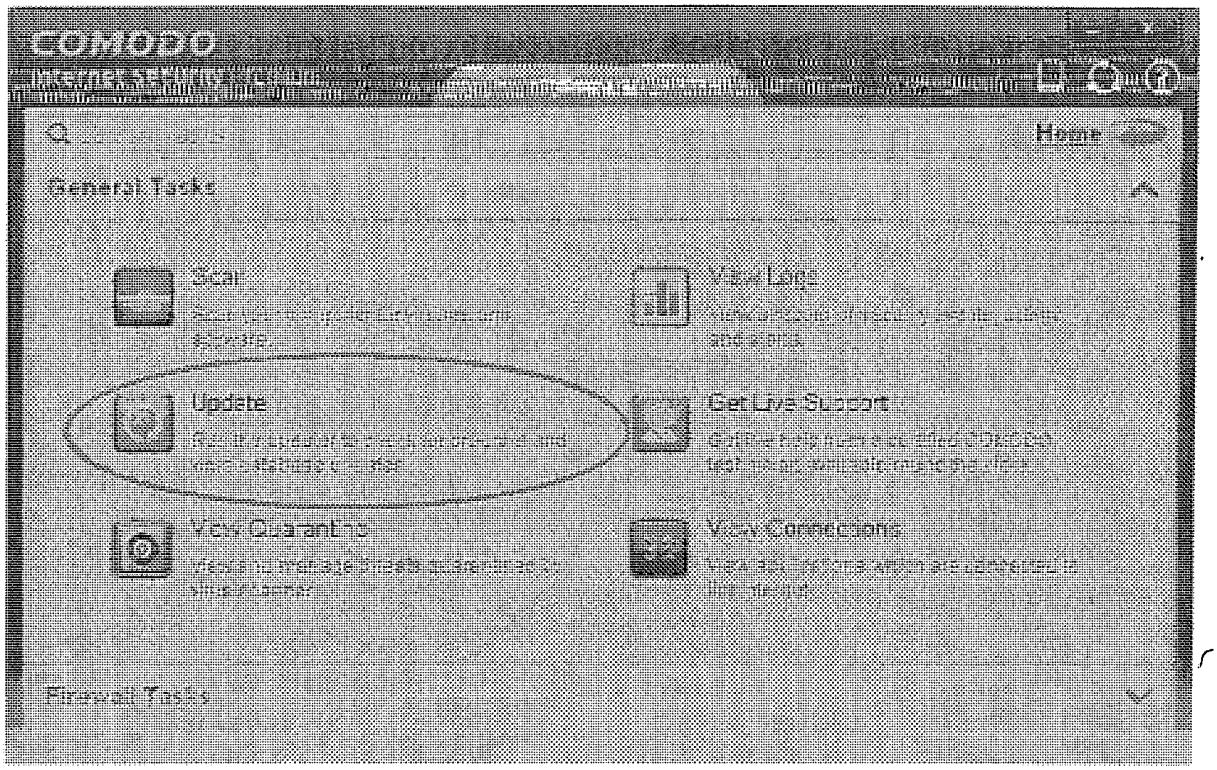
2.4. Manage Virus Database and Program Updates

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

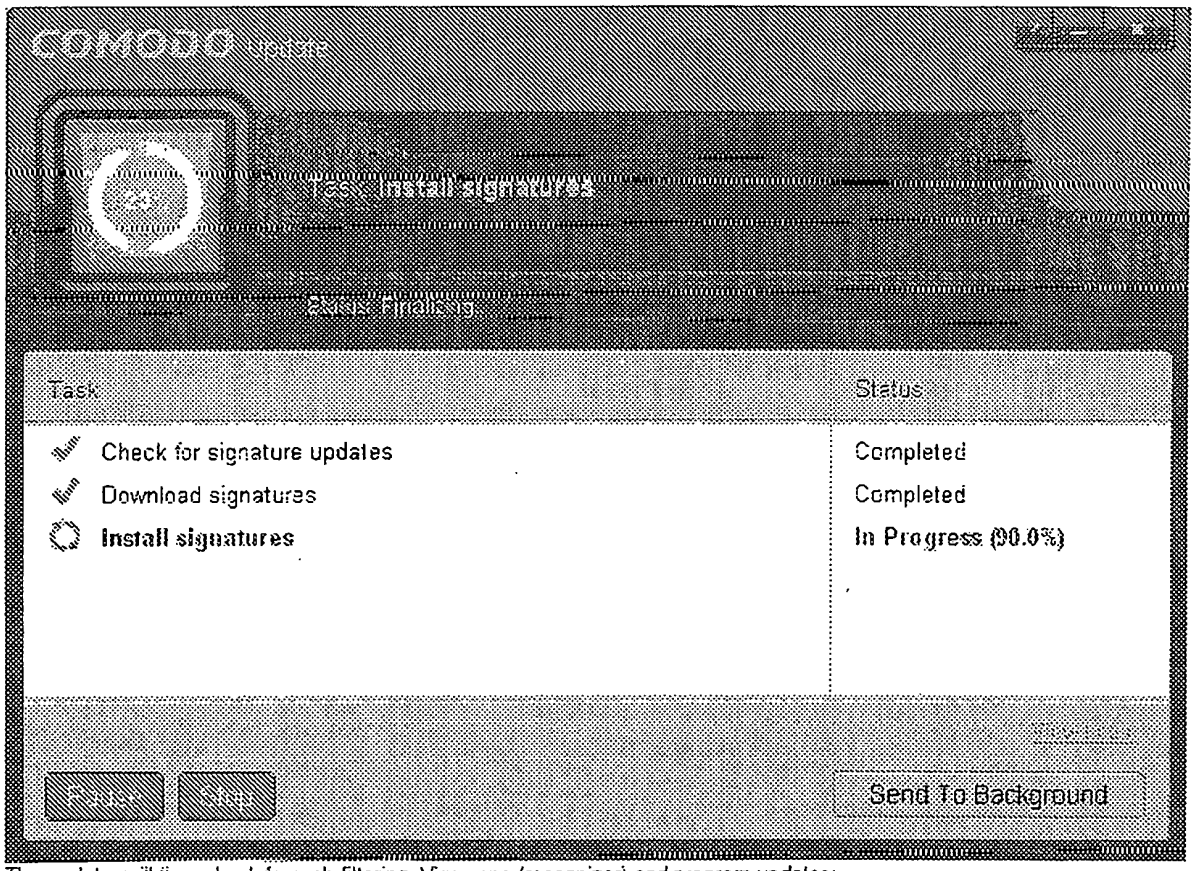
Note: You must be connected to Internet to download updates.

To manually check for the latest virus and program updates

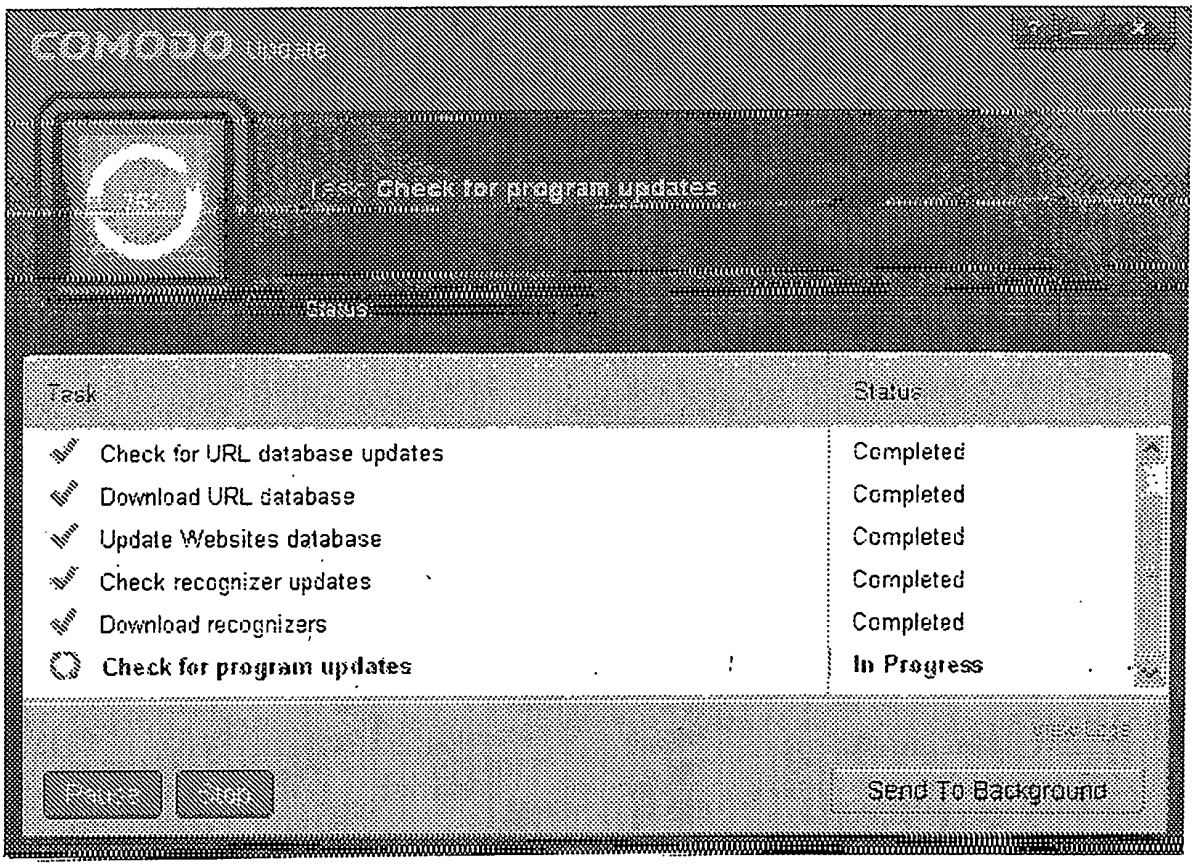
1. Switch to the 'Tasks' screen and click 'General Tasks' to open the 'General Tasks' interface.
2. Click 'Update'. The application will start checking for program and database updates



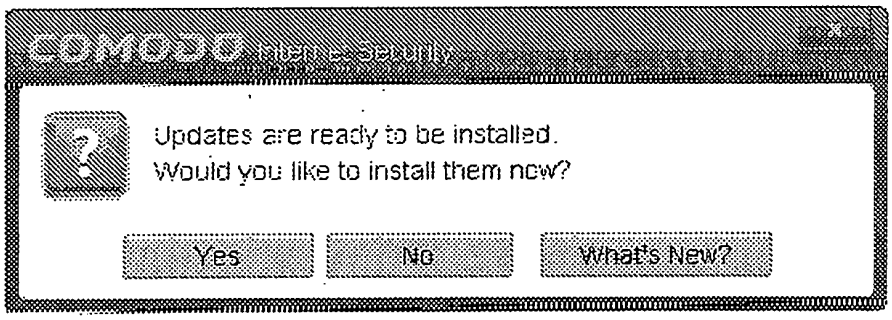
Signature updates will be downloaded and installed first if they are available:



The updater will then check for web filtering, Viruscope (recognizer) and program updates:



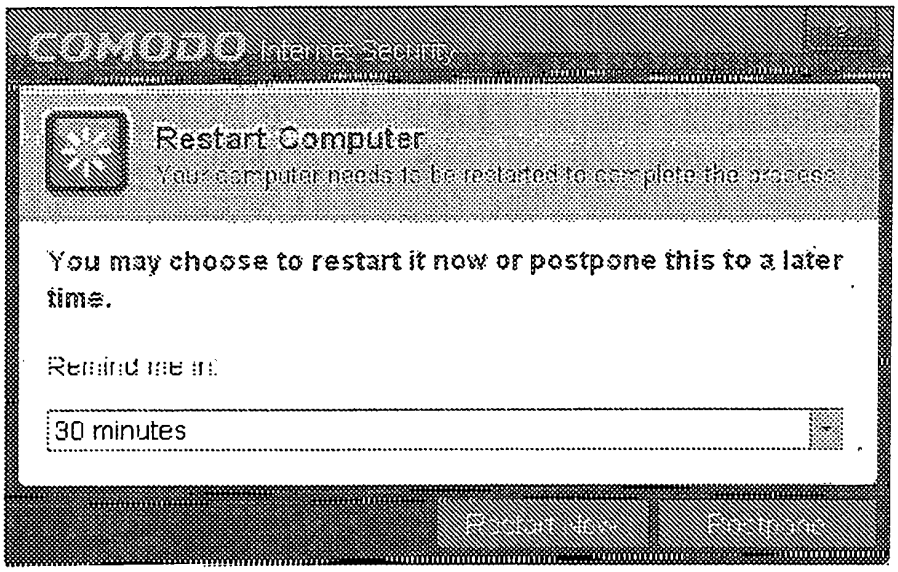
When all updates have been download you will be asked to confirm installation at the following dialog:



- Click 'Yes' to begin installation:

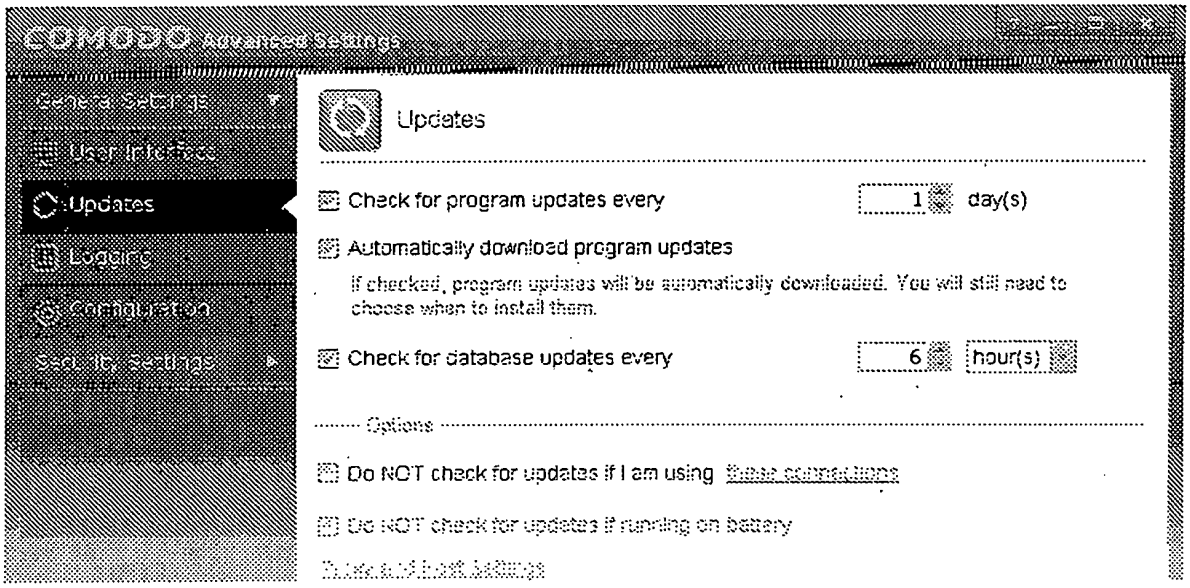
During the update process, new software components or features sometimes become available for installation. As these may alter the behavior of CIS in some manner, please carefully review these types of update before agreeing to their installation.

Your computer will need to be restarted to complete the update process. You can restart immediately or can select a period of after which you want to be reminded and click 'Postpone'.



Automatic Updates

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

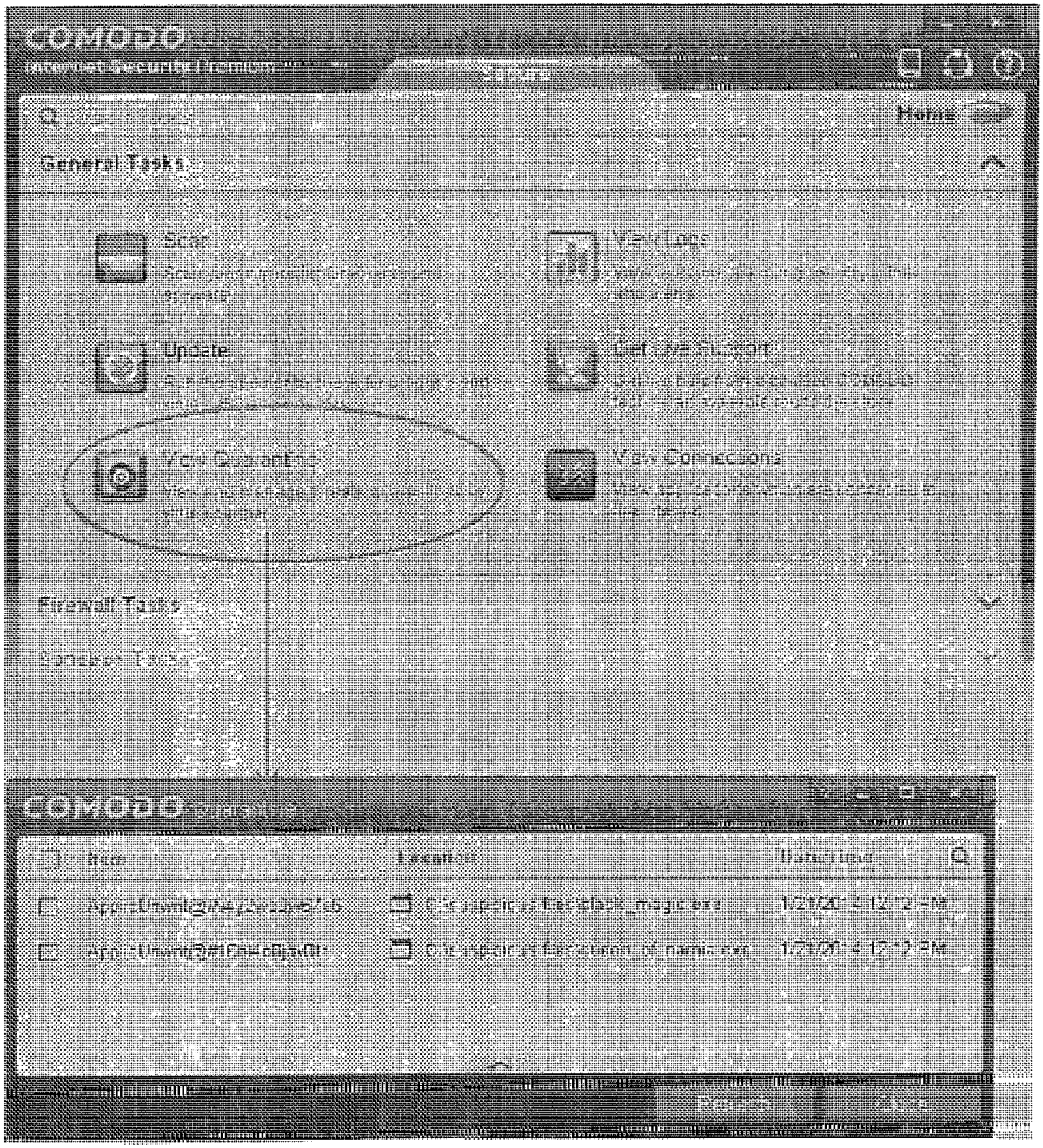


You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. Refer to Scan Profiles for more details.

2.5. Manage Quarantined Items

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

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



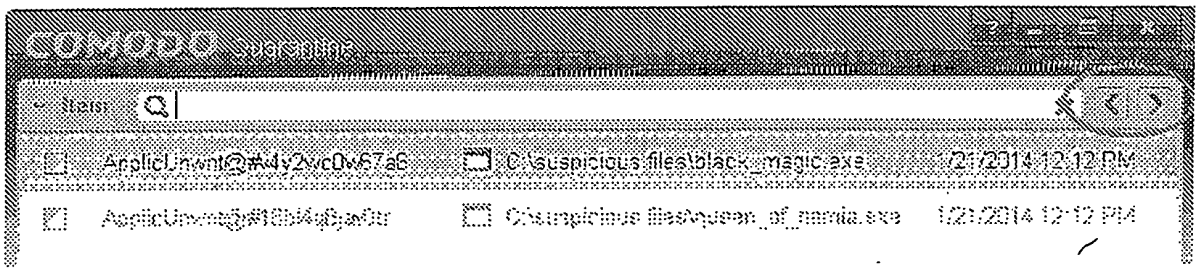
The 'Quarantine' interface displays a list of items moved to Quarantine from the results of real-time scanning, on-demand scanning and manually.

Column Descriptions

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

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

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



The Quarantined Items interface also allows you to:

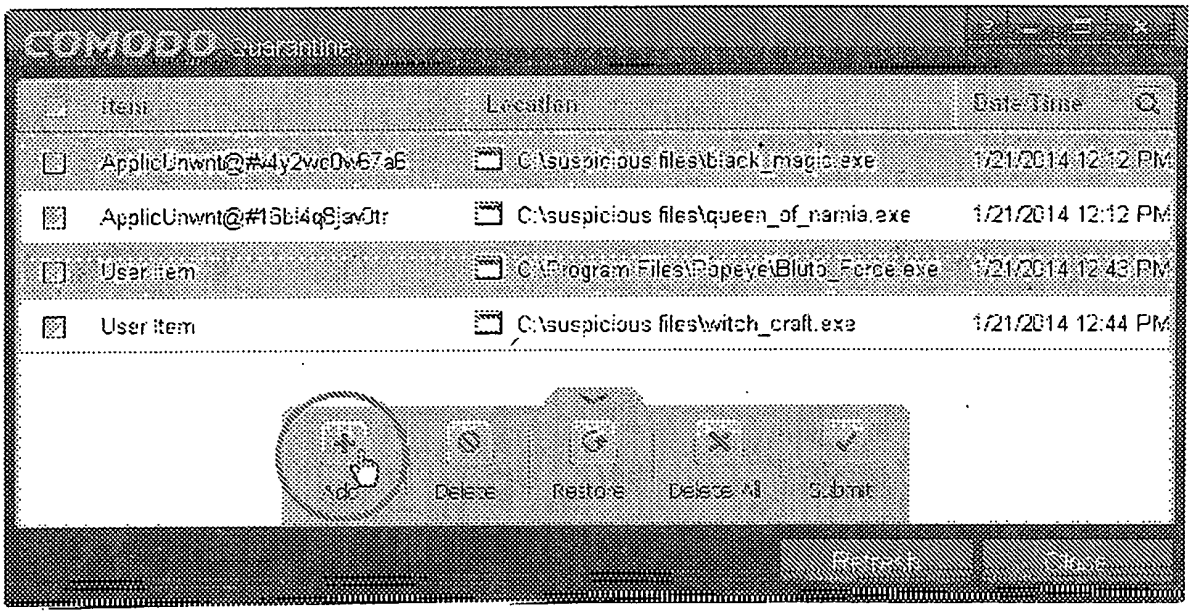
- Manually add applications, executables or other files, that you do not trust, as a Quarantined Item
- Delete a selected quarantined item from the system
- Restore a quarantined item to its original location
- Delete all quarantined items
- Submit selected quarantined items to Comodo for analysis

Manually adding files as Quarantined Items

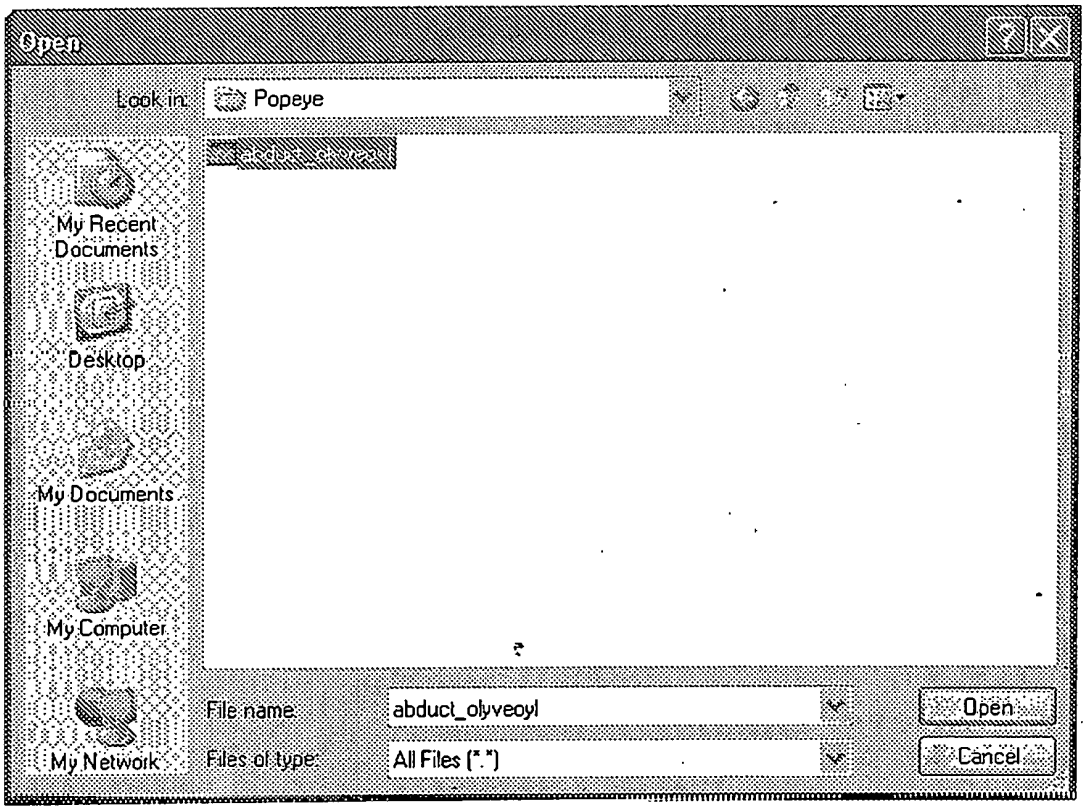
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

To manually add a Quarantined Item

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



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



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

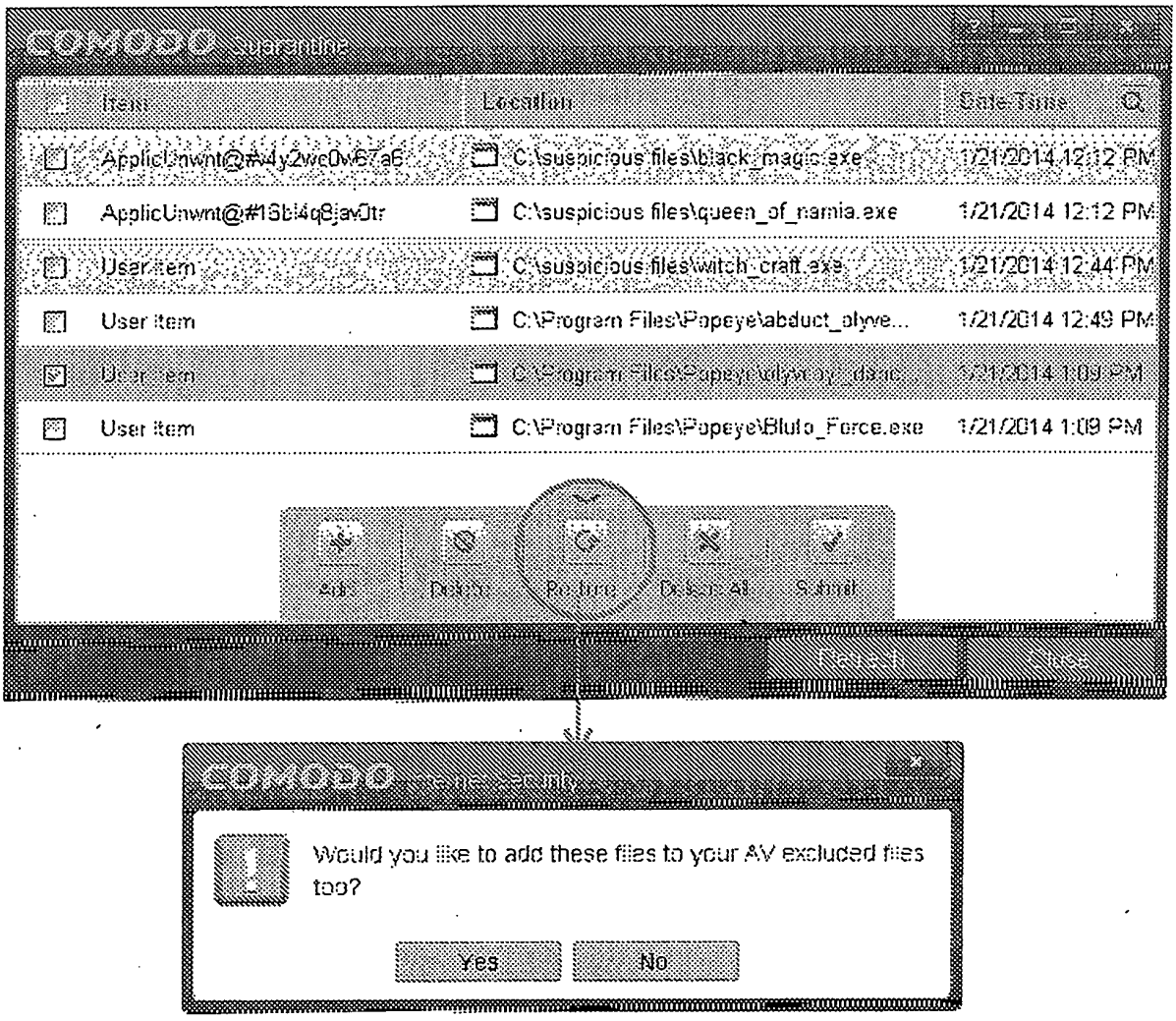
To delete a quarantined item from the system

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

This deletes the file from the system permanently.

To restore a quarantined item to its original location

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



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

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

To remove all the quarantined items permanently

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

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

To submit selected quarantined items to Comodo for analysis

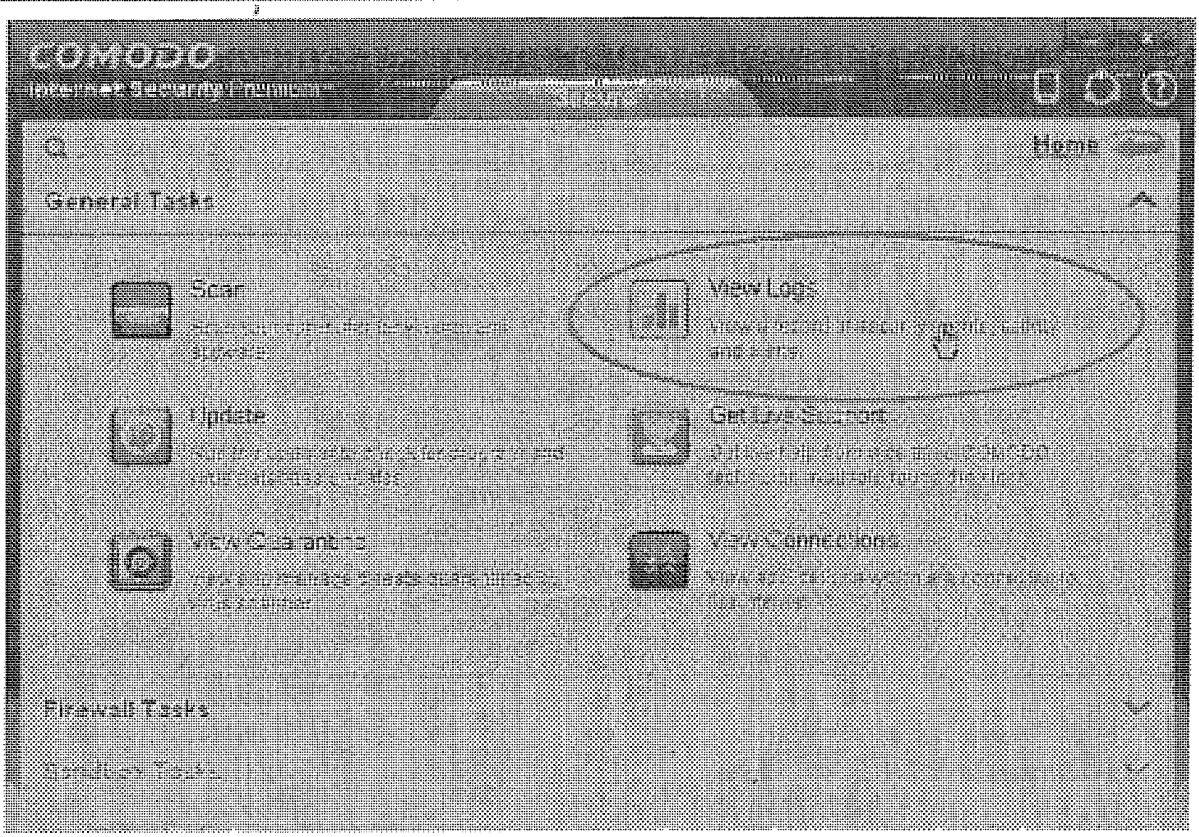
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

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

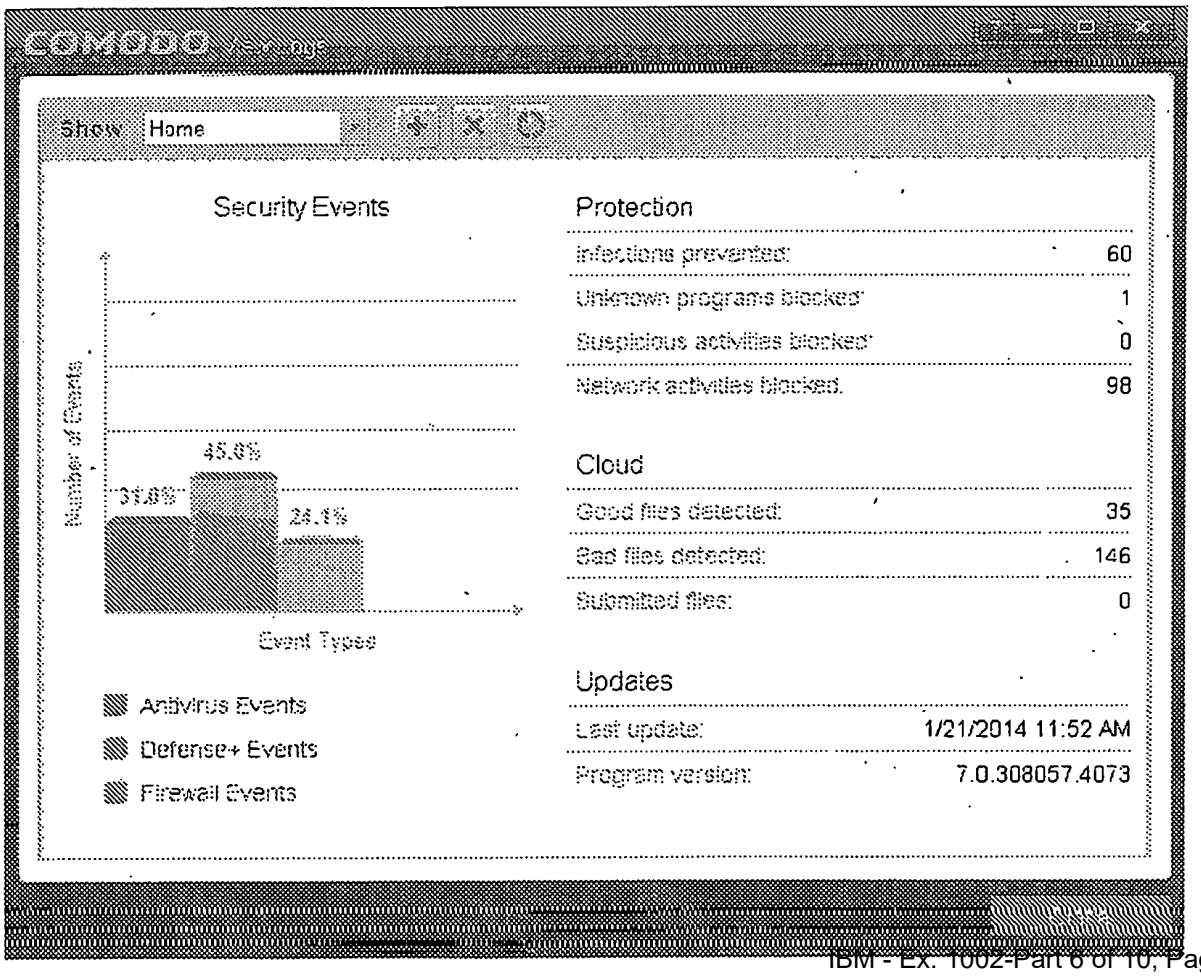
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

2.6. View CIS Logs

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



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



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

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

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

'Logs per Module':

- Antivirus
- Firewall
- Defense+
- Website Filtering

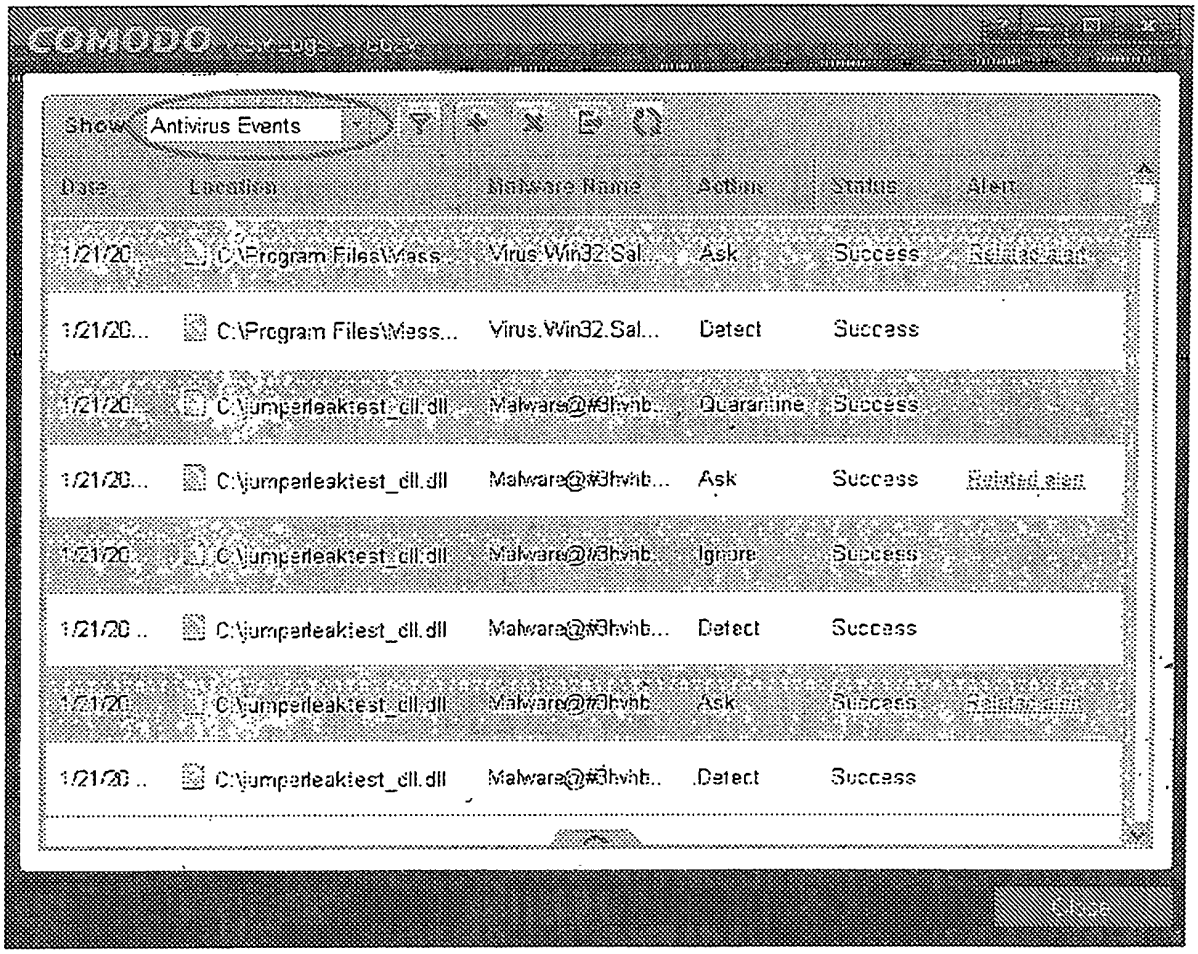
'Other Logs':

- Alerts Displayed
- Tasks Launched
- Configuration Changes

2.6.1. Antivirus Logs

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

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



Column Descriptions

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

- To export the Antivirus logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button.
- To refresh the Antivirus logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu..
- To clear the Antivirus logs click the 'Clear' button.

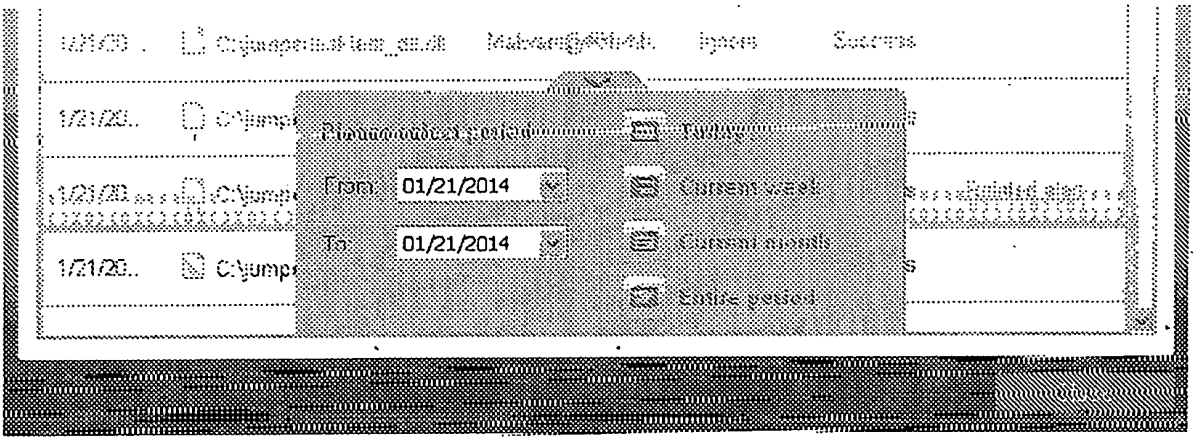
2.6.1.1. Filtering Antivirus Logs

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

- Preset Time Filters
- Advanced Filters

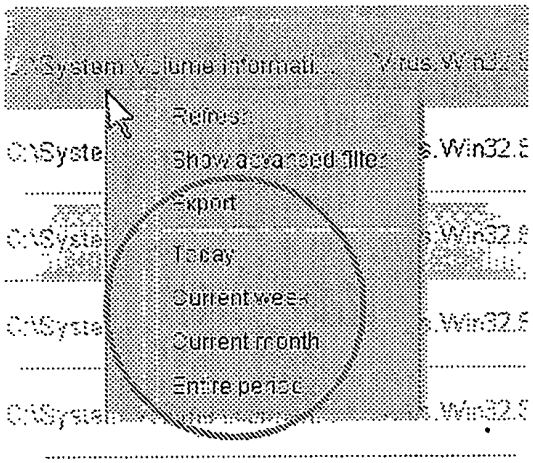
Preset Time Filters:

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



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

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



Advanced Filters:

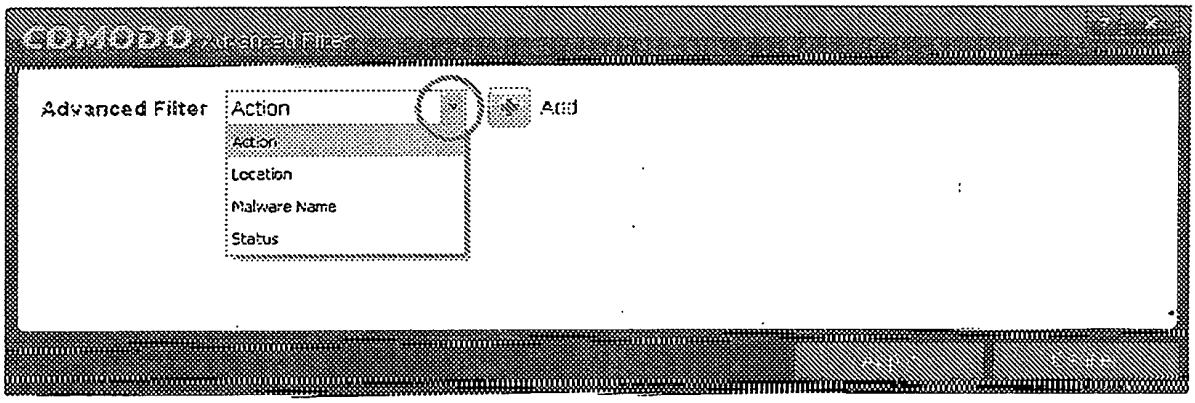
Having chosen a preset time filter, you can further refine the displayed events according to specific filters. Following are available filters for Antivirus logs and their meanings:

- **Action** - Displays events according to the response (or action taken) by the Antivirus
- **Location** - Displays only the events logged from a specific location

- **Malware Name** - Displays only the events logged corresponding to a specific malware
- **Status** - Displays the events according to the status after the action taken. It can be either 'Success' or 'Fail'

To configure Advanced Filters for Antivirus events

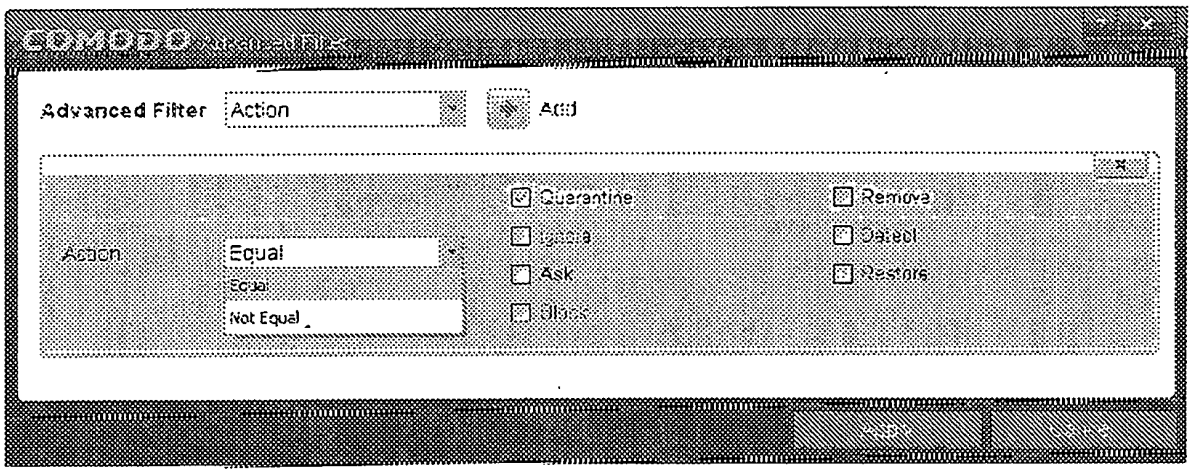
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for AV events will open
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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

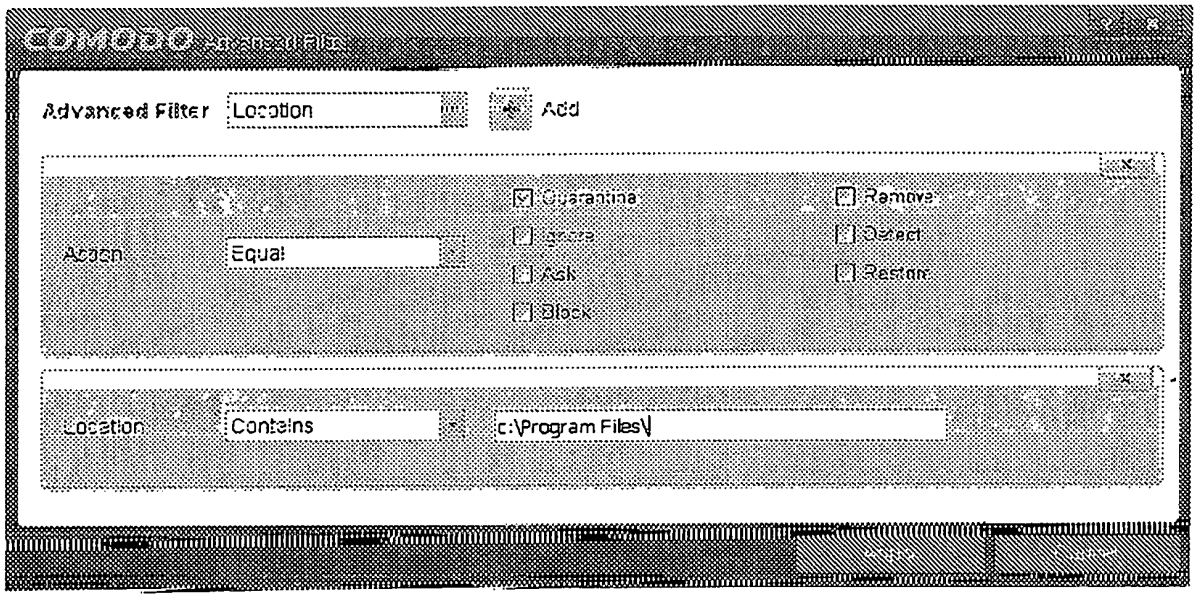


a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
   - Quarantine: Displays events where the user chose to quarantine a file
   -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

- Ask: Displays events when user was asked by alert concerning some Defense+, Firewall or Antivirus event
- Restore: Displays events of the applications that were quarantined and restored
- Block: Displays events of the applications that were blocked

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

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

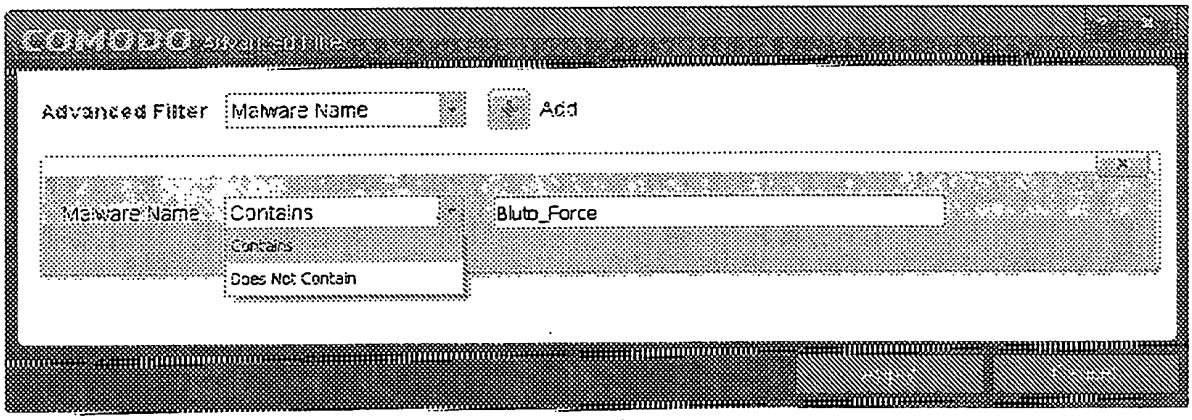


a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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

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

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

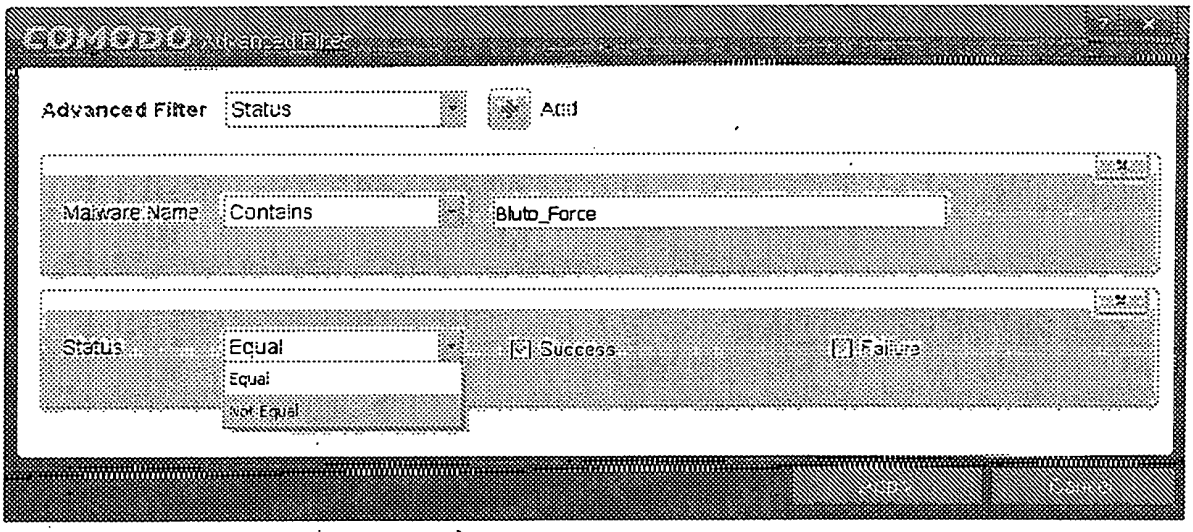


a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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

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

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



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

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

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

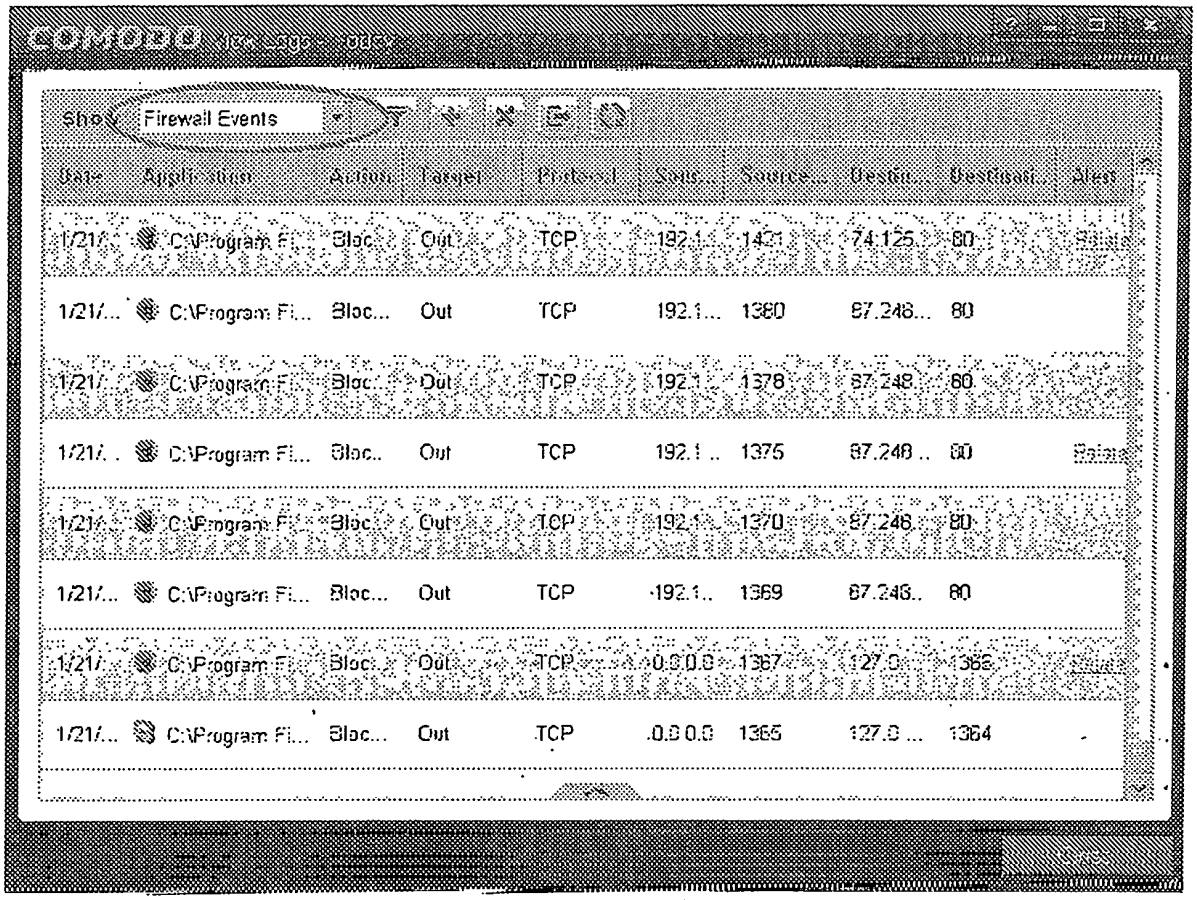
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Antivirus log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.2. Firewall Logs

Comodo Internet Security records a history of all actions taken by the firewall. Firewall 'Events' are generated and recorded for various reasons - including whenever an application or process makes a connection attempt that contravenes a rule in your Rule sets or whenever there is a change in Firewall configuration.

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



Column Descriptions

1. **Date** - Contains precise details of the date and time of the connection attempt.
2. **Application** - Indicates which application or process propagated the event. If the application has no icon, the default system icon for executable files are used
3. **Action** - Contains the flags attached to the events, indicating how the firewall has reacted to the connection attempt.
4. **Target** - Indicates whether the connection attempt is inbound or outbound.
5. **Protocol** - Represents the Protocol used by the application that attempted to create the connection. This is usually TCP/IP or UDP - which are the most heavily used networking protocols.
6. **Source IP** - States the IP address of the host that made the connection attempt. This is usually the IP address of your computer for outbound connections.
7. **Source Port** - States the port number on the host at the source IP which was used to make this connection attempt.
8. **Destination IP** - States the IP address of the host to which the connection attempt was made. This is usually the IP address of your computer for inbound connections.
9. **Destination Port** - States the port number on the host at the destination IP to which the connection attempt was made.
10. **Alert** - Gives the details of the alert displayed for the event

- To export the Firewall logs as a HTML file click the Export button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the Open button.

- To refresh the Firewall logs, click the Refresh button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu..
- To clear the Firewall logs click the Clear button.

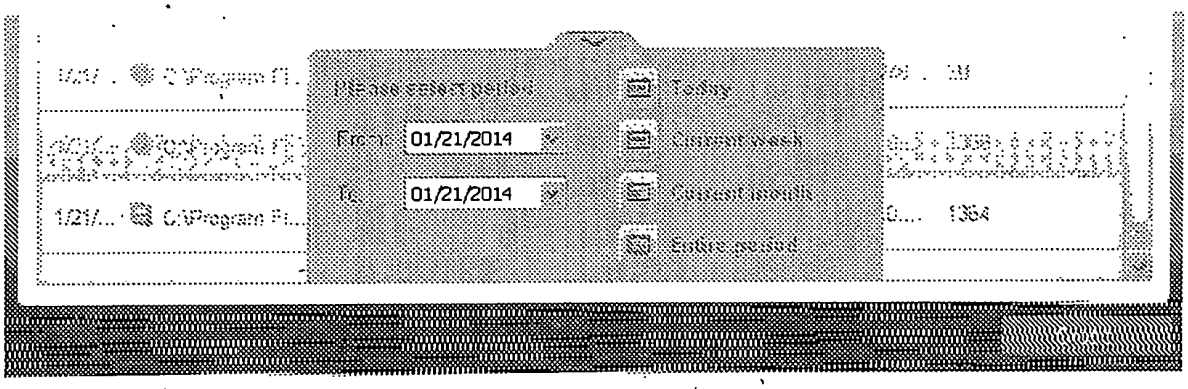
2.6.2.1. Filtering Firewall Logs

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

- Preset Time Filters
- Advanced Filters

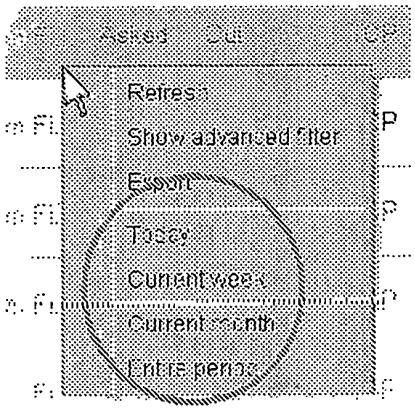
Preset Time Filters:

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



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

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



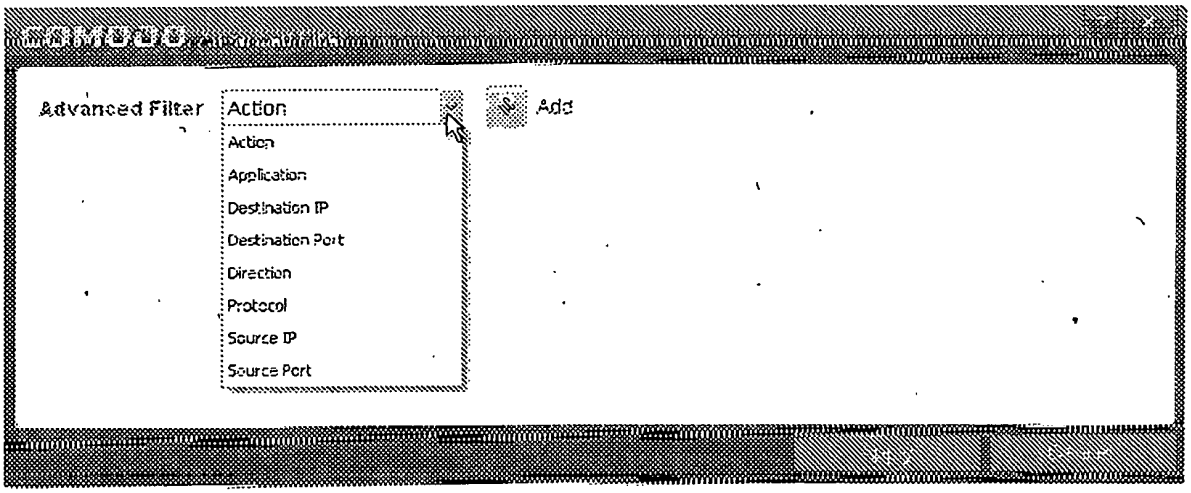
Advanced Filters

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

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

To configure Advanced Filters for Firewall events

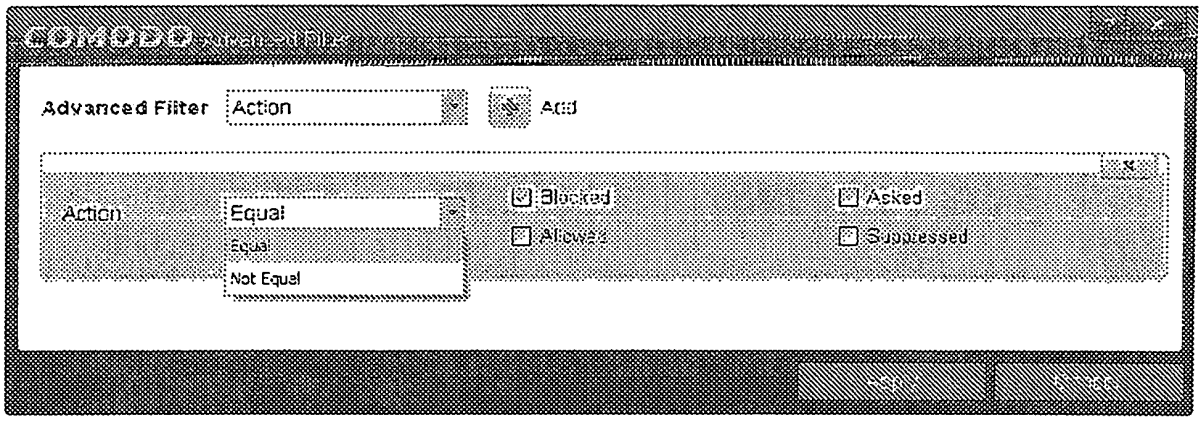
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

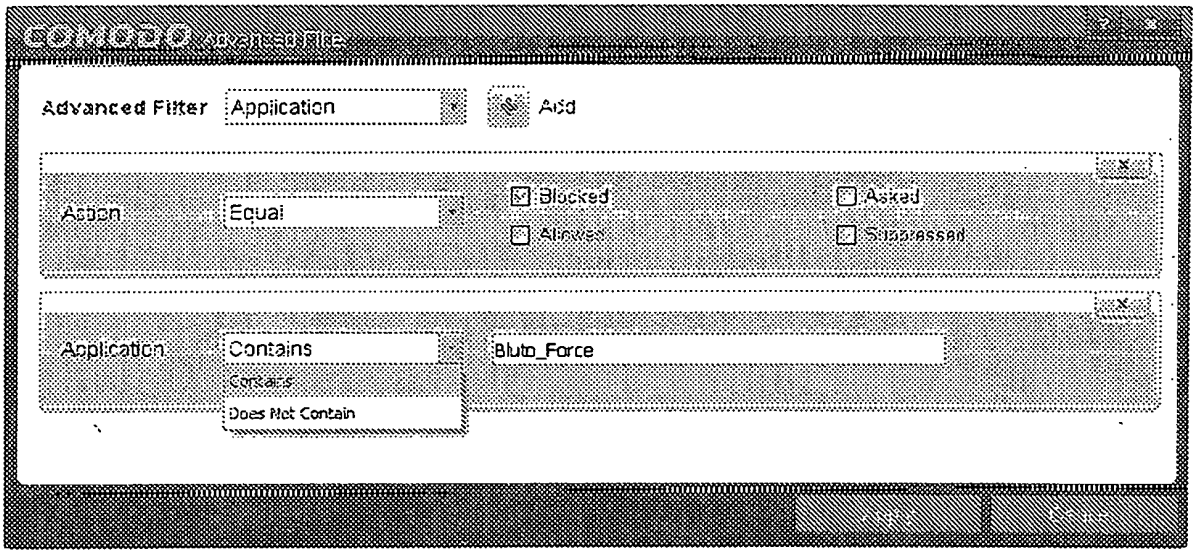
Following are the options available in the 'Advanced Filter' drop-down:

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



a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
   - Blocked: Displays list of events that were blocked
   - Allowed: Displays list of events that were allowed
   - Asked: Displays list of events that were asked to the user
   - Suppressed: Displays list of events that were suppressed by the user

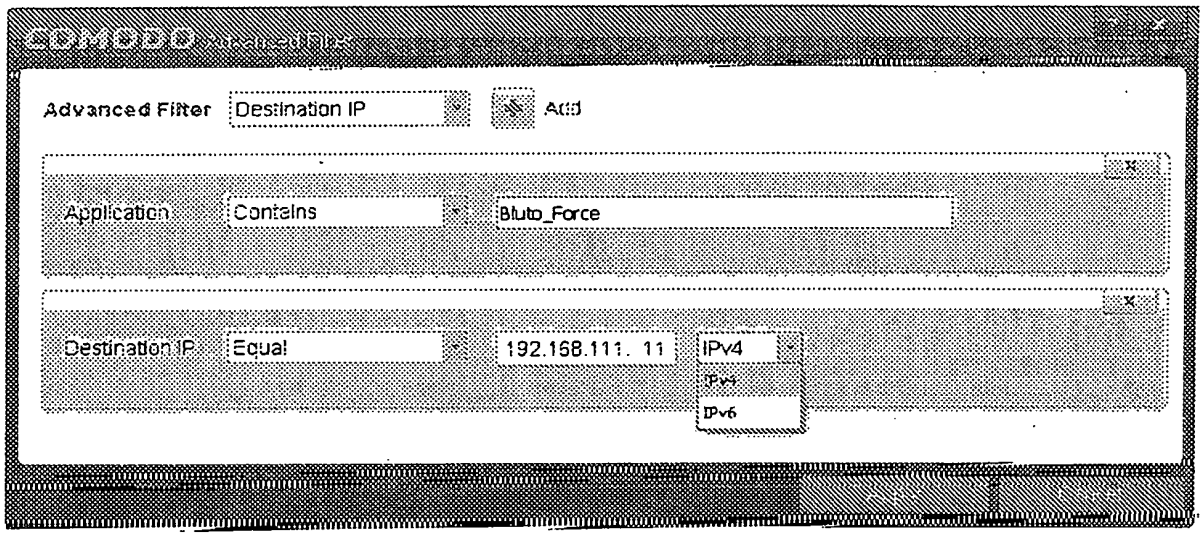
ii. **Application**: Selecting the 'Application' option displays a drop-down box and text entry field.



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

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

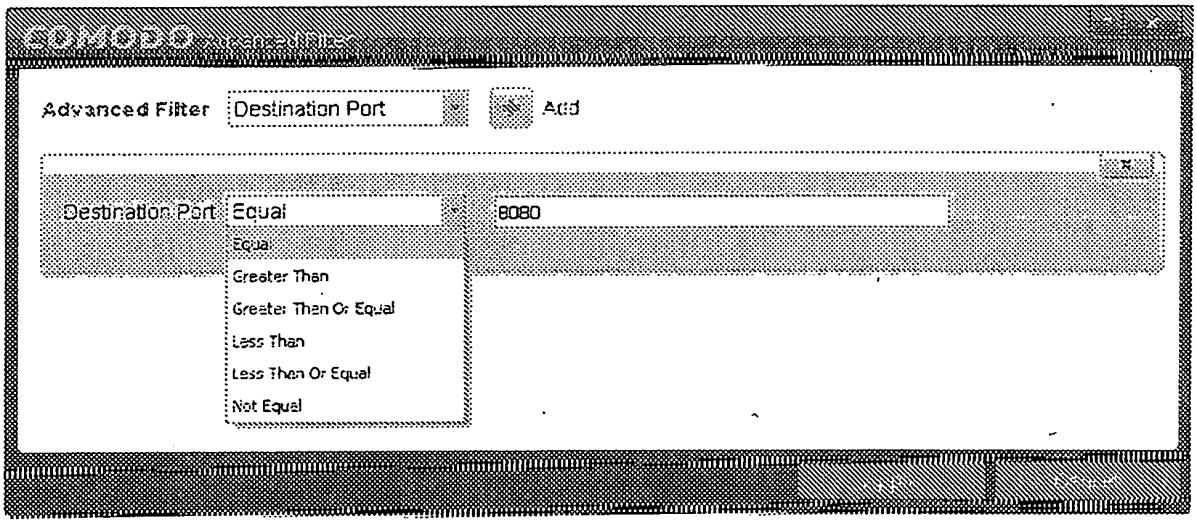
iii. **Destination IP**: Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.



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

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

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

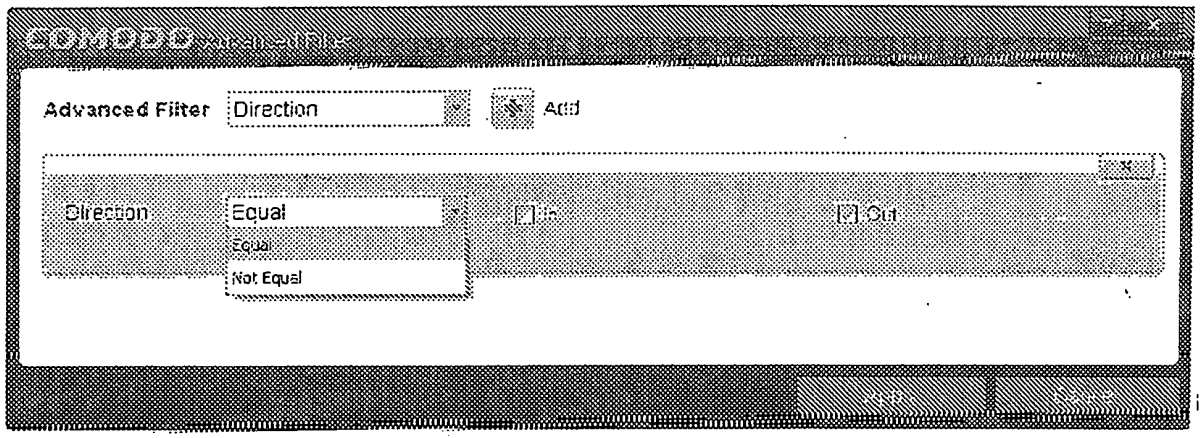


a) Select any one of the following option the drop-down box.
   - Equal
   - Greater than
   - Greater than or Equal
   - Less than
   - Less than or Equal
   - Not Equal

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

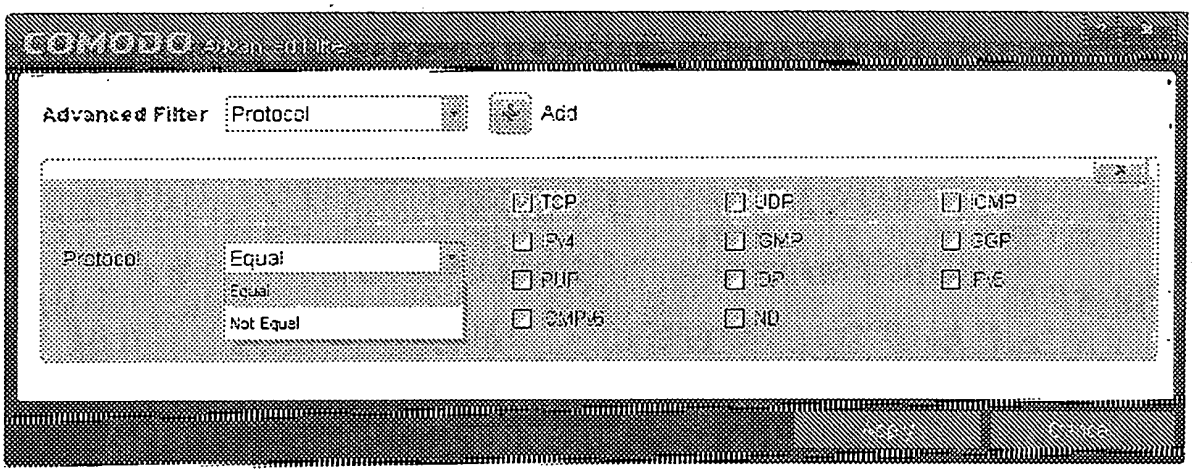
For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

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



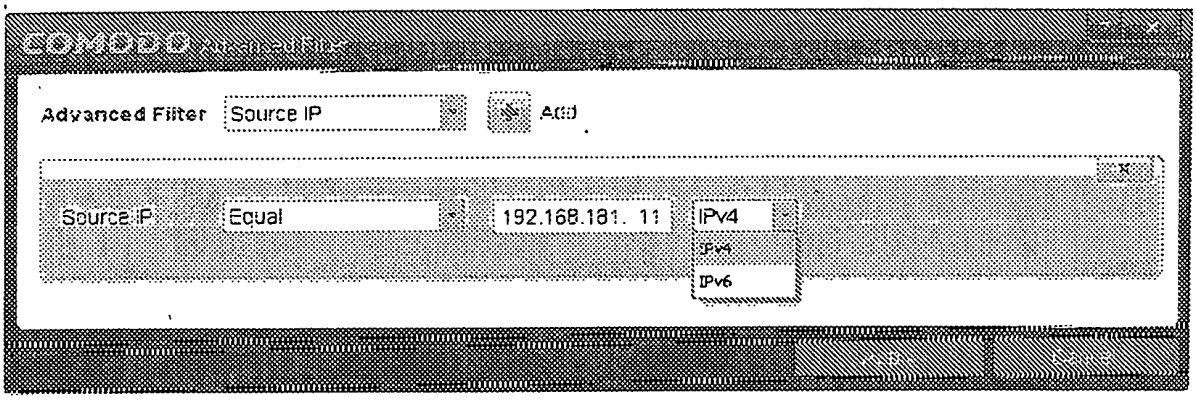
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the check box of the specific filter parameters to refine your search. The parameter available are:
   - In: Displays a list of events that were directed into the system
   - Out: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

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



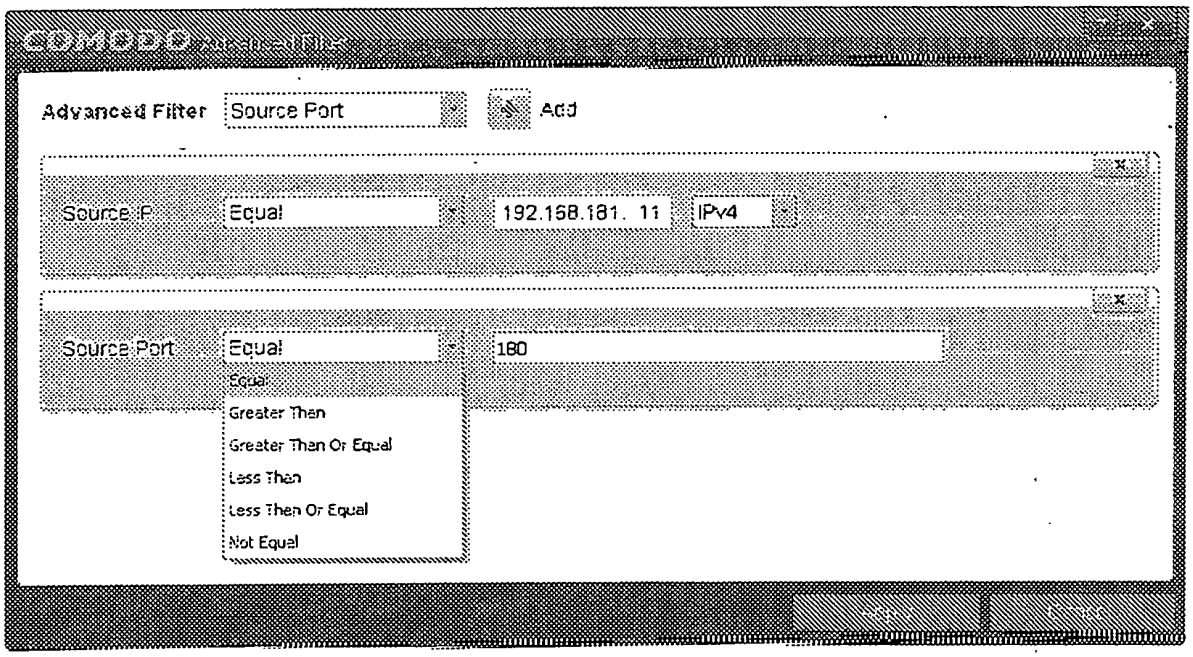
a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
   - TCP
   - UDP
   - ICMP
   - IPV4
   - IGMP
   - GGP
   - PUP
   - IDP
   - IPV6
   - ICMPV6
   - ND

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



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

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



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

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

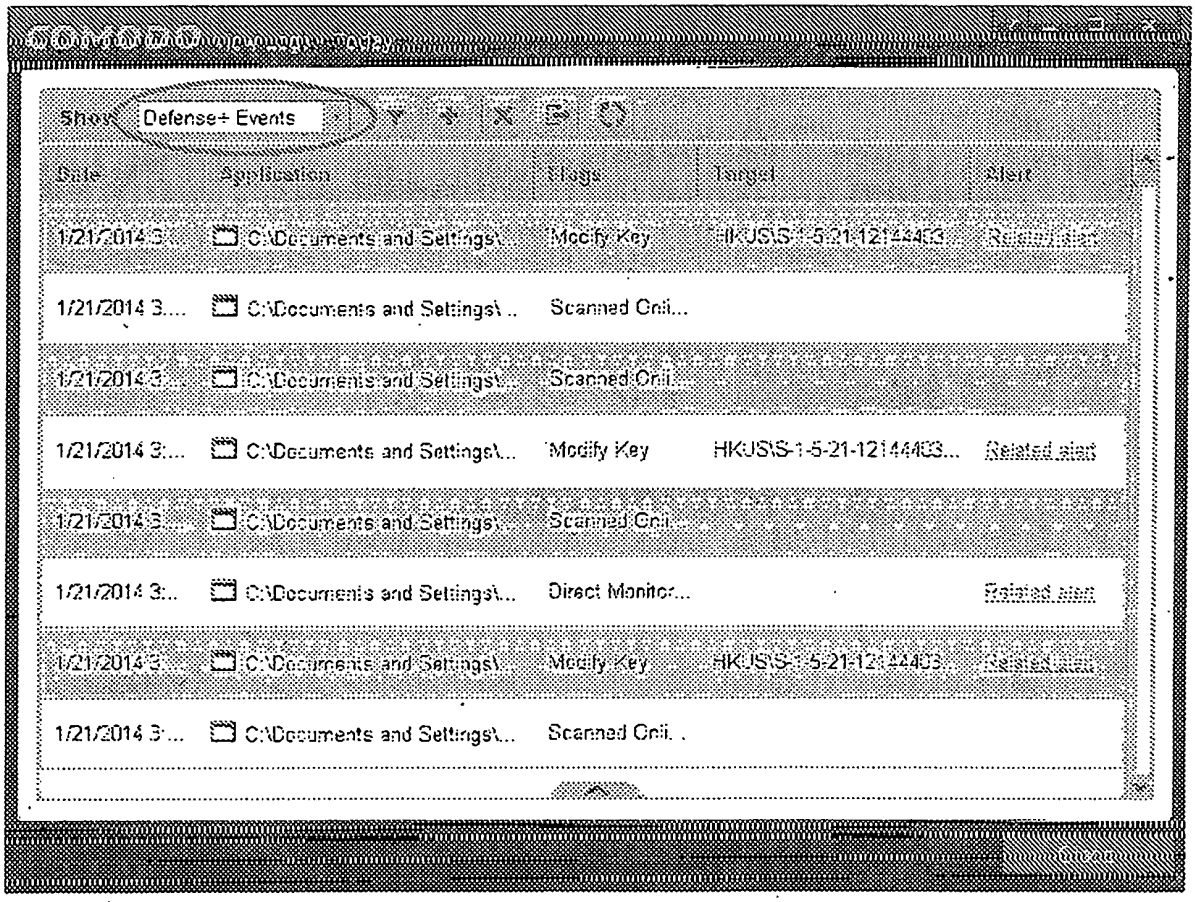
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.3. Defense+ Logs

Comodo Internet Security records a history of all actions taken by Defense+. Defense+ 'Events' are generated and recorded for various reasons. Examples include changes in HIPS settings, when an application is auto-sandboxed by Behavior Blocker, when an application or process attempts to access restricted areas or when an action occurs that contravenes your HIPS Rulesets.

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



Column Descriptions

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

- To export the Defense+ logs as a HTML file click the 'Export' button or right click inside the log viewer and

choose 'Export' from the context sensitive menu.

- To open a stored CIS log file, click the 'Open' button.
- To refresh the Defense+ logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the Defense+ logs click the 'Clear' button.

