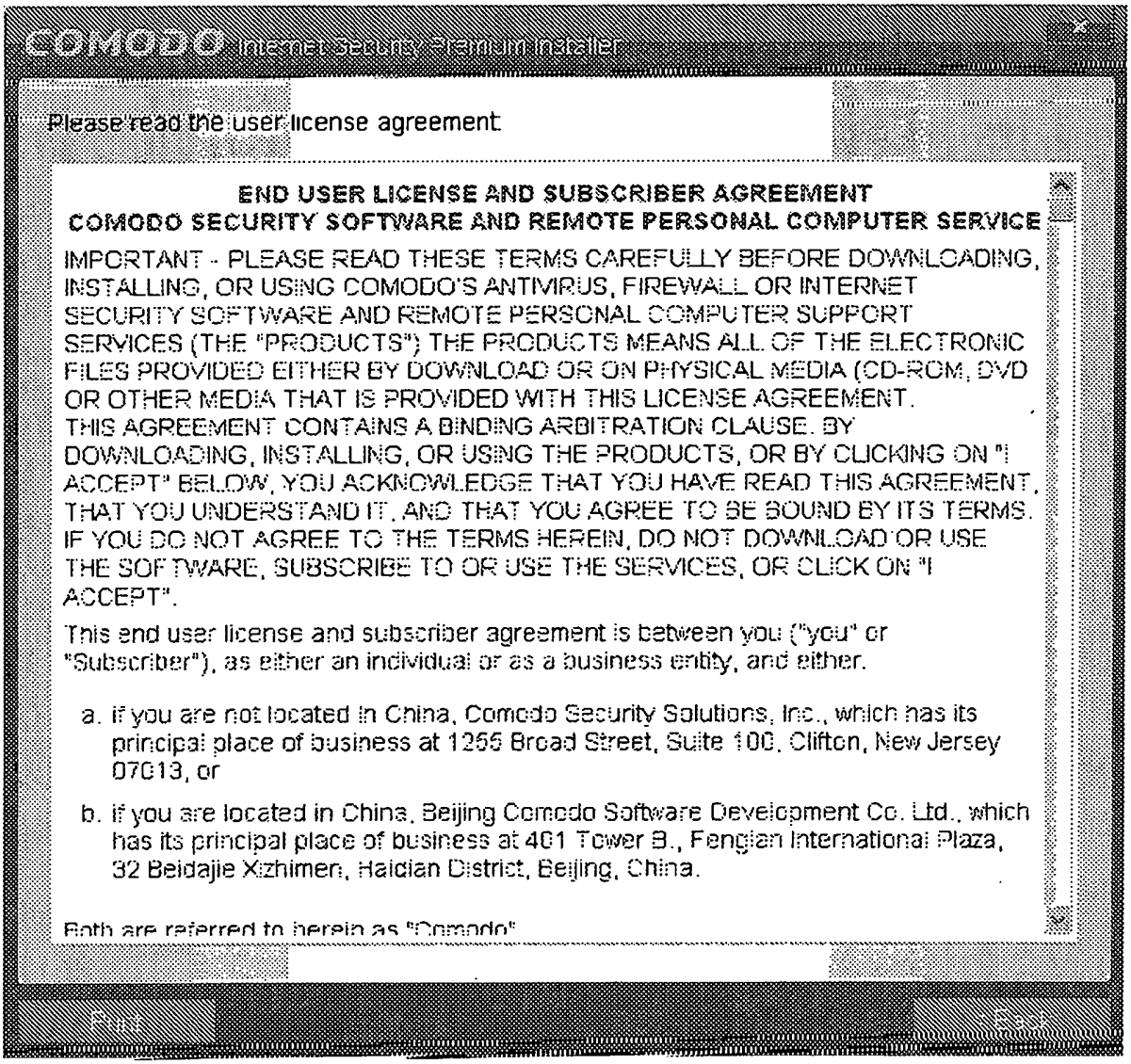
**Browser Homepage**

Your default home page and search engine will be set to Yahoo!

- Please review and/or modify the settings in the dialog.

**End User License Agreements**

- Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.




After reading the agreements, click the 'Back' button to return to the installation configuration screen.

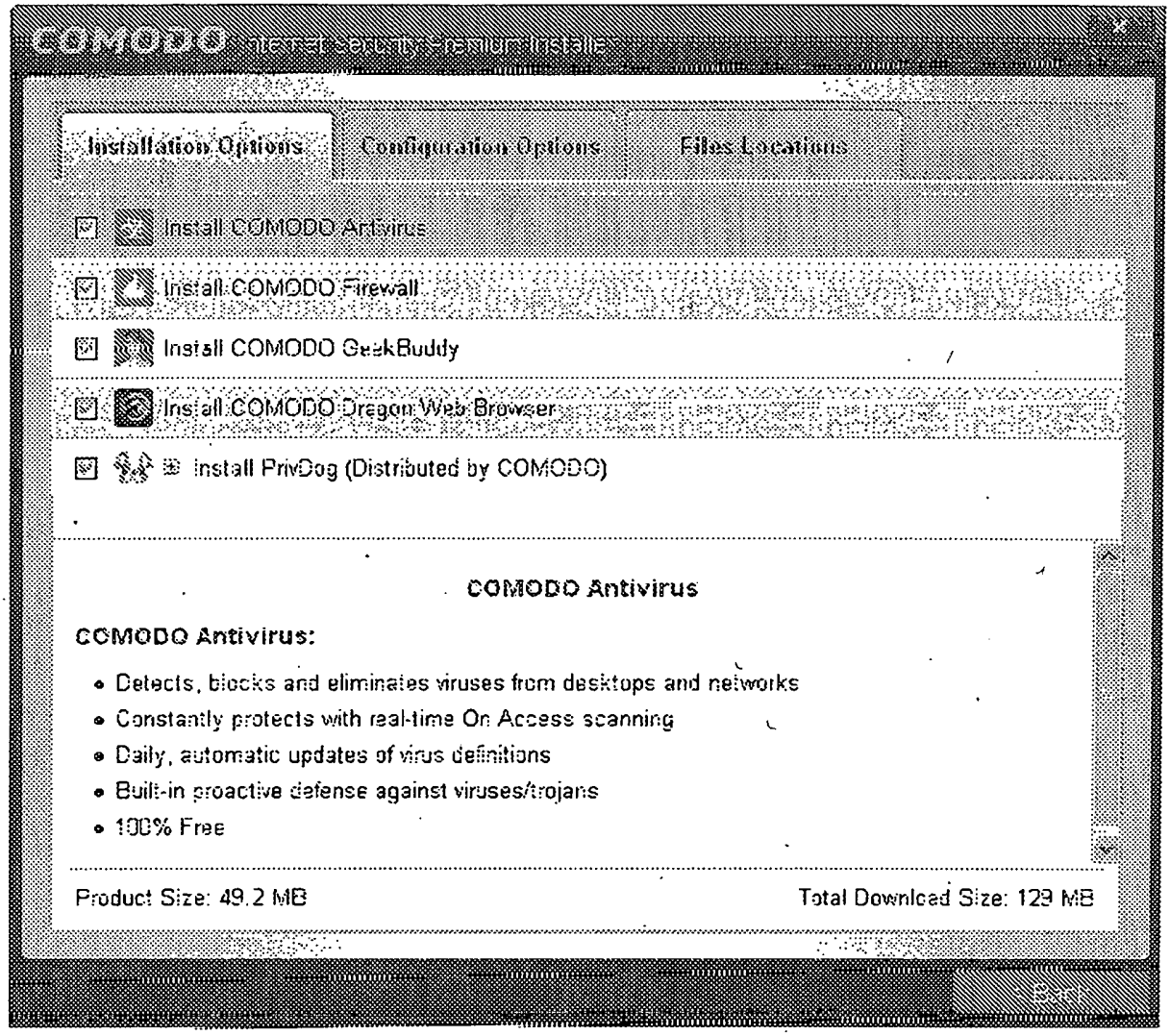
Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installation'. Otherwise, click 'Agree and Install' to begin installation.

## Customizing Installation

Clicking the 'Customize Installation' link opens an advanced options interface that enables you to choose which elements you would like to install, configure security popup alerts and choose the installation path. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select all the components to get the full benefit of the product.

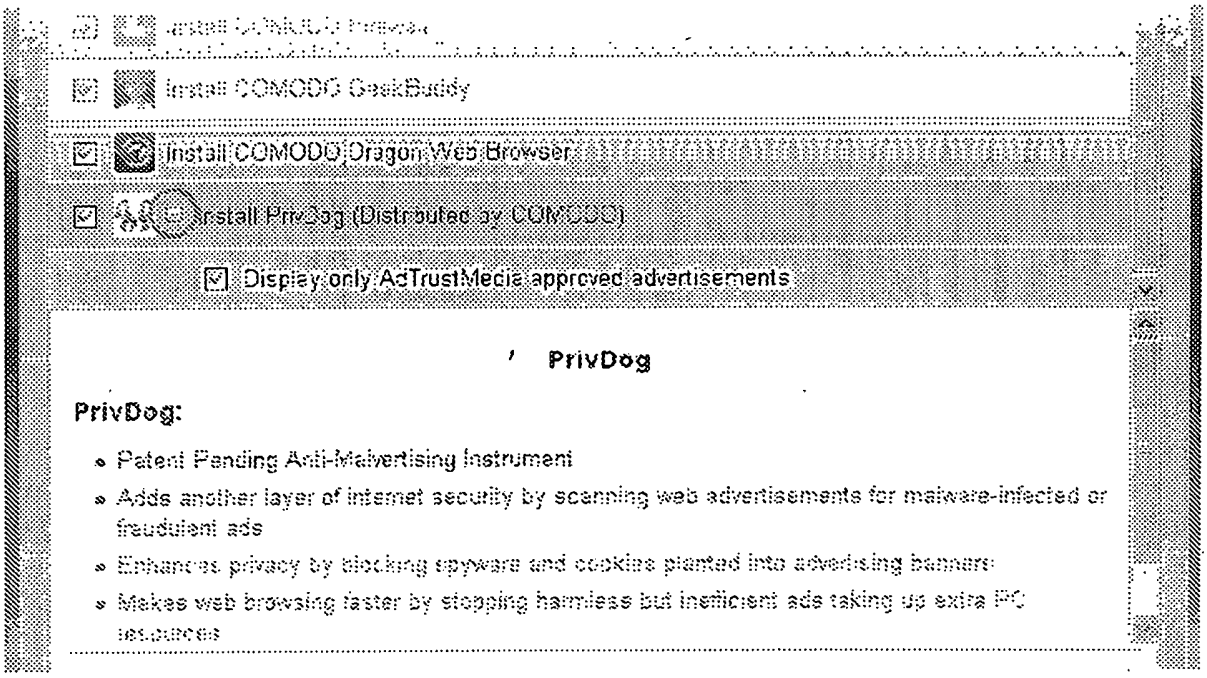
**Select Components to Install** (Click to go back to Step 2)

Click the 'Installation Options' tab to select the components to be installed.




- **Install COMODO Firewall** - Selecting this option installs Comodo Firewall and Defense+ components. Deselect this option, if you already have third party Firewall protection activated in your computer system. Comodo Firewall installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO Antivirus** - Selecting this option installs Comodo Antivirus and Defense+ components. Deselect this option, if you already have a third party virus protection activated in your computer system. Comodo Antivirus installation is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- **Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.
- **Install PrivDog** - PrivDog is a browser extension that improves the transparency, privacy and speed of your online experience by automatically detecting and blocking processes that are attempting to track your online activity. Whenever you visit a website, PrivDog will display the number of privacy threats it has blocked in the top-right corner of your browser. Clicking the PrivDog icon will reveal a more detailed breakdown of the types of threats it has stopped, which can include advertising networks, 3rd party trackers, cookies, widgets and other data collection processes. The extension can also block all current banner ads in a webpage and replace them with safe and trusted ads. If you elect to install PrivDog, the extension will be automatically installed in any supported browsers detected on your system (Comodo Dragon, Comodo IceDragon, Google Chrome and Mozilla Firefox). You can remove the extension at any time from within the browser itself. Refer to the section Introduction to PrivDog for more details.

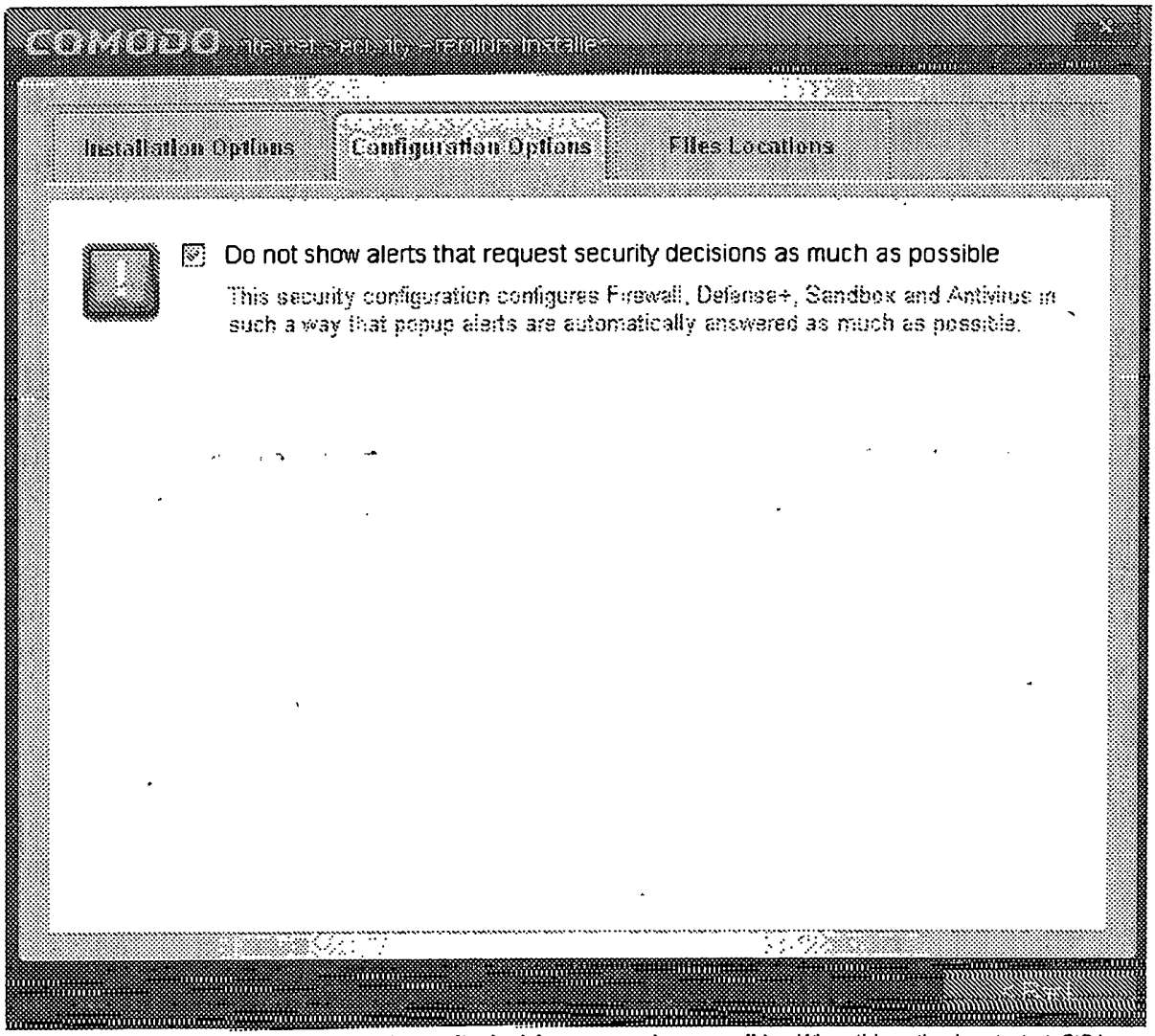
- Select the checkbox 'Install PrivDog' if you want to install PrivDog.




- Click the '+' button beside 'Install PrivDog' and select the 'Display only AdTrustMedia approved advertisements' checkbox, if you choose to view only ads from AdTrustMedia in your browser.

**Configuration Options**

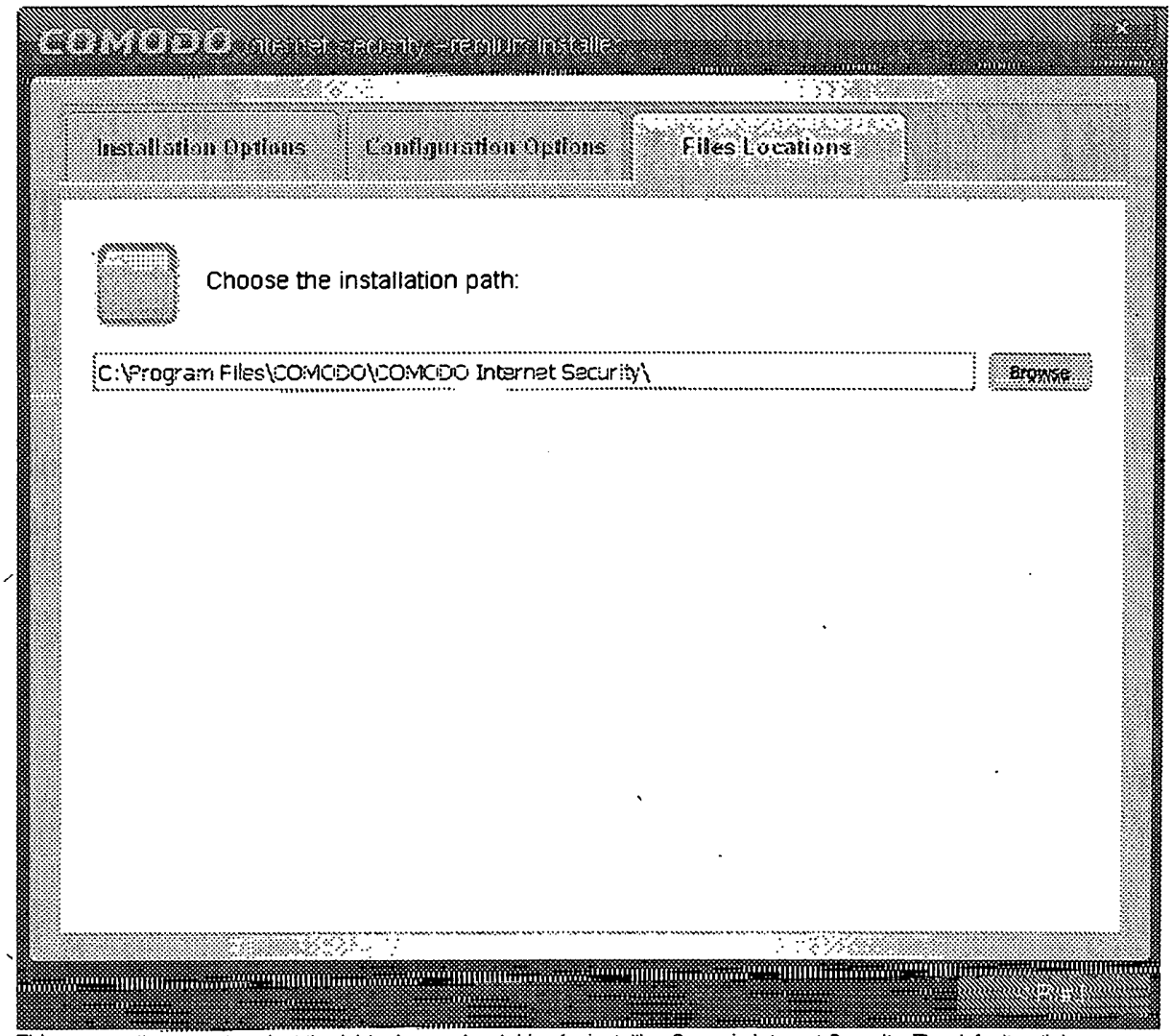
- Click the 'Configuration Options' tab to configure pop-up alert options.




- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

### Choosing Installation Location

Click the 'Files Locations' tab to choose the installation path.



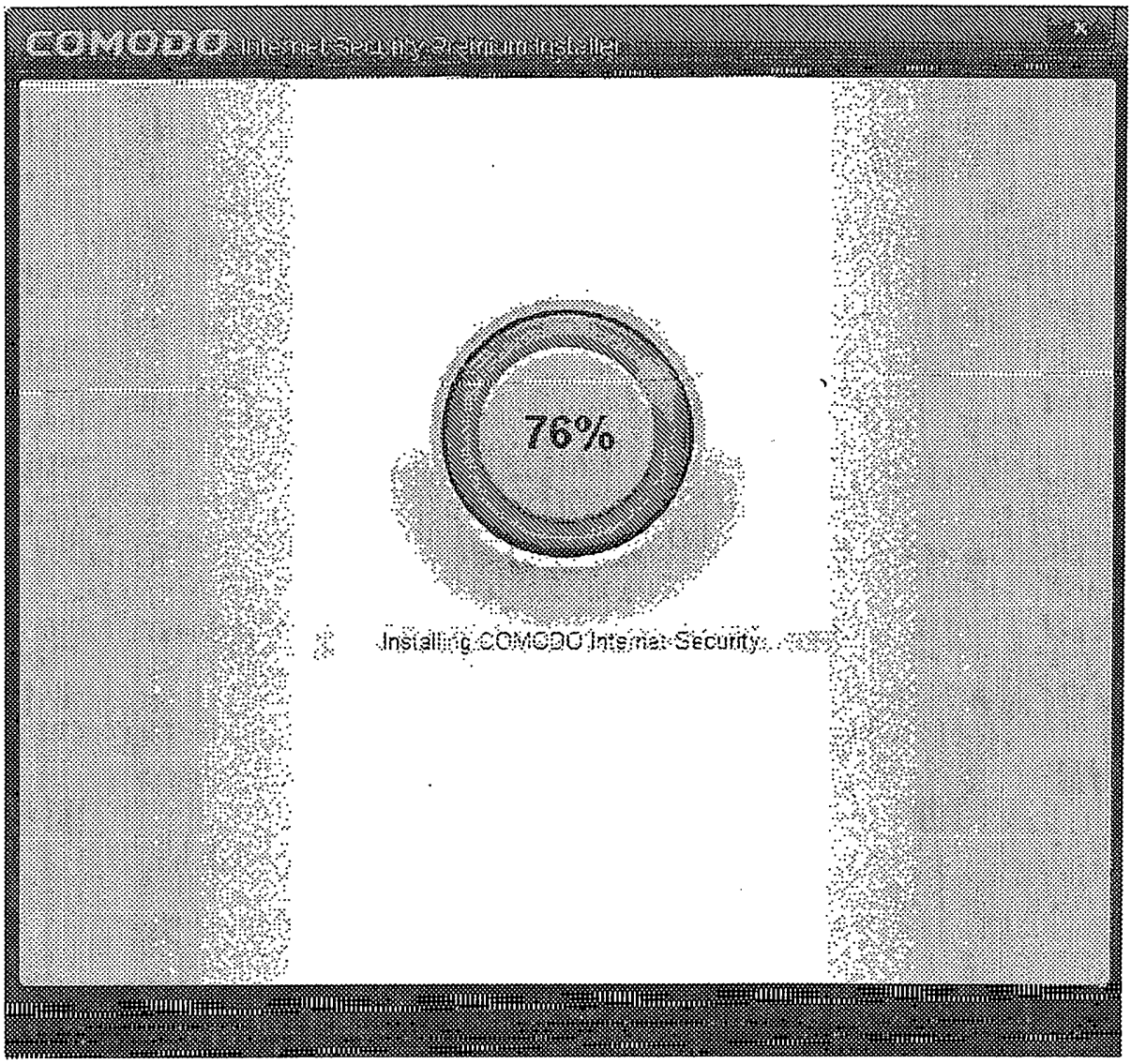

This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

After customizing your installation, click the 'Back' button to return to the installation configuration screen.

- Once you are satisfied with your settings, click 'Agree and Install' to begin installation (Click to go back to Step 2).

**Step 3 - Installation Progress**

The installation progress will be displayed...



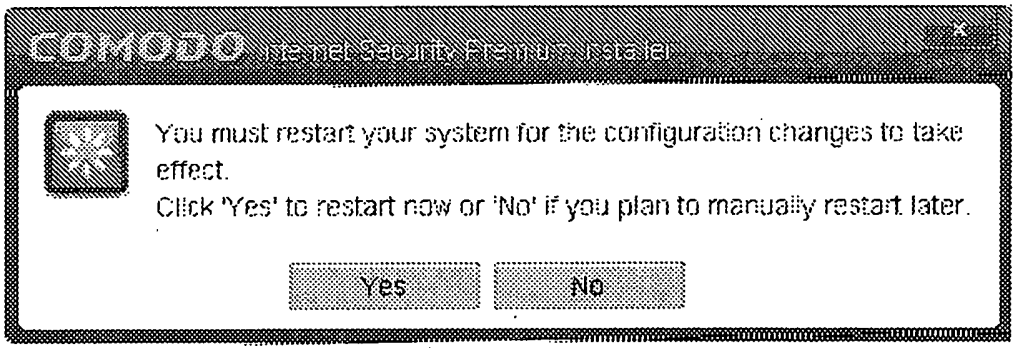

...and on completion, the successfully completed dialog will be displayed.




- Click the 'Close' button.

**Step 4 - Restarting Your System**

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

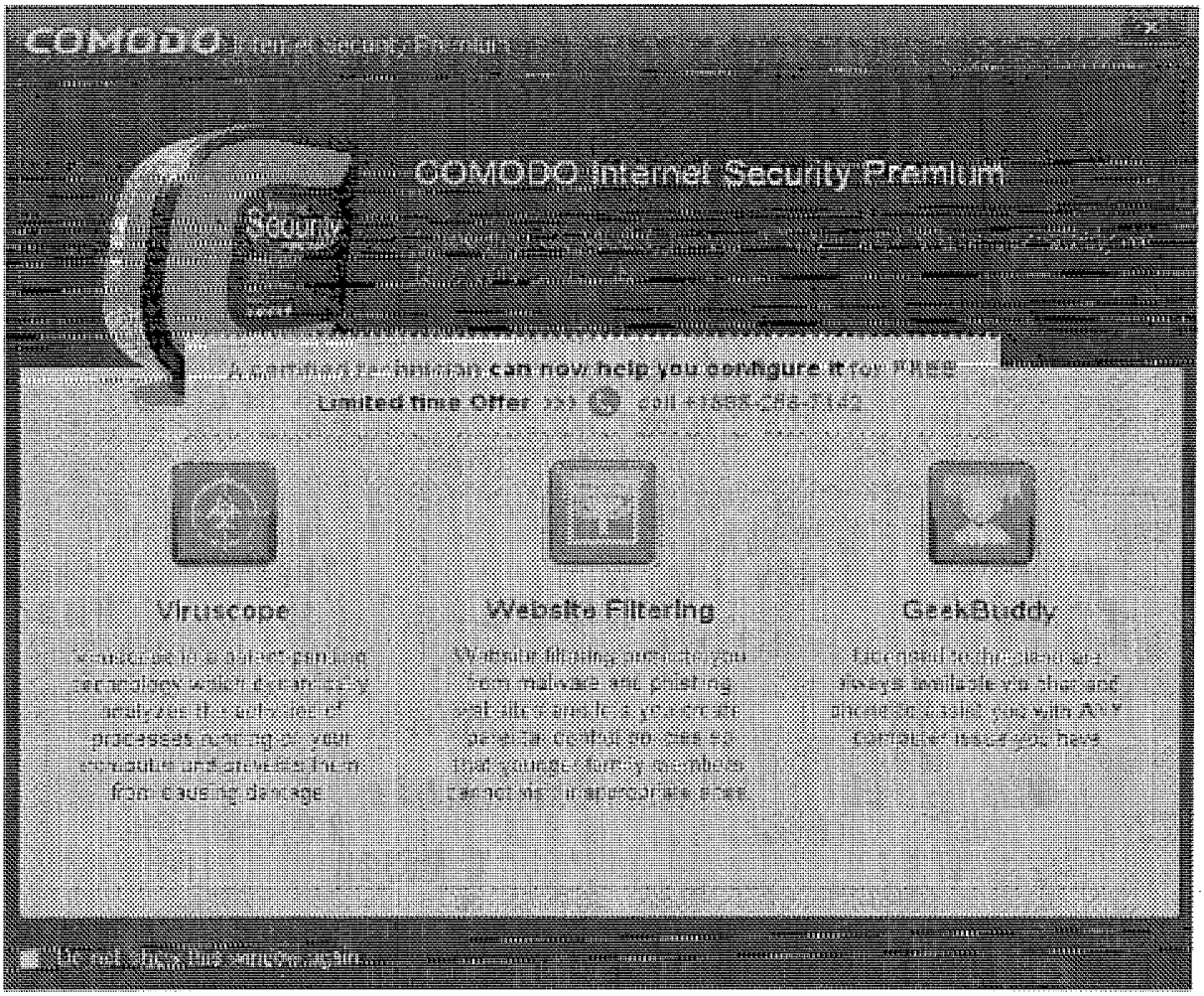



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

**Step 5 - After Restarting Your System**

After restarting, a 'thankyou' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice.




This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

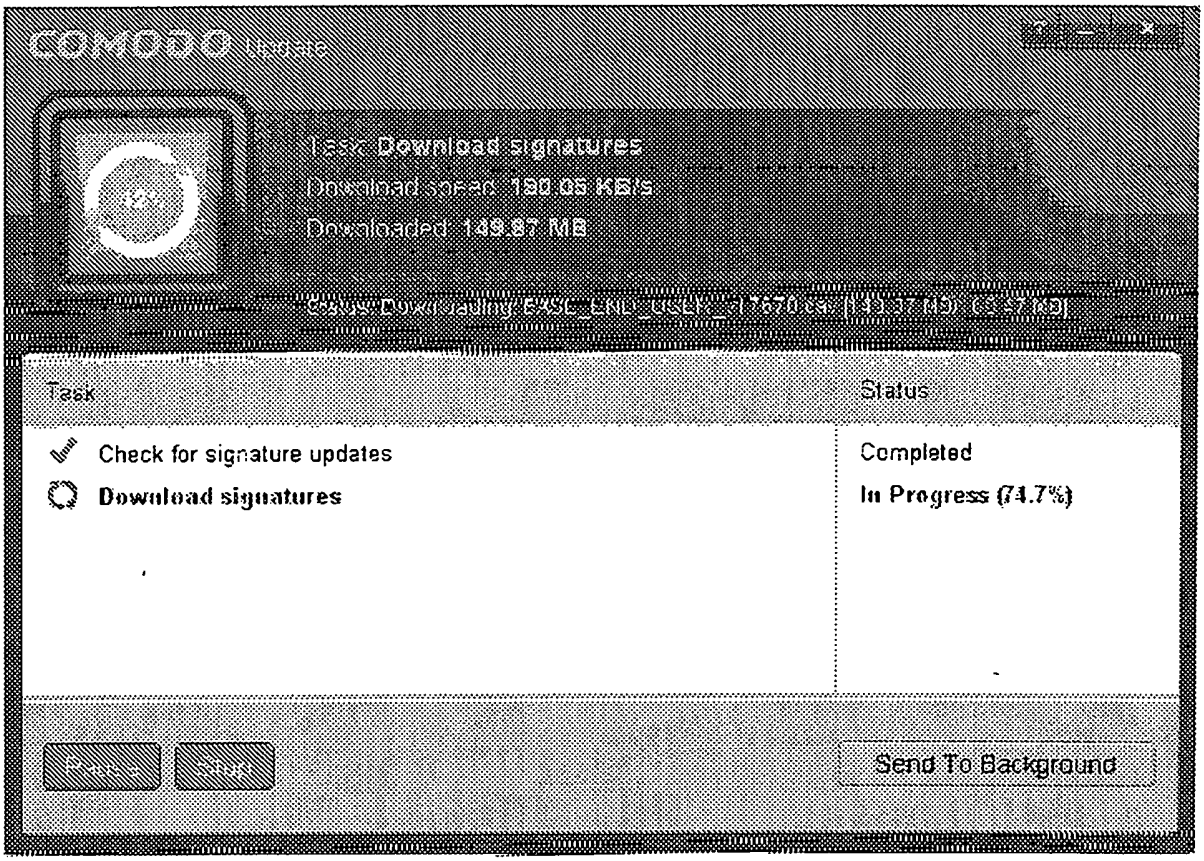



- Select your location from the three options above
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

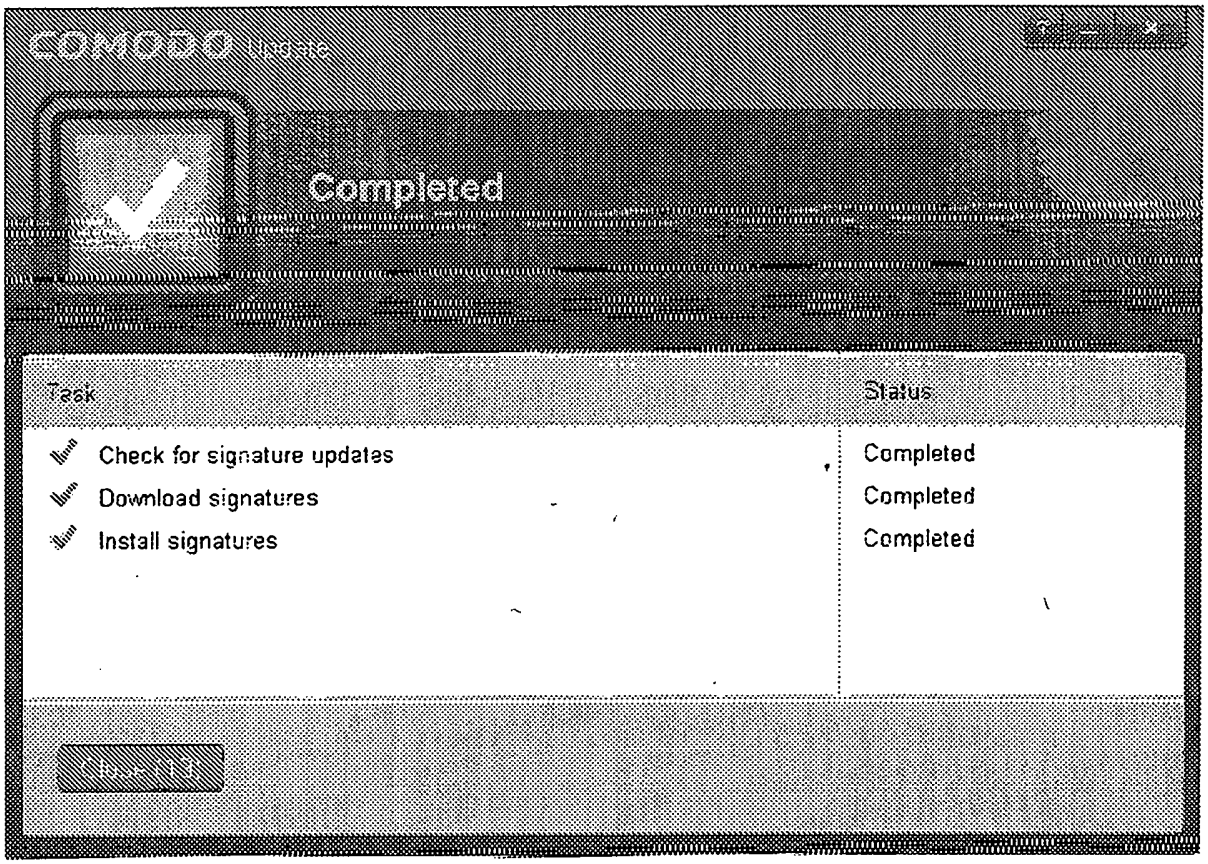
The CIS interface will open.



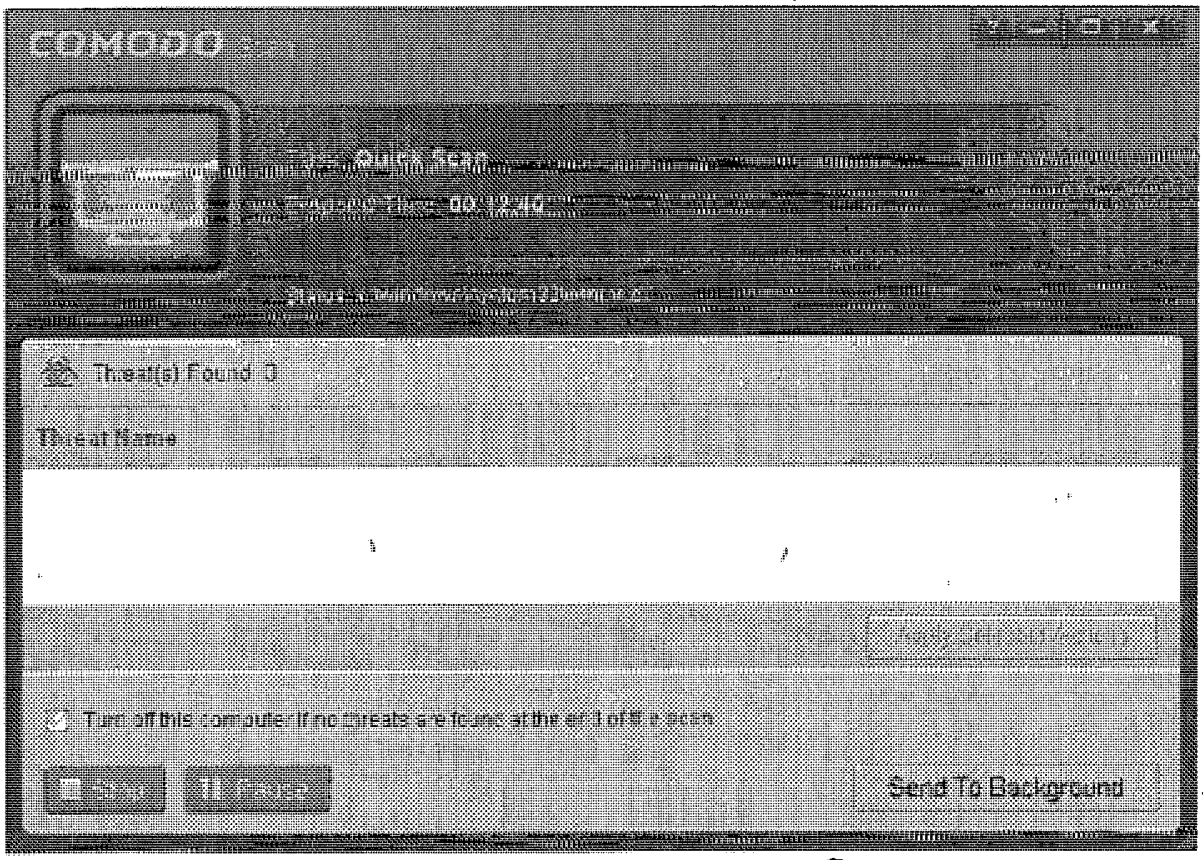

The virus database will be updated automatically for the first time after installation.




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

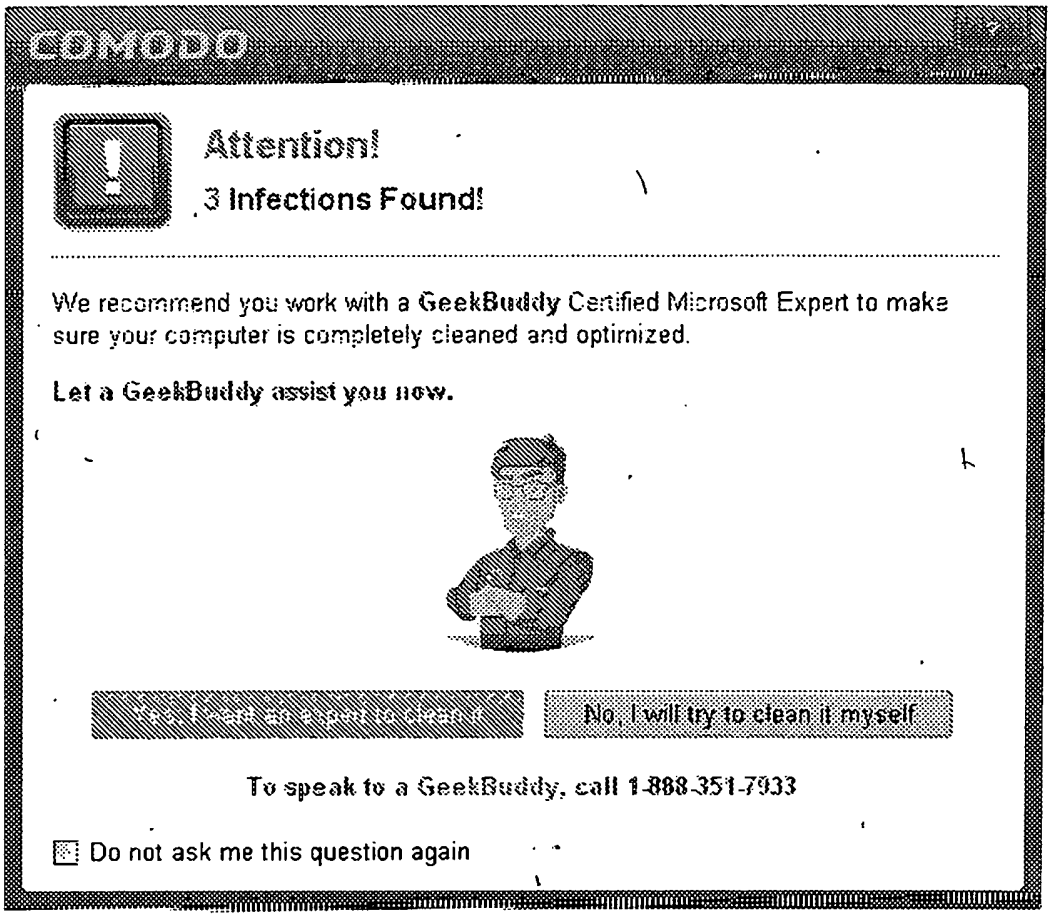



CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



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

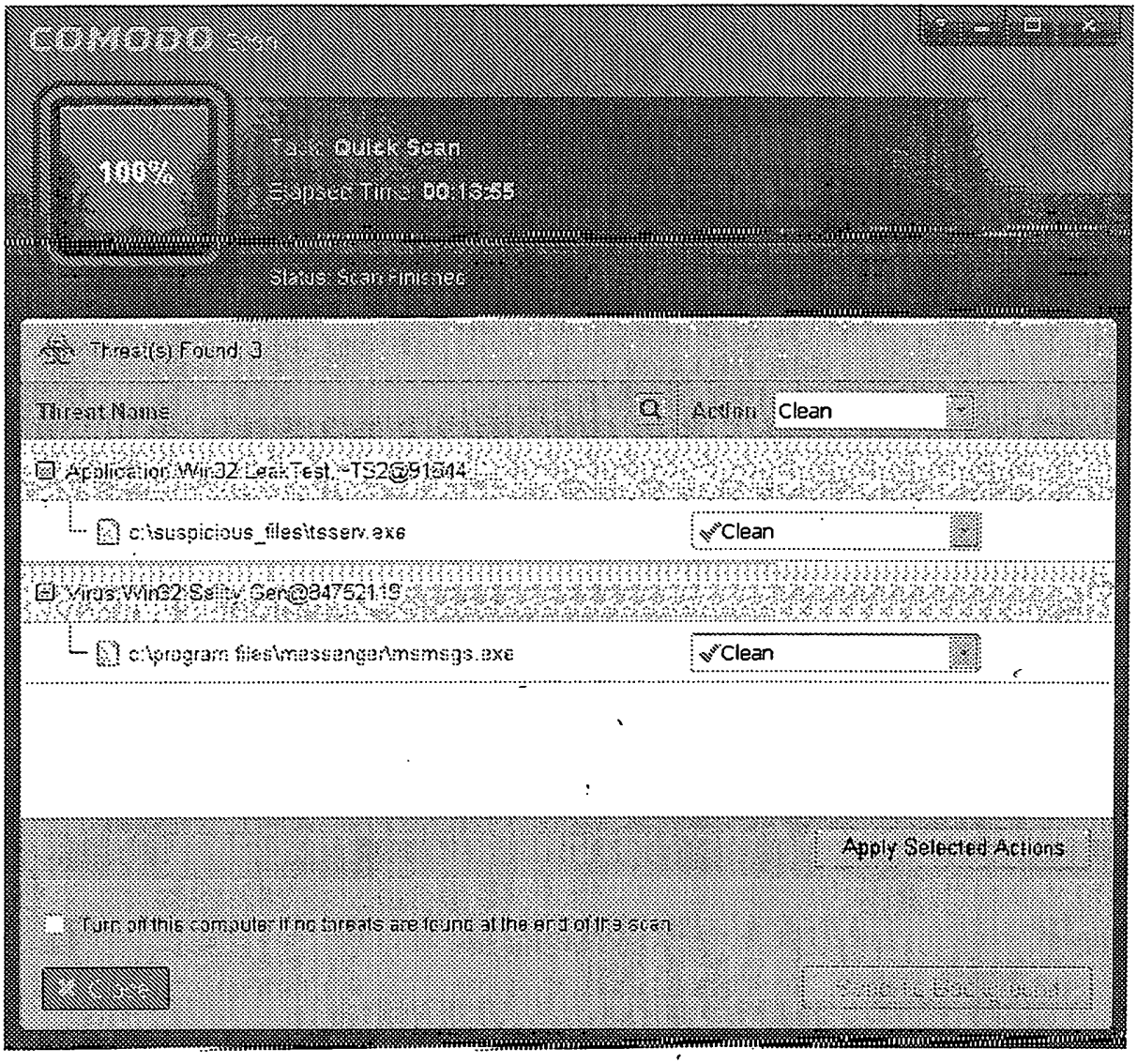
After the scanning is complete, and any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.




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

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

- If you wish to clean the infections yourself, select 'No, I will try to clean it myself'. The scan results screen will be displayed. The results will contain a list of files identified with threats or infections (Viruses, Rootkits, Malware and so on) and provide you the options for cleaning. An example results screen is shown below:




If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section 'Processing Infected Files' for more details.

## 1.3.2. CIS Pro - Installation and Activation

Note - Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. Click here to read the full note.

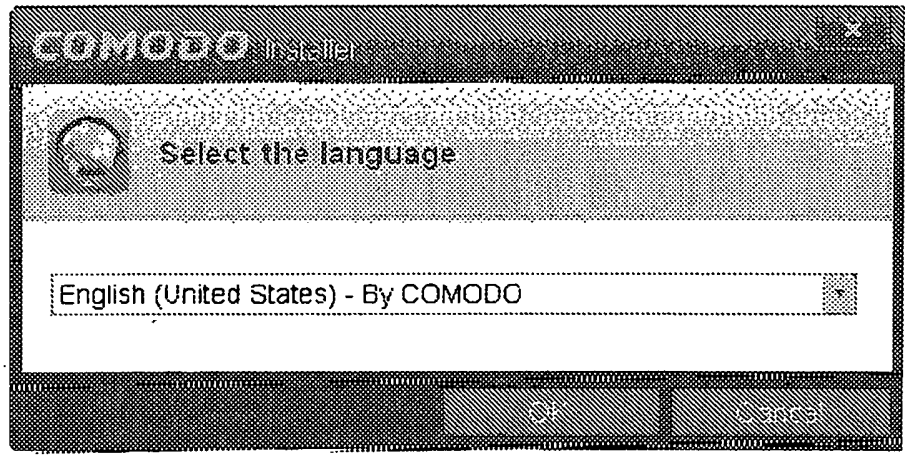
Comodo Internet Security Pro can be downloaded from http://www.comodo.com/home/download/download.php?prod=cis-pro after signing up for subscription and includes, Comodo Dragon, GeekBuddy and the Comodo Guarantee.

- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or 64 bit setup files.

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

**Step 1 - Choosing the Interface Language**

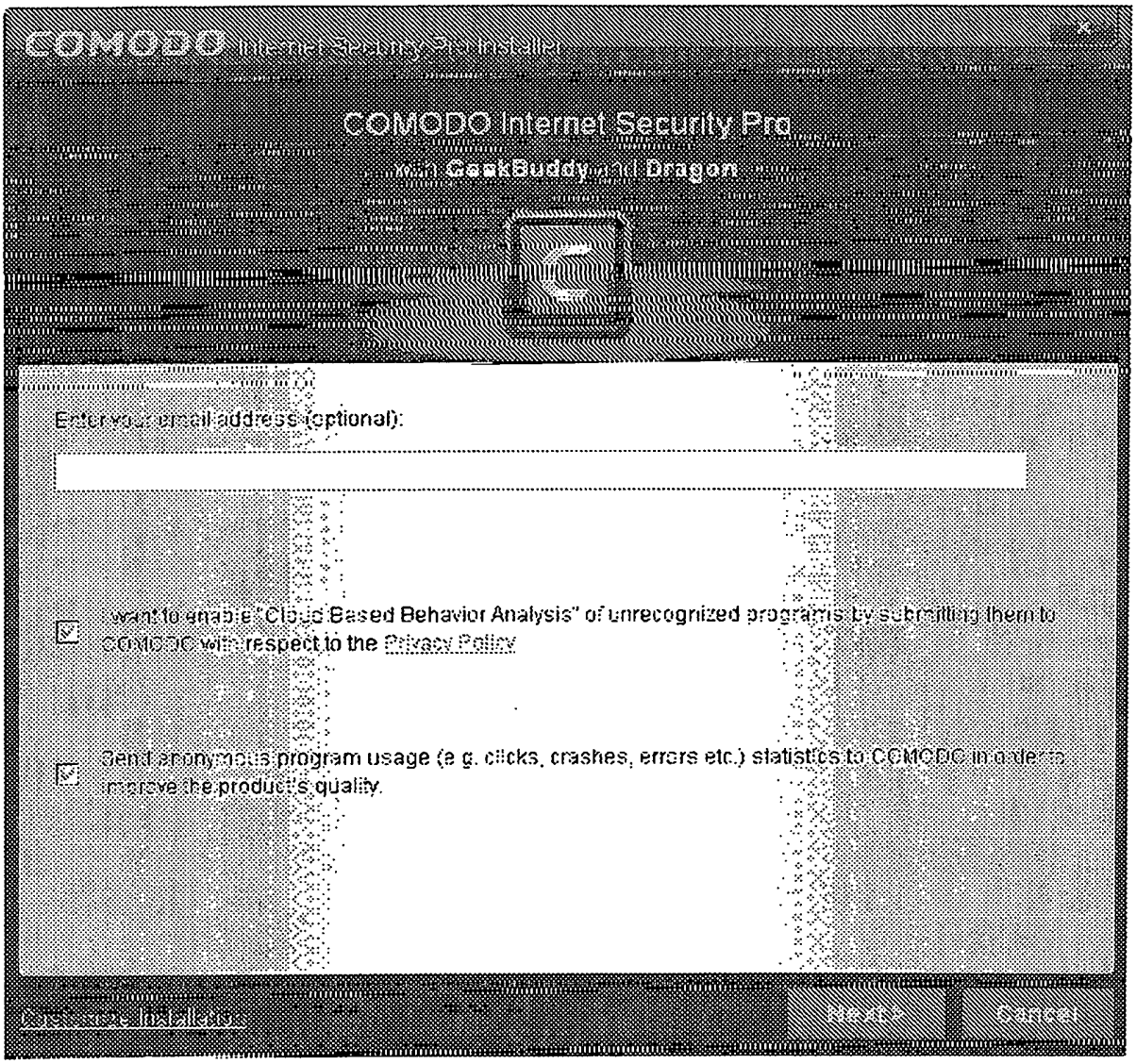
The installation wizard starts automatically and the 'Select the language' dialog is displayed. Comodo Internet Security is available in several languages.




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

**Step 2 - Installation Configuration**

The installation configuration screen will be displayed.




- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

**Receive Comodo News and Notifications**

If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

**Cloud Based Behavior Analysis**

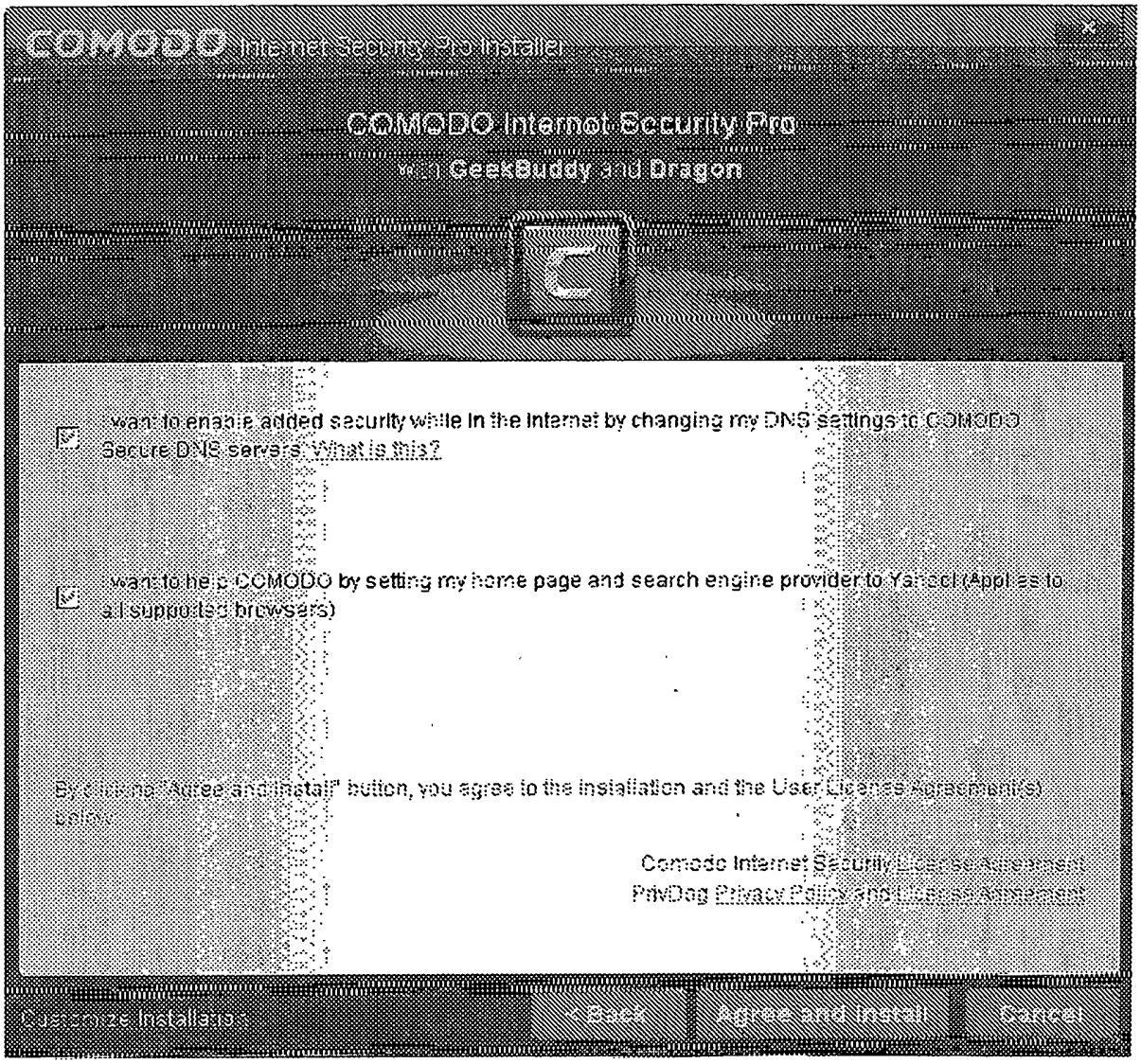
Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

**Send Program Usage Data**

Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from Advanced Settings > General Settings > Log Settings interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.
- Click the 'Next' button.

In the next screen, you can choose to configure your DNS Settings and Browser Home page.




- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

**DNS Settings**

Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

In this step of installation of Comodo Internet Security, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to Appendix 2 Comodo Secure DNS Service.

To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

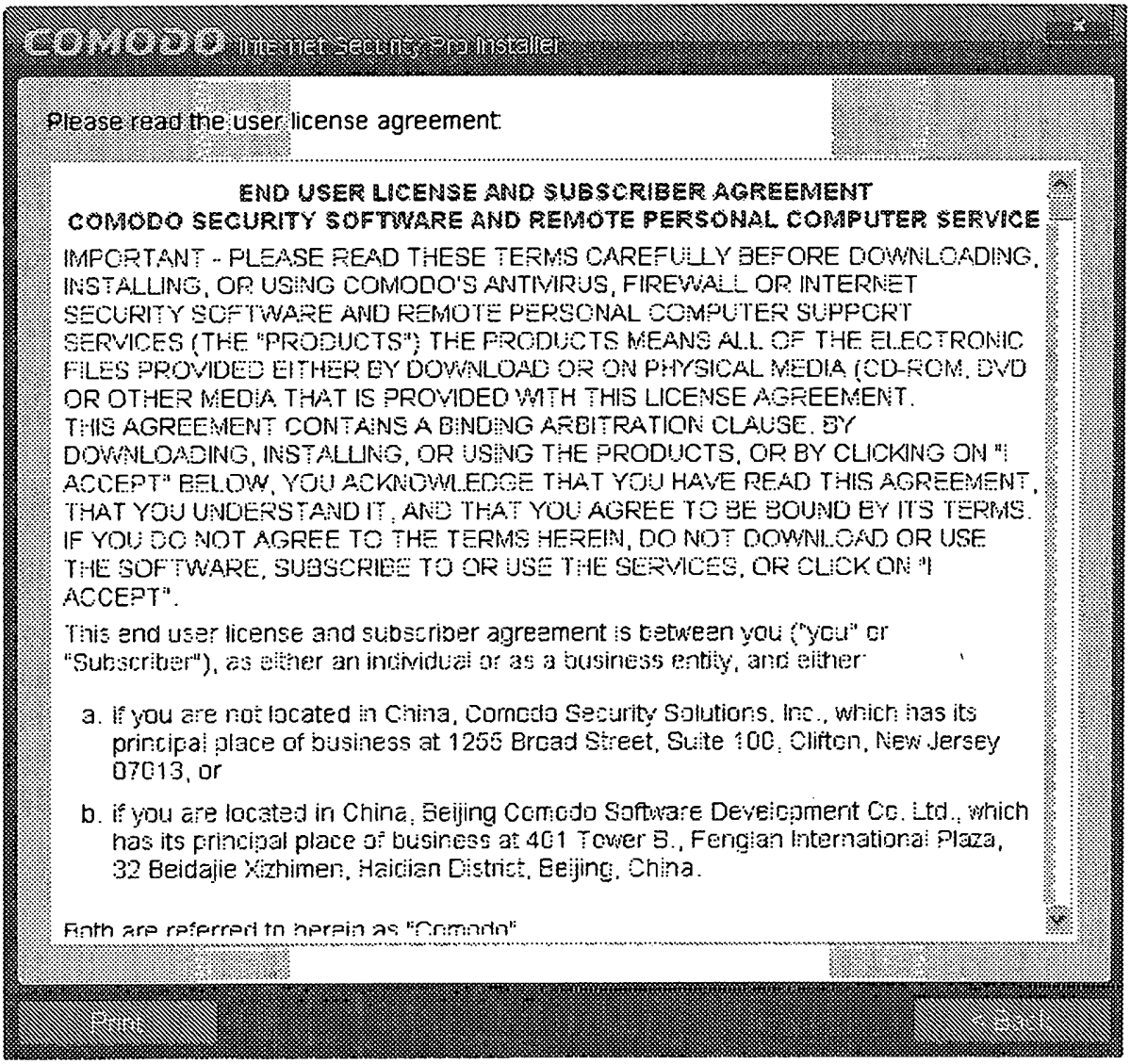
**Browser Homepage**

Your default browser home page and the search engine will be set as Yahoo!

- Please review and/or modify the settings in the dialog.

**End User License Agreement**

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.




After reading the agreement, click the 'Back' button to return to the installation configuration screen.

Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installer'. Otherwise, click 'Agree and Install' to begin installation.

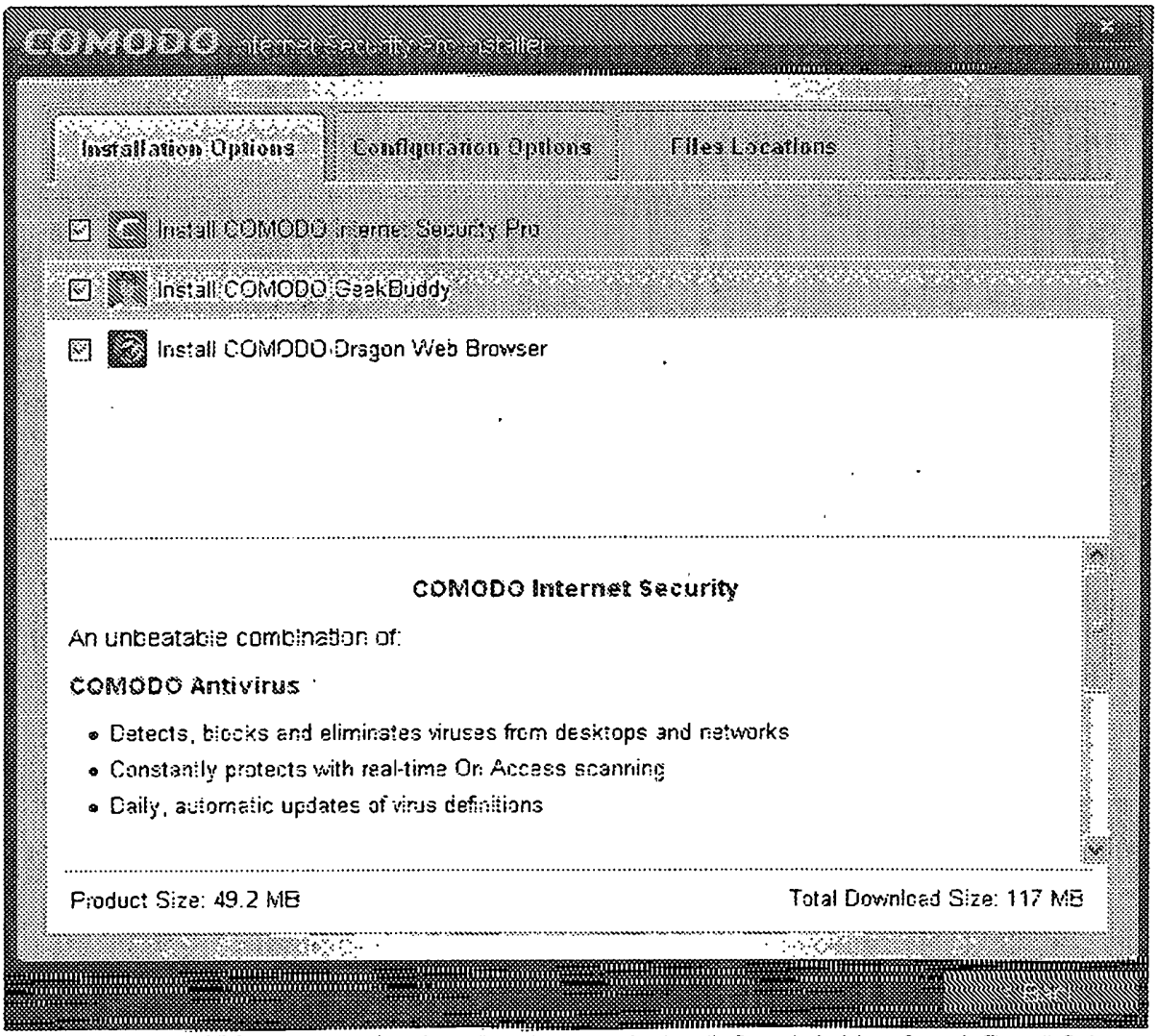
### Customizing Installation

Clicking the 'Customize Installer' link opens an advanced options interface that enables you to choose which elements you would like to install, configure security popup alerts and choose the installation path. In order to obtain maximum protection, Comodo recommends that you uninstall any third party personal Firewall and Antivirus in your system and select all the

components to get the maximum benefit from Comodo Internet Security Pro 2013.

**Select the Components to Install** (Click to go back to Step 2)

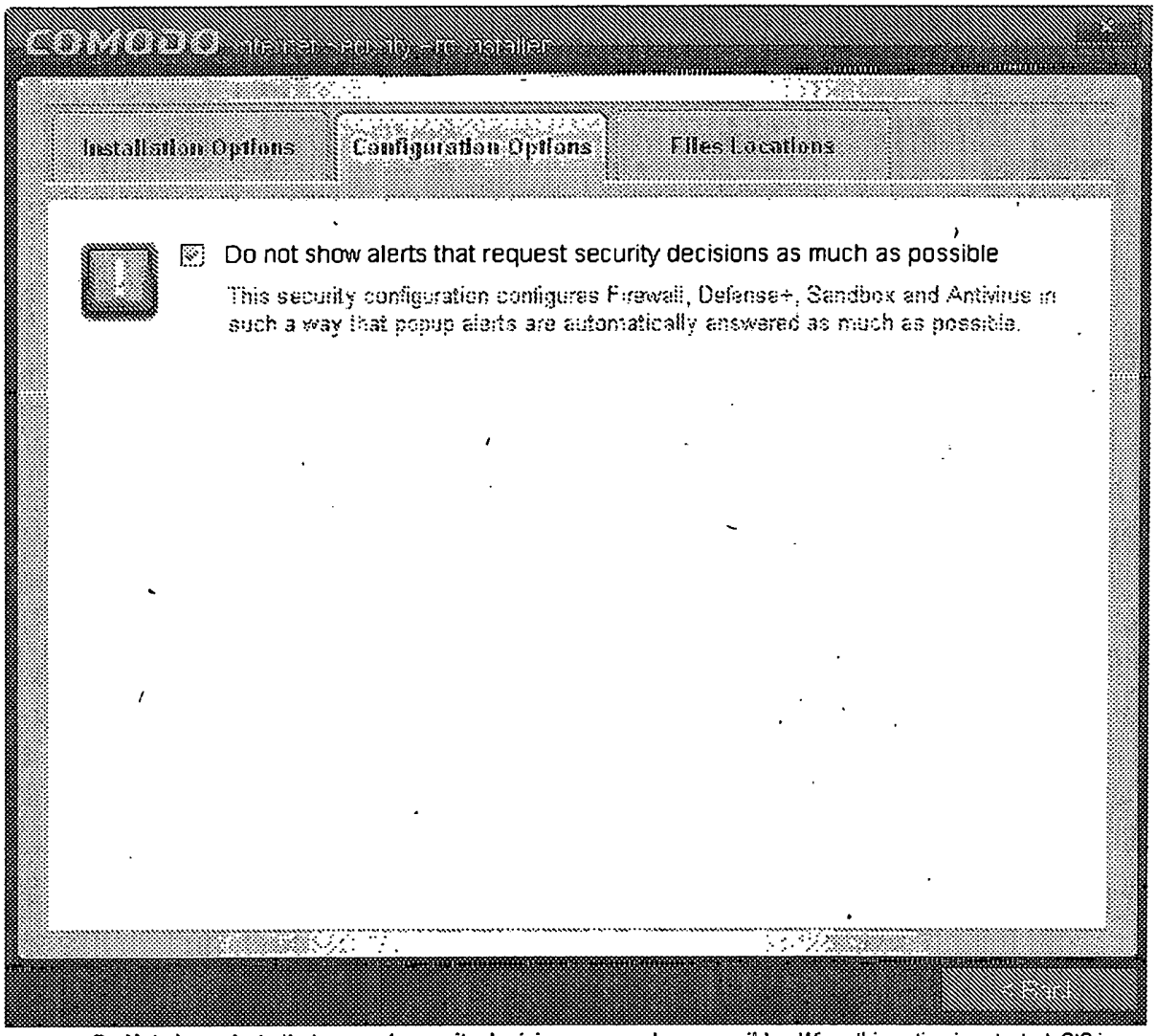
- Click the 'Installation Options' tab to select the components to be installed.




- **Install COMODO Internet Security Pro** - Selecting this option installs Comodo Antivirus, Comodo Firewall, Defense+ components and PrivDog. Installing CIS Pro is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- **Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.

### Configuration Options

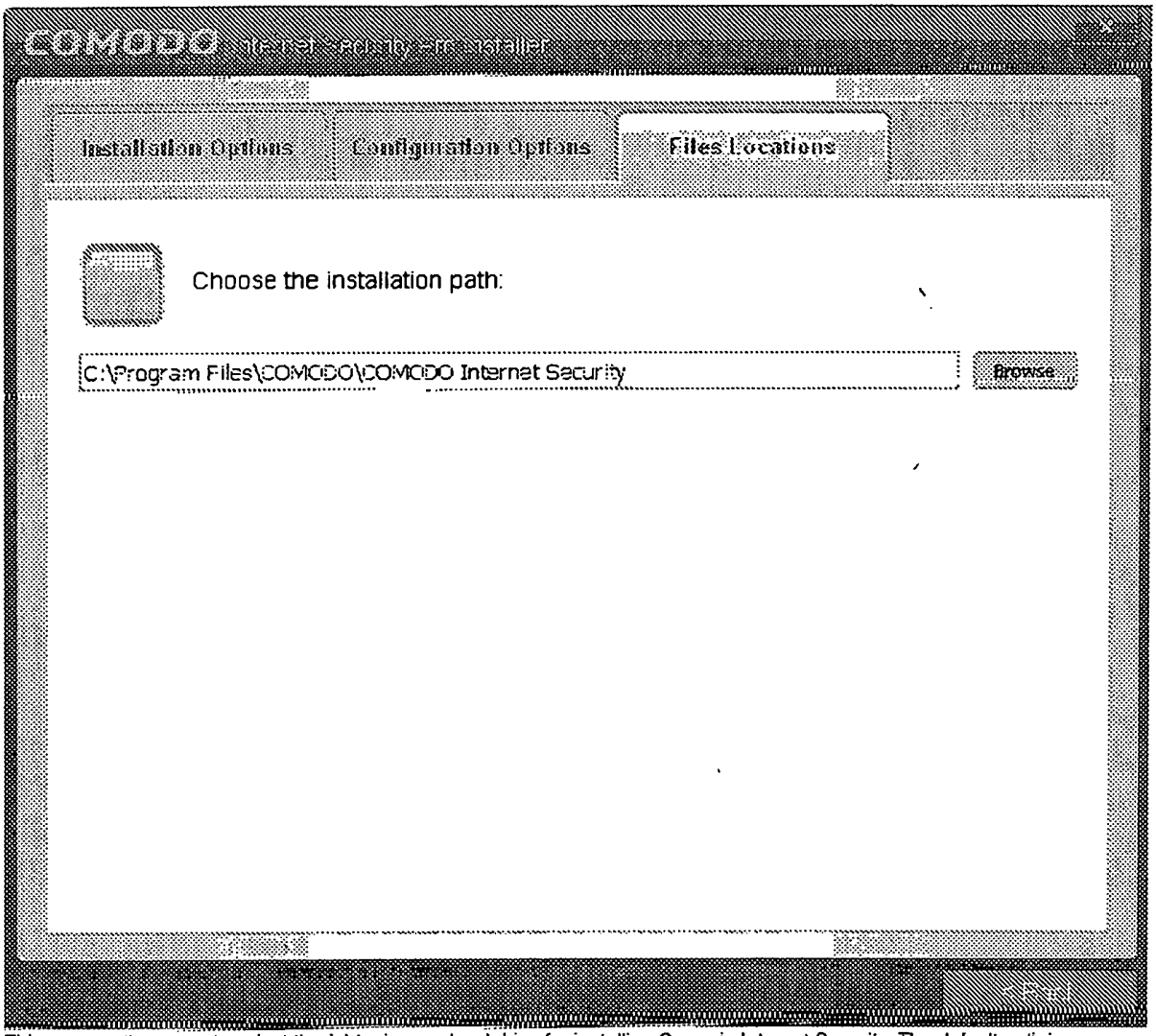
- Click the 'Configuration Options' tab to configure pop-up alert options.




- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

**Choose the Installation Location**

- Click the 'Files Locations' tab to choose the installation path.



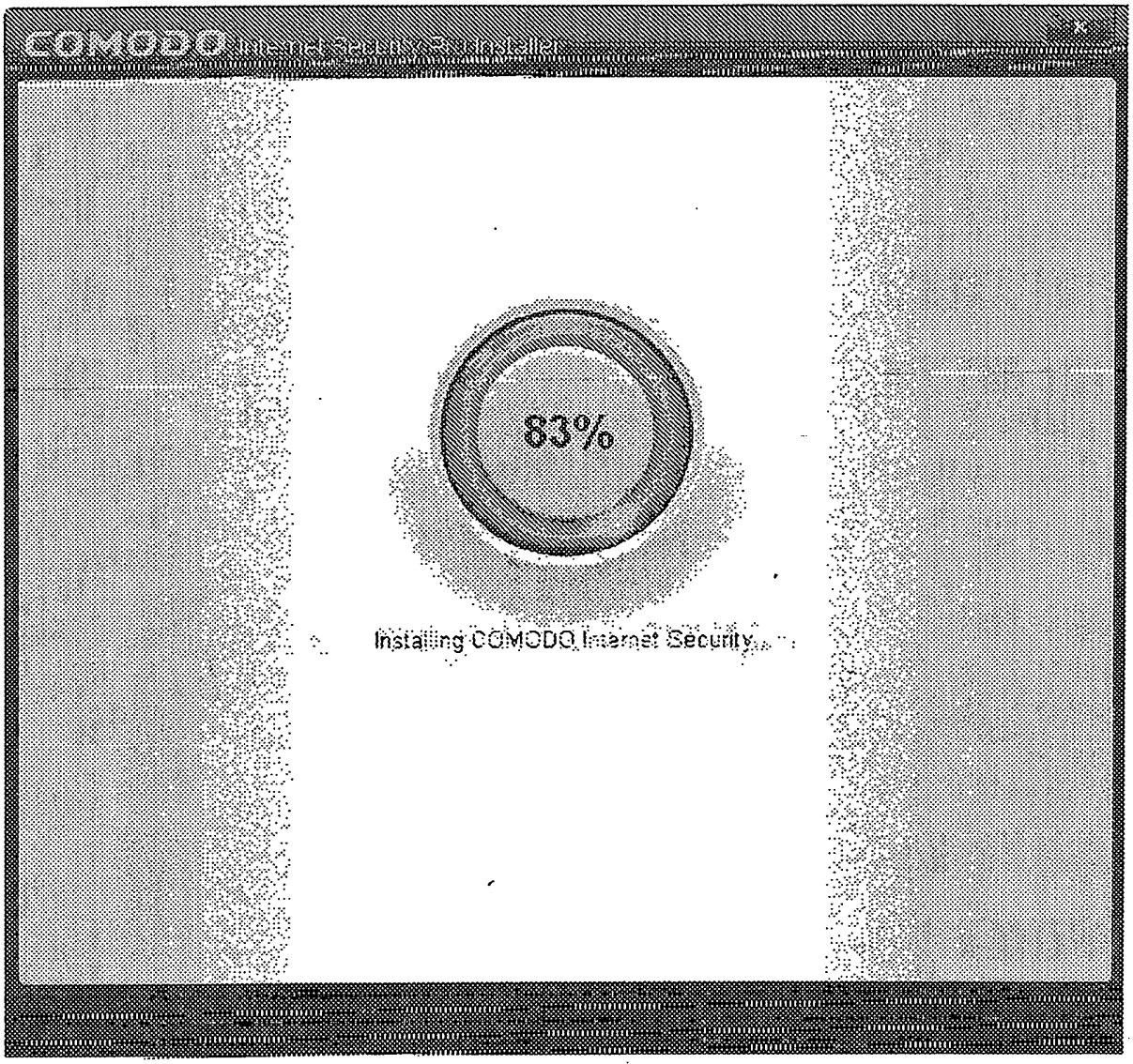

This screen allows you to select the folder in your hard drive for installing Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

After customizing your installation, click the 'Back' button to return to the installation configuration screen.

Click the 'Agree and Install' button to proceed with the installation.

**Step 3 - Installation Progress** (Click to go back to Step 2)

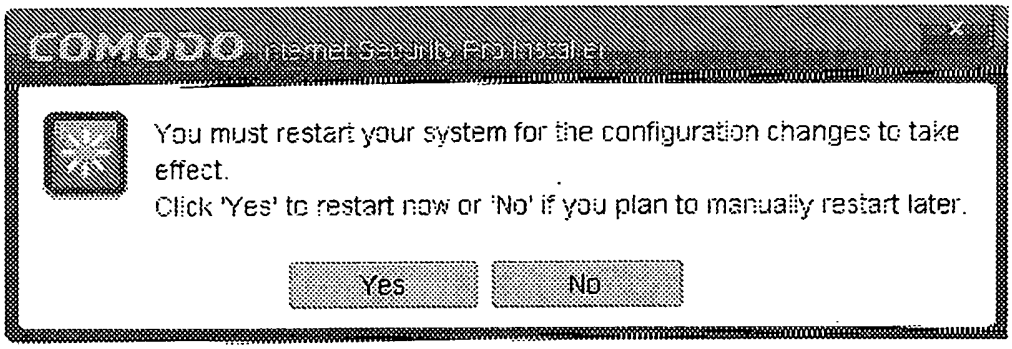
The installation progress will be displayed...




...and on completion, the restart dialog will be displayed.

**Step 4 - Restarting Your System**

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

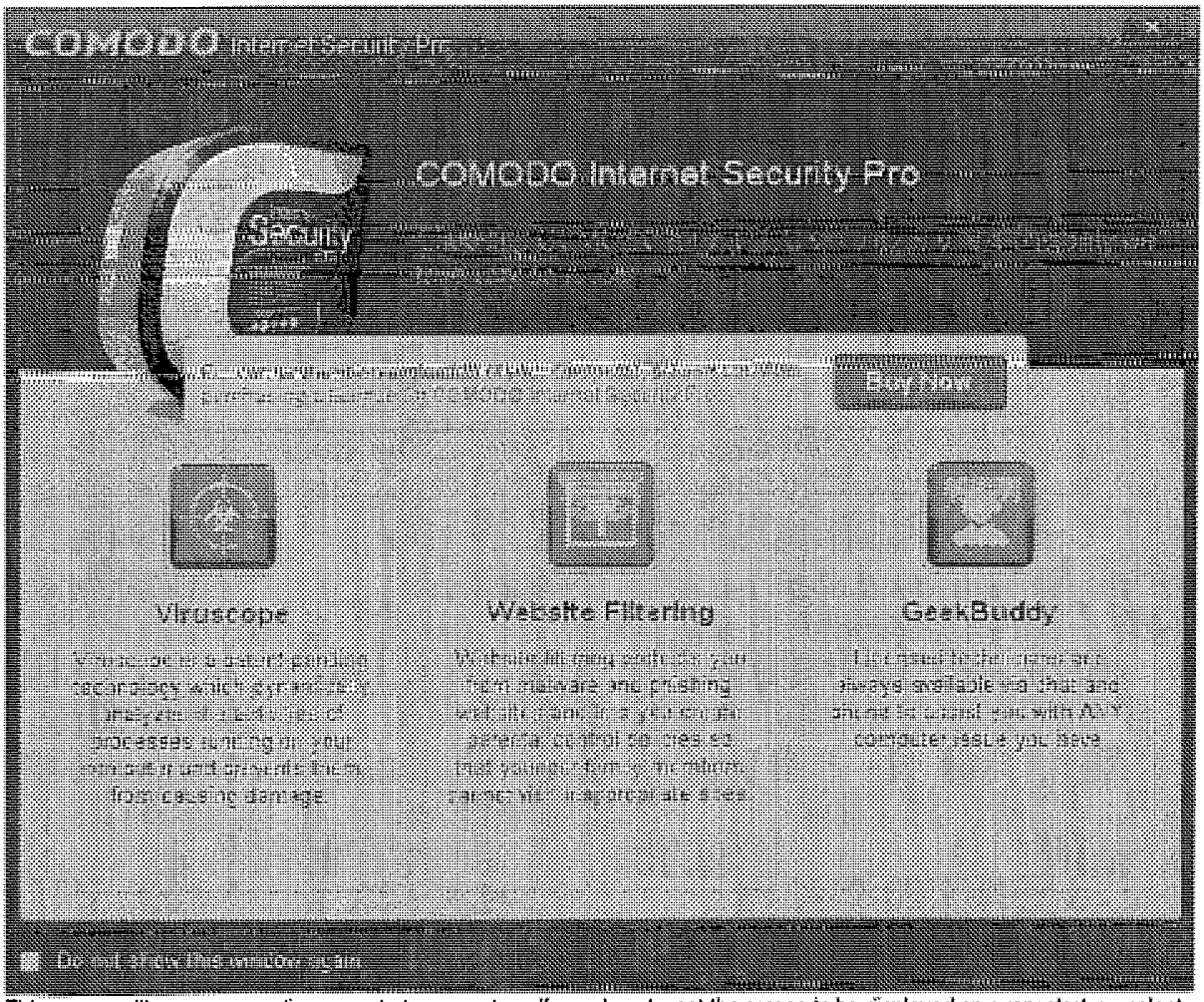



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

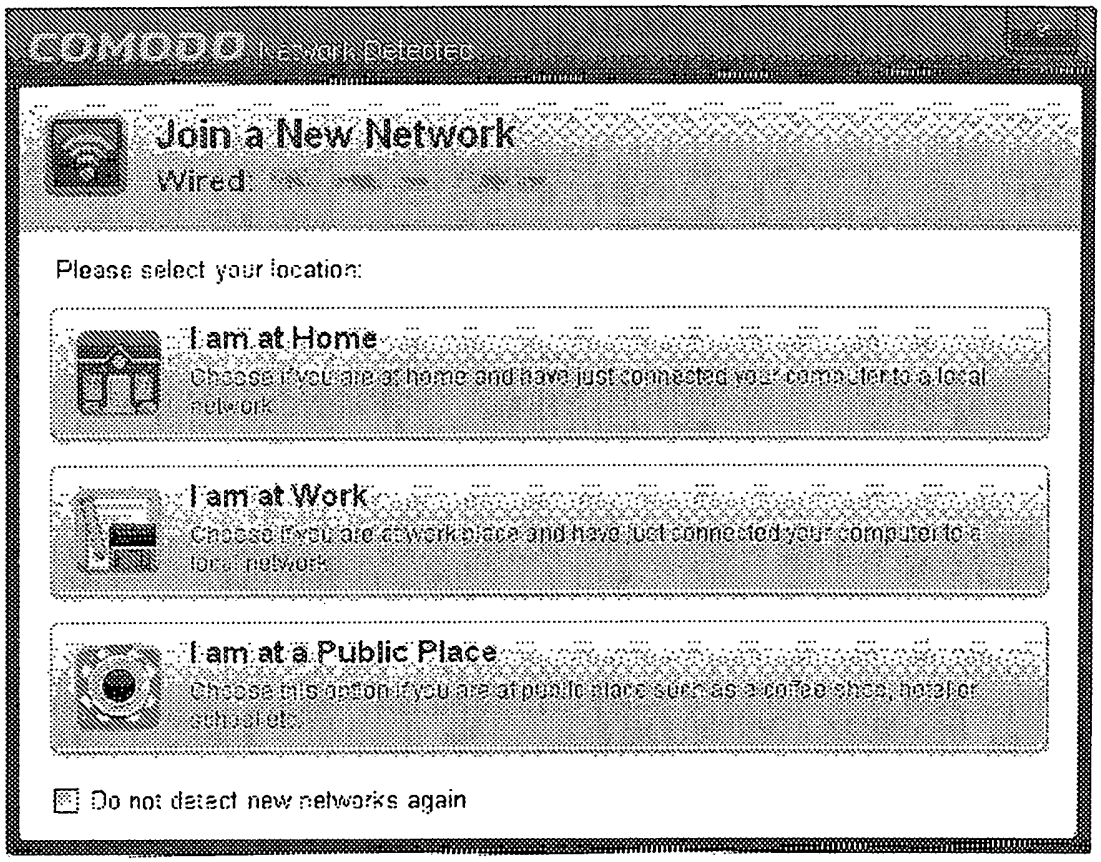
**Step 5 - After Restarting Your System**

After restarting, a 'thankyou' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice. You can also purchase license key from this screen if you have not done so already.




This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

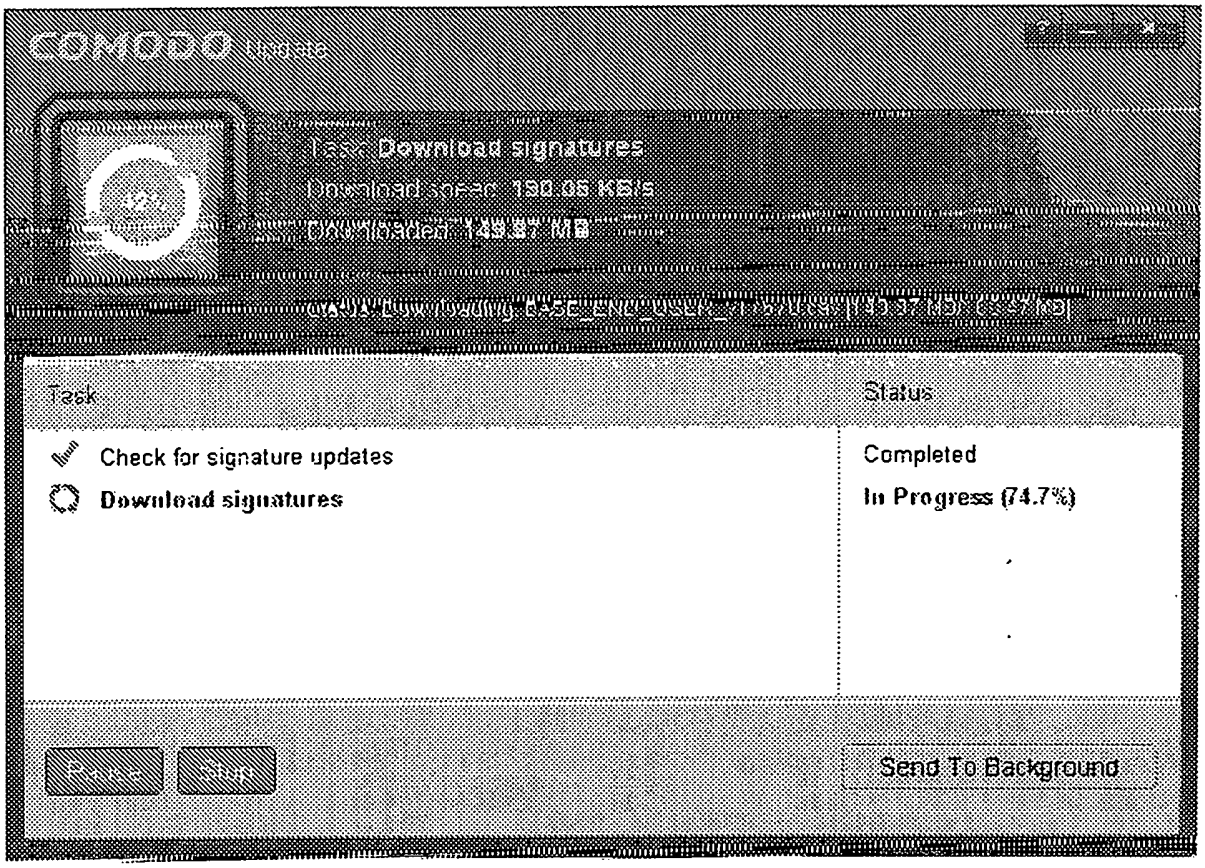



- Select your location from the three options above
- Select 'Do not automatically detect new networks' if you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard')

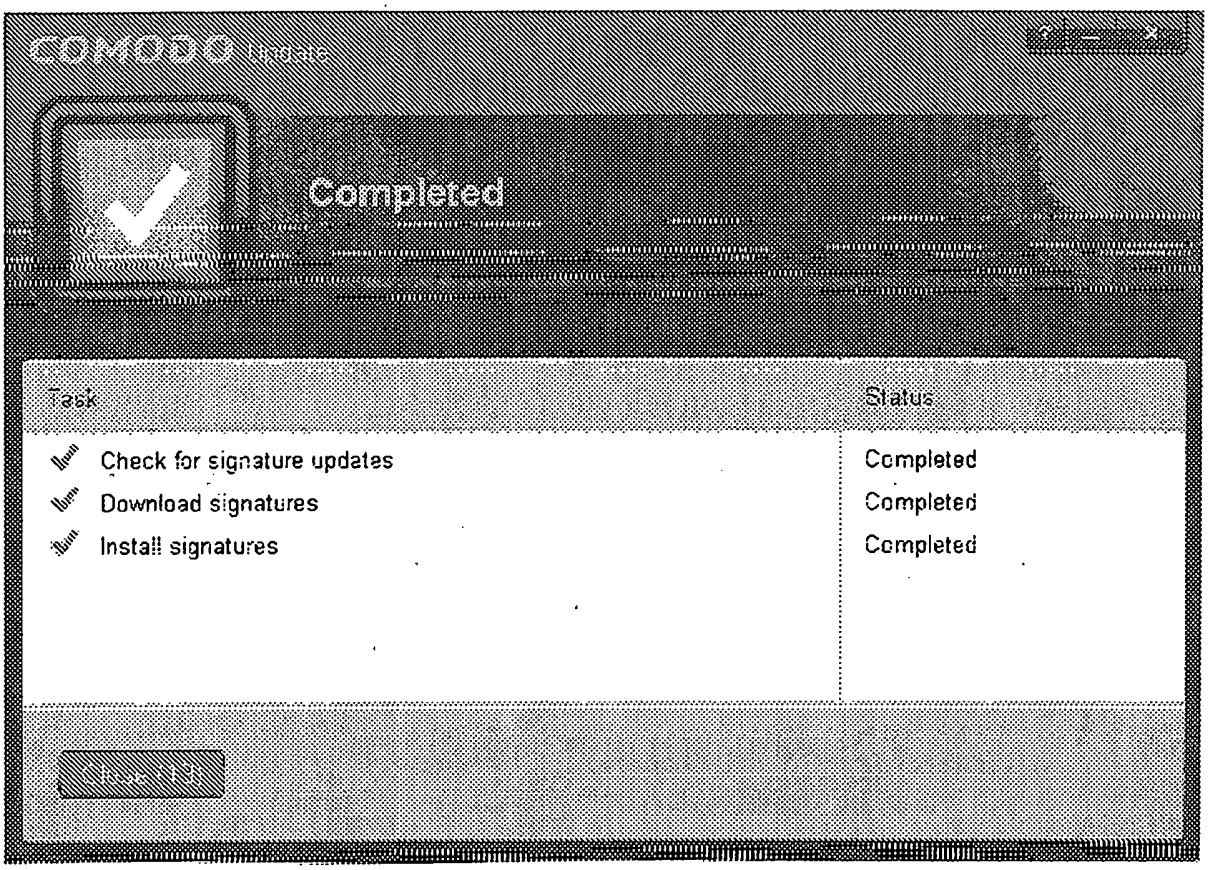
The main interface will be displayed:



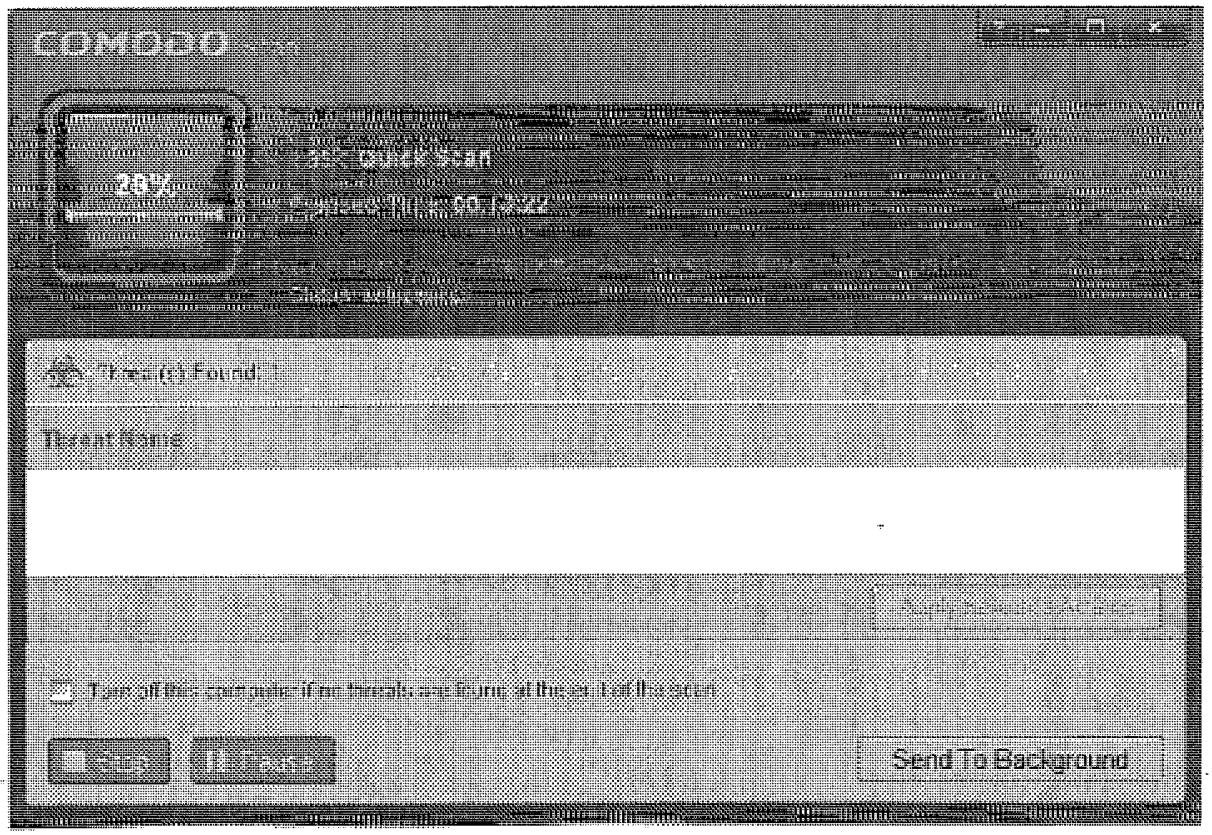

CIS will start its first virus database update at the background. You can view the progress by bringing the update task to foreground from the Task Manager interface. Refer to the section 'Manage CIS Tasks' for more details.




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

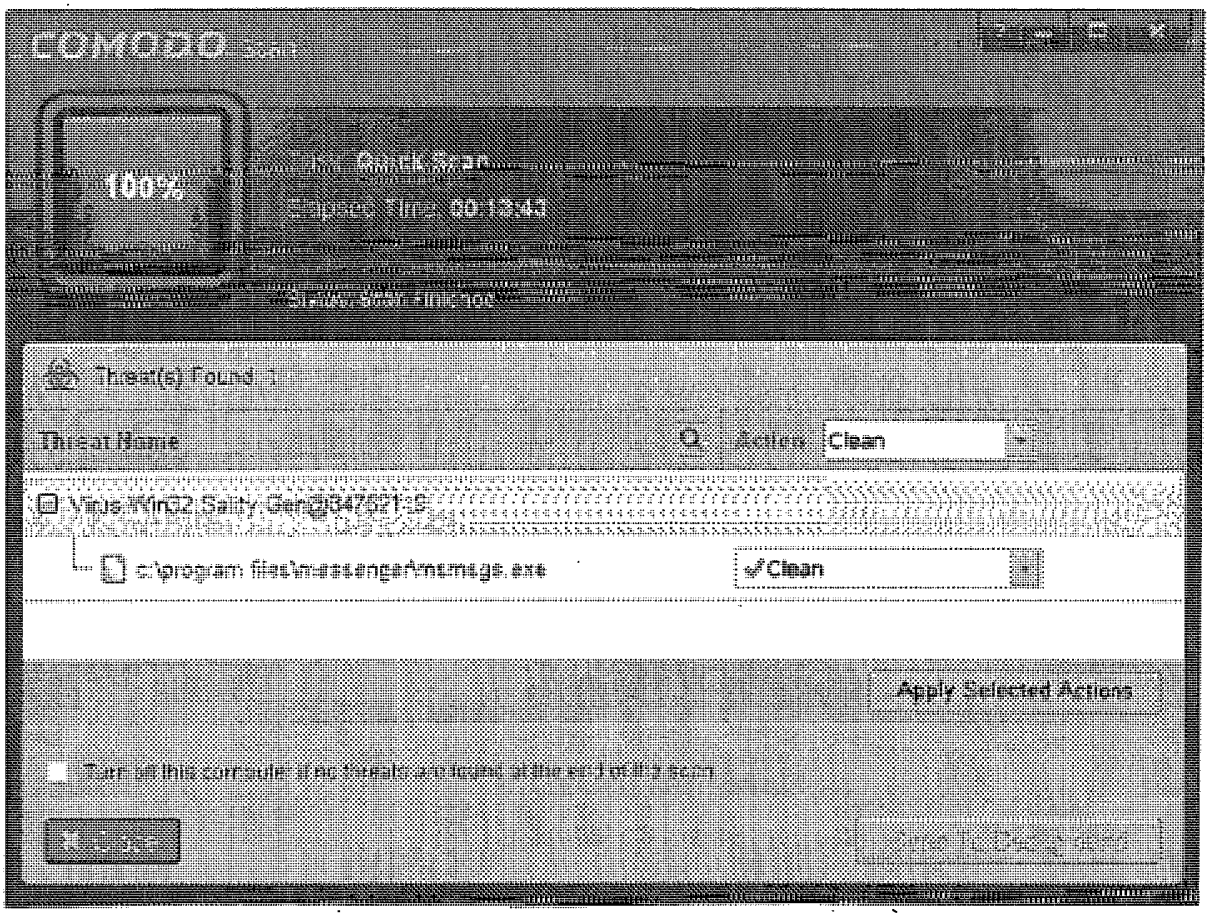



CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.



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

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




If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section 'Processing Infected Files' for more details.

Important Note: After successful installation, you need to activate the license for using the product. In order to get your guarantee coverage, you need to activate the license first.

- For full explanation on activation of license after installation of the product, refer to Activating Your License.
- For full explanation on activation of your guarantee, refer to Activating Your Guarantee Coverage.

## 1.3.3. CIS Complete - Installation and Activation

Note : Before beginning installation, please ensure you have uninstalled any other antivirus and firewall products that are on your computer. Click here to read the full note.

Comodo Internet Security Complete can be downloaded from www.comodo.com/home/internet-security/internet-security-complete.php after signing up for subscription and includes Comodo Dragon, GeekBuddy, Comodo Backup, TrustConnect and the Comodo Guarantee.

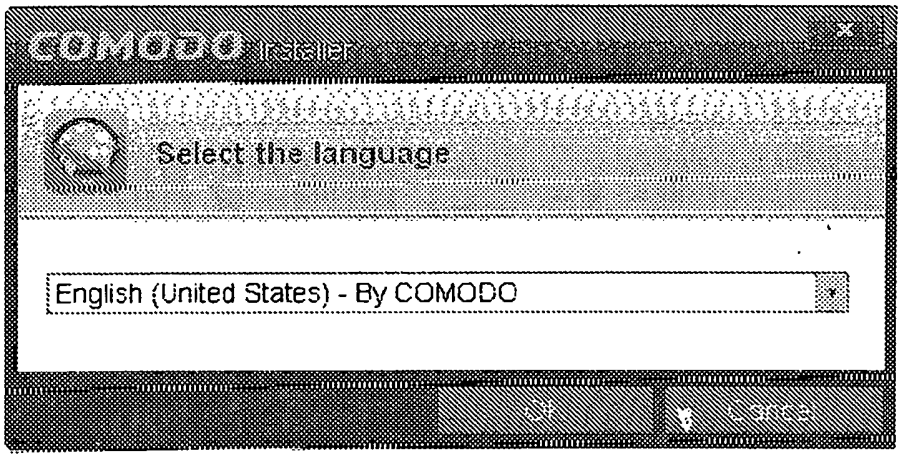
- Choose whether you want the 32 or 64 bit version of CIS then click 'download'
- If you are unsure which version you need, select the 32/64-bit Windows Installer. This executable contains BOTH 32 and 64 bit installers. The setup routine will automatically detect which version of Windows you have and install the appropriate version. Please note, the Universal Windows Installer is a much larger download than the individual 32 or

64 bit setup files.

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

**Step 1 - Choosing the Interface Language**

The language selection dialog will be displayed.

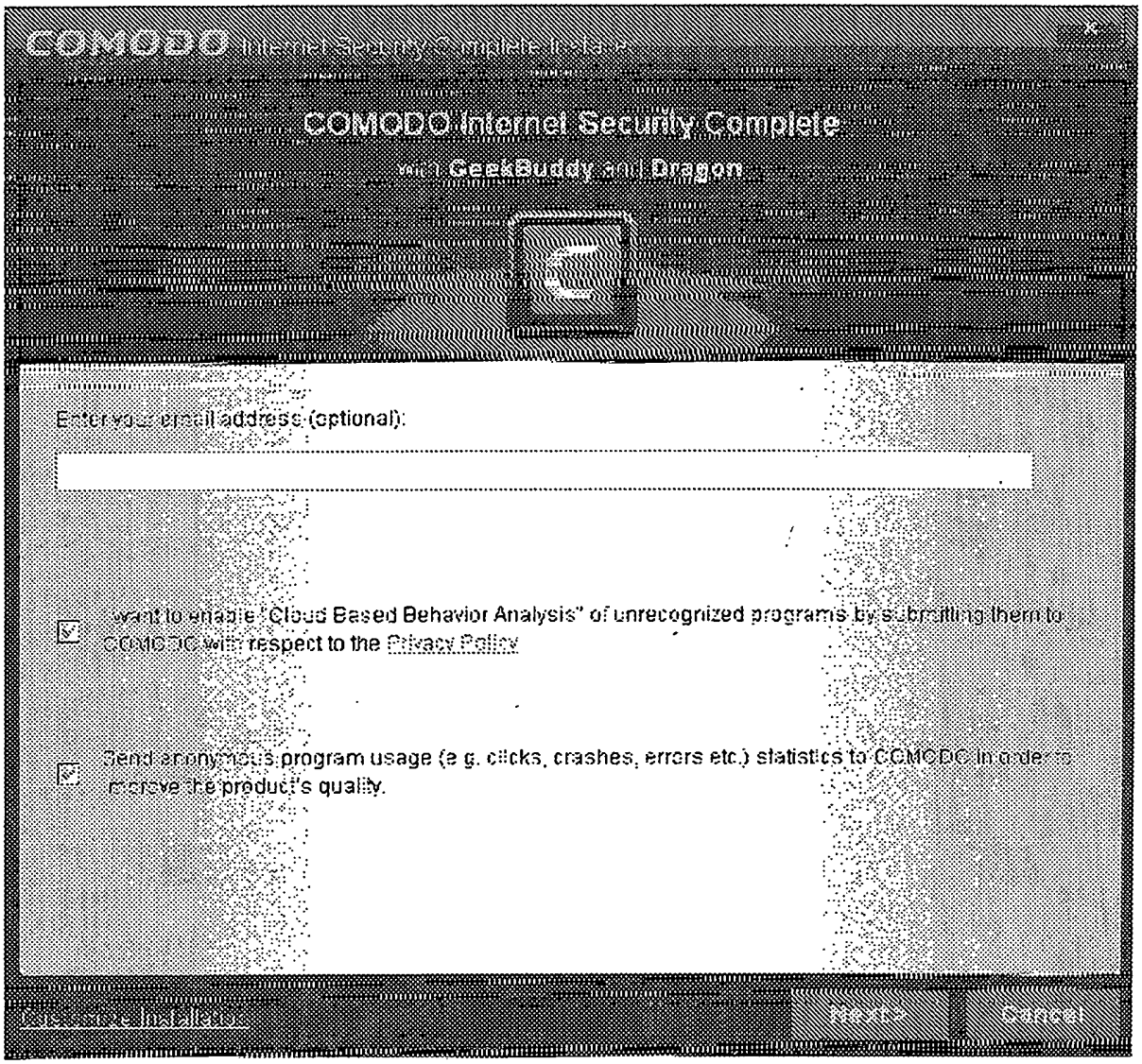



Comodo Internet Security is available in several languages.

- Select the language in which you wish the wizard should continue and Comodo Internet Security Complete is to be installed, from the drop-down menu and click 'OK'.

**Step 2 - Installation Configuration**

The installation configuration screen will be displayed.




- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

**Receive Comodo News and Notifications**

If you wish to sign up for news about Comodo products then enter your email address in the space provided. This is optional.