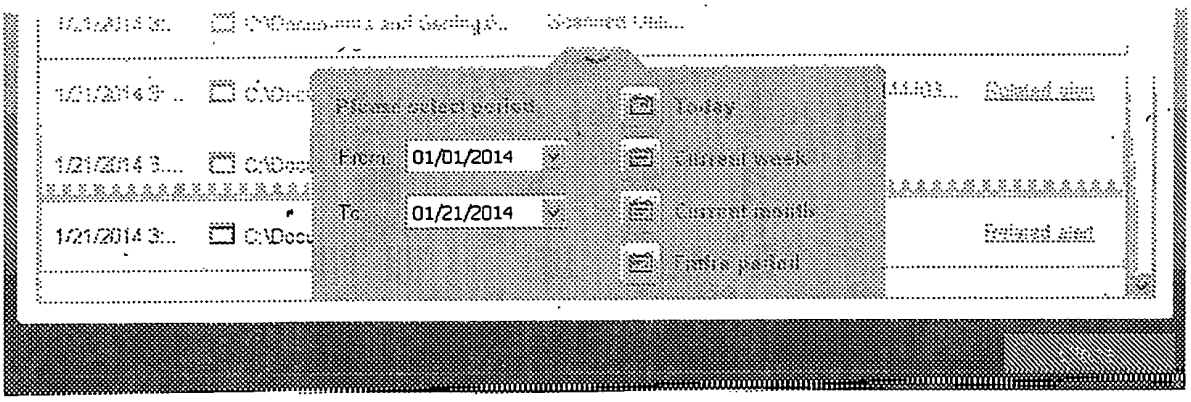
2.6.3.1. Filtering Defense+ Logs

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

- Preset Time Filters
- Advanced Filters

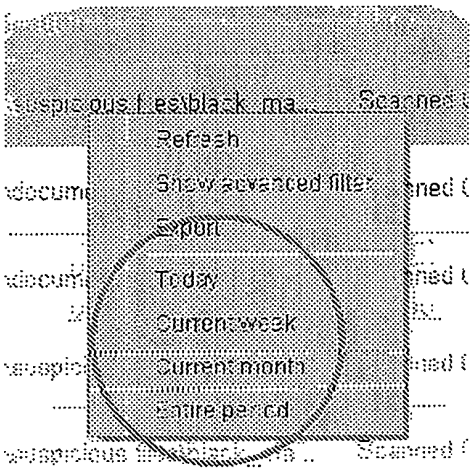
Preset Time Filters

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



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

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



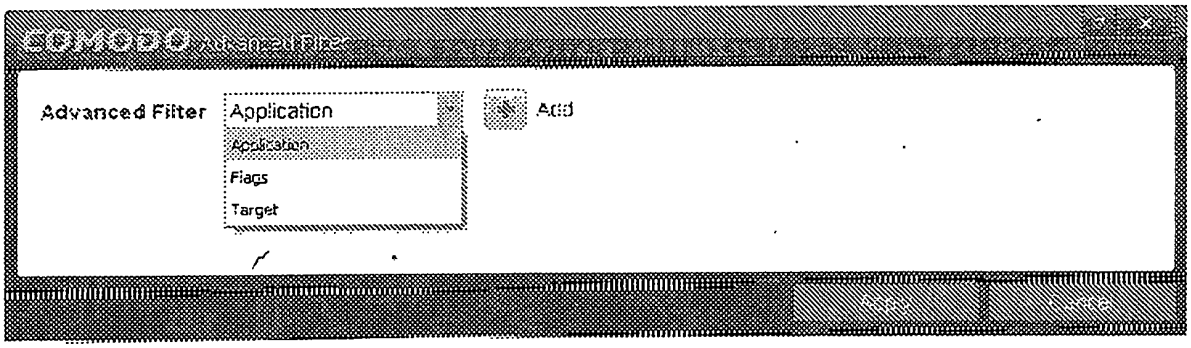
Advanced Filters

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

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

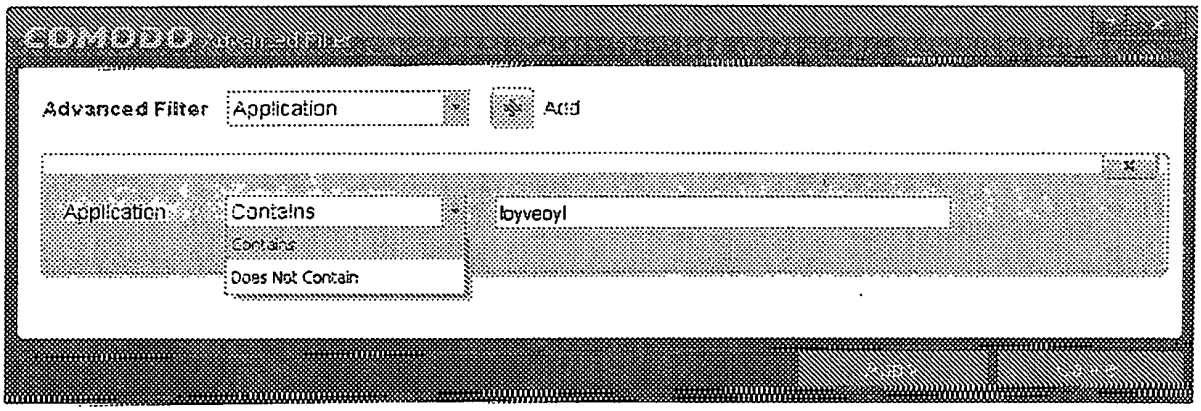
To configure Advanced Filters for Defense+ events

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Defense+ events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

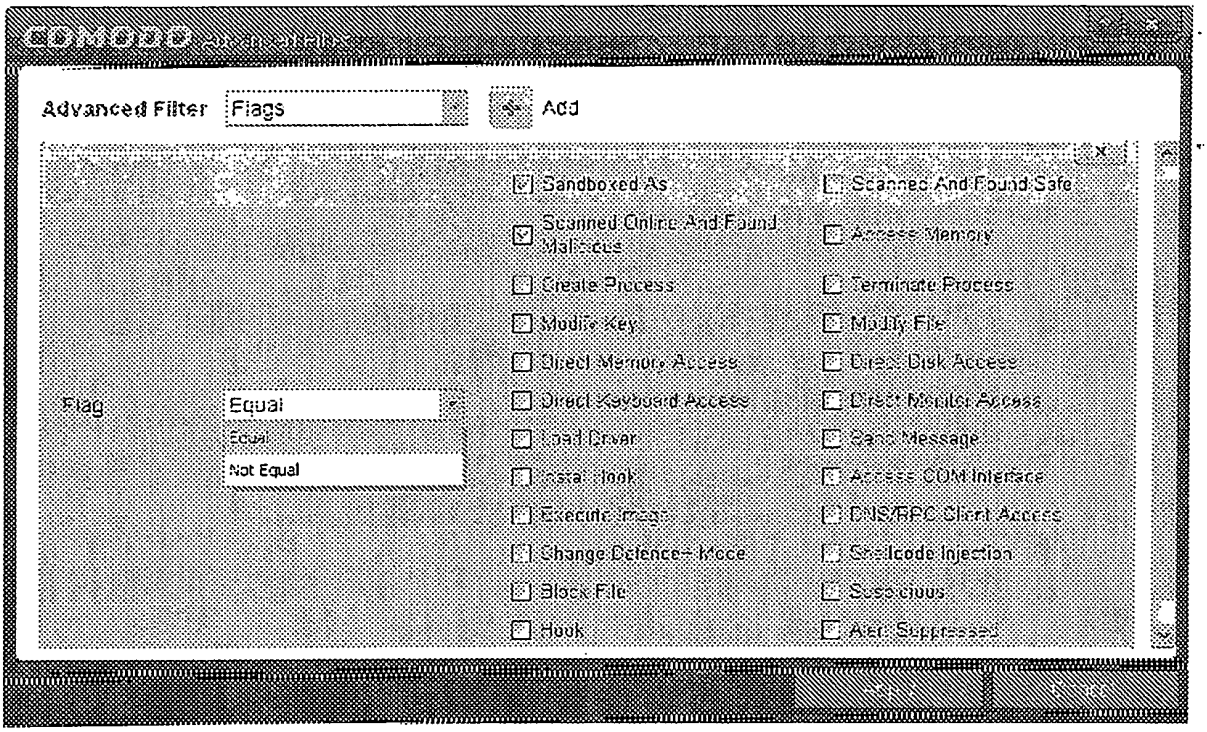
i. **Application**: Adding the 'Application' option displays a drop-down field and text entry field.



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

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

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



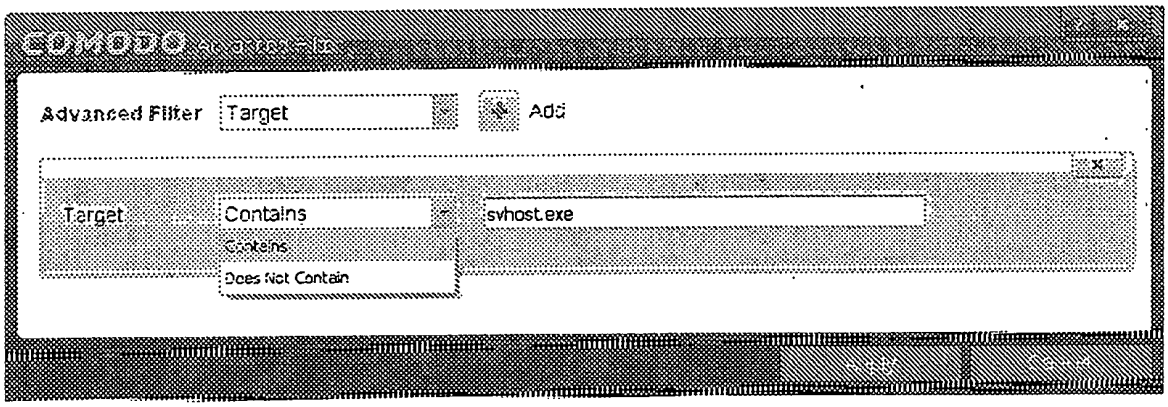
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- Sandboxed As
- Scanned Online and Found Safe
- Scanned Online and Found Malicious
- Access Memory
- Create Process
- Terminate Process

- Modify Key
- Modify File
- Direct Memory Access
- Direct Disk Access
- Direct Keyboard Access
- Direct Monitor Access
- Load Driver
- Send Message
- Install Hook
- Access COM Interface
- Execute Image
- DNS/RPC Client Access
- Change Defense+ Mode
- Shellcode Injection
- Block File
- Suspicious
- Hook
- Alert Suppressed

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

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



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

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

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

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

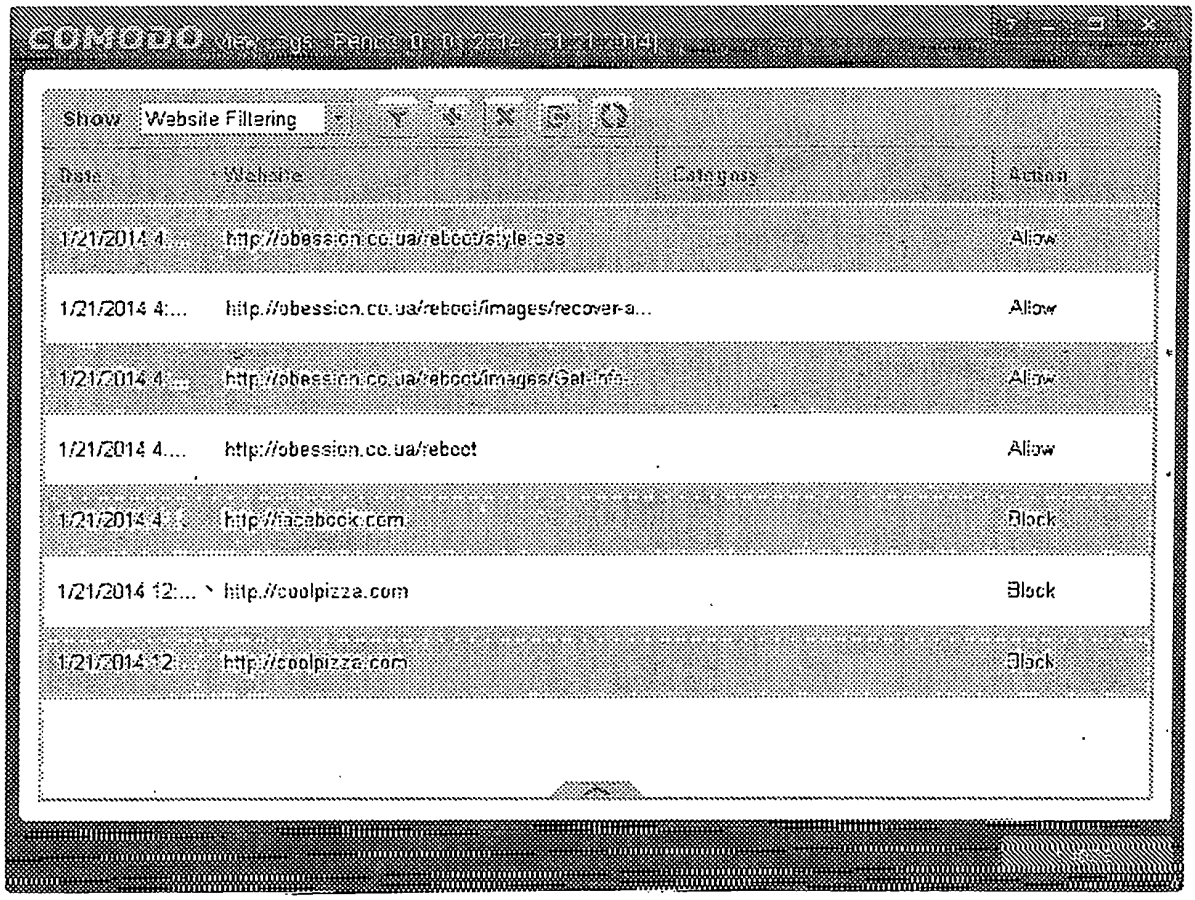
- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those Defense+ entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.4. 'Website Filtering' Logs

Comodo Internet Security maintains a log of Websites allowed or blocked to specific users by the 'Website Filter'.

You can configure rules to allow or block access to specific websites for particular users of your computer under Advanced Settings > Security Settings > Firewall Settings > Website Filtering. For more details on configuring the Website Filter, refer to the section Website Filtering. The Website Filtering log enables you to analyze the attempts made by the other users to access the blocked or allowed websites.

The 'Website Filtering' logs can be viewed by choosing the 'Website Filtering' from the 'Show' drop-down of the log viewer interface.



Column Descriptions

1. **Date** - Contains precise details of the date and time of the event.
2. **Website** - Shows the url of the website that was blocked or allowed as per the rules configured in the Website Filtering interface.
3. **Category** - Indicates the predefined category to which the website belongs.
4. **Action** - Indicates whether the access to the website was allowed or blocked to the user.

- To export the 'Website Filtering' logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button.
- To refresh the Alerts logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu..

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

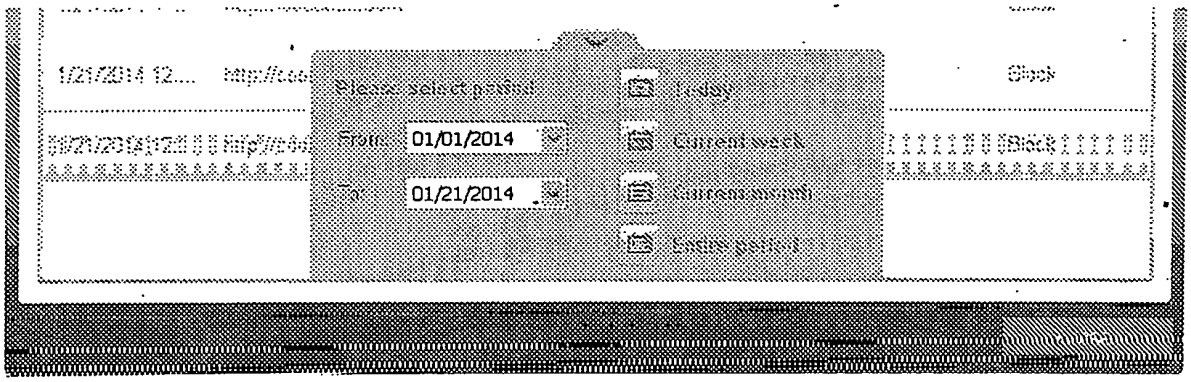
2.6.4.1. Filtering 'Website Filtering' Logs

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

- Preset Time Filters
- Advanced Filters

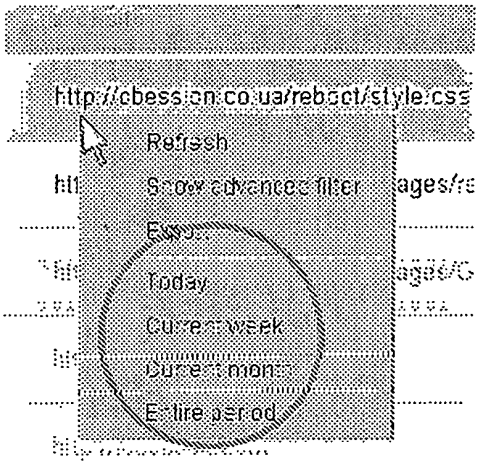
Preset Time Filters

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



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

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



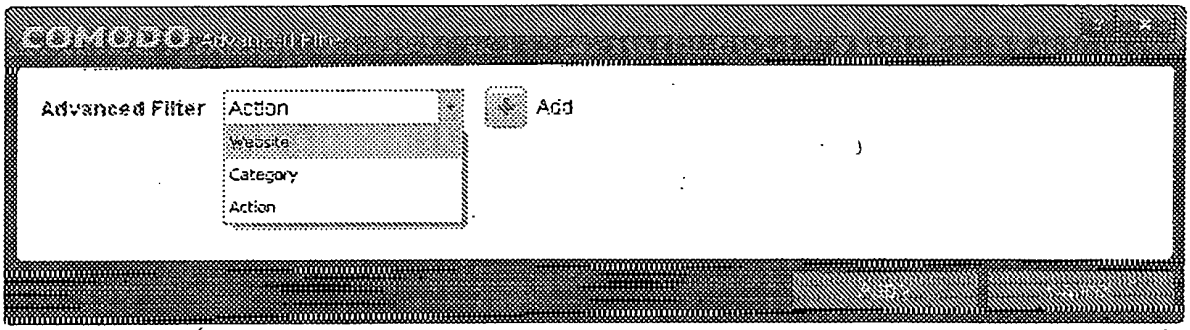
Advanced Filters

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

- **Website** - Displays only the events that involve a specific website
- **Category** - Displays only the events that involve attempts to access the websites of the specified category
- **Action** - Displays only the events that involved the specified action

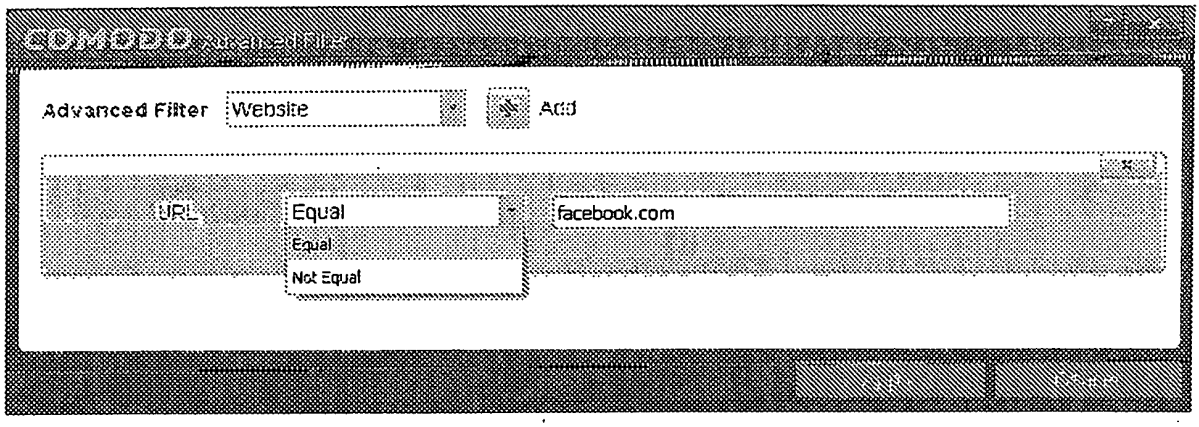
To configure Advanced Filters for Defense+ events

1. Click the funnel button from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Website Filtering' events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

i. **Website**: Adding the 'Website' option displays a drop-down menu and text entry field.

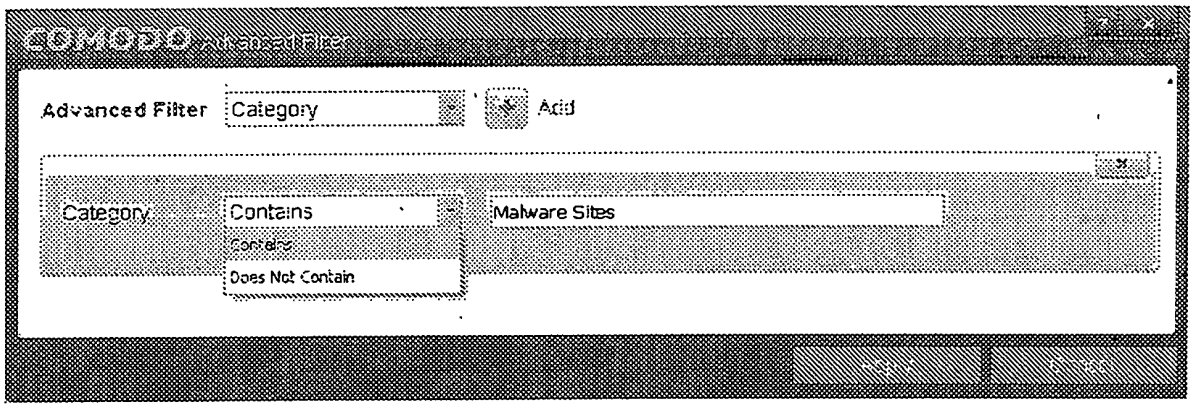


a) Select 'Equal' or 'Not Equal' option from the drop-down menu.

b) Enter the url of the website that needs to be filtered.

For example, if you choose 'Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that involve the website 'facebook.com' in the 'Website' column will be displayed. If you choose 'Not Equal' option from the drop-down and enter the phrase 'facebook.com' in the text field, then all events that do not involve 'facebook.com' will be displayed.

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

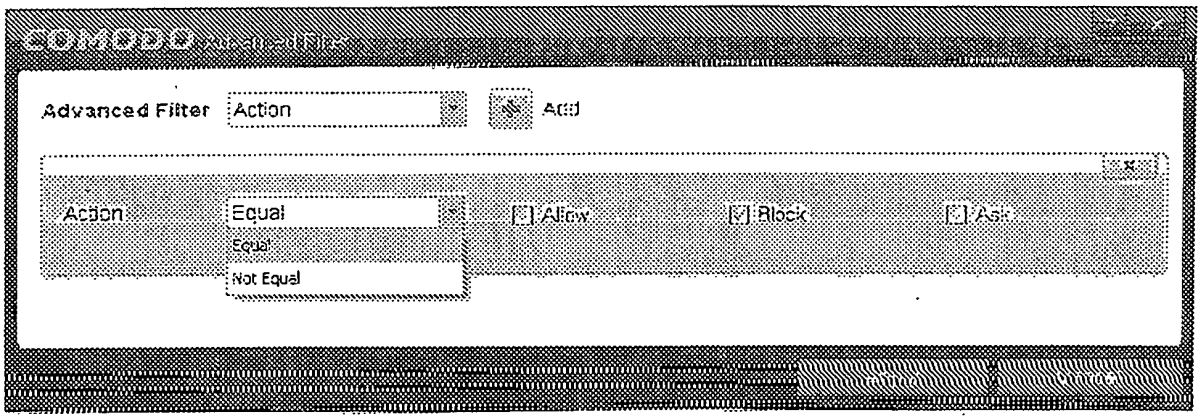


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

b) Enter the predefined category of websites that needs to be filtered from the Category column.

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'Malware Sites' in the text field, then all events that involve the websites falling within the category will be displayed. If you choose 'Does Not Contain' option from the drop-down and enter the phrase 'Malware Sites' in the text field, then all events that do not involve the websites defined within the Malware Sites category will be displayed.

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



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

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

- Allow
- Block
- Ask

For example, if you choose 'Equal' option from the drop-down and select 'Block' from the checkboxes, only the events that involve blocking the access to the websites to the users will be displayed. If you choose 'Not Equal' option from the drop-down and select 'Block' check box, all the events that do not involve blocking the websites will be displayed. You can select more than one check box options from this interface, as required.

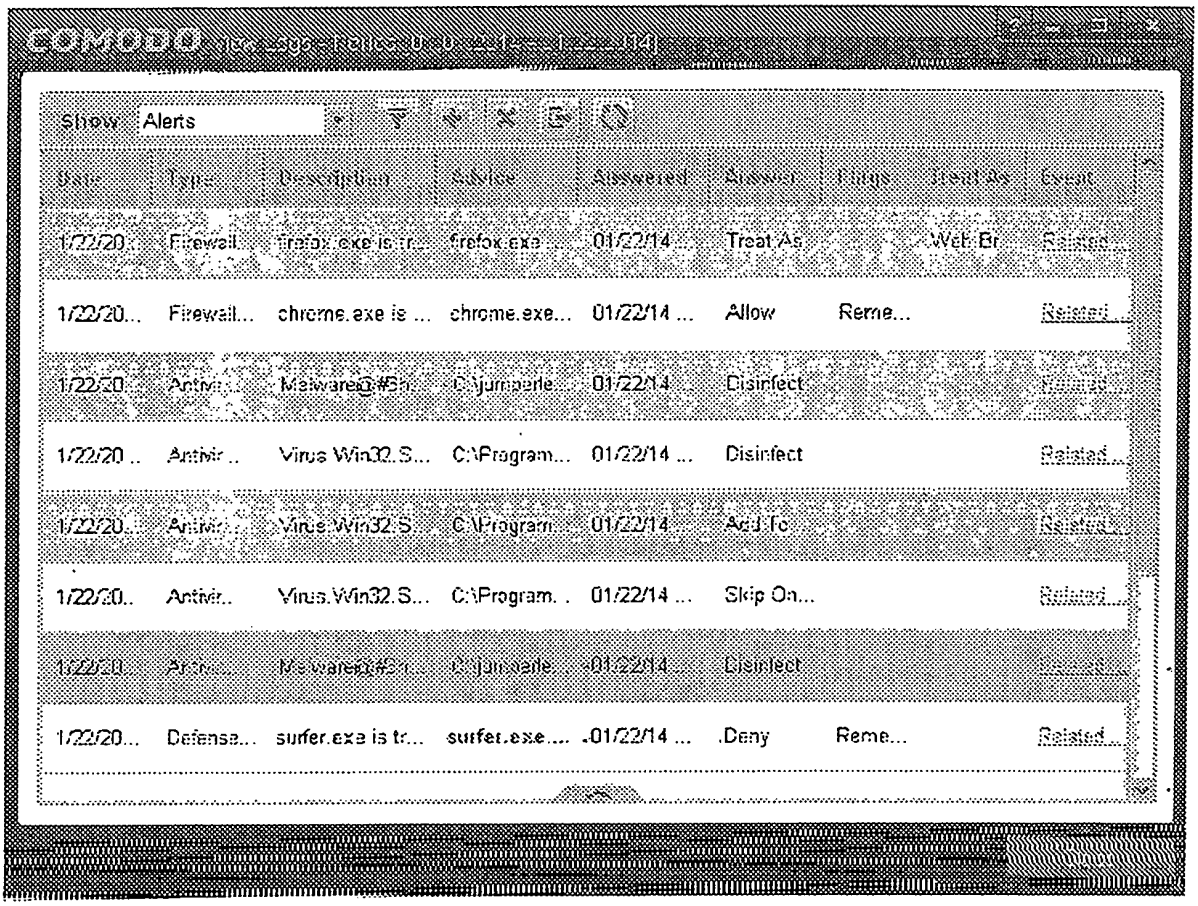
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Website Filtering log viewer. Only those 'Website Filtering' log entries selected based on your filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.5. 'Alerts' Logs

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

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



Column Descriptions

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

- To export the Alerts logs as a HTML file click the 'Export' button  or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button .
- To refresh the Alerts logs, click the 'Refresh' button  or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the Alerts logs click the 'Clear' button .

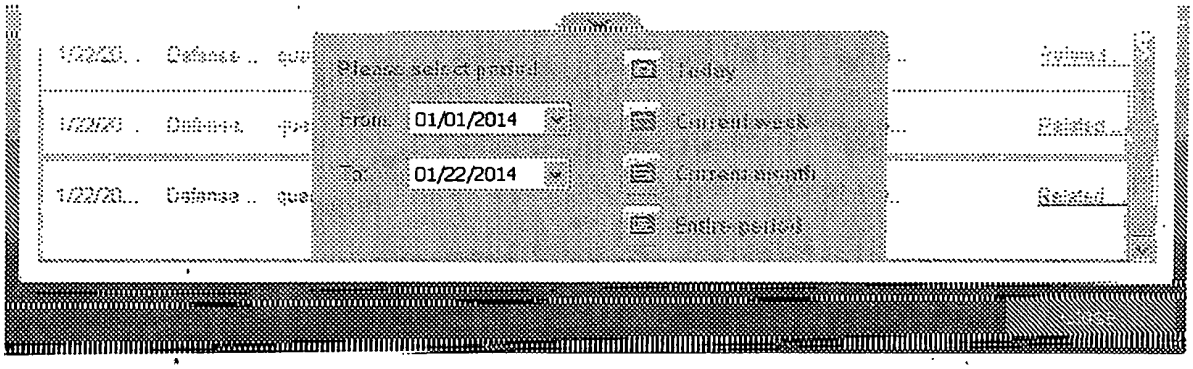
2.6.5.1. Filtering 'Alerts Displayed' Logs

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

- Preset Time Filters
- Advanced Filters

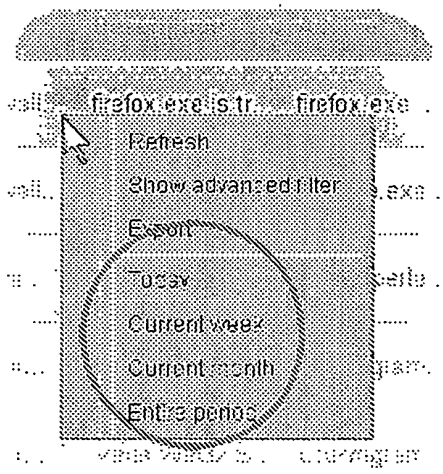
Preset Time Filters

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



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

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



Advanced Filters

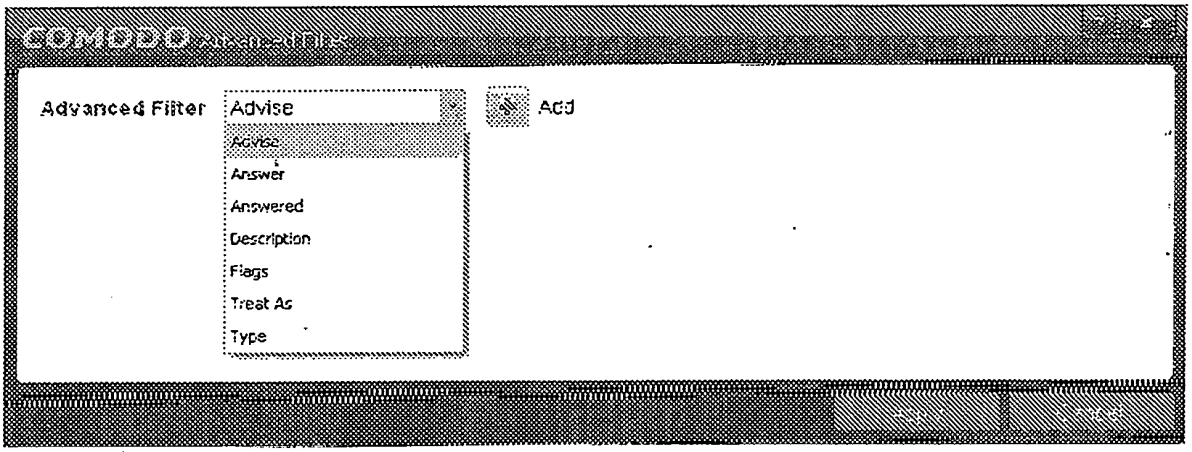
You can further refine the displayed events according to specific filters. Following are available filters for 'Alerts' logs and their meanings:

- **Advice:** Displays only the log of alerts that matches the advice entered

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

To configure Advanced Filters for Alerts Displayed

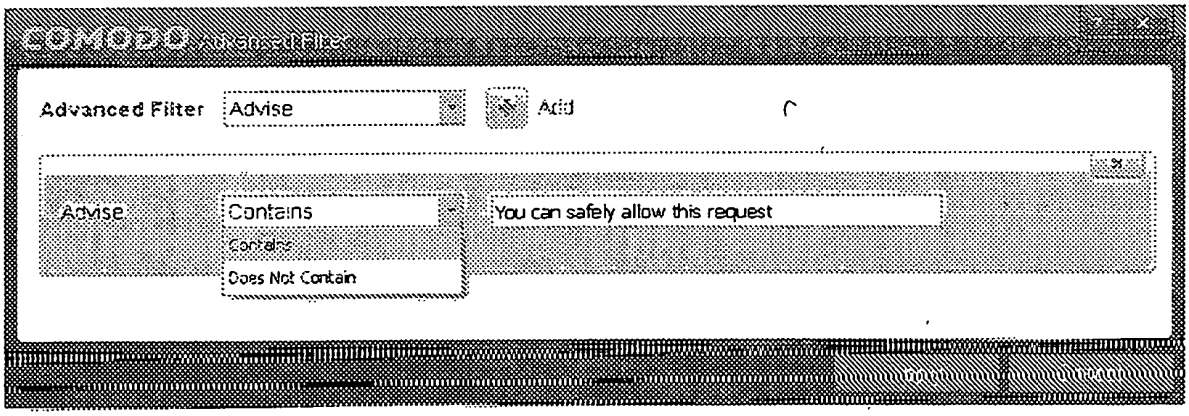
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Alerts' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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

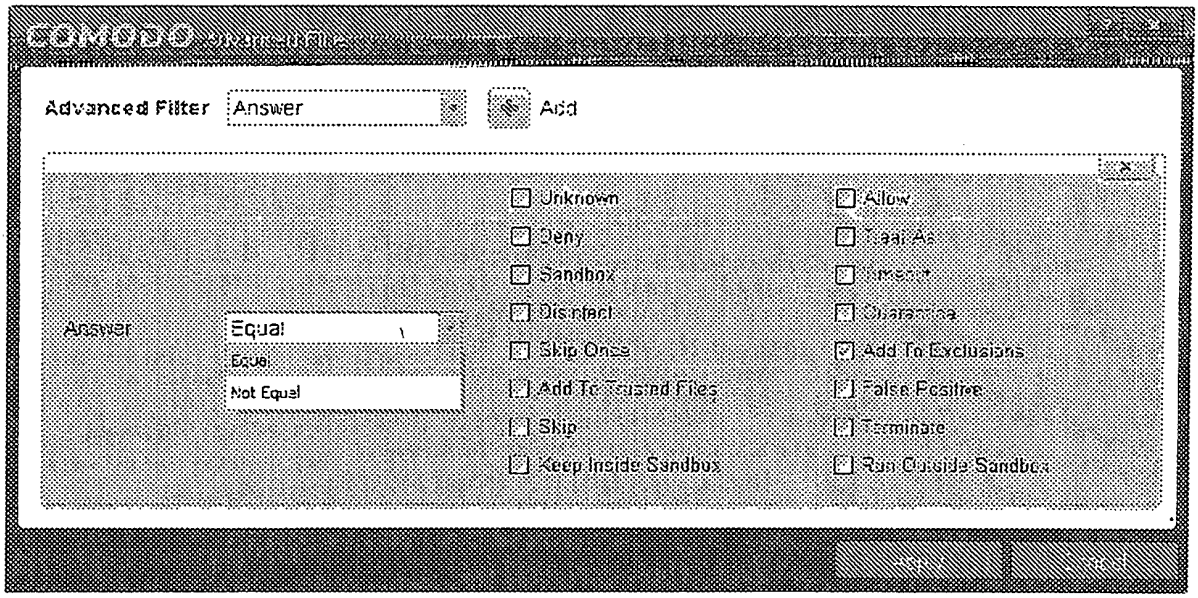


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
b) Enter the text or word as your filter criteria.

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

be displayed.

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



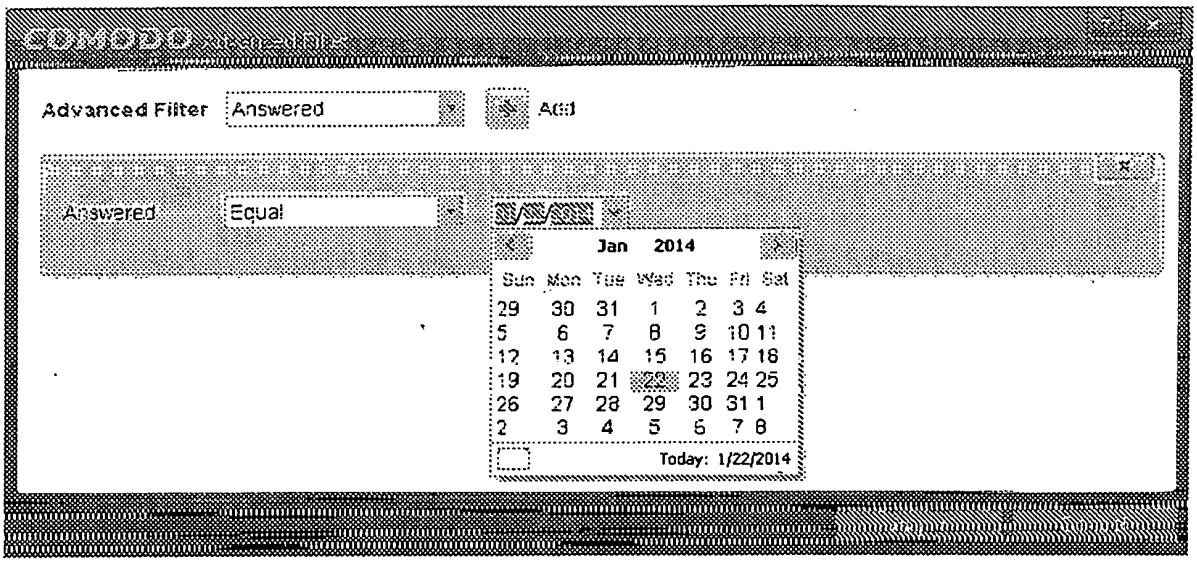
a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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

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

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

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

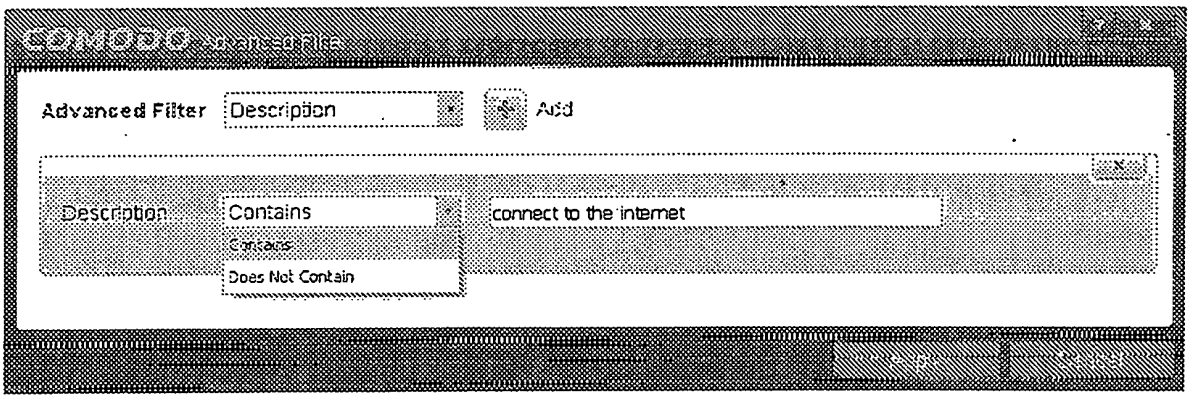


a) Select any one of the following option the drop-down box.
   - Equal
   - Not Equal

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

For example, if you select 'Equal' from the drop-down and select '01/22/2014', only the log of alerts answered on 01/22/2014 will be displayed.

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

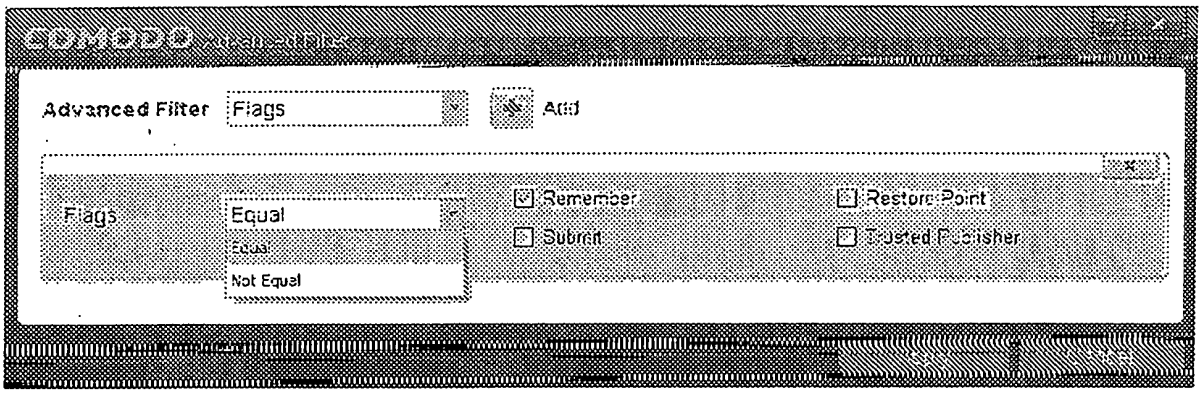


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

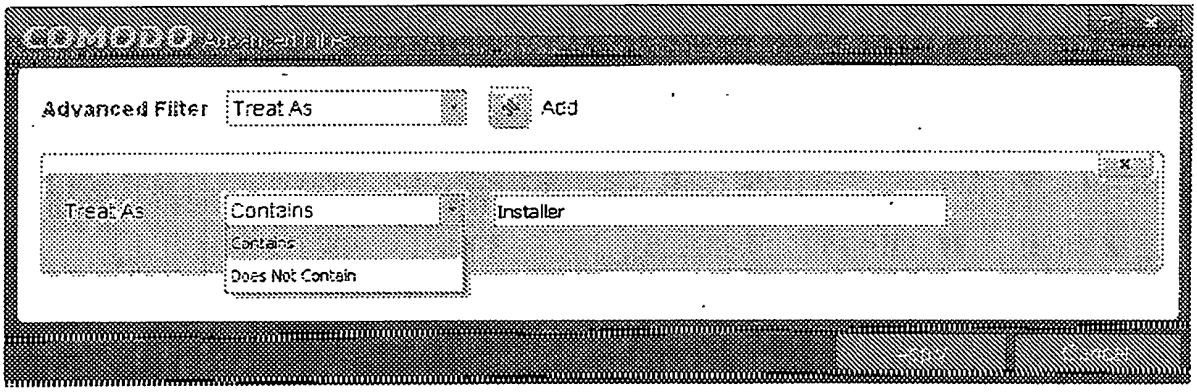
v. **Flags**: The 'Flags' option enables you filter the entries based on the flags set for the kinds of actions against the event triggered by the file. Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.



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

For example, if you choose 'Equal' from the drop-down and select 'Remember' from the checkbox options, only the log entries of alerts for which 'Remember my answer' option was selected will be displayed.

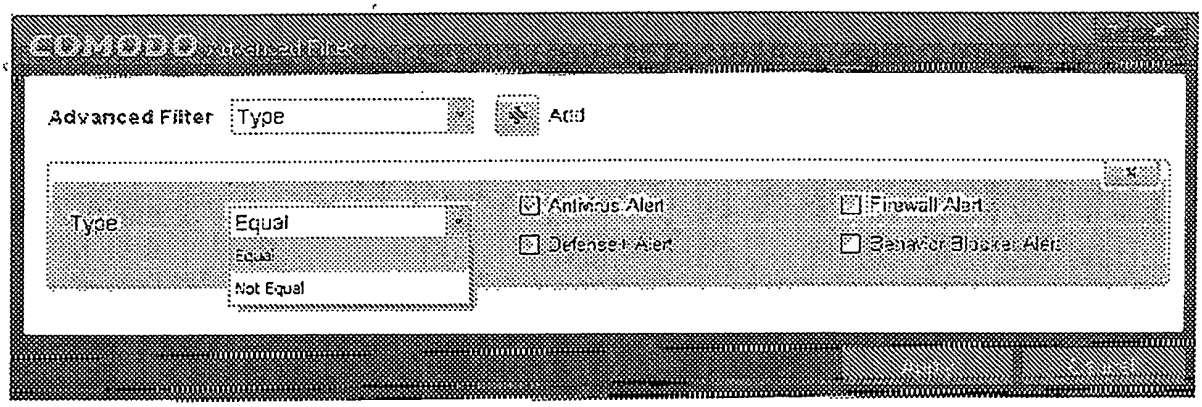
vi. **Treat As**: The 'Treat As' enables you to filter the log entries based on their 'Treat As' response you entered in the pop-up alert. Selecting the 'Treat As' option displays a drop-down menu and text entry field.



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
b) Enter the text or word as your filter criteria

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

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



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

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

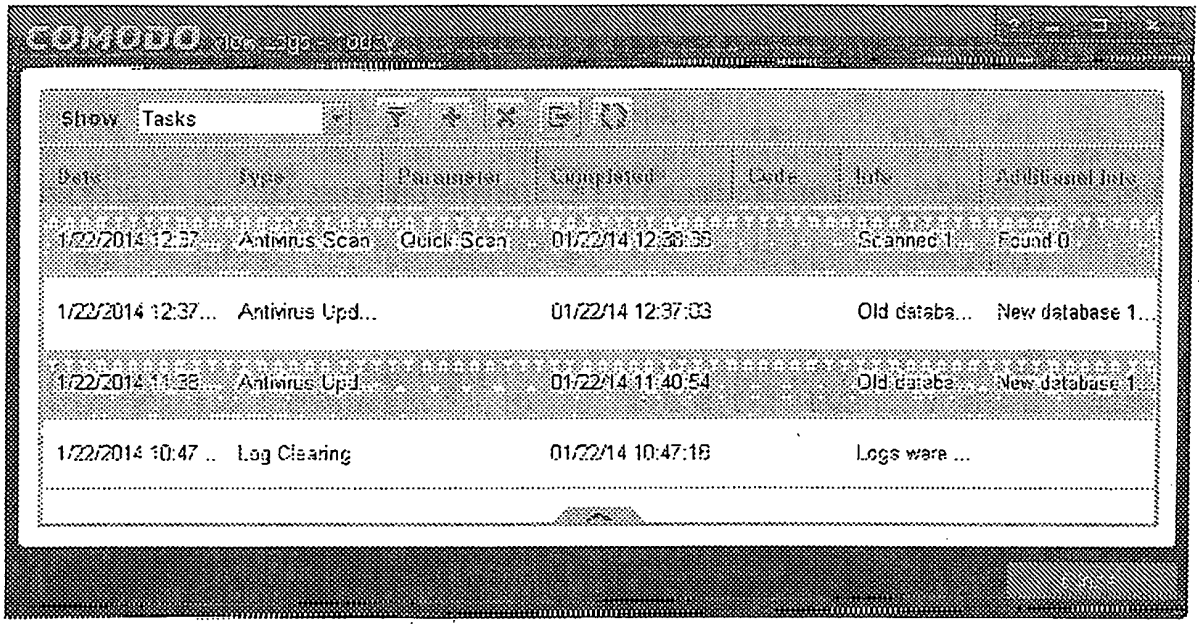
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the 'Alerts' log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.6. Tasks

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

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



Column Descriptions

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

- To export the Tasks logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button.
- To refresh the Tasks logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the Tasks logs click the 'Clear' button.

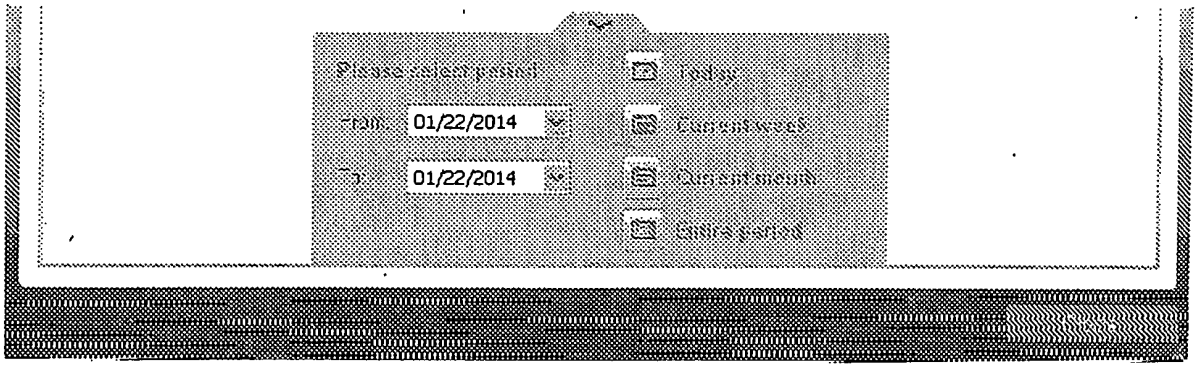
2.6.6.1. Filtering 'Tasks Launched' Logs

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

- Preset Time Filters
- Advanced Filters

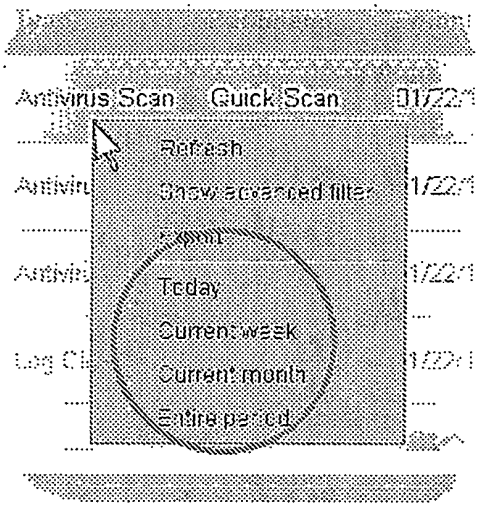
Preset Time Filters

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



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

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



Advanced Filters

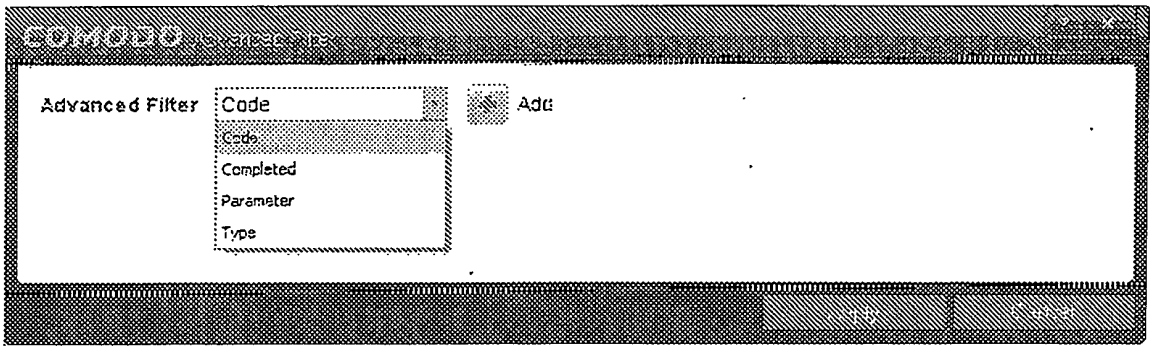
You can further refine the displayed events according to specific filters. Following are available filters for 'Tasks' logs and their meanings:

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

To configure Advanced Filters for 'Tasks' logs

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Tasks log viewer will open.

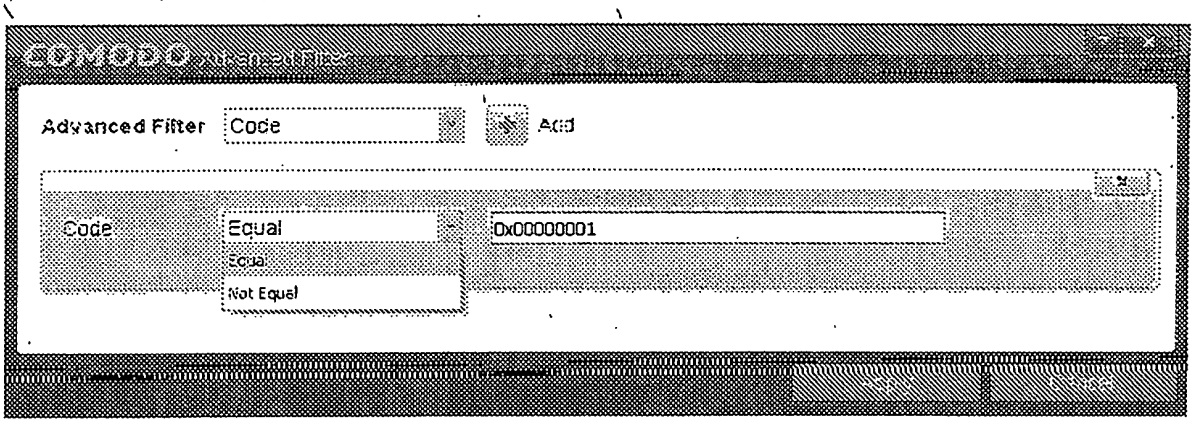
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

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

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

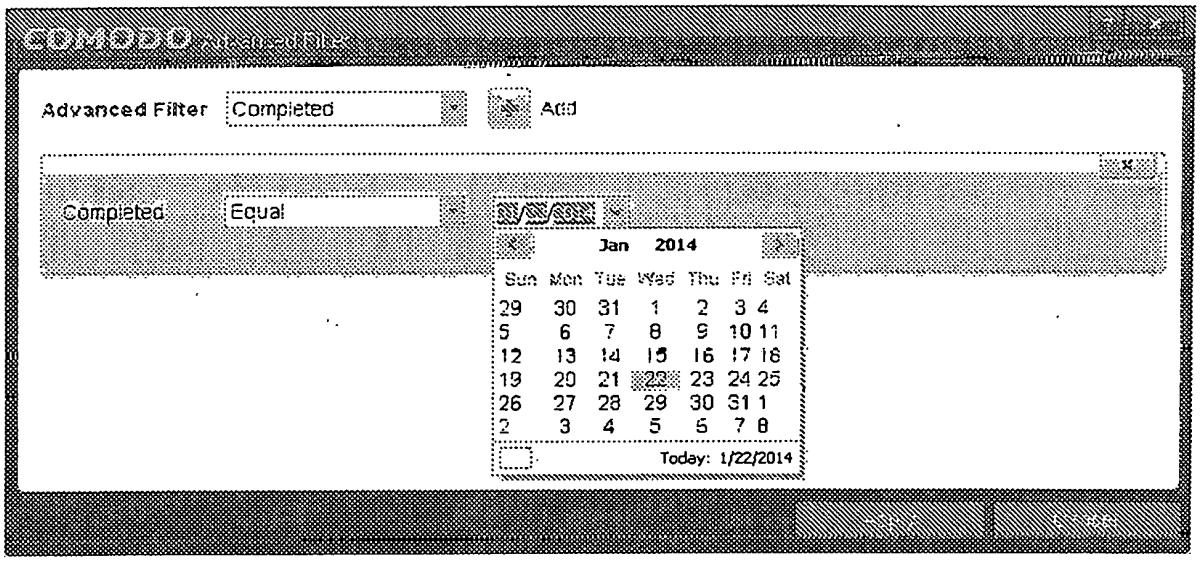


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.

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

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

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

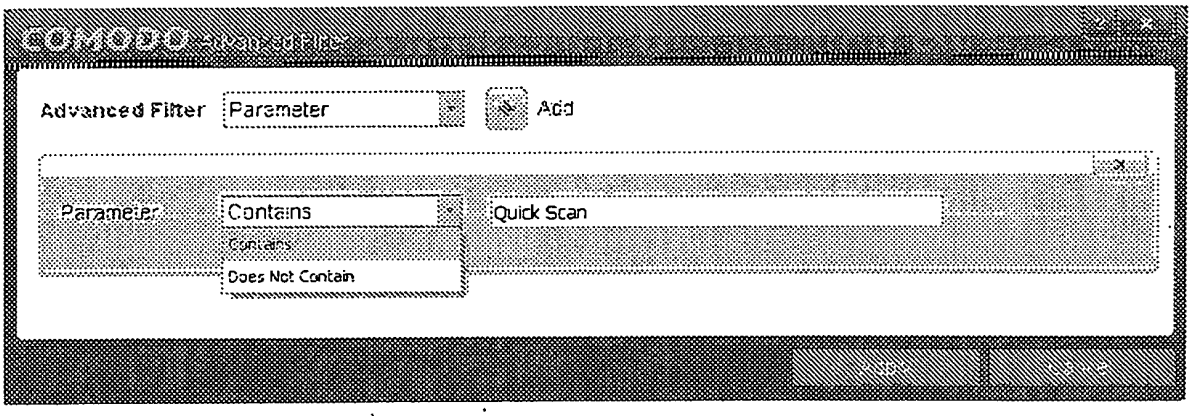


a) Select any one of the following option the drop-down box.
   - Equal
   - Not Equal

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

For example, if you select 'Equal' from the drop-down and select '01/22/2014', only the log of Tasks completed on 01/22/2014 will be displayed.

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

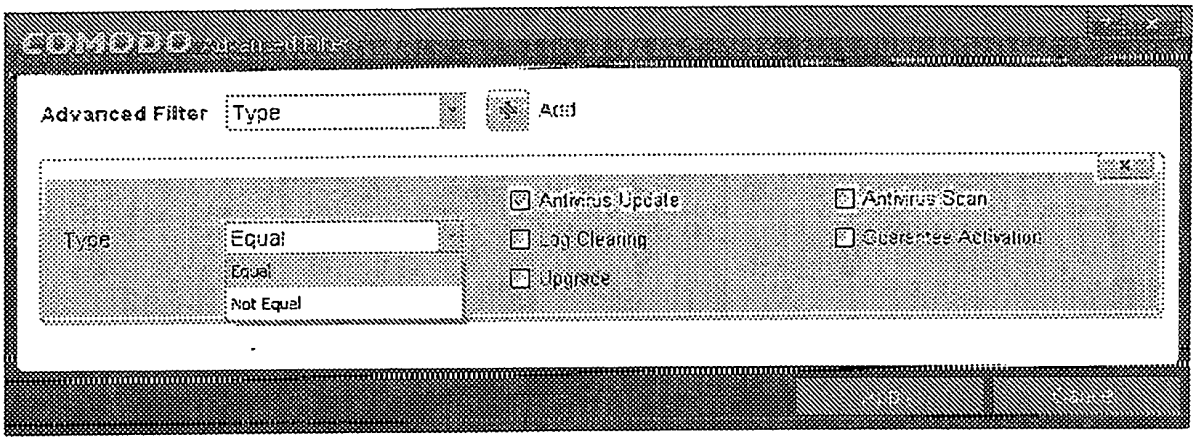


a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

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

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



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

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

- Antivirus update
- Antivirus Scan
- Clearing Logs
- Activation of guarantee
- Version upgrade

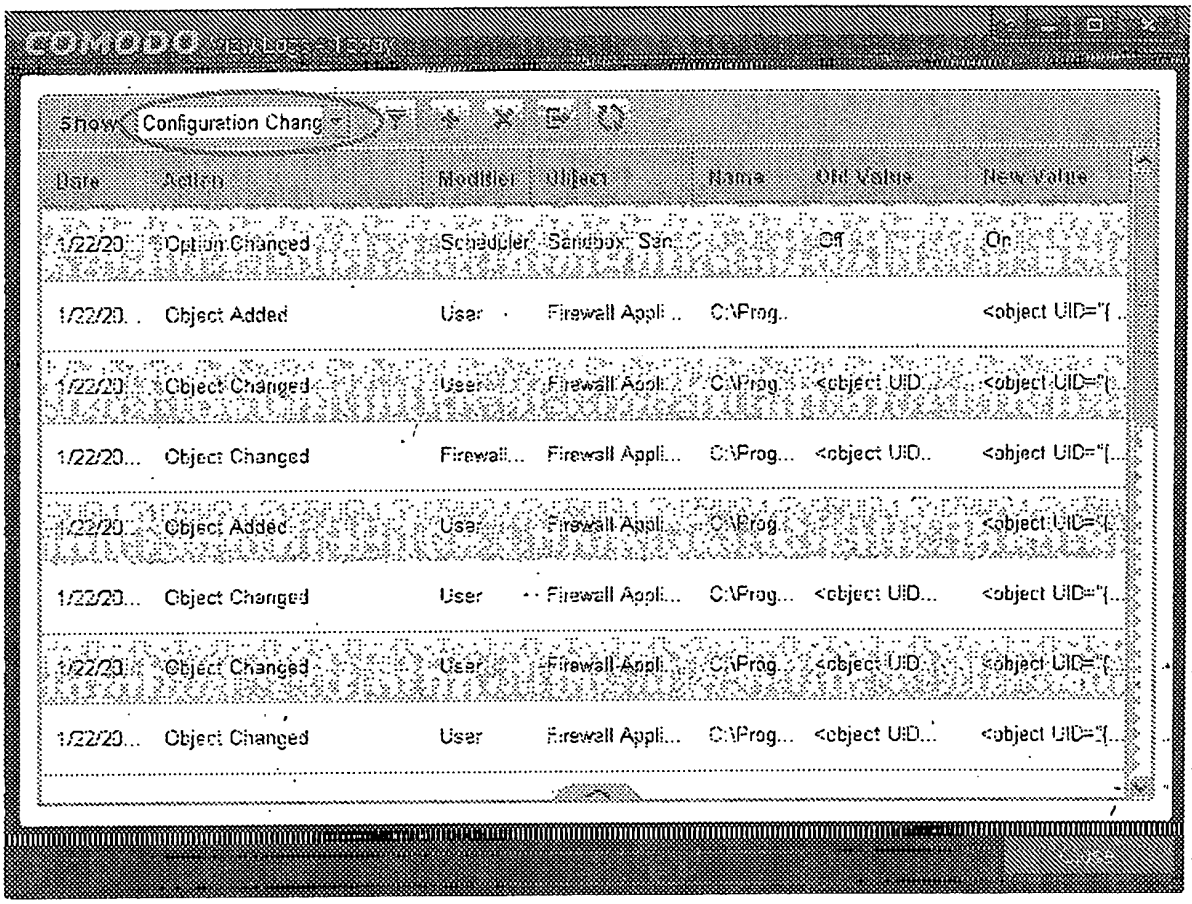
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Tasks log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.6.7. Configuration Changes

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

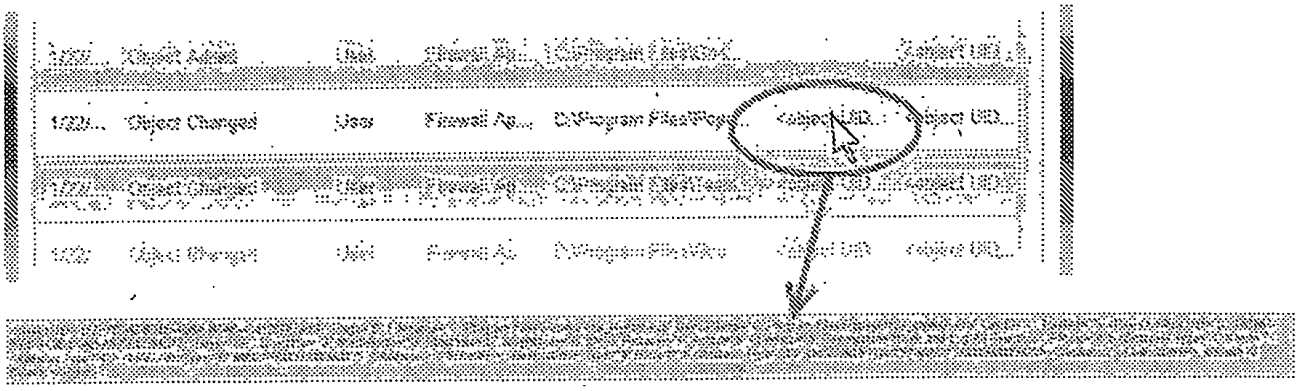
The 'Configuration Changes' logs can be viewed by selecting 'Configuration Changes' from the 'Show' drop-down of the log viewer interface.



Column Descriptions

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

- To view the full details of a configuration change, place the mouse cursor on the entry in the Old Value or New Value column of the respective row.



- To export the Configuration Changes logs as a HTML file click the 'Export' button or right click inside the log viewer and choose 'Export' from the context sensitive menu.
- To open a stored CIS log file, click the 'Open' button.
- To refresh the Configuration Changes logs, click the 'Refresh' button or right click inside the log viewer and choose 'Refresh' from the context sensitive menu.
- To clear the Configuration Changes logs click the 'Clear' button.

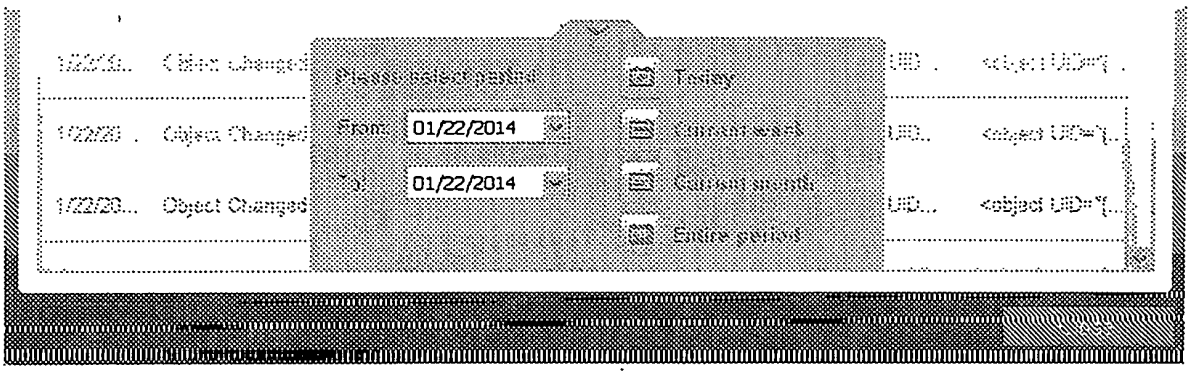
2.6.7.1. Filtering 'Configuration Changes' Logs

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

- Preset Time Filters
- Advanced Filters

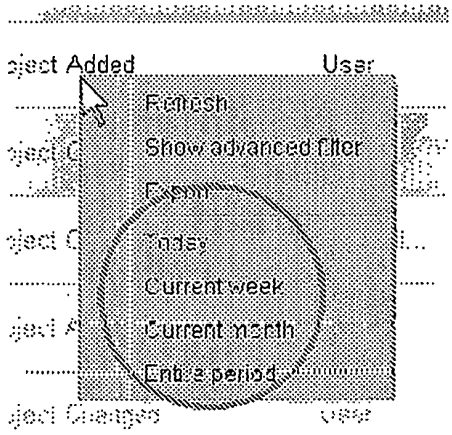
Preset Time Filters

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



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

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



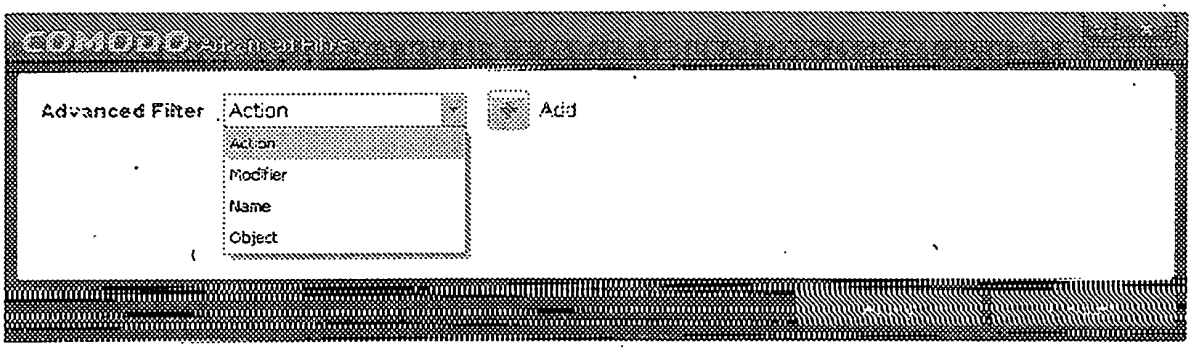
Advanced Filters

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

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

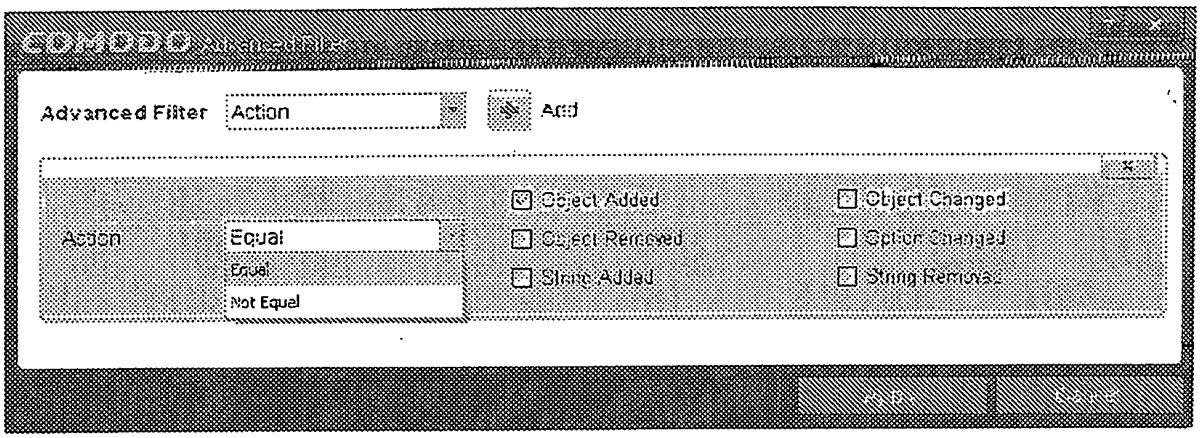
To configure Advanced Filters for Configuration Changes Logs

1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Configuration Changes' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.



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

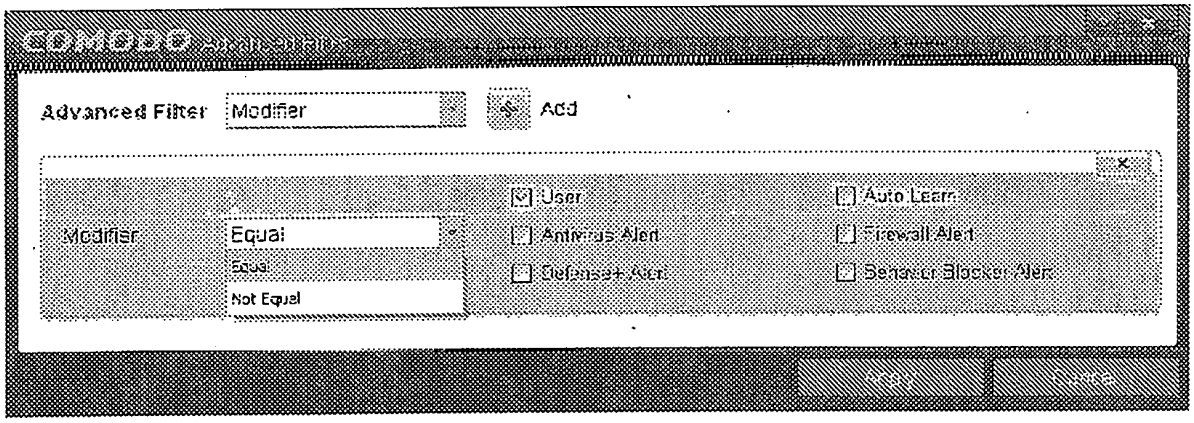
i. **Action:** The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.



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

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

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

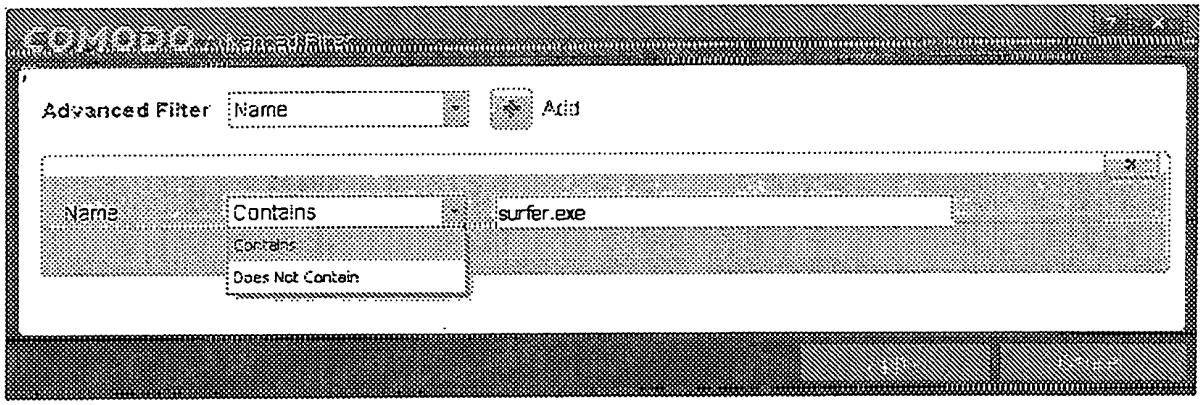


a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:
   - User
   - Auto Learn
   - Antivirus Alert
   - Firewall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

For example, if you have chosen Equal in the drop-down and selected 'Antivirus Alert' checkbox, then only the log

entries related to the configuration changes effected by responses to Antivirus Alerts will be displayed.

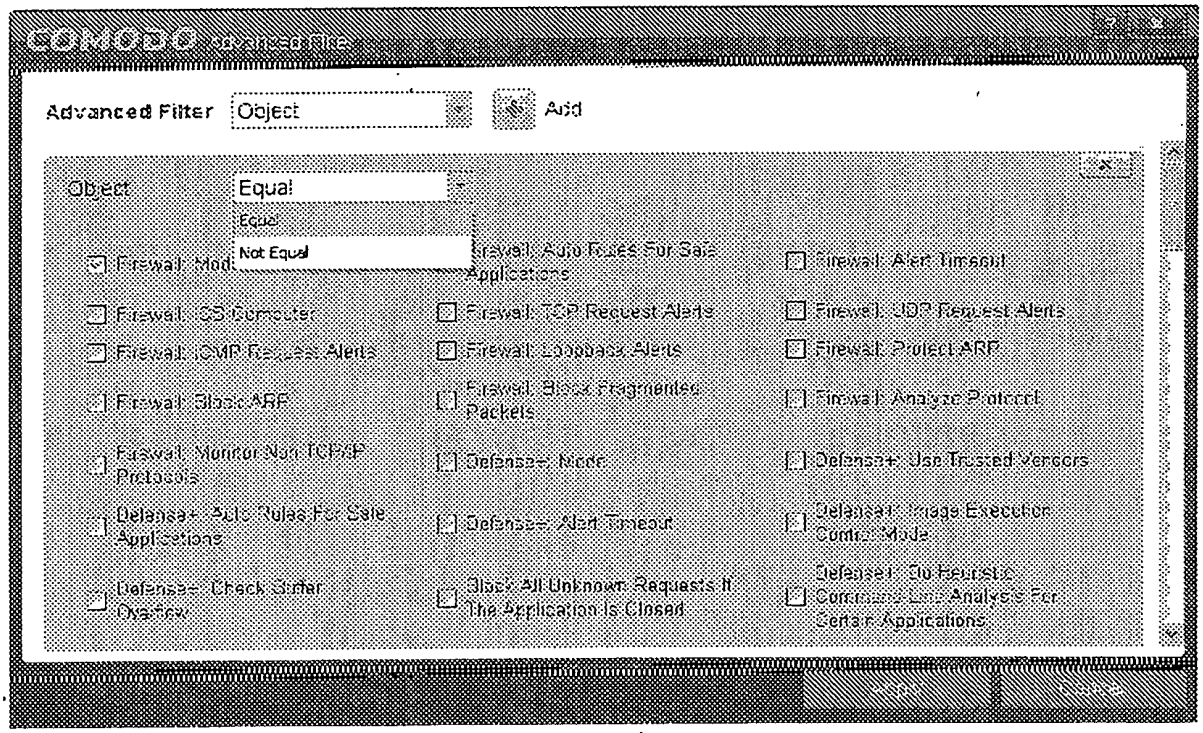
iii. **Name**: The 'Name' option allows you to filter the log entries by entering the name of the parameter changed. Selecting the 'Name' option displays a drop-down field and text entry field.



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

For example, if you choose 'Contains' option from the drop-down and enter the phrase 'surfer.exe' in the text field, then only the log entries containing the surfer.exe in the name column will be displayed.

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



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

For example, if you have chosen 'Equal' from the drop-down and selected 'Firewall: Mode ' checkbox, only the log entries related to the change of Firewall mode will be displayed.

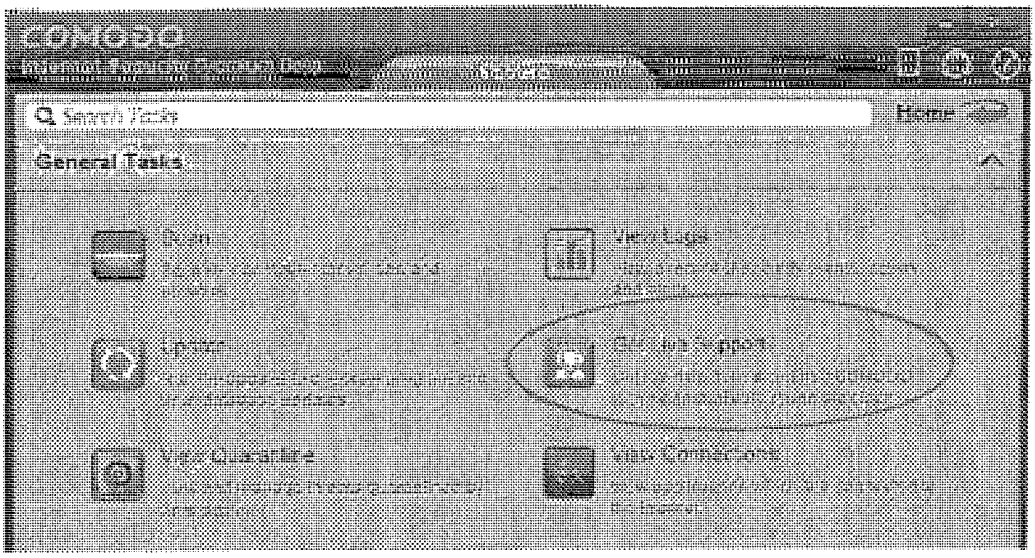
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and

click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- Click 'Apply' for the filters to be applied to the Configuration Changes log viewer. Only those entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button at the top right of each filter pane and click 'Apply'.

2.7. Get Live Support

Opens the GeekBuddy instant-chat client and connects you to a Comodo support technician.



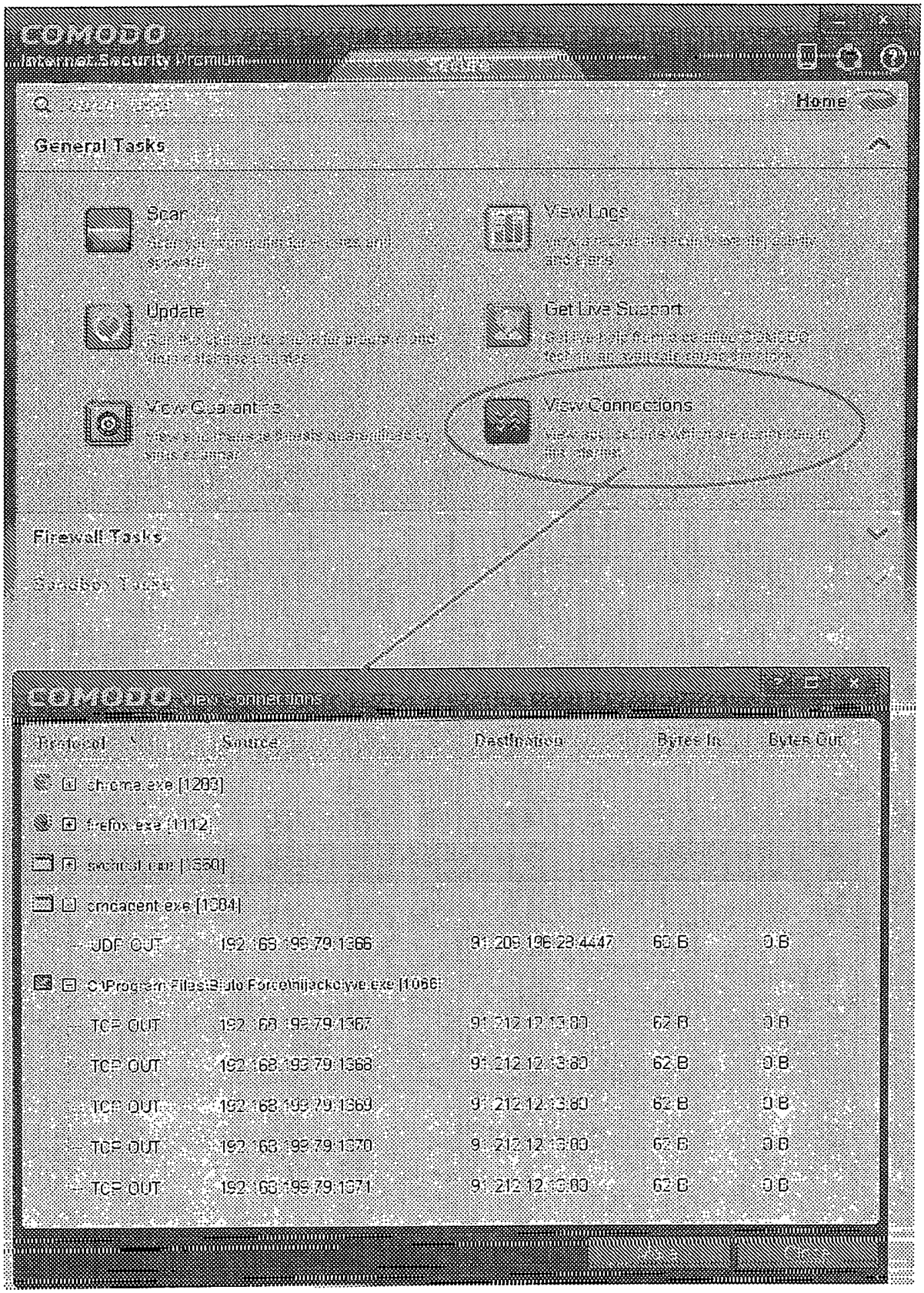
GeekBuddy technicians can help solve most computer issues that you are experiencing. Do you need help to get rid of a particularly nasty virus? Has your computer slowed down to a crawl for no apparent reason? Are you having trouble setting up that wireless router you just bought? GeekBuddy techs can offer you expert guidance and, with your permission, can even remote-desktop into your computer and fix your problems while you sit back and watch. For more details about this service, please refer to Comodo GeekBuddy.

2.8. View Active Internet Connections

The 'View Connections' interface displays an at-a-glance summary of all currently active Internet connections on a per-application basis. You can view all the applications that are connected; all the individual connections that each application is responsible for; the direction of the traffic; the source IP and port and the destination IP and port. You can also see the total amount of traffic that has passed in and out of your system over each connection.

This list is updated in real time whenever an application creates a new connection or drops an existing connection. The 'View Connections' is an extremely useful aid when testing firewall configuration; troubleshooting new firewall policies and rules; monitoring the connection activity of individual applications and your system as a whole and for terminating any unwanted connections.

The 'View active Connections' interface can be accessed by clicking 'View Connections' from the 'General Tasks' interface. Alternatively, this screen can be accessed by clicking the number above Inbound or Outbound in the Advanced View of the Home screen in the Firewall pane.



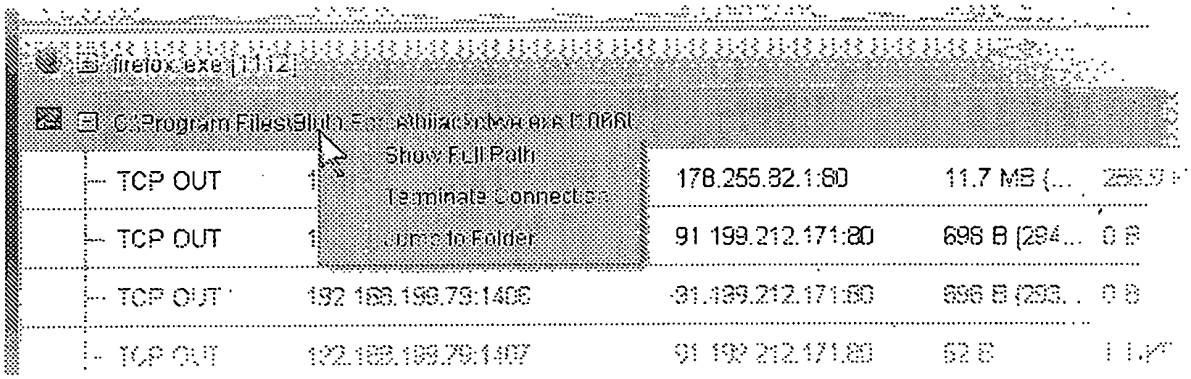
The 'View Connections' interface displays list of all the currently active Internet connections by initiated by various applications as a Tree structure.

Column Descriptions

- **Protocol** - Shows the application that is making the connection, the protocol it is using and the direction of the traffic. Each application may have more than one connection at any time. Clicking + at the left of the application name expands the list of connections made by it.
- **Source (IP : Port)** - The source IP Address and source port that the application is connecting through. If the application is waiting for communication and the port is open, it is described as 'Listening'.
- **Destination (IP : Port)** - The destination IP Address and destination port address that the application is connecting to. This is blank if the 'Source' column is 'Listening'.
- **Bytes In** - Represents the total bytes of incoming data since this connection was first allowed.
- **Bytes Out** - Represents the total bytes of outgoing data since this connection was first allowed.

Context Sensitive Menu

- Right click on an item in the list to see the context sensitive menu.



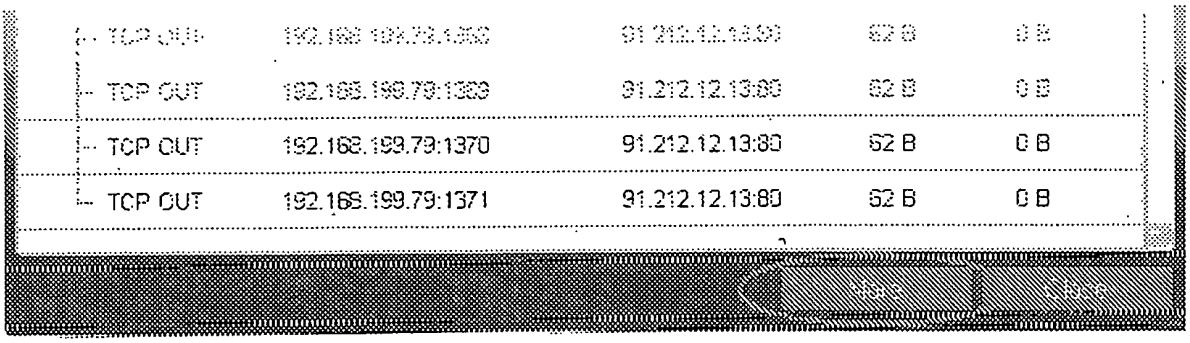
- If you wish to view the full path of the application, right click on the application name and select 'Show Full Path'.
- If you wish to terminate a connection belonging to an application, right click on the specific connection and click 'Terminate Connection'.
- If you wish to open the folder containing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

Identify and Kill Unsafe Network Connections

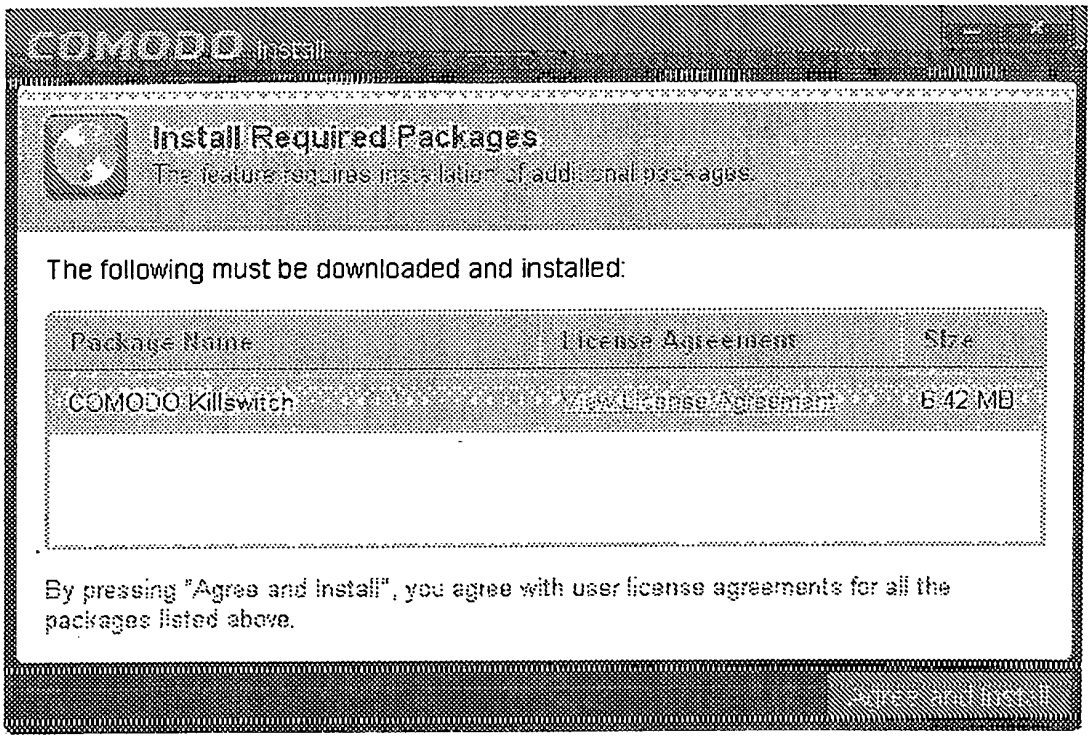
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides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

Comodo KillSwitch can show ALL running processes in granular detail– exposing even those that were invisible or very deeply hidden. You can simultaneously shut down every unsafe process with a single click and can even trace the process back to the parent malware.