**Cloud Based Behavior Analysis**

Any file that is identified as unrecognized is sent to the Comodo Instant Malware Analysis (CIMA) server for behavior analysis. Each file is executed in a virtual environment on Comodo servers and tested to determine whether it contains any malicious code. The results will be sent back to your computer in around 15 minutes. Comodo recommends users leave this setting enabled. Read the privacy policy by clicking the 'Privacy Policy' link.

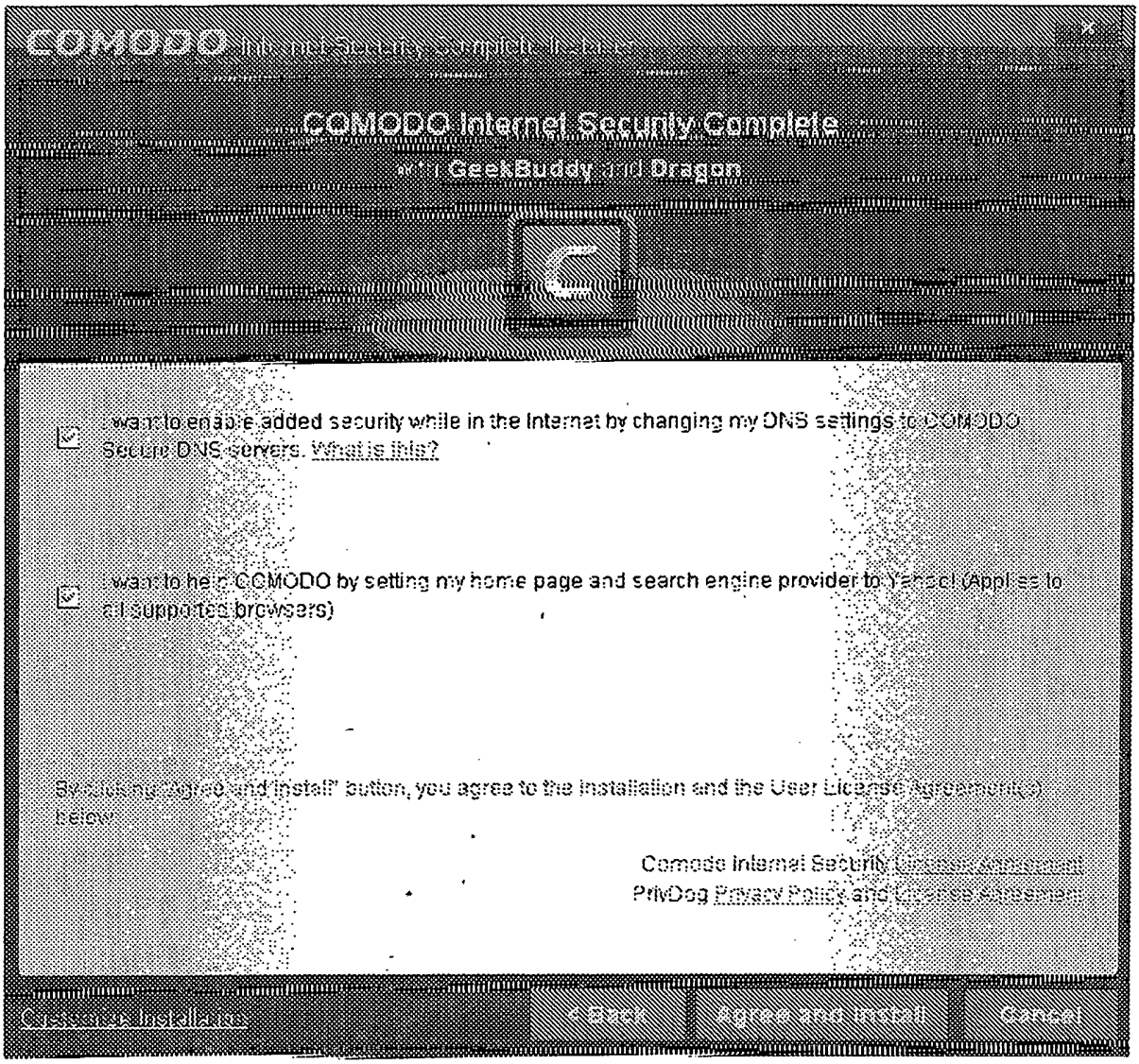
**Send Program Usage Data**

Comodo collects collects the usage details from millions of CIS users to analyze their usage patterns for the continual enhancement of the product. Your CIS installation will collect details on how you use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. Comodo recommends users leave this setting enabled. You can change this setting from Advanced Settings > General Settings > Log Settings interface, at anytime after installation.

- Please review and/or modify the settings in the dialog.

- Click the 'Next' button.

  In the next screen, you can choose to configure your DNS Settings and Browser Home page.




- If you click 'Customize Installation' then you can choose advanced options. These include which CIS components you wish to install, the ability to choose CIS installation path and other advanced CIS configuration settings.

  **DNS Settings**

  Comodo Secure DNS service replaces your existing Recursive DNS Servers and resolves all your DNS requests exclusively through Comodo's proprietary Directory Services Platform. Comodo's worldwide network of redundant DNS servers provide fast and secure Internet browsing experience without any hardware or software installation.

  In addition, Comodo's Secure DNS ensures safety against attacks in the form of malware, spyware, phishing etc., by blocking access to malware-hosting sites, by any program running in your system.

  For more details on Comodo Secure DNS Service and to know how to enable or disable the service, refer to Appendix 2 Comodo Secure DNS Service.

  In this step of installation of CIS Complete, the DNS settings of your computer can be changed automatically to direct to our DNS servers. You can disable the service at anytime and revert to your previous settings.

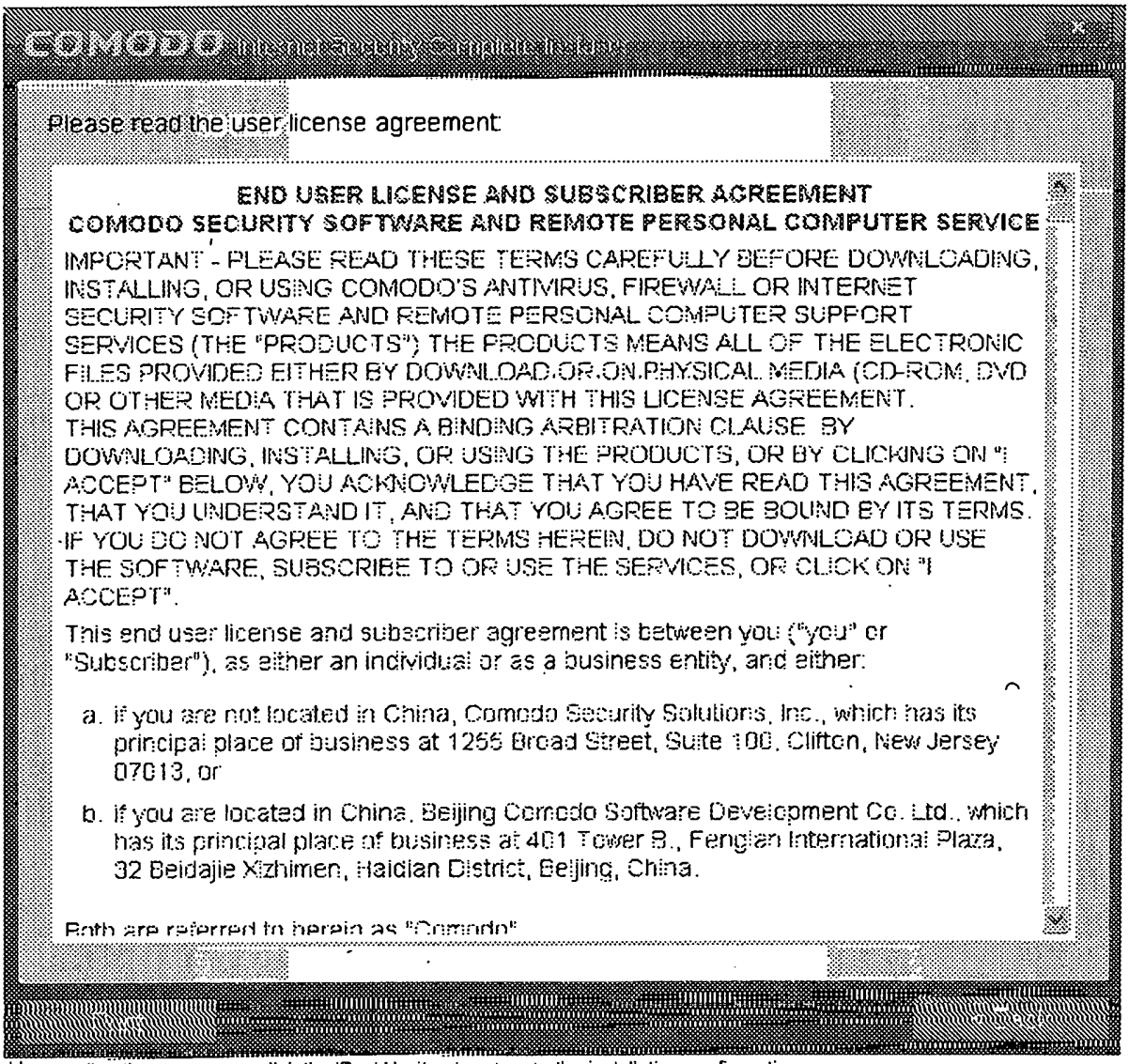
  To enable Comodo Secure DNS, select 'Change my DNS Servers to COMODO SecureDNS Servers. Click the 'What is this' link to know more about Comodo Secure DNS servers.

  **Browser Homepage**

Your default browser home page and the search engine will be set as Yahoo!

**End User License Agreements**

Read the complete User License Agreements by clicking the 'License Agreement' links of Comodo Internet Security and PrivDog respectively before proceeding with the installation. To read the PrivDog privacy policy link, click the Privacy Policy link next to it.




After reading the agreement, click the 'Back' button to return to the installation configuration screen.

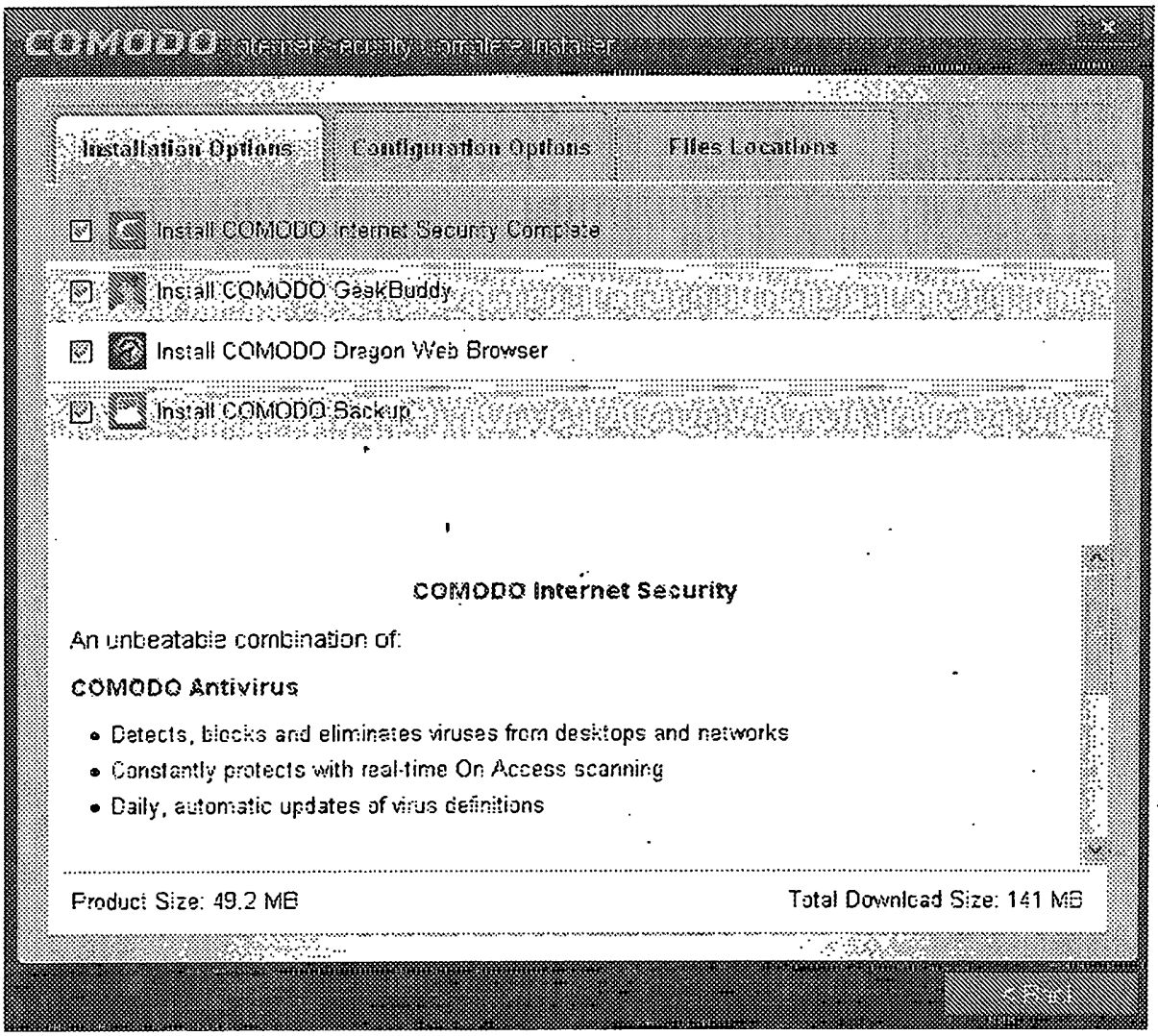
Once back at the main installer screen, if you wish to configure advanced options, click 'Customize Installation'. Otherwise, click 'Agree and Install' to begin installation.

### Customizing Installation

Click the 'Customize Installation' link to select the components to be installed, enable security popup alerts to be minimized and choose installation path.

### Selecting Components to Install (Click to go back to Step 2)

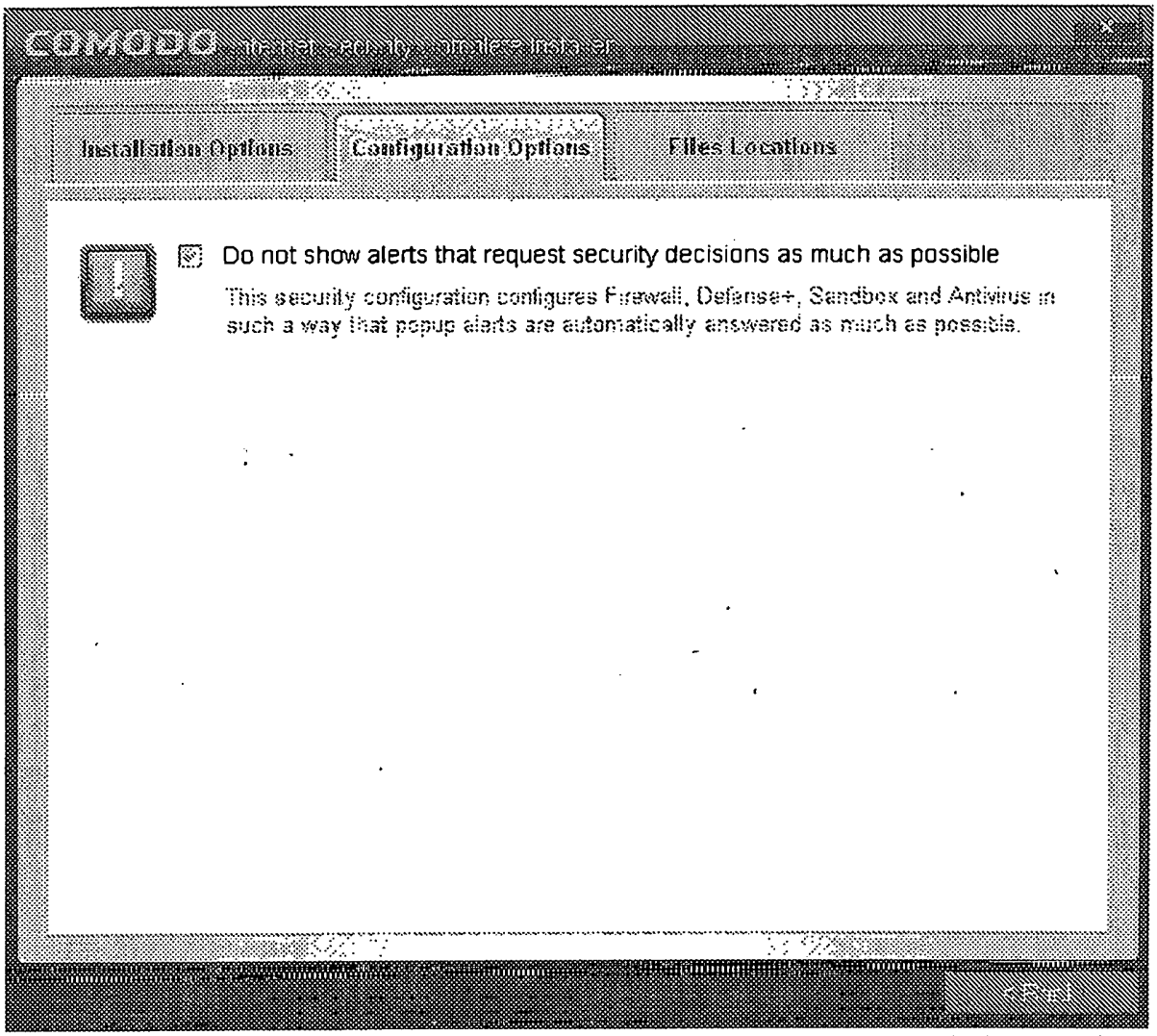
- Click the 'Installation Options' tab to select the components to be installed.




- **Install COMODO Internet Security Complete** - Selecting this option installs Comodo Antivirus, Comodo Firewall, Defense+ components and Comodo PrivDog. Installing CIS Complete is mandatory to qualify for the virus free guarantee.
- **Install COMODO GeekBuddy** - Selecting this option installs GeekBuddy, a 24 x 7 remote support service in which Comodo experts can help you solve any computer related problems you may encounter. Refer to the section Comodo GeekBuddy for more details.
- **Install COMODO Dragon Web Browser** - Selecting this option installs Comodo Dragon, a fast and versatile Internet browser based on Chromium technology and infused with Comodo's unparalleled level of security. Refer to the section Comodo Dragon for more details.
- **Install COMODO Backup** - Selecting this option installs Comodo Backup, a powerful and easy-to-use desktop application that helps home and business users protect their valuable data against damage or loss. Refer to the section Comodo Backup for more details.

### Configuration Options

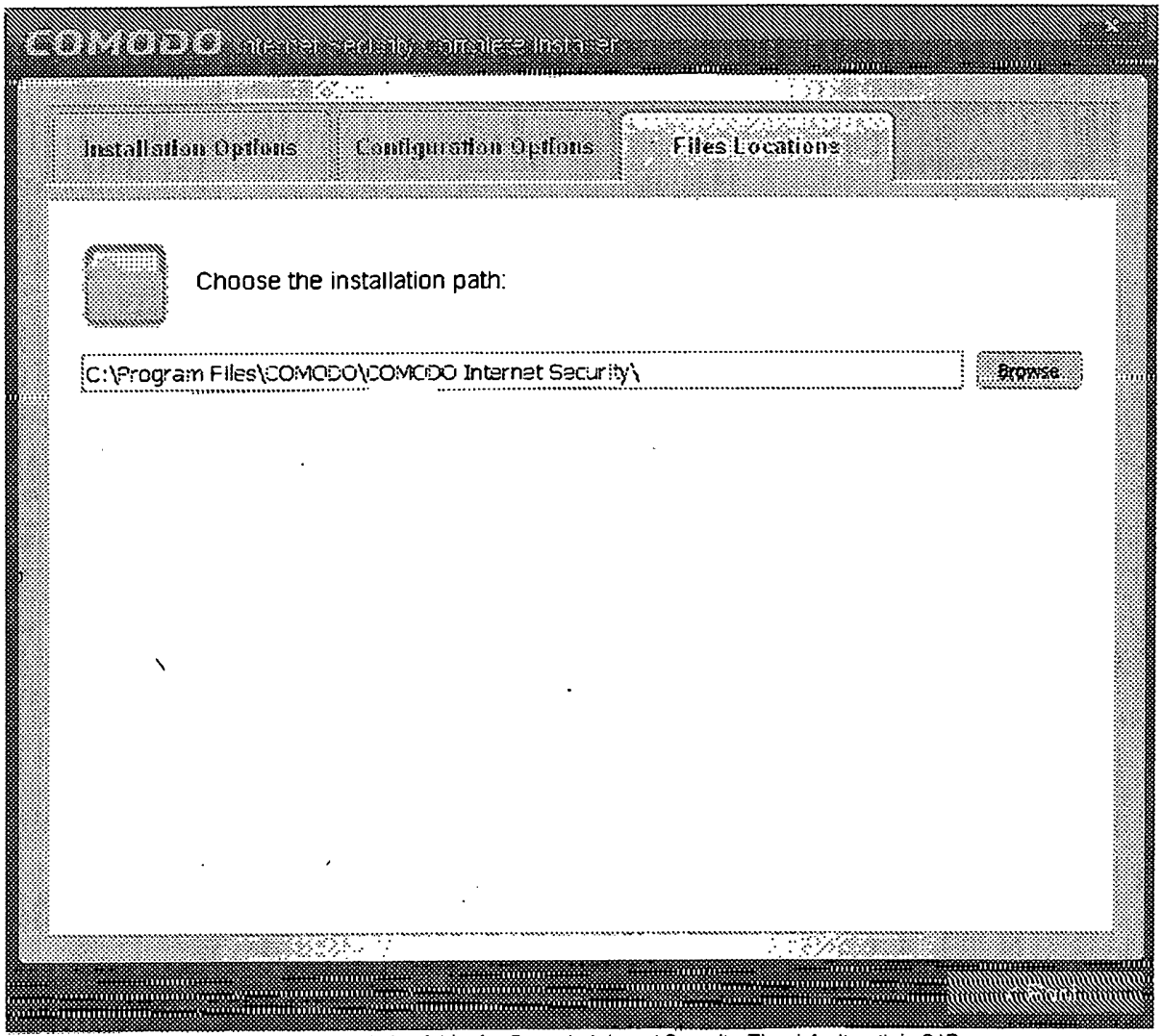
- Click the 'Configuration Options' tab to configure pop-up alert options.




- **Do Not show alerts that request security decisions as much as possible** - When this option is selected, CIS is configured to automatically deal with most issues in a secure manner without raising a popup alert - thus minimizing user intervention. Most users should leave this option at the default state of enabled. Advanced users wishing to gain greater insight into CIS actions and/or to have more control over security decisions may wish to disable this option.

**Choosing Installation Location**

- Click the 'Files Locations' tab to choose the installation path.



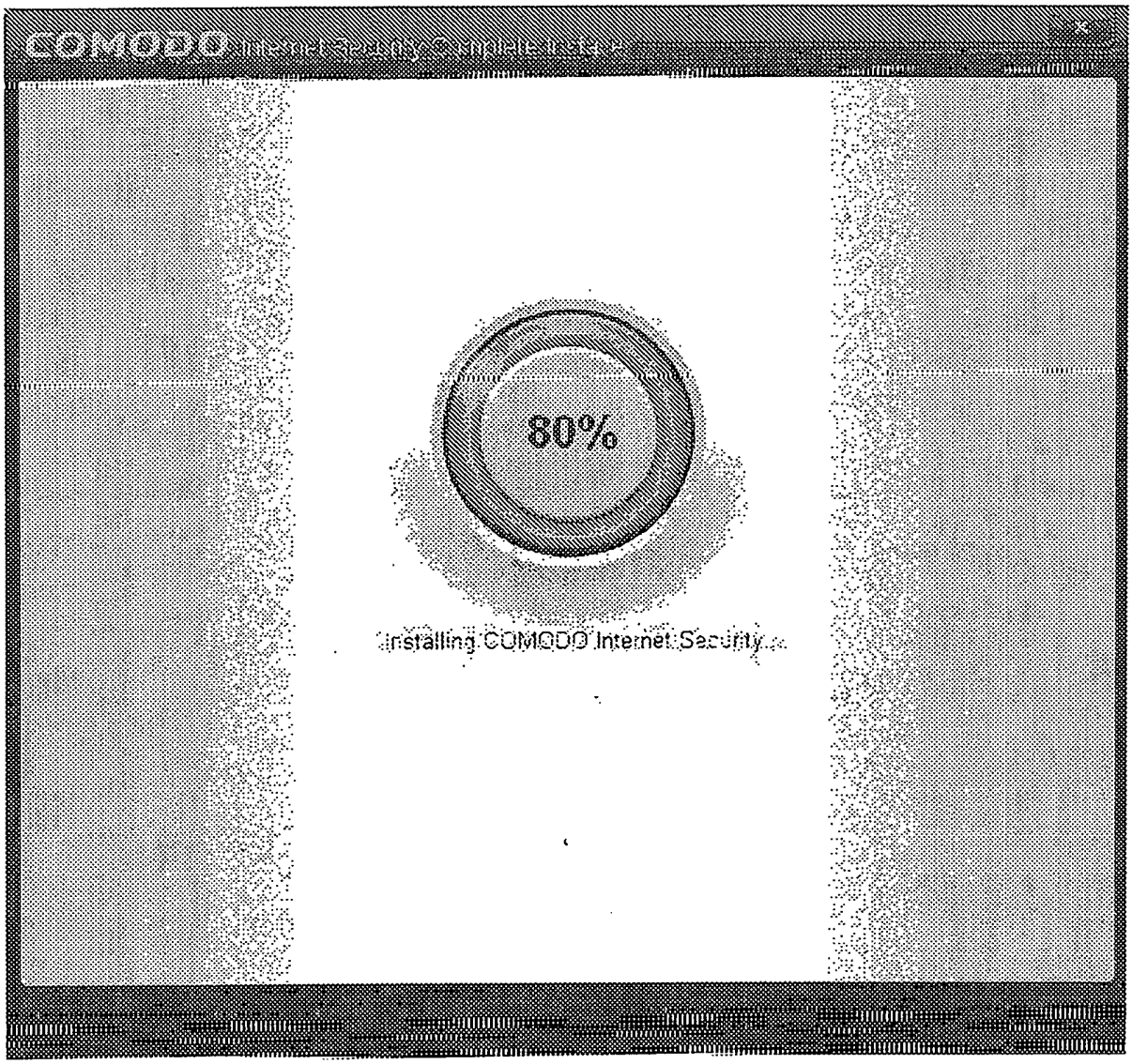

This interface allows you to set the installation folder for Comodo Internet Security. The default path is C:\Program Files\COMODO\COMODO Internet Security. If you want to install the application in a location other than the default location, click 'Browse' to choose a different location.

After customizing your installation, click the 'Back' button to return to the installation configuration screen.

- Click the 'Agree and Install' button to proceed with the installation.

**Step 3 - Installation progress** (Click to go back to Step 2)

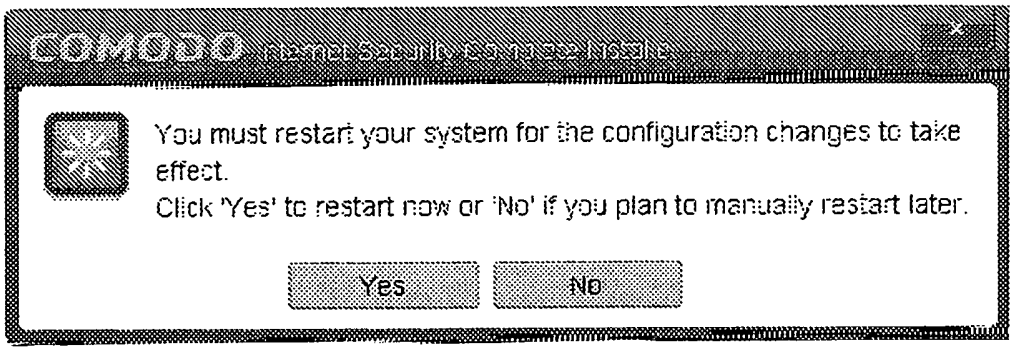
The installation progress will be displayed...




...and on completion, the restart dialog will be displayed.

**Step 4 - Restarting Your System**

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

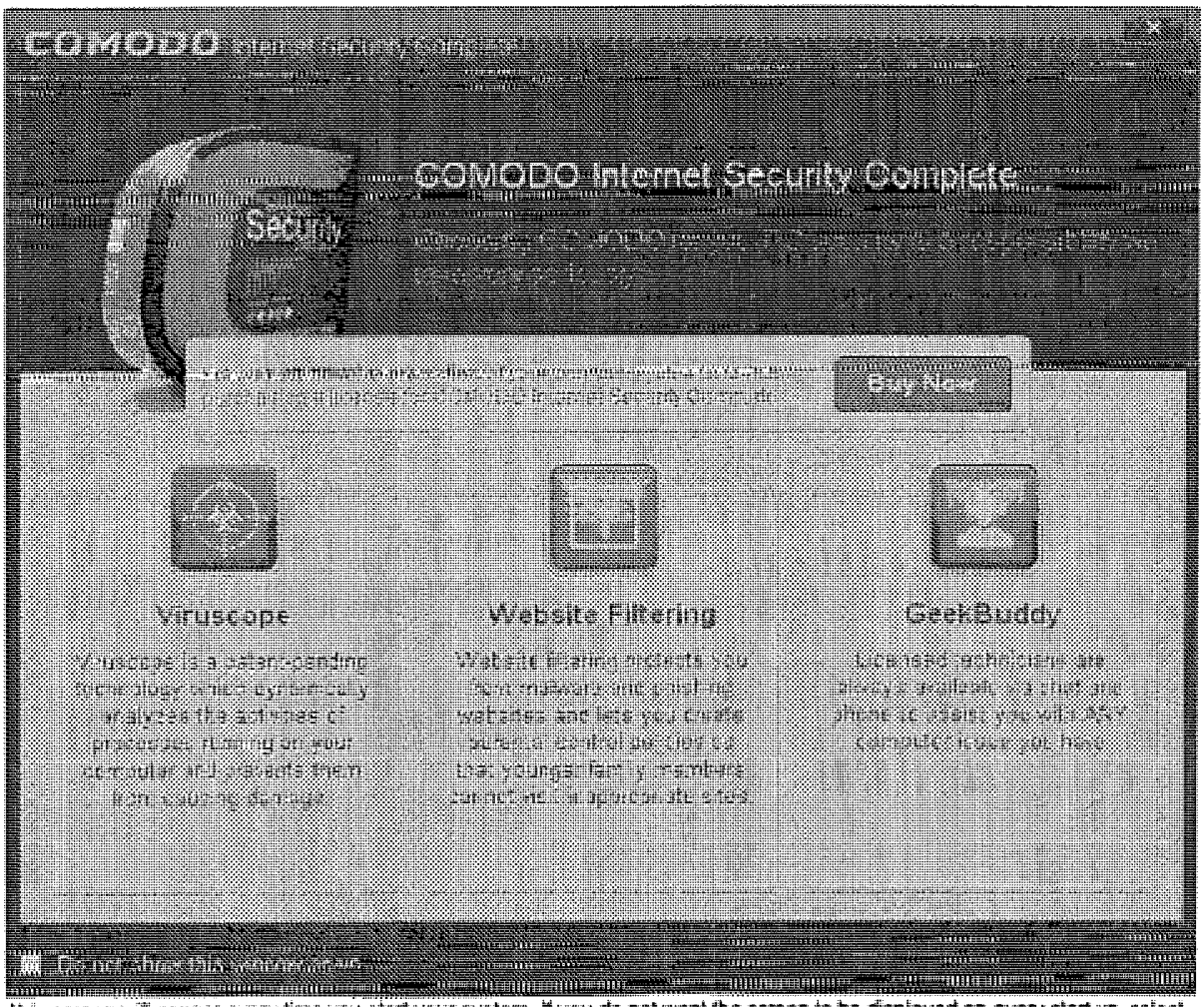



Please save any unsaved data and click 'Yes' to restart the system. If you want to restart the system at a later time, click 'No'.

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

**Step 5 - After Restarting Your System**

After restarting, a 'Start Up' screen will appear. This contains a summary of the components you chose to install as well as some friendly advice. You can also purchase license key from this screen if you have not done so already.



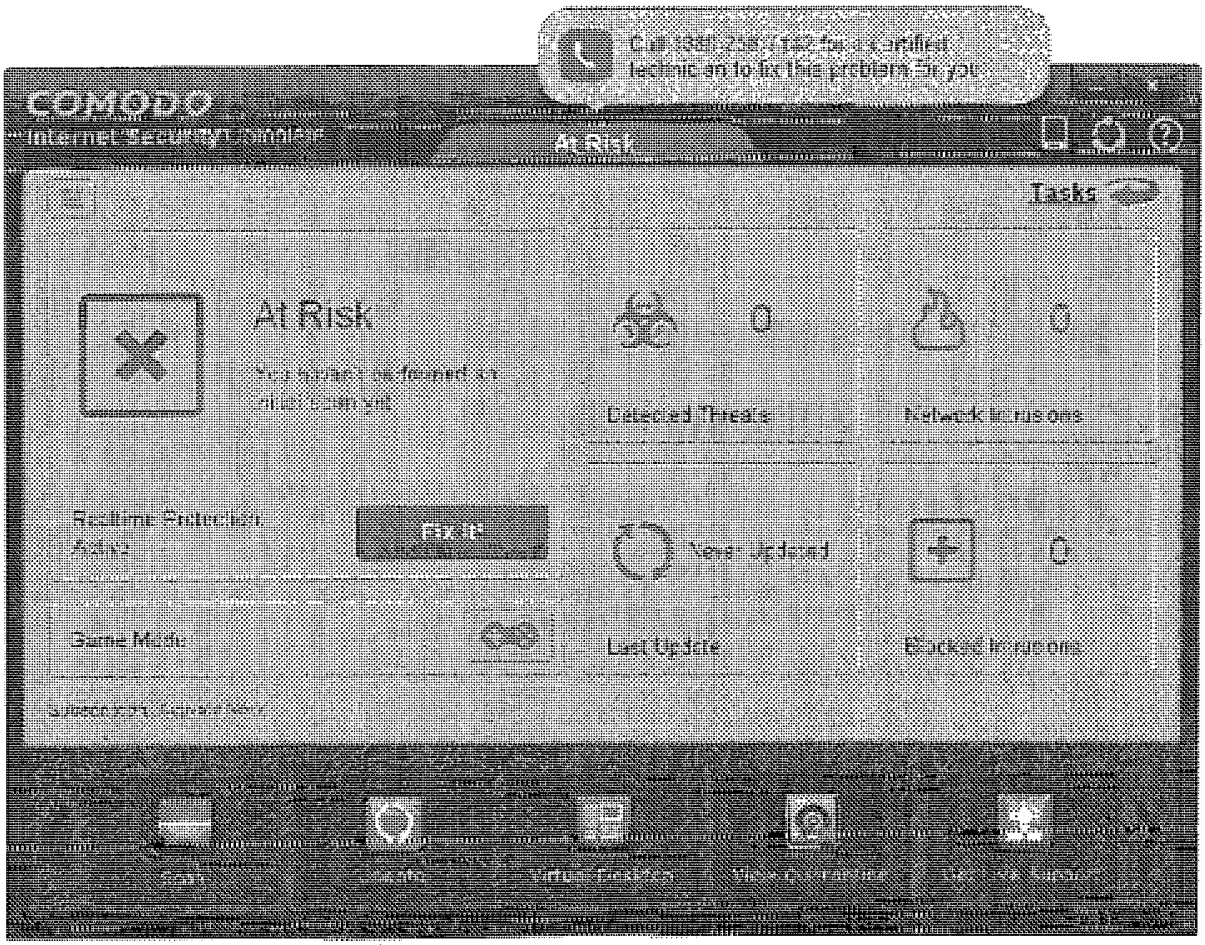

This screen will appear every time you start your system. If you do not want the screen to be displayed on every start up, select the check box 'Do not show this window again' before closing the window.

If your computer is connected to a home or work network, then you are prompted to configure it at the 'New Network Detected!' dialog. At the top of the dialog, the connectivity mode will be displayed, whether wired or wireless.

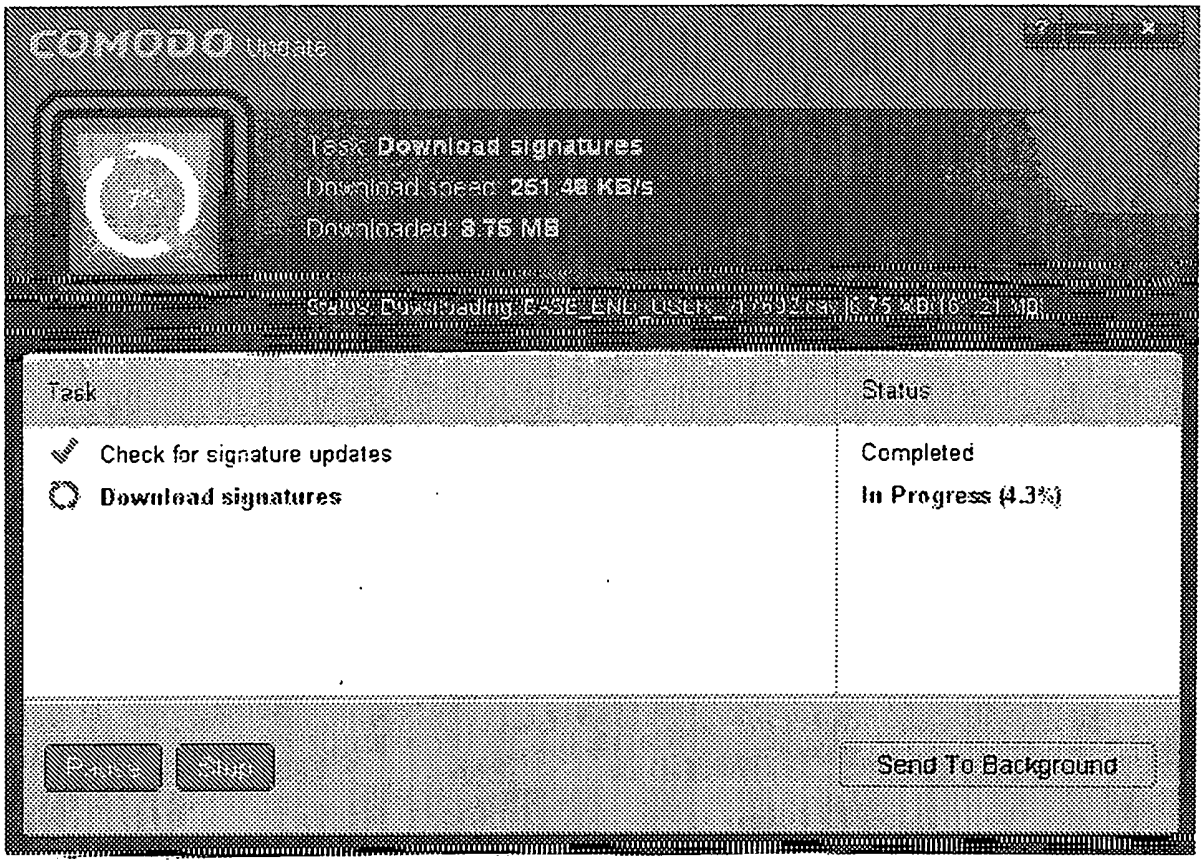



- Select your location from the three options
- Select 'Do not automatically detect new networks' If you are an experienced user that wishes to manually set-up their own trusted networks (this can be done in 'Network Zones' and through the 'Stealth Ports Wizard').

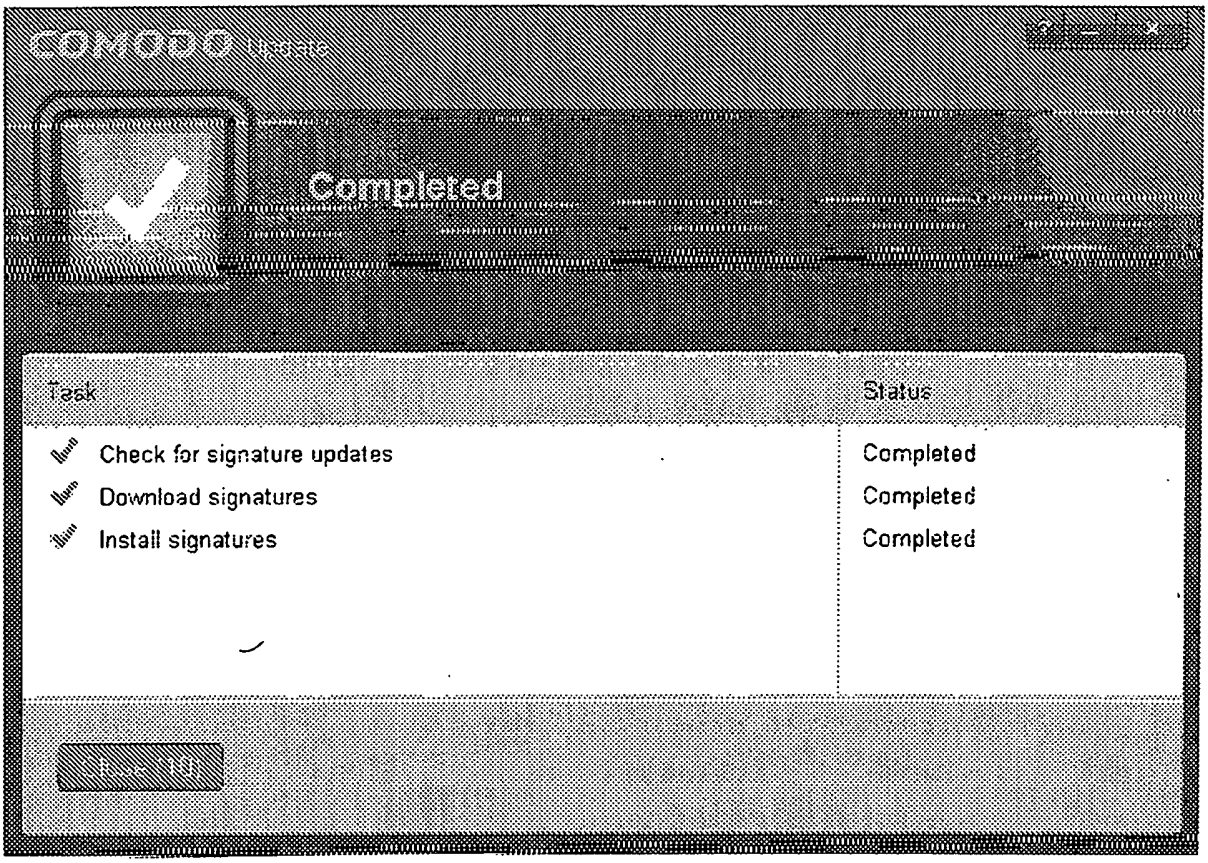
The main interface will be displayed:



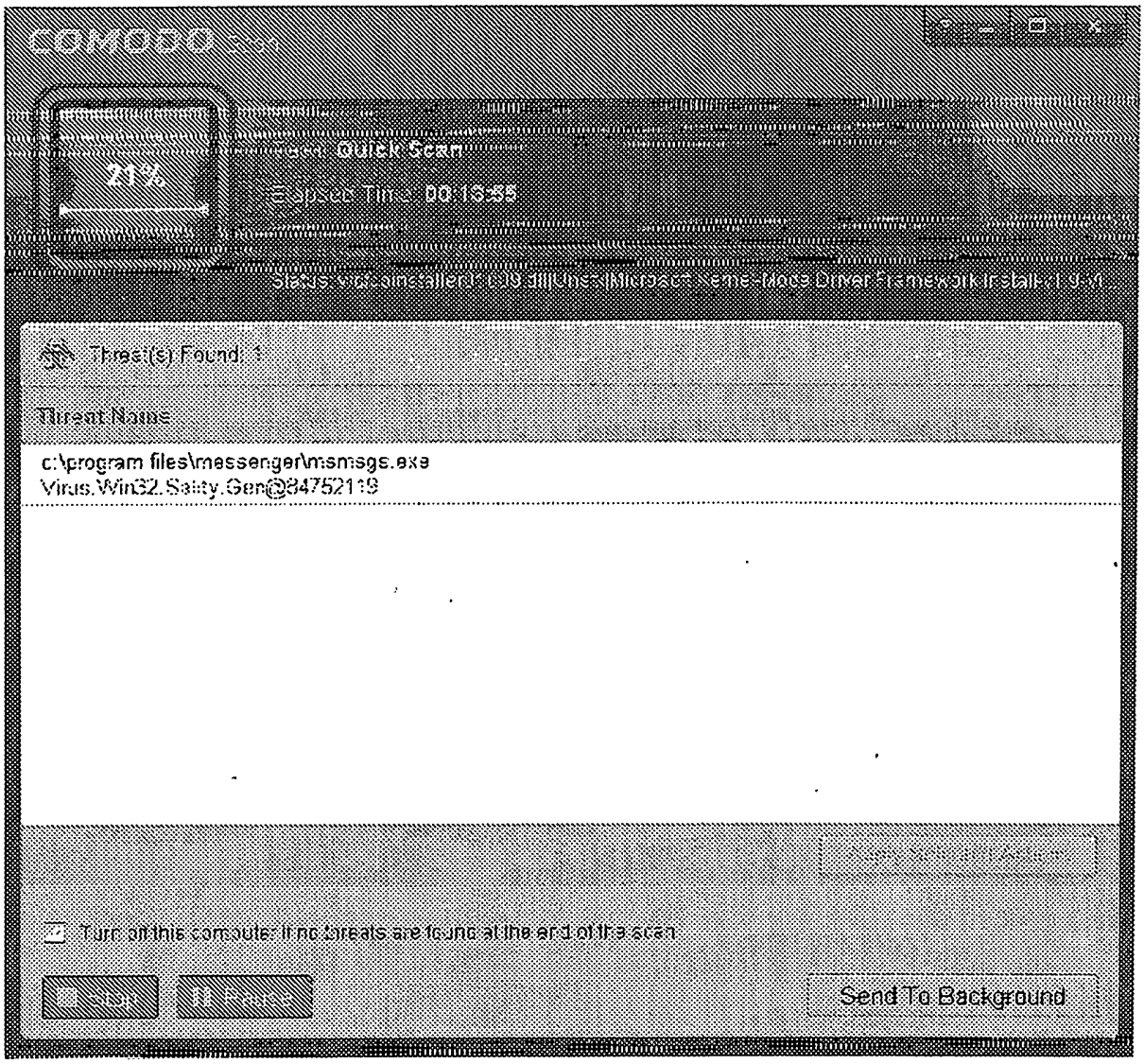

CIS will start its first virus database update at the background. You can view the progress by bringing the update task to foreground from the Task Manager interface. Refer to the section 'Manage CIS Tasks' for more details.




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

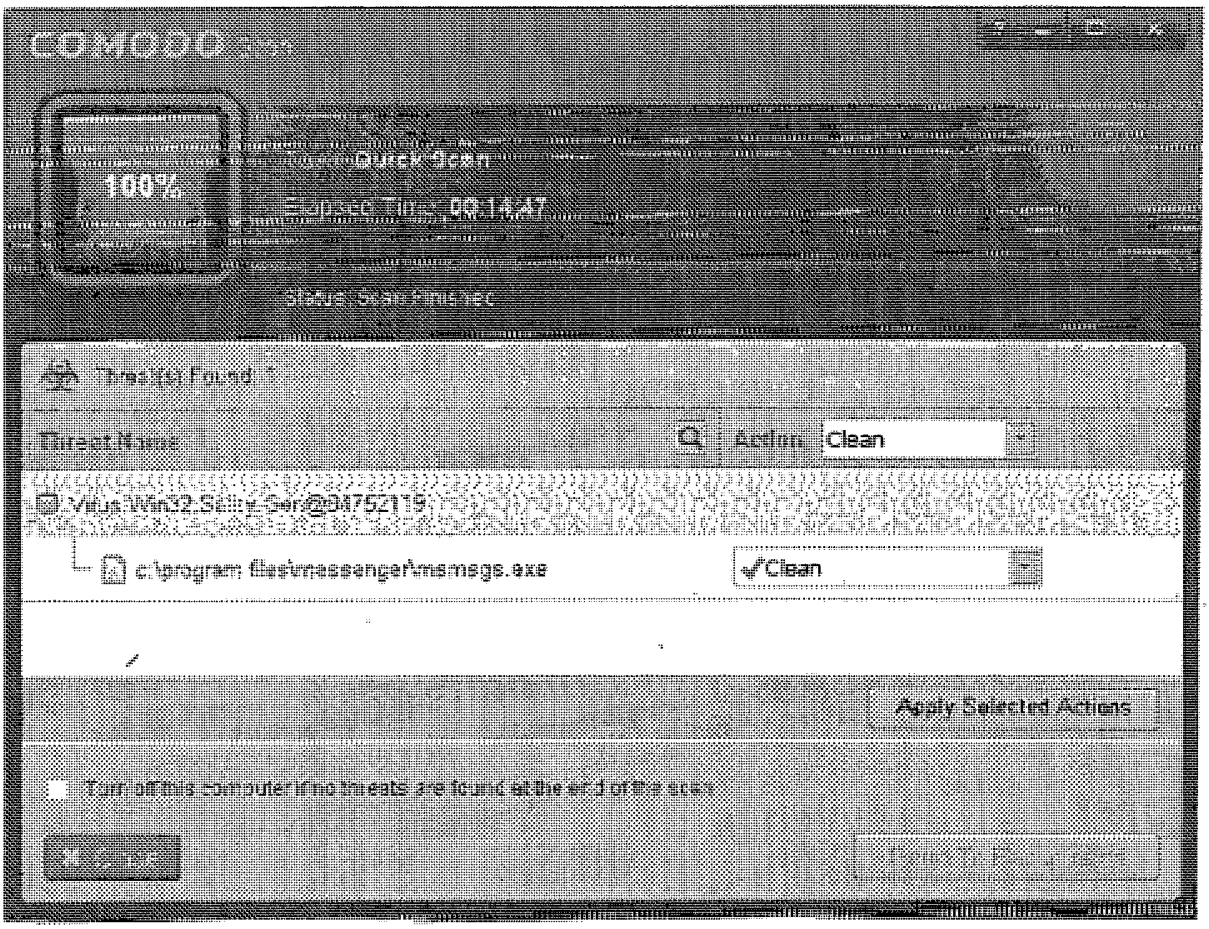



CIS will commence a Quick Scan of system memory, autorun entries, hidden services, boot sectors and other critical areas automatically after the virus database has been updated.




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

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




If any threats are detected, they will be displayed and you can choose to take appropriate action from any of the drop-down fields in the screen and click 'Apply Selected Actions' button. Refer to the section 'Processing Infected Files' for more details.

Important Note: After successful installation, you need to activate the license for using the product. In order to get your guarantee coverage and TrustConnect service enabled, you need to activate the license first.

- For full explanation on activation of license after installation of the product, refer to Activating Your License.
- For full explanation on activation of your guarantee, refer to Activating Your Guarantee Coverage.

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

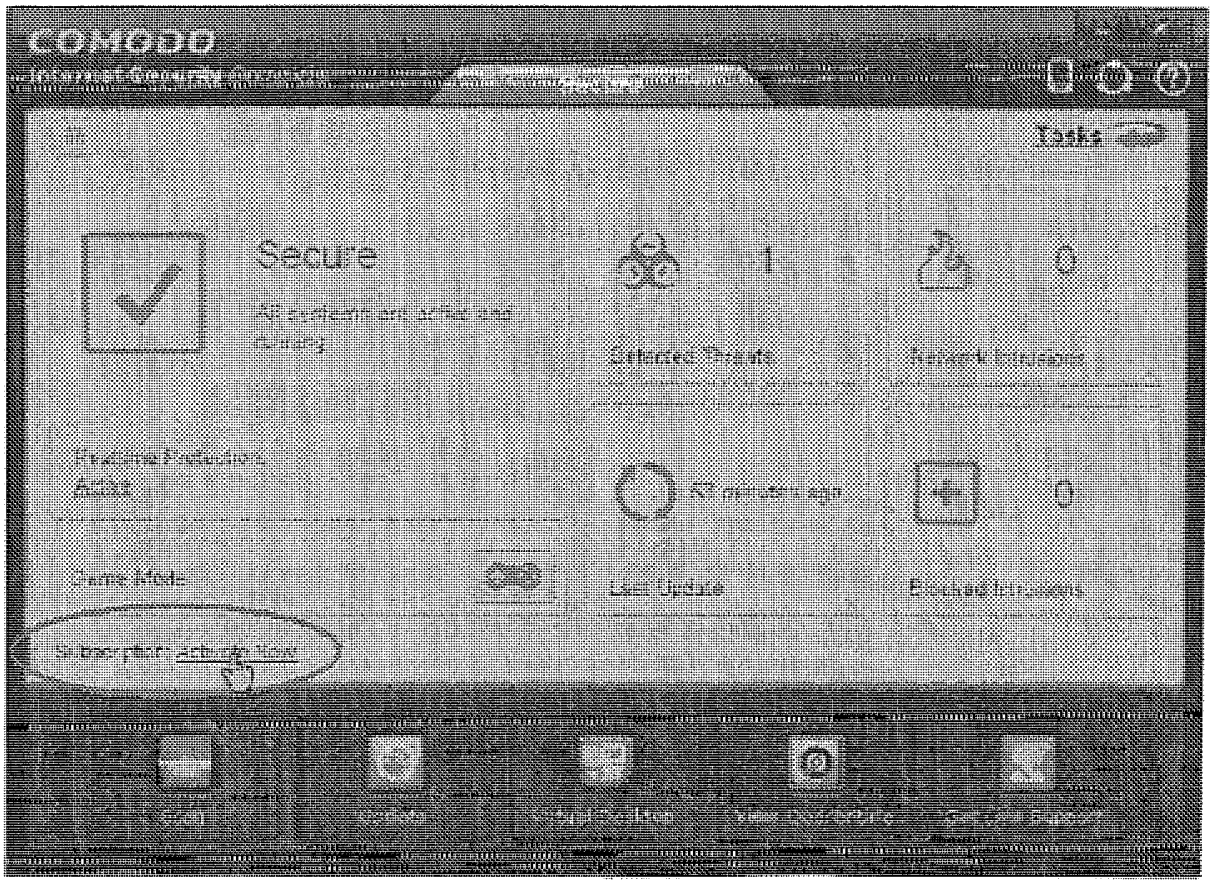
CIS Pro and CIS Complete should be activated after installation for continued use of the product. You will get alerts to activate the license if it has not been done so.

- Activating Your License;
- Activating Your Guarantee Coverage;
- Renewal of Your License.

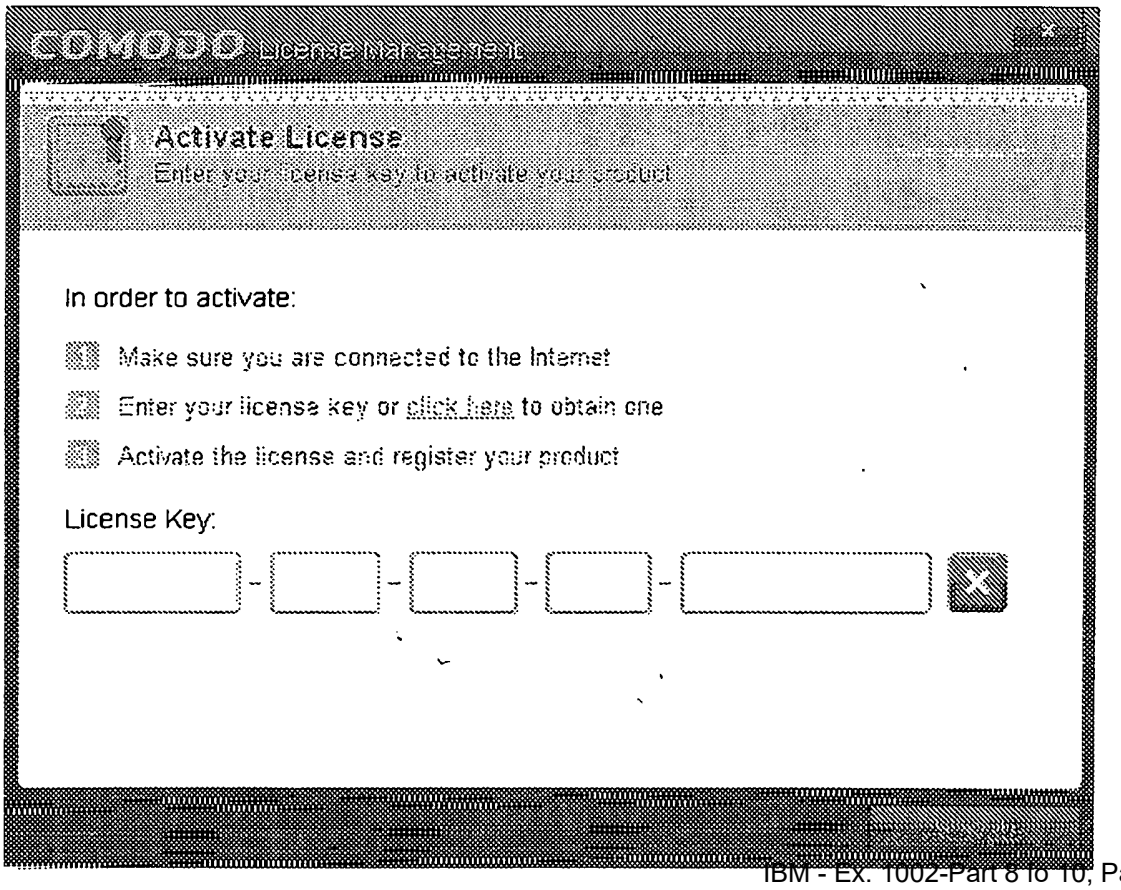
### 1.3.4.1. Activating Your License

- Start the Comodo Internet Security application as explained in the section Starting Comodo Internet Security.

**Step 1:** To activate your License, click 'Activate Now' beside 'Subscription' in the home screen.

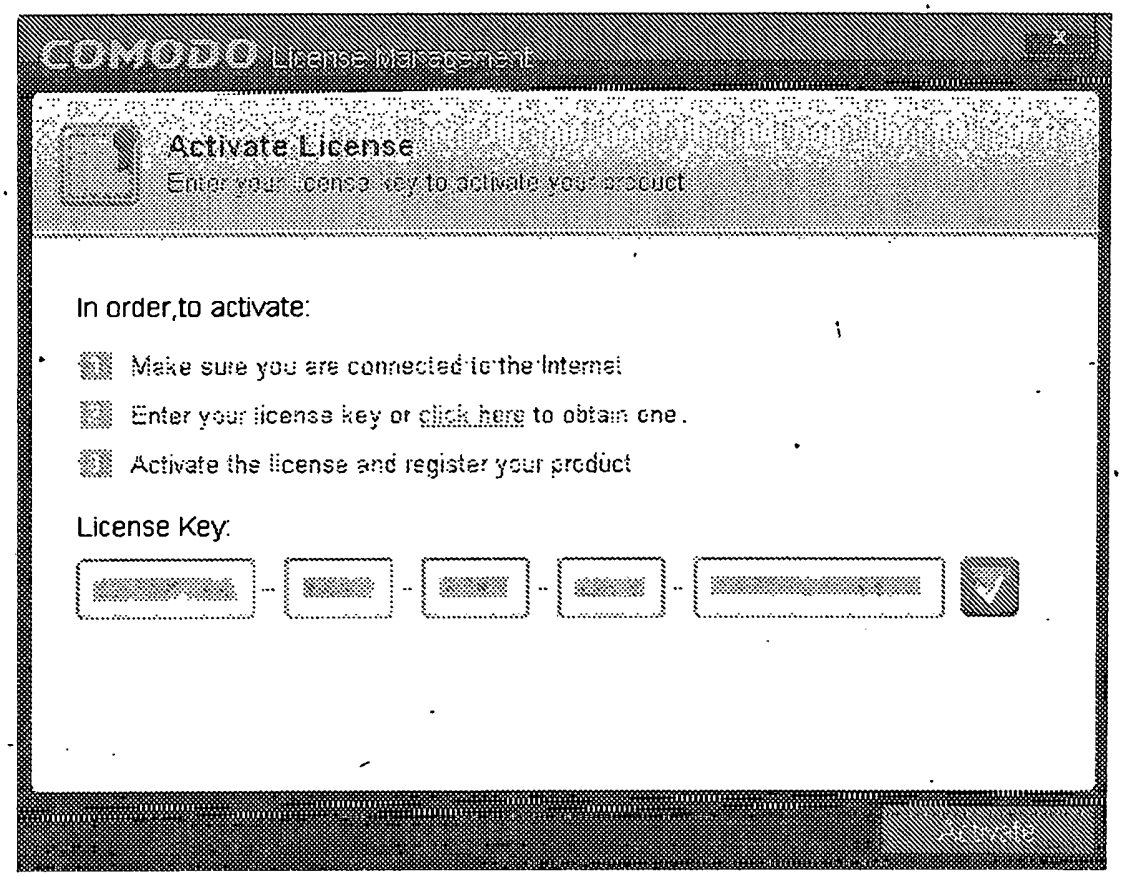



The License Activation Wizard will start.

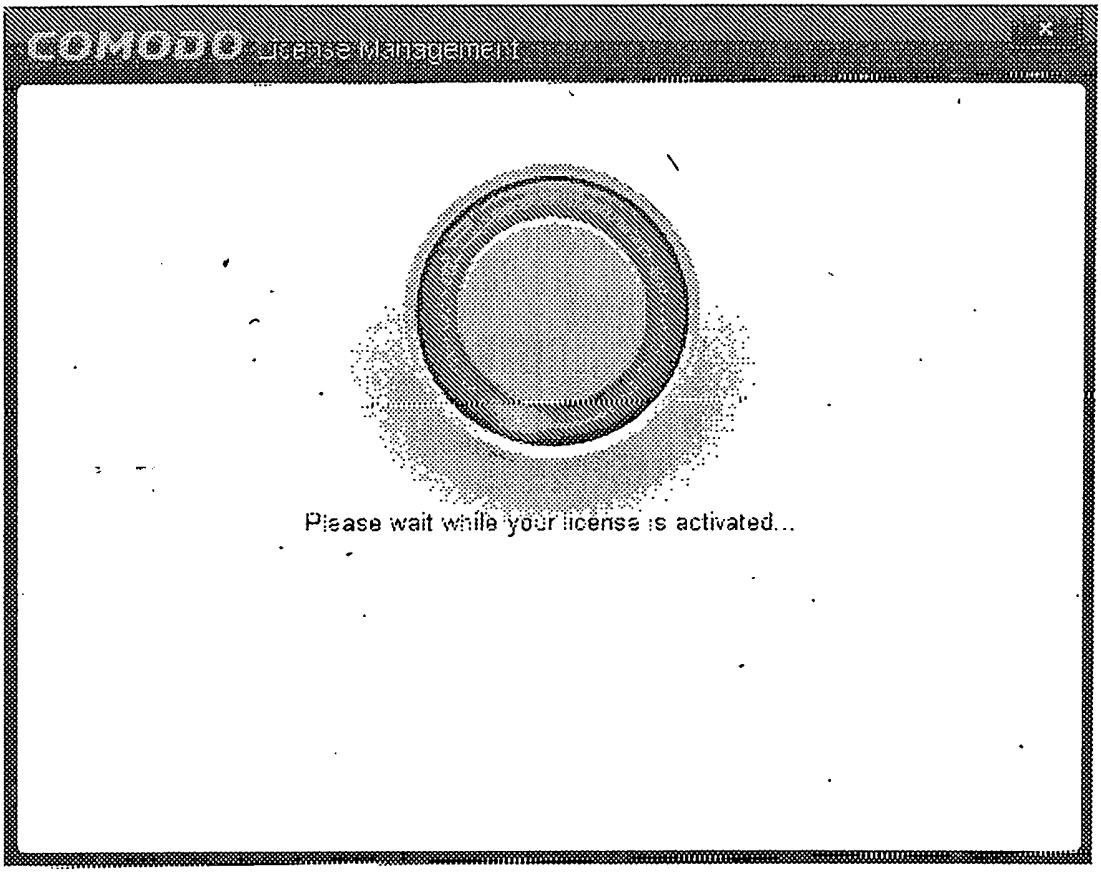


- You should have received your License key through email if you have purchased CIS Pro. For CIS Complete, the license key is available on the DVD itself or printed on an insert included in the box packaging. Enter the license key and click 'Activate'.

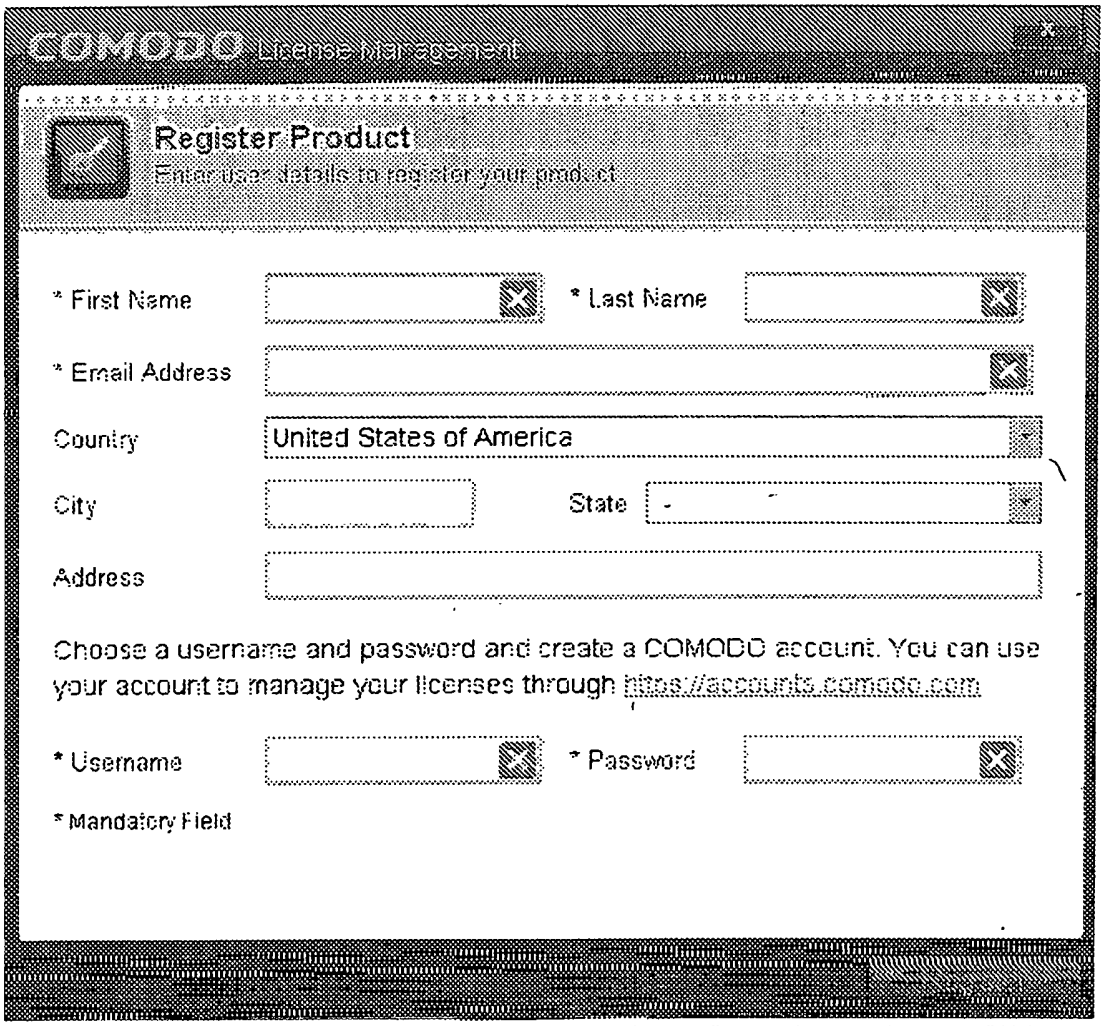
Tip: If you haven't subscribed for Comodo Internet Security - Pro or Complete so far, click the 'click here' link. You will be taken to the Comodo website enabling you to purchase the license.



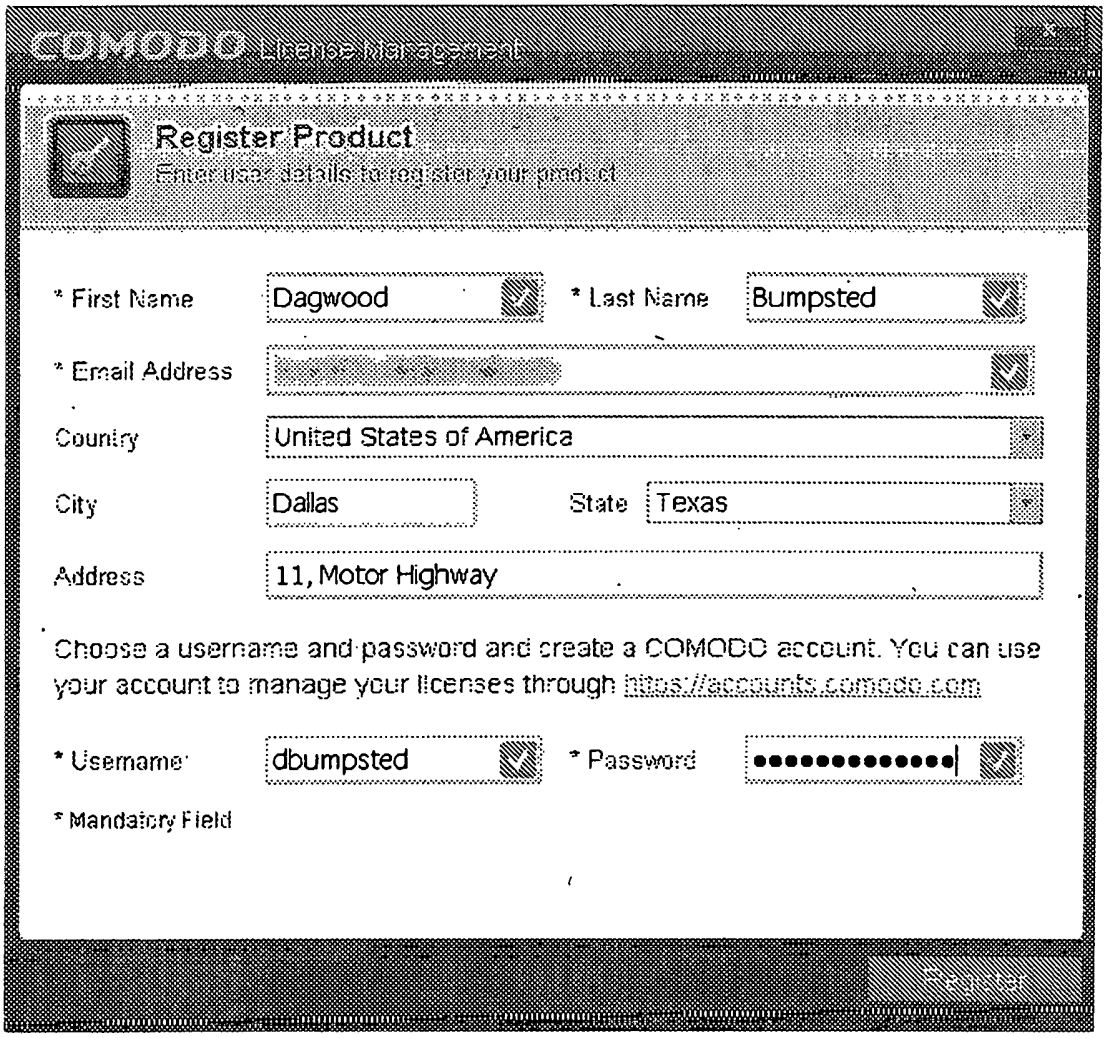

- The wizard starts validating your key.




If you have not registered as an user in Comodo Accounts Manager (CAM), the following screen will be displayed.



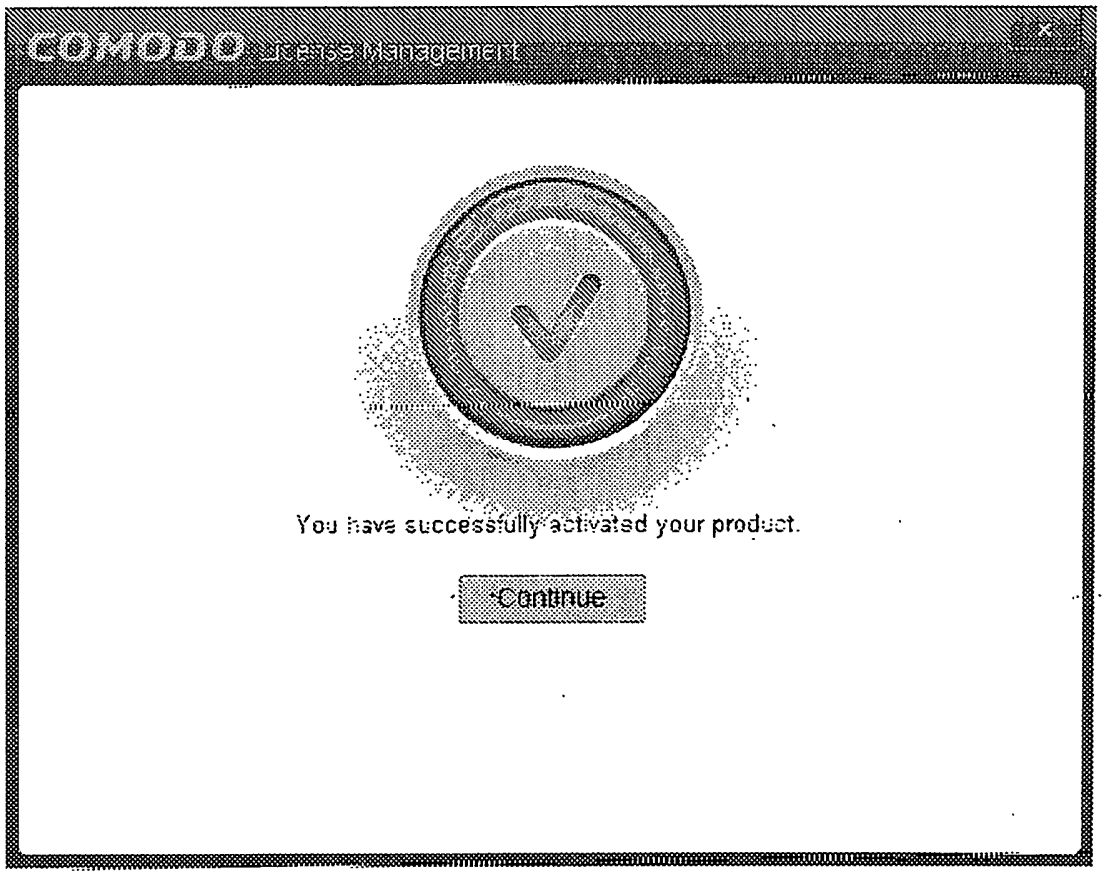

- Fill up the registration form with the login details and password for your Comodo Accounts Manager (CAM) account.




| Field | Description |
|---|---|
| Name | Enter your first name |
| Last Name | Enter your last name |
| Email | Enter your email address |
| Address | Enter your address |
| City | Enter your city name |
| Country | Select your country from the drop-down box |
| State | Select your state from the drop-down box |
| Address | Enter you full address |
| **Create a new COMODO Account** | |
| • Enter your username and password to create a new Comodo account with Comodo Accounts Manager (CAM) | |

- Click 'Register'

On successful validation, your subscription will be activated and a confirmation screen will be displayed.




- Click 'Continue' to exit the wizard.

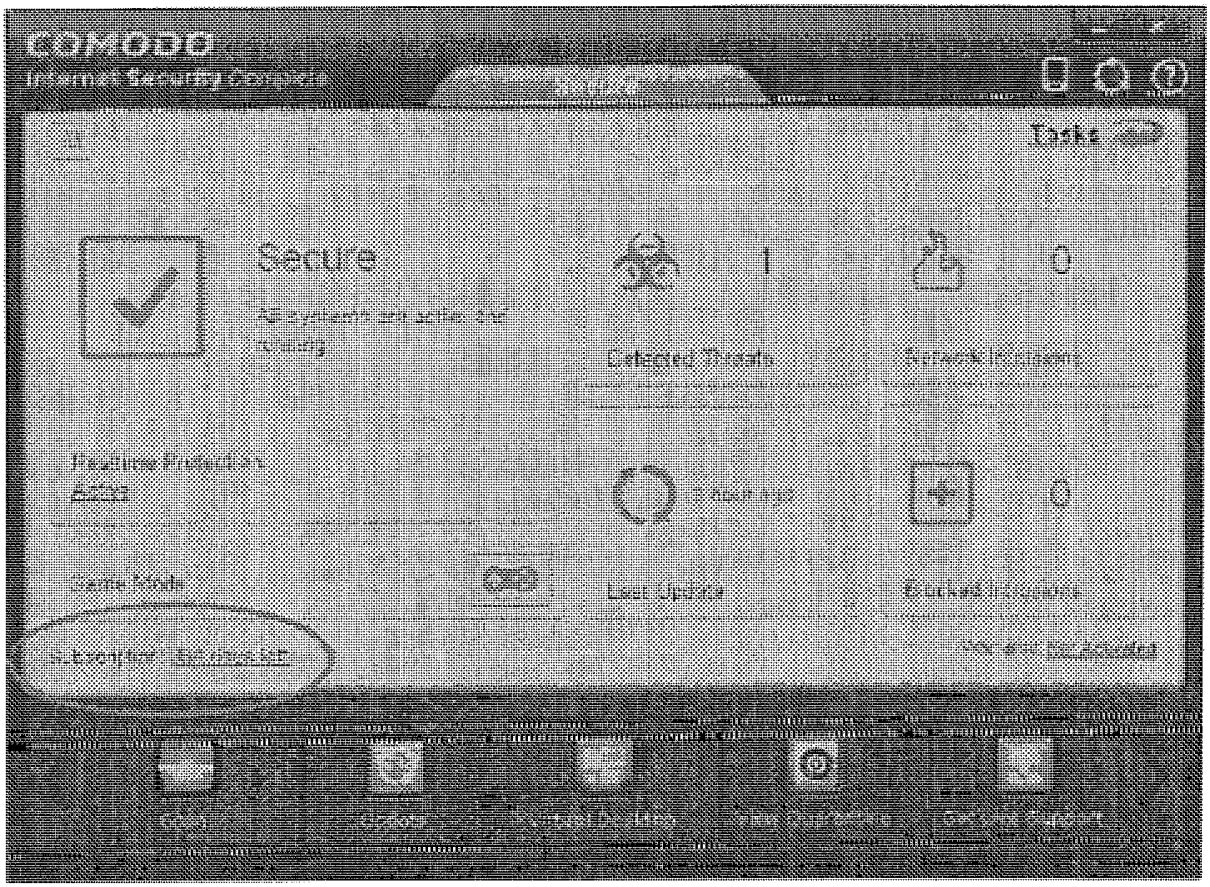
For CIS Pro users - Your CIS Pro product will be activated.

For CIS Complete users - Your CIS Complete product will be activated along with Comodo Backup and TrustConnect

- Accessing Comdo Backup online storage space - Use the login credentials provided during the CIS Complete registration step.
- Using the TrustConnect service - The TrustConnect service will be automatically enabled after successful activation of the license. Please refer to the section TrustConnect Overview for more details on how to use the service.

Tip: You can also enter your activation key by clicking the link 'Enter a license key' in the About dialog, accessible by clicking Help icon > About from the title bar.

The main interface will display the number of days left for the license before it should be renewed.




## 1.3.4.2. Activating Your Guarantee Coverage

The Comodo Guarantee is available to customers of CIS Pro and CIS Complete versions. Before enabling guarantee coverage, customers should first have activated their licence. Full details on activating the license can be found in Activating Your License section.

- Please note that if you wish to use and activate the Comodo guarantee then you must have installed Comodo Internet Security (both Antivirus and Firewall components) and Comodo GeekBuddy. You must also have run and passed a Comodo Antivirus scan using the latest signature database. Please see the End User License Agreement (EULA) for full details.

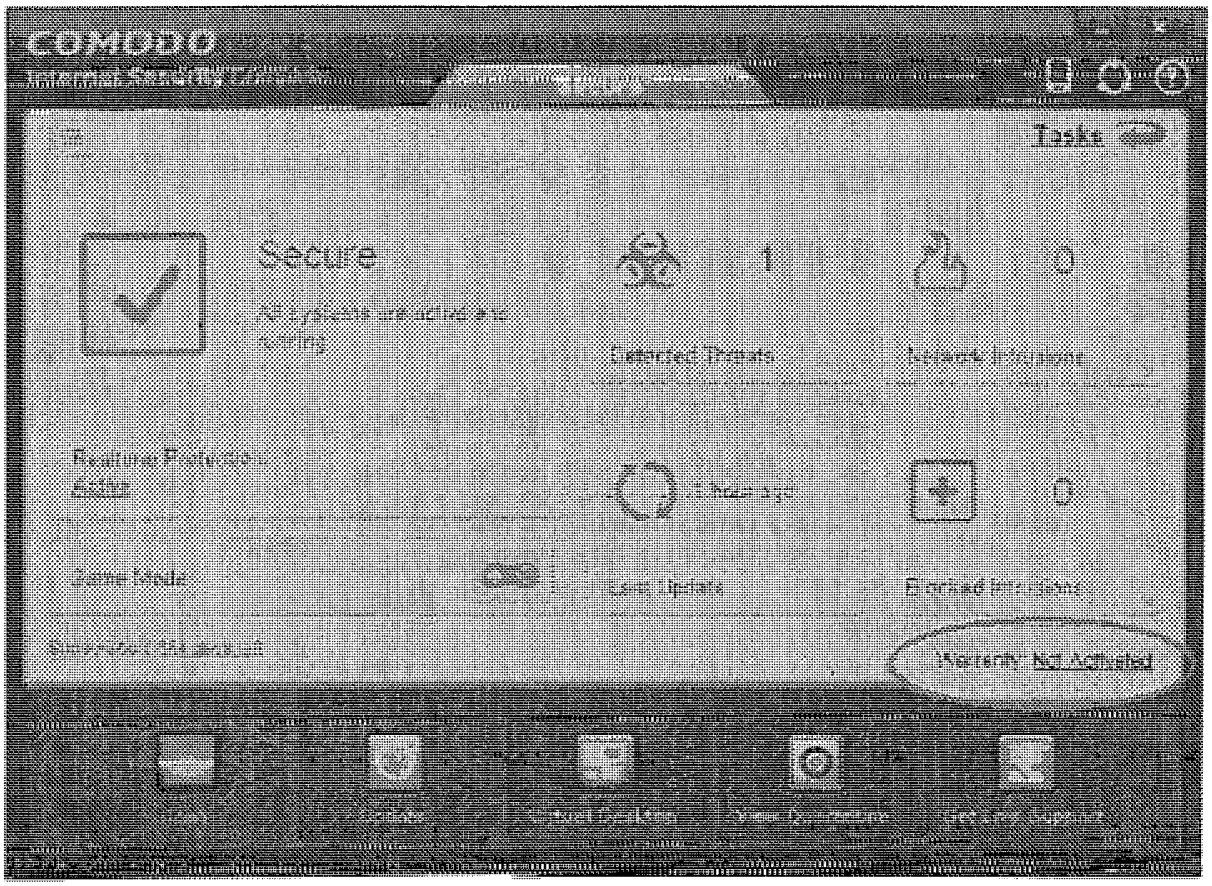
**Limits:** The guarantee is limited to the lesser of:

- The actual cost of the computer;
- An aggregate total of $500 for all claims paid under a single license key, and
- The actual cost of a Comodo specified and authorized third party provider to repair the computer to an operating condition ('Guarantee Limit').

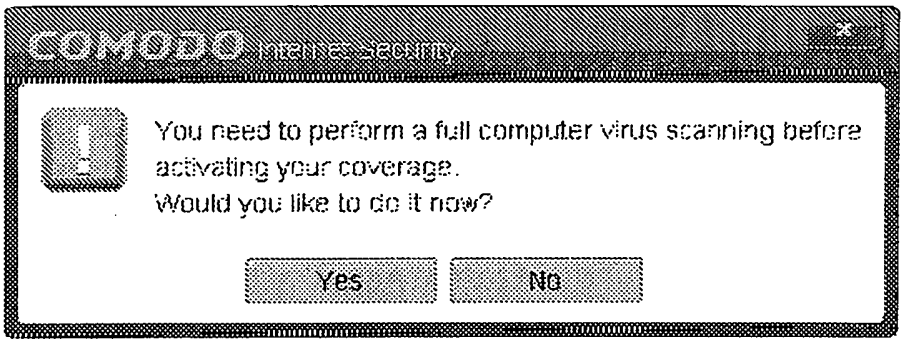
- The guarantee is limited to repairing the computer over the Internet to an operational state and excludes all claims for lost or expected profits, lost or corrupted data, lost or deleted work, or lost or damaged personal files. Comodo does not guarantee against the loss of any file or information. The guarantee is void if you breached this agreement, failed to follow the procedures described in this Section 3 of the EULA or failed to pay any fees applicable to your use of the Software.
- Full Terms and Conditions on the Comodo Guarantee Coverage can be read in Section 3 of CIS EULA (Step 2 of the Installation process for CIS Pro and Step 1 for CIS Complete).

more details on running an Antivirus Scan Click here.

**Step 1:** To activate your guarantee coverage, click 'Not Activated' beside 'Warranty' in the home screen.



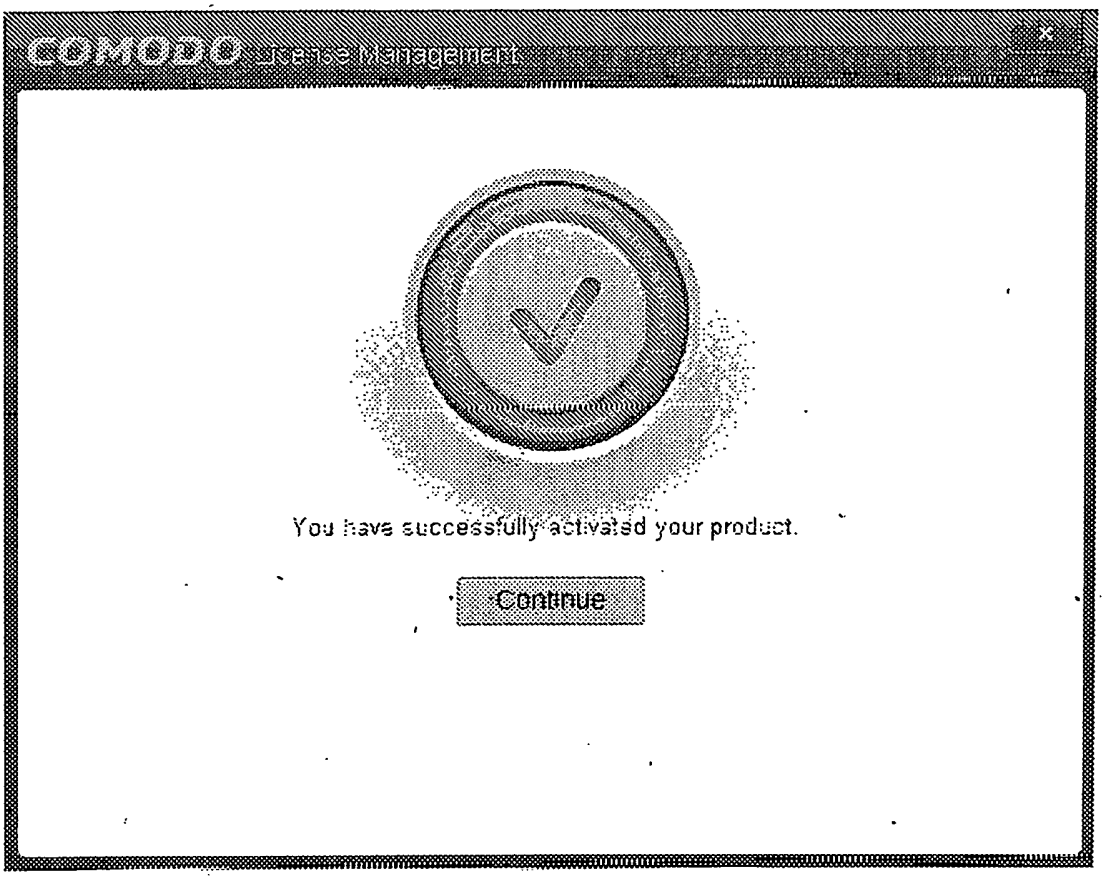

A full system scan to remove all known viruses is a mandatory requirement if your computer is to be eligible for guarantee coverage. If this step has already been performed (and your system is clean), then the process moves to step 2.




Click 'Yes' to run a full computer scan. Refer to the section Run a Full Computer Scan for more details on scanning your full computer and cleaning the infected files. All the infections and threats identified during the scan should be cleaned for your computer to be qualify for the warranty.

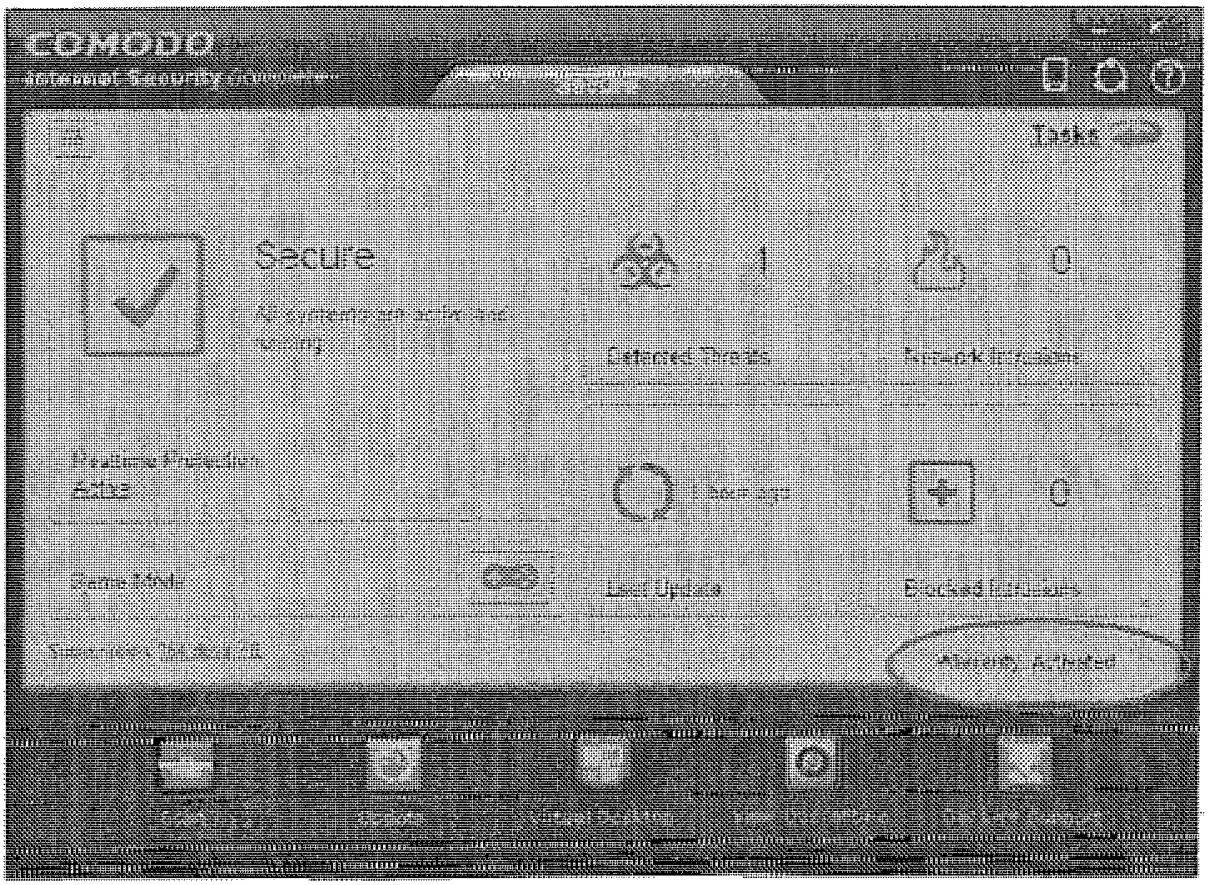
**Step 2:** The next stage is to run the Guarantee Activation Wizard again.

- Click 'Not Activated' beside 'Warranty:' again. The Guarantee Activation Wizard will start and on completion the 'successfully activated' screen will be displayed.




- Click 'Continue' to complete the activation wizard

Successfully activating your Guarantee will change the information displayed beside 'Warranty:' in the Home screen.

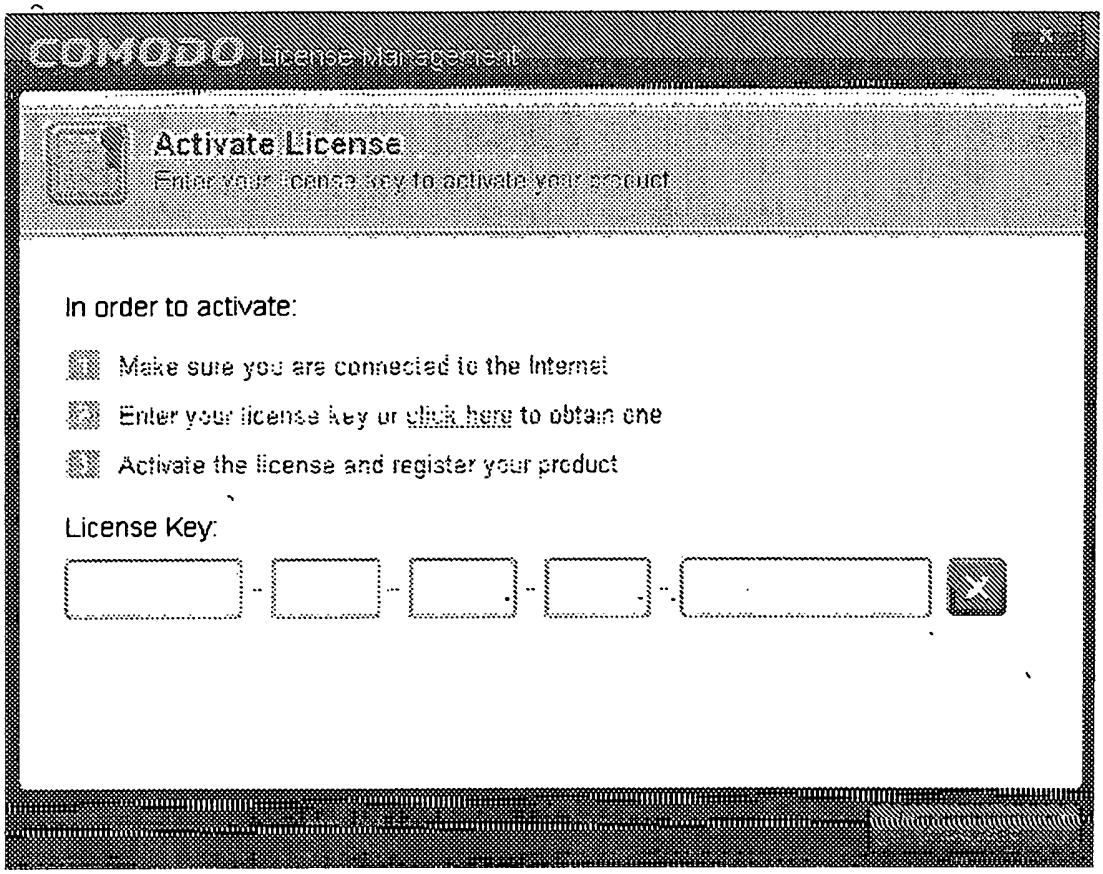



## 1.3.4.3. Renewal of Your License

In order to enjoy continuous services from Comodo after the license period of your CIS Pro/Complete has expired, you need to renew your License.

To renew or upgrade your license, click the 'Activate Now' link beside 'Subscription' on the CIS home screen (alternatively, click 'No. of days left').

The Product Activation Wizard will start.




- Click the 'click here' link. You will be taken to https://secure.comodo.com/home/purchase.php?afi=Comodo&rs=7&pid=9&cid=RkJEMUZENjMzQUM4RDIDNDE4MzBDQjc1NDIENUIzRkY&lid=&.
- Select your CIS Package.
- Select 'returning user' in the 'Sign-up Information' area, enter your login and password and complete the payment procedures.
- The License key will be sent to you by email. Activate your License using the new key to enjoy the continued services.

# 1.4. Starting Comodo Internet Security

After installation, Comodo Internet Security automatically starts whenever you start Windows and the CIS Widget will be displayed. In order to configure and view settings within Comodo Internet Security, you need to access the main interface.

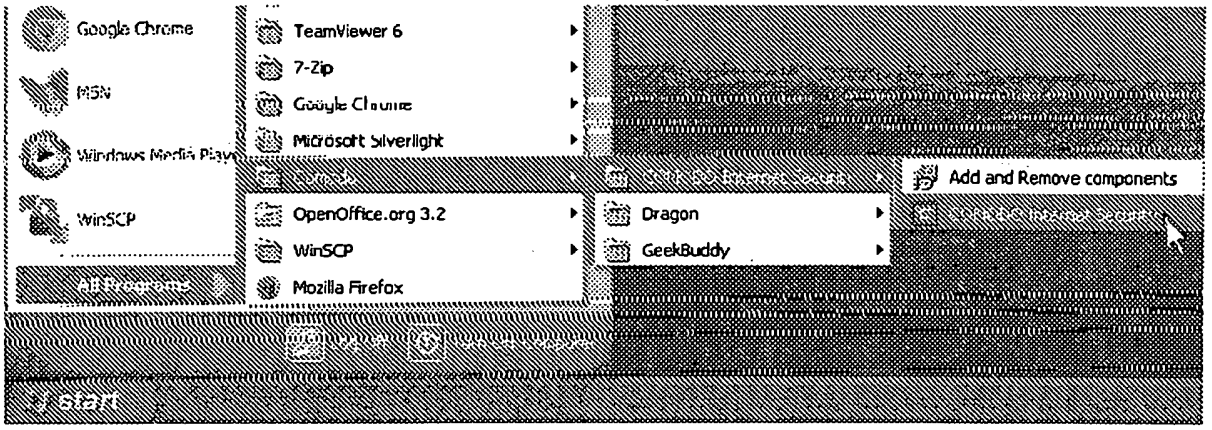
There are 4 different ways to access the main interface of Comodo Internet Security:

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

Start Menu

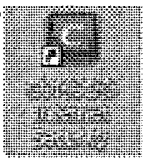
You can access Comodo Internet Security via the Windows Start Menu.

- Click **Start** and select **All Programs > Comodo > COMODO Internet Security > COMODO Internet Security.**



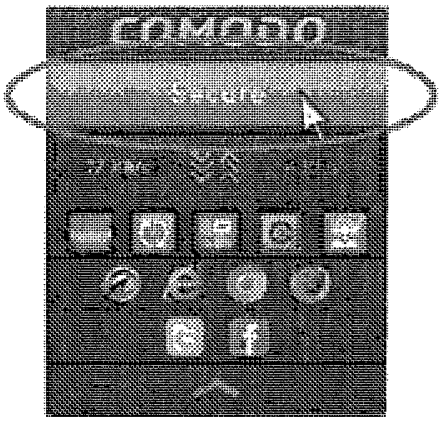

### Windows Desktop

- Just double click the shield icon in the desktop to start Comodo Internet Security.



### Widget

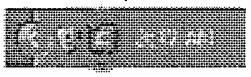
- Just click the information bar in the widget to start CIS.



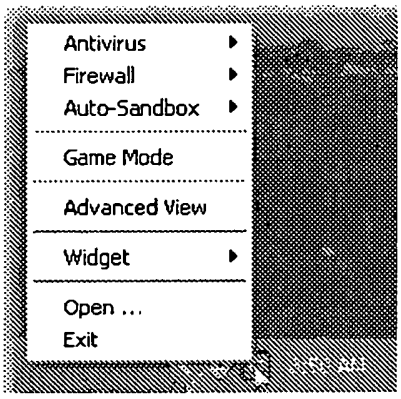
You can also view other details in the widget such as inbound and outbound traffic, number of tasks running, shortcuts to common CIS tasks and browsers and links to social media sites Twitter and Facebook. Refer to the section 'The Widget' for more details.

### CIS Tray Icon

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



By right-clicking on the tray icon, you can access short cuts to selected settings such as enabling or disabling Antivirus real-time scan, Firewall, Behavior Blocker, Widget, Game Mode option and switch the CIS to Advanced or Compact View.




**Game Mode** - Switches CIS to Game Mode to enable you to play your games without any interruptions from various alerts in your computer. The operations that can interfere with users' gaming experience are either suppressed or postponed.

In game mode:

- Defense+/Firewall alerts are suppressed as if they are in training mode;
- AV database updates and scheduled scans are postponed until the gaming is over;
- Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Game Mode to resume alerts and scheduled scans.

**Widget** - Click here for more details on CIS Widget.

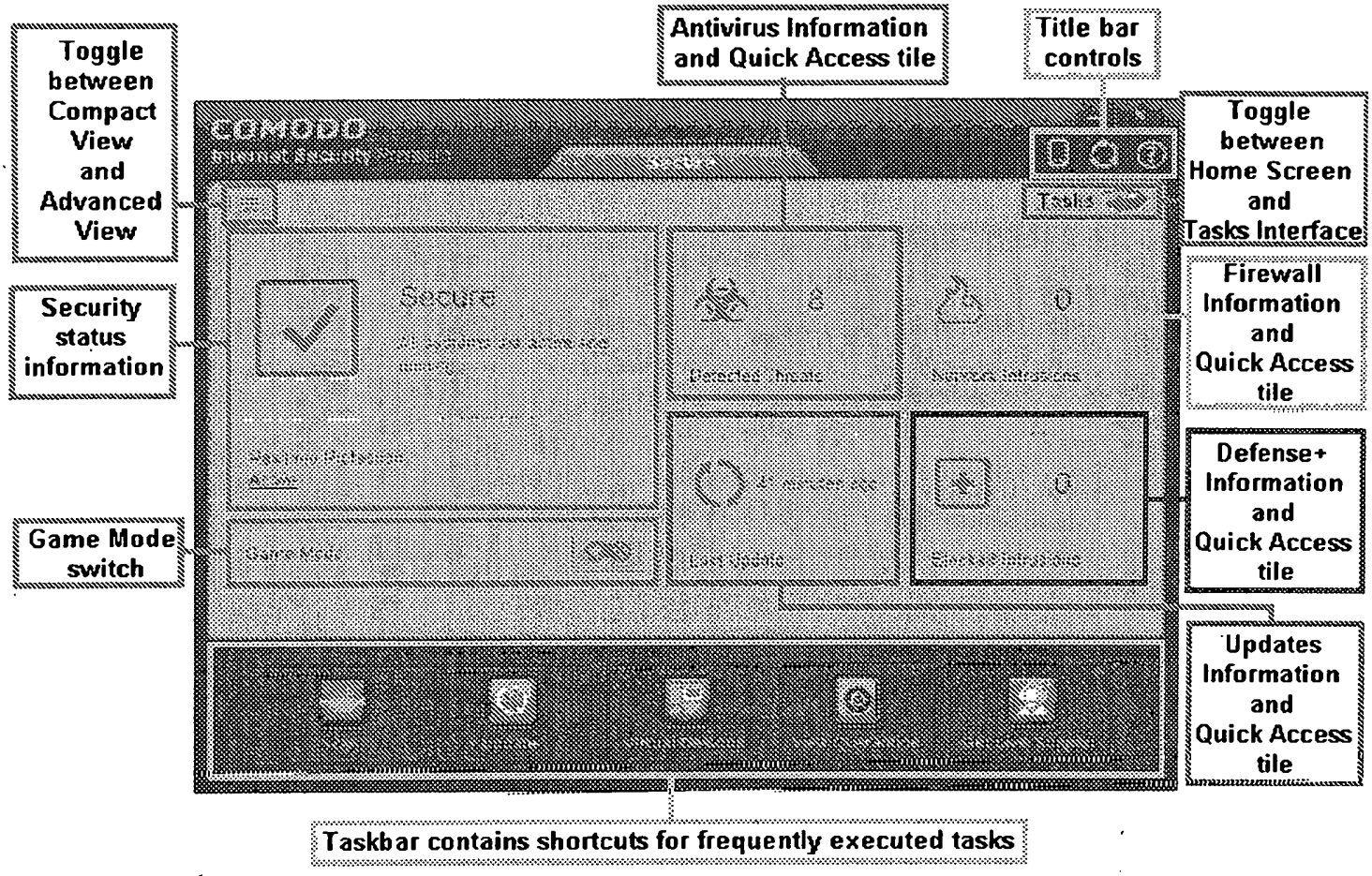
Refer to the section "The System Tray Icon for more details.

# 1.5. The Main Interface

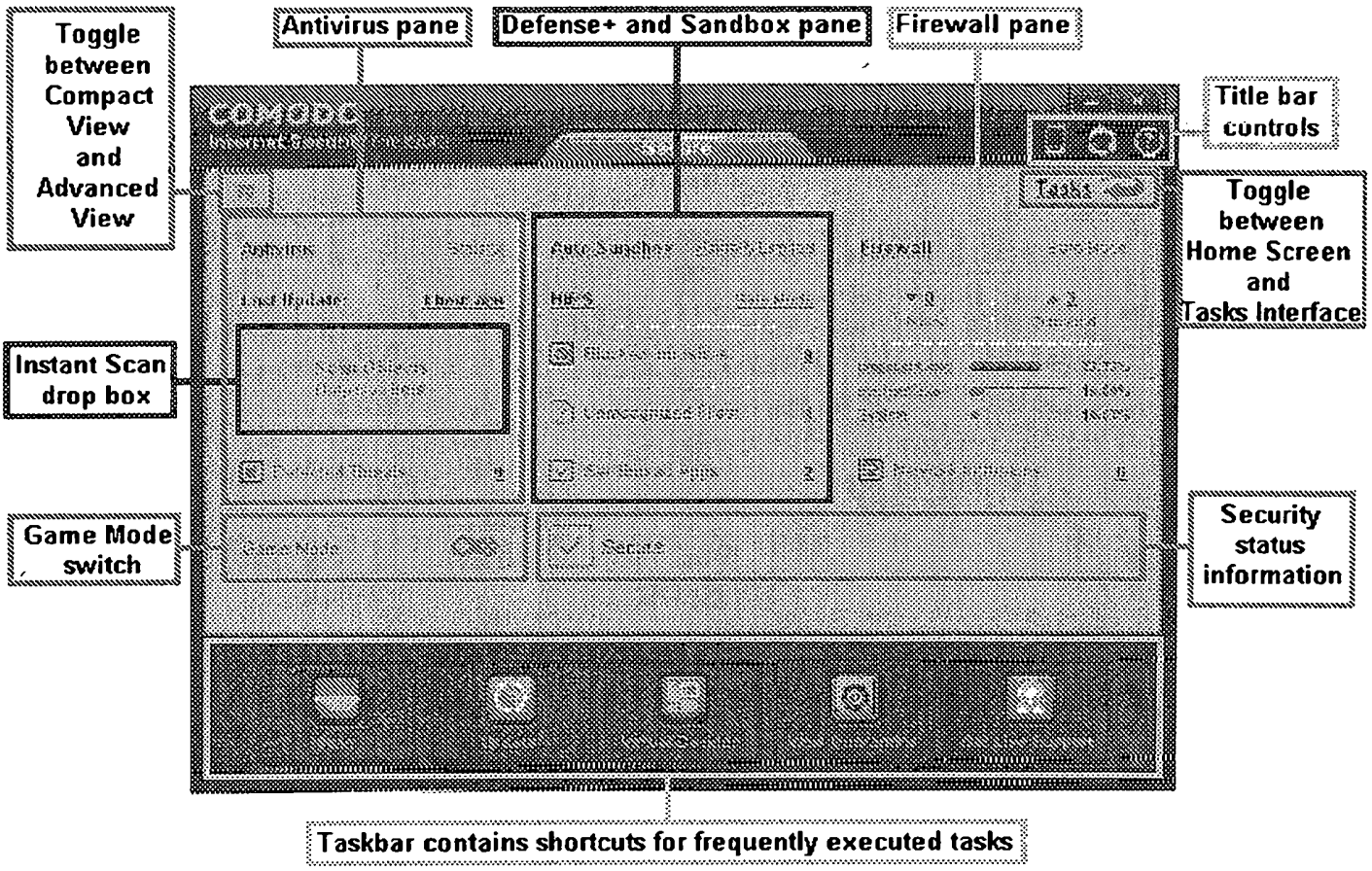
The CIS interface is designed to be as clean and informative as possible while letting you carry out any task you want with the minimum of fuss. Each tile on the home screen contains important security and update information and allows you to quickly delve further into areas of interest.

- Click the curved arrow at the upper right to switch between the home screen and the tasks interface.
- Instantly run a virus scan on a file or folder by dragging it into the scan box.
- Switch on 'Game Mode' to make sure nothing interrupts you while you play a full screen game.
- Change the entire look and feel of the home screen from Advanced Settings.
- The Task Bar at the bottom of the home screen allows one-click access to important features such as the antivirus scanner, the Virtual Desktop, the update checker and the CIS Task Manager.
- Flip between 'Compact View' and 'Advanced View' by using the toggle button at the upper left  or from the system tray icon

Compact View



Advanced View




The advanced view shows antivirus, firewall and sandbox activity in greater detail. This includes the number of detected threats, last virus database update time, number of inbound and outbound connections and more.

This view also allows you to quickly change security settings for each component.

Click the following links for more information:

- The Home Screen
- The Tasks interface
- The Widget
- The System Tray Icon

## 1.5.1. The Home Screen

You can switch the display between the 'Home' screen and the 'Tasks' interface by clicking the green arrow at the upper right of the interface:

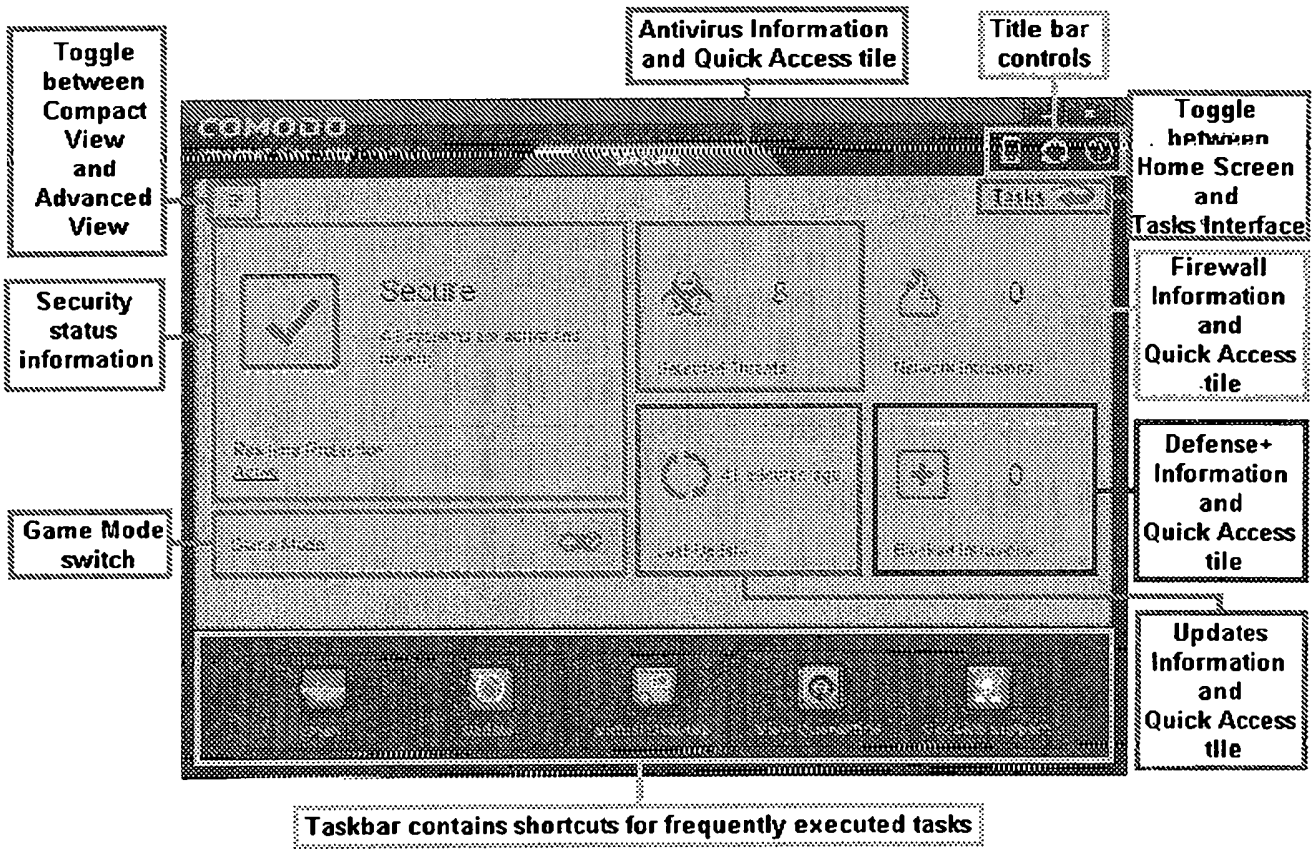
The home screen itself is available in two formats, 'Compact' view and 'Advanced' view. Use the button at the top-left to switch between them.

The following areas are common to both compact and advanced views:

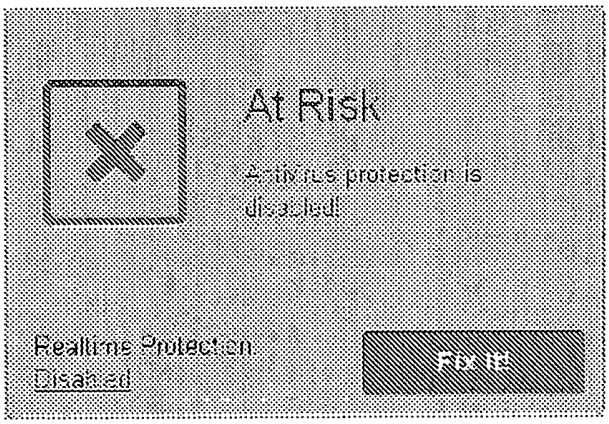
- Adding tasks to the Task Bar
- Title bar controls
- Game mode

## Compact View

Compact View presents a simple, easy to understand interface that allows users to quickly launch key tasks and gain an immediate overview of the security of their computer. The large 'security information' tile on the left provides at-a-glance information on overall system security and allows you to run an appropriate CIS task if threats are found. The four tiles on the right provide information from specific CIS security components and act as shortcuts to run an instant antivirus scan, run an update, view network traffic and to configure sandbox/host intrusion settings.




The security information tile on the left will inform you if any component is disabled or any if other problems are found:



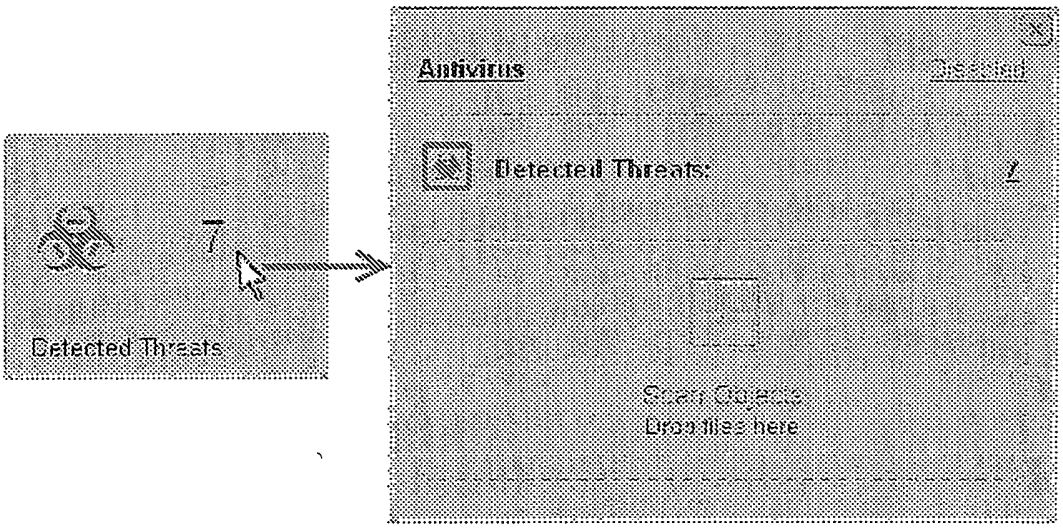
You can easily rectify the issue by clicking the 'Fix it!' button. CIS will automatically take necessary actions to resolve the problem.

From the Compact View of the home screen you can:

- Instantly scan objects
- Enable or disable security components

### Instantly scan objects

Click the 'Antivirus' tile in the middle of the (compact) home screen to open the drag-and-drop scanner:

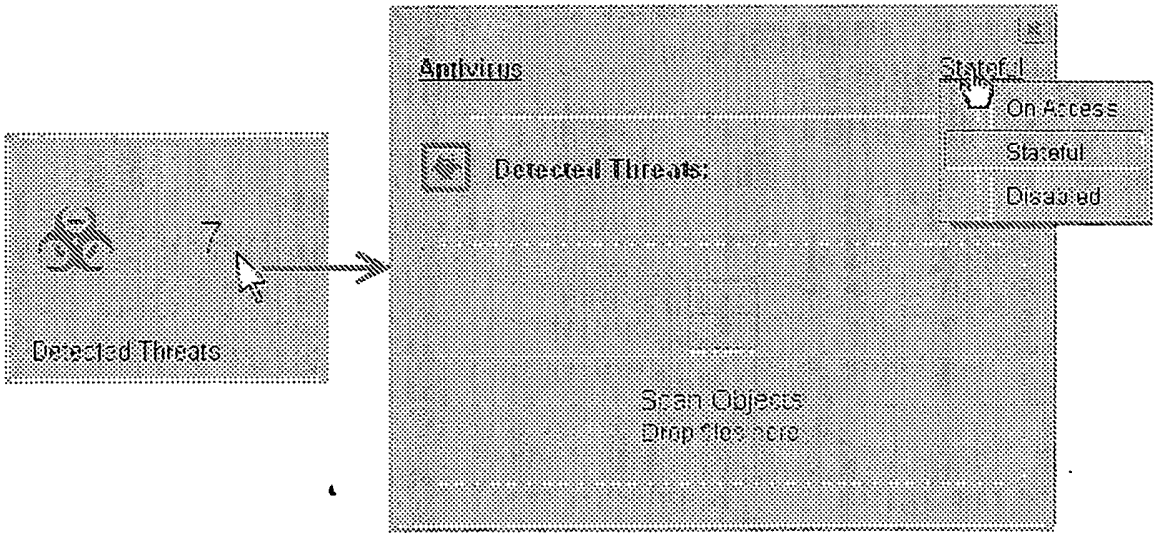



To run an instant scan, navigate to the file/folder that you want to scan and just drag-and-drop the file into the 'Scan Objects' box. The virus scan will commence immediately. Refer to 'Instantly Scan Individual Files and Folders' for more details.

### Enable or disable security components

The four tiles on the right can each be flipped to display more detailed information and options

- **Antivirus** - Click the Antivirus tile to flip open a more detailed tile which displays current antivirus settings, the number of detected threats and the drag-and-drop scanner.
  - Click the link at the top-right to quickly switch AV modes between 'On Access', 'Stateful' and 'Disabled'. Refer to the section 'Real-time Scanner Settings' for more details.

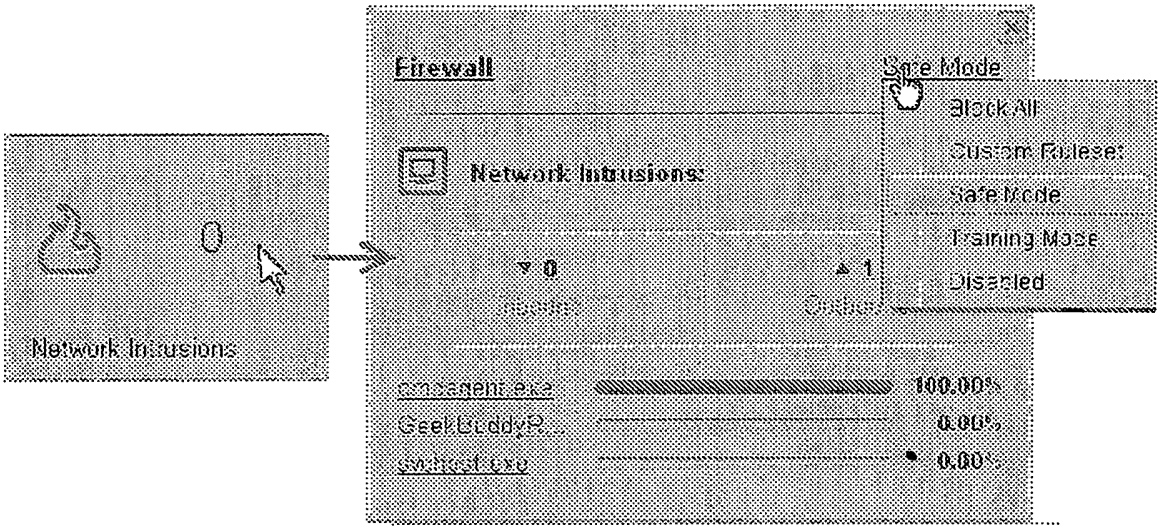



  - Click 'Antivirus' at upper-left to open the 'Realtime Scanner Settings' interface. Refer to the section 'Real-

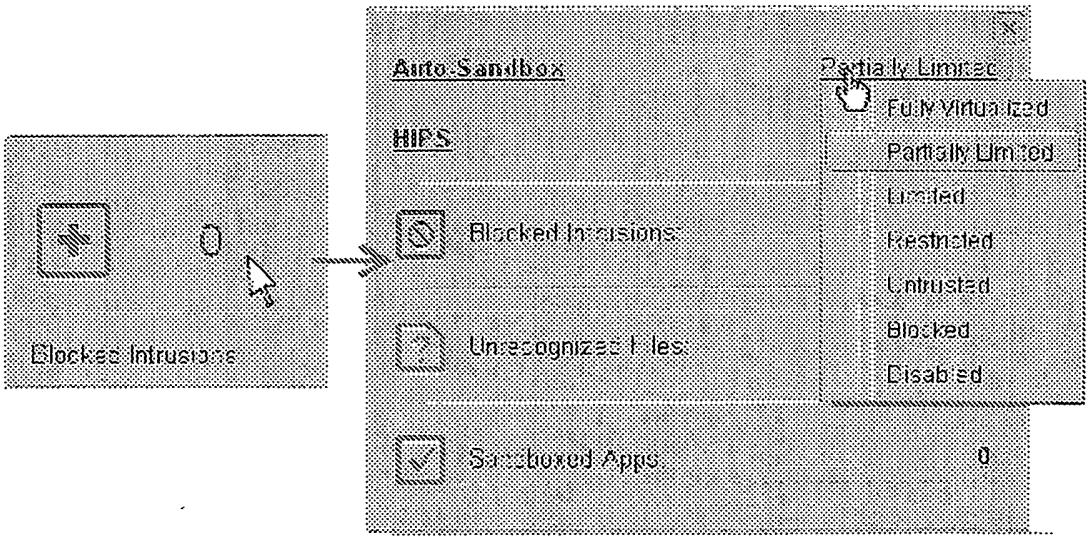
time Scanner Settings' for more details.

- Click the number of threats detected to open the Antivirus Log Viewer Module.
- Click the 'X' in the top right corner to return to the 4-tile view.

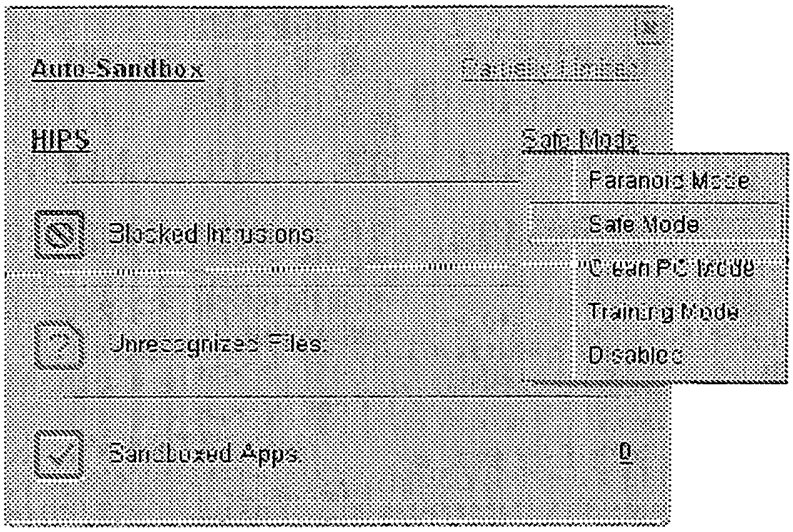
- **Firewall** - Click the Firewall tile to flip open a more detailed pane which displays the current firewall mode, the number of detected network intrusions, the number of current inbound and outbound connections and the share of network bandwidth used by internet-connected applications.
  - Click the link at the top-right to view or modify the current firewall mode. Refer to the section 'Firewall Behavior Settings' for more details.




  - Click 'Firewall' to open the detailed 'Firewall Settings' interface. Refer to the section 'Firewall Behavior Settings' for more details.
  - Click the number of detected network intrusions to open the Firewall Log Viewer Module.
  - Click the numbers over 'inbound' and 'outbound' to open the View Connections dialog. You can also do this by clicking the application names at the bottom of the pane.
  - Click the 'X' in the top right corner to return to the 4-tile view.
- **Defense+** - Click the Defense+ tile to flip open a more detailed pane which displays the current Auto-Sandbox and HIPS modes and a statistical summary of events handled by the Behavior Blocker component.
  - Click **Auto-Sandbox** to open the Behavior Blocker Settings interface. Refer to the section 'Behavior Blocker' for more details.
  - Click the link to the right of this to view and modify auto-sandbox security levels. Refer to the section 'Behavior Blocker' for more details.

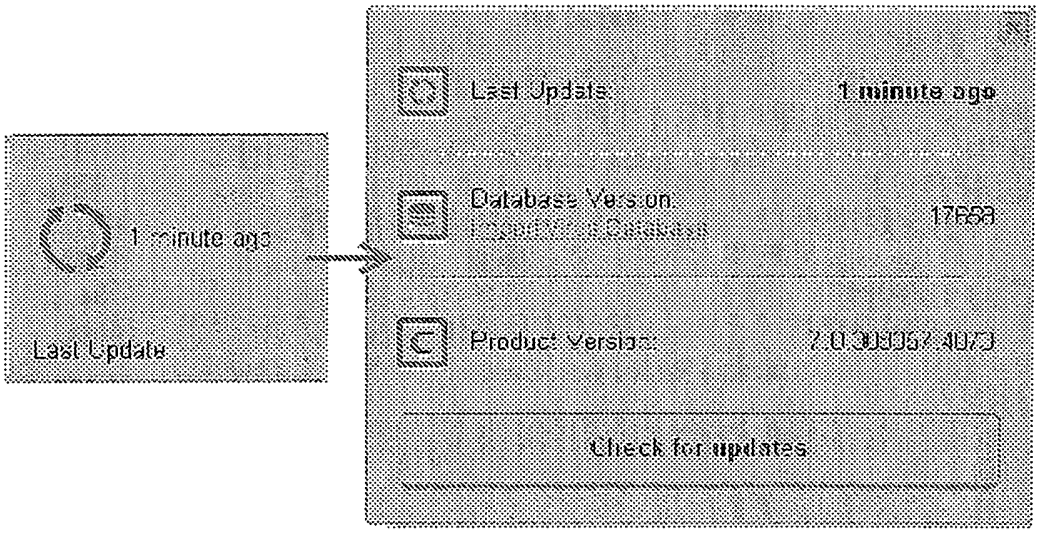


- Click **HIPS** to open the 'HIPS Settings' interface. Refer to the section 'HIPS Behavior Settings' for more details.
- Click the link to the right of this to view and modify HIPS security modes. Refer to the section 'HIPS Behavior Settings' for more details.




- Click the number of Blocked intrusions to open the Defense+ Log Viewer module.
- Click the number of Unrecognized Files to open the Unrecognized Files interface.
- Click the number of Sandboxed Apps to open the Active Process List dialog.

- **Updates** - Click the 'Updates' tile to open a more detailed pane which displays when the virus database was last updated, the database version number and the software version number.

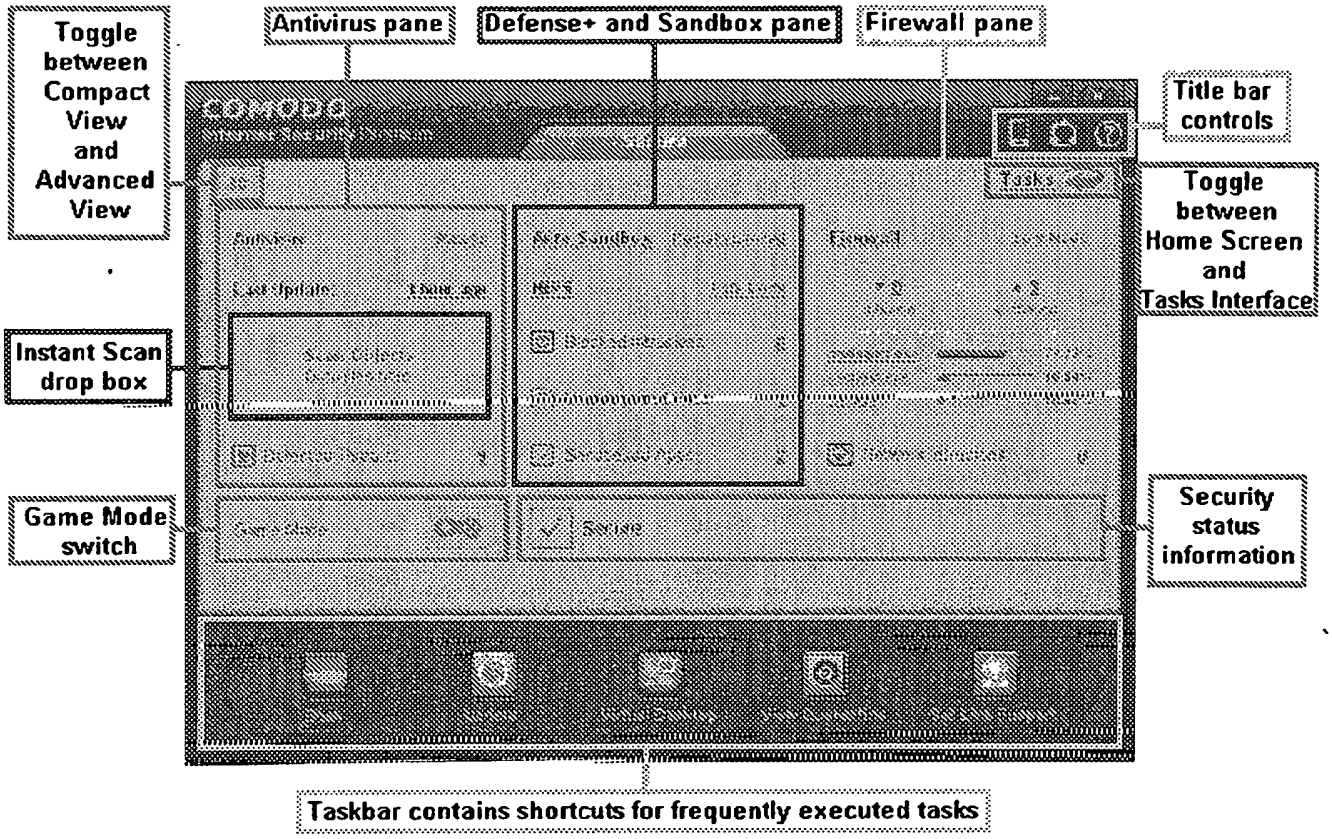



- Click on either the time of the last update or the 'Check for Updates' button to manually check for available updates. Refer to the section Manage Virus Database and Product Updates section for more details.
- Click the 'X' in the top right corner to return to the 4-tile view.

## Advanced View

The 'Advanced View' provides a more finely-detailed view of the security status of each of the Antivirus, Defense+ and Firewall components.

Switch to advanced view by clicking the toggle button at the top-left of the home screen:

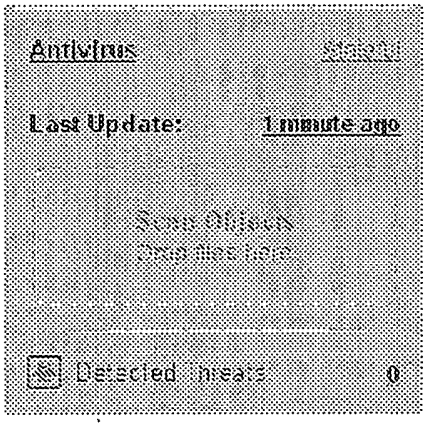



Click the following links to find out more:

- Antivirus Pane
- Defense+ and Sandbox Pane
- Firewall Pane

Antivirus Pane

The Antivirus pane allows you to configure antivirus mode, see when the virus database was last updated, view antivirus logs and instantly scan files and folders.

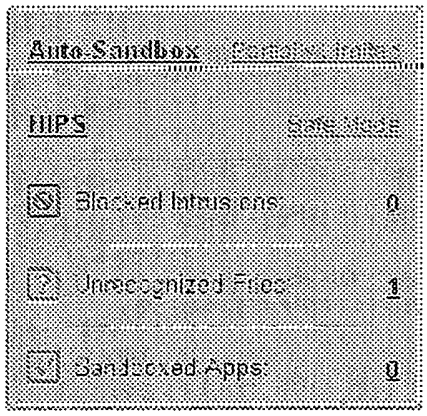



- **Antivirus** - Displays the current security level of the real-time antivirus scanner. Click on the security mode text to quickly switch between modes. Click 'Antivirus' to open the Realtime Scanner Settings interface. Refer to the section 'Real-time Scanner Settings' for more details.
- **Last Update** - Displays when the virus database was updated. Click the text link to start the updates again.

- **Detected Threats** - Displays the number of malware threats discovered so far from the start of current session as a link. Clicking this number will open the Antivirus Logs panel.
- **Scan Objects** - Drag-and-drop files, folders or even entire drives into this box to instantly scan them. Refer to the section Instantly Scan Files and Folders for more details.

### Defense+ and Sandbox Pane

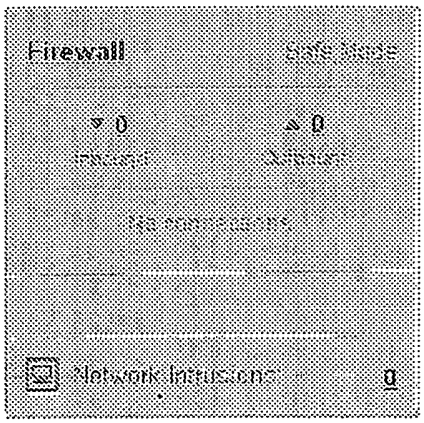
The Defense+ and Sandbox Pane allows you to quickly configure Auto-Sandbox and HIPS settings, view Defense+ logs and easily view the number of blocked intrusions, unrecognized files and sandboxed applications.




- Auto-Sandbox - Displays the current security level of the Behavior Blocker. Click on the security level itself to view or change it. Click **Auto-Sandbox** to open the 'Behavior Blocker Settings interface.' Refer to the section 'Behavior Blocker' for more details.
- **HIPS** - Click the text of the current HIPS mode to view or modify the mode. Click the word HIPS to open the 'HIPS Settings' interface. Refer to the section 'HIPS Behavior Settings' for more details.
- **Blocked Intrusions** - Displays the number of intrusions blocked by HIPS. Clicking on the numbered link will open the Defense+ logs. Refer to the section Defense+ Logs for more details.
- **Unrecognized Files** - Displays the number of files that are not recognized by CIS. These files may be considered as awaiting categorization. Clicking on the numbered link will open the Unrecognized Files screen which will allow you to run a file-lookup and to submit unknown files to Comodo for analysis. Refer to the section Unrecognized Files for more details.
- Sandboxed Apps - Displays the number of applications that are currently running inside the sandbox. Clicking the numbered link beside it will open the 'Active Processes List (Sandboxed Only)', which provides details of currently sandboxed applications. Refer to the section 'View Active Process List' for more details.

### Firewall Pane

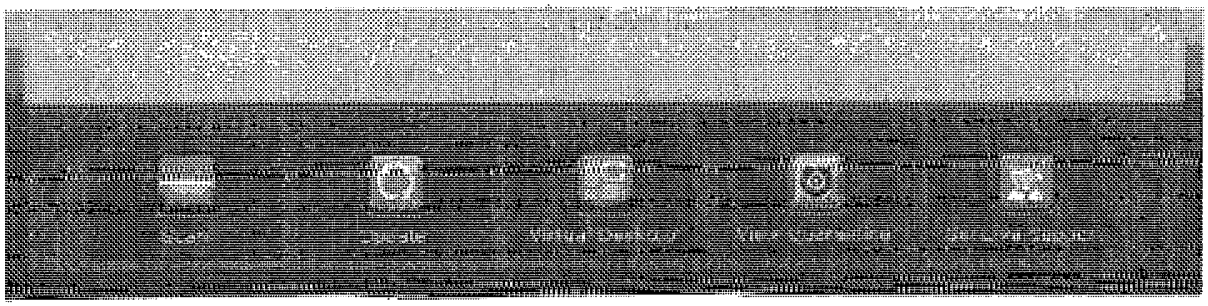
The Firewall Pane allows you to configure Firewall settings, view the number of inbound and outbound connections and the number of network intrusion attempts blocked by Firewall since the start of current session of CIS.



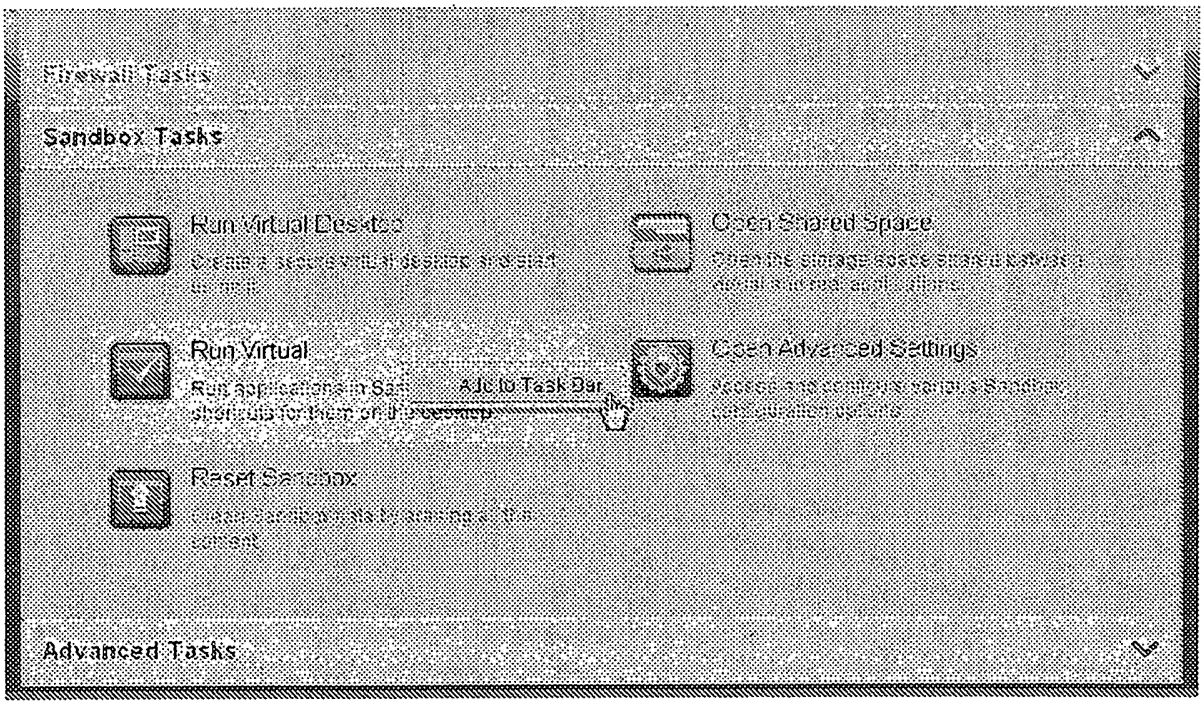
- Firewall - Displays the firewall's current security mode. Click on the level itself to quickly view and modify it. Click on '**Firewall**' to open the Firewall Settings interface. Refer to the section 'Firewall Behavior Settings' for more details.
- **Inbound / Outbound Connections** - A numerical summary of currently active inbound and outbound connections to and from the system. Clicking on the numbered link will open the View Connections screen. Refer to the section 'View Active Internet Connections' for more details.
- **Traffic** - The Traffic area of the pane displays a bar graph showing applications that are currently connected to the internet and are sending or receiving data. The summary also displays the % of total traffic each application is responsible for and the filename of the executable. Clicking on any application name will open the View Connections screen.
- **Network Intrusions** - Displays the total number of intrusion attempts blocked by firewall since the start of the current session. Clicking on the numbered link will open the Firewall Logs screen. Refer to the section 'Firewall Logs' for more details.

### Adding tasks to the Task Bar

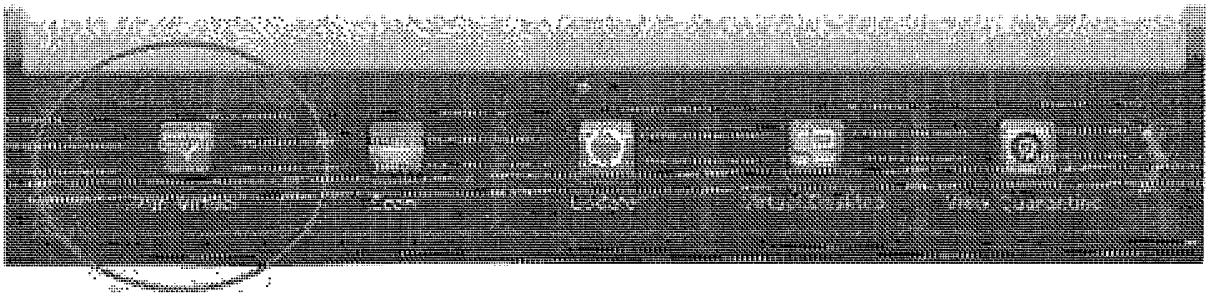
The task bar contains a set of shortcuts which will launch common tasks with a single click. You can add any task you wish to this toolbar. Click the handles < > on the left and right sides of the task bar to scroll through all tasks.



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

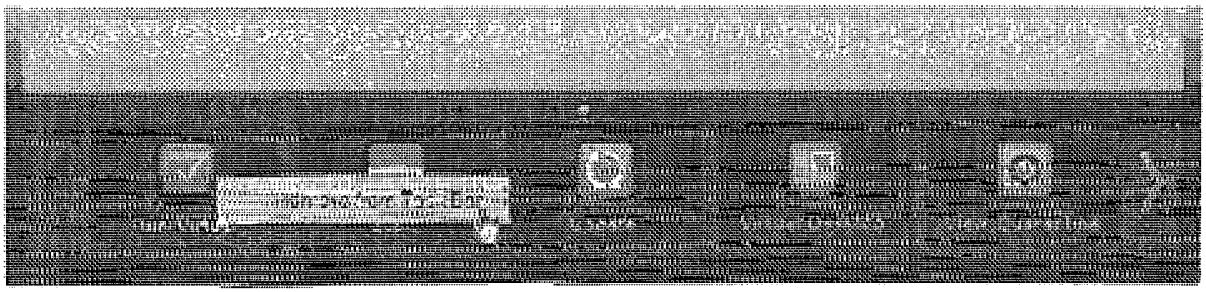



- The selected task will be added to the Task Bar.



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

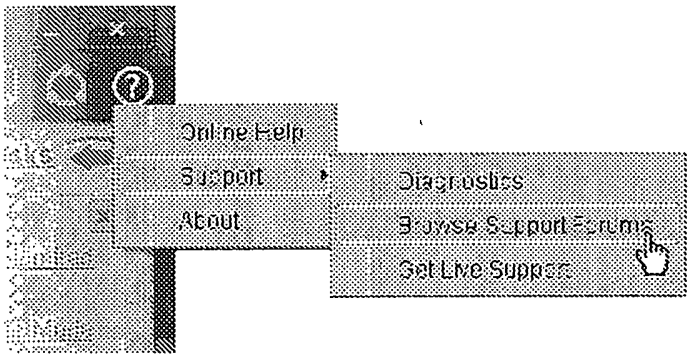
- To remove a task shortcut from the Task Bar, right click on it and choose 'Remove from task bar'.



Title bar controls

The title bar (top right) contains shortcuts for:

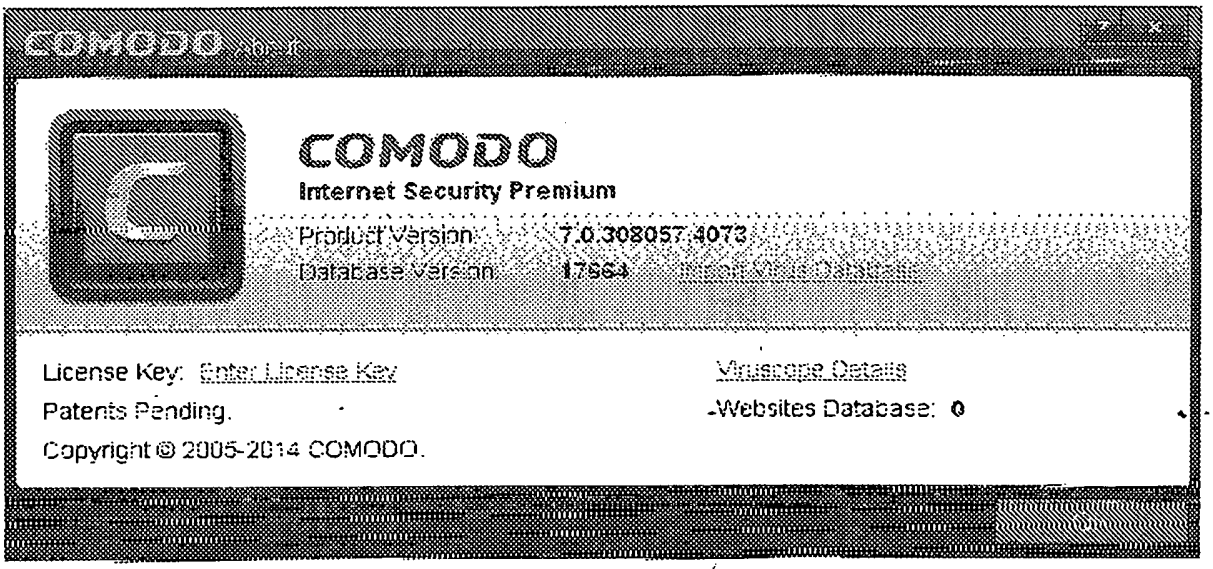
- Comodo Mobile Security app for Android phones and tablets. - Click the mobile icon and scan the QR code with your device to download the latest version of the app. You can also get the app from our website, https://m.comodo.com/ or from the Google Play app store at https://play.google.com/store/apps/details?id=com.comodo.pimsecure
- Refer your Friends - Click the icon to open the 'Comodo Friends' website. Register an account for free, recommend CIS to your friends and get attractive rewards. Visit http://friends.comodo.com/ for more details.
- Get Help - Click the help icon for the following options:




- Online Help - Opens Comodo Internet Security's online help guide at http://help.comodo.com/topic-72-1-522-6207-Introduction-to-Comodo-Internet-Security.html.
- Support - Click this link for the following options:
- Diagnostics - Helps to identify any problems with your installation.

- Browse Support Forum - Links to Comodo User Forums.
- Get Live Support - Launches the GeekBuddy support client.

- **About** - Displays the product version, virus signature database version, website database version (website filtering URLs), details of active Viruscope Recognizers and copyright information. The 'About' dialog also allows you to import a locally stored virus database and to enter a license key for CIS Pro.




- Click Import Virus Database to import a locally stored virus signature database into CIS.
- Click Enter License Key to upgrade to CIS Pro. Refer to the section 'Activating CIS Pro/Complete Services after Installation' for more details.
- Click Viruscope Details to open a dialog which shows the Viruscope Recognizers that are active on your system. Refer to the Behavior Blocker section for more details.

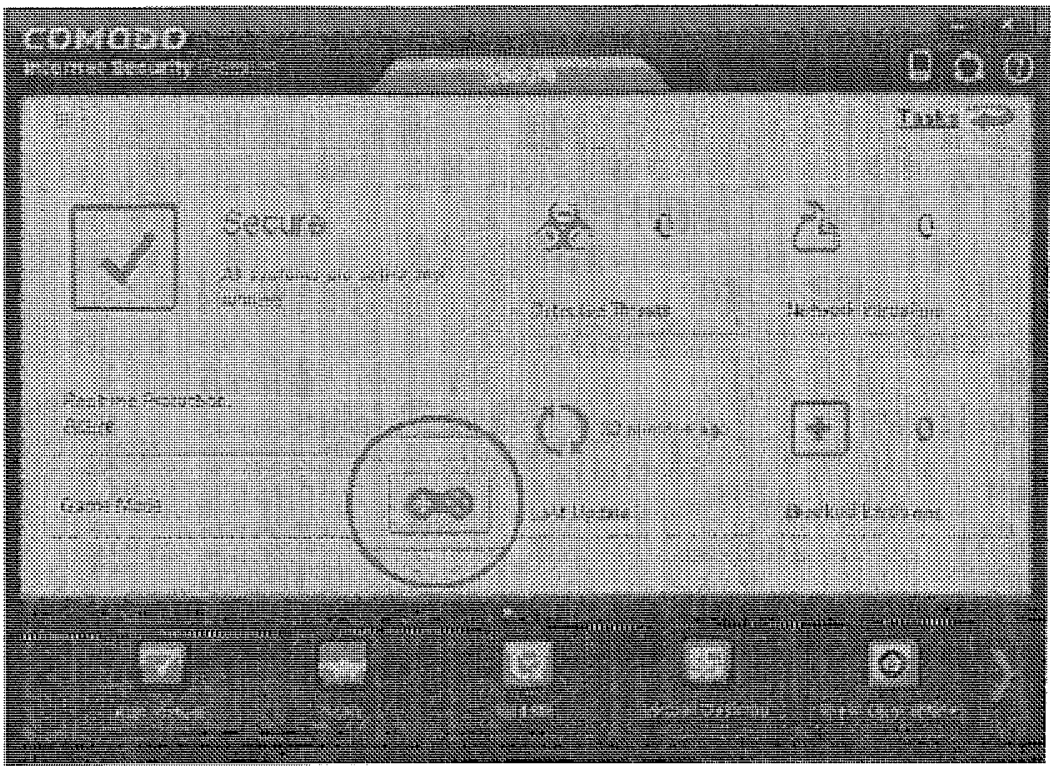
Game mode

Game Mode enables you to play your games without interruptions or alerts. Operations that can interfere with a user's gaming experience are either suppressed or postponed.
In game mode:

- Defense+/Firewall alerts are suppressed.
- AV database updates and scheduled scans are postponed until the gaming is over.
- Automatic isolation of unknown applications and real-time virus detection are still functional.

**To switch to Game mode**

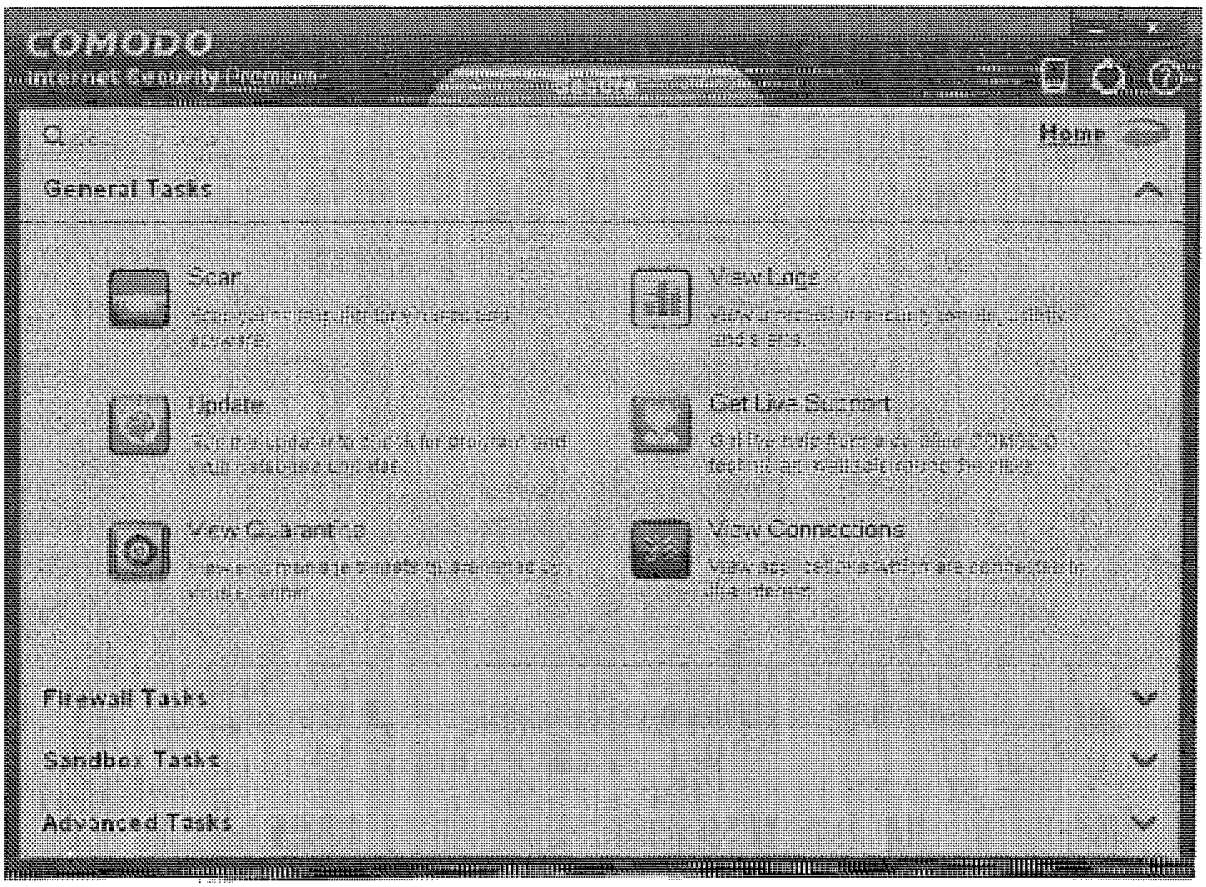
- Click the Game Mode switch at the bottom left of the Home Screen




- Deactivate Game Mode to resume alerts and scheduled scans.

## 1.5.2. The Tasks Interface

The items in the 'Tasks' area allow you to configure every aspect of Comodo internet security.



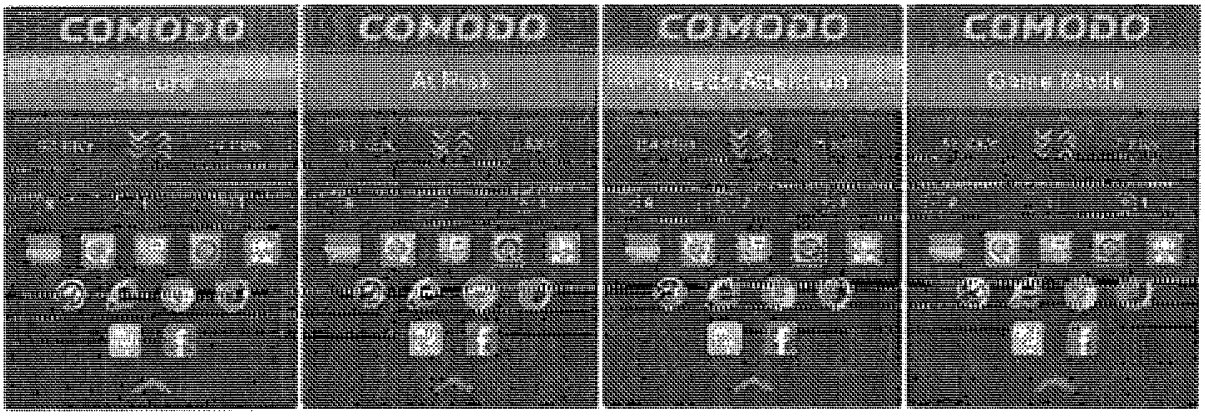

Tasks are broken down into four main sections. Click the following links for more details on each:

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

## 1.5.3. The Widget

The CIS Widget is a handy control that lives on your desktop and provides at-a-glance information about overall security status, inbound and outbound traffic, sandboxed applications, unrecognized files and more. The Widget starts automatically with CIS unless it is disabled from the System Tray icon or in the 'User Interface' of General Settings.

Right clicking on the Widget opens a context sensitive menu similar to the one displayed when you right click on the CIS system tray icon. The context sensitive menu allows you to enable or disable CIS components and configure various settings. Refer to section The System Tray Icon for more details.

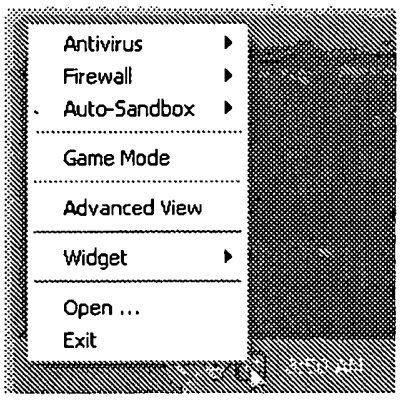


- The color coded row at the top of the widget displays your current security status. Double-clicking on 'At Risk' or 'Needs Attention' opens the appropriate interface for you to take action immediately.
- The second row displays information about incoming and outgoing network traffic. The network traffic row is displayed only if 'Show Traffic pane' under 'Widget options of CIS tray icon or Widget right click menu is enabled. Refer to The System Tray Icon for more details. (***Default = Enabled***)
- The third row tells you current status of the CIS application:
  - The first button [redacted] displays the number of programs/processes that are currently running in the sandbox. Clicking the button opens the Active Process List interface, which allows you to identify and terminate unnecessary processes. Clicking the 'More' button in this interface will open the KillSwitch application. If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the sections View Active Process List and Identify and Kill Unsafe Processes for more details.
  - The second button [redacted] tells you how many CIS tasks are currently running. Clicking this button opens the Windows Task Manager interface.
  - The third button [redacted] displays how many files have been added to the 'Unrecognized Files' list and are pending submission to Comodo for analysis. Clicking this button opens the Unrecognized Files interface.

  The status row is displayed only if 'Show Status Pane' is enabled. Check this by right clicking the tray icon or the widget itself and look under 'Widget' options. Refer to The System Tray Icon for more details. (***Default = Disabled***)
- The forth row contains shortcuts for the five common tasks you have in the task bar at the bottom of the home screen. Clicking the shortcut on the widget will run the task. The 'Common Tasks' row is displayed only if 'Show Common Tasks Pane' is enabled under 'Widget' options of the CIS tray icon or the widget right-click menu. Refer to The System Tray Icon for more details. (***Default = Enabled***)
- The fifth row displays the browsers installed on your computer. Clicking on a browser icon will open the browser inside the sandbox for a secure browsing session. You can tell the browser is running in the sandbox because it will have a green border around it. Refer to Running an application inside the sandbox for more details. The 'Browsers' row is displayed only if 'Show Browsers Pane' is enabled under the 'Widget' section of the CIS tray right-click menu. This can also be viewed by right-clicking the widget itself. Refer to The System Tray Icon for more details. (***Default = Enabled***)
- The last row on the widget provides links to social networking sites. This row is displayed only if 'Show Connect Pane' is enabled. To check this setting, right-click on the CIS tray icon and look at the 'Widget' section. Alternatively, right-click the widget itself. Refer to The System Tray Icon for more details. (***Default = Enabled***)
- You can expand or collapse the Widget by clicking the arrow at the bottom.

## 1.5.4. The System Tray Icon

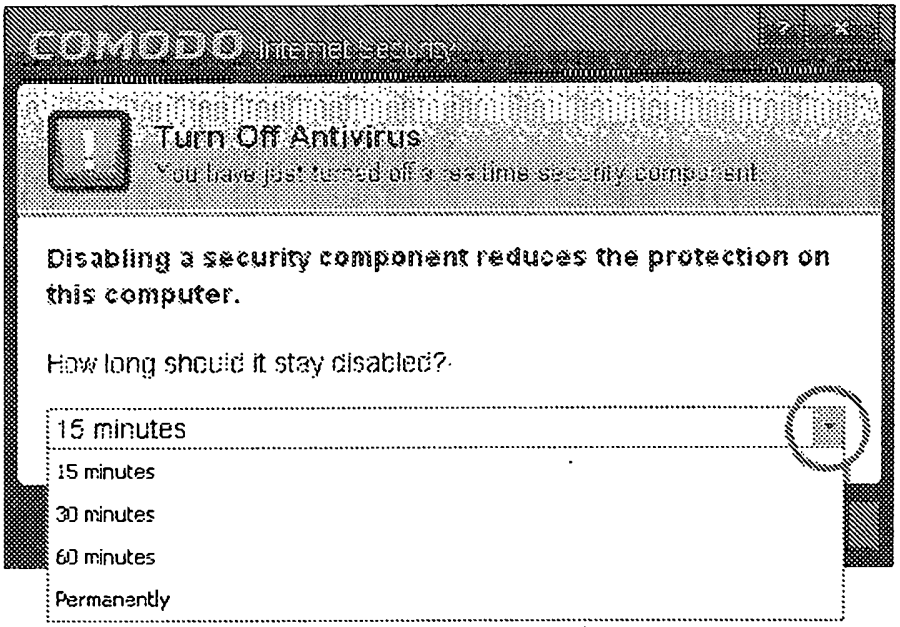
Double-clicking the system tray icon will quickly open the CIS interface. Right-clicking the icon opens a context sensitive menu that allows you to configure various application settings:




The options available for the Antivirus, Firewall and Auto-sandbox menu-items depend on whether you are using Compact View or Advanced View.

| Compact View | Advanced View |
|---|---|
| **Antivirus** - You can enable or disable Real-time antivirus scan.<br><br>**Firewall** - You can enable or disable Firewall.<br><br>**Auto-Sandbox** - You can enable or disable Auto-Sandbox. Refer to the section 'Behavior Blocker' for more details. | **Antivirus** - Options available are On Access, Stateful and Disabled. Refer to Antivirus Pane for more details.<br><br>**Firewall** - Options available are Block All, Custom Ruleset, Safe Mode, Training Mode and Disabled. Refer to the section 'Firewall Behavior Settings' for more details.<br><br>**Auto-Sandbox** - Options available are Fully Virtualized, Partially Limited, Limited, Restricted, Untrusted, Blocked and Disabled. Refer to the section 'Behavior Blocker' for more details.<br><br>**HIPS** - Options available are Paranoid Mode, Safe Mode, Clean PC Mode, Training Mode and Disabled. Refer to the section HIPS Behavior Settings for more details. |

If you disable either the antivirus, the firewall or the auto-sandbox from the right-click menu, then the security info bars on the main interface and the widget will turn red. You will also see a pop-up warning which allows you to specify how long the feature should remain disabled:



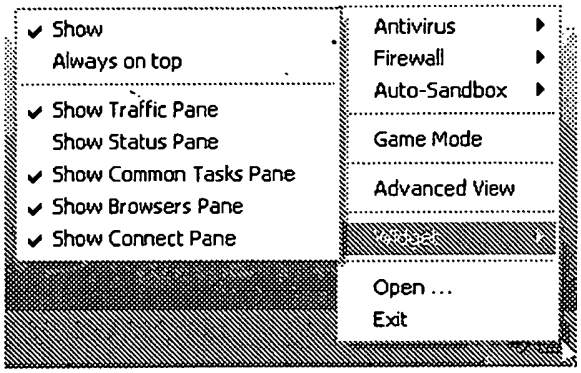
Select the period and click 'OK'. Unless you have selected 'Permanently', the security component will be automatically re-enabled after the stated time period has elapsed. You can, of course, manually re-enable at any time by right-clicking the tray icon and selecting 'Enable' for the component in question.

- **Game Mode** - Switches CIS into Game Mode so you can play your games without any interruptions from various alerts in your computer. Operations that can interfere with the gaming experience are either suppressed or postponed.

  In game mode:
  - Defense+/Firewall alerts are suppressed.
  - AV database updates and scheduled scans are postponed until the gaming is over.
  - Automatic isolation of unknown applications and real-time virus detection are still functional.

Deactivate Game Mode to resume alerts and scheduled scans.

- **Advanced View** - Switches the Home Screen between Compact View and Advanced View
- **Widget** - Select whether the Widget is shown and which widget components are included:




  - **Show**: Toggles the widget on or off (***Default** = **Enabled***)
  - **Always on top**: Displays the widget on top of all windows currently running on your computer. (***Default** = **Disabled***)
  - **Show Traffic Pane**: Displays the network traffic row on the widget. (***Default** = **Enabled***)
  - **Show Status Pane**: Displays the security status tab at the top of the widget. (***Default** = **Disabled***)
  - **Show Common Tasks Pane**: Displays the row containing shortcuts to common CIS tasks. (***Default** = **Disabled***)
  - **Show Browsers Pane**: Displays the row containing shortcuts to your installed browsers. (***Default** = **Enabled***)
  - **Show Connect Pane**: Displays the row containing the shortcuts to social networking sites. (***Default** = **Enabled***)
- **Open** - Opens the CIS interface.
- **Exit** - Closes the CIS application.

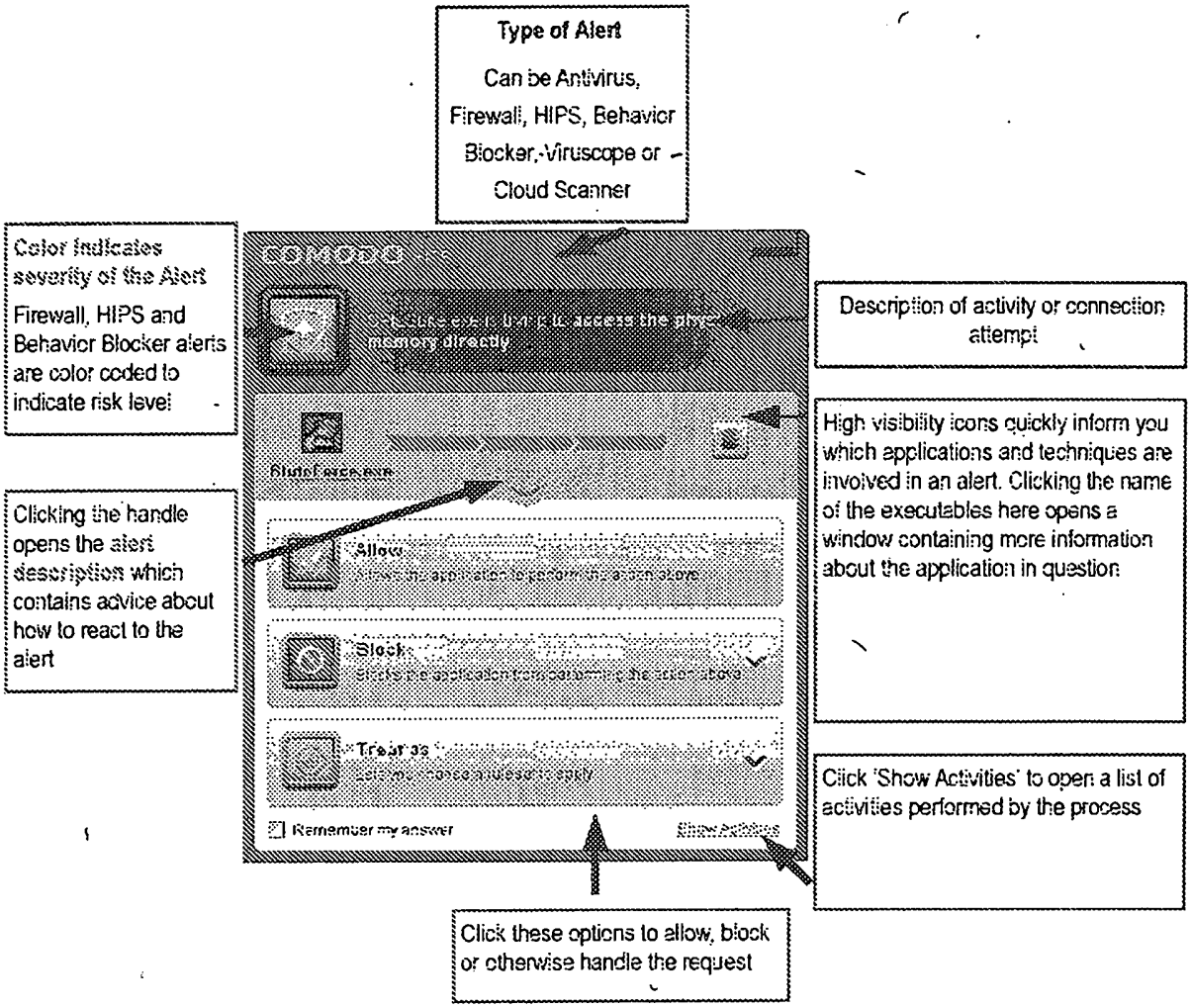
# 1.6. Understanding Security Alerts

- Alerts Overview
  - Alert Types
  - Severity Levels
  - Descriptions
- Antivirus Alerts
- Firewall Alerts
- HIPS Alerts

- Behavior BlockerAlerts
- Elevated Privilege Alerts
- Auto-Sandbox Alerts
- Viruscope Alerts

### Alerts Overview

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




### Alert Types

Comodo Internet Security alerts come in five main varieties. Click the name of the alert (at the start of the following bullets) if you want more help with a particular alert type.

- Antivirus Alerts - Shown whenever virus or virus-like activity is detected. AV alerts will be displayed only when Antivirus is enabled and the option 'Do not show antivirus alerts' is disabled in Real-time Scanner Settings.
- Firewall Alerts - Shown whenever a process attempts unauthorized network activity. Firewall alerts will be displayed only when the Firewall is enabled and the option 'Do not show popup alerts' is disabled in Firewall Settings.
- HIPS Alerts - Shown whenever an application attempts an unauthorized action or tries to access protected

areas. HIPS alerts will only be generated if HIPS is enabled and Do NOT show popup alerts is disabled.

- Behavior Blocker Alerts (including Elevated Privilege Alerts) - Shown whenever an application tries to modify operating system or related files and when the Behavior Blocker automatically sandboxes an unrecognizable file. Behavior Blocker / Auto-Sandbox Alerts will be displayed only when auto-sandboxing is enabled under Behavior Blocker settings. Privilege Alerts will only be shown if enabled.
- Viruscope Alerts - Shown whenever a currently running process attempts to take suspicious actions. Viruscope alerts allow you to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer. Viruscope Alerts will be displayed only when Viruscope is enabled under Behavior Blocker settings.

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

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

### Severity Level

The shield icons at the upper left of each alert are color coded according to the risk level presented by the activity or request. However, it cannot be stressed enough that you should read the entire alert before reaching a decision on whether to allow or block the alert.

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

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

### Alert Description

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



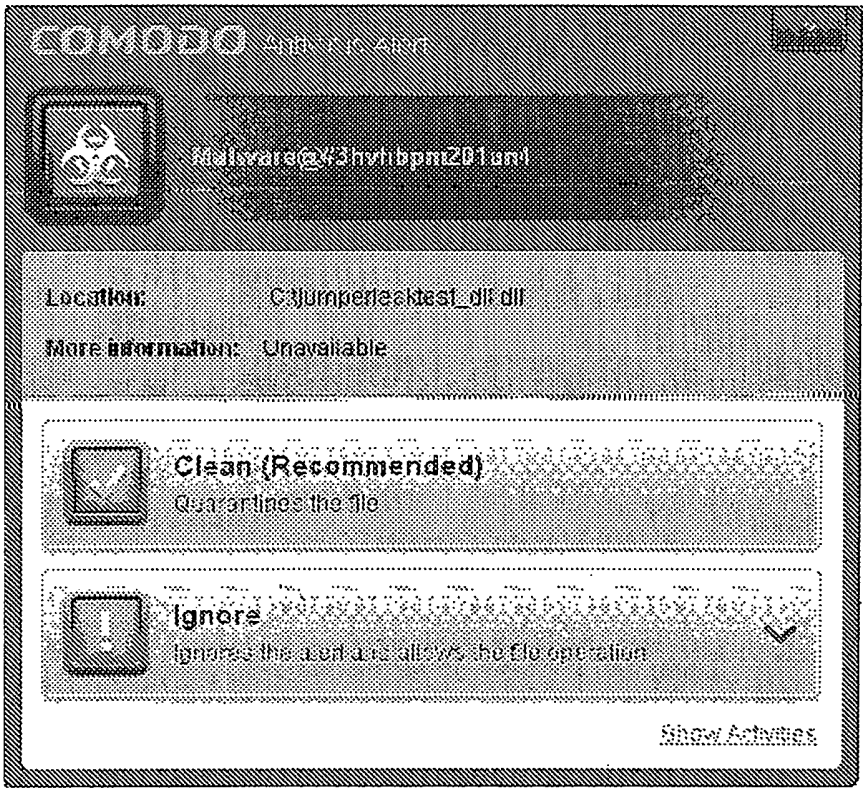

The description tells you the name of the software/executable that caused the alert; the action that it is attempting to perform and how that action could potentially affect your system. You can also find helpful advice about how you should respond.

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

### Answering an Antivirus Alert

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

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




Tip: Clicking the Show Activities link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

The Show Activities link is available only if Viruscope is enabled under Advanced Settings > Defense+ > Behavior Blocker Settings. If none of the processes associated with the infected application has started before the alert is generated, the Show Activities link is disabled and will not open the Process Activities List dialog.

The following response-options are available:

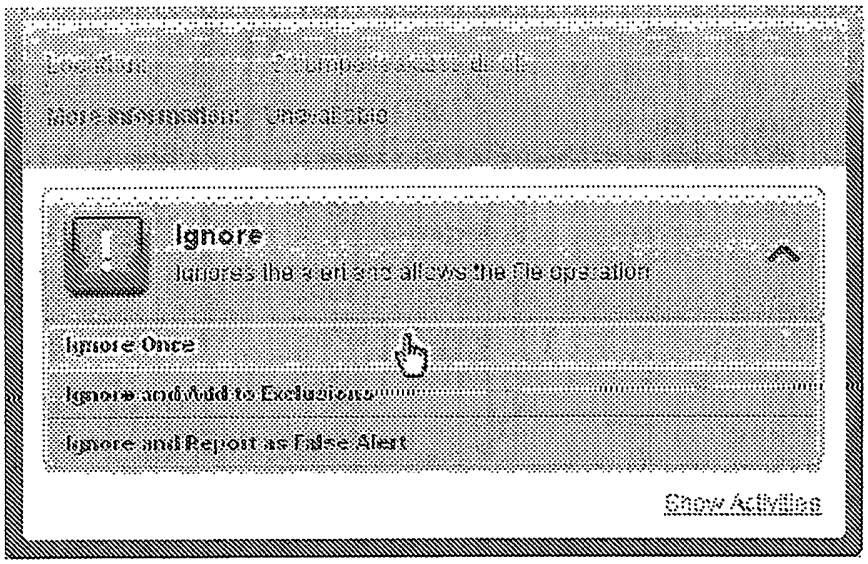
- **Clean** - Disinfects the file if a disinfection routine exists. If no routine exists for the file then it will be moved to Quarantine. If desired, you can submit the file/application to Comodo for analysis from the Quarantine interface. Refer to Manage Quarantined Items for more details on quarantined files.

  The Viruscope subsytem integrated with the Antivirus, also monitors the changes made to your computer by the virus or virus-like activities automatically reverts them, if you choose to clean the infected file or application, when Viruscope is enabled under Behavior Blocker settings.

Note: Though Viruscope has power to reverse majority of types of changes effected by the process(es) evoked by blocked applications, it has some limitations. Very few of the file activities that make permanent changes could be reverted. Examples include:

- Deletion of a file
- Moving a file to a different folder/location
- Loading a file image into a process, i.e. DLL file loading

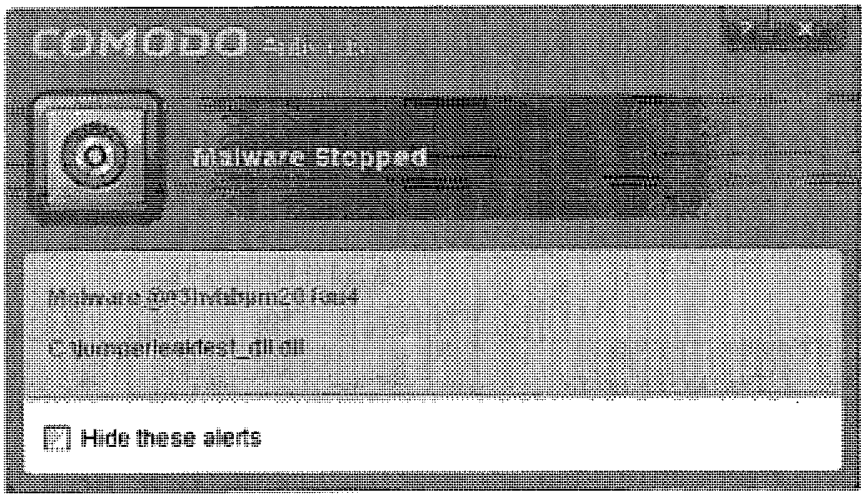
- **Ignore** - Allows the process to run and does not attempt to clean the file or move it to quarantine. Only click 'Ignore' if you are absolutely sure the file is safe. Clicking 'Ignore' will open three further options:




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

### Antivirus Notification

If you have chosen to not to show Antivirus Alerts through Advanced Settings > Security Settings > Antivirus Settings > Realtime Scanner Settings by leaving the option 'Do not show antivirus alerts' enabled (***default=enabled***) and if CIS identifies a virus or other malware in real time, it will immediately block malware and provide you with instant on-screen notification:




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

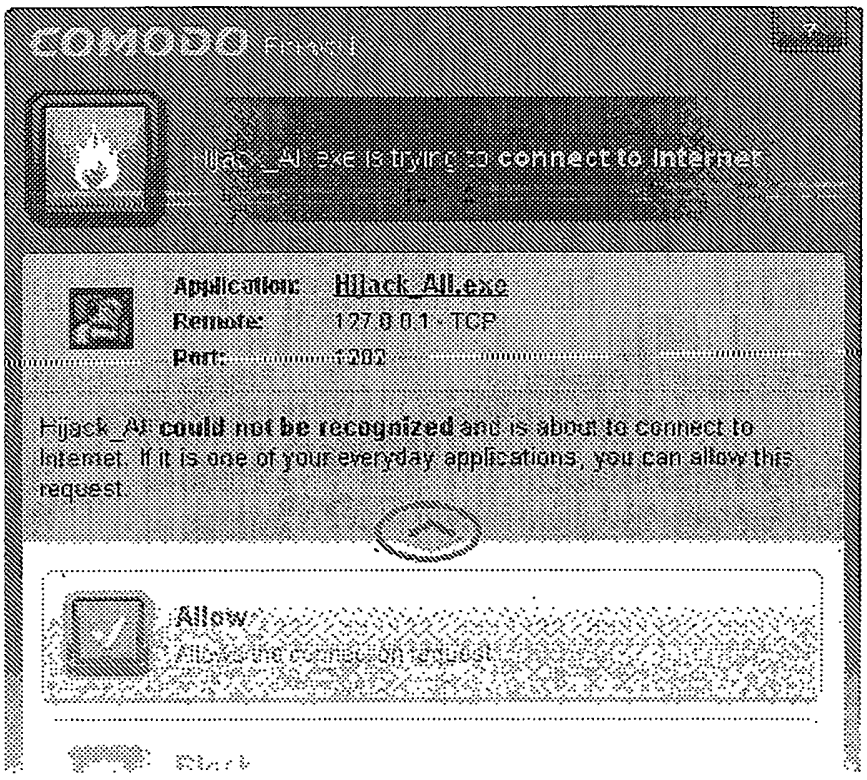
### Answering Firewall Alerts

CIS generates a firewall alert when it detects unauthorized network connection attempts or when traffic runs contrary to one of your application or global rules. Each firewall alert allows you to set a default response that CIS should automatically implement if the same activity is detected in future. The followings steps will help you answer a Firewall alert:



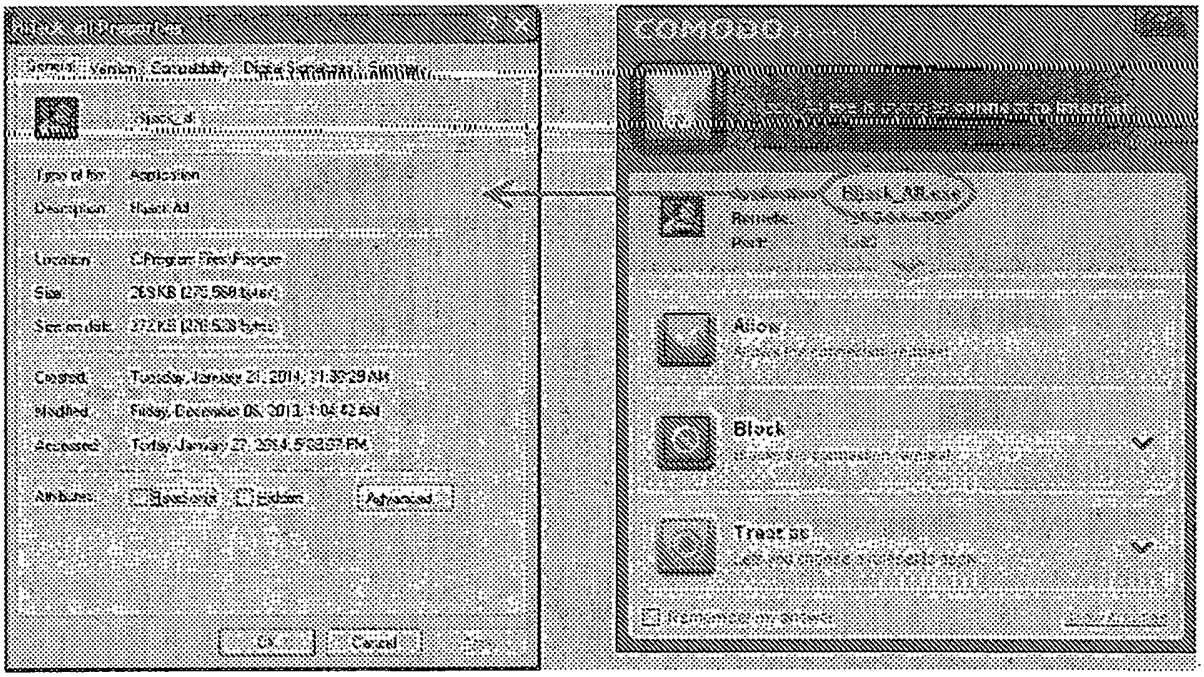

Tip: Clicking the Show Activities link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

The Show Activities link is available only if Viruscope is enabled under Advanced Settings > Defense+ > Behavior Blocker Settings. If none of the processes associated with the application that makes the connection attempt has started before the alert is generated, the Show Activities link is disabled and will not open the Process Activities List dialog.




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

   If it is one of your everyday applications and you want to allow it Internet access to then you should select **Allow**.



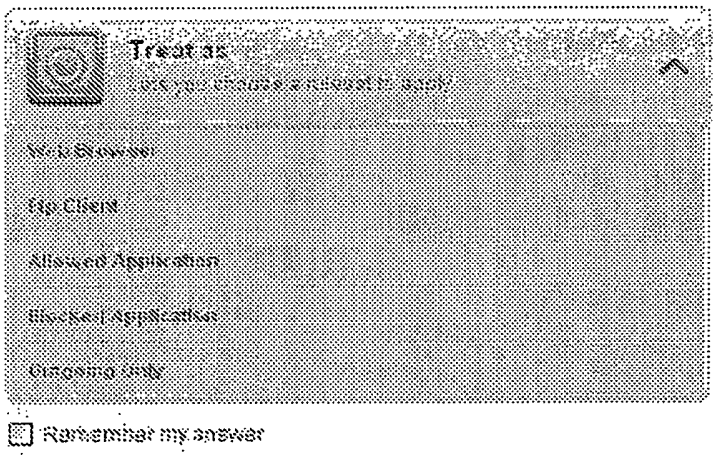

In all cases, clicking on the name of the application opens a properties window that can help you determine whether or not to proceed.

If you don't recognize the application then we recommend you **Block** the application. By clicking the handle to expand

the alert, you can choose to block the connection (connection is not allowed to proceed) or block & terminate (connection is not allowed to proceed and the process/application that made the request is shut down).



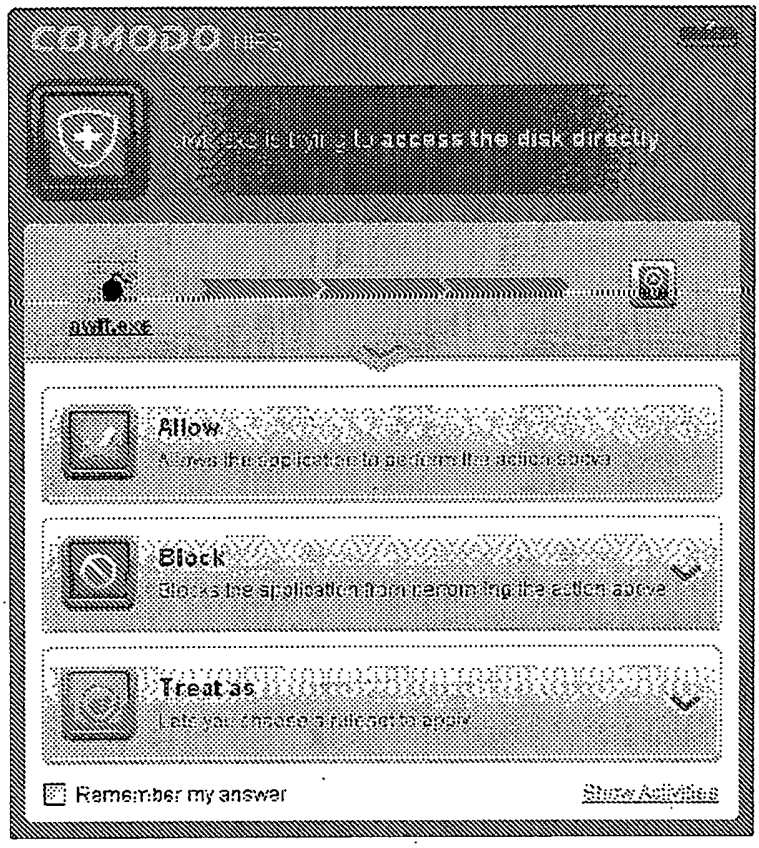

2. If you are sure that it is one of your everyday application, try to use the **'Treat As'** option as much as possible. This allows you to deploy a predefined firewall ruleset on the target application. For example, you may choose to apply the policy **Web Browser** to the known and trusted applications 'Internet Explorer', 'Firefox' and 'Opera'. Each predefined ruleset has been specifically designed by Comodo to optimize the security level of a certain type of application.




Remember to check the box **Remember My Answer** for the ruleset to be applied in future.

3. If the Firewall alert reports a behavior, consistent with that of a malware in the security considerations section, then you should block the request AND select **Remember My Answer** to make the setting permanent.

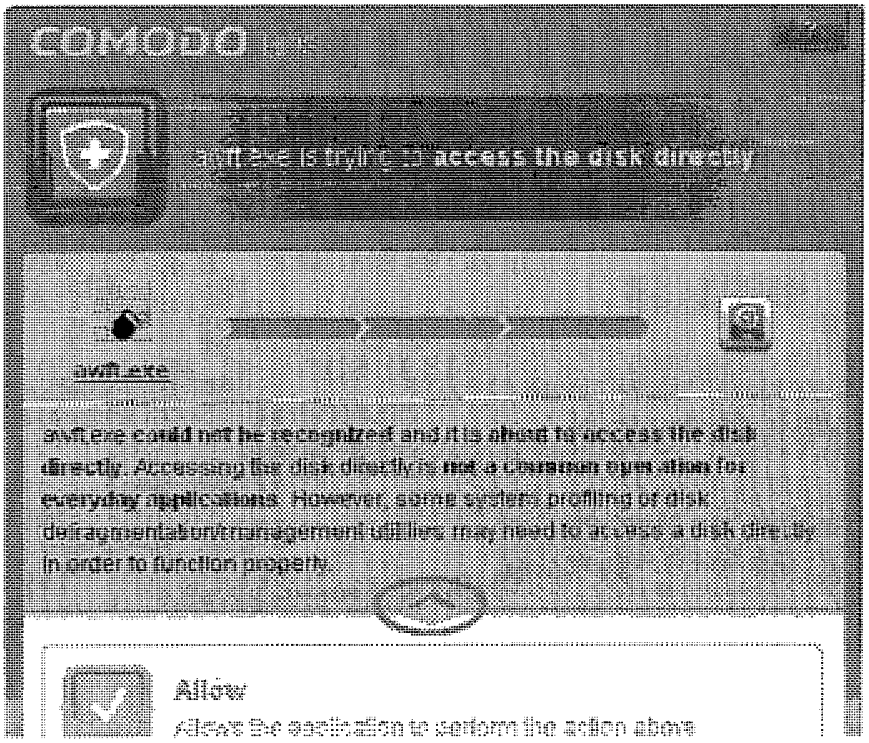
Comodo Internet Security generates a HIPS alert based on the behavior of applications and processes running on your system. Please read the following advice before answering a HIPS alert:




Tip: Clicking the Show Activities link at the bottom right will open the Process Activities List dialog. The Process Activities dialog will display the list activities of the processes run by the application.

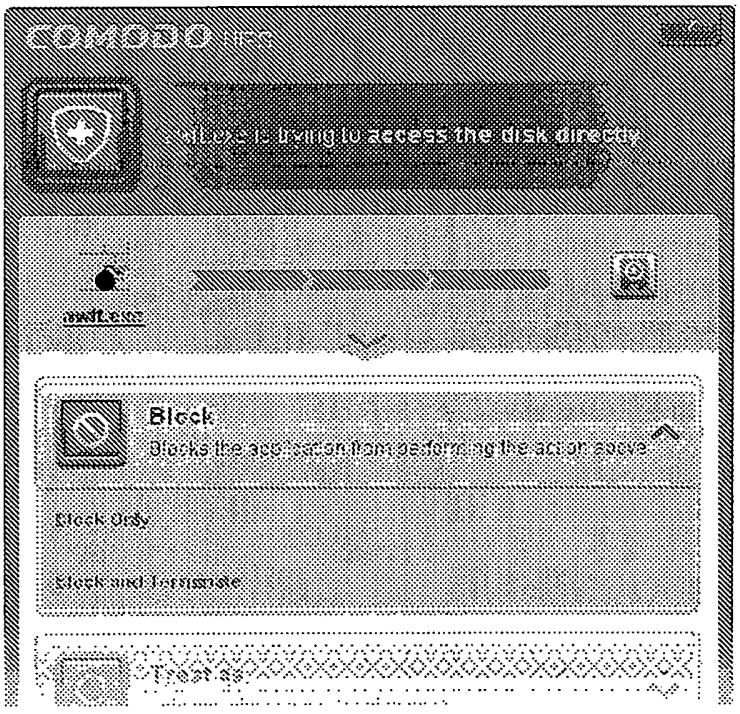
The Show Activities link is available only if Viruscope is enabled under Advanced Settings > Defense+ > Behavior Blocker Settings. If none of the processes associated with the application has started before the alert is generated, the Show Activities link is disabled and will not open the Process Activities List dialog.

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

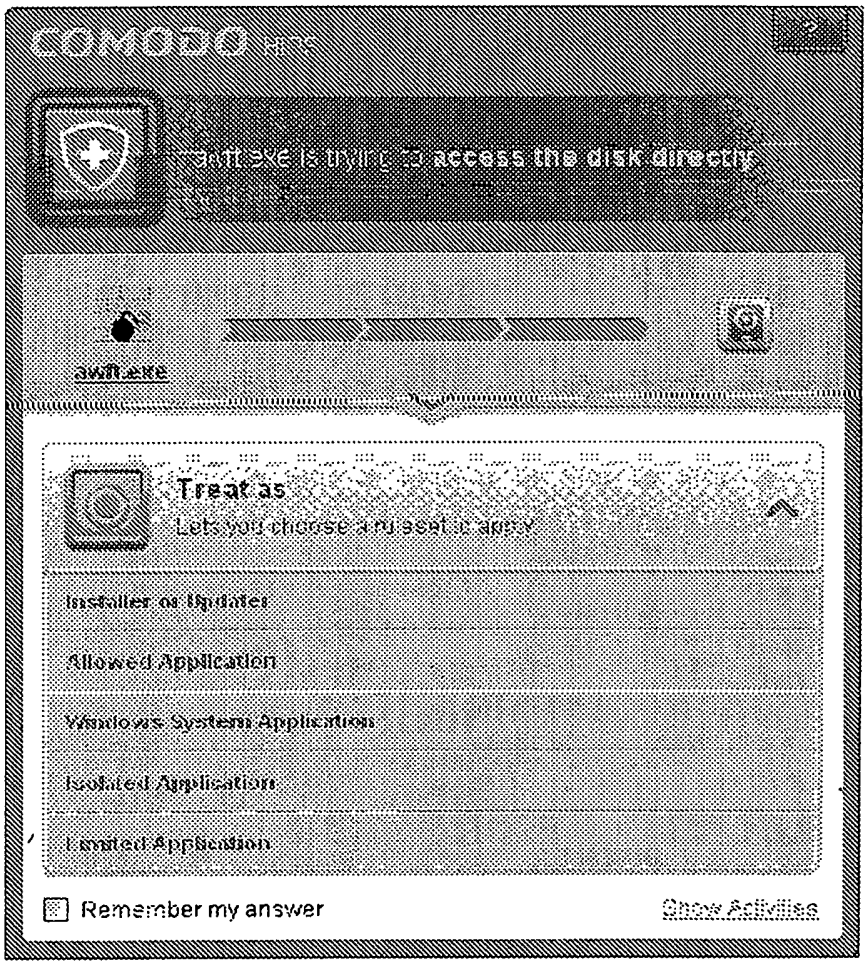



If it is one of your everyday applications and you simply want it to be allowed to continue then you should select **Allow**.

If you don't recognize the application then we recommend you select **Block** the application. You can choose to just block the connection or to block & terminate.

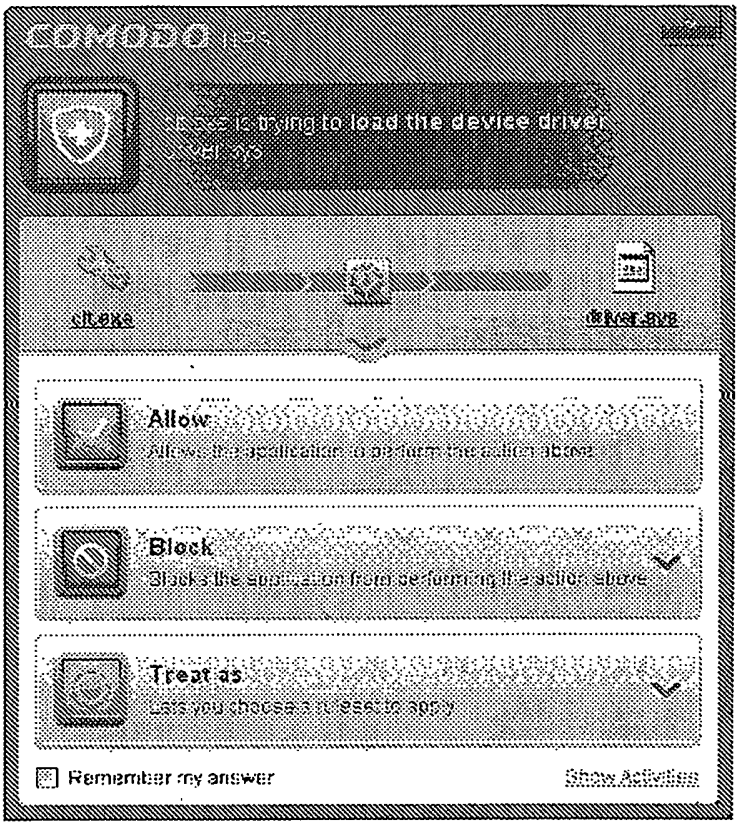



2. If you are sure that it is one of your everyday applications and want to enforce a security policy (ruleset) to it, please use the 'Treat As' option. This applies a predefined HIPS ruleset to the target application.




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

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




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




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




Were you installing new software or trying to download an application from the Internet? If you are downloading a file

from the 'net, select **Allow**, without selecting **Remember my answer** option to cut down on the creation of unnecessary rules within the firewall.

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

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

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

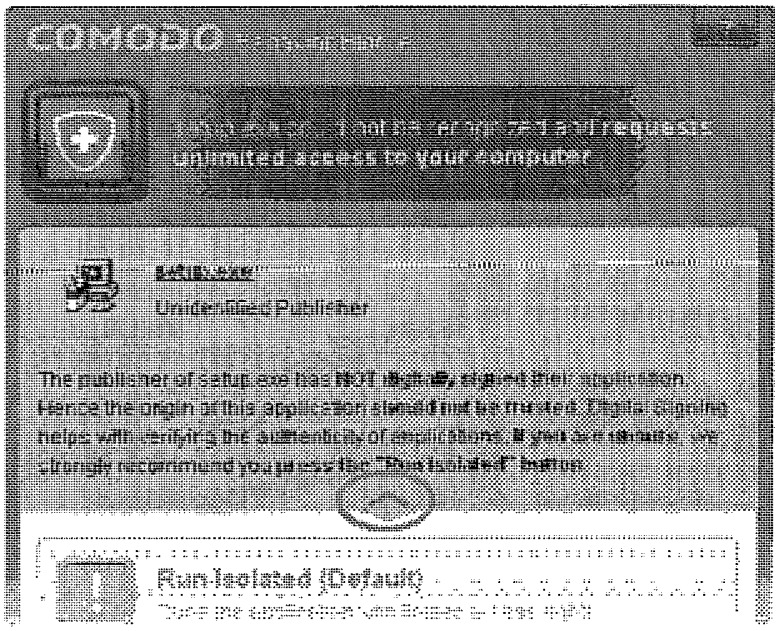
### Answering a Behavior Blocker Alert

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

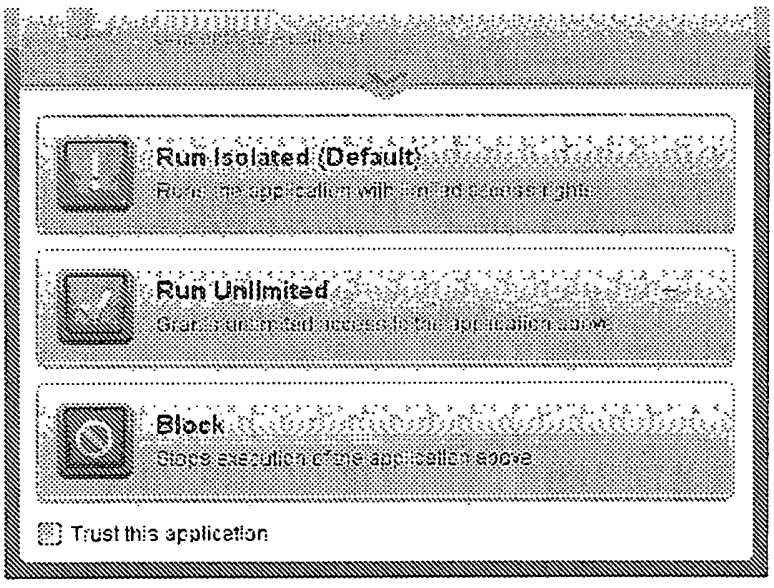
Please read the following advice before answering a Behavior Blocker alert:



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




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




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

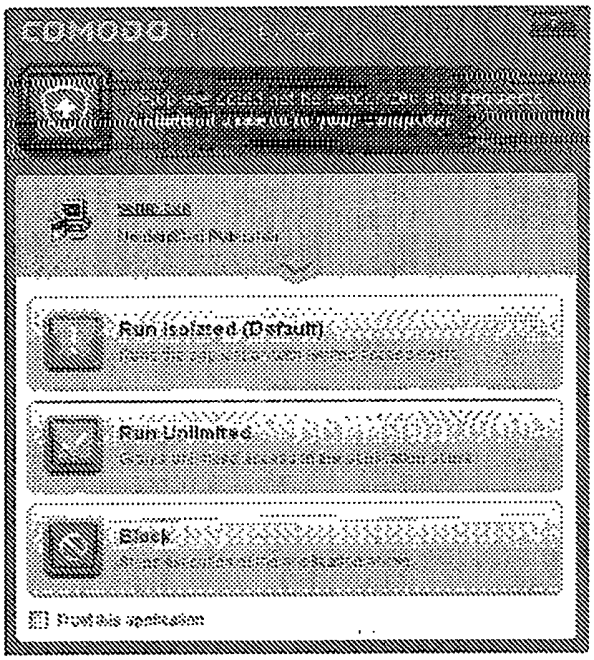
### Run with Elevated Privileges Alert

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

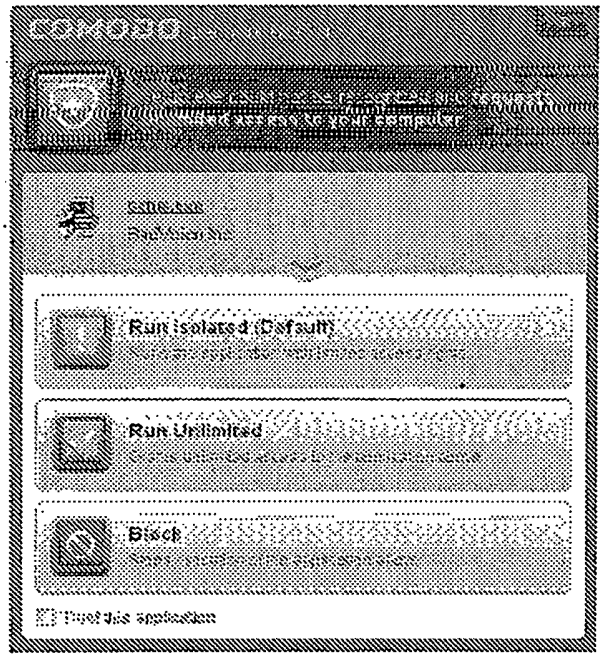
- If you have good reason to trust the publisher of the software then you can click the '**Run Unlimited**' button. This will grant the elevated privilege request and allow the installer to run.
- If you are unsure of the safety of the software, then Comodo recommends that you run it with restricted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

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

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




**Unknown and not Digitally Signed**




**Unknown and Digitally Signed but not yet whitelisted (Not yet a 'Trusted Vendor')**

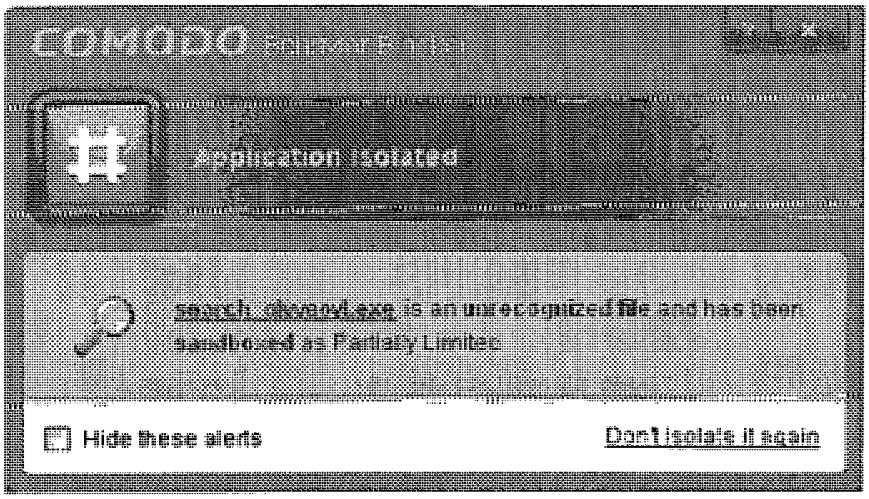
- Unknown and unsigned installers should be either isolated or blocked.
- Unknown but signed installers can be allowed to run if you trust the publisher, or may be isolated if you would like to evaluate the behavior of the application.

Also see:

- 'Unknown Files: The Auto-Sandboxing and Scanning Processes' - to understand the decision making process behind why CIS chooses to sandbox certain applications.
- 'Trusted Software Vendors' - for an explanation of digitally signed files and 'Trusted Software Vendors'.

Auto-Sandbox Alerts

The Behavior Blocker will display an alert whenever it auto-sandboxes an unknown application:




The alert will show the name of the executable that has been auto-sandboxed. The application will be automatically added to Unrecognized Files list.

- Clicking the name of the application will open the Unrecognized Files interface, that displays a list of the unrecognized files including the currently auto-sandboxed application.
- Clicking Don't isolate it again removes the application from the Unrecognized Files list and adds it to the Trusted Files list, so that the application will not be auto-sandboxed in future. Choose this option if you are absolutely sure that the executable is safe.

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

Also see:

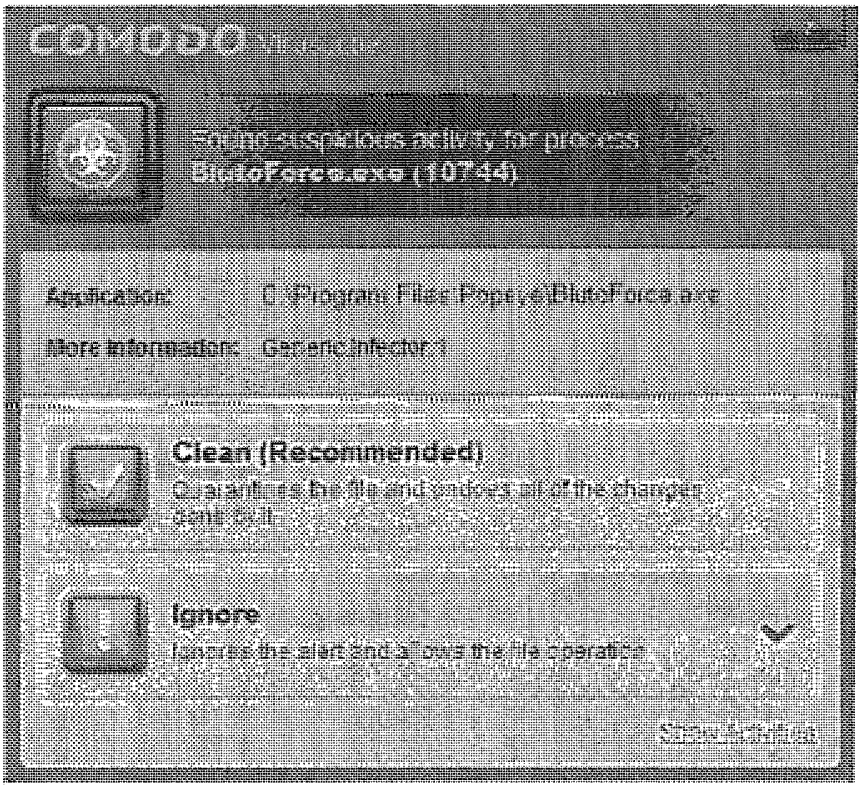
- 'Unknown Files: The Auto-Sandboxing and Scanning Processes' - to understand the decision making process behind why CIS chooses to auto-sandbox certain applications.