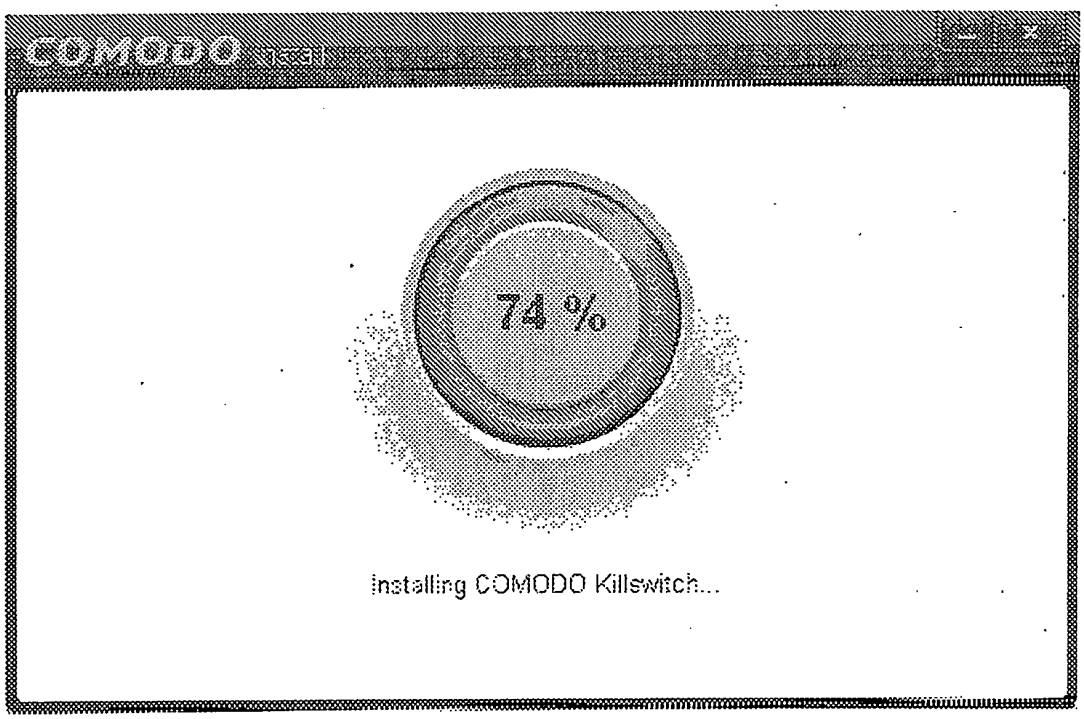
Comodo KillSwitch can be directly accessed from the 'View Connections' by clicking the 'More' button.



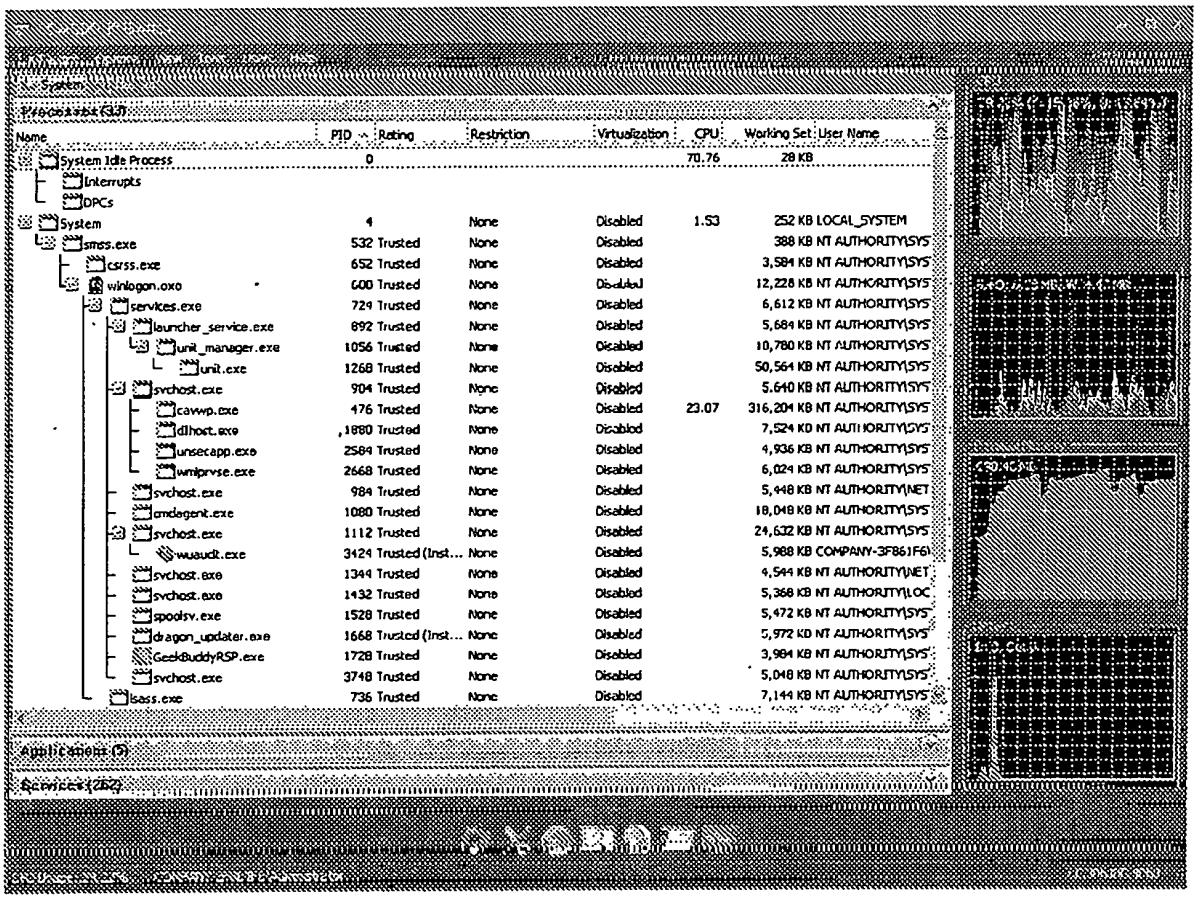
If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



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



On completion of installation, the Comodo KillSwitch main interface will be opened. Clicking the Network tab will display the the Network Connections and Network Utilization panes.



- Details of how to use KillSwitch to view granular details on current network connections and terminate unsafe connections can be found at http://help.comodo.com/topic-119-1-328-3577-Viewing-and-Handling-Network-Connections-and-Usage.html.
- The complete user guide for Comodo KillSwitch is available at http://help.comodo.com/topic-119-1-328-3518-Introduction-to-KillSwitch.html

2.9. View Active Process List

The Active Process List interface displays all currently active processes initiated by applications that are currently running in the sandbox environment . By tracing an application's parent process, CIS can detect whether a non-trusted application is attempting to spawn an already trusted application and thus deny access rights for that trusted application. This system provides the very highest protection against Trojans, malware and rootkits that try to use trusted software to launch an attack. By default, the list displays the processes of sandboxed applications only, but can be made to display all the processes from the right-click options.

The processes of sandboxed applications include:

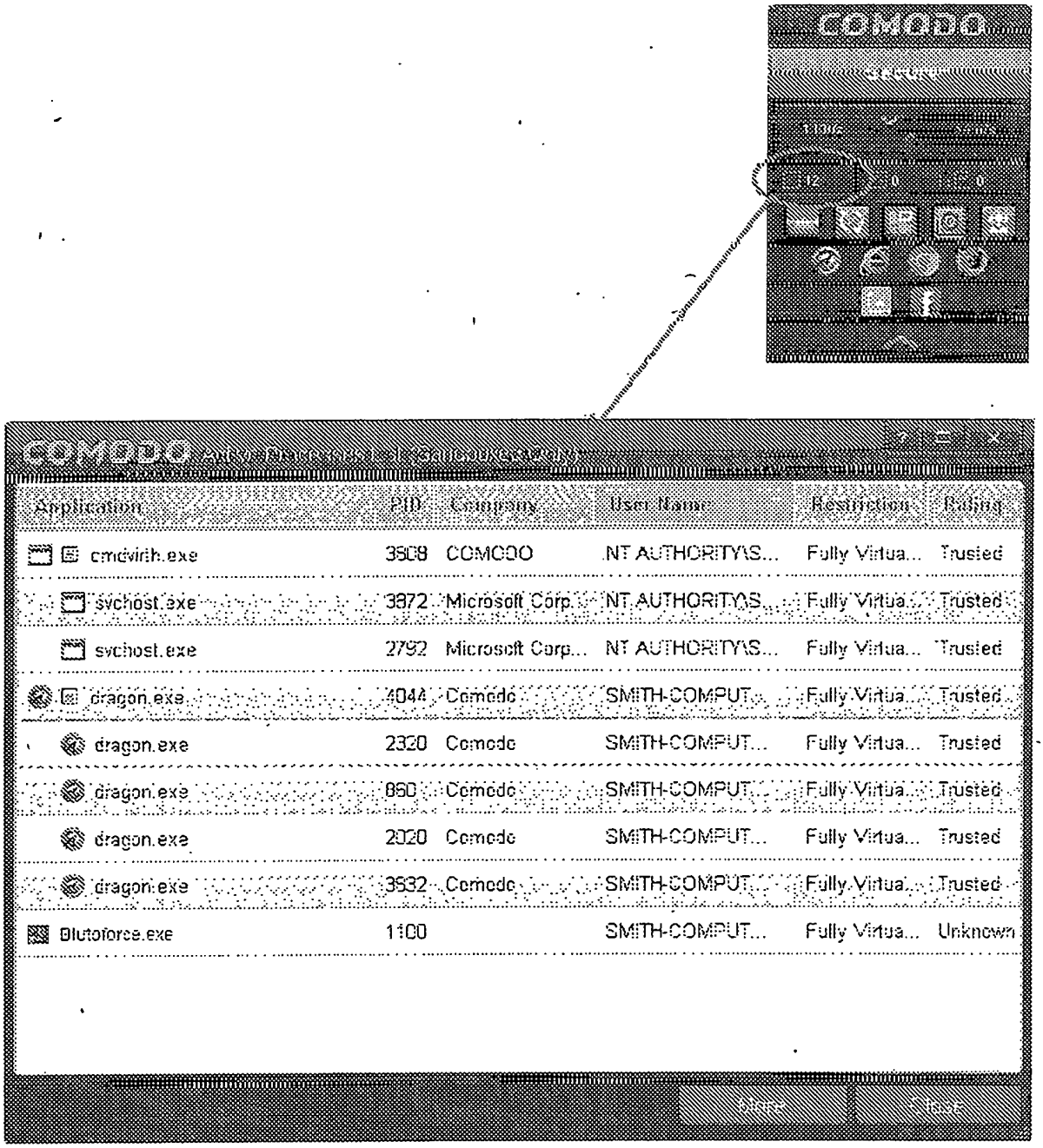
- Auto-Sandbox - Unrecognized applications are run inside the auto sandbox with access restriction as selected in the 'Auto-sandbox unknown applications as' drop down in Behavior Blocker.
- Run Virtual - Applications that are selected and run in Sandbox. Refer to 'Run an Application in the Sandbox' for more details.
- Applications that are run inside the sandbox using the context sensitive menu - Click here for more details.
- Running browsers inside the sandbox from the Widget - Click here for more details.
- Drag-and-drop applications on to CIS Home Screen - Click here for more details.

- Programs that are added manually - Refer to the section 'Configure the Sandbox' for more details.

To view Active Process list

- Click the first box in the status pane (third row) in the CIS Widget.

Note: The Status Pane is not displayed by default in the widget. To enable the Status Pane, right click on the CIS tray icon and select 'Show Status Pane' from the options.



- Alternatively, the screen can be accessed by clicking the number beside 'Sandboxed Apps' in the Advanced View of the Home screen in the Defense+ and Sandbox pane.

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

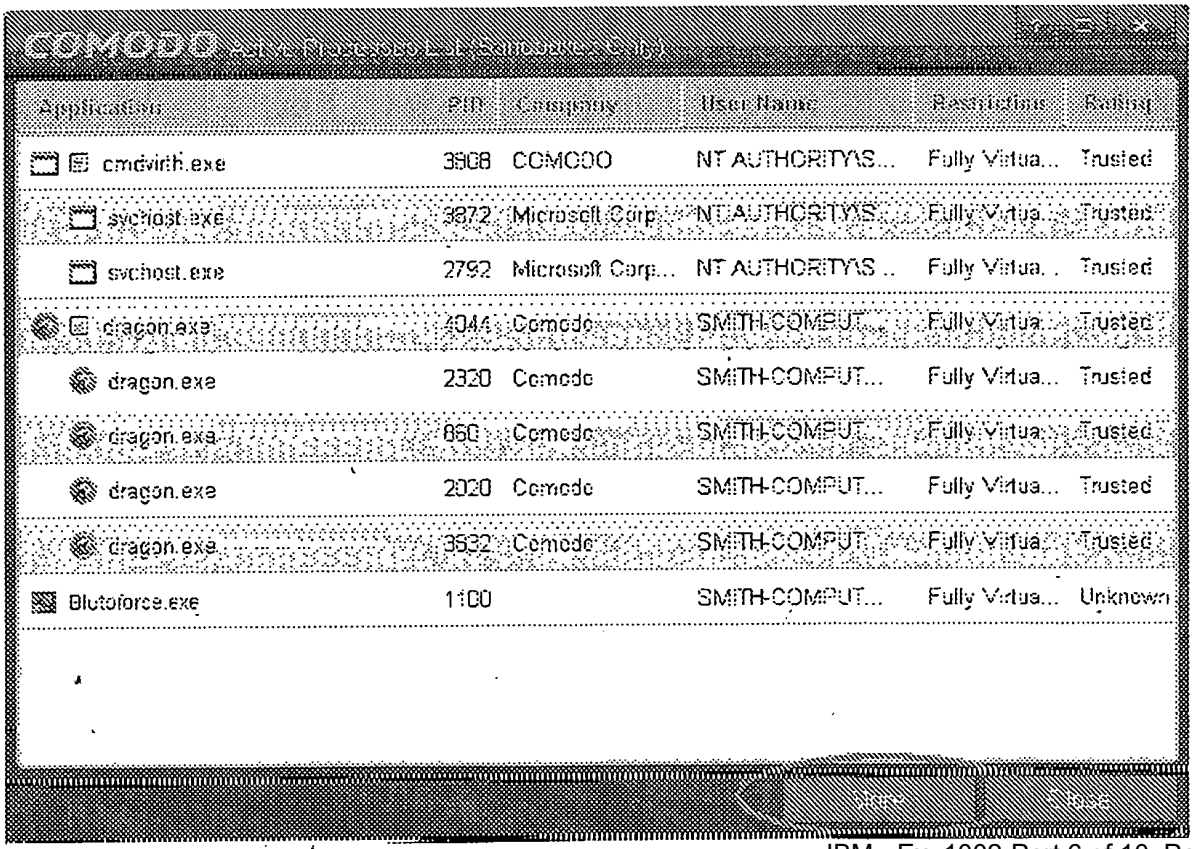
Column Descriptions

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

Right-click on any process to:

- Show full path: Displays the location of the the executable in addition to it's name.
- Show Sandboxed Only: Displays the details of the sandboxed programs only. Disable this option to view all the current active process list.
- Add to Trusted Files: The selected unknown program is added to Trusted Files list.
- Online Lookup: The selected program is compared with the Comodo database of programs and results declared whether it is safe or not.
- Submit: The selected application will be sent to Comodo for analysis.
- Jump to Folder: The folder containing the executable file of the application will open.
- Show Activities: Opens the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application. The 'Show Activities' option is available only if Viruscope is enabled under Advanced Settings > Defense+ > Behavior Blocker Settings.

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



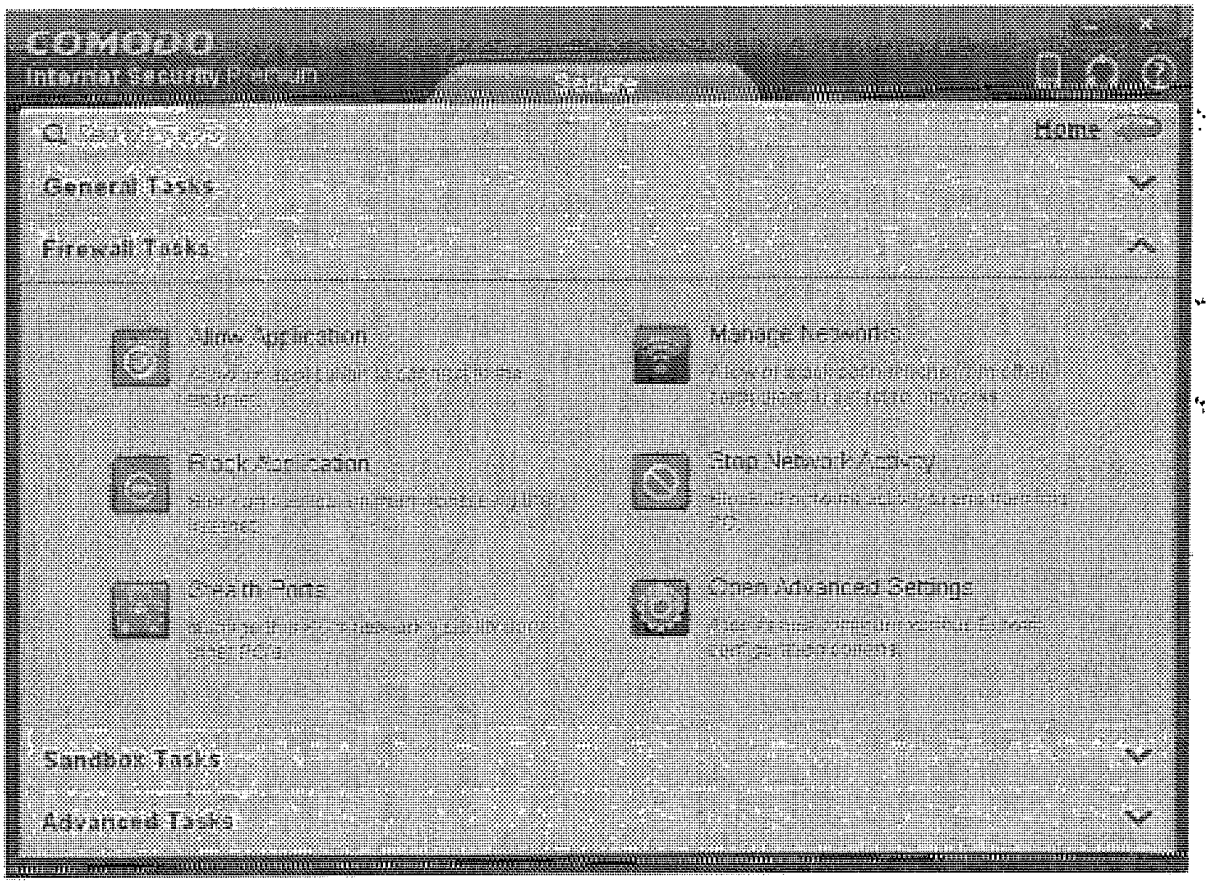
If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the section Identify and Kill Unsafe Processes for more details.

3.Firewall Tasks - Introduction

The Firewall component of Comodo Internet Security (hereafter known simply as Comodo Firewall) offers the highest levels of security against inbound and outbound threats, stealths your computer's ports against hackers and blocks malicious software from transmitting your confidential data over the Internet. Comodo Firewall makes it easy for you to specify exactly which applications are allowed to connect to the Internet and immediately warns you when there is suspicious activity.

It can be accessed at all times by clicking on the 'Firewall Tasks' band from the 'Tasks' interface.

The Firewall Tasks area provides easy access to all major features and settings. From here, you can configure Internet access rights per-application, stealth your computer ports, manage available networks and even block all network traffic in and out of your computer. In 'Advanced Settings' you'll be able to specify overall firewall behavior and configure advanced settings such as application rules, rulesets, network zones and port sets.



Click the links below to see detailed explanations of each area in this section:

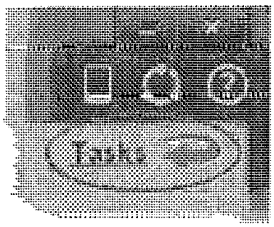
- Allow or block Internet access to applications selectively
- Stealth your computer ports
- Manage network connections
- Stop all network activity
- Advanced firewall settings

3.1. Allow or Block Internet Access to Applications Selectively

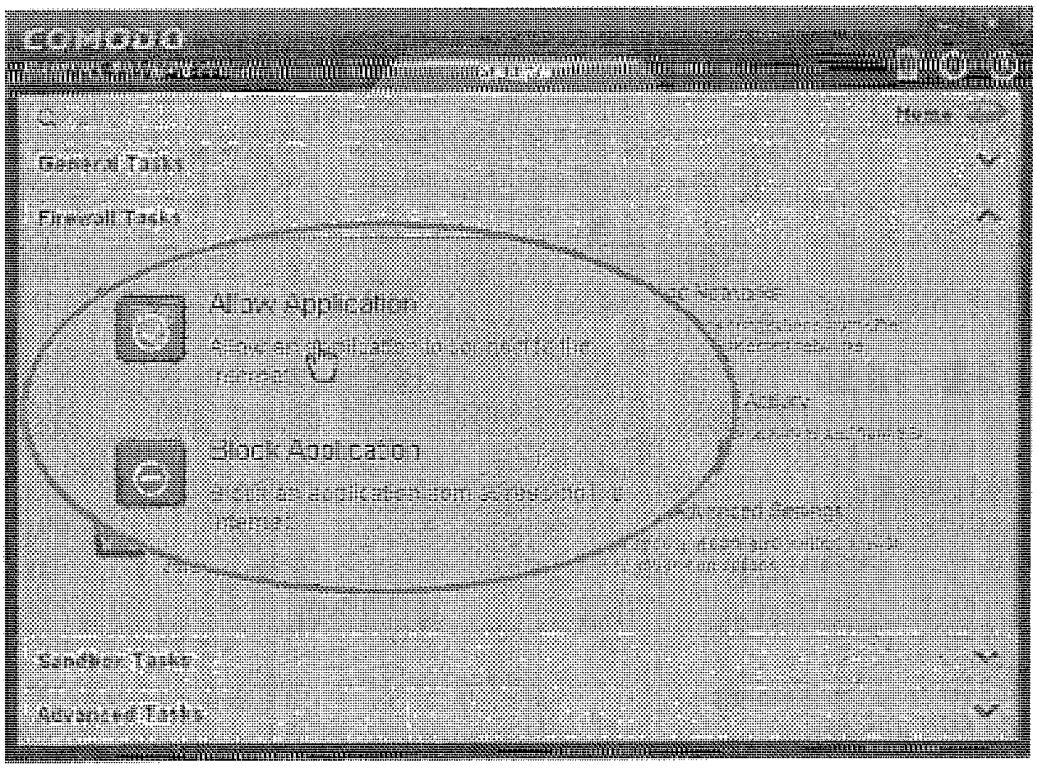
The Firewall Tasks interface allows you to selectively allow or block certain applications from accessing the Internet. These shortcuts represent a convenient way to create an automatic 'Allow Requests' rule or 'Block Requests' rule for individual applications - meaning that inbound and outbound connections are automatically permitted or not permitted to these applications respectively.

To open the 'Firewall Tasks' interface:

- Click the 'Tasks' arrow from the CIS home screen:



- Click on the 'Firewall Tasks' band from the 'Tasks' interface:



To allow an application to access to the Internet:

- Click the 'Allow Application' button from the 'Firewall Tasks' interface.
- Navigate to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to allow Internet access to the selected application.

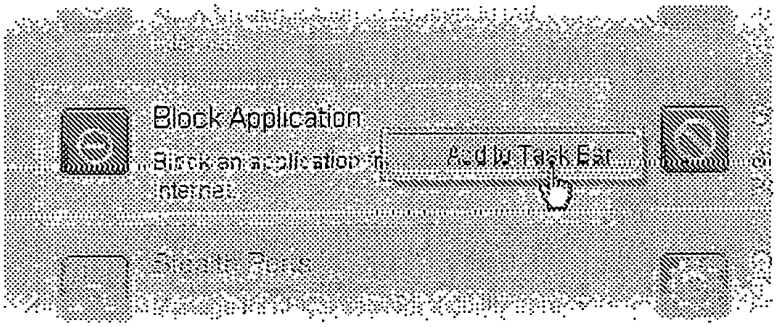
To block an application's Internet access rights

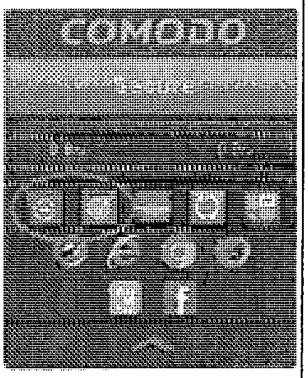
- Click the 'Block Application' button from the 'Firewall Tasks' interface.
- Browse to the main executable of the application in the 'Open' dialog.
- Click 'Open'. A rule will be created to prohibit Internet access to the selected application.

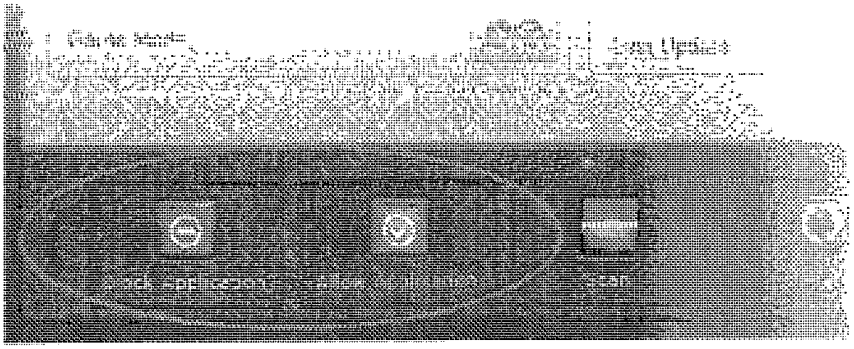
The advanced application rules interface can be accessed by clicking 'Tasks' from the CIS home screen > Firewall Tasks > Open Advanced Settings > Application rules. The application you just allowed or blocked should be listed here. For further information

on application rules governing Internet access rights, see Application Rules.

Tip: if you plan to regularly allow/block applications, you can right click on the appropriate button and select 'Add to Taskbar'. It will then be quickly accessible from both the CIS home screen and the widget:







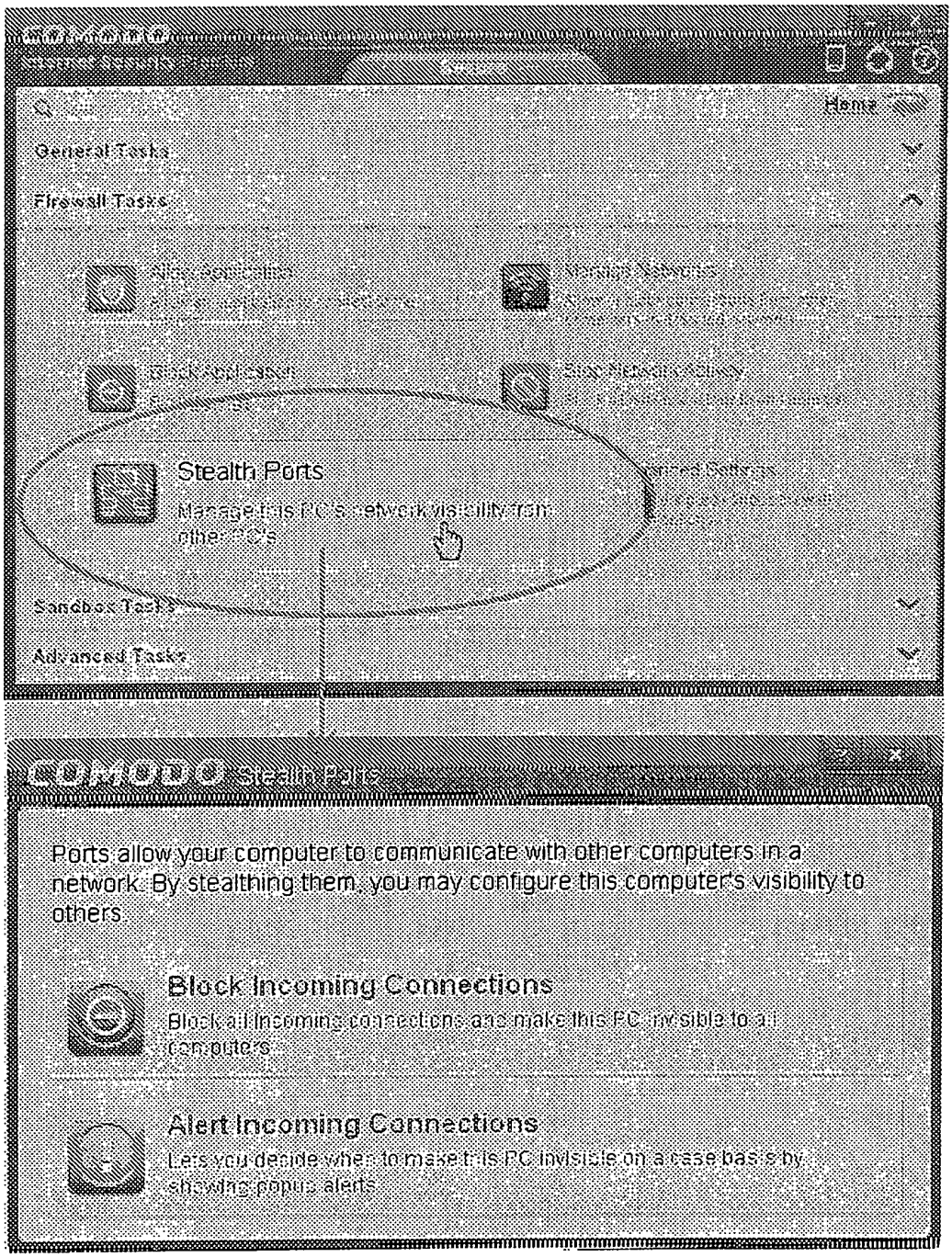
3.2. Stealth your Computer Ports

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

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

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

- Click on 'Stealth Ports' link in Firewall Tasks

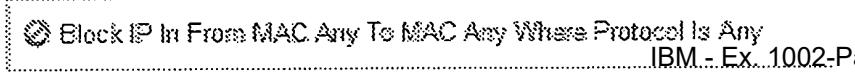


You have two options to choose from:

Block incoming connections

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

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



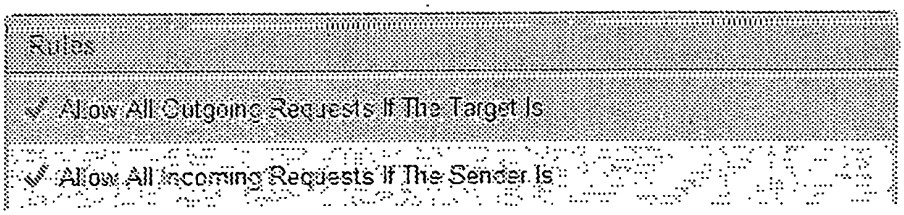
If you would like more information on the meaning and construction of rules, please click here.

Alert incoming connections

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

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

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

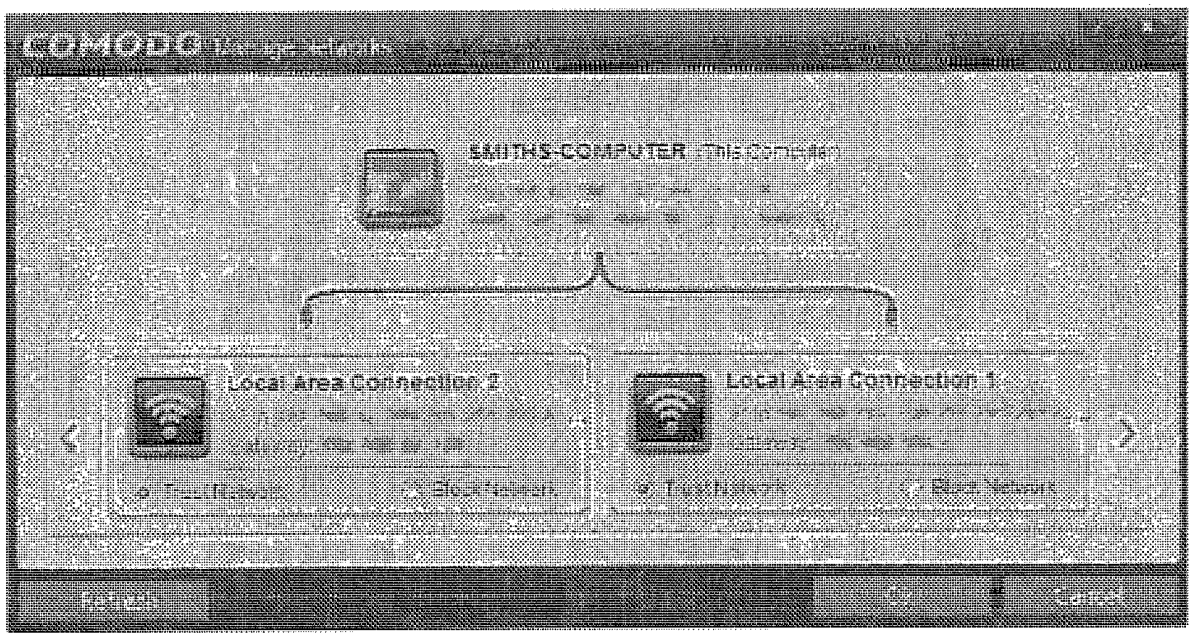


If you would like more information on the meaning and construction of rules, please click here.

3.3. Manage Network Connections

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

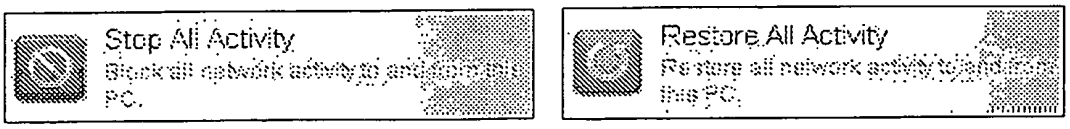
- You can choose to trust or block a network by selecting the appropriate radio button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks.
- Use the handles (< >) to scroll through all available networks or computers
- Use the refresh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



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

3.4. Stop all Network Activities

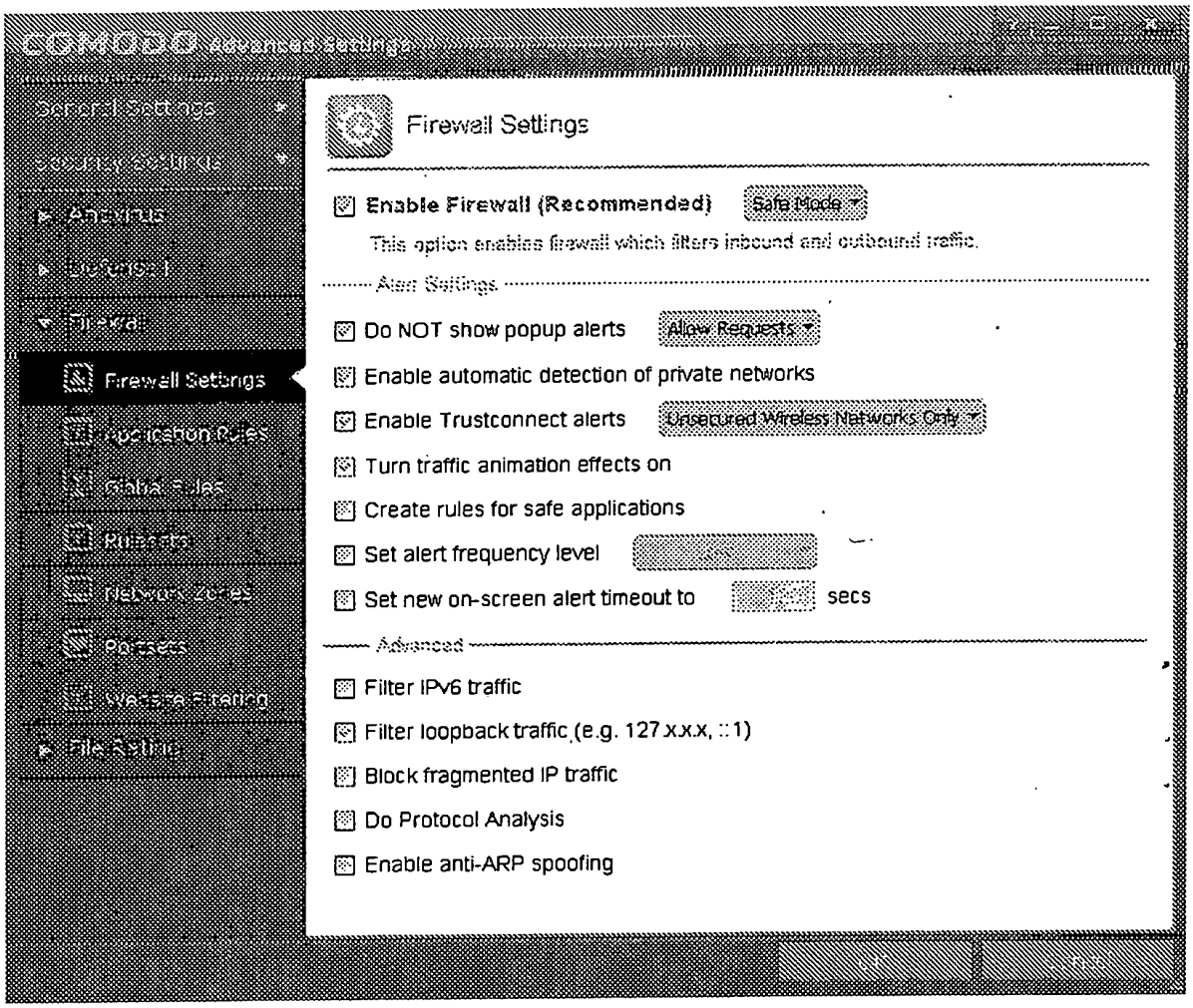
As the name suggests, the 'Stop all network activity' button instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and all available networks (including the Internet). Connections will remained closed until you re-enable them by clicking the button a second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



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

3.5. Advanced Firewall Settings

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



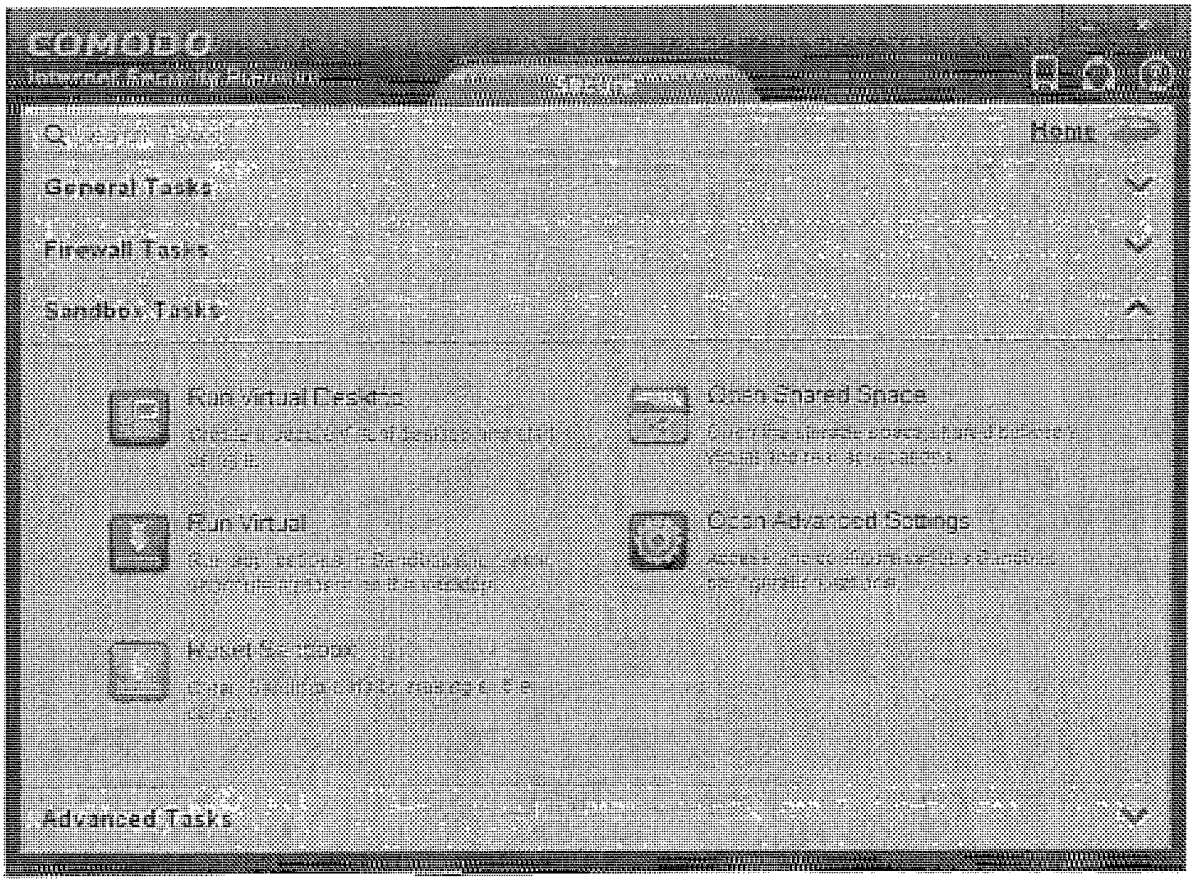
The interface is divided into six main sections - Firewall Settings, Application Rules, Global Rules, Rulesets, Network Zones and Portsets. Click the links below to jump to more details on each section:

- The Firewall Settings area allows you to configure the security of your computer and the frequency of alerts that are generated.
- The Application Rules area allows users to view, manage and define the network and Internet access rights of applications on your system.
- The Global Rules area allows users view, manage and define overall Firewall ruleset that applies to your computer and is independent of application rules.
    - Both application rules and global rules are consulted when the firewall is determining whether or not to allow or block a connection attempt.
    - For Outgoing connection attempts, the application rules are consulted first and then the global rules.
    - For incoming connection attempts, the global rules are consulted first and then application specific rules.
- The Rulesets area contains a list of preset Firewall rules that can be re-used and applied to multiple applications. For example, there is a 'Browser' rule, an 'Email Client' rule and rules for 'Trusted' and 'Blocked' applications.
- The Network Zones area allows you to group IP addresses and ranges into named zones. Once defined, privileges and rules can be applied to these zones in other areas of CIS. For example, global and application rules can be applied to network zones. This interface also allows you to block network zones.
- The Portsets area contains groups of important / regularly used port numbers that can be easily selected as part of a global or application rule.
- The Website Filtering area allows you to create website filtering rules which let you determine which sites certain

users can or cannot access.

4. Sandbox Tasks - Introduction

Comodo Internet Security features a fully functional sandbox called the 'Virtual Desktop'- an isolated operating environment for running unknown, untrusted and suspicious applications. Applications executed inside the sandbox/Virtual Desktop will not affect other processes, programs or data on your real computer. In addition to running suspicious applications inside the sandbox on an ad-hoc basis, you can create a specific list of programs that should always run in the sandbox.



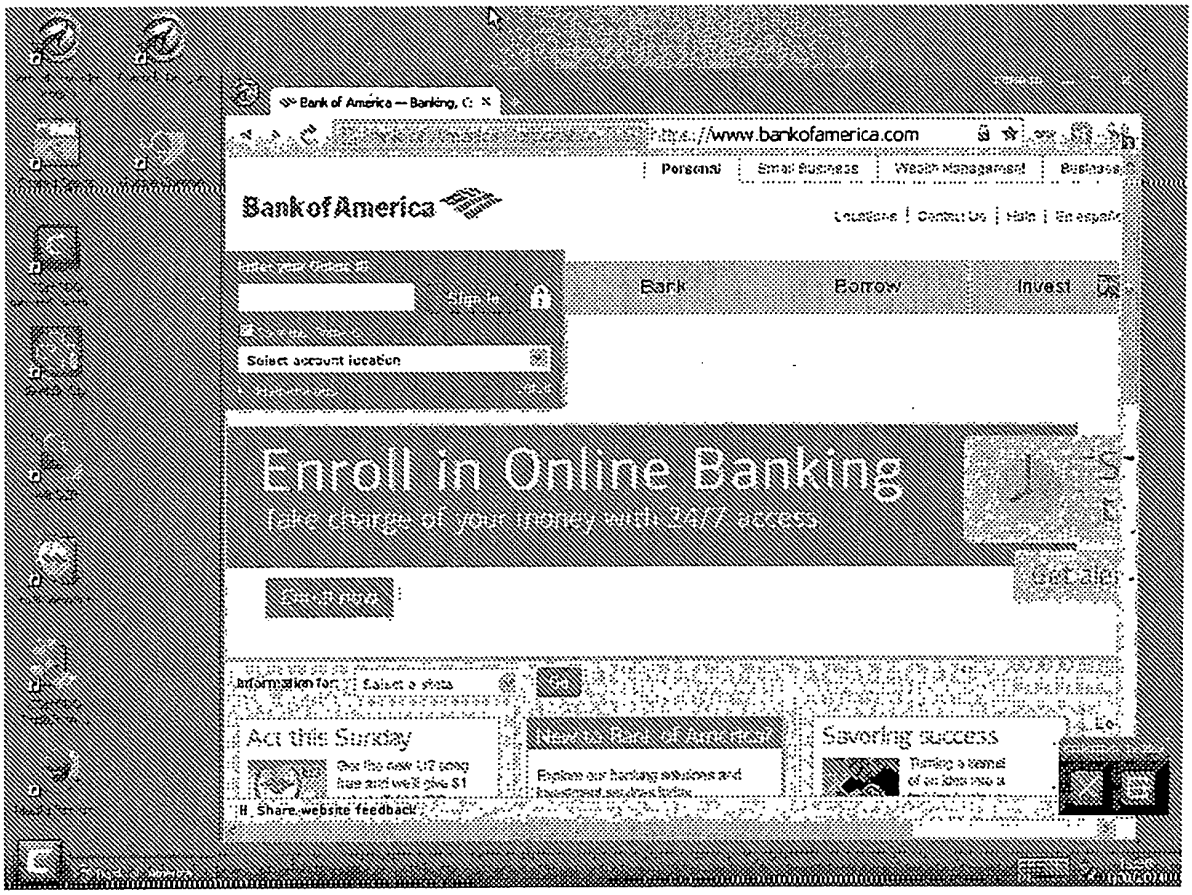
Note: The sandbox referred to here is a full environment and is distinct to the 'auto-sandbox' configured under Behavior Blocker. Users can, however, enable 'Full Virtualization' of auto-sandboxed files in the Behavior Blocker settings.

The Sandbox Tasks interface has shortcuts for the following tasks:

- Run Virtual Desktop - Starts the Virtual Desktop
- **Open Shared Space** - Opens the folder 'Shared Space' which is shared by your host operating system and the Virtual Desktop. The folder is created by the Virtual Desktop at the location 'C:\Documents and Settings\All Users\Application Data\Shared Space'. The folder can be opened in both your host operating system and inside the Virtual Desktop, and enables to share files and applications between the OS and the Virtual Desktop.
- Run Virtual - Allows you to run individual applications in the sandbox
- Reset Sandbox - Allows you to clear all data written by programs run inside the sandbox
- Open Advanced Settings - Add programs that should always run inside the sandbox and access advanced sandbox settings. This is covered in the 'Configure the Sandbox' section of 'Advanced Settings'

4.1. The Virtual Desktop

The Virtual Desktop is a sandboxed operating environment inside of which you can run programs and browse the Internet without fear that those activities will damage your real computer. Applications running in the Virtual Desktop also leave no cookies or history behind on your real system, making it a secure environment for Internet banking and online shopping. It is also ideal for visiting any risky websites/links and for testing out beta/unstable software.



Virtual Desktop at a glance:

- The Virtual Desktop can run any program that you can run in regular Windows and is particularly useful for browsing the Internet in a secure manner.
- Any changes made to files and settings in the Virtual Desktop will not affect the original versions on your host system. Changes will only be visible in the Virtual System itself.
- Similarly, any changes made by malicious programs or unstable beta software will not damage your real computer.
- Any files you wish to keep and access from your host operating system can be saved to 'Shared Space'.
- The Virtual Desktop can be password-protected for added privacy.
- The virtual keyboard allows you to securely enter confidential passwords without fear of key-logging software.
- The Virtual Desktop UI can be used in both 'Classic' (Windows style) and 'Tablet' modes by selecting the mode from Settings.
- You can reset the Virtual Desktop and clear shared space at any time. We recommend that you do this regularly to maximize your privacy and security. Please note that all settings, stored data and any applications installed sandboxed will be deleted.

Click the following links to find out more details on:

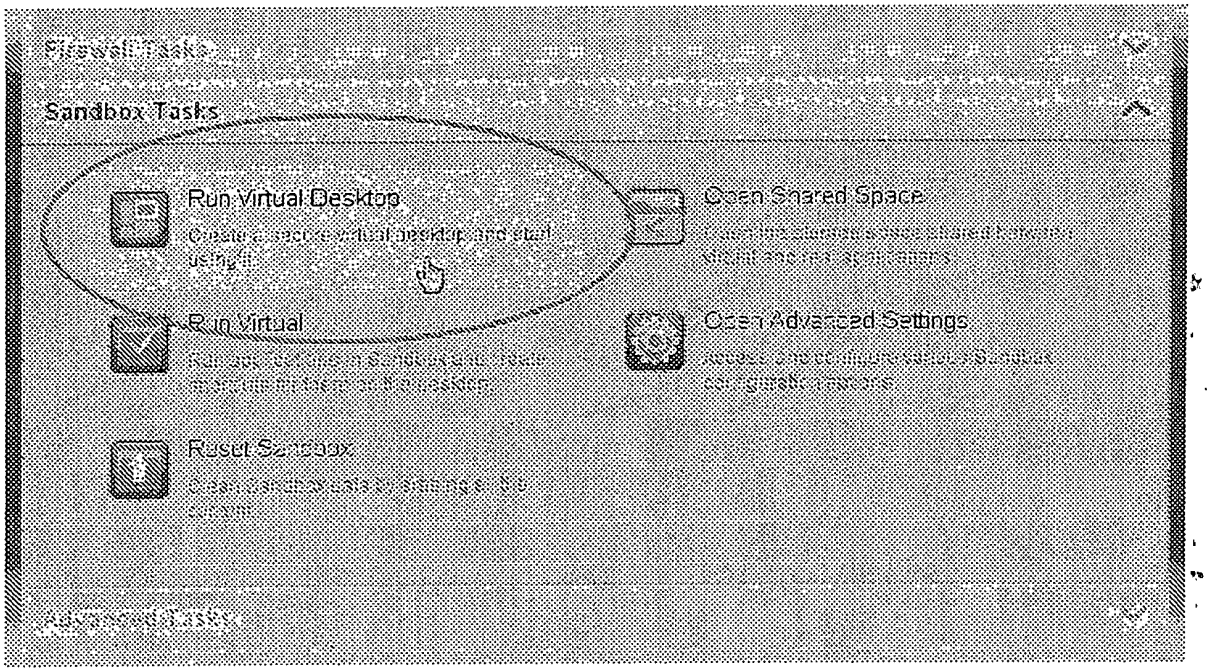
- Starting the Virtual Desktop
- The Main Interface

- Run Browsers inside Virtual Desktop
- Open Files and Run Applications inside Virtual Desktop
- Configuring the Virtual Desktop
- Closing the Virtual Desktop

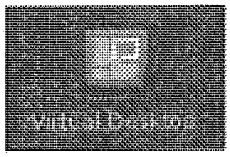
4.1.1. Starting the Virtual Desktop

The Virtual Desktop can be started by:

- Clicking Tasks > Sandbox Tasks > Run Virtual Desktop

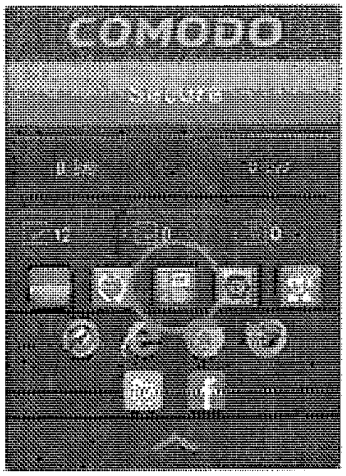


OR

- by clicking the Virtual Desktop shortcut button  from the task bar at the bottom of Home Interface

OR

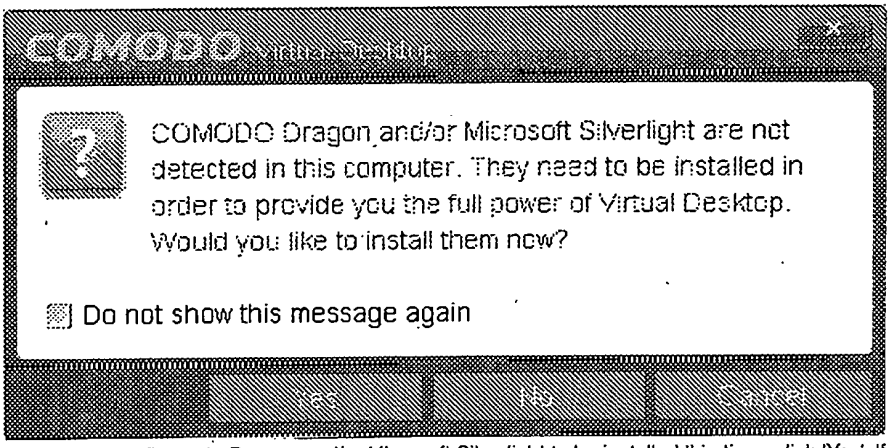
- By clicking the Virtual Desktop shortcut button from the CIS widget



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

- Comodo Dragon Browser
- Microsoft Silverlight

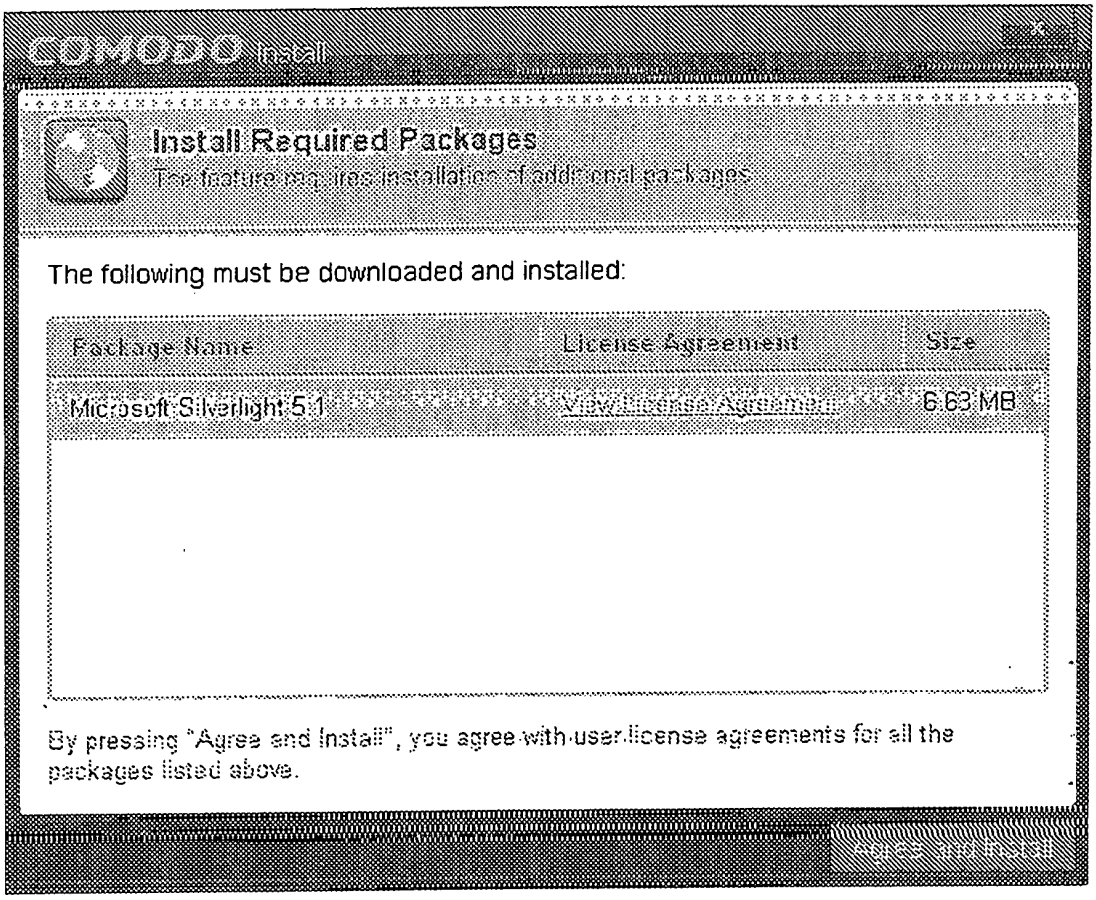
Whenever you run the Virtual Desktop, Comodo Internet Security checks whether these components are installed. If they aren't, you will be prompted to install them.



- If you want Comodo Dragon and/or Microsoft Silverlight to be installed this time, click 'Yes'. If not, click 'Cancel'. You will be prompted to install them, next time when you start the Virtual Desktop.
- If you do not want the applications to be installed at all, click 'No'.

- Click 'Yes' to download and install the software.

The 'Install Required Packages' dialog will be displayed.



- Click 'View License Agreement' to read the license agreement of the additional software to be installed
- Click Agree and Install to download and install the required software

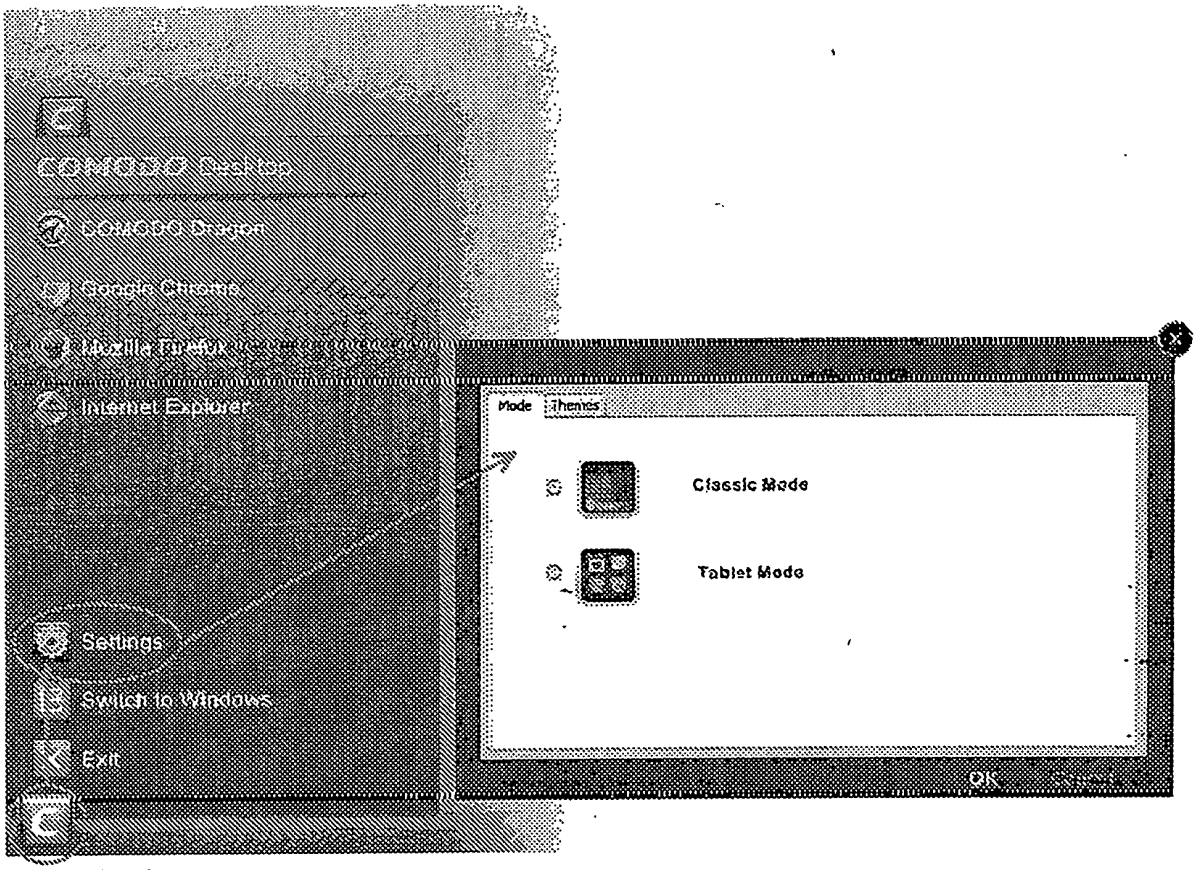
The software package(s) will be downloaded and installed automatically.

4.1.2. The Main Interface

The Virtual Desktop is presented with two switchable interfaces:

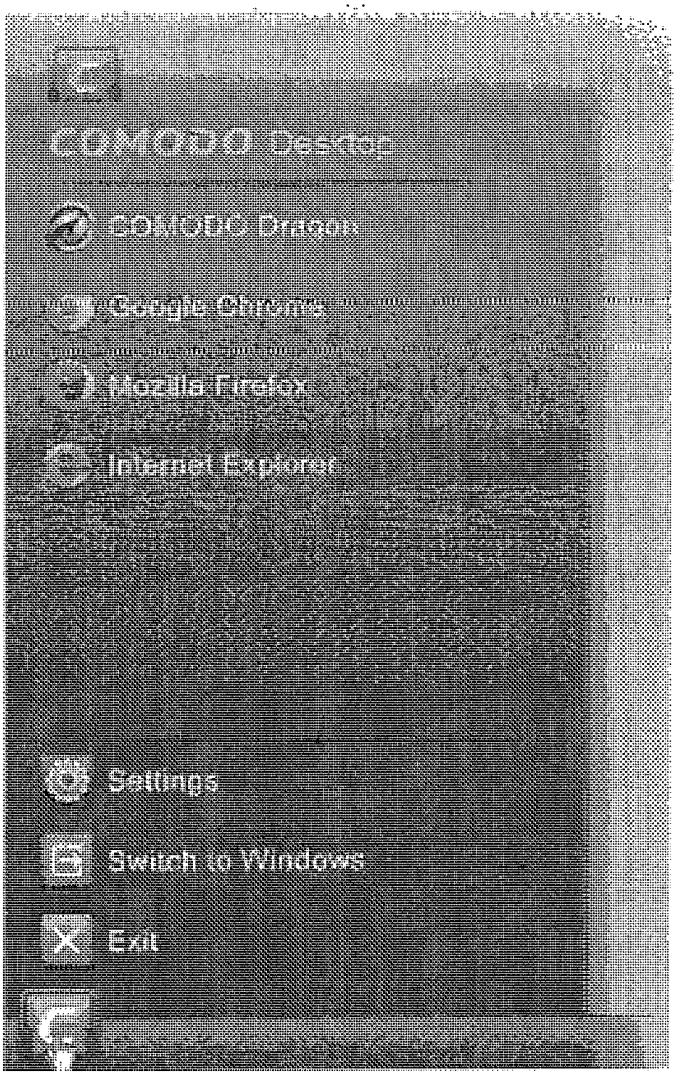
- Classic Windows style Desktop mode
- Tablet mode

You can switch between these two modes by clicking the green 'C' button at bottom-left then 'Settings' (C Button > Settings > 'Mode' tab). Refer to the table below for a comparison of different modes of the Virtual Desktop main interface.



In 'Classic' mode,

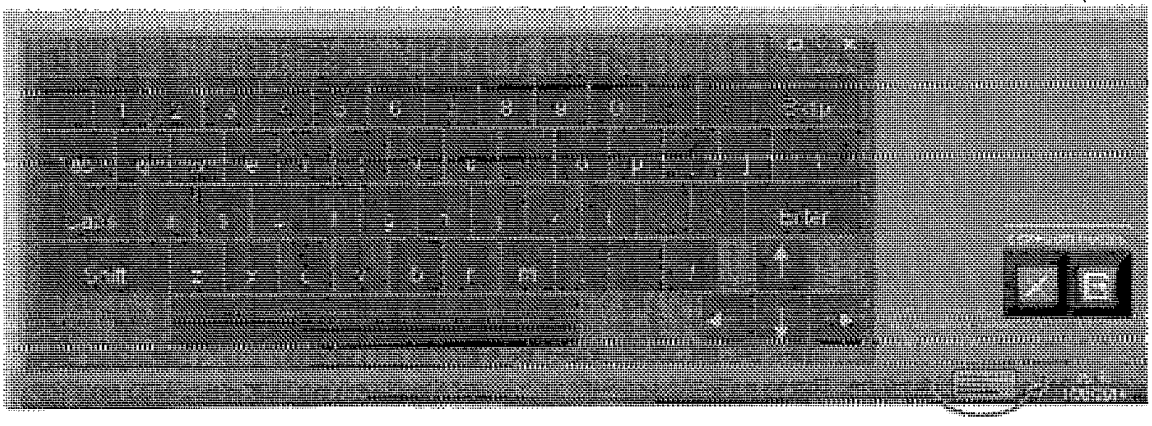
- All items on your real desktop are displayed. Clicking the shortcuts on the Virtual Desktop will run the program or file inside the virtual computer system.
- Clicking the green 'C' button at bottom-left will open a Windows-style 'Start Menu'.



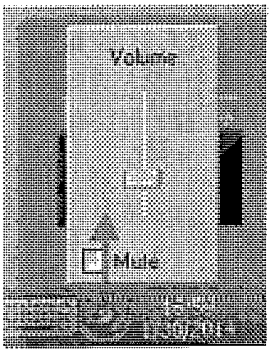
The start menu allows you to:

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

- Clicking the keyboard icon on the system tray opens a virtual keyboard that can be used to input confidential data like website user-names, passwords and credit card numbers.



- Clicking the 'Volume Control' icon at the system tray enables you to control the system volume.



- Right-clicking on the task bar and selecting 'Watch Activity' opens the 'Windows Task Manager' to view your computer's performance, close unresponsive programs and to troubleshoot problems with Windows.



Tablet Mode

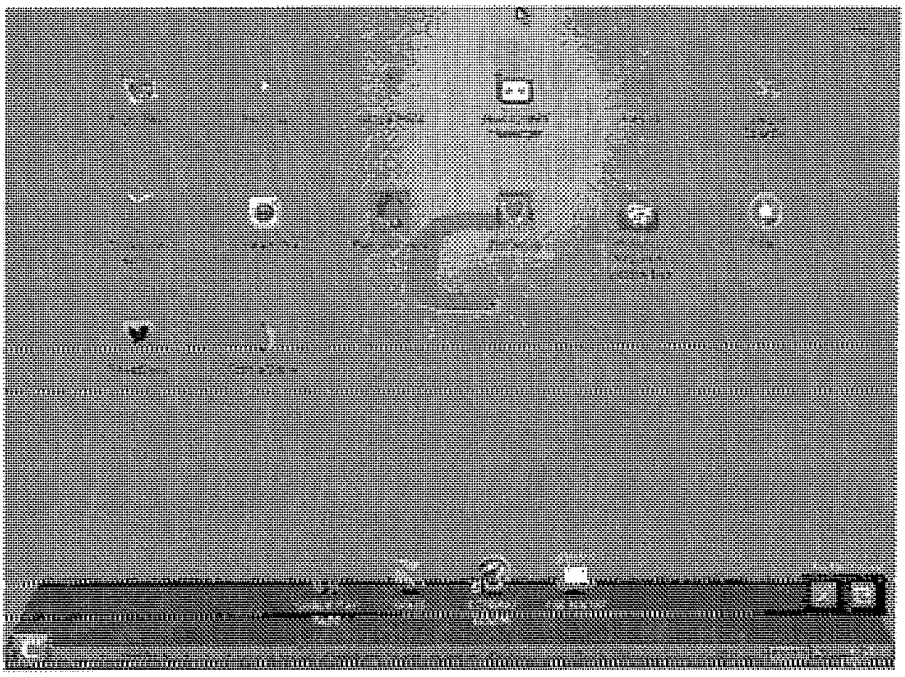
To switch to 'Tablet' mode from 'Classic' mode, click the green 'C'  button at bottom left followed by Settings > Mode and select 'Tablet Mode'.

There are two variations of this mode:

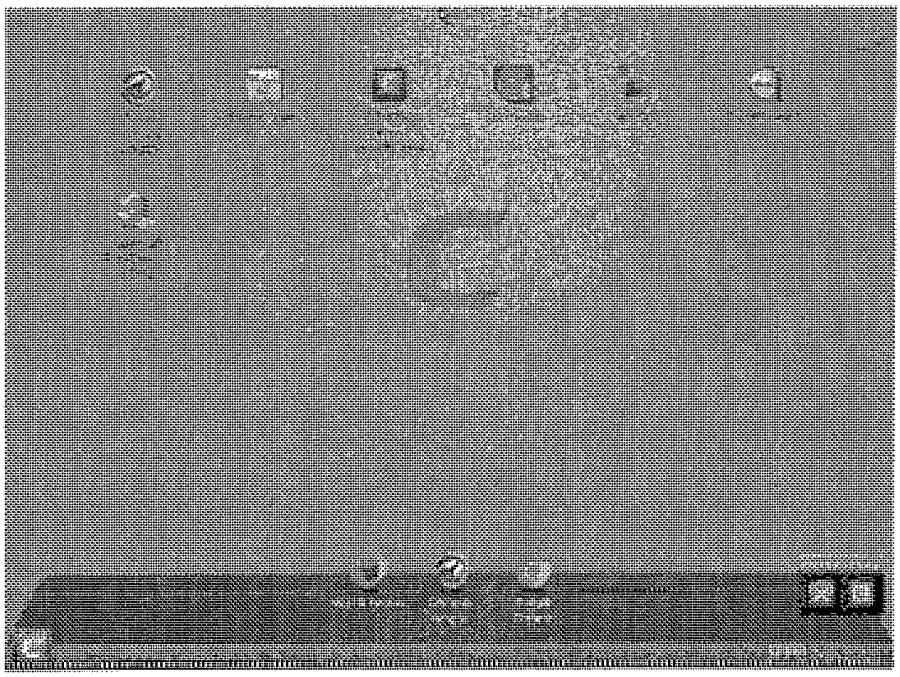
1. Mode A - Pure Tablet device - A touch-screen interface that will be familiar to users of modern smart devices. The home page displays a set of popular apps covering games, social media and networking. You can, of course, install your own apps from the app market.
    - To install your own apps, click the App Market icon from the launch bar. You will be taken to https://chrome.google.com/webstore/category/home?utm_source=COMODO-Kiosk. Select the apps you want to install from the web-store.
2. Mode B - Tablet device + Windows - The home page displays the desktop items from your real system. The task bar from classic mode is present along with the green 'C' button and the virtual keyboard. The launch strip will display all installed browsers.

You can swap between the two modes by clicking the green arrow at the top right corner: 

You can swipe the home screen in both left and right directions to navigate between successive home pages.



Tablet Mode A - Pure Tablet



Tablet Mode B - Tablet + Windows

The following table gives a comparison of the classic and tablet modes of the main interface:

Classic Mode	Mode A - Pure Tablet	Mode B - Tablet + Windows
Windows desktop style interface.	Tablet style interface.	Tablet style interface.
Your real desktop shortcuts and files are displayed	Shortcut icons of the apps installed on the tablet are displayed	Your real desktop shortcuts and files are displayed
Shortcuts and files are laid out vertically as they would be on a Windows desktop	Shortcuts are laid out horizontally	Shortcuts and files are laid out horizontally

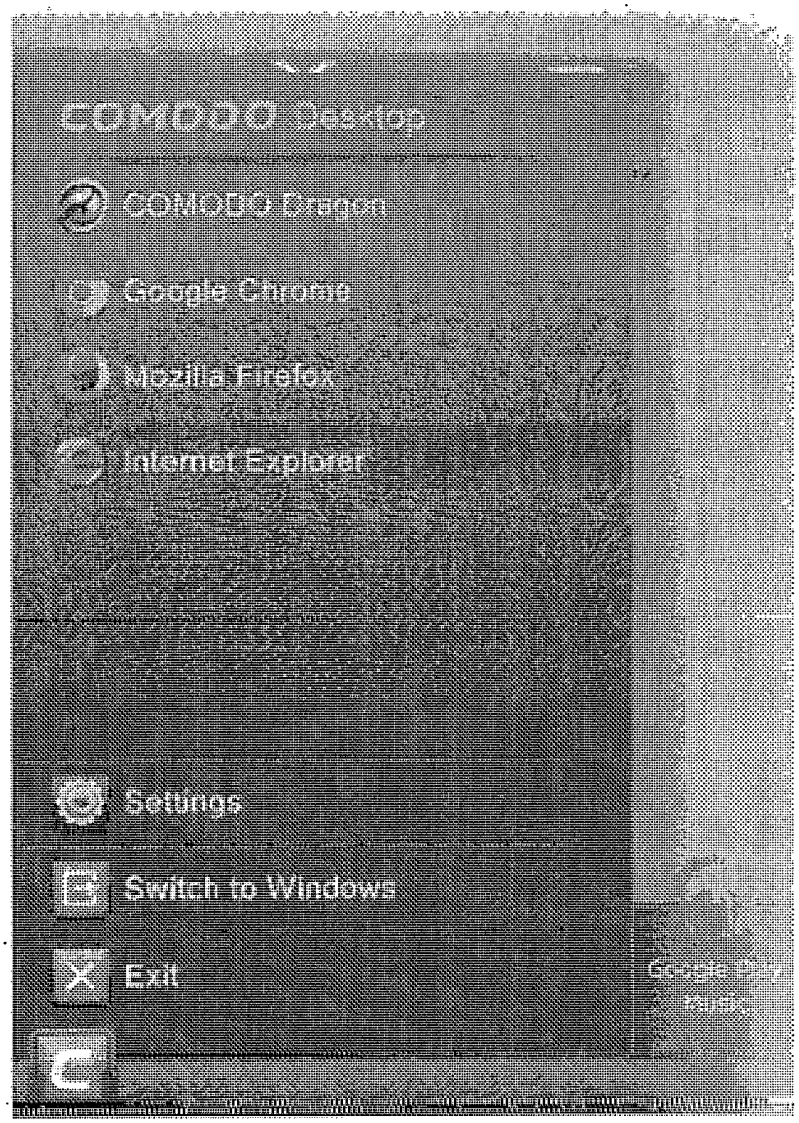
No Launch Bar	Browser shortcuts are displayed on the launch bar at the bottom	Browser shortcuts are displayed on the launch bar at the bottom
Cannot have multiple home screens	Can have multiple home screens	Can have multiple home screens if you have many shortcuts and files
Cannot swipe the screen to move between home screens	Can swipe the screen to move between home screens	Can swipe the screen to move between home screens

4.1.3. Running Browsers inside the Virtual Desktop

The Virtual Desktop provides an extremely secure environment for internet related activities because it isolates your browser from the rest of your computer. Just by visiting them, malicious websites can install viruses malware, rootkits and spyware onto your computer that can allow hackers to steal confidential information. Surfing the 'net from inside the virtual computer system removes this threat by preventing websites from installing applications on your real computer. Furthermore, the Virtual Keyboard allows you to securely enter user-names, credit card numbers and passwords without fear of key-logging software recording your physical keystrokes.

To run a browser inside the Virtual Desktop

1. Click the 'C' button at bottom left
2. Select the browser you want to run:



Your choice of browser will open inside the virtual desktop, ready for secure surfing:



Browsing history and other records of your internet activity will not be stored on your computer when your session is finished.

4.1.4. Opening Files and Running Applications inside the Virtual Desktop

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

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

Desktop Shortcuts

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

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

Shared Space

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

The Shared Space can be accessed in the following ways:

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

- Click the 'Shared Space' desktop shortcut icon

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

1. Open the 'Shared Space' as mentioned above
2. Copy/Move the application or the file to be opened into the Shared Space
3. Start 'Virtual Desktop'
4. Open Shared Space inside the Virtual Desktop by clicking the 'Shared Space' icon in the home screen.

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

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

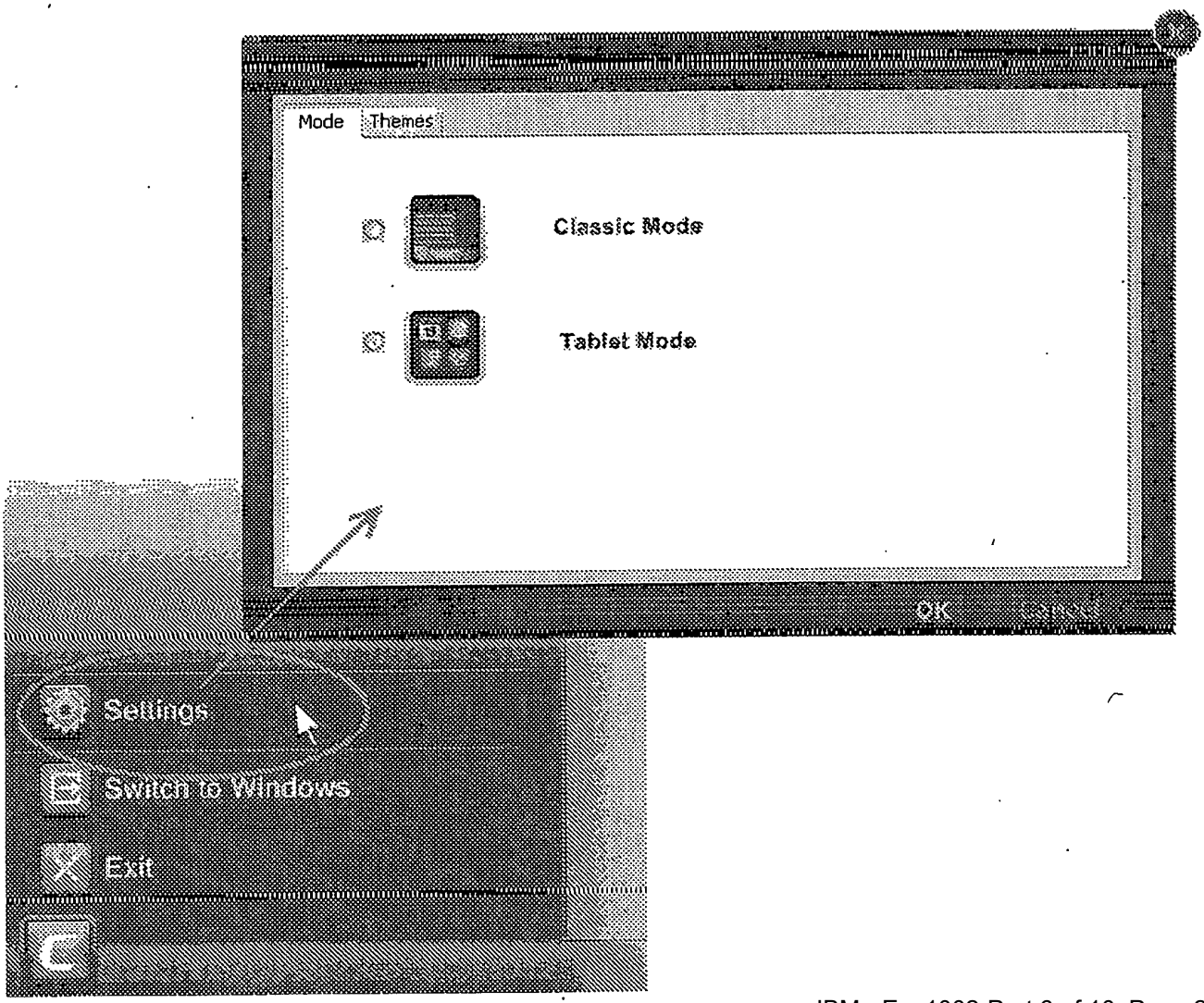
The changes you make to the file will be stored to the file only inside the Virtual Desktop and not in the real computer system.

4.1.5. Configuring the Virtual Desktop

The settings panel allows you to specify the Virtual Desktop operational mode and to modify its look and feel.

To open the settings panel:

1. Click the 'C' button at bottom left.
2. Select 'Settings' from the start menu. The Settings panel will open.



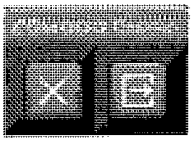
The Settings panel has two tabs:

- **Mode** - Allows you to select the display mode of the Virtual Desktop between Classic Windows mode and Tablet Mode (Default)
- **Themes** - Allows you to choose the appearance of the Virtual Desktop

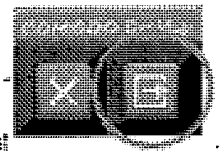
3. Click OK for your settings to take effect

4.1.6. Closing the Virtual Desktop

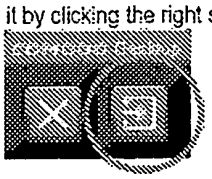
The shortcuts at the bottom right of the Virtual Desktop, allow you to temporarily switch to your real computer system, if you plan to continue using the virtual desktop at a later time, or to fully exit the Virtual Desktop.



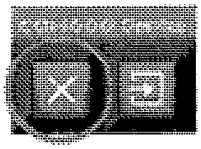
To temporarily switch to your real Windows system



- Click the right button from the shortcuts pane at the bottom right
- Alternatively, Click the 'C' button at bottom left and choose 'Switch to Windows' from the Virtual Desktop Start Menu.

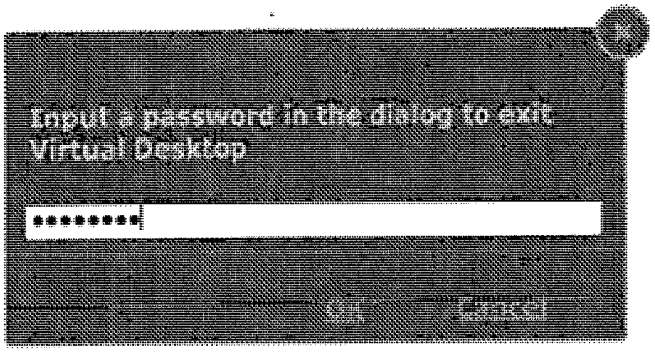
The Virtual Desktop will be temporarily closed. You can quickly return to it by clicking the right switch from the Virtual Desktop shortcut buttons displayed at the bottom right of your Windows Desktop  or by clicking 'Run Virtual Desktop' from the 'Sandbox Tasks' interface.

To close the Virtual Desktop



- Click the X button from the Virtual Desktop shortcuts pane at the bottom right
- Alternatively, Click the 'C' button at bottom left and choose 'Exit' from the Virtual Desktop Start Menu.

In either case, if password protection is enabled under Advanced Settings > Security Settings > Defense+ > Sandbox Settings, you will be prompted to enter the password. Else the Virtual Desktop will be closed.



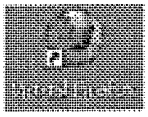
- Enter the password and click OK.

Note: Remember to save the changes before you exit the Virtual Desktop. Your changes will be lost if you exit the Virtual Desktop.

4.2. Run an Application in the Sandbox

Comodo Internet Security allows you to run programs inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that you have downloaded or for applications that you are not sure that you trust. Adding a program in this way means that it will run in the Sandbox this time only. On subsequent executions it will not run in the sandbox (presuming it passes the sandboxing process).