### Answering a Viruscope Alert

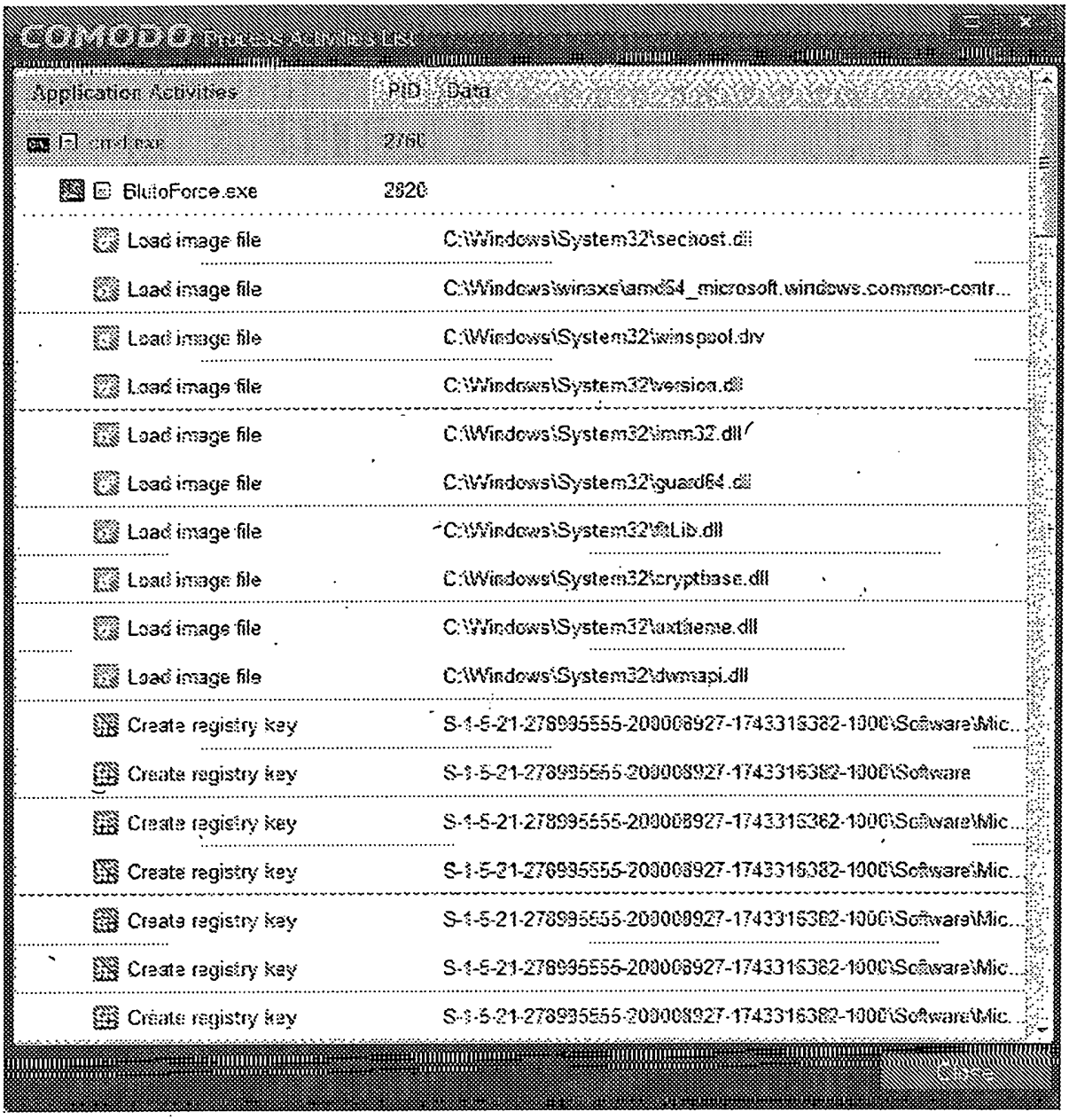
Comodo Internet Security generates a Viruscope alert if a running process performs an action that might represent a threat to your privacy and/or security. Please note that Viruscope alerts are not always definitive proof that malicious activity has taken place. Rather, they are an indication that a process has taken actions that you ought to review and confirm because they have the potential to be malicious. You can review all actions taken by clicking the 'Show Activities' link.

Please read the following advice before answering a Viruscope alert:

1. Carefully read the information displayed in the alert. The 'More Information' section provides you the nature of the suspicious action.




- If you are not sure on the authenticity of the parent application indicated in the 'Application' field, you can safely reverse the changes effected by the process and move the parent application to quarantine by clicking 'Clean'.
- If it is a trusted application, you can allow the process to run, by clicking Ignore and selecting the option from the drop-down.
    - Ignore Once -The process is allowed to run this time only. If the process attempts to execute on future occasions, another Viruscope alert is displayed.
    - Ignore and Add to Trusted Files - The process is allowed to run and and the parent application is moved to the Trusted Files list - effectively making this the 'Ignore Permanently' choice. No alert is generated if the same application runs again.
- To view the activities of the processes, click the Show Activities link at the bottom right. The Process Activities List dialog will open with a list of activities exhibited by the process.



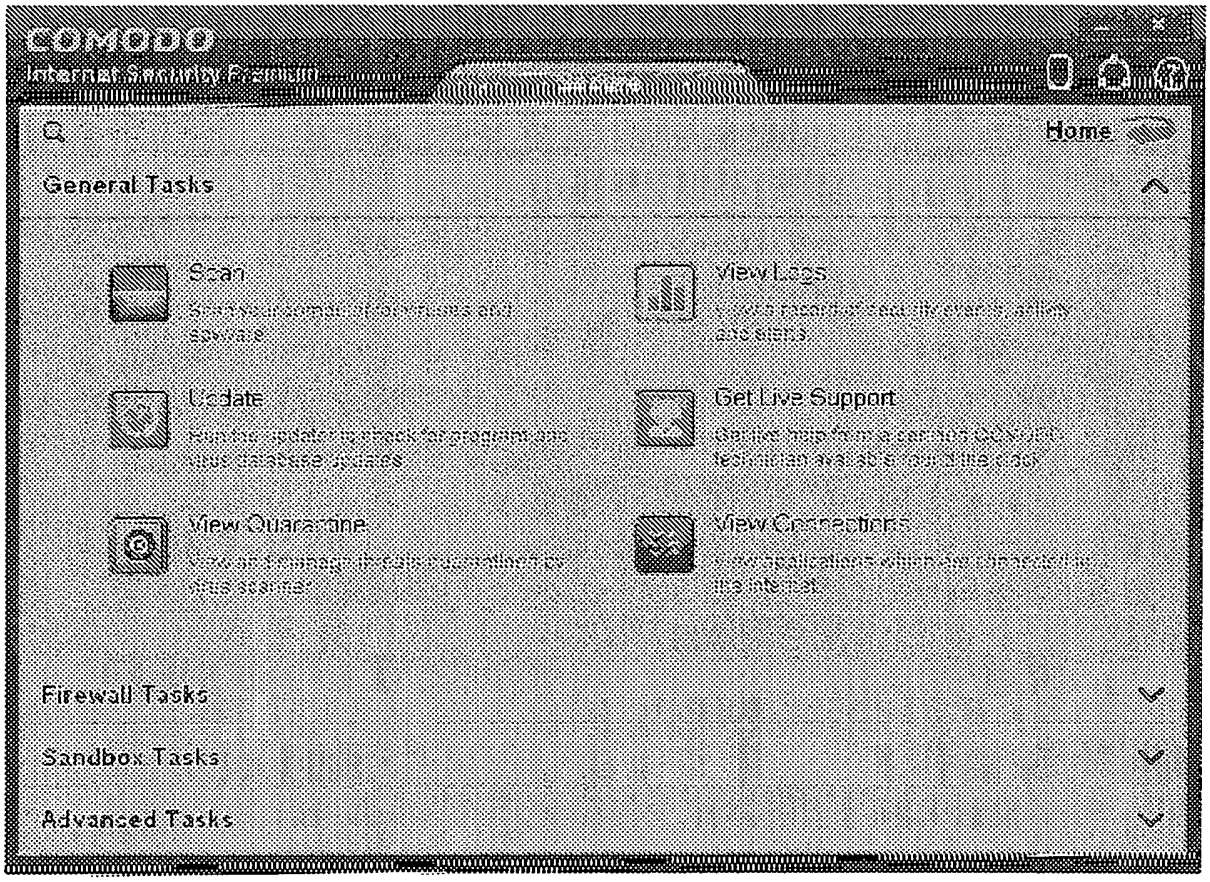

**Column Descriptions**

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

- Data - Displays the file affected by the action.

# 2. General Tasks - Introduction

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

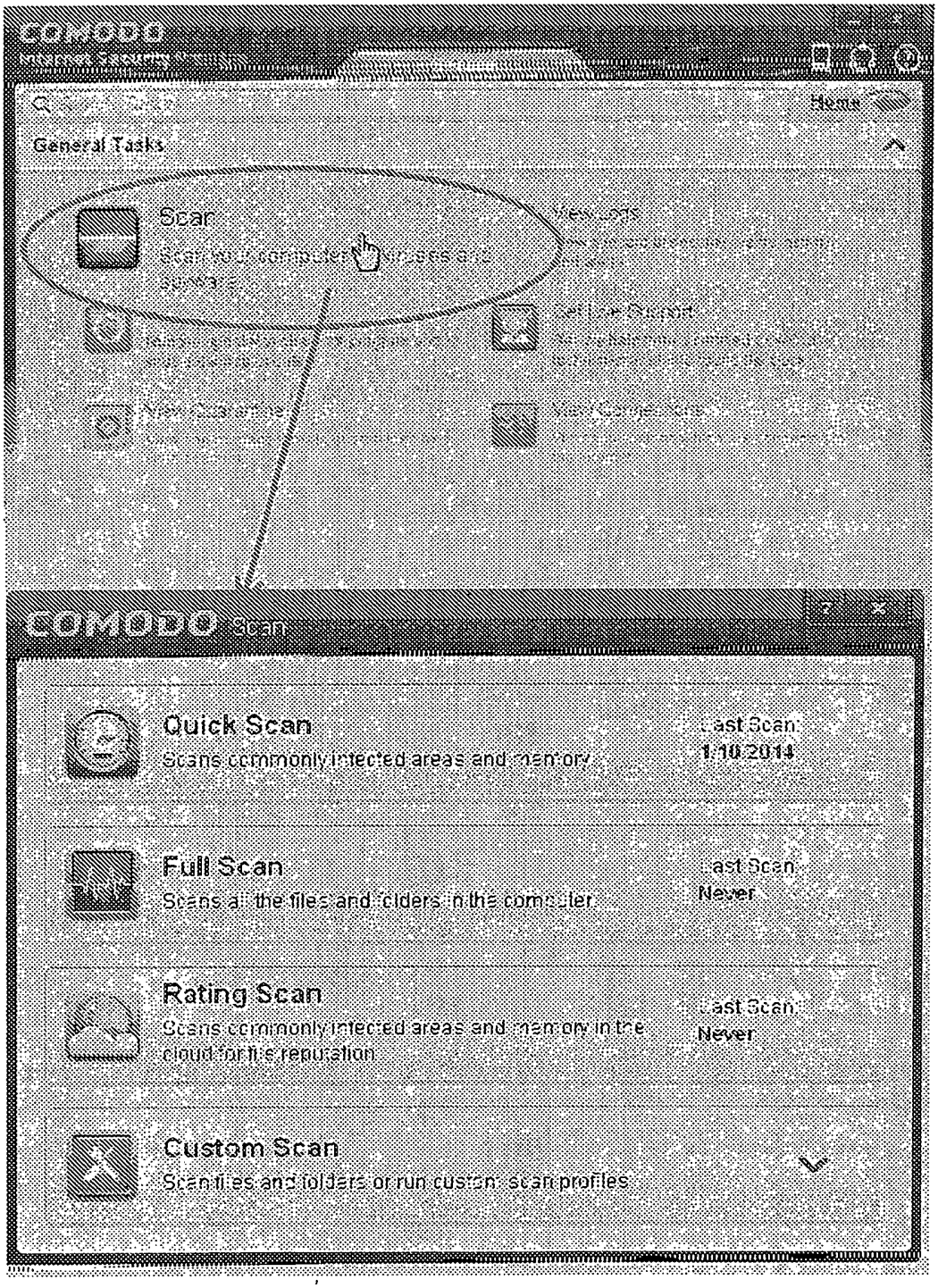



'General Tasks' contains the following areas. Click the links to jump to the help page for that topic.

- Scan and Clean your Computer
- Manage Virus Database and Program Updates
- Manage Quarantined Items
- View CIS Logs
- Get Live Support
- Manage CIS Tasks
- View Active Internet Connections

## 2.1. Scan and Clean Your Computer

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




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

- Run a Quick Scan
- Run a Full Computer Scan
- Run a Rating Scan
- Run a Custom Scan
  - Scan a Folder
  - Scan a File
  - Create and Schedule a Custom Scan

- Scan individual file/folder
- Processing Infected Files

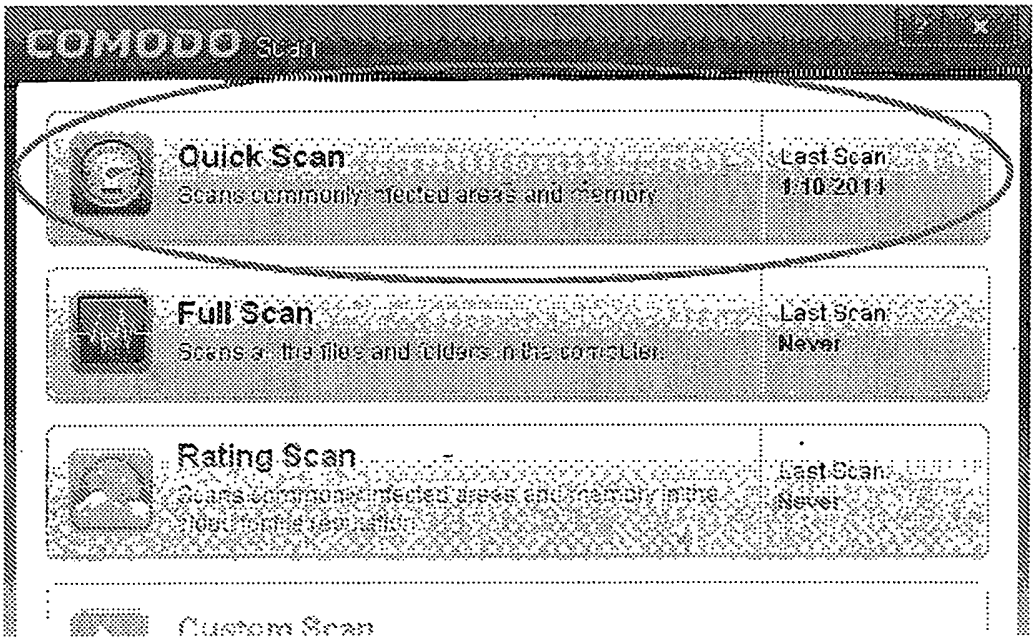
## 2.1.1. Run a Quick Scan

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

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

**To run a Quick Scan**

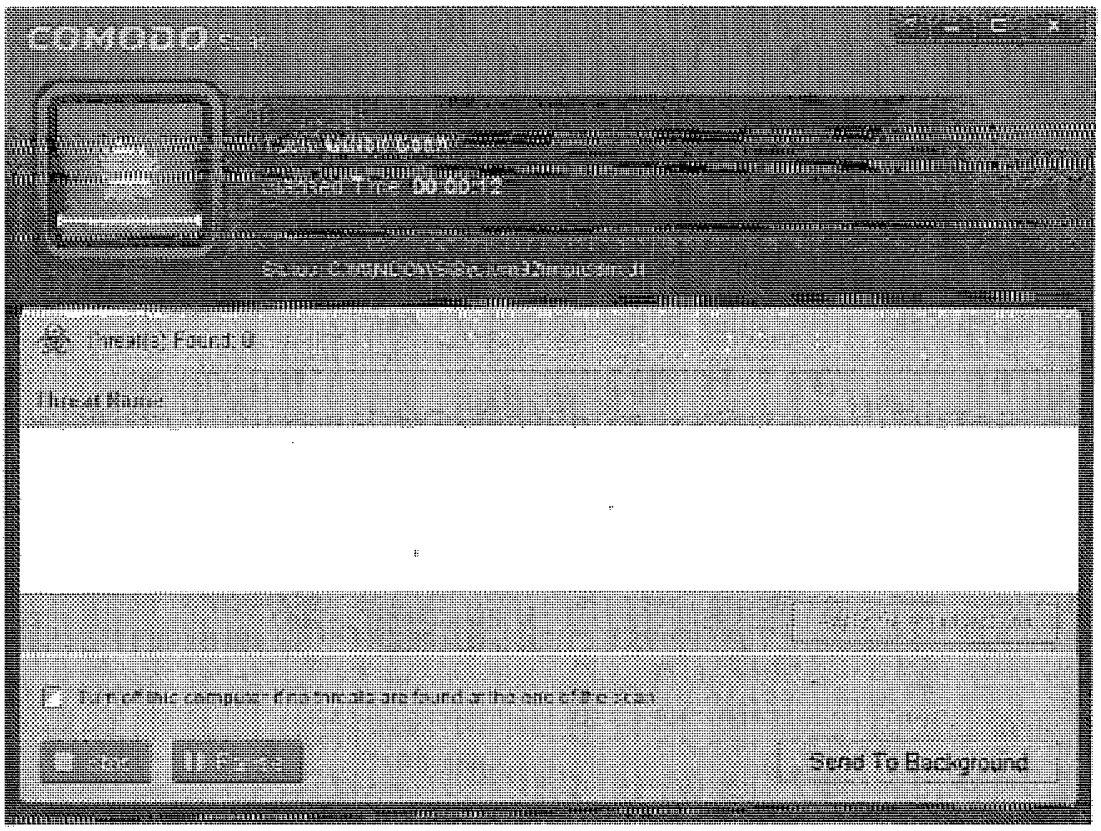
- Click 'Scan' from the General Tasks interface and click 'Quick Scan' from the 'Scan' interface.



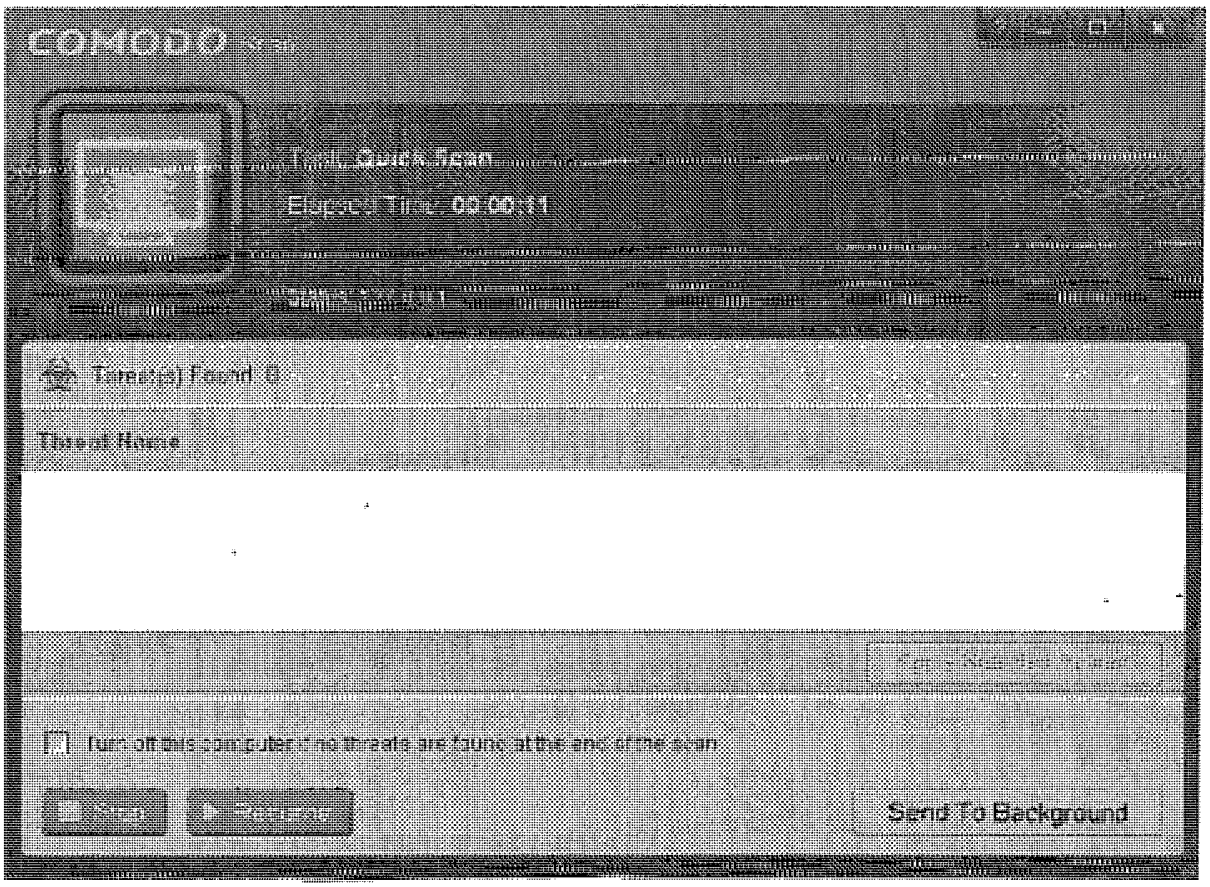

The scanner will start and first check whether your virus signature database is up-to-date:



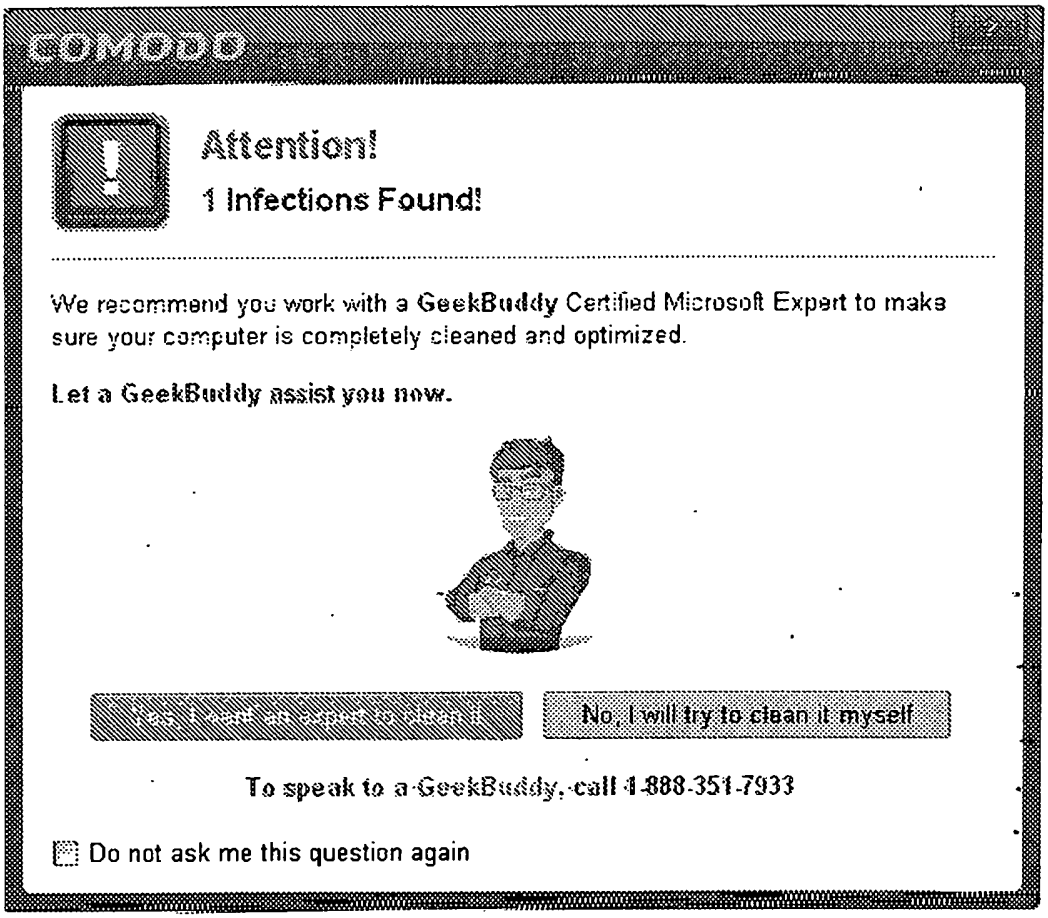

If the database is outdated, the scanner will first download and install the latest version. Once complete, the scan will begin and scan progress will be displayed:




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



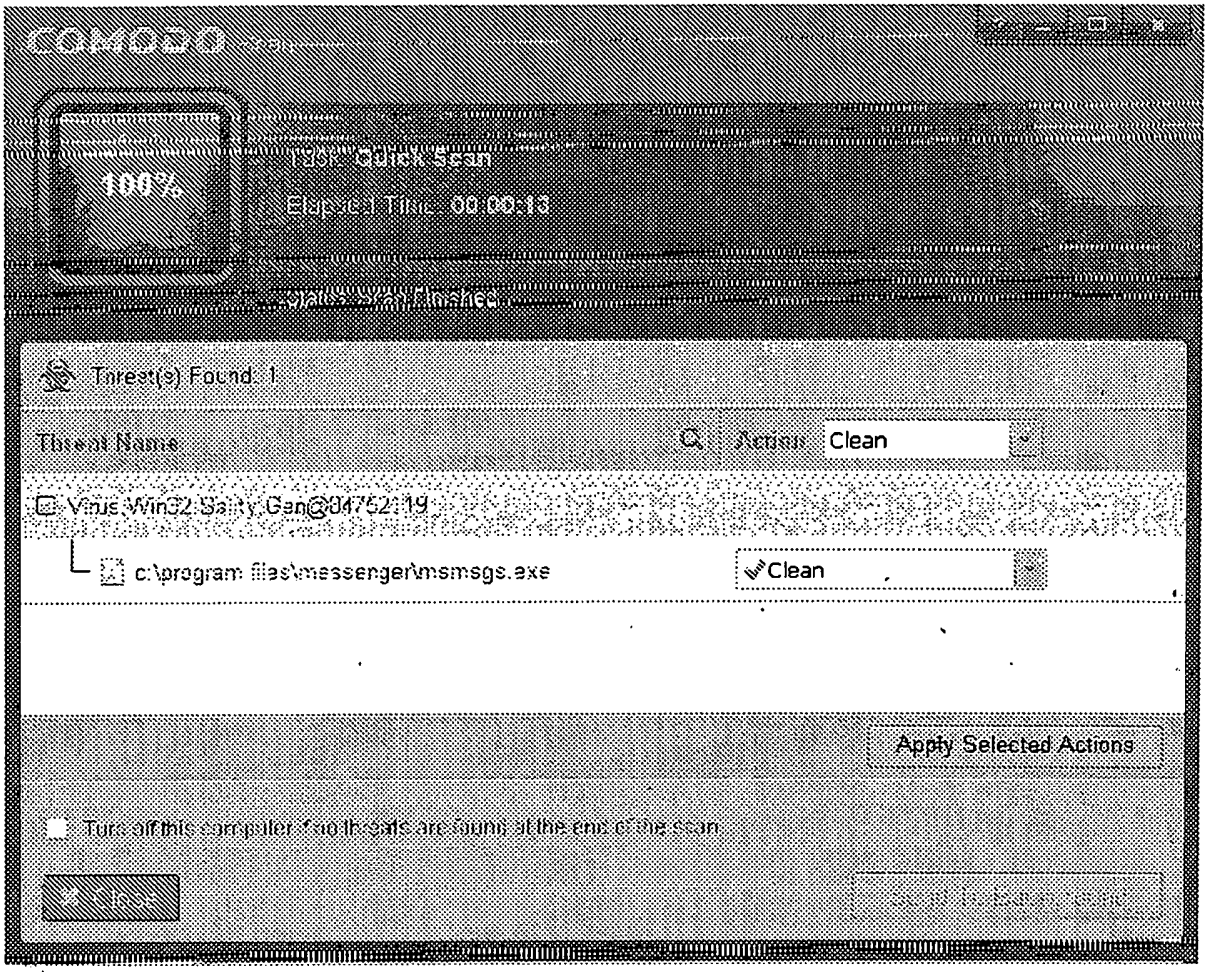

- An alert screen will be displayed at the end of the scan if issues were detected. The alert will display the number of threats/infections discovered and present you with cleaning options:




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

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

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




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

## 2.1.2. Run a Full Computer Scan

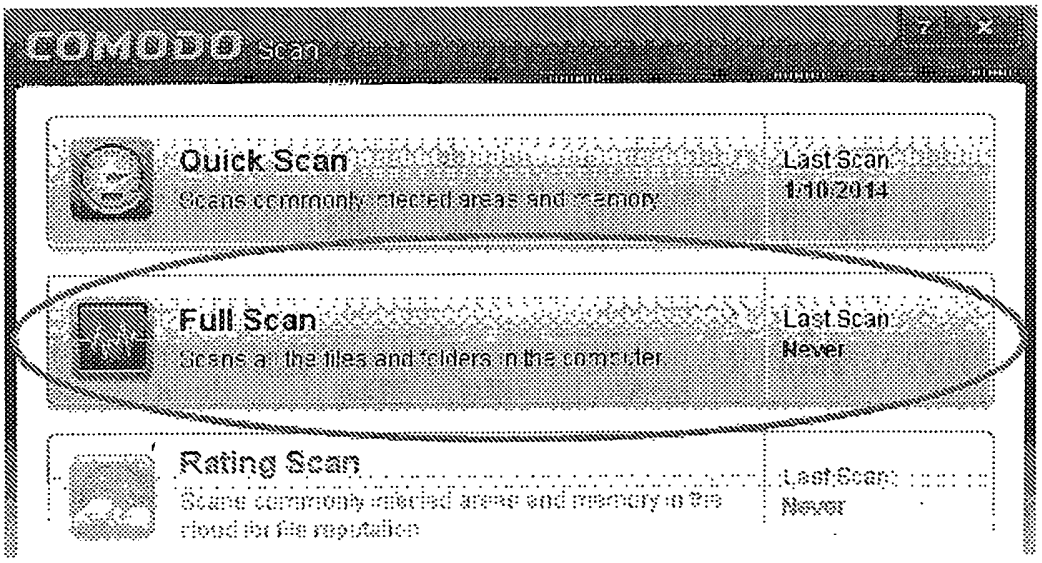
A 'Full System Scan' scans every local drive, folder and file on your system. External devices such as USB drives, storage drives and digital cameras will also be scanned.

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

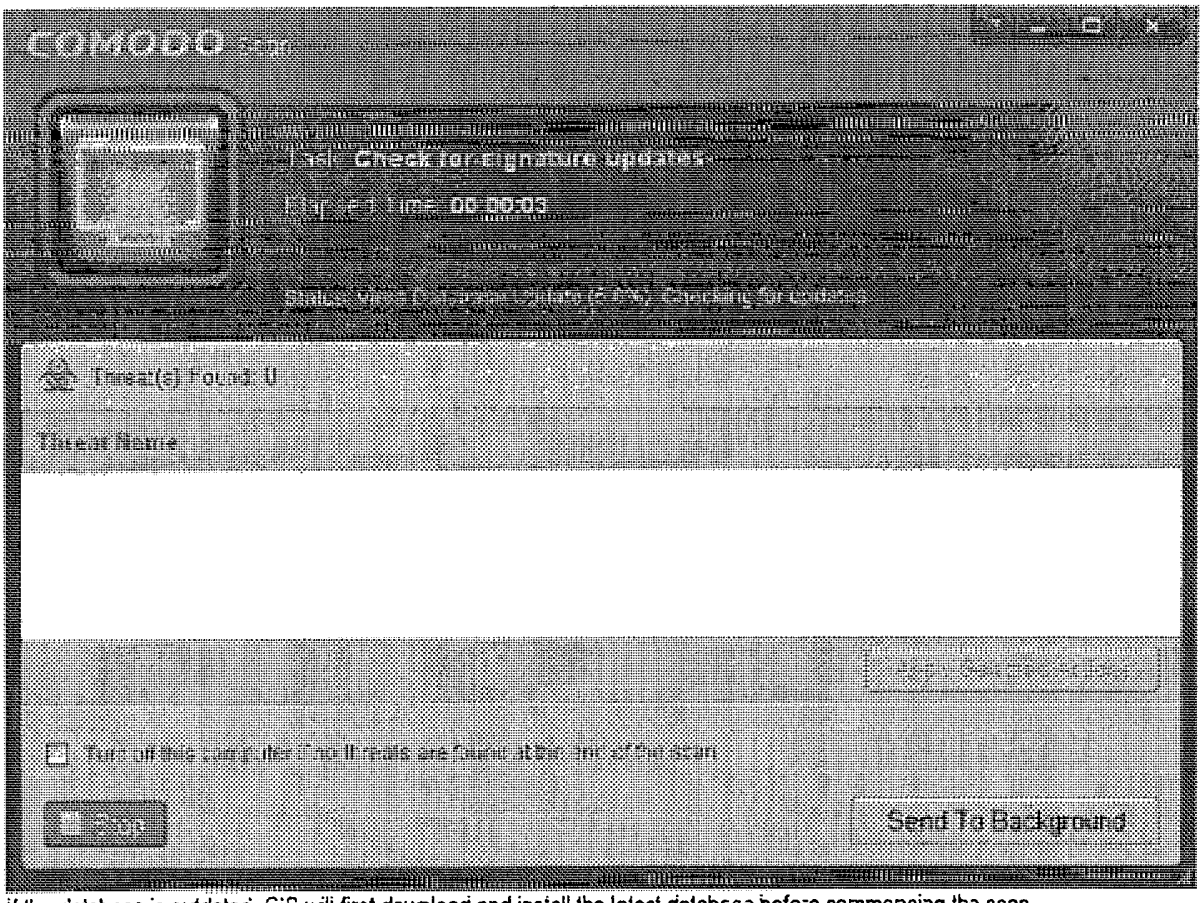
Refer to Antivirus Settings > Scan Profiles for more details.

**To run a Full Computer Scan**

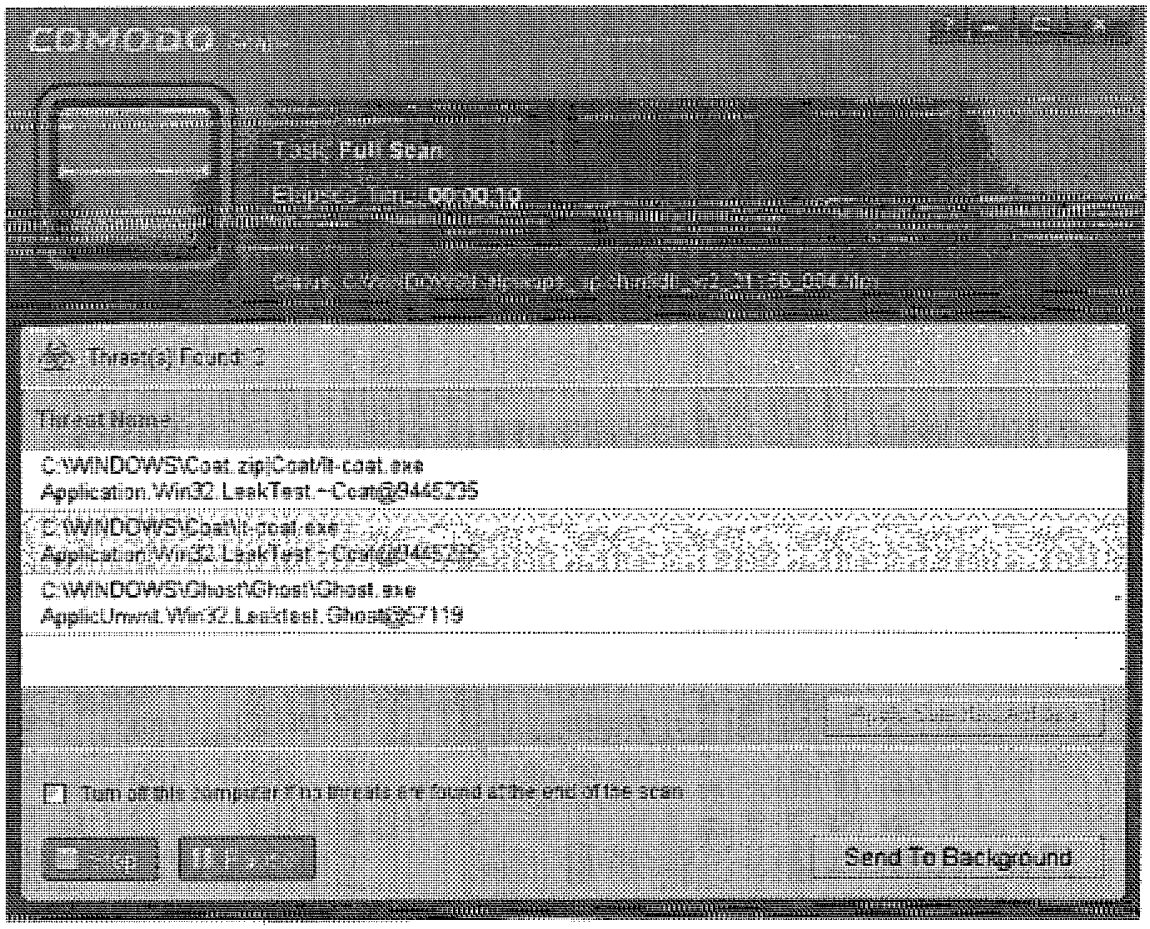
- Click 'Scan' from the General Tasks interface the click 'Full System Scan' from the 'Scan' interface.



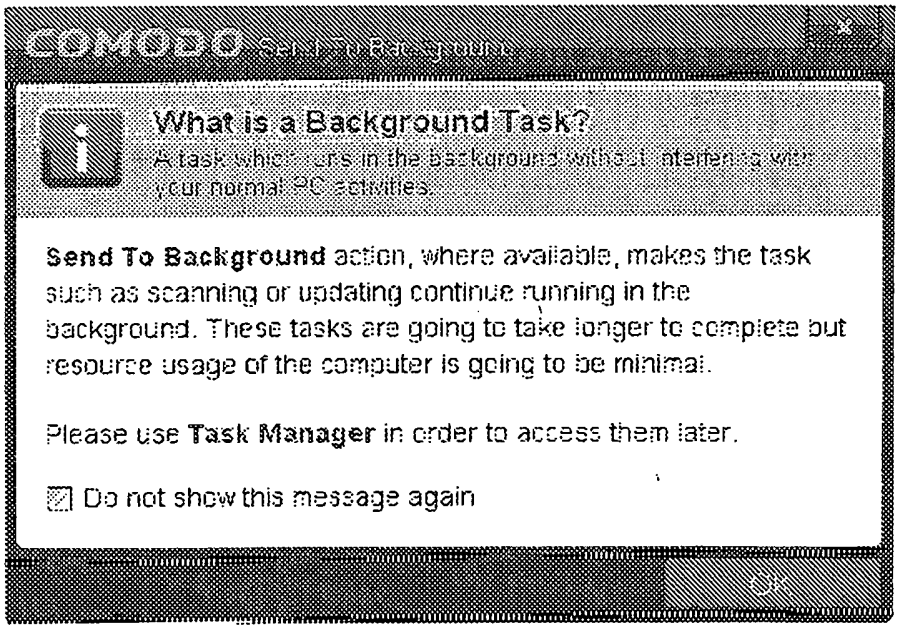

The scanner will start and first check whether your virus signature database is up-to-date.



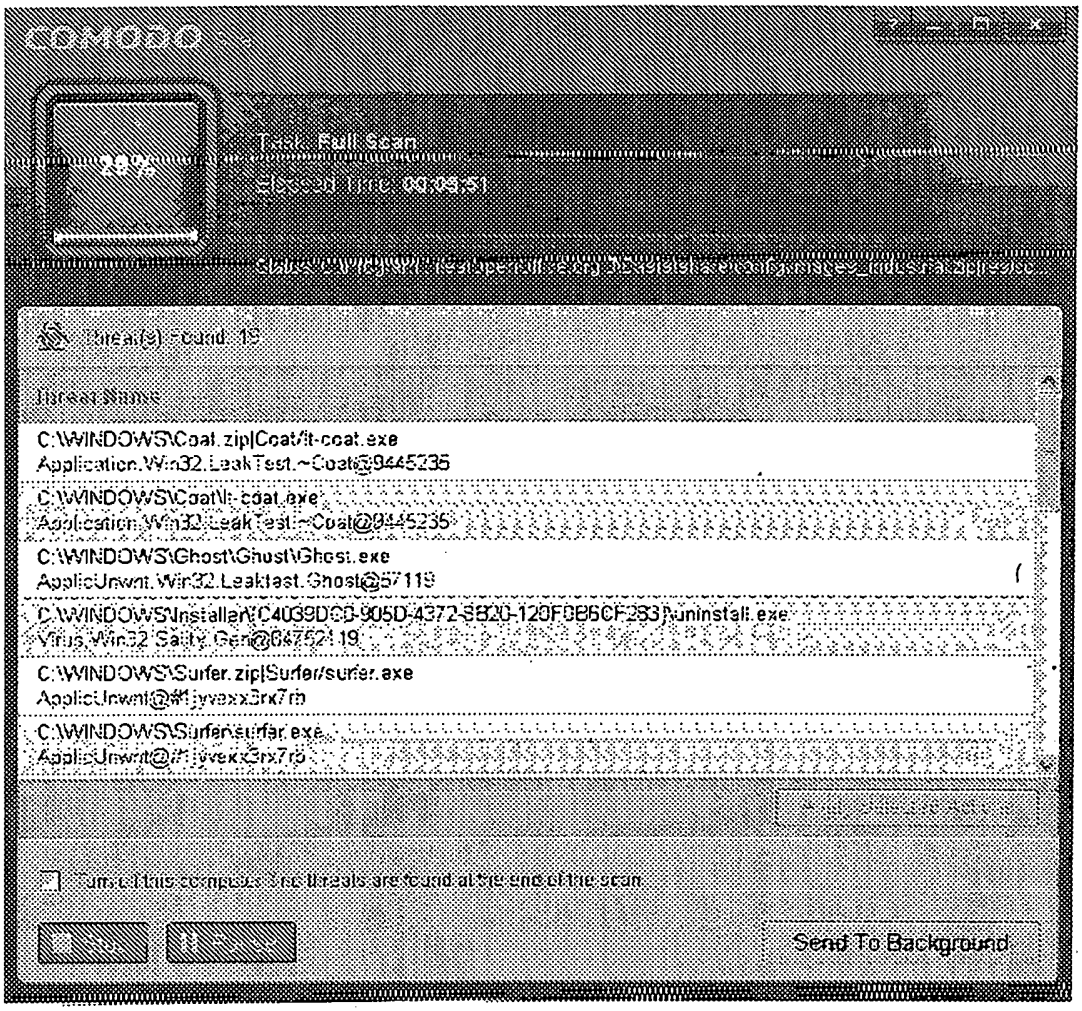

If the database is outdated, CIS will first download and install the latest database before commencing the scan.



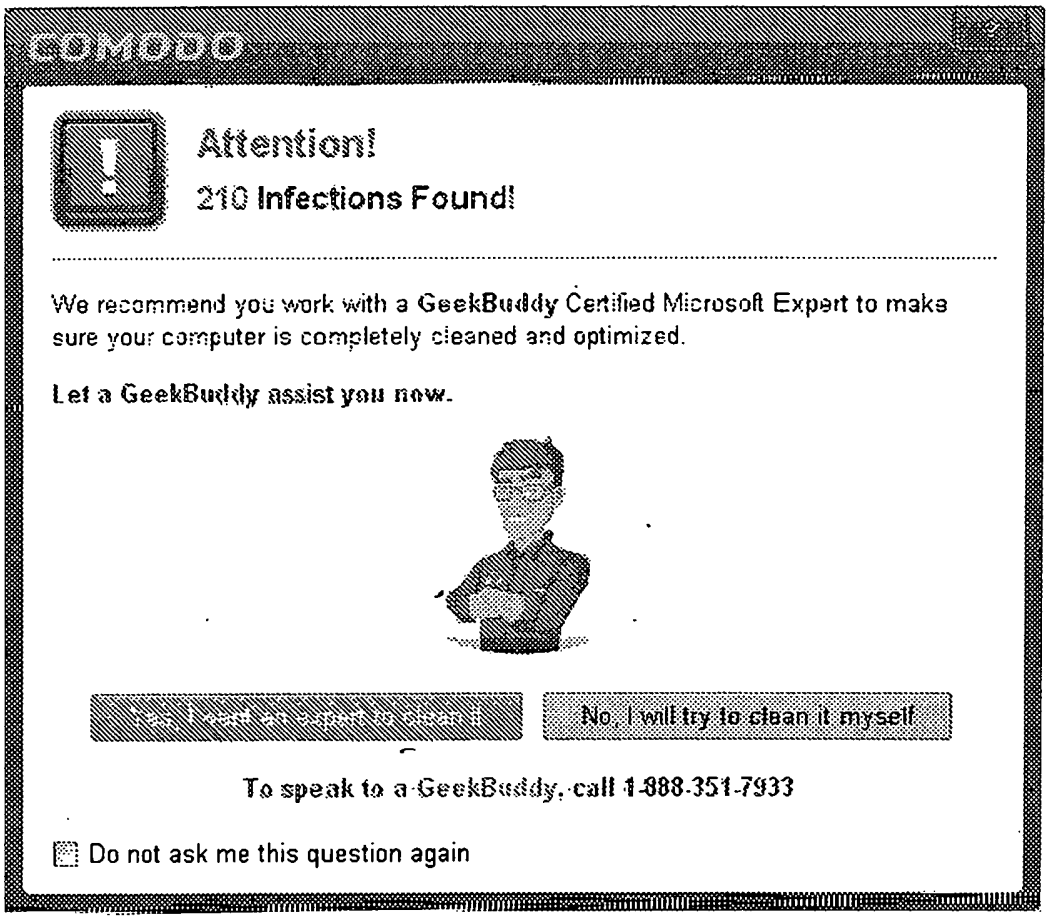

- You can pause, resume or stop the scan by clicking the appropriate button. If you want to run the scan in the background, click 'Send to Background'.



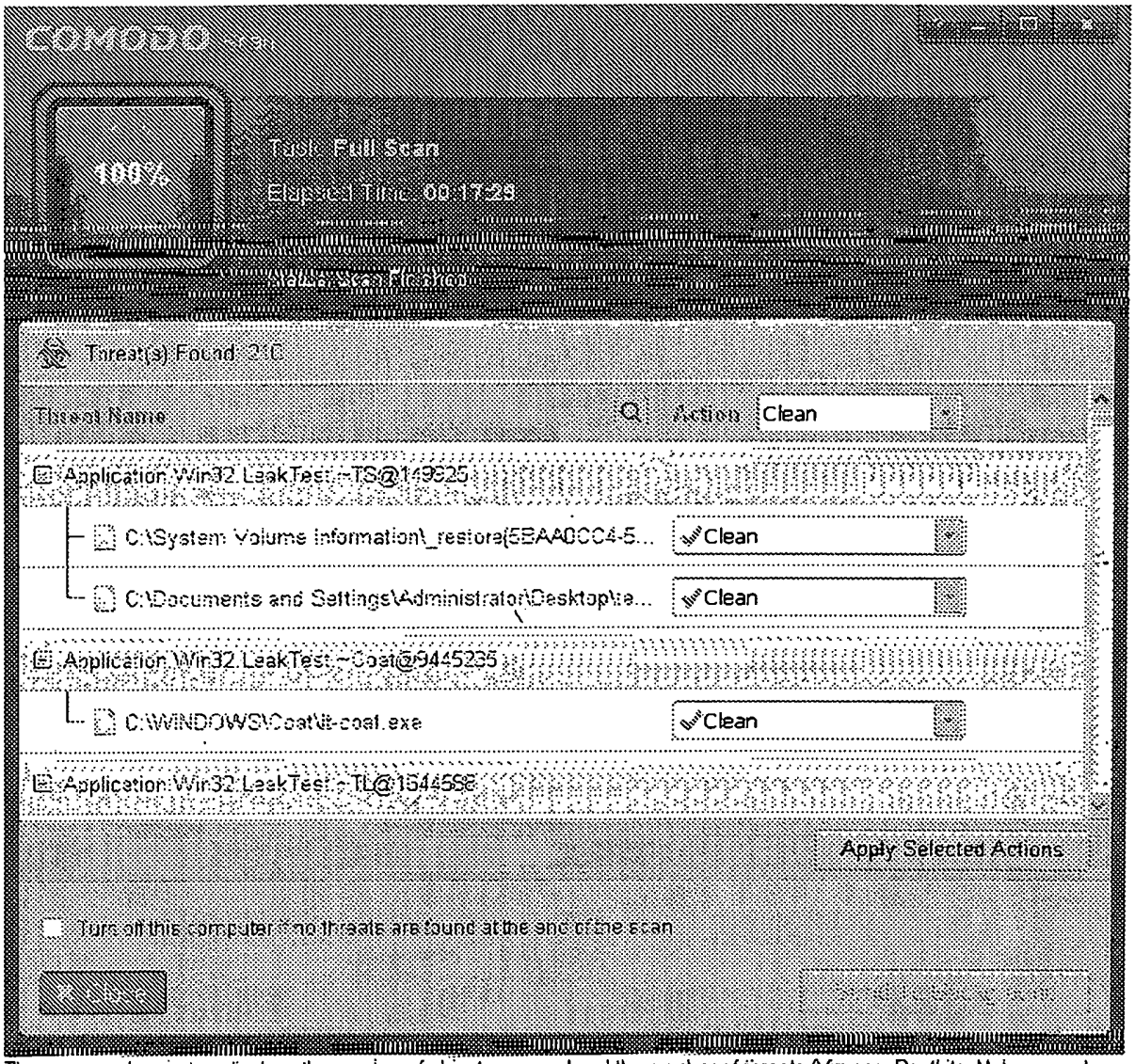

If you send to the background, you can continue to check scan progress by clicking 'Task Manager' on the home screen or by clicking 'Open Task Manager' icon from the 'Advanced Tasks' interface.




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




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




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

## 2.1.3. Run a Rating Scan

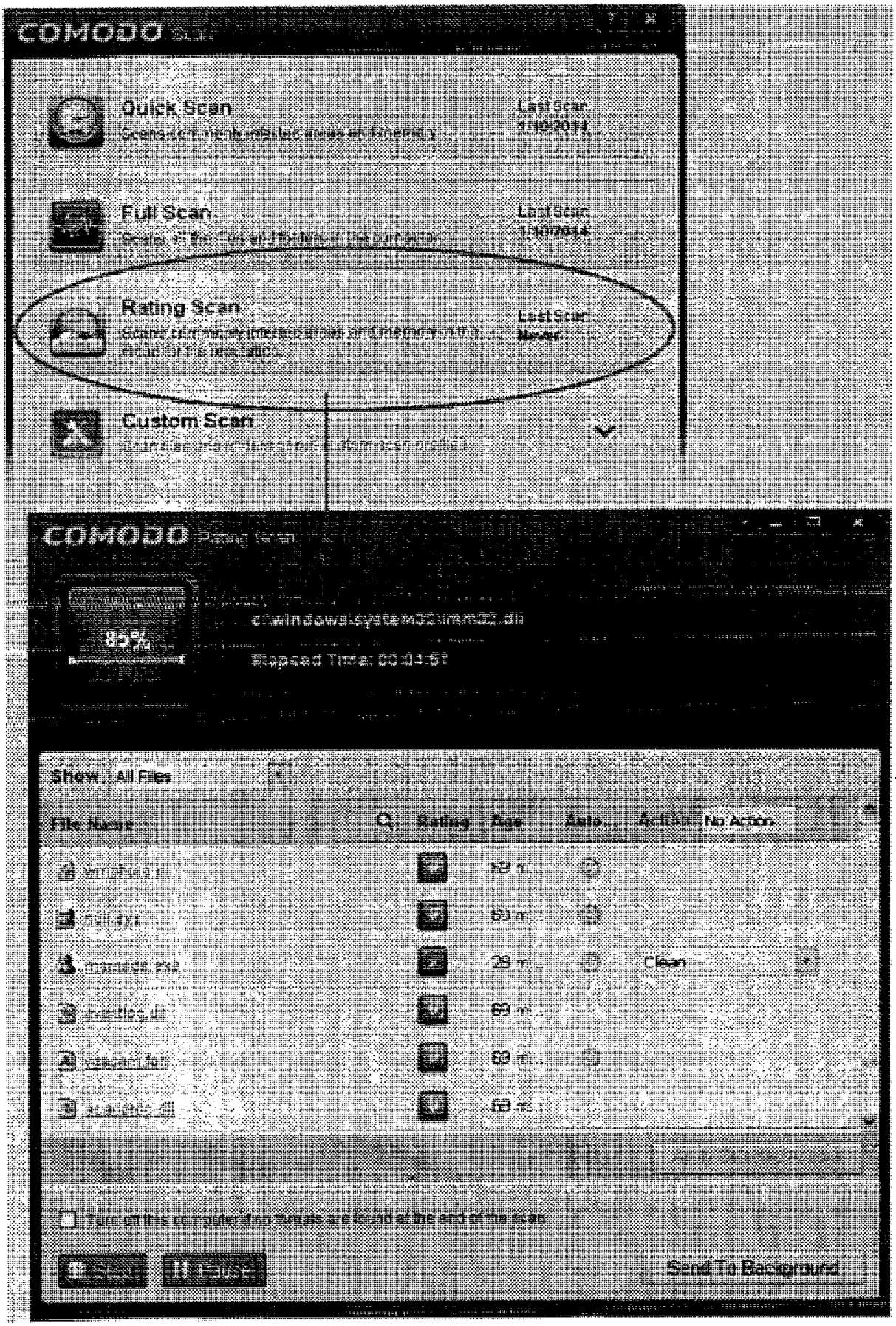
The 'Rating Scan' feature runs a cloud-based assessment on files on your computer to assess how trustworthy they are.

Based on the trustworthiness, the files are rated as:

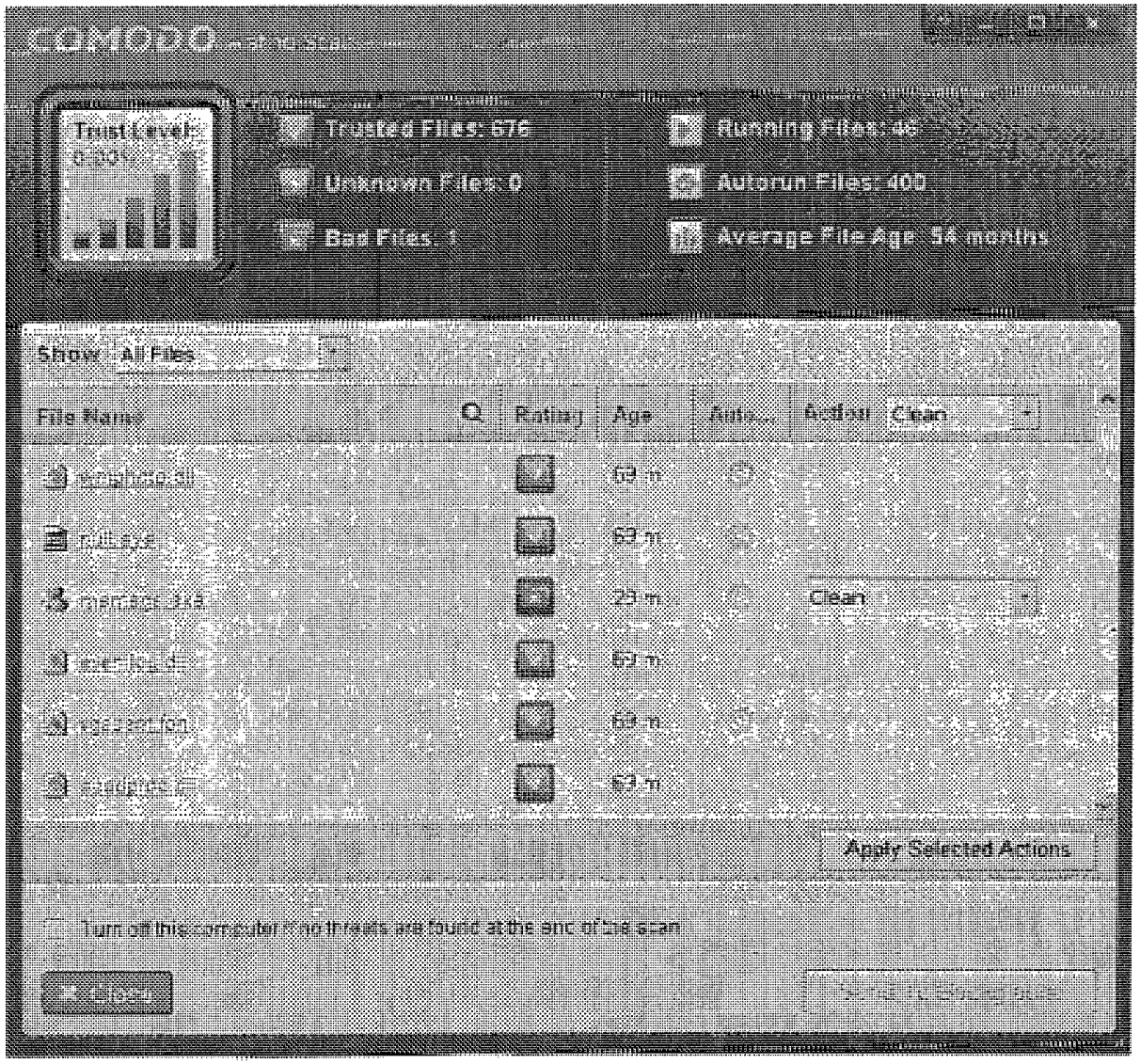
- Trusted - the file is safe
- Unknown - the trustworthiness of the file could not be assessed
- Bad - the file is unsafe and may contain malicious code. You will be presented with disinfection options for such files.

**To run a Rating scan**

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

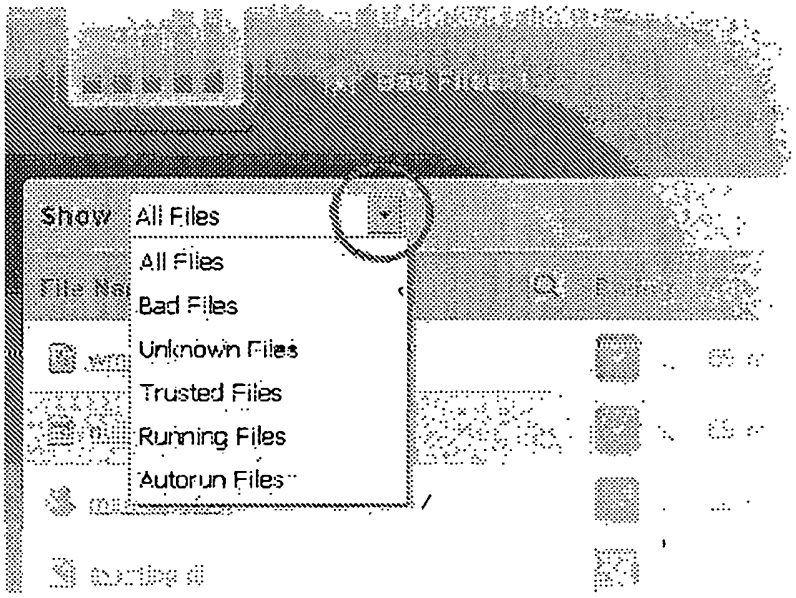



After the cloud scanners have finished their analysis, file ratings will be displayed as follows:

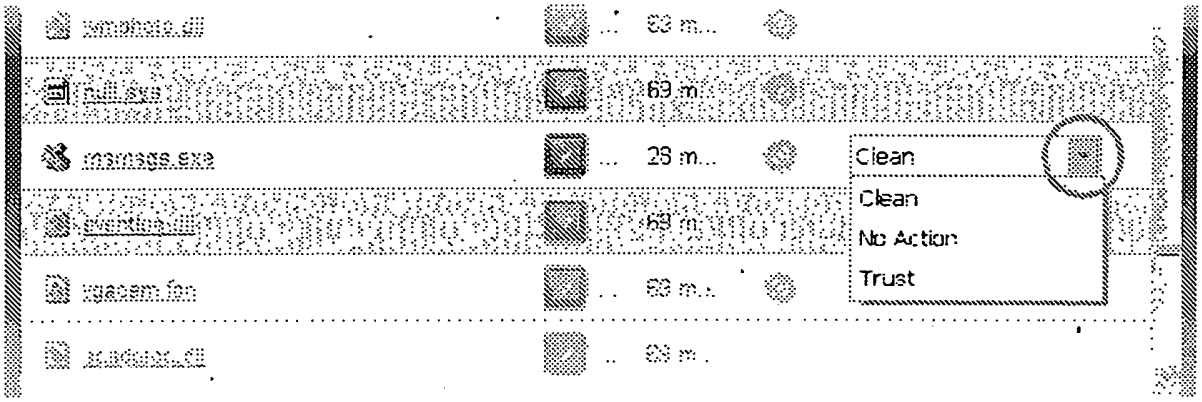



- **File Name**: The file which was scanned
- **Rating**: The rating of the file as per the cloud based analysis
- **Age**: The period of time that the file has been stored on your computer
- **Autorun**: Indicates whether the file is an auto-run file or not. Malicious auto-run files could be ruinous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

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

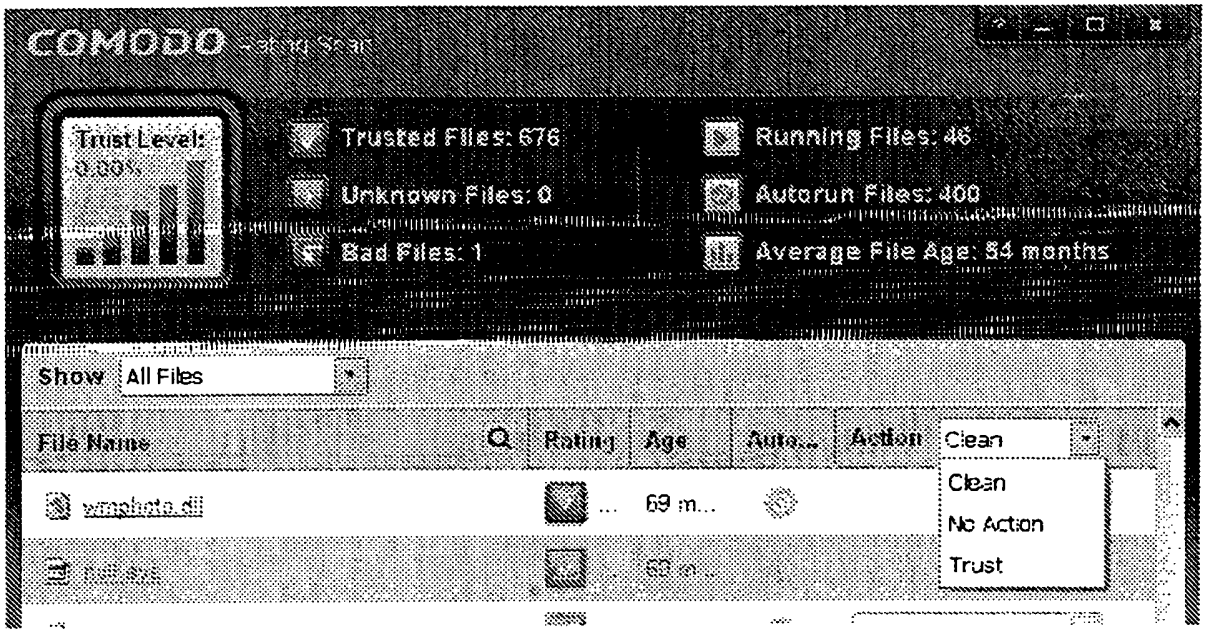



Each file identified as 'Bad' is accompanied with a drop-down box that allows you to 'Clean', 'Trust' or 'Take no action'

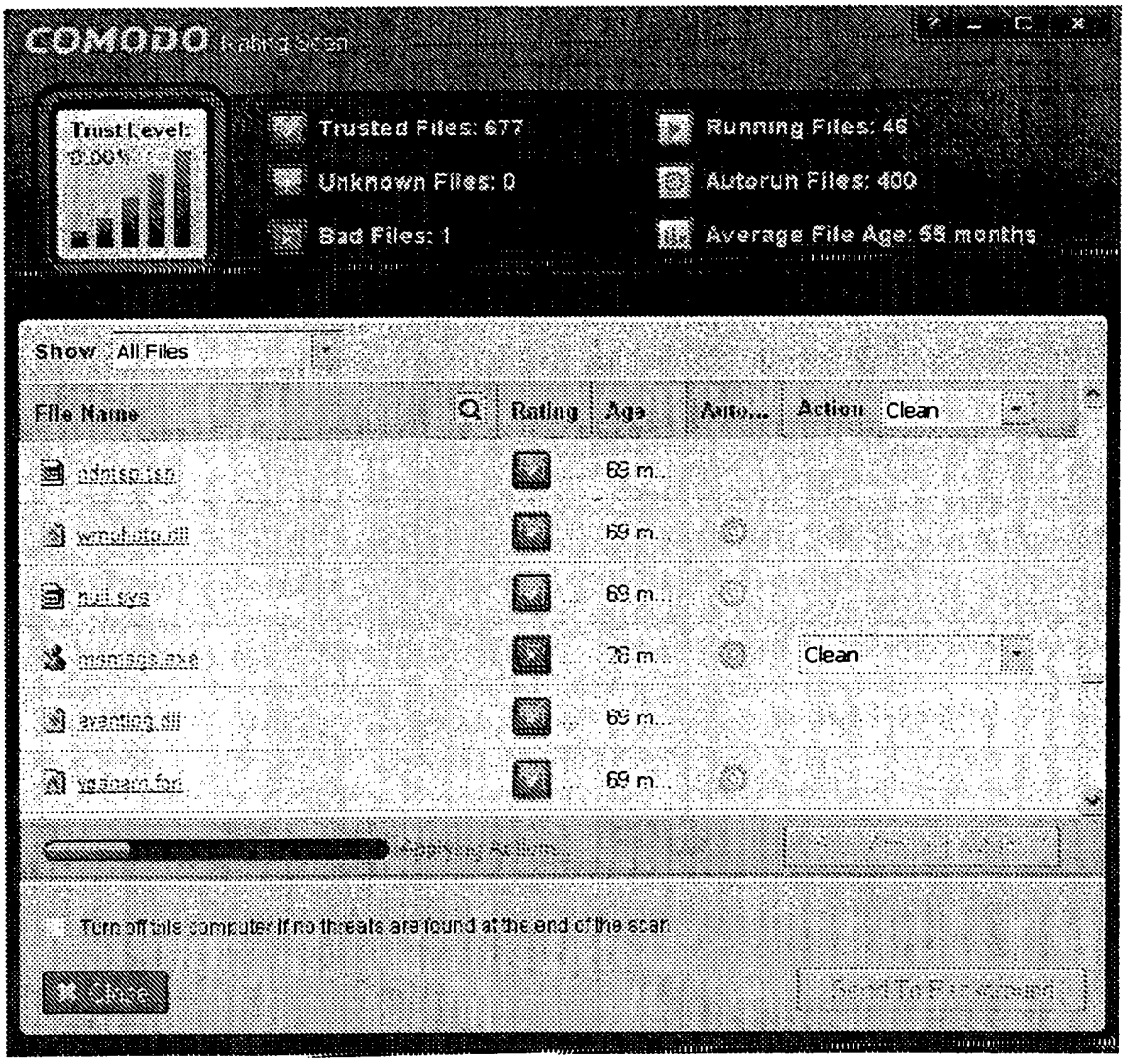



- **Clean** - If a disinfection routine is available for the selected infection(s), Comodo Antivirus will disinfect the application and retain the application file. If a disinfection routine is not available, Comodo Antivirus will move the files to Quarantine for later analysis. See Manage Quarantined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

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




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

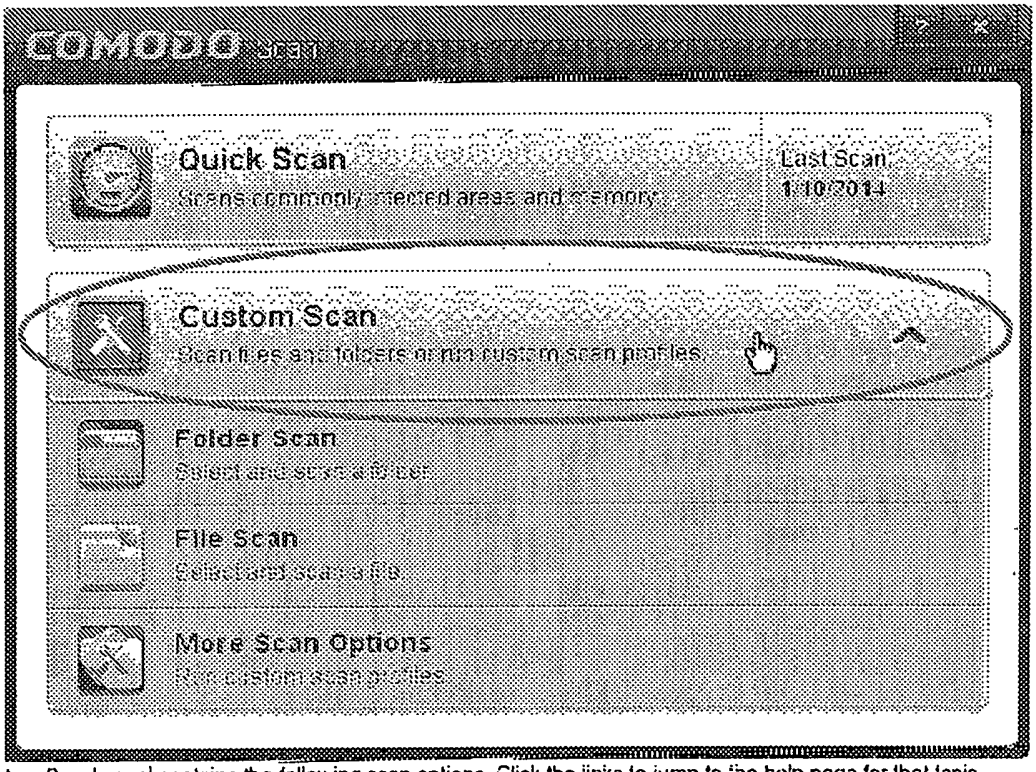


- Click 'Close' to exit.

## 2.1.4. Run a Custom Scan

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

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




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

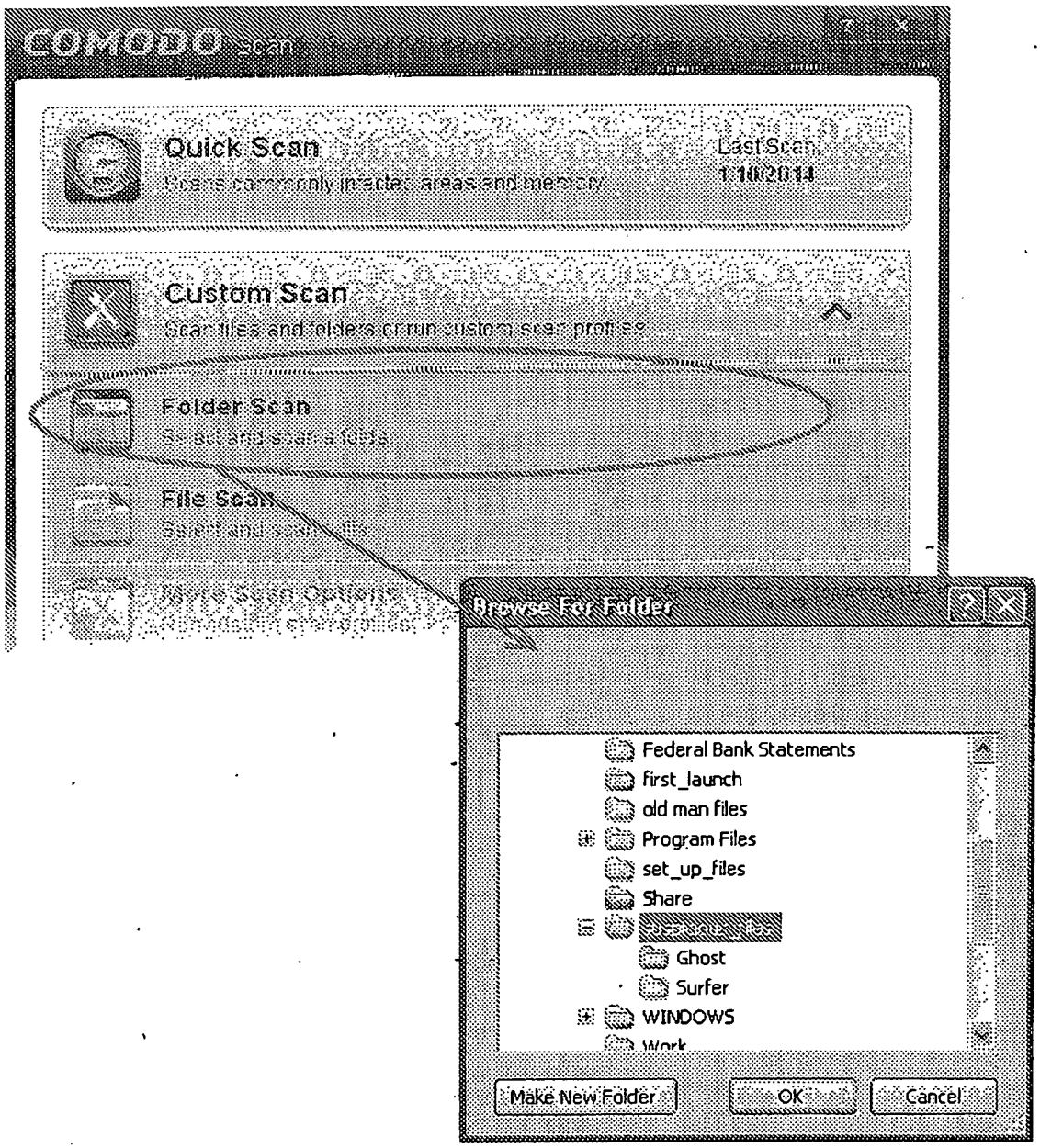
- Folder Scan - scan individual folders
- File Scan - scan an individual file
- More Scan Options - create a custom scan profile here

### 2.1.4.1. Scan a Folder

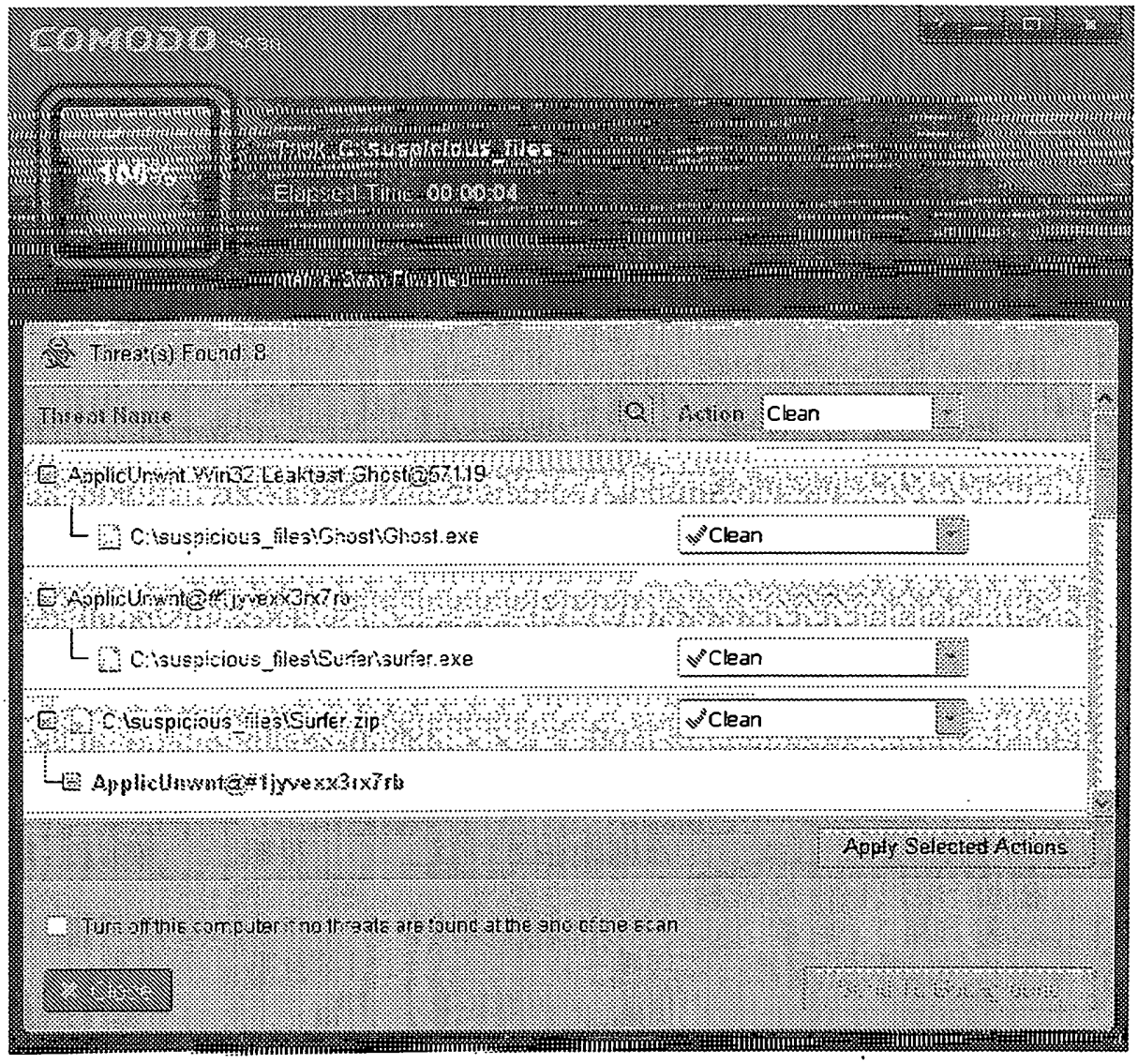
The custom scan allows you to scan a specific folder stored in your hard drive, CD/DVD or in external devices like a USB drive connected to your computer. For example you might have copied a folder from another computer in your network, an external device or downloaded from Internet and want to scan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

**To scan a specific folder**

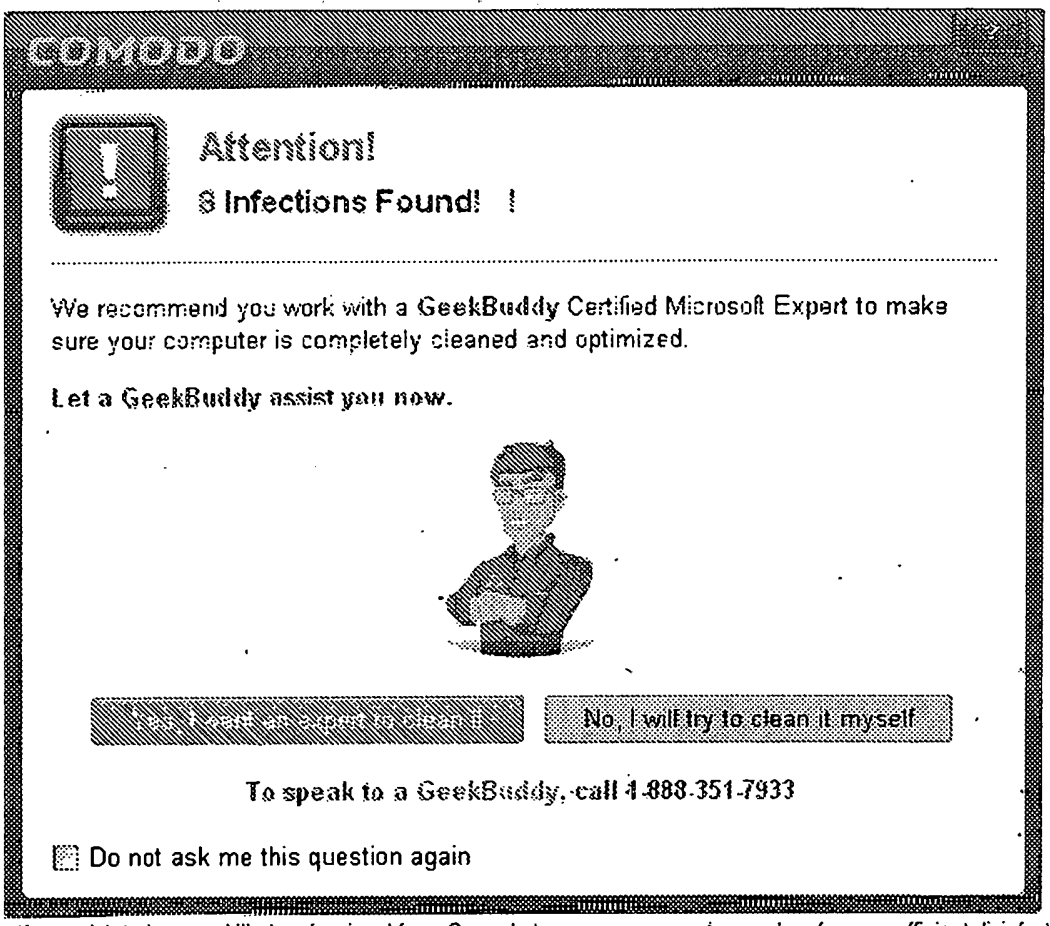
- Click Scan from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'Folder Scan' from the 'Custom Scan' pane
- Navigate to the folder to be scanned in the 'Browse for Folder' window and click OK.



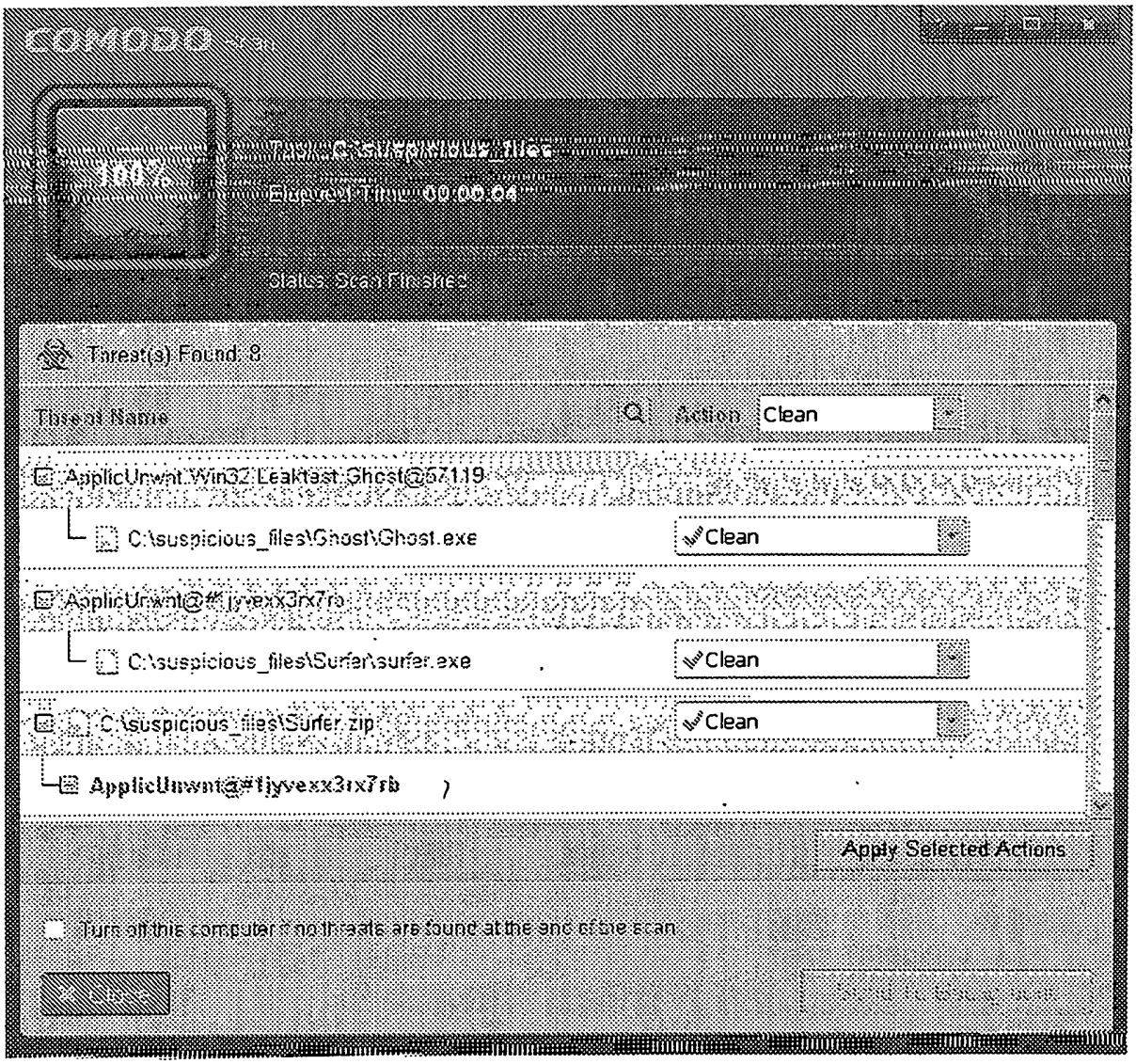

The folder will be scanned instantly and the results will be displayed with a list of any identified infections




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




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




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

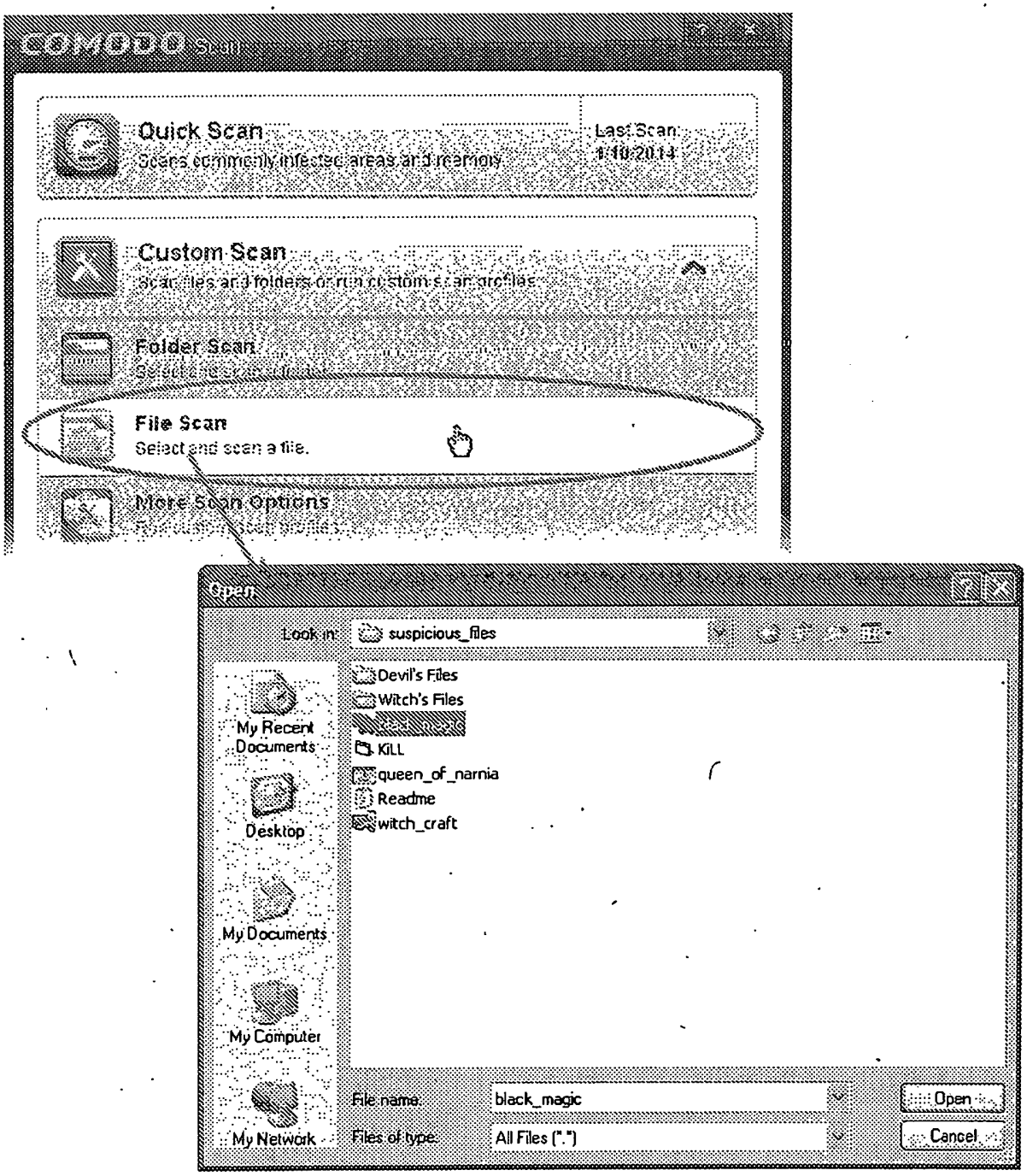
Tip: Alternatively, you can perform an express scan on a folder by dragging and dropping it onto the CIS interface or by right clicking it. Refer to Scan Individual File/Folder for more details.

## 2.1.4.2. Scan a File

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

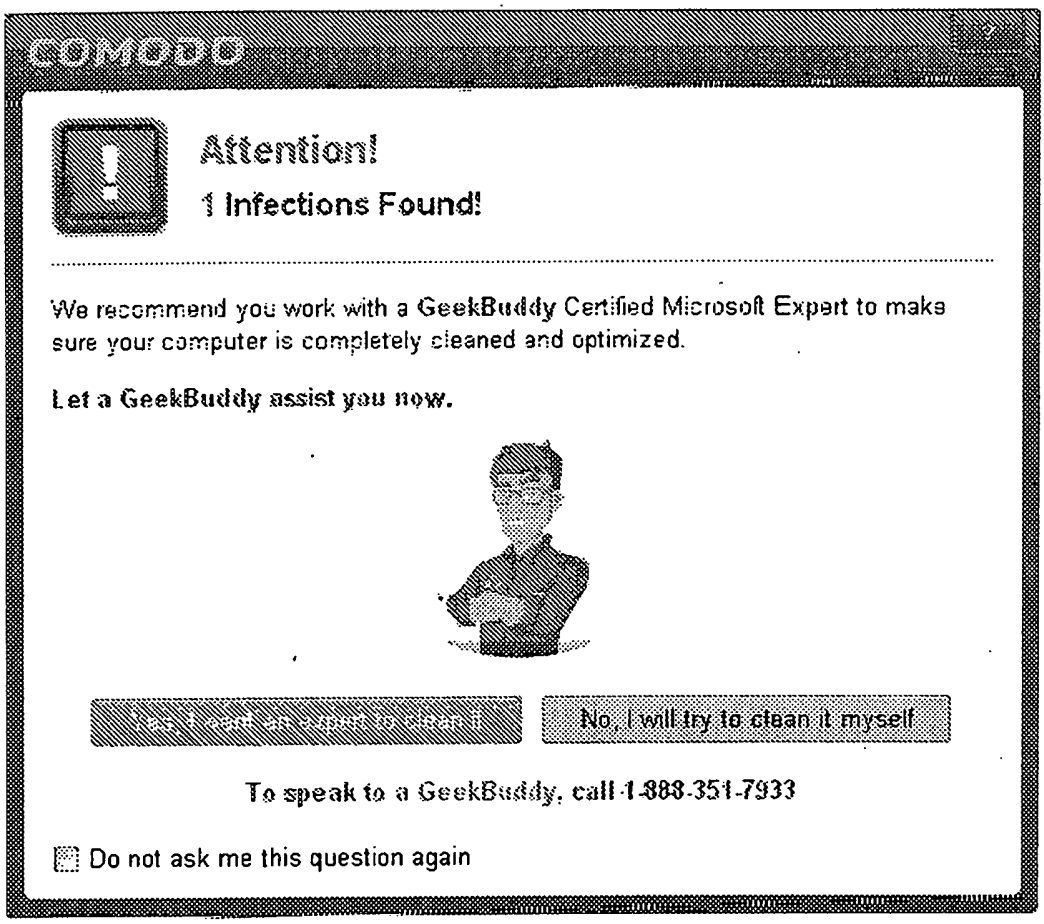
**To scan a specific file**

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

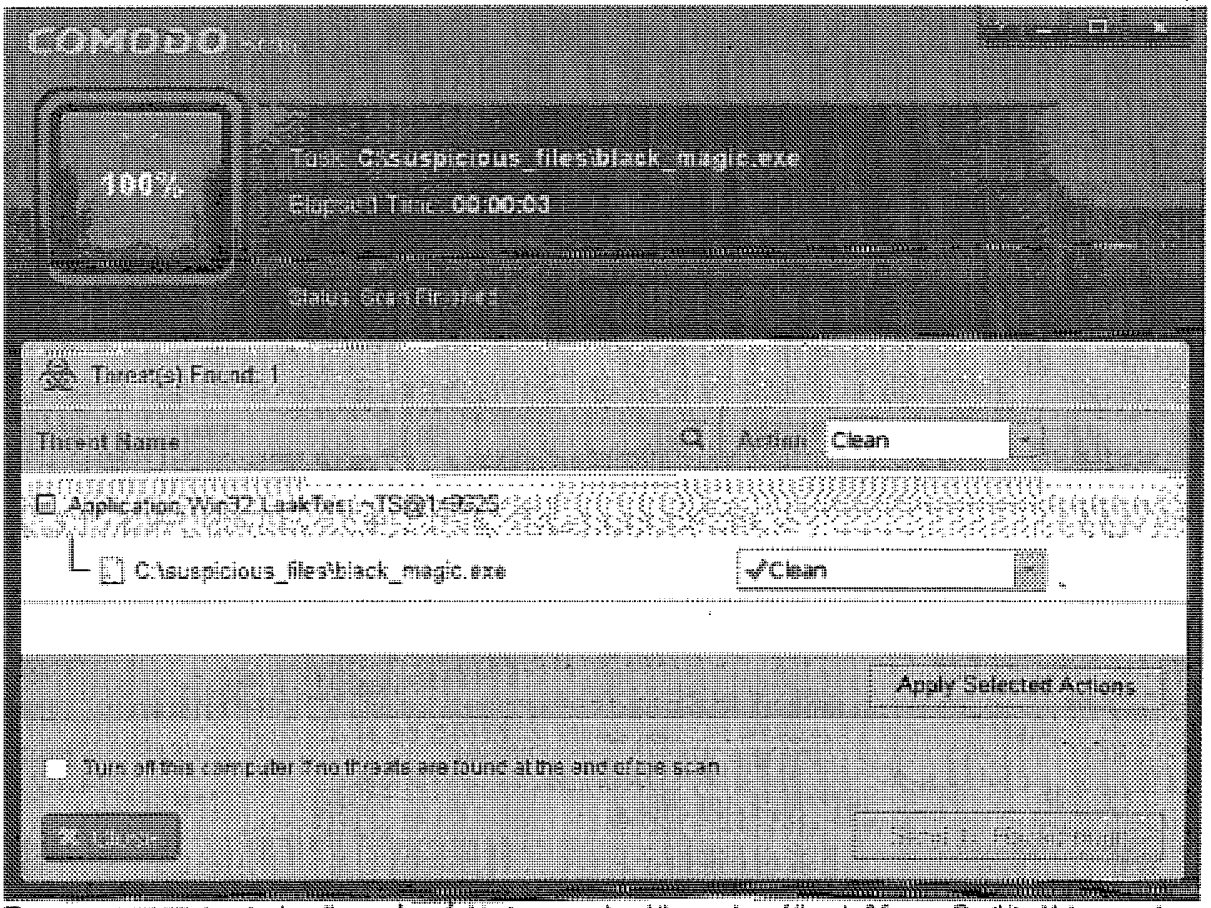



The file will be scanned instantly.

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




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




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

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

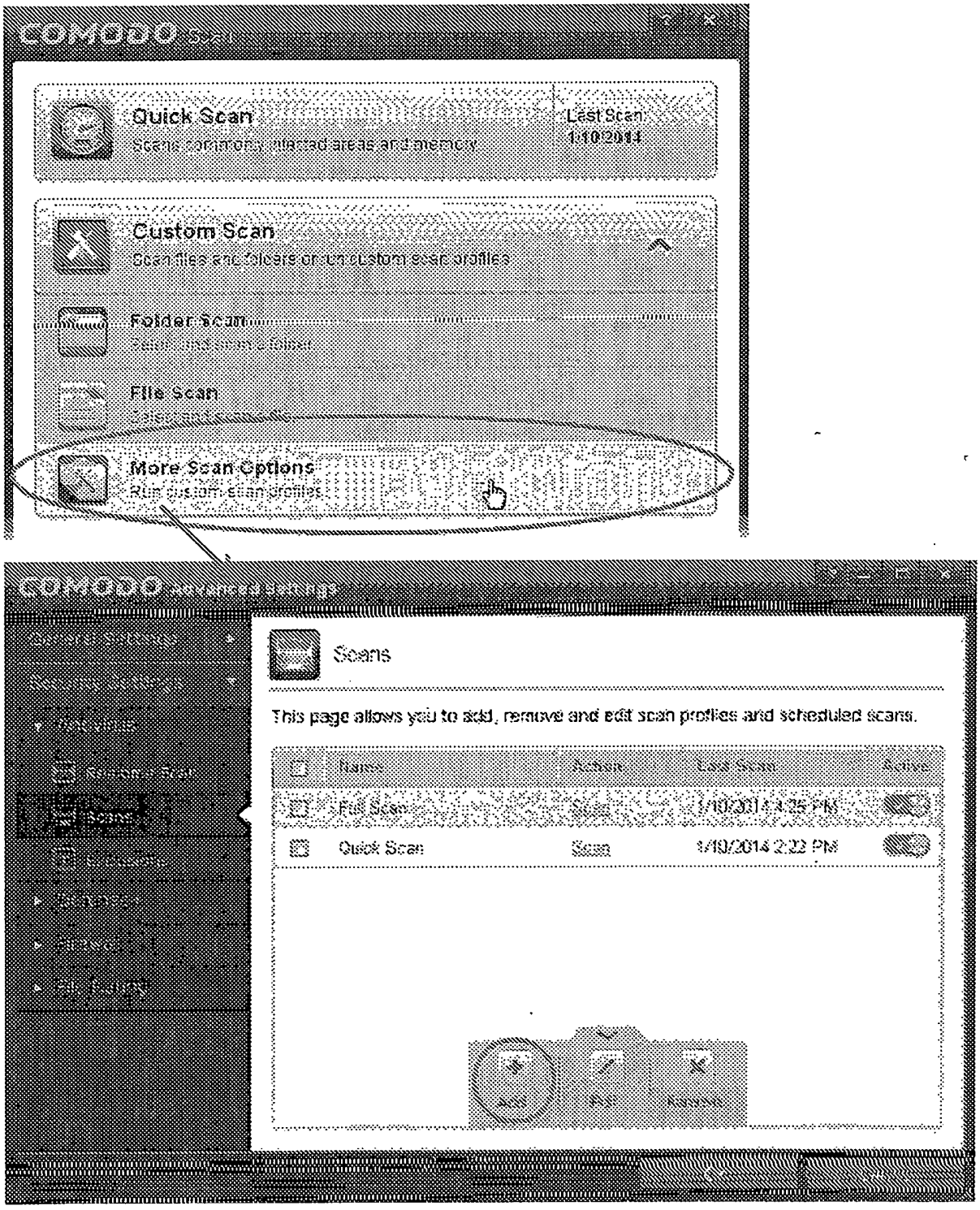
## 2.1.4.3. Create, Schedule and Run a Custom Scan

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

- Creating a Scan Profile
- Running a custom scan

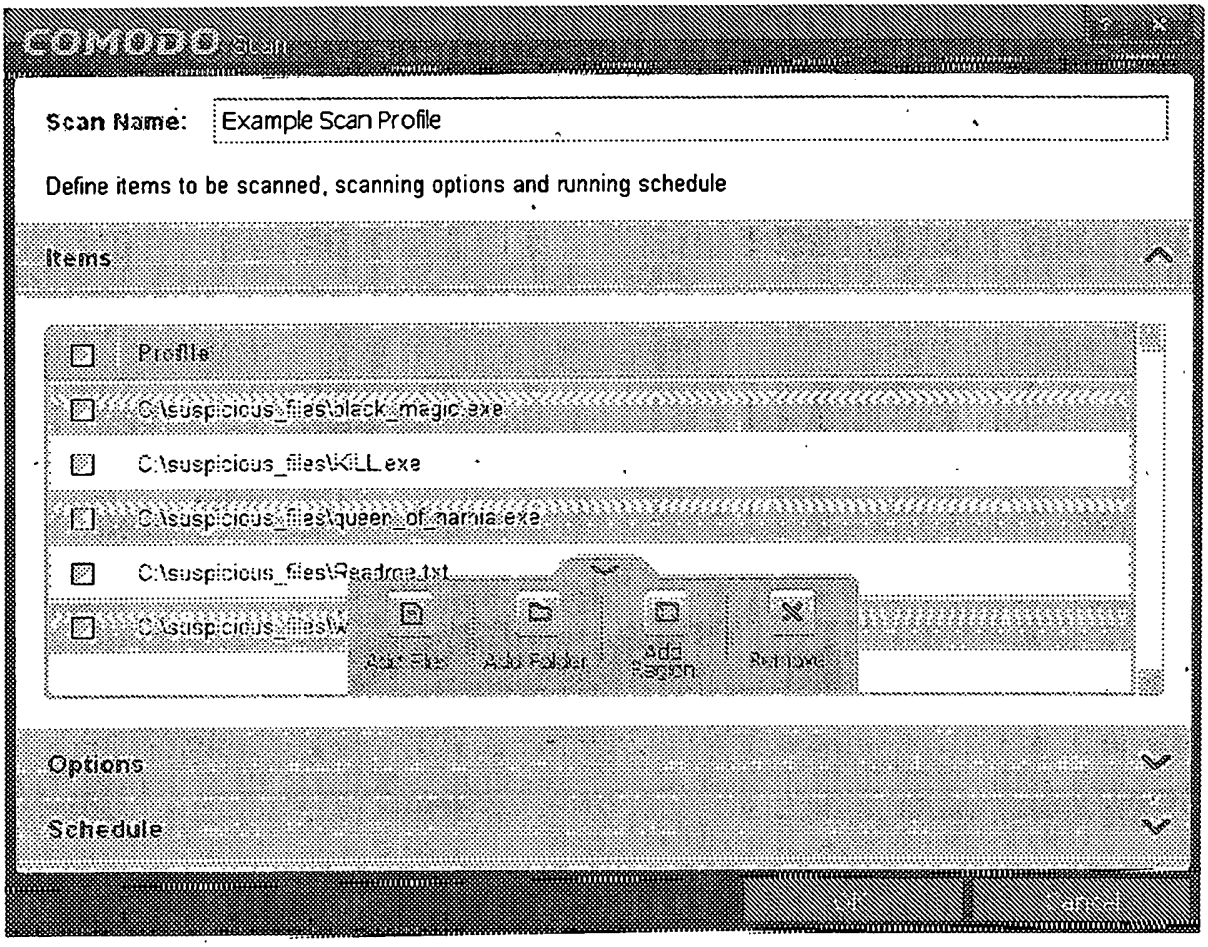
**To create a custom profile**

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

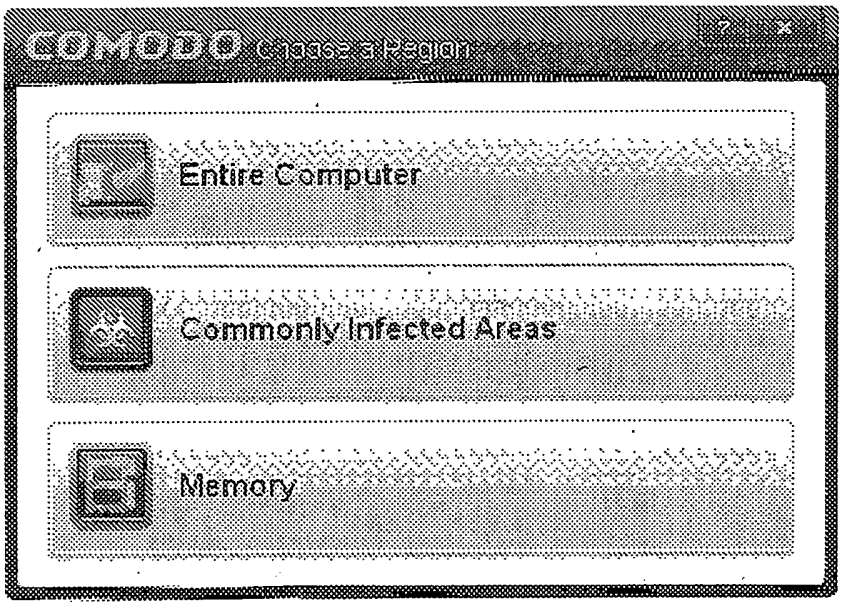



The scan profile interface will be displayed.

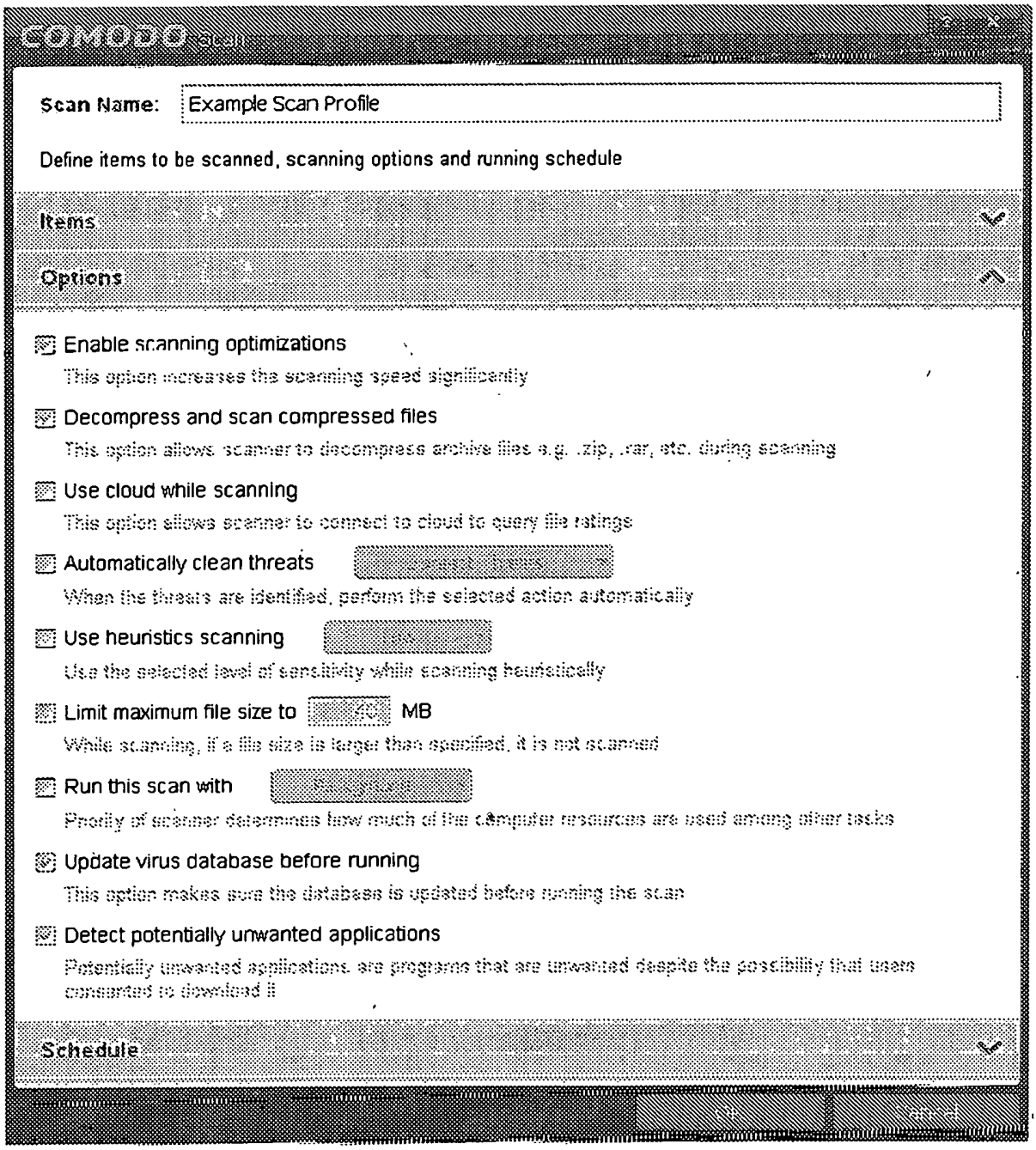
- Type a name for the profile in the 'Scan Name' text box
- Click the handle at the bottom of the interface to select items to be included in the profile:




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




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




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

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

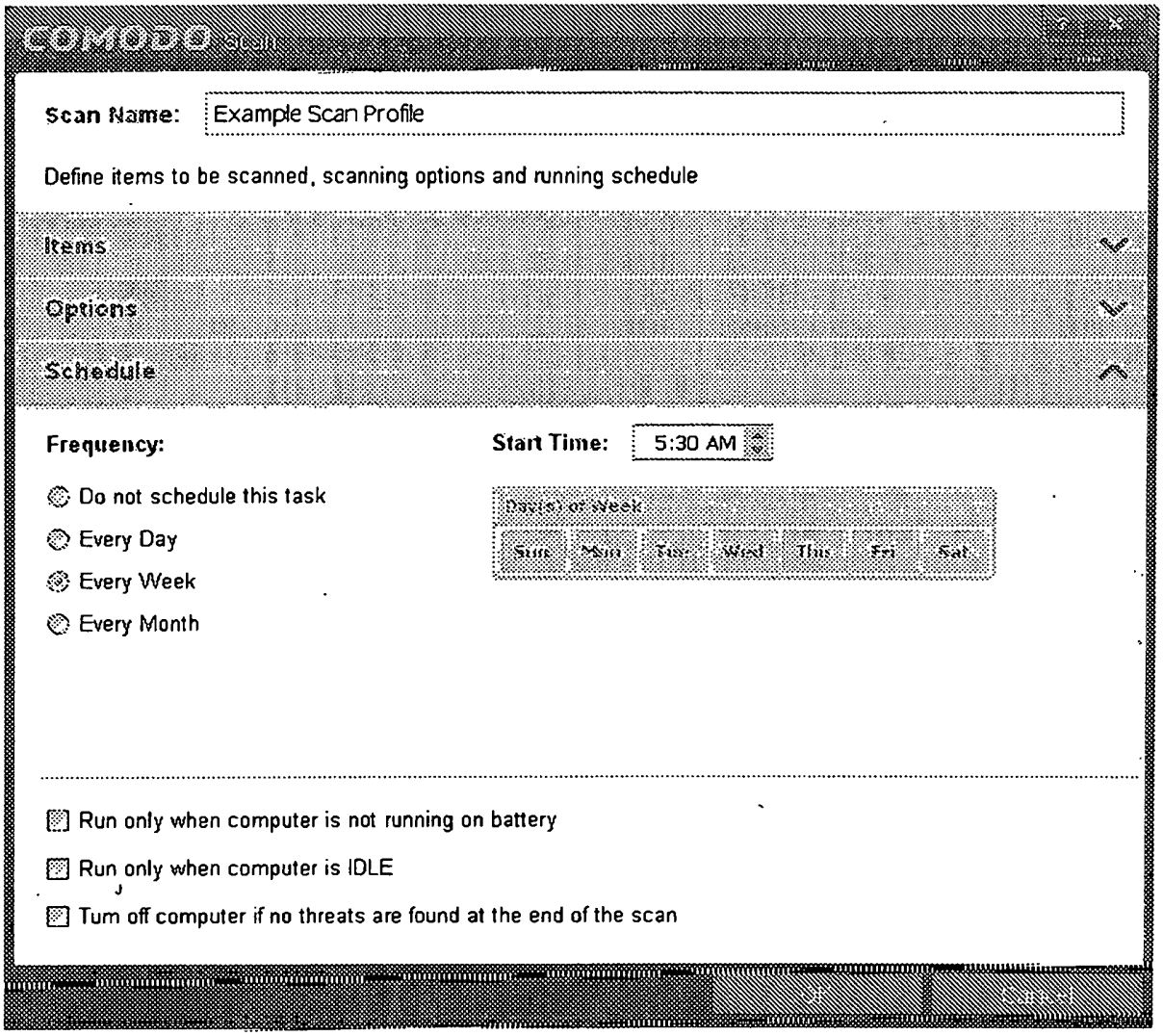
Background Info: Comodo Internet Security employs various heuristic techniques to identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code patterns similar to those in known viruses. If it is found to do so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

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

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

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

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

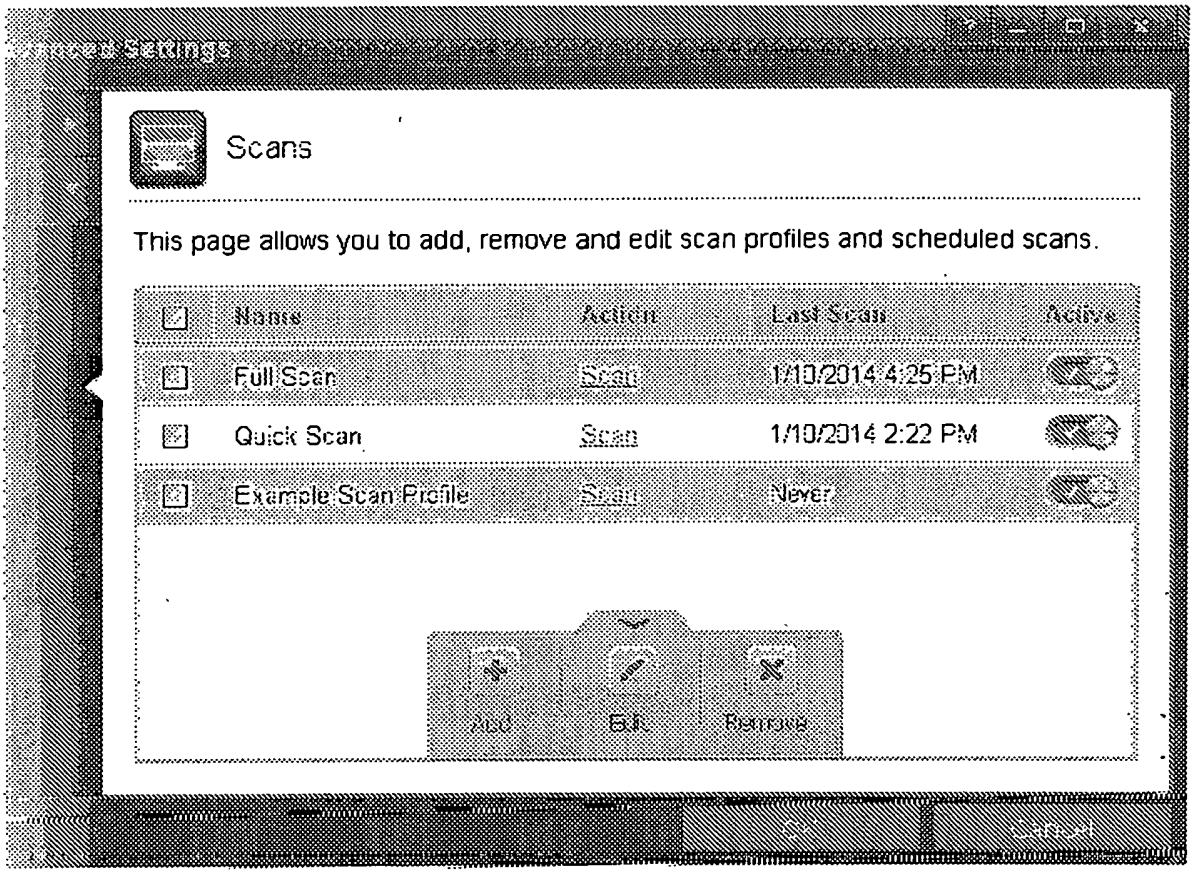



- **Do not schedule this task** - The scan profile will be created but will not be run automatically. The profile will be available for manual on-demand scanning
- **Every Day** - The Antivurus starts scanning the areas defined in the scan profile every day at the time specified in the Start Time field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

- Click OK to save the profile.

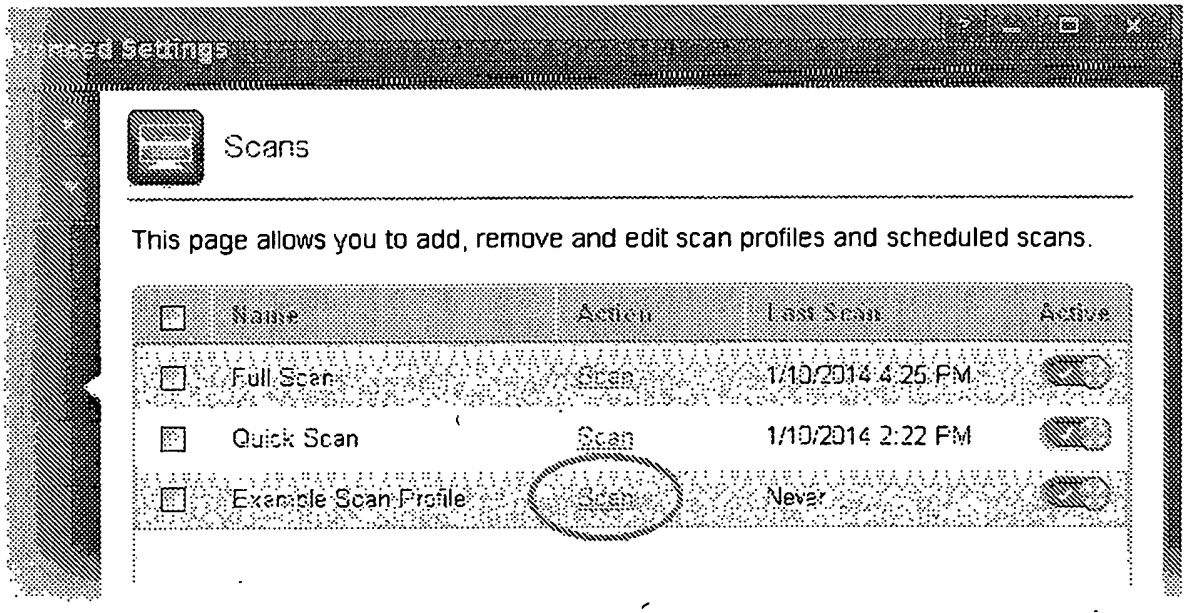
Note: The schedule scan will run only if it is enabled. Click the button under the Active column beside the respective profile row to toggle between on and off status.

The profile will be available for deployment in future.

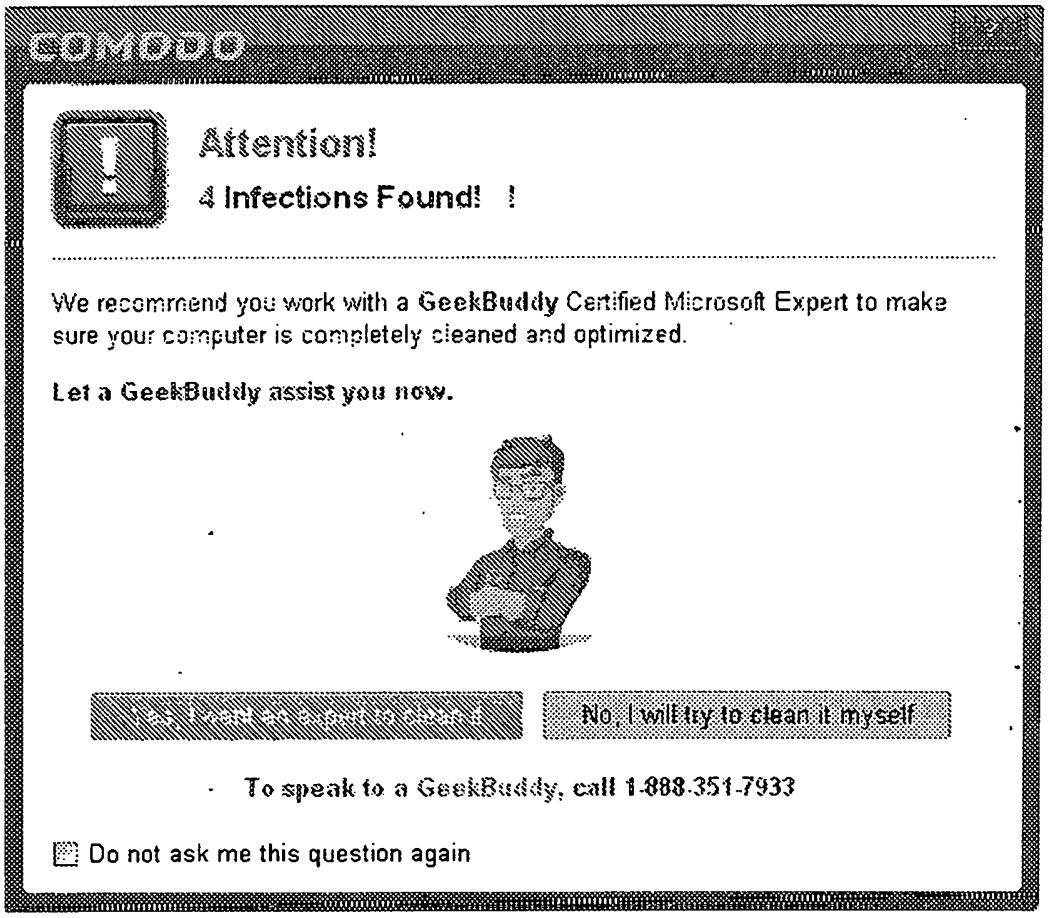



**To run a custom scan**

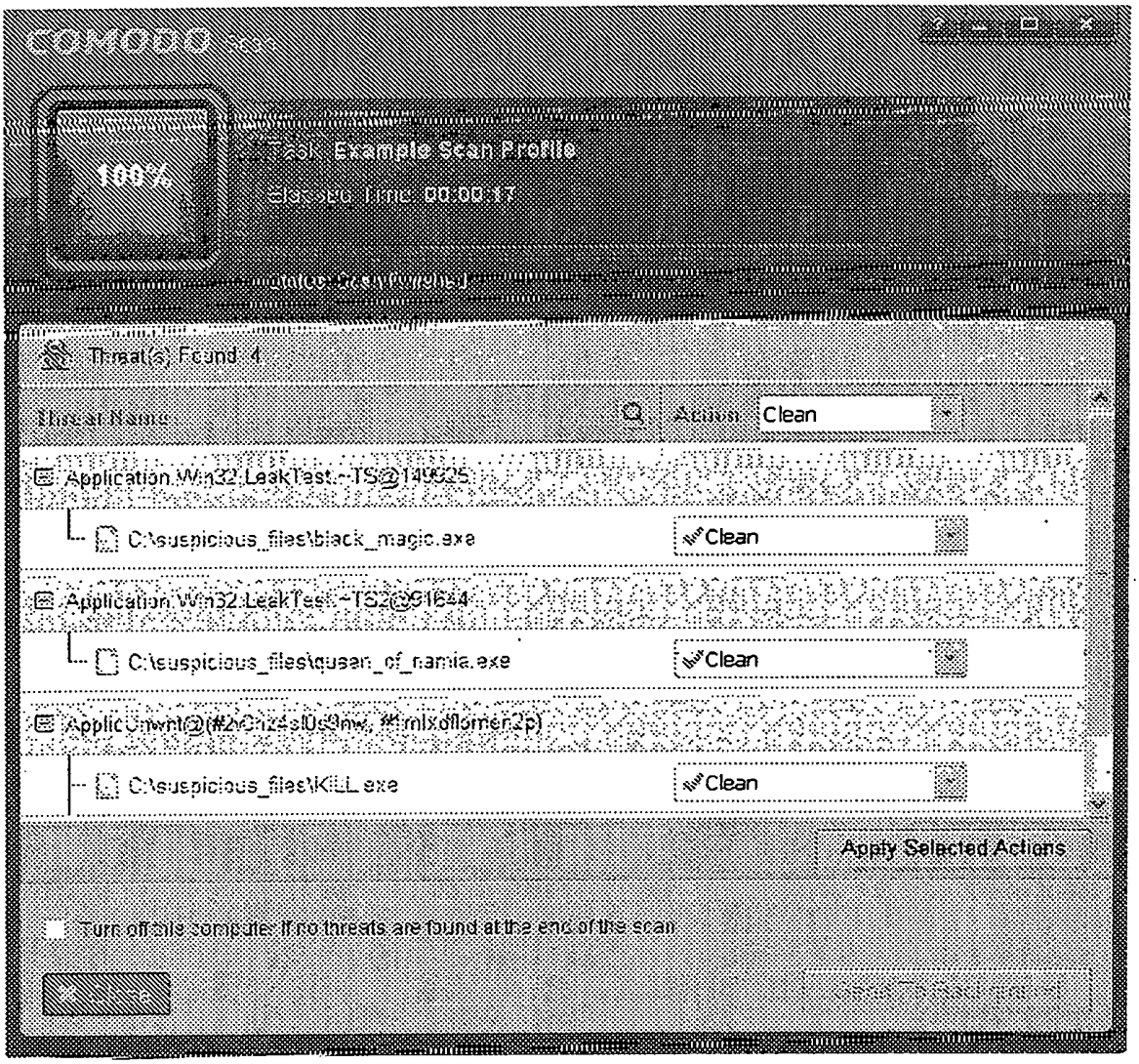
- Click 'Scan' from the 'General Tasks' interface and Click 'Custom Scan' from the 'Scan' interface
- Click 'More Scan Options' from the 'Custom Scan' pane
- The 'Advanced Settings' interface will be displayed with 'Scans' panel opened.
- Click 'Scan' beside the required scan profile.



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




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



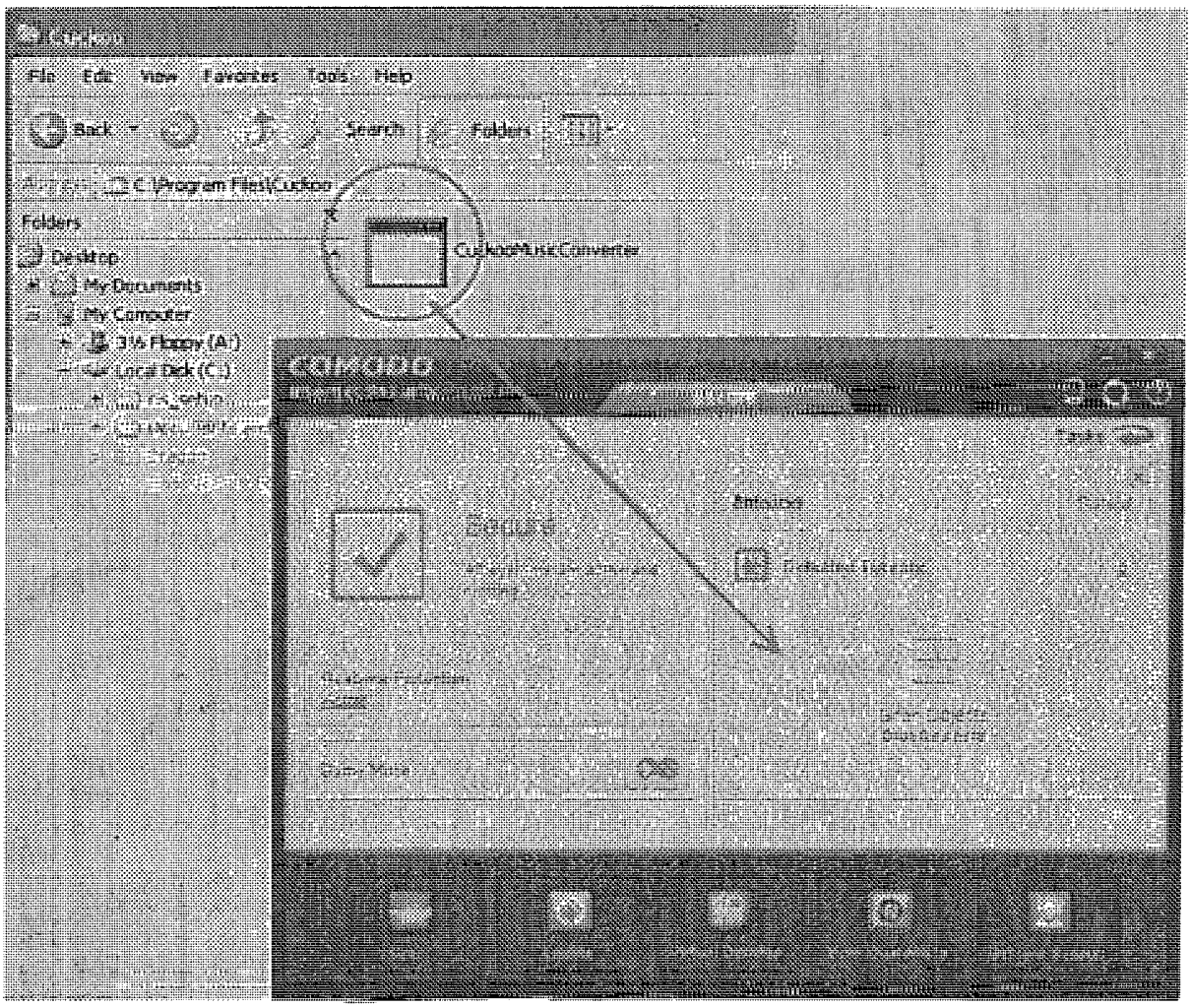

- The scan results window displays the number of objects scanned and the number of threats (Viruses, Rootkits, Malware and so on). You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

## 2.2. Instantly Scan Files and Folders

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

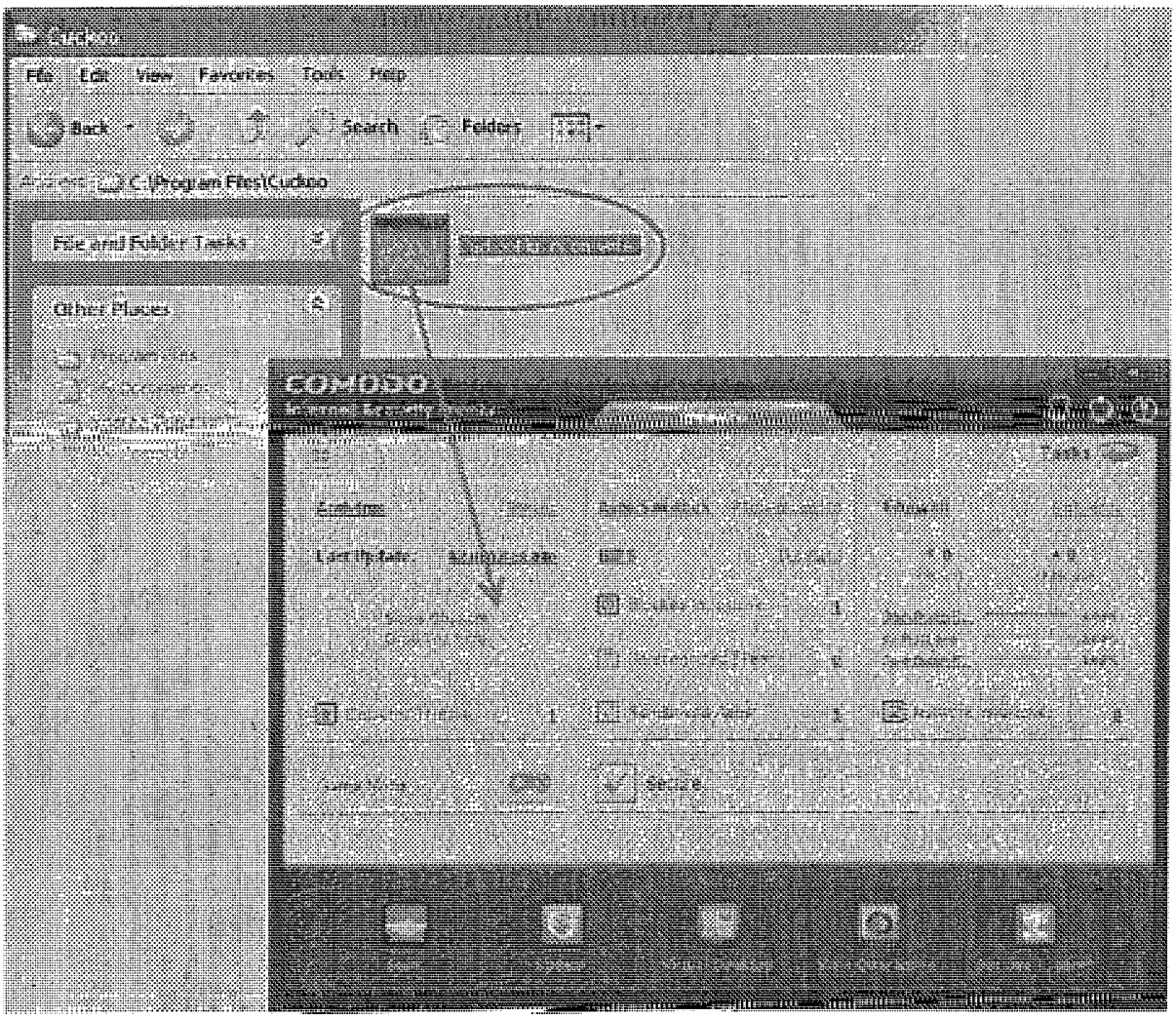
**To instantly scan an item**

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



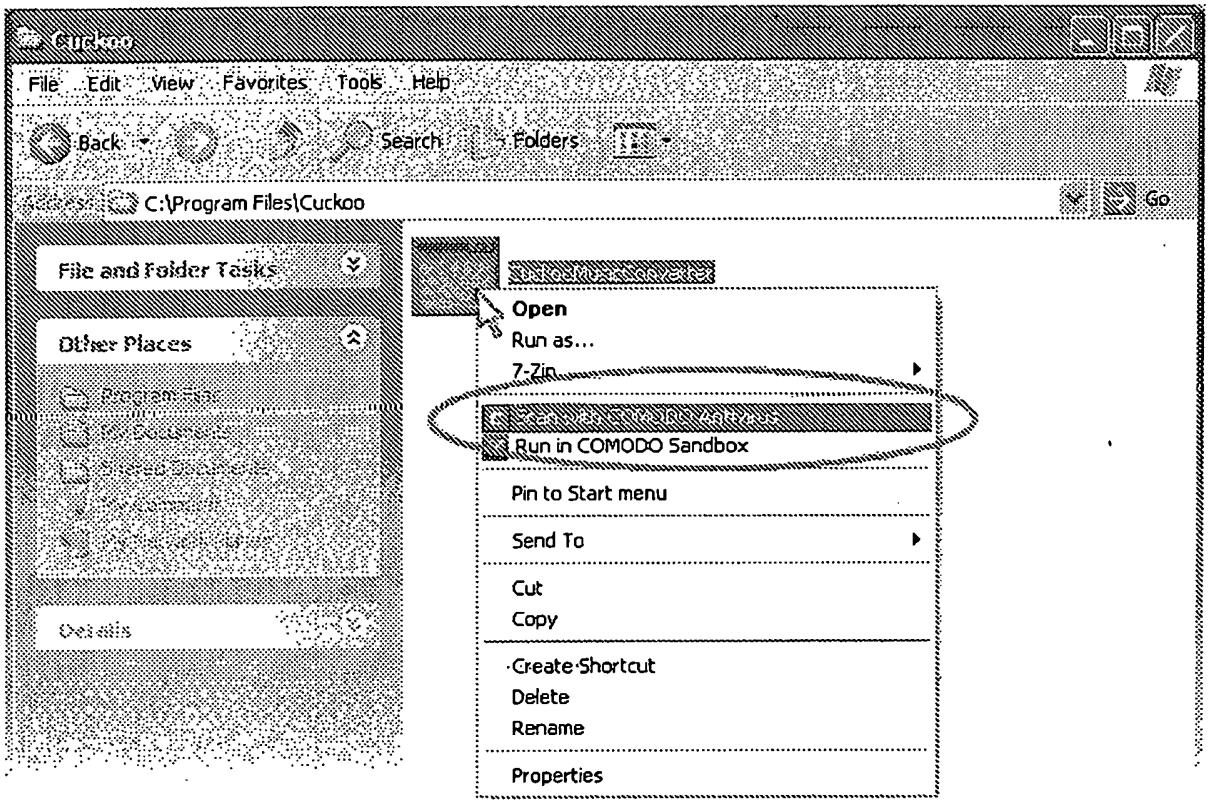

OR

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

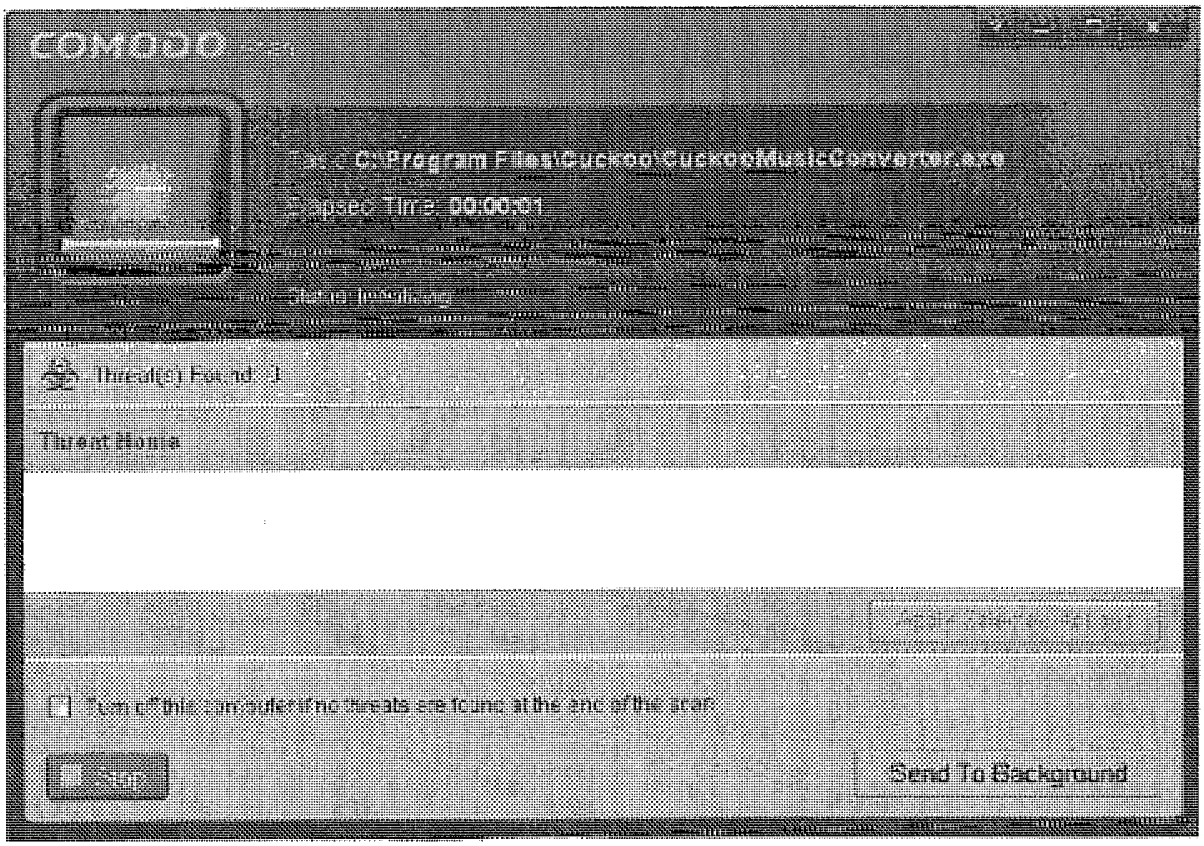



OR

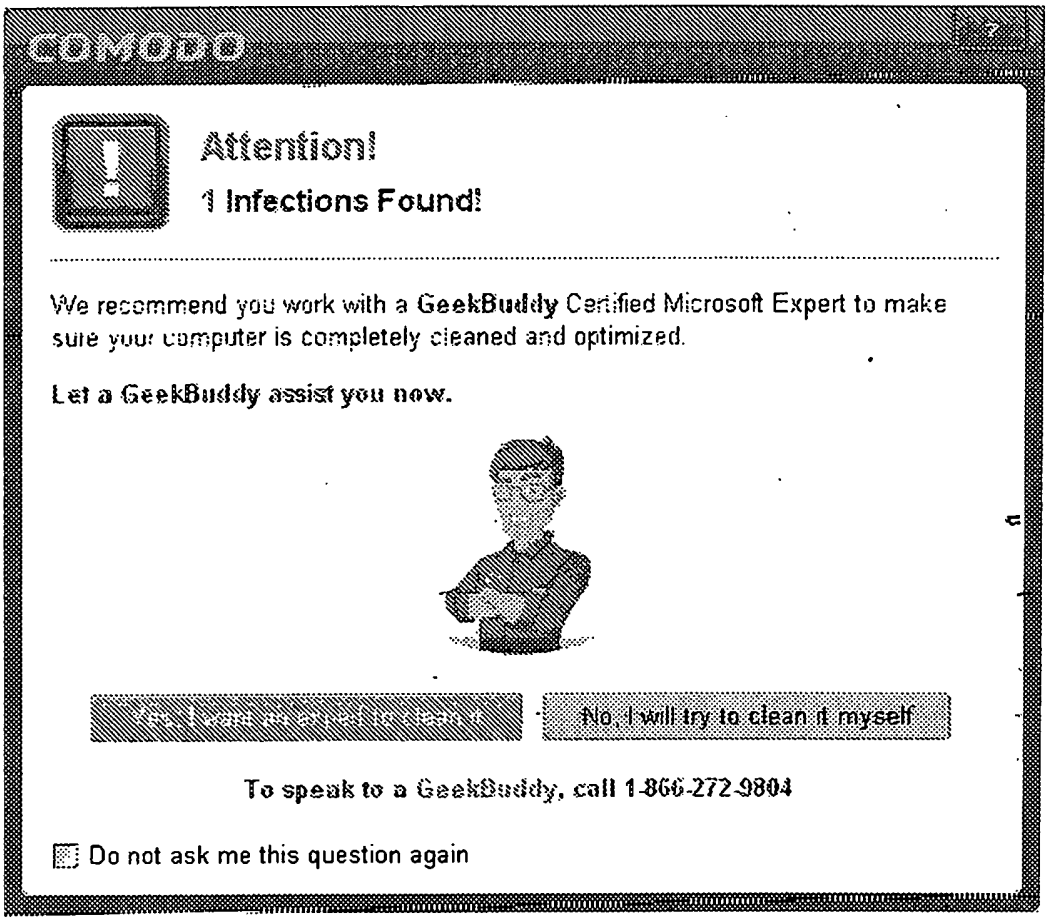
- Right click on the item and select Scan with 'Comodo Antivirus' from the context sensitive menu



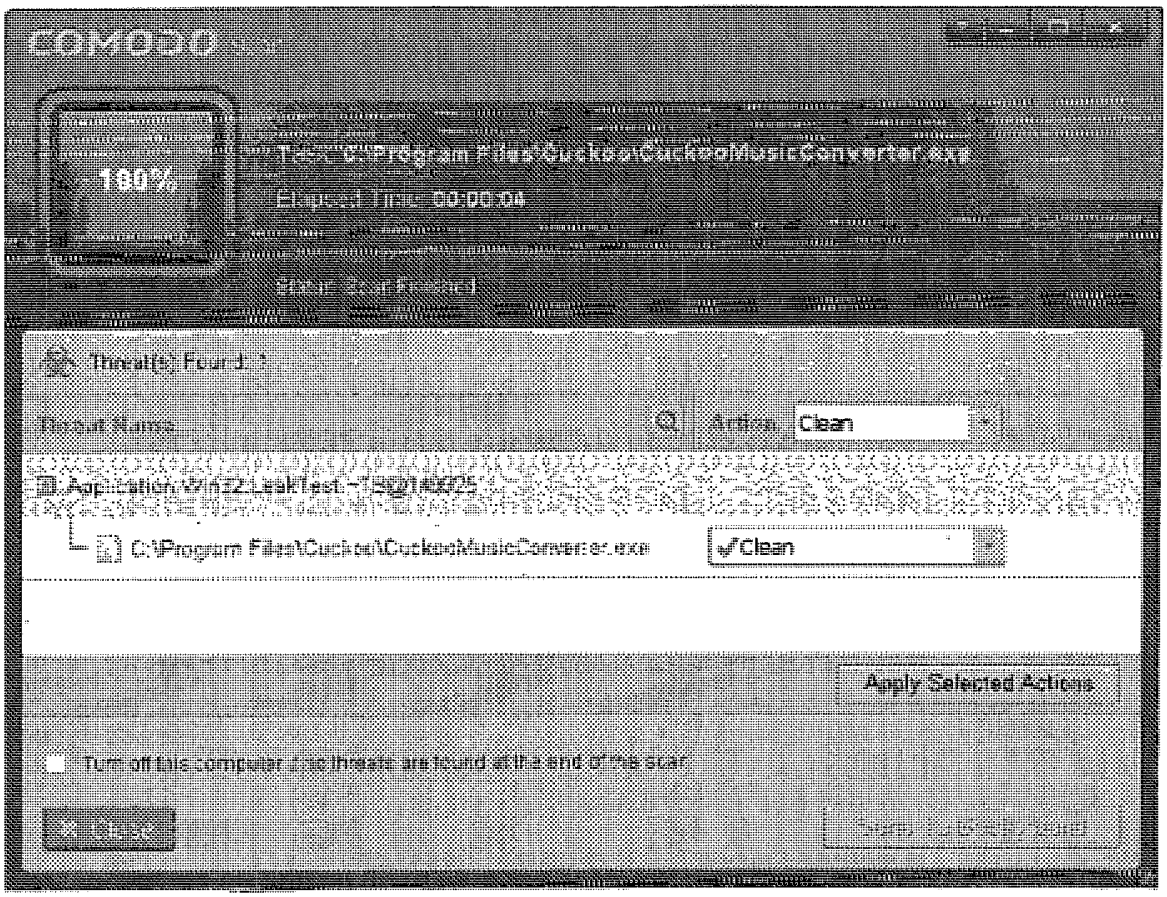

The item will be scanned immediately.



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



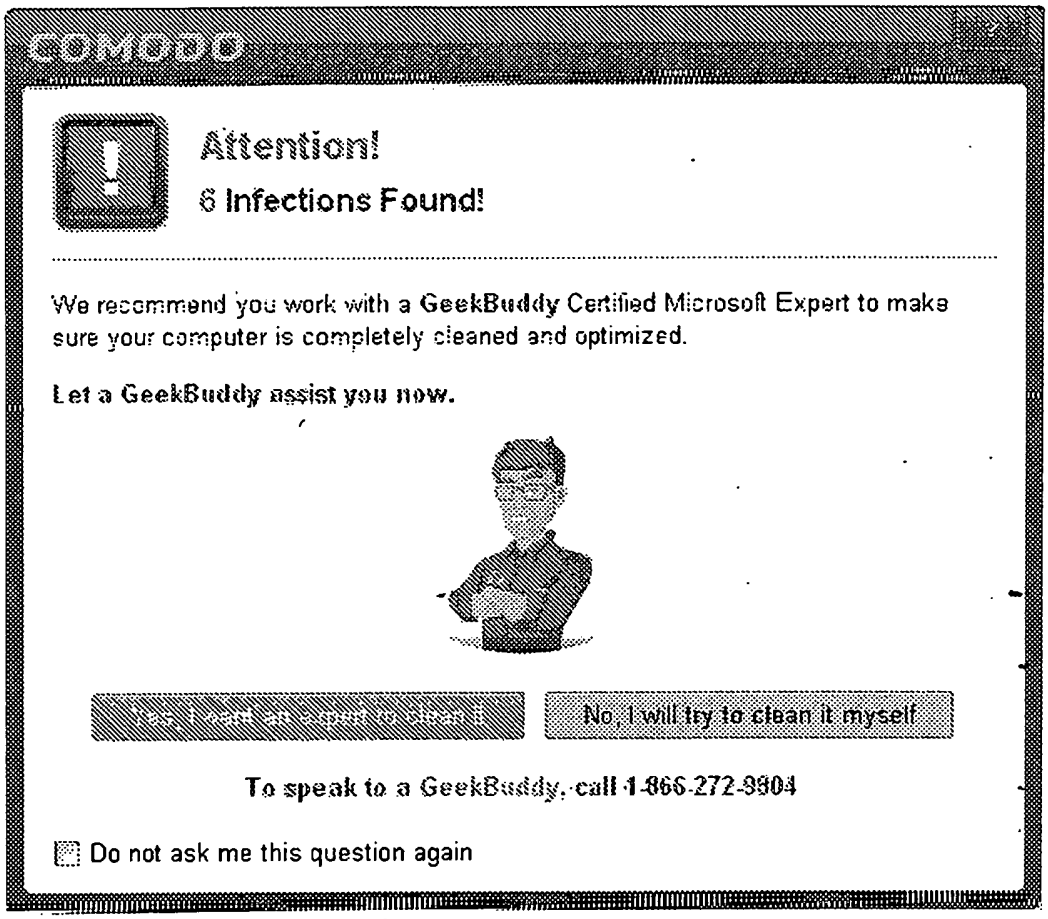

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up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



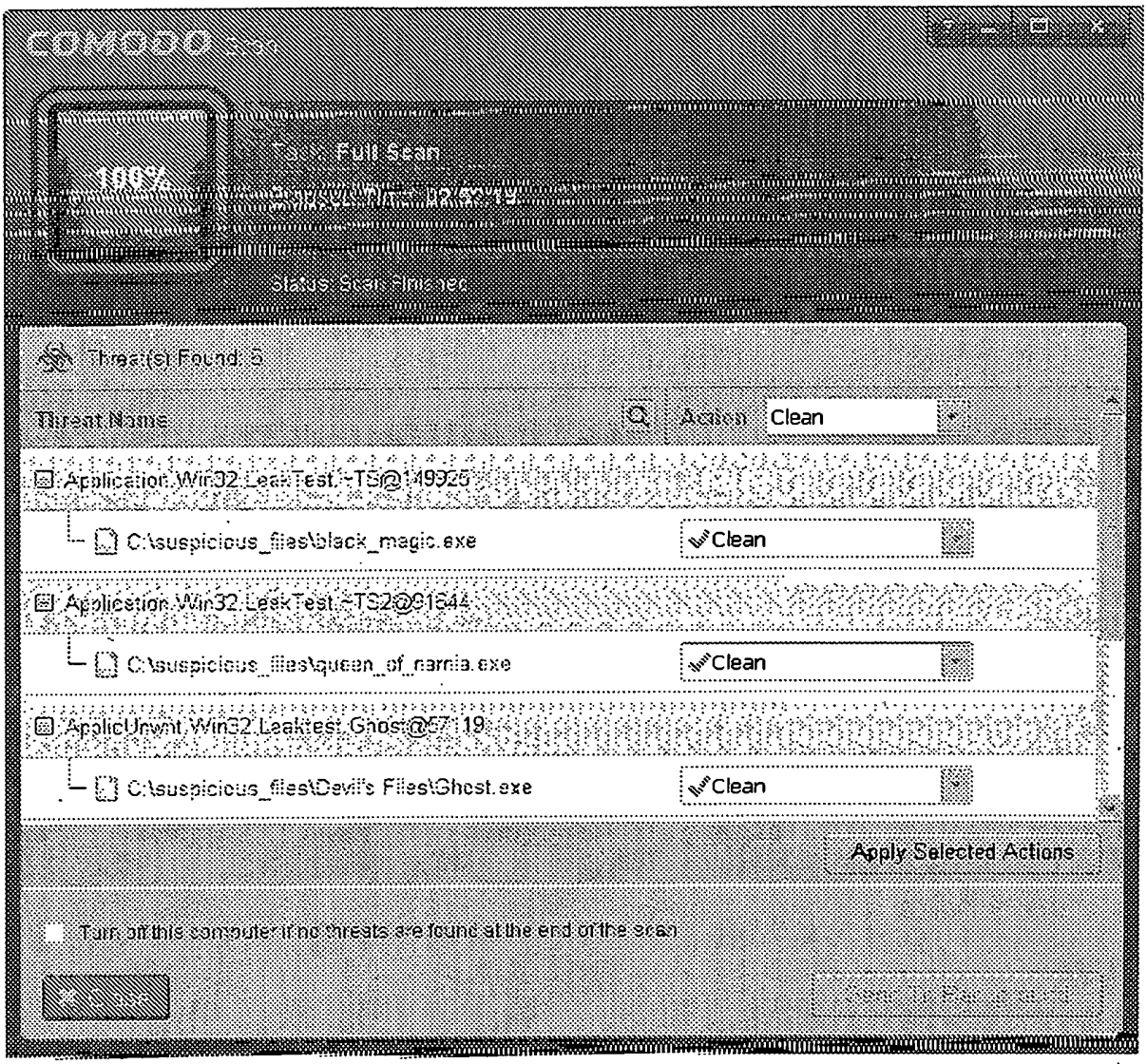

You can choose to clean, move to quarantine or ignore the threat based in your assessment. Refer to Processing the infected files for more details.

## 2.3. Processing Infected Files

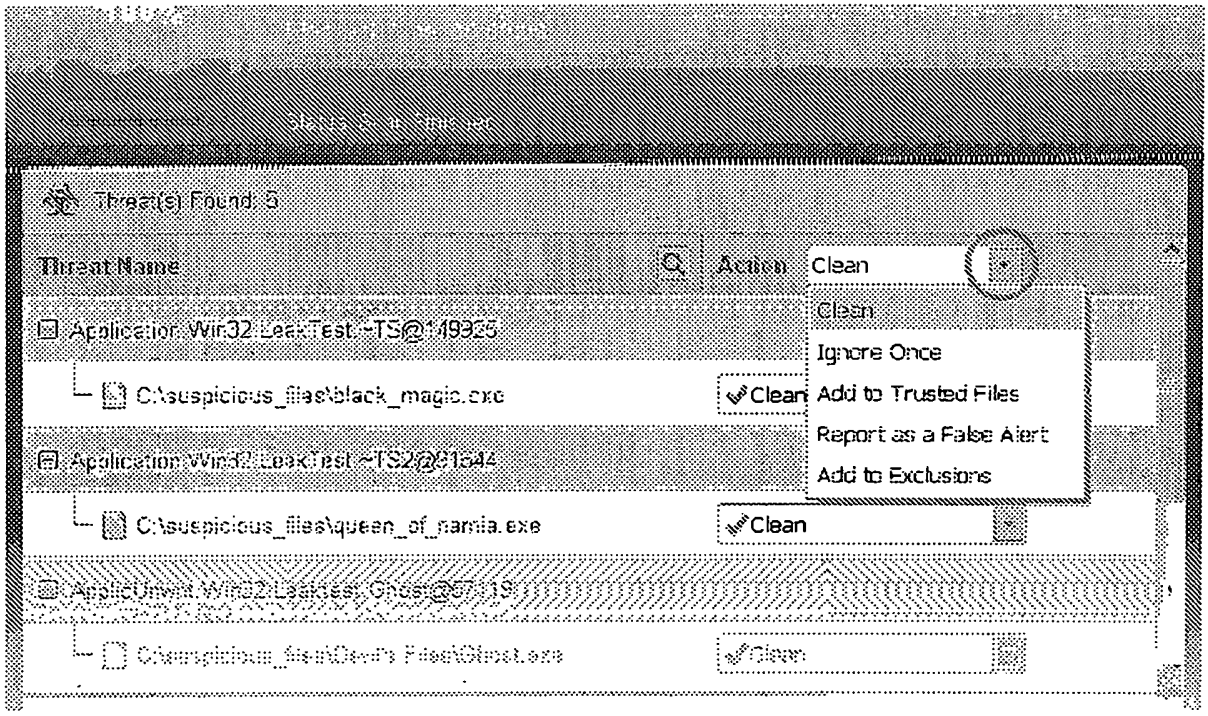
On completion of any on-demand or scheduled scanning, if any threats are found, an alert screen will be displayed. The alert will display the number of threats/infections discovered by the scanning and provide you the options for cleaning.



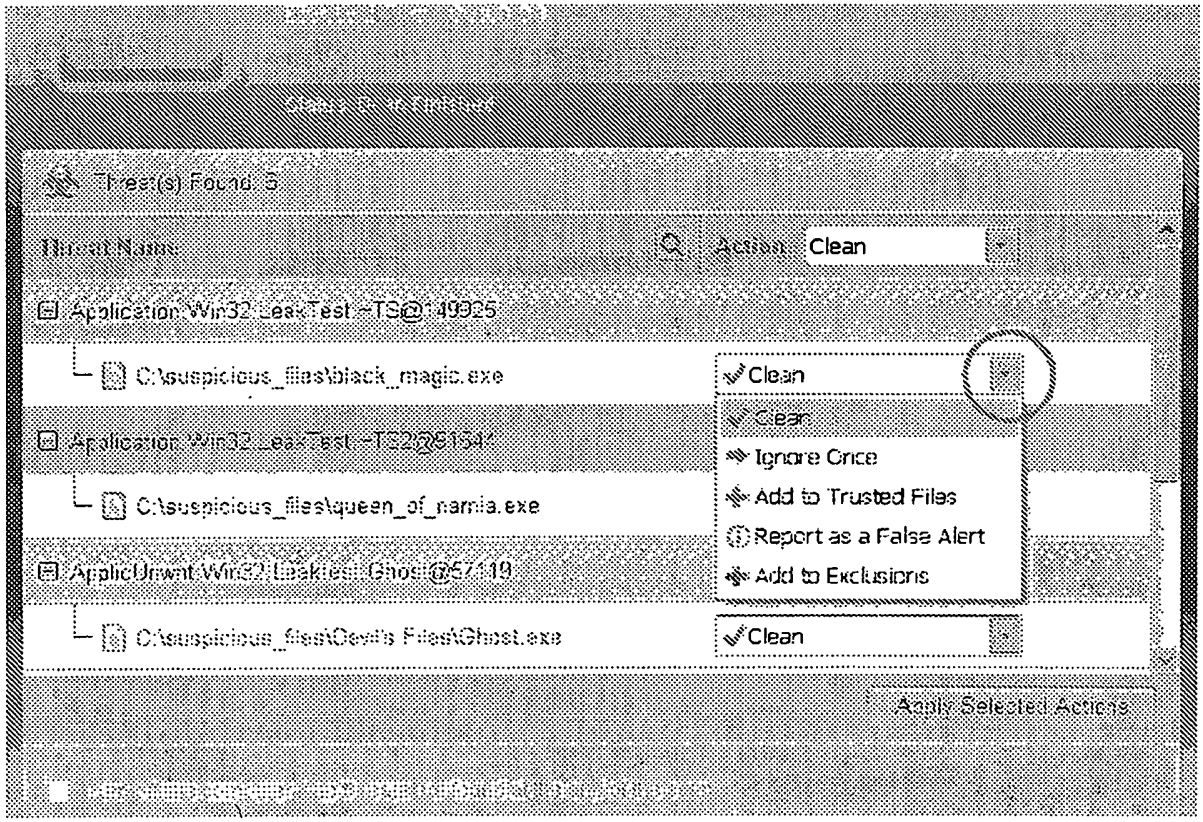

- If you wish to have a skilled professional from Comodo to access your system and perform an efficient disinfection, click 'Yes, I want an expert to clean it'. If you are a first-time user, you will be taken to Comodo GeekBuddy webpage to sign-up for a GeekBuddy subscription. If you have already signed-up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




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




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



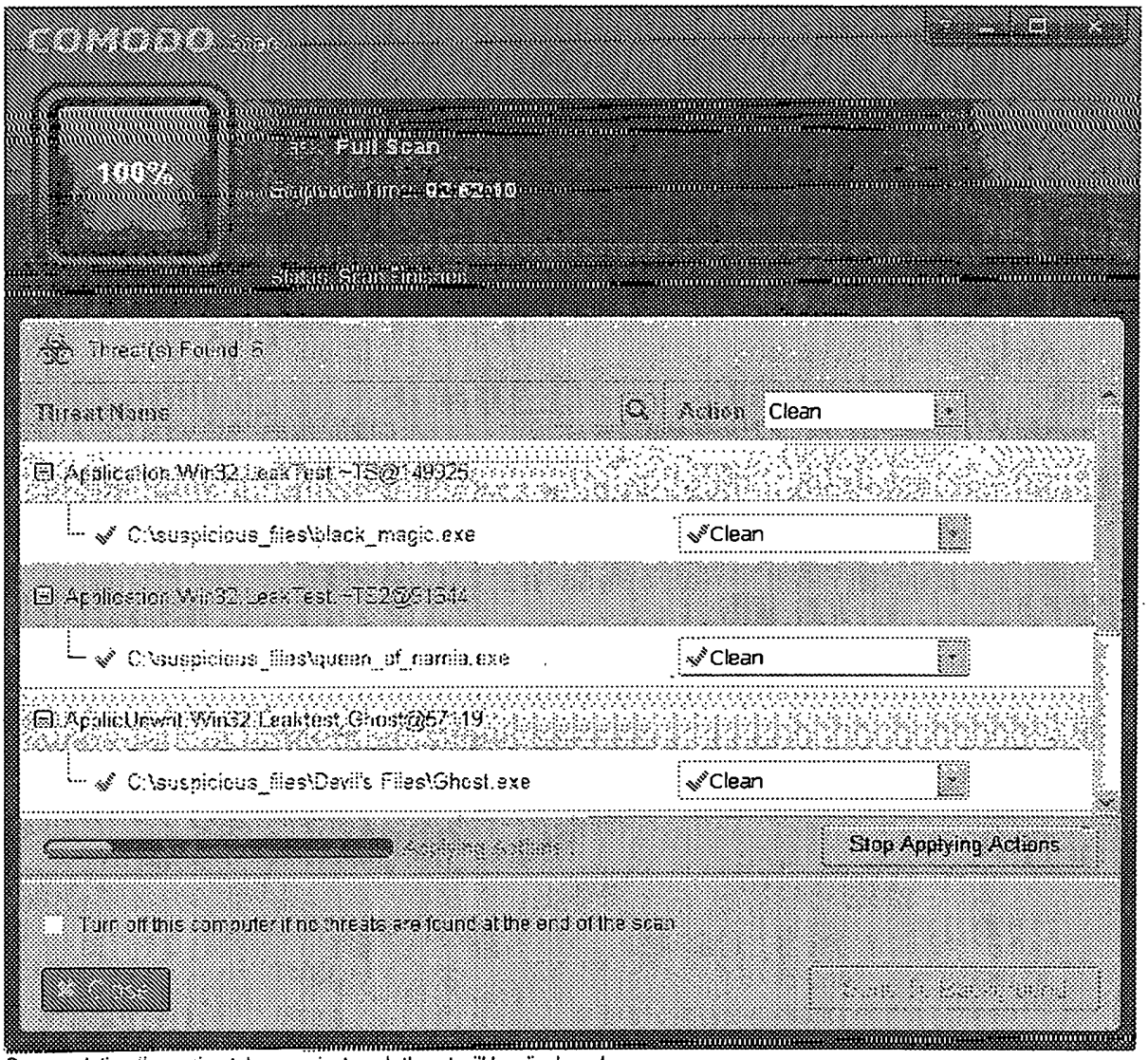

The choices for the actions available are:

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

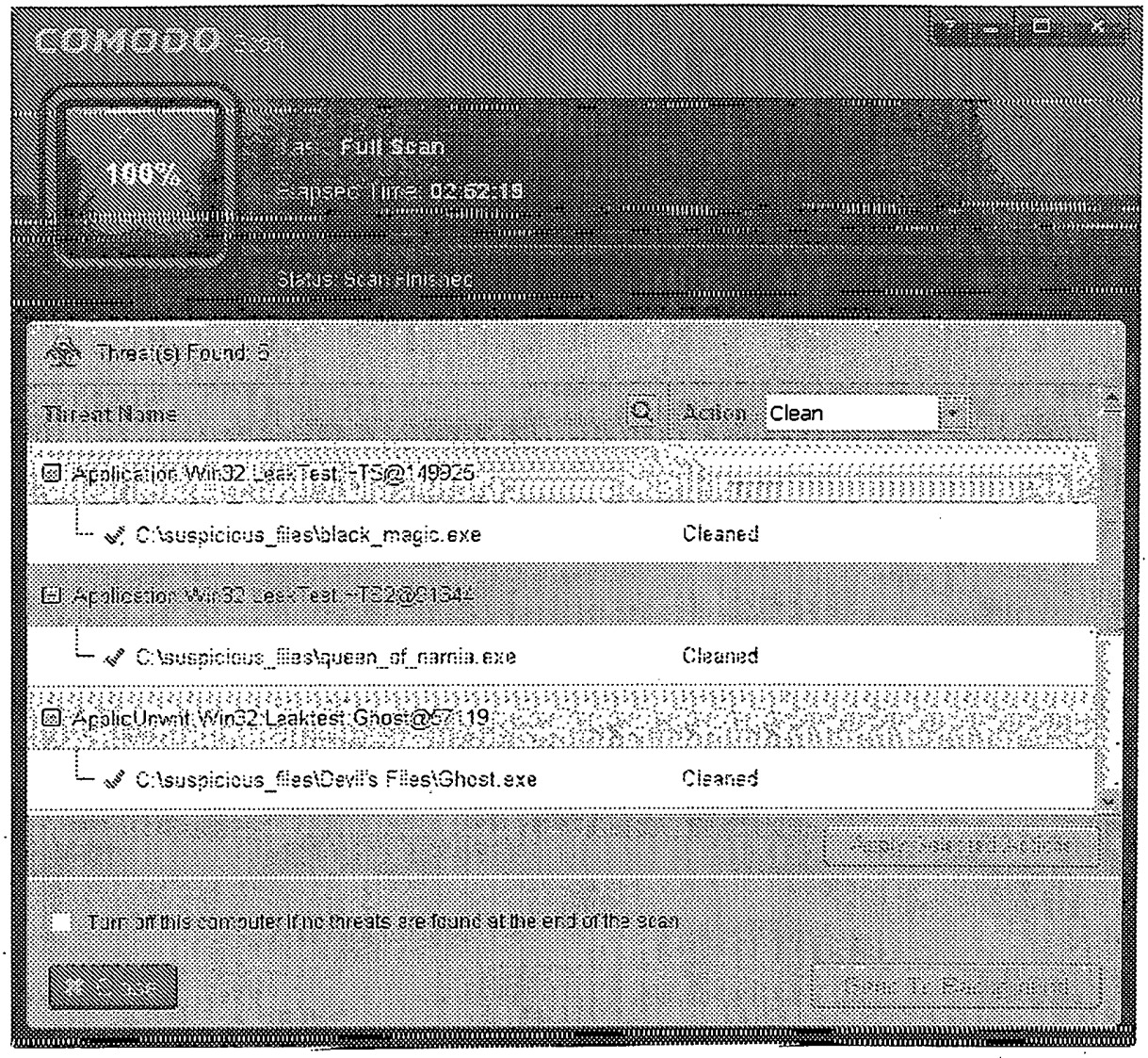
move the infections to Quarantine for later analysis and restoring/removal of the files. For more details on quarantine feature, refer to Manage Quarantined Items.

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

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




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




- Click 'Close' to close the results window.

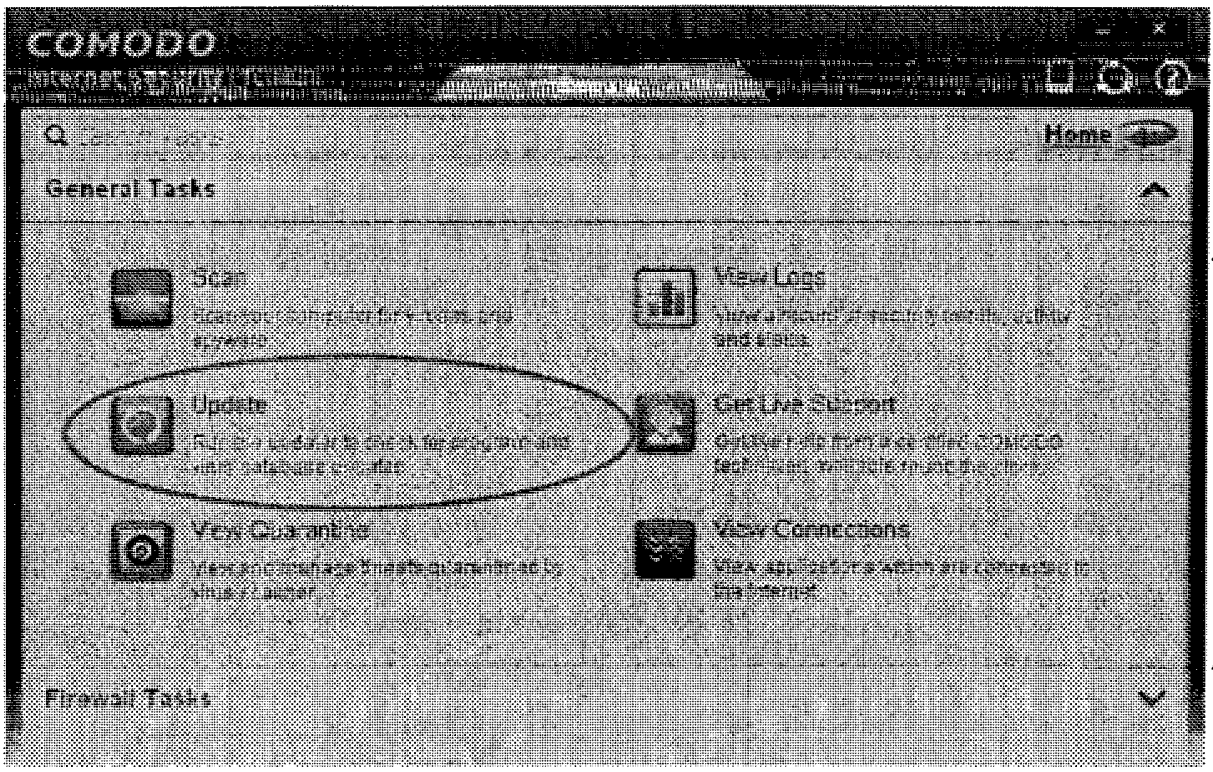
## 2.4. Manage Virus Database and Program Updates

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

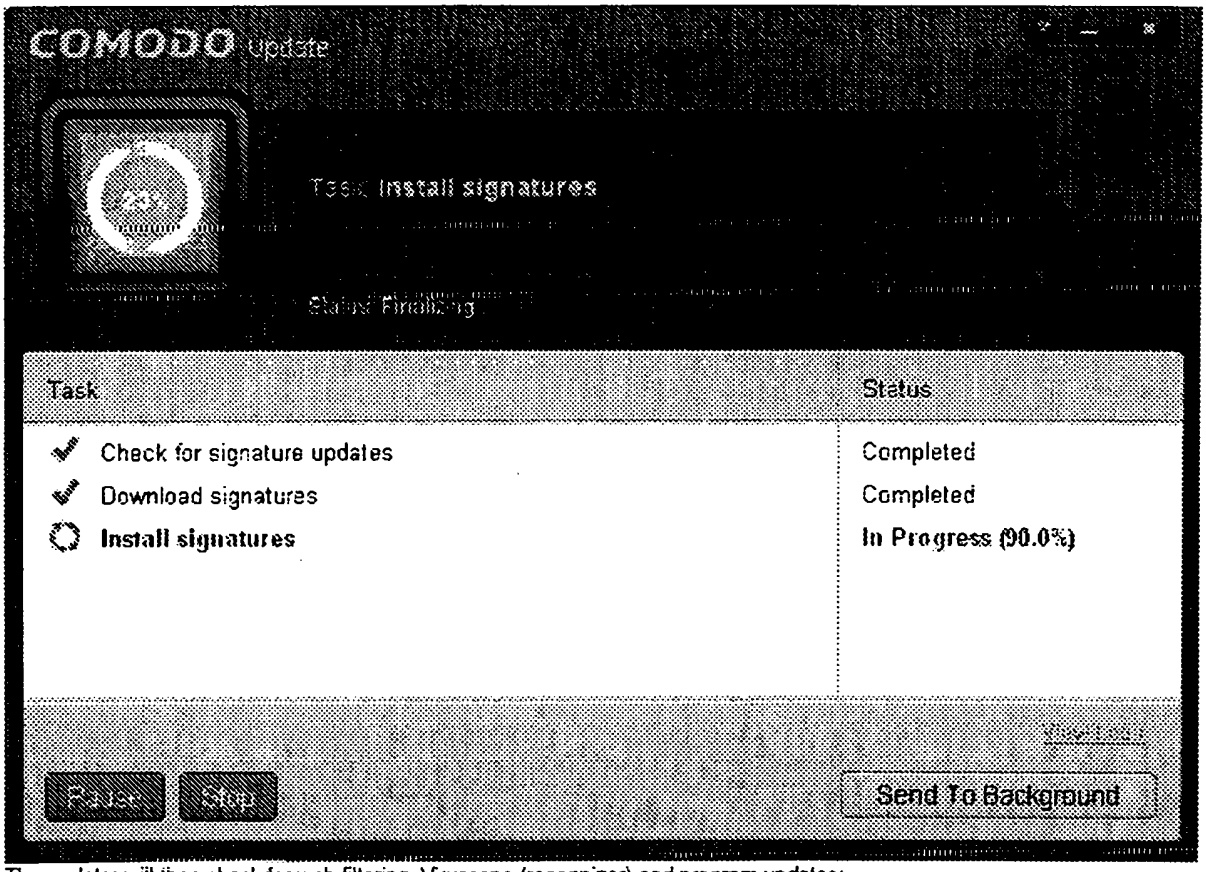
| Note: You must be connected to Internet to download updates. |
|---|

**To manually check for the latest virus and program updates**

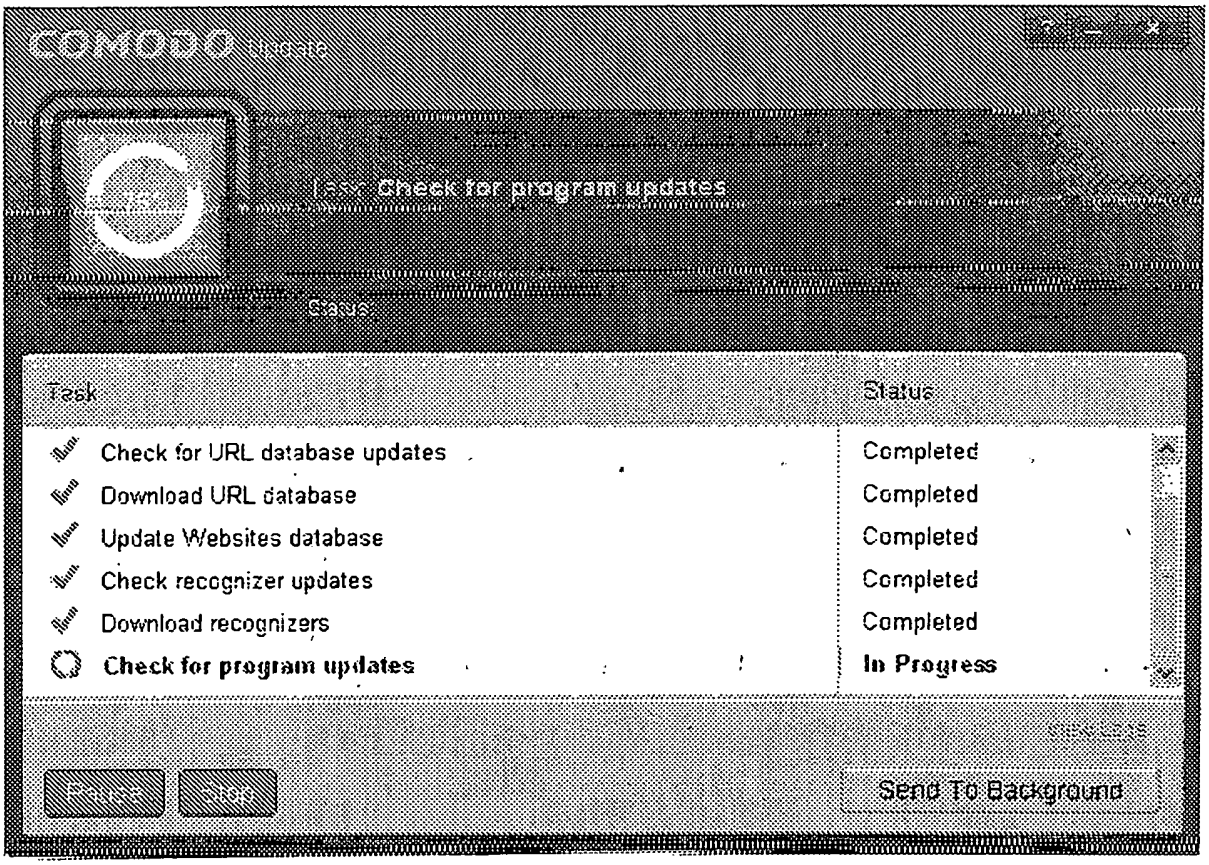
1. Switch to the 'Tasks' screen and click 'General Tasks' to open the 'General Tasks' interface.
2. Click 'Update'. The application will start checking for program and database updates




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




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



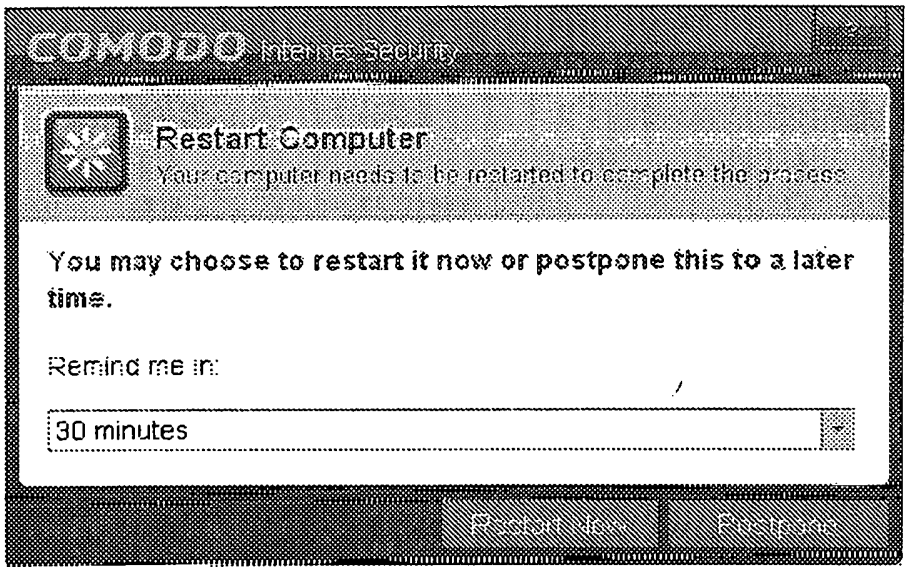

When all updates have been download you will be asked to confirm installation at the following dialog:




- Click 'Yes' to begin installation.

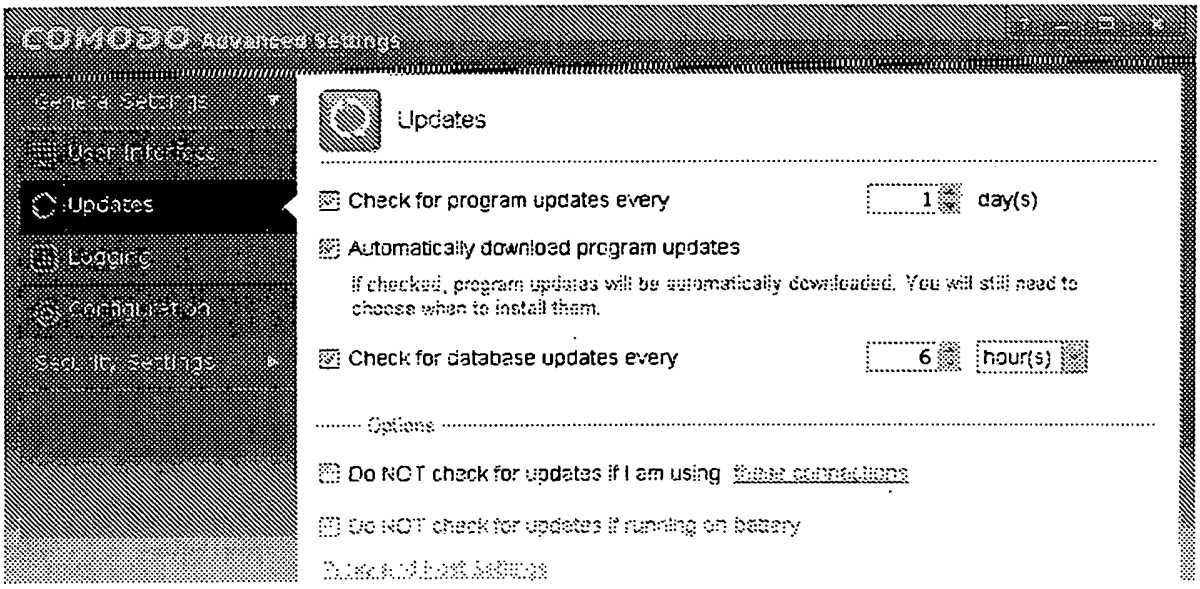
During the update process, new software components or features sometimes become available for installation. As these may alter the behavior of CIS in some manner, please carefully review these types of update before agreeing to their installation.

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




**Automatic Updates**

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

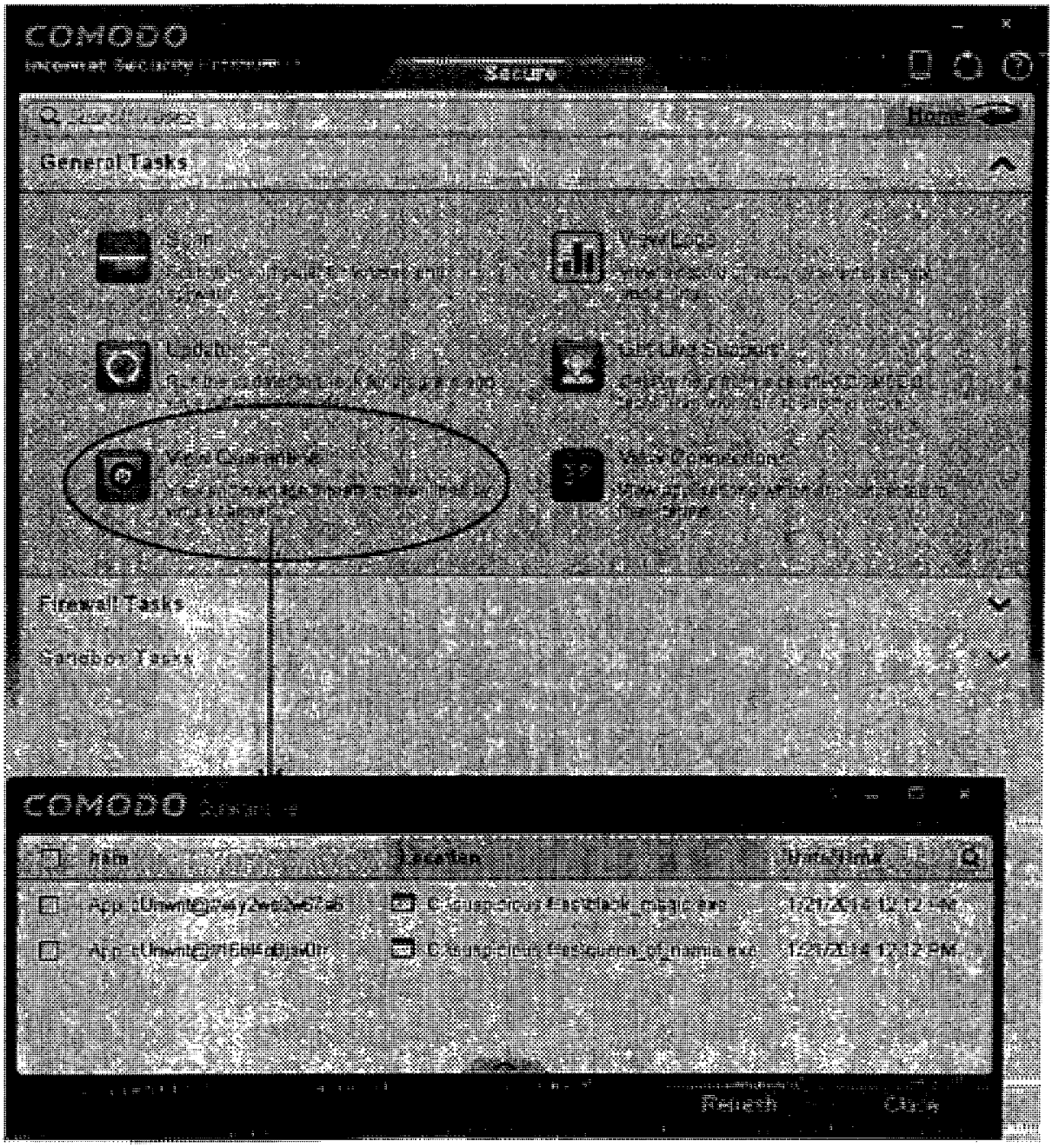



You can also configure Comodo Antivirus to download updates automatically before any on-demand scan. Refer to Scan Profiles for more details.

# 2.5. Manage Quarantined Items

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

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



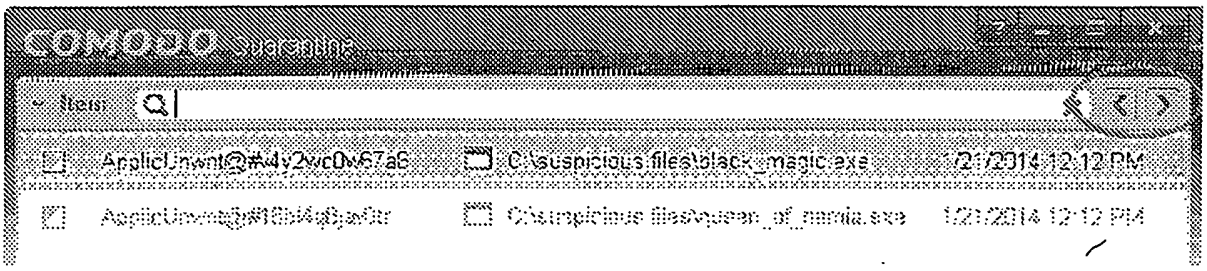

The 'Quarantine' interface displays a list of items moved to Quarantine from the results of real-time scanning, on-demand scanning and manually.

**Column Descriptions**

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

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

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




The Quarantined Items interface also allows you to:

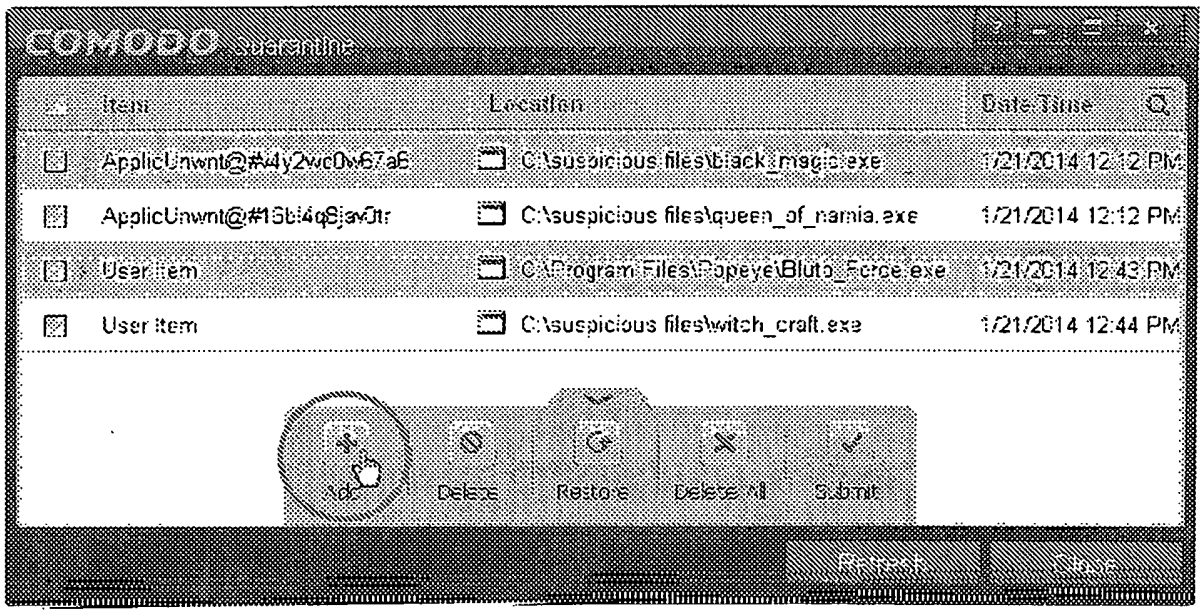
- Manually add applications, executables or other files, that you do not trust, as a Quarantined Item
- Delete a selected quarantined item from the system
- Restore a quarantined item to its original location
- Delete all quarantined items
- Submit selected quarantined items to Comodo for analysis

### Manually adding files as Quarantined Items

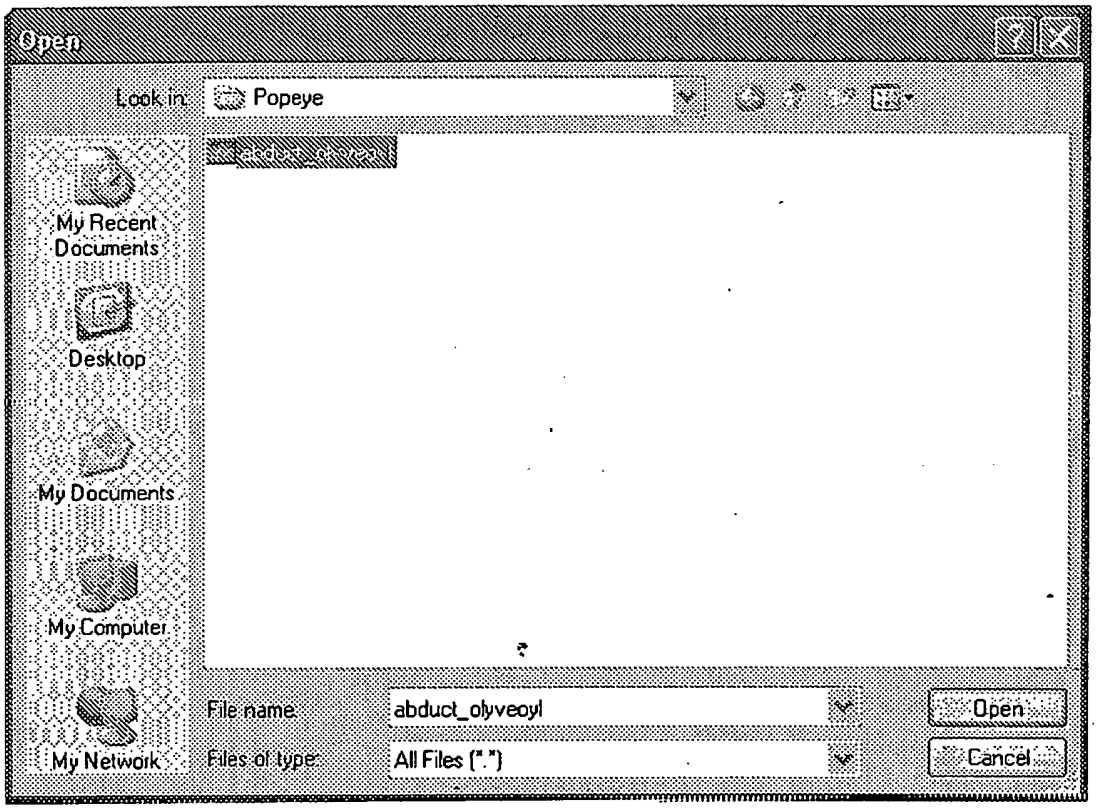
If you have a file, folder or drive that you suspect may contain a virus and not been detected by the scanner, then you have the option to isolate that item in quarantine.

**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.

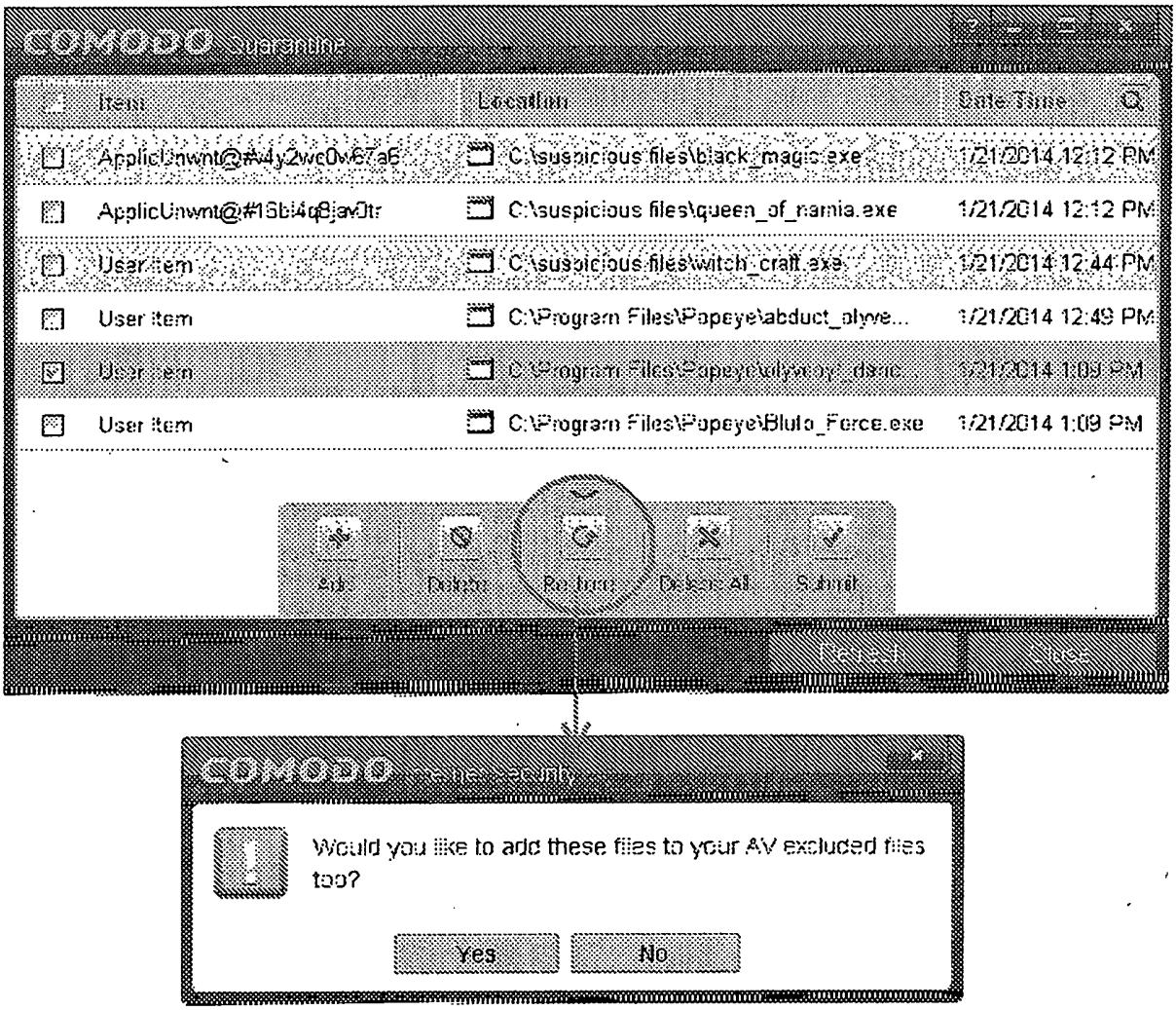
**To delete a quarantined item from the system**

- 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**

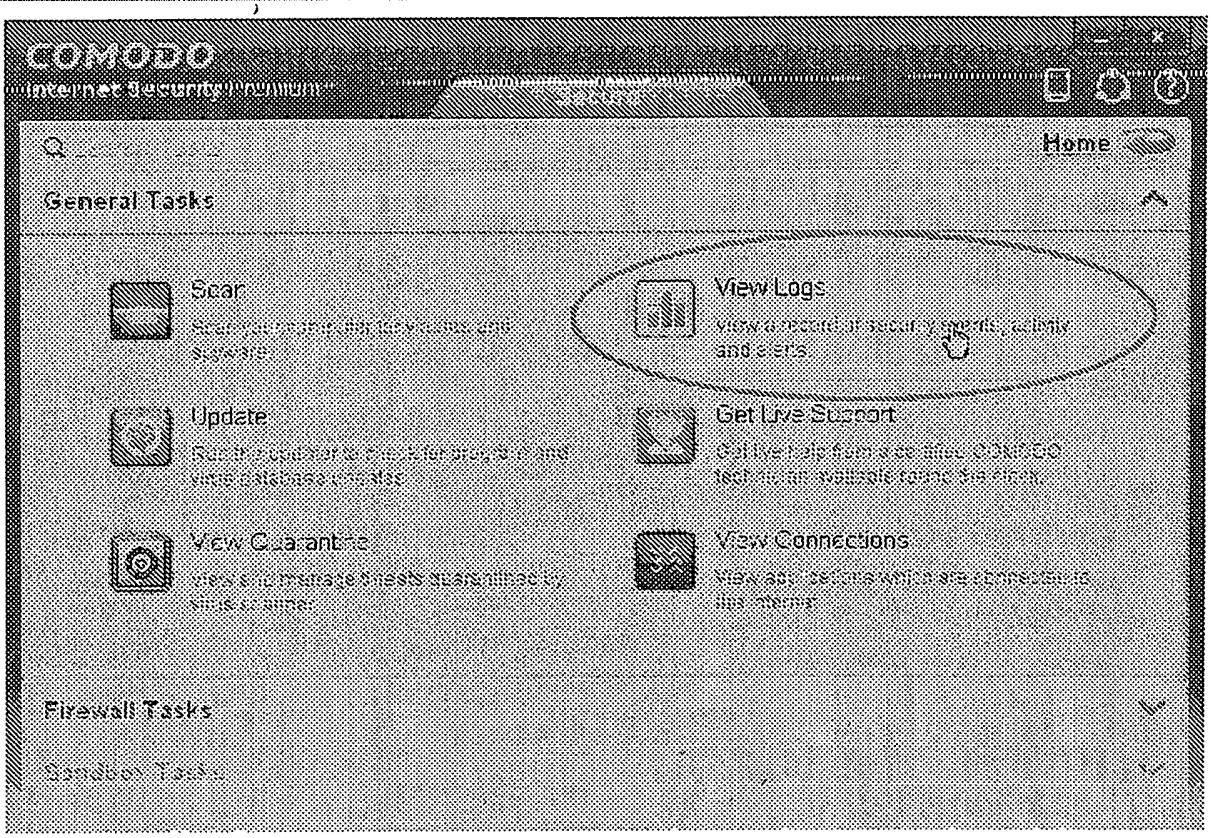
- Select the item(s) from the Quarantine interface
- Click the handle from the bottom of the interface and select 'Submit' option.

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).

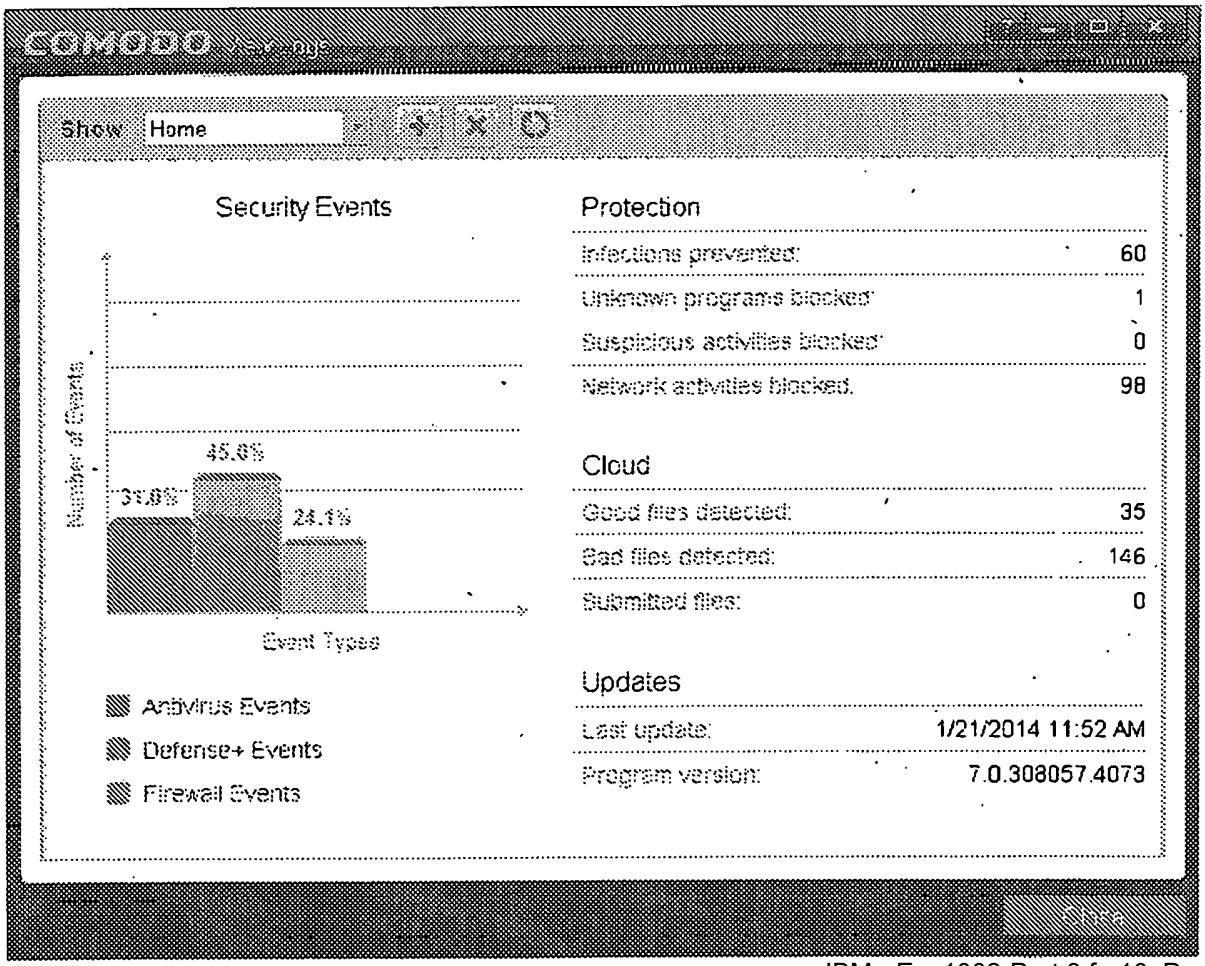
Note: Quarantined files are stored using a special format and do not constitute any danger to your computer.

# 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

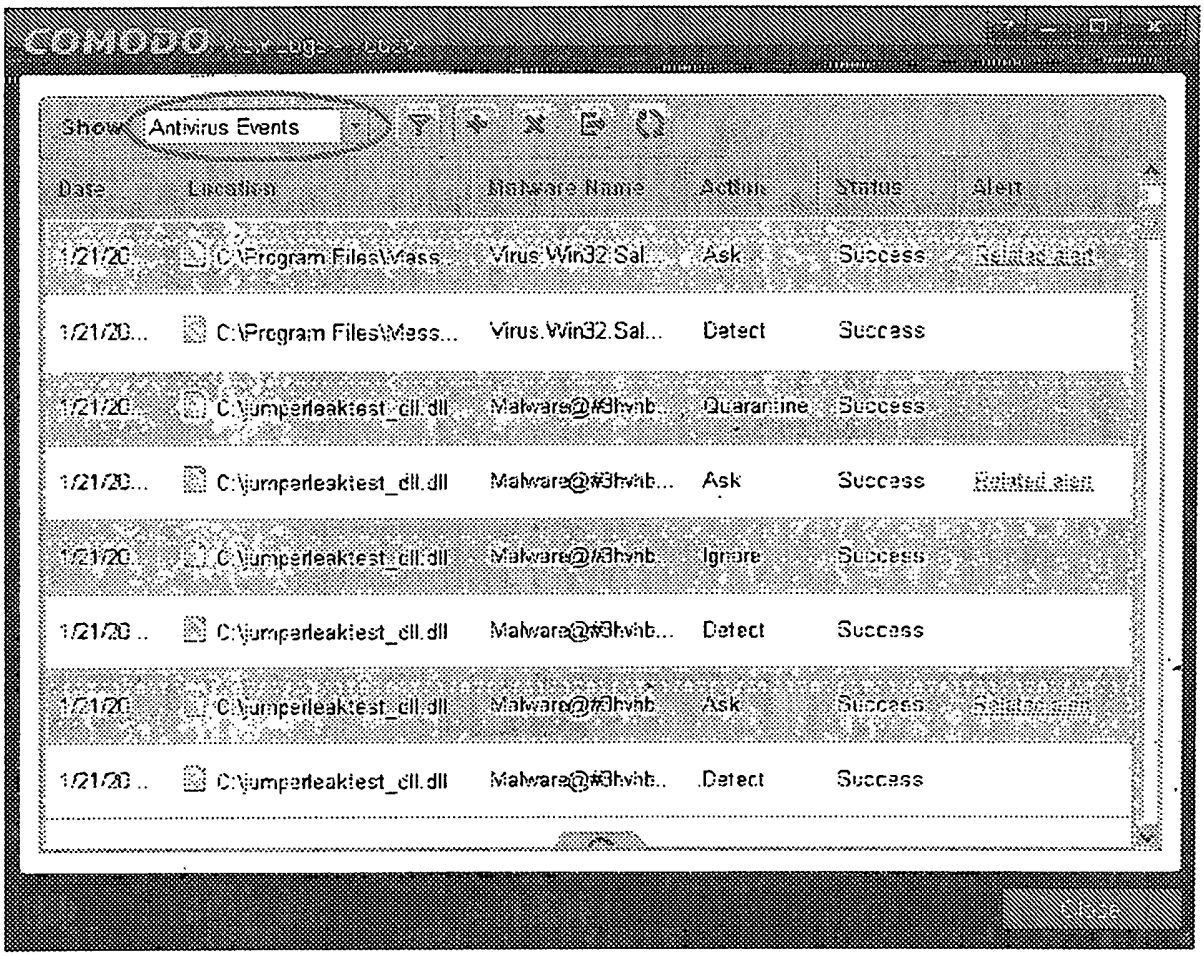
'Other Logs':

- 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.