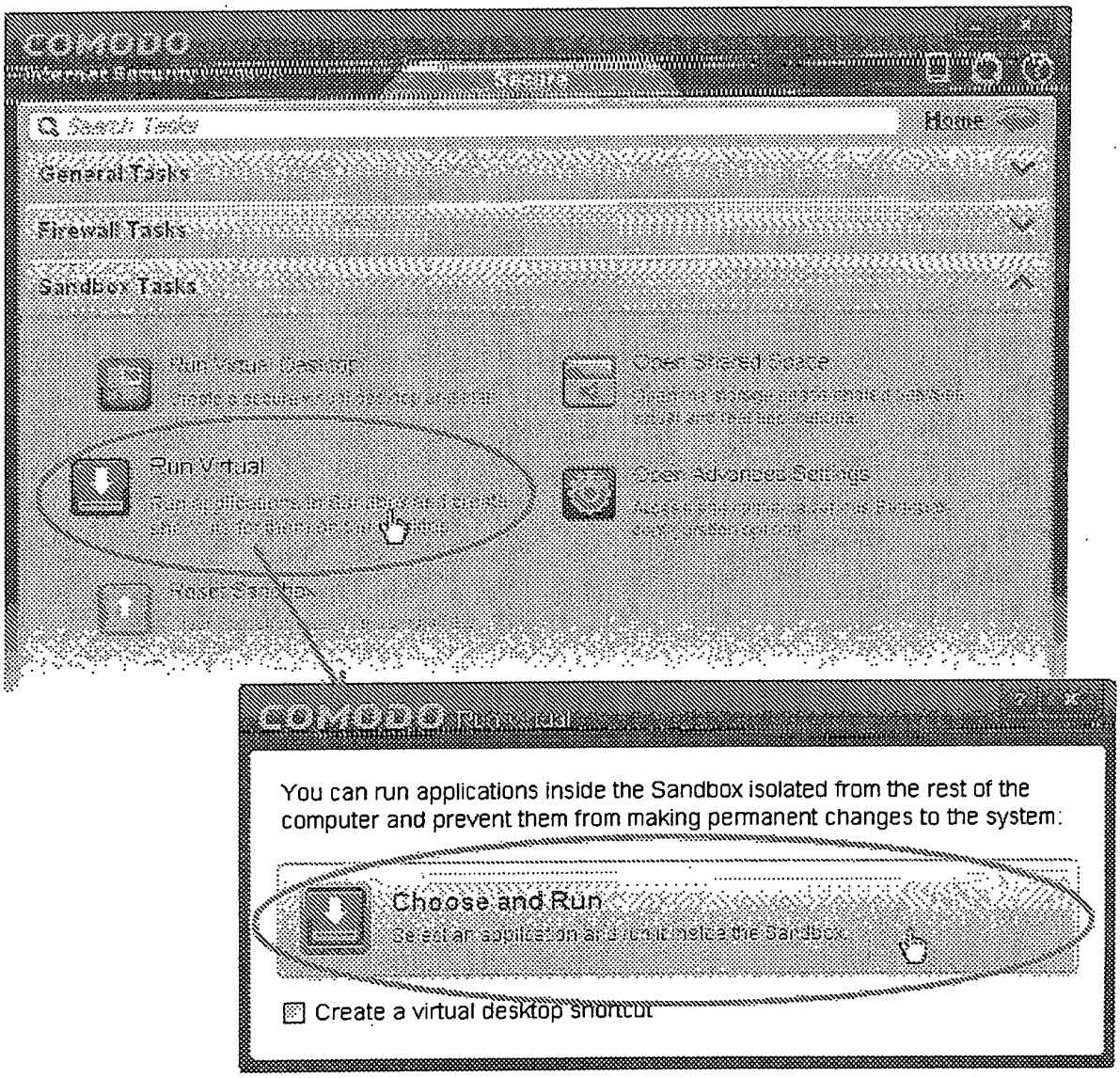
You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



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

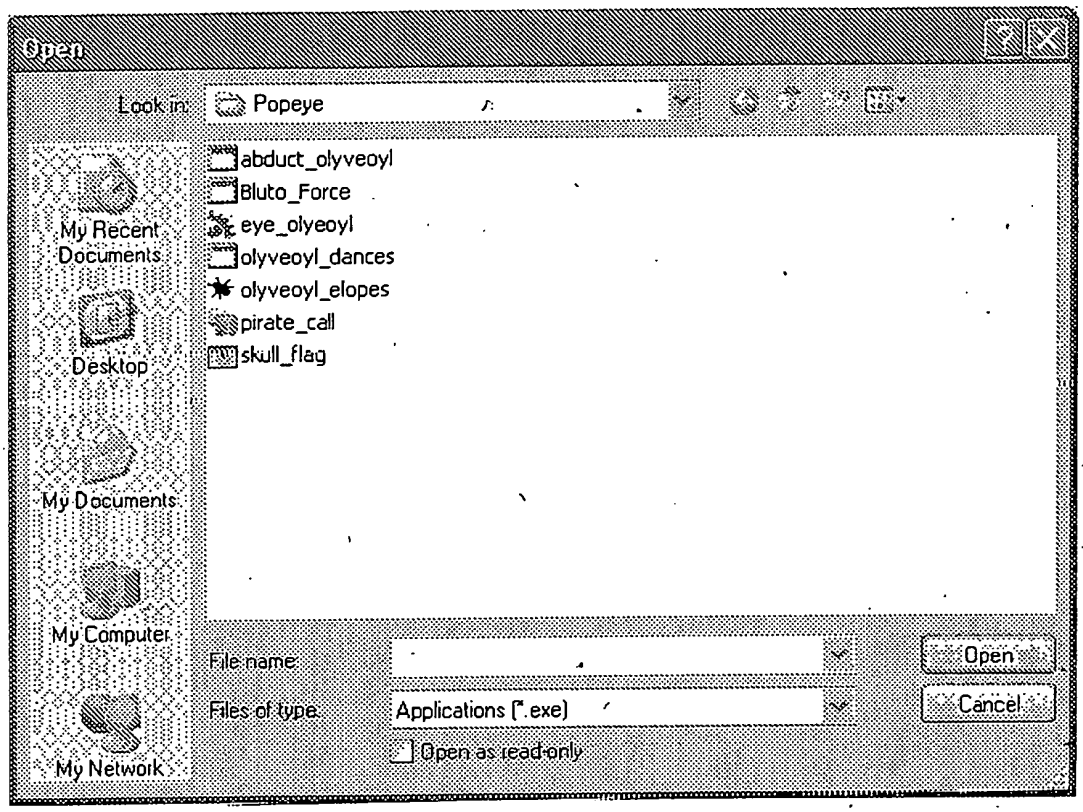
To run an application in the Sandbox

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



The 'Run Virtual' dialog will be displayed.

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



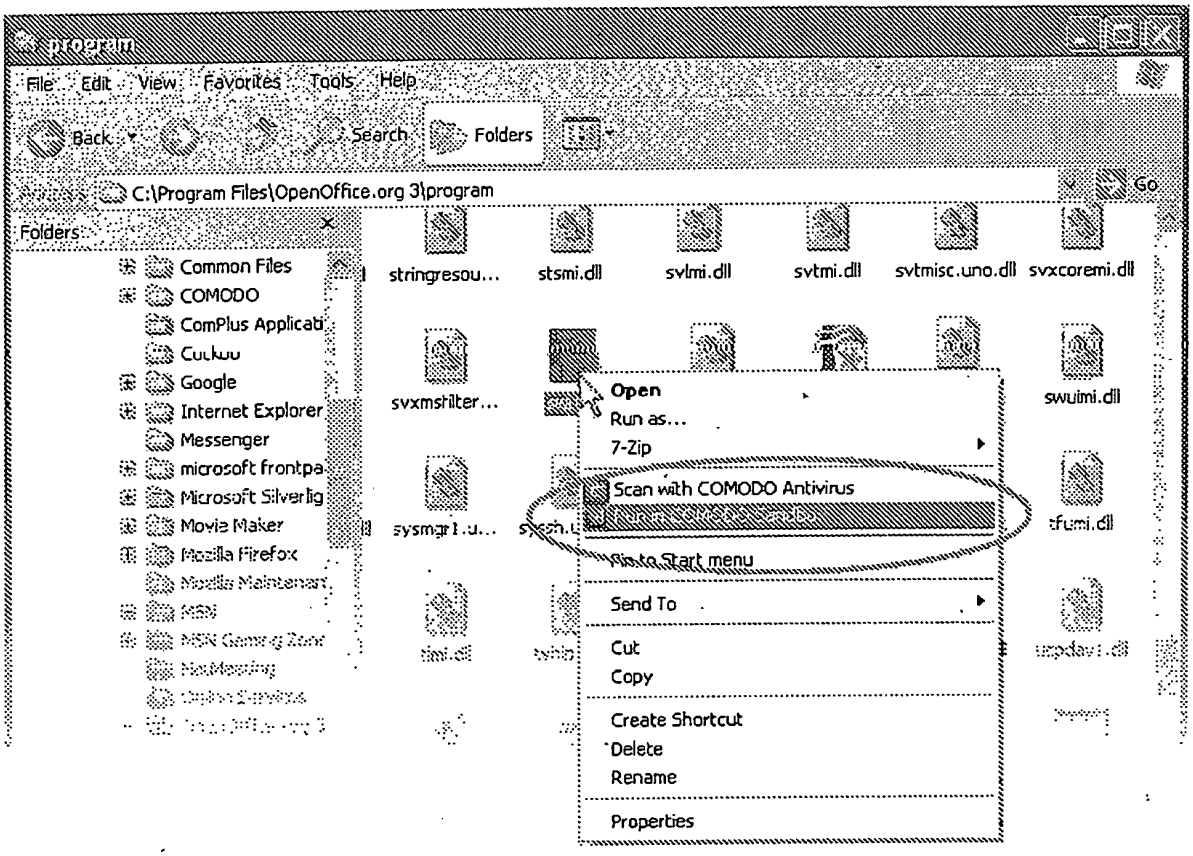
3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

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

- From the context sensitive menu
- Running browsers inside sandbox

Running a program from the context sensitive menu

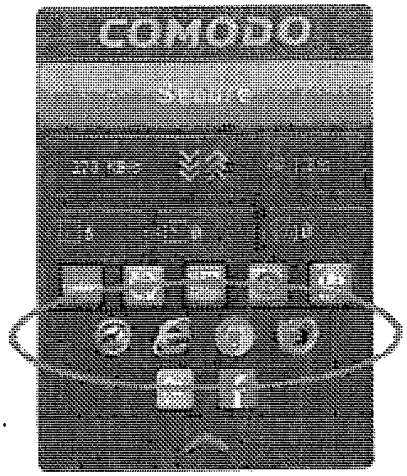
- Navigate to the program in your system that you want to run in sandboxed environment and right click on it



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

Running Browsers inside the Sandbox

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



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

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



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

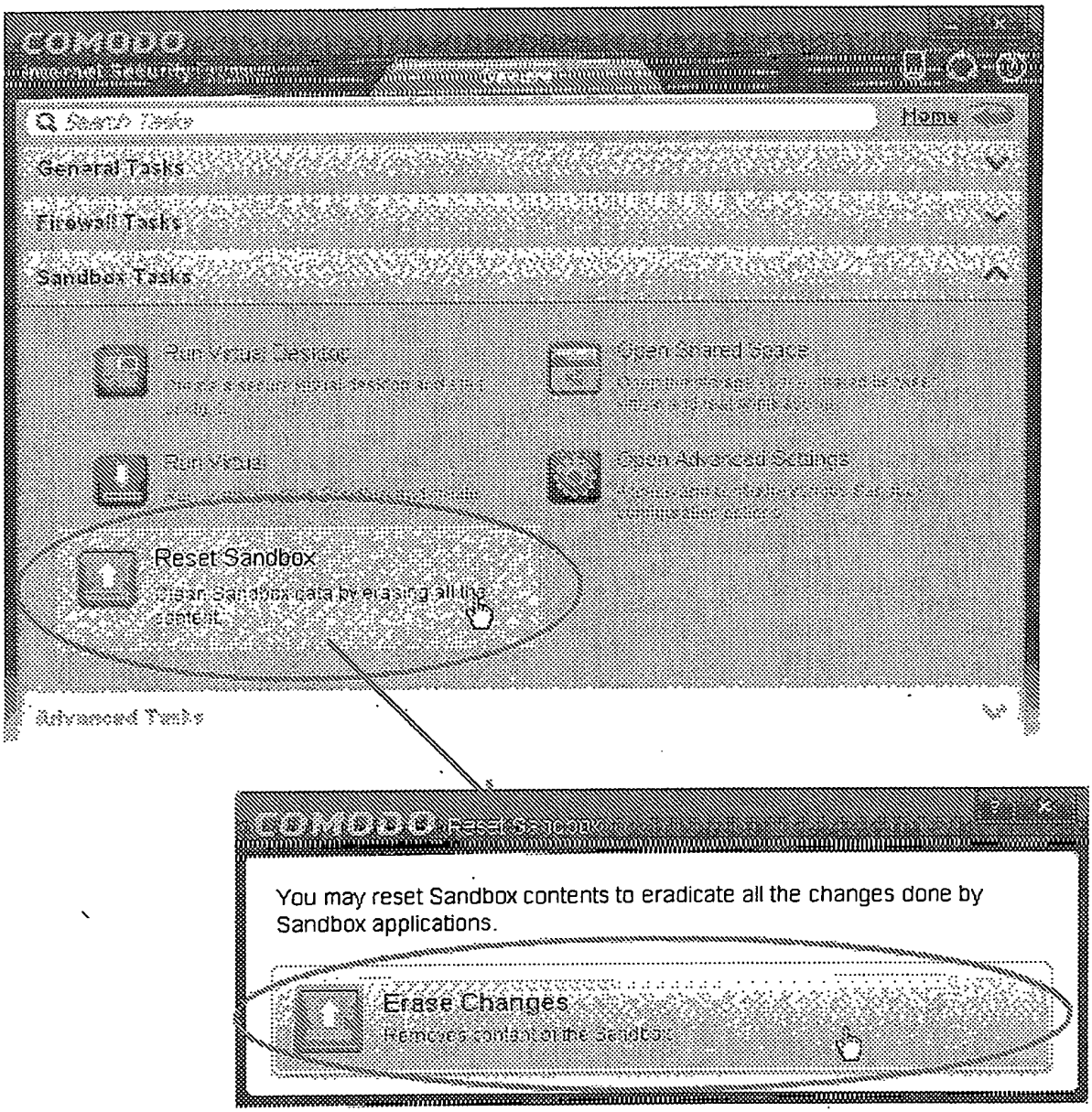
4.3. Reset the Sandbox

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

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

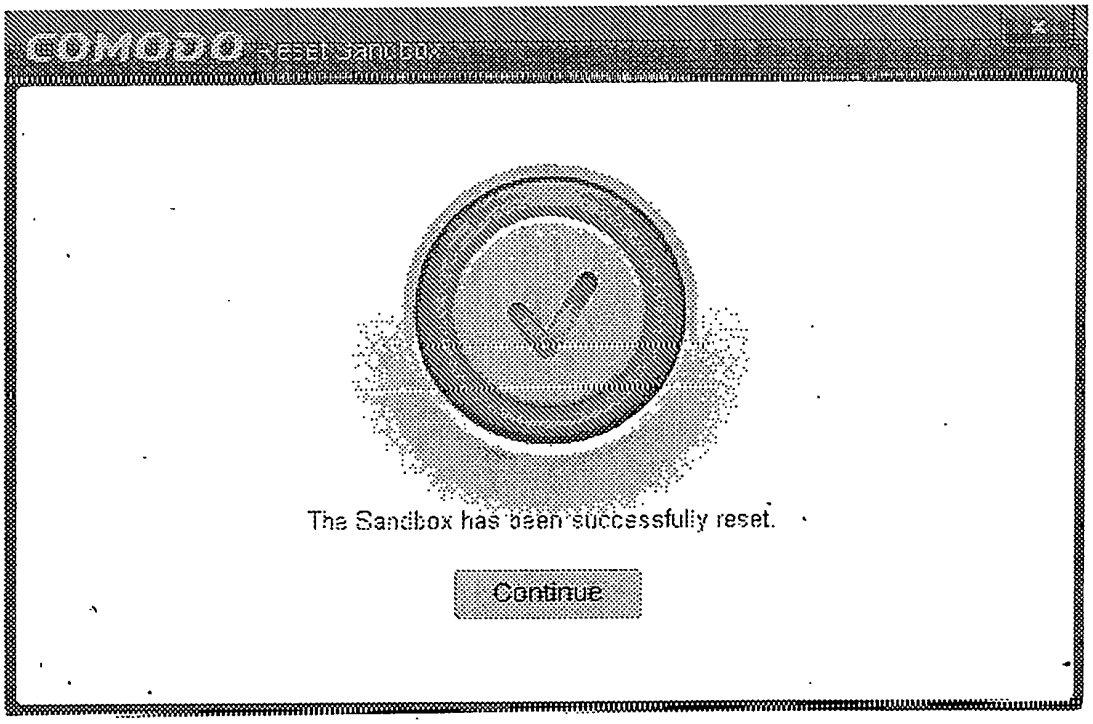
To clear the sandbox

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



The 'Reset Sandbox' dialog will appear.

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

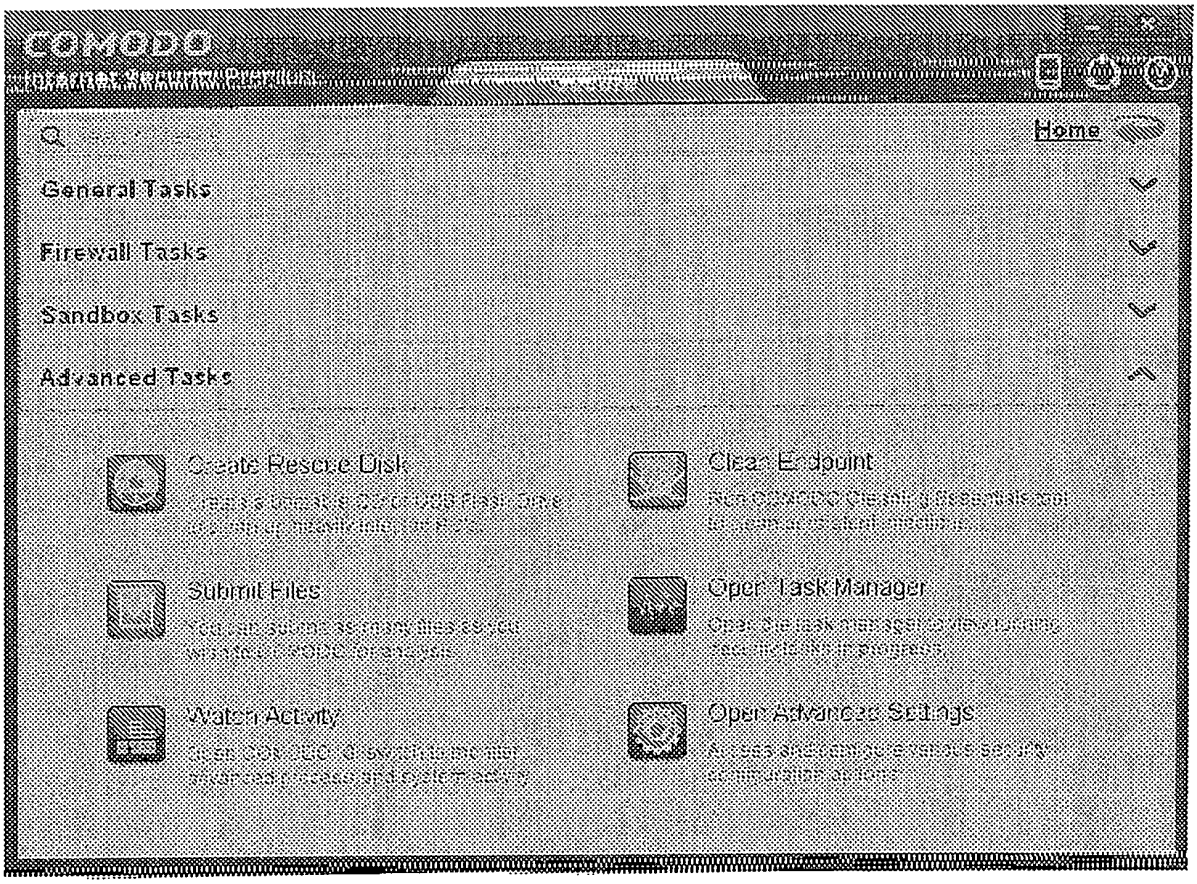


5. Advanced Tasks - Introduction

The 'Advanced Tasks' area allows you modify the overall configuration of CIS, manage CIS tasks like AV scans and updates currently running in the backgound or in minimized window and to take advantage of several other Comodo utilities. Click the following links to find out more about each item:

- Create Rescue Disk - Burn a bootable ISO that lets you run virus scans in pre-boot environments
- Submit Files - Directly Submit unknown/suspicious files to Comodo for analysis
- Watch Activity - Use Comodo Killswitch to identify unsafe processes and manage system activity
- Clean Endpoint - Deploy Comodo Cleaning Essentials to eradicate persistent infections from your PC
- Task Manager - Manage priorities of, stop, pause and resume currently running CIS tasks like Antivirus scans and updates
- Open Advanced Settings - Configure overall behavior, define custom rulesets and much more

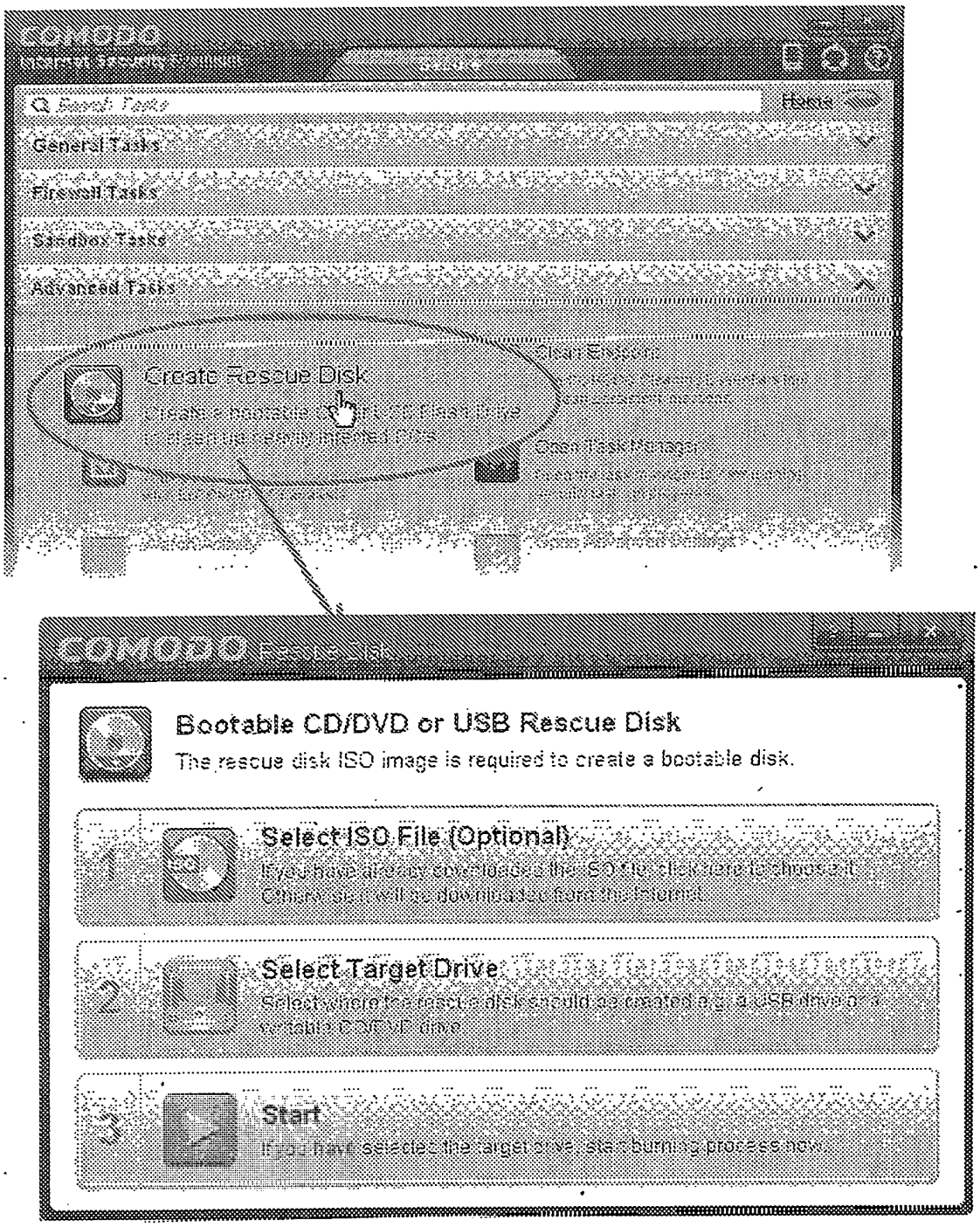
Some of these utilities require the download and installation of additional setup files. After installation, the utility will start directly next time you click the button.



5.1. Create a Rescue Disk

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

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

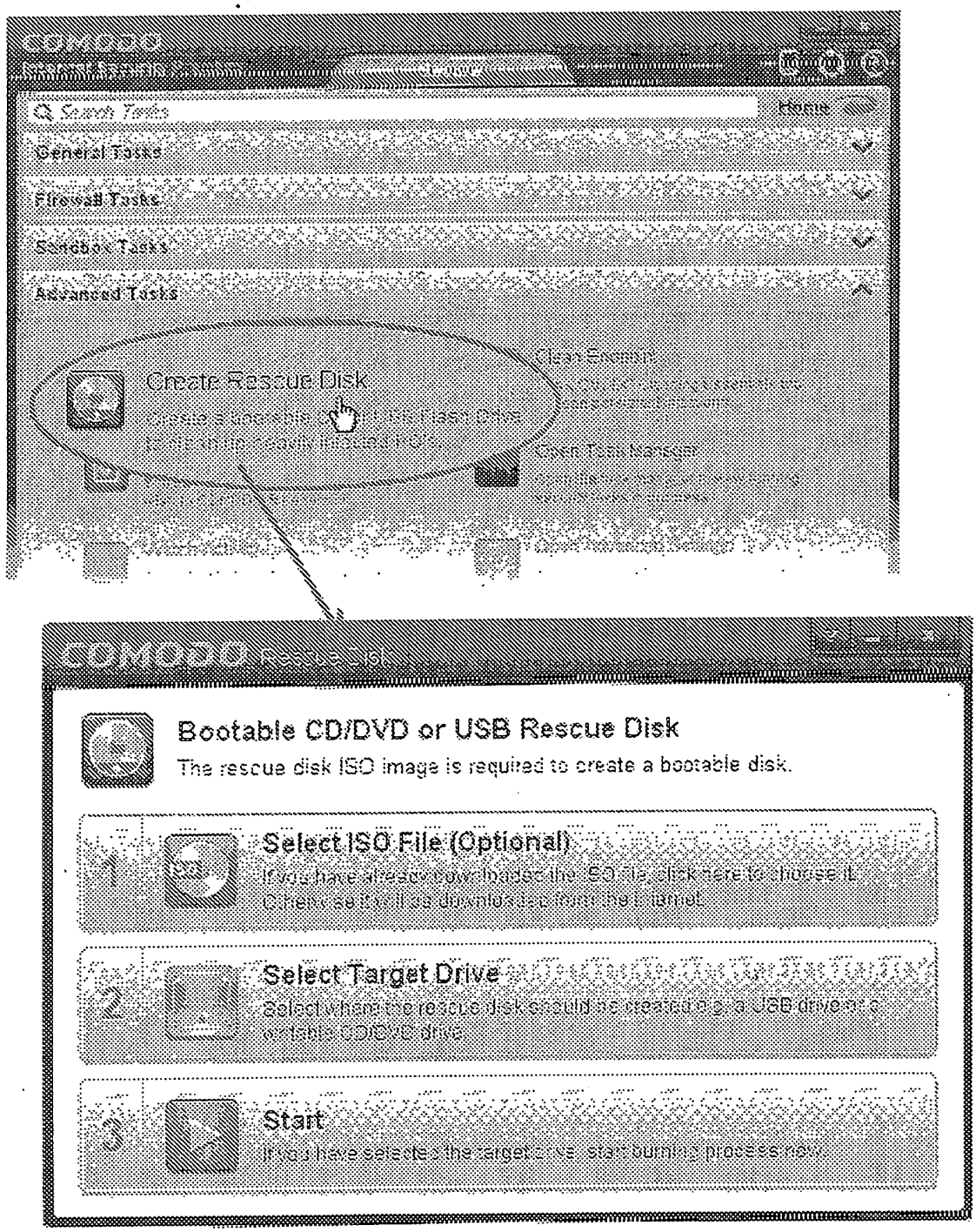


After you have burned the ISO, you need to boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

- Details of how to change boot order on your computer can be found in the Rescue Disk user guide at http://help.comodo.com/topic-176-1-493-5227-Changing-Boot-Order.html
- Details of how to initiate CRD after booting can be found at http://help.comodo.com/topic-176-1-493-5228-Booting-to-and-Starting-Comodo-Rescue-Disk.html
- Details of how to start running scans on your pre-boot environment are available at http://help.comodo.com/topic-176-1-493-5216-Starting-Comodo-Cleaning-Essentials.html and http://help.comodo.com/topic-176-1-493-5217-CCE-Interface.html

5.1.1. Downloading and Burning Comodo Rescue Disk

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



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

Step 1- Select the ISO file

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

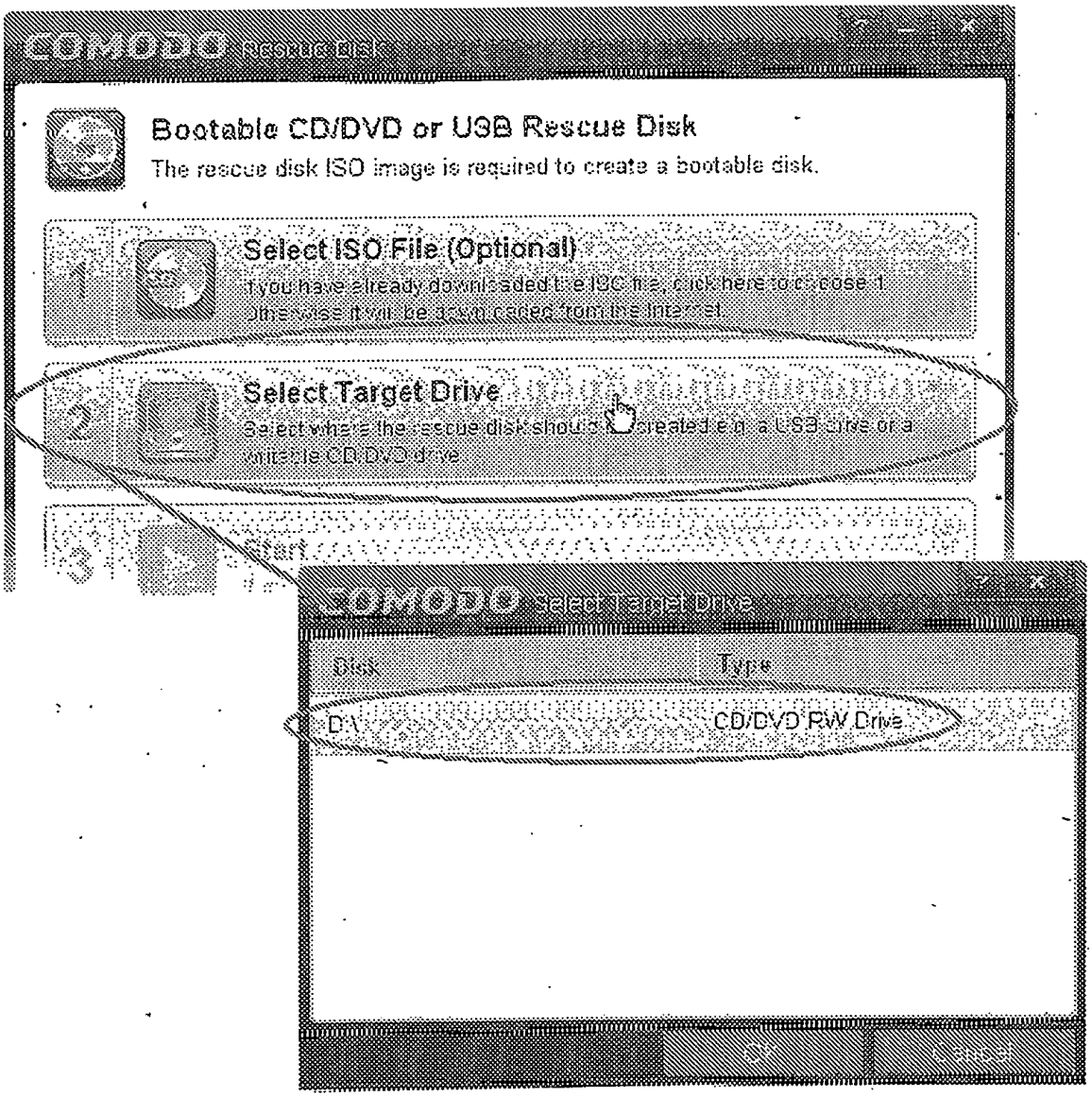
- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

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

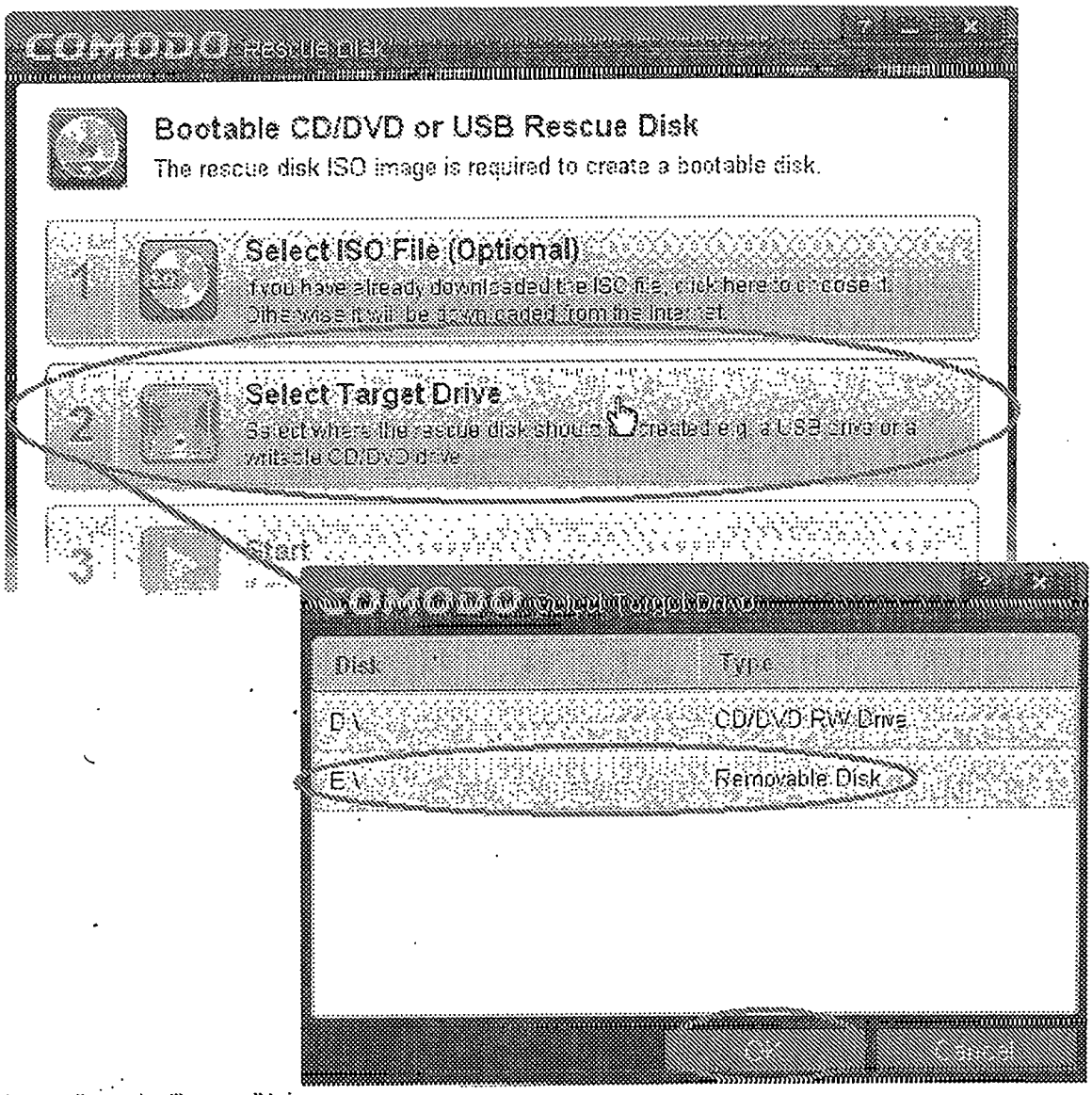
To burn the Rescue disk on a CD or a DVD

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



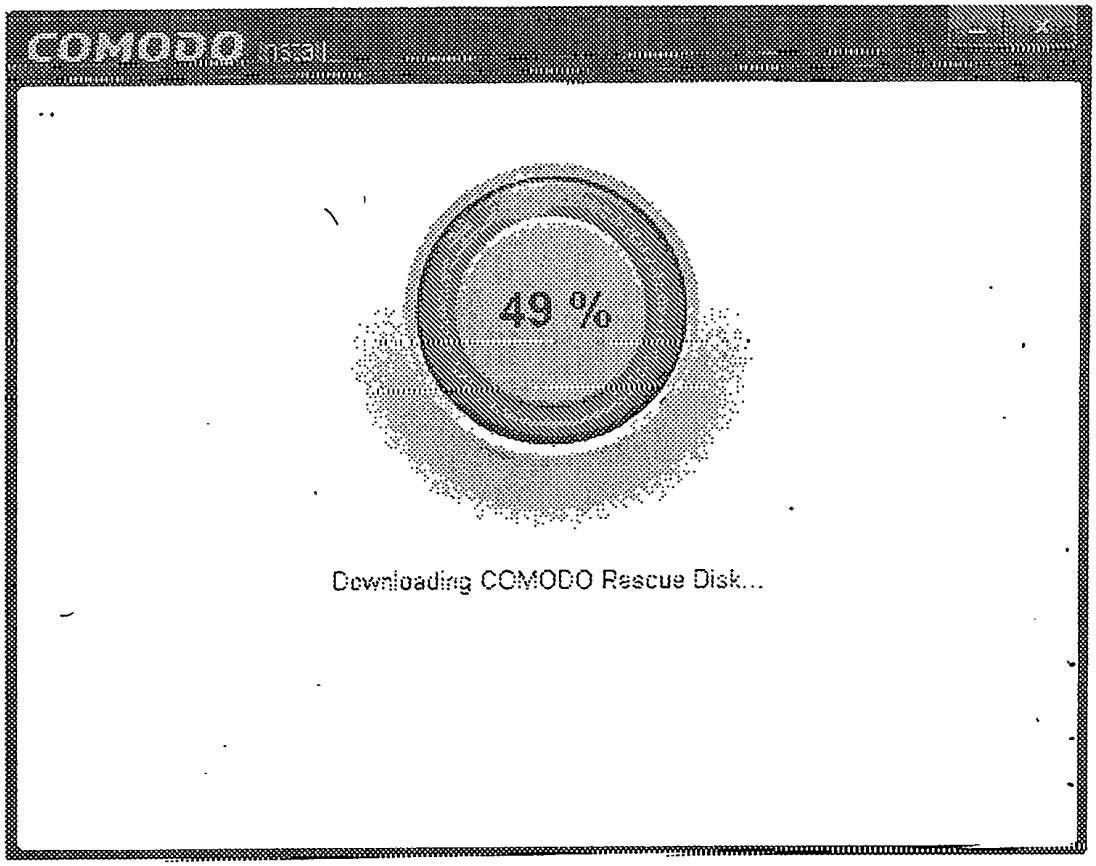
To burn the Rescue disk on a USB Drive

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

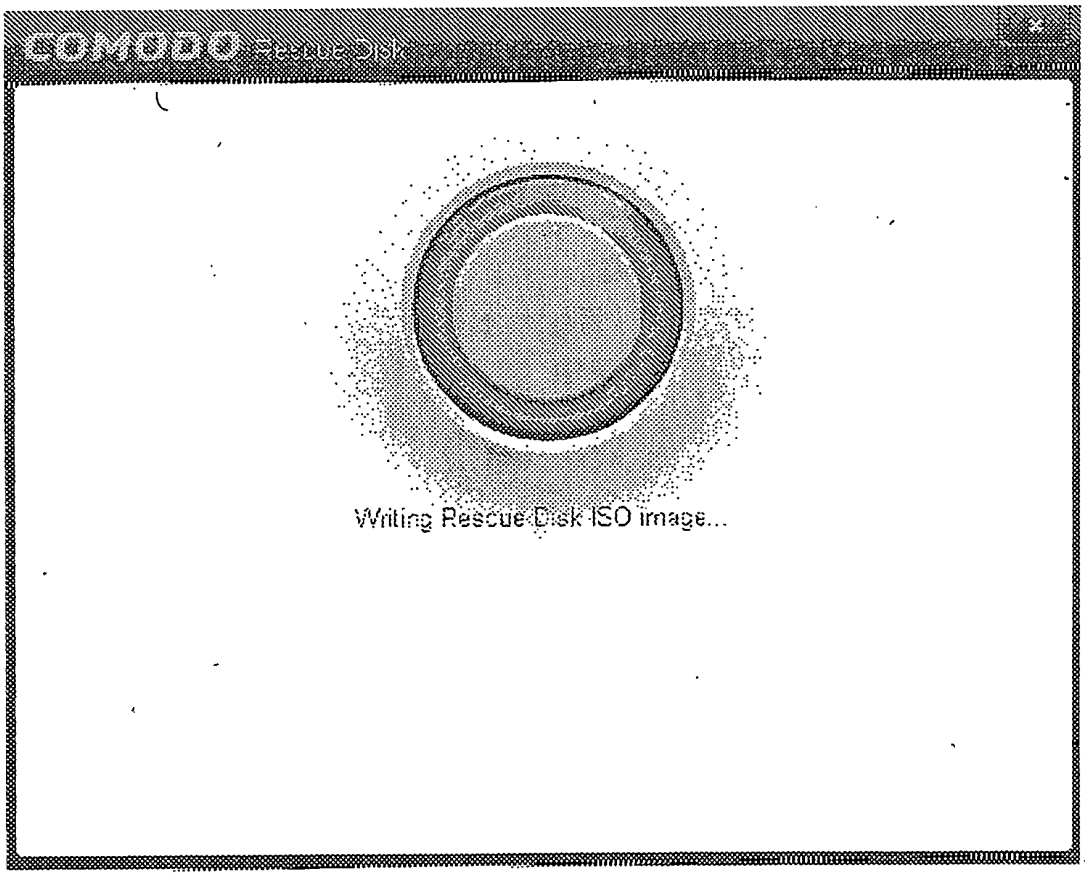


Step 3 - Burn the Rescue Disk

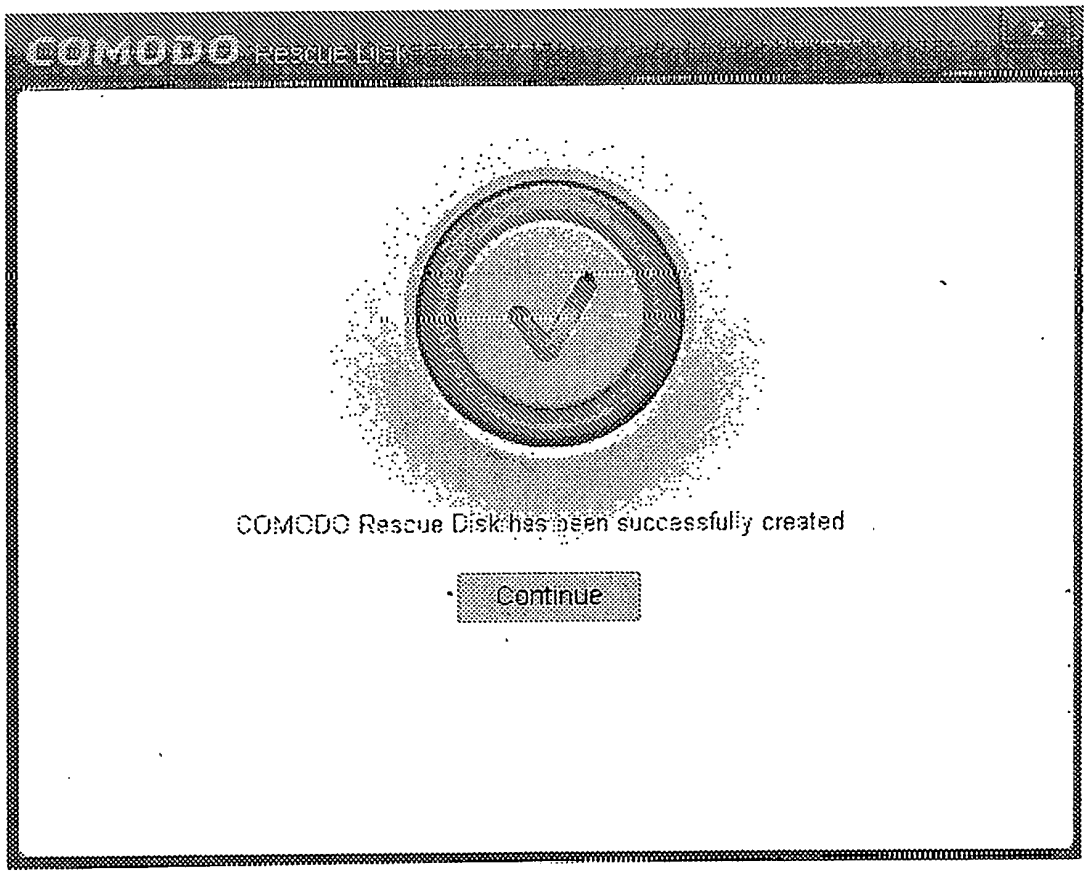
- After you selected the target drive, click 'Start'. If you have selected an .iso file from your hard disk, the burning of the disk will start immediately. Else, the .iso file will be downloaded from Comodo Servers.



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



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



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

5.2. Remove Deeply Hidden Malware

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

Major features include:

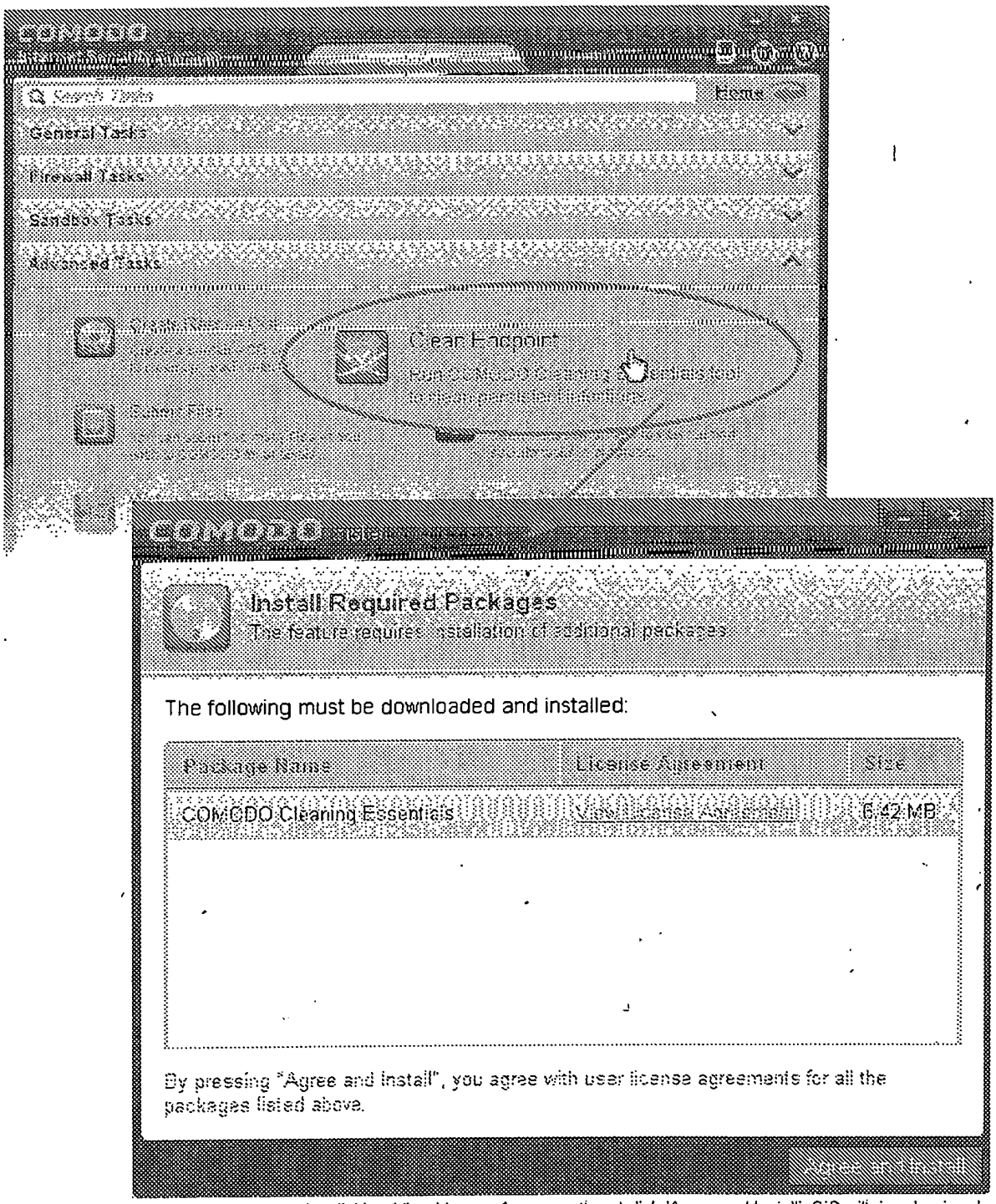
- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits, hidden files and malicious registry keys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

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

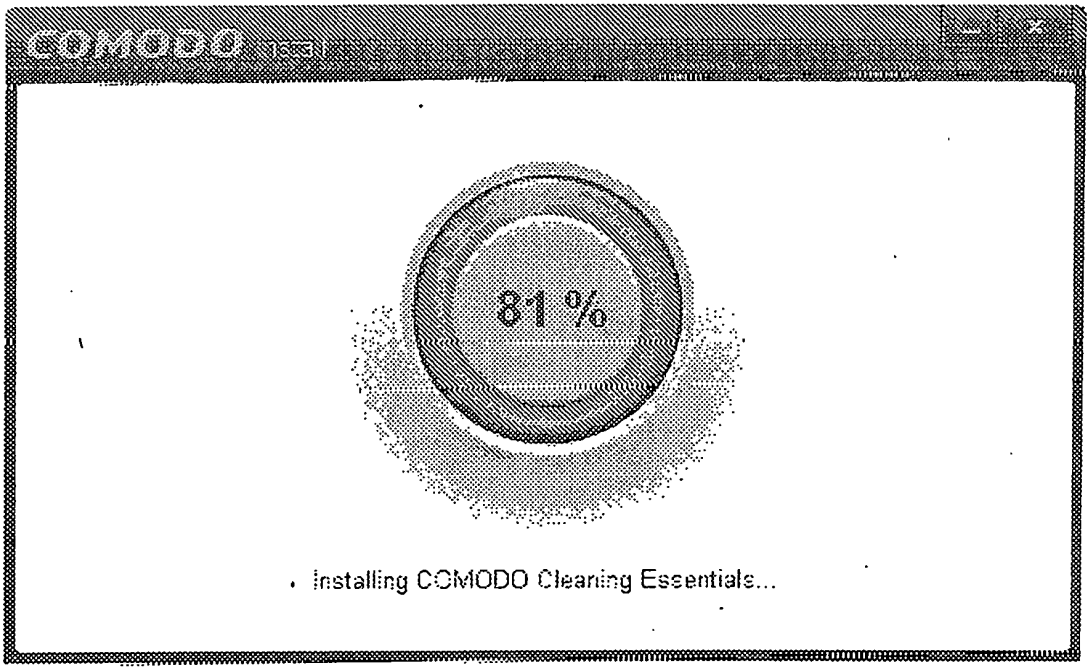
For more details on the features and usage of the application, please refer to the online guide at http://help.comodo.com/topic-119-1-328-3518-Introduction-to-Comodo-Cleaning-Essentials.html.

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

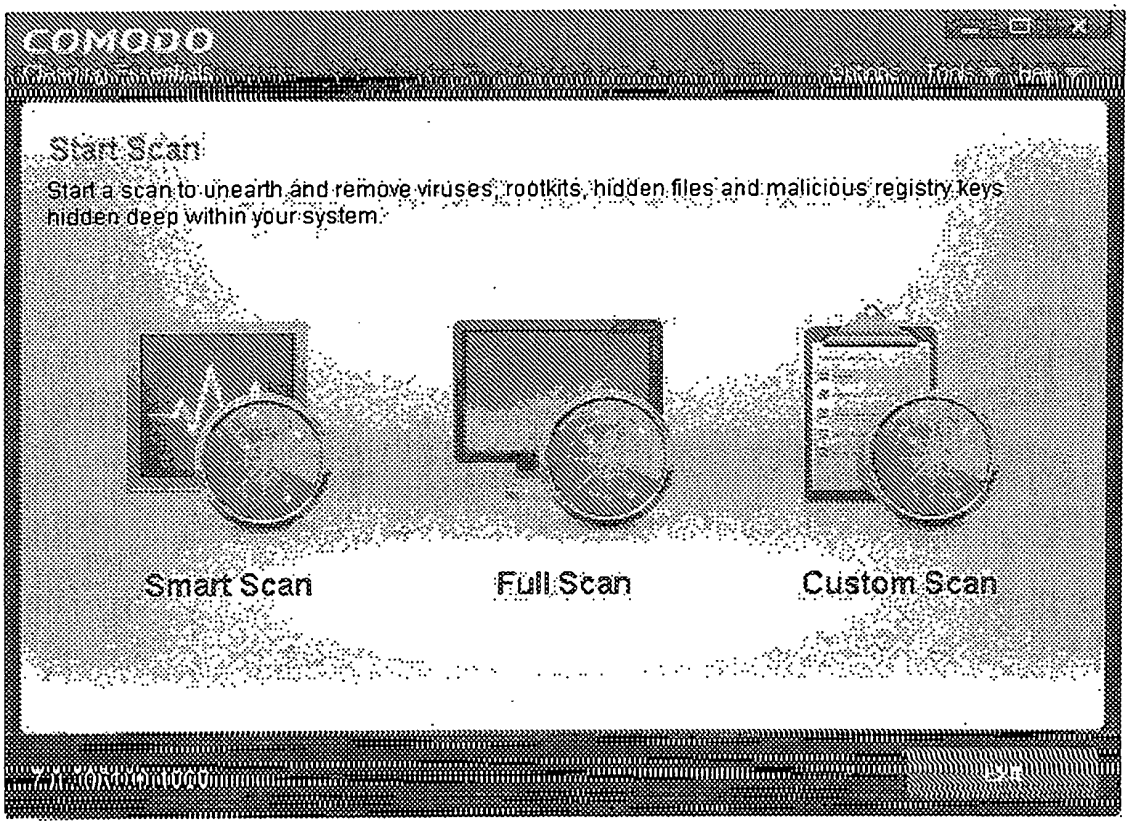
- Clicking the 'Clean Endpoint' for the first time, CIS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.



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



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



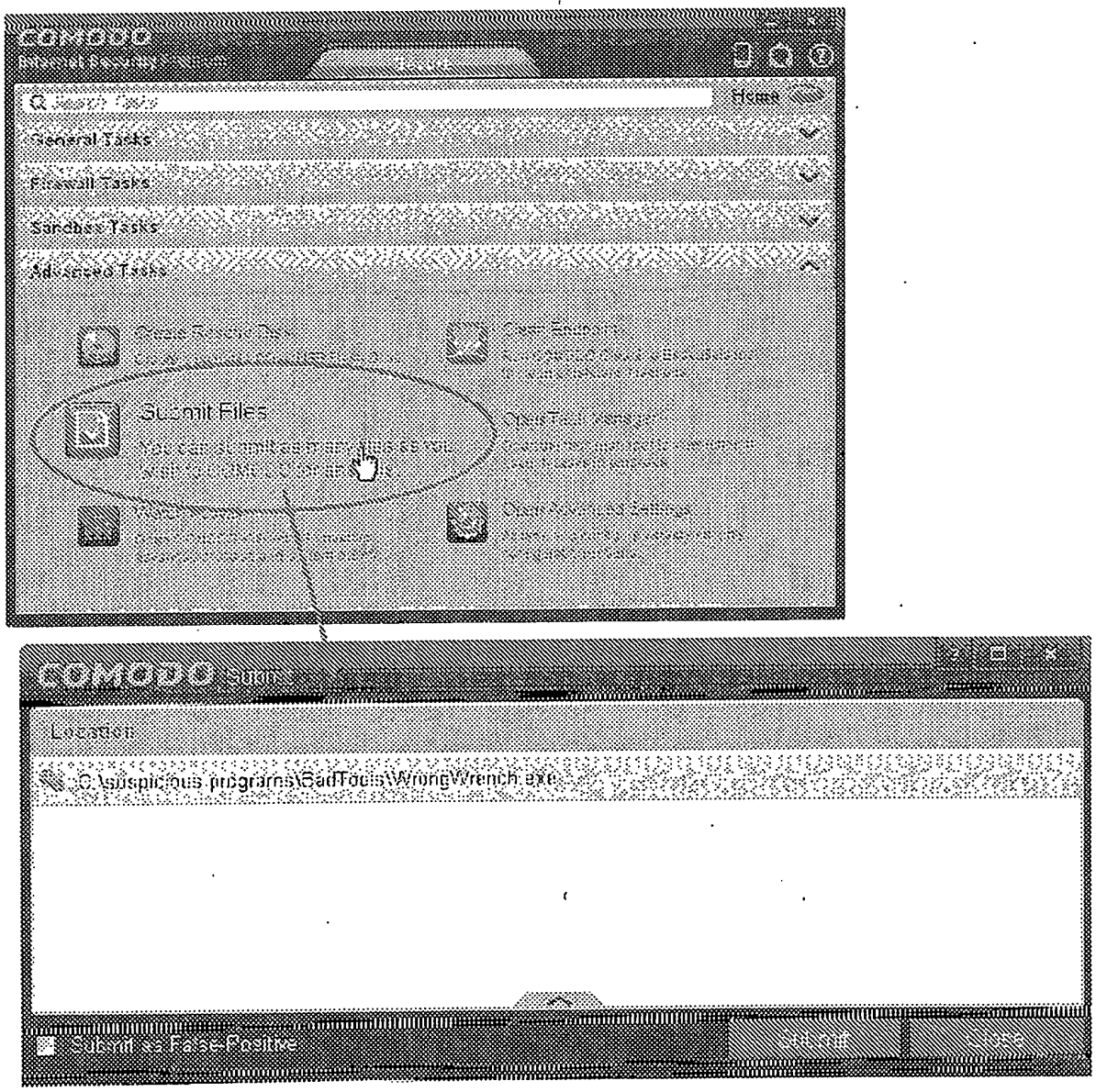
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at http://help.comodo.com/topic-115-1-328-3525-The-Main-Interface.html
- On clicking the 'Clean Endpoint' button from next time onwards, Comodo Cleaning Essentials will be opened.

5.3. Submit Files

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

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

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

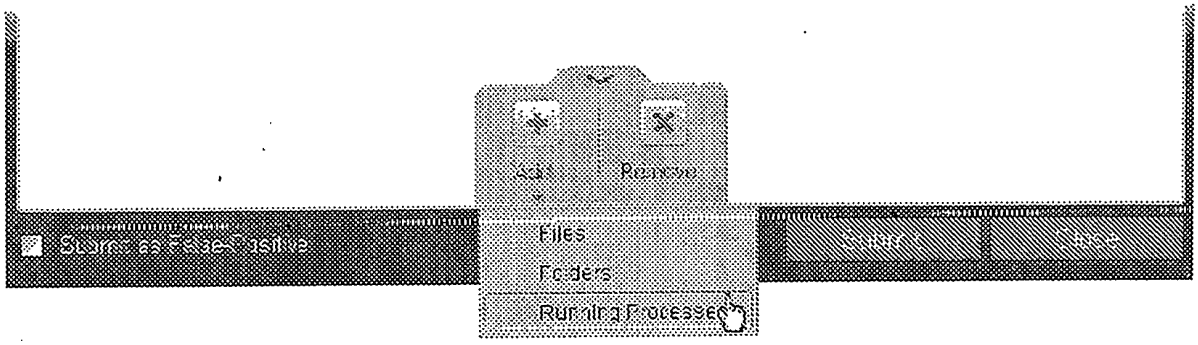


Clicking the handle at the bottom center of the panel opens the following options:

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

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

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



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

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

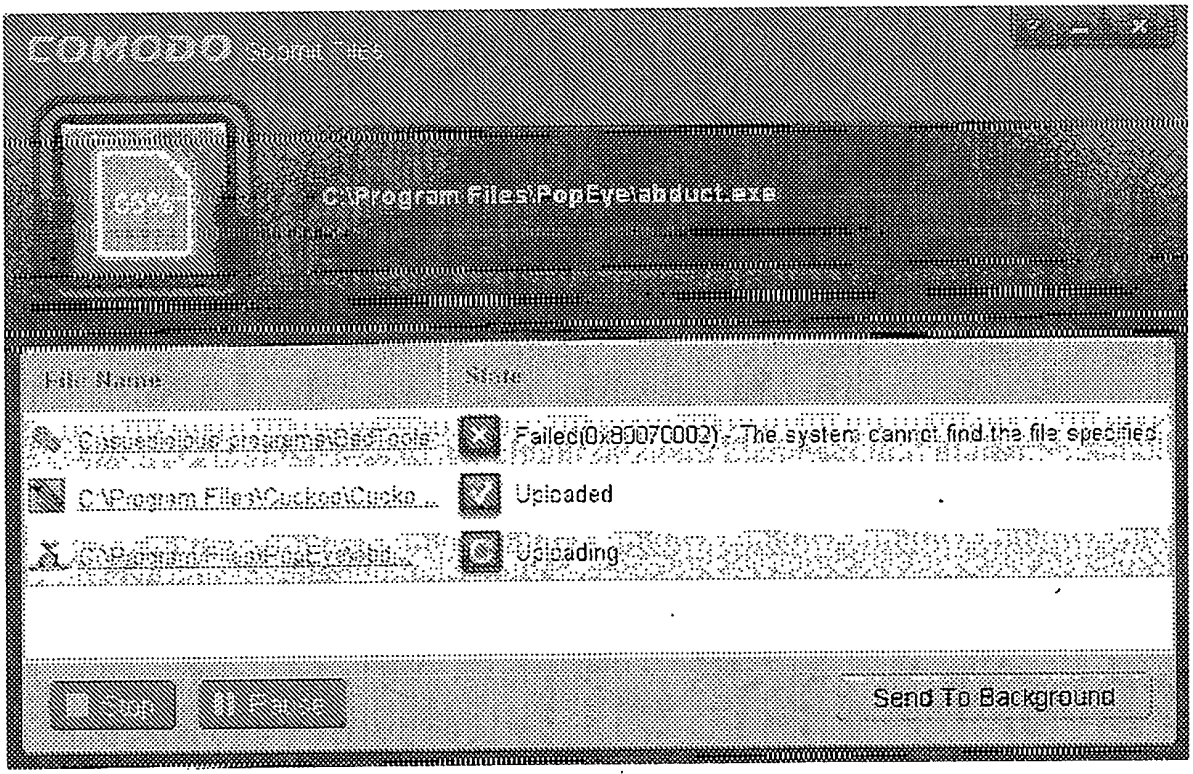
- Repeat the process to add more files and to submit them at-once.

To remove the files from 'Submit Files' list

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

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

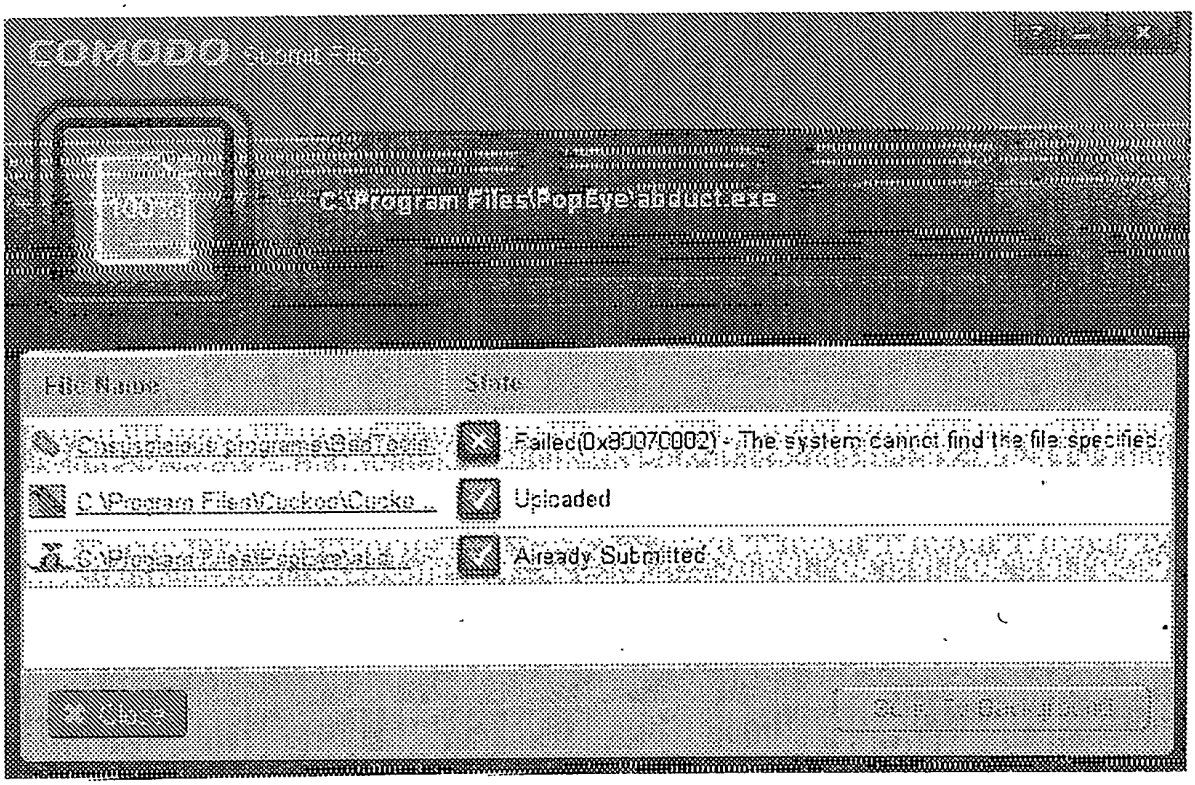
The files will be submitted and the progress will be displayed



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

When a file is first submitted, Comodo's online file look-up service will check whether the file is already queued for analysis by

our technicians. The results screen displays these results on completion.



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

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

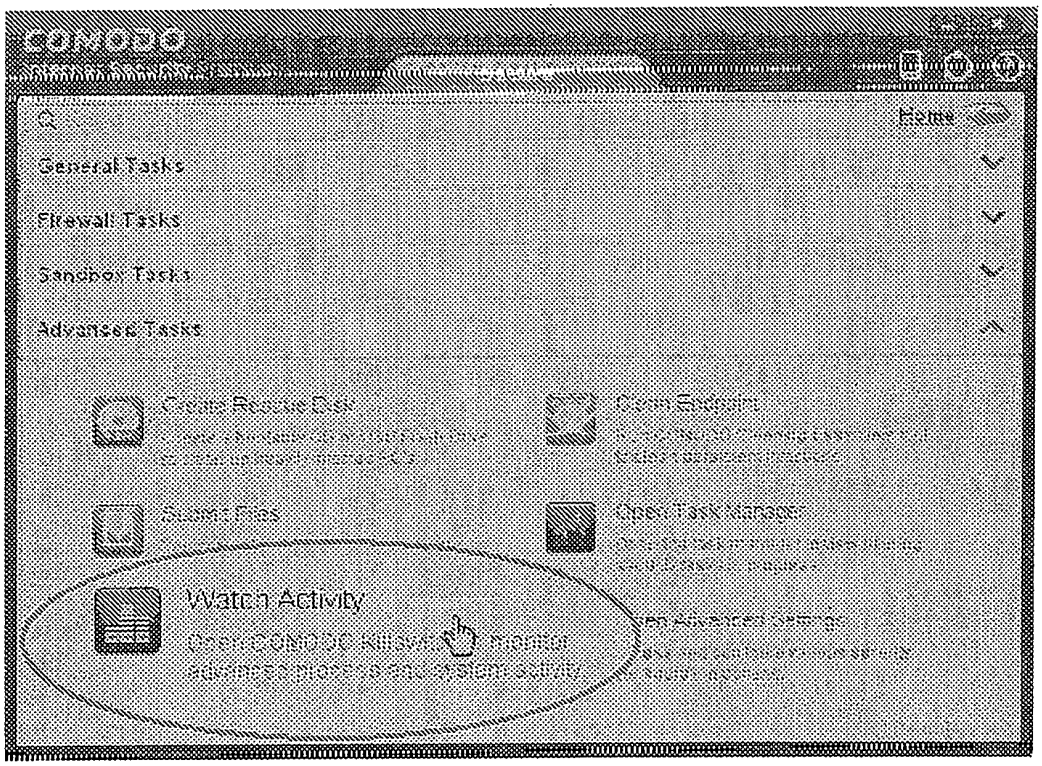
The list of files submitted from your computer can be viewed from the Submitted Files interface.

5.4. Identify and Kill Unsafe Running Processes

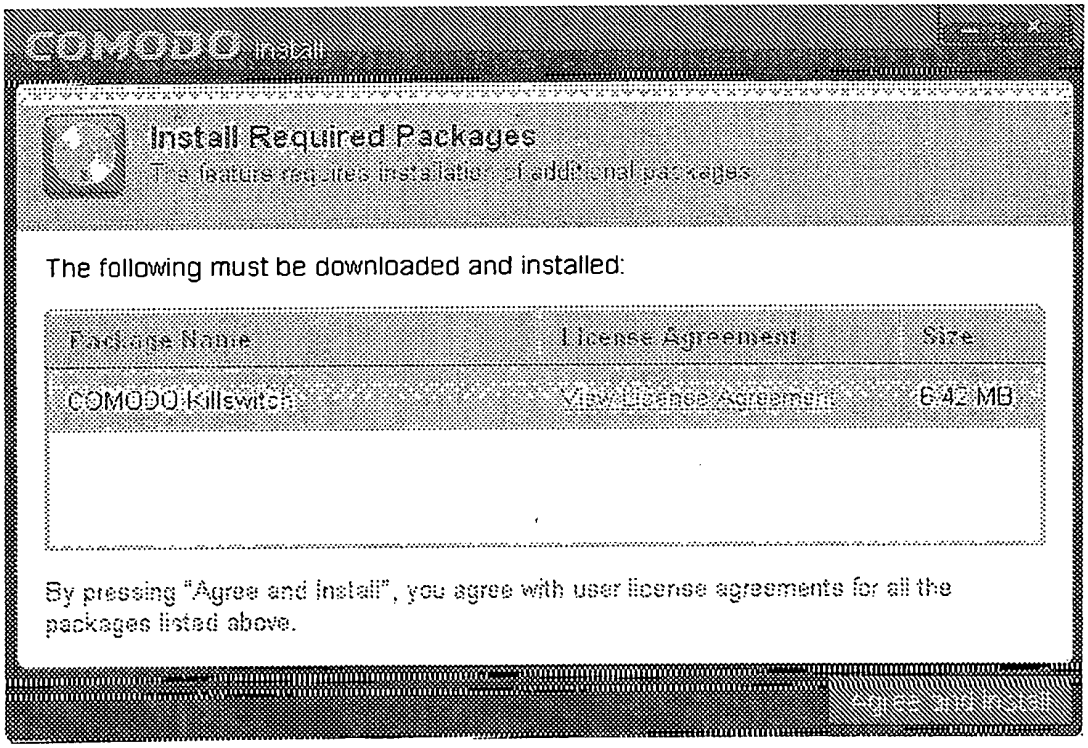
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer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

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

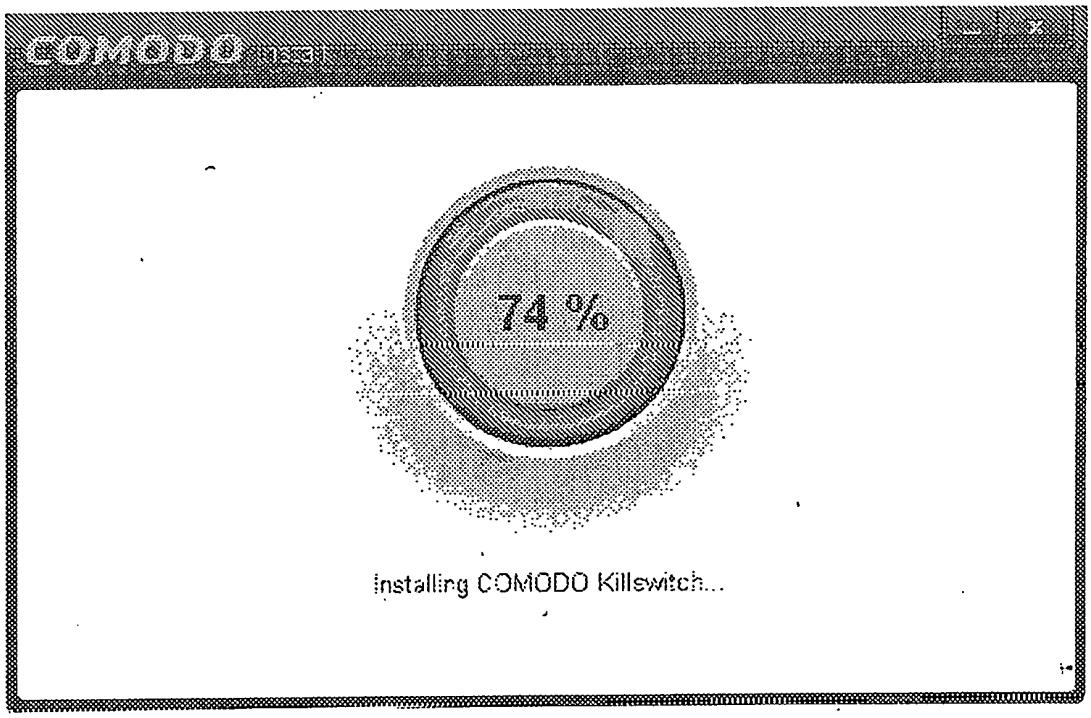
Comodo KillSwitch can be directly accessed from the CIS interface by clicking the 'Watch Activity' button in the 'Advanced Tasks' interface.



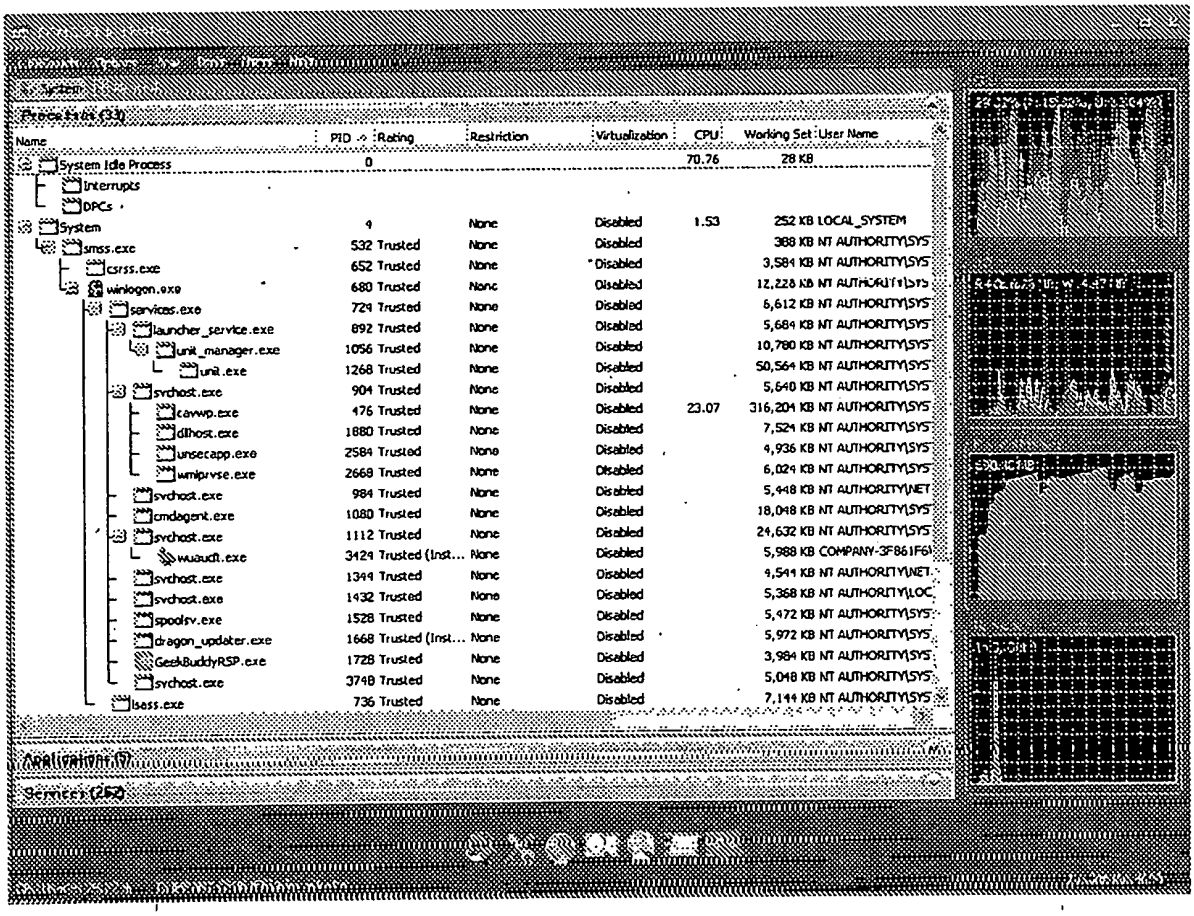
- Killswitch is a component of Comodo Cleaning Essentials. If you have already installed Comodo Cleaning Essentials by clicking 'Clean Endpoint' from the 'Advanced Tasks' interface, clicking the 'Watch Activity' will open the KillSwitch interface directly. Refer to the section Remove Deeply Hidden Malware for more details on installing Cleaning Essentials.
- Otherwise, on clicking the 'Watch Activity' for the first time, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.



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



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

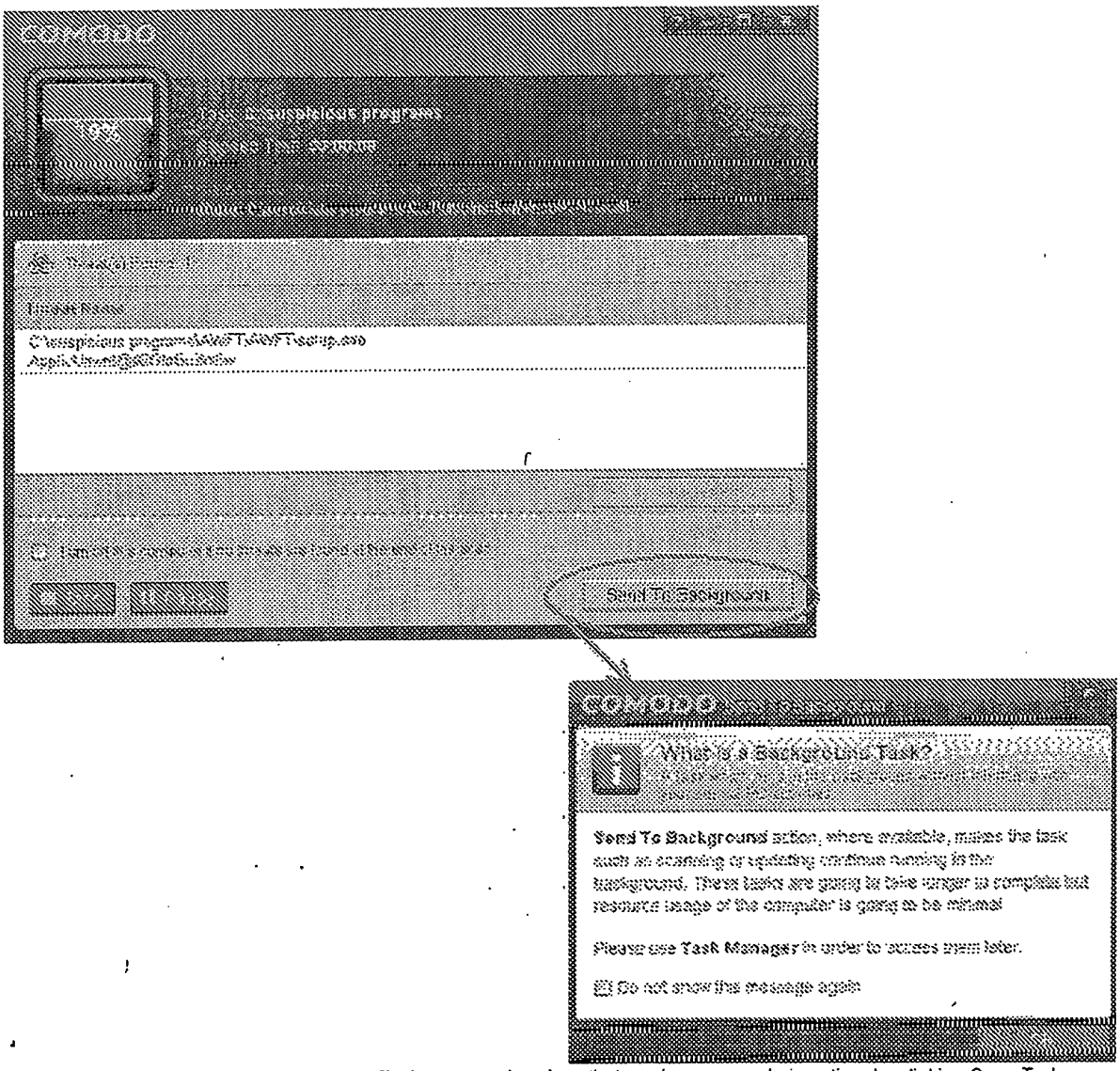


On clicking the 'Watch Activity' button from next time onwards, Comodo Killswitch will be opened.

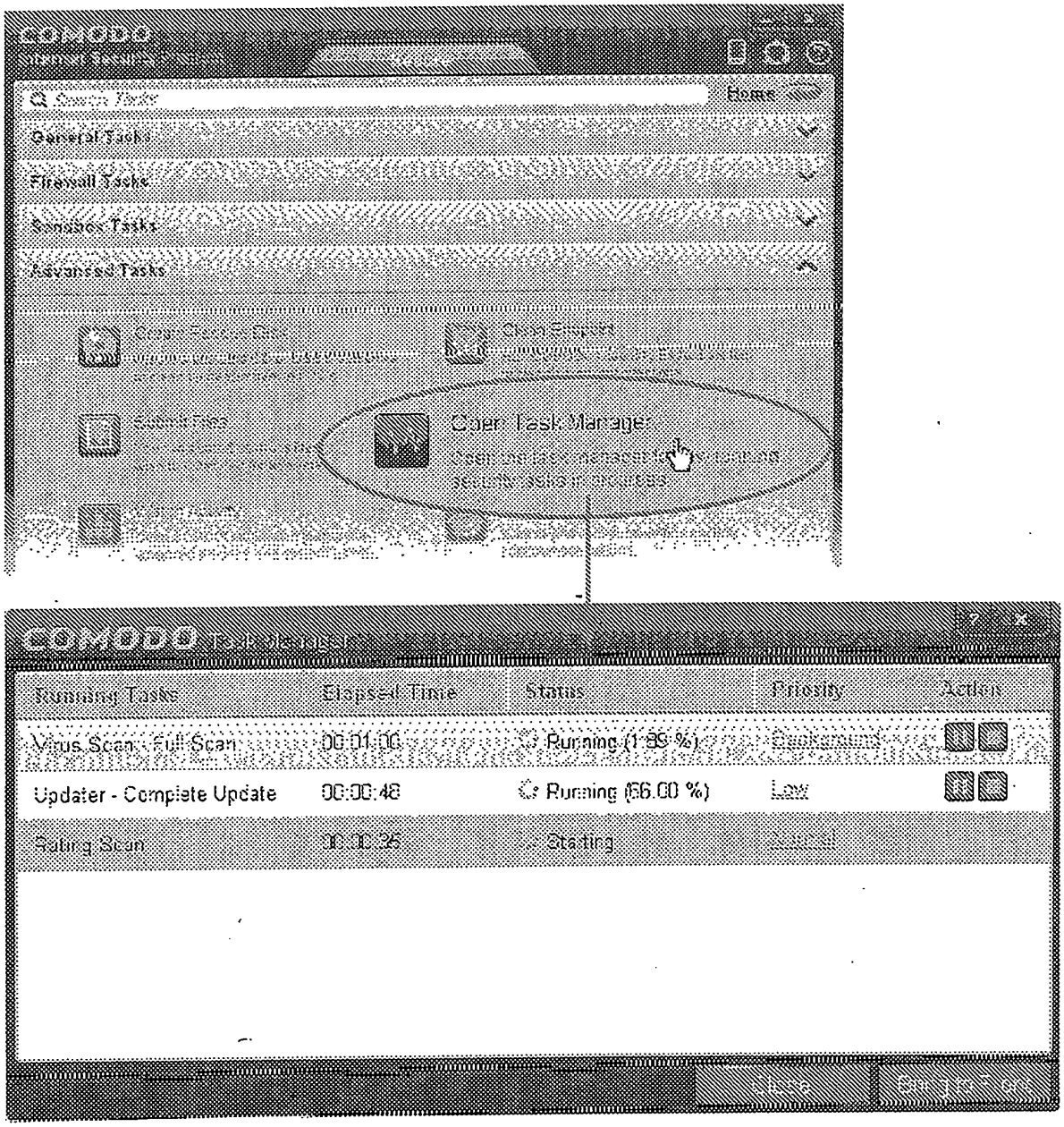
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html

5.5. Manage CIS Tasks

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



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



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

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

From the Task Manager interface, you can:

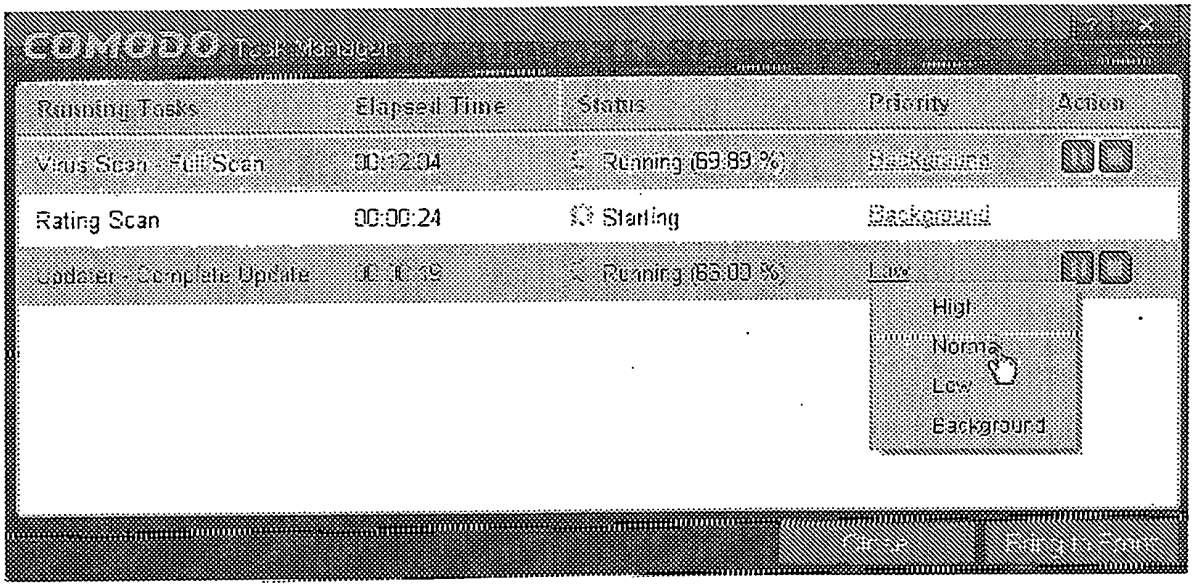
- Reassign priorities to the tasks
- Pause/Resume or Stop a running task
- Bring a selected task to foreground

Reassigning Priorities for a task:

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

To change the priority for a task

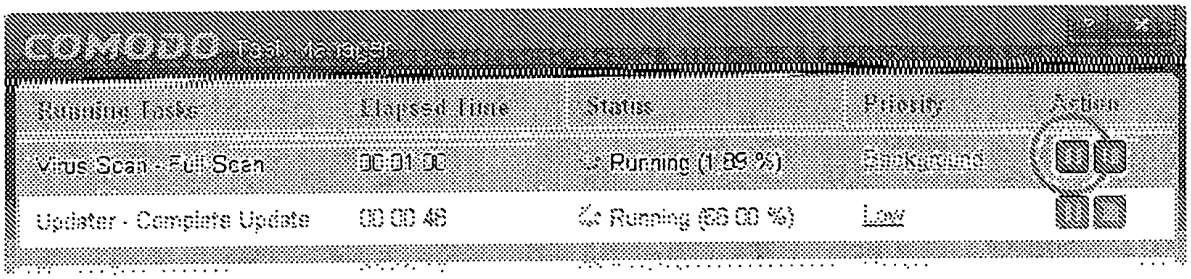
- Click on the current priority and select the priority you want to assign from the options.