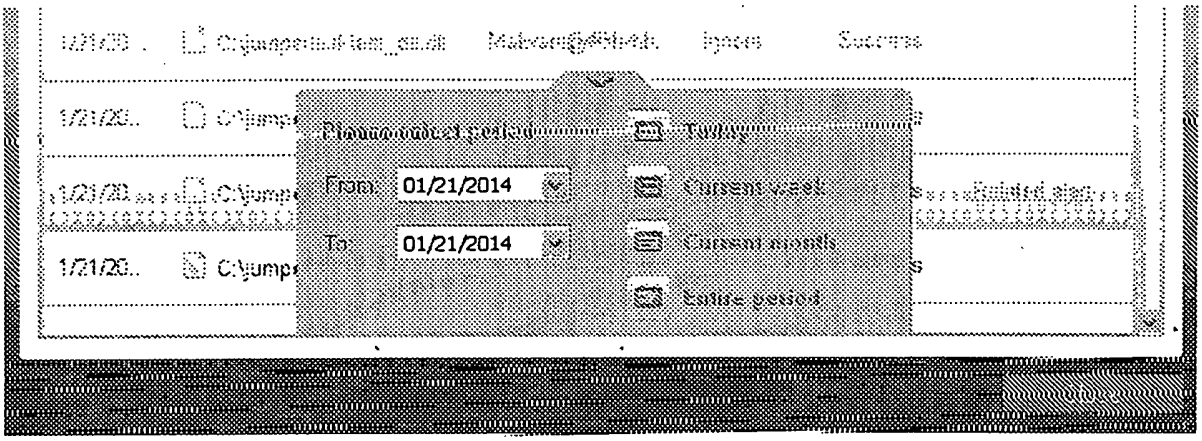
## 2.6.1.1. Filtering Antivirus Logs

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

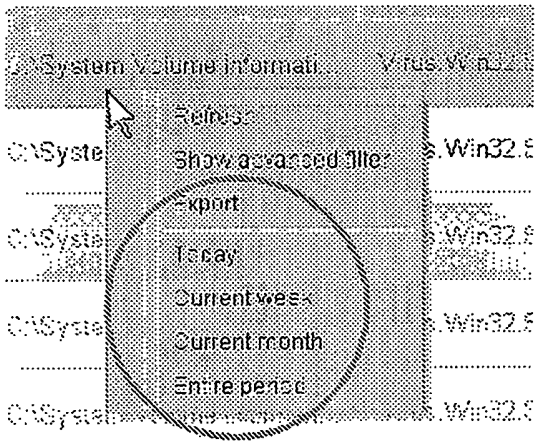
Preset Time Filters:

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:

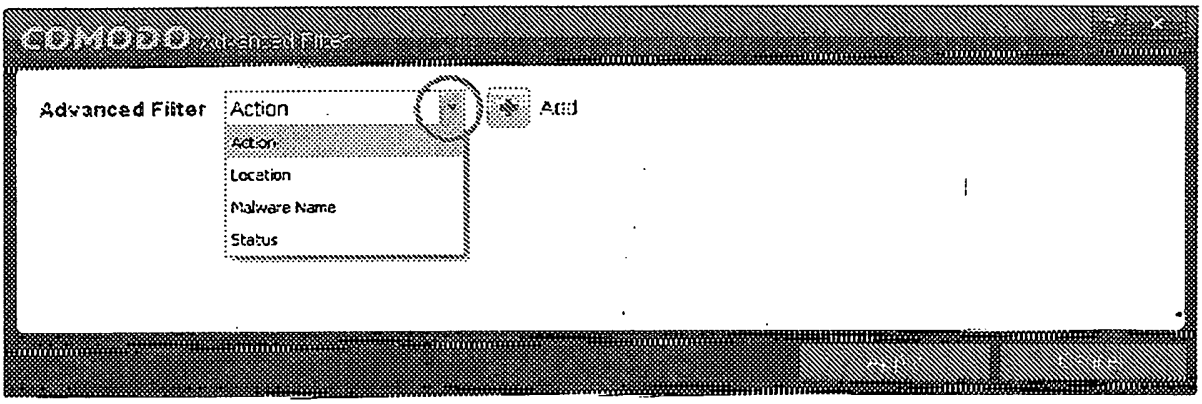
Having chosen a preset time filter, you can further refine the displayed events according to specific filters. Following are available filters for Antivirus logs and their meanings:

- **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**

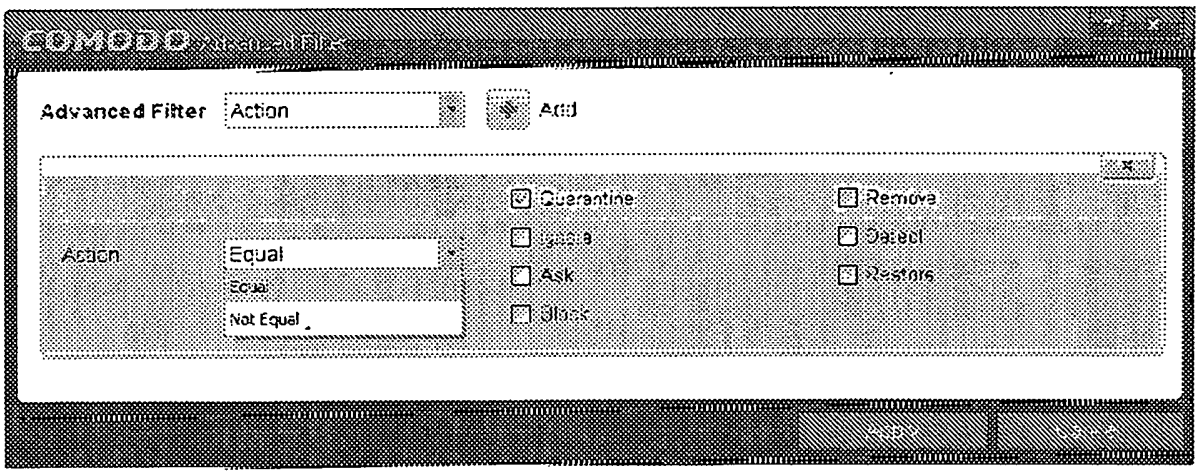
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for AV events will open
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.




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.



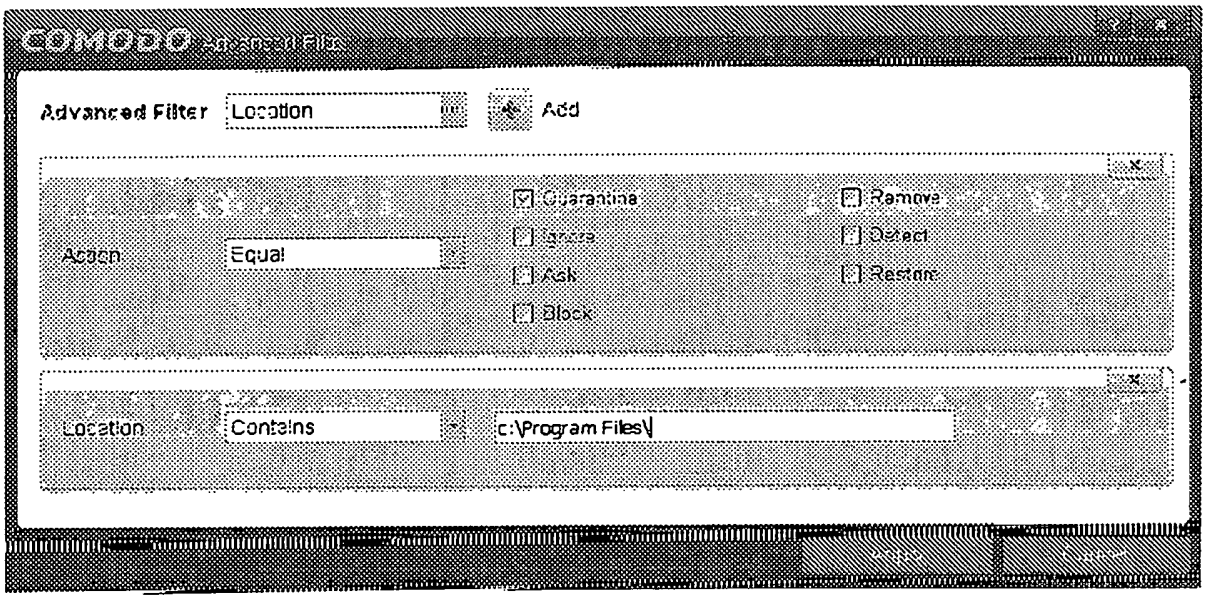

a) Select 'Equal' or 'Not Equal' option from the drop down. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:

- 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.

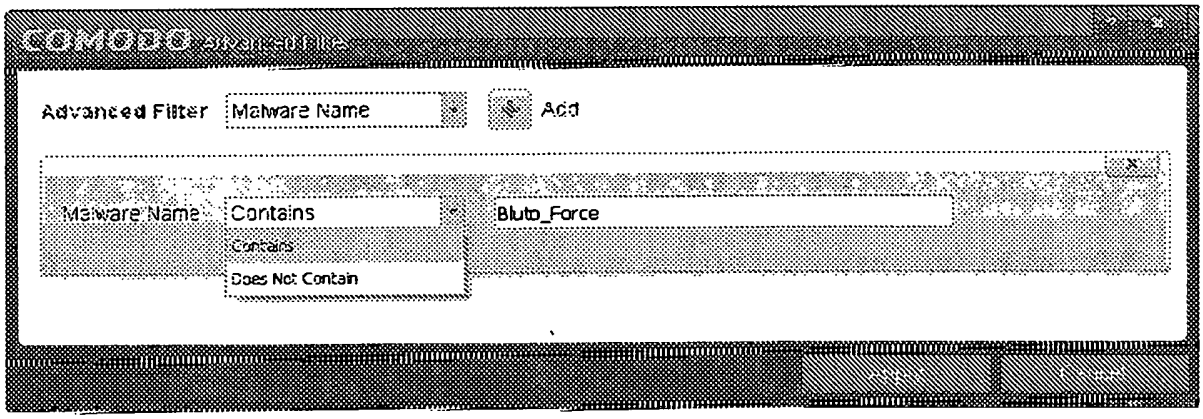



a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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.

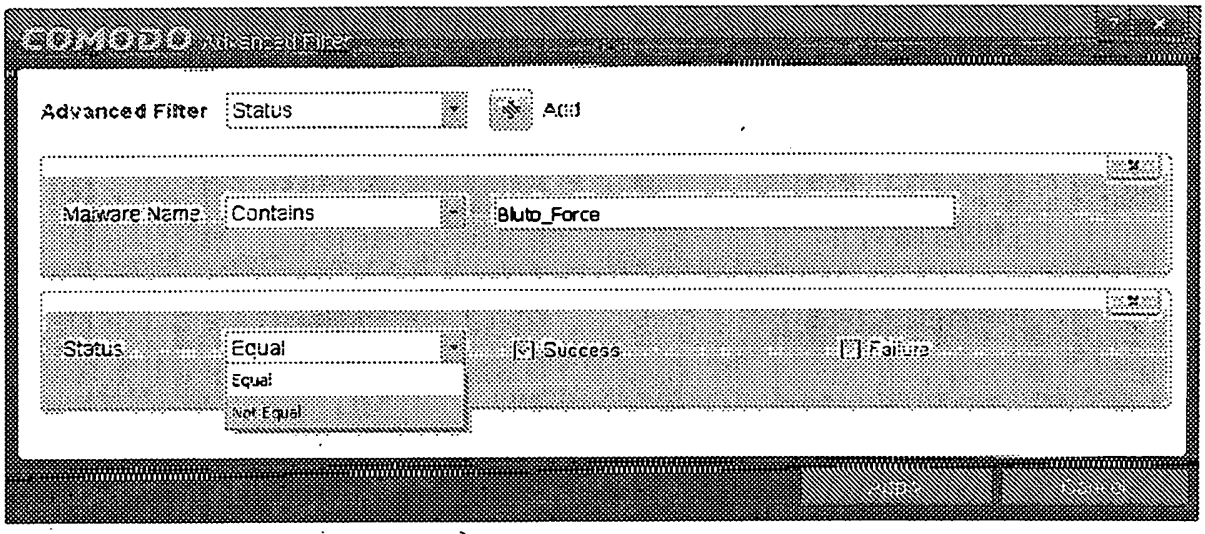



a) Select 'Contains' or 'Does Not Contain' option from the drop-down field.

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)

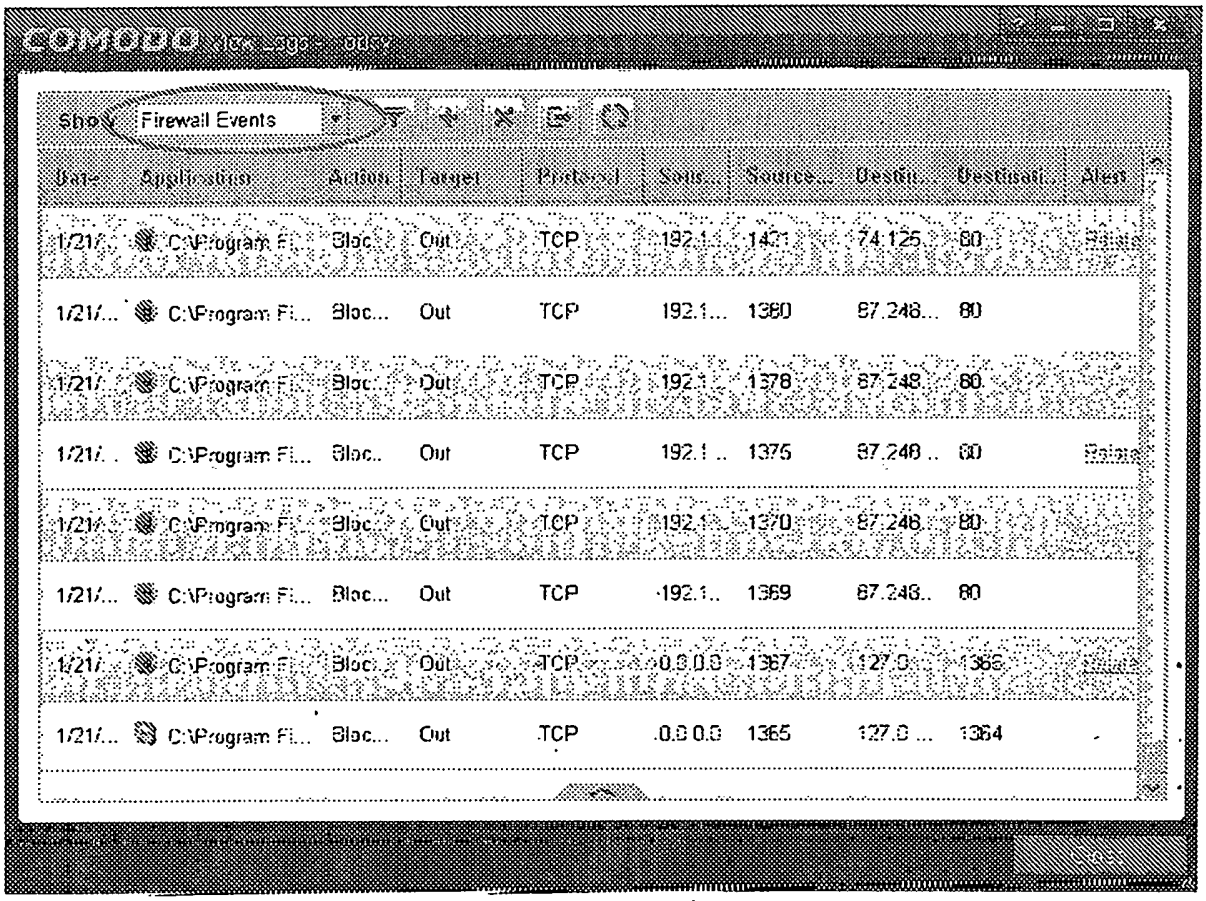
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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.

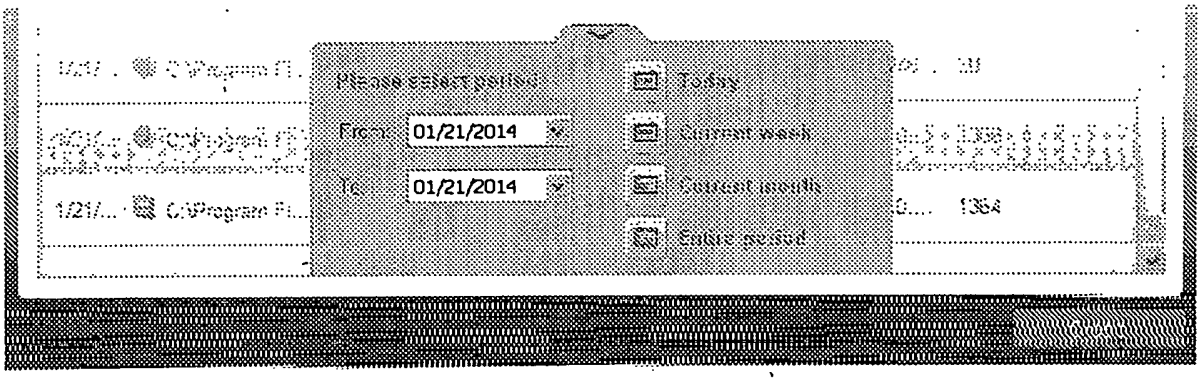
## 2.6.2.1. Filtering Firewall Logs

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

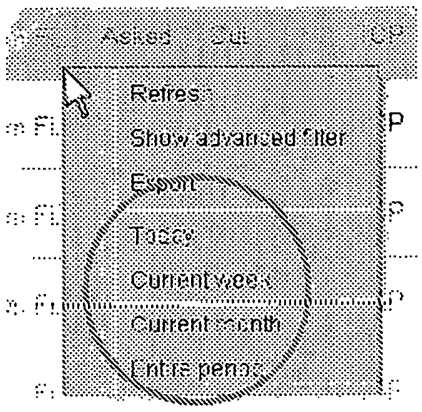
Preset Time Filters:

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.



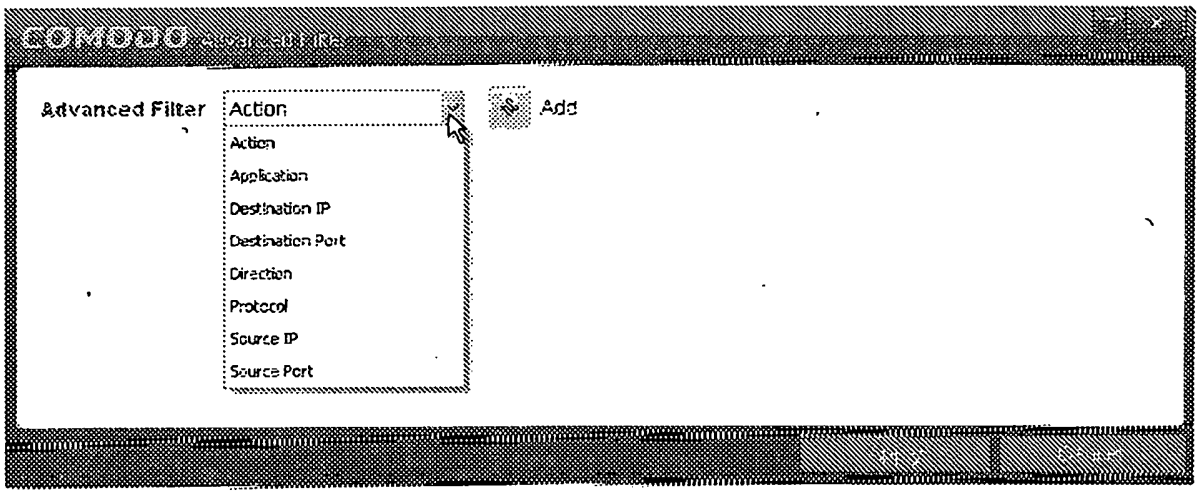
Advanced Filters

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**

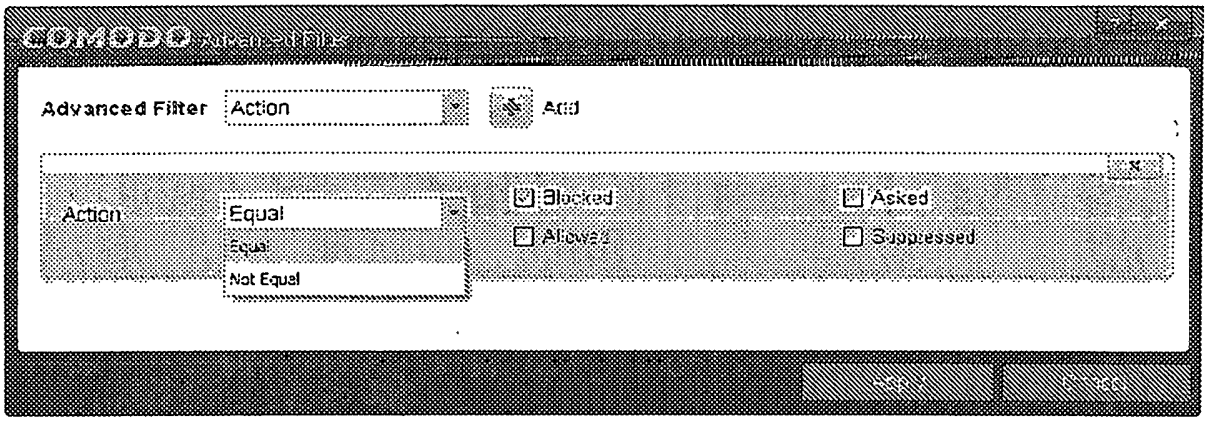
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for Firewall events will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply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

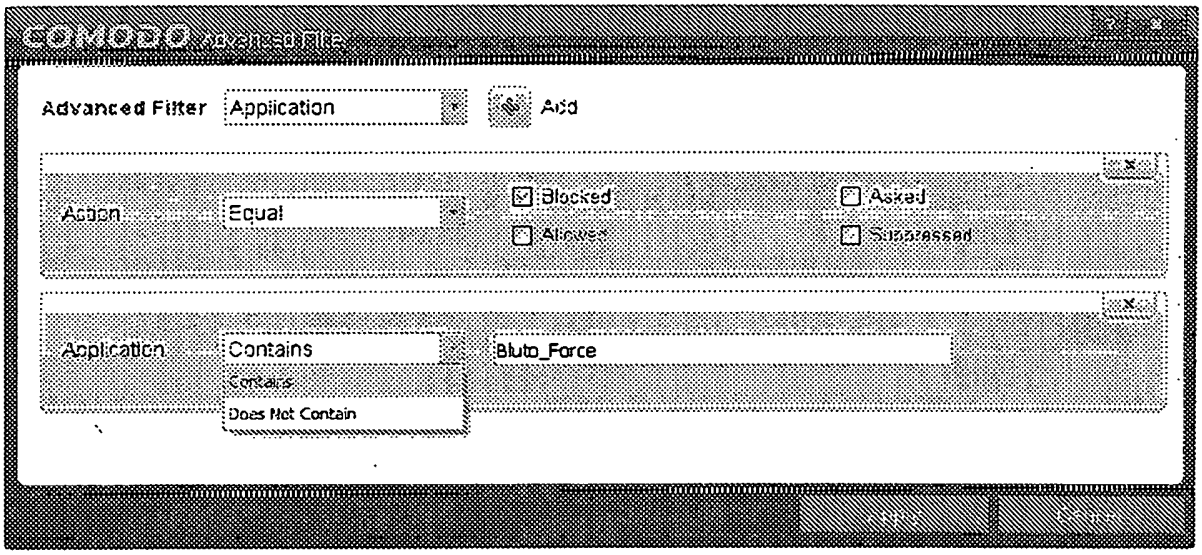
Following are the options available in the 'Advanced Filter' drop-down:

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

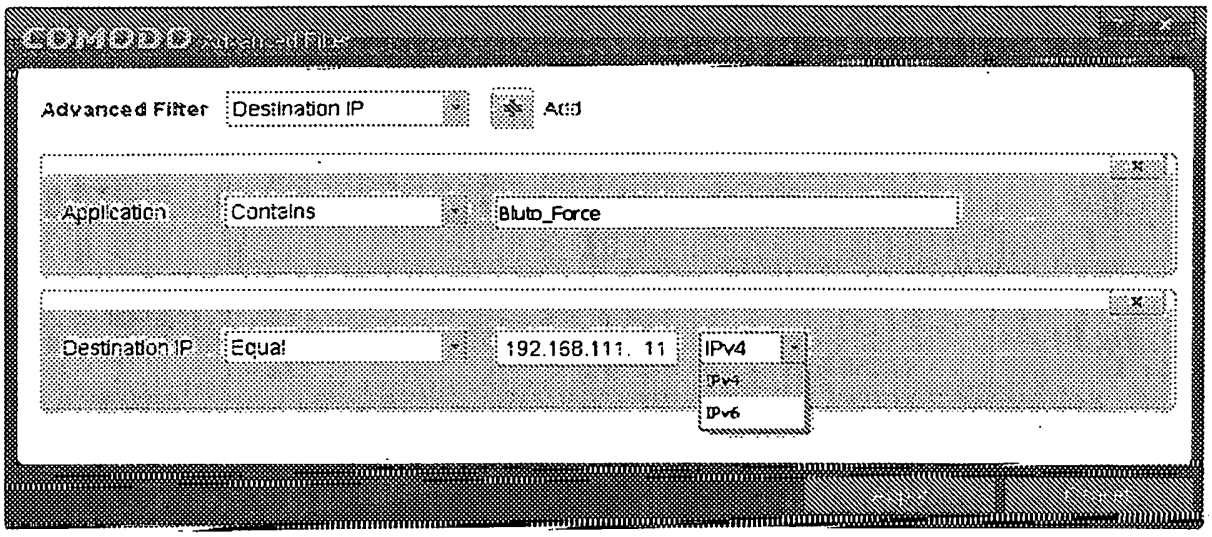
ii. **Application**: Selecting the 'Application' option displays a drop-down box and text entry field.




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.

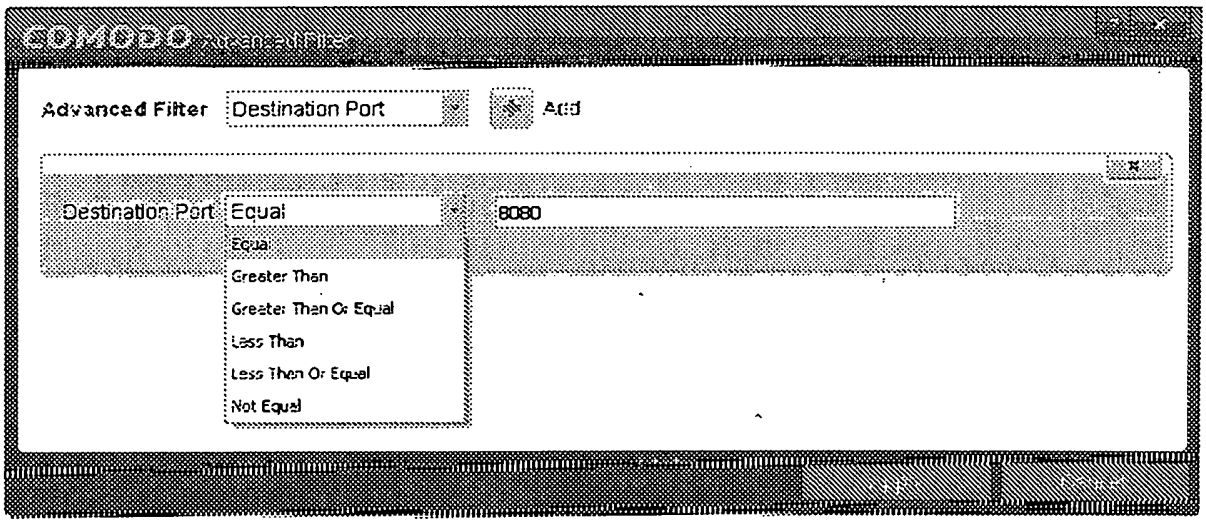
iii. **Destination IP**: Selecting the 'Destination IP' option displays two drop-down boxes and a text entry field.




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.

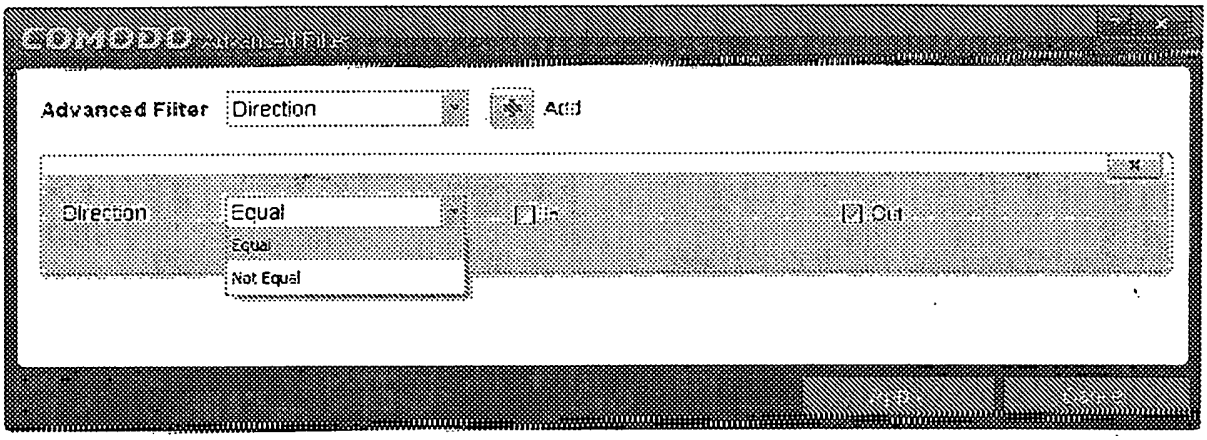



a) Select any one of the following option the drop-down box.
   - Equal
   - Greater than
   - Greater than or Equal
   - Less than
   - Less than or Equal
   - Not Equal

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

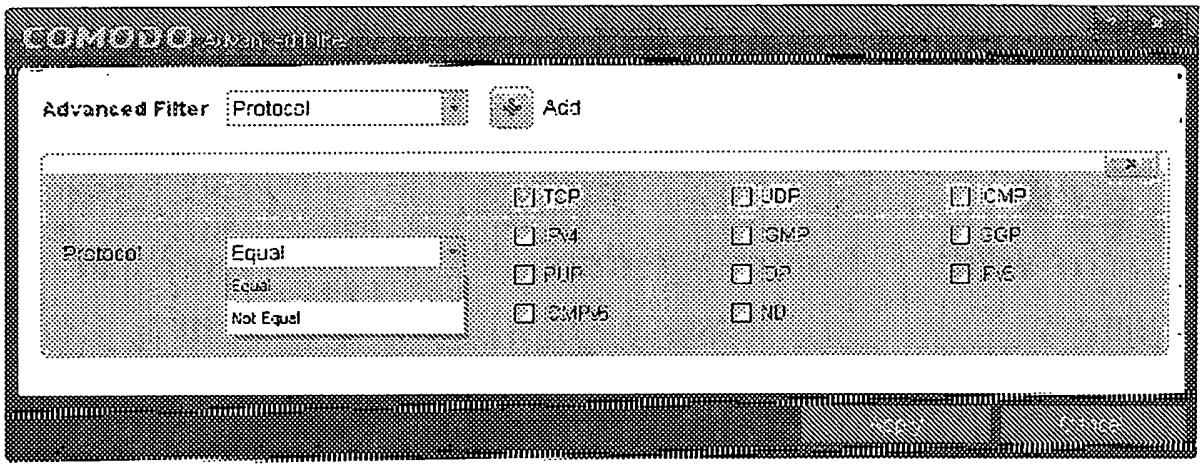
For example, if you choose 'Equal' option from the drop-down and enter 8080 in the text field, then all events containing the entry '8080' in the 'Destination Port' column will be displayed.

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



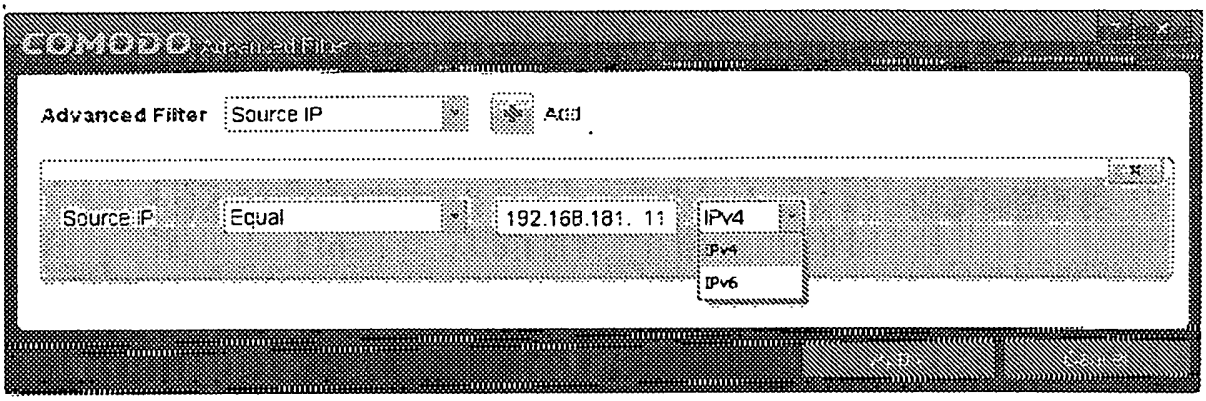

a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the check box of the specific filter parameters to refine your search. The parameter available are:
   - In: Displays a list of events that were directed into the system
   - Out: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



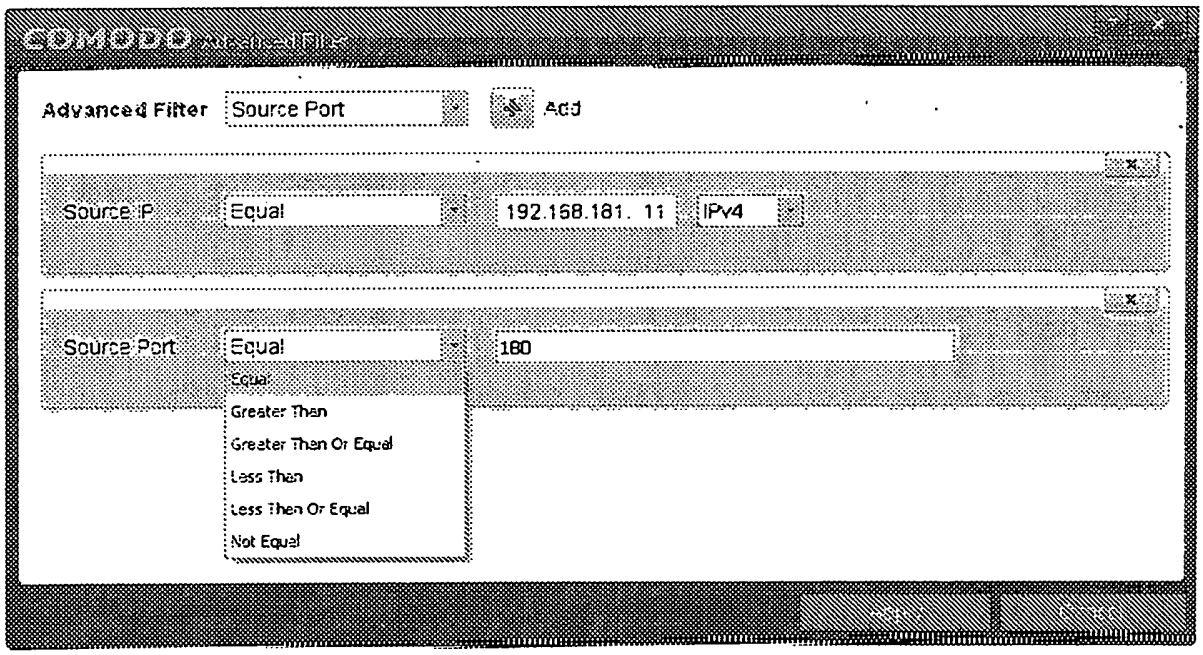

a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific filter parameters to refine your search. The parameter available are:
   - TCP
   - UDP
   - ICMP
   - IPV4
   - IGMP
   - GGP
   - PUP
   - IDP
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

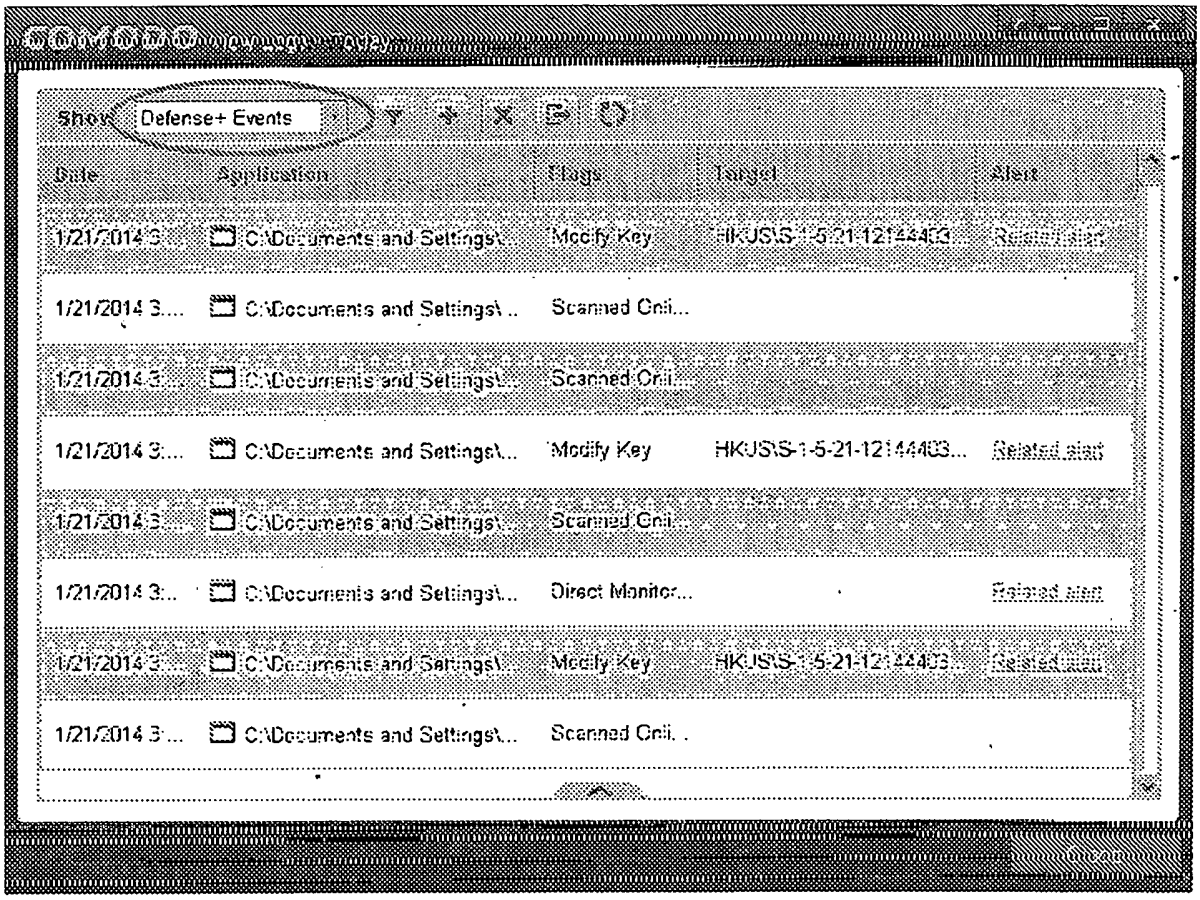
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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.

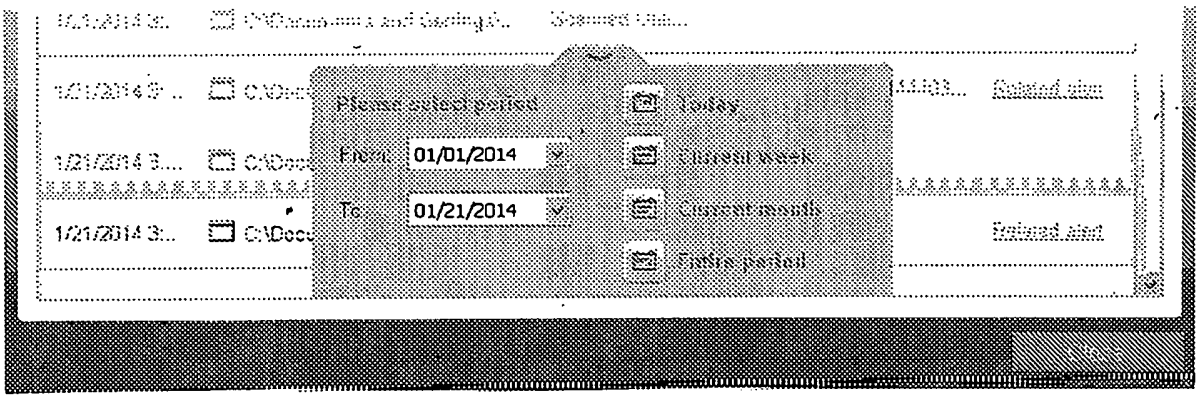
### 2.6.3.1. Filtering Defense+ Logs

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

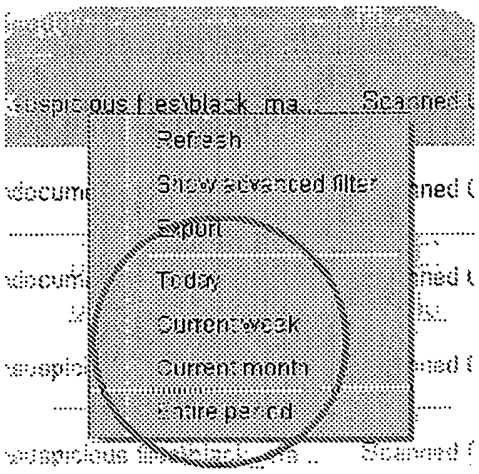
Preset Time Filters

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.



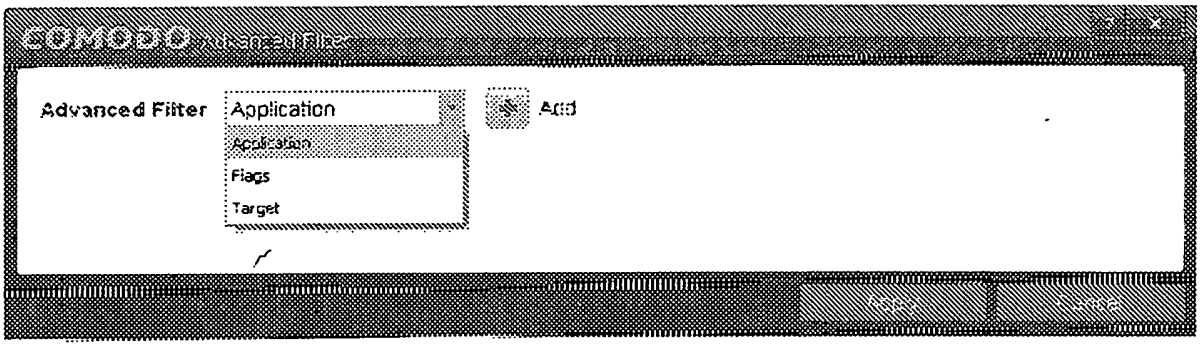

Advanced Filters

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

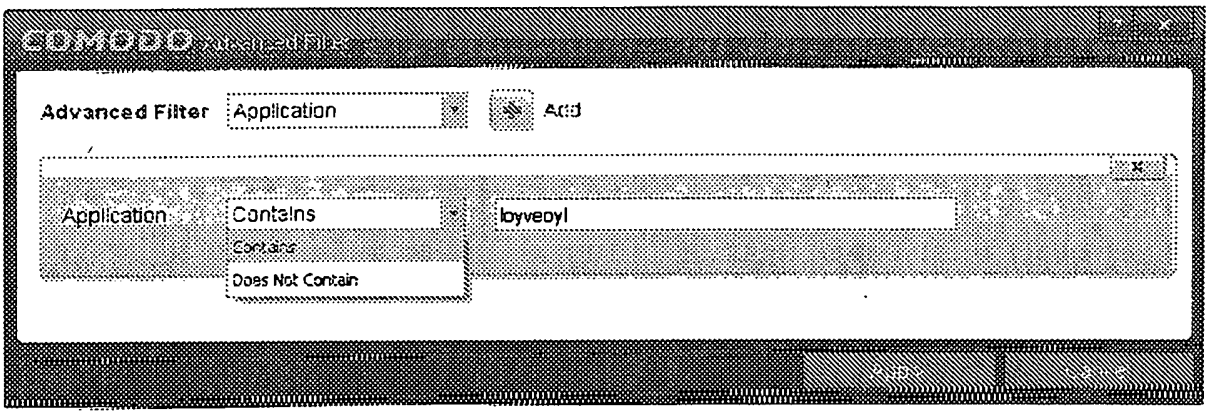
**To configure Advanced Filters for Defense+ events**

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:

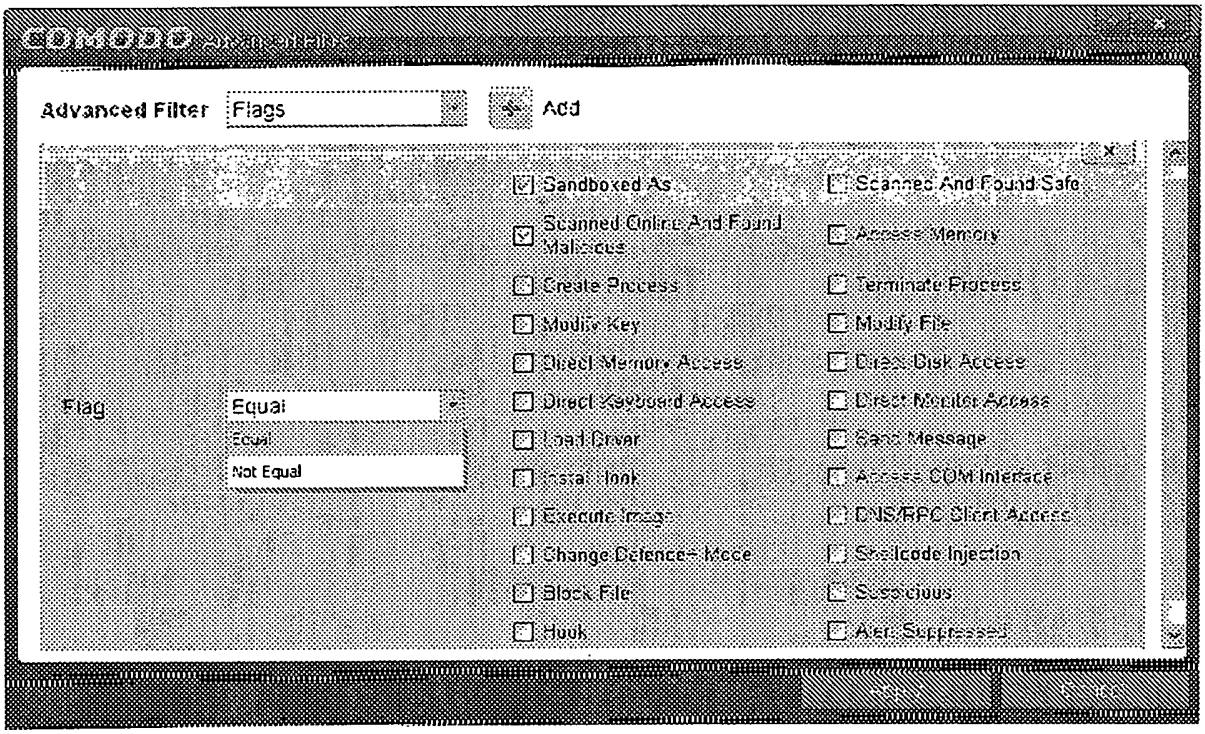
i. **Application**: Adding the 'Application' option displays a drop-down field and text entry field.




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.



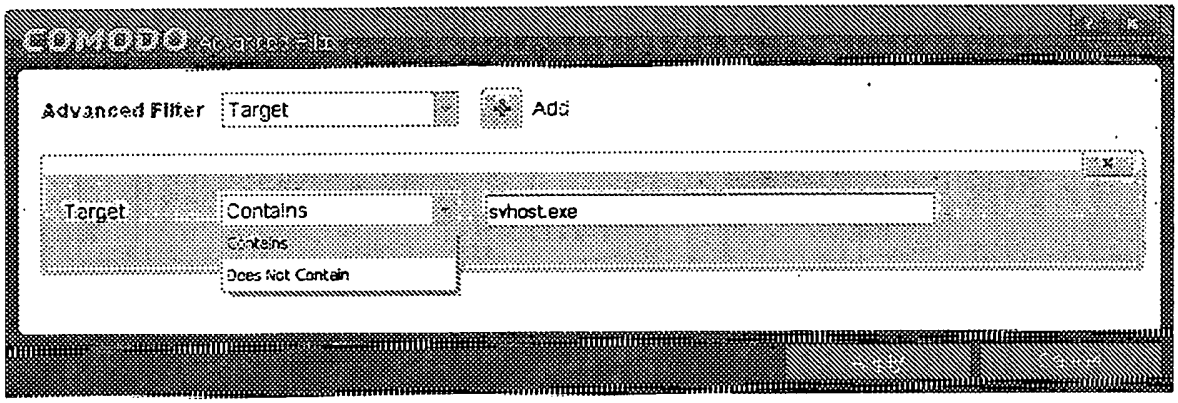

a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.
b) Now select the check-boxes of the specific filter parameters to refine your search. The parameter available are:

- 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.

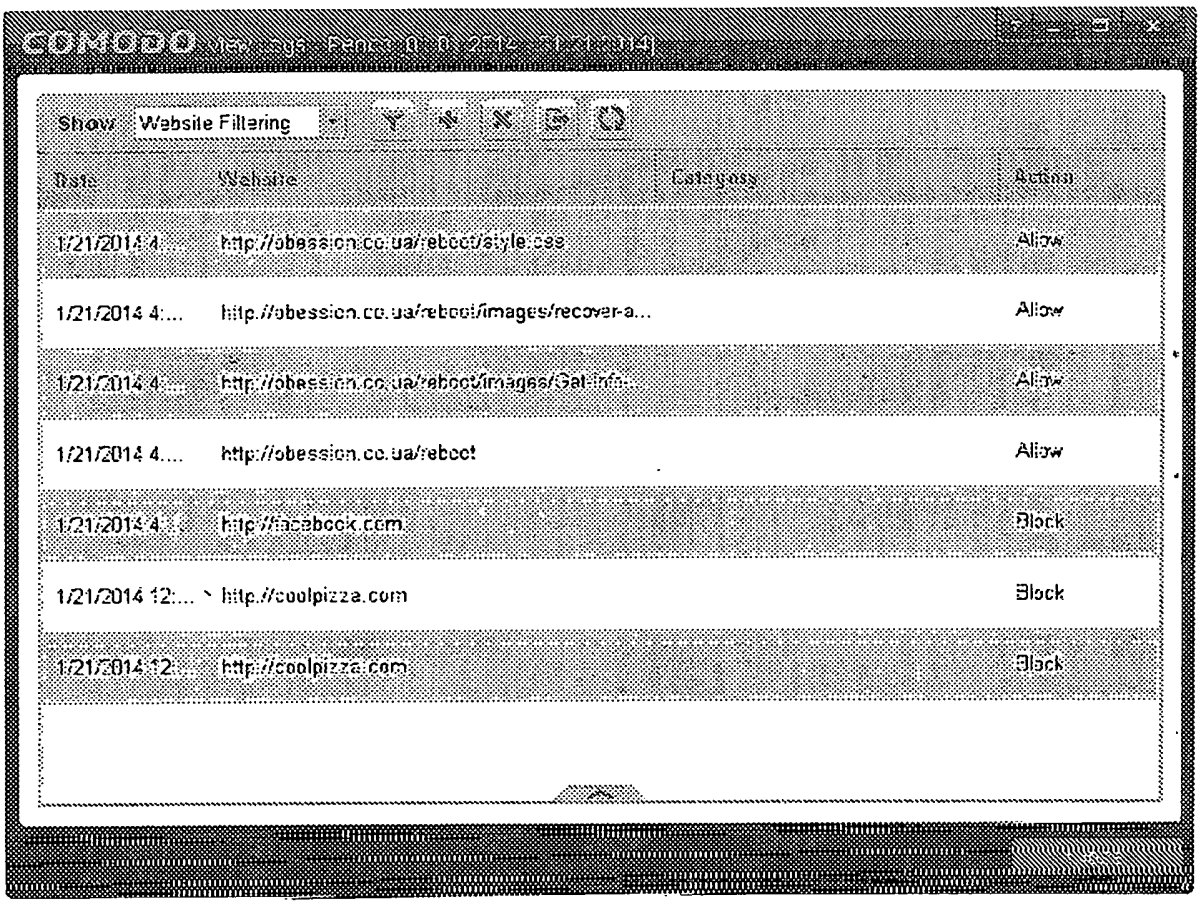
- Click 'Apply' for the filters to be applied to the Firewall log viewer. Only those Defense+ entries selected based on your set filter criteria will be displayed in the log viewer.
- For clearing all the filters, open 'Advanced Filter' pane and remove all the filters one-by-one by clicking the 'X' button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

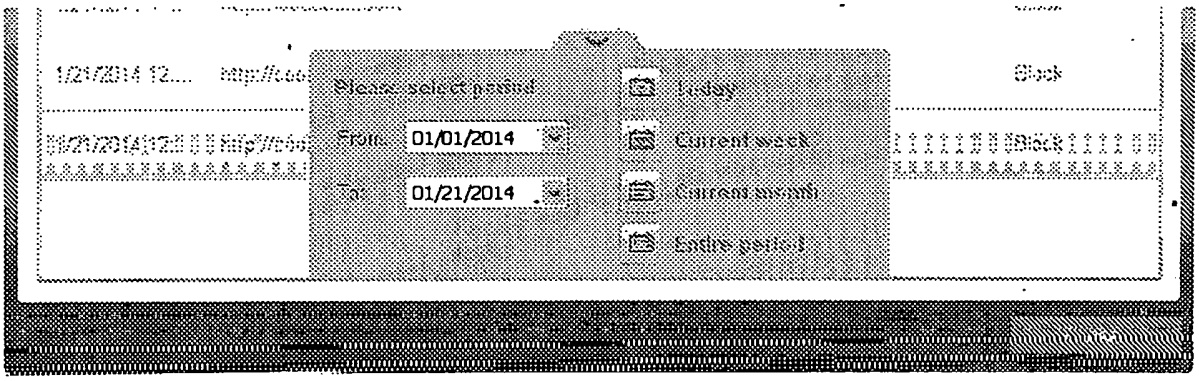
### 2.6.4.1. Filtering 'Website Filtering' Logs

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

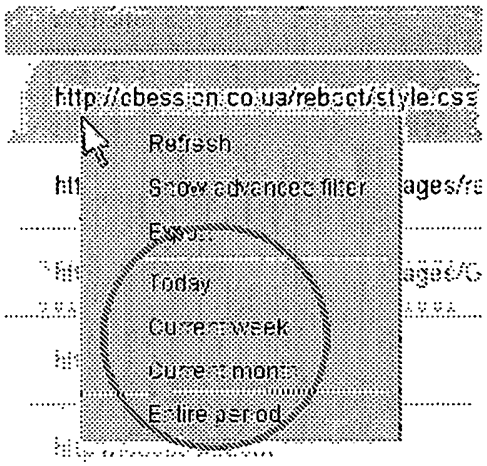
Preset Time Filters

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.



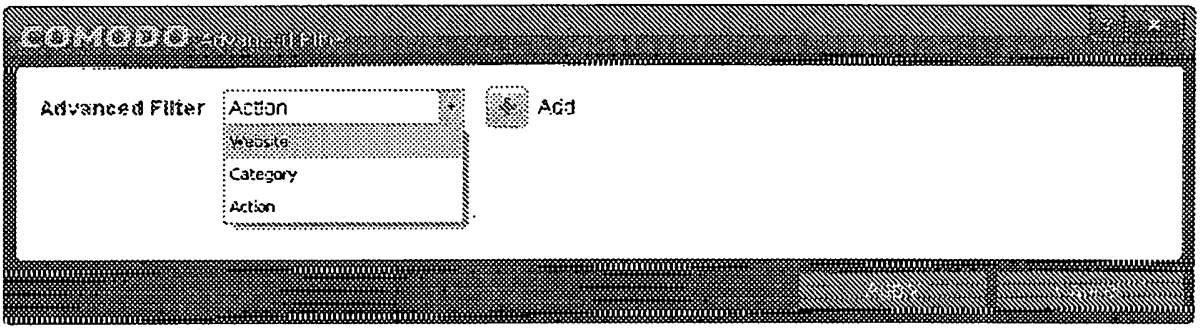

Advanced Filters

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

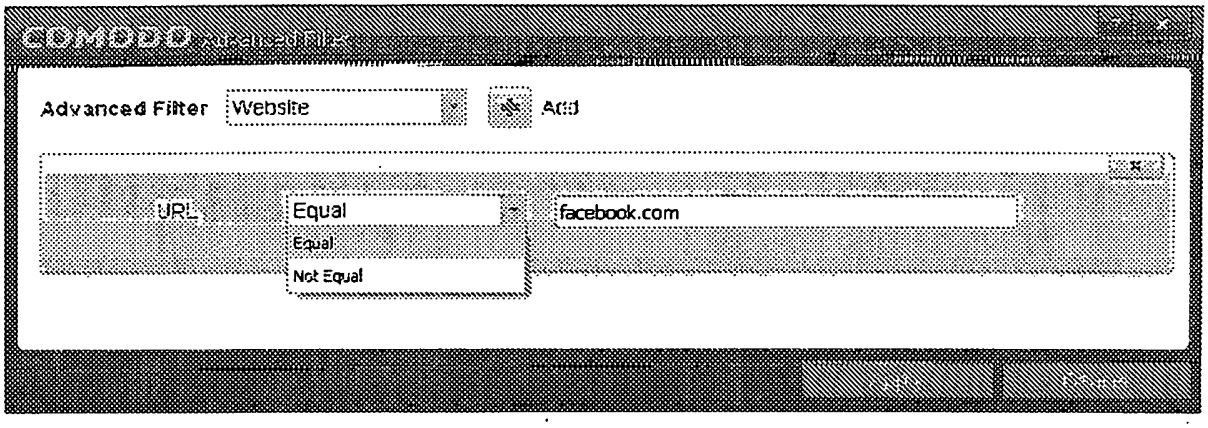
**To configure Advanced Filters for Defense+ events**

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.

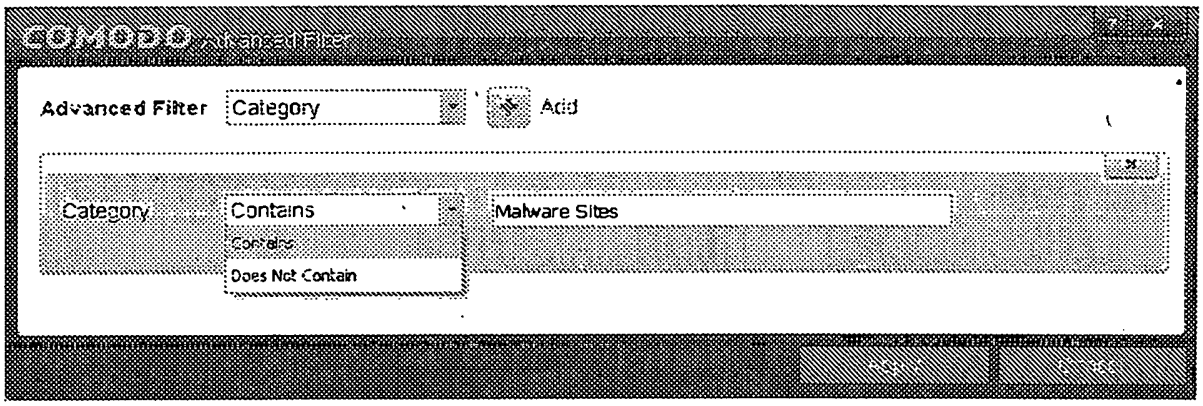



a) Select 'Equal' or 'Not Equal' option from the drop-down menu.

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.

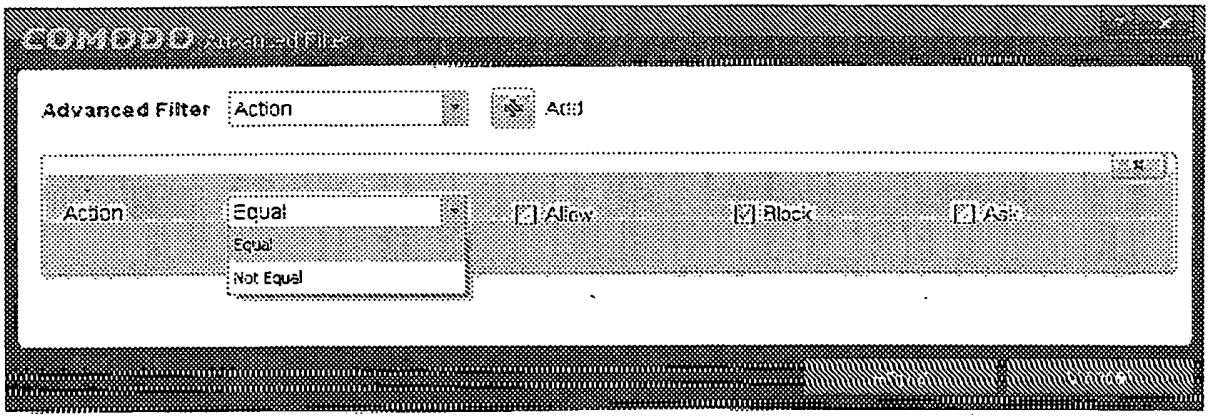



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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.

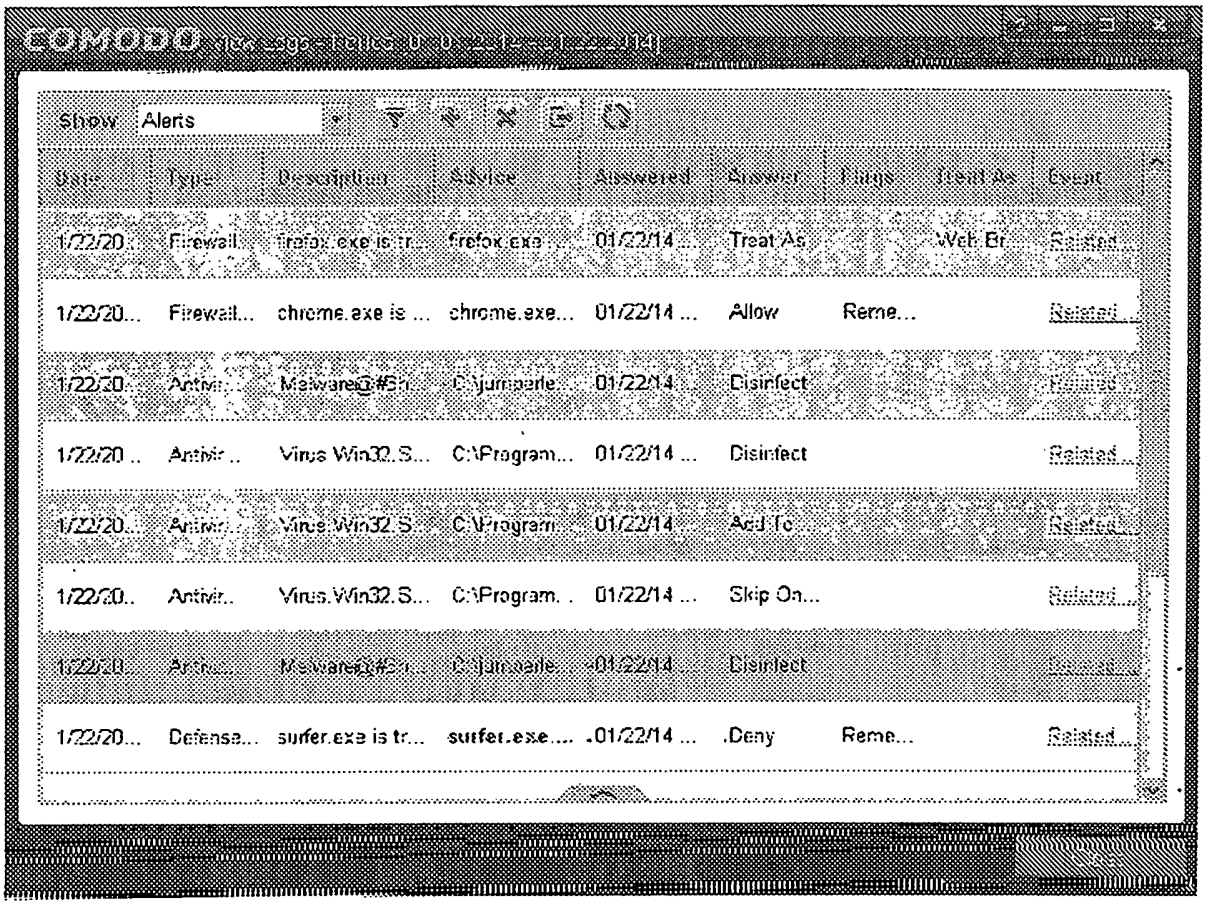
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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  .

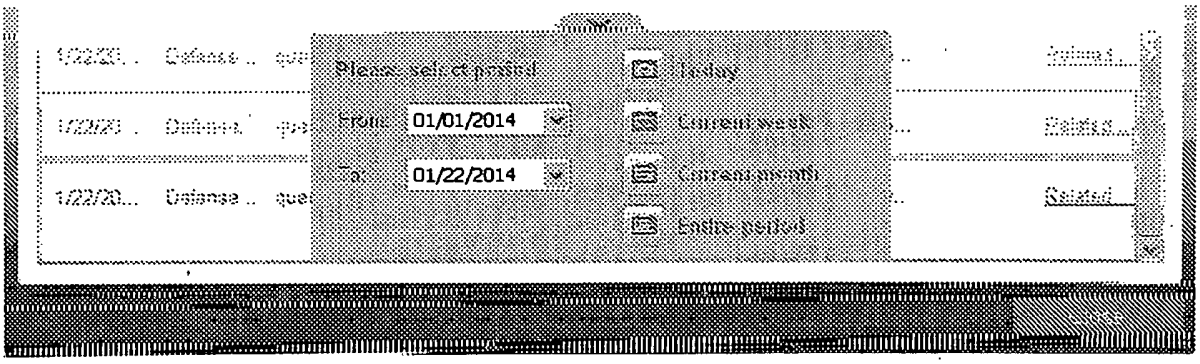
## 2.6.5.1. Filtering 'Alerts Displayed' Logs

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

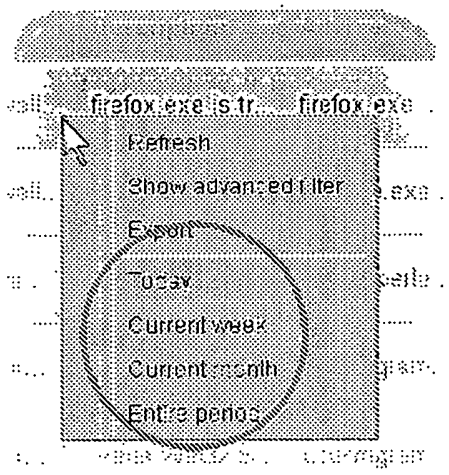
Preset Time Filters

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

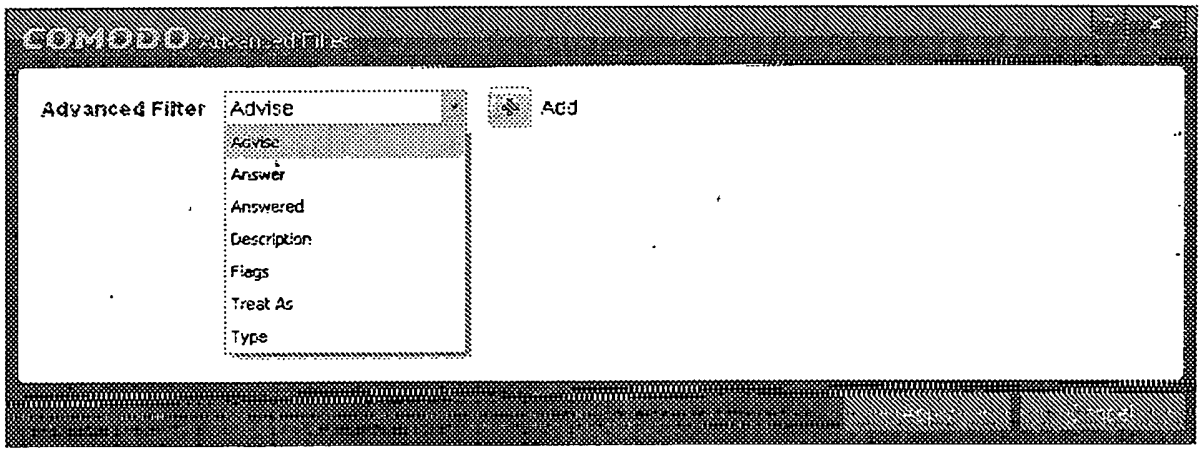
You can further refine the displayed events according to specific filters. Following are available filters for 'Alerts' logs and their meanings:

- **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**

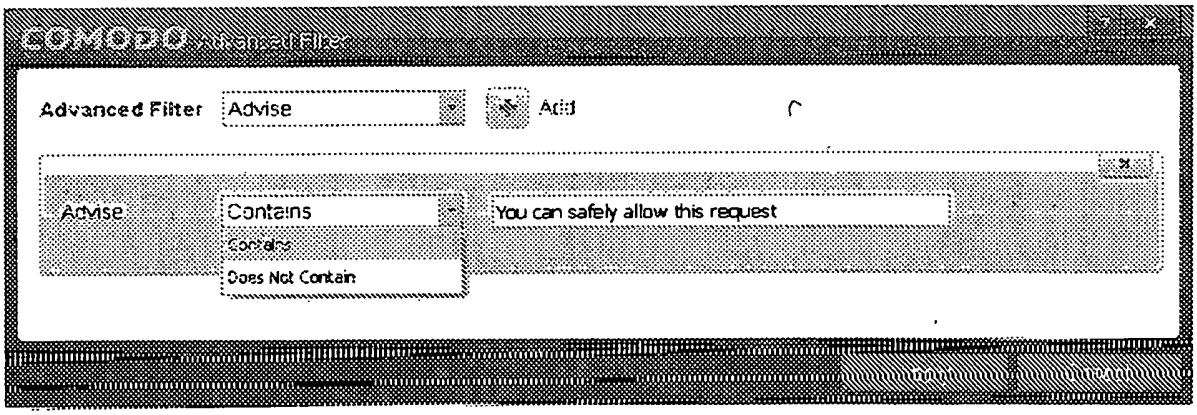
1. Click the funnel button  from the title bar or right click inside the log viewer module and choose 'Show Advanced Filter' from the context sensitive menu. The Advanced Filter interface for 'Alerts' logs will open.
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the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

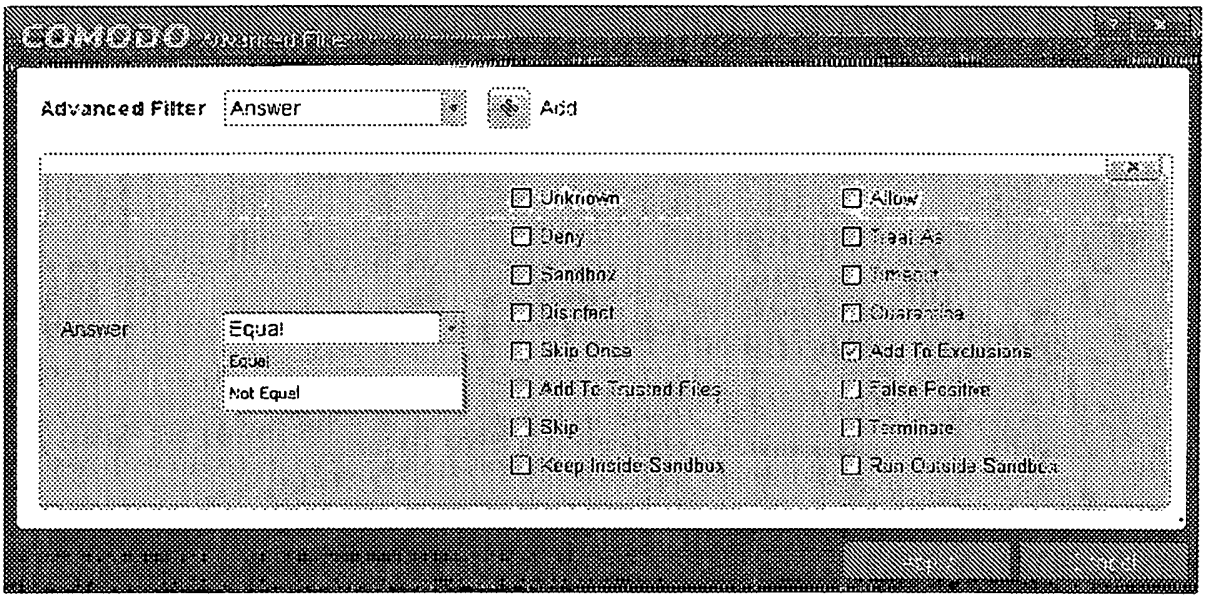



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.
b) Enter the text or word as your filter criteria.

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.



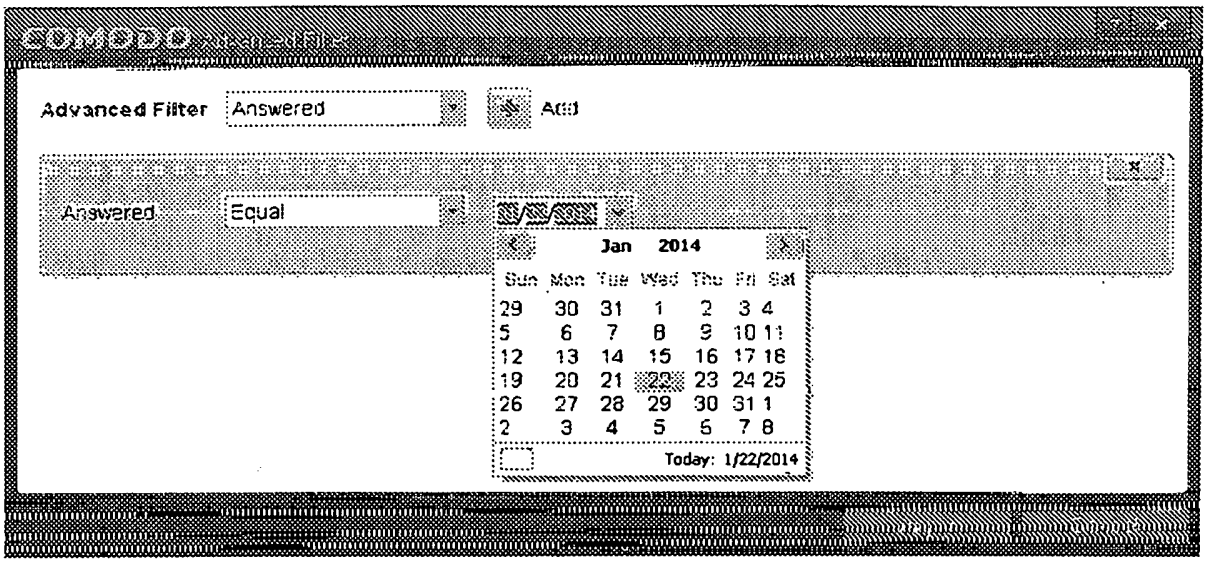

a) Select 'Equal' or 'Not Equal' option from the drop down menu. 'Not Equal' will invert your selected choice.

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.

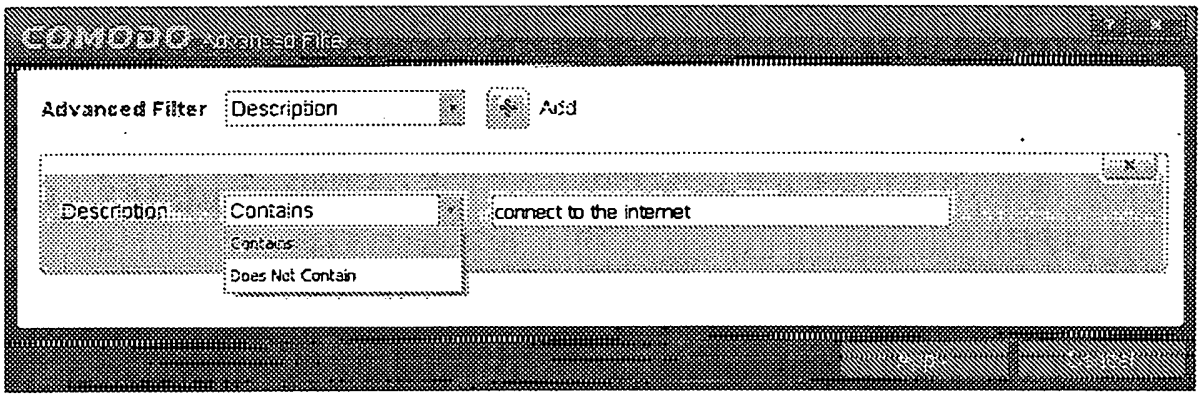



a) Select any one of the following option the drop-down box.
   - Equal
   - Not Equal

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.

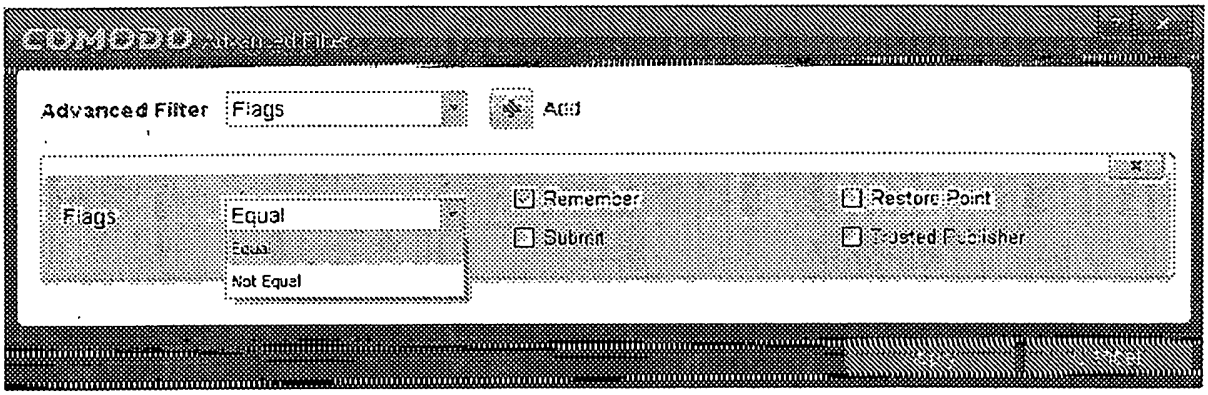



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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.

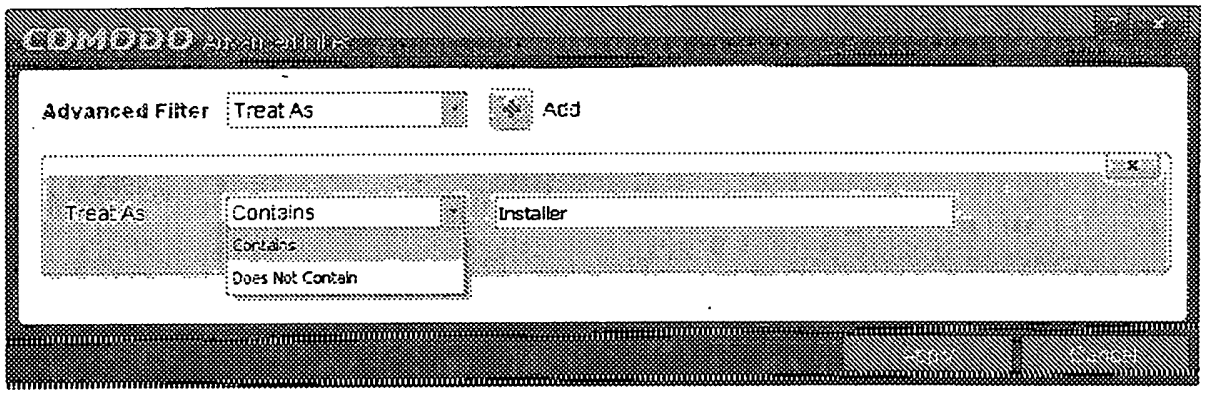
v. **Flags**: The 'Flags' option enables you filter the entries based on the flags set for the kinds of actions against the event triggered by the file. Selecting the 'Flags' option displays a drop down menu and a set of specific filter parameters that can be selected or deselected.




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.

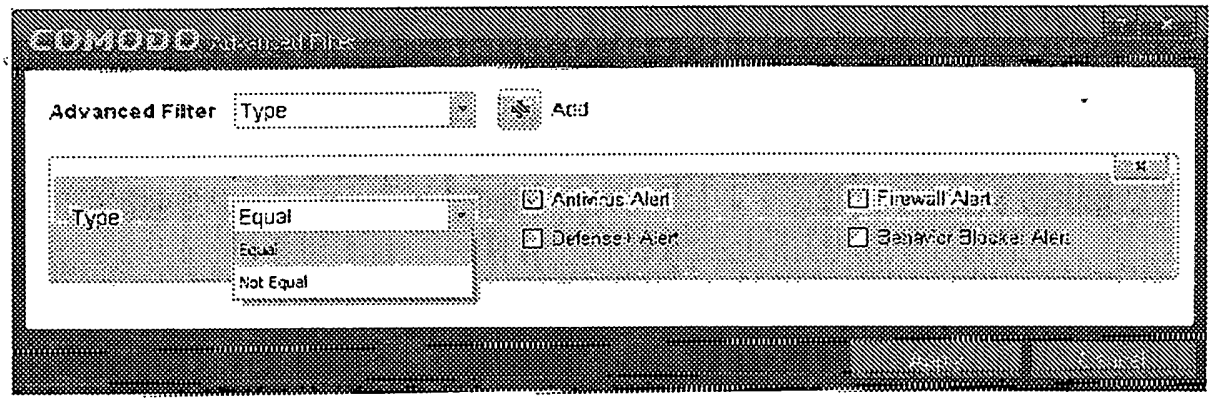
vi. **Treat As**: The 'Treat As' enables you to filter the log entries based on their 'Treat As' response you entered in the pop-up alert. Selecting the 'Treat As' option displays a drop-down menu and text entry field.




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.

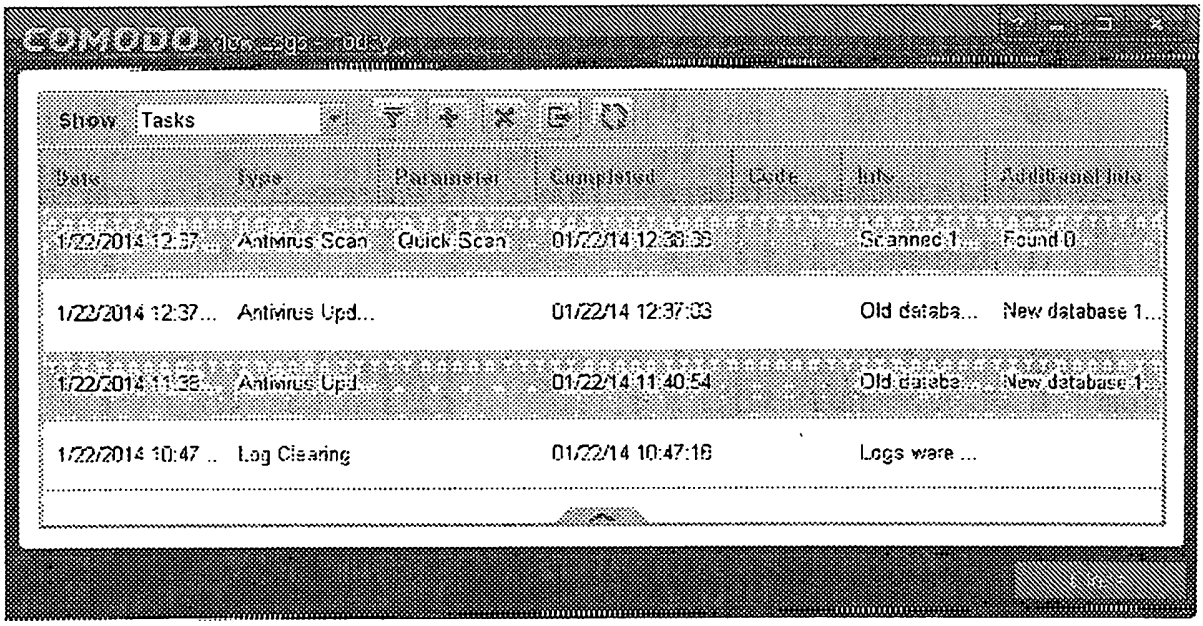
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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.

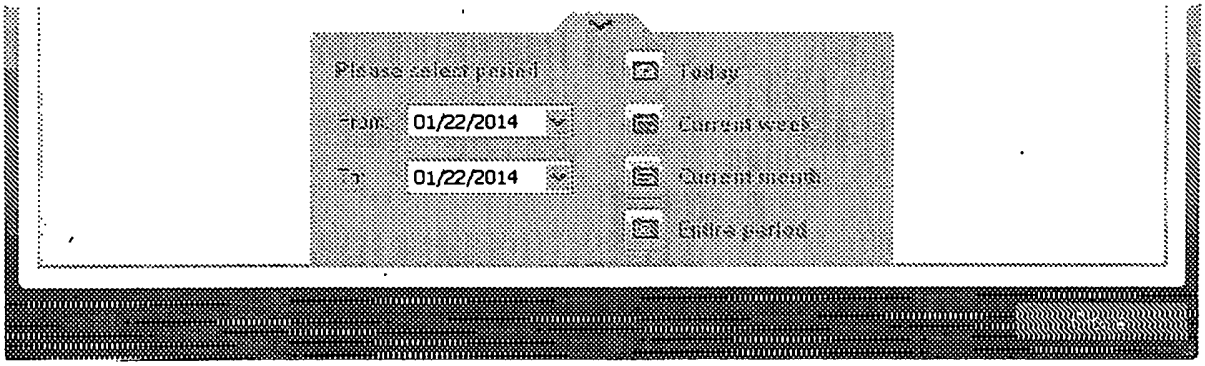
## 2.6.6.1. Filtering 'Tasks Launched' Logs

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

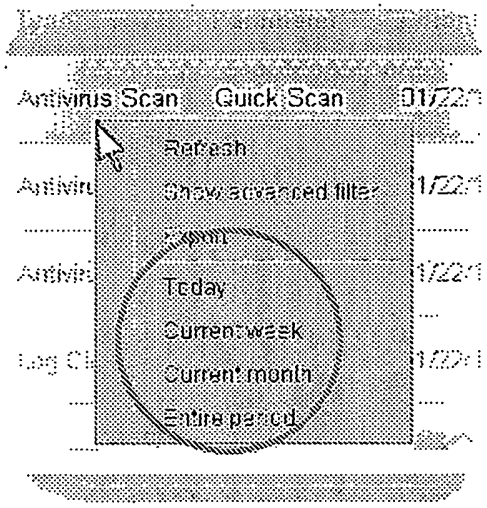
Preset Time Filters

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

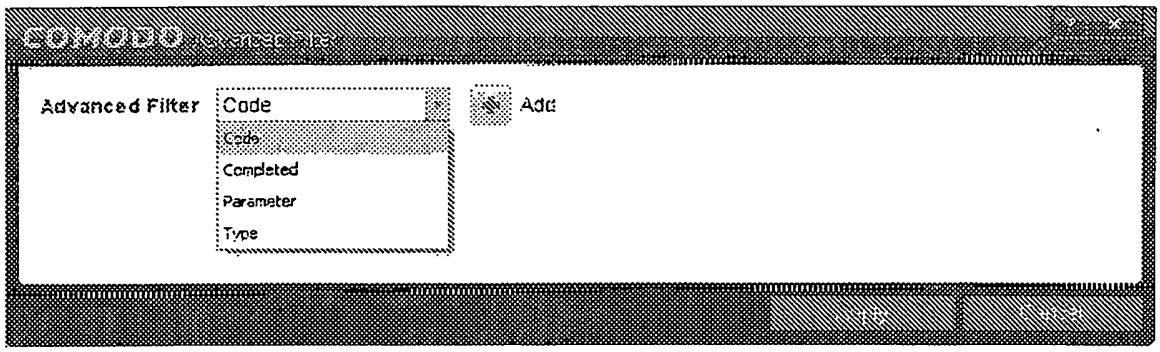
You can further refine the displayed events according to specific filters. Following are available filters for 'Tasks' logs and their meanings:

- **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.

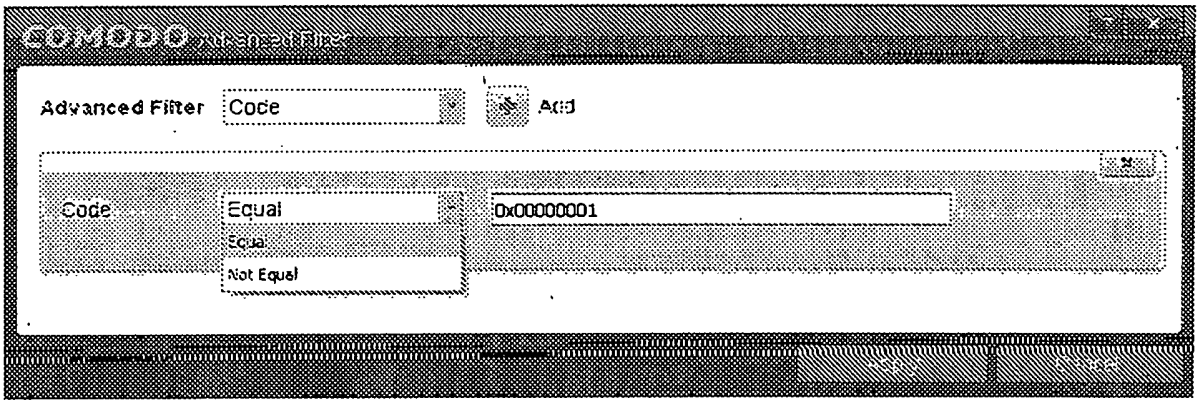
2. Select the filter from the 'Advanced Filter' drop-down and click 'Add' to apply the filter.




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:

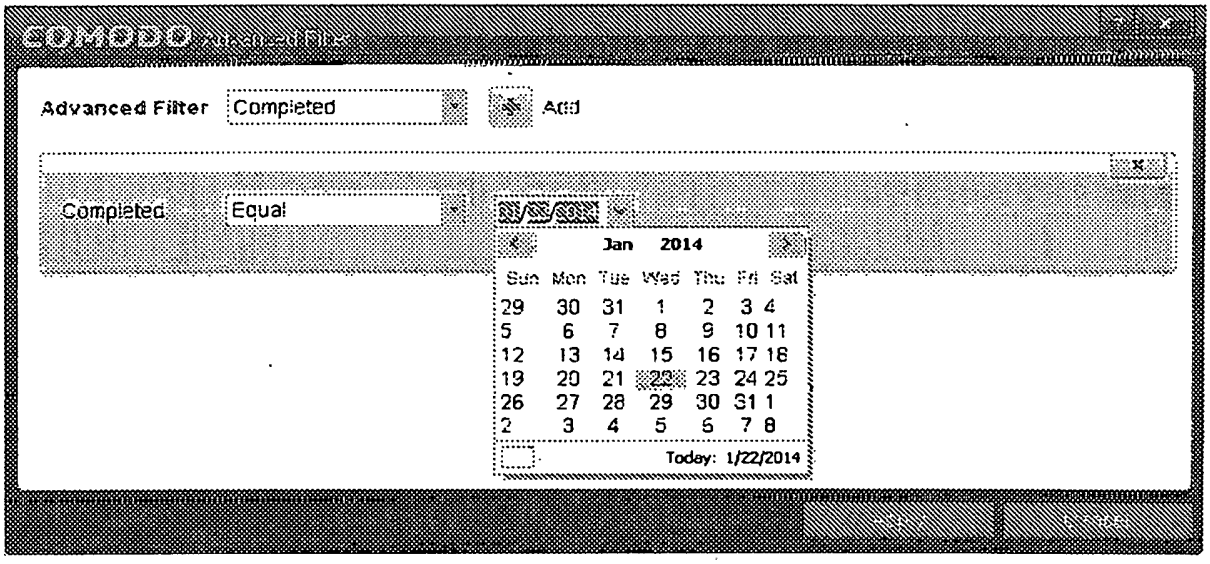
i. **Code**: The Code option enables you to filter the tasks based on their code value. Selecting the 'Code' option displays a drop-down field and text entry field.




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.

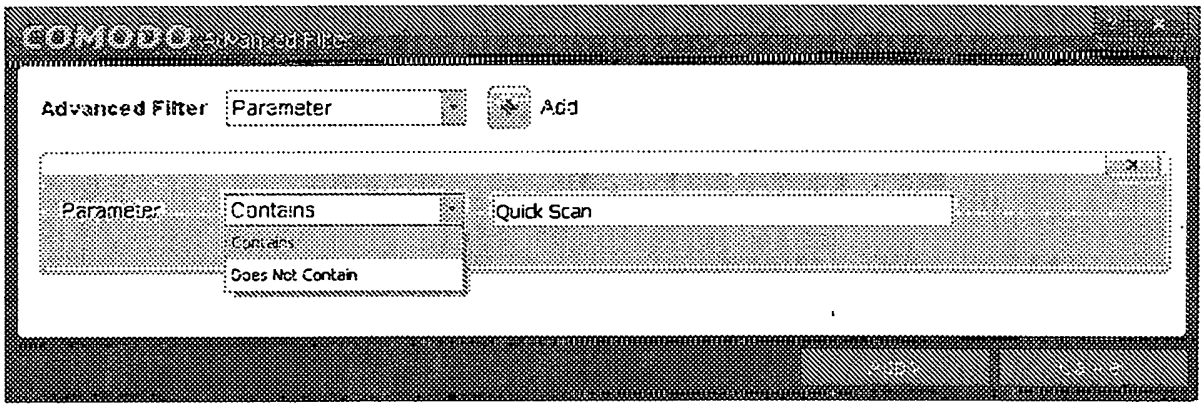



a) Select any one of the following option the drop-down box.
   - Equal
   - Not Equal

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.

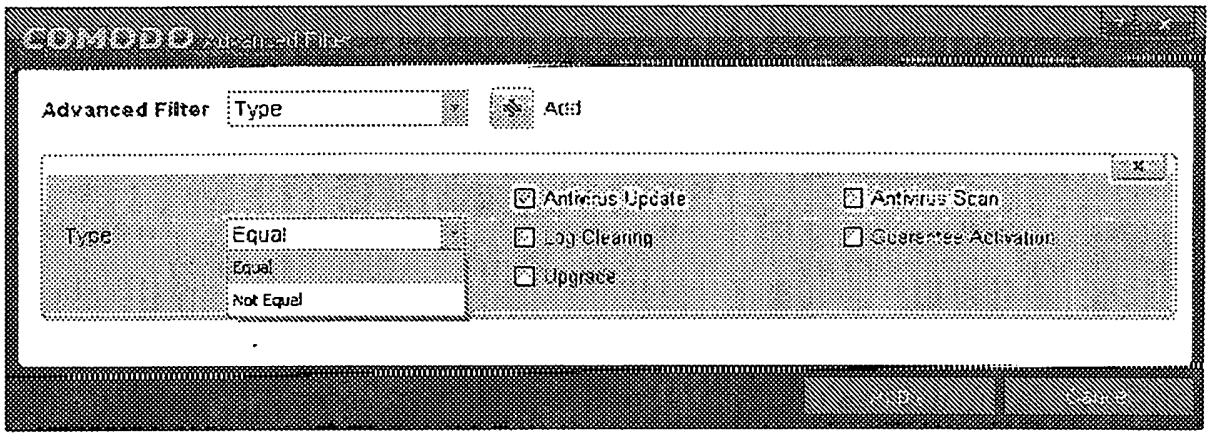



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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

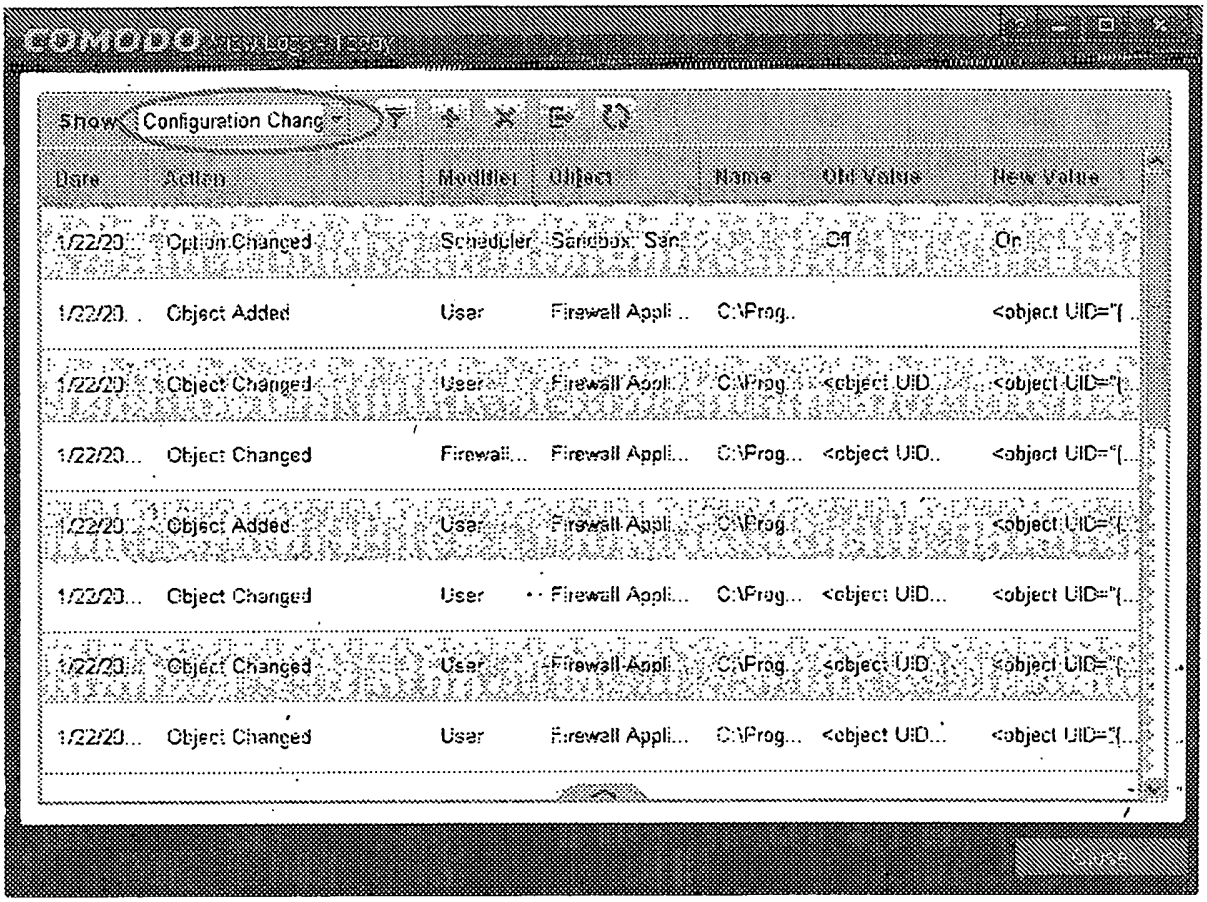
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and click 'Add'. You can also remove a filter type by clicking the 'X' button at the top right of the filter pane.

- 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.

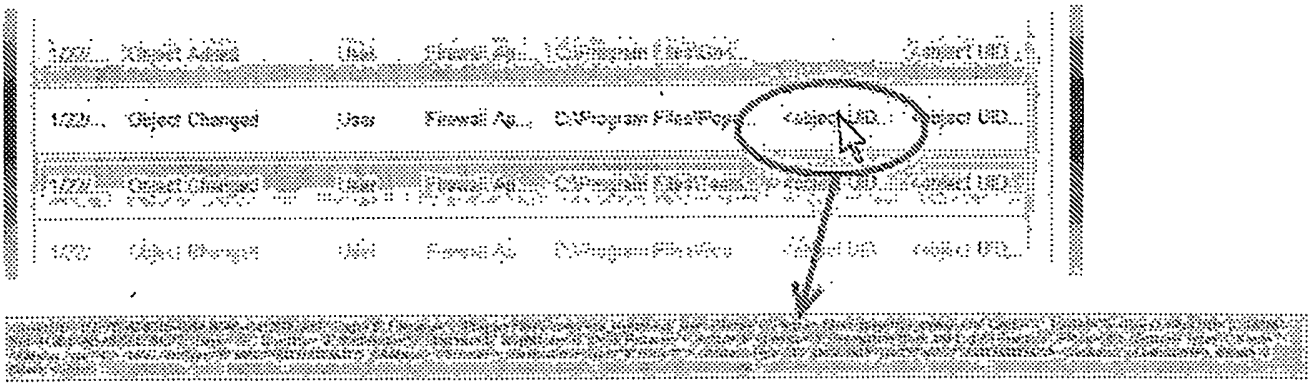
The 'Configuration Changes' logs can be viewed by selecting 'Configuration Changes' from the 'Show' drop-down of the log viewer interface.




**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.

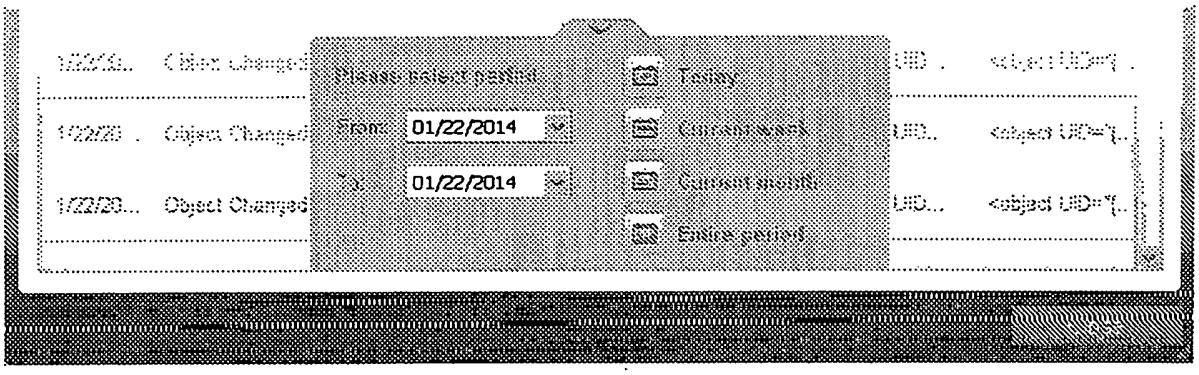
### 2.6.7.1. Filtering 'Configuration Changes' Logs

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

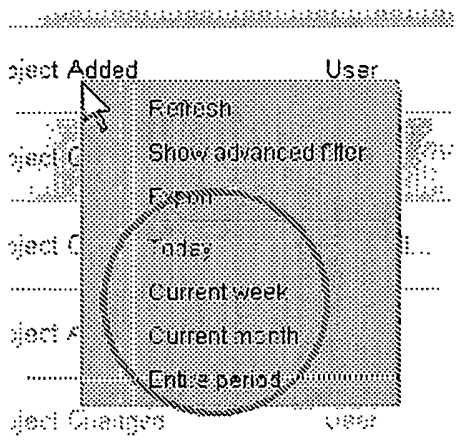
Preset Time Filters

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.