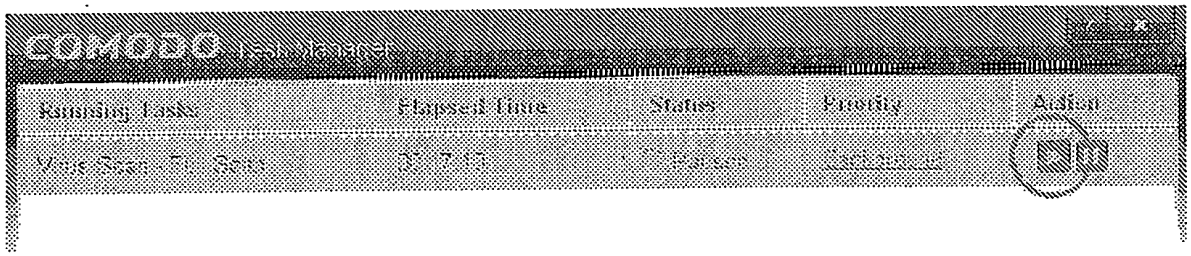
Pausing/Resuming or Stopping running tasks

The Action column displays the Pause/Resume and Stop buttons

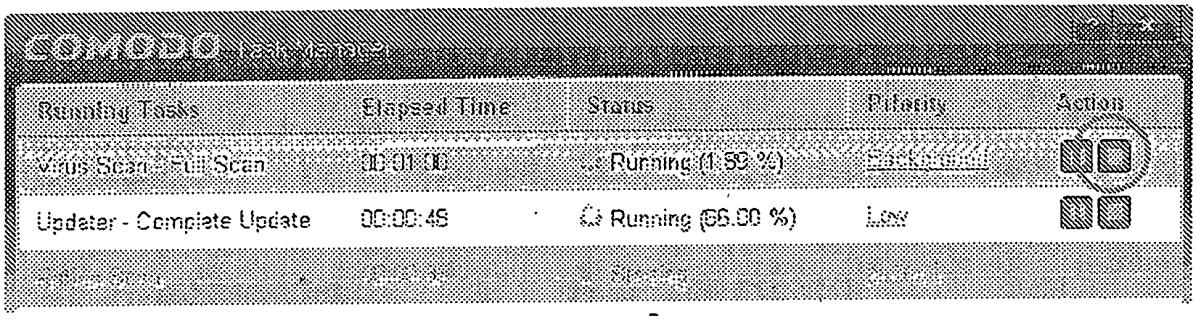
- To pause a running task, click the Pause button



- To resume a paused task, click the Resume button

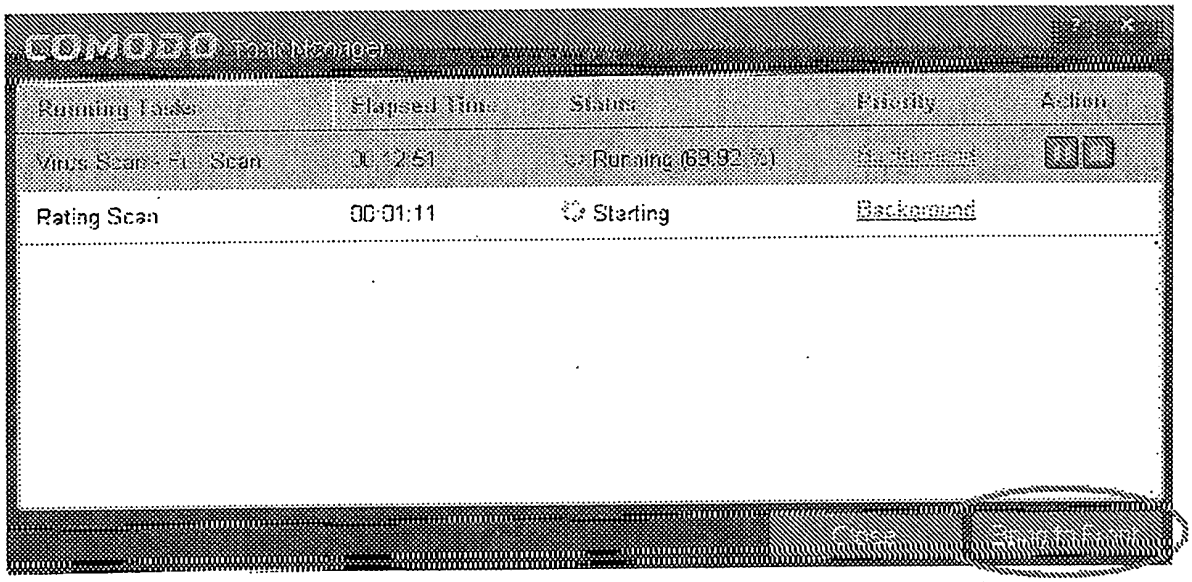


- To stop a running task, click the stop button

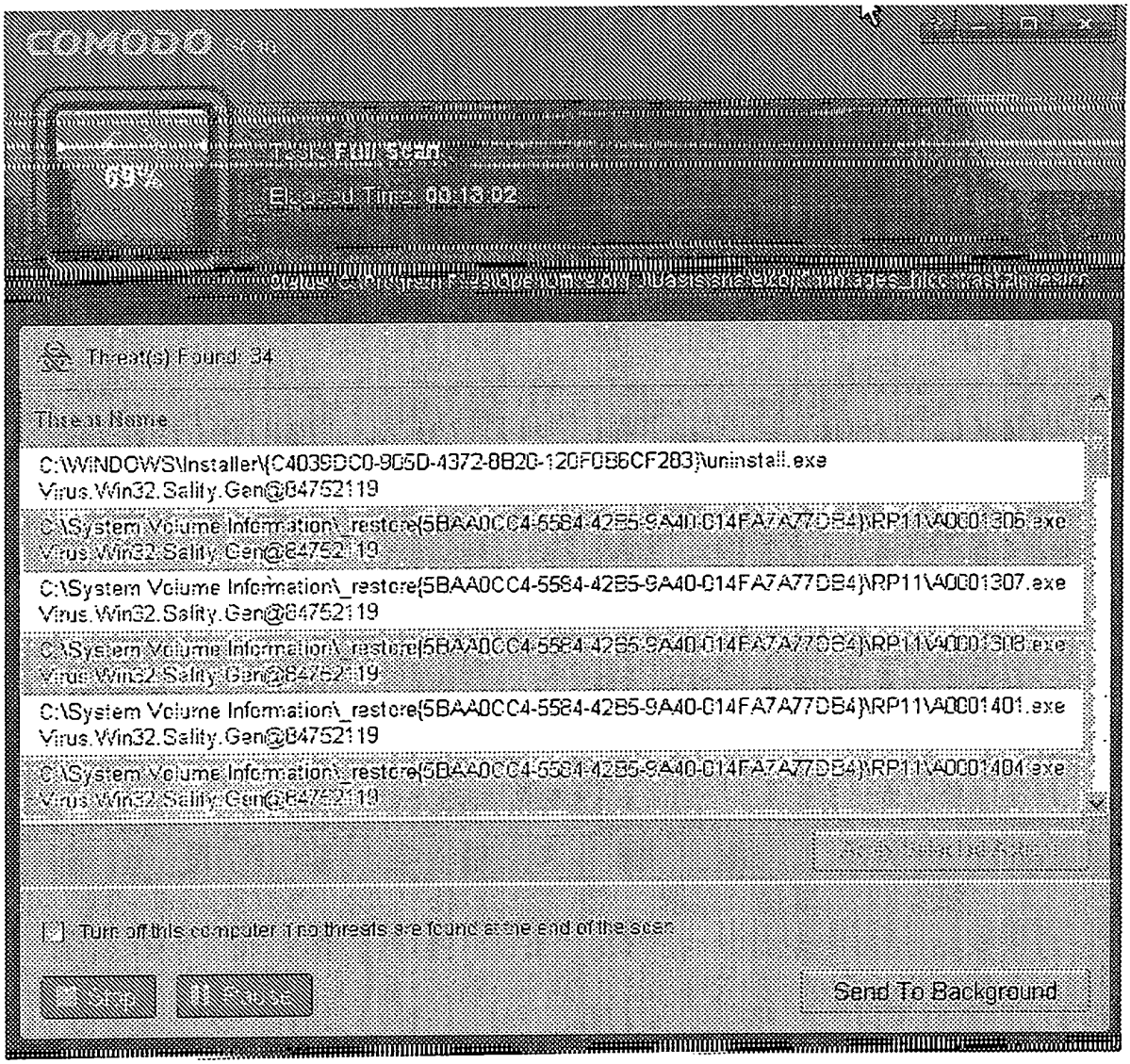


Bringing a running task to foreground

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



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

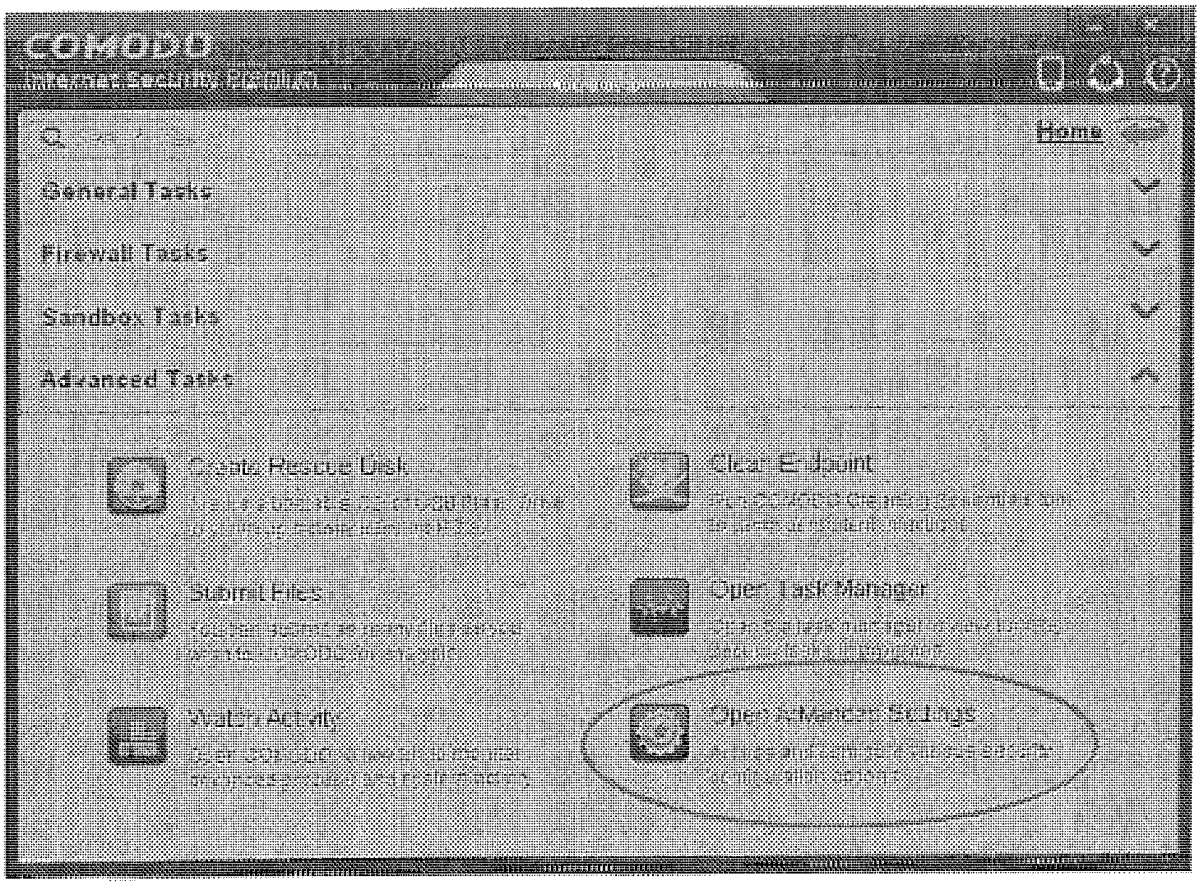


6. Advanced Settings

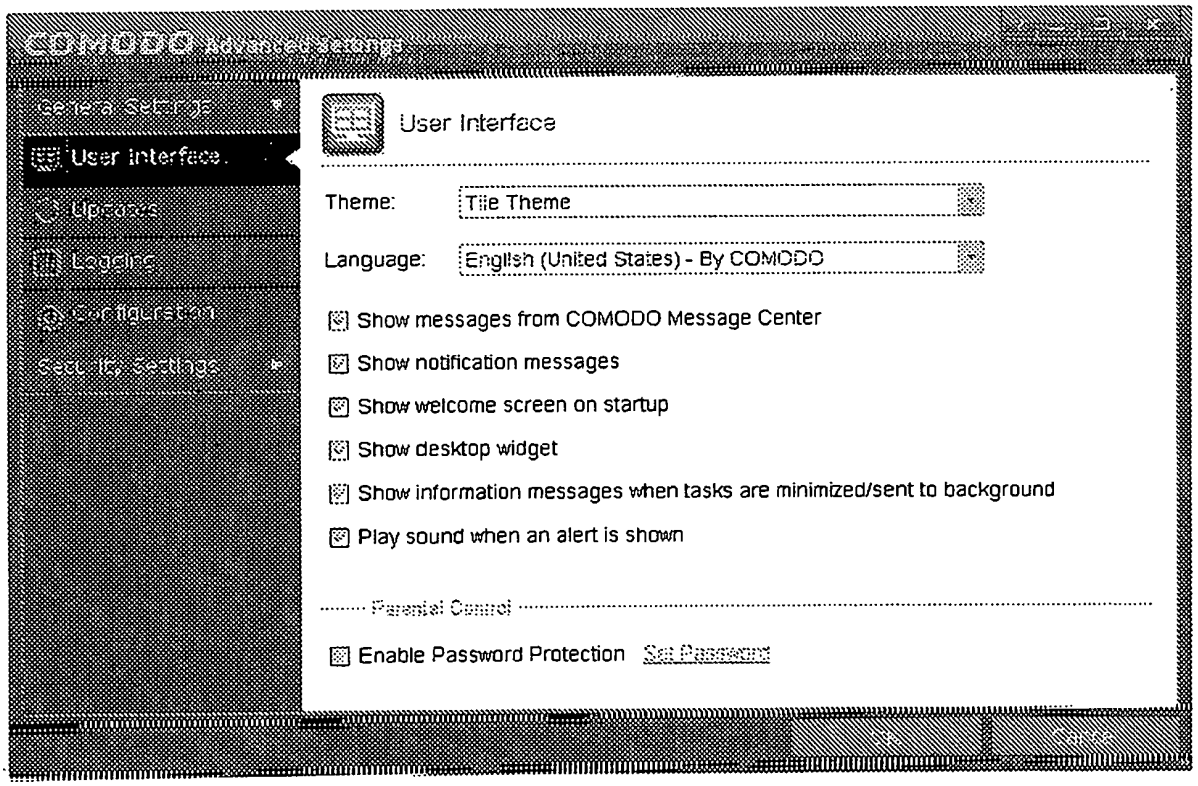
The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Internet Security. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced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

To open 'Advanced Settings':

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



The 'Advanced Settings' panel will open:



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

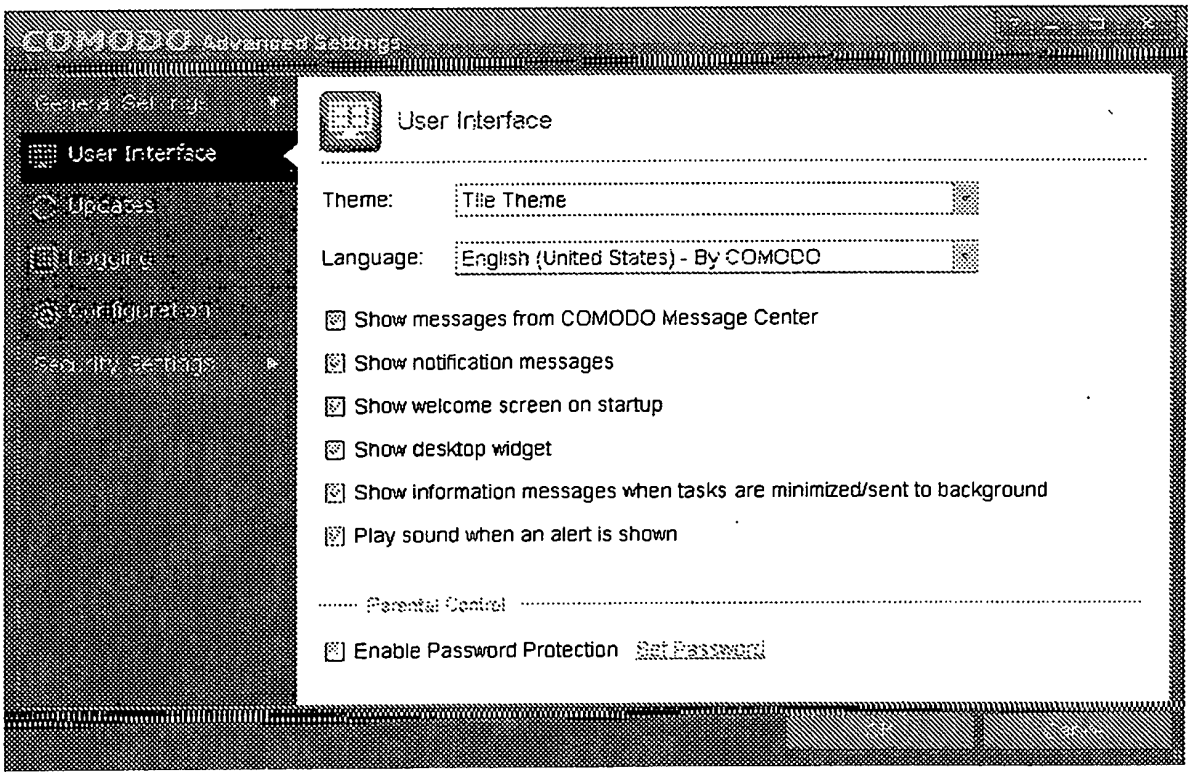
- General Settings - Allows you to configure the appearance and behavior of the application

- Customize User Interface
- Configure Program and database Updates
- Log Settings
- Manage CIS Configurations

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

6.1. General Settings

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

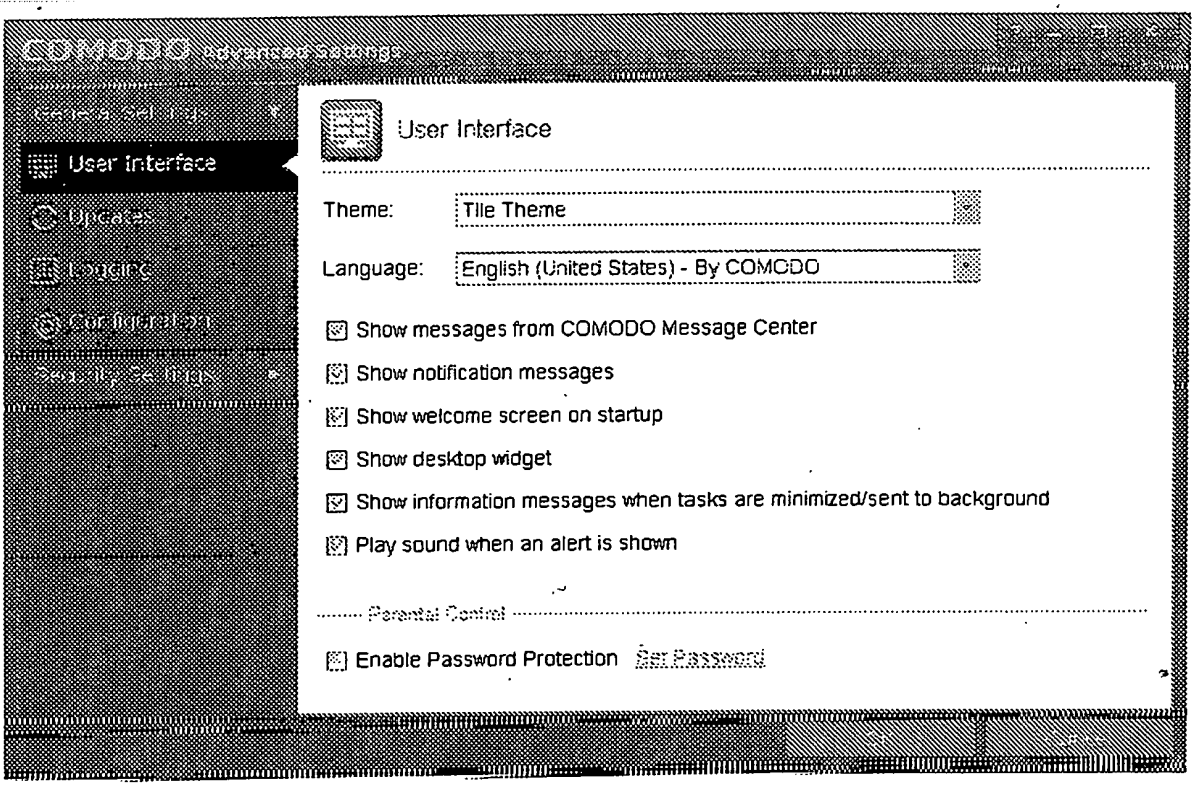


The category has the following settings:

- User Interface
- Updates
- Logging
- Configuration

6.1.1. Customize User Interface

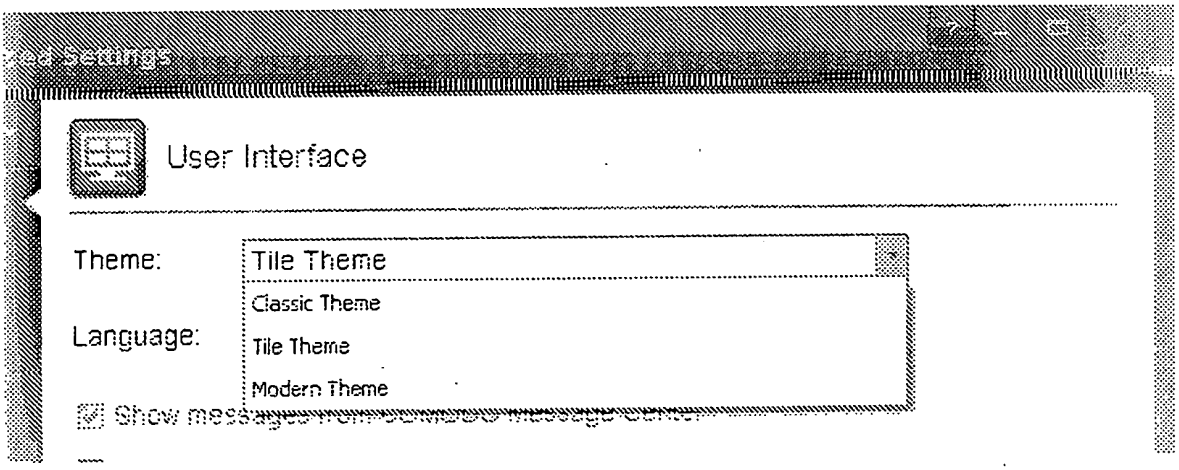
The 'User Interface' tab lets you choose the display theme, interface language and customize the look and feel of Comodo Internet Security according to your preferences. You can also configure how messages are displayed and enable password protection for your settings.



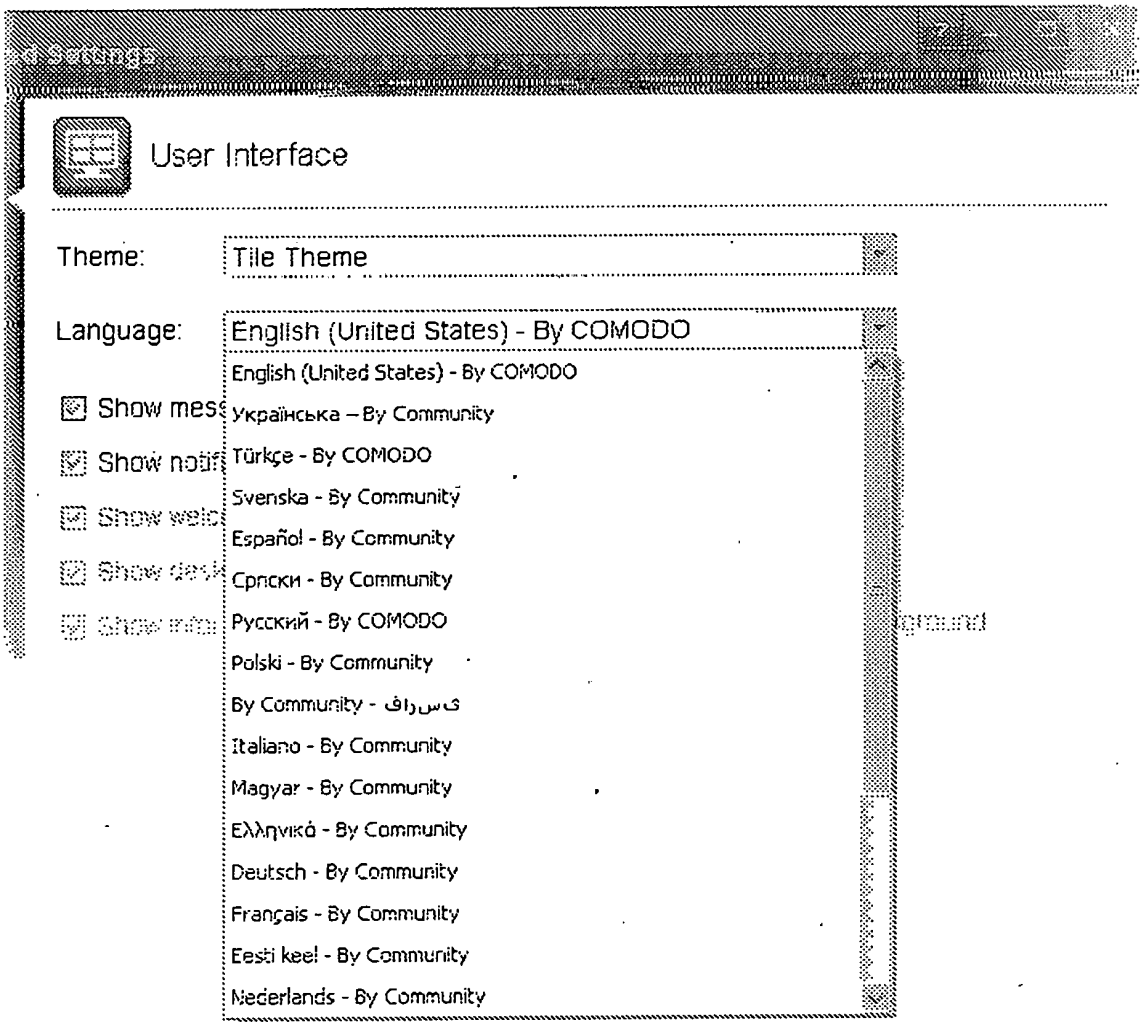
The User Interface Settings allows you configure the following:

- Themes
- Language
- Show messages from COMODO Message Center
- Show notification messages
- Show Welcome screen on start up
- Show desktop widget
- Show information messages when tasks are minimized/sent to background
- Play sound when an alert is shown
- Enable Password Protection

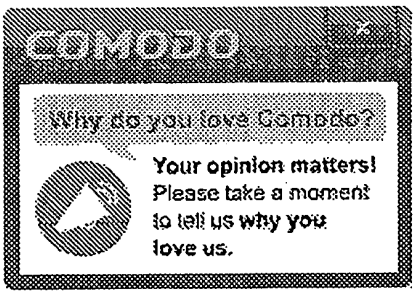
- **Theme** - The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (***Default = Tile Theme***).



- **Language Settings** - Comodo Internet Security is available in multiple languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (***Default = English (United States)***).



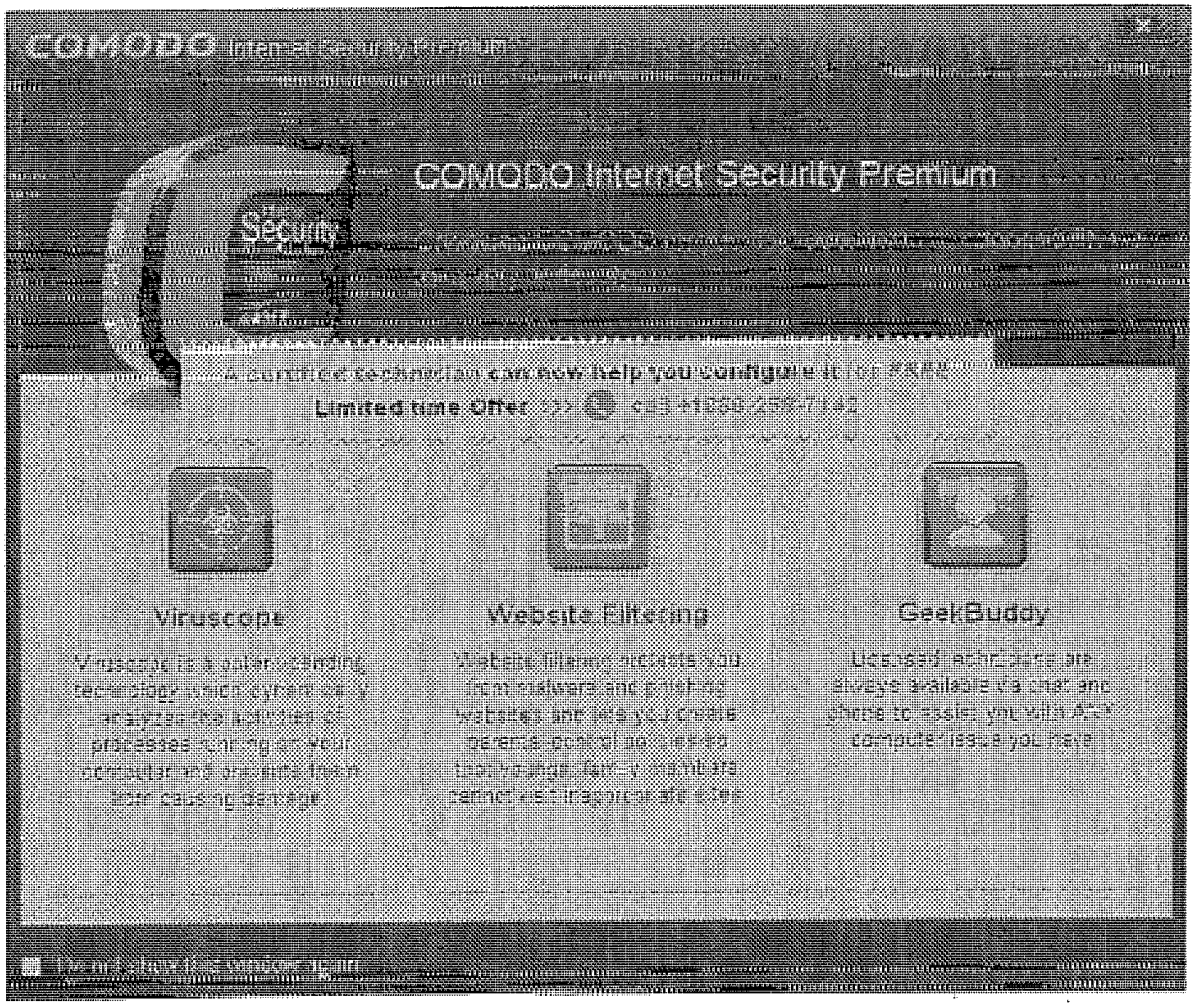
- **Show messages from COMODO Message Center** - If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world.



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

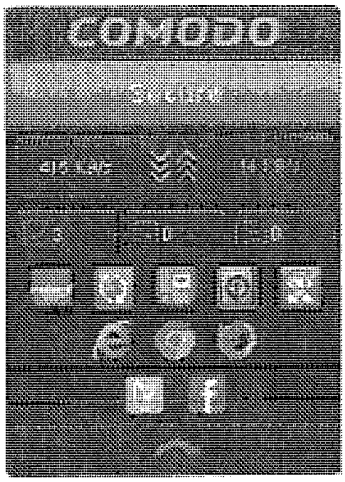
- **Show notification messages** - These are the CIS system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CIS is taking and any CIS status updates. For example ' Comodo Firewall is learning ' or 'Defense+ is learning ' are generated when these modules are learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in Antivirus > Real-time Scan settings screen. Clear this check box if you do not want to see these system messages (***Default = Enabled***).
- **Show Welcome Screen on start up** - If enabled, CIS will display a welcome screen when the application first starts

(*Default = Enabled*):



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

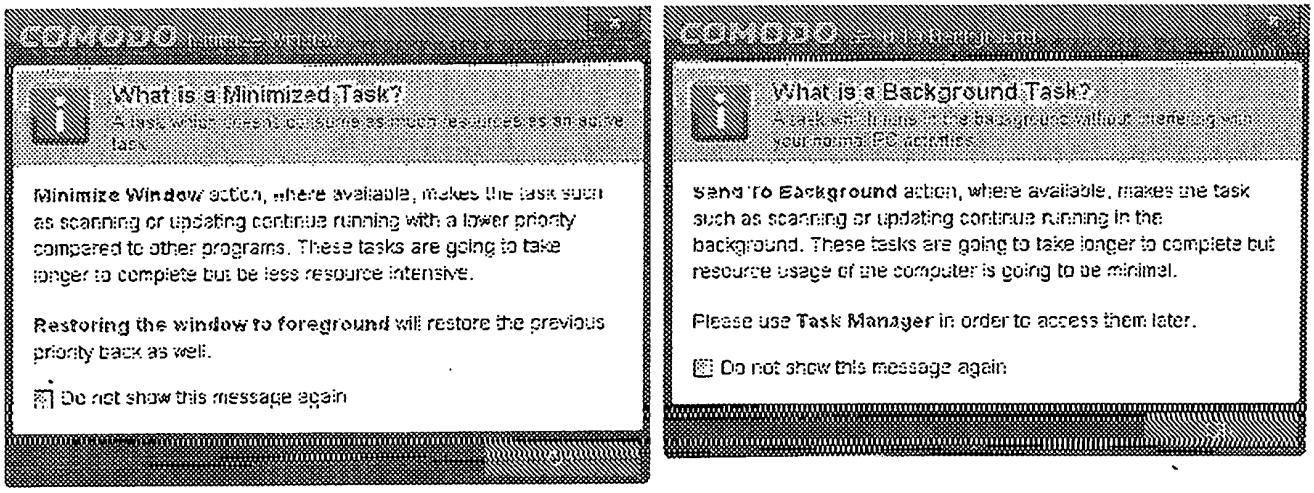
- **Show desktop widget** - The CIS desktop widget displays at-a-glance information about CIS security status, speed of outgoing and incoming traffic, number of background tasks and links to social networking sites.



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

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

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



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

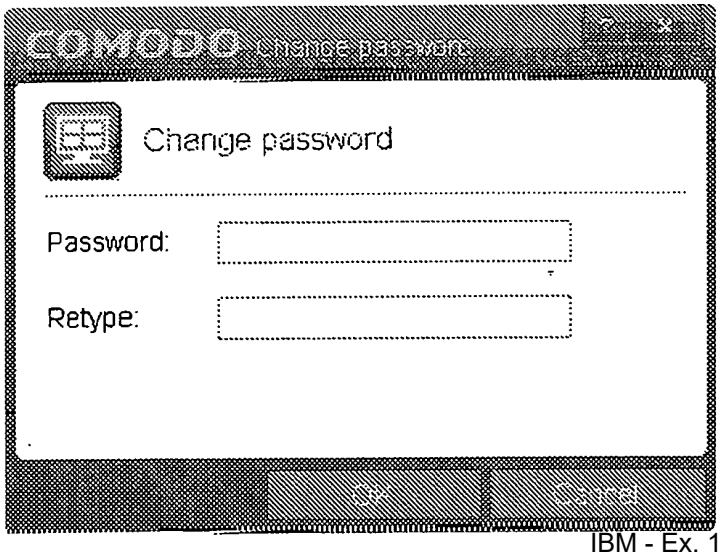
Tip: You can also disable these messages in the message window itself by selecting 'Do not show this message again'

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

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

  To enable password protection

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

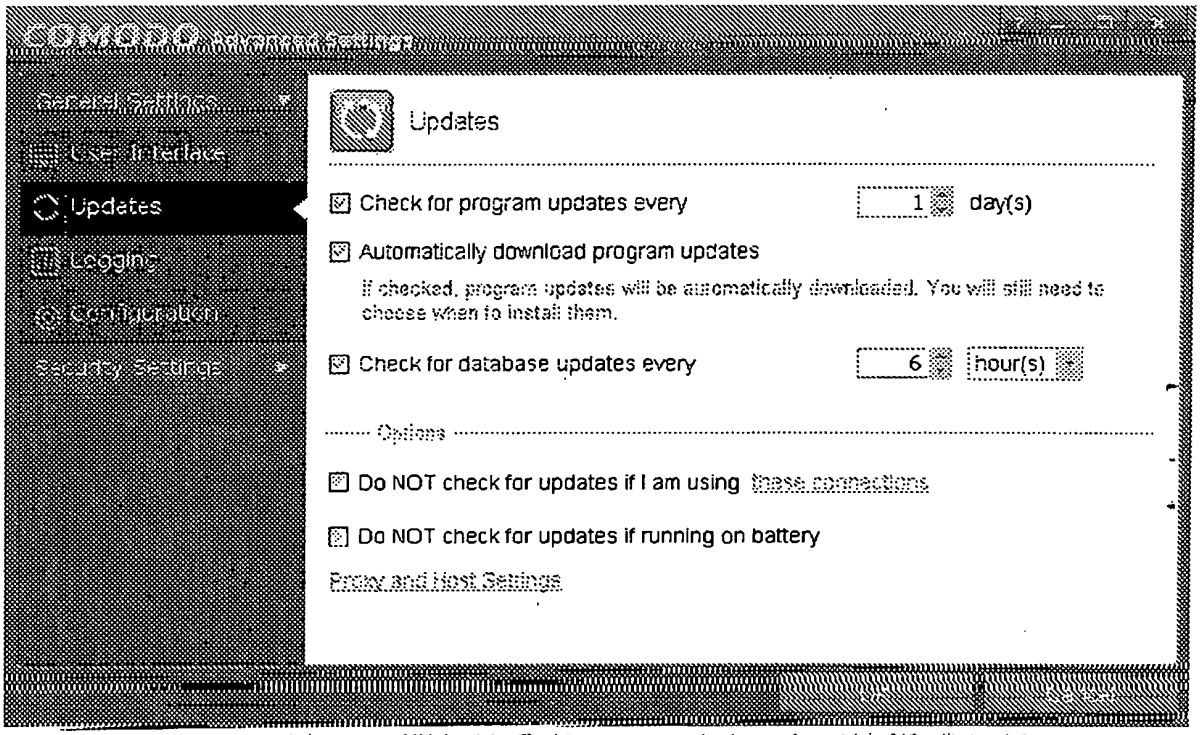


- Enter and confirm your password then click OK. Make sure to create a strong password containing a mixture of uppercase and lowercase characters, numbers and symbols so that it cannot be easily guessed by others.

6.1.2. Configure Program and Virus Database Updates

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

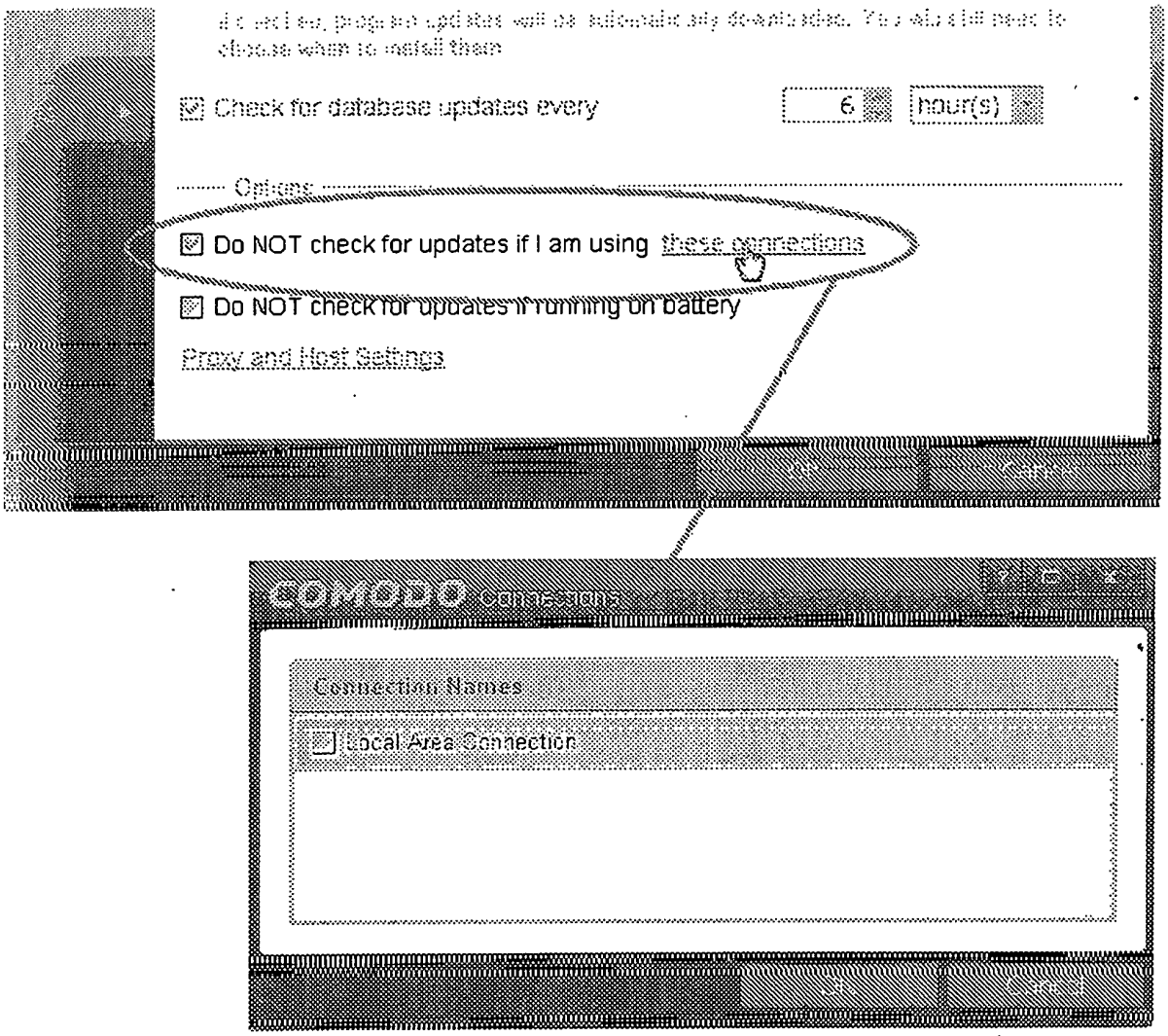
This screen can be accessed by clicking 'Updates' under the 'General Settings' section of 'Advanced Settings':



- **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.

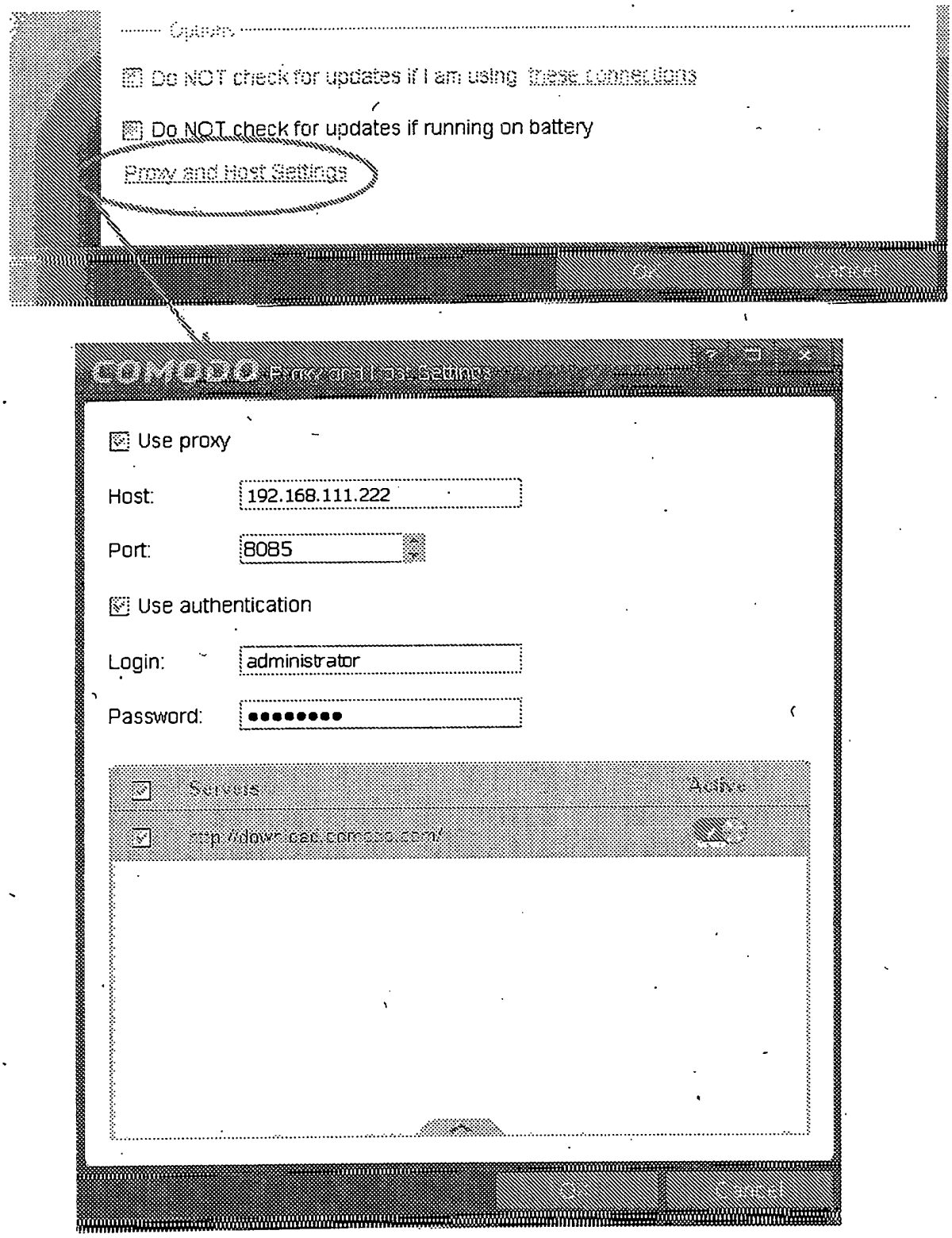
- **Do NOT check for updates if running on battery** - If enabled, CIS will not download updates if it detects your computer is running from battery power. This is intended to extend battery lifetime on laptops. ***(Default = Enabled)***

- **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.

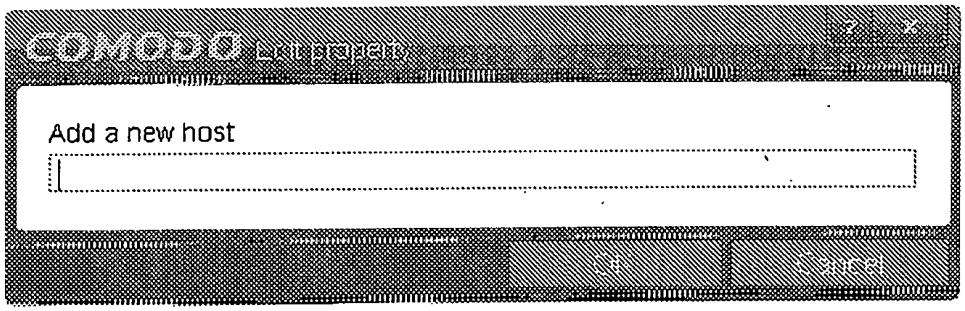
Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php

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.

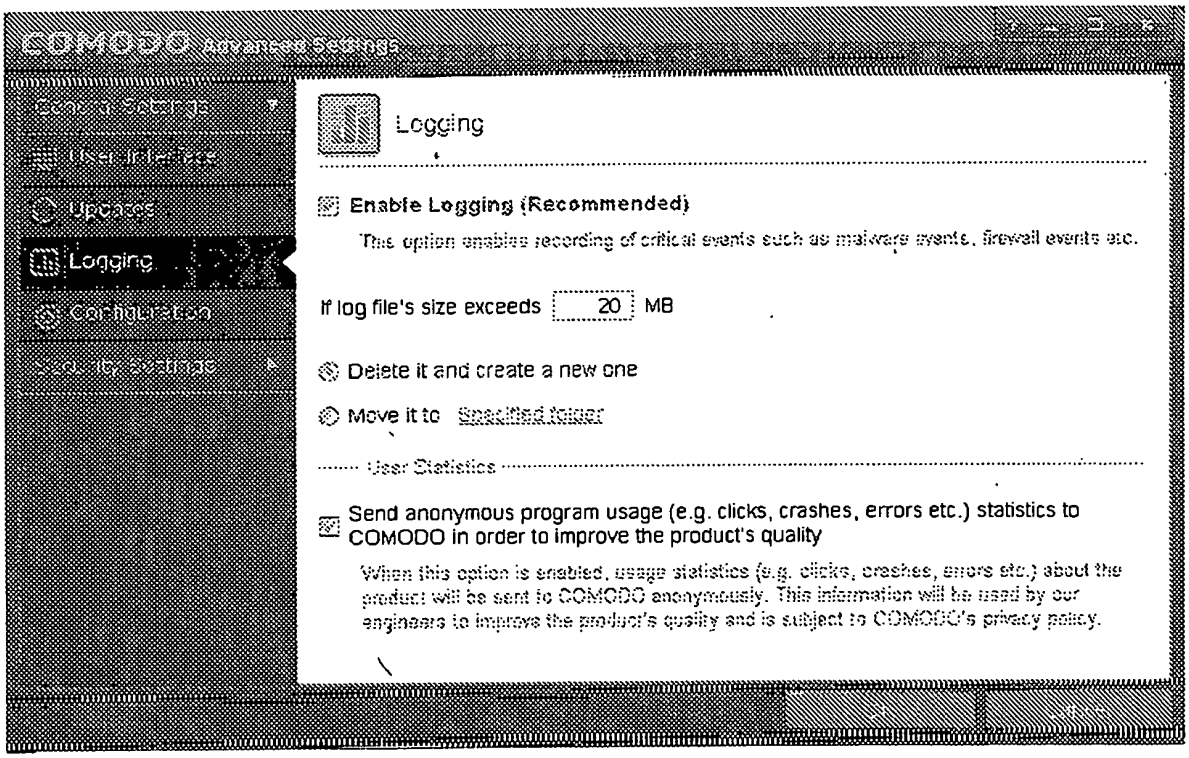


- If you specify multiple servers:
  - Activate or deactivate each update server using the 'Active' toggle switch alongside it
  - Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CIS will commence downloading from the first server that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

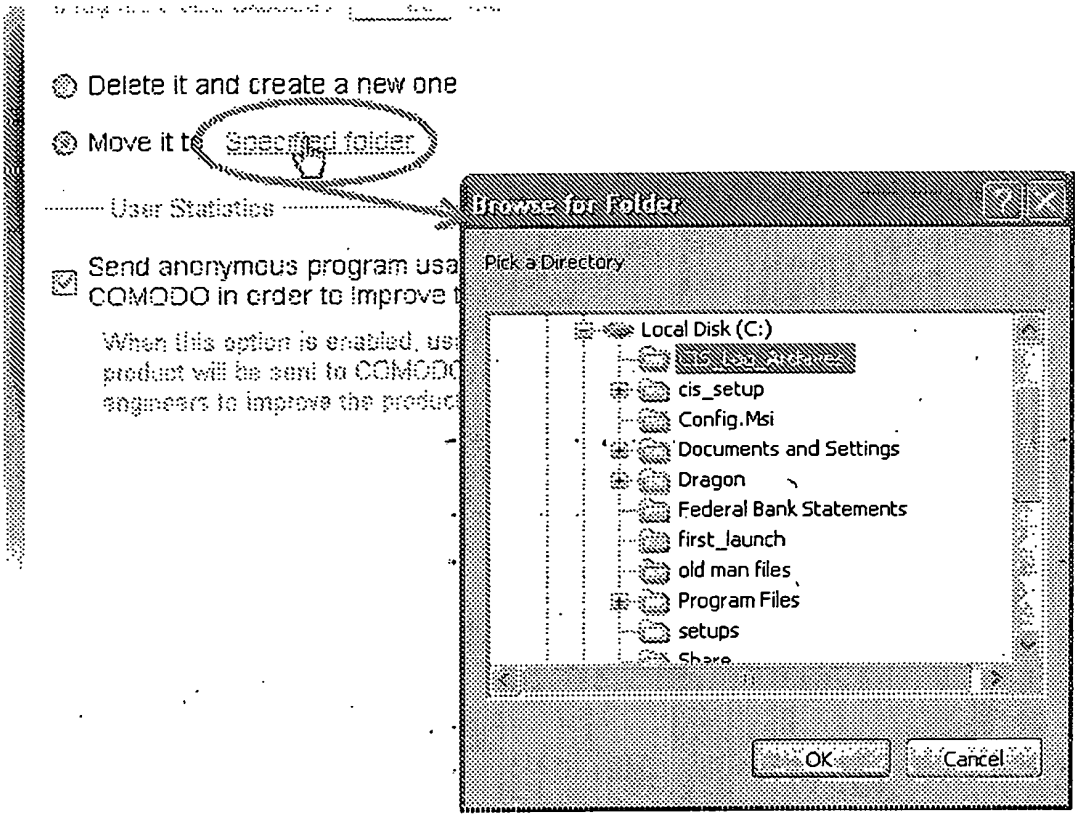


- **Enable Logging** - CIS logs events only if this setting is enabled. (*Default = Enabled*)
- **If the log file's size exceeds (Mb(s))** - Enables you to specify behavior when the log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending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

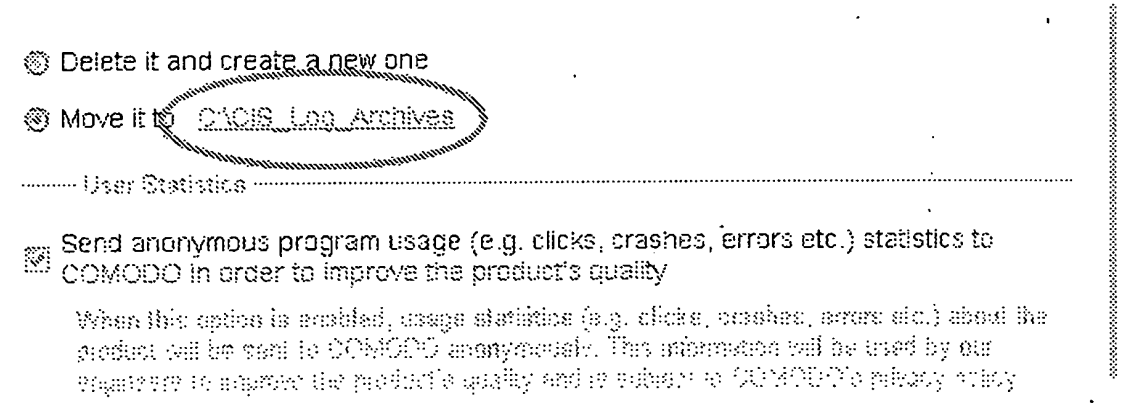
(MB)' *(Default = 20MB).*

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 installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Any such information

IPR2025-00379 (IBM v. Croga)

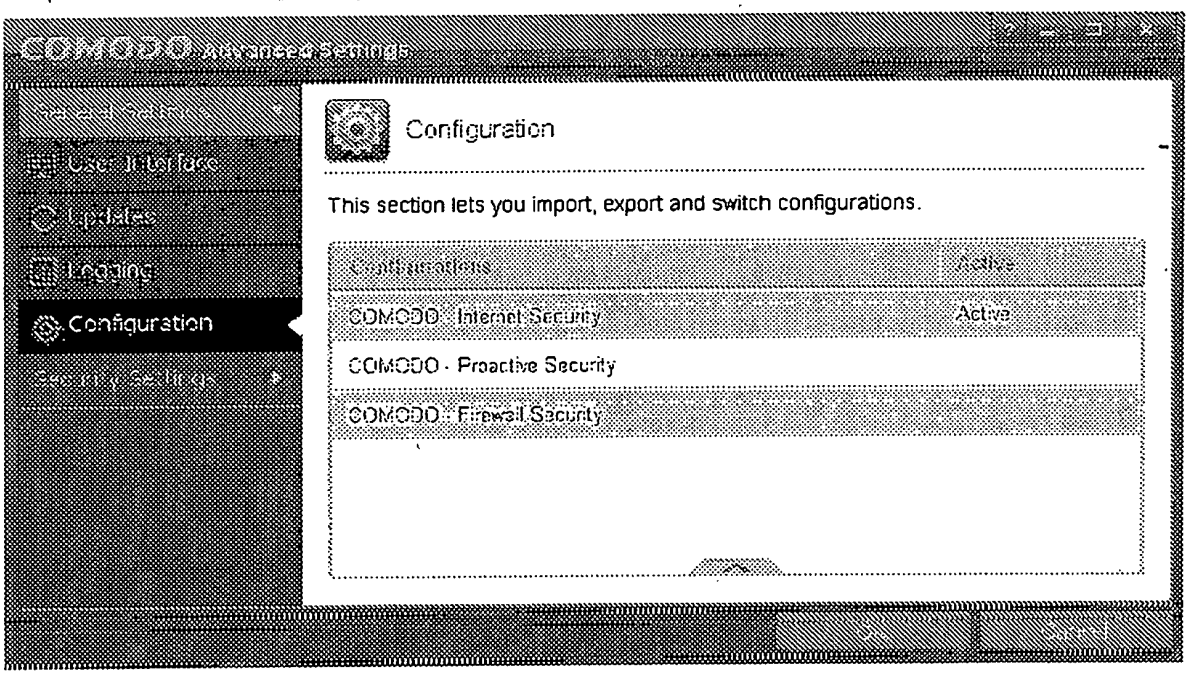
is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. ***(Default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

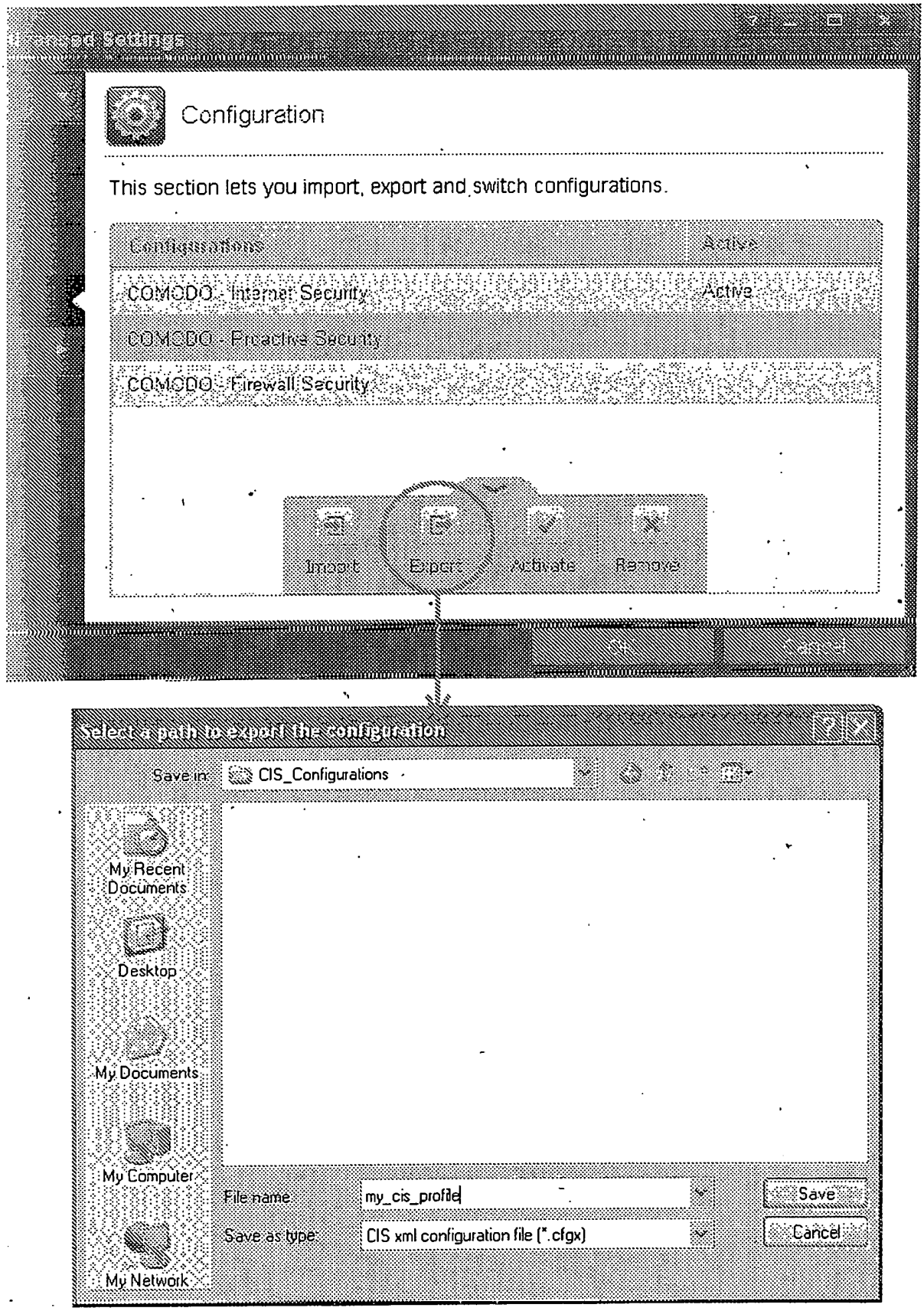
The CIS configurations can be exported/imported, activated and managed through the Configuration panel accessible by clicking 'Configuration' tab under 'General Settings' in 'Advanced Settings' interface.

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.

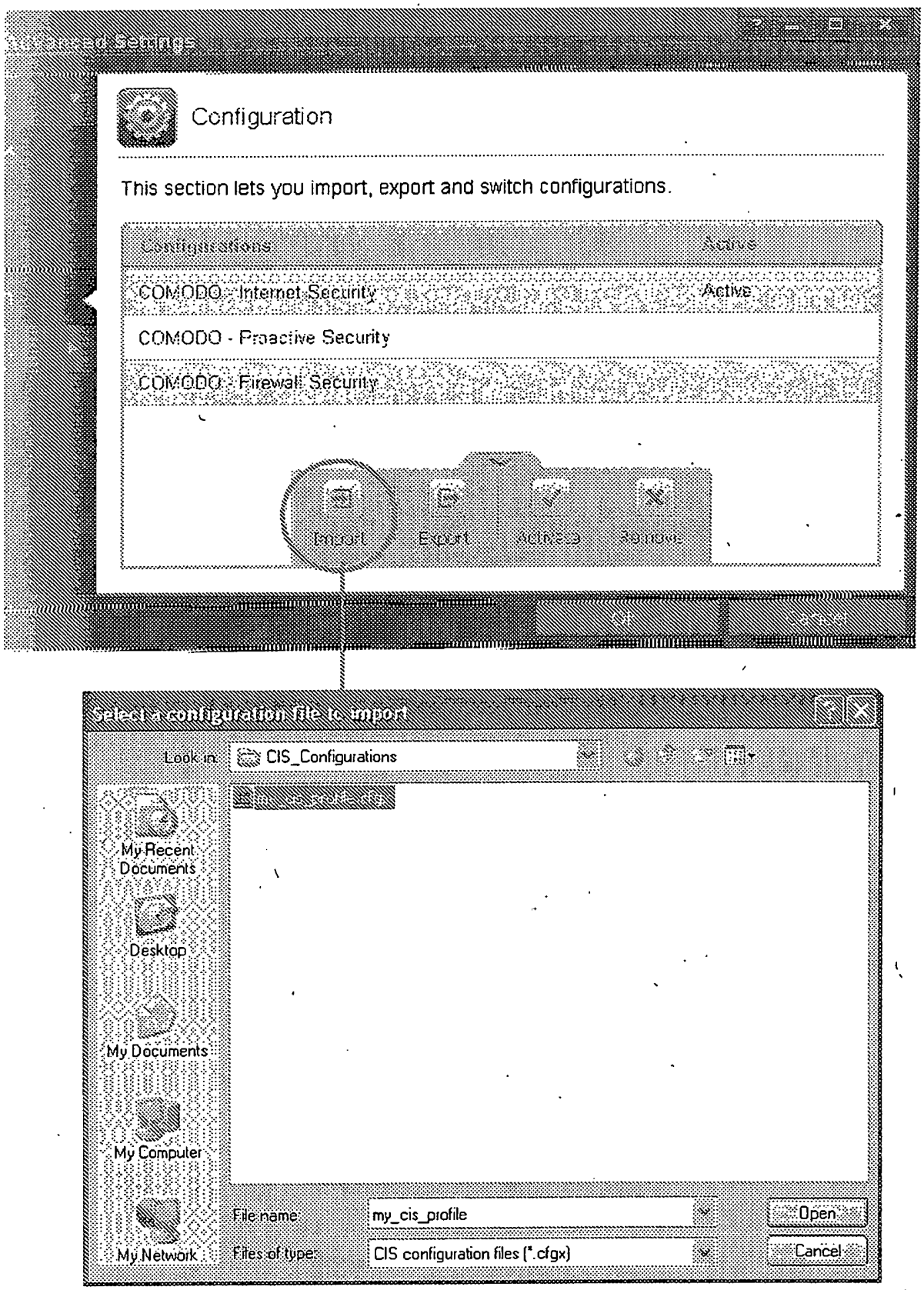


Importing a saved configuration from a file

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.

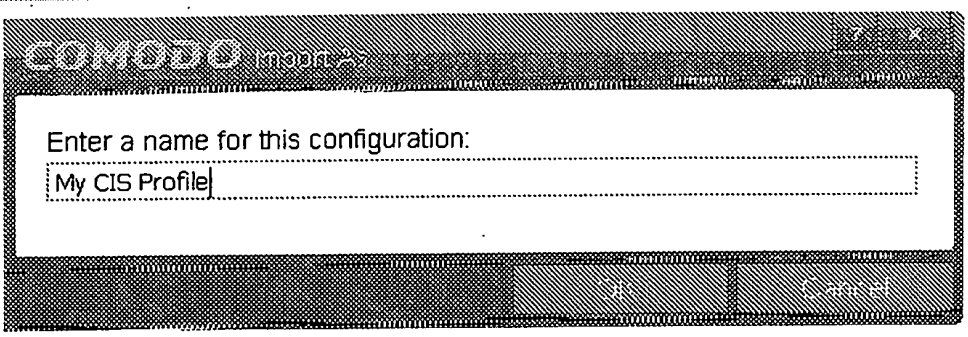
To import a profile

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.

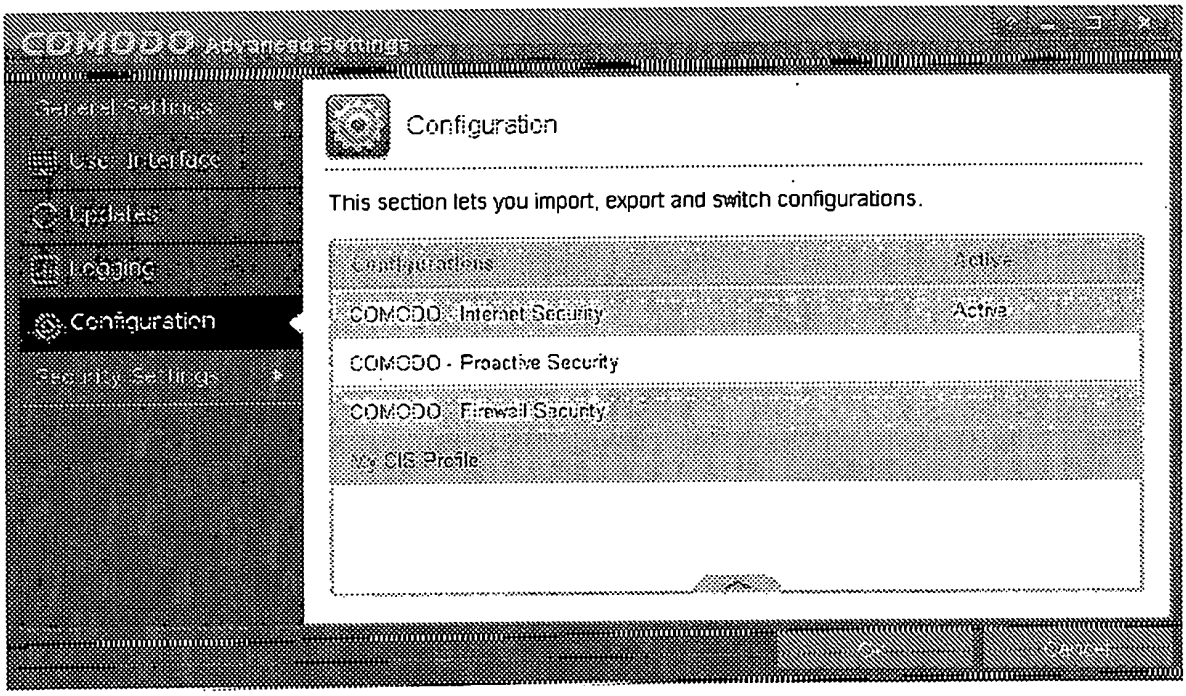
2. Navigate to the location of the saved profile and click 'Open'.
3. The 'Import As' dialog will appear. Enter a name for the profile you wish to import and click 'OK'.



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



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

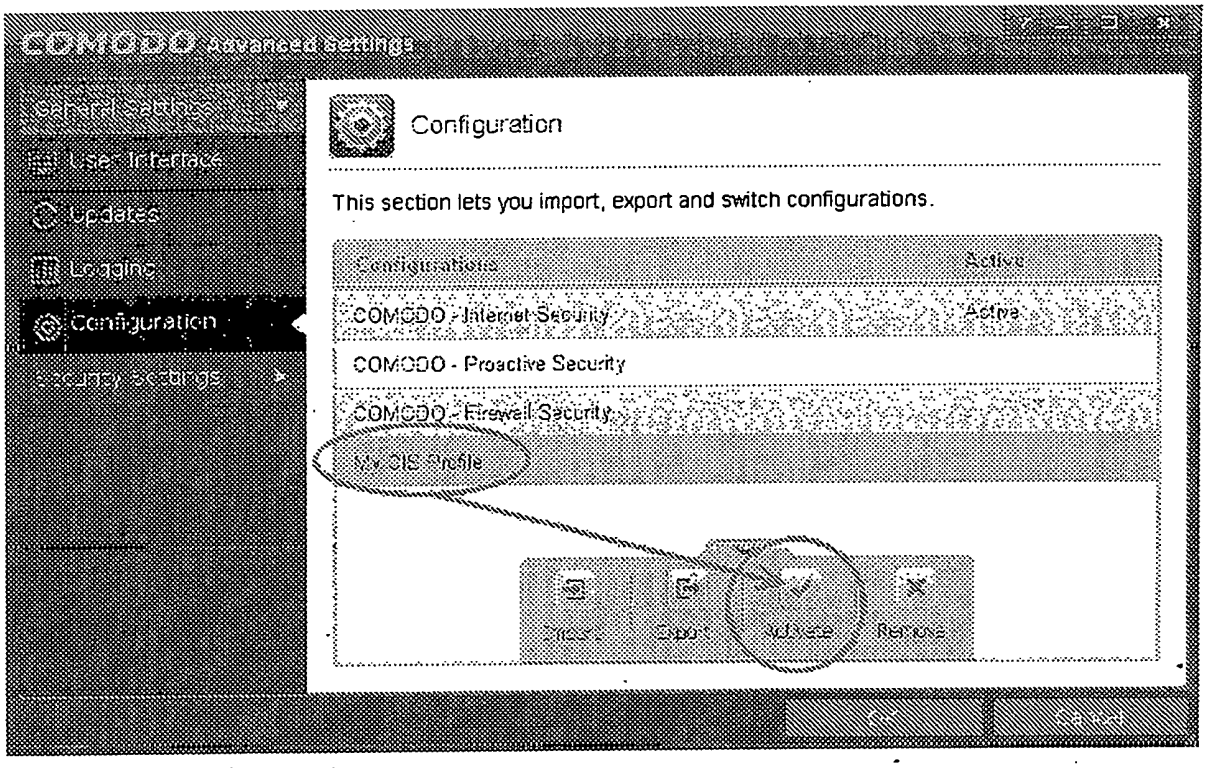


Selecting and implementing a different configuration profile

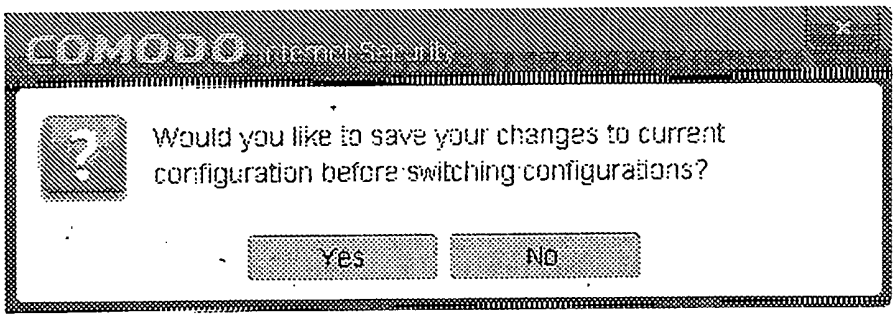
You can change the configuration profile active in CIS at any time from the 'Configurations' panel

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.

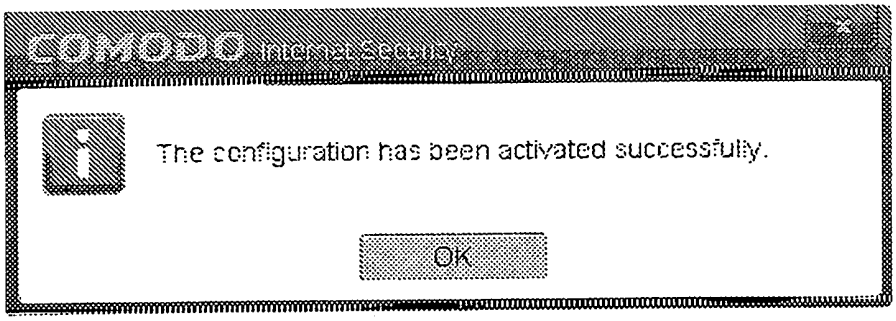


You will be prompted to save the changes to the settings in you current profile before the new profile is deployed.

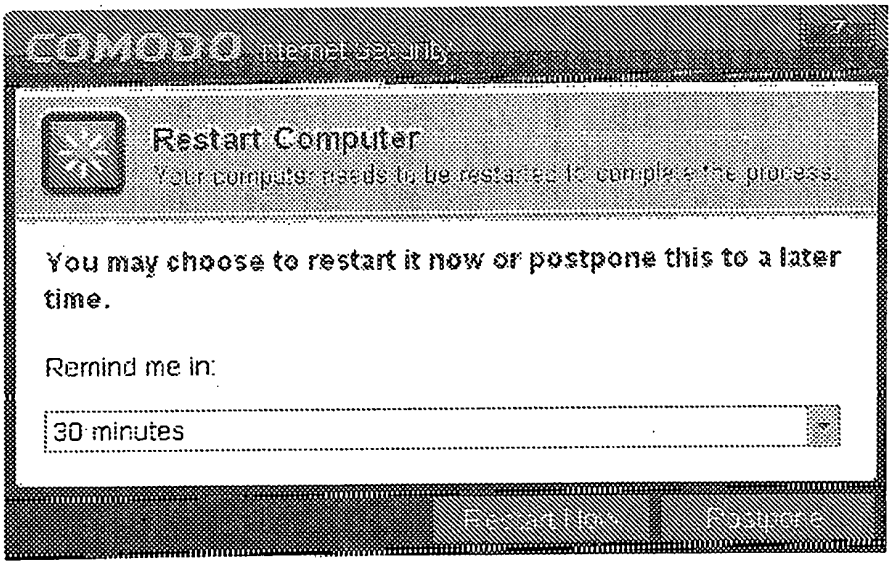


3. Click 'Yes' to save any setting changes in the current configuration, else click 'No'.

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.



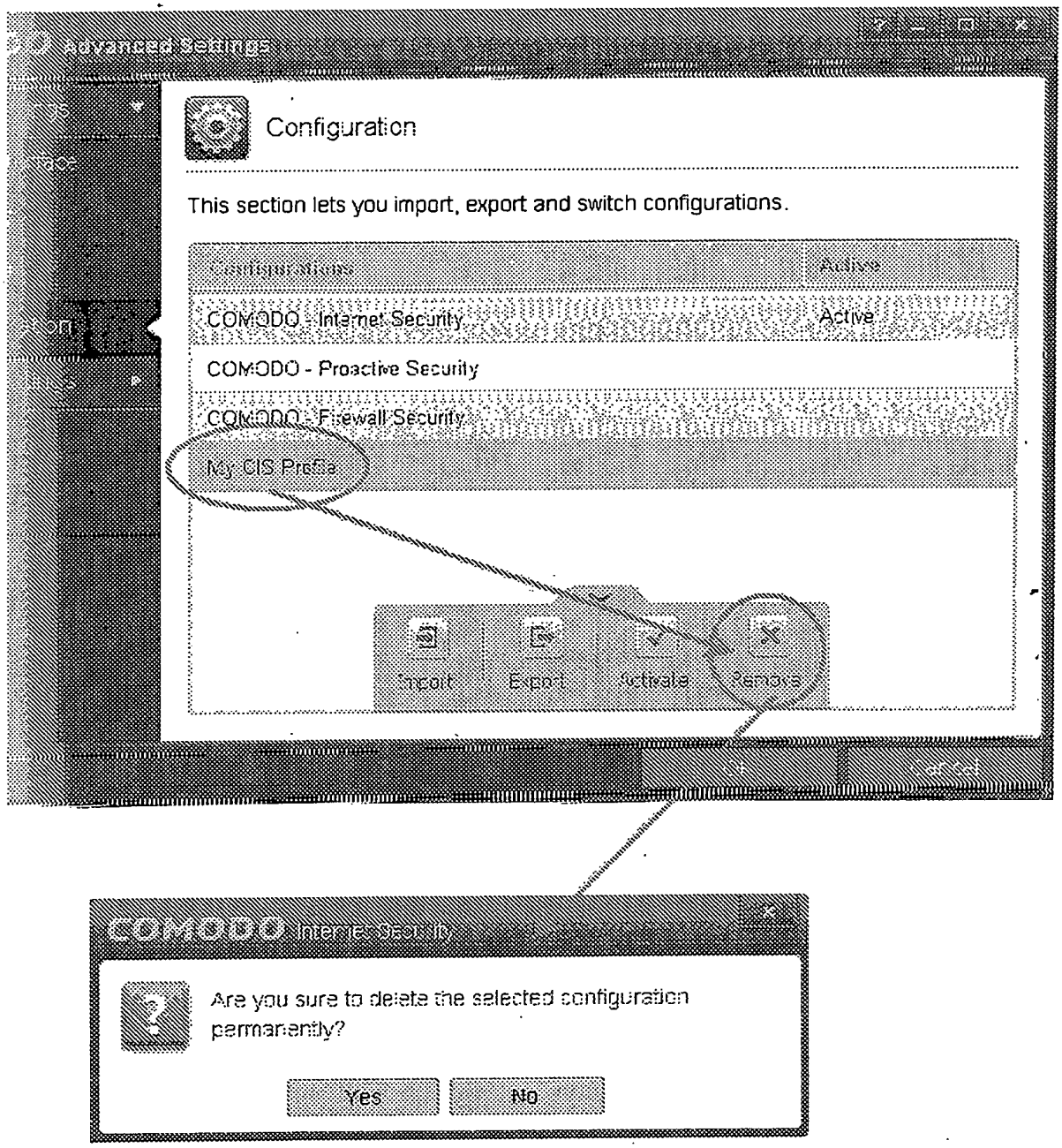
- If your want to restart the computer immediately, save all your work and click 'Restart Now'.
- If you want to restart the computer at a later time, select when you need to be reminded from the drop-down and click 'Postpone'.

Deleting an inactive configuration profile

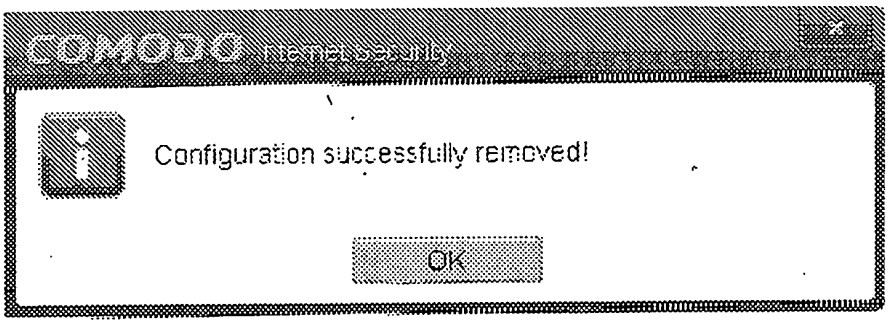
You can remove any unwanted configuration profiles from the list of stored configuration profiles. You cannot delete the profile that Comodo Internet Security is currently using - only the inactive ones. For example if the COMODO - Internet Security is the active profile, you can only delete the inactive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

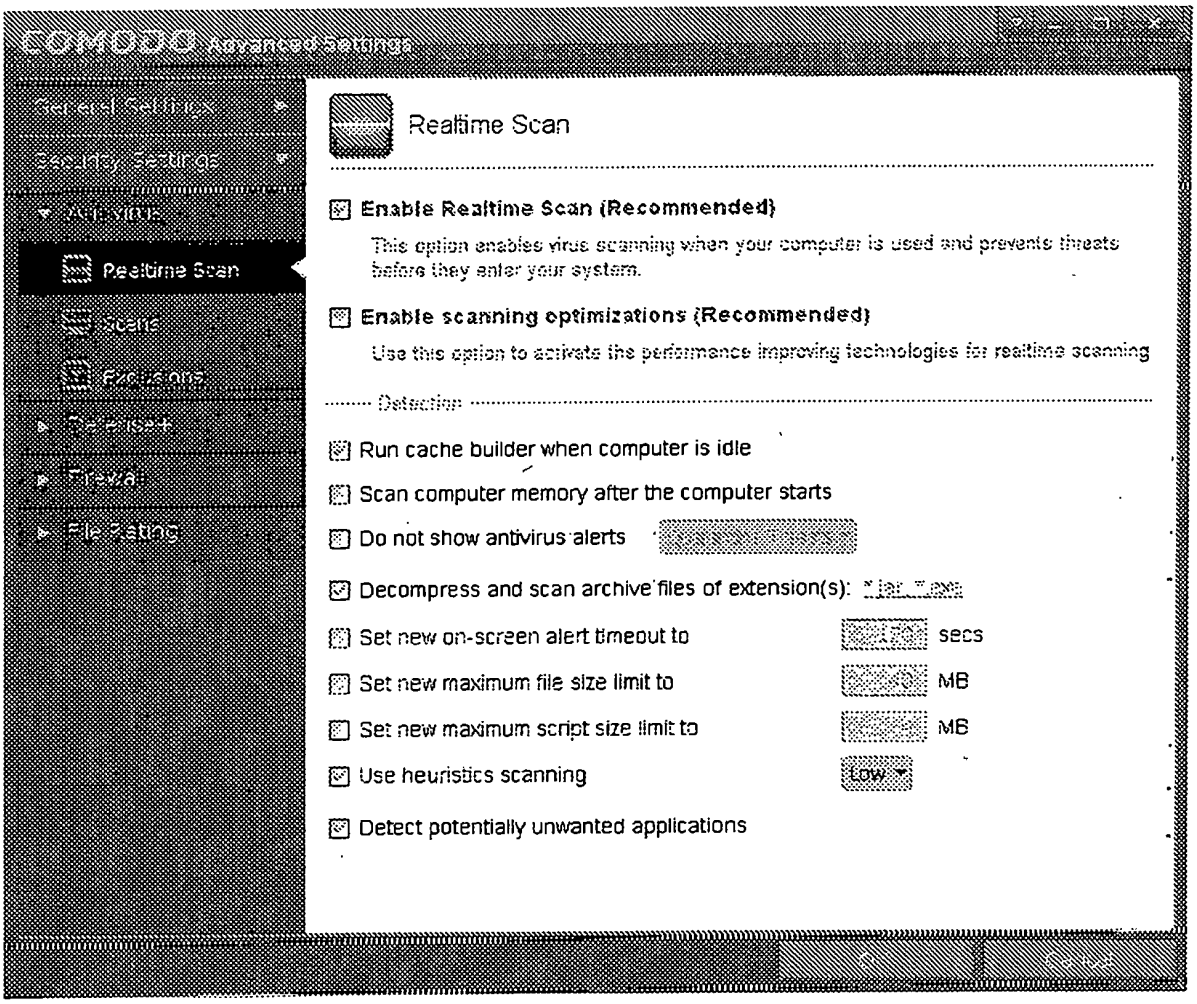


3. Click 'Yes'. The configuration profile will be deleted from your computer.



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.