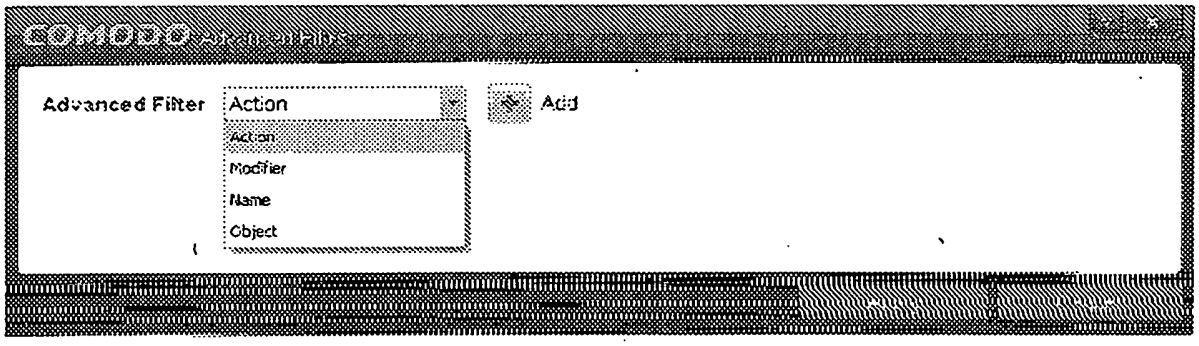

Advanced Filters

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

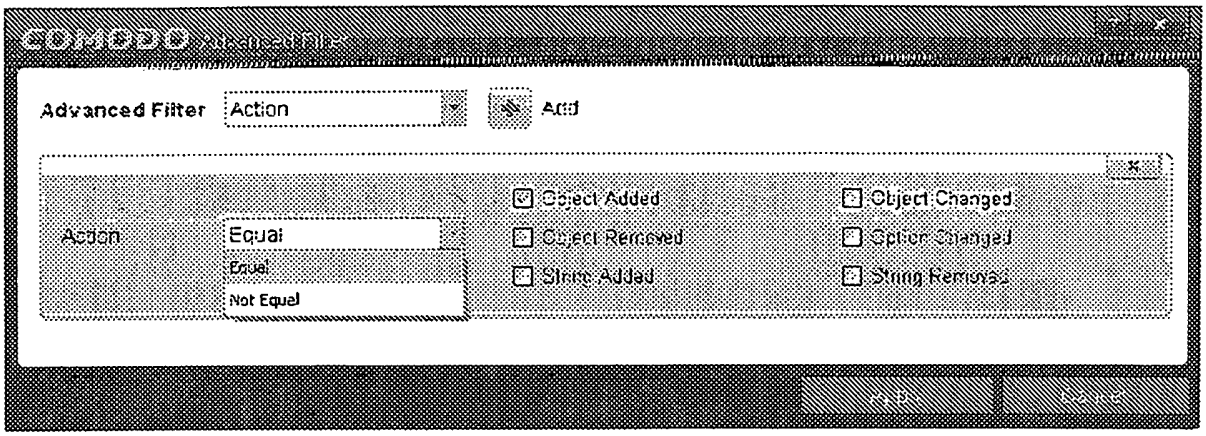
**To configure Advanced Filters for Configuration Changes Logs**

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:

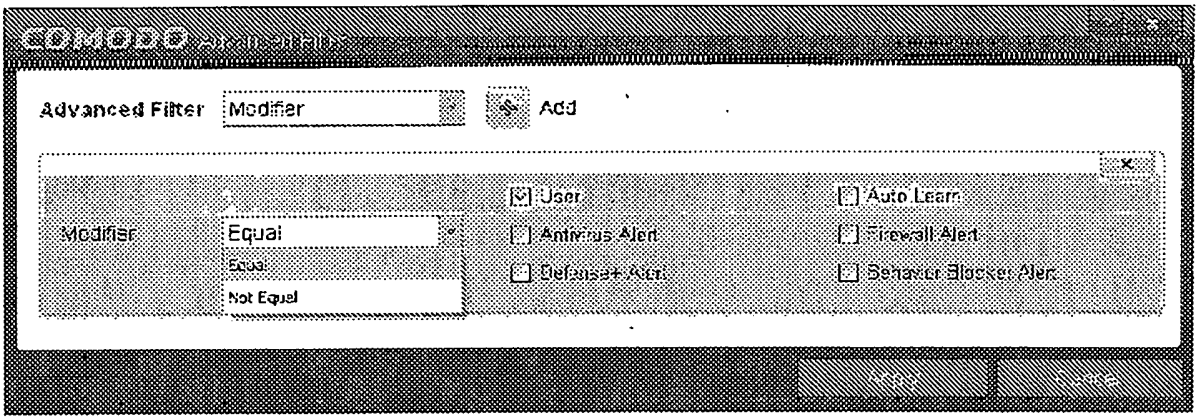
i. **Action**: The 'Action' option allows you to filter the log entries based on the actions executed like change in options, addition of objects, strings and so on. Selecting the 'Action' option displays a drop-down box and a set of specific filter parameters that can be selected or deselected.




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.

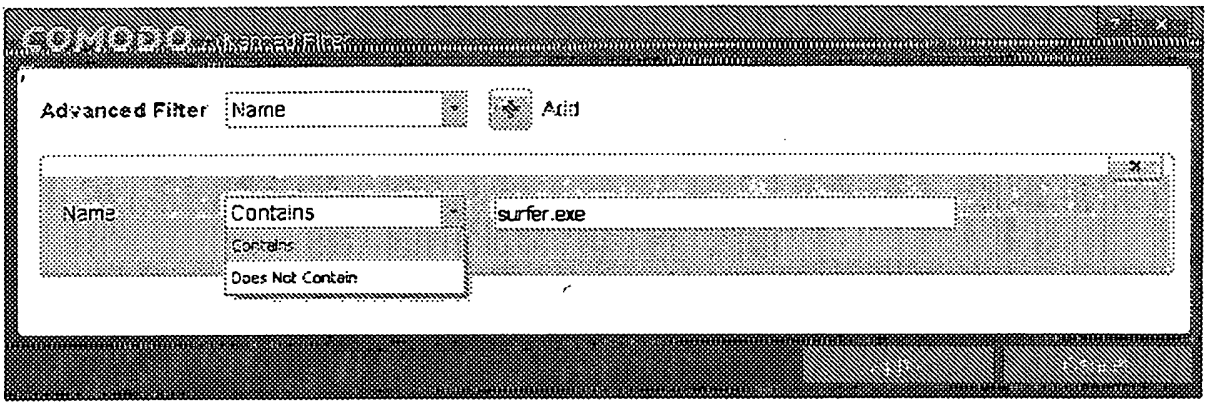



a) Select 'Equal' or 'Not Equal' option from the drop-down box. 'Not Equal' will invert your selected choice.
b) Now select the checkboxes of the specific entities that has effected the change, to refine your search. The parameters available are:
   - User
   - Auto Learn
   - Antivirus Alert
   - Firewall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

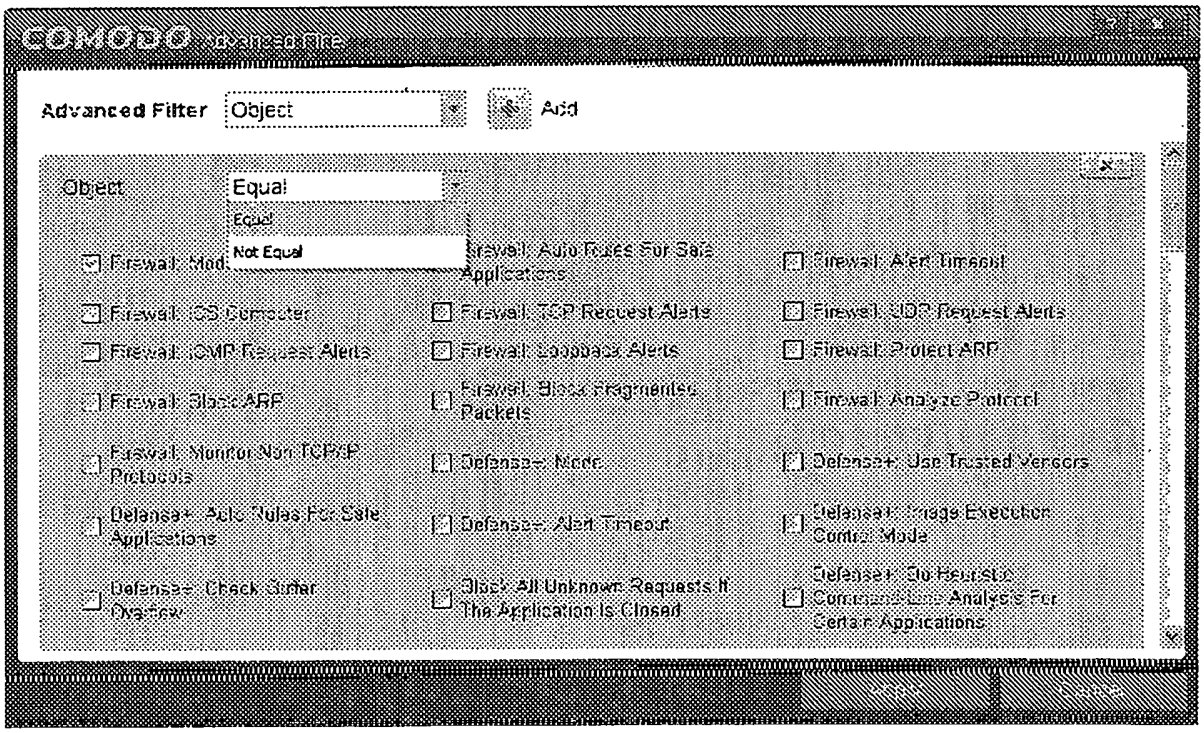



a) Select 'Contains' or 'Does Not Contain' option from the drop-down menu.

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.

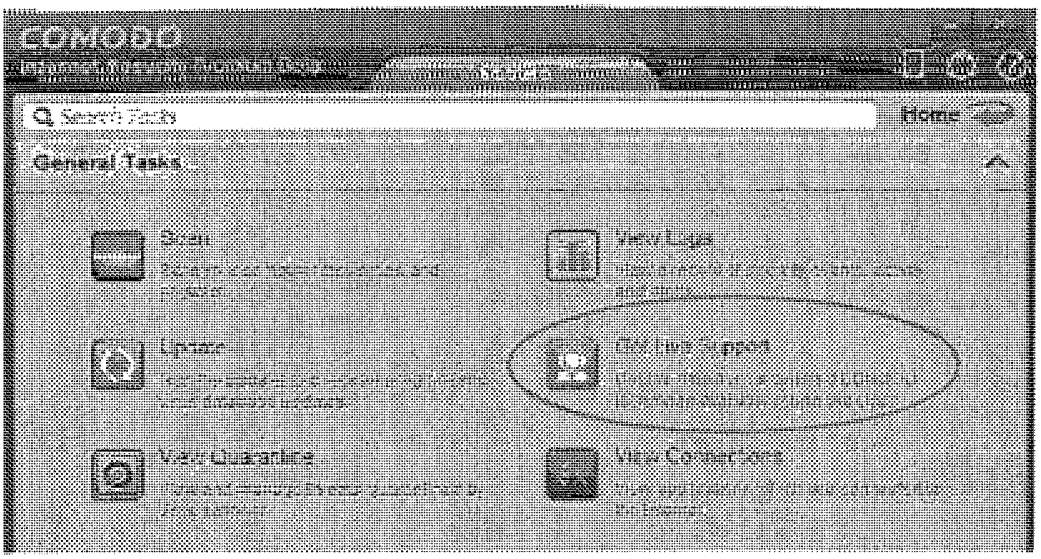
Note: More than one filter can be added in the 'Advanced Filter' pane. After adding one filter type, select the next filter type and

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.



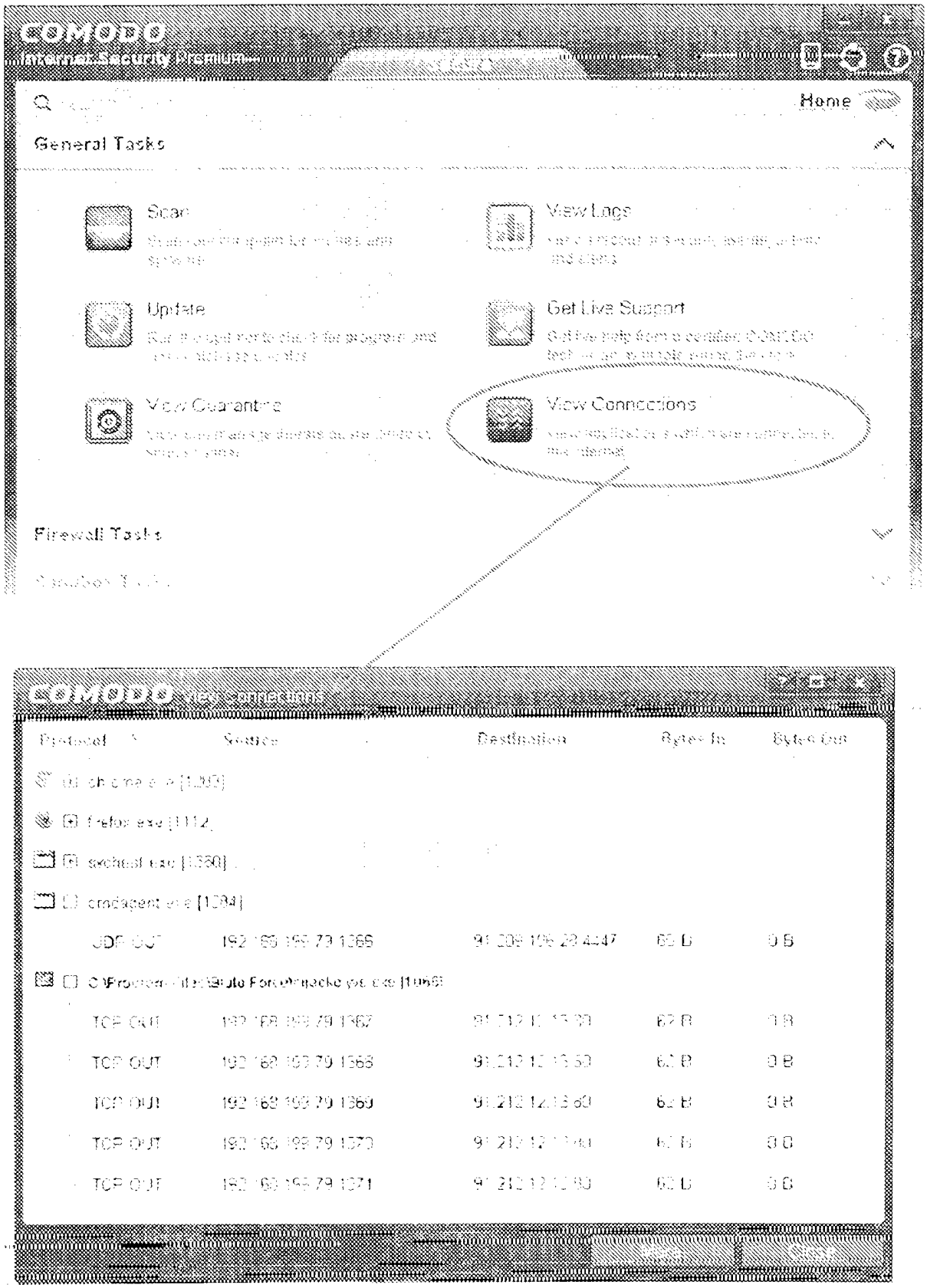

GeekBuddy technicians can help solve most computer issues that you are experiencing. Do you need help to get rid of a particularly nasty virus? Has your computer slowed down to a crawl for no apparent reason? Are you having trouble setting up that wireless router you just bought? GeekBuddy techs can 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.



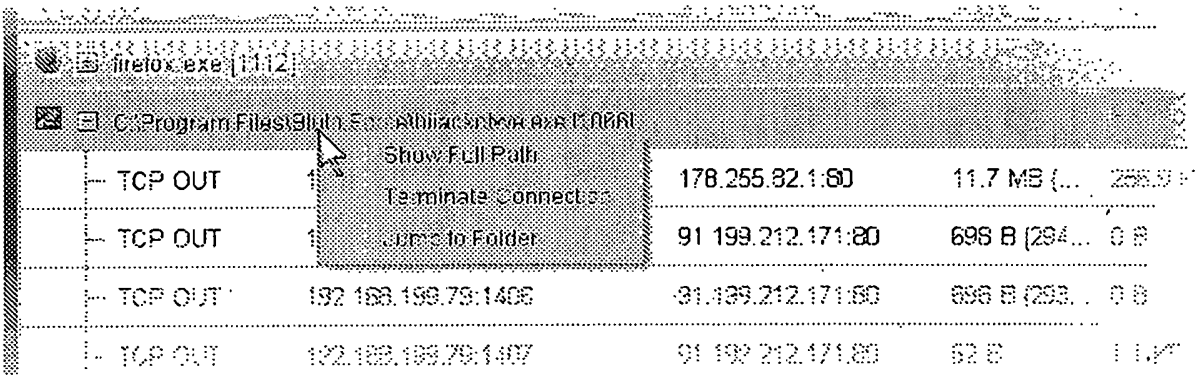

The 'View Connections' interface displays a list of all the currently active Internet connections by initiated by various applications as a Tree structure.

**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.



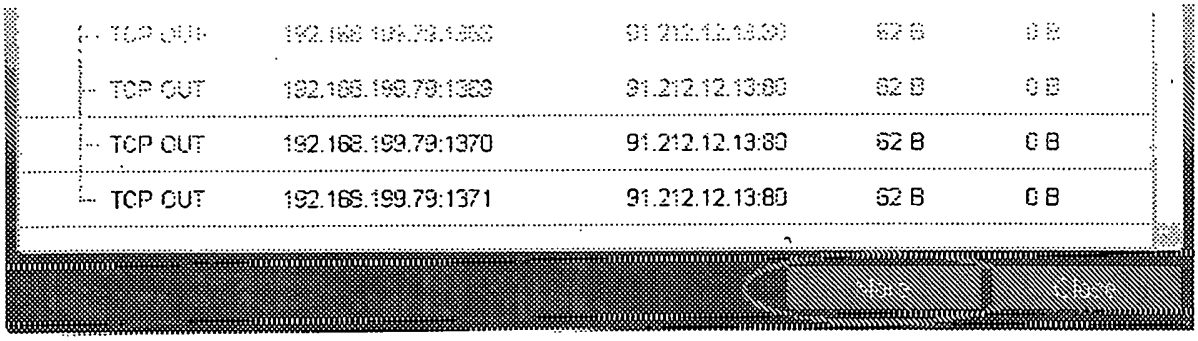

- If you wish to view the full path of the application, right click on the application name and select 'Show Full Path'.
- If you wish to terminate a connection belonging to an application, right click on the specific connection and click 'Terminate Connection'.
- If you wish to open the folder containing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

Identify and Kill Unsafe Network Connections

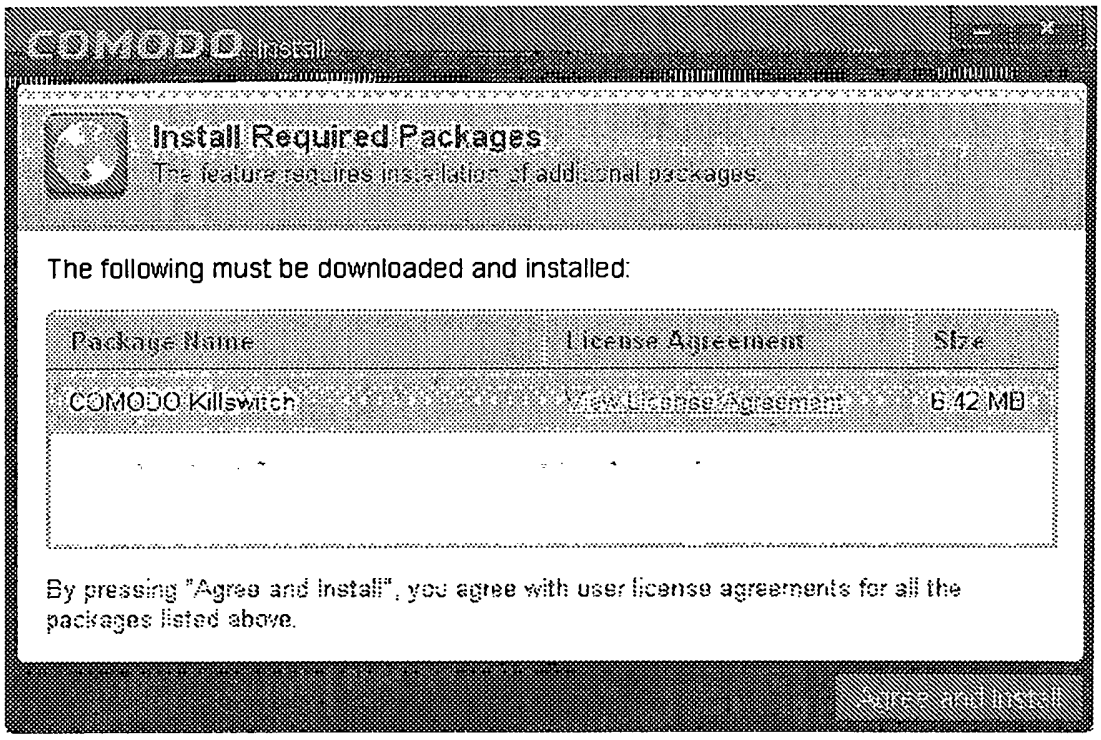
KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate unsafe processes and network connections that are running on their computer. Apart from offering unparalleled insight and control over computer processes and connections, KillSwitch provides 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.

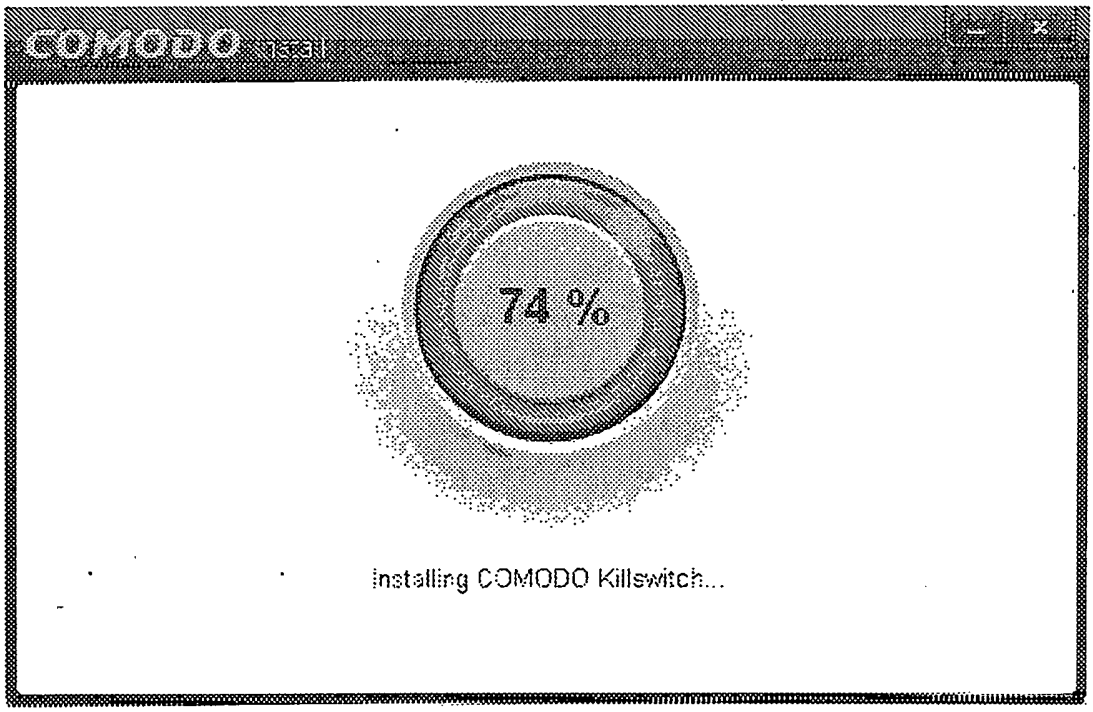
Comodo KillSwitch can be directly accessed from the 'View Connections' by clicking the 'More' button.



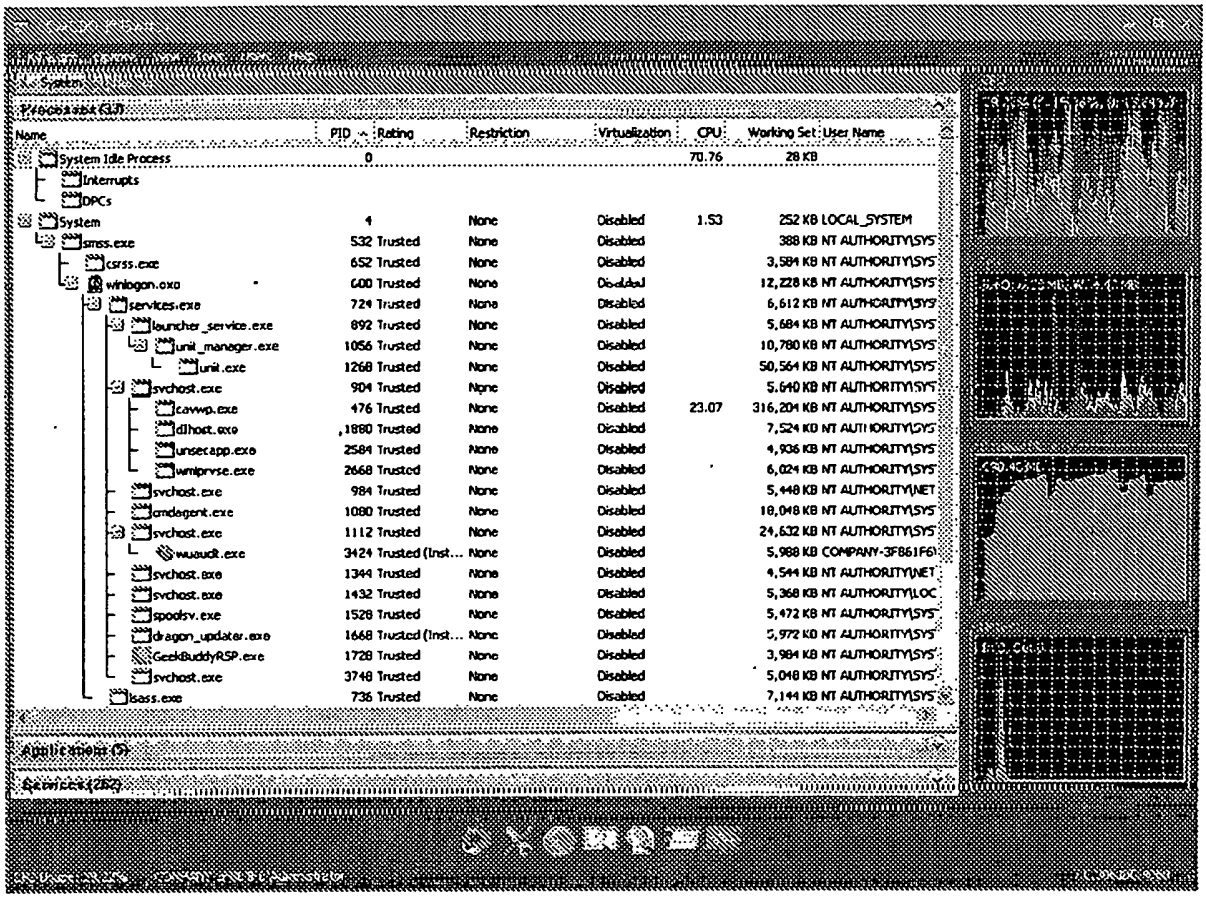

If Comodo KillSwitch is already installed in your computer, clicking 'More' will open the application. If not, CIS will download and install Comodo Killswitch. Once installed, clicking this button in future will open the Killswitch interface.




- 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-118-1-328-3577-Viewing-and-Handling-Network-Connections-and-Usage.html.
- The complete user guide for Comodo KillSwitch is available at http://help.comodo.com/topic-118-1-328-3518-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:

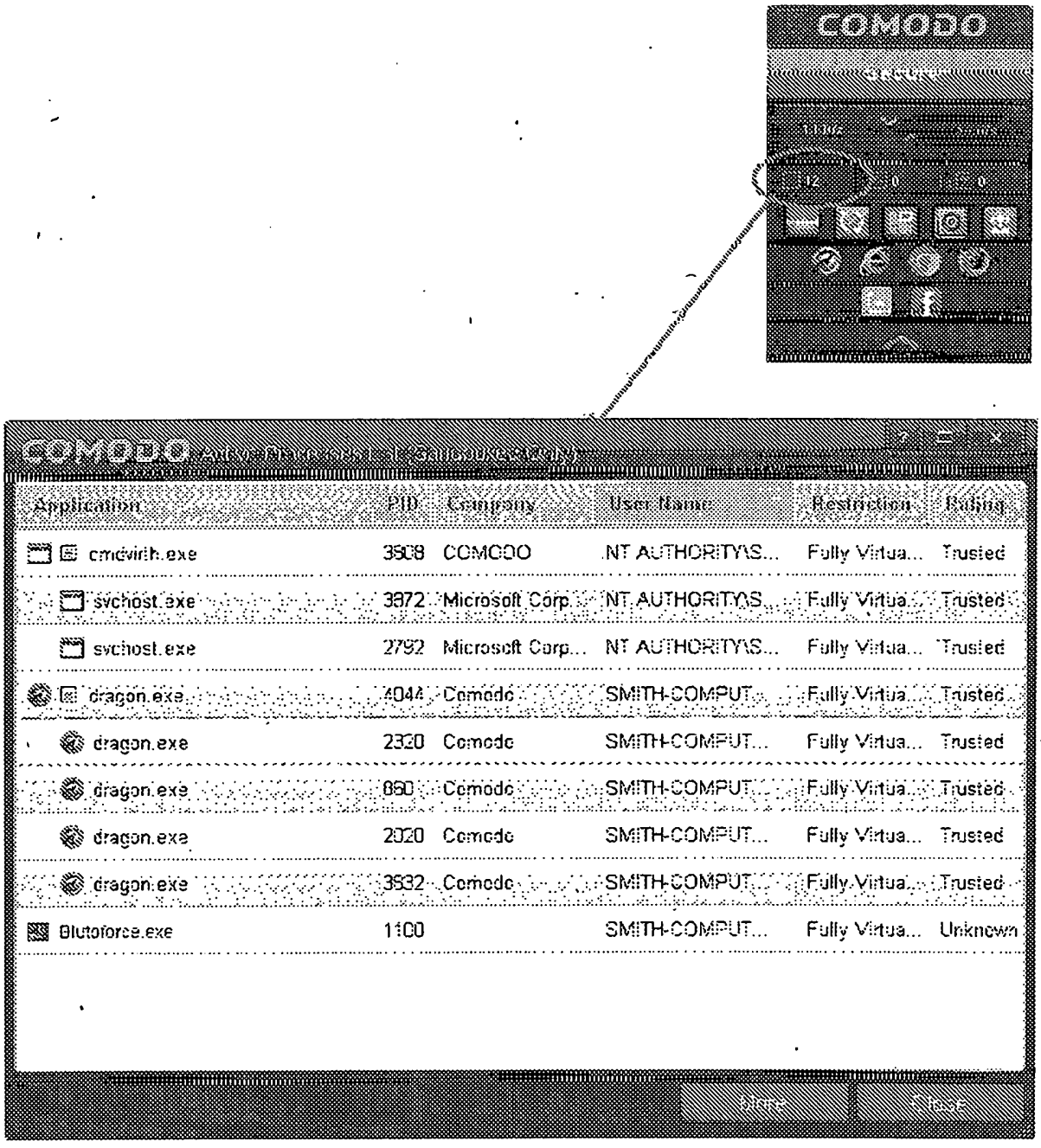
- Auto-Sandbox - Unrecognized applications are run inside the auto sandbox with access restriction as selected in the 'Auto-sandbox unknown applications as' drop down in Behavior Blocker.
- Run Virtual - Applications that are selected and run in Sandbox. Refer to 'Run an Application in the Sandbox' for 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.

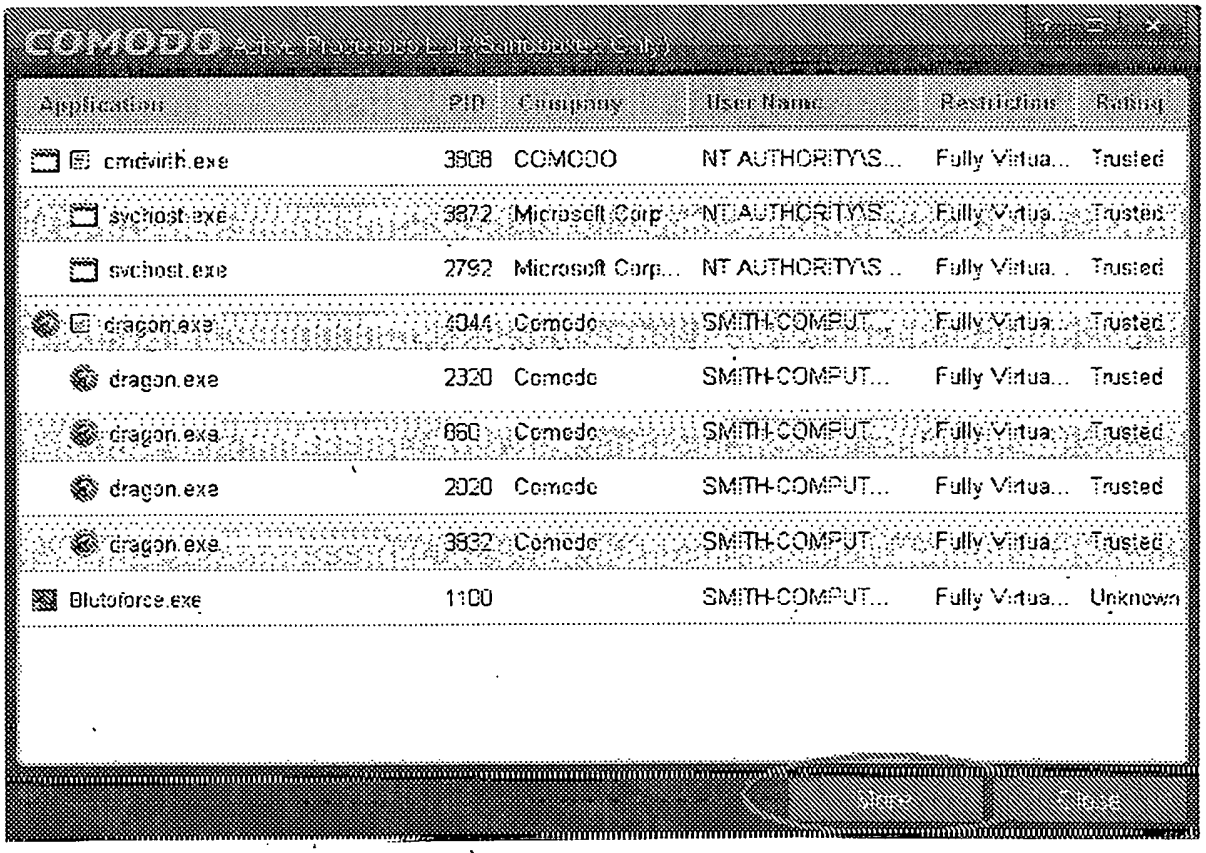
**Column Descriptions**

- 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.



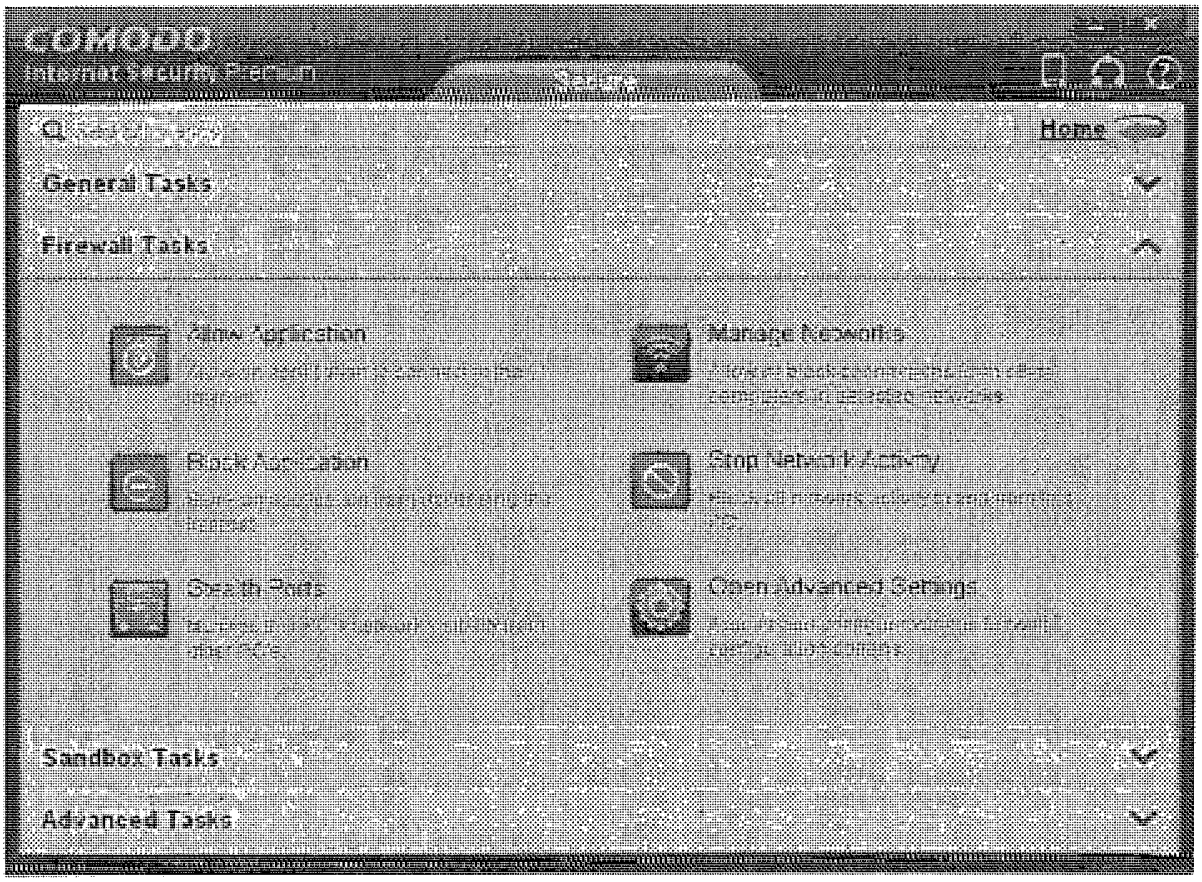
If KillSwitch is not yet installed, clicking this button will prompt you to download the application. Refer to the section Identify and Kill Unsafe Processes for more details.

# 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:

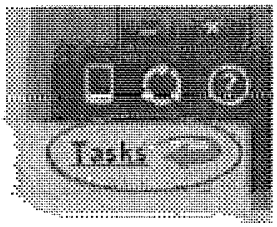
- Allow or block Internet access to applications selectively
- Stealth your computer ports
- Manage network connections
- Stop all network activity
- Advanced firewall settings

# 3.1. Allow or Block Internet Access to Applications Selectively

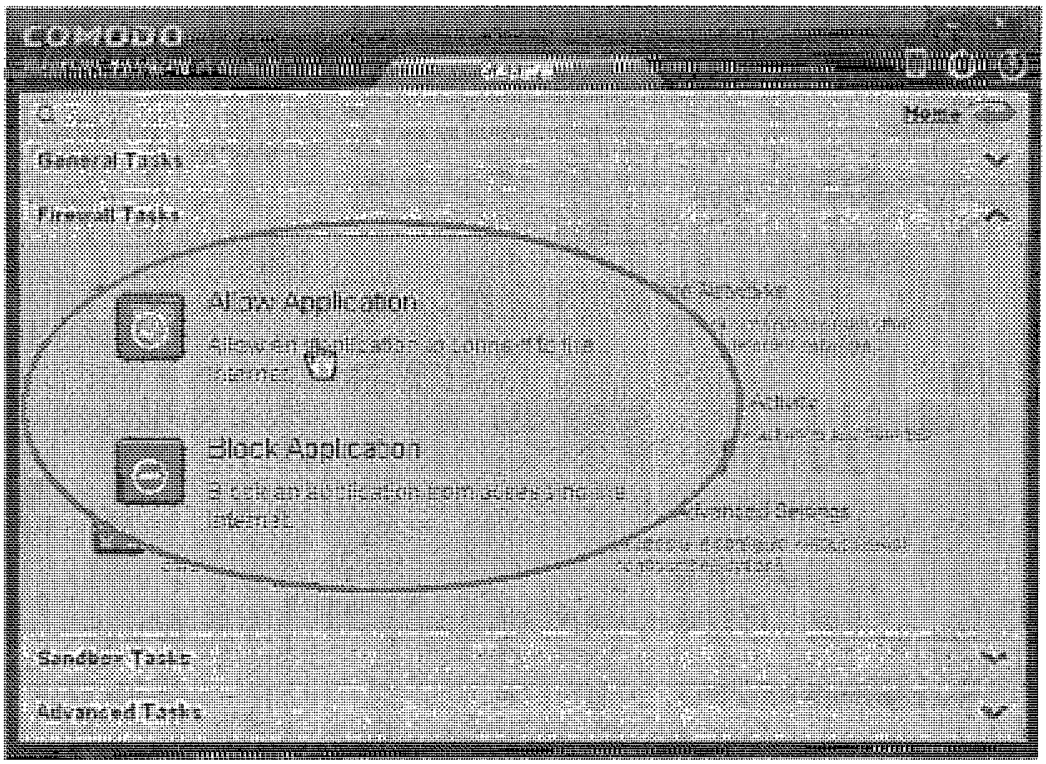
The Firewall Tasks interface allows you to selectively allow or block certain applications from accessing the Internet. These shortcuts represent a convenient way to create an automatic 'Allow Requests' rule or 'Block Requests' rule for individual applications - meaning that inbound and outbound connections 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.

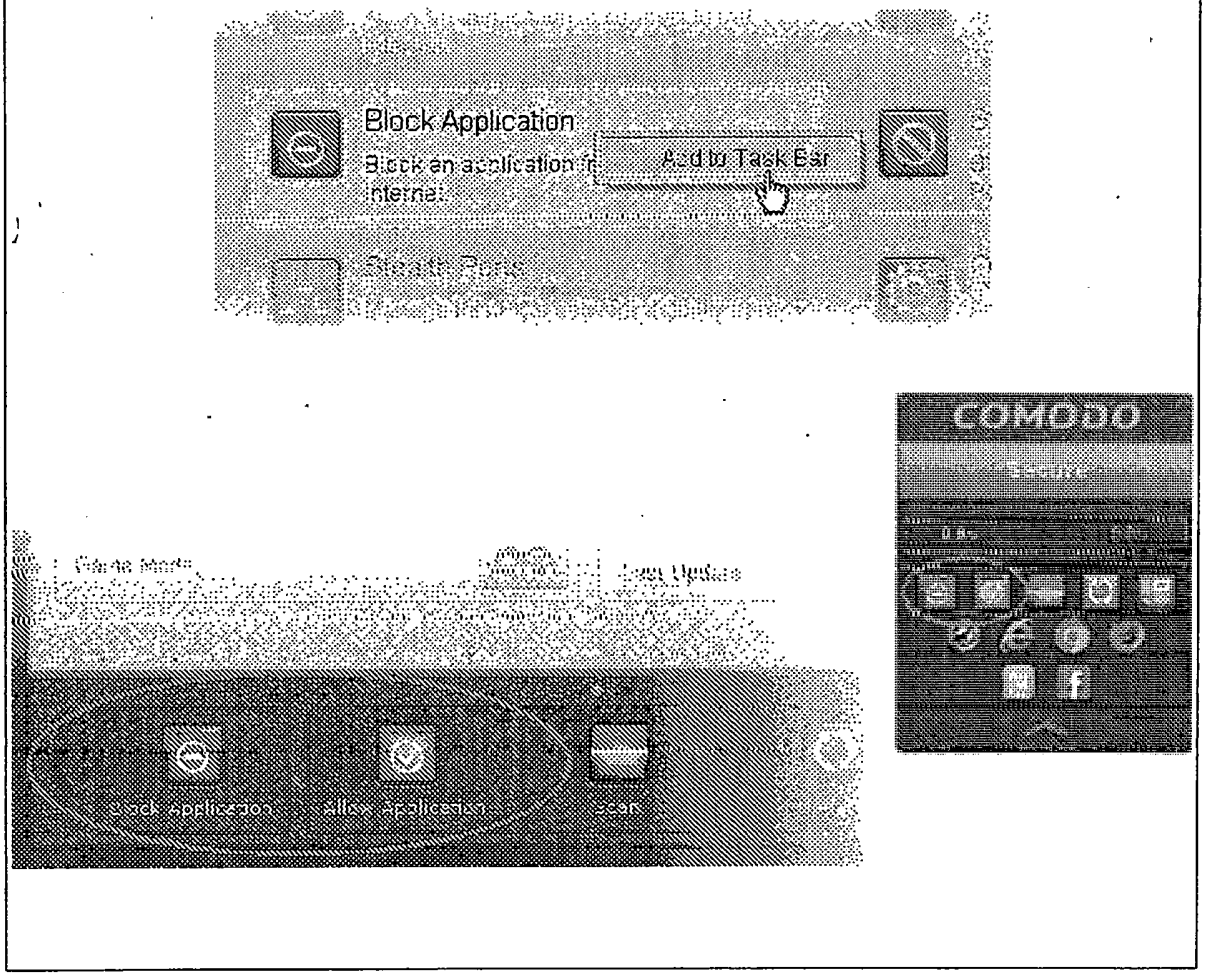
To block an application's Internet access rights

- 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:



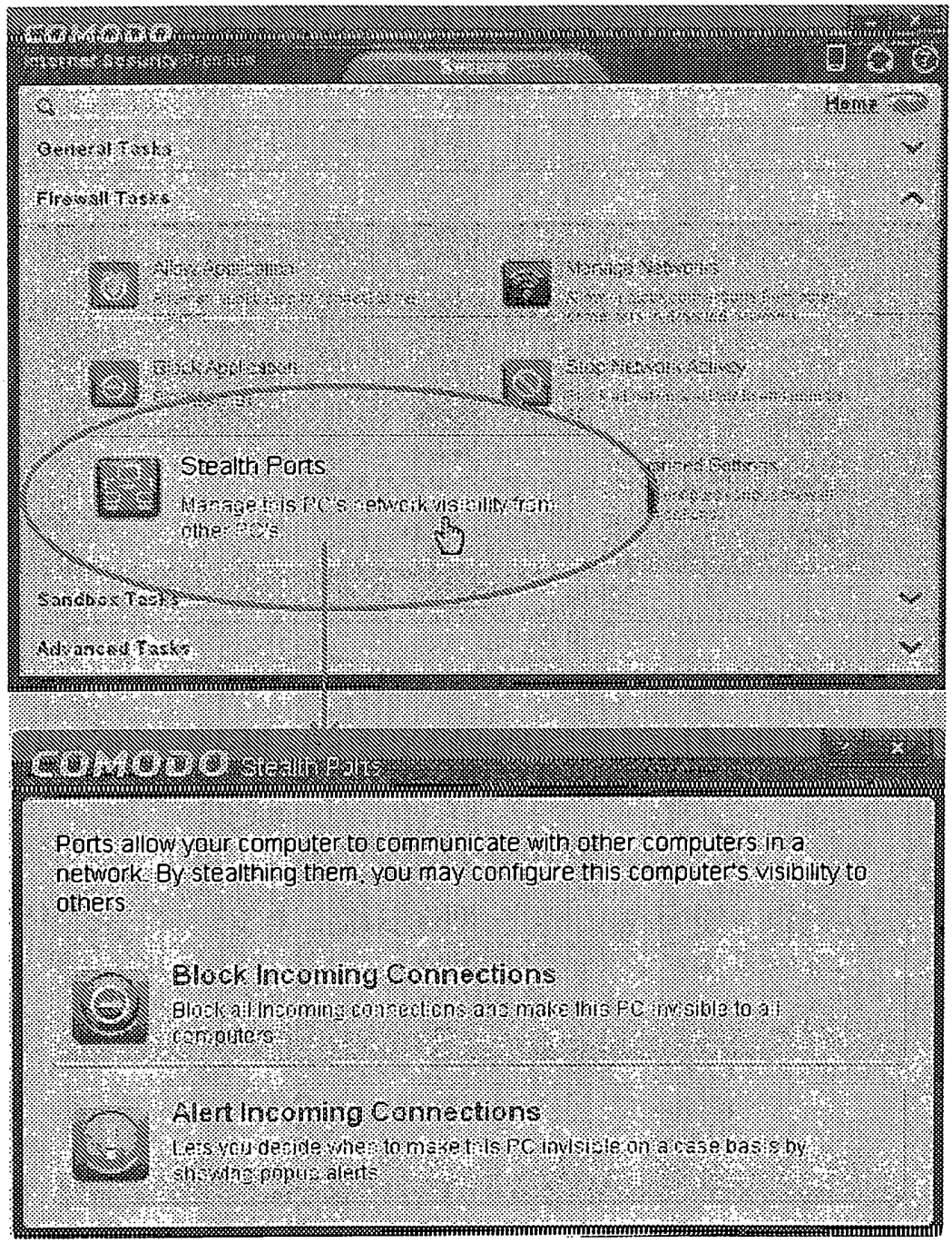

## 3.2. Stealth your Computer Ports

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

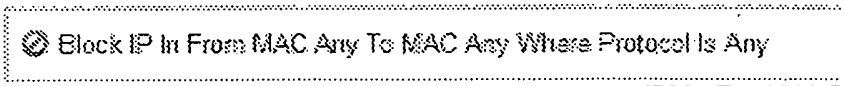



You have two options to choose from:

**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**



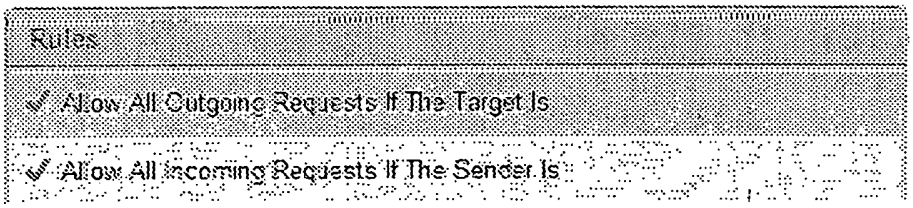
If you would like more information on the meaning and construction of rules, please click here.

**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**

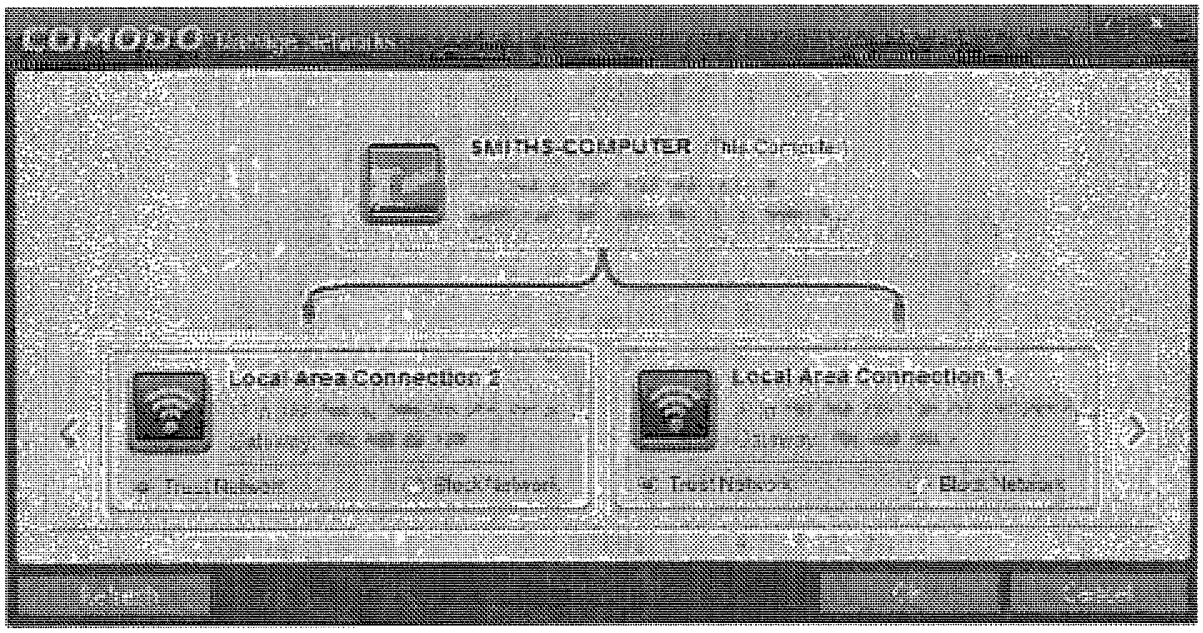



If you would like more information on the meaning and construction of rules, please click here.

# 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.

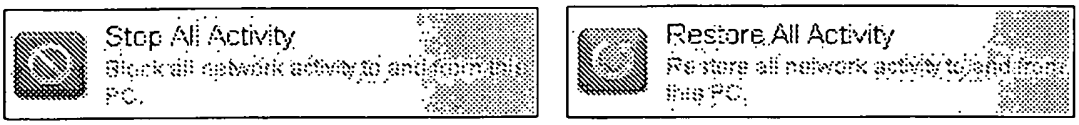
- You can choose to trust or block a network by selecting the appropriate radio button under the network in question. You will not be able to receive any inbound or outbound traffic from blocked networks.
- Use the handles (< >) to scroll through all available networks or computers
- Use the refresh 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

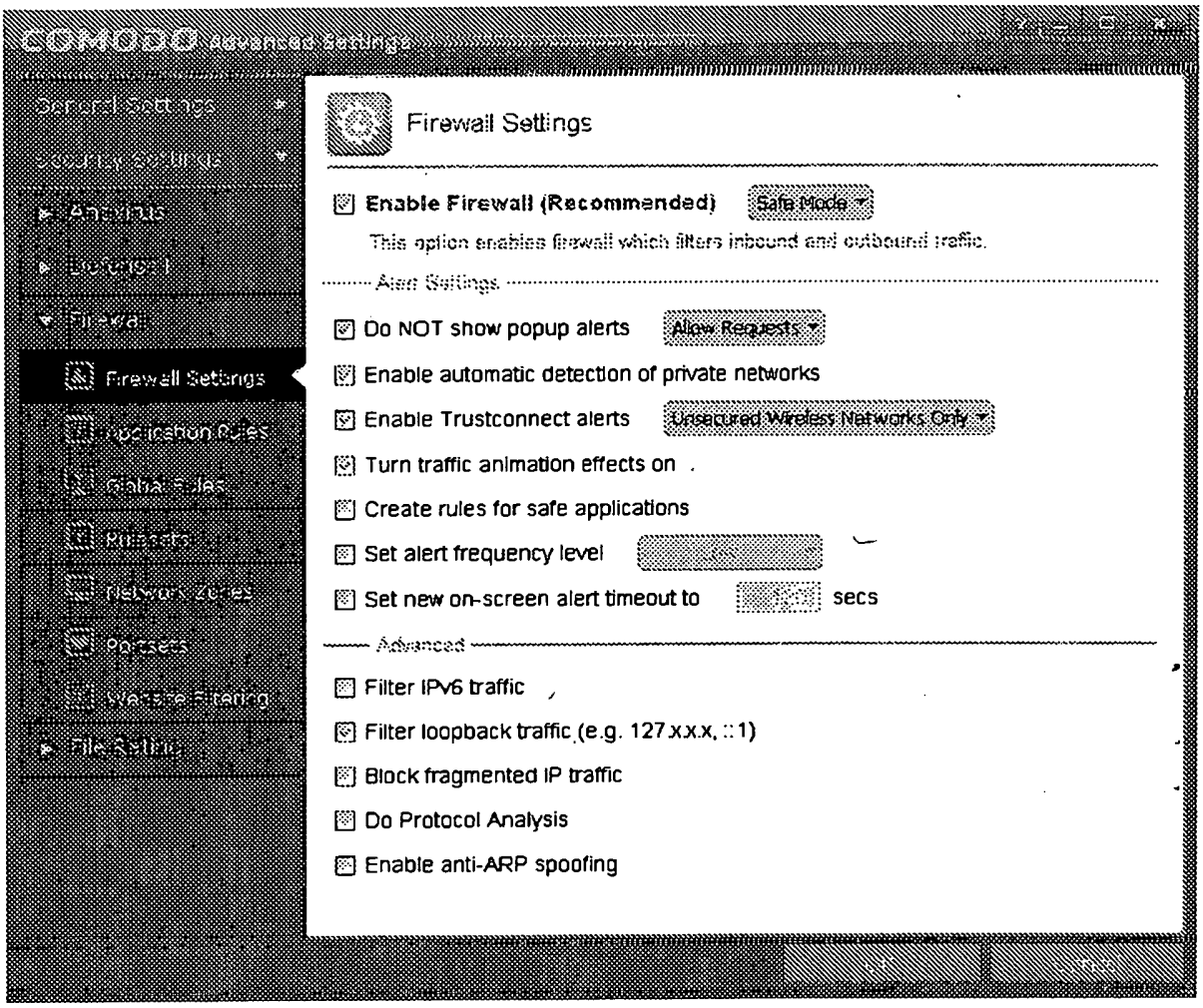
As the name suggests, the 'Stop all network activity' button instructs the firewall to immediately cut-off all inbound/outbound communication between your computer and all available networks (including the Internet). Connections will remained closed until you re-enable them by clicking the button a second 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':



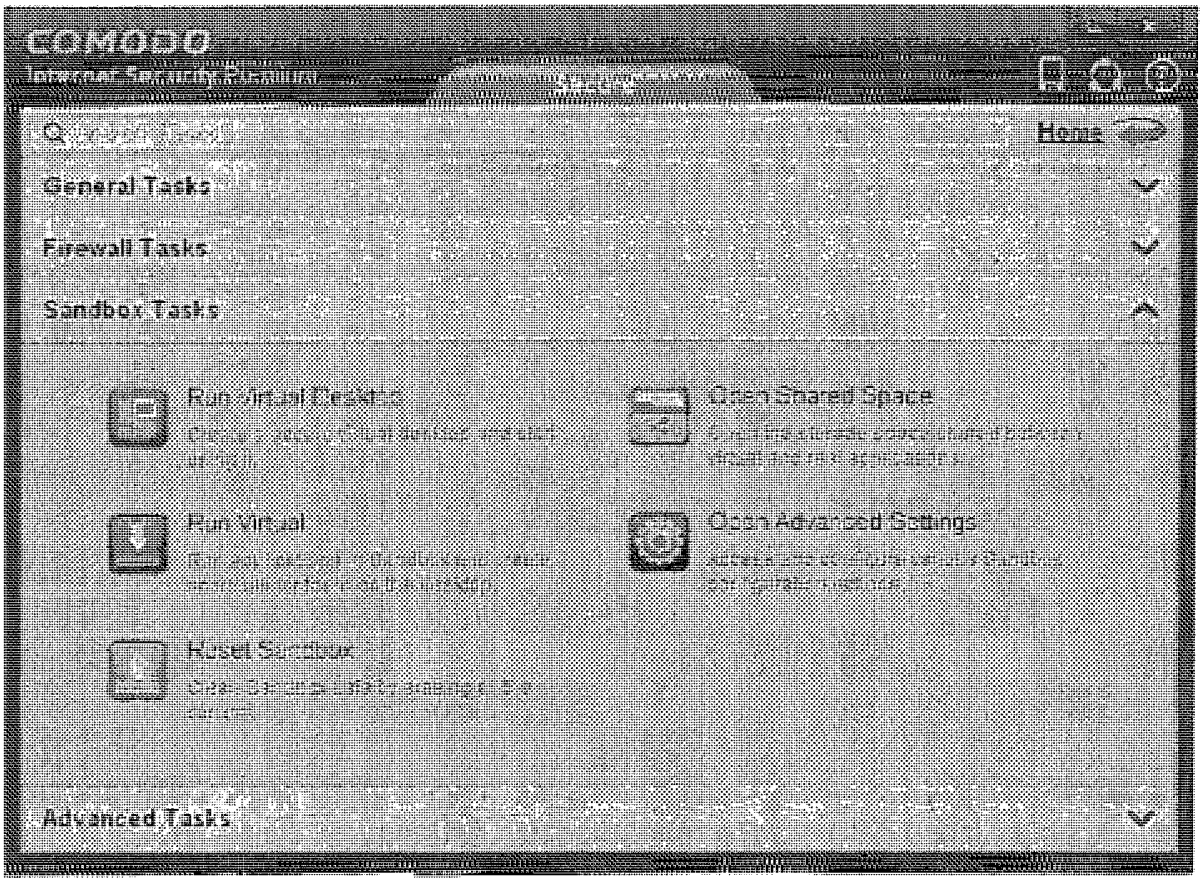

The interface is divided into six main sections - Firewall Settings, Application Rules, Global Rules, Rulesets, Network Zones and Portsets. Click the links below to jump to more details on each section:

- 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.



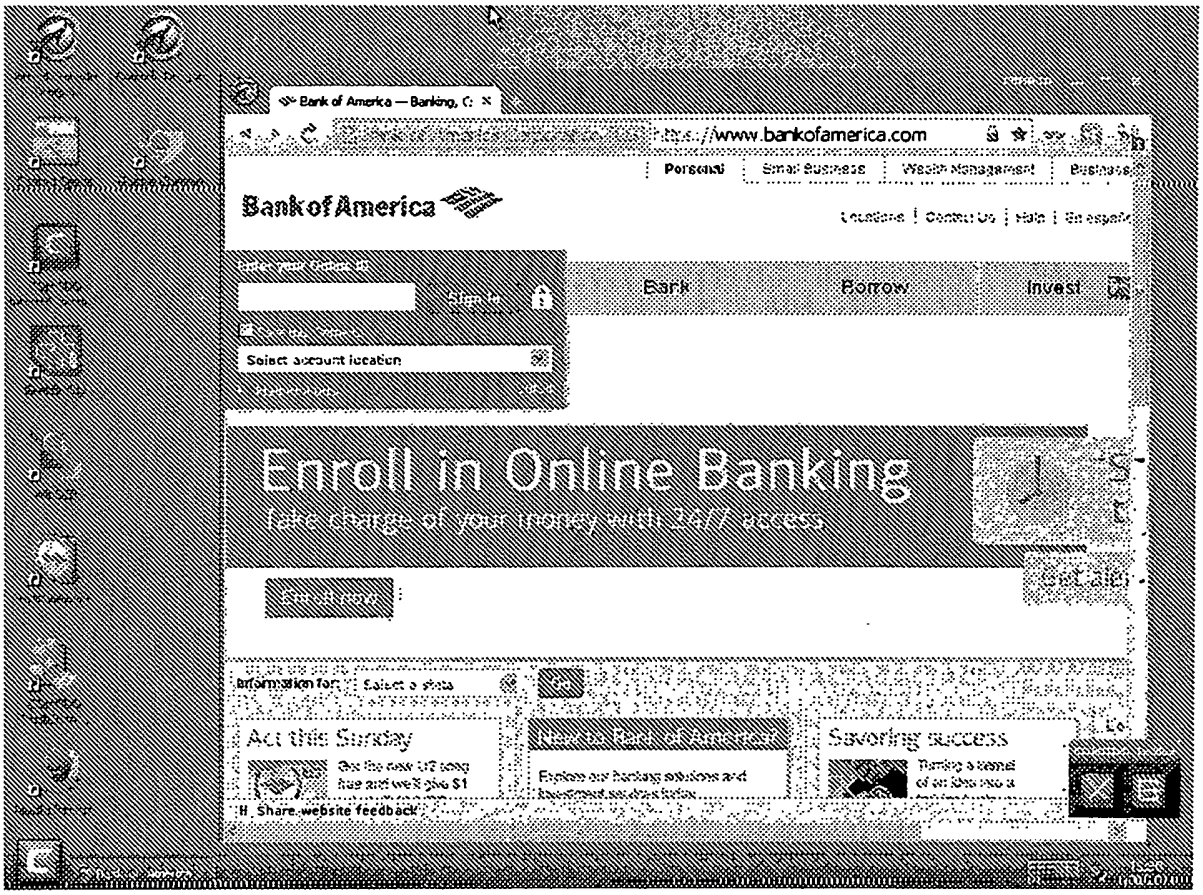

Note: The sandbox referred to here is a full environment and is distinct to the 'auto-sandbox' configured under Behavior Blocker. Users can, however, enable 'Full Virtualization' of auto-sandboxed files in the Behavior Blocker settings.

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:

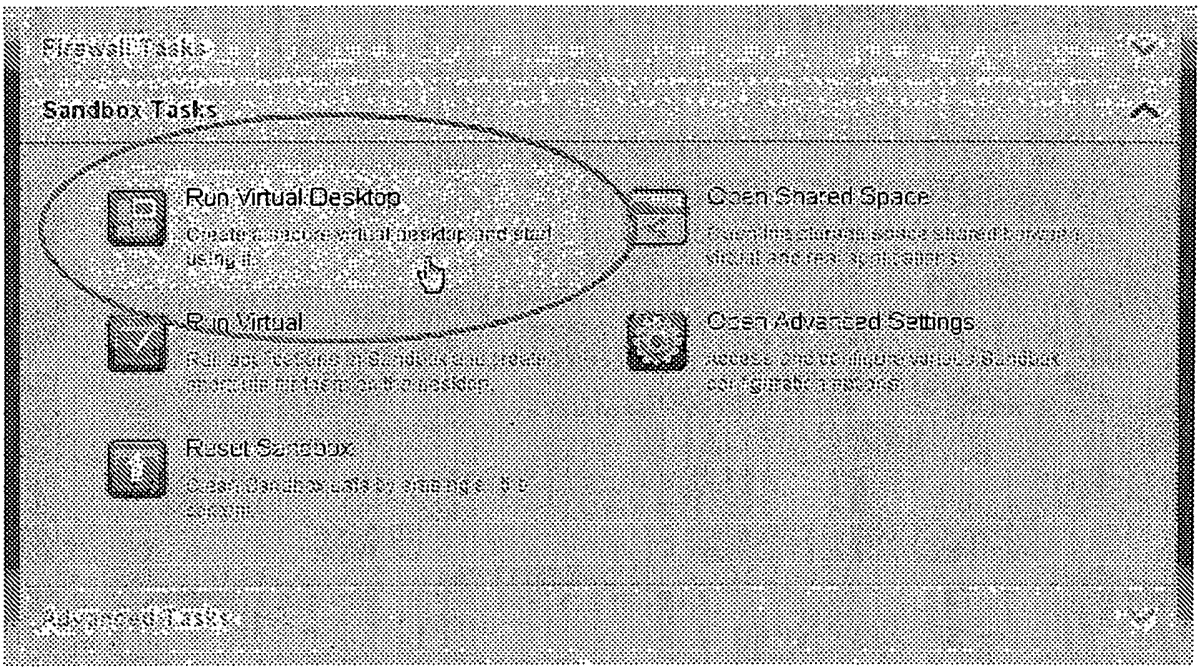
- Starting the Virtual Desktop
- The Main Interface

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

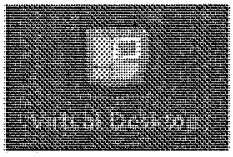
## 4.1.1. Starting the Virtual Desktop

The Virtual Desktop can be started by:

- Clicking Tasks > Sandbox Tasks > Run Virtual Desktop

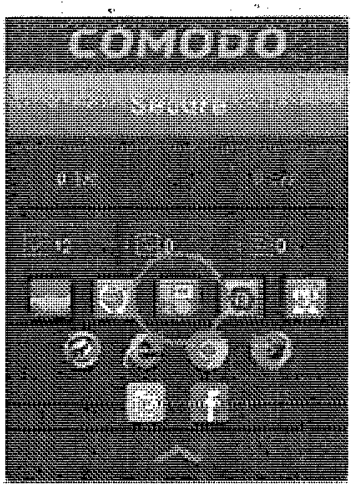



OR

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

  OR

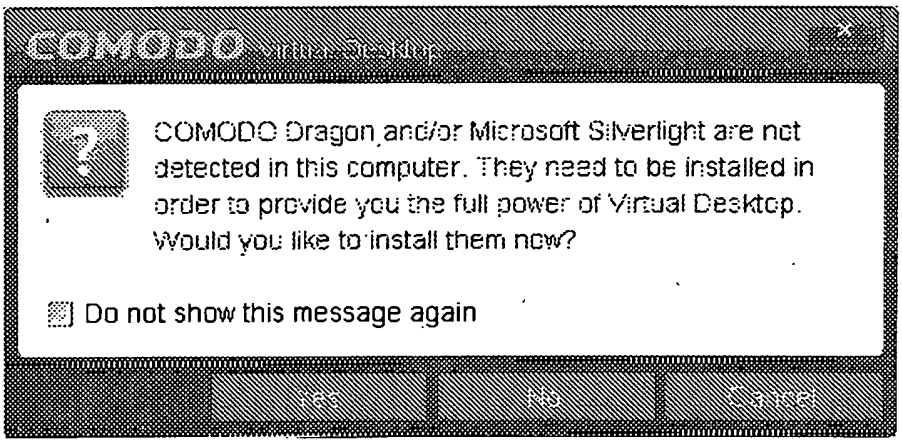
- By clicking the Virtual Desktop shortcut button from the CIS widget




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

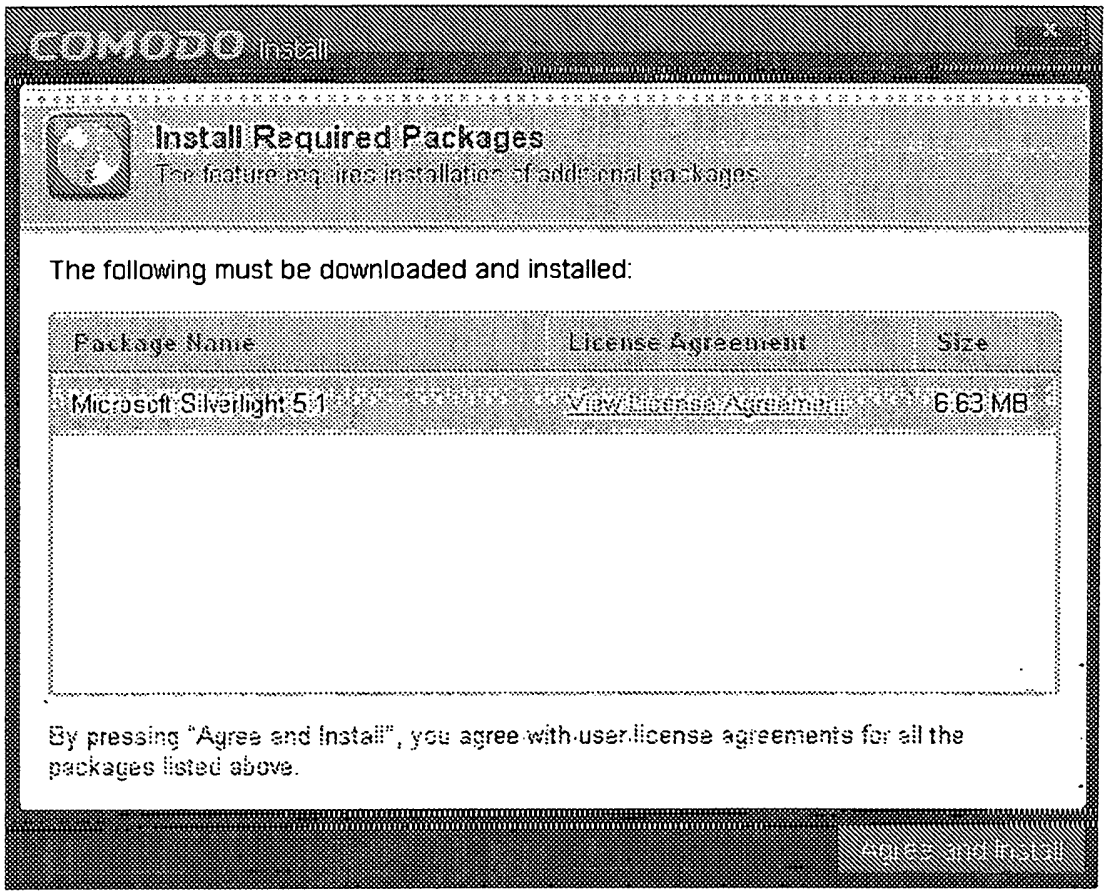
- Comodo Dragon Browser
- Microsoft Silverlight

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

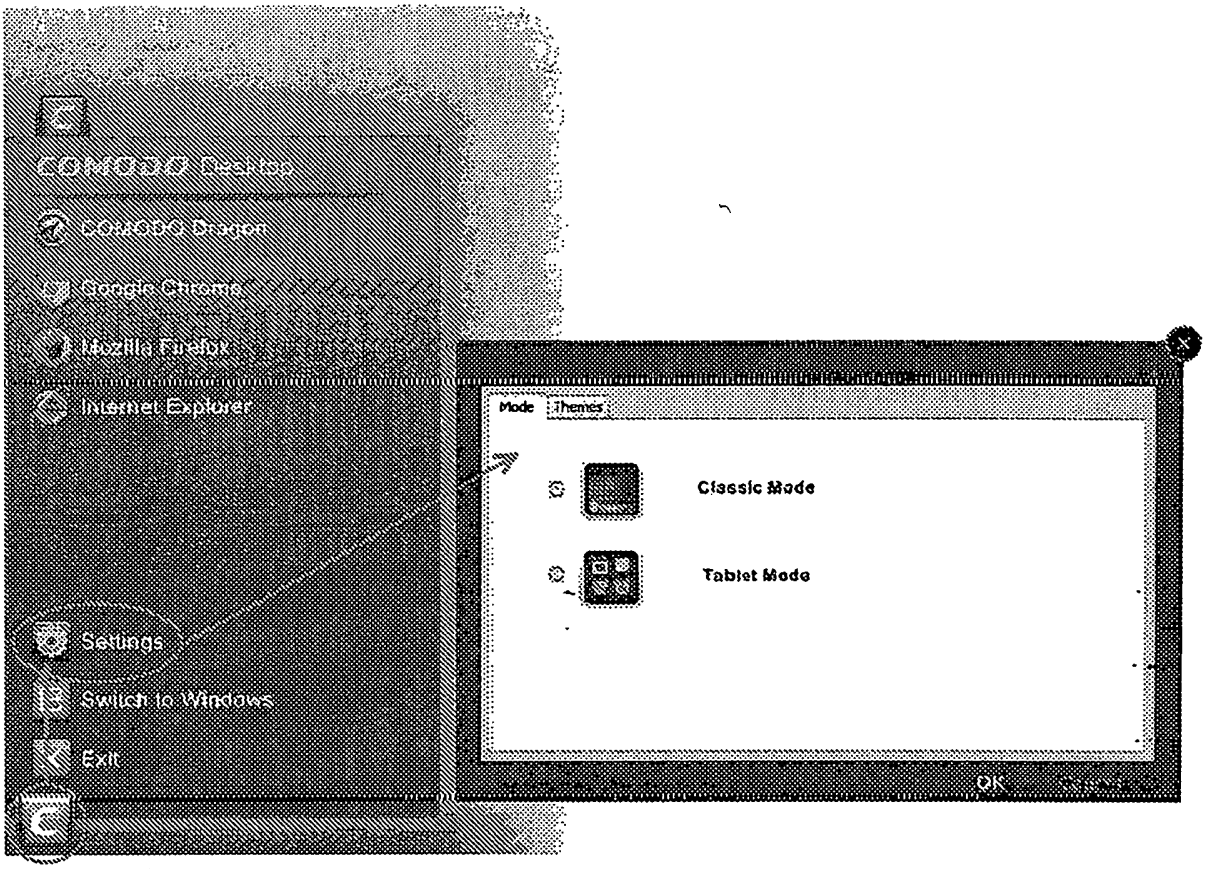
The software package(s) will be downloaded and installed automatically.

## 4.1.2. The Main Interface

The Virtual Desktop is presented with two switchable interfaces:

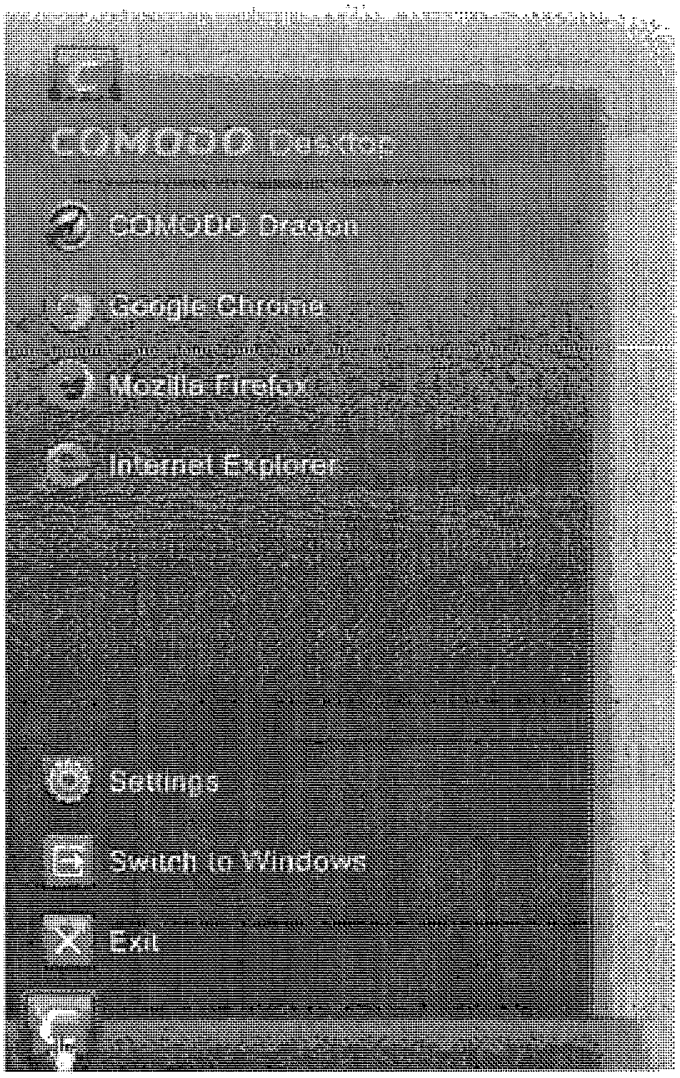
- Classic Windows style Desktop mode
- Tablet mode

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,

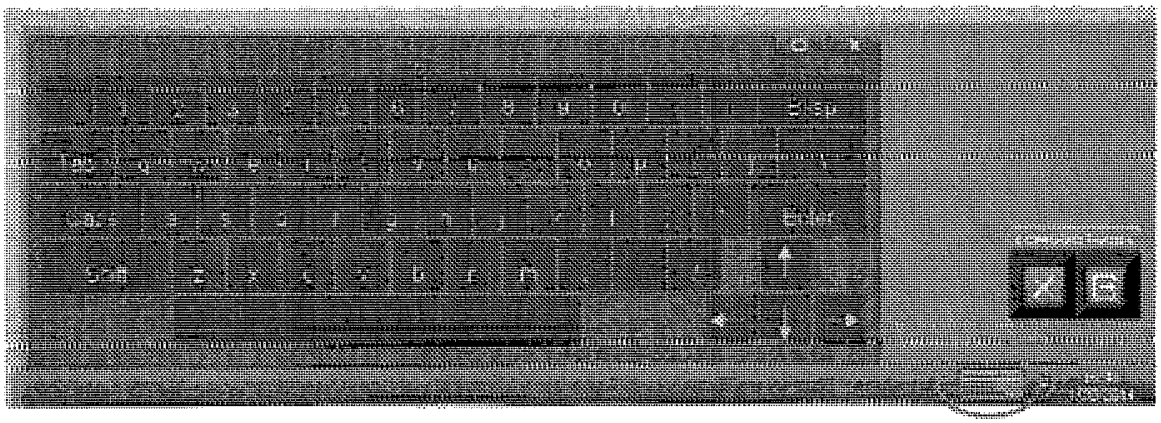
- All items on your real desktop are displayed. Clicking the shortcuts on the Virtual Desktop will run the program or file inside the virtual computer system.
- Clicking the green 'C' button at bottom-left will open a Windows-style 'Start Menu'.



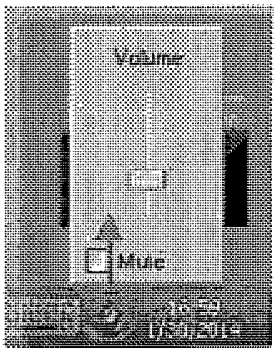

The start menu allows you to:

- 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

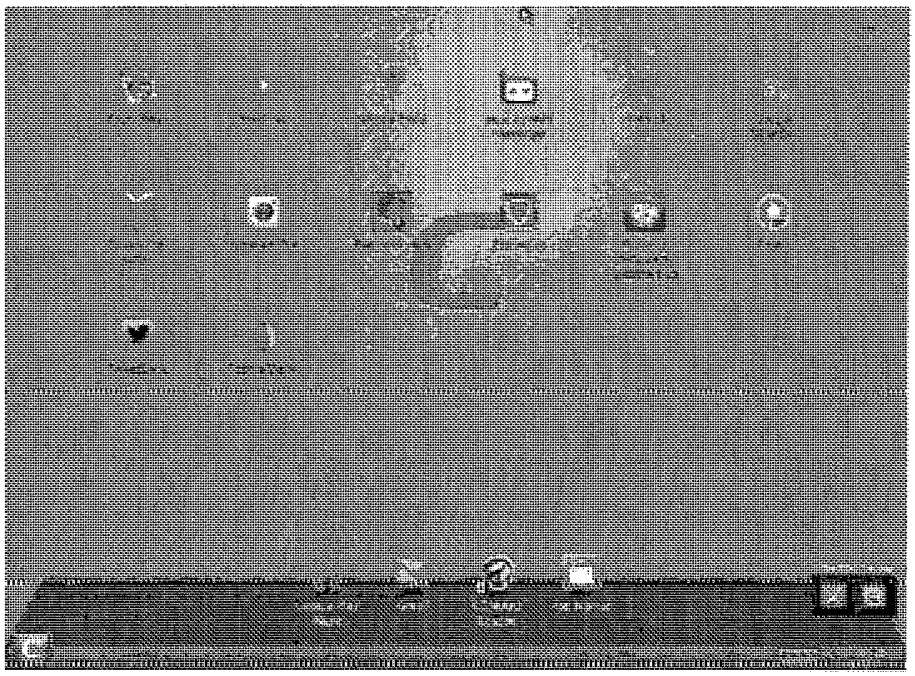
To switch to 'Tablet' mode from 'Classic' mode, click the green 'C'  button at bottom left followed by Settings > Mode and select 'Tablet Mode'.

There are two variations of this mode:

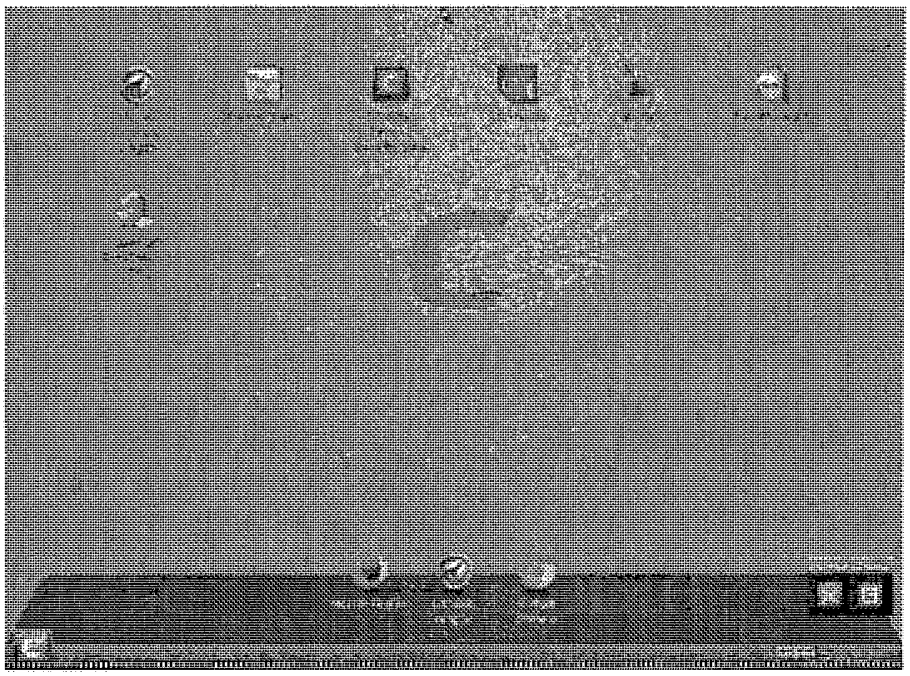
1. Mode A - Pure Tablet device - A touch-screen interface that will be familiar to users of modern smart devices. The home page displays a set of popular apps covering games, social media and networking. You can, of course, install your own apps from the app market.
    - To install your own apps, click 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 |

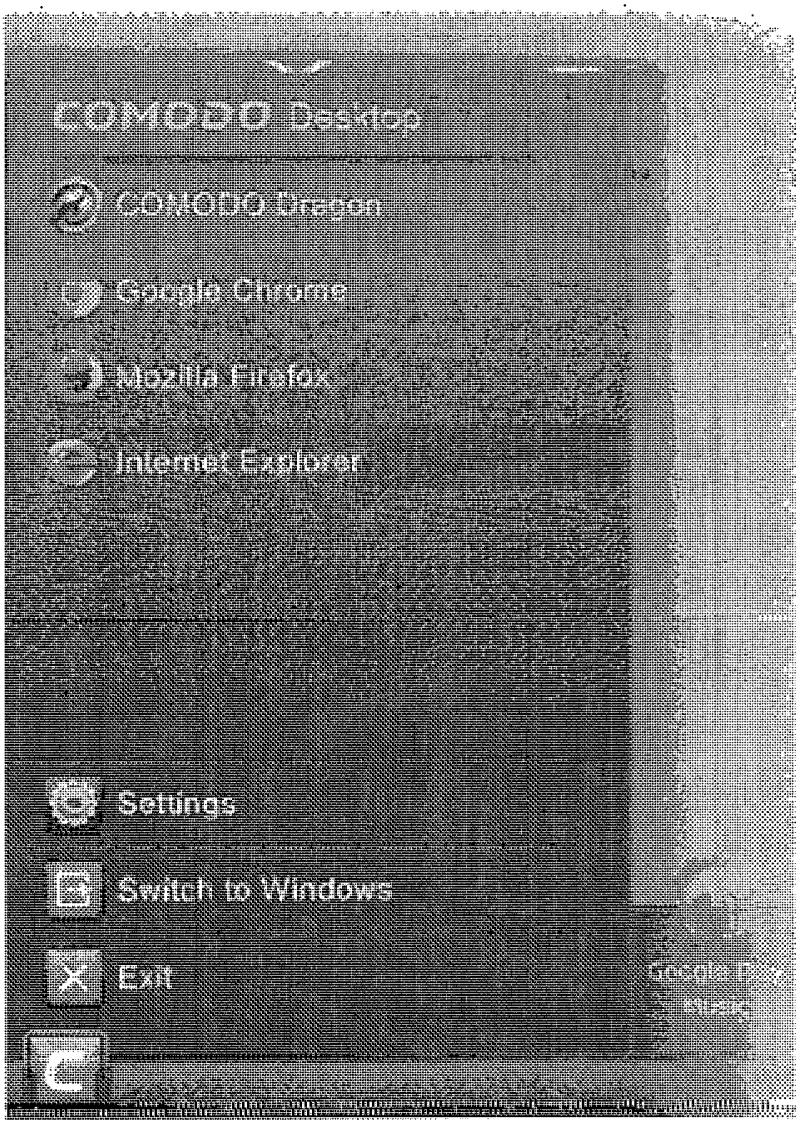
| | | |
|---|---|---|
| No Launch Bar | Browser shortcuts are displayed on the launch bar at the bottom | Browser shortcuts are displayed on the launch bar at the bottom |
| Cannot have multiple home screens | Can have multiple home screens | Can have multiple home screens if you have many shortcuts 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.

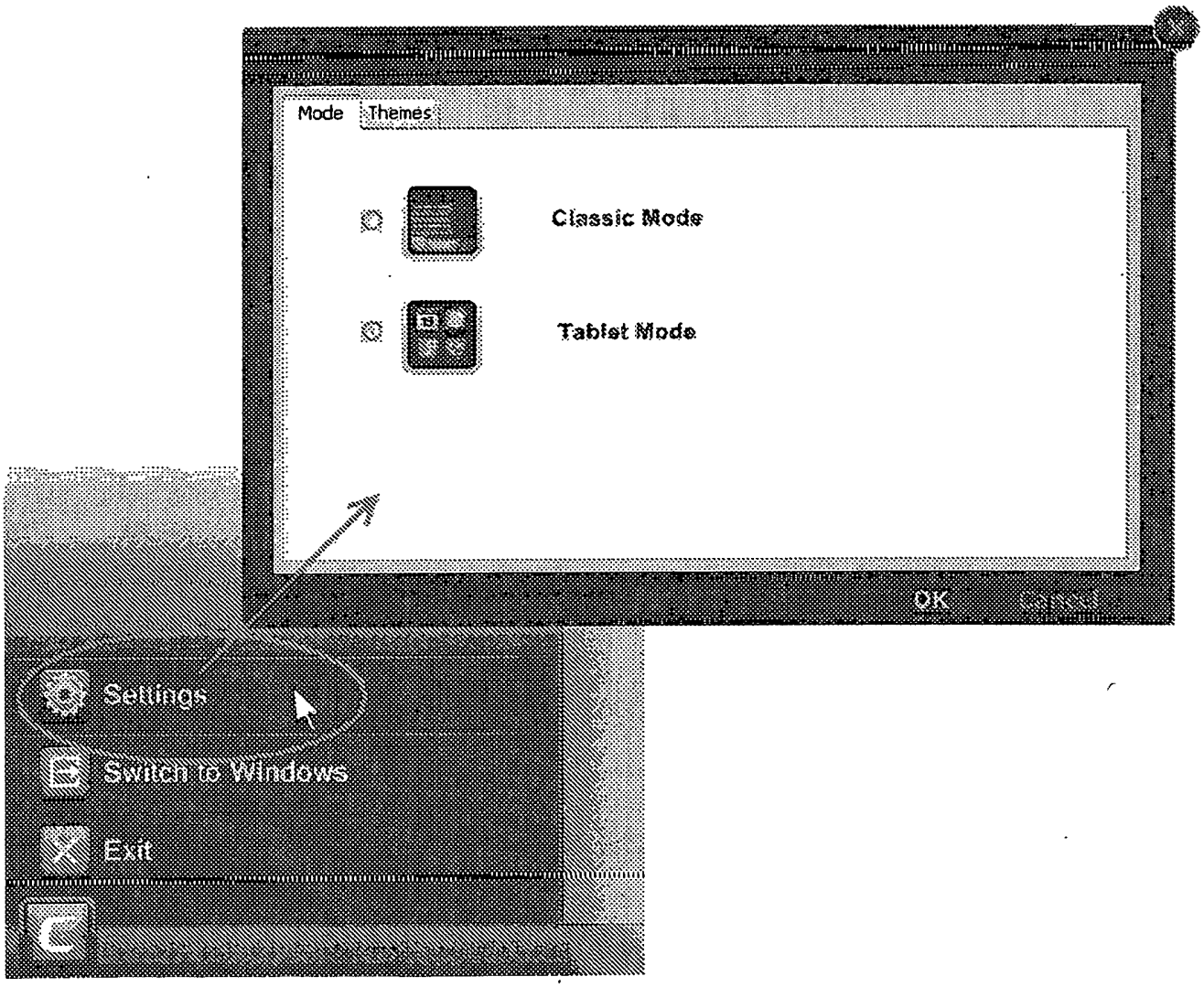
The changes you make to the file will be stored to the file only inside the Virtual Desktop and not in the real computer system.

## 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.



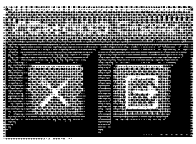
The Settings panel has two tabs:

- **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

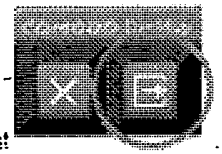
3. Click OK for your settings to take effect

## 4.1.6. Closing the Virtual Desktop

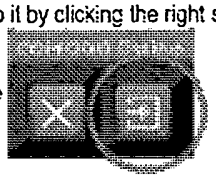
The shortcuts at the bottom right of the Virtual Desktop, allow you to temporarily switch to your real computer system, if you plan to continue using the virtual desktop at a later time, or to fully exit the Virtual Desktop.



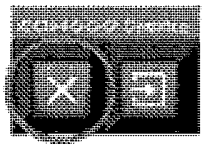
**To temporarily switch to your real Windows system**



- 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.

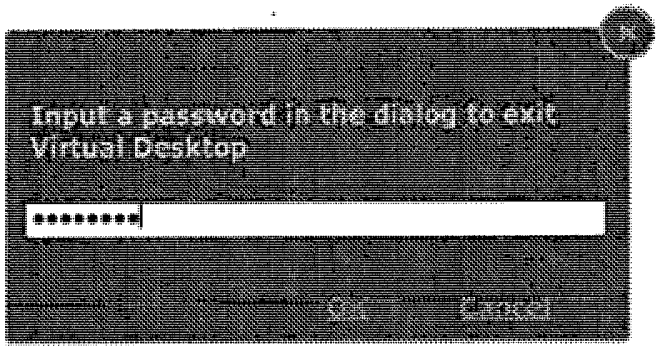
The Virtual Desktop will be temporarily closed. You can quickly return to it by clicking the right switch from the Virtual Desktop shortcut buttons displayed at the bottom right of your Windows Desktop  or by clicking 'Run Virtual Desktop' from the 'Sandbox Tasks' interface.

**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.



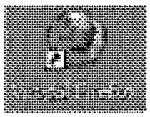

- Enter the password and click OK.

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).

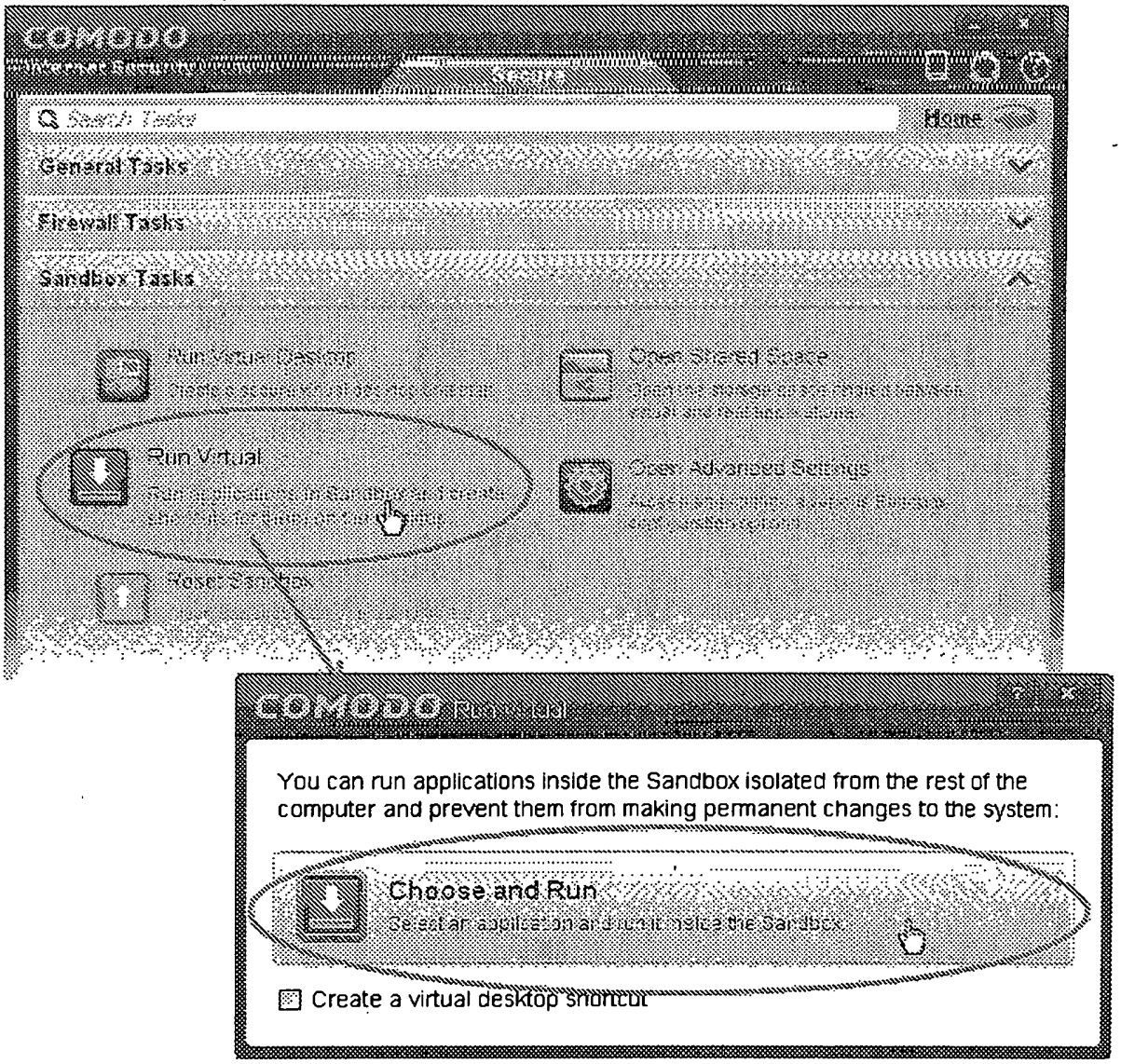
You can also create a desktop shortcut to run the application inside the sandbox on future occasions. The following image shows how a 'virtual' shortcut will appear on your desktop:



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

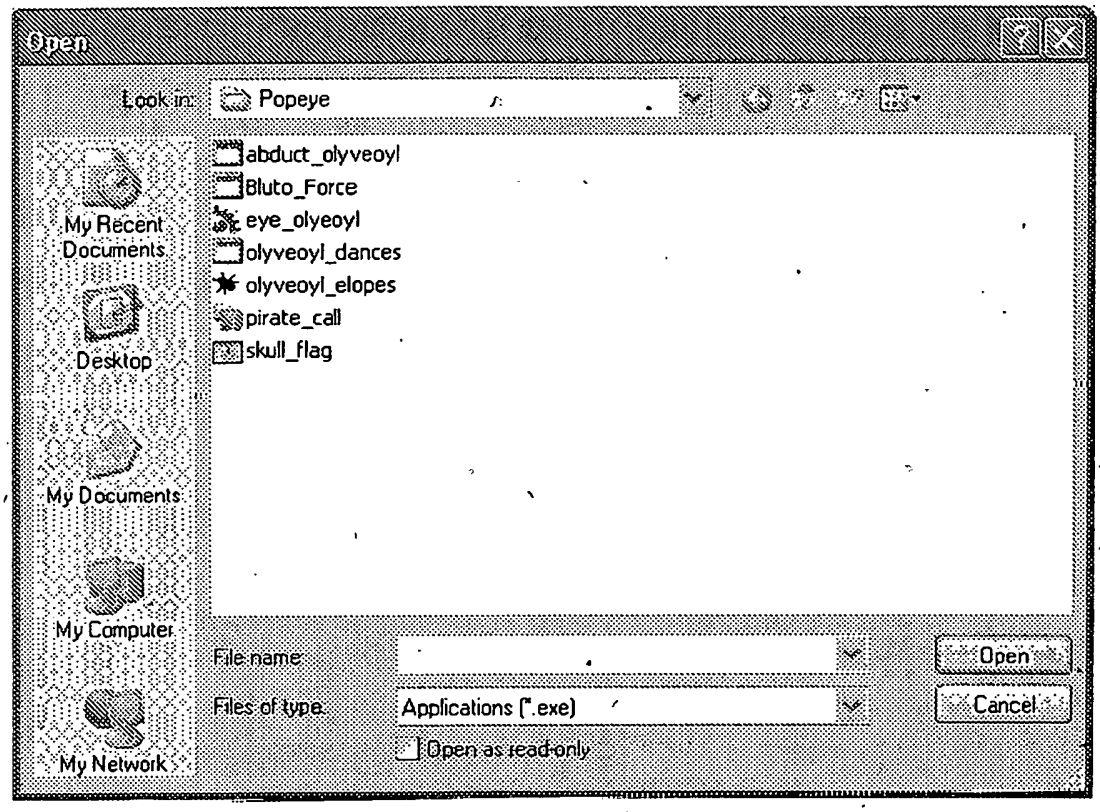
**To run an application in the Sandbox**

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'.



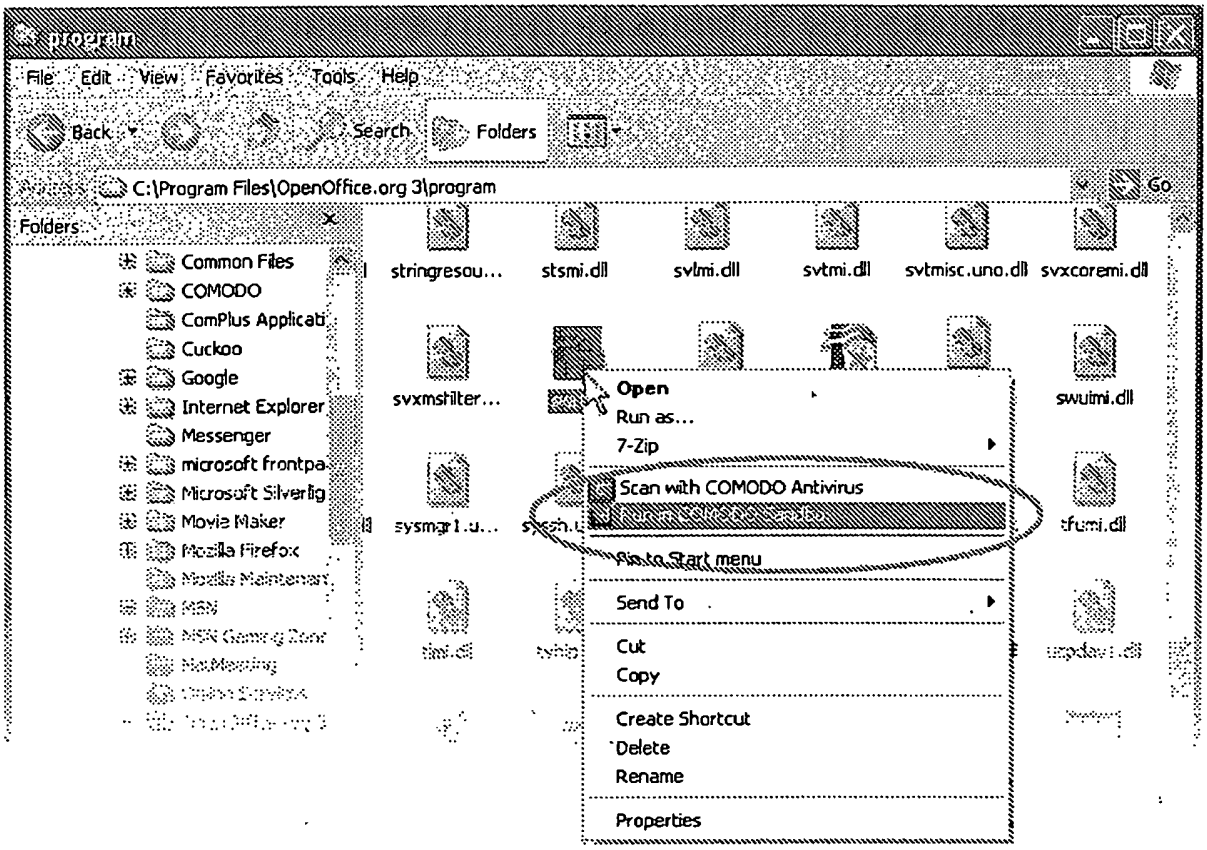

3. Browse to the application and click 'Open'. In the example above, Open Office Writer is chosen.

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.

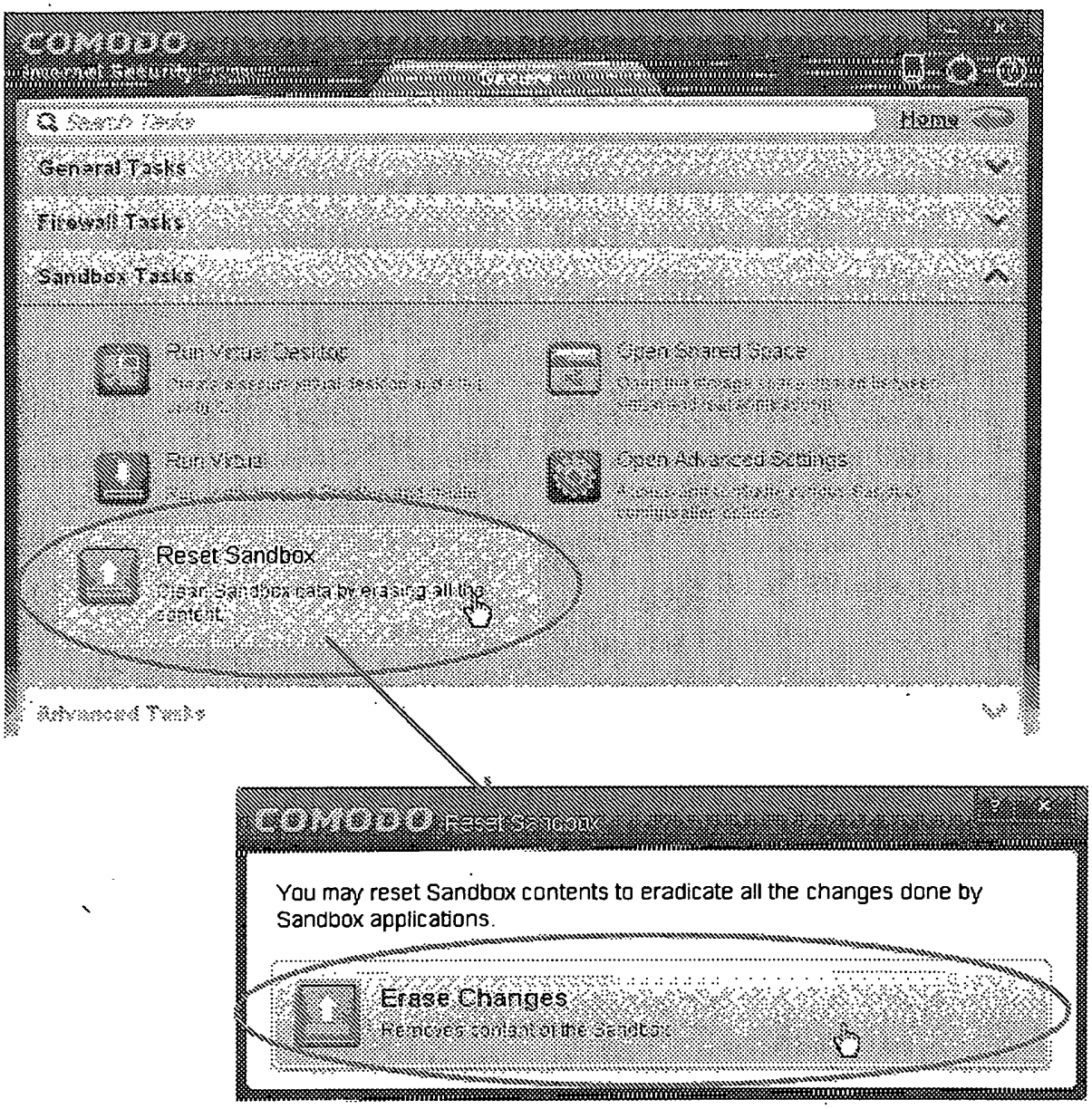
## 4.3. Reset the Sandbox

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.