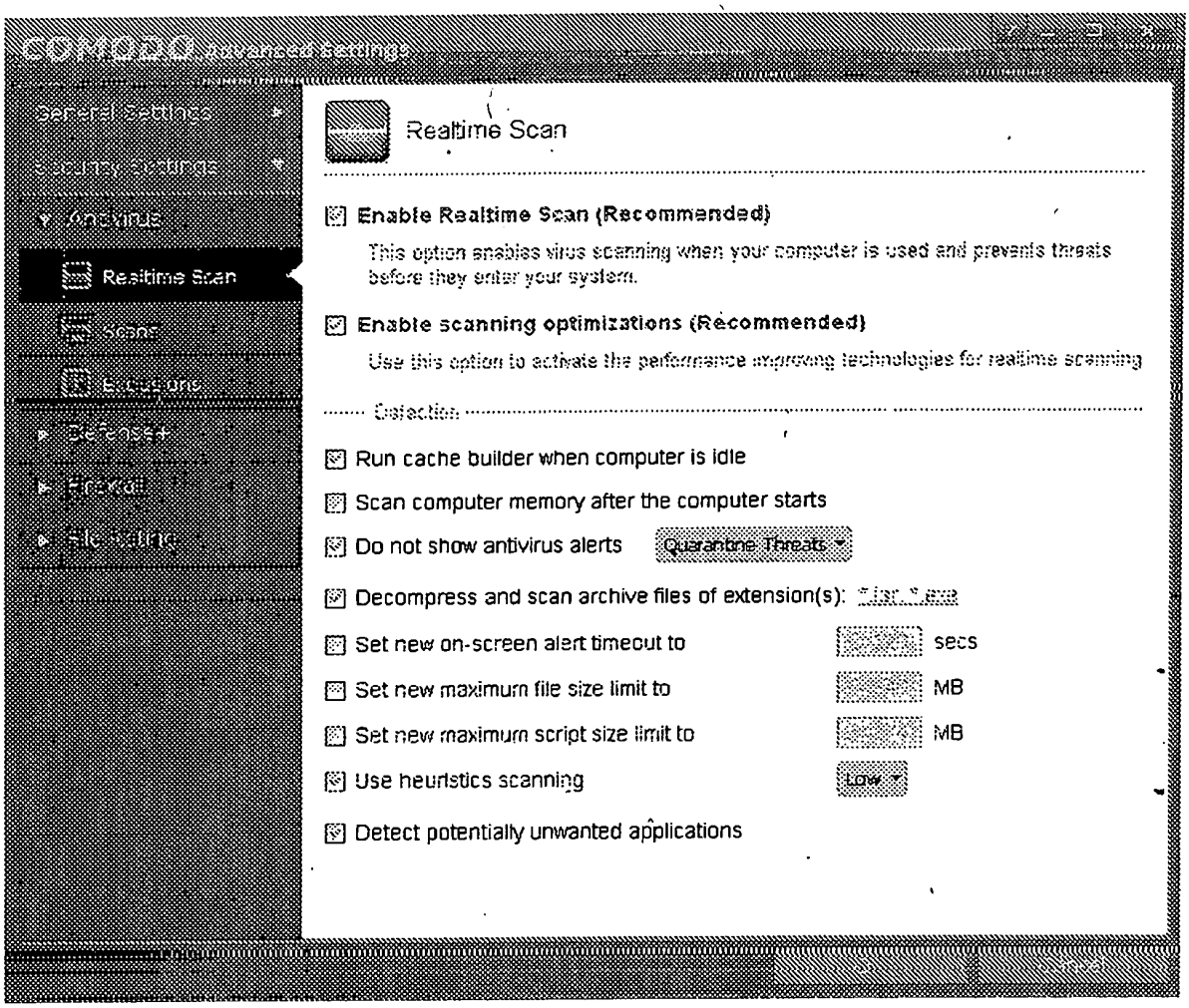
6.2.1.1. Real-time Scanner Settings

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

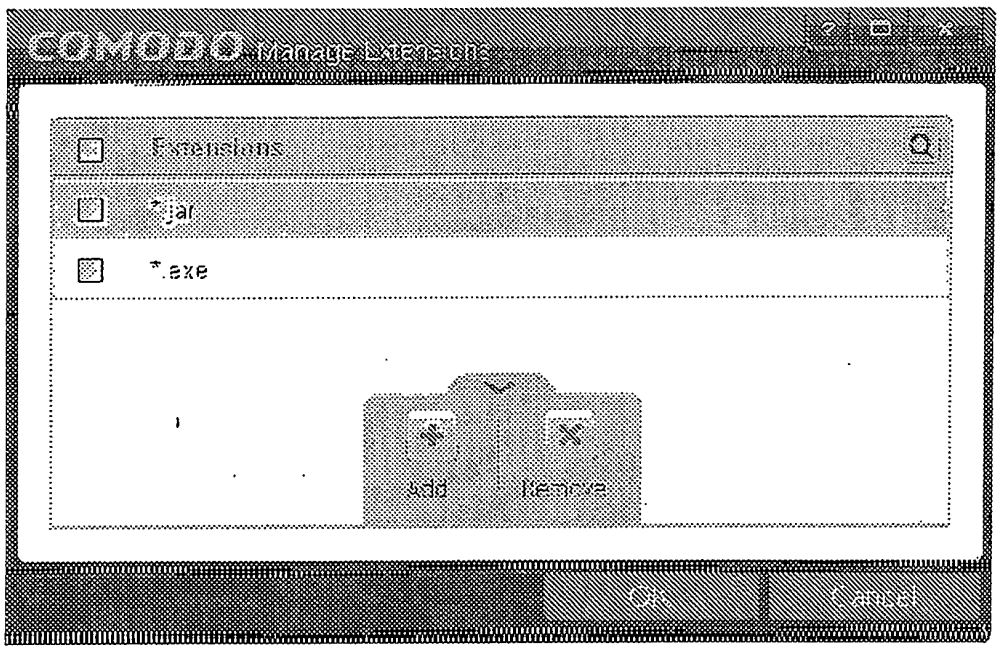
- **Run cache builder when computer is idle** - CIS runs the Antivirus Cache Builder whenever the computer is idle, to boost the real-time scanning. If you do not want the Cache Builder to run, deselect this option (*Default = Enabled*).
- **Scan computer memory after the computer starts** - When this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

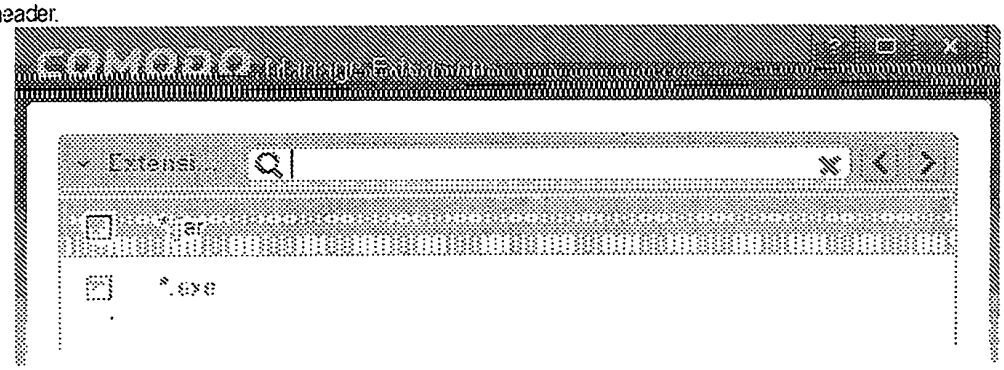
- **Decompress and scan archive files of extension(s)** - Comodo Antivirus can scan all types of archive files such as .jar, RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB if this option is left selected. You will be alerted to the presence of viruses in compressed files before you even open them. ***(Default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



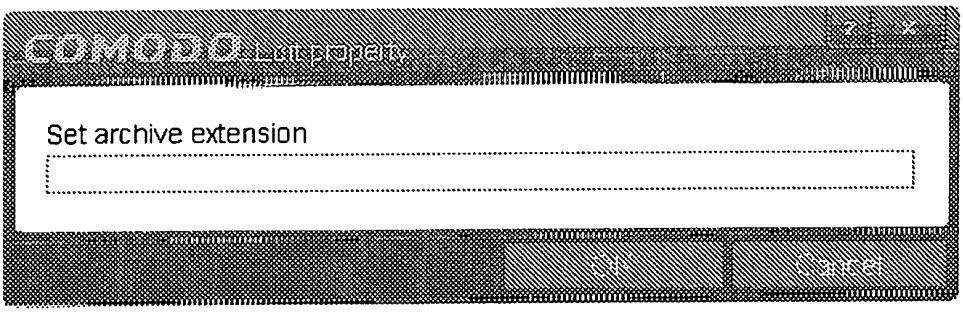
You can use the search option to find a specific file extension in the list by clicking the search icon at the far right in the column header.



- 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

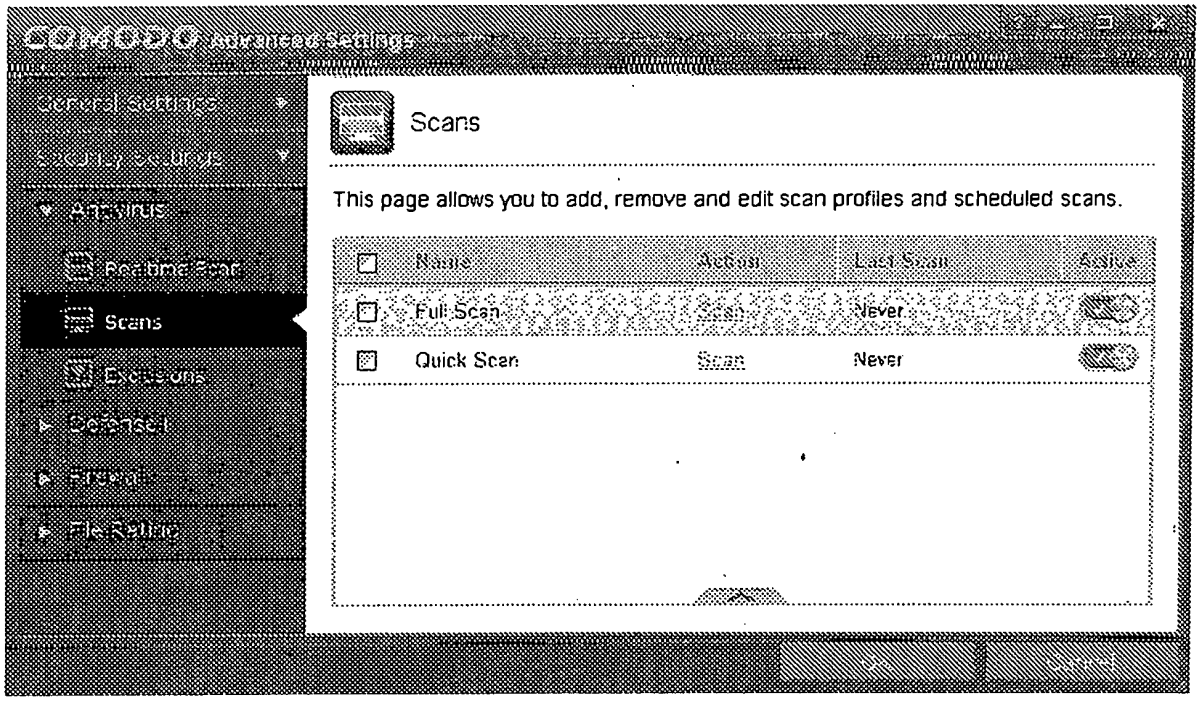
The Scan Profiles area allows you to view, edit, create and run custom virus scans. Each profile is a collection of scanner settings that tell CIS:

- 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.

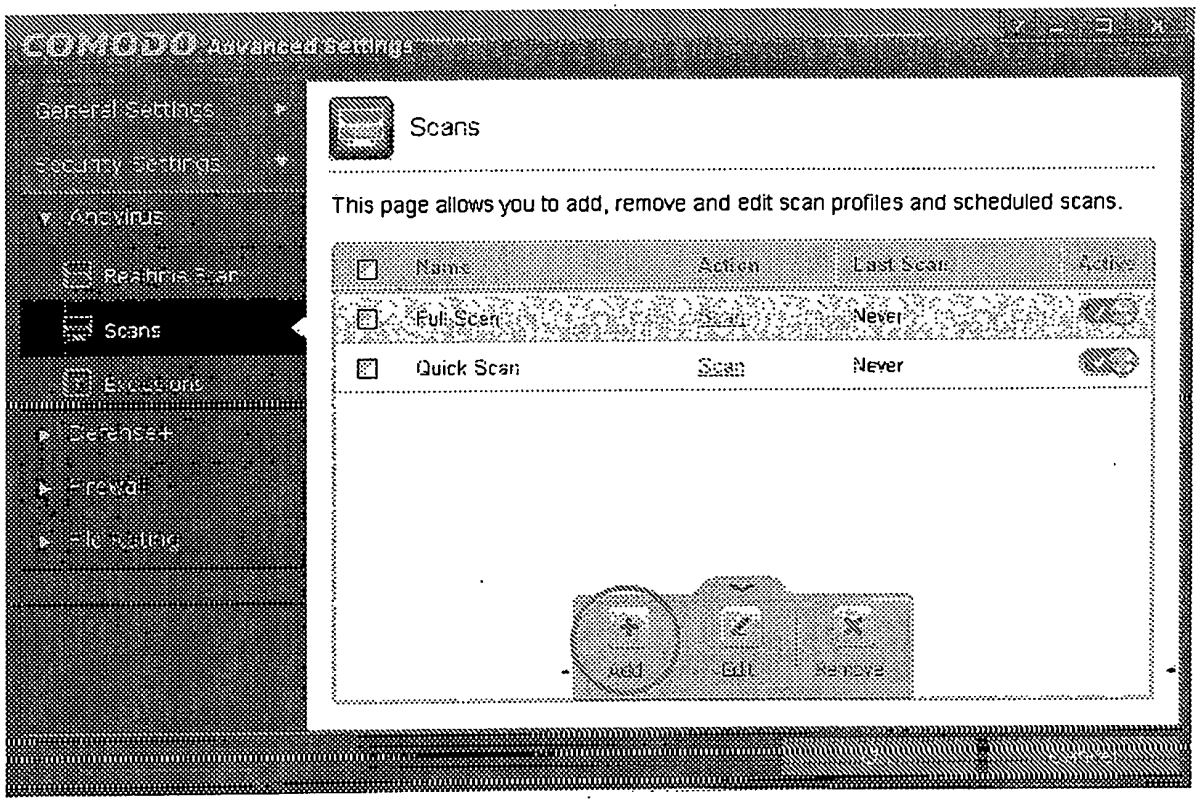
You can run a profile-scan immediately by clicking the 'Scan' link alongside it. Click the handle at the foot of the interface if you wish to edit, remove or add a profile.

Click the following links for more details on:

- Creating a Scan Profile
- Running a custom scan

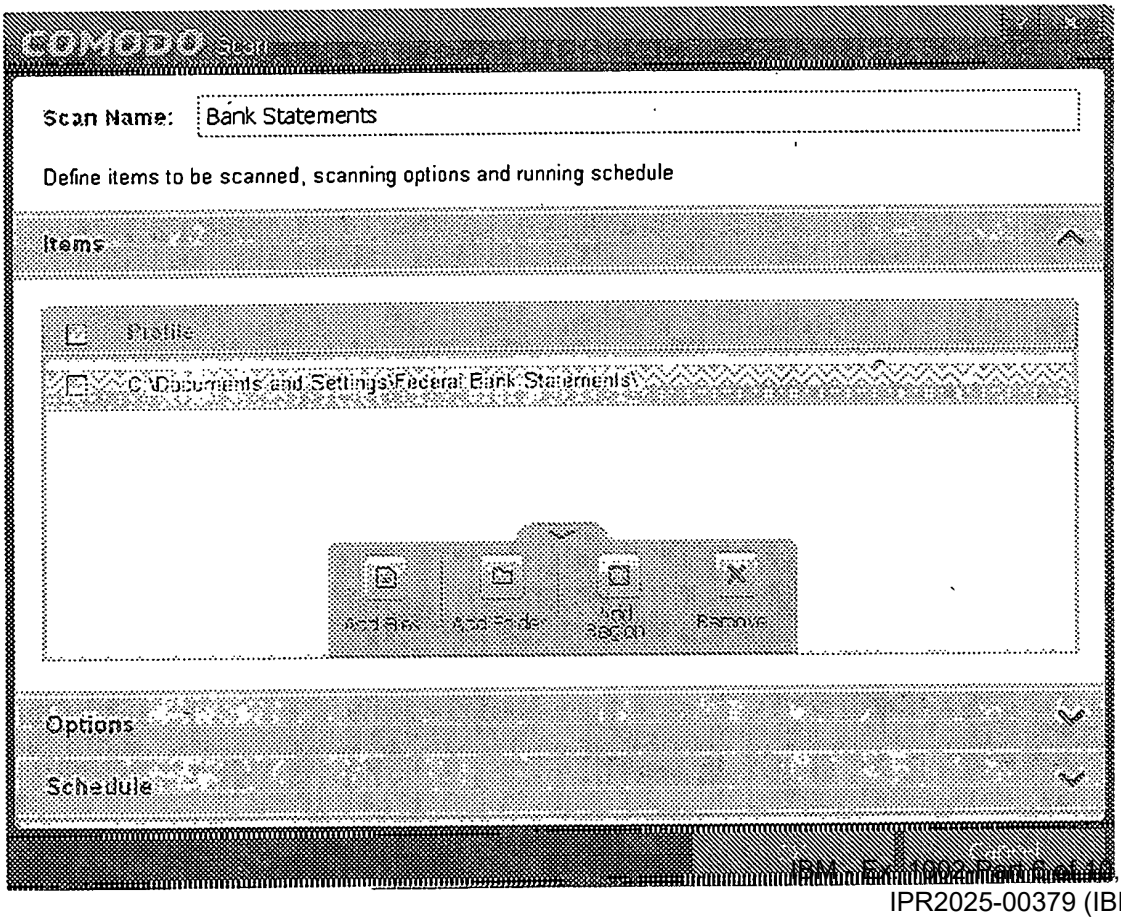
To create a custom profile

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

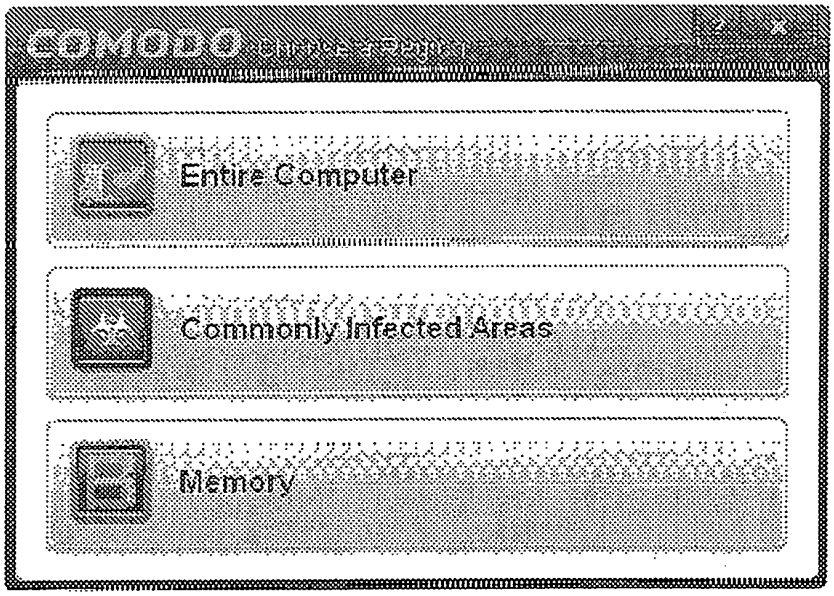


The scan profile interface will be displayed.

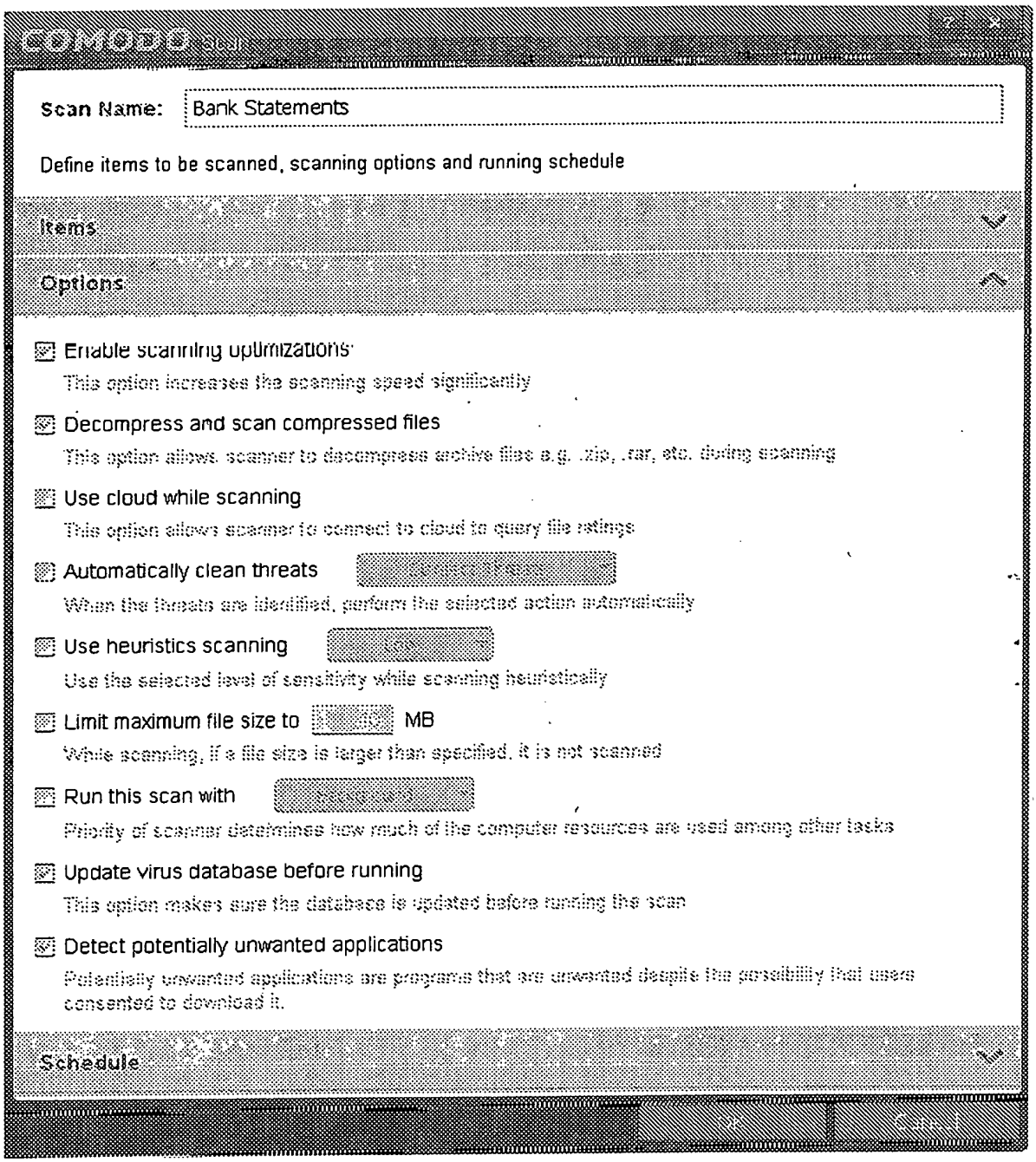
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items that should be included in the profile



- **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



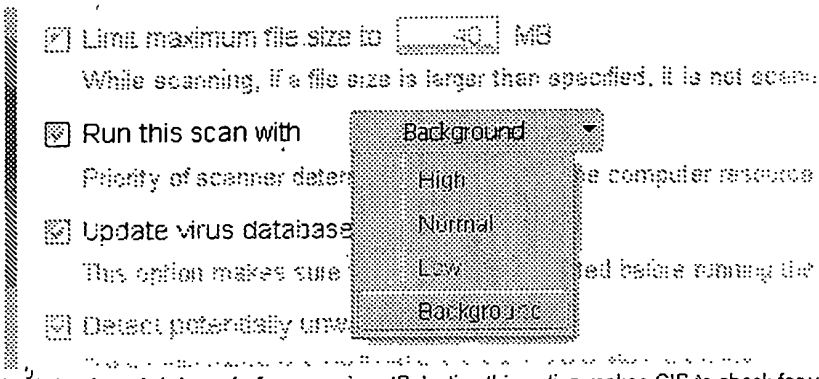
- **Options:**
  - **Enable scanning optimizations** - On selecting this option, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process ***(Default = Enabled)***.
  - **Decompress and scan compressed files** - When this 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.

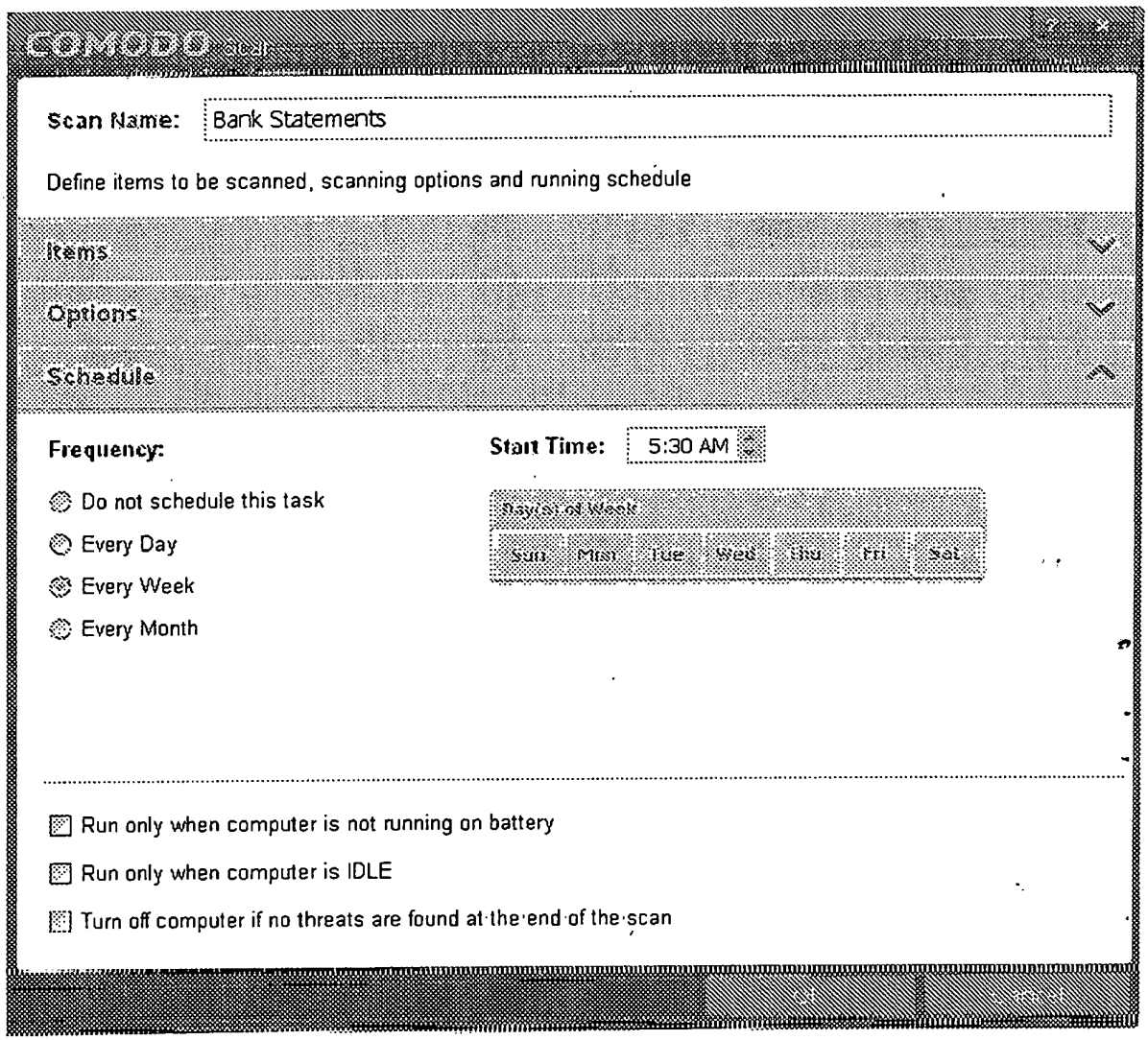
  This allows CIS to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  - **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'

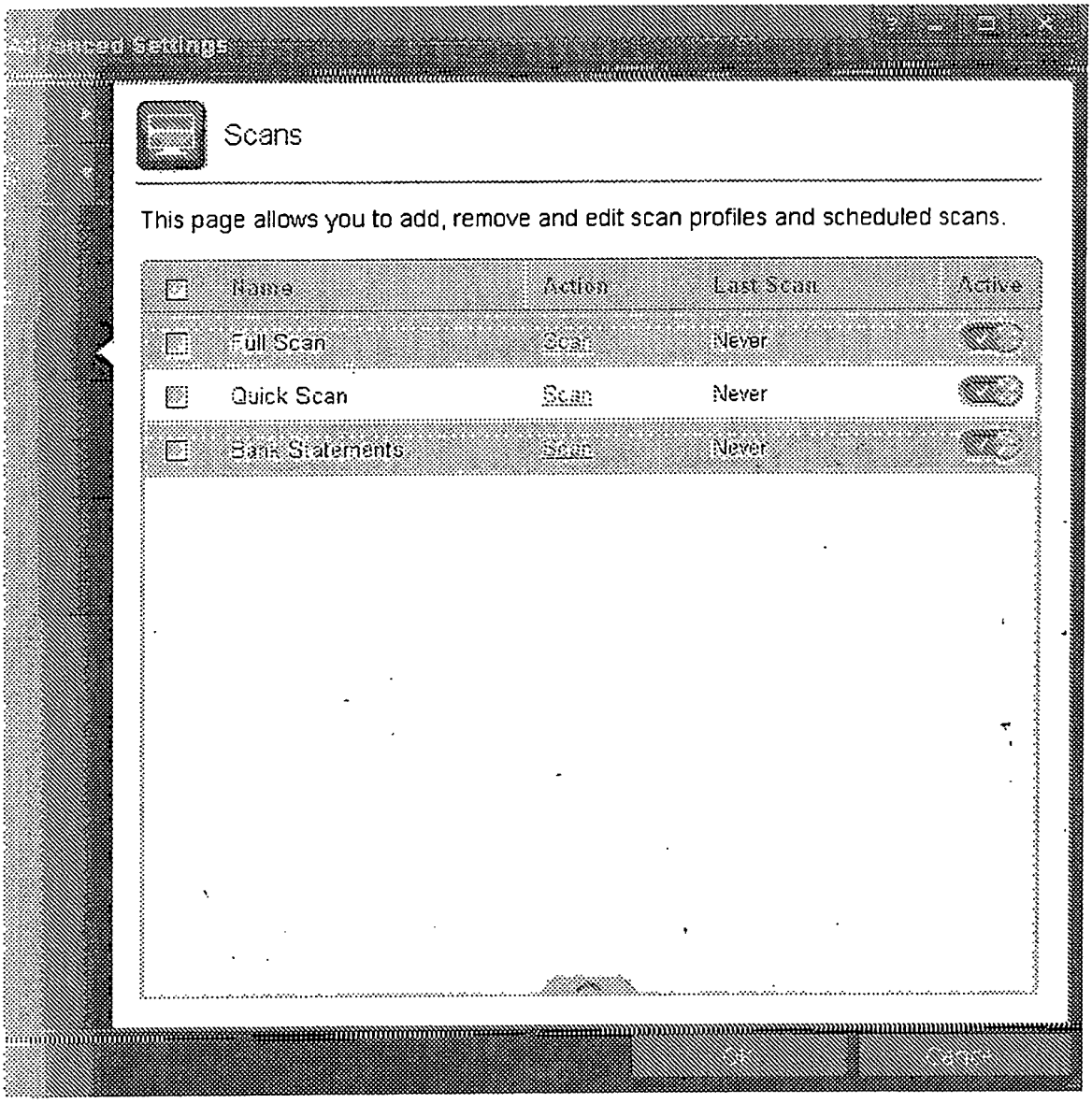


- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - Runs the scan every day at the time specified
- **Every Week** - Scans the areas defined in the scan profile on the day(s) 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 adopter connected to mains supply and not on battery.
- **Run only when computer id IDLE** - Select this option if you do not want to disturbed when involved in computer related activities. The scheduled can will run only if the computer is in idle state
- **Turn off computer if no threats are found at the end of the scan** - Selecting this option turns your computer off, if no threats are found during the scan. This is useful when you are scheduling the scans to run at nights.

- Click OK to save the profile.

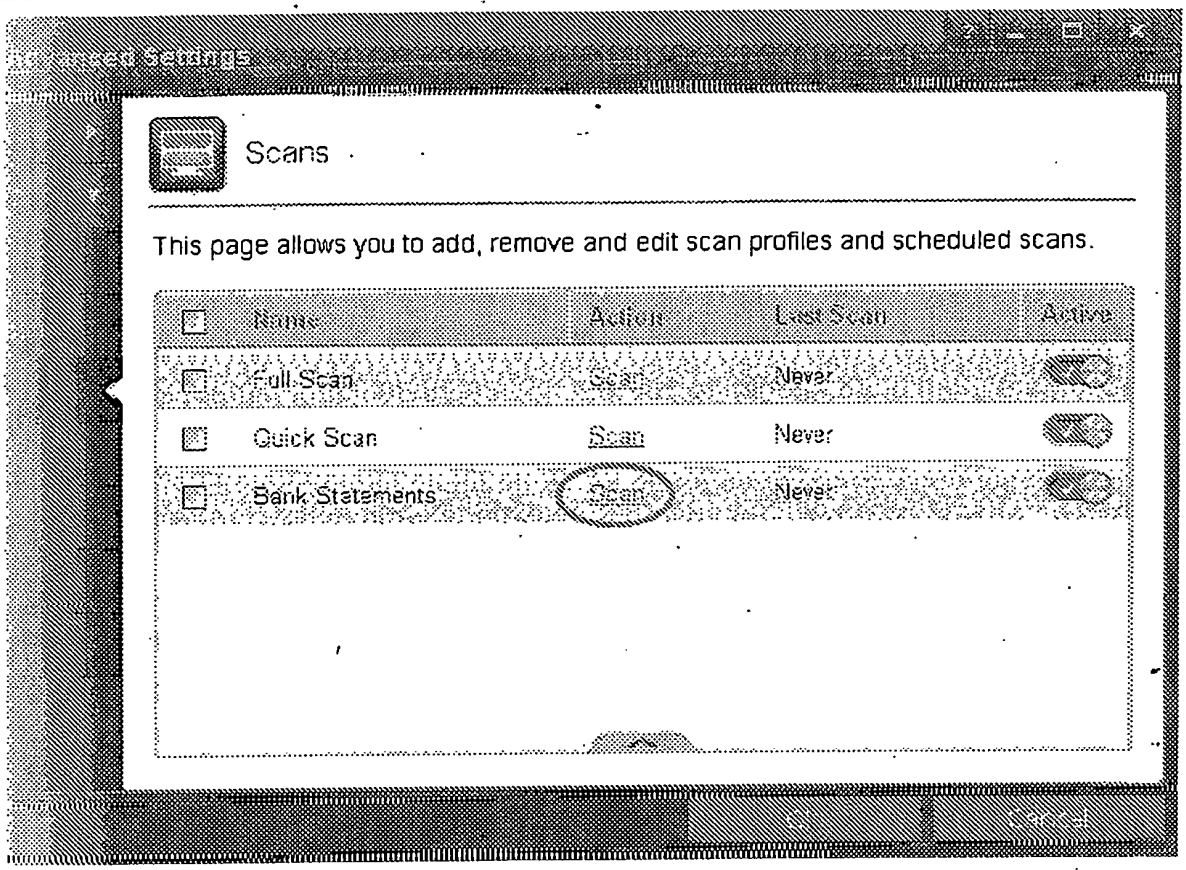
Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row

to toggle between on and off status.

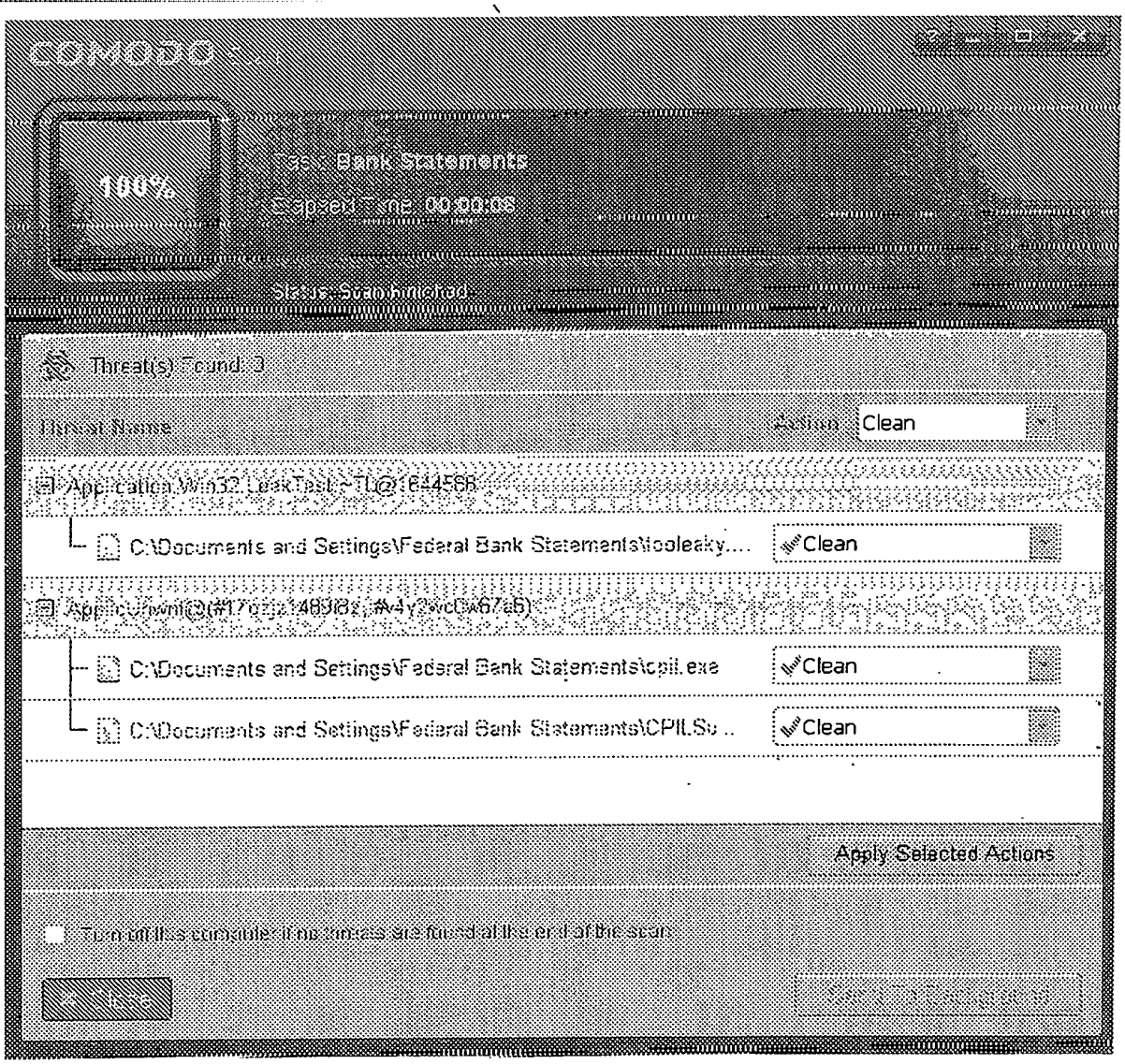


To run a custom scan as per scan profile

- 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.



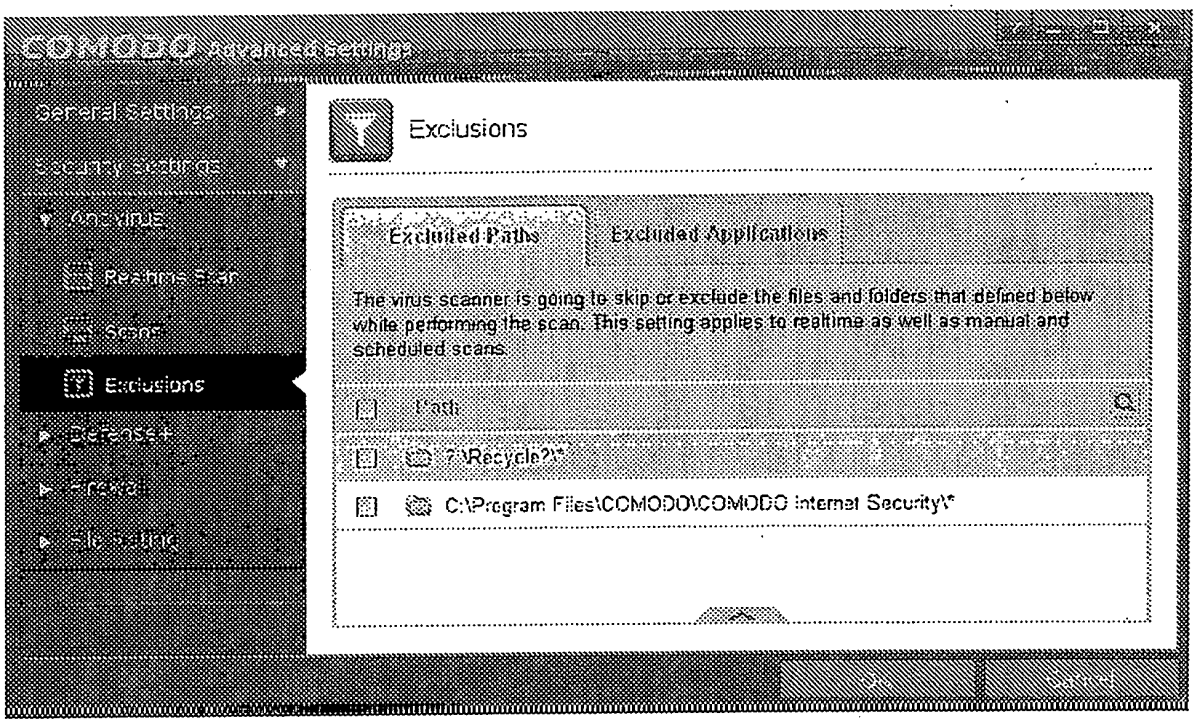
You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

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.

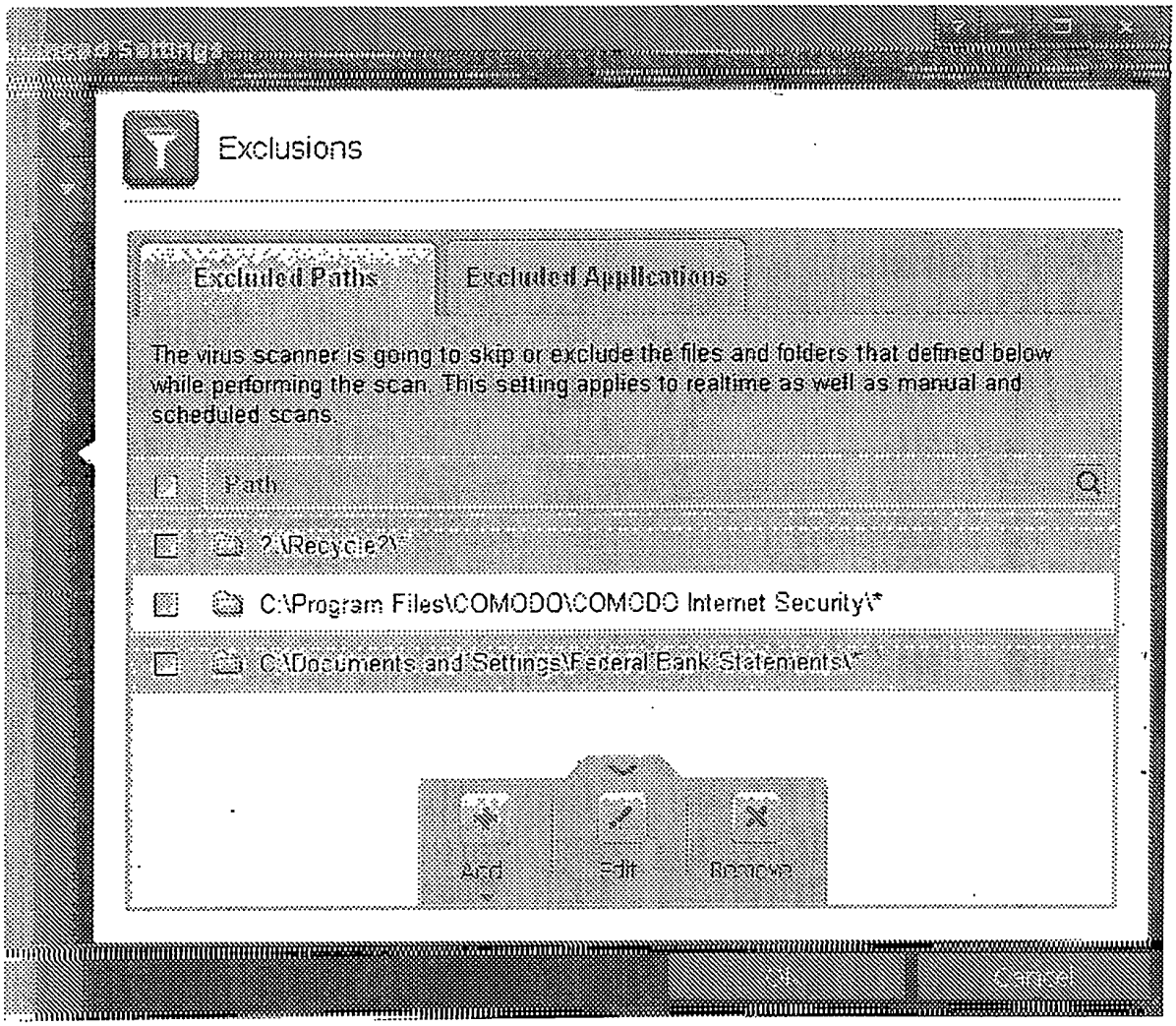


The 'Exclusions' panel has two tabs:

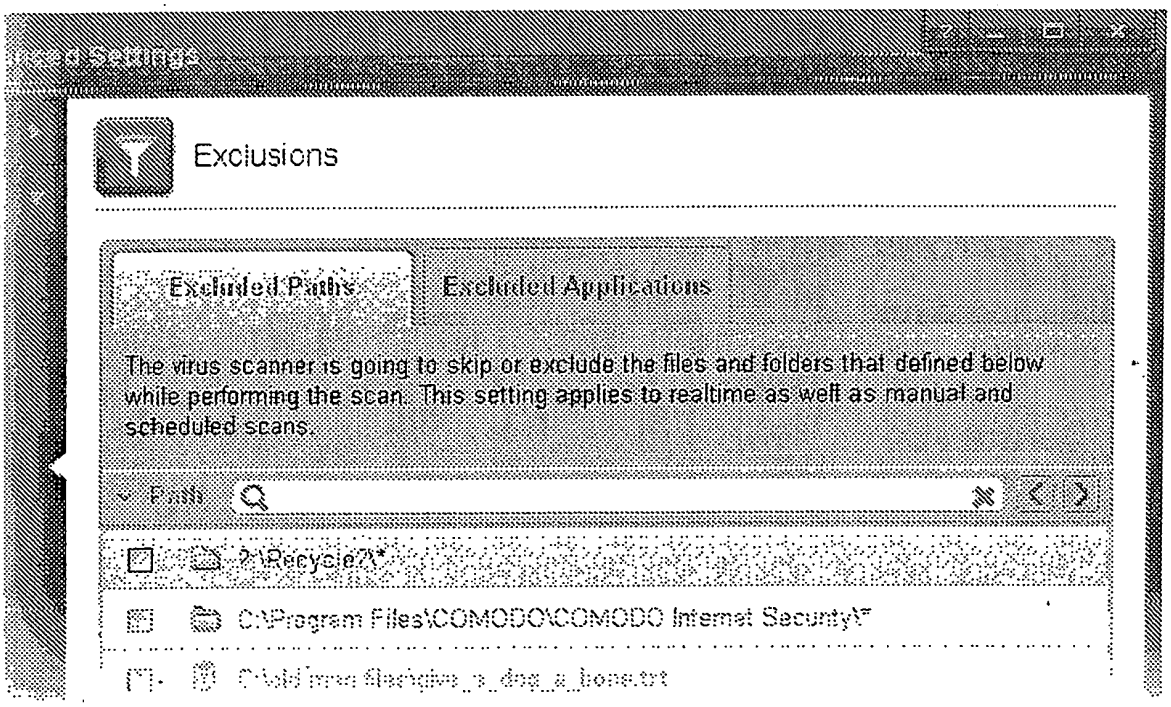
- **Excluded Paths** - Displays a list of paths/folders/files in your computer, which are excluded from both real-time and on-demand antivirus scans. Refer to the section Excluding Drives/Folders/Files from all types of scans for more details on adding and removing exclusion items in this interface.
- **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.



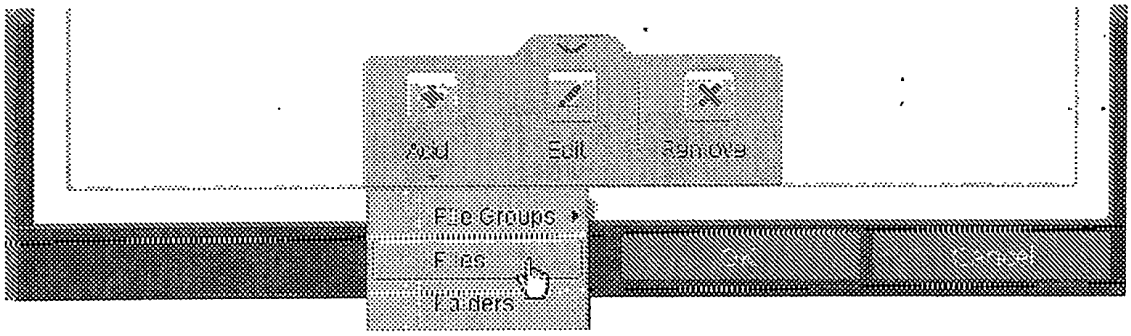
You can use the search option to find a specific excluded path, folder or file from the list by clicking the search icon at the far right in the column header.



- 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



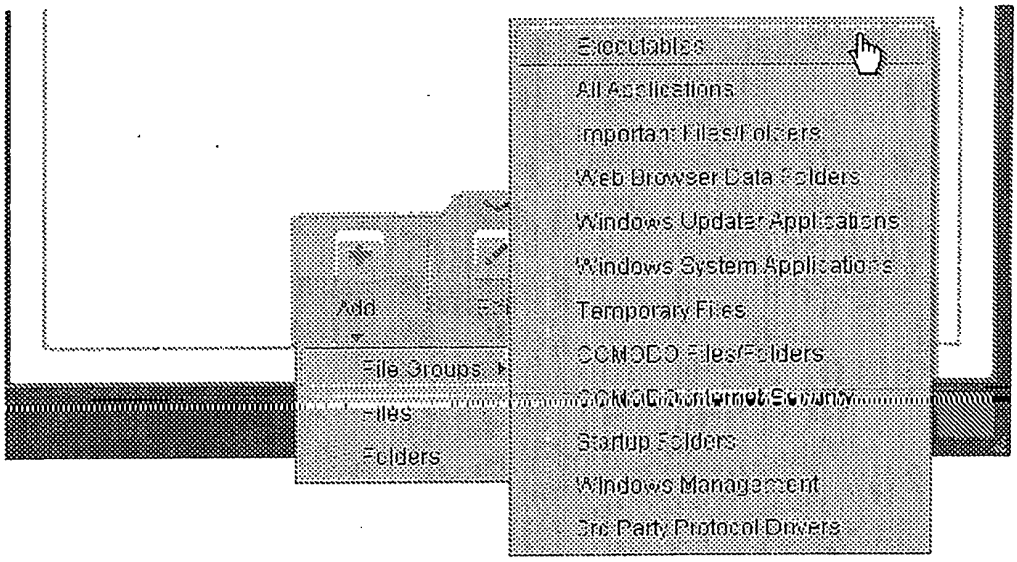
You can choose to add a:

- 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.

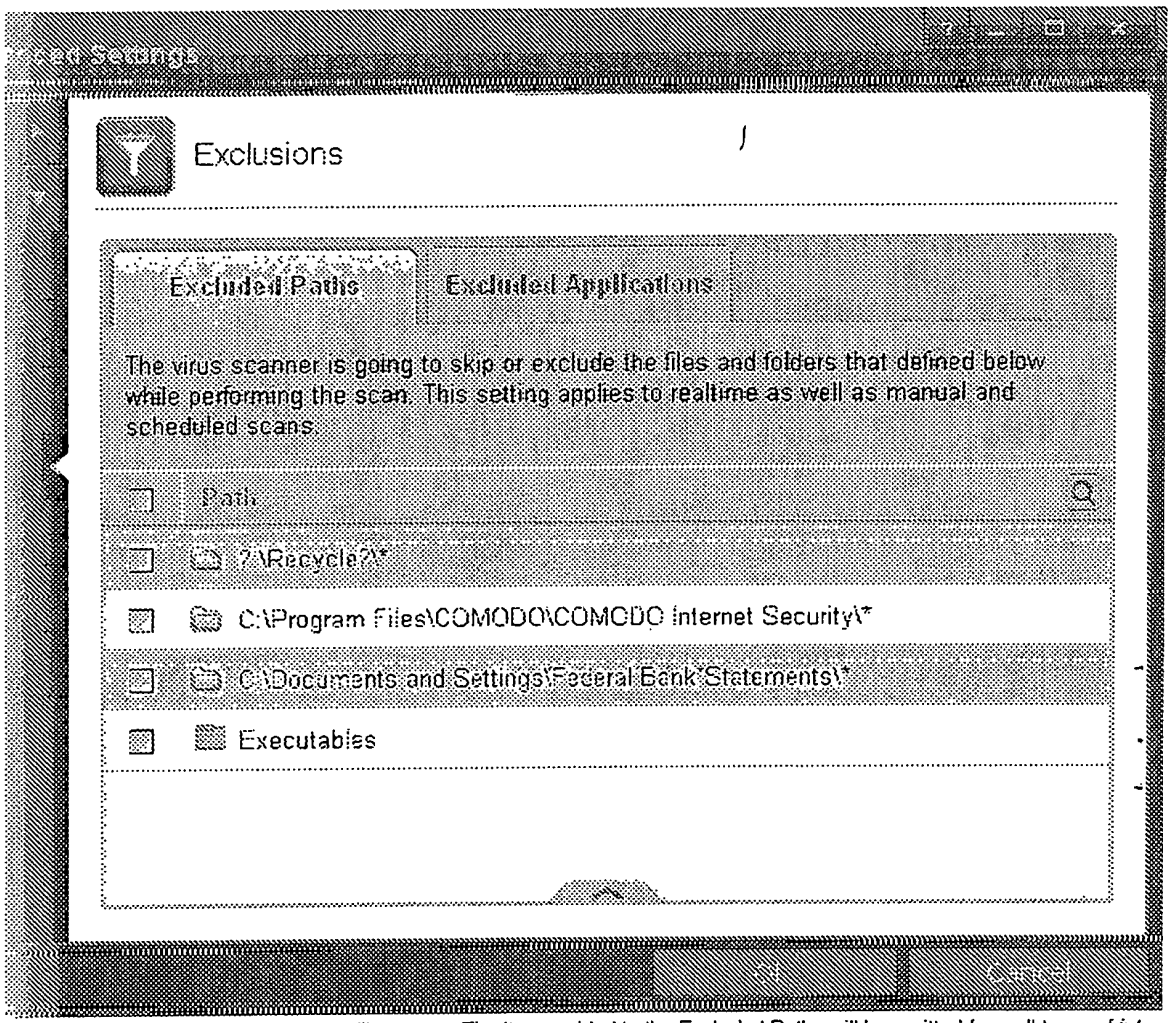


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

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.

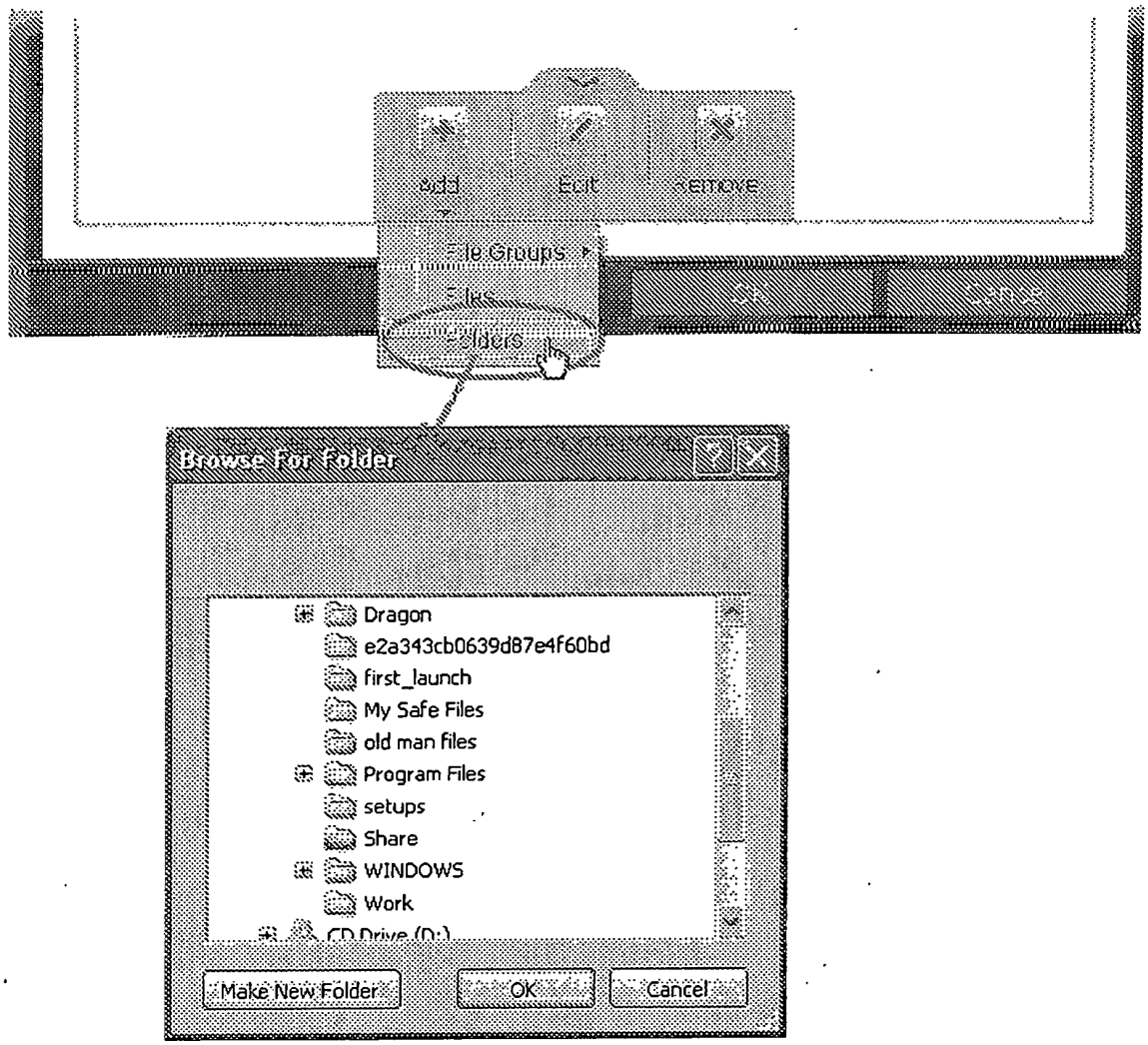
The file groups will be added to Excluded Paths.



- 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

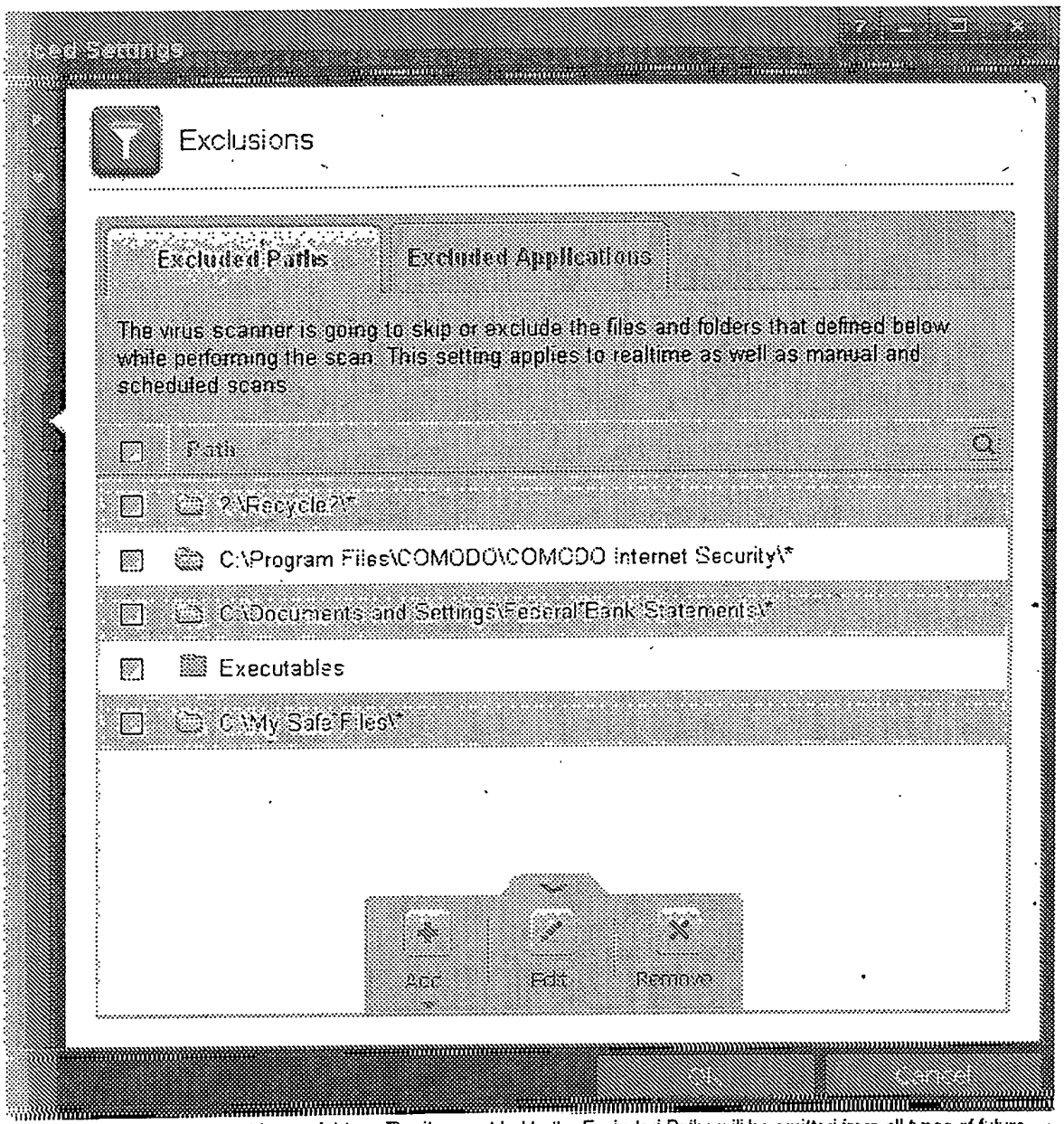
- To add a folder, choose 'Folders' from the 'Add' drop-down.



The 'Browse for Folder' dialog will appear.

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

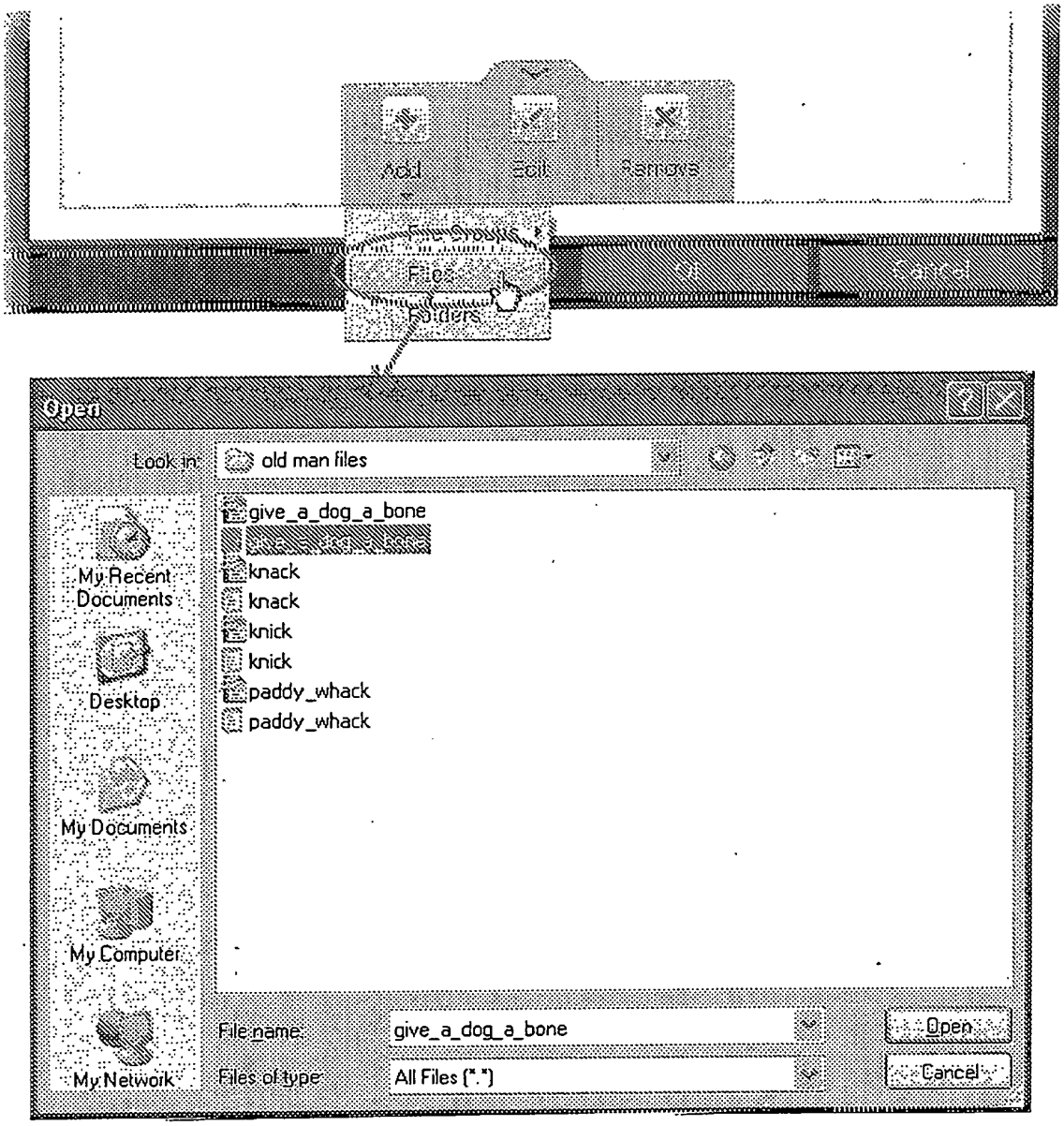
The drive partition/folder will be added to Excluded Paths.



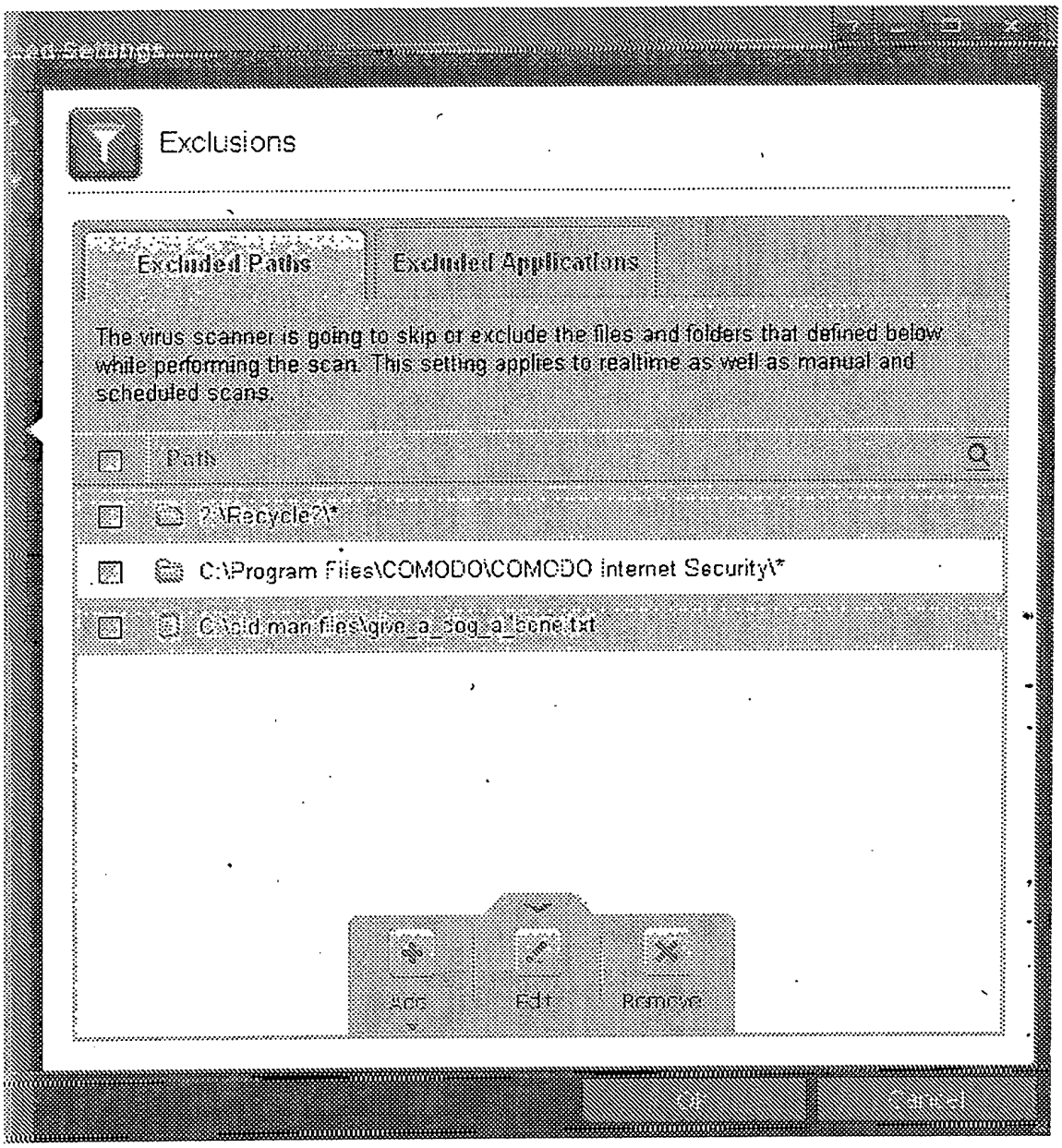
- Repeat process to add more folders. The items added to the Excluded Paths will be omitted from all types of future Antivirus scans.

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'

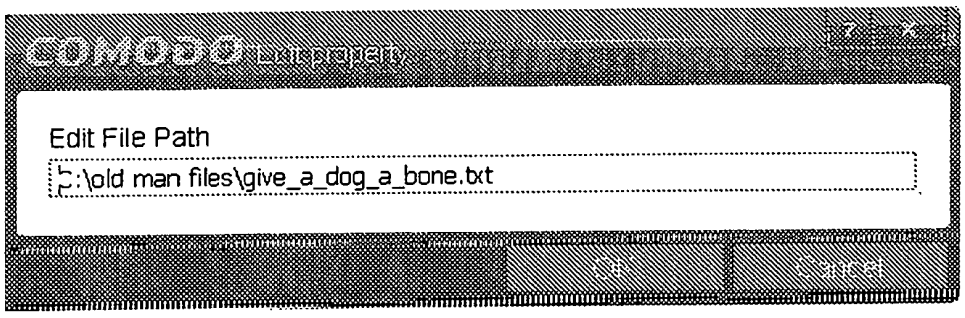


The file will be added to Excluded Paths.

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

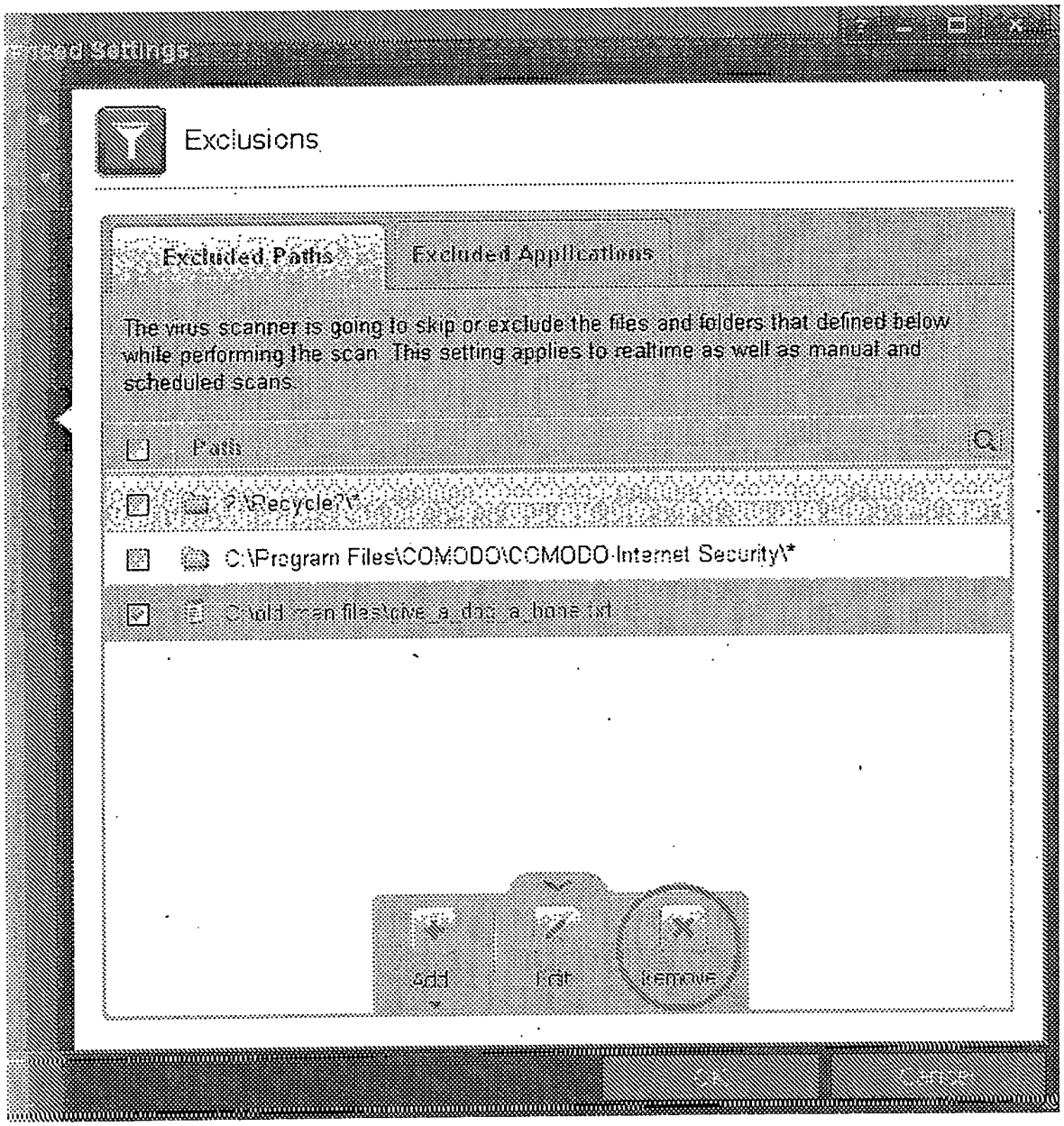
To edit the path of an added item

- 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.



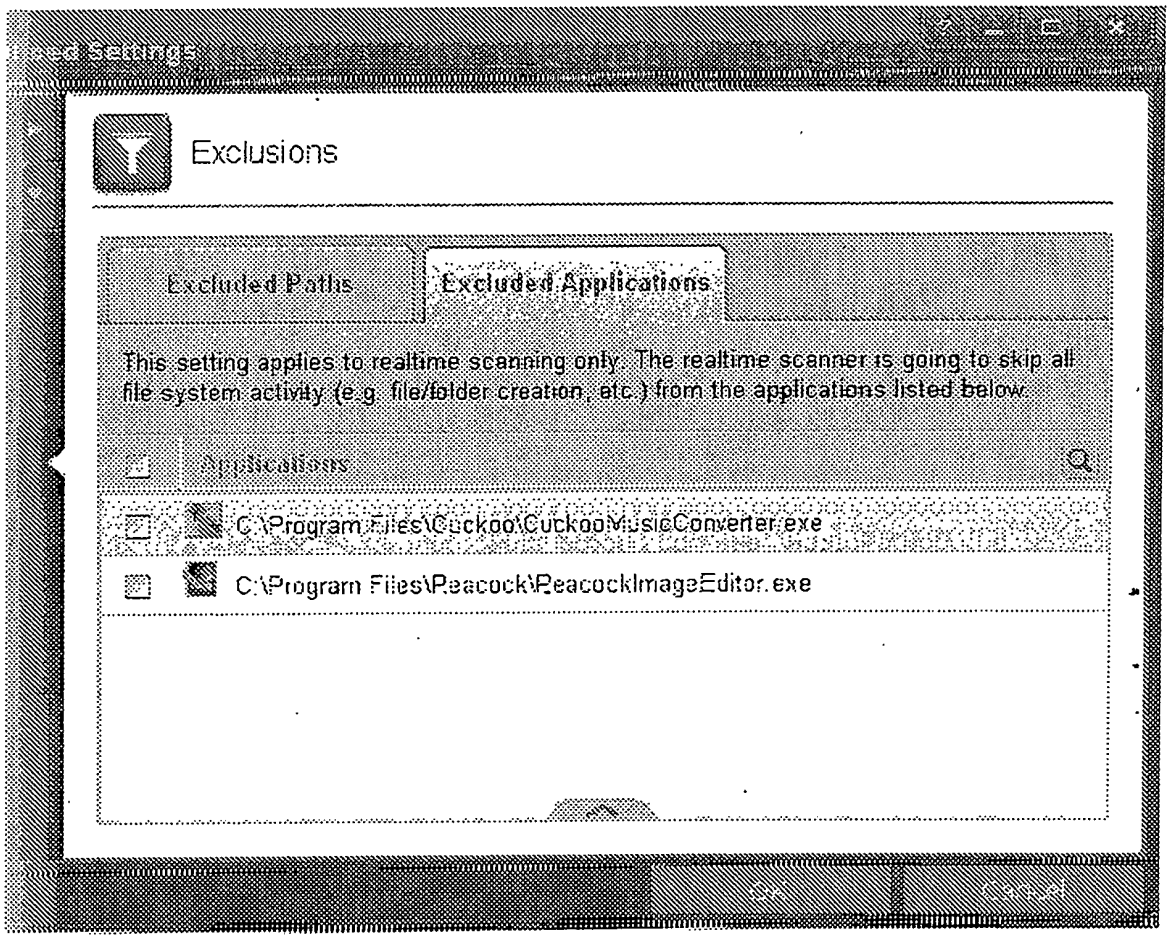
To remove an item from the Excluded Paths

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

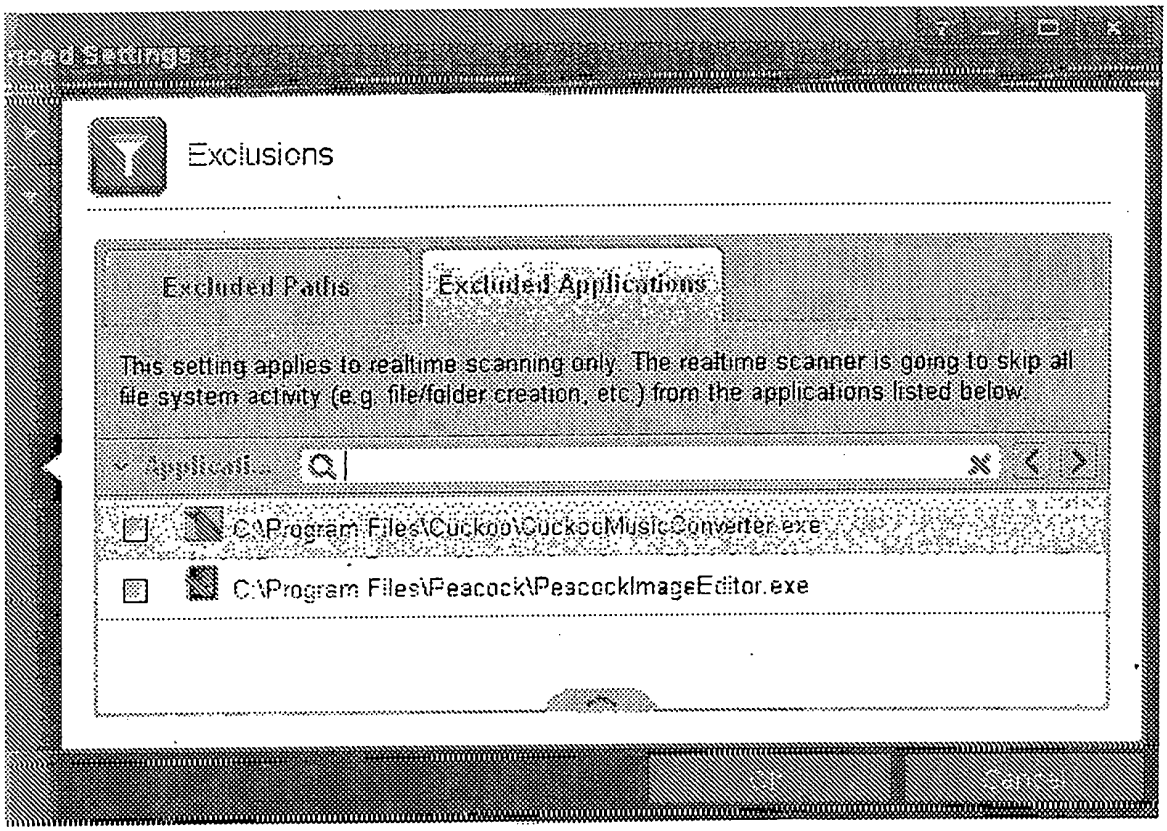


- Click 'OK' in the 'Advanced Settings' dialog for your settings to take effect.

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.



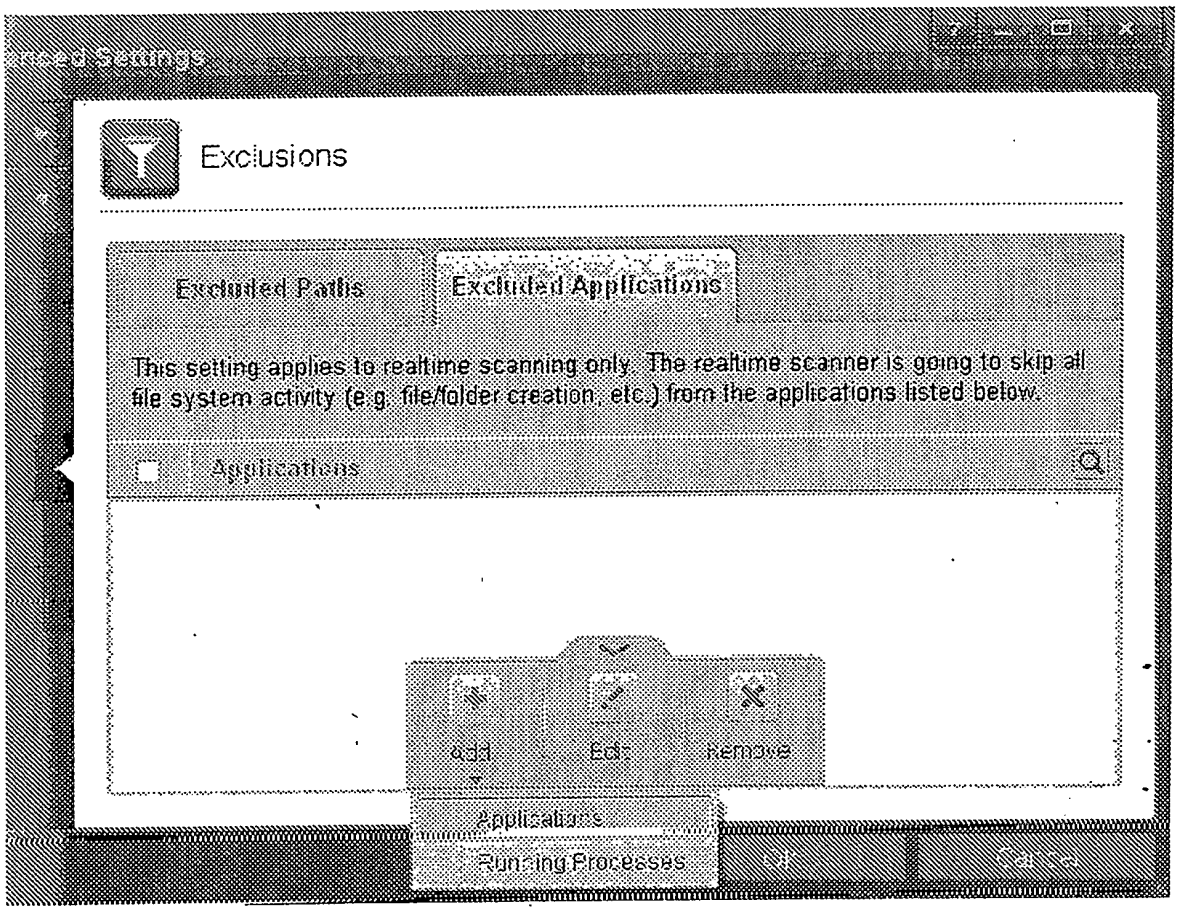
You can use the search option to find a specific excluded application from the list by clicking the search icon at the far right in the column header.



- 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

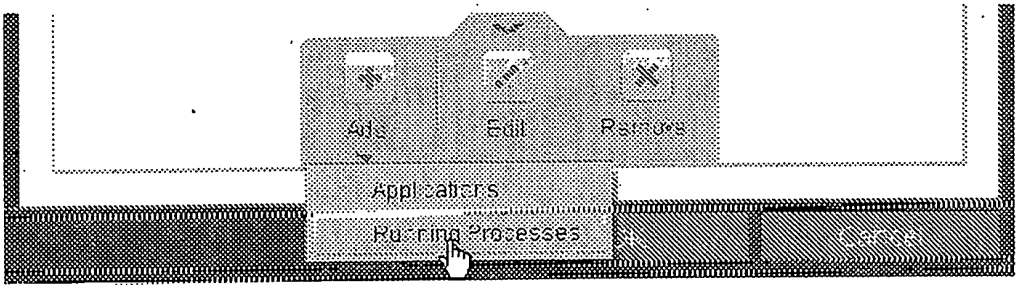


You can choose to add an application by:

- 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.

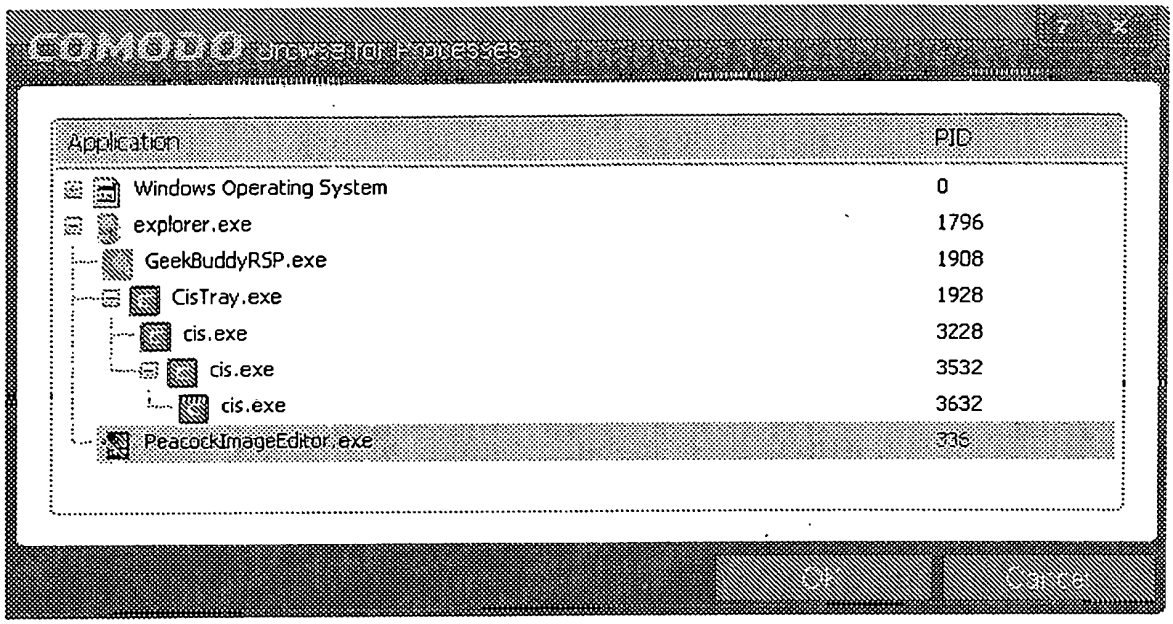
Adding an application from a running processes

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

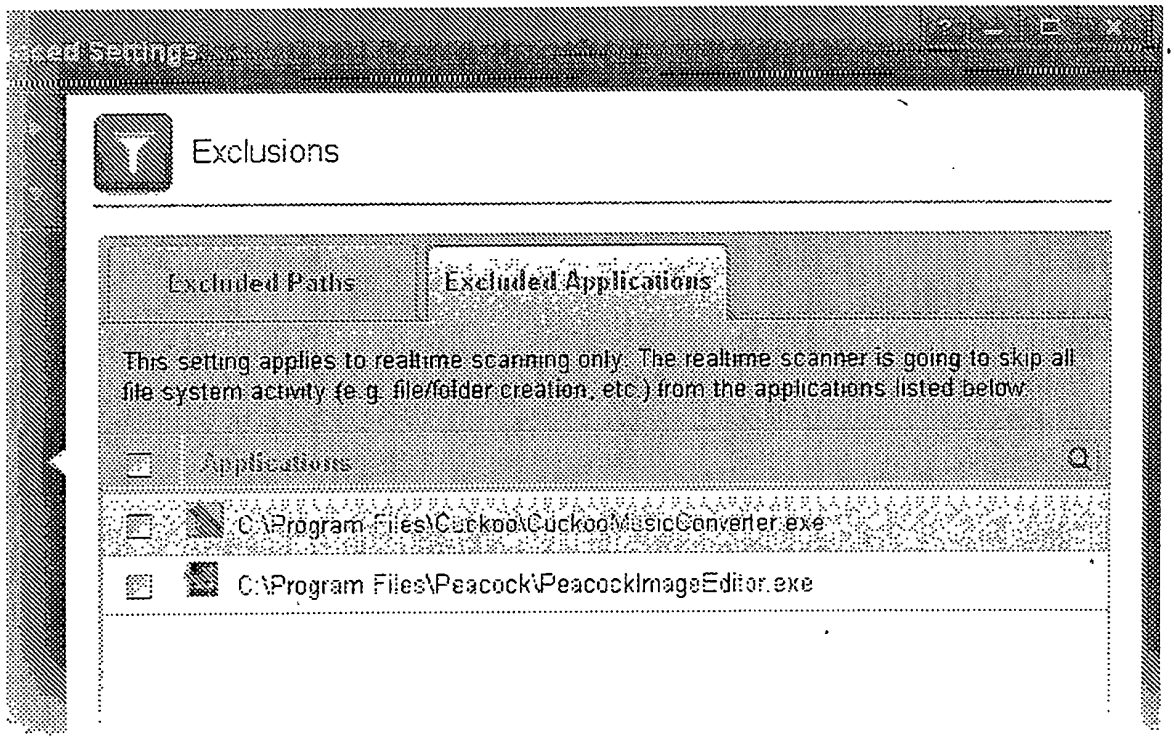


A list of currently running processes in your computer will be displayed

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

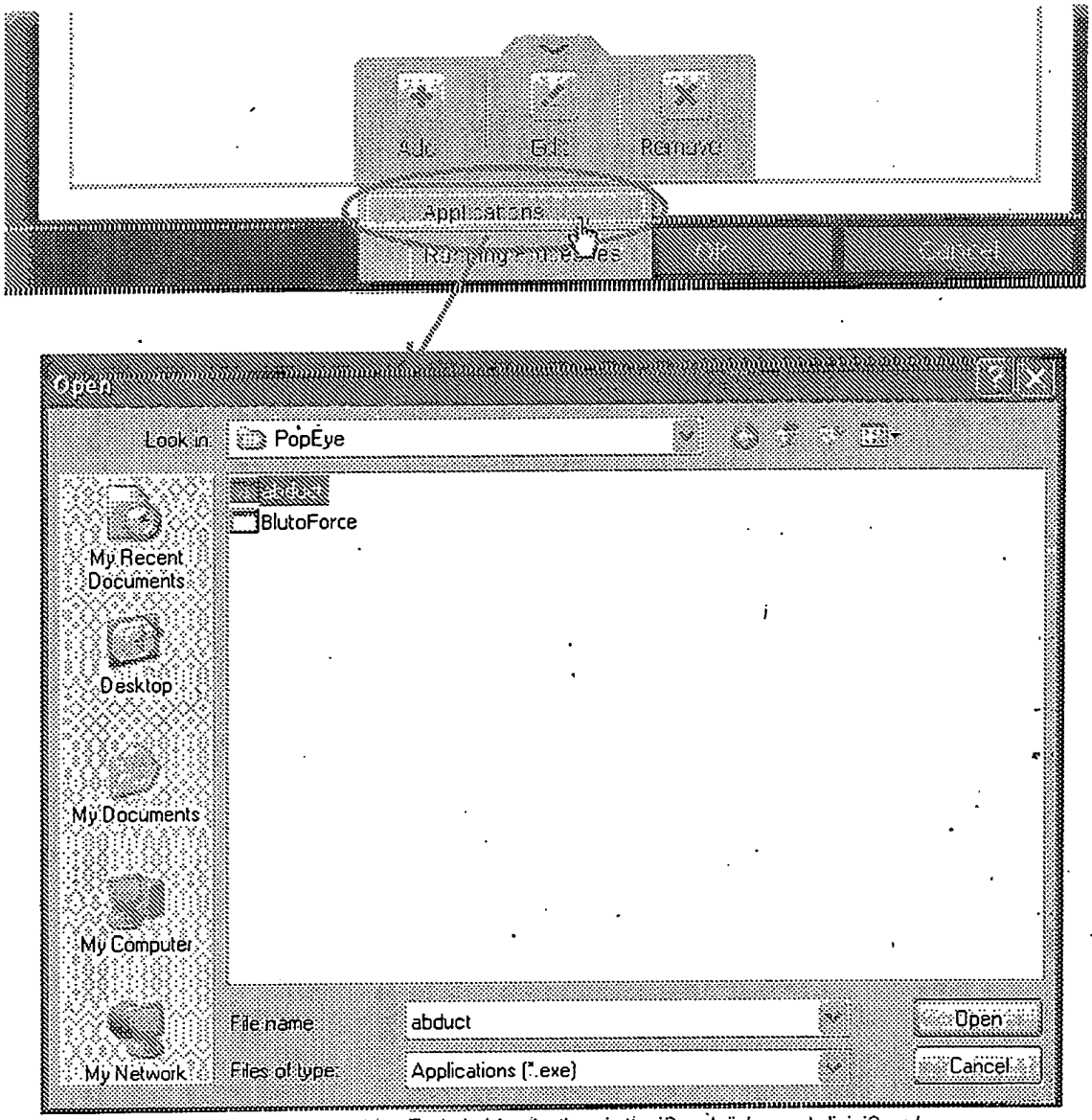


The application will be added to Excluded Applications.



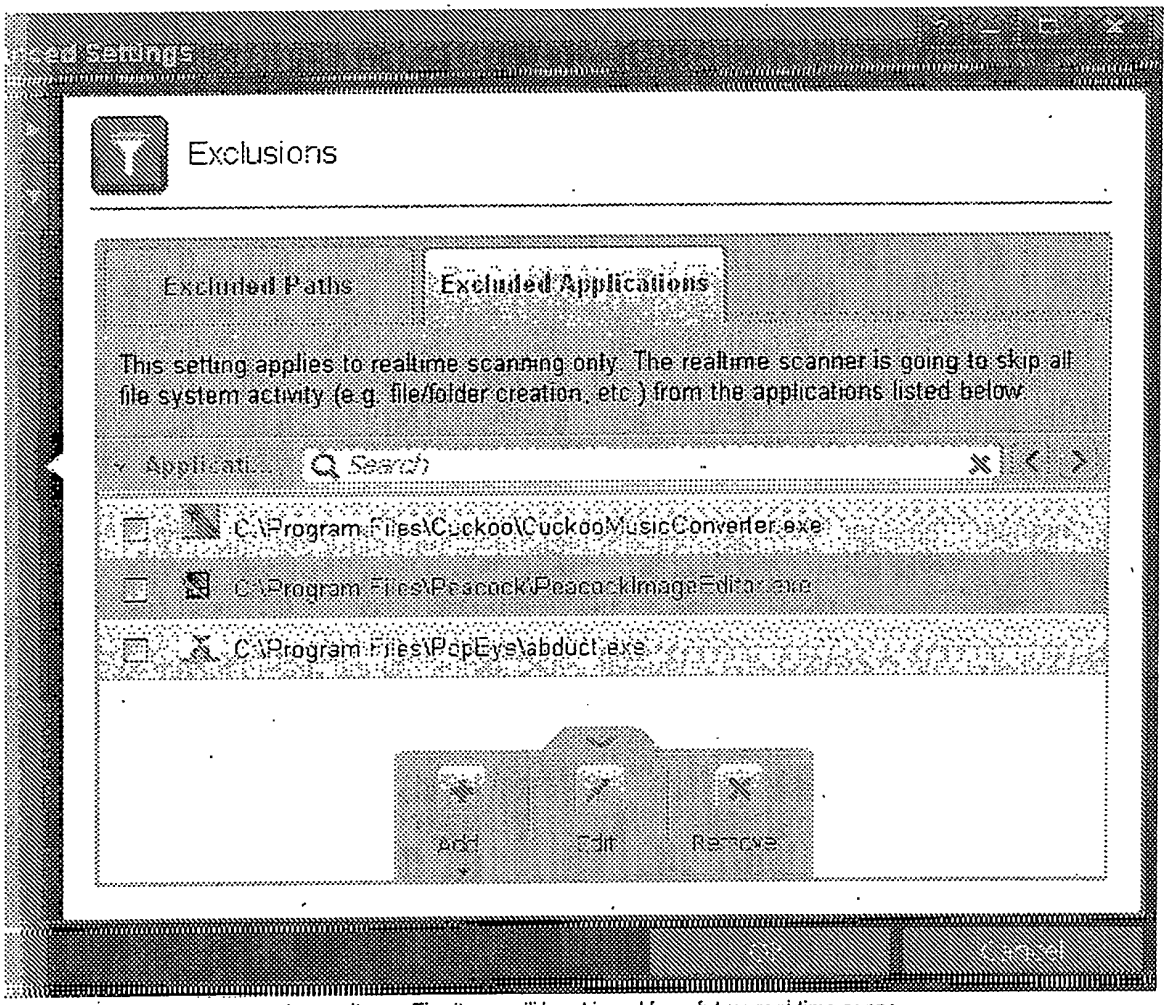
Browsing to the Application

- 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'.

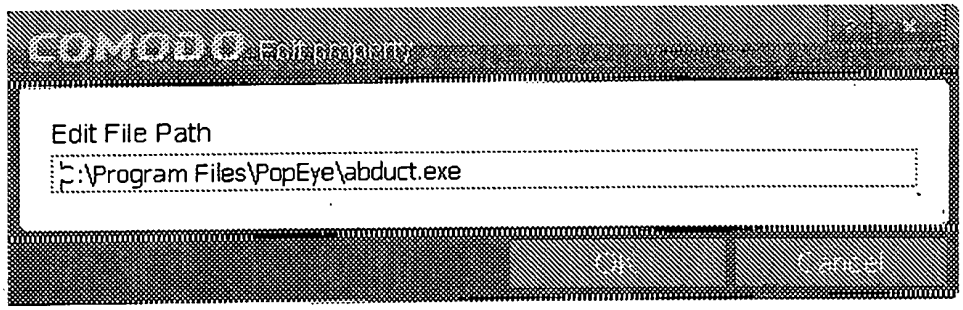
The file will be added to 'Excluded Applications'.



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

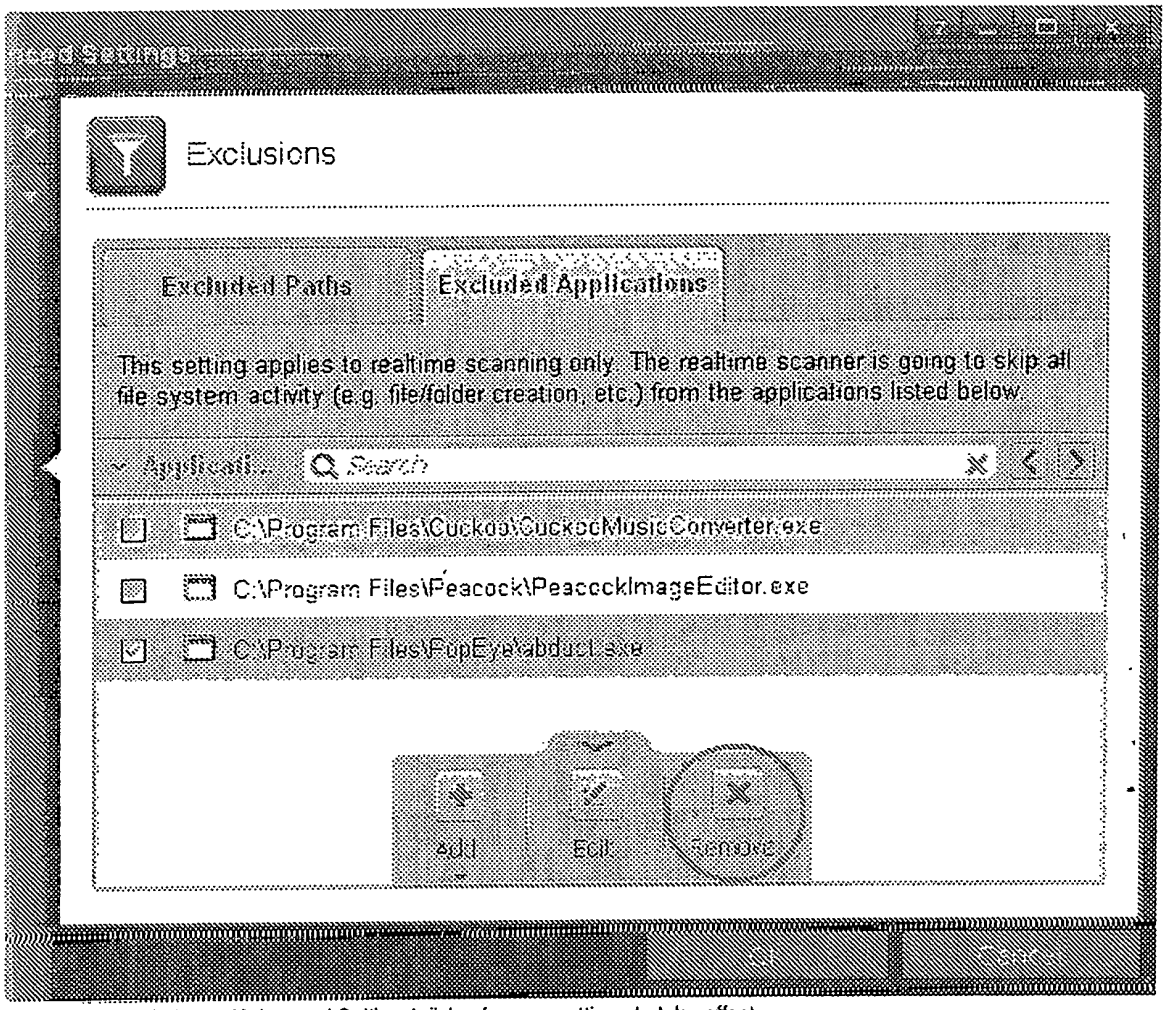
To edit the path of the application added to Excluded Application

- 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

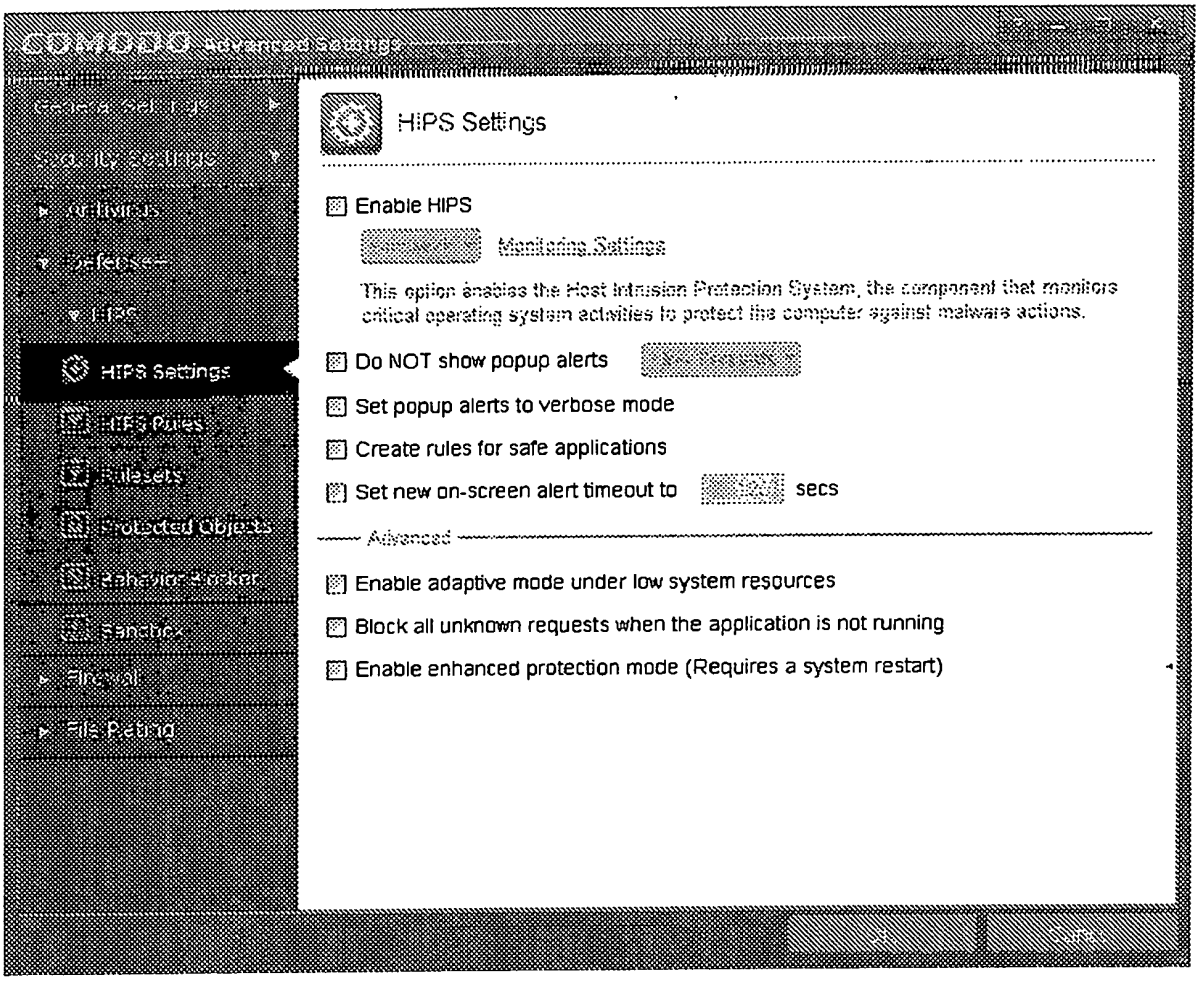
- Select the item, click the handle from the bottom center and select 'Remove'.



- 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

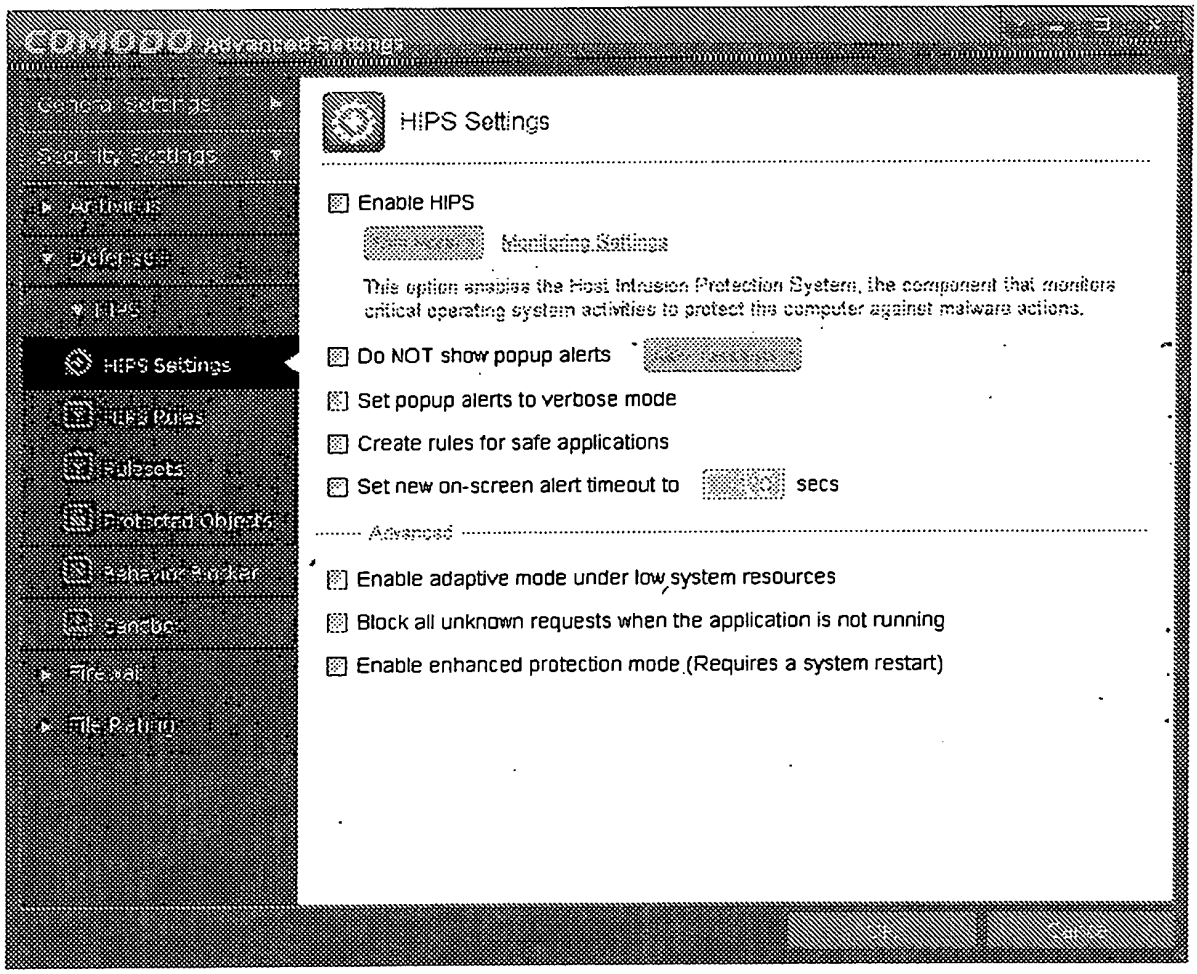
HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo Internet Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely 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



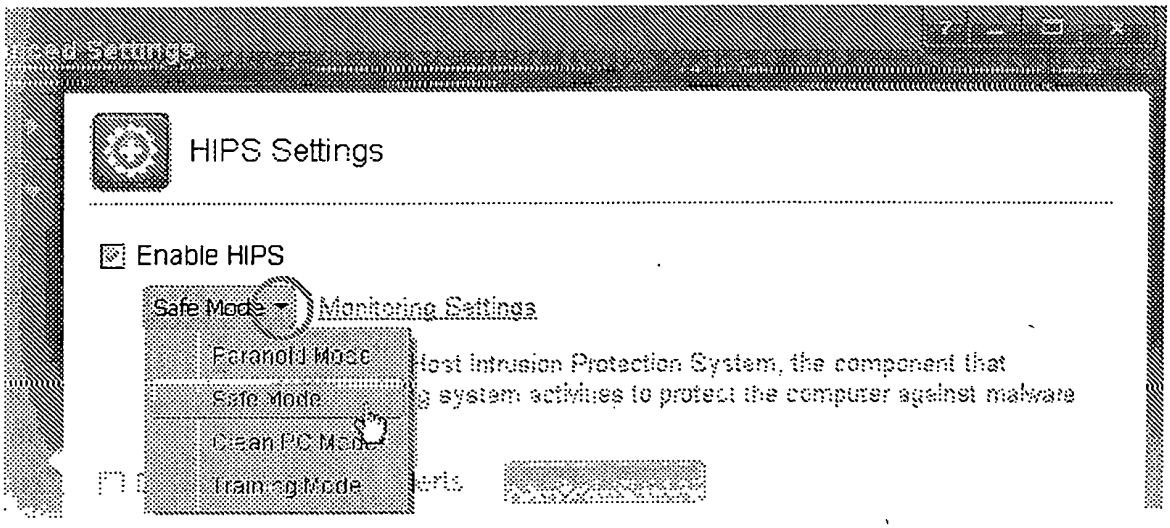
- **Enable HIPS** - Allows you to enable/disable the HIPS protection. ***(Default=Disabled)***

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:



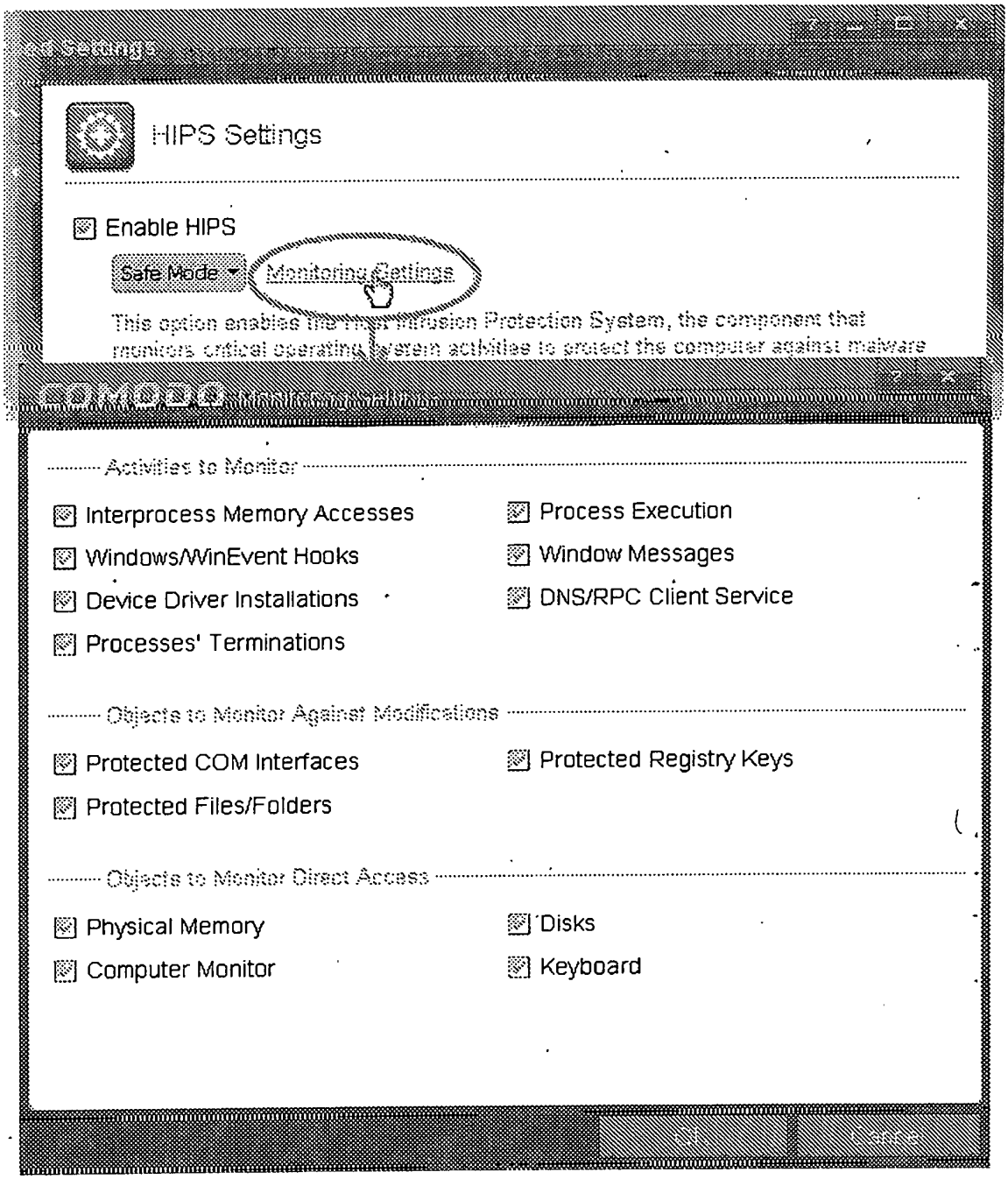
The choices available are:

- **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, malware often [illegible]

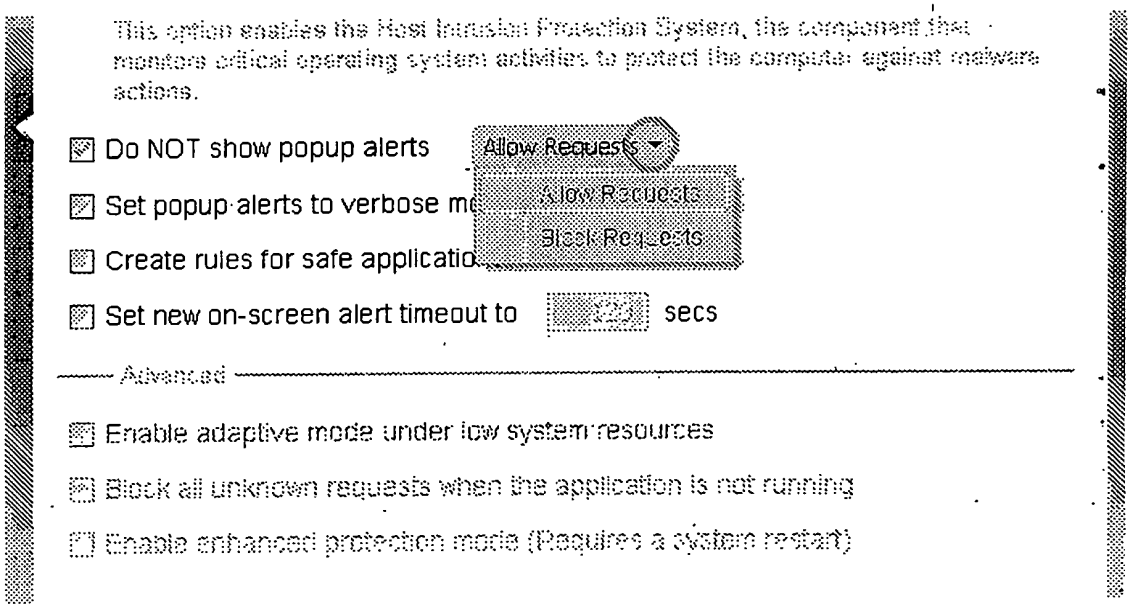
of spyware programs that use such access to monitor users' activities. (for example, to take screen shots of your current desktop; to record your browsing activities etc) ***(Default = Enabled).***

- **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).

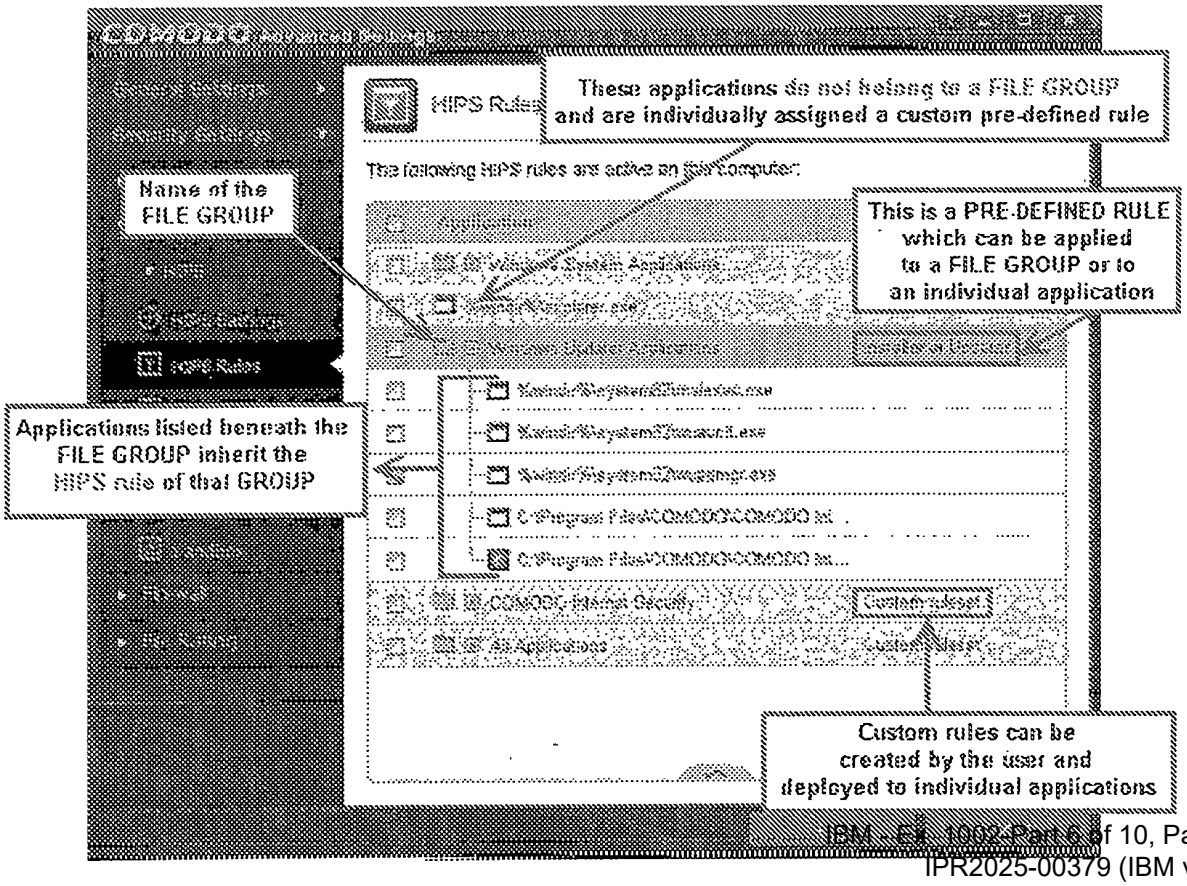
- **Set new on-screen alert time out to:** Determines how long the HIPS shows an alert for without any user intervention. By default, the timeout is set at 120 seconds. You may adjust this setting to your own preference.

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

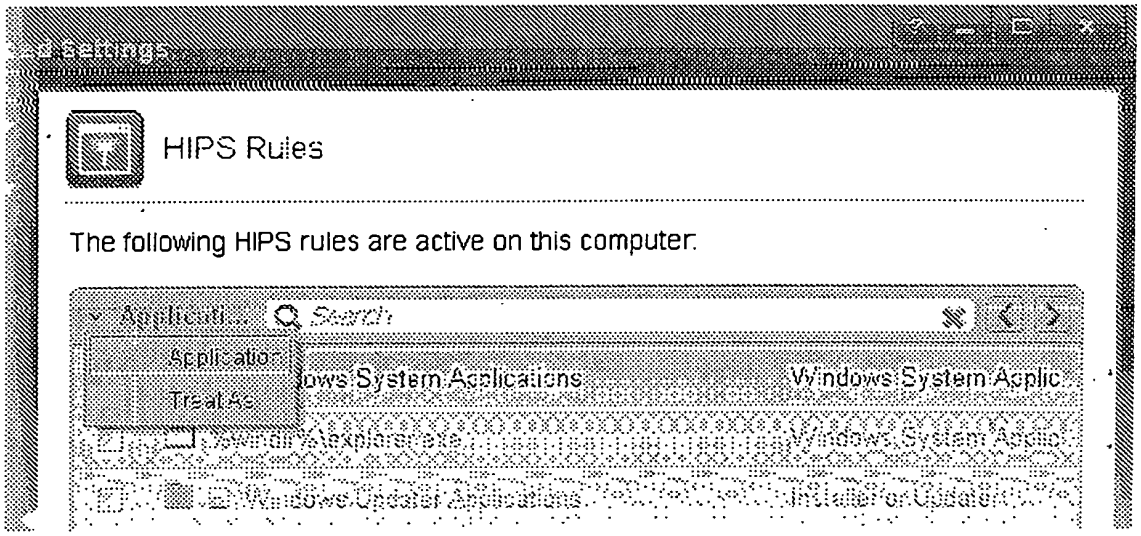
The HIPS rules tab lists the different groups of applications installed in your system and the Rulesets applied to them. You can change the ruleset applied to selected applications and also create custom rulesets to be applied to selected applications.



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

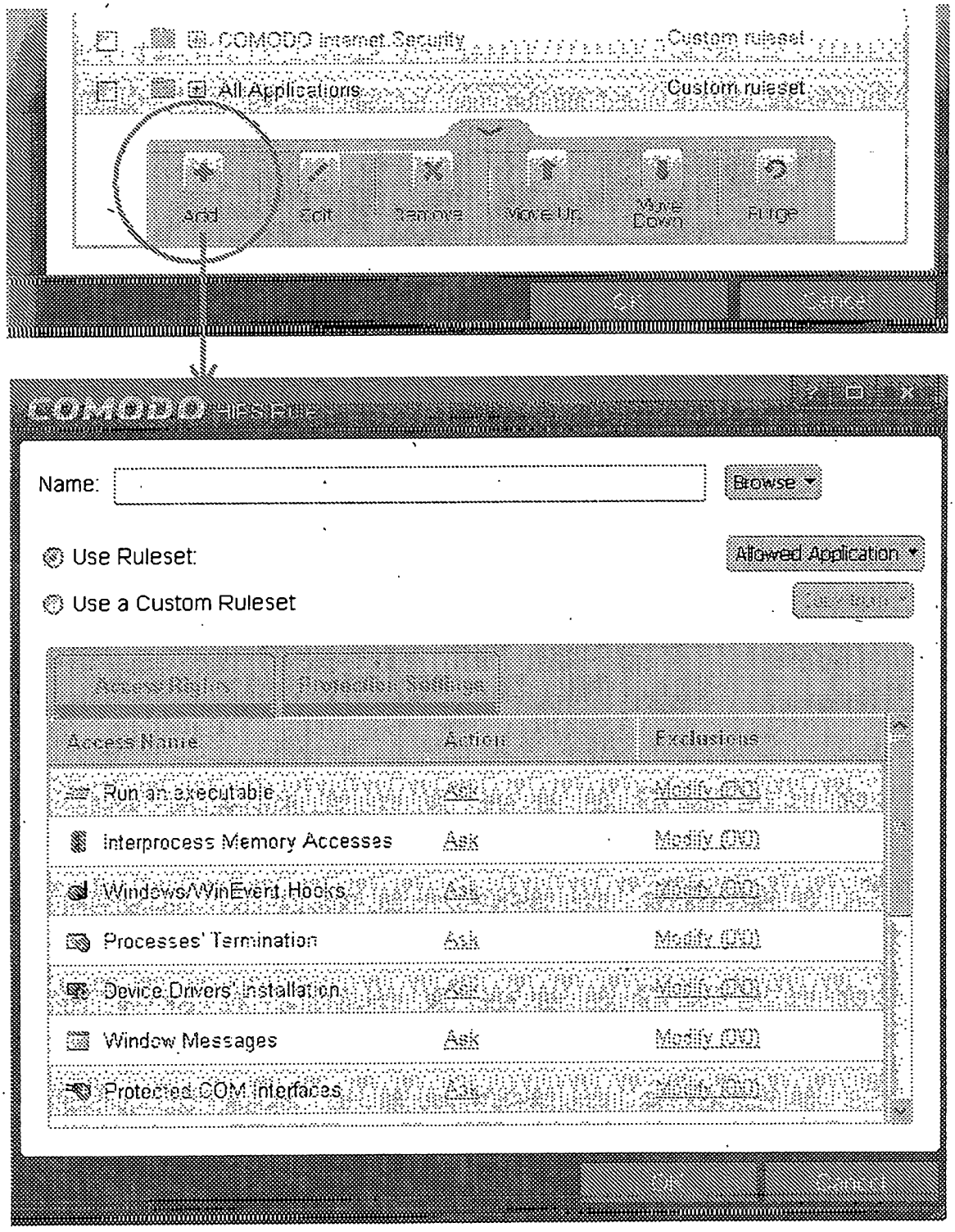
To begin defining an application's HIPS Ruleset

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.

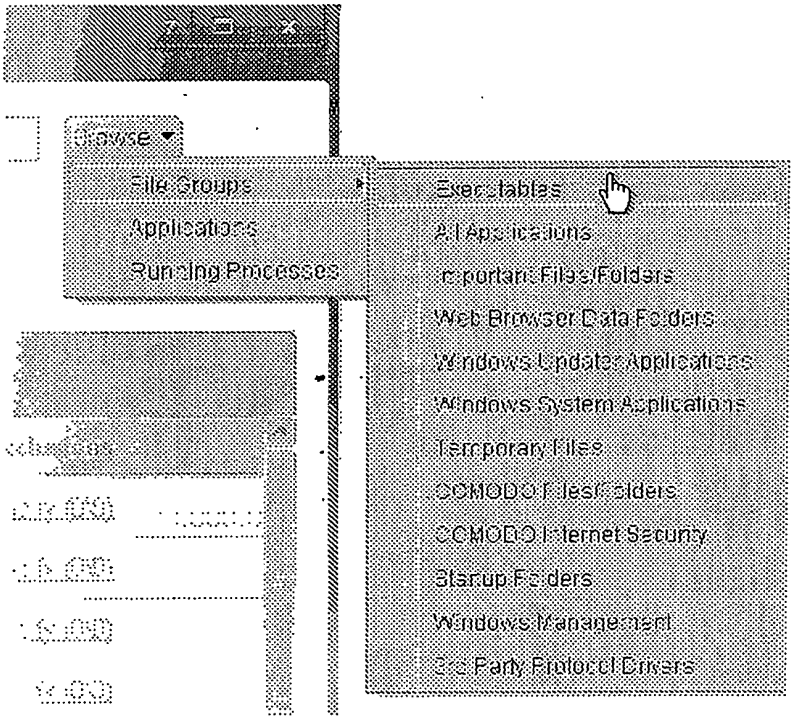


Because you are defining the HIPS rule settings for a new application, you can notice that the 'Name' box is blank. (If you were editing an existing rule instead, then this interface would show that application's name with installation path or application group's name.)

- 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.

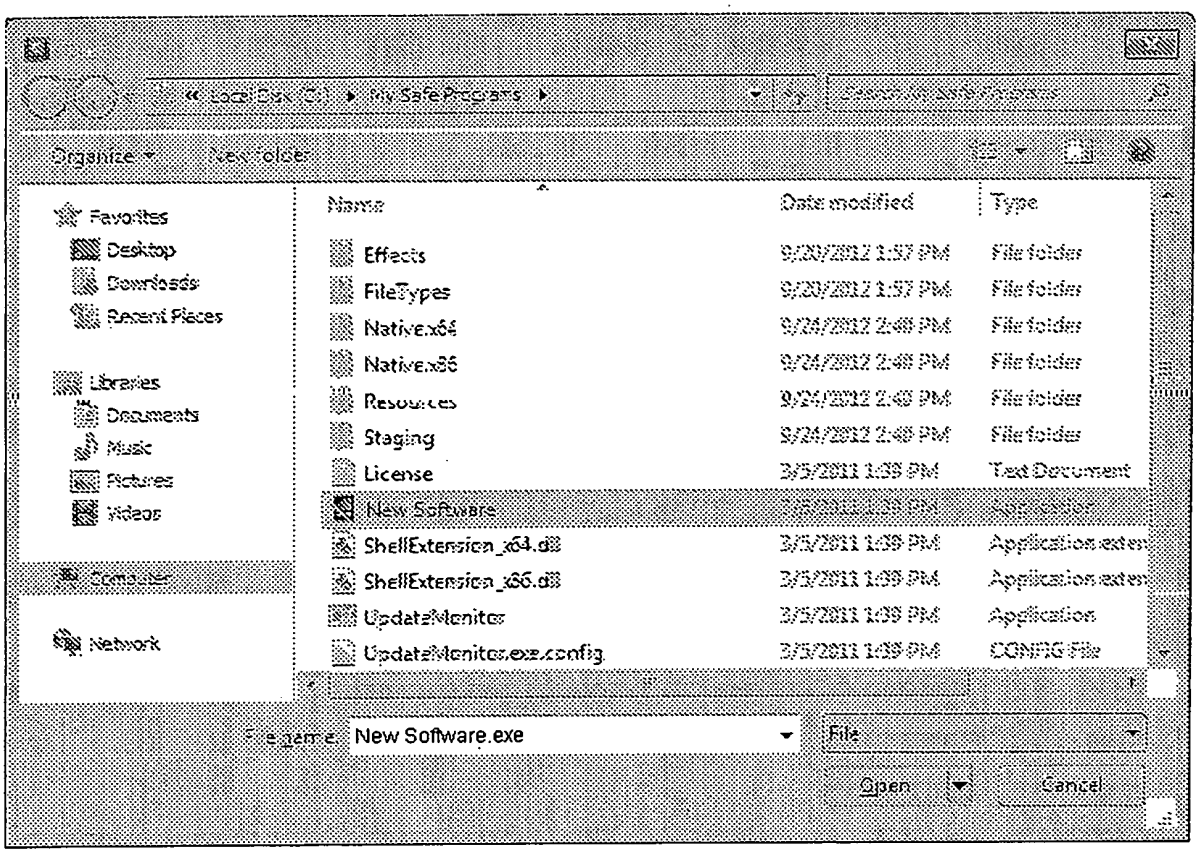


To view the file types and folders that are affected by choosing one of these options, you need to visit the 'File Groups' interface.

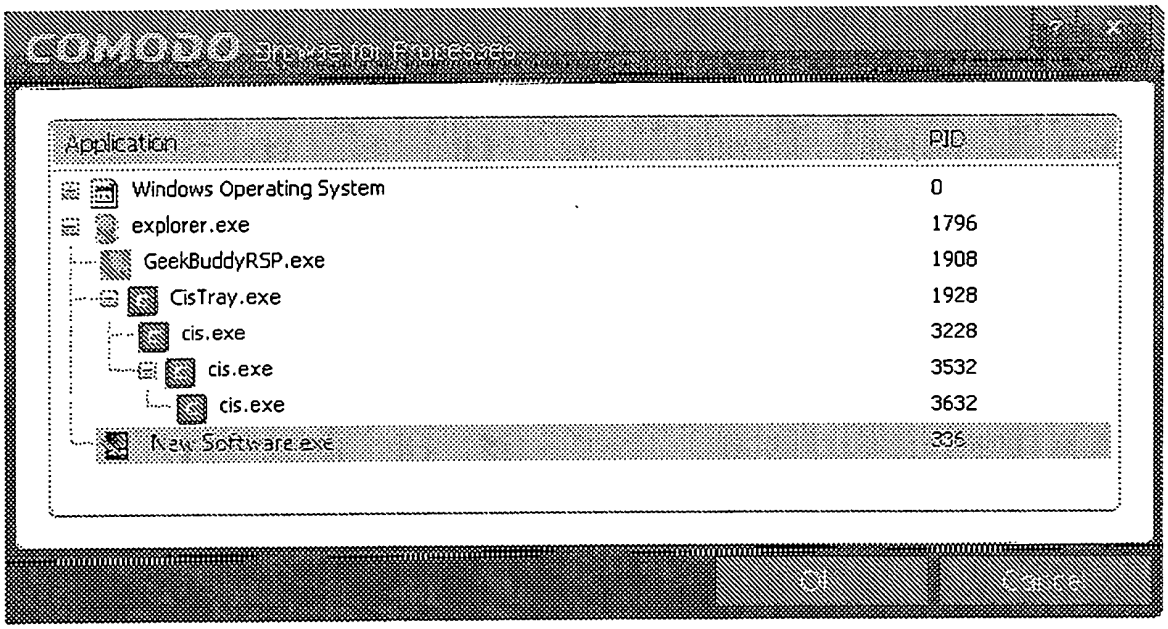
The ' File Groups interface can be accessed by the following method:

- 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.



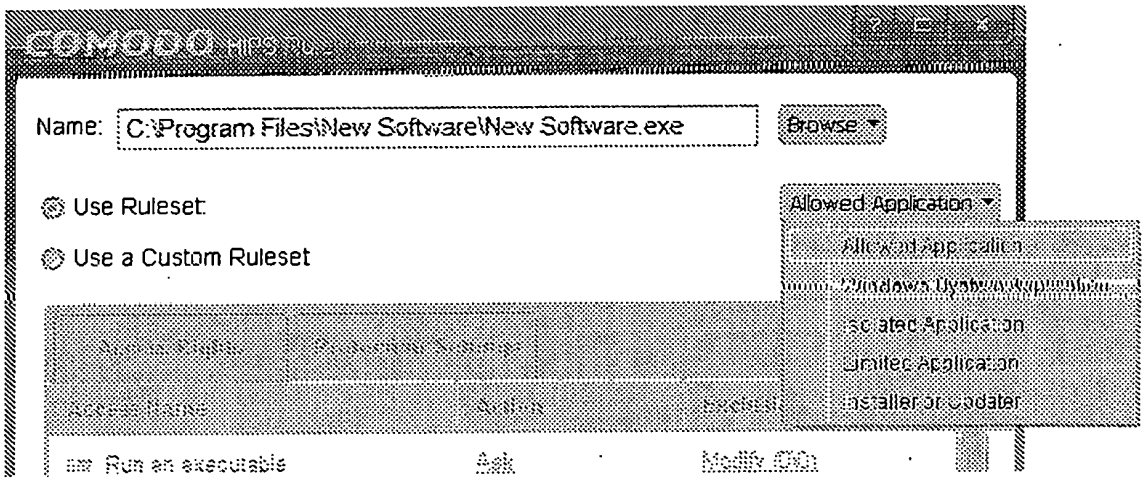
Having selected the individual application, running process or file group, the next stage is to Configure the rules for this ruleset.

Step 2 - Configure the HIPS Ruleset for this application

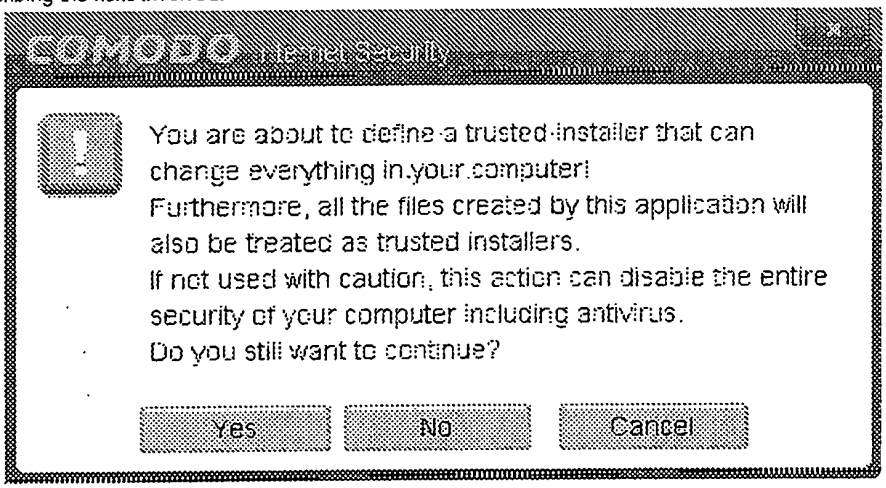
There are two broad options available for selecting a ruleset that applies to an application - Use Ruleset or Use a Custom Ruleset.

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

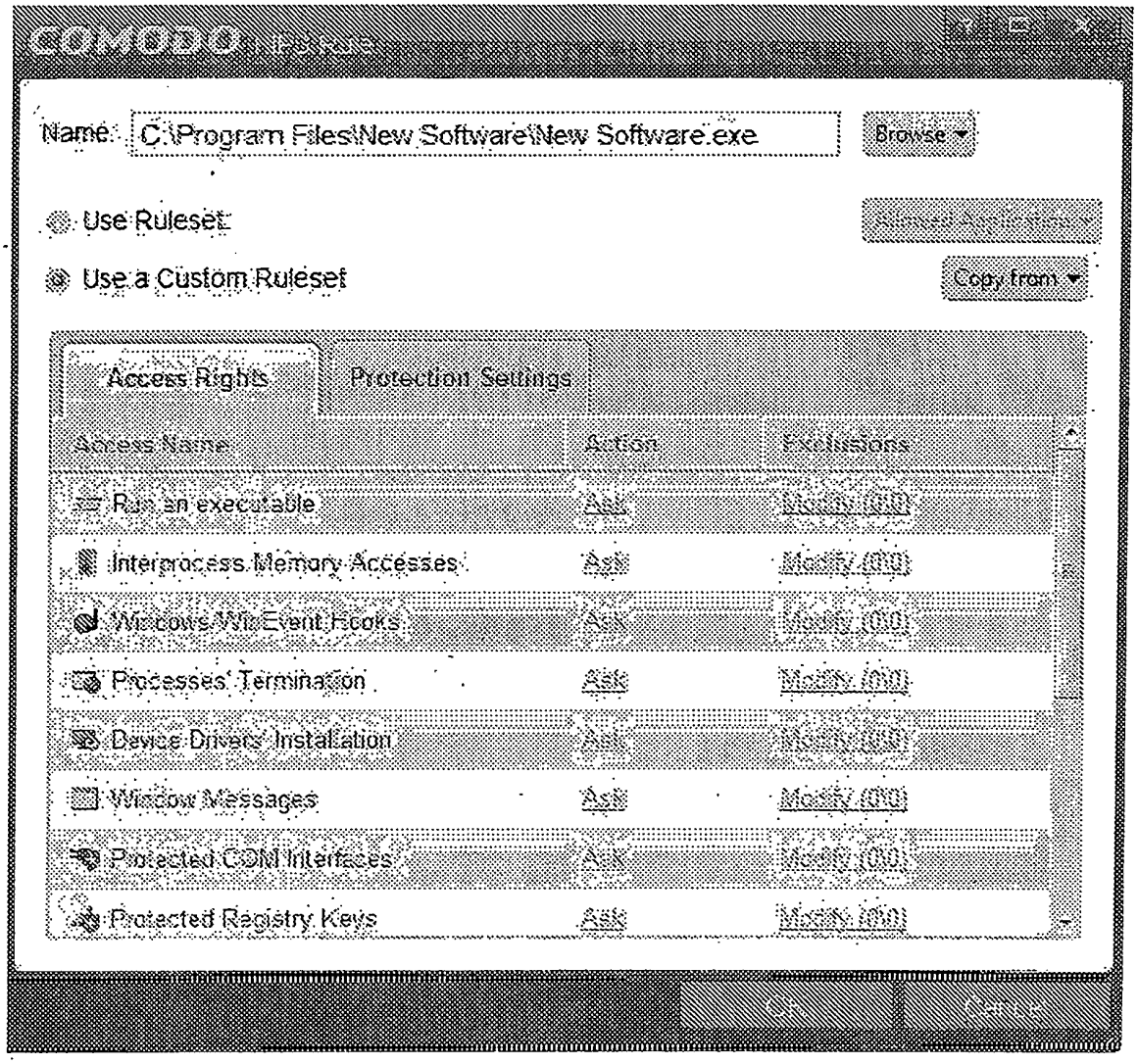


General Note: Predefined Rulesets, once chosen, cannot be modified directly from this interface - they can only be modified and defined using the 'Rulesets' interface. If you require the ability to add or modify settings for an specific application then you are effectively creating a new, custom ruleset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

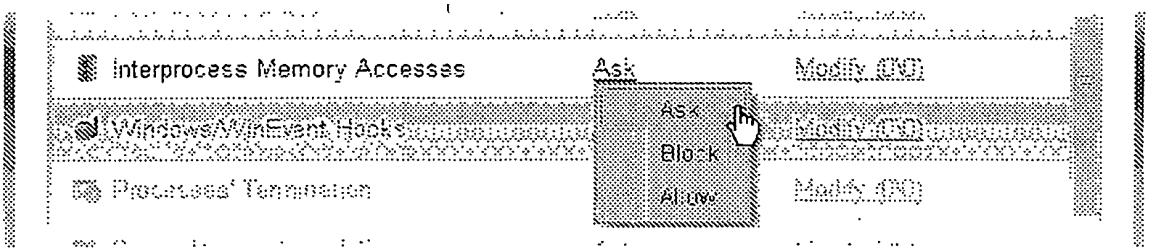
2. **Use a Custom Ruleset** - designed for more experienced users, the 'Custom Ruleset' option enables full control over the configuration specific security ruleset and the parameters of each rule within that ruleset. The Custom ruleset has two main configuration areas - Access Rights and Protection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

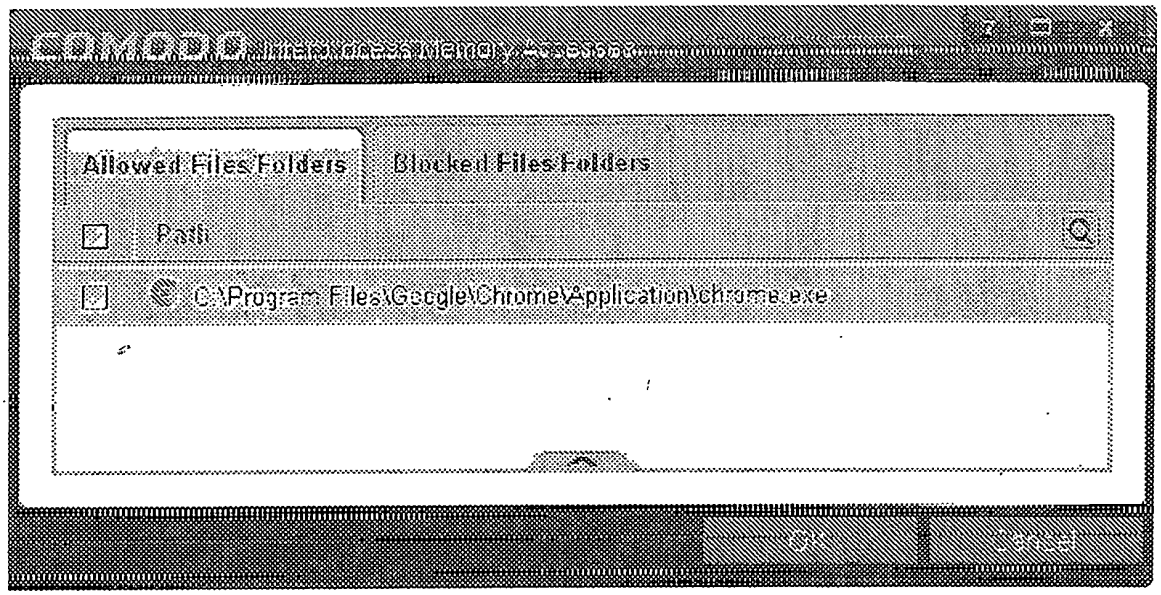
   i. **Access Rights** - The Process Access Rights tab allows you to determine what activities the applications in your custom ruleset are allowed to execute. These activities are called 'Access Names'.



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:



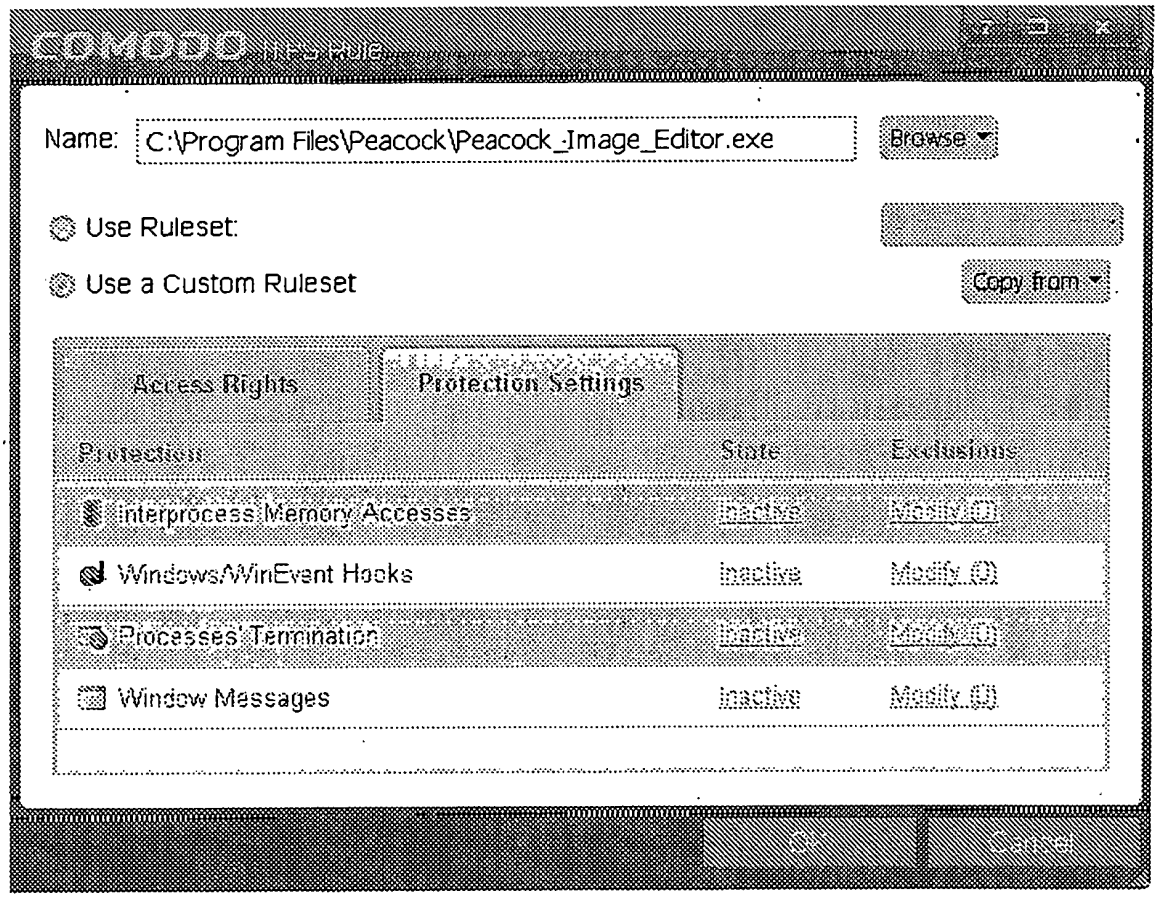
- Exceptions to your choice of 'Ask', 'Allow' or 'Block' can be specified for the ruleset by clicking the 'Modify' link on the right.
- Select the 'Allowed Applications' or 'Blocked Applications' tab depending on the type of exception you wish to create.



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

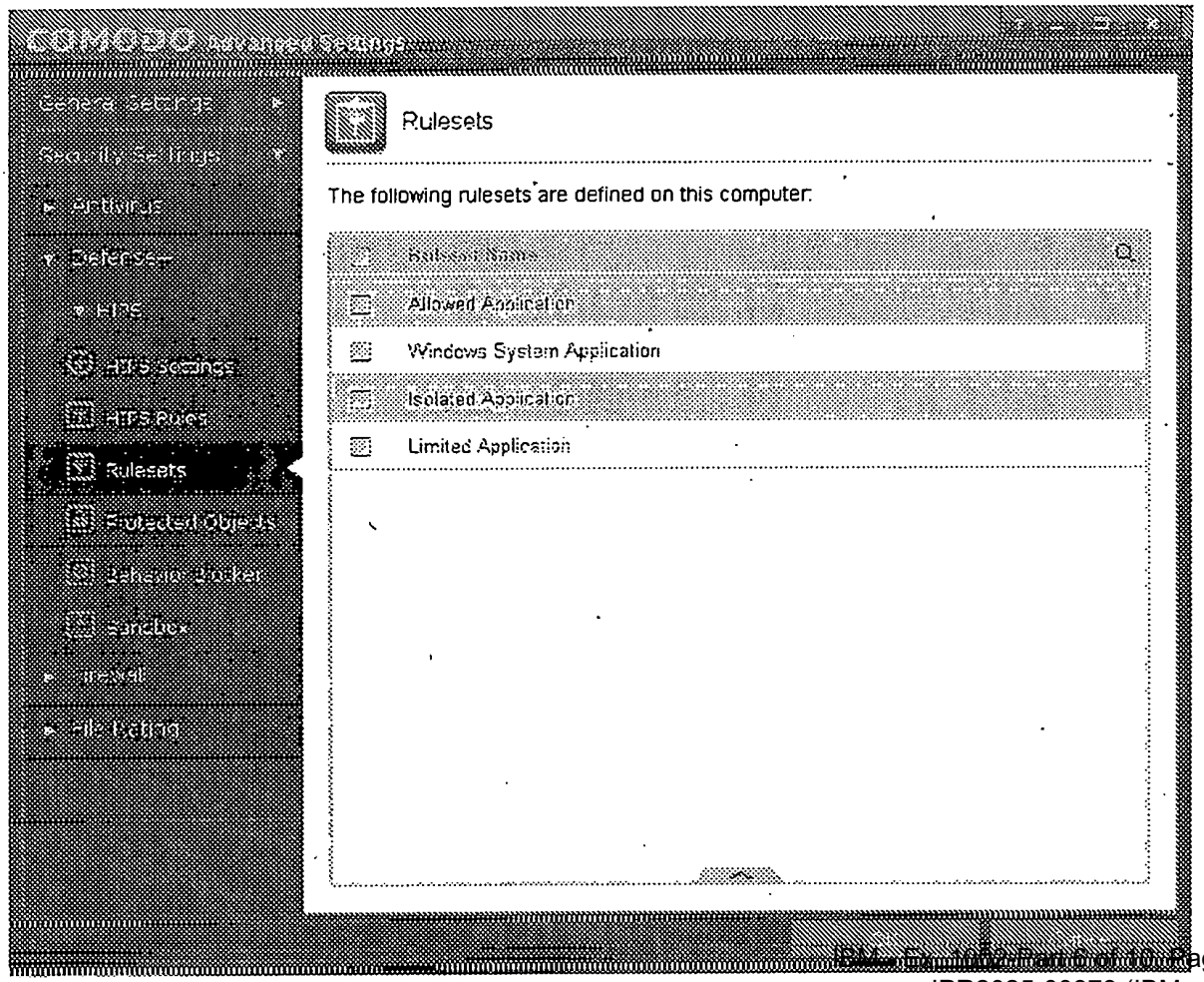
A Pre-defined ruleset is a set of access rights and protection settings that has been saved and can be re-used and deployed on multiple applications or groups. Each ruleset is comprised of a number of 'Rules' and each of these 'Rules' is defined by a set of conditions/settings/parameters. 'Predefined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

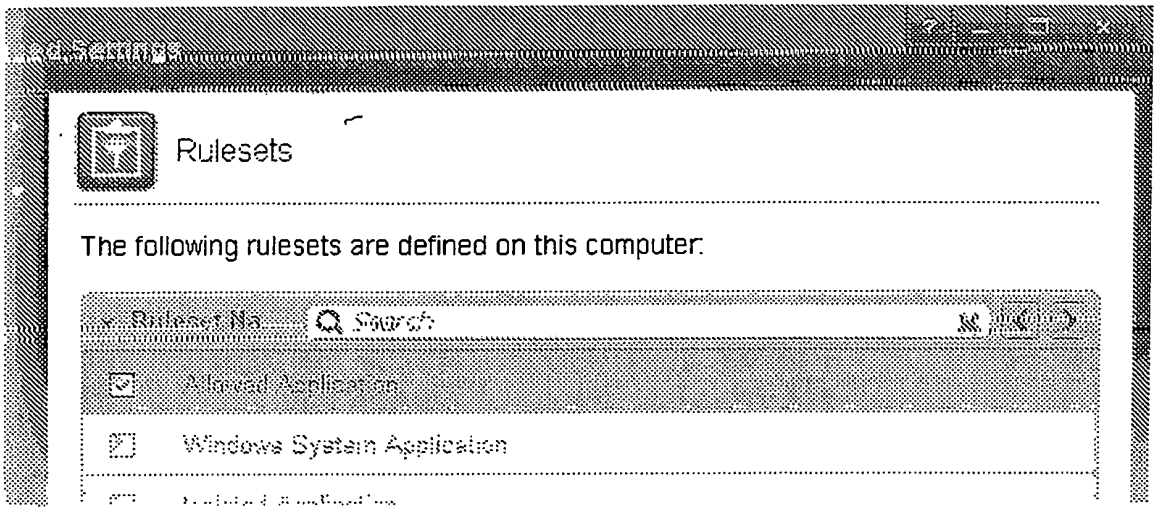
Although each application's ruleset could be defined from the ground up by individually configuring its constituent rules, this practice may prove time consuming if it had to be performed for every single program on your system. For this reason, Comodo Internet Security contains a selection of rulesets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

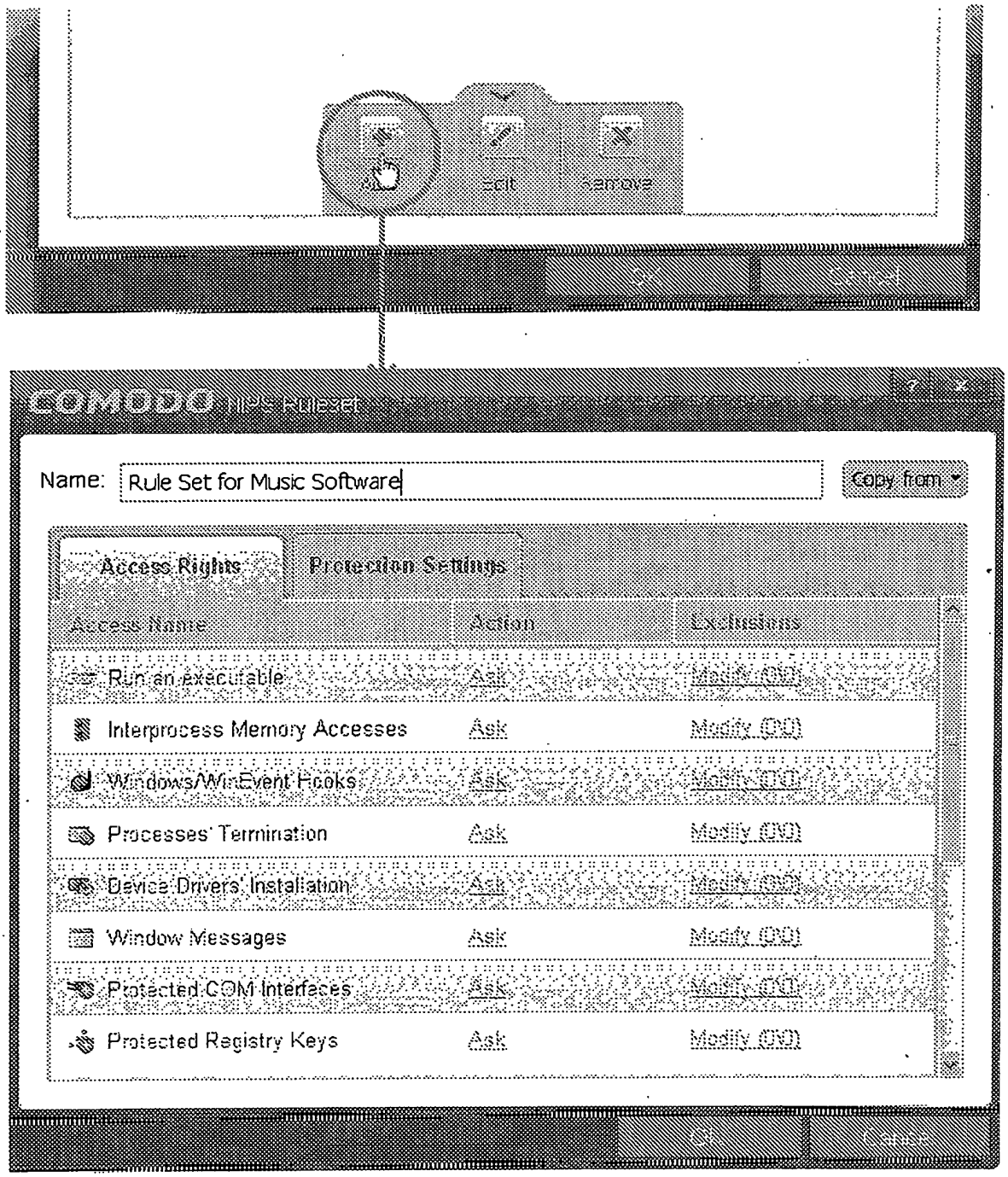
  or

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

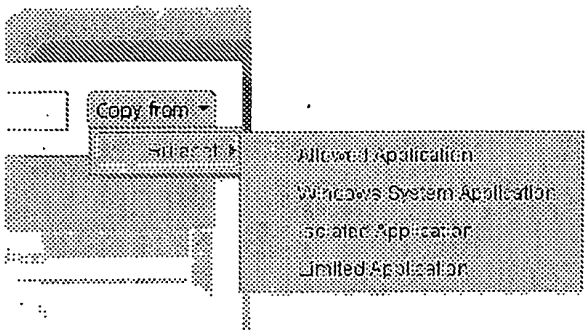
From here, you can modify a ruleset and, if desired, make changes to its 'Access Rights' and 'Protection Settings'. Any changes you make here are automatically rolled out to all applications that are currently applied with the ruleset.

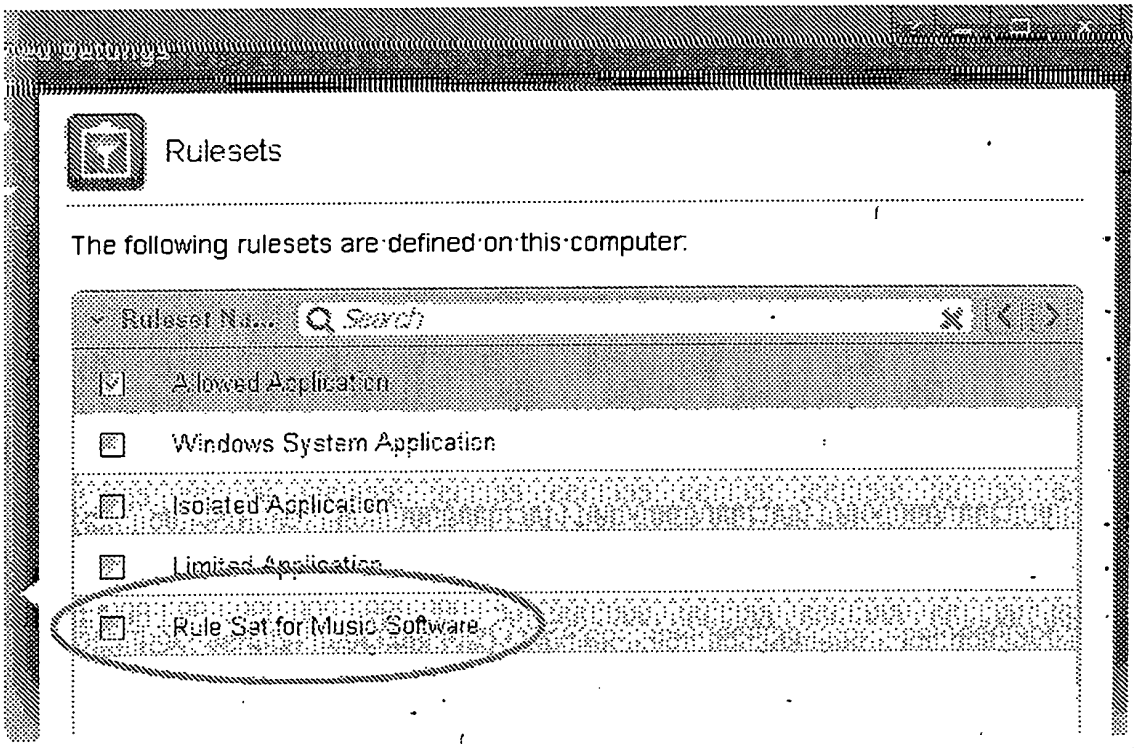
To create a new predefined ruleset

- 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.



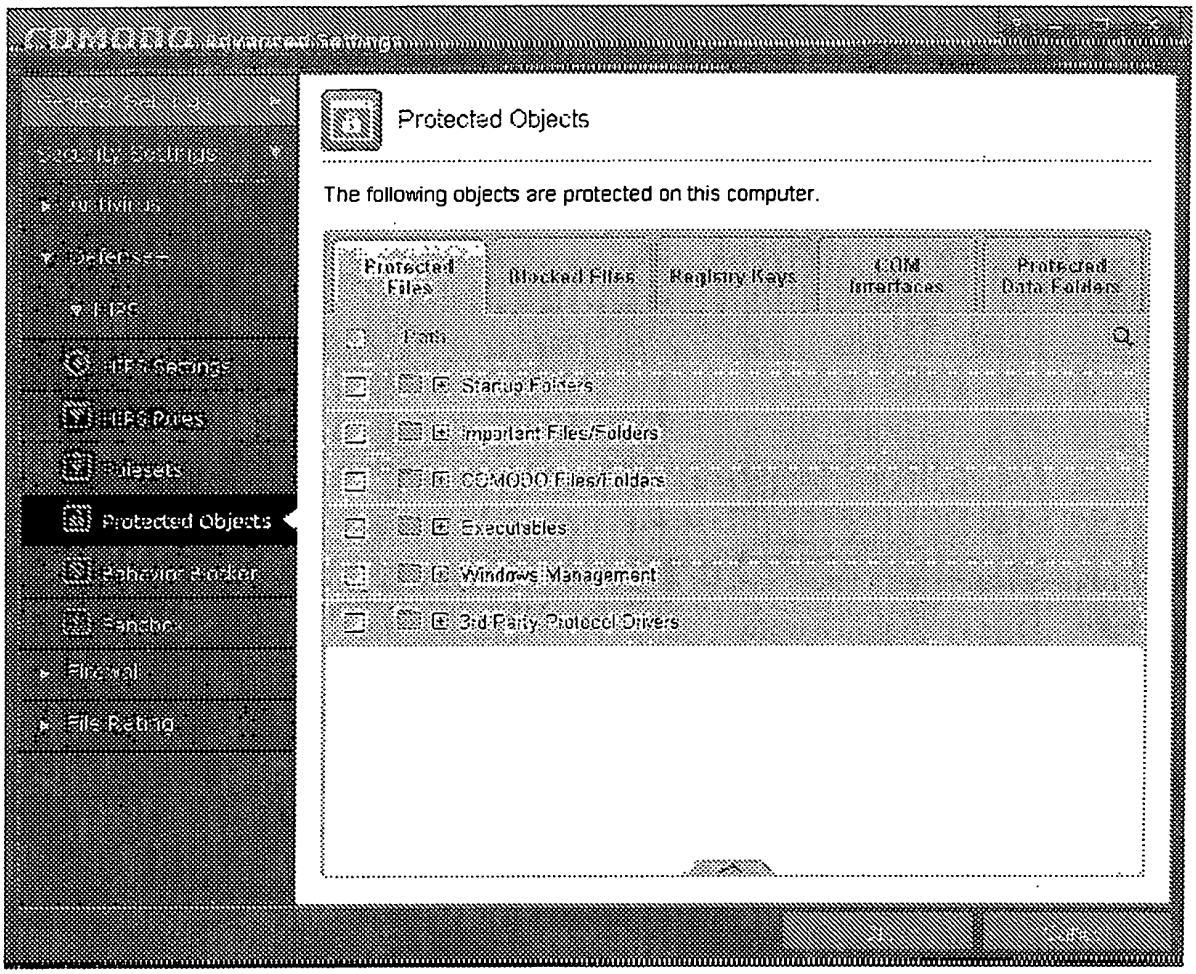


Once created, your ruleset is available for deployment onto specific application or file groups via the Active HIPS Rules interface.

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.