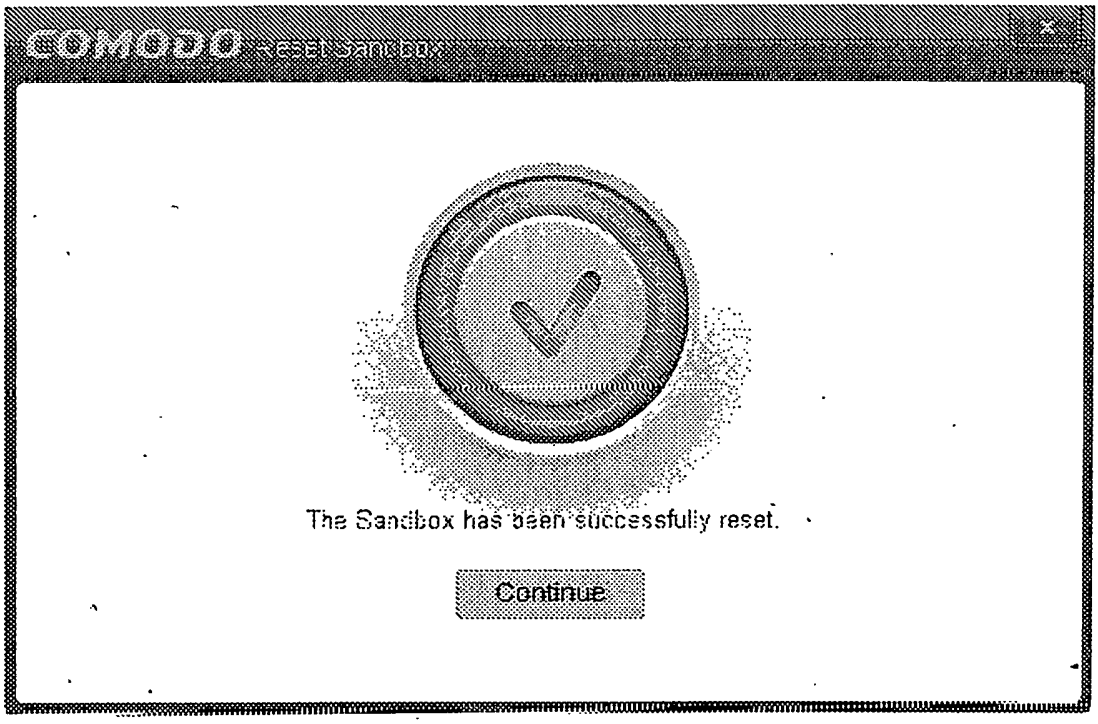
**To clear the sandbox**

- 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.

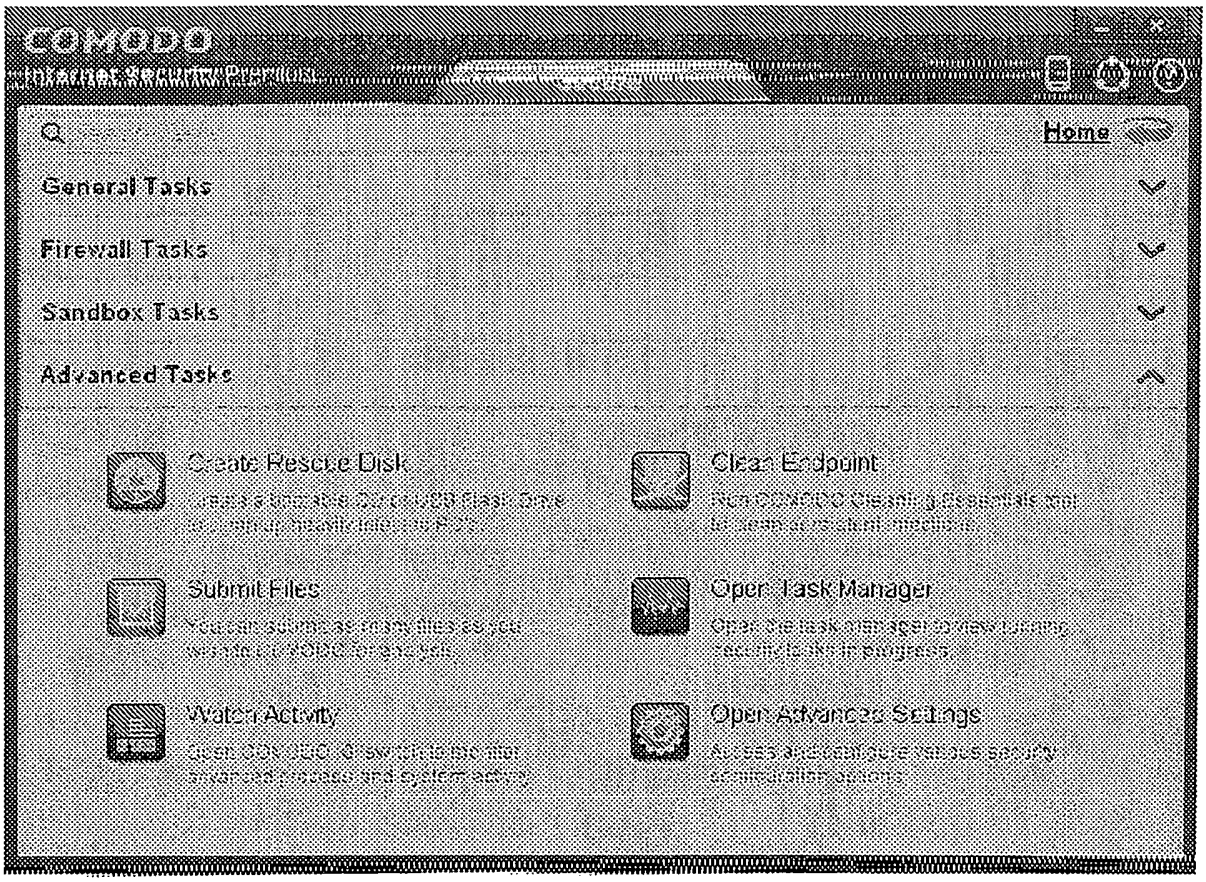



# 5.Advanced Tasks - Introduction

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

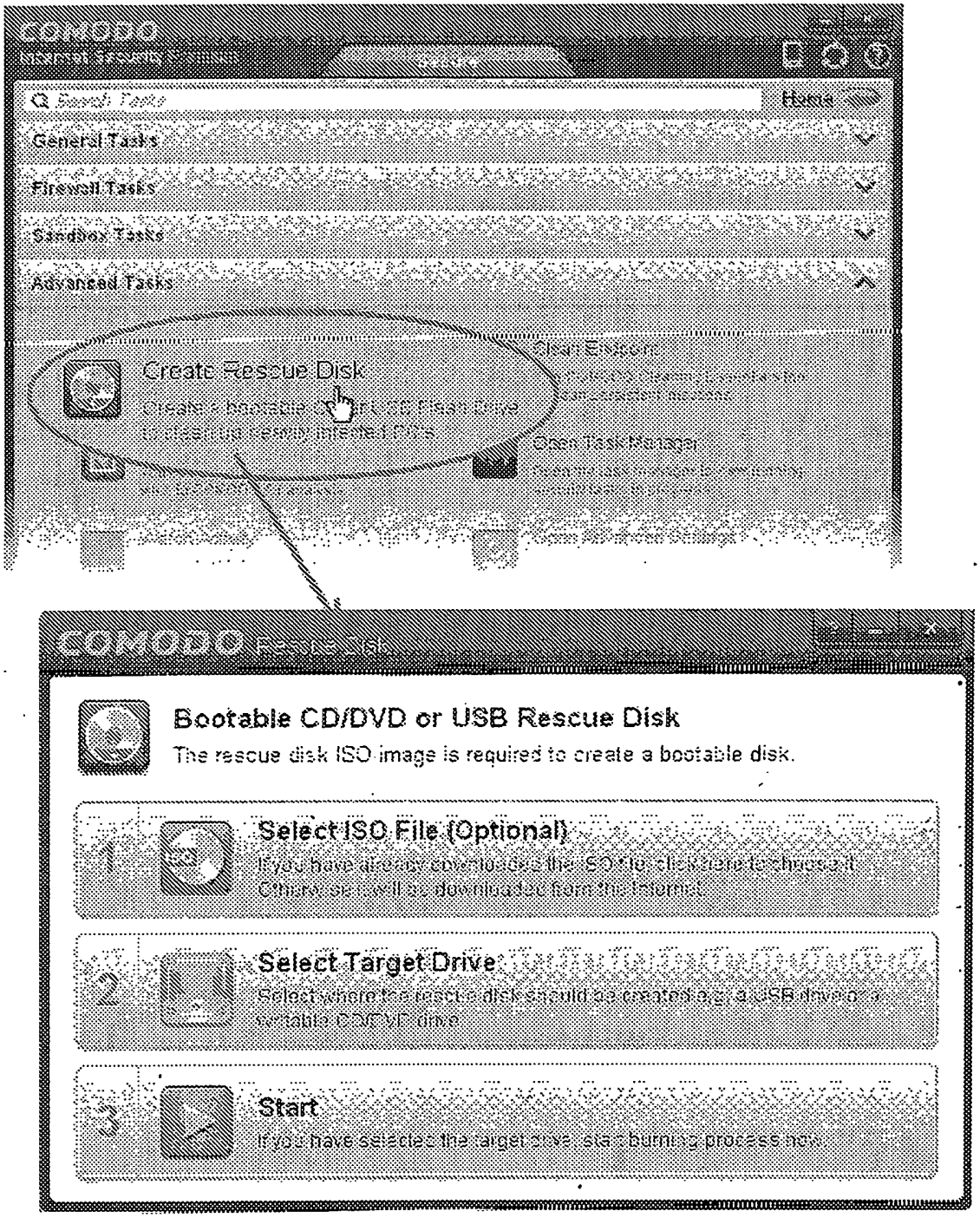
Some of these utilities require the download and installation of additional setup files. After installation, the utility will start directly next time you click the button.




# 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

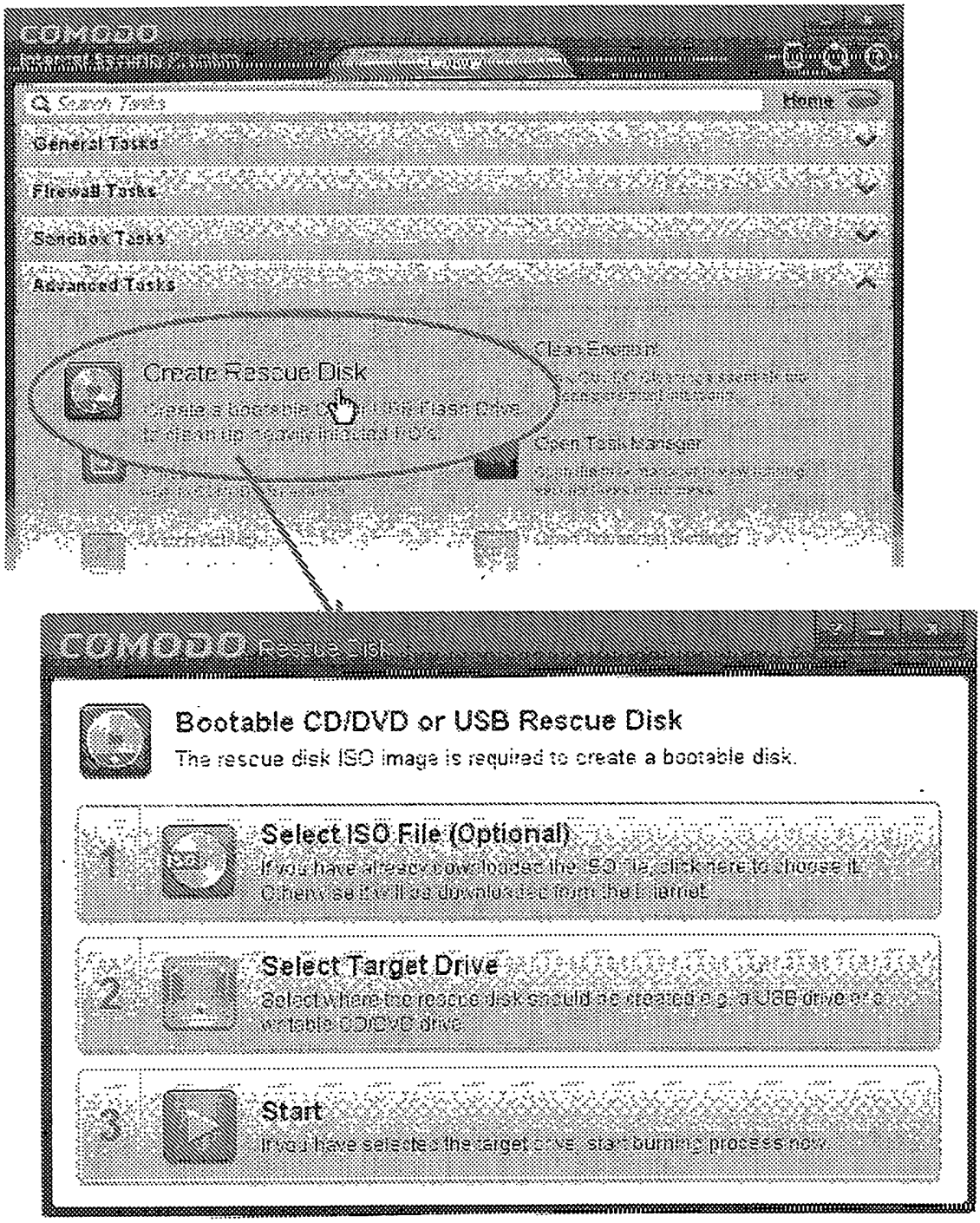



After you have burned the ISO, you need to boot your system to the rescue disk in order to use the scanner in your pre-boot environment.

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

## 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 .isc 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.

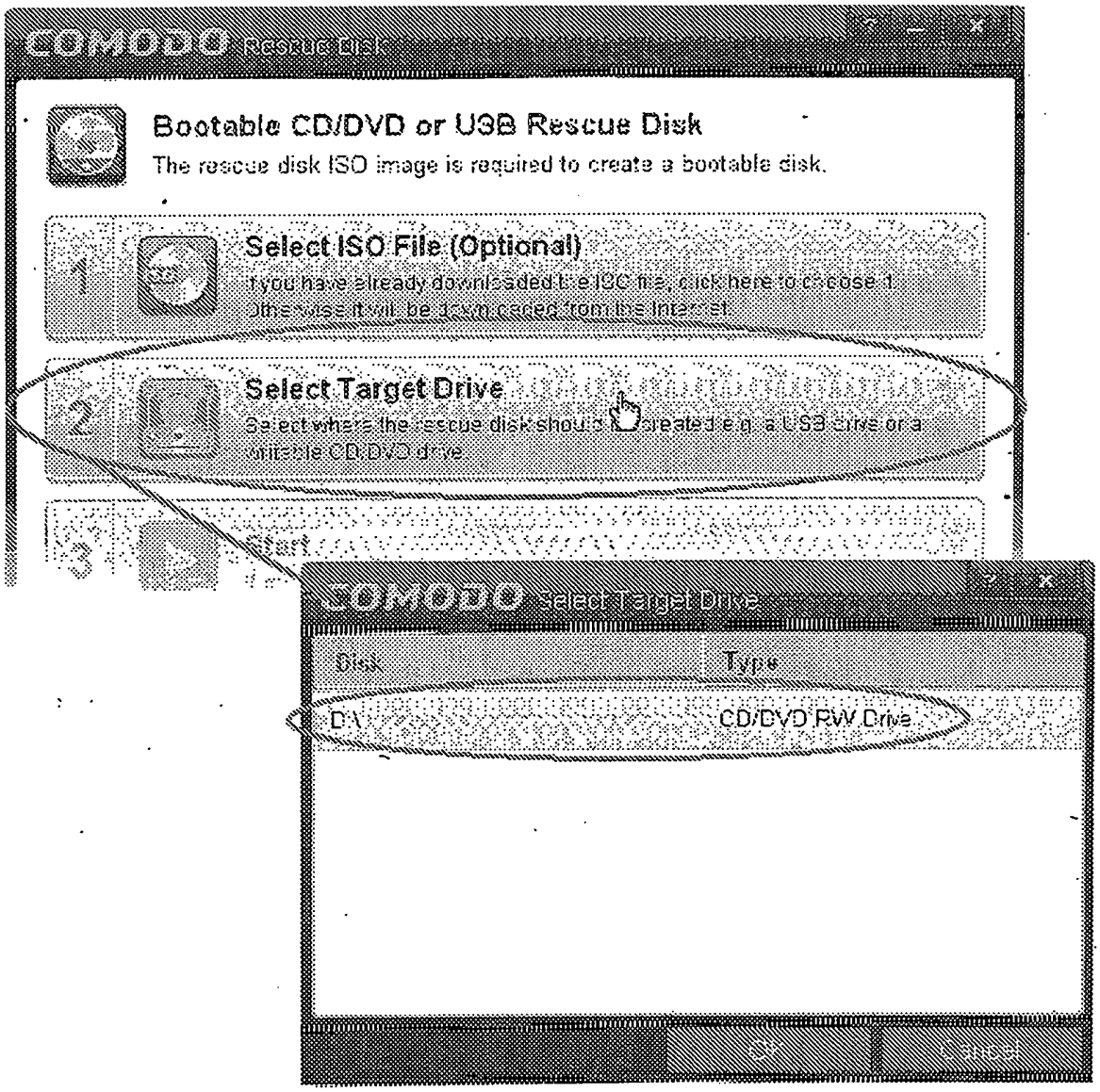
- Click Select ISO File (Optional) and navigate to the comodo_rescue_disk.iso file

Step 2 Select target drive

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

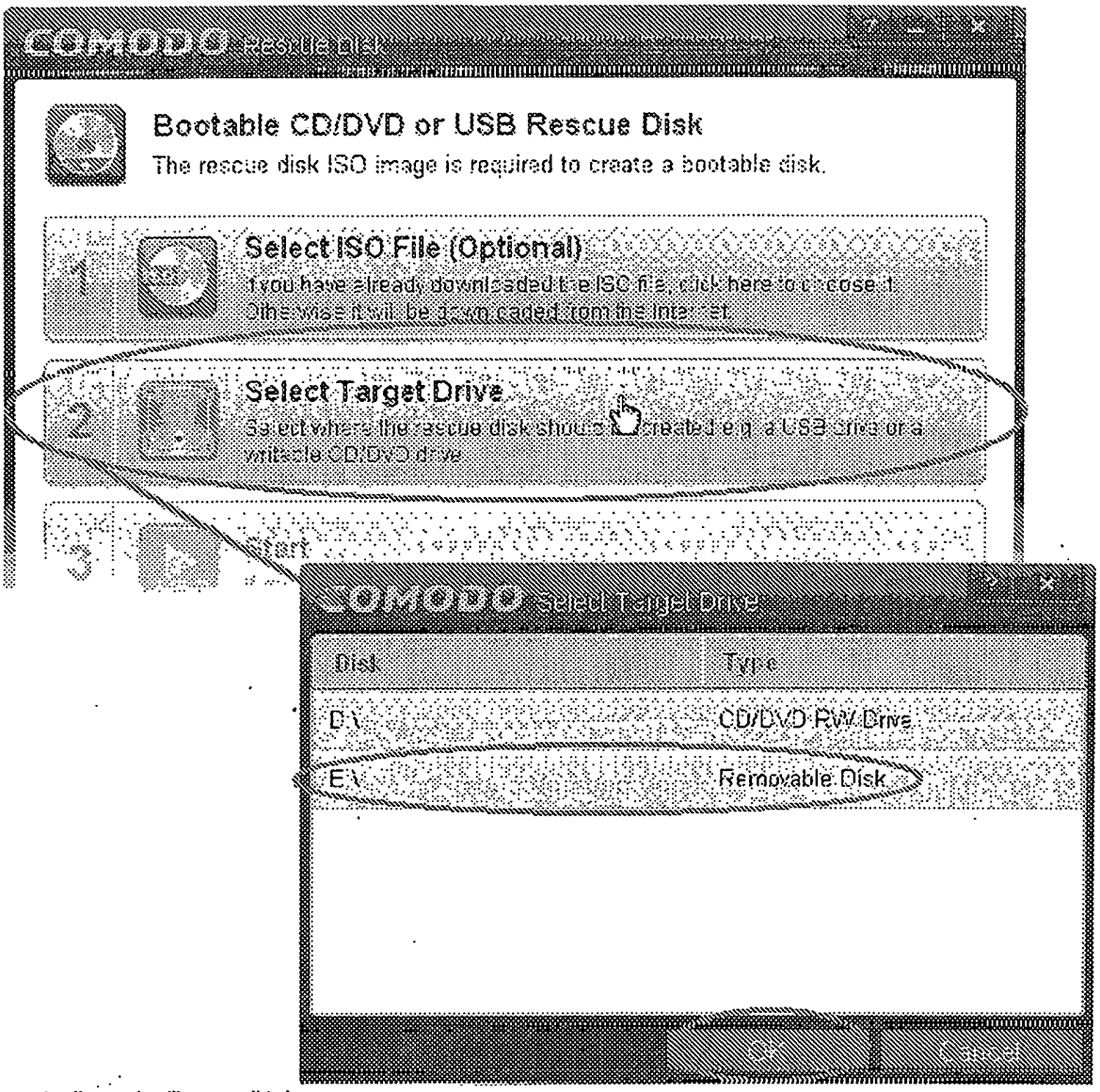
**To burn the Rescue disk on a CD or a DVD**

- 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



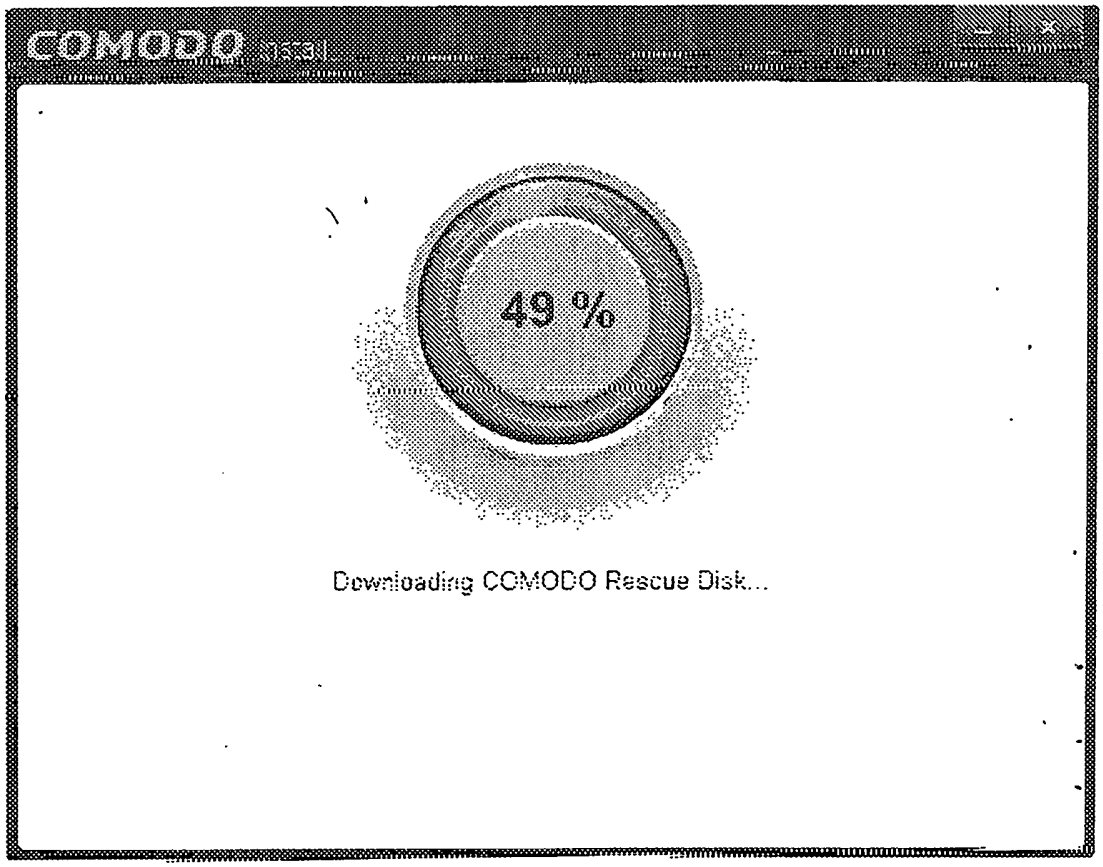

**To burn the Rescue disk on a USB Drive**

- 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

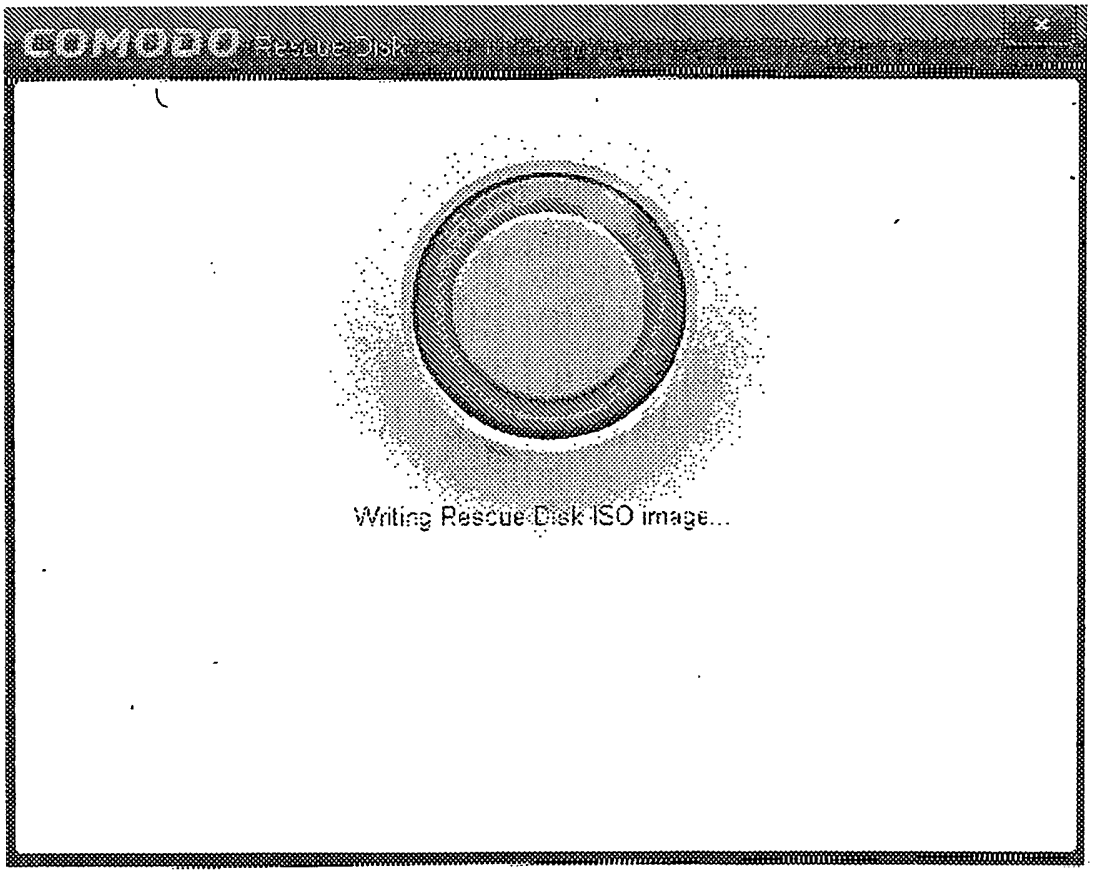



Step 3 - Burn the Rescue Disk

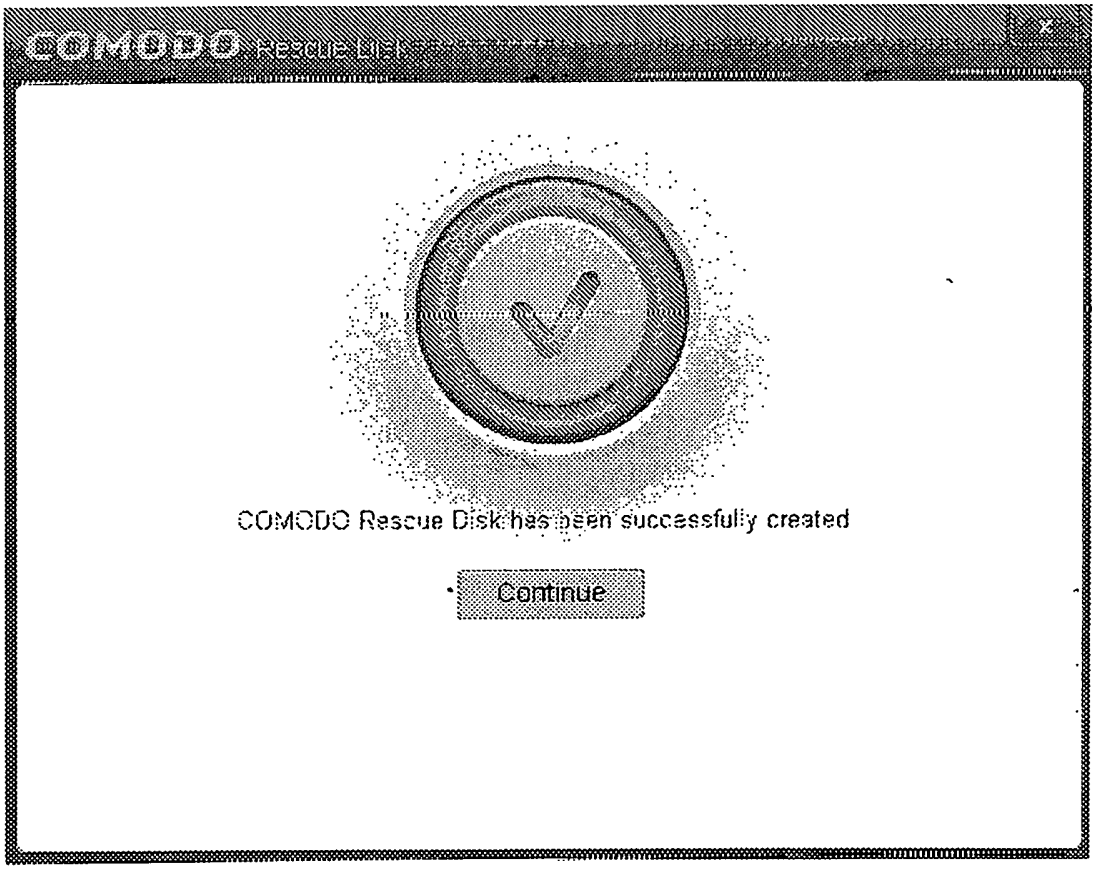
- After you selected the target drive, click 'Start'. If you have selected an .iso file from your hard disk, the burning of the disk will start immediately. Else, the .iso file will be downloaded from Comodo Servers.




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:

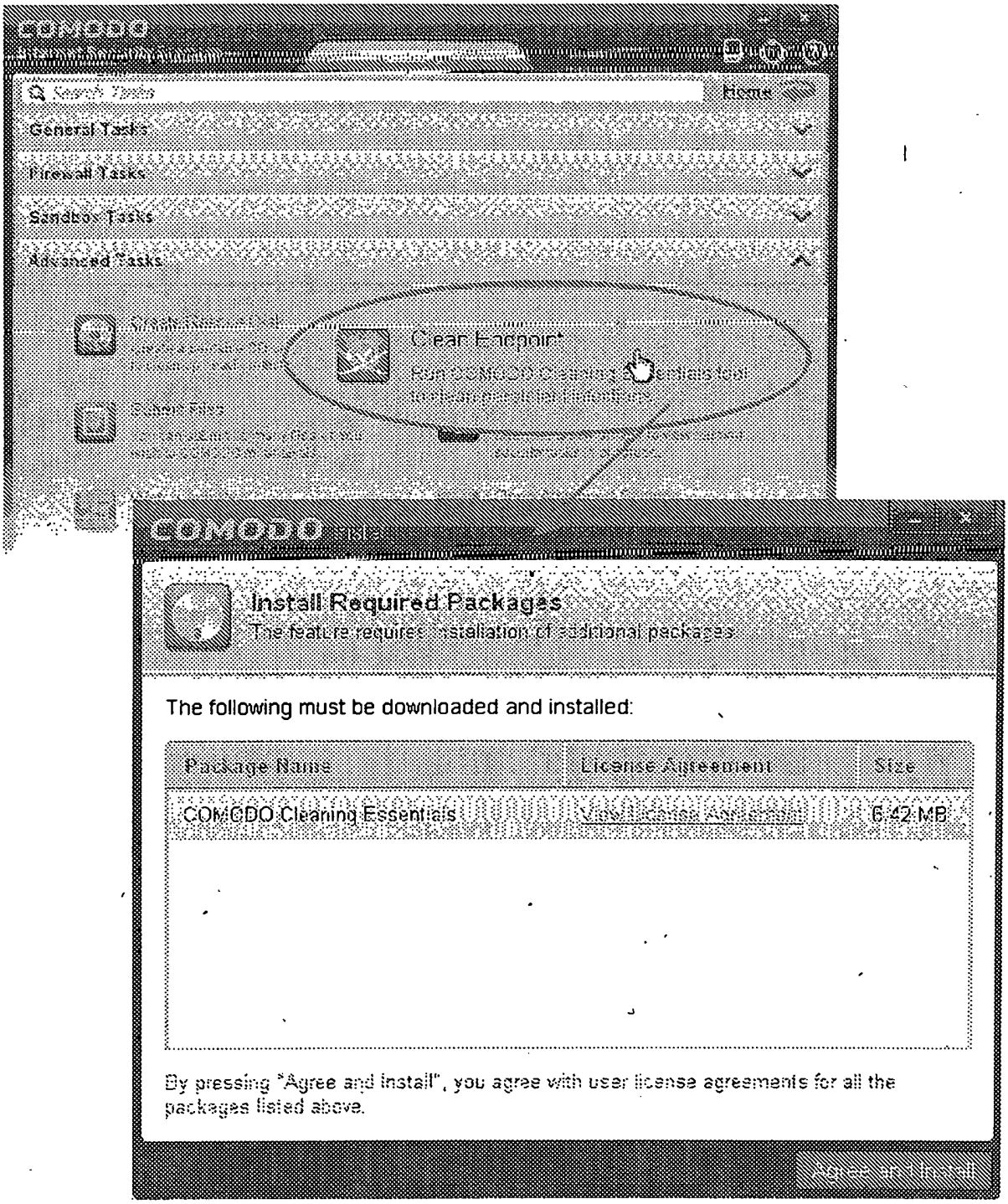
- **KillSwitch** - an advanced system monitoring tool that allows users to identify, monitor and stop any unsafe processes that are running on their system.
- **Malware scanner** - Fully customizable scanner capable of unearthing and removing viruses, rootkits, hidden files and malicious registry keys 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.

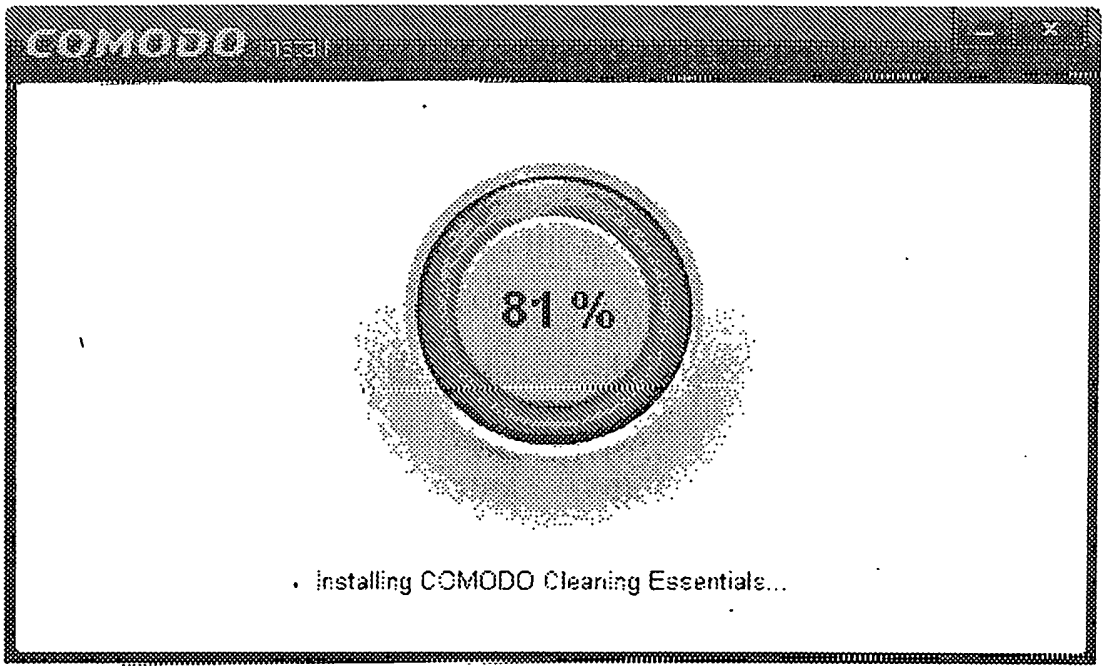
For more details on the features and usage of the application, please refer to the online guide at http://help.comodo.com/topic-119-1-328-3516-Introduction-to-Comodo-Cleaning-Essentials.html.

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

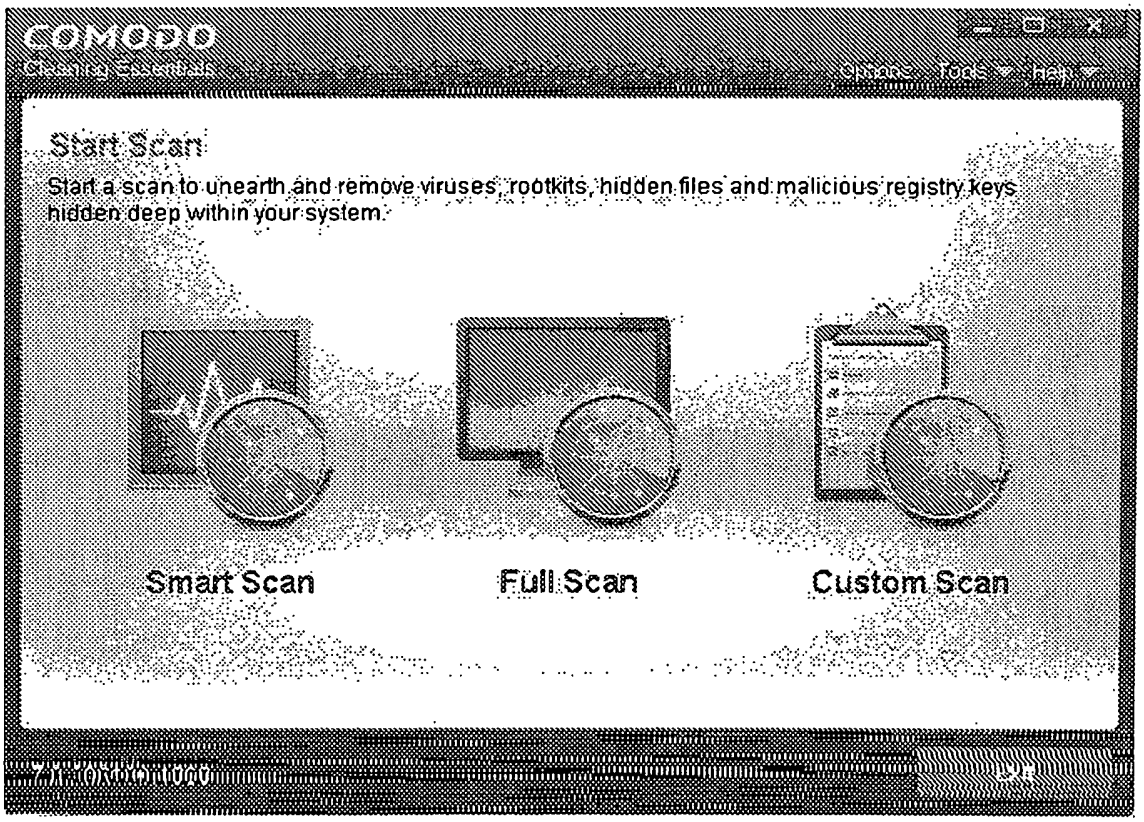
- Clicking the 'Clean Endpoint' for the first time, CIS will download and install Comodo Cleaning Essentials. Once installed, clicking this button in future will open the CCE interface.




- 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.



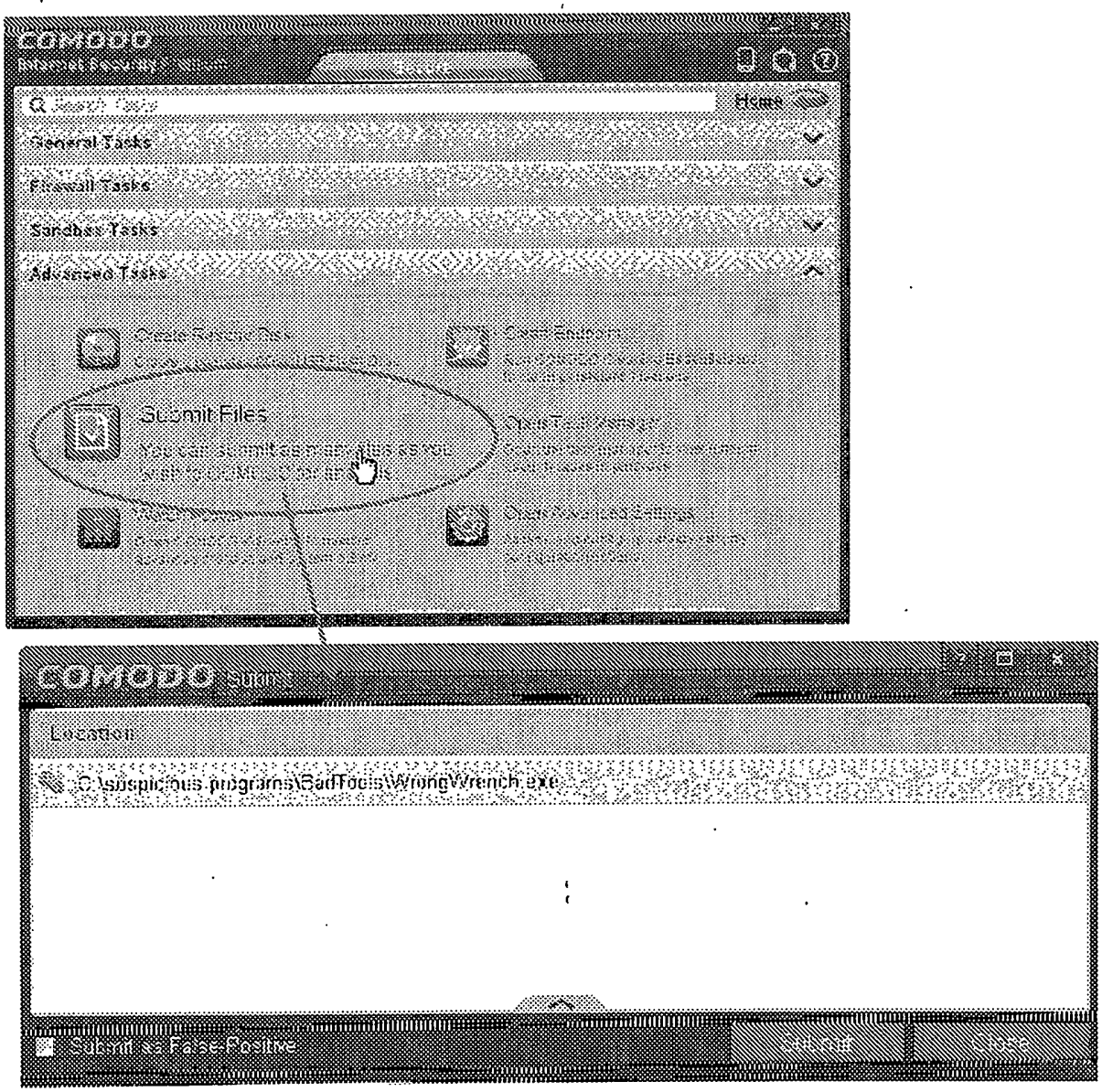

- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at http://help.comodo.com/topic-115-1-328-3525-The-Main-Interface.html
- On clicking the 'Clean Endpoint' button from next time onwards, Comodo Cleaning Essentials will be opened.

# 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'

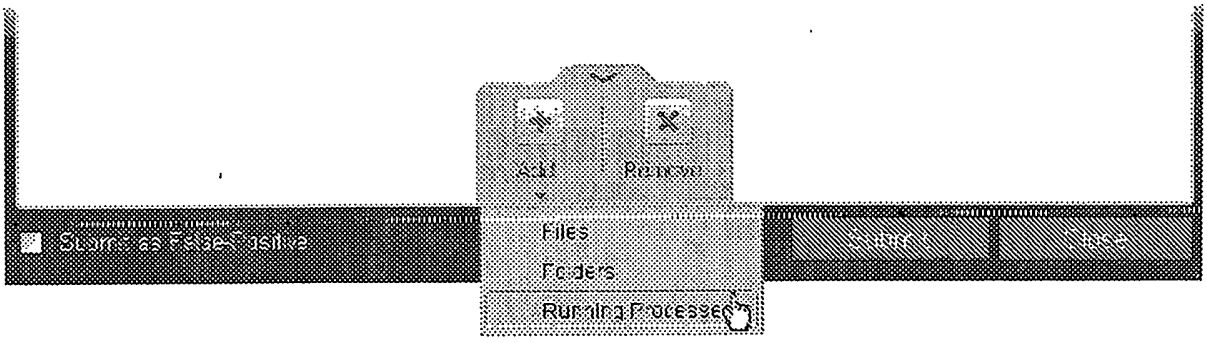



Clicking the handle at the bottom center of the panel opens the following options:

- 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:

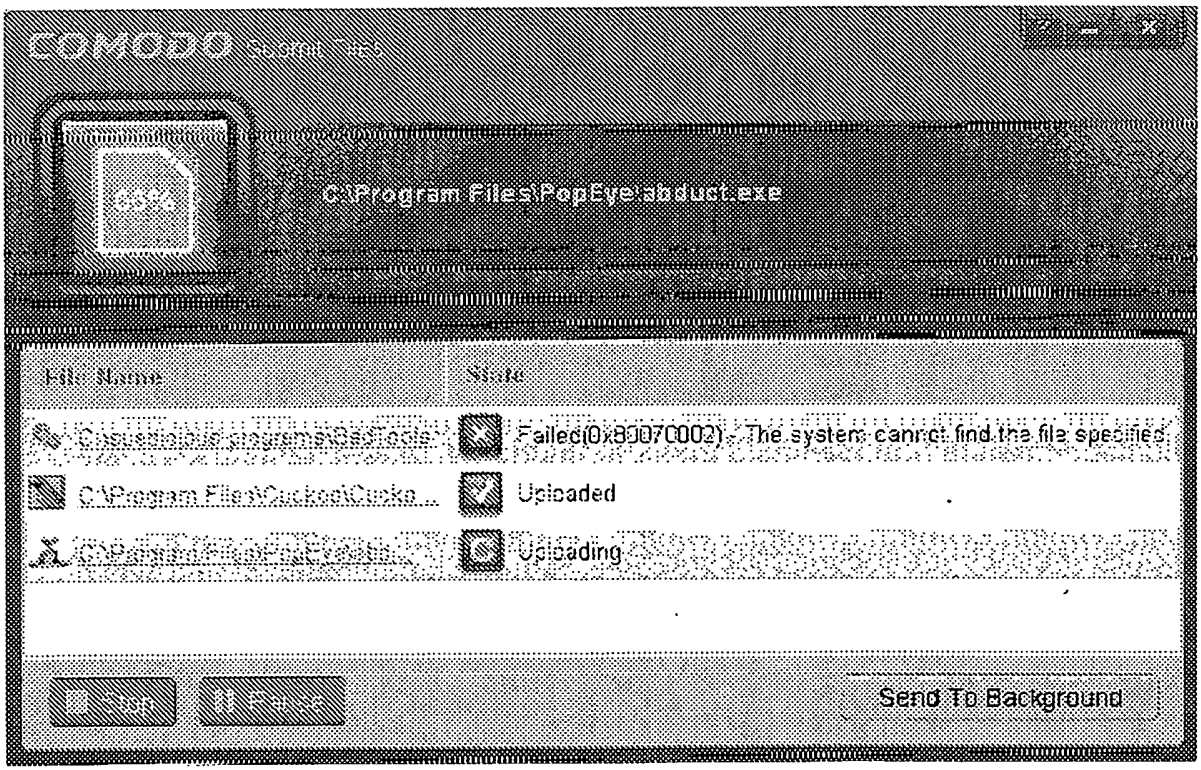
- **Files** - Allows you to navigate to the file or executable of the program you wish to add.
- **Folders** - Allows you to navigate to the folder you wish to add. All the files in the folder will be added to the 'Trusted Files' list.
- **Running Processes** - Allows you to select a currently running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

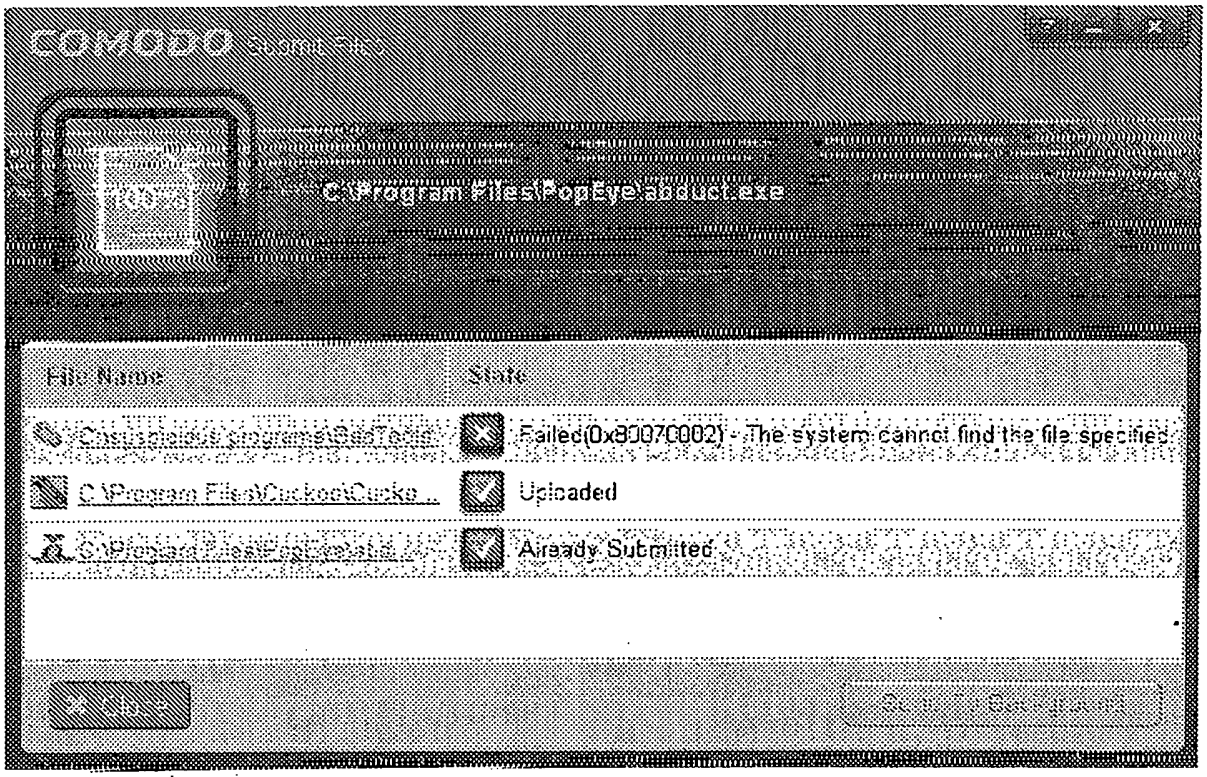
The files will be submitted and the progress will be displayed




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).

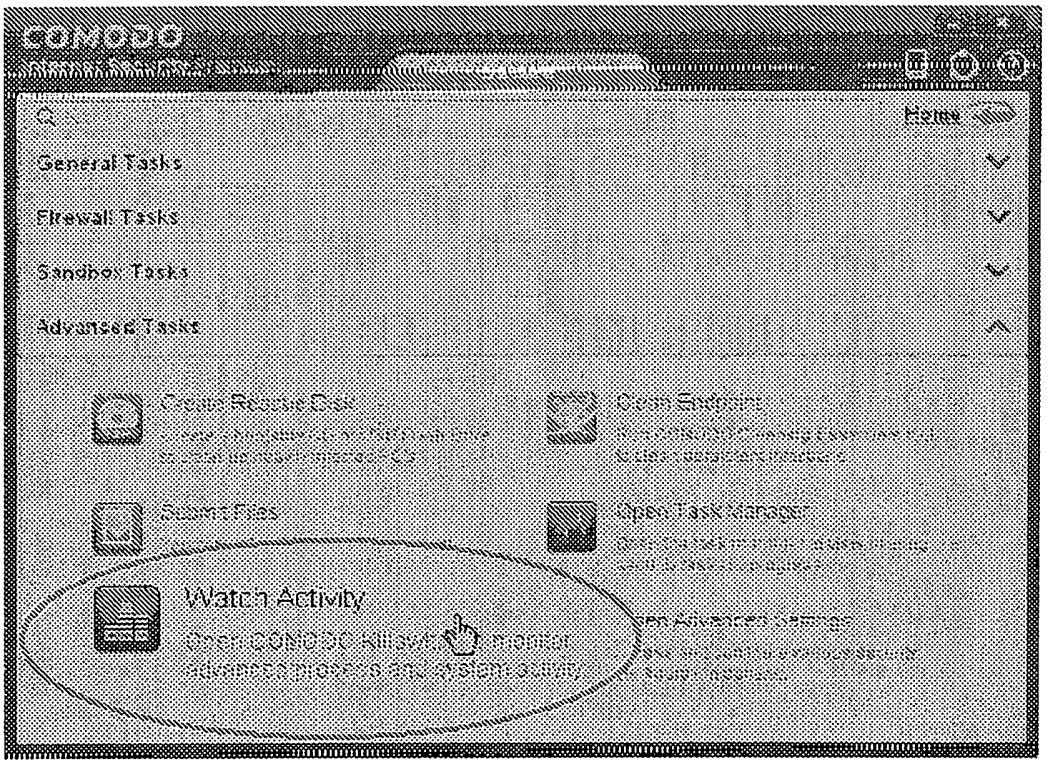
The list of files submitted from your computer can be viewed from the Submitted Files interface.

# 5.4. Identify and Kill Unsafe Running Processes

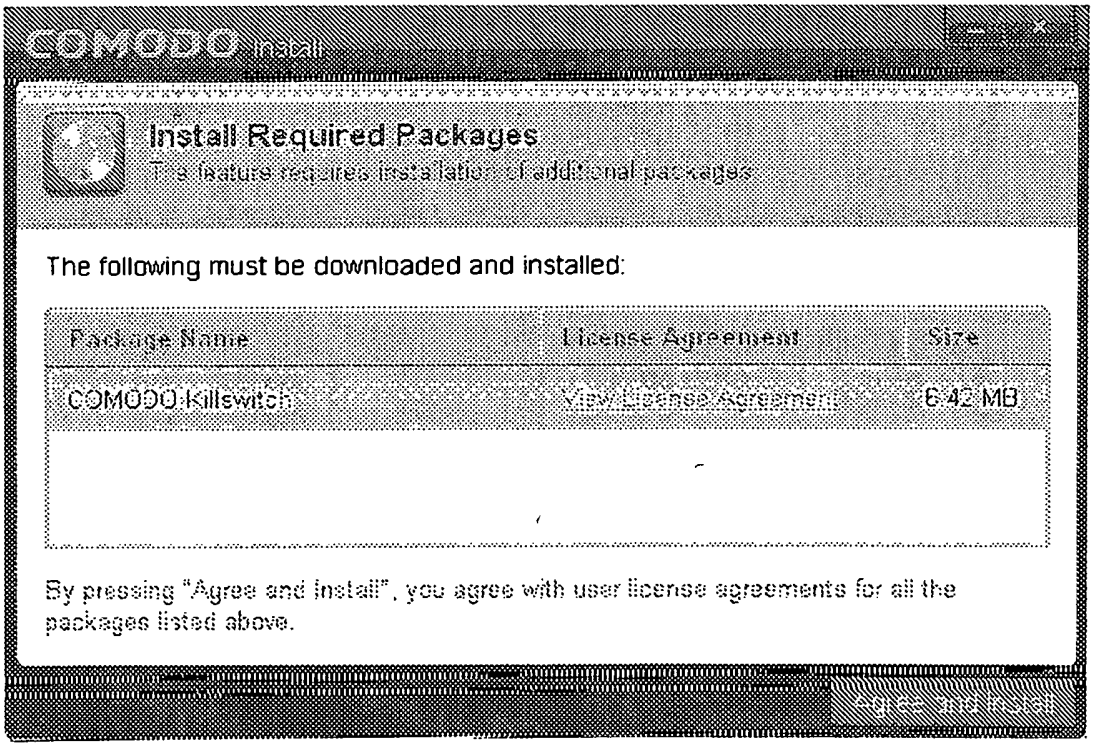
Comodo KillSwitch is an advanced system monitoring tool that allows users to quickly identify, monitor and terminate any unsafe processes that are running on their system. Apart from offering unparalleled insight and control over computer processes, KillSwitch provides you with yet another powerful layer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

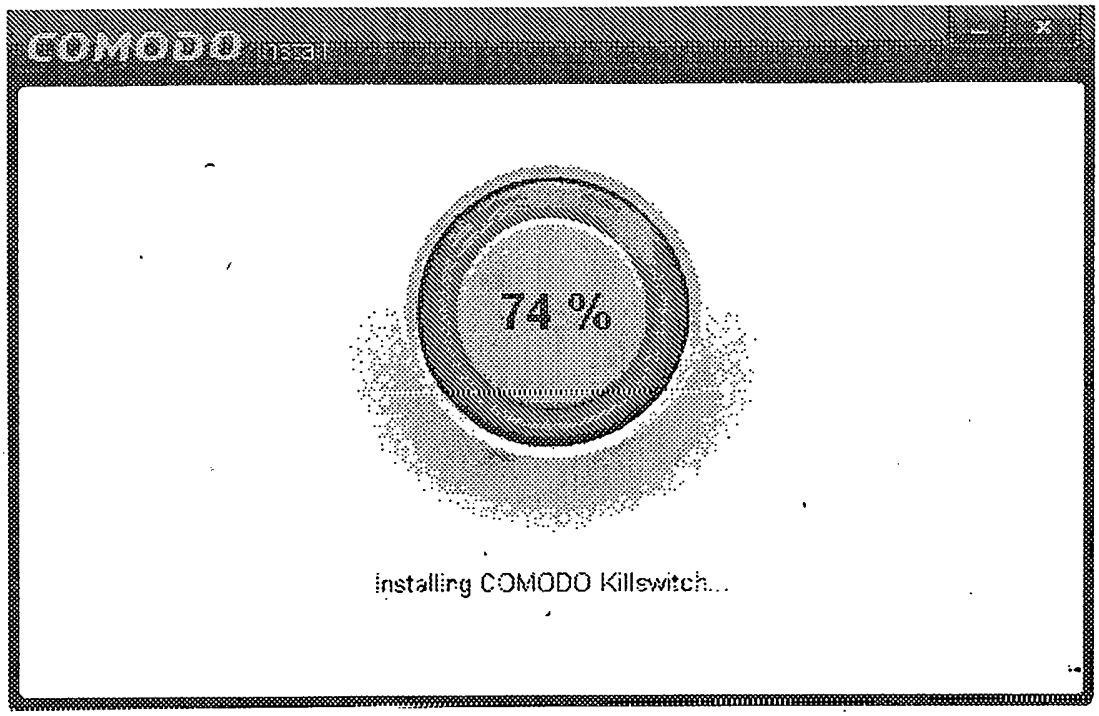
Comodo KillSwitch can be directly accessed from the CIS interface by clicking the 'Watch Activity' button in the 'Advanced Tasks' interface.



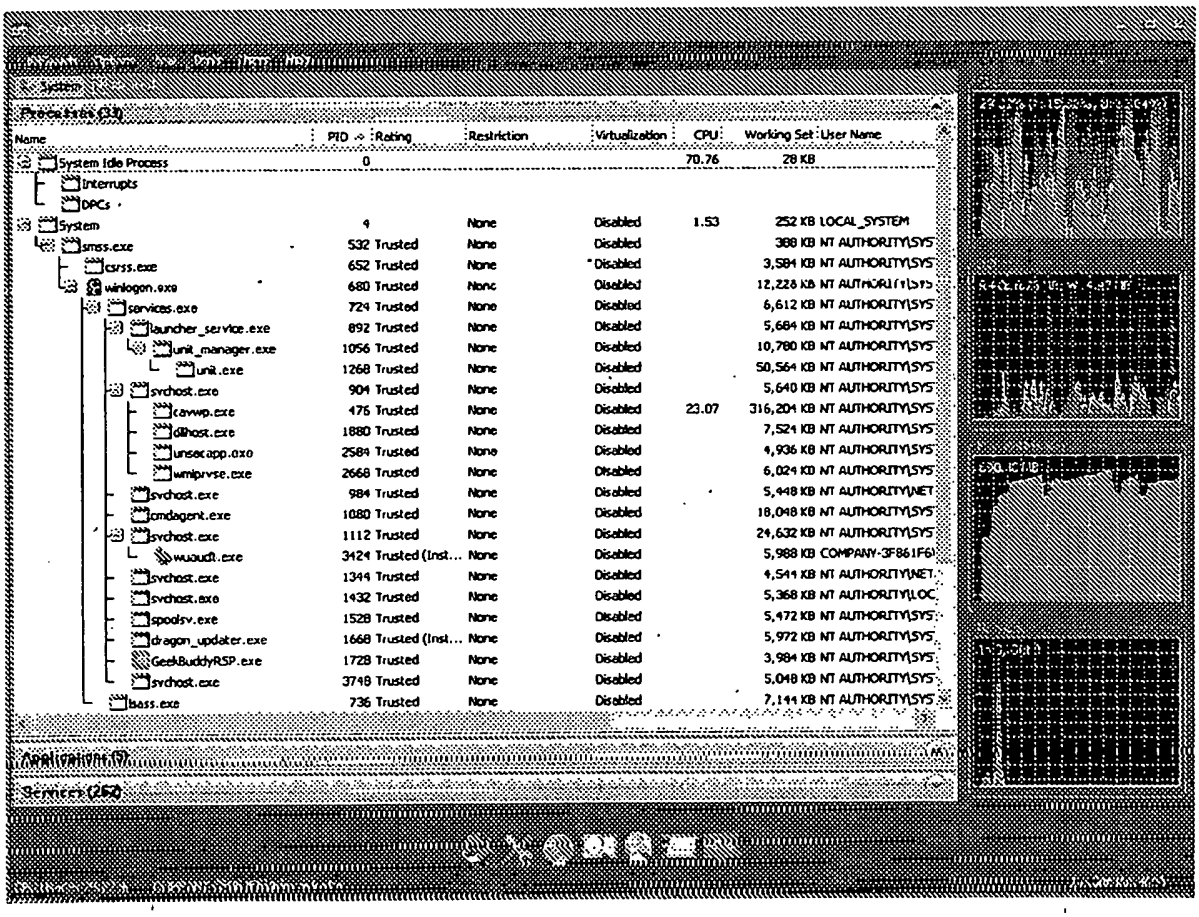

- Killswitch is a component of Comodo Cleaning Essentials. If you have already installed Comodo Cleaning Essentials by clicking 'Clean Endpoint' from the 'Advanced Tasks' interface, clicking the 'Watch Activity' will open the KillSwitch interface directly. Refer to the section Remove Deeply Hidden Malware 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.

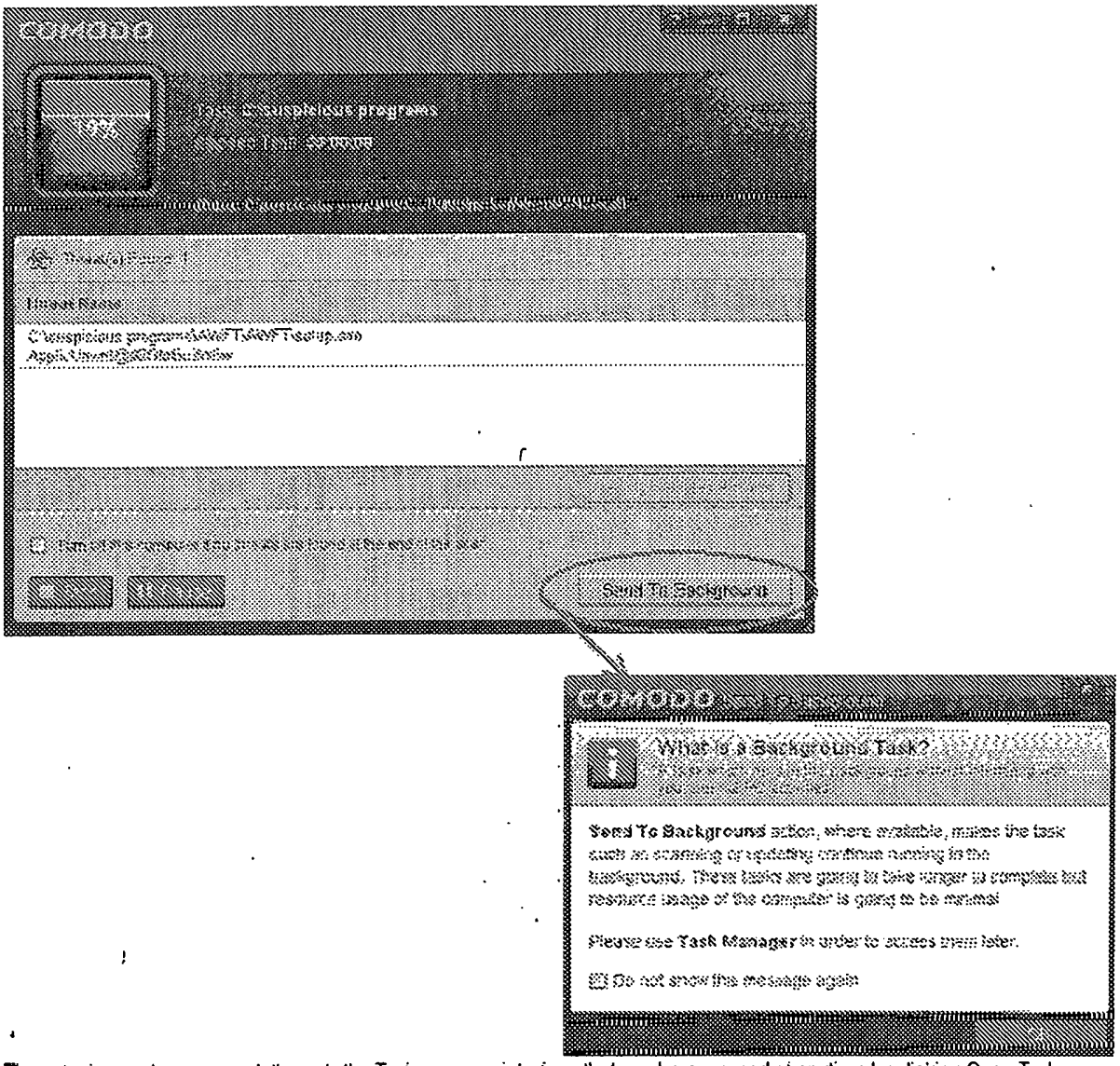


On clicking the 'Watch Activity' button from next time onwards, Comodo Killswitch will be opened.

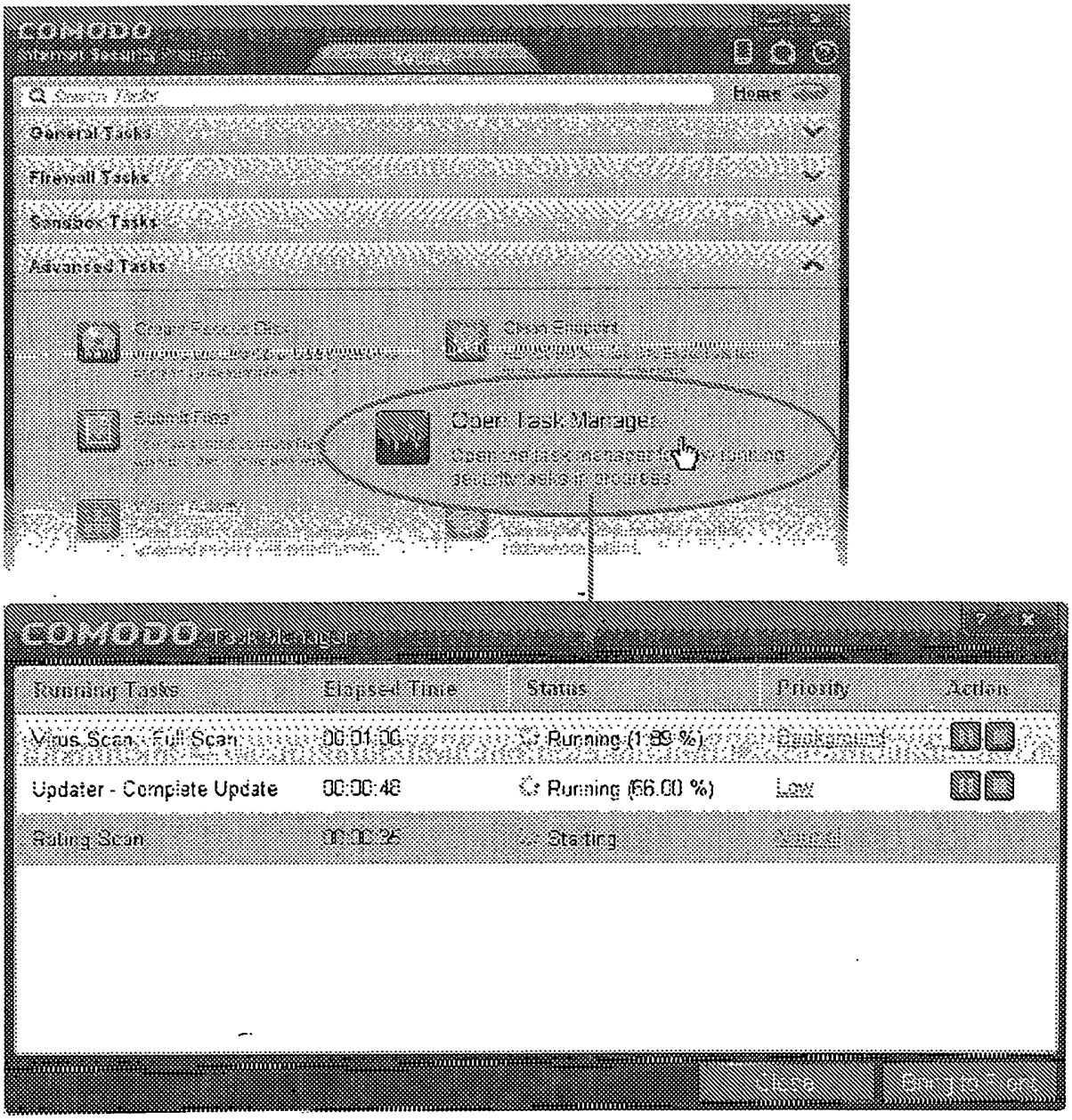
- Details of how to use KillSwitch to monitor and terminate unsafe process from the main interface can be found at http://help.comodo.com/topic-119-1-328-3529-The-Main-Interface.html

# 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:

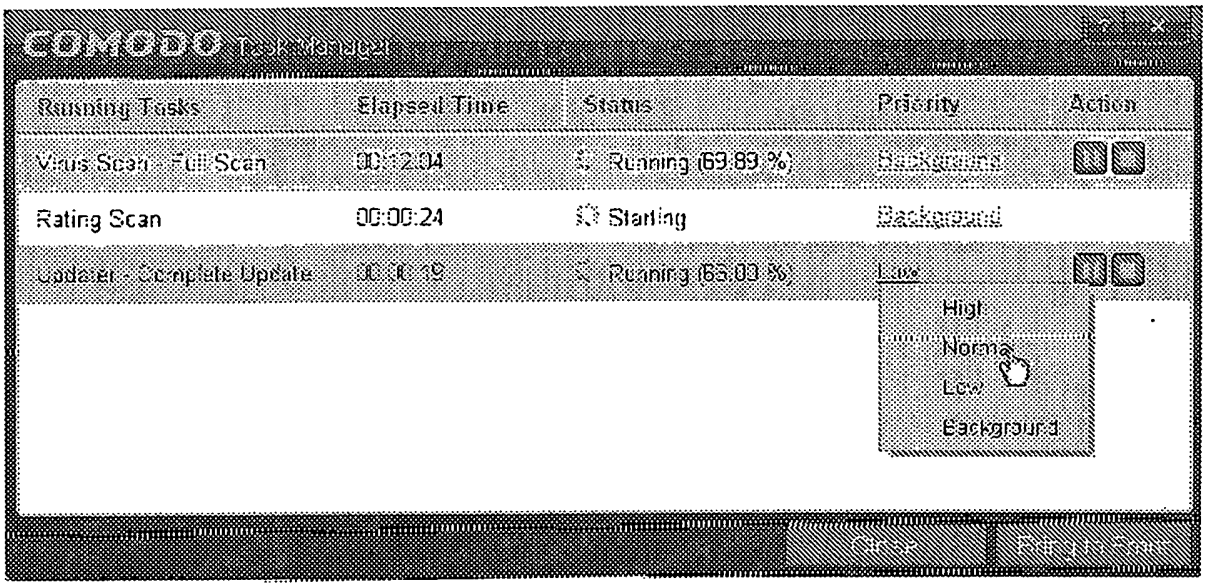
- Reassign priorities to the tasks
- Pause/Resume or Stop a running task
- Bring a selected task to foreground

## 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**

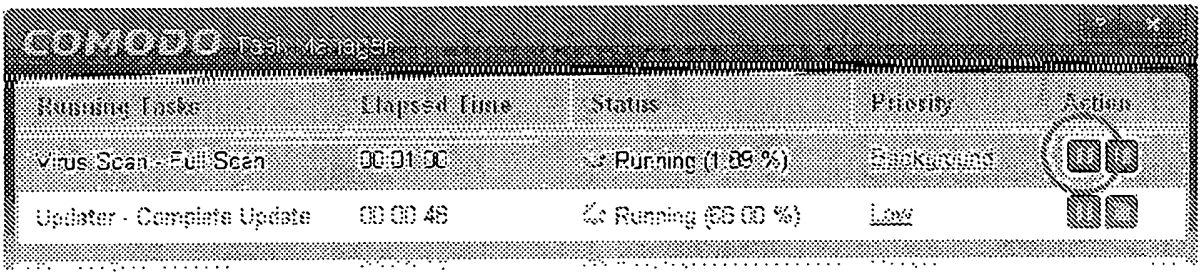
- Click on the current priority and select the priority you want to assign from the options.



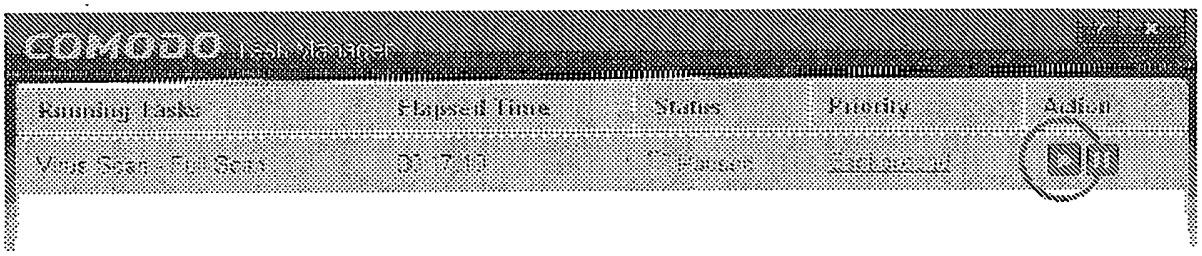

Pausing/Resuming or Stopping running tasks

The Action column displays the Pause/Resume and Stop buttons

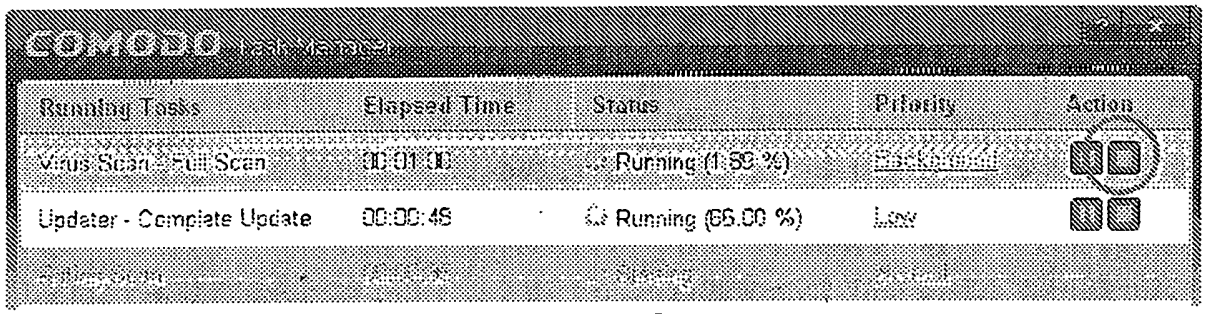
- To pause a running task, click the Pause button




- To resume a paused task, click the Resume button

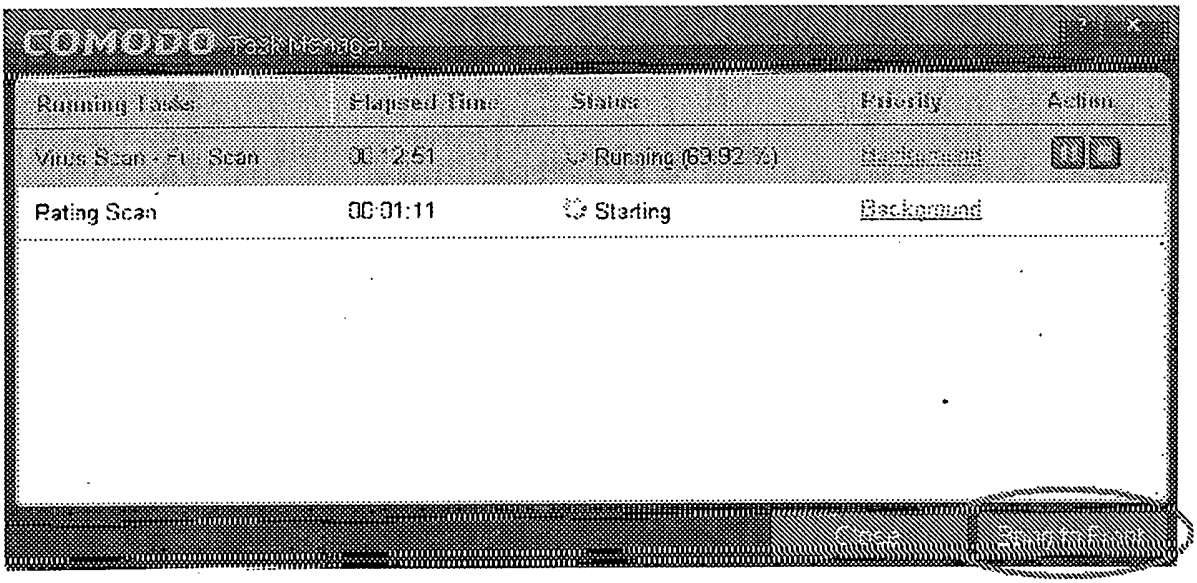



- To stop a running task, click the stop button

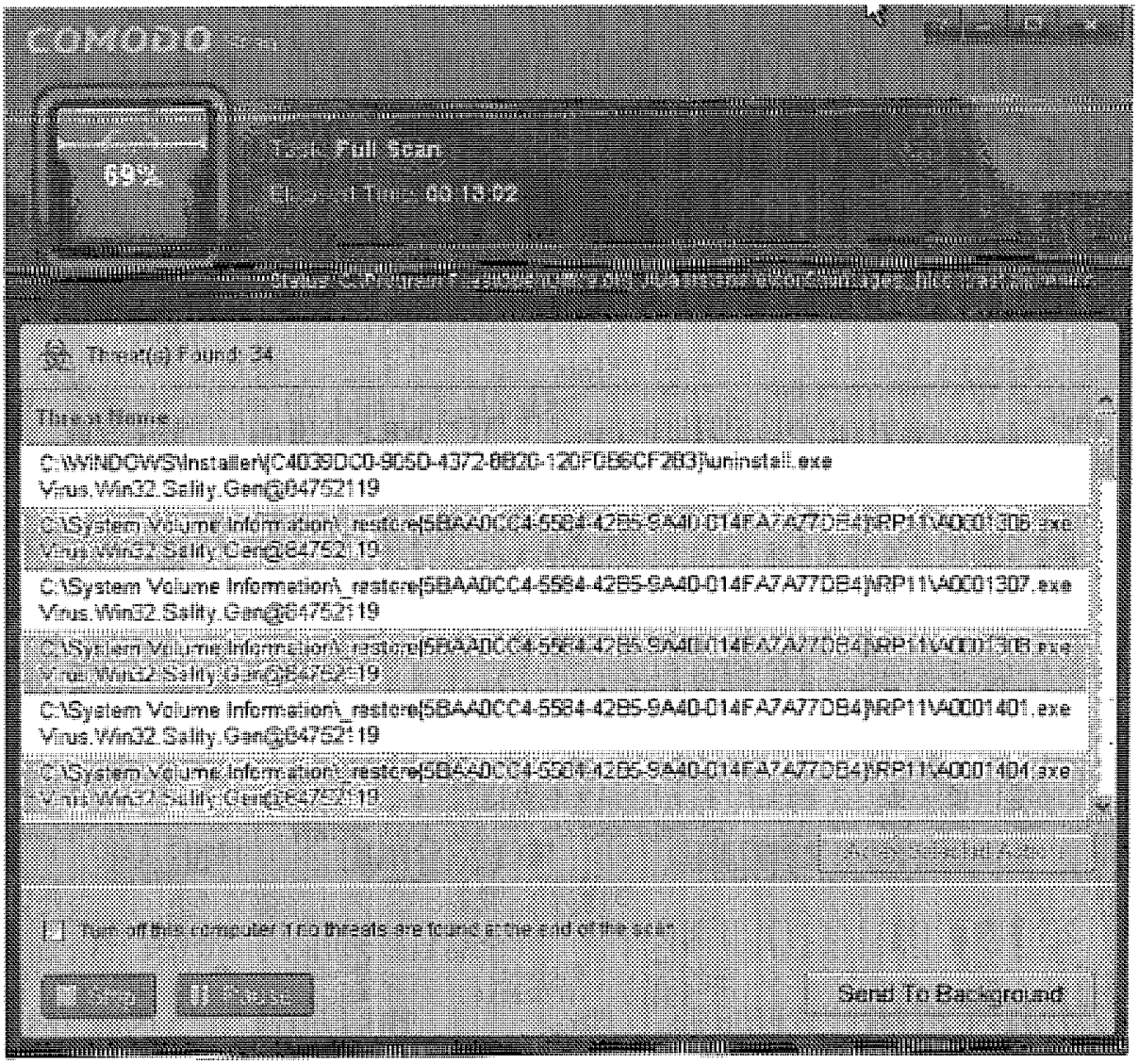



Bringing a running task to foreground

- 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.

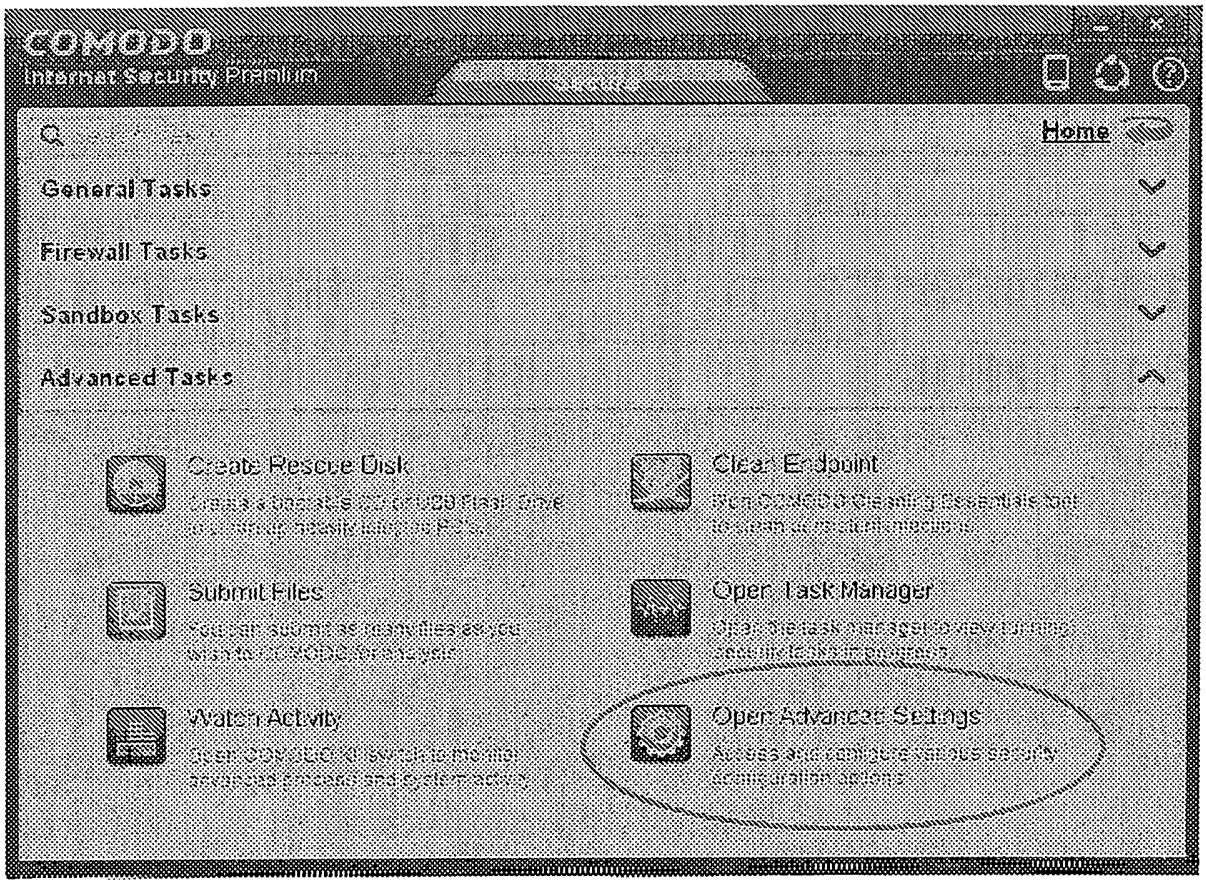



# 6. Advanced Settings

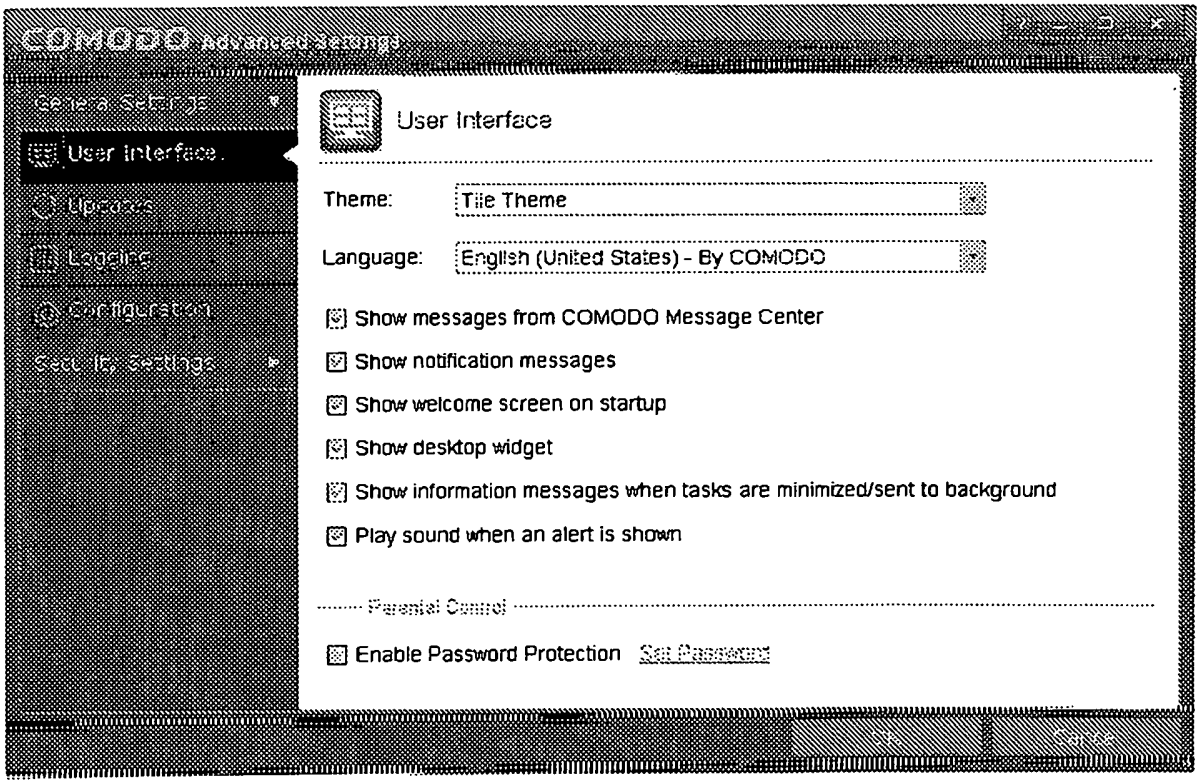
The 'Advanced Settings' area allows you to configure every aspect of the operation, behavior and appearance of Comodo Internet Security. The 'General Settings' section lets you specify top-level preferences regarding the interface, updates and event logging. The 'Security Settings' section lets advanced 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 virus exclusions, 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:

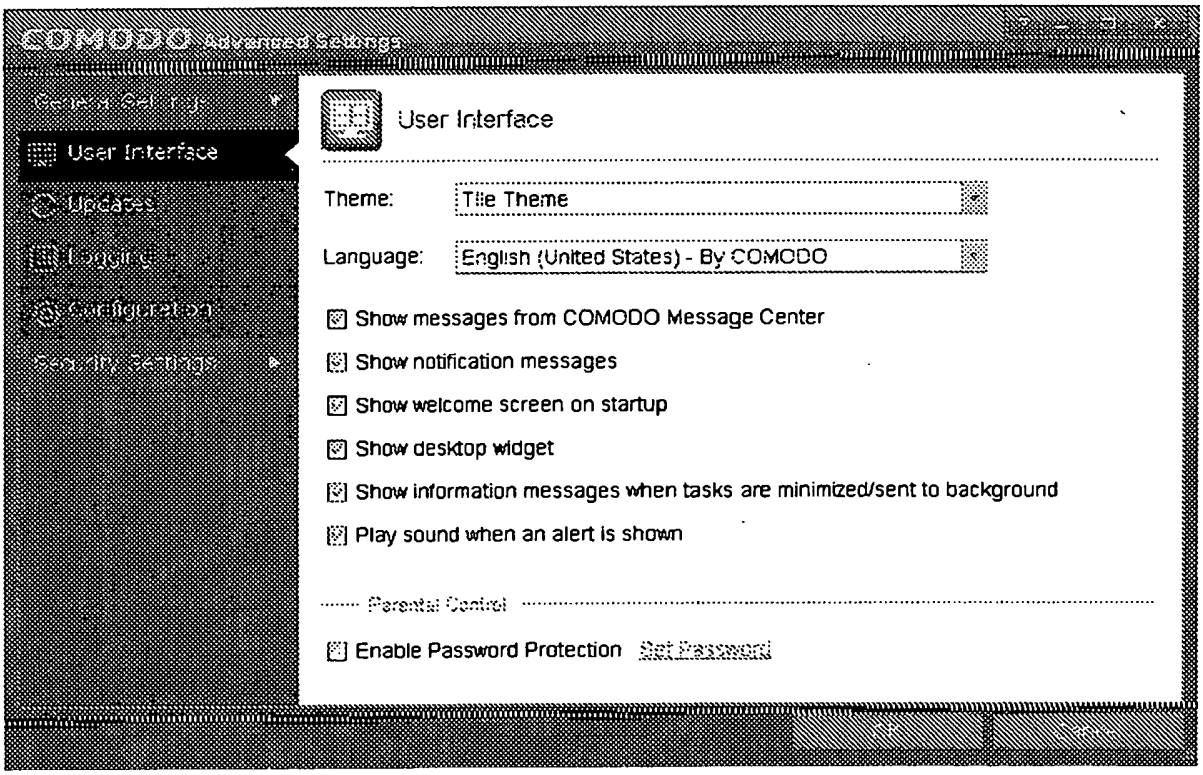
- General Settings - Allows you to configure the appearance and behavior of the application

- 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.

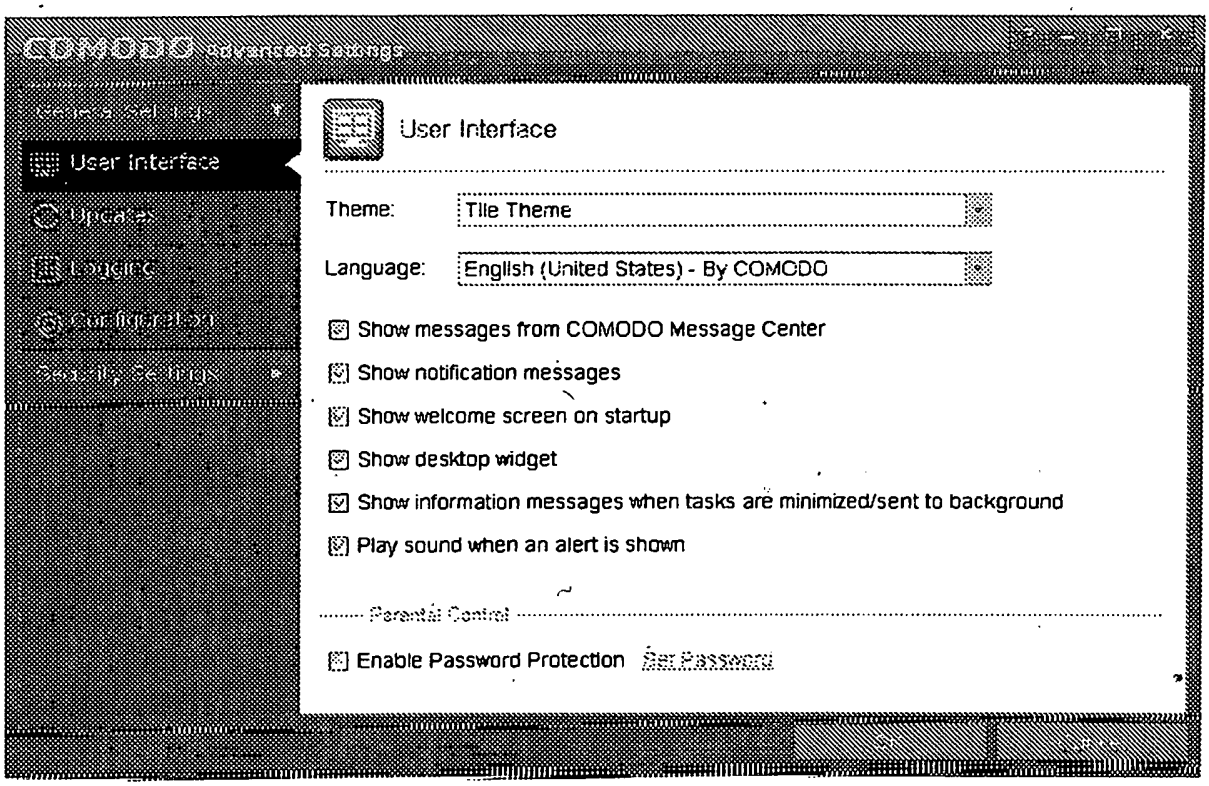



The category has the following settings:

- User Interface
- Updates
- Logging
- Configuration

## 6.1.1. Customize User Interface

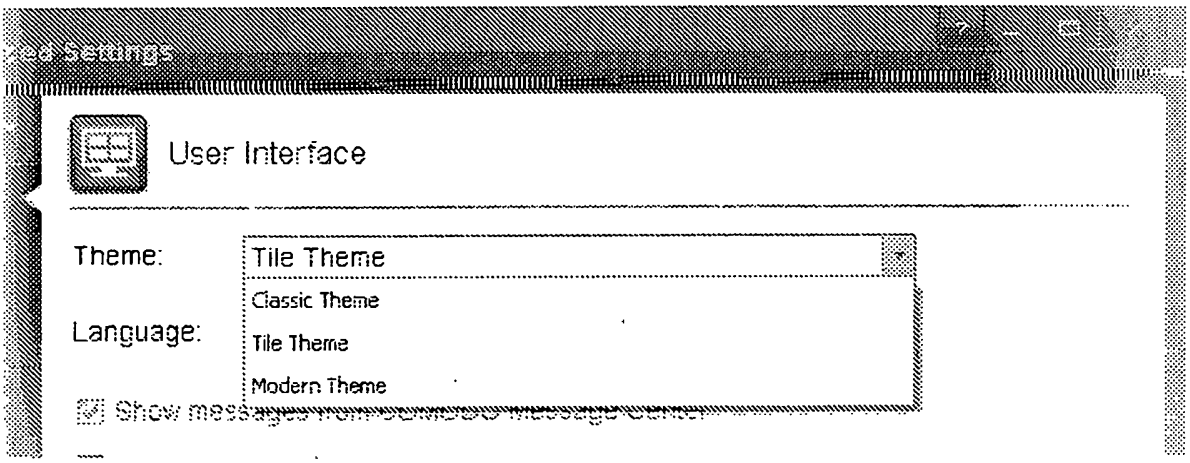
The 'User Interface' tab lets you choose the display theme, interface language and customize the look and feel of Comodo Internet Security according to your preferences. You can also configure how messages are displayed and enable password protection for your settings.



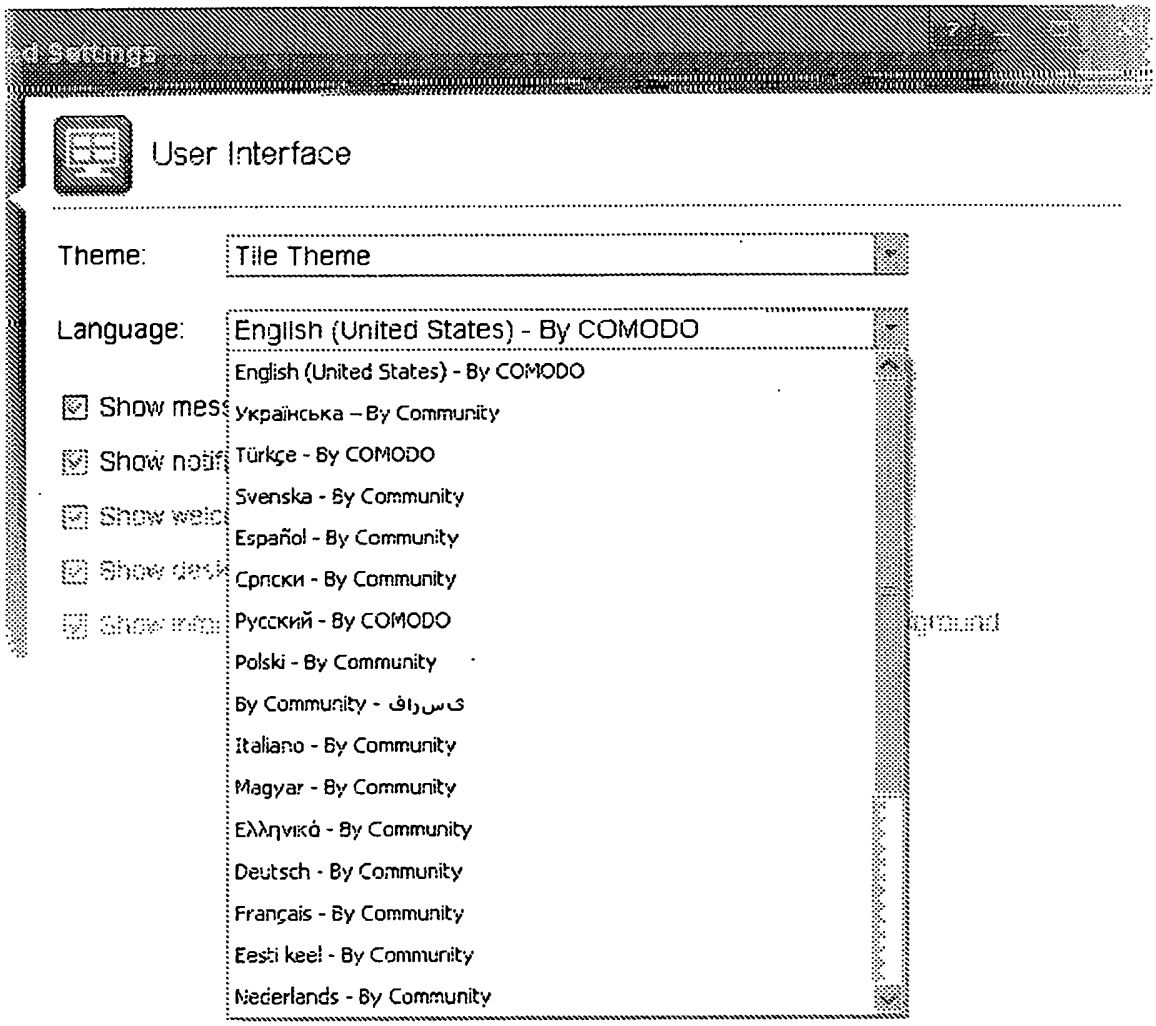

The User Interface Settings allows you configure the following:

- 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

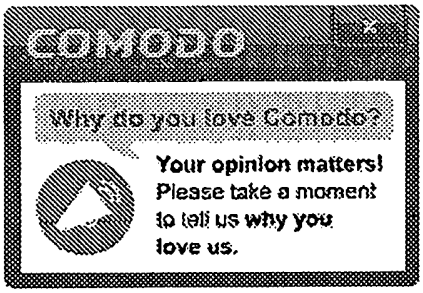
- **Theme** - The 'Themes' drop-down allows you to choose the colors and appearance of the GUI as you prefer (***Default = Tile Theme***).



- **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 .