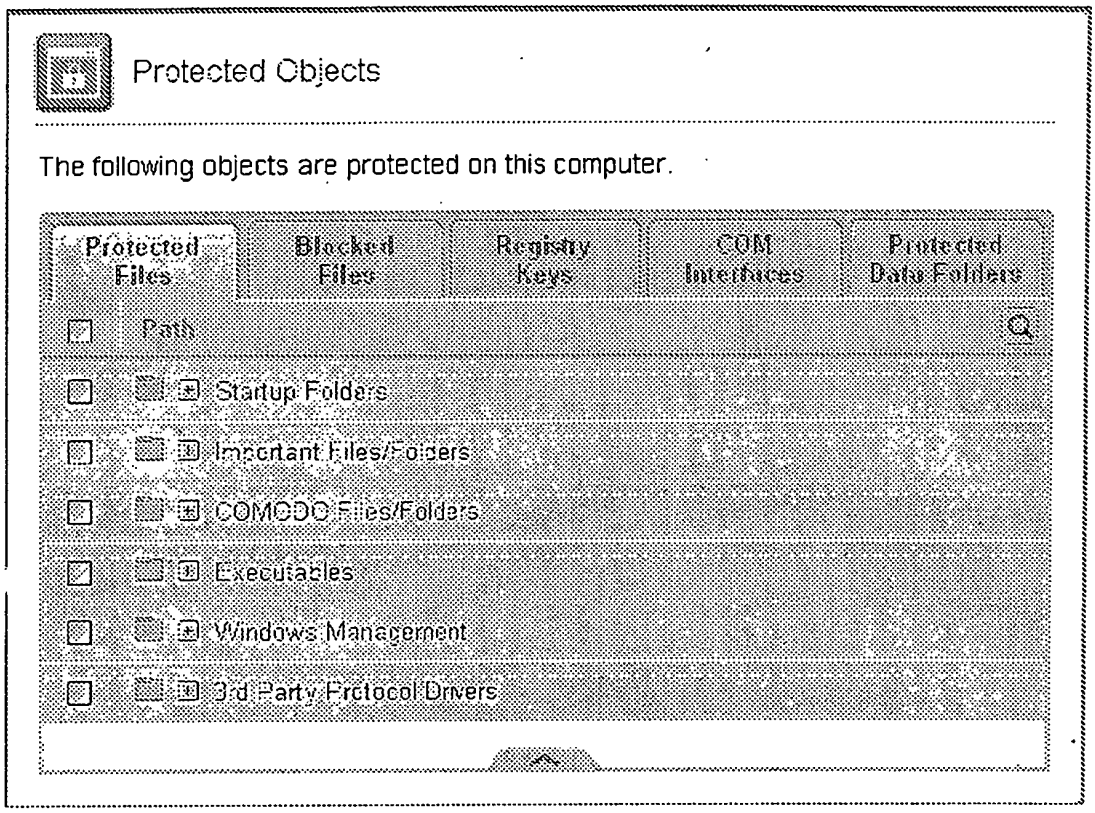


The panel has five tabs:

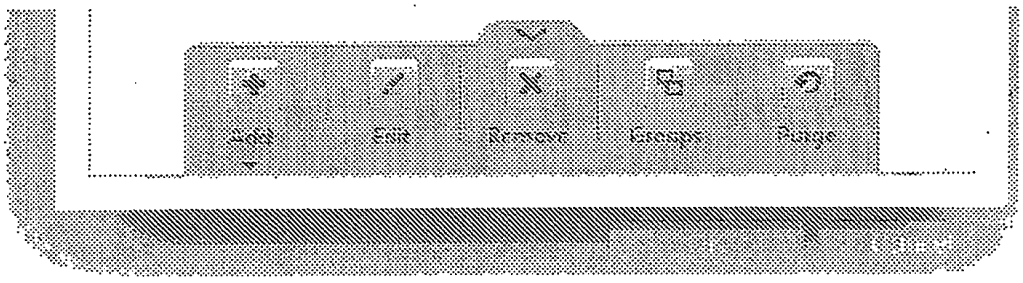
- Protected Files - Allows you to specify programs, applications and files that are to be protected from changes
- Blocked Files - Allows you to specify programs, applications and files that are to be blocked from execution and opening
- Registry Keys - Allows you to specify registry keys that are to 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.

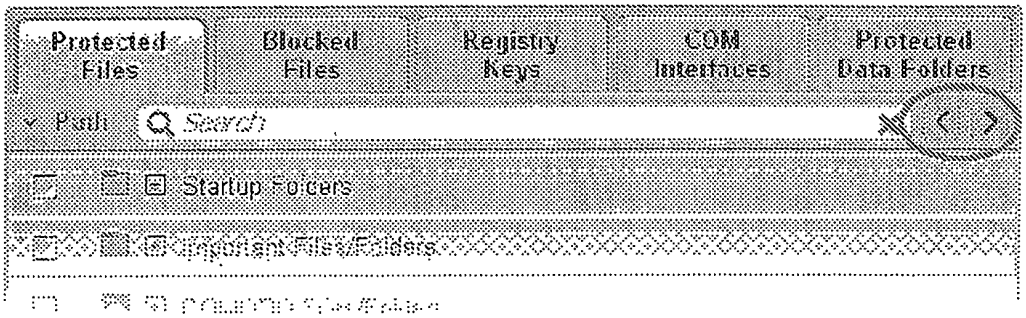


Clicking the handle at the bottom of the interface opens an options panel with the following options:

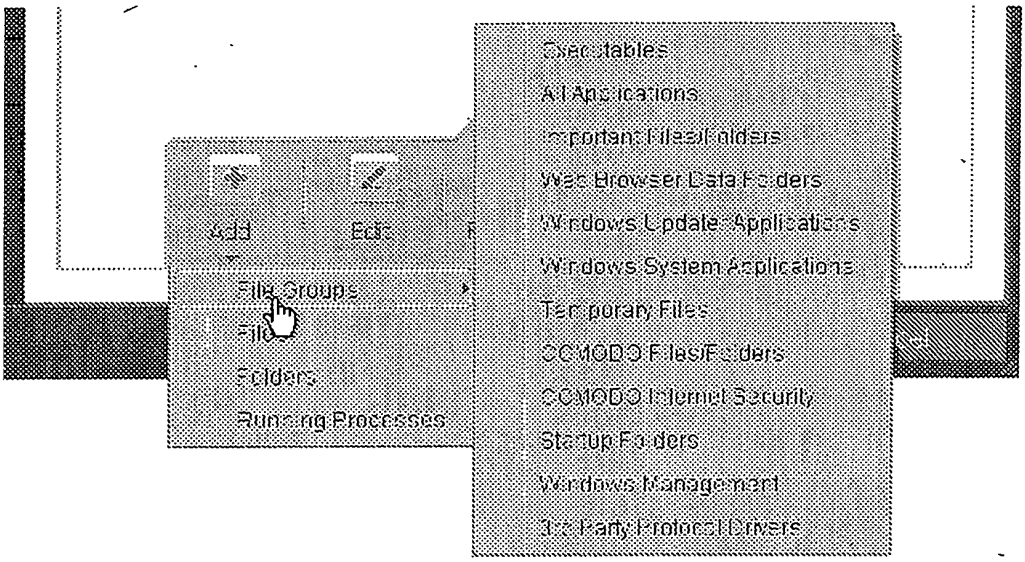


- **Add** - Allows you to add individual files, programs, applications to Protected Files.
- **Edit** - Allows you to edit the path of the file or group of a selected item in the Protected Files interface.
- **Remove** - Deletes the currently highlighted file or file group.
- **Groups** - Opens the Manage 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



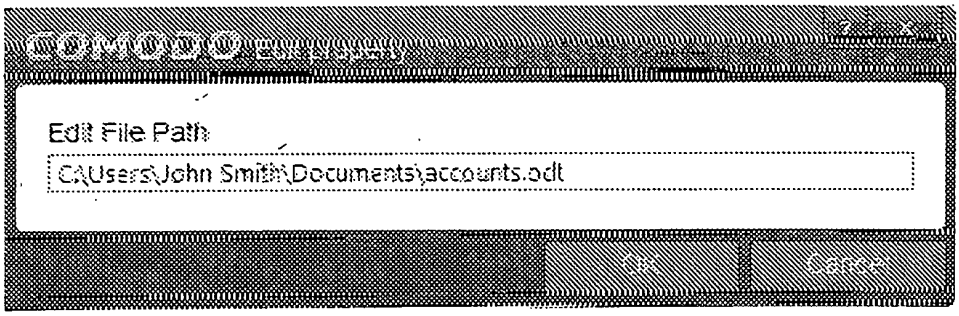
- Click the handle from the bottom center and select 'Add'.

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.

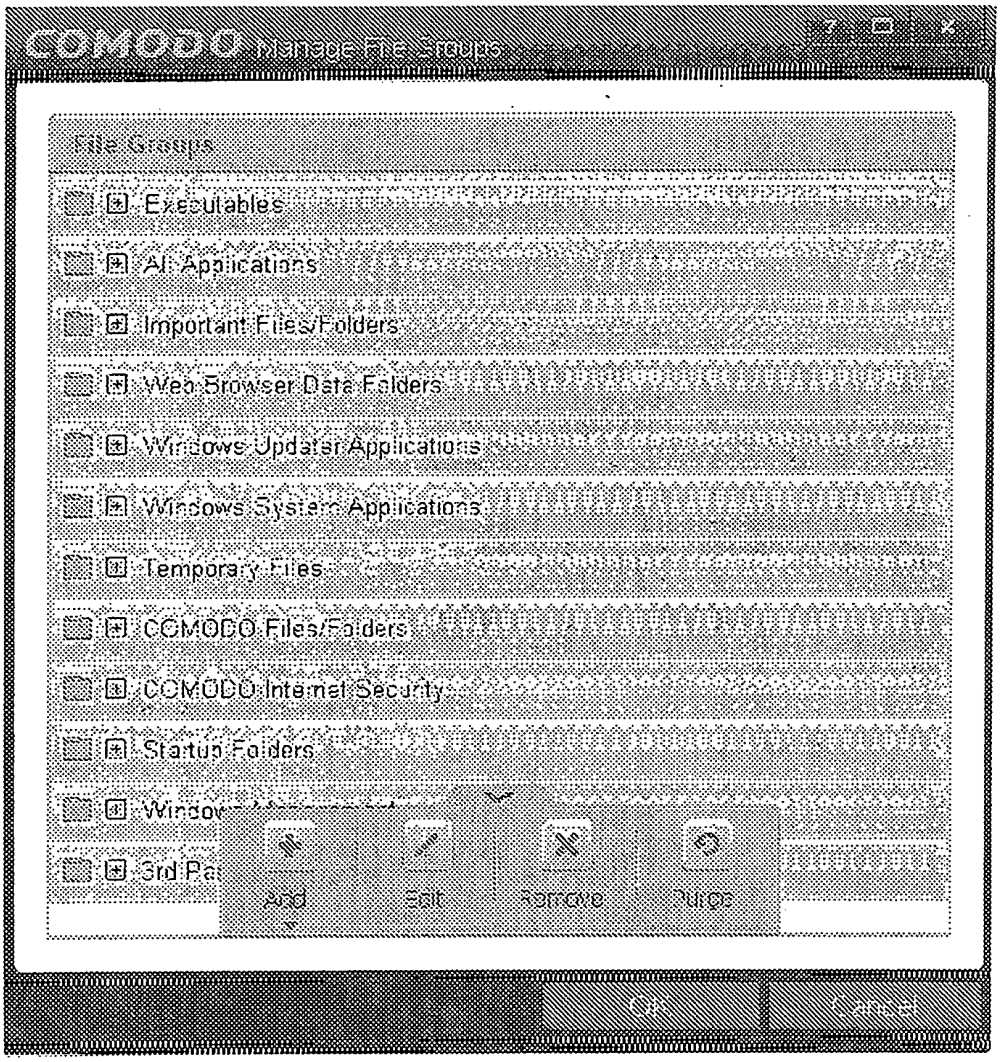
File Groups

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.

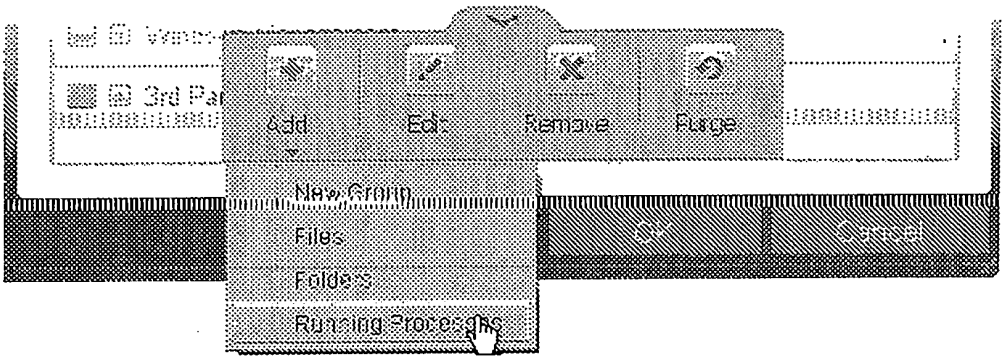


This interface allows you to

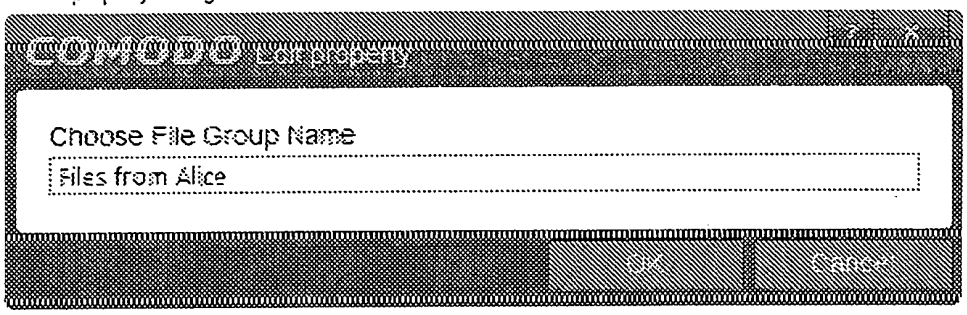
- Create a new File Group
- Edit the names of an Existing File Group
- Add a file to an existing file group
- Remove existing file group(s) or individual file(s) from existing group

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



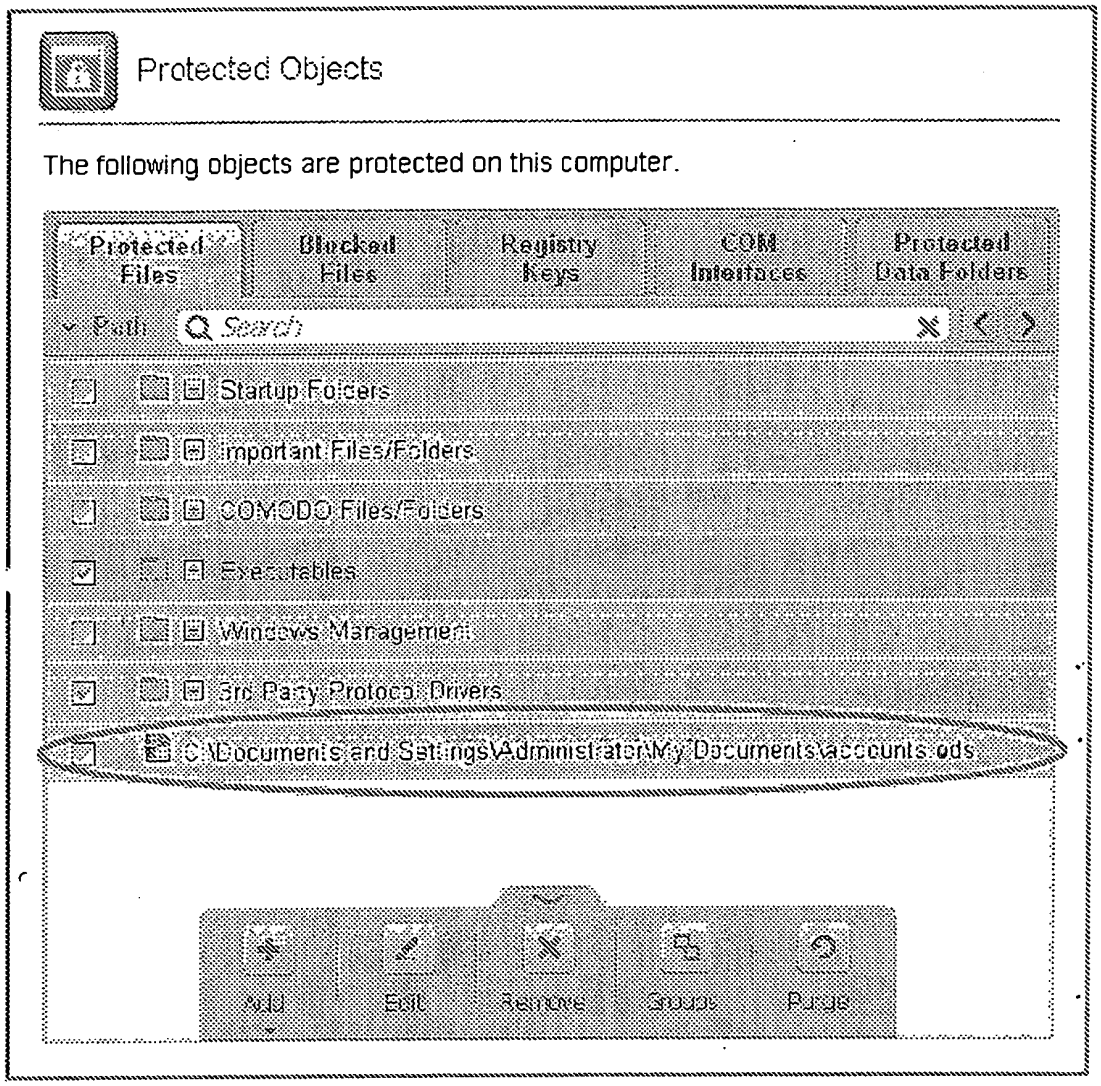
- **Add files to a group** - Select the Group, click the handle and select Add. Choose from 'Files', 'Folders' or 'Running Processes' to add files by browsing to the file or folder or from currently running processes

- 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'.

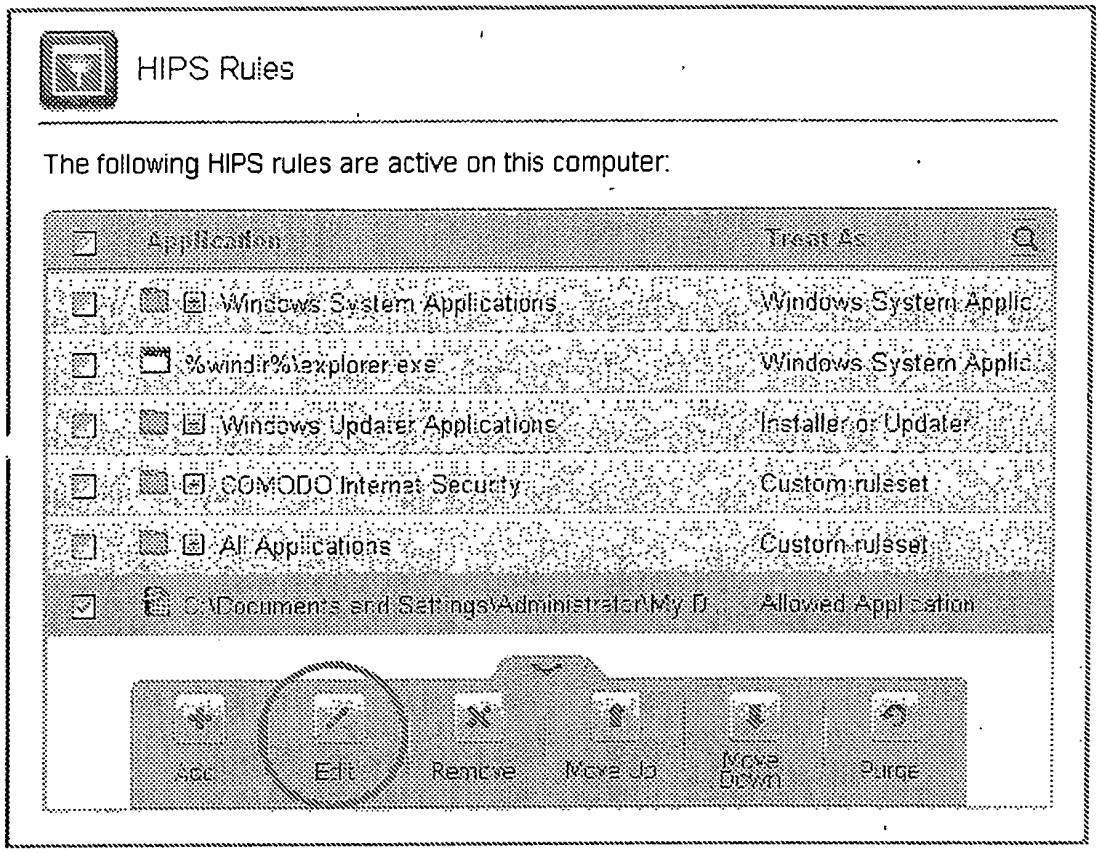
Exceptions

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'.

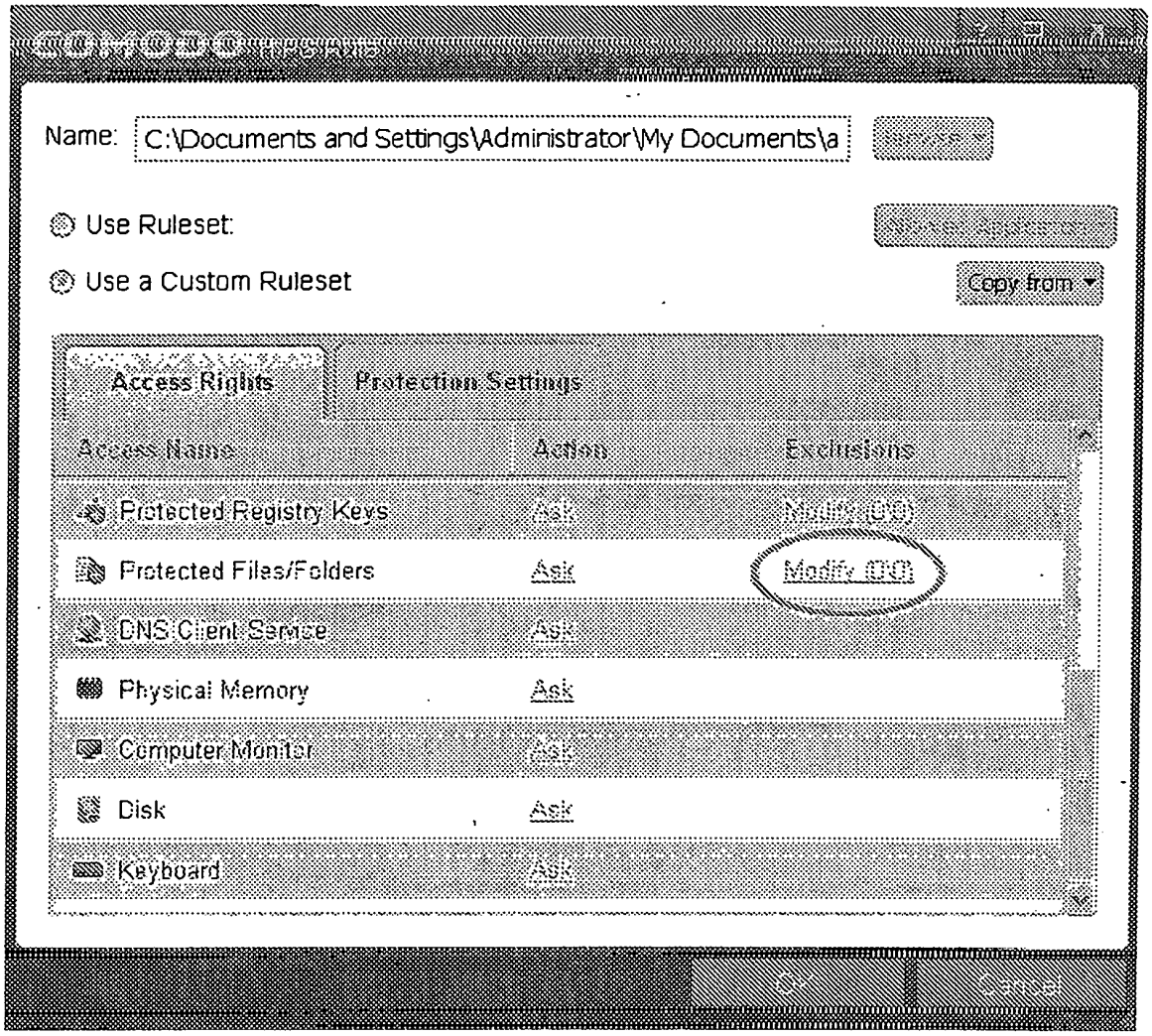
- First add Accounts.odt to Protected Files area.



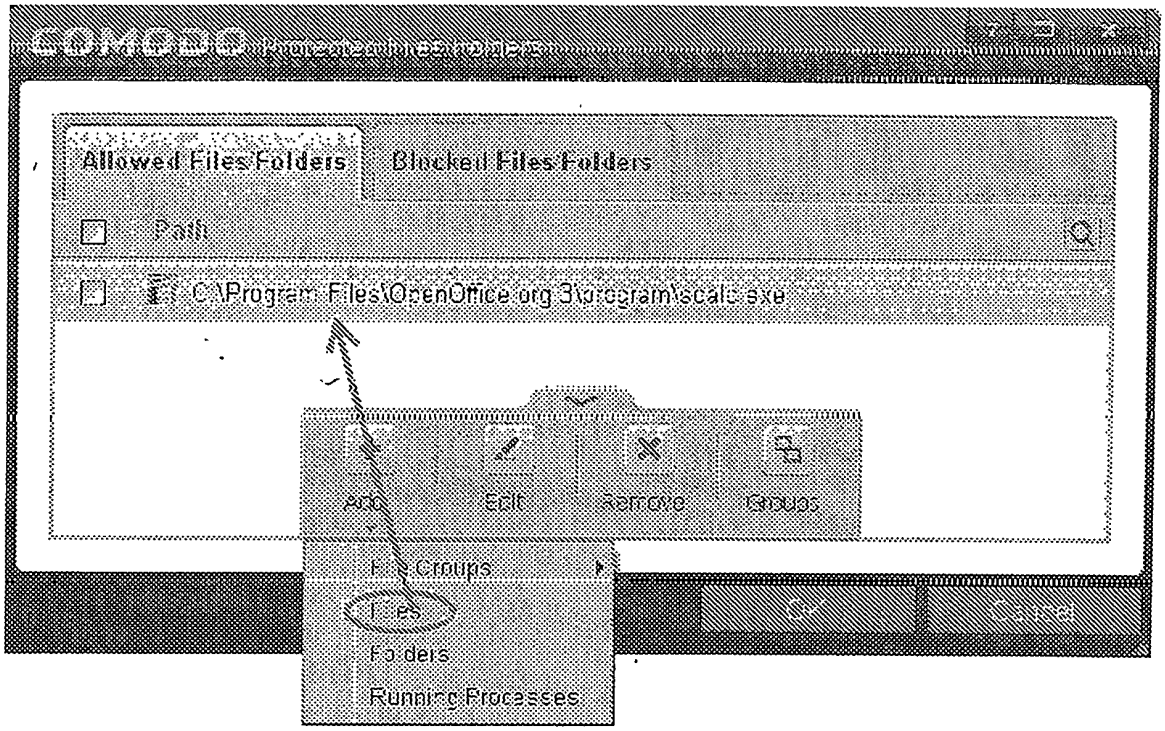
- Then go to HIPS Rules interface and add it to the list of applications. Click the handle at the bottom and choose 'Edit' after selecting the checkbox beside it.



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



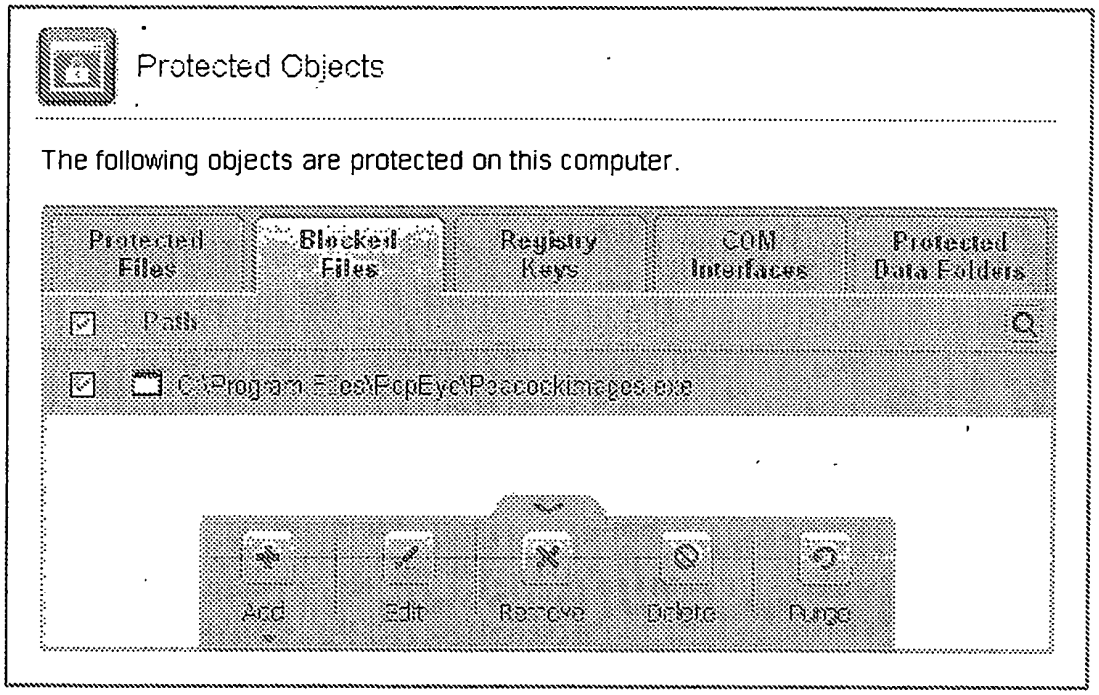
- Under the 'Access Rights' tab, click the link 'Modify' beside the entry Protected Files/Folders. The Protected Files and Folders interface will appear.
- Under the 'Allowed Files/Folders' tab, click the handle, choose 'Add' > 'Files' and add scalc.exe as exceptions to the 'Ask' or 'Block' rule in the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



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

6.2.2.4.2. Blocked Files

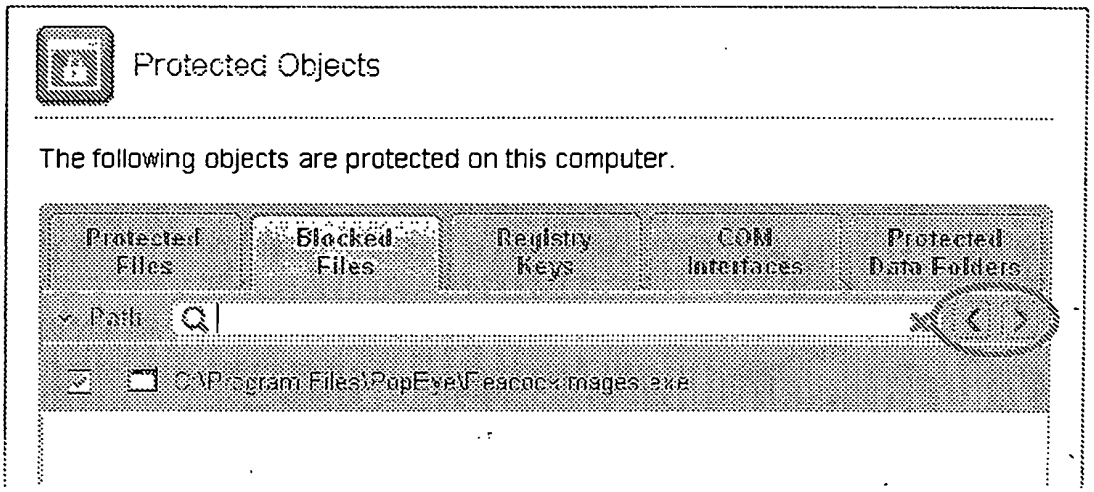
Defense+ allows you to lock-down files and folders by completely denying all access rights to them from other processes or users - effectively cutting it off from the rest of your system. If the file you block is an executable, then neither you nor anything else is able to run that program. Unlike files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



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

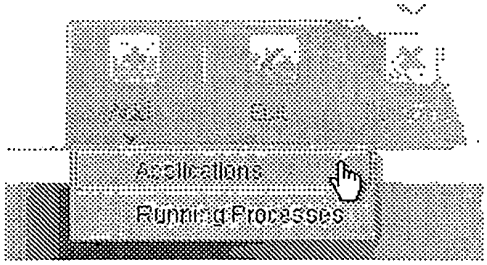
- Add - Allows you to add individual files, programs, applications to Blocked Files.
- Edit - Allows you to edit the path of the file.
- Remove - Releases the currently highlighted file from the blocked files list.
- Delete - Deletes the highlighted file from your computer
- **Purge** - Runs a system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

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'.

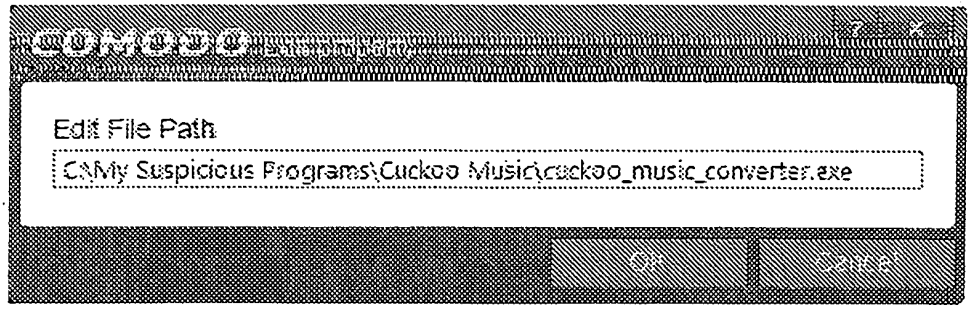


You can add the files by following methods:

- 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'.

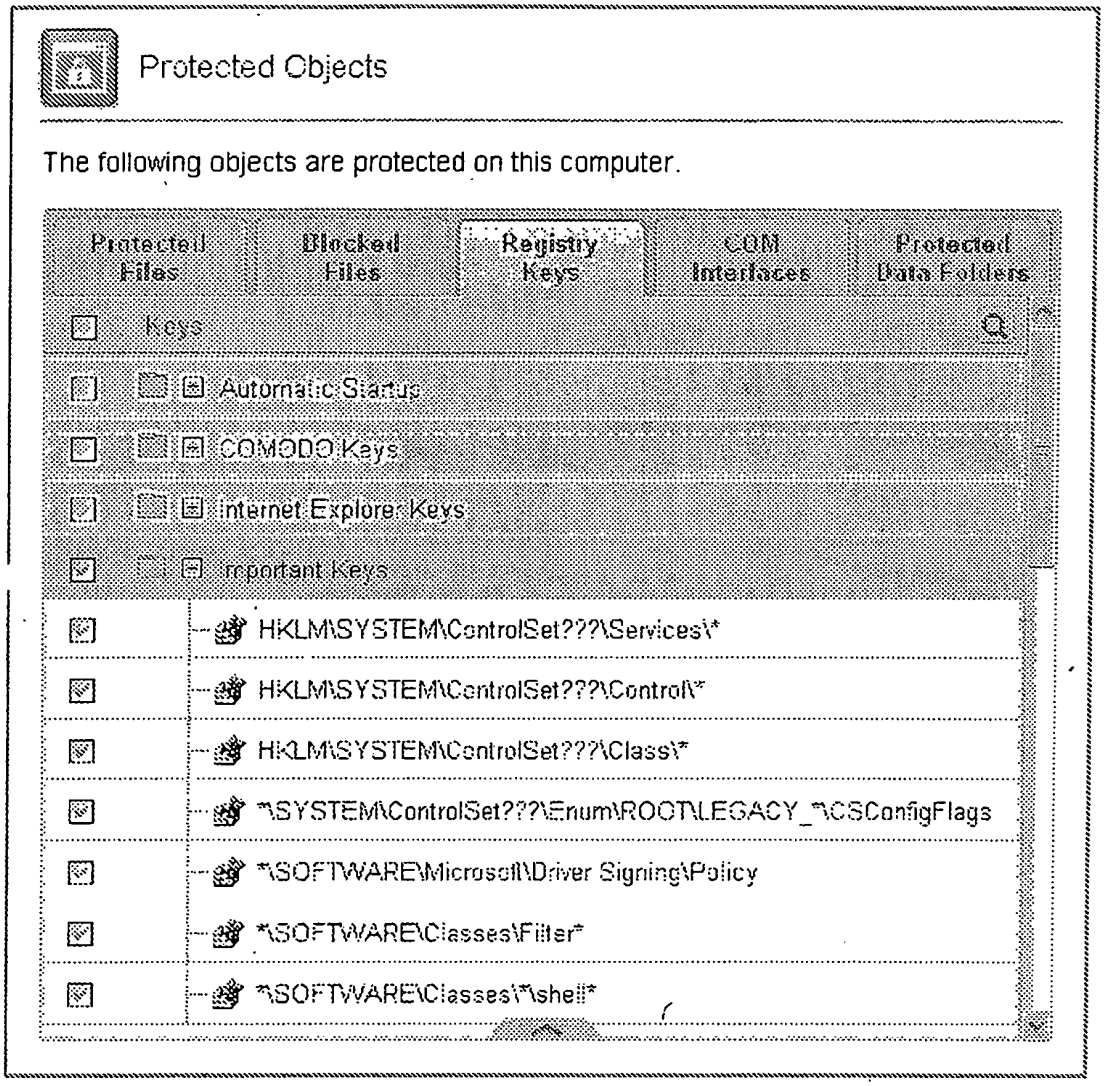
The selected item will be deleted from your computer immediately.

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'.

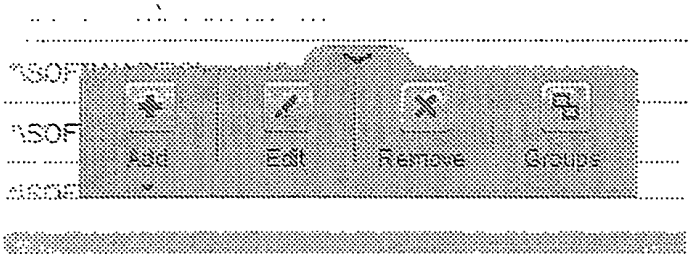
6.2.2.4.3. Protected Registry Keys

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.



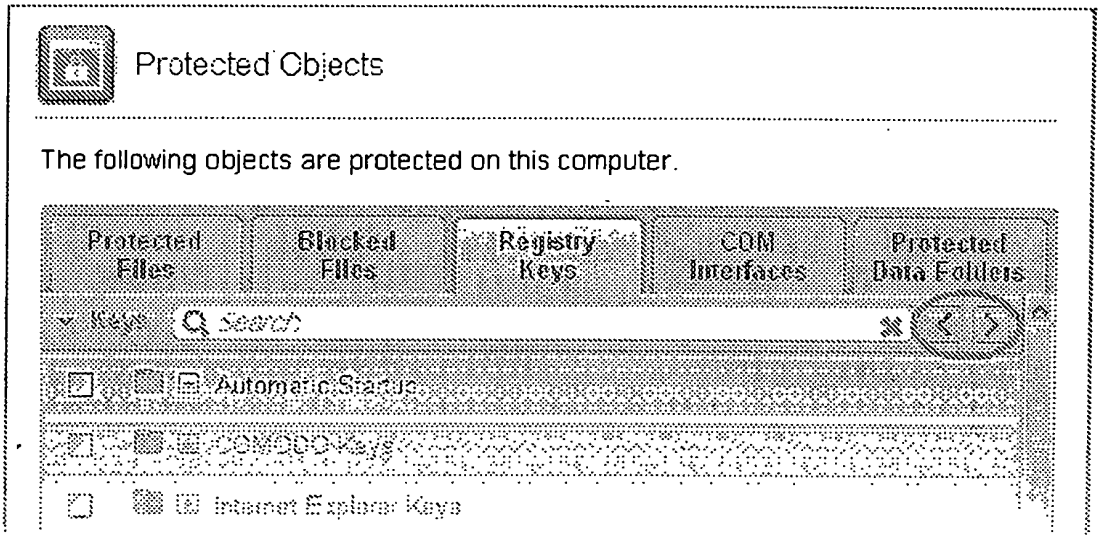
Clicking the handle at the bottom of the interface opens an options panel with the following options:



- 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.

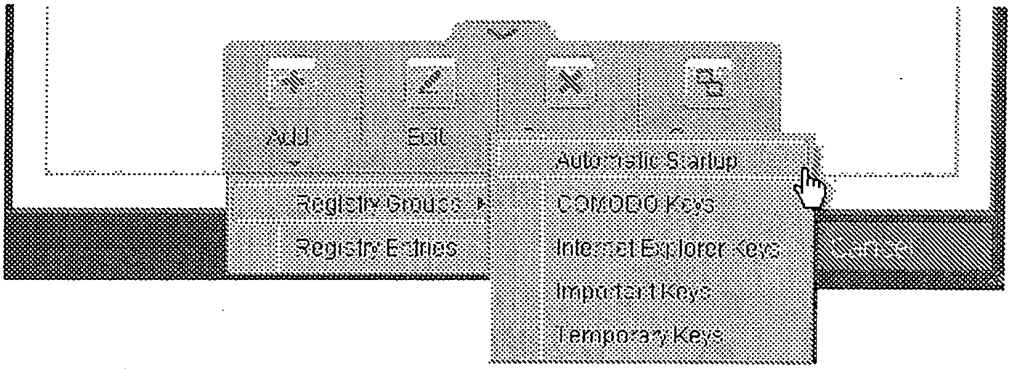
You can use the search option to find a specific registry key or group in the list by clicking the search icon at the far right in

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.



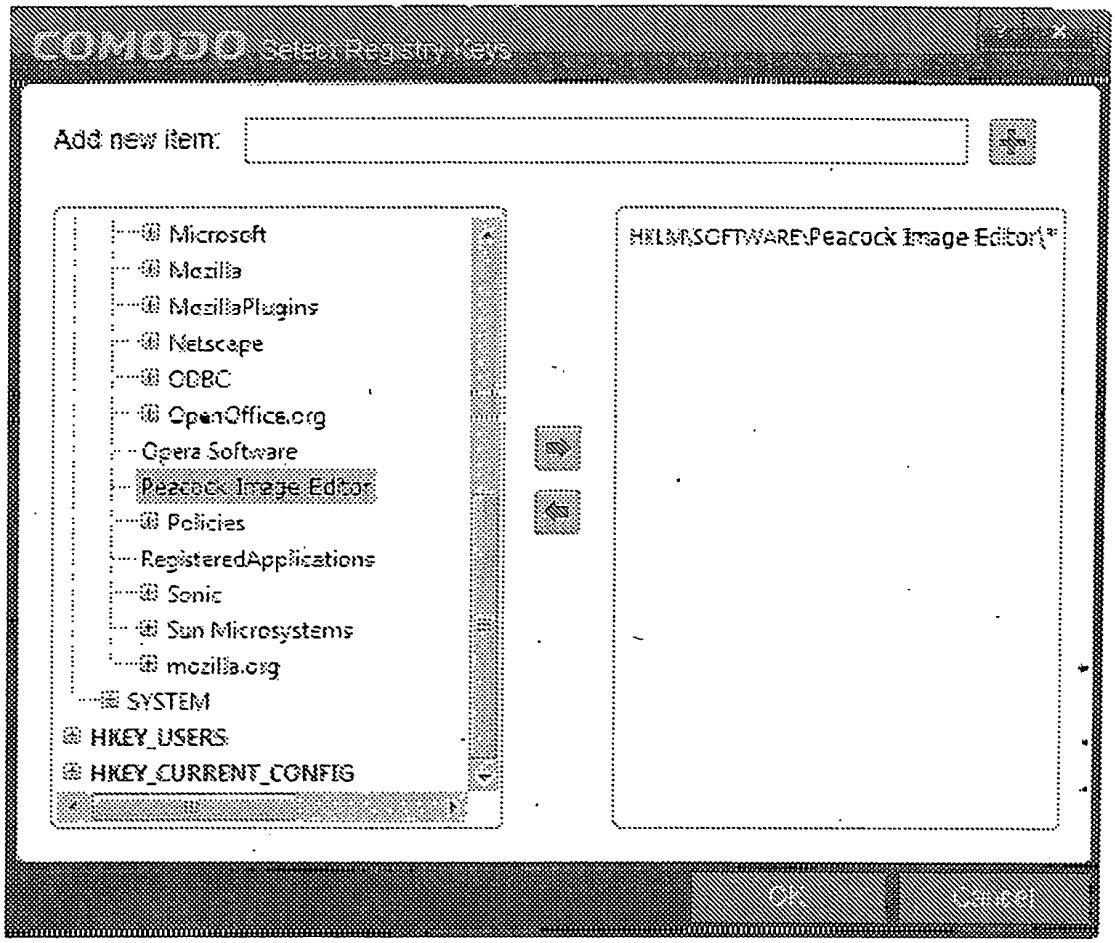
To manually add an individual Registry key or Registry Group

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



You can add the items by following methods:

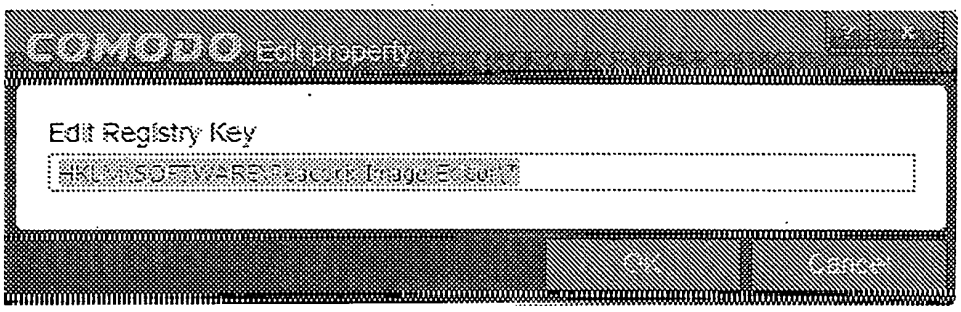
- **Adding Registry Groups** - Selecting Registry Groups allows you to batch select and import predefined groups of important registry keys. Comodo Internet Security provides a default selection of 'Automatic Startup' (keys), 'Comodo Keys', 'Internet Explorer Keys' and 'Important Keys'. For explanations 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.

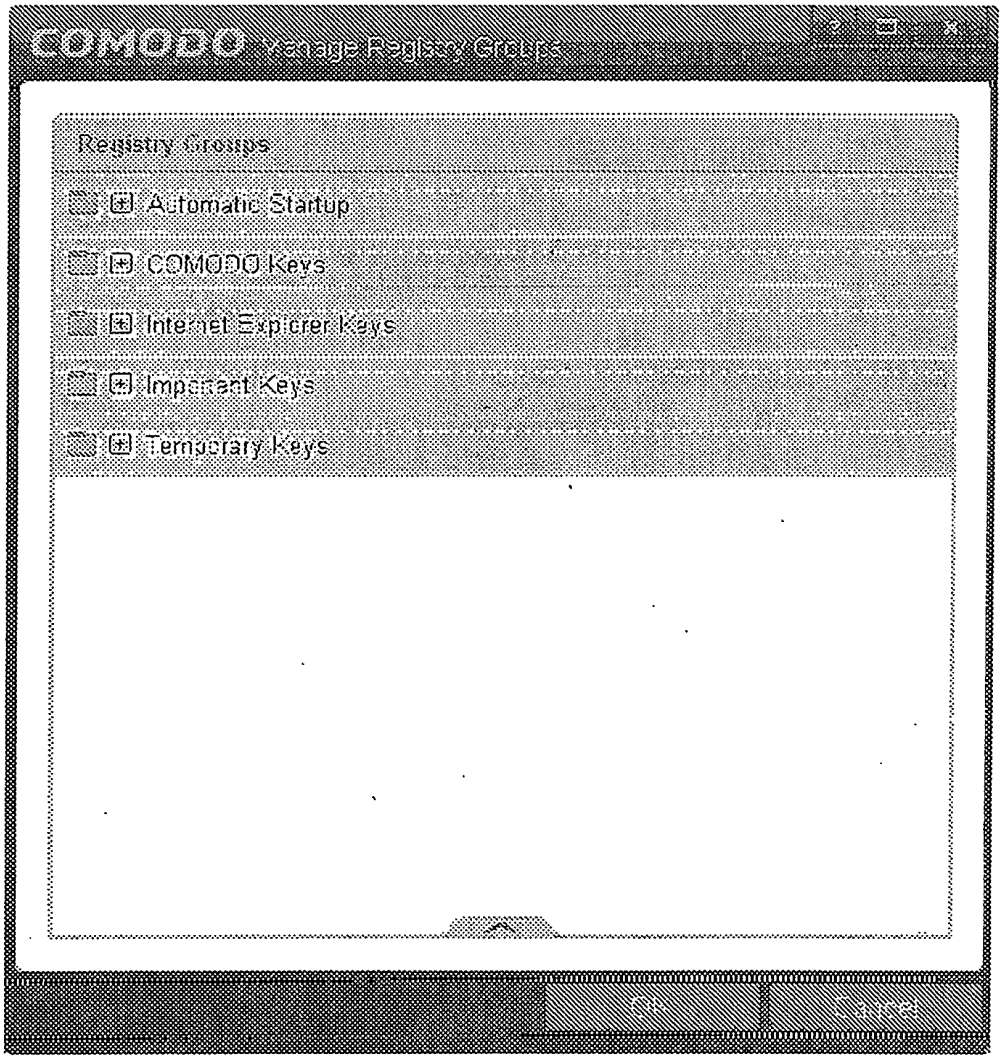
Registry Groups

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'.

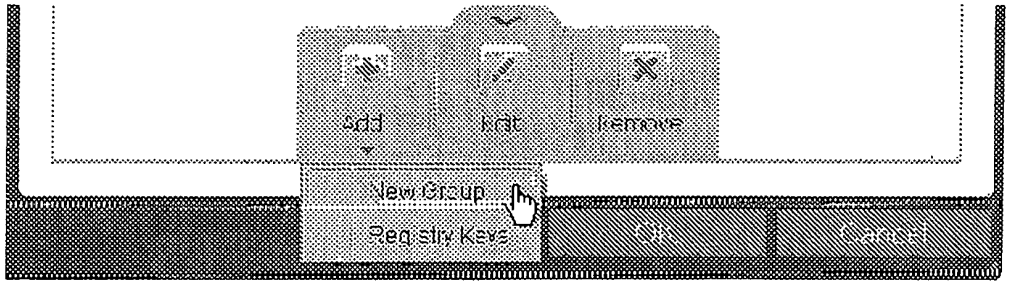
The 'Manage Registry Groups' interface will open.



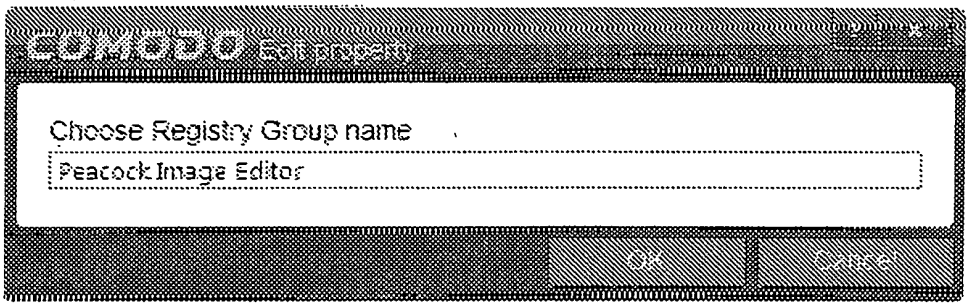
This interface allows you to

- 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

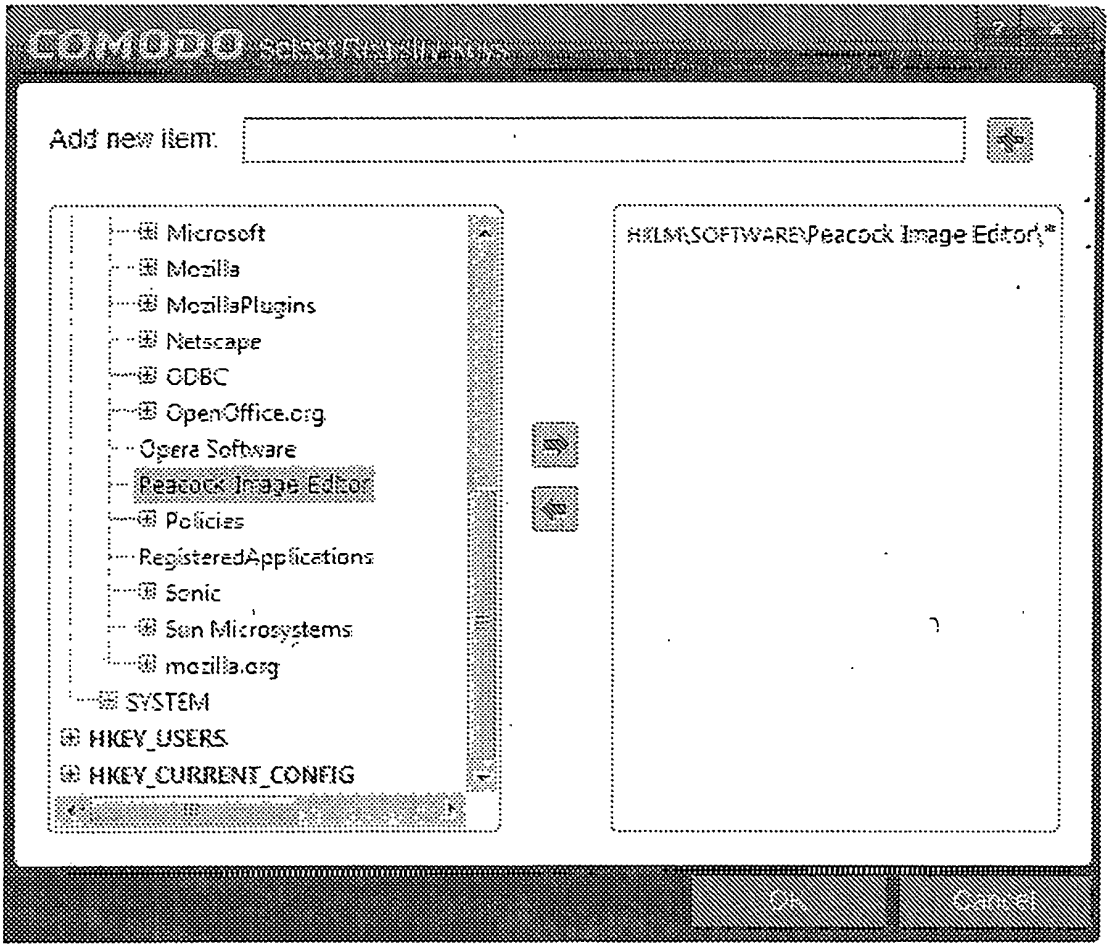
- To add a new group or add key(s) to an existing group, click the handle from the bottom and click 'Add'.



- **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



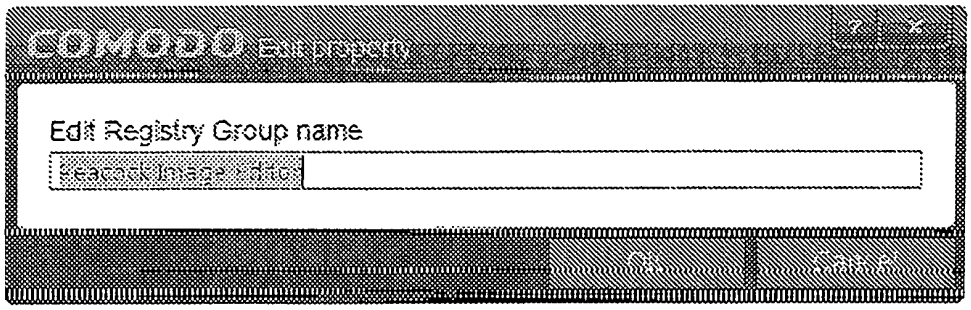
- **Add keys to a group** - Select the Group, click the handle and click Add and choose 'Registry Keys'. The 'Select Registry Keys' dialog will be opened.



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



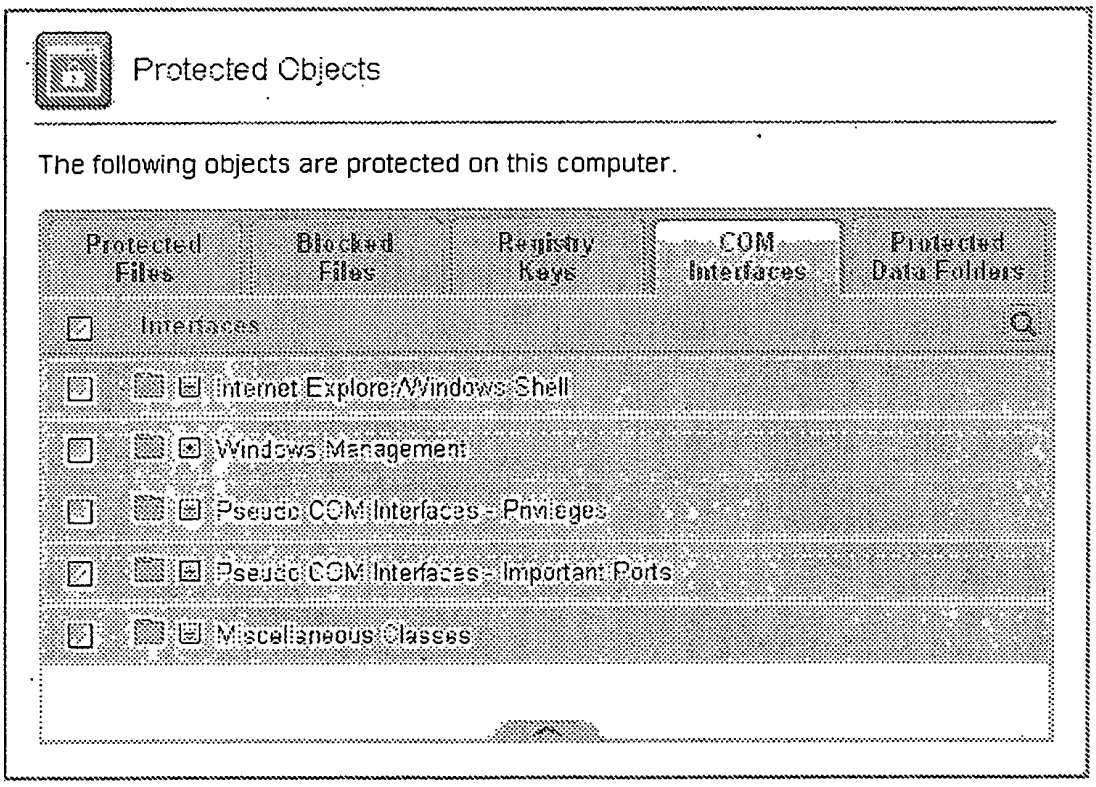
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual file from a group, click + at the left of the group to expand the group, select the key or entry to be removed, click the handle and choose 'Remove'.

6.2.2.4.4. Protected COM interfaces

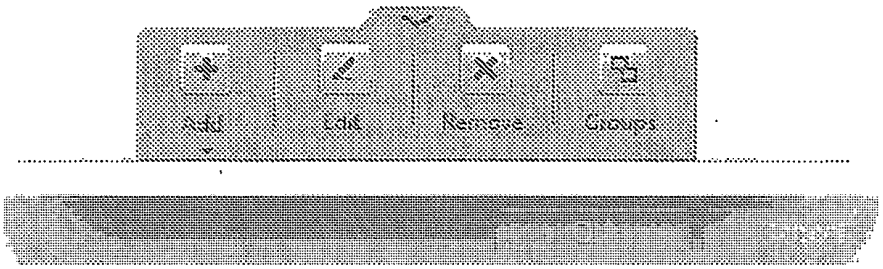
Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate. COM is used as the basis for Active X and OLE - two favorite targets of hackers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

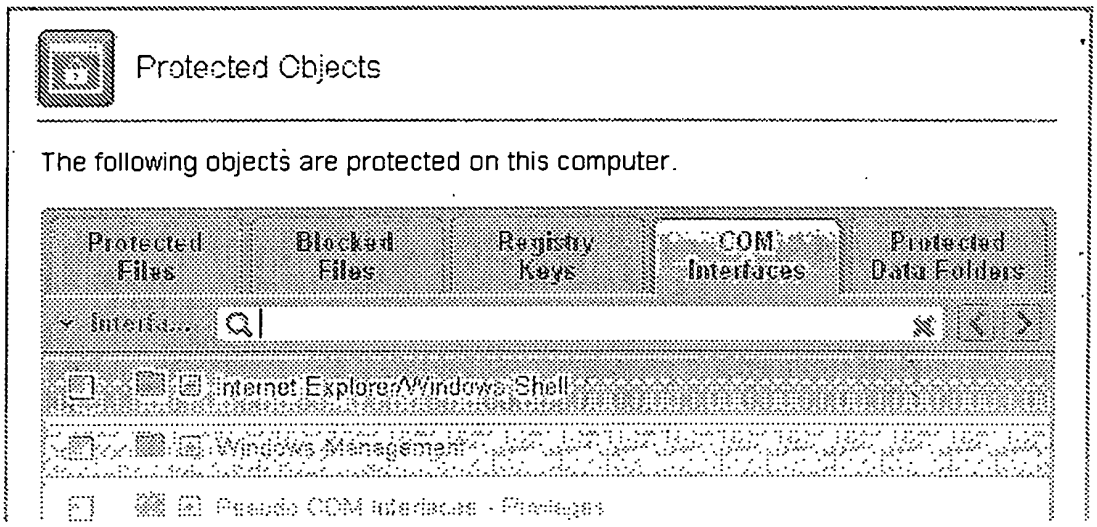


Clicking the handle at the bottom of the interface opens an options panel with the following options:



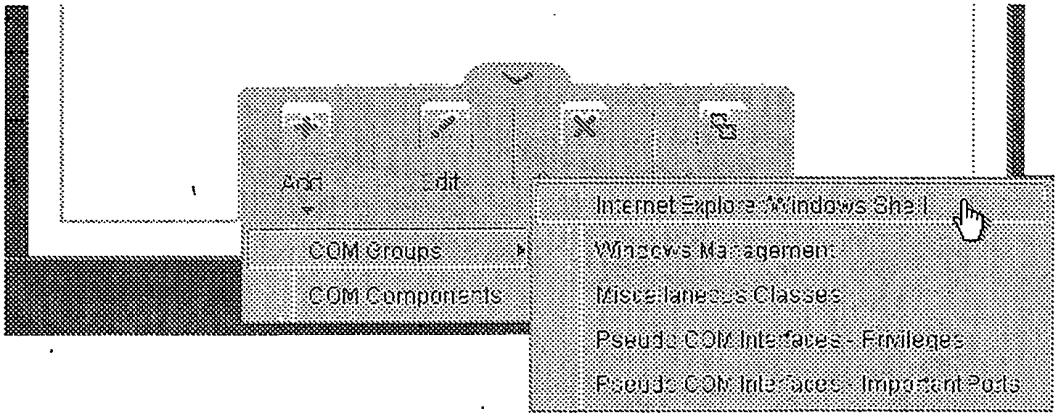
- Add - Allows you to add COM groups or individual COM components to COM Protection list.
- Edit - Allows you to edit the COM Class.
- Remove - Deletes the currently highlighted COM group or individual COM component from the COM Protection list.
- Groups - Opens the Manage COM Groups interface that allows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



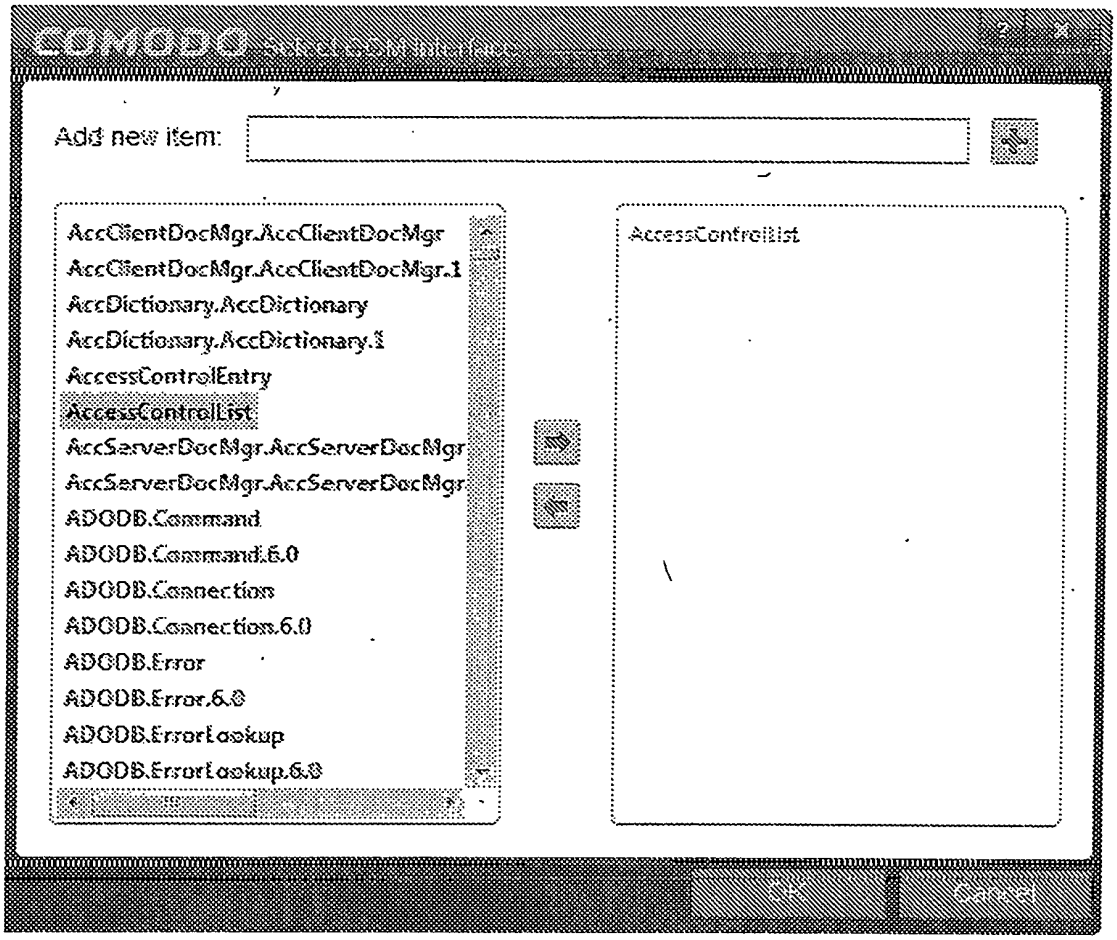
To manually add a COM Group or individual COM component

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



You can add the items by following methods:

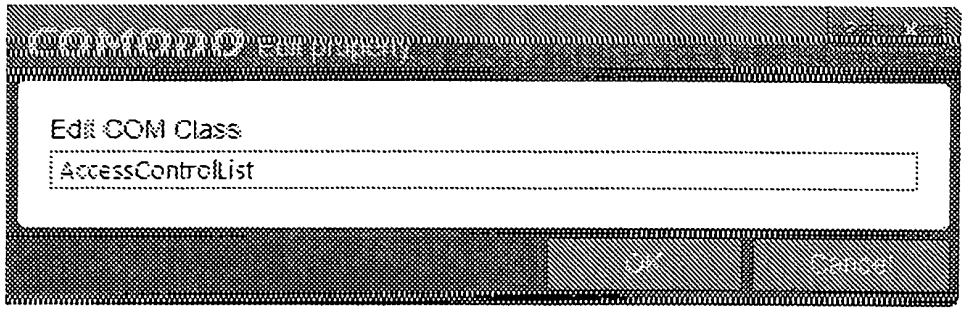
- **Adding COM Groups** - Selecting COM Groups allows you to batch select and import predefined groups of important COM interface components. For explanations on editing existing COM groups and creating new groups refer to the section COM Groups.
- **Adding COM Components** - Selecting 'COM components'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

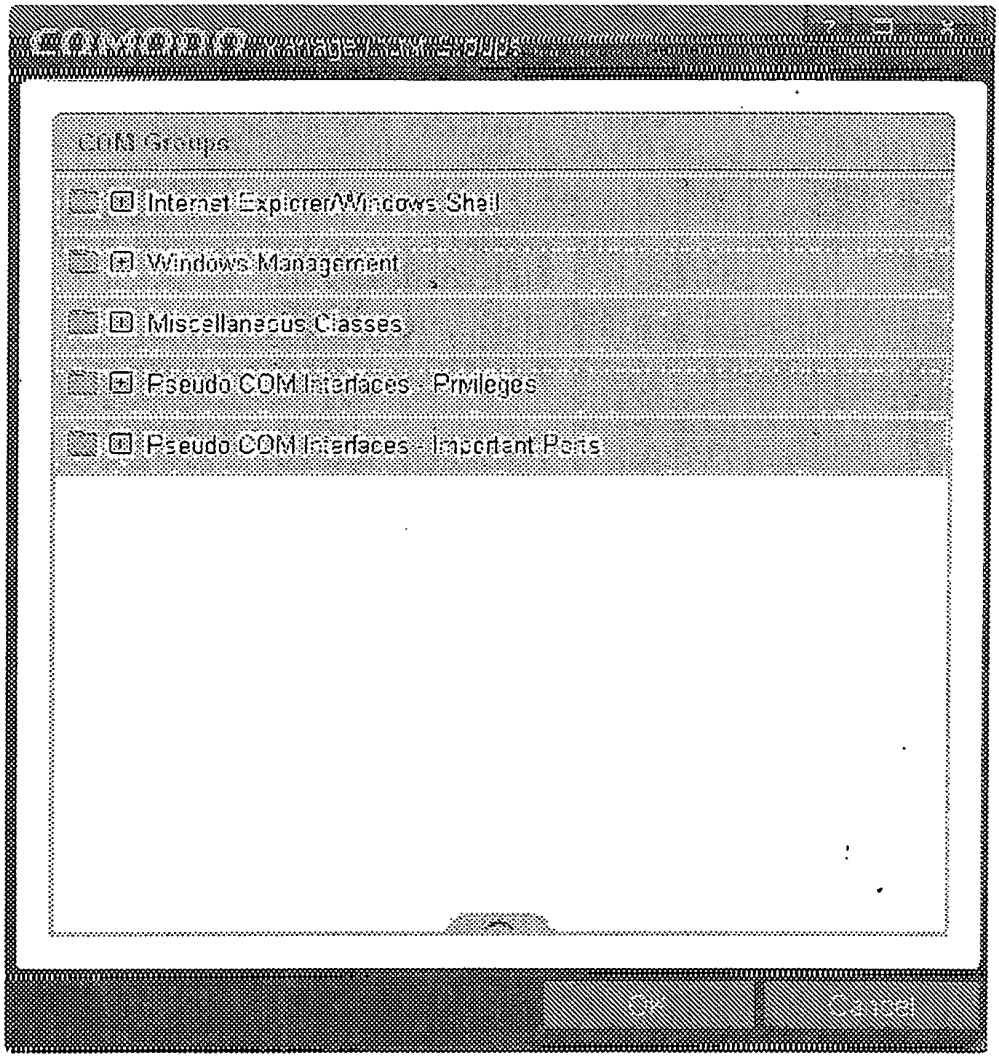
COM Groups

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'.

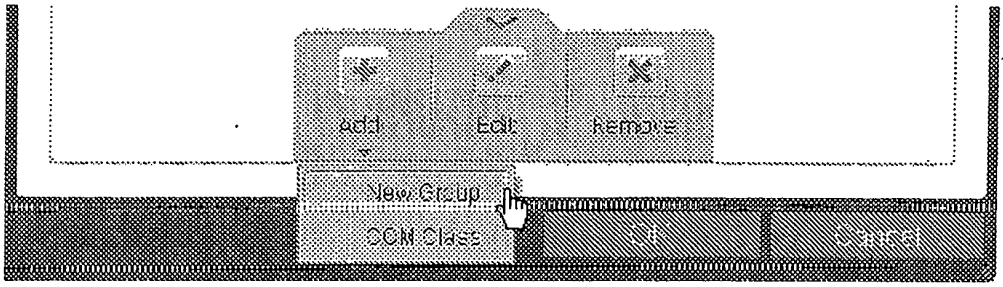
The 'Manage COM Groups' interface will open.



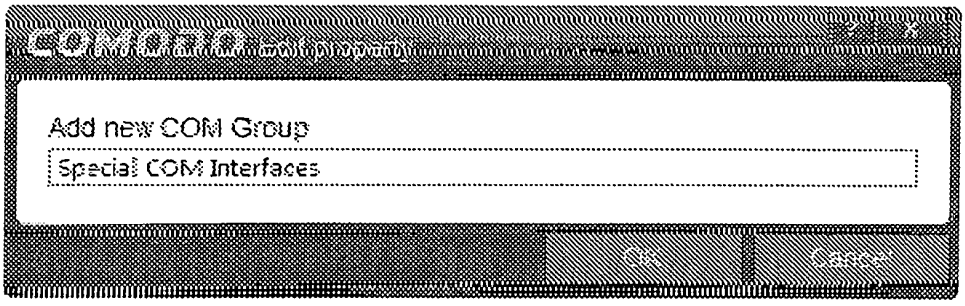
This interface allows you to:

- 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

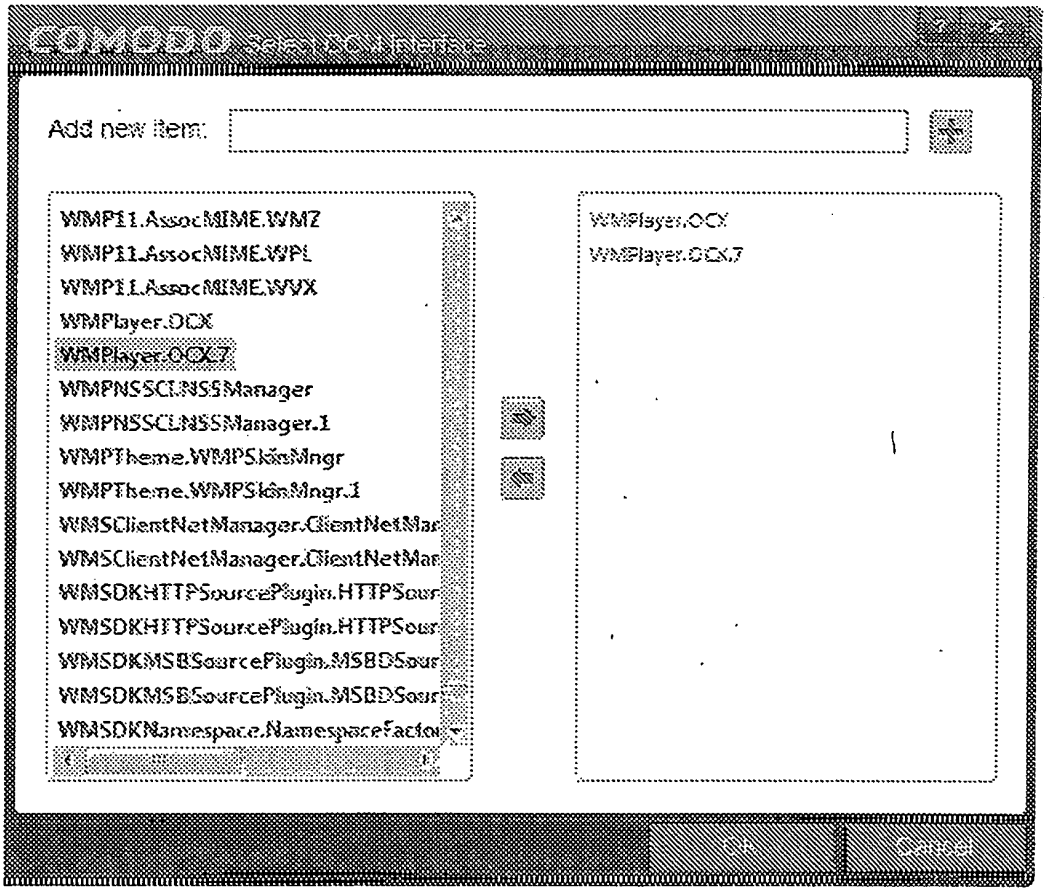
- To add a new group or add new COM Component(s) to an existing group, click the handle from the bottom and click 'Add'.



- **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.



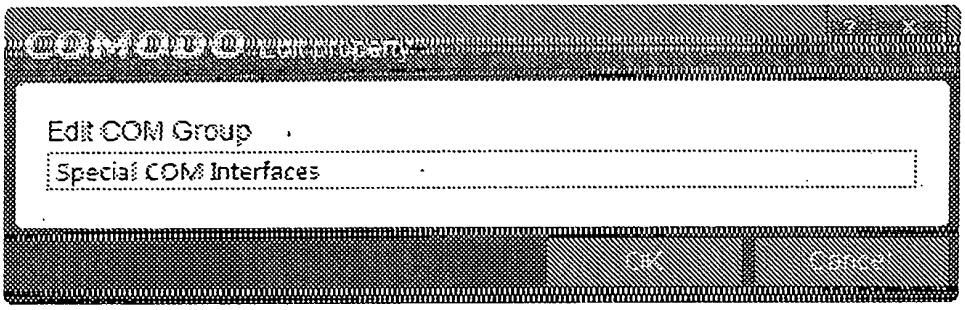
- **Add COM Components to a group** - Select the Group, click the handle and click Add and choose 'COM Class. The 'Select COM Interface' dialog will be opened.



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



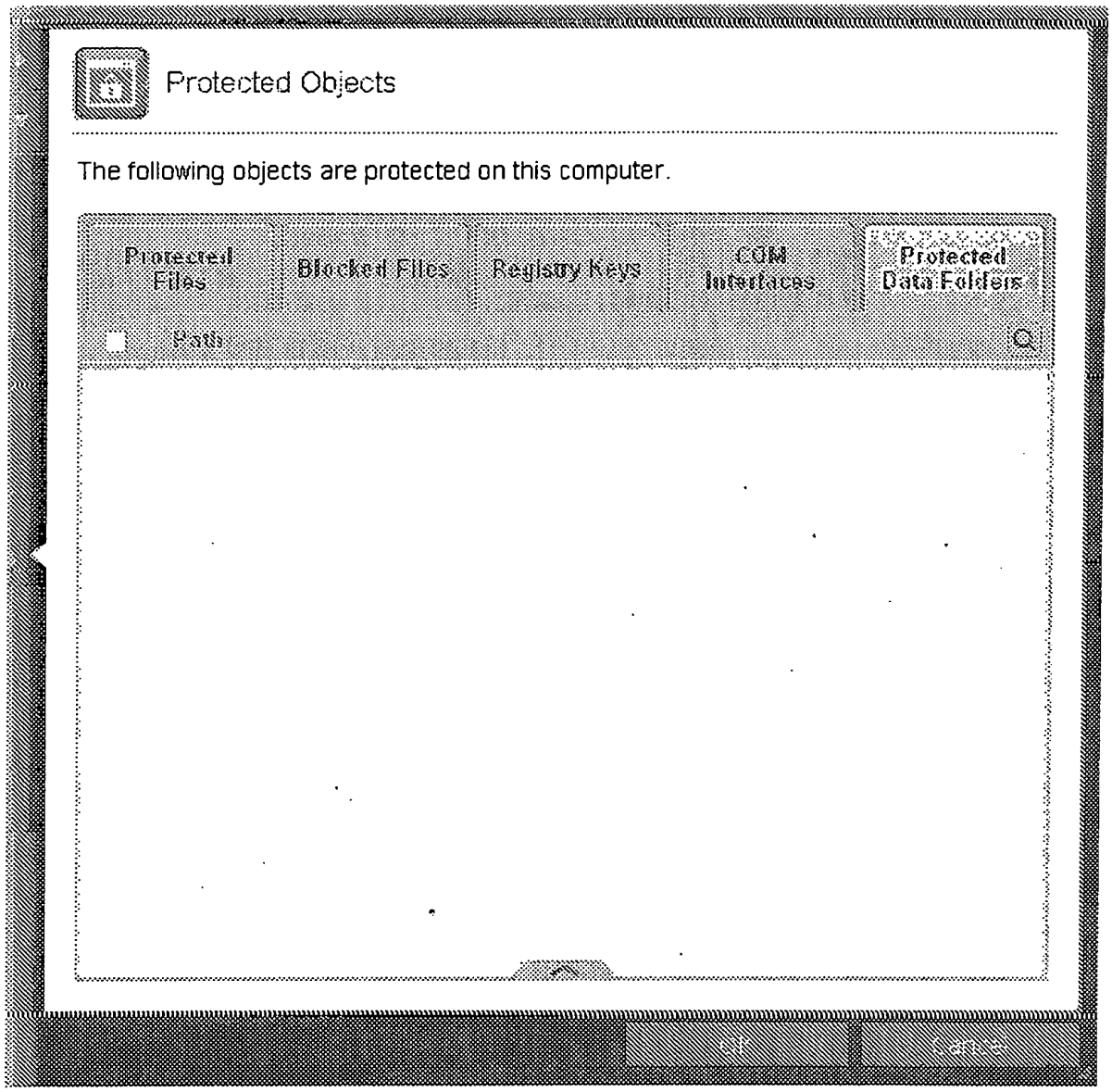
- To remove a group, select the group, click the handle and choose Remove.
- To remove an individual COM Component from a group, click + at the left of the group to expand the group, select the item to be removed, click the handle and choose 'Remove'.

6.2.2.4.5. Protected Data Folders

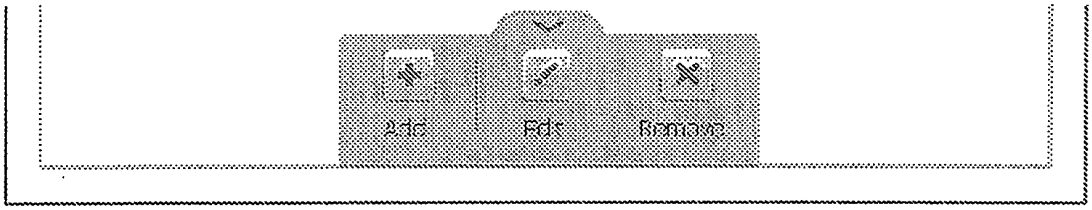
The data files in the folders listed under the Protected Data Folders area cannot be seen, accessed or modified by any known or unknown application that is running inside the sandbox.

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:

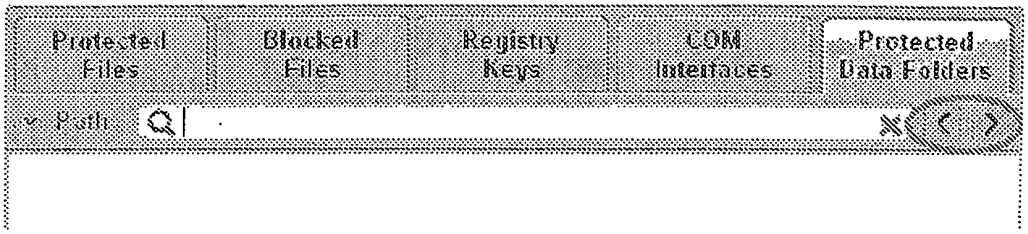


Clicking the handle at the bottom of the interface opens an options panel with the following options:



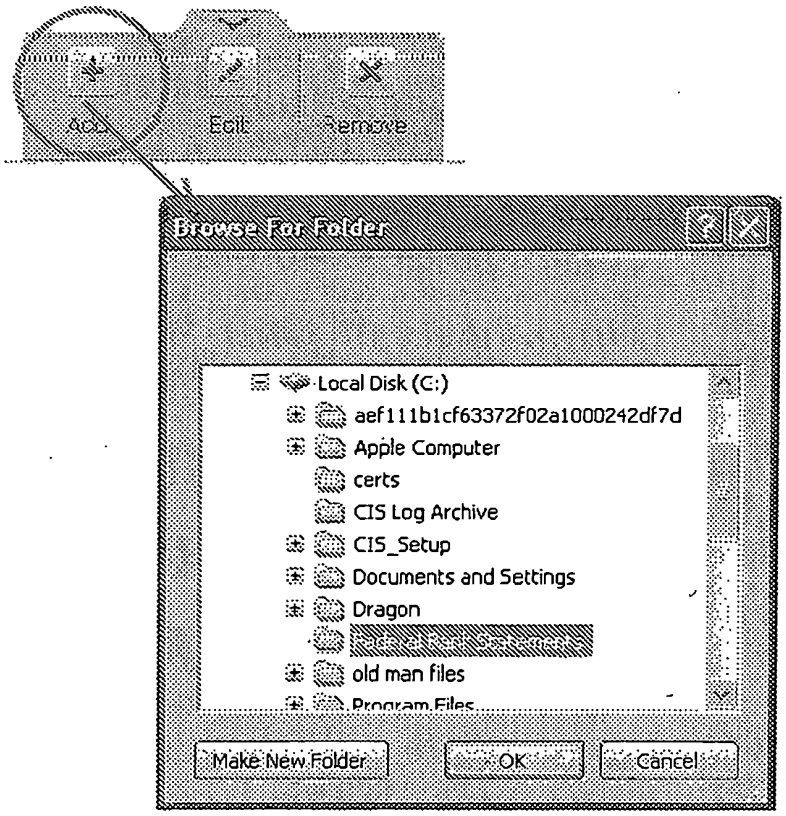
- Add - Allows you to add folders to Protected Data Folders list.
- Edit - Allows you to edit the path of the added folders.
- Remove - Deletes the currently selected folder.

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.